

運用・管理

| | |
|------------------------------|----|
| システム | 10 |
| ログイン | 10 |
| 再起動 | 10 |
| システム時計の設定 | 11 |
| システム名の設定 | 12 |
| システムチェック | 13 |
| 記憶装置とファイルシステム | 14 |
| 物理デバイス | 14 |
| NVS (Non-Volatile Storage) | 14 |
| フラッシュメモリー | 14 |
| ファイルシステム | 15 |
| ファイル名 | 15 |
| ワイルドカード | 17 |
| ファイルの操作 | 18 |
| コンフィグレーション | 22 |
| 設定の保存と復元 | 22 |
| コマンドプロセッサ | 24 |
| ログイン | 24 |
| コマンドプロンプト | 24 |
| コマンドライン編集キー | 25 |
| コマンド入力時の注意事項 | 25 |
| コンソールメッセージ | 26 |
| コマンド入力補助機能 | 27 |
| 入力候補の表示 | 28 |
| キーワードの補完 | 31 |
| パラメーター値の説明 | 31 |
| オンラインヘルプ | 32 |
| 端末画面のページ当たり行数 | 33 |
| エイリアス (別号) | 33 |
| ユーザー認証データベース | 35 |
| ユーザーレベル | 35 |
| コマンドプロンプト | 35 |
| デフォルトアカウント | 36 |
| ユーザー認証処理の順序 | 36 |

| | |
|---|----|
| ユーザーアカウントの管理 | 37 |
| 認証サーバー | 39 |
| ユーザー認証処理の順序 | 39 |
| RADIUS サーバー | 39 |
| 本製品がサポートしている RADIUS 属性一覧 | 40 |
| ポート認証 | 42 |
| 概要 | 42 |
| ポート認証方式 (Authenticator) | 43 |
| EAP 認証方式 | 43 |
| 基本設定 | 44 |
| Authenticator | 44 |
| Authenticator (ダイナミック VLAN) | 45 |
| Supplicant | 47 |
| 認証サーバー | 47 |
| アップロード・ダウンロード | 49 |
| ダウンロード | 49 |
| ネットワーク経由でのダウンロード | 49 |
| 非同期ポート経由でのダウンロード | 50 |
| アップロード | 51 |
| ネットワーク経由でのアップロード | 51 |
| 非同期ポート経由でのアップロード | 51 |
| ソフトウェア | 52 |
| ファイル名 | 52 |
| ファームウェアファイル (リリースファイル) | 52 |
| パッチファイル | 52 |
| セットアップツールにおけるバージョン表記 | 52 |
| ファームウェアファイル (リリースファイル) の有効化 | 53 |
| インストール (ファームウェア構成) 情報 | 53 |
| フィーチャー (追加機能) ライセンス | 54 |
| メール送信 | 55 |
| 基本設定 | 55 |
| メール機能の使用例 | 55 |
| セキュリティ | 58 |
| セキュリティモード / ノーマルモード | 58 |
| モードの変更 | 61 |
| Remote Security Officer (RSO) | 62 |
| Manager レベルでのセキュリティタイマー | 63 |
| ログ | 64 |
| デフォルトのログ設定 | 64 |
| ログの閲覧 | 65 |
| ログ設定のカスタマイズ手順 | 65 |
| ログ出力先の定義 | 66 |

| | |
|---|-----|
| メッセージフィルターの追加 | 67 |
| ログ設定の確認 | 68 |
| 設定例 | 69 |
| syslog サーバーへのログ転送 | 69 |
| メール送信 | 69 |
| 資料編 | 70 |
| メッセージフォーマット | 70 |
| ログレベル | 71 |
| ログフィルターの条件指定に使える比較演算子 | 71 |
| モジュール ID とモジュール名 | 73 |
| タイプ/サブタイプ | 76 |
| syslog 形式への変換 | 88 |
| スクリプト | 90 |
| トリガー | 92 |
| SNMP | 94 |
| SNMPv1/SNMPv2c | 94 |
| 基本設定 | 94 |
| その他 | 95 |
| SNMPv3 | 96 |
| 基本設定 | 96 |
| その他 | 98 |
| SNMPv1/v2c/v3 の共通事項 | 98 |
| NTP | 100 |
| 基本設定 | 100 |
| NTP サーバーとしての動作 | 101 |
| 付録 | 101 |
| 定義済みのタイムゾーン名一覧 | 101 |
| Secure Shell | 103 |
| 基本設定 | 103 |
| 暗号鍵の作成 | 103 |
| SSH サーバーの起動 | 104 |
| SSH ユーザーの登録 | 104 |
| SSH クライアントからの接続 | 107 |
| その他 | 108 |
| コマンドリファレンス編 | 110 |
| 機能別コマンド索引 | 110 |
| ACTIVATE FLASH COMPACTION | 117 |
| ACTIVATE PORTAUTH PORT REAUTHENTICATE | 118 |
| ACTIVATE SCRIPT | 120 |
| ACTIVATE TRIGGER | 121 |
| ADD ALIAS | 122 |
| ADD FILE | 123 |

| | |
|------------------------------------|-----|
| ADD LOG OUTPUT | 126 |
| ADD LOG RECEIVE | 128 |
| ADD NTP PEER | 130 |
| ADD RADIUS SERVER | 131 |
| ADD SCRIPT | 133 |
| ADD SNMP COMMUNITY | 134 |
| ADD SNMP GROUP | 136 |
| ADD SNMP TARGETADDR | 138 |
| ADD SNMP TARGETPARAMS | 140 |
| ADD SNMP USER | 142 |
| ADD SNMP VIEW | 144 |
| ADD SSH USER | 147 |
| ADD TRIGGER | 149 |
| ADD USER | 151 |
| ADD USER RSO | 153 |
| CLEAR FLASH TOTALLY | 155 |
| CLEAR NVS TOTALLY | 156 |
| COPY | 157 |
| CREATE CONFIG | 158 |
| CREATE FFILE | 159 |
| CREATE FILE | 161 |
| CREATE LOG OUTPUT | 164 |
| CREATE SNMP COMMUNITY | 167 |
| CREATE TRIGGER CPU | 169 |
| CREATE TRIGGER FIREWALL | 171 |
| CREATE TRIGGER INTERFACE | 173 |
| CREATE TRIGGER MEMORY | 175 |
| CREATE TRIGGER MODULE | 177 |
| CREATE TRIGGER PERIODIC | 180 |
| CREATE TRIGGER REBOOT | 182 |
| CREATE TRIGGER TIME | 184 |
| DEACTIVATE SCRIPT | 186 |
| DELETE ALIAS | 187 |
| DELETE FFILE | 188 |
| DELETE FILE | 189 |
| DELETE INSTALL | 190 |
| DELETE LOG OUTPUT | 191 |
| DELETE LOG RECEIVE | 192 |
| DELETE MAIL | 193 |
| DELETE NTP PEER | 194 |
| DELETE NVS | 195 |
| DELETE RADIUS SERVER | 196 |

| | |
|--|-----|
| DELETE SCRIPT | 197 |
| DELETE SNMP COMMUNITY | 198 |
| DELETE SNMP GROUP | 199 |
| DELETE SNMP TARGETADDR | 200 |
| DELETE SNMP TARGETPARAMS | 201 |
| DELETE SNMP USER | 202 |
| DELETE SNMP VIEW | 203 |
| DELETE SSH USER | 204 |
| DELETE TRIGGER | 205 |
| DELETE USER | 206 |
| DELETE USER RSO | 207 |
| DESTROY LOG OUTPUT | 208 |
| DESTROY PATCH | 209 |
| DESTROY SNMP COMMUNITY | 210 |
| DESTROY TRIGGER | 211 |
| DISABLE FEATURE | 212 |
| DISABLE HTTP SERVER | 213 |
| DISABLE LOG | 214 |
| DISABLE LOG GENERATION | 215 |
| DISABLE LOG OUTPUT | 216 |
| DISABLE LOG RECEPTION | 217 |
| DISABLE MAIL DEBUG | 218 |
| DISABLE NTP | 219 |
| DISABLE PORTAUTH | 220 |
| DISABLE PORTAUTH DEBUG | 221 |
| DISABLE PORTAUTH PORT | 222 |
| DISABLE RELEASE | 223 |
| DISABLE SNMP | 224 |
| DISABLE SNMP AUTHENTICATE_TRAP | 225 |
| DISABLE SNMP COMMUNITY | 226 |
| DISABLE SNMP COMMUNITY TRAP | 227 |
| DISABLE SSH SERVER | 228 |
| DISABLE SSH USER | 229 |
| DISABLE SYSTEM SECURITY_MODE | 230 |
| DISABLE TELNET SERVER | 231 |
| DISABLE TRIGGER | 232 |
| DISABLE USER | 233 |
| DISABLE USER RSO | 234 |
| DISCONNECT | 235 |
| DUMP | 236 |
| DUMP NVS | 238 |
| EDIT | 240 |

| | |
|---|-----|
| ENABLE FEATURE | 242 |
| ENABLE HTTP SERVER | 243 |
| ENABLE LOG | 244 |
| ENABLE LOG GENERATION | 245 |
| ENABLE LOG OUTPUT | 246 |
| ENABLE LOG RECEPTION | 247 |
| ENABLE MAIL DEBUG | 248 |
| ENABLE NTP | 249 |
| ENABLE PORTAUTH | 250 |
| ENABLE PORTAUTH DEBUG | 251 |
| ENABLE PORTAUTH PORT | 252 |
| ENABLE RELEASE | 256 |
| ENABLE SNMP | 257 |
| ENABLE SNMP AUTHENTICATE_TRAP | 258 |
| ENABLE SNMP COMMUNITY | 259 |
| ENABLE SNMP COMMUNITY TRAP | 260 |
| ENABLE SSH SERVER | 261 |
| ENABLE SSH USER | 262 |
| ENABLE SYSTEM SECURITY_MODE | 263 |
| ENABLE TELNET SERVER | 264 |
| ENABLE TRIGGER | 265 |
| ENABLE USER | 266 |
| ENABLE USER RSO | 267 |
| FLUSH LOG OUTPUT | 268 |
| HELP | 269 |
| IF THEN ELSE ENDIF | 270 |
| LOAD | 271 |
| LOGIN | 273 |
| LOGOFF | 274 |
| MAIL | 275 |
| MODIFY | 277 |
| MODIFY NVS | 278 |
| PURGE LOG | 279 |
| PURGE NTP | 280 |
| PURGE PORTAUTH PORT | 281 |
| PURGE SNMP | 282 |
| PURGE TRIGGER | 283 |
| PURGE USER | 284 |
| RECONNECT | 285 |
| RENAME | 286 |
| RESET FILE PERMANENTREDIRECT | 287 |
| RESET LOADER | 288 |

| | |
|---|-----|
| RESET NTP | 289 |
| RESET PORTAUTH PORT | 290 |
| RESET PORTAUTH PORT MULTIMIB | 291 |
| RESET USER | 292 |
| RESTART | 293 |
| SET CONFIG | 295 |
| SET HELP | 296 |
| SET INSTALL | 297 |
| SET LOADER | 298 |
| SET LOG OUTPUT | 300 |
| SET LOG OUTPUT FILTER | 303 |
| SET LOG RECEIVE | 305 |
| SET LOG UTCOFFSET | 306 |
| SET MAIL | 308 |
| SET MANAGER ASYN | 309 |
| SET NTP UTCOFFSET | 310 |
| SET PASSWORD | 312 |
| SET PORTAUTH PORT | 313 |
| SET PORTAUTH PORT SUPPLICANTMAC | 317 |
| SET PORTAUTH USERNAME | 320 |
| SET RADIUS | 322 |
| SET SCRIPT | 323 |
| SET SNMP ASNBERPADDING | 324 |
| SET SNMP COMMUNITY | 325 |
| SET SNMP ENGINEID | 326 |
| SET SNMP GROUP | 327 |
| SET SNMP LOCAL | 328 |
| SET SNMP TARGETADDR | 329 |
| SET SNMP TARGETPARAMS | 330 |
| SET SNMP TRAPDELAY | 331 |
| SET SNMP USER | 332 |
| SET SSH SERVER | 333 |
| SET SSH USER | 334 |
| SET SYSTEM CONTACT | 335 |
| SET SYSTEM DISTINGUISHEDNAME | 336 |
| SET SYSTEM LOCATION | 337 |
| SET SYSTEM NAME | 338 |
| SET SYSTEM TERRITORY | 339 |
| SET TELNET | 340 |
| SET TIME | 341 |
| SET TRIGGER CPU | 342 |
| SET TRIGGER FIREWALL | 344 |

| | |
|--|-----|
| SET TRIGGER INTERFACE | 346 |
| SET TRIGGER MEMORY | 348 |
| SET TRIGGER MODULE | 350 |
| SET TRIGGER PERIODIC | 352 |
| SET TRIGGER REBOOT | 354 |
| SET TRIGGER TIME | 356 |
| SET TTY | 358 |
| SET USER | 359 |
| SHOW ALIAS | 361 |
| SHOW BUFFER | 362 |
| SHOW CONFIG | 363 |
| SHOW CPU | 365 |
| SHOW DEBUG | 366 |
| SHOW EXCEPTION | 367 |
| SHOW FEATURE | 369 |
| SHOW FFILE | 372 |
| SHOW FILE | 374 |
| SHOW FILE PERMANENTREDIRECT | 376 |
| SHOW FLASH | 378 |
| SHOW FLASH PHYSICAL | 380 |
| SHOW HTTP SERVER | 382 |
| SHOW INSTALL | 384 |
| SHOW LOADER | 386 |
| SHOW LOG | 388 |
| SHOW LOG COUNTER | 392 |
| SHOW LOG OUTPUT | 395 |
| SHOW LOG QUEUE | 398 |
| SHOW LOG RECEIVE | 400 |
| SHOW LOG STATUS | 402 |
| SHOW MAIL | 404 |
| SHOW MANAGER ASYN | 406 |
| SHOW NTP | 407 |
| SHOW NVS | 409 |
| SHOW NVS FREE | 411 |
| SHOW PATCH | 412 |
| SHOW PORTAUTH | 413 |
| SHOW PORTAUTH COUNTER | 416 |
| SHOW PORTAUTH PORT | 419 |
| SHOW PORTAUTH PORT MULTISUPPLICANT | 424 |
| SHOW PORTAUTH TIMER | 428 |
| SHOW RADIUS | 431 |
| SHOW RELEASE | 433 |

| | |
|----------------------------------|-----|
| SHOW SCRIPT | 434 |
| SHOW SESSIONS | 436 |
| SHOW SNMP | 437 |
| SHOW SNMP COMMUNITY | 441 |
| SHOW SNMP GROUP | 443 |
| SHOW SNMP TARGETADDR | 445 |
| SHOW SNMP TARGETPARAMS | 447 |
| SHOW SNMP USER | 449 |
| SHOW SNMP VIEW | 451 |
| SHOW SSH | 453 |
| SHOW SSH SESSIONS | 461 |
| SHOW SSH USER | 462 |
| SHOW STARTUP | 464 |
| SHOW SYSTEM | 465 |
| SHOW TELNET | 468 |
| SHOW TIME | 469 |
| SHOW TRIGGER | 470 |
| SHOW TTY | 475 |
| SHOW USER | 478 |
| SHOW USER RSO | 482 |
| SSH | 484 |
| TELNET | 486 |
| UPLOAD | 489 |
| WAIT | 491 |

システム

基本的なシステム管理コマンドについて説明します。

ログイン

本製品に対する設定は、コンソールポート（非同期シリアルポート）に接続したコンソールターミナル、または、ネットワーク上の Telnet クライアントから行います。

- ✧ Telnet を使用するには、あらかじめコンソールターミナルからログインし、本製品に IP アドレス等を設定しておく必要があります。IP の設定については「IP」の章をご覧ください。

コンソールターミナルを接続するか Telnet で接続すると、「login: 」というログインプロンプトが表示されます。コンソールターミナルを接続してもログインプロンプトが表示されない場合は、「Enter」を何回か押してみてください。

ご購入時の状態では、Manager（管理者）レベルのユーザー「manager」だけが登録されています。初期パスワードは「friend」です。「login:」に対してユーザー名「manager」を、「Password:」に対してパスワード「friend」を入力してください。ログインに成功すると、コマンドプロンプトが表示されます。

```
login: manager
Password: friend（実際には表示されません）

Manager >
```

- ✧ デフォルトのパスワードを使い続けることはセキュリティ上好ましくありませんので、初回ログイン時に変更することをお勧めします。詳細は「運用・管理」の「ユーザー認証データベース」をご覧ください。
- ✧ Telnet 接続の場合、ログインプロンプトが表示されてから 1 分以内にログインしないと、Telnet セッションが切断されます。
- ✧ 既定回数（デフォルトは 5 回）連続してログインに失敗すると、コンソールターミナルでは一定時間（デフォルトは 10 分）ログインプロンプトが表示されなくなります。また、Telnet 接続の場合はセッションが切断され、該当クライアントからの Telnet 接続要求が同じ期間拒否されるようになります。これらの設定は、SET USER コマンド（359 ページ）の LOGINFAIL、LOCKOUTPD パラメーターで変更できます。
- ✧ ファイアウォール機能が有効なルーターに対して、Telnet 経由でマルチホーミングの設定を行うと、Telnet が切断されます。

再起動

システムを再起動するには RESTART コマンド（293 ページ）を使います。

- ✧ 再起動を実行する前に、現在の設定内容をファイルに保存したかどうかをご確認ください。設定の保存については、「運用・管理」の「コンフィグレーション」をご覧ください。

コールドスタート（ハードウェアリセット）を実行するには REBOOT オプションを使います。

RESTART REBOOT ↵

コールドスタートでは、ハードウェア的にリセットをかけ、自己診断テストの実行、ソフトウェアのロードを行った後、起動スクリプトを読み込んで起動します。

ウォームスタート（ソフトウェアリセット）を実行するには ROUTER オプションを使います。

RESTART ROUTER ↵

ウォームスタートでは、起動スクリプトだけを読み直して設定を初期化します。起動スクリプトは SET CONFIG コマンド（295 ページ）で指定します。現在の起動スクリプトは SHOW CONFIG コマンド（363 ページ）で確認できます。

- ※ SNMP トラップの送信を有効にしている場合、RESTART コマンド（293 ページ）実行時は、REBOOT オプション（ハードウェアリセット）、ROUTER オプション（ソフトウェアリセット）のどちらを指定した場合でも、coldStart トラップが送信されます。warmStart トラップは、RESET IP コマンド（「IP」の 337 ページ）を実行したときに送信されます。

ウォームスタート時には、読み込みなおす設定ファイルを CONFIG パラメーターで指定することもできます。CONFIG パラメーターで指定した設定ファイルは一回だけ有効です。次に再起動するときは、（CONFIG パラメーターで再度指定しない限り）SET CONFIG コマンド（295 ページ）で設定した起動スクリプトが読み込まれます。

RESTART ROUTER CONFIG=test.cfg ↵

システム時計の設定

内蔵時計の日付と時刻をあわせるには SET TIME コマンド（341 ページ）を使います。

日付は「日-月-年」、時刻は「時:分:秒」の形式で指定します。月は英語月名の先頭 3 文字で指定します。大文字小文字の区別はありません。

| | |
|-----------------|-----|
| 1 月 (January) | Jan |
| 2 月 (February) | Feb |
| 3 月 (March) | Mar |
| 4 月 (April) | Apr |
| 5 月 (May) | May |
| 6 月 (June) | Jun |
| 7 月 (July) | Jul |
| 8 月 (August) | Aug |
| 9 月 (September) | Sep |
| 10 月 (October) | Oct |
| 11 月 (November) | Nov |
| 12 月 (December) | Dec |

表 1:

日付と時刻を設定するには次のようにします。ここでは 2010 年 4 月 20 日 19 時に設定します。

```
SET DATE=20-Apr-2010 TIME=19:00:00 ↵
```

時刻だけを修正します。

```
SET TIME=19:02:00 ↵
```

日付だけを修正します。

```
SET DATE=20-Apr-2010 ↵
```

現在の日付と時刻を確認するには SHOW TIME コマンド (469 ページ) を実行します。

NTP (Network Time Protocol) に準拠した時刻サーバーを利用して、時刻を正確に保つこともできます。詳細は「運用・管理」の「NTP」をご覧ください。

システム名の設定

システム名 (MIB-II オブジェクト sysName) を設定すると、コマンドプロンプトにシステム名が表示されるようになります。SNMP (Simple Network Management Protocol) を使用しない場合であっても、複数のシステムを管理しているときは、各システムに異なる名前を設定しておく、どのシステムにログインしているのかがわかりやすくなり便利です。

システム名 (sysName) を設定するには SET SYSTEM NAME コマンド (338 ページ) を使います。

```
SET SYSTEM NAME=omiya ↵
```

sysName にホスト名を含む完全なドメイン名を設定しておく、DNS 使用時にドメイン名の補完が行われます。たとえば、sysName に「gw.example.com」を設定した場合、TELNET コマンド (486 ページ) を「TELNET bulbul」のように実行すると、短いホスト名「bulbul」のあとに「example.com」(sysName に設定したフルドメインから先頭要素を取り除いたもの) が補われ、「bulbul.example.com」に対して DNS 検索が行われます。

また、DHCP クライアント機能を使用する場合には、DHCP Discover/Request メッセージの HostName フィールドにシステム名がセットされます。DHCP で IP アドレスを配布する ISP (インターネットサービスプロバイダー) の中には、HostName フィールドを使ってクライアントの識別/認証を行っているところがあります。そのような場合は、システム名として ISP から指定されたホスト名を設定してください。

なお、SNMP の設定については「運用・管理」の「SNMP」をご覧ください。また、IP の名前解決については、「IP」の「名前解決」をご覧ください。

本製品はデフォルトで HTTP サーバー (サポート対象外) が有効になっているため、IP 有効時は TCP ポート 80 番がオープンしています。セキュリティを重視する場合は、DISABLE HTTP SERVER コマンド (213 ページ) を実行して、HTTP サーバーを無効にしてください。

※ HTTP サーバーはデフォルトで有効になっていますが、サポート対象外です。

HTTP サーバーを無効にします。

DISABLE HTTP SERVER ↓

HTTP サーバーの状態は SHOW HTTP SERVER コマンド (382 ページ) で確認できます。

SHOW HTTP SERVER ↓

システムチェック

システムの基本情報を確認するための各種コマンドを紹介します。

システムの全般的な情報は SHOW SYSTEM コマンド (465 ページ) で確認できます。

システムログは SHOW LOG コマンド (388 ページ) で確認できます。詳細については「運用・管理」の「ログ」をご覧ください。

前回起動時の自己診断テストの結果は SHOW STARTUP コマンド (464 ページ) で確認できます。

例外状況の発生ログは SHOW EXCEPTION コマンド (367 ページ) で確認します。

システムの詳細な情報を確認するには SHOW DEBUG コマンド (366 ページ) を実行します。

メモリーに関する情報は SHOW BUFFER コマンド (362 ページ) で確認します。

CPU の使用率は SHOW CPU コマンド (365 ページ) で確認します。

記憶装置とファイルシステム

本製品の 2 次記憶装置とファイルシステムについて説明します。

物理デバイス

本製品は、システム再起動後もデータが保持される 2 次記憶装置として、NVS (Non-Volatile Storage) とフラッシュメモリーを搭載しています。

これらのデバイス上にはファイルシステムが構築されており、ファイル単位でデータにアクセスすることが可能です。詳しくは次節「ファイルシステム」をご覧ください。

NVS (Non-Volatile Storage)

NVS (バッテリーバックアップされた CMOS メモリー) は小容量の記憶装置で、モジュールのコンフィグレーションテーブルや、パッチファイル、スクリプトファイルなどを保存できます。

NVS のブロック情報を確認するには SHOW NVS コマンド (409 ページ) を使います。

```
SHOW NVS ↵
```

NVS の空き状況などは SHOW NVS FREE コマンド (411 ページ) で確認できます。

```
SHOW NVS FREE ↵
```

フラッシュメモリー

フラッシュメモリーは比較的大容量の記憶装置で、ファームウェア (リリース) ファイル、パッチファイル、設定スクリプトファイルなどを保存するために使います。

通常のファイル操作はこのメモリーに対して行います。後述するファイルの操作では、デバイス名を省略するとフラッシュメモリー上のファイルに対する操作となります。

フラッシュメモリー上のファイルシステムに関する情報は SHOW FLASH コマンド (378 ページ) で確認できます。

```
SHOW FLASH ↵
```

フラッシュメモリーの物理情報を確認するには SHOW FLASH PHYSICAL コマンド (380 ページ) を使います。

```
SHOW FLASH PHYSICAL ↵
```

フラッシュメモリーのコンパクション (メモリー上のゴミ削除) を行うには ACTIVATE FLASH COMPACTION コマンド (117 ページ) を使います。「Flash compaction successfully completed.」というメッセージが表示されるまで、システムを再起動したり、ファイル作成、編集、リネーム、削除などの操作を行ったりしないでください (状況によっては、コンパクション完了まで 1 ~ 5 分かかることがあります)。

ACTIVATE FLASH COMPACTION ↵

- ㄱ ㄱ 컴팩션 실행中は、絶対にシステムの再起動やフラッシュメモリーに対する操作（ファイル作成、編集、リネーム、削除など）を行わないでください。

コンパクションは必要に応じて自動実行されるため、通常運用ではこのコマンドを実行する必要はありませんが、空き容量が足りているように見えるにもかかわらずファイルをダウンロードできないといった状況では、本コマンドの実行により解決する可能性があります。このような状況は、ファームウェアなどサイズの大きいファイルを削除した直後に起こります。

ファイルシステム

本製品では、物理デバイス上にファイルシステムが構築されており、デバイス上のデータを「ファイル」としてアクセスすることが可能です。このとき、物理デバイスの違いを意識する必要はありません。

ファイル名

ファイル名は次の形式で表されます。ディレクトリー（フォルダー）の概念はありません。

device:filename.ext

| | |
|----------|--|
| device | デバイス名。flash（フラッシュメモリー）か nvs（NVS）のどちらか。大文字小文字の区別はありません。省略時は flash を指定したことになります |
| filename | ファイル名（ベース名）。文字数は 1～28 文字。ただし、8 文字を超える場合は特殊な扱いを受けます（「長いファイル名」を参照）。半角英数字とハイフン（-）が使えます。大文字・小文字の区別はありませんが、表示には大文字・小文字の区別が反映されます。 |
| ext | 拡張子。ファイル名には必ず拡張子をつける必要があります。文字数は 1～3 文字。半角英数字とハイフン（-）が使えます。大文字・小文字の区別はありませんが、表示には大文字・小文字の区別が反映されます |

表 2:

次におもな拡張子の一覧を示します。

| 拡張子 | ファイルタイプ |
|-----|--|
| rez | 圧縮形式のファームウェア（リリース）ファイル |
| paz | 圧縮形式のパッチファイル。システムが起動するときに、ファームウェアに対して動的に適用されます |
| cfg | 設定スクリプトファイル。システムの設定情報を保存します。scp との間に明確な区別はありませんが、慣例として設定内容を保存するスクリプトには cfg を使います |

| | |
|-----|--|
| scp | 実行スクリプトファイル。cfg との間に明確な区別はありませんが、慣例としてトリガースクリプトやバッチファイル的なスクリプトには scp を使います |
| hlp | オンラインヘルプファイル。SET HELP コマンドで設定し、HELP コマンドで閲覧します |
| lic | ライセンスファイル。ファームウェア（リリース）や追加機能（フィーチャー）のライセンス情報を格納しているファイルです。絶対に削除しないでください |
| ins | 起動時に読み込むファームウェアや設定ファイルの情報を格納しているファイルです |
| dhc | DHCP サーバーの設定情報ファイルです |
| txt | プレーンテキストファイル |

表 3:

以下のファイルは特殊な役割を持ちます。他のファイルも同様ですが、ファイルの取り扱い（削除、リネームなど）にはご注意ください。

| ファイル名 | 役割 |
|--------------|---|
| boot.cfg | デフォルトの起動スクリプトファイル。SET CONFIG コマンドで起動スクリプトが設定されていない（none）ときは、本ファイルが存在していれば起動時に自動実行されます。起動スクリプトが設定されている場合は、設定されているファイルが実行されます |
| config.ins | 起動時に読み込む設定スクリプト（起動スクリプト）ファイルの情報を保存しているファイル。SET CONFIG コマンドを実行すると作成（上書き）されます |
| prefer.ins | 起動時にロードするファームウェアファイルの情報を保存しています |
| enabled.sec | セキュリティーモードへの移行時に自動作成されるファイル。システムに対し、起動時にセキュリティーモードへ移行すべきことを示すファイルです |
| random.rnd | IPsec などの処理で使用されるファイルです。自動的に作成・更新されるため、ユーザーが意識する必要はありません |
| release.lic | リリースライセンスファイル。ファームウェア（リリース）のライセンス情報を持つファイルです。削除しないようご注意ください |
| feature.lic | フィーチャーライセンスファイル。追加機能（フィーチャー）のライセンス情報を持つファイルです。削除しないようご注意ください |
| longname.lfn | 短いファイル名（8.3 形式）と長いファイル名（28.3 形式）の対応を保持しています。ファイル名（ベース名）部分が 8 文字を超えるファイルを作成すると自動的に作成され、以後自動的に更新されます。削除しないようご注意ください。 |
| dyndns.sec | ダイナミック DNS 機能を使用したときに自動的に作成されるファイル。ダイナミック DNS の対象となっている IP アドレス情報を持つファイルです |

表 4:

長いファイル名

ファイル名（ベース名）部分（以下、filename）が 8 文字を超えるファイルは、長い名前（28.3 形式）と短

い名前（8.3 形式）の 2 つの名前を持ちます。短い名前は、長い名前を一定の基準にしたがって切りつめたものです。長い名前のファイルを作成すると、短い名前が自動的に生成されます。次に一例を示します。

- 長い名前：verylongfilename.cfg
- 短い名前：verylo~0.cfg

※ 名前の切りつめは、既存のファイルと名前が重複しないよう考慮して行われます。そのため、あるファイル名（長い名前）から、常に同じ名前（短い名前）が導き出されるわけではありません。

ファイルシステムに保存されるのは短い名前で、長い名前は特殊なファイル longname.lfn に保存されます。longname.lfn は、filename 部分が 8 文字を超えるファイルを最初に作ったときに自動的に作成され、以後自動的に更新されます。

なお、filename が最初から 8 文字以内の場合は、名前は 1 つだけ（8.3 形式だけ）です。

SHOW FILE コマンド（374 ページ）では、（長い名前があるときは）長い名前で表示されます。

```
SHOW FILE ↵
```

SHOW FFILE コマンド（372 ページ）では、（長い名前があっても）短い名前で表示されます。

```
SHOW FFILE ↵
```

短い名前と長い名前の対応を確認するには、SHOW FILE コマンド（374 ページ）で longname.lfn を指定します。

```
SHOW FILE=longname.lfn ↵
```

コマンドラインでファイル名を指定するときは、原則として長い名前と短い名前のどちらで指定してもかまいません。

```
SET CONFIG=verylongfilename.cfg ↵
```

または

```
SET CONFIG=verylo~0.cfg ↵
```

- ※ DELETE FFILE コマンド（188 ページ）と SHOW FFILE コマンド（372 ページ）は長い名前を認識しません。短い名前で指定してください。
- ※ 短い名前は、長い名前を持つファイルを作成したときに自動的に生成されますが、常に同じ名前に切りつめられるわけではありません。すでに存在するファイルと名前が重複しないように選択されます。長い名前を持つファイルを短い名前で指定するときは、必ず SHOW FILE コマンド（374 ページ）で longname.lfn を指定して対応表を確認してから指定してください。
- ※ コマンド実行時に長い名前を指定しても、CREATE CONFIG コマンド（158 ページ）で保存した設定スクリプト中では短い名前になることがあります（SHOW CONFIG コマンド（363 ページ）の DYNAMIC オプションで表示される設定スクリプトも同様です）。

ワイルドカード

ファイル进行操作するコマンドの中には、ワイルドカード（*）を使って複数のファイルを一度に指定できるものがあります。ワイルドカード（*）は「任意の文字列」を示すもので、次のように使います。

ファイルシステム（フラッシュ、NVS）上の圧縮形式のファームウェアファイル（.rez）をすべて表示

```
SHOW FILE=*:*.*.rez ↵
```

フラッシュメモリー上のテキストファイルの一覧を表示（device 省略時は flash とみなされる）

```
SHOW FILE=*.txt ↵
```

NVS 上のスクリプトファイルをすべて削除

```
DELETE FILE=nvs:*.*.scp ↵
```

DELETE FILE コマンド（189 ページ）と SHOW FILE コマンド（374 ページ）では、次のような指定（前方一致）も可能です。

```
DELETE FILE=gw*.*.scp ↵
```

※ 後方一致（*base.cfg）や中間一致（*foo*.cfg）は使えません。

ワイルドカードが使えるコマンドには以下のようなものがあります。

- DELETE FFILE コマンド（188 ページ）
- DELETE FILE コマンド（189 ページ）
- SHOW FFILE コマンド（372 ページ）
- SHOW FILE コマンド（374 ページ）

ファイルの操作

おもなファイル操作についてコマンド例を示します。

ファイルの一覧は、SHOW FILE コマンド（374 ページ）で表示できます。

```
SHOW FILE ↵
```

特定ファイルの一覧を見たいときはワイルドカードを使います。

```
SHOW FILE=*.*.scp ↵
```

ファイルの内容を見るには、SHOW FILE コマンド（374 ページ）で（ワイルドカードでない）ファイル名を指定します。ただし、SHOW FILE コマンド（374 ページ）で見ることができるのはテキスト形式のファイル（.txt、.scp、.cfg など）だけです。

```
SHOW FILE=mitai.cfg ↵
```

ファイルを削除するには DELETE FILE コマンド (189 ページ) を使います。ワイルドカードで複数ファイルをまとめて消すことも可能です。

```
DELETE FILE=iranai.cfg ↵
```

```
DELETE FILE=*.txt ↵
```

- ✧ 削除したファイルを元に戻すことはできません。ファイル操作時は十分注意を払ってください。
- ✧ config.ins、prefer.ins、release.lic、feature.lic は、システムの動作に必要なファイルです。誤って削除しないようご注意ください。
- ✧ ワイルドカードを使ってファイルを削除するときは、必要なファイルまで削除してしまわないよう十分にご注意ください。

ファイル名を変更するには RENAME コマンド (286 ページ) を使います。

```
RENAME old.scp new.scp ↵
```

テキスト形式のファイルを編集するには、EDIT コマンド (240 ページ) (内蔵フルスクリーンエディター) を使います。

```
EDIT myscript.scp ↵
```

コマンドやスクリプトの出力をコンソールではなくファイルに保存 (リダイレクト) することもできます。これには、CREATE FILE コマンド (161 ページ)、ADD FILE コマンド (123 ページ) を使います。

- 通常の情報表示コマンド (「SHOW XXXX」など) の出力をリダイレクトする場合は、ADD FILE コマンド (123 ページ) や CREATE FILE コマンド (161 ページ) を PERMANENTREDIRECT オプションなしで実行します。
 - － コマンドやスクリプトの出力を新規ファイルに保存するには、CREATE FILE コマンド (161 ページ) を次のようにして実行します。

```
CREATE FILE=output.txt COMMAND="show system" ↵
```

- ✧ CREATE FILE コマンド (161 ページ) は、指定したファイルがすでに存在しているとエラーになります。既存ファイルを強制的に上書きするには、次項で説明する FORCE オプションを指定してください。また、既存ファイルに追記するには次々項で説明する ADD FILE コマンド (123 ページ) を使ってください。
- － コマンドやスクリプトの出力を既存ファイルに上書き保存するには、CREATE FILE コマンド (161 ページ) を FORCE オプション付きで実行します。

```
CREATE FILE=output.txt FORCE COMMAND="show system" ↵
```

※ FORCE オプションを使用した場合、CREATE FILE コマンド (161 ページ) 実行前の既存ファイルの内容は失われますのでご注意ください。

- コマンドやスクリプトの出力を既存ファイルに追記するには、ADD FILE コマンド (123 ページ) を次のようにして実行します。

```
ADD FILE=output.txt COMMAND="show release" ↵
```

※ 指定したファイルが存在しない場合は新規作成されます (この場合、CREATE FILE コマンド (161 ページ) と同じ動作になります)。

- デバッグオプションの出力 (「ENABLE XXXX DEBUG」などで有効化) をリダイレクトする場合は、ADD FILE コマンド (123 ページ) や CREATE FILE コマンド (161 ページ) を PERMANENTREDIRECT オプション付きで実行します。

次に、デバッグオプション出力をファイルに保存するための手順を示します。

1. ADD FILE コマンド (123 ページ) や CREATE FILE コマンド (161 ページ) において、デバッグオプションを有効化する「ENABLE XXXX DEBUG」コマンドを指定します。このとき PERMANENTREDIRECT オプションを忘れないようにしてください。

```
CREATE FILE=swidebug.txt COMMAND="enable switch debug=all"
PERMANENTREDIRECT ↵
```

上記コマンドを実行することにより、「enable switch debug=all」が実行され、デバッグオプションが有効になります。これ以降、デバッグオプションの出力は新規作成されたファイル swidebug.txt に継続的に書き込まれていきます。これを実現するため、swidebug.txt は書き込み用にオープンされた状態となり、他のコマンドによって操作できないようロックされます。

2. デバッグオプション出力のリダイレクトを終えるには、RESET FILE PERMANENTREDIRECT コマンド (287 ページ) を実行して対象ファイルへの出力を終了し、ファイルをクローズします。これによりファイルのロックも解除されます。

```
RESET FILE=swidebug.txt PERMANENTREDIRECT ↵
```

※ デバッグオプション出力をいったんファイルにリダイレクトすると、ファイルをクローズしても、該当デバッグオプション出力はコンソールに表示されなくなります。デバッグオプション出力をコンソールに表示させたい場合は、再度「ENABLE XXXX DEBUG」コマンドを実行してください。なお、リダイレクト中に「ENABLE XXXX DEBUG」を実行すると、ファイルへの出力が停止しますのでご注意ください。

3. ファイルをクローズしてもデバッグオプションは有効なままなので、これを明示的に無効化します。

```
DISABLE SWITCH DEBUG=ALL ↵
```

LOAD コマンド (271 ページ) を使って、別のコンピューターからファイルをダウンロードすることもできます。次の例では TFTP サーバー 192.168.1.11 から long.scp をフラッシュメモリにダウンロードしています。ダウンロードには、HTTP や ZMODEM を使うこともできます。

```
LOAD FILE=long.scp SERVER=192.168.1.11 DEST=flash ↵
```

UPLOAD コマンド (489 ページ) を使えば、テキスト形式のファイルを TFTP サーバーにアップロードすることができます。次の例では、設定スクリプト taisetsu.cfg を TFTP サーバーにアップロードします。ZMODEM によるアップロードも可能です。

```
UPLOAD FILE=taisetsu.cfg SERVER=192.168.1.11 ↵
```

- ※ TFTP サーバーの実装 (UNIX 系 OS の tftpd など) によっては、サーバー上にあらかじめファイルを作成しておかないとファイルのアップロードができないものがあります。これは、ファイルの新規作成に失敗するためです。このような場合は、サーバー上で空のファイルを作成し、すべてのユーザーに書き込み権限を与えてからアップロードしてみてください。

```
UNxXOS[1]# cd /tftpboot
UNxXOS[2]# touch karappo.cfg
UNxXOS[3]# chmod 666 karappo.cfg
```

コンフィグレーション

本製品では、コマンド入力によって設定した内容を、テキスト形式のスクリプトファイルとして保存することができます。さまざまな設定を異なる名前のファイルとして保存しておき、必要に応じて切り替えて使うことが可能です。

設定の保存と復元

コンソールなどから設定した内容はランタイムメモリー上にあるため、システムを再起動すると消えてしまいます。次回以降も同じ設定を使いたい場合は、設定内容をスクリプトファイルに保存する必要があります。

メモリー上の設定内容をファイルに保存するには、CREATE CONFIG コマンド (158 ページ) を使います。ファイルの拡張子は「.cfg」か「.scp」とします。たとえば、現在の設定内容を「mynet.cfg」に保存するには、次のようにします。指定したファイルが存在しない場合は新規に作成され、すでに存在していた場合は上書きされます。

```
CREATE CONFIG=mynet.cfg ↵
```

本コマンドで作成したファイルには、設定内容がスクリプト形式で保存されます。ただし、スクリプトの内容は一定の基準にしたがった書式に変換されているため、コマンドラインで入力したものとまったく同じではありません (たとえば、長い行は ADD と SET のように複数行に分けて保存されます)。しかし、保存されている情報は同じです。また、ログインパスワードは暗号化 (MD5 ダイジェスト) して保存されます。

設定をファイルに保存しただけでは、再起動時に自動復元されません。SET CONFIG コマンド (295 ページ) を使って、保存した設定スクリプトが次回起動時に読み込まれるよう設定する必要があります。起動時に読み込まれる設定スクリプトのことを、「起動スクリプト」、「起動ファイル」、「起動時設定ファイル」などと呼びます。

```
SET CONFIG=mynet.cfg ↵
```

現在の起動スクリプトを確認するには、オプションなしで SHOW CONFIG コマンド (363 ページ) を実行します。

```
SHOW CONFIG ↵
```

現在のメモリー上の設定内容を確認するには、SHOW CONFIG コマンド (363 ページ) に DYNAMIC オプションを付けて実行します。設定内容がスクリプト形式で表示されます。

```
SHOW CONFIG DYNAMIC ↵
```

DYNAMIC オプションにモジュール名を与えることにより、特定モジュールの設定だけを確認することもできます。たとえば、IP の設定だけを確認するには次のようにします。

```
SHOW CONFIG DYNAMIC=IP ↵
```

次回、空の設定で起動させたいときは、起動スクリプトを「なし」にします。これは、設定をいちからやりなおしたいときなどに便利です。SET CONFIG コマンド (295 ページ) に NONE を指定してください。

```
SET CONFIG=NONE ↵
```

起動スクリプトを「なし」に設定しても、「boot.cfg」という名前のファイルが存在すると、起動時に自動実行されます。

起動スクリプトの設定を変更せずに、一度だけ別の設定ファイルで再起動（ウォームスタート）するには、RESTART コマンド（293 ページ）の CONFIG パラメーターに設定ファイル名を指定します。コールドスタート（RESTART REBOOT）時には、CONFIG パラメーターは指定できません。

```
RESTART ROUTER CONFIG=1kaikiri.cfg ↵
```

同様に、一度だけ空の設定で再起動したいときは、RESTART コマンド（293 ページ）の CONFIG パラメーターに NONE を指定します。このときは boot.cfg は実行されません。

```
RESTART ROUTER CONFIG=NONE ↵
```

コマンドプロセッサ

本製品に対する設定は、コンソールポート（非同期シリアルポート）に接続したコンソールターミナル、または、ネットワーク上の Telnet クライアントから、コマンドプロセッサ（コマンドラインインターフェース）にアクセスして行います。ここではコマンド入力に関する基本的な事柄について説明します。

ログイン

コマンドプロセッサにアクセスするには、コンソールポート（非同期シリアルポート）に接続したコンソールターミナルからログインするか、Telnet 経由でログインする必要があります。

- ✧ Telnet を使用するには、あらかじめコンソールターミナルからログインし、本製品に IP アドレス等を設定しておく必要があります。ご購入時の状態では IP が有効になっていないため、初回ログイン時は必ずコンソールからログインすることになります。なお、IP の設定については「IP」の章をご覧ください。

コンソールターミナルを接続するか Telnet で接続すると、「login: 」というログインプロンプトが表示されます。コンソールターミナルを接続してもログインプロンプトが表示されない場合は、「Enter」を何回か押してみてください。

ご購入時の状態では、Manager（管理者）レベルのユーザー「manager」だけが登録されています。初期パスワードは「friend」です。「login:」に対してユーザー名「manager」を、「Password:」に対してパスワード「friend」を入力してください。ログインに成功すると、コマンドプロンプトが表示されます。

```
login: manager
Password: friend (実際には表示されません)

Manager >
```

- ✧ デフォルトのパスワードを使い続けることはセキュリティ上好ましくありませんので、初回ログイン時に変更することをお勧めします。詳細は「運用・管理」の「ユーザー認証データベース」をご覧ください。
- ✧ Telnet 接続の場合、ログインプロンプトが表示されてから 1 分以内にログインしないと、Telnet セッションが切断されます。
- ✧ 既定回数（デフォルトは 5 回）連続してログインに失敗すると、コンソールターミナルでは一定時間（デフォルトは 10 分）ログインプロンプトが表示されなくなります。また、Telnet 接続の場合はセッションが切断され、該当クライアントからの Telnet 接続要求が同じ期間拒否されるようになります。これらの設定は、SET USER コマンド（359 ページ）の LOGINFAIL、LOCKOUTPD パラメーターで変更できます。

コマンドプロンプト

デフォルトの設定では、どのユーザーレベルでログインしているかによってコマンドプロンプトの表示が異なります。

- ✧ SET ASYN コマンド（「インターフェース」の 50 ページ）の PROMPT パラメーターでプロンプト文字列を変更している場合は、ユーザーレベルに関わりなく設定した文字列が表示されます。

- User レベル

>

- Manager レベル

Manager >

- Security Officer レベル

SecOff >

なお、SET SYSTEM NAME コマンド (338 ページ) でシステム名 (sysName) を設定しているときは、「>」の前にシステム名が表示されます。複数のシステムを管理しているような場合、システム名にわかりやすい名前を付けておくこと各システムを区別しやすくなり便利です。

```
Manager > set system name="GW/Saidaiji"
```

```
Info (134003): Operation successful.
```

```
Manager GW/Saidaiji>
```

コマンドライン編集キー

コマンドラインでは、以下の編集機能を使うことができます (VT100 互換の端末エミュレーターが必要です)。

| キー | 機能 |
|----------------------|---|
| | 1 文字右に移動 |
| | 1 文字左に移動 |
| Ctrl/A | 行頭に移動 |
| Ctrl/E | 行末に移動 |
| Delete または Backspace | カーソルの左にある文字を削除 |
| Ctrl/U | コマンド行の消去 |
| Ctrl/O | 挿入モード (デフォルト) と上書きモードの切り替え |
| または Ctrl/B | コマンド履歴をさかのぼる |
| または Ctrl/F | コマンド履歴を進める |
| Tab または Ctrl/I | 入力途中のキーワードを補完、あるいは、次に入力可能なキーワードの候補一覧を表示 |
| Ctrl/R | 入力途中のコマンドとマッチする最新のコマンド履歴を表示 |
| Ctrl/Q | SHOW XXXX コマンドの表示を中断 |

表 5:

コマンド入力時の注意事項

コマンド入力時には以下のことがらに注意してください。

1 行で入力できるコマンドの最大文字数はスペースを含めて 1000 文字です。通常の用途では事実上無制限ですが、コマンド行が長くなり 1 行におさまらない場合は、コマンドの省略形を使うか、コマンドを複数行に分けてください (ADD と SET など)。

- SET SYSTEM NAME コマンド (338 ページ) でシステム名を設定している場合は、システム名の分だけ短くなります。

「ADD」、「IP」などのキーワード (予約語) は大文字小文字を区別しないので、どちらで入力してもかまいません。一方、パラメーターとして与える値の中には、パスワードのように大文字小文字を区別するものと、ユーザー名のように大文字小文字を区別しないものがあります。コマンドリファレンス等でご確認の上入力してください。

コマンドは一意的に識別できる範囲で省略可能です。たとえば、SHOW FILE コマンド (374 ページ) は次のように省略して入力することができます。

```
SH FI ↓
```

- コマンドの省略形は、キーワードの増減によって変更される可能性があります (ソフトウェアのバージョンによって異なる可能性があります)。

ログインユーザーの権限 (ユーザーレベル) によって実行できるコマンドが異なります。通常の管理作業は Manager レベルで行います。また、セキュリティモードでは Security Officer レベルの権限が必要です。

コマンドの効果は (エラーがなければ) 入力直後にあらわれます。再起動などを行う必要はありません。ただし、設定内容は再起動すると消えてしまうので、再起動後にも同じ設定を使いたいときは CREATE CONFIG コマンド (158 ページ) でファイルに保存してください。詳細は「運用・管理」の「コンフィグレーション」などを参考にしてください。

コンソールメッセージ

コマンド入力後、実行結果や構文エラーを知らせるメッセージが表示されることがあります。

```
Manager > add ip int=eth0 ip=192.168.10.1

Warning (2005267): The IP module is not enabled.

Manager > enable ip

Info (1005287): IP module has been enabled.

Manager > show ip interfaith

Error (3005012): Parameter "interfaith" not recognised.
```

メッセージは次のような形式になっています。

```
レベル (番号): 本文
```

- 「レベル」はメッセージの重要度を示す単語で、次のどれかになります。
 - Info：コマンドの実行に成功したことを示す
 - Warning：コマンドの実行には成功したが、関連する事柄に注意すべき点があることを示す
 - Error：コマンドの実行に失敗したことを示す
- ※ コンソールメッセージの「レベル」は、ログメッセージの「ログレベル」とは異なります。「レベル」は、ログメッセージタイプ「021/MSG」のサブタイプ「001/INFO」,「002/WARN」,「003/ERROR」に対応しています。詳しくは、「運用・管理」の「ログ」にある「タイプ/サブタイプ」をご覧ください。
- 「番号」は3つのフィールドからなる7桁のメッセージコードです。

smmnnnn

- 「s」はメッセージの重要度を示す 1 桁の数字です。1 (Info) 2 (Warning) 3 (Error) の 3 種類があります。意味は前述の「レベル」と同じです。
 - 「mmm」はメッセージを出力したモジュールを示す 3 桁の数字です。詳しくは、「運用・管理」の「ログ」にある「モジュール ID とモジュール名」をご覧ください。
 - 「nnn」は個々のメッセージを識別するための 3 桁の数字です。001 ~ 255 は全モジュール共通のメッセージ、256 ~ 999 はモジュールごとに異なるメッセージです。
- 「本文」はメッセージ本文（英文）です。

コマンド入力補助機能

コマンドプロセッサには、コマンドの入力を補助する機能がいくつか備わっています。コマンド入力補助機能には次の種類があります。

- 入力候補の表示
- キーワードの補完
- パラメーター値の説明

これらの補助機能を利用するには、コマンドの入力途中で「？」か「TAB」キーを入力します。次にコマンド入力補助機能の使い方をまとめます。

| 書式 | 使用方法 | 機能 |
|----------------------------|--------------------------------|-------------------------------|
| 入力候補の表示（次のキーワード） | | |
| ? または <TAB> | コマンドラインの先頭で「?」か「TAB」キーを入力 | コマンドラインの先頭で入力可能なキーワードの一覧を表示する |
| keywords | 1 つ以上のキーワード（keywords）を入力 | カーソル位置に入力可能なキーワードの一 |
| ? または keywords <TAB> | した後、スペースを入れ、その後で「?」か「TAB」キーを入力 | 覧を表示する |

| 入力候補の表示（入力途中のキーワード） | | |
|-----------------------------|--|--|
| partial-keyword? | 何らかの文字列（partial-keyword）を入力した後、スペースを入れずに「?」を入力 | カーソル位置に入力可能なキーワードのうち、partial-keyword で始まるものの一覧を表示する |
| キーワードの補完 | | |
| partial-keyword<TAB> | 何らかの文字列（partial-keyword）を入力した後、スペースを入れずに「TAB」キーを入力 | カーソル位置に入力可能なキーワードのうち、partial-keyword で始まるものが1つだけであれば、partial-keyword を補完して完全なキーワードにする。partial-keyword で始まるキーワードが複数存在する場合は、候補の一覧を表示する |
| パラメーター値の説明 | | |
| keyword=? または keyword=<TAB> | 何らかの文字列（keyword）を入力した後、等号（=）を入れ、その後で「?」か「TAB」キーを入力 | keyword をパラメーター名と見なし、同パラメーターに指定可能な値の説明を表示する |

表 6: コマンド入力補助機能の使い方

以下、それぞれの機能について、実例を挙げながら解説します。

入力候補の表示

入力候補の表示機能は、現在のカーソル位置に入力可能なキーワード（コマンド名やパラメーター名、オプション名）の一覧を表示する機能です。コマンドの入力途中で「?」や「TAB」キーを入力することによって使用します。

- 「?」や「TAB」キーで表示されるキーワードの中には、サポート対象外のものも含まれます。原則として、本コマンドリファレンスに記載されていないコマンドやキーワード、機能はサポート対象外となります。詳細はリリースノートなどでご確認ください。

入力候補のキーワードは1行に1つずつ表示されます。また、コマンドラインの先頭キーワード（ADD、ENABLE など）やモジュール名キーワード（SYSTEM、IP など）の場合は、簡単な説明（英文）も表示されます。

次のキーワード候補を表示

コマンドラインの先頭で「?」か「TAB」キーを押す、あるいは、いくつかのキーワードを入力した後にスペースを入れ、その後「?」か「TAB」キーを押すと、次に入力可能なキーワードの一覧が表示されます。

たとえば、コマンドラインの先頭で「?」か「TAB」キーを押すと次のように表示されます（実際には「?」やタブ文字は表示されません）。

| | |
|------------------------|---|
| Manager > ? (または<TAB>) | |
| ACTivate | Cause an action to be taken immediately |
| ADD | Add new items to existing objects or instances |
| CLear | Erase memory (NVS or FLASH) totally - use with extreme caution! |

| | |
|-----------|--|
| Connect | Connect to a named Telnet or interactive host service or asyn port |
| COPy | Copy a file in NVS or FLASH memory |
| CREate | Make a new object or new instance of an object |
| ... | |
| SHow | Display states and settings of all parameters and objects |
| SSH | Use Secure Shell to log into a remote device securely |
| START | Start the packet generator for diagnostic purposes |
| STop | Terminate a current ping, trace route, or packet generator |
| TELnet | Use Telnet to login to a remote device |
| TRace | Use trace route to see what path packets take to a destination |
| UPLoad | Transfer a file from FLASH or NVS memory to a remote server |
| Manager > | |

画面の左側に列挙されているのが、コマンドラインの先頭キーワードとして有効な単語の一覧です（表示項目はファームウェアのバージョンによって異なる可能性があります）。大文字の部分は、各キーワードを一意に識別するため、最低限入力しなくてはならない部分を示しています。

画面の右側は、キーワードの簡単な説明（英文）です。

- 「？」や「TAB」キーで表示されるキーワードの中には、サポート対象外のものも含まれます。原則として、本コマンドリファレンスに記載されていないコマンドやキーワード、機能はサポート対象外となります。詳細はリリースノートなどでご確認ください。

つぎに、コマンドラインでさきほどの候補一覧から「SHOW」を入力し、さらに半角スペースを一文字入力した上で再度「？」か「TAB」キーを押すと、次のように表示されます。

| | |
|-----------------------------|---|
| Manager > show ? (または<TAB>) | |
| ACC | Display information about calls, scripts and domain name |
| ADSL | Display information about an ADSL interface |
| ALIAS | List the currently-defined aliases for long command sequences |
| ... | |
| TRace | Display TRACE configuration and results of the latest command |
| TRIGger | Display general trigger settings, or info about specific triggers |
| TTy | Display information about one or all of the TTY devices present |
| UPNP | Display the Universal Plug and Play state or configuration |
| USer | Display information about RSO or the User Authentication Facility |
| VLAN | Display information about the specified VLAN or the debug mode |
| VOIP | Display information about VOIP configuration or status |
| VRRP | Display diagnostic information about VRRP virtual routers |
| WANLB | Display information about WAN Load Balance, resources or sessions |
| X25C | Display X25C information |
| X25T | Display information about the X.25 DTE or call parameters |
| Manager > show | |

さらに「SYSTEM」を入力し、半角スペースを一文字入力した上で再度「?」か「TAB」キーを押すと、次のように表示されます。

```
Manager > show system ? (または<TAB>)

<enter>
DUMP          Display information that is dumped when an exception is generated
FACTory       Display information of use to the factory
MANUfactured  Display the date when the unit was manufactured
SErialnumber  Display the hardware serial number of the base unit
STARUp        Display the status of the unit after startup

Manager > show system
```

<enter>は、これ以上キーワードを入力せずに「Enter」キーを押してコマンドラインを完成させることもできる、という意味です。この例では、「show system」だけでも、コマンドラインとして完結していることを示しています。

入力途中のキーワード候補を表示

コマンドラインに何らかの文字列を入力した後、スペースを入れずに「?」を入力すると、カーソル位置に入力可能なキーワードのうち、入力した文字列で始まるものの一覧が表示されます。

たとえば、コマンドラインに「a」と入力した後、スペースを入れずに「?」を入力すると、次のように表示されます（実際には「?」は表示されません）。

```
Manager > a?

ACTivate      Cause an action to be taken immediately
ADD           Add new items to existing objects or instances

Manager > a
```

また、「add ip h」と入力した後で「?」を入力すると、次のように表示されます。

```
Manager > add ip h?

HElper        Adds port/s to list of UDP ports to listen for on the interface
HOSt          Adds a user-defined name for an IP host to the host name table

Manager > add ip h
```

指定した文字列で始まるキーワード候補がないときは、次のように表示されます。この例は、「add ip」の後に「g」で始まるキーワードは指定できないことを示しています。

```
Manager > add ip g

Error (3005012): The string "g" was not recognised as a parameter for this comma
nd. Either an invalid parameter was entered or the parameter was spelt incorrect
ly.
```

```
Manager >
```

キーワードの補完

一つ前で説明した「入力途中のキーワード候補を表示」とよく似ていますが、コマンドラインに何らかの文字列を入力した後、スペースを入れずに「TAB」キーを入力すると、カーソル位置に入力可能なキーワードのうち、指定した文字列で始まるものが1つだけの場合、入力途中のキーワードを補完して完全なキーワードにしてくれます。指定した文字列で始まるキーワードが複数存在する場合は、「？」キーと同じく候補の一覧が表示されます。

たとえば、コマンドラインに「ad」と入力した後、スペースを入れずに「TAB」キーを入力すると、次のように表示されます（実際にはタブ文字は表示されません）。

```
Manager > ad<TAB>

Manager > add
```

また、「add ip h」と入力した後で「TAB」キーを入力すると、「add ip」の後に「h」で始まる候補は2つあるため、次のように表示されます（「？」キーのときと同じ）。

```
Manager > add ip h<TAB>

HElper      Adds port/s to list of UDP ports to listen for on the interface
HOst        Adds a user-defined name for an IP host to the host name table

Manager > add ip h
```

ここで、もう一文字「o」を入力してから「TAB」キーを押すと、候補が1つになるため、次のように補完されます。

```
Manager > add ip ho<TAB>

Manager > add ip host
```

指定した文字列で始まるキーワード候補がないときは、何も表示されず、コマンドラインも変更されません。この例は、「add ip」の後に「g」で始まるキーワードは指定できないことを示しています。

```
Manager > add ip g<TAB>

Manager > add ip g
```

パラメーター値の説明

コマンドライン上でキーワードを入力した後、等号(=)を入れ、その後で「？」か「TAB」キーを入力すると、指定したキーワードをパラメーター名と見なし、該当パラメーターに指定すべき値の説明が表示されます。

たとえば、コマンドラインで「set switch port=」と入力してから「？」か「TAB」キーを押すと、次のように PORT パラメーターに指定すべき値の説明が表示されます。

```
Manager > set switch port=? (または<TAB>)
```

```
required - the keyword ALL, an Ethernet switch port number, a range of Ethernet
switch port numbers separated by a hyphen, or a comma-separated list of Etherne
t switch port numbers and/or ranges
```

```
Manager > set switch port=
```

真偽値 (TRUE/FALSE、ON/OFF、YES/NO) など、特定の値・キーワードを取るパラメーターの場合は、次のように表示されます。

```
Manager > set switch port=1 speed=? (または<TAB>)
```

```
required - AUTOnegotiate 10MHAlf 10MFUll 100MHAlf 100MFUll
1000MHAlf 1000MFUll 10MHAUto 10MFAuto 10MAUto 100MHAUto 100MFAuto 100MAUto
1000MHAUto 1000MFAuto
```

```
Manager > set switch port=1 speed=
```

```
Manager > set portauth idtoggle=? (または<TAB>)
```

```
required - OFF ON
```

```
Manager > set portauth idtoggle=
```

指定したキーワードが値を取れない場合は、次のように表示されます。この例は、「enable ip」の「ip」には値を指定できないことを示しています。

```
Manager > enable ip=? (または<TAB>)
```

```
No value allowed
```

```
Manager > enable ip=
```

オンラインヘルプ

オンラインヘルプを見るには、HELP コマンド (269 ページ) を使います。

オプションなしで HELP コマンド (269 ページ) を実行すると、ヘルプファイルのトップページが表示されます。

```
HELP ↓
```

トップページの一覧にしたがい、表示させたいトピックを指定すると該当項目が表示されます。

```
HELP IP ↓
```

トピックによってはさらに深い項目がある場合もあります。その場合は画面の表示にしたがってトピック

名を多段で指定します。

HELP IP INTERFACE ↵

ヘルプファイルはソフトウェアとともに配布されています。HELP コマンド (269 ページ) が使用するヘルプファイルは SET HELP コマンド (296 ページ) で変更できます。

SET HELP=help.hlp ↵

端末画面のページ当たり行数

デフォルトの端末設定では、1 ページあたり行数が 22 に設定されています。コマンドの出力結果が 22 行よりも長い場合は 21 行ごとに表示が一時停止し、最下行に次のようなメッセージが表示され、キー入力待ち状態になります。

```
--More--  (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

ここでは次のキー操作が可能です。

| | |
|-------|-------------------|
| Space | 次の 1 ページを表示します |
| Enter | 次の 1 行を表示します |
| c | 残りすべてを一気に表示します |
| q | 表示を中止し、プロンプトに戻ります |

表 7:

一度表示された行をさかのぼることはできません。

ページ当たり行数は SET ASYN コマンド (「インターフェース」の 50 ページ) で変更できます。

SET ASYN PAGE=30 ↵

ページ単位の一時停止を無効にするには、PAGE パラメーターに OFF を指定します。

SET ASYN PAGE=OFF ↵

一時停止後に「C」キーを押した場合や一時停止を無効にしている場合は、コマンドの出力が完了するまでプロンプトが表示されません。このようなときは、Ctrl/Q (Ctrl キーを押しながら Q キーを押す) で表示を中断することができます (コマンドによっては中断できないこともあります)。

エイリアス (別名)

コマンドエイリアス機能を利用すると、長いコマンド行に短い別名を付けることができます。

エイリアスの定義は ADD ALIAS コマンド (122 ページ) で行います。たとえば、「ls」でファイル一覧が表示されるようにするには、次のようにします。

ADD ALIAS=ls STRING="show file" ↵

エイリアスは入力直後に一回だけ展開され、その後コマンド解析部に送られます。展開されたコマンド行にエイリアスが含まれていても再帰的に展開されることはありません。

エイリアスの一覧は SHOW ALIAS コマンド (361 ページ) で確認できます。

```
SHOW ALIAS ↵
```

エイリアスを削除するには DELETE ALIAS コマンド (187 ページ) を使います。

```
DELETE ALIAS=ls ↵
```

ユーザー認証データベース

ユーザーレベル

ユーザーアカウントは、権限によって次の3つのレベルに分けられます。各レベルの権限は、動作モード（ノーマルモードとセキュリティーモード）によっても異なります。デフォルトの動作モードはノーマルモードです。動作モードの詳細については、「運用・管理」の「セキュリティー」をご覧ください。

- User レベル
- Manager レベル
- Security Officer レベル

User（一般ユーザー）レベルのユーザーは、ノーマルモード、セキュリティーモードのどちらであっても、自分自身に関する設定（端末設定やパスワード）などごく限られたコマンドしか実行できません。User レベルは、おもに WAN 経由で接続してくる PPP ユーザーを認証するために使います。詳細は「PPP」の章をご覧ください。

Manager（管理者）レベルのユーザーは、ノーマルモードにおいてすべてのコマンドを実行する権限を持ちます。初期導入時の設定作業を始め、ほとんどの管理・設定作業は Manager レベルのアカウントを使用して行います。ただし、セキュリティーモードでは第2位のレベルに降格され、セキュリティーに関するコマンド（セキュリティーコマンド）が実行できなくなります。

Security Officer レベルのユーザーは、ノーマルモードにおいてすべてのコマンドを実行する権限を持ちます。また、セキュリティーモードでもすべてのコマンドを実行できる最高位のユーザーです。セキュリティーモードでの管理作業は Security Officer レベルのアカウントを使用して行います。Security Officer レベルのユーザーが登録されていないと、セキュリティーモードには移行できません。

コマンドプロンプト

デフォルトの設定では、どのユーザーレベルでログインしているかによってコマンドプロンプトの表示が異なります。

- SET ASYN コマンド（「インターフェース」の50ページ）の PROMPT パラメーターでプロンプト文字列を変更している場合は、ユーザーレベルに関わりなく設定した文字列が表示されます。

- User レベル

```
>
```

- Manager レベル

```
Manager >
```

- Security Officer レベル

```
SecOff >
```

なお、SET SYSTEM NAME コマンド（338ページ）でシステム名（sysName）を設定しているときは、「>」の前にシステム名が表示されます。複数のシステムを管理しているような場合、システム名にわかりやすい

名前を付けておくと各システムを区別しやすくなり便利です。

```
Manager > set system name="GW/Saidaiji"

Info (134003): Operation successful.

Manager GW/Saidaiji>
```

デフォルトアカウント

ご購入時の状態では、Manager レベルのユーザー「manager」が登録されています。初期導入時の設定作業を始め、ほとんどの管理・設定作業はこのアカウントを使用して行います。

- ✧ セキュリティモードを使用するときは、別途 Security Officer レベルのアカウントを作成し、そのアカウントで管理作業を行います（Security Officer レベルのユーザーが登録されていないと、セキュリティモードには移行できません）
- ユーザー名：manager
- パスワード：friend

デフォルトのパスワードを使い続けることはセキュリティ上好ましくありませんので、初回ログイン時に変更することをお勧めします。パスワードの変更には SET PASSWORD コマンド（312 ページ）を使います。

```
Manager > set password

Old password: abcababc （現在のパスワードを入力。入力したパスワードは実際には表示されない）
New password: xyzxyz （新しいパスワードを入力）
Confirm: xyzxyz （確認のため、新しいパスワードをもう一度入力）
プロンプトが表示されないときはここで「Enter」を押す
```

- ✧ Manager レベルのパスワードを忘れると回復できません。パスワード変更時にはご注意ください。

次回起動時にも変更したパスワードが有効になるよう、CREATE CONFIG コマンド（158 ページ）で設定をファイルに保存し、SET CONFIG コマンド（295 ページ）で起動スクリプトに指定してください。詳細は「運用・管理」の「コンフィグレーション」をご覧ください。

```
Manager > create config=basic.cfg

Info (149003): Operation successful.

Manager > set config=basic.cfg

Info (149003): Operation successful.
```

ユーザー認証処理の順序

本製品はユーザー認証機構として、ユーザー認証データベースだけでなく、RADIUS（Remote Access Dial-In User Service）サーバーにも対応しています。ログイン時の認証は次の順序で行われます。

1. ユーザー認証データベース
2. RADIUS サーバー (ADD RADIUS SERVER コマンド (131 ページ) で登録したもの)

いずれかのステップで認証に成功すればログインが許可されます。RADIUS については、「運用・管理」の「認証サーバー」をご覧ください。

ユーザーアカウントの管理

ユーザーアカウントの追加や削除は、ノーマルモードでは Manager レベル以上、セキュリティモードでは Security Officer レベルのユーザーで行います。

ユーザー作成時には以下の情報が必要です。

| 情報 | パラメーター | 必須？ | 内容 |
|------------|-------------|------------------|--|
| ユーザー名 | USER | 必須 | 半角英数字 1～64 文字。大文字小文字の区別はなし |
| パスワード | PASSWORD | 必須 | 半角英数および記号 1～32 文字。空白可。大文字小文字の区別あり。デフォルトでは最小文字数が 6 文字以上に制限されている |
| ユーザーレベル | PRIVILEGE | オプション(省略時は User) | User、Manager、Security Officer から選択 |
| ログイン権 | LOGIN | User レベルの場合必須 | コマンドラインインターフェースへのログインを許可するかどうか |
| Telnet 実行権 | TELNET | オプション(デフォルトは NO) | ログインしたユーザーに TELNET コマンドの実行を許可するかどうか |
| コメント | DESCRIPTION | オプション | ユーザーに関するコメント |

表 8:

ユーザーを追加するには ADD USER コマンド (151 ページ) を使います。ユーザーレベルは PRIVILEGE パラメーターで指定します (省略時は USER レベル)。

```
ADD USER=swadmin PRIVILEGE=MANAGER PASSWORD=s69ro28n ↵
```

パスワードに空白を含めるときはダブルクォートで囲んでください。

```
ADD USER=swadmin PRIVILEGE=MANAGER PASSWORD="voi4 dia 239o" ↵
```

USER レベルのユーザーを作成するときは LOGIN パラメーターの指定が必須です。このパラメーターは、コマンドラインインターフェースへのアクセスを許可するかどうかを指定するもので、PPP ユーザーなどログインの必要がないユーザーに余分な権限を与えないようにするものです。ログインユーザーの場合は、YES (TRUE) を指定します。

```
ADD USER=panp PRIVILEGE=USER PASSWORD=KER3ira6ai LOGIN=YES ↵
```

自分のパスワードを変更するには SET PASSWORD コマンド (312 ページ) を使います。他のユーザー

のパスワードを変更するときは、SET USER コマンド (359 ページ) の PASSWORD パラメーターを使います。

```
SET USER=other PASSWORD=alapaK0re ↵
```

- ＼ デフォルトアカウントである manager 以外のユーザー情報は、他の設定情報と同様ランタイムメモリー上に作成されます。また、manager アカウントのパスワードを変更した場合も同様です。そのため、システムを再起動すると消えてしまいますので、CREATE CONFIG コマンド (158 ページ) でファイルに保存し、SET CONFIG コマンド (295 ページ) で起動時にユーザー情報が復元されるようにしてください。詳細は「運用・管理」の「コンフィグレーション」をご覧ください。なお、設定スクリプト中ではパスワードは暗号化されて保存されます。

- ＼ Manager レベルのパスワードを忘れると回復できません。パスワード変更時にはご注意ください。

ユーザーの一覧は SHOW USER コマンド (478 ページ) で確認できます。

```
SHOW USER ↵
```

ユーザー認証機構のデフォルト設定では、6 文字より短いパスワードは使用できないようになっています。パスワードの最小文字数は、SET USER コマンド (359 ページ) の MINPWDLEN パラメーターで変更できます。

```
SET USER MINPWDLEN=8 ↵
```

その他、ユーザー認証機構のグローバルな設定パラメーター (連続ログイン失敗時のロックアウト時間など) は、SET USER コマンド (359 ページ) で変更できます。

ユーザー認証関係の各種設定や統計情報は、SHOW USER コマンド (478 ページ) に CONFIGURATION オプションを付けることで表示できます。

```
SHOW USER CONFIGURATION ↵
```

認証サーバー

本製品は、ユーザー認証機構として、内部のユーザー認証データベースに加えて、RADIUS (Remote Authentication Dial In User Service) サーバーをサポートしています。

ユーザー認証処理の順序

ログイン名とパスワードを受け取った本製品は、最初にユーザー認証データベースを検索します。マッチするエントリーがあった場合はその時点で認証成功となります。マッチするエントリーがなかった場合は RADIUS サーバーに認証を要求します。RADIUS サーバーが登録されていない、あるいは RADIUS サーバーから Access-Reject が返ってきた場合は認証失敗、RADIUS サーバーから Access-Accept が返ってきた場合は認証成功となります。

RADIUS サーバー

RADIUS サーバーは、ユーザー認証に使用できるほか、ファイアウォールのアクセスルールを集中管理する目的でも使用できます。詳細は「ファイアウォール」の章をご覧ください。

RADIUS サーバーを登録するには、ADD RADIUS SERVER コマンド (131 ページ) を使用します。RADIUS サーバーの IP アドレスと共有パスワードを指定してください。

```
ADD RADIUS SERVER=192.168.10.10 SECRET=Valid8Me ↵
```

認証パケットのやり取りにはデフォルトで UDP ポート 1645 番が使用されます。また、アカウントिंगパケットには同 1646 番が使用されます。これらを変更するには、PORT パラメーター (認証) と ACCPORT パラメーター (アカウントिंग) を使用します。RFC2865 では認証用ポートを 1812 番、RFC2866 ではアカウントング用ポートを 1813 番としています。RADIUS サーバーの設定を確認して適宜変更してください。

```
ADD RADIUS SERVER=192.168.10.10 PORT=1812 ACCPORT=1813 ↵
```

RADIUS サーバーの登録を解除するには、DELETE RADIUS SERVER コマンド (196 ページ) を使用します。

```
DELETE RADIUS SERVER=192.168.10.10 ↵
```

登録されている RADIUS サーバーの一覧を表示するには、SHOW RADIUS コマンド (431 ページ) を使用します。

```
SHOW RADIUS ↵
```

RADIUS サーバーで管理するユーザーの権限 (ユーザーレベル) は、各ユーザーの Service-Type 属性で指定します。

Service-Type 属性値

ユーザーレベル

| | |
|-------------------|----------------------|
| Administrative(6) | Security Officer レベル |
| NAS Prompt(7) | Manager レベル |
| Login(1) | User レベル |

表 9:

- ※ Service-Type 属性に上記以外の値がセットされている場合、および、Service-Type 属性が付加されていない場合は、RADIUS サーバーから Access-Accept が返ってきてもログイン認証は失敗となりますのでご注意ください。

RADIUS サーバーのクライアント情報ファイルとユーザー情報ファイルの例を示します。詳細は RADIUS サーバーのマニュアルをご覧ください。

[/etc/raddb/clients]

```
# client          secret
192.168.10.1      RouterA
```

[/etc/raddb/users]

```
alpha Password = "PasswordA"
      Framed-IP-Address = 192.168.10.240
      Framed-IP-Netmask = 255.255.255.255
      Idle-Timeout = 120

beta Password = "PasswordB"
      Framed-IP-Address = 192.168.10.241
      Framed-IP-Netmask = 255.255.255.255
      Idle-Timeout = 120
```

本製品がサポートしている RADIUS 属性一覧

| 属性名 | 使用される時期 | 説明 |
|--------------------|----------------------|---------------------------------------|
| User-Name | 認証要求/アカウンティング 要求時 | 認証するユーザー名 |
| User-Password | 認証要求時 | ユーザーのパスワード |
| CHAP-Password | 認証要求時 | CHAP 認証時のパスワード (チャレンジに対するレスポンス) |
| NAS-IP-Address | 認証要求/アカウンティング 要求時 | 認証を要求する NAS (クライアント) の IP アドレス |
| Framed-IP-Address | 認証受理 (accept) 時 | ユーザーの IP アドレス |
| Framed-IP-Netmask | 認証受理 (accept) 時 | ユーザーのネットマスク |
| Callback-Number | 認証受理 (accept) 時 | コールバック番号 |
| Framed-Route | 認証受理 (accept) 時 | 認証されたユーザーのために NAS (クライアント) が設定すべき経路情報 |
| Framed-IPX-Network | 認証受理 (accept) 時 | ユーザーの IPX ネットワーク番号 |

| | | |
|--------------------------|------------------------|---|
| Session-Timeout | 認証受理 (accept) 時 | ユーザーセッションの有効期限 (秒) |
| Idle-Timeout | 認証受理 (accept) 時 | 無通信時のセッションタイムアウト (秒) |
| Calling-Station-Id | 認証要求時 | NAS (クライアント) に接続してきたユーザーの発番号 |
| Framed-AppleTalk-Network | 認証受理 (accept) 時 | ユーザーの AppleTalk ネットワーク番号 |
| Framed-AppleTalk-Zone | 認証受理 (accept) 時 | ユーザーのデフォルト AppleTalk ゾーン |
| CHAP-Challenge | 認証要求時 | NAS (クライアント) がユーザーに送信する CHAP チャレンジ |
| Acct-Status-Type | アカウントリング開始時 | サービスの開始、終了などを示す |
| Acct-Input-Octets | アカウントリング終了時 | サービス提供中に該当ポートで受信したデータ量 (オクテット) |
| Acct-Output-Octets | アカウントリング終了時 | サービス提供中に該当ポートから送信したデータ量 (オクテット) |
| Acct-Session-Id | アカウントリング開始/アカウントリング終了時 | セッション ID |
| Acct-Authentic | アカウントリング開始時 | ユーザー認証の方法 |
| Acct-Session-Time | アカウントリング終了時 | Framed User へのサービス提供時間 (秒) |
| Acct-Input-Packets | アカウントリング終了時 | Framed User へのサービス提供中に該当ポートから受信したデータ量 (パケット数) |
| Acct-Output-Packets | アカウントリング終了時 | Framed User へのサービス提供中に該当ポートに向けて送信したデータ量 (パケット数) |
| Acct-Terminate-Cause | アカウントリング終了時 | セッション終了の理由 |

表 10:

ポート認証

本製品は、ポート単位で LAN 上のユーザーや機器を認証するポート認証機能を実装しています。ポートに接続された機器（および機器を使用するユーザー。以下同様）の認証方法としては、大きく分けて次の 2 種類をサポートしています。

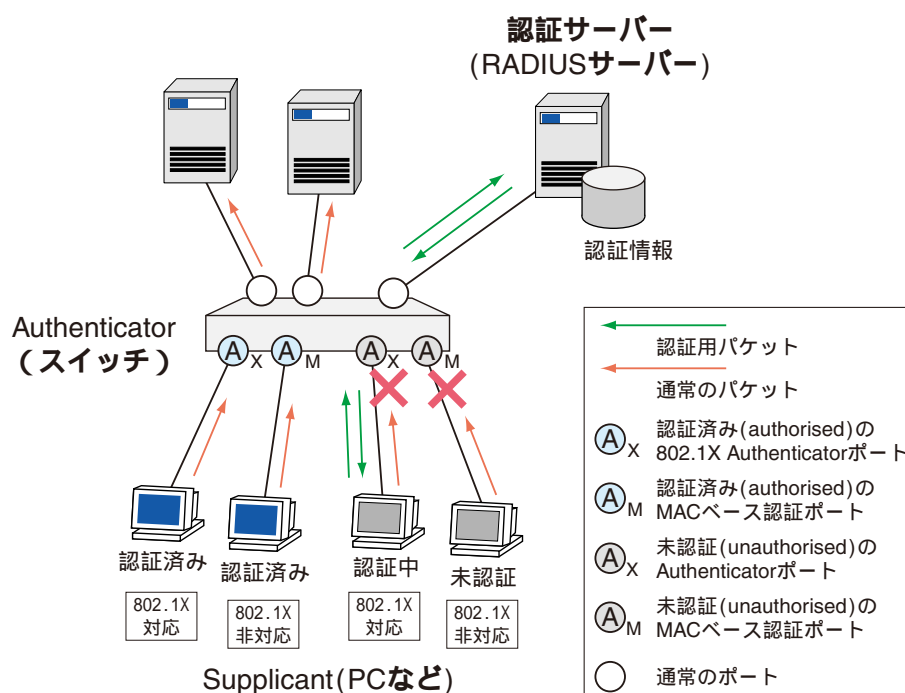
- IEEE 802.1X 認証（以下、802.1X 認証）
- MAC アドレスベース認証（以下、MAC ベース認証）

802.1X 認証は、EAP（Extensible Authentication Protocol）というプロトコルを使って、ユーザー単位で認証を行うしくみです。802.1X 認証を利用するには、認証する側と認証される側の両方が 802.1X に対応している必要があります。

一方、MAC ベース認証は、機器の MAC アドレスに基づいて機器単位で認証を行うしくみです。認証される側に特殊な機能を必要としないため、802.1X 認証の環境に 802.1X 非対応の機器（例：ネットワークプリンター）を接続したい場合などに利用できます。おもに、802.1X 認証を補完するものとして利用されます。802.1X および MAC ベースのポート認証機能を使用すれば、ポートに接続された機器を認証し、認証に成功したときだけ同機器からの通信、および、同機器への通信を許可するよう設定できます。また、認証に成功した機器を特定の VLAN にアサインすることも可能です（ダイナミック VLAN）。さらに、本製品は Supplicant 機能にも対応しているため、他の機器から認証を受けるよう設定することもできます。

概要

ポート認証のシステムは、通常下記の 3 要素から成り立っています。



- Authenticator (認証者): ポートに接続してきた Supplicant (クライアント) を認証する機器またはソフトウェア。802.1X 認証では EAP メッセージの交換によって Supplicant を認証する (ユーザー認証)。また、MAC ベース認証では Supplicant の MAC アドレスによって認証を行う (機器認証)。認証に成功した場合はポート経由の通信を許可、失敗した場合はポート経由の通信を拒否する。認証処理そのものは、認証サーバー (RADIUS サーバー) に依頼する (Supplicant の情報を認証サーバーに中継して、認証結果 (成功・失敗) を受け取る)。
- 認証サーバー (RADIUS サーバー): Authenticator の要求に応じて、Supplicant を認証する機器またはソフトウェア。ユーザー名、パスワード、MAC アドレス、所属 VLAN などの認証情報を一元管理している。Authenticator との間の認証情報の受け渡しには RADIUS プロトコルを用いる。
- Supplicant (クライアント): ポートへの接続時に Authenticator から認証を受ける機器またはソフトウェア。802.1X の認証を受けるためには、802.1X Supplicant の機能を備えている必要がある。802.1X Supplicant 機能は、一部の OS に標準装備されているほか、単体のクライアントソフトウェアとして用意されていることもある。一方、MAC ベースの認証を受けるために特殊な機能は必要ない。

本製品の各スイッチポート/Ethernet ポートは、上記のうち、Authenticator と Supplicant になることができます (Authenticator であると同時に Supplicant でもあるような設定も可能)。認証サーバー (RADIUS サーバー) は別途用意する必要があります。

- ✧ 本製品では、複数台の Supplicant を個々に認証する使用方法 (Multi-Supplicant モード) は Ethernet ポートのみでサポートしています。

ポート認証方式 (Authenticator)

本製品のポートを Authenticator として設定する場合、設定できる認証方式と、設定可能なポートの種類は以下のとおりです。

| ポート認証方式 | 設定可能なポートの種類 | |
|-----------------------------------|-------------------|-------------------|
| | ダイナミック VLAN なしの場合 | ダイナミック VLAN ありの場合 |
| 802.1X 認証 (Single-Supplicant モード) | ETH/VLAN | VLAN のみ |
| 802.1X 認証 (Multi-Supplicant モード) | ETH のみ | 未サポート |
| MAC ベース認証 (Multi-Supplicant モード) | ETH のみ | 未サポート |

表 11: Authenticator として設定できるポート認証方式

- Single-Supplicant モード: Supplicant が 1 台だけ接続されていることを想定したモードです。
- Multi-Supplicant モード: 複数の Supplicant を個々に認証するモードです。
- ダイナミック VLAN: 使用すると、認証結果に応じて、Supplicant が所属する VLAN を動的に変更できます。
- 同一ポートで 802.1X 認証と MAC ベース認証の併用はできません。
- ユーザー単位でのダイナミック VLAN による VLAN 割り当てはできません。

EAP 認証方式

802.1X 認証では、EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP など様々な認証方式が使用されています。このうち、本製品の 802.1X 認証モジュールが現在サポートしている EAP 認証方式は以下のとおりです。

- Authenticator 時 : EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-OTP(MD4/MD5)
- Supplicant 時 : EAP-MD5、EAP-OTP(MD4/MD5)

基本設定

本製品を使ってポート認証のシステムを運用するための基本的な設定例を示します。以下の例では、メインの認証方式として 802.1X 認証を使用します。(より具体的な設定例については設定例集をご覧ください。)

Authenticator

本製品を Authenticator として使用する場合の基本設定を示します。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。

ここでは、すべてのポートが VLAN default に所属していることを前提に、ポート 1～3 で 802.1X 認証を行うものとします。また、RADIUS サーバーはポート 4 (通常のポート) に接続されているものとします。

1. 802.1X では RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。IP モジュールを有効にし、VLAN default に IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=vlan-default IP=192.168.10.5 MASK=255.255.255.0 ↵
```

※ ここでは RADIUS サーバーが VLAN default 上にあるものと仮定しています。他の VLAN 上にあるときは、RADIUS サーバーまでの経路を適切に設定してください。

2. RADIUS サーバーの IP アドレスと UDP ポート、共有パスワードを指定します。

```
ADD RADIUS SERVER=192.168.10.130 PORT=1812 ACCPORT=1813
SECRET=himitsu ↵
```

3. 802.1X 認証機能を有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

4. ポート 1～3 で 802.1X 認証を行うよう設定します。「TYPE=AUTHENTICATOR」の指定により、ポート 1～3 は Authenticator ポートとなります。

```
ENABLE PORTAUTH=8021X PORT=1-3 TYPE=AUTHENTICATOR ↵
```

- ✧ 802.1X 認証の Authenticator ポート（および MAC ベース認証ポート）では、VRRP を使用できません。また、802.1X 認証の Authenticator ポート（および MAC ベース認証ポート）をタグ付きに設定することはできません。
- ✧ RADIUS サーバーを接続するポートは、Authenticator ポートにしないでください。Authenticator ポートにする場合は、ENABLE PORTAUTH PORT コマンド（252 ページ）/SET PORTAUTH PORT コマンド（313 ページ）の CONTROL パラメーターを AUTHORISED に設定してください。

Authenticator（ダイナミック VLAN）

ダイナミック VLAN（Dynamic VLAN Assignemnt）は、RADIUS サーバーから受け取った認証情報に基づいてポートの所属 VLAN を動的に変更する機能です。本製品では、802.1X 認証の Single-Supplciant モード（スイッチポートのみ）で使用可能です。

以下、本製品を Authenticator として使用し、さらにダイナミック VLAN 機能を利用する場合の基本設定を示します。Authenticator としての動作には、IP の設定と RADIUS サーバーの指定が必須です。

ここでは、利用者機器のために 3 つの VLAN「A」、「B」、「C」を用意します。また、RADIUS サーバーを接続するための VLAN「R」も作成します。各ポートに接続された機器は、認証成功後、RADIUS サーバー側から返された VLAN（「A」、「B」、「C」のどれか）に自動的にアサインされます。

ここでは、ポート 1～3 で 802.1X 認証を行うものとします。また、RADIUS サーバーは、VLAN「R」所属のポート 4（通常のポート）に接続されているものとします。

1. VLAN を作成します。

```
CREATE VLAN=A VID=10 ↵
CREATE VLAN=B VID=20 ↵
CREATE VLAN=C VID=30 ↵
CREATE VLAN=R VID=1000 ↵
```

2. RADIUS サーバーを接続するポート 4 を VLAN「R」に割り当てます。

```
ADD VLAN=R PORT=4 ↵
```

3. 802.1X では RADIUS サーバーを使って認証を行うため、最初に RADIUS サーバーと通信するための設定をします。IP モジュールを有効にし、VLAN「R」に IP アドレスを設定します。

```
ENABLE IP ↵
ADD IP INT=vlan-R IP=192.168.10.5 MASK=255.255.255.0 ↵
```

- ✧ ここでは RADIUS サーバーが VLAN「R」上にあるものと仮定しています。他の VLAN 上にあるときは、RADIUS サーバーまでの経路を適切に設定してください。

4. RADIUS サーバーの IP アドレスと UDP ポート、共有パスワードを指定します。

```
ADD RADIUS SERVER=192.168.10.130 PORT=1812 ACCPORT=1813
SECRET=himitsu ↵
```

5. 802.1X 認証機能を有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

6. ポート 1~3 で 802.1X 認証を行うよう設定します。「TYPE=AUTHENTICATOR」の指定により、ポート 1~3 は Authenticator ポートとなります。また、「VLANASSIGNMENT=ENABLED」の指定により、ダイナミック VLAN を有効にします。

```
ENABLE PORTAUTH=8021X PORT=1-3 TYPE=AUTHENTICATOR
VLANASSIGNMENT=ENABLED ↵
```

※ 本製品でダイナミック VLAN を使用する場合、Single-Suppliant モード (Suppliant1 台だけを想定した使用方法) のみ使用できます。また、設定可能なポートはスイッチポートのみです。

※ 802.1X 認証の Authenticator ポートをタグ付きに設定することはできません。

※ RADIUS サーバーを接続するポートは、Authenticator ポートにしないでください。Authenticator ポートにする場合は、ENABLE PORTAUTH PORT コマンド (252 ページ) /SET PORTAUTH PORT コマンド (313 ページ) の CONTROL パラメーターを AUTHORISED に設定してください。

ダイナミック VLAN の動作仕様は次のとおりです。

- Suppliant の認証に失敗した場合、ポートは本来の VLAN (ADD VLAN PORT コマンド (「VLAN」の 11 ページ) で指定した VLAN) の所属となります。ポート越えの通信は不可能です。
- RADIUS サーバーから有効な VLAN の情報が返ってきた場合、ポートはその VLAN の所属となります。認証に成功すれば、ポート越えの通信も可能です。
- RADIUS サーバーから無効な VLAN の情報が返ってきた場合、ポートは本来の VLAN 所属となります。また、認証も失敗となるため、ポート越えの通信は不可能です。
- RADIUS サーバーから VLAN の情報が返ってこなかった場合、ポートは本来の VLAN 所属となります。認証に成功すれば、ポート越えの通信も可能です。
- 該当ポートまたはシステム全体でポート認証が無効に設定された場合、ポートは本来の VLAN 所属となります。ポート認証が無効なので、ポート越えの通信に関する制限はありません。
- 未認証のポート、および、CONTROL=UNAUTHORISED (未認証固定) または CONTROL=AUTHORISED (認証済み固定) に設定されたポートは、本来の VLAN 所属となります。

ポートがダイナミック VLAN にアサインされているときは、ADD VLAN PORT コマンド (「VLAN」の 11 ページ) で該当ポートの所属 VLAN を変更しても、設定変更は直ちには反映されません。ポートがダイナミック VLAN から本来の VLAN に戻るのは、次のときです。

- 認証セッションのタイムアウト時。
- リンクがダウンしたとき。
- ポート上でポート認証が無効にされたとき (DISABLE PORTAUTH PORT コマンド (222 ページ))。
- システム上でポート認証が無効にされたとき (DISABLE PORTAUTH コマンド (220 ページ))。

Supplicant

本製品を 802.1X Supplicant として使用する場合の基本設定を示します。ここでは、ポート 1 が認証を受けるものとします。Supplicant としての動作においては、IP の設定は必須ではありません。

1. 802.1X 認証モジュールを有効にします。

```
ENABLE PORTAUTH=8021X ↵
```

2. ポート 1 で認証を受けるよう設定します。認証を受けるためのユーザー名とパスワードを指定してください。「TYPE=SUPPLICANT」の指定により、ポート 1 は Supplicant ポートとなります。

```
ENABLE PORTAUTH=8021X PORT=1 TYPE=SUPPLICANT USERNAME=atswitch
PASSWORD=atpasswd ↵
```

認証サーバー

ポート認証機能を利用するために必要な認証サーバー (RADIUS サーバー) の設定項目について簡単に説明します。

- ✧ 認証サーバーの詳細な設定方法については、ご使用のサーバー製品のマニュアルをご参照ください。
- 802.1X 認証において、ダイナミック VLAN を使用しないときは、ユーザーごとに下記の属性を定義してください。

| 属性名 | 属性値 | 備考 |
|---------------|-------|--|
| User-Name | ユーザー名 | 認証対象のユーザー名 (例: "user1", "userB") |
| User-Password | パスワード | (EAP-MD5、EAP-PEAP、EAP-TTLS 使用時) ユーザー名に対応するパスワード (例: "dbf8a9hve", "h1mi2uDa4o") EAP-TLS 使用時は不要 (別途、ユーザー電子証明書の用意が必要) |

表 12: 802.1X 認証 (ダイナミック VLAN なし)

- ✧ 認証方式として EAP-TLS を使う場合は、RADIUS サーバーの電子証明書と各ユーザーの電子証明書を用意し、各コンピューター上に適切にインストールしておく必要があります。また、認証方式として EAP-PEAP、EAP-TTLS を使う場合は、RADIUS サーバーの電子証明書を用意し、各コンピューター上に適切にインストールしておく必要があります。詳細は RADIUS サーバーおよび Supplicant (OS や専

用ソフトウェアなど)のマニュアルをご参照ください。

- MAC ベース認証を使用する場合は、機器ごとに下記の属性を定義してください。

| 属性名 | 属性値 | 備考 |
|---------------|----------|--|
| User-Name | MAC アドレス | 認証対象機器の MAC アドレス (例: "00-00-f4-11-22-33") a~f は小文字で指定 |
| User-Password | MAC アドレス | 認証対象機器の MAC アドレス。User-Name と同じ値を指定すること |

表 13: MAC ベース認証 (ダイナミック VLAN なし)

- また、802.1X 認証でダイナミック VLAN を使用するときは、前述の諸属性に加え、下記の 3 属性を追加設定してください。

| 属性名 | 属性値 | 備考 |
|-------------------------|------------------|--|
| Tunnel-Type | VLAN (13) | 固定値。指定方法はサーバーに依存 |
| Tunnel-Medium-Type | IEEE-802 (6) | 固定値。指定方法はサーバーに依存 |
| Tunnel-Private-Group-ID | VLAN 名 か VLAN ID | 認証対象のユーザーや機器が認証をパスした後に所属させる VLAN の名前か VLAN ID (例: "sales", 10) |

表 14: ダイナミック VLAN 用の属性

アップロード・ダウンロード

本製品は、TFTP、HTTP、ZMODEM を利用したファイルのアップロード、ダウンロードが可能です。

ダウンロード

ファイルのダウンロードには、IP ネットワーク経由で行う方法（TFTP、HTTP）と、非同期コンソールポート経由で行う方法（ZMODEM）があります。保存先のファイルシステムに余裕があれば、任意のファイルをダウンロードできます。

ネットワーク経由でのダウンロード

ネットワーク経由でファイル転送を行うためには IP の設定が必要です。詳細は「IP」の章をご覧ください。DNS サーバーアドレスを設定している場合は、SERVER パラメーターにホスト名（フルドメイン名）を指定できます。詳細は「IP」の「名前解決」をご覧ください。

TFTP サーバー 192.168.10.5 からファイル myfile.cfg をダウンロードします。

```
LOAD METHOD=TFTP SERVER=192.168.10.5 FILE=myfile.cfg DESTINATION=FLASH ↵
```

HTTP（Web）サーバー 192.168.10.10 からファイルをダウンロードします。ダウンロードするファイル（LOAD コマンド（271 ページ）の FILE パラメーター）は、サーバー上のドキュメントルートからのフルパスで指定します。たとえば、URL が「http://192.168.10.10/~admin/myscript.scp」なら、「/~admin/myscript.scp」と指定します。

```
LOAD METHOD=HTTP SERVER=192.168.10.10 FILE=~admin/myscript.scp
DESTINATION=FLASH ↵
```

ダウンロードするファイルの名前が、本製品のファイルシステムで扱えない形式の場合（サポートされていない拡張子が付いている、ファイル名が 28.3 を超える、など）は、DESTFILE パラメーターで保存時のファイル名を指定できます。たとえば、Web サーバー上で「longlonglonglongname.txt」という名前を持つファイルを「longname.txt」として保存するには、次のようにします。

```
LOAD METHOD=HTTP SERVER=192.168.10.10 FILE=/doc/longlonglonglongname.txt
DESTFILE=longname.txt DESTINATION=FLASH ↵
```

サーバーをホスト名（FQDN）で指定することもできます。その場合は、あらかじめ ADD IP DNS コマンド（「IP」の 173 ページ）で DNS サーバーを指定しておく必要があります。プライマリー DNS サーバーのアドレスが 192.168.10.5 であれば、次のようにします。

```
ADD IP DNS PRIMARY=192.168.10.5 ↵
LOAD METHOD=HTTP SERVER=www.example.com FILE=/index.html
DESTFILE=index.htm ↵
```

HTTP プロキシ経由でダウンロードするには、HTTPPROXY と PROXYPORT パラメーターでプロキシの IP アドレス（またはホスト名）とポートを指定します。

プロキシは LOAD コマンド（271 ページ）で指定してもかまいませんが、毎回入力するのは面倒なので、次のように SET LOADER コマンド（298 ページ）で HTTPPROXY と PROXYPORT のデフォルト値を設定しておくといでしょう。

```
SET LOADER HTTPPROXY=proxy.example.com PROXYPORT=3128 ↵
```

＼ HTTPPROXY にホスト名を指定する場合は、ADD IP DNS コマンド（「IP」の 173 ページ）で DNS サーバーを設定しておく必要があります。

デフォルト値を設定しておけば、LOAD コマンド（271 ページ）で HTTPPROXY と PROXYPORT の指定を省くことができます。

```
LOAD METHOD=HTTP SERVER=www.example.com FILE=/conf/basic.cfg ↵
```

デフォルト値として設定したパラメーターをクリアするには、SET LOADER コマンド（298 ページ）で DEFAULT を指定します。

```
SET LOADER HTTPPROXY=DEFAULT PROXYPORT=DEFAULT ↵
```

HTTP の Basic 認証を要求するサイトからファイルをダウンロードするには、USERNAME、PASSWORD パラメーターでユーザー名とパスワードを指定します。

```
LOAD METHOD=HTTP SERVER=www.example.com FILE=/private/michaya.cfg
USERNAME=mikan PASSWORD=cq23u5h8 ↵
```

SET LOADER コマンド（298 ページ）で設定したデフォルト値など、LOADER モジュールの各種設定は SHOW LOADER コマンド（386 ページ）で確認できます。

```
SHOW LOADER ↵
```

非同期ポート経由でのダウンロード

ZMODEM でファイルをダウンロードします。次のコマンドを入力すると画面に「**B0....」のような文

字列が表示され、受信待ち状態になるので、コンソール側で ZMODEM の送信プロセスを起動してください。一般的なターミナルソフトなら、メニューに ZMODEM 転送のようなコマンドがあるはずです。

```
LOAD METHOD=ZMODEM ASYN=0 ↵
```

アップロード

アップロードは UPLOAD コマンド (489 ページ) で行います。プロトコルは TFTP と ZMODEM が使えます。なお、ダウンロードとは違い、アップロードできるファイルはテキストファイル (.cfg や .txt) だけです。

ネットワーク経由でのアップロード

ネットワーク経由でファイル転送を行うためには IP の設定が必要です。詳細は「IP」の章をご覧ください。

TFTP サーバー 192.168.10.5 にファイル critical.cfg をアップロードします。

```
UPLOAD METHOD=TFTP FILE=critical.cfg server=192.168.10.5 ↵
```

- ＼ TFTP サーバーの実装 (UNIX 系 OS の tftpd など) によっては、サーバー上にあらかじめファイルを作成しておかないとファイルのアップロードができないものがあります。これは、ファイルの新規作成に失敗するためです。このような場合は、サーバー上で空のファイルを作成し、すべてのユーザーに書き込み権限を与えてからアップロードしてみてください。

```
UNxXOS[1]# cd /tftpboot
UNxXOS[2]# touch critical.cfg
UNxXOS[3]# chmod 666 critical.cfg
```

非同期ポート経由でのアップロード

ZMODEM でファイルをアップロードします。

```
UPLOAD METHOD=ZMODEM FILE=ivaluabl.scp ASYN=0 ↵
```

ソフトウェア

本製品のソフトウェアについて説明します。

ファイル名

本製品のソフトウェアは、ファームウェアファイル（リリースファイル）とパッチファイルで構成されています。バージョンによりパッチファイルがないこともあります。

ファームウェアファイル（リリースファイル）

ソフトウェアの本体です。ファームウェアファイルのバージョンは、ピリオドで区切られた3つの数字「major.minor.interim」（例：バージョン2.9.1）の形式で表されます。「major」はメジャーバージョン番号、「minor」はマイナーバージョン番号です。「interim」は、不具合修正などのために提供されていたパッチファイルがファームウェアに反映された時点で加算されます。

本製品のファームウェアファイルは「55-rrr.REZ」のようなファイル名で提供されます。「55-」は適用機種を表します。「rrr」は「major.minor.interim」からピリオドを取り除いた3桁の数値です。拡張子「.REZ」は圧縮された形式のリリースファイルであることを示します。mm-rrrの後に「a」「b」「c」のような文字が追加される場合もあります。

- ファームウェアファイルは、「55rrr-mm.REZ」のようなファイル名で提供される場合もあります。この場合のバージョン表記は、「major.minor.interim-mm」（例：バージョン2.9.1-23）の形式になります。「mm」はメンテナンス番号と呼び、後述するパッチ番号にほぼ相当します。不具合修正をパッチファイルとして提供するのはなく、ファームウェアファイル自体を修正して提供するような場合にこの形式のファイル名、バージョン表記が使われます。

パッチファイル

パッチファイルは、ファームウェアに対する暫定的な不具合修正のために使用されるもので、「mmrrr-pp.PAZ」というファイル名で提供されます。パッチファイル名は、適用機種を示す「mm」、パッチの対象となるリリースのバージョン番号「rrr」、パッチ番号「pp」で構成されます。パッチ番号は通常「01」から始まります。例えば「55-291.REZ」に対して、初めて提供されるパッチは「55291-01.PAZ」となります。最新のパッチファイルは、パッチ番号「01」から不具合修正された内容のすべてを含む形式で提供されます（対象となるファームウェアに適用可能なパッチファイルは1つだけです）。拡張子「.PAZ」は圧縮された形式のパッチファイルであることを示します。

- 不具合修正をパッチファイルとして提供するのではなく、ファームウェアファイル自体を修正して提供することもあります。

セットアップツールにおけるバージョン表記

セットアップツールでは、バージョン番号を「major.minor.interim PLpp」のように表します。各数値は上記の各ファイル説明での項目と同様です。ただし、「pp」の十の位の桁の「0」は表記しません（例「2.9.1

PL1」。

ファームウェアファイル（リリースファイル）の有効化

ファームウェアを使用するためにはライセンスが必要です。ファームウェアファイルをフラッシュメモリにダウンロードしても、ライセンス情報を入力して有効化するまでは使用できません。

ㄨ 以下の作業はセットアップツールが自動的に行いますので、通常は必要ありません。

ファームウェアを有効化するには、ライセンスパスワードとバージョン番号の情報がが必要です。ここではバージョン番号を「major.minor.interim」の形式とします。

ファームウェアの有効化には ENABLE RELEASE コマンド（256 ページ）を使います。

```
ENABLE RELEASE=55-291.rez NUMBER=2.65545 PASSWORD=a689E8113492 ㄱ
```

NUMBER パラメーターに指定する値「x.y」は、次のようにして求めます。

- 「x」はファームウェアの major バージョンです。たとえば、バージョン 2.9.1 なら 2 になります。
- 「y」は「65536 × interim+minor」で求めます。バージョン 2.9.1 なら、65536 × 1 + 9 で 65545 になります。

ㄨ バージョン 2.7 以降のバージョンアップ時には、バージョン番号の「major.minor」部分が変更されない限り、パスワードの入力を省略できます。たとえば、バージョン 2.7.4 から 2.7.5 へのバージョンアップでは、「major.minor」部分がともに「2.7」なので、バージョン 2.7.5 のファームウェアを有効化する際に、PASSWORD パラメーターを省略できます。ただし、ENABLE RELEASE コマンド（256 ページ）自体は実行する必要がありますのでご注意ください（ライセンスパスワードなしでファームウェアの有効化ができる、という意味です）。

ファームウェアライセンスの情報は SHOW RELEASE コマンド（433 ページ）で見ることができます。

```
SHOW RELEASE ㄱ
```

インストール（ファームウェア構成）情報

起動時にロードすべきファームウェアファイルとパッチファイルは、「インストール」情報としてシステムに保存されています。

インストール情報には以下の 3 種類があります。

| | |
|-----------|--|
| TEMPORARY | 一度しか使用されないテスト用インストール情報 |
| PREFERRED | 通常使用するファームウェアとパッチファイルの情報 |
| DEFAULT | 緊急時に使用するインストール情報。EPROM 上のファームウェアから起動する |

表 15:

ㄨ 以下の作業はセットアップツールが自動的に行いますので、通常は必要ありません。

起動時に使用するファームウェアは SET INSTALL コマンド（297 ページ）で設定します。

```
SET INSTALL=PREFERRED RELEASE=55-291.rez PATCH=55291-01.paz ↵
```

インストール情報を削除するには DELETE INSTALL コマンド (190 ページ) を使います。

```
DELETE INSTALL=PREFERRED ↵
```

インストールの設定情報を確認するには SHOW INSTALL コマンド (384 ページ) を使います。

```
SHOW INSTALL ↵
```

フィーチャー (追加機能) ライセンス

本製品では、付加的な機能をライセンス制で提供しています。これらの追加機能を使用するためには、フィーチャーライセンスを購入し、ライセンスを有効化する必要があります。詳細については、ライセンス付属の文書をご覧ください。

フィーチャーライセンスを有効化するには、ENABLE FEATURE コマンド (242 ページ) を使います。

```
ENABLE FEATURE=NOEX PASSWORD=jogefogojoge ↵
```

現在有効化されているフィーチャーの一覧は SHOW FEATURE コマンド (369 ページ) で確認できます。

```
SHOW FEATURE ↵
```

メール送信

本製品は簡易的な電子メール送信機能（メールクライアント）を備えています。この機能は、トリガーを使ってイベントの発生を管理者に通知したり、ログをメールで送信したりするときに便利です。

本製品のメール機能には次の制限があります。

- 送信のみで受信はできない。
- MIME エンコードをサポートしていない（日本語のメッセージも不可）。
- コマンドラインからメールを送るには、Manager（ノーマルモード時）か Security Officer（セキュリティーモード時）の権限が必要。
- 送信元メールアドレスは「manager@ホスト名」固定です。（ホスト名は SET MAIL コマンド（308 ページ）の HOSTNAME パラメーターで指定します）
- POP before SMTP、SMTP AUTH には対応していません。
- Submission ポートには対応していません。

基本設定

メールの送信に必要な基本的な設定について説明します。ここでは次のような構成を想定します。

| | |
|--------------------|----------------------|
| ルーターのフルドメイン名（FQDN） | gw.tw.example.com |
| ネームサーバーの IP アドレス | 192.168.28.1 |
| 管理者のメールアドレス | admin@is.example.com |

表 16:

メール機能を使用するには、自ドメイン名と DNS サーバーアドレスの設定が必要です。ドメイン名は SET MAIL コマンド（308 ページ）、DNS サーバーは ADD IP DNS コマンド（「IP」の 173 ページ）で設定します（アドレスを IP アドレスで指定するときは DNS サーバーの設定は必要ありません）。

なお、ここでは IP 関連の設定（アドレス設定や経路設定）は完了しているものとします。

1. ルーター自身の完全なホスト名（フルドメイン名。FQDN=Fully Qualified Domain Name）を設定します。

```
SET MAIL HOSTNAME=gw.tw.example.com ↵
```

2. DNS サーバー（ネームサーバー）のアドレスを設定します。

```
ADD IP DNS PRIMARY=192.168.28.1 ↵
```

メール機能の使用例

これでメールを送るための設定は完了です。以下、メール機能の実際の使用例を示します。メールの送信は MAIL コマンド（275 ページ）で行います。

コマンドラインから短いメールメッセージを送るには次のようにします。管理者のアドレスにテストメー

ルを送ってみましょう。

```
MAIL TO=admin@is.example.com SUBJECT="test1" MESSAGE="This is a test" ↵
```

TOに宛先のメールアドレス、SUBJECTにサブジェクト、MESSAGEにメッセージ本文を指定します。メッセージに使用できる文字は、半角英数字と半角スペースおよびアンダースコア（_）で、長さは131文字までです。メッセージ中にスペースを入れる場合は2重引用符（"）で囲んでください。

本製品のメールクライアントは、DNSを使って宛先ドメイン（例ではis.example.com）のMXレコードを検索し、メールエクステンジャーに直接メールを送信します。一般的なメールクライアントのように中継用のSMTPサーバー（送信メールサーバー）をしません。そのため、宛先ドメインのMXレコードを引けない環境ではメールを送ることができません。

ただし、DNSが引けなくても、宛先メールサーバーのIPアドレスがわかっている場合は、メールアドレスのドメイン部分にサーバーのIPアドレスをブラケットで囲んで書くことでメール送信が可能です。次の例では、宛先サーバーのIPアドレスが172.16.10.100であると仮定しています。

```
MAIL TO=admin@[172.16.10.100] SUBJECT="test2" MESSAGE="Koremo test
desu" ↵
```

FILEパラメーターを使用すれば、テキスト形式のファイル（.cfg、.scp、.txt）をメール本文として送ることができます。次の例では、設定ファイル「basic.cfg」をメール本文として管理者に送信します。

```
MAIL TO=admin@is.example.com SUBJECT="config file" FILE=basic.cfg ↵
```

トリガー機能を利用すれば、イベント発生時にメールを自動的に送信することができます。次の例では、再起動トリガー（CREATE TRIGGER REBOOT コマンド（182ページ））を使って、コールドスタート時に管理者にメールを送るよう設定します。

```
ENABLE TRIGGER ↵
CREATE TRIGGER=1 REBOOT=ALL SCRIPT=mail.scp ↵
```

スクリプト「mail.scp」

```
MAIL TO=admin@is.example.com SUBJECT="%N rebooted" MESSAGE="%N(SN:%S) re-
booted at %D %T"
```

ここではトリガースクリプト起動時に渡される特別な引数を使って、再起動したシステムの名称（%N）やシリアル番号（%S）、日時（%D、%T）をメールのサブジェクトと本文に埋め込んでいます。次に、メールメッセージの例を示します。

```
Subject: ar1 rebooted
From: manager@gw.tw.example.com
To: <admin@is.example.com>
Date: Wed, 29 Aug 2001 23:59:40

ar1(SN:41906093) rebooted at 29-Aug-2001 23:59:40
```

次の例では、ファイアウォールトリガー（CREATE TRIGGER FIREWALL コマンド（171ページ））を

使って、ポートスキャンの開始を検出したときに管理者にメールを送るよう設定します。メールはサブジェクトのみとし、ファイアウォールトリガーの引数を利用してサブジェクトに攻撃者の IP アドレスが入るようにします。

```
ENABLE TRIGGER ↓
```

```
CREATE TRIGGER=2 FIREWALL=PORTSCAN MODE=START SCRIPT=pscans.scp ↓
```

スクリプト「pscans.scp」の内容

```
MAIL TO=admin@is.example.com SUBJECT="Portscan from %2 started"
```

ログをメールで送信することもできます。次の例では、ログメッセージが 10 個たまるときにメールで管理者に送信されるよう設定しています (CREATE LOG OUTPUT コマンド (164 ページ) と ADD LOG OUTPUT コマンド (126 ページ))。

```
CREATE LOG OUTPUT=1 DEST=email TO=admin@is.example.com MESS=10 ↓
```

```
ADD LOG OUTPUT=1 ALL ↓
```

メール機能の設定やメールキューの状態を表示するには SHOW MAIL コマンド (404 ページ) を使います。

```
Manager > show mail
```

```
MAIL
```

```
Host Name ..... gw.tw.example.com
SMTP Server ..... not set
State ..... alive
Debug ..... disabled
Mails Sent ..... 4
```

| Date/Time | Id | To | Subject | State | Retries |
|------------|------|----------------------|---------|---------|---------|
| ----- | | | | | |
| 5 11:11:15 | 0003 | admin@is.example.com | | Connect | 0 |
| ----- | | | | | |

メールキュー内のメールを削除するには DELETE MAIL コマンド (193 ページ) を使います。上記 SHOW MAIL コマンド (404 ページ) の出力例で表示されているメール Id 「0003」を削除するには、次のようにします。

```
DELETE MAIL=3 ↓
```

セキュリティ

セキュリティモード/ノーマルモード

本製品には、次の2つの動作モードがあります。

| モード | 動作 |
|-----------|---|
| ノーマルモード | デフォルトの動作モードです |
| セキュリティモード | より高いセキュリティレベルを実現するためのモードです。ログインセキュリティや管理コマンドの実行権が厳しく制限されます。ルーターの管理に関するセキュリティを高めたい場合や、IPsecなどのセキュリティ機能を利用するときに使います |

表 17:

動作モードによってアクセスレベルの権限が変わります。ノーマルモード時、Manager レベルと Security Officer レベルは同等の権限を持ちますが、セキュリティモードでは多くの操作に Security Officer 権限が必要となります。

| レベル | デフォルトアカウント | ノーマルモード時の権限 | セキュリティモード時の権限 |
|------------------|--------------------------------|-------------------------------|-------------------------------|
| User | なし | ユーザー自身に関する設定などごく一部のコマンドのみ実行可能 | ユーザー自身に関する設定などごく一部のコマンドのみ実行可能 |
| Manager | ユーザー名 manager/ パスワード friend | すべてのコマンドを実行可能 | セキュリティコマンドを除くすべてのコマンドを実行可能 |
| Security Officer | なし | すべてのコマンドを実行可能 | すべてのコマンドを実行可能 |

表 18:

セキュリティモード時には、以下のコマンドの実行に Security Officer の権限が必要となります。

- ACTIVATE SCRIPT コマンド (120 ページ)
- ADD FRAMERELAY DLC コマンド (「フレームリレー」の 12 ページ) の ENCRYPTION パラメーター
- ADD IP INTERFACE コマンド (「IP」の 185 ページ)
- ADD PKI CERTIFICATE コマンド (「PKI」の 13 ページ)
- ADD PKI CRL コマンド (「PKI」の 15 ページ)
- ADD PKI LDAPREPOSITORY コマンド (「PKI」の 17 ページ)
- ADD SCRIPT コマンド (133 ページ)
- ADD SSH USER コマンド (147 ページ)
- ADD USER コマンド (151 ページ)
- ADD USER RSO コマンド (153 ページ)

- CLEAR NVS TOTALLY コマンド (156 ページ)
- CREATE CONFIG コマンド (158 ページ)
- CREATE ENCO KEY コマンド (「暗号・圧縮」の18 ページ)
- CREATE FRAMERELAY コマンド (「フレームリレー」の14 ページ) の DEFENCRYPTION パラメーター
- CREATE IPSEC BUNDLESPECIFICATION コマンド (「IPsec」の39 ページ)
- CREATE IPSEC POLICY コマンド (「IPsec」の41 ページ)
- CREATE IPSEC SASPECIFICATION コマンド (「IPsec」の46 ページ)
- CREATE ISAKMP POLICY コマンド (「IPsec」の48 ページ)
- CREATE PKI ENROLLMENTREQUEST コマンド (「PKI」の18 ページ)
- CREATE PKI KEYUPDATEREQUEST コマンド (「PKI」の21 ページ)
- CREATE PPP コマンド (「PPP」の37 ページ)
- CREATE PPP TEMPLATE コマンド (「PPP」の43 ページ)
- CREATE SNMP COMMUNITY コマンド (167 ページ)
- CREATE STAR コマンド (「暗号・圧縮」の22 ページ)
- DEACTIVATE SCRIPT コマンド (186 ページ)
- DELETE FILE コマンド (189 ページ)
- DELETE NVS コマンド (195 ページ)
- DELETE PKI CERTIFICATE コマンド (「PKI」の22 ページ)
- DELETE PKI CRL コマンド (「PKI」の23 ページ)
- DELETE PKI LDAPREPOSITORY コマンド (「PKI」の24 ページ)
- DELETE SCRIPT コマンド (197 ページ)
- DELETE SSH USER コマンド (204 ページ)
- DELETE USER コマンド (206 ページ)
- DELETE USER RSO コマンド (207 ページ)
- DESTROY ENCO KEY コマンド (「暗号・圧縮」の24 ページ)
- DESTROY IPSEC BUNDLESPECIFICATION コマンド (「IPsec」の53 ページ)
- DESTROY IPSEC POLICY コマンド (「IPsec」の54 ページ)
- DESTROY IPSEC SASPECIFICATION コマンド (「IPsec」の55 ページ)
- DESTROY ISAKMP POLICY コマンド (「IPsec」の56 ページ)
- DESTROY PKI ENROLLMENTREQUEST コマンド (「PKI」の25 ページ)
- DESTROY PKI KEYUPDATEREQUEST コマンド (「PKI」の26 ページ)
- DESTROY STAR コマンド (「暗号・圧縮」の25 ページ)
- DISABLE FEATURE コマンド (212 ページ)
- DISABLE IPSEC コマンド (「IPsec」の57 ページ)
- DISABLE IPSEC POLICY DEBUG コマンド (「IPsec」の58 ページ)
- DISABLE ISAKMP コマンド (「IPsec」の59 ページ)
- DISABLE ISAKMP DEBUG コマンド (「IPsec」の60 ページ)
- DISABLE PKI DEBUG コマンド (「PKI」の27 ページ)
- DISABLE SSH SERVER コマンド (228 ページ)
- DISABLE SSH USER コマンド (229 ページ)
- DISABLE USER コマンド (233 ページ)

- DISABLE USER RSO コマンド (234 ページ)
- DUMP コマンド (236 ページ)
- DUMP NVS コマンド (238 ページ)
- EDIT コマンド (240 ページ)
- ENABLE FEATURE コマンド (242 ページ)
- ENABLE IPSEC コマンド (「IPsec」の 61 ページ)
- ENABLE IPSEC POLICY DEBUG コマンド (「IPsec」の 62 ページ)
- ENABLE ISAKMP コマンド (「IPsec」の 65 ページ)
- ENABLE ISAKMP DEBUG コマンド (「IPsec」の 66 ページ)
- ENABLE PKI DEBUG コマンド (「PKI」の 29 ページ)
- ENABLE PPP DEBUG コマンド (「PPP」の 57 ページ)
- ENABLE PPP TEMPLATE DEBUG コマンド (「PPP」の 59 ページ)
- ENABLE SNMP コマンド (257 ページ)
- ENABLE SSH SERVER コマンド (261 ページ)
- ENABLE SSH USER コマンド (262 ページ)
- ENABLE STAR DEBUGGING コマンド (「暗号・圧縮」の 31 ページ)
- ENABLE STAR MKTTRANSFER コマンド (「暗号・圧縮」の 32 ページ)
- ENABLE USER コマンド (266 ページ)
- ENABLE USER RSO コマンド (267 ページ)
- LOAD コマンド (271 ページ)
- MAIL コマンド (275 ページ)
- MODIFY コマンド (277 ページ)
- MODIFY NVS コマンド (278 ページ)
- PURGE IPSEC コマンド (「IPsec」の 74 ページ)
- PURGE PKI コマンド (「PKI」の 31 ページ)
- PURGE USER コマンド (284 ページ)
- RENAME コマンド (286 ページ)
- RESET ENCO COUNTERS コマンド (「暗号・圧縮」の 33 ページ)
- RESET IPSEC COUNTER コマンド (「IPsec」の 75 ページ)
- RESET IPSEC POLICY COUNTER コマンド (「IPsec」の 77 ページ)
- RESET IPSEC SA COUNTER コマンド (「IPsec」の 78 ページ)
- RESET USER コマンド (292 ページ)
- SET CONFIG コマンド (295 ページ)
- SET ENCO KEY コマンド (「暗号・圧縮」の 36 ページ)
- SET FRAMERELAY コマンド (「フレームリレー」の 37 ページ) の DEFENCRYPTION パラメーター
- SET FRAMERELAY DLC コマンド (「フレームリレー」の 40 ページ) の ENCRYPTION パラメーター
- SET INSTALL コマンド (297 ページ)
- SET IP INTERFACE コマンド (「IP」の 376 ページ)
- SET IPSEC BUNDLESPECIFICATION コマンド (「IPsec」の 81 ページ)
- SET IPSEC POLICY コマンド (「IPsec」の 82 ページ)
- SET IPSEC SASPECIFICATION コマンド (「IPsec」の 86 ページ)
- SET IPSEC UDPPORT コマンド (「IPsec」の 87 ページ)

- SET PKI コマンド (「PKI」の 32 ページ)
- SET PKI CERTIFICATE コマンド (「PKI」の 33 ページ)
- SET PKI CRL コマンド (「PKI」の 34 ページ)
- SET PKI LDAPREPOSITORY コマンド (「PKI」の 35 ページ)
- SET PPP コマンド (「PPP」の 63 ページ)
- SET PPP TEMPLATE コマンド (「PPP」の 70 ページ)
- SET SCRIPT コマンド (323 ページ)
- SET SNMP COMMUNITY コマンド (325 ページ)
- SET SSH SERVER コマンド (333 ページ)
- SET SSH USER コマンド (334 ページ)
- SET STAR コマンド (「暗号・圧縮」の 38 ページ)
- SET USER コマンド (359 ページ)
- SHOW CONFIG コマンド (363 ページ)
- SHOW ENCO KEY コマンド (「暗号・圧縮」の 48 ページ)
- SHOW FEATURE コマンド (369 ページ)
- SHOW FILE コマンド (374 ページ)
- SHOW NVS コマンド (409 ページ)
- SHOW PPP CONFIG コマンド (「PPP」の 75 ページ)
- SHOW STAR コマンド (「暗号・圧縮」の 50 ページ)
- SHOW STAR MKTTRANSFER LOG コマンド (「暗号・圧縮」の 54 ページ)
- SHOW STAR NETKEY コマンド (「暗号・圧縮」の 56 ページ)
- UPLOAD コマンド (489 ページ)

モードの変更

セキュリティーモードに移行するためには、あらかじめ Security Officer レベルのユーザーを作成しておく必要があります。セキュリティーモードに移行すると、Manager レベルは第 2 位の権限レベルに降格され、セキュリティーに関するコマンドを実行できなくなります。

1. Security Officer レベルのユーザーを作成します。

```
ADD USER=secoff PRIVILEGE=SECURITYOFFICER PASSWORD="top secret" ↵
```

2. セキュリティーモードに移行すると、Telnet 接続では Security Officer レベルでログインできなくなる (他のレベルならログイン可) ので、必要に応じて後述する RSO (Remote Security Officer) の設定をしておきます。RSO は、あらかじめ指定したアドレスからのみセキュリティーモード時でも Security Officer レベルでのログインを許可する機能です。

```
ENABLE USER RSO ↵
```

```
ADD USER RSO IP=192.168.10.5 ↵
```

3. セキュリティーモードに移行するには ENABLE SYSTEM SECURITY_MODE コマンド (263 ページ) を実行します。このコマンドを実行すると、ファイルシステム上に「enabled.sec」ファイルが作

成されます。システム起動時に本ファイルが存在すればセキュリティモードとなります。このファイルを削除したり、修正、編集、コピー、リネーム等を行わないでください。

```
ENABLE SYSTEM SECURITY_MODE ↵
```

現在の動作モードを確認するには SHOW SYSTEM コマンド (465 ページ) を実行します。「Security Mode」が Enabled ならセキュリティモード、Disabled ならノーマルモードです。

Security Officer レベルでログインしなおすと、コマンドプロンプトが「SecOff >」に変わります。

Security Officer レベルでログインすると、セキュリティタイマーがスタートします。このタイマーはセキュリティ関連コマンドを実行するたびにリセットされます。一定時間セキュリティコマンドを実行しないとタイマーがタイムアウトし、ログインユーザーの権限は Manager レベルに格下げされます。格下げされた状態でセキュリティコマンドを実行しようとする、あらためて Security Officer レベルのパスワードを要求されます。

セキュリティタイマーのデフォルト値は 60 秒です。この値を変更するには、SET USER コマンド (359 ページ) の SECUREDELAY パラメーターを使用します。

```
SET USER SECUREDELAY=90 ↵
```

セキュリティモード時に SET CONFIG コマンド (295 ページ) で起動スクリプトを変更するときは注意が必要です。たとえば、SET CONFIG=NONE を実行すると、起動スクリプトは空になりますが、動作モードはセキュリティモードのままになります。この状態でシステムを再起動すると、Security Officer レベルのユーザーが存在しないことになるため、多くのコマンドが実行できなくなります。このような状態になった場合は、DISABLE SYSTEM SECURITY_MODE コマンド (230 ページ) を実行するしかありません。

ノーマルモードに戻るには DISABLE SYSTEM SECURITY_MODE コマンド (230 ページ) を実行します。このコマンドを実行すると、「enabled.sec」ファイルが削除されます。

Remote Security Officer (RSO)

セキュリティモードでは、Security Officer レベルでの Telnet ログインが原則として禁止されています。Remote Security Officer (RSO) は、信頼できる特定の IP アドレスに限り Security Officer レベルでの Telnet ログインを許可する機能です。

1. RSO アクセス (Security Officer レベルでの Telnet ログイン) を有効にするには、ENABLE USER RSO コマンド (267 ページ) を使います。

```
ENABLE USER RSO ↵
```

2. Security Officer レベルでの Telnet ログインを許可するアドレス (RSO アドレス) を追加するには、ADD USER RSO コマンド (153 ページ) を使います。

```
ADD USER RSO IP=192.168.10.5 ↵
```

MASK パラメーターを使えば、許可するアドレスを範囲指定することもできます (サブネットなど)。省略時は 32 ビットマスク (単一ホストの指定) となります。

```
ADD USER RSO IP=172.16.10.0 MASK=255.255.255.0 ↵
```

RSO アドレスを削除するには DELETE USER RSO コマンド (207 ページ) を使います。

```
DELETE USER RSO=172.16.10.0 ↵
```

RSO アドレスの一覧を見るには SHOW USER RSO コマンド (482 ページ) を使います。

```
SHOW USER RSO ↵
```

RSO アクセスを無効にするには DISABLE USER RSO コマンド (234 ページ) を使います。

```
DISABLE USER RSO ↵
```

Manager レベルでのセキュリティータイマー

Manager レベルでログインしているときは、以下のコマンドがセキュリティーコマンドと見なされ、セキュリティーモード時と同様のセキュリティータイマーが適用されます。

- ADD USER コマンド (151 ページ)
- DELETE USER コマンド (206 ページ)
- PURGE USER コマンド (284 ページ)
- SET MANAGER ASYN コマンド (309 ページ)
- SET USER コマンド (359 ページ)

これらのコマンドを実行するとセキュリティータイマーはリセットされます。これらのコマンドを一定時間 (SET USER コマンド (359 ページ) の SECUREDELAY パラメーター) 実行しないとタイマーがタイムアウトし、次にこれらのコマンドを実行したときにパスワードの入力が求められます。規定回数 (SET USER コマンド (359 ページ) の MANPWDFAIL パラメーター) ログインに失敗すると、強制的にログアウトさせられます (Telnet の場合はセッションが切断されます)。

ログ

本製品のログ機能について説明します。

ログ機能はデフォルトで有効になっており、メモリー（RAM と NVS）上に保存されるよう設定されています。メモリー上のログは、SHOW LOG コマンド（388 ページ）で見ることができます。

また、ログメッセージは、出力先の設定によって syslog サーバーに転送したり、メールで送信したりすることもできます。メッセージフィルターを使って、特定の条件を満たしたメッセージだけを保存・転送するよう設定することもできます。

デフォルトのログ設定

ご購入時の状態では、2 つの特殊な出力先「TEMPORARY」と「PERMANENT」が登録されており、以下の基準でログメッセージを保存するよう設定されています。

- 「TEMPORARY」: ログレベル 3（INFO）以上のメッセージを RAM 上に 200 件まで記録。電源オンの間だけ保持される
- 「PERMANENT」: ログレベル 3（INFO）以上のメッセージを NVS（不揮発性メモリー）上に 20 件まで記録。電源を切っても保持される

これらのログは SHOW LOG コマンド（388 ページ）で見ることができます。

RAM 上のログ（TEMPORARY）を見るには次のようにします。

```
SHOW LOG ↵
```

または

```
SHOW LOG=TEMPORARY (SHOW LOG=TE と省略できます) ↵
```

NVS 上のログ（PERMANENT）を見るには次のようにします。

```
SHOW LOG=PERMANENT (SHOW LOG=PE と省略できます) ↵
```

SET LOG OUTPUT コマンド（300 ページ）、ADD LOG OUTPUT コマンド（126 ページ）でこれらの出力先定義の内容を変更することにより、RAM および NVS 上に保存されるメッセージの条件を変更することができます。以下にいくつか例を示します。詳細は以下の各節をご覧ください。

RAM 上に保存されるログメッセージのログレベルを 2（DETAIL）以上に変更するには、次のようにします。

```
SET LOG OUTPUT=TEMPORARY FILTER=1 SEVERITY=>2 ↵
```

すべてのメッセージが RAM 上に保存されるようにするには次のようにします。

```
SET LOG OUTPUT=TEMPORARY FILTER=1 ALL ↵
```

RAM 上に保存するメッセージの数を 500 に増やすには次のようにします。


```
SET LOG OUTPUT=TEMPORARY MESSAGES=500 ↵
```

ログの閲覧

メモリー（RAM、NVS）上のログを見るには SHOW LOG コマンド（388 ページ）を使います。

すべてのログを見るには次のようにします。

```
SHOW LOG ↵
```

最新のログだけを見るには次のようにします。

```
SHOW LOG TAIL ↵
```

TAIL パラメーターに数値を指定すれば、最新の x 個だけを見ることができます。省略時は最新の 20 個が表示されます。

```
SHOW LOG TAIL=50 ↵
```

逆順（新しい順）にログを表示させるには REVERSE を使います。通常は古い順に表示されます。

```
SHOW LOG REVERSE ↵
```

REVERSE パラメーターに数値を指定すれば、最新の x 個だけを新しい順に見ることができます。

```
SHOW LOG REVERSE=20 ↵
```

特定モジュールのログだけを見たいときは次のようにします。

```
SHOW LOG MODULE=FIRE ↵
```

ログ設定のカスタマイズ手順

ログの設定は、次の 2 つの要素を組み合わせることによって行います。

1. 出力先の定義：ログの出力先（RAM、メールアドレス、syslog サーバーなど）や出力フォーマットなどを定義します。ログの出力先には以下のデバイスや宛先を指定できます。
 - ランタイムメモリー（RAM）
 - 不揮発性メモリー（NVS）
 - コンソールポート
 - メール送信
 - syslog サーバー（syslogd）に転送。メッセージは syslog 形式に変換された上で送信される。
 - SRLP（Secure Router Logging Protocol）で別のルーターに転送
2. メッセージフィルターの追加：個々のログメッセージの内容（メッセージタイプ、サブタイプ、ログレベルなど）に応じて、出力する・しないを決定します。出力先の定義にメッセージフィルターを関

連付けることによって初めてログメッセージが出力されるようになります。

以下、各手順について例を挙げながら解説します。

ログ出力先の定義

デフォルト以外の場所（RAM、NVS 以外）にログを出力するには、最初に出先を定義する必要があります。これには CREATE LOG OUTPUT コマンド（164 ページ）を使います。ユーザーが定義する出力先は 1～20 の出力先 ID で区別します。

以下にいくつか例を示します。

syslog サーバーにログを転送する場合は、DESTINATION パラメーターに SYSLOG を、SERVER パラメーターに syslog サーバーの IP アドレスを指定します。

```
CREATE LOG OUTPUT=1 DESTINATION=SYSLOG SERVER=192.168.10.5 ↵
```

ログをメールで送る場合は、DESTINATION パラメーターに EMAIL を、TO パラメーターに送信先のメールアドレスを指定します。

```
CREATE LOG OUTPUT=2 DESTINATION=EMAIL TO=admin@is.example.com ↵
```

メール送信時は、一通のメールでいくつのログメッセージを送信するかを指定することができます。デフォルトでは、ログメッセージが 100 件たまるごとにメールが送信されます。

逆に言うとメッセージが 100 件たまるまでメールが送信されませんので、よりリアルタイムにメッセージを受け取りたいときは MESSAGES パラメーターで一度に送信するメッセージ数を減らします。次の例ではメッセージが 10 件たまるごとにメールで送信します。

```
CREATE LOG OUTPUT=2 DESTINATION=EMAIL TO=admin@is.example.com
MESSAGES=10 ↵
```

一度作成した出力先定義の内容を変更したいときは、SET LOG OUTPUT コマンド（300 ページ）を使います。たとえば、出力先「1」の syslog サーバーアドレスを変更したいときは次のようにします。

```
SET LOG OUTPUT=1 SERVER=192.168.10.100 ↵
```

出力先の設定内容を確認するには SHOW LOG OUTPUT コマンド（395 ページ）を使います。

```
SHOW LOG OUTPUT ↵
```

OUTPUT パラメーターに出力先 ID を指定すると、より詳細な情報を見ることができます。

```
SHOW LOG OUTPUT=1 ↵
SHOW LOG OUTPUT=TEMPORARY ↵
```

さらに FULL オプションを付けると、メッセージフィルターの情報も表示されるようになります。フィルターについては次節で述べます。

```
SHOW LOG OUTPUT FULL ↓
SHOW LOG OUTPUT=1 FULL ↓
```

ログ出力先の定義を削除するには DESTROY LOG OUTPUT コマンド (208 ページ) を使います。

```
DESTROY LOG OUTPUT=3 ↓
```

メッセージフィルターの追加

出力先を定義しただけでは、ログメッセージは出力されません。出力先定義にメッセージフィルターを関連付け、出力すべきメッセージの種類を指定する必要があります。メッセージフィルターの追加は ADD LOG OUTPUT コマンド (126 ページ) で行います。1 つの出力先に対して複数のフィルターエントリを設定することも可能です。

すべてのログメッセージを出力する場合は ALL を指定します。

```
ADD LOG OUTPUT=1 ALL ↓
```

特定のモジュールに関するログだけを出力させたいときは、MODULE パラメーターにモジュール ID かモジュール名を指定します。たとえば、ファイアウォールに関するログだけを出力させたい場合は次のようなフィルターを追加します。

```
ADD LOG OUTPUT=2 MODULE=FIREWALL ↓
```

モジュール ID、モジュール名については、「モジュール ID とモジュール名」をご覧ください。

メッセージフィルターの設定では、「大きい」「小さい」「等しい」「等しくない」「~を含む」などの比較演算子を使えます。ファイアウォール以外のログだけを出力させたい場合は次のように否定演算子「!」を使います。

```
ADD LOG OUTPUT=3 MODULE=!FIREWALL ↓
```

比較演算子については「ログフィルターの条件指定に使える比較演算子」をご覧ください。

ログレベル 6 (URGENT) 以上のログだけを出力させたい場合は次のようにします。

```
ADD LOG OUTPUT=4 SEVERITY=>6 ↓
```

ログレベルの一覧については「ログレベル」をご覧ください。

ログメッセージ本文に「unknown」という文字列が含まれるメッセージだけを出力したいときは次のようにします。大文字小文字は区別されません。

```
ADD LOG OUTPUT=5 MSGTEXT=%unknown ↓
```

複数の条件を同時に指定することもできます。ファイアウォールに関するログのうち、ログレベルが 6 (URGENT) 以上のメッセージだけを出力したいときは次のようにします。

```
ADD LOG OUTPUT=6 MODULE=FIREWALL SEVERITY=>6 ↓
```

メッセージフィルターの設定を確認するには、SHOW LOG OUTPUT コマンド (395 ページ) の FULL オプションを使います。

```
SHOW LOG OUTPUT FULL ↓
SHOW LOG OUTPUT=1 FULL ↓
```

出力先定義からログフィルターを削除するには DELETE LOG OUTPUT コマンド (191 ページ) を使います。FILTER パラメーターにはフィルターエントリーの番号を指定します。デフォルトでは、フィルター番号は ADD LOG OUTPUT コマンド (126 ページ) で追加した順に付けられます。番号を確認するには、SHOW LOG OUTPUT コマンド (395 ページ) を FULL オプション付きで実行します。

```
DELETE LOG OUTPUT=3 FILTER=1 ↓
DELETE LOG OUTPUT=3 FILTER=ALL ↓
```

ログ設定の確認

ログの出力先定義は SHOW LOG OUTPUT コマンド (395 ページ) で確認します。TE (TEMPORARY) は、デフォルトで定義されている出力先です。

```
Manager > show log output
```

| OD# | Type | Port | Server | Msg | Zone | Fmt | Email Address | ESQMP |
|-----|--------|------|--------|------|---------|-----|--------------------|-------|
| 01 | Email | | | 0002 | - | S | admin@fried-telesi | YNN-- |
| PE | NVS | | | 0020 | Default | | | YY--- |
| TE | Memory | | | 0200 | Default | | | YY--- |

各出力先定義の詳細や、関連付けられているメッセージフィルターの内容を確認するには、SHOW LOG OUTPUT コマンド (395 ページ) に FULL オプションを付けます。

```
Manager > show log output=1 full

Output Definition ..... 1
Enabled ..... Yes
Type ..... Email
Max Messages ..... 2
Time Zone ..... Not set
Format ..... Full
Email Address ..... admin@is.example.com
Secure ..... No
Queue Only ..... No
```

```
Filter 1:
  ALL
```

ログモジュールのステータスは、SHOW LOG STATUS コマンド（402 ページ）で確認できます。

```
Manager > show log status

Log System Status
-----

Log Module Status ..... Enabled
Log Message Generation ..... Enabled
Log Message Reception (via network) ... Enabled
Log Message Output ..... Enabled
Local Time Offset (from UTC) ..... Not set
Next Message ID ..... 338
Number of Output Definitions ..... 3
```

設定例

syslog サーバーへのログ転送

ここでは、すべてのログを syslog サーバーに転送するための設定を示します。IP 等の設定は終わっているものとします。

1. ログの出力先を定義します。ここでは、syslog サーバー 192.168.10.5 にログメッセージを転送します。

```
CREATE LOG OUTPUT=1 DESTINATION=SYSLOG SERVER=192.168.10.5 ↵
```

2. すべてのログメッセージを出力するメッセージフィルターを追加します。

```
ADD LOG OUTPUT=1 ALL ↵
```

syslog サーバーがリモートからの接続を受け付けるよう設定されていれば、ルーターの生成するすべてのログメッセージが syslog サーバーに送られ、記録されるようになります。syslog サーバー上で各メッセージがどのように処理されるかは、syslogd の設定ファイル /etc/syslog.conf の内容によって決まります。syslog サーバーの詳細については、サーバーシステム上のマニュアルページ syslogd(8)、syslog.conf(5)、syslog(1)、logger(1) 等をご参照ください。

メール送信

ログメッセージをメールで送りたいときは次のようにします。

1. メール送信機能の基本設定をします。

```
SET MAIL HOSTNAME=gw.tw.example.com ↵
ADD IP DNS PRIMARY=192.168.1.1 ↵
```

2. ログの出力先を定義します。ここでは、ログメッセージが 10 個たまるとに、メールで admin@is.example.com に送信するよう設定します。

```
CREATE LOG OUTPUT=2 DESTINATION=EMAIL TO=admin@is.example.com
MESSAGE=10 ↵
```

※ メールは、ログメッセージが MESSAGE パラメーターで指定した数たまった時点で送信されます。MESSAGE パラメーターを指定しなかった場合はデフォルト値の 100 が採用されるため、すぐにはメールが送信されないことがあります。

3. すべてのログメッセージを出力するメッセージフィルターを追加します。

```
ADD LOG OUTPUT=2 ALL ↵
```

※ 複数のログフィルターにそれぞれ複数のログ出力インターフェースを使用する場合、フィルターによって分類されたログメッセージが 1 つのメールで送信されません。

資料編

メッセージフォーマット

ログメッセージは下記のフィールドで構成されています。ただし出力時には、出力先定義の内容により、一部のフィールドだけが表示されたり、フォーマットが変換されたりすることがあります。

| フィールド | サイズ (バイト) | 説明 |
|-------------|-----------|-----------------------------|
| Msg ID | 4 | メッセージ ID |
| Flags | 2 | フラグとログレベル |
| Date | 2 | メッセージが生成された日付 (現地時間) |
| Time | 3 | メッセージが生成された時刻 (現地時間) |
| Origin IP | 4 | メッセージ生成者の IP アドレス |
| Module | 2 | メッセージを生成したモジュール |
| Type | 2 | メッセージタイプ |
| SubType | 2 | メッセージサブタイプ |
| Source File | 12 | メッセージを生成したプログラムソースファイル名 |
| Source Line | 2 | メッセージを生成したプログラムソースファイル内の行番号 |
| Reference | 15 | 参考情報 (ユーザー名、ISDN コール名など) |
| Message | 80 | メッセージ本文 |

表 19:

| Date/Time | Mod | Type | SType | Dev | Origin | MSGID | Source | File/Line |
|-------------|-----|------------------|-------|-------|---------|-------|--------|-----------------|
| 09:52:27 | 3 | USER | USER | LON | 00016 | Local | 00063 | usermain.c:2709 |
| 03-JUL-2001 | | manager | | | LOCTIME | | | |
| | | manager login on | | port0 | | | | |

ログレベル

ログメッセージは、イベントの重要度によって次のように分類されます。

| ログレベル | 呼称 | 説明 |
|-------|-----------|---|
| 7 | CRITICAL | きわめて重大な障害が発生している |
| 6 | URGENT | 緊急を要する情報。障害が発生し、システムの動作に影響を与える（与えた）可能性がある |
| 5 | IMPORTANT | 管理者の注意を要する重要な情報。障害の可能性がある |
| 4 | NOTICE | 管理者の注意を要するかもしれない情報 |
| 3 | INFO | 各種イベントの通知。通常運用を示すもので緊急性はない |
| 2 | DETAIL | 詳細な情報。通常運用時には無視してもかまわないが、役に立つこともあるかもしれない |
| 1 | TRIVIAL | さらに詳細な情報 |
| 0 | DEBUG | デバッグ用のきわめて詳細な情報。大量のメッセージが出力される可能性あり |

表 20:

ログフィルターの条件指定に使える比較演算子

| 演算子 | 例 | 意味 |
|--------------|---------------------------------------|---|
| < (以下) | SEVERITY=<5 (ログレベルが5以下) | フィールドの値が指定値以下の場合にマッチ |
| > (以上) | SEVERITY=>6 (ログレベルが6以上) | フィールドの値が指定値以上の場合にマッチ |
| ! (等しくない) | TYPE=!CMD (メッセージタイプがCMD でなければマッチ) | フィールドの値が指定値と異なればマッチ |
| 指定なし (等しい) | MODULE=FIREWALL | フィールドの値が指定値と等しければマッチ |
| % (部分文字列を含む) | MSGTEXT=%failed (メッセージ本文に「failed」を含む) | フィールドの値に指定した文字列が含まれていればマッチ。テキストフィールドでのみ有効 |

表 21:

ㄨ 比較演算子の前には必ず等号 (=) が必要です。

モジュール ID とモジュール名

次にモジュール ID とモジュール名の一覧を示します。

ㄨ 一覧には未サポートのモジュールも含まれています。

| ID | モジュール名 | 説明 |
|----|----------------|--|
| 0 | NONE | |
| 1 | - | 予約済み |
| 2 | FR, FRAMERELAY | フレームリレー DTE データリンクレイヤーモジュール |
| 3 | PPP | PPP (Point-to-Point Protocol) モジュール |
| 4 | APPLE | AppleTalk ルーティングモジュール |
| 5 | IP, IPG | IP (Internet Protocol) ルーティングモジュール。RIP、ICMP、UDP、SNMP を含む |
| 6 | IPX | Novell IPX ルーティングモジュール |
| 7 | SYN | 同期 (Synchronous) インターフェースドライバー。未サポート |
| 8 | DNT, DECNET | DECnet ルーティングモジュール。未サポート |
| 9 | - | 予約済み |
| 10 | - | 予約済み |
| 11 | - | 予約済み |
| 12 | - | 予約済み |
| 13 | X25C | X.25 DCE (レイヤー 3) ハンドラー。未サポート |
| 14 | Q931 | ITU-T 標準 Q.931 ISDN 呼制御 |
| 15 | - | 予約済み |
| 16 | - | 予約済み |
| 17 | LAPB | LAPB データリンクレイヤーモジュール (X.25 用)。未サポート |
| 18 | TEST | ルーター内蔵のハードウェア (インターフェース、コプロセッサ等) テストモジュール |
| 19 | LAPD | LAPD データリンクレイヤーモジュール (ISDN D チャンネル用) |
| 20 | STT | STT (Synchronous Tunnelling over TCP) モジュール。未サポート |
| 21 | STRM, STREAM | Stream プリンティング。未サポート |
| 22 | TCP | TCP (Transmission Control Protocol) モジュール |
| 23 | ETH | Ethernet ドライバーと論理リンク制御モジュール |
| 24 | PERM | Permanent assignments モジュール。未サポート |
| 25 | TS, TSERVER | ターミナルサーバーモジュール |

| | | |
|----|---------------|---|
| 26 | LPD | LPD (Line Printer Daemon) プリンターサーバーモジュール。未サポート |
| 27 | BRG | ブリッジモジュール |
| 28 | COMP | 圧縮モジュール |
| 29 | - | 予約済み |
| 30 | X25T | X.25 DTE (レイヤー 3) ハンドラー。未サポート |
| 31 | FLASH | FLASH デバイスドライバー |
| 32 | - | 予約済み |
| 33 | TLNT, TELNET | Telnet モジュール |
| 34 | SYS, SYSTEM | 一般システムモジュール |
| 35 | CH | コマンドプロセッサ |
| 36 | TTY | ターミナルドライバー (Telnet、非同期ポート用) |
| 37 | ICC, ISDNCC | ISDN 呼制御モジュール |
| 38 | MIOX | MIOX (Multiprotocol Interconnect Over X.25) モジュール。未サポート |
| 39 | BOOTP | BOOTP モジュール |
| 40 | NTP | NTP (Network Time Protocol) モジュール |
| 41 | BRI | ISDN BRI インターフェースデバイスドライバー |
| 42 | PRI | ISDN PRI インターフェースデバイスドライバー |
| 43 | PORT | 非同期ポートモジュール (デバイス非依存部分) |
| 44 | ENC, ENCRYPT | 暗号モジュール |
| 45 | USER | ユーザーログインモジュール。ユーザー認証データベースなど |
| 46 | ACC | 非同期コールコントロール (ACC) モジュール |
| 47 | ASYN | 非同期ポートモジュール (デバイス非依存部分) |
| 48 | LOAD | LOADER モジュール。リリースファイル、パッチファイルのダウンロード。その他のファイルのアップロード、ダウンロード等を司る |
| 49 | INST, INSTALL | インストールモジュール。ROM、FLASH、NVS からのブートストラップを司る |
| 50 | OSPF | OSPF (Open Shortest Path First) モジュール |
| 51 | RAD, RADIUS | RADIUS モジュール |
| 52 | GRE | GRE (Generic Routing Encapsulation) モジュール |
| 53 | TRG, TRIGGER | トリガーモジュール |
| 54 | SCR | スクリプトモジュール |
| 55 | TDM | TDM (Time Division Multiplexing) モジュール |
| 56 | FILE | ファイルサブシステム |
| 57 | LOG | ロギングモジュール |
| 58 | PING | マルチプロトコル Ping モジュール |
| 59 | SNMP | SNMP エージェントモジュール |

| | | |
|----|-----------|--|
| 60 | SCC | SCC ドライバー |
| 61 | PBX | PBX モジュール (アナログポート) |
| 62 | SA | SA (Security Association) モジュール |
| 63 | SYNCC | Synchronous Call Control |
| 64 | NAT | NAT (Network Address Translation) モジュール |
| 65 | - | 予約済み |
| 66 | IPV6 | IPv6 (Internet Protocol Version 6) モジュール |
| 67 | L2TP | L2TP (Layer Two Tunnelling Protocol) モジュール |
| 68 | - | 予約済み |
| 69 | HOSTMIB | Host Resources MIB |
| 70 | DHCP | DHCP (Dynamic Host Configuration Protocol) モジュール |
| 71 | INTERFACE | インターフェースモジュール |
| 72 | - | 予約済み |
| 73 | ENCO | 暗号・圧縮モジュール |
| 74 | STAR | STAR モジュール |
| 75 | SSH | SSH (Secure Shell) クライアント/サーバーモジュール |
| 76 | RSVP | RSVP (Resource Reservation Protocol) モジュール |
| 77 | FIREWALL | ファイアウォールモジュール |
| 78 | MAIL | SMTP (メール) クライアントモジュール |
| 79 | TPAD | TPAD (Transaction Packet Assembler/Disassembler) モジュール |
| 80 | - | 予約済み |
| 81 | IPSEC | IPsec モジュール |
| 82 | ISAKMP | ISAKMP モジュール |
| 83 | FINGER | FINGER クライアントモジュール |
| 84 | HTTP | HTTP クライアント/サーバーモジュール |
| 85 | DCP | DCP (Device Control Protocol) |
| 86 | RMON | RMON (Remote Monitoring) エージェント |
| 87 | SWITCH | レイヤー 3 スイッチングモジュール |
| 88 | VRRP | VRRP (Virtual Router Redundancy Protocol) モジュール |
| 89 | VLAN | VLAN (バーチャル LAN) |
| 90 | PCI | PCI ドライバー |
| 91 | GARP | GARP (Generic Attribute Registration Protocol) モジュール |
| 92 | STP | STP (Spanning Tree Protocol) モジュール |
| 93 | GUI | Web インターフェース |
| 94 | OSI | OSI (Open Systems Interconnection) |
| 95 | PKI | PKI (Public Key Infrastructure) モジュール |
| 96 | LDAP | LDAP (Lightweight Directory Access Protocol) モジュール |
| 97 | PIM | PIM (Protocol Independent Multicast) モジュール |

| | | |
|-----|-------|--|
| 98 | DVMRP | DVMRP (Distance Vector Multicast Routing Protocol) モジュール |
| 99 | - | 予約済み |
| 100 | - | 予約済み |
| 101 | - | 予約済み |
| 102 | - | 予約済み |
| 103 | BGP | BGP-4 (Border Gateway Protocol version 4) |

表 22:

タイプ/サブタイプ

ログメッセージのタイプ、サブタイプは次の通りです。

ㄱ 一覧には未サポートのタイプ/サブタイプも含まれています。

| タイプ ID/名称 | タイプ説明 | サブタイプ ID/名称 | サブタイプ説明 |
|-----------|--|-------------|---|
| 000/NULL | 該当するタイプ、サブタイプなし | 000/NULL | メッセージタイプに対応していない旧バージョンのログシステムが生成したメッセージ |
| 001/REST | 再起動 | 001/NORM | 通常の再起動 |
| | | 002/CRASH | クラッシュ後再起動 |
| | | 003/FAIL | 再起動・セルフテストに失敗 |
| 002/PINT | 物理インターフェース (BRI0、SYN1、PORT1、ETH0 など) | 001/UP | リンクアップ |
| | | 002/DOWN | リンクダウン |
| | | 003/WARN | 障害の兆候あり |
| | | 004/ERROR | 障害検出 |
| | | 005/RESET | リセット |
| | | 006/NTON | CARD=x LINE=y. NT has power. |
| | | 007/NTOFF | CARD=x LINE=y. NT power failure. |
| | | 008/CREATE | 活線状態での取り付け |
| | | 009/DEST | 活線状態での取り外し |
| 003/CALL | ISDN コール、ACC コール | 001/UP | 発呼 |

| | | | |
|-----------|----------------------------------|------------|--------------------------------------|
| 004/DLINK | データリンク層モジュール (例: LAPB、LAPD) | 002/DOWN | 切断 |
| | | 003/WARN | 障害の兆候あり |
| | | 004/ERROR | 障害検出 |
| | | 005/RESET | リセット |
| | | 001/UP | リンクアップ |
| | | 002/DOWN | リンクダウン |
| | | 003/WARN | 障害の兆候あり |
| | | 004/ERROR | 障害検出 |
| | | 005/RESET | リセット |
| 005/VINT | 仮想的なインターフェース (例: PPP0、FR1、SLIP2) | 006/PNORM | CARD=x LINE=y PER normal. |
| | | 007/PHIGH | CARD=x LINE=y PER limit exceeded. |
| | | 008/ACT | 起動 |
| | | 009/DEACT | 切断 |
| | | 001/UP | リンクアップ |
| | | 002/DOWN | リンクダウン |
| | | 003/WARN | 障害の兆候あり |
| | | 004/ERROR | 障害検出 |
| | | 005/RESET | リセット |
| 006/CIRC | 仮想回線 (サーキット) (例: DLC (論理パス)) | 006/ACT | オンデマンドインターフェースの起動 |
| | | 007/CREATE | インターフェースが作成 (CREATE) された |
| | | 008/DEST | インターフェースが削除 (DESTROY) された |
| | | 001/UP | リンクアップ |
| | | 002/DOWN | リンクダウン |
| | | 003/WARN | 障害の兆候あり |
| | | 004/ERROR | 障害検出 |
| | | 005/RESET | リセット |

| | | | |
|-----------|------------------|-----------|----------------------------------|
| | | 006/CONF | 自動設定やオプション のネゴシエーション |
| 007/ATT | モジュールのアタッチ | 001/ATTCH | モジュールがアタッチ された |
| | | 002/DETCH | モジュールがデタッチ された |
| | | 003/FAIL | モジュールのアタッチ に失敗した |
| 008/EXCEP | 予期しない例外状態の 検出 | 000/RESET | 再起動 |
| | | 001/EXTNO | External contact open. |
| | | 002/EXTNC | External contact closed. |
| | | 008/BUS | バスエラー |
| | | 012/ADDR | アドレスエラー |
| | | 016/INSTR | 不正な命令 |
| | | 032/PRIV | 権限違反 |
| | | 040/LINEA | Line A emulator |
| | | 044/LINEF | Line F emulator |
| | | 096/SPUR | Spurious interrupt |
| | | 128/TRAP0 | Trap #0 (fatal) |
| | | 132/TRAP1 | Trap #1 (restart) |
| | | 136/TRAP2 | Trap #2 (assert) |
| 009/BUFF | メモリー | 001/LEV1 | 空きメモリーがバッフ ァーレベル1を下回っ た |
| | | 002/LEV2 | 空きメモリーがバッフ ァーレベル2を下回っ た |
| | | 003/LEV3 | 空きメモリーがバッフ ァーレベル3を下回っ た |
| 010/LIC | ライセンス情報 | 001/REL | リリースライセンス情 報 |
| | | 002/COMP | ソフトウェア圧縮ライ センス情報 |
| 011/AUTH | 認証 | 001/OK | 認 証 成 功 (LOGIN、 CONNECT など) |

| | | | |
|------------|--|------------|----------------------------------|
| 012/BATCH | トリガー/スクリプト | 002/FAIL | 認証失敗 |
| | | 003/RFAIL | 連続的な認証失敗 |
| | | 001/ACT | トリガー/スクリプトの起動 |
| | | 002/CMD | トリガー/スクリプトコマンド |
| 014/LPD | LPD(プリンターサーバー) | 003/OUT | トリガー/スクリプトの出力 |
| | | | |
| 015/SYSLOG | syslog 経由で受信したメッセージのファシリティー(メッセージ生成元モジュール) | 000/KERN | カーネル(LOG_KERN) |
| | | 008/USER | ユーザープロセス(LOG_USER) |
| | | 016/MAIL | メールサブシステム(LOG_MAIL) |
| | | 024/DAEMON | システムデーモン(LOG_DAEMON) |
| | | 032/AUTH | セキュリティ/認証システム(LOG_AUTH) |
| | | 040/SYSLOG | syslog デーモン(syslogd)(LOG_SYSLOG) |
| | | 048/LPR | プリンタースプーラーサブシステム(LOG_LPD) |
| | | 056/NEWS | ネットニュースサブシステム(LOG_NEWS) |
| | | 064/UUCP | UUCP サブシステム(LOG_UUCP) |
| | | 072/CRON | 定期実行デーモン(cron)(LOG_CRON) |

| | | | |
|-----------|--------------------|--------------|--|
| | | 080/AUTHPRIV | セキュリティー/認証システム（特定ユーザーだけが読めるようにすべきもの）(LOG_AUTHPRIV) |
| | | 128/LOCAL0 | ローカル用に予約 (LOG_LOCAL0) |
| | | 136/LOCAL1 | ローカル用に予約 (LOG_LOCAL1) |
| | | 144/LOCAL2 | ローカル用に予約 (LOG_LOCAL2) |
| | | 152/LOCAL3 | ローカル用に予約 (LOG_LOCAL3) |
| | | 160/LOCAL4 | ローカル用に予約 (LOG_LOCAL4) |
| | | 168/LOCAL5 | ローカル用に予約 (LOG_LOCAL5) |
| | | 176/LOCAL6 | ローカル用に予約 (LOG_LOCAL6) |
| | | 184/LOCAL7 | ローカル用に予約 (LOG_LOCAL7) |
| 016/ACC | 非同期コールコントロール (ACC) | 001/SCR | スクリプトが見つからない |
| | | 002/CALL | ACC コールが見つからない |
| | | 003/PORT | ポートが存在しない |
| | | 004/ACT | 起動 |
| | | 005/DEACT | 切断 |
| | | 006/DIAL | ダイヤルイン接続が確立 |
| 017/NVS | NVS (不揮発性メモリー) | 001/RFAIL | NVS ブロックのオープン/読み込みエラー |
| | | 002/WFAIL | NVS ブロックへの書き込みエラー |
| | | 003/CFAIL | NVS ブロックの作成エラー |
| 018/FLASH | FLASH メモリー | | |
| 019/USER | ユーザー | 001/LON | ログオン (ログイン) |
| | | 002/LOFF | ログオフ |

| | | | |
|------------|-------------------------------------|-----------|---------------------------------------|
| | | 003/ADD | アカウント追加 |
| | | 004/DEL | アカウント削除 |
| | | 005/PWCHG | パスワード変更 |
| | | 006/PWERR | 管理者パスワード変更 失敗 |
| | | 007/PWSET | 管理者パスワード変更 成功 |
| | | 008/LOOP | ログインプロンプトで のループバック障害 |
| | | 009/TACQ | TACACS 要求 |
| | | 010/TACR | TACACS 応答 |
| | | 011/LFAIL | ログイン失敗 |
| | | 001/MGR | 管理者コマンド |
| | | 002/USER | 一般ユーザーコマンド |
| 020/CMD | コマンドプロセッサ | | |
| 021/MSG | コンソールメッセージ | 001/INFO | 一般的な情報 |
| | | 002/WARN | 警告 |
| | | 003/ERROR | エラー |
| 022/CONFIG | ルーター/ネットワー クのコンフィグレーションに関する情報/警告 | 001/TOPO | ネットワークトポロ ジー関係 |
| | | 002/NTNUM | ネットワーク番号の 重複 (IPX、AppleTalk など) |
| | | 003/NTNAM | ネットワーク名の重複 (AppleTalk など) |
| | | 004/SWINS | 活線状態でのボード挿 入 |
| | | 005/SWIN | 活線状態でのスワップ イン |
| | | 006/SWOUT | 活線状態でのスワップ アウト |
| | | 007/SWDEL | 活線状態でのボード交 換 (別種類のものに変 更) |
| | | | |
| | | | |
| | | | |
| 023/IPFILT | IP フィルター | 001/PASS | IP フィルターによる パケット通過 |
| | | 002/FAIL | IP フィルターによる パケット破棄 |

| | | | |
|------------|------------------------|------------|---------------------------------|
| | | 003/DUMP | IP フィルターによる パケットダンプ |
| | | 004/FRAG | IP フラグメントフィ ルターによるパケット 破棄 |
| | | 005/SA | SA による IP パケット 破棄 |
| | | 006/SRCRT | IP ソースルートフィ ルターによるパケット 破棄 |
| | | 007/RECRT | IP 経路記録パケット 転送 |
| 024/INTERR | 予期しない内部エラー | 001/BDPKT | システムコード内で不正 パケットを検出 |
| | | 002/IVPAR | 不正なパラメーターを 検出 |
| | | 003/BDATT | 下位層へのアタッチに 失敗 |
| 025/IPNAT | IP NAT (レン ジ NAT) | 001/FAIL | NAT によるパケット 破棄 |
| | | 002/INTCP | 外から中への TCP コ ネクション開始 |
| | | 003/INUDP | 外から中への UDP フ ロー開始 |
| | | 004/OUTTCP | 中から外への TCP コ ネクション開始 |
| | | 005/OUTUDP | 中から外への UDP フ ロー開始 |
| 026/LIMIT | 内部的な制限値オー バー | 001/IPXSV | IPX サービステーブル の空き容量ゼロ |
| | | 002/IPXRT | IPX ルートテーブルの 空き容量ゼロ |
| | | 003/SWCMP | ソフトウェア圧縮チャ ンネルがすべて使用中 |
| 027/DHCP | DHCP | 001/BIND | デバイスにアドレスを 割り当て |
| | | 002/FREE | デバイスからアドレス を解放 |
| | | 003/FAIL | デバイスへのアドレス 割り当てを拒否 |

| | | | |
|----------|-------------------------|-----------------|-----------------------|
| 028/PBX | PBX(アナログポート) | 001/OIF | ルーター側の問題により発呼失敗 |
| | | 002/ONF | 網側の問題により発呼失敗 |
| | | 003/OOK | 発呼成功 |
| | | 004/IIF | ルーター側の問題により着呼失敗 |
| | | 005/INF | 網側の問題により着呼失敗 |
| | | 006/IOK | 着呼成功 |
| | | 007/OVER | 優先発信 (オーバーライド) |
| | | 008/POVER | 高優先度オーバーライド |
| | | 009/HOOK | Extension on/off hook |
| | | 010/FEAT | PBX の各種機能有効化 |
| 029/RSO | リモートセキュリティーオフィサー(RSO) | 001/ADD | RSO アドレス追加 |
| | | 002/DELETE | RSO アドレス削除 |
| | | 003/ENABLED | RSO 有効化 |
| | | 004/DISABLED | RSO 無効化 |
| | | 005/ACCEPT | RSO アクセスを受理 |
| | | 006/REJECT | RSO アクセスを拒否 |
| 030 | | | 予約済み |
| 031/ENCO | ENCO (暗号・圧縮) モジュール | 001/9711 | Hifin 9711 チップサブシステム |
| | | 002/STACSW | STAC SW サブシステム |
| | | 003/CRYP | Cryptech チップサブシステム |
| | | 004/PAC | PAC カードサブシステム |
| | | 005/MAC | MAC カードサブシステム |
| 032/RSVP | RSVP | 001/PATH_REMOVE | Path 削除 |
| | | 002/PATH_ADDED | Path 追加 |

| | | | |
|--------------|--------------|---------------------|--------------------------|
| | | 003/SESSION_REMOVED | セッション削除 |
| | | 004/SESSION_ADDED | セッション追加 |
| | | 005/RESV_ADDED | 帯域予約追加 |
| | | 006/RESV_REMOVED | 帯域予約削除 |
| | | 007/RESV_DENIED_RES | リソース不足による予約拒否 |
| 033/SSH | Secure Shell | 001/USER_ADD | SSH ユーザー追加 |
| | | 002/USER_DELETE | SSH ユーザー削除 |
| | | 003/USER_SET | SSH ユーザーの設定変更 |
| | | 004/ENABLED | SSH サーバー有効化 |
| | | 005/DISABLED | SSH サーバー無効化 |
| | | 006/ACCEPT | SSH 接続受理 |
| | | 007/REJECT | SSH 接続拒否 |
| | | 008/DISCONNECT | SSH 接続切断 |
| 034/TPAD | TPAD | 001/TCONN | TPAD 端末セッション接続 |
| | | 002/TDISC | TPAD 端末セッション切断 |
| | | 003/CALL | TPAD が X.25 による発呼を試行 |
| | | 004/CLEAR | TPAD または網により X.25 コールを切断 |
| | | 005/FAIL | X.25 コールの発呼に失敗 |
| | | 006/ONLINE | コール確立。トランザクション開始準備完了 |
| | | 007/OFFLINE | コール完了・切断 |
| 035/MAIL | メールサブシステム | 001/SUBMIT | SMTP サーバーにメッセージ送信 |
| | | 002/START | SMTP サーバーとのセッション開始 |
| | | 003/END | SMTP サーバーとのセッション切断 |
| | | 004/ERROR | SMTP サーバーからエラーを受信 |
| 036/FIREWALL | ファイアウォール | 001/INATCP | 外部から内部への TCP セッション開始 |

| | |
|---------------|------------------------------|
| 002/INAUDP | 外部から内部への UDP フロー開始 |
| 003/INAICMP | 外部から内部への ICMP フロー開始 |
| 004/INAOTHER | 外部から内部へのその 他 IP フロー開始 |
| 005/OUTATCP | 内部から外部への TCP セッション開始 |
| 006/OUTAUDP | 内部から外部への UDP フロー開始 |
| 007/OUTAICMP | 内部から外部への ICMP フロー開始 |
| 008/OUTAOTHER | 内部から外部へのその 他 IP フロー開始 |
| 009/INDTCP | 外部から内部への TCP セッションを拒 否 |
| 010/INDUDP | 外部から内部への UDP フローを拒否 |
| 011/INDICMP | 外部から内部への ICMP フローを拒否 |
| 012/INDOTHER | 外部から内部へのその 他 IP フローを拒否 |
| 013/OUTDTCP | 内部から外部への TCP セッションを拒 否 |
| 014/OUTDUDP | 内部から外部への UDP フローを拒否 |
| 015/OUTDICMP | 内部から外部への ICMP フローを拒否 |
| 016/OUTDOTHER | 内部から外部へのその 他 IP フローを拒否 |
| 017/ATTACK | 攻撃を受けている |
| 018/ENABLE | ファイアウォール有効 化 |
| 019/DISABLE | ファイアウォール無効 化 |
| 020/DESTROY | ファイアウォールポリ シー削除 |

| | | | |
|----------------|-----------------|----------------|---------------------------------|
| | | 022/SYNQCHNG | ファイアウォール Syn キュー状態の変化 |
| | | 023/HTTP | HTTP 接続を拒否 |
| | | 024/NOSESSION | アクティブな TCP セ ッションなし |
| | | 025/NEWSESSION | 最初の TCP セッショ ン作成 |
| | | 026/SIPALG | ALG エラーを検出 |
| | | 027/LIMITRULE | 上限ルールにより接続 を拒否 |
| 037/ACCOUNTING | アカウンティング | 001/START | トラフィックフロー開 始 |
| | | 002/UPDATE | トラフィックフローの 統計更新 |
| | | 003/END | トラフィックフロー終 了 |
| 038/FEATURE | フィーチャーライセン ス | 001/EXP | フィーチャーライセン スの試用期限終了 |
| 039 | | | 予約済み |
| 040 | | | 予約済み |
| 041 | | | 予約済み |
| 042/IPSEC | IPsec | 001/MSG | 一般情報 |
| | | 002/INERR | 内向きプロセス |
| | | 003/OUTERR | 外向きプロセス |
| 043/ISAKMP | ISAKMP | 001/XCHG | ISAKMP エクスチェ ンジ |
| | | 002/SA | SA |
| | | 003/ERROR | エラー |
| | | 004/MSG | 一般情報 |
| 044/BOOTP | BOOTP | 001/ETHCONF | Ethernet インターフ ェースの設定 |
| 045/HTTP | HTTP サーバー | 001/GETOK | GET 成功 |
| | | 002/GETFAIL | GET 失敗 |
| | | 003/EXCPT | 例外イベント |
| 046/VRRP | VRRP | 001/MRET | マスタールーターから バックアップルーター に移行 |

| | | | |
|----------------|-----------------------------------|---------------|---|
| | | 002/MNEW | 新しいマスタールーターの選出 |
| | | 003/BADAD | 無効な Advertisement パケット受信 |
| | | 004/NOIP | IP インターフェースなし |
| | | 005/RISMAST | マスタールーターに移行 |
| | | 006/PRIORITY | ルーター優先度変更 |
| 047/PPPOE | PPPoE | 001/SNA | 要求されたサービスは現在使用不可能 |
| | | 002/NAS | 要求されたサービスが存在しない |
| 048/FILE | ファイル | 001/DIR | ディレクトリーエントリーの追加 / 削除エラー |
| | | 002/CREATE | ファイル作成 |
| | | 003/DELETE | ファイル削除 |
| | | 004/RENAME | ファイル名変更 |
| 049/IPv6FILTER | IPv6 フィルター | 001/FILT_PASS | IPv6 フィルターによるパケット通過 |
| | | 002/FILT_FAIL | IPv6 フィルターによるパケット破棄 |
| | | 003/FILT_DUMP | IPv6 フィルターによるパケットダンプ |
| 050/PKI | PKI (Public Key Infrastructure) | 001/PKI_CERT | PKI 証明書メッセージ (PKI certificate message) |
| | | 002/PKI_CRL | PKI 証明書失効リストメッセージ (PKI certificate revocation list message) |
| | | 003/PKI_OP | PKI オペレーショナルプロトコルメッセージ (PKI operational protocol message) |

| | | | |
|-------------|---------------------------|-----------------|---|
| | | 004/PKIMP | PKI マネージメント プロトコルメッセージ (PKI management protocol message) |
| 051/SYSINFO | システムステータス情 報 | 001/PS | 電源状態の変化 |
| | | 002/FAN | ファン状態の変化 |
| | | 003/TEMP | 温度状態の変化 |
| 052/DNS | DNS キャッシュ | | DNS キャッシュ |
| 075/SQOS | SQOS(Software Qo- S) | 001/PAUS | トラフィッククラスー 時停止 |
| | | 002/UNPAUS | トラフィッククラスー 時停止解除 |
| | | 003/QEXCE | キュー上限超過 |
| | | 004/DCEXCE | DAR クラシファイア 上限超過 |
| 077/WANLB | WAN ロードバランス | 001/RESSTSTE | リソース状態の変化 |
| | | 002/NORES | アクティブなリソース なし |
| | | 003/HEALTHCHECK | ヘルスチェック用ホス ト到達不可 |
| | | 004/DNSFAILURE | DNS 問い合わせ失敗 |
| 092/MSG | ダイナミック DNS | 001/INFO | ダイナミック DNS ホ ストのアップデート |
| | | 002/WARN | ダイナミック DNS ホ ストのアップデート失 敗 |

表 23:

syslog 形式への変換

ログメッセージを syslog サーバーに転送するときは、あらかじめ syslog 形式にメッセージが変換されます。

ログレベルと syslog レベルのマッピング

ログメッセージのログレベルは、syslog の「レベル」に以下の通りマッピングされます。

| ログレベル | syslog レベル |
|---------------|------------|
| 7 (CRITICAL) | LOG_EMER |
| 6 (URGENT) | LOG_ALERT |
| 5 (IMPORTANT) | LOG_CRI |

| | |
|-------------|-------------|
| 4 (NOTICE) | LOG_ERR |
| 3 (INFO) | LOG_WARNING |
| 2 (DETAIL) | LOG_NOTICE |
| 1 (TRIVIAL) | LOG_INFO |
| 0 (DEBUG) | LOG_DEBUG |

表 24:

メッセージタイプと syslog ファシリティの対応表

本製品のログメッセージタイプは、syslog の「ファシリティ」に以下の通りマッピングされます。

| メッセージタイプ | syslog ファシリティ | 意味 |
|-----------|---------------|-------------------------------|
| 000/NULL | LOG_USER | メッセージタイプなしのメッセージ |
| 010/LIC | LOG_USER | ライセンス情報 |
| 011/AUTH | LOG_AUTH | 認証 |
| 012/BATCH | LOG_CRON | トリガー/スクリプト |
| 014/LPD | LOG_LPR | LPD プリンターサーバー |
| 001/REST | LOG_LOCAL7 | 再起動 |
| 008/EXCEP | LOG_LOCAL7 | 例外状況 |
| 009/BUFF | LOG_LOCAL7 | メモリー |
| 002/PINT | LOG_LOCAL6 | 物理インターフェース (BRI、SYN、PORT など) |
| 004/DLINK | LOG_LOCAL6 | データリンク層モジュール (LAPB、LAPD) |
| 003/CALL | LOG_LOCAL5 | ISDN コール、ACC コール |
| 005/VINT | LOG_LOCAL5 | 仮想的なインターフェース (PPP、SLIP、FR など) |
| 006/CIRC | LOG_LOCAL4 | 仮想回線 (フレームリレー DLC など) |
| 007/ATT | LOG_LOCAL4 | モジュールのアタッチ/デタッチ |
| その他 | LOG_USER | 上記以外のメッセージタイプ |

表 25:

メッセージタイプごとに異なるファシリティを使用するのではなく、出力先ごとに決まったファシリティ (LOG_LOCAL1 ~ LOG_LOCAL7) を使うこともできます。これには、CREATE LOG OUTPUT コマンド (164 ページ)、SET LOG OUTPUT コマンド (300 ページ) の FACILITY パラメーターを使用します。たとえば、syslog サーバー 192.168.10.5 宛てのメッセージすべてにファシリティ「LOG_LOCAL1」をセットするには、次のようにします。

```
CREATE LOG OUTPUT=1 DESTINATION=SYSLOG SERVER=192.168.10.5
FACILITY=LOCAL1 ↵
```

スクリプト

スクリプト機能は、あらかじめファイルに記述された一連のコマンドを一括して実行する機能です。スクリプトは設定情報の保存に使うほか、頻繁に行う一連の処理をまとめたシェルスクリプト/バッチファイル的な使い方をしたり、トリガー機能と組み合わせてイベント発生時になんらかの処理を自動実行させたりと、工夫次第でさまざまな用途が考えられる便利な機能です。

スクリプトファイルは拡張子が.scp か.cfg のファイルで、内容はルーターの管理コマンドを列挙したテキストファイルです。慣例として、.cfg は設定情報を保存する設定スクリプト、.scp はバッチファイル的なスクリプトに使われますが、絶対的な区別はありません。

スクリプトファイルを作成するには、次の方法があります。

- 内蔵スクリーンエディター (EDIT コマンド (240 ページ)) で作成・編集する

```
EDIT myscript.scp ↵
```

- ADD SCRIPT コマンド (133 ページ) SET SCRIPT コマンド (323 ページ) でコマンドラインから作成する。

```
ADD SCRIPT=simple.scp TEXT="show file" ↵
```

- LOAD コマンド (271 ページ) を使って別のコンピューター上で作成したファイルをダウンロードする。

```
LOAD METHOD=TFTP FILE=basic.scp SERVER=192.168.1.3 DEST=FLASH ↵
```

スクリプトは次のときに実行されます。

- コマンドラインから ACTIVATE SCRIPT コマンド (120 ページ) を実行したとき

```
ACTIVATE SCRIPT=gogo.scp ↵
```

- ルーターの起動時 (SET CONFIG コマンド (295 ページ) で指定された起動スクリプトが読み込まれ実行される)
- トリガーから呼び出されたとき

なお、boot.cfg という名前のスクリプトは特殊で、もし存在していれば起動時に自動実行されます (ただし、SET CONFIG コマンド (295 ページ) で起動時設定ファイルが指定されていないとき)。

スクリプト内の各行を実行するときは、一行実行するごとに短いウェイトが入ります。これは、スクリプトの実行がシステム本来の動作に与える影響を少なくするためです。なお、boot.cfg だけはウェイトなしで実行されます。

スクリプトが出力した文字列は、通常端末画面に出力されます。boot.cfg だけは特別で、デフォルトではログに出力されるよう設定されています。

また、ACTIVATE SCRIPT コマンド (120 ページ) でスクリプトを実行するときは、OUTPUT=LOG を指定することにより、出力をログに送ることができます。

＼ ただし、スクリプトが出力するログメッセージのログレベルが 2 (DETAIL) であるため、デフォルト設定では

システムログには記録されません。

スクリプトには最大 8 つまで引数を与えることができます。
コマンドラインから実行するときは、次のように指定します。

```
ACTIVATE SCRIPT=getargs.scp arg1 arg2 arg3 arg4 arg5 arg6 arg7 arg8 ↵
```

スクリプト中では、引数 1 (arg1) ~ 8 (arg8) を変数 %1 ~ %8 として参照できます。これらの変数はスクリプトの実行直前に実際の値に置き換えられます。

＼ 引数の長さが 31 文字を超えた場合、スクリプト中では 31 文字に切り詰められます。

また、スクリプト中ではグローバルな特殊変数として次の 4 つを使用できます。

| 変数名 | 内容 |
|-----|------------------------------------|
| %D | システム日付。dd-mmm-yyyy の形式 |
| %T | システム時刻。hh:mm:ss の形式 |
| %N | システム名。SET SYSTEM NAME コマンドで設定したもの |
| %S | シリアル番号。SHOW SYSTEM コマンドで表示されるものと同じ |

表 26: スクリプトの特殊変数

トリガーからスクリプトが呼び出されるときは、トリガーの種類によって異なる種類の引数が自動的に渡されます。たとえば、ファイアウォールトリガーは、第 1 引数 (%1) としてファイアウォールポリシー名を、第 2 引数 (%2) として攻撃者の IP アドレスをスクリプトに渡します。詳細は「運用・管理」の「トリガー」をご覧ください。

スクリプト内では、条件分岐構文 IF THEN ELSE ENDIF を使用できます。

```
IF string1 {EQ|NE} string2 THEN
    commands...
ELSE
    commands..
ENDIF
```

ELSE 節は省略できます。

EQ、NE は文字列比較演算子で、それぞれ等しい、等しくないを示します。比較時には大文字小文字は区別されません。条件判断の結果が真であれば THEN 節が、偽であれば ELSE 節（存在する場合。ないときは IF THEN ENDIF のあとに飛ぶ）が実行されます。

スクリプトの中でだけ使用できるコマンドに WAIT コマンド（491 ページ）があります。これは指定した秒数だけ待機するものです。

```
WAIT 5 ↵
```

スクリプトファイルの内容を確認するには、SHOW SCRIPT コマンド（434 ページ）を使います。

```
SHOW SCRIPT=myscript.scp ↵
```

トリガー

トリガー機能は、決められた時刻や特定のイベントが発生したときに、任意のスクリプトを自動実行する機能です。この機能を利用すれば、時間帯によってルーターの設定を変えたり、攻撃を受けたときにメールで管理者に通知したりすることができます。

トリガーには次の種類があります。

| 種類 | 説明 |
|--------------|---|
| CPU トリガー | CPU の負荷率がしきい値を超えたときに起動される |
| メモリートリガー | メモリーの空き容量がしきい値を超えたときに起動される |
| ファイアウォールトリガー | ファイアウォールイベント（攻撃検知など）の発生時に起動される |
| 再起動トリガー | システム起動（再起動）時に起動される |
| モジュールトリガー | モジュールイベントの発生時に起動される。イベント内容はモジュールによって異なる |
| 定期実行トリガー | 一定の間隔（たとえば 1 時間ごと）で繰り返し起動される |
| 定時トリガー | 決められた時刻に起動される |
| インターフェーストリガー | 指定したインターフェースのリンクステータスが変化するとき（リンクアップ、リンクダウンなど）に起動される |

表 27:

各トリガーには複数のスクリプトを関連付けることができます。また、トリガーの実行回数に制限を設けることも可能です（たとえば、5 回実行されたらトリガーを無効にするなど）。

トリガー機能を使用するには、トリガーモジュールを有効にする必要があります。デフォルトは無効です。

```
ENABLE TRIGGER ↓
```

トリガーを作成するには次のコマンドを使います。以下、トリガーの種類ごとに例を示します。

- CPU の負荷が 80%を超えたら、cpuwarn.scp を実行する CPU トリガー「1」を作成

```
CREATE TRIGGER=1 CPU=80 DIRECTION=UP SCRIPT=cpuwarn.scp ↓
```

- 空きメモリー容量が 30%を切ったら、memwarn.scp を実行するメモリートリガー「2」を作成

```
CREATE TRIGGER=2 MEMORY=30 DIRECTION=DOWN SCRIPT=memwarn.scp ↓
```

- 攻撃開始を検知したら、fwmail.scp を実行して管理者にメールを送るファイアウォールトリガー「3」を作成

```
CREATE TRIGGER=3 FIREWALL=ALL MODE=START SCRIPT=mail.scp ↓
```

- システムクラッシュ後に crash.scp を実行して管理者にメールを送る再起動トリガー「4」を作成

```
CREATE TRIGGER=4 REBOOT=CRASH SCRIPT=crash.scp ↓
```

- バージナルルーター「10」のマスタールーターになったら、bemaster.scp を実行するモジュールトリガー「5」を作成

```
CREATE TRIGGER=5 MODULE=VRRP EVENT=UPMASTER VRID=10
SCRIPT=bemaster.scp ↓
```

- 3 時間に一回 patrol.scp を実行する定期実行トリガー「6」を作成

```
CREATE TRIGGER=6 PERIODIC=180 SCRIPT=patrol.scp ↓
```

- 毎日夜 11 時に pppon.scp を実行して PPP コネクションを開く定時トリガー「7」を作成

```
CREATE TRIGGER=7 TIME=23:00 SCRIPT=pppon.scp ↓
```

- PPP インターフェース「0」がリンクダウン（LCP がダウン）したら、pppdown.scp を実行するインターフェーストリガー「8」を作成

```
CREATE TRIGGER=8 INTERFACE=ppp0 CP=LCP EVENT=DOWN
SCRIPT=pppdown.scp ↓
```

テストなどのため、トリガーを手動で起動するには ACTIVATE TRIGGER コマンド（121 ページ）を使います。

```
ACTIVATE TRIGGER=1 ↓
```

トリガーにスクリプトを追加するには、ADD TRIGGER コマンド（149 ページ）を使います。

```
ADD TRIGGER=2 SCRIPT=second.scp ↓
```

トリガーからスクリプトを削除するには、DELETE TRIGGER コマンド（205 ページ）を使います。NUMBER パラメーターには、スクリプトのインデックス番号を指定します。

```
DELETE TRIGGER=2 NUMBER=2 ↓
```

トリガーを削除するには、DESTROY TRIGGER コマンド（211 ページ）を使います。

```
DESTROY TRIGGER=5 ↓
```

トリガーの情報を確認するには、SHOW TRIGGER コマンド（470 ページ）を使います。

```
SHOW TRIGGER=3 ↓
```

```
SHOW TRIGGER=3 FULL ↓
```

```
SHOW TRIGGER=3 SUMMARY ↓
```

```
SHOW TRIGGER=3 STATUS ↓
```

```
SHOW TRIGGER=3 COUNT ↓
```

SNMP

本製品は、ネットワーク管理プロトコル SNMP (Simple Network Management Protocol) のバージョン 1 (SNMPv1)、バージョン 2c (SNMPv2c)、バージョン 3 (SNMPv3) に対応しています。

SNMPv3 では、認証・暗号化機能や MIB オブジェクトへのアクセス制御など大幅な拡張がなされています。そのため、バージョン 1、2c とバージョン 3 では設定方法が大きく異なります。以下では、最初にバージョン 1、2c の設定を紹介し、その後バージョン 3 の設定について解説します。

SNMPv1/SNMPv2c

ここでは、SNMPv1/SNMPv2c の設定方法について解説します。

基本設定

ここでは、SNMPv1/SNMPv2c を利用するために必要な最小限の設定を紹介します。以下の例では、IP の設定は終わっているものとします。

| SNMP コミュニティー | viewers (読み出しのみ) |
|------------------------------|------------------|
| SNMP 管理ホスト (v1) の IP アドレス | 192.168.10.5 |
| SNMP 管理ホスト (v2c) の IP アドレス | 192.168.10.6 |
| SNMP トラップホスト (v1) の IP アドレス | 192.168.10.5 |
| SNMP トラップホスト (v2c) の IP アドレス | 192.168.10.6 |

表 28:

1. SNMP エージェントを有効にします。また、認証トラップをオンにして、不正な SNMP アクセスに対してトラップを発生するように設定します。

```
ENABLE SNMP ↵
ENABLE SNMP AUTHENTICATE_TRAP ↵
```

2. SNMP コミュニティーを作成します。ここでは、読み出しのみが可能なコミュニティー「viewers」を作成しています。

```
CREATE SNMP COMMUNITY=viewers ACCESS=READ ↵
```

✎ コミュニティー名は大文字と小文字を区別するのでご注意ください。

✎ コミュニティー名は SNMP においてパスワードのような役割を果たします。よく考えた上で命名してください。特に、書き込み権限のあるコミュニティー名の設定には注意が必要です。不用意に書き込み権限のあるコミュニティーを作成すると、ルーターの設定を外部から変更されてしまう可能性がありますのでご注意ください。

✎ 多くのネットワーク機器や SNMP マネージャーソフトには、慣例として読み出し権限のみのコミュニ

ティーとして「public」が、書き込み権限ありのコミュニティとして「private」がデフォルトで設定されています。

3. SNMP コミュニティー「viewers」に管理ホストとトラップホストを追加します。

エージェントは、ここで指定した管理ホストからの SNMP 要求にだけ応答します。管理ホストを追加するときに SNMPv1、SNMPv2c の区別は必要ありません。SNMPv1 の要求に対しては SNMPv1 で、SNMPv2c の要求に対しては SNMPv2c で応答します。

またトラップは、ここで指定したトラップホストにのみ送信されます。トラップホストを追加するときは、各ホストが SNMPv1、SNMPv2c のどちらに対応しているかを意識してください。SNMPv1 形式のトラップを受信したいホストは TRAPHOST (V1TRAPHOST も同じ) パラメーターで、SNMPv2c 形式のトラップを受信したいホストは V2CTRAPHOST パラメーターで追加してください。

```
ADD SNMP COMMUNITY=viewers MANAGER=192.168.10.5
    TRAPHOST=192.168.10.5 ↵
ADD SNMP COMMUNITY=viewers MANAGER=192.168.10.6
    V2CTRAPHOST=192.168.10.6 ↵
```

4. 「viewers」コミュニティ所属のトラップホストに対するトラップの送信を有効にします。

```
ENABLE SNMP COMMUNITY=viewers TRAP ↵
```

✎ 本コマンドを実行しないとトラップが送信されません。

✎ SNMP トラップの送信を有効にしている場合、RESTART コマンド (293 ページ) 実行時は、REBOOT オプション (ハードウェアリセット) ROUTER オプション (ソフトウェアリセット) のどちらを指定した場合でも、coldStart トラップが送信されます。warmStart トラップは、RESET IP コマンド (「IP」の 337 ページ) を実行したときに送信されます。

基本設定は以上です。

これにより、SNMP 管理ホストから本製品の MIB 情報を取得できるようになります。また、本製品からの SNMP トラップがトラップホストに送信されるようになります。

その他

管理ホストやトラップホストを追加するには、ADD SNMP COMMUNITY コマンド (134 ページ) を使います。次の例では、コミュニティ「viewers」に管理ホスト「192.168.10.10」、トラップホスト (SNMPv1 形式)「192.168.10.10」を追加しています。

```
ADD SNMP COMMUNITY=viewers MANAGER=192.168.10.10 TRAPHOST=192.168.10.10 ↵
```

✎ 管理ホストを追加するときは、SNMPv1、SNMPv2c の区別は不要です。どちらも MANAGER パラメーターで追加できます。一方、トラップホストを追加するときは、SNMPv1 形式のトラップを受信するホストなら TRAPHOST (または V1TRAPHOST) パラメーター、SNMPv2c 形式のトラップを受信するホストなら V2CTRAPHOST パラメーターを使ってください。

- 管理ホストを指定するときは、「192.168.20.0/24」のようにマスク長を付加して範囲指定することも可能です。なお、トラップホストは範囲指定できません。

書き込み権限のあるコミュニティを作成するには、CREATE SNMP COMMUNITY コマンド (167 ページ) の ACCESS パラメーターに「WRITE」を指定します (ACCESS パラメーター省略時の権限は読み込みのみ (READ) です)。

```
CREATE SNMP COMMUNITY=admins ACCESS=WRITE MANAGER=192.168.10.5 ↵
```

本製品の SNMP エージェントは、デフォルトでは管理ホストとして登録されたコンピューター以外からの SNMP 要求には応答しません。この制限をなくすには、コミュニティの OPEN (open access) パラメーターを YES にします。次に具体例を挙げます。

- コミュニティ作成時に OPEN=YES を指定 (省略時は OPEN=NO となります)

```
CREATE SNMP COMMUNITY=viewers ACCESS=READ OPEN=YES ↵
```

- コミュニティ作成後は SET SNMP COMMUNITY コマンド (325 ページ) を使います。

```
SET SNMP COMMUNITY=viewers OPEN=YES ↵
```

本製品は、SNMPv1 の要求には SNMPv1 で、SNMPv2c の要求には SNMPv2c で応答します。トラップ以外の SNMP オペレーションについては、バージョンを意識する必要はありません。ただし、トラップについては、送信先 (トラップホスト) ごとに v1、v2c どちらの形式を使うか指定する必要があります。これには、CREATE SNMP COMMUNITY コマンド (167 ページ)、ADD SNMP COMMUNITY コマンド (134 ページ) の TRAPHOST (または V1TRAPHOST)、V2CTRAPHOST パラメーターを使います。たとえば、192.168.10.10 には SNMPv1 形式のトラップを送り、192.168.10.20 には SNMPv2c 形式のトラップを送るには、次のように設定します。

```
ADD SNMP COMMUNITY=viewers TRAPHOST=192.168.10.10
V2CTRAPHOST=192.168.10.20 ↵
```

SNMP の設定を確認するには、SHOW SNMP コマンド (437 ページ)、SHOW SNMP COMMUNITY コマンド (441 ページ) を使います。

```
SHOW SNMP ↵
```

```
SHOW SNMP COMMUNITY=viewers ↵
```

SNMPv3

ここでは、SNMPv3 の設定方法について解説します。

基本設定

ここでは、SNMPv3 を利用するために必要な最小限の設定を紹介します。以下の例では、IP の設定は終わっ

ているものとします。

1. SNMP エージェントを有効にします。また、認証トラップをオンにして、不正な SNMP アクセスに対してトラップを発生するように設定します。

```
ENABLE SNMP ↵
ENABLE SNMP AUTHENTICATE_TRAP ↵
```

2. ビューを定義します。ビューは、MIB ツリーのどの部分にアクセスさせるかを定義するものです。ここでは、internet ノード (1.3.6.1) 以下をあらわすビュー「most」と、mib-2 ノード (1.3.6.1.2.1) 以下をあらわすビュー「standard」を作成します。

```
ADD SNMP VIEW=most MIB=internet TYPE=INCLUDE ↵
ADD SNMP VIEW=standard MIB=mib-2 TYPE=INCLUDE ↵
```

＼ ビューを定義するときは、MIB ノードを「1.3.6.1.2.1」のような OID (Object Identifier) で指定する方法と、「mib-2」のような名前指定する方法があります。OID で指定するときは ADD SNMP VIEW コマンド (144 ページ) の OID パラメーターを、名前指定するときは MIB パラメーターを使います。なお、名前指定できるのは、システムにあらかじめ登録されている代表的なノードだけです。既定のノード名については、ADD SNMP VIEW コマンド (144 ページ) の解説にある表をご覧ください。

＼ ビュー名は大文字と小文字を区別するのでご注意ください。

3. ユーザーグループを作成します。SNMPv3 の設定では、ユーザーグループごとに、通信時の認証・暗号化の有無 (セキュリティレベル) とビューへのアクセス権を設定します。

ここでは管理者グループ「admins」と閲覧者グループ「operators」を定義します。admins グループのユーザーには、most ビューへのフルアクセス権を与えます。また、通信時には認証と暗号化の両方を必須とします。一方、operators グループのユーザーには、standard ビューへの読み出しアクセス権だけを与えます。こちらは認証だけを必須とします。

```
ADD SNMP GROUP=admins SECURITYLEVEL=authPriv READVIEW=most
WRITEVIEW=most NOTIFYVIEW=most ↵
ADD SNMP GROUP=operators SECURITYLEVEL=authNoPriv READVIEW=standard ↵
```

4. ユーザーを作成します。ユーザー作成時には所属グループを指定します。また、所属グループで定められたセキュリティレベルにあわせて、認証・暗号化に使うプロトコルとパスワードを指定します。ここでは、admins グループのユーザー supervisor と operators グループのユーザー zein を作成します。

```
ADD SNMP USER=supervisor GROUP=admins AUTHPROTOCOL=SHA
  AUTHPASSWORD=jogejoge PRIVPROTOCOL=DES PRIVPASSWORD=mugomugo ↵
ADD SNMP USER=zein GROUP=operators AUTHPROTOCOL=MD5
  AUTHPASSWORD=fugafuga ↵
```

- ターゲットを定義します。ターゲットは、SNMPv1/v2c におけるトラップホストのようなもので、トラップなど通知メッセージの送信先となります。ターゲットを追加するには、最初にターゲットとの通信に使うパラメーターセットを定義し、その後ターゲットのアドレスを指定します。

- ターゲットパラメーターセット psuper を定義します。パラメーターセットを作成するときは、通知メッセージの送信時に使用するセキュリティレベルとユーザー名を指定します。ここでは、ユーザー名としてすでに定義済みの supervisor を使います（認証・暗号化の両方を使用）。

```
ADD SNMP TARGETPARAMS=psuper SECURITYLEVEL=authPriv
  USER=supervisor ↵
```

- ターゲット（通知メッセージの送信先）の IP アドレスと、通信時に使用するパラメーターセットを指定します。ターゲット名は任意に付けられます（ここでは tpR30）。

```
ADD SNMP TARGETADDR=tpR30 PARAMS=psuper IP=172.28.28.156 ↵
```

※ SNMP トラップの送信を有効にしている場合、RESTART コマンド（293 ページ）実行時は、REBOOT オプション（ハードウェアリセット）、ROUTER オプション（ソフトウェアリセット）のどちらを指定した場合でも、coldStart トラップが送信されます。warmStart トラップは、RESET IP コマンド（「IP」の 337 ページ）を実行したときに送信されます。

基本設定は以上です。

これにより、SNMPv3 対応の管理ソフトウェアから本製品の MIB 情報を取得できるようになります。また、本製品からの SNMP トラップがターゲットに送信されるようになります。

その他

SNMP エンジン ID を変更するには、SET SNMP ENGINEID コマンド（326 ページ）を使います。なお、同コマンドを実行すると、登録済みの SNMP ユーザーが削除されるのでご注意ください。

```
SET SNMP ENGINEID=001122334455667788 ↵
```

SNMPv1/v2c/v3 の共通事項

リンクアップ/リンクダウントラップは、デフォルトではオフになっています。リンクトラップを有効に

するには、ENABLE INTERFACE LINKTRAP コマンド（「インターフェース」の 32 ページ）を使います。スイッチポートは「portx」（x はポート番号）の形式で指定します。

```
ENABLE INT=port1 LINKTRAP ↓
```

VLAN インターフェース単位でリンクトラップを有効にするには次のようにします。ENABLE INTERFACE LINKTRAP コマンド（「インターフェース」の 32 ページ）では、VLAN 名を使った「vlan-white」のような指定はできませんのでご注意ください。

```
ENABLE INT=vlan10 LINKTRAP ↓
```

- ＼ VLAN インターフェースは、所属ポートがすべてリンクダウンして初めて「リンクダウン」状態になります。一方、VLAN 所属ポートが 1 ポートでもリンクアップすれば、該当 VLAN インターフェースは「リンクアップ」状態になります。スイッチポート、VLAN インターフェースのリンクステータスは、SHOW INTERFACE コマンド（「インターフェース」の 89 ページ）で確認できます。

リンクトラップの設定を確認するには SHOW INTERFACE コマンド（「インターフェース」の 89 ページ）を使います。「ifLinkUpDownTrapEnable」欄が「Enabled」ならリンクトラップが有効です。

```
SHOW INT=port1 ↓
```

本製品のシステム名（system.sysName.0）を設定するには SET SYSTEM NAME コマンド（338 ページ）を使います。

```
SET SYSTEM NAME=kkRouter ↓
```

システム名にフルドメイン名を設定しておくと、TELNET コマンド（486 ページ）実行時に必要に応じてドメイン名の補完が行われます。たとえば、システム名に「kkRouter.example.com」を設定した場合、TELNET コマンド（486 ページ）を「TELNET bulbul」のように実行すると、短いホスト名「bulbul」のあとに「example.com」が補われ、「bulbul.example.com」に対して DNS 検索が行われます。

本製品の設置場所（system.sysLocation.0）を設定するには SET SYSTEM LOCATION コマンド（337 ページ）を使います。

```
SET SYSTEM LOCATION="8F, TTC Bldg" ↓
```

本製品の管理責任者（system.sysContact.0）を設定するには SET SYSTEM CONTACT コマンド（335 ページ）を使います。

```
SET SYSTEM CONTACT="Taro ARAIDO (Ext 2602)" ↓
```

NTP

NTP (Network Time Protocol) を利用すると、ネットワーク上の NTP サーバーから時刻情報を取得し、システムの時計を常に正確にあわせておくことができます。ログなどの記録日時を正確に保つためにも、NTP の利用をおすすめします。

基本設定

NTP を使用するために最低限必要な設定を示します。ここでは次のような構成のネットワークを想定しています。IP の設定は終わっているものとします。

| | |
|-------------------------|------------------|
| NTP サーバーの IP アドレス | 192.168.10.5 |
| タイムゾーン (UTC からのオフセット) | JST (+9:00:00) |

表 29:

1. NTP モジュールを有効にします。

```
ENABLE NTP ↵
```

2. NTP サーバーの IP アドレスを指定します。サーバーは 1 つしか設定できません。

```
ADD NTP PEER=192.168.10.5 ↵
```

3. タイムゾーン (UTC からのオフセット) を設定します。NTP から得られる時刻情報は UTC (協定世界時) なので、必ずオフセットを指定してください。日本標準時 (JST) は UTC より 9 時間進んでいるので、次のように指定します。

```
SET NTP UTCOFFSET=+9:00:00 ↵
```

また、定義済みのタイムゾーン名を使って次のように指定することもできます。

```
SET NTP UTCOFFSET=JST ↵
```

4. 念のため NTP モジュールをいったんリセットします。

```
RESET NTP ↵
```

基本設定は以上です。

これにより、定期的に NTP サーバーに問い合わせを行い、システムの時計が自動的に調整されるようになります。

現在時刻は SHOW TIME コマンド (469 ページ) で確認します。

```
Manager > SHOW TIME
```

```
System time is 11:17:41 on Tuesday 03-Jul-2001.
```

NTP に関する情報は SHOW NTP コマンド (407 ページ) で確認します。

```

Manager > SHOW NTP

-----
NTP Module Configurations
-----
Status           : ENABLED
Host Address      : 192.168.10.169
UTC offset        : +09:00:00 (JST)
Last Updated      : 11:19:38 on 03-Jul-2001
Last Delta        : +0.94

Configured Peer
-----
192.168.10.5

Counters
-----
Packets Sent      : 0000000002
Packets Received   : 0000000002
Packets w/ head error : 0000000000
Packets w/ data error : 0000000000

```

NTP サーバーとしての動作

本製品の NTP モジュールは、「サーバーモード」および「クライアントモード」に対応しています。通常時はクライアントモードとして動作します。NTP クライアントからリクエストを受けた場合、クライアントへ応答を返すまでの間、サーバーモードとして動作します。

本製品が NTP サーバー（サーバーモード）として動作するためには、本製品が上位の NTP サーバーと接続されている必要があります。（上記の基本設定のように、ADD NTP PEER コマンド（130 ページ）で上位サーバーの IP アドレスを指定します。本製品はセカンダリータイムサーバーとして動作します。）

- クライアント側から本製品を NTP サーバーとして利用するためには、クライアント側の NTP の動作モードが「クライアントモード」である必要があります。Windows などの OS では、NTP のデフォルト動作モードが「対称アクティブモード」であるため、各クライアントで「クライアントモード」への設定変更が必要です。

付録

定義済みのタイムゾーン名一覧

| | | |
|------|--------|----------------------------------|
| ASIA | +8:00 | Asia |
| ACDT | +10:30 | Australian Central Daylight Time |
| ACST | +9:30 | Australian Central Standard Time |
| AEDT | +11:00 | Australian Eastern Daylight Time |

| | | |
|---------|--------|----------------------------------|
| AEST | +10:00 | Australian Eastern Standard Time |
| AWST | +8:00 | Australian Western Standard Time |
| BST | +1:00 | British Standard Time |
| CHINA | +8:00 | China |
| GMT | +0:00 | Greenwich Mean Time |
| UK | +0:00 | Greenwich Mean Time |
| HK | +8:00 | Hong Kong |
| JST | +9:00 | Japan Standard Time |
| MET | +1:00 | Mid-European time |
| NZDT | +13:00 | New Zealand Daylight Time |
| NZST | +12:00 | New Zealand Standard Time |
| SING | +8:00 | Singapore |
| TAIWAN | +8:00 | Taiwan |
| UTC | +0:00 | Universal Coordinated Time |
| CDT | -5:00 | US Central Daylight Time |
| CST | -6:00 | US Central Standard Time |
| EDT | -4:00 | US Eastern Daylight Time |
| EST | -5:00 | US Eastern Standard Time |
| MDT | -6:00 | US Mountain Daylight Time |
| MST | -7:00 | US Mountain Standard Time |
| PDT | -7:00 | US Pacific Daylight Time |
| PST | -8:00 | US Pacific Standard Time |
| DEFAULT | - | - |
| NONE | - | - |

表 30: タイムゾーン名一覧

Secure Shell

Secure Shell (SSH) は、暗号技術を利用してネットワーク経由のログインなどを安全に行うためのプロトコルです。通信内容の暗号化により盗聴や改ざんを防ぐほか、サーバーホストやユーザーの認証機能によってなりすましによる攻撃を防御することもできます。本製品は、SSHv1 のみに対応しています。

従来の Telnet では、パスワードを含む通信内容が平文のままネットワーク上を流れてしまうため、セキュリティを重視する環境では、Telnet でなく SSH を使ったほうがよいでしょう。

本製品の SSH モジュールは以下の機能をサポートしています。

- SSH サーバーと SSH クライアント
- 鍵長 512 ~ 2048 ビットの RSA 公開鍵。ルーター上で作成した鍵をファイルへ書き出すことや、ファイルから鍵を取り込むことも可能
- セッションの暗号化には共通鍵暗号アルゴリズム DES を使用
- 端末セッションだけでなく、コマンドの遠隔実行も可能

基本設定

ここでは、本製品を SSH サーバー (192.168.1.5) および SSH クライアントとして動作させるための基本設定について説明します。

暗号鍵の作成

最初に、サーバー側で 2 つの RSA 鍵ペア (ホスト鍵とサーバー鍵) を作成します。

1. セキュリティーモードで管理作業を行うことのできる Security Officer レベルのユーザーを作成します。ルーター上で作成した暗号鍵は、セキュリティモードでないとルーター再起動によって消去されてしまいます。セキュリティモードに移行するためには、Security Officer レベルのユーザーを登録しておく必要があります。

```
ADD USER=secoff PASSWORD=Passwords PRIVILEGE=SECURITYOFFICER ↵
```

2. ホスト鍵 (Host Key) を作成します。この鍵はサーバー自身の RSA 公開鍵ペアです。推奨鍵長は 1024 ビットです。SSH コネクションの開始時には、ホスト鍵ペアの公開鍵がクライアントに送られます。クライアントはこの鍵をチェックすることにより、接続相手が意図したサーバーであるかどうかを確認できます。

```
CREATE ENCO KEY=1 TYPE=RSA LENGTH=1024 DESCRIPTION="My host_key" ↵
```

3. サーバー鍵 (Server Key) を作成します。サーバー鍵は SSH コネクション開始時の鍵交換に用いられる RSA 公開鍵ペアです。サーバーの設定により、一定の間隔で新しく作り直されます。サーバー鍵の長さは最小 512 バイトで、なおかつ、ホスト鍵より 128 ビット以上短くなくてはなりません。

```
CREATE ENCO KEY=2 TYPE=RSA LENGTH=768 DESCRIPTION="My server_key" ↵
```

鍵番号は 0 ~ 65535 の範囲で自由に付けられます。以後、鍵は番号だけで識別することになるため、鍵を

作成するときは、DESCRIPTION パラメーターを使って、鍵の用途などコメントを付けておくといでしょう。このコメントは SHOW ENCO KEY コマンド（「暗号・圧縮」の 48 ページ）で鍵一覧を表示するときに表示されます。

RSA 鍵の作成には時間がかかります。上記コマンドを入力すると「RSA Key Generation process started.」と表示され、バックグラウンドで鍵の生成処理が始まります。鍵の作成中は CPU 負荷が高くなり、コンソールからのキー入力に対する反応が鈍くなります。鍵の作成が終わると「RSA Key generation process completed.」と表示されます。

作成した鍵の情報は SHOW ENCO KEY コマンド（「暗号・圧縮」の 48 ページ）で確認できます。

```
SHOW ENCO KEY ↵
SHOW ENCO KEY=1 ↵
```

セキュリティーモードに移行するには、ENABLE SYSTEM SECURITY_MODE コマンド（263 ページ）を使います。ただし、移行後は Security Officer レベルでないと各種設定が行えなくなりますのでご注意ください。セキュリティーモードを必要とする構成の設定を行う場合は、最初に Security Officer レベルのユーザーを作成しておき、ノーマルモードのまま各種設定を行い、すべての設定が完了して初めてセキュリティーモードに移行するのが便利です。

```
ENABLE SYSTEM SECURITY_MODE ↵
```

SSH サーバーの起動

サーバー上でホスト鍵とサーバー鍵を作成したら、SSH サーバーを起動します。このとき、ホスト鍵とサーバー鍵の番号を指定する必要があります。

ホスト鍵「1」、サーバー鍵「2」を使って SSH サーバーを稼働させます。

```
ENABLE SSH SERVER HOSTKEY=1 SERVERKEY=2 ↵
```

デフォルトでは、サーバー鍵の自動更新は行われません。自動更新を行うようにするには、EXPIRYTIME パラメーターで更新間隔（時間）を指定します。EXPIRYTIME パラメーターの省略時は 0（更新しない）となります。次の例では、24 時間（1 日）ごとに鍵を更新するよう設定しています。

```
ENABLE SSH SERVER HOSTKEY=1 SERVERKEY=2 EXPIRYTIME=24 ↵
```

㍻ 鍵の生成は負荷の高い処理なので、自動更新を行う場合は深夜などトラフィック負荷の少ない時間帯になるよう更新間隔を調整するとよいでしょう。

㍻ SSH サーバーを起動すると、ルーター内蔵 Telnet サーバーへのアクセスはできなくなります。

SSH サーバーの状態を確認するには、SHOW SSH コマンド（453 ページ）を使います。

```
SHOW SSH ↵
```


SSH ユーザーの登録

SSH サーバーを利用するには、SSH サーバー上で ADD SSH USER コマンド (147 ページ) を実行し、SSH ユーザーを登録する必要があります。SSH サーバーが有効になっていても、SSH ユーザーが登録されていないとサーバーにはアクセスできません。

SSH ユーザーは、本製品のユーザー認証データベースに登録されていなくてもかまいませんが、その場合ログイン時の権限は USER レベル (一般ユーザー権限) となります。SSH ユーザーと同じ名前のユーザーがルーターのデータベースに登録されている場合は、ユーザーデータベースでの権限が SSH ログインにも適用されます。

SSH ユーザーの設定方法は、使用するログイン認証方式によって異なります。ログイン方式には、次の 2 種類があります。

- パスワード認証：ユーザー名とパスワードによる認証方式です。
- RSA 認証：公開鍵による認証方式です。

1 ユーザーに対し、認証方式は 1 つだけしか選べません。

パスワード認証の場合

パスワード認証は、クライアントがユーザー名とパスワードをサーバーに送り、これをサーバーが確認する方法です。SSH ではパスワードを暗号化して送るため、ネットワーク上でパスワードを盗まれる可能性が低くなっています。

一般ユーザーの登録

```
ADD SSH USER=kuro PASSWORD=testpasswd1 ↵
```

ユーザー認証データベースに登録されていない名前の SSH ユーザーは、USER レベルとなります。また、ユーザー認証データベースに登録されている名前と同じであっても、登録されているユーザーの権限が USER レベルなら、SSH ユーザーも USER レベルとなります。

Manager 権限を持つユーザーの登録

```
ADD USER=shiro PASSWORD=testpasswd2 PRIVILEGE=MANAGER ↵
ADD SSH USER=shiro PASSWORD=testpasswd2 ↵
```

- ◈ ユーザー認証データベースに登録されているユーザー (ADD USER コマンド (151 ページ) で登録したユーザー) と同じ名前の SSH ユーザーを登録した場合、ユーザー権限はデータベースと同じになりますが、パスワードは別々に設定できます。ADD SSH USER コマンド (147 ページ) の PASSWORD パラメーターで指定したパスワードは、SSH ログイン時のパスワード認証でのみ使用されます。

SSH ユーザーは SHOW SSH USER コマンド (462 ページ) で確認します。

```
SHOW SSH USER ↵
SHOW SSH USER=shiro ↵
```

RSA 認証の場合

RSA 認証は、SSH クライアントユーザーの RSA 公開鍵ペアを利用して認証を行う方式です。秘密鍵を持っているのが SSH ユーザーだけであるという前提に立って、サーバーがユーザーを認証します。

RSA 認証を使用するときは、SSH クライアント側であらかじめユーザーの認証用公開鍵ペアを用意し、公開鍵を SSH サーバー上に登録しておく必要があります。

本製品を SSH クライアントにするときは、クライアントとなるルーター上で CREATE ENCO KEY コマンド（「暗号・圧縮」の 18 ページ）を実行し、認証鍵を作成します。

1. RSA 鍵ペアを作成します。鍵長は 512 ビット以上にします。推奨最大値は 1024 ビットです。これ以上鍵長を長くしても、処理が遅くなるだけで安全性はそれほど向上しないようです。

```
CREATE ENCO KEY=100 TYPE=RSA LENGTH=1024 ↵
```

2. 作成した鍵ペアの公開鍵を SSH サーバーに送るため、ファイルに書き出します。KEY パラメーターには書き出したい鍵の番号、FILE パラメーターには書き出し先のファイル名を指定します。ファイルの拡張子は key とします。また、FORMAT パラメーターには書き出す際のフォーマットを指定します。SSH で使うときは SSH を指定します。

```
CREATE ENCO KEY=100 TYPE=RSA FILE=pote.key FORMAT=SSH ↵
```

クライアントが PC などの場合は、SSH パッケージに含まれる ssh-keygen などの鍵生成プログラムを使ってユーザーの公開鍵ペアを作ります。鍵生成プログラムの使い方については、プログラム付属のマニュアル等をご覧ください。ここで挙げているのはあくまでも一例です（ssh-keygen コマンドの例）。

```
pote@clientpc:~> ssh-keygen -t rsa1 -C pote@clientpc
Generating RSA keys:  Key generation complete.
Enter file in which to save the key (/home/pote/.ssh/identity):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/pote/.ssh/identity.
Your public key has been saved in /home/pote/.ssh/identity.pub.
The key fingerprint is:
e9:0e:68:2a:8a:a3:75:dd:f1:61:37:09:fc:f6:a3:b2 pote@clientpc
```

クライアント側で認証鍵を作成したら、鍵ペアのうちの公開鍵を SSH サーバー側に転送します。TFTP 経由で転送するのがよいでしょう。

クライアント側

1. クライアントが本製品の場合は、UPLOAD コマンド（489 ページ）を使ってユーザーの公開鍵ファイルを TFTP サーバーにアップロードします。ここでは TFTP サーバーの IP アドレスを 192.168.10.5 とします。

```
UPLOAD FILE=pote.key SERVER=192.168.10.5 ↵
```

クライアントが PC などの場合は、TFTP サーバーを動かして自分自身が TFTP サーバーになるか、あるいは、TFTP クライアントを使って別の TFTP サーバーに公開鍵ファイルを転送してください。そのとき、ファイルの拡張子を .key にしておいてください。

サーバー側

1. 次に SSH サーバー側で LOAD コマンド (271 ページ) を実行し、TFTP サーバーからユーザーの公開鍵ファイルをダウンロードします。

```
LOAD FILE=pote.key SERVER=192.168.10.5 DESTINATION=FLASH ↓
```

2. 鍵ファイルは、ダウンロードしただけでは使えません。CREATE ENCO KEY コマンド (「暗号・圧縮」の 18 ページ) でファイルから鍵を取り込む必要があります。

```
CREATE ENCO KEY=100 TYPE=RSA FILE=pote.key FORMAT=SSH ↓
```

※ CREATE ENCO KEY コマンド (「暗号・圧縮」の 18 ページ) で FILE パラメーターを指定した場合、ファイルが存在するときは、そのファイルから情報を読み込んで鍵を作成します。ファイルが存在しないときは、KEY パラメーターで指定した既存の鍵情報をファイルに書き出します。

3. SSH ユーザーを登録します。このとき、ユーザーの公開鍵番号を KEY パラメーターで指定します。
一般ユーザーの登録

```
ADD SSH USER=bote KEYID=100 ↓
```

Manager 権限を持つユーザーの登録

```
ADD USER=pote PASSWORD=testpasswd3 PRIVILEGE=MANAGER ↓
```

```
ADD SSH USER=pote KEYID=100 ↓
```

※ RSA 認証を使う場合、ADD USER コマンド (151 ページ) の PASSWORD パラメーターで指定したパスワードは使用されません (コンソールからのログインや Telnet ログインで使用されます)。

SSH ユーザーは SHOW SSH USER コマンド (462 ページ) で確認します。

```
SHOW SSH USER ↓
```

```
SHOW SSH USER=pote ↓
```

SSH クライアントからの接続

クライアントが本製品の場合は、クライアント側で以下のコマンドを実行します。

パスワード認証の場合

```
SSH 192.168.10.1 USER=shiro PASS=testpasswd2 ↓
```

RSA 認証の場合

```
SSH 192.168.10.1 USER=pote KEYID=100 ↓
```

※ 初めて SSH サーバーに接続したときは、必ず以下のメッセージが表示され接続に失敗します。

```
Host key not recognised - saved as ssh.key
SSH. Session closed.
```

これはエラーではなく、SSH サーバーから SSH クライアント宛てにホスト鍵が送られたことを知らせるメッセージです。これにより、サーバーのホスト鍵がクライアントのファイルシステム上に「ssh.key」という名前で保存されます。上記のメッセージが表示された場合は、SSH クライアント側で次のコマンドを実行し、SSH サーバーのホスト鍵を登録してください。

```
CREATE ENCO KEY=10 TYPE=RSA FILE=ssh.key DESCRIPTION="SSH server's
hostkey" FORMAT=SSH ↵
```

一度このコマンドを実行した後は、上記コマンドでただちに接続できるようになります。

クライアントが PC などの場合は、PC 用の SSH クライアントソフトウェアを起動してサーバーに接続してください。通常、初回接続時にはホスト鍵の確認が行われます。ご使用の SSH クライアントのマニュアルをご覧ください。サーバー確認の手順を行ってください。

- 本製品は暗号アルゴリズムとして DES しかサポートしていません。うまく接続できないときは、クライアントの設定で使用する暗号アルゴリズムを確認してください。DES を使用するよう設定されていない場合は、設定を変更してください。

SSH セッションの状態は SHOW SSH SESSIONS コマンド (461 ページ) で確認できます。

```
SHOW SSH SESSIONS ↵
```

その他

CREATE ENCO KEY コマンド (「暗号・圧縮」の 18 ページ) で作成・登録した暗号鍵はセキュリティシステムの「鍵」となる重要な情報であるため、CREATE CONFIG コマンド (158 ページ) で作成する設定ファイルとは別に保存されます (鍵の管理は ENCO (暗号・圧縮) モジュールの役割です)。ただし、セキュリティモードでないと鍵情報が再起動によって削除されてしまうため、暗号鍵を使用する場合は Security Officer レベルのユーザーを作成して、セキュリティモードに移行してください。

SSH サーバーにログインするには、ADD SSH USER コマンド (147 ページ) で SSH 用のユーザーを登録しておかなくてはなりません。SSH サーバーが有効になっていても、SSH ユーザーが登録されていないと、いかなるユーザーもログインできません。SHOW SSH USER コマンド (462 ページ) を実行してもユーザーが表示されないときは、SSH ユーザーが登録されていません。「SSH ユーザーの登録」を参考にして、SSH ユーザーを登録してください。

SSH ユーザーが 5 回連続してログインに失敗すると、該当ユーザーは自動的に無効状態 (ログインできない状態) になります。無効状態のユーザーを再度有効にするには、サーバー上で ENABLE SSH USER コマンド (262 ページ) を実行する必要があります。

```
ENABLE SSH USER=carelessuser ↵
```

SSH ユーザーの有効・無効は SHOW SSH USER コマンド (462 ページ) で確認できます。

```
SHOW SSH USER ↵
SHOW SSH USER=carelessuser ↵
```

SSH サーバーへの接続許可を特定の SSH クライアント (IP アドレス) だけに制限することもできます。これには、ADD SSH USER コマンド (147 ページ)、SET SSH USER コマンド (334 ページ) の IPADDRESS、MASK パラメーターを使います。クライアント制限は SSH ユーザーごとに設定します。たとえば、ユーザー pote に対し、IP アドレス 192.168.10.100 のホストからのみ接続を許可するよう設定するには、次のようにします。

```
ADD SSH USER=pote PASSWORD=passpote IPADDRESS=192.168.10.100 ↵
```

また、接続できるクライアントをサブネット 192.168.10.0/24 内に制限するには、次のようにします。

```
ADD SSH USER=pote PASSWORD=passpote IPADDRESS=192.168.10.0
MASK=255.255.255.0 ↵
```

本製品から他の SSH サーバーに接続するには、SSH コマンド (484 ページ) を使います。パスワード認証の場合は、次のようにします。

```
SSH 192.168.10.5 USER=pote PASSWORD=passpote ↵
```

RSA 認証の場合は、CREATE ENCO KEY コマンド (「暗号・圧縮」の 18 ページ) で自分の鍵を作成・登録した上で、次のように鍵番号を指定します。

```
SSH 192.168.10.5 USER=pote KEYID=10 ↵
```

ログインせずにサーバー上で単独のコマンドだけを実行させたい場合は、次のようにします。ただし、遠隔コマンド実行には Manager レベル以上の権限が必要ですのでご注意ください。SSH ユーザーに Manager レベル以上の権限を与える方法については、「SSH ユーザーの登録」をご覧ください。

```
SSH 192.168.10.5 USER=pote PASSWORD=passpote COMMAND="show firewall
event=deny" ↵
```

SSH 使用時には、以下の SSH 関連イベントがログに記録されます。

- SSH ユーザーの追加、削除、設定変更
- SSH サーバーの有効化、無効化
- SSH コネクションの開始、終了、拒否

コマンドリファレンス編

機能別コマンド索引

システム

| | |
|--|-----|
| DISABLE HTTP SERVER | 213 |
| EDIT | 240 |
| ENABLE HTTP SERVER | 243 |
| HELP | 269 |
| LOGIN | 273 |
| LOGOFF | 274 |
| RESTART | 293 |
| SET HELP | 296 |
| SET SYSTEM CONTACT | 335 |
| SET SYSTEM DISTINGUISHEDNAME | 336 |
| SET SYSTEM LOCATION | 337 |
| SET SYSTEM NAME | 338 |
| SET SYSTEM TERRITORY | 339 |
| SET TIME | 341 |
| SHOW BUFFER | 362 |
| SHOW CPU | 365 |
| SHOW DEBUG | 366 |
| SHOW EXCEPTION | 367 |
| SHOW HTTP SERVER | 382 |
| SHOW STARTUP | 464 |
| SHOW SYSTEM | 465 |
| SHOW TIME | 469 |

記憶装置とファイルシステム

| | |
|-------------------------------------|-----|
| ACTIVATE FLASH COMPACTION | 117 |
| ADD FILE | 123 |
| CLEAR FLASH TOTALLY | 155 |
| CLEAR NVS TOTALLY | 156 |
| COPY | 157 |
| CREATE FFILE | 159 |
| CREATE FILE | 161 |
| DELETE FFILE | 188 |
| DELETE FILE | 189 |
| DELETE NVS | 195 |
| DUMP | 236 |
| DUMP NVS | 238 |

| | |
|---|-----|
| MODIFY | 277 |
| MODIFY NVS | 278 |
| RENAME | 286 |
| RESET FILE PERMANENTREDIRECT | 287 |
| SHOW FFILE | 372 |
| SHOW FILE | 374 |
| SHOW FILE PERMANENTREDIRECT | 376 |
| SHOW FLASH | 378 |
| SHOW FLASH PHYSICAL | 380 |
| SHOW NVS | 409 |
| SHOW NVS FREE | 411 |
| コンフィグレーション | |
| CREATE CONFIG | 158 |
| SET CONFIG | 295 |
| SHOW CONFIG | 363 |
| コマンドプロセッサ | |
| ADD ALIAS | 122 |
| DELETE ALIAS | 187 |
| SHOW ALIAS | 361 |
| ユーザー認証データベース | |
| ADD USER | 151 |
| DELETE USER | 206 |
| DISABLE USER | 233 |
| ENABLE USER | 266 |
| PURGE USER | 284 |
| RESET USER | 292 |
| SET PASSWORD | 312 |
| SET USER | 359 |
| SHOW USER | 478 |
| 認証サーバー | |
| ADD RADIUS SERVER | 131 |
| DELETE RADIUS SERVER | 196 |
| SET RADIUS | 322 |
| SHOW RADIUS | 431 |
| ポート認証 | |
| ACTIVATE PORTAUTH PORT REAUTHENTICATE | 118 |
| DISABLE PORTAUTH | 220 |
| DISABLE PORTAUTH DEBUG | 221 |
| DISABLE PORTAUTH PORT | 222 |
| ENABLE PORTAUTH | 250 |

| | |
|--|-----|
| ENABLE PORTAUTH DEBUG | 251 |
| ENABLE PORTAUTH PORT | 252 |
| PURGE PORTAUTH PORT | 281 |
| RESET PORTAUTH PORT | 290 |
| RESET PORTAUTH PORT MULTIMIB | 291 |
| SET PORTAUTH PORT | 313 |
| SET PORTAUTH PORT SUPPLICANTMAC | 317 |
| SET PORTAUTH USERNAME | 320 |
| SHOW PORTAUTH | 413 |
| SHOW PORTAUTH COUNTER | 416 |
| SHOW PORTAUTH PORT | 419 |
| SHOW PORTAUTH PORT MULTISUPPLICANT | 424 |
| SHOW PORTAUTH TIMER | 428 |
| アップロード・ダウンロード | |
| LOAD | 271 |
| RESET LOADER | 288 |
| SET LOADER | 298 |
| SHOW LOADER | 386 |
| UPLOAD | 489 |
| ソフトウェア | |
| DELETE INSTALL | 190 |
| DESTROY PATCH | 209 |
| DISABLE FEATURE | 212 |
| DISABLE RELEASE | 223 |
| ENABLE FEATURE | 242 |
| ENABLE RELEASE | 256 |
| SET INSTALL | 297 |
| SHOW FEATURE | 369 |
| SHOW INSTALL | 384 |
| SHOW PATCH | 412 |
| SHOW RELEASE | 433 |
| メール送信 | |
| DELETE MAIL | 193 |
| DISABLE MAIL DEBUG | 218 |
| ENABLE MAIL DEBUG | 248 |
| MAIL | 275 |
| SET MAIL | 308 |
| SHOW MAIL | 404 |
| セキュリティー | |
| ADD USER RSO | 153 |

| | |
|--|-----|
| DELETE USER RSO | 207 |
| DISABLE SYSTEM SECURITY_MODE | 230 |
| DISABLE USER RSO | 234 |
| ENABLE SYSTEM SECURITY_MODE | 263 |
| ENABLE USER RSO | 267 |
| SET MANAGER ASYN | 309 |
| SHOW MANAGER ASYN | 406 |
| SHOW USER RSO | 482 |

ログ

| | |
|----------------------------------|-----|
| ADD LOG OUTPUT | 126 |
| ADD LOG RECEIVE | 128 |
| CREATE LOG OUTPUT | 164 |
| DELETE LOG OUTPUT | 191 |
| DELETE LOG RECEIVE | 192 |
| DESTROY LOG OUTPUT | 208 |
| DISABLE LOG | 214 |
| DISABLE LOG GENERATION | 215 |
| DISABLE LOG OUTPUT | 216 |
| DISABLE LOG RECEPTION | 217 |
| ENABLE LOG | 244 |
| ENABLE LOG GENERATION | 245 |
| ENABLE LOG OUTPUT | 246 |
| ENABLE LOG RECEPTION | 247 |
| FLUSH LOG OUTPUT | 268 |
| PURGE LOG | 279 |
| SET LOG OUTPUT | 300 |
| SET LOG OUTPUT FILTER | 303 |
| SET LOG RECEIVE | 305 |
| SET LOG UTCOFFSET | 306 |
| SHOW LOG | 388 |
| SHOW LOG COUNTER | 392 |
| SHOW LOG OUTPUT | 395 |
| SHOW LOG QUEUE | 398 |
| SHOW LOG RECEIVE | 400 |
| SHOW LOG STATUS | 402 |

スクリプト

| | |
|------------------------------|-----|
| ACTIVATE SCRIPT | 120 |
| ADD SCRIPT | 133 |
| DEACTIVATE SCRIPT | 186 |
| DELETE SCRIPT | 197 |
| IF THEN ELSE ENDIF | 270 |

| | |
|-----------------------|-----|
| SET SCRIPT | 323 |
| SHOW SCRIPT | 434 |
| WAIT | 491 |

トリガー

| | |
|------------------------------------|-----|
| ACTIVATE TRIGGER | 121 |
| ADD TRIGGER | 149 |
| CREATE TRIGGER CPU | 169 |
| CREATE TRIGGER FIREWALL | 171 |
| CREATE TRIGGER INTERFACE | 173 |
| CREATE TRIGGER MEMORY | 175 |
| CREATE TRIGGER MODULE | 177 |
| CREATE TRIGGER PERIODIC | 180 |
| CREATE TRIGGER REBOOT | 182 |
| CREATE TRIGGER TIME | 184 |
| DELETE TRIGGER | 205 |
| DESTROY TRIGGER | 211 |
| DISABLE TRIGGER | 232 |
| ENABLE TRIGGER | 265 |
| PURGE TRIGGER | 283 |
| SET TRIGGER CPU | 342 |
| SET TRIGGER FIREWALL | 344 |
| SET TRIGGER INTERFACE | 346 |
| SET TRIGGER MEMORY | 348 |
| SET TRIGGER MODULE | 350 |
| SET TRIGGER PERIODIC | 352 |
| SET TRIGGER REBOOT | 354 |
| SET TRIGGER TIME | 356 |
| SHOW TRIGGER | 470 |

SNMP

| | |
|------------------------------------|-----|
| ADD SNMP COMMUNITY | 134 |
| ADD SNMP GROUP | 136 |
| ADD SNMP TARGETADDR | 138 |
| ADD SNMP TARGETPARAMS | 140 |
| ADD SNMP USER | 142 |
| ADD SNMP VIEW | 144 |
| CREATE SNMP COMMUNITY | 167 |
| DELETE SNMP COMMUNITY | 198 |
| DELETE SNMP GROUP | 199 |
| DELETE SNMP TARGETADDR | 200 |
| DELETE SNMP TARGETPARAMS | 201 |
| DELETE SNMP USER | 202 |

| | |
|--|-----|
| DELETE SNMP VIEW | 203 |
| DESTROY SNMP COMMUNITY | 210 |
| DISABLE SNMP | 224 |
| DISABLE SNMP AUTHENTICATE_TRAP | 225 |
| DISABLE SNMP COMMUNITY | 226 |
| DISABLE SNMP COMMUNITY TRAP | 227 |
| ENABLE SNMP | 257 |
| ENABLE SNMP AUTHENTICATE_TRAP | 258 |
| ENABLE SNMP COMMUNITY | 259 |
| ENABLE SNMP COMMUNITY TRAP | 260 |
| PURGE SNMP | 282 |
| SET SNMP ASNBERPADDING | 324 |
| SET SNMP COMMUNITY | 325 |
| SET SNMP ENGINEID | 326 |
| SET SNMP GROUP | 327 |
| SET SNMP LOCAL | 328 |
| SET SNMP TARGETADDR | 329 |
| SET SNMP TARGETPARAMS | 330 |
| SET SNMP TRAPDELAY | 331 |
| SET SNMP USER | 332 |
| SHOW SNMP | 437 |
| SHOW SNMP COMMUNITY | 441 |
| SHOW SNMP GROUP | 443 |
| SHOW SNMP TARGETADDR | 445 |
| SHOW SNMP TARGETPARAMS | 447 |
| SHOW SNMP USER | 449 |
| SHOW SNMP VIEW | 451 |

NTP

| | |
|-----------------------------|-----|
| ADD NTP PEER | 130 |
| DELETE NTP PEER | 194 |
| DISABLE NTP | 219 |
| ENABLE NTP | 249 |
| PURGE NTP | 280 |
| RESET NTP | 289 |
| SET NTP UTCOFFSET | 310 |
| SHOW NTP | 407 |

ターミナルサービス

| | |
|---------------------------------|-----|
| DISABLE TELNET SERVER | 231 |
| DISCONNECT | 235 |
| ENABLE TELNET SERVER | 264 |
| RECONNECT | 285 |

| | |
|-------------------------|-----|
| SET TELNET | 340 |
| SET TTY | 358 |
| SHOW SESSIONS | 436 |
| SHOW TELNET | 468 |
| SHOW TTY | 475 |
| TELNET | 486 |

Secure Shell

| | |
|------------------------------|-----|
| ADD SSH USER | 147 |
| DELETE SSH USER | 204 |
| DISABLE SSH SERVER | 228 |
| DISABLE SSH USER | 229 |
| ENABLE SSH SERVER | 261 |
| ENABLE SSH USER | 262 |
| SET SSH SERVER | 333 |
| SET SSH USER | 334 |
| SHOW SSH | 453 |
| SHOW SSH SESSIONS | 461 |
| SHOW SSH USER | 462 |
| SSH | 484 |

ACTIVATE FLASH COMPACTION

カテゴリー：運用・管理 / 記憶装置とファイルシステム

ACTIVATE FLASH COMPACTION

解説

フラッシュメモリーのコンパクション（メモリー上のゴミ削除）を実行する。

コンパクションが完了するまで（コンソールに「Flash compaction successfully completed.」と表示されるまで）、電源断や再起動、フラッシュメモリーに対する操作（ファイル作成、編集、リネーム、削除など）を行ってはならない。コンパクションは必要に応じて自動的に行われるので、通常このコマンドを使う必要はない。

入力・出力・画面例

```
Manager bulbul> activate flash compaction

Info (1031260): Flash compacting...
DO NOT restart the router, or power down until compaction is completed.

Manager bulbul>
Info (1031261): Flash compaction successfully completed.
```

備考・注意事項

ファイルダウンロード時にフラッシュメモリーの空き容量が足りないというメッセージが表示される場合は、本コマンドを実行してみるとよい。

コンパクション中は、絶対にシステム再起動や電源断、フラッシュメモリーに対する操作（ファイル作成、編集、リネーム、削除など）を行わないこと。

関連コマンド

SHOW FFILE (372 ページ)

SHOW FLASH (378 ページ)

ACTIVATE PORTAUTH PORT REAUTHENTICATE

カテゴリー：運用・管理 / ポート認証

ACTIVATE PORTAUTH [= {8021X|MACBASED}] **PORT**={*eth-port*|*port-list*|ALL}
REAUTHENTICATE [SUPPLICANTMAC=*macadd*]

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

macadd: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

解説

指定ポートに接続されている Supplicant を再認証する。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。
 省略時は 8021X と見なされる。

PORT ポート。実際には、指定したポートのうち、PORTAUTH で指定した認証方式を使用しているポートだけが対象となる。また、PORTAUTH に 8021X を指定した場合は、Authenticator として設定されているポート (TYPE=AUTHENTICATOR または TYPE=BOTH) でのみ、認証プロセスが再実行される。

SUPPLICANTMAC Supplicant の MAC アドレス。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。

例

ポート 4 に接続されている 802.1X Supplicant を再認証する。

```
ACTIVATE PORTAUTH PORT=4 REAUTHENTICATE
```

eth0 ポートに接続されている MAC ベース Supplicant を再認証する。

```
ACTIVATE PORTAUTH=MACBASED PORT=eth0 REAUTHENTICATE
```

関連コマンド

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

ACTIVATE SCRIPT

カテゴリー：運用・管理 / スクリプト

ACTIVATE SCRIPT=filename [OUTPUT={LOG}] [*parameters*]

filename: ファイル名（拡張子は.scp か.cfg）

parameters: スクリプトに対する引数（スペース区切りで 8 個まで。スクリプト中では変数%1～%8 で参照できる）

解説

指定したスクリプトを実行する。

パラメーター

SCRIPT スクリプトファイル名（拡張子は.scp または.cfg）。拡張子を省略した場合は.scp とみなされる。

OUTPUT スクリプトが出力する文字列の送り先。現時点では LOG（ログに出力）のみサポート。指定がない場合は TTY（端末画面）に出力される。

例

引数を 2 つとるスクリプト sendmail.scp を実行する。

```
ACTIVATE SCRIPT=sendmail.scp "someone@somewhere.xxx" "warning"
```

備考・注意事項

OUTPUT=LOG を指定しても、デフォルトでは SHOW LOG コマンドでスクリプトの実行結果を見ることができない。これは、スクリプト出力のログレベル（SEVERITY）が 2 であるのに対し、ログ機能のデフォルト設定ではログレベル 3 以上のメッセージしか記録しないようなフィルターが定義されているため。

引数の長さが 31 文字を超えた場合、スクリプト中では 31 文字に切り詰められる。

関連コマンド

ADD SCRIPT（133 ページ）

DEACTIVATE SCRIPT（186 ページ）

DELETE SCRIPT（197 ページ）

SET SCRIPT（323 ページ）

SHOW SCRIPT（434 ページ）

ACTIVATE TRIGGER

カテゴリー：運用・管理 / トリガー

ACTIVATE TRIGGER=trigger-id

trigger-id: トリガー番号 (1 ~ 250)

解説

指定したトリガーを手動で起動する。

本コマンドでは、DISABLE TRIGGER コマンドで無効状態にしたトリガーであっても起動できる。また、TEST=ON のトリガーの場合も、SCRIPT パラメーターで指定したスクリプトが実際に起動される（本来、TEST=ON のトリガーは、起動されたことがログに残るだけで、スクリプトは実行されない）。

ただし、本コマンドで起動した場合は、トリガーの実行回数を制御する REPEAT カウンターや最終実行時間の値は変更されない。

パラメーター

TRIGGER トリガー番号

例

トリガー「2」を起動する。

ACTIVATE TRIGGER=2

関連コマンド

CREATE TRIGGER CPU (169 ページ)
 CREATE TRIGGER FIREWALL (171 ページ)
 CREATE TRIGGER INTERFACE (173 ページ)
 CREATE TRIGGER MEMORY (175 ページ)
 CREATE TRIGGER MODULE (177 ページ)
 CREATE TRIGGER PERIODIC (180 ページ)
 CREATE TRIGGER REBOOT (182 ページ)
 CREATE TRIGGER TIME (184 ページ)
 DISABLE TRIGGER (232 ページ)
 ENABLE TRIGGER (265 ページ)
 SHOW TRIGGER (470 ページ)

ADD ALIAS

カテゴリー：運用・管理 / コマンドプロセッサ

ADD ALIAS=alias STRING=string

alias: エイリアス名 (1~132 文字。大文字小文字を区別しない。空白を含む場合はダブルクォートで囲む)

string: 文字列 (1~132 文字。空白を含む場合はダブルクォートで囲む)

解説

コマンドの別名 (エイリアス) を定義する。

コマンドラインからの入力行にエイリアスが含まれていた場合、コマンド解釈前にエイリアスが置換文字列に展開される。展開は一度だけ行われる (展開後の文字列にエイリアスが含まれていても展開されない)。

パラメーター

ALIAS エイリアス名

STRING 展開後の文字列を指定する

例

ファイル一覧を表示するエイリアス「ls」を定義する。

```
ADD ALIAS=ls STRING="show file"
```

関連コマンド

DELETE ALIAS (187 ページ)

SHOW ALIAS (361 ページ)

ADD FILE

カテゴリー：運用・管理 / 記憶装置とファイルシステム

ADD FILE=filename [COMMAND=string] [SCRIPT=filename] [PERMANENTREDIRECT]
[LIMIT=0..1048576]

filename: ファイル名

string: 文字列 (1~255 文字。空白を含む場合はダブルクォートで囲む)

解説

指定されたコマンド行やスクリプトを実行し、その出力を指定されたテキストファイルに追記 (リダイレクト) する。

パラメーター

FILE 出力先のテキストファイル名。指定したファイルが存在しない場合は作成される (この場合は CREATE FILE コマンドと同じ動作になる)

COMMAND 実行するコマンド行。通常は情報表示用の「SHOW XXXX」コマンドを指定する。空白を含む場合はダブルクォートで囲むこと。SCRIPT パラメーターと同時に指定することはできない

SCRIPT 実行するスクリプトファイル名。COMMAND パラメーターと同時に指定することはできない

PERMANENTREDIRECT 指定したコマンド行やスクリプトの出力を継続的にファイルへ追記したいときに指定する。このオプションは、COMMAND パラメーターにデバッグオプションを有効化する「ENABLE XXXX DEBUG」コマンドを指定した場合、あるいは、SCRIPT パラメーターに「ENABLE XXXX DEBUG」コマンドを含むスクリプトを指定した場合にのみ有効。本オプションを指定した場合、FILE パラメーターで指定したテキストファイルは書き込み用にオープンされたままの状態となり、他のコマンドによって表示、変更などの操作ができないようロックされる。該当ファイルへの出力を終了しファイルをクローズするには、RESET FILE PERMANENTREDIRECT コマンドを実行すること

LIMIT 出力先テキストファイルの上限サイズ (バイト)。省略時は 204800 バイト

入力・出力・画面例

```
Manager > show file=time.txt
File : time.txt
1:
2:
3: System time is 11:18:48 on Thursday 01-Nov-2007.

Manager > add file=time.txt command="show time"
Info (1056003): Operation successful.
```

```

Manager > show file=time.txt
File : time.txt
1:
2:
3: System time is 11:18:48 on Thursday 01-Nov-2007.
4:
5:
6: System time is 11:19:00 on Thursday 01-Nov-2007.

Manager > add file=time.txt command="enable ip debug=all" permanentredirect
Info (1056003): Operation successful.

Manager > reset file=time.txt permanentredirect
Info (1056278): time.txt redirection - operation complete.

Manager > show file=time.txt
File : time.txt
1:
2:
3: System time is 11:18:48 on Thursday 01-Nov-2007.
4:
5:
6: System time is 11:19:00 on Thursday 01-Nov-2007.
7:
8:
9: Info (1005287): All IP debugging has been enabled.
10: <I/C/B=vlan1/2/0, l=60, ttl=128, p=1, addr=192.168.20.11>192.168.20.1
11: >I/C/T/R/Id=Loc/0/fw/??/61533, l=60, ttl=64, p=1, addr=192.168.20.1>192.168.20.11
12: <I/C/B=vlan1/2/0, l=60, ttl=128, p=1, addr=192.168.20.11>192.168.20.1
13: >I/C/T/R/Id=Loc/0/fw/??/61534, l=60, ttl=64, p=1, addr=192.168.20.1>192.168.20.11
...

Manager > disable ip debug=all
Info (1087003): Operation successful.

```

例

既存ファイル iproute.txt にコマンド行「show ip route」の実行結果を追記する。ここで iproute.txt が存在しない場合は新規作成される。

```
ADD FILE=iproute.txt COMMAND="show ip route"
```

既存ファイル ipdebug.txt にデバッグコマンド「enable ip debug=all」の出力を継続的に追記する。追記出力を終了しファイルをクローズするには、RESET FILE PERMANENTREDIRECT コマンドを実行する。なお、ファイルをクローズしてもデバッグオプションは有効なままなので、この例では「disable ip debug=all」を実行してデバッグオプションも無効にすること。

```
ADD FILE=ipdebug.txt COMMAND="enable ip debug=all" PERMANENTREDIRECT
```

備考・注意事項

COMMAND パラメーターで指定したコマンド行や、SCRIPT パラメーターで指定したスクリプトは、本コマンドの入力と同時に実行される。

「SHOW XXXX」コマンドの出力をファイルに保存したいとき、PERMANENTREDIRECT オプションは意味を持たないので指定しないこと。同オプションを指定して「SHOW XXXX」コマンドを実行した場合は、本コマンド入力時に実行された「SHOW XXXX」コマンドの出力だけがファイルに書き込まれ、それ以降「SHOW XXXX」コマンドを実行してもそれらはファイルに追記されず、ただファイルだけがオープン（ロック）されたままとなるので注意。

「ENABLE XXXX DEBUG」コマンドによるデバッグ出力をファイルに保存したいときは、必ず PERMANENTREDIRECT オプションを指定すること。同オプションを指定せずに「ENABLE XXXX DEBUG」コマンドを実行した場合は、デバッグオプション有効化コマンドの実行に成功した、あるいは失敗したというメッセージだけがファイルに保存されるので注意。

「ENABLE XXXX DEBUG」コマンドを本コマンドから実行した場合、ファイルへの出力が完了しても、該当デバッグ出力はコンソールに表示されない。これは、PERMANENTREDIRECT オプションを指定したかどうかとは関係ない。デバッグ出力をコンソールに表示させたい場合は、再度「ENABLE XXXX DEBUG」コマンドを実行すること。なお、ファイルへの出力中に「ENABLE XXXX DEBUG」コマンドを再実行すると、ファイルへの出力が停止するので注意。

「ENABLE XXXX DEBUG」コマンドを本コマンドから実行した場合、ファイルへの出力が完了しても、該当デバッグオプションは有効なままとなる。これは、PERMANENTREDIRECT オプションを指定したかどうかとは関係ない。ファイルへの出力が完了し、デバッグ出力の収集が完了したら、「DISABLE XXXX DEBUG」コマンドを実行して、デバッグオプションを無効にすること。

関連コマンド

CREATE FILE (161 ページ)

RESET FILE PERMANENTREDIRECT (287 ページ)

SHOW FILE (374 ページ)

SHOW FILE PERMANENTREDIRECT (376 ページ)

ADD LOG OUTPUT

カテゴリー：運用・管理 / ログ

```
ADD LOG OUTPUT={TEMPORARY|PERMANENT|output-id} [FILTER=entry-id]
[ACTION={PROCESS|IGNORE}] [ALL] [DATE=[op]date] [DEVICE=[op]device]
[FILE=[op]filename] [MASK=ipadd] [MSGTEXT=[op]string]
[MODULE=[op]module-id] [ORIGIN=ipadd] [REFERENCE=[op]string]
[SEVERITY=[op]severity] [SOURCELINE=[op]line-num]
[SUBTYPE=[op]subtype-id] [TIME=[op]time] [TYPE=[op]type-id]
```

output-id: ログ出力 ID (1~20)

entry-id: エントリー番号 (1~)

op: 比較演算子 (「<」(小さい)「>」(大きい)「!」(等しくない)「」(等しい)「%」(以下の文字列を含む))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31) mmm は月 (英語月名の頭3文字。例: APR) yyyy は西暦年)

device: デバイス番号

filename: ファイル名 (1~12 文字)

ipadd: IP アドレスまたはネットマスク

string: 文字列

module-id: モジュール名またはモジュール番号 (0~255)

severity: ログレベル (0~7)

line-num: 行番号 (1~)

subtype-id: ログメッセージのサブタイプ名または ID

time: 時刻 (hh:mm:ss の形式。hh は時 (0~23) mm は分 (0~59) ss は秒 (0~59))

type-id: ログメッセージのタイプ名または ID

解説

ログ出力先にメッセージフィルターのエントリーを追加し、出力するログメッセージの条件を指定する。CREATE LOG OUTPUT コマンドで出力先を定義しただけでは、ログメッセージは出力されない。本コマンドで出力するメッセージの条件を指定する必要がある。

パラメーター

OUTPUT ログ出力先 ID。1~20 の任意の番号か、特殊なキーワード「TEMPORARY」(RAM) または「PERMANENT」(NVS) を指定する。

FILTER メッセージフィルターのエントリー番号。省略時は、エントリーリストの末尾に追加される。

ACTION フィルターアクション。このエントリーにマッチしたメッセージを処理 (PROCESS) するか、無視 (IGNORE) するかを指定。省略時は PROCESS。

ALL すべてのメッセージにマッチさせたいときに指定する。他の条件と同時に指定することはできない。

DATE メッセージの日付。省略時はすべての日付にマッチする。

DEVICE デバイス番号。省略時はすべてのデバイスにマッチする。

FILE 該当モジュールのソースプログラムファイル名 (例: logmain.c)。ソースファイル名は、SHOW LOG コマンドに FULL オプションを付けたときに表示される。省略時はすべてのファイル名にマッ

チする。

MASK ネットマスク。メッセージの生成元 IP アドレスを示す ORIGIN パラメーターと組み合わせて使用する。省略時は 255.255.255.255 (単一ホスト)。

MSGTEXT メッセージ本文と比較する文字列。省略時はすべてのメッセージにマッチする。スペースを含む文字列を指定する場合は、比較演算子も含めて文字列を「”(ダブルクォーテーション)で囲む。

MODULE モジュール番号またはモジュール名。省略時はすべてのモジュールにマッチする。

ORIGIN ログ生成元の IP アドレス。MASK パラメーターと組み合わせて範囲指定が可能。デフォルトではすべての IP アドレスにマッチする。

REFERENCE メッセージ中の参考情報。省略時はすべてにマッチする。

SEVERITY メッセージのログレベル。省略時はすべてのログレベルにマッチする。

SOURCELINE メッセージを生成したソースプログラムファイルの行番号。省略時はすべての行にマッチする。

SUBTYPE メッセージのサブタイプ名またはサブタイプ番号。省略時はすべてのサブタイプにマッチする。

TIME メッセージの時刻。省略時はすべての時刻にマッチする。

TYPE メッセージのタイプ名またはサブタイプ番号。省略時はすべてのサブタイプにマッチする。

例

ファイアウォールのログだけを出力するフィルターエントリーを、ログ出力先定義「3」に追加する。

```
ADD LOG OUTPUT=3 MODULE=FIREWALL
```

ログレベル 6 以上のメッセージだけを出力するフィルターエントリーを、ログ出力先定義「4」に追加する。

```
ADD LOG OUTPUT=4 SEVERITY=>6
```

関連コマンド

CREATE LOG OUTPUT (164 ページ)

DELETE LOG OUTPUT (191 ページ)

SET LOG OUTPUT (300 ページ)

SHOW LOG OUTPUT (395 ページ)

ADD LOG RECEIVE

カテゴリー：運用・管理 / ログ

ADD LOG RECEIVE={*ipadd*|**ANY**} [MASK=*ipadd*] [ALLOW={YES|NO}] [PROTOCOL={ALL|BOTH|NEW|OLD|SYSLOG}] [PASSWORD={*password*|NONE}]

ipadd: IP アドレスまたはネットマスク

password: パスワード (1～16 文字。任意の印刷可能文字を使用可能。空白を含む場合はダブルクォートで囲む)

解説

ログ受信テーブルにエントリーを追加する。

ログ受信テーブルは、どの IP アドレスから、どのプロトコル、どのパスワードでログを受信するかを指定するもの。各エントリーは、ログ送信元の IP アドレス/マスクと、受信可否、プロトコル、パスワードで構成される。

ログ送信元の IP アドレスが複数のエントリーにマッチする場合は、もっともマスクの長い (対象アドレスがもっとも限定された) エントリーにしたがって処理される (エントリーの追加順序は意味をもたない)。

パラメーター

RECEIVE ログ送信元の IP アドレス。MASK と組み合わせて範囲を指定することも可能。ANY と 0.0.0.0 はすべての IP アドレスを示す。

MASK RECEIVE パラメーターで指定したアドレスに対するマスク。IP アドレスを範囲指定するときに使う。ただし、RECEIVE=ANY または RECEIVE=0.0.0.0 のときは指定できない。省略時は、RECEIVE で指定した IP アドレスがクラス A、B、C のネットワークアドレスなら各クラスの標準マスク、それ以外なら 255.255.255.255 (単一ホスト) となる。

ALLOW RECEIVE/MASK で指定した IP アドレスからのログを受け入れるかどうか。YES なら受け入れ、NO なら拒否する。省略時は YES。

PROTOCOL RECEIVE/MASK で指定した IP アドレスから、どのプロトコルでログを受け入れるかを指定する。OLD (Net Manage Message Protocol)、NEW (SRLP)、SYSLOG、BOTH (OLD と NEW)、ALL (OLD、NEW、SYSLOG のすべて) から選択する。省略時は BOTH。

PASSWORD SRLP プロトコルにおいて、ログ送信元を認証するためのパスワードを指定する。省略時はパスワード認証を行わない。本パラメーターは、SRLP 使用時のみ有効 (PROTOCOL=NEW または BOTH、ALL のとき)。

例

IP アドレス 192.168.1.1 の機器から転送されてきたログを SRLP で受信する。

```
ADD LOG RECEIVE=192.168.1.1 PROTOCOL=NEW
```


関連コマンド

DELETE LOG RECEIVE (192 ページ)

SET LOG RECEIVE (305 ページ)

SHOW LOG RECEIVE (400 ページ)

ADD NTP PEER

カテゴリー：運用・管理 / NTP

ADD NTP PEER=*ipadd*

ipadd: IP アドレス

解説

時刻同期をとる NTP サーバーの IP アドレスを設定する。NTP サーバーは 1 つしか設定できない。

パラメーター

PEER NTP サーバーの IP アドレス

例

NTP サーバー「192.168.10.5」を使って時刻を合わせる。タイムゾーンは日本 (JST +09:00)

ENABLE NTP

ADD NTP PEER=192.168.10.5

SET NTP UTCOFFSET=JST

RESET NTP

関連コマンド

DELETE NTP PEER (194 ページ)

ADD RADIUS SERVER

カテゴリー：運用・管理 / 認証サーバー

```
ADD RADIUS SERVER=ipadd SECRET=password [PORT=port] [ACCPORT=port]
[LOCAL={NONE|1..15}]
```

ipadd: IP アドレス

password: パスワード (1~63 文字。英数字とアンダースコア、スペースを使用可能。大文字小文字を区別する。空白を含む場合はダブルクォートで囲む)

port: UDP ポート番号 (0~65535)

解説

認証サーバーリストに RADIUS (Remote Authentication Dial In User Server) サーバーを追加する。RADIUS サーバーは、ユーザー認証に使用できるほか、ファイアウォールのアクセスルールを集中管理する目的で使用することもできる。

パラメーター

SERVER RADIUS サーバーの IP アドレス。

SECRET RADIUS サーバーとの通信に使う共有パスワード。

PORT RADIUS サーバーの認証用 UDP ポート番号。0 を指定した場合は、RADIUS サーバーのアカウントティング機能だけを利用し、認証機能は使わない。省略時はデフォルトの 1645 番を使う。

ACCPORT RADIUS サーバーのアカウントティング用 UDP ポート番号。0 を指定した場合は、RADIUS サーバーの認証機能だけを利用し、アカウントティング機能は使わない。省略時はデフォルトの 1646 番を使う。

LOCAL 本 RADIUS サーバーとの通信に使用するローカル IP インターフェースの番号。ローカル IP インターフェースを指定した場合、本 RADIUS サーバー宛て要求パケットの始点 IP アドレスとして、指定したローカル IP インターフェースの IP アドレスが使用される。また、NAS-IP-Address 属性の値にも、ローカル IP インターフェースの IP アドレスが使用される。省略時は NONE (ローカル IP インターフェースを使用しない。この場合、要求パケットの始点 IP アドレスはシステムが決める)。

例

認証サーバーリストに RADIUS サーバー 192.168.10.5 を追加する。パスワードは「pOR8Gd」

```
ADD RADIUS SERVER=192.168.10.5 SECRET=pOR8Gd
```

RADIUS サーバーのアカウントティング機能だけを使用する

```
ADD RADIUS SERVER=192.168.10.5 SECRET=pOR8Gd PORT=0
```

備考・注意事項

RFC2865、RFC2866 ではポート番号 1812、1813 を RADIUS に割り当てている。これらのポートを使うサーバーを利用するには、PORT、ACCPORT パラメーターを指定すること。

関連コマンド

ADD IP LOCAL (「IP」の 188 ページ)

DELETE RADIUS SERVER (196 ページ)

SET RADIUS (322 ページ)

SHOW IP INTERFACE (「IP」の 478 ページ)

SHOW RADIUS (431 ページ)

ADD SCRIPT

カテゴリー：運用・管理 / スクリプト

ADD SCRIPT=filename TEXT=string [LINE=line-num]

filename: ファイル名（拡張子は.scp か.cfg）

string: 文字列（1～127 文字）

line-num: 行番号（1～）

解説

スクリプトファイルにテキスト一行分を追加する。

パラメーター

SCRIPT スクリプトファイル名。拡張子は.cfg か.scp。拡張子を省略した場合は.scp とみなされる。

TEXT 追加するテキスト

LINE テキストを挿入する箇所の行番号。省略時はファイルの末尾に追加される。

例

スクリプトファイル「handmade.scp」にテキストを追加する。

```
ADD SCRIPT=handmade.scp TEXT="show file"
```

備考・注意事項

特に理由がない限り、スクリプトの作成・編集には EDIT コマンド（内蔵スクリーンエディター）を使うか、PC/WS 上の使い慣れたエディターで編集して TFTP 等で転送するほうが便利。

本コマンドは、ログインした状態でコマンドラインから実行することを想定している。設定スクリプトファイル（.CFG）記述した場合は意図した結果にならないことがあるので注意。

関連コマンド

ACTIVATE SCRIPT（120 ページ）

DEACTIVATE SCRIPT（186 ページ）

DELETE SCRIPT（197 ページ）

SET SCRIPT（323 ページ）

SHOW SCRIPT（434 ページ）

WAIT（491 ページ）

ADD SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

```
ADD SNMP COMMUNITY=community [MANAGER=ipadd[/masklen]] [TRAPHOST=ipadd]  
[V1TRAPHOST=ipadd] [V2CTRAPHOST=ipadd]
```

community: SNMP コミュニティー名 (1～15 文字。大文字小文字を区別する)

ipadd: IP アドレス

masklen: マスク長 (0～32)

解説

(SNMPv1/v2c) SNMP コミュニティーに管理ステーション、トラップホストを追加する。

パラメーター

COMMUNITY SNMP コミュニティー名

MANAGER SNMP オペレーションを許可する管理ステーション。マスク長を付加することで範囲指定も可能。本エージェントは、MANAGER に登録されていないホストからの SNMP 要求には応答しない。ただし、SNMP コミュニティーの OPEN パラメーターが YES の場合は、MANAGER パラメーターの設定にかかわらず、すべての SNMP 要求に応答する。

TRAPHOST SNMPv1 トラップの送信先ホスト。ここで指定したホストには SNMPv1 形式のトラップが送信される。

V1TRAPHOST SNMPv1 トラップの送信先ホスト。TRAPHOST パラメーターと同じ。

V2CTRAPHOST SNMPv2c トラップの送信先ホスト。ここで指定したホストには SNMPv2c 形式のトラップが送信される。

例

SNMP コミュニティー「public」に管理ステーションを追加する。

```
ADD SNMP COMMUNITY=public MANAGER=192.168.20.5
```

備考・注意事項

SNMP トラップは、ENABLE SNMP COMMUNITY TRAP コマンドを実行してコミュニティのトラップ設定を有効にしないと送信されないので注意が必要。

TRAPHOST (または V1TRAPHOST) と V2CTRAPHOST に同じホストを指定してもよい

関連コマンド

CREATE SNMP COMMUNITY (167 ページ)
DELETE SNMP COMMUNITY (198 ページ)
DESTROY SNMP COMMUNITY (210 ページ)
DISABLE SNMP COMMUNITY (226 ページ)
DISABLE SNMP COMMUNITY TRAP (227 ページ)
ENABLE SNMP COMMUNITY (259 ページ)
ENABLE SNMP COMMUNITY TRAP (260 ページ)
SET SNMP COMMUNITY (325 ページ)
SHOW SNMP COMMUNITY (441 ページ)

ADD SNMP GROUP

カテゴリー：運用・管理 / SNMP

```
ADD SNMP GROUP=group SECURITYLEVEL={noAuthNoPriv|authNoPriv|authPriv}  
[READVIEW=view] [WRITEVIEW=view] [NOTIFYVIEW=view]
```

group: SNMP グループ名 (1～32 文字。大文字小文字を区別する)

view: SNMP ビュー名 (1～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ユーザーグループを定義する。

グループ名とセキュリティレベルの組み合わせは一意でなくてはならない。

パラメーター

GROUP SNMP グループ名

SECURITYLEVEL 本グループ所属のユーザーに求められる最低限のセキュリティレベルを指定する。

noAuthNoPriv (認証なし・暗号化なし) authNoPriv (認証あり・暗号化なし) authPriv (認証あり・暗号化あり) から選択する。

READVIEW 本グループ所属のユーザーが読み出せる MIB オブジェクトの範囲 (ビュー) を指定する。

ビューは ADD SNMP VIEW コマンドで定義する。READVIEW の指定がない場合、本グループ所属のユーザーはいかなる MIB オブジェクトも読み出せない。

WRITEVIEW 本グループ所属のユーザーが書き込める MIB オブジェクトの範囲 (ビュー) を指定する。

ビューは ADD SNMP VIEW コマンドで定義する。WRITEVIEW の指定がない場合、本グループ所属のユーザーはいかなる MIB オブジェクトにも書き込めない。

NOTIFYVIEW 本グループ所属のユーザーが受け取れる通知 MIB オブジェクトの範囲 (ビュー) を指定

する。ビューは ADD SNMP VIEW コマンドで定義する。NOTIFYVIEW の指定がない場合、本グループ所属のユーザーはいかなる通知 MIB オブジェクトも受け取れない。

例

SNMP グループ「admins」を定義する。セキュリティレベルは authPriv (認証あり・暗号化あり)。読み出し、書き込み、通知受信のすべてにおいて、internet ノード (1.3.6.1) 以下のすべてのオブジェクトにアクセスできるよう設定する。

```
ADD SNMP VIEW=most MIB=internet TYPE=INCLUDE
```

```
ADD SNMP GROUP=admins SECURITYLEVEL=authPriv READVIEW=most WRITEVIEW=most  
NOTIFYVIEW=most
```


SNMP グループ「mib2operators」を定義する。セキュリティーレベルは authNoPriv（認証あり・暗号化なし）。mib-2 ノード（1.3.6.1.2.1）以下の読み出しだけを許可する。

```
ADD SNMP VIEW=standard MIB=mib-2 TYPE=INCLUDE
```

```
ADD SNMP GROUP=mib2operators SECURITYLEVEL=authNoPriv READVIEW=standard
```

関連コマンド

ADD SNMP USER（142 ページ）

ADD SNMP VIEW（144 ページ）

DELETE SNMP GROUP（199 ページ）

SET SNMP GROUP（327 ページ）

SHOW SNMP（437 ページ）

SHOW SNMP GROUP（443 ページ）

SHOW SNMP USER（449 ページ）

SHOW SNMP VIEW（451 ページ）

ADD SNMP TARGETADDR

カテゴリー：運用・管理 / SNMP

ADD SNMP TARGETADDR=target PARAMS=params IP=ipadd [UDP=port]

target: SNMP ターゲット名 (1~32 文字。大文字小文字を区別する)

params: SNMP ターゲットパラメーターセット名 (1~32 文字。大文字小文字を区別する)

ipadd: IP アドレス

port: UDP ポート番号 (1~255)

解説

(SNMPv3) ターゲット (通知メッセージの送信先) を追加する。

パラメーター

TARGETADDR SNMP ターゲット名

PARAMS SNMP ターゲットパラメーターセット名。ADD SNMP TARGETPARAMS コマンドで定義したパラメーターセットの名前を指定する。

IP ターゲットの IP アドレス

UDP ターゲットのリスニング UDP ポート。1~255 の範囲で指定する。省略時は 162

例

SNMP ターゲット「tpR30」を追加する。ターゲットホストの IP アドレスは 172.28.28.156、UDP ポートはデフォルト 162 を使うものとする。ターゲットパラメーターセット「pzein」で定義したセキュリティレベルは authNoPriv (認証あり・暗号化なし) ユーザー名は zein。

```
ADD SNMP TARGETPARAMS=pzein SECURITYLEVEL=authNoPriv USER=zein
```

```
ADD SNMP TARGETADDR=tpR30 PARAMS=pzein IP=172.28.28.156
```

備考・注意事項

ターゲットにどの通知メッセージが送信されるかは、ユーザーが所属しているグループの NOTIFYVIEW パラメーター (ADD SNMP GROUP コマンド) で決まる。ユーザー名はパラメーターセット (ADD SNMP TARGETPARAMS コマンド) で指定する。また、ユーザーの所属グループは、ADD SNMP USER コマンドの GROUP パラメーターで指定する。

関連コマンド

ADD SNMP GROUP (136 ページ)

ADD SNMP TARGETPARAMS (140 ページ)
ADD SNMP USER (142 ページ)
ADD SNMP VIEW (144 ページ)
DELETE SNMP TARGETADDR (200 ページ)
SHOW SNMP (437 ページ)
SHOW SNMP GROUP (443 ページ)
SHOW SNMP TARGETADDR (445 ページ)
SHOW SNMP TARGETPARAMS (447 ページ)
SHOW SNMP USER (449 ページ)
SHOW SNMP VIEW (451 ページ)

ADD SNMP TARGETPARAMS

カテゴリー：運用・管理 / SNMP

ADD SNMP TARGETPARAMS=*params* **SECURITYLEVEL=**{noAuthNoPriv|authNoPriv|authPriv} **USER=***username*

params: SNMP ターゲットパラメーターセット名 (1～32 文字。大文字小文字を区別する)

username: SNMP ユーザー名 (1～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ターゲット (通知メッセージの送信先) との通信に使用するパラメーターセット (セキュリティレベルとユーザー名) を定義する。

パラメーター

TARGETPARAMS SNMP ターゲットパラメーターセット名

SECURITYLEVEL 本ターゲットパラメーターセットにおいて求められるセキュリティレベルを指定する。noAuthNoPriv (認証なし・暗号化なし) authNoPriv (認証あり・暗号化なし) authPriv (認証あり・暗号化あり) から選択する。USER パラメーターで指定したユーザーのセキュリティレベルと同じレベルを指定すること。

USER SNMP ユーザー名。ADD SNMP USER コマンドで定義したユーザー名を指定する。

例

SNMP ターゲットパラメーターセット「pzein」を定義する。セキュリティレベルは authNoPriv (認証あり・暗号化なし) ユーザー名は zein とする。

```
ADD SNMP TARGETPARAMS=pzein SECURITYLEVEL=authNoPriv USER=zein
```

関連コマンド

ADD SNMP GROUP (136 ページ)

ADD SNMP TARGETADDR (138 ページ)

ADD SNMP USER (142 ページ)

ADD SNMP VIEW (144 ページ)

DELETE SNMP TARGETPARAMS (201 ページ)

SHOW SNMP (437 ページ)

SHOW SNMP GROUP (443 ページ)

SHOW SNMP TARGETADDR (445 ページ)

SHOW SNMP TARGETPARAMS (447 ページ)

SHOW SNMP USER (449 ページ)

SHOW SNMP VIEW (451 ページ)

ADD SNMP USER

カテゴリー：運用・管理 / SNMP

```
ADD SNMP USER=username [GROUP=group] [AUTHPROTOCOL={NONE|MD5|SHA}]
[AUTHPASSWORD=password] [PRIVPROTOCOL={NONE|DES}]
[PRIVPASSWORD=password]
```

username: SNMP ユーザー名 (1～32 文字。大文字小文字を区別する)

group: SNMP グループ名 (1～32 文字。大文字小文字を区別する)

password: パスワード (8～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ユーザーを追加する。

パラメーター

USER SNMP ユーザー名

GROUP SNMP グループ名。ADD SNMP GROUP コマンドで定義したグループ名を指定する。

AUTHPROTOCOL 認証プロトコル。MD5、SHA、NONE(認証なし)から選択する。省略時は NONE。

AUTHPASSWORD 認証パスワード。AUTHPROTOCOL に MD5 か SHA を指定した場合の必須パラメーター。

PRIVPROTOCOL 暗号化プロトコル。DES、NONE(暗号化なし)から選択する。省略時は NONE。

AUTHPROTOCOL に NONE を指定した場合は、PRIVPROTOCOL にも NONE を指定しなくてはならない(「認証なし・暗号化あり」の組み合わせは認められていないため)。

PRIVPASSWORD 暗号化パスワード。PRIVPROTOCOL に DES を指定した場合の必須パラメーター。

例

SNMP ユーザー「supervisor」を定義する。所属グループ「admins」のセキュリティーレベルが authPriv (認証あり・暗号化あり) なので、認証用のプロトコルとパスワード、暗号化用のプロトコルとパスワードのすべてを指定している。

```
ADD SNMP USER=supervisor GROUP=admins AUTHPROTOCOL=MD5
AUTHPASSWORD=cugacuga PRIVPROTOCOL=DES PRIVPASSWORD=mugomugo
```

SNMP ユーザー「zein」を定義する。所属グループ「mib2operators」のセキュリティーレベルは authNoPriv (認証あり・暗号化なし) なので、認証用のプロトコルとパスワードのみ指定している。

```
ADD SNMP USER=zein GROUP=mib2operators AUTHPROTOCOL=SHA  
AUTHPASSWORD=jogejoge
```

関連コマンド

ADD SNMP GROUP (136 ページ)
ADD SNMP TARGETPARAMS (140 ページ)
DELETE SNMP USER (202 ページ)
SET SNMP USER (332 ページ)
SHOW SNMP GROUP (443 ページ)
SHOW SNMP USER (449 ページ)

ADD SNMP VIEW

カテゴリー：運用・管理 / SNMP

ADD SNMP VIEW=view OID=node-oid [TYPE={INCLUDE|EXCLUDE}]

ADD SNMP VIEW=view MIB=node-name [TYPE={INCLUDE|EXCLUDE}]

view: SNMP ビュー名 (1～32 文字。大文字小文字を区別する)

node-oid: MIB ノード OID (1.3.6.1 のように整数とピリオドで構成された文字列。数字は 32 個まで使用できる)

node-name: MIB ノード名 (既定のノード名。別表を参照)

解説

(SNMPv3) ビューにエントリーを追加する。

ビューは、複数のエントリーで構成されるリスト。各エントリーは、MIB ノードの OID と該当ノードをビューに含めるかどうかの指定 (INCLUDE、EXCLUDE) からなる。

ある OID がビューに含まれるかどうかは、その OID がマッチする最も長いエントリーの指定 (INCLUDE、EXCLUDE) によって決まる (最長一致)。したがって、エントリーの追加順序は意味を持たない。

なお、最長一致検索を実現するため、リストは OID の辞書順にソートされている (SHOW SNMP VIEW コマンドで確認できる)。そのため、リストを先頭から検索した場合に、最後にマッチしたエントリーが採用されると考えてもよい (ラストマッチ)。

パラメーター

VIEW SNMP ビュー名

OID MIB ノードの OID (Object Identifier)。MIB パラメーターとは同時に指定できない。

MIB MIB ノードの名前。指定できる名前と対応する OID は別表を参照。OID パラメーターとは同時に指定できない。なお、名前で指定した場合であっても、設定をファイルに保存するときは OID に変換される。

TYPE 指定した MIB ノードをビューに含めるかどうか。INCLUDE (含める)、EXCLUDE (含めない) から選択する。省略時は INCLUDE。

| ノード名 | OID |
|------------|---------------|
| internet | 1.3.6.1 |
| mib-2 | 1.3.6.1.2.1 |
| system | 1.3.6.1.2.1.1 |
| interfaces | 1.3.6.1.2.1.2 |
| at | 1.3.6.1.2.1.3 |
| ip | 1.3.6.1.2.1.4 |
| icmp | 1.3.6.1.2.1.5 |

| | |
|---------------|-----------------|
| tcp | 1.3.6.1.2.1.6 |
| udp | 1.3.6.1.2.1.7 |
| egp | 1.3.6.1.2.1.8 |
| transmission | 1.3.6.1.2.1.10 |
| snmp | 1.3.6.1.2.1.11 |
| bgp | 1.3.6.1.2.1.15 |
| rmon | 1.3.6.1.2.1.16 |
| bridge | 1.3.6.1.2.1.17 |
| host | 1.3.6.1.2.1.25 |
| mau | 1.3.6.1.2.1.26 |
| if | 1.3.6.1.2.1.31 |
| private | 1.3.6.1.4 |
| alliedTelesyn | 1.3.6.1.4.1.207 |
| snmpV2 | 1.3.6.1.6 |
| snmpModules | 1.3.6.1.6.3 |
| snmpFramework | 1.3.6.1.6.3.10 |
| snmpMPD | 1.3.6.1.6.3.11 |
| snmpTarget | 1.3.6.1.6.3.12 |
| snmpUsm | 1.3.6.1.6.3.15 |
| snmpVacm | 1.3.6.1.6.3.16 |

表 31: 既定の MIB ノード名

例

internet ノード (1.3.6.1) 以下の全オブジェクトを含む SNMP ビュー「most」を定義する。

```
ADD SNMP VIEW=most MIB=internet TYPE=INCLUDE
```

mib-2 ノード (1.3.6.1.2.1) 以下の全オブジェクトを含む SNMP ビュー「standard」を定義する。

```
ADD SNMP VIEW=standard MIB=mib-2 TYPE=INCLUDE
```

原則として mib-2 ノード (1.3.6.1.2.1) 以下の全オブジェクトを含むが、tcp ノード (1.3.6.1.2.1.6) と udp ノード (1.3.6.1.2.1.7) 以下は含まない SNMP ビュー「mib2notcpudp」を定義する。マッチングは OID の最長一致で行われるため、エントリーの追加順序は意味を持たない。したがって、以下の 3 コマンドは異なる順序で入力しても同じ動作となる。

```
ADD SNMP VIEW=mib2notcpudp MIB=mib-2 TYPE=INCLUDE
```

```
ADD SNMP VIEW=mib2notcpudp MIB=tcp TYPE=EXCLUDE
```

```
ADD SNMP VIEW=mib2notcpudp MIB=udp TYPE=EXCLUDE
```

関連コマンド

ADD SNMP GROUP (136 ページ)

DELETE SNMP VIEW (203 ページ)

SHOW SNMP GROUP (443 ページ)

SHOW SNMP VIEW (451 ページ)

ADD SSH USER

カテゴリー：運用・管理 / Secure Shell

```
ADD SSH USER=username {PASSWORD=password|KEYID=key-id} [IPADDRESS=ipadd]  
[MASK=ipadd]
```

username: ユーザー名 (1～15 文字)

password: パスワード (1～31 文字)

key-id: 鍵番号 (0～65535)

ipadd: IP アドレスまたはネットマスク

解説

SSH ユーザーを追加する。

このとき、該当ユーザーの認証方式をパスワード認証と RSA 認証から選択する。

ルーターに対する SSH アクセスは、このコマンドで登録したユーザーに限られる。SSH ユーザーが登録されていない場合、ルーターに対する SSH 接続はすべて拒否される。

ユーザー認証データベースに登録されているものと同じログイン名を指定した場合、SSH ユーザーにはデータベースと同じユーザー権限が適用される。一方、認証データベースに登録されていない SSH ユーザーの権限は USER レベルとなる。

パラメーター

USER SSH ユーザー名。

PASSWORD SSH パスワード。パスワード認証を使用するときに指定する。ユーザー認証データベースのパスワードと同じでなくてもよい。KEYID と同時に指定することはできない。

KEYID ユーザーの RSA 公開鍵番号 (CREATE ENCO KEY でインポートしたもの)。RSA 認証を使用するときに指定する。PASSWORD と同時に指定することはできない。

IPADDRESS ログイン元 (SSH クライアント) の IP アドレス。MASK と組み合わせて、ログイン元を制限するときに使う。デフォルトでは制限なし。

MASK ネットマスク。IPADDRESS パラメーターと組み合わせて、ログイン元ホストを制限するときに使う。

例

Manager 権限を持つユーザー「admin」を SSH ユーザーとして登録する (RSA 認証)。ユーザーの RSA 公開鍵は、ENCO モジュールの鍵番号「10」として登録されている。

```
ADD USER=admin PASSWORD=jogefoge PRIVILEGE=MANAGER
```

```
ADD SSH USER=admin KEYID=10
```

ユーザー「sshuser」を登録する。認証方式はパスワード認証。

```
ADD SSH USER=sshuser PASSWORD=sshpasswd
```

関連コマンド

CREATE ENCO KEY (「暗号・圧縮」の 18 ページ)

DELETE SSH USER (204 ページ)

SET SSH USER (334 ページ)

SHOW SSH USER (462 ページ)

ADD TRIGGER

カテゴリー：運用・管理 / トリガー

ADD TRIGGER=trigger-id SCRIPT=filename... [NUMBER=index]

trigger-id: トリガー番号 (1~250)

filename: ファイル名 (拡張子は.scip か.cfg)

index: スクリプト番号 (1~5)

解説

トリガーにスクリプトを追加する。

パラメーター

TRIGGER トリガー番号

SCRIPT スクリプトファイル名 (.scip または.cfg)。SCRIPT パラメーターは、1 コマンドラインに複数個指定できる。スクリプトの実行は記述順。1 つのトリガーに関連付けられるスクリプトは最高 5 個。

NUMBER 追加するスクリプトの挿入位置。省略時はスクリプトリストの末尾に追加される。

例

トリガー「2」にスクリプトファイル step.scip と jump.scip を追加する。

```
ADD TRIGGER=2 SCRIPT=step.scip SCRIPT=jump.scip
```

関連コマンド

CREATE TRIGGER CPU (169 ページ)

CREATE TRIGGER FIREWALL (171 ページ)

CREATE TRIGGER INTERFACE (173 ページ)

CREATE TRIGGER MEMORY (175 ページ)

CREATE TRIGGER MODULE (177 ページ)

CREATE TRIGGER PERIODIC (180 ページ)

CREATE TRIGGER REBOOT (182 ページ)

CREATE TRIGGER TIME (184 ページ)

DELETE TRIGGER (205 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SET TRIGGER CPU (342 ページ)

SET TRIGGER FIREWALL (344 ページ)
SET TRIGGER INTERFACE (346 ページ)
SET TRIGGER MEMORY (348 ページ)
SET TRIGGER MODULE (350 ページ)
SET TRIGGER PERIODIC (352 ページ)
SET TRIGGER REBOOT (354 ページ)
SET TRIGGER TIME (356 ページ)
SHOW TRIGGER (470 ページ)

ADD USER

カテゴリー：運用・管理 / ユーザー認証データベース

```
ADD USER=login-name PASSWORD=password [LOGIN={TRUE|FALSE|ON|OFF|YES|NO}]
[DESCRIPTION=string] [PRIVILEGE={USER|MANAGER|SECURITYOFFICER}]
[TELNET={YES|NO}] [IPADDRESS=ipadd] [NETMASK=ipadd] [MTU=40..1500]
```

login-name: ログイン名(1～64文字。大文字小文字を区別しない。空白不可。入力可能文字:!#\$%&'()*+,-./0123456789;<=>@ABCDEFGHIJKLMNOPQRSTUVWXYZ)

password: パスワード(1～32文字。大文字小文字を区別する。空白を使用する場合、全体をダブルクォーテーション(" ")で

囲む。入力可能文字:!#\$%&'()*+,-./0123456789;<=>@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|})

string: 文字列(1～24文字)

ipadd: IP アドレスまたはネットマスク

解説

認証データベースにユーザーを追加する。

パラメーター

USER ログイン名。大文字小文字を区別しない。

PASSWORD パスワード。大文字小文字を区別する。デフォルトは6文字以上のパスワードを設定する必要がある。

LOGIN ユーザーにコマンドラインインターフェースへのログインを許すかどうか。PRIVILEGE パラメーターを省略した場合および PRIVILEGE パラメーターに USER を指定した場合は必須。ユーザーレベルが MANAGER/SECURITYOFFICER のユーザーにもログインを許可しないよう設定できるため注意が必要。

DESCRIPTION ユーザーに関するコメント

PRIVILEGE ユーザーレベル。一般ユーザー(USER) 管理者(MANAGER) Security Officer(SECURITYOFFICER) から選択する。省略時は USER レベル。

TELNET 別ホストへの Telnet を許すかどうか。ログインしたユーザーに、TELNET コマンドを使用させるかどうかを指定する。省略時は NO。

IPADDRESS ユーザーに割り当てる IP アドレス。PPP など接続してきたユーザーに割り当てるためのもの。NETMASK の指定も必須。

NETMASK ユーザーが使用するネットマスク。IPADDRESS と組で指定する。

MTU ユーザーの MTU 値を 40～1500 の範囲で指定する。

例

Manager 権限のユーザー「HIYO」を作成する。パスワードは「il0vEba7」。

```
ADD USER=HIYO PASSWORD=i10vEba7 PRIVILEGE=MANAGER
```

Security Officer 権限のユーザー「super」を作成する。

```
ADD USER=super DESCRIPTION="super user" PASSWORD=ureBus  
PRIVILEGE=SECURITYOFFICER
```

PPP ユーザー UserA を登録する。コマンドラインへのログインは許可しない。

```
ADD USER=UserA PASSWORD=arappap LOGIN=NO
```

PPP ユーザー UserB を登録する。IP アドレス 192.168.10.231 を固定的に割り当てる。

```
ADD USER=UserB PASSWORD=araraynoh IP=192.168.10.231  
NETMASK=255.255.255.255 LOGIN=NO
```

関連コマンド

DELETE USER (206 ページ)

DISABLE SYSTEM SECURITY_MODE (230 ページ)

DISABLE USER (233 ページ)

ENABLE SYSTEM SECURITY_MODE (263 ページ)

ENABLE USER (266 ページ)

PURGE USER (284 ページ)

RESET USER (292 ページ)

SET USER (359 ページ)

SHOW USER (478 ページ)

ADD USER RSO

カテゴリー：運用・管理 / セキュリティー

ADD USER RSO IP=*ipadd* [MASK=*ipadd*]

ipadd: IP アドレスまたはネットマスク

解説

セキュリティーモード時に Security Officer 権限で Telnet ログインできるホストの IP アドレス (RSO アドレス。RSO=Remote Security Officer) を設定する。

ネットマスクによる範囲指定も可能。セキュリティーモードでは、本コマンドで指定したアドレス範囲外からは Security Officer 権限での Telnet ログインができない。

パラメーター

IP RSO アドレスのベースアドレスを指定する。

MASK ベースアドレスに対するネットマスク値を指定する。省略時は、255.255.255.255 (単一ホスト) を指定したものとみなされる。

例

ホスト 172.16.10.6 を Remote Security Officer として設定する

```
ADD USER RSO IP=172.16.10.6
```

ネットワーク 192.168.200.0/24 上の全ホストを Remote Security Officer として設定する

```
ADD USER RSO IP=192.168.200.0 MASK=255.255.255.0
```

全ホストを Remote Security Officer として設定する

```
ADD USER RSO IP=0.0.0.0 MASK=0.0.0.0
```

備考・注意事項

IP パラメーターに 0.0.0.0、MASK パラメーターに 0.0.0.0 を設定すると、インターネット上の不定グローバル IP から Telnet ログインすることができるが、高レベルのセキュリティーを保つことができないので注意が必要。

関連コマンド

DELETE USER RSO (207 ページ)

DISABLE SYSTEM SECURITY_MODE (230 ページ)

DISABLE USER RSO (234 ページ)

ENABLE SYSTEM SECURITY_MODE (263 ページ)

ENABLE USER RSO (267 ページ)

SHOW USER RSO (482 ページ)

CLEAR FLASH TOTALLY

カテゴリー：運用・管理 / 記憶装置とファイルシステム

CLEAR FLASH TOTALLY

解説

フラッシュメモリーの内容を全消去する。

備考・注意事項

フラッシュメモリー上のすべてのデータが失われるため、特別な理由なく本コマンドを実行しないよう注意。

関連コマンド

SHOW FLASH (378 ページ)

CLEAR NVS TOTALLY

カテゴリー：運用・管理 / 記憶装置とファイルシステム

CLEAR NVS TOTALLY

解説

不揮発性メモリー（NVS）の内容を全消去する。

備考・注意事項

NVS 上のすべてのデータが失われるため、特別な理由なく本コマンドを実行しないよう注意。

関連コマンド

SHOW NVS (409 ページ)

SHOW NVS FREE (411 ページ)

COPY

カテゴリー：運用・管理 / 記憶装置とファイルシステム

COPY *src-filename dst-filename*

src-filename: コピー元ファイル名 ([device:]filename.ext の形式。device:省略時は flash:と見なされる)

dst-filename: コピー先ファイル名 ([device:]filename.ext の形式。device:省略時は flash:と見なされる)

解説

ファイルをコピーする。

例

フラッシュメモリー上のファイル cur.cfg を curbak.cfg という名前でコピーする。

```
COPY cur.cfg curbak.cfg
```

関連コマンド

RENAME (286 ページ)

SHOW FILE (374 ページ)

CREATE CONFIG

カテゴリー：運用・管理 / コンフィグレーション

CREATE CONFIG=filename [SET]

filename: ファイル名（拡張子は.scf か.cfg）

解説

現在の設定内容（メモリー上の設定内容）をスクリプトファイルに保存する。

パラメーター

CONFIG 設定スクリプトファイル名。拡張子は「.CFG」か「.SCP」。指定したファイルがすでに存在していた場合は上書きされる。存在しない場合は新規作成される。

SET 設定内容をスクリプトファイルに保存すると同時に、該当ファイルを起動時設定ファイルとして設定したい場合は本オプションを指定する（本コマンド実行後に SET CONFIG コマンドを実行しても同じ）。

例

現在の設定情報を basic.cfg に保存し、再起動後も同じ設定が使われるようにする（SET オプションを使うと 1 コマンドで済ませられる）。

```
CREATE CONFIG=basic.cfg
```

```
SET CONFIG=basic.cfg
```

または

```
CREATE CONFIG=basic.cfg SET
```

備考・注意事項

設定内容は一定の法則にしたがってスクリプト化されるため、必ずしも入力したコマンドがそのまま保存されるとは限らない。

関連コマンド

RESTART (293 ページ)

SET CONFIG (295 ページ)

SHOW CONFIG (363 ページ)

CREATE FFILE

カテゴリー：運用・管理 / 記憶装置とファイルシステム

CREATE FFILE=filename {DATA=value-list|ADDRESS=address LENGTH=length}

filename: ファイル名

value-list: バイト列 (16 進数。1 バイトごとにカンマで区切る。最大 80 バイト)

address: メモリーアドレス (16 進数)

length: バイト長 (16 進数)

解説

フラッシュファイルシステム上にファイルを作成する。

DATA パラメーターでファイルの内容を指定する方法と、ADDRESS パラメーターと LENGTH パラメーターで元データの位置と大きさを指定し、新規ファイルにコピーする方法がある。

パラメーター

FFILE 作成するファイルの名前

DATA ファイルの内容を 16 進表記のバイト列として指定する。「DATA=50,4F,54,45,4E,45,4B,4F」のように各バイトを 16 進数で表し、バイトごとにカンマで区切って指定する。

ADDRESS ソースデータの開始アドレスを指定する。

LENGTH ソースデータの長さを指定する。

例

8 つのバイト「0x50,0x4F,0x54,0x45,0x4E,0x45,0x4B,0x4F」からなる「TINY.TXT」を作成する。

```
CREATE FFILE=TINY.TXT DATA=50,4F,54,45,4E,45,4B,4F
```

アドレス「0x00」からの 0xC0000 バイトを「BIG.FIL」にコピーする。

```
CREATE FFILE=BIG.FIL ADDRESS=0 LENGTH=C0000
```

備考・注意事項

通常使う必要はない。

関連コマンド

DELETE FFILE (188 ページ)

CREATE FFILE

SHOW FFILE (372 ページ)

CREATE FILE

カテゴリー：運用・管理 / 記憶装置とファイルシステム

CREATE FILE=filename [FORCE] [COMMAND=string] [SCRIPT=filename]
[PERMANENTREDIRECT] [LIMIT=0..1048576]

filename: ファイル名

string: 文字列（1～255 文字。空白を含む場合はダブルクォートで囲む）

解説

指定されたコマンド行やスクリプトを実行し、その出力を指定されたテキストファイルに保存（リダイレクト）する。

パラメーター

FILE 出力先のテキストファイル名。指定したファイルが存在しない場合は作成される。指定したファイルが存在している場合はエラーになるが、FORCE オプションを指定した場合は強制的に上書きする

FORCE FILE パラメーターで指定したテキストファイルを上書きしてよい場合に指定する。本オプションを指定しない場合は、FILE パラメーターで指定したファイルが存在しているとエラーになる

COMMAND 実行するコマンド行。通常は情報表示用の「SHOW XXXX」コマンドを指定する。空白を含む場合はダブルクォートで囲むこと。SCRIPT パラメーターと同時に指定することはできない

SCRIPT 実行するスクリプトファイル名。COMMAND パラメーターと同時に指定することはできない

PERMANENTREDIRECT 指定したコマンド行やスクリプトの出力を継続的にファイルへ書き込みたいときに指定する。このオプションは、COMMAND パラメーターにデバッグオプションを有効化する「ENABLE XXXX DEBUG」コマンドを指定した場合、あるいは、SCRIPT パラメーターに「ENABLE XXXX DEBUG」コマンドを含むスクリプトを指定した場合にのみ有効。本オプションを指定した場合、FILE パラメーターで指定したテキストファイルは書き込み用にオープンされたままの状態となり、他のコマンドによって表示、変更などの操作ができないようロックされる。該当ファイルへの出力を終了しファイルをクローズするには、RESET FILE PERMANENTREDIRECT コマンドを実行すること

LIMIT 出力先テキストファイルの上限サイズ（バイト）。省略時は 204800 バイト

入力・出力・画面例

```
Manager > create file=time.txt command="show time"
Info (1056003): Operation successful.

Manager > show file=time.txt
File : time.txt
1:
2:
```

```

3: System time is 11:13:59 on Thursday 01-Nov-2007.

Manager > create file=time.txt command="show time"
Error (3056063): time.txt already exists.

Manager > create file=time.txt force command="show time"
Info (1056003): Operation successful.

Manager > show file=time.txt
File : time.txt
1:
2:
3: System time is 11:14:14 on Thursday 01-Nov-2007.

Manager > create file=ipdebug.txt command="enable ip debug=all" permanentredirect
Info (1056003): Operation successful.

Manager > reset file=ipdebug.txt permanentredirect
Info (1056278): ipdebug.txt redirection - operation complete.

Manager > show file=ipdebug.txt
File : ipdebug.txt
1:
2:
3: Info (1005287): All IP debugging has been enabled.
4: <I/C/B=vlan1/2/0, l=60, ttl=128, p=1, addr=192.168.20.11>192.168.20.1
5: >I/C/T/R/Id=Loc/0/fw/??/61533, l=60, ttl=64, p=1, addr=192.168.20.1>192.168.20.11
6: <I/C/B=vlan1/2/0, l=60, ttl=128, p=1, addr=192.168.20.11>192.168.20.1
7: >I/C/T/R/Id=Loc/0/fw/??/61534, l=60, ttl=64, p=1, addr=192.168.20.1>192.168.20.11
...

Manager > disable ip debug=all
Info (1087003): Operation successful.

```

例

新規ファイル iproute.txt を作成し、コマンド行「show ip route」の実行結果を出力する。iproute.txt がすでに存在していた場合はエラーになる。

```
CREATE FILE=iproute.txt COMMAND="show ip route"
```

既存ファイルに上書き出力したいときは、FORCE オプションを付ける。一方、既存ファイルに追記したいときは、ADD FILE コマンドを使う。

```
CREATE FILE=iproute.txt FORCE COMMAND="show ip route"
```

新規ファイル ipdebug.txt にデバッグコマンド「enable ip debug=all」の出力を継続的に書き込む。出力

を終了しファイルをクローズするには、RESET FILE PERMANENTREDIRECT コマンドを実行する。なお、ファイルをクローズしてもデバッグオプションは有効なままなので、この例では「disable ip debug=all」を実行してデバッグオプションも無効にすること。

```
CREATE FILE=ipdebug.txt COMMAND="enable ip debug=all" PERMANENTREDIRECT
```

備考・注意事項

COMMAND パラメーターで指定したコマンド行や、SCRIPT パラメーターで指定したスクリプトは、本コマンドの入力と同時に実行される。

「SHOW XXXX」コマンドの出力をファイルに保存したいとき、PERMANENTREDIRECT オプションは意味を持たないので指定しないこと。同オプションを指定して「SHOW XXXX」コマンドを実行した場合は、本コマンド入力時に実行された「SHOW XXXX」コマンドの出力だけがファイルに書き込まれ、それ以降「SHOW XXXX」コマンドを実行してもそれらはファイルに追記されず、ただファイルだけがオープン（ロック）されたままとなるので注意。

「ENABLE XXXX DEBUG」コマンドによるデバッグ出力をファイルに保存したいときは、必ず PERMANENTREDIRECT オプションを指定すること。同オプションを指定せずに「ENABLE XXXX DEBUG」コマンドを実行した場合は、デバッグオプション有効化コマンドの実行に成功した、あるいは失敗したというメッセージだけがファイルに保存されるので注意。

「ENABLE XXXX DEBUG」コマンドを本コマンドから実行した場合、ファイルへの出力が完了しても、該当デバッグ出力はコンソールに表示されない。これは、PERMANENTREDIRECT オプションを指定したかどうかとは関係ない。デバッグ出力をコンソールに表示させたい場合は、再度「ENABLE XXXX DEBUG」コマンドを実行すること。なお、ファイルへの出力中に「ENABLE XXXX DEBUG」コマンドを再実行すると、ファイルへの出力が停止するので注意。

「ENABLE XXXX DEBUG」コマンドを本コマンドから実行した場合、ファイルへの出力が完了しても、該当デバッグオプションは有効なままとなる。これは、PERMANENTREDIRECT オプションを指定したかどうかとは関係ない。ファイルへの出力が完了し、デバッグ出力の収集が完了したら、「DISABLE XXXX DEBUG」コマンドを実行して、デバッグオプションを無効にすること。

関連コマンド

ADD FILE (123 ページ)

RESET FILE PERMANENTREDIRECT (287 ページ)

SHOW FILE (374 ページ)

SHOW FILE PERMANENTREDIRECT (376 ページ)

CREATE LOG OUTPUT

カテゴリー：運用・管理 / ログ

```
CREATE LOG OUTPUT={TEMPORARY|PERMANENT|output-id} DESTINATION={EMAIL|  
MEMORY|NVS|PORT|ROUTER|SYSLOG} [FORMAT={FULL|MSGONLY|SUMMARY}]  
[MAXQUEUESEVERITY=severity] [MESSAGES=count] [PASSWORD={password|NONE}]  
[ASYN=asyn-number] [QUEUEONLY={YES|NO}] [SECURE={YES|NO}] [SERVER=ipadd]  
[TO=email-addr] [ZONE={time-zone|utc-offset}] [FACILITY={DEFAULT|  
LOCAL1..LOCAL7}]
```

output-id: ログ出力 ID (1~20)

severity: ログレベル (0~7)

count: 個数 (1~)

password: パスワード (1~16 文字)

asyn-number: 非同期ポート番号 (0)

ipadd: IP アドレス

email-addr: 電子メールアドレス

time-zone: タイムゾーン名

utc-offset: 協定世界時 (UTC) からのオフセット (+23:59:59 ~ -23:59:59)

解説

ログの出力先を定義する。

出力先の定義後は、ADD LOG OUTPUT コマンドでメッセージフィルターを追加し、どのようなメッセージを出力するかを指定する必要がある。

パラメーター

OUTPUT ログ出力先 ID。1~20 の任意の番号か、特殊なキーワード「TEMPORARY」(RAM) または「PERMANENT」(NVS) を指定する。TEMPORARY を指定した場合、MAXQUEUESEVERITY、QUEUEONLY、SECURE の各パラメーターは指定できず、DESTINATION は MEMORY しか指定できない。また、PERMANENT を指定したときは、DESTINATION に NVS しか指定できない (NVS (不揮発性メモリー) 搭載機種でのみ有効)。

DESTINATION ログメッセージの出力先。EMAIL (TO パラメーターで指定されたアドレスに電子メールで送信)、MEMORY (RAM 上に保存。OUTPUT パラメーターに TEMPORARY を指定したときのみ有効)、NVS (不揮発性メモリー上に保存。OUTPUT パラメーターに PERMANENT を指定したときのみ有効)、PORT (ASYN パラメーターで指定した非同期ポートに出力)、ROUTER (SERVER パラメーターで指定したルーターに Secure Router Logging Protocol (SRLP) を使って転送)、SYSLOG (SERVER パラメーターで指定した syslog サーバーに転送。メッセージは syslog フォーマットに変換される) から選択する。

FORMAT 非同期ポートに出力するログメッセージの形式。FULL (すべての情報を表示。1 ログエントリが複数行に渡って表示される。空行がエントリーの区切りになる)、MSGONLY (テキストメッ

セージのみを表示) SUMMARY (サマリーを表示。表示されないフィールドもある) デフォルトは SUMMARY。DESTINATION パラメーターに PORT を指定した場合のみ有効。

MAXQUEUESEVERITY QUEUEONLY パラメーターに YES を指定した (キューがいっぱいになるまでログを出力しない) ときに、すぐに出力せずにキューに入れる最大のログレベルを指定する。QUEUEONLY が YES のときは、MAXQUEUESEVERITY よりも低いログレベルのメッセージは、キューの長さが MESSAGES パラメーターの値に達するまでキューイングされる。一方、MAXQUEUESEVERITY 以上のログレベルを持つメッセージが生成されたときは、ただちにキューがフラッシュ (処理) される。DESTINATION パラメーターに PORT か SYSLOG を指定しているとき、および、OUTPUT パラメーターに TEMPORARY を指定しているときは、本パラメーターは指定できない。デフォルトは 7、すなわちキューがいっぱいにならないうちに処理されるのは、最高のログレベルを持つメッセージが来たときだけとなる。

MESSAGES DESTINATION が SYSLOG の場合は、キューの長さ。DESTINATION が NVS か MEMORY のときは、保存するメッセージの最大数。最大値に達したときは、古いメッセージから順番に削除される。DESTINATION が EMAIL の場合は、一度に送信されるメッセージの数。DESTINATION が PORT のときは、本パラメーターは指定できない。DESTINATION が SYSLOG のときのデフォルトは 20、MEMORY のときのデフォルトは 200、EMAIL のときは 100。NVS のときは 20。

PASSWORD SRLP でログを転送する際、転送先から認証を受けるためのパスワード。DESTINATION が ROUTER の場合にのみ有効。パスワードそのものは送信されず、代わりに MD5 によるメッセージダイジェストが送られる。デフォルトはパスワードなし。

ASYN ログを出力する非同期ポートの番号。DESTINATION に PORT を指定した場合にのみ有効。

QUEUEONLY キューがいっぱいになるまでメッセージを処理しないかどうか。DESTINATION に PORT を指定した場合、および、OUTPUT に TEMPORARY を指定した場合は、本パラメーターは指定できない。DESTINATION に SYSLOG を指定した場合、本パラメーターは動作しない。デフォルトは NO。

SECURE この出力先が「安全」かどうかを指定する。NO を指定した場合、パスワード変更など一部のメッセージが出力されなくなる。OUTPUT に TEMPORARY を指定した場合は、本パラメーターは指定できない。DESTINATION が ROUTER で PASSWORD が指定されている場合、および、DESTINATION が MEMORY か NVS の場合のデフォルトは YES。その他の場合のデフォルトは NO。

SERVER DESTINATION が ROUTER か SYSLOG の場合に、メッセージの転送先 IP アドレスを指定する。ROUTER の場合は、SRLP (Secure Router Logging Protocol) サーバー (UDP 5023 番)、SYSLOG の場合は syslog サーバー (UDP 514 番) を指定する。

TO DESTINATION に EMAIL を指定した場合に送信先メールアドレスを指定する。

ZONE タイムゾーン名または UTC からのオフセットを指定する。

FACILITY DESTINATION が SYSLOG の場合、送信する syslog メッセージの「ファシリティ」を指定する。DEFAULT を指定した場合は、既定の対応表 (解説編参照) にしたがって、本製品のメッセージタイプが syslog ファシリティに変換される。LOCAL1~LOCAL7 を指定した場合は、本出力先宛ての syslog メッセージすべてに指定したファシリティ値がセットされる。デフォルトは DEFAULT (既定の対応表に基づいてファシリティを決定)。

例

すべてのログを syslog サーバー 192.168.1.2 に送る

```
CREATE LOG OUTPUT=1 DESTINATION=SYSLOG SERVER=192.168.1.2  
ADD LOG OUTPUT=1 FILTER=1 ALL
```

関連コマンド

ADD LOG OUTPUT (126 ページ)
DELETE LOG OUTPUT (191 ページ)
DESTROY LOG OUTPUT (208 ページ)
DISABLE LOG OUTPUT (216 ページ)
ENABLE LOG OUTPUT (246 ページ)
SET LOG OUTPUT (300 ページ)

CREATE SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

```
CREATE SNMP COMMUNITY=community [ACCESS={READ|WRITE}]
[MANAGER=ipadd[/masklen]] [TRAPHOST=ipadd] [V1TRAPHOST=ipadd]
[V2CTRAHOST=ipadd] [OPEN={ON|OFF|YES|NO|TRUE|FALSE}]
```

community: SNMP コミュニティー名 (1～15 文字。大文字小文字を区別する)

ipadd: IP アドレス

masklen: マスク長 (0～32)

解説

(SNMPv1/v2c) SNMP コミュニティーを作成する。

パラメーター

COMMUNITY SNMP コミュニティー名

ACCESS コミュニティーのアクセス権を指定する。READ (デフォルト) は読み出しのみを許可、WRITE は読み書き両方を許可する。

MANAGER SNMP オペレーションを許可するホストを指定する。マスク長を付加することで範囲指定も可能。本製品は、MANAGER に登録されていないホストからの SNMP 要求には応答しない。ただし、SNMP コミュニティーの OPEN パラメーターが YES の場合は、MANAGER パラメーターの設定にかかわらず、すべての SNMP 要求に応答する。トラップホスト同様、複数指定する場合はコミュニティ作成後に ADD SNMP COMMUNITY で追加する。

TRAPHOST SNMPv1 トラップの送信先ホストを指定する。コミュニティには複数のトラップホストを指定できるが、CREATE SNMP COMMUNITY コマンドでは 1 つしか指定できない。複数のトラップホストを使う場合は、コミュニティ作成後に ADD SNMP COMMUNITY コマンドで追加する。

V1TRAPHOST SNMPv1 トラップの送信先ホスト。TRAPHOST パラメーターと同じ。

V2CTRAHOST SNMPv2c トラップの送信先ホスト。ここで指定したホストには SNMPv2c 形式のトラップが送信される。

OPEN SNMP オペレーションをすべてのホストに開放するかどうかを示す。NO (デフォルト) は、MANAGER パラメーターで指定したホストのみに制限することを示す。YES を指定すると、すべての SNMP 要求を受け入れる。ON、YES、TRUE および OFF、NO、FALSE はそれぞれ同じ意味。

例

SNMP コミュニティー「public」を作成する。

```
CREATE SNMP COMMUNITY=public
```

書き込み権限のある SNMP コミュニティー「admins」を作成し、管理ステーション兼トラップホストとして 172.20.1.1 を指定する。

```
CREATE SNMP COMMUNITY=admins ACCESS=WRITE MANAGER=172.20.1.1  
TRAPHOST=172.20.1.1
```

備考・注意事項

SNMP トラップは、ENABLE SNMP COMMUNITY TRAP コマンドを実行してコミュニティのトラップ設定を有効にしないと送信されないので注意が必要。

関連コマンド

ADD SNMP COMMUNITY (134 ページ)
DELETE SNMP COMMUNITY (198 ページ)
DESTROY SNMP COMMUNITY (210 ページ)
DISABLE SNMP (224 ページ)
DISABLE SNMP COMMUNITY (226 ページ)
DISABLE SNMP COMMUNITY TRAP (227 ページ)
ENABLE SNMP (257 ページ)
ENABLE SNMP COMMUNITY (259 ページ)
ENABLE SNMP COMMUNITY TRAP (260 ページ)
SET SNMP COMMUNITY (325 ページ)
SHOW SNMP COMMUNITY (441 ページ)

CREATE TRIGGER CPU

カテゴリー：運用・管理 / トリガー

```
CREATE TRIGGER=trigger-id CPU=1..100 [DIRECTION={UP|DOWN|ANY}]
[AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]
[REPEAT={YES|NO|ONCE|FOREVER|count}] [SCRIPT=filename...]
[STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

filename: ファイル名 (拡張子は.scp か.cfg)

解説

CPU トリガーを作成する。

CPU トリガーは、CPU 負荷率が指定値を横切ったときに起動される。DIRECTION パラメーターにより、上回ったとき、下回ったとき、上回ったときと下回ったときの指定が可能。トリガーから実行されるスクリプトには、特殊な引数として、%D (日付)、%T (時刻)、%N (システム名)、%S (シリアル番号) が渡される。

パラメーター

TRIGGER トリガー番号

CPU しきい値。CPU 負荷率をパーセンテージで指定する。

DIRECTION 起動条件。UP (しきい値まで上がるか上回ったとき)、DOWN (しきい値まで下がるか下回ったとき)、ANY (両方) から選択する。デフォルトは ANY。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設け

ないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

SCRIPT トリガー起動時に実行するスクリプトファイルを指定する。SCRIPT パラメーターは、1 コマンドラインに複数個指定できる。また、トリガー作成後にも、ADD TRIGGER コマンドで追加可能。スクリプトの実行は記述順。1 つのトリガーに関連付けられるスクリプトは最高 5 個。

STATE トリガーの有効・無効。省略時のデフォルト値は ENABLED。無効状態のトリガーは自動的に起動されないが、ACTIVATE TRIGGER コマンドを使えば手動で起動できる。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

例

CPU の負荷が 80%を超えたら、cpuwarn.scp を実行する CPU トリガー「1」を作成する。

```
CREATE TRIGGER=1 CPU=80 DIRECTION=UP SCRIPT=cpuwarn.scp
```

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SET TRIGGER CPU (342 ページ)

SHOW TRIGGER (470 ページ)

CREATE TRIGGER FIREWALL

カテゴリー：運用・管理 / トリガー

```
CREATE TRIGGER=trigger-id FIREWALL={ALL|DOSATTACK|FRAGATTACK|HOSTSCAN|  
PORTSCAN|SMURFATTACK|SYNATTACK|TCPATTACK} [MODE={START|END|BOTH}]  
[AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]  
[REPEAT={YES|NO|ONCE|FOREVER|count}] [SCRIPT=filename...]  
[STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1 ~ 250)

time: 時刻 (hh:mm の形式。hh は時 (0 ~ 23) mm は分 (0 ~ 59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1 ~ 31) mmm は月 (英語月名の頭 3 文字。例: APR) yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1 ~ 40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1 ~ 4294967294)

filename: ファイル名 (拡張子は.scp か.cfg)

解説

ファイアウォールトリガーを作成する。

ファイアウォールトリガーは、指定したファイアウォールイベント (各種攻撃の開始、終了、またはその両方) が発生したときに起動される。トリガーから実行されるスクリプトには、特殊な引数として、%D (日付)、%T (時刻)、%N (システム名)、%S (シリアル番号) が渡される。また、ファイアウォールトリガーは、起動するスクリプトに 2 つの引数を渡す。引数 1 (%1) はファイアウォールポリシー名、引数 2 (%2) は攻撃元の IP アドレス。

パラメーター

TRIGGER トリガー番号

FIREWALL ファイアウォールの攻撃イベント名。指定した攻撃イベントの発生時にトリガーが起動される。MODE パラメーターと組み合わせることにより、より細かい指定が可能。

MODE 攻撃のどのタイミングでトリガーを起動させるかを指定する。START は攻撃開始時、END は攻撃終了時、BOTH は攻撃開始時と攻撃終了時にトリガーを起動する。デフォルトは BOTH。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL

はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

SCRIPT トリガー起動時に実行するスクリプトファイルを指定する。SCRIPT パラメーターは、1 コマンドラインに複数個指定できる。また、トリガー作成後にも、ADD TRIGGER コマンドで追加可能。スクリプトの実行は記述順。1 つのトリガーに関連付けられるスクリプトは最高 5 個。

STATE トリガーの有効・無効。省略時のデフォルト値は ENABLED。無効状態のトリガーは自動的に起動されないが、ACTIVATE TRIGGER コマンドを使えば手動で起動できる。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

例

ポートスキャン開始の検出時に管理者にメールを送るファイアウォールトリガーを作成する。メールはサブジェクトのみ。サブジェクトには攻撃者の IP アドレスと、ファイアウォールポリシー名が入る。

```
CREATE TRIGGER=1 FIREWALL=PORTSCAN MODE=START SCRIPT=pscans.scp
```

スクリプト「pscans.scp」の内容

```
MAIL TO=admin@mydomain.xxx SUBJECT="Portscan from %2 (Policy: %1)"
```

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SET FIREWALL POLICY ATTACK (「ファイアウォール」の 131 ページ)

SET TRIGGER FIREWALL (344 ページ)

SHOW TRIGGER (470 ページ)

CREATE TRIGGER INTERFACE

カテゴリー：運用・管理 / トリガー

```
CREATE TRIGGER=trigger-id INTERFACE=interface EVENT={UP|DOWN|FAIL|ANY}
[CP={BCP|CCP|IPCP|LCP}] [AFTER=time] [BEFORE=time] [{DATE=date|
DAYS=day-list}] [NAME=string] [REPEAT={YES|NO|ONCE|FOREVER|count}]
[SCRIPT=filename...] [STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

interface: インターフェース名

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

filename: ファイル名 (拡張子は .scp か .cfg)

解説

インターフェーストリガーを作成する。

インターフェーストリガーは、指定インターフェースのリンクステータスが変化したときに起動される。トリガーから実行されるスクリプトには、特殊な引数として、%D (日付)、%T (時刻)、%N (システム名)、%S (シリアル番号) が渡される。

パラメーター

TRIGGER トリガー番号

INTERFACE 監視するインターフェース名を指定する。指定できるのは、Ethernet インターフェース (ethX)、VLAN インターフェース (vlanX)、PPP インターフェース (pppX) のみ。PPP インターフェースの場合は、CP パラメーターも指定可能。

EVENT 該当インターフェースのリンクステータスがどのように変化した場合にトリガーを起動させるかを指定する。UP はリンクアップ時、DOWN はリンクダウン時、FAIL はリンクアップ失敗時、ANY はすべてのリンクステータス変化時を意味する。Ethernet、VLAN インターフェースでは、UP と DOWN のみ有効。

CP 監視する PPP コントロールプロトコルを指定する。INTERFACE に PPP インターフェースを指定した場合にのみ有効。トリガースクリプトには、%1 (PPP インターフェース名)、%2 (コントロールプロトコル)、%3 (イベント名) の3つの引数が渡される。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

SCRIPT トリガー起動時に実行するスクリプトファイルを指定する。SCRIPT パラメーターは、1 コマンドラインに複数個指定できる。また、トリガー作成後にも、ADD TRIGGER コマンドで追加可能。スクリプトの実行は記述順。1 つのトリガーに関連付けられるスクリプトは最高 5 個。

STATE トリガーの有効・無効。省略時のデフォルト値は ENABLED。無効状態のトリガーは自動的に起動されないが、ACTIVATE TRIGGER コマンドを使えば手動で起動できる。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SET TRIGGER INTERFACE (346 ページ)

SHOW TRIGGER (470 ページ)

CREATE TRIGGER MEMORY

カテゴリー：運用・管理 / トリガー

```
CREATE TRIGGER=trigger-id MEMORY=1..100 [DIRECTION={UP|DOWN|ANY}]
[AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]
[REPEAT={YES|NO|ONCE|FOREVER|count}] [SCRIPT=filename...]
[STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

filename: ファイル名 (拡張子は .scp か .cfg)

解説

メモリートリガーを作成する。

メモリートリガーは、空きメモリー容量が指定値を横切ったときに起動される。DIRECTION パラメーターにより、上回ったとき、下回ったとき、上回ったときと下回ったときの指定が可能。トリガーから実行されるスクリプトには、特殊な引数として、%D (日付)、%T (時刻)、%N (システム名)、%S (シリアル番号) が渡される。

パラメーター

TRIGGER トリガー番号

MEMORY しきい値。空きメモリー容量をパーセンテージで指定する。

DIRECTION 起動条件。UP (しきい値まで上がるか上回ったとき)、DOWN (しきい値まで下がるか下回ったとき)、ANY (両方) から選択する。デフォルトは ANY。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返し

を許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

SCRIPT トリガー起動時に実行するスクリプトファイルを指定する。SCRIPT パラメーターは、1 コマンドラインに複数個指定できる。また、トリガー作成後にも、ADD TRIGGER コマンドで追加可能。スクリプトの実行は記述順。1 つのトリガーに関連付けられるスクリプトは最高 5 個。

STATE トリガーの有効・無効。省略時のデフォルト値は ENABLED。無効状態のトリガーは自動的に起動されないが、ACTIVATE TRIGGER コマンドを使えば手動で起動できる。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

例

空きメモリー容量が 20%を切ったら、memwarn.scp を実行するメモリートリガー「1」を作成する。

```
CREATE TRIGGER=1 MEMORY=20 DIRECTION=DOWN SCRIPT=memwarn.scp
```

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SET TRIGGER MEMORY (348 ページ)

SHOW TRIGGER (470 ページ)

CREATE TRIGGER MODULE

カテゴリー：運用・管理 / トリガー

CREATE TRIGGER=trigger-id MODULE=module-name EVENT=event

[*module-parameters...*] [AFTER=*time*] [BEFORE=*time*] [{DATE=*date*|
DAYS=*day-list*}] [NAME=*string*] [REPEAT={YES|NO|ONCE|FOREVER|*count*}]
[SCRIPT=*filename...*] [STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]

trigger-id: トリガー番号 (1~250)

module-name: モジュール名

event: モジュール独自のイベント名

module-parameters: モジュール独自のパラメーター

time: 時刻 (hh:mm の形式。hh は時 (0~23) mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31) mmm は月 (英語月名の頭3文字。例: APR) yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

filename: ファイル名 (拡張子は.scp か.cfg)

解説

モジュールトリガーを作成する。

モジュールトリガーは、指定モジュールのイベントが発生したときに起動される。モジュールトリガーのパラメーターは、指定モジュールによって異なる。トリガーから実行されるスクリプトには、特殊な引数として、%D (日付) %T (時刻) %N (システム名) %S (シリアル番号) が渡される。

サポートしているモジュールトリガーの一覧については、別表を参照。また、各モジュールトリガーの詳細仕様については、各機能の解説編を参照のこと。

パラメーター

TRIGGER トリガー番号

MODULE モジュール名

EVENT モジュール独自のイベント名

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

SCRIPT トリガー起動時に実行するスクリプトファイルを指定する。SCRIPT パラメーターは、1 コマンドラインに複数個指定できる。また、トリガー作成後にも、ADD TRIGGER コマンドで追加可能。スクリプトの実行は記述順。1 つのトリガーに関連付けられるスクリプトは最高 5 個。

STATE トリガーの有効・無効。省略時のデフォルト値は ENABLED。無効状態のトリガーは自動的に起動されないが、ACTIVATE TRIGGER コマンドを使えば手動で起動できる。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

| モジュール | 独自イベント | 独自パラメーター | 発生条件 |
|--------|------------|---------------------------|---------------------|
| SWITCH | LINKDOWN | PORT | スイッチポートがリンクダウン |
| | LINKUP | PORT | スイッチポートがリンクアップ |
| BGP | MEMORY | なし | メモリー不足により BGP 経路を破棄 |
| | PEERSTATE | PEER, BGPSTATE, DIRECTION | BGP ピア（との通信）状態が変化 |
| PING | DEVICEDOWN | POLL | 監視対象機器への到達性喪失 |
| | DEVICEUP | POLL | 監視対象機器への到達性回復 |
| VRRP | DOWNMASTER | VRID | マスタールーターがバックアップに降格 |
| | UPMASTER | VRID | バックアップルーターがマスターに昇格 |

表 32: モジュールトリガー一覧（詳細は各機能の解説編を参照）

例

バーチャルルーター「10」のマスタールーターになったら、bemaster.scp を実行するモジュールトリガーを作成

```
CREATE TRIGGER=1 MODULE=VRRP EVENT=UPMASTER VRID=10 SCRIPT=bemaster.scp
```

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SET TRIGGER MODULE (350 ページ)

SHOW TRIGGER (470 ページ)

CREATE TRIGGER PERIODIC

カテゴリー：運用・管理 / トリガー

```
CREATE TRIGGER=trigger-id PERIODIC=minutes [{DATE=date|DAYS=day-list}]
  [AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]
  [REPEAT={YES|NO|ONCE|FOREVER|count}] [SCRIPT=filename...]
  [STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

minutes: 時間 (1~1439 分)

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31) mmm は月 (英語月名の頭 3 文字。例: APR) yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

time: 時刻 (hh:mm の形式。hh は時 (0~23) mm は分 (0~59))

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

filename: ファイル名 (拡張子は .scp か .cfg)

解説

定期実行トリガーを作成する。

定期実行トリガーは、指定した間隔で繰り返し実行される。トリガーから実行されるスクリプトには、特殊な引数として、%D (日付) %T (時刻) %N (システム名) %S (シリアル番号) が渡される。

パラメーター

TRIGGER トリガー番号

PERIODIC トリガーの起動間隔を分で指定する。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

SCRIPT トリガー起動時に実行するスクリプトファイルを指定する。SCRIPT パラメーターは、1 コマンドラインに複数個指定できる。また、トリガー作成後にも、ADD TRIGGER コマンドで追加可能。スクリプトの実行は記述順。1 つのトリガーに関連付けられるスクリプトは最高 5 個。

STATE トリガーの有効・無効。省略時のデフォルト値は ENABLED。無効状態のトリガーは自動的に起動されないが、ACTIVATE TRIGGER コマンドを使えば手動で起動できる。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

例

3 時間に一回 patrol.scp を実行する定期実行トリガー「1」を作成

```
CREATE TRIGGER=1 PERIODIC=180 SCRIPT=patrol.scp
```

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SET TRIGGER PERIODIC (352 ページ)

SHOW TRIGGER (470 ページ)

CREATE TRIGGER REBOOT

カテゴリー：運用・管理 / トリガー

```
CREATE TRIGGER=trigger-id REBOOT={RESTART|CRASH|ALL} [{DATE=date|
    DAYS=day-list}] [AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}]
    [NAME=string] [REPEAT={YES|NO|ONCE|FOREVER|count}] [SCRIPT=filename...]
    [STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31) mmm は月 (英語月名の頭3文字。例: APR) yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

time: 時刻 (hh:mm の形式。hh は時 (0~23) mm は分 (0~59))

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

filename: ファイル名 (拡張子は .scp か .cfg)

解説

再起動トリガーを作成する。

再起動トリガーは、システムの再起動時に実行される。トリガーから実行されるスクリプトには、特殊な引数として、%D (日付) %T (時刻) %N (システム名) %S (シリアル番号) が渡される。

パラメーター

TRIGGER トリガー番号

REBOOT トリガーの起動条件となる再起動イベントを指定する。CRASH はクラッシュによる再起動、RESTART はクラッシュ以外の原因による再起動を意味する。ALL はすべての再起動を示す。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

SCRIPT トリガー起動時に実行するスクリプトファイルを指定する。SCRIPT パラメーターは、1 コマンドラインに複数個指定できる。また、トリガー作成後にも、ADD TRIGGER コマンドで追加可能。スクリプトの実行は記述順。1 つのトリガーに関連付けられるスクリプトは最高 5 個。

STATE トリガーの有効・無効。省略時のデフォルト値は ENABLED。無効状態のトリガーは自動的に起動されないが、ACTIVATE TRIGGER コマンドを使えば手動で起動できる。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

例

システムクラッシュ後に crash.scp を実行して管理者にメールを送る再起動トリガー「1」を作成

```
CREATE TRIGGER=1 REBOOT=CRASH SCRIPT=crash.scp
```

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SET TRIGGER REBOOT (354 ページ)

SHOW TRIGGER (470 ページ)

CREATE TRIGGER TIME

カテゴリー：運用・管理 / トリガー

```
CREATE TRIGGER=trigger-id TIME=time [{DATE=date|DAYS=day-list}]
      [SCRIPT=filename...] [NAME=string] [REPEAT={YES|NO|ONCE|FOREVER|count}]
      [STATE={ENABLED|DISABLED}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

filename: ファイル名 (拡張子は.scp か.cfg)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

解説

定時トリガーを作成する。

定時トリガーは指定した時刻に起動される。トリガーから実行されるスクリプトには、特殊な引数として、%D (日付)、%T (時刻)、%N (システム名)、%S (シリアル番号) が渡される。

パラメーター

TRIGGER トリガー番号

TIME トリガーの起動時刻を指定する。分まで指定できるが、前後約5秒の誤差がある。一般的には指定時刻の5秒後に起動されることが多い。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

SCRIPT トリガー起動時に実行するスクリプトファイルを指定する。SCRIPT パラメーターは、1 コマンドラインに複数個指定できる。また、トリガー作成後にも、ADD TRIGGER コマンドで追加可能。スクリプトの実行は記述順。1 つのトリガーに関連付けられるスクリプトは最高5個。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

STATE トリガーの有効・無効。省略時のデフォルト値は ENABLED。無効状態のトリガーは自動的に起動されないが、ACTIVATE TRIGGER コマンドを使えば手動で起動できる。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

例

毎日夜 11 時に pppon.scp を実行して PPP コネクションを開く定時トリガー「1」を作成

```
CREATE TRIGGER=1 TIME=23:00 SCRIPT=pppon.scp
```

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SET TRIGGER TIME (356 ページ)

SHOW TRIGGER (470 ページ)

DEACTIVATE SCRIPT

カテゴリー：運用・管理 / スクリプト

DEACTIVATE SCRIPT=*filename*

filename: ファイル名（拡張子は.scp か.cfg）

解説

実行中のスクリプトを停止させる。

パラメーター

SCRIPT スクリプトファイル名

例

実行中のスクリプト「runrun.scp」を停止させる。

```
DEACTIVATE SCRIPT=runrun.scp
```

関連コマンド

ACTIVATE SCRIPT (120 ページ)

ADD SCRIPT (133 ページ)

DELETE SCRIPT (197 ページ)

SET SCRIPT (323 ページ)

SHOW SCRIPT (434 ページ)

DELETE ALIAS

カテゴリー：運用・管理 / コマンドプロセッサ

DELETE ALIAS=*alias*

alias: エイリアス名（1～132 文字。大文字小文字を区別しない。空白を含む場合はダブルクォートで囲む）

解説

コマンドの別名（エイリアス）を削除する。

パラメーター

ALIAS エイリアス名

例

エイリアス「ls」を削除する。

```
DELETE ALIAS=ls
```

関連コマンド

ADD ALIAS (122 ページ)

SHOW ALIAS (361 ページ)

DELETE FFILE

カテゴリー：運用・管理 / 記憶装置とファイルシステム

DELETE FFILE=filename

filename: ファイル名（ワイルドカード指定可能）

解説

フラッシュファイルシステム上のファイルを削除する。

パラメーター

FFILE ファイル名を指定する。ワイルドカード（*）も指定可能。長い名前（28.3 形式）は認識しないので、短い名前（8.3 形式）で指定すること。

関連コマンド

CREATE FFILE（159 ページ）

SHOW FFILE（372 ページ）

DELETE FILE

カテゴリー：運用・管理 / 記憶装置とファイルシステム

DELETE FILE=*filename*

filename: ファイル名（ワイルドカード指定可能）

解説

ファイルを削除する。

パラメーター

FILE ファイル名。ワイルドカード（*）も指定可能

例

noneed.cfg を削除する。

```
DELETE FILE=noneed.cfg
```

拡張子が.txt のファイルをすべて削除する。

```
DELETE FILE=*.txt
```

関連コマンド

RENAME (286 ページ)

SHOW FILE (374 ページ)

DELETE INSTALL

カテゴリー：運用・管理 / ソフトウェア

DELETE INSTALL=**{TEMPORARY|PREFERRED|DEFAULT}**

解説

インストール（ファームウェア構成）情報を削除する。

「インストール」には、起動時にロードすべきファームウェアの情報、具体的にはリリースファイルとパッチファイル（オプション）の組み合わせが記録されている。インストールには、TEMPORARY（一度しか使用されないテスト用インストール）、PREFERRED（通常使用するインストール）、DEFAULT（緊急時に使用するインストール。EPROM 上のファームウェアから起動する）がある。

パラメーター

INSTALL 削除するインストールの種類を指定する。DEFAULT インストールの場合は、パッチファイルの情報のみが削除される。

関連コマンド

SET INSTALL (297 ページ)

SHOW INSTALL (384 ページ)

DELETE LOG OUTPUT

カテゴリー：運用・管理 / ログ

DELETE LOG OUTPUT={**TEMPORARY**|**PERMANENT**|*output-id*} **FILTER**={**ALL**|*entry-id*}

output-id: ログ出力 ID (1~20)

entry-id: エントリー番号 (1~)

解説

ログ出力先の定義からメッセージフィルターエントリーを削除する。

パラメーター

OUTPUT ログ出力先 ID。1~20 の任意の番号か、特殊なキーワード「TEMPORARY」(RAM) または「PERMANENT」(NVS) を指定する。

FILTER メッセージフィルターのエントリー番号。ALL を指定した場合は、指定したログ出力定義からすべてのフィルターエントリーが削除される。

例

ログ出力先定義「1」から、メッセージフィルターエントリー「2」を削除する。

```
DELETE LOG OUTPUT=1 FILTER=2
```

ログ出力先定義「2」から、すべてのフィルターエントリーを削除する。

```
DELETE LOG OUTPUT=2 FILTER=ALL
```

関連コマンド

ADD LOG OUTPUT (126 ページ)

SHOW LOG OUTPUT (395 ページ)

DELETE LOG RECEIVE

カテゴリー：運用・管理 / ログ

DELETE LOG RECEIVE={*ipadd*|**ANY**}

ipadd: IP アドレス

解説

ログ受信テーブルからエントリーを削除する。

パラメーター

RECEIVE 削除するホストまたはネットワークの IP アドレスを指定する。ANY と 0.0.0.0 はすべての IP アドレスに対するエントリーを示す。

例

IP アドレス 192.168.1.1 の機器からのログメッセージ受信を停止する。

DELETE LOG RECEIVE=192.168.1.1

関連コマンド

ADD LOG RECEIVE (128 ページ)

SET LOG RECEIVE (305 ページ)

SHOW LOG RECEIVE (400 ページ)

DELETE MAIL

カテゴリー：運用・管理 / メール送信

DELETE MAIL=message-id

message-id: メッセージ番号 (16 進数。0 ~ ffff)

解説

メール送信キュー内のメールを削除する。

パラメーター

MAIL メッセージ番号。SHOW MAIL コマンドで確認可能。

例

メール送信キューから 8c3f 番のメールを削除する。

DELETE MAIL=8c3f

関連コマンド

MAIL (275 ページ)

SET MAIL (308 ページ)

SHOW MAIL (404 ページ)

DELETE NTP PEER

カテゴリー：運用・管理 / NTP

DELETE NTP PEER=*ipadd*

ipadd: IP アドレス

解説

NTP サーバーの IP アドレスを削除する。

パラメーター

PEER NTP サーバーの IP アドレス

関連コマンド

ADD NTP PEER (130 ページ)

DELETE NVS

カテゴリー：運用・管理 / 記憶装置とファイルシステム

DELETE NVS BLOCK=*block-id* INDEX=*index*

block-id: ブロック ID (16 進数)

index: ブロックインデックス (16 進数)

解説

BLOCK と INDEX で指定された NVS ブロックを削除する。

パラメーター

BLOCK ブロック ID

INDEX ブロックインデックス

関連コマンド

CLEAR NVS TOTALLY (156 ページ)

DUMP NVS (238 ページ)

MODIFY NVS (278 ページ)

SHOW NVS (409 ページ)

SHOW NVS FREE (411 ページ)

DELETE RADIUS SERVER

カテゴリー：運用・管理 / 認証サーバー

DELETE RADIUS SERVER=*ipadd*

ipadd: IP アドレス

解説

認証サーバーリストから RADIUS (Remote Authentication Dial In User Server) サーバーを削除する。

パラメーター

SERVER RADIUS サーバーの IP アドレス

例

認証サーバーリストから RADIUS サーバー 192.168.10.5 を削除する。

DELETE RADIUS SERVER=192.168.10.5

関連コマンド

ADD RADIUS SERVER (131 ページ)

SHOW RADIUS (431 ページ)

DELETE SCRIPT

カテゴリー：運用・管理 / スクリプト

DELETE SCRIPT=filename [LINE=line-num]

filename: ファイル名（拡張子は.scp か.cfg）

line-num: 行番号（1～）

解説

スクリプトファイルから指定行を削除する。あるいは、スクリプトファイルそのものを削除する。
LINE を指定したときは指定行のみ、ファイル名しか指定しなかったときはファイルそのものが削除される。

パラメーター

SCRIPT スクリプトファイル名

LINE 削除する行の行番号。指定時は指定行のみが削除される。省略時はファイルそのものが削除される。

例

basic.cfg の 5 行目を削除する。

```
DELETE SCRIPT=basic.cfg LINE=5
```

advanced.cfg を削除する。

```
DELETE SCRIPT=advanced.cfg
```

関連コマンド

ACTIVATE SCRIPT (120 ページ)

ADD SCRIPT (133 ページ)

DEACTIVATE SCRIPT (186 ページ)

DELETE FILE (189 ページ)

SET SCRIPT (323 ページ)

SHOW SCRIPT (434 ページ)

DELETE SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

```
DELETE SNMP COMMUNITY=community [MANAGER=ipadd[/masklen]]  
[TRAPHOST=ipadd] [V1TRAPHOST=ipadd] [V2CTRAPHOST=ipadd]
```

community: SNMP コミュニティー名 (1～15 文字。大文字小文字を区別する)

ipadd: IP アドレス

masklen: マスク長 (0～32)

解説

(SNMPv1/v2c) SNMP コミュニティーから管理ステーション、トラップホストを削除する。

パラメーター

COMMUNITY SNMP コミュニティー名

MANAGER SNMP オペレーションを許可する管理ステーションを指定する。マスク長を付加することで範囲指定も可能。本製品は、MANAGER に登録されていないホストからの SNMP 要求には応答しない。ただし、SNMP コミュニティーの OPEN パラメーターが YES の場合は、MANAGER パラメーターの設定にかかわらず、すべての SNMP 要求に応答する。

TRAPHOST SNMPv1 トラップの送信先ホスト

V1TRAPHOST SNMPv1 トラップの送信先ホスト。TRAPHOST パラメーターと同じ。

V2CTRAPHOST SNMPv2c トラップの送信先ホスト

関連コマンド

ADD SNMP COMMUNITY (134 ページ)

CREATE SNMP COMMUNITY (167 ページ)

DESTROY SNMP COMMUNITY (210 ページ)

DISABLE SNMP COMMUNITY (226 ページ)

ENABLE SNMP COMMUNITY (259 ページ)

SET SNMP COMMUNITY (325 ページ)

SHOW SNMP COMMUNITY (441 ページ)

DELETE SNMP GROUP

カテゴリー：運用・管理 / SNMP

DELETE SNMP GROUP=*group* **SECURITYLEVEL={noAuthNoPriv|authNoPriv|authPriv}**

group: SNMP グループ名 (1～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ユーザーグループを削除する。

パラメーター

GROUP SNMP グループ名

SECURITYLEVEL セキュリティーレベル。ADD SNMP GROUP コマンドで指定したのと同じレベルを指定すること。

関連コマンド

ADD SNMP GROUP (136 ページ)

SET SNMP GROUP (327 ページ)

SHOW SNMP GROUP (443 ページ)

DELETE SNMP TARGETADDR

カテゴリー：運用・管理 / SNMP

DELETE SNMP TARGETADDR=*target*

target: SNMP ターゲット名 (1~32 文字。大文字小文字を区別する)

解説

(SNMPv3) ターゲット (通知メッセージの送信先) を削除する。

パラメーター

TARGETADDR SNMP ターゲット名

関連コマンド

ADD SNMP TARGETADDR (138 ページ)

SET SNMP TARGETADDR (329 ページ)

SHOW SNMP TARGETADDR (445 ページ)

DELETE SNMP TARGETPARAMS

カテゴリー：運用・管理 / SNMP

DELETE SNMP TARGETPARAMS=*params*

params: SNMP ターゲットパラメーターセット名 (1～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ターゲット (通知メッセージの送信先) との通信に使用するパラメーターセット (セキュリティレベルとユーザー名) を削除する。

パラメーター

TARGETPARAMS SNMP ターゲットパラメーターセット名

関連コマンド

ADD SNMP TARGETPARAMS (140 ページ)

SET SNMP TARGETPARAMS (330 ページ)

SHOW SNMP TARGETPARAMS (447 ページ)

DELETE SNMP USER

カテゴリー：運用・管理 / SNMP

DELETE SNMP USER=*username*

username: SNMP ユーザー名 (1～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ユーザーを削除する。

パラメーター

USER SNMP ユーザー名

関連コマンド

ADD SNMP USER (142 ページ)

SET SNMP USER (332 ページ)

SHOW SNMP USER (449 ページ)

DELETE SNMP VIEW

カテゴリー：運用・管理 / SNMP

DELETE SNMP VIEW=view OID=node-oid

DELETE SNMP VIEW=view MIB={node-name|ALL}

view: SNMP ビュー名 (1～32 文字。大文字小文字を区別する)

node-oid: MIB ノード OID (1.3.6.1 のように整数とピリオドで構成された文字列。数字は 32 個まで使用できる)

node-name: MIB ノード名 (既定のノード名。ADD SNMP VIEW コマンドの表を参照)

解説

(SNMPv3) ビューから特定のエントリーを削除する。またはビューそのものを削除する。

パラメーター

VIEW SNMP ビュー名

OID MIB ノードの OID (Object Identifier)。MIB パラメーターとは同時に指定できない。

MIB MIB ノードの名前。指定できる名前と対応する OID は ADD SNMP VIEW コマンドの表を参照。

OID パラメーターとは同時に指定できない。ALL を指定した場合は、ビュー全体が削除される。

例

SNMP ビュー「various」から private ノード (1.3.6.1.4) のエントリーを削除する。

```
DELETE SNMP VIEW=various MIB=private
```

SNMP ビュー「most」を削除する。

```
DELETE SNMP VIEW=most MIB=ALL
```

関連コマンド

ADD SNMP VIEW (144 ページ)

SHOW SNMP VIEW (451 ページ)

DELETE SSH USER

カテゴリー：運用・管理 / Secure Shell

DELETE SSH USER=*username*

username: ユーザー名 (1～15 文字。英数字。空白不可)

解説

SSH ユーザーを削除する。

パラメーター

USER SSH ユーザー名

関連コマンド

ADD SSH USER (147 ページ)

SET SSH USER (334 ページ)

SHOW SSH USER (462 ページ)

DELETE TRIGGER

カテゴリー：運用・管理 / トリガー

DELETE TRIGGER=*trigger-id* **NUMBER=***index*

index: スクリプト番号 (1~5)

trigger-id: トリガー番号 (1~250)

解説

トリガーからスクリプトを削除する。

パラメーター

TRIGGER トリガー番号

NUMBER スクリプト番号。

関連コマンド

ADD TRIGGER (149 ページ)

CREATE TRIGGER CPU (169 ページ)

CREATE TRIGGER FIREWALL (171 ページ)

CREATE TRIGGER INTERFACE (173 ページ)

CREATE TRIGGER MEMORY (175 ページ)

CREATE TRIGGER MODULE (177 ページ)

CREATE TRIGGER PERIODIC (180 ページ)

CREATE TRIGGER REBOOT (182 ページ)

CREATE TRIGGER TIME (184 ページ)

DESTROY TRIGGER (211 ページ)

SET TRIGGER CPU (342 ページ)

SET TRIGGER FIREWALL (344 ページ)

SET TRIGGER INTERFACE (346 ページ)

SET TRIGGER MEMORY (348 ページ)

SET TRIGGER MODULE (350 ページ)

SET TRIGGER PERIODIC (352 ページ)

SET TRIGGER REBOOT (354 ページ)

SET TRIGGER TIME (356 ページ)

SHOW TRIGGER (470 ページ)

DELETE USER

カテゴリー：運用・管理 / ユーザー認証データベース

DELETE USER=*login-name*

login-name: ログイン名 (1~64 文字。英数字のみ使用可能。大文字小文字を区別しない。空白不可)

解説

ユーザー認証データベースからユーザーを削除する。

パラメーター

USER 削除するユーザーのログイン名を指定する。

例

ユーザー fly を削除する。

```
DELETE USER=fly
```

関連コマンド

ADD USER (151 ページ)
DISABLE USER (233 ページ)
ENABLE USER (266 ページ)
PURGE USER (284 ページ)
RESET USER (292 ページ)
SET USER (359 ページ)
SHOW USER (478 ページ)

DELETE USER RSO

カテゴリー：運用・管理 / セキュリティー

DELETE USER RSO IP=*ipadd*

ipadd: IP アドレス

解説

セキュリティーモード時に Security Officer 権限で Telnet ログインできるホストの IP アドレス (RSO アドレス。RSO=Remote Security Officer) を削除する。

セキュリティーモードで動作中は、RSO として登録されたアドレス範囲外からは Security Officer 権限での Telnet ログインができない。

パラメーター

IP RSO アドレスのベースアドレス

関連コマンド

ADD USER RSO (153 ページ)

DISABLE USER RSO (234 ページ)

ENABLE USER RSO (267 ページ)

SHOW USER RSO (482 ページ)

DESTROY LOG OUTPUT

カテゴリー：運用・管理 / ログ

DESTROY LOG OUTPUT=**{TEMPORARY|PERMANENT|*output-id*}**

output-id: ログ出力 ID (1 ~ 20)

解説

ログの出力先定義を削除する。

パラメーター

OUTPUT ログ出力先 ID。1 ~ 20 の任意の番号か、特殊なキーワード「TEMPORARY」(RAM) または「PERMANENT」(NVS) を指定する。

例

ログ出力先定義「1」を削除する。

DESTROY LOG OUTPUT=1

関連コマンド

CREATE LOG OUTPUT (164 ページ)

SHOW LOG OUTPUT (395 ページ)

DESTROY PATCH

カテゴリー：運用・管理 / ソフトウェア

DESTROY PATCH=*filename*

filename: ファイル名

解説

指定したパッチファイルを削除する。

パラメーター

PATCH パッチファイル名

関連コマンド

DELETE FILE (189 ページ)

LOAD (271 ページ)

SHOW PATCH (412 ページ)

DESTROY SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

DESTROY SNMP COMMUNITY=community

community: SNMP コミュニティー名 (1～15 文字。大文字小文字を区別する)

解説

(SNMPv1/v2c) SNMP コミュニティーを削除する。

パラメーター

COMMUNITY SNMP コミュニティー名

関連コマンド

ADD SNMP COMMUNITY (134 ページ)
CREATE SNMP COMMUNITY (167 ページ)
DISABLE SNMP COMMUNITY (226 ページ)
ENABLE SNMP COMMUNITY (259 ページ)
SET SNMP COMMUNITY (325 ページ)
SHOW SNMP COMMUNITY (441 ページ)

DESTROY TRIGGER

カテゴリー：運用・管理 / トリガー

DESTROY TRIGGER=*trigger-id*

trigger-id: トリガー番号 (1~250)

解説

トリガーを削除する。

パラメーター

TRIGGER トリガー番号

関連コマンド

ADD TRIGGER (149 ページ)
CREATE TRIGGER CPU (169 ページ)
CREATE TRIGGER FIREWALL (171 ページ)
CREATE TRIGGER INTERFACE (173 ページ)
CREATE TRIGGER MEMORY (175 ページ)
CREATE TRIGGER MODULE (177 ページ)
CREATE TRIGGER PERIODIC (180 ページ)
CREATE TRIGGER REBOOT (182 ページ)
CREATE TRIGGER TIME (184 ページ)
DELETE TRIGGER (205 ページ)
DISABLE TRIGGER (232 ページ)
ENABLE TRIGGER (265 ページ)
PURGE TRIGGER (283 ページ)
SHOW TRIGGER (470 ページ)

DISABLE FEATURE

カテゴリー：運用・管理 / ソフトウェア

DISABLE FEATURE=**{*featurename*|*index*}**

featurename: フィーチャー名 (1~12 文字)

index: フィーチャー番号 (1~)

解説

フィーチャーライセンスを無効にする。

パラメーター

FEATURE フィーチャー名または SHOW FEATURE コマンドで表示されるフィーチャー番号

関連コマンド

ENABLE FEATURE (242 ページ)

SHOW FEATURE (369 ページ)

DISABLE HTTP SERVER

カテゴリー：運用・管理 / システム

DISABLE HTTP SERVER

解説

HTTP サーバー（サポート対象外）を無効にする。

本製品はデフォルトで HTTP サーバー（サポート対象外）が有効になっているため、IP 有効時は TCP ポート 80 番がオープンしている。セキュリティを重視する場合は、本コマンドを実行して、HTTP サーバーを無効にすること。

関連コマンド

ENABLE HTTP SERVER (243 ページ)

SHOW HTTP SERVER (382 ページ)

DISABLE LOG

カテゴリー：運用・管理 / ログ

DISABLE LOG

解説

ログ機能を無効にする。デフォルトは有効。

関連コマンド

DISABLE LOG GENERATION (215 ページ)

DISABLE LOG OUTPUT (216 ページ)

DISABLE LOG RECEPTION (217 ページ)

ENABLE LOG (244 ページ)

DISABLE LOG GENERATION

カテゴリー：運用・管理 / ログ

DISABLE LOG GENERATION

解説

ログの生成を無効にする。

他のルーターからのログメッセージ受信や受信したメッセージの処理には影響しない。デフォルトは有効。

関連コマンド

DISABLE LOG (214 ページ)

DISABLE LOG OUTPUT (216 ページ)

DISABLE LOG RECEPTION (217 ページ)

ENABLE LOG GENERATION (245 ページ)

DISABLE LOG OUTPUT

カテゴリー：運用・管理 / ログ

DISABLE LOG OUTPUT [= {TEMPORARY|*output-id*}]

output-id: ログ出力 ID (1 ~ 20)

解説

指定した出力先へのログ出力を一時的に無効にする。

パラメーター

OUTPUT 無効にするログ出力先定義を指定する。指定しなかったときは、TEMPORARY を除くすべてのログ出力が無効になる。

関連コマンド

DISABLE LOG (214 ページ)

DISABLE LOG GENERATION (215 ページ)

DISABLE LOG RECEPTION (217 ページ)

ENABLE LOG OUTPUT (246 ページ)

DISABLE LOG RECEPTION

カテゴリー：運用・管理 / ログ

DISABLE LOG RECEPTION

解説

ログの受信機能（syslog、SRLP、Net Manage Message Protocol）を無効にする。
システム内でのログ生成と処理には影響しない。デフォルトは有効。

関連コマンド

DISABLE LOG (214 ページ)

DISABLE LOG GENERATION (215 ページ)

DISABLE LOG OUTPUT (216 ページ)

ENABLE LOG RECEPTION (247 ページ)

DISABLE MAIL DEBUG

カテゴリー：運用・管理 / メール送信

DISABLE MAIL DEBUG

解説

メール送信機能のデバッグを停止する。

関連コマンド

ENABLE MAIL DEBUG (248 ページ)

SHOW MAIL (404 ページ)

DISABLE NTP

カテゴリー：運用・管理 / NTP

DISABLE NTP

解説

NTP モジュールを無効にする。デフォルトは無効。

関連コマンド

ENABLE NTP (249 ページ)

PURGE NTP (280 ページ)

RESET NTP (289 ページ)

DISABLE PORTAUTH

カテゴリー：運用・管理 / ポート認証

DISABLE PORTAUTH [= {8021X|MACBASED}]

解説

ポート認証機能（802.1X 認証または MAC ベース認証）を無効にする。デフォルトはどちらとも無効。

パラメーター

PORTAUTH 認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。
省略時は 8021X と見なされる。

関連コマンド

DISABLE PORTAUTH PORT（222 ページ）

ENABLE PORTAUTH（250 ページ）

ENABLE PORTAUTH PORT（252 ページ）

SHOW PORTAUTH PORT（419 ページ）

SHOW PORTAUTH PORT MULTISUPPLICANT（424 ページ）

DISABLE PORTAUTH DEBUG

カテゴリー：運用・管理 / ポート認証

DISABLE PORTAUTH [= {8021X|MACBASED}] **DEBUG**={ALL|PACKET|STATE}
PORT={eth-port|port-list|ALL}

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

解説

指定ポートで、ポート認証機能 (802.1X 認証または MAC ベース認証) のデバッグを無効にする。デフォルトは全ポート無効。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証) MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

DEBUG デバッグオプション。ALL (すべて) PACKET (パケット送受信) STATE (状態遷移) から選択する。PACKET は、PORTAUTH に 8021X を指定したときだけ有効。

PORT ポート

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH DEBUG (251 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SHOW PORTAUTH PORT (419 ページ)

DISABLE PORTAUTH PORT

カテゴリー：運用・管理 / ポート認証

DISABLE PORTAUTH [= {8021X|MACBASED}] **PORT**={*eth-port*|*port-list*|ALL}

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

解説

指定ポートで、ポート認証機能 (802.1X 認証または MAC ベース認証) を無効にする。デフォルトは全ポート無効。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。
省略時は 8021X と見なされる。

PORT ポート

関連コマンド

DISABLE PORTAUTH (220 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SHOW PORTAUTH PORT (419 ページ)

DISABLE RELEASE

カテゴリー：運用・管理 / ソフトウェア

DISABLE RELEASE=*filename*

filename: ファイル名

解説

指定したリリースファイルに関するライセンスを削除する。

パラメーター

RELEASE リリースファイル名

関連コマンド

ENABLE RELEASE (256 ページ)

SHOW RELEASE (433 ページ)

DISABLE SNMP

カテゴリー：運用・管理 / SNMP

DISABLE SNMP

解説

(SNMPv1/v2c/3) SNMP モジュールを無効にする。デフォルトは無効。

関連コマンド

DISABLE SNMP COMMUNITY (226 ページ)

ENABLE SNMP (257 ページ)

ENABLE SNMP COMMUNITY (259 ページ)

SHOW SNMP (437 ページ)

SHOW SNMP COMMUNITY (441 ページ)

DISABLE SNMP AUTHENTICATE_TRAP

カテゴリー：運用・管理 / SNMP

DISABLE SNMP AUTHENTICATE_TRAP

解説

(SNMPv1/v2c/3) SNMP 認証トラップの生成を無効にする。デフォルトは無効。

関連コマンド

DISABLE SNMP (224 ページ)

ENABLE SNMP (257 ページ)

ENABLE SNMP AUTHENTICATE_TRAP (258 ページ)

SHOW SNMP (437 ページ)

DISABLE SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

DISABLE SNMP COMMUNITY=community

community: SNMP コミュニティー名（1～15 文字。大文字小文字を区別する）

解説

（SNMPv1/v2c）指定した SNMP コミュニティーを一時的に無効にする。

パラメーター

COMMUNITY SNMP コミュニティー名

関連コマンド

DISABLE SNMP（224 ページ）

ENABLE SNMP（257 ページ）

ENABLE SNMP COMMUNITY（259 ページ）

SHOW SNMP（437 ページ）

SHOW SNMP COMMUNITY（441 ページ）

DISABLE SNMP COMMUNITY TRAP

カテゴリー：運用・管理 / SNMP

DISABLE SNMP COMMUNITY=*community* TRAP

community: SNMP コミュニティ名 (1～15 文字。大文字小文字を区別する)

解説

(SNMPv1/v2c) 指定した SNMP コミュニティにおけるトラップの生成を無効にする。デフォルトは無効。

パラメーター

COMMUNITY SNMP コミュニティ名

例

コミュニティ「public」におけるトラップの生成を無効にする。

DISABLE SNMP COMMUNITY=public TRAP

関連コマンド

ENABLE SNMP COMMUNITY TRAP (260 ページ)

DISABLE SSH SERVER

カテゴリー：運用・管理 / Secure Shell

DISABLE SSH SERVER

解説

SSH サーバー機能を無効にする。デフォルトは無効。

備考・注意事項

SSH サーバーを停止すると、ルーター内蔵 Telnet サーバーが有効になる。

関連コマンド

ENABLE SSH SERVER (261 ページ)

SET SSH SERVER (333 ページ)

SHOW SSH (453 ページ)

DISABLE SSH USER

カテゴリー：運用・管理 / Secure Shell

DISABLE SSH USER=*username*

username: ユーザー名 (1～15 文字。英数字。空白不可)

解説

指定した SSH ユーザーを一時的に無効にする。

ADD SSH USER コマンドによる追加直後は有効になっている。ただし、5 回連続してログインに失敗すると自動的に無効状態になる。その場合は、ENABLE SSH USER コマンドで再度有効化するまで、該当ユーザーは SSH によるログインができない。

パラメーター

USER SSH ユーザー名

関連コマンド

ADD SSH USER (147 ページ)

DELETE SSH USER (204 ページ)

ENABLE SSH USER (262 ページ)

SET SSH USER (334 ページ)

SHOW SSH USER (462 ページ)

DISABLE SYSTEM SECURITY_MODE

カテゴリー：運用・管理 / セキュリティー

DISABLE SYSTEM SECURITY_MODE

解説

システムの動作モードをセキュリティーモードからノーマルモードに変更する。
セキュリティーモードでのみ保存可能なファイル（暗号鍵ファイルなど）は、本コマンド実行により削除される。

関連コマンド

ADD USER (151 ページ)

ENABLE SYSTEM SECURITY_MODE (263 ページ)

SET USER (359 ページ)

SHOW SYSTEM (465 ページ)

SHOW USER (478 ページ)

DISABLE TELNET SERVER

カテゴリー：運用・管理 / ターミナルサービス

DISABLE TELNET SERVER

解説

Telnet サーバー機能を無効にする。デフォルトは有効。

関連コマンド

ENABLE TELNET SERVER (264 ページ)

SHOW TELNET (468 ページ)

DISABLE TRIGGER

カテゴリー：運用・管理 / トリガー

DISABLE TRIGGER [=trigger-id]

trigger-id: トリガー番号 (1~250)

解説

トリガー機能を無効にする。あるいは、指定したトリガーを一時的に無効にする。
デフォルトでは、トリガー機能は無効。作成直後のトリガーは、STATE=DISABLED を指定しない限り有効。

パラメーター

TRIGGER トリガー番号。省略時はトリガー機能全体が無効になる。

関連コマンド

ACTIVATE TRIGGER (121 ページ)

DELETE TRIGGER (205 ページ)

DESTROY TRIGGER (211 ページ)

ENABLE TRIGGER (265 ページ)

PURGE TRIGGER (283 ページ)

SHOW TRIGGER (470 ページ)

DISABLE USER

カテゴリー：運用・管理 / ユーザー認証データベース

DISABLE USER=*login-name*

login-name: ログイン名 (1~64 文字。英数字のみ使用可能。大文字小文字を区別しない。空白不可)

解説

指定したユーザーアカウントを一時的に無効にする。

パラメーター

USER ログイン名

関連コマンド

ADD USER (151 ページ)

DELETE USER (206 ページ)

ENABLE USER (266 ページ)

PURGE USER (284 ページ)

RESET USER (292 ページ)

SET USER (359 ページ)

SHOW USER (478 ページ)

DISABLE USER RSO

カテゴリー：運用・管理 / セキュリティー

DISABLE USER RSO

解説

セキュリティーモードにおいて Security Officer ユーザーの Telnet ログインを禁止する。デフォルトは禁止。
本コマンドの実行時に Telnet ログインしていた Security Officer レベルのユーザーは、直ちに Security Officer の権限を失う。

関連コマンド

ADD USER RSO (153 ページ)

DELETE USER RSO (207 ページ)

ENABLE USER RSO (267 ページ)

SHOW USER RSO (482 ページ)

DISCONNECT

カテゴリー：運用・管理 / ターミナルサービス

DISCONNECT 1..5

解説

端末セッションを終了させる。

本コマンドは「D」と省略できる。セッション番号は SHOW SESSIONS コマンドで確認する。

例

端末セッション 2 を終了する。

```
DISCONNECT 2
```

関連コマンド

RECONNECT (285 ページ)

SHOW SESSIONS (436 ページ)

TELNET (486 ページ)

DUMP

カテゴリー：運用・管理 / 記憶装置とファイルシステム

DUMP [ADDRESS=*address*] [LENGTH=*length*] [SIZE={BYTE|WORD|LONG}]
[SPACE={SD|SP|UD|UP|UR}]

address: メモリーアドレス (16 進数)

length: バイト長 (16 進数)

解説

メモリーの内容を 16 進ダンプする。

パラメーター

ADDRESS ダンプ開始アドレス。省略時は前回ダンプした範囲の次のアドレスとなる。また、キーワード ADDRESS だけを指定した場合は、前回と同じアドレスが対象となる。

LENGTH ダンプするバイト数。16 進数で指定する。省略時は前回と同じ値が使用される。

SIZE データを何バイトずつまとめて表示するか。BYTE、WORD、LONG から選択する。省略時は前回と同じ値が使用される。なお、SIZE パラメーターは表示方法を指定するだけであり、ダンプするデータの量を指定する LENGTH パラメーターとは関係がない。LENGTH パラメーターは、SIZE パラメーターの指定にかかわらず、つねにバイト単位で指定する。

SPACE ダンプ対象の CPU アドレス空間。UD(User Data) UP(User Program) UR(User Reserved) SD (Supervisor Data) SP (Supervisor Program) から選択する。

入力・出力・画面例

```
Manager > dump address=0 length=80 size=long
00000000  00021ee4 55551111 55551111 55551111      ....UU..UU..UU..
00000010  55551111 55551111 55551111 55551111      UU..UU..UU..UU..
00000020  55551111 55551111 55551111 55551111      UU..UU..UU..UU..
00000030  55551111 55551111 55551111 55551111      UU..UU..UU..UU..
00000040  55551111 55551111 55551111 55551111      UU..UU..UU..UU..
00000050  55551111 55551111 55551111 55551111      UU..UU..UU..UU..
00000060  55551111 55551111 55551111 55551111      UU..UU..UU..UU..
00000070  55551111 55551111 55551111 55551111      UU..UU..UU..UU..
```

例

FF00 番地から 256 バイトをワード単位でダンプする

DUMP ADDRESS=FF00 LENGTH=FF SIZE=WORD

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

MODIFY (277 ページ)

DUMP NVS

カテゴリー：運用・管理 / 記憶装置とファイルシステム

```
DUMP NVS [BLOCK=block-id] [INDEX=index] [LENGTH=length] [OFFSET=offset]
[SIZE={BYTE|WORD|LONG}]
```

block-id: ブロック ID (16 進数)
index: ブロックインデックス (16 進数)
length: バイト長 (16 進数)
offset: バイトオフセット (16 進数)

解説

NVS ブロックの内容を 16 進ダンプする。
起動後初めて実行するときは、BLOCK、INDEX、LENGTH を指定する必要がある。2 回目以降は、指定しなかったパラメーターについては前回の値が使用される。

パラメーター

BLOCK ブロック ID。SHOW NVS コマンドで確認できる。
INDEX ブロックインデックス。SHOW NVS コマンドで確認できる。
LENGTH ダンプするデータの長さ
OFFSET ダンプ開始位置
SIZE データを何バイトずつまとめて表示するか。BYTE、WORD、LONG から選択する。省略時は前回と同じ値が使用される。なお、SIZE パラメーターは表示方法を指定するだけであり、ダンプするデータの量を指定する LENGTH パラメーターとは関係がない。LENGTH パラメーターは、SIZE パラメーターの指定にかかわらず、つねにバイト単位で指定する。

| | |
|--------|------------------------------|
| ID | ブロック ID |
| Index | ブロックインデックス |
| Offset | ダンプ開始位置のオフセット |
| Length | ダンプデータ長 |
| Size | データ表示単位。BYTE、LONG、WORD のいずれか |
| Offset | 該当行のオフセット |
| Data | データ (16 進表示) |
| ASCII | データ (ASCII 表示) |

表 33:

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

CLEAR NVS TOTALLY (156 ページ)

DELETE NVS (195 ページ)

MODIFY NVS (278 ページ)

SHOW NVS (409 ページ)

SHOW NVS FREE (411 ページ)

EDIT

カテゴリー：運用・管理 / システム

EDIT [*filename*]

filename: ファイル名

解説

内蔵フルスクリーンエディターを起動する。

変更内容を破棄して終了は Ctrl/C、保存して終了は Ctrl/K, Ctrl/X。詳細なキーバインドは別表を参照のこと。

| 凡例 | |
|----------------------|--|
| Ctrl/ | 「Ctrl」キーを押しながら キーを押す。たとえば「Ctrl/E」は、「Ctrl」キーを押しながら「E」キーを押すことを意味する |
| Ctrl/ , Ctrl/ | 「Ctrl/」, 「Ctrl/」の順に押す。「Ctrl」キーは押したままでもかまわない。たとえば「Ctrl/K, Ctrl/X」は、「Ctrl/K」, 「Ctrl/X」の順に押すことを意味する |
| カーソル移動 | |
| または Ctrl/Z | 1 行上に移動 |
| または Ctrl/X | 1 行下に移動 |
| | 1 文字右に移動 |
| | 1 文字左に移動 |
| Ctrl/B | ファイル先頭に移動 |
| Ctrl/D | ファイルの末尾に移動 (Telnet ログイン時に Ctrl/D を押すとセッションが終了させられてしまうので注意) |
| Ctrl/A | 行頭に移動 |
| Ctrl/E | 行末に移動 |
| Ctrl/U | 1 画面上に移動 |
| Ctrl/V | 1 画面下に移動 |
| Ctrl/F | 1 単語右に移動 |
| 削除 | |
| Delete または Backspace | カーソルの左にある文字を削除 |
| Ctrl/Y | 現在行を削除 |
| Ctrl/T | 1 単語削除 |
| ブロック編集 | |
| Ctrl/K, Ctrl/B | ブロックマークを開始 |
| Ctrl/K, Ctrl/D | ブロックマークを終了 |

| | |
|----------------|-------------------|
| Ctrl/K, Ctrl/U | ブロックをカット（切り取り） |
| Ctrl/K, Ctrl/C | ブロックをコピー |
| Ctrl/K, Ctrl/Y | ブロックを消去 |
| Ctrl/K, Ctrl/V | カーソル位置にペースト（貼り付け） |
| 検索 | |
| Ctrl/K, Ctrl/F | 検索 |
| Ctrl/L | 次を検索 |
| 保存・終了 | |
| Ctrl/K, Ctrl/X | 変更を保存して終了 |
| Ctrl/C | 変更を破棄して終了 |
| 入力モード切り替え | |
| Ctrl/I | 挿入モード（デフォルト） |
| Ctrl/O | 上書きモード |
| その他 | |
| Ctrl/W | 画面を再描画 |
| Ctrl/K, Ctrl/H | エディターのオンラインヘルプを表示 |
| Ctrl/K, Ctrl/O | ファイルを開く |

表 34: Edit コマンドのキーバインド

例

設定スクリプトファイル BASIC.CFG を編集する。

```
EDIT BASIC.CFG
```

備考・注意事項

日本語 Windows 付属のハイパーターミナルでは矢印キーが使えない。

関連コマンド

DELETE FILE (189 ページ)

LOAD (271 ページ)

SHOW FILE (374 ページ)

ENABLE FEATURE

カテゴリー：運用・管理 / ソフトウェア

ENABLE FEATURE=featurename PASSWORD=password

featurename: フィーチャー名 (1～12 文字)

password: パスワード (16 進数。最小 16 文字)

解説

フィーチャーライセンスを有効にする。

パラメーター

FEATURE フィーチャー名

PASSWORD フィーチャーライセンスのパスワード

関連コマンド

DISABLE FEATURE (212 ページ)

SHOW FEATURE (369 ページ)

ENABLE HTTP SERVER

カテゴリー：運用・管理 / システム

備考：本機能はサポート対象外です

ENABLE HTTP SERVER

解説

HTTP サーバー（サポート対象外）を有効にする。

本製品はデフォルトで HTTP サーバー（サポート対象外）が有効になっているため、IP 有効時は TCP ポート 80 番がオープンしている。セキュリティを重視する場合は、DISABLE HTTP SERVER コマンドを実行して、HTTP サーバーを無効にすること。

関連コマンド

DISABLE HTTP SERVER (213 ページ)

SHOW HTTP SERVER (382 ページ)

ENABLE LOG

カテゴリー：運用・管理 / ログ

ENABLE LOG

解説

ログ機能を有効にする。デフォルトは有効。

関連コマンド

DISABLE LOG (214 ページ)

ENABLE LOG GENERATION (245 ページ)

ENABLE LOG OUTPUT (246 ページ)

ENABLE LOG RECEPTION (247 ページ)

ENABLE LOG GENERATION

カテゴリー：運用・管理 / ログ

ENABLE LOG GENERATION

解説

ログの生成を有効にする。デフォルトは有効。

関連コマンド

DISABLE LOG GENERATION (215 ページ)

ENABLE LOG (244 ページ)

ENABLE LOG OUTPUT (246 ページ)

ENABLE LOG RECEPTION (247 ページ)

ENABLE LOG OUTPUT

カテゴリー：運用・管理 / ログ

ENABLE LOG OUTPUT [= {TEMPORARY | *output-id*}]

output-id: ログ出力 ID (1 ~ 20)

解説

指定した出力先へのログ出力を再度有効にする。

パラメーター

OUTPUT 有効にするログ出力先定義を指定する。指定しなかったときは、TEMPORARY を除くすべてのログ出力が有効になる。

関連コマンド

DISABLE LOG OUTPUT (216 ページ)

ENABLE LOG (244 ページ)

ENABLE LOG GENERATION (245 ページ)

ENABLE LOG RECEPTION (247 ページ)

ENABLE LOG RECEPTION

カテゴリー：運用・管理 / ログ

ENABLE LOG RECEPTION

解説

ログの受信機能（syslog、SRLP、Net Manage Message Protocol）を有効にする。デフォルトは有効。

関連コマンド

DISABLE LOG RECEPTION（217 ページ）

ENABLE LOG（244 ページ）

ENABLE LOG GENERATION（245 ページ）

ENABLE LOG OUTPUT（246 ページ）

ENABLE MAIL DEBUG

カテゴリー：運用・管理 / メール送信

ENABLE MAIL DEBUG

解説

メール送信機能のデバッグを有効にする。

有効時には、メールの送信過程がコマンドを実行した端末に逐一表示される。デフォルトは無効。

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

DISABLE MAIL DEBUG (218 ページ)

SHOW MAIL (404 ページ)

ENABLE NTP

カテゴリー：運用・管理 / NTP

ENABLE NTP

解説

NTP モジュールを有効にする。デフォルトは無効。

関連コマンド

DISABLE NTP (219 ページ)

PURGE NTP (280 ページ)

RESET NTP (289 ページ)

ENABLE PORTAUTH

カテゴリー：運用・管理 / ポート認証

ENABLE PORTAUTH [= {8021X|MACBASED}]

解説

ポート認証機能（802.1X 認証または MAC ベース認証）を有効にする。デフォルトはどちらも無効。
ポート認証を使用するためには、個々のスイッチポートでもポート認証機能を有効にする必要がある
（ENABLE PORTAUTH PORT コマンド）。

パラメーター

PORTAUTH 認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。
省略時は 8021X と見なされる。

関連コマンド

DISABLE PORTAUTH（220 ページ）
DISABLE PORTAUTH PORT（222 ページ）
ENABLE PORTAUTH PORT（252 ページ）
SHOW PORTAUTH PORT（419 ページ）
SHOW PORTAUTH PORT MULTISUPPLICANT（424 ページ）

ENABLE PORTAUTH DEBUG

カテゴリー：運用・管理 / ポート認証

ENABLE PORTAUTH [= {8021X|MACBASED}] **DEBUG**={ALL|PACKET|STATE}
PORT={eth-port|port-list|ALL}

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

解説

指定ポートで、ポート認証機能 (802.1X 認証または MAC ベース認証) のデバッグを有効にする。デフォルトは全ポート無効。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証) MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

DEBUG デバッグオプション。ALL (すべて) PACKET (パケット送受信) STATE (状態遷移) から選択する。PACKET は、PORTAUTH に 8021X を指定したときだけ有効。

PORT ポート

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

DISABLE PORTAUTH DEBUG (221 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SHOW PORTAUTH PORT (419 ページ)

ENABLE PORTAUTH PORT

カテゴリー：運用・管理 / ポート認証

```
ENABLE PORTAUTH[=8021X] PORT={eth-port|port-list|ALL} TYPE=AUTHENTICATOR
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [MAXREQ=1..10] [MODE={MULTI|
SINGLE}] [PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=0..65535]
[REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=1..10] [REAUTHPERIOD=1..86400]
[SERVERTIMEOUT=1..60] [SUPPTIMEOUT=1..60] [TXPERIOD=1..65535]
[GUESTVLAN={vlanname|1..4085|NONE}] [SECUREVLAN={ON|OFF}]
[VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}]
```

```
ENABLE PORTAUTH[=8021X] PORT={eth-port|port-list|ALL} TYPE=BOTH
[CONTROL={AUTHORISED|UNAUTHORISED|AUTO}] [MAXREQ=1..10] [MODE=SINGLE]
[PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|
FALSE}] [REAUTHMAX=1..10] [REAUTHPERIOD=1..86400] [SERVERTIMEOUT=1..60]
[SUPPTIMEOUT=1..60] [TXPERIOD=1..65535] [GUESTVLAN={vlanname|1..4085|
NONE}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}] [AUTHPERIOD=1..60]
[HELDPERIOD=0..65535] [MAXSTART=1..10] [STARTPERIOD=1..60]
[USERNAME=login-name PASSWORD=password [METHOD={OTP [ENCRYPTION={MD4|
MD5}}]|STANDARD}]]
```

```
ENABLE PORTAUTH[=8021X] PORT={eth-port|port-list|ALL} TYPE=SUPPLICANT
[AUTHPERIOD=1..60] [HELDPERIOD=0..65535] [MAXSTART=1..10]
[STARTPERIOD=1..60] [USERNAME=login-name PASSWORD=password [METHOD={OTP
[ENCRYPTION={MD4|MD5}}]|STANDARD}]]
```

```
ENABLE PORTAUTH=MACBASED PORT={eth-port|ALL} [CONTROL={AUTHORISED|AUTO|
UNAUTHORISED}] [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|FALSE}]
[REAUTHPERIOD=1..86400] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|
DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|
NONE}]
```

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

vlanname: VLAN 名 (1~32 文字。英数字とアンダースコア (_) ハイフンを使用可能。大文字小文字を区別しない)

login-name: ログイン名 (1~64 文字。英数字のみ使用可能)

password: パスワード (1~64 文字。英数字のみ使用可能)

解説

指定ポートで、ポート認証機能(802.1X 認証または MAC ベース認証)を有効にする。各ポートでは、802.1X 認証か MAC ベース認証のどちらか一方だけを使用できる。また、802.1X 認証を使用する場合は、各ポートを Authenticator、Supplicant、Authenticator かつ Supplicant (Both) のいずれかに設定できる。デフォルトは全ポート無効。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証) MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

PORT ポート

TYPE (802.1X ポート)802.1X 認証におけるスイッチポートの役割。AUTHENTICATOR(Authenticator ポート) SUPPLICANT (Supplicant ポート) BOTH (Authenticator ポートかつ Supplicant ポート) のいずれかを指定する。なお、Multi-Supplicant モード (MODE=MULTI) を使用する場合、TYPE=BOTH は指定できない。TYPE=AUTHENTICATOR を指定すること。

CONTROL (802.1X Authenticator ポート、MAC ベース認証ポート) 手動設定による Authenticator ポートの状態。AUTO(認証結果に応じて変動) UNAUTHORISED(未認証固定) AUTHORISED (認証済み固定) から選択する。デフォルトは AUTO。通常は AUTO のままでよい。ただし、RADIUS サーバーの接続先ポートを Authenticator に設定している場合は、本パラメーターを AUTHORISED に設定する必要がある。

MAXREQ (802.1X Authenticator ポート) Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

MODE (802.1X Authenticator ポート) Authenticator ポートのモード。Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード (MODE=SINGLE) と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード (MODE=MULTI) がある。Single-Supplicant モードでは、該当ポート配下に最初に接続された Supplicant だけが認証対象となる (その他の Supplicant からの通信を許可するかどうかは、PIGGYBACK パラメーターで制御可能)。Multi-Supplicant モードでは、該当ポート配下に接続された個々の Supplicant を識別し、個別に認証を行う。なお、Multi-Supplicant モードを使用する場合、TYPE パラメーターには BOTH を指定できない。AUTHENTICATOR を指定すること。デフォルトは SINGLE。

PIGGYBACK (802.1X Single-Supplicant Authenticator ポート) Single-Supplicant モード (MODE=SINGLE) において、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうかを指定する。TRUE なら許可、FALSE なら拒否。ETH ポートのみ FALSE に設定可能。デフォルトは TRUE。

QUIETPERIOD (802.1X Authenticator ポート、MAC ベース認証ポート) Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間 (秒)。この期間中は受信したパケットをすべて破棄する。デフォルトは 60 秒。

REAUTHENABLED (802.1X Authenticator ポート、MAC ベース認証ポート) 認証に成功した Supplicant を定期的に再認証するかどうか。TRUE なら再認証する、FALSE なら再認証しない。デフォルトは FALSE。

REAUTHMAX (802.1X Authenticator ポート) 再認証時における EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

REAUTHPERIOD (802.1X Authenticator ポート、MAC ベース認証ポート) Supplicant の再認証間

隔 (秒)。デフォルトは 3600 秒。

SERVERTIMEOUT (802.1X Authenticator ポート) RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間 (秒)。デフォルトは 30 秒。

SUPPTIMEOUT (802.1X Authenticator ポート) Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒)。デフォルトは 30 秒。

TXPERIOD (802.1X Authenticator ポート) Supplicant に EAPOL パケットを再送信する間隔 (秒)。デフォルトは 30 秒。

GUESTVLAN (802.1X Single-Supplicant Authenticator ポート) ゲスト VLAN を指定する。装置上に設定されている VLAN の名前か VLAN ID を指定すること。NONE はゲスト VLAN を使用しないことを意味する。EAPOL パケットをまだ受信していないとき、該当ポートはゲスト VLAN の所属となる。最初の EAPOL パケットを受信すると、該当ポートはゲスト VLAN から削除され、本来の所属 VLAN に復帰する。本パラメーターは、Single-Supplicant モード (MODE=SINGLE) でのみ有効。デフォルトは NONE。

SECUREVLAN (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、有効な VLAN でありさえすれば認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。デフォルトは ON。

VLANASSIGNMENT (802.1X Authenticator ポート、MAC ベース認証ポート) ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。デフォルトは ENABLED。

MIBRESET (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証を使用しているポートにおいて、古い Supplicant 情報をエージアウトするかどうか。デフォルトは ENABLED。

TRAP (802.1X Authenticator ポート、MAC ベース認証ポート) ポート認証機能に関する SNMP トラップを送信するかどうか。SUCCESS を指定した場合は、Supplicant の認証に成功したときと、認証情報が時間切れになったときに SNMP トラップを送信する。FAILURE を指定した場合は、Supplicant の認証に失敗したときに SNMP トラップを送信する。BOTH を指定したときは、SUCCESS と FAILURE の両方の場合に SNMP トラップを送信する。NONE はトラップを送信しない。デフォルトは NONE。

AUTHPERIOD (802.1X Supplicant ポート) Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間 (秒)。デフォルトは 30 秒。

HELDPERIOD (802.1X Supplicant ポート) 認証失敗後、Authenticator との通信を試みない期間 (秒)。デフォルトは 60 秒。

MAXSTART (802.1X Supplicant ポート) EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、Authenticator が存在しておらずポート認証の必要はないと判断する。デフォルトは 3 回。

STARTPERIOD (802.1X Supplicant ポート) Authenticator に EAPOL-Start パケットを再送信する間隔 (秒)。デフォルトは 30 秒。

USERNAME (802.1X Supplicant ポート) 指定スイッチポートが Supplicant として動作する場合に使うユーザー名。必ず PASSWORD パラメーターと組で指定すること。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

PASSWORD (802.1X Supplicant ポート) 指定スイッチポートが Supplicant として動作する場合に使うパスワード。必ず USERNAME パラメーターと組で指定すること。METHOD パラメーターに STANDARD を指定した場合、または、METHOD パラメーターを省略した場合は、6～63 文字の文字列を指定する。METHOD パラメーターに OTP を指定した場合は、10～63 文字の文字列（認証サーバー上で設定した OTP Initialisation Password と同じ値）を指定する。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

METHOD (802.1X Supplicant ポート) パスワード送信時の暗号化方式。STANDARD (EAP-MD5) または OTP (One-Time Password) から選択する。OTP を指定した場合は、ENCRYPTION パラメーターでワンタイムパスワードの生成アルゴリズムも指定する必要がある。デフォルトは STANDARD。

ENCRYPTION (802.1X Supplicant ポート) ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

備考・注意事項

802.1X 認証を有効にした Authenticator ポートをタグ付きに設定することはできない。

Multi-Supplicant モード (MODE=MULTI) は 802.1X 規格に準拠しておらず、セキュリティ上のリスクがあるため、通常は Single-Supplicant モード (MODE=SINGLE) のまま使用すること。

802.1X 認証の Multi-Supplicant モードおよび MAC ベース認証は、ETH インターフェースでのみサポート。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (118 ページ)

ENABLE PORTAUTH (250 ページ)

SET PORTAUTH PORT (313 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (317 ページ)

SHOW PORTAUTH (413 ページ)

SHOW PORTAUTH COUNTER (416 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

SHOW PORTAUTH TIMER (428 ページ)

ENABLE RELEASE

カテゴリー：運用・管理 / ソフトウェア

ENABLE RELEASE=filename NUMBER=release-number [PASSWORD=password]

filename: ファイル名

release-number: リリース番号 (x.y の形式。x は major バージョン。y は 65536 × interim バージョン+minor バージョン)

password: パスワード (16 進数。大文字小文字を区別しない)

解説

ファームウェア (リリースファイル) を有効にする。

パラメーター

RELEASE ファームウェア (リリースファイル) 名。本製品のファームウェアは、55-rrr.rez または 55-rrr.rel の形式となる。rrr は major バージョン、minor バージョン、interim バージョンの数字をつなげたものを示す。なお、mm-rrr の後に「a」「b」「c」のような文字が追加される場合もある。

PASSWORD リリースライセンスパスワード。

NUMBER リリース番号。x.y の形式。x は major バージョン。y は 65536 × interim バージョン+minor バージョンで求められる。たとえば、バージョン 2.9.1 ならば、x=2、y=65545 (65536 × 1 + 9) で、NUMBER=2.65545 となる。

関連コマンド

DISABLE RELEASE (223 ページ)

SHOW RELEASE (433 ページ)

ENABLE SNMP

カテゴリー：運用・管理 / SNMP

ENABLE SNMP

解説

(SNMPv1/v2c/3) SNMP モジュールを有効にする。デフォルトは無効。

関連コマンド

DISABLE SNMP (224 ページ)

DISABLE SNMP COMMUNITY (226 ページ)

ENABLE SNMP COMMUNITY (259 ページ)

SHOW SNMP (437 ページ)

SHOW SNMP COMMUNITY (441 ページ)

ENABLE SNMP AUTHENTICATE_TRAP

カテゴリー：運用・管理 / SNMP

ENABLE SNMP AUTHENTICATE_TRAP

解説

(SNMPv1/v2c/3) SNMP 認証トラップの生成を有効にする。デフォルトは無効。

備考・注意事項

実際にトラップが送信されるようにするには、トラップ送信先ホストの設定 (ADD SNMP COMMUNITY TRAPHOST=ipadd \) および、トラップの有効化 (ENABLE SNMP COMMUNITY TRAP) が必要

関連コマンド

DISABLE SNMP (224 ページ)

DISABLE SNMP AUTHENTICATE_TRAP (225 ページ)

ENABLE SNMP (257 ページ)

SHOW SNMP (437 ページ)

ENABLE SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

ENABLE SNMP COMMUNITY=community

community: SNMP コミュニティー名（1～15 文字。大文字小文字を区別する）

解説

（SNMPv1/v2c）無効状態の SNMP コミュニティーを有効にする。

パラメーター

COMMUNITY SNMP コミュニティー名

関連コマンド

DISABLE SNMP（224 ページ）

DISABLE SNMP COMMUNITY（226 ページ）

ENABLE SNMP（257 ページ）

SHOW SNMP（437 ページ）

SHOW SNMP COMMUNITY（441 ページ）

ENABLE SNMP COMMUNITY TRAP

カテゴリー：運用・管理 / SNMP

ENABLE SNMP COMMUNITY=community TRAP

community: SNMP コミュニティー名 (1～15 文字。大文字小文字を区別する)

解説

(SNMPv1/v2c) 指定した SNMP コミュニティーにおける SNMP トラップの生成を有効にする。デフォルトは無効。

トラップはコミュニティのトラップホスト (TRAPHOST) に送信される。

パラメーター

COMMUNITY SNMP コミュニティー名

例

コミュニティ「public」でトラップの生成を有効にする。

```
ENABLE SNMP COMMUNITY=public TRAP
```

備考・注意事項

トラップホストを設定しても、本コマンドを実行しないとトラップが送信されないので注意が必要。

インターフェースリンクトラップはデフォルトでオフになっている。オンにするには、ENABLE INTERFACE LINKTRAP コマンドを実行する。

SNMP トラップの送信を有効にしている場合、RESTART コマンド実行時は、REBOOT オプション (ハードウェアリセット) SWITCH オプション (ソフトウェアリセット) のどちらを指定した場合でも coldStart トラップが送信される。warmStart トラップは、RESET IP コマンドを実行したときに送信される。

関連コマンド

DISABLE SNMP COMMUNITY TRAP (227 ページ)

ENABLE INTERFACE LINKTRAP (「インターフェース」の 32 ページ)

ENABLE SSH SERVER

カテゴリー：運用・管理 / Secure Shell

ENABLE SSH SERVER HOSTKEY=*key-id* SERVERKEY=*key-id* [EXPIRYTIME=*hours*]
 [LOGINTIMEOUT=*seconds*]

key-id: 鍵番号 (0 ~ 65535)

hours: 時間

seconds: 時間 (秒)

解説

SSH サーバー機能を有効にする。デフォルトは無効。

SSH サーバー起動時には、ホスト鍵 (Host Key) とサーバー鍵 (Server Key) という 2 つの RSA 公開鍵ペアを指定する必要がある。これらの鍵は CREATE ENCO KEY であらかじめ作成しておく。

パラメーター

HOSTKEY ホスト鍵の鍵番号を指定する。推奨鍵長は 1024 ビット。CREATE ENCO KEY コマンドで作成する (TYPE=RSA)。

SERVERKEY サーバー鍵の鍵番号を指定する。鍵長はホスト鍵より 128 ビット以上短く、なおかつ 512 ビット以上でなくてはならない。CREATE ENCO KEY コマンドで作成する (TYPE=RSA)。

EXPIRYTIME サーバー鍵の有効期間 (時間)。サーバー鍵は、有効期間が過ぎると自動的に更新 (再生成) される。0 は無期限 (自動更新しない) を示す。デフォルトは 0。

LOGINTIMEOUT ログインタイムアウト (秒)。接続確立後、ここで指定した時間内にログインしなかった場合はサーバー側からコネクションを切断する。デフォルトは 60 秒。

備考・注意事項

SSH サーバーを起動すると、ルーター内蔵 Telnet サーバーへのアクセスはできなくなる (TCP ポートが閉じられる)。

関連コマンド

DISABLE SSH SERVER (228 ページ)

SET SSH SERVER (333 ページ)

SHOW SSH (453 ページ)

ENABLE SSH USER

カテゴリー：運用・管理 / Secure Shell

ENABLE SSH USER=*username*

username: ユーザー名 (1～15 文字。英数字。空白不可)

解説

無効状態の SSH ユーザーを有効にする。

ADD SSH USER コマンドによる追加直後は有効になっている。ただし、5 回連続してログインに失敗すると自動的に無効状態になる。その場合は、本コマンドで再度有効化するまで、該当ユーザーは SSH によるログインができない。

パラメーター

USER SSH ユーザー名

関連コマンド

ADD SSH USER (147 ページ)

DELETE SSH USER (204 ページ)

DISABLE SSH USER (229 ページ)

SET SSH USER (334 ページ)

SHOW SSH USER (462 ページ)

ENABLE SYSTEM SECURITY_MODE

カテゴリー：運用・管理 / セキュリティー

ENABLE SYSTEM SECURITY_MODE

解説

動作モードをノーマルモードからセキュリティーモードに移行する。

セキュリティーモードでは多くのコマンドの実行に Security Officer 権限が必要となる。Security Officer レベルのユーザーが作成されていないと本コマンドは失敗する。

関連コマンド

ADD USER (151 ページ)

DISABLE SYSTEM SECURITY_MODE (230 ページ)

SET USER (359 ページ)

SHOW SYSTEM (465 ページ)

SHOW USER (478 ページ)

ENABLE TELNET SERVER

カテゴリー：運用・管理 / ターミナルサービス

ENABLE TELNET SERVER

解説

Telnet サーバー機能を有効にする。デフォルトは有効。

本製品の Telnet サーバーは、IPv6 が有効であれば IPv6 経由での接続も受け入れる。

関連コマンド

DISABLE TELNET SERVER (231 ページ)

SHOW TELNET (468 ページ)

ENABLE TRIGGER

カテゴリー：運用・管理 / トリガー

ENABLE TRIGGER [=trigger-id]

trigger-id: トリガー番号 (1~250)

解説

トリガー機能を有効にする。あるいは、指定したトリガーを有効にする。
デフォルトでは、トリガー機能は無効。作成直後のトリガーは、STATE=DISABLED を指定しない限り有効。

パラメーター

TRIGGER トリガー番号。省略時はトリガー機能全体が無効になる。

関連コマンド

ACTIVATE TRIGGER (121 ページ)
 CREATE TRIGGER CPU (169 ページ)
 CREATE TRIGGER FIREWALL (171 ページ)
 CREATE TRIGGER INTERFACE (173 ページ)
 CREATE TRIGGER MEMORY (175 ページ)
 CREATE TRIGGER MODULE (177 ページ)
 CREATE TRIGGER PERIODIC (180 ページ)
 CREATE TRIGGER REBOOT (182 ページ)
 CREATE TRIGGER TIME (184 ページ)
 DELETE TRIGGER (205 ページ)
 DESTROY TRIGGER (211 ページ)
 DISABLE TRIGGER (232 ページ)
 PURGE TRIGGER (283 ページ)
 SET TRIGGER CPU (342 ページ)
 SET TRIGGER FIREWALL (344 ページ)
 SET TRIGGER INTERFACE (346 ページ)
 SET TRIGGER MEMORY (348 ページ)
 SET TRIGGER MODULE (350 ページ)
 SET TRIGGER PERIODIC (352 ページ)
 SET TRIGGER REBOOT (354 ページ)
 SET TRIGGER TIME (356 ページ)
 SHOW TRIGGER (470 ページ)

ENABLE USER

カテゴリー：運用・管理 / ユーザー認証データベース

ENABLE USER=*login-name*

login-name: ログイン名 (1~64 文字。英数字のみ使用可能。大文字小文字を区別しない。空白不可)

解説

指定したユーザーアカウントを有効にする。

パラメーター

USER ログイン名

関連コマンド

ADD USER (151 ページ)
DELETE USER (206 ページ)
DISABLE USER (233 ページ)
PURGE USER (284 ページ)
RESET USER (292 ページ)
SET USER (359 ページ)
SHOW USER (478 ページ)

ENABLE USER RSO

カテゴリー：運用・管理 / セキュリティー

ENABLE USER RSO

解説

セキュリティモードであっても、Security Officer レベルユーザーの Telnet ログインを許可する。
許可時は、セキュリティモードにおいても、ADD USER RSO コマンドで指定した IP アドレスからに限り、Security Officer レベルのユーザーで Telnet ログインが可能。許可していない場合（デフォルト）セキュリティモードでは Security Officer レベルのユーザーは Telnet ログインができない。

関連コマンド

ADD USER RSO (153 ページ)

DELETE USER RSO (207 ページ)

DISABLE USER RSO (234 ページ)

SHOW USER RSO (482 ページ)

FLUSH LOG OUTPUT

カテゴリー：運用・管理 / ログ

FLUSH LOG OUTPUT [= {TEMPORARY | *output-id*}]

output-id: ログ出力 ID (1 ~ 20)

解説

ログメッセージキューに格納されているメッセージをただちに処理させる。

パラメーター

OUTPUT ログ出力 ID を指定する。TEMPORARY を指定した場合は、メモリー上のログがすべて削除される。それ以外を指定した場合は、指定したログ出力 ID のメッセージがキューからフラッシュされる。無指定の場合は、すべてのメッセージがフラッシュされる。

関連コマンド

PURGE LOG (279 ページ)

HELP

カテゴリー：運用・管理 / システム

HELP [*topic*]

topic: ヘルプトピック

解説

オンラインヘルプを表示する。

使用するヘルプファイルは SET HELP コマンドで変更できる。また、現在使用しているヘルプファイルは SHOW SYSTEM コマンドで確認できる。

例

オンラインヘルプのトップページを見る

```
HELP
```

オンラインヘルプの IP の項目を見る

```
HELP IP
```

関連コマンド

SET HELP (296 ページ)

SHOW SYSTEM (465 ページ)

IF THEN ELSE ENDIF

カテゴリー：運用・管理 / スクリプト

```
IF string1 {EQ|NE} string2 THEN commands [ELSE commands] ENDIF
```

string1: 比較対象文字列 (1 ~ 255 文字)

string2: 比較対象文字列 (1 ~ 255 文字)

commands: コマンド列

解説

2 つの文字列 (*string1*、*string2*) の比較結果に基づき条件分岐を行うための制御構文。本構文は、スクリプト中でのみ使用可能。

演算子 EQ は 2 つの文字列が等しいときに真、NE は 2 つの文字列が等しくないときに真を返す。比較時は大文字小文字が区別されない。

条件式 (*string1* {EQ|NE} *string2*) が真のときは THEN 節 (THEN ~ ENDIF または THEN ~ ELSE) が実行され、その後 ENDIF の次から実行が継続される。

条件式が偽のときは、ELSE 節があれば ELSE 節 (ELSE ~ ENDIF) が実行され、その後 ENDIF の次からスクリプトの実行が継続される。

条件式が偽で、なおかつ ELSE 節がないときは、ただちに ENDIF の次に飛ぶ。

備考・注意事項

スクリプト中でのみ使用可能。

関連コマンド

WAIT (491 ページ)

LOAD

カテゴリー：運用・管理 / アップロード・ダウンロード

```
LOAD [METHOD=TFTP] [SERVER={hostname|ipadd}] [FILE=filename]
      [DESTFILE=destfilename] [DESTINATION={FLASH|NVS}] [DELAY=seconds]
```

```
LOAD [METHOD={HTTP|WEB|WWW}] [SERVER={hostname|ipadd}]
      [SERVPORT={1..65535|DEFAULT}] [FILE=filename] [DESTFILE=destfilename]
      [DESTINATION={FLASH|NVS}] [HTTPPROXY={hostname|ipadd}]
      [PROXYPORT=1..65535] [USERNAME=username] [PASSWORD=password]
      [DELAY=seconds]
```

```
LOAD [METHOD=ZMODEM] [ASYN=asyn-number] [FILE=filename]
      [DESTINATION={FLASH|NVS}] [DELAY=seconds]
```

hostname: ホスト名

ipadd: IP アドレス

filename: ファイル名 (1~100 文字)

destfilename: ファイル名 (28.3 形式)

seconds: 時間 (0~4294967295 秒)

password: パスワード (1~60 文字)

username: ユーザー名 (1~60 文字)

asyn-number: 非同期ポート番号 (0)

解説

ファイルをダウンロードする。TFTP、HTTP、ZMODEM の各プロトコル/サーバーが使用可能。
指定しなかったオプションについては、SET LOADER コマンドで設定したデフォルト値が使用される。

パラメーター

METHOD 転送プロトコル。TFTP、HTTP (WEB、WWW も同じ)、ZMODEM のいずれかを指定する。

SERVER TFTP/Web サーバーのフルドメイン名 (FQDN) または IP アドレス。METHOD に TFTP、HTTP (または WEB、WWW) を指定したときのみ有効。FQDN を指定するには、ADD IP DNS コマンドで DNS サーバーを設定しておく必要がある

SERVPORT Web サーバーの TCP ポート番号。METHOD に HTTP (または WEB、WWW) を指定したときのみ有効。デフォルトは 80

FILE ダウンロード対象ファイル名。サーバー上のフルパスで指定する

DESTFILE ダウンロード後のファイル名

DESTINATION ダウンロードしたファイルの保存先デバイス。NVS (不揮発性メモリー) か FLASH (フラッシュメモリー) を指定する。デフォルトは FLASH

HTTPPROXY HTTP プロキシのフルドメイン名 (FQDN) または IP アドレス。METHOD に HTTP

(または WEB、WWW) を指定したときのみ有効。FQDN を指定するには、ADD IP DNS コマンドで DNS サーバーを設定しておく必要がある

PROXYPORT HTTP プロキシの TCP ポート番号。METHOD に HTTP (または WEB、WWW) を指定したときのみ有効。HTTPPROXY を指定している場合のみ有効。省略時は 80

DELAY コマンド投入からダウンロード開始までの時間 (秒)

USERNAME HTTP Basic 認証用のユーザー名。METHOD に HTTP (または WEB、WWW) を指定したときのみ有効

PASSWORD HTTP Basic 認証用のパスワード。METHOD に HTTP (または WEB、WWW) を指定したときのみ有効

ASYN 非同期ポート番号。METHOD に ZMODEM を指定したときのみ有効

例

TFTP サーバー 192.168.10.103 からファイル「basic.cfg」をダウンロードする。

```
LOAD METHOD=TFTP SERVER=192.168.10.103 FILE=basic.cfg
```

Web サーバー「www.example.com」上のファイル「example-0001.cfg」を HTTP でダウンロードし、ex0001.cfg という名前で保存する。ダウンロード対象ファイルを一般的な URL で表記すると、「http://www.example.com/confdir/example-0001.cfg」になる。

```
ADD IP DNS PRIMARY=192.168.10.5
```

```
LOAD METHOD=HTTP SERVER=www.example.com FILE=/confdir/example-0001.cfg
  DESTFILE=ex0001.cfg
```

備考・注意事項

HTTP プロキシを利用する場合、HTTPPROXY と PROXYPORT は SET LOADER コマンドでデフォルト値として設定するのがよい。

関連コマンド

SET LOADER (298 ページ)

SHOW LOADER (386 ページ)

UPLOAD (489 ページ)

LOGIN

カテゴリー：運用・管理 / システム

LOGIN [*login-name*]

login-name: ログイン名 (1~64 文字。英数字のみ使用可能。大文字小文字を区別しない。空白不可)

解説

指定ユーザーの権限でログインしなおす。

login-name を指定したときは、いったんログアウトし、ログインプロンプト (login:) で *login-name* を入力した直後の状態になる (パスワード入力待ちになる)。ログイン名を指定しなかった場合は、ログインプロンプトに戻るだけで、事実上 LOGOFF コマンドと同じ。LOGON も同義

備考・注意事項

本コマンドを実行すると、現在のログインセッションがいったん終了させられることに注意。すなわち、Telnet 接続時に本コマンドを実行すると、Telnet セッション自体が切断されてしまう。

関連コマンド

LOGOFF (274 ページ)

LOGOFF

カテゴリー：運用・管理 / システム

LOGOFF

解説

ログインセッションからログアウトする。LOGOUT も同義

関連コマンド

LOGIN (273 ページ)

MAIL

カテゴリー：運用・管理 / メール送信

MAIL TO=*email-addr* {**FILE=***filename*|**MESSAGE=***string*} [**SUBJECT=***string*]
 [ETRN=*domain-name*]

email-addr: 電子メールアドレス

filename: ファイル名

domain-name: ドメイン名

string: 文字列 (1~131 文字)

解説

指定アドレスに電子メールを送る。

事前に SET MAIL コマンドで自ホスト名を設定しておく必要がある。

パラメーター

TO 宛先メールアドレス。user@domain.xxx の形式か user@[192.168.100.5] の形式で指定する。前者の場合は DNS サーバーの設定も必要 (ADD IP DNS コマンド)。後者の IP アドレスは宛先ドメインのメールエクスチェンジャー (MX)。

FILE テキストファイル名。メール本文として送信される。MESSAGE と同時に指定することはできない。

MESSAGE メール本文の文字列。FILE と同時に指定することはできない。

SUBJECT メールのタイトル

ETRN TO で指定したメールサーバーに対し、ETRN で指定したドメイン宛のメールをすべてキューから送出するよう要求する。

例

admin@mydomain.xxx にメールを送る。

```
MAIL TO=admin@mydomain.xxx SUBJECT="test" MESSAGE="This is a test."
```

備考・注意事項

user@domain.xxx の形式でアドレスを指定した場合は、DNS を使って宛先ドメイン (domain.xxx) の MX レコードを検索し、メールエクスチェンジャーに直接メールを送信する。そのため、宛先ドメインの MX レコードを引けない環境ではメールを送ることができない。ただし、その場合でもメールエクスチェンジャーの IP アドレスがわかっているならば、user@[ipaddress] の形式でアドレスを指定することにより送信可能。

関連コマンド

DELETE MAIL (193 ページ)

SET MAIL (308 ページ)

SHOW MAIL (404 ページ)

MODIFY

カテゴリー：運用・管理 / 記憶装置とファイルシステム

MODIFY ADDRESS=address SIZE={BYTE|LONG|WORD} VALUE={value-list|string}
 [SPACE={SD|SP|UD|UP|UR}]

address: メモリーアドレス (16 進数)

value-list: バイト列 (16 進数。指定単位ごとにカンマで区切る。最大 5 バイト)

string: 文字列 (ダブルクォートで囲む。1～12 文字)

解説

メモリーの内容を変更する。

パラメーター

ADDRESS ベースアドレス

SIZE 値の大きさ。BYTE、WORD、LONG から選択。

VALUE 変更後のデータ。SIZE で指定した単位ごとにカンマで区切った 16 進数列 (最大 5 バイト。例: VALUE=12,4ac,0,14e,65) か、ダブルクォートで囲んだ文字列 (最大 12 文字。例: VALUE="string") で指定する。

SPACE CPU アドレス空間。UD (User Data) \ UR (User Program) \ UR (User Reserved) \ SD (Supervisor Data) \ SP (Supervisor Program) が指定可能。省略時は SD。

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

DUMP (236 ページ)

MODIFY NVS

カテゴリー：運用・管理 / 記憶装置とファイルシステム

MODIFY NVS **BLOCK=***block-id* **INDEX=***index* **OFFSET=***offset* **SIZE={**BYTE|LONG|WORD**}** **VALUES=***value-list*

block-id: ブロック ID (16 進数)

index: ブロックインデックス (16 進数)

offset: バイトオフセット (16 進数)

value-list: バイト列 (16 進数。指定単位ごとにカンマで区切る)

解説

BLOCK と INDEX で指定された NVS ブロックの内容を変更する。

パラメーター

BLOCK ブロック ID

INDEX ブロックインデックス

OFFSET ブロック先頭からのオフセット

SIZE 書き込むサイズ

VALUES 書き込む値。16 進数をカンマ区切りで並べる (例: VALUES=fe,a2)。

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

CLEAR NVS TOTALLY (156 ページ)

DELETE NVS (195 ページ)

DUMP NVS (238 ページ)

SHOW NVS (409 ページ)

SHOW NVS FREE (411 ページ)

PURGE LOG

カテゴリー：運用・管理 / ログ

PURGE LOG [= {TEMPORARY | *output-id*}]

output-id: ログ出力 ID (1 ~ 20)

解説

ログ機能に関する設定を削除、あるいは、ログ出力キュー内のメッセージを削除する。
出力先を指定しなかった場合、ログ機能の設定がデフォルトに戻る。ユーザー定義の出力先はすべて削除され、ログ出力キュー内のログメッセージはすべて消去される。出力先を指定した場合は、キューに格納されている該当出力先宛てのメッセージだけが削除され、ログ機能の設定は変更されない。

パラメーター

LOG ログ出力先を指定する。指定時は、キューに格納されている該当出力先宛てのメッセージだけが削除され、ログ機能の設定は変更されない。指定しなかったときは、ログ機能の設定がすべてデフォルトに戻る。その場合、ユーザー定義の出力先はすべて削除され、ログ出力キュー内のログメッセージはすべて消去される。

備考・注意事項

不用意に本コマンドを実行しないよう注意。

関連コマンド

DISABLE LOG (214 ページ)

ENABLE LOG (244 ページ)

PURGE NTP

カテゴリー：運用・管理 / NTP

PURGE NTP

解説

NTP の設定情報をすべて削除する。

備考・注意事項

不用意に本コマンドを実行しないよう注意。

関連コマンド

DISABLE NTP (219 ページ)

ENABLE NTP (249 ページ)

RESET NTP (289 ページ)

PURGE PORTAUTH PORT

カテゴリー：運用・管理 / ポート認証

PURGE PORTAUTH [= {8021X|MACBASED}] **PORT**={*eth-port*|*port-list*|ALL}

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

解説

指定ポートにおけるポート認証機能 (802.1X 認証、MAC ベース認証) の設定をすべて削除する。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。
省略時は 8021X と見なされる。

PORT ポート

備考・注意事項

ランタイムメモリー上にある、指定ポートの 802.1X 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

DISABLE PORTAUTH (220 ページ)

DISABLE PORTAUTH PORT (222 ページ)

SHOW PORTAUTH PORT (419 ページ)

PURGE SNMP

カテゴリー：運用・管理 / SNMP

PURGE SNMP

解説

(SNMPv1/v2c/3)SNMP 関連の設定(コミュニティ、ターゲット、ユーザー、ユーザーグループ、ビューなど)をすべて消去し、SNMP モジュールを無効にする。

備考・注意事項

ランタイムメモリー上にある SNMP 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

本コマンドを実行しても、ENABLE SNMP AUTHENTICATE_TRAP コマンドの設定は消去されない。消去する場合は、DISABLE SNMP AUTHENTICATE_TRAP コマンドを実行すること。

関連コマンド

ADD SNMP COMMUNITY (134 ページ)
ADD SNMP GROUP (136 ページ)
ADD SNMP TARGETADDR (138 ページ)
ADD SNMP TARGETPARAMS (140 ページ)
ADD SNMP USER (142 ページ)
ADD SNMP VIEW (144 ページ)
CREATE SNMP COMMUNITY (167 ページ)
DISABLE SNMP AUTHENTICATE_TRAP (225 ページ)
ENABLE SNMP (257 ページ)
ENABLE SNMP AUTHENTICATE_TRAP (258 ページ)
ENABLE SNMP COMMUNITY (259 ページ)
ENABLE SNMP COMMUNITY TRAP (260 ページ)
SHOW SNMP (437 ページ)

PURGE TRIGGER

カテゴリー：運用・管理 / トリガー

PURGE TRIGGER

解説

トリガー機能の設定情報をすべて削除する。
作成したトリガーはすべて削除され、トリガー機能は無効になる。

備考・注意事項

不用意に本コマンドを実行しないよう注意。

関連コマンド

CREATE TRIGGER CPU (169 ページ)
CREATE TRIGGER FIREWALL (171 ページ)
CREATE TRIGGER INTERFACE (173 ページ)
CREATE TRIGGER MEMORY (175 ページ)
CREATE TRIGGER MODULE (177 ページ)
CREATE TRIGGER PERIODIC (180 ページ)
CREATE TRIGGER REBOOT (182 ページ)
CREATE TRIGGER TIME (184 ページ)
DELETE TRIGGER (205 ページ)
DESTROY TRIGGER (211 ページ)
DISABLE TRIGGER (232 ページ)
ENABLE TRIGGER (265 ページ)
SET TRIGGER CPU (342 ページ)
SET TRIGGER FIREWALL (344 ページ)
SET TRIGGER INTERFACE (346 ページ)
SET TRIGGER MEMORY (348 ページ)
SET TRIGGER MODULE (350 ページ)
SET TRIGGER PERIODIC (352 ページ)
SET TRIGGER REBOOT (354 ページ)
SET TRIGGER TIME (356 ページ)
SHOW TRIGGER (470 ページ)

PURGE USER

カテゴリー：運用・管理 / ユーザー認証データベース

PURGE USER

解説

MANAGER を除くすべてのユーザーを認証データベースから削除する。
MANAGER のパスワードはデフォルトの friend に戻る。

備考・注意事項

不用意に本コマンドを実行しないよう注意。

関連コマンド

ADD USER (151 ページ)
DELETE USER (206 ページ)
DISABLE USER (233 ページ)
ENABLE USER (266 ページ)
RESET USER (292 ページ)
SET USER (359 ページ)
SHOW USER (478 ページ)

RECONNECT

カテゴリー：運用・管理 / ターミナルサービス

RECONNECT 1..5

解説

一時中断した端末セッションに再接続する。
セッション番号は SHOW SESSIONS コマンドで確認できる。

例

中断していた端末セッション 2 に再接続する。

RECONNECT 2

関連コマンド

DISCONNECT (235 ページ)
SHOW SESSIONS (436 ページ)
TELNET (486 ページ)

RENAME

カテゴリー：運用・管理 / 記憶装置とファイルシステム

RENAME *src-filename* *dst-filename*

src-filename: 変更前ファイル名

dst-filename: 変更後ファイル名

解説

ファイル名を変更する。

関連コマンド

DELETE FILE (189 ページ)

SHOW FILE (374 ページ)

RESET FILE PERMANENTREDIRECT

カテゴリー：運用・管理 / 記憶装置とファイルシステム

RESET FILE [=filename] **PERMANENTREDIRECT**

filename: ファイル名

解説

コマンドやスクリプトの出力を保存（リダイレクト）するため書き込み用にオープンされているファイルをクローズし、ロックを解除する。

ADD FILE コマンドや CREATE FILE コマンドを PERMANENTREDIRECT オプション付きで実行した場合、該当コマンドで指定したファイルは、本コマンドを実行するまでオープン（かつロック）されたままの状態となる。

パラメーター

FILE 出力先のテキストファイル名。具体的なファイル名を省略した場合は、オープン中のすべてのファイルが対象となる

例

デバッグ情報の出力先テキストファイル ipdebug.txt をクローズする。

```
RESET FILE=ipdebug.txt PERMANENTREDIRECT
```

備考・注意事項

本コマンドを実行しても、ADD FILE コマンドや CREATE FILE コマンドの入力時に「ENABLE XXXX DEBUG」コマンドで有効化したデバッグオプションは無効化されないので、必要に応じて「DISABLE XXX DEBUG」コマンドを実行し、デバッグオプションを無効にすること。

関連コマンド

ADD FILE (123 ページ)

CREATE FILE (161 ページ)

SHOW FILE (374 ページ)

SHOW FILE PERMANENTREDIRECT (376 ページ)

RESET LOADER

カテゴリー：運用・管理 / アップロード・ダウンロード

RESET LOADER

解説

ファイル転送をつかさどる LOADER モジュールをリセットする。
実行中のファイル転送はすべて中断され、ファイル転送に用いられていたリソースはすべて解放される。また、作成途中のファイルは削除される。

関連コマンド

LOAD (271 ページ)

SET LOADER (298 ページ)

SHOW LOADER (386 ページ)

RESET NTP

カテゴリー：運用・管理 / NTP

RESET NTP

解説

NTP モジュールをリセットする。

ダイナミックな設定情報をすべて削除し、スタティックな設定情報を読み直し、NTP リクエストを送信する。

関連コマンド

DISABLE NTP (219 ページ)

ENABLE NTP (249 ページ)

PURGE NTP (280 ページ)

RESET PORTAUTH PORT

カテゴリー：運用・管理 / ポート認証

RESET PORTAUTH [= {8021X|MACBASED}] **PORT**={*eth-port*|*port-list*|ALL}
 [SUPPLICANTMAC=*macadd*]

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

macadd: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

解説

指定ポートにおけるポート認証機能 (802.1X 認証、MAC ベース認証) の状態をリセットする。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。
 省略時は 8021X と見なされる。

PORT ポート

SUPPLICANTMAC Supplicant の MAC アドレス。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。

関連コマンド

DISABLE PORTAUTH (220 ページ)

DISABLE PORTAUTH PORT (222 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

RESET PORTAUTH PORT MULTIMIB

カテゴリー：運用・管理 / ポート認証

RESET PORTAUTH [= {8021X|MACBASED}] **PORT**={*eth-port*|ALL} **MULTIMIB**

eth-port: ETH インターフェース名 (eth0 のように指定)

解説

802.1X Multi-SupPLICANT モードの Authenticator ポート、または、MAC ベース認証ポートにおいて、未認証かつ SET PORTAUTH PORT SUPPLICANTMAC コマンドで設定していない SupPLICANT の情報をクリアする。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

PORT ポート。本コマンドは、Multi-SupPLICANT モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。

関連コマンド

DISABLE PORTAUTH (220 ページ)

DISABLE PORTAUTH PORT (222 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (317 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

RESET USER

カテゴリー：運用・管理 / ユーザー認証データベース

RESET USER [=login-name] **COUNTERS** [= {ALL|GLOBAL|USER}]

login-name: ログイン名 (1~64 文字。英数字のみ使用可能。大文字小文字を区別しない。空白不可)

解説

ユーザーごとのログイン統計カウンター、あるいは、ユーザー認証機構のグローバルカウンターをリセットする。

パラメーター

USER ログイン名を指定した場合は、該当ユーザーのログイン統計カウンターだけがリセットされる。

COUNTERS リセットするカウンターの種類。USER パラメーターにログイン名を指定しなかった場合、ALL (すべてのカウンター)、GLOBAL (グローバルカウンター)、USER (全ユーザーのログイン統計カウンター) が指定できる。USER パラメーターにログイン名を指定した場合、COUNTERS パラメーターには USER (該当ユーザーのログイン統計カウンター) しか指定できない。

関連コマンド

ADD USER (151 ページ)

DELETE USER (206 ページ)

DISABLE USER (233 ページ)

ENABLE USER (266 ページ)

PURGE USER (284 ページ)

SET USER (359 ページ)

SHOW USER (478 ページ)

RESTART

カテゴリー：運用・管理 / システム

RESTART {**REBOOT**|**ROUTER**} [CONFIG={*filename*|NONE}]

filename: ファイル名（拡張子は.scp か.cfg）

解説

システムを再起動する。

パラメーター

REBOOT コールドスタート（ハードウェアリセット）を実行する。この場合 CONFIG パラメーターは指定できない。

ROUTER ウォームスタート（ソフトウェアリセット）を実行する。CONFIG パラメーターで再起動後に読み込む設定ファイルを指定できる。

CONFIG 再起動時に読み込む設定スクリプトファイル。ウォームスタート時（ROUTER オプション指定時）のみ指定可能。NONE を指定した場合は設定ファイルを読み込まずに起動する（空の設定で立ち上がる）。本オプションを指定しなかった場合は、SET CONFIG コマンドで設定した起動時設定ファイルが読み込まれる。

例

ウォームスタートする。

```
RESTART ROUTER
```

1 度だけ空の設定で再起動する。

```
RESTART ROUTER CONFIG=NONE
```

1 度だけ TEMP.CFG の設定で再起動する。

```
RESTART ROUTER CONFIG=TEMP.CFG
```

ルーターをハードウェアリセットする。

```
RESTART REBOOT
```

関連コマンド

SHOW CONFIG (363 ページ)

SHOW EXCEPTION (367 ページ)

SHOW STARTUP (464 ページ)

SET CONFIG

カテゴリー：運用・管理 / コンフィグレーション

SET CONFIG=*filename*

filename: ファイル名（拡張子は.scp か.cfg）

解説

起動時に読み込まれるデフォルトの設定ファイル（起動時設定ファイル）を指定する。

パラメーター

CONFIG 設定スクリプトファイル（.cfg または.scp）

関連コマンド

CREATE CONFIG（158 ページ）

RESTART（293 ページ）

SHOW CONFIG（363 ページ）

SET HELP

カテゴリー：運用・管理 / システム

SET HELP=filename

filename: ファイル名

解説

HELP コマンドが使用するヘルプファイルを指定する。
現在の設定は SHOW SYSTEM コマンドで確認できる。

パラメーター

HELP ヘルプファイル名

例

ヘルプファイルとして help.hlp を使うよう設定する。

```
SET HELP=help.hlp
```

関連コマンド

HELP (269 ページ)

SHOW SYSTEM (465 ページ)

SET INSTALL

カテゴリー：運用・管理 / ソフトウェア

SET INSTALL=**{TEMPORARY|PREFERRED|DEFAULT}** [RELEASE={*filename*|EPROM}]
[PATCH[=*filename*]]

filename: ファイル名

解説

インストール（ファームウェア構成）情報を変更する。

「インストール」には起動時にロードすべきファームウェアの情報、具体的にはリリースファイルとパッチファイル（オプション）の組み合わせが記録されている。インストールには、TEMPORARY（一度しか使用されないテスト用インストール）、PREFERRED（通常使用するインストール）、DEFAULT（緊急時に使用するインストール。EPROM 上のファームウェアから起動する）がある。

パラメーター

INSTALL インストールの種類

RELEASE リリースファイル名（拡張子 .rez）。DEFAULT インストールの場合は EPROM を指定する。

PATCH パッチファイル名（拡張子 .paz）

例

リリースファイル 55-292.rez、パッチファイル 55292-01.paz の組み合わせを通常使用するファームウェアとして設定する。

```
SET INSTALL=PREFERRED RELEASE=55-292.rez PATCH=55292-01.paz
```

関連コマンド

DELETE INSTALL（190 ページ）

SHOW INSTALL（384 ページ）

SET LOADER

カテゴリー：運用・管理 / アップロード・ダウンロード

```
SET LOADER [METHOD={HTTP|TFTP|WEB|WWW|ZMODEM|DEFAULT}] [SERVER={hostname|
ipadd|DEFAULT}] [SERVPORT={1..65535|DEFAULT}] [FILE=filename]
[DESTINATION={FLASH|NVS|DEFAULT}] [HTTPPROXY={hostname|ipadd|DEFAULT}]
[PROXYPORT={1..65535|DEFAULT}] [ASYN={asyn-number|DEFAULT}]
[USERNAME=username] [PASSWORD=password] [DELAY={seconds|DEFAULT}]
```

hostname: ホスト名

ipadd: IP アドレス

filename: ファイル名

asyn-number: 非同期ポート番号 (0)

username: ユーザー名 (1~60 文字)

password: パスワード (1~60 文字)

seconds: 時間 (0~4294967295 秒)

解説

LOAD コマンドの各パラメーターにデフォルト値 (省略時に使用する値) を設定する。

LOAD コマンド実行時に指定されなかったパラメーターについては、本コマンドで設定したデフォルト値が使用される。

パラメーター

METHOD 転送プロトコル。TFTP、HTTP (WEB、WWW も同じ)、ZMODEM のいずれかを指定する。

DEFAULT を指定した場合はデフォルトの TFTP に戻る

SERVER TFTP/Web サーバーのフルドメイン名 (FQDN) または IP アドレス。FQDN を指定するには、

ADD IP DNS コマンドで DNS サーバーを設定しておく必要がある。DEFAULT を指定した場合は未設定 (デフォルト) に戻る

SERVPORT Web サーバーの TCP ポート番号。DEFAULT を指定した場合はデフォルトの 80 に戻る

FILE ダウンロード対象ファイル名

DESTINATION ダウンロードしたファイルの保存先デバイス。NVS (不揮発性メモリー) か FLASH (フラッシュメモリー) を指定する。DEFAULT を指定した場合はデフォルトの FLASH に戻る

HTTPPROXY HTTP プロキシのフルドメイン名 (FQDN) または IP アドレス。FQDN を指定するには、ADD IP DNS コマンドで DNS サーバーを設定しておく必要がある。DEFAULT を指定した場合は未設定 (デフォルト) に戻る

PROXYPORT HTTP プロキシの TCP ポート番号。DEFAULT を指定した場合はデフォルトの 80 に戻る

ASYN 非同期ポート番号。ZMODEM でダウンロードするときに使う。DEFAULT を指定した場合は未設定 (デフォルト) に戻る

USERNAME HTTP Basic 認証用のユーザー名。DEFAULT を指定した場合は未設定 (デフォルト) に

戻る

PASSWORD HTTP Basic 認証用のパスワード。DEFAULT を指定した場合は未設定（デフォルト）に

戻る

DELAY コマンド（LOAD コマンド）投入からダウンロード開始までの時間（秒）。DEFAULT を指定した場合はデフォルトの 0 に戻る

関連コマンド

LOAD (271 ページ)

SHOW LOADER (386 ページ)

SET LOG OUTPUT

カテゴリー：運用・管理 / ログ

```
SET LOG OUTPUT={TEMPORARY|PERMANENT|output-id} [DESTINATION={EMAIL|  
MEMORY|NVS|PORT|ROUTER|SYSLOG}] [FORMAT={FULL|MSGONLY|SUMMARY}]  
[MAXQUEUESEVERITY=severity] [MESSAGES=count] [PASSWORD={password|NONE}]  
[ASYN=asyn-number] [QUEUEONLY={YES|NO}] [SECURE={YES|NO}] [SERVER=ipadd]  
[TO=email-addr] [ZONE={time-zone|utc-offset}] [FACILITY={DEFAULT|  
LOCAL1..LOCAL7}]
```

output-id: ログ出力 ID (1~20)

severity: ログレベル (0~7)

count: 個数 (1~)

password: パスワード (1~16 文字)

asyn-number: 非同期ポート番号 (0)

ipadd: IP アドレス

email-addr: 電子メールアドレス

time-zone: タイムゾーン名

utc-offset: 協定世界時 (UTC) からのオフセット (+23:59:59 ~ -23:59:59)

解説

ログ出力先の定義を変更する。

パラメーター

OUTPUT ログ出力先 ID。1~20 の任意の番号か、特殊なキーワード「TEMPORARY」(RAM) または「PERMANENT」(NVS) を指定する。TEMPORARY を指定した場合、MAXQUEUESEVERITY、QUEUEONLY、SECURE の各パラメーターは指定できず、DESTINATION は MEMORY しか指定できない。また、PERMANENT を指定したときは、DESTINATION に NVS しか指定できない (NVS (不揮発性メモリー) 搭載機種でのみ有効)。

DESTINATION ログメッセージの出力先。EMAIL (TO パラメーターで指定されたアドレスに電子メールで送信)、MEMORY (RAM 上に保存。OUTPUT パラメーターに TEMPORARY を指定したときのみ有効)、NVS (不揮発性メモリー上に保存。OUTPUT パラメーターに PERMANENT を指定したときのみ有効)、PORT (ASYN パラメーターで指定した非同期ポートに出力)、ROUTER (SERVER パラメーターで指定したルーターに Secure Router Logging Protocol (SRLP) を使って転送)、SYSLOG (SERVER パラメーターで指定した syslog サーバーに転送。メッセージは syslog フォーマットに変換される) から選択する。

FORMAT 非同期ポートに出力するログメッセージの形式。FULL (すべての情報を表示。1 ログエントリーが複数行に渡って表示される。空行がエントリーの区切りになる)、MSGONLY (テキストメッセージのみを表示)、SUMMARY (サマリーを表示。表示されないフィールドもある)。デフォルトは SUMMARY。DESTINATION パラメーターに PORT を指定した場合のみ有効。

MAXQUEUESEVERITY QUEUEONLY パラメーターに YES を指定した（キューがいっぱいになるまでログを出力しない）ときに、すぐに出力せずにキューに入れる最大のログレベルを指定する。QUEUEONLY が YES のときは、MAXQUEUESEVERITY よりも低いログレベルのメッセージは、キューの長さが MESSAGES パラメーターの値に達するまでキューイングされる。一方、MAXQUEUESEVERITY 以上のログレベルを持つメッセージが生成されたときは、ただちにキューがフラッシュ（処理）される。DESTINATION パラメーターに PORT か SYSLOG を指定しているとき、および、OUTPUT パラメーターに TEMPORARY を指定しているときは、本パラメーターは指定できない。デフォルトは 7、すなわちキューがいっぱいにならないうちに処理されるのは、最高のログレベルを持つメッセージが来たときだけとなる。

MESSAGES DESTINATION が SYSLOG の場合は、キューの長さ。DESTINATION が NVS か MEMORY のときは、保存するメッセージの最大数。最大値に達したときは、古いメッセージから順番に削除される。DESTINATION が EMAIL の場合は、一度に送信されるメッセージの数。DESTINATION が PORT のときは、本パラメーターは指定できない。DESTINATION が SYSLOG のときのデフォルトは 20、MEMORY のときのデフォルトは 200、EMAIL のときは 100。NVS のときは 20。

PASSWORD SRLP でログを転送する際、転送先から認証を受けるためのパスワード。DESTINATION が ROUTER の場合にのみ有効。パスワードそのものは送信されず、代わりに MD5 によるメッセージダイジェストが送られる。デフォルトはパスワードなし。

ASYN ログを出力する非同期ポートの番号。DESTINATION に PORT を指定した場合にのみ有効。

QUEUEONLY キューがいっぱいになるまでメッセージを処理しないかどうか。DESTINATION に PORT を指定した場合、および、OUTPUT に TEMPORARY を指定した場合は、本パラメーターは指定できない。DESTINATION に SYSLOG を指定した場合、本パラメーターは動作しない。デフォルトは NO。

SECURE この出力先が「安全」かどうかを指定する。NO を指定した場合、パスワード変更など一部のメッセージが出力されなくなる。OUTPUT に TEMPORARY を指定した場合は、本パラメーターは指定できない。DESTINATION が ROUTER で PASSWORD が指定されている場合、および、DESTINATION が MEMORY か NVS の場合のデフォルトは YES。その他の場合のデフォルトは NO。

SERVER DESTINATION が ROUTER か SYSLOG の場合、メッセージの転送先 IP アドレスを指定する。ROUTER の場合は、SRLP (Secure Router Logging Protocol) サーバー (UDP 5023 番)、SYSLOG の場合は syslog サーバー (UDP 514 番) を指定する。

TO DESTINATION に EMAIL を指定した場合の、送信先メールアドレスを指定する。

ZONE タイムゾーン名または UTC からのオフセットを指定する。

FACILITY DESTINATION が SYSLOG の場合、送信する syslog メッセージの「ファシリティ」を指定する。DEFAULT を指定した場合は、既定の対応表（解説編参照）にしたがい、本製品のメッセージタイプが syslog ファシリティに変換される。LOCAL1～LOCAL7 を指定した場合は、本出力先宛ての syslog メッセージすべてに指定したファシリティ値がセットされる。デフォルトは DEFAULT（既定の対応表に基づいてファシリティを決定）。

関連コマンド

CREATE LOG OUTPUT (164 ページ)

DESTROY LOG OUTPUT (208 ページ)

SHOW LOG OUTPUT (395 ページ)

SET LOG OUTPUT FILTER

カテゴリー：運用・管理 / ログ

```
SET LOG OUTPUT={TEMPORARY|PERMANENT|output-id} FILTER=entry-id
[ACTION={PROCESS|IGNORE}] [ALL] [DATE=[op]date] [DEVICE=[op]device]
[FILE=[op]filename] [MASK=ipadd] [MSGTEXT=[op]string]
[MODULE=[op]module-id] [ORIGIN=ipadd] [REFERENCE=[op]string]
[SEVERITY=[op]severity] [SOURCELINE=[op]line-num]
[SUBTYPE=[op]subtype-id] [TIME=[op]time] [TYPE=[op]type-id]
```

output-id: ログ出力 ID (1~20)

entry-id: エントリー番号 (1~)

op: 比較演算子 (「<」(小さい)「>」(大きい)「!」(等しくない)「」(等しい)「%」(以下の文字列を含む))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31) mmm は月 (英語月名の頭 3 文字。例: APR) yyyy は西暦年)

device: デバイス番号

filename: ファイル名 (1~12 文字)

ipadd: IP アドレスまたはネットマスク

string: 文字列

module-id: モジュール名またはモジュール番号 (0~255)

severity: ログレベル (0~7)

line-num: 行番号 (1~)

subtype-id: ログメッセージのサブタイプ名または ID

time: 時刻 (hh:mm:ss の形式。hh は時 (0~23) mm は分 (0~59) ss は秒 (0~59))

type-id: ログメッセージのタイプ名または ID

解説

ログ出力先に関連付けられたログメッセージフィルターの設定を変更する。

パラメーター

OUTPUT ログ出力先 ID。1~20 の任意の番号か、特殊なキーワード「TEMPORARY」(RAM) または「PERMANENT」(NVS) を指定する。

FILTER メッセージフィルターのエントリー番号。省略時は、フィルターリストの末尾に追加される。

ACTION フィルターアクション。このエントリーにマッチしたメッセージを処理 (PROCESS) するか、無視 (IGNORE) するかを指定。省略時は PROCESS。

ALL すべてのメッセージにマッチさせたいときに指定する。他の条件と同時に指定することはできない。

DATE メッセージの日付。省略時はすべての日付にマッチする。

DEVICE デバイス番号。省略時はすべてのデバイスにマッチする。

FILE 該当モジュールのソースプログラムファイル名 (例: logmain.c)。ソースファイル名は、SHOW LOG コマンドに FULL オプションを付けたときに表示される。省略時はすべてのファイル名にマッチする。

MASK ネットマスク。メッセージの生成元 IP アドレスを示す ORIGIN パラメーターと組み合わせて使

用する。省略時は 255.255.255.255 (単一ホスト)。

MSGTEXT メッセージ本文と比較する文字列。省略時はすべてのメッセージにマッチする。

MODULE モジュール番号またはモジュール名。省略時はすべてのモジュールにマッチする。

ORIGIN ログ生成元の IP アドレス。MASK パラメーターと組み合わせて範囲指定が可能。デフォルトではすべての IP アドレスにマッチする。

REFERENCE メッセージ中の参考情報。省略時はすべてにマッチする。

SEVERITY メッセージのログレベル。省略時はすべてのログレベルにマッチする。

SOURCELINE メッセージを生成したソースプログラムファイルの行番号。省略時はすべての行にマッチする。

SUBTYPE メッセージのサブタイプ名またはサブタイプ番号。省略時はすべてのサブタイプにマッチする。

TIME メッセージの時刻。省略時はすべての時刻にマッチする。

TYPE メッセージのタイプ名またはサブタイプ番号。省略時はすべてのサブタイプにマッチする。

関連コマンド

ADD LOG OUTPUT (126 ページ)

CREATE LOG OUTPUT (164 ページ)

DESTROY LOG OUTPUT (208 ページ)

SHOW LOG OUTPUT (395 ページ)

SET LOG RECEIVE

カテゴリー：運用・管理 / ログ

SET LOG RECEIVE={*ipadd*|**ANY**} [MASK=*ipadd*] [ALLOW={YES|NO}] [PROTOCOL={ALL|
BOTH|NEW|OLD|SYSLOG}] [PASSWORD={*password*|NONE}]

ipadd: IP アドレスまたはネットマスク

password: パスワード (1～16 文字。任意の印刷可能文字を使用可能。空白を含む場合はダブルクォートで囲む)

解説

ログ受信テーブルのエントリーを変更する。

パラメーター

RECEIVE ログ送信元の IP アドレス。MASK と組み合わせて範囲を指定することも可能。ANY と 0.0.0.0 はすべての IP アドレスを示す。

MASK RECEIVE パラメーターで指定したアドレスに対するマスク。ただし、RECEIVE=ANY または RECEIVE=0.0.0.0 のときは指定できない。

ALLOW RECEIVE/MASK で指定した IP アドレスからのログを受け入れるかどうか。YES なら受け入れ、NO なら拒否する。

PROTOCOL RECEIVE/MASK で指定した IP アドレスから、どのプロトコルでログを受け入れるかを指定する。OLD (Net Manage Message Protocol)、NEW (SRLP)、SYSLOG、BOTH (OLD と NEW)、ALL (OLD、NEW、SYSLOG のすべて) から選択する。

PASSWORD SRLP プロトコルにおいて、ログ送信元を認証するためのパスワードを指定する。省略時はパスワード認証を行わない。本パラメーターは、SRLP 使用時のみ有効 (PROTOCOL=NEW または BOTH、ALL のとき)。

関連コマンド

ADD LOG RECEIVE (128 ページ)

DELETE LOG RECEIVE (192 ページ)

SHOW LOG RECEIVE (400 ページ)

SET LOG UTCOFFSET

カテゴリー：運用・管理 / ログ

SET LOG UTCOFFSET={*time-zone*|*utc-offset*}

time-zone: タイムゾーン名

utc-offset: 協定世界時 (UTC) からのオフセット (+23:59:59 ~ -23:59:59)

解説

現地時間と協定世界時 (UTC) の差を設定する。

パラメーター

UTCOFFSET 協定世界時からのオフセットを指定する。定義済みのタイムゾーン名または時間差で指定する。時間差で指定する場合、UTC より進んでいる場合はプラス (+) を、遅れている場合はマイナス (-) を付ける。

| | | |
|--------|--------|----------------------------------|
| ASIA | +8:00 | Asia |
| ACDT | +10:30 | Australian Central Daylight Time |
| ACST | +9:30 | Australian Central Standard Time |
| AEDT | +11:00 | Australian Eastern Daylight Time |
| AEST | +10:00 | Australian Eastern Standard Time |
| AWST | +8:00 | Australian Western Standard Time |
| BST | +1:00 | British Standard Time |
| CHINA | +8:00 | China |
| GMT | +0:00 | Greenwich Mean Time |
| UK | +0:00 | Greenwich Mean Time |
| HK | +8:00 | Hong Kong |
| JST | +9:00 | Japan Standard Time |
| MET | +1:00 | Mid-European time |
| NZDT | +13:00 | New Zealand Daylight Time |
| NZST | +12:00 | New Zealand Standard Time |
| SING | +8:00 | Singapore |
| TAIWAN | +8:00 | Taiwan |
| UTC | +0:00 | Universal Coordinated Time |
| CDT | -5:00 | US Central Daylight Time |
| CST | -6:00 | US Central Standard Time |
| EDT | -4:00 | US Eastern Daylight Time |

| | | |
|---------|-------|---------------------------|
| EST | -5:00 | US Eastern Standard Time |
| MDT | -6:00 | US Mountain Daylight Time |
| MST | -7:00 | US Mountain Standard Time |
| PDT | -7:00 | US Pacific Daylight Time |
| PST | -8:00 | US Pacific Standard Time |
| DEFAULT | - | - |
| NONE | - | - |

表 35: タイムゾーン名一覧

例

UTC オフセットをタイムゾーンで指定する (日本)

```
SET LOG UTCOFFSET=JST
```

UTC オフセットを時間差で指定する (日本)

```
SET LOG UTCOFFSET=+9:00:00
```

関連コマンド

SHOW LOG STATUS (402 ページ)

SET MAIL

カテゴリー：運用・管理 / メール送信

SET MAIL HOSTNAME=*hostname*

hostname: ホスト名

解説

メールサーバーとの通信時に使用する自ホスト名を設定する。

自ホスト名は、SMTP セッション開始時に、SMTP の HELO コマンドの引数として送信される。メール送信（MAIL コマンド）を実行するには、本コマンドで自ホスト名を設定しておく必要がある。

パラメーター

HOSTNAME 自ホスト名。フルドメイン名（FQDN=Fully Qualified Domain Name）で指定する。設定を解除するときは NONE を指定する。

例

メール送信時に使用する自ホスト名として、white.mydomain.xxx を設定する。

```
SET MAIL HOSTNAME=white.mydomain.xxx
```

関連コマンド

SHOW MAIL（404 ページ）

SET MANAGER ASYN

カテゴリー：運用・管理 / セキュリティー

SET MANAGER ASYN=**{*asyn-number*|NONE}**

asyn-number: 非同期ポート番号 (0)

解説

指定した非同期ポートをマネージャーポートに設定する。

マネージャーポートは、ログインせずに MANAGER (管理者) 権限を得られるポート (SET ASYN コマンドの SECURE パラメーターが OFF のポート)。マネージャーポートは 1 つしか設定できない。

パラメーター

ASYN 非同期ポート番号。指定したポートがマネージャーポートになる。すでに他のポートがマネージャーポートに設定されていた場合、そのポートはマネージャーポートでなくなる (セキュアモードがオンになる)。NONE を指定した場合、マネージャーポートは存在しなくなる。

関連コマンド

LOGIN (273 ページ)

SET ASYN (「インターフェース」の 50 ページ)

SHOW MANAGER ASYN (406 ページ)

SET NTP UTCOFFSET

カテゴリー：運用・管理 / NTP

SET NTP UTCOFFSET={*time-zone*|*utc-offset*}

time-zone: タイムゾーン名

utc-offset: 協定世界時 (UTC) からのオフセット (+23:59:59 ~ -23:59:59)

解説

現地時間と協定世界時 (UTC) の差を設定する。NTP で扱われる時間はすべて UTC なので、必ずオフセットを設定する必要がある。

パラメーター

UTCOFFSET 協定世界時からのオフセットを指定する。定義済みのタイムゾーン名または時間差で指定する。時間差で指定する場合、UTC より進んでいる場合はプラス (+) を、遅れている場合はマイナス (-) を付ける。

| | | |
|--------|--------|----------------------------------|
| ASIA | +8:00 | Asia |
| ACDT | +10:30 | Australian Central Daylight Time |
| ACST | +9:30 | Australian Central Standard Time |
| AEDT | +11:00 | Australian Eastern Daylight Time |
| AEST | +10:00 | Australian Eastern Standard Time |
| AWST | +8:00 | Australian Western Standard Time |
| BST | +1:00 | British Standard Time |
| CHINA | +8:00 | China |
| GMT | +0:00 | Greenwich Mean Time |
| UK | +0:00 | Greenwich Mean Time |
| HK | +8:00 | Hong Kong |
| JST | +9:00 | Japan Standard Time |
| MET | +1:00 | Mid-European time |
| NZDT | +13:00 | New Zealand Daylight Time |
| NZST | +12:00 | New Zealand Standard Time |
| SING | +8:00 | Singapore |
| TAIWAN | +8:00 | Taiwan |
| UTC | +0:00 | Universal Coordinated Time |
| CDT | -5:00 | US Central Daylight Time |
| CST | -6:00 | US Central Standard Time |

| | | |
|---------|-------|---------------------------|
| EDT | -4:00 | US Eastern Daylight Time |
| EST | -5:00 | US Eastern Standard Time |
| MDT | -6:00 | US Mountain Daylight Time |
| MST | -7:00 | US Mountain Standard Time |
| PDT | -7:00 | US Pacific Daylight Time |
| PST | -8:00 | US Pacific Standard Time |
| DEFAULT | - | - |
| NONE | - | - |

表 36: タイムゾーン名一覧

例

UTC オフセットをタイムゾーンで指定する（日本）。

```
SET NTP UTCOFFSET=JST
```

UTC オフセットを時間差で指定する（日本）。

```
SET NTP UTCOFFSET=+9:00:00
```

関連コマンド

```
SHOW NTP ( 407 ページ )
```

SET PASSWORD

カテゴリー：運用・管理 / ユーザー認証データベース

SET PASSWORD

解説

ログインパスワードを変更する。

プロンプトが表示されるので、現在のパスワードと新しいパスワード（確認のため2回）を入力する。

入力・出力・画面例

```
Manager > set password
```

Old password: abcababc （現在のパスワードを入力。入力したパスワードは実際には表示されない）

New password: xyzxyz （新しいパスワードを入力）

Confirm: xyzxyz （確認のため、新しいパスワードをもう一度入力）

プロンプトが表示されないときはここで「Enter」を押す

関連コマンド

ADD USER (151 ページ)

SET USER (359 ページ)

SET PORTAUTH PORT

カテゴリ：運用・管理 / ポート認証

```
SET PORTAUTH[=8021X] PORT={eth-port|port-list|ALL} TYPE=AUTHENTICATOR
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [MAXREQ=1..10] [MODE={MULTI|
SINGLE}] [PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=0..65535]
[REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=1..10] [REAUTHPERIOD=1..86400]
[SERVERTIMEOUT=1..60] [SUPPTIMEOUT=1..60] [TXPERIOD=1..65535]
[GUESTVLAN={vlanname|1..4085|NONE}] [SECUREVLAN={ON|OFF}]
[VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}]
```

```
SET PORTAUTH[=8021X] PORT={eth-port|port-list|ALL} TYPE=BOTH
[CONTROL={AUTHORISED|UNAUTHORISED|AUTO}] [MAXREQ=1..10] [MODE=SINGLE]
[PIGGYBACK={TRUE|FALSE}] [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|
FALSE}] [REAUTHMAX=1..10] [REAUTHPERIOD=1..86400] [SERVERTIMEOUT=1..60]
[SUPPTIMEOUT=1..60] [TXPERIOD=1..65535] [GUESTVLAN={vlanname|1..4085|
NONE}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}] [AUTHPERIOD=1..60]
[HELDPERIOD=0..65535] [MAXSTART=1..10] [STARTPERIOD=1..60]
[USERNAME=login-name PASSWORD=password [METHOD={OTP [ENCRYPTION={MD4|
MD5}}]|STANDARD}]]
```

```
SET PORTAUTH[=8021X] PORT={eth-port|port-list|ALL} TYPE=SUPPLICANT
[AUTHPERIOD=1..60] [HELDPERIOD=0..65535] [MAXSTART=1..10]
[STARTPERIOD=1..60] [USERNAME=login-name PASSWORD=password [METHOD={OTP
[ENCRYPTION={MD4|MD5}}]|STANDARD}]]
```

```
SET PORTAUTH=MACBASED PORT={eth-port|ALL} [CONTROL={AUTHORISED|AUTO|
UNAUTHORISED}] [QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|FALSE}]
[REAUTHPERIOD=1..86400] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|
DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|
NONE}]
```

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1~。ハイフン、カンマを使った複数指定も可能)

login-name: ログイン名 (1~64 文字。英数字のみ使用可能)

password: パスワード (1~64 文字。英数字のみ使用可能)

vlanname: VLAN 名 (1~32 文字。英数字とアンダースコア (_)、ハイフンを使用可能。大文字小文字を区別しない)

解説

指定ポートにおけるポート認証機能（802.1X 認証または MAC ベース認証）の設定を変更する。

パラメーター

PORTAUTH 認証メカニズム。8021X（802.1X 認証）MACBASED（MAC ベース認証）から選択する。省略時は 8021X と見なされる。

PORT ポート

TYPE（802.1X ポート）802.1X 認証におけるスイッチポートの役割。AUTHENTICATOR（Authenticator ポート）SUPPLICANT（Supplicant ポート）BOTH（Authenticator ポートかつ Supplicant ポート）のいずれかを指定する。なお、Multi-Supplicant モード（MODE=MULTI）を使用する場合、TYPE=BOTH は指定できない。TYPE=AUTHENTICATOR を指定すること。

CONTROL（802.1X Authenticator ポート、MAC ベース認証ポート）手動設定による Authenticator ポートの状態。AUTO（認証結果に応じて変動）UNAUTHORISED（未認証固定）AUTHORISED（認証済み固定）から選択する。デフォルトは AUTO。通常は AUTO のままでよい。ただし、RADIUS サーバーの接続先ポートを Authenticator に設定している場合は、本パラメーターを AUTHORISED に設定する必要がある。

MAXREQ（802.1X Authenticator ポート）Supplicant に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

MODE（802.1X Authenticator ポート）Authenticator ポートのモード。Supplicant が 1 台だけ接続されていることを想定した Single-Supplicant モード（MODE=SINGLE）と、Supplicant が複数台接続されていることを想定した Multi-Supplicant モード（MODE=MULTI）がある。Single-Supplicant モードでは、該当ポート配下に最初に接続された Supplicant だけが認証対象となる（その他の Supplicant からの通信を許可するかどうかは、PIGGYBACK パラメーターで制御可能）。Multi-Supplicant モードでは、該当ポート配下に接続された個々の Supplicant を識別し、個別に認証を行う。なお、Multi-Supplicant モードを使用する場合、TYPE パラメーターには BOTH を指定できない。AUTHENTICATOR を指定すること。デフォルトは SINGLE。

PIGGYBACK（802.1X Single-Supplicant Authenticator ポート）Single-Supplicant モード（MODE=SINGLE）において、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうかを指定する。TRUE なら許可、FALSE なら拒否。ETH ポートのみ FALSE に設定可能。デフォルトは TRUE。

QUIETPERIOD（802.1X Authenticator ポート、MAC ベース認証ポート）Supplicant の認証に失敗した後、Supplicant との通信を拒否する期間（秒）。この期間中は受信したパケットをすべて破棄する。デフォルトは 60 秒。

REAUTHENABLED（802.1X Authenticator ポート、MAC ベース認証ポート）認証に成功した Supplicant を定期的に再認証するかどうか。TRUE なら再認証する、FALSE なら再認証しない。デフォルトは FALSE。

REAUTHMAX（802.1X Authenticator ポート）再認証時における EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

REAUTHPERIOD（802.1X Authenticator ポート、MAC ベース認証ポート）Supplicant の再認証間隔（秒）。デフォルトは 3600 秒。

SERVERTIMEOUT（802.1X Authenticator ポート）RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）。デフォルトは 30 秒。

SUPPTIMEOUT (802.1X Authenticator ポート) Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒)。デフォルトは 30 秒。

TXPERIOD (802.1X Authenticator ポート) Supplicant に EAPOL パケットを再送信する間隔 (秒)。デフォルトは 30 秒。

GUESTVLAN (802.1X Single-Supplicant Authenticator ポート) ゲスト VLAN を指定する。装置上に設定されている VLAN の名前か VLAN ID を指定すること。NONE はゲスト VLAN を使用しないことを意味する。EAPOL パケットをまだ受信していないとき、該当ポートはゲスト VLAN の所属となる。最初の EAPOL パケットを受信すると、該当ポートはゲスト VLAN から削除され、本来の所属 VLAN に復帰する。本パラメーターは、Single-Supplicant モード (MODE=SINGLE) でのみ有効。デフォルトは NONE。

SECUREVLAN (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、有効な VLAN でありさえすれば認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。デフォルトは ON。

VLANASSIGNMENT (802.1X Authenticator ポート、MAC ベース認証ポート) ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。デフォルトは ENABLED。

MIBRESET (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証を使用しているポートにおいて、古い Supplicant 情報をエージアウトするかどうか。デフォルトは ENABLED。

TRAP (802.1X Authenticator ポート、MAC ベース認証ポート) ポート認証機能に関する SNMP トラップを送信するかどうか。SUCCESS を指定した場合は、Supplicant の認証に成功したときと、認証情報が時間切れになったときに SNMP トラップを送信する。FAILURE を指定した場合は、Supplicant の認証に失敗したときに SNMP トラップを送信する。BOTH を指定したときは、SUCCESS と FAILURE の両方の場合に SNMP トラップを送信する。NONE はトラップを送信しない。デフォルトは NONE。

AUTHPERIOD (802.1X Supplicant ポート) Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間 (秒)。デフォルトは 30 秒。

HELDPERIOD (802.1X Supplicant ポート) 認証失敗後、Authenticator との通信を試みない期間 (秒)。デフォルトは 60 秒。

MAXSTART (802.1X Supplicant ポート) EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、Authenticator が存在しておらずポート認証の必要はないと判断する。デフォルトは 3 回。

STARTPERIOD (802.1X Supplicant ポート) Authenticator に EAPOL-Start パケットを再送信する間隔 (秒)。デフォルトは 30 秒。

USERNAME (802.1X Supplicant ポート) 指定スイッチポートが Supplicant として動作する場合に使うユーザー名。必ず PASSWORD パラメーターと組で指定すること。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・

パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

PASSWORD (802.1X Supplicant ポート) 指定スイッチポートが Supplicant として動作する場合に使うパスワード。必ず USERNAME パラメーターと組で指定すること。METHOD パラメーターに STANDARD を指定した場合、または、METHOD パラメーターを省略した場合は、6～63 文字の文字列を指定する。METHOD パラメーターに OTP を指定した場合は、10～63 文字の文字列（認証サーバー上で設定した OTP Initialisation Password と同じ値）を指定する。本パラメーターを設定した場合、該当ポートでは、SET PORTAUTH USERNAME コマンドで設定するグローバルなユーザー名・パスワード・暗号化方式ではなく、本コマンドで設定した値が使用される。

METHOD (802.1X Supplicant ポート) パスワード送信時の暗号化方式。STANDARD (EAP-MD5) または OTP (One-Time Password) から選択する。OTP を指定した場合は、ENCRYPTION パラメーターでワンタイムパスワードの生成アルゴリズムも指定する必要がある。デフォルトは STANDARD。

ENCRYPTION (802.1X Supplicant ポート) ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

備考・注意事項

802.1X 認証の Multi-Supplicant モードおよび MAC ベース認証は、ETH インターフェースでのみサポート。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (118 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (317 ページ)

SHOW PORTAUTH (413 ページ)

SHOW PORTAUTH COUNTER (416 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

SHOW PORTAUTH TIMER (428 ページ)

SET PORTAUTH PORT SUPPLICANTMAC

カテゴリー：運用・管理 / ポート認証

```
SET PORTAUTH[=8021X] PORT={eth-port|ALL} SUPPLICANTMAC=macadd
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [MAXREQ=1..10]
[QUIETPERIOD=0..65535] [REAUTHENABLED={TRUE|FALSE}] [REAUTHMAX=1..10]
[REAUTHPERIOD=1..86400] [SERVERTIMEOUT=1..60] [SUPPTIMEOUT=1..60]
[TXPERIOD=1..65535] [SECUREVLAN={ON|OFF}] [VLANASSIGNMENT={ENABLED|
DISABLED}] [MIBRESET={ENABLED|DISABLED}] [TRAP={SUCCESS|FAILURE|BOTH|
NONE}] [DEFAULT]
```

```
SET PORTAUTH=MACBASED PORT={eth-port|ALL} SUPPLICANTMAC=macadd
[CONTROL={AUTHORISED|AUTO|UNAUTHORISED}] [QUIETPERIOD=0..65535]
[REAUTHENABLED={TRUE|FALSE}] [REAUTHPERIOD=1..86400] [SECUREVLAN={ON|
OFF}] [VLANASSIGNMENT={ENABLED|DISABLED}] [MIBRESET={ENABLED|DISABLED}]
[TRAP={SUCCESS|FAILURE|BOTH|NONE}] [DEFAULT]
```

eth-port: ETH インターフェース名 (eth0 のように指定)

macadd: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

解説

802.1X Multi-SupPLICANT モードで動作している Authenticator ポート、または、MAC ベース認証ポートに対し、特定の MAC アドレスを持つ SupPLICANT 固有のパラメーターを設定する。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。省略時は 8021X と見なされる。

PORT ポート。本コマンドは、Multi-SupPLICANT モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。

SUPPLICANTMAC SupPLICANT の MAC アドレス。

CONTROL (802.1X Authenticator ポート、MAC ベース認証ポート) 手動設定による Authenticator ポートの状態。AUTO (認証結果に応じて変動)、UNAUTHORISED (未認証固定)、AUTHORISED (認証済み固定) から選択する。デフォルトは AUTO。通常は AUTO のままでよい。ただし、RADIUS サーバーの接続先ポートを Authenticator に設定している場合は、本パラメーターを AUTHORISED に設定する必要がある。

MAXREQ (802.1X Authenticator ポート) SupPLICANT に対する EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

QUIETPERIOD (802.1X Authenticator ポート、MAC ベース認証ポート) SupPLICANT の認証に失敗した後、SupPLICANT との通信を拒否する期間 (秒)。この期間中は受信したパケットをすべて破棄する。

デフォルトは 60 秒。

REAUTHENABLED (802.1X Authenticator ポート、MAC ベース認証ポート) 認証に成功した Supplicant を定期的に再認証するかどうか。TRUE なら再認証する、FALSE なら再認証しない。デフォルトは FALSE。

REAUTHMAX (802.1X Authenticator ポート) 再認証時における EAPOL-Request パケットの最大再送回数。デフォルトは 2 回。

REAUTHPERIOD (802.1X Authenticator ポート、MAC ベース認証ポート) Supplicant の再認証間隔 (秒)。デフォルトは 3600 秒。

SERVERTIMEOUT (802.1X Authenticator ポート) RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間 (秒)。デフォルトは 30 秒。

SUPPTIMEOUT (802.1X Authenticator ポート) Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒)。デフォルトは 30 秒。

TXPERIOD (802.1X Authenticator ポート) Supplicant に EAPOL パケットを再送信する間隔 (秒)。デフォルトは 30 秒。

SECUREVLAN (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証でダイナミック VLAN を使用しているとき、2 番目以降の Supplicant の認証方法を指定する。本パラメーターに ON を指定した場合は、2 番目以降の Supplicant は、最初に認証を通った Supplicant と同じ VLAN でないと認証されない。一方、OFF を指定した場合は、有効な VLAN でありさえすれば認証をパスする。ただし、2 番目以降の Supplicant は、実際には最初に認証をパスした Supplicant と同じ VLAN の所属となる。本パラメーターは、Multi-Supplicant モード (MODE=MULTI) のポートか、MAC ベース認証のポートでのみ使用可能。デフォルトは ON。

VLANASSIGNMENT (802.1X Authenticator ポート、MAC ベース認証ポート) ダイナミック VLAN の有効・無効。有効時は、RADIUS サーバーが返してきた Tunnel-Private-Group-ID の値をもとに、指定ポートの所属 VLAN を動的に変更する。デフォルトは ENABLED。

MIBRESET (802.1X Multi-Supplicant Authenticator ポート、MAC ベース認証ポート) 802.1X 認証の Multi-Supplicant モード (MODE=MULTI) か MAC ベース認証を使用しているポートにおいて、古い Supplicant 情報をエージアウトするかどうか。デフォルトは ENABLED。

TRAP (802.1X Authenticator ポート、MAC ベース認証ポート) ポート認証機能に関する SNMP トラップを送信するかどうか。SUCCESS を指定した場合は、Supplicant の認証に成功したときと、認証情報が時間切れになったときに SNMP トラップを送信する。FAILURE を指定した場合は、Supplicant の認証に失敗したときに SNMP トラップを送信する。BOTH を指定したときは、SUCCESS と FAILURE の両方の場合に SNMP トラップを送信する。NONE はトラップを送信しない。デフォルトは NONE。

DEFAULT 指定した Supplicant 固有のポート認証設定を破棄するときに指定する。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (118 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SET PORTAUTH PORT (313 ページ)

SHOW PORTAUTH (413 ページ)

SHOW PORTAUTH COUNTER (416 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

SHOW PORTAUTH TIMER (428 ページ)

SET PORTAUTH USERNAME

カテゴリー：運用・管理 / ポート認証

SET PORTAUTH [=8021X] **USERNAME**=*login-name* **PASSWORD**=*password* [METHOD={OTP
[ENCRYPTION={MD4|MD5}]|STANDARD}]

login-name: ログイン名 (1～64 文字。英数字のみ使用可能。大文字小文字を区別しない)

password: パスワード (文字数は認証方式によって異なる。英数字のみ使用可能。大文字小文字を区別する)

解説

Supplicant 時に使用するグローバルなユーザー名、パスワード、パスワード暗号化方式およびアルゴリズムを設定する。

本コマンドで設定するのは、Supplicant ポート固有のユーザー名、パスワードが設定されていないときに使用するグローバル値。ENABLE PORTAUTH PORT コマンド、SET PORTAUTH PORT コマンドで Supplicant ポート固有のユーザー名が設定されているときは、本コマンドで設定した値ではなく、Supplicant ポート固有の設定値が使用される。

パラメーター

PORTAUTH 認証メカニズム。本コマンドでは 8021X (802.1X 認証) のみ有効。省略時は 8021X と見なされるため、特に指定する必要はない。

USERNAME 認証を受けるためのユーザー名。デフォルトは portAuthportAuth

PASSWORD 認証を受けるためのパスワード。METHOD パラメーターに STANDARD を指定した場合は、6～63 文字の文字列を指定する。METHOD パラメーターに OTP を指定した場合は、10～63 文字の文字列 (認証サーバー上で設定した OTP Initialisation Password と同じ値) を指定する。デフォルトは portAuthportAuth

METHOD パスワード送信時の暗号化方式。STANDARD (EAP-MD5) または OTP (One-Time Password) から選択する。OTP を指定した場合は、ENCRYPTION パラメーターでワンタイムパスワードの生成アルゴリズムも指定する必要がある。デフォルトは STANDARD。

ENCRYPTION ワンタイムパスワードの生成アルゴリズム。MD4、MD5 から選択する。デフォルトは MD5。METHOD パラメーターに OTP を指定した場合の必須パラメーター。

備考・注意事項

パスワードは設定ファイルに平文のまま保存されるため、管理には注意すること。

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (118 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)
SET PORTAUTH PORT (313 ページ)
SET PORTAUTH PORT SUPPLICANTMAC (317 ページ)
SHOW PORTAUTH (413 ページ)
SHOW PORTAUTH COUNTER (416 ページ)
SHOW PORTAUTH PORT (419 ページ)
SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)
SHOW PORTAUTH TIMER (428 ページ)

SET RADIUS

カテゴリー：運用・管理 / 認証サーバー

SET RADIUS [TIMEOUT=1..15] [DEADTIME=0..1440] [RETRANSMITCOUNT=1..5]

解説

RADIUS (Remote Authentication Dial In User Server) サーバーとの通信に使用するパラメーターを変更する。

パラメーター

TIMEOUT RADIUS サーバーへの要求に対する応答待ち時間 (秒)。要求送信後 TIMEOUT 秒以内に応答がない場合はその回の通信がタイムアウトしたと見なす。デフォルトは 6 秒。

DEADTIME RADIUS サーバーへの要求が規定回数 (1 + RETRANSMITCOUNT 回) タイムアウトしたときに、該当サーバーが「使用不可」と見なして同サーバーの使用を抑制する時間 (分)。デフォルトは 0 分 (使用を抑制しない)。

RETRANSMITCOUNT RADIUS サーバーへの要求再送回数。RADIUS サーバーへの要求がタイムアウトしたときは、最大 RETRANSMITCOUNT 回まで再送を試みる。RETRANSMITCOUNT 回再送しても応答がなかった場合は、該当 RADIUS サーバーが「使用不可」と見なして、認証サーバーリスト内の次のサーバーに要求を送信する。また、「使用不可」と見なしたサーバーの使用を、DEADTIME (分) の間だけ抑制する。デフォルトは 3 回。

備考・注意事項

DEADTIME パラメーターのデフォルト値は 0 分だが、この場合無応答のサーバーに対しても毎回要求を送信する。このため、認証サーバーリストの先頭に登録されている RADIUS サーバーが応答しない場合、毎回このサーバーの応答がタイムアウトするまで待つこととなり、結果として認証時間が長くなる。これを回避するには、DEADTIME パラメーターの値を 1 分以上の適切な値に設定すること。

関連コマンド

ADD RADIUS SERVER (131 ページ)

SHOW RADIUS (431 ページ)

SET SCRIPT

カテゴリー：運用・管理 / スクリプト

```
SET SCRIPT=filename LINE=line-num [AFTER=line-num] [BEFORE=line-num]
[TEXT=string]
```

filename: ファイル名 (拡張子は.scp か.cfg)

line-num: 行番号 (1 ~)

string: 文字列 (1 ~ 127 文字)

解説

スクリプトファイル内の行を変更する。

指定行の内容を変更したり、指定行を他の行と入れ替えたりできる。

パラメーター

SCRIPT スクリプトファイル名

LINE 変更対象の行番号。

AFTER 行番号を指定。LINE で指定した行が、AFTER で指定した行の後ろに移動する

BEFORE 行番号を指定。LINE で指定した行が、BEFORE で指定した行の前に移動する

TEXT 変更後のテキスト

例

basic.scp の 2 行目を「reset ppp=0」に変更する。

```
SET SCRIPT=basic.scp LINE=2 TEXT="reset ppp=0"
```

advanced.scp の 10 行目を現 7 行目の前に移動する。

```
SET SCRIPT=advanced.scp LINE=10 BEFORE=7
```

関連コマンド

ACTIVATE SCRIPT (120 ページ)

ADD SCRIPT (133 ページ)

DEACTIVATE SCRIPT (186 ページ)

DELETE SCRIPT (197 ページ)

SHOW SCRIPT (434 ページ)

SET SNMP ASNBERPADDING

カテゴリー：運用・管理 / SNMP

SET SNMP ASNBERPADDING={ON|YES|TRUE|OFF|NO|FALSE}

解説

SNMP のエンコード方式を設定する。

パラメーター

ASNBERPADDING SNMP マネージャーからの Get 要求に対し、返信する値（カウンター値）が特定の範囲にある場合、カウンター値の先頭 1Byte を省略するかどうかを示す。（特定の範囲とは、2 進数で表記した場合に先頭 9bit が全て 1 となる数値。32bit カウンターの場合は 4286578688 ~ 4294967295。）ON（デフォルト）の場合、カウンター値の先頭 1Byte を省略しない。OFF を指定すると、カウンター値の先頭 1Byte を省略する。ON、YES、TRUE および OFF、NO、FALSE はそれぞれ同じ意味。

SET SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

SET SNMP COMMUNITY=community [ACCESS={READ|WRITE}] [OPEN={ON|OFF|YES|NO|TRUE|FALSE}]

community: SNMP コミュニティ名 (1～15 文字。大文字小文字を区別する)

解説

(SNMPv1/v2c) SNMP コミュニティの設定パラメーターを変更する。

パラメーター

COMMUNITY SNMP コミュニティ名

ACCESS コミュニティのアクセス権を指定する。READ (デフォルト) は読み出し (get、get-next) のみを許可、WRITE は読み書き両方 (get、get-next、set) を許可する。

OPEN SNMP オペレーションをすべてのホストに開放するかどうかを示す。NO (デフォルト) は、MANAGER パラメーターで指定したホストのみに制限することを示す。YES を指定すると、すべての SNMP 要求を受け入れる。ON、YES、TRUE および OFF、NO、FALSE はそれぞれ同じ意味。

関連コマンド

CREATE SNMP COMMUNITY (167 ページ)

DESTROY SNMP COMMUNITY (210 ページ)

SHOW SNMP COMMUNITY (441 ページ)

SET SNMP ENGINEID

カテゴリー：運用・管理 / SNMP

SET SNMP ENGINEID=id

id: SNMP エンジン ID (5~32 バイトの 16 進数)

解説

(SNMPv3) エンジン ID (snmpEngineID) を変更する。
本コマンドを実行すると、定義済みの SNMP ユーザーがすべて削除される (削除前に確認のプロンプトが出る)。

パラメーター

ENGINEID SNMP エンジン ID。5~32 バイトの 16 進数で指定する。すべて 0 の値、および、すべて F の値は使用できない。

備考・注意事項

通常はデフォルトのエンジン ID を使用すればよい。デフォルトのエンジン ID は長さ 11 オクテット (バイトと同義。以下はバイトとする) で、次のようにして生成される。

- (1) 第 1~4 バイトは、弊社のプライベート・エンタープライズ番号「000000CF」(16 進。10 進数では 207) の第 1 バイトの先頭ビットを立てたもので、固定値「800000CF」となる。
- (2) 第 5 バイトは固定値「03」(16 進) で、これは後続の値が MAC アドレスであることを示す。
- (3) 第 6~11 バイトは MAC アドレス。

関連コマンド

SHOW SNMP (437 ページ)

SET SNMP GROUP

カテゴリー：運用・管理 / SNMP

```
SET SNMP GROUP=group SECURITYLEVEL={noAuthNoPriv|authNoPriv|authPriv}  
[READVIEW=view] [WRITEVIEW=view] [NOTIFYVIEW=view]
```

group: SNMP グループ名 (1～32 文字。大文字小文字を区別する)

view: SNMP ビュー名 (1～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ユーザーグループの設定を変更する。

パラメーター

GROUP SNMP グループ名

SECURITYLEVEL 本グループ所属のユーザーに求められる最低限のセキュリティーレベルを指定する。

noAuthNoPriv (認証なし・暗号化なし) authNoPriv (認証あり・暗号化なし) authPriv (認証あり・暗号化あり) から選択する。

READVIEW 本グループ所属のユーザーが読み出せる MIB オブジェクトの範囲 (ビュー) を指定する。

ビューは ADD SNMP VIEW コマンドで定義する。READVIEW の指定がない場合、本グループ所属のユーザーはいかなる MIB オブジェクトも読み出せない。

WRITEVIEW 本グループ所属のユーザーが書き込める MIB オブジェクトの範囲 (ビュー) を指定する。

ビューは ADD SNMP VIEW コマンドで定義する。WRITEVIEW の指定がない場合、本グループ所属のユーザーはいかなる MIB オブジェクトにも書き込めない。

NOTIFYVIEW 本グループ所属のユーザーが受け取れる通知 MIB オブジェクトの範囲 (ビュー) を指定する。

ビューは ADD SNMP VIEW コマンドで定義する。NOTIFYVIEW の指定がない場合、本グループ所属のユーザーはいかなる通知 MIB オブジェクトも受け取れない (通知メッセージが送信されない)。

関連コマンド

ADD SNMP GROUP (136 ページ)

ADD SNMP USER (142 ページ)

ADD SNMP VIEW (144 ページ)

DELETE SNMP GROUP (199 ページ)

SHOW SNMP GROUP (443 ページ)

SHOW SNMP USER (449 ページ)

SHOW SNMP VIEW (451 ページ)

SET SNMP LOCAL

カテゴリー：運用・管理 / SNMP

SET SNMP LOCAL={NONE|1..15} [VERSION={V1|V2|V3|ALL}]

解説

(SNMPv1/v2c/3) SNMP メッセージの送信に使うローカル IP インターフェース (ループバックインターフェース) を指定する。

パラメーター

LOCAL SNMP パケットの送信に使用するローカル IP インターフェースの番号。ローカル IP インターフェースを指定した場合、SNMP パケットの始点 IP アドレスとして、指定したローカル IP インターフェースの IP アドレスが使用される。省略時は NONE (ローカル IP インターフェースを使用しない。この場合、SNMP パケットの始点 IP アドレスはシステムが決める)。

VERSION 対象となる SNMP のバージョン。省略時は ALL (すべてのバージョンが対象)。

関連コマンド

ADD IP LOCAL (「IP」の 188 ページ)

ENABLE SNMP (257 ページ)

SET IP LOCAL (「IP」の 379 ページ)

SHOW IP INTERFACE (「IP」の 478 ページ)

SHOW SNMP (437 ページ)

SET SNMP TARGETADDR

カテゴリー：運用・管理 / SNMP

SET SNMP TARGETADDR=*target* [*PARAMS=params*] [*IP=ipadd*] [*UDP=port*]

target: SNMP ターゲット名 (1~32 文字。大文字小文字を区別する)

params: SNMP ターゲットパラメーターセット名 (1~32 文字。大文字小文字を区別する)

ipadd: IP アドレス

port: UDP ポート番号 (1~255)

解説

(SNMPv3) ターゲット (通知メッセージの送信先) の設定を変更する。

パラメーター

TARGETADDR SNMP ターゲット名

PARAMS SNMP ターゲットパラメーターセット名。ADD SNMP TARGETPARAMS コマンドで定義したパラメーターセットの名前を指定する。

IP ターゲットの IP アドレス

UDP ターゲットのリスニング UDP ポート。1~255 の範囲で指定する。省略時は 162

関連コマンド

ADD SNMP TARGETADDR (138 ページ)

ADD SNMP TARGETPARAMS (140 ページ)

DELETE SNMP TARGETADDR (200 ページ)

SHOW SNMP TARGETADDR (445 ページ)

SHOW SNMP TARGETPARAMS (447 ページ)

SET SNMP TARGETPARAMS

カテゴリー：運用・管理 / SNMP

SET SNMP TARGETPARAMS=*params* [SECURITYLEVEL={noAuthNoPriv|authNoPriv|authPriv}] [USER=*username*]

params: SNMP ターゲットパラメーターセット名 (1～32 文字。大文字小文字を区別する)

username: SNMP ユーザー名 (1～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ターゲット (通知メッセージの送信先) との通信に使用するパラメーターセット (セキュリティレベルとユーザー名) の内容を変更する。

パラメーター

TARGETPARAMS SNMP ターゲットパラメーターセット名

SECURITYLEVEL 本ターゲットパラメーターセットにおいて求められるセキュリティレベルを指定する。noAuthNoPriv (認証なし・暗号化なし) authNoPriv (認証あり・暗号化なし) authPriv (認証あり・暗号化あり) から選択する。USER パラメーターで指定したユーザーのセキュリティレベルと同じレベルを指定すること。

USER SNMP ユーザー名。ADD SNMP USER コマンドで定義したユーザー名を指定する。

関連コマンド

ADD SNMP TARGETPARAMS (140 ページ)

DELETE SNMP TARGETPARAMS (201 ページ)

SHOW SNMP TARGETPARAMS (447 ページ)

SET SNMP TRAPDELAY

カテゴリー：運用・管理 / SNMP

SET SNMP TRAPDELAY=10..600

解説

起動時におけるすべての SNMP トラップを送信するタイミングを設定する。

パラメーター

TRAPDELAY すべての SNMP トラップを送信するタイミングを遅らせる時間(秒)。デフォルトは 10 秒。

SET SNMP USER

カテゴリー：運用・管理 / SNMP

```
SET SNMP USER=username [GROUP=group] [AUTHPROTOCOL={NONE|MD5|SHA}]
    [AUTHPASSWORD=password] [PRIVPROTOCOL={NONE|DES}]
    [PRIVPASSWORD=password]
```

username: SNMP ユーザー名 (1～32 文字。大文字小文字を区別する)

group: SNMP グループ名 (1～32 文字。大文字小文字を区別する)

password: パスワード (8～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ユーザーの設定を変更する。

パラメーター

USER SNMP ユーザー名

GROUP SNMP グループ名。ADD SNMP GROUP コマンドで定義したグループ名を指定する。

AUTHPROTOCOL 認証プロトコル。MD5、SHA、NONE(認証なし)から選択する。省略時は NONE。

AUTHPASSWORD 認証パスワード。AUTHPROTOCOL に MD5 か SHA を指定した場合の必須パラメーター。

PRIVPROTOCOL 暗号化プロトコル。DES、NONE(暗号化なし)から選択する。省略時は NONE。

AUTHPROTOCOL に NONE を指定した場合は、PRIVPROTOCOL にも NONE を指定しなくてはならない(「認証なし・暗号化あり」の組み合わせは認められていないため)。

PRIVPASSWORD 暗号化パスワード。PRIVPROTOCOL に DES を指定した場合の必須パラメーター。

関連コマンド

ADD SNMP USER (142 ページ)

DELETE SNMP USER (202 ページ)

SHOW SNMP USER (449 ページ)

SET SSH SERVER

カテゴリー：運用・管理 / Secure Shell

```
SET SSH SERVER [HOSTKEY=key-id] [SERVERKEY=key-id] [EXPIRYTIME=hours]  
[LOGINTIMEOUT=seconds]
```

key-id: 鍵番号 (0 ~ 65535)

hours: 時間

seconds: 時間 (秒)

解説

SSH サーバー機能の設定を変更する。

パラメーター

HOSTKEY ホスト鍵の鍵番号を指定する。推奨鍵長は 1024 ビット。CREATE ENCO KEY コマンドで作成する (TYPE=RSA)。

SERVERKEY サーバー鍵の鍵番号を指定する。鍵長はホスト鍵より 128 ビット以上短く、なおかつ 512 ビット以上でなくてはならない。CREATE ENCO KEY コマンドで作成する (TYPE=RSA)。

EXPIRYTIME サーバー鍵の有効期間 (時間)。サーバー鍵は、有効期間が過ぎると自動的に更新 (再生成) される。0 は無期限 (自動更新しない) を示す。デフォルトは 0。

LOGINTIMEOUT ログインタイムアウト (秒)。接続確立後、ここで指定した時間内にログインしなかった場合はサーバー側から接続を切断する。デフォルトは 60 秒。

関連コマンド

DISABLE SSH SERVER (228 ページ)

ENABLE SSH SERVER (261 ページ)

SHOW SSH (453 ページ)

SET SSH USER

カテゴリー：運用・管理 / Secure Shell

```
SET SSH USER=username {PASSWORD=password|KEYID=key-id} [IPADDRESS=ipadd]  
[MASK=ipadd]
```

username: ユーザー名 (1～15 文字。英数字。空白不可)

password: パスワード (1～31 文字)

key-id: 鍵番号 (0～65535)

ipadd: IP アドレスまたはネットマスク

解説

SSH ユーザーの設定を変更する。

パラメーター

USER SSH ユーザー名。

PASSWORD SSH パスワード。パスワード認証を使用するときに指定する。ユーザー認証データベースのパスワードと同じでなくてもよい。KEYID と同時に指定することはできない。

KEYID ユーザーの RSA 公開鍵番号 (CREATE ENCO KEY でインポートしたもの)。RSA 認証を使用するときに指定する。PASSWORD と同時に指定することはできない。

IPADDRESS ログイン元 (SSH クライアント) の IP アドレス。MASK と組み合わせて、ログイン元を制限するときに使う。デフォルトでは制限なし。

MASK ネットマスク。IPADDRESS パラメーターと組み合わせて、ログイン元ホストを制限するときに使う。

関連コマンド

ADD SSH USER (147 ページ)

DELETE SSH USER (204 ページ)

SHOW SSH USER (462 ページ)

SET SYSTEM CONTACT

カテゴリー：運用・管理 / システム

SET SYSTEM CONTACT=string

string: 文字列 (1~255 文字。使用可能な文字は半角英数字、半角記号 (!"#\$%&'()*+,-./:;<=>@[\\]>^_`{|}~ 半角空白。文字列の先頭にダブルクォートを使用することはできない。また、文字列に空白を含む場合は、前後をダブルクォート(")で囲む必要がある。この場合、文字列中にダブルクォートを含んではならない。また、半角記号の ? は使用できない)

解説

システムの管理責任者を示す MIB オブジェクト sysContact の値を設定する。

パラメーター

CONTACT システム管理責任者名 (sysContact)

例

sysContact を設定する。

```
SET SYSTEM CONTACT="admin@1sys.mydomain.xxx"
```

関連コマンド

SET SYSTEM LOCATION (337 ページ)

SET SYSTEM NAME (338 ページ)

SHOW SYSTEM (465 ページ)

SET SYSTEM DISTINGUISHEDNAME

カテゴリー：運用・管理 / システム

SET SYSTEM DISTINGUISHEDNAME={*dist-name*|NONE}

dist-name: X.500 識別名 (DN) ("cn=myname,o=myorg,c=jp" の形式)

解説

PKI、ISAKMP で使用する X.500 識別名 (DN) を設定する。

パラメーター

DISTINGUISHEDNAME X.500 識別名 (DN)。LDAP の各種属性値をカンマで区切って列挙したもの。
cn (Common Name) o (Organization) c (Country) などの属性値は小文字で記述する必要がある。

例

識別名として「cn=pote,o=orange,c=jp」を設定する

```
SET SYSTEM DISTINGUISHEDNAME="cn=pote,o=orange,c=jp"
```

関連コマンド

CREATE PKI ENROLLMENTREQUEST (「PKI」の 18 ページ)

SHOW SYSTEM (465 ページ)

SET SYSTEM LOCATION

カテゴリー：運用・管理 / システム

SET SYSTEM LOCATION=string

string: 文字列 (1～255 文字。使用可能な文字は半角英数字、半角記号 (!"#\$%&'()*+,-./:;<=>@[\\]>^_`{|}~ 半角空白。文字列の先頭にダブルクォートを使用することはできない。また、文字列に空白を含む場合は、前後をダブルクォート(")で囲む必要がある。この場合、文字列中にダブルクォートを含んではならない。また、半角記号の ? は使用できない)

解説

システムの設置場所を示す MIB オブジェクト sysLocation の値を設定する。

パラメーター

LOCATION システム設置場所 (sysLocation)

例

sysLocation を設定する。

```
SET SYSTEM LOCATION="8F, TTT Bldg."
```

関連コマンド

SET SYSTEM CONTACT (335 ページ)

SET SYSTEM NAME (338 ページ)

SHOW SYSTEM (465 ページ)

SET SYSTEM NAME

カテゴリー：運用・管理 / システム

SET SYSTEM NAME=string

string: 文字列（1～245 文字。使用可能な文字は半角英数字、半角記号（! " # \$ % & ' () * + , - . / : ; < = > @ [\] ^ _ ' { | } ） 半角空白。文字列の先頭にダブルクォートを使用することはできない。また、文字列に空白を含む場合は、前後をダブルクォート（"）で囲む必要がある。この場合、文字列中にダブルクォートを含んではならない。また、半角記号の ? は使用できない）

解説

システムの名称を示す MIB オブジェクト sysName の値を設定する。

パラメーター

NAME システム名（sysName）。設定したシステム名はプロンプトの先頭に表示される。

例

sysName を設定する。

```
SET SYSTEM NAME="white.mydomain.xxx"
```

備考・注意事項

sysName にルーターのフルドメイン名（ホスト名を含む完全なドメイン名）を設定しておく、ドットを含まないホスト名の IP アドレスを DNS で検索する際に、「フルドメイン名から先頭要素（最初のドットまで）を取り除いたもの」を検索対象ホスト名に付加する。たとえば、sysName に「myrouter.mydomain.xx.jp」を設定している場合、「TELNET hispc」というコマンドを実行すると、「hispc.mydomain.xx.jp」に対して DNS の検索が行われる。

また、DHCP クライアント機能を使う場合、sysName の内容が DHCP Discover/Request メッセージの HostName フィールドに設定されて送信される。DHCP で IP アドレスを配布する ISP の中には、HostName によってクライアントを識別/認証しているところがある。その場合は、本コマンドで ISP から指定されたホスト名を設定する必要がある。

関連コマンド

SET SYSTEM CONTACT (335 ページ)

SET SYSTEM LOCATION (337 ページ)

SHOW SYSTEM (465 ページ)

SET SYSTEM TERRITORY

カテゴリー：運用・管理 / システム

SET SYSTEM TERRITORY={AUSTRALIA|CHINA|EUROPE|JAPAN|KOREA|NEWZEALAND|USA}

解説

製品を使用する地域を設定する。この情報は、Q931、PRI モジュールが地域に適したデフォルト値を設定するために用いる。デフォルトは JAPAN

パラメーター

TERRITORY 地域

備考・注意事項

通常変更する必要はない。

関連コマンド

SET PRI (「インターフェース」の 57 ページ)

SET Q931 (「ISDN」の 41 ページ)

SET SYSTEM CONTACT (335 ページ)

SET SYSTEM LOCATION (337 ページ)

SET SYSTEM NAME (338 ページ)

SHOW PRI CONFIGURATION (「インターフェース」の 93 ページ)

SHOW PRI STATE (「インターフェース」の 100 ページ)

SHOW Q931 (「ISDN」の 59 ページ)

SHOW SYSTEM (465 ページ)

SET TELNET

カテゴリー：運用・管理 / ターミナルサービス

SET TELNET [TERMTYPE=*string*] [INSERTNULL={ON|OFF}] [LISTENPORT=*port*]
[MAXSESSIONS={1-32}]

string: 文字列 (1~31 文字。空白を含む場合はダブルクォートで囲む)

port: TCP ポート番号 (1~65535)

解説

Telnet クライアント、Telnet サーバー機能の設定を変更する。

パラメーター

TERMTYPE Telnet サーバーへの接続時に送信する端末タイプ文字列。デフォルトでは UNKNOWN が送られる。

INSERTNULL CR のあとにヌル文字を挿入するかどうか。デフォルトは OFF。

LISTENPORT Telnet サーバーのリスニング TCP ポート。デフォルトは 23

MAXSESSIONS 同時接続可能な Telnet セッション数。ここで設定した値のセッション数になると、次に張ろうとするセッションが破棄される。また、設定する際に確立されているセッション数以下の値は設定できない。デフォルトは 32。

関連コマンド

ENABLE TELNET SERVER (264 ページ)

SHOW TELNET (468 ページ)

TELNET (486 ページ)

SET TIME

カテゴリー：運用・管理 / システム

SET [TIME=*time*] [DATE=*date*]

time: 時刻 (hh:mm:ss の形式。hh は時 (0~23) mm は分 (0~59) ss は秒 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31) mmm は月 (英語月名の頭3文字。例: APR) yyyy は西暦年)

解説

内蔵時計の日付と時刻を設定する。

パラメーター

TIME 時刻

DATE 日付

例

システム時計を 2001 年 8 月 9 日 19 時に設定する。

```
SET DATE=9-Aug-2001 TIME=19:00:00
```

時刻だけを修正する。

```
SET TIME=19:02:00
```

備考・注意事項

NTP を使って時刻を正確に保つこともできる。

関連コマンド

ADD NTP PEER (130 ページ)

SHOW TIME (469 ページ)

SET TRIGGER CPU

カテゴリー：運用・管理 / トリガー

```
SET TRIGGER=trigger-id [CPU [=1..100]] [DIRECTION={UP|DOWN|ANY}]
    [AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]
    [REPEAT={YES|NO|ONCE|FOREVER|count}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

解説

CPU トリガーの設定パラメーターを変更する。

パラメーター

TRIGGER トリガー番号

CPU しきい値。CPU 負荷率をパーセンテージで指定する。

DIRECTION 起動条件。UP (しきい値まで上がるか上回ったとき)、DOWN (しきい値まで下がるか下回ったとき)、ANY (両方) から選択する。デフォルトは ANY。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実

行される。デフォルトは NO。

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

CREATE TRIGGER CPU (169 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SHOW TRIGGER (470 ページ)

SET TRIGGER FIREWALL

カテゴリー：運用・管理 / トリガー

```
SET TRIGGER=trigger-id [FIREWALL [= {ALL|DOSATTACK|FRAGATTACK|HOSTSCAN|
PORTSCAN|SMURFATTACK|SYNATTACK|TCPATTACK}]] [MODE= {START|END|BOTH}]
[AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]
[REPEAT= {YES|NO|ONCE|FOREVER|count}] [TEST= {YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

解説

ファイアウォールトリガーの設定パラメーターを変更する。

パラメーター

TRIGGER トリガー番号

FIREWALL ファイアウォールの攻撃イベント名。指定した攻撃イベントの発生時にトリガーが起動される。MODE パラメーターと組み合わせることにより、より細かい指定が可能。

MODE 攻撃のどのタイミングでトリガーを起動させるかを指定する。START は攻撃開始時、END は攻撃終了時、BOTH は攻撃開始時と攻撃終了時にトリガーを起動する。デフォルトは BOTH。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返すを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT バ

ラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

CREATE TRIGGER FIREWALL (171 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SHOW TRIGGER (470 ページ)

SET TRIGGER INTERFACE

カテゴリー：運用・管理 / トリガー

```
SET TRIGGER=trigger-id [INTERFACE=interface] EVENT={UP|DOWN|FAIL|ANY}
[CP={BCP|CCP|IPCP|LCP}] [AFTER=time] [BEFORE=time] [{DATE=date|
```

```
DAYS=day-list}] [NAME=string] [REPEAT={YES|NO|ONCE|FOREVER|count}}]
```

```
[TEST={YES|NO|ON|OFF}}]
```

trigger-id: トリガー番号 (1~250)

interface: インターフェース名

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

解説

インターフェーストリガーの設定パラメーターを変更する。

パラメーター

TRIGGER トリガー番号

INTERFACE 監視するインターフェース名を指定する。指定できるのは、Ethernet インターフェース (ethX)、VLAN インターフェース (vlanX)、PPP インターフェース (pppX) のみ。PPP インターフェースの場合は、CP パラメーターも指定可能。

EVENT 該当インターフェースのリンクステータスがどのように変化した場合にトリガーを起動させるかを指定する。UP はリンクアップ時、DOWN はリンクダウン時、FAIL はリンクアップ失敗時、ANY はすべてのリンクステータス変化時を意味する。Ethernet、VLAN インターフェースでは、UP と DOWN のみ有効。

CP 監視する PPP コントロールプロトコルを指定する。INTERFACE に PPP インターフェースを指定した場合にのみ有効。トリガースクリプトには、%1 (PPP インターフェース名)、%2 (コントロールプロトコル)、%3 (イベント名) の3つの引数が渡される。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL

はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

CREATE TRIGGER INTERFACE (173 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SHOW TRIGGER (470 ページ)

SET TRIGGER MEMORY

カテゴリー：運用・管理 / トリガー

```
SET TRIGGER=trigger-id [MEMORY [=1..100]] [DIRECTION={UP|DOWN|ANY}]
[AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]
[REPEAT={YES|NO|ONCE|FOREVER|count}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

解説

メモリートリガーの設定パラメーターを変更する。

パラメーター

TRIGGER トリガー番号

MEMORY しきい値。空きメモリー容量をパーセンテージで指定する。

DIRECTION 起動条件。UP (しきい値まで上がるか上回ったとき)、DOWN (しきい値まで下がるか下回ったとき)、ANY (両方) から選択する。デフォルトは ANY。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実

行される。デフォルトは NO。

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

CREATE TRIGGER MEMORY (175 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SHOW TRIGGER (470 ページ)

SET TRIGGER MODULE

カテゴリー：運用・管理 / トリガー

```
SET TRIGGER=trigger-id [MODULE] [module-parameters...] [AFTER=time]
[BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string] [REPEAT={YES|NO|
ONCE|FOREVER|count}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

module-parameters: モジュール独自のパラメーター

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

解説

モジュールトリガーの設定パラメーターを変更する。

パラメーター

TRIGGER トリガー番号

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

関連コマンド

ACTIVATE TRIGGER (121 ページ)
ADD TRIGGER (149 ページ)
CREATE TRIGGER MODULE (177 ページ)
DESTROY TRIGGER (211 ページ)
DISABLE TRIGGER (232 ページ)
ENABLE TRIGGER (265 ページ)
SHOW TRIGGER (470 ページ)

SET TRIGGER PERIODIC

カテゴリー：運用・管理 / トリガー

```
SET TRIGGER=trigger-id [PERIODIC [=minutes]] [{DATE=date|DAYS=day-list}]
[AFTER=time] [BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string]
[REPEAT={YES|NO|ONCE|FOREVER|count}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

minutes: 時間 (1~1439 分)

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31) mmm は月 (英語月名の頭 3 文字。例: APR) yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

time: 時刻 (hh:mm の形式。hh は時 (0~23) mm は分 (0~59))

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

解説

定期トリガーの設定パラメーターを変更する。

パラメーター

TRIGGER トリガー番号

PERIODIC トリガーの起動間隔を分で指定する。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)

CREATE TRIGGER PERIODIC (180 ページ)

DESTROY TRIGGER (211 ページ)

DISABLE TRIGGER (232 ページ)

ENABLE TRIGGER (265 ページ)

SHOW TRIGGER (470 ページ)

SET TRIGGER REBOOT

カテゴリー：運用・管理 / トリガー

```
SET TRIGGER=trigger-id [REBOOT[={RESTART|CRASH|ALL}]] [AFTER=time]
[BEFORE=time] [{DATE=date|DAYS=day-list}] [NAME=string] [REPEAT={YES|NO|
ONCE|FOREVER|count}] [TEST={YES|NO|ON|OFF}]
```

trigger-id: トリガー番号 (1~250)

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

解説

再起動トリガーの設定パラメーターを変更する。

パラメーター

TRIGGER トリガー番号

REBOOT トリガーの起動条件となる再起動イベントを指定する。CRASH はクラッシュによる再起動、RESTART はクラッシュ以外の原因による再起動を意味する。ALL はすべての再起動を示す。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

AFTER 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、AFTER で指定した時刻から深夜 24 時までの間だけ有効となる。

BEFORE 一日のうちトリガーが有効な時間を制限するパラメーター。トリガーは、深夜 0 時から BEFORE で指定した時刻までの間だけ有効となる。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

関連コマンド

ACTIVATE TRIGGER (121 ページ)
ADD TRIGGER (149 ページ)
CREATE TRIGGER REBOOT (182 ページ)
DESTROY TRIGGER (211 ページ)
DISABLE TRIGGER (232 ページ)
ENABLE TRIGGER (265 ページ)
SHOW TRIGGER (470 ページ)

SET TRIGGER TIME

カテゴリー：運用・管理 / トリガー

```
SET TRIGGER=trigger-id [TIME[=time]] [{DATE=date|DAYS=day-list}]
[NAME=string] [REPEAT={YES|NO|ONCE|FOREVER|count}] [TEST={YES|NO|ON|
OFF}]
```

trigger-id: トリガー番号 (1~250)

time: 時刻 (hh:mm の形式。hh は時 (0~23)、mm は分 (0~59))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31)、mmm は月 (英語月名の頭3文字。例: APR)、yyyy は西暦年)

day-list: 曜日リスト (MON、TUE、WED、THU、FRI、SAT、SUN、WEEKDAY、WEEKEND、ALL の組み合わせ。複数指定時はカンマで区切る)

string: 文字列 (1~40 文字。空白を含む場合はダブルクォートで囲む)

count: 回数 (1~4294967294)

解説

定時トリガーの設定パラメーターを変更する。

パラメーター

TRIGGER トリガー番号

TIME トリガーの起動時刻を指定する。分まで指定できるが、前後約5秒の誤差がある。一般的には指定時刻の5秒後に起動されることが多い。

DATE 一年のうちトリガーが有効な日を一日だけに制限するパラメーター。DAYS と同時には指定できない。

DAYS 一週間のうちトリガーが有効な日を制限するパラメーター。カンマ区切りで複数曜日を指定可能。WEEKDAY は MON,TUE,WED,THU,FRI と同義。また、WEEKEND は SAT,SUN と同義。ALL はすべての曜日。デフォルトは ALL。DATE と同時には指定できない。

NAME トリガー名。SHOW TRIGGER コマンドで表示されるもので、メモとして使う。

REPEAT トリガーを一度だけ実行するか、それとも、何度でも繰り返し実行するかを指定する。繰り返しを許す場合は、繰り返しの限度も指定できる。YES と FOREVER は同義で、実行回数に制限を設けないことを示す。NO と ONCE は同義で、一回だけしか実行を許可しないことを示す。回数を指定した場合は、指定回数まで実行を許可する。デフォルトは FOREVER。

TEST トリガーをテストモードにするかどうか。テストモードのトリガーは起動されても、SCRIPT パラメーターで指定したスクリプトを実行せず、ログにトリガーの起動を記録するだけ。ただし、ACTIVATE TRIGGER コマンドで手動起動された場合は、テストモードであってもスクリプトが実行される。デフォルトは NO。

関連コマンド

ACTIVATE TRIGGER (121 ページ)

ADD TRIGGER (149 ページ)
CREATE TRIGGER TIME (184 ページ)
DESTROY TRIGGER (211 ページ)
DISABLE TRIGGER (232 ページ)
ENABLE TRIGGER (265 ページ)
SHOW TRIGGER (470 ページ)

SET TTY

カテゴリー：運用・管理 / ターミナルサービス

```
SET TTY [HISTORY=0..99] [PAGE=4..99] [PROMPT={string|DEFAULT|OFF}]
[TYPE={DUMB|VT100}]
```

string: 文字列（1～15 文字。空白を含む場合はダブルクォートで囲む）

解説

外部からの Telnet 接続時に動的作成される仮想端末デバイス（TTY）のデフォルト属性値を設定する。

パラメーター

HISTORY コマンドバッファに保存するコマンド履歴の最大数を 0～99 の範囲で指定する。HISTORY パラメーターにゼロをセットしても、すでに存在するコマンド履歴は消去されない。コマンド履歴を削除するには、RESET ASYN HISTORY コマンドを使う。デフォルトは 30。

PAGE 端末の 1 画面当たり行数を 4～99 の範囲で指定する。デフォルトは 22。OFF を指定した場合は、ページ単位での一時停止が行われなくなる。

PROMPT プロンプト文字列。DEFAULT を指定するとデフォルトに戻る。

TYPE 非同期ポートに接続する端末の種類。VT100 を指定した場合、標準的な VT100 エスケープシーケンスが使用される。DUMB に設定した場合は、VT100 エスケープシーケンスを使用せず、ダム端末モードで動作する。デフォルトは VT100。

関連コマンド

SET ASYN（「インターフェース」の 50 ページ）

SHOW ASYN（「インターフェース」の 65 ページ）

SHOW TTY（475 ページ）

SET USER

カテゴリー：運用・管理 / ユーザー認証データベース

```
SET USER=login-name [LOGIN={TRUE|FALSE|ON|OFF|YES|NO}]
[DESCRIPTION=string] [PASSWORD=password] [PRIVILEGE={USER|MANAGER|
SECURITYOFFICER}] [TELNET={YES|NO}] [IPADDRESS=ipadd] [NETMASK=ipadd]
[MTU=40..1500]
```

```
SET USER [LOGIN={TRUE|FALSE|ON|OFF|YES|NO}] [LOGINFAIL=1..10]
[LOCKOUTPD=1..30000] [MANPWDFAIL=1..5] [SECUREDELAY=10..3600]
[MINPWDLEN=1..23]
```

login-name: ログイン名(1～64文字。大文字小文字を区別しない。空白不可。入力可能文字:!#\$%&'()*+,-./0123456789;<=>@ABCDEFGHI

password: パスワード(1～32文字。大文字小文字を区別する。空白を使用する場合、全体をダブルクォーテーション(" ")で

囲む。入力可能文字:!#\$%&'()*+,-./0123456789;<=>@ABCDEFGHIJKLMNPOQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}

string: 文字列(1～24文字)

ipadd: IP アドレスまたはネットマスク

解説

登録ユーザーの情報を変更する(ユーザー名を指定したとき)。あるいは、ユーザー認証データベースのグローバル設定パラメーターを変更する(ユーザー名を指定しなかったとき)。

パラメーター

USER ログイン名。大文字小文字を区別しない。ログイン名を指定したときは、該当ユーザーの設定を変更する。ログイン名を指定しなかったときは、ユーザー認証データベースのグローバル設定を変更する。

LOGIN USER(一般ユーザー)レベルのユーザーにコマンドラインインターフェースへのログインを許可かどうか。ユーザーレベルがMANAGER/SECURITYOFFICERのユーザーにもログインを許可しないよう設定できるため注意が必要。USERパラメーターでログイン名を指定しなかった場合は、現在登録されているUSERレベルの全ユーザーのLOGINパラメーターが変更される。

DESCRIPTION ユーザーに関するコメント

PASSWORD パスワード。大文字小文字を区別する。デフォルトは6文字以上のパスワードを設定する必要がある。

PRIVILEGE ユーザーレベル。一般ユーザー(USER)、管理者(MANAGER)、Security Officer(SECURITYOFFICER)から選択する。

TELNET 別ホストへのTelnetを許可かどうか。ログインしたユーザーにTELNETコマンドを使用させるかどうかを指定する。

IPADDRESS ユーザーに割り当てるIPアドレス。NETMASKと組で指定する。

NETMASK ユーザーが使用するネットマスク。IPADDRESSと組で指定する。

MTU ユーザーのMTU値を40～1500の範囲で指定する。

LOGINFAIL 連続したログイン失敗の最大数。デフォルトは5回。コンソールターミナルで LOGINFAIL 回連続してログインに失敗すると、次のログインプロンプトが表示されるまで LOCKOUTPD 秒待たされる。Telnet 接続時はセッションが切断され、該当ホストからの Telnet 接続が LOCKOUTPD 秒間拒否される。

LOCKOUTPD LOGINFAIL 回連続してログインに失敗した場合に、次のログインプロンプトを表示するまでの待機時間（秒）。Telnet 接続でのログイン連続失敗時は該当ホストからの Telnet 接続を拒否する時間。デフォルトは 600 秒。

MANPWDFAIL セキュリティコマンド（ADD USER コマンド、DELETE USER コマンド、PURGE USER コマンド、SET MANAGER ASYN コマンド、SET USER コマンド）入力時のパスワード入力で失敗が許される最大回数。デフォルトは 3。

SECUREDELAY セキュリティコマンドのタイムアウト。デフォルトは 60 秒。

MINPWDLEN パスワードの最小文字数。デフォルトは 6 文字。

例

ユーザー secadmin のパスワードを変更する。

```
SET USER=secadmin PASSWORD=newpass
```

10 文字よりも短いパスワードを設定できないようにする。

```
SET USER MINPWDLEN=10
```

関連コマンド

ADD USER (151 ページ)

DELETE USER (206 ページ)

DISABLE SYSTEM SECURITY_MODE (230 ページ)

DISABLE USER (233 ページ)

ENABLE SYSTEM SECURITY_MODE (263 ページ)

ENABLE USER (266 ページ)

PURGE USER (284 ページ)

RESET USER (292 ページ)

SHOW USER (478 ページ)

SHOW ALIAS

カテゴリー：運用・管理 / コマンドプロセッサ

SHOW ALIAS

解説

定義済みエイリアスの一覧を表示する。

入力・出力・画面例

```
Manager > show alias
Alias ..... ls
  String .... show file

Alias ..... mv
  String .... rename
```

関連コマンド

ADD ALIAS (122 ページ)

DELETE ALIAS (187 ページ)

SHOW BUFFER

カテゴリー：運用・管理 / システム

SHOW BUFFER

解説

搭載メモリー、空きメモリーなどの情報を表示する。

入力・出力・画面例

```
Manager > show buffer

Memory ( DRAM ) ..... 65536 kB
Free Memory ..... 77 %
Free fast buffers ..... 0
Total fast buffers ..... 0
Free buffers ..... 25094
Total buffers ..... 26668
Buffer level 3 ..... 125   (don't process input frames)
Buffer level 2 ..... 250   (don't do monitor or command output)
Buffer level 1 ..... 500   (don't buffer up log messages)
Buffer level 0 ..... 1500  (warning via snmp trap)
```

| | |
|--------------------|---|
| Memory (DRAM) | 実装されている DRAM メモリーの総容量 |
|) | |
| Free Memory | DRAM メモリーの空き (%) |
| Free fast buffer | 未使用の高速メモリーバッファ数。この値が 0 であっても、通常のメモリーバッファ (Free buffers) が空いていれば問題ない |
| Total fast buffer | 高速メモリーバッファの総数。高速メモリーバッファは、DRAM 上の特定領域に確保されたバッファで、他の領域に確保されたバッファよりも高速なアクセスが可能。ロードされたリリースファイルやパッチファイルの大きさによって、高速メモリーバッファの総数は変動する。また、高速メモリーバッファを使用できない機種もある (その場合、Total fast buffer は 0 となる) |
| Free buffers | 未使用のメモリーバッファ数 |
| Total Free buffers | メモリーバッファの総数 |
| Buffer level n | 未使用のメモリーバッファ数が、各レベルで指定した数以下になると、カッコ内に表示されている処理を停止する |

表 37:

SHOW CONFIG

カテゴリー：運用・管理 / コンフィグレーション

SHOW CONFIG [DYNAMIC [=module-name]]

module-name: モジュール名

解説

起動時設定ファイル名を表示する。また、DYNAMIC オプションを指定した場合は、現在の設定内容（メモリー上の設定内容）を設定ファイルと同じ形式で表示する。

パラメーター

DYNAMIC 現在の設定内容を設定スクリプトの形式で表示する。モジュール名を指定した場合（例：SHOW CONFIG DYNAMIC=IP）は、該当モジュールの設定だけが表示される。

入力・出力・画面例

```
Manager > show config

Boot configuration file: flash:ispsfw.cfg (exists)
Current configuration: flash:ispsfw.cfg

Manager > show config dynamic=firewall

#
# FIREWALL configuration
#
enable firewall
create firewall policy="net"
disable firewall policy="net" identproxy
enable firewall policy="net" log=inal,inde
enable firewall policy="net" icmp_f=all
add firewall policy="net" int=vlan1 type=private
add firewall policy="net" int=ppp0 type=public
add firewall poli="net" nat=enhanced int=vlan1 gblin=ppp0
```

| | |
|-------------------------|--|
| Boot configuration file | 起動時設定ファイル名（カッコ内は該当ファイルが存在しているかどうか）。 起動時設定ファイルが設定されていないときは、「Not set」と表示される |
| Current Configuration | 最後の（再）起動時に読み込んだ設定ファイル名 |

表 38:

関連コマンド

CREATE CONFIG (158 ページ)

RESTART (293 ページ)

SET CONFIG (295 ページ)

SHOW CPU

カテゴリー：運用・管理 / システム

SHOW CPU

解説

CPU の使用状況を表示する。

入力・出力・画面例

```
Manager > show cpu

CPU Utilisation ( as a percentage )
-----
Maximum since router restarted ..... 31
Maximum over last 5 minutes ..... 31
Average since router restarted ..... 5
Average over last 5 minutes ..... 5
Average over last minute ..... 4
Average over last 10 seconds ..... 5
Average over last second ..... 13
-----
```

| | |
|--------------------------------|----------------|
| Maximum since router restarted | 最大負荷率 |
| Maximum over last 5 minutes | 過去 5 分間の最大負荷率 |
| Average since router restarted | 過去 30 分間の平均負荷率 |
| Average over last 5 minutes | 過去 5 分間の平均負荷率 |
| Average over last minute | 過去 1 分間の平均負荷率 |
| Average over last 10 seconds | 過去 10 秒間の平均負荷率 |
| Average over last second | 過去 1 秒間の平均負荷率 |

表 39:

関連コマンド

SHOW BUFFER (362 ページ)

SHOW DEBUG

カテゴリー：運用・管理 / システム

SHOW DEBUG [STACK]

解説

デバッグ情報を表示する。

パラメーター

STACK 前回クラッシュしたときのスタックダンプを表示する。

入力・出力・画面例

```
Manager > show debug stack
-----
This is a PRODUCTION version of code
-----

Router RESTART occurred
Check exception table for restart cause

STACK DUMP
-----

00001260: 00000000 00000580 00000001 00000001
00001270: 00010000 ffffffff 45464748 494a4b4c
00001280: 005c8338 00001034 4d4e4f50 51525354
00001290: 55565758 595a4142 00001449 45462000
000012a0: 20004344 4546c008 43444546 43444546
000012b0: 000e13f8 000a00d6 4748494a 4b4c4d4e
000012c0: 4f505152 53545556 5758595a 41424344
000012d0: 45464748 494a4b4c 4d4e4f50 51525354
000012e0: 55565758 595a4142 43444546 4748494a
000012f0: 4b4c4d4e 4f505152 53545556 5758595a
```

関連コマンド

SHOW EXCEPTION (367 ページ)

SHOW LOG (388 ページ)

SHOW STARTUP (464 ページ)

SHOW SYSTEM (465 ページ)

SHOW EXCEPTION

カテゴリー：運用・管理 / システム

SHOW EXCEPTION

解説

例外発生ログを表示する。

入力・出力・画面例

```

Manager > show exception

Spurious interrupts = 0

Router exception list
-----
No: 01
  Offset/Type : $008/Bus error          Address   : $43444546
  Time        : 12:49:15 on 28-Sep-2001  Clock Log  : 12:48:16 on 28-Sep-2001
  SSW         : $00d6                   Fault Addr : $43444546

No: 02
  Offset/Type : $07c/Watchdog timer      Address   : $002cd46a
  Time        : 12:46:19 on 28-Sep-2001  Clock Log  : 12:45:37 on 28-Sep-2001

No: 03
  Offset/Type : $008/Bus error          Address   : $002d1eda
  Time        : 12:40:40 on 28-Sep-2001  Clock Log  : 12:40:38 on 28-Sep-2001
  SSW         : $0045                   Fault Addr : $51009e18

No: 04
  Offset/Type : $008/Bus error          Address   : $002d1eda
  Time        : 12:34:40 on 28-Sep-2001  Clock Log  : 12:34:22 on 28-Sep-2001
  SSW         : $0045                   Fault Addr : $51009e20

No: 05
  Offset/Type : $008/Bus error          Address   : $002d1eda
  Time        : 12:06:25 on 28-Sep-2001  Clock Log  : 12:06:05 on 28-Sep-2001
  SSW         : $0045                   Fault Addr : $51009e18

No: 06
  Offset/Type : $008/Bus error          Address   : $002d1eda
  Time        : 11:53:09 on 28-Sep-2001  Clock Log  : 11:52:09 on 28-Sep-2001
  SSW         : $0045                   Fault Addr : $51009e18

No: 07

```

SHOW EXCEPTION

| | | | |
|-------------|---------------------------|------------|---------------------------|
| Offset/Type | : \$008/Bus error | Address | : \$002d1eda |
| Time | : 18:44:18 on 19-Sep-2001 | Clock Log | : 18:44:03 on 19-Sep-2001 |
| SSW | : \$0045 | Fault Addr | : \$51009e20 |

SHOW FEATURE

カテゴリー：運用・管理 / ソフトウェア

SHOW FEATURE [= {*featurename* | *index*}]

featurename: フィーチャー名 (1~12 文字)

index: フィーチャー番号 (1~)

解説

フィーチャーライセンスの情報を表示する。

パラメーター

FEATURE フィーチャー名または SHOW FEATURE コマンドで表示されるフィーチャー番号。省略時はすべてのフィーチャーの概要が表示される。指定時は該当フィーチャーの詳細な情報が表示される。

入力・出力・画面例

```
Manager > show feature
```

```
The Special Feature Licences:
```

| Index | FeatureName | Licence | Period |
|-------|-------------|---------|--------|
|-------|-------------|---------|--------|

| | | | |
|---|---------|------|---|
| 1 | FACTORY | full | - |
|---|---------|------|---|

```
The current valid features :
```

```
Triple DES Encryption
```

```
Secure Shell
```

```
FIREWALL
```

```
IPv6
```

```
AES
```

```
Software QoS
```

```
Software QoS on Tunnels
```

| | |
|-------------|--|
| Index | フィーチャーライセンスのインデックス番号 |
| FeatureName | フィーチャー名 |
| Licence | ライセンスの種類。Full (フルライセンス)「password incorrect」(パスワード無効のため使用不可)のいずれか |

| | |
|----------------------------|---------------------------|
| Period | ライセンスの有効期間。フルライセンスの場合は「-」 |
| The current valid features | 本ライセンスにより使用可能な機能の一覧 |

表 40:

関連コマンド

DISABLE FEATURE (212 ページ)

ENABLE FEATURE (242 ページ)

SHOW FFILE

カテゴリー：運用・管理 / 記憶装置とファイルシステム

SHOW FFILE [=filename] [CHECK]

filename: ファイル名（ワイルドカード指定可能）

解説

フラッシュファイルシステム（FFS）上のファイル一覧およびフラッシュメモリーの空き容量などを表示する。

パラメーター

FFILE ファイル名パターン（ワイルドカード）またはファイル名を指定する。省略時はすべてのファイルが表示される。長い名前（28.3 形式）は認識しないので、短い名前（8.3 形式）で指定すること。

CHECK ファイルのチェックサムを照合する。

入力・出力・画面例

```
Manager > show ffile
```

| module | name | type | size | file date & time | address | check |
|--------|----------|------|---------|----------------------|----------|-------|
| | ud | cfg | 579 | 20-Apr-2010 15:51:44 | F800006C | - |
| | 55001d1 | hlp | 74019 | 20-Apr-2010 11:47:20 | F83A12D0 | - |
| | prefer | ins | 64 | 20-Apr-2010 22:05:32 | F83A1008 | - |
| | longname | lfn | 17 | 20-Apr-2010 12:09:10 | F83B5124 | - |
| | random | rnd | 3904 | 20-Apr-2010 12:02:00 | F83B4150 | - |
| | 55001d1 | scp | 3292 | 20-Apr-2010 11:47:46 | F83B3434 | - |
| | snmpengn | sec | 40 | 20-Apr-2010 11:45:40 | F83A1268 | - |
| inst | release | lic | 32 | 20-Apr-2010 22:05:28 | F83A0FA8 | - |
| load | 55290105 | rez | 3804184 | 20-Apr-2010 22:03:51 | F8000350 | - |

```
flash use:
```

```
files ..... 3886820 bytes (9 files)
garbage .... 660 bytes
free ..... 11710088 bytes
block size . 131072 bytes
total ..... 15728640 bytes
```

dev

ファイルが格納されているデバイス名

| | |
|------------------|------------------------------------|
| creator | ファイルの作成者（モジュール名） |
| name | ファイル名（拡張子を除く） |
| type | ファイルタイプ（拡張子） |
| size | ファイルサイズ（バイト） |
| file date & time | ファイル作成日時 |
| address | ファイルの開始アドレス（16 進数） |
| check | データチェックの結果（CHECK オプション指定時にのみ表示される） |
| files | フラッシュメモリー上のファイル占有容量 |
| garbage | フラッシュメモリー上の削除ファイル（ゴミ）占有容量 |
| free | フラッシュメモリーの空き容量 |
| block size | 必要最小ブロックサイズ |
| total | フラッシュメモリーの総容量 |

表 41:

関連コマンド

CREATE FFILE (159 ページ)

DELETE FFILE (188 ページ)

SHOW FILE

カテゴリー：運用・管理 / 記憶装置とファイルシステム

SHOW FILE [=filename]

filename: ファイル名（ワイルドカード指定可能）

解説

ファイルシステム上のファイル一覧、あるいは指定したテキストファイルの内容を表示する。

パラメーター

FILE ファイル名パターン（ワイルドカード）またはファイル名を指定する。省略時はファイル一覧が表示される。パターン指定時は、マッチするファイルの一覧が表示される。ファイル名を指定した場合は、該当ファイルがテキストファイルならその内容が表示される。テキストファイルでない場合は、その旨が表示される。ファイル名（ベース名）部分が8文字を超える長い名前のファイルが存在するときは、本パラメーターに longname.lfn を指定すると、長い名前（28.3 形式）と短い名前（8.3 形式）の対応表が表示される。

入力・出力・画面例

| Manager > show file | | | | | |
|---------------------|--------|---------|----------------------|-------|--|
| Filename | Device | Size | Created | Locks | |
| ----- | | | | ----- | |
| 559122c0.rez | flash | 4151896 | 20-Apr-2010 20:22:59 | 0 | |
| dave55c.rez | flash | 4149372 | 20-Apr-2010 16:32:24 | 0 | |
| feature.lic | flash | 39 | 20-Apr-2010 16:33:31 | 0 | |
| help.hlp | flash | 130804 | 20-Apr-2010 16:33:30 | 0 | |
| longname.lfn | flash | 17 | 20-Apr-2010 16:33:23 | 0 | |
| prefer.ins | flash | 64 | 20-Apr-2010 20:24:29 | 0 | |
| release.lic | flash | 64 | 20-Apr-2010 20:24:23 | 0 | |
| sys14a.cfg | flash | 101 | 20-Apr-2010 20:25:02 | 0 | |
| accsave.acc | nvs | 124 | 20-Apr-2010 09:02:42 | 0 | |
| random.rnd | nvs | 3904 | 20-Apr-2010 08:57:12 | 0 | |
| ----- | | | | ----- | |

| | |
|----------|---------------------------------|
| Filename | ファイル名 |
| Device | ファイルが格納されているデバイス名。flash または nvs |
| Size | ファイルサイズ（バイト） |

| | |
|---------|-------------------|
| Created | ファイル作成日時 |
| Locks | ファイルを使用しているプロセスの数 |

表 42: ファイル一覧の表示項目

例

ファイルシステム上のファイル一覧を表示

```
SHOW FILE
```

設定ファイル (.cfg) の一覧を表示

```
SHOW FILE=* .cfg
```

設定ファイル ip.cfg の内容を表示

```
SHOW FILE=ip.cfg
```

長い名前 (28.3 形式) と短い名前 (8.3 形式) の対応表を表示

```
SHOW FILE=longname.lfn
```

関連コマンド

DELETE FILE (189 ページ)

SHOW FILE PERMANENTREDIRECT

カテゴリー：運用・管理 / 記憶装置とファイルシステム

SHOW FILE [=filename] **PERMANENTREDIRECT**

filename: ファイル名

解説

コマンドやスクリプトの出力を保存（リダイレクト）するため書き込み用にオープンされているファイルの情報を表示する。

ADD FILE コマンドや CREATE FILE コマンドを PERMANENTREDIRECT オプション付きで実行した場合、該当コマンドで指定したファイルは、RESET FILE PERMANENTREDIRECT コマンドを実行するまでオープン（かつロック）されたままの状態となる。本コマンドでは、それらオープン中のファイルを確認できる。

パラメーター

FILE 出力先のテキストファイル名。具体的なファイル名を省略した場合は、オープン中のすべてのファイルが対象となる

入力・出力・画面例

```
Manager > show file permanentredirect

TTY      Current  Limit   File
Instance Size
-----
      17      3451   204800 ipdebug.txt
-----

Manager > show file=ipdebug.txt permanentredirect
File..... ipdebug.txt
TTY Instance.... 17
Current size.... 5439
Limit..... 204800
Input(s)..... COMMAND="enable ip debug=all"
```

| | |
|--------------|------------------|
| TTY Instance | 仮想端末デバイス（TTY）番号 |
| Current Size | ファイルサイズ（バイト） |
| Limit | ファイルサイズの上限值（バイト） |

| File | 出力先ファイル名 |
|------|----------|
|------|----------|

表 43: ファイル名無指定時

| File | 出力先ファイル名 |
|--------------|--|
| TTY Instance | 仮想端末デバイス (TTY) 番号 |
| Current size | ファイルサイズ (バイト) |
| Limit | ファイルサイズの上限值 (バイト) |
| Input(s) | ファイルに出力される情報の出所。ADD FILE コマンド、CREATE FILE コマンドで指定した COMMAND、SCRIPT パラメーターの内容がそのまま表示される |

表 44: ファイル名指定時

例

オープン中のファイル一覧を表示する。

```
SHOW FILE PERMANENTREDIRECT
```

オープン中のファイル ipdebug.txt の情報を表示する。

```
SHOW FILE=ipdebug.txt PERMANENTREDIRECT
```

関連コマンド

ADD FILE (123 ページ)

CREATE FILE (161 ページ)

RESET FILE PERMANENTREDIRECT (287 ページ)

SHOW FILE (374 ページ)

SHOW TTY (475 ページ)

SHOW FLASH

カテゴリー：運用・管理 / 記憶装置とファイルシステム

SHOW FLASH

解説

フラッシュファイルシステム（FFS）に関する情報を表示する。

入力・出力・画面例

```
Manager > show flash

FFS info:
global operation ..... none
flash autowrite ..... disabled
compaction count ..... 35
est compaction time ... 336 seconds
files ..... 14606960 bytes (22 files)
garbage ..... 1600 bytes
free ..... 989008 bytes
required free block ... 131072 bytes
total ..... 15728640 bytes

diagnostic counters:
event      successes      failures
-----
get         0              0
open        0              0
read       35103          0
close      10763          0
complete   31              0
write     473572          0
create     31              0
put         1              0
delete     10              0
check      34              0
erase     112              0
compact     1              0
verify      0              0
-----
```

| | |
|------------------|--|
| global operation | フラッシュに対して実行中の処理。none、restarting、erasing、compacting、verifying のいずれか |
|------------------|--|

| | |
|---------------------|------------------------|
| compaction count | 全消去後のコンパクション実行回数 |
| est compaction time | 現時点におけるコンパクションの推定所要時間 |
| files | ファイルが使用している容量 |
| garbage | 削除されたファイルが使用している容量 |
| free | 未使用容量 |
| required free block | 必要最小ブロックサイズ |
| total | フラッシュの総容量 |
| diagnostic counters | 各種 FFS オペレーションの成功/失敗回数 |

表 45:

関連コマンド

ACTIVATE FLASH COMPACTION (117 ページ)

SHOW FLASH PHYSICAL (380 ページ)

SHOW FLASH PHYSICAL

カテゴリー：運用・管理 / 記憶装置とファイルシステム

SHOW FLASH PHYSICAL

解説

フラッシュメモリーの物理情報を表示する。

入力・出力・画面例

```
Manager > show flash physical
total size ..... 16 MBytes
  available to FFS ... 15 MBytes
  available to boot .. 1 MBytes
device type ..... 28F128
devices ..... 1
location ..... built in
programming power ..... off
block erase time ..... 1000 milliseconds
total erase blocks .... 128
  FFS erase blocks ... 120
  Boot erase blocks .. 8
erase block size ..... 128 kBytes
erase bit state ..... 1
page buffers ..... 1
size of page buffer ... 32 bytes
```

| | |
|---------------------|--|
| total size | 合計容量 |
| available to FFS | フラッシュファイルシステム（FFS）に割り当てられた容量 |
| available to boot | ブートコードに割り当てられた容量 |
| device type | フラッシュデバイスのタイプ |
| devices | フラッシュデバイスの数 |
| location | フラッシュメモリーの実装形態。「SIMM stick」か「built in」 |
| programming power | プログラミングパワーの状態。on か off |
| block erase time | 消去ブロック消去所要時間 |
| total erase blocks | 消去ブロック数 |
| erase block size | 消去ブロックサイズ（バイト） |
| erase bit state | 消去ビットの状態 |
| page buffers | ページバッファ数 |
| size of page buffer | ページバッファサイズ（バイト） |

表 46:

関連コマンド

SHOW FLASH (378 ページ)

SHOW HTTP SERVER

カテゴリー：運用・管理 / システム

SHOW HTTP SERVER

解説

HTTP サーバー（サポート対象外）の設定および状態を表示する。

入力・出力・画面例

```
Manager > show http server

HTTP Server
-----
Status ..... Enabled
SSL Security ..... OFF
SSL Key ID ..... -
Port ..... 80
Listen port ..... Open

Sessions opened ..... 0
Sessions closed ..... 0
Received requests ..... 0
Unknown requests ..... 0
Transmitted replies ..... 0
Aborted replies ..... 0
Transmitted replies on bad session .... 0
Authorisation successes ..... 0
Authorisation failures ..... 0
-----
```

| | |
|-------------------|-----------------------------------|
| Status | HTTP サーバーの状態。Enabled または Disabled |
| SSL Security | 未サポート |
| SSL Key ID | 未サポート |
| Port | 未サポート |
| Listen port | 未サポート |
| Sessions opened | 未サポート |
| Sessions closed | 未サポート |
| Received requests | 未サポート |
| Unknown requests | 未サポート |

| | |
|------------------------------------|-------|
| Transmitted replies | 未サポート |
| Aborted replies | 未サポート |
| Transmitted replies on bad session | 未サポート |
| Authorisation successes | 未サポート |
| Authorisation failures | 未サポート |

表 47:

関連コマンド

DISABLE HTTP SERVER (213 ページ)

ENABLE HTTP SERVER (243 ページ)

SHOW INSTALL

カテゴリー：運用・管理 / ソフトウェア

SHOW INSTALL

解説

インストール（ファームウェア構成）情報を表示する。

入力・出力・画面例

```

Manager > show install

Install      Release                Patch                GUI
-----
Temporary    -                        -                    -
Preferred    flash:559200c1.rez      -                    -
Default      EPROM (55-1.0.7)        -                    -
-----

Current install
-----
Preferred    flash:559200c1.rez      -                    -
-----

Install history
-----
No Temporary release selected
Preferred release selected
Preferred release successfully installed
-----

```

| | |
|-----------------|---|
| Install | インストールの種類。Temporary、Preferred、Default のいずれか |
| Release | リリースファイル |
| Patch | パッチファイル |
| GUI | 未サポート |
| Current install | 現在実行中のファームウェア構成 |
| Install history | 起動時の INSTALL モジュールの動作記録 |

表 48:

関連コマンド

DELETE INSTALL (190 ページ)

SET INSTALL (297 ページ)

SHOW LOADER

カテゴリー：運用・管理 / アップロード・ダウンロード

SHOW LOADER

解説

LOADER モジュールのデフォルト設定値および進行中のファイル転送処理の状態を表示する。

入力・出力・画面例

```
Manager > show loader

Loader Information
-----
Defaults:
  Method ..... TFTP
  File ..... -
  Server ..... -
  HTTP Proxy ..... -
  Proxy Port ..... Default ( 80 )
  Asyn ..... -
  Destination ..... Flash
  Delay (sec) ..... 0

Last Load:
  Method ..... -
  File ..... -
  Destination ..... -
  Delay (sec) ..... 0
  Status ..... Idle
  Last Message ..... -
-----
```

| | |
|--------------|---|
| Defaults | LOAD コマンドおよび UPLOAD コマンドのデフォルト値 |
| Current Load | 現在行われているファイル転送処理のパラメーター値 |
| Last Load | 前回のファイル転送処理で使用されたパラメーター値 |
| Method | 転送プロトコル。TFTP、HTTP (WEB、WWW)、ZMODEM のいずれか |
| File | 転送中のファイル名 |
| Server | サーバーの IP アドレスまたはホスト名 (TFTP または HTTP のときのみ有効) |
| HTTP Proxy | HTTP プロキシの IP アドレスまたはホスト名 (METHOD=HTTP で、プロキシ使用時のみ有効) |

| | |
|--------------|---|
| Proxy Port | HTTP プロキシの TCP ポート番号 (METHOD=HTTP で、プロキシ使用時のみ有効) |
| Asyn | 非同期ポート番号 (METHOD=ZMODEM の場合のみ有効) |
| Destination | ダウンロード先デバイス |
| Delay | コマンド実行から実際にファイル転送処理を開始するまでの時間 (秒) |
| Status | LOADER モジュールの状態。Idle、Waiting、Loading、Load Complete、Load Aborted のいずれか。SHOW LOADER コマンドで「Load Complete」または「Load Aborted」と表示されたあと、もう一度 SHOW LOADER を実行すると、Status は「Idle」になる |
| Load Level | ファイル転送の進行状況 (%)。Status が Loading のときだけ表示される |
| Last Message | 前回のファイル転送処理時のメッセージ。起動直後および転送処理実行中 (Loading) は「-」と表示される |

表 49:

関連コマンド

LOAD (271 ページ)

SET LOADER (298 ページ)

UPLOAD (489 ページ)

SHOW LOG

カテゴリー：運用・管理 / ログ

```
SHOW LOG [=output-id] [DATE=[op]date] [DEVICE=[op]device]
[FILE=[op]filename] [FULL] [MASK=ipadd] [MODULE=[op]module-id] [MSGONLY]
[MSGTEXT=[op]string] [ORIGIN=ipadd] [REFERENCE=[op]string]
[REVERSE=[count]] [SEVERITY=[op]severity] [SOURCELINE=[op]line-num]
[SUBTYPE=[op]subtype-id] [TAIL=[count]] [TIME=[op]time]
[TYPE=[op]type-id] [ZONE={time-zone|utc-offset}]
```

output-id: ログ出力 ID (1~20)

op: 比較演算子 (「<」(小さい) 「>」(大きい) 「!」(等しくない) 「」(等しい) 「%」(以下の文字列を含む))

date: 日付 (dd-mmm-yyyy の形式。dd は日 (1~31) mmm は月 (英語月名の頭3文字。例: APR) yyyy は西暦年)

device: デバイス番号

filename: ファイル名 (1~12 文字)

ipadd: IP アドレスまたはネットマスク

string: 文字列

module-id: モジュール名またはモジュール番号 (0~255)

count: 個数 (1~)

severity: ログレベル (0~7)

line-num: 行番号 (1~)

subtype-id: ログメッセージのサブタイプ名または ID

time: 時刻 (hh:mm:ss の形式。hh は時 (0~23) mm は分 (0~59) ss は秒 (0~59))

type-id: ログメッセージのタイプ名または ID

time-zone: タイムゾーン名

utc-offset: 協定世界時 (UTC) からのオフセット (+23:59:59 ~ -23:59:59)

解説

ログを表示する。各種条件を指定して、表示項目を絞り込むこともできる。

パラメーター

LOG ログ出力先 ID。省略時は TEMPORARY (RAM 上のログ) が表示対象となる。

DATE メッセージの日付。省略時はすべての日付にマッチする。

DEVICE デバイス番号。省略時はすべてのデバイスにマッチする。

FILE 該当モジュールのソースプログラムファイル名 (例: logmain.c)。ソースファイル名は、SHOW LOG コマンドに FULL オプションを付けたときに表示される。省略時はすべてのファイル名にマッチする。

FULL ログメッセージの全フィールドを表示する。各メッセージは空行で区切られる。FULL オプションを付けないときは、各メッセージが簡潔なサマリーモードで表示される。

MASK ネットマスク。メッセージの生成元 IP アドレスを示す ORIGIN パラメーターと組み合わせて使用する。省略時は 255.255.255.255 (単一ホスト)。

MSGONLY ログメッセージのメッセージ本文だけを表示させたいときに指定する。

MSGTEXT メッセージ本文と比較する文字列。省略時はすべてのメッセージにマッチする。スペースを含む文字列を指定する場合は、比較演算子も含めて文字列を「`”`」(ダブルクォーテーション)で囲む。

MODULE モジュール番号またはモジュール名。省略時はすべてのモジュールにマッチする。

ORIGIN ログ生成元の IP アドレス。MASK パラメーターと組み合わせて範囲指定が可能。デフォルトではすべての IP アドレスにマッチする。

REFERENCE メッセージ中のリファレンス。省略時はすべてのリファレンスにマッチする。

REVERSE ログメッセージを逆順(新しい順)に表示する。数値を指定した場合は、最新の REVERSE 個が新しい順に表示される。

SEVERITY メッセージのログレベル。省略時はすべてのログレベルにマッチする。

SOURCELINE メッセージを生成したソースプログラムファイルの行番号。省略時はすべての行にマッチする。

SUBTYPE メッセージのサブタイプ名またはサブタイプ番号。省略時はすべてのサブタイプにマッチする。

TAIL 最新のログメッセージだけを表示する。単に TAIL と指定した場合は最新の 20 メッセージが表示される。値を指定したときは、最新の TAIL 個が表示される。

TIME メッセージの時刻。省略時はすべての時刻にマッチする。

TYPE メッセージのタイプ名またはサブタイプ番号。省略時はすべてのサブタイプにマッチする。

ZONE タイムゾーンを指定する。

入力・出力・画面例

| Manager > show log | | | | | |
|--------------------|---|------|-------|-------|---|
| Date/Time | S | Mod | Type | SType | Message |
| ----- | | | | | |
| 23 15:57:00 | 4 | ENCO | ENCO | PAC | M18X Security Engine Found. |
| 23 15:57:00 | 4 | ENCO | ENCO | PAC | M18X Security Engine Initialised. |
| 23 15:57:00 | 3 | LOG | | | IGMP packet trapping is active for IGMP snooping, L3FILT is activated |
| 23 15:57:00 | 6 | FIRE | FIRE | ENBLD | 23-Mar-2005 15:57:00 Firewall enabled |
| 23 15:57:00 | 4 | ENCO | ENCO | STAC | STAC SW Initialised |
| 23 15:57:00 | 7 | SYS | REST | NORM | Router startup, ver 2.7.1-00, 04-Mar-2005, Clock Log: 15:56:23 on 23-Mar-2005 |
| 23 15:57:00 | 6 | SYS | SYSIN | FAN | Main fan status is not good |
| 23 15:57:02 | 3 | PPP | VINT | UP | ppp0: Interface has come up and is able to send and receive data |
| 23 15:57:02 | 3 | PPP | AUTH | OK | ppp0: CHAP authentication over eth0-any succeeded |
| 23 15:57:02 | 3 | PPP | VINT | UP | ppp1: Interface has come up and is able to send and receive data |
| 23 15:57:02 | 3 | PPP | AUTH | OK | ppp1: CHAP authentication over eth1-any succeeded |
| 23 15:57:02 | 3 | IPG | CIRC | CONF | Remote request to set ppp0 IP to 10.0.0.200 accepted |
| 23 15:57:02 | 3 | IPG | CIRC | CONF | Remote request to set ppp1 IP to 10.0.1.200 accepted |
| 23 15:57:03 | 3 | USER | USER | LON | manager login on port0 |

SHOW LOG

```
23 15:57:06 3 CH MSG WARN No patches found
23 15:58:17 4 FIRE FIRE INDTC TCP 10.100.10.5:1024 10.0.0.200:80
23 15:58:17 4 FIRE FIRE INDTC flow rejected by policy rule
23 15:59:07 6 FIRE FIRE ATTK 23-Mar-2005 15:59:07 Denial of service attack
from 10.100.10.5 is underway
-----
```

| | |
|-----------|------------------------------|
| Date/Time | ログメッセージの生成日時。日付は日（1～31）のみの表示 |
| S | ログメッセージのログレベル |
| Mod | ログを生成したモジュール名 |
| Type | メッセージタイプ |
| SType | メッセージサブタイプ |
| Message | メッセージ本文 |

表 50:

| | |
|------------------|---|
| Date/Time | ログメッセージの生成日時。UTC オフセットを折り込み済み |
| S | ログメッセージのログレベル |
| Mod | ログを生成したモジュール名 |
| Type | メッセージタイプ |
| SType | メッセージサブタイプ |
| Dev | ログメッセージのトリガーとなったデバイス（非同期ポートや TTY セッションなど） |
| Origin | ログメッセージの生成元。Local（自分自身が生成）またはリモートホスト（SRLP や syslog による転送元）の IP アドレス |
| MSGID | メッセージ ID |
| Source File/Line | ログメッセージを生成したモジュールのソースプログラムファイル名と行番号 |
| Ref | ログメッセージの参考情報（Reference）フィールド |
| Flags | ログメッセージの Flags フィールド。LOCTIME、SECURE、CMDOUT がある |
| Message | メッセージ本文 |

表 51: FULL オプション指定時

例

RAM 上のログ（TEMPORARY ログ）を見る

SHOW LOG

最新のファイアウォール関連ログメッセージを見る

SHOW LOG MODULE=FIRE

関連コマンド

PURGE LOG (279 ページ)

SHOW LOG STATUS (402 ページ)

SHOW LOG COUNTER

カテゴリー：運用・管理 / ログ

SHOW LOG COUNTER

解説

ログ機能の診断カウンターを表示する。

入力・出力・画面例

```

Manager > show log counter
Log Counters

Idle loop passes ..... 355
Transmit passes ..... 11

Messages Generated ..... 103

Messages Received (Syslog) ..... 0
Messages Received (Old protocol) ..... 0
Messages Received (New protocol, SRLP) ..... 0

Messages Rejected (Syslog) ..... 0
Messages Rejected (Old protocol) ..... 0
Messages Rejected (New protocol, SRLP) ..... 0
Messages Rejected (Module disabled) ..... 0
Messages Rejected (Generation disabled) ..... 0
Messages Rejected (Reception disabled) ..... 0
Messages Rejected (Bad parameters) ..... 0

Messages with invalid time ..... 0

Messages Transmitted (Syslog) ..... 26
Messages Transmitted (New protocol, SRLP) ..... 10

Messages Retransmitted (New protocol, SRLP) ..... 7
ACKs Sent (New protocol) ..... 0
ACKs Sent (Old protocol) ..... 0
ACKs Received (New protocol, SRLP) ..... 6

Message transmissions failed (New protocol, SRLP) ..... 0

Messages processed via OD 1 ..... 26 (Syslog)
Messages processed via OD 2 ..... 11 (Router)
Messages processed via OD TE ..... 15 (Memory)

```


| | |
|---|--|
| Idle loop passes | アイドルループからログメッセージハンドラープ ロセスが起動された回数 |
| Transmit passes | ログメッセージ送信プロセス起動回数 |
| Messages Generated | 生成ログメッセージ数 |
| Messages Received (Syslog) | syslog により受信したログメッセージ数 |
| Messages Received (Old protocol) | Net Manage Message Protocol により受信した ログメッセージ数 |
| Messages Received (New protocol, SRLP) | SRLP(Secure Router Log Protocol)により受信 したログメッセージ数 |
| Messages Rejected (Syslog) | syslog メッセージのうち受信を拒否した数 |
| Messages Rejected (Old protocol) | Net Manage Message Protocol メッセージのう ち受信を拒否した数 |
| Messages Rejected (New protocol, SRLP) | SRLP(Secure Router Log Protocol)メッセージ のうち受信を拒否した数 |
| Messages Rejected (Module disabled) | 受信したログメッセージのうち、ログ機能が無効 状態だったために破棄されたものの数 |
| Messages Rejected (Generation disabled) | ソフトウェアモジュールからのログメッセージの うち、ログメッセージの生成が無効状態だったた め破棄されたものの数 |
| Messages Rejected (Reception disabled) | 受信したログメッセージのうち、ログ受信が無効 状態だったために破棄されたものの数 |
| Messages Rejected (Bad parameters) | 受信したログメッセージのうち、無効なパラメー ターを含んでいたために破棄されたものの数 |
| Messages with invalid time | タイムスタンプが無効だったメッセージの数 |
| Messages Transmitted (Syslog) | syslog で送信したログメッセージの数 |
| Messages Transmitted (New protocol, SRLP) | SRLP で送信したログメッセージの数 |
| Messages Retransmitted (New protocol, SRLP) | SRLP で再送信したログメッセージの数 |
| ACKs Sent (New protocol) | SRLP で受信したログメッセージに対する確認応 答 (ACK) 送信数 |
| ACKs Sent (Old protocol) | Net Manage Message Protocol で受信したログ メッセージに対する確認応答 (ACK) 送信数 |
| ACKs Received (New protocol, SRLP) | SRLP で送信したログメッセージに対する確認応 答 (ACK) 受信数 |
| Message transmissions failed | SRLP でのログメッセージ送信に失敗した回数 |
| Messages processed via OD n | 該当するログ出力定義によって処理されたメッ セージ数。メッセージのあとのかっこ内は出力先 (DESTINATION) |

表 52:

関連コマンド

SHOW LOG (388 ページ)

SHOW LOG OUTPUT (395 ページ)

SHOW LOG QUEUE (398 ページ)

SHOW LOG STATUS (402 ページ)

SHOW LOG OUTPUT

カテゴリー：運用・管理 / ログ

```
SHOW LOG OUTPUT [= {TEMPORARY|PERMANENT|output-id}] [{FILTER=entry-id|FULL}]
```

output-id: ログ出力 ID (1~20)
entry-id: エントリー番号 (1~)

解説

ログ出力先の定義内容を表示する。

パラメーター

- OUTPUT** ログ出力先 ID。省略時はすべてのログ出力先定義が表示される。
- FILTER** 指定したフィルターに関する詳細な情報を表示する。FULL オプションと同時に指定することはできない。
- FULL** 各出力先の定義内容を詳細に表示する。FILTER パラメーターと同時に指定することはできない。

入力・出力・画面例

```
Manager > show log output

OD#  Type      Port Server      Msg  Zone      Fmt Email Address      ESQMP
-----
PE   NVS                0020 Default              YY---
TE   Memory          0200 Default              YY---
-----

Manager > show log output=temporary

Output Definition ..... Temporary
Enabled ..... Yes
Type ..... Memory
Max Messages ..... 200
Time Zone ..... Not set
Secure ..... Yes
```

| | |
|------|---|
| OD# | ログ出力 ID |
| Type | ログ出力先。Memory、NVS、Port、Router、Syslog のいずれか |
| Port | ログ出力先の非同期ポート番号。Type が Port の場合にのみ有効 |

| | |
|---------------|---|
| Server | ログ転送先の IP アドレス。Type が Router か Syslog の場合にのみ有効 |
| Msg | 該当出力定義においてキューに格納できる最大メッセージ数 |
| Zone | タイムゾーン (Default、GMT、UTC、- (未設定) 、タイムゾーン名、-23:59:59 ~ +23:59:59) |
| Fmt | 該当出力定義におけるログメッセージのフォーマット。Full か Summary |
| Email Address | ログを送信先の電子メールアドレス。Type が Email の場合にのみ有効 |
| ESQMP | ENABLED、SECURE、QUEUEONLY、MAXQUEUESEVERITY、PASSWORD 各パラメーターの設定を示す。ENABLED、SECURE、QUEUEONLY の場合、Y は Yes を、N は No を、-は適用不可を示す。MAXQUEUESEVERITY は、0 ~ 7 のログレベルを、PASSWORD は、- (未設定) または* (設定済み) を示す |

表 53:

| | |
|---------------------|--|
| Output Definition | ログ出力 ID または、PE (Permanent)、TE (Temporary) のいずれか |
| Enabled | ログ出力定義の状態。Enabled か Disabled |
| Type | ログ出力先。Memory、NVS、Port、Router、Syslog のいずれか |
| IP Address (Server) | ログ転送先の IP アドレス。Type が Router か Syslog の場合にのみ有効 |
| Zone | タイムゾーン (Default、GMT、UTC、Not set (未設定)、-23:59:59 ~ +23:59:59 およびタイムゾーン名) |
| Secure | このログ出力先が安全かどうか |
| Queue Only | キュー格納のみかどうか |
| Max Messages | 該当出力定義においてキューに格納できる最大メッセージ数 |
| Filter # | ログメッセージフィルター番号、フィルター条件、マッチ時のアクション。条件「ALL」はすべてのメッセージにマッチすることを示す。アクションは Process か Ignore のどちらか |
| Port | ログ出力先の非同期ポート番号。Type が Port の場合にのみ有効 |
| Format | 該当出力定義におけるログメッセージのフォーマット。Full か Summary |
| Email Address | ログを送信先の電子メールアドレス。Type が Email の場合にのみ有効 |
| Password | SRLP で他のルーターに転送する場合に認証を受けるためのパスワード。NONE は未設定を示す |
| Max Queue Severity | 処理されずにキューイングされる最大のログレベル。0 (最低) ~ 7 (最高) |

表 54: FULL オプション指定時

例

現在定義されているログ出力先の一覧を表示する。

```
SHOW LOG OUTPUT
```

ログ出力先「1」の詳細情報を表示する。

```
SHOW LOG OUTPUT=1
```

ログ出力先「1」のさらに詳細な情報（メッセージフィルターを含む）を表示する。

```
SHOW LOG OUTPUT=1 FULL
```

関連コマンド

ADD LOG OUTPUT (126 ページ)

CREATE LOG OUTPUT (164 ページ)

DELETE LOG OUTPUT (191 ページ)

DESTROY LOG OUTPUT (208 ページ)

SET LOG OUTPUT (300 ページ)

SHOW LOG STATUS (402 ページ)

SHOW LOG QUEUE

カテゴリー：運用・管理 / ログ

SHOW LOG QUEUE

解説

ログメッセージキュー内のメッセージに関する情報を表示する。

入力・出力・画面例

```
Manager > show log queue
```

| Queue | RAM Messages | NVS Messages | Type |
|-------|--------------|--------------|--------|
| 01 | 0000/0100 | 0000/0000 | Syslog |
| 02 | 0003/0100 | 0000/0000 | Router |
| TE | 0007/0200 | 0000/0000 | Memory |

```
-----
```

Outstanding SRLP Messages (Sent but not acknowledged)

| OD# | Message ID | Last Attempt | Attempts | Delay |
|-----|------------|--------------|----------|-------|
| 02 | 1 | 979 | 1 | 1 |
| 02 | 2 | 979 | 1 | 1 |
| 02 | 3 | 979 | 1 | 1 |

```
-----
```

| | |
|--------------|---|
| Queue | ログ出力 ID (1 ~ 20) または TE (TEMPORARY)、 PE (PERMANENT) |
| RAM Messages | 現在 RAM 上に保存されているメッセージ数 / RAM 上に保存可能な最大メッセージ数 |
| NVS Messages | 現在 NVS 上に保存されているメッセージ数 / NVS 上に保存可能な最大メッセージ数 |
| Type | メッセージの最終的な送信先。Memory、NVS、Port、Router、Syslog のいずれか |
| OD# | ログ出力 ID |
| Message ID | メッセージ ID |
| Last Attempt | 最後にメッセージ送信を試みた時刻。深夜 0 時からの経過分数 |
| Attempts | メッセージの送信試行回数 |
| Delay | 前回の送信試行から次の送信までの間隔 (分) |

表 55:

関連コマンド

SHOW LOG (388 ページ)

SHOW LOG OUTPUT (395 ページ)

SHOW LOG STATUS (402 ページ)

SHOW LOG RECEIVE

カテゴリー：運用・管理 / ログ

SHOW LOG RECEIVE [= { *ipadd* | ANY }] [MASK = *ipadd*]

ipadd: IP アドレスまたはネットマスク

解説

ログ受信テーブルの内容を表示する。

パラメーター

RECEIVE ログ送信元の IP アドレス。MASK と組み合わせて範囲を指定することも可能。ANY と 0.0.0.0 はすべての IP アドレスを示す。

MASK RECEIVE パラメーターで指定したアドレスに対するマスク。ただし、RECEIVE=ANY または RECEIVE=0.0.0.0 のときは指定できない。

入力・出力・画面例

```
Manager > show log receive
```

| Type | IP/Network Addr | Netmask | Protocol | Password |
|-------|-----------------|-----------------|-------------|----------|
| Allow | 192.168.1.1 | 255.255.255.255 | OLD NEW --- | |

| | |
|-----------------|---|
| Type | 該当アドレスからのログ受信を許可するかどうか。Allow (許可) Reject (拒否) |
| IP/Network Addr | ログ送信元のベース IP アドレス。Any はすべての IP アドレスを示す |
| Netmask | IP/Network Addr に対するネットマスク |
| Protocol | 該当 IP アドレスからログを受信するときに使うプロトコル。OLD (Net Manage Message Protocol) NEW (SRLP) SYS (syslog) の 3 種類がある |
| Password | SRLP 使用時の認証パスワード。未設定時は空欄 |

表 56:

関連コマンド

ADD LOG RECEIVE (128 ページ)

DELETE LOG RECEIVE (192 ページ)

SET LOG RECEIVE (305 ページ)

SHOW LOG STATUS (402 ページ)

SHOW LOG STATUS

カテゴリー：運用・管理 / ログ

SHOW LOG STATUS

解説

ログ機能の設定情報を表示する。

入力・出力・画面例

```
Manager > show log status

Log System Status
-----

Log Module Status ..... Enabled
Log Message Generation ..... Enabled
Log Message Reception (via network) ... Enabled
Log Message Output ..... Enabled
Local Time Offset (from UTC) ..... Not set
Next Message ID ..... 59
Number of Output Definitions ..... 2
```

| | |
|-------------------------------------|---|
| Log Module Status | ログ機能の有効・無効 |
| Log Message Generation | ログ生成の有効・無効 |
| Log Message Reception (via network) | ログ受信の有効・無効 |
| Log Message Output | ログ出力の有効・無効 |
| Local Time Offset (from UTC) | ログモジュールが使用する UTC オフセット (+23:59:59 ~ -23:59:59)、「-」は未設定を示す |
| Next Message ID | 次のメッセージ ID |
| Number of Output Definitions | 定義済み出力先の数 |

表 57:

関連コマンド

- DISABLE LOG (214 ページ)
- DISABLE LOG GENERATION (215 ページ)
- DISABLE LOG OUTPUT (216 ページ)
- DISABLE LOG RECEPTION (217 ページ)
- ENABLE LOG (244 ページ)

ENABLE LOG GENERATION (245 ページ)
ENABLE LOG OUTPUT (246 ページ)
ENABLE LOG RECEPTION (247 ページ)
SHOW LOG (388 ページ)

SHOW MAIL

カテゴリー：運用・管理 / メール送信

SHOW MAIL

解説

メール送信機能の設定および送信キュー内のメール一覧を表示する。

入力・出力・画面例

```
Manager > show mail
```

MAIL

```
Host Name ..... routerb.tw.mydomain.xxx
SMTP Server ..... not set
State ..... alive
Debug ..... disabled
Mails Sent ..... 4
```

| Date/Time | Id | To | Subject | State | Retries |
|------------|------|-----------------------|---------|---------|---------|
| 5 11:11:15 | 0003 | admin@is.mydomain.xxx | | Connect | 0 |

| | |
|-------------|---|
| Host Name | 自ホスト名 (SET MAIL コマンドで設定) |
| SMTP Server | 未サポート |
| State | メール送信機能の状態。「alive」(動作中)「DEAD - name server not set」(停止中 - DNS 未設定)「DEAD - hostname not set」(停止中 - 自ホスト名未設定) |
| Debug | デバッグ機能の状態。「enabled」または「disabled」 |
| Mails Sent | 前回の再起動後に送信したメールの数 |
| Date/Time | 該当メッセージがスプールされた日時 |
| Id | メッセージ ID。DELETE MAIL コマンドでスプールからメールを削除するときに指定する |
| To | 宛先メールアドレス |
| Subject | メールタイトル |
| State | 該当メッセージの送信状態。initial (処理開始) get MX-IP (MX レコード検索中) get IP (DNS 検索中) Connect (SMTP サーバーとの TCP 接続確立) S-helo (HELO コマンド送信中) S-from (MAIL FROM コマンド送信中) S-rcpt (RCPT TO コマンド送信中) S-data (DATA コマンド送信中) S-header (メールヘッダー送信中) S-file (ファイルからメール本文を送信中) S-buffer (メッセージ本文を送信中) S-last (メッセージ終端のドットを送信中) S-done (メッセージ送信完了) S-quit (QUIT コマンドを送信中) |
| Retries | メッセージの再送回数 |

表 58:

関連コマンド

DELETE MAIL (193 ページ)

DISABLE MAIL DEBUG (218 ページ)

ENABLE MAIL DEBUG (248 ページ)

MAIL (275 ページ)

SHOW MANAGER ASYN

カテゴリー：運用・管理 / セキュリティー

SHOW MANAGER ASYN

解説

マネージャーポート（ログイン不要なポート）として設定されている非同期ポートの番号を表示する。

入力・出力・画面例

```
Manager > show manager asyn  
  
No manager port is defined.
```

関連コマンド

LOGIN (273 ページ)

SET ASYN (「インターフェース」の 50 ページ)

SET MANAGER ASYN (309 ページ)

SHOW NTP

カテゴリー：運用・管理 / NTP

SHOW NTP

解説

NTP の設定情報を表示する。

入力・出力・画面例

```

Manager > show ntp

-----
NTP Module Configurations
-----
Status           : ENABLED
Host Address      : 172.16.28.169
UTC offset        : +09:00:00 (JST)
Last Updated      : 11:19:38 on 03-Jul-2001
Last Delta        : +0.94

Configured Peer
-----
172.16.28.1

Counters
-----
Packets Sent      : 0000000002
Packets Received  : 0000000002
Packets w/ head error : 0000000000
Packets w/ data error : 0000000000

```

| | |
|-----------------------|-----------------------------------|
| Status | NTP モジュールの状態 (ENABLED か DISABLED) |
| Host Address | NTP モジュールの IP アドレス |
| UTC offset | 協定世界時 (UTC) からのオフセット |
| Last Updated | NTP による内蔵時計の最終更新日時 |
| Last Delta | 最終更新時の内蔵時計の修正量 (誤差) |
| Configured Peer | NTP サーバーの IP アドレス |
| Packets Sent | 送信 NTP パケット数 |
| Packets Received | 受信 NTP パケット数 |
| Packets w/ head error | 受信 NTP パケットのうちヘッダーエラーがあったものの数 |

| Packets w/ data error | 受信 NTP パケットのうちデータエラーがあったものの数 |
|-----------------------|------------------------------|
|-----------------------|------------------------------|

表 59:

関連コマンド

ADD NTP PEER (130 ページ)

SET NTP UTCOFFSET (310 ページ)

SHOW NVS

カテゴリー：運用・管理 / 記憶装置とファイルシステム

SHOW NVS [BLOCK=*block-id* [INDEX=*index*]]

block-id: ブロック ID (16 進数)

index: ブロックインデックス (16 進数)

解説

NVS (不揮発性メモリー) のメモリーブロック構成を表示する。

パラメーター

BLOCK ブロック ID

INDEX ブロックインデックス

入力・出力・画面例

```
Manager > show nvs
```

| Block ID | Index | Size (bytes) | Creation Date | Creator ID | Block Address |
|-------------|----------|-----------------|------------------|---------------|------------------|
| 0000001a | 00000003 | 0000001a | 09-Apr-2001 | 00000012 | ffe00200 |
| 00000032 | 00000002 | 00000050 | 09-Apr-2001 | 00000022 | ffe00400 |
| 00000038 | 00000000 | 00000000 | **-*-**-**** | 00000021 | ffe00000 |
| 00000043 | 00000001 | 000000b4 | 05-Jul-2001 | 00000029 | ffe02c00 |
| 00000043 | 00000002 | 00000f78 | 05-Jul-2001 | 00000029 | ffe04200 |
| 00000043 | 00000003 | 00000058 | 05-Jul-2001 | 00000029 | ffe05400 |
| 00000045 | 000003fc | 00000de4 | 05-Jul-2001 | 00000026 | ffe01c00 |
| 00000045 | 000003fd | 00000024 | 05-Jul-2001 | 00000026 | ffe01a00 |

| | |
|---------------|---------------------------------------|
| Block ID | ブロック ID (16 進) |
| Index | ブロックインデックス (16 進) |
| Size (bytes) | ブロックサイズ (バイト) (16 進) |
| Creation Date | ブロックの作成日。「**-*-**-**」は作成日が未定義であることを示す |
| Creator ID | ブロックを作成したモジュールの ID |
| Block Address | ブロックアドレス |

表 60:

関連コマンド

CLEAR NVS TOTALLY (156 ページ)

SHOW NVS FREE (411 ページ)

SHOW NVS FREE

カテゴリー：運用・管理 / 記憶装置とファイルシステム

SHOW NVS FREE

解説

NVS（不揮発性メモリー）の空き容量を表示する。

入力・出力・画面例

```
Manager > show nvs free

Number of free sectors          232
Number of bytes in free sectors 114144
```

関連コマンド

CLEAR NVS TOTALLY（156 ページ）

SHOW NVS（409 ページ）

SHOW PATCH

カテゴリー：運用・管理 / ソフトウェア

SHOW PATCH

解説

パッチファイルの情報を表示する。

入力・出力・画面例

```
Manager > show patch
```

Patch files

| Name | Device | Size | Version |
|--------------|--------|------|---------|
| 55271-01.paz | flash | 8564 | 2.7-1 |

| | |
|---------|---------------------|
| Name | パッチファイル名 |
| Device | パッチファイルが格納されているデバイス |
| Size | パッチファイルのサイズ（バイト） |
| Version | パッチファイルのバージョン |

表 61:

関連コマンド

DESTROY PATCH (209 ページ)

LOAD (271 ページ)

SHOW PORTAUTH

カテゴリー：運用・管理 / ポート認証

SHOW PORTAUTH [= {8021X|MACBASED}]

解説

ポート認証機能（802.1X 認証、MAC ベース認証）の全般的な設定と状態を表示する。

パラメーター

PORTAUTH 認証メカニズム。8021X（802.1X 認証）、MACBASED（MAC ベース認証）から選択する。
省略時は 8021X と見なされる。

入力・出力・画面例

```
Manager > show portauth=8021x
```

```
802.1x System
```

```
-----
SystemAuthControl..... ENABLED
Global Username..... portAuthPortAuth
Global Password..... portAuthPortAuth
Global Encryption Method..... OTP
Global Encryption Type..... MD5
Number of Multi Supplicants.. 4 (limit 480)
```

| Port | PAE Capabilities | Protocol Version |
|-------|------------------|------------------|
| eth0 | None | 1 |
| eth1 | None | 1 |
| port1 | Supplicant | 1 |
| port2 | Authenticator | 1 |
| port3 | Both | 1 |
| port4 | None | 1 |

```
Manager > show portauth=macbased
```

```
MAC Based Authentication System
```

```
-----
SystemAuthControl..... ENABLED
Number of Supplicants.....4 (limit 480)
```

| Port | PAE Capabilities | Protocol Version |
|------|------------------|------------------|
|------|------------------|------------------|

| | | |
|-------|---------------|---|
| ----- | | |
| eth0 | None | 1 |
| eth1 | None | 1 |
| port1 | Supplicant | 1 |
| port2 | Authenticator | 1 |
| port3 | Both | 1 |
| port4 | None | 1 |

| | |
|-----------------------------|---|
| SystemAuthControl | 802.1X 認証機能の有効・無効 |
| Global Username | Supplicant 時のユーザー名 (Supplicant として動作しているポートが認証を受けるときに使用するユーザー名。該当ポート固有のユーザー名が設定されているときは、本ユーザー名ではなくポート固有のユーザー名を使用する) |
| Global Password | Supplicant 時のパスワード (Supplicant として動作しているポートが認証を受けるときに使用するパスワード。該当ポート固有のパスワードが設定されているときは、本パスワードではなくポート固有のパスワードを使用する) |
| Global Encryption Method | Supplicant 時のパスワード暗号化方式。Standard、OTP のいずれか |
| Global Encryption Type | Supplicant 時のパスワード暗号化方式に OTP を使用している場合のワンタイムパスワード生成アルゴリズム。MD4、MD5 のいずれか |
| Number of Multi Supplicants | Supplicant の数 (カッコ内はシステムがサポートしている Supplicant の最大数) |
| Port | スイッチポートのインターフェース名 |
| PAE Capabilities | 802.1X 認証におけるスイッチポートの役割。Authenticator、Supplicant、Both、None のいずれか |
| Protocol Version | EAPOL プロトコルバージョン |

表 62: PORTAUTH=8021X のとき

| | |
|-----------------------------|--|
| SystemAuthControl | MAC ベース認証機能の有効・無効 |
| Number of Multi Supplicants | Supplicant の数 (カッコ内はシステムがサポートしている Supplicant の最大数) |
| Port | スイッチポートのインターフェース名 |
| PAE Capabilities | 該当スイッチポートにおける MAC ベース認証の有効・無効 |

表 63: PORTAUTH=MACBASED のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (118 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SET PORTAUTH PORT (313 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (317 ページ)

SHOW PORTAUTH COUNTER (416 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

SHOW PORTAUTH TIMER (428 ページ)

SHOW PORTAUTH COUNTER

カテゴリー：運用・管理 / ポート認証

SHOW PORTAUTH [=8021X] **COUNTER PORT**={*eth-port*|*port-list*|**ALL**}

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

解説

指定ポートの 802.1X 統計カウンターを表示する。

パラメーター

PORTAUTH 認証メカニズム。本コマンドでは 8021X (802.1X 認証) のみ有効。省略時は 8021X と見なされるため、特に指定する必要はない。

PORT ポート

入力・出力・画面例

```
Manager > show portauth counter port=3
802.1X Counters
-----
port3
PAE Type..... Authenticator
  Last EAPOL Frame Version.... 1
  Last EAPOL Frame Source..... 00-00-e2-59-56-48

  Receive                                Transmit
    EAPOL Frames..... 32      EAPOL Frames..... 122
    EAPOL Start Frames..... 0    EAP Req/Id Frames..... 70
    EAPOL Logoff Frames..... 0    EAP Request Frames..... 3
    EAP Resp/Id Frames..... 29
    EAP Response Frames..... 3
    EAP Length Error Frames.... 0
    Invalid EAPOL Frames..... 0

Manager > show portauth counter port=4
802.1X Counters
-----
port4
PAE Type..... Both

Authenticator - Attached Supplicant(s)
  Last EAPOL Frame Source..... 00-00-f4-95-30-6a
```


MAC Address..... 00-00-e2-59-56-48
 Last EAPOL Frame Version..... 1

| Receive | | Transmit | |
|-----------------------------|---|-------------------------|---|
| EAPOL Frames..... | 3 | EAPOL Frames..... | 3 |
| EAPOL Start Frames..... | 0 | EAP Req/Id Frames..... | 1 |
| EAPOL Logoff Frames..... | 0 | EAP Request Frames..... | 1 |
| EAP Resp/Id Frames..... | 2 | | |
| EAP Response Frames..... | 1 | | |
| EAP Length Error Frames.... | 0 | | |
| Invalid EAPOL Frames..... | 0 | | |

MAC Address..... 00-00-f4-95-30-6a
 Last EAPOL Frame Version..... 1

| Receive | | Transmit | |
|-----------------------------|---|-------------------------|---|
| EAPOL Frames..... | 3 | EAPOL Frames..... | 3 |
| EAPOL Start Frames..... | 0 | EAP Req/Id Frames..... | 1 |
| EAPOL Logoff Frames..... | 0 | EAP Request Frames..... | 1 |
| EAP Resp/Id Frames..... | 2 | | |
| EAP Response Frames..... | 1 | | |
| EAP Length Error Frames.... | 0 | | |
| Invalid EAPOL Frames..... | 0 | | |

Supplicant

Last EAPOL Frame Version.... 0
 Last EAPOL Frame Source..... ff-ff-ff-ff-ff-ff

| Receive | | Transmit | |
|-----------------------------|---|--------------------------|---|
| EAPOL Frames..... | 0 | EAPOL Frames..... | 3 |
| EAP Req/Id Frames..... | 0 | EAPOL Start Frames..... | 3 |
| EAP Request Frames..... | 0 | EAPOL Logoff Frames..... | 0 |
| Invalid EAPOL Frames..... | 0 | EAP Resp/Id Frames..... | 0 |
| EAP Length Error Frames.... | 0 | EAP Response Frames..... | 0 |

| | |
|------------------------------|---|
| Interface | スイッチポートのインターフェース名 |
| PAE Type | 802.1X 認証におけるスイッチポートの役割。Authenticator、Supplicant、Both のいずれか |
| Authenticator としての設定 | |
| Last EAPOL Frame Version | 最後に受信した EAPOL パケットのバージョン |
| MAC Address | 本ポートに接続されている Supplicant の MAC アドレス |
| Last EAPOL Frame Source | 最後に受信した EAPOL パケットの送信元 MAC アドレス |
| EAPOL Frames(Receive) | EAPOL パケットの受信総数 |
| EAPOL Start Frames(Receive) | EAPOL-Start パケットの受信数 |
| EAPOL Logoff Frames(Receive) | EAPOL-Logoff パケットの受信数 |

| | |
|----------------------------------|---|
| EAP Resp/Id Frames(Receive) | EAP-Response/Identity パケットの受信数 |
| EAP Response Frames(Receive) | EAP-Response パケットの受信数 |
| EAP Length Error Frames(Receive) | 受信した EAP パケットのうち、Length フィールドにエラーがあったものの数 |
| Invalid EAPOL Frames(Receive) | 受信した EAPOL パケットのうち、Type フィールドにエラーがあったものの数 |
| EAPOL Frames(Transmit) | EAPOL パケットの送信総数 |
| EAP Req/Id Frames(Transmit) | EAPOL-Request/Identity パケットの送信数 |
| EAP Request Frames(Transmit) | EAP-Request パケットの送信数 |
| Supplicant としての設定 | |
| EAPOL Frames(Receive) | EAPOL パケットの受信数 |
| EAP Req/Id Frames(Receive) | EAPOL-Request/Identity パケットの受信数 |
| EAP Request Frames(Receive) | EAP-Request パケットの受信数 |
| Invalid EAPOL Frames(Receive) | 受信した EAPOL パケットのうち、Type フィールドにエラーがあったものの数 |
| EAP Length Error Frames(Receive) | 受信した EAP パケットのうち、Length フィールドにエラーがあったものの数 |
| EAPOL Frames(Transmit) | EAPOL パケットの送信総数 |
| EAPOL Start Frames(Transmit) | EAPOL-Start パケットの送信数 |
| EAPOL Logoff Frames(Transmit) | EAPOL-Logoff パケット送信数 |
| EAP Resp/Id Frames(Transmit) | EAP-Response/Identity パケットの送信数 |
| EAP Response Frames(Transmit) | EAP-Response パケットの送信数 |

表 64:

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (118 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SET PORTAUTH PORT (313 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (317 ページ)

SHOW PORTAUTH (413 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

SHOW PORTAUTH TIMER (428 ページ)

SHOW PORTAUTH PORT

カテゴリー：運用・管理 / ポート認証

SHOW PORTAUTH [= {8021X|MACBASED}] **PORT**={*eth-port*|*port-list*|ALL}

eth-port: ETH インターフェース名 (eth0 のように指定)

port-list: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

解説

指定ポートにおけるポート認証機能 (802.1X 認証、MAC ベース認証) の設定を表示する。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証)、MACBASED (MAC ベース認証) から選択する。
省略時は 8021X と見なされる。

PORT ポート

入力・出力・画面例

```
Manager > show portauth=8021x port=1

802.1X Configuration
-----
Interface: port1
  PAE Type..... Authenticator
    Authenticator PAE State..... AUTHENTICATED
    Port Status..... authorised
    Backend Authenticator State... IDLE
    AuthControlPortControl..... Auto
    quietPeriod..... 60
    txPeriod..... 30
    suppTimeout..... 30
    serverTimeout..... 30
    maxReq..... 2
    reAuthMax..... 2
    reAuthPeriod..... 3600
    reAuthEnabled..... False
    piggyBack..... True
    keyTransmissionEnabled..... False (not supported)
    adminControlledDirections.... Both (not supported)
    guestVlan..... None (VLAN ID=0)
    trap..... None
    vlanAssignment..... Enabled
```

```
Manager > show portauth=8021x port=3
```

802.1X Configuration

```
Interface: port3
```

```
PAE Type..... Both
```

Multi-SupPLICANT Authenticator

Default Settings

```
AuthControlPortControl..... Auto
quietPeriod..... 60
txPeriod..... 30
suppTimeout..... 30
serverTimeout..... 30
maxReq..... 2
reAuthMax..... 2
reAuthPeriod..... 3600
reAuthEnabled..... False
secureVlan..... On
trap..... None
mibReset..... Enabled
vlanAssignment..... Enabled
```

Attached SupPLICANT(s)

```
MAC Address..... 00-00-e2-59-56-48
Authenticator PAE State..... AUTHENTICATED
Port Status..... authorised
Backend Authenticator State... IDLE
AuthControlPortControl..... Auto
quietPeriod..... 60
txPeriod..... 30
suppTimeout..... 30
serverTimeout..... 30
maxReq..... 2
reAuthMax..... 2
reAuthPeriod..... 3600
reAuthEnabled..... False
keyTransmissionEnabled..... False (not supported)
operControlledDirections..... False (not supported)
secureVlan..... On
trap..... None
mibReset..... Enabled
vlanAssignment..... Disabled
```

```
Manager > show portauth=macbased port=eth0
```

MAC Based Authentication Configuration

```
Interface: eth0
```

```
PAE Status..... Enabled
```

```
Number of SupPLICANTS.... 1
```

```

Default Settings
  AuthControlPortControl..... Auto
  quietPeriod..... 60
  reAuthPeriod..... 3600
  reAuthEnabled..... False
  secureVlan..... On
  trap..... None
  mibReset..... Enabled
  vlanAssignment..... Enabled

Attached Supplicant(s)
  MAC Address..... 00-00-f4-42-01-6b
  Authenticator PAE State..... AUTHENTICATED
  Port Status..... authorised
  Backend Authenticator State... IDLE
  AuthControlPortControl..... Auto
  quietPeriod..... 60
  reAuthPeriod..... 3600
  reAuthEnabled..... False
  secureVlan..... On
  trap..... None
  mibReset..... Enabled
  vlanAssignment..... Enabled

```

| | |
|-----------------------------|--|
| Interface | スイッチポートのインターフェース名 |
| PAE Type | 802.1X 認証におけるスイッチポートの役割。Authenticator、Supplicant、Both のいずれか |
| | Authenticator としての設定 |
| MAC Address | Supplicant の MAC アドレス |
| Authenticator PAE State | Authenticator としての状態。INITIALISE (初期化)、DISCONNECTED (未接続)、CONNECTING (接続中)、AUTHENTICATING (認証中)、AUTHENTICATED (認証済み)、ABORTING (認証断念中)、HELD (待機中)、FORCEAUTH (「 認証済み 」 に固定設定)、FORCEUNAUTH (「 未認証 」 に固定設定) のいずれか |
| Port Status | ポートの状態。unauthorised (未認証) か authorised (認証済み) |
| Backend Authenticator State | 認証機構の状態。IDLE (アイドル)、INITIALISE (初期化)、RESPONSE (Supplicant から応答受信)、REQUEST (認証サーバーに要求送信)、SUCCESS (認証成功)、FAIL (認証失敗)、TIMEOUT (タイムアウト) のいずれか |
| AuthControlPortControl | 手動設定によるポート状態。Auto (認証結果に応じて変動。通常の設定)、forceUnauthorised (未認証に固定)、forceAuthorised (認証済みに固定) のいずれか |

| | |
|---------------------------|---|
| quietPeriod | 認証失敗後、Supplicant との通信を拒否する期間（秒） |
| txPeriod | Supplicant に EAPOL パケットを再送信する間隔（秒） |
| suppTimeout | Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒） |
| serverTimeout | RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒） |
| maxReq | Supplicant に対する EAPOL-Request パケットの最大再送回数 |
| reAuthMax | 再認証時における EAPOL-Request パケットの最大再送回数 |
| reAuthPeriod | Supplicant を再認証する間隔（秒） |
| reAuthEnabled | 再認証の有効・無効 |
| piggyBack | Single-Supplicant モードにおいて、最初に接続された Supplicant の認証に成功した後、他のデバイスからのパケットも許可するかどうか |
| keyTransmissionEnabled | 未サポート |
| adminControlledDirections | 未サポート |
| secureVlan | ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効 |
| trap | ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか |
| mibReset | 古い Supplicant 情報をエージアウトするかどうか |
| vlanAssignment | ダイナミック VLAN の有効・無効 |
| Supplicant としての設定 | |
| heldPeriod | 認証失敗後、Authenticator との通信を試みない期間（秒） |
| authPeriod | Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒） |
| startPeriod | Authenticator に EAPOL-Start パケットを再送信する間隔（秒） |
| maxStart | EAPOL-Start パケットの最大送信回数。Supplicant ポートは、EAPOL-Start パケットを MAXSTART 回送信しても応答がない場合、Authenticator が存在しておらずポート認証の必要はないと判断する |
| Supplicant PAE State | Supplicant としての状態。Authorised と Unauthorised のいずれか |

表 65: PORTAUTH=8021X のとき

| | |
|-----------------------------|--|
| Interface | スイッチポートのインターフェース名 |
| PAE Status | 該当スイッチポートにおける MAC ベース認証の有効・無効 |
| Number of Supplicants | MAC ベース Supplicant の数 |
| MAC Address | Supplicant の MAC アドレス |
| Authenticator PAE State | Authenticator としての状態。INITIALISE (初期化)、DISCONNECTED (未接続)、CONNECTING (接続中)、AUTHENTICATING (認証中)、AUTHENTICATED (認証済み)、ABORTING (認証断念中)、HELD (待機中)、FORCEAUTH (「認証済み」に固定設定)、FORCEUNAUTH (「未認証」に固定設定) のいずれか |
| Port Status | ポートの状態。unauthorised (未認証) か authorised (認証済み) |
| Backend Authenticator State | 認証機構の状態。IDLE (アイドル)、INITIALISE (初期化)、RESPONSE (Supplicant から応答受信)、REQUEST (認証サーバーに要求送信)、SUCCESS (認証成功)、FAIL (認証失敗)、TIMEOUT (タイムアウト) のいずれか |
| AuthControlPortControl | 手動設定によるポート状態。Auto (認証結果に応じて変動。通常の設定)、forceUnauthorised (未認証に固定)、forceAuthorised (認証済みに固定) のいずれか |
| quietPeriod | 認証失敗後、Supplicant との通信を拒否する期間 (秒) |
| reAuthPeriod | Supplicant を再認証する間隔 (秒) |
| reAuthEnabled | 再認証の有効・無効 |
| secureVlan | ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効 |
| trap | ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか |
| mibReset | 古い Supplicant 情報をエージアウトするかどうか |
| vlanAssignment | ダイナミック VLAN の有効・無効 |

表 66: PORTAUTH=MACBASED のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (118 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SET PORTAUTH PORT (313 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (317 ページ)

SHOW PORTAUTH (413 ページ)

SHOW PORTAUTH COUNTER (416 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

SHOW PORTAUTH TIMER (428 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT

カテゴリー：運用・管理 / ポート認証

SHOW PORTAUTH [= {8021X|MACBASED}] **MULTISUPPLICANT PORT** = {*eth-port*|ALL}
 [SUPPLICANTMAC=*macadd*]

eth-port: ETH インターフェース名 (eth0 のように指定)

macadd: MAC アドレス (xx-xx-xx-xx-xx-xx の形式)

解説

802.1X Multi-SupPLICant モードで動作している Authenticator ポート、または、MAC ベース認証ポートの基本設定、および、接続/設定されている SupPLICant の情報を表示する。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証) MACBASED (MAC ベース認証) から選択する。
 省略時は 8021X と見なされる。

PORT ポート

SUPPLICANTMAC SupPLICant の MAC アドレス

入力・出力・画面例

```
Manager > show portauth multisuppliment port=eth0
802.1X Multi-SupPLICant Configuration
-----
Interface: eth0
Multi-SupPLICant Authenticator
Number of Multi SupPLICants..... 1
  Default Settings
    AuthControlPortControl..... Auto
    quietPeriod..... 60
    txPeriod..... 30
    suppTimeout..... 30
    serverTimeout..... 30
    maxReq..... 2
    reAuthMax..... 2
    reAuthPeriod..... 3600
    reAuthEnabled..... False
    secureVlan..... On
    trap..... None
    mibReset..... Enabled
    vlanAssignment..... Enabled

Attached SupPLICant(s)
```



```

MAC Address..... 00-00-f4-95-30-6a
Authenticator PAE State..... AUTHENTICATED
Port Status..... authorised
Backend Authenticator State... IDLE
AuthControlPortControl..... Auto
quietPeriod..... 60
txPeriod..... 30
suppTimeout..... 30
serverTimeout..... 30
maxReq..... 2
reAuthMax..... 2
reAuthPeriod..... 1800
reAuthEnabled..... True
keyTransmissionEnabled..... False (not supported)
adminControlledDirections.... Both (not supported)
secureVlan..... On
trap..... None
mibReset..... Enabled
vlanAssignment..... Enabled

```

Manager > show portauth=macbased multisuppliant port=eth0

MAC Based Authentication Configuration

Interface: eth0

```

PAE Status..... Enabled
Number of Supplicants.... 1
Default Settings
AuthControlPortControl..... Auto
quietPeriod..... 60
reAuthPeriod..... 3600
reAuthEnabled..... False
secureVlan..... On
trap..... None
mibReset..... Enabled
vlanAssignment..... Enabled

```

Attached Supplicant(s)

```

MAC Address..... 00-00-f4-22-33-44
Authenticator PAE State..... INITIALISE
Port Status..... unauthorised
Backend Authenticator State... IDLE
AuthControlPortControl..... Auto
quietPeriod..... 60
reAuthPeriod..... 3600
reAuthEnabled..... False
secureVlan..... On
trap..... Both
mibReset..... Enabled
vlanAssignment..... Enabled

```

| | |
|-----------------------------|--|
| Default Settings | 明示的に設定していない Supplicant に適用される設定値の一覧 |
| Attached Supplicant(s) | 明示的に設定した Supplicant に適用される設定値の一覧、および、ポート配下に接続されている Supplicant の情報一覧 |
| Authenticator PAE State | Authenticator としての状態。INITIALISE (初期化)、DISCONNECTED (未接続)、CONNECTING (接続中)、AUTHENTICATING (認証中)、AUTHENTICATED (認証済み)、ABORTING (認証断念中)、HELD (待機中)、FORCEAUTH (「認証済み」に固定設定)、FORCEUNAUTH (「未認証」に固定設定) のいずれか |
| Port Status | ポートの状態。unauthorised (未認証) か authorised (認証済み) |
| Backend Authenticator State | 認証機構の状態。IDLE (アイドル)、INITIALISE (初期化)、RESPONSE (Supplicant から応答受信)、REQUEST (認証サーバーに要求送信)、SUCCESS (認証成功)、FAIL (認証失敗)、TIMEOUT (タイムアウト) のいずれか |
| AuthControlPortControl | 手動設定によるポート状態。Auto (認証結果に応じて変動。通常の設定)、forceUnauthorised (未認証に固定)、forceAuthorised (認証済みに固定) のいずれか |
| quietPeriod | 認証失敗後、Supplicant との通信を拒否する期間 (秒) |
| txPeriod | Supplicant に EAPOL パケットを再送信する間隔 (秒) |
| suppTimeout | Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間 (秒) |
| serverTimeout | RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間 (秒) |
| maxReq | Supplicant に対する EAPOL-Request パケットの最大再送回数 |
| reAuthMax | 再認証時における EAPOL-Request パケットの最大再送回数 |
| reAuthPeriod | Supplicant を再認証する間隔 (秒) |
| reAuthEnabled | 再認証の有効・無効 |
| keyTransmissionEnabled | 未サポート |
| adminControlledDirections | 未サポート |
| secureVlan | ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効 |
| trap | ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか |
| mibReset | 古い Supplicant 情報をエージアウトするかどうか |
| vlanAssignment | ダイナミック VLAN の有効・無効 |

表 67: PORTAUTH=8021X のとき

| | |
|------------------------|---|
| Default Settings | 明示的に設定していない Supplicant に適用される設定値の一覧 |
| Attached Supplicant(s) | 明示的に設定した Supplicant に適用される設定値の一覧、および、ポート配下に接続されている Supplicant の情報一覧 |

| | |
|-----------------------------|--|
| Authenticator PAE State | Authenticator としての状態。INITIALISE (初期化)、DISCONNECTED (未接続)、CONNECTING (接続中)、AUTHENTICATING (認証中)、AUTHENTICATED (認証済み)、ABORTING (認証断念中)、HELD (待機中)、FORCEAUTH (「 認証済み 」 に固定設定)、FORCEUNAUTH (「 未認証 」 に固定設定) のいずれか |
| Port Status | ポートの状態。unauthorised (未認証) か authorised (認証済み) |
| Backend Authenticator State | 認証機構の状態。IDLE (アイドル)、INITIALISE (初期化)、RESPONSE (Supplicant から応答受信)、REQUEST (認証サーバーに要求送信)、SUCCESS (認証成功)、FAIL (認証失敗)、TIMEOUT (タイムアウト) のいずれか |
| AuthControlPortControl | 手動設定によるポート状態。Auto (認証結果に応じて変動。通常の設定)、forceUnauthorised (未認証に固定)、forceAuthorised (認証済みに固定) のいずれか |
| quietPeriod | 認証失敗後、Supplicant との通信を拒否する期間 (秒) |
| reAuthPeriod | Supplicant を再認証する間隔 (秒) |
| reAuthEnabled | 再認証の有効・無効 |
| secureVlan | ダイナミック VLAN 有効時、2 番目以降に接続された Supplicant の所属 VLAN が、最初に認証を通った Supplicant と同じでないと認証を許可しない機能の有効・無効 |
| trap | ポート認証機能に関する SNMP トラップを送信するかどうか。また、どのようなときに送信するか |
| mibReset | 古い Supplicant 情報をエージアウトするかどうか |
| vlanAssignment | ダイナミック VLAN の有効・無効 |

表 68: PORTAUTH=MACBASED のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (118 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SET PORTAUTH PORT (313 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (317 ページ)

SHOW PORTAUTH (413 ページ)

SHOW PORTAUTH COUNTER (416 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH TIMER (428 ページ)

SHOW PORTAUTH TIMER

カテゴリー：運用・管理 / ポート認証

SHOW PORTAUTH [= {8021X|MACBASED}] **TIMER PORT**={eth-port|port-list|ALL}

eth-port: ETH インターフェース名 (eth0 のように指定)
port-list: スイッチポート番号 (1～。ハイフン、カンマを使った複数指定も可能)

解説

指定ポートにおけるポート認証機能 (802.1X 認証または MAC ベース認証) の各種タイマー (残り時間) を表示する。

パラメーター

PORTAUTH 認証メカニズム。8021X (802.1X 認証) MACBASED (MAC ベース認証) から選択する。
省略時は 8021X と見なされる。
PORT ポート

入力・出力・画面例

```

Manager > show portauth=8021x timer port=3
802.1X Timers
-----
Interface: port3                                PAE Type..... Both

Authenticator
    aWhile      quietWhile      reAuthWhen      txWhen
    00           00000           00048           00000

Supplicant
    authWhile    heldWhile      startWhen
    00           00000           20

Manager > show portauth=8021x timer port=4
802.1X Timers
-----
Interface: port4                                PAE Type..... Both

Attached Supplicant: 00-00-e2-59-56-48
    aWhile      quietWhile      reAuthWhen      txWhen
    00           00000           00000           00000

Attached Supplicant: 00-00-f4-95-30-6a
    aWhile      quietWhile      reAuthWhen      txWhen

```

| | | | |
|--|------------|------------|-------|
| 00 | 00000 | 00000 | 00000 |
| Supplicant | | | |
| authWhile | heldWhile | startWhen | |
| 00 | 00000 | 26 | |
| Manager > show portauth=macbased timer port=eth0 | | | |
| MAC Based Authentication Timers | | | |
| ----- | | | |
| Interface: eth0 | | | |
| Supplicant | quietWhile | reAuthWhen | |
| ----- | | | |
| 00-00-f4-42-01-6b | 00000 | 00000 | |

| | |
|---------------------|---|
| Interface | スイッチポートのインターフェース名 |
| PAE Type | 802.1X 認証におけるスイッチポートの役割。Authenticator、Supplicant、Both のいずれか |
| Authenticator 用タイマー | |
| aWhile | Supplicant に EAP-Request を送信した後、Supplicant からの応答を待つ時間（秒）。または、RADIUS サーバーに Access-Request を送信した後、RADIUS サーバーからの応答を待つ時間（秒）。前者の初期値は SUPPTIMEOUT パラメーターの値、後者の初期値は SERVERTIMEOUT パラメーターの値となる |
| quietWhile | 認証失敗後、Supplicant との通信を拒否する期間（秒）を示すタイマー。QUIETPERIOD パラメーターの値が初期値となる |
| reAuthWhen | Supplicant を再認証するまでの残り時間（秒）。REAUTHPERIOD パラメーターの値が初期値となる |
| txWhen | Supplicant に EAPOL パケットを再送信するまでの待ち時間（秒）。TX-PERIOD パラメーターの値が初期値となる |
| Supplicant 用タイマー | |
| authWhile | Authenticator に EAP-Response パケットを送信した後、Authenticator からの応答を待つ時間（秒）。AUTHPERIOD パラメーターの値が初期値となる |
| heldWhile | 認証失敗後、Authenticator との通信を試みない期間（秒）を示すタイマー。HELDPERIOD パラメーターの値が初期値となる |
| startWhen | Authenticator に EAPOL-Start パケットを送信するまでの待ち時間（秒）。STARTPERIOD パラメーターの値が初期値となる |

表 69: PORTAUTH=8021X のとき

| | |
|------------|-------------------------------|
| Interface | スイッチポートのインターフェース名 |
| Supplicant | MAC ベース Supplicant の MAC アドレス |

| | |
|------------|---|
| quietWhile | 認証失敗後、Supplicant との通信を拒否する期間（秒）を示すタイマー。QUI-ETPERIOD パラメーターの値が初期値となる |
| reAuthWhen | Supplicant を再認証するまでの残り時間（秒）。REAUTHPERIOD パラメーターの値が初期値となる |

表 70: PORTAUTH=MACBASE のとき

関連コマンド

ACTIVATE PORTAUTH PORT REAUTHENTICATE (118 ページ)

ENABLE PORTAUTH (250 ページ)

ENABLE PORTAUTH PORT (252 ページ)

SET PORTAUTH PORT (313 ページ)

SET PORTAUTH PORT SUPPLICANTMAC (317 ページ)

SHOW PORTAUTH (413 ページ)

SHOW PORTAUTH COUNTER (416 ページ)

SHOW PORTAUTH PORT (419 ページ)

SHOW PORTAUTH PORT MULTISUPPLICANT (424 ページ)

SHOW RADIUS

カテゴリー：運用・管理 / 認証サーバー

SHOW RADIUS

解説

登録されている RADIUS (Remote Authentication Dial In User Server) サーバーの一覧を表示する。

入力・出力・画面例

```
Manager > show radius

RADIUS Server Parameters
-----
Server Retransmit Count..... 3
Server Timeout..... 6 sec
Server Dead Time..... 5 min
-----
Server          Port  AccPort  LocalInterface  Radius      Accounting
                  Status      Status
-----
192.168.10.10    1645    1646    Not set        Alive       Alive
172.28.28.10     1645    1646    Not set        Dead (49sec) Alive
-----
```

| | |
|-------------------------|---|
| Server Retransmit Count | RADIUS サーバーへの要求再送回数 |
| Server Timeout | RADIUS サーバーへの要求に対する応答待ち時間 |
| Server Dead Time | RADIUS サーバーへの要求が規定回数 (1 + Server Retransmit Count 回) タイムアウトしたときに、該当サーバーが「使用不可」であると見なして同サーバーの使用を抑制する時間 |
| Server | RADIUS サーバーの IP アドレス |
| Port | 認証サーバーのポート番号 |
| AccPort | アカウントティングサーバーのポート番号 |
| Secret | RADIUS サーバーとの通信に用いる共有パスワード。アスタリスクで表示される |
| LocalInterface | RADIUS サーバーとの通信に使用するローカル IP インターフェース名 (localX の形式。X はローカル IP インターフェース番号 (1 ~ 15)) |
| Radius Status | 認証サーバーの状態。Alive (使用可能)、Dead (使用不可) のどちらか。Dead の場合は、カッコ内に使用抑制時間の残り時間が表示される |

| | |
|-------------------|---|
| Accounting Status | アカウントティングサーバーの状態。Alive（使用可能）、Dead（使用不可）のどちらか。Dead の場合は、カッコ内に使用抑制時間の残り時間が表示される |
|-------------------|---|

表 71:

関連コマンド

ADD RADIUS SERVER (131 ページ)

DELETE RADIUS SERVER (196 ページ)

SHOW RELEASE

カテゴリー：運用・管理 / ソフトウェア

SHOW RELEASE

解説

リリース（ファームウェア）ライセンスの情報を表示する。

入力・出力・画面例

| Manager > show release | | |
|------------------------|---------|--------|
| Release | Licence | Period |
| ----- | ----- | ----- |
| 55292-00.rez | full | - |
| ----- | ----- | ----- |

| | |
|---------|----------------------------------|
| Release | リリースファイルのフルパス名 |
| Licence | ライセンスの種類。通常「full」（フルライセンス）と表示される |
| Period | ライセンスの有効期間（試用版の場合） |

表 72:

関連コマンド

DISABLE RELEASE (223 ページ)

ENABLE RELEASE (256 ページ)

SHOW SCRIPT

カテゴリー：運用・管理 / スクリプト

SHOW SCRIPT [=filename]

filename: ファイル名（拡張子は.scp か.cfg）

解説

スクリプトファイルの一覧、あるいは、指定したスクリプトの内容を表示する。

パラメーター

SCRIPT 表示するスクリプトファイルの名前。省略時はファイルシステム上にあるスクリプトファイルの一覧が表示される。

入力・出力・画面例

```

Manager > show script

Configuration Scripts:

```

| Filename | Device | Size | Created | Locks |
|--------------|--------|------|----------------------|-------|
| ----- | | | | |
| bekopstn.cfg | flash | 3234 | 10-Jun-2001 14:25:25 | 0 |
| boot.cfg | flash | 357 | 11-Jan-2001 10:39:26 | 0 |
| ipsec.cfg | flash | 5349 | 03-Oct-2001 14:07:32 | 0 |
| ipsecl2t.cfg | flash | 5723 | 03-Oct-2001 19:16:16 | 0 |
| ipsecudp.cfg | flash | 5654 | 03-Oct-2001 17:33:02 | 0 |
| ipv6.cfg | flash | 4525 | 03-Oct-2001 16:45:18 | 0 |
| ipv6bad.cfg | flash | 4210 | 22-Jun-2001 01:43:07 | 0 |
| rsasig.cfg | flash | 5615 | 04-Oct-2001 20:22:27 | 0 |
| wak0712.cfg | flash | 3906 | 12-Jul-2001 21:45:12 | 0 |
| wakadsl.cfg | flash | 3571 | 20-Jun-2001 22:03:23 | 0 |
| wakadsl2.cfg | flash | 3896 | 30-Jun-2001 23:46:05 | 0 |
| wakadsl3.cfg | flash | 3764 | 30-Jun-2001 12:00:51 | 0 |
| wakpstn.cfg | flash | 3429 | 18-Jun-2001 00:57:53 | 0 |
| ----- | | | | |

```

General Scripts:

```

| Filename | Device | Size | Created | Locks |
|--------------|--------|------|----------------------|-------|
| ----- | | | | |
| doreset.scp | flash | 48 | 02-Oct-2001 14:00:54 | 0 |
| sendmail.scp | flash | 30 | 22-Jul-2001 11:08:35 | 0 |

```
-----

Manager > show script=sendmail.scp

File : sendmail.scp

1:mail to=%1 sub=%2 message=%3
```

| | |
|----------|-------------------------------|
| Filename | スクリプトファイル名 |
| Device | スクリプトファイルの格納先デバイス。nvs か flash |
| Size | ファイルサイズ (バイト) |
| Created | ファイル作成日時 |
| Locks | ファイルを使用しているプロセスの数 |

表 73:

例

ファイルシステム上にあるスクリプトの一覧を表示する。

SHOW SCRIPT

スクリプトファイル「myscript.scp」の内容を表示する。

SHOW SCRIPT=myscript.scp

関連コマンド

- ACTIVATE SCRIPT (120 ページ)
- ADD SCRIPT (133 ページ)
- DEACTIVATE SCRIPT (186 ページ)
- DELETE SCRIPT (197 ページ)
- SET SCRIPT (323 ページ)

SHOW SESSIONS

カテゴリー：運用・管理 / ターミナルサービス

SHOW SESSIONS

解説

現在のログインセッション（コンソールセッション、Telnet セッション）で利用可能な 5 つの仮想端末セッション（他ホストへの Telnet）の状態を表示する。

セッションスロットごとに、IP アドレス（TELNET ipadd）、ホスト名（TELNET hostname）、not connected（未接続）のいずれかの情報が表示される。

入力・出力・画面例

```
SecOff > show session

Session information for Asyn 0

session 1 connected to 192.168.10.103
session 2 not connected
session 3 not connected
session 4 not connected
session 5 not connected
```

関連コマンド

DISCONNECT（235 ページ）

RECONNECT（285 ページ）

SHOW SNMP

カテゴリー：運用・管理 / SNMP

SHOW SNMP

解説

SNMP モジュールの情報を表示する。

入力・出力・画面例

```

Manager > show snmp

SNMP configuration:
  Status ..... Enabled
  Authentication failure traps .... Enabled
  Local Interface SNMPv1 ..... Not Set
  Local Interface SNMPv2 ..... Not Set
  Local Interface SNMPv3 ..... Not Set
  Community ..... public
    Access ..... read-only
    Status ..... Enabled
    Traps ..... Enabled
    Open access ..... No

SNMPv3 engine information:
  snmpEngineID ..... 800000cf030000cd123456
  snmpEngineBoots ..... 6
  snmpEngineTime ..... 1388

SNMP counters:
  inPkts ..... 15006          outPkts ..... 15006
  inBadVersions ..... 0       outTooBigs ..... 0
  inBadCommunityNames ..... 0 outNoSuchNames ..... 0
  inBadCommunityUses ..... 0 outBadValues ..... 0
  inASNParseErrs ..... 6      outGenErrs ..... 0
  inTooBigs ..... 0           outGetRequests ..... 0
  inNoSuchNames ..... 0       outGetNexts ..... 0
  inBadValues ..... 0         outSetRequests ..... 0
  inReadOnly ..... 0          outGetResponses ..... 14981
  inGenErrs ..... 0           outTraps ..... 6
  inTotalReqVars ..... 14977
  inTotalSetVars ..... 0
  inGetRequests ..... 0
  inGetNexts ..... 14977
  inSetRequests ..... 0
  inGetResponses ..... 0

```

| | |
|----------------------------|----|
| inTraps | 0 |
| SNMPv3 counters: | |
| UnsupportedSecLevels | 0 |
| NotInTimeWindows | 0 |
| UnknownUserNames | 1 |
| UnknownEngineIDs | 14 |
| WrongDigests | 4 |
| DecryptionErrors | 0 |
| UnknownSecModels | 0 |
| InvalidMsgs | 0 |
| UnknownPDUHandlers | 0 |

| | |
|------------------------------|---|
| SNMP configuration セクション | SNMP モジュールの基本設定が表示される |
| Status | SNMP エージェントの状態。Enabled か Disabled |
| Authentication failure traps | 認証トラップの有効・無効 |
| Local Interface SNMPv1 | SNMPv1 パケットの送信に使用するローカル IP インターフェース (ループバックインターフェース)。未設定時は Not Set |
| Local Interface SNMPv2 | SNMPv2c パケットの送信に使用するローカル IP インターフェース (ループバックインターフェース)。未設定時は Not Set |
| Local Interface SNMPv3 | SNMPv3 パケットの送信に使用するローカル IP インターフェース (ループバックインターフェース)。未設定時は Not Set |
| Community | コミュニティー名 |
| Access | コミュニティーのアクセス権。read-only、read-write のどちらか |
| Status | コミュニティーの状態。Enabled か Disabled |
| Traps | トラップ生成の有効・無効 |
| Open access | すべてのホストから SNMP によるアクセスを許可するかどうか。Yes または NoSNMPv3 engine information セクション |
| snmpEngineID | エンジン ID |
| snmpEngineBoots | エンジン初期化 (再起動) 回数。エンジン ID が変更されると 1 に戻る |
| snmpEngineTime | エンジン初期化後の経過時間 (秒) |
| SNMP counters セクション | SNMP 関連の統計カウンターが表示される |
| inPkts | 受信 SNMP パケット数 |
| inBadVersions | 未サポートのバージョン番号を持つ SNMP メッセージの受信総数 |
| inBadCommunityNames | 不明なコミュニティー名を持つ SNMP メッセージの受信総数 |
| inBadCommunityUses | コミュニティー名とオペレーションの権限が一致しない SNMP メッセージの受信総数 |
| inASNParseErrs | ASN.1 構文エラーによりデコードできなかった SNMP メッセージの受信総数 |
| inTooBigs | エラー状態フィールドに「tooBig」がセットされていた SNMP メッセージの受信総数 |
| inNoSuchNames | エラー状態フィールドに「noSuchName」がセットされていた SNMP メッセージの受信総数 |

| | |
|-----------------------|---|
| inBadValues | エラー状態フィールドに「badValue」がセットされていた SNMP メッセージの受信総数 |
| inReadOnly | エラー状態フィールドに「readOnly」がセットされていた SNMP メッセージの受信総数 |
| inGenErrs | エラー状態フィールドに「genErr」がセットされていた SNMP メッセージの受信総数 |
| inTotalReqVars | 受信した GetRequest および GetNextRequest メッセージに応じて読み出された MIB オブジェクトの合計数 |
| inTotalSetVars | 受信した SetRequest メッセージに応じて変更された MIB オブジェクトの合計数 |
| inGetRequests | 受信した GetRequest メッセージの総数 |
| inGetNexts | 受信した GetNextRequest メッセージの総数 |
| inSetRequests | 受信した SetRequest メッセージの数 |
| inGetResponses | 受信した GetResponse メッセージの総数 |
| inTraps | 受信した SNMP トラップの総数 |
| outPkts | 送信 SNMP パケット数 |
| outTooBig | エラー状態フィールドに「tooBig」をセットして送信された SNMP メッセージの数 |
| outNoSuchNames | エラー状態フィールドに「noSuchName」をセットして送信された SNMP メッセージの数 |
| outBadValues | エラー状態フィールドに「badValue」をセットして送信された SNMP メッセージの数 |
| outGenErrs | エラー状態フィールドに「genErr」をセットして送信された SNMP メッセージの数 |
| outGetRequests | 送信した GetRequest メッセージの総数 |
| outGetNexts | 送信した GetNextRequest メッセージの総数 |
| outSetRequests | 送信した SetRequest メッセージの総数 |
| outGetResponses | 送信した GetResponse メッセージの総数 |
| outTraps | 送信した SNMP トラップの総数 |
| SNMPv3 counters セクション | SNMPv3 固有の統計カウンターが表示される |
| UnsupportedSecLevels | 未サポートのセキュリティレベルを含む SNMP パケット受信数 |
| NotInTimeWindows | 規定の時間内 (Time Window 内) に受信できなかった SNMP パケット受信数 |
| UnknownUserNames | 不明なユーザー名を含む SNMP パケット受信数 |
| UnknownEngineIDs | 不明なエンジン ID を含む SNMP パケット受信数 |
| WrongDigests | 認証データ (ダイジェスト) の値が予期したものと異なる SNMP パケット受信数 |
| DecryptionErrors | 復号できなかった SNMP パケット受信数 |
| UnknownSecModels | 未サポートのセキュリティモデルを含む SNMP パケット受信数 |

| | |
|--------------------|----------------------------|
| InvalidMsgs | 不正なコンポーネントを含む SNMP パケット受信数 |
| UnknownPDUHandlers | 不明な PDU を含む SNMP パケット受信数 |

表 74:

関連コマンド

CREATE SNMP COMMUNITY (167 ページ)

DISABLE SNMP (224 ページ)

DISABLE SNMP AUTHENTICATE_TRAP (225 ページ)

ENABLE SNMP (257 ページ)

ENABLE SNMP AUTHENTICATE_TRAP (258 ページ)

SET SNMP ENGINEID (326 ページ)

SET SNMP LOCAL (328 ページ)

SHOW SNMP COMMUNITY (441 ページ)

SHOW SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

SHOW SNMP COMMUNITY=community

community: SNMP コミュニティー名（1～15 文字。大文字小文字を区別する）

解説

（SNMPv1/v2c）SNMP コミュニティーの情報を表示する。

パラメーター

COMMUNITY SNMP コミュニティー名

入力・出力・画面例

```
Manager > show snmp community=public

SNMP community information:
  Name ..... public
  Access ..... read-only
  Status ..... Enabled
  Traps ..... Disabled
  Open access ..... No
  Manager ..... 192.168.1.11
  Manager ..... 192.168.1.5
  Manager ..... 192.168.1.2
  Trap host ..... 192.168.1.11
  V2c Trap host ..... 192.168.1.11
  V2c Trap host ..... 192.168.1.5
```

| | |
|---------------|---|
| Name | コミュニティー名 |
| Access | コミュニティーのアクセス権。read-only、read-write のどちらか |
| Status | コミュニティーの状態。Enabled か Disabled |
| Traps | トラップ生成の有効・無効 |
| Open access | すべてのホストから SNMP によるアクセスを許可するかどうか。Yes または No |
| Manager | 本コミュニティー名でのアクセスを許可された管理ステーション（SNMP マネージャー）の IP アドレス |
| Trap host | SNMPv1 トラップの送信先 IP アドレス |
| V2c Trap host | SNMPv2c トラップの送信先 IP アドレス |

表 75:

関連コマンド

SHOW SNMP (437 ページ)

SHOW SNMP GROUP

カテゴリー：運用・管理 / SNMP

SHOW SNMP GROUP [=group]

group: SNMP グループ名 (1～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ユーザーグループの設定内容を表示する。

パラメーター

GROUP SNMP グループ名。省略時はすべてのグループが表示される。

入力・出力・画面例

```
Manager > show snmp group

SNMP Group information:
  Group Name ..... admins
    Security Level ..... authPriv
    Read View ..... most
    Write View ..... most
    Notification View ..... most
    Row Status ..... active
  Group Name ..... mib2operators
    Security Level ..... authNoPriv
    Read View ..... standard
    Write View ..... -
    Notification View ..... most
    Row Status ..... active
```

| Group Name | グループ名 |
|-------------------|--|
| Security Level | セキュリティーレベル。noAuthNoPriv (認証なし・暗号化なし) authNoPriv (認証あり・暗号化なし) authPriv (認証あり・暗号化あり) のいずれか |
| Read View | 読み出しアクセス可能なビュー名 |
| Write View | 書き込みアクセス可能なビュー名 |
| Notification View | 通知を受信可能なビュー名 |
| Row Status | グループの状態。active、notInService、notReady のいずれか |

表 76:

関連コマンド

ADD SNMP GROUP (136 ページ)

SET SNMP GROUP (327 ページ)

SHOW SNMP TARGETADDR

カテゴリー：運用・管理 / SNMP

SHOW SNMP TARGETADDR [=target]

target: SNMP ターゲット名 (1~32 文字。大文字小文字を区別する)

解説

(SNMPv3) ターゲット (通知メッセージの送信先) の設定内容を表示する。

パラメーター

TARGETADDR SNMP ターゲット名。省略時はすべてのターゲットが表示される。

入力・出力・画面例

```

Manager > show snmp target

SNMP target address information:
  Target Address Name ..... mg2
    IP address ..... 172.28.28.16
    UDP port ..... 162
    Target Address Params ..... psupervisor
    Row Status ..... active
  Target Address Name ..... tpR30
    IP address ..... 172.28.28.156
    UDP port ..... 162
    Target Address Params ..... pzein
    Row Status ..... active

```

| | |
|-----------------------|---|
| Target Address Name | ターゲット名 |
| IP address | IP アドレス |
| UDP port | UDP ポート番号 |
| Target Address Params | ターゲットパラメーターセット名 |
| Row Status | ターゲットの状態。active、notInService、notReady のいずれか |

表 77:

関連コマンド

ADD SNMP TARGETADDR (138 ページ)

[ADD SNMP TARGETPARAMS \(140 ページ \)](#)

[DELETE SNMP TARGETADDR \(200 ページ \)](#)

[SET SNMP TARGETADDR \(329 ページ \)](#)

[SHOW SNMP TARGETPARAMS \(447 ページ \)](#)

SHOW SNMP TARGETPARAMS

カテゴリー：運用・管理 / SNMP

SHOW SNMP TARGETPARAMS [=params]

params: SNMP ターゲットパラメーターセット名 (1~32 文字。大文字小文字を区別する)

解説

(SNMPv3) ターゲット (通知メッセージの送信先) との通信に使用するパラメーターセット (セキュリティレベルとユーザー名) の設定内容を表示する。

パラメーター

TARGETPARAMS SNMP ターゲットパラメーターセット名。省略時はすべてのパラメーターセットが表示される。

入力・出力・画面例

```

Manager > show snmp targetparams

SNMP target params information:
  Target Params Name ..... psupervisor
    Security Level ..... authPriv
    User Name ..... supervisor
    Row Status ..... active
  Target Params Name ..... pzein
    Security Level ..... authNoPriv
    User Name ..... zein
    Row Status ..... active
    
```

| | |
|--------------------|--|
| Target Params Name | ターゲットパラメーターセット名 |
| Security Level | セキュリティレベル。noAuthNoPriv(認証なし・暗号化なし) authNoPriv (認証あり・暗号化なし) authPriv (認証あり・暗号化あり) のいずれか |
| User Name | ユーザー名 |
| Row Status | ターゲットパラメーターセットの状態。active、notInService、notReady のいずれか |

表 78:

関連コマンド

ADD SNMP TARGETPARAMS (140 ページ)

DELETE SNMP TARGETPARAMS (201 ページ)

SET SNMP TARGETPARAMS (330 ページ)

SHOW SNMP USER

カテゴリー：運用・管理 / SNMP

SHOW SNMP USER [=username]

username: SNMP ユーザー名 (1～32 文字。大文字小文字を区別する)

解説

(SNMPv3) ユーザーの設定内容を表示する。

パラメーター

USER SNMP ユーザー名

入力・出力・画面例

```
Manager > show snmp user

SNMP User information:
  User Name ..... zein
    Group Name ..... mib2operators
    Auth Protocol ..... SHA
    Priv Protocol ..... NONE
    Row Status ..... active
  User Name ..... supervisor
    Group Name ..... admins
    Auth Protocol ..... MD5
    Priv Protocol ..... DES
    Row Status ..... active
```

| | |
|---------------|---|
| User Name | ユーザー名 |
| Group Name | 所属先グループ名 |
| Auth Protocol | 認証プロトコル |
| Priv Protocol | 暗号化プロトコル |
| Row Status | ユーザーの状態。active、not in service、not ready のいずれか |

表 79:

関連コマンド

ADD SNMP USER (142 ページ)

[DELETE SNMP USER \(202 ページ \)](#)

[SET SNMP USER \(332 ページ \)](#)

SHOW SNMP VIEW

カテゴリー：運用・管理 / SNMP

SHOW SNMP VIEW [=view]

view: SNMP ビュー名 (1~32 文字。大文字小文字を区別する)

解説

(SNMPv3) ビューの設定内容を表示する。

パラメーター

VIEW SNMP ビュー名。ビュー名を指定しなかった場合は、定義されているビュー名の一覧が表示される。ビュー名を指定した場合は、指定したビューの設定内容が表示される。

入力・出力・画面例

```

Manager > show snmp view

SNMP View information:
  SNMP View name(s):
    most
    standard
    mib2notcpudp

Manager > show snmp view=mib2notcpudp

SNMP View information:
  View Name ..... mib2notcpudp
  OID ..... 1.3.6.1.2.1
    MIB ..... mib-2
    Type ..... include
    Row Status ..... active
  OID ..... 1.3.6.1.2.1.6
    MIB ..... tcp
    Type ..... exclude
    Row Status ..... active
  OID ..... 1.3.6.1.2.1.7
    MIB ..... udp
    Type ..... exclude
    Row Status ..... active

```

| | |
|------------|--|
| View Name | ビュー名 |
| OID | ビューに含まれる (Type=include) または含まれない (Type=exclude) MIB ノードの OID (Object Identifier) |
| MIB | OID で示される MIB ノードの名前。OID に該当するノード名がシステムに定義されている場合のみ表示される |
| Type | OID で示される MIB ノードがビューに含まれているかどうか。include なら含まれ、exclude なら含まれない |
| Row Status | ビューの状態。active、not in service、not ready のいずれか |

表 80:

備考・注意事項

ビュー内のエントリは OID の辞書順にソートされて表示される。

関連コマンド

ADD SNMP VIEW (144 ページ)

DELETE SNMP VIEW (203 ページ)

SHOW SSH

カテゴリー：運用・管理 / Secure Shell

SHOW SSH [COUNTERS]

解説

SSH サーバーおよびクライアント機能の設定情報または統計情報を表示する。

パラメーター

COUNTERS SSH に関する統計カウンターを表示する。省略時は SSH の設定情報が表示される。

入力・出力・画面例

```
Manager > show ssh

SSH Configuration
Version..... 1.5
Server Enabled..... TRUE
Maximum Sessions ..... 6
Port..... 22
Host Key ID..... 1
Host Key Bits..... 1024
Server Key ID..... 2
Server Key Bits..... 768
Server Key Expiry(hours)... 1
Login Timeout(secs)..... 60
Idle Timeout(secs) ..... Off
Authentication Available... Password,RSA
Ciphers Available..... DES
Services Available..... Shell,Cmd

Manager > show ssh counters

Secure Shell Counters:

    inOctets          16866   outOctets          43477
    rxPkt             743    txPkt              785
    rxPktCheckFail    0     txPktFail          0
    rxVersionID       9     txVersionID        9

    rxMSGDisconnect   4     txMSGDisconnect    0
    rxSMSGPublicKey   0     txSMSGPublicKey    9
    rxCMSGSessionKey  5     txCMSGSessionKey   0
    rxCMSGUser        5     txCMSGUser         0
```

| | | | |
|--------------------------|-----|--------------------------|-----|
| rxCMSSAuthRhosts | 0 | txCMSSAuthRhosts | 0 |
| rxCMSSAuthRSA | 8 | txCMSSAuthRSA | 0 |
| rxSMSSAuthRSACHallenge | 0 | txSMSSAuthRSACHallenge | 0 |
| rxCMSSAuthRSAResponse | 0 | txCMSSAuthRSAResponse | 0 |
| rxCMSSAuthPassword | 2 | txCMSSAuthPassword | 0 |
| rxCMSSAuthRhostsRSA | 0 | txCMSSAuthRhostsRSA | 0 |
| rxSMSSSuccess | 0 | txSMSSSuccess | 7 |
| rxSMSSFailure | 0 | txSMSSFailure | 14 |
| rxCMSSReqCompression | 0 | txCMSSReqCompression | 0 |
| rxCMSSReqX11Forwarding | 0 | txCMSSReqX11Forwarding | 0 |
| rxCMSSReqPortForwarding | 0 | txCMSSReqPortForwarding | 0 |
| rxCMSSReqAgentForwarding | 0 | txCMSSReqAgentForwarding | 0 |
| rxCMSSReqPty | 1 | txCMSSReqPty | 0 |
| rxCMSSWindowSize | 0 | txCMSSWindowSize | 0 |
| rxCMSSExecShell | 1 | txCMSSExecShell | 0 |
| rxCMSSExecCmd | 0 | txCMSSExecCmd | 0 |
| rxCMSSStdInData | 708 | txCMSSStdInData | 0 |
| rxSMSSStdOutData | 0 | txSMSSStdOutData | 746 |
| rxSMSSStdErrData | 0 | txSMSSStdErrData | 0 |
| rxCMSSGEof | 0 | txCMSSGEof | 0 |
| rxSMSSExitStatus | 0 | txSMSSExitStatus | 0 |
| rxCMSSExitConfirmation | 0 | txCMSSExitConfirmation | 0 |
| rxUnSupportedMsg | 0 | | |
| rxUnknownMsg | 0 | | |
| encodeSKSuccess | 0 | decodeSKSuccess | 5 |
| encodeSKFail | 0 | decodeSKFail | 0 |
| getHostKeyFail | 0 | getServerKeyFail | 0 |
| serverKeyReGenerated | 0 | | |
| encoderSACHallengeGood | 0 | decoderSACHallengeGood | 0 |
| encoderSACHallengeFail | 0 | decoderSACHallengeFail | 0 |
| getUserKeyFail | 0 | | |
| encoConfigured | 5 | encoConfigureFail | 0 |
| encoDetached | 0 | encoDead | 0 |
| encoEncodeStart | 767 | encoDecodeStart | 729 |
| encoEncoded | 767 | encoDecoded | 729 |
| encoEncodeFail | 0 | encoDecodeFail | 0 |
| encoEncodeResetDone | 0 | encoDecodeResetDone | 0 |
| encoEncodeResetFail | 0 | encoDecodeResetFail | 0 |
| encoEncodeDiscard | 0 | encoDecodeDiscard | 0 |

| | |
|------------------|----------------------------------|
| Version | 対応している SSH プロトコルのバージョン |
| Server Enabled | SSH サーバー機能が有効かどうか |
| Maximum Sessions | |
| Port | SSH サーバーの TCP リスニングポート。デフォルトは 22 |
| Host Key ID | ホストキーの鍵番号 |

| | |
|---------------------------|---|
| Host Key Bits | ホストキーの長さ (768 ~ 2048 ビット) |
| Server Key ID | サーバーキーの鍵番号 |
| Server Key Bits | サーバーキーの長さ (<= ホストキー長 - 128 ビット かつ >= 512 ビット) |
| Server Key Expiry (hours) | サーバーキーの有効期間 (時間) |
| Login Timeout (secs) | ログインタイムアウト (秒) |
| Idle Timeout (secs) | |
| Authentication Available | 使用可能な認証方式。Password または RSA |
| Ciphers Available | 使用可能な暗号アルゴリズム (DES のみ) |
| Services Available | 使用可能なサービス。Shell または Cmd |

表 81: 設定情報 (COUNTERS オプションなし)

| | |
|-------------------|--|
| inOctets | 受信オクテット数 |
| outOctets | 送信オクテット数 |
| rxPkt | 受信パケット数 |
| txPkt | 送信パケット数 |
| rxPktCheckFail | チェックサムエラーパケット受信数 |
| txPktFail | 送信前破棄パケット数 (エラーによる) |
| rxVersionID | バージョン ID メッセージ受信数 |
| txVersionID | バージョン ID メッセージ送信数 |
| rxMSGDisconnect | セッション切断メッセージ (SSH_MSG_DISCONNECT) 受信数 |
| txMSGDisconnect | セッション切断メッセージ (SSH_MSG_DISCONNECT) 送信数 |
| rxSMSGPublicKey | SSH_SMSG_PUBLIC_KEY メッセージ受信数 (本機の SSH クライアントによる)。同メッセージには、リモートサーバーのホストキー、サーバーキー公開鍵、使用可能な暗号アルゴリズムと認証方式が含まれる |
| txSMSGPublicKey | SSH_SMSG_PUBLIC_KEY メッセージ送信数 (本機の SSH サーバーによる)。同メッセージには、自機のホストキー、サーバーキー公開鍵、使用可能な暗号アルゴリズムと認証方式が含まれる |
| rxCMSSGSessionKey | SSH_CMSG_SESSION_KEY メッセージ受信数 (本機の SSH サーバーによる)。同メッセージには、リモートクライアントが選択した暗号アルゴリズム、サーバー側から受け取った 64 ビットクッキーのコピー、クライアントのプロトコルフラグ、サーバーのホストキーとサーバーキーで暗号化されたセッションキーが含まれる |
| txCMSSGSessionKey | SSH_CMSG_SESSION_KEY メッセージ送信数 (本機の SSH クライアントによる)。同メッセージには、本機のクライアントが選択した暗号アルゴリズム、リモートサーバーから受け取った 64 ビットクッキーのコピー、クライアントのプロトコルフラグ、リモートサーバーのホストキーとサーバーキーで暗号化したセッションキーが含まれる |

| | |
|------------------------|--|
| rxCMMSGUser | SSH.CMSG.USER メッセージ受信数（本機の SSH サーバーによる）。同メッセージにはログインユーザー名が含まれる |
| txCMMSGUser | SSH.CMSG.USER メッセージ送信数（本機の SSH クライアントによる）。同メッセージにはログインユーザー名が含まれる |
| rxCMMSGAuthRhosts | 本機の SSH サーバーが受信した SSH.CMSG.AUTH.RHOSTS メッセージ数。同メッセージには.rhosts 認証で使うリモートクライアントのユーザー名が含まれる。txCMMSGAuthRhosts |
| rxCMMSGAuthRSA | 本機の SSH サーバーが受信した SSH.CMSG.AUTH.RSA メッセージ数。同メッセージには、リモートクライアントの RSA 公開鍵が含まれる |
| txCMMSGAuthRSA | 本機の SSH クライアントが送信した SSH.CMSG.AUTH.RSA メッセージ数。同メッセージには、ローカルクライアントの RSA 公開鍵が含まれる |
| rxSMSGAuthRSAChallenge | 本機の SSH クライアントが受信した SSH.SMSG.AUTH.RSA.CHALLENGE メッセージ数。同メッセージには、暗号化されたリモートサーバーのチャレンジメッセージが含まれる |
| txSMSGAuthRSAChallenge | 本機の SSH サーバーが送信した SSH.SMSG.AUTH.RSA.CHALLENGE メッセージ数。同メッセージには、リモートクライアント宛てのチャレンジメッセージが含まれる |
| rxCMMSGAuthRSAResponse | 本機の SSH サーバーが受信した SSH.CMSG.AUTH.RSA.RESPONSE メッセージ数。同メッセージにはクライアントからのチャレンジレスポンスが含まれる |
| txCMMSGAuthRSAResponse | 本機の SSH クライアントが送信した SSH.CMSG.AUTH.RSA.RESPONSE メッセージ数。同メッセージにはサーバーからのチャレンジに対するレスポンスが含まれる |
| rxCMMSGAuthPassword | 本機の SSH サーバーが受信した SSH.CMSG.AUTH.PASSWORD メッセージ数。同メッセージには、リモートクライアントの平文パスワードが含まれる。txCMMSGAuthPassword |
| rxCMMSGAuthRhostsRSA | 本機の SSH サーバーが受信した SSH.CMSG.AUTH.RHOSTS.RSA メッセージ数。同メッセージにはリモートクライアントのユーザー名と、.rhosts/RSA 認証用のホストキー（公開鍵）が含まれる |
| txCMMSGAuthRhostsRSA | 本機の SSH クライアントが送信した SSH.CMSG.AUTH.RHOSTS.RSA メッセージ数。同メッセージには、ローカルクライアントのユーザー名と、.rhosts/RSA 認証用のホストキー（公開鍵）が含まれる |
| rxSMSGSuccess | 本機の SSH クライアントが受信した SSH.SMSG.SUCCESS メッセージ数。同メッセージはリクエスト成功を示す |
| txSMSGSuccess | 本機の SSH サーバーが送信した SSH.SMSG.SUCCESS メッセージ数。同メッセージはリクエスト成功を示す |

| | |
|-------------------------|---|
| rxMSGFailure | 本機の SSH クライアントが受信した SSH.MSG.FAILURE メッセージ数。同メッセージはリクエスト失敗を示す |
| txMSGFailure | 本機の SSH サーバーが送信した SSH.MSG.FAILURE メッセージ数。同メッセージはリクエスト失敗を示す |
| rxMSGReqCompression | 本機の SSH サーバーが受信した SSH.MSG.REQUEST.COMPRESSION メッセージ数。同メッセージは、接続の圧縮を要求する |
| txMSGReqCompression | 本機の SSH クライアントが送信した SSH.MSG.REQUEST.COMPRESSION メッセージ数。同メッセージは、接続の圧縮を要求する |
| rxMSGReqX11Forwarding | 本機の SSH サーバーが受信した SSH.MSG.X11.REQUEST.FORWARDING メッセージ数。同メッセージは X11 接続の転送を要求する |
| txMSGReqX11Forwarding | 本機の SSH クライアントが送信した SSH.MSG.X11.REQUEST.FORWARDING メッセージ数。同メッセージは X11 接続の転送を要求する |
| rxMSGReqPortForwarding | 本機の SSH サーバーが受信した SSH.MSG.PORT.FORWARD.REQUEST メッセージ数。同メッセージはポートフォワーディングを要求する |
| txMSGReqPortForwarding | SSH クライアントが送信した SSH.MSG.PORT.FORWARD.REQUEST メッセージ数。同メッセージはポートフォワーディングを要求する |
| rxMSGReqAgentForwarding | 本機の SSH サーバーが受信した SSH.MSG.AGENT.REQUEST.FORWARDING メッセージ数。同メッセージは、接続を認証エージェントに転送するよう要求する |
| txMSGReqAgentForwarding | 本機の SSH クライアントが送信した SSH.MSG.AGENT.REQUEST.FORWARDING メッセージ数。同メッセージは、接続を認証エージェントに転送するよう要求する |
| rxMSGReqPty | 本機の SSH サーバーが受信した SSH.MSG.REQUEST.PTY メッセージ数。同メッセージは疑似端末 (Pseudo Terminal) デバイスの割り当てを要求する |
| txMSGReqPty | 本機の SSH クライアントが送信した SSH.MSG.REQUEST.PTY メッセージ数。同メッセージは疑似端末 (Pseudo Terminal) デバイスの割り当てを要求する |
| rxMSGWindowSize | 本機の SSH クライアントが送信した SSH.MSG.WINDOW.SIZE メッセージ数。同メッセージはクライアントの新しいウィンドウサイズを指定する |

| | |
|-----------------|---|
| txMSGWindowSize | 本機の SSH サーバーが受信した SSH_MSG_WINDOW_SIZE メッセージ数。同メッセージはクライアントの新しいウィンドウサイズを指定する |
| rxMSGExecShell | 本機の SSH サーバーが受信した SSH_MSG_EXEC_SHELL メッセージ数。同メッセージはインタラクティブな端末セッションを開始するために使用される |
| txMSGExecShell | 本機の SSH クライアントが送信した SSH_MSG_EXEC_SHELL メッセージ数。同メッセージはインタラクティブな端末セッションを開始するために使用される |
| rxMSGExecCmd | 本機の SSH サーバーが受信した SSH_MSG_EXEC_CMD メッセージ数。同メッセージにはサーバー上で実行すべきコマンドが含まれる |
| txMSGExecCmd | 本機の SSH クライアントが送信した SSH_MSG_EXEC_CMD メッセージ数。同メッセージにはサーバー上で実行すべきコマンドが含まれる |
| rxMSGStdInData | 本機の SSH クライアントが受信した SSH_MSG_STDIN_DATA メッセージ数。同メッセージには、リモートサーバー上のアプリケーションが標準出力に書き込んだデータが含まれる |
| txMSGStdInData | 本機の SSH クライアントが送信した SSH_MSG_STDOUT_DATA メッセージ数。同メッセージには、リモートサーバーの標準入力に書き込まれるデータが含まれる |
| rxMSGStdOutData | 本機の SSH サーバーが受信した SSH_MSG_STDOUT_DATA メッセージ数。同メッセージには、ローカルサーバーの標準入力に書き込まれるデータが含まれる。txMSGStdOutData |
| rxMSGStdErrData | 本機の SSH クライアントが受信した SSH_MSG_STDERR_DATA メッセージ数。同メッセージには、リモートサーバー上のアプリケーションが標準エラー出力に書き込んだデータが含まれる |
| txMSGStdErrData | 本機の SSH サーバーが送信した SSH_MSG_STDERR_DATA メッセージ数。同メッセージには、ローカルサーバー上のアプリケーションが標準エラー出力に書き込んだデータが含まれる |
| rxMSGEOF | 本機の SSH サーバーが受信した SSH_MSG_EOF メッセージ数。同メッセージはリモートクライアントからのデータ入力終了を示す |
| txMSGEOF | 本機の SSH クライアントが送信した SSH_MSG_EOF メッセージ数。同メッセージは、ローカルクライアントからのデータ入力終了を示す |
| rxMSGExitStatus | 本機の SSH クライアントが受信した SSH_MSG_EXITSTATUS メッセージ数。同メッセージは、リモートサーバー上でシェルやコマンドの実行が終了したことを示す。txMSGExitStatus |

| | |
|-------------------------|--|
| rxCMSSGExitConfirmation | 本機のSSHサーバーが受信したSSH_CMSG_EXIT_CONFIRMATIONメッセージ数。これは、サーバーがクライアントに送信したSSH_SMSG_EXITSTATUSメッセージへの応答 |
| txCMSSGExitConfirmation | 本機のSSHクライアントが送信したSSH_CMSG_EXIT_CONFIRMATIONメッセージ数。これは、サーバーから受信したSSH_SMSG_EXITSTATUSメッセージへの応答 |
| rxUnSupportedMsg | 本機のSSHサーバーが受信した未サポートオプションへの要求メッセージ数 |
| rxUnknownMsg | 本機のSSHサーバーが受信した不明なオプションへの要求メッセージ数。encodeSKSuccess |
| decodeSKSuccess | セッションキーのRSA復号化に成功した回数 |
| encodeSKFail | セッションキーの暗号化に失敗した回数 |
| decodeSKFail | セッションキーの復号化に失敗した回数 |
| getHostKeyFail | ENCOモジュールからのホストキー取得に失敗した回数 |
| getServerKeyFail | ENCOモジュールからのサーバーキー取得に失敗した回数 |
| serverKeyReGenerated | サーバーキーを生成しなおした回数 |
| encodeRSAChallengeGood | サーバーがRSA認証用のチャレンジを暗号化した回数 |
| decodeRSAChallengeGood | サーバーがRSA認証用のチャレンジを復号化した回数 |
| encodeRSAChallengeFail | サーバーがRSA認証用のチャレンジの暗号化に失敗した回数 |
| decodeRSAChallengeFail | サーバーがRSA認証用のチャレンジの復号化に失敗した回数 |
| getUserKeyFail | サーバーがENCOモジュールからユーザーのRSA鍵取得に失敗した回数 |
| encoEncodeConfigured | セッション用に暗号化チャンネルが設定された回数 |
| encoDecodeConfigured | セッション用に復号化チャンネルが設定された回数 |
| encoEncodeConfigureFail | サーバーが暗号化チャンネルの設定に失敗した回数 |
| encoDecodeConfigureFail | サーバーが復号化チャンネルの設定に失敗した回数 |
| encoEncodeDetached | セッション用の暗号化チャンネルが削除された回数 |
| encoDecodeDetached | セッション用の復号化チャンネルが削除された回数 |
| encoEncodeDead | 暗号化エンジンが障害により停止した回数 |
| encoDecodeDead | 復号化エンジンが障害により停止した回数 |
| encoEncodeStart | ENCOチャンネル上で暗号化ジョブが開始された回数 |
| encoDecodeStart | ENCOチャンネル上で復号化ジョブが開始された回数 |
| encoEncoded | 暗号化ジョブが完了した回数 |
| encoDecoded | 復号化ジョブが完了した回数 |
| encoEncodeFail | 暗号化ジョブが完了できなかった回数 |
| encoDecodeFail | 復号化ジョブが完了できなかった回数 |
| encoEncodeResetDone | 暗号化チャンネルがリセットされた回数 |

| | |
|---------------------|------------------------------|
| encoDecodeResetDone | 復号化チャンネルがリセットされた回数 |
| encoEncodeResetFail | サーバーが暗号化チャンネルのリセットに失敗した回数 |
| encoDecodeResetFail | サーバーが復号化チャンネルのリセットに失敗した回数 |
| encoEncodeDiscard | ENCO モジュールによって暗号化ジョブが破棄された回数 |
| encoDecodeDiscard | ENCO モジュールによって復号化ジョブが破棄された回数 |

表 82: 統計情報 (COUNTERS オプションあり)

関連コマンド

DISABLE SSH SERVER (228 ページ)

ENABLE SSH SERVER (261 ページ)

SET SSH SERVER (333 ページ)

SHOW SSH SESSIONS (461 ページ)

SHOW SSH SESSIONS

カテゴリー：運用・管理 / Secure Shell

SHOW SSH SESSIONS

解説

現在オープン中の SSH セッション一覧を表示する。

サーバーセッションとクライアントセッションの両方が表示される。

入力・出力・画面例

| SecOff > show ssh sessions | | | | | | |
|----------------------------|-------|-----|---------------|---------|-------|-------------------|
| Secure Shell Sessions | | | | | | |
| ID | Type | Dir | Peer Address | User | State | Octets In/Out |
| 1 | Shell | In | 172.16.28.126 | manager | OPEN | 00003606/00004497 |
| 2 | Shell | Out | 172.16.28.185 | secoff | OPEN | 00001065/00000613 |

| | |
|---------------|---|
| ID | セッション ID |
| Type | セッション種別。Listen (接続待ちのセッション)、Shell (インタラクティブなログインセッション)、Cmd (リモートコマンド実行) のいずれか |
| Dir | セッションの方向。In (リモートクライアントから自機サーバーへ) または Out (自機クライアントからリモートサーバーへ) |
| Peer Address | リモートエンドの IP アドレス |
| User | ユーザー名。認証完了前は「-」と表示される |
| State | セッションの状態。Initial (接続開始)、Starting (ホスト間認証実行中)、Authen (ユーザー認証実行中)、Request (セッション種別のネゴシエーション中)、Open (セッション確立中) のいずれか |
| Octets In/Out | 送受信オクテット数 |

表 83:

関連コマンド

DISABLE SSH SERVER (228 ページ)

ENABLE SSH SERVER (261 ページ)

SET SSH SERVER (333 ページ)

SHOW SSH (453 ページ)

SHOW SSH USER

カテゴリー：運用・管理 / Secure Shell

SHOW SSH USER [=username]

username: ユーザー名 (1～15 文字。英数字。空白不可)

解説

SSH ユーザーの情報を表示する。

パラメーター

USER 表示する SSH ユーザー名を指定。省略時はすべての SSH ユーザーの一覧が表示される。指定時は該当ユーザーの詳細情報が表示される。

入力・出力・画面例

```
Manager > show ssh user

Secure Shell User List

User           IpAddr           Authentication   KeyId           Status
-----
admin          0.0.0.0          RSA              100             enabled
manager        0.0.0.0          Password         0               enabled

Manager > show ssh user=admin

User..... admin
Status..... Enabled
Authentication method..... RSA
RSA key ID..... 100
Shell..... Yes
IpAddress..... 0.0.0.0
Mask..... 255.255.255.255
Failed Logins..... 2
```

| | |
|----------------|-----------------------|
| User | SSH ユーザー名 |
| IpAddr | ログインが許可されている IP アドレス |
| Authentication | 認証方式。Password または RSA |
| KeyId | RSA 認証で用いる鍵番号 |

| | |
|--------|-------------------------------|
| Status | アカウントの状態。Enabled または Disabled |
|--------|-------------------------------|

表 84: ユーザー無指定（一覧表示）の場合

| | |
|----------------------|-------------------------------|
| User | SSH ユーザー名 |
| Status | アカウントの状態。Enabled または Disabled |
| Authorisation method | 認証方式。Password または RSA |
| RSA key ID | RSA 認証で用いる鍵番号 |
| Shell | シェルを利用可能か。TRUE または FALSE |
| IpAddress | ログインが許可されている IP アドレス |
| Mask | IpAddress に対するネットマスク |
| Failed Logins | ログイン失敗回数 |

表 85: ユーザー指定の場合

関連コマンド

ADD SSH USER (147 ページ)

DELETE SSH USER (204 ページ)

DISABLE SSH USER (229 ページ)

ENABLE SSH USER (262 ページ)

SET SSH USER (334 ページ)

SHOW STARTUP

カテゴリー：運用・管理 / システム

SHOW STARTUP

解説

起動時のシステム診断結果を表示する。エラーを示す項目には「>」が付く。

入力・出力・画面例

```
Manager > show startup

Router Startup Status Flag is 00400400, which means:
-----
  65536k of RAM found
Router OK prior to this startup
Battery backed RAM battery OK
NVS not corrupted
Real time clock not corrupted
Real time clock, time set
Router software download OK
Router vector download OK
-----
```


SHOW SYSTEM

カテゴリー：運用・管理 / システム

SHOW SYSTEM

解説

システム情報を表示する。

入力・出力・画面例

```

Manager > show system

Router System Status                               Time 16:41:12 Date 17-Aug-2010.
Board      ID Bay  Board Name                      Host Id Rev   Serial number
-----
Base       257    AR570S                               0 M2-0   D16561013
-----
Memory -    DRAM :131072 kB    FLASH : 32768 kB
Chip Revisions -
-----
SysDescription
CentreCOM AR570S version 2.9.2-00 30-Jul-2010
SysContact

SysLocation

SysName

SysDistName

SysUpTime
1230 ( 00:00:12 )
Boot Image      : 570-104.fbr size 771920 16-Mar-2006
Software Version: 2.9.2-00 30-Jul-2010
Release Version : 2.9.2-00 30-Jul-2010
Patch Installed : NONE
Territory       : japan
Country         : none
Help File       : help.hlp

Main Fan        : On
CPU Fan         : On

Temperature     : 43 Celsius
Main Fan Speed  : 5921 RPM
CPU Fan Speed   : 6026 RPM

```

```
Voltage Status ( Rail : Read )
  1.2V : 1.18V   2.5V : 2.60V   3.3V : 3.33V
  5.0V : 5.01V  12.0V : 11.99V
```

```
Battery voltage : 3.26V
```

```
Configuration
```

```
Boot configuration file: None
```

```
Current configuration: None
```

```
Security Mode      : Disabled
```

| | |
|-------------------------|--|
| Board | 基板の種類 |
| ID | 基板の ID |
| Bay | IO Module や IC Module が実装されているベイの番号 |
| Board Name | 基板の名称 |
| Rev | 基板のリビジョンとハードウェア改修レベル |
| Serial number | 基板のシリアル番号 |
| DRAM | 実装されている DRAM メモリー容量 |
| FLASH | 実装されている FLASH メモリーの容量 |
| SysDescription | 製品およびファームウェアの概要 (MIB-II の sysDescr) |
| SysContact | 管理責任者 (MIB-II の sysContact) |
| SysLocation | 設置場所 (MIB-II の sysLocation) |
| SysName | システム名 (MIB-II の sysName) |
| SysDistName | X.500 識別名 (DN = Distinguished Name) |
| SysUpTime | 稼働時間 (前回リブートしてからの時間) |
| Software Version | パッチバージョン |
| Release Version | ソフトウェアリリースバージョン |
| Patch Installed | インストールされているパッチの説明。NONE はパッチなし |
| Territory | 地域 (australia、 china、 europe、 japan、 korea、 newzealand、 usa) |
| Help File | HELP コマンドが使用するヘルプファイル名 |
| Main Fan | ファンの状態 |
| Temperature | 本製品内部の温度。Celsius () で表示 |
| Main Fan Speed | ファンの回転数。RPM (毎分回転数) で表示 |
| Voltage Status | 1.2V、2.5V、3.3V、5.0V、12.0V 各電源の実際の供給電圧 |
| Battery voltage | バッテリー電圧 |
| Boot configuration file | 起動時に読み込まれる設定ファイル名 |
| Current configuration | 現在の設定のもととなったファイル名 |
| Security Mode | セキュリティーモードで動作しているか。enabled または disabled |

表 86:

関連コマンド

DISABLE SYSTEM SECURITY_MODE (230 ページ)

ENABLE SYSTEM SECURITY_MODE (263 ページ)

SET HELP (296 ページ)

SET SYSTEM CONTACT (335 ページ)

SET SYSTEM DISTINGUISHEDNAME (336 ページ)

SET SYSTEM LOCATION (337 ページ)

SET SYSTEM NAME (338 ページ)

SHOW TELNET

カテゴリー：運用・管理 / ターミナルサービス

SHOW TELNET

解説

Telnet サーバーの状態などを表示する。

入力・出力・画面例

```
Manager > show telnet

TELNET Module Configuration
-----
Telnet Server ..... Enabled
Telnet Server Listen Port ..... 23
Telnet Terminal Type ..... UNKNOWN
Telnet Insert Null's ..... Off
Telnet Com Port Control ..... Disabled
Telnet Current Sessions ..... 0
Telnet Session Limit ..... 32
Telnet Idle Timeout ..... Off
-----
```

| | |
|---------------------------|-------------------------------|
| Telnet Server | Telnet サーバーの有効・無効 |
| Telnet Server Listen Port | Telnet サーバーのリスニング TCP ポート |
| Telnet Terminal Type | Telnet サーバーへの接続時に送信する端末タイプ文字列 |
| Telnet Insert Null's | CR のあとにヌル文字を挿入するかどうか |
| Telnet Com Port Control | 未サポート |
| Telnet Current Sessions | 現在確立している Telnet セッション数 |
| Telnet Session Limit | 同時確立可能な Telnet セッションの最大数 |
| Telnet Idle Timeout | Telnet セッションのアイドル時タイムアウト（秒） |

表 87:

関連コマンド

DISABLE TELNET SERVER (231 ページ)

ENABLE TELNET SERVER (264 ページ)

SHOW TIME

カテゴリー：運用・管理 / システム

SHOW TIME

解説

現在の日付と時刻を表示する。

入力・出力・画面例

```
Manager > show time  
  
System time is 21:59:55 on Tuesday 20-Apr-2010.
```

関連コマンド

SET TIME (341 ページ)

SHOW TRIGGER

カテゴリー：運用・管理 / トリガー

SHOW TRIGGER [=trigger-id] [{COUNTER|FULL|STATUS|SUMMARY}]

trigger-id: トリガー番号 (1~250)

解説

トリガーおよびトリガーモジュールに関する情報を表示する。

パラメーター

TRIGGER トリガー番号。省略時はすべてのトリガーに関するサマリー情報が表示される。

COUNTER トリガー機能全体の統計カウンターが表示される。トリガー番号は指定できない。

FULL トリガーに関する詳細な情報が表示される。

STATUS トリガー機能の状態に関する情報が表示される。トリガー番号は指定できない。

SUMMARY すべてのトリガーに関するサマリー情報が表示される。

入力・出力・画面例

```
Manager > show trigger
```

| TR# | Type & Details | Name | En | Te | Rept | #Scr | Days/Date |
|-----|----------------|------|----|----|------|------|-----------|
| 001 | Reboot (All) | | Y | N | Yes | 01 | MTWTFSS |
| 002 | CPU (80 %) UP | | Y | N | Yes | 01 | MTWTFSS |

```
Manager > show trigger counter
```

```
Trigger Module Counters
```

```
-----
Polls (05 sec timer) ..... 28
Idle loop entry count ..... 0
Time trigger checks ..... 26
Time trigger queue rebuilds ..... 4
Trigger activations ..... 1
Time triggers activated today ..... 0
Periodic triggers activated today .. 0
Interface triggers activated today . 0
Resource triggers activated today .. 0
Module triggers activated today .... 0
```

```

Manager > show trigger=2 full

Trigger ..... 2
Name ..... -
Type and details ..... CPU (80 %) UP
Days ..... Daily
Enabled ..... Enabled
Test ..... No
Repeat ..... Yes
Created/Modified ..... 13-Jul-2001 16:16:02
Number of Activations ..... 0
Last Activation ..... **-*-*** **:**:**
Number of scripts ..... 1

    mail.scp

```

```

Manager > show trigger status

```

Trigger Module Configuration

General

```

    Trigger Module ..... Enabled
    Triggers configured ..... 2
    Queued Commands ..... 0

```

Time Triggers

```

    Configured ..... 0
    Active ..... 0
    Activated today ..... 0

```

Periodic Triggers

```

    Configured ..... 0
    Active ..... 0
    Activated today ..... 0

```

Reboot Triggers

```

    Configured ..... 1

```

Interface Triggers

```

    Configured ..... 0

```

Resource Triggers

```

    Configured ..... 1
    Active ..... 1
    Activated today ..... 0

```

Module Triggers

```

    Configured ..... 0
    Activated today ..... 0

```

| | |
|----------------|---|
| TR# | トリガー番号 |
| Type & Details | トリガーの種類とその他の情報 |
| Name | トリガー名（メモ） |
| En | 有効かどうか |
| Te | テストモードかどうか |
| Rept | 複数回実行の可否。Yes（可） No（不可）あるいは残り実行回数。残り実行回数が一回になると表示が No になり、もう実行できなくなると、En フィールドの表示が N になる |
| #Scr | 設定されているスクリプトの数 |
| Days/Date | トリガーが有効な曜日または日時。有効な曜日が頭文字（MTWTFSS）で表される。無効な曜日は「-」で示される |

表 88:

| | |
|-----------------------|---|
| Trigger | トリガー番号 |
| Name | トリガー名（メモ） |
| Type and details | トリガーの種類とその他の情報 |
| Other parameters | モジュールトリガー独自のパラメーター |
| Days | トリガーが有効な曜日。Weekdays（月～金） Weekends（土日） Daily（毎日）あるいは各曜日が表示される。Days と Date はどちらか一方のみ表示される |
| Date | トリガーが有効な日付。Days と Date はどちらか一方のみ表示される |
| Enabled | トリガーの有効・無効 |
| Test | テストモードかどうか |
| Repeat | 複数回実行の可否。Yes（可） No（不可）あるいは残り実行回数 |
| Created/Modified | 作成日時あるいは最終修正日時 |
| Number of Activations | トリガーが起動された回数（前回の再起動後） |
| Last Activation | 最終起動日時（手動起動は含めない） |
| Number of scripts | スクリプト数とスクリプト名一覧 |

表 89: FULL オプション

| | |
|--------------------------|-----------------------|
| General セクション | トリガー機能全般に関する情報 |
| Trigger Module | トリガー機能の有効・無効 |
| Triggers configured | トリガー数 |
| Queued commands | 実行待ちコマンド数 |
| Time Triggers セクション | 定時トリガーに関する情報 |
| Periodic Triggers セクション | 定期トリガーに関する情報 |
| Reboot Triggers セクション | 再起動トリガーに関する情報 |
| Interface Triggers セクション | インターフェーストリガーに関する情報 |
| Resource Triggers セクション | CPU およびメモリートリガーに関する情報 |

| | |
|-----------------------|-----------------|
| Module Triggers セクション | モジュールトリガーに関する情報 |
| Configured | トリガー数 |
| Active | 現在有効なトリガー数 |
| Activated today | 今日実行された回数 |

表 90: STATUS オプション

| | |
|------------------------------------|---|
| Polls (05 sec timer) | トリガーイベントのチェック回数 |
| Idle loop entry count | トリガーモジュールがコマンド実行を準備した回数 |
| Time trigger checks | トリガーモジュールが定時トリガーをチェックした回数 |
| Time trigger queue rebuilds | 定時トリガーの追加、削除、変更、あるいは、システム日時の変更があったために、定時トリガーキューを再構成した回数 |
| Trigger activations | トリガー起動回数 |
| Time triggers activated today | 定時トリガーの起動回数（本日） |
| Periodic triggers activated today | 定期トリガーの起動回数（本日） |
| Interface triggers activated today | インターフェーストリガーの起動回数（本日） |
| Resource triggers activated today | CPU またはメモリートリガーの起動回数（本日） |
| Module triggers activated today | モジュールトリガーの起動回数（本日） |

表 91: COUNTER オプション

関連コマンド

ACTIVATE TRIGGER (121 ページ)
 ADD TRIGGER (149 ページ)
 CREATE TRIGGER CPU (169 ページ)
 CREATE TRIGGER FIREWALL (171 ページ)
 CREATE TRIGGER INTERFACE (173 ページ)
 CREATE TRIGGER MEMORY (175 ページ)
 CREATE TRIGGER MODULE (177 ページ)
 CREATE TRIGGER PERIODIC (180 ページ)
 CREATE TRIGGER REBOOT (182 ページ)
 CREATE TRIGGER TIME (184 ページ)
 DELETE TRIGGER (205 ページ)
 DESTROY TRIGGER (211 ページ)
 DISABLE TRIGGER (232 ページ)
 ENABLE TRIGGER (265 ページ)
 PURGE TRIGGER (283 ページ)
 SET TRIGGER CPU (342 ページ)
 SET TRIGGER FIREWALL (344 ページ)
 SET TRIGGER INTERFACE (346 ページ)
 SET TRIGGER MEMORY (348 ページ)

SET TRIGGER MODULE (350 ページ)
SET TRIGGER PERIODIC (352 ページ)
SET TRIGGER REBOOT (354 ページ)
SET TRIGGER TIME (356 ページ)

SHOW TTY

カテゴリー：運用・管理 / ターミナルサービス

SHOW TTY [=tty-number|ALL] [{SUMMARY|DEFAULT}]

tty-number: 仮想端末デバイス (TTY) 番号

解説

仮想端末デバイス (TTY) の情報を表示する。

非同期ポートには、それぞれ専用の TTY が存在する。また、Telnet セッションや端末サービスの開始時には、それぞれ TTY が動的に作成される。

パラメーター

TTY 端末デバイス番号。省略時はコマンドを入力した端末デバイスの情報が表示される。ALL を指定した場合は、すべての端末デバイスの情報が表示される。USER (一般ユーザー) 権限のポートから実行するときは、端末番号は指定できない (実行ポートの端末デバイスに関する情報が表示される)。

SUMMARY 端末デバイスごとに 1 行のみのサマリー情報を表示する。

DEFAULT Telnet 接続時に動的生成される端末デバイスのデフォルト設定パラメーターを表示する。本オプション指定時は、TTY パラメーターに端末番号や ALL を指定することはできない。

入力・出力・画面例

```
SecOff > show tty

TTY information
Instance ..... 16
Login Name ..... secoff
Description ..... Asyn 0
Secure ..... yes
Connections to .....
Current connection ..... none
In flow state ..... on
Out flow state ..... on
Attached module ..... Terminal server
Attached module instance .. 0
Type ..... VT100
Service ..... none
Prompt ..... default
Echo ..... yes
Attention ..... break
Manager ..... yes
```

```

Edit mode ..... insert
History length ..... 20
Page size ..... 22

```

| | |
|--------------------------|--|
| Instance | 仮想端末デバイス (TTY) 番号 |
| Login name | この端末にログインしているユーザーの名前 |
| Description | 端末名。非同期ポートの場合は SET ASYN コマンドの NAME パラメーター |
| Secure | セキュアモードの有効・無効。セキュアモードが有効の場合、該当端末デバイスからコマンドプロセッサにアクセスするには、最初にログインが必要。非同期ポートはデフォルトでセキュアモードが有効になっている。また、Telnet セッションは常にセキュアモードが有効 |
| Connections to | 接続中の端末デバイス一覧 |
| Current connection | 接続中の端末デバイスのうち、現在アクティブなものの番号 |
| In flow state | 受信時フロー制御の有効・無効 |
| Out flow state | 送信時フロー制御の有効・無効 |
| Attached module | アタッチされているユーザーモジュール。デフォルトは Terminal Server (ターミナルサーバーモジュール) |
| Attached module instance | アタッチされているモジュールのインスタンス番号 |
| Type | 端末タイプ。dump (ダム端末) または VT100 |
| Service | 本端末デバイスが所属している端末サービス名 |
| Prompt | プロンプト。default、off、login、password、confirm、encapsulation、あるいはユーザー定義の文字列 |
| Echo | 入力文字のエコー |
| Attention | 端末セッションから抜けるためのアテンションキャラクター。none、break、char のいずれか |
| Manager | MANAGER (管理者) 権限の有無 |
| Edit mode | 入力モード。? (不明) insert (挿入モード) overstrike (上書きモード) |
| History length | コマンド履歴の最大保持数 |
| Page size | 1 ページ当たりの行数。ページャー機能がオフのときは off |

表 92:

| | |
|-------------|--|
| TTY | 仮想端末デバイス (TTY) 番号 |
| Description | 端末名。非同期ポートの場合は SET ASYN コマンドの NAME パラメーター (デフォルトは「Port #」)。ルーターへの Telnet セッションの場合は「Telnet #」。別ポートへの接続の場合はサービス名。外部ホストへの Telnet の場合は IP アドレス |
| User name | ログインユーザーの名前 |
| Module | アタッチされているユーザーモジュール |

| | |
|-------------|-----------------------|
| Inst | ユーザーモジュールのインスタンス番号 |
| Mgr | MANAGER (管理者) 権限の有無 |
| Connections | 接続中の端末デバイス一覧 |

表 93: SUMMARY オプション

| | |
|----------------|---|
| History length | コマンド履歴の最大保持数 |
| Page length | 1 ページ当たりの行数。ページャー機能がオフのときは off |
| Prompt | プロンプト。default、off、login、password、confirm、encapsulation、あるいはユーザー定義の文字列 |
| Type | 端末タイプ。dump (ダム端末) または VT100 |

表 94: DEFAULT オプション

関連コマンド

SET ASYN (「インターフェース」の 50 ページ)

SET TTY (358 ページ)

SHOW ASYN (「インターフェース」の 65 ページ)

SHOW USER

カテゴリー：運用・管理 / ユーザー認証データベース

SHOW USER [=login-name] [CONFIGURATION]

login-name: ログイン名 (1~64 文字。英数字のみ使用可能。大文字小文字を区別しない。空白不可)

解説

ユーザー認証データベースの情報、または、ユーザー認証モジュールの設定情報を表示する。

パラメーター

USER ユーザー名

CONFIGURATION ユーザー認証モジュールの設定および統計情報を表示する。USER パラメーターと同時に指定することはできない。

入力・出力・画面例

```
SecOff > show user

Number of logged in Security Officers currently active.....1

User Authentication Database
-----
Username: manager (Manager Account)
  Status: enabled   Privilege: manager   Telnet: yes   Login: yes
  Logins: 2         Fails: 0           Sent: 0       Rcvd: 0
  Authentications: 0 Fails: 0
Username: secoff ()
  Status: enabled   Privilege: Sec Off   Telnet: no    Login: yes
  Logins: 1         Fails: 0           Sent: 0       Rcvd: 0
  Authentications: 0 Fails: 0
-----

Active (logged in) Users
-----

User          Port/Device
  Login Time          Location
-----
secoff        Asyn 0
    08:47:50 20-Apr-2010    local
manager       Telnet 2
```

| | |
|--|---------------------------|
| 08:59:17 20-Apr-2010 | 192.168.1.200 |
| ----- | |
| SecOff > show user configuration | |
| User module configuration and counters | |
| ----- | |
| Security parameters | |
| login failures before lockout | 5 (LOGINFAIL) |
| lockout period | 600 seconds (LOCKOUTPD) |
| manager password failures before logoff .. | 3 (MANPWDFAIL) |
| maximum security command interval | 600 seconds (SECUREDELAY) |
| minimum password length | 6 characters (MINPWDLEN) |
| TACACS retries | 3 (TACRETRIES) |
| TACACS timeout period | 5 seconds (TACTIMEOUT) |
| semi-permanent manager port | none |
| Security counters | |
| logins | 4 authentications 0 |
| managerPwdChanges | 0 defaultAcctRecoveries 1 |
| unknownLoginNames | 0 tacacsLoginReqs 0 |
| totalPwdFails | 1 tacacsLoginRejs 0 |
| managerPwdFails | 0 tacacsReqTimeouts 0 |
| securityCmdLogoffs | 0 tacacsReqFails 0 |
| loginLockouts | 0 databaseClearTotallys 0 |
| ----- | |

| User Authentication Database セクション | 登録ユーザーの情報が表示される |
|--|--|
| Number of logged in Security Officers currently active | 現在ログイン中の Security Officer レベルのユーザー。セキュリティタイマー (SECUREDELAY) 満了により権限を失っているユーザーは数えない |
| Username | ログイン名 |
| Status | アカウントの有効・無効 |
| Privilege | ユーザーレベル (権限)。Sec Off (Security Officer) \ manager (管理者) \ user (一般ユーザー) のいずれか |
| Telnet | 他ホストへの TELNET が許可されているかどうか |
| Logins | ログイン成功回数 |
| Fails | ログイン失敗回数 |
| Sent | ユーザーからスイッチへの送信オクテット数 |

| | |
|--------------------------------|--|
| Rcvd | スイッチからユーザーへの送信オクテット数 |
| Active (logged in) Users セクション | 現在ログイン中のユーザー一覧が表示される |
| User | ログイン名 |
| Port/Device | ログインポートまたはデバイス。「Asyn x」、「Telnet x」、「SSH x」のいずれかの形式。x はインスタンス番号 |
| Location | ユーザーがどこからログインしているか。コンソールポートからログインしているときは「local」、リモートログイン時はログイン元の IP アドレスが表示される |
| Login Time | ログイン日時 |

表 95:

| | |
|---|--|
| login failures before lockout | 連続したログインの失敗回数 (LOGINFAIL パラメーター)。この回数連続してログインに失敗すると、LOCKOUTPD 秒間はログインできなくなる (ロックアウト) |
| lockout period | LOGINFAIL 回連続してログインに失敗した場合にログイン不可能となる秒数 (LOCKOUTPD パラメーター) |
| manager password failures before logoff | セキュリティコマンド入力時のパスワード入力での失敗が許される回数 (MANPWDFAIL パラメーター) |
| maximum security command interval | セキュリティコマンドのタイムアウト (SECUREDELAY パラメーター) |
| minimum password length | パスワードの最小文字数 (MINPWDLEN パラメーター) |
| semi-permanent manager port | マネージャーポートの番号 |
| logins | ルーターへのログイン回数 |
| managerPwdChanges | Manager レベルのパスワード変更回数 |
| unknownLoginNames | 存在しないユーザー名でのログイン試行回数 |
| totalPwdFails | (存在するログイン名に対して) 正しくないパスワードが入力された回数 |
| managerPwdFails | セキュリティコマンド実行時に正しくないパスワードが入力された回数 |
| securityCmdLogoffs | セキュリティコマンド実行時に正しくないパスワードが入力されたため、Manager レベルのユーザーが強制的にログアウトさせられた回数 |

| | |
|-----------------------|---------------------------------|
| loginLockouts | 連続したログイン失敗によりログインロックアウトが施行された回数 |
| databaseClearTotallys | ユーザーデータベースがクリアされた回数 |

表 96: CONFIGURATION オプション指定時

関連コマンド

ADD USER (151 ページ)

DELETE USER (206 ページ)

DISABLE SYSTEM SECURITY_MODE (230 ページ)

DISABLE USER (233 ページ)

ENABLE SYSTEM SECURITY_MODE (263 ページ)

ENABLE USER (266 ページ)

PURGE USER (284 ページ)

RESET USER (292 ページ)

SET USER (359 ページ)

SHOW USER RSO

カテゴリー：運用・管理 / セキュリティー

SHOW USER RSO

解説

RSO (Remote Security Officer) の設定情報を表示する。
RSO とは、システムがセキュリティーモードで動作しているときに、Security Officer レベルでの Telnet ログインを許可されているホストのこと。セキュリティーモード時には、RSO として登録されたホスト以外からは Security Officer レベルでのログインができないようになっている。

入力・出力・画面例

```
SecOff > show user rso

Remote Security Officer Access is enabled

Remote Security Officer Log
-----
Remote Security Officer ... 172.16.28.126/255.255.255.255
Failed logins ..... 0
Last failed login ..... **_***_*** **.*.*
Successful logins ..... 2
Last successful login ..... 10-Jul-2001 19:32:55
-----

Illegal Login Attempts
IP Address          Date/Time           Attempts
-----
172.16.28.103       10-Jul-2001 19:34:58      2
172.16.28.1         10-Jul-2001 19:33:47      1
-----
```

| | |
|-----------------------------------|---|
| Remote Security Officer Access is | RSO ログインの有効・無効 (ENABLE USER RSO コマンドで設定) |
| Remote Security Officer | RSO の IP アドレス (IP アドレス/ネットマスク) |
| Failed logins | RSO のログイン失敗回数 |
| Last failed login | 最新のログイン失敗日時。「**_***_*** **.*.*」はログイン失敗の記録がないことを示す |
| Successful logins | RSO のログイン成功回数 |
| Last successful login | 最新のログイン成功日時。「**_***_*** **.*.*」はログイン成功の記録がないことを示す |

| | |
|------------------------|---|
| Illegal login attempts | RSO アドレス以外からの Security Officer ログイン試行記録 |
| IP address | Telnet クライアントの IP アドレス |
| Date/time | ログイン試行日時 |
| Attempts | 試行回数 |

表 97:

関連コマンド

ADD USER RSO (153 ページ)

DELETE USER RSO (207 ページ)

DISABLE SYSTEM SECURITY_MODE (230 ページ)

DISABLE USER RSO (234 ページ)

ENABLE SYSTEM SECURITY_MODE (263 ページ)

ENABLE USER RSO (267 ページ)

SSH

カテゴリー：運用・管理 / Secure Shell

SSH *ipadd* USER=*username* {PASSWORD=*password*|KEYID=*key-id*}
 [COMMAND=*string*]

ipadd: IP アドレス

username: ユーザー名 (1~15 文字。英数字)

password: パスワード (1~31 文字)

key-id: 鍵番号 (0~65535)

string: 文字列 (1~80 文字)

解説

SSH サーバーにログインする。または SSH サーバー上でコマンドを実行させる。

- ・SSH セッションを終了させるには、接続先ホストからログアウトする。
- ・SSH セッションから一時的に抜けてプロンプトに戻るには、非同期ポートからログインしている場合は「Break」を送信、Telnet で別ホストからログインしている場合は「Ctrl-P」を入力する。セッションからプロンプトに戻るための文字 (アテンションキャラクター) は、SET ASYN コマンドの ATTENTION パラメーターで変更できる。
- ・一時中断したセッションに戻るには、「Ctrl-X」を何回か押して該当するセッションを表示させ、「Enter」を押す。または、SHOW SESSIONS コマンドでセッションの一覧を確認し、RECONNECT コマンドで再接続する。

パラメーター

USER ログインユーザー名

PASSWORD パスワード認証で使うログインパスワード

KEYID RSA 鍵番号。RSA 認証で使う自分の秘密鍵番号。RSA 認証では、クライアント側にユーザーの秘密鍵、サーバー側にユーザーの公開鍵が必要

COMMAND SSH サーバー上で実行させるコマンドライン。本パラメーターを指定したときは、コマンド実行後にコネクションが切断される。本パラメーターを指定しなかったときは、SSH サーバーにログインして対話型セッションを開始する。

例

SSH サーバー 192.168.10.1 にユーザー名 root、パスワード 8nyara でログインする。

```
SSH 192.168.10.1 USER=root PASSWORD=8nyara
```

SSH サーバー 192.168.10.1 にユーザー名 root、RSA 鍵 10 番を使ってログインする。

```
SSH 192.168.10.1 USER=root KEYID=10
```

SSH サーバー 192.168.10.1 上で「SHOW IP INTERFACE」を実行し、結果を端末画面に出力させる。

```
SSH 192.168.10.1 USER=root PASSWORD=8nyara COMMAND="show ssh int"
```

備考・注意事項

サーバーに初めて接続したときは「Host key not recognised - saved as ssh.key」というメッセージが表示されてセッションが切られるが、これは該当サーバーのホスト鍵を初めて受け取ったことを示すものでエラーではない。その場合、サーバーのホスト鍵が「ssh.key」という名前で自動的に保存されているはずなので、CREATE ENCO KEY コマンドを実行してサーバーのホスト鍵を登録する。このとき鍵の TYPE は RSA、FORMAT は SSH を指定する。

関連コマンド

CREATE ENCO KEY (「暗号・圧縮」の 18 ページ)

SHOW SSH SESSIONS (461 ページ)

TELNET

カテゴリー：運用・管理 / ターミナルサービス

TELNET {*ipadd*|*hostname*}

ipadd: IP アドレス (IPv4 または IPv6)

hostname: ホスト名

解説

指定したホストに Telnet 接続する。

- ・セッションを終了させるには、接続先ホストからログアウトする。また、非同期ポートからログインしている場合は「Ctrl-D」を押しても接続を切ることができる。
- ・セッションから一時的に抜けてプロンプトに戻るには、非同期ポートからログインしている場合は「Break」を送信、Telnet で別ホストからログインしている場合は「Ctrl-P」を入力する。セッションからプロンプトに戻るための文字 (アテンションキャラクター) は、SET ASYN コマンドの ATTENTION パラメーターで変更できる。
- ・一時中断したセッションに戻るには、「Ctrl-X」を何回か押して該当するセッションを表示させ、「Enter」を押す。または、SHOW SESSIONS コマンドでセッションの一覧を確認し、RECONNECT コマンドで再接続する。

入力・出力・画面例

```
Manager ar.joge.net> telnet afrika

Info (105327): Resolving host name "afrika.joge.net" to IP address.

Info (105328): Host name resolved to 172.16.28.1.

Info (133256): Attempting Telnet connection to afrika.joge.net, Please wait ....

Telnet セッションが確立
U*IX (afrika.joge.net) (ttyp2)

login: usouser
Password:

[chkmail] You have new mail.

inbox          : 6
urgent         : 3
-----
Total          : 9
```

To Do

- Complete reference manual.
- Eat ramen.

afrika:~> ここで Break を送信するか Ctrl-P を押し、一時的にセッションから抜ける

Session 1 to afrika.joge.net paused

プロンプトに戻った

Manager ar.joge.net> show ip int

| Interface | Type | IP Address | Bc | Fr | PArp | Filt | RIP | Met. | SAMode | IPSc |
|-----------|----------|---------------|------|-----|------|------|------------|--------|--------|------|
| Pri. Filt | Pol.Filt | Network Mask | MTU | VJC | GRE | OSPF | Met. | DBcast | Mul. | |
| ----- | | | | | | | | | | |
| Local | --- | Not set | - | - | - | --- | -- | | Pass | -- |
| --- | --- | Not set | 1500 | - | | --- | -- | | --- | --- |
| eth0 | Static | 10.10.10.100 | 1 | n | On | --- | 01 | | Pass | No |
| --- | --- | 255.255.255.0 | 1500 | - | | --- | 0000000001 | No | | Rec |
| eth1 | Static | 172.16.28.160 | 1 | n | On | --- | 01 | | Pass | No |
| --- | --- | 255.255.255.0 | 1500 | - | | --- | 0000000001 | No | | Rec |
| ----- | | | | | | | | | | |

端末セッション一覧を確認

Manager ar.joge.net> show session

Session information for Telnet 1

```
session 1 connected to afrika.joge.net
session 2 not connected
session 3 not connected
session 4 not connected
session 5 not connected
```

Ctrl-X を押して希望するセッションを表示させ、Enter を押す

Manager ar.joge.net> reconnect 1 (afrika.joge.net) [Enter]

Info (136271): Reconnected to session 1 (afrika.joge.net).

Telnet セッションに戻った。何も表示されないときは、Enter を押す

afrika:~> logout

ログアウトしてセッションを終了

TELNET session now CLOSED.

```
Manager ar.joge.net>
```

備考・注意事項

ホスト名を指定する場合は、あらかじめ ADD IP DNS コマンドでネームサーバーのアドレスを設定しておく必要がある。ホスト名は通常フルドメイン名 (FQDN) で指定しなくてはならないが、SET SYSTEM NAME コマンドでホスト名を含む完全なドメイン名 (FQDN) を設定しておけば、接続先として短いホスト名 (例: afrika) を指定することもできる。

この場合、「sysName に設定したフルドメイン名から先頭要素 (最初のドットまで) を取り除いたもの」が検索対象ホスト名の後に付加される。たとえば、sysName に「myrouter.mydomain.xx.jp」(myrouter がルーター自身の短いホスト名) を設定している場合、「TELNET hispc」というコマンドを実行すると、「hispc.mydomain.xx.jp」に対して DNS の検索が行われる。

関連コマンド

ADD IP DNS (「IP」の 173 ページ)
ADD IP HOST (「IP」の 184 ページ)
DELETE IP HOST (「IP」の 238 ページ)
DISCONNECT (235 ページ)
RECONNECT (285 ページ)
SET IP HOST (「IP」の 375 ページ)
SET SYSTEM NAME (338 ページ)
SET TELNET (340 ページ)
SHOW IP HOST (「IP」の 475 ページ)
SHOW SESSIONS (436 ページ)

UPLOAD

カテゴリー：運用・管理 / アップロード・ダウンロード

UPLOAD [METHOD={TFTP|ZMODEM}] [FILE=*filename*] [SERVER={*hostname*|*ipadd*}]
[ASYN=*asyn-number*]

filename: ファイル名

hostname: ホスト名

ipadd: IP アドレス

asyn-number: 非同期ポート番号 (0)

解説

TFTP、ZMODEM でファイルをアップロードする。

指定しなかったパラメーターについては、SET LOADER コマンドで設定したデフォルト値が用いられる。

パラメーター

METHOD 転送プロトコル。TFTP の場合は SERVER の指定が必要。また、ZMODEM の場合は ASYN の指定が必要。デフォルトは TFTP。

FILE アップロードするファイル名

SERVER TFTP サーバーのホスト名または IP アドレス。ホスト名を指定する場合は、ADD IP DNS コマンドで DNS サーバーアドレスを設定しておく必要がある。

ASYN ZMODEM で使用する非同期ポートの番号

例

フラッシュファイルシステム上のファイル「foobar.scp」を TFTP サーバー「192.168.1.103」にアップロードする

```
UPLOAD FILE=foobar.scp SERVER=192.168.1.103
```

フラッシュファイルシステム上のファイル「basic.cfg」を非同期ポート asyn0 経由で端末に ZMODEM 転送する。

```
UPLOAD FILE=basic.cfg METHOD=ZMODEM ASYN=0
```

関連コマンド

LOAD (271 ページ)

SET LOADER (298 ページ)

UPLOAD

SHOW FILE (374 ページ)

SHOW LOADER (386 ページ)

WAIT

カテゴリー：運用・管理 / スクリプト

WAIT *seconds*

seconds: 時間（秒）

解説

指定された秒数ウェイトを実行する。本コマンドはスクリプト中でのみ有効。

備考・注意事項

スクリプト中でのみ使用可能。

関連コマンド

IF THEN ELSE ENDIF（270 ページ）