

運用・管理

システム	8
ログイン	8
再起動	9
システム時計の設定	9
システム名の設定	10
システムチェック	10
コマンドラインプロセッサ	11
ログイン	11
コマンドプロンプト	12
コマンドライン編集キー	12
コマンド入力時の注意事項	14
コンソールメッセージ	14
次に選択可能なキーワードを表示する「?」	15
オンラインヘルプ	16
端末画面のページあたり行数	16
記憶装置とファイルシステム	18
物理デバイス	18
NVS	18
フラッシュメモリー	18
ファイルシステム	18
ファイル名	18
ファイルの操作	19
コンフィグレーション	21
設定の保存と復元	21
ユーザー認証データベース	23
ユーザーレベル	23
コマンドプロンプト	23
デフォルトアカウント	23
ユーザー認証処理の順序	24
ユーザーアカウントの管理	24
認証サーバー	28
ユーザー認証処理の順序	28
RADIUS サーバー	28
RADIUS サーバーのアカウントिंग機能	29

RADIUSクライアント	30
アップロード・ダウンロード	31
ダウンロード	31
ネットワーク経由でのダウンロード	31
コンソールポート経由でのダウンロード	32
アップロード	32
ネットワーク経由でのアップロード	32
コンソールポート経由でのアップロード	33
システム内のファームウェアファイルの転送	33
マスターからスレーブスイッチへのファイルの転送	34
ログ	36
デフォルトのログ設定	36
ログの閲覧	36
ログの保存	37
syslog サーバーへのログ転送	37
メッセージフィルターの追加	38
ログ設定の確認	38
資料編	39
メッセージの表示項目	39
ログレベル	40
モジュール ID とモジュール名	40
syslog 形式への変換	42
SNMP	45
SNMPv1/SNMPv2c	45
基本設定	45
その他	47
SNMPv3	48
基本設定	49
その他	51
SNMPv1/v2c/v3 の共通事項	51
SNTP	53
基本設定	53
マネージメントアクセスコントロール	55
マネージメントアクセスコントロールリスト (Management ACL)	55
基本設定	56
攻撃検出	59
SYN Flood Attack	59
Smurf Attack	60
Land Attack	60
Teardrop Attack	61
Ping of Death Attack	61
IP Options Attack	62

鍵作成・管理	63
暗号アルゴリズム	63
RSA	63
Secure Shell	65
SSH サーバー	65
パスワード認証	65
PKI	68
PKI とは	68
基本設定	68
エンハンススタッキング	70
基本設定	71
マスタースイッチからスレーブスイッチへのファームウェアファイルと設定ファイルの転送	71
コマンドリファレンス編	73
機能別コマンド索引	73
ACCESS SWITCH	78
ADD LOG OUTPUT	79
ADD MGMTACL	80
ADD PKI CERTIFICATE	81
ADD RADIUSSERVER	82
ADD SNMP COMMUNITY	84
ADD SNMPV3 USER	85
ADD SNTP PEER	86
ADD USER	87
CLEAR SCREEN	89
COPY	90
CREATE CONFIG	91
CREATE ENCO KEY	92
CREATE LOG OUTPUT	94
CREATE MGMTACL	96
CREATE PKI CERTIFICATE	98
CREATE PKI ENROLLMENTREQUEST	99
CREATE SNMP COMMUNITY	100
CREATE SNMPV3 ACCESS	102
CREATE SNMPV3 COMMUNITY	104
CREATE SNMPV3 GROUP	106
CREATE SNMPV3 NOTIFY	107
CREATE SNMPV3 TARGETADDR	108
CREATE SNMPV3 TARGETPARAMS	110
CREATE SNMPV3 VIEW	112
DELETE EXCEPTIONLOG	114
DELETE FILE	115
DELETE MGMTACL	116

DELETE PKI CERTIFICATE	117
DELETE RADIUSERVER	118
DELETE SNMP COMMUNITY	119
DELETE SNMPV3 USER	120
DELETE SNTP PEER	121
DELETE USER	122
DESTROY ENCO KEY	123
DESTROY LOG OUTPUT	124
DESTROY MGMTACL	125
DESTROY SNMP COMMUNITY	126
DESTROY SNMPV3 ACCESS	127
DESTROY SNMPV3 COMMUNITY	128
DESTROY SNMPV3 GROUP	129
DESTROY SNMPV3 NOTIFY	130
DESTROY SNMPV3 TARGETADDR	131
DESTROY SNMPV3 TARGETPARAMS	132
DESTROY SNMPV3 VIEW	133
DISABLE AUTHENTICATION	134
DISABLE INTERFACE LINKTRAP	135
DISABLE LOG	136
DISABLE LOG OUTPUT	137
DISABLE MGMTACL	138
DISABLE RADIUSACCOUNTING	139
DISABLE SNMP	140
DISABLE SNMP COMMUNITY	141
DISABLE SNMP TRAP	142
DISABLE SNTP	144
DISABLE SSH SERVER	145
DISABLE TELNET	146
DISABLE USER	147
ENABLE AUTHENTICATION	148
ENABLE INTERFACE LINKTRAP	149
ENABLE LOG	150
ENABLE LOG OUTPUT	151
ENABLE MGMTACL	152
ENABLE RADIUSACCOUNTING	153
ENABLE SNMP	154
ENABLE SNMP COMMUNITY	155
ENABLE SNMP TRAP	156
ENABLE SNTP	158
ENABLE SSH SERVER	159
ENABLE TELNET	161

ENABLE USER	162
EXIT	163
FORMAT DEVICE	164
HELP	165
LOAD	166
LOGOFF	168
LOGOUT	169
PURGE AUTHENTICATION	170
PURGE LOG	171
PURGE MGMTACL	172
PURGE SNMPV3 ACCESS	173
PURGE SNMPV3 NOTIFY	174
PURGE SNMPV3 TARGETADDR	175
PURGE SNMPV3 VIEW	176
PURGE SNTP	177
PURGE USER	178
QUIT	179
RENAME	180
RESET USER	181
RESET USERCONFIG	182
RESTART	183
SAVE CONFIGURATION	184
SAVE LOG	185
SET ASYN	186
SET AUTHENTICATION	187
SET CONFIG	188
SET DOS	189
SET DOS IPOPTION	190
SET DOS LAND	191
SET DOS PINGOFDEATH	192
SET DOS SMURF	193
SET DOS SYNFLOOD	194
SET DOS TEARDROP	195
SET ENCO KEY	196
SET LOG FULLACTION	197
SET LOG OUTPUT	198
SET MGMTACL	199
SET PASSWORD	200
SET PKI CERTIFICATE	201
SET RADIUSACCOUNTING	202
SET RADIUSSERVER	203
SET SNMP COMMUNITY	204

SET SNMPV3 ACCESS	205
SET SNMPV3 COMMUNITY	206
SET SNMPV3 GROUP	208
SET SNMPV3 NOTIFY	209
SET SNMPV3 TARGETADDR	210
SET SNMPV3 TARGETPARAMS	212
SET SNMPV3 USER	214
SET SNMPV3 VIEW	215
SET SNTP	216
SET SSH SERVER	218
SET SWITCH CONSOLETIMER	219
SET SWITCH STACKMODE	220
SET SYSTEM CONTACT	221
SET SYSTEM DISTINGUISHEDNAME	222
SET SYSTEM LOCATION	223
SET SYSTEM NAME	224
SET TELNET	225
SET TIME	226
SET USER	227
SET USERCONFIG	229
SHOW ASYN	230
SHOW AUTHENTICATION	231
SHOW BUFFER	233
SHOW CONFIG	235
SHOW CPU	237
SHOW DEBUG	240
SHOW DOS	241
SHOW DOS IPOPTION	243
SHOW DOS LAND	245
SHOW DOS PINGOFDEATH	247
SHOW DOS SMURF	249
SHOW DOS SYNFLOOD	251
SHOW DOS TEARDROP	253
SHOW ENCO KEY	255
SHOW EXCEPTIONLOG	256
SHOW FILE	257
SHOW FLASH	259
SHOW INTERFACE	260
SHOW LOG	264
SHOW LOG OUTPUT	267
SHOW LOG STATUS	269
SHOW MGMTACL	270

SHOW PKI CERTIFICATE	272
SHOW RADIUSACCOUNTING	275
SHOW REMOTELIST	276
SHOW SNMP	277
SHOW SNMP COMMUNITY	278
SHOW SNMP TRAP	280
SHOW SNMPV3 ACCESS	282
SHOW SNMPV3 COMMUNITY	284
SHOW SNMPV3 ENGINEID	286
SHOW SNMPV3 GROUP	287
SHOW SNMPV3 NOTIFY	289
SHOW SNMPV3 TARGETADDR	290
SHOW SNMPV3 TARGETPARAMS	292
SHOW SNMPV3 USER	294
SHOW SNMPV3 VIEW	296
SHOW SNTP	298
SHOW SSH	299
SHOW SYSTEM	301
SHOW TIME	304
SHOW USER	305
SHOW USERCONFIG	307
UPLOAD	309

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。

- ネットワーク上のコンピューターから Telnet を使用して本製品にログインするには、あらかじめコンソールターミナルからログインして、VLAN インターフェースに管理用の IP アドレスを割り当て（IP インターフェースを作成し）、該当インターフェースをローカル IP インターフェース（マネージメント VLAN インターフェース）と呼ばれる遠隔管理用のインターフェースとして指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」と User（一般ユーザー）レベルのユーザー「operator」が登録されています。

「manager」の初期パスワードは「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*で表示されます)

#
```

「operator」の初期パスワードは「operator」です。「Login:」に対してユーザー名「operator」を、「Password:」に対してパスワード「operator」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: operator
Password: operator (実際には*で表示されます)

$
```

- 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「ユーザー管理」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 10 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

USERCONFIG コマンド (229 ページ) の LOGINFAIL、LOCKOUTPD パラメーターで変更できます。

- 同時にログイン可能なユーザーは Manager (管理者) レベルのユーザー 1 と User (一般ユーザー) レベルのユーザー 9 のあわせて 10 ユーザーです。ただし、ネットワーク経由でログインする場合は、Manager レベルのユーザー 1 と User レベルのユーザー 8 のあわせて 9 ユーザーまでです。Manager レベルのユーザーは複数ログインできません。

再起動

システムを再起動するには RESTART コマンド (183 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。

RESTART コマンド (183 ページ) を実行すると、コールドスタート (ハードウェアリセット) が実行されます。

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。

RESTART コマンド (183 ページ) の CONFIG パラメーターを指定して、読み込みなおす設定ファイルを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 1 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 (188 ページ) で設定した起動スクリプトが読み込まれます。

```
RESTART SWITCH 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 (226 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。

日付と時刻を設定するには次のようにします。ここでは 2009 年 5 月 17 日 19 時に設定します。

```
SET DATE=17-05-2009 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=17-05-2009 ↓
```

現在の日付と時刻を確認するには SHOW TIME コマンド (304 ページ) を実行します。

月は英語月名の先頭 3 文字で表示されます。

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:

SNTP (Simple 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「SNTP」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 (224 ページ) を使います。

```
SET SYSTEM NAME=c9424t <J
```

設定したシステム名は、製品タイトルの下にも表示されます。

```

Allied Telesis AT-9424T - ATS63 v2.11.1J
c9424t
c9424t#

```

SNMP マネージャーからシステム名を変更した場合、SHOW CONFIG コマンド (235 ページ) の DYNAMIC オプションではすぐに確認できますが、プロンプトに反映されるのは、ログアウト、再ログイン後です。なお、SNMP の設定については「運用・管理」の「SNMP」をご覧ください。

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 (301 ページ) で確認できます。

システムログは SHOW LOG コマンド (264 ページ) で確認できます。詳細については「運用・管理」/「ログ」をご覧ください。

例外状況の発生ログは SHOW EXCEPTIONLOG コマンド (256 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 (240 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 (233 ページ) で確認します。

CPU の使用率は SHOW CPU コマンド (237 ページ) で確認します。

コマンドラインプロセッサ

本製品は設定のためのコマンドプロセッサ (コマンドラインインターフェース) を備えています。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、ローカル IP インターフェー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」と User (一般ユーザー) レベルのユーザー「operator」が登録されています。

「manager」の初期パスワードは「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*で表示されます)

#
  
```

「operator」の初期パスワードは「operator」です。「Login:」に対してユーザー名「operator」を、「Password:」に対してパスワード「operator」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: operator
Password: operator (実際には*で表示されます)

$
  
```

- ☞ 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「ユーザー管理」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 10 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 USERCONFIG コマンド（229 ページ）の LOGINFAIL、LOCKOUTPD パラメーターで変更できます。
- 同時にログイン可能なユーザーは Manager（管理者）レベルのユーザー 1 と User（一般ユーザー）レベルのユーザー 9 のあわせて 10 ユーザーです。ただし、ネットワーク経由でログインする場合は、Manager レベルのユーザー 1 と User レベルのユーザー 8 のあわせて 9 ユーザーまでです。Manager レベルのユーザーは複数ログインできません。

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。

- User レベル

```
$
```

- Manager レベル

```
#
```

- SET ASYN コマンド（186 ページ）の PROMPT パラメーターでプロンプトに文字列を設定している場合は、それぞれのプロンプトの前に設定した文字列が表示されます。

```
# set asyn prompt=kumanomi
kumanomi#
```

なお、プロンプト文字列を設定していない場合に、SET SYSTEM NAME コマンド（224 ページ）でシステム名（sysName）を設定しているときは、プロンプト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。

```
# set system name="c9424/8F"
c9424/8F#
```

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）。

機能	キー
1文字右に移動	または Ctrl/F
1文字左に移動	または Ctrl/B
カーソルの左にある文字を削除	Backspace
カーソル位置の文字を削除（カーソルが行末にあるときは、カーソルの左にある文字を削除する）	Delete または Ctrl/D

カーソル位置から行末までを削除	Ctrl/K
コマンド行の消去	Esc2 回 押下 または Ctrl/U
コマンド履歴をさかのぼる	または Ctrl/P
コマンド履歴を進める	または Ctrl/N
コマンドの中止	Ctrl/C
行頭へ移動	Ctrl/A または Home
行末へ移動	Ctrl/E または End

表 2:

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 1499 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 (224 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。

コマンドは一意に識別できる範囲で省略可能です。たとえば、SHOW SYSTEM コマンド (301 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 SY ↓
```

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。

コマンドの実行結果は (エラーがなければ) すぐに本製品に反映されますので、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 (91 ページ) でファイルに保存し、SET CONFIG コマンド (188 ページ) で、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に設定してください。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。

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。以下に、「ERROR CODE」(エラーメッセージ) の例を示します。

- コマンドが不完全な場合

```
# set
ERROR CODE = CLI_COMMAND_INCOMPLETE
```

- 該当するコマンドがない場合

```
# set systemname=sales
ERROR CODE = CLI_COMMAND_NOT_FOUND_OR_AMBIGUOUS
```

- 必要なパラメーターが指定されていない場合

```
# set system
ERROR CODE = CLI_PARAMETER_MISSING
```

- 必要な値が指定されていない場合

```
# set system name=
ERROR CODE = CLI_VALUE_EXPECTED
```

次に選択可能なキーワードを表示する「？」

コマンドの入力途中で「？」キーを押すと、次に選択可能なキーワード（コマンド名やパラメーター名、オプション名）の一覧が表示されます。

たとえば、コマンドラインの先頭で「？」キーを押すと次のように表示されます（「？」は表示されません）。

```
# ?
Available commands:
ACTivate - Activates an instance of an object type
ADD      - Adds an instance of an object type
CLear    - Clears all data relating to the object
COpy     - Copy file
CReate   - Makes a new instance of an object type
DELeTe   - Removes an instance of an object
DEStroy  - Destroys an object instance
DISable  - Suspends the object operation while retaining its configuration
ENable   - Allows an object to enter its operational state
EXit     - Quits the current management session
FORMAT   - Formats a file system drive
Help     - Displays available commands
LOAD     - Downloads a file
LOGOff   - Logs out of the current management session
LOGOUt   - Logs out of the current management session
PIng     - Pings an IP address
PURge    - Clears all the object's configurable data and disables it
Quit     - Quits the current management session
REName   - Rename file
RESEt    - Restores the object to its stored configuration
REStart  - Restart the switch
SAve     - Saves configuration
SEt      - Sets the configuration of an existing object
SHow     - Displays diagnostic information to the user
```

```
Upload - Uploads a file
```

「Available commands:」以下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）。

- ☞ 「？」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。詳細はリリースノートなどをご確認ください。

次に、コマンドラインで上記のキーワード一覧から「add」を入力し、さらに半角スペースを1文字入力した上で再度「？」キーを押すと、次のように表示されます。

- ☞ 何らかの文字列を入力した後で「？」キーを押すときは、文字列の後ろに半角スペースを入力してから「？」キーを押す必要があります。

```
# add ?
Available commands:
add Bootp      - Adds BOOTP Relay destination IP address of BOOTP server
add Dhcp       - Adds DHCP SERVER information
add Ip         - Adds IP Interface
add LOg        - Adds a filter to the log Output Definition
add MGmtacl    - Adds entries to Management ACL table
add MStp       - Adds attributes to MSTP
add PKi        - Adds a PKI certificate
add PORTAUth   - Adds Port access control configuration parameters
add Qos        - Adds attributes to QoS
add Radiusserver - Adds RADIUS authentication server
add SNMP       - Adds attributes to an existing SNMP community
add SNMPV3     - Adds a new entry to SNMPv3 table
add SNTp       - Adds SNTp server
add SWitch     - Adds attributes to the switch
add User       - Adds user to the user management database
add Vlan       - Adds attributes to an existing VLAN
add VRrp       - Adds an IP address or monitored interface to a virtual router
# add
```

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（165 ページ）を使います。

HELP コマンド（165 ページ）を実行すると、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が表示されます（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）。

端末画面のページあたり行数

1 ページあたり行数は 15（空白行を含まず）に設定されています。コマンドの出力結果が 15 行よりも長い場合は表示が一時停止し、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 3:

一度表示された行をさかのぼることはできません。

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。

フラッシュメモリー上には独自の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

NVS (Non-Volatile Storage : 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、ログや例外発生ログ、DHCP Snooping のクライアント情報が保存されます。

フラッシュメモリー

フラッシュメモリーは (NVS に比べて) 大容量の記憶装置で、ファームウェアファイル、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。

フラッシュメモリーは一般的なコンピューターのハードディスクに相当する記憶装置です。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。コマンド上での名称は「flash」です。多くのコマンドでは、デバイス名の指定を省略すると、フラッシュメモリーを指定したことになります。

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 (259 ページ) で確認できます。

SHOW FLASH ↓

ファイルシステム

本製品では、フラッシュメモリー上にファイルシステムが構築されており、物理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。

ファイル名

ファイル名は次の形式で表されます。

device:filename.ext

device デバイス名。flash (フラッシュメモリー)。大文字小文字の区別はありません。

filename	ファイル名（ベース名）。文字数は1~28文字。半角英数字と記号（`' @ # \$ % ^ & () _ - { }`）が使えます。大文字・小文字の区別はありません。
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。本製品で認識できる拡張子は、下記の表を参照してください。

表 4:

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
img	ファームウェアファイル
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。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。
key	RSA 公開鍵ファイル
log	ログを保存したファイル

表 5:

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。
enc1.ukf	CREATE ENCO KEY コマンドで作成された RSA 鍵ペアのファイル。このファイルはコピーやファイル名の変更、削除を行うことができません。DESTROY ENCO KEY コマンドを実行すると、自動的に削除されます。(enc 後の番号は、KeyID です。)

表 6:

📁 フラッシュメモリー上のファイルシステムには、ディレクトリー（フォルダー）の概念はありません。

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（257 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=*.cfg ↓
```

ファイルの内容を見るには、SHOW FILE コマンド (257 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 (257 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 (.cfg、.log 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 (115 ページ) を使います。

```
DELETE FILE=iranai.cfg ↵
```

✎ 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。

ファイルをコピーするには COPY コマンド (90 ページ) を使います。

```
COPY current.cfg backup.cfg ↵
```

ファイル名を変更するには RENAME コマンド (180 ページ) を使います。

```
RENAME old.cfg new.cfg ↵
```

LOAD コマンド (166 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 test.cfg をダウンロードしています。ダウンロードには、XMODEM、HTTP を使うこともできます。

```
LOAD METHOD=TFTP DESTFILE=test.cfg SERVER=192.168.1.11 FILE=test.cfg ↵
```

UPLOAD コマンド (309 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。XMODEM によるアップロードも可能です。

```
LOAD METHOD=TFTP DESTFILE=taisetsu.cfg SERVER=192.168.1.11  
FILE=taisetsu.cfg ↵
```

✎ 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。

新規にファイルを作成し、メモリー上の設定内容を保存するには、CREATE CONFIG コマンド (91 ページ) を使います。ファイルの拡張子は「.cfg」とします。たとえば、現在の設定内容を「mylan.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。(ファイルが存在する場合は、確認のメッセージが表示されます。Y キーを押して、Yes を選択するとファイルは上書きされます。N キーを押して、No を選択するとファイルの上書きは行われません。)

```
CREATE CONFIG=mylan.cfg ↓
```

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、MD5 でハッシュ値に変換されて保存されます。

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 (188 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=mylan.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 (235 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 (235 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 ↓
```

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 (188 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（コールドスタート）するには、RESTART コマンド（183 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。

```
RESTART SWITCH 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（183 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 SWITCH CONFIG=NONE ↓
```

現在の起動時設定ファイルに、メモリー上の設定内容を保存するには、SAVE CONFIGURATION コマンド（184 ページ）を使います。

```
SAVE CONFIGURATION ↓
```

- ☞ 本コマンドを実行すると、SHOW CONFIG コマンド（235 ページ）を実行して、「Boot configuration file」欄に表示されるファイルに、メモリー上の設定内容が保存されます。この欄に、「None」と表示されている場合は、SET CONFIG コマンド（188 ページ）で起動スクリプトを設定し、本コマンドで設定内容を保存します。

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2つのレベルに分けられます。

- User レベル
- Manager レベル

User (一般ユーザー) レベルのユーザーは、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 経由での接続受け入れ時認証のために用意されているものですが、本製品は WAN インターフェースを持たないため、ほとんど使用する機会はありません。

Manager (管理者) レベルのユーザーは、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、すべての管理・設定作業は Manager レベルのアカウントを使用して行います。

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。

- User レベル

```
$
```

- Manager レベル

```
#
```

- ☞ SET ASYN コマンド (186 ページ) の PROMPT パラメーターでプロンプトに文字列を設定している場合は、それぞれのプロンプトの前に設定した文字列が表示されます。

```
# set asyn prompt=kumanomi
kumanomi#
```

なお、プロンプト文字列を設定していない場合に、SET SYSTEM NAME コマンド (224 ページ) でシステム名 (sysName) を設定しているときは、プロンプト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。

```
# set system name="c9424/8F"
c9424/8F#
```

デフォルトアカウント

本製品には、Manager (管理者) レベルのユーザー「manager」と User (一般ユーザー) レベルのユーザー

「operator」が登録されています。

「manager」の初期パスワードは「friend」です。また、「operator」の初期パスワードは「operator」です。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 (200 ページ) を使います。「manager」のパスワードを変更するには、次のようにします。

```
# set password
Enter current manager password->***** (現在のパスワードを入力。*で表示される)
Enter new manager password->***** (新しいパスワードを入力。*で表示される)
Re-enter manager password ->***** (確認のため、新しいパスワードをもう一度入力)
```

📌 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 (91 ページ) で設定をファイルに保存し、SET CONFIG コマンド (188 ページ) で起動スクリプトに指定してください。詳細は「コンフィグレーション」をご覧ください。

```
# create config=basic.cfg
Creating configuration file "basic.cfg" ..... done!
# set config=basic.cfg
Setting boot configuration file name ..... done!
```

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、パスワードによるユーザー認証だけでなく、RADIUS (Remote Access Dial-In User Service) サーバーに対応しています。ログイン時の認証は次の順序で行われます。

1. RADIUS サーバー (ADD RADIUSSERVER コマンド (82 ページ) で登録したもの)
2. パスワードによるユーザー認証

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、「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、Manager 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/オプション	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 から選択
セッションタイプ	SESSIONTYPE	オプション (省略時は ALL)	ユーザーがログインできるセッションタイプ。CONSOLE、TELNET、SSH、ENAHNCEDSTACKING、ALL から選択
コメント	DESCRIPTION	オプション	ユーザーに関するコメント

表 7:

ユーザーを追加するには ADD USER コマンド (87 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=ATKK PASSWORD=i10vEba7 PRIVILEGE=MANAGER ↓
```

ユーザー「ATKK」を有効にします。

```
ENABLE USER=ATKK ↓
```

ユーザー「ATKK」を無効にします。

```
DISABLE USER=ATKK ↓
```

ユーザー「ATKK」を削除します。

```
DELETE USER=ATKK ↓
```

ユーザー「ATKK」のカウンター値をリセットします。

```
RESET USER=ATKK COUNTER ↓
```

ユーザーの一覧は SHOW USER コマンド (305 ページ) で確認できます。

```
SHOW USER ↓
```

現在ログインしているユーザーのパスワードを変更するには SET PASSWORD コマンド (200 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 (227 ページ) の PASSWORD パラメーターを使います。

```
SET USER=manager PASSWORD=panda ↓
```

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 USERCONFIG コマンド (229 ページ) の MINPWDLEN パラメーターで変更できます。

```
SET USERCONFIG MINPWDLEN=5 ↓
```

- ☞ デフォルトアカウントである manager、operator 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 (91 ページ) でファイルに保存し、SET CONFIG コマンド (188 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」/「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。

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 USERCONFIG コマンド (229 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 USERCONFIG コマンド (307 ページ) で表示できます。

SHOW USERCONFIG ↓

認証サーバー

本製品は、ユーザー認証機構として、ユーザー名とパスワードによる認証に加えて、RADIUS (Remote Authentication Dial In User Service) サーバーをサポートしています。

- ④ ADD RADIUSSERVER コマンド (82 ページ) で認証サーバーリストに追加された RADIUS サーバーと本製品が接続された状態で、ENABLE AUTHENTICATION コマンド (148 ページ) により認証が有効の場合は、RADIUS サーバーに登録したログイン名/パスワードでしか本製品にログインすることができません。本製品に設定されているユーザー名/パスワードでログインする場合は、ENABLE AUTHENTICATION コマンド (148 ページ) を実行しないでください。

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、RADIUS サーバーに認証を要求します。RADIUS サーバーに登録されていない、あるいは RADIUS サーバーから Access-Reject が返ってきた場合は、認証は失敗、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 サーバーとの通信がタイムアウトした場合、または、RADIUS クライアントが無効の場合は、ユーザー名とパスワードの検証を行い、ユーザー名とパスワードが合った場合はその時点で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、ポート認証でも使用できます。詳細は「スイッチング」の「ポート認証」をご覧ください。

本製品では、RADIUS サーバーを 3 台まで登録することができ、その優先順位も指定することができます。RADIUS サーバーを使用して、ユーザー認証を行うために最低限必要な設定は、次のとおりです。

以下の例では、RADIUS サーバーの IP アドレスを 192.168.10.10、優先順位 1 番、RADIUS サーバー個別のパスワードを Valid8Me と仮定しています。

1. RADIUS サーバーを登録します。ADD RADIUSSERVER コマンド (82 ページ) を使用し、RADIUS サーバーの IP アドレスとサーバーの優先順位、パスワードを指定してください。

```
ADD RADIUSSERVER SERVER=192.168.10.10 ORDER=1 SECRET=Valid8Me ↓
```

2. 認証モードを有効にします。

```
ENABLE AUTHENTICATION ↓
```

認証パケットのやり取りに使用する UDP ポート番号およびアカウントングパケットに使用する UDP ポート番号を変更するには、PORT パラメーター (認証) と ACCPORT パラメーター (アカウントング) を指定してください。(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。デフォルトでは、この設定になっています) RADIUS サーバーの設定を確認し、適切なポート番号を指定してください。

```
ADD RADIUSSERVER SERVER=192.168.10.10 ORDER=1 PORT=1645 ACCPORT=1646 ↓
```

RADIUS サーバーの登録を削除するには、DELETE RADIUSSERVER コマンド (118 ページ) を使用します。

```
DELETE RADIUSSERVER SERVER=192.168.10.10 ↓
```

RADIUS サーバー共通で使用するパスワードやタイムアウト時間などの、認証モードの設定を変更するには、SET AUTHENTICATION コマンド (187 ページ) を使用します。

```
SET AUTHENTICATION SECRET=himitu TIMEOUT=60 ↓
```

認証モードの設定や、登録されている RADIUS サーバーの一覧を表示するには、SHOW AUTHENTICATION コマンド (231 ページ) を使用します。

```
SHOW AUTHENTICATION ↓
```

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 属性で指定できます。

Service-Type 属性値	ユーザーレベル
Administrative(6)	Manager レベル
NAS Prompt(7)	User レベル

表 8:

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

RADIUS サーバーのアカウントिंग機能

本製品では、RADIUS 認証したユーザーのネットワーク利用状況を収集するための、RADIUS アカウントングプロトコルをサポートしているため、RADIUS サーバーのアカウントング機能を使用することができます。

アカウントサーバーは、RADIUS サーバーとして設定したサーバーになります。複数の RADIUS サーバーが設定されている場合には、認証に使用されたサーバーを使用します。本機能は、RADIUS サーバーの設定を行わないと使用できません。

RADIUS アカウンティング機能を有効にするには、ENABLE RADIUSACCOUNTING コマンド (153 ページ) を使用します。

```
ENABLE RADIUSACCOUNTING ↓
```

RADIUS アカウンティング機能を無効にするには、DISABLE RADIUSACCOUNTING コマンド (139 ページ) を使用します。

```
DISABLE RADIUSACCOUNTING ↓
```

RADIUS サーバーのアカウント機能に関する設定を変更する場合には、SET RADIUSACCOUNTING コマンド (202 ページ) を使用します。RADIUS サーバーのアカウント用 UDP ポート番号を変更するには、下記のコマンドを実行します。

```
SET RADIUSACCOUNTING SERVERPORT=1814 ↓
```

RADIUS サーバーのアカウント機能に関する設定を確認には、SHOW RADIUSACCOUNTING コマンド (275 ページ) を使用します。

```
SHOW RADIUSACCOUNTING ↓
```

RADIUS クライアント

RADIUS サーバーとの通信に対して、Timeout/Deadtime/RetransmitCount を設定することができます。また、RADIUS Access-Request パケットの始点 IP アドレスとなるインターフェースを指定することができます。

RADIUS サーバーとの通信に関するパラメーターを変更するには SET RADIUSSERVER コマンド (203 ページ) を使用します。RADIUS サーバーとのタイムアウト秒数を設定するには下記コマンドを実行します。

```
SET RADIUSSERVER TIMEOUT=10 ↓
```

RADIUS Access-Request の始点 IP アドレスとなるインターフェースを指定するには、ADD RADIUSSERVER コマンド (82 ページ) を使用します。

```
ADD RADIUSSERVER SERVER=192.168.100.10 SECRET=secret LOCAL=vlan-red ↓
```

アップロード・ダウンロード

本製品は、TFTP (Trivial File Transfer Protocol) XMODEM を利用したファイルのアップロード・ダウンロード、HTTP を利用したファイルのダウンロードが可能です。

- ☞ TFTP、HTTP を使うには、事前にローカル IP インターフェース (マネージメント VLAN インターフェース) の設定が必要です。詳しくは「IP」の「IP インターフェース」を参照してください。

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、コンソールポート経由で行う方法 (XMODEM) 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。

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 DESTFILE=myfile.cfg SERVER=192.168.10.5 FILE=myfile.cfg
↓
```

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、TFTP サーバー上で「test.txt」という名前を持つファイルを「test.cfg」として保存するには、次のようにします。

```
LOAD METHOD=TFTP DESTFILE=test.cfg SERVER=192.168.10.5 FILE=test.txt ↓
```

TFTP サーバー 192.168.10.5 からファームウェアファイル ats63j.img をダウンロードし、本製品のファームウェアを切り替えたい場合は、DESTFILE に APPBLOCK を指定します。

```
LOAD METHOD=TFTP DESTFILE=APPBLOCK SERVER=192.168.10.5 FILE=ats63j.img ↓
```

- ☞ ファームウェアの切り替えには時間がかかります。本製品が再起動するまでの間は、絶対に電源を切らないでください。書き込み中に電源を切ると、本製品を起動できなくなる可能性があります。

TFTP サーバー 192.168.10.5 からファームウェアファイル ats63j.img をダウンロードし、フラッシュメモリーに保存したい場合 (ファームウェアの切り替えは行われたい) は、DESTFILE にファイル名を指定します。

```
LOAD METHOD=TFTP DESTFILE=ats63_v200.img SERVER=192.168.10.5
FILE=ats63j.img ↓
```

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 (166 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 DESTFILE=myscript.scp SERVER=192.168.10.10
FILE=~admin/myscript.scp ↵
```

コンソールポート経由でのダウンロード

XMODEM でファイルをダウンロードします。

```
LOAD METHOD=XMODEM DESTFILE=test.cfg ↵
```

コマンドを入力すると操作を続けるかどうかのメッセージが表示されますので、Y キーを押して、Yes を選択します。画面上に文字列が表示され、受信待ち状態になりますので、コンソール側で XMODEM 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 XMODEM 転送のようなコマンドがあるはずです。

- ☞ XMODEM でファイルをダウンロードする際は、スイッチポートの通信を停止するようにしてください。

XMODEM でファームウェアファイルをダウンロードし、本製品のファームウェアを切り替えたい場合は、DESTFILE に APPBLOCK を指定します。

```
LOAD METHOD=XMODEM DESTFILE=APPBLOCK ↵
```

- ☞ ファームウェアの切り替えには時間がかかります。本製品が再起動するまでの間は、絶対に電源を切らないでください。書き込み中に電源を切ると、本製品を起動できなくなる可能性があります。

XMODEM でファームウェアファイルをダウンロードし、フラッシュメモリーに保存したい場合 (ファームウェアの切り替えは行われぬ) は、DESTFILE にファイル名を指定します。

```
LOAD METHOD=XMODEM DESTFILE=ats63.v200.img ↵
```

アップロード

アップロードは UPLOAD コマンド (309 ページ) で行います。プロトコルは TFTP と XMODEM が使えます。

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
DESTFILE=critical.cfg ↵
```

- ✎ 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
```

現在稼働中のファームウェアを、TFTP サーバー 192.168.10.5 にファームウェアファイル backup.img としてアップロードする場合は、SRCFILE/FILE に APPBLOCK を指定します。

```
UPLOAD METHOD=TFTP DESTFILE=backup.img SERVER=192.168.10.5
FILE=APPBLOCK ↵
```

現在の起動時設定ファイルを、TFTP サーバー 192.168.10.5 にアップロードする場合は、SRCFILE/FILE に SWITCHCFG を指定します。

```
UPLOAD METHOD=TFTP DESTFILE=backup.cfg SERVER=192.168.10.5
FILE=SWITCHCFG ↵
```

コンソールポート経由でのアップロード

XMODEM でファイルをアップロードします。

```
UPLOAD METHOD=XMODEM FILE=test.log ↵
```

コマンドを入力すると操作を続けるかどうかのメッセージが表示されますので、Y キーを押して、Yes を選択します。コンソール側で XMODEM の受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 XMODEM 転送のようなコマンドがあるはずですが。

- ✎ XMODEM でファイルをアップロードロードする際は、スイッチポートの通信を停止するようにしてください。

現在稼働中のファームウェアを、XMODEM でアップロードする場合は、SRCFILE/FILE に APPBLOCK を指定します。

```
UPLOAD METHOD=XMODEM FILE=APPBLOCK ↵
```

現在の起動時設定ファイルを、XMODEM でアップロードする場合は、SRCFILE/FILE に SWITCHCFG を指定します。

```
UPLOAD METHOD=XMODEM FILE=SWITCHCFG ↵
```

システム内のファームウェアファイルの転送

LOAD コマンド (166 ページ) で、METHOD に LOCAL を指定すると、フラッシュメモリー内のファームウェアファイルをアプリケーション領域にダウンロード (転送) し、起動時に使用するファームウェアファイルを切り替えることができます。

また、UPLOAD コマンド (309 ページ) で、METHOD に LOCAL を指定すると、現在稼働中のファームウェアをフラッシュメモリーにファイルとして保存することができます。

フラッシュメモリー内のファームウェアファイルをアプリケーション領域に転送し、本製品のファームウェアを切り替えたい場合は、DESTFILE に APPBLOCK を指定します。

```
LOAD METHOD=LOCAL DESTFILE=APPBLOCK FILE=ats63_v200.img ↵
```

現在稼働中のファームウェアを、フラッシュメモリーにファイルとして保存したい場合は、SRCFILE/FILE に APPBLOCK を指定します。

```
UPLOAD METHOD=LOCAL DESTFILE=backup.img FILE=APPBLOCK ↵
```

マスターからスレーブスイッチへのファイルの転送

UPLOAD コマンド (309 ページ) で、METHOD に REMOTESWITCH を指定すると、現在稼働中のファームウェアおよび設定ファイルを、マスタースイッチからスレーブスイッチに転送することができます。

マスタースイッチからスレーブスイッチにファームウェアファイルを転送する場合は、SRCFILE/FILE に APPBLOCK を指定します。

```
UPLOAD METHOD=REMOTESWITCH FILE=APPBLOCK SWITCHLIST=1 ↵
```

マスタースイッチからスレーブスイッチに、現在の起動時設定ファイルを転送する場合は、SRCFILE/FILE に SWITCHCFG を指定します。

```
UPLOAD METHOD=REMOTESWITCH FILE=SWITCHCFG SWITCHLIST=1 ↵
```

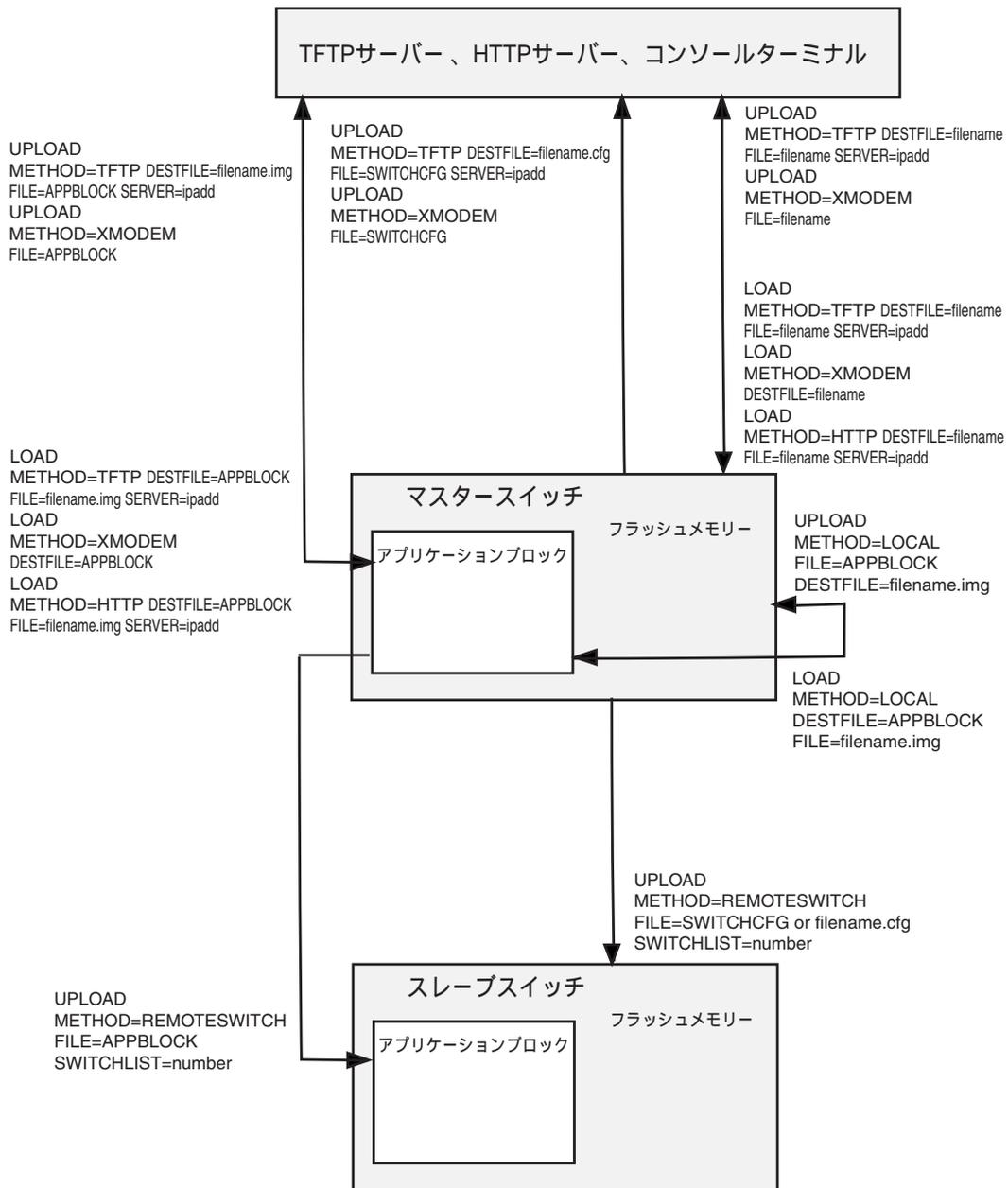
- ☞ マスタースイッチからスレーブスイッチに起動時設定ファイルを転送すると、スレーブスイッチは再起動し、IP アドレスおよびスタックモードの設定以外は、書き換えられます。

マスタースイッチからスレーブスイッチに、フラッシュメモリー内の設定ファイルを転送する場合は、SRCFILE/FILE にファイル名を指定します。

```
UPLOAD METHOD=REMOTESWITCH FILE=test.cfg SWITCHLIST=1 ↵
```

- ☞ マスタースイッチからスレーブスイッチに設定ファイルを転送すると、スレーブスイッチは再起動し、すべての設定が書き換えられます。

次の図は、ファイル操作のイメージ図です。



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（264 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」: メッセージを RAM 上に 4000 件まで記録。電源オンの間だけ保持される
- 「PERMANENT」: メッセージを 2000 件まで、NVS（不揮発性メモリー）上に記録。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（264 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=T 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=P と省略できます) ↓
```

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（264 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 ↓
```

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 ↓
```

ログのレベルおよびモジュールを指定することで、特定のログだけを表示することができます。ログのレベルおよび指定できるモジュールの一覧については、次の「資料編」をご覧ください。

特定レベルのログだけを見たいときは次のようにします。

```
SHOW LOG SEVERITY=E ↓
```

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=VLAN ↓
```

ログの保存

ログをファイルとして保存するには、SAVE LOG コマンド (185 ページ) を使います。

ログをファイルに保存するには次のようにします。ファイルの拡張子は、「.log」とします。

```
SAVE LOG FILENAME=hozon.log ↓
```

ログのレベルおよびモジュールを指定することで、特定のログだけを保存することができます。

特定レベルのログだけを保存したいときは次のようにします。

```
SAVE LOG FILENAME=hozon.log SEVERITY=E ↓
```

特定モジュールのログだけを保存したいときは次のようにします。

```
SAVE LOG FILENAME=hozon.log MODULE=VLAN ↓
```

syslog サーバーへのログ転送

ログメッセージは、syslog サーバー (syslogd) に転送することもできます。設定手順は、次のとおりです。

- ☞ syslog を使うには、事前にローカル IP インターフェース (マネージメント VLAN インターフェース) の設定が必要です。詳しくは「IP」の「IP インターフェース」を参照してください。

ここでは、すべてのメッセージを 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=2 DESTINATION=SYSLOG SERVER=192.168.10.5 ↓
```

2. メッセージフィルターを追加します。

```
ADD LOG OUTPUT=2 MODULE=ALL SEVERITY=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、スイッチ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。メッセージは syslog 形式に変換された上で、送信されます。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。

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=2 DESTINATION=SYSLOG SERVER=192.168.10.5 ↓
```

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 (198 ページ) を使います。たとえば、出力先「2」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=2 SERVER=192.168.10.100 ↓
```

ログ出力先の定義を削除するには DESTROY LOG OUTPUT コマンド (124 ページ) を使います。

```
DESTROY LOG OUTPUT=2 ↓
```

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 (79 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。

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、VLAN 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=VLAN ↓
```

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。

ログレベルが E (Error) と W (Warning) 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=2 SEVERITY=E,W ↓
```

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。

複数の条件を同時に指定することもできます。VLAN に関するログのうち、ログレベルが E (Error) 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=VLAN SEVERITY=E ↓
```

ログ設定の確認

ログの出力先定義は SHOW LOG OUTPUT コマンド (267 ページ) で確認します。Permanent と Temporary は、デフォルトで定義されている出力先です。

```
# show log output
OutputID  Type           Status      Details
```

```
-----
0      Permanent      Enabled   Wrap on Full
1      Temporary      Enabled   Wrap on Full
2      Syslog         Enabled   192.168.1.20
```

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 (267 ページ) に FULL オプションを付けます。

```
# show log output=2 full

Output ID ..... 2
Output Type ..... Syslog
Status ..... Enabled
Server IP Address ..... 192.168.1.20
Message Format ..... Extended
Facility Level ..... DEFAULT
Event Severity ..... All
Event Module ..... All
```

ログモジュールのステータスは、SHOW LOG STATUS コマンド (269 ページ) で確認できます。

```
# show log status

Event Log Configuration:
Event Logging ..... Enabled
Number of Output Definitions .... 3
```

資料編

メッセージの表示項目

ログメッセージには下記の項目が表示されます。

項目	説明
Severity	ログレベル
Date	メッセージが生成された日付 (現地時間)
Time	メッセージが生成された時刻 (現地時間)
Event	メッセージを生成したモジュールと、イベントの簡潔な説明
Event ID	イベント ID。aabccc の形式で表示。aa はモジュール ID、b はログレベル、ccc はモジュール内で一意のイベント ID (SHOW LOG コマンドで FULL オプションを指定したときに表示される)
Source File:Line Number	メッセージを生成したプログラムソースファイル名とソースファイル内の行番号 (SHOW LOG コマンドで FULL オプションを指定したときに表示される)

表 9:

S	Date	Time	EventID	Source	File:Line Number
			Event		

I	05/14/09	15:08:54	183001	fileapp.c:131	
				file: File System initialized	

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
E	Error	運用上の障害があることを示すメッセージ
W	Warning	運用上、潜在的な障害の恐れがあることを示すメッセージ
I	Information	通常の運用におけるメッセージ

表 10:

- このほかに、Debug (エラーに伴うデバッグ用メッセージ。きわめて詳細な情報で、大量のメッセージが出力される可能性あり) が表示されることがありますが、運用上必要な情報ではありません。

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、および SHOW LOG コマンド (264 ページ) の MODULE パラメーターに設定する場合の文字列の一覧を示します。

ID	モジュール名	設定値	備考
1	システム	SYSTEM	
2	コマンドラインプロセッサ	CLI	
3	ログ	EVTLOG	
4	MAC アドレス管理	MAC	
5	スパニングツリー (RSTP/MSTP を含む)	STP	
6	バーチャル LAN	VLAN	
7	GARP	GARP	未サポート
8	ポート設定	PCFG	
9	ポートミラーリング	PMIRR	
10	ポートトランキング	PTRUNK	
11	ポートセキュリティ	PSEC	
12	ポート認証	PACCESS	
13	ACL	ACL	

14	DoS	DOS	
15	マネージメントアクセスコントロール	MGMTACL	
16	IP	IP	
17	エンハンスドスタッキング	ESTACK	
18	ファイルシステム	FILE	
19	IGMP スヌーピング	IGMPSNOOP	
20	QoS	QOS	
21	TIME(SNTP を含む)	TIME	
22	TFTP	TFTP	
23	RRP Snooping	RRP	
24	HTTP	HTTP	未サポート
25	TELNET	TELNET	
26	SNMP	SNMP	
27	RADIUS	RADIUS	
28	TACACS	TACACS	未サポート
29	ENCO	ENCO	
30	PKI	PKI	
31	SSL	SSL	
32	SSH	SSH	
33	WDT	WATCHDOG	未サポート
34	RTC	RTC	未サポート
35	USER	USER	未サポート
36	コンフィグ	CFG	
37	ケーブルテスト	CABLE	未サポート
38	Classifier	CLASSIFIER	
39	PoE	POE	未サポート
40	LACP	LACP	未サポート
41	RPS	RPS	
42	MLD スヌーピング	MLDSNOOP	
43	EPSR スヌーピング	EPSRSNOOP	
44	FAN コントロール	FAN_CTRL	未サポート
45	VRRP	VRRP	
46	BOOTP リレー	BOOTPRELAY	
47	DHCP サーバー	DHCPSVR	
48	Web 認証	WEBAUTH	
49	ループガード (LDF 検出)	LOOPDETECTION	
50	ループガード (受信レート検出)	STORMDETECTION	
51	DNS リレー	DNSRELAY	

52	IP ヘルパー	IPHELPER	
53	DHCP スヌーピング	DHCPSNOOP	
54	EPSR	EPSR	未サポート

表 11:

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」に以下のとおりマッピングされます。

ログレベル	syslog レベル
E (Error)	LOG_ERR
W (Warning)	LOG_WARNING
I (Information)	LOG_INFO

表 12:

モジュール/イベントと syslog ファシリティーのマッピング

デフォルトでは、syslog サーバーに送信される各ログメッセージには、生成元のモジュールまたはイベントに応じて下記の syslog ファシリティーが割り当てられます。

モジュール	syslog ファシリティー	備考
1. システム (SYSTEM)	LOG_LOCAL0	
2. コマンドラインプロセッサ (CLI)	LOG_LOCAL0	
3. ログ (EVTLOG)	LOG_LOCAL0	
4. MAC アドレス管理 (MAC)	LOG_LOCAL0	
5. スパニングツリー (RSTP/MSTP を含む) (STP)	LOG_LOCAL6	
6. バーチャル LAN (VLAN)	LOG_LOCAL6	
7. GARP (GARP)	LOG_LOCAL0	未サポート
8. ポート設定 (PCFG)	LOG_LOCAL6	
9. ポートミラーリング (PMIRR)	LOG_LOCAL6	
10. ポートトランキング (PTRUNK)	LOG_LOCAL6	
11. ポートセキュリティ (PSEC)	LOG_SECURITY	
12. ポート認証 (PACCESS)	LOG_SECURITY	
13. ACL (ACL)	LOG_LOCAL0	
14. DoS (DOS)	LOG_SECURITY	
15. マネージメントアクセスコントロール (MGMTACL)	LOG_SECURITY	

16. IP (IP)	LOG_LOCAL0	
17. エンハンススタッキング (ESTACK)	LOG_LOCAL0	
18. ファイルシステム (FILE)	LOG_LOCAL0	
19. IGMP スヌーピング (IGMPSNOOP)	LOG_LOCAL0	
20. QoS (QOS)	LOG_LOCAL0	
21. TIME(SNTP を含む) (TIME)	LOG_CRON	
22. TFTP (TFTP)	LOG_LOCAL0	
23. RRP Snooping (RRP)	LOG_LOCAL0	
24. HTTP (HTTP)	LOG_LOCAL0	未サポート
25. TELNET (TELNET)	LOG_LOCAL0	
26. SNMP (SNMP)	LOG_LOCAL0	
27. RADIUS (RADIUS)	LOG_SECURITY	
28. TACACS (TACACS)	LOG_SECURITY	未サポート
29. ENCO (ENCO)	LOG_SECURITY	
30. PKI (PKI)	LOG_SECURITY	
31. SSL (SSL)	LOG_SECURITY	
32. SSH (SSH)	LOG_SECURITY	
33. WDT (WATCHDOG)	LOG_LOCAL0	未サポート
34. RTC (RTC)	LOG_CRON	未サポート
35. USER (USER)	LOG_LOCAL0	未サポート
36. コンフィグ (CFG)	LOG_LOCAL0	
37. ケーブルテスト (CABLE)	LOG_LOCAL0	未サポート
38. Classifier (CLASSIFIER)	LOG_LOCAL0	
39. PoE (POE)	LOG_LOCAL0	未サポート
40. LACP (LACP)	LOG_LOCAL6	未サポート
41. RPS (RPS)	LOG_LOCAL0	
42. MLD スヌーピング (MLDSNOOP)	LOG_LOCAL0	
43. EPSR スヌーピング (EPSRSNOOP)	LOG_LOCAL0	
44. FAN コントロール (FAN_CTRL)	LOG_LOCAL0	未サポート
45. VRRP (VRRP)	LOG_LOCAL0	
46. BOOTP リレー (BOOTPRELAY)	LOG_LOCAL0	
47. DHCP サーバー (DHCP SVR)	LOG_LOCAL0	
48. Web 認証 (WEBAUTH)	LOG_LOCAL0	
49. ループガード (LDF 検出) (LOOPDETECTION)	LOG_LOCAL0	
50. ループガード (受信レート検出) (STORMDETECTION)	LOG_LOCAL0	
51. DNS リレー (DNSRELAY)	LOG_LOCAL0	
52. IP ヘルパー (IPHELPER)	LOG_LOCAL0	
53. DHCP スヌーピング (DHCP SNOOP)	LOG_LOCAL0	

表 13:

なお、上記マッピングの例外として、次のイベントは生成元モジュールに関係なく特定のファシリティにマッピングされます。

- LOG_LOCAL7 にマッピングされるイベント
 - ファン障害を検出したとき
 - メモリー不足
 - 温度異常を検出したとき
- LOG_SECURITY にマッピングされるイベント
 - ユーザーログインに失敗したとき
 - ユーザーログイン失敗を繰り返してロックアウトされたとき
 - ロックアウト状態でログインしようとしたとき
 - ユーザーがログインしたとき
 - ユーザーがログアウトしたとき
 - ユーザーが追加されたとき
 - ユーザーが削除されたとき
 - 認証モードの有効・無効が設定されたとき
 - ユーザーパスワードが変更されたとき
 - MANAGER 権限のユーザーがリモートからログインしている状態でコンソールポートから MANAGER 権限のユーザーがログインしたため、リモートログインセッションが強制切断されたとき

モジュールやイベント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 (94 ページ)、SET LOG OUTPUT コマンド (198 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 ↵
```

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。

- ☞ SNMP を使うには、事前にローカル IP インターフェース (マネージメント VLAN インターフェース) の設定が必要です。詳しくは「IP」の「IP インターフェース」を参照してください。

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 管理ホストの IP アドレス	192.168.10.5
SNMP トラップホストの IP アドレス	192.168.10.5

表 14:

1. SNMP エージェントを有効にします。

```
ENABLE SNMP ↓
```

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、スイッチ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ーとして「private」がデフォルトで設定

されています。本製品にも、この2つのコミュニティがデフォルトで設定されています。

3. SNMP コミュニティ「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。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。

```
ADD SNMP COMMUNITY=viewers TRAPHOST=192.168.10.5
MANAGER=192.168.10.5 ↓
```

基本設定は以上です。

これにより、SNMP マネージャー (192.168.10.5) 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 トラップがマネージャーに送信されるようになります。

☞ 本コマンドで指定したトラップホストには、SNMPv2c 形式のトラップが送信されます。

本製品で、SNMP バージョン 1 (SNMPv1) のみ対応のトラップホストにトラップを送信するためには、CREATE SNMP COMMUNITY コマンド (100 ページ) で作成したのとは別のコミュニティを作成し、トラップホストの設定を行う必要があります。

下記の設定コマンドの必要な部分のみ変更して、入力してください。コマンドの順序もそのまま入力してください。

SNMP コミュニティ	v1trap (v1 対応トラップ送信のみ)
SNMP トラップホストの IP アドレス	192.168.10.10 (v1 のみ対応のトラップホスト)

表 15:

設定コマンド

```
create snmpv3 view=MyView subtree=1.3.6.1 storagetype=nonvolatile ↓
create snmpv3 access=MyAccess securitymodel=v1
securitylevel=noauthentication notifyview=MyView
storagetype=nonvolatile ↓
create snmpv3 notify=MyNotify tag=MyTag storagetype=nonvolatile ↓
create snmpv3 targetaddr=MyTarget params=MyTraps ipAddress=192.168.10.10
taglist=MyTag storagetype=nonvolatile ↓
create snmpv3 targetparams=MyTraps username=MyUser securitymodel=v1
messageprocessing=v1 securitylevel=noauthentication
storagetype=nonvolatile ↓
create snmpv3 group username=MyUser securitymodel=v1 groupname=MyAccess
storagetype=nonvolatile ↓
create snmpv3 community index=1 communityname=v1trap securityname=MyUser
storagetype=nonvolatile ↓
```

上記の設定コマンドのうち、下記のパラメーターは、ご使用の環境に合わせて変更してください。

CREATE SNMPV3 TARGETADDR コマンド	
TARGETADDR	1～63文字の英数字で指定
IPADDRESS	v1のみ対応のトラップホストのIPアドレス
CREATE SNMPV3 COMMUNITY コマンド	
INDEX	1～63文字の英数字で指定
COMMUNITYNAME	コミュニティー名 (CREATE SNMP COMMUNITY コマンドで作成したのとは違うコミュニティー名を指定してください)

表 16:

v1 対応のトラップホストを複数設定する場合は、CREATE SNMPV3 TARGETADDR コマンドで追加します。TARGETADDR パラメーターには、異なる文字列を指定してください。

```
add snmpv3 targetaddr=MyTarget2 ↓
```

追加した v1 対応のトラップホストを削除する場合は、DESTROY SNMPV3 TARGETADDR コマンドで削除します。

```
destroy snmpv3 targetaddr=MyTarget2 ↓
```

v1 対応のトラップ送信用コミュニティーを複数設定する場合は、CREATE SNMPV3 COMMUNITY コマンドで追加します。INDEX パラメーターには、異なる文字列を指定してください。

```
create snmpv3 community index=2 ↓
```

追加した v1 対応のトラップ送信用コミュニティーを削除する場合は、DESTROY SNMPV3 COMMUNITY コマンドで削除します。

```
destroy snmpv3 community index=2 ↓
```

設定をすべて削除するには、下記のコマンドを入力してください。コマンドの順序もこのまま入力してください。

```
destroy snmpv3 community index=1 ↓
destroy snmpv3 group username=MyUser securitymodel=v1 ↓
destroy snmpv3 targetparams=MyTraps ↓
destroy snmpv3 targetaddr=MyTarget ↓
destroy snmpv3 notify=MyNotify ↓
destroy snmpv3 access=MyAccess securitymodel=v1
securitylevel=noauthentication ↓
destroy snmpv3 view=MyView subtree=1.3.6.1 ↓
```

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(84 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「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 ↓
```

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(100 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(204 ページ)を使います。

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

SNMP の設定を確認するには、SHOW SNMP コマンド(277 ページ)、SHOW SNMP COMMUNITY コマンド(278 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。

本製品では、下記の設定を行います。(それぞれの設定は、テーブルとして管理されます。)

- ユーザーの作成
ユーザー名、ユーザーの認証プロトコル (MD5 と SHA から選択) およびパスワード、暗号化パスワード (プロトコルは DES のみ対応) を設定します。
ユーザーの作成は、ADD SNMPV3 USER コマンド(85 ページ)で行います。
- ビューの定義
ビュー名、MIB オブジェクトの範囲とそれをビューに含めるか含めないかを指定します。
ビューの定義は、CREATE SNMPV3 VIEW コマンド(112 ページ)で行います。
- ユーザーグループの作成
ユーザーグループ名、ユーザーグループのセキュリティモデル (SNMPv1、v2c、v3 から選択)、セキュリティレベル (通信時の認証・暗号化の有無。認証なし・暗号化なし、認証あり・暗号化なし、

認証あり・暗号化ありから選択)、ユーザーが読み出し可能なビュー、書き込み可能なビュー、通知可能なビューを指定します。(ビューは、CREATE SNMPV3 VIEW コマンド(112 ページ)で定義されます。)

ユーザーグループの作成は、CREATE SNMPV3 ACCESS コマンド(102 ページ)で行います。

- ユーザーとユーザーグループの対応付け
ユーザーが所属するユーザーグループとセキュリティモデル(SNMPv1、v2c、v3 から選択)を指定します。(ユーザーは、ADD SNMPV3 USER コマンド(85 ページ)で作成されます。また、ユーザーグループは、CREATE SNMPV3 ACCESS コマンド(102 ページ)で作成されます。) ユーザーとユーザーグループの対応付けは、CREATE SNMPV3 GROUP コマンド(106 ページ)で行います。
- 通知名の定義
通知名、通知メッセージのタイプを指定します。
通知名の定義は、CREATE SNMPV3 NOTIFY コマンド(107 ページ)で行います。
- ターゲット(通知メッセージの送信先)を追加
ターゲット名、ターゲットパラメーターセット名、ターゲットの IP アドレスなどを指定します。
ターゲットの追加は、CREATE SNMPV3 TARGETADDR コマンド(108 ページ)で行います。
- ターゲットとの通信に使用するパラメーターセットの定義
ターゲットパラメーターセット名、ユーザー名、セキュリティモデル(SNMPv1、v2c、v3 から選択)、セキュリティレベル(通信時の認証・暗号化の有無。認証なし・暗号化なし、認証あり・暗号化なし、認証あり・暗号化ありから選択)を指定します。
パラメーターセットの定義は、CREATE SNMPV3 TARGETPARAMS コマンド(110 ページ)で行います。
- コミュニティーの作成
コミュニティー名、コミュニティーに対するパスワード、ユーザー名などを指定します。
コミュニティーの作成は、CREATE SNMPV3 COMMUNITY コマンド(104 ページ)で行います。

📌 SNMPv1/v2c 対応のコミュニティーの作成や管理ホストおよびトラップホストを追加する場合は、CREATE SNMPV3 COMMUNITY コマンド(104 ページ)ではなく、CREATE SNMP COMMUNITY コマンド(100 ページ)をご使用ください。ただし、SNMPv1 のみ対応のトラップホストにトラップを送信するためには、SNMPv3 用のコマンドを使わなければなりません。本章の「SNMPv1/SNMPv2c」の「基本設定」「本製品で、SNMP パージョン 1 (SNMPv1) のみ対応のトラップホストにトラップを送信するためには」以降の説明を参照して設定を行ってください。

本製品で、SNMPv3 に関する設定を行う場合は、上記の順番で設定することをお勧めします。

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。

📌 ADD SNMPV3 USER コマンド(85 ページ)で作成したユーザーは、その他の SNMPv3 に関する設定とは異なり、CREATE CONFIG コマンド(91 ページ)で設定ファイルに保存されません。設定を保存するには、SAVE CONFIGURATION コマンド(184 ページ)を実行してください。また、SET CONFIG コマンド(188 ページ)で NONE を指定し、起動時設定ファイルの設定がなしでもユーザーは削除されません。ユーザーを削除する場合は、DELETE SNMPV3 USER コマンド(120 ページ)で削除し、SAVE CONFIGURATION コマンド

(184 ページ) を実行してください。ただし、SAVE CONFIGURATION コマンド (184 ページ) を実行しても、SNMPv3 ユーザーに関する設定は、ユーザーがアップロード・ダウンロード可能な設定ファイルには保存されませんので、設定のバックアップを行う場合には、本製品からアップロードした設定ファイルとは別に SNMPv3 USER 設定コマンドをテキストファイルなどで保管してください。

ユーザー名	systemadmin24
ビュー名	internet
グループ名	Managers
読み出しビュー名	internet
書き込みビュー名	internet
通知ビュー名	internet
通知タグ	sysadminTag
ターゲット	host451
パラメーターセット	SNMPmanagerPC

表 17:

1. SNMP エージェントを有効にします。

```
ENABLE SNMP ↵
```

2. ユーザーを作成します。SNMPv3 の設定では、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、ユーザー「systemadmin24」を作成しています。

```
ADD SNMPV3 USER=systemadmin24 AUTHENTICATION=MD5
  AUTHPASSWORD=kumanomi PRIVPASSWORD=imonamuk
  STORAGETYPE=nonvolatile ↵
```

3. 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「internet」を作成します。

```
CREATE SNMPV3 VIEW=internet SUBTREE=1.3.6.1 TYPE=INCLUDED
  STORAGETYPE=nonvolatile ↵
```

☞ ビューを定義するときは、MIB ノードを「1.3.6.1.」のような OID (Object Identifier) で指定する方法と、「internet」のような名前で指定する方法があります。どちらも、CREATE SNMPV3 VIEW コマンド (112 ページ) の SUBTREE パラメーターで指定します。なお、名前で指定できるのは、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。

4. 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「managers」を定義します。managers グループのユーザーには、internet 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。

```
CREATE SNMPV3 ACCESS=managers SECURITYMODEL=V3 SECURITYLEVEL=PRIVACY
  READVIEW=internet WRITEVIEW=internet NOTIFYVIEW=internet
  STORAGETYPE=nonvolatile ↓
```

5. ユーザーとユーザーグループの対応付けを行います。ユーザーが、どのグループに所属するかを定義します。

ここではユーザー「systemadmin24」が、管理者グループ「managers」に所属するものとします。

```
CREATE SNMPV3 GROUP USERNAME=systemadmin24 SECURITYMODEL=V3
  GROUPNAME=managers STORAGETYPE=nonvolatile ↓
```

6. 通知名を定義します。通知メッセージのフォーマットなどを定義します。

```
CREATE SNMPV3 NOTIFY=sysadmintrap TAG=sysadmintag TYPE=TRAP
  STORAGETYPE=nonvolatile ↓
```

7. ターゲットを追加します。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（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などを指定します。

```
CREATE SNMPV3 TARGETADDR=host451 PARAMS=SNMPmanagerPC
  IPADDRESS=192.168.1.100 TAGLIST=sysadminTag
  STORAGETYPE=nonvolatile ↓
```

8. 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などを指定します。

```
CREATE SNMPV3 TARGETPARAMS=SNMPmanagerPC USERNAME=systemadmin24
  SECURITYMODEL=V3 MESSAGEPROCESSING=V3 SECURITYLEVEL=PRIVACY
  STORAGETYPE=nonvolatile ↓
```

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 を参照するには、SHOW SNMPV3 ENGINEID コマンド（286 ページ）を使います。

```
SHOW SNMPV3 ENGINEID ↓
```

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、デフォルトでオンになっています。

リンクトラップの設定を確認するには SHOW INTERFACE コマンド（260 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 interface=1 ↓
```

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 (224 ページ) を使います。

```
SET SYSTEM NAME=c9424 ↓
```

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 (223 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 (221 ページ) を使います。

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

SNTP

SNTP (Simple Network Time Protocol) を利用すると、ネットワーク上の SNTP 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、SNTP の利用をおすすめします。

SNTP プロトコルは、NTP プロトコルをベースに、クライアントの時刻合わせ用途に向けて軽量化したプロトコルですので、本製品では、SNTP サーバーと NTP サーバーのどちらにも対応します。

基本設定

SNTP 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。

SNTP 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 18:

1. SNTP モジュールを有効にします。

```
ENABLE SNTP ↓
```

2. SNTP 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 SNTP PEER コマンド (86 ページ) を使います。

```
ADD SNTP 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。SNTP 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。SET SNTP コマンド (216 ページ) を使います。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 SNTP UTCOFFSET=9 ↓
```

基本設定は以上です。

これにより、定期的に SNTP 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 (304 ページ) で確認します。

```
# show time
System time is 10:57:47 on 12-May-2009
```

SNTP に関する情報は SHOW SNTP コマンド (298 ページ) で確認します。

```
# show sntp
SNTP Configuration:
Status ..... Enabled
Server ..... 192.168.10.5
```

```
UTC Offset ..... +9
Daylight Savings Time (DST) ... Disabled
Poll Interval ..... 600 seconds
Last Delta ..... +0 seconds
```

マネージメントアクセスコントロール

マネージメントアクセスコントロールは、本製品宛ての IP 通信（ユニキャスト IP パケット）を制限する機能です。

次に本機能の基本仕様を示します。

- 本機能は、本製品宛てのユニキャスト IP パケットにのみ適用され、ブロードキャストパケットやマルチキャストパケット、非 IP パケット、本製品宛てでないスイッチング対象パケットやルーティング対象パケットには適用されません。
ただし、本製品宛てユニキャスト IP パケットの中にも、次に述べる 2 つの例外があります。
 - Web 認証用 HTTP/HTTPS サーバー宛てのパケットはつねに許可
本機能の有効・無効や Management ACL の設定内容にかかわらず、本製品の Web 認証用 HTTP/HTTPS サーバー宛て TCP パケットはつねに許可します。
 - SSH サーバー宛てのパケットはつねに破棄
本機能の有効時には、Management ACL の設定にかかわらず、本製品の SSH サーバー宛て TCP パケットをつねに破棄します。したがって、本機能と SSH サーバーは併用できません。
 - 本機能はデフォルト無効です。
 - 本機能の有効時は、マネージメントアクセスコントロールリスト（Management ACL）のエントリーと合致するパケットだけを受け入れ、それ以外のパケットは破棄します。
 - 受信したパケットと Management ACL の照合は、エントリーの登録順に行います。合致するエントリーが見つかった場合はパケットを受け入れ、それ以降のエントリーとの照合は行いません。どのエントリーにも合致しないパケットは破棄します。
- 📎 マネージメントアクセスコントロールを有効にする場合は、Management ACL にエントリーが登録されていることを確認してから有効にしてください。Management ACL にエントリーが登録されていない場合、Web 認証用 HTTP/HTTPS サーバー宛ての TCP パケットを除くすべての本体宛てパケットを破棄します。
- 📎 SSH サーバーを利用する場合は、マネージメントアクセスコントロールを有効にしないでください。マネージメントアクセスコントロールの有効時は、Management ACL の設定にかかわらず、本製品宛ての SSH パケットをすべて破棄します。

マネージメントアクセスコントロールリスト（Management ACL）

本機能では、Management ACL にエントリーを作成することで、受け入れるパケットの条件を登録します。エントリーは 256 個まで作成可能です。

Management ACL の各エントリーで指定可能な条件は次の 3 つです。受信したパケットがエントリーのすべての条件を満たした場合、エントリーに合致したと見なします。

- 受信スイッチポート（PORTLIST）
単一ポートだけでなく複数ポートの指定も可能。省略時は ALL（すべてのポート）
- 始点 IP アドレス（IPADDRESS/MASK）
マスク指定により、単一アドレスだけでなくアドレス範囲の指定も可能。省略時は 0.0.0.0/0.0.0.0（すべてのアドレス）

- パケットの種類 (APPLICATION)
指定方法については次の表を参照。省略時は ALL (本機能の適用対象となるすべてのパケット)

	Telnet	ICMP(Echo-Req)	ICMP(Echo-Req 以外)	HTTP ダウンロード	UDP
APPLICATION=TELNET		x			
APPLICATION=PING	x				
APPLICATION=ALL					

表 19: APPLICATION パラメーターの値と対象パケット

次に、本製品宛てのユニキャスト IP パケットを受信したときの動作を説明します。

- 本機能が無効のときは、すべてのパケットを受け入れます。
- 本機能が有効でも、Management ACL にエントリーが登録されていないときは、Web 認証用 HTTP/HTTPS サーバー宛ての TCP パケットを除く、すべてのパケットを破棄します。
- 本機能が有効で、Management ACL にエントリーが登録されているときは、受信パケットがいずれかのエントリーに合致した場合に該当パケットを受け入れます。どのエントリーにも合致しなかったパケットは破棄します。

各種パケットがエントリーに合致するのは次の場合です。

- Telnet パケット (終点ポートが 23 の本体宛て TCP パケット)
受信スイッチポートと始点 IP アドレスが PORTLIST、IPADDRESS/MASK に一致する、APPLICATION=TELNET または ALL のエントリーに合致
- Ping パケット (ICMP Type が Echo Request の本体宛て ICMP パケット)
受信スイッチポートと始点 IP アドレスが PORTLIST、IPADDRESS/MASK に一致する、APPLICATION=PING または ALL のエントリーに合致
- Ping 以外の ICMP パケット (ICMP Type が Echo Request 以外の本体宛て ICMP パケット)
受信スイッチポートと始点 IP アドレスが PORTLIST、IPADDRESS/MASK に一致する、APPLICATION=TELNET、PING、または、ALL のエントリーに合致
- HTTP ダウンロードパケット (LOAD コマンド (166 ページ) で開始した HTTP ダウンロードの戻りパケット)
受信スイッチポートと始点 IP アドレスが PORTLIST、IPADDRESS/MASK に一致する、APPLICATION=TELNET、PING、または、ALL のエントリーに合致
- UDP パケット (RADIUS、TFTP、SNMP、SNTP、DHCP、DNS など各種アプリケーションの本体宛てパケット)
受信スイッチポートと始点 IP アドレスが PORTLIST、IPADDRESS/MASK に一致する、APPLICATION=TELNET、PING、または、ALL のエントリーに合致
- 本機能が有効のとき、本製品の Web 認証用 HTTP/HTTPS サーバー宛て TCP パケットは常に受け入れます。
- 本機能が有効のとき、本製品の SSH サーバー宛て TCP パケットはつねに破棄します。したがって、本機能と SSH サーバーは併用できません。

基本設定

Management ACL の設定は、次の手順で行います。

1. Management ACL を作成します。CREATE MGMTACL コマンド (96 ページ) を使って、受け入れるバケットの条件を登録します。

- IP アドレス 192.168.10.10 からの Telnet アクセス (厳密には ICMP Echo Request と SSH を除くすべての本体宛てパケット) を許可する場合

```
CREATE MGMTACL ID=10 IPADDRESS=192.168.10.10 MASK=255.255.255.255
APPLICATION=TELNET ↓
```

- IP アドレス範囲 192.168.20.0/24 (192.168.20.0 ~ 192.168.20.255) からの Ping (厳密には Telnet と SSH を除くすべての本体宛てパケット) を許可する場合

```
CREATE MGMTACL ID=20 IPADDRESS=192.168.20.0 MASK=255.255.255.0
APPLICATION=PING ↓
```

- スイッチポート 1 ~ 12 からは SSH を除くすべてのパケットを許可する場合

```
CREATE MGMTACL ID=30 PORTLIST=1-12 APPLICATION=ALL ↓
```

2. マネージメントアクセスコントロールを有効にします。ENABLE MGMTACL コマンド (152 ページ) を使います。

```
ENABLE MGMTACL ↓
```

設定は以上です。

既存のエントリーに許可対象のパケットの種類を追加するには、ADD MGMTACL コマンド (80 ページ) を使います。

```
ADD MGMTACL ID=10 APPLICATION=PING ↓
```

既存のエントリーから許可対象のパケットの種類を削除するには、DELETE MGMTACL コマンド (116 ページ) を使います。

```
DELETE MGMTACL ID=10 APPLICATION=PING ↓
```

Management ACL からエントリーを削除するには、DESTROY MGMTACL コマンド (125 ページ) を使います。

```
DESTROY MGMTACL ID=10 ↓
```

マネージメントアクセスコントロールを無効にするには、DISABLE MGMTACL コマンド (138 ページ) を使います。

```
DISABLE MGMTACL ↓
```

マネージメントアクセスコントロールの状態と Management ACL の内容を参照するには、SHOW

MGMTACL コマンド (270 ページ) を使用します。

```
SHOW MGMTACL ↓
```

特定のエントリーの内容を参照するには、SHOW MGMTACL コマンド (270 ページ) の ID パラメーターでエントリー番号を指定します。

```
SHOW MGMTACL ID=10 ↓
```

攻撃検出

攻撃検出は、下記の DoS 攻撃を受けたとき、この攻撃から本製品を守るために、攻撃を受けたことを通知したり、不正なパケットを破棄したりする機能です。

SYN Flood Attack	TCP の Syn パケットを断続的に送りつけ、ハーフオープンのコネクションを大量に生成し（始点アドレスを詐称するため、Syn/Ack への返答はない）標的システムのコネクションキーを枯渇させる
Smurf Attack	始点アドレスを詐称（標的のアドレスを設定する）した Ping パケットを中継サイトのディレクテッドブロードキャストアドレスに送り、中継サイトから標的サイトに大量にリプライを送りつけさせる
Land Attack	始点と終点に同じアドレスを設定した IP パケットによる DoS 攻撃。システムのバグをねらう
Teardrop Attack	IP パケットのオフセット情報を偽造したパケットを送り、パケットの復元処理をうまくできないといった、TCP/IP 実装上の問題をついた攻撃
Ping of Death	システムのバグをつくもので、特定サイズの Ping パケットを送りつけることによりシステムをクラッシュさせる
IP Options Attack	不正な IP オプションを含むパケットを送りつける

表 20:

攻撃検出に関する仕様は、次のとおりです。

- スイッチポートでは、一度に複数の攻撃に対する防御を有効にできる
 - Smurf Attack および Land Attack の攻撃検出機能を有効にする場合は、本製品が所属するネットワークの IP アドレスおよびサブネットマスクを指定が必要。また、Land Attack の場合は、アップリンクポートの指定も必要
 - Smurf Attack および SYN Flood Attack 以外の攻撃検出機能では、ミラーポートを設定することができるので、不正なパケットを解析することができる
- ☞ 攻撃検出機能と DHCP Snooping は同時に有効にできません。
- ☞ 攻撃検出機能を有効にする場合、Teardrop Attack および Ping of Death 攻撃検出に関しては、CPU に負荷がかかるので、注意して使用してください。

SYN Flood Attack

この攻撃を検出するために、スイッチポートでは、いくつかの SYN パケットを受信したかをモニターし、SYN パケットが SYN/ACK パケットの 2 倍以上、かつ、1 秒あたり 20 以上の SYN パケットを受信した場合に、次のアクションを実行します。

- SNMP トラップをマネージメントステーションに送る
- 1 分以内に受信した TCP Syn パケットを破棄する（ただし、すでにオープンしている TCP コネクションは継続する）

この攻撃検出のメカニズムは、スイッチの CPU での処理に影響を与えないため、一度に多くのポートに攻撃検出のための設定を行っても、スイッチのパフォーマンスには影響しません。

スイッチポートに、SYN Flood Attack を検出するように設定するには、SET DOS SYNFLOOD コマンド (194 ページ) を使います。

```
SET DOS SYNFLOOD PORT=18-20 STATE=ENABLE ↓
```

Smurf Attack

この攻撃を検出するために、スイッチポートでは、受信した ICMP Echo (Ping) リクエストの宛先アドレスがブロードキャストアドレスでないかどうかをチェックし、宛先アドレスがブロードキャストアドレスの場合は、このパケットを破棄します。

この攻撃検出のメカニズムは、スイッチの CPU での処理に影響を与えないため、一度に多くのポートに攻撃検出のための設定を行っても、スイッチのパフォーマンスには影響しません。

スイッチポートに、Smurf Attack を検出するように設定するには、SET DOS SMURF コマンド (193 ページ) を使います。

```
SET DOS SMURF PORT=18-20 STATE=ENABLE ↓
```

Smurf Attack を検出するには、SET DOS コマンド (189 ページ) を使って、スイッチの属するネットワークの IP アドレスとサブネットマスクを設定します。

```
SET DOS IPADDRESS=192.168.10.1 SUBNET=255.255.255.0 ↓
```

IP アドレスとサブネットマスク設定を表示するには、SHOW DOS コマンド (241 ページ) を使います。

Land Attack

この攻撃を検出するために、スイッチの所属するネットワークに外部から入ってくるパケットと、外部に行くパケットをチェックします。ネットワーク内で生成され、宛先アドレスがローカル IP アドレスである場合は、ネットワークの外には転送せず、またネットワーク外で生成され、送信元アドレスがローカル IP である場合は、ネットワーク内には転送されません。

この攻撃検出のメカニズムは、スイッチの CPU での処理に影響を与えないため、すべてのポートに設定を行っても、スイッチの動作には影響がありません。

スイッチポートに、Land Attack を検出するように設定するには、SET DOS LAND コマンド (191 ページ) を使います。

```
SET DOS LAND PORT=5,7 STATE=ENABLE ↓
```

Land Attack を検出するには、SET DOS コマンド (189 ページ) を使って、スイッチの属するネットワークの IP アドレスとサブネットマスク、およびアップリンクポートを設定します。

```
SET DOS IPADDRESS=192.168.10.1 SUBNET=255.255.255.0 UPLINKPORT=24 ↓
```

IP アドレスとサブネットマスク、およびアップリンクポートの設定を表示するには、SHOW DOS コマンド (241 ページ) を使います。

- 📎 スイッチにルーターなどが接続されていない場合は、Land Attack 検出に関する設定をする必要はありません。

Teardrop Attack

このタイプの攻撃を検出するために、スイッチポートで受信したフラグメントされた IP パケットを、すべてスイッチの CPU に送ります。CPU は関連のある、連続したフラグメントをサンプリングし、不正なオフセットを持ったフラグメントがないかどうかをチェックします。不正なフラグメントが見つかった場合には、下記のアクションを実行します。

- SNMP トラップをマネージメントステーションに送る
- 不正なオフセットを持ったフラグメントを破棄し、1 分間、受信したすべての IP フラグメントを破棄します。

- 📎 この機能を実行すると CPU の処理に影響を与えるので、注意して使用してください。スイッチの停止を招くこともありますので、使用する場合には、適用ポートを限定してお使いください。また、このような事態を避けるためにも、一度にこの機能を有効にするのは、アップリンクポートとその他に 1 ポートまでにすることをお勧めします。

スイッチポートに、Teardrop Attack を検出するように設定するには、SET DOS TEARDROP コマンド (195 ページ) を使います。

```
SET DOS TEARDROP PORT=24 STATE=ENABLE ↓
```

Ping of Death Attack

この攻撃を検出するために、スイッチポートでフラグメントされた ICMP Echo (Ping) リクエストの最後のフラグメントを検索し、そのオフセットからパケットのサイズが 65536 バイト以上かどうかを調査します。65536 バイト以上の場合には、そのフラグメントをスイッチの CPU に転送し、最終的なパケットサイズを決定します。その結果、パケットのサイズが 65536 バイト以上と決まった場合には、下記のアクションを実行します。

- SNMP トラップをマネージメントステーションに送る
- フラグメントを破棄し、1 分間に受信した、すべてのフラグメントされた ICMP Echo (Ping) リクエストを破棄します。

- 📎 この攻撃検出のメカニズムは、Teardrop Attack ほどではありませんが、スイッチの CPU での処理に影響を与えます。スイッチポート間の通信には影響がありませんが、IGMP パケットやスパンニングツリーの BPDU などの CPU イベントの処理に影響を与えます。このため、この攻撃を最も受けやすいポートにのみ限定して機能を有効にすることをお勧めします。

スイッチポートに、Ping of Death Attack を検出するように設定するには、SET DOS PINGOFDEATH コマンド (192 ページ) を使います。

```
SET DOS PINGOFDEATH PORT=1,5 STATE=ENABLE ↓
```

IP Options Attack

IP Option Attack の種類は多いので、本製品では、その違いを区別するのではなく、スイッチポートで受信した IP パケットのうち、IP オプションを含んでいるものをカウントアップして、この数が 1 秒あたり 20 パケットを超すと、IP Option Attack の可能性があるものと判断し、下記のアクションを実行します。

- SNMP トラップをマネージメントステーションに送る
- 1 分間に受信した IP オプションを含むパケットを破棄する

この攻撃検出のメカニズムは、スイッチの CPU での処理に影響を与えないため、一度に多くのポートに攻撃検出のための設定を行っても、スイッチのパフォーマンスには影響しません。

スイッチポートに、IP Options Attack を検出するように設定するには、SET DOS IPOPTION コマンド (190 ページ) を使います。

```
SET DOS IPOPTION PORT=5,7 STATE=ENABLE ↓
```

鍵作成・管理

本製品の暗号・圧縮 (ENCO = Encryption and Compression) モジュールについて説明します。ENCO モジュールは、本製品のセキュリティ機能の土台となるベースモジュールであり、SSL (Web 認証機能で使用) や SSH などの機能は本モジュールを利用して実現されます。

暗号アルゴリズム

ENCO モジュールは暗号アルゴリズムとして、RSA (鍵長 512 ~ 1536 ビット) をサポートしています。

RSA

RSA 鍵は SSH のサーバー鍵、ホスト鍵、認証鍵および SSL を使用した Web 認証時の公開鍵として使われます。

RSA 鍵を作成するには、CREATE ENCO KEY コマンド (92 ページ) の TYPE パラメーターに RSA を指定し、LENGTH パラメーターで鍵の長さ (bit) を指定します。有効範囲は 512 ~ 1536bit です。鍵は長いほど安全性が高まりますが、作成に時間がかかるようになります。現実的な鍵長は 1024bit とわれています。

```
CREATE ENCO KEY=2 TYPE=RSA LENGTH=1024 DESCRIPTION="my key pair" ↓
```

- ☞ RSA 鍵の作成には時間がかかります。鍵の作成が終わると「Key Generation completed with [Success]」と表示されます。
- ☞ RSA 鍵の作成を行うと、CPU に処理に負荷がかかるので、スイッチの動作に影響を与えます。RSA 鍵の作成は、本製品をネットワークに接続していない状態か、ネットワークの負荷が低いときに行うことをお勧めします。
- ☞ CREATE ENCO KEY コマンド (92 ページ) はコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。また、本コマンドで作成された鍵設定はユーザーがアップロード・ダウンロード可能な設定ファイルには保存されませんので、設定のバックアップを行う場合には、本製品からアップロードした設定ファイルとは別に設定コマンド自体をテキストファイルなどで保管してください。

作成した鍵ペアから公開鍵をファイルに書き出すには、CREATE ENCO KEY コマンド (92 ページ) の FILE パラメーターで書き出し先のファイル名 (拡張子は .key) を指定し、KEY パラメーターには作成した鍵ペアの番号を指定します。鍵ファイルのフォーマットは FORMAT パラメーターで指定します。

```
CREATE ENCO KEY=2 TYPE=rsa FILE=mypublic.key FORMAT=hex ↓
```

鍵ファイルから公開鍵を取り込むには、CREATE ENCO KEY コマンド (92 ページ) の FILE パラメーターに既存の鍵ファイル (拡張子は .key) を指定し、KEY パラメーターには未作成の (空いている) 鍵番号を指定します。鍵ファイルのフォーマットは FORMAT パラメーターで指定します。

```
CREATE ENCO KEY=3 TYPE=rsa FILE=hispublic.key FORMAT=hex ↓
```

作成した鍵の情報は SHOW ENCO KEY コマンド (255 ページ) で確認できます。

SHOW ENCO KEY ↓

```
# show enco key
```

ID	Algorithm	Length	Digest	Description
1	RSA-Private	512	E8DD94FB	my key pair1
2	RSA-Private	1024	FCFAD301	my key pair2
3	RSA-Private	1536	95631D26	my key pair3
4	RSA-Public	512	E8DD94FB	

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、サーバーやユーザーの認証機能によってなりすましを防ぐ効果もあります。

本製品は、SSH バージョン 1 (1.5) とバージョン 2 のサーバー機能を備えています (ともに IPv4 上のみ)。セッションの暗号アルゴリズムは 3DES/RC4/128bit AES/192bit AES/256bit AES、認証方式はパスワード認証をサポートしています。

- ☞ SSH を使うには、事前にローカル IP インターフェース (マネージメント VLAN インターフェース) の設定が必要です。詳しくは「IP」の「IP インターフェース」を参照してください。
- ☞ SSH サーバーを利用する場合は、マネージメントアクセスコントロールを有効にしないでください。マネージメントアクセスコントロールの有効時は、Management ACL の設定にかかわらず、本製品宛での SSH パケットをすべて破棄します。

SSH サーバー

ここでは、本製品を SSH サーバーとして動作させるための基本設定について説明します。SSH は IPv4 上で動作するため、IPv4 の設定までは完了しているものとします。

SSH サーバーの運用にあたっては、以下の点に注意してください。

- プロトコルバージョンは SSH バージョン 1 (1.5) とバージョン 2
 - 暗号アルゴリズムは 3DES/RC4/128bit AES/192bit AES/256bit AES
 - 認証方式はパスワード認証のみ
- ☞ SSH サーバー有効時にも Telnet サーバーは有効のままです。必要な場合は Telnet サーバーを無効にしてください。

以下に基本設定を示します。

パスワード認証

パスワード認証で SSH サーバーを運用するための最低限の設定を示します。なお、IPv4 の設定までは済んでいるものとします。

1. SSH サーバーのホスト鍵 (Host Key) を鍵番号「1」として作成します。推奨鍵長は 1024 ビットです。

```
CREATE ENCO KEY=1 TYPE=RSA LENGTH=1024 DESCRIPTION=host ↓
```

- ☞ RSA 鍵の作成には時間がかかります。「Key Generation completed with [Success]」と表示されるまで待ってから、次の手順に進んでください。また、RSA 鍵の作成を行うと、CPU に処理に負荷がかかるので、スイッチの動作に影響を与えます。RSA 鍵の作成は、本製品をネットワークに接続していない状態か、ネットワークの負荷が低いときに行うことをお勧めします。

✎ CREATE ENCO KEY コマンド (92 ページ) はコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。また、本コマンドで作成された鍵設定はユーザーがアップロード・ダウンロード可能な設定ファイルには保存されませんので、設定のバックアップを行う場合には、本製品からアップロードした設定ファイルとは別に設定コマンド自体をテキストファイルなどで保管してください。

✎ 鍵番号は 0~65535 の範囲で自由に選択できます。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よいでしょう。このコメントは SHOW ENCO KEY コマンド (255 ページ) で表示されます。

- SSH サーバーのサーバー鍵 (Server Key) を鍵番号「2」として作成します。サーバー鍵は最小長 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。一般的な長さは 768 バイトです。

```
CREATE ENCO KEY=2 TYPE=RSA LENGTH=768 DESCRIPTION=server ↵
```

✎ RSA 鍵の作成には時間がかかります。「Key Generation completed with [Success]」と表示されるまで待ってから、次の手順に進んでください。

- SSH サーバーを有効化します。このとき、手順 1、2 で作成したホスト鍵とサーバー鍵の番号を指定します。

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

SSH 経由でのログイン失敗が 50 回連続した場合、下記のようなログが出力され、SSH サーバーが自動的に無効化されます。SSH サーバーを再度有効化するには、手動で ENABLE SSH SERVER コマンド (159 ページ) を実行してください。なお、SSH 経由のログインには、SET USERCONFIG コマンド (229 ページ) の LOGINFAIL は適用されません。

```
I 09/22/11 11:52:02 ssh:  SSH server disabled
W 09/22/11 11:52:02 system:  SSH server disabled.  Continuous invalid
login attempts.  Possible server attack from 172.17.20.33
```

作成した鍵の情報は SHOW ENCO KEY コマンド (255 ページ) で確認できます。

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

デフォルトではサーバー鍵の自動更新は行われません。自動更新を行うには、ENABLE SSH SERVER コマンド (159 ページ) か SET SSH SERVER コマンド (218 ページ) の EXPIRYTIME パラメーターで 0 以外の更新間隔 (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、SSH サーバーを有効化するときに、5 時間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=5 ↵
```

サーバーを有効化した後で設定を変更するには、SET SSH SERVER コマンド (218 ページ) を使います。

```
SET SSH SERVER EXPIRYTIME=5 ↓
```

SSH サーバーの状態は SHOW SSH コマンド (299 ページ) で確認できます。

```
SHOW SSH ↓
```

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 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

PKI

本製品の PKI (Public Key Infrastructure) モジュールについて説明します。PKI モジュールを使用すると、SSL を使用した Web 認証が利用できるようになります。

PKI とは

PKI (Public Key Infrastructure) は、公開鍵暗号を安心して利用するための基盤技術です。公開鍵暗号の信頼性は、使用する公開鍵が本当に対象者のものであるかに依存しています。PKI システムでは、認証局 (CA) が発行する公開鍵証明書により、公開鍵とその所有者の関係を証明する仕組みが提供されています。本製品では ITU-T X.509 勧告の定める公開鍵証明書を利用した PKI システムを使用することができます。

基本設定

PKI の基本的な設定方法を示します。なお、公開鍵については「鍵作成・管理」をご覧ください。

自己署名した公開鍵証明書 my-cert を作成します。KEYPAIR パラメーターには使用する公開鍵の番号を指定し、SERIALNUMBER パラメーターには任意の数字を指定します。

```
CREATE PKI CERTIFICATE=my-cert KEYPAIR=0 SERIALNUMBER=0 ↵
```

本コマンドを実行すると、本製品のファイルシステム上に公開鍵証明書 my-cert.cer が発行されます。

- このコマンドはコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。また、本コマンドで作成された公開鍵証明書は設定ファイルには含まれませんのでご注意ください。

本製品の証明書データベースに自己署名した公開鍵証明書 my-cert.cer を登録します。LOCATION パラメーターには本製品のファイルシステム上に存在する公開鍵証明書の名前を指定し、TYPE パラメーターには自身が発行した証明書であることを示す self を指定します。

```
ADD PKI CERTIFICATE="My Certificate" LOCATION=my-cert.cer TYPE=SELF ↵
```

公開鍵証明書の発行要求ファイル enroll を作成します。第三者機関へ公開鍵証明書の発行を依頼する際は本コマンドで発行要求ファイル (拡張子.csr) を作成し、提出します。KEYPAIR パラメーターには使用する公開鍵の番号を指定し、FORMAT パラメーターには発行要求ファイルのフォーマットを指定します。

```
CREATE PKI ENROLLMENTREQUEST="enroll" KEYPAIR=0 FORMAT=pem ↵
```

本コマンドを実行すると、本製品のファイルシステム上に発行要求ファイル enroll.csr が発行されます。

- このコマンドはコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。また、本コマンドで作成された証明書要求ファイルは設定ファイルには含まれませんのでご注意ください。

証明書データベースに登録されている証明書の情報は SHOW PKI CERTIFICATE コマンド (272 ページ) で確認できます。

SHOW PKI CERTIFICATE ↓

```
# show pki certificate

Certificate Database:
Name                State      MTrust  Type  Source
-----
CA's Certificate    Trusted   True    CA    Command
EE's Certificate    Trusted   True    EE    Command
My Certificate      Trusted   True    Self  Command
-----
```

エンハンススタッキング

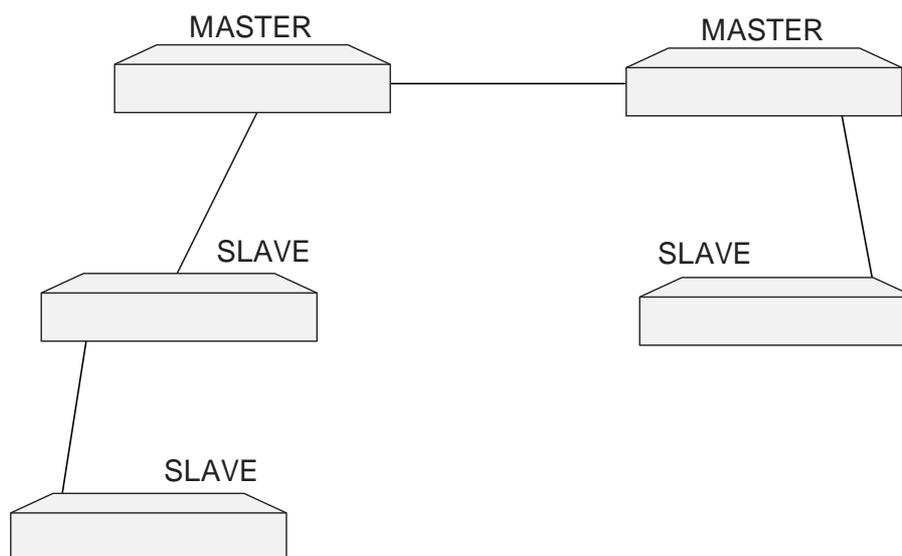
エンハンススタッキングは、ネットワーク内に存在する複数のスイッチを、1 台のスイッチから一括して制御するための機能です。

エンハンススタッキング機能には、次の特長があります。

- マスタースイッチに設定された IP アドレスを、エンハンススタッキンググループで共有可能
- マスタースイッチからスレーブスイッチにログイン可能
- マスタースイッチからスレーブスイッチに、TFTP によるファームウェアや設定ファイルのダウンロードが可能
- ネットワークに新しく追加した本製品に設定をすることなく、マスタースイッチから制御可能（デフォルトで、スレーブに設定されている）

エンハンススタッキンググループは、マスターとスレーブと呼ばれるスイッチで構成されます。

マスタースイッチは、他のスイッチを制御するために使用するスイッチです。スレーブスイッチは、マスタースイッチから制御可能なスイッチです。



エンハンススタッキング機能の仕様は、以下のようになっています。

- マスタースイッチは、最大 8 台までのスレーブスイッチとマスタースイッチが制御可能
- エンハンススタッキンググループ内では、最低 1 台のマスタースイッチが必要であるが、マスタースイッチを複数台設定することも可能
- エンハンススタッキンググループは、同一サブネット内で形成する
- スレーブスイッチは複数のマスタースイッチから制御可能であるが、同時には制御できない
- エンハンススタッキンググループ内に、エンハンススタッキング機能を持たないスイッチ（UNAVAILABLE スイッチ）が介在していても、本機能は使用可能

エンハンススタッキングを使用する場合、マスタースイッチとスレーブスイッチを接続するには、下記のとおり接続してください。

- スレーブスイッチ側は、Default_VLAN に所属するポートにマスタースイッチを接続する。Default_VLAN 以外の VLAN に所属するポートに接続した場合は、IP インターフェースを作成して IP アドレスを設定しなければならない。
- マスタースイッチ側は、ローカルインターフェースに設定した VLAN に所属するポートにスレーブスイッチを接続する。

☞ SNMPv3 を使用して、エンハンススタッキンググループのスレーブスイッチにアクセスすることはできません。

☞ マスタースイッチからスレーブスイッチに SNMP 経由でエンハンススタッキング接続している最中に、他のスイッチから該当のマスタースイッチに Telnet や SNMP による接続を行わないでください。

基本設定

エンハンススタッキングの設定は、次の手順で行います。ここでは、スイッチ A をマスタースイッチとし、1 つのグループを作成します。

1. マスタースイッチを設定します。SET SWITCH STACKMODE コマンド (220 ページ) を使って、マスタースイッチを指定します。

```
SET SWITCH STACKMODE=MASTER ↓
```

2. マスタースイッチに IP アドレスを設定します。

```
ADD IP INTERFACE=vlan1 IP=192.168.1.10 MASK=255.255.255.0 ↓
```

3. Default_VLAN をローカルインターフェースとして指定します。

```
SET IP LOCAL INTERFACE=vlan1 ↓
```

4. エンハンススタッキング機能を有効にたくないスイッチがある場合は、SET SWITCH STACKMODE コマンド (220 ページ) を使って指定します。

```
SET SWITCH STACKMODE=UNAVAILABLE ↓
```

設定は以上です。

エンハンススタッキンググループに属するスイッチを表示するには、SHOW REMOTELIST コマンド (276 ページ) を使います。

```
SHOW REMOTELIST ↓
```

マスタースイッチから、制御したいスイッチに接続するには、ACCESS SWITCH コマンド (78 ページ) を使います。

```
ACCESS SWITCH NUMBER=1 ↓
```

マスタースイッチからスレーブスイッチへのファームウェアファイルと設定ファイル

UPLOAD コマンド (309 ページ) で、METHOD に REMOTESWITCH を指定すると、現在稼働中のファームウェアおよび設定ファイルを、マスタースイッチからスレーブスイッチに転送することができます。

マスタースイッチからスレーブスイッチにファームウェアファイルを転送する場合は、SRCFILE/FILE に APPBLOCK を指定します。

```
UPLOAD METHOD=REMOTESWITCH FILE=APPBLOCK SWITCHLIST=1 ↓
```

マスタースイッチからスレーブスイッチに、現在の起動時設定ファイルを転送する場合は、SRCFILE/FILE に SWITCHCFG を指定します。

```
UPLOAD METHOD=REMOTESWITCH FILE=SWITCHCFG SWITCHLIST=1 ↓
```

- ✎ マスタースイッチからスレーブスイッチに起動時設定ファイルを転送すると、スレーブスイッチは再起動し、IP アドレスおよびスタックモードの設定以外は、書き換えられます。

マスタースイッチからスレーブスイッチに、フラッシュメモリー内の設定ファイルを転送する場合は、SRCFILE/FILE にファイル名を指定します。

```
UPLOAD METHOD=REMOTESWITCH FILE=test.cfg SWITCHLIST=1 ↓
```

- ✎ マスタースイッチからスレーブスイッチに設定ファイルを転送すると、スレーブスイッチは再起動し、すべての設定が書き換えられますが、ステータスの設定は転送されません。

コマンドリファレンス編

機能別コマンド索引

システム

CLEAR SCREEN	89
DELETE EXCEPTIONLOG	114
EXIT	163
HELP	165
LOGOFF	168
LOGOUT	169
QUIT	179
RESTART	183
SET SYSTEM CONTACT	221
SET SYSTEM DISTINGUISHEDNAME	222
SET SYSTEM LOCATION	223
SET SYSTEM NAME	224
SET TIME	226
SHOW BUFFER	233
SHOW CPU	237
SHOW DEBUG	240
SHOW EXCEPTIONLOG	256
SHOW SYSTEM	301
SHOW TIME	304

記憶装置とファイルシステム

COPY	90
DELETE FILE	115
FORMAT DEVICE	164
RENAME	180
SHOW FILE	257
SHOW FLASH	259

コンフィグレーション

CREATE CONFIG	91
SAVE CONFIGURATION	184
SET CONFIG	188
SHOW CONFIG	235

ユーザー認証データベース

ADD USER	87
DELETE USER	122
DISABLE USER	147

ENABLE USER	162
PURGE USER	178
RESET USER	181
RESET USERCONFIG	182
SET PASSWORD	200
SET USER	227
SET USERCONFIG	229
SHOW USER	305
SHOW USERCONFIG	307
認証サーバー	
ADD RADIUSSERVER	82
DELETE RADIUSSERVER	118
DISABLE AUTHENTICATION	134
DISABLE RADIUSACCOUNTING	139
ENABLE AUTHENTICATION	148
ENABLE RADIUSACCOUNTING	153
PURGE AUTHENTICATION	170
SET AUTHENTICATION	187
SET RADIUSACCOUNTING	202
SET RADIUSSERVER	203
SHOW AUTHENTICATION	231
SHOW RADIUSACCOUNTING	275
アップロード・ダウンロード	
LOAD	166
UPLOAD	309
ログ	
ADD LOG OUTPUT	79
CREATE LOG OUTPUT	94
DESTROY LOG OUTPUT	124
DISABLE LOG	136
DISABLE LOG OUTPUT	137
ENABLE LOG	150
ENABLE LOG OUTPUT	151
PURGE LOG	171
SAVE LOG	185
SET LOG FULLACTION	197
SET LOG OUTPUT	198
SHOW LOG	264
SHOW LOG OUTPUT	267
SHOW LOG STATUS	269

SNMP

ADD SNMP COMMUNITY	84
ADD SNMPV3 USER	85
CREATE SNMP COMMUNITY	100
CREATE SNMPV3 ACCESS	102
CREATE SNMPV3 COMMUNITY	104
CREATE SNMPV3 GROUP	106
CREATE SNMPV3 NOTIFY	107
CREATE SNMPV3 TARGETADDR	108
CREATE SNMPV3 TARGETPARAMS	110
CREATE SNMPV3 VIEW	112
DELETE SNMP COMMUNITY	119
DELETE SNMPV3 USER	120
DESTROY SNMP COMMUNITY	126
DESTROY SNMPV3 ACCESS	127
DESTROY SNMPV3 COMMUNITY	128
DESTROY SNMPV3 GROUP	129
DESTROY SNMPV3 NOTIFY	130
DESTROY SNMPV3 TARGETADDR	131
DESTROY SNMPV3 TARGETPARAMS	132
DESTROY SNMPV3 VIEW	133
DISABLE INTERFACE LINKTRAP	135
DISABLE SNMP	140
DISABLE SNMP COMMUNITY	141
DISABLE SNMP TRAP	142
ENABLE INTERFACE LINKTRAP	149
ENABLE SNMP	154
ENABLE SNMP COMMUNITY	155
ENABLE SNMP TRAP	156
PURGE SNMPV3 ACCESS	173
PURGE SNMPV3 NOTIFY	174
PURGE SNMPV3 TARGETADDR	175
PURGE SNMPV3 VIEW	176
SET SNMP COMMUNITY	204
SET SNMPV3 ACCESS	205
SET SNMPV3 COMMUNITY	206
SET SNMPV3 GROUP	208
SET SNMPV3 NOTIFY	209
SET SNMPV3 TARGETADDR	210
SET SNMPV3 TARGETPARAMS	212
SET SNMPV3 USER	214
SET SNMPV3 VIEW	215

SHOW INTERFACE	260
SHOW SNMP	277
SHOW SNMP COMMUNITY	278
SHOW SNMP TRAP	280
SHOW SNMPV3 ACCESS	282
SHOW SNMPV3 COMMUNITY	284
SHOW SNMPV3 ENGINEID	286
SHOW SNMPV3 GROUP	287
SHOW SNMPV3 NOTIFY	289
SHOW SNMPV3 TARGETADDR	290
SHOW SNMPV3 TARGETPARAMS	292
SHOW SNMPV3 USER	294
SHOW SNMPV3 VIEW	296
SNTP	
ADD SNTP PEER	86
DELETE SNTP PEER	121
DISABLE SNTP	144
ENABLE SNTP	158
PURGE SNTP	177
SET SNTP	216
SHOW SNTP	298
非同期ポート	
SET ASYN	186
SET SWITCH CONSOLETIMER	219
SHOW ASYN	230
ターミナルサービス	
DISABLE TELNET	146
ENABLE TELNET	161
SET TELNET	225
マネージメントアクセスコントロール	
ADD MGMTACL	80
CREATE MGMTACL	96
DELETE MGMTACL	116
DESTROY MGMTACL	125
DISABLE MGMTACL	138
ENABLE MGMTACL	152
PURGE MGMTACL	172
SET MGMTACL	199
SHOW MGMTACL	270

攻撃検出

SET DOS	189
SET DOS IPOPTION	190
SET DOS LAND	191
SET DOS PINGOFDEATH	192
SET DOS SMURF	193
SET DOS SYNFLOOD	194
SET DOS TEARDROP	195
SHOW DOS	241
SHOW DOS IPOPTION	243
SHOW DOS LAND	245
SHOW DOS PINGOFDEATH	247
SHOW DOS SMURF	249
SHOW DOS SYNFLOOD	251
SHOW DOS TEARDROP	253
鍵作成・管理	
CREATE ENCO KEY	92
DESTROY ENCO KEY	123
SET ENCO KEY	196
SHOW ENCO KEY	255
Secure Shell	
DISABLE SSH SERVER	145
ENABLE SSH SERVER	159
SET SSH SERVER	218
SHOW SSH	299
PKI	
ADD PKI CERTIFICATE	81
CREATE PKI CERTIFICATE	98
CREATE PKI ENROLLMENTREQUEST	99
DELETE PKI CERTIFICATE	117
SET PKI CERTIFICATE	201
SHOW PKI CERTIFICATE	272
エンハンススタッキング	
ACCESS SWITCH	78
SET SWITCH STACKMODE	220
SHOW REMOTELIST	276

ACCESS SWITCH

カテゴリー：運用・管理 / エンハンススタッキング

ACCESS SWITCH [NUMBER=*index*] [MACADDRESS=*macadd*]

index: リスト番号

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

解説

MASTER スイッチから制御可能なスイッチに接続する。

パラメーター

NUMBER SHOW REMOTELIST コマンドで表示される、「Num」に表示された番号を指定する。

MACADDRESS 対象スイッチの MAC アドレスを指定する。

例

リスト番号 1 のスイッチに接続する。

```
ACCESS SWITCH NUMBER=1
```

関連コマンド

SET SWITCH STACKMODE (220 ページ)

ADD LOG OUTPUT

カテゴリー：運用・管理 / ログ

```
ADD LOG OUTPUT=output-id MODULE={ALL|module-list} SEVERITY={ALL|  
severity-list}
```

output-id: ログ出力 ID (2~20)

module-list: モジュール名 (カンマを使った複数指定も可)

severity-list: ログレベル (E,W,I で指定。カンマを使った複数指定も可)

解説

ログ出力先に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。2~20 の任意の番号を指定する。

MODULE モジュール名。

SEVERITY メッセージのログレベル。

例

VLAN のログだけを出力するように、ログ出力先定義「3」に設定する。

```
ADD LOG OUTPUT=3 MODULE=VLAN SEVERITY=ALL
```

関連コマンド

CREATE LOG OUTPUT (94 ページ)

SET LOG OUTPUT (198 ページ)

SHOW LOG OUTPUT (267 ページ)

ADD MGMTACL

カテゴリー：運用・管理 / マネージメントアクセスコントロール

```
ADD MGMTACL ID=1..256 APPLICATION={TELNET|PING|ALL}
```

解説

Management ACL (マネージメントアクセスコントロールリスト) のエントリーに、許可するパケットの種類を追加する。

パラメーター

ID エントリー番号

APPLICATION アクセスを許可するパケットの種類。指定値については、CREATE MGMTACL コマンドのページに掲載されている表を参照

例

エントリー「10」で許可するパケットの種類に「PING」を追加する。

```
ADD MGMTACL ID=10 APPLICATION=PING
```

関連コマンド

DELETE MGMTACL (116 ページ)

SET MGMTACL (199 ページ)

SHOW MGMTACL (270 ページ)

ADD PKI CERTIFICATE

カテゴリー：運用・管理 / PKI

ADD PKI CERTIFICATE=string LOCATION=filename [TRUSTED={YES|NO|ON|OFF|TRUE|FALSE}] [TYPE={CA|EE|SELF}]

string: 証明書の名前 (1~24 文字。使用可能な文字は半角英数字 (大文字・小文字を区別する)、半角記号 (# \$ % & ' () ~ | - ^ \ @ ' { + * } [; :] , . / -)、文字列に半角空白、!= を含む場合は、前後をダブルクォート (") で囲む必要がある。)
filename: ファイル名 (1~28 文字。英数字と記号 (# \$ % & ' () ~ - ^ \ @ ' { + } -) が使用可能。拡張子は.cer)

解説

証明書データベースに公開鍵証明書を登録する。

パラメーター

CERTIFICATE 証明書データベースで表示される証明書の名前。

LOCATION 登録する証明書ファイル (.cer) の名前。

TRUSTED 登録する証明書を自動的に信頼するかどうか。YES/ON/TRUE、NO/OFF/FALSE で設定する。デフォルトは YES/ON/TRUE。

TYPE 登録する証明書のタイプを指定する。CA (認証局が発行した証明書)、EE (認証局以外が発行した証明書)、SELF (本製品が発行した証明書) から選択。デフォルトは EE。

関連コマンド

CREATE PKI CERTIFICATE (98 ページ)

CREATE PKI ENROLLMENTREQUEST (99 ページ)

DELETE PKI CERTIFICATE (117 ページ)

SET PKI CERTIFICATE (201 ページ)

SHOW PKI CERTIFICATE (272 ページ)

ADD RADIUSERVER

カテゴリ：運用・管理 / 認証サーバー

```
ADD RADIUSERVER {SERVER|IPADDRESS}=ipadd ORDER=1..3 [SECRET=secret]
  [PORT=port] [ACCPORT=port] [LOCAL={vlanname|1..4094|NONE}]
```

ipadd: IP アドレス

secret: 共有パスワード (1~39 文字。使用可能な文字は半角英数字、半角記号 (!#\$%&'()=~-^`@\`{+*}{;:] ,.-<>?)、大文字・小文字を区別する。文字列に半角空白、=<>!?を含む場合は、前後をダブルクォート(")で囲む必要がある。文字列中にダブルクォートを含んではならない)

port: UDP ポート番号 (1~65535)

vlanname: VLAN 名 (1~15 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

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。

パラメーター

SERVER/IPADDRESS RADIUS サーバーの IP アドレス。

ORDER RADIUS サーバーの優先順位を 1~3 の範囲で指定する。

SECRET RADIUS サーバー個別のパスワード。

PORT RADIUS サーバーの認証用 UDP ポート番号。デフォルトは 1812 番。

ACCPORT RADIUS サーバーのアカウント用 UDP ポート番号。デフォルトは 1813 番。

LOCAL RADIUS Access-Request の始点 IP アドレスとなるインターフェースを指定する。VLAN 名、VID または、NONE。デフォルトは NONE。NONE の場合、RADIUS サーバーへの送信先の VLAN インターフェースの IP が始点 IP アドレスとなる。

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」、優先順位は 1、認証用ポートは 1812、アカウント用ポートは 1813 番

```
ADD RADIUSERVER SERVER=192.168.10.5 ORDER=1 SECRET=pOR8Gd PORT=1812
  ACCPORT=1813
```

備考・注意事項

RADIUSERVER は、RADIUS のみでも入力可能。

RADIUS サーバーの設定は、3 つまで独立して行うことができるが、アカウントサーバーの設定は 1 つで、すべての RADIUS サーバーで共有される。このため、ここで指定したアカウント用 UDP ポー

ト番号の設定は、すべての RADIUS サーバーで共通となる。

関連コマンド

DELETE RADIUSSERVER (118 ページ)

SET RADIUSSERVER (203 ページ)

SHOW AUTHENTICATION (231 ページ)

ADD SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

ADD SNMP COMMUNITY=community [TRAPHOST=*ipadd*] [MANAGER=*ipadd*]

community: SNMP コミュニティ名 (1~32 文字。英数字が使用可能。大文字・小文字を区別する。)(ダブルクォー
ト) [] (スクエアブラケット) \ (バックスラッシュ、円マーク) 半角スペースは使用できない)

ipadd: IP アドレス

解説

SNMP コミュニティ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 コミュニティ名。

TRAPHOST 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。トラップはここで指定したホストにだけ送信される。

MANAGER SNMP オペレーションを許可する管理ステーション。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 リクエストには応答しない。ただし、SNMP コミュニティ
の OPEN プロパティが 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 リクエストに応答する。

例

SNMP コミュニティ「public」に管理ステーションを追加する。

```
ADD SNMP COMMUNITY=public MANAGER=192.168.20.5
```

関連コマンド

CREATE SNMP COMMUNITY (100 ページ)
DELETE SNMP COMMUNITY (119 ページ)
DESTROY SNMP COMMUNITY (126 ページ)
DISABLE SNMP COMMUNITY (141 ページ)
ENABLE SNMP COMMUNITY (155 ページ)
SET SNMP COMMUNITY (204 ページ)
SHOW SNMP COMMUNITY (278 ページ)

ADD SNMPV3 USER

カテゴリ：運用・管理 / SNMP

```
ADD SNMPV3 USER=username [AUTHENTICATION={MD5|SHA}]
    [AUTHPASSWORD=password] [PRIVPASSWORD=password] [STORAGETYPE={VOLATILE|
NONVOLATILE}]
```

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

password: パスワード (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) ユーザーを作成する。

パラメーター

USER SNMP ユーザー名。

AUTHENTICATION 認証プロトコル。MD5、SHA から選択する。このパラメーターを指定しないと、NONE (認証なし) になる。

AUTHPASSWORD 認証パスワード。AUTHENTICATION に、MD5 か SHA を指定した場合の必須パラメーター。

PRIVPASSWORD 暗号化パスワード。暗号化パスワードを指定すると、暗号化あり (DES) になる。AUTHENTICATION が NONE (認証なし) の場合は、指定できない。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP ユーザー「systemadmin24」を追加する。

```
ADD SNMPV3 USER=systemadmin24 AUTHENTICATION=MD5 AUTHPASSWORD=kumanomi
    PRIVPASSWORD=imonamuk STORAGETYPE=nonvolatile
```

関連コマンド

DELETE SNMPV3 USER (120 ページ)

SET SNMPV3 USER (214 ページ)

SHOW SNMPV3 USER (294 ページ)

ADD SNTP PEER

カテゴリー：運用・管理 / SNTP

ADD SNTP PEER=*ipadd*

ipadd: IP アドレス

解説

時刻同期をとる SNTP サーバーの IP アドレスを設定する。SNTP サーバーは 1 つしか設定できない。

パラメーター

PEER SNTP サーバーの IP アドレス。

例

SNTP 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 SNTP
ADD SNTP PEER=192.168.10.5
SET SNTP UTCOFFSET=9
```

関連コマンド

DELETE SNTP PEER (121 ページ)

ADD USER

カテゴリ：運用・管理 / ユーザー認証データベース

```
ADD USER=login-name PASSWORD={password|NONE} [DESCRIPTION={string|NONE}]
  [PRIVILEGE={USER|MANAGER}] [SESSIONTYPE={CONSOLE|TELNET|SSH|
  ENAHNCEDSTACKING|ALL}]
```

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)

password: パスワード (1~32 文字。使用可能な文字は半角英数字、半角記号 (!#\$%&'()=~|^@\'+*}{;:] ,.-<>?)。大文字・小文字を区別する。文字列に半角空白、=<>!?を含む場合は、前後をダブルクォート(")で囲む必要がある。文字列中にダブルクォートを含んではならない。)

string: 文字列 (1~24 文字。使用可能な文字は半角英数字、半角記号 (!#\$%&'()=~|^@\'+*}{;:] ,.-<>?)。文字列に半角空白、=<>!?を含む場合は、前後をダブルクォート(")で囲む必要がある。文字列中にダブルクォートを含んではならない。)

解説

認証データベースにユーザーを追加する。

作成できるユーザー数は16。デフォルトで登録されている「manager」と「operator」を含めて、システム全体で18ユーザーまで登録可能。

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。パスワードを設定しない場合はNONEを指定する。

DESCRIPTION ユーザーに関するコメントを設定する。DESCRIPTIONを設定しない場合はNONEを指定する。

PRIVILEGE ユーザーレベル。一般ユーザー (USER)、管理者 (MANAGER) から選択する。省略時はUSERレベル。

SESSIONTYPE このユーザーがログインできるセッションタイプを指定する。CONSOLE(シリアルポート)、TELNET、SSH、ENAHNCEDSTACKING から選択する。ALLを指定した場合はいずれのセッションタイプからもログインできる。複数のセッションタイプを指定する場合は、「,」区切りで指定する。

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=il0vEba7 PRIVILEGE=MANAGER
```

備考・注意事項

パスワードをなしに設定 (PASSWORD=NONE) するときは、SET USERCONFIG コマンドの MIN-PWDLEN パラメーターを 0 に設定する。

ユーザー情報、パスワードは、CREATE CONFIG コマンドや SAVE CONFIGURATION コマンドを実行することにより設定ファイルに保存される。

関連コマンド

DELETE USER (122 ページ)

DISABLE USER (147 ページ)

ENABLE USER (162 ページ)

PURGE USER (178 ページ)

RESET USER (181 ページ)

SET USER (227 ページ)

SHOW USER (305 ページ)

CLEAR SCREEN

カテゴリー：運用・管理 / システム

CLEAR SCREEN

解説

スクリーン上の表示をクリアする。

COPY

カテゴリー：運用・管理 / 記憶装置とファイルシステム

COPY [*device:*] **filename1.ext** [*device:*] **filename2.ext**

device: ファイルが記憶されている媒体。flash を指定

filename1.ext: コピー元ファイル名

filename2.ext: コピー先ファイル名

解説

ファイルをコピーする。

関連コマンド

LOAD (166 ページ)

SHOW FILE (257 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*

filename: ファイル名 (1~28 文字。英数字と記号 (` ' @ # \$ % ^ & () _ - { }) が使用可能。拡張子は.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」。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。

入力・出力・画面例

```
# create config=kumanomi.cfg
Creating configuration file "kumanomi.cfg" ..... done!
```

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。

```
CREATE CONFIG=basic.cfg
SET CONFIG=basic.cfg
```

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。

ファイルが存在する場合は、確認のメッセージが表示される。Y キーを押して、Yes を選択するとファイルは上書きされ、N キーを押して、No を選択するとファイルの上書きは行われない。

関連コマンド

```
RESTART ( 183 ページ )
SET CONFIG ( 188 ページ )
SHOW CONFIG ( 235 ページ )
```

CREATE ENCO KEY

カテゴリー：運用・管理 / 鍵作成・管理

```
CREATE ENCO KEY=key-id TYPE=RSA [LENGTH=512..1536] [DESCRIPTION=string]
```

```
CREATE ENCO KEY=key-id TYPE=RSA [DESCRIPTION=string] [FILE=filename]
  [FORMAT={HEX|SSH|SSH2}]
```

key-id: 鍵番号 (0~65535)

string: 文字列 (1~127 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む)

filename: ファイル名 (1~59 文字。拡張子は.key)

解説

RSA 鍵ペアの作成、公開鍵の書き出し、公開鍵の取り込みを実行する。

作成または取り込んだ鍵の情報は、CREATE CONFIG コマンドで作成する設定ファイルとは別個に、フラッシュメモリー上に保存される。

パラメーター

KEY 鍵番号。

TYPE 鍵の種類。サポートしているのは RSA (RSA 公開鍵) のみ。rsa を指定した場合は、LENGTH あるいは FILE パラメーターが必要。FILE を指定した場合は、KEY で指定した番号の鍵がすでに存在しているかどうかによって動作が異なる。鍵が存在していない場合は、指定ファイルから公開鍵を取り込む。KEY で指定した鍵がすでに存在するときは、指定ファイルに公開鍵を書き出す。FILE を指定せずに LENGTH だけを指定した場合は、指定した長さの RSA 公開鍵ペアがランダムに作成される。

LENGTH 作成する鍵の長さ。RSA 公開鍵の場合はビットで指定する。RSA 公開鍵の長さは 32 の倍数でなくてはならず、有効な長さの範囲は 512~1536 ビット。SSH で使用する鍵の長さは 512~1536 ビットとする。

DESCRIPTION 鍵の説明文 (コメント)

FILE RSA 公開鍵ファイル名。拡張子は.key。本パラメーター指定時は、鍵ファイルの形式を FORMAT パラメーターで指定する必要がある。KEY パラメーターで指定した RSA 公開鍵ペアが存在し、FILE で指定したファイルが存在していない場合は、指定ファイルに公開鍵が書き出される。KEY パラメーターで指定した鍵が存在せず、FILE で指定したファイルが存在している場合は、指定ファイルから公開鍵がインポートされる。

FORMAT RSA 公開鍵ファイルのフォーマット。サポートしているのは HEX (16 進フォーマット。他の機器と鍵を交換する場合に使用) と SSH/SSH2 (Secure Shell 用フォーマット)。FILE 指定時の必須パラメーター。デフォルトは、HEX。

入力・出力・画面例

```
#create enco key=1 type=rsa length=1024 description=host
```

```
This step will take approximately 2 minutes to complete.
During this time the switch CPU will be very busy which might
impact its normal operation!
Key generation will take some time. Please wait...
Key Generation completed with [Success]
```

例

RSA 公開鍵ペアを作成する。鍵長の有効範囲は 512 ~ 1536 ビット。

```
CREATE ENCO KEY=3 TYPE=RSA LENGTH=1024 DESCRIPTION="my key pair"
```

作成した RSA 鍵ペアの公開鍵を SSH フォーマットでファイル mypublic.key に書き出す。

```
CREATE ENCO KEY=3 TYPE=RSA FILE=mypublic.key FORMAT=SSH
```

他者から入手した公開鍵ファイル hispub.key を鍵番号「4」としてインポートする。

```
CREATE ENCO KEY=4 TYPE=RSA FILE=hispub.key FORMAT=SSH DESCRIPTION="His
public key"
```

備考・注意事項

コンソールから入力したときだけ有効なコマンド。設定ファイルにこのコマンドを記述しておいても無効。また、本コマンドで作成された鍵設定はユーザーがアップロード・ダウンロード可能な設定ファイルには保存されないため、設定のバックアップを行う場合には、本製品からアップロードした設定ファイルとは別に設定コマンド自体をテキストファイルなどで保管する必要がある。

関連コマンド

DESTROY ENCO KEY (123 ページ)

SET ENCO KEY (196 ページ)

SHOW ENCO KEY (255 ページ)

CREATE LOG OUTPUT

カテゴリー：運用・管理 / ログ

```
CREATE LOG OUTPUT=output-id DESTINATION=SYSLOG SERVER=ipadd
  [FACILITY={DEFAULT|LOCAL1|LOCAL2|LOCAL3|LOCAL4|LOCAL5|LOCAL6|LOCAL7}]
  [SYSLOGFORMAT={NORMAL|EXTENDED}]
```

output-id: ログ出力 ID (2~20)

ipadd: IP アドレス

解説

syslog サーバーの設定および syslog サーバーの出力先を定義する。

出力先の定義後は、ADD LOG OUTPUT コマンドでログ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。2~20 の任意の番号を指定する (0 は PERMANENT、1 は TEMPORARY に割り当て済み)。

DESTINATION ログメッセージの出力先。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) を指定する。

SERVER メッセージの転送先 IP アドレスを指定する。syslog サーバー (UDP 514 番) を指定する。

FACILITY syslog メッセージのファシリティコードを指定する。DEFAULT の場合は、既定のマッピング (解説編参照) にしたがって各メッセージのファシリティコードが決まる。LOCAL1~LOCAL7 を指定した場合は、本出力先宛てのすべての syslog メッセージで指定したファシリティコードが使用される。デフォルトは DEFAULT (既定のマッピングによってファシリティコードを決定)。

SYSLOGFORMAT syslog メッセージのフォーマット。EXTENDED (時刻情報とシステム名 (sysName) が付加される) と NORMAL (既存のフォーマット) から選択する。デフォルトは EXTENDED。

例

すべてのログを syslog サーバー 192.168.1.2 に送る

```
CREATE LOG OUTPUT=2 DESTINATION=SYSLOG SERVER=192.168.1.2
ADD LOG OUTPUT=2 MODULE=ALL SEVERITY=ALL
```

備考・注意事項

syslog を使うには、事前にローカル IP インターフェース (マネージメント VLAN インターフェース) の設

定が必要。詳しくは「IP」の「IP インターフェース」を参照のこと。

関連コマンド

ADD LOG OUTPUT (79 ページ)

DESTROY LOG OUTPUT (124 ページ)

DISABLE LOG OUTPUT (137 ページ)

ENABLE LOG OUTPUT (151 ページ)

SET LOG OUTPUT (198 ページ)

CREATE MGMTACL

カテゴリー：運用・管理 / マネージメントアクセスコントロール

```
CREATE MGMTACL ID=1..256 [PORTLIST={port-list|ALL}] [IPADDRESS=ipadd]
[MASK=ipadd] [APPLICATION={TELNET|PING|ALL}]
```

ipadd: IP アドレス

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

Management ACL (マネージメントアクセスコントロールリスト) にアクセス制御エントリーを追加する。マネージメントアクセスコントロールの有効時は、受信スイッチポート、始点 IP アドレス、アプリケーションがいずれのエントリーに合致する本体宛て IP パケットだけを受け入れ、その他のパケットは破棄する。

パラメーター

ID エントリー番号

PORTLIST 受信スイッチポート番号。省略した場合は ALL となる

IPADDRESS 始点 IP アドレス。省略した場合は「0.0.0.0」となる

MASK IPADDRESS パラメーターで指定した IP アドレスのマスク (IP アドレスのどの部分をフィルタリング条件として有効にするか) を指定する。特定の機器の IP アドレスだけを指定したい場合は「255.255.255.255」を指定する。また、192.168.20.0/24 のようなサブネットを指定したい場合は「255.255.255.0」を指定する。省略した場合は「0.0.0.0」となる

APPLICATION アクセスを許可するパケットの種類。指定値については別表を参照。省略時は ALL (本機能の適用対象となるすべてのパケット) となる

	Telnet	ICMP(Echo-Req)	ICMP(Echo-Req 以外)	HTTP ダウンロード	UDP
APPLICATION=TELNET		×			
APPLICATION=PING	×				
APPLICATION=ALL					

表 21: APPLICATION パラメーターの値と対象パケット

例

IP アドレス 192.168.10.10 からの Telnet アクセス (厳密には ICMP Echo Request と SSH を除くすべての本体宛てパケット) を許可するエントリー「10」を追加

```
CREATE MGMTACL ID=10 IPADDRESS=192.168.10.10 MASK=255.255.255.255  
APPLICATION=TELNET
```

IP アドレス 192.168.20.0/24 の範囲からの Ping (厳密には Telnet と SSH を除くすべての本体宛てパケット) を許可するエントリー「20」を追加

```
CREATE MGMTACL ID=20 IPADDRESS=192.168.20.0 MASK=255.255.255.0  
APPLICATION=TELNET
```

スイッチポート 1~12 からの SSH を除くすべてのパケットを許可するエントリー「30」を追加

```
CREATE MGMTACL ID=30 PORTLIST=1-12 APPLICATION=ALL
```

備考・注意事項

本コマンドでエントリーを追加しないまま、マネージメントアクセスコントロールを有効にすると、Telnet などを使用して本製品にリモートでアクセスできなくなるので注意。

エントリーは、256 個まで登録可能。

関連コマンド

DESTROY MGMTACL (125 ページ)

SET MGMTACL (199 ページ)

SHOW MGMTACL (270 ページ)

CREATE PKI CERTIFICATE

カテゴリー：運用・管理 / PKI

```
CREATE PKI CERTIFICATE=string KEYPAIR=key-id SERIALNUMBER=0..2147483647
  [SUBJECT=distinguished-name] [FORMAT={DER|PEM}]
```

string: 証明書の名前 (1~24 文字。使用可能な文字は半角英数字 (大文字・小文字を区別する)、半角記号 (# \$ % & ' () ~ | - ^ \ @ ' { + * } [; :] , . / -)。文字列に半角空白、!= を含む場合は、前後をダブルクォート (") で囲む必要がある。)。
key-id: 暗号化鍵ペアの ID。0~65535。

distinguished-name: X.500 識別名 (DN)。1~128 文字 (CN (Common Name、64 文字)、OU (Organizational Unit、64 文字)、O (Organization、64 文字)、L (Locality、64 文字)、ST (State or Province、64 文字)、C (Country、2 文字) を入力可能)。使用可能な文字は半角英数字と半角記号 (! # \$ % & ' () = ~ | - ^ \ @ ' { + * } [; :] . - < > ? 半角空白)。前後をダブルクォート (") で囲み、各種属性値をカンマで区切って列挙。("cn=myname,o=myorg,c=jp" の形式)

解説

公開鍵証明書を作成する。

パラメーター

CERTIFICATE 自己証明書の証明書名。この名前が証明書ファイルが作成される (名前が name なら、ファイル名は name.cer となる)。

KEYPAIR 証明書を作成するときに使用する、暗号化鍵ペアの ID。

SERIALNUMBER 証明書のシリアル番号。

SUBJECT X.500 識別名 (DN)。各種属性値をカンマで区切って列挙したもの。SET SYSTEM DISTINGUISHEDNAME を設定している場合は省略できる。

FORMAT 証明書が使用するフォーマットのタイプ。DER (バイナリ) または、PEM (ASCII コード)。デフォルトは DER。

備考・注意事項

コンソールから入力したときだけ有効なコマンド。設定ファイルにこのコマンドを記述しておいても無効。また、本コマンドで作成された公開鍵証明書は設定ファイルには含まれないので注意が必要。

関連コマンド

ADD PKI CERTIFICATE (81 ページ)

DELETE FILE (115 ページ)

DELETE PKI CERTIFICATE (117 ページ)

SHOW FILE (257 ページ)

CREATE PKI ENROLLMENTREQUEST

カテゴリー：運用・管理 / PKI

```
CREATE PKI ENROLLMENTREQUEST=string KEYPAIR=key-id [FORMAT={DER|PEM}]
[TYPE=PKCS10]
```

string: 証明書の名前 (1~24 文字。使用可能な文字は半角英数字 (大文字・小文字を区別する)、半角記号 (# \$ % & ' () ~ | - ^ \ @ ' { + * } [; :] , . / -)。文字列に半角空白、!= を含む場合は、前後をダブルクォート (") で囲む必要がある。)
key-id: 暗号化鍵ペアの ID。0~65535。

解説

公開鍵証明書の発行要求を作成する。

パラメーター

ENROLLMENTREQUEST 証明書発行要求ファイル名を指定する (name と指定すると、ファイル名は name.csr となる)

KEYPAIR 証明書を作成するときに使用する、暗号化鍵ペアの ID。

FORMAT 証明書が使用するフォーマットのタイプ。DER (バイナリ) または、PEM (ASCII コード)。デフォルトは DER。

TYPE 証明書発行要求の形式。PKCS #10 のみサポート。

備考・注意事項

コンソールから入力したときだけ有効なコマンド。設定ファイルにこのコマンドを記述しておいても無効。また、本コマンドで作成された証明書要求ファイルは設定ファイルには含まれないので注意が必要。

関連コマンド

ADD PKI CERTIFICATE (81 ページ)

DELETE FILE (115 ページ)

DELETE PKI CERTIFICATE (117 ページ)

SHOW FILE (257 ページ)

CREATE SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

```
CREATE SNMP COMMUNITY=community [ACCESS={READ|WRITE}] [TRAPHOST=ipadd]
[MANAGER=ipadd] [OPEN={ON|OFF|YES|NO|TRUE|FALSE}]
```

community: SNMP コミュニティー名 (1~32 文字。英数字が使用可能。大文字・小文字を区別する。"(ダブルクォート) [] (スクエアブラケット) \ (バックスラッシュ、円マーク)、半角スペースは使用できない)

ipadd: IP アドレス

解説

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 (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。

TRAPHOST SNMPv2c トラップの送信先ホストを指定する。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。コミュニティー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、コミュニティー作成後に ADD SNMP COMMUNITY コマンドで追加する。

MANAGER SNMP オペレーションを許可するホストを指定する。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 リクエストには応答しない。ただし、SNMP コミュニティーの OPEN プロパティが 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 リクエストに回答する。トラップホスト同様、複数指定する場合はコミュニティー作成後に ADD SNMP COMMUNITY コマンドで追加する。

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 リクエストを受け入れる。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
```

関連コマンド

ADD SNMP COMMUNITY (84 ページ)
DELETE SNMP COMMUNITY (119 ページ)
DESTROY SNMP COMMUNITY (126 ページ)
DISABLE SNMP (140 ページ)
DISABLE SNMP COMMUNITY (141 ページ)
ENABLE SNMP (154 ページ)
ENABLE SNMP COMMUNITY (155 ページ)
SET SNMP COMMUNITY (204 ページ)
SHOW SNMP COMMUNITY (278 ページ)

CREATE SNMPV3 ACCESS

カテゴリー：運用・管理 / SNMP

```
CREATE SNMPV3 ACCESS=group SECURITYMODEL={V1|V2C|V3}
SECURITYLEVEL={NOAUTHENTICATION|AUTHENTICATION|PRIVACY} [READVIEW=view]
[WRITEVIEW=view] [NOTIFYVIEW=view] [STORAGETYPE={VOLATILE|NONVOLATILE}]
```

group: SNMP グループ名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

view: SNMP ビュー名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) ユーザーグループを作成する。

パラメーター

ACCESS SNMP グループ名。

SECURITYMODEL 本グループ所属のユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。

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。NOAUTHENTICATION (認証なし、暗号化なし)、AUTHENTICATION (認証あり、暗号化なし)、PRIVACY (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、CREATE SNMPV3 VIEW コマンドで定義する。指定がない場合、本グループ所属のユーザーは、MIB オブジェクトを読み出せない。

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、CREATE SNMPV3 VIEW コマンドで定義する。指定がない場合、本グループ所属のユーザーは、MIB オブジェクトを書き込めない。

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、CREATE SNMPV3 VIEW コマンドで定義する。指定がない場合、本グループ所属のユーザーは、MIB オブジェクトの通知を受け取れない。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP グループ「managers」を定義する。セキュリティーモデルは V3、セキュリティーレベルは認証/暗号有り。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に設定する。

```
CREATE SNMPV3 ACCESS=managers SECURITYMODEL=V3 SECURITYLEVEL=PRIVACY  
  READVIEW=internet WRITEVIEW=internet NOTIFYVIEW=internet  
  STORAGETYPE=nonvolatile
```

備考・注意事項

デフォルトで、SNMPv1 用に、defaultV1GroupReadOnly、defaultV1GroupReadWrite の 2 つのグループが、SNMPv2c 用に、defaultV2cGroupReadOnly、defaultV2cGroupReadWrite の 2 つのグループが定義されている。

関連コマンド

DESTROY SNMPV3 ACCESS (127 ページ)

SET SNMPV3 ACCESS (205 ページ)

SHOW SNMPV3 ACCESS (282 ページ)

CREATE SNMPV3 COMMUNITY

カテゴリー：運用・管理 / SNMP

```
CREATE SNMPV3 COMMUNITY INDEX=index COMMUNITYNAME=community
SECURITYNAME=username [TRANSPORTTAG=tag] [STORAGETYPE={VOLATILE|
```

NONVOLATILE}]

index: インデックス名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

community: SNMP コミュニティー名 (1~63 文字。英数字が使用可能。大文字・小文字を区別する。"(ダブルクォート) [] (スクエアブラケット) \ (バックスラッシュ、円マーク) 半角スペースは使用できない)

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

tag: タグ名 (1~255 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) SNMP コミュニティーを作成する。

パラメーター

INDEX コミュニティー名。

COMMUNITYNAME コミュニティーに対するパスワードを指定する。

SECURITYNAME SNMPv1 および v2c のユーザー名を指定する。(ADD SNMPV3 USER コマンドで作成したユーザー名は指定しない)。

TRANSPORTTAG タグ名。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP コミュニティー「Index3」を定義する。

```
CREATE SNMPV3 COMMUNITY INDEX=Index3 COMMUNITYNAME=test SECURITYNAME=test
TRANSPORTTAG=trans STORAGETYPE=nonvolatile
```

備考・注意事項

SNMPv1/v2c 対応のコミュニティを作成する場合は、CREATE SNMP COMMUNITY コマンドを使う。

関連コマンド

DESTROY SNMPV3 COMMUNITY (128 ページ)

SET SNMPV3 COMMUNITY (206 ページ)

SHOW SNMPV3 COMMUNITY (284 ページ)

CREATE SNMPV3 GROUP

カテゴリー：運用・管理 / SNMP

```
CREATE SNMPV3 GROUP USERNAME=username SECURITYMODEL={V1|V2C|V3}
    GROUPNAME=group [STORAGETYPE={VOLATILE|NONVOLATILE}]
```

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

group: SNMP グループ名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) ユーザーとユーザーグループの対応付けを定義する。

パラメーター

USERNAME SNMP ユーザー名。ユーザーは、ADD SNMPV3 USER コマンドで定義する。

GROUPNAME SNMP グループ名。グループは、CREATE SNMPV3 ACCESS コマンドで定義する。

SECURITYMODEL 本グループ所属のユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP ユーザー「systemadmin24」と SNMP グループ「managers」を対応付ける。

```
CREATE SNMPV3 GROUP USERNAME=systemadmin24 SECURITYMODEL=V3
    GROUP=managers STORAGETYPE=nonvolatile
```

備考・注意事項

デフォルトで、SNMPv1/v2c用に、defaultV1GroupReadOnly、defaultV1GroupReadWrite、defaultV2cGroupReadOnly、defaultV2cGroupReadWrite が定義されている。

関連コマンド

DESTROY SNMPV3 GROUP (129 ページ)

SET SNMPV3 GROUP (208 ページ)

SHOW SNMPV3 GROUP (287 ページ)

CREATE SNMPV3 NOTIFY

カテゴリー：運用・管理 / SNMP

```
CREATE SNMPV3 NOTIFY=notify [TAG=tag] [TYPE={TRAP|INFORM}]
[STORAGETYPE={VOLATILE|NONVOLATILE}]
```

notify: 通知名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

tag: タグ名 (1~255 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) 通知名を定義する。

パラメーター

NOTIFY 通知名。

TAG タグ名。

TYPE 通知メッセージのフォーマットを指定する。TRAP (トラップ) または INFORM (インフォメーション) かを選択する。デフォルトは、TRAP (トラップ)。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

通知名「sysadmintrap」を定義する。

```
CREATE SNMPV3 NOTIFY=sysadmintrap TAG=sysadmintag TYPE=TRAP
STORAGETYPE=nonvolatile
```

関連コマンド

DESTROY SNMPV3 NOTIFY (130 ページ)

SET SNMPV3 NOTIFY (209 ページ)

SHOW SNMPV3 NOTIFY (289 ページ)

CREATE SNMPV3 TARGETADDR

カテゴリー：運用・管理 / SNMP

CREATE SNMPV3 TARGETADDR=target PARAMS=params IPADDRESS=ipadd

[UDPPORT={0..65535}] [TIMEOUT={0..2147483647}] [RETRIES={0..255}]
[TAGLIST=tag] [STORAGETYPE={VOLATILE|NONVOLATILE}]

target: SNMP ターゲット名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

ipadd: IP アドレス

tag: タグ名 (1~255 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する。複数のタグを指定する場合はスペースで区切る)

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。CREATE SNMPV3 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。

IPADDRESS ターゲットの IP アドレス。

UDPPORT ターゲットのリスニング UDP ポート。0~65535 の範囲を指定する。デフォルトは、162。

TIMEOUT インフォームメッセージを送信し、返信を受け取るまでのタイムアウト時間 (単位はミリ秒) を指定。デフォルトは、1500 (ミリ秒)。

RETRIES インフォームメッセージを再送する回数を指定。デフォルトは、3 (回)。

TAGLIST タグ名。CREATE SNMPV3 NOTIFY コマンド、または、CREATE SNMPV3 COMMUNITY コマンドで定義したタグ名を指定する。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP ターゲット「host451」を定義する。

```
CREATE SNMPV3 TARGETADDR=host451 PARAMS=SNMPmanagerPC
IPADDRESS=192.168.1.100 TAGLIST=sysadminTag STORAGETYPE=nonvolatile
```

備考・注意事項

SNMPv1/v2c 対応のトラップホストを追加する場合は、CREATE SNMP COMMUNITY コマンドまたは、ADD SNMP COMMUNITY コマンドを使う。

関連コマンド

DESTROY SNMPV3 TARGETADDR (131 ページ)

SHOW SNMPV3 TARGETADDR (290 ページ)

CREATE SNMPV3 TARGETPARAMS

カテゴリー：運用・管理 / SNMP

```
CREATE SNMPV3 TARGETPARAMS=params USERNAME=username SECURITYMODEL={V1|
V2C|V3} MESSAGEPROCESSING={V1|V2C|V3} SECURITYLEVEL={NOAUTHENTICATION|
AUTHENTICATION|PRIVACY} [STORAGETYPE={VOLATILE|NONVOLATILE}]
```

params: SNMP ターゲットパラメーターセット名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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 (セキュリティーレベルとユーザー名)などを定義する。

パラメーター

TARGETPARAMS SNMP ターゲットパラメーターセット名。

USERNAME SNMP ユーザー名。ユーザーは、ADD SNMPV3 USER コマンドで定義する

SECURITYMODEL SNMP ユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。

MESSAGEPROCESSING SECURITYMODEL に V1 または V2C を指定した場合に、処理やメッセージ送信に使用する SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。SECURITYMODEL に V3 を指定した場合は、自動的に V3 が指定される。

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ーレベルを指定する。NOAUTHENTICATION (認証なし・暗号化なし)、AUTHENTICATION (認証あり・暗号化なし)、PRIVACY (認証あり・暗号化あり) から選択する。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP ターゲットパラメーターセット「SNMPmanagerPC」を定義する。

```
CREATE SNMPV3 TARGETPARAMS=SNMPmanagerPC USERNAME=systemadmin24
SECURITYMODEL=V3 MESSAGEPROCESSING=V3 SECURITYLEVEL=PRIVACY
STORAGETYPE=nonvolatile
```

備考・注意事項

デフォルトで、SNMPv2c 用に、defaultTgtPrmprivate、defaultTgtPrmpublic が定義されている。
セキュリティーレベルの設定は、USERNAME で指定したユーザー名の設定（ADD SNMPV3 USER コマンド）と同じ設定にする。

関連コマンド

DESTROY SNMPV3 TARGETPARAMS (132 ページ)

SET SNMPV3 TARGETPARAMS (212 ページ)

SHOW SNMPV3 TARGETPARAMS (292 ページ)

CREATE SNMPV3 VIEW

カテゴリー：運用・管理 / SNMP

```
CREATE SNMPV3 VIEW=view SUBTREE={node-oid|node-name} [MASK=mask]
[TYPE={INCLUDED|EXCLUDED}] [STORAGETYPE={VOLATILE|NONVOLATILE}]
```

view: SNMP ビュー名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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 (ノード名)

mask: MIB ノード OID のマスク (xx:xx:xx 形式で、16 進数値で指定。長さは OID の長さに応じて変更可能)

解説

(SNMPv3) ビューを定義する。

パラメーター

VIEW SNMP ビュー名。

SUBTREE MIB ノードを OID (Object Identifier) または名前 (internet など) で指定する。

MASK MIB ノード OID のマスク。16 進数値で指定。たとえば、1.3.6.1 の 6 の部分をマスクしたい場合、「1101(2) = D(16)」となり、「DF(16)」と指定する。xx:xx:xx までの長さが足りない場合は、1 バイト単位で省略可能。

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。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

internet ノード (1.3.6.1) 以下のオブジェクトを含む SNMP ビュー「internet」を定義する。

```
CREATE SNMPV3 VIEW=internet SUBTREE=1.3.6.1 TYPE=INCLUDED
STORAGETYPE=nonvolatile
```

mib-2 ノード (1.3.6.1.2.1) 以下のオブジェクトを含むが、tcp ノード (1.3.6.1.2.1.6) だけは含まない SNMP ビュー「mib2notcp」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 2 コマンドは異なる順序で入力しても同じ動作となる。

```
CREATE SNMPV3 VIEW=mib2notcp SUBTREE=1.3.6.1.2.1 TYPE=INCLUDED
  STORAGETYPE=nonvolatile
CREATE SNMPV3 VIEW=mib2notcp SUBTREE=1.3.6.1.2.1.6 TYPE=EXCLUDED
  STORAGETYPE=nonvolatile
```

備考・注意事項

デフォルトで、SNMPv1/v2c用に、defaultViewAll が作成されている。

関連コマンド

DESTROY SNMPV3 VIEW (133 ページ)

SET SNMPV3 VIEW (215 ページ)

SHOW SNMPV3 VIEW (296 ページ)

DELETE EXCEPTIONLOG

カテゴリー：運用・管理 / システム

DELETE EXCEPTIONLOG={*filename*|ALL}

filename: ファイル名

解説

例外発生ログを削除する。

パラメーター

EXCEPTIONLOG 削除するログの名前。ALL を指定した場合、すべての例外発生ログを削除する。

例

例外発生ログ `except0.exc` を削除する

```
DELETE EXCEPTIONLOG=except0.exc
```

関連コマンド

SHOW EXCEPTIONLOG (256 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=[*device*:]**filename**

device: ファイルが記憶されている媒体。flash を指定

filename: ファイル名

解説

ファイルを削除する。

パラメーター

FILE ファイル名。

例

noneed.cfg を削除する。

```
DELETE FILE=noneed.cfg
```

備考・注意事項

削除したファイルを元に戻すことはできないので、ファイル操作時は十分に注意を払うこと。

関連コマンド

RENAME (180 ページ)

SHOW FILE (257 ページ)

DELETE MGMTACL

カテゴリ：運用・管理 / マネージメントアクセスコントロール

```
DELETE MGMTACL ID=1..256 APPLICATION={TELNET|PING}
```

解説

Management ACL (マネージメントアクセスコントロールリスト) のエントリーから、許可するパケットの種類を削除する。

パラメーター

ID エントリー番号

APPLICATION アクセスを許可するパケットの種類。指定値については、CREATE MGMTACL コマンドのページに掲載されている表を参照

例

エントリー「10」で許可するパケットの種類から「Telnet」を削除する。

```
DELETE MGMTACL ID=10 APPLICATION=TELNET
```

関連コマンド

ADD MGMTACL (80 ページ)

SHOW MGMTACL (270 ページ)

DELETE PKI CERTIFICATE

カテゴリー：運用・管理 / PKI

DELETE PKI CERTIFICATE={*string*|**ALL**}

string: 証明書の名前 (1~24 文字。使用可能な文字は半角英数字 (大文字・小文字を区別する) 半角記号 (# \$ % & ' () ~ | - ^ \ @ ' { + * } [; :] , . / -) 文字列に半角空白、!= を含む場合は、前後をダブルクォート (") で囲む必要がある。)

解説

証明書データベースに登録されている公開鍵証明書を削除する。

パラメーター

CERTIFICATE 証明書データベースで表示される証明書の名前。

関連コマンド

ADD PKI CERTIFICATE (81 ページ)

CREATE PKI CERTIFICATE (98 ページ)

CREATE PKI ENROLLMENTREQUEST (99 ページ)

SET PKI CERTIFICATE (201 ページ)

SHOW PKI CERTIFICATE (272 ページ)

DELETE RADIUSSERVER

カテゴリー：運用・管理 / 認証サーバー

DELETE RADIUSSERVER {SERVER|IPADDRESS}=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/IPADDRESS 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 RADIUSSERVER SERVER=192.168.10.5
```

関連コマンド

ADD RADIUSSERVER (82 ページ)

SET RADIUSSERVER (203 ページ)

SHOW AUTHENTICATION (231 ページ)

DELETE SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

DELETE SNMP COMMUNITY=community [TRAPHOST=*ipadd*] [MANAGER=*ipadd*]

community: SNMP コミュニティ名 (1~32 文字。英数字が使用可能。大文字・小文字を区別する。)(ダブルクォー
ト) [] (スクエアブラケット) \ (バックスラッシュ、円マーク) 半角スペースは使用できない)

ipadd: IP アドレス

解説

SNMP コミュニティ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 コミュニティ名。

TRAPHOST SNMPv2c トラップの送信先ホスト。

MANAGER SNMP オペレーションを許可する管理ステーション。

関連コマンド

ADD SNMP COMMUNITY (84 ページ)

CREATE SNMP COMMUNITY (100 ページ)

DESTROY SNMP COMMUNITY (126 ページ)

DISABLE SNMP COMMUNITY (141 ページ)

ENABLE SNMP COMMUNITY (155 ページ)

SET SNMP COMMUNITY (204 ページ)

SHOW SNMP COMMUNITY (278 ページ)

DELETE SNMPV3 USER

カテゴリ：運用・管理 / SNMP

DELETE SNMPV3 USER=*username*

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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。

例

SNMP ユーザー「systemadmin24」を削除する。

```
DELETE SNMPV3 USER=systemadmin24
```

関連コマンド

ADD SNMPV3 USER (85 ページ)

SHOW SNMPV3 USER (294 ページ)

DELETE SNTP PEER

カテゴリー：運用・管理 / SNTP

DELETE SNTP PEER=*ipadd*

ipadd: IP アドレス

解説

Sntp サーバーの IP アドレスを削除する。

パラメーター

PEER Sntp サーバーの IP アドレス。

関連コマンド

ADD SNTP PEER (86 ページ)

DELETE USER

カテゴリ：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。デフォルトユーザー (MANAGER、OPERATOR) は削除できない。

例

ユーザー fly を削除する。

```
DELETE USER=fly
```

備考・注意事項

削除しようとしたユーザーが、MANAGER レベルで、かつ、システムで最後の有効 (Enable) なユーザーである場合、削除できない。

関連コマンド

ADD USER (87 ページ)

DISABLE USER (147 ページ)

ENABLE USER (162 ページ)

PURGE USER (178 ページ)

RESET USER (181 ページ)

SET USER (227 ページ)

SHOW USER (305 ページ)

DESTROY ENCO KEY

カテゴリー：運用・管理 / 鍵作成・管理

DESTROY ENCO KEY=key-id

key-id: 鍵番号 (0~65535)

解説

指定した鍵を削除する。

フラッシュメモリー上の鍵が格納されていた領域は上書きされ、鍵情報が取得できないように処置される。

パラメーター

KEY 鍵番号。

関連コマンド

CREATE ENCO KEY (92 ページ)

SET ENCO KEY (196 ページ)

SHOW ENCO KEY (255 ページ)

DESTROY LOG OUTPUT

カテゴリー：運用・管理 / ログ

DESTROY LOG OUTPUT=*output-id*

output-id: ログ出力 ID (2~20)

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。2~20 の任意の番号を指定する。

例

ログ出力先定義「2」を削除する。

```
DESTROY LOG OUTPUT=2
```

関連コマンド

CREATE LOG OUTPUT (94 ページ)

SHOW LOG OUTPUT (267 ページ)

DESTROY MGMTACL

カテゴリ：運用・管理 / マネージメントアクセスコントロール

DESTROY MGMTACL ID=1..256

解説

Management ACL (マネージメントアクセスコントロールリスト) からアクセス制御エントリーを削除する。

パラメーター

ID エントリー番号

入力・出力・画面例

```
# destroy mgmtacl id=10
Entry Deleted
```

例

エントリー「10」を削除する。

```
DESTROY MGMTACL ID=10
```

備考・注意事項

本コマンドでエントリーを削除し、すべてのエントリーを削除した状態で、マネージメントアクセスコントロールを有効にすると、Telnet などを使用して本製品にリモートでアクセスできなくなるので注意。

関連コマンド

CREATE MGMTACL (96 ページ)

SET MGMTACL (199 ページ)

SHOW MGMTACL (270 ページ)

DESTROY SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

DESTROY SNMP COMMUNITY=*community*

community: SNMP コミュニティ名 (1~32 文字。英数字が使用可能。大文字・小文字を区別する。)"(ダブルクォート) \ [] (スクエアブラケット) \ (バックスラッシュ、円マーク) 半角スペースは使用できない)

解説

SNMP コミュニティを削除する。

パラメーター

COMMUNITY SNMP コミュニティ名。

関連コマンド

ADD SNMP COMMUNITY (84 ページ)

CREATE SNMP COMMUNITY (100 ページ)

DISABLE SNMP COMMUNITY (141 ページ)

ENABLE SNMP COMMUNITY (155 ページ)

SET SNMP COMMUNITY (204 ページ)

SHOW SNMP COMMUNITY (278 ページ)

DESTROY SNMPV3 ACCESS

カテゴリー：運用・管理 / SNMP

```
DESTROY SNMPV3 ACCESS=group SECURITYMODEL={V1|V2C|V3}  
SECURITYLEVEL={NOAUTHENTICATION|AUTHENTICATION|PRIVACY}
```

group: SNMP グループ名 (1～63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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

ACCESS SNMP グループ名。

SECURITYMODEL 本グループ所属のユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。

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。NOAUTHENTICATION (認証なし、暗号化なし)、AUTHENTICATION (認証あり、暗号化なし)、PRIVACY (認証あり、暗号化あり) から選択する。

関連コマンド

CREATE SNMPV3 ACCESS (102 ページ)

SET SNMPV3 ACCESS (205 ページ)

SHOW SNMPV3 ACCESS (282 ページ)

DESTROY SNMPV3 COMMUNITY

カテゴリ：運用・管理 / SNMP

DESTROY SNMPV3 COMMUNITY INDEX=*index*

index: インデックス名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) SNMP コミュニティを削除する。

パラメーター

INDEX コミュニティ名。

例

SNMP コミュニティ「Index3」の定義を削除する。

```
DESTROY SNMPV3 COMMUNITY INDEX=Index3
```

関連コマンド

CREATE SNMPV3 COMMUNITY (104 ページ)

SHOW SNMPV3 COMMUNITY (284 ページ)

DESTROY SNMPV3 GROUP

カテゴリー：運用・管理 / SNMP

DESTROY SNMPV3 GROUP USERNAME=username SECURITYMODEL={V1|V2C|V3}

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) ユーザーとユーザーグループの対応付けを削除する。

パラメーター

USERNAME SNMP ユーザー名。

SECURITYMODEL 本グループ所属のユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。

例

SNMP ユーザー「systemadmin24」の SNMP グループへの対応付けを削除する。

```
DESTROY SNMPV3 GROUP USERNAME=systemadmin24 SECURITYMODEL=V3
```

関連コマンド

CREATE SNMPV3 GROUP (106 ページ)

SET SNMPV3 GROUP (208 ページ)

SHOW SNMPV3 GROUP (287 ページ)

DESTROY SNMPV3 NOTIFY

カテゴリー：運用・管理 / SNMP

DESTROY SNMPV3 NOTIFY=*notify*

notify: 通知名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) 通知名の定義を削除する。

パラメーター

NOTIFY 通知名。

例

通知名「sysadmintrap」の定義を削除する。

```
DESTROY SNMPV3 NOTIFY=sysadmintrap
```

関連コマンド

CREATE SNMPV3 NOTIFY (107 ページ)

SHOW SNMPV3 NOTIFY (289 ページ)

DESTROY SNMPV3 TARGETADDR

カテゴリ：運用・管理 / SNMP

DESTROY SNMPV3 TARGETADDR=*target*

target: SNMP ターゲット名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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。

例

SNMP ターゲット「host451」の定義を削除する。

```
DESTROY SNMPV3 TARGETADDR=host451
```

関連コマンド

CREATE SNMPV3 TARGETADDR (108 ページ)

SET SNMPV3 TARGETADDR (210 ページ)

SHOW SNMPV3 TARGETADDR (290 ページ)

DESTROY SNMPV3 TARGETPARAMS

カテゴリ：運用・管理 / SNMP

DESTROY SNMPV3 TARGETPARAMS=*params*

params: SNMP ターゲットパラメーターセット名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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

CREATE SNMPV3 TARGETPARAMS (110 ページ)

SHOW SNMPV3 TARGETPARAMS (292 ページ)

DESTROY SNMPV3 VIEW

カテゴリー：運用・管理 / SNMP

DESTROY SNMPV3 VIEW=view SUBTREE={*node-oid*|*node-name*}

view: SNMP ビュー名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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 (規定のノード名)

解説

(SNMPv3) ビューの定義を削除する。

パラメーター

VIEW SNMP ビュー名。

SUBTREE MIB ノードを OID (Object Identifier) または名前 (internet など) で指定する。

例

SNMP ビュー「mib2notcp」から tcp ノード (1.3.6.1.2.1.6) を削除する。

```
DESTROY SNMPV3 VIEW=mib2notcp SUBTREE=1.3.6.1.2.1.6
```

関連コマンド

CREATE SNMPV3 VIEW (112 ページ)

SET SNMPV3 VIEW (215 ページ)

SHOW SNMPV3 VIEW (296 ページ)

DISABLE AUTHENTICATION

カテゴリー：運用・管理 / 認証サーバー

DISABLE AUTHENTICATION

解説

認証モードを無効にする。デフォルトは、無効。

関連コマンド

ENABLE AUTHENTICATION (148 ページ)

SHOW AUTHENTICATION (231 ページ)

DISABLE INTERFACE LINKTRAP

カテゴリー：運用・管理 / SNMP

DISABLE INTERFACE [=interface] **LINKTRAP**

interface: ポート番号 (1~24)

解説

指定したインターフェースでリンクアップ/リンクダウントラップを生成しないようにする。デフォルトは有効 (トラップを生成する)。

リンクトラップの設定は SHOW INTERFACE コマンドで確認できる (ifLinkUpDownTrapEnable)。

パラメーター

INTERFACE ポート番号 (1~24) を指定する。SHOW INTERFACE コマンドの「ifIndex」で確認できる。

例

スイッチポート 1 でリンクアップ/リンクダウントラップの生成を無効にする。

```
DISABLE INTERFACE=1 LINKTRAP
```

関連コマンド

ENABLE INTERFACE LINKTRAP (149 ページ)

SHOW INTERFACE (260 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

ENABLE LOG (150 ページ)

DISABLE LOG OUTPUT

カテゴリー：運用・管理 / ログ

DISABLE LOG OUTPUT[=*output-id*]

output-id: ログ出力 ID (2~20)

解説

指定した出力先へのログ出力を無効にする。

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、すべてのログ出力が無効になる。

関連コマンド

DISABLE LOG (136 ページ)

ENABLE LOG OUTPUT (151 ページ)

DISABLE MGMTACL

カテゴリー：運用・管理 / マネージメントアクセスコントロール

DISABLE MGMTACL

解説

マネージメントアクセスコントロールを無効にする。デフォルトは無効。

例

マネージメントアクセスコントロールを無効にする。

```
DISABLE MGMTACL
```

関連コマンド

CREATE MGMTACL (96 ページ)

ENABLE MGMTACL (152 ページ)

SHOW MGMTACL (270 ページ)

DISABLE RADIUSACCOUNTING

カテゴリー：運用・管理 / 認証サーバー

DISABLE RADIUSACCOUNTING

解説

RADIUS (Remote Authentication Dial In User Server) サーバーのアカウントिंग機能を無効にする。
デフォルトは、無効。

関連コマンド

ENABLE RADIUSACCOUNTING (153 ページ)

SHOW RADIUSACCOUNTING (275 ページ)

DISABLE SNMP

カテゴリー：運用・管理 / SNMP

DISABLE SNMP

解説

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 (141 ページ)

ENABLE SNMP (154 ページ)

ENABLE SNMP COMMUNITY (155 ページ)

SHOW SNMP (277 ページ)

SHOW SNMP COMMUNITY (278 ページ)

DISABLE SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

DISABLE SNMP COMMUNITY=*community*

community: SNMP コミュニティ名 (1~32 文字。英数字が使用可能。大文字・小文字を区別する。)"(ダブルクォート) \ (スクエアブラケット) \ (バックスラッシュ、円マーク) 半角スペースは使用できない)

解説

指定した SNMP コミュニティを無効にする。

パラメーター

COMMUNITY SNMP コミュニティ名。

関連コマンド

DISABLE SNMP (140 ページ)

ENABLE SNMP (154 ページ)

ENABLE SNMP COMMUNITY (155 ページ)

SHOW SNMP (277 ページ)

SHOW SNMP COMMUNITY (278 ページ)

DISABLE SNMP TRAP

カテゴリー：運用・管理 / SNMP

DISABLE SNMP [AUTHENTICATE_TRAP] [TRAP={AUTHENTICATION|COLDSTART|NEWROOT|FAN|DOS|STPSTATECHANGE|TEMPERATURE|LINK|INTRUSION|TOPOLOGYCHANGE|STORMDETECT|LOOPDETECT|ALL}]

解説

SNMP トラップの生成を無効にする。デフォルトは有効。

パラメーター

AUTHENTICATE_TRAP SNMP 認証トラップの生成を無効にする。TRAP=AUTHENTICATION と同義。

TRAP 送信を無効にするトラップを選択。AUTHENTICATION、COLDSTART、NEWROOT、FAN、DOS、STPSTATECHANGE、TEMPERATURE、LINK、INTRUSION、TOPOLOGYCHANGE、STORMDETECT、LOOPDETECT、ALL のいずれか。カンマ区切りによる複数指定が可能。ALL を指定した場合はすべてのトラップの送信が無効になる。

トラップ	トラップ送信のタイミング
AUTHENTICATION	異なる SNMP コミュニティー名のメッセージ受信時
COLDSTART	ハードウェアリセットによるシステム起動時
NEWROOT	STP において新しいルートへの切り替わり時
FAN	ファンの回転異常検出時
DOS	DoS 攻撃検出時
STPSTATECHANGE	STP においてステータス変更時
TEMPERATURE	温度異常検出時
LINK	ポートのリンクアップ・リンクダウン時
INTRUSION	ポートセキュリティにおいて不正パケット受信時
TOPOLOGYCHANGE	STP においてトポロジー変更時
STORMDETECT	受信レート検出においてループの検出時、アクション実行時、アクションからの復旧時
LOOPDETECT	LDF 検出においてループの検出時、アクション実行時、アクションからの復旧時

表 22:

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) が必要。

関連コマンド

ADD SNMP COMMUNITY (84 ページ)

DISABLE SNMP (140 ページ)

ENABLE SNMP (154 ページ)

ENABLE SNMP TRAP (156 ページ)

SHOW SNMP (277 ページ)

SHOW SNMP TRAP (280 ページ)

DISABLE SNTP

カテゴリー：運用・管理 / SNTP

DISABLE SNTP

解説

SNTP 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 SNTP (158 ページ)

PURGE SNTP (177 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。

関連コマンド

ENABLE SSH SERVER (159 ページ)

SET SSH SERVER (218 ページ)

SHOW SSH (299 ページ)

DISABLE TELNET

カテゴリー：運用・管理 / ターミナルサービス

DISABLE TELNET

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 (161 ページ)

DISABLE USER

カテゴリ：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無効にする。

パラメーター

USER ログイン名。

例

ユーザー「ATKK」を無効にする。

```
DISABLE USER=ATKK
```

備考・注意事項

無効にしようとしたユーザーが、MANAGER レベルで、かつ、システムで最後の有効 (Enable) なユーザーである場合、無効にできない。

関連コマンド

ADD USER (87 ページ)

DELETE USER (122 ページ)

ENABLE USER (162 ページ)

PURGE USER (178 ページ)

RESET USER (181 ページ)

SET USER (227 ページ)

SHOW USER (305 ページ)

ENABLE AUTHENTICATION

カテゴリー：運用・管理 / 認証サーバー

ENABLE AUTHENTICATION

解説

認証モードを有効にする。デフォルトは、無効。

関連コマンド

DISABLE AUTHENTICATION (134 ページ)

SHOW AUTHENTICATION (231 ページ)

ENABLE INTERFACE LINKTRAP

カテゴリ：運用・管理 / SNMP

ENABLE INTERFACE [=interface] **LINKTRAP**

interface: ポート番号 (1~24)

解説

指定したインターフェースでリンクアップ/リンクダウントラップを生成するようにする。デフォルトは有効 (トラップを生成する)。

リンクトラップの設定は SHOW INTERFACE コマンドで確認できる (ifLinkUpDownTrapEnable)。

パラメーター

INTERFACE ポート番号 (1~24) を指定する。SHOW INTERFACE コマンドの「ifIndex」で確認できる。

例

スイッチポート 1 でリンクアップ/リンクダウントラップの生成を有効にする。

```
ENABLE INTERFACE=1 LINKTRAP
```

関連コマンド

DISABLE INTERFACE LINKTRAP (135 ページ)

SHOW INTERFACE (260 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 (136 ページ)

ENABLE LOG OUTPUT

カテゴリー：運用・管理 / ログ

ENABLE LOG OUTPUT[=*output-id*]

output-id: ログ出力 ID (2~20)

解説

指定した出力先へのログ出力を有効にする。

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、すべてのログ出力が有効になる。

関連コマンド

DISABLE LOG OUTPUT (137 ページ)

ENABLE LOG (150 ページ)

ENABLE MGMTACL

カテゴリー：運用・管理 / マネージメントアクセスコントロール

ENABLE MGMTACL

解説

マネージメントアクセスコントロールを有効にする。デフォルトは無効。

例

マネージメントアクセスコントロールを有効にする。

```
ENABLE MGMTACL
```

備考・注意事項

本コマンドでマネージメントアクセスコントロールを有効にする場合は、Management ACL にエントリーが登録されていることを確認してから有効にすること。Management ACL にエントリーが登録されていない場合、本製品は自分宛ての IP パケットをすべて破棄する。

SSH サーバーを利用する場合は、マネージメントアクセスコントロールを有効にしないこと。マネージメントアクセスコントロールの有効時は、Management ACL の設定にかかわらず、本製品宛ての SSH パケットをすべて破棄する。

関連コマンド

CREATE MGMTACL (96 ページ)

DISABLE MGMTACL (138 ページ)

ENABLE SSH SERVER (159 ページ)

SHOW MGMTACL (270 ページ)

ENABLE RADIUSACCOUNTING

カテゴリー：運用・管理 / 認証サーバー

ENABLE RADIUSACCOUNTING

解説

RADIUS (Remote Authentication Dial In User Server) サーバーのアカウントिंग機能を有効にする。
デフォルトは、無効。

関連コマンド

DISABLE RADIUSACCOUNTING (139 ページ)

SHOW RADIUSACCOUNTING (275 ページ)

ENABLE SNMP

カテゴリー：運用・管理 / SNMP

ENABLE SNMP

解説

SNMP モジュールを有効にする。デフォルトは無効。

備考・注意事項

SNMP を使うには、事前にローカル IP インターフェース (マネージメント VLAN インターフェース) の設定が必要。詳しくは「IP」の「IP インターフェース」を参照のこと。

関連コマンド

DISABLE SNMP (140 ページ)

DISABLE SNMP COMMUNITY (141 ページ)

ENABLE SNMP COMMUNITY (155 ページ)

SHOW SNMP (277 ページ)

SHOW SNMP COMMUNITY (278 ページ)

ENABLE SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

ENABLE SNMP COMMUNITY=*community*

community: SNMP コミュニティ名 (1~32 文字。英数字が使用可能。大文字・小文字を区別する。)"(ダブルクォート) \ [] (スクエアブラケット) \ (バックスラッシュ、円マーク) 半角スペースは使用できない)

解説

無効状態の SNMP コミュニティを有効にする。デフォルトは有効。

パラメーター

COMMUNITY SNMP コミュニティ名。

関連コマンド

DISABLE SNMP (140 ページ)

DISABLE SNMP COMMUNITY (141 ページ)

ENABLE SNMP (154 ページ)

SHOW SNMP (277 ページ)

SHOW SNMP COMMUNITY (278 ページ)

ENABLE SNMP TRAP

カテゴリー：運用・管理 / SNMP

```
ENABLE SNMP [AUTHENTICATE_TRAP] [TRAP={AUTHENTICATION|COLDSTART|NEWROOT|
FAN|DOS|STPSTATECHANGE|TEMPERATURE|LINK|INTRUSION|TOPOLOGYCHANGE|
STORMDETECT|LOOPDETECT|ALL}]
```

解説

SNMP トラップの生成を有効にする。デフォルトは有効。

パラメーター

AUTHENTICATE_TRAP SNMP 認証トラップの生成を有効にする。TRAP=AUTHENTICATION と同義。

TRAP 送信するトラップを選択。AUTHENTICATION、COLDSTART、NEWROOT、FAN、DOS、STPSTATECHANGE、TEMPERATURE、LINK、INTRUSION、TOPOLOGYCHANGE、STORMDETECT、LOOPDETECT、ALL のいずれか。カンマ区切りによる複数指定が可能。ALL を指定した場合はすべてのトラップが送信される。

トラップ	トラップ送信のタイミング
AUTHENTICATION	異なる SNMP コミュニティ名のメッセージ受信時
COLDSTART	ハードウェアリセットによるシステム起動時
NEWROOT	STP において新しいルートへの切り替わり時
FAN	ファンの回転異常検出時
DOS	DoS 攻撃検出時
STPSTATECHANGE	STP においてステータス変更時
TEMPERATURE	温度異常検出時
LINK	ポートのリンクアップ・リンクダウン時
INTRUSION	ポートセキュリティにおいて不正パケット受信時
TOPOLOGYCHANGE	STP においてトポロジー変更時
STORMDETECT	受信レート検出においてループの検出時、アクション実行時、アクションからの復旧時
LOOPDETECT	LDF 検出においてループの検出時、アクション実行時、アクションからの復旧時

表 23:

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、トラップホストの設定 (ADD SNMP COMMUNITY TRAPHOST=ipadd) が必要。

TRAP=LINK を指定した場合、実際にトラップを送信するためには、ENABLE INTERFACE LINKTRAP コマンドを実行する必要がある。

TRAP=INTRUSION を指定した場合、実際にトラップを送信するためには、SET SWITCH PORT SECURITYMODE コマンドの INTRUSIONACTION パラメーターを TRAP または、DISABLE に設定する必要がある。

関連コマンド

ADD SNMP COMMUNITY (84 ページ)

DISABLE SNMP (140 ページ)

DISABLE SNMP TRAP (142 ページ)

ENABLE SNMP (154 ページ)

SHOW SNMP (277 ページ)

SHOW SNMP TRAP (280 ページ)

ENABLE SNTP

カテゴリー：運用・管理 / SNTP

ENABLE SNTP

解説

SNTP 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 SNTP (144 ページ)

PURGE SNTP (177 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 (0 ~ 5 時間)

seconds: 時間 (60 ~ 600 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を 60 ~ 600 (秒) で指定する。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 180 秒。

備考・注意事項

SSH を使うには、事前にローカル IP インターフェース (マネージメント VLAN インターフェース) の設定が必要。詳しくは「IP」の「IP インターフェース」を参照のこと。

SSH サーバーを利用する場合は、マネージメントアクセスコントロールを有効にしないこと。マネージメントアクセスコントロールの有効時は、Management ACL の設定にかかわらず、本製品宛での SSH パケットをすべて破棄する。

SSH 経由でのログイン失敗が 50 回連続した場合、下記のようなログが出力され、SSH サーバーが自動的に無効化される。SSH サーバーを再度有効化するには、手動で本コマンドを実行すること。なお、SSH 経由でのログインには、SET USERCONFIG コマンドの LOGINFAIL は適用されない。

```
I 09/22/11 11:52:02 ssh: SSH server disabled
```

```
W 09/22/11 11:52:02 system: SSH server disabled. Continuous invalid login attempts. Possible server attack from 172.17.20.33
```

関連コマンド

DISABLE SSH SERVER (145 ページ)

ENABLE MGMTACL (152 ページ)

SET SSH SERVER (218 ページ)

SHOW SSH (299 ページ)

ENABLE TELNET

カテゴリー：運用・管理 / ターミナルサービス

ENABLE TELNET

解説

Telnet サーバー機能を有効にする。デフォルトは有効。

備考・注意事項

Telnet を使うには、事前にローカル IP インターフェース（マネージメント VLAN インターフェース）の設定が必要。詳しくは「IP」の「IP インターフェース」を参照のこと。

関連コマンド

DISABLE TELNET (146 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。

例

ユーザー「ATKK」を有効にする。

```
ENABLE USER=ATKK
```

関連コマンド

ADD USER (87 ページ)

DELETE USER (122 ページ)

DISABLE USER (147 ページ)

PURGE USER (178 ページ)

RESET USER (181 ページ)

SET USER (227 ページ)

SHOW USER (305 ページ)

EXIT

カテゴリー：運用・管理 / システム

EXIT

解説

ログインセッションからログアウトする。LOGOUT コマンド、LOGOFF コマンド、QUIT コマンドも同義。

FORMAT DEVICE

カテゴリー：運用・管理 / 記憶装置とファイルシステム

FORMAT DEVICE=FLASH

解説

デバイスのフォーマットを行う。

パラメーター

DEVICE 物理デバイスを指定する。指定できるのは、FLASHのみ。

備考・注意事項

アプリケーションブロックのファームウェアファイル以外は削除される。

HELP

カテゴリー：運用・管理 / システム

HELP

解説

オンラインヘルプを表示する。

入力・出力・画面例

```
# help
Available commands:
ACTivate - Activates an instance of an object type
ADD      - Adds an instance of an object type
CLear   - Clears all data relating to the object
COpy    - Copy file
CReate  - Makes a new instance of an object type
DELeTe  - Removes an instance of an object
DEStroy - Destroys an object instance
DISable - Suspends the object operation while retaining its configuration
ENable  - Allows an object to enter its operational state
EXit    - Quits the current management session
FORMAT  - Formats a file system drive
Help    - Displays available commands
LOAD    - Downloads a file
LOGOFF  - Logs out of the current management session
LOGOUT  - Logs out of the current management session
PING    - Pings an IP address
PURge   - Clears all the object's configurable data and disables it
Quit    - Quits the current management session
REName  - Rename file
RESEt   - Restores the object to its stored configuration
REStArT - Restart the switch
SAve    - Saves configuration
SEt     - Sets the configuration of an existing object
SHow    - Displays diagnostic information to the user
Upload  - Uploads a file
```

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 DESTFILE={ [device:] filename|APPBLOCK } {SRCFILE|
  FILE}=filename SERVER=ipadd
```

```
LOAD METHOD=XMODEM DESTFILE={ [device:] filename|APPBLOCK }
```

```
LOAD METHOD=LOCAL DESTFILE=APPBLOCK {SRCFILE|FILE}=[device:] filename
```

```
LOAD METHOD={HTTP|WEB|WWW} DESTFILE={ [device:] filename|APPBLOCK }
  {SRCFILE|FILE}=filename [HTTPPROXY=ipadd] [PROXYPORT=1..65535]
  SERVER=ipadd [SERVPORT=1..65535] [USERNAME=username] [PASSWORD=password]
```

device: ファイルが記憶されている媒体。flash を指定

filename: ファイル名 (1~28 文字)

ipadd: IP アドレス

password: パスワード (1~60 文字)

username: ユーザー名 (1~60 文字)

解説

ファイルをダウンロードする。TFTP、XMODEM、HTTP の各プロトコル/サーバーが使用可能。METHOD に LOCAL を指定すると、フラッシュメモリ内のファームウェアファイルをアプリケーションブロックにダウンロード (転送) し、起動時に使用するファームウェアファイルを切り替えることができる。

パラメーター

METHOD 転送プロトコル。TFTP、XMODEM、LOCAL、HTTP、WEB、WWW のいずれかを指定する。

DESTFILE ダウンロード後のファイル名。ファームウェアファイル (.img) を、APPBLOCK を指定してダウンロードした場合、本製品は再起動し、起動時に使用するファームウェアが転送されたファイルに切り替わる。ファームウェアファイルを、ファイル名を指定してダウンロードした場合は、フラッシュメモリに保存されるのみ。

SRCFILE/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。

HTTPPROXY 転送プロトコルに HTTP、WEB、WWW を指定した際、プロキシサーバー経由で HTTP サーバーにアクセスする場合はプロキシサーバーの IP アドレスを指定する。

PROXYPORT 転送プロトコルに HTTP、WEB、WWW を指定した際、プロキシサーバー経由で HTTP サーバーにアクセスする場合はプロキシ用のポート番号を指定する。デフォルトは 80 番。

SERVER TFTP サーバー、HTTP サーバーの IP アドレス。

SERVPORT HTTP サーバーのポート番号。デフォルトは 80 番。

USERNAME HTTP で認証が必要な際に使用するユーザー名。

PASSWORD HTTP で認証が必要な際に使用するパスワード。

例

設定ファイル「settei.cfg」を TFTP サーバー「192.168.1.103」からダウンロードする

```
LOAD METHOD=TFTP DESTFILE=settei.cfg SERVER=192.168.1.103 FILE=settei.cfg
```

備考・注意事項

SRCFILE/FILE と DESTFILE にファイル名を指定する場合は、同じ拡張子を指定する。

設定ファイルをダウンロードしても、自動的に起動時設定ファイルに設定されない。SET CONFIG コマンドで起動時設定ファイルとして設定する。

エンハンススタッキング機能で、マスタースイッチからスレーブスイッチに接続している場合は、XMODEM は使えない。

TFTP、HTTP を使うには、事前にローカル IP インターフェース（マネージメント VLAN インターフェース）の設定が必要。詳しくは「IP」の「IP インターフェース」を参照のこと。

関連コマンド

COPY (90 ページ)

UPLOAD (309 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 コマンド、QUIT コマンド、EXIT コマンドも同義。

LOGOUT

カテゴリー：運用・管理 / システム

LOGOUT

解説

ログインセッションからログアウトする。LOGOFF コマンド、QUIT コマンド、EXIT コマンドも同義。

PURGE AUTHENTICATION

カテゴリー：運用・管理 / 認証サーバー

PURGE AUTHENTICATION

解説

認証モードの設定をデフォルト状態に戻す。

関連コマンド

DISABLE AUTHENTICATION (134 ページ)

ENABLE AUTHENTICATION (148 ページ)

SET AUTHENTICATION (187 ページ)

SHOW AUTHENTICATION (231 ページ)

PURGE LOG

カテゴリー：運用・管理 / ログ

PURGE LOG [= {TEMPORARY|PERMANENT}]

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り、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 (136 ページ)

ENABLE LOG (150 ページ)

PURGE MGMTACL

カテゴリー：運用・管理 / マネージメントアクセスコントロール

PURGE MGMTACL

解説

Management ACL (マネージメントアクセスコントロールリスト) からアクセス制御エントリーをすべて消去する。

例

マネージメントアクセスコントロールからアクセス制御エントリーを消去する。

```
PURGE MGMTACL
```

関連コマンド

ADD MGMTACL (80 ページ)

CREATE MGMTACL (96 ページ)

SET MGMTACL (199 ページ)

PURGE SNMPV3 ACCESS

カテゴリー：運用・管理 / SNMP

PURGE SNMPV3 ACCESS

解説

(SNMPv3) ユーザーグループをすべて削除する。

例

SNMP グループの定義をすべて削除する。

```
PURGE SNMPV3 ACCESS
```

関連コマンド

CREATE SNMPV3 ACCESS (102 ページ)

DESTROY SNMPV3 ACCESS (127 ページ)

SHOW SNMPV3 ACCESS (282 ページ)

PURGE SNMPV3 NOTIFY

カテゴリー：運用・管理 / SNMP

PURGE SNMPV3 NOTIFY

解説

(SNMPv3) 通知名の定義をすべて削除する。

例

通知名の定義をすべて削除する。

```
PURGE SNMPV3 NOTIFY
```

関連コマンド

CREATE SNMPV3 NOTIFY (107 ページ)

DESTROY SNMPV3 NOTIFY (130 ページ)

SHOW SNMPV3 NOTIFY (289 ページ)

PURGE SNMPV3 TARGETADDR

カテゴリー：運用・管理 / SNMP

PURGE SNMPV3 TARGETADDR

解説

(SNMPv3) ターゲット (通知メッセージの送信先) をすべて削除する。

例

SNMP ビューの定義をすべて削除する。

```
PURGE SNMPV3 TARGETADDR
```

関連コマンド

CREATE SNMPV3 TARGETADDR (108 ページ)

DESTROY SNMPV3 TARGETADDR (131 ページ)

SHOW SNMPV3 TARGETADDR (290 ページ)

PURGE SNMPV3 VIEW

カテゴリー：運用・管理 / SNMP

PURGE SNMPV3 VIEW

解説

(SNMPv3) ビューの定義をすべて削除する。

例

SNMP ビューの定義をすべて削除する。

```
PURGE SNMPV3 VIEW
```

関連コマンド

CREATE SNMPV3 VIEW (112 ページ)

DESTROY SNMPV3 VIEW (133 ページ)

SHOW SNMPV3 VIEW (296 ページ)

PURGE SNTP

カテゴリー：運用・管理 / SNTP

PURGE SNTP

解説

SNTP モジュールの設定情報をすべて消去する。

備考・注意事項

ランタイムメモリー上にある SNTP 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 SNTP (144 ページ)

ENABLE SNTP (158 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

デフォルトユーザー (MANAGER、OPERATOR) 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、OPERATOR の設定をデフォルトに戻す。

備考・注意事項

ランタイムメモリー上にあるユーザー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

ADD USER (87 ページ)

DELETE USER (122 ページ)

DISABLE USER (147 ページ)

ENABLE USER (162 ページ)

RESET USER (181 ページ)

SET USER (227 ページ)

SHOW USER (305 ページ)

QUIT

カテゴリー：運用・管理 / システム

QUIT

解説

ログインセッションからログアウトする。LOGOFF コマンド、LOGOUT コマンド、EXIT コマンドと同義。

RENAME

カテゴリー：運用・管理 / 記憶装置とファイルシステム

RENAME [*device:*]**src-filename** [*device:*]**dst-filename**

device: ファイルが記憶されている媒体。flash を指定。変更前と変更後ファイル名の指定は、同じにすること

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 (115 ページ)

SHOW FILE (257 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*|ALL} COUNTER

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

ユーザーアカウントのカウンターをリセットする。

パラメーター

USER ユーザーアカウントのカウンター値をリセットしたいユーザー名を指定する。ALL を指定するとすべてのユーザーアカウントのカウンター値がリセットされる。

例

ユーザー「ATKK」のカウンター値をリセットする。

```
RESET USER=ATKK COUNTER
```

関連コマンド

ADD USER (87 ページ)

DELETE USER (122 ページ)

DISABLE USER (147 ページ)

ENABLE USER (162 ページ)

PURGE USER (178 ページ)

SET USER (227 ページ)

SHOW USER (305 ページ)

RESET USERCONFIG

カテゴリー：運用・管理 / ユーザー認証データベース

RESET USERCONFIG COUNTER

解説

ユーザー認証機能のカウンター値をリセットする。

例

ユーザー認証機能のカウンター値をリセットする

```
RESET USERCONFIG COUNTER
```

関連コマンド

SET USERCONFIG (229 ページ)

SHOW USERCONFIG (307 ページ)

RESTART

カテゴリー：運用・管理 / システム

RESTART {**REBOOT**|**SWITCH**} [CONFIG={*filename*|NONE}]

filename: ファイル名 (拡張子は.cfg)

解説

システムを再起動する。コールドスタート (ハードウェアリセット) 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。

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。

SWITCH コールドスタート (ハードウェアリセット) 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。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。NONE を指定した場合は、起動時設定ファイルの設定がなしになる。

例

スイッチをハードウェアリセットする。

```
RESTART REBOOT
```

一度だけ TEMP.CFG の設定で再起動する。

```
RESTART SWITCH CONFIG=TEMP.CFG
```

関連コマンド

SHOW CONFIG (235 ページ)

SAVE CONFIGURATION

カテゴリー：運用・管理 / コンフィグレーション

SAVE CONFIGURATION

解説

現在の設定内容（メモリー上の設定内容）を、現在設定されている起動時設定ファイルに保存する。

入力・出力・画面例

```
# save configuration
Saving current configuration ..... done!
```

備考・注意事項

起動時設定ファイルが「NONE」の場合は実行できないため、SET CONFIG コマンドで起動スクリプトを設定する必要がある。

起動時設定ファイルとして指定されているファイルが存在しない場合、このコマンドを実行するとエラーになる。

関連コマンド

SHOW CONFIG (235 ページ)

SAVE LOG

カテゴリー：運用・管理 / ログ

SAVE LOG [= {TEMPORARY|PERMANENT}] **FILENAME=filename** [FULL]
 [MODULE=module-name] [REVERSE] [SEVERITY=severity] [OVERWRITE]

filename: ファイル名 (1~28 文字。英数字が使用可能。拡張子は.log)

module-name: モジュール名

severity: ログレベル (E、W、I で指定)

解説

ログをファイルに保存する。

パラメーター

LOG 保存対象のログを、TEMPORARY (RAM 上のログ) または PERMANENT (NVS 上のログ) で指定する。省略時は TEMPORARY (RAM 上のログ) が保存対象となる。

FILENAME ログを保存するファイル名。

FULL ログメッセージの全フィールドを保存する。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保存される。

MODULE 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。

REVERSE ログメッセージを逆順 (新しい順) に保存する。

SEVERITY メッセージのログレベル。E (Error)、W (Warning) または I (Information) で指定。省略時はすべてのログレベルにマッチする。

OVERWRITE このオプションを指定すると、同じファイル名のログファイルがあった場合、上書き保存される。(このオプションを指定しないと、同じファイル名のログファイルがあった場合には、メッセージが表示されてログファイルは作成されない)

入力・出力・画面例

```
# save log filename=test.log
This operation can take a long time. Do you want to continue? [Yes/No] -> YES
Saving log to file...Complete
```

関連コマンド

PURGE LOG (171 ページ)

SHOW LOG (264 ページ)

SET ASYN

カテゴリー：運用・管理 / 非同期ポート

```
SET ASYN [PROMPT={string|NONE|DEFAULT|OFF}] [SPEED={1200|2400|4800|9600|  
19200|38400|57600|115200}]
```

string: 文字列 (1~16 文字。空白を含む場合はダブルクォートで囲む)

解説

非同期ポートの設定パラメーターを変更する。
本コマンドで変更した設定内容はただちに有効となる。

パラメーター

PROMPT プロンプト文字列。DEFAULT、NONE、OFF を指定するとデフォルトに戻る。
SPEED 非同期ポートの通信速度。指定できる通信速度は機種によって異なる。未サポートの速度を指定した場合は、エラーメッセージが表示されコマンドは無視される。デフォルトは 9600。

入力・出力・画面例

```
# set asyn prompt=kumanomi  
kumanomi#
```

例

プロンプト文字列に、「kumanomi」を指定する。

```
SET ASYN PROMPT=kumanomi
```

関連コマンド

SHOW ASYN (230 ページ)

SET AUTHENTICATION

カテゴリー：運用・管理 / 認証サーバー

SET AUTHENTICATION [METHOD=RADIUS] [SECRET=*secret*] [TIMEOUT=1..60]

secret: 共有パスワード (1~39 文字。使用可能な文字は半角英数字、半角記号 (!#\$%&'()=^-_@' {+*} [;:] , . - < > ?) 大文字・小文字を区別する。文字列に半角空白、= < > ! ? を含む場合は、前後をダブルクォート (") で囲む必要がある。文字列中にダブルクォートを含んではならない)

解説

認証モードの設定を変更する。

パラメーター

METHOD RADIUS を指定する。

SECRET RADIUS サーバーとの通信に使う共有パスワード。デフォルトは AT1。

TIMEOUT 1~60 (秒) の範囲で指定する。デフォルトは 6 秒。SET RADIUSSERVER コマンドの TIMEOUT パラメーターと同義。

関連コマンド

SHOW AUTHENTICATION (231 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={*[device:]filename*|NONE}

device: ファイルが記憶されている媒体。flash を指定

filename: ファイル名 (1~28 文字。英数字と記号 (` ' @ # \$ % ^ & () _ - { }) が使用可能。拡張子は.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)。NONE を指定した場合は、起動時設定ファイルの設定がなしになる。ただし、boot.cfg という名前のファイルが存在した場合は、起動時に自動実行される。

備考・注意事項

存在しないファイルを指定して本コマンドを実行した後、SHOW CONFIG コマンドで確認すると、「Boot configuration file」欄のファイル名の後に、(Not found) と表示される。

上記の状態です再起動すると、boot.cfg という名前のファイルが存在する/しないに関わらず、Default の設定で起動する。

関連コマンド

CREATE CONFIG (91 ページ)

RESTART (183 ページ)

SHOW CONFIG (235 ページ)

SET DOS

カテゴリー：運用・管理 / 攻撃検出

SET DOS [IPADDRESS=*ipadd*] [SUBNET=*ipadd*] [UPLINKPORT=*port-number*]

ipadd: IP アドレス

port-number: スイッチポート番号 (1~)

解説

攻撃検出機能に関する設定を行う。

Smurf Attack および Land Attack 検出に関して、IP アドレスとサブネットマスクを設定する。また、Land Attack に関しては、アップリンクポートも指定する。

パラメーター

IPADDRESS IP アドレス。スイッチに接続されているデバイスの1つ (最も小さいアドレスが望ましい) の IP アドレスを指定。

SUBNET サブネットマスク。スイッチが属するネットワークのサブネットマスクを指定。たとえば、スイッチに接続されているデバイスのアドレスが、192.168.1.1 ~ 192.168.1.255 の範囲であった場合、サブネットマスクには、255.255.255.0 を指定する。

UPLINKPORT ルーターなどに接続されているポートを指定。指定できるのは1ポート。このパラメーターは、Land attack の通知設定に使用される。

例

Land attack の通知設定のために、IP アドレスに 192.168.10.1、サブネットに 255.255.255.0、アップリンクポートにポート 24 を指定する。

```
SET DOS IPADDRESS=192.168.10.1 SUBNET=255.255.255.0 UPLINKPORT=24
```

関連コマンド

SHOW DOS (241 ページ)

SET DOS IPOPTION

カテゴリー：運用・管理 / 攻撃検出

```
SET DOS IPOPTION PORT={port-list|ALL} [STATE={ENABLE|DISABLE}]  
[MIRRORING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}]
```

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

IP Options Attack 検出に関する設定を行う。

パラメーター

PORT 対象ポートを指定。

STATE IP Options Attack に対する攻撃検出機能の有効・無効を設定。ENABLE(有効)または DISABLE(無効)を指定する。デフォルトは DISABLE(無効)。

MIRRORING 不正パケットをミラーリングする・しないを設定。実際にミラーリングを開始するには、SET SWITCH MIRROR コマンドでミラーポートを設定する。

例

対象ポートにポート 5、7 を指定し、機能を有効にする。

```
SET DOS IPOPTION PORT=5,7 STATE=ENABLE
```

関連コマンド

SHOW DOS IPOPTION (243 ページ)

SET DOS LAND

カテゴリー：運用・管理 / 攻撃検出

```
SET DOS LAND PORT={port-list|ALL} [STATE={ENABLE|DISABLE}]  
[MIRRORING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}]
```

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

Land Attack 検出に関する設定を行う。

パラメーター

PORT 対象ポートを指定。

STATE Land Attack に対する攻撃検出機能の有効・無効を設定。ENABLE (有効) または DISABLE (無効) を指定する。デフォルトは DISABLE (無効)。

MIRRORING 不正パケットをミラーリングする・しないを設定。実際にミラーリングを開始するには、SET SWITCH MIRROR コマンドでミラーポートを設定する。

例

対象ポートにポート 5 と 7 を指定し、機能を有効にする。

```
SET DOS LAND PORT=5,7 STATE=ENABLE
```

関連コマンド

SET DOS (189 ページ)

SHOW DOS (241 ページ)

SHOW DOS LAND (245 ページ)

SET DOS PINGOFDEATH

カテゴリー：運用・管理 / 攻撃検出

```
SET DOS PINGOFDEATH PORT={port-list|ALL} [STATE={ENABLE|DISABLE}]  
[MIRRORING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}]
```

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

Ping of Death 攻撃検出に関する設定を行う。

パラメーター

PORT 対象ポートを指定。

STATE Ping of Death に対する攻撃検出機能の有効・無効を設定。ENABLE (有効) または DISABLE (無効) を指定する。デフォルトは DISABLE (無効)。

MIRRORING 不正パケットをミラーリングする・しないを設定。実際にミラーリングを開始するには、SET SWITCH MIRROR コマンドでミラーポートを設定する。

例

対象ポートにポート 1、5 を指定し、機能を有効にする。

```
SET DOS PINGOFDEATH PORT=1,5 STATE=ENABLE
```

備考・注意事項

この機能は、CPU に負荷が集中するため、この機能を必要とするポート以外では、この機能を有効にしないことを推奨。

関連コマンド

SHOW DOS PINGOFDEATH (247 ページ)

SET DOS SMURF

カテゴリー：運用・管理 / 攻撃検出

```
SET DOS SMURF PORT={port-list|ALL} STATE={ENABLE|DISABLE}
```

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

Smurf Attack 検出に関する設定を行う。

パラメーター

PORT 対象ポートを指定。

STATE Smurf Attack に対する攻撃検出機能の有効・無効を設定。ENABLE (有効) または DISABLE (無効) を指定する。デフォルトは DISABLE (無効)。

例

対象ポートにポート 18~20 を指定し、機能を有効にする。

```
SET DOS SMURF PORT=18-20 STATE=ENABLE
```

関連コマンド

SET DOS (189 ページ)

SHOW DOS (241 ページ)

SHOW DOS SMURF (249 ページ)

SET DOS SYNFLOOD

カテゴリー：運用・管理 / 攻撃検出

```
SET DOS SYNFLOOD PORT={port-list|ALL} STATE={ENABLE|DISABLE}
```

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

SYN Flood Attack 検出に関する設定を行う。

パラメーター

PORT 対象ポートを指定。

STATE SYN Flood Attack に対する攻撃検出機能の有効・無効を設定。ENABLE(有効)または DISABLE(無効)を指定する。デフォルトは DISABLE(無効)。

例

対象ポートにポート 18~20 を指定し、機能を有効にする。

```
SET DOS SYNFLOOD PORT=18-20 STATE=ENABLE
```

関連コマンド

SHOW DOS SYNFLOOD (251 ページ)

SET DOS TEARDROP

カテゴリー：運用・管理 / 攻撃検出

```
SET DOS TEARDROP PORT={port-list|ALL} [STATE={ENABLE|DISABLE}]  
[MIRRORING={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}]
```

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

Teardrop Attack 検出に関する設定を行う。

パラメーター

PORT 対象ポートを指定。

STATE Teardrop Attack に対する攻撃検出機能の有効・無効を設定。ENABLE (有効) または DISABLE (無効) を指定する。デフォルトは DISABLE (無効)。

MIRRORING 不正パケットをミラーリングする・しないを設定。実際にミラーリングを開始するには、SET SWITCH MIRROR コマンドでミラーポートを設定する。

例

対象ポートにポート 24 を指定し、機能を有効にする。

```
SET DOS TEARDROP PORT=24 STATE=ENABLE
```

備考・注意事項

この機能は、CPU に負荷が集中するため、一度に機能を有効にするポートは、アップリンクポートともう 1 ポートにとどめることを推奨。

関連コマンド

SHOW DOS TEARDROP (253 ページ)

SET ENCO KEY

カテゴリー：運用・管理 / 鍵作成・管理

SET ENCO KEY=*key-id* [DESCRIPTION=*string*]

key-id: 鍵番号 (0~65535)

string: 文字列 (1~127 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む)

解説

既存鍵の説明文を変更する。

パラメーター

KEY 鍵番号。

DESCRIPTION 鍵の説明。

関連コマンド

CREATE ENCO KEY (92 ページ)

DESTROY ENCO KEY (123 ページ)

SHOW ENCO KEY (255 ページ)

SET LOG FULLACTION

カテゴリー：運用・管理 / ログ

SET LOG FULLACTION [TEMPORARY={HALT|WRAP}] [PERMANENT={HALT|WRAP}]

解説

ログメッセージが最大保存数を超えた場合の保存方法を指定する。

パラメーター

TEMPORARY 出力先が TEMPORARY のログメッセージ (RAM 上に保存されるメッセージ) が、最大保存数を超えた場合の保存方法。HALT (最大件数を超過したログは保存しない) または、WRAP (最大件数を超過した場合、古いログから順に上書きしていく) のどちらかを選択。デフォルトは、WRAP。

PERMANENT 出力先が PERMANENT のログメッセージ (NVS 上に保存されるメッセージ) が、最大保存数を超えた場合の保存方法。HALT (最大件数を超過したログは保存しない) または、WRAP (最大件数を超過した場合、古いログから順に上書きしていく) のどちらかを選択。デフォルトは、WRAP。

例

TEMPORARY のログメッセージが最大保存数を超えた場合に、超過したログを破棄する。

```
SET LOG FULLACTION TEMPORARY=HALT
```

関連コマンド

SHOW LOG STATUS (269 ページ)

SET LOG OUTPUT

カテゴリー：運用・管理 / ログ

```
SET LOG OUTPUT=output-id [DESTINATION=SYSLOG] [SERVER=ipadd]
[FACILITY={DEFAULT|LOCAL1|LOCAL2|LOCAL3|LOCAL4|LOCAL5|LOCAL6|LOCAL7}]
[SYSLOGFORMAT={NORMAL|EXTENDED}] [MODULE={ALL|module-list}]
[SEVERITY={ALL|severity-list}]
```

output-id: ログ出力 ID (2~20)

ipadd: IP アドレス

module-list: モジュール名 (カンマを使った複数指定も可)

severity-list: ログレベル (E,W,I で指定。カンマを使った複数指定も可)

解説

syslog サーバーの設定および syslog サーバーの出力先定義を変更する。

パラメーター

OUTPUT ログ出力先 ID。2~20 の任意の番号を指定する。

DESTINATION ログメッセージの出力先。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) を指定する。

SERVER DESTINATION が SYSLOG の場合に、メッセージの転送先 IP アドレスを指定する。syslog サーバー (UDP 514 番) を指定する。

FACILITY syslog メッセージのファシリティコードを指定する。DEFAULT の場合は、既定のマッピング (解説編参照) にしたがって各メッセージのファシリティコードが決まる。LOCAL1~LOCAL7 を指定した場合は、本出力先宛てのすべての syslog メッセージで指定したファシリティコードが使用される。デフォルトは DEFAULT (既定のマッピングによってファシリティコードを決定)。

SYSLOGFORMAT syslog メッセージのフォーマット。EXTENDED (時刻情報とシステム名 (sysName) が付加される) と NORMAL (既存のフォーマット) から選択する。デフォルトは EXTENDED。

MODULE モジュール名。

SEVERITY メッセージのログレベル。

関連コマンド

CREATE LOG OUTPUT (94 ページ)

DESTROY LOG OUTPUT (124 ページ)

SHOW LOG OUTPUT (267 ページ)

SET MGMTACL

カテゴリー：運用・管理 / マネージメントアクセスコントロール

```
SET MGMTACL ID=1..256 [PORTLIST={port-list|ALL}] [IPADDRESS=ipadd]
[MASK=ipadd] [APPLICATION={TELNET|PING|ALL}]
```

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)

ipadd: IP アドレス

解説

Management ACL (マネージメントアクセスコントロールリスト) のアクセス制御エントリの設定を変更する。

パラメーター

ID エントリ番号

PORTLIST 受信スイッチポート番号。省略した場合は ALL が指定される

IPADDRESS 始点 IP アドレス。省略した場合は「0.0.0.0」が指定される

MASK IPADDRESS パラメーターで指定した IP アドレスのマスク (IP アドレスのどの部分をフィルタリング条件として有効にするか) を指定する。特定の機器の IP アドレスだけを指定したい場合は「255.255.255.255」を指定する。また、192.168.20.0/24 のようなサブネットを指定したい場合は「255.255.255.0」を指定する。省略した場合は「0.0.0.0」が指定される

APPLICATION アクセスを許可するパケットの種類。指定値については、CREATE MGMTACL コマンドのページに掲載されている表を参照

例

エントリ「10」で許可する機器の IP アドレスを 192.168.1.20 に変更する。

```
SET MGMTACL ID=10 IPADDRESS=192.168.1.20 MASK=255.255.255.255
```

関連コマンド

CREATE MGMTACL (96 ページ)

SHOW MGMTACL (270 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

現在ログインしているユーザーのパスワードを変更する。
プロンプトが表示されるので、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

```
# set password
Enter current manager password->***** (現在のパスワードを入力。*で表示される)
Enter new manager password->***** (新しいパスワードを入力。*で表示される)
Re-enter manager password ->***** (確認のため、新しいパスワードをもう一度入力)
```

備考・注意事項

文字列を入力しない(0文字)とパスワードが設定されないのに注意。
文字列を入力しない(0文字)ときは、SET USERCONFIG コマンドの MINPWDLEN パラメーターを0に設定する。
ユーザー情報、パスワードは、CREATE CONFIG コマンドや SAVE CONFIGURATION コマンドを実行することにより設定ファイルに保存される。

関連コマンド

SET USER (227 ページ)

SET PKI CERTIFICATE

カテゴリー：運用・管理 / PKI

SET PKI CERTIFICATE=string [TRUSTED={YES|NO|ON|OFF|TRUE|FALSE}]
 [TYPE={CA|EE|SELF}]

string: 証明書の名前 (1~24 文字。使用可能な文字は半角英数字 (大文字・小文字を区別する)、半角記号 (# \$ % & ' () ~ | - ^ \ @ ' { + * } [; :] , . / -)。文字列に半角空白、!= を含む場合は、前後をダブルクォート (") で囲む必要がある。)

解説

証明書データベースに登録されている公開鍵証明書の信頼レベルおよびタイプを変更する。

パラメーター

CERTIFICATE 証明書データベースで表示される証明書の名前。

TRUSTED デジタル証明書の発行元が信用できるかどうか。YES/ON/TRUE、NO/OFF/FALSE で設定する。デフォルトは YES/ON/TRUE。

TYPE デジタル証明書のタイプを指定する。CA (認証局が発行した証明書)、EE (認証局以外が発行した証明書)、SELF (本製品が発行した証明書) から選択。デフォルトは EE。

関連コマンド

ADD PKI CERTIFICATE (81 ページ)
 CREATE PKI CERTIFICATE (98 ページ)
 CREATE PKI ENROLLMENTREQUEST (99 ページ)
 DELETE PKI CERTIFICATE (117 ページ)
 SHOW PKI CERTIFICATE (272 ページ)

SET RADIUSACCOUNTING

カテゴリー：運用・管理 / 認証サーバー

```
SET RADIUSACCOUNTING [SERVERPORT=port] [TYPE=NETWORK]  
  [TRIGGER={START_STOP|STOP_ONLY}] [UPDATEENABLE={ENABLED|DISABLED}]  
  [INTERVAL=30..300]
```

port: UDP ポート番号 (1 ~ 65535)

解説

RADIUS (Remote Authentication Dial In User Server) サーバーのアカウントिंग機能の設定を変更する。

パラメーター

SERVERPORT RADIUS サーバーのアカウントिंग用 UDP ポート番号。デフォルトは 1813 番。

TYPE アカウントिंग情報を転送して蓄積する場所を指定する。NETWORK (アカウントिंगサーバー) のみが指定可能。

TRIGGER アカウントिंग要求パケットをサーバーに送出するタイミングを設定する。START_STOP (利用開始時と終了時にパケット送信) と STOP_ONLY (利用終了時にのみパケット送信) から選択。デフォルトは、START_STOP。

UPDATEENABLE ユーザーが利用中に、利用状況をサーバーに送信するアカウントिंग要求 (インターリム) パケットを送信するかどうかを指定する。ENABLED (送信する) か DISABLED (送信しない) から選択。デフォルトは、DISABLED。

INTERVAL インターリムパケットを送信する間隔を設定する。30 ~ 300 (秒) の範囲で設定。デフォルトは、60 (秒)。

関連コマンド

SHOW RADIUSACCOUNTING (275 ページ)

SET RADIUSSERVER

カテゴリ：運用・管理 / 認証サーバー

SET RADIUSSERVER [TIMEOUT=1..60] [DEADTIME=0..1440]
[RETRANSMITCOUNT=1..5]

解説

RADIUS クライアントのパラメーターを設定する。

パラメーター

TIMEOUT RADIUS Access-Request へのレスポンス待ち時間 (秒)。デフォルトは 6 秒。SET AUTHENTICATION コマンドの TIMEOUT パラメーターと同義。

DEADTIME RADIUS サーバーからの応答が無い場合、指定された時間 (分) は当該 RADIUS サーバーへのリクエストを行わない。デフォルトは、0 分 (Deadtime 無し)。

RETRANSMITCOUNT RADIUS サーバーからの応答が無い場合、指定された回数の再送を行う。デフォルトは 3 回。

関連コマンド

ADD RADIUSSERVER (82 ページ)

DELETE RADIUSSERVER (118 ページ)

SHOW AUTHENTICATION (231 ページ)

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 (1~32 文字。英数字が使用可能。大文字・小文字を区別する。)"(ダブルクォート) [] (スクエアブラケット) \ (バックスラッシュ、円マーク) 半角スペースは使用できない)

解説

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 (100 ページ)

DESTROY SNMP COMMUNITY (126 ページ)

SHOW SNMP COMMUNITY (278 ページ)

SET SNMPV3 ACCESS

カテゴリー：運用・管理 / SNMP

```
SET SNMPV3 ACCESS=group SECURITYMODEL={V1|V2C|V3}
    SECURITYLEVEL={NOAUTHENTICATION|AUTHENTICATION|PRIVACY} [READVIEW=view]
    [WRITEVIEW=view] [NOTIFYVIEW=view] [STORAGETYPE={VOLATILE|NONVOLATILE}]
```

group: SNMP グループ名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

view: SNMP ビュー名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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

ACCESS SNMP グループ名。

SECURITYMODEL 本グループ所属のユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。

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。NOAUTHENTICATION (認証なし、暗号化なし)、AUTHENTICATION (認証あり、暗号化なし)、PRIVACY (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、CREATE SNMPV3 VIEW コマンドで定義する。指定がない場合、本グループ所属のユーザーは、MIB オブジェクトを読み出せない。

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、CREATE SNMPV3 VIEW コマンドで定義する。指定がない場合、本グループ所属のユーザーは、MIB オブジェクトを書き込めない。

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、CREATE SNMPV3 VIEW コマンドで定義する。指定がない場合、本グループ所属のユーザーは、MIB オブジェクトの通知を受け取れない。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

関連コマンド

CREATE SNMPV3 ACCESS (102 ページ)

SHOW SNMPV3 ACCESS (282 ページ)

SET SNMPV3 COMMUNITY

カテゴリー：運用・管理 / SNMP

```
SET SNMPV3 COMMUNITY INDEX=index [COMMUNITYNAME=community]
  [SECURITYNAME=username] [TRANSPORTTAG=tag] [STORAGETYPE={VOLATILE|
  NONVOLATILE}]
```

index: インデックス名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

community: SNMP コミュニティー名 (1~63 文字。英数字が使用可能。大文字・小文字を区別する。"(ダブルクォート) [] (スクエアブラケット) \ (バックスラッシュ、円マーク) 半角スペースは使用できない)

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

tag: トランスポート名 (1~255 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) SNMP コミュニティーの設定を変更する。

パラメーター

INDEX コミュニティー名。

COMMUNITYNAME コミュニティーに対するパスワードを指定する。

SECURITYNAME SNMPv1 および v2c のユーザー名を指定する。(ADD SNMPV3 USER コマンドで作成したユーザー名は指定しない)。

TRANSPORTTAG タグ名。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP コミュニティー「Index3」のパスワードの設定を変更する。

```
SET SNMPV3 COMMUNITY INDEX=Index3 COMMUNITYNAME=kumakuma
  SECURITYNAME=test TRANSPORTTAG=trans STORAGETYPE=nonvolatile
```

備考・注意事項

SNMPv1/v2c 用にデフォルトで設定されているコミュニティ「public」「private」の設定を変更することはできない。

関連コマンド

CREATE SNMPV3 COMMUNITY (104 ページ)

SHOW SNMPV3 COMMUNITY (284 ページ)

SET SNMPV3 GROUP

カテゴリー：運用・管理 / SNMP

```
SET SNMPV3 GROUP USERNAME=username SECURITYMODEL={V1|V2C|V3}  
[GROUPNAME=group] [STORAGETYPE={VOLATILE|NONVOLATILE}]
```

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

group: SNMP グループ名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) ユーザーとユーザーグループの対応付けの設定を変更する。

パラメーター

USERNAME SNMP ユーザー名。ユーザーは、ADD SNMPV3 USER コマンドで定義する。

SECURITYMODEL 本グループ所属のユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。

GROUPNAME SNMP グループ名。グループは、CREATE SNMPV3 ACCESS コマンドで定義する。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP ユーザー「systemadmin24」の対応を SNMP グループ「operators」に変更する。

```
SET SNMPV3 GROUP USERNAME=systemadmin24 SECURITYMODEL=V3 GROUP=operators  
STORAGETYPE=nonvolatile
```

関連コマンド

DESTROY SNMPV3 GROUP (129 ページ)

SHOW SNMPV3 GROUP (287 ページ)

SET SNMPV3 NOTIFY

カテゴリー：運用・管理 / SNMP

```
SET SNMPV3 NOTIFY=notify [TAG=tag] [TYPE={TRAP|INFORM}]
[STORAGETYPE={VOLATILE|NONVOLATILE}]
```

notify: 通知名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

tag: タグ名 (1~255 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) 通知名の定義を変更する。

パラメーター

NOTIFY 通知名。

TAG タグ名。

TYPE 通知メッセージのフォーマットを指定する。TRAP (トラップ) または INFORM (インフォメーション) かを選択する。デフォルトは、TRAP (トラップ)。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

通知名「sysadmintrap」のタグ名の設定を変更する。

```
SET SNMPV3 NOTIFY=sysadmintrap TAG=testtag TYPE=TRAP
STORAGETYPE=nonvolatile
```

関連コマンド

CREATE SNMPV3 NOTIFY (107 ページ)

DESTROY SNMPV3 NOTIFY (130 ページ)

SHOW SNMPV3 NOTIFY (289 ページ)

SET SNMPV3 TARGETADDR

カテゴリー：運用・管理 / SNMP

SET SNMPV3 TARGETADDR=target PARAMS=params IPADDRESS=ipadd

[UDPPORT=0..65535] [TIMEOUT=0..2147483647] [RETRIES=0..255]
[TAGLIST=tag] [STORAGETYPE={VOLATILE|NONVOLATILE}]

target: SNMP ターゲット名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

ipadd: IP アドレス

tag: タグ名 (1~255 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する。複数のタグを指定する場合はスペースで区切る)

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。CREATE SNMPV3 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。

IPADDRESS ターゲットの IP アドレス。

UDPPORT ターゲットのリスニング UDP ポート。0~65535 の範囲を指定する。デフォルトは、162。

TIMEOUT インフォームメッセージを送信し、返信を受け取るまでのタイムアウト時間 (単位はミリ秒) を指定。デフォルトは、1500 (ミリ秒)。

RETRIES インフォームメッセージを再送する回数を指定。デフォルトは、3 (回)。

TAGLIST タグ名。CREATE SNMPV3 NOTIFY コマンド、または、CREATE SNMPV3 COMMUNITY コマンドで定義したタグ名を指定する。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP ターゲット「host451」の IP アドレスの設定を変更する。

```
SET SNMPV3 TARGETADDR=host451 PARAMS=SNMPmanagerPC
IPADDRESS=192.168.1.200 STORAGETYPE=nonvolatile
```

関連コマンド

CREATE SNMPV3 TARGETADDR (108 ページ)

SHOW SNMPV3 TARGETADDR (290 ページ)

SET SNMPV3 TARGETPARAMS

カテゴリー：運用・管理 / SNMP

```
SET SNMPV3 TARGETPARAMS=params [USERNAME=username] [SECURITYMODEL={V1|
V2C|V3}] [MESSAGEPROCESSING={V1|V2C|V3}]
[SECURITYLEVEL={NOAUTHENTICATION|AUTHENTICATION|PRIVACY}]
[STORAGETYPE={VOLATILE|NONVOLATILE}]
```

params: SNMP ターゲットパラメーターセット名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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の設定を変更する。

パラメーター

TARGETPARAMS SNMP ターゲットパラメーターセット名。

USERNAME SNMP ユーザー名。ユーザーは、ADD SNMPV3 USER コマンドで定義する。

SECURITYMODEL SNMP ユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。

MESSAGEPROCESSING SECURITYMODEL に V1 または V2C を指定した場合に、処理やメッセージ送信に使用する SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。SECURITYMODEL に V3 を指定した場合は、自動的に V3 が指定される。

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ーレベルを指定する。NOAUTHENTICATION (認証なし・暗号化なし)、AUTHENTICATION (認証あり・暗号化なし)、PRIVACY (認証あり・暗号化あり) から選択する。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP ターゲットパラメーターセット「SNMPmanagerPC」の SECURITYLEVEL の設定を変更する。

```
SET SNMPV3 TARGETPARAMS=SNMPmanagerPC USERNAME=systemadmin24
  SECURITYMODEL=V3 MESSAGEPROCESSING=V3 SECURITYLEVEL=AUTHENTICATION
  STORAGETYPE=nonvolatile
```

関連コマンド

CREATE SNMPV3 TARGETPARAMS (110 ページ)

SHOW SNMPV3 TARGETPARAMS (292 ページ)

SET SNMPV3 USER

カテゴリ：運用・管理 / SNMP

```
SET SNMPV3 USER=username [AUTHENTICATION={MD5|SHA}]
    [AUTHPASSWORD=password] [PRIVPASSWORD=password] [STORAGETYPE={VOLATILE|
    NONVOLATILE}]
```

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

password: パスワード (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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。

AUTHENTICATION 認証プロトコル。MD5、SHA から選択する。このパラメーターを指定しないと、NONE (認証なし) になる。

AUTHPASSWORD 認証パスワード。AUTHENTICATION に、MD5 か SHA を指定した場合の必須パラメーター。

PRIVPASSWORD 暗号化パスワード。暗号化パスワードを指定すると、暗号化あり (DES) になる。AUTHENTICATION が NONE (認証なし) の場合は、指定できない。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP ユーザー「systemadmin24」の認証プロトコルの設定を変更する。

```
SET SNMPV3 USER=systemadmin24 AUTHENTICATION=SHA AUTHPASSWORD=kumakuma
    STORAGETYPE=nonvolatile
```

関連コマンド

ADD SNMPV3 USER (85 ページ)

SHOW SNMPV3 USER (294 ページ)

SET SNMPV3 VIEW

カテゴリー：運用・管理 / SNMP

```
SET SNMPV3 VIEW=view [SUBTREE={node-oid|node-name}] [MASK=mask]
[TYPE={INCLUDED|EXCLUDED}] [STORAGETYPE={VOLATILE|NONVOLATILE}]
```

view: SNMP ビュー名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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 (規定のノード名)

mask: MIB ノード OID のマスク (xx:xx:xx 形式で、16 進数値で指定。長さは OID の長さに応じて変更可能)

解説

(SNMPv3) ビューの設定を変更する。

パラメーター

VIEW SNMP ビュー名。

SUBTREE MIB ノードを OID (Object Identifier) または名前 (internet など) で指定する。

MASK MIB ノード OID のマスク。16 進数値で指定。たとえば、1.3.6.1 の 6 の部分をマスクしたい場合、「1101 (2) = D (16)」となり、「DF (16)」と指定する。xx:xx:xx までの長さが足りない場合は、1 バイト単位で省略可能。

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。

STORAGETYPE 設定を保存する (NONVOLATILE) か、保存しない (VOLATILE) かを選択する。デフォルトは、VOLATILE (保存しない)。

例

SNMP ビュー「standard」の TYPE の設定を変更する。

```
SET SNMPV3 VIEW=standard SUBTREE=1.3.6.1.2.1 TYPE=EXCLUDED
STORAGETYPE=nonvolatile
```

関連コマンド

CREATE SNMPV3 VIEW (112 ページ)

DESTROY SNMPV3 VIEW (133 ページ)

SHOW SNMPV3 VIEW (296 ページ)

SET SNTP

カテゴリ：運用・管理 / SNTP

SET SNTP [DST={ENABLED|DISABLED}] [POLLINTERVAL=60..1200]
[UTCOFFSET=-12..12]

解説

Sntp に関する設定を変更する。

Sntp で扱われる時間はすべて UTC なので、必ず現地時間と協定世界時 (UTC) の差 (オフセット) を設定する必要がある。

パラメーター

DST Daylight Savings Time (DST) サマータイムの有効 (ENABLED)、無効 (DISABLED) を設定する。デフォルトは、無効。

POLLINTERVAL Sntp サーバーから時刻を取得する時間間隔。60 ~ 1200 (秒) で指定する。デフォルトは 600。

UTCOFFSET 協定世界時からのオフセットを指定する。-12 ~ +12 までの時間差で指定する。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。デフォルトは 0。

+8:00	Asia
+10:30	Australian Central Daylight Time
+9:30	Australian Central Standard Time
+11:00	Australian Eastern Daylight Time
+10:00	Australian Eastern Standard Time
+8:00	Australian Western Standard Time
+1:00	British Standard Time
+8:00	China
+0:00	Greenwich Mean Time
+0:00	Greenwich Mean Time
+8:00	Hong Kong
+9:00	Japan Standard Time
+1:00	Mid-European time
+13:00	New Zealand Daylight Time
+12:00	New Zealand Standard Time
+8:00	Singapore

+8:00	Taiwan
+0:00	Universal Coordinated Time
-5:00	US Central Daylight Time
-6:00	US Central Standard Time
-4:00	US Eastern Daylight Time
-5:00	US Eastern Standard Time
-6:00	US Mountain Daylight Time
-7:00	US Mountain Standard Time
-7:00	US Pacific Daylight Time
-8:00	US Pacific Standard Time

表 24: 時間差一覧

例

UTC オフセットを時間差で指定する (日本)。

```
SET NTP UTCOFFSET=9
```

関連コマンド

SHOW SNTP (298 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 (0 ~ 5 時間)

seconds: 時間 (60 ~ 600 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を 60 ~ 600 (秒) で指定する。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 180 秒。

関連コマンド

DISABLE SSH SERVER (145 ページ)

ENABLE SSH SERVER (159 ページ)

SHOW SSH (299 ページ)

SET SWITCH CONSOLETIMER

カテゴリー：運用・管理 / 非同期ポート

SET SWITCH CONSOLETIMER=1..60

解説

コンソールのタイムアウト時間を設定する。

パラメーター

CONSOLETIMER コンソールのタイムアウト時間を、1～60（分）で指定する。デフォルトは10。

例

コンソールのタイムアウト時間を20（分）に指定する。

SET SWITCH CONSOLETIMER=20

関連コマンド

SHOW SWITCH（「スイッチング」の186ページ）

SET SWITCH STACKMODE

カテゴリー：運用・管理 / エンハンススタッキング

SET SWITCH STACKMODE={MASTER|SLAVE|UNAVAILABLE}

解説

本製品のエンハンススタッキンググループ内での役割を指定する。

パラメーター

STACKMODE エンハンススタッキンググループ内での役割を指定。MASTER(他のスイッチを制御するための使用するスイッチ)、SLAVE(MASTERから制御可能なスイッチ)またはUNAVAILABLE(エンハンススタッキンググループに属さないスイッチ)から選択する。デフォルトは、SLAVE。

例

MASTER スイッチに設定する。

```
SET SWITCH STACKMODE=MASTER
```

関連コマンド

SHOW REMOTELIST (276 ページ)

SET SYSTEM CONTACT

カテゴリー：運用・管理 / システム

SET SYSTEM CONTACT={*string*|NONE}

string: 文字列 (0~39 文字。使用可能な文字は半角英数字、半角記号 (!#\$%&'()=~/^-`@\`{+*}[;:],.-<>?)、文字列に半角空白、=<>!?を含む場合は、前後をダブルクォート(")で囲む必要がある。文字列中にダブルクォートを含んではならない。)

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)。設定なし (デフォルト) には、「set system contact=NONE」と入力する。

例

sysContact を設定する。

```
SET SYSTEM CONTACT="admin@1sys.mydomain.com"
```

関連コマンド

SET SYSTEM LOCATION (223 ページ)

SET SYSTEM NAME (224 ページ)

SHOW SYSTEM (301 ページ)

SET SYSTEM DISTINGUISHEDNAME

カテゴリー：運用・管理 / システム

SET SYSTEM DISTINGUISHEDNAME={*string*|NONE}

string: X.500 識別名 (DN)。1~128 文字 (CN (Common Name、64 文字)、OU (Organizational Unit、64 文字)、O (Organization、64 文字)、L (Locality、64 文字)、ST (State or Province、64 文字)、C (Country、2 文字) を入力可能)。使用可能な文字は半角英数字と半角記号 (! # \$ % & ' () = ~ | - ^ \ @ ' { + * } [; :] , . _ < > ? 半角空白)。前後をダブルクォート (") で囲み、各種属性値をカンマで区切って列挙。("cn=myname,o=myorg,c=jp" の形式)

解説

PKI 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)。各種属性値をカンマで区切って列挙したもの。

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"
```

備考・注意事項

X.500 識別名に「/」を使用することはできない。「/」は設定ファイルでは「,」に変換される。

関連コマンド

CREATE PKI CERTIFICATE (98 ページ)

CREATE PKI ENROLLMENTREQUEST (99 ページ)

SET SYSTEM LOCATION

カテゴリー：運用・管理 / システム

SET SYSTEM LOCATION={*string*|NONE}

string: 文字列 (0~39 文字。使用可能な文字は半角英数字、半角記号 (!#\$%&'()=^-`@\{+*}[;:],.-<>?)、文字列に半角空白、=<>!?を含む場合は、前後をダブルクォート(")で囲む必要がある。文字列中にダブルクォートを含んではならない。)

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)。設定なし (デフォルト) には、「set system location=NONE」と入力する。

例

sysLocation を設定する。

```
SET SYSTEM LOCATION="8F, TTT Bldg."
```

関連コマンド

SET SYSTEM CONTACT (221 ページ)

SET SYSTEM NAME (224 ページ)

SHOW SYSTEM (301 ページ)

SET SYSTEM NAME

カテゴリー：運用・管理 / システム

SET SYSTEM NAME={*string*|NONE}

string: 文字列 (0~39 文字。使用可能な文字は半角英数字、半角記号 (!#\$%&'()=~|^@\'+*}{;:] ,.-<>?)、文字列に半角空白、=<>!?を含む場合は、前後をダブルクォート(")で囲む必要がある。文字列中にダブルクォートを含んではならない。)

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。設定なし (デフォルト) にするには、「set system name=NONE」と入力する。

例

sysName を設定する。

```
SET SYSTEM NAME="white.mydomain.com"
```

備考・注意事項

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 (221 ページ)

SET SYSTEM LOCATION (223 ページ)

SHOW SYSTEM (301 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 INSERTNULL={ON|OFF}

解説

Telnet サーバー機能の設定を変更する。

パラメーター

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。

関連コマンド

ENABLE TELNET (161 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-mm-yyyy の形式。dd は日 (1~31) mm は月 (01~12) yyyy は西暦年 2035 まで)

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 2009 年 12 月 30 日 19 時に設定する。

```
SET DATE=30-12-2009 TIME=19:00:00
```

時刻だけを修正する。

```
SET TIME=19:02:00
```

備考・注意事項

SNTP 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 SNTP PEER (86 ページ)

ENABLE SNTP (158 ページ)

SHOW TIME (304 ページ)

SET USER

カテゴリ：運用・管理 / ユーザー認証データベース

```
SET USER={MANAGER|OPERATOR|login-name} [PASSWORD=password|NONE]
      [DESCRIPTION=string|NONE] [PRIVILEGE={MANAGER|USER}] [SESSIONTYPE={ALL|
      CONSOLE|TELNET|SSH|ENHANCEDSTACKING}]
```

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)

password: パスワード (1~32 文字。使用可能な文字は半角英数字、半角記号 (!#\$%&'()=~-^`@\'+*}{;:] ,.-<>?)、大文字・小文字を区別する。文字列に半角空白、=<>!?を含む場合は、前後をダブルクォート(")で囲む必要がある。文字列中にダブルクォートを含んではならない。)

string: 文字列 (1~24 文字。使用可能な文字は半角英数字、半角記号 (!#\$%&'()=~-^`@\'+*}{;:] ,.-<>?)、文字列に半角空白、=<>!?を含む場合は、前後をダブルクォート(")で囲む必要がある。文字列中にダブルクォートを含んではならない。)

解説

ユーザーアカウントの設定を変更する。

パラメーター

USER ログイン名。MANAGER、OPERATOR、または、ADD USER コマンドで追加したログイン名を指定する。

PASSWORD パスワード。大文字小文字を区別する。

DESCRIPTION ユーザーに関するコメントを変更する。DESCRIPTION を設定しない場合は NONE を指定する。

PRIVILEGE ユーザーレベルを変更する。一般ユーザー (USER)、管理者 (MANAGER) から選択する。

SESSIONTYPE ユーザーがログインできるセッションタイプを変更する。CONSOLE(シリアルポート)、TELNET、SSH、ENAHNCEDSTACKING から選択する。ALL を指定した場合はいずれのセッションタイプからもログインできる。複数のセッションタイプを指定する場合は「,」区切りで指定する。

例

MANAGER のユーザーパスワードを変更する。

```
SET USER=manager PASSWORD=panda
```

備考・注意事項

一般ユーザー (USER) は本コマンドを実行することができないため、パスワードを変更する際は、SET PASSWORD コマンドを実行する必要がある。

MANAGER レベルのユーザーを USER レベルに変更しようとしたとき、そのユーザーが MANAGER レベルで、かつ、システムで最後の有効な (Enable) ユーザーである場合は PRIVILEGE を USER レベルに変更することはできない。

パスワードをなしに設定 (PASSWORD=NONE) するときは、SET USERCONFIG コマンドの MIN-PWDLEN パラメーターを 0 に設定する。

ユーザー情報、パスワードは、CREATE CONFIG コマンドや SAVE CONFIGURATION コマンドを実行することにより設定ファイルに保存される。

関連コマンド

SHOW USER (305 ページ)

SET USERCONFIG

カテゴリー：運用・管理 / ユーザー認証データベース

SET USERCONFIG [LOGINFAIL=1..10] [LOCKOUTPD=1..3000] [MINPWDLEN=0..23]

解説

ユーザー認証機能の設定を変更する。

パラメーター

LOGINFAIL 連続したログイン失敗の回数を指定する。連続してこの回数ログインに失敗すると一定時間、失敗したセッション経由でログインできなくなる（ロックアウトされる）。デフォルトは5回。

LOCKOUTPD ロックアウトが発生した場合、次にログインを認めるまでの時間（秒）を指定する。デフォルトは600秒。

MINPWDLEN パスワードの最小文字数を指定する。ユーザーアカウントを作成する場合や、パスワード変更時、この値より短い文字数のパスワードを入力するとエラーとなる。デフォルトは6文字。

例

パスワードの最小文字数を5文字に設定する。

```
SET USERCONFIG MINPWDLEN=5
```

備考・注意事項

SSH 経由のログインには、LOGINFAIL は適用されない（LOGINFAIL 回連続してログインに失敗してもロックアウトは発生しない）。ただし、SSH サーバーの仕様として、50 回連続してログインに失敗するとSSH サーバー自体が無効化され、以後ログインできなくなる（ENABLE SSH SERVER コマンドのページも参照）。

関連コマンド

RESET USERCONFIG (182 ページ)

SHOW USERCONFIG (307 ページ)

SHOW ASYN

カテゴリー：運用・管理 / 非同期ポート

SHOW ASYN

解説

非同期ポートの情報を表示する。

入力・出力・画面例

```
# show asyn
Asynchronous Port (Console) Information:
  Baud Rate ..... 9600
  Parity ..... NONE
  Data bits ..... 8
  Stop bits ..... 1
  Prompt ..... "
```

Baud Rate	通信速度。デフォルトは 9600
Parity	パリティ設定
Data bits	1 キャラクターあたりデータビット数
Stop bits	1 キャラクターあたりストップビット数
Prompt	プロンプト文字列 (ユーザー定義文字列)

表 25:

関連コマンド

SET ASYN (186 ページ)

SHOW AUTHENTICATION

カテゴリー：運用・管理 / 認証サーバー

SHOW AUTHENTICATION

解説

認証モードの設定を表示する。

入力・出力・画面例

```
# show authentication

Authentication Information:
  Status ..... Disabled
  Authentication Method ..... RADIUS

RADIUS Configuration:
  Global Encryption Key ..... ATI
  Server Timeout ..... 6 seconds
  Server Deadtime ..... 0 minutes
  Server Retransmit Count ..... 3

RADIUS Servers:

Server IP Address  Auth Port  Encryption Key          Auth Req  Auth Resp
Local Interface    Source IP Address      DeadTime(sec)
-----
192.168.1.11      1812      test                    0         0
NONE              192.168.1.1          0
0.0.0.0          1812      <Not Defined>          0         0
0.0.0.0          1812      <Not Defined>          0         0
0.0.0.0          1812      <Not Defined>          0         0
```

Status	認証モードの状態。Disabled か Enabled
Authentication Method	認証プロトコル。RADIUS
Global Encryption Key	サーバー共通のパスワード
Server Timeout	サーバー共通のタイムアウト値
Server Deadtime	無応答の RADIUS サーバーへの要求送信抑制期間
Server Retransmit Count	RADIUS サーバーへの要求再送回数
Server IP Address	RADIUS サーバーの IP アドレス
Auth Ports	RADIUS サーバーの認証用 UDP ポート番号

Encryption Key	サーバー個別のパスワード
Auth Req	RADIUS サーバーに対して送った認証リクエストの数
Auth Resp	RADIUS サーバーから受け取った返信の数
Local Interface	ローカルインターフェース
Source IP Address	始点 IP アドレス
DeadTime(sec)	RADIUS サーバーからの応答が無い場合の再送を行うまでの秒数

表 26:

備考・注意事項

Auth Req と Auth Resp はユーザー認証のみカウントする。ポート認証はカウントしない。

関連コマンド

ADD RADIUSSERVER (82 ページ)
DELETE RADIUSSERVER (118 ページ)
DISABLE AUTHENTICATION (134 ページ)
ENABLE AUTHENTICATION (148 ページ)
SET AUTHENTICATION (187 ページ)
SET RADIUSSERVER (203 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

```
# show buffer
Memory Information:
Memory ( DRAM ) ..... 131072 kB
System Pool:
  Total memory ..... 111844 kB
  Free memory ..... 96481 kB (86 %)
Layer-3 Pool:
  Total memory ..... 4000 kB
  Free memory ..... 3049 kB (76 %)
SNMP Pool:
  Total memory ..... 1536 kB
  Free memory ..... 1467 kB (95 %)
SNMP Event Pool:
  Total memory ..... 64 kB
  Free memory ..... 63 kB (99 %)
Event Log Pool:
  Total memory ..... 448 kB
  Free memory ..... 409 kB (91 %)
Communication Buffer:
  Total buffer ..... 300
  Free buffer ..... 300
```

Memory (DRAM)	実装されている DRAM の容量
System Pool セクション	システムで利用するメモリープール
Total memory	システムプールの総メモリーサイズ
Free memory	システムプールの空きメモリーサイズ (%)
Layer-3 Pool セクション	レイヤー 3 関連モジュールが利用するメモリープール
Total memory	レイヤー 3 プールの総メモリーサイズ
Free memory	レイヤー 3 プールの空きメモリーサイズ (%)
SNMP Pool セクション	SNMP エージェントが利用するメモリープール
Total memory	SNMP プールの総メモリーサイズ

Free memory	SNMP プールの空きメモリーサイズ (%)
SNMP Event Pool セクション	SNMP トラップで利用するメモリープール
Total memory	SNMP イベントプールの総メモリーサイズ
Free memory	SNMP イベントプールの空きメモリーサイズ (%)
Event Log Pool セクション	イベントログで利用するメモリープール
Total memory	イベントログプールの総メモリーサイズ
Free memory	イベントログプールの空きメモリーサイズ (%)
Communication Buffer セクション	本体宛通信で利用する通信バッファ
Total buffer	通信バッファの総数
Free buffer	未使用の通信バッファ数

表 27:

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 該当モジュールの現在の設定内容を設定スクリプトの形式で表示する。指定しない場合はすべてのモジュールについて表示する。

入力・出力・画面例

```
# show config
Boot configuration file ..... "boot.cfg" (Exists)
Current configuration ..... "boot.cfg"

# show config dynamic
---Start of current configuration -----

#
# System Configuration
#

#
# User Authentication Configuration
#
set user=manager password=3af00c6cad11f7ab5db4467b66ce503eff
set user=operator password=4b583376b2767b923c3e1da60d10de59ff

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

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、「None」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 28:

関連コマンド

CREATE CONFIG (91 ページ)

RESTART (183 ページ)

SET CONFIG (188 ページ)

SHOW CPU

カテゴリー：運用・管理 / システム

SHOW CPU [HISTORY]

解説

CPU の使用状況を表示する。

パラメーター

HISTORY 過去 60 秒間、1 時間、30 時間の CPU 使用率の履歴をグラフ形式で表示。省略した場合は、過去 1 秒間、20 秒間、60 秒間の CPU の平均使用率を表示する。

入力・出力・画面例

```
# show cpu
CPU averages:
 1 second: 69%, 20 seconds: 69%, 60 seconds: 69%
#
# show cpu history
Per second CPU load history

100
 90
 80 *           *           *           *           *           *
 70 *****
 60
 50
 40
 30
 20
 10
 |...|...|...|...|...|...|...|...|...|...|...|...
 Oldest                                     Newest
      CPU load% per second (last 60 seconds)
        * = average CPU load%

Per minute CPU load history

100
 90
 80 ++++++
 70 *****
 60
```


* = average	過去 30 分間の平均 CPU 使用率
- = minimum	過去 30 分間の最低 CPU 使用率
+ = maximum	過去 30 分間の最高 CPU 使用率

表 30: HISTORY オプション指定時

SHOW DEBUG

カテゴリー：運用・管理 / システム

SHOW DEBUG

解説

デバッグ情報を表示する。

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。ご使用に際しては、弊社技術担当にご相談ください。

備考・注意事項

Continuous 選択後、表示を中断するには Ctrl/C キーを押す。

関連コマンド

SHOW EXCEPTIONLOG (256 ページ)

SHOW LOG (264 ページ)

SHOW SYSTEM (301 ページ)

SHOW DOS

カテゴリー：運用・管理 / 攻撃検出

SHOW DOS [IPADDRESS] [SUBNET] [UPLINKPORT]

解説

攻撃検出機能に関する設定を表示する。
オプションを省略した場合はすべての情報を表示する。

パラメーター

IPADDRESS 設定された IP アドレスを表示。
SUBNET 設定されたサブネットマスクを表示。
UPLINKPORT 設定されているアップリンクポートを表示。

入力・出力・画面例

```
# show dos ipaddress
Subnet Ip address is ..... 192.168.10.1

# show dos subnet
Subnet is ..... 255.255.255.0

# show dos uplinkport
Uplink Port is ..... 24
```

Subnet Ip address is	IP アドレス
----------------------	---------

表 31: IPADDRESS オプション指定時

Subnet is	サブネットマスク
-----------	----------

表 32: SUBNET オプション指定時

Uplink Port is	アップリンクポート
----------------	-----------

表 33: UPLINKPORT オプション指定時

関連コマンド

SHOW DOS

SET DOS (189 ページ)

SHOW DOS IPOPTION

カテゴリー：運用・管理 / 攻撃検出

SHOW DOS IPOPTION [PORT={*port-list*|ALL}]

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

IP Options Attack 検出に関する設定を表示する。

パラメーター

PORT ポート番号。複数指定が可能。ALL を指定した場合、省略した場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show dos ipoption
Port  Status      Mirroring
1     Disable     No
2     Disable     No
3     Disable     No
4     Disable     No
5     Disable     No
6     Disable     No
7     Disable     No
8     Disable     No
9     Disable     No
10    Disable     No
11    Disable     No
12    Disable     No
13    Disable     No
14    Disable     No
15    Disable     No
16    Disable     No
17    Disable     No
18    Disable     No
19    Disable     No
20    Disable     No
21    Disable     No
22    Disable     No
23    Disable     No
24    Disable     No
```

Port	ポート番号
Status	IP Options Attack に対する攻撃検出機能の状態。Enable か Disable
Mirroring	不正パケットをミラーリングする (Yes) かしない (No) かを表示

表 34:

関連コマンド

SET DOS IPOPTION (190 ページ)

SHOW DOS LAND

カテゴリー：運用・管理 / 攻撃検出

SHOW DOS LAND [PORT={*port-list*|ALL}]

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

Land Attack 検出に関する設定を表示する。

パラメーター

PORT ポート番号。複数指定が可能。ALL を指定した場合、省略した場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show dos land
Port  Status      Mirroring
1     Disable     No
2     Disable     No
3     Disable     No
4     Disable     No
5     Disable     No
6     Disable     No
7     Disable     No
8     Disable     No
9     Disable     No
10    Disable     No
11    Disable     No
12    Disable     No
13    Disable     No
14    Disable     No
15    Disable     No
16    Disable     No
17    Disable     No
18    Disable     No
19    Disable     No
20    Disable     No
21    Disable     No
22    Disable     No
23    Disable     No
```

Port	ポート番号
Status	Land Attack に対する攻撃検出機能の状態。Enable か Disable
Mirroring	不正パケットをミラーリングする (Yes) かしない (No) かを表示

表 35:

関連コマンド

SET DOS (189 ページ)

SHOW DOS (241 ページ)

SHOW DOS PINGOFDEATH

カテゴリー：運用・管理 / 攻撃検出

SHOW DOS PINGOFDEATH [PORT={*port-list*|ALL}]

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

Ping of Death 攻撃検出に関する設定を表示する。

パラメーター

PORT ポート番号。複数指定が可能。ALL を指定した場合、省略した場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show dos pingofdeath
Port  Status      Mirroring
1     Disable     No
2     Disable     No
3     Disable     No
4     Disable     No
5     Disable     No
6     Disable     No
7     Disable     No
8     Disable     No
9     Disable     No
10    Disable     No
11    Disable     No
12    Disable     No
13    Disable     No
14    Disable     No
15    Disable     No
16    Disable     No
17    Disable     No
18    Disable     No
19    Disable     No
20    Disable     No
21    Disable     No
22    Disable     No
23    Disable     No
24    Disable     No
```

Port	ポート番号
Status	Ping of Death 攻撃検出機能の状態。Enable か Disable
Mirroring	不正パケットをミラーリングする (Yes) かしない (No) かを表示

表 36:

関連コマンド

SET DOS PINGOFDEATH (192 ページ)

SHOW DOS SMURF

カテゴリー：運用・管理 / 攻撃検出

SHOW DOS SMURF [PORT={*port-list*|ALL}]

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

Smurf Attack 検出に関する設定を表示する。

パラメーター

PORT ポート番号。複数指定が可能。ALL を指定した場合、省略した場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show dos smurf port
Port  Status      Mirroring
1     Disable     None
2     Disable     None
3     Disable     None
4     Disable     None
5     Disable     None
6     Disable     None
7     Disable     None
8     Disable     None
9     Disable     None
10    Disable     None
11    Disable     None
12    Disable     None
13    Disable     None
14    Disable     None
15    Disable     None
16    Disable     None
17    Disable     None
18    Disable     None
19    Disable     None
20    Disable     None
21    Disable     None
22    Disable     None
23    Disable     None
24    Disable     None
```

Port	ポート番号
Status	Smurf Attack に対する攻撃検出機能の状態。Enable か Disable
Mirroring	ミラーポートを設定できないので、None を表示

表 37:

関連コマンド

SET DOS (189 ページ)

SET DOS SMURF (193 ページ)

SHOW DOS (241 ページ)

SHOW DOS SYNFLOOD

カテゴリー：運用・管理 / 攻撃検出

SHOW DOS SYNFLOOD [PORT={*port-list*|ALL}]

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

SYN Flood Attack 検出に関する設定を表示する。

パラメーター

PORT ポート番号。複数指定が可能。ALL を指定した場合、省略した場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show dos synflood port
Port  Status      Mirroring
1     Disable     None
2     Disable     None
3     Disable     None
4     Disable     None
5     Disable     None
6     Disable     None
7     Disable     None
8     Disable     None
9     Disable     None
10    Disable     None
11    Disable     None
12    Disable     None
13    Disable     None
14    Disable     None
15    Disable     None
16    Disable     None
17    Disable     None
18    Disable     None
19    Disable     None
20    Disable     None
21    Disable     None
22    Disable     None
23    Disable     None
24    Disable     None
```

Port	ポート番号
Status	SYN Flood Attack に対する攻撃検出機能の状態。Enable か Disable
Mirroring	ミラーポートを設定できないので、None を表示

表 38:

関連コマンド

SET DOS SYNFLOOD (194 ページ)

SHOW DOS TEARDROP

カテゴリー：運用・管理 / 攻撃検出

SHOW DOS TEARDROP [PORT={*port-list*|ALL}]

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

Teardrop Attack 検出に関する設定を表示する。

パラメーター

PORT ポート番号。複数指定が可能。ALL を指定した場合、省略した場合はすべてのポートが対象となる。

入力・出力・画面例

```
# show dos teardrop
Port  Status      Mirroring
1     Disable     No
2     Disable     No
3     Disable     No
4     Disable     No
5     Disable     No
6     Disable     No
7     Disable     No
8     Disable     No
9     Disable     No
10    Disable     No
11    Disable     No
12    Disable     No
13    Disable     No
14    Disable     No
15    Disable     No
16    Disable     No
17    Disable     No
18    Disable     No
19    Disable     No
20    Disable     No
21    Disable     No
22    Disable     No
23    Disable     No
24    Disable     No
```

Port	ポート番号
Status	Teardrop Attack に対する攻撃検出機能の状態。Enable か Disable
Mirroring	不正パケットをミラーリングする (Yes) かしない (No) かを表示

表 39:

関連コマンド

SET DOS TEARDROP (195 ページ)

SHOW ENCO KEY

カテゴリー：運用・管理 / 鍵作成・管理

SHOW ENCO KEY [=key-id]

key-id: 鍵番号 (0~65535)

解説

鍵の情報を表示する。

パラメーター

KEY 鍵番号。本パラメーターを省略した場合は、ENCO モジュールが保持している鍵の一覧が表示される。

入力・出力・画面例

```
# show enco key
ID      Algorithm      Length Digest      Description
1       RSA-Private      1024  B3FEB122  host
2       RSA-Public       1024  B3FEB122
```

ID	鍵番号
Algorithm	鍵の種類。RSA-Private、RSA-Public のどちらか
Length	RSA 鍵の長さ (ビット)
Digest	鍵データのメッセージダイジェスト
Description	鍵の説明 (CREATE ENCO KEY コマンドの DESCRIPTION パラメーター)

表 40:

関連コマンド

CREATE ENCO KEY (92 ページ)

DESTROY ENCO KEY (123 ページ)

SET ENCO KEY (196 ページ)

SHOW EXCEPTIONLOG

カテゴリー：運用・管理 / システム

SHOW EXCEPTIONLOG [=filename]

filename: ファイル名

解説

例外発生ログを表示する。

パラメーター

EXCEPTIONLOG 表示するログの名前。省略時はログファイルの一覧が表示される。

入力・出力・画面例

```
# show exceptionlog
FileName                Size                Created
-----
except0.exc             636                10/06/2009 18:54:01
except1.exc             636                10/06/2009 16:48:40
-----

# show exceptionlog
*** No Files Found!!!
```

例

例外発生ログを表示する

```
SHOW EXCEPTIONLOG
```

関連コマンド

DELETE EXCEPTIONLOG (114 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] [DEVICE=FLASH]

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。

DEVICE ファイルの存在する物理デバイスを指定する。FLASH を指定。

入力・出力・画面例

```
# show file

File Name                               Device  Size(Bytes)  Last Modified
-----
boot.cfg                                flash   1561         11/07/2009 18:20:10
test01.cfg                               flash   1869         11/10/2009 15:46:56
test02.cfg                               flash   1561         11/07/2009 18:21:24
test03.cfg                               flash   1561         11/07/2009 18:21:58
test04.cfg                               flash   1629         11/10/2009 14:02:36
-----
```

FileName	ファイル名
Device	Device ファイルが格納されているデバイス名。flash
Size(Bytes)	ファイルサイズ (バイト)
Last Modified	ファイルの最終更新日時

表 41:

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

関連コマンド

DELETE FILE (115 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

```
# show flash
Flash:
-----
Files ..... 6552576 bytes (7 files)
Free ..... 1671168 bytes
Total ..... 8223744 bytes
-----
```

files	ファイルが使用している容量
free	未使用容量
total	フラッシュの総容量

表 42:

関連コマンド

SHOW FILE (257 ページ)

SHOW INTERFACE

カテゴリー：運用・管理 / SNMP

SHOW INTERFACE [= {*ifindex*|ALL}] [COUNTER]

ifindex: インターフェースのインデックス番号

解説

指定したインターフェースの情報を表示する。

パラメーター

INTERFACE インターフェースのインデックス番号 (*ifIndex*)、または、ALL を指定する。インデックス番号は、SHOW INTERFACE コマンドの「*ifIndex*」で確認できる。省略時はすべてのインターフェースに関する情報が表示される。指定時は、該当インターフェースの状態が表示される。

COUNTER COUNTER を指定した場合、指定したポートまたは、すべてのポートのカウンター情報が表示される。

入力・出力・画面例

```
# show interface
```

Interfaces		sysUpTime: 6 days 07:15:44		
ifIndex	Interface	ifAdminStatus	ifOperStatus	ifLastChange
1	Port_01	Up	Down	00:00:03
2	Port_02	Up	Down	00:00:03
3	Port_03	Up	Down	00:00:03
4	Port_04	Up	Down	00:00:03
5	Port_05	Up	Down	00:00:03
6	Port_06	Up	Down	00:00:03
7	Port_07	Up	Down	00:00:03
8	Port_08	Up	Down	00:00:03
9	Port_09	Up	Down	00:00:03
10	Port_10	Up	Down	00:00:03
11	Port_11	Up	Down	00:00:03
12	Port_12	Up	Down	00:00:03
13	Port_13	Up	Down	00:00:03
14	Port_14	Up	Down	00:00:03
15	Port_15	Up	Down	00:00:03
16	Port_16	Up	Down	00:00:03
17	Port_17	Up	Down	00:00:03
18	Port_18	Up	Down	00:00:03

```

19  Port_19      Up           Down        00:00:03
20  Port_20      Up           Down        00:00:03
21  Port_21      Up           Down        00:12:21
22  Port_22      Up           Down        00:00:03
23  Port_23      Up           Down        00:00:03
24  Port_24      Up           Down        00:00:03
-----

# show interface=all
Interface..... Port_01
  ifIndex..... 1
  ifMTU..... 9198
  ifSpeed..... 0
  ifAdminStatus..... Up
  ifOperStatus..... Down
  ifLinkUpDownTrapEnable... Enabled

Interface Counters

  ifInOctets ..... 0          ifOutOctets ..... 0
  ifInUcastPkts ..... 0        ifOutUcastPkts ..... 0
  ifInNUcastPkts ..... 0       ifOutNUcastPkts ..... 0
  ifInDiscards ..... 0         ifOutDiscards ..... 0
  ifInErrors ..... 0           ifOutErrors ..... 0

Interface..... Port_02
  ifIndex..... 2
  ifMTU..... 9198
  ifSpeed..... 0
  ifAdminStatus..... Up
  ifOperStatus..... Down
  ifLinkUpDownTrapEnable... Enabled

Interface Counters

  ifInOctets ..... 0          ifOutOctets ..... 0
  ifInUcastPkts ..... 0        ifOutUcastPkts ..... 0
  ifInNUcastPkts ..... 0       ifOutNUcastPkts ..... 0
  ifInDiscards ..... 0         ifOutDiscards ..... 0
  ifInErrors ..... 0           ifOutErrors ..... 0
:
:

# show interface=1 counter

Interface Counters

Interface: Port_01
  ifInOctets ..... 0          ifOutOctets ..... 0
  ifInUcastPkts ..... 0        ifOutUcastPkts ..... 0

```

ifInNUcastPkts	0	ifOutNUcastPkts	0
ifInDiscards	0	ifOutDiscards	0
ifInErrors	0	ifOutErrors	0

sysUpTime	システム起動後の経過時間
ifIndex	インターフェーステーブルのインデックス (ifIndex)
Interface	インターフェース名
ifAdminStatus	管理者が設定したインターフェースの状態。「Up」、「Down」、「Testing」のいずれか
ifOperStatus	実際のインターフェースの動作状態。「Up」、「Down」、「Testing」のいずれか
ifLastChange	該当インターフェースが現在の動作状態になったときの sysUptime の値

表 43: インターフェース無指定時

ifIndex	インターフェーステーブルのインデックス (ifIndex)
ifMTU	インターフェースの最大転送単位 (MTU) すなわち送信可能なパケットの最大サイズ
ifSpeed	インターフェースの帯域幅 (推定)
ifAdminStatus	管理者が設定したインターフェースの状態。「Up」、「Down」、「Testing」のいずれか
ifOperStatus	実際のインターフェースの動作状態。「Up」、「Down」、「Testing」のいずれか
ifLinkUpDownTrapEnable	リンクトラップの有効・無効。Enabled か Disabled
ifInOctets	受信オクテット数
ifInUcastPkts	受信ユニキャストパケット数
ifInNUcastPkts	受信したマルチキャストパケット、ブロードキャストパケットの数
ifInDiscards	破棄された受信パケット数
ifInErrors	エラーのため破棄された受信パケット数
ifOutOctets	送信オクテット数
ifOutUcastPkts	送信ユニキャストパケット数
ifOutNUcastPkts	送信したマルチキャストパケット、ブロードキャストパケットの数
ifOutDiscards	破棄された送信パケット数
ifOutErrors	エラーのため送信されずに破棄されたパケット数

表 44: インターフェース指定時

ifInOctets	受信オクテット数
ifInUcastPkts	受信ユニキャストパケット数
ifInNUcastPkts	受信したマルチキャストパケット、ブロードキャストパケットの数

ifInDiscards	破棄された受信パケット数
ifInErrors	エラーのため破棄された受信パケット数
ifOutOctets	送信オクテット数
ifOutUcastPkts	送信ユニキャストパケット数
ifOutNUcastPkts	送信したマルチキャストパケット、ブロードキャストパケットの数
ifOutDiscards	破棄された送信パケット数
ifOutErrors	エラーのため送信されずに破棄されたパケット数

表 45: COUNTER オプション指定時

関連コマンド

DISABLE INTERFACE LINKTRAP (135 ページ)

ENABLE INTERFACE LINKTRAP (149 ページ)

SHOW LOG

カテゴリー：運用・管理 / ログ

```
SHOW LOG [= {TEMPORARY|PERMANENT}] [FULL] [MODULE=module-list] [REVERSE]
           [SEVERITY=severity-list]
```

module-list: モジュール名 (カンマを使った複数指定も可)

severity-list: ログレベル (E,W,I で指定。カンマを使った複数指定も可)

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 表示対象のログを、TEMPORARY (RAM 上のログ) または PERMANENT (NVS 上のログ) で指定する。省略時は TEMPORARY (RAM 上のログ) が表示対象となる。

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。

MODULE 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。

REVERSE ログメッセージを逆順 (新しい順) に表示する。

SEVERITY メッセージのログレベル。E (Error)、W (Warning) または I (Information) で指定。省略時はすべてのログレベルにマッチする。

入力・出力・画面例

```
# show log

Total Number of Events: 8

S Date      Time      Event
-----
I 11/28/09 16:39:04 qos: QoS initialized
I 11/28/09 16:39:05 pcfg: PortConfig initialized
I 11/28/09 16:39:05 ptrunk: Port Trunking initialized
I 11/28/09 16:39:05 vlan: VLAN initialized

# show log full

Total Number of Events: 125

S Date      Time      EventID  Source File:Line Number
           Event
-----
```

```

I 11/28/09 16:39:01 033005 evtlogapp.c:1975
                        evtlog: Created Output Definition, ID 0, Type Permanent
I 11/28/09 16:39:01 033005 evtlogapp.c:1999
                        evtlog: Created Output Definition, ID 1, Type Temporary
I 11/28/09 16:39:01 033004 evtlogapp.c:223
                        evtlog: Event log initialized
I 11/28/09 16:39:03 183001 fileapp.c:143
                        file: File System initialized

```

S	ログメッセージのログレベル
Date	ログメッセージの生成日
Time	ログメッセージの生成時間。日付は日(1~31)のみの表示
Event	ログを生成したモジュール名:メッセージ本文

表 46:

S	ログメッセージのログレベル
Date	ログメッセージの生成日
Time	ログメッセージの生成時間。日付は日(1~31)のみの表示
Event ID	イベント ID
Source File:Line Number	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
Event	ログを生成したモジュール名:メッセージ本文

表 47: FULL オプション指定時

例

NVS 上のログ (PERMANENT ログ) を見る

```
SHOW LOG=PERMANENT
```

最新のシステム関連ログメッセージを見る

```
SHOW LOG MODULE=SYSTEM
```

備考・注意事項

NVS 上のログを表示するとき、特定の文字列より長い場合、途中までしか表示されないことがあるが、RAM 上のログ、または syslog サーバーに転送されたログは最後まで表示される。

関連コマンド

PURGE LOG (171 ページ)

SHOW LOG OUTPUT

カテゴリー：運用・管理 / ログ

SHOW LOG OUTPUT [=output-id] [FULL]

output-id: ログ出力 ID (0~20)

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。

FULL 各出力先の定義内容を詳細に表示する。

入力・出力・画面例

```
# show log output

OutputID  Type           Status         Details
-----
0         Permanent     Enabled        Wrap on Full
1         Temporary     Enabled        Wrap on Full
2         Syslog        Enabled        192.168.1.20

# show log output=1 full

Output ID ..... 1
Output Type ..... Temporary
Status ..... Enabled
Log Full Action ..... Wrap on Full
Event Severity ..... All
Event Module ..... All
```

OutputID	ログ出力 ID
Type	ログ出力先。Permanent、Temporary、Syslog のいずれか
Server	ログ転送先の IP アドレス。Type が Syslog の場合にのみ有効
Status	ログ出力定義の状態。Enabled か Disabled
Details	Type が Permanent または Temporary の場合は、ログメッセージが最大保存数を超えた場合の保存方法。Type が Syslog の場合は、syslog サーバーのアドレス

表 48:

OutputID	ログ出力 ID
Type	ログ出力先。Permanent、Temporary、Syslog のいずれか
Status	ログ出力定義の状態。Enabled か Disabled
Log Full Action	ログメッセージが最大保存数を越えた場合の保存方法。Type が Permanent または Temporary の場合のみ
Server IP Address	ログ転送先の IP アドレス。Type が Syslog の場合のみ
Message Format	syslog メッセージのフォーマット。Extended(時刻情報とシステム名(sysName)が付加される)または Normal(既存のフォーマット)。Type が Syslog の場合のみ
Facility Level	syslog メッセージのファシリティコード。Type が Syslog の場合のみ
Event Severity	マッチするメッセージのログレベル
Event Module	マッチするメッセージのモジュール

表 49: 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を表示する。

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

関連コマンド

ADD LOG OUTPUT (79 ページ)

CREATE LOG OUTPUT (94 ページ)

DESTROY LOG OUTPUT (124 ページ)

SET LOG OUTPUT (198 ページ)

SHOW LOG STATUS (269 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

```
# show log status

Event Log Configuration:
Event Logging ..... Enabled
Number of Output Definitions .... 2
```

Event Logging	ログ機能の有効・無効
Number of Output Definitions	定義されているログ出力先の数

表 50:

関連コマンド

DISABLE LOG (136 ページ)

ENABLE LOG (150 ページ)

SET LOG FULLACTION (197 ページ)

SHOW LOG (264 ページ)

SHOW MGMTACL

カテゴリー：運用・管理 / マネージメントアクセスコントロール

SHOW MGMTACL [ID=1..256]

解説

マネージメントアクセスコントロールの状態およびリストに登録されているエントリーを表示する。

パラメーター

ID エントリー番号。指定時は該当エントリーだけを表示する。省略時はマネージメントアクセスコントロールの状態とすべてのエントリーを表示する

入力・出力・画面例

```
# show mgmtacl
Management ACL Status ..... Disable

-----

MgmtACL ID ..... 5
IP Address ..... 192.168.1.1
Mask ..... 255.255.255.0
Port List ..... 2,4,6
Application ..... PING

-----

MgmtACL ID ..... 10
IP Address ..... 192.168.1.100
Mask ..... 255.255.255.0
Port List ..... 1,3,5
Application ..... ALL

# show mgmtacl id=10

-----

MgmtACL ID ..... 10
IP Address ..... 192.168.1.100
Mask ..... 255.255.255.0
Port List ..... 1,3,5
Application ..... ALL
```

Management ACL Status マネージメントアクセスコントロールの状態。Enable または Disable

ID	エントリー番号
IP Address	IP アドレス
Mask	マスク
Port List	受信スイッチポート番号
Application	許可対象パケットの種類。TELNET、PING、ALL のいずれか。詳細は CREATE MGMTACL コマンドのページに掲載されている表を参照

表 51:

例

Management ACL (マネージメントアクセスコントロールリスト) の状態とすべてのエントリーを表示。

```
SHOW MGMTACL
```

エントリー「10」だけを表示。

```
SHOW MGMTACL ID=10
```

関連コマンド

ADD MGMTACL (80 ページ)

CREATE MGMTACL (96 ページ)

DELETE MGMTACL (116 ページ)

DESTROY MGMTACL (125 ページ)

DISABLE MGMTACL (138 ページ)

ENABLE MGMTACL (152 ページ)

SET MGMTACL (199 ページ)

SHOW PKI CERTIFICATE

カテゴリー：運用・管理 / PKI

SHOW PKI CERTIFICATE [=string]

string: 証明書の名前 (1~24 文字。使用可能な文字は半角英数字 (大文字・小文字を区別する) 半角記号 (# \$ % & ' () ~ | - ^ \ @ ' { + * } [; :] , . / -)。文字列に半角空白、!= を含む場合は、前後をダブルクォート (") で囲む必要がある。)

解説

証明書データベース内の証明書に関する情報を表示する。

パラメーター

CERTIFICATE 証明書の名前。

入力・出力・画面例

```
# show pki certificate
Certificate Database:
Name                State      MTrust  Type  Source
-----
test                Trusted   True    EE    Command
-----
#
#
# show pki certificate=test
Certificate:
Name ..... test
State ..... Trusted
Manually Trusted ... True
Type ..... EE
Source ..... Command

Version ..... V3 (0X2)
Serial Number ..... 0 (0X0)
Signature Alg ..... md5WithRSAEncryption
Public Key Alg ..... rsaEncryption
Not Valid Before ... Jan  1 04:38:32 1980 GMT
Not Valid After ... Dec 31 04:38:32 1981 GMT
Subject ..... CN=1.1.1.2
Issuer ..... CN=1.1.1.2
MD5 Fingerprint ... 49:52:A8:59:CC:54:3C:52:17:97:85:54:67:91:C4:FA
SHA1 Fingerprint ... FF:F8:C5:53:F3:32:31:E4:92:F4:95:41:8A:C2:D1:9D:CE:E0:45:7F
```

Name	証明書の名前。ユーザーがつけたもの、あるいは、スイッチが自動的に取得した証明書の場合は証明書の Subject
State	証明書の信頼レベル。Trusted (信頼できる) Untrusted (まだ信頼できない) Validating (検証中) のいずれか
MTrust	ユーザーのコマンド入力によって手動で「信頼できる」ものとして設定されたかどうか。True か False
Type	証明書の種類。SELF (ルーター自身の証明書) CA (認証局の証明書) EE (その他エンドエンティティの証明書) がある
Source	証明書がどのようにしてデータベースに登録されたか。Command (ユーザーのコマンド入力) のみ

表 52:

Certificate セクション	証明書に関する情報が表示される
Name	証明書の名前。ユーザーがつけたもの、あるいは、ルーターが自動的に取得した証明書の場合は証明書の Subject
State	証明書の信頼レベル。Trusted (信頼できる) Untrusted (まだ信頼できない) Validating (検証中) のいずれか
Manually Trusted	ユーザーのコマンド入力によって手動で「信頼できる」ものとして設定されたかどうか。True か False
Type	証明書の種類。SELF (ルーター自身の証明書) CA (認証局の証明書) EE (その他エンドエンティティの証明書) がある
Source	証明書がどのようにしてデータベースに登録されたか。Command (ユーザーのコマンド入力) のみ
Version	証明書が準拠している X.509 のバージョン
Serial Number	証明書のシリアル番号
Signature Alg	証明書に対する電子署名に用いられたアルゴリズム
Public Key Alg	証明書の発行対象である公開鍵のアルゴリズム
Not Valid Before	証明書の有効期間開始日 (発効日)
Not Valid After	証明書の有効期間終了日 (失効日)
Subject	証明書の所有者 (サブジェクト) の識別名
Issuer	証明書の発行者の識別名
MD5 Fingerprint	MD5 による証明書のフィンガープリント
Sha1 Fingerprint	ハッシュ関数 SHA1 による証明書のフィンガープリント

表 53: 名前指定時

備考・注意事項

証明書のシリアル番号が-2147483649 以下、2147483648 以上 のとき、Serial Number は、xx:xx:xx:xx... の形式で表示される。

関連コマンド

ADD PKI CERTIFICATE (81 ページ)

DELETE PKI CERTIFICATE (117 ページ)

SET PKI CERTIFICATE (201 ページ)

SHOW RADIUSACCOUNTING

カテゴリ：運用・管理 / 認証サーバー

SHOW RADIUSACCOUNTING

解説

RADIUS (Remote Authentication Dial In User Server) サーバーのアカウントिंग機能の設定を表示する。

入力・出力・画面例

```
# show radiusaccounting
Radius Accounting Configuration
-----
Radius Accounting Status .....: Disabled
Radius Accounting Port.....: 1813
Radius Accounting Type.....: Network
Radius Accounting Trigger Type.....: Start_Stop
Radius Accounting Update Status.....: Disabled
Radius Accounting Update Interval...: 60
```

Radius Accounting Status	アカウントिंग機能の状態。Enabled か Disabled
Radius Accounting Port	RADIUS サーバーのアカウントिंग用 UDP ポート番号
Radius Accounting Type	アカウントング情報を転送して蓄積する場所。NETWORK (アカウントングサーバー) のみ
Radius Accounting Trigger Type	アカウントング要求パケットをサーバーの送出するタイミング。START_STOP か STOP_ONLY
Radius Accounting Update Status	ユーザーが利用中に、利用状況をサーバーに送信するアカウントング要求 (インターリム) パケットを送信するかどうか。Enabled か Disabled
Radius Accounting Update Interval	インターリムパケットを送信する間隔

表 54:

関連コマンド

DISABLE RADIUSACCOUNTING (139 ページ)

ENABLE RADIUSACCOUNTING (153 ページ)

SET RADIUSACCOUNTING (202 ページ)

SHOW REMOTELIST

カテゴリー：運用・管理 / エンハンススタッキング

SHOW REMOTELIST

解説

エンハンススタッキンググループに属するスイッチを表示する。

入力・出力・画面例

```
# show remotelist
Searching for slave devices. Please wait...

Num  MAC Address          Name                Switch  Software  Switch
     MAC Address          Name                Mode    Version   Model
-----
01   00:30:84:00:00:00    Slave              Slave   S63 v1.1.1  CentreCOM 9408L
```

Num	リスト番号
MAC Address	製品の MAC アドレス
Name	製品のシステム名
Switch Mode	エンハンススタッキンググループ内での役割。MASTER または SLAVE
Software Version	製品のファームウェアバージョン
Switch Model	製品名

表 55:

例

エンハンススタッキンググループに属するスイッチを表示する

```
SHOW REMOTELIST
```

備考・注意事項

MASTER スイッチからのみ参照可能。

関連コマンド

SET SWITCH STACKMODE (220 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

```
# show snmp
SNMP Information:
  Status ..... Disabled
  Community ..... private
    Access ..... Read|Write
    Status ..... Enabled
    Open Access ..... No
  Community ..... public
    Access ..... Read Only
    Status ..... Enabled
    Open Access ..... No
```

Status	SNMP エージェントの状態。Enabled か Disabled
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
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

表 56:

例

SNMP モジュールの情報を表示する

```
SHOW SNMP
```

関連コマンド

SHOW SNMP COMMUNITY (278 ページ)

SHOW SNMP COMMUNITY

カテゴリー：運用・管理 / SNMP

SHOW SNMP COMMUNITY=community

community: SNMP コミュニティ名 (1~32 文字。英数字が使用可能。大文字・小文字を区別する。)(ダブルクォート) \ (スクエアブラケット) \ (バックスラッシュ、円マーク) 半角スペースは使用できない)

解説

SNMP コミュニティの情報を表示する。

パラメーター

COMMUNITY SNMP コミュニティ名。

入力・出力・画面例

```
# show snmp community=private
SNMP Community Information:
  Name ..... private
  Access ..... Read|Write
  Status ..... Enabled
  Manager ..... 192.168.10.5
  Trap Host ..... 192.169.10.5
```

Name	コミュニティ名
Access	コミュニティのアクセス権。Read Only、Read Write のどちらか
Status	コミュニティの状態。Enabled か Disabled
Manager	SNMP オペレーションを許可されたホストの IP アドレス
Trap Host	SNMP トラップの送信先ホストの IP アドレス

表 57:

例

SNMP コミュニティ「private」の情報を表示する

```
SHOW SNMP COMMUNITY=private
```

関連コマンド

SHOW SNMP (277 ページ)

SHOW SNMP TRAP

カテゴリー：運用・管理 / SNMP

SHOW SNMP TRAP

解説

SNMP トラップの送信が有効/無効であるか表示する

入力・出力・画面例

```
# show snmp trap
SNMP Trap Information:
  Authentication Failure Traps..... Enabled
  Intrusion Traps ..... Enabled
  Link Traps ..... Enabled
  ColdStart Traps ..... Enabled
  NewRoot Traps ..... Enabled
  Fan Traps ..... Enabled
  DOS Traps ..... Enabled
  STPStateChange Traps ..... Enabled
  RPSStateChange Traps ..... Enabled
  Temperature Traps ..... Enabled
  TopologyChange Traps ..... Enabled
  Storm Detection Traps ..... Enabled
  Loop Detection Traps ..... Enabled
```

Authentication failure traps	異なる SNMP コミュニティ名のメッセージ受信時のトラップ送信の有効・無効
Intrusion Traps	ポートセキュリティにおいて不正パケット受信時のトラップ送信の有効・無効
Link Traps	スイッチポートのリンクアップ・ダウン時のトラップ送信の有効・無効
ColdStart Traps	ハードウェアリセットによるシステム起動時のトラップ送信の有効・無効
NewRoot Traps	スパニングツリーにおいて新しいルートへの切り替わり時のトラップ送信の有効・無効
Fan Traps	ファンの回転異常検出時のトラップ送信の有効・無効
DOS Traps	DoS 攻撃検出時のトラップ送信の有効・無効
STPStateChange Traps	スパニングツリーにおいてステータス変更時のトラップ送信の有効・無効

RPSStateChange Traps	未サポート。設定に関係なくトラップは送信されない
Temperature Traps	筐体の温度異常検出時のトラップ送信の有効・無効
TopologyChange Traps	スパニングツリーにおいてトポロジー変更発生時のトラップ送信の有効・無効
Storm Detection Traps	受信レート検出によるループの検出、アクション実行、アクションからの復旧のトラップの有効・無効
Loop Detection Traps	LDF 検出によるループの検出、アクション実行、アクションからの復旧のトラップの有効・無効

表 58:

関連コマンド

DISABLE SNMP (140 ページ)

DISABLE SNMP TRAP (142 ページ)

ENABLE SNMP (154 ページ)

ENABLE SNMP TRAP (156 ページ)

SHOW SNMP (277 ページ)

SHOW SNMPV3 ACCESS

カテゴリー：運用・管理 / SNMP

SHOW SNMPV3 ACCESS=group [SECURITYMODEL={V1|V2C|V3}]
 [SECURITYLEVEL={NOAUTHENTICATION|AUTHENTICATION|PRIVACY}]

group: SNMP グループ名 (1～63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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表示する。

パラメーター

ACCESS SNMP グループ名。

SECURITYMODEL 本グループ所属のユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。セキュリティーモデルを指定しなかった場合は、指定したグループ名のエントリーがすべて表示される。

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。NOAUTHENTICATION (認証なし、暗号化なし)、AUTHENTICATION (認証あり、暗号化なし)、PRIVACY (認証あり、暗号化あり) から選択する。セキュリティーレベルを指定しなかった場合は、指定したグループ名のエントリーがすべて表示される。

入力・出力・画面例

```
# show snmpv3 access=managers

Group Name ..... managers
Context Prefix .....
Security Model ..... v3
Security Level ..... AuthPriv
  Context Match ..... Exact
  Read View ..... internet
  Write View ..... internet
  Notify View ..... internet
  Storage Type ..... NonVolatile
  Row Status ..... Active
```

Group Name	SNMP グループ名
Security Model	SNMP プロトコル。v1、v2c または v3 のいずれか

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
Context Match	常に E x a c t
Read View	読み出し可能なビュー名
Write View	書き込み可能なビュー名
Notify View	通知を受信可能なビュー名
Storage Type	設定を保存するか (NonVolatile) しないか (Volatile)
Row Status	ユーザーの状態。active、not in service、not ready のいずれか

表 59:

例

SNMP グループ「managers」の設定内容を表示する。

```
SHOW SNMPV3 ACCESS=managers
```

関連コマンド

CREATE SNMPV3 ACCESS (102 ページ)
DESTROY SNMPV3 ACCESS (127 ページ)
SET SNMPV3 ACCESS (205 ページ)

SHOW SNMPV3 COMMUNITY

カテゴリー：運用・管理 / SNMP

SHOW SNMPV3 COMMUNITY INDEX [=index]

index: インデックス名 (1～63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) SNMP コミュニティーの設定情報を表示する。

パラメーター

INDEX コミュニティー名。コミュニティ名を指定しない場合は、すべてのコミュニティが表示される。

入力・出力・画面例

```
# show snmpv3 community

Community Index ..... Index3
  Community Name ..... test
  Security Name ..... test
  Transport Tag ..... trans
  Storage Type ..... Volatile
  Row Status ..... Active
```

Community Index	コミュニティ名
Community Name	コミュニティに対するパスワード
Security Name	SNMPv1 および v2c のユーザー名
Transport Tag	トランスポート名
Storage Type	設定を保存するか (NonVolatile) しないか (Volatile)
Row Status	ユーザーの状態。active、not in service、not ready のいずれか

表 60:

例

SNMP コミュニティー「Index3」の設定を表示する。

```
SHOW SNMPV3 COMMUNITY INDEX=Index3
```

備考・注意事項

SNMPv1/v2c用にデフォルトで設定されているコミュニティー「public」「private」の設定が表示されるが、SNMPv3コマンドで設定を変更することはできない。

関連コマンド

CREATE SNMPV3 COMMUNITY (104 ページ)

DESTROY SNMPV3 COMMUNITY (128 ページ)

SET SNMPV3 COMMUNITY (206 ページ)

SHOW SNMPV3 ENGINEID

カテゴリ：運用・管理 / SNMP

SHOW SNMPV3 ENGINEID

解説

(SNMPv3) 本製品のエンジン ID を表示する。

入力・出力・画面例

```
# show snmpv3 engineid

SNMP Engine ID ..... 80:00:00:CF:03:00:0C:46:64:59:7B
```

例

本製品のエンジン ID を表示する。

SHOW SNMPV3 ENGINEID

SHOW SNMPV3 GROUP

カテゴリー：運用・管理 / SNMP

SHOW SNMPV3 GROUP [USERNAME=*username*] [SECURITYMODEL={V1|V2C|V3}]

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) ユーザーに対応付けられているユーザーグループを表示する。

パラメーター

USERNAME SNMP ユーザー名。ユーザー名を指定しなかった場合は、すべてのユーザーの定義が表示される。

SECURITYMODEL 本グループ所属のユーザーに関連づける SNMP プロトコルのバージョンを指定する。V1 (SNMPv1)、V2C (SNMPv2c)、V3 (SNMPv3) から選択する。バージョンを指定しなかった場合は、すべてのバージョンの定義が表示される。

入力・出力・画面例

```
# show snmpv3 group username=systemadmin24

Security Model ..... v3
Security Name ..... systemadmin24
  Group Name ..... managers
  Storage Type ..... Volatile
  Row Status ..... Active
```

Security Model	対応プロトコル
Security Name	SNMP ユーザー名
Group Name	SNMP グループ名
Storage Type	設定を保存するか (NonVolatile) しないか (Volatile)
Row Status	ユーザーの状態。active、not in service、not ready のいずれか

表 61:

例

SNMP ユーザー「systemadmin24」に対応付けられているグループを表示する。

```
SHOW SNMPV3 GROUP USERNAME=systemadmin24
```

関連コマンド

CREATE SNMPV3 GROUP (106 ページ)

SET SNMPV3 GROUP (208 ページ)

SHOW SNMPV3 NOTIFY

カテゴリー：運用・管理 / SNMP

SHOW SNMPV3 NOTIFY [=notify]

notify: 通知名 (1~63文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) 通知名の定義を表示する。

パラメーター

NOTIFY 通知名。通知名を指定しなかった場合は、すべての定義が表示される。

入力・出力・画面例

```
# show snmpv3 notify=sysadmintrap

Notify Name ..... sysadmintrap
  Notify Tag .....
  Notify Type ..... Trap
  Storage Type ..... Volatile
  Row Status ..... Active
```

例

通知名「sysadmintrap」の定義を表示する。

```
SHOW SNMPV3 NOTIFY=sysadmintrap
```

関連コマンド

CREATE SNMPV3 NOTIFY (107 ページ)

DESTROY SNMPV3 NOTIFY (130 ページ)

SET SNMPV3 NOTIFY (209 ページ)

SHOW SNMPV3 TARGETADDR

カテゴリー：運用・管理 / SNMP

SHOW SNMPV3 TARGETADDR [=target]

target: SNMP ターゲット名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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。ターゲット名を指定しなかった場合は、すべてのターゲットが表示される。

入力・出力・画面例

```
# show snmpv3 targetaddr=host451

Target Address Name ..... host451
  IP Address ..... 192.168.1.100
  UDP Port# ..... 162
  Timeout ..... 1500
  Retries ..... 3
  Tag List ..... sysadmintag
  Parameters ..... SNMPmanagerPC
  Storage Type ..... Volatile
  Row Status ..... Active
```

Target Address Name	SNMP ターゲット名
IP Address	ターゲットの IP アドレス
UDP Port#	ターゲットのリスニング UDP ポート
Timeout	インフォームメッセージのタイムアウト時間
Retries	インフォームメッセージの再送回数
Tag List	タグ名
Parameters	SNMP ターゲットパラメーターセット名
Storage Type	設定を保存するか (NonVolatile) しないか (Volatile)
Row Status	ユーザーの状態。active、not in service、not ready のいずれか

表 62:

例

SNMP ターゲット「host451」の設定内容を表示する。

```
SHOW SNMPV3 TARGETADDR=host451
```

関連コマンド

CREATE SNMPV3 TARGETADDR (108 ページ)

DESTROY SNMPV3 TARGETADDR (131 ページ)

SET SNMPV3 TARGETADDR (210 ページ)

SHOW SNMPV3 TARGETPARAMS

カテゴリー：運用・管理 / SNMP

SHOW SNMPV3 TARGETPARAMS [=params]

params: SNMP ターゲットパラメーターセット名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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の設定を表示する。

パラメーター

TARGETPARAMS SNMP ターゲットパラメーターセット名。SNMP ターゲットパラメーターセット名を指定しなかった場合は、すべての定義が表示される。

入力・出力・画面例

```
# show snmpv3 targetparams=SNMPmanagerPC

Target Parameter Name ..... SNMPmanagerPC
  Message Processing Model .. v3
  Security Model ..... v3
  Security Name ..... sytemadmin24
  Security Level ..... AuthPriv
  Storage Type ..... NonVolatile
  Row Status ..... Active
```

Target Parameter Name	SNMP ターゲットパラメーターセット名
Message Processing Model	対応プロトコル
Security Model	対応プロトコル
Security Name	SNMP ユーザー名
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
Storage Type	設定を保存するか (NonVolatile) しないか (Volatile)
Row Status	ユーザーの状態。active、not in service、not ready のいずれか

表 63:

例

SNMP パラメーターセット「SNMPmanagerPC」の設定内容を表示する。

```
SHOW SNMPV3 TARGETPARAMS=SNMPmanagerPC
```

関連コマンド

CREATE SNMPV3 TARGETPARAMS (110 ページ)

DESTROY SNMPV3 TARGETPARAMS (132 ページ)

SET SNMPV3 TARGETPARAMS (212 ページ)

SHOW SNMPV3 USER

カテゴリー：運用・管理 / SNMP

SHOW SNMPV3 USER [=username]

username: SNMP ユーザー名 (1~32 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。大文字・小文字を区別する)

解説

(SNMPv3) ユーザーの設定を表示する。

パラメーター

USER SNMP ユーザー名。ユーザー名を省略した場合は、すべてのユーザーについて表示する。

入力・出力・画面例

```
# show snmpv3 user=systemadmin24

Engine Id ..... 80:00:00:CF:03:00:0C:46:64:59:7B
User Name ..... systemadmin24
  Authentication Protocol ... MD5
  Privacy Protocol ..... DES
  Storage Type ..... NonVolatile
  Row Status ..... Active
```

Engine Id	エンジン ID
User Name	SNMP ユーザー名
Authentication Protocol	認証プロトコル (MD5、SHA または NONE)
Privacy Protocol	暗号化プロトコル (DES または NONE)
Storage Type	設定を保存するか (NonVolatile) しないか (Volatile)
Row Status	ユーザーの状態。active、not in service、not ready のいずれか

表 64:

例

SNMP ユーザー「systemadmin24」の設定を表示する。

```
SHOW SNMPV3 USER=systemadmin24
```

関連コマンド

ADD SNMPV3 USER (85 ページ)

DELETE SNMPV3 USER (120 ページ)

SET SNMPV3 USER (214 ページ)

SHOW SNMPV3 VIEW

カテゴリ：運用・管理 / SNMP

SHOW SNMPV3 VIEW [=view] [SUBTREE={node-oid|node-name}]

view: SNMP ビュー名 (1~63 文字。英数字が使用可能。空白を含む場合はダブルクォートで囲む。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 (規定のノード名)

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、すべてのビューが表示される。

SUBTREE MIB ノードを OID (Object Identifier) または名前 (internet など) で指定する。MIB ノードを指定しなかった場合は、指定したビュー名のエントリーがすべて表示される。

入力・出力・画面例

```
# show snmpv3 view=mib2notcp

View Name ..... mib2notcp
Subtree OID ..... 1.3.6.1.2.1
  Subtree Mask.....
  View Type ..... Included
  Storage Type ..... NonVolatile
  Row Status ..... Active

View Name ..... mib2notcp
Subtree OID ..... 1.3.6.1.2.1.6
  Subtree Mask.....
  View Type ..... Excluded
  Storage Type ..... Volatile
  Row Status ..... Active
```

View Name	SNMP ビュー名
Subtree OID	MIB ノードの OID
Subtree Mask	MIB ノード OID のマスク
View 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

Storage Type	設定を保存するか (NonVolatile) しないか (Volatile)
Row Status	ユーザーの状態。active、not in service、not ready のいずれか

表 65:

例

SNMP ビュー「mib2notcp」の設定内容を表示する。

```
SHOW SNMPV3 VIEW=mib2notcp
```

関連コマンド

CREATE SNMPV3 VIEW (112 ページ)

DESTROY SNMPV3 VIEW (133 ページ)

SET SNMPV3 VIEW (215 ページ)

SHOW SNTP

カテゴリー：運用・管理 / SNTP

SHOW SNTP

解説

SNTP の設定情報を表示する。

入力・出力・画面例

```
# show sntp
SNTP Configuration:
  Status ..... Disabled
  Server ..... 0.0.0.0
  UTC Offset ..... +0
  Daylight Savings Time (DST) ... Disabled
  Poll Interval ..... 600 seconds
  Last Delta ..... +0 seconds
```

Status	SNTP モジュールの状態。Enabled か Disabled
Server	SNTP サーバーの IP アドレス
UTC Offset	協定世界時 (UTC) からのオフセット (時間)
Daylight Savings Time (DST)	サマータイムの設定状態。Enabled か Disabled
Poll Interval	SNTP サーバーへの問い合わせ間隔 (秒)
Last Delta	最終更新時の内蔵時計の修正量 (誤差)

表 66:

例

SNTP の設定情報を表示する

```
SHOW SNTP
```

関連コマンド

ADD SNTP PEER (86 ページ)

SET SNTP (216 ページ)

SHOW SSH

カテゴリー：運用・管理 / Secure Shell

SHOW SSH

解説

SSH サーバーおよびクライアント機能の設定情報を表示する。

入力・出力・画面例

```
# show ssh

Secure Shell Server Configuration

Versions Supported ..... 1.3, 1.5, 2.0
Server Status ..... Enabled
Server Port ..... 22
Host Key ID ..... 1
Host Key Bits ..... 1024
Server Key ID ..... 3
Server Key Bits ..... 768
Server Key Expiry ..... 0 hours
Login Timeout ..... 180 seconds
Authentication Available .. Password
Ciphers Available ..... 3DES, 128 bit AES, 192 bit AES, 256 bit AES,
                          Arcfour (RC4)
MACs Available ..... hmac-sha1, hmac-md5
Data Compression ..... Available
```

Versions Supported	対応している SSH プロトコルのバージョン
Server Status	SSH サーバー機能の状態。Enabled か Disabled
Server Port	SSH サーバーの TCP リスニングポート
Host Key ID	ホスト鍵の鍵番号
Host Key Bits	ホスト鍵長 (ビット)
Server Key ID	サーバー鍵の鍵番号
Server Key Bits	サーバー鍵長 (ビット)
Server Key Expiry	サーバー鍵の有効期間 (時間)
Login Timeout	ログインタイムアウト (秒)
Authentication Available	使用可能な認証方式。Password (パスワード認証) のみ
Ciphers Available	使用可能な暗号アルゴリズム。3DES/RC4/128bit AES/192bit AES/256bit AES

MACs Available	使用可能な Message Authentication Code (MAC)。hmac-sha1 と hmac-md5
Data Compression	データ圧縮が有効かどうか

表 67: 設定情報

例

SSH サーバーおよびクライアント機能の設定情報を表示する

```
SHOW SSH
```

関連コマンド

DISABLE SSH SERVER (145 ページ)

ENABLE SSH SERVER (159 ページ)

SET SSH SERVER (218 ページ)

SHOW SYSTEM

カテゴリー：運用・管理 / システム

SHOW SYSTEM [SERIALNUMBER] [MACADDRESS] [MODELNAME]

解説

システム情報を表示する。

パラメーター

SERIALNUMBER シリアル番号を表示する。

MACADDRESS MAC アドレスを表示する。

MODELNAME 製品名を表示する。

入力・出力・画面例

```
# show system

System Information:

MAC Address ..... 00:15:77:9C:D3:EF      IP Address ..... 0.0.0.0
Model Name ..... AT-9424T                Subnet Mask ..... 0.0.0.0
Serial Number ..... A04035Q081200105     System Up Time ... 0D:00H:04M:38S
System Revision .... B

Bootloader ..... ATS63_LOADER v3.2.1     Build Date ... Jul  1 2009 11:31:24
Application ..... ATS63 v2.11.1J         Build Date ... Apr  5 2010 11:41:38

System Name .....
Administrator .....
Location .....

System 1.25V Power ..... Normal          System 2.5V Power ..... Normal
System 3.0V Power ..... Normal          System 3.3V Power ..... Normal
System 12V Power ..... Normal
System Temperature ..... Normal
System Fan 1 Speed ..... Normal         System Fan 2 Speed ..... Normal
Main PSU ..... On

# show system serialnumber
Serial Number ..... S05525A023600001

# show system macaddress
MAC Address ..... 00:30:84:00:02:00
```

```
# show system modelname
Model Name ..... AT-9424T
```

MAC Address	製品の MAC アドレス
Model Name	製品名
Serial Number	製品のシリアル番号
SystemRevision	製品のハードウェアリビジョン
IP Address	IP アドレス
Subnet Mask	サブネットマスク
System Up Time	稼働時間 (前回リブートしてからの時間)
Bootloader	ブートローダーの名称、バージョン
Build Date	ブートローダーのビルト日時
Application	ファームウェアの名称、バージョン
Build Date	ファームウェアのビルト日時
System Name	システム名 (MIB-II の sysName)
Administrator	管理責任者 (MIB-II の sysContact)
Location	設置場所 (MIB-II の sysLocation)
System Power	各電源ユニットの供給電圧状態。Normal/Warning/Failed (読み取り失敗)、1.25V/2.5V/3.0V/3.3V/12V の状態が表示される
System Temperature	システム内の温度。Normal/Warning/Failed (読み取り失敗)
System Fan Speed	ファンの回転数。Normal/Warning/Failed (読み取り失敗)、ファン 1~2 の状態が表示される
Main PSU	本製品の電源ユニットの状態。On または Off

表 68:

Serial Number	製品のシリアル番号
---------------	-----------

表 69: SERIALNUMBER オプション指定時

MAC Address	製品の MAC アドレス
-------------	--------------

表 70: MACADDRESS オプション指定時

Model Name	製品名
------------	-----

表 71: MODELNAME オプション指定時

例

システム情報を表示する

```
SHOW SYSTEM
```

シリアル番号を表示する

```
SHOW SYSTEM SERIALNUMBER
```

MAC アドレスを表示する

```
SHOW SYSTEM MACADDRESS
```

製品名を表示する

```
SHOW SYSTEM MODELNAME
```

備考・注意事項

ファンの異常を検出すると、System Fan Speed では Warning 表示になるが、ログには Fan failure が出力される。

ファン・温度の異常な状態が継続した場合、5分または10分ごとにログとトラップが出力される。

関連コマンド

SET SYSTEM CONTACT (221 ページ)

SET SYSTEM LOCATION (223 ページ)

SET SYSTEM NAME (224 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

```
# show time
System time is 17:29:50 on 28-Nov-2009
```

例

現在の日付と時刻を表示する

SHOW TIME

関連コマンド

SET TIME (226 ページ)

SHOW USER

カテゴリ：運用・管理 / ユーザー認証データベース

SHOW USER [= {*login-name* | ALL}]

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

ユーザーアカウントの情報を表示する。

パラメーター

USER ユーザーアカウント情報を表示したいユーザー名を指定する。省略した場合はすべてのユーザーアカウント情報を表示する。

入力・出力・画面例

```
# show user

User Authentication Database
-----
Username: manager (Manager Account)
  Status: enabled   Privilege: manager
  Session: All
  Logins: 3         Fails: 2
Username: operator (User Account)
  Status: enabled   Privilege: user
  Session: All
  Logins: 0         Fails: 0
-----

Active (logged in) Users
-----
User
  Device           Login Time           Location
-----
manager
  Asyn             06:11:28 24-Mar-2009  local
-----
```

User Authentication Database セクション	登録ユーザーの情報が表示される
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)。「user」、「manager」のいずれか
Session	ログインできるセッションタイプ。「All」、「Console」、「Telnet」、「SSH」、「Enhanced Stacking」のいずれか
Logins	ログイン成功回数
Fails	ログイン失敗回数
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
Device	ログインデバイス (セッションタイプ)
Login Time	ログイン日時
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

表 72:

例

現在ログインしているユーザーのユーザー権限を表示する

```
SHOW USER
```

関連コマンド

SET PASSWORD (200 ページ)

SET USER (227 ページ)

SHOW USERCONFIG

カテゴリー：運用・管理 / ユーザー認証データベース

SHOW USERCONFIG

解説

ユーザー認証機能の設定および、カウンターを表示する。

入力・出力・画面例

```
# show userconfig

User module configuration and counters
-----
Security parameters
 login failures before lockout .....      5           (LOGINFAIL)
 lockout period .....                    600 seconds (LOCKOUTPD)
 minimum password length .....           6 characters (MINPWDLEN)

Security counters
 logins .....                             7
 managerPwdChanges .....                 0
 unknownLoginNames .....                0
 totalPwdFails .....                    0
 loginLockouts .....                    0
 databaseClearTotallys .....            0
-----
```

Security parameters セクション	ユーザー認証機能のパラメーターが表示される
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)
minimum password length	パスワードの最小文字数 (MINPWDLEN パラメーター)
Security counters セクション	ユーザー認証機能のカウンターが表示される
logins	本製品へのログイン回数
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
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 73:

関連コマンド

RESET USERCONFIG (182 ページ)

SET USERCONFIG (229 ページ)

UPLOAD

カテゴリ：運用・管理 / アップロード・ダウンロード

```
UPLOAD METHOD=TFTP {SRCFILE|FILE}={ [device:] filename|APPBLOCK|SWITCHCFG}
      SERVER=ipadd DESTFILE=filename
```

```
UPLOAD METHOD=XMODEM {SRCFILE|FILE}={ [device:] filename|APPBLOCK|
      SWITCHCFG}
```

```
UPLOAD METHOD=LOCAL {SRCFILE|FILE}=APPBLOCK DESTFILE=[device:] filename
```

```
UPLOAD METHOD=REMOTESWITCH {SRCFILE|FILE}={ [device:] filename|APPBLOCK|
      SWITCHCFG} SWITCHLIST=switch-list [VERBOSE={YES|NO|ON|OFF|TRUE|FALSE}]
```

device: ファイルが記憶されている媒体。flash を指定

filename: ファイル名

ipadd: IP アドレス

switch-list: リモートスイッチのスイッチ番号 (カンマを使った複数指定も可能)

解説

TFTP、XMODEM でファイルをアップロードする。

METHOD に LOCAL を指定すると、アプリケーションブロック内のファームウェアをフラッシュメモリにアップロード (コピー) する。

METHOD に REMOTESWITCH を指定すると、マスタースイッチのファームウェアまたは設定ファイルをスレーブスイッチにアップロード (転送) する。

パラメーター

METHOD 転送プロトコル。TFTP、XMODEM、LOCAL、REMOTESWITCH を指定。

SRCFILE/FILE アップロード対象のファイル名。APPBLOCK を指定した場合は、アプリケーションブロック内のファームウェアファイルが対象となる。SWITCHCFG を指定した場合は、現在設定されている起動時設定ファイルが対象となる。

SERVER TFTP サーバーの IP アドレス。

DESTFILE アップロード後のファイル名。METHOD に TFTP を指定した場合に設定する。

SWITCHLIST METHOD に REMOTESWITCH を指定した場合に、ファイルの転送先のスレーブスイッチの番号を指定する。スレーブスイッチの番号は、SHOW REMOTELIST コマンドで、「Num」に表示される番号で指定。

VERBOSE METHOD に REMOTESWITCH を指定した場合に、ファイル転送のオペレーションの詳細を表示する/しないを選択する。デフォルトは、YES (表示する)。

例

設定ファイル「test.cfg」を TFTP サーバー「192.168.1.103」にアップロードする

```
UPLOAD METHOD=TFTP FILE=test.cfg SERVER=192.168.1.103 DESTFILE=test.cfg
```

備考・注意事項

エンハンススタッキング機能で、マスタースイッチからスレーブスイッチに接続している場合は、XMODEM は使えない。

マスタースイッチからスレーブスイッチにファームウェアファイルを転送すると、スレーブスイッチは再起動し、起動時に使用するファームウェアが転送されたファイルに切り替わる。

マスタースイッチからスレーブスイッチに設定ファイルを転送すると、スレーブスイッチは再起動し、起動時設定ファイルが転送されたファイルに切り替わる。

SRCFILE/FILE に SWTCHCFG を指定した場合は、IP アドレス、スタックモードの設定は書き換えられないが、ファイル名を指定した場合は、すべての設定が書き換えられる。

TFTP を使うには、事前にローカル IP インターフェース（マネージメント VLAN インターフェース）の設定が必要。詳しくは「IP」の「IP インターフェース」を参照のこと。

関連コマンド

LOAD (166 ページ)

SHOW FILE (257 ページ)