



最初にお読みください

# CentreCOM® 8700SL シリーズ リリースノート

この度は、CentreCOM 8700SL シリーズ（以下、CentreCOM を省略）をお買いあげいただき、誠にありがとうございました。このリリースノートは、取扱説明書（J613-M0019-00 Rev.A、613-000900 Rev.A）とコマンドリファレンス（J613-M0019-01 Rev.N）の補足や、ご使用前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

## 1 ソフトウェアバージョン 2.9.1-21

## 2 重要：2.6.1 pl12 以前からバージョンアップするときの注意事項

ソフトウェアバージョン **2.6.1 pl12** 以前から **2.9.1-21** にバージョンアップすると、最初の再起動時に「設定なし」の状態では起動する場合があります。

このようなときは、バージョンアップ後にコンソールからログインし、SET CONFIG コマンドで起動時設定ファイルを指定しなおした後、本製品を再起動してください。例えば、バージョンアップ前に mynet.cfg という設定ファイルを使用していた場合は、次のようにします。

```
SET CONFIG=mynet.cfg
```

```
RESTART SWITCH
```

また、リモートからバージョンアップを行うときは、バージョンアップ後アクセス不能に陥ることを避けるため、次の手順にしたがってバージョンアップを行ってください。

1. バージョン **2.6.1 pl12** 以前で動作している本製品にログインします。
2. 次のコマンドを実行し、Boot configuration file: に表示されるファイル名をメモします。

```
SHOW CONFIG
```

3. 次のコマンドを実行し、現在の設定を boot.cfg に保存します。boot.cfg は、「設定なし」で起動したときに自動実行される特殊なファイルです。

```
CREATE CONFIG=boot.cfg
```

4. ログアウトします。
5. 「バージョンアップ手順書」の指示にしたがって、**2.9.1-21** にバージョンアップします。
6. バージョン **2.9.1-21** で動作している本製品にログインします。
7. 次のコマンドを実行します。xxxx には手順 2 でメモしたファイル名を指定します。

```
SET CONFIG=xxxx
```

8. 手順 3 で作成した boot.cfg を削除します。

```
DELETE FILE=boot.cfg
```

9. 以上です。

### 3 重要：ハードウェアリビジョンに関する注意 (8724SL V2 のみ)

---

ハードウェアリビジョン D1 以降の 8724SL V2 にソフトウェアをダウンロードする場合は、**2.9.1-16** 以降をご使用ください。

ハードウェアリビジョンは、8724SL V2 の底面に貼付されているシリアル番号シール（バーコード）に記載されています。

(例)




### 4 追加サポートされた機能

---

ソフトウェアバージョン **2.9.1-20** 以降において、以下の機能を追加サポートしました。

#### 4.1 ループガード (LDF 検出)

 **【コマンドリファレンス】 / 【スイッチング】 / 【ポート】**

ループガード機能として LDF 検出機能をサポートしました。本機能は、一定時間毎に特殊な試験フレーム (LDF) を送出し、接続機器を介して同じ LDF が同じ筐体に戻って来た場合に、受信ポートをディセーブルにしたり、ログに記録したりする機能です。なお、LDF 検出機能はリリース済みのソフトウェアバージョン **2.9.1-20** 以降でのサポートとなります。

### 5 本バージョンで修正された項目

---

ソフトウェアバージョン **2.9.1-20** から **2.9.1-21** へのバージョンアップにおいて、以下の項目が修正されました。

- 5.1 サポート対象外の HTTP サーバーが有効なとき（デフォルトは有効）、細工された特殊な HTTP リクエストを受信するとリポートすることがありましたが、これを修正しました。
- 5.2 SSH サーバー機能において、大量の暗号化データを処理中に SSH クライアントとのセッションが切断されるとメモリーリークが発生することがありましたが、これを修正しました。
- 5.3 OSPF と IP ルートフィルターの併用時、IP ルートフィルターの設定に関連する、宛先 IP アドレスが同一でマスクだけが異なる経路が複数ある場合、OSPF の経路情報が正常に登録されないことがありましたが、これを修正しました。
- 5.4 OSPF ASBR としての動作中に再起動すると AS 外部経路を正しく通知しなくなることがありましたが、これを修正しました。
- 5.5 IPv6 サブネットルーターエニーキャストアドレス宛での Ping パケットを受信するとリポートすることがありましたが、これを修正しました。
- 5.6 ファイアウォール NAT（インターフェース NAT のダイナミック ENAT）使用時、PRIVATE 側インターフェースがリンクダウンしていると、PRIVATE 側インターフェースの IP アドレスに宛てた PUBLIC 側からの Ping パケットに誤って応答していましたが、これを修正しました。

- 5.7 ファイアウォール有効時、TCP 以外のフラグメントパケットを Tiny Fragment Attack と誤認識して破棄していましたが、これを修正しました。
- 5.8 下記の条件をすべて満たした設定で DHCP サーバー機能を使用している場合、DHCP レンジが設定されている VLAN の 1 つがリンクアップしている状態で、それ以外の VLAN がリンクアップするとリポートすることがありましたが、これを修正しました。
- ・ 2 つ以上の VLAN に対して DHCP レンジが設定されている
  - ・ 各 DHCP レンジ設定に「PROBE=ARP」の設定が含まれている

下記の項目は、ソフトウェアバージョン **2.9.1-20** のリリースノートに記載されていませんでしたが、実際には **2.9.1-20** で修正されていました。

- 5.9 CREATE SWITCH TRUNK コマンドの PORT パラメーターでトランクポートを指定した場合、指定ポートがマルチプル VLAN (Protected Port VLAN) の同一グループ所屬であるかのチェックが行われませんでした。これを修正しました。
- 5.10 ファイアウォール有効時、RTSP パケット (ポート番号: 554) を許可するようルールを設定しても、パケットが転送されませんでした。これを修正しました。
- 5.11 ファイアウォール NAT を使用している環境で、PUBLIC 側から PRIVATE 側へ traceroute を実行すると、PRIVATE 側から返信される ICMP メッセージ (TTL Exceeded) 内のオリジナルヘッダーに PRIVATE 側アドレスが未変換のまま残っていましたが、これを修正しました。

## 6 本バージョンでの制限事項

---


ソフトウェアバージョン **2.9.1-21** には、以下の制限事項があります。

### 6.1 RADIUS

 [「コマンドリファレンス」](#) / [「運用・管理」](#) / [「認証サーバー」](#)

- 複数の IP インターフェイス (IP アドレス) を設定している場合、RADIUS Access-Request パケットの始点 IP アドレスと NAS-IP-Address の値が異なることがあります。両者を一致させたい場合は、RADIUS サーバーの指定時 (ADD RADIUS SERVER コマンドの実行時) に、LOCAL パラメーターでローカル IP インターフェイスを指定してください。
- RADIUS サーバーを複数登録している場合、最初に登録した RADIUS サーバーに対してのみ、SET RADIUS コマンドの RETRANSMITCOUNT パラメーターが正しく動作しません。最初の RADIUS サーバーへの再送回数のみ、RETRANSMITCOUNT の指定値よりも 1 回少なくなります。


### 6.2 ZMODEM によるファイル受信

 [「コマンドリファレンス」](#) / [「運用・管理」](#) / [「アップロード・ダウンロード」](#)

ZMODEM によるファイル受信 (LOAD METHOD=ZMODEM) にターミナルソフト側で送信をキャンセルすると、コマンドプロンプトに復帰しないことがあります。ターミナルソフトが Windows 付属のハイパーターミナルの場合、本現象は起こりません。

---

### 6.3 ログ

 **「コマンドリファレンス」 / 「運用・管理」 / 「ログ」**

CREATE LOG OUTPUT コマンドの QUEUEONLY、MAXQUEUESEVERITY パラメーターが機能しません。

---


### 6.4 スクリプト

 **「コマンドリファレンス」 / 「運用・管理」 / 「スクリプト」**

スクリプトで IF THEN ELSE 文を使用する際、比較対象文字列の長さが 32 文字以上の場合、スクリプトが正しく動作しません。31 文字以下の長さの比較対象文字列を使用してください。

---


### 6.5 SNMP

 **「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」**

- イーサネット MIB の dot3StatsCarrierSenseErrors の値が取得できません。
- イーサネット MIB の dot3StatsFrameTooLongs が正しくカウントアップされません。
- プライベート MIB の atrMacBasedAuthPaeState において、本来と異なる値を持つものがあります。
  - ・ authenticated(5) になるべき MIB の値が、authenticating(6) になります。
  - ・ held(7) になるべき MIB の値が、aborting(6) になります。
  - ・ SET PORTAUTH PORT コマンドで「SET PORTAUTH=MACBASED PORT=5 CONTROL=AUTHORISED!UNAUTHORISED」を設定しても、MIB の値が forceAuth(8) または forceUnauth(9) にならず、initialise(1) になります。
- プライベート MIB の atrMacBasedAuthControlledPortStatus において、本来と異なる値を持つものがあります。
  - ・ 認証を行っていないにもかかわらず MIB の値が unauthorised(2) にならず、authorised(1) になります。
  - ・ SET PORTAUTH PORT コマンドで「SET PORTAUTH=MACBASED PORT=xx CONTROL=AUTHORISED!UNAUTHORISED」を設定しても、MIB の値が forceAuth(10) または forceUnauth(12) にならず、never(1) になります。
- プライベート MIB の restart の値を Get Next Request では取得できません。Get Request ならば取得できます。

---

### 6.6 NTP

 **「コマンドリファレンス」 / 「運用・管理」 / 「NTP」**

SET NTP UTCOFFSET=NONE を実行した後、設定を保存して再起動すると、起動時に「Invalid zone or time for UTC offset.」というエラーメッセージが表示されます。タイムゾーンをデフォルト値に戻す場合は、SET NTP UTCOFFSET=UTC (または GMT) のように指定してください。

---

### 6.7 SET ASYN コマンド

 **「コマンドリファレンス」 / 「運用・管理」 / 「ターミナルサービス」**

SET ASYN コマンドの PROMPT パラメーターでコマンドプロンプトの文字列を変更した後、「SHOW CONFIG DYNAMIC」を実行すると、プロンプト文字列がデフォルト設定に戻ります (SET ASYN コマンドの設定自体はダイナミックコンフィグ中に残っています)。

---

## 6.8 TELNET コマンド

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「ターミナルサービス」

TELNET コマンドの実行時に DNS サーバーへの問い合わせが行われた場合、DNS サーバーからの応答に IPv6 アドレスが含まれていると、TELNET コマンドが反応しなくなります。

---


## 6.9 BPDU フォワーディング

 **参照** 「コマンドリファレンス」 / 「スイッチング」

BPDU フォワーディング有効時、受信した BPDU に 4 Byte のデータを付加して転送します。

---


## 6.10 ポートトランッキング

 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」

コマンドの入力順によっては、トランクグループ内にタグなしポートとタグ付きポートの両方を所属させてもエラーになりません。これを回避するため、トランクグループの作成は (1) メンバーポートのタグ設定、(2) トランクグループの作成、の順に行ってください。

---


## 6.11 ポートセキュリティ


 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」


ポートセキュリティがオンのポートで受信したパケットの VLAN ID が、ポートの所属 VLAN と一致しない場合でも、アドレスを FDB に登録します。


---

## 6.12 ループガード (LDF 検出)

 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「ログ」

 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「スパンニングツリー (STP/RSTP)」


 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「ポート認証」

- LDF 検出機能とスパンニングツリープロトコル (STP/RSTP) を併用するときは、ルートブリッジにだけ LDF 検出の設定を行ってください。
- LDF 検出機能と 802.1X 認証を併用するときは、デフォルトの Single-Suppliant モードを使ってください。Multi-Suppliant モードは使えません。  
(MAC ベース認証には Single-Suppliant モード、Multi-Suppliant モードの区別がないため、本制限は適用されません)
- LDF 検出機能と MAC ベース認証を併用するときは、LDF の宛先 MAC アドレス (FE-FF-FF-xx-xx-xx。xx-xx-xx はスイッチの MAC アドレス下位 3 オクテット) を MAC ベース認証ユーザーとして RADIUS サーバーに登録してください。  
なお、本設定は、LDF 検出と MAC ベース認証を併用するときだけに必要な特殊な設定です (通常の MAC ベース認証ユーザーは認証対象機器の MAC アドレス (送信元 MAC アドレス) になります)。
- LDF 検出機能と MAC ベース認証を併用するときは、SET PORTAUTH PORT SUPPLICANTMAC コマンド (Suppliant 固有設定) を使わないでください。  
(802.1X 認証は Single-Suppliant モードのみ併用可能なため、Multi-Suppliant モード用の同コマンドはもともと使用できません)

- LDF 検出機能と MAC ベース認証を併用しているときは、「FDB のエージングタイム × 2」（デフォルトでは  $300 \times 2 = 600$  秒）の間隔で認証に関するログメッセージが出力されます。これを回避するには、ログメッセージフィルターで該当ログ（条件：TYPE=portauth、MSGTEXT=%fe-ff-ff）を無視（ACTION=IGNORE）するよう設定してください。

---


### 6.13 LACP (IEEE 802.3ad)

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「LACP \(IEEE 802.3ad\)」](#)

LACP によって自動生成されたトランクグループのメンバーポートに対して CREATE SWITCH TRUNK コマンドを実行すると、通信ができなくなります。

---


### 6.14 バーチャル LAN

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「バーチャル LAN」](#)

Protected VLAN の所属ポートをミラーリングのソースポートに設定すると、Protected VLAN のポート間で通信ができなくなります。

---


### 6.15 スパニングツリープロトコル (STP/RSTP)

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「スパニングツリー \(STP/RSTP\)」](#)

スパニングツリープロトコル (STP) 有効時、スイッチポートがリンクダウンしても STP のポート状態が Forwarding のまま変化しません。このため、スパニングツリーの再構成にかかる時間が最大エージタイム (MaxAge) の分だけ長くなります。

---


### 6.16 フォワーディングデータベース

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「フォワーディングデータベース」](#)

- エラーパケットを受信したときも、送信元 MAC アドレスをフォワーディングデータベース (FDB) に登録します。
- フィルタリング対象の MAC アドレスを持つ機器が、PORT パラメーターで指定したのとは異なるポートに接続されている場合、本製品から該当 MAC アドレスに宛てたパケットに対して、ACTION=DISCARD のスタティックエントリー（スイッチフィルター）が正しく機能しません。

---

### 6.17 ハードウェア IP フィルター

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ハードウェア IP フィルター」](#)

- 8748SL では、ポート 25 ~ 48 とポート 49 で受信したパケットに対して、ハードウェア IP フィルターの SENDNONUNICASTTOPORT、SENDEPORT アクションが機能しません。
- フレームタイプ 802.3 raw の IPX パケットにマッチさせるため、DSAP / SSAP = 0xFFFF の条件を持つフィルターエントリーを作成した場合、このエントリーはフレームタイプ Ethernet 2 の IPX パケットにもマッチしてしまいます。
- ADD SWITCH L3FILTER MATCH コマンドで IMPORT=False、または EMPORT=False を指定すると、IMPORT=True、EMPORT=True の設定で動作します。False で動作させたい場合は、IMPORT、EMPORT パラメーターを指定しないでください（デフォルトで False の設定になります）。

- フレームフォーマットとして 802.2 LLC を指定したハードウェア IP フィルターに対し、ADD SWITCH L3FILTER ENTRY コマンドで TYPE=0000 のエントリーを作成しようとするとエラーになります。また、このとき表示されるエラーメッセージが適切ではありません。

---


## 6.18 ポート認証

 **「コマンドリファレンス」 / 「スイッチング」 / 「ポート認証」**

- 802.1X Multi-Suppllicant モードの Authenticator ポートでは、Port Status が authorised でも IGMP Query パケットがフラッディングされません。
- ENABLE/SET PORTAUTH PORT コマンドの SERVERTIMEOUT パラメーターが正しく動作しません。これは、SET RADIUS コマンドの TIMEOUT パラメーターと RETRANSMITCOUNT パラメーターの設定が優先されているためです。SET RADIUS コマンドで TIMEOUT × (RETRANSMITCOUNT + 1) の値を SERVERTIMEOUT より大きく設定した場合は、SERVERTIMEOUT の設定が正しく機能します。
- RADIUS サーバーによってダイナミック VLAN を割り当てられた Suppllicant がリンクダウン、ログオフなどで存在しなくなった場合、プライベート MIB の AuthPreAuthVlan、AuthPostAuthVlan が不正な値を返します。
- ポートの 802.1X 認証機能をいったん無効にしてから再度有効にすると、Authenticator は Suppllicant の MAC アドレスをゲスト VLAN 上で学習しません。
- MAC ベース認証において再認証に失敗しても、プライベート MIB の atrMacBasedAuthUnauthenticated トラップが送信されません。

---


## 6.19 DHCP Snooping

 **「コマンドリファレンス」 / 「スイッチング」 / 「DHCP Snooping」**

(8748SL のみ) DHCP Snooping 使用時、接続可能クライアント数 (SET DHCPSPNOOPING PORT コマンドの MAXLEASES パラメーター) は、システム全体で 503 以下になるよう設定してください。MAXLEASES の合計が 504 以上の状態で設定を保存して再起動すると、起動時にエラーが発生することがあります。

---


## 6.20 IP 統計情報

 **「コマンドリファレンス」 / 「IP」**

ファイアウォール有効時、SHOW IP INTERFACE COUNTER コマンドで表示される受信パケットカウンター (ifInPkts、ifInBcastPkts、ifInUcastPkts、ifInDiscards) に、実際の受信パケット数の 2 倍の値が表示されます。

---


## 6.21 ディレクティブブロードキャストパケット

 **「コマンドリファレンス」 / 「IP」**


特定 VLAN に対するディレクティブブロードキャスト転送をオンにしている場合、ブロードキャスト MAC アドレス (FF-FF-FF-FF- FF-FF) 宛でのディレクティブブロードキャストパケットを (別 VLAN で) 受信すると、それ以降、本体 MAC アドレス宛てに送信された通常のディレクティブブロードキャストパケットを転送できなくなります。

---

## 6.22 IP モジュール無効時の注意事項

 [「コマンドリファレンス」 / 「IP」](#)

 [「コマンドリファレンス」 / 「IP」 / 「IP インターフェース」](#)

 [「コマンドリファレンス」 / 「IP」 / 「ARP」](#)

IP モジュールが無効の状態では IP インターフェースの作成 (ADD IP INTERFACE コマンド) とスタティック ARP エントリーの登録 (ADD IP ARP コマンド) を順に行くとリポートしません。これを回避するため、IP 関連の設定は ENABLE IP コマンドで IP モジュールを有効にしてから行うようにしてください。

---

## 6.23 ローカル IP インターフェース (ループバックインターフェース)

 [「コマンドリファレンス」 / 「IP」 / 「IP インターフェース」](#)

ローカル IP インターフェース (ループバックインターフェース) にブロードキャストアドレスを指定してもエラーになりません。ローカル IP インターフェースに IP アドレスを割り当てるときは、割り当てようとしている IP アドレスがご使用のネットワークにおいて利用可能なものであるかどうかを確認してください。

---

## 6.24 Gratuitous ARP

 [「コマンドリファレンス」 / 「IP」 / 「IP インターフェース」](#)

IP インターフェースの設定 (ADD/SET IP INTERFACE コマンド) で Gratuitous ARP を受け入れないようにしても、Gratuitous ARP Request パケット受信時には ARP キャッシュを更新します。

---

## 6.25 ADD IP ROUTE コマンド

 [「コマンドリファレンス」 / 「IP」 / 「経路制御」](#)

ADD IP ROUTE コマンドで METRIC1 パラメーターに値を指定し、METRIC2 パラメーターには値を指定しない場合、METRIC2 パラメーターに省略時の 1 が設定されず、METRIC1 パラメーターで指定した値が設定されます。

---


## 6.26 RIP

 [「コマンドリファレンス」 / 「IP」 / 「経路制御 \(RIP\)」](#)

ADD/SET IP RIP コマンドの DEMAND パラメーターを YES にした後で再び NO (デフォルト) に戻すと、RIP 経路がタイムアウトなくなります。

---

## 6.27 OSPF

 [「コマンドリファレンス」 / 「IP」 / 「経路制御 \(OSPF\)」](#)

- SET OSPF コマンドで DEFROUTE=OFF を指定しても、デフォルトルートの AS 外部 LSA を生成します (DEFROUTE=OFF が機能しません)。
- ADD/SET OSPF REDISTRIBUTE コマンドで SUBNET=OFF を指定しても、クラスフル、クラスレス両方の経路を取り込みます (SUBNET=OFF が機能しません)。



---

## 6.28 DNS キャッシュ

 **「コマンドリファレンス」 / 「IP」 / 「名前解決」**

DNS キャッシュ機能のキャッシュサイズを 1 に設定した場合、最初のキャッシュエントリーがエージングも上書きもされずに残り続けます。キャッシュサイズを 1 に設定しないでください。

---

## 6.29 UDP ブロードキャストヘルパー

 **「コマンドリファレンス」 / 「IP」 / 「UDP ブロードキャストヘルパー」**

フラグメント化されている UDP ブロードキャストパケットは転送されません。

---

## 6.30 DVMRP

 **「コマンドリファレンス」 / 「IP マルチキャスト」 / 「DVMRP」**

- DVMRP インターフェースを削除し、再度追加した場合、該当インターフェース上の DVMRP 経路がホールドダウン状態のままとなります。
- DVMRP が有効で、IGMP Snooping が無効のとき、マルチキャストデータがフラッディングされません。

---

## 6.31 PIM

 **「コマンドリファレンス」 / 「IP マルチキャスト」 / 「PIM」**

- (PIM-DM) Prune 中に上流ルーターの Generation ID が変更されても Prune メッセージを再送せず、結果として、次の Prune メッセージを送信するタイミングまで不要なマルチキャストトラフィックを受信してしまいます。
- (PIM-SM) すべてのポートがリンクダウンしている状態で ADD PIM BSRCANDIDATE コマンドを実行すると、警告メッセージが表示されます。

---

## 6.32 IGMP

 **「コマンドリファレンス」 / 「IP マルチキャスト」 / 「IGMP」**

Last Member Query Interval タイマーの起動中に Report メッセージを受信しても、同タイマーが更新されず、Group-specific Membership Query を再送信してしまいます。

---

## 6.33 IGMP Snooping

 **「コマンドリファレンス」 / 「IP マルチキャスト」 / 「IGMP Snooping」**

- SET IGMPSPNOOPING ROUTERMODE コマンドでパラメーターに NONE を指定しても、224.0.0.1 および 224.0.0.2 からのマルチキャストパケットを受信した場合には All Group を作成します。All Group を作成しない場合は、DISABLE IP IGMP ALLGROUP コマンドを使用してください。
- DVMRP または PIM を有効にしているとき、IGMP Snooping を無効に設定しても、マルチキャストトラフィックの受信インターフェース (VLAN) においては、該当トラフィックが VLAN 内にフラッディングされません。

---

## 6.34 MVR

 **「コマンドリファレンス」 / 「IP マルチキャスト」 / 「MVR」**

(8748SL のみ) 「1 ~ 24、50」と「25 ~ 48、49」のポートグループをまたぐ構成で複数の VLAN を作成し、MVR を利用したマルチキャスト通信を行っているとき、片方のポートグループで IGMP Leave メッセージを受信すると、もう片方のポートグループでもマルチキャスト通信が停止します。

---

## 6.35 ファイアウォール

 **「コマンドリファレンス」 / 「ファイアウォール」**

- PUBLIC 側で受信したパケットを破棄した場合、SHOW FIREWALL POLICY コマンドの COUNTER オプションで表示される Total Packets Received カウンターが 2 ずつカウントされます。
- ファイアウォールポリシーにアクセスリストを登録する場合、IP アドレスリストよりルール番号の大きい MAC アドレスリストは有効になりません。MAC アドレスリストのルール番号は IP アドレスリストのルール番号よりも小さくなるように設定してください。
- PUBLIC 側から PRIVATE 側に対して FTP 通信を行った場合、SHOW FIREWALL SESSION コマンドで不要なセッションが表示されることがあります。これは表示だけの問題であり、動作には影響ありません。
- PUBLIC 側インターフェースにルール NAT (エンハンスド、リバース、ダブルのいずれか) を設定した場合、PUBLIC 側から PRIVATE 側への FTP 通信が正常に行えないことがあります。
- 攻撃検出機能によって攻撃を検出したとき、検出されたパケットが許可されているにも関わらず、SHOW FIREWALL EVENT コマンドの出力では Deny Event (拒否イベント) に表示されます。
- ファイアウォール有効時、TCP コネクションキュー内に確立したセッションが残ってしまいます。

---

## 7 取扱説明書・コマンドリファレンスの補足・誤記訂正

取扱説明書とコマンドリファレンスの補足事項です。

---


### 7.1 8724SL の最大消費電力

 **「取扱説明書」 132 ページ**

取扱説明書には 8724SL の最大消費電力が「51W」と記載されていますが、正しくは「50W」です。

---


### 7.2 HTTP サーバー (サポート対象外)

 **「コマンドリファレンス」 / 「運用・管理」 / 「システム」**

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

---

### 7.3 弊社 CentreNET SwimRadius (Ver.1.1 pl 0 以前) 使用時の注意

 [「コマンドリファレンス」](#) / [「運用・管理」](#) / [「認証サーバー」](#)


本製品自身（コマンドラインインターフェース）へのログイン認証に弊社 CentreNET SwimRadius の Ver.1.1 pl 0 以前を使用する場合は、以下の点にご注意ください。

なお、Ver.1.1 pl 1 以降の SwimRadius は、ユーザーごとに Service-Type 属性の有無と値を設定できるようになっているため、下記の制限はありません。

- Ver.1.1 pl 0 以前の SwimRadius は、Telnet で接続してきたユーザーの認証要求に対して Access-Accept（認証成功）を返すとき、Service-Type 属性を付加しますが、同属性の値としてはつねに Administrative(6) をセットするため、Ver.1.1 pl 0 以前の SwimRadius によって認証された Telnet ユーザーは、つねに Security Officer レベルでログインすることとなります。
- Ver.1.1 pl 0 以前の SwimRadius は、コンソールポート経由で接続してきたユーザーの認証要求に対して Access-Accept（認証成功）を返すときに Service-Type 属性を付加しません。本製品は Service-Type 属性のない Access-Accept を受信した場合は該当ユーザーのログインを許可しないため、コンソールポート経由のログイン認証を Ver.1.1 pl 0 以前の SwimRadius で行うことはできません。

---


### 7.4 DESTINATION=ROUTER のログ出力先定義

 [「コマンドリファレンス」](#) / [「運用・管理」](#) / [「ログ」](#)

DESTINATION=ROUTER のログ出力先定義を使用するときは、ログの送信側と受信側で同一ファームウェア（ファイル名とバージョンが同じもの）を使用してください。それ以外の構成はサポート対象外とさせていただきますのでご注意ください。

---

### 7.5 送信元アドレスがマルチキャスト MAC アドレスの Ethernet フレーム

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ポート」](#)


 [「コマンドリファレンス」](#) / [「IP」](#) / [「ARP」](#)

受信した Ethernet フレームの送信元アドレスがマルチキャスト MAC アドレスだった場合、このフレームは転送されずに破棄されます。

ただし、ENABLE IP MACDISPARITY コマンドを実行した上で、マルチキャスト MAC アドレスのスタティック ARP エントリを登録すれば、このマルチキャスト MAC アドレスを送信元とする Ethernet フレームを転送させることが可能です。

---


### 7.6 スイッチポートの統計カウンター（8748SL のみ）

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ポート」](#)

8748SL では、ポートグループ「1～24、50」と「25～48、49」をまたぐパケットは、SHOW SWITCH PORT COUNTER コマンドで表示される ifOutUcastPkts、ifOutErrors、DropEvents カウンターにカウントされません。

---


### 7.7 1000Mbps ポートのフラッディングレート

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ポート」](#)

リンクしている 10/100Mbps ポートの数によって、拡張モジュールの 1000Mbps ポートのブロードキャスト、マルチキャストの転送率が下がる場合があります。

---


## 7.8 ポート帯域制限機能の受信レート上限値とTCP通信のスループット


 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ポート」](#)

スイッチポートに受信レート上限値 (INGRESSLIMIT) を設定している場合、同ポートを経由したTCPの通信では、TCPデータのスループットが設定した上限値よりも低くなります (低下の度合いは通信状況に依存します)。これはTCPプロトコルの特性として、帯域制限機能によって破棄されたパケットの再送処理などが発生するためです。また、TCP以外においても、同様の再送処理を行うプロトコルではこの現象が発生する可能性があります。

---

## 7.9 ポート帯域制限機能の受信レート上限値とハードウェアIPフィルタ

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ポート」](#)

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ハードウェアIPフィルタ」](#)

ポート帯域制限機能の受信レート上限値 (INGRESSLIMIT) とハードウェアIPフィルタを併用している場合、ハードウェアIPフィルタのNODROPエントリーにマッチしたパケットに対して、受信レート上限値が適用されないことがあります。これを回避するには、EDITコマンドで設定ファイルを開き、受信レート上限値の設定コマンド (SET SWITCH PORT=x INGRESSLIMIT=x) がハードウェアIPフィルタ設定コマンドの後にくるよう編集するか、あるいは、次のような再起動トリガーを定義して、起動時に受信レート上限値の設定が自動的に再入力されるようにしてください。

再起動トリガーの設定例

```
ENABLE TRIGGER
```


```
CREATE TRIGGER=1 REBOOT=ALL SCRIPT=INGRESS.SCP
```

トリガースクリプト INGRESS.SCP の例

```
SET SWITCH PORT=1 INGRESSLIMIT=1000
```

---

## 7.10 ダイナミックポートセキュリティー

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ポート」](#)

ダイナミックポートセキュリティー使用時 (RELEARN=ON)、スイッチポートがロックされた後に、ADD SWITCH FILTER コマンドでスタティックエントリーを追加するとき、ENTRY パラメーターを省略するとエントリー番号が0から始まり、結果的に設定保存後の再起動時にエラーが発生することがあります。これを回避するため、スイッチポートのロック後にスタティックエントリーを追加するときは、ENTRY パラメーターに0から始まる番号を指定してください。

---


## 7.11 マルチプルスパンニングツリープロトコル (MSTP)

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「マルチプルスパンニングツリープロトコル」](#)

DISABLE MSTP MSTI PORT コマンドを実行してマルチプルスパンニングツリープロトコル (MSTP) を無効にしたポートでは、MACアドレスの学習が行われません。BPDUを送信する必要がないポートでは、DISABLE MSTP MSTI PORT コマンドを使用するのではなく、SET MSTP CIST PORT コマンドのEDGEPORTパラメーターにYESを指定してエッジポートに設定してください。

---

## 7.12 フォワーディングデータベース

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「フォワーディングデータベース」](#)

1 回目のエージアウトでは、すべてのダイナミックエントリーがフォワーディングデータベースから削除されない場合があります。ただし、2 回目以降のエージアウトではすべてのダイナミックエントリーが削除されます。

---

## 7.13 ハードウェア IP フィルター

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ハードウェア IP フィルター」](#)

- IPv6 ルーティングを有効にしている場合、ルーティング対象の IPv6 パケットに対して、EtherType = 0x86DD (IPv6) の条件を持つハードウェア IP フィルターエントリーがマッチしません。ルーティング対象の IPv6 パケットをフィルタリングするには、IPv6 フィルターを使用してください。ルーティング対象でない (スイッチングされる) IPv6 パケットには、前述のハードウェア IP フィルターがマッチします。
- IPX ルーティングを有効にしている場合、ルーティング対象の IPX パケットに対しては、SENDMIRROR 以外のアクションが機能しません。また、SENDMIRROR アクションと EPORT パラメーターは併用できません。ルーティング対象の IPX パケットをフィルタリングするには、IPX トラフィックフィルターを使用してください。なお、ルーティング対象でない (スイッチングされる) IPX パケットには、すべてのアクションが機能します (ただし、IP パケットを前提としている MOVETOSTOPRIO、SETTOS、MOVEPRIOTOTOS、SETIPDSCP アクションは使用不可)。

---


## 7.14 ポート認証

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ポート認証」](#)

ポート認証 (802.1X 認証、MAC ベース認証) を有効にしたポートでは、ポートトラッキング、スパンニングツリープロトコル、ポートセキュリティーを使用できません。また、802.1X 認証の Authenticator ポートと MAC ベース認証ポートをタグ付きに設定することはできません。

---

## 7.15 ICMP TTL Exceeded メッセージの送出インターフェース

 [「コマンドリファレンス」](#) / [「IP」](#)

ICMP TTL Exceeded メッセージは、(他のインターフェース上に最適経路が存在していても) TTL=1 の IP パケットを受信したインターフェースから送出されます。

---


## 7.16 IP マルチキャストのハードウェア処理

 [「コマンドリファレンス」](#) / [「IP マルチキャスト」](#) / [「概要」](#)

スイッチ間をタグ付きポートで接続している場合、タグ付きポートを通過する IP マルチキャストパケットは、最初に ADD IP INTERFACE コマンドを実行した VLAN の VID を持つものだけがハードウェア処理の対象となり、他の VID を持つパケットはソフトウェア処理となります。ソフトウェア処理される場合のパフォーマンスは「ワイヤースピード ÷ VLAN 数」となります。タグ VLAN 環境で IP マルチキャストを使用するときは、タグ付きポートに割り当てる VLAN 数を 3 つまでにすることをおすすめします。

---

## 7.17 ルーター通知 (RA)

 **「コマンドリファレンス」 / 「IPv6」 / 「近隣探索」**

システム再起動により IPv6 インターフェースがダウンした場合は、Lifetime=0 のルーター通知 (RA) パケットを送信しません。

---

## 7.18 PIM

 **「コマンドリファレンス」 / 「IP マルチキャスト」 / 「PIM」**

(PIM-DM/PIM-SM) マルチキャストデータの通信負荷が高いと、PIM パケットを処理できず、マルチキャスト通信が途絶えることがあります。これを避けるには、次のようなハードウェア IP フィルターを設定し、PIM パケットを優先的に処理させるようにしてください。


```
ADD SWITCH L3FILTER MATCH=DIP DCLASS=HOST
```


```
ADD SWITCH L3FILTER=1 ENTRY DIP=224.0.0.13 PRIO=5 AC=SEND
```

---

## 7.19 IGMP Snooping/MLD Snooping 無効時のポート帯域制限 (INGRESSLIMIT) 設定

 **「コマンドリファレンス」 / 「スイッチング」 / 「ポート」**

 **「コマンドリファレンス」 / 「IP マルチキャスト」 / 「IGMP Snooping」**

 **「コマンドリファレンス」 / 「IPv6 マルチキャスト」 / 「MLD Snooping」**

IGMP Snooping や MLD Snooping を無効に設定しているときは (デフォルトは有効)、スイッチポートの受信レート上限値 (INGRESSLIMIT) を 1000Kbps 未満に設定しないでください。1000Kbps 未満に設定すると、該当ポートで受信したマルチキャストパケットが他のポートにフラッディングされなくなります。

---

## 8 未サポートコマンド (機能)

以下のコマンド (機能) はサポート対象外ですので、あらかじめご了承ください。

- 以下のキーワードを含む全コマンド

ENABLE、ADD、SET、SHOW などの後に [?] キーを押すと表示される機能別キーワードです。

ACC, APPLTALK, BRI, CLASSIFIER, CLNS, DHCP6, EPSR, ETH, FRAMERELAY, GARP, GRE, GUI, HTTP, IPSEC, ISAKMP, ISDN, L2TP, LAPB, LAPD, LDAP, LLDAP, LOADBALANCER, LB, LPD, MACFF, MIOX, PKI, PKT, PRI, Q931, RSVP, SA, SERVICE, SKEY, SSL, STACK, STAR, STARTUP, STREAM, STT, SYN, TACACS, TACPLUS, TEST, TPAD, VLANRELAY, X25C, X25T, TDM, DS3, VOIP

- 以下のコマンド (パラメーター)

太字はコマンド名、細字は該当コマンドのパラメーター名です。

**COPY/DUMP/MODIFY**  
**SET/START/STOP PKT**  
**SHOW BUFFER** [SCAN[=ADDRESS]] [QUEUEPOINTERS]]  
**SHOW SYSTEM TEMPERATURE**  
**SET SYSTEM HOSTID**  
**SET SYSTEM TERRITORY**

```
SET SYSTEM DISTINGUISHEDNAME
LOAD [METHOD=LDAP] [ATTRIBUTE] [BASEOBJECT]
TRACE [ADDRONLY]
PING [APPLEADDR] [OSIADDRESS] [SAPPLEADDRESS] [SOSIADDRESS]
SET PING [APPLEADDR] [OSIADDRESS] [SAPPLEADDRESS] [SOSIADDRESS]
PURGE FILE TRANSLATIONTABLE
PURGE PING TOTALLY
SET/SHOW SWITCH SOCK
SHOW SWITCH MEMORY
SHOW SWITCH SWTABLE
SET SWITCH PORT [MULTICASTMODE] [SPEED={xxxMHAUTO ; xxxMFAUTO ;
1000MHAF}]
DISABLE/ENABLE SWITCH BIST
SET VLAN VIRTACTIVATION
ADD/DELETE/SET IP FILTER [PRIORITY]
ADD/SET IP ROUTE FILTER [POLICY] [PROTOCOL={STATIC ; INTERFACE}]
ADD/DELETE/DISABLE/ENABLE/SET/SHOW IP EGP
ADD/DELETE/SET/SHOW IP SA
ADD/SET IP INTERFACE [VJC] [PRIORITYFILTER] [MULTICAST]
[IGMPPROXY]
ADD/DELETE/SET IP ROUTE BLACKHOLE
ADD/SET IP RIP [NEXTHOP]
SET IP RIP NEWIPADDRESS
SET IP ARP [DLCI] [CIRCUIT]
CREATE/DESTROY/SHOW IP POOL
SHOW IP ROUTE [CACHE]
SHOW IP CACHE
SHOW IP ROUTE TEMPLATE
SHOW IP ROUTE MULTICAST
SET/SHOW IP FLOW
DISABLE/ENABLE IP FOFILTER
DISABLE/ENABLE IP MULTICASTSWITCHING
DISABLE/ENABLE IP SRCROUTE
ADD IP ROUTEMAP [MATCH TAG]
ADD IPV6 INTERFACE IPADDRESS={DHCP;DHCPTMP;PD} [APPINT] [HINT]
[KEY] [PRIORITYFILTER] [TYPE=ANYCAST]
SET IPV6 INTERFACE [PRIORITYFILTER]
ADD/SET IPV6 FILTER [PRIORITY]
DISABLE/ENABLE IPV6 FLOW
ADD/SET PIM6 INTERFACE [MODE=DENSE] [SRCAPABLE]
SET PIM6 [SOURCEALIVETIME] [SRINTERVAL]
SHOW PIM6 [STATEREFRRESH]
ADD/DELETE/SET DVMRP [DLC]
ADD/DELETE/SET DVMRP INTERFACE [DLC]
DISABLE/ENABLE ENCO COMPSTATISTICS
SHOW ENCO CHANNEL
SHOW ENCO COUNTER={DES ; HMAC ; JOBPROCESSING ; PRED ; STAC ;
USER ; UTIL}
```

SHOW IPX CALLLOG  
CREATE QOS  
ADD/DELETE QOS  
SET QOS PORT  
SET QOS POLICY  
SET QOS TRAFFICCLASS  
SET QOS FLOWGROUP  
SHOW QOS POLICY  
SHOW QOS TRAFFICCLASS  
SHOW QOS FLOWGROUP  
ADD/SET PIM INTERFACE [SRCAPABLE] [DLCI]  
DELETE PIM INTERFACE [SRCAPABLE]  
SHOW PIM [STATEREFRRESH]  
ADD/SET PIM BSRCANDIDATE [HASHMASKLENGTH]  
CREATE/DESTROY PPP [AUTHMODE] [BAPMODE] [CBMODE] [CBDELAY]  
[COPY] [DEBUGMAXBYTES] [DESCRIPTION] [FRAGMENT]  
[FRAGOVERHEAD] [LOGIN] [MAXLINKS] [MRU] [NULLFRAGTIMER]  
[NUMBER] [TYPE]  
ADD/DELETE PPP [AUTHENTICATION] [CBDELAY] [CBMODE] [CBNUMBER]  
[CBOperation] [COMPALGORITHM] [COMPRESSION] [CONFIGURE]  
[MODEM] [NUMBER] [PREDCHECK] [RESTART] [STACHECK] [TERMINATE]  
[TYPE]  
ADD/DELETE/SET PPP ACSERVICE  
ADD/DELETE/DISABLE/ENABLE/SET PPP TEMPLATE  
ADD/DELETE PPP MAXSESSIONS  
ADD/DELETE PPP ACRADIUS  
ADD/DELETE PPP VLAN  
DISABLE/ENABLE PPP ACCESSCONCENTRATOR  
ACTIVATE PPP RXPKT  
SET BOOTP MAXHOPS  
DISABLE/ENABLE DHCP [BOOTP]  
DISABLE/ENABLE DHCPSPNOOPING STRICTUNICAST  
ADD/DELETE DHCPSPNOOPING BINDING [ROUTER]  
ADD/DELETE/ENABLE/SHOW DHCPSPNOOPING XLA  
DISABLE/ENABLE DHCPSPNOOPING IPFILTERING  
DISABLE/ENABLE DHCPSPNOOPING LOG  
SET DHCPSPNOOPING ARPSECURITY [ACTION={NONE|DISABLE}]  
ENABLE DHCPSPNOOPING BLOCK={ALL,IP}  
DISABLE/ENABLE BGP DAMPING  
CREATE/SET BGP DAMPING PARAMETERSET  
ADD/SET IP RIP REDISTRIBUTE [ROUtemAP] [LIMIT] [METRIC] [SUBNET]  
ADD/SET OSPF REDISTRIBUTE [ROUtemAP]  
ADD/SET OSPF AREA [NSSATRANSLATOR] [NSSASTABILITY]  
ADD/CREATE/DELETE/DESTROY/SHOW FIREWALL POLICY DYNAMIC  
ADD/DELETE FIREWALL POLICY HTTPFILTER  
ADD FIREWALL POLICY INTERFACE [TRUSTPRIVATE]  
ADD/DELETE FIREWALL POLICY PROXY



```
ADD/SET FIREWALL POLICY RULE [ENCAPSULATION]
[NATTYPE={ENAPT;NATP}] [TTL]
ADD/DELETE FIREWALL POLICY SPAMOURCES
ADD/DELETE/SET/SHOW FIREWALL POLICY UDPDPTTIMEOUT
DISABLE/ENABLE FIREWALL POLICY HTTPCOOKIES
DISABLE/ENABLE FIREWALL POLICY SMTPRELAY
DISABLE/ENABLE/SET/SHOW FIREWALL SIPALG
RESET/SHOW FIREWALL POLICY MACCACHE
SET FIREWALL POLICY [FTPDATAPOINT] [ICMPUNREACHABLETIMEOUT]
[MACCACHETIMEOUT] [RADIUSLIMIT]
SET FIREWALL POLICY SMTPDOMAIN
SHOW FIREWALL POLICY USER
ADD/DELETE/DISABLE/ENABLE/SET/SHOW FIREWALL MONITOR
ADD/DELETE/SET/SHOW FIREWALL POLICY LIMITRULE
ADD/DELETE FIREWALL POLICY NAT={ENAPT}
DISABLE/ENABLE FIREWALL SESSIONREPORT
RESET FIREWALL SIPALG AUTOCLIENTS
RESET FIREWALL SIPALG COUNTER
SET FIREWALL POLICY ATTACK
ADD/DELETE IGMPSPNOOPING VLAN ROUTERPORT
SET IGMPSPNOOPING VLAN QUERYSOLICIT
ENABLE/SET PORTAUTH[=8021X] [AUTOAUTHENTICATE]
DISABLE/ENABLE SWITCH LOOPDETECTION={BOTH;BCCOUNTER}
DISABLE/ENABLE SWITCH LOOPDETECTION DEBUG
SET SWITCH LOOPDETECTION=BCCOUNTER
SHOW SWITCH LOOPDETECTION=BCCOUNTER
```

## 9 コマンドリファレンスについて

---

最新のコマンドリファレンス（J613-M0019-01 Rev.N）は弊社ホームページに掲載されています。

本リリースノートは、上記のコマンドリファレンスに対応した内容になっていますので、お手持ちのコマンドリファレンスが上記のものでない場合は、弊社 Web ページで最新の情報をご覧ください。

<http://www.allied-telesis.co.jp/>