J613-M0019-04 Rev.L 080115

Allied Telesis

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）とコマンドリファレンス（J613-M0019-01 Rev.J）の補足や、ご使用の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　2.9.1-13

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 **2.9.1-13** 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、**2.9.1-13** にバージョンアップします。
6. バージョン **2.9.1-13** 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　本バージョンで追加された機能

ソフトウェアバージョン **2.9.1-05** から **2.9.1-13** へのバージョンアップにおいて、以下の機能が追加されました。

3.1　PPPoE における PADT 送信機能

参照 **「コマンドリファレンス」/「PPP 」**

PPPoE セッション確立中に電源オフ・オンや異常リブートが発生した場合、網側の装置からは確立していたセッション ID をもったパケットが送信されますが、この際、PADT を送信し、網側装置の持つ PPPoE セッションの削除を促すよう、機能拡張しました。なお、本機能を使用するための設定は不要です。

4　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 **2.9.1-05** から **2.9.1-13** 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。

4.1　セキュリティーモードで動作中に、RSO（Remote Security Officer）として登録されていない IP アドレスから Security Officer レベルでのログインが試行された場合、ログイン自体は正しく拒否するものの、このときに出力するログメッセージの内容が適切でありませんでしたが、これを修正しました。

4.2　プライベート MIB の instRelMajor、instRelMinor、instRelInterim の値を取得できませんでしたが、これを修正しました。

4.3　プライベート MIB の topologyChange トラップと newRoot トラップが送信されませんでしたが、これを修正しました。

4.4　プライベート MIB の configFile の値が、起動時設定ファイルの名前（Boot configuration file）ではなく、起動時に読み込んだ設定ファイル名（Current Configuration）になっていましたが、これを修正しました。

4.5　Rapid モードのスパニングツリープロトコル（RSTP）有効時、Topology change が起きた後、FDB 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。

4.6　Rapid モードのスパニングツリープロトコル（RSTP）有効時、ブリッジ MIB の dot1dStpPortState の値が正しくないことがありましたが、これを修正しました。

4.7　Rapid モードのスパニングツリープロトコル（RSTP）、ポートトランキング、VRRP の併用環境において、VRRP のマスター切り替え時に FDB と ARP キャッシュの同期がとれないことがありましたが、これを修正しました。

4.8　マルチプルスパニングツリープロトコル（MSTP）を有効にすると、ミラーポートからも BPDU を送信していましたが、これを修正しました。

4.9　SET MSTP コマンドの PROTOCOLVERSION パラメーターに RSTP を指定するとループが発生していましたが、これを修正しました。

4.10 マルチプルスパニングツリープロトコル（MSTP）を有効にすると、ランタイムコンフィグから DELETE VLAN コマンドの設定が削除されていましたが、これを修正しました。

4.11 8748SL において、パケットの入力ポートと出力ポートがポートグループ「1 ～ 24、50」と「25 ～ 48、49」をまたいだ場合（例：入力ポート「1」、出力ポート「25」の場合など）に、許可されるべきパケットが破棄されることがありましたが、これを修正しました。

4.12 DHCP Snooping 有効時、バインディングデータベースに登録されていない始点 IP アドレスを持つ IP パケットがフィルタリングされませんでしたが、これを修正しました。

4.13 SET TRACE コマンドにおいて、MINTTL（最小ホップ数）に MAXTTL（最大ホップ数）より大きい値を指定してもエラーになりませんでしたが、これを修正しました。

4.14 TRACE コマンドにおいて、パラメーター指定が正しくないときに表示が文字化けしていましたが、これを修正しました。

4.15 ICMP ルーター通知機能において、IP インターフェースの起動直後に 4 回通知メッセージを送信していましたが、RFC1256 の規定どおり起動直後の送信回数を 3 回に変更しました。

4.16 コマンドラインから「SET OSPF RIP=BOTH」を入力し、「SET OSPF RIP=EXPORT」と「ADD OSPF REDISTRIBUTE PROTOCOL=RIP」の 2 コマンドに自動変換されたあとに設定をファイルに保存し、起動時設定ファイルに指定した上で再起動すると、「ADD OSPF REDISTRIBUTE PROTOCOL=RIP」の設定が有効になりませんでしたが、これを修正しました。

4.17 OSPF が無効のとき、SET OSPF コマンドで BGPLIMIT パラメーターの値を変更しても、ADD/SET OSPF REDISTRIBUTE PROTOCOL=BGP コマンドの LIMIT パラメーターに値の変更が反映されませんでしたが、これを修正しました。

4.18 PURGE OSPF コマンドを実行しても、ADD OSPF REDISTRIBUTE コマンドによる設定内容が消去されませんでしたが、これを修正しました。

4.19 準スタブエリア（NSSA）のエリア境界ルーター（ABR）で RESET OSPF コマンドを実行したとき、タイプ 7 LSA がタイプ 5 LSA に変換されないことがありましたが、これを修正しました。

4.20 OSPF において、同一宛先かつ同一コストの AS 外部経路が複数存在する場合、そのうちの 1 つしか IP 経路表に反映しませんでしたが、これを修正しました。

4.21 BGP-4 において、ピアから経路情報の配信を受けている状態で、自身が配信している経路情報を「DELETE BGP NET=x.x.x.x」や「DELETE BGP IMPORT=xxx」で削除した場合に、WITHDRAW メッセージを送信しないことがありましたが、これを修正しました。

4.22 SET IP FILTER コマンドで LOG パラメーター（ログへの記録）を有効化すると、対象エントリーから宛先 IP アドレスの設定（DESTINATION、DMASK）が削除されていましたが、これを修正しました。

4.23 ICMPv6 Time Exceeded パケットの送信時に ICMPv6 カウンターの InTimeExcds がカウントアップされていましたが、これを修正しました。

4.24 IPv6 脆弱性（JVNVU#267289）への対策を行いました。

4.25 PIM-SM において、(S,G) null Register メッセージのパケットフォーマットが正しくありませんでしたが、これを修正しました。

4.26 PIM-SM と VRRP の併用時、バックアップルーターのマルチキャスト送信者側インターフェースがダウンすると、マルチキャストトラフィックが停止して再開しないことがありましたが、これを修正しました。

4.27 ADD FIREWALL POLICY コマンドでダイナミック ENAT の PUBLIC インターフェースに IP と LIST を指定したルールを設定した場合、エラーメッセージが表示されていましたが、これを修正しました。

4.28 ファイアウォールの攻撃検出機能において、一回のポートスキャンに対して、「Port scan attack is underway」というログメッセージを 2 度出力していましたが、これを修正しました。

4.29 SHOW FIREWALL EVENT コマンドで表示されるイベント情報は、内部テーブルがいっぱいになると古い情報から削除されます。このとき攻撃開始のイベント情報が削除されてしまうと、攻撃の終了を検出しても攻撃終了のイベントを通知しなくなっていましたが、これを修正しました。

4.30 ファイアウォールにおいて、同じ内容のルールを複数設定できていましたが、これを修正しました。

4.31 ファイアウォールとローカル IP インターフェースを併用した場合、本製品自身の送信するパケットが、NAT 処理されずに送出されることがありましたが、これを修正しました。

4.32 VRRP において、バーチャルルーター（VR）の動作している VLAN インターフェース上にトランクグループが存在していると、ポート 1 から不正な VRRP パケットが送信されていましたが、これを修正しました。

4.33 DHCP サーバー機能において、DHCP クライアントが接続されているのとは異なるインターフェースを SET IP LOCAL コマンドでデフォルトローカル IP インターフェースに設定していると、DHCP クライアントから BROADCAST フラグの立った DHCP Discover メッセージを受信しても、DHCP Offer メッセージを返しませんでしたが、これを修正しました。

4.34 DHCP サーバー機能において、ユニキャストの DHCP Request メッセージに応答しませんでしたが、これを修正しました。

以下の項目は、ソフトウェアバージョン **2.9.1-05** のリリースノートに制限事項として記載されていましたが、その後の調査により本製品の動作に問題がないことが確認されましたので、制限事項から削除いたします。

4.35 Join/Prune Interval（SET PIM6 コマンドの JPINTERVAL）の設定を変更しても、Join/Prune Holdtime が変更されません。

以下の 項目は、ソフトウェアバージョン **2.9.1-05** 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 **2.9.1-05** で修正済みでしたので、制限事項より削除いたします。

4.36 プリエンプトモード OFF かつ優先度 231 以上でバックアップルーターとして動作している場合、マスタールーターがダウンしてもマスターに移行しません

5　本バージョンでの制限事項

ソフトウェアバージョン **2.9.1-13** には、以下の制限事項があります。

5.1　RADIUS

参照　「コマンドリファレンス」/「運用・管理」/「認証サーバー」

○　複数の IP インターフェース（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 インターフェー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。

5.2　ZMODEM によるファイル受信

参照　「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中（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。

5.3　ログ

参照　「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。

5.4 スクリプト

参照 「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。

5.5 SNMP

参照 「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。

5.6 NTP

参照 「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。

5.7 SET ASYN 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」

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）。

5.8 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。

5.9 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。

5.10 ポートトランキング

参照「コマンドリファレンス」/「スイッチング」/「ポート」

○ 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（Private VLAN）の同一グループ所属であるかのチェックが行われません。これを回避するため、マルチプル VLAN とポートトランキングを併用するときは、先にトランクグループを作成してから、トランクグループをマルチプル VLAN に割り当ててください。

○ 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。

5.11 ポートセキュリティー

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ー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。

5.12 LACP（IEEE 802.3ad）

参照「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。

5.13 バーチャル LAN

参照「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てしまいます。

5.14 スパニングツリープロトコル（STP/RSTP）

参照「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。

5.15 フォワーディングデータベース

参照「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。

5.16 ハードウェア IP フィルター

参照「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）。

5.17 ポート認証

参照「コマンドリファレンス」/「スイッチング」/「ポート認証」

○ 802.1X Multi-Supplicant 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 Supplicant 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 Supplicant 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。

5.18 IP 統計情報

参照「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。

5.19 ディレクティドブロードキャストパケット

参照「コマンドリファレンス」/「IP」

特定 VLAN に対するディレクティド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）宛てのディレクティド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ドブロードキャストパケットを転送できなくなります。

5.20 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）

参照「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。

5.21 Gratuitous ARP

参照「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。

5.22 ADD IP ROUTE コマンド

参照「コマンドリファレンス」/「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。

5.23 RIP

参照「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しなくなります。

5.24 OSPF

参照「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。

5.25 DNS キャッシュ

参照「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。

5.26 DVMRP

参照「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。

5.27 PIM

参照「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。

5.28 IGMP

参照「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。

5.29 IGMP Snooping

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

○ SET IGMPSNOOPING 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。

5.30 MVR

参照「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。

5.31 ファイアウォール

参照「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（エンハンスト、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。

○ 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。これを回避するには、RTSP のポート番号を変更してください。

○ 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（Time-to-live 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ります。

6 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。

6.1 HTTP サーバー（サポート対象外）

参照「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。セキュリティーを重視する場合は、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。

6.2 弊社 CentreNET SwimRadius 使用時の注意

参照「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 を使用する場合は、以下の点にご注意ください。

○ 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、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。

○ 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）を返すときは 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 SwimRadius で行うことはできません。

6.3 DESTINATION=ROUTER のログ出力先定義

参照「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。

6.4 送信元アドレスがマルチキャストアドレスのフレーム

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。

6.5 スイッチポートの統計カウンター（8748SL のみ）

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。

6.6 1000Mbps ポートのフラッディングレート

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。

6.7 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

参照「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。

6.8 ダイナミックポートセキュリティー

参照「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 から始まらず、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。

6.9 マルチプルスパニングツリープロトコル（MSTP）

参照「コマンドリファレンス」/「スイッチング」/「マルチプルスパ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。

6.10 フォワーディングデータベース

参照「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。

6.11 ハードウェア IP フィルター

参照「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）。

6.12 ポート認証

参照「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、ポートトランキング、スパ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。

6.13 IP マルチキャストのハードウェア処理

参照「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。

6.14 ルーター通知（RA）

参照「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。

6.15 PIM

参照「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=SENDC
```

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

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」/「IP マルチキャスト」/「IGMP Snooping」

参照「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。

7 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, APPLETALK, BRI, CLASSIFIER, CLNS, DHCP6, EPSR, ETH, FRAMERELAY, GARP, GRE, GUI, HTTP, IPSEC, ISAKMP, ISDN, L2TP, LAPB, LAPD, LDAP, LLDP, 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 ¦ 1000MHALF}]
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¦DHCPTEMP¦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 [STATEREFRESH]
ADD/DELETE/SET DVMRP [DLC]
ADD/DELETE/SET DVMRP INTERFACE [DLC]
DISABLE/ENABLE ENCO COMPSTATISTICS
SHOW ENCO CHANNEL
SHOW ENCO COUNTER={DES ¦ HMAC ¦ JOBPROCCESSING ¦ 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 [STATEREFRESH]
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] [STACCHECK] [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 DHCPSNOOPING STRICTUNICAST
ADD/DELETE DHCPSNOOPING BINDING [ROUTER]
ADD/DELETE/ENABLE/SHOW DHCPSNOOPING XLA
DISABLE/ENABLE DHCPSNOOPING IPFILTERING
DISABLE/ENABLE DHCPSNOOPING LOG
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 SPAMSOURCES
ADD/DELETE/SET/SHOW FIREWALL POLICY UDPPORTTIMEOUT
DISABLE/ENABLE FIREWALL POLICY HTTPCOOKIES
DISABLE/ENABLE FIREWALL POLICY SMTPRELAY
DISABLE/ENABLE/SET/SHOW FIREWALL SIPALG
RESET/SHOW FIREWALL POLICY MACCACHE
SET FIREWALL POLICY [FTPDATAPORT] [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
CREATE/SET VRRP ADVERTISEMENT
ADD/DELETE IGMPSNOOPING VLAN ROUTERPORT
SET IGMPSNOOPING VLAN QUERYSOLICIT

8　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.J）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/