



最初にお読みください

CentreCOM® FS900Mシリーズ リリースノート

この度は、CentreCOM FS900M シリーズ（CentreCOM FS909M/FS917M/FS926M/FS909M-PS/FS917M-PS/FS926M-PS。以下、特に記載がないかぎり、「本製品」と表記します）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（FS900Mシリーズ：613-000324 Rev.B FS900M-PSシリーズ：613-000341 Rev.C）とコマンドリファレンス（613-000325 Rev.F）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 ファームウェアバージョン 1.6.1

2 本バージョンで仕様変更された機能

ファームウェアバージョン 1.6.0 から 1.6.1 へのバージョンアップにおいて、以下の機能が仕様変更されました。

2.1 ポート認証とループガードの LDF 検出の併用

ポート認証の Authenticator ポートで、ループガードの LDF 検出が併用できるようになりました。

なお、ファームウェアバージョン 1.6.0 のリリースノートには掲載がありませんが、本機能の併用はバージョン 1.6.0 から可能です。

3 本バージョンで修正された項目

ファームウェアバージョン 1.6.0 から 1.6.1 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。

3.1 オンラインヘルプにおいて、以下の項目を修正しました。

- ・ Help Disable IP のヘルプの表記が正しくない
- ・ 日本語解説の改行位置が正しくない
- ・ トピックの表示がアルファベット順ではない

3.2 Telnet 接続時、RESTART コマンドを実行し、本製品を再起動するかどうかのメッセージ（Do restart system now ? (Y/N):）が表示されたところで、Telnet セッションを切断すると、以後本製品に対して Telnet 接続ができなくなっていました。これを修正しました。


3.3 RADIUS アカウンティング機能において、コンソール、Telnet、Web GUI のいずれかによるログイン認証時に、本製品から送られる Accounting-Interim-Update パケットの NAS-Port 属性に不正な値が付与されるため、本製品がリポートすることがありましたが、これを修正しました。

- 3.4 RADIUS アカウンティング機能有効時、Web GUI でログイン認証を行ったあと、画面の表示更新を繰り返し行うことによって再び表示されたログイン画面において、ログイン認証に失敗することがありましたが、これを修正しました。
- 3.5 RADIUS アカウンティング機能有効時、Web GUI でログイン認証を行ったあと、CLI からログアウトをすると、CLI でログイン認証が行われていないにもかかわらず、Accounting-Request パケットが送信されていましたが、これを修正しました。
- 3.6 ミラーポートに設定したポートの情報を SHOW SWITCH PORT コマンドで表示できませんでしたが、これを修正しました。
- 3.7 コンボポートの 10/100/1000BASE-T ポートに対して、SET SWITCH PORT コマンドの SPEED パラメーターで 1000MFULL を設定し、その後フローコントロールの有効 / 無効設定を変更すると、100Mbps でのリンクが可能になっていましたが、これを修正しました。
- 3.8 ポートランキングと IGMP Snooping の併用時、トランクポートがリンクダウンすると、マルチキャストデータが VLAN 内にフラッディングされていましたが、これを修正しました。
- 3.9 (FS926M/FS926M-PS のみ) IGMP Snooping 有効時、ポート 25, 26 が SHOW IGMP SNOOPING コマンドの Router Port、Host Ports に正しく表示されない、ポート 25, 26 で IGMP メッセージ受信時にマルチキャストデータがフラッディングされるなど、IGMP Snooping が正しく動作しませんでしたでしたが、これを修正しました。
- 3.10 ポートランキングとスパニングツリープロトコル (STP) を同一ポートに設定している場合、STP をいったん無効にし、再度有効にすると、該当ポートから BPDU が送出されませんでしたでしたが、これを修正しました。
- 3.11 スパニングツリープロトコル (STP) において、DISABLE SWITCH PORT コマンドで無効に設定された STP ポートで、物理的なリンクダウン・リンクアップが発生すると、STP ポートの状態が Disabled から Discarding/Learning/Forwarding に遷移していましたが、これを修正しました。
- 3.12 Web GUI のポートステータス表示画面において、コンボポートの極性自動切替 (AutoMDI) に「Enable」、極性 (Polarity) に「MDI」が表示されていましたが、コンボポートでは MDI/MDI-X の設定変更はできないため、「Not applicable」が表示されるよう修正しました。
- 3.13 Web GUI の IGMP Snooping 画面で、IGMP Snooping によるマルチキャストグループが 64 エントリーまでしか表示されませんでしたでしたが、これを修正しました。

4 本バージョンでの制限事項

ファームウェアバージョン 1.6.1 には、以下の制限事項があります。

4.1 サーバー機能の TCP ポート番号

 「コマンドリファレンス」 / 「運用・管理」

本製品サーバー機能の TCP ポート番号を変更するときに、2 種類のサーバー間で TCP ポート番号のデフォルト値を入れ替えるような設定（例：Telnet サーバーのポート番号 = 21、FTP サーバーのポート番号 = 23）をして、設定ファイル保存後本製品を再起動すると、設定ファイルを上から順に読み込む際に変更後のポート番号とデフォルトのポート番号が重複する状態が発生し、エラーで設定が有効になりません。


このような設定をする場合は、設定ファイルに直接コマンドを記述するようにしてください。

4.2 フラッシュメモリーの空き容量

 「コマンドリファレンス」 / 「運用・管理」 / 「ファイルシステム」

フラッシュメモリーに 128KByte 以上の設定ファイルが存在する状態で、起動時設定ファイルの指定を切り替え続けていると、本製品がハングアップする場合があります。

4.3 SNMP

 「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」

- SNMP マネージャーのタイムアウトによって、同時に 5 個以上の SNMP マネージャーから ifEntry を Get できない場合があります。SNMP マネージャーのタイムアウト値を長く設定するようにしてください。
- ファームウェアバージョン 1.4.1 で、ループガード（受信レート検出 / LDF 検出）がサポートされ、CREATE SNMP COMMUNITY コマンドおよび ENABLE SNMP TRAP コマンドの TRAP パラメーターに STORMDETECTION と LOOPDETECTION の指定ができるようになりました。これにより、バージョン 1.4.0 以前で TRAP パラメーターに ALL を指定している場合、1.4.1 以降へのバージョンアップ時に設定が以下のように反映されますので、ご注意ください。

バージョン 1.3.0 以前で ALL を指定して作成された設定ファイル：

CREATE SNMP COMMUNITY コマンド

→ STORMDETECTION と LOOPDETECTION が含まれます。

ENABLE SNMP TRAP コマンド

→ STORMDETECTION と LOOPDETECTION は含まれません。

バージョン 1.4.0 で ALL を指定して作成された設定ファイル：

CREATE SNMP COMMUNITY コマンド

→ STORMDETECTION と LOOPDETECTION は含まれません。

ENABLE SNMP TRAP コマンド

→ STORMDETECTION と LOOPDETECTION は含まれません。


- SNMP マネージャーから、トランクポートをディセーブルに変更する設定をしても、エラーで設定が有効になりません。トランクポートをディセーブルに設定する場合は、CLI または Web GUI を使用してください。

4.4 ターミナルサービス：Telnet サーバー機能

 「コマンドリファレンス」 / 「運用・管理」 / 「ターミナルサービス」


SNMP マネージャーにおいて、探索条件として Telnet サーバー機能が動作しているかどうかを確認する（動作している機器に対しては Telnet 接続をする）という指定をして、機器の自動探索を行うと、本製品から Telnet 接続ができなくなる場合があります。SNMP マネージャーで機器の自動探索を行う場合は、Telnet サーバー機能が動作しているかどうかを確認する条件をはずすようにしてください。

4.5 RADIUS サーバー

 「コマンドリファレンス」 / 「運用・管理」 / 「認証サーバー」

802.1X 認証有効時、SET RADIUS コマンドの DEAD-ACTION パラメーターで PERMIT を設定しても、RADIUS サーバーからの応答がないときに、通信ができなくなる場合があります。


4.6 フォワーディングデータベース

 「コマンドリファレンス」 / 「フォワーディングデータベース」

MAC アドレス（ダイナミックエントリー）のソフトウェア FDB への登録処理に時間がかかります。登録にかかる時間の目安は以下のとおりです。


- 128 件：数秒
- 4000 件：30 秒以内
- 8000 件：1 分程度

4.7 ポートセキュリティ

 「コマンドリファレンス」 / 「スイッチング」


スパニングツリーとポートセキュリティの Limited モードを異なるポートで同時に使用する場合、ポートセキュリティ有効ポートで MAC アドレスを学習している最中に、SET SWITCH PORT コマンドの LEARN パラメーターで値を変更する設定をしないでください。スパニングツリーでトポロジーチェンジが発生する可能性があります。

4.8 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」

デフォルト VLAN 以外の VLAN に所属するポートに対して、SET SWITCH PORT コマンドで ACCEPTABLE パラメーターに VLAN を指定し、設定を保存後本製品を再起動すると、起動時に「Port X does not belong to the VLAN specified」というエラーが表示されます。エラーは表示されますが、設定は正しく反映されます。


4.9 EPSR アウェア

 「コマンドリファレンス」 / 「スイッチング」 / 「EPSR アウェア」

- SNMP トラップの送信が有効で、かつ、EPSR アウェアの動作モードが TRANSIT のとき、Telnet 接続によって EPSR ドメインの有効 / 無効設定を変更すると、本製品がリブートする場合があります。
EPSR ドメインの有効 / 無効設定を変更する場合は、あらかじめ SNMP を無効に設定し、SNMP トラップの送信が無効の状態で行うようにしてください。

- EPSR アウェアの動作モードが TRANSIT のとき、EPSR リングを経由して、Telnet 接続によってマネージメント VLAN をデータ VLAN として設定すると、それ以降 Telnet 接続ができなくなる場合があります。
これを回避するには、以下のいずれかの処置を行ってください。
 - ・ EPSR リングを経由せずに Telnet 接続をするようにしてください。
 - ・ Telnet ではなく、コンソールポートで本製品に接続してください。

4.10 マルチプル VLAN (Protected Port VLAN)

 「コマンドリファレンス」 / 「バーチャル LAN」


Protected Port VLAN でアップリンクポートに設定されたポートを、いったん DELETE VLAN PORT コマンドで削除し、再度 ADD VLAN PORT コマンドで同一 VLAN にクライアントポートとして追加すると、該当ポートがクライアントポートとして動作しません（設定上はクライアントポートになりますが、動作はアップリンクポートのままです）。
このような設定をした場合は、設定を保存後本製品を再起動するようにしてください。

4.11 IGMP Snooping

 「コマンドリファレンス」 / 「IGMP Snooping」


- タグ VLAN にしか所属していないタグ付きポートで、タグなしの IGMP Query メッセージを受信した場合、タグ付きの状態でフラッディングされます。
- IGMP Snooping 有効時、メンバーが存在するポートをミラーポートに設定しても、IGMP Snooping 用のテーブルから該当ポートの情報が削除されません。
- IGMP Snooping 有効時、IGMP パケットの通信中にグループの所属 VLAN を変更すると、IGMP Snooping 用のテーブルから変更前の VLAN 情報が削除されません。
- IGMP Snooping と、EPSR アウェアまたはスパンニングツリープロトコル併用時、経路の切り替えが発生したときにマルチキャストグループの登録がクリアされないため、切り替え前に登録されたルーターポートが残ったままになります。
なお、EPSR アウェアについては、ファームウェアバージョン 1.6.0 で CREATE EPSR コマンドに DELETEMCAST オプションが追加され、リングトポロジーチェンジ発生時にマルチキャストグループのエントリを FDB から削除する設定が可能になりました。
- 始点 IP アドレスが 0.0.0.0 で、同一 MAC アドレスの IGMP Report メッセージを複数回続けて受信すると、受信の際にグループのタイマーが更新されません。SHOW IGMP SNOOPING コマンドで表示される Address (IGMP グループに所属しているノードの MAC アドレス) に、受信したメッセージの数分だけ同一 MAC アドレスのエントリが追加されます。
また、始点 IP アドレスが 0.0.0.0 の IGMP Leave メッセージを受信しても、ルーターポートに転送されず、離脱処理が行われません。
- IGMP Snooping のルーターポートとトランクポートが同一ポートで併用されていると、グループ登録後、IGMP Leave メッセージを受信してもルーターポートに転送されません。


4.12 MLD Snooping

 **「コマンドリファレンス」 / 「MLD Snooping」**

- (FS926M/FS926M-PS のみ) MLD Snooping 有効時、ポート 25 がルーターポートに設定されている場合、ポート 26 で MLD Report を受信しても、グループが登録されません (ポート 26 以外のポートで受信した場合は正常に登録されます)。
- (FS926M/FS926M-PS のみ) MLD Snooping 有効時、コンボポートがルーターポートに設定されていると、登録されたグループ宛での MLD Report を受信してもルーターポートに転送されません。
- MLD メッセージの受信により自動登録されたグループと同じグループアドレスを指定して、ADD MLDSNOOPING VLAN コマンドを使って手動でグループエントリーを追加すると、自動登録されたグループエントリーはいったん削除される仕様ですが、SHOW MLDSNOOPING コマンドで MLD Snooping の情報を表示すると、自動登録されたグループエントリーが残ったままになっています。
これは表示だけの問題であり、動作には影響ありません。


4.13 IGMP Snooping/MLD Snooping

 **「コマンドリファレンス」 / 「IGMP Snooping」**

 **「コマンドリファレンス」 / 「MLD Snooping」**


ポートランキングと IGMP Snooping または MLD Snooping の併用時、トランクグループ内で最も番号の小さいポートを DISABLE SWITCH PORT コマンドで無効に設定すると、トランクグループ内のそれ以外のポートでマルチキャストデータが転送されなくなります。ただし、DISABLE SWITCH PORT コマンド実行時に LINK=DISABLE を指定して、該当ポートを物理的にリンクダウンさせると、本現象は発生しません。

4.14 ポート認証

 **「コマンドリファレンス」 / 「ポート認証」**

DHCP サーバー使用環境に DHCP パケット転送機能を使用して Web 認証を導入した場合 (認証前の Supplicant はゲスト VLAN の所属で、認証成功後に DHCP サーバーが存在するマネージメント VLAN の所属になるような構成)、DHCP サーバーからの未学習のユニキャストパケットが Web 認証ポートに転送されず、Windows XP が動作する Supplicant において IP アドレスの取得に時間がかかることがあります。

4.15 スパニングツリー

 **「コマンドリファレンス」 / 「スパニングツリープロトコル」**

本製品の実装では、トポロジーチェンジ発生時にエッジポートに設定されたポートの FDB が消去されます。

4.16 Web GUI

「コマンドリファレンス」 / 「Web GUI」

- Web GUI でマルチプル VLAN(Protected Port 版) のポート設定を行う際、グループ番号の設定変更とタグなし / タグ付きの設定変更を同時に行うことができますが、個別に変更するようにしてください。
グループ番号の変更とタグなし→タグ付きの変更を同時に行った場合、該当ポートがタグなしとしてデフォルト VLAN にも追加されます。
- マルチプル VLAN (Protected Port VLAN) において、同一 VLAN に複数のアップリンクポートが設定されているとき、アップリンクポートのうちの 1 ポートを削除する設定を行うと、該当ポート番号以降のすべてのポートが削除されます。
このような設定は CLI で行うようにしてください。
- コンボポートに対して Speed=1000MFULL と Combo=Fiber-Auto の設定は同時にできない仕様ですが、Web GUI の「スイッチ設定 - ポート」画面で「全ポート設定」ボタンによって、全ポートを対象に SPEED=Auto、1000MFull 以外の通信モード、Combo=Fiber-Auto の設定をすると、コンボポートに Speed=1000MFULL と Combo=Fiber-Auto の不正な組み合わせで設定がされます。
- 存在しない RADIUS サーバーを登録し、GUI からのログイン時にデフォルト以外のユーザー名とパスワードを入力すると、RADIUS 認証のタイムアウトが発生するまでの時間が設定時間よりも長くなる場合があります。
本現象は、CLI では発生しません。
- 「ポート認証 - ポート設定」画面において、Authenticator または Supplicant ポートの設定を行うときに、指定ポートに併用不可機能が設定されているポートが含まれていても (下記のリスト参照)、エラーにならずに設定ができてしまいます。

以下のポートを含んで、Authenticator ポートに設定しようとした場合：

- ・ ミラーポート
- ・ トランクポート
- ・ STP ポート
- ・ MSTP ポート
- ・ EPSR リングポート
- ・ スタティックエントリ登録ポート
- ・ ポートセキュリティー有効ポート
- ・ コンボポート

以下のポートを含んで、Supplicant ポートに設定しようとした場合：

- ・ ミラーポート
- ・ トランクポート
- ・ STP ポート
- ・ MSTP ポート
- ・ EPSR リングポート


- EPSR アウェアの Transit モード有効時、Web GUI の「機器監視 - EPSR」画面のリンク (リングを構成するポートの状態) に、Forwarding と Blocking が表示されず、Up と表示されます。
Transit モード時のポートの状態は、CLI の SHOW EPSR コマンドで確認するようにしてください。

- 通信負荷が高い状態で、Web GUI からファームウェアをダウンロードすると、ファームウェアのアップデート完了後、アップデートの進捗画面が自動的に閉じられないことがあります。

5 取扱説明書・コマンドリファレンスの補足

取扱説明書、および「CentreCOM FS900M シリーズ コマンドリファレンス 1.6.0 (613-000325 Rev.F)」の補足事項です。

5.1 ポート認証 / ループガード

 「コマンドリファレンス」 / 「スイッチング」

 「コマンドリファレンス」 / 「ポート認証」

コマンドリファレンスに以下の記述がありますが、ファームウェアバージョン 1.6.0 以降、ポート認証の Authenticator ポートでループガードのLDF 検出が併用できるようになりましたので、訂正してお詫びいたします。

- スイッチング / ループガード
 - ・ Note - ポートセキュリティの Limited モードに設定されたポート、ポート認証の Authenticator ポートでは LDF 検出は併用できません。
正しくは、「ポートセキュリティの Limited モードに設定されたポートでは LDF 検出は併用できません」になります。
- ポート認証
 - ・ Note - Authenticator ポートでは LDF 検出は併用できません。

5.2 ポート認証 / EPSR


コマンドリファレンスに記載がありませんが、ポート認証の Authenticator ポートと Supplicant ポートを、EPSR のリングを構成するポートにすることはできません。

5.3 ポートランキング / スパニングツリープロトコル / ループガードの併用

コマンドリファレンスに「ポートランキング、スパニングツリープロトコル、ループガード、これらすべての機能を同時に使用することはできません。」という記述がありますが、3つの機能を同時に使用しない場合は併用をサポートしています（下記組み合わせでの併用は可能です）。


- ・ ポートランキングとスパニングツリープロトコル
- ・ ポートランキングとループガード
- ・ スパニングツリープロトコルとループガード

5.4 SNTP

 「コマンドリファレンス」 / 「運用・管理」 / 「SNTP」

登録された SNTP サーバーがネットワーク上に存在しない状態で RESET NTP コマンドを連続して実行すると、ARP Request が正常に送信されない可能性があります。このような状態で RESET NTP コマンドを連続して実行する場合は、1分以上の間隔をあけるようにしてください。

5.5 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」 / 「フォワーディングデータベース」


- 宛先 MAC アドレスが 01-80-C2-00-00-00 から 01-80-C2-00-00-FF の場合、送信元 MAC アドレスが FDB に登録されません。
- FDB のエントリー数が最大値に達している状態では、MLD Snooping によるマルチキャストグループの登録、ADD SWITCH FILTER コマンドによる IPv6 マルチキャストアドレスの登録ができません。

5.6 IP

 **参照** 「コマンドリファレンス」 / 「IP」


ICMP エコー要求 (Ping) パケットを受信したとき、応答に 30 ミリ秒程度かかる場合がありますが、これは正常動作です。

5.7 BPDU 透過

 **参照** 「コマンドリファレンス」 / 「スイッチング」


BPDU 透過機能有効時、タグ付きポートにタグなしの BPDU を送信した場合、タグ付きの状態フラグがフラグgingされます。

5.8 ポートランキング

 **参照** 「コマンドリファレンス」 / 「スイッチング」

- 通信中にトランクポートを抜き差しすると、該当ポートで MAC アドレスが再登録されますが、SHOW SWITCH FDB コマンドで再登録された MAC アドレスが表示されるまでに時間がかかります。
これは表示だけの問題であり、動作には影響ありません。
- ENABLE SWITCH PORT FLOW/DISABLE SWITCH PORT FLOW コマンドで、トランクグループ内の 1 ポートだけを指定してフローコントロールの有効 / 無効設定をしても、グループ内の残りのポートには設定が反映されません。
トランクポートにフローコントロールを設定する場合は、グループ内の全ポートを指定するようにしてください。


5.9 ポートミラーリング

 **参照** 「コマンドリファレンス」 / 「スイッチング」

本製品から送信される以下のパケットについては、ミラーリングされません。


- ・ IGMP (IGMP Snooping 有効時)
- ・ MLD (MLD Snooping 有効時)
- ・ EAP (ポート認証有効時)
- ・ BPDU (スパニングツリープロトコル有効時)
- ・ DHCP (Web 認証 : DHCP パケット転送機能有効時)
- ・ EPSR (EPSR アウェア有効時。Healthcheck メッセージを除く)
- ・ LDF (LDF 検出有効時)

5.10 ポートセキュリティ

 **「コマンドリファレンス」 / 「スイッチング」**


- ポートセキュリティの Dynamic Limited モード使用時、SHOW SWITCH PORT コマンドに SECURITY パラメータを指定して実行したときに表示される「Learned」の MAC アドレス数が、実際に学習されている数より少なく表示される場合があります。
- ポートセキュリティの Limited モードは、ポートセキュリティ有効ポートの所属 VLAN でポートが 2 ポート以上リンクアップしている状態で使用してください。2 ポート以上リンクアップしていないと、未学習のユニキャスト / マルチキャストパケットによる MAC アドレスの学習ができません。

5.11 パケットストームプロテクション

 **「コマンドリファレンス」 / 「スイッチング」**


- FDB にスタティック登録されていないマルチキャストパケットは、SET SWITCH PORT コマンドの DLFLIMIT パラメータの対象として制御されます。
- 予約済みマルチキャストパケット (01-80-c2-00-00-00 ~ 01-80-c2-00-00-2f) は、SET SWITCH PORT コマンドの MCLIMIT パラメータの対象として制御されません。
- パケットストームプロテクションの有効 / 無効を複数ポートで異なる設定にする場合は、SET SWITCH PORT コマンドの BCLIMIT、DLFLIMIT、MCLIMIT パラメータを、省略せずに 3 つすべて設定するようにしてください。
パラメータを省略すると、最後に設定したポートの ON/OFF 設定と同じ設定になります。

5.12 ループガード

 **「コマンドリファレンス」 / 「スイッチング」**

ポート認証の Multi-SupPLICANT モードと LDF 検出によるループガードを、同一ポートで併用するときは、仕様上ループ発生時の LDF 検出に時間がかかる場合があるため、LDF 送出間隔を最小値 (= 1 秒) に近い値に設定することを推奨します。
また、受信レート検出も併用すると、より効果的です。

5.13 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」**


- リンクアップしているポートに対して、SET SWITCH PORT コマンドの SPEED パラメータに現在の通信モードと同じモードを指定してコマンドを実行すると、該当ポートがリンクダウンします。
- オートネゴシエーションでリンクしている 1000M 光ポート (SFP ポート) に対して、通信モードを 1000M Full Duplex 固定に変更する設定を行っても、リンクダウンは発生しません。
- イングレスフィルタリング無効時は、受信パケットの VID が受信ポートの所属 VLAN と一致していない場合でも該当パケットは破棄されませんが、ポート認証やポートセキュリティによってスタティックエントリーとして FDB に登録されている MAC アドレスを送信元 MAC アドレスに持つパケットについては、VID が一致していないと転送されずに破棄されます。

5.14 EPSR アウェア

 「コマンドリファレンス」 / 「スイッチング」 / 「EPSR アウェア」


EPSR アウェア有効時、本製品から送出されるリンクアップ / リンクダウン、EPSR のトラップと syslog サーバ宛でのログメッセージが、タイミングによっては EPSR のマスターノードで破棄される場合があります。

5.15 IGMP Snooping

 「コマンドリファレンス」 / 「IGMP Snooping」

- Leave メッセージを受信したあとも Group Address、VLAN 名は SET IGMP Snooping TIMEOUT コマンドで設定した時間まで削除されません。TIMEOUT=0 設定時は Leave メッセージ受信後、約 60 秒で削除されます。
- 存在しないマルチキャストグループ宛での Group-specific Membership Query を受信すると、破棄されずにフラッディングされます。

5.16 MLD Snooping

 「コマンドリファレンス」 / 「MLD Snooping」


- IPv6 マルチキャストアドレスと一致した MAC アドレスのパケットを受信すると、マルチキャストグループとして登録してしまふことがあります。
- MLDv2 Report、MLDv1 Done メッセージは、常に受信 VLAN 内にフラッディングされます。

5.17 ポート認証

 「コマンドリファレンス」 / 「ポート認証」

- SET PORTAUTH PORT コマンドで MODE パラメータに MULTI (Multi-Suppliant モード) を指定したポートに対して、さらに SET PORTAUTH PORT コマンドの PIGGYBACK パラメータに ENABLED を指定して実行することが可能です。設定が反映されることはなく、動作に影響はありません (Multi-Suppliant モードのポートでは、PIGGYBACK は有効になりません)。
- MAC ベース認証 / Web 認証は、認証ポートの所属 VLAN でポートが 2 ポート以上リンクアップしている状態で使用してください。2 ポート以上リンクアップしていないと、未学習のユニキャスト / マルチキャストパケットによる MAC アドレスの学習ができません。

5.18 スパニングツリープロトコル

 「コマンドリファレンス」 / 「スパニングツリープロトコル」

スパニングツリープロトコル (STP、RSTP、MSTP) とポートトランキング併用時、トランクポートから送信される BPDU のポート ID フィールドには、最大ポート番号 + トランクグループ ID + 1 が使用されます。トランクグループ ID は作成した順に 0 (ゼロ) から割り当てられます。

5.19 Web GUI

「コマンドリファレンス」 / 「Web GUI」

コンボポートではポートセキュリティーを有効にできないため、CLI の SHOW SWITCH PORT コマンドで表示される Security Mode には「Not applicable」と表示されますが、Web GUI のポートステータス表示画面では、セキュリティーモード (SecurityMode) に「Automatic」と表示されます。

6 未サポートコマンド (機能)

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

```
SET HTTP SERVER PORT
SET SYSTEM LANG
ENABLE/DISABLE WATCHDOG MEMORY
SHOW WATCHDOG
```

7 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「CentreCOM FS900M シリーズ コマンドリファレンス 1.6.0 (613-000325 Rev.F)」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。

※パーツナンバー「613-000325 Rev.F」は、コマンドリファレンスの全ページ(左下)に入っています。

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