613-000530 Rev.F 081215

Allied Telesis

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　ファームウェアバージョン　1.6.0

2　本バージョンで追加された機能

ファームウェアバージョン 1.5.0 から 1.6.0 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。各機能の詳細については、「CentreCOM FS900M シリーズ コマンドリファレンス 1.6.0（613-000325 Rev.F）」をご覧ください。

2.1　EPSR アウェアの機能拡張

参照「コマンドリファレンス」/「スイッチング」/「EPSRアウェア」

○　EPSR のアウェア機能に「プリフォワーディング状態での障害回復ポートのブロッキング」および「トラップ送信機能」を加えた動作モードが追加されました。CREATE EPSR コマンドの MODE パラメーターで TRANSIT を指定します。

○　リングトポロジーチェンジが発生したときに、FDB から IGMP Snooping/MLD Snooping によるマルチキャストグループのエントリーを削除する設定ができるようになりました。CREATE EPSR コマンドで DELETEMCAST オプションを指定します。ただし、MLD Snooping の IPv6 マルチキャストアドレスが FDB にスタティック登録されている場合は、このオプションを指定しても該当のエントリーは削除されません。

2.2　ポートセキュリティーの Limited モード

参照「コマンドリファレンス」/「スイッチング」

ポートごとに学習可能な MAC アドレス数の上限を設定し、学習済みの MAC アドレスが上限値に達すると、それ以降に受信した未知のアドレスを持つパケットは不正なものとみなして破棄する Limited モードに対応しました。Limited モードでは、学習した MAC アドレスはスタティック MAC アドレスとして扱われ、エージングによって削除されません。
SET SWITCH PORT コマンドの SECURITYMODE パラメーターで LIMITED を指定し、LEARN パラメーターで MAC アドレス数の上限値を設定します。

2.3 MLD Snooping

参照「コマンドリファレンス」/「MLD Snooping」

VLAN 環境において不要な IPv6 マルチキャストトラフィックをフィルタリングする MLD Snooping に対応しました。MLD v1、MLD v2 への対応が可能です。
詳細は、コマンドリファレンス「MLD Snooping」をご覧ください。

2.4 IGMP Snooping のマルチキャストトラフィック制御

参照「コマンドリファレンス」/「IGMP Snooping」

IGMP Snooping 有効時、VLAN 内にグループメンバーが存在しないとマルチキャストパケットはフラッディングされますが、これを避けるために、VLAN 単位で宛先となるマルチキャストグループアドレスを登録できるようになりました。本設定により、VLAN 内にグループメンバーが存在しない場合、登録されたグループ宛てのマルチキャストパケットはルーターポートにのみ転送されます。設定は、ADD IGMPSNOOPING コマンドで行います。

2.5 Web 認証：DHCP パケット転送機能

参照「コマンドリファレンス」/「ポート認証」

Web 認証有効時、未認証 Supplicant と本製品の IP アドレスが割り当てられた VLAN（マネージメント VLAN）との間で DHCP/BOOTP パケットが転送できるようになりました。機能の有効化・無効化は SET PORTAUTH DHCPPASSTHROUGH コマンドで行います。デフォルトは無効です。
これにより、DHCP サーバー使用環境への Web 認証の導入が容易になりました。詳細は、コマンドリファレンス「ポート認証」をご覧ください。

2.6 検疫ソリューション対応

マイクロソフト社「Windows Server 2008」標準の NAP（ネットワークアクセス保護）、シマンテック社の NAC（Network Access Control）に対応しました。

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 1.5.0 から 1.6.0 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 本製品の MIB を正しくコンパイルできない場合がありましたが、これを修正しました。

3.2 SET CONSOLE コマンドの PAGE パラメーターに OFF（または 0）を指定していると、Ctrl/C（Ctrl キーを押しながら C キーを押す動作）で画面出力を中止できませんでしたが、これを修正しました。

3.3 Telnet ログイン時、画面にイベントメッセージが表示されている最中に、Telnet 切断や新たな Telnet 接続が行われると、本製品がリブートする場合がありましたが、これを修正しました。

3.4 本製品に IP アドレスが設定されているとき、特定の MAC アドレスにかぎり、エラーで FDB へのスタティック登録ができませんでしたが、これを修正しました。

3.5 FDB のエントリー数が最大値に達している状態で、SHOW SWITCH FDB コマンドに SW（ソフトウェア FDB）を指定して実行すると、全エントリーが表示されませんでしたが、これを修正しました。

3.6 SET SWITCH PORT コマンドの PORT パラメーターに ALL、SPEED パラメーターに AUTONEGOTIATE 以外を指定して実行すると、コンボポートに対して 1000MFULL が設定されていましたが、これを修正しました。

3.7 ループガード（LDF 検出 / 受信レート検出）において、BLOCKTIMEOUT パラメーター（自動的に実行前の状態に戻るまでの時間）に NONE が指定されていると、アクションでディセーブルになったポートに対してケーブルの抜き差しをしても、実行前の状態に戻りませんでしたが、これを修正しました。

3.8 スパニングツリーとループガードの受信レート検出を同一ポートで併用した場合、ポートがスパニングツリーの Discarding の状態であるにもかかわらず、ループガードのアクションによってポートのディセーブルが実行されることがありましたが、これを修正しました。

3.9 ポートトランキングと EPSR アウェアを同一ポートで併用したときに、該当ポートがいったんリンクダウンし、再度リンクアップすると、Healthcheck メッセージが受信できなくなり、ループが発生していましたが、これを修正しました。

3.10 EAP 透過機能有効時、タグなしポートからタグ付きパケットが送出されることがありましたが、これを修正しました。

3.11 ループガードの LDF 検出において、SET SWITCH LOOPDETECTION コマンドの SECURE パラメーターに ON を指定した場合、LDF の送信から受信までに 1 秒以上かかると、受信すべき LDF を破棄していましたが、これを修正しました。

3.12 ポート認証において、SET PORTAUTH PORT コマンドで PORTAUTH=AUTO、MODE=MULTI の指定をして、本製品を Authenticator にした場合、802.1X 認証後に認証済み Supplicant から本製品宛てへの通信ができなくなっていましたが、これを修正しました。

3.13 Web 認証において、認証成功後に Supplicant の端末を、ケーブルの抜き差しによって、認証ポートではない別のポートに移動すると、端末から本製品宛てへの通信ができなくなっていましたが、これを修正しました。

3.14 スパニングツリー有効ポートに対して、DISABLE SWITCH PORT コマンドを実行し、その後 DISABLE STP コマンドと ENABLE SWITCH PORT コマンドを実行しても、該当ポートが通信可能になりませんでしたが、これを修正しました。

3.15 スパニングツリー有効時、FDB に 3000 件以上 MAC アドレスが登録された状態で、SHOW SWITCH FDB コマンドに HW（ハードウェア FDB）を指定して実行すると、トポロジーチェンジが発生していましたが、これを修正しました。

3.16 スパニングツリー有効時、FDB に 8192 件 MAC アドレスが登録された状態で、ポートセキュリティー（Secure モード）の設定を行うと、トポロジーチェンジが発生していましたが、これを修正しました。

3.17 Web GUI において、ポート認証のポート設定画面で、モードに Multi を指定していても、Piggy back モードで Enabled の選択が可能でしたが、選択不可の状態（グレーアウト）になるよう修正しました。

3.18 Web GUI において、ポート認証のポート設定画面でモードを Single、かつ、ダイナミック VLAN を Disabled に設定し、いったん別画面を表示後、再度ポート設定画面に戻ると、ゲスト VLAN の VLAN 名が入力不可の状態（グレーアウト）になっていましたが、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 1.6.0 には、以下の制限事項があります。

4.1 フラッシュメモリーの空き容量

参照 「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。

4.2 SNMP

参照 「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。

4.3 RADIUS サーバー

参照「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。

4.4 Telnet

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 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 接続ができなくなります。
Telnet ログイン中に本製品を再起動する必要がある場合は、Web GUI から実行してください。

4.5 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」

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

4.6 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」

スパニングツリーとポートセキュリティーの 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ー有効ポートで 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。

4.7 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」

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。ミラーポートのポート情報は、Web GUI の「スイッチ設定」-「ポート」-「ポートステータス表示」画面で確認してください。

4.8 IGMP Snooping

参照「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ーを FDB から削除する設定が可能になりました。

4.9 スパニングツリー

参照「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。

4.10 Web GUI

参照「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。

○ 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。

○ IGMP Snooping によるマルチキャストグループの登録は 192 エントリーまで可能ですが、Web GUI の「スイッチ設定」-「IGMP Snooping」画面では、64 エントリーまでしか表示されません。
65 エントリー以上表示させる場合は、CLI 上で SHOW IGMPSNOOPING を実行してください。

○ 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 SNTP

参照「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。

5.2 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。

5.3 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。

5.4 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、タグ付きの状態でフラッディングされます。

5.5 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」

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。

5.6 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」

○ ポートセキュリティーの Dynamic Limited モード使用時、SHOW SWITCH PORT コマンドに SECURITY パラメーター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ーの Limited モードは、ポートセキュリティー有効ポートの所属 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。

5.7 パケットストームプロテクション

参照「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 パラメーター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 パラメーターの対象として制御されません。

5.8 スイッチング

参照「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 パラメーター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ー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。

5.9 IGMP Snooping

参照「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 IGMPSNOOPING 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ての 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。

5.10 MLD Snooping

参照「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うことがあります。

○ 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。

5.11 ポート認証

参照「コマンドリファレンス」/「ポート認証」

○ SET PORTAUTH PORT コマンドで MODE パラメーターに MULTI（Multi-Supplicant 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 パラメーターに 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-Supplicant 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。

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

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/