613-000530 Rev.J 100906

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　1.6.9

2　重要：製品リビジョンに関する注意

製品リビジョン Rev.K1 以降の製品にファームウェアをダウンロードする場合は、本バージョン（1.6.9）以降をご使用ください。
ファームウェアバージョン 1.6.1 以前のファームウェアでは、Rev.K1 以降の製品への対応が行われていないため、Rev.K1 以降の製品での使用は未サポートとなります。
製品リビジョンは、本製品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。

3　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 1.6.1 から 1.6.9 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　QoS 機能の優先度設定

参照「コマンドリファレンス」/「QoS」

ENABLE QOS/DISABLE QOS コマンドが追加され、QoS による優先制御を優先させるか（ENABLE QOS）、パケット転送のパフォーマンスを優先させるか（DISABLE QOS）を選択できるようになりました。DISABLE QOS コマンドの実行により、本製品は QoS による優先制御よりもパケット転送のパフォーマンスを優先させるように最適化されます。

ファームウェアバージョン 1.6.1 以前のファームウェアでは常に有効（QoS による優先制御優先）でしたが、バージョン 1.6.9 以降のファームウェアではデフォルトで無効（パケット転送のパフォーマンス優先）になります。

バージョン 1.6.1 以前からバージョン 1.6.9 以降にバージョンアップした場合は、起動時設定ファイルの指定の有無によって、バージョンアップ後の動作が以下のように異なります。

- 起動時設定ファイルの指定なし（SET CONFIG=NONE）
  →無効（パフォーマンス優先）の状態で起動
- 起動時設定ファイルの指定あり（SET CONFIG=filename）
  →有効（QoS 優先）の状態で起動

コマンドの解説および注意事項については、「7.7 QoS：ENABLE/DISABLE/SHOW QOS コマンド」を参照してください。

3.2 ポート認証の機能拡張

参照 「コマンドリファレンス」/「ポート認証」

○ 認証可能な Supplicant の数をポートあたり 10 から 50 に拡張しました。システム全体の数は 240 で変更ありません。

○ IEEE 802.1X-2004 準拠モードに対応し、802.1X 認証で使用する EAPOL のバージョンを選択できるようになりました。
SET PORTAUTH PORT コマンドの EAPOLVERSION パラメーターで 1 を指定すると 802.1X-2001 準拠モード、2を指定すると 802.1X-2004 準拠モードになります。デフォルトは 1 です。

コマンドの解説については、「7.20 ポート認証：SET PORTAUTH PORT コマンド EAPOLVERSION パラメーター」を参照してください。

4 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 1.6.1 から 1.6.9 へのバージョンアップにおいて、以下の仕様変更が行われました。

4.1 フォワーディングデータベースのエージングタイム

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」

SET SWITCH AGEINGTIMER コマンドに設定可能な最大値が 16383（秒）から 1000000（秒）に変更されました。

コマンドの解説については、「7.6 フォワーディングデータベース：SET SWITCH AGEINGTIMER コマンド」を参照してください。

5 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 1.6.1 から 1.6.9 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 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でしたが、これを修正しました。

5.2 オンラインヘルプの SET CONFIG コマンドの書式が正しくありませんでしたが、これを修正しました。

5.3 日付と時刻の設定時にリアルタイムクロックへのアクセスに失敗すると、本製品がリブートすることがありましたが、これを修正しました。

5.4 フラッシュメモリーの容量不足で CREATE CONFIG コマンドが失敗したとき、指定したファイルがすでに存在する場合、そのファイルが削除されていましたが、これを修正しました。

5.5 FTP によるファームウェアの転送に失敗した後、再度本製品の FTP サーバーに接続すると、本製品がリブートすることがありましたが、これを修正しました。

5.6 FTP クライアントでホスト種別を自動判別にした場合、本製品に正しく FTP 接続できないことがありましたが、これを修正しました。

5.7 PURGE LOG および FLUSH LOG OUTPUT コマンド実行直後に、SHOW LOG コマンドに TAIL を指定して実行すると、本製品がリブートしていましたが、これを修正しました。

5.8 SHOW LOG コマンドにおいて、TAIL パラメーターで指定した件数のログが表示されない場合がありましたが、これを修正しました。

5.9 SHOW LOG コマンドに DATE、TIME、SEVERITY パラメーターを指定して、繰り返しコマンドを実行していると、メモリーが枯渇し、SNMP のアクセスに対して応答できなくなることがありましたが、これを修正しました。

5.10 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でしたが、これを修正しました。

5.11 SNMP 有効時、本製品 IP アドレスの設定を変更すると、SNMP へのアクセス、トラップの送信ができなくなっていましたが、これを修正しました。

5.12 SNMP において、ブリッジ MIB の dot1dStpTopChanges が、正しくカウントアップしませんでしたが、これを修正しました。

5.13 SNMP コミュニティーを登録し、GUI で表示した状態で、DELETE SNMP COMMUNITY コマンドによって削除後に GUI で表示しようとするとリブートしていましたが、これを修正しました。

5.14 IP アドレスが設定されていない状態で SNMP トラップが送信される状況になるとリブートが発生していましたが、これを修正しました。

5.15 SNTP モジュールを無効に設定した後 RESET NTP コマンドを実行すると、Last Updated と Last Delta の値が初期化されませんでしたが、これを修正しました。

5.16 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したが、これを修正しました。

5.17 Telnet 接続時、本製品から送信されるデータの改行コード「CR+LF」に Null が付加されていましたが、これを修正しました。

5.18 SET ACCESS FILTER ENTRY コマンドのエラーメッセージでフィルター名が正しく表示されませんでしたが、これを修正しました。

5.19 RADIUS アカウンティング機能において、コンソール（user-1）と Telnet（user-2）のような 2 ユーザーのログイン認証が行われたときに、Accounting-Interim-Update パケットが、後から認証された 1 ユーザー分しか送出されませんでしたが、これを修正しました。

5.20 RADIUS アカウンティング機能において、Accounting-Interim-Update パケットの送信が有効に設定されていても、1 ～ 3 パケット送信後に送信が停止していましたが、これを修正しました。
また、Accounting-Interim-Update パケットの送信後に本製品からログアウトをすると、Stop 属性の Accounting-Request パケットが送信されない場合がありましたが、これを修正しました。

5.21 DELETE SWITCH FILTER コマンド（または Web GUI の「機器監視 - FDB」）で、登録されているスタティックエントリーの削除を実行すると、削除失敗のエラーが表示されるにもかかわらず、スタティックエントリーは削除されていましたが、これを修正しました。

5.22 IP アドレスが DHCP に設定された状態から、固定または IP アドレスなしに設定した場合、DHCP クライアントが正常に停止しないことがありましたが、これを修正しました。

5.23 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ていましたが、これを修正しました。

5.24 タグ付きポートとして設定したポートを、デフォルト VLAN から削除すると、「delete vlan=default port=x」の設定が設定ファイルに表示されないため、設定を保存後再起動すると、設定が反映されていない状態で起動していましたが、これを修正しました。

5.25 EPSR アウェアにおいて、ENABLE SWITCH PORT コマンドによって Down のポートを Blocking に変更した場合にログメッセージが出力されていましたが、これを修正しました。また、Blocking のポートに対して、ENABLE SWITCH PORT コマンドを実行すると、同じログメッセージが 2 個出力されていましたが、これを修正しました。

5.26 すでにトランキング対象として設定済みのポートを再度トランクポートとして設定した場合のエラー表示が、条件によって異なっていましたが、これを修正しました。

5.27 SNMP トラップの送信を有効にした状態で、Telnet 接続により動作モード TRANSIT の EPSR ドメインを有効または無効に設定すると、リブートが発生していましたが、これを修正しました。

5.28 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したが、これを修正しました。

5.29 ポートがリンクアップするまでのオートネゴシエーションの処理時間が通常よりも長くかかる環境において、正しい値を読み取れずにエラーになる場合がありましたが、これを修正しました。

5.30 EPSR アウェアと MAC ベース認証の併用時、Supplicant の認証成功前に大量のトラフィックを受信して CPU に高負荷がかかると、EPSR マスターノードからの Healthcheck メッセージを受信できずに、EPSR のリンクダウンが発生することがありましたが、認証ポートの受信レートを監視して、一定のしきい値を超えた場合には未認証時の受信パケットを破棄するように改善しました。
上記のような環境下では、Supplicant MAC 透過機能を利用するなどして、未認証時の受信パケットによって CPU に高負荷がかからないようにしてください。

5.31 トランクグループのメンバーポートがすべてリンクダウンしたとき、FDB がクリアされずにリンクアップ後に通信できなくなることがありましたが、これを修正しました。

5.32 トランクグループ内でリンクしているポートが 1 ポート以下のときに、トランクグループに対してポートの追加または削除を行うと、内部エラーが表示されることがありましたが、これを修正しました。

5.33 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でしたが、これを修正しました。

5.34 （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でしたが、これを修正しました。

5.35 （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ての MLD Report を受信してもルーターポートに転送されませんでしたが、これを修正しました。

5.36 IGMP Snooping において、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でしたが、これを修正しました。

5.37 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でしたが、これを修正しました。

5.38 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したが、これを修正しました。

5.39 ポート認証において、EAP-PEAP 認証で RADIUS サーバーと通信したときにリブートが発生することがありましたが、これを修正しました。

5.40 ポート認証において、Supplicant の認証に成功したポートに対して、認証方式を変更するなど認証が解除される操作を行っても、Stop 属性の Accounting-Request パケットが送信されませんでしたが、これを修正しました。

5.41 ポート認証において、複数の Supplicant の認証を実施しているポートに対して、SET PORTAUTH PORT コマンドの TYPE パラメーターに NONE を指定して、ポート認証を無効にしても、Stop 属性の Accounting-Request パケットが 1 つの Supplicant 分しか送信されませんでしたが、これを修正しました。

5.42 ポート認証において、SET PORTAUTH PORT コマンドで PORTAUTH=AUTO を指定しているとき、MAC ベース認証によって認証済みの Supplicant と同一の送信元 MAC アドレスを持つ EAP パケットを受信すると、MAC ベース認証にもかかわらず、認証が解除されていましたが、これを修正しました。

5.43 ポートセキュリティーが有効なポートに STP を設定した場合のエラーメッセージを、適切なメッセージに修正しました。

5.44 RSTP において、6 台以上のスイッチによるリング構成時に、スイッチ間のリンクダウンから通信復旧まで約 30 秒の時間がかかっていましたが、これを修正しました。

5.45 SHOW CONFIG コマンドなどで複数画面に渡る情報を表示中に、Web GUI で設定を変更するとリブートが発生することがありましたが、これを修正しました。

5.46 Web GUI において、ログインパスワードに設定された文字列のうち 9 文字目以降がログイン認証に使用されていませんでしたが、これを修正しました。

5.47 Web GUI のマルチプル 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ていましたが、これを修正しました。

5.48 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されていましたが、これを修正しました。

5.49 Web GUI で、すでに存在する VLAN ID を別の VLAN 名で追加する操作を行うと、エラーメッセージが表示されるにもかかわらず、該当 VLAN が削除されていましたが、これを修正しました。

5.50 Web GUI の「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、エラーにならずに設定ができていましたが、これを修正しました。（ミラーポート、トランクポート、STP 有効ポート、EPSR リングポートは、Authenticator/Supplicant ポートに設定できません。また、スタティックエントリー登録ポート、ポートセキュリティー有効ポート、コンボポートは Authenticator ポートに設定できません。）

5.51 認証済み Supplicant が存在する Authenticator ポートを、Web GUI で所属 VLAN から削除する設定ができませんでしたが、これを修正しました。

5.52 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 と表示されていましたが、これを修正しました。

5.53 Web GUI の「機器監視 - システム情報」の「詳細情報表示」ボタンをクリックしたときに表示される「システム - 詳細表示」で情報が一部欠落していましたが、これを修正しました。

5.54 Web GUI において、「機器監視 - ログ」-「ログ表示条件」の「表示件数」に「#」を入力して「ログ表示」または「ログ保存」をクリックすると「500 Internal Server Error」が表示されていましたが、これを修正しました。

5.55 Web GUI において、Internet Explorer 7 および 8 の設定によっては、ファームウェアの転送に失敗する場合がありましたが、これを修正しました。

6 本バージョンでの制限事項

ファームウェアバージョン 1.6.9 には、以下の制限事項があります。

6.1 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。

6.2 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。

6.3 ターミナルサービス

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 サーバー機能において、複数のセッションで本製品へのログインとログアウトを長時間にわたって繰り返し行っていると、コンソールが応答しなくなったり、リブートが発生したりすることがあります。

6.4 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。

○ RADIUS アカウンティング機能有効時に、RADIUS サーバーから Access-Reject パケットを受信すると、本製品から Failed 属性が付加された Accounting-Request パケットが送信されます。

6.5 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

6.6 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。

6.7 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」

送出ポート決定アルゴリズムが異なる機器とポートトランキングを組んでいる場合、パケット通信中にマスターポートを抜き差しすると、瞬間的にループが発生することがあります。

6.8 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。

6.9 EPSR アウェア

参照「コマンドリファレンス」/「スイッチング」/「EPSR アウェア」

EPSR アウェアの動作モードが TRANSIT の場合、障害発生時に再起動を行うと、ポートがブロッキング状態のままになり、データ VLAN の通信ができなくなる可能性があります。

これは、再起動時に Double Fail への対応が正常に動作せず、プリフォワーディング状態からフォワーディング状態に遷移できないため、データ VLAN のリンクがブロックされたままになることで発生します。
本現象発生時には、ブロッキング状態のリングに接続しているポートを一度リンクダウンさせ、再度リンクアップさせることにより、復旧させることができます。

6.10 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。

6.11 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 PORTAUTH=AUTO を指定した場合、Web 認証において認証失敗（Held）になるまでのログイン試行回数にばらつきがあります。
- ○ SHOW PORTAUTH コマンドで表示される「Number of Total Supplicants」（システム全体の Supplicant 数）に、まれに実際の値と異なる値が表示されることがあります。
  なお、「Number of Total Supplicants」はファームウェアバージョン 1.6.9 で追加された項目になります（「7.21 ポート認証：SHOW PORTAUTH コマンド表示項目の Number of Total Supplicants」を参照してください）。
- ○ PIGGYBACK=ENABLED に設定されている 802.1X Authenticator ポートにおいて、Supplicant の認証時に FDB に登録されたスタティックエントリーが数秒後に削除されます。また、その後に同一 Supplicant と通信を行うと、Supplicant の MAC アドレスはダイナミックエントリーとして FDB に登録されます。

6.12 スパニングツリープロトコル

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。

6.13 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 VLAN）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 版）において、1 つの Uplink グループにタグ付きポートとタグなしポートを混在させる設定がエラーになりません。このような設定はしないようにしてください。

○ 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。

○ 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。

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、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・誤記訂正です。

7.1 ポート認証 / ループガード

参照 **「コマンドリファレンス」/「ポート認証」**
参照 **「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ーの 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ーの 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。

7.2 ポート認証 /EPSR アウェア

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

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。

7.3 ポートトランキング / スパニングツリープロトコル / ループガード

参照 **「コマンドリファレンス」/「スイッチング」**
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」**

コマンドリファレンスに「ポートトランキング、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）。

- ポートトランキングとスパニングツリープロトコル
- ポート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

7.4 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。

7.5 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。

7.6 フォワーディングデータベース：SET SWITCH AGEINGTIMER コマンド

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」

ファームウェアバージョン 1.6.9 で、SET SWITCH AGEINGTIMER コマンドに設定可能な最大値が 16383（秒）から 1000000（秒）に変更されましたので、以下に補足します。

○ SET SWITCH AGEINGTIMER=1..1000000

AGEINGTIMER: エージングタイム。1 ～ 1000000 秒。この時間内に受信されなかったダイナミックエントリーは削除される。デフォルトは 300（秒）

7.7 QoS：ENABLE/DISABLE/SHOW QOS コマンド

参照「コマンドリファレンス」/「QoS」

ファームウェアバージョン 1.6.9 で ENABLE QOS/DISABLE QOS/SHOW QOS コマンドが追加され、QoS による優先制御を優先させるか（ENABLE QOS）、パケット転送のパフォーマンスを優先させるか（DISABLE QOS）を選択できるようになりましたので、以下に補足します。

ファームウェアバージョン 1.6.1 以前のファームウェアでは常に有効（QoS による優先制御優先）でしたが、バージョン 1.6.9 以降のファームウェアではデフォルトで無効（パケット転送のパフォーマンス優先）になります。

バージョン 1.6.1 以前からバージョン 1.6.9 以降にバージョンアップした場合は、起動時設定ファイルの指定の有無によって、バージョンアップ後の動作が以下のように異なります。

- 起動時設定ファイルの指定なし（SET CONFIG=NONE）
  →無効（パフォーマンス優先）の状態で起動
- 起動時設定ファイルの指定あり（SET CONFIG=filename）
  →有効（QoS 優先）の状態で起動

○ ENABLE QOS
スイッチ内部のパケットバッファー制御を、パケット転送のパフォーマンスより QoS の優先制御を優先するように最適化する。

本コマンドを実行した場合は、設定を保存後、再起動する必要がある。デフォルトは無効（パケット転送のパフォーマンス優先）。

備考・注意事項

- パケット転送のパフォーマンスが輻輳時にデフォルト状態より低下する場合がある。
- ENABLE QOS コマンドを実行しなくても、QoS の設定・動作は可能だが、パケット転送のパフォーマンスを優先させるため、優先制御の効果が出にくい状態になることがある。

○ DISABLE QOS

スイッチ内部のパケットバッファー制御を、QoS の優先制御よりパケット転送のパフォーマンスを優先するように最適化する。
本コマンドを実行した場合は、設定を保存後、再起動する必要がある。デフォルトは無効（パケット転送のパフォーマンス優先）。

備考・注意事項

DISABLE QOS コマンドを設定した場合、以下の機能との併用は未サポート。

- HOL ブロッキング防止
- フローコントロール
- スパニングツリープロトコル
- EPSR アウェア
- ループガード（LDF 検出）

HOL ブロッキング防止やフローコントロールとの併用が未サポートであり、また、QoS による優先制御の効果が出にくいことから、本製品宛ての通信においてパケットロスが発生し、一時的に通信できなくなる可能性がある。

○ SHOW QOS

QoS 優先設定の情報を表示する。

```
Manager > show qos

QoS Information

-----------------------------------------------------

  Configured State .......... Disabled

  Actual State .............. Disabled

  Scheduling ................ Weighted Round-Robin

-----------------------------------------------------
```

Configured State	QoS の設定の状態。Enabled または Disable
Actual State	実際の QoS の状態。Enabled または Disable
Scheduling	QoS のスケジューリング方式。Weighted Round-Robin または Strict

7.8 スイッチング：ポート

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。

7.9 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。

7.10 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」

○ 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。

7.11 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）

○ ソースポートを複数設定している状態で、あるソースポートから入力されたパケットが、L2 スイッチングされて別のソースポートから出力された場合、ミラーポートにはパケットが 1 個だけ出力されます。

7.12 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。

7.13 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。

○ 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 パラメーターを、省略せずに 3 つすべて設定するようにしてください。
パラメーターを省略すると、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。

7.14 ループガード

参照 「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。

○ 受信レート検出機能を使用する際、エラーパケットを受信した場合も受信レートカウンターに計上されます。

7.15 EPSR アウェア

参照 「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 サーバー宛て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。

7.16 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後も 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。

7.17 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。

○ 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。

7.18 IGMP Snooping/MLD Snooping

参照 「コマンドリファレンス」/「IGMP Snooping」
参照 「コマンドリファレンス」/「MLD Snooping」

ポートトランキングと 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。

7.19 ポート認証

参照 「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の「ゲスト VLAN」に、解説として以下の補足をします。

ゲスト VLAN は、未認証時にのみ割り当てられる、同一 VLAN 内での通信が可能な VLAN です。
ゲスト VLAN を設定していない場合、未認証の状態ではたとえ同一 VLAN 所属のポート間であっても通信できませんが、これらのポートに対して同じゲスト VLAN を設定しておけば、未認証状態でもゲスト VLAN 内にかぎって通信が可能になります。なお、認証にパスした後は、ゲスト VLAN ではなくポート本来の VLAN、あるいは、ダイナミック VLAN によって割り当てられた VLAN の所属となります。

○ 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。

○ ゲスト VLAN と VLANASSIGNMENTTYPE=PORT の併用は 802.1X 認証の Single-Supplicant モードでのみ可能です。Multi-Supplicant モード、および MAC ベース認証と Web 認証の Single-Supplicant モードでは、ゲスト VLAN と VLANASSIGNMENTTYPE=PORT を併用することはできません。

7.20 ポート認証：SET PORTAUTH PORT コマンド EAPOLVERSION パラメーター

参照 「コマンドリファレンス」/「ポート認証」

ファームウェアバージョン 1.6.9 で SET PORTAUTH PORT コマンドに EAPOLVERSION パラメーターが追加されましたので、以下に補足します。

○ SET PORTAUTH PORT [EAPOLVERSION={1|2}]

EAPOLVERSION:（802.1X Authenticator ポート）EAPOL のバージョン。1 は IEEE 802.1X-2001 準拠モード、2 は IEEE 802.1X-2004 準拠モード。デフォルトは 1。

○ SHOW PORTAUTH PORT AUTHENTICATOR

```
Manager > show portauth port=5
-----All Authenticator Configuration ----------------------------------------
--------------------------------------------------------------------------------
Port Number                    5
Auth Mode                      MACBASED
Port Control                   Auto
Supplicant Mode                Multi
eapolVersion          [8021x]  1
Quiet Period                   60
～以下省略～
```

eapolVersion	EAPOL のバージョン。1、2 のいずれか。1 は IEEE 802.1X-2001 準拠モード、2 は IEEE 802.1X-2004 準拠モード

7.21 ポート認証：SHOW PORTAUTH コマンド表示項目の Number of Total Supplicants

参照「コマンドリファレンス」/「ポート認証」

ファームウェアバージョン 1.6.9 で SHOW PORTAUTH コマンドの表示項目に Number of Total Supplicants が追加されましたので、以下に補足します。

○ SHOW PORTAUTH

```
Manager > show portauth
Port Access Configuration Information:
 Port Access Control.............. Enabled
 Authentication Method ............ RADIUS EAP
 DHCP Pass Through ................ Enabled
 Number of Total Supplicants..... 0/240
～以下省略～
```

Number of Total Supplicants	システム全体の Supplicant 数

7.22 スパニングツリープロトコル

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」

○ スパニングツリーで Point to Point が無効の場合、上位のブリッジから proposal フラグがセットされた BPDU を受信しても、agreement フラグがセットされた BPDU が返されません。

○ 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。

7.23 Web GUI

参照 「コマンドリファレンス」/「Web GUI」

○ コマンドリファレンスの下記の場所に、CLI でしか実行できない操作項目の記載がありますが、「ファイルの削除」と「指定したファイルの内容表示」は Web GUI でも実行できますので、訂正してお詫びいたします。

- Web GUI/ 概要 / コマンドラインインターフェースとの機能の違い
- Web GUI/ マネージメント / ファイル管理

○ 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。

○ コマンドリファレンスの Web GUI/ スイッチ設定 / マルチプル VLAN（Protected Port 版）のポート（Ports）の解説において、「「AUTO」を指定すると PORT で指定した各ポート番号ごとに、グループが自動的に割り当てられます。」という記載がありますが、Web GUI の「VLAN 設定 - 追加」画面で「AUTO」を選択することはできませんので、訂正してお詫びいたします。

○ コマンドリファレンスの Web GUI/ 機器監視 / ログカウンターに「ログクリア」ボタンの説明がありませんので、以下に補足します。

- 「ログクリア」ボタンをクリックすると、ログカウンターがリセットされ、メモリー上のログが削除されます。

8 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

9 コマンドリファレンスについて

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、あわせてご覧ください。

コマンドリファレンスのパーツナンバー「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/