613-000530 Rev.R 160215

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　1.6.30

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、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　本バージョンで修正された項目

ファームウェアバージョン 1.6.28 から 1.6.30 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　特定の SNMP Manager からのアクセスによって、まれに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。

3.2　SET RADIUS コマンドの DEAD-ACTION パラメーターを設定した場合、2 台目以降の認証端末は DEAD-ACTION が実行されませんでしたが、これを修正しました。

3.3　同時に複数の Supplicant を処理する際に RADIUS サーバーへの要求再送回数を誤ってカウントアップしていましたが、これを修正しました。

3.4　Single Supplicant モードの MAC 認証にて、RADIUS サーバーとの認証処理が正常に完了しない場合、認証ステータスが不正な状態として残り、該当ポートにて MAC 認証が行えなくなっておりましたが、これを修正しました。

3.5　MAC 認証時に Server Timeout が発生するとポートがリセットされるまで、同ポートで再認証が行われませんでしたが、これを修正しました。

3.6　IGMP Snooping 使用時に、マルチキャストの登録処理に失敗し、マルチキャストパケットが転送不可となる場合がありましたが、これを修正しました。

3.7 RADIUS パケットの送信処理が正常に行われず、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。

3.8 DHCP パケット転送機能（dhcppassthrough）が有効な時に、ICMP ヘッダーのチェックサムが 0x0043 の ICMP パケットを受信すると、認証前にも関わらず、DHCP パケットだと誤認してしまいパケットを転送していましたが、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 1.6.30 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 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。

4.4 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。

○ ポート認証で RADIUS サーバーを 2 台登録し、かつ 2 台の RADIUS サーバーの共有パスワード（Secret 値）を異なる文字列に設定すると、認証に成功しない場合があります。ポート認証で 2 台の RADIUS サーバーを利用する場合は、Secret 値を同じ文字列に設定してください。

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 フォワーディングデータベース：SET SWITCH FDB 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」

SET SWITCH FDB コマンドの動作モードが DEFAULT の場合おいて、FDB に多数の MAC アドレスが登録されていると、ポート認証に失敗することがあります。

なお、本現象が発生した場合には本バージョンで追加した SET SWITCH FDB コマンドにて回避することが可能です。
コマンドの詳細は、「3.1 SET SWITCH FDB コマンド /SHOW SWITCH FDB コマンド」をご参照ください。

4.7 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。

4.8 QoS

参照「コマンドリファレンス」/「QoS」

PURGE QOS コマンドを実行しても、SET QOS SCHEDULING コマンドで設定した、MODE パラメーターがデフォルトの設定（WRR）に戻りません。コンフィグ上は QOS 関連の設定が消えるものの動的に動作が変更されません。再起動後は設定どおりの正常動作となります。

4.9 スイッチング

参照「コマンドリファレンス」/「スイッチング」

1000M Full Duplex 固定設定の SFP ポートで RESET SWITCH/ENABLE SWITCH PORT コマンドを実行すると、オートネゴシエーションでリンクします。このような場合には、再度ケーブルを接続しなおすと、正しく動作します。

4.10 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」

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。

4.11 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」

ソースポートがタグなしポートの場合、ミラーポートではタグ付きパケットが出力されます。ソースポートが1ポートおよび2ポート以上に設定された場合、どちらの場合もタグ付きパケットが出力されます。

4.12 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」

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。

4.13 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。

○ 同一ポート上で複数（2 つ以上 ）の EPSR ドメインを設定すると、あるドメインがフォワーディング状態となった際に、他のドメインもフォワーディング状態となり、ループが発生する場合があります。

4.14 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。

4.15 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（「5.25 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。

○ MAC ベース認証において、複数の VLAN に所属しているポートを認証ポートに設定した場合、同一 MAC アドレスからのパケットが該当ポートの複数の VLAN で受信され、認証が行われると、先に受信した VLAN での認証しか成功しない場合があります。

○ Web 認証において、リンクダウンをともなわない Supplicant のポート移動時に、Supplicant がログアウトしてからポートを移動しても、移動先で認証に失敗することがあります。

○ SET PORTAUTH PORT コマンドでサポート対象外のパラメーターの組み合わせを設定した場合、GUESTVLAN パラメーターに VLAN ID を指定するとエラーとなりますが、VLAN 名を指定した場合は本来はエラーになるのが正しいにもかかわらず、エラーとなりません。

4.16 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。

4.17 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。

5 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。

5.1 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。

5.2 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。

5.3 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

5.4 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。

5.5 RADIUS アカウンティング機能

参照「コマンドリファレンス」/「運用・管理」/「認証サーバー」

RADIUS アカウンティング機能を有効、アカウンティング要求を定期的に送信する UPDATEENABLE を有効にしていても、RADIUS サーバーが Accounting-Interim-Update パケットの Accounting-Request パケットに対して、Accounting-Response パケットを返さない場合、送信間隔の設定時間を過ぎても Accounting-Interim-Update パケットの再送は行いません。

5.6 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。

○ コマンドリファレンスの解説編に「学習機能をオフにすると、ほとんどのフレームが同一 VLAN 内の全ポートに出力されるようになるため、スイッチというよりも HUB に近い動作となります」という記述がありますが、本製品では学習機能をオフにすることができないため、この記述は当てはまりません。

5.7 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）

5.8 フォワーディングデータベース：SET SWITCH FDB 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 FDB コマンドが新たに追加され、フォワーディングデータベース（FDB）に関する設定を変更できるようになりましたので、以下に補足します。デフォルトでは DEFAULT の設定になります。

SET SWITCH FDB MODE={DEFAULT|STATIC-OVERRIDE}

DEFAULT: Version1.6.14 以前と同様の動作モード。

STATIC-OVERRIDE: FDB テーブルのインデックスが重なる場合にダイナミックエントリーを削除し、スタティックエントリーを登録する動作モード。

5.9 フォワーディングデータベース：SHOW SWITCH FDB 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、SHOW SWITCH FDB コマンドの表示項目に Mode が追加されましたので、以下に補足します。

SHOW SWITCH FDB

```
Manager > show switch fdb

Mode ..... Static Override

Switch Forwarding Database (Software)
-----------------------------------------------------------------
VLAN     MAC Address         Status     Port
-----------------------------------------------------------------
1          00-00-01-02-00-00     Dynamic   3
1          00-00-01-02-00-01     Dynamic   3
1          00-00-01-02-00-02     Dynamic   3
1          00-00-01-02-00-03     Dynamic   3
1          00-00-01-02-03-02     Dynamic   3
1          00-00-01-02-04-02     Dynamic   3
1          00-00-01-02-05-02     Dynamic   3
-----------------------------------------------------------------
```

Mode	FDB の動作モード。Default か Static Override。

5.10 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 Disabled
Actual State	実際の QoS の状態。Enabled または Disabled
Scheduling	QoS のスケジューリング方式。Weighted Round-Robin または Strict

5.11 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。

5.12 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。

5.13 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。

5.14 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。

5.15 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。

5.16 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。

5.17 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。

○ コマンドリファレンスの解説編には「アクション実行後は、タイマーが起動し、指定した時間が経過するとアクション実行前の状態に戻ります」とありますが、タイマー満了前でも次の条件を満たした場合はアクションが解除されます（LDF 検出、受信レート検出の両機能に共通）。

- ENABLE SWITCH PORT コマンドが設定されたとき
- DISABLE SWITCH PORT コマンドが設定されたとき
- リンクダウンが発生したとき（ACTION=LINKDOWN は除く）
- ポートセキュリティーの DISABLE アクションが実行されたとき
- ポートセキュリティーの DISABLE アクションが解除されたとき

○　ループガード機能は、ループ検出によりアクション実行前にループ検知のログ及び SNMP トラップを送信する仕様であるため、トラップ送信先の MAC アドレスが学習できていない場合、本体からの送信パケットがループしてしまうことがあります。

ただし、以下の方法により、本体からの送信パケットのループ発生頻度を下げることが可能です。

- トラップ送信先の MAC アドレスをスタティック登録する。
- トラップ送信先（監視用 PC）から定期的にスイッチを監視する。
- ループガード機能の BLOCKTIMEOUT パラメーターを NONE に設定する。

5.18 LDF 検出

参照「コマンドリファレンス」/「スイッチング」

○　配下の HUB やスイッチにて輻輳などにより LDF が消失した場合、ループを検出できない場合があります。

○　LDF のデフォルト送信間隔は 120 秒です。LDF の検出時間を短くしたいときは、SET SWITCH LOOPDETECTION コマンドの INTERVAL パラメーターで送信間隔を短く設定してください。LDF 検出機能の効果を最大にするには、送信間隔を最小値の 1 秒に設定する必要があります。ただし、送信間隔を短くするとソフトウェア処理に負荷がかかり、本製品宛て通信の応答時間など、他の機能の動作性能が低下する可能性があります。

5.19 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」

○　ファームウェアバージョン 1.6.9 から 1.6.14 へのバージョンアップにおいて、EPSR（トランジットノード）を有効化するときにリング接続ポートが両方ともリンクアップしている場合の動作（各種状態の設定）が以下のとおりに変更されましたので、以下に補足します。

	バージョン 1.6.9 まで	バージョン 1.6.14 から
EPSR ドメインの状態	Links-Up	Pre-Forwarding
リングを構成する第 1 ポートの状態	Forwarding	Forwarding
リングを構成する第 2 ポートの状態	Forwarding	Blocking

○　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。

○　コマンドリファレンスの解説編に掲載されている「トランジットノードの機能」の表（「ノードの種類」セクション）において、「デバッグ表示機能」の記載内容に誤りがありましたので下記のとおり訂正します。

誤

トランジットノードの機能	フル実装	アウェア機能（本製品の実装）	スヌーピング機能
デバッグ表示機能	○	○	×

正

トランジットノードの機能	フル実装	アウェア機能（本製品の実装）	スヌーピング機能
デバッグ表示機能	○	×	×

5.20 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。

5.21 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。

5.22 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。

5.23 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。

○ PORTAUTH=AUTO で認証を行った場合、通常 MAC ベース認証で問い合わせを行い、失敗した場合 802.1X 認証で再度認証を行いますが、Multi-Supplicant モードで Supplicant から EAP-start を受信すると 802.1X 認証で問い合わせを行います。

○ 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。

○ ファームウェアバージョン 1.6.9 では、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。

○ ポート認証機能において、SET AUTHENTICATION コマンドの DEAD-ACTION パラメーターに PERMIT を指定し、RADIUS サーバーからの応答がないときに通信を許可するよう設定する場合は、下記の条件を満たすように各パラメーターを設定してください。

SERVERTIMEOUT > TIMEOUT × (RETRANSMITCOUNT + 1) × RADIUS サーバー数

SERVERTIMEOUT	SET PORTAUTH PORT コマンドのパラメーター。デフォルト 30 秒（MAC ベース認証ポートでは 30 秒固定）
TIMEOUT	SET AUTHENTICATION コマンドのパラメーター。デフォルト 6 秒
RETRANSMITCOUNT	SET AUTHENTICATION コマンドのパラメーター。デフォルト 3 回
RADIUS サーバー数	ADD RADIUSSERVER SERVER コマンドで登録した RADIUS サーバーの数

特に RADIUS サーバーを 2 台登録する場合は、各パラメーターがデフォルトのままだと条件を満たさないため、条件を満たすように設定を変更する必要があります。

○ ポート認証機能でゲスト VLAN やダイナミック VLAN を使用し、Supplicant が DHCP サーバーから IP アドレスを取得する場合は、認証前の VLAN において DHCP サーバーのリースタイムを短く設定する必要があります。

5.24 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

5.25 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

5.26 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。

5.27 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。

○ スイッチ設定 / ポート / ポート設定画面の「設定」ボタンを押すと、対象ポートがいったんリンクダウンします。
設定内容に変更がない場合や、ポート名称だけを変更した場合などにもリンクダウンしますのでご注意ください。

○ コマンドリファレンスの Web GUI/ スイッチ設定 / スパニングツリーの解説において、基本設定の「スパニングツリー有効」で Rapid STP を無効にするポートについての記載に誤りがありました。下記のとおり訂正して、お詫びいたします。

誤

■ スパニングツリー有効
Rapid STP を有効にするポートにチェックを付けます。
Rapid STP を無効にするポートにチェックを付けます。

正

■ スパニングツリー有効
Rapid STP を有効にするポートにチェックを付けます。
Rapid STP を無効にするポートはチェックを外します。

○ コマンドリファレンスの Web GUI/ スイッチ設定 /EPSR の解説において、「EPSR ドメイン - 変更」画面で「EPSR ドメイン名（EpsrDomainName）」、「モード（Mode）」、「マルチキャストアドレス削除（DeleteMcast)」、「コントロール VLAN（ControlVlan）」が設定可能な項目として記載されていますが、「EPSR ドメイン - 変更」ではこれらの項目は変更できませんので、訂正してお詫びいたします。

5.28 SHOW SWITCH PORT COUNTER コマンド

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は、SHOW SWITCH PORT COUNTER コマンドで表示される下記統計カウンターの説明として「未サポート（常に 0 を表示）」と記載されていますが、「常に 0 を表示」という記述は誤りです。ただし、これらの統計カウンター自体は、コマンドリファレンスの記述どおり未サポートです。

- Transmit - Discards
- ExcessiveCollisions

○ コマンドリファレンスの SHOW SWITCH PORT COUNTER コマンドで表示される Receive - Discards についての記載に誤りがありました。下記のとおり訂正して、お詫びいたします。

誤

バッファーのオーバーフローなどで破棄された受信パケット数

正

ポートセキュリティーにより不正とみなされ、破棄された受信パケット数

5.29 LOOPDETECTION/STORMDETECTION トラップ

参照 「コマンドリファレンス」/「運用・管理」/「SNMP」

コマンドリファレンスの以下のコマンドで LOOPDETECTION/STORMDETECTION トラップについての記載に誤りがありました。

- ADD SNMP COMMUNITY
- CREATE SNMP COMMUNITY
- DELETE SNMP COMMUNITY
- DISABLE SNMP TRAP
- ENABLE SNMP TRAP
- SHOW SNMP TRAP

それぞれのトラップの説明は正しくは以下のとおりですので、訂正してお詫びいたします。

LOOPDETECTION：
LDF 検出においてループ検出 / アクション実行 / アクションのタイムアウトや、ENABLE SWITCH PORT コマンドの設定によるアクション実行前の状態への復旧時に送信されるトラップ

STORMDETECTION：
受信レート検出においてパケットストーム検出 / アクション実行 / アクションのタイムアウトや、ENABLE SWITCH PORT コマンドの設定によるアクション実行前の状態への復旧時に送信されるトラップ

6　サポートリミット一覧

パフォーマンス	
VLAN 登録数	256
MAC アドレス（FDB）登録数	8K
IPv4 ホスト（ARP）登録数	-
IPv4 ルート登録数	-
リンクアグリゲーション	
グループ数（筐体あたり）	FS909M（-PS）：2 FS917M（-PS）：2 FS926M（-PS）：3 ※1
ポート数（グループあたり）	4
ハードウェアパケットフィルター	
登録数	-
認証端末数	
認証端末数（ポートあたり）	50
認証端末数（装置あたり）	240
マルチプルダイナミック VLAN（ポートあたり）	-
マルチプルダイナミック VLAN（装置あたり）	-
ローカル RADIUS サーバー	
ユーザー登録数	-
RADIUS クライアント（NAS）登録数	-
その他	
VRF-Lite インターフェース数	-
IPv4 マルチキャストルーティングインターフェース数	-

※　表中では、K=1024
※1 10BASE-T/100BASE-TX ポートで 2 グループ、ギガビットポートで 1 グループ設定可能。合わせて 3 グループサポートします。

7　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
RESET PORTAUTH PORT
ENABLE/DISABLE WATCHDOG MEMORY
SHOW WATCHDOG

8　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/