613-000530 Rev.D 080314

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.D）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　1.4.1

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 1.4.0 から 1.4.1 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 1.4.1（613-000325 Rev.D）」をご覧ください。

2.1　ループガード

参照「コマンドリファレンス」/「スイッチング」

受信レート検出：
パケットの受信レートがポートごとに設定された上限値を上回った場合に、該当ポートに対してリンクダウンやブロードキャストパケットの受信停止といったアクションをさせることで、ループの発生を防止する受信レート検出に対応しました。
ENABLE SWITCH STORMDETECTION コマンドで機能を有効にし、SET SWITCH STORMDETECTION コマンドでパラメーターの設定を行います。

LDF 検出：
一定時間ごとに特殊な試験フレーム（LDF）を送出し、接続機器を介して同じ LDF が同じ筐体に戻って来た場合に、LDF 送出ポートに対してリンクダウンやブロードキャストパケットの受信停止といったアクションをさせることで、ループの発生を防止する LDF 検出に対応しました。
ENABLE SWITCH LOOPDETECTION コマンドで機能を有効にし、SET SWITCH LOOPDETECTION コマンドでパラメーターの設定を行います。

なお、ループガードは CLI でのみ設定可能です。

2.2　SHOW SWITCH PORT COUNTER コマンドの表示内容

参照「コマンドリファレンス」/「スイッチング」

SHOW SWITCH PORT COUNTER コマンドで表示される内容に以下の項目が追加されました。

Receive（受信トラフィックカウンター）：
PauseFrames（PAUSE フレーム数）

UndersizePkts（アンダーサイズフレーム数）
Fragments（フラグメントフレーム数）
Jabbers（ジャバーフレーム数）

Transmit（送信トラフィックカウンター）：
PauseFrames（PAUSE フレーム数）

2.3 DISABLE SWITCH PORTコマンドの LINK パラメーター

参照「コマンドリファレンス」/「スイッチング」

DISABLE SWITCH PORT コマンドに LINK パラメーターが追加され、ポートをディセーブルにすると同時に、物理的にリンクダウンさせるかどうかを指定できるようになりました。LINK=DISABLE を指定した場合、ポートが物理的にリンクダウンします。LINK パラメーター省略時および LINK=ENABLE を指定した場合、ポートはリンクアップしたままとなります。なお、本機能は CLI でのみ設定可能です。

3 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 1.4.0 から 1.4.1 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。

3.1 DISABLE SWITCH PORTコマンドの仕様変更

参照「コマンドリファレンス」/「スイッチング」

DISABLE SWITCH PORT コマンドでトランクグループに所属しているスイッチポートを無効にできるようになりました。ステータスが無効のスイッチポートをトランクグループに追加することも可能です。

4 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 1.4.0 から 1.4.1 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。

4.1 ブロードキャスト、マルチキャスト（予約済みマルチキャストを除く）、未学習のユニキャストパケットを 0.08Mbps（64Byte パケット長の場合は 160pps）以上受信していると、本製品宛ての ARP に応答しない場合がありましたが、これを修正しました。

4.2 パケット長が 340Byte 以上のブロードキャスト、マルチキャストパケットを 0.11Mbps 以上受信していると、本製品宛ての通信でパケットロスが発生していましたが、これを修正しました。

4.3 本製品宛てのユニキャストパケットを 0.08Mbps（64Byte パケット長の場合は 160pps）以上受信していると、フローコントロール（802.3x PAUSE）が動作していましたが、これを修正しました。

4.4 オブジェクト ID「ipNetToMediaNetAddress(1.3.6.1.2.1.4.22.1.3)」に、IP アドレスが逆の順序（192.168.1.1 の場合、1.1.168.192）でセットされていましたが、これを修正しました。

4.5 ipAdEntIfIndex（1.3.6.1.2.1.4.20.1.2）および ipNetToMediaIfIndex（1.3.6.1.2.1.4.22.1.1）に、IfIndex（1.3.6.1.2.1.2.2.1.1）にない IfIndex が設定されていましたが、これを修正しました。

4.6 SNMP マネージャーによって、FAN、TEMPERATURE、VOLTAGE、LOGIN トラップが正しく識別されない場合がありましたが、これを修正しました。

4.7 MAC アドレスが複数登録されている状態で、ブリッジ MIB からインターフェース MIB にかけての Get Next を実行すると、SNMP や Ping に応答しなくなる場合がありましたが、これを修正しました。

4.8 ARP キャッシュに大量のエントリーが登録されている場合、プライベート MIB と MIB-II の IP グループの取得に時間がかかっていましたが、これを修正しました。

4.9 プライベート MIB のトラップを送信し続けるような状況にあると、メモリーリークを起こし、本製品宛ての通信ができなくなる、本製品がリブートするなどの現象が発生していましたが、これを修正しました。

4.10 ファームウェアバージョン 1.3.0 以前で作成された設定ファイルに enable snmp trap=fan の設定が含まれる場合、バージョン 1.4.0 では、コマンドがエラーとなり設定が反映されませんでしたが、バージョン 1.4.1 以降では、エラーにならないように修正しました。

4.11 本製品宛ての通信に高負荷がかかっていると、Telnet の接続エラーが発生し、本製品がハングアップすることがありましたが、これを修正しました。

4.12 RADIUS アカウンティング機能有効時、大量の Accounting-Response パケットを受信するとメモリーリークが発生していましたが、これを修正しました。

4.13 FDB にスタティック MAC アドレスが 2048 個登録されている状態で、認証ポートを移動させると、まれに RADIUS サーバーのスタティック MAC アドレスが削除され、移動先のポートで認証ができなくなることがありましたが、これを修正しました。

4.14 FDB にスタティック MAC アドレスが 2048 個登録されている状態で、ポートセキュリティーのモードを変更すると、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。

4.15 FDB に大量の MAC アドレスが登録されている状態で、本製品宛ての通信を長時間実行していると、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。

4.16 本製品自身の MAC アドレスがスタティックエントリーとして FDB に登録されている場合、設定を保存し、再起動するとエラーが発生する場合がありましたが、これを修正しました。

4.17 SHOW SWITCH FDB コマンドに SW を指定してソフトウェア FDB を表示させるとき、MAC アドレスの登録数が多いと、実際に学習されているアドレスが表示されるまでに時間がかかっていましたが、これを修正しました。

4.18 本製品では、ICMP Redirect メッセージは無視される仕様ですが、処理が行われる場合があったため、これを修正しました。

4.19 1 つのポートに対して、通信モードの固定設定（SPEED で AUTONEGOTIATE 以外を指定）とパケットストームプロテクションの設定（BCLIMIT/DLFLIMIT/MCLIMIT）を同時に行い、設定を保存後本製品を再起動すると該当ポートがリンクアップしなくなっていましたが、これを修正しました。

4.20 ポートを DISABLE SWITCH PORT コマンドで無効にした設定で本製品を起動後、ENABLE SWITCH PORT コマンドで該当ポートを有効にしても通信ができませんでしたが、これを修正しました。

4.21 トランクグループ所属ポートの通信モード（トランクグループ全体ではなくポート個々の通信モード）がオートネゴシエーション以外に設定されている場合、該当ポートのリセットを行うと、通信ができなくなっていましたが、これを修正しました。

4.22 (FS909M-PS/FS917M-PS/FS926M-PS のみ）本製品宛ての通信に高負荷がかかっている状態で SHOW SYSTEM コマンドを実行すると、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。

4.23 スパニングツリーと IGMP Snooping 併用時、IGMP パケットを高レートで長時間受信し続けると、不正なトポロジーチェンジや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。

4.24 ポート認証有効時、Authenticator ポートとしてリンクしているポートに対して、SET PORTAUTH PORT コマンドで TYPE パラメーターに NONE を指定して実行後、さらに同コマンドで TYPE パラメーターに AUTHENTICATOR を指定して実行すると、該当ポートで再認証がされませんでしたが、これを修正しました。

4.25 Authenticator ポートを Multi-Supplicant モードから Single-Supplicant モードに設定変更して認証を行うと、認証後再度 Supplicant に EAP-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。

4.26 802.1X Authenticator ポートと MAC ベース認証ポートが混在し、それぞれで認証が行われた場合、SHOW PORTAUTH コマンドで正しい内容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。

4.27 ゲスト VLAN 設定時、いったんポート認証モジュールを無効にしてから再度有効にすると、Authenticator ポートが未認証の状態であるにもかかわらず、ゲスト VLAN の所属になりませんでしたが、これを修正しました。

4.28 ダイナミック VLAN 有効時、いったんポート認証モジュールを無効にしてから再度有効にすると、RADIUS サーバーから有効な VLAN の情報が返ってきているにもかかわらず、ポートが本来の VLAN 所属となっていましたが、これを修正しました。

4.29 802.1X 認証において、2 台の RADIUS サーバーが登録された状態で本製品を起動後、優先順位 2 のサーバーでのみ認証が行われた場合、1 回目の認証に失敗していましたが、これを修正しました。

4.30 ポートがダイナミック VLAN にアサインされているとき、ADD VLAN PORT コマンドで該当ポートの（本来の）所属 VLAN を変更した場合、認証済みの Supplicant がいなくなっても、設定変更が反映されず、変更前の VLAN に所属していましたが、これを修正しました。

4.31 ダイナミック VLAN が有効で、かつ Multi-Supplicant モードのときに、1 台目の Supplicant が認証失敗、2 台目の Supplicant が認証成功後、再度待機中だった 1 台目の Supplicant の認証を行うと、SHOW PORTAUTH コマンドで 1 台目の Supplicant の情報が 2 つ表示されていましたが、これを修正しました。

4.32 ダイナミック VLAN が有効で、かつ Multi-Supplicant モードのときに、複数の Supplicant の認証が同時に行われ、認証に成功した Supplicant と失敗した Supplicant への処理が重なると、ポートがダイナミック VLAN にアサインされず、本来の VLAN 所属になっていましたが、これを修正しました。

4.33 Service-Type 属性のない Access-Accept パケットを受信しても認証が成功していましたが、認証失敗となるように修正しました。

4.34 本製品から送出される Accounting-Interim-Update パケットの NAS-Port 属性に Authenticator の物理ポート番号＋1 の値がセットされていましたが、これを修正しました。

4.35 SET PORTAUTH PORT コマンドで CONTROL パラメーターに UNAUTHORISED が設定されているポートが、DISABLE PORTAUTH コマンドでポート認証モジュールを無効にしたあと、通信できなくなっていましたが、これを修正しました。

4.36 MAC ベース認証と IGMP Snooping の併用時、FDB に不要な MAC アドレスが登録される、または登録されるべきマルチキャストアドレスが登録されないことがありましたが、これを修正しました。

4.37 ポート認証時、FDB に最大数まで MAC アドレスが登録されていると、認証済みの Supplicant を FDB に登録できず、Authenticator ポートの状態は待機中になりますが、このときに Stop 属性を持つ Accounting-Request パケットを送信し、セッションの終了が RADIUS サーバーに通知されるように修正しました。

4.38 DISABLE SWITCH PORT コマンドで無効に設定されているポートに対して、さらに Authenticator ポートにする設定を行うと、該当ポートからパケットが送信されていましたが、これを修正しました。

4.39 802.1X Authenticator ポートを PIGGYBACK=ENABLED に設定されたまま MAC ベース認証ポートに変更できていましたが、MAC ベース認証ポートでは PIGGYBACK=DISABLED になるように修正しました。

4.40 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 ploposal 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 が返されませんでしたが、これを修正しました。

4.41 スパニングツリー有効時、BPDU の受信のタイミングによっては、ルートブリッジからの情報が反映されず、ループが発生する場合がありましたが、これを修正しました。

4.42 FDB に大量の MAC アドレスが登録されている状態でスパニングツリーのトポロジーチェンジが発生すると、トポロジー再構築後、本製品宛ての通信がただちに復旧しない場合がありましたが、これを修正しました。

4.43 ダイナミック VLAN 有効時、認証と再認証が繰り返し行われていると、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。

4.44 ポート認証有効時、Web GUI 上でゲスト VLAN に指定されている VLAN を削除しようとしても、正しい内容のエラーメッセージが表示されませんでしたが、これを修正しました。

4.45 Web GUI で、「ログ表示」や「FDB 表示」などのウィンドウを表示させた状態で、「ポート認証 - ポート設定」の Authenticator ポートの設定画面を開けませんでしたが、これを修正しました。

5 本バージョンでの制限事項

ファームウェアバージョン 1.4.1 には、以下の制限事項があります。

5.1 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。

5.2 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 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。

5.3 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。SET RADIUS コマンドの DEADTIME パラメーターが 0（ゼロ＝デフォルト）の場合、本現象は発生しません。

5.4 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

5.5 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。

5.6 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。

5.7 IGMP Snooping について

参照「コマンドリファレンス」/「IGMP Snooping」

○ IGMP Snooping でグループが登録される前に、マルチキャストデータを高レートで受信し続けると、グループが登録されていない状態では IGMP パケットが転送されない場合があります。

○ 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。

5.8 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 ベース認証において、Authenticator ポートと同一の VLAN にリンクアップしているポートがないと、未学習のユニキャストパケット受信時に認証が開始されません。

5.9 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。

5.10 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。

○ Web GUI の「セキュリティー設定」-「ポート認証」の「ポート設定」で、Authenticator ポートのモード（Mode）にMulti を指定していても、Piggy back モード（PiggyBack）で Enabled の選択が可能です。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、Piggy back モードは有効になりません）。

6 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 1.4.1（613-000325 Rev.D）」の補足事項です。

6.1 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。

6.2 SET SWITCH PORT コマンドの SPEED パラメーター

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。

6.3 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。

6.4 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。

6.5 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。

6.6 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。

6.7 ポート認証

参照「コマンドリファレンス」/「ポート認証」

本製品の RADIUS パケットの Framed MTU は 1024Byte に設定してあります。このため、認証・検疫動作に 1024Byte を超えるデータサイズを必要とする一部の EAP との間で認証ができないことがあります。

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

ADD/SET/DELETE PORTAUTH PORT SUPPLICANTMAC

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「CentreCOM FS900M シリーズ コマンドリファレンス 1.4.1（613-000325 Rev.D）」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.D」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/