



613-000710 Rev.P 130315



最初にお読みください

CentreCOM® 9424T/SP-E リリースノート

この度は、CentreCOM 9424T/SP-E 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、取扱説明書とコマンドリファレンスの補足や、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 2.5.12J

2 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 2.5.9J から 2.5.12J 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。

- 2.1 ログ出力をとまなうパケットを高負荷で受信した場合に、CPU を介する通信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。
- 2.2 SHOW DEBUG コマンド実行後、スイッチポートまたはポートカウンタをリセットし、再度 SHOW DEBUG コマンドを実行すると、本製品が再起動しましたが、これを修正しました。
- 2.3 ポート認証が設定されているとき、認証ポートではない通常のポートで IGMP メッセージ (Membership Report など) を受信し、PURGE LOG コマンド実行後、SHOW SWITCH FDB コマンドや SHOW LOG コマンドを実行すると、本製品が再起動していましたが、これを修正しました。
- 2.4 特定の Telnet クライアントから、Telnet 接続できませんでしたが、これを修正しました。
- 2.5 Rapid STP 有効時、エッジポートに設定されたポートでリンクアップ・ダウンが発生すると、トポロジーチェンジのログ、トラップが生成されていましたが、これを修正しました。
- 2.6 ルーティング後のパケットが常にユーザプライオリティー 7 で扱われていましたが、これを修正しました。
- 2.7 同一ポート上で 802.1X 認証と MAC ベース認証を併用しているとき、特定の Supplicant に対する認証方式が 802.1X 認証から MAC ベース認証に切り替わっても、802.1X 認証で使っていた State 属性値を RADIUS サーバーに送信していたため認証が正常に行われないことがありましたが、これを修正しました。

- 2.8 ポートトラッキングとポート認証を併用しているとき、トラックポートで学習されている MAC アドレスと同じ MAC アドレスからのパケットをポート 1 で受信しても、認証に成功するにも関わらず、破棄されていましたが、これを修正しました。
- 2.9 トラックポートで学習されている MAC アドレスと同じ MAC アドレスを持つ Supplicant がポート 1 にて Web 認証を試みた際、Web 認証の画面が表示されませんが、これを修正しました。
- 2.10 ローカル IP インターフェースが設定されているとき、ファイル転送 (TFTP)、ログ転送 (syslog)、SNTP において、筐体から送信されるパケットの送信元 IP アドレスに、ローカル IP インターフェースの IP アドレスではなく、最短経路のダイレクトインターフェースの IP アドレスを使用していたが、これを修正しました。
- 2.11 DHCP/BOOTP リレーエージェント機能を有効にしても、DHCP サーバーから送信された DHCPNAK メッセージが転送されませんでした。これを修正しました。
- 2.12 SHOW DEBUG コマンド実行時、ごくまれに本製品が再起動する場合がありますが、これを修正しました。

3 本バージョンでの制限事項

ファームウェアバージョン 2.5.12J には、以下の制限事項があります。

3.1 MSTP とポートトラッキングの併用

マルチプルスパンニングツリープロトコル (MSTP) とポートトラッキングは併用できません。


3.2 ポート認証 (802.1X 認証 / MAC ベース認証) と攻撃検出機能の併用

ポート認証 (802.1X 認証 / MAC ベース認証) と攻撃検出機能は併用できません。

3.3 IGMP Snooping とポートセキュリティの併用

IGMP Snooping とポートセキュリティは併用できません。

3.4 マネージメントアクセスコントロール

 [「コマンドリファレンス」](#) / [「運用・管理」](#) / [「マネージメントアクセスコントロール」](#)


エントリーがない状態でマネージメントアクセスコントロールを有効にした場合は、ARP パケットの受信も許可しなくなる (ARP Request に応答しない) 仕様ですが、一度エントリーを追加して削除するという操作によってエントリーがない状態にした場合は、ARP パケットの受信が許可されるようになります。

3.5 SHOW CONFIG DYNAMIC コマンド

 [「コマンドリファレンス」](#) / [「運用・管理」](#) / [「コンフィグレーション」](#)

設定ファイルの保存中に、SHOW CONFIG コマンドを DYNAMIC オプションを指定して実行すると、該当の設定ファイルが破損する場合があります。


3.6 コンパクトフラッシュ

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「記憶装置とファイルシステム」

コンパクトフラッシュ上のファイルに対して、ディレクトリーを指定して以下のコマンドを実行することができません。


- ・ COPY
- ・ RENAME
- ・ DELETE
- ・ SET CFLASH DIR

3.7 認証サーバー

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「認証サーバー」


RADIUS アカウンティング機能において、Acct-Status-Type 属性が Stop の Accounting-Request パケットに User-Name が含まれません。

3.8 TFTP サーバーを使用したアップロード・ダウンロード

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「アップロード・ダウンロード」


TFTP サーバーからダウンロードした 45Byte より小さいファイルを TFTP サーバーにアップロードすると、本製品がリブートすることがあります。

3.9 ログ

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「ログ」


本製品 (CPU) 宛てのパケットを高レートで受信していると、「rps: RPS not present」という不正なログが出力される場合があります。これは表示だけの問題であり、動作には影響ありません。

3.10 SNMP

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」


複数の SNMP マネージャーから同時にプライベート MIB の取得を繰り返し行っていると、本製品の SNMP エージェントが応答しなくなる場合があります。

3.11 EAP パケット透過機能

 **参照** 「コマンドリファレンス」 / 「スイッチング」

SET SWITCH MULTICASTMODE に B、C、D または E を指定して EAP パケット透過機能を有効にしたとき、タグなしレポートで受信した 68Byte 以上の EAP パケットが正しく転送されません。

3.12 ポート設定


 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」

- SET SWITCH PORT コマンドの COMBO パラメーターに FIBER (SFP の光ファイバーポート) を指定するときは、あらかじめ該当ポートの通信モードを AUTONEGOTIATE または 1000MFULL に設定しておいてください。

通信モードが 10/100M のまま FIBER に設定して保存すると、再起動時に FIBER の設定がエラーではじかれます。


- SET SWITCH PORT コマンドの SPEED パラメーターで 10MHAUTO、10MFAUTO、100MHAUTO、100MFAUTO のいずれかに設定されたポートに対して、RESET SWITCH PORT コマンドを実行すると、設定ファイルに SPEED パラメーターの設定は残っていますが、実際には AUTONEGOTIATE でリンクされます。SPEED パラメーターを設定しなおすか、本製品を再起動してください。

3.13 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」 / 「ポート」


- ARP エントリーが登録されているポートを含めてトランクグループを作成すると、負荷分散が行われません。トランクグループ作成後、RESET IP INTERFACE コマンドで ARP エントリーを削除すると、正常に負荷分散されるようになります。
- 作成済みのトランクグループにポートを追加すると、FDB にポート番号が正常に登録されず、通信ができなくなります。該当トランクポートをいったんリンクダウン→リンクアップさせると、通信可能になります。
- トランクグループからポートを削除し、該当ポートで通信を行うと、トランクポートではないにもかかわらず、FDB のポート番号に削除前のトランクグループ ID が登録されます。

3.14 ポートセキュリティ

 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」


- 本製品に IP アドレスが設定されているとき、ポートセキュリティが有効なポートで、本製品の IP アドレス宛の ARP Request を受信すると、ARP Reply がフラッディングされます。
- ポートセキュリティ有効ポートにおいて、通信が許可されている端末との間で通信が行われたあと、該当端末を別のポートに移動すると移動先のポートでも通信ができてしまいます。該当端末の ARP エントリーがエージングで削除されていれば、移動先のポートで通信はできません。

3.15 EPSR Snooping

 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「EPSR Snooping」


SHOW/DISABLE EPSRSNOOPING コマンドの CONTROLVLAN パラメーターに VLAN 名が 20 文字のコントロール VLAN を VLAN 名で指定することができません。VLAN 名が 20 文字のコントロール VLAN は、VLAN ID で指定するようにしてください。

3.16 マルチプル VLAN (Protected Ports VLAN)

 **参照** 「コマンドリファレンス」 / 「バーチャル LAN」


Protected Ports VLAN のクライアントポートとタグ付きポートは同一ポートに設定できない仕様ですが、先にクライアントポートを設定し、次に同一ポートをタグ付きポートにする設定を行うと、設定がエラーではじかれません。

3.17 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」 / 「STP」


スパニングツリー有効時、DISABLE SWITCH PORT コマンドを実行すると、SHOW STP PORT コマンドの表示項目「State」において、該当ポートが Blocking で表示されます。表示上の問題であり動作には問題ありません。

3.18 ラビッドスパニングツリー

 **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」 / 「Rapid STP」


Rapid STP 有効時、DISABLE SWITCH PORT コマンドを実行すると、SHOW RSTP コマンドに PORTSTATE パラメーターを指定して表示される「Enable」において、該当ポートが Disabled で表示されます。表示上の問題であり動作には問題ありません。

3.19 ポリシーベース QoS

 **参照** 「コマンドリファレンス」 / 「QoS」 / 「ポリシーベース QoS」

- トラフィックが同一 QoS ポリシー内の複数のトラフィッククラスにマッチした場合、CREATE QOS TRAFFICCLASS コマンドの MAXBANDWIDTH パラメーター（最大帯域設定）が正しく動作しません。
MAXBANDWIDTH パラメーターを指定する場合は、同一 QoS ポリシー内で、複数のトラフィッククラスにマッチするような設定（IP と TCP、TCP と TCP ポートなど一方がもう一方を包括するようなフィルターの指定）をしないようにしてください。
- CREATE QOS POLICY コマンドの REDIRECTPORT パラメーターでトラフィックの出力先ポートとして指定されたポートから送出されるパケットにタグが付与されます。ただし、REDIRECTPORT に指定されたポートと同じポートグループ（1～12のグループまたは13～24のグループ）内から転送されたパケットに限り、本現象が発生します。
- SET QOS TRAFFICCLASS コマンドの EXCEEDREMARKVALUE パラメーターに NONE を指定することができません（エラーではじかれます）。EXCEEDREMARKVALUE パラメーターを NONE に戻す場合は、該当のトラフィッククラスを DESTROY QOS TRAFFICCLASS で一度削除し、トラフィッククラスを作成しなおしてください。

3.20 ハードウェアパケットフィルター

 **参照** 「コマンドリファレンス」 / 「ハードウェアパケットフィルター」

ハードウェアパケットフィルターを設定する場合には、以下の点にご注意ください。

- アクションに許可（permit）を使用する場合は、許可（permit）が指定されているエントリーを最後（最も大きい番号）になるように設定してください。

コマンドリファレンスの「ハードウェアパケットフィルター」 / 「概要・基本設定」に、許可（permit）のエントリーが最後（最も大きい番号）になっていない例が掲載されていますので、訂正してお詫びいたします。

誤：

■ 192.168.20.100 のみ双方向の通信が可能。

CREATE CLASSIFIER=1 IPDADDR=192.168.20.100/32 ↓

CREATE CLASSIFIER=2 IPSADDR=192.168.20.100/32 ↓

```
CREATE CLASSIFIER=3 PROTOCOL=ARP ↓  
CREATE CLASSIFIER=4 ↓  
CREATE ACL=1 ACTION=PERMIT CLASSIFIERLIST=1 PORTLIST=ALL ↓  
CREATE ACL=2 ACTION=PERMIT CLASSIFIERLIST=2 PORTLIST=ALL ↓  
CREATE ACL=3 ACTION=PERMIT CLASSIFIERLIST=3 PORTLIST=ALL ↓  
CREATE ACL=4 ACTION=DENY CLASSIFIERLIST=4 PORTLIST=ALL ↓
```

正：

■ 192.168.20.100 のみ双方向の通信が可能。

```
CREATE CLASSIFIER=1 IPDADDR=192.168.20.100/32 ↓  
CREATE CLASSIFIER=2 IPSADDR=192.168.20.100/32 ↓  
CREATE CLASSIFIER=3 PROTOCOL=ARP ↓  
CREATE CLASSIFIER=4 ↓  
CREATE ACL=1 ACTION=DENY CLASSIFIERLIST=4 PORTLIST=ALL ↓  
CREATE ACL=2 ACTION=PERMIT CLASSIFIERLIST=1 PORTLIST=ALL ↓  
CREATE ACL=3 ACTION=PERMIT CLASSIFIERLIST=2 PORTLIST=ALL ↓  
CREATE ACL=4 ACTION=PERMIT CLASSIFIERLIST=3 PORTLIST=ALL ↓
```

上記設定を行っても、設定どおりにフィルターが動作しない場合は、設定を保存後再起動してください。

- アクション許可 (permit) とアクション破棄 (deny) を併用する場合は、許可 (permit) と破棄 (deny) の各エントリーに同じ IP マスク値 (例：24 ビット) を設定しないでください。
許可 (permit) と破棄 (deny) の各エントリーで同じ IP マスク値を使用する場合は、必ず、どちらか片方のエントリーにその他のパラメーター (例：UDP など) を指定してください。

3.21 ポート認証


参照 「コマンドリファレンス」 / 「スイッチング」 / 「ポート認証」

- ポートを Authenticator ポートに設定すると、同ポートで自動的にイーグレスフィルタリングが有効になり、その設定が設定ファイルに書き込まれます。Authenticator ポートではイーグレスフィルタリングが有効になっている必要がありますので、イーグレスフィルタリングの設定は変更しないようにしてください。
- SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの MODE パラメーターに MULTI、CONTROL パラメーターに AUTHORISED を指定しているとき、SHOW PORTAUTH (PORT) または SHOW PORTACCESS (PORT) コマンドでサブリカント数が正しく表示されない場合があります。
- Authenticator ポートに、ADD SWITCH FILTER コマンドによるスタティック MAC アドレスの登録が可能です。登録されたスタティック MAC アドレスで通信をすることはできません。
- ダイナミック VLAN で、認証されたポートを別の MST インスタンスに所属する VLAN に指定した場合、同一 VLAN 内でも通信ができなくなります。
- ポートがゲスト VLAN に割り当てられているとき、ゲスト VLAN に所属する別の PC から未学習のユニキャストアドレスでは通信できません。
- MAC ベース認証使用時、SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの REAUTHPERIOD パラメーターで指定する Supplicant の再認証間隔が、

FDB のエージングタイムよりも短く設定されていると、Supplicant の MAC アドレスがエージングによって削除されなくなります。


- Web 認証の HTTP リダイレクト機能において、Supplicant のアクセス先が URL パラメーター付きの URL (?name=value が付加されている URL) の場合、Web 認証画面にリダイレクトされません。
- 802.1X 認証において、SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの PORTMOVEREAUTH パラメーターが DISABLED (再認証を行う) に設定されているとき、Authenticator ポートに HUB などを介して接続されている Supplicant を、同一スイッチ内の別の Authenticator ポートに (Authenticator ポートをリンクダウンさせずに) 移動して認証を行うと、ARP の登録が更新されず、移動先のポートで通信できません。
- 802.1X 認証または Web 認証と、ゲスト VLAN 併用時、Supplicant に対して認証許可状態を解除しても、ただちにゲスト VLAN の所属にならないことがあります。
- ポート認証設定時に自動的に設定ファイルに書き込まれる「set switch port(s)=X unicastegressfiltering=yes」が、認証ポートでリンクダウンが発生すると、SHOW CONFIG コマンドの DYNAMIC オプションで表示されなくなる場合があります。

3.22 IP

 **「コマンドリファレンス」 / 「IP」**


サーバーとして使用される UDP または TCP ポート番号がヘッダーの終点ポートにセットされた TTL=1 のパケットを受信すると、ICMP Time Exceeded メッセージが送信されません。

3.23 IP インターフェース

 **「コマンドリファレンス」 / 「IP」 / 「IP インターフェース」**


大量の IP インターフェースを作成すると、IP アドレスは割り当てられるにも関わらず CLI 上にエラーが出力されることがあります。この場合、当該インターフェースの ifEntry は取得できません。

3.24 ARP

 **「コマンドリファレンス」 / 「IP」 / 「ARP」**

ARP 解決されていない IP アドレス宛てのルーティングされた 1 パケット目の TTL の値が 2 減算されます。

3.25 IPv6 マルチキャスト

 **「コマンドリファレンス」 / 「IPv6 マルチキャスト」**

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。


4 取扱説明書・コマンドリファレンスの補足・誤記訂正

同梱の取扱説明書、および「CentreCOM 9424T/SP-E コマンドリファレンス 2.5 (613-000699 Rev.E)」の補足事項です。

4.1 本製品起動時のご注意


本製品の電源をオンにしてから起動が完了するまでの間は、電源ケーブルを抜いたり、リセットボタンを押したりしないでください。

4.2 SNMP

 **「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」**


- プライベート MIB の `atiStkSwSysProductInfoTable` 内 `atiStkSwSysDCState` が正しい値を返しません。リダンダント電源装置「CentreCOM RPS3204」使用時は、`SHOW SYSTEM` コマンドで本製品の電源とリダンダント電源装置の電源の On/Off を確認してください。
- 本製品の仕様では、`ipAdEntIfIndex` および `ifIndex` には、物理ポート数 + (VLAN ID × 16) の値が付与されます。

4.3 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」**


- リンクダウンをとまなわない端末移動があった場合、学習機能により登録された MAC アドレスがエージングするまで、通信が復旧しないことがあります。
- IP インターフェースを複数作成すると、FDB に PORT0 (ゼロ) の MAC アドレス (本製品の MAC アドレス) が複数表示されます。
- ポートグループ 1 ~ 12 とポートグループ 13 ~ 24 グループ間で通信を行った場合、同一の MAC アドレスがどちらのポートの FDB にも表示される場合があります。
- FDB にエントリーが多数登録されている状態で、SNMP 経由でプライベート MIB の FDB エントリー情報を取得しようとすると、「Error allocating memory」というエラーログが出力され、FDB エントリー情報を取得できない場合があります。

4.4 複数ポートから 1 ポートへの通信

 **「コマンドリファレンス」 / 「スイッチング」**

- Jumbo フレームを複数ポートから 1 ポートに対して同時に送信すると、受信した 1 ポートからフレームが転送されません。
- ポートグループ 1 ~ 12 とポートグループ 13 ~ 24 間の通信において、複数ポートから 1 ポートに対して同時にパケットを送信し、パケットロスが発生した場合、送信ポートによってパケットの損失率にばらつきがあります。

4.5 ポリシーベース QoS


 **「コマンドリファレンス」 / 「QoS」 / 「ポリシーベース QoS」**

コマンドリファレンスの「QoS」 / 「ポリシーベース QoS」 / 「送信優先度の設定」の説明において、以下の注意書きがありますが、バージョン 2.5.12J で、ルーティング後のパケットも正

しいプライオリティーで扱われるようになりました。バージョン 2.5.12J以降のファームウェアでは、この注意は必要ありませんので、訂正してお詫びいたします。

Note - ルーティング後のパケットは常にユーザープライオリティー 7 で扱われます (L2 スイッチングされたパケットはユーザープライオリティー 0 で扱われます)。このため、意図的にプライオリティー 7 に設定されたパケットとルーティング後のパケットが同一プライオリティーで扱われることとなります。優先させたいパケットがある場合、優先させたくない (優先度の低い) パケットに対してプライオリティーを下げる設定を行うようにしてください。

4.6 ポート認証

 「コマンドリファレンス」 / 「スイッチング」 / 「ポート認証」

- ポート認証が有効で、SET RADIUSERVER コマンドの DEADTIME パラメーターが 0 (ゼロ=デフォルト) のとき、RADIUS サーバーを 3 台登録し、本製品からの Access-Request に対して 3 台とも応答がないと、全サーバーに対して同時に Access-Request パケットが再送されます。
- ポート認証が有効で、SET RADIUSERVER コマンドの DEADTIME パラメーターが 0 (ゼロ=デフォルト) のとき、優先順位 3 のサーバーでのみ認証が行われた場合、認証のたびに 3 台のサーバーに対して Access-Request パケットが送信されます。また、優先順位 2 のサーバーでのみ認証が行われた場合は、優先順位 1 と 2 のサーバーに対して Access-Request パケットが送信されます。

4.7 DNS リレー

 「コマンドリファレンス」 / 「IP」 / 「DNS リレー」

本製品の DNS リレーは Web 認証の HTTP リダイレクト機能用として実装しています。DNS キャッシュを持っていないため、大量の DNS query を処理する性能はありません。

5 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。

```
MENU
SET SWITCH CONSOLEMODE
SET AUTHENTICATION METHOD=TACACS
ADD/DELETE TACACS SERVER
ENABLE/DISABLE/SET/SHOW HTTP SERVER

SET SWITCH PORT
[BACKPRESSURE={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}]
[BPLIMIT={1..7935}] [FCTRLLIMIT={1..7935}]

SET PORTAUTH PORT/SET PORTACCESS PORT
[FORCERENEWING={ENABLED|DISABLED}]
SET PORTAUTH IDTOGGLE

SET SWITCH PORT SECURITYMODE=PACONTROL
CREATE/DESTROY/ADD/DELETE/SET/SHOW LACP
ENABLE/DISABLE/SET/SHOW/PURGE GARP
SET VLAN={vlanname|1..4094} [TYPE=PORTBASED]
PURGE/SHOW PKI
SET PKI CERTSTORELIMIT
SET/SHOW SSL

SHOW IP ROUTE FDB

SET BOOTP RELAY MAXHOPS

ADD SWITCH FDB [MODE={LOCKED|STATIC}]
ADD SWITCH FILTER [MODE={LOCKED|STATIC}]
```

6 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 9424T/SP-E コマンドリファレンス 2.5 (613-000699 Rev.E)」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「613-000699 Rev.E」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/>