J613-M0109-11 Rev.L 090410

Allied Telesis

CentreCOM® 9424T/SP　リリースノート

この度は、CentreCOM 9424T/SP 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　2.3.3J

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 2.3.2J から 2.3.3J 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 9424T/SP コマンドリファレンス 2.3（J613-M0109-12 Rev.G）」をご覧ください。

2.1　マネージメントアクセスコントロールのポート指定

参照「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」

マネージメントアクセスコントロールリストの条件に、本製品へのアクセスを許可するポートを指定できるようになりました。
CREATE MGMTACL コマンドの PORTLIST パラメーターで指定します。

2.2　例外発生ログの保存と表示

参照「コマンドリファレンス」/「運用・管理」/「システム」

クラッシュによるリブートが発生した場合に、ログが NVS に保存されるようになりました。
ログを表示するには SHOW EXCEPTIONLOG コマンド、削除するには DELETE EXCEPTIONLOG コマンドを使用します。

2.3　CPU およびメモリー使用率の表示

参照「コマンドリファレンス」/「運用・管理」/「システム」

CPU およびメモリーの使用率を表示できるようになりました。
CPU 使用率は SHOW CPU コマンドで表示します。過去 1 秒間、20 秒間、60 秒間の CPU 平均使用率をパーセンテージ（%）で表します。HISTORY オプションを指定すると、過去 60 秒間、1 時間、30 時間の CPU 使用率の履歴がグラフ形式で表示されます。また、CPU 使用率は SNMP 経由でも取得可能です。
メモリーの使用率は SHOW BUFFER コマンドで表示します。

2.4　SHOW DEBUG コマンドの追加

参照「コマンドリファレンス」/「運用・管理」/「システム」

デバッグ情報を表示するための SHOW DEBUG コマンドが追加されました。SHOW CONFIG コマンドの INFO オプション指定時と同義のコマンドです。

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものです。ご使用に際しては、弊社技術担当にご相談ください。

2.5 ユーザー認証機能の拡張

参照 「コマンドリファレンス」/「運用・管理」/「ユーザー管理」

ユーザー認証機能を以下のとおり拡張しました。

○ **ユーザーアカウントの追加・削除**
デフォルトアカウント（manager、operator）以外に最大 16 個のユーザーアカウントが作成可能になりました。ユーザーアカウントの追加・削除は、ADD USER/DELETE USER コマンドで行います。なお、デフォルトアカウントを削除することはできません。

○ **ユーザーアカウントの有効化・無効化**
指定したユーザーアカウントの有効化・無効化を設定できます。ENABLE USER/DISABLE USER コマンドを使います。

○ **セッションタイプの指定**
ユーザーごとに、ログインする際の接続方法（セッションタイプ）をコンソール、Telnet、SSH、エンハンストスタッキングのいずれかに限定することができます（複数指定も可能）。ADD USER/SET USER コマンドの SESSIONTYPE パラメーターで指定します。

○ **ロックアウトまでのログイン失敗回数とロックアウト期間の設定**
SET USERCONFIG コマンドの LOGINFAIL パラメーターでロックアウトまでの連続したログイン失敗回数、LOCKOUTPD パラメーターでロックが解除されるまでの時間（秒）を設定できます。デフォルトはログイン失敗回数が 5 回、ロックアウト期間が 600 秒です。

○ **パスワードの最小文字数設定**
SET USERCONFIG コマンドの MINPWDLEN パラメーターでパスワードの最小文字数を変更できます。デフォルトは 6 文字です。

2.6 HTTP クライアント機能

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」

HTTP クライアント機能に対応し、HTTP によるファイルのダウンロードが可能になりました。
LOAD コマンドで METHOD パラメーターに HTTP を指定します（WEB、WWW も指定可）。HTTP サーバーのポート番号（SERVERPORT）、プロキシー経由で使用する場合にプロキシーサーバーの IP アドレス（HTTPPROXY）とポート番号（PROXYPORT）、HTTP で認証が必要な場合にユーザー名（USERNAME）とパスワード（PASSWORD）の設定も可能です。

2.7 インターフェースの一覧表示と統計カウンター表示

参照 「コマンドリファレンス」/「運用・管理」/「SNMP」

SHOW INTERFACE コマンドが以下のとおり拡張および仕様変更されました。

○ **インターフェース無指定時**
インターフェースの指定を省略した場合は、すべてのインターフェースに関する情報が簡潔に一覧で表示されるようになりました。

○ インターフェース指定時
インターフェースを指定した場合は、従来のインターフェース情報に加え、統計カウンターが表示されるようになりました。

○ COUNTER オプション指定時
新たに COUNTER オプションが追加され、指定したインターフェースまたはすべてのインターフェースの統計カウンターのみを表示できるようになりました。

2.8 10/100Mbps の通信モード追加

参照「コマンドリファレンス」/「スイッチング」/「ポート」

SET SWITCH PORT コマンドに 10MHAUTO、10MFAUTO、100MHAUTO、100MFAUTO パラメーターが追加されました。
オートネゴシエーション有効の状態で通信速度を固定させるモードで、それぞれ以下のビットが通知されます。

10MHAUTO：10M Half
10MFAUTO：10M Full/Half
100MHAUTO：10M Full/Half, 100M Half
100MFAUTO：10M Full/Half, 100M Full/Half

2.9 ポートステータスと統計カウンターの一覧表示

参照「コマンドリファレンス」/「スイッチング」/「ポート」

SHOW SWITCH PORT コマンドに SUMMARY オプションが追加され、ポートステータスが簡潔に一覧で表示されるようになりました。
また、SHOW SWITCH PORT コマンドの COUNTER オプションに SUMMARY の選択肢が追加され、統計カウンターを簡潔に一覧で表示できるようになりました。従来の詳細な統計カウンターを表示する場合は、COUNTER オプションに DETAIL を指定します。

2.10 クラシファイア：MAC アドレスの範囲指定によるフィルタリング

参照「コマンドリファレンス」/「クラシファイア」

クラシファイアの条件パラメーターに MACDMASK/MACSMASK が追加され、MAC アドレスの範囲指定が可能になりました。
CREATE CLASSIFIER コマンドの MACDMASK（宛先 MAC アドレスに対するマスク）、MACSMASK（送信元 MAC アドレスに対するマスク）パラメーターで指定します。

2.11 ハードウェアパケットフィルターの新動作モード（エンハンスモード）

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に従来とは異なる処理フローを持つ新たな動作モード（エンハンスモード）が追加されました。従来の動作モード（レガシーモード）では、許可（permit）のアクションが指定されているエントリーから順に処理が行われていましたが、エンハンスモードではエントリー ID 番号の小さい順に処理が行われます。

これにより、マスク長の異なるサブネット単位でのフィルター制御や、条件 A にマッチする通信は許可しながら、条件 A ＋ B は破棄したいといったマッチ条件の一部が重なるケースなど、レガシーモードでは実現が難しかったフィルター設定が可能になりました。

レガシーモードとエンハンスモードの切り替えは、ENABLE ACL LEGACYMODE/DISABLE ACL LEGACYMODE コマンドで行います。デフォルトは ENABLE ACL LEGACYMODE で、ファームウェアバージョン 2.3.3J へのバージョンアップ後は、レガシーモードで動作します。バージョン 2.3.2J 以前のファームウェアでハードウェアパケットフィルターを設定している場合は、エンハンスモードへの切り替え後に設定をしなおすようにしてください。設定はそれぞれの動作モードにあわせて行う必要があります。

エンハンスモードについての詳細は、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」をご覧ください。

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 2.3.2J から 2.3.3J 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。各機能の詳細については、「CentreCOM 9424T/SP コマンドリファレンス 2.3（J613-M0109-12 Rev.G）」をご覧ください。

3.1　802.1X 認証とスパニングツリープロトコルの併用

802.1X 認証とスパニングツリープロトコルが併用できるようになりました（Authenticator ポートをスパニングツリーポートに設定できるようになりました）。

3.2　Ping：応答時間の表示変更

参照 **「コマンドリファレンス」/「IP」**

PING コマンド実行時、応答時間の表示が以下のとおり仕様変更されました。

変更前：
実際の値＝ 0 ～ 9ms　画面表示＝ 0 ms
実際の値＝ 10 ～ 19ms　画面表示＝ 1 ms
実際の値＝ 20 ～ 29ms　画面表示＝ 2 ms

変更後：
実際の値＝ 0 ～ 9ms　画面表示＝ ＜ 10 ms
実際の値＝ 10 ～ 19ms　画面表示＝＜ 20 ms
実際の値＝ 20 ～ 29ms　画面表示＝＜ 30 ms

本製品の仕様上、応答時間は 10ms 単位での表示になります。

3.3　ARP エントリー数の拡張

参照 **「コマンドリファレンス」/「IP」/「ARP」**

ARP エントリーの登録数が 10 個から 2048 個に拡張されました。

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 2.3.2J から 2.3.3J 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　設定ファイルを本製品からコンピューターに転送すると、機能ごとに異なる改行コードが付加されていましたが、CR+LF に統一しました。

4.2 SHOW CONFIG コマンドにDYNAMIC オプションを指定して設定ファイルを表示したときに、CREATE QOS POLICY コマンドの EGRESSPORT パラメーターに不要なスペースが入っていましたが、これを修正しました。

4.3 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したが、これを修正しました。

4.4 本製品から送出される Accounting-Interim-Update パケットにAcct-Session-Id 属性が含まれていませんでしたが、これを修正しました。

4.5 ファイルサイズが 45Byte 以下のファイルを 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したが、これを修正しました。

4.6 XMODEM によるファイル転送中に、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。

4.7 転送可能なファイルサイズの上限値・下限値が TFTP と XMODEM で異なっていましたが、上限 4,096,000Byte、下限 0（ゼロ）Byte に統一しました。

4.8 Land Attack 検出機能設定時、不正パケット検出の際に SNMP トラップが送出されませんでしたが、これを修正しました。

4.9 Ping of Death Attack 検出機能設定時、不正パケット検出の際に CLI へのメッセージ表示、SNMP トラップの送出が行われていませんでしたが、これを修正しました。

4.10 ポート 24 で攻撃検出機能が動作していませんでしたが、これを修正しました。

4.11 Ping of Death Attack 検出機能で不正パケットのミラーリングを設定した場合、ミラーポートとして設定されたポートではないポートにもパケットがミラーリングされていましたが、これを修正しました。

4.12 ログ機能が Disabled（無効）の状態で PURGE LOG コマンドを実行するとログ機能が Enabled（有効）になっていましたが、これを修正しました。

4.13 SAVE LOG コマンドで保存されたログファイルを、SHOW FILE コマンドで表示すると、最後の行にエラーメッセージが表示されていましたが、表示されないように修正しました。

4.14 SNMPv3 における認証回避の脆弱性を修正しました。

4.15 ポートがリンクダウンした状態で所属するトランクグループを削除すると、トランクグループ内で最も番号の小さいポート以外のポートがリンクアップしても通信ができませんでしたが、これを修正しました。

4.16 ポートがリンクアップした状態で所属するトランクグループを削除すると、ポート 1 を接続しない限り、トランクポートだったポートで通信ができませんでしたが、これを修正しました。

4.17 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ーが有効なポートで、本製品の IP アドレス宛ての ARP Request を受信すると、ARP Reply がフラッディングされていましたが、これを修正しました。

4.18 ポートセキュリティーの LIMITED モードで、不正アクセス時のアクションとして SNMP トラップを送信する設定をしても、トラップが送信されませんでしたが、これを修正しました。

4.19 Protected Ports VLAN の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でしたが、エラーではじかれるように修正しました。

4.20 Rapid STP 有効時、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 が消去されていましたが、これを修正しました。

4.21 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でしたが、これを修正しました。

4.22 ハードウェアパケットフィルターにおいて、エントリーを複数作成する場合に、アクションに許可（permit）が指定されているエントリーが最後（最も大きい番号）になるように設定する必要がありましたが、新動作モード（エンハンスモード）においてこの制限は解除されました。

4.23 ハードウェアパケットフィルターにおいて、アクションに許可（permit）を指定したエントリーに、アクションを破棄（deny）に指定したエントリーよりも大きなエントリー番号を設定しても、許可（permit）を指定したエントリーが正しく処理されない場合がありましたが、新動作モード（エンハンスモード）においてこの制限は解除されました。

4.24 802.1X 認証の Single-Supplicant モードで Supplicant が登録されると、EAP-Request パケットの宛先が条件によって異なっていましたが、常にマルチキャストで送信されるように修正しました。

4.25 802.1X 認証の Single-Supplicant モードで Supplicant が登録されると、EAP-Failure パケットがユニキャストで送信されていましたが、マルチキャストで送信されるように修正しました。

4.26 EAP-Request パケットの再送信回数が最大値を越えると EAP-Failure パケットが送信されますが、802.1X 認証の Single-Supplicant モード時には、最後の EAP-Request パケット送信直後に EAP-Failure が送信されていたため、これを修正しました。

4.27 802.1X 認証において、RADIUS サーバーからの応答がなくタイムアウトが発生した場合に、本製品から EAP-Failure パケットが 2 個分送信されていましたが、これを修正しました。

4.28 本製品がサポートする Supplicant の最大数はシステムあたり 480 ですが、481 以上の Supplicant の認証が可能だったため、これを修正しました。

4.29 本製品が 802.1X 認証の Authenticator のとき、ユーザー名の文字数が 19 文字以上で、かつ 4 の倍数 -1（19, 23, 27 文字など）に設定されている Supplicant を認証すると、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。

4.30 MAC ベース認証使用時、認証直後の Supplicant の無通信期間が FDB のエージングタイムより短いにもかかわらず、Supplicant の MAC アドレスがエージングにより FDB から削除され、認証許可状態が解除されていましたが、これを修正しました。

4.31 IP インターフェース作成時または本製品起動時（設定ファイル読み込み時）に、配下のポートがすべてリンクダウンしているにもかかわらず、IP インターフェースはアップした状態になっていましたが、これを修正しました。

4.32 IGMP と MLD のグループが登録されている状態で、IGMP グループ宛てのマルチキャストパケットを受信すると、MLD のルーターポートにも転送されていましたが、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 **2.3.3J** には、以下の制限事項があります。

5.1 ファームウェアバージョン 2.3.2J リリースノートの訂正

ファームウェアバージョン 2.3.2J のリリースノートに掲載しました下記項目ですが、その後の調査によって、本製品では発生しないことが判明したため、制限事項から削除しました。

- ○ 3.13 ポートトランキング
- ○ 3.20 ポート認証の 5 番目
- ○ 3.21 ARP

5.2 MSTP とポートトランキングの併用

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

5.3 ポート認証と攻撃検出機能の併用

ポート認証と攻撃検出機能は併用できません。

5.4 IGMP Snooping とポートセキュリティーの併用

IGMP Snooping とポートセキュリティーは併用できません。

5.5 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。

5.6 バーチャル LAN

参照「コマンドリファレンス」/「バーチャル LAN」

ゲスト VLAN を設定している VLAN に、DESTROY VLAN コマンドを実行すると、VLAN が削除されてしまいます。

5.7 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。

5.8 ラピ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。

5.9 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。

5.10 QoS

参照「コマンドリファレンス」/「QoS」/「QoS」

SET QOS SCHEDULING コマンドに WRR（ラウンドロビン）、WEIGHTS パラメーターの Q7 に 0（ゼロ）を指定して、キュー 7 が最優先（STRICT）になる設定をした場合、ユーザープライオリティー値 7 を持つフラッディングパケットが最優先で転送されません。

5.11 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」

○ レガシーモードでは、エントリーを複数作成する場合に、アクションに許可（permit）が指定されているエントリーが最後（最も大きい番号）になるように設定する必要がありますが、新動作モード（エンハンスモード）ではこの制限は解除されます。

○ レガシーモードでは、アクションに許可（permit）を指定したエントリーに、アクションを破棄（deny）に指定したエントリーよりも大きなエントリー番号を設定しても、許可（permit）を指定したエントリーが正しく処理されない場合がありますが、新動作モード（エンハンスモード）ではこの制限は解除されます。

5.12 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。

○ ポートを Authenticator ポートに設定すると、設定ファイルにイーグレスフィルタリングを有効にする設定が自動的に書き込まれますが、ポート認証を無効に設定しても、イーグレスフィルタリング有効の設定が解除されません。

○ ポートを 802.1X Authenticator ポートに設定すると、設定ファイルに「set switch port=xx securitymode=pacontrol」という設定（未サポートのセキュリティーモード設定）が自動的に書き込まれます。

○ ポートがリンクダウンしているときに、SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの CONTROL パラメーターを設定変更できません。

○ 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）コマンドでサプリカント数が正しく表示されない場合があります。

○ 802.1X Authenticator ポートまたは MAC ベース認証ポートに、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。

○ ポート認証使用時、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ポートに（Authenticator ポートをリンクダウンさせずに）移動することはできません。

○ ポートに対して、最初に Supplicant/Authenticator ポートの設定を行い、次にVLAN の設定（タグなしポートとして設定）を行うと、エラーで VLAN の設定ができません。また、本製品の仕様では、Supplicant/Authenticator ポートをタグ付きに設定することはできませんが、上記手順でタグ付きの設定を行っても、エラーになりません。Supplicant/Authenticator ポートの設定を行う場合は、最初に VLAN の設定を行うようにしてください。

○ MAC アドレスベース認証では、Supplicant のMAC アドレスがエージングによりFDB から削除されると、認証許可状態が解除されます。

○ 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。

○ Authenticator ポートにゲスト VLAN を設定している状態で、DISABLE PORTAUTH コマンドを実行しても、ゲスト VLAN に割り当てられてしまいます。

5.13 ARP

参照「コマンドリファレンス」/「IP」/「ARP」

始点 IP アドレスが 0.0.0.0 の ARP パケット受信時に、誤った内容が ARP キャッシュに登録されることがあります。

5.14 IPv6 マルチキャスト

参照「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。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 コマンドリファレンス 2.3（J613-M0109-12 Rev.G)」の補足事項です。

5.15 ファームウェアバージョン 2.3.2J リリースノートの訂正

ファームウェアバージョン 2.3.2Jのリリースノートに掲載しました「4.15　バーチャル LAN」ですが、その後の調査によって、本製品では発生しないことが判明したため、コマンドリファレンスの補足から削除しました。

5.16 エンハンストスタッキング

参照「コマンドリファレンス」/「運用・管理」/「エンハンストスタッキング」

○ マスタースイッチからスレーブスイッチに SNMP 経由でエンハンストスタッキング接続している最中に、他のスイッチから該当のマスタースイッチに Telnet や SNMP による接続を行わないでください。

○ エンハンストスタッキングを使用する場合、マスタースイッチとスレーブスイッチを接続するには、下記のとおりに接続してください。

- スレーブスイッチ側は、Default_VLAN に所属するポートにマスタースイッチを接続してください。Default_VLAN 以外の VLAN に所属するポートに接続した場合は、IP インターフェースを作成して IP アドレスを設定しなければなりません。
- マスタースイッチ側は、ローカルインターフェースに設定した VLAN に所属するポートにスレーブスイッチを接続してください。

5.17 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。

5.18 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」

○ ADD RADIUSSERVER コマンドで認証サーバーリストに追加された RADIUS サーバーと本製品が接続された状態で、ENABLE AUTHENTICATION コマンドにより認証が有効の場合は、RADIUS サーバーに登録したログイン名 / パスワードでしか本製品にログインすることができません。

本製品に設定されているユーザー名 / パスワードでログインする場合は、ENABLE AUTHENTICATION コマンドを実行しないでください。

○ ユーザー認証において、本製品から送信される Access-Request パケットの再送回数は 3 回が仕様ですが、2 回しか送信されません。

5.19 SNMP

参照 **「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。

○ ブリッジ MIB の dot1dStpPort Table 内の dot1dStpPortEnable を変更しても設定は変更されません。本製品では、ポート単位でスパニングツリープロトコルの有効 / 無効を変更することはできません。

○ SNMP マネージャーからシステム名を設定した場合、ログアウト / ログイン後にシステム名がプロンプトに反映されます。

5.20 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」**

○ リンクダウンをとも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。

○ 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。

○ 予約マルチキャストアドレスを、FDB にスタティックエントリーとして登録することはできません。

5.21 複数ポートから 1 ポートへの通信

参照 **「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。

5.22 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」**

トランキンググループの最若番ポートを抜き差しすると、接続の組み合わせによって、ポートのリンクアップトラップが生成されない場合があります。

5.23 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」/「ポート」

ポートミラーリング機能が有効の場合、「01:80:C2:00:00:00」などの予約マルチキャストアドレスをソースポートで受信すると、ミラーポートからパケットが重複して送信されます。

5.24 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」

○ 複数の Protected Ports VLAN が存在し（例えば VLAN10 と VLAN20 が存在するような場合）、アップリンクポートの一部を共有している場合、VLAN10 のクライアントから VLAN20 宛てにパケットを送信すると、VLAN20 のアップリンクポートだけでなくクライアントポートにも送信されます。

○ SET SWITCH MULTICASTMODE コマンドで B（BPDU/EAP パケットを、VLAN を超えて、すべてのポートに転送する）が設定されていると、マルチプル VLAN（Protected Ports VLAN）のグループを超えて BPDU/EAP パケットが同一 VLAN 内にフラッディングされます。

5.25 ラピ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」

○ ラピッドスパニングツリープロトコルを有効にし、トランクグループに所属したポートがリンクアップすると、そのポートの通信速度の設定に関係なく、ポートプライオリティーが 64、パスコストが 2000 に設定されます。

○ ACTIVATE STP/MSTP コマンドを実行すると、設定ファイルに保存されますが、ACTIVATE RSTP コマンドを実行しても、設定ファイルには保存されません。

5.26 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」

○ CREATE QOS TRAFFICCLASS コマンドの MAXBANDWIDTH パラメーターに 0（ゼロ）を指定すると、帯域ゼロのトラフィッククラスが作成されますが、このトラフィッククラスが割り当てられた QoS ポリシー作成直後の一定量の通信、および本製品再起動直後の一定量の通信に限り、該当ポートからのトラフィックがフィルターされません（帯域ゼロになりません）。

○ 出力ポートに QoS ポリシーを関連づけた場合、フィルターの対象となるのは学習済みのユニキャストアドレス宛てのトラフィックのみです。未学習のユニキャスト / マルチキャストアドレス、およびブロードキャスト宛てのトラフィックは対象になりません。また、学習済みのマルチキャストアドレス宛てのトラフィックも対象になりません。

5.27 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」

○ ポート認証が有効のとき、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。

○ RADIUS サーバーへの通信不可および RADIUS サーバーからの応答が遅延したときに、Access-Request パケットの再送が行われません。

5.28 MLD Snooping

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD Snooping」

マルチキャストルーターが接続されるポートが存在しない状態で、Multicast Listener Report を受信すると、すべてのポートに転送されます。
SET IPV6 MLDSNOOPING コマンドの ROUTERPORT パラメーターでポートを設定すれば転送されません。

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 SYSTEM DISTINGUISHEDNAME
MENU
SET SWITCH CONSOLEMODE
SET AUTHENTICATION METHOD=TACACS
ADD/DELETE TACACS SERVER
SET SWITCH PORT
[BACKPRESSURE={YES¦NO¦ON¦OFF¦TRUE¦FALSE¦ENABLED¦DISABLED}]
[BPLIMIT={1..7935}][FCTRLLIMIT={1..7935}]
SET SWITCH PORT SECURITYMODE=PACONTROL
CREATE/DESTROY/ADD/DELETE/SET/SHOW LACP
ADD SWITCH FDB MODE=LOCKED
ADD SWITCH FILTER MODE=LOCKED
ENABLE/DISABLE/SET/SHOW PURGE GARP
SET VLAN={vlanname¦1..4049}[TYPE=PORTBASED]
CREATE/ADD/DELETE/SET/SHOW/PURGE PKI
SET/SHOW SSL

7 コマンドリファレンスについて

最新の取扱説明書「CentreCOM 9424T/SP、9408LC/SP 取扱説明書（J613-M0109-10 Rev.C）」およびコマンドリファレンス「CentreCOM 9424T/SP コマンドリファレンス 2.3（J613-M0109-12 Rev.G）」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、上記のマニュアルに対応した内容になっていますので、お手持ちのマニュアル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。

コマンドリファレンスのパーツナンバー「J613-M0109-12 Rev.G」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/