613-000710 Rev.L 090226



Allied Telesis

# 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　2.5.1J

## 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 2.4.1J から2.5.1J 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-E コマンドリファレンス 2.5（613-000699 Rev.D）」をご覧ください。

### 2.1　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。

### 2.2　RADIUS Access-Request の始点 IP アドレス設定

参照「コマンドリファレンス」/「運用・管理」/「認証サーバー」

Access-Request パケットの始点IP アドレスとなるインターフェースを設定できるようになりました。ADD RADIUSSERVER コマンドのLOCAL パラメーターでインターフェースを指定します。指定しない場合は、パケットを送出したインターフェースの IP アドレスがセットされます。

### 2.3　RADIUS サーバーとの通信に関するパラメーター設定コマンド追加

参照「コマンドリファレンス」/「運用・管理」/「認証サーバー」

RADIUS サーバーとの通信に関するパラメーター（応答待ち時間、再送回数など）が設定できるようになりました。
設定は、SET RADIUSSERVER コマンドの TIMEOUT、DEADTIME、RETRANSMITCOUNT パラメーターで行います。

### 2.4　検疫ソリューション対応

マイクロソフト社「Windows Server 2008」標準の NAP（ネットワークアクセス保護）、シマンテック社の NAC（Network Access Control）に対応しました。
本対応はポート認証のマルチプルダイナミック VLAN（VLANASSIGNMENTTYPE=USER 設定時）において有効です。

## 2.5 SET SWITCH MULTICASTMODE コマンドのパラメーター追加

参照「コマンドリファレンス」/「スイッチング」

SET SWITCH MULTICASTMODE コマンドに「E」が追加され、EAP パケットがタグ付きポートからはタグ付きで、タグなしポートからはタグなしでフラッディングされる設定ができるようになりました。
BPDU パケットについては、「E」は「D」と同じ動作で、タグ付きポートからもタグなしでフラッディングされます。

## 2.6 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

## 2.7 Web 認証の機能拡張

参照「コマンドリファレンス」/「スイッチング」/「ポート認証」

Web 認証機能を以下のとおり拡張しました。

○ HTTP リダイレクト
Web 認証ポートにおいて、受信したHTTP リクエストをWeb 認証サーバーの IP アドレスにリダイレクトする HTTP リダイレクト機能に対応しました。
機能の有効化・無効化は、SET WEBAUTHSERVER コマンドの HTTPREDIRECT パラメーターで行います。デフォルトは無効です。

○ セッションキープ
HTTP リダイレクト機能有効時にリダイレクト前の URL を記憶しておき、Web 認証成功後に記憶しておいた URL にリダイレクトさせるセッションキープ機能に対応しました。
機能の有効化・無効化は、SET WEBAUTHSERVER コマンドの SESSIONKEEP パラメーターで行います。デフォルトは無効です。

○ プロキシーサーバー対応
プロキシーサーバー使用環境に Web 認証を導入するための設定項目が追加されました。
SET WEBAUTHSERVER コマンドの PROXYSERVER パラメーターで本製品が生成する PAC ファイルに記述されるプロキシーサーバーの IP アドレス、PROXYPORT パラメーターでプロキシーサーバーのポート番号を指定します。
HTTP リダイレクト機能と同時に設定することで、プロキシーサーバーへのアクセスもリダイレクトすることができます。

詳細は、コマンドリファレンス「ポート認証」をご覧ください。

### 2.8 DNS リレー

参照「コマンドリファレンス」/「IP」/「DNS リレー」

本製品に対する DNS リクエストを、実際のDNS サーバーにリレーする DNS リレー機能に対応しました。詳細は、コマンドリファレンス「DNS リレー」をご覧ください。
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。

### 2.9 DHCP/BOOTP リレーの機能拡張

参照「コマンドリファレンス」/「IP」/「DHCP/BOOTP リレー」

DHCP/BOOTP リレー関連コマンドにINTERFACE パラメーターが追加され、IP インターフェース単位で機能の有効化・無効化および転送先の IP アドレスを設定できるようになりました（転送先の IP アドレスは 1 個のインターフェースにつき最大 8 個まで設定可能）。

これにともない、DHCP サーバー機能と DHCP/BOOTP リレー機能の併用が可能になりました。DHCP サーバー機能はシステム単位、DHCP/BOOTP リレー機能はインターフェース単位で設定を行います。DHCP パケットの受信インターフェースで DHCP/BOOTP リレー機能が有効であれば DHCP/BOOTP リレーが動作し、無効でかつ DHCP サーバー機能が有効であれば DHCP サーバーが動作します。

## 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 2.4.1J から2.5.1J 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-E コマンドリファレンス 2.5（613-000699 Rev.D）」をご覧ください。

### 3.1 ポート認証とタグ VLANの併用

同一ポートでポート認証とタグ VLAN を併用できるようになりました（Authenticator ポートをタグ付きに設定できるようになりました）。802.1X/MACアドレスベース /Web 認証すべての認証方式で併用が可能です。
ただし、Authenticator ポートをタグ付きに設定する場合、ダイナミック VLAN、ゲスト VLAN を併用することはできません。
また、Supplicant ポートをタグ付きに設定することはできません。

### 3.2 Web 認証と DHCP/BOOTP リレーの併用

Web 認証ポートにおいて、未認証 Supplicant（DHCP/BOOTP クライアント）に対してもリレー機能が使用できるようになりました。

### 3.3 802.1X 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）。

## 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 2.4.1J から2.5.1J 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　SHOW PORT=X（X はポート番号）という存在しないコマンドを実行した場合に、エラーではじかれるよう修正しました。

4.4　RADIUS サーバー 2 台登録時、優先順位 1 のサーバーから応答がなく、優先順位 2 のサーバーに Access-Request パケットを送信したときに、優先順位 2 のサーバーから Access-Challenge パケットを受信すると、再び優先順位 1 のサーバーにAccess-Request パケットを送信していましたが、これを修正しました。

4.5　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。

4.6　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 回が仕様でしたが、2 回しか送信されていませんでしたので、これを修正しました。なお、ファームウェアバージョン 2.5.1J で、SET RADIUSSERVER コマンドが追加され、RETRANSMITCOUNT パラメーターで再送回数を設定変更できるようになりました。

4.7　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。

4.8　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。

4.9　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。

4.10 攻撃検出機能設定時、Land Attack の不正パケットを受信すると、本来表示されるべきでないデバッグメッセージが表示されることがありましたが、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 SNMPv3 における認証回避の脆弱性を修正しました。

**4.14** SET SWITCH PORT コマンドの COMBO パラメーターで設定した内容を SHOW SWITCH PORT コマンドで確認することができませんでしたが、これを修正しました。

**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** 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。

**4.18** 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。

**4.19** 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。

**4.20** ポートを 802.1X 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、802.1X 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なかったため、これを修正しました。

**4.21** 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ていましたが、書き込まれないように修正しました。

**4.22** SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの SERVERTIMEOUT/SERVTIMEOUT パラメーターに 31（秒）以上の値を指定すると、タイムアウト値が 60（秒）で動作していましたが、設定値どおりに動作するよう修正しました。

**4.23** 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でしたが、これを修正しました。

**4.24** 本製品の仕様では、先に認証ポートとして設定されたポートに対して VLAN の設定変更はできませんが、タグ付きポートにする設定ができていましたので、エラーで設定できないように修正しました。

**4.25** 1 つのポートに対して MAC アドレスベース認証と Web 認証を設定しているとき、MAC アドレスベース認証中に Web 認証を行うと認証失敗となり、ログインページに戻りますが、ログインページに「Login Failed! Could not authenticate」のエラーメッセージが表示されなかったため、これを修正しました。

**4.26** RADIUS サーバーに送信される Access-Request パケットの始点IP アドレスに、パケットを送出したインターフェースの IP アドレスがセットされていましたが、ADD RADIUSSERVER コマンドの LOCAL パラメーターでインターフェースが設定できるようになりました。

**4.27** ポート認証において、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でしたが、これを修正しました。

**4.28** ポート認証使用時、ローカルインターフェース以外の IP インターフェース配下にある認証済みのポートから、ローカルインターフェースへの Telnet や SNMP による接続ができませんでしたが、これを修正しました。

**4.29** 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。

**4.30** 802.1X 認証の Single-Supplicant モードで Supplicant が登録されると、EAP-Request パケットが 1 パケットしか送信されませんでしたが、これを修正しました。

**4.31** RADIUS サーバーによって、マルチプルダイナミック VLAN を割り当てられた Supplicant が、新しい IP アドレスが付与されるまでの間、本来の VLAN の IP アドレスで、本製品で ARP 解決された IP アドレス宛てにルーティングできていましたが、これを修正しました。

**4.32** Web 認証サーバーの IP アドレスを設定していないと、認証成功前にもかかわらず、Supplicant から本製品経由でルーティングされるアドレスの外部 Web サーバーにアクセスが可能でしたが、これを修正しました。

**4.33** 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。

**4.34** 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。

**4.35** Web 認証サーバー機能有効時、認証ポートではないポートからHTTP パケットのソフトウェアルーティングができませんでしたが、これを修正しました。

**4.36** Web 認証において、いったん認証に成功した Supplicant から、ARP 解決がされていない異なるネットワークの外部 Web サーバー宛てにアクセスすると、認証画面が表示されていましたが、これを修正しました。

**4.37** 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。

**4.38** ダウンした状態の IP インターフェースを削除し、削除した IP インターフェースと同一の IP アドレスを持つ別の IP インターフェースを作成しようとすると、エラーで設定できませんでしたが、これを修正しました。

**4.39** 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。

**4.40** RIP 有効時、ポートのリンクダウンが発生すると、該当ネットワークでルーティングループが発生していましたが、これを修正しました。

**4.41** クラス標準でないサブネットマスクを持つ RIP インターフェースにおいて、サブネット化されたアドレス（10.10.0.0、172.16.10.0、192.168.1.128 など）の経路情報を受信した場合、受信インターフェースの IP アドレスやサブネットマスクを考慮せず、クラス A アドレスには 16 ビット、クラス B アドレスには 24 ビット、クラス C アドレスには 32 ビットのマスクを一律に適用した上で経路表に反映していましたが、これを修正しました。

**4.42** 宛先までの経路が 2 つ存在する RIP ネットワークにおいて、一方の経路がダウンしたときに、もう一方の経路に切り替わりませんでしたが、これを修正しました。

**4.43** 始点 IP アドレスが 0.0.0.0 の Gratuitous ARP パケット受信時に、ARP キャッシュに登録されるよう修正しました。

**4.44** 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。

**4.45** VRRP において、ポート 24 をタグ付きポートに設定し、所属 VLAN を監視対象インターフェースとして設定した場合、ポート 24 のリンクダウンにより監視対象インターフェースがダウンしても、バーチャルルーターの優先度が下がりませんでしたが、これを修正しました。

**4.46** DHCP サーバー機能使用時に本製品がクラッシュする場合がありましたが、これを修正しました。

以下の項目は、ファームウェアバージョン 2.4.1J のリリースノートに記載されていませんでしたが、実際には 2.4.1J で修正済みでした。

**4.47** Default_VLAN に IP アドレスを設定していない状態で、他の VLAN に IP アドレスを設定し IP インターフェースを作成すると、「Set Management VLAN failed」という不正なログが出力されていましたが、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 2.5.1J には、以下の制限事項があります。

## 5.1　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。

## 5.2　ポート認証（802.1X 認証 /MAC アドレスベース認証）と攻撃検出機能の併用

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

## 5.3　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。

## 5.4　マネージメントアクセスコントロール

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」

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。

## 5.5　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

## 5.6　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。

## 5.7　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。

## 5.8 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。

○ 本製品起動後最初に SNMP 要求を受信したインターフェースが、ローカルインターフェース以外のインターフェースの場合、応答パケットの始点アドレスにローカルインターフェースの IP アドレスではなく、要求パケットを受信したインターフェースの IP アドレスがセットされます。
ローカルインターフェース以外のインターフェースから応答パケットが送出されるため、利用する SNMP マネージャーによっては、監視ができない場合があります。

## 5.9 コンボポートのメディア選択設定

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。

## 5.10 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」/「ポート」

○ CREATE SWITCH TRUNK コマンドの SELECT パラメーターに MAC アドレスの選択基準（MACSRC、MACDEST、MACBOTH）が指定されていると、ルーティング後のパケットが負荷分散されずに送出されます。

○ 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。

## 5.11 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」

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ます。

## 5.12 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。

○ 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。

## 5.13 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。

## 5.14 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。

## 5.15 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。

## 5.16 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。

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。

## 5.17 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。

○ MAC アドレスベース認証と Web 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。

## 5.18 IP

参照「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。

## 5.19 ARP

参照「コマンドリファレンス」/「IP」/「ARP」

○ 異なるネットワークから本製品（CPU）宛ての通信を連続的に行うと、ARP が解決しているにもかかわらず、ARP Request が送信される場合があります。

○ 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。

## 5.20 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。

# 6　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.D）」の補足事項です。

## 6.1　ポート認証のマルチプルダイナミック VLANと Protected Ports VLAN の併用

ポート認証のマルチプルダイナミック VLAN（SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの VLANASSIGNMENTTYPE=USER による設定）と、Protected Ports VLAN は併用できません。

## 6.2　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。

○　SNMPv3 を使用して、エンハンストスタッキンググループのスレーブスイッチにアクセスすることはできません。

○　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。

## 6.3　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。

## 6.4　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。

## 6.5　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。

## 6.6 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」

○ 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。

○ 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。

○ 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。

## 6.7 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。

## 6.8 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。

## 6.9 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。

○ L3 スイッチングされるパケットは、ルーティング処理後にミラーポートに出力されます。

○ 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、L3 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、ミラーポートにはルーティング処理後のパケットが 1 個だけ出力されます。

## 6.10 バーチャル LAN

参照「コマンドリファレンス」/「バーチャル LAN」

MAC アドレス VLAN に MAC アドレスを追加したとき、別の VLAN から、MAC アドレス VLAN に追加した MAC アドレスを送信元 MAC アドレスとして持つ機器同士で双方向のユニキャスト通信を行うと、パケットが転送されてしまいます。

## 6.11 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。

## 6.12 MAC アドレス VLAN

参照「コマンドリファレンス」/「バーチャル LAN」

MAC アドレス VLAN で本製品宛ての通信、およびルーティングをさせることはできません。

## 6.13 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。

## 6.14 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。

## 6.15 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」

○ ポート認証が有効で、SET RADIUSSERVER 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 RADIUSSERVER 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。

### 6.16 PKI

参照 「コマンドリファレンス」/「スイッチング」/「PKI」

○ 証明書のシリアル番号が -2147483649 以下、2147483648 以上の場合、SHOW PKI CERTIFICATE コマンドで表示される Serial Number の項には、xx:xx:xx:xx... の形式で表示されます。

○ SET SYSTEM DISTINGUISHEDNAME コマンドで「/」を使用しないでください（「/」は未サポート）。「/」は設定ファイルで「,」に変換されます。

### 6.17 Ping

参照 「コマンドリファレンス」/「IP」

本製品から指定アドレスに対して Ping を実行したとき、応答時間が実際の値の 1/10 の値で画面上に表示されます。

例：
実際の値＝ 10 ～ 19 ms 画面表示＝ 1 ms
実際の値＝ 20 ～ 29 ms 画面表示＝ 2 ms

### 6.18 DNS リレー

参照 「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。

### 6.19 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。

## 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。

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}]

## 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 9424T/SP-E コマンドリファレンス 2.5（613-000699 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、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.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/**