613-002083 Rev.A 141219

Allied Telesis

CentreCOM® *x210*シリーズ リリースノート

この度は、CentreCOM x210 シリーズをお買いあげいただき、誠にありがとうございます。このリリースノートは、取扱説明書、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 5.4.4-2.3

2 重要：注意事項

2.1 AMF におけるファームウェアバージョンの混在について

参照「コマンドリファレンス」/「運用・管理」/「システム」

AMF メンバーとして x210/x200 シリーズを使用する場合、AMF マスターと x210/x200 のファームウェアバージョンは次表◎または○の組み合わせでご使用ください。

		x210/x200 シリーズ		
		5.4.4-0.x	5.4.4-1.x	5.4.4-2.x
AMF マスター	5.4.4-0.x	○	◎	◎
	5.4.4-1.x	×	◎	◎
	5.4.4-2.x	◎ ※	◎	◎

◎ = 利用可能（マスターにメンバープロダクト拡張ライセンスは不要です）
○ = 利用可能（マスターにメンバープロダクト拡張ライセンスが必要です）
× = 利用不可（x210/x200 シリーズが AMF ネットワークに参加できません）

※ AMF マスターが 5.4.4-2.x で x210/x200 シリーズが 5.4.4-0.x のとき、x210/x200 のオートリカバリーを実行すると x210/x200 のコンソールに「An AMF-ALL license must exist on the ATMF Master for this node's recovery」のようなログメッセージが出力されますが、これは表示上の問題でオートリカバリーの動作には影響ありません。

3 本バージョンで追加・拡張された機能

ファームウェアバージョン **5.4.4-1.1** から **5.4.4-2.3** へのバージョンアップにおいて、以下の機能が追加・拡張されました。

3.1 リンクフラッピング検出機能

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

リンクフラッピング検出機能（linkflap action コマンド）をサポートしました。本機能有効時は、特定のスイッチポートで 15 秒以内に 15 回以上リンクステータスが変動（ダウン→アップまたはアップ→ダウン）した場合、該当ポートを shutdown します。初期設定は無効です。

3.2 Web 認証の機能拡張・機能改善

参照「コマンドリファレンス」/「インターフェース」/「ポート認証」

○ Web 認証画面のカスタマイズ機能が下記のとおり拡張されました。詳細はコマンドリファレンスをご覧ください。

- 新しく追加された auth-web-server page xxxx コマンドを用いて、Web 認証関連ページのタイトル、サブタイトル、ウェルカムメッセージ、認証成功メッセージなどを変更できるようになりました（ただし日本語は使えません）。
- 外部 Web サーバー上に用意した任意のログインフォームを Web 認証画面として使用することができるようになりました。

なお、既存のカスタマイズ機能はバージョンアップ後もそのまま使用できます。

○ Web 認証と DHCP Snooping の併用が可能になりました。

○ これまで Web 認証では、ネットワーク構成によって認証成功画面が表示されなかったり、認証成功後ログオフするための画面にアクセスできなかったりするケースがありましたが、本バージョンでは Web 認証機能の設計を見直し、そのようなケースでも認証成功画面やログオフ画面の表示が可能となりました。

○ これまで Web 認証では、ネットワーク構成に応じて設定内容を細かく調整する必要がありましたが、本バージョンからは基本的に Web 認証機能を有効化するだけで、さまざまなネットワーク構成に対応できるようになりました。

なお、これにともない、設定コマンドの削除・変更が行われています。詳しくは仕様変更 4.1（p.3）をご覧ください。

○ Web 認証サーバーにおいて、HTTPS 標準である 443 番ポート以外への通信を Web 認証サーバーの HTTPS 待ち受けポートにリダイレクトできるようになりました。設定は、新しく追加された auth-web-server ssl intercept-port コマンドで行います。

○ Web 認証サーバーにおいて、HTTP と HTTPS を同時に有効化することができるようになりました。同時有効化の設定は、auth-web-server ssl コマンドに追加された hybrid オプションで行います。

○ Web 認証サーバーの HTTPS リダイレクト機能において、リダイレクト先 URL に含める Web 認証サーバーのホスト名を任意に設定できるようになりました。これにより、独自証明書を利用している環境において、HTTPS リダイレクト機能を経由したアクセス時にも Web ブラウザーの警告が出ないようにすることが可能となります。設定は、新しく追加された auth-web-server host-name コマンドで行います。

3.3 IGMP Snooping におけるルーターポート登録アドレスのカスタマイズ

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

IGMP Snooping において、制御用マルチキャストグループアドレス宛てパケットを受信したときの動作を変更できるようになりました。新しく追加された ip igmp snooping routermode、ip igmp snooping routermode address コマンドを使うことで、どのアドレス宛てのパケットを受信したときに該当ポートをルーターポート（すべてのマルチキャストパケットを出力するポート）にするかを任意に設定できます。

4　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 **5.4.4-1.1** から **5.4.4-2.3** 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。

4.1　Web 認証の仕様変更

参照 「コマンドリファレンス」/「インターフェース」/「ポート認証」

Web 認証機能に関して、下記の仕様変更を行いました。

○　Web 認証機能の機能改善 3.2（p.2）にともない、下記のコマンドが削除されました。

- auth-web-server mode
- auth-web-server http-redirect
- auth-web-server sslport
- auth-web-server blocking-mode
- auth-web-server gateway

旧バージョンで HTTPS を有効化し、auth-web-server sslport コマンドを使用していた場合、バージョンアップ後のランニングコンフィグでは、同じ意味を持つ auth-web-server port コマンドに自動変換されます（特に設定変更は不要です）。

また、それ以外のコマンドがスタートアップコンフィグから読み込まれた場合は単に無視されますが、Web 認証の機能改善により旧バージョンでこれらのコマンドを設定していたのと同等の動作を行いますので、旧バージョンで前記のコマンドを使用していた場合もコンフィグの変更は不要です。

○　Web 認証機能の機能改善 3.2（p.2）にともない、auth-web forward コマンドの初期設定が変更されました。また、A.B.C.D パラメーターと dns、udp パラメーターの併用がサポートされました。

[旧バージョン]
すべての受信・転送が無効。

[本バージョン]
ARP、DHCP、DNS の受信・転送が有効。

旧バージョンで Web 認証を使用しており、なおかつ、ARP、DHCP、DNS の受信・転送を有効にしていなかった場合、バージョンアップ後は ARP、DHCP、DNS の受信・転送が有効な状態になりますので、これが望ましくない場合は下記のコマンドを実行して不要なパケットの受信・転送を無効化してください。

- no auth-web forward arp
- no auth-web forward dhcp
- no auth-web forward dns

4.2　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」/「L2 スイッチング」/「フォワーディングデータベース」

FDB エントリーでパリティーエラーが発生した場合、復旧のため再起動を実施していましたが、該当する FDB エントリーだけを再登録するよう仕様変更しました。

5　本バージョンで修正された機能

ファームウェアバージョン **5.4.4-1.1** から **5.4.4-2.3** 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。

5.1　ミラーポートに設定していたポートのミラー設定を解除し、VLAN に所属させても、dot1qVlanStaticTable（1.3.6.1.2.1.17.7.1.4.3）にポート情報が表示されませんでしたが、これを修正しました。

5.2 同一 VLAN 内にタグ付きポートとタグなしポートが混在している環境では、dot1x eap コマンドの forward-vlan パラメーターがサポート対象外でしたが、本バージョンから使用できるようになりました。

5.3 DHCP を使用する環境で Web 認証を行う場合、認証済み Supplicant の認証情報が保持されている状態で、別の未認証 Supplicant に同じ IP アドレスが配布されると、未認証 Supplicant が認証を受けられませんでしたが、本バージョンからは認証後に端末の Gratuitous ARP を受信した認証情報内の IP アドレスを書き換えるようになったため、認証時に IP アドレスが重複することがなくなりました。

5.4 Web 認証サーバーにおいて、HTTP 待ち受けポートがひとつもない状態のとき（初期設定で no auth-web-server intercept-port 80 を実行した状態）に、show auth-web-server コマンドを実行すると関連プロセスが異常終了していましたが、これを修正しました。

5.5 802.1X 認証の認証処理中に、同じ Supplicant から EAPOL-Start を受信すると、認証に失敗したり、認証プロセス自体が異常終了することがありましたが、これを修正しました。

5.6 MLD Snooping 有効時、ルーターポートで MLD Report を受信した場合に、同ポートから該当 MLD Report を再送信することがありましたが、これを修正しました。

5.7 MLD Snooping 有効時、受信した MLD Report パケットを同一 VLAN 内にフラッディングすることがありましたが、これを修正しました。

5.8 AMF ノード名が重複すると AMF ネットワークが分断されることがありましたが、これを修正しました。

5.9 AMF ノード名が重複したときにどちらかのノード名を「host_xxxx_xxxx_xxxx」形式に強制変更する動作が正しく行われないことがありましたが、これを修正しました。

5.10 AMF クリーン状態のノードが自動検出メカニズムによって AMF ネットワークに参加した場合、このノードをワーキングセットから操作できないことがありましたが、これを修正しました。

下記の項目は、Web 認証機能の機能改善 3.2（p.2）、仕様変更 4.1（p.3）にともない、本バージョンでは適用外となりましたので、制限事項から除外いたしました。

5.11 Web 認証において、一度プロミスキャスモードに設定すると、その後インターセプトモードに変更しても、プロミスキャスモード設定時と同様に、動作します。インターセプトモードに設定を変更後、コンフィグを保存し、再起動した場合は、インターセプトモードとして動作します。

下記の項目は、Web 認証機能の制限事項 6.20「Web 認証とゲスト VLAN は併用できません」により本バージョンでは適用外となりましたので、制限事項から除外いたしました。

5.12 Web 認証とゲスト VLAN を併用する際には、ダイナミック VLAN を併用してください。

下記の項目は、ファームウェアバージョン **5.4.4-1.1** のリリースノートに制限事項として記載されていましたが、実際には **5.4.4-0.4** で修正されていました。

5.13 SFP ポートをホットスワップすると、他の SFP ポートがリンクダウン・リンクアップします。

6 本バージョンでの制限事項

ファームウェアバージョン **5.4.4-2.3** には、以下の制限事項があります。

6.1 システム

参照「コマンドリファレンス」/「運用・管理」/「システム」

○ システム起動時に下記のコンソールメッセージやログメッセージが出力されることがありますが、動作には影響ありません。

コンソールメッセージ
stop: Unable to stop job: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.
xx:xx:xx awplus init: getty (ttyS0) main process (XXXX) terminated with status 1

ログメッセージ
daemon.warning awplus init: network/getty_console (ttyS0) main process (XXXX) terminated with status 1

○ show ecofriendly コマンドの表示には、ecofriendly led コマンドの設定状態しか反映されません（筐体上の MODE LED 表示切替ボタンによるエコ LED 機能のオン・オフは反映されません）。

○ ドメインリストを設定する場合、最初にトップレベルドメインだけのものを設定すると、同一トップレベルドメインを持つ他のドメインリストを使用しません。その結果、ホスト名を指定した Ping に失敗することがあります。

○ ライセンスを無効化すると、不要なエラーメッセージがログに出力されます。ライセンス自体は正常に削除されます。

○ タイムゾーンの設定を変更したとき（clock timezone コマンド実行後）は、設定を保存しシステムを再起動してください。

6.2 コマンドラインインターフェース（CLI）

参照「コマンドリファレンス」/「運用・管理」/「コマンドラインインターフェース」

○ edit コマンドを使用すると、コンソールターミナルのサイズが自動で変更されてしまいます。

○ コマンドラインインターフェース（CLI）の操作中に Ctrl/C や Ctrl/Z を入力して反応がなくなった場合は、もう一度 Ctrl/C を入力するか、Ctrl/D を入力してください。

○ enable コマンド（非特権 EXEC モード）のパスワード入力に連続して失敗した場合、エラーメッセージに続いて表示されるプロンプトの先頭に「enable-local 15」という不要な文字列が表示されます。

6.3 ファイル操作

参照「コマンドリファレンス」/「運用・管理」/「ファイル操作」

ファイル名にはスペースは使用できません。

6.4 コンフィグレーション

参照「コマンドリファレンス」/「運用・管理」/「コンフィグレーション」

boot config-file コマンドにおいて、コンフィグファイルを相対パスで指定した場合、show boot コマンドや show system コマンドにおいても相対パスで表示されます。その場合でも起動時コンフィグとして正常に動作しますが、atmf provision node clone コマンドにおける複製元ノードでは、起動時コンフィグを相対パスで指定せず、絶対パスで指定してください。

6.5 ユーザー認証

参照「コマンドリファレンス」/「運用・管理」/「ユーザー認証」

○ TACACS+ サーバーを利用したコマンドアカウンティング（aaa accounting commands）有効時、end コマンドのログは TACACS+ サーバーに送信されません。

○ TACACS+ サーバーを利用した CLI ログインのアカウンティングにおいて、SSH 経由でログインしたユーザーのログアウト時に Stop メッセージを送信しません。

○ スクリプトで実行されたコマンドは TACACS+ サーバーへは送信されません。

6.6 RADIUS クライアント

参照「コマンドリファレンス」/「運用・管理」/「RADIUS クライアント」

radius-server host コマンドの retransmit パラメーター、または、radius-server retransmit コマンドで 0 を指定しても、初期値の 3 回再送を行います。

6.7 ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○ no log buffered コマンドを入力してランタイムメモリー（RAM）へのログ出力を一度無効にした後、default log buffered コマンドを実行しても、ログ出力が再開しません。その場合は「log buffered」を実行することにより再開できます。

○ 複数の VLAN に所属する SFP モジュールをホットスワップすると、次のようなログが表示されます。

user.warning awplus NSM[XXXX]: 601 log messages were dropped - exceeded the log rate limit

これは短時間に大量のログメッセージが生成されたため一部のログ出力を抑制したことを示すものです。ログを抑制せずに出力させたい場合は、log-rate-limit nsm コマンドで単位時間あたりのログ出力上限設定を変更してください。

6.8 トリガー

参照「コマンドリファレンス」/「運用・管理」/「トリガー」

トリガー設定時、script コマンドで指定したスクリプトファイルが存在しない場合、コンソールに出力されるメッセージ内のスクリプトファイルのパスが誤っています。

誤： % Script /flash/script-3.scp does not exist. Please ensure it is created before
正： % Script flash:/script-3.scp does not exist. Please ensure it is created before

また、スクリプトファイルが存在しないにもかかわらず前述のコマンドは入力できてしまうため、コンフィグに反映され、show trigger コマンドのスクリプト情報にもこのスクリプトファイルが表示されます。

6.9 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ snmp-server enable trap コマンドは、省略せずに入力してください。省略した場合、実行できない、または、コンソールの表示が乱れることがあります。

○ IP-MIB は未サポートです。

○ VLAN 名を SNMP の dot1qVlanStaticName から設定する場合は、31 文字以内で設定してください。

6.10 sFlow

参照「コマンドリファレンス」/「運用・管理」/「sFlow」

sflow collector コマンドで UDP ポートを変更したのち、UDP ポートを初期値に戻す場合は、「no sflow collector」ではなく「sflow collector port 6343」を実行してください。

6.11 NTP

参照「コマンドリファレンス」/「運用・管理」/「NTP」

○ 初期設定時など、NTP を設定していない状態で show ntp status コマンドを入力すると、NTP サーバーと同期していることを示す以下のようなメッセージが表示されます。

Clock is synchronized, stratum 0, actual frequency is 0.000PPM, presicion is 2

○ NTPv4 を使用している場合、ntp master コマンドによる NTP 階層レベル（Stratum）の設定と NTP サーバーによる時刻の取得を併用すると、NTP サーバーによって自動決定される階層レベルが優先されます。

○ NTP による時刻の同期を設定している場合、時刻の手動変更は未サポートとなります。

○ ntp master コマンドで <1-15> パラメーターを省略した場合、NTP 階層レベル（Stratum）は 6 になるべきですが、実際は 12 になります。この問題を回避するため、同コマンドでは NTP 階層レベルを明示的に指定してください。

6.12 端末設定

参照「コマンドリファレンス」/「運用・管理」/「Telnet」

仮想端末ポート（Telnet/SSH クライアントが接続する仮想的な通信ポート）がすべて使用されているとき、write memory など一部のコマンドが実行できなくなります。

6.13 Telnet

参照「コマンドリファレンス」/「運用・管理」/「Telnet」

本製品から他の機器に Telnet で接続しているとき、次のようなメッセージが表示されます。
No entry for terminal type "network";
using vt100 terminal settings.

6.14 Secure Shell

参照「コマンドリファレンス」/「運用・管理」/「Secure Shell」

○ SSH サーバーにおけるセッションタイムアウト（アイドル時タイムアウト）は、ssh server session-timeout コマンドで設定した値の 2 倍で動作します。

○ 本製品の SSH サーバーに対して、次に示すような非対話式 SSH 接続（コマンド実行）をしないでください。
※ 本製品の IP アドレスを 192.168.10.1 と仮定しています。

```
clientHost> ssh manager@192.168.10.1 "show system"
```

6.15 インターフェース

参照「コマンドリファレンス」/「インターフェース」

○ AT-x210-9GT の SFP ポートでは、polarity コマンドでのインターフェースの極性の固定設定は未サポートです。

○ AT-x210-9GT の SFP ポートで Copper SFP（AT-MG8T）を使用する際、Polarity Auto でリンクアップしたときの表示が必ず MDI と表示されてしまいます。

○ AT-x210-9GT の SFP ポートで copper SFP（AT-MG8T）を使用し、対向機に接続した状態で起動した場合、起動中にもかかわらず、対向に接続したポートがリンクアップしてしまう時間があります。

○ AT-x210-16GT/AT-x210-24GT のコンボ SFP ポートにおいて、1000M Full 固定設定は未サポートです。

6.16 ポートミラーリング

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

複数ポートにインターフェースモードのコマンドを発行するときは、interface コマンドで対象ポートを指定するときに、通常ポートとして使用できないミラーポートを含めないようにしてください。ミラーポートを含めた場合、一部のポートに設定が反映されなかったり、エラーメッセージが重複して表示されたりすることがあります。

6.17 MAC アドレススラッシング検出

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

MAC アドレススラッシングプロテクションにおいて、vlan-disable、link-down アクション実行時のログメッセージに誤りがありますので、下記のとおり読み替えてください。

[vlan-disable の場合]
誤：Thrash: Loop Protection has disabled "port" on ifindex XXXX vlan X
正：Thrash: Loop Protection has disabled "VLAN" on ifindex XXXX vlan X
[link-down の場合]
誤：Thrash: Loop Protection has disabled "port" on ifindex XXXX
正：Thrash: Loop Protection has disabled "port-link" on ifindex XXXX

6.18 ループガード

参照 「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ LDF 検出機能のアクションが vlan-disable となっている VLAN の所属ポートで、switchport enable vlan コマンドを実行しないでください。

○ LDF 検出の port-disable アクションによってポートがシャットダウン状態になっていても、show interface コマンドの administrative state 欄には err-disabled ではなく UP と表示されます。またこのとき、MIB の ifAdminStatus も UP になります。LDF 検出のポート状態を確認するには、show loop-protection コマンドを使ってください。

6.19 リンクアグリゲーション

参照 「コマンドリファレンス」/「インターフェース」/「リンクアグリゲーション」

○ スタティックチャンネルグループ（手動設定のトランクグループ）において、shutdown コマンドによって無効にしていたポートに対して no shutdown コマンドを入力しても、ポートが有効にならないことがあります。この場合は、再度 shutdown コマンド、no shutdown コマンドを入力してください。

○ スタティックチャンネルグループのインターフェースを shutdown コマンドにより無効に設定した後、リンクアップしているポートをそのスタティックチャンネルグループに追加すると、該当するインターフェースが再び有効になります。

○ show interface コマンドで表示される poX インターフェース（LACP チャンネルグループ）の input packets 欄と output packets 欄の値には、リンクダウンしているメンバーポートの値が含まれません。
LACP チャンネルグループ全体の正確な値を確認するには、poX インターフェースではなく各メンバーポートのカウンターを参照してください。

6.20 ポート認証

参照 「コマンドリファレンス」/「インターフェース」/「ポート認証」

○ 802.1X 認証において、認証を 3 台以上の RADIUS サーバーにて行う場合、はじめの 2 台の RADIUS サーバーにて認証に失敗した際、Authenticator から 3 台目の RADIUS サーバーに Access-Request が送信されません。

○ 認証済みポートが認証を解除されても、マルチキャストトラフィックが該当ポートに転送され続ける場合があります。

○ バージョン **5.4.3-2.5** より前のファームウェアにおいて、一度でも Web 認証サーバー（HTTPS）用の独自 SSL 証明書をインストール（copy xxxxx web-auth-https-file）したことがある場合、独自証明書を削除して、Web 認証サーバーにシステム付属の証明書を使わせるには、次の手順を実行してください。

1. 独自にインストールした SSL 証明書を削除する。
awplus# erase web-auth-https-file

2. HTTP サービスを再起動する。
awplus(config)# no service http
awplus(config)# service http

またはシステムを再起動する（※ 未保存の設定がある場合は再起動前に保存してください）。
awplus# reboot

また、ユーザー SSL 証明書をインストール (copy xxxxx web-auth-https-file) した場合、web 認証を行うためには、次の手順を実行してください。

SSL 証明書をインストール後、HTTP サービスを再起動する。
awplus(config)# no service http
awplus(config)# service http

または筐体を再起動する。

○ 802.1X 認証と Web 認証の 2 ステップ認証機能利用時は、認証スイッチと RADIUS サーバーとの間で使用する認証方式を、802.1X 認証と Web 認証でそれぞれ別の方式に設定してください。

○ auth-mac password コマンドの password 名に「encrypted」を設定することはできません。

○ インターフェース上で、dot1x port-control コマンドを設定する前に dot1x control-direction コマンドを設定しないでください。設定すると「no dot1x control-direction」を実行しても、dot1x control-direction コマンドを削除することができなくなります。その場合は、「no dot1x port-control」を実行してください。

○ 約 20 端末ほどの Supplicant が Web 認証に失敗すると、その後 Web 認証が動作しなくなります。

○ Web 認証とゲスト VLAN は併用できません。

○ Web 認証サーバーのセッションキープ機能有効時、Web 認証端末が認証画面にアクセスしてから認証に成功するまでの間に、端末上のバックグラウンドプログラム等が自発的な HTTP 通信を試みた場合、認証成功後に意図したページへリダイレクトされないことがあります。

○ HTTPS を有効化した Web 認証サーバーにおいて、短い間隔で Supplicant の認証を行うと、認証可能な Supplicant 数が auth max-supplicant コマンドで設定した値よりも少なくなることがあります。

○ Web 認証において再認証を続けて行うと、show cpu コマンドで表示される userspace の値が 100% を超えますが、これは表示上の問題であり、認証は正常に行われます。

6.21 VLAN

参照 「コマンドリファレンス」/「L2 スイッチング」/「バーチャル LAN」

○ プライベート VLAN からプライマリー VLAN を削除する場合は、事前にプライマリー VLAN、セカンダリー VLAN ともに、プライベート VLAN の関連付けを解除してください。その後、プライマリー VLAN のみを削除、再作成し、改めてプライベート VLAN とプライマリー VLAN、セカンダリー VLAN の関連付けを行ってください。

○ エンハンストプライベート VLAN を設定したポートからプライベート VLAN 用ポートとしての設定を削除すると、該当のポートでパケットが転送できなくなります。プライベート VLAN 用ポートとしての設定を削除した後は、本製品を再起動してください。

○ プライベート VLAN 設定時に一度設定したホストポートは、その後設定を削除しても、show vlan private-vlan の表示に反映されず、ホストポートとして表示されたままになります。

○ プライベート VLAN でセカンダリー VLAN を削除したとき、private-vlan association コマンドの設定を削除することができなくなります。

○ タグ付きのトランクポートにポート認証が設定されている際、認証の設定を維持したままポートトランキングの設定を削除し、ネイティブ VLAN の設定を行う場合は、一度タグなし VLAN に設定を変更してから再度ポートトランキングを設定し、ネイティブ VLAN の設定変更を行ってください。

○ マルチプル VLAN（プライベート VLAN）を CLI から設定した場合、コマンドの入力順序によってはプロミスキャスポート・ホストポート間の通信ができなくなる場合があります。その場合は、設定を保存してから再起動してください。

○ switchport trunk allowed vlan コマンドで、デフォルト VLAN（VID=1）をタグ VLAN 扱いにした場合、switchport trunk native vlan none を指定してもタグなしフレームが破棄されません。

○ 1 ポートに適用する VLAN クラシファイアグループは 2 グループまでにしてください。

○ 同じ VLAN クラシファイアグループ内に複数のルールを定義した場合、設定順ではなく番号順に反映されます。

6.22 UDLD

参照「コマンドリファレンス」/「L2 スイッチング」/「UDLD」

UDLD が Unidirectional を検出した場合、show interface コマンドの administrative state 欄には err-disabled と表示されますが、このとき標準 MIB の ifAdminStatus は UP を示します。

6.23 イーサネットリングプロテクション（EPSR）

参照「コマンドリファレンス」/「L2 スイッチング」/「イーサネットリングプロテクション」

EPSR 内のリンクダウンが発生した機器が、マスターからのリンクダウンパケットを受け取っても FDB 情報をクリアしない場合があります。また、リンクダウンが発生した機器は本来であれば FDB の全クリアする必要がありますが、該当ポートの FDB はリンクダウンによってクリアされるため、通信に影響はありません。

6.24 IP インターフェース

参照「コマンドリファレンス」/「IP」/「IP インターフェース」

本バージョンでは DHCP クライアント機能を使用できません。DHCP クライアント機能を使用する場合は、バージョン 5.4.4-0.4 以前のファームウェアをご使用ください。

6.25 ARP

参照「コマンドリファレンス」/「IP」/「ARP」

マルチキャスト MAC アドレスをもつスタティック ARP エントリーを作成した後、それを削除してから arp-mac-disparity コマンドを有効にして、同一のエントリーをダイナミックに再学習させる場合は、設定後にコンフィグを保存して再起動してください。

6.26 IPv6

参照「コマンドリファレンス」/「IPv6」

○ 自身の IPv6 アドレス宛に ping を実行するとエラーメッセージが表示されます。

○ フラグメントされた IPv6 Echo Request は利用できません。利用した場合 Duplicate パケットは正しく再構築されませんのでご注意ください。

6.27 IGMP Snooping

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

○ マルチキャストグループをスタティックに登録している状態で、同じマルチキャストグループをダイナミックに学習すると、その後スタティック登録したグループを削除しても、show ip igmp groups コマンドと show ip igmp snooping statistics interface コマンドの表示からは該当グループが削除されません。これは表示だけの問題で動作には影響ありません。

○ IGMP Snooping が有効な状態で、一旦無効にし、再度有効にした場合、その後に受信する IGMP Report を全ポートにフラッディングします。IGMP Snooping を再度有効にした後、clear ip igmp group コマンドを実行して全てのエントリーを消去することで回避できます。

○ Include リスト（送信元指定）付きのグループレコードが登録されている状態で、あるポートに接続された唯一のメンバーからグループ脱退要求を受信すると、そのポートには該当グループのマルチキャストトラフィックが転送されなくなりますが、他のポートで同じグループへの参加要求を受信すると、脱退要求によって転送のとまっていたポートでもマルチキャストの転送が再開されてしまいます（この転送は、脱退要求を受信したポートの Port Member list タイマーが満了するまで続きます）。

○ ダイナミック登録されたルーターポートを改めてスタティックに設定した場合、ダイナミック登録されてから一定時間が経過すると設定が削除されます。また、一定時間が経過するまでの間、コンフィグ上にはスタティック設定が表示されますが、ip igmp snooping mrouter interface コマンドを no 形式で実行しても、コンフィグから削除することができません。ルーターポートをスタティックに設定する場合は、該当のポートがダイナミック登録されていないことを確認してください。

○ 未認識の IGMP メッセージタイプを持つ IGMP パケットは破棄されます。

○ 不正な IP チェックサムを持つ IGMP Query を受信しても破棄しません。そのため、当該の IGMP Query を受信したインターフェースはルーターポートとして登録されてしまいます。

6.28 MLD Snooping

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

○ clear ipv6 mld コマンド実行時に「% No such Group-Rec found」というエラーメッセージが表示されることがありますが、コマンドの動作には問題ありません。

○ MLD Snooping の Report 抑制機能が有効なとき（初期設定は有効）、ルーターポートで受信した MLDv1 Report または Done メッセージを受信ポートから再送出してしまいます。これを回避するには、「no ipv6 mld snooping report-suppression」で Report 抑制機能を無効化してください。

○ MLD メッセージを受信する環境では MLD Snooping を有効にしてください。MLD snooping が無効に設定されたインターフェースで MLD メッセージを受信すると次のようなログが出力されます。

NSM[1414]: [MLD-DECODE] Socket Read: No MLD-IF for interface port6.0.49

6.29 ハードウェアアクセスリスト

参照「コマンドリファレンス」/「トラフィック制御」/「アクセスリスト」

ハードウェアアクセスリストをサポートリミットまで使用する設定を行った場合は、設定をスタートアップコンフィグに保存し、いったん再起動してください。

6.30 Quality of Service

参照「コマンドリファレンス」/「トラフィック制御」/「Quality of Service」

○ match dscp コマンドの設定を削除する際、no match dscp と入力するとエラーとなります。no match ip-dscp コマンドを入力することで、設定を削除できます。

○ wrr-queue disable queue コマンドを設定している状態で no mls qos コマンドにより QoS 自体を無効にする場合は、先に no wrr-queue disable queue コマンドを実行してください。

○ QoS の送信スケジューリング方式（PQ、WRR）が混在するポートを手動設定のトランクグループ（スタティックチャンネルグループ）に設定した場合、ポート間の送信スケジュールが正しく同期されません。トランクグループを設定した場合は、個々のポートに同じ送信スケジュール方式を設定しなおしてください。

○ クラスマップに追加するアクセスリストの名前は 20 文字以内にしてください。

○ ポリシーマップ名に「|」を使用しないでください。

○ 受信レート検出（QoS ストームプロテクション）機能の storm-action コマンドの初期値に portdisable が設定されています。

○ QoS ストームプロテクションの linkdown アクションを解除するときは、switchport enable vlan コマンドではなく「no shutdown」を使ってください。

○ QoS ストームプロテクションの portdisable アクションによってポートがシャットダウン状態になっていても、show interface コマンドの administrative state 欄には err-disabled ではなく UP と表示されます。またこのとき、MIB の ifAdminStatus も UP になります。

6.31 DHCP サーバー

参照「コマンドリファレンス」/「IP 付加機能」/「DHCP サーバー」

○ 同じ DHCP クライアントから 2 回目の割り当て要求があった場合、割り当て中の IP アドレスは show ip dhcp binding コマンドの実行結果で表示される IP アドレス割り当て状況に残ったままになります。リースしているアドレスの使用期間が満了すると、当該の IP アドレスは割り当て状況一覧から消去されます。

○ show ip dhcp binding コマンドで DHCP クライアントへの IP アドレス割り当て状況を確認するとき、いくつかの DHCP プールに関する情報が表示されないことがあります。

6.32 アライドテレシスマネージメントフレームワーク（AMF）

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク（AMF）」

○ AMF リンクとして使用しているスタティックチャンネルグループの設定や構成を変更する場合は、次に示す手順 A・B のいずれかにしたがってください。

[手順 A]
1. 該当スタティックチャンネルグループに対して shutdown を実行する。
2. 設定や構成を変更する。
3. 該当スタティックチャンネルグループに対して no shutdown を実行する。

[手順 B]
1. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して no switchport atmf-link を実行する。
2. 設定や構成を変更する。
3. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して switchport atmf-link を実行する。

○ リブートローリング機能でファームウェアバージョンを A から B に更新する場合、すでに対象ノードのフラッシュメモリー上にバージョン B のファームウェアイメージファイルが存在していると、ファームウェアの更新に失敗します。このような場合は、対象ノードから該当するファームウェアイメージファイルを削除してください。

○ AMF マスターが AMF メンバーよりも後に AMF ネットワークに参加するとき、AMF マスターのコンフィグにてその他メンバーからのワーキングセット利用やリモートログインに制限がかけてあっても、既存のメンバーに対してこれらの制限が反映されません。再度 AMF マスター上で atmf restricted-login コマンドを実行することで、全ての AMF メンバーに対して制限をかけることができます。

○ AMF クロスリンクを抜き差しすると、show atmf links statistics コマンドの表示結果にて、Discards カウンターが 8 ずつ増加します。

○ AMF 仮想リンクを使用している環境において、仮想リンクが通過する経路上の最小 MTU（経路 MTU）が 1500 バイト未満の場合（例：PPPoE 接続のルーターを介して仮想リンクを設定している場合）、ワーキングセットプロンプトで実行したコマンドの結果が表示されずにプロンプトが返ってくることがあります。本現象を回避するには、ルーター間で L2TP や IPsec などのトンネリング設定を行い（AMF 仮想リンクのトンネリングパケットをさらにもう一回トンネリングする）、トンネルの入り口で AMF トンネリングパケットをフラグメント化、トンネル出口で再構成することで、1500 バイトの AMF トンネリングパケットが破棄されないようにしてください。

○ オートリカバリーが成功したにもかかわらず、リカバリー後に正しく通信できない場合は、代替機の接続先が交換前と同じポートかどうかを確認してください。
誤って交換前とは異なるポートに代替機を接続してしまった場合は、オートリカバリーが動作したとしても、交換前とネットワーク構成が異なるため、正しく通信できない可能性がありますのでご注意ください。

○ atmf cleanup コマンドの実行後、再起動時に HSL のエラーログが表示されますが、通信には影響はありません。

○ atmf provision node clone コマンドで新規ノードの事前設定をクローン作成する場合は、複製元ノードの起動時コンフィグ（boot config-file コマンド）が絶対パスで指定されていることを確認してください。

○ AMF と EPSR を併用しているとき、EPSR リング内の AMF クロスリンクで接続している箇所がリンクダウンしていると、AMF のオートリカバリーが正常に完了しません。手動リカバリーを利用してください。

7 マニュアルの補足・誤記訂正

各種ドキュメントの補足事項および誤記訂正です。

7.1 サポートする SFP/SFP+ モジュールについて

本製品がサポートする SFP/SFP+ モジュールの最新情報については、弊社ホームページをご覧ください。

7.2 AT-x210-24GT

参照 「取扱説明書」（Rev.A）

取扱説明書 Rev.A（613-001621 Rev.A）に掲載されている AT-x210-24GT の情報には誤りがあります。AT-x210-24GT に関する正しい情報は、取扱説明書 Rev.B（613-001621 Rev.B）でご確認ください。

7.3 ループガード（LDF 検出）

参照 「コマンドリファレンス」/「インターフェース」/「スイッチポート」

ファームウェアバージョン **5.4.3-0.1** のリリースノート（Rev.F）には、「LACP と LDF 検出は併用できません」とありますが、LACP と LDF 検出は問題なく併用できます。

7.4 HOL ブロッキング防止

ジャンボフレームに対して HOL ブロッキング防止を機能させるには QoS 機能を有効化（mls qos enable）してください。QoS 機能が無効の場合、ジャンボフレームに対しては HOL ブロッキング防止が機能しません。

8 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）	8 ※1
ポート数（グループあたり）	8
ハードウェアパケットフィルター	
登録数	118 ※2※3※4
認証端末数	
認証端末数（ポートあたり）	320
認証端末数（装置あたり）	480
マルチプルダイナミック VLAN（ポートあたり）	8
マルチプルダイナミック VLAN（装置あたり）	40
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 スタティックチャンネルグループは 4 グループ、LACP は 4 グループ設定可能。合わせて 8 グループをサポートします。
※2 アクセスリストのエントリー数を示します。
※3 1 ポートにのみ設定した場合の最大数。エントリーの消費量はルール数やポート数に依存します。
※4 ユーザー設定とは別に、アクセスリストを使用する機能を有効化した場合に消費されるエントリーを含みます。

9 未サポート機能（コマンド）

最新のコマンドリファレンスに記載されていない機能、コマンドはサポート対象外ですので、あらかじめご了承ください。最新マニュアルの入手先については、次節「最新マニュアルについて」をご覧ください。

10 最新マニュアルについて

最新の取扱説明書「CentreCOM x210 シリーズ 取扱説明書」（613-001621 Rev.B）、コマンドリファレンス「CentreCOM x210 シリーズ コマンドリファレンス」（613-001681 Rev.H）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、これらの最新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、弊社ホームページで最新の情報をご覧ください。

http://www.allied-telesis.co.jp/