613-001683 Rev.L 140625

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 5.4.4-0.4

2 重要：注意事項

2.1 AMF における異なるファームウェアバージョンのメンバーの共存

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 ノードのファームウェアを **5.4.3** 系列から **5.4.4** 系列にバージョンアップするときは、最初にすべての AMF メンバーを **5.4.4** 系列にバージョンアップしてから、最後に AMF マスターをバージョンアップしてください（atmf working-set で「group all」を指定し、atmf reboot-rolling で一括バージョンアップする場合は、自動的にこの順序（メンバー → マスターの順）でバージョンアップを行います）。先に AMF マスターをバージョン **5.4.4** 系列にバージョンアップした場合、バージョン **5.4.3-3.7** より前（**5.4.3-2.x** 以前）の AMF メンバーが AMF ネットワークに参加できなくなりますのでご注意ください。

○ メジャーバージョンが異なるファームウェアの混在は、ファームウェアバージョンアップ時など一時的な使用に限定し、継続的な運用には使用しないでください。

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 **5.4.3-2.6** から **5.4.4-0.4** 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 RADIUS サーバーへの Supplicant VLAN ID 通知機能

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」

ポート認証において、Supplicant の VLAN ID を RADIUS サーバーに通知できるようになりました。初期設定では Supplicant の VLAN ID を通知しませんが、新しく追加された auth radius send vlan-id コマンドを設定すると、Supplicant の VLAN ID が RADIUS サーバーに通知されるようになります。これにより、RADIUS サーバー側において、ユーザー名に加えて VLAN ID をも考慮に入れた認証・設定配布システムなどを構築できるようになります。

3.2 2 ステップ認証

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」

ポート認証において、MAC ベース認証 /802.1X 認証 /Web 認証のうち 2 つの認証方式に連続して成功したときだけ通信を許可する設定（2 ステップ認証）が可能になりました。

3.3 プロキシー環境での Web 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」

プロキシーサーバーを使用している環境でも、Web 認証を利用できるようになりました。

3.4 MAC 認証用共通パスワード

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」

MAC ベース認証において RADIUS サーバーに認証を要求するときのパスワードとして、個々の Supplicant の MAC アドレスではなく、全 Supplicant に共通な任意の文字列を使うように設定する auth-mac password コマンドをサポートしました。
本コマンドを使用することにより、MAC ベース認証 → Web 認証または MAC ベース認証 → 802.1X 認証の 2 ステップ認証を使用する際に、Authenticator（本製品）・RADIUS サーバー間で使用する認証方式を、MAC ベース認証と Web/802.1X 認証とでそれぞれ別の方式に設定する必要がなくなります。

3.5 HTTP リダイレクト

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 認証において、HTTP リダイレクト（auth-web-server http-redirect コマンド）をサポートしました。

3.6 Group-specific クエリーのフラッディング抑止設定

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

IGMP Snooping の Querier 機能において、Group-Specific Membership Query をフラッディングせずに、該当グループのメンバーが存在するポートにだけ送信させるオプションが追加されました。初期設定ではフラッディングしますが、新しく追加された ip igmp flood specific-query コマンドを no 形式で実行することにより、メンバーが存在するポートにだけ送信するようになります。

3.7 未登録マルチキャストグループの保持時間設定

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、未登録マルチキャストグループの保持時間を設定する ip igmp snooping source-timeout コマンドをサポートしました。

3.8 access-list hardware(seq entry) コマンドのワイルドカードマスク対応

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」

access-list hardware(seq entry) コマンドにおいて、ワイルドカードマスクの指定をサポートしました。

3.9 AMF メンバー機能

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 メンバー機能をサポートしました。
AMF ネットワークにおいて x210 をメンバーとして管理するためには、AMF マスターに AMF メンバープロダクト拡張ライセンスが必要です。

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 **5.4.3-2.6** から **5.4.4-0.4** 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 exception coredump size コマンドの削除

参照「コマンドリファレンス」/「運用・管理」/「システム」

exception coredump size コマンドは削除されました。

4.2 フューチャーライセンス

参照「コマンドリファレンス」/「運用・管理」/「システム」

license コマンドの no 形式から index NUMBER パラメーターが削除されました。

4.3 ホスト名の使用可能文字変更

参照「コマンドリファレンス」/「運用・管理」/「システム」

hostname コマンドで設定するホスト名に使用できる文字が、半角英数字とハイフン、アンダースコアに制限されるようになりました。

4.4 TACACS+ 使用時の仮想端末ポート同時使用数

参照「コマンドリファレンス」/「運用・管理」/「ユーザー認証」

CLI ログイン認証に TACACS+ を使用するとき、仮想端末ポート（VTY）を 33 まで同時に使用できるようになりました。

4.5 show interface コマンド

参照「コマンドリファレンス」/「インターフェース」

下記の機能によってポートがシャットダウン状態になったとき、show interface コマンドで該当ポートの状態が「err-disabled」と表示されるように仕様変更されました。。
MAC アドレススラッシングプロテクション
LDF 検出
UDLD
ポートセキュリティー
AMF セーフコンフィグ
DHCP Snooping
QoS ストームプロテクション
BPDU ガード

4.6 802.1X 認証と Web 認証の併用時の動作

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」

2 ステップ認証のサポートにより、802.1X 認証と Web 認証を併用する場合の動作が変更になりました。

○ 旧バージョンでの動作
802.1X 認証と Web 認証併用時は、802.1X で認証に失敗すると認証プロセスが完了となっていました。
○ 本バージョンからの動作
802.1X 認証と Web 認証併用時は、802.1X で認証に失敗すると Web 認証に移行し、Web 認証でも認証に失敗すると認証プロセスが完了になります。

4.7 CHANGE_TO_INCLUDE メッセージ受信時のログレベル

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

CHANGE_TO_INCLUDE IGMP/MLD メッセージを受信した時に「Rexmit failed」というログが warning レベルで出力されていましたが、informational レベルで出力されるよう変更しました。

4.8 MLDv2 Snooping の仕様変更

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

ソースリスト付きの MLDv2 Report は受信せずに破棄するようになりました。
IPv6 マルチキャスト環境で本製品を使用する場合は、クライアント側で MLDv2 のソースリストを使用しないよう設定するか、MLD Querier 側で MLDv1 を使うよう設定してください。

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 **5.4.3-2.6** から **5.4.4-0.4** 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 ping などを実行中にコンソールがタイムアウトすると、プロセスがバックグラウンドで動いたままの状態になっていましたが、これを修正しました。

5.2 copy コマンドで「*」を使用して複数のファイルを TFTP サーバーへアップロードする際、コピー元に対象のファイルが見つからない場合、「Successful operation」と表示されていましたが、正しくエラーメッセージが表示されるよう修正しました。

5.3 TFTP サーバーへのリモートコピー（アップロード）時、Write Request パケットで送信するファイル名の先頭に余分なスラッシュ（/）を付加していたため、TFTP サーバーによっては転送に失敗することがありましたが、これを修正しました。

5.4 TFTP サーバーに copy コマンドでファイルをコピーする際に、ネットワーク到達不可状態であった場合、CLI 上に表示されるエラーメッセージに余分な文字列が付加されることがありましたが、これを修正しました。

5.5 ファイルシステム上に作成したフォルダーを別のフォルダーの中に移動させる際、移動先のフォルダーの中に既に同名フォルダーがある場合、既存のフォルダーの中にフォルダーの中身を移動していましたが、移動させた際に既存の同名フォルダーを上書きするよう修正しました。

5.6 「:」を含むファイル名でファイルを作成した場合、show file コマンドでそのファイル内容が表示されませんでしたが、正しく表示されるよう修正しました。

5.7 SCP サーバーとのファイルの送受信時、サーバーと通信できない場合は、エラーメッセージが表示されるように修正されました。

5.8 show tech-support コマンドによって内部的に実行されたコマンド操作は、TACACS+ サーバーにコマンドアカウンティングメッセージとして送信されませんでしたが、これを修正しました。

5.9 ユーザーの認証に成功したあと、show auth-web all コマンドを入力すると関連プロセス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。

5.10 show trigger コマンドに counter パラメーターを指定した際に表示されるトリガーの統計情報に不適切な項目がありましたが、これを修正しました。

5.11 fallingAlarm トラップが正しい OID で送信されていませんでしたが、これを修正しました。

5.12 LDF 検出、MAC アドレススラッシングプロテクション、UDLD、QoS ストームプロテクションの働きによりスイッチポートがリンクダウンした場合、SNMP 経由で取得する ifAdminStatus の値が誤って DOWN になっていましたが、これを修正しました。

5.13 SNMP マネージャーから at-license.mib の LicenseIndex 値を取得すると、CLI や SSH などからログインした際に確認できる値と異なる場合がありましたが、これを修正しました。

5.14 RMON-MIB の historyControlTable および alarmTable のに対する SNMP Set に失敗していましたが、これを修正しました。

5.15 SNMP のプライベート MIB 経由で取得したファイルパスの形式が正しくありませんでしたが、これを修正しました。

5.16 sflow collector コマンドで sflow の UDP ポートを設定したとき、コンフィグに反映されていませんでしたが、これを修正しました。

5.17 DNS サーバーを複数登録（ip name-server）している場合、NTP サーバーの追加コマンド（ntp server）を実行すると、プロンプトが戻るまで 1 分以上かかる場合がありましたが、これを修正しました。

5.18 show ntp associations コマンドに detail パラメーターを指定して実行した際、org time と xmt time の値が正しく表示されていませんでしたが、これを修正しました。

5.19 NTP 脆弱性（JVNVU#96176042）への対策を行いました。

5.20 同時に大量の Telnet または SSH アクセスを受けると機器の再起動が発生していましたが、これを修正しました。

5.21 SFP モジュール AT-MG8T 上のスイッチポートを MDI 固定に設定しているにもかかわらず、対向装置の MDI 固定ポートとストレートケーブルで接続した場合に該当ポートがリンクアップすることがありましたが、これを修正しました。

5.22 AT-x210-16GT、AT-x210-24GT の SFP ポートで、1000M Full 固定設定すると通信できませんでしたが、これを修正しました。

5.23 非特権 EXEC モードで show static-channel-group コマンドを「show sta」という省略形で実行すると、同コマンドだけでなく show startup-config コマンドの出力も表示されていましたが、これを修正しました。

5.24 Web 認証で、auth-web-server redirect-delay-time コマンドでリダイレクト時間を設定した場合に、初期設定値を設定しても、ランニングコンフィグ上に表示されていましたが、これを修正しました。

5.25 認証ポートが直接 Supplicant のリンクアップ / ダウンを検知しない環境において、一度 Web 認証に失敗した後に Supplicant が DHCP にて IP アドレスの再取得を実施すると、再度 Web 認証を実施した際に認証画面が表示されませんでしたが、これを修正しました。

5.26 MAC 認証とダイナミック VLAN を併用した際、通信中に FDB のクリアを伴う再認証が発生すると、Supplicant が認証されず通信が切断されることがありましたが、これを修正しました。

5.27 Web 認証を設定したトランクグループにおいて、所属ポートのリンクアップ時に多数の Supplicant が同時に通信、認証を行った場合、未認証の Supplicant で通信が行えてしまうことがありましたが、これを修正しました。

5.28 RSTP モードでスパニングツリープロトコルを使用している場合、ローミング認証に失敗することがありましたが、これを修正しました。

5.29 VLAN4091、4092 を通常の VLAN として使用すると、スイッチングできないことがありましたが、これを修正しました。

5.30 プライベート VLAN を設定する場合、プロミスキャスポートよりもホストポートを先に設定すると、通信できないことがありましたが、これを修正しました。

5.31 switchport trunk allowed vlan コマンドで none を指定すると、所属ポートの少ない VLAN 宛ての通信ができなくなる場合がありましたが、これを修正しました。

5.32 switchport trunk allowed vlan コマンドに except パラメーターを指定した場合、まれに ARP 応答などが正しく行われなくなることがありましたが、これを修正しました。

5.33 Ping コマンドを実行したときに正しいログが表示されませんでしたが、これを修正しました。

5.34 VLAN インターフェースに設定されている IP アドレスにラベルを設定してもコンフィグに反映されませんでしたが、これを修正しました。

5.35 IP アドレスを設定していない VLAN インターフェース宛に IP パケットを受信すると、異なる VLAN インターフェースにパケットを転送していましたが、これを修正しました。

5.36 IGMPv2 のパケット（Report、Leave）や、IGMPv3 のパケット（Change_To_Exclude、Change_To_Include）を受信したときに、「Failed to find real Src-Rec from a Clone!」、「Invalid Rexmit HRT」のログが大量に表示されることがありましたが、これを修正しました。

5.37 IGMP Snooping の Query Interval パラメーターの設定が、IGMP Snooping を一旦無効にして再度有効にするまで反映されませんでしたが、これを修正しました。

5.38 MLDv2 のソースフィルタリングを使用する環境において、本製品配下のホストは同一サブネットから配信される IPv6 マルチキャストパケットを受信できませんでしたが、これを修正しました。

5.39 DHCP のリース時間の最小値は 20 秒にもかかわらず、20 秒未満を設定しようとした時のエラーメッセージとして「Lease must be at least one minute」と表示されていましたが、これを修正しました。

5.40 show ip dhcp binding コマンドで ClientId が正しく表示されませんでしたが、これを修正しました。

5.41 DHCP サーバーのネットワーク設定をベース IP アドレスとサブネットマスクで入力すると DHCP のプロセスが正常に動作しませんでしたが、これを修正しました。

5.42 banner exec コマンドを no 形式で入力したコンフィグが実行されている場合、Web GUI にログインすることができませんでしたが、これを修正しました。

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 **5.4.4-0.4** 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。

○ 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。

6.2 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。

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 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。

6.5 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。

○ email ログ機能を使用時に、宛先との通信に失敗し続けると、一時的に CPU とメモリーの使用率が増加します。再び通信できる状態になると、すぐに CPU/ メモリーの使用率は以前の状態に戻ります。

6.6 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。

6.7 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。

6.8 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。

6.9 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.

6.10 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。

6.11 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

6.12 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。

6.13 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。

6.14 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」

○ dot1x control-direction コマンドの both オプションは未サポートです。

○ 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。

6.15 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。

6.16 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」

DHCP クライアント機能によって IP アドレスを取得したとき、IP アドレス使用状況確認パケットを送出しません。

6.17 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。

6.18 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。

6.19 IGMP Snooping

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

○ 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。

6.20 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。

○ MLDv2 において、グループエントリーがスタティック登録されている状態で、同じグループがダイナミックに登録され、待機時間が経過した時、ダイナミック登録されたエントリーとともに、スタティック登録されたエントリーもコンフィグから削除されます

○ MLD メッセージを受信する環境では MLD を有効に設定してください。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

6.21 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。

6.22 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。

6.23 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 switchportatmf-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。

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。

7.5 Web 認証（SSL 証明書）

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 認証で HTTPS 使用時、さらに、プロキシーもしくはインターセプトモード / プロミスキャスモードを併用する場合は、独自の SSL 証明書を Authenticator および Supplicant のブラウザーにインストールしてください。

独自の SSL 証明書を使用しない場合、余計なトラフィックを発生させ筐体に負荷をかける要因となります。そのため、上記併用時は、デフォルトのファームウェア組み込み SSL 証明書の使用はお控えください。

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.F）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 Web ページで最新の情報をご覧ください。

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