613-002063 Rev.A 141219

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　5.4.3-3.16

2　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 **5.4.3-3.16** 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 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・リンクアップしていましたが、これを修正しました。

2.2 SSL/TLS MITM の脆弱性（CVE-2014-0224）への対策を行いました。

2.3 SSLv3 プロトコル脆弱性（CVE-2014-3566）への対策を行いました。これにともない、Web 認証 /Web GUI 用の HTTPS サーバーは SSLv3 による接続を受け付けなくなりました。

2.4 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。

2.5 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。

2.6 RADIUS Access-Request パケットを送信した後、RADIUS サーバーの応答待ち時間までに Supplicant 情報が削除されると、認証プロセスが正しく機能しませんでしたが、これを修正しました。

2.7 システム稼働時間（sysUpTime）が 248.5 日以上経過している状態で VCS マスター切り替えや SFP モジュールのホットスワップが発生した場合、コンフィグ再読み込みを行ったポートのランニングコンフィグに「no lldp transmit」が追加されていましたが、これを修正しました。

2.8 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。

2.9 SSH 脆弱性（CVE-2014-2532 と CVE-2014-2653）への対策を行いました。

2.10 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。

2.11 802.1X 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。

2.12 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。

2.13 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。

2.14 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。

2.15 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。

2.16 Web GUI の Java アプレットファイルのバージョンが 543_04 以前の場合、banner exec コマンドを no 形式で使用することができませんでしたが、Java アプレットファイルのバージョン 543_05 で、これを修正しました。なお、本件は Java アプレットで修正された問題であり、ファームウェアのバージョンには依存しません。

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 **5.4.3-3.16** には、以下の制限事項があります。

3.1 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）。

○ no ip domain-lookup コマンドを実行する以前に、1 度でも ntp server コマンドの設定を行ってしまうと、no ip domain-lookup コマンドを実行したとしても DNS へ問い合わせを行ってしまいます。trigger コマンドで再起動時に no ip domain-lookup コマンドが ntp server コマンドより先に実行されるように設定することにより、no ip domain-lookup の機能が正常に動作します。

3.2 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。

3.3 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」

ZMODEM で転送するファイルのサイズは 3MByte 以下にしてください。

3.4 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」

○ アクセスが許可されていないホスト / ユーザーから SSH でログインしようとした場合、コンソール上にデバッグメッセージが表示されます。

○ tacacs-server timeout コマンドで設定できるタイムアウト値の最大は 190 秒です。

○ CLI ログイン認証に TACACS+ を使用するとき、同時に使用できる仮想端末ポート（VTY）の数は 20 までとなります。また内部のユーザー認証データベースを使用するときは、同時に使用できる仮想端末ポート（VTY）の数は 33 までとなります。

○ CLI ログイン認証に TACACS+ サーバーを利用、かつ、特権パスワード（enable password）を設定している環境において、TACACS+ サーバーダウンにより装置本体のユーザー認証データベースで認証された権限 15 のローカルユーザーが enable コマンドを実行した場合、本来なら権限 15 のユーザーには要求されない特権パスワードの入力プロンプトが表示されます。その場合は任意の文字列を入力することで、特権 EXEC モードに移行できます。

○ 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。

3.5 ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○ 保存するメッセージの最大量が log size コマンドで設定した値と異なります。

○ 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。

3.6 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。

3.7 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ LACP を使用しトランクグループを作成した際、対向機器の SNMP マネージャーで linkDown トラップを受信できない場合があります。送信先ホストの設定をする際、通知メッセージの形式で informs を指定すると informs パケットが受信できます。

○ fallingAlarm トラップが正しい OID で送信されません。

○ SNMP MIB で、ifHCInUcastPkts と ifHCOutUcastPkts の値が正しくありません。それぞれ、ユニキャストパケットの受信数と送信数を示すはずですが、ブロードキャスト / マルチキャストパケットもカウントされてしまいます。

○ 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。

○ atFilev2FileViewerName を利用する場合は、ファイルシステム上に 112 文字以上のファイル名を持つファイルが存在しないことを確認してください。

○ 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、show interface コマンドの administrative state は正しく UP を示しますが、SNMP 経由で取得する ifAdminStatus の値は誤って DOWN になっています。

3.8 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 sflow の UDP ポートを設定したとき、コンフィグに反映されず、保存、再起動で初期設定に戻ってしまいます。再起動した場合は、再度設定してください。SNMP マネージャーから設定した場合も同様です。

○ sFlow MIB の sFlowFsReceiver と sFlowCpReceiver の値を変更後、初期値に戻すためには sFlow を無効にする必要があります。

3.9 NTP

参照「コマンドリファレンス」/「運用・管理」/「NTP」

○ 実際には NTP サーバーと時刻同期が取れていない状態でも、show ntp associations コマンド上では同期済みと表示される場合があります。

○ すでに NTP サーバーが設定されている状態で、別のサーバーに設定を変更した場合、一度設定を削除した後、新規に設定を追加してください。削除せずに変更した場合、正しく同期しない場合があります。

○ 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

○ show ntp association detail コマンドの org time および xmt time の表示が、NTP による同期の有無にかかわらず、「06:28:16.000 UTC Thu Feb 7 2036」を示します。これは表示だけの問題で、システムの時計の動作には影響しません。

○ 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。

○ 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す。

3.10 端末の 1 画面当たり表示行数

参照「コマンドリファレンス」/「運用・管理」/「端末設定」

コンソールターミナルおよび仮想端末における 1 画面当たり表示行数は、実際のコンソールターミナルや仮想端末に表示できる行数より小さい値に設定してください。

3.11 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.

3.12 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」

○ show interface コマンドで表示される dropped カウンターがカウントされません。show platform port counters コマンドの ifInDiscards カウンターで確認してください。

○ AT-x210-9GT の SFP ポートでは、polarity コマンドによる MDI/MDI-X 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-x210-16GT/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。

○ 通信速度が 1000Mbps の SFP ポートで通信速度を 100Mbps に設定すると、設定をオートネゴシエーションに戻してもリンクダウンしたままになります。通信速度を 1000Mbps、デュプレックスモードを Full Duplex に設定する、または SFP モジュールを抜き差しすることで通信が復旧します。

3.13 スイッチポート

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」

○ egress-rate-limit コマンドでポートに送信レートの上限値を設定すると、上限値が設定されていないポートでも、送信レートが制限されることがあります。本現象は約 700Byte 以上のブロードキャスト、マルチキャストパケット送信時に発生します。

○ mru コマンドの「?」ヘルプで表示される最大値はサポート範囲外の値になっています。本製品がサポートする最大値は、コマンドリファレンスに記載されている下記の値ですので、この範囲内で使用してください。

mru <68-9216>（SFP ポートは 68-9000）

3.14 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検出時の動作に learn-disable アクションを設定しているとき、MAC アドレススラッシング検出後、MAC アドレスの学習が停止されないことがあります。

○ MAC アドレススラッシングプロテクション設定時、ループを検出したすべてのポートが、設定した動作を行います。

○ 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

3.15 ポートセキュリティー

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」

○ ジャンボフレームはポートセキュリティーの対象になりません。

○ ポートセキュリティーによって学習された MAC アドレスをエージアウトしないよう設定し、ポートセキュリティーの不正パケット受信時の動作を指定している場合、ポート

セキュリティーを無効にしてもスタティック MAC アドレスがコンフィグに残ったままになります。コンフィグに残ってしまったスタティック MAC アドレスは、no mac address-table static または、clear mac address-table コマンドで削除してください。

○ ポートセキュリティーにおいて、不正パケット受信時の動作を shutdown に設定している状態で、ポートセキュリティーを無効にすると、ログが正しく出力されず、show interface status コマンドでインターフェースのステータスが正しく表示されません。shutdown コマンドでインターフェースを無効にし、その後有効にすることで正しく表示されます。

○ ポートセキュリティーと UDLD は併用できません。

3.16 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 検出機能により、ループを検出した VLAN のポートが無効化されている場合、switchport enable vlan コマンドを VID を指定せずに実行しても、無効化されている VLAN のポートは有効になりません。LDF 検出機能により無効化されている VLAN のポートを有効にするには、switchport enable vlan コマンドを VID を指定して実行してください。

○ 本来、LDF 機能はアクセスリストのエントリーに空きがない場合には使用できませんが、アクセスリストのエントリーに空きがない場合でも、loop-protection loop-detect コマンドを 1 回入力し、エラーメッセージが表示された後に、再度同じコマンドを入力すると、コマンドが実行されてしまいます。
また、loop-protection loop-detect コマンドを 1 回入力し、エラーメッセージが表示された後に、当該のポートからアクセスリストのエントリーを削除すると、アクセスリストの登録数と最大数が正しく表示されなくなります。

○ タグ付きポートで LDF 検出の vlan-disable アクション（初期値）を使用する場合は、該当ポートのネイティブ VLAN をなしに設定してください（switchport trunk native vlan none）。

3.17 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。

3.18 パケットストームプロテクション

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」

リンク速度の異なるポートが混在する環境において、高速なポートにパケットストームプロテクションの設定を行った場合、高速なポートから低速なポートへの転送レートは、パケットストームプロテクションの設定値よりも低くなります。

3.19 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」

○ ポート認証と LACP を同一ポートで併用することはできません。認証ポートでは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）で設定するようにしてください。

○ スタティックチャンネルグループの対向機器の先に SNMP マネージャーが接続されている場合、スタティックチャンネルグループのメンバーポートをリンクアップした際、対向機器のリンクアップトラップが SNMP マネージャーに送信されないことがあります。

○ トランクグループ（saX, poX）に対して egress-rate-limit コマンドを実行した場合、送信レート上限値はトランクグループ全体に対してではなく、メンバーポート単位で適用されます。またこのとき、ランニングコンフィグ上でもトランクグループではなくメンバーポートに対する設定に変換されます（CLI からメンバーポートに対して同コマンドを実行するとエラーになりますが、スタートアップコンフィグから読み込んだときはエラーになりません）。

○ 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。

○ マルチキャストパケットの受信中に LACP チャンネルグループのメンバーポートをリンクダウンさせると次のようなログメッセージが出力されますが、動作には影響ありません。

2012 Nov 2 02:22:47 user.err x210-1 HSL[572]: HSL: ERROR: Can't find multicast FDB entry : Port port1.0.3 mac (0100.5e00.0002) VID 20

○ 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。

3.20 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」

○ EAP 透過機能で forward（受信した EAPOL パケットを VLAN に関係なくすべてのポートに転送する）に設定した場合、ポートミラーリングのソースポートからコピーされた EAPOL パケットとは別にミラーポートへ EAPOL パケットが転送されます。

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

○ Supplicant の再認証間隔（reAuthPeriod）の初期値は 3600 秒ですが、2 回目の再送間隔は約 1800 秒と前回の再送間隔の約半分になります。一定間隔で再送する場合は、auth timeout reauth-period コマンドで初期値以外の値を設定してください。

○ 802.1X 認証の Supplicant がログオフしても、ステータスが Connecting になりません。

○ 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。

○ 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。

○ インターセプトモード / プロミスキャスモードとセッションキープ機能（auth-web-server session-keep）を併用する場合、ログインするタイミングによってはセッションキープが期待どおり動作しないことがあります。その場合は、dot1x timeout tx-period コマンド（本来は 802.1X 認証用のコマンド）でセッションキープの URL 記憶時間を初期値の 30 秒よりも長くしてください（300 秒程度）。

○ 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た場合、未認証 Supplicant は認証を受けることができません。この状況は、最初に認証を受けた Supplicant が認証後に別の IP アドレスを割り当てられた場合や、認証済み Supplicant がリンクダウンをともなわずに切断された場合などに発生する可能性があります。これ

を回避するには、DHCP のリース時間を Supplicant の再認証間隔（auth timeout reauth-period コマンド）よりも大きく設定してください。

3.21 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」

○ vlan コマンドは数値とカンマ、ハイフンだけを受け付ける仕様ですが、指定値にこれら以外の文字が含まれていてもエラーになりません。このとき、意図した VLAN が作成されなかったり（例：「10,20」のつもりで「10.20」と誤入力すると「10」しか作成されない）、意図したのとは異なる VLAN が作成されたりする（例：「1001」のつもりで「100q」と誤入力すると「100」が作成される）場合がありますのでご注意ください。

○ 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 のプロミスキャスポートに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）を設定した場合、再起動後、ホストポートへパケットが転送されません。再起動後、プロミスキャスポートの設定を再入力すると、パケットが正常に転送されるようになります。

3.22 スパニングツリープロトコル

参照「コマンドリファレンス」/「L2 スイッチング」/「スパニングツリープロトコル」

○ チャンネルグループを作成後に MSTP を有効にすると、FDB に学習した MAC アドレスがケーブルがリンクダウンしてもクリアされません。チャンネルグループを作成する前に MSTP を有効にしてください。

○ RSTP/MSTP 使用時、スイッチがプロポーザルフラグを持つ BPDU を繰り返し受信する特殊な環境において、通信ができなくなることがあります。

3.23 EPSR

参照「コマンドリファレンス」/「L2 スイッチング」/「EPSR」

EPSR と MAC アドレススラッシングプロテクション併用時、EPSR のトポロジーチェンジにより、ループが検出される場合があります。EPSR とループガードを併用する場合は LDF 検出機能を使用してください。

3.24 DHCP Snooping

参照「コマンドリファレンス」/「L2 スイッチング」/「DHCP Snooping」

○ snmp-server enable trap コマンドで DHCP Snooping 関連のトラップを有効に設定しているとき、ip dhcp snooping violation コマンドでトラップを設定しようとすると、「SNMP trap for DHCP Snooping is disabled」というメッセージが表示され、トラップの設定が有効になりません。トラップを設定する場合は、ip dhcp snooping violation コマンド、snmp-server enable trap コマンドの順に入力してください。また、上記のエラーメッセージが表示された場合は、再度 snmp-server enable trap コマンドを入力することで、トラップの設定が有効になります。

○ ip dhcp snooping agent-option allow-untrusted コマンドを実行し、リレーエージェント情報オプション（オプションコード 82）を含む DHCP パケットの Untrusted ポートでの受信を有効（破棄しない）に設定しても、リレーエージェント情報オプションを含む DHCP パケットが破棄されます。

3.25 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」

ループバックインターフェースに IP アドレスを設定した時、ループバックインターフェース宛のルートエントリーがハードウェアテーブルに登録されません。

3.26 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。

3.27 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。

3.28 IGMP Snooping

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

○ ip igmp static-group コマンドで source パラメーターを指定しても、指定した送信元 IP アドレス以外からのマルチキャストパケットも指定したポートにだけ送信してしまいます。

○ スタティックマルチキャストグループが登録されている状態で、該当のマルチキャストグループと同じグループアドレス宛ての Join メッセージを他のポートから受信すると、その後 Leave メッセージを受信しても、そのポートには該当マルチキャストグループ宛のマルチキャストパケットが転送されるようになります。

○ IGMP Snooping の IGMP Querier 機能を有効にした状態で IP アドレスを変更すると、変更後正しい IP アドレスで Query を送信しません。IP アドレスを変更する場合は、IGMP Querier 機能を無効にし、変更後、再度有効にしてください。

○ 空の Exclude リストを持つグループレコードが存在している状態で、同グループに対する Exclude リスト追加要求（BLOCK_OLD_SOURCES）を受信すると、それ以降該当グループがタイムアウトしたり、脱退メッセージ（CHANGE_TO_INCLUDE{}）を受信したりしても、該当グループが正しく削除されません。

○ 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。

○ 複数ポートの IGMPv3 ホストから ALLOW_NEW_SOURCES レポートによる同一グループの登録があった後、いずれかのホストから該当グループの MODE_IS_INCLUDE レポートを受信すると、show ip igmp snooping statistics interface コマンドの Port member list の表示において、MODE_IS_INCLUDE を受信していないポートのタイマーも更新されます。これは表示だけの問題であり、MODE_IS_INCLUDE を受信していないポートは、最初に ALLOW_NEW_SOURCES で登録したときのタイマーが満了すると削除されます。

○ 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）。

○ VLAN ID のみ異なる、未登録の IP マルチキャストトラフィックをタグ付きポートで受信すると、該当マルチキャストトラフィックは、登録済みの VLAN を除く他のすべての VLAN でフラッディングされます。ただし、各 VLAN で該当マルチキャストグループのメンバーが登録されると、IGMP Snooping が正常に動作するようになり、フラッディングは行われなくなります。

○ IGMP Snooping をいったん無効にし、再度有効にする場合は、システムを再起動してください。

○ 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。

○ グローバルコンフィグモードの ip igmp snooping コマンド、インターフェースモードの ip igmp snooping コマンドのどちらか一方のみが実行されている状態では、不要なパケットが複製され出力されます。

○ IGMP Snooping の設定を無効で起動した場合、有効に変更しても、IGMP パケットが正しく転送されません。IGMP Snooping を無効から有効に設定変更した場合は、設定を保存し再起動してください。

3.29 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。

○ グローバルコンフィグモードの ipv6 mld snooping コマンド、インターフェースモードの ipv6 mld snooping コマンドのどちらか一方のみが実行されている状態では、不要なパケットが複製され出力されます。

○ MLD Snooping の設定を無効で起動した場合、有効に変更しても、MLD パケットが正しく転送されません。MLD Snooping を無効から有効に設定変更した場合は、設定を保存し再起動してください。

○ 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 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。

○ MLD Snooping をいったん無効にし、再度有効にする場合は、システムを再起動してください。

3.30 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」

○ ntp access-group コマンドによって NTP サービスに対するアクセス制御の設定を行う場合、ホストを許可（permit）する形式で標準 IP アクセスリストを作成していると、エントリーにマッチするホストのみでなく、マッチしないホストも時刻の同期を行うことができてしまいます。標準 IP アクセスリストを作成する際、許可するホストを指定したあとに、すべてを拒否（deny any）するエントリーを追加してください。

○ ハードウェアアクセスリストで UDLD パケットを破棄する設定は未サポートです。

3.31 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」/「トラフィック制御」/「ハードウェアパケットフィルター」

IGMP パケットはハードウェアパケットフィルターでフィルタリングできません。

3.32 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」

○ QoS の match eth-format protocol コマンドで AppleTalk パケットを制御できません。

○ 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。

3.33 Ping ポーリング

参照「コマンドリファレンス」/「IP 付加機能」/「Ping ポーリング」

Ping ポーリング機能を一旦無効化してから再度有効化すると、プロセス終了を示す以下のようなログが表示されますが、動作に問題はありません。
init: network/ping-poll main process (13750) killed by HUP signal

4 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。

4.1 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。

4.2 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。

4.3 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。

4.4 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。

5　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。

6　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。

7　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.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、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/