613-001467 Rev.N 140912

Allied Telesis

CentreCOM® *x200*シリーズ リリースノート

この度は、CentreCOM x200 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　5.4.4-1.1

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
AMF マスター	5.4.4-0.x	○	◎
	5.4.4-1.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）

マスター、x210/x200 とも **5.4.4-0.x** 系列で動作している状態から、**5.4.4-1.x** 系列にバージョンアップするときは、最初に x210/x200 を **5.4.4-1.x** 系列にバージョンアップしてから、AMF マスターをバージョンアップしてください。
先に AMF マスターを **5.4.4-1.x** 系列にバージョンアップした場合、バージョン **5.4.4-0.x** で動作している x210/x200 シリーズが 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。

「メンバープロダクト拡張ライセンス」の要不要については、3 ページの「4.2 AMF メンバープロダクト拡張ライセンス」もご覧ください。

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 **5.4.4-0.4** から **5.4.4-1.1** 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 ループガード（LDF 検出）の機能拡張

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」

○ ループガードの LDF 検出に fast-block 機能が追加されました。
fast-block 無効時は、ループを検出したすべてのポートでループ検出時の動作（以下、アクション）を実行しますが、fast-block 有効時は、ループを検出したポートのうち、ループの解除に必要なポートでのみアクションを実行し、ループの解除に不要なポートではアクションを実行しなくなります。
設定は loop-protection コマンドに追加された fast-block オプションで行います。なお、fast-block 機能と port-disable アクションは併用できません。
また、本機能追加にともない、show loop-protection コマンドの表示内容に本機能の有効・無効を示す欄が追加されました。

○ LDF 検出機能において、ループ検出後ただちにアクションを実行するのではなく、一定期間待機してからアクションを実行する設定が可能になりました。ループ検出後の待機時間は新しく追加された loop-protection action-delay-time コマンドで設定します（初期値は 0 秒）。本機能は、複数のスイッチで LDF 検出を使用している環境において、ループ発生箇所にもっとも近いスイッチでのみアクションを実行させたい場合に有効です。

3.2 Web 認証：ユーザー名・パスワードの文字数拡張

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 認証を行うユーザーのユーザー名とパスワードに、& = @ を使用できるようになりました。

3.3 アライドテレシスマネージメントフレームワーク（AMF）の機能拡張

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」

○ オートリカバリーまたはゼロタッチインストレーションが動作中、AMF メンバー側で、これらの機能が実行中であることが視覚的に判断できるように LED が点滅するようになりました。
- オートリカバリーまたはゼロタッチインストレーションが動作中は、機器本体のポート LED が 0.5 秒ごとに 1 つずつ点灯します。すべて点灯したら、いっぺんにすべての LED が消灯して、また順に点灯を繰り返します。
- オートリカバリーまたはゼロタッチインストレーションに失敗した場合は、機器本体のポート LED が 1.5 秒間隔ですべて点灯 / 消灯を繰り返します。この際、atmf recover コマンドによる手動復元を選択すると、LED が消灯します。

なお、この機能による LED の点灯動作中は、findme コマンドおよび ecofriendly led コマンドは機能しません。

○ AMF ノードをオートリカバリーするため前提条件である「AMF クリーン状態」を 1 コマンドで実現する atmf cleanup コマンドが追加されました。

○ 新規ノードのファームウェアやコンフィグを事前設定し、AMF ネットワーク内の場所（新規ノードの接続先となる既存ノードのポート）と関連付けることにより、新規ノードを接続したときにオートリカバリーと同じ要領で新規ノードの自動セットアップ（ゼロタッチインストレーション）を行えるようになりました。

事前設定情報は新しく追加された atmf provision node clone コマンドか atmf provision node create コマンドで作成し、その他の各種 atmf provision node xxxx コマンドで編集します。また、事前設定情報を既存ノードのポートに関連付けるには、インターフェースモードの atmf provision コマンドを使います。

○ 同一ポート上でスパニングツリープロトコルと AMF を併用できるようになりました。

○ AMF ノードの一括バージョンアップ時に、ファームウェアイメージファイルの転送と起動用ファームウェアの設定変更だけを行い、再起動までは行わない動作が可能になりました。これは、既存の atmf reboot-rolling コマンドの代わりに、新しく追加された atmf distribute firmware コマンドを使うことで実現できます。

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 **5.4.4-0.4** から **5.4.4-1.1** 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 show system コマンド、show license コマンドの表示項目変更

参照 「コマンドリファレンス」/「運用・管理」/「システム」

show system コマンドから「User Configured Territory」欄が削除されました。また、show license コマンドの「OEM Territory」欄が「Board region」欄に変更されました。

4.2 AMF メンバープロダクト拡張ライセンス

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」

ファームウェアバージョン **5.4.4-0.x** では、x210/x200 シリーズ（**5.4.4-0.x**）をメンバーとして管理する場合、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したが、本バージョンからは同ライセンスが不要となります。
なお、本変更に関連して、x210/x200 シリーズを AMF メンバーと使用する場合、マスターと x210/x200 のファームウェアバージョンの組み合わせに関して制限事項があります。詳しくは 1 ページの「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」をご覧ください。

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 **5.4.4-0.4** から **5.4.4-1.1** 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 異なる機種のファームウェアイメージファイルを boot system コマンドで指定しても エラーになりませんでしたが、これを修正しました。

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

5.3 copy コマンドにおいて、コピー元ファイルをワイルドカードで指定した場合、該当ファイルを TFTP サーバーのサブディレクトリーにコピーできませんでしたが、これを修正しました。

5.4 copy コマンド実行時に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。

5.5 aaa local authentication attempts max-fail コマンドで設定されている回数連続してログインに失敗しても、ログインロックアウトがかかりませんでしたが、これを修正しました。

5.6 email ログ機能使用時、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ていましたが、これを修正しました。

5.7 IGMP パケットの処理に問題があり、不要なログが出力される場合がありましたが、これを修正しました。

5.8 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。

5.9 AT-SYSINFO-MIB（プライベート MIB）を取得できませんでしたが、これを修正しました。

5.10 NTP サービスに対するアクセス制御の設定をした場合に、正常に起動できなかったり、関連プロセスが異常終了する場合がありましたが、これを修正しました。

5.11 NTP の設定をしていないにもかかわらず NTP request に応答していましたが、これを修正しました。

5.12 IPv4 Telnet サーバーを無効化できませんでしたが、これを修正しました。

5.13 IPv6 Telnet サーバーが正常に動作しませんでしたが、これを修正しました。

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

5.15 LDF 検出の port-disable アクションが実行されているポートをリンクダウンさせると、その後リンクアップしなおしたときに LDF が送信されなくなっていましたが、これを修正しました。

5.16 show platform port counter コマンドの ifInDiscards がレイヤー 2/ レイヤー 3 でユニキャスト受信時にカウントアップしていた問題を修正しました。

5.17 異なるポートに接続された同一グループ所属のマルチキャストホストが同時に脱退すると、Invalid Rexmit HRT（3）! のエラーログを誤って表示していましたが、これを修正しました。

5.18 QoS ストームプロテクション機能で portdisable アクションを設定しているとき、storm-downtime（設定単位は秒）の秒数を storm-window（設定単位はミリ秒）の秒数以上に設定していると、storm-downtime を経過してもアクションが解除されず、通信ができなくなっていましたが、これを修正しました。

5.19 mls qos enable コマンドを一旦無効にし、再度有効にすると本来送信キュー 0 を通るはずのパケットがキュー 4 を使用して通信されていましたが、これを修正しました。

5.20 AMF ノードに 64 文字のノード名を設定すると該当ノードにリモートログインできませんでしたが、これを修正しました。

5.21 トランクグループ（LAG）の AMF 接続ポートがリンクアップ・リンクダウンを繰り返すと、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。

5.22 起動した AMF ノードが、既存 AMF ドメインのドメインコントローラーになった場合、該当ノードから他のノードへの AMF リモートログインが正常に行えないことがありましたが、これを修正しました。

5.23 AMF 仮想リンク使用時、仮想リンクで接続されたノードと同じ AMF ドメイン内でネットワーク構成に変化が起きた場合、該当ドメインが 2 つに分断されていましたが、これを修正しました。

5.24 リング構成の AMF ネットワークにおいて、リング内の AMF メンバーを取り外しても、AMF ネットワーク上の情報が更新されないことがありましたが、これを修正しました。

5.25 AMF 仮想リンクで AMF ネットワークに接続しているノードにおいて、AMF 仮想リンクの接続ポートを切断した場合、該当ノード配下のノードが AMF ネットワークから離脱したことをマスターが認識できないことがありましたが、これを修正しました。

5.26 リング構成の AMF ネットワークにおいて、あるノードのリング接続ポートを両方ともリンクダウンさせ、再度リンクアップさせると、AMF ネットワーク上でストームが発生することがありましたが、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 **5.4.4-1.1** 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。

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 に所属するポートを持つ 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。

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。

○ 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。

○ 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」/「端末設定」

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。

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」/「インターフェース」

○ AT-x200-GE-52T の SFP ポートで、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-x200-GE-52T 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。

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 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」

1518 オクテットより長いパケットを受信しても show platform port counters コマンドの OversizePkts 値がカウントされません。

6.18 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

6.19 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。

6.20 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。

6.21 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. 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

○ 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。

○ auth-web method コマンドで認証方式を変更した場合は、対象ポートをいったんリンクダウンさせ、その後リンクアップさせてください。

○ 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 パラメーターはサポート対象外になります。

○ 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。

○ 802.1X 認証が有効化されたポートがリンクアップする際、誤って以下のログが出力されますが、動作に影響はありません。

Interface portx.x.x: set STP state to BLOCKING

○ 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。

6.22 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。

○ 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。

○ 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。

6.23 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。

○　2000pps を超える速度で ARP Request を受信すると、それに対する応答ができない場合があります。

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」

○　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。

○ 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。

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 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。

6.30 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。

6.31 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。

○ 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。

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 フィーチャーライセンス AT-x200-GE-FL02 と AT-x200-GE-FL03

ファームウェアバージョン **5.3.4A-3.4** より、AT-x200-GE-28T/52T 共通の IPv6 ライセンス「AT-x200-GE-FL02」とアプリケーションライセンス「AT-x200-GE-FL03」をサポートしました。既存の IPv6 ライセンス「AT-x200-GE-28T-IPv6」と「AT-x200-GE-52T-IPv6」はファームウェアバージョン **5.3.4A-3.4** 以降でも引き続き使用できます。

7.2 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。

7.3 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.J）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。

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）	16 ※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
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）	40
マルチプルダイナミック VLAN（装置あたり）	120
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 8 グループ、LACP は 8 グループ設定可能。合わせて 16 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 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。

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「AT-x200-GE-28T/AT-x200-GE-52T 取扱説明書」（613-001396 Rev.B）、コマンドリファレンス「CentreCOM x200 シリーズ コマンドリファレンス」（613-001463 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/