613-002035 Rev.A 141010

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 5.4.4-0.5

2 重要：注意事項

2.1 ファームウェアバージョン 5.3.4A-1.2 リリース前に IPv6 ライセンスを購入された方へ

ファームウェアバージョン **5.3.4A-1.2** リリース前に IPv6 ライセンスを有効化した機器で UDLD/SNMP の IPv6 対応機能を使用する場合は、IPv6 ライセンスのライセンスパスワードを更新する必要がありますので、弊社サポートセンターまたは保守契約締結時にご案内差し上げております「窓口のご案内」記載の窓口までご連絡ください。

2.2 ファームウェアバージョンアップ時の注意事項

ファームウェアバージョンアップを実施する際は、show memory コマンドでメモリーの空き容量を確認して下さい。free の数値が 45000KByte を下回る場合、ファームウェアバージョンアップに失敗することがありますので、本製品の電源 OFF/ON を実施後、ファームウェアバージョンアップを実施して下さい。
なお、free の数値が 45000KByte 超える場合でも、ファームウェアバージョンアップ時に解析用のログが生成される場合がありますが、ファームウェアバージョンアップに影響はありません。

2.3 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 **5.4.4-0.5** 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。

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

3.2 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。

3.3 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。

4 本バージョンでの制限事項

ファームウェアバージョン **5.4.4-0.5** には、以下の制限事項があります。

4.1 システム

「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。

4.2 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。

4.3 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。

4.4 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。

4.5 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。

4.6 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。

4.7 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。

4.8 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。

○ 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。

4.9 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.

○ IPv4 Telnet サーバーの無効化、IPv6 Telnet サーバーの有効化および無効化が正しく動作しません。

4.10 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-x200-GE-52T 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。

4.11 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」

○ 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。

○　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。

4.12 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

4.13 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。

4.14 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。

4.15 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

○ 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。

○ 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。

4.16 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。セカンダリー VLAN を削除する場合は、事前に private-vlan association コマンドの設定を削除してください。

○ 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。

4.17 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。

4.18 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。

4.19 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。

4.20 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。

○ 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) ! のエラーログが出力されます。これは、グループエントリーを手動で削除した場合も、タイマー満了で自動的に削除された場合も同様です。

4.21 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 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

4.22 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。

4.23 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。

4.24 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。

○ 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。

5 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。

5.1 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。

5.2 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。

5.3 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。

6 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。

7　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。

8　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.G）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/