613-001683 Rev.Y 151218

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 5.4.5-2.1

2 重要：注意事項

2.1 5.4.5-0.1 より前のバージョンからバージョンアップする方へ

バージョン 5.4.5-0.1 より AMF パケットフォーマットが変更されました。5.4.5-0.1 以降のバージョンで、AMF とアクセスリストを併用する場合、AMF マネージメントサブネット（atmf management subnet ※）内の通信を許可するようにしてください。

※ 初期値は 172.31.0.0/16

2.2 ファームウェアバージョンアップ時の注意事項

タイムゾーンの設定が入っている状態で 5.4.3 以前から、5.4.4 以降のファームウェアへバージョンアップした場合、バージョンアップ後にタイムゾーンの設定を反映させるため、再度システムの再起動が必要となります。

2.3 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/3.x 5.4.5-x.x
AMF マスター	5.4.4-0.x	○	◎	◎
	5.4.4-1.x	×	◎	◎
	5.4.4-2.x/3.x 5.4.5-x.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 **5.4.5-1.2** から **5.4.5-2.1** 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　マネージメント ACL

参照 「コマンドリファレンス」/「運用・管理」/「端末設定」

製品へのリモートアクセス（Telnet/SSH）を標準アクセスリストで制御するマネージメント ACL 機能をサポートしました。追加したコマンドは以下の通りです。

- vty access-class
- vty ipv6 access-class

3.2　ループガードの機能拡張

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」

○　QoS ストームプロテクション（QSP）機能が、ログメッセージの出力と SNMP トラップの送信に対応しました。

○　ループガード（LDF/MAC アドレススラッシングプロテクション /QSP）のアクション実行中にポート LED を特定のパターンで点滅させることにより、アクションの実行を視覚的に知らせる機能（findme trigger コマンド）をサポートしました。

3.3　スタティック /LACP チャンネルグループの設定可能数柔軟化

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」

これまで、スタティックチャンネルグループと LACP チャンネルグループはそれぞれ 4 つまでしか作成できませんでしたが、本バージョンからはスタティックチャンネルグループと LACP チャンネルグループをあわせて 8 つまで作成できるようになりました。

3.4　Web 認証画面のメッセージ言語切り替え（日英）

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 認証画面に表示される基本的なメッセージの言語を英語と日本語から選択できるようになりました（auth-web-server page language コマンド）。初期設定は英語です。

3.5　ポート認証用の RADIUS 属性追加・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」

ポート認証機能において、認証要求パケットに下記の RADIUS 属性を付加し、RADIUS サーバーに追加情報を通知できるようになりました。

○　Service-Type 属性：RADIUS サーバーに認証方式を通知する
○　NAS-Identifier 属性：RADIUS サーバーに認証ポートの所属 VLAN を通知する

初期設定では上記属性を付加しませんが、それぞれ auth radius send service-type、auth radius send nas-identifier コマンドで有効化できます。

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 **5.4.5-1.2** から **5.4.5-2.1** 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 起動時のシステム時刻チェック

参照 **「コマンドリファレンス」/「運用・管理」/「システム」**

スタートアップ時にシステム時刻をチェックし、1999 年 23 時 59 分 59 秒以前であった場合は、2000 年 1 月 1 日 0 時 0 分 0 秒にセットするようになりました。
また、上記プロセスにより時刻が変更された場合は以下のようなログが記録されます。

- user.warning awplus clockcheck: Fixing invalid system time(Thu Jan 1 12:00:26 1970)

4.2 ログ

参照 **「コマンドリファレンス」/「運用・管理」/「ログ」**

○ DDM（Digital Diagnostic Monitoring）対応モジュール挿抜時のログメッセージを変更しました。

抜いた場合

変更前
HPI: HOTSWAP Pluggable [IFNAME] hotswapped out: [Module_Name]
変更後
Pluggable[724]: Pluggable [Module_Name] removed from [IFNAME]

挿した場合

変更前
HPI: HOTSWAP Pluggable [IFNAME] hotswapped in: [Module_Name]
変更後
Pluggable[738]: Pluggable [Module_Name] inserted into [IFNAME]

○ コマンド実行時のログメッセージにおいて、そのコマンドを実行した端末の接続元 IP アドレスもしくはインターフェースが表示されるように仕様を変更しました。

4.3 MAC アドレススラッシングプロテクション

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」**

MAC アドレススラッシングプロテクションにおいて、アクション実行時のログメッセージに、MAC アドレス、ポート情報、VLAN 情報が付与されるようになりました。

4.4 バーチャル LAN

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」**

LAG インターフェース（saX、poX）に VLAN クラシファイアを設定できていましたが、設定できないように仕様変更されました。リンクアグリゲーションと VLAN クラシファイアを併用する場合は、LAG インターフェースではなくメンバーポートに設定するようにしてください。

4.5 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 mode master コマンドを実行した際に表示されるエラーメッセージを以下に変更しました。
Master Node support is not available.

4.6 ログレベルの変更

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD」

下記メッセージのログレベルを warning から informational に変更しました。
NSM[1414]: [MLD-DECODE] Socket Read: No MLD-IF for interface

4.7 QoS

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 0 と設定した場合であっても L2 トラフィックがマッチしていましたが、IP パケットのみにマッチするように修正しました。

○ QoS ポリシーマップが内部システム ACL よりも優先制御されていましたが、内部システムのハードウェア ACL が優先されるように変更されました。

○ unknown unicast に対しては、ルートのタイプにより受信キューが Q0 または Q1 に変更されていましたが、常に Q0 を使用するように変更されました。

4.8 show atmf node コマンド

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」

スタック可能なスイッチはすべて S と表示されていましたが、VCS 機能を no stack enable で無効にした場合、N と表示されるよう仕様変更されました。

5 本バージョンで修正された項目

ファームウェアバージョン **5.4.5-1.2** から **5.4.5-2.1** 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 Linux Kernel に関する脆弱性（CVE-2015-1465）への対策を行いました。

5.2 OpenSSL 脆弱性（CVE-2015-1788、CVE-2015-1790 ～ 1793、CVE-2015-4000）への対策を行いました。

5.3 Linux Kernel に関する脆弱性（CVE-2015-5364 および CVE-2015-5366）への対策を行いました。

5.4 DNS への問い合わせ機能を有効にすると、起動時に snmpd のエラーメッセージが表示され、コンフィグの読み込みに時間がかかることがありましたが、これを修正しました。

5.5 特権 EXEC モードへの移行権限を持たないユーザーが enable コマンドを実行する場合の以下の問題を修正しました。

- enable password コマンドを CLI から動的に設定した場合、前記ユーザーが enable コマンドを実行してもパスワードの入力を求めるプロンプトが表示されない。
- enable password コマンドが設定されていないにもかかわらず、設定を保存して再起動すると、前記ユーザーが enable コマンドを実行したときに特権パスワードの入力を求めるプロンプトが誤って表示される。

5.6 TFTP の転送速度が遅くなっていましたが、これを修正しました。

5.7 ログイン認証に RADIUS サーバーを使用している場合、RADIUS サーバーでユーザーに対する特権レベルを変更しても、Authenticator を再起動しない限り、そのユーザーは変更前の特権レベルでログインしてしまっていましたが、これを修正しました。

5.8 RADIUS サーバーや TACACS+ サーバーでのユーザー認証による CLI ログイン時、ユーザー認証データベースに同一ユーザー名が登録されている場合は、ユーザー認証データベース側の権限レベルを使用していましたが、これを修正しました。

5.9 RADIUS サーバーから受信したパケット内に 49 オクテット以上の State 属性が含まれていた場合、その属性を削除してしまうことがありましたが、これを修正しました。

5.10 NTP クライアント機能使用時、NTP によってシステム時刻が西暦 2000 年よりも前に変更されると、その後 show log コマンドを実行してもログが表示されなくなることがありましたが、これを修正しました。

5.11 SNMPv3 のユーザーを削除したときは、設定を保存して再起動する必要がありましたが、これを修正しました。

5.12 インターフェースの状態が約 248 日間変更されないと、show interface コマンドで表示される Time since last state change 欄の内容が不正な値になっていましたが、これを修正しました。

5.13 ポートセキュリティーが設定されたポートに、MAC aging を無効にするために no switchport port-security aging を設定した時に、極稀に製品が再起動することがありましたが修正されました。

5.14 thrash-limiting action learn-disable と thrash-limiting timeout 0 を併用した場合のエラーメッセージが % ではじまっていませんでしたが、これを修正しました。

5.15 LDF 検出機能を無効にし再度有効にすると、ログメッセージが生成されませんでしたが、これを修正しました。

5.16 VCS 構成のスイッチと LACP で接続している状況において、対向スイッチでマスター切り替えが発生するとエラーログを出力していましたが、これを修正しました。

5.17 LACP を有効にしたポート上で RIP などの予約マルチキャストパケットを受信するとエラーメッセージを出力することがありましたが、これを修正しました。

5.18 IEEE 802.1X 認証機能を無効にしているとき、show dot1x コマンドを実行してもエラーメッセージを出力しませんでしたが、これを修正しました。

5.19 HTTPS にて Web 認証を使用した際、不正な通信を行うと機器が再起動してしまうことがありましたが、これを修正しました。

5.20 vlan classifier activate コマンドが適応されているポートがリンクアップしている状態で、no vlan classifier activate を実行した場合、筐体宛て通信ができなくなることがありましたが、これを修正しました。

5.21 マルチプルダイナミック VLAN 使用時に、認証成功しているにもかかわらず通信できないことがありましたが、これを修正しました。

5.22 デフォルトコンフィグで起動後、show mac address-table コマンドを入力すると内部的に使われるブロードキャスト MAC アドレスが登録されているように表示されていましたが、これを修正しました。

5.23 認証済みの Supplicant の情報が show arp コマンドで正しく表示されませんでしたが、これを修正しました。

5.24 マルチキャスト MAC アドレスを持つホストを ARP 登録した際、フラッディングしないにもかかわらず show arp 上は flood と表示されていましたが、これを修正しました。

5.25 ip igmp snooping routermode address コマンドで制御用マルチキャストグループアドレスを設定している場合、IGMP Snooping が正しく機能せず、配送すべきでないポートにもマルチキャストパケットが転送されていましたが、これを修正しました。

5.26 QoS 有効時、本体宛て ARP reply が低い優先度のキューで取り扱われる場合がありましたが、これを修正しました。

5.27 リブートローリングの失敗によりローカルエリアが孤立した場合、AMF コントローラー上で show atmf area コマンドを実行すると reachable と表示されていましたが、これを修正しました。

5.28 AMF エリアリンクを物理ポートによる接続から、仮想エリアリンクに動的に変更した場合、エリアマスターを再起動するまで仮想エリアリンクが動作しませんでしたが、これを修正しました。

5.29 show atmf detail を実行した際、ドメインの IP 情報が誤って表示されていましたが、これを修正しました。

5.30 AMF コントローラーを使用している環境で AMF メンバーのオートリカバリーを実行する場合は、メンバーがローカルマスターより先にコントローラーにバックアップデータを問い合わせていましたが、これを修正しました。

5.31 AMF のローカルマスターとメンバーがオートリカバリーにより復旧した後、ローカルマスターからメンバーへのリモートログインが一時的にできなくなりましたが、これを修正しました。

5.32 AMF メンバーが離脱した際、AMF のメンバーの管理情報が記録されている .configs/atmf-links.conf の中からエントリーが削除されないことがありましたが、これを修正しました。

5.33 AMF と EPSR の併用時、EPSR リングのダウン、アップが発生した場合に AMF の Blocking ポートの位置が変化することがありましたが、これを修正しました。

5.34 中間階層のドメインコントローラーが AMF ネットワークからはずれた場合、既に存在しないにも関わらずノードリストに表示されていましたが、これを修正しました。

5.35 AMF 仮想リンクを使用している AMF ネットワークで、リブートローリングを実施すると、メンバーノードの ATMFD が再起動することがありましたが、これを修正しました。

5.36 AMF クロスリンクで構成されたリング内の機器で atmf cleanup コマンドを実施すると、リカバリーに失敗していましたが、これを修正しました。

5.37 マスターからのホップ数が 4 以上ある AMF ネットワーク内でトポロジーチェンジが発生すると、エッジの AMF ノードが異常終了してしまう場合がありましたが、これを修正しました。

5.38 AMF を使用している環境で AMF マネージメントサブネットを変更した場合に、変更前の AMF マスターの IP アドレスを NTP サーバーとして保持したままとなっていましたが、これを修正しました。

5.39 AMF マネージメント VLAN 内でパケットストームが発生すると AMF マスターからメンバーが認識できなくなっていましたが、これを修正しました。

5.40 show atmf links コマンドで表示されるリスト上から area-link に所属しているトランクグループが削除できませんでしたが、これを修正しました。

5.41 atmf network-name コマンドが設定されていない状態で「no atmf enable」を実行すると HSL エラーログが表示されていましたが、これを修正しました。

5.42 HTTP リクエストに Host パラメーターが含まれない場合、関連プロセスが再起動することがありましたが、これを修正しました。

5.43 ユーザー認証方式として RADIUS を設定している場合、GUI にログインできない場合がありましたが、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 **5.4.5-2.1** 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）。

○ 検索ドメインリスト（ip domain-list）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エントリーを使用しません。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。

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。

○ 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。

○ do コマンド入力時、do の後にコマンド以外の文字や記号を入力しないでください。

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」

○ ファイル名にスペースは使用できません。

○ move コマンドでファイルを移動する時、移動先に同じ名前のサブディレクトリーが存在する場合、移動に成功したというメッセージが表示されますが、実際には成功していません。その場合は、ファイル名を変更してから移動してください。

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。

○ 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。

6.6 スクリプト

参照「コマンドリファレンス」/「運用・管理」/「スクリプト」

間違ったコマンドを入力したスクリプトファイルを実行した場合、本来ならば、コンソール上に "% Invalid input detected at '^' marker." のエラーメッセージが出力されるべきですが、エラーメッセージが出力されないため、スクリプトファイルが正常に終了したかのように見えてしまいますが、通信には影響はありません。

6.7 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。

○ 定時トリガー（type time）を連続で使用する場合は 1 分以上の間隔をあけてください。連続で実行すると show trigger counter で表示される Trigger activations のカウンターが正しくカウントされません。

6.8 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ snmp-server enable trap コマンドにおいて、「sn enable trap」などと入力を省略した場合、入力したコマンドがホスト名欄に表示されコマンドが認識されない、または、コンソールの表示が乱れることがあります。コマンドは tab 補完などを利用し省略せずに入力してください。

○ 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。

○ SNMP マネージャーから MIB 取得要求を連続的に受信すると、"ioctl 35123 returned -1" のようなログが出力されることがありますが、通信には影響ありません。

6.9 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。

6.10 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。

6.11 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。

6.12 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.

6.13 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"
```

○ SSH ログイン時、ログアウトするときに以下のログが表示されますが、動作に影響はありません。
23:50:43 awplus sshd[2592]: error: Received disconnect from 192.168.1.2: disconnected by server request

○ manager 以外のユーザー名でログインする際、SSH 接続に RSA 公開鍵を使用した場合であってもパスワードが要求されますので、ユーザー名に紐付くパスワードを入力してください。

○ AlliedWare 製品から AlliedWare Plus 製品への SSH 接続は未サポートです。

6.14 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。

6.15 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。

○ ミラーポートとして設定されたポートは、どの VLAN にも属していない状態となりますが、mirror interface none で、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 ） にポート情報が当該 VLAN に表示されません。ポートに mirror interface コマンドでソースポートのインターフェースとトラフィックの向きを設定した後、設定を外すとポート情報が正しく表示されるようになります。

6.16 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。

○ MAC アドレススラッシングの検出を SNMP トラップで通知する際、MAC アドレススラッシングプロテクションによるアクションの実施を知らせるトラップが、MAC アドレススラッシングの検出を知らせるトラップよりもわずかに先に送信されることがあります。この現象はトラップでのみ発生し、show log の表示では入れ替わることはないため、実際の順番はログを確認してください。

○ LDF 検出と QoS ストームプロテクションを併用する場合、両方の検出時の動作に port-disable を選択しないでください。どちらか片方は、異なる動作を選択してください。

○ LDF 検出機能でループを検知し、検出時の動作が行われているとき、当該ポートが所属する VLAN を変更しないでください。VLAN を変更した場合、検出時の動作に問題はありませんが、show loop-protection コマンドによる表示が旧 VLAN と新 VLAN の両方表示されます。

6.17 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。

○ トランクグループ（saX、poX）を無効化（shutdown）した状態でメンバーポートを削除しないでください。

6.18 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。

○ 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。

○ 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。

○ 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。

○ 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。

○ 認証成功後の Supplicant の情報が ARP テーブルに登録されないことがありますが、動作に影響はありません。

6.19 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。

○ 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。

○ インターフェースにプライベート VLAN の設定をしたままプライベート VLAN を削除することはできません。プライベート VLAN を削除する場合は次の手順で VLAN を削除するようにしてください。

1. インターフェースに対して switchport mode private-vlan コマンドを no 形式で実行して VLAN の設定を解除する。
2. private-vlan コマンドを no 形式で実行してプライベート VLAN を削除する。

6.20 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。

6.21 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。

○ EPSR スーパーループプリベンション構成において、優先順位の低いリングの一部が切れている状態かつ、Common Link が切れている状態で、その Common Link を持つ機器が、再起動をすると、優先順位の低いリングへの接続ポートがリンクアップしているにも関わらず、ポートのステータスがブロッキングになっているため、通信ができません。正しく配線されていることを確認してから起動するようにしてください。

6.22 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。

○ VLAN インターフェース（vlanX）に対して mtu コマンドを実行すると、ランニングコンフィグ上では該当 VLAN のメンバーポートに対しても mtu コマンドを適用した状態になります。そのため、その状態で設定を保存すると、再起動時スイッチポートに対して mtu コマンドを実行できないためエラーメッセージが出力されますが、動作には影響ありません。

6.23 経路制御

参照「コマンドリファレンス」/「IP」/「経路制御」

show ip route コマンドで、デフォルトルート（0.0.0.0/0）にマッチするアドレスを指定した場合、経路が正しく表示されませんが、これは表示上の問題で実際の通信には問題ありません。

6.24 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。

○ 本製品の ARP Request に対して、ブロードキャストアドレス宛ての ARP Reply が返ってきた場合、その情報は本製品の ARP キャッシュに登録されません。

6.25 IPv6

参照「コマンドリファレンス」/「IPv6」

○ 自身の IPv6 アドレス宛てに 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。

6.26 IPv6 インターフェース

参照「コマンドリファレンス」/「IPv6 ルーティング」/「IPv6 インターフェース」

受信したルーター通知（RA）パケットにより IPv6 インターフェースのアドレスを自動設定する場合、RA パケットに MTU オプションが設定されていてもその値を採用しません。

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。

○ IGMP Snooping 利用時、IGMP Querier を挟まないネットワーク上にマルチキャストサーバーとホストがいる場合、ホストが離脱した後もタイムアウトするまでパケットが転送され続けます。clear ip igmp コマンドで手動でエントリーを削除してください。

○ IGMP の Querier と IGMP Snooping 有効になっている機器が別に存在する場合、上位の Querier から Query を受け取った際に、レポート抑制機能によって自身がレポートを送信しますが、配下にグループメンバーが存在していない場合でも、Querier にレポートを送信してしまう場合があります。レポート抑制機能を無効化することで本事象は回避できます。

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。

○ clear ipv6 mld group * ですべてのグループを削除した場合、ルーターポートのエントリーも削除されてしまいます。clear ipv6 mld group ff1e::1 のように特定のグループを指定した場合は削除されないため、グループを指定し削除してください。また、削除されてしまった場合も MLD Query を受信すれば再登録されます。

○ 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 Snooping を無効にしても一部の MLD Snooping の機能が動作し続けます。このため、show コマンド上の MLD エントリーが更新されつづけたり、MLD のパケットを受信した際に MLD が動作していることを示すログが出力されます。

○ MLD Snooping を一時的に無効にして再度有効にする場合は、無効にしてから有効にするまでに約 5 分間隔を空けてください。

6.29 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」

○ ARP や IGMP など CPU で処理されるパケットに対してイングレスフィルターが正しく動作しません。
ARP に関しては、以下の設定でフィルターすることが可能です。

```
mls qos enable
access-list 4000 deny any any vlan 100
class-map class1
match access-group 4000
policy-map policy1
class default
class class1
interface port2.0.24
service-policy input policy
```

○ ハードウェア IP アクセスリストにおいて、アクションが copy-to-mirror または send-to-mirror のアクセスリストがポートに適用されているとき、mirror interface を別のポートに再設定する際は、以下の手順で行ってください。

1. 設定済みのポートからアクセスリストの設定を解除 (no access-group)
2. 設定済みのポートからミラーポートの設定を解除（no mirror interface）
3. 移行したいポートへミラーポートを再設定 (mirror interface none)
4. 移行したいポートへアクセスリストの設定 (access-group)

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。

○ ポリシーマップ名に「|」を使用しないでください。

○ 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。

○ mls qos enable コマンドを no 形式で実行しても、一部の mls qos 関連のコマンドがランニングコンフィグから削除されないことがあります。不要な場合は no 形式で実行して削除してください。

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。

○ DHCP プールが複数設定された環境で show ip dhcp binding コマンドを使用する際は、DHCP プール名やクライアントの IP を指定した状態で実行してください。

○ 多数の DHCP プールを作成している環境において、ネットワークアドレス部に 10 か 100 の数字を含む IP アドレス（10.1.1.1/24、172.16.100.5/24 など）を払い出した場合、10 の部分が 2 ～ 9 になっている別のアドレス（10.1.1.1 に対して 2.1.1.1 や 9.1.1.1 など）、および、100 の部分が 11 ～ 99 になっている別の IP アドレス（172.16.100.5 に対して 172.16.11.5 や 172.16.99.5 など）のリース情報が消えることがあります。

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 ネットワーク内にマスターノードが存在しない場合でも AMF ネットワークが構成できてしまいますが、AMF 機能は利用できません。

○ 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。

○ 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。

○ 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。

○ AMF バーチャルリンクの設定を削除した際、show atmf links detail で表示される「Special Link Present」が FALSE にならないことがあります。再起動することで正しく表示されます。

○ AMF ネットワーク名を変更すると、システム再起動を推奨するログの出力と共に、ノードの離脱、再加入が発生しますが、全ノードが再加入できないことがあります。AMF ネットワーク名を変更した後は、必ず再起動を行ってください。再加入できないノードに対しては、Telnet などでログインし、再起動を実施してください。

○ バックアップ先 SSH サーバーに接続できない状況では、「show atmf backup server-status」コマンドの応答に 1 分程度の時間がかかります。

○ AMF と EPSR の併用時、AMF マスターと AMF メンバー間のリンクタイプを、AMF クロスリンクから AMF リンクに変更した後は、AMF マスターと AMF メンバーそれぞれでリンクタイプ設定を保存して再起動してください。ただし、AMF 経由で AMF マスターから AMF メンバーのリンクタイプを変更すると、その時点で AMF の接続が切れてしまうため、設定の保存と再起動が AMF マスターから行えません。そのため、本設定の変更を行う場合には、AMF 経由ではできませんので、コンソールや TELNET/SSH で接続して行ってください。

○ AT-Vista Manager を使用時、DomainController/BackupDomainController になっている AMF メンバーの Management IPv6 Address がノード詳細画面に表示されません。

○ ファームウェアバージョン 5.4.5-0.x 以前のファームウェアを使用している機器と、AMF 仮想リンクで接続した際に、AMF ネットワークへ正常に参加できないことがあり

ます。接続するインターフェースの MTU 値を 1442 に変更することで正常に参加することができます。

○ 同一デバイス間で複数のエリア仮想リンクを使用している時、一方の設定を削除した場合、リンクステータスは Active のままとなります。この時、もう一方のリンクのリンクステータスに Active と表示されるべきですが何も表示されません。これは表示上だけの問題であり通信に影響はありません。

○ LACP と AMF を併用している場合、LACP チャンネルグループのメンバーポートがリンクダウンすると、次のようなエラーログが出力されますが、これはログのみの問題で、AMF や通信には影響ありません。
- kern.err XXXX kernel: Unexpected parent vlan4092 found for [IFNAME]
- kern.err XXXX kernel: Parent interface vlan4092 found while deleting [IFNAME]

6.33 Web GUI

参照「コマンドリファレンス」/「Web GUI」

Web GUI へのアクセス時、GUI Java アプレットの起動前と起動後の 2 回、ユーザー名とパスワードを入力する画面が表示されます。ログインするためにはどちらの画面でも手順 6 で設定したユーザー名とパスワードを入力してください。

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）以降でご確認ください。

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 ※1	8K
IPv4 ホスト（ARP）登録数 ※1	-
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 ※2
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 ※3※4※5
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 ※6
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 インスタンス数	-
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 システム内部で使用する値も含みます。
※2 スタティックチャンネルグループ、LACP それぞれ 8 グループまで設定可能となります。スタティックチャンネルグループと LACP を併用した場合、合わせて 8 グループまで設定可能となります。
※3 アクセスリストのエントリー数を示します。
※4 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。
※5 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 推奨値は 8

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.C）、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.M）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/