613-002006 Rev.C 150116

CentreCOM® *x310* シリーズ　リリースノート

この度は、CentreCOM x310 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　5.4.4-2.4

2　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 **5.4.4-1.1** から **5.4.4-2.4** 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。

2.1　リンクフラッピング検出機能

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」

リンクフラッピング検出機能（linkflap action コマンド）をサポートしました。本機能有効時は、特定のスイッチポートで 15 秒以内に 15 回以上リンクステータスが変動（ダウン→アップまたはアップ→ダウン）した場合、該当ポートを shutdown します。初期設定は無効です。

2.2　Web 認証の機能改善

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。

○　Web 認証画面のカスタマイズ機能が下記のとおり拡張されました。詳細はコマンドリファレンスをご覧ください。
- 新しく追加された auth-web-server page xxxx コマンドを用いて、Web 認証関連ページのタイトル、サブタイトル、ウェルカムメッセージ、認証成功メッセージなどを変更できるようになりました（ただし日本語は使えません）。
- 外部 Web サーバー上に用意した任意のログインフォームを Web 認証画面として使用することができるようになりました。

なお、既存のカスタマイズ機能はバージョンアップ後もそのまま使用できます。

○　Web 認証と DHCP Snooping の併用が可能になりました。

○　これまで Web 認証では、ネットワーク構成によって認証成功画面が表示されなかったり、認証成功後ログオフするための画面にアクセスできなかったりするケースがありましたが、本バージョンでは Web 認証機能の設計を見直し、そのようなケースでも認証成功画面やログオフ画面の表示が可能となりました。

○ これまで Web 認証では、ネットワーク構成に応じて設定内容を細かく調整する必要がありましたが、本バージョンからは基本的に Web 認証機能を有効化するだけで、さまざまなネットワーク構成に対応できるようになりました。

なお、これにともない、設定コマンドの削除・変更が行われています。詳しくは仕様変更 5.1（p.5）をご覧ください。

2.3 power-inline max コマンド

参照 「コマンドリファレンス」/「インターフェース」/「Power over Ethernet」

PoE スイッチポートから出力可能な電力の上限値を設定する power-inline max コマンド（インターフェースモード）をサポートしました。

2.4 IGMP Snooping におけるルーターポート登録アドレスのカスタマイズ

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、制御用マルチキャストグループアドレス宛てパケットを受信したときの動作を変更できるようになりました。新しく追加された ip igmp snooping routermode、ip igmp snooping routermode address コマンドを使うことで、どのアドレス宛てのパケットを受信したときに該当ポートをルーターポート（すべてのマルチキャストパケットを出力するポート）にするかを任意に設定できます。

3 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 **5.4.4-1.1** から **5.4.4-2.4** 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。

3.1 Web 認証の仕様変更

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」

○ Web 認証機能の機能改善 4.4（p.4）にともない、下記のコマンドが削除されました。

- auth-web-server mode
- auth-web-server http-redirect
- auth-web-server sslport
- auth-web-server blocking-mode

旧バージョンで HTTPS を有効化し、auth-web-server sslport コマンドを使用していた場合、バージョンアップ後のランニングコンフィグでは、同じ意味を持つ auth-web-server port コマンドに自動変換されます（特に設定変更は不要です）。

また、それ以外のコマンドがスタートアップコンフィグから読み込まれた場合は単に無視されますが、Web 認証の機能改善により旧バージョンでこれらのコマンドを設定していたのと同等の動作を行いますので、旧バージョンで前記のコマンドを使用していた場合もコンフィグの変更は不要です。

○ Web 認証機能の機能改善 2.2（p.1）にともない、auth-web forward コマンドの初期設定が変更されました。また、A.B.C.D パラメーターと dns、udp パラメーターの併用がサポートされました。

[旧バージョン]
すべての受信・転送が無効。

[本バージョン]

ARP、DHCP、DNS の受信・転送が有効。

旧バージョンで Web 認証を使用しており、なおかつ、ARP、DHCP、DNS の受信・転送を有効にしていなかった場合、バージョンアップ後は ARP、DHCP、DNS の受信・転送が有効な状態になりますので、これが望ましくない場合は下記のコマンドを実行して不要なパケットの受信・転送を無効化してください。

- no auth-web forward arp
- no auth-web forward dhcp
- no auth-web forward dns

4 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 **5.4.4-1.1** から **5.4.4-2.4** 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。

4.1 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。

4.2 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 パラメーターがサポート対象外でしたが、本バージョンから使用できるようになりました。

4.3 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ると、未認証 Supplicant が認証を受けられませんでしたが、本バージョンからは認証後に端末の Gratuitous ARP を受信した認証情報内の IP アドレスを書き換えるようになったため、認証時に IP アドレスが重複することがなくなりました。

4.4 Web 認証サーバーにおいて、HTTP 待ち受けポートがひとつもない状態のとき（初期設定で no auth-web-server intercept-port 80 を実行した状態）に、show auth-web-server コマンドを実行すると関連プロセスが異常終了していましたが、これを修正しました。

4.5 802.1X 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。

4.6 「no service power-inline」は未サポートでしたが、本バージョンから使用可能になりました。

4.7 VCS 無効時、show ip dhcp snooping binding および show ip dhcp snooping acl の表示結果に DHCP Snooping テーブル（バインディングデータベース）の情報が正しく反映されていませんでしたが、これを修正しました。

4.8 MLD Snooping 有効時、ルーターポートで MLD Report を受信した場合に、同ポートから該当 MLD Report を再送信することがありましたが、これを修正しました。

4.9 AMF ノード名が重複すると AMF ネットワークが分断されることがありましたが、これを修正しました。

4.10 VCS 構成の AMF ノードにおいて、スタティックチャンネルグループを AMF 接続ポートに設定している場合、該当ノードで VCS の reboot rolling を実行すると、一部のノードが AMF ネットワークに参加できなくなることがありましたが、これを修正しました。

4.11 AMF ノード名が重複したときにどちらかのノード名を「host_xxxx_xxxx_xxxx」形式に強制変更する動作が正しく行われないことがありましたが、これを修正しました。

4.12 VCS のマスター・スレーブ間で AMF ノード情報に不整合が生じることがありましたが、これを修正しました。

4.13 AMF クリーン状態のノードが自動検出メカニズムによって AMF ネットワークに参加した場合、このノードをワーキングセットから操作できないことがありましたが、これを修正しました。

4.14 VCS メンバーの起動中に、他の VCS メンバーの再起動や電源断が発生した場合、一部の設定が有効にならない場合がありましたが、機能改善により発生しなくなりました。

4.15 VCS の reboot rolling 後、「HAL_Link_Server filter 0x101260c0 returned error (-1) - recovered」のようなエラーメッセージが出力されることがありましたが、これを修正しました。

下記の項目は、ファームウェアバージョン 5.4.4-1.1 以前のリリースノートに制限事項として記載されておりますが、関連機能の改善により、本バージョンでは事象が発生しないことを確認したため、制限事項から除外いたしました。

4.16 （AT-x310-26FP/AT-x310-50FP のみ）機器を再起動すると、以下の誤ったログが表示されます。

- HSL: ERROR: Can't set port PoE LED state for portx.y.z

4.17 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す。

4.18 Web 認証と MAC ベース認証 /802.1X 認証の併用時に、プロミスキャスモードとダイナミック VLAN を使用する場合は、Supplicant のデフォルトゲートウェイとして本製品（Authenticator）を指定しないでください。

下記の項目は、Web 認証機能の機能改善 2.2（p.1）、仕様変更 3.1（p.2）にともない、本バージョンでは適用外となりましたので、制限事項から除外いたしました。

4.19 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。

4.20 インターセプト / プロミスキャスモードとセッションキープ機能が有効なとき、認証成功後にセッションキープが動作せずページが切り替わらないときがあります。その場合は、Supplicant 側で Web ブラウザーをいったん終了させ、再度立ち上げてアクセスしなおしてください。

下記の項目は、Web 認証機能の制限事項 5.23（p.11、p.12）「Web 認証とゲスト VLAN は併用できません。」により本バージョンでは適用外となりましたので、制限事項から除外いたしました。

4.21 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。

5 本バージョンでの制限事項

ファームウェアバージョン **5.4.4-2.4** には、以下の制限事項があります。

5.1 システム

参照「コマンドリファレンス」/「運用・管理」/「システム」

○ reboot/reload コマンドで stack-member パラメーターを指定した場合、確認メッセージが表示されますが、ここで Ctrl/Z や Ctrl/C を入力した場合はその後 Enter キーを入力してください。Ctrl/Z や Ctrl/C を入力しただけではコマンドプロンプトに戻りません。

○ USB メモリーを挿入したまま起動すると、LED が点灯・点滅しません。USB メモリーは起動後に挿入しなおしてください。

○ 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。

○ 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。

5.2 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。

5.3 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」

○ edit, mkdir, rmdir, show file, show file systems コマンドを使用して Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB 上のファイルにアクセスした場合、ASK-256-8GB/16GB/32GB 上のアクセス LED が点滅状態のままになることがあります。その場合は、「dir usb:/」のように、USB メモリーにアクセスする操作をもう一度行ってください。

○ ファイル名にスペースは使用できません。

○ USB メモリーを装着した際、エラーメッセージが表示されることがありますが、これは表示だけの問題であり、動作に影響はありません。

○ copy コマンドのコピー元として、ユーザー認証が必要な http URL は指定できません。該当する URL を指定してもエラーメッセージは出力されませんが、ファイルコピーには失敗します。

5.4 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。

5.5 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+ 認証を使用して VCS マスターにログイン後、他のスタックメンバーにリモートログインしている最中に、ほかの TACACS+ セッションが同じユーザー名、パスワードでログインすると、以下のメッセージが出力されます。
・ You don't exist, go away!

○ 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。

5.6 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。

5.7 RADIUS サーバー

参照「コマンドリファレンス」/「運用・管理」/「RADIUS サーバー」

○ server auth-port コマンドによりローカル RADIUS サーバーの認証用 UDP ポート番号を 63998 以上に設定しようとすると、関連プロセスが再起動するログが出力されます。また、上記の UDP ポート番号を使用してポート認証を行うことができません。

○ ローカル RADIUS サーバーに登録するユーザー名の長さは 63 文字までにしてください。

5.8 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。

○ 以下のログがコンソールに表示されないことがあります。
- Configuration update completed for portxxx
- Member x (xxxx.xxxx.xxxx) has become the Active Master

○ permanent ログにメッセージフィルターを追加した後、default log コマンドを実行してログ出力設定を初期値に戻しても、追加したメッセージフィルターが削除されません。メッセージフィルターを削除するには、log(filter) コマンドを no 形式で実行してください。

○ 起動時において、電源ユニットに関するログが不自然なタイミングで表示されます。

○ 複数の VLAN に所属するポートを持つラインカードを再起動または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。

5.9 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」

スクリプト機能を使って OSPF のルーティングプロセスを再起動することはできません。再起動が必要な場合はコマンドから直接実行してください。

5.10 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。

○ インターフェースのリンクステータスが 1 秒未満の短い間隔で変化した場合、該当インターフェースを監視するインターフェーストリガーが起動しない場合があります。

○ 「show trigger counter」で表示される定時トリガー（type time）の起動回数が正しくないことがあります。

5.11 LLDP

参照「コマンドリファレンス」/「運用・管理」/「LLDP」

○ VCS 構成時、LLDP MIB の lldpPortConfigAdminStatus は未サポートです。

○ トランクポートに LLDP を設定すると、show lldp neighbors interface コマンドで表示される LLDP 有効ポートが正しく表示されません。

5.12 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ VCS 構成のシャーシに GetNext Request を送信すると、SNMP が「no such object」と応答することがあります。

○ 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。

○ 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。

5.13 sFlow

参照「コマンドリファレンス」/「運用・管理」/「sFlow」

○ sFlow パケットを送信するスイッチポートをタグ付きポートに設定しないでください。

○ 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。

5.14 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 サーバーと同期されているのにもかかわらず、VCS スレーブ側の show log コマンド結果に、同期が取れていないことを表す以下のエラーメッセージが出力されることがあります。
- ntpd_intres[4295]: host name not found:

○ 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。

5.15 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。

5.16 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.

○ 非特権モードでホスト名を使用して、Telnet 経由でリモートデバイスにログインする場合は、ドメイン名まで指定してください。

5.17 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"
```

5.18 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」

○ IPv6 アドレスを持つインターフェースに show interface コマンドを入力した際の結果に、実際のホップリミットの値が表示されません。

○ LACP チャンネルグループがリンクダウンしているとき、show interface コマンドでは該当グループのパケットカウンターがすべて 0 と表示されます。

5.19 フローコントロール

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」

○ 10G ポートでは、show flowcontrol interface コマンドの RxPause カウンターが正しく表示されません。

○ 通信速度をオートネゴシエーションで決定しているとき、show flowcontrol interface コマンドで確認できる oper の状態が on になると、そのポートがリンクダウンした後も、表示が更新されません。これは表示のみの問題であり、動作に影響はありません。

○ フローコントロールとバックプレッシャーを同一ポートに設定し、フローコントロールを無効にすると、バックプレッシャーが動作しなくなります。フローコントロールとバックプレッシャーを同一ポートに設定しないでください。

5.20 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 送信間隔（loop-protection コマンドの ldf-interval パラメーター）を 1 秒に設定する場合、ループ検出時の動作持続時間（loop-protection timeout コマンド）は 2 秒以上に設定してください（初期値は 7 秒）。

○ 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

○ 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。

○ LDF 検出の port-disable アクションによってポートがシャットダウン状態になっていても、show interface コマンドの administrative state 欄には err-disabled ではなく UP と表示されます。またこのとき、MIB の ifAdminStatus も UP になります。LDF 検出のポート状態を確認するには、show loop-protection コマンドを使ってください。

5.21 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。

5.22 リンクアグリゲーション（IEEE 802.3ad）

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。

○ リンクアグリゲーションを設定した状態で、[no] mac address-table acquire コマンドを実行すると、不要なログメッセージが出力されますが、MAC アドレステーブルの自動学習機能には影響ありません。

5.23 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。

○ 802.1X 認証と Web 認証の 2 ステップ認証機能利用時に、ローカル RADIUS サーバーは使用できません。また、2 ステップ認証で ローカル RADIUS サーバー以外の

RADIUS サーバーを使用するときは、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。

○ 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

○ Web 認証とゲスト VLAN は併用できません。

○ Web 認証サーバーのセッションキープ機能有効時、Web 認証端末が認証画面にアクセスしてから認証に成功するまでの間に、端末上のバックグラウンドプログラム等が自発的な HTTP 通信を試みた場合、認証成功後に意図したページへリダイレクトされないことがあります。

5.24 Power over Ethernet

参照「コマンドリファレンス」/「インターフェース」/「Power over Ethernet」

○ PoE に対応した機器（AT-x310-26FP、AT-x310-50FP）と PoE に対応していない機器（AT-x310-26FT、AT-x310-50FT）が混在した VCS 環境において、power-inline enable コマンドを入力すると、PoE に対応していない機器に対するエラーメッセージが表示されますが、一部の非 PoE ポートの分しか表示されません。

○ power-inline enable コマンドを no 形式で実行し、PoE 給電機能を無効に設定すると、本来、show power-inline コマンドの Oper の表示が「Disabled」と表示されるべきですが、受電機器が接続されたポートでは「Off」と表示されます。

○ PoE 電源の電力使用量が最大供給電力を上回った場合、show power-inline interface detail コマンドの Detection Status は「Denied」と表示されるべきですが、「Off」と表示されてしまいます。
同様に、ポートの出力電力が上限値を上回った場合、「Fault」と表示されるべきですが、「Off」と表示されてしまいます。

○ ポートの出力電力が上限値を上回った状態で数分間放置すると、実際に接続している受電機器の電力クラスと異なる電力クラスが表示される、または「n/a」と表示されることがあります。また、これに伴って Max も実際とは異なる値が表示されます。ポートの出力電力が上限値未満に戻ると、表示も回復します。

○ ポートの出力電力が上限値を上回った状態のとき、show power-inline の Oper の表示が、実際の「Fault（ポートの出力電力が上限値を上回ったために給電を停止している）」ではなく「Denied（PoE 電源の電力使用量が最大供給電力を上回ったために給電を停止している）」となることがあります。

○ プリスタンダード方式の受電機器を接続した場合、ポートがリンクアップしないことがあります。ポートがリンクアップしないときは、ケーブルの抜き差しを行ってください。

○ 受電機器（PD）によっては、PoE ポートに接続してから給電が開始されるまで 30 秒程度かかる場合があります。

○ PoE に対応している x310 シリーズ（AT-x310-26FP/AT-x310-50FP）の PoE ポート同士を接続するときは、no power-inline enable で両ポートの PoE 機能を無効にしてください。

5.25 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」

○ 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。

○ switchport trunk allowed vlan コマンドの except パラメーターに、該当ポートのネイティブ VLAN として設定されている VLAN を指定しないでください。except パラメーターでネイティブ VLAN を指定した場合、設定内容が正しくランニングコンフィグに反映されず、実際の VLAN 設定状態との間に不一致が発生します。

○ 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。

○ エンハンストプライベート VLAN 使用時に、セカンダリーポート（端末接続用ポート）配下の端末から本製品に対する Telnet、Ping などを拒否するには、アクセスリストで通信を制限してください。

○ 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。

○ 511 個以上の VLAN を設定するか、511 個以上の VLAN が設定されたコンフィグを読み込んだとき、511 番目以降に作成された VLAN1 つごとに下記のようなログが出力されます。
  ・ user.err awplus HSL[1078]: HSL: ERROR: Could not create L3 interface in hardware for interface vlan534 834 ret(-6)
  また、その VLAN には IP を設定することができません。

5.26 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。

5.27 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」

spanning-tree enable コマンドは、STP、RSTP、MSTP どれにでも使用可能であるにもかかわらず、Description には enable multiple spanning tree protocol と誤った表示がされます。
STP を無効にするコマンドとして no spanning-tree enable" がありますが、ヘルプを表示させると、% Unrecognized command と誤った表示がされます。
spanning-tree xxxx enable コマンドで、xxxx の部分を変更しても、共通の Description である enable spanning tree protocol としか表示されません。

5.28 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。

5.29 フォワーディングデータベース

参照「コマンドリファレンス」/「L2 スイッチング」/「フォワーディングデータベース」

MAC アドレスをスタティック登録する mac address-table static コマンドにおいて、discard（破棄）アクションは動作しないため使用しないでください。

5.30 IP インターフェース

参照「コマンドリファレンス」/「L2 スイッチング」/「IP インターフェース」

ip directed-broadcast コマンドを設定している VLAN インターフェース上でディレクティドブロードキャストパケットを受信すると、他のインターフェースから該当 VLAN インターフェース配下へのディレクティドブロードキャストパケットを転送しなくなることがあります。その場合は、該当 VLAN インターフェースを shutdown → no shutdown してください。

5.31 経路制御

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御」

○ デフォルト経路を登録しているにもかかわらず、show ip route database コマンドで「Gateway of last resort is not set」と表示される場合がありますが、表示だけの問題で通信には影響ありません。

○ IP 経路が 20 エントリー以上登録されていると、デフォルト経路を登録しているにもかかわらず、show ip route コマンドで「Gateway of last resort is not set」と表示される場合がありますが、表示だけの問題で通信には影響ありません。

○ ネクストホップが直結サブネット上にないスタティック経路は未サポートです。

5.32 ARP

参照「コマンドリファレンス」/「IP ルーティング」/「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。

5.33 IPv6 ルーティング

参照「コマンドリファレンス」/「IPv6 ルーティング」

○ 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。

○ IPv6 において、インターフェース経路（直接経路）が 2 重に登録されることがあります。

○ IPv6 において、VLAN が削除されたとき、リンクローカルアドレスが IPv6 転送表から消えません。

○ 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。

○ ルーター通知（RA）による IPv6 アドレス自動設定では、複数のデフォルト経路を取得しても IPv6 転送表（FIB）に登録されるデフォルト経路は 1 つになります。

○ VLAN インターフェースに IPv6 アドレスを設定する場合、装置全体で 250 インターフェースを超えないようにしてください。

○ IPv6 環境で本体宛て通信を行う場合、ipv6 forwarding を有効にしてください（初期設定は無効）。

5.34 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。

5.35 近隣探索

参照「コマンドリファレンス」/「IPv6 ルーティング」/「近隣探索」

イベントログ上に「Neighbor discovery has timed out on link eth1->5」のログメッセージが不要に表示されることがあります。これは表示上の問題であり通信には影響はありません。

5.36 IGMP

参照「コマンドリファレンス」/「IP マルチキャスト」/「IGMP」

○ show ip igmp groups コマンドの表示結果に、IGMP を有効に設定していない VLAN が表示されることがあります。これは show ip igmp groups コマンドの表示だけの問題であり、動作に影響はありません。

○ マルチキャストグループをスタティックに登録した後、登録したインターフェースにスタティックに登録してあるものと同じマルチキャストグループの参加、離脱が発生すると、マルチキャストグループがコンフィグから削除しても消せなくなります。
この場合は、マルチキャストグループにメンバーが参加した状態で ip igmp static-group コマンドを no 形式で実行するか、IGMP 機能を一旦無効にし、再度有効にすると、マルチキャストグループは正常に削除されます。

5.37 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。

5.38 MLD

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD」

○ 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。

○ 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 パケットの Max Query Response Time フィールドの値が、本製品の設定の 1/100 の数値で送出されます。MLD をお使いの際は、ipv6 mld query-max-response-time コマンドでなるべく大きい値（最大値は 240）を設定してください。

○ 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

○ MLD の Non-Queriers は、レコードタイプが BLOCK_OLD_SOURCES の MLDv2 Report メッセージを受信しても、指定された送信元アドレスを削除しません。

○ MLDv1 と MLDv2 混在環境において、MLDv2 Report で Exclude モードになっている状態で、MLDv1 Report を受信した場合、該当アドレスは Exclude モードのソースリストから削除されているにもかかわらず、その後、該当アドレスからのマルチキャストパケットが転送されません。

5.39 MLD Snooping

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

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。

5.40 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」

ハードウェアアクセスリストをサポートリミットまで使用する設定を行った場合は、設定をスタートアップコンフィグに保存し、いったん再起動してください。

5.41 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 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。

○ sFlow と IPv6 QoS ストームプロテクション機能の併用は未サポートとなります。
sFlow を使用する場合は、QoS ストームプロテクション機能の代わりに、QoS メータリング（シングルレートポリサー）機能を使用してください。

○ 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。

○ mls qos map cos-queue コマンドで cos-queue マップを変更していても、マルチキャストパケットの CPU 宛て送信キューが、デフォルトの cos-queue マップにしたがって決定される場合があります。これらのマルチキャストパケットを任意の CPU 宛て送信キューに振り分けるには、remark new-cos コマンドを使って該当パケットの内部 CoS 値を書き換えてください。その際、該当パケットに対しては、デフォルトの cos-queue マップが適用されることにご注意ください。

○ ポリシーマップ名に「¦」（縦棒）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。

○ QoS ストームプロテクションの portdisable アクションによってポートがシャットダウン状態になっていても、show interface コマンドの administrative state 欄には err-disabled ではなく UP と表示されます。またこのとき、MIB の ifAdminStatus も UP になります。

5.42 攻撃検出

参照「コマンドリファレンス」/「IP 付加機能」/「攻撃検出」

攻撃検出機能を有効から無効に変更しても、同機能に割り当てられたハードウェアフィルタリング用のシステム内部領域は解放されません。同領域を開放するには、システムを再起動してください。

5.43 DNS リレー

参照「コマンドリファレンス」/「IP 付加機能」/「DNS リレー」

○ DNS のキャッシュサイズまたはタイムアウトの設定を変更すると、IPv6 DNS キャッシュエントリーが削除されます。

○ ip dns forwarding cache コマンドは未サポートです。

5.44 DHCP リレー

参照「コマンドリファレンス」/「IP 付加機能」/「DHCP リレー」

セカンダリー IP アドレスを設定したインターフェースで DHCP リレーを有効にした場合、セカンダリー IP アドレスが優先的に使用されます。

5.45 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 クロスリンク、EPSR、VCS を使用した構成で、VCS メンバーがダウンし、復旧した際、復旧した VCS メンバーに接続されている AMF ノードが認識されません。
EPSR リング内では、AMF Node Depth 値が異なる AMF ノード同士は AMF リンクで接続してください。

○ VCS 構成において、スタックリンクに障害が発生し VCS メンバーが Disabled Master 状態になると、スタックリンクとレジリエンシーリンク以外のポートは無効化されますが、EPSR を併用している場合、show atmf nodes コマンドの結果には、Disabled Master 状態となり無効化されたポートに接続された AMF ノードが表示されてしまいます。
EPSR リング内では、AMF マスターからの距離（ホップ数）の異なる AMF ノード同士は、AMF クロスリンクではなく AMF リンクで接続してください。

○ 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、VCS を併用している環境において、VCS スレーブの機器の電源を落とす、または、スタックケーブルを抜いた際、配下のノードが AMF ネットワークから脱退したまま参加しないことがあります。VCS スレーブを再起動する、または、該当インターフェースに no switchport atmf-link/switchport atmf-link コマンドを実行することで、配下のノードも AMF ネットワークに復帰できます。

○ 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 メンバーよりも後から 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、すべての 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 マスター上で atmf recover コマンドによってメンバーノードの内蔵フラッシュメモリーの復元を実行した場合、復元が完了しても、マスターノード上で完了を示すメッセージが出力されません。復元の完了は、対象ノードにおけるログ出力によって確認できます。

○ 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。

5.46 バーチャルシャーシスタック（VCS）

参照「コマンドリファレンス」/「バーチャルシャーシスタック」

○ VCS スレーブを交換する際、マスターとスタックケーブルで接続して電源をオンにした後、通常、スタック ID を変更し、AMF を有効に設定するため、2 回の再起動が必要になりますが、AMF ネットワークに所属後、コンフィグの同期に時間がかかり、コンフィグの同期後に以下のようなエラーメッセージが表示され、もう一度再起動を要求されます。
- Post startup check found the following errors:
- Processes not ready:
- authd bgpd epsrd irdpd lacpd lldpd mstpd ospf6d ospfd pdmd pim6d pimd ripd ripngd rmond sflowd vrrpd
- Timed out after 300 seconds
- Bootup failed, rebooting in 3 seconds.
- Do you wish to cancel the reboot? (y) :

○ LDF が検出され link-down アクションが実行されている間にループを解消し、VCS マスター切り替えが発生すると、LDF 検出時アクションが実行されたポートが設定時間経過後も復旧しません。
該当のポートにて shutdown コマンドを no 形式で実行すると、リンクが復旧します。

○ VCS と EPSR を併用する場合、reboot rolling コマンドを実行した際に約 1 分程度の通信断が発生する場合があります。

○ マスター切り替えが発生したとき、「Failed to delete 'manager'」というメッセージが表示されることがあります。これは表示だけの問題で動作には影響しません。

○ VCS 構成時、EPSR と IGMP を併用している場合、IGMP タイマーは初期値より短く設定しないでください。

○ VCS グループのファームウェア自動同期は 2 台構成時のみサポートとなります。3 台以上で VCS を構成する場合は手動で同じファームウェアバージョンにそろえてください。

○ 同一ネットワーク上に複数の VCS グループが存在する場合は、バーチャル MAC アドレスの下位 12 ビットとして使用されるバーチャルシャーシ ID を、該当する VCS グループ間で重複しないように設定してください。バーチャルシャーシ ID の設定は、stack

virtual-chassis-id コマンドで行います。また、VCS グループのバーチャルシャーシ ID は、show stack コマンドを detail オプション付きで実行したときに表示される「Virtual Chassis ID」欄で確認できます。

○ VCS 構成時に udld aggressive-mode コマンドを設定する場合は、全ポートに設定せず、必要なポートにのみ設定してください。全ポートに設定している場合、VCS メンバーのいずれかが再起動すると、該当メンバーのレジリエンシーリンクを除く全ポートでアグレッシブモードが解除されます（ランニングコンフィグには no udld aggressive-mode という設定が追加されます）。

○ VCS スレーブのスイッチポートに wrr-queue disable queues コマンドを設定している場合、再起動には reboot rolling/reload rolling コマンドではなく、通常の reboot/reload コマンドを使ってください。reboot rolling/reload rolling を使用すると、再起動後スレーブのスイッチポートに wrr-queue disabled queues コマンドが適用されません。

○ VCS と AMF の併用時に reboot rolling を実行すると、通常よりも通信復旧に時間がかかる場合があります。

○ VCS と RSTP の併用時に reboot rolling を実行すると、通常よりも通信復旧に時間がかかる場合があります。

○ VCS 構成においてログを出力しない再起動、またはカーネルリブートが発生した後、新規マスターの全ポートのリンクダウン・アップが一時的に発生します。

○ VCS 構成において HSL プロセスが異常終了した場合、新規マスターの全ポートのリンクダウン・アップが発生します。

○ VCS 構成時、スレーブに接続したコンソールターミナルからの CLI ログイン時には、TACACS+ サーバーを用いたログイン認証ができません。ユーザー認証データベースによる認証は可能です。

○ VCS メンバーが VCS グループからいったん離脱し、その後再加入してきた場合、再加入したメンバー上にメンバーポートを持つ LACP チャンネルグループのカウンター（show interface コマンドで表示されるもの）が実際の 2 倍の値を示します。

○ 3 台以上のノードでスタックを組んでいる際、VCS マスター切り替えを行うと、レジリエンシーリンクに関する下記のエラーログが出力されることがあります。
- Resiliency link healthchecks have failed, but master(member-xx) is still online

○ EPSR のトランジットノードで VCS のローリングリブートを行った場合、10 秒程度の通信断が発生することがあります。

○ VCS 構成において RSTP を使用しているとき、VCS のマスター切り替えが発生するとマルチキャストの通信が復旧するまでに 6 秒以上かかります。

6 マニュアルの補足・誤記訂正

最新マニュアル（取扱説明書、コマンドリファレンス）の補足事項および誤記訂正です。

6.1 サポートする SFP モジュールについて

本製品がサポートする 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。

6.2 GVRP 未サポート

参照 「CentreCOM x310 シリーズ 取扱説明書」（Rev.A）70 ページ

取扱説明書（Rev.A）70 ページの準拠規格欄に「IEEE 802.1Q-2003 GVRP」の記述がありますが、正しくはサポート対象外となります。

6.3 VCS マスター / アクティブ CFC 切り替え時における AMF ノードの動作

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」

参照 「コマンドリファレンス」/「バーチャルシャーシスタック」

AMF ノードで VCS マスターの切り替えやアクティブ CFC の切り替えが発生した場合、該当ノードが一時的に AMF ネットワークから離脱し、その後再参加します。この動作は AMF ネットワーク上で行われるものであり、データプレーンの通信には影響ありません

7　サポートリミット一覧

パフォーマンス	
VLAN 登録数	4094
MAC アドレス（FDB）登録数	16K
IPv4 ホスト（ARP）登録数	512
IPv4 ルート登録数	64※1
リンクアグリゲーション	
グループ数（筐体あたり）	128※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	116※3※4※5
認証端末数	
認証端末数（ポートあたり）	1K
認証端末数（装置あたり）	1K
マルチプルダイナミック VLAN（ポートあたり）	1K
マルチプルダイナミック VLAN（装置あたり）	1K
ローカル RADIUS サーバー	
ユーザー登録数	3
RADIUS クライアント（NAS）登録数	1※6
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 インターフェース経路、スタティック経路を含めた登録数です。
※2 スタティックチャンネルグループは 96 グループ、LACP は 32 グループ設定可能。合わせて 128 グループをサポートします。
※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 radius-server local コマンドでローカル RADIUS サーバーを有効にした際に、自動登録されるローカルホスト（127.0.0.1）を含みます。ローカルホスト以外の RADIUS クライアント（NAS）を登録したい場合は、”no nas 127.0.0.1” でローカルホストを削除することで登録可能です。

8　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。

9　最新マニュアルについて

最新の取扱説明書「CentreCOM x310 シリーズ 取扱説明書」(613-001925 Rev.A)、コマンドリファレンス「CentreCOM x310 シリーズ コマンドリファレンス」(613-001988 Rev.B) は弊社ホームページに掲載されています。

なお、VCS の設定、運用に関する情報は、コマンドリファレンスに合わせて掲載しております。

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/