613-002404 Rev.A 161228

CentreCOM® *x510* シリーズ・*AT-IX5-28GPX* リリースノート

この度は、CentreCOM x510 シリーズ、AT-IX5-28GPX 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　5.4.4-3.8

2　重要：注意事項

2.1　ファームウェアバージョンアップ時の注意事項

AT-x510-28GPX、AT-x510-52GPX、AT-IX5-28GPX をファームウェアバージョン **5.4.3-3.7** 以前から **5.4.3-3.9** 以降に更新後、最初の起動時には、必要に応じて PoE チップのソフトウェア更新が行われるため、起動時間が通常より 30 秒程度長くなる可能性があります。

2.2　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」/「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　本バージョンで追加・拡張された機能

ファームウェアバージョン **5.4.4-3.6** から **5.4.4-3.8** 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　ip igmp trusted コマンド

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

ip igmp trusted コマンドが追加されました。対象スイッチポートにおいて、選択したパラメーターのパケットを IGMP Snooping で処理するように設定します。no 形式で実行した場合は、選択したパラメーターのパケットを IGMP Snooping で処理せずに破棄します。

ip igmp trusted コマンド

書式

```
[no]ip igmp trusted {all|query|report|routermode}
```

パラメーター

all:	すべての IGMP パケットと ip igmp snooping routermode コマンドで指定されているパケット
query:	IGMP Query
report:	IGMP Membership Report
routermode:	ip igmp snooping routermode コマンドで指定されているパケット

3.2 match dscp コマンド

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 コマンドと match ip-precedence コマンドはこれまで IPv4 パケットにのみ対応していましたが、本バージョンより IPv6 パケットにもマッチするようになりました。IPv6 パケットにおいて、match dscp は Traffi c Class フィールドの先頭 6 ビット、match ip-precedence は Traffi c Class フィールドの先頭 3 ビットにマッチします。

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 **5.4.4-3.6** から **5.4.4-3.8** 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 ログの仕様変更

参照「コマンドリファレンス」/「運用・管理」/「ログ」

ポートセキュリティーの不正パケット受信時に表示されるログに、不正な MAC アドレスが表示されるようになりました。

4.2 ポートセキュリティーの仕様変更

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

ポートセキュリティーが有効なポートで受信したパケットの送信元 MAC アドレスが FDB に手動登録されている場合、FDB に登録されているポートと受信したポートが異なっていても不正パケットとして扱わない仕様でしたが、本バージョンより、受信したパケットの送信元 MAC アドレスが FDB に手動登録されていても、FDB に登録されているポートと受信したポートが異なる場合は不正パケットとして扱うよう仕様変更しました。

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 **5.4.4-3.6** から **5.4.4-3.8** 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 glibc に関する脆弱性（CVE-2015-0235）への対策を行いました。

5.2 OpenSSL 脆弱性（CVE-2014-3569 ～ 3572、CVE-2014-8275、CVE-2015-0204 ～ 0206）への対策を行いました。

5.3 リンクアグリゲーション使用時、ブロードキャストパケットがリンクアグリゲーションインターフェースへ正しく転送されない場合がありましたが、これを修正しました。

5.4 MAC ベース認証を使用しているポートでループによるストームが発生した後、ループを解除した際に Supplicant が接続されている別ポート上で連続的にトラフィックを受信し続けていると、認証解除と認証処理が繰り返されることがありましたが、これを修正しました。

5.5 switchport 上にレジリエンシーリンクを設定しているとき、LAG インターフェース上で「switchport trunk allowed vlan all」コマンドを使用すると、LAG インターフェースとそこに所属している物理インターフェース上で VLAN の設定に差異が生じることがありましたが、これを修正しました。

5.6 まれに、VLAN に関連する内部処理の異常が原因で通信停止や AMF 離脱などが発生することがありましたが、これを修正しました。

5.7 MSTP/RSTP のトポロジーチェンジ発生時に、BPDU のブリッジ ID が対向スイッチの値になることがありましたが、これを修正しました。

5.8 clear mac address-table コマンドの dynamic オプションでダイナミックエントリーを削除しようとすると関連プロセスが再起動していましたが、これを修正しました。

5.9 DHCP Snooping 機能の ARP セキュリティーが有効な VLAN で、不正ではない ARP パケットが正常に登録されないことがありましたが、これを修正しました。

5.10 VRRP において、バーチャル IP アドレスと異なるネットワークからバーチャル IP アドレス宛ての通信に応答しませんでしたが、これを修正しました。

5.11 VCS 構成において、OSPF の ASBR として動作する場合、グレースフルリスタート機能を使用することはできませんでしたが、本バージョンより使用することができるようになりました。

5.12 マルチキャストパケットを受信中に、IGMP Report パケットとマルチキャストの UDP パケットを受信し続けていると nsm 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。

5.13 show mls qos interface storm-status コマンド実行時、複数のインターフェースを指定した場合、再起動することがありましたが、これを修正しました。

5.14 atmf working-set コマンドの実行後に atmf reboot-rolling コマンドでファームウェアを更新した場合、一部の AMF ノードで正常にファームウェアを更新できないことがありましたが、これを修正しました。

5.15 VCS 構成のレジリエンシーリンクにおいて、まれにマスターからのヘルスチェックパケットの送信が停止し、その後復旧しない場合がありましたが、これを修正しました。

5.16 stack resiliencylink コマンドで VCS 管理用 VLAN を指定すると、VCS が切断されてしまうことがありましたが、これを修正しました。

5.17 VCS メンバーが加入するとまれにレジリエンシーリンク上でヘルスチェックパケットが転送されなくなることがありましたが、これを修正しました。

5.18 4 台の VCS 構成時、IGMP などの制御系パケットを高レートで受信し続けると VCS メンバーがクラッシュ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 **5.4.4-3.8** 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」

○ 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。

○ AT-x510-28GPX、AT-x510-52GPX、AT-IX5-28GPX（PoE スイッチ）で findme 機能を動作させた場合、Link LED のみが点滅します。

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。

○ 非特権 EXEC モードで show log permanent コマンドを実行した場、"%Permanent logging is not available on this device" のようなログが出力され、実行できません。

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」

○ Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB を装着している状態でシステムを再起動した場合、再起動時 SecureUSB メモリーの仕様によりロックがかかるため、再起動後に USB メモリーのセキュリティーを解除するための PIN コードを再度入力してください。

○ 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。

○ ECMP 経路を経由して行う TFTP でのファイル転送は未サポートです。

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+ 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。

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 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。

○ サポートリミット以上のユーザー情報が記載されている CSV ファイルを読み込んだとき、ローカル RADIUS サーバーには 1 件も登録されないにも関わらず、「Successful operation」と表示されます。

6.8 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。

○ （AT-x510-28GPX/AT-x510-52GPX のみ）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。また、2 つの電源ユニットがどちらも正しく動作しているにもかかわらず、一方についてのログしか表示されない場合があります。

○ 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。

6.9 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」

（x510 シリーズのみ）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。

6.10 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。

6.11 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。

6.12 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。

○ 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。

6.13 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。

6.14 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。

○ NTP サーバーを二つ設定すると、正しく時刻同期できなくなる場合があります。

6.15 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。

6.16 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。

6.17 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"
```

6.18 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。

6.19 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」

○ 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。

○ 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。

6.20 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。

6.21 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。

○ VCS メンバーが脱退した後は、ミラーポートの設定を変更しても動作に反映されません。VCS メンバーが加入しなおすと正しく動作するようになります。

6.22 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。

6.23 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。

○ 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

○ 認証ポートが MAC 認証、Web 認証を併用しており、かつ直接 Supplicant の Linkup/Down を検知しない環境にて、一度 Web 認証に失敗した後、Supplicant が DHCP の再取得を実施すると、その後 MAC 認証が実施されません。

○ 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、802.1X 認証と Web 認証の 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。

○ 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。

○ 同一ポート上でポート認証、マルチプルダイナミック VLAN、リンクアグリゲーション（ポートトランキング）、DHCP リレーエージェント機能を併用することはできません。

○ VCS 構成で Web 認証を LAG インターフェースに設定している時、マスター切り替えが二回発生した後、Web 認証ページにアクセスできなくなります。

6.24 Power over Ethernet（AT-x510-28GPX、AT-x510-52GPX、AT-IX5-28GPX のみ）

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-x510-28GPX, AT-x510-52GPX）と PoE に対応していない機器（AT-x510-28GTX, AT-x510-52GTX, AT-x510-28GSX, AT-x510DP-28GTX, AT-x510DP-52GTX）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。

○ （AT-IX5-28GPX のみ）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。

6.25 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。

○ 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。

6.26 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。

6.27 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」

○ VCS と PIM-SM を併用している時、リブートローリングを行うと 20 秒程度のマルチキャストトラフィックの通信断が発生します。

○ スパニングツリープロトコルにおいて、ポートの役割（Role）が Rootport または Alternate から Designated に変更されると、ハロータイム ×3 秒後に下記のログが出力され、トポロジーの再構築が行われます。これによるトラフィックへの影響はありません。
・ BPDU Skew detected on port port1.0.1, beginning role reselection

○ 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。

6.28 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 と GVRP の併用は未サポートになります。

○ 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 のトポロジーチェンジによりパケットが CPU に転送される際、以下のログメッセージが出力される場合がありますが、通信に影響はありません。
- 'cmsg_transport_tipc_broadcast_client_send 161: [TRANSPORT] Failed to send tipc broadcast'

6.29 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。

6.30 IP インターフェース

参照「コマンドリファレンス」/「IP ルーティング」/「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。

6.31 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」

○ maximum-paths コマンドを設定して、等コストパスの最大値を変更しても有効になりません。

○ 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。

6.32 RIP（x510 シリーズのみ）

参照「コマンドリファレンス」/「IP ルーティング」/「経路制御（RIP）」

○ RIP 認証機能において、複数のパスワード（キーチェーン）を設定した時、送信される RIP パケットの中に含まれるパスワードは、1 番目に設定したパスワードのみになります。

○ RIP で通知するネットワークの範囲を指定するとき 32 ビットマスクで指定しないでください。

○ cisco-metric-behavior コマンドは未サポートです。

○ RIP パケットを送受信する RIP インターフェースの数は 250 までとしてください。

○ 機器の持つ RIP インターフェースが含まれ、サブネットマスクの異なる経路を受信した場合、その経路をダイナミック登録しません。スタティック登録してください。

6.33 OSPF（x510 シリーズのみ）

参照 「コマンドリファレンス」/「IP ルーティング」/「経路制御（OSPF）」

○ VRRP が動作する機器は、OSPF のエリア境界ルーター（ABR）に設定することはできません。
ABR でグレースフルリスタートが発生した後、隣接関係をダウンさせると、隣接関係を保持していたサブネットのサマリー LSA が削除されます。

○ OSPF において、代表ルーター（DR）として動作している時に clear ip ospf process コマンドを入力すると、隣接ルーターが DR に変更されます。

○ OSPF 使用時、グレースフルリスタート後や VCS のマスター切り替え後に show ip ospf route コマンドを実行すると、インターフェース経路の種別が通常の「C（Connected）」ではなく「O（OSPF）」と表示されます。これは表示だけの問題であり、通信には影響ありません。また、インターフェースのダウンや OSPF プロセスの再起動によって解消されます。

○ OSPF の経路フィルタリングにおいて、match metric コマンドを使った特定経路の破棄ができません。

○ OSPF で完全スタブエリア（area stub no-summary）に指定すると、本来そのエリア内にはデフォルトルートのみを通知するべきですが、各エリアへのルート情報（タイプ 3LSA）が通知されてしまいます。

○ 異なる OSPF プロセス間の OSPF 再通知は未サポートになります。

○ VCS と OSPF MD5 認証を併用している場合、VCS マスター切り替え後の再参加の際に通信が一時的に切断します。

○ overflow database コマンドを no 形式で実行した場合、設定を有効にするには再起動が必要となります。

○ OSPF 環境でルートマップを使用して IP 経路表へ特定のネットワークのみの経路を登録させる場合、受信した LSU パケット内部の経路エントリーの最初から 255 個までしかルートマップの動作対象になりません。対向機器から受信するルート数は 255 以内におさまるようにしてください。

○ VCS 構成時、OSPF の ASBR として動作している機器において、グレースフルリスタート機能を無効にしている場合、VCS のマスター切り替え後に AS 外部 LSA の更新処理を行わなくなります。復旧させるには、clear ip ospf process コマンドを実行して

ください。OSPF グレースフルリスタート機能を無効にしたい場合、対象機器では OSPF グレースフルリスタート機能を有効に設定し、隣接する OSPF ピアにおいて、その補助動作を行わないよう設定してください。

6.34 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。

6.35 VRRP

参照「コマンドリファレンス」/「IP ルーティング」/「VRRP」

○ VRRP を使用していない装置では VRRP トラップを有効にしないでください。VRRP トラップの有効化・無効化は、snmp-server enable trap コマンドの vrrp オプションで行います。初期設定は無効です。

○ VRRPv3 とローカルプロキシー ARP を併用時、実 IP を用いたマスタールーターではローカルプロキシー ARP は使用できますが、仮想 IP を用いたバックアップルーターではローカルプロキシー ARP が動作しません。

6.36 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。

○ 本バージョンでは DHCPv6 クライアント機能および DHCPv6 PD クライアント機能を使用できません。DHCPv6 クライアント機能や DHCPv6 PD 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。

○ 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）。

6.37 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。

6.38 RIPng（x510 シリーズのみ）

参照「コマンドリファレンス」/「IPv6 ルーティング」/「RIPng」

RIPng の cisco-metric-behavior コマンドは未サポートになります。

6.39 OSPFv3（x510 シリーズのみ）

参照「コマンドリファレンス」/「IPv6 ルーティング」/「経路制御（OSPFv3）」

○ OSPFv3 使用時、passive-interface コマンドで指定するパッシブインターフェースには、実在するインターフェースのみを指定してください。

○ OSPFv3 の OSPF ネイバー暗号化方式を設定すると、次の不要なログが出力されます。これは表示だけの問題であり、動作には影響ありません。

Authentication/Encryption algorithm error, or SA key is wrong.

○ OSPFv3 の AS 境界ルーターで集約された経路エントリーが LSDB に登録されるときメトリックが 1 増加します。

○ 経路集約により作成された null スタティック経路は IPv6 転送表（FIB）に表示されませんので、show ipv6 route database コマンドで表示される IPv6 経路表（RIB）で確認してください。

○ OSPFv3 の認証機能は未サポートです。

○ OSPFv3 で仮想リンクを使用している場合、グレースフルリスタートは未サポートです。

○ restart ipv6 ospf graceful コマンド以外の要因でグレースフルリスタートが実行された場合、グレース期間が設定値の 2 倍の値で動作します。

6.40 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。

6.41 PIM（x510 シリーズのみ）

参照「コマンドリファレンス」/「IP マルチキャスト」/「PIM」

○ PIM-DMv4 インターフェースをサポートリミット値まで設定した後、VLAN インターフェースから PIM-DMv4 の設定を削除し、別の VLAN インターフェースに PIM-DMv4 を設定しようとすると、下記のエラーが出力され、設定ができません。その場合は、設定を保存してから再起動してください。
% Maximum number of pim-dm interfaces reached

○ PIM-SSM の範囲外のマルチキャストアドレスを受信しても破棄しません。

○ PIM-DM インターフェースをすべて無効化しても、IP マルチキャスト経路表の Upstream エントリーがすぐに削除されませんが、通信には影響ありません。また、該当エントリーはエージアウトによって削除されます。

6.42 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。

○ IGMP プロキシーにおいて、下流インターフェースに指定している VLAN を無効にしても、上流インターフェースにグループ情報が残り続けます。

○ ip igmp proxy-service コマンドの設定を取り消す場合は、いったん対象 VLAN インターフェースを「shutdown」してから、「no ip igmp proxy-service」を実行し、その後 VLAN インターフェースを「no shutdown」してください。

○ ip igmp static-group コマンドで登録したスイッチポートをタグなし、またはタグつきポートに変更すると、IGMP のエントリーは残っているにもかかわらず、PIM の（*,G）エントリーが削除された状態になります。

○ 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。

○ clear ip mroute コマンドでマルチキャスト経路エントリーを削除すると、ip igmp static-group コマンドで設定した IGMP のスタティックエントリーも削除されてしまいます。clear ip mroute コマンド実行後は、ip igmp static-group コマンドを再実行してください。

○ IGMP プロキシーとして動作しているスイッチが Leave メッセージを上位ルーターへ転送した後、当該グループが削除されているにもかかわらず上位ルーターからの GroupSpecificQuery に対して Join メッセージを返してしまうことがあります。その結果、上位ルーター上から不要なマルチキャストパケットを受信し続けてしまいますが、エントリーが Expire すれば解消されます。

○ IGMP プロキシーを使っているスイッチで、グループが離脱した後に上位ルーター側の VLAN インターフェースがダウンすると、最大で 260 秒の間離脱したグループがホスト側のポートに再登録できなくなることがあります。対象グループを clear ip mroute コマンドを実行し削除することで復旧します。

6.43 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

6.44 IPv6 マルチキャスト

参照「コマンドリファレンス」/「IPv6 マルチキャスト」

○ IPv6 マルチキャストと OSPFv3 認証機能は併用できません。

○ スタティック登録した IPv6 マルチキャスト経路の設定を削除すると、他のスタティック登録した経路も削除されてしまいます。消えてしまったルートを再登録するか、再起動することで通信は復旧します。

6.45 PIMv6（x510 シリーズのみ）

参照「コマンドリファレンス」/「IPv6 マルチキャスト」/「PIM」

○ PIMv6 使用時、PIMv6 インターフェースが最大まで設定されているとき、それらの VLAN の一つを削除しても、新たに VLAN インターフェースに PIMv6 を設定することができません。VLAN インターフェースから PIMv6 の設定を削除してから、VLAN を削除してください。

○ VRRPv3 と PIM-SMv6 は併用できません。

○ ipv6 pim ext-srcs-directly-connected コマンドは未サポートです。

6.46 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。

○ MLDv2 インターフェースにおいて、終点 IPv6 アドレスがマルチキャストアドレスの MLDv1 Report は受信しますが、終点 IPv6 アドレスが MLDv2 インターフェースのユニキャストアドレスになっている MLDv1 Report は受信せずに破棄します。

○ 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。

○ clear ipv6 mroute コマンドでマルチキャスト経路エントリーを削除すると、ipv6 mld static-group コマンドで設定した MLD のスタティックエントリーも削除されてしまいます。clear ipv6 mroute コマンド実行後は、ipv6 mld static-group コマンドを再実行してください。

6.47 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。

○ 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

6.48 ハードウェアアクセスリスト

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。

○ 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 policy1
```

6.49 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。
- ○ 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。
- ○ ポリシーベースルーティング使用時、TTL=1 のパケットを受信しても、パケットを破棄せずに転送してしまいます。そのため、トレースルートの実行結果が誤って表示される場合があります。

6.50 攻撃検出

参照「コマンドリファレンス」/「トラフィック制御」/「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。

6.51 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」

ip dns forwarding cache コマンドは未サポートです。

6.52 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。

6.53 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。

○ インターフェースから DHCP リレーの設定を解除することができません。

6.54 DHCPv6 サーバー

参照「コマンドリファレンス」/「IP 付加機能」/「DHCPv6 サーバー」

○ DHCPv6 サーバー機能において、動的に割り当てるアドレスの最終有効時間が infinite（無期限）の場合、IPv6 アドレスを配布しても、show コマンドに反映されません。

○ DHCPv6 サーバー使用時、DHCPv6 サーバー配下のホストに、DHCP プール内の IPv6 アドレスを固定設定しないでください。

○ DHCPv6 プールのサポートリミットは 200 個です。

6.55 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 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。

○ 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。

○ 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。

○ VCS と AMF を併用している環境で、VCS バックアップメンバーが加入直後に、AMF マスターから atmf working-set コマンドを実行すると x510 配下の機器がワーキングセットグループに加入できません。VCS バックアップメンバーが加入後に atmf working-set コマンドを実行する場合は、一分以上経過してからにしてください。

6.56 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、PIM、EPSR の併用構成において、トランジットノード間のリンク障害などにより EPSR のトポロジーが変更されると、通信復旧まで 2 ～ 15 秒程度かかる場合があります。

○ VCS スレーブのスイッチポートに wrr-queue disable queues コマンドや wrr-queue egress-rate-limit 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、wrr-queue egress-rate-limit 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 構成でハードウェアパケットフィルターやポリシーマップによるトラフィック制御を実施している場合、VCS メンバーの加入時にトラフィック制御が一瞬無効になります。

○ VCS 構成時、スタティックチャンネルグループ上では受信レート検出（QoS ストームプロテクション）を使用できません。LACP チャンネルグループでは使用可能です。

○ システム起動後に findme コマンドを一度でも実行している場合、VCS のマスター切り替えが発生すると、その後 findme コマンドが動作しなくなります。

○ VCS と OSPFv3 ASBR の併用時、VCS のマスター・スレーブで異なるインターフェース（VLAN）を用いたマルチパス構成は未サポートです。

○ 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、多数のマルチキャストグループが存在する場合、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時間がかかります。

○ VCS 構成の製品を EPSR でトランジットノードとして使用しているとき、16 以上の VLAN のタグパケットを受信している状態でリブートローリングを行うと、パケットが重複してスイッチングされることがあります。

○ OSPFv3 使用時、（VCS/CFC）マスターフェイルオーバーが発生すると、まれに IPv6 トラフィックの通信が 6 秒程度停止する場合があります。

○ VCS 構成において、レジリエンシーリンクをループ構成にしているとき、ディセーブルマスター（Disabled Master：全スイッチポートを無効にしている一時的なマスター状態）がマスター（Active Master）に遷移した後にレジリエンシーリンク内でループが発生します。

○ VCS 構成で Web 認証を行う際、事前設定がはいったコンフィグファイルを起動時コンフィグに指定し、対象の VCS メンバーが存在しない場合、サプリカントがログインページにアクセスできない場合があります。

○ 3 台以上の VCS 構成において、LDF 検出によりブロッキングポートが作成されている VCS メンバーで再起動が発生した場合、他の VCS メンバーで例外処理が発生する場合があります。

7 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）等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 オプションモジュール製品の保証期限

参照 「製品保証書」

下記オプション（別売）モジュール製品のパッケージに 90 日間の製品保証書が入っている場合がありますが、ご購入より 1 年間保証いたします。

- AT-PWR250-70
- AT-PWR800-70
- AT-PWR250R-80
- AT-PWR100R-70
- AT-StackXS/1.0
- AT-StackOP/0.3
- AT-StackOP/9.0

7.3 LLDP-MED MIB

参照 「CentreCOM x510 シリーズ 取扱説明書」（Rev.C）76 ページ

上記取扱説明書の「本製品の仕様」/「サポートする MIB」欄において、「LLDP-MED MIB（ANSI/TIA-1057）」は特定の機種でのみサポートという意味の記述がありますが、実際にはすべての機種で同 MIB をサポートしています。

7.4 定格入力電流値

参照 「AT-x510DP-28GTX/AT-x510DP-52GTX/AT-IX5-28GPX 取扱説明書」（Rev.B）85 ページ

上記取扱説明書において、AT-PWR800-70/AT-PWR250-70 の定格入力電流値に誤りがありましたので、下記のとおり訂正いたします。

誤：

AT-PWR800-70：12A
AT-PWR250-70：3.0A

正：

AT-PWR800-70：10A
AT-PWR250-70：5.0A

7.5 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」

UTP ケーブルを接続したとき、1000M でのリンクアップが可能であるにもかかわらず、1000M より低いリンクスピードにてリンクアップする場合があります。その場合は UTP ケーブルを接続しなおしてください。

7.6 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.B）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。

7.7 SecureUSB メモリー使用時の注意事項

参照「コマンドリファレンス」/「運用・管理」/「システム」

参照「コマンドリファレンス」/「運用・管理」/「ファイル操作」

○ Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB を装着している状態でシステムを再起動した場合、再起動時 SecureUSB メモリーの仕様によりロックがかかります。USB 内のファームウェアファイルを起動用ファームウェアに指定して、再起動しないでください。

○ Apricorn 社の SecureUSB メモリー ASK-256-8GB/16GB/32GB をロックがかかったまま本製品に挿入すると、デバイス認識のリトライと失敗を繰り返すログが約 3 分間出続けますが、正常なものです。

7.8 802.1X 認証と Web 認証の併用時の動作

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」

2 ステップ認証のサポートにより、802.1X 認証と Web 認証を併用する場合の動作がファームウェアバージョン **5.4.3-3.7** から変更になりました。

5.4.3-2.5 以前の動作

802.1X 認証と Web 認証併用時は、802.1X で認証に失敗すると認証プロセスが完了となっていました。

5.4.3-3.7 以降の動作

802.1X 認証と Web 認証併用時は、802.1X で認証に失敗すると Web 認証に移行し、Web 認証でも認証に失敗すると認証プロセスが完了になります。

7.9 clear ip mroute コマンド

参照「コマンドリファレンス」/「IP マルチキャスト」

clear ip mroute コマンドはファームウェアバージョン **5.4.4-3.6** からサポートしています。本コマンドで、IP マルチキャスト経路表から指定したエントリーを削除します。

clear ip mroute コマンド

書式

```
clear ip mroute {*|GROUP [SOURCE]}
```

パラメーター

*: すべての IGMP パケットと ip igmp snooping routermode コマンドで指定されているパケット

GROUP [SOURCE] :=A.B.C.D [A.B.C.D]:
マルチキャストグループアドレスとマルチキャスト送信者の IP アドレス。送信者の IP アドレスは省略可。指定したグループ、あるいは、グループと送信者の組に対応するエントリーだけを対象にする

8　サポートリミット一覧

パフォーマンス	
VLAN 登録数	単体：4094 VCS：2000 ※1
MAC アドレス（FDB）登録数	単体：16K VCS：4K ※2
IPv4 ホスト（ARP）登録数	単体：2K VCS：768 ※3
IPv4 ルート登録数	1K ※4
リンクアグリゲーション	
グループ数（筐体あたり）	128 ※5
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	240 ※6 ※7 ※8
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	100
RADIUS クライアント（NAS）登録数	24
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	31

※　表中では、K=1024
※1 VCS 構成時、VCS グループに設定する VLAN の数は 2000 個までをサポートします。
※2 VCS 構成時、フォワーディングデータベース（FDB）のエントリー数は 4K 個までサポートします。
※3 VCS 構成時、IPv4 ホスト登録数（ARP エントリー数）は最大で 768 個までサポートします。
※4 インターフェース経路、スタティック経路、ダイナミック経路など、各種経路情報を含めた登録数です。
※5 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。
※6 アクセスリストのエントリー数を示します。
※7 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。
※8 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。

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 x510 シリーズ 取扱説明書」（613-001684 Rev.C）、「AT-x510DP-28GTX/AT-x510DP-52GTX/AT-IX5-28GPX 取扱説明書」（613-001836 Rev.B）、コマンドリファレンス「CentreCOM x510 シリーズ コマンドリファレンス」（613-001763 Rev.J）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、別紙「CentreCOM x510 シリーズ VCS 設定 / 運用マニュアル」に掲載しておりましたが、「CentreCOM x510 シリーズ コマンドリファレンス」（613-001763 Rev.B）以降、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/