613-002137 Rev.C 150911

CentreCOM® *x510L* シリーズ リリースノート

この度は、CentreCOM x510L 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 5.4.5-1.1

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 **5.4.5-0.4** から **5.4.5-1.1** へのバージョンアップにおいて、以下の機能が追加・拡張されました。

2.1 光ファイバーモジュールの状態監視

参照 **「コマンドリファレンス」/「運用・管理」/「システム」**

光ファイバーモジュール（SFP、SFP+）の動作状態監視結果を表示する show system pluggable diagnostics コマンド、および、動作状態監視結果を格納するプライベート MIB をサポートしました。

2.2 snmp-server legacy-ifadminstatus コマンド

参照 **「コマンドリファレンス」/「運用・管理」/「SNMP」**

ファームウェアバージョン 5.4.3-3.x/5.4.4 以降では、LDF 検出、MAC アドレススラッシングプロテクション、受信レート検出（QoS ストームプロテクション）、UDLD などの機能によってポートがリンクダウンしたときに show interface コマンドで表示されるポート状態として err-disabled が導入されましたが、これにともなって err-disabled 状態時でも標準 MIB の ifAdminStatus は UP のままとなるよう仕様変更が行われました。
しかし、本バージョンで追加された snmp-server legacy-ifadminstatus コマンドを実行することにより、各種機能によってポートがリンクダウンしたときに ifAdminStatus が Down となる、err-disabled 状態導入以前の動作を再現することができます。

2.3 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

2.4 Supplicant が認証ポートから非認証ポートに移動した場合の通信継続

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/802.1X 認証において、認証済み Supplicant が認証ポートから非認証ポート（通常ポート）に移動した場合、これまでは通信ができなくなっていましたが、本バージョンから通信を継続できるようになりました。具体的には、認証済み Supplicant の MAC アドレスを持つパ

ケットを非認証ポートで受信した場合、スタティックに登録されている該当 Supplicant の MAC アドレスを FDB から削除するように動作が変更されました。

2.5 DHCP Snooping とマルチプル VLAN（プライベート VLAN）の併用

参照「コマンドリファレンス」/「L2 スイッチング」/「DHCP Snooping」

これまで、DHCP Snooping とマルチプル VLAN（プライベート VLAN）は併用できませんでしたが、本バージョンから併用が可能になりました。なお、両機能の併用時にはいくつかの注意事項があります。詳細はコマンドリファレンスをご覧ください。

2.6 LACP チャンネルグループ上での AMF 接続

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」

これまで、自動設定のトランクグループ（LACP チャンネルグループ）を AMF 接続ポート（AMF リンクまたは AMF クロスリンク）に設定することはできませんでしたが、本バージョンから可能になりました。

2.7 仮想リンク経由で接続している AMF ノードのオートリカバリー

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」

これまで、仮想リンク経由で AMF ネットワークに接続している AMF ノードは事前設定を行わないと AMF マスターに接続できないため、オートリカバリーができませんでしたが、本バージョンからは隣接するノードの補助によりこうしたノードでもオートリカバリーが可能になりました。

具体的には、仮想リンクを持つ AMF ノード（以下、該当ノード）のコンフィグが、該当ノードと AMF リンクか AMF クロスリンクで接続している AMF ノード（以下、隣接ノード）に自動的にバックアップされるようになりました。

これにより、該当ノードは次に示す 2 つのステップでオートリカバリーを実行できるようになっています。

(1) 隣接ノードに自動バックアップされたコンフィグをダウンロードして仮想リンクを復旧
(2) 復旧した仮想リンク経由でマスターからファームウェアやライセンスを含む通常のオートリカバリーを実施

本バージョン以降、本機能はつねに有効であり、設定なしで動作します。ただし、本機能を利用する場合、リカバリー対象ノードには仮想リンクだけでなく、AMF リンクか AMF クロスリンクで接続した隣接ノードが必要です。また、リカバリー対象ノードと隣接ノードがともに本バージョン以降で動作している必要があります。

2.8 Web GUI のアイドル時タイムアウト

参照「コマンドリファレンス」/「Web GUI」

Web GUI にログインしたユーザーが一定期間操作を行わなかった場合に自動的にログアウトさせる機能をサポートしました。本機能は初期設定では無効ですが、新しく追加された gui-timeout コマンドでタイムアウトまでの時間を設定することにより有効となります。

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 **5.4.5-0.4** から **5.4.5-1.1** へのバージョンアップにおいて、以下の機能が仕様変更されました。

3.1 show atmf links コマンドの表示内容変更

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）」

show atmf links コマンドの detail オプションで出力される Port Area Id、Port Area Name は対向メンバーのエリア ID、エリア名を表していましたが、本バージョンより自装置が所属するエリア ID、エリア名を表すように変更されました。

3.2 Web GUI

参照「コマンドリファレンス」/「Web GUI」

GUI 上から接続している IP アドレスの変更はできませんでしたが、5.4.5-1.1 より IP アドレスの変更ができるようになりました。ただし、接続している IP アドレスを変更後は新しい IP アドレスに接続し GUI を開き直してください。

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 **5.4.5-0.4** から **5.4.5-1.1** へのバージョンアップにおいて、以下の項目が修正されました。

4.1 copy コマンドにおいて、コピー元に current-software（実行中のファームウェアイメージ）、コピー先に外部メディア（USB メモリーや SDHC カード）上のファイルまたはディレクトリーを指定した場合、コピーが完了する前にコピー成功のメッセージ（Successful operation）が表示されていましたが、これを修正しました。

4.2 ntp server コマンドまたは ntp peer コマンドを設定する前に ntp source コマンドを設定すると、NTP が正しく動作しませんでしたが、これを修正しました。

4.3 ブロードキャスト / マルチキャストの送信パケットが正しくミラーリングされないことがありましたが、これを修正しました。

4.4 LDF 検出中のトランクグループ（saX、poX）からメンバーポートを削除すると、関連プロセスが異常終了し、システムが再起動することがありましたが、これを修正しました。

4.5 PIM 使用時にマルチキャスト経路が更新されると関連プロセスが異常終了することがありましたが、これを修正しました。

4.6 ポリシーマップに CoS 値の設定が行われているまま、no mls qos で、QoS を一度無効にしたあと、再度 QoS を有効にすると、パケットが CoS 値の設定どおりに処理されませんでしたが、これを修正しました。

4.7 なんらかの原因で IMI プロセスが再起動した場合、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、IMI プロセスが再起動しても正常に AMF ネットワークに参加できるよう修正しました。

4.8 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ことがありましたが、これを修正しました。

4.9 3 台以上の VCS 構成において、レジリエンシーリンクを使用時、スタックケーブル抜けなどでマスターと他 2 台（ディセーブルマスターとバックアップメンバー）という分断が発生してディセーブルマスターとバックアップメンバーのスイッチポートがリンクダウンした後、ディセーブルマスターの機器を再起動すると、当該スイッチのスイッチポートがリンクアップし、スタックメンバーとして加入していましたが、これを修正しました。

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 **5.4.5-1.1** 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。

○ AT-x510L-28GP、AT-x510L-52GP（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。

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。

○ 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。

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」**

○ 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。

○ 起動用ファームウェアに設定されているフラッシュメモリー上のファイルと同名のファイルが外部メディア（USB メモリー、SDHC カード）に存在している場合、外部メディア上の該当ファイルを delete コマンドで削除できません。その場合は delete コマンドに force オプションを指定して削除してください。

5.4 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+ 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。

5.5 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。

5.6 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。

○ 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-x510L-28GP/AT-x510L-52GP 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。

5.7 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。

5.8 トリガー

参照「コマンドリファレンス」/「運用・管理」/「トリガー」

○ トリガー設定時、script コマンドで指定したスクリプトファイルが存在しない場合、コンソールに出力されるメッセージ内のスクリプトファイルのパスが誤っています。

誤：% Script /flash/script-3.scp does not exist. Please ensure it is created before
正：% Script flash:/script-3.scp does not exist. Please ensure it is created before

また、スクリプトファイルが存在しないにもかかわらず前述のコマンドは入力できてしまうため、コンフィグに反映され、show trigger コマンドのスクリプト情報にもこのスクリプトファイルが表示されます。

○ 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。

5.9 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。

5.10 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。

○ snmp-server enable trap コマンドにおいて、snmp-server の文字列を省略し、sn enable trap と入力すると、入力したコマンドがホスト名欄に表示され、コマンドは認識されません。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。

○ 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。

○ SNMPv3 のユーザーを削除したときは、設定を保存して再起動してください。

5.11 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。

5.12 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。

5.13 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。

5.14 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。

5.15 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。

5.16 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。

5.17 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。

○ 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。

5.18 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）。

○ 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。

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」

○ 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。

5.20 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。

○ VCS 構成時、マスター切り替え後に、show interface コマンドをトランクポートに対して実行した際に表示される送受信パケット数が、重複してカウントされます。実際にはパケットを重複して出していることはありません。正確な値が必要な場合はメンバーポートのカウンターを合計してください。

○ 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。

○ トランクグループ（saX、poX）のステータスを無効から有効に変更するときは、必ず saX、poX インターフェースに対して「no shutdown」を実行してください。メンバーポートに対して「no shutdown」を実行すると、該当ポートの所属するトランクグループに設定された機能が動作しなくなることがあります。誤ってメンバーポートに「no shutdown」を実行してしまった場合は、ケーブルを抜き差しすることで復旧します。

○ VCS 構成でトランクグループを使用している場合、スタックメンバーが VCS に加入する際、一時的にトランクグループのインターフェースではなくポート自身で MAC アドレスを学習してしまい、MAC アドレススラッシングプロテクションが誤動作する場合があります。VCS 構成でトランクグループを使用している場合、トランクグループのインターフェースでは MAC アドレススラッシング検出時の動作を None に設定してください。

5.21 ポート認証

参照 「コマンドリファレンス」/「インターフェース」/「ポート認証」

○ 802.1X 認証において、認証を 3 台以上の RADIUS サーバーにて行う場合、はじめの 2 台の RADIUS サーバーにて認証に失敗した際、Authenticator から 3 台目の RADIUS サーバーに Access-Request が送信されません。

○ 認証済みポートが認証を解除されても、マルチキャストトラフィックが該当ポートに転送され続ける場合があります。

○ 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。

○ 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

○ 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 構成において、802.1X 認証を使用しローミング認証が無効のとき、マスター切り替え後に認証済みのサプリカントが別の認証ポートへ移動すると、移動先での初回の認証に失敗することがあります。そのような場合は再度認証を行ってください。

○ VCS のスタックメンバー間でローミング認証を行う場合は認証ポートでダイナミック VLAN を有効にしないでください。

○ 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。

○ 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。

○ ARP テーブルに端末の ARP が登録されないため、L3 環境で認証成功後、L3 通信がソフトウェアルーティングになってしまいます。L2 通信には影響ありません。

5.22 Power over Ethernet（AT-x510L-28GP、AT-x510L-52GP 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-x510L-28GP, AT-x510L-52GP）と PoE に対応していない機器（AT-x510L-28GT, AT-x510L-52GT）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。

○ 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。

○ 給電中のポートの PoE 給電機能を無効化しないでください。

○ PoE+ が有効なポートで PoE+ とそれより電力の低いクラスの PoE の信号を短時間に受信した場合、PoE+ 準拠の電力を供給してしまいます。

○ power-inline max コマンドで受電機器の消費電力を下回る値を設定しないでください。また、給電機器で設定している値を超えた電力要求がくると繰り返しトラップを出してしまいますが、通信に影響はありません。

5.23 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。

○ 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。

5.24 GVRP

参照「コマンドリファレンス」/「L2 スイッチング」/「GVRP」

Join Empty イベントタイプの GVRP PDU を受信すると広告対象でない VLAN も作成されます。

5.25 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。

5.26 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」

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

5.27 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'

○ EPSR スーパーループプリベンション構成時、多量の ARP Request パケットを受け続けているときにマスター切り替えが発生し、旧マスターが再加入したあと、マスターとスレーブ間の同期がとられる前にもう一度マスター切り替えが発生すると、EPSR のポートステータスの Forwarding となるべき箇所が Blocked となり、通信ができなくなります。

○ 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。

5.28 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」

clear mac address-table コマンドを使用して認証情報を削除する場合、dynamic パラメーターと address パラメーターを指定してください。それ以外のパラメーターを指定した場合は情報は削除されません。

5.29 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」

○ 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。

○ DHCP クライアント機能を有効に設定できる VLAN インターフェースの最大数は 2000 となります。

○ 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。

5.30 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。

○ いずれかの VLAN が無効化（shutdown）されている状態で、ip route コマンドの宛先ネットワークアドレスを 32 ビットマスクで設定すると、その経路のネクストホップが所属している VLAN がアップするたびに下記のログが出力されますが、通信に影響はありません。

HSL: ERROR: Error creating egress to hardware: Invalid configuration
HSL: ERROR: Error adding egress to hardware: Invalid configuration
HSL: ERROR: Error adding connected route to hardware

前記のログ出力を制限したい場合は無効化されている VLAN を「no shutdown」で有効にするか、32 ビットマスクで設定している宛先ネットワークアドレスを 31 ビット以下に変更してください。

5.31 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。

○ 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。

5.32 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。

○ VRRP のプリエンプトモードを有効にする場合は、バーチャルルーターの優先度が重複しないように設定してください。

○ VLAN に IP アドレスを設定していない状態で VRRP の設定はしないでください。

○ VRRPv3 を使用しているインターフェースの IPv6 グローバルユニキャストアドレスを変更する場合は、最初に当該インターフェース上のバーチャルルーターの設定を削除した後、IPv6 アドレスを変更し、その後バーチャルルーターの設定をしてください。

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 アドレス宛てに 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、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。

○ 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。

○ VCS 構成で IPv6 ルーティングを行う場合、MTU の変更をしないでください。IPv6 ルーティングを行う際に MTU を変更する必要がある場合は VCS を使用しないでください。

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。

○ DHCPv6 クライアント機能を使用した場合、DECLINE カウンターが動作しません。

○ IPv4 アドレスと IPv6 アドレスの両方を設定している VLAN インターフェースで IPv4 の VRRP だけを有効にした場合、IPv6 Router Advertisement が送信されなくなります。

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。

○ ipv6 nd reachable-time コマンドを使用することができません。Reachable Time フィールドは初期値のまま使用してください。

5.36 IP マルチキャスト

参照「コマンドリファレンス」/「IP マルチキャスト」

マルチキャストのルート情報は VCS 間で同期されません。マスター、スレーブで個々に登録が行われているため、通信への影響はありません。

5.37 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。

○ 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 プロキシー機能は、送信元指定付きの IGMPv3 パケットをサポートしていません。IGMP プロキシー使用時は、送信元を指定する機能のない IGMPv1、IGMPv2 か、送信元指定なしの IGMPv3 を使用してください。

5.38 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。

○ 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。

5.39 IPv6 マルチキャストルーティング

参照「コマンドリファレンス」/「IPv6 マルチキャスト」

IPv6 環境でマルチキャストルーティングを使用する場合は、上流インターフェースで MLD Snooping を無効にしてください。

5.40 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

○ 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。

○ トランクグループに MLD のグループエントリーをスタティック登録すると、(S,G) エントリーに加えて (*,G) エントリーも作成されます。

○ 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。

5.41 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 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。

5.42 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」

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
```

5.43 ハードウェアパケットフィルター

参照「コマンドリファレンス」/「トラフィック制御」/「ハードウェアパケットフィルター」

VCS のマスター切り替え後に、既存のハードウェアパケットフィルターへ新規フィルター条件を追加した場合、シーケンス番号が正しく割り振られません。追加処理は正常にできているため、show access-list コマンドの表示順にフィルタリングは機能します。

5.44 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。

○ 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。

○ 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でアクションが実行されたポートがマスター切り替えなどでダウンして事前設定された状態になったとき、ポートステータスの表示が err-disabled のままですが、表示上の問題で動作に影響はありません。また、再加入するなどして事前設定された状態ではなくなったときには正常な表示に戻ります。

○ 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。

5.45 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。

5.46 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 リレーと VRRP を併用した場合、VRRP のバーチャル IP アドレス宛てに転送された DNS パケットを DNS サーバーに転送することができません。クライアントには VRRP のバーチャル IP アドレスではなく、VRRP マスタールーターの LAN 側実 IP アドレスをプライマリー DNS サーバーアドレスに、また VRRP バックアップルーターの LAN 側実 IP アドレスをセカンダリー DNS サーバーアドレスとして設定してください。

5.47 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。

5.48 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。

○ DHCP リレー機能において転送可能な DHCP メッセージの最大長を設定した場合、その最大長より大きなパケットを受信してもパケットを正しく破棄せず、DHCP オプションの一部を削除して転送してしまうことがあります。

5.49 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。

○ 複数の DHCPv6 プールを設定する際は、アドレス範囲やプレフィックスが異なる DHCPv6 プールに重複しないように設定してください。

5.50 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。

○ 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。

○ 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 x510L シリーズ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。

○ 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 と表示されてしまいます。

○ 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。

○ 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は、ローカルマスターを再起動してください。

○ 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ます。

○ 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、AMF コントローラーと通信可能であることを確認してからリカバリーを実行してください。

○ 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すが、復旧後約 5 分が経過するとリモートログインを行えるようになります。

5.51 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。

○ 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 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 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。

○ VCS 構成において、大量のルート情報を持っているときにメンバーが加入すると、スレーブを経由する通信の断絶時間が通常より長くなることがあります。また、複数のメンバーが同時に加入するときにもスレーブを経由する通信の断絶時間が通常より長くなることがありますので、再起動を行う場合はローリングリブートを使用してください。マスターを経由する通信には影響はありません。

○ 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。

○ レジリエンシーリンクが設定されたポートに QoS ストームプロテクションを設定しても警告メッセージが表示されなくなりましたが、併用はできません。

○ 4 台以上の VCS 構成の際に reboot rolling コマンドを実行すると、まれに VCS メンバーの内 1 台が、1 回多く再起動する場合がありますが、再起動後は正常に VCS を構成し動作します。

○ VCS 構成時、reload rolling/reboot rolling の実行時や VCS マスターの重複時に一部の VCS メンバーで関連プロセスが異常終了し再起動することがあります。再起動後は正常に VCS グループに復帰します。

○ VCS のスレーブ側で受信し、それをマスター側へ複製する際の CPU 宛てパケットの Queue が誤っています。

○ vlan mode stack-local-vlan コマンドによって、死活監視用の VLAN（スタックローカル VLAN）を使用している環境において、VCS マスターがダウンし、復旧しても、その復旧した機器の死活監視用の VLAN からの ICMP Reply が復旧しない場合があります。通常の通信 (死活監視用の VLAN 以外の VLAN での通信) は影響ありません。

○ 死活監視用の VLAN（スタックローカル VLAN）を使用する際は、死活監視用の VLAN 上で no ip igmp snooping を実行してください。

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）等の補足事項および誤記訂正です。

6.1 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。

6.2 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-StackXS/1.0

6.3 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」

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。

6.4 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。

○ 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。

7　サポートリミット一覧

パフォーマンス	
VLAN 登録数	単体：4094※1 VCS：2000
MAC アドレス（FDB）登録数 ※2	単体：16K※3 VCS：4K
IPv4 ホスト（ARP）登録数 ※2	単体：2K※4 VCS：768
IPv4 ルート登録数	1K ※5
リンクアグリゲーション	
グループ数（筐体あたり）	128 ※6
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	246 ※7 ※8 ※9
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	-

※　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 システム内部で使用する値を含みます。
※3 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。
※4 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。
※5 システムパフォーマンス上、インターフェース経路は 256、スタティック経路は 256 まで登録可能。これ以上の登録は動作保証外です。
※6 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。
※7 アクセスリストのエントリー数を示します。
※8 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。
※9 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。

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 x510L シリーズ 取扱説明書」（613-002068 Rev.A）、コマンドリファレンス「CentreCOM x510L シリーズ コマンドリファレンス」（613-002106 Rev.C）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/