613-002108 Rev.D 150824

AT-AR3050S/AT-AR4050S リリースノート

この度は、AT-AR3050S/AT-AR4050S 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、取扱説明書と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　USB 型データ通信端末による PPP 接続

参照「コマンドリファレンス」/「PPP」

下記の USB 型データ通信端末を利用した PPP 接続に対応しました。

○　NTT ドコモ L-03F
○　NTT コミュニケーションズ UX302NC
○　ソフトバンクモバイル 203HW

なお、サポートする USB 型データ通信端末の最新情報は、弊社ホームページでご確認ください。

2.2　MSS 書き換えの機能拡張

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」

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」

PPP インターフェース上に限定されていた TCP MSS 値の書き換え設定（ip tcp adjust-mss コマンド）が、Ethernet およびトンネルインターフェース上でも可能になりました。またこれまで、MSS 値の書き換えは IPv4 上の TCP パケットに限定されていましたが、新しく追加された ipv6 tcp adjust-mss コマンドにより IPv6 上の TCP パケットに対しても MSS 値の書き換え設定が可能になりました。

2.3　AMF 仮想リンク

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク（AMF）」

AMF 仮想リンクをサポートしました。本製品には最大 60 本の仮想リンクを設定可能です。

2.4 AMF マスター機能（AT-AR4050S のみ）

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）」

AT-AR4050S において AMF マスター機能をサポートしました。AMF マスターライセンス（10 メンバー）により最大 10 台のメンバーを管理可能です。

※AMF マスター機能は AT-AR4050S でのみ利用可能です（AT-AR3050S では利用できません）。

※AT-AR4050S は外部メディアとして USB メモリーと SDHC カードの両方をサポートしていますが、AMF バックアップデータの保存先としては SDHC カードのみ使用可能です。

2.5 AMF バックアップ先の冗長化（AT-AR4050S のみ）

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）」

これまで、AMF のバックアップ先としては、外部 SSH サーバー 2 台、または、外部メディア（USB メモリーか SD/SDHC カード）のどちらか一方しか使えませんでしたが、本バージョンからは両方を同時に使用できるようになりました。これにより、外部 SSH サーバーに接続できないときでも、外部メディアを利用したバックアップ・リストアが可能となります。本機能は初期状態では無効ですが、新しく追加された atmf backup redundancy enable コマンドで有効化できます。

※AT-AR4050S は外部メディアとして USB メモリーと SDHC カードの両方をサポートしていますが、AMF バックアップデータの保存先としては SDHC カードのみ使用可能です。

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（AMF）」

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（AMF）」

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）によって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。

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

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。

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　起動時に下記のメッセージが表示され、サブスクリプションライセンスを有効化できなくなることがありましたが、これを修正しました。

licensing[1285]: ERROR: creating license source from trusted storage: category - public, code - 0x70000024 (Storage binding break found.), system - 0x00000000, location - 0x000f0048 licensing[1285]: fne_feature_licensed 241: Error Initializing client objec

4.2　システム例外の発生時にログファイルを出力する仕組みが正しく動作しないことがありましたが、これを修正しました。

4.3　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。

4.4　WAN ポート（eth1、eth2）を shutdown コマンドで無効化した場合、該当ポートに関する linkDown トラップが送信されませんでしたが、これを修正しました。

4.5　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。

4.6　OSPF が有効な IP インターフェースをいったん削除し、再設定した場合、該当インターフェースで OSPF が有効になりませんでしたが、これを修正しました。

4.7　circuit-failover コマンドを使用している HA モードの VRRP マスタールーターにおいて、LAN ポートのリンクダウンによって VRRP マスターから別の状態に遷移し、その後 LAN ポートがリンクアップした場合、HA LED が橙色の点滅ではなく橙色の点灯になっていましたが、橙色で点滅するよう修正しました。

4.8　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。

4.9 IP レピュテーションデータベースのダウンロード中に IP レピュテーション機能を無効にした場合、再度有効にしても同機能が有効にならない場合がありましたが、これを修正しました。

4.10 ファイアウォールルールと NAT ルールをあわせて 100 個以上設定した場合、スループットが極端に低下することがありましたが、これを修正しました。

4.11 トラフィックシェーピングルールの設定時に、未定義のエンティティーやアプリケーションを指定した場合、トラフィックシェーピング機能を有効にした後でエンティティーやアプリケーションを定義しても、該当ルールが有効になりませんでしたが、これを修正しました。

4.12 PPP インターフェース上に設定したトンネルインターフェースでダイナミック経路制御プロトコルを使用している場合、PPP インターフェースのダウン、アップ後にトンネルインターフェースの通信が復旧しても、ダイナミック経路制御プロトコルによる経路情報の交換ができないことがありましたが、これを修正しました。

4.13 トンネルインターフェースを削除した後、すぐに同じ番号のトンネルインターフェースを作成すると、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。

4.14 IPsec トンネルを多数作成して使用し続けると、下記のようなエラーメッセージが出力されていましたが、これを修正しました。

iked: [INTERNAL_ERR]: sockmisc.c:xxxx:s6endfromto(): bind 1 (Cannot assign requested address)

4.15 認証アルゴリズム SHA256 が正常に動作していなかったため、SHA256 を使用する他社製品との IPsec 接続ができませんでしたが、これを修正しました。

なお本修正により、ファームウェアバージョン **5.4.5-0.4** までの本製品と **5.4.5-1.1** 以降の本製品との間では IPsec 接続ができなくなっています。本製品同士で IPsec 接続を行う場合はファームウェアのバージョンを揃えてください。

4.16 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。

4.17 AMF 接続ポート（AMF リンク）において、AMF の制御パケットを低優先度で出力していましたが、これを修正しました。

4.18 ご購入時の状態であるにもかかわらず AMF のオートリカバリーに失敗することがありましたが、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」

○　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

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 atmf backup 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:/」コマンドにて USB メモリーにアクセスする操作を行ってください。

○　ファイル名には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。

○　フラッシュメモリーから SDHC カードまたは USB メモリーにファイルをコピーする時、途中で SDHC カードや USB メモリーを抜くと、実際はコピーに失敗しているにもかか

わらず、（Fail を表すメッセージではなく、）「successful」というメッセージが表示されます。

○ フラッシュメモリーから SDHC カードまたは USB メモリーにファイルをコピーする時、実際にコピーが完了しても、すぐにコピー完了のメッセージが表示されないことがあります。

○ システム起動時に自動実行されるフラッシュメモリー上のファイルシステムチェックにおいて、まれにエラーが出力されることがありますが、動作には問題ありません。

○ SDHC メモリーカードを装着してすぐに取り外すと、SDHC カードスロットの LED が点灯したままになることがあります。その場合は SDHC カードを装着しなおすことで LED 表示が正常に戻ります。

○ 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+ 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。

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。

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」

○ スクリプト機能を使って OSPF、BGP 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。

○ 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上記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。

○ 複数のトリガーが同時に起動されると、「show trigger counter」で表示されるカウンターが正しい値を表示しなくなります。

5.9 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ 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。

5.10 NTP

参照「コマンドリファレンス」/「運用・管理」/「NTP」

○ 初期設定時など、NTP を設定していない状態で show ntp status コマンドを入力すると、NTP サーバーと同期していることを示す以下のようなメッセージが表示されます。
Clock is synchronized, stratum 0, actual frequency is 0.000PPM, presicion is 2

○ NTPv4 を使用している場合、ntp master コマンドによる NTP 階層レベル（Stratum）の設定と NTP サーバーによる時刻の取得を併用すると、NTP サーバーによって自動決定される階層レベルが優先されます。

○ NTP による時刻の同期を設定している場合、時刻の手動変更は未サポートとなります。

○ ntp master コマンドで <1-15> パラメーターを省略した場合、NTP 階層レベル（Stratum）は 6 になるべきですが、実際は 12 になります。この問題を回避するため、同コマンドでは NTP 階層レベルを明示的に指定してください。

5.11 仮想端末（vty）

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。

5.12 Telnet

参照「コマンドリファレンス」/「運用・管理」/「Telnet」

○ 本製品から他の機器に Telnet で接続しているとき、次のようなメッセージが表示されます。

```
No entry for terminal type "network";
using vt100 terminal settings.
```

○ 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。

5.13 Secure Shell

参照「コマンドリファレンス」/「運用・管理」/「Secure Shell」

○ SSH サーバーにおけるセッションタイムアウト（アイドル時タイムアウト）は、ssh server session-timeout コマンドで設定した値の 2 倍で動作します。

○ 本製品の SSH サーバーに対して、次に示すような非対話式 SSH 接続（コマンド実行）をしないでください。
※ 本製品の IP アドレスを 192.168.10.1 と仮定しています。

```
clientHost> ssh manager@192.168.10.1 "show system"
```

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

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

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

5.14 インターフェース

参照「コマンドリファレンス」/「インターフェース」

○ 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。

5.15 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」

○ 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。

○ 複数ポートにインターフェースモードのコマンドを発行するときは、interface コマンドで対象ポートを指定するときに、通常ポートとして使用できないミラーポートを含めないようにしてください。ミラーポートを含めた場合、一部のポートに設定が反映されなかったり、エラーメッセージが重複して表示されたりすることがあります。

○ ミラーポートとして設定されたポートは、どの VLAN にも属していない状態となりますが、mirror interface none で、ポートのミラー設定を解除し VLAN に所属させても dot1qVlanStaticTable（1.3.6.1.2.1.17.7.1.4.3 ） にポート情報が当該 VLAN に表示されません。ポートに mirror interface コマンドでソースポートのインターフェースとトラフィックの向きを設定した後、設定を外すとポート情報が正しく表示されるようになります。

○ パケットストームプロテクション機能の設定コマンド storm-control level において、受信上限値として 0.0 を設定できません。

5.16 リンクアグリゲーション

参照「コマンドリファレンス」/「インターフェース」/「リンクアグリゲーション」

○ スタティックチャンネルグループ（手動設定のトランクグループ）において、shutdown コマンドによって無効にしていたポートに対して no shutdown コマンドを入力しても、ポートが有効にならないことがあります。
この場合は、再度 shutdown コマンド、no shutdown コマンドを入力してください。

○ スタティックチャンネルグループのインターフェースを shutdown コマンドにより無効に設定した後、リンクアップしているポートをそのスタティックチャンネルグループに追加すると、該当するインターフェースが再び有効になります。

○ show interface コマンドで表示される poX インターフェース（LACP チャンネルグループ）の input packets 欄と output packets 欄の値には、リンクダウンしているメンバーポートの値が含まれません。
LACP チャンネルグループ全体の正確な値を確認するには、poX インターフェースではなく各メンバーポートのカウンターを参照してください。

○ 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。

○ 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。

○ リンクアグリゲーション（LACP およびスタティックチャンネルグループ）使用時に show mac address-table コマンドを実行すると、チャンネルグループ番号ではなく実際に使用されているポート番号が表示されますが、これは表示だけの問題であり動作には影響ありません。

5.17 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」

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。

5.18 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

5.19 USB 型データ通信端末による PPP 接続

参照「コマンドリファレンス」/「PPP」

USB 型データ通信端末「ソフトバンクモバイル 203HW」を LTE 回線のみ使用する設定にしている場合、本製品の USB ポートに 203HW を接続した状態で PPP 関連の設定を変更したときは、いったん USB ポートから 203HW を取り外し、装着しなおしてください。

5.20 ブリッジング

参照「コマンドリファレンス」/「ブリッジング」

○ 実インターフェースとその上に作成した 802.1Q サブインターフェースの Up/Down 状態が異なる場合、サブインターフェースに IP アドレスを設定することができません。サブインターフェースに IP アドレスを設定するときは、実インターフォースとサブインターフェースの Up/Down 状態を合わせてください。

○ 802.1Q サブインターフェースに説明文（description）を設定している場合、「no encapsulation dot1q」で該当サブインターフェースの設定を削除しても、ランニングコンフィグ上に該当サブインターフェースの設定が残ってしまいます。サブインターフェースの設定を削除する場合は、初めに「no description」で説明文を削除してからサブインターフェースの設定を削除してください。

○ 複数の 802.1Q サブインターフェースに対して、同一の IPv4 アドレスや IPv6 アドレスを設定してもエラーになりませんのでご注意ください。

○ L3 トンネルインターフェース（IPsec、GRE、IPv6）は 802.1Q サブインターフェースをサポートしません。これらのインターフェース上に encapsulation dot1q コマンドで 802.1Q サブインターフェースを作成してもエラーになりませんが、動作しないため設定しないでください。

○ bridge-group コマンドでトンネルインターフェースをソフトウェアブリッジに割り当てるとき、次のようなメッセージが表示される場合がありますが、動作に影響はありません。

Warning: Interface tunnel0 is not fully configure yet

5.21 mtu コマンド

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」

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。

5.22 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。

○ 本製品は ECMP（等コストマルチパスルーティング）をサポートしていますが、通信（フロー）単位で送出インターフェースを振り分けるフローベースではなく、パケット単位で振り分けるラウンドロビン方式で動作します。

5.23 RIP

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。

○ PPP インターフェース上に設定した IPsec トンネルインターフェースでは RIP を使用しないでください。サポート対象外です。

○ distribute-list コマンドでトンネルインターフェースを指定した場合、起動時に該当コマンド行がエラーになります。これを回避するには、インターフェーストリガーを使用してトンネルインターフェースがアップしたときに distribute-list コマンドが実行されるようにしてください。

5.24 OSPF

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

○ 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 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。

○ 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。

○ OSPF モードおよび OSPFv3 モードの passive-interface コマンドで、インターフェースを指定せずに実行してすべてのインターフェースで有効にした後、no 形式で一部のインターフェースのみを無効にする操作は行わないでください。

○ PPP インターフェース上に設定した IPsec トンネルインターフェースで OSPF を使用する場合は、該当 IPsec トンネルインターフェースに対して mtu コマンドを実行し、同インターフェースを通るパケットのサイズが 1300 バイト以下になるよう調整してください。

○ OSPF を使用している環境でセカンダリー IP アドレスの設定を動的に行った場合、セカンダリー IP アドレスと同一サブネットのアドレス宛てに本製品の ssh コマンドや ping コマンドなどを実行した場合、始点アドレスとしてプライマリー IP アドレスをセットしたパケットを送信してしまいます。通信先でマネージメント ACL などのアクセス元制限を行っている場合は、本製品のプライマリー IP アドレスからのアクセスも許可するよう設定してください。

5.25 BGP

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

○ IPv6 の BGP 機能において、redistribute コマンドで static を指定するとデフォルトルートを BGP 経路表に追加してしまいます。

○ iBGP セッションにおいて、ORIGINATOR_ID 属性値を「0.0.0.0」として通知してしまいます。

○ IPv4/IPv6 BGP ピアとの接続状態が Established から Idle に変わった場合、show ip bgp summary、show bgp ipv6 summary コマンドの表示項目 Up/Down にはセッション切断後の経過時間が表示されるべきですが、Never と表示されます。

5.26 ARP

参照「コマンドリファレンス」/「IP ルーティング」/「ARP」

○ VRRP とプロキシー ARP の両方を有効にしている VLAN インターフェースにおいて、バーチャル IP アドレスがマスタールーターの実アドレスではない場合、接続機器からの ARP Request に対して、バーチャル MAC アドレスではなく受信インターフェースの実 MAC アドレスで応答することがあります。

○ 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。

5.27 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。

○ ha associate コマンドを設定した状態でバーチャルルーターの設定を削除すると、HA LED が点灯したままになることがあります。バーチャルルーターの設定を削除する場合は、あらかじめ「no ha association」で HA モードの設定を削除した後、バーチャルルーターを削除してください。

○ VRRP のステータス変更時に下記のログメッセージが出力されますが、VRRP の動作に影響はありません。

VRRPD[1255]: VRRP Event: Transition to MASTER state for 2/1/vlan[vid]
HSL[1225]: HSL: ERROR: Insufficient space in Field Processor to add VRRP trap ARP entry

5.28 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、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。

○ 「no ipv6 forwarding」で IPv6 パケット転送機能を無効化した場合、下記の警告メッセージが表示されますが、実際には再起動は不要です。

% Warning: IPV6 forwarding will not be disabled until the switch reboots.

5.29 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。

5.30 RIPng

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

cisco-metric-behavior コマンドは未サポートです。

5.31 OSPFv3

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。

○ IPv6 トンネルインターフェース上で OSPFv3 を使用しルート情報を交換した場合、対向のトンネルインターフェース上に割り当てられた IPv6 アドレスのみ 128 ビットマスクで登録されますが、通信に影響はありません。

○ OSPFv3 において、自装置のトンネルインターフェースの経路情報を通知するとき、メトリックを 0 として通知します。

○ OSPFv3 と BGP4+ の併用環境において、BGP4+ 経路を OSPFv3 で再通知する場合、AS 外部 LSA のネクストホップアドレスとしてリンクローカルアドレスを設定してしまいます。BGP4+ 経路を OSPFv3 で再通知する場合、ルートマップを使用してネクストホップアドレスを変更してください。

○ エリア間経路として通知していたインターフェース経路を AS 外部経路に変更する場合は、最初に「no redistribute connected」を実行してから、「redistribute connected」を入力してください。

5.32 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。

5.33 PIM

参照「コマンドリファレンス」/「IP マルチキャスト」/「PIM」

○ 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。

○ PIM Prune メッセージを受信してもテーブル上から当該グループが完全に削除されないことがあります。ただし、マルチキャストパケットが転送され続けることはありません。（PIM-SMv4、PIM-SMv6 共通 ）

5.34 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 が有効化されている VLAN の所属ポートで受信した IGMP Leave メッセージは、同一 VLAN 内にフラッディングされます。

○ 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。

5.35 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 が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。

5.36 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。

5.37 PIMv6

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。

○ 本バージョンでサポートしている PIM-SMv6 は、ソース指定無しの JOIN (*,G)Join のみサポートで、ソース指定有りの JOIN (S,G)Join は未サポートとなります。

○ 同一インターフェース上で ipv6 pim sparse-mode コマンドを繰り返し実行すると PIM-SMv6 が有効にならなくなる場合があるため、複数回実行しないでください。

○ ipv6 pim spt-threshold コマンドを no 形式で実行しないでください。

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

○ 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。

○ 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。

5.39 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。

○ 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。

5.40 UTM

参照「コマンドリファレンス」/「UTM」

○ Web コントロールモードの rule コマンドを no 形式で実行するとき（ルールを削除するとき）、存在しないルール番号を指定してもエラーになりません。ルール番号をミスタイプした場合など、削除したつもりのルールが削除されていなくても気付かない可能性があるため、ルール削除時にはご注意ください。

○ ファイアウォールルールと NAT ルールの Hits カウンターは、2147483647 を超えるとマイナス表示になります。

○ エンティティー定義に使う zone、network、host コマンドのエラーメッセージでは使用可能文字にアットマーク（@）が含まれていますが、実際にはアットマークは使用できません。

○ ファイアウォールと NAT の最大ルール数は両機能あわせて 500 ですが、ルール数が 500 に近づくにつれてパフォーマンスが低下するため、なるべくルール数は少なく設定してください。

○ 無効な NAT ルールが存在する状態で show nat rule コマンドを実行すると、次のようなログが出力されます。
yyyy mm dd hh:mm:ss user.err awplus firewalld: NAT: Sending iptables -t nat -L PORT_FORWARDING_RULE_10 -v -x 2>&1 ¦ grep DNAT ¦ awk '{print $1}' failed

○ アプリケーションコントロール（DPI）機能を有効にした場合、NAT ルールにおいてアプリケーション「ftp」が正しく動作しなくなります。これを回避するため、アプリケーションコントロール（DPI）機能を使用する場合は、下記のようにして FTP 通信を表すカスタムアプリケーション「ftp」を定義してください。

```
awplus(config)# application ftp
awplus(config-application)# protocol tcp
awplus(config-application)# sport 1024 to 65535
awplus(config-application)# dport 21
```

○ application コマンドで作成するカスタムアプリケーション定義名は 63 文字以内にしてください。

5.41 トラフィックシェーピング

参照「コマンドリファレンス」/「トラフィック制御」/「トラフィックシェーピング」

○ トラフィックシェーピングルールを設定していない状態で仮想帯域を設定し、その後トラフィックシェーピング機能を有効にした場合、show traffic-shaping interface コマンドの結果が正常に表示されません。これを回避するには、最初にトラフィックシェーピング機能を有効にしてください。

○ トラフィックシェーピングルールの設定時に、未定義のアプリケーションを指定するとエラーメッセージが出力されます。トラフィックシェーピングルールを設定するときは、使用するアプリケーションをあらかじめ定義してから、ルールを設定してください。

○ トラフィックシェーピング機能を有効にしているとき、次のようなログメッセージが出力されることがありますが、動作には影響ありません。
kernel: HTB: quantum of class 10001 is big. Consider r2q change

5.42 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。

5.43 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。

5.44 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。

○ 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。

5.45 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。

5.46 トンネルインターフェース

参照「コマンドリファレンス」/「VPN」/「トンネルインターフェース」

○ システム起動時、トンネルインターフェースは最初にアップした後、いったんダウンして再度アップしますが、通信に影響はありません。

○ 複数のトンネルインターフェースで同じ対向アドレス（tunnel destination）を設定した場合、2 つ目以降のトンネルインターフェースでは対向アドレスの設定削除ができません。2 つ目以降のトンネルインターフェースで対向アドレスを変更したい場合は、tunnel destination コマンドを再実行して上書き設定するか、いったん該当トンネルインターフェースを削除したのち、再作成してください。

○ 無効化されているトンネルインターフェースを「no shutdown」で有効化すると、最初にアップした後、いったんダウンして再度アップします。

○ interface コマンドでトンネルインターフェースを作成したら、移行先のインターフェースモードで引き続きトンネリング方式（tunnel mode xxxx）などの設定を行ってください。interface コマンドで作成しただけのトンネルインターフェースは、show interface コマンドでは確認できますが、ランニングコンフィグでは確認できず、また「no interface tunnelX」で削除することもできません。

○ GRE および IPv6 トンネルインターフェースの TTL を tunnel ttl コマンドで変更した場合は、設定を保存して再起動してください。変更後に再起動しないと、ルーティングが正常に行われなくなることがあります。

○ トンネルインターフェースを削除した場合、下記の不要なログメッセージが出力されますが、動作への影響はありません。

```
BGP[1293]: Parse error for message Link Down ret=-1
PIM-SMv6[1262]: Parse error for message Link Down ret=-1
PIM-DM[1272]: Parse error for message Link Down ret=-1
PIM-SM[1290]: Parse error for message Link Down ret=-1
```

○ トンネルインターフェースの下位インターフェース（親インターフェース）に対して「shutdown」/「no shutdown」を繰り返し実行しないでください。繰り返し実行すると、トンネル経由の通信が行えなくなることがあります。

○ トンネルインターフェース上でダイナミックルーティングプロトコルを使用している場合、該当トンネルインターフェースを削除し、再度追加した場合は、設定を保存して再起動してください。

○ トンネルインターフェースの MTU を変更すると次のようなエラーメッセージがログに出力されますが、通信には影響ありません。
2015 May 18 12:38:47 user.err A1-Edge HSL[1253]: HSL: ERROR: Error finding iif L2 interface info 11
2015 May 18 12:38:47 user.err A1-Edge HSL[1253]: HSL: ERROR: Group (239.255.1.1) Source

○ tunnel source コマンドでは「lo」から始まる無効なインターフェース名を設定することができますが、動作しないため該当インターフェースを指定しないようにしてください。

○ PPP インターフェース上に作成したトンネルインターフェースは、PPP インターフェースがアップすると、最初にアップした後、いったんダウンして再度アップしますが、通信に影響はありません。

○ トンネルインターフェースの設定を変更した場合は、設定を保存して再起動してください。

○ PPP インターフェース上にトンネルインターフェースを作成している場合、PPP インターフェースのアップ時に下記のログメッセージが出力されることがありますが、動作には影響ありません。
kern.crit awplus kernel: protocol 0806 is buggy, dev tunnel1

5.47 IPsec

参照「コマンドリファレンス」/「VPN」/「IPsec」

○ IPsec を使用するトンネルインターフェースのサポートリミットは最大 100 個です。本件は IPsec トンネルインターフェースに限らず、tunnel protection ipsec コマンドで IPsec 保護を適用した L2TPv3、GRE、IPv6 トンネルインターフェースにも当てはまります。

○ 多数の IPsec over IPv6 トンネルインターフェースが同時に VPN 接続を開始した場合、不正な ISAKMP メッセージを送信することがありますが、その後正常な ISAKMP メッセージを送信するため、VPN 接続には問題ありません。

○ IPsec トンネルインターフェース上で転送できる最大パケットサイズは 2700 バイトです。

○ 対向機器との IPsec 接続が切断されても ISAKMP SA および IPsec SA が削除されないことがありますが、対向機器から新しい IPsec セッションが開始されれば新しい SA を作成します。

○ システム起動後、最初の IPsec 接続では通常よりも時間がかかることがあります。

○ 対向する両方の装置がほぼ同時に IPsec 接続を開始した場合、IPsec 接続が確立しても、show ipsec sa コマンドで確立した IPsec SA の情報が表示されないことがありますが、通信への影響はありません。

○ crypto isakmp key コマンドにおいて、対向装置の ISAKMP ID を IPv6 アドレスで指定するときは、RFC5952（IPv6 アドレスの推奨表記）に準拠する形式で IPv6 アドレスを指定してください。RFC5952 に準拠しない形式で IPv6 アドレスを指定した場合は、設定を保存して再起動すると、事前共有鍵の復号化に失敗するようになるためご注意ください。

○ IPsec トンネルインターフェースを複数使用している場合、IPsec SA のネゴシエーション時に次のようなログメッセージが表示されますが、IPsec 接続に問題はありません。

daemon.err DUTB iked: [INTERNAL_ERR]: ike_pfkey.c:218:log_rcpfk_error(): 0:? - ?:(nil):sadb_poll: error at the kernel on DELETE, No such process
daemon.warning DUTB iked: [PROTO_WARN]: ikev2.c:4656:ikev2_process_delete(): 998:192.168.224.2[500] - 192.168.224.1[500]:(nil):can't find sa for proto ESP spi 0x02ed3167

○ IPsec トンネルインターフェースでは、show interface コマンドの送信パケット（output packets）カウンターがカウントされません。これは表示だけの問題であり、通信には影響ありません。

5.48 L2TPv3

参照「コマンドリファレンス」/「VPN」/「L2TPv3」

L2TPv3 トンネルインターフェース経由で SSH を使用する場合は、mtu コマンドで L2TPv3 トンネルインターフェースの MTU を 1300 バイト以下に設定してください。

5.49 OpenVPN

参照「コマンドリファレンス」/「VPN」/「OpenVPN」

○ OpenVPN Tun(L3) トンネルインターフェースの設定時、「IP packet with unknown IP version=15 seen」というログメッセージが出力されることがありますが、動作に影響はありません。

○ 接続が確立されている OpenVPN トンネルインターフェースを削除すると、次のようなエラーメッセージが表示されますが、通信には問題ありません。

PIM-DM[1280]: Parse error for message Link Down ret=-1

5.50 GRE

参照「コマンドリファレンス」/「VPN」/「GRE」

IPsec 保護（tunnel protection ipsec）を適用している GRE トンネルインターフェース上にトラフィックが存在する状態で該当インターフェースがダウンした場合、informational レベルの下記ログメッセージが繰り返し出力されます。ただし、本ログメッセージは informational レベルのため、初期設定では buffered ログ、permanent ログには保存されず、show log、show log permanent コマンドでも確認できません。

iked: [INTERNAL_ERR]: ikev2_auth.c:555:ikev2_auth_verify(): 4:xx.xx.xx.xx[500] - yy.yy.yy.yy[500]:(nil):no shared key with peer

5.51 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 リンクとして使用しているスタティックチャンネルグループの設定や構成を変更する場合は、次に示す手順 A・B のいずれかにしたがってください。

[手順 A]
1. 該当スタティックチャンネルグループに対して shutdown を実行する。
2. 設定や構成を変更する。
3. 該当スタティックチャンネルグループに対して no shutdown を実行する。

[手順 B]
1. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して no switchport atmf-link を実行する。
2. 設定や構成を変更する。
3. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して switchport atmf-link を実行する。

○ リブートローリング機能でファームウェアバージョンを A から B に更新する場合、すでに対象ノードのフラッシュメモリー上にバージョン B のファームウェアイメージファイルが存在していると、ファームウェアの更新に失敗します。このような場合は、対象ノードから該当するファームウェアイメージファイルを削除してください。

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

○ AMF マスターが AMF メンバーよりも後に AMF ネットワークに参加するとき、AMF マスターのコンフィグにてその他メンバーからのワーキングセット利用やリモートログインに制限がかけてあっても、既存のメンバーに対してこれらの制限が反映されません。再度 AMF マスター上で atmf restricted-login コマンドを実行することで、全ての AMF メンバーに対して制限をかけることができます。

○ AMF 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。

○ 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。

○ 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 マスターによる自動バックアップの実行時に本製品のバックアップが失敗することがありますが、次のバックアップタイミングでは成功します。

○ AMF 仮想リンクを複数使用してリング構成の AMF 環境を構築する際は、AMF ドメインコントローラー同士を接続する仮想リンクの ID を小さく設定し、AMF 接続ポートのステータスが「Forwarding」になるようにしてください。

○ 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。

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

○ HA モード VRRP を使用する AMF メンバーと、AMF マスターとの間で AMF 仮想リンクが 1 本のみ設定されている（VRRP マスタールーターとバックアップルーターの共通 IP アドレスを AMF 仮想リンクの終端アドレスとして指定した）構成において、VRRP マスタールーターがダウンした場合、他の AMF メンバーにワーキングセット経由で接続できなくなることがあります。このような構成で AMF 仮想リンクを使用する場合は、VRRP を構成する各 AMF メンバーの LAN 側 IP アドレスを終端アドレスとして、AMF 仮想リンクを複数設定してください。

6 マニュアルの補足

6.1 サポートする USB 型データ通信端末

サポートする USB 型データ通信端末につきましては、弊社ホームページでご確認ください。

6.2 USB ポート LED

参照「取扱説明書」24 ページ

USB ポートにデータ通信端末を装着する場合、USB ポート LED の動作は次のようになります。

LED	色	状態	表示内容
USB	緑	点灯	データ通信端末が装着され、本製品によって正しく認識されています。
	橙	点灯	データ通信端末として使用できない機器が装着されています。
	ー	消灯	データ通信端末が装着されていません（装着された機器を認識できない場合を含みます）。

6.3 サブスクリプションライセンス

参照「コマンドリファレンス」/「UTM」

サブスクリプションライセンスはファームウェアバージョン **5.4.5-1.1** 以降でのみご使用いただけます。

6.4 サポートする OpenVPN クライアント

参照「コマンドリファレンス」/「VPN」/「OpenVPN」

本バージョンでは、OpenVPN クライアントとして下記 OS/ アプリケーションの組み合わせをサポートします。

OS	アプリケーション
Windows7 (32bit)	OpenVPN GUI v5 (2.3.6)
	OpenVPN GUI v7 (2.3.7)
	vpnux Client (ver.1.3.0.0)
Windows7 (64bit)	OpenVPN GUI v5 (2.3.6)
	OpenVPN GUI v7 (2.3.7)
	vpnux Client (ver.1.3.0.0)
Windows8.1 (64bit)	OpenVPN GUI v5 (2.3.6)
	OpenVPN GUI v7 (2.3.7)
	vpnux Client (ver.1.3.0.0)
MAC OS X	Tunnelblick 3.4.3
Android 4.4.x	OpenVPN for Android 0.6.29
iOS 8	OpenVPN Connect 1.0.5

7　サポートリミット一覧

	AT-AR3050S	AT-AR4050S
パフォーマンス		
VLAN 登録数	4094	
MAC アドレス（FDB）登録数	1024	
IPv4 ホスト（ARP）登録数	1024	
IPv4 ルート		
IPv4 スタティックルート登録数	1000	
RIPv1/v2 ルート登録数	1500	
OSPFv2 ルート登録数	1000	
BGP4 ルート登録数	10000	
IPv6 ルート		
IPv6 スタティックルート登録数	1000	
RIPng ルート登録数	1500	
OSPFv3 ルート登録数	1000	
BGP4+ ルート登録数	10000	
リンクアグリゲーション		
グループ数（筐体あたり）	2※1	
ポート数（グループあたり）	4※2	
VPN		
IKEv2 同時接続可能セッション数	100※3	
L2TPv3 同時接続可能セッション数	256※3	
PPPoE		
PPPoE 同時接続可能セッション数	20	
ローカル RADIUS サーバー ※4		
ユーザー登録数	5000	
RADIUS クライアント（NAS）登録数	1000	
ファイアウォール		
セッション数	65535	
ルール数	500※5	

※1 スタティックチャンネルグループと LACP チャンネルグループを合わせて 2 グループまでサポートします。
※2 LAN 側スイッチポートのみ使用可能です。
※3 共有するトンネルインターフェースの合計値です。
※4 OpenVPN でのみ使用可能です。
※5 ファイアウォールルールと NAT ルールを合わせて 500 ルールをサポートします。

8　最新マニュアルについて

最新の取扱説明書（613-002124 Rev.A）とコマンドリファレンス（613-002107 Rev.D）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/