613-002211 Rev.B 151109

Allied Telesis

CentreCOM® *Secure Hub SH230*シリーズ リリースノート

この度は、CentreCOM Secure Hub SH230 シリーズ（以下、SH230 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、本製品の位置づけや、参照すべきマニュアル、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　5.4.5-1.3

2　本製品について

SH230 シリーズは、CentreCOM x230 シリーズと同様のハードウェア・アーキテクチャーを採用し、一部の機能を限定することで高いコストパフォーマンスを実現した製品です。

ご使用にあたっては、本リリースノートと以下に述べる x230 シリーズ用のマニュアル（取扱説明書、コマンドリファレンス）を参照してください。これらのマニュアルは、弊社ホームページに掲載されています。

2.1　ハードウェア

SH230 シリーズ各機種のハードウェアは、本体の製品名表示が異なる点を除き x230 シリーズの下記機種と同様のハードウェア・アーキテクチャーを採用しています。

SH230 シリーズ	x230 シリーズ	参照すべき取扱説明書
AT-SH230-10GP	AT-x230-10GP	CentreCOM x230 シリーズ 取扱説明書（613-001870 Rev.C）
AT-SH230-18GP	AT-x230-18GP	
AT-SH230-28GP	AT-x230-28GP	

SH230 シリーズ各機種の取り扱いについては、「参照すべき取扱説明書」欄に記載した x230 シリーズ用の取扱説明書をご参照ください。その際、製品名を x230 シリーズのものから SH230 シリーズのものに読み替えてくださいますようお願い申し上げます。

2.2　ファームウェア

SH230 シリーズのファームウェアは SH230 シリーズ専用であり、x230 シリーズのファームウェアとは異なりますが、サポート機能に差分がある点を除き、ファームウェアの動作は基本的に同じです。

SH230 シリーズ用ファームウェアの機能とコマンドについては、後述するサポート機能の差分を念頭に置きながら、下記の x230 シリーズ用コマンドリファレンスをご参照ください。その際、適宜製品名を x230 シリーズのものから SH230 シリーズのものに読み替えてくださいますようお願い申し上げます。

参照すべきコマンドリファレンス
CentreCOM x230 シリーズ コマンドリファレンス 5.4.5 （ファームウェアバージョン 5.4.5-1.1 用）（613-001990 Rev.F）

2.3 サポート機能

SH230 シリーズのサポート機能を、前述の x230 シリーズ用コマンドリファレンスに掲載されているサポート機能との差分として示します。

サポート対象外、または機能が制限されるもの

コマンドリファレンスに掲載されている下記の機能は、SH230 シリーズではサポート対象外であるか、機能が制限されます。

- **ローカル RADIUS サーバー**
  「運用・管理」/「RADIUS サーバー」の全コマンドがサポート対象外です。

- **NTP サーバー**
  「運用・管理」/「NTP」の下記コマンドはサポート対象外です。
  （NTP クライアント機能はサポート対象）
  ntp access-group
  ntp broadcastdelay
  ntp master

- **AMF メンバー機能の制限**
  本製品の AMF メンバー機能はエッジノード向けの限定版であり、通常の AMF メンバーと比べて下記の制限があります。
  ○ AMF ネットワークへの接続が AMF リンク 1 本に限定される
  ○ AMF クロスリンク、AMF 仮想リンクは使用できない

  これにともない、「アライドテレシスマネージメントフレームワーク（AMF）」/「コマンド」の下記コマンドはサポート対象外になります。
  （これら以外にマスター、コントローラー用のコマンドもサポート対象外です）
  atmf virtual-link
  show atmf virtual-links
  switchport atmf-crosslink

- **AMF マスターのバージョン制限**
  SH230 シリーズを AMF メンバーとして管理するには、AMF マスターにバージョン 5.4.5-2.x 以降のファームウェアが必要です。

- **Web GUI**
  「Web GUI」の掲載内容はすべてサポート対象外です。

その他、仕様やサポート条件が異なるもの

コマンドリファレンスに掲載されている下記の機能は、x230 シリーズと SH230 シリーズで仕様やサポート条件が異なります。

- **製品名（Board Name）表示と SNMP のシステム識別子（sysObjectID）**
  show system コマンドの Board Name 欄には SH230 シリーズの製品名が表示されます。また、sysObjectID にも SH230 シリーズ固有の値がセットされます。

- **UDLD**
  UDLD は、x230 シリーズではフィーチャーライセンスが必要ですが、SH230 シリーズではフィーチャーライセンスなしで使用できます。

- **AMF リカバリーと予約済みグループ名**
  AMF において SH230 シリーズと x230 シリーズは別機種として扱われますので、リカバリー時に x230 シリーズの代替機として SH230 シリーズを使う、あるいは、SH230 シリーズの代替機として x230 シリーズを使うことはできません。また、ワーキングセットにおいて、すべての SH230 シリーズを表す予約済みグループ名は sh230 となります。

3 本バージョンでの制限事項

ファームウェアバージョン **5.4.5-1.3** には、以下の制限事項があります。

3.1 システム

参照 **「コマンドリファレンス」/「運用・管理」/「システム」**

○ システム起動時に下記のコンソールメッセージやログメッセージが出力されることがありますが、動作には影響ありません。

・ コンソールメッセージ
stop: Unable to stop job: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.
xx:xx:xx awplus init: getty (ttyS0) main process (XXXX) terminated with status 1

・ ログメッセージ
daemon.warning awplus init: network/getty_console (ttyS0) main process (XXXX) terminated with status 1

○ 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。

3.2 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。

○ コマンドラインインターフェース（CLI）の操作中に Ctrl/C や Ctrl/Z を入力して反応がなくなった場合は、もう一度 Ctrl/C を入力するか、Ctrl/D を入力してください。

○ 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。

3.3 ファイル操作

参照 **「コマンドリファレンス」/「運用・管理」/「ファイル操作」**

○ ファイル名にスペースは使用できません。

○ フラッシュメモリーから SDHC カードにファイルをコピーするとき、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。

○ 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。

3.4 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。

3.5 ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○ no log buffered コマンドを入力してランタイムメモリー（RAM）へのログ出力を一度無効にした後、default log buffered コマンドを実行しても、ログ出力が再開しません。その場合は「log buffered」を実行することにより再開できます。

○ 複数の VLAN に所属する SFP モジュールをホットスワップすると、次のようなログが表示されます。

user.warning awplus NSM[XXXX]: 601 log messages were dropped - exceeded the log rate limit

これは短時間に大量のログメッセージが生成されたため一部のログ出力を抑制したことを示すものです。ログを抑制せずに出力させたい場合は、log-rate-limit nsm コマンドで単位時間あたりのログ出力上限設定を変更してください。

3.6 スクリプト

参照「コマンドリファレンス」/「運用・管理」/「スクリプト」

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

3.7 トリガー

参照「コマンドリファレンス」/「運用・管理」/「トリガー」

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

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

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

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

3.8 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

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

○ IP-MIB は未サポートです。

○ VLAN 名を SNMP の dot1qVlanStaticName から設定する場合は、31 文字以内で設定してください。

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

3.9 sFlow

参照「コマンドリファレンス」/「運用・管理」/「sFlow」

sflow collector コマンドで UDP ポートを変更したのち、UDP ポートを初期値に戻す場合は、「no sflow collector」ではなく「sflow collector port 6343」を実行してください。

3.10 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

○ 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。

3.11 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。

3.12 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.
```

3.13 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。

3.14 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」

○ SFP ポートでは、polarity コマンドでのインターフェースの極性の固定設定は未サポートです。

○ SFP ポートで Copper SFP（AT-MG8T）を使用する際、Polarity Auto でリンクアップしたときの表示が必ず MDI と表示されてしまいます。

○ インターフェースの状態が約 248 日間変更されないと、show interface コマンドで表示される Time since last state change 欄の内容が不正になります。

3.15 ポートミラーリング

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

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

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

3.16 ループガード

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ LDF 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。

3.17 リンクアグリゲーション

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

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

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

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

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

○ 同じ認証設定を持つ複数の LACP チャンネルグループ上でゲスト VLAN を使用している場合、これらの LACP チャンネルグループに対して同時に shutdown コマンドを実行しないでください。この操作を行うと認証関連プロセスが異常終了し、システムを再起動するまで認証を再開できなくなります。

3.18 ポート認証

参照 「コマンドリファレンス」/「インターフェース」/「ポート認証」

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

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

○ 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。

○ 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。

3.19 Power over Ethernet

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

○ 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。

○ 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。

○ インターフェースで PoE 機能を無効にし、再度機能を有効にしたい場合は、5 秒程度経ったあとに行ってください。

3.20 バーチャル LAN

参照 「コマンドリファレンス」/「インターフェース」/「バーチャル LAN」

○ プライベート VLAN からプライマリー VLAN を削除する場合は、事前にプライマリー VLAN、セカンダリー VLAN ともに、プライベート VLAN の関連付けを解除してください。その後、プライマリー VLAN のみを削除、再作成し、改めてプライベート VLAN とプライマリー VLAN、セカンダリー VLAN の関連付けを行ってください。

○ エンハンストプライベート VLAN を設定したポートからプライベート VLAN 用ポートとしての設定を削除すると、該当のポートでパケットが転送できなくなります。プライベート VLAN 用ポートとしての設定を削除した後は、本製品を再起動してください。

○ プライベート VLAN 設定時に一度設定したホストポートは、その後設定を削除しても、show vlan private-vlan の表示に反映されず、ホストポートとして表示されたままになります。

○ プライベート VLAN でセカンダリー VLAN を削除したとき、private-vlan association コマンドの設定を削除することができなくなります。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。

○ 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。

3.21 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。

3.22 イーサネットリングプロテクション（EPSR）

参照「コマンドリファレンス」/「L2 スイッチング」/「イーサネットリングプロテクション」

EPSR 内のリンクダウンが発生した機器が、マスターからのリンクダウンパケットを受け取っても FDB 情報をクリアしない場合があります。また、リンクダウンが発生した機器は本来であれば FDB の全クリアする必要がありますが、該当ポートの FDB はリンクダウンによってクリアされるため、通信に影響はありません。

3.23 IP インターフェース

参照「コマンドリファレンス」/「IP」/「IP インターフェース」

○ DHCP クライアント機能によって IP アドレスを取得したとき、IP アドレス使用状況確認パケットを送出しません。

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

3.24 ARP

参照「コマンドリファレンス」/「IP」/「ARP」

○ マルチキャスト MAC アドレスをもつスタティック ARP エントリーを作成した後、それを削除してから arp-mac-disparity コマンドを有効にして、同一のエントリーをダイナミックに再学習させる場合は、設定後にコンフィグを保存して再起動してください。

○ 同一 MAC アドレスに対して複数の ARP エントリー（異なる IP アドレス）を登録している場合、そのうちの 1 つを削除すると、残りの ARP エントリーに対応する FDB エントリーも削除されます。その場合は、手動でスタティックな FDB エントリーを登録してください。

○ 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。

○ 認証済みの Supplicant の情報が show arp コマンドで表示されませんが、表示上の問題で実際には通信は可能です。

3.25 IPv6

参照「コマンドリファレンス」/「IPv6」

○ 自身の IPv6 アドレス宛てに ping を実行するとエラーメッセージが表示されます。

○ フラグメントされた IPv6 Echo Request は利用できません。利用した場合 Duplicate パケットは正しく再構築されませんのでご注意ください。

3.26 IGMP Snooping

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

○ マルチキャストグループをスタティックに登録している状態で、同じマルチキャストグループをダイナミックに学習すると、その後スタティック登録したグループを削除しても、show ip igmp groups コマンドと show ip igmp snooping statistics interface コマンドの表示からは該当グループが削除されません。これは表示だけの問題で動作には影響ありません。

○ IGMP Snooping が有効な状態で、一旦無効にし、再度有効にした場合、その後に受信する IGMP Report を全ポートにフラッディングします。
IGMP Snooping を再度有効にした後、clear ip igmp group コマンドを実行して全てのエントリーを消去することで回避できます。

○ Include リスト（送信元指定）付きのグループレコードが登録されている状態で、あるポートに接続された唯一のメンバーからグループ脱退要求を受信すると、そのポートには該当グループのマルチキャストトラフィックが転送されなくなりますが、他のポートで同じグループへの参加要求を受信すると、脱退要求によって転送のとまっていたポートでもマルチキャストの転送が再開されてしまいます（この転送は、脱退要求を受信したポートの Port Member list タイマーが満了するまで続きます）。

○ ダイナミック登録されたルーターポートを改めてスタティックに設定した場合、ダイナミック登録されてから一定時間が経過すると設定が削除されます。また、一定時間が経過するまでの間、コンフィグ上にはスタティック設定が表示されますが、ip igmp snooping mrouter interface コマンドを no 形式で実行しても、コンフィグから削除することができません。
ルーターポートをスタティックに設定する場合は、該当のポートがダイナミック登録されていないことを確認してください。

○ 未認識の IGMP メッセージタイプを持つ IGMP パケットは破棄されます。

○ 不正な IP チェックサムを持つ IGMP Query を受信しても破棄しません。そのため、当該の IGMP Query を受信したインターフェースはルーターポートとして登録されてしまいます。

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

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

3.27 MLD Snooping

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

○ clear ipv6 mld コマンド実行時に「% No such Group-Rec found」というエラーメッセージが表示されることがありますが、コマンドの動作には問題ありません。

○ MLD メッセージを受信する環境では MLD Snooping を有効にしてください。MLD snooping が無効に設定されたインターフェースで MLD メッセージを受信すると次のようなログが出力されます。

NSM[1414]: [MLD-DECODE] Socket Read: No MLD-IF for interface port6.0.49

○ MLD Snooping の Report 抑制機能が有効なとき（初期設定は有効）、ルーターポートで受信した MLDv1 Report または Done メッセージを受信ポートから再送出してしまいます。これを回避するには、「no ipv6 mld snooping report-suppression」で Report 抑制機能を無効化してください。

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

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

3.28 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
```

○ show platform classifier statistics utilization brief コマンドにおいて、QoS 機能が使用できる内部領域の総容量（Total）が 896 と表示されますが、正しくは 384 です。

3.29 Quality of Service

参照「コマンドリファレンス」/「トラフィック制御」/「Quality of Service」

○ match dscp コマンドの設定を削除する際、no match dscp と入力するとエラーとなります。no match ip-dscp コマンドを入力することで、設定を削除できます。

○ wrr-queue disable queue コマンドを設定している状態で no mls qos コマンドにより QoS 自体を無効にする場合は、先に no wrr-queue disable queue コマンドを実行してください。

○ QoS の送信スケジューリング方式（PQ、WRR）が混在するポートを手動設定のトランクグループ（スタティックチャンネルグループ）に設定した場合、ポート間の送信スケジュールが正しく同期されません。トランクグループを設定した場合は、個々のポートに同じ送信スケジュール方式を設定しなおしてください。

○ ポリシーマップ名に「|」（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。

○ 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。

3.30 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 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。

○ 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。

○ 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 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 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。

○ SH230 シリーズと x230 シリーズが混在する AMF ネットワークにおいて、atmf distribute firmware または atmf reboot-rolling コマンドで AMF ノードのファームウェアを更新する場合、SH230 シリーズと x230 シリーズは他の機種と同時に更新せず、「SH230 シリーズだけ」、「x230 シリーズだけ」というように個別にワーキングセットを指定して更新してください。

また、前記コマンドの URL パラメーターには、ファームウェアイメージファイルを明示的に指定してください。

例）atmf reboot-rolling で SH230 シリーズと x230 シリーズを更新する場合

(1) SH230 シリーズだけを対象とするワーキングセットに入り、SH230 用のイメージファイルを指定してファームウェアを更新

```
SBx81# atmf working-set group sh230
AMF001[2]# atmf reboot-rolling usb:/fw/SH230-5.4.5-1.x.rel
```

(2) x230 シリーズだけを対象とするワーキングセットに入り、x230 用のイメージファイルを指定してファームウェアを更新

```
AMF001[2]# atmf working-set group x230
AMF001[4]# atmf reboot-rolling usb:/fw/x230-5.4.5-1.x.rel
```

4 マニュアルの補足・誤記訂正

各種ドキュメントの補足事項および誤記訂正です。

4.1 サポートする SFP モジュールについて

本製品がサポートする SFP モジュールの最新情報については、弊社ホームページをご覧ください。

5 サポートリミット一覧

パフォーマンス	
VLAN 登録数	256
MAC アドレス（FDB）登録数 ※1	16K
IPv4 ホスト（ARP）登録数 ※1	-
IPv4 ルート登録数	-
リンクアグリゲーション	
グループ数（筐体あたり）	28 ※2※3
ポート数（グループあたり）	8
ハードウェアパケットフィルター	
登録数	118 ※4※5※6
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	-
RADIUS クライアント（NAS）登録数	-
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 システム内部で使用する値を含みます。
※2 AT-SH230-28GP の場合。AT-SH230-10GP は 10 グループ、AT-SH230-18GP は 18 グループをサポートします。
※3 スタティックチャンネル、LACP 合わせて 28 グループをサポートします。
※4 アクセスリストのエントリー数を示します。
※5 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。
※6 ユーザー設定とは別に、アクセスリストを使用する機能を有効化した場合に消費されるエントリーを含みます。

6　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。

7　マニュアルについて

本製品使用時にご参照いただくマニュアルは、1 ページの「2 本製品について」に記載されています。本リリースノートは、同ページ記載のマニュアルに対応した内容になっていますので、必要に応じて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/