613-001467 Rev.A 101210

CentreCOM® *x200*シリーズ リリースノート

この度は、CentreCOM x200 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 5.3.4A-0.1

2 本バージョンでの制限事項

ファームウェアバージョン **5.3.4A-0.1** には、以下の制限事項があります。

2.1 show tech-support コマンド

参照「コマンドリファレンス」/「運用・管理」/「システム」

show tech-support コマンド実行時に不正なエラーメッセージが表示されます。これは表示だけの問題で、ファイルへの出力は正常に行われます。

2.2 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ 本製品で SNMPv3 を使用して、SNMP マネージャーとして SwimView を接続した環境において、本製品を再起動すると、SwimView との接続ができなくなります。
なお、SNMP マネージャーとして Swim Manager を接続した場合は、本現象は発生しません。また、SwimView を接続した場合でも、SNMPv1 または SNMPv2c を使用する場合は、本現象は発生しません。

○ Ether-Like.mib、dot3StatsTable の値が一部 CLI 上の値と一致しない場合があります。
dot3StatsTable には主にポートカウンター情報のオブジェクトがあります。
ポートカウンター情報は CLI の show platform port counters コマンドで確認してください。

2.3 SSH サーバー

参照「コマンドリファレンス」/「運用・管理」/「Secure Shell」

SSH サーバーのリスニング TCP ポート番号を 23 に設定しないてください。23 に設定すると不正なログが大量に出力されます。

2.4 ポートセキュリティー

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ ポートセキュリティーの restrict アクションを有効化しているポートにおいて、不正なパケットを受信するたびに SNMP トラップを送信します（SNMP トラップは、各 MAC アドレスに対して最初の一回だけ送信するのが本来の仕様です）。

○ ポートセキュリティーにおいて、不正パケット受信時のアクションとして shutdown（DISABLE）が実行されたときに、show port-security interface コマンドで表示される Port Status が ENABLED のままになります。

○ ポートセキュリティーにおいて、不正パケット受信時のアクションが実行されてポートがロックされたあと、ポートセキュリティーを無効にしても、show port-security interface コマンドで表示される Lock Status が LOCKED のままになります。

○ ポートセキュリティーにおいて、不正パケット受信時のアクションとして shutdown（DISABLE）が実行されたあと、clear mac address-table コマンドでスタティックエントリーを削除すると、show port-security interface コマンドで表示される Lock Status が LOCKED から UNLOCKED に変わり、ポートがリンクダウンしたままになります。
ポートのロックを解除するには、switchport port-security コマンドを no 形式で実行してください。

2.5 MAC アドレススラッシング検出

参照 「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ MAC アドレススラッシング検出時、動作のログが出力されません。

○ MAC アドレススラッシング検出時の動作に port-disable または link-down を指定したとき、検出後の動作継続時間内に、該当ポートに対して shutdown コマンドを no 形式で実行しても、手動で動作を解除できず、以下のような状態になります。
port-disable 設定時：ポートの無効化が解除されず、該当ポートで通信を再開できません。
link-down 設定時：ポートはリンクアップしますが、thrash-limiting コマンドで設定された動作の持続時間が経過するまで、MAC アドレススラッシング検出を再開できません。

○ MAC アドレススラッシング検出時の動作に vlan-disable を指定したとき、検出後の動作継続時間内に、該当 VLAN に対して switchport enable vlan コマンドを実行しても、手動で動作を解除できず、VLAN を有効にできません。

2.6 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」

MSTP を設定後、LDF 検出機能を有効にし、MSTP を無効にするか MST インスタンスに関連付けられた VLAN を削除すると、LDF が送出されなくなります。
LDF の送出を再開させるには、システムを再起動してください。
ただし、MST インスタンスを作成せずに MSTP を有効にしただけの場合は、現象は発生しません。また、RSTP では本現象は発生しません。

2.7 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」

○ フローコントロール（802.3x PAUSE の受信）を有効にすると、スイッチポートのデュプレックスがオートネゴシエーション以外の固定設定であっても、フローコントロールが動作します。

○ SFP モジュールを装着した状態でシステムを再起動すると、ifOutDiscards カウンターがカウントアップします。本現象は AT-MG8T 装着時には発生しません。

○ egress-rate-limit コマンドでポートに送信レートの上限値を設定すると、上限値が設定されていないポートでも、送信レートが制限されることがあります。本現象は約 700Byte 以上のブロードキャスト、マルチキャストパケット送信時に発生します。

2.8 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」

○ ポート認証と LACP を同一ポートで併用することはできません。認証ポートでは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）で設定するようにしてください。

○ 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）とパケットストームプロテクションを併用するときは、グループ内のスイッチポートに対してパケットストームプロテクションを設定するようにしてください。スタティックチャンネルグループに対して設定すると、パケットストームプロテクションが正しく動作しません。

2.9 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」

○ 複数の Supplicant が同時に Web 認証を行った場合、いずれかの Supplicant の認証に失敗し、認証画面が崩れた状態で表示される（User name 欄だけが表示される）ことがあります。そのような場合は、Web ブラウザーで「再読込」を実行してください。

○ Web 認証と Auth-fail VLAN 併用時、認証失敗した Supplicant が Auth-fail VLAN の所属になったとき、Supplicant の Web 認証画面に認証失敗のメッセージが表示されず、「Authenticated」と表示されます。これは表示だけの問題で動作には影響しません。

○ Web 認証の Ping ポーリング機能を有効にし、auth-web-server ping-poll failcount コマンドで Supplicant がいなくなったと判断する Ping 無応答の回数を 1 に設定すると、Supplicant が Ping に応答しているにもかかわらず、認証が解除されます。failcount には 2 以上の値を指定するようにしてください。

○ 802.1X 認証または MAC ベース認証と MSTP を同一筐体内で併用し、かつ認証ポートでゲスト VLAN を使用した場合、認証成功時と認証解除時に不正なエラーメッセージが表示されます。これは表示だけの問題で動作には影響しません。

○ auth supplicant-mac コマンドで特定の MAC アドレスを持つ Supplicant 固有のパラメーターが設定されている場合、該当 Supplicant の認証にタイムアウトしていったん本製品から EAP-Failure が送信されると、その後 Supplicant から EAPOL-Start を受信しても、EAP-Request ではなく EAP-Failure を返すため、認証を開始できなくなります。

○ Web 認証において、auth max-supplicant コマンドで設定された最大数まで Supplicant が認証されている状態にもかかわらず、新たな Supplicant から Web 認証

サーバーへのアクセスが可能です。この際、認証画面には HTTP 403 エラーが表示されます。

○ Web 認証のインターセプトモードが設定されているとき、no auth-web-server mode promiscuous コマンドの実行で、インターセプトモードの設定が無効になります。

○ Web 認証において、Web 認証用 DHCP サーバー機能とインターセプトモードを使用したとき、DHCP によって IP アドレスを動的に取得する Supplicant と IP アドレスが静的に割り当てられている Supplicant が異なる認証ポートに接続されていると、IP アドレスの重複を Supplicant が解消できない場合があります。
インターセプトモードを使用する場合は、Web 認証用 DHCP サーバー機能ではなく、通常の DHCP サーバー機能を使用してください。また、Supplicant に貸し出す動的 IP アドレスの範囲は、IP アドレスが静的に割り当てられている Supplicant の IP アドレスが除外されるように構成してください。

○ Web 認証用の DHCP サーバー機能使用時、X.X.X.0 や X.X.X.255 など割り当てるべきでない IP アドレスや、別のネットワークの IP アドレスを貸し出す場合があります。
Web 認証用の DHCP サーバー機能を使用する場合、ポート認証を使用するインターフェースには、ホスト部ができるだけ小さい値の IP アドレスを割り当てるようにしてください。

○ 同一ポート上で 802.1X 認証、MAC ベース認証、Web 認証を併用した場合、または MAC ベース認証と Web 認証を併用した場合に、Web 認証用 DHCP サーバー機能を使用すると、認証前の Supplicant が Web 認証用 DHCP サーバーから IP アドレスを取得できません。このような場合は、Web 認証用 DHCP サーバー機能ではなく、通常の DHCP サーバー機能を使用してください。

2.10 マルチプル VLAN（プライベート VLAN）

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」

一度マルチプル VLAN（プライベート VLAN）の構成を組んだあとに、設定を削除する（プライベート VLAN が設定されていない状態に戻す）と、内部的に設定が残ったままになり、ホストポートとして設定されていたポート間で通信ができなくなります。
プライベート VLAN で使用した VLAN を no vlan コマンドでいったん削除すると通信が復旧します。

2.11 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」

○ BPDU ガード機能の動作中に、グローバルコンフィグモードにて spanning-tree portfast bpdu-guard コマンドを no 形式で実行してリンクアップしたあと、再度 spanning-tree portfast bpdu-guard コマンドを実行すると、BPDU ガード機能が動作しません。
ケーブルを抜き差しすることで、再度 BPDU ガード機能が動作します。
また、インターフェースモードにて spanning-tree portfast bpdu-guard コマンドを実行する場合は、本現象は発生しません。

○ 動作モードの設定（spanning-tree mode コマンド）が RSTP のとき、no spanning-tree force-version コマンドを使用して明示的なバージョン指定を削除することができません。no 形式を用いずに適切なバージョンを指定して設定しなおしてください。

○ ターミナルモニター実行中 spanning-tree enable コマンドを no 形式で実行すると不正なエラーメッセージが表示されます。これは表示だけの問題で動作には影響しません。

○ spanning-tree priority コマンドを no 形式で実行してもポートプライオリティーが初期値に戻りません。初期値に戻す場合は、spanning-tree priority コマンドでポートプライオリティーを 128 に変更してください。

2.12 DHCP Snooping

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

DHCP Snooping 有効時、ループガードの LDF 検出によって port-disable の動作が継続しているポートでは、DHCP メッセージがフィルタリングされずに通過します。

2.13 IGMP Snooping

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

○ フィルターモードが Exclude モード（MODE_IS_EXCLUDE）で、送信元アドレスが指定されている IGMPv3 Report メッセージを受信しても、該当グループが登録されません。送信元リストが空の MODE_IS_EXCLUDE は正しく認識されます。

○ CHANGE_TO_INCLUDE_MODE を Record Type に持つ IGMPv3 Report メッセージを受信しても、グループのフィルターモードが Exclude から Include に切り替わりません。

○ BLOCK_OLD_SOURCES を Record Type に持つ IGMPv3 Report メッセージを受信しても、すでに登録されている送信者リストから削除されません。また、ルーターポートに上記の Report メッセージが転送されません。

○ IGMPv2 ホストと IGMPv3 ホストが同一 VLAN 上に存在する場合、IGMPv2 ホストによるグループへの参加が先に行われていると、あとから CHANGE_TO_EXCLUDE{} を Record Type を持つ IGMPv3 Report メッセージを受信しても認識できません。マルチキャストルーターからの General Query メッセージに対して、IGMPv3 ホストが MODE_IS_EXCLUDE の Report メッセージを返した場合は、正しく認識します。

○ IGMP Snooping をいったん無効にし、再度有効にする場合は、システムを再起動してください。

2.14 MLD Snooping

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

○ MLDv2 Snooping において、グループのフィルターモードが Exclude モードであるにもかかわらず、送信元リストの当該アドレスを送信元とするマルチキャストパケットが転送されます。
Include モードではマルチキャストトラフィックは正常にフィルタリングされます。

○　ルーターポート上で BLOCK_OLD_SOURCES を Record Type に持つ MLDv2 Report メッセージを受信しても、送信者リストの当該アドレスは削除または変更されません。

2.15 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」

○　グローバルコンフィグモードで IGMP Snooping を無効にすると、show platform classifier statistics utilization brief コマンドで表示される ACL（ハードウェアアクセスリストによる内部領域の消費量）が -1 になります。これは表示だけの問題で動作には影響しません。

○　ハードウェアアクセスリストを作成するときに、終点ポート番号を範囲で指定した場合、範囲の上限値が始点ポート番号に指定した値よりも小さいとエラーで設定ができません。
例）始点ポート番号：80、終点ポート番号：1 ～ 60 を許可
access-list 3001 permit udp any eq 80 any range 1 60

このような場合は、アクセスリストを 2 個に分けて作成することで、設定が可能になります（61 ～ 80 を破棄する設定を追加します）。
access-list 3000 deny udp any eq 80 any range 61 80
access-list 3001 permit udp any eq 80 any range 1 80

2.16 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」

○　QoS ポリシーマップが適用されたスイッチポートに対して、適用を解除する設定を行っても、該当インスタンスにおいて QoS が使用するシステム内部領域が 1 つ消費されたままになり、すべての領域が解放されません。
すべての領域を解放するには、システムを再起動してください。

○　QoS ポリシーマップのフィルタリング機能において、フレームフォーマットに 802.2 LLC を指定しても、正しくフィルタリングされません。

○　QoS ストームプロテクション機能において、対象トラフィッククラスの受信レートが設定した上限値を超過した場合の動作として、受信ポートの無効化（portdisable）を指定していても、実際には受信ポートが物理的にリンクダウンします（linkdown 指定時と同じ動作になります）。

○　QoS ストームプロテクション機能において、受信レート超過時の動作に linkdown を指定したとき、動作継続時間内に shutdown コマンドを no 形式で実行しても、手動で動作を解除できません。ポートはリンクアップしますが、storm-downtime コマンドで設定された動作の持続時間が経過するまで、QoS ストームプロテクション機能を再開できません。

○　QoS ストームプロテクション機能において、storm-action コマンドを no 形式で実行して初期値（portdisable）に戻す設定をしても、コンフィグ上には「storm-action unknown」として反映されます。実際には、初期値である portdisable として正常に動作します。

○ QoS ストームプロテクション機能において、受信レート超過時の動作に vlandisable を指定したとき、動作継続時間内に該当ポートからポリシーマップを削除すると、switchport enable vlan コマンドを no 形式で実行しても、手動で動作を解除できなくなります。

2.17 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」

DHCP サーバー機能において、リース時間が 59 秒以下に設定されている状態でクライアントに IP アドレスが割り当てられると、clear ip dhcp binding コマンドで DHCP サーバーのリース情報を削除できなくなります。

3 マニュアルの補足・誤記訂正

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

3.1 準拠規格

参照「取扱説明書」（Rev.A）53 ページ

取扱説明書（Rev.A）53 ページ「本製品の仕様」に記載されている準拠規格の表記に一部誤りがありましたので、下記のとおり訂正いたします。

誤：

IEEE 802.3u 100BASE-TX, 100BASE-FX, 100BASE-BX
IEEE 802.3ah 1000BASE-BX10

IEEE 802.1D Spanning Tree
IEEE 802.1Q VLAN Tagging
IEEE 802.1s Multiple Spanning Tree
IEEE 802.1w Rapid Spanning Tree

正：

IEEE 802.3u 100BASE-TX, 100BASE-FX
IEEE 802.3ah 100BASE-BX, 1000BASE-BX10

IEEE 802.1D-2004 Spanning Tree, Rapid Spanning Tree
※ IEEE 802.1w Rapid Spanning Tree を含む
IEEE 802.1Q-2005 VLAN Tagging, Multiple Spanning Tree
※ IEEE 802.1s Multiple Spanning Tree を含む

4 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。

5　最新マニュアルについて

最新の取扱説明書「AT-x200-GE-52T 取扱説明書」（613-001396 Rev.A）、コマンドリファレンス「CentreCOM x200 シリーズ コマンドリファレンス」（613-001463 Rev.A）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 Web ページで最新の情報をご覧ください。

http://www.allied-telesis.co.jp/