



最初にお読みください

CentreCOM® AR560S リリースノート

この度は、CentreCOM AR560S をお買いあげいただき、誠にありがとうございました。
このリリースノートは、取扱説明書（613-001301 Rev.A）とコマンドリファレンス（613-001314 Rev.F）の補足や、ご使用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 2.9.2-14

2 本バージョンで追加された機能

ファームウェアバージョン 2.9.2-11 から 2.9.2-14 へのバージョンアップにおいて、以下の機能が追加されました。

2.1 IPv6 over IPv4/6to4 トンネルインターフェースにおける MSS クランプ機能

 参照「コマンドリファレンス」 / 「IPv6」 / 「IPv6 インターフェース」

IPv6 over IPv4 および 6to4 トンネルインターフェースにおいて、IPv6 上の TCP Syn パケットを監視し、TCP ヘッダー内の MSS オプションの値が 1220 を超える場合、同オプションの値を 1220 に書き換える MSS クランプ機能をサポートしました。本機能はつねに有効であり、無効にはできません。また、MSS の値は 1220 固定です。

なお、本機能では、IPv6 パケットが IPv4 パケットにカプセル化される時点で、IPv6 パケット内 TCP Syn パケットの MSS オプション値を書き換えます。IPv6 パケットのカプセル化を解除するときは、書き換えを行いません。

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 2.9.2-11 から 2.9.2-14 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 インターフェース統計カウンターの表示変更

 参照「コマンドリファレンス」 / 「インターフェース」

本バージョンより、下記のコマンドで 64 ビットの MIB カウンター ifHCInOctets と ifHCOctets が表示されるようになっていますが、これらのカウンターは未サポートです。

- ・ SHOW INTERFACE (COUNTERS オプション指定時)
- ・ SHOW SWITCH PORT COUNTER
- ・ SHOW ETH COUNTERS

また、MIB オブジェクト ifHCInOctets と ifHCOctets も同様に未サポートとなります。

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 2.9.2-11 から 2.9.2-14 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 ログメール送信機能を使用した場合に、一部のログを送信できない場合がありますでしたが、これを修正しました。
- 4.2 起動時にトリガースクリプトが実行される際、スクリプトファイルのファイル名（ベース名）が9文字以上だと該当スクリプトを正常に実行できない場合がありますでしたが、これを修正しました。
- 4.3 スイッチポートの DESCRIPTION を削除した際に、SHOW INTERFACE COUNTERS で表示されるスイッチポートのインターフェース名がデフォルトの表示に戻りませんでしたでしたが、これを修正しました。
- 4.4 ADD BRIDGE FILTER コマンドの PORT パラメーターに無効な文字列を指定するとリブートすることがありましたが、これを修正しました。
- 4.5 OSPF が設定された IP インターフェースを通じてパケットを送信中に、同 IP インターフェースを削除すると機器が再起動していましたが、これを修正しました。
- 4.6 IPsec/ISAKMP 使用時、対向機器のアドレスを FQDN で指定する場合は、DNS キャッシュ機能との併用ができませんでしたが、本バージョンより併用が可能になりました。
- 4.7 6 番目に設定された IP インターフェースで DNS サーバーからの DNS レスポンスパケットを受信した場合、DNS による解決に失敗していましたが、これを修正しました。なお本事象は、本製品の DNS リレー機能を使用する場合と、本製品自身が直接 DNS 解決をする場合に発生するものであり、本製品配下の DNS クライアントが直接 DNS サーバーに問い合わせる場合には発生しませんでした。
- 4.8 DVMRP を使用したマルチキャストルーティング環境において、同一 VLAN に複数のホストが存在するとき、ホストが接続されているポートの 1 つがリンクダウンすると、他のポートに接続されたホストへのマルチキャストトラフィックも一時的に停止することがありましたが、これを修正しました。
- 4.9 ファイアウォール有効時、フラグメントされたマルチキャストパケットを受信してもルーティングしませんでしたでしたが、これを修正しました。
- 4.10 2 つのファイアウォールポリシーにおいて、複数の VLAN と 1 つの WAN インターフェースとの間で ENAT を使用している場合、片方のポリシーに設定されている外部から内部への通信を許可するルールが動作しないことがありましたが、これを修正しました。
- 4.11 DHCPv6 サーバー機能使用時に、DHCPv6 クライアントが接続されているポートの所属 VLAN を変更すると、該当クライアントが変更後の VLAN で IPv6 アドレスを取得しようとしても、正しい IPv6 アドレスを割り当てられませんでしたでしたが、これを修正しました。

- 4.12 DHCPv6 サーバー機能使用時に、DHCPv6 クライアントが異なる VLAN 所属のポートに移動した場合、該当クライアントが移動後の VLAN で IPv6 アドレスを取得しようとしても、正しい IPv6 アドレスを割り当てられませんでした。これを修正しました。
- 4.13 WAN ロードバランスとファイアウォールの併用時、ポリシーフィルターが適用されている TCP セッションが TCP RST によってクローズすると、該当セッションが WAN ロードバランスセッションに登録されていましたが、これを修正しました。
- 4.14 WAN ロードバランスのヘルスチェックパケットが誤って同一の WAN インターフェースより送信され、結果としてヘルスチェックパケットを用いた負荷分散や障害の検出が正しく動作していませんでしたが、これを修正しました。
- 4.15 QoS 機能において中間トラフィッククラスを使用している場合、DWRR を使用するとリポートする可能性がありましたが、これを修正しました。
- 4.16 L2TP インターフェースで OSPF オンデマンドを使用した場合、L2TP の自動接続ができませんでしたが、これを修正しました。
- 4.17 ルーター間の L2TP 接続環境において、L2TP トンネル経由の通信中に L2TP トンネルが切断されると、まれに再接続と切断を繰り返すことがありましたが、これを修正しました。
- 4.18 SHOW ISAKMP SA で表示される Policy name 欄に誤ったポリシー名が表示され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・注意事項

ファームウェアバージョン 2.9.2-14 には、以下の制限事項や注意事項があります。

5.1 認証サーバー

 **「コマンドリファレンス」 / 「運用・管理」 / 「認証サーバー」**

RADIUS サーバーを複数登録している場合、最初に登録した RADIUS サーバーに対してのみ、SET RADIUS コマンドの RETRANSMITCOUNT パラメーターが正しく動作しません。最初の RADIUS サーバーへの再送回数のみ、RETRANSMITCOUNT の指定値よりも 1 回少なくなります。本現象は 802.1X 認証を使用した場合のみ発生します。

5.2 ログ

 **「コマンドリファレンス」 / 「運用・管理」 / 「ログ」**

スクリプトの実行結果を Syslog サーバーに転送すると、20 行分しか送信されません。

5.3 ジャンポフレーム

 **「コマンドリファレンス」 / 「インターフェース」**

本製品宛てのジャンポフレームを受信するとリポートするおそれがあります。本製品はジャンポフレームに対応していないため、本製品と接続する他の機器ではジャンポフレームをオフにしてください。

5.4 インターフェース

 **「コマンドリファレンス」 / 「インターフェース」**

- SHOW SWITCH COUNTER コマンドで表示される Receive Octets の値が受信したフレームサイズよりも 12 オクテット多く表示されます。
- SHOW SWITCH PORT COUNTER コマンドで表示されるスイッチポートの統計カウンター Transmit Discards はつねに「0」であるべきですが、カウントアップされる場合があります。
- 「RESET INTERFACE COUNTER」の実行後に「RESET SWITCH PORT COUNTER」を実行すると、「SHOW INTERFACE COUNTER」で表示されるスイッチポートのカウンターが異常な値を示すことがあります。その場合は、もう一度「RESET INTERFACE COUNTER」を実行して、該当カウンターをリセットしてください。なお、カウンター値が異常になるのは「SHOW INTERFACE COUNTER」の表示だけであり、MIB で取得する値には影響しません。
- LAN 側スイッチポートでは、長さが 1518 オクテット（タグなし）または 1522 オクテット（タグ付き）を超えるフレームを破棄せずに転送してしまいます。
- RESET ETH COUNTER コマンドを実行しても、ifInOctets カウンターがリセットされません。再度、RESET ETH COUNTER コマンドを実行してください。
- SHOW ETH COUNTER コマンドで表示される ifOutOctets および ifInOctets の値が送受信したフレームのサイズよりも 8 オクテット多く表示されます。
- 「RESET ETH COUNTER」や「RESET INTERFACE COUNTER」の実行後、「SHOW ETH COUNTER」や「SHOW INTERFACE COUNTER」で表示されるカウンターが異常な値を示す場合があります。

5.5 ポート認証

 **「コマンドリファレンス」 / 「運用・管理」 / 「ポート認証」**

- ENABLE/SET PORTAUTH PORT コマンドの SERVETIMEOUT パラメーターが正しく動作しません。これは、SET RADIUS コマンドの TIMEOUT パラメーターと RETRANSMITCOUNT パラメーターの設定が優先されているためです。SET RADIUS コマンドで $\text{TIMEOUT} \times (\text{RETRANSMITCOUNT} + 1)$ の値を SERVETIMEOUT より大きく設定した場合は、SERVETIMEOUT の設定が正しく機能します。
- DISABLE PORTAUTH コマンドで、PORTAUTH パラメーターに 8021X を指定すると、EAP Success パケットを送信してしまいます。
- RESET ETH コマンドによって Ethernet インターフェースを初期化しても、認証状態は初期化されません。
- 802.1X 認証済みのクライアントがログオフした場合、ログオフしたクライアントの MAC アドレスがフォワーディングデータベース（FDB）に保持されたままになります。

5.6 ブリッジング

 **参照** 「コマンドリファレンス」 / 「ブリッジング」

- ポート 1 がタグ付きパケットのブリッジングの対象となる VLAN に所属し、その VLAN に IP アドレスが設定されている場合、ポート 1 から VLAN の IP アドレス宛での通信をしようとすると、ルーターが ARP に応答せず、通信ができません。これはポート 1 でのみ発生し、他のポートでは発生しません。
- SET BRIDGE STRIPVLANTAG コマンドで、ブリッジの際に VLAN タグをはずさない設定にしてある場合、LACP パケットが送信できません。これを回避するには、ETH ポートを使用してください。

5.7 OSPF

 **参照** 「コマンドリファレンス」 / 「IP」 / 「経路制御 (OSPF)」

- MD5 認証を行う OSPF インターフェースにおいて、大量の LSU (Link State Update) パケットを受信した場合、「MD5 authentication Fails」のログが出力されます。
- OSPF の仮想リンクは使用できません。

5.8 DNS

 **参照** 「コマンドリファレンス」 / 「IP」 / 「名前解決」

- ダイナミック DNS のアップデートで、以下の 2 つのケースにおいて、アップデートは再送されません。
 - ・ 本製品からの TCP SYN パケットに対して、ダイナミック DNS サーバーからの SYN ACK パケットが返って来ない場合
 - ・ 本製品からの TCP SYN パケットに対して、ICMP Host Unreachable メッセージが返される場合
- ダイナミック DNS のアップデート (HTTP GET) に対する応答として、ダイナミック DNS (HTTP) サーバーから特定のエラーコード (404 Not Found) を受信すると、SHOW DDNS コマンドの Suggested actions の項目に HTML タグの一部が表示されることがあります。

5.9 DNS リレー

 **参照** 「コマンドリファレンス」 / 「IP」 / 「DNS リレー」

- DNS リレー機能有効時、下記条件のとき、クライアントからの名前解決要求に対してクライアントが指定したアドレスとは異なるアドレスで応答します。
 - ・ 2 つ以上の VLAN が設定されており、それぞれが異なる IP ネットワークに所属している
 - ・ DNS クライアントが、DNS サーバーのアドレスとして自身が所属していない VLAN の IP アドレスを指定している

これを回避するには、自身が所属している VLAN の IP アドレスを DNS サーバーとして設定してください。

- DNS リレーと DNS キャッシュの併用時、あるドメインの IPv6 アドレス (AAAA レコード) が DNS キャッシュに登録されている状態で、DNS クライアントから該当ドメインの IPv4 アドレス (A レコード) に対する問い合わせを受けた場合、キャッシュ済みの IPv6 アドレスを返答してしまいます。またこれとは逆に、あるドメインの IPv4 アドレス (A レコード) がキャッシュされている状態で、該当ドメインの IPv6 アドレス (AAAA レコード) を要求された場合、キャッシュ済みの IPv4 アドレスを返答してしまいます。この事象を回避するには DNS キャッシュ機能を無効化してください。

5.10 IPv6

参照「コマンドリファレンス」 / 「IPv6」

- RIPng 経路を利用して IPv6 マルチキャスト通信を行っている場合、経路が無効 (メトリック値が 16) になっても、しばらくその経路を利用して通信を行います。
- 6to4 トンネルは、本製品 1 台につき 1 個だけをサポートします。
- 6to4 トンネルコマンドを保存し、再起動するとエラーメッセージが出力されます。(動作に問題はありません。)
- ガーベージコレクションタイマーが動作中の RIPng 経路は、新しいメトリック値を持つ経路情報を受信しても、タイマーが満了するまで経路情報を更新しません。

5.11 ファイアウォール

参照「コマンドリファレンス」 / 「ファイアウォール」

- HTTP プロキシ機能使用時、受信した HTTP パケットに複数の Cookie 要求が含まれている場合、DISABLE FIREWALL POLICY HTTPCOOKIES コマンドを実行していても、その Cookie 要求を破棄せずにフォワードしてしまいます。
- RTSP、RTP を使用した VoD (Video on Demand) にて RTSP のネゴシエーションによって決定された RTP 受信用の UDP ポート番号を使用した RTP パケットを破棄します。
- ファイアウォールにてリモート IP を指定せずにダブル NAT ルールを設定すると、ルーターがすべての Gratuitous ARP に対して応答してしまうため、Host にてアドレス重複を検出し、通信できないことがあります。
- ファイアウォールにて動的に IP アドレスが割り当てられるインターフェースを Public インターフェースとして設定した際、ルール NAT の GBLIP パラメーターに "0.0.0.0" を設定すると、NAT 後のソースアドレスが Public インターフェースの IP ではなく、"0.0.0.0" に変換されるためパケットを送信しません。
- ファイアウォールにて 3 つ以上のファイアウォールポリシーが設定され、かつそれぞれのポリシーにルールが設定されていても、設定されたポリシーのうち 2 つのポリシーのルールしか正しく動作しません。ポリシーにルールを設定する場合はポリシーを 2 つまでにしてください。

※ 本件、以前のリリースノートでは「ファイアウォールにて 3 つ以上のポリシーが設定されているとき、最初のポリシーに設定されているルールが正しく動作しません」と記載しておりましたが、その後の調査にもとづき上記の通り訂正させていただきます。

- ファイアウォール機能有効時、SHOW IP COUNTER コマンドで表示される ETH インターフェースの受信カウンターが実際に受信したパケット数の 2 倍にカウントされます。
- ファイアウォールルールにマッチするパケットを受信すると SHOW FIREWALL POLICY COUNTER コマンドで表示される Total Packets Received カウンターが実際に受信したパケット数よりも 1 つ多くカウントされます。
- NAT ループバックの設定で FTP を行うと、3 ウェイハンドシェイクが終了しているにもかかわらず、FTP パケットが破棄されます。
- ファイアウォールでダイナミックインターフェーステンプレートを使用する構成において、ADD FIREWALL POLICY RULE コマンドで既存ルールの番号を指定した場合、重複しないようにルール番号の再設定が行われますが、異なるルールに対して、同じルール番号が設定される場合があります。重複する番号を持つルールは、どちらも動作しており、表示上の問題となります。
- 本製品自身が送信するパケットにスタティック NAT (1 対 1 のアドレス変換) を適用する場合は、インターフェース NAT のスタティック NAT (NAT=STANDARD) ではなく、ルール NAT のスタンダード NAT (NATTYPE=STANDARD) を使用してください。インターフェース NAT のスタティック NAT では意図したとおりに NAT が行われないことがあります。

5.12 DHCPv6 サーバー

 **「コマンドリファレンス」 / 「DHCPv6 サーバー」**

- DHCPv6 サーバーで認証機能を使用した場合、ADD DHCP6 KEY コマンドの STRICT パラメーターが動作しません。
- ADD DHCP6 POLICY コマンドで DHCPv6 サーバーの設定を変更しても、サーバーから Reconfigure メッセージが送信されません。ADD DHCP6 POLICY コマンドの実行後、さらに SET DHCP6 POLICY コマンドを実行してください。これにより、Reconfigure メッセージが送信されます。

5.13 GRE

 **「コマンドリファレンス」 / 「GRE」**

GRE 機能有効時、SHOW IP COUNTER コマンドで表示される ETH インターフェースの受信カウンターが実際に受信したパケット数の 2 倍にカウントされます。

5.14 L2TP

 **「コマンドリファレンス」 / 「L2TP」**

ADD L2TP USER コマンドで ACTION パラメーターに dnslookup を指定し、PREFIX パラメーターは未設定とした場合、設定を保存し、再起動するとコンフィグエラーになります。これを回避するには、再起動トリガーで ADD L2TP USER コマンドを再入力してください。

5.15 IPsec

参照「コマンドリファレンス」 / 「IPsec」

- Android OS 標準の VPN クライアントではない独自 VPN クライアントを実装して IPsec DPD に対応したスマートフォン N-06C とリモートアクセス VPN を行うと、N-06C の送信する R-U-THERE メッセージを受信しても本製品は R-U-THEREACK メッセージを返しません。
これを回避するには、PPP LCP エコーの間隔を短くするなどして、通信中は端末側からの IPsec DPD を動作させないようにしてください。
- SET ISAKMP POLICY コマンドで IPsec DPD と ISAKMP ハートビートを同時に指定すると、DPD の動作モードが正しく反映されません。IPsec DPD と ISAKMP ハートビートを設定する場合には、同時に指定しないようにしてください。
- SET IPSEC POLICY コマンドを実行した場合、該当する IPsec ポリシー上に確立している IPsec SA が削除されますが、削除された IPsec SA に IP ルートテンプレートが設定されている場合、テンプレートを通じて追加された経路が削除されません。
DELETE IP ROUTE コマンドで該当する IP ルート情報を削除することにより、この不整合から復旧させることができます。
- 拠点側の IP アドレスが不定であり、ISAKMP フェーズ 1 の IKE 交換モードが Aggressive モードである環境において、センター側の設定に ISAKMP ポリシーが以下の順で登録されていると、拠点側からの ISAKMP ポリシーによる相手ルーターの検索時、本来適合させたい ISAKMP ポリシー (2) に適合せず、リモート ID 未設定のポリシー (1) にマッチしてしまいます。
(1) ISAKMP の相手ルーターの ID (リモート ID) が未設定の ISAKMP ポリシー
(2) 本来適合させたい ISAKMP ポリシー
この現象は IPsec DPD、ISAKMP ハートビートのどちらを使用している場合でも発生します。
たとえば、以下の設定を利用した場合、IKE ネゴシエーションが行われると、センター側では ISAKMP ポリシー `i_a` が誤って選択されます。
<センター側：アドレス固定 >
CREATE ISAKMP POLICY="i_a" PEER=ANY MODE=AGGRESSIVE KEY=1
MSGRETRYLIMIT=3 DELETEDELAY=10
CREATE ISAKMP POLICY="i_b" PEER=ANY MODE=AGGRESSIVE KEY=1
SENDNOTIFY=TRUE DELETEDELAY=10 HEARTBEATMODE=BOTH
REMOTEID="id_b"
<拠点側：アドレス不定 >
CREATE ISAKMP POLICY="i_b" PEER=10.0.0.1 MODE=AGGRESSIVE KEY=1
SENDNOTIFY=TRUE HEARTBEATMODE=BOTH LOCALID="id_b"
これを回避するには、コマンドリファレンス (「IPsec」 / 「概要・基本設定」) に示されているように、相手ルーターの ID を正しく設定してください。

6 コマンドリファレンスの補足・誤記訂正

コマンドリファレンス (613-001314 Rev.F) の補足事項です。

6.1 ADD USER/SET USER コマンド

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「ユーザー認証データベース」

コマンドリファレンスの記載に誤りがありましたので、下記のとおり訂正いたします。

誤：

```
login-name: ログイン名 (1 ~ 64 文字。英数字のみ使用可能。大文字小文字を区別し  
ない。空白不可。入力可能文字：!0123456789ABCDEFGHIJKLMNPOQRST  
UVWXYZabcdefghijklmnopqrstuvwxyz)
```

正：

```
login-name: ログイン名 (1 ~ 64 文字。大文字小文字を区別しない。空白不可。入力  
可能文字：!#$%&'()*+,-./0123456789:;<=>@ABCDEFGHIJKLMN  
OPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~)
```

6.2 ICMP

 **参照** 「コマンドリファレンス」 / 「IP」

本体宛 ICMPv4/v6 Echo Request パケットの ICMP チェックサムフィールド値が「0xffff」である場合、同フィールドの値が「0x0000」であると見なしてチェックサムを検証します。

6.3 OSPF

 **参照** 「コマンドリファレンス」 / 「IP」 / 「経路制御 (OSPF)」

- SET OSPF コマンドの RIP パラメーターに EXPORT が BOTH を指定し、OSPF の経路情報を RIP 経路に取り込む設定をした場合、元となる OSPF 経路のメトリック値によって RIP で通知される経路のメトリック値は次のようになります。
 - ・ OSPF メトリック値が 8 未満の場合：RIP でもそのまま通知
 - ・ OSPF メトリック値が 8 以上の場合：RIP ではメトリック値を 8 に固定して通知
- OSPF の ASBR として、ROUTE パラメーター値が同一となる複数のスタティック経路の再配布を行う際に、その中に MASK パラメーター値が 32 ビットの経路が含まれる場合、一部の LSA が再配布できなくなります。ASBR にて 32 ビットマスクのスタティック経路を再配布する場合はご注意ください。

【問題が発生するスタティック経路の登録例】

```
ADD IP ROUTE=192.168.1.128 MASK=255.255.255.128 (再配布されなくなる LSA)  
ADD IP ROUTE=192.168.1.128 MASK=255.255.255.255
```

6.4 CREATE IPSEC SASPECIFICATION コマンド

 **参照** 「コマンドリファレンス」 / 「IPsec」

すでに CREATE IPSEC SASPECIFICATION コマンドで設定されていた PROTOCOL パラメーターの設定を変更した場合 (DESTROY IPSEC SASPECIFICATION コマンドで削除後に CREATE IPSEC SASPECIFICATION コマンドで再設定した場合) には、設定内容をスタートアップコンフィグに保存して再起動してください。設定を保存して再起動しないと、設定が正しく反映されない場合があります。

7 取扱説明書とコマンドリファレンスについて

最新の取扱説明書（613-001301 Rev.A）とコマンドリファレンス（613-001314 Rev.F）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、上記の取扱説明書とコマンドリファレンスに対応した内容になっていますので、お手持ちの取扱説明書、コマンドリファレンス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。

※ パーツナンバー「613-001314 Rev.F」は、コマンドリファレンスの全ページ（左下）に入っています。

<http://www.allied-teleasis.co.jp/>