613-001312 Rev.F 120323

Allied Telesis

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.C）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　2.9.2-07

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 2.9.2-01 から 2.9.2-07 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　DISABLE SWITCH PORT コマンドの LINK パラメーターの追加

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」

DISABLE SWITCH PORT コマンドに LINK パラメーターが追加されました。LINK パラメーターに DISABLE を指定することによって、スイッチポートを物理的にリンクダウンさせることが可能になりました。

コマンド

```
DISABLE SWITCH PORT={port-list|ALL} [LINK={DISABLE|ENABLE}]
SHOW SWITCH PORT
```

2.2　WAN/ETH ポートの無効 / 有効設定

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

新規に追加された DISABLE ETH コマンドによって WAN 側 Ethernet ポートを無効にすることが可能になりました。本コマンドで LINK パラメーターに DISABLE を指定することによって、ポートを物理的にリンクダウンさせることができます。また、新規に追加された ENABLE ETH コマンドによって、無効にした WAN 側 Ethernet ポートを有効にすることができます。

コマンド

```
DISABLE ETH=eth-interface [LINK={DISABLE|ENABLE}]
ENABLE ETH=eth-interface
SHOW ETH STATE
```

2.3　SHOW IPSEC ISAKMP コマンドの追加

参照　「コマンドリファレンス」/「IPsec」

新規に追加された SHOW IPSEC ISAKMP コマンドによって、IPsec SA ごとに関連する ISAKMP SA を一覧表示することが可能になりました。

コマンド

```
SHOW IPSEC ISAKMP
```

2.4 Responder Rekey Extension 機能

参照 「コマンドリファレンス」/「IPsec」/「ISKAMP」

Responder Rekey Extension 機能が追加されました。Android 端末などの ISAKMP/IPsec キープアライブ機能を持たない機器との接続時に、対向機器の死活監視が可能になりました。CREATE ISAKMP POLICY/SET ISAKMP POLICY コマンドに追加された REKEY パラメーターで本機能を有効にできます。本機能が有効な場合、ISAKMP SA 保持時間満了まで IPsec SA の通信の有無を監視し、通信がなくなるまで ISAKMP の保持時間を延長し続けます。ISAKMP SA 保持時間満了時に IPsec 通信の停止を検知すると ISAKMP SA と該当 ISAKMP SA に管理されている IPsec SA を削除します。

コマンド

```
CREATE ISAKMP POLICY=policy PEER=ANY [REKEY={ON|OFF|TRUE|FALSE}]
SET ISAKMP POLICY=policy PEER=ANY [REKEY={ON|OFF|TRUE|FALSE}]
SHOW ISAKMP POLICY
```

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 2.9.2-01 から 2.9.2-07 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 PPPoE サービス名の最大文字数の拡張

参照 「コマンドリファレンス」/「PPP」

以下のコマンドで指定する PPPoE サービス名に設定できる文字数が 18 文字から 64 文字に拡張されました。

コマンド

```
ADD PPP=ppp-interface OVER=physical-interface
CREATE PPP=ppp-interface OVER=physical-interface
DELETE PPP=ppp-interface OVER=physical-interface
SET PPP=ppp-interface [OVER=physical-interface]
ADD PPP ACSERVICE=service-name TEMPLATE=template
 ACINTERFACE=interface
DELETE PPP ACSERVICE=service-name
SET PPP ACSERVICE=service-name
```

3.2 CREATE PPP/SET PPP コマンドの PADRRETRY パラメーターの追加

参照 「コマンドリファレンス」/「PPP」

CREATE PPP/SET PPP コマンドに PADRRETRY パラメーターが追加されました。

PPPoE ディスカバリーステージで送信した PADR に対して PPPoE AC (Access Concentrator) から PADS が送信されてこなかった場合に、前バージョンまではディスカバリーステージを 3 回実施後に終了しましたが、PADRRETRY パラメーターに 0 を指定することでディスカバリーステージを繰り返し実施することが可能になりました。

コマンド

```
CREATE PPP=ppp-interface OVER=physical-interface [PADRretry={0|15}]
SET PPP=ppp-interface [PADRretry={0|15}]
SHOW PPP CONFIG
SHOW PPP LIMITS
```

3.3 ICMP チェックサム検証の仕様変更

参照 「コマンドリファレンス」/「IP」

本体宛て 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、前バージョンまでは該当パケットをチェックサムエラーで破棄していましたが、本バージョンからは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するよう仕様変更しました。

3.4 SET DDNS コマンドのサポート対象パラメーターの変更

参照 「コマンドリファレンス」/「IP」/「名前解決」

Dynamic Network Services 社が提供するダイナミック DNS サービス DynDNS.com（http://www.dyndns.com/）の Dynamic DNS Free サービスで提供されていたワイルドカード機能が有料化されたため、SET DDNS コマンドに含まれる WILDCARD パラメーターを未サポートとさせていただきます。

3.5 SQoS の仮想帯域設定時のトークンバケットサイズ選択パラメーターの追加

参照 「コマンドリファレンス」/「QoS」

CREATE SQOS TRAFFICCLASS/SET SQOS TRAFFICCLASS コマンドに MINBURST パラメーターが追加され、仮想帯域設定時のトークンバケットサイズの計算方式を選択することが可能になりました。MINBURST パラメーターに YES/ON を指定した場合、新しい計算方式（バケットサイズが少なくなる）を使用します。

コマンド

```
CREATE SQOS TRAFFICCLASS=tc-list [VIRTBW={bandwidth|NONE}]
 [MINBURST={YES|NO|ON|OFF}]
SET SQOS TRAFFICCLASS=tc-list [VIRTBW={bandwidth|NONE}]
 [MINBURST={YES|NO|ON|OFF}]
```

3.6 ISAKMP の IPsec SA 管理方法の変更

参照 「コマンドリファレンス」/「IPsec」/「ISKAMP」

IPsec 通信を行う際、IPsec SA が必ず ISAKMP SA に管理されている状態を保つように仕様を拡張しました。本バージョンより、IPsec SA を管理する ISAKMP SA が明確になりました。これにより IPsec SA が ISAKMP SA と連動して動作するようになり、ISAKMP SA が削除される際に IPsec SA も同時に削除され、管理されていない IPsec SA が存在することがなくなりました。

コマンド

```
SHOW IPSEC POLICY [SABUNDLE]
```

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 2.9.2-01 から 2.9.2-07 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　本製品が Telnet や BGP などの TCP コネクションを確立している状態において、TCP の状態が TIMEWAIT のときに再送データを受信すると、それ以降再送データを受信しなくても不要な ACK を再送していましたが、これを修正しました。

4.2　BGP ピアへの通知時に経路属性を変更するルートマップ（OUTROUTEMAP）において、プレフィックスに応じて異なる属性値をセットするよう設定しても、意図した属性値がセットされないことがありましたが、これを修正しました。

4.3　BGP セッションが Established 状態になる前にピアから UPDATE メッセージを受信した場合、このメッセージを破棄してしまい、メッセージ内の経路情報を学習できないことがありましたが、これを修正しました。

4.4　SET SYSTEM NAME コマンドで完全なドメイン名（FQDN）を設定していても、PING コマンド、TRACE コマンドでは、短いホスト名を指定した場合にドメイン名の補完が行われませんでしたが、これを修正しました。

4.5　IPv6 over IPv4 トンネリングインターフェース、および、6to4 トンネリングインターフェースを経由した通信において、最初の 1 パケットを破棄していましたが、これを修正しました。

4.6　PIM-SM において、ランデブーポイント（RP）への到達性が一定期間失われると、その後 RP への到達性が復帰してもマルチキャスト経路がすぐに復旧しないことがありましたが、これを修正しました。

4.7　ランデブーポイント（RP）への経路が切断された後、PIM ツリーの RPF Neighbour to RP に不正な IP アドレスが表示されていましたが、これを修正しました。

4.8　L2TP/IPSec によるリモートアクセス環境で、L2TP の接続要求パケットの再送が行われると、L2TP の接続に失敗する場合がありましたが、これを修正しました。

4.9　IP ルートテンプレートによって経路情報が自動登録されている場合に、IPsec SA 更新時に該当 IPsec ポリシーを使用した通信が発生していないと、旧 IPsec SA を削除する際に当該経路情報も削除してしまっていましたが、これを修正しました。

4.10　複数の拠点との間に IPsec SA を確立するセンター側において、DISABLE IPSEC コマンドによってすべての IPsec SA が削除される場合、1 つの拠点にすべての Delete ペイロードを送信してしまい、結果としてほとんどの拠点側にて Delete メッセージを受信できませんでしたが、これを修正しました。

4.11 1 つの NAT 機器の配下にある複数の Android 端末からルーターに対して NAT トラバーサルを使用して VPN 接続を行うと、最後に接続してきた端末のみの通信が維持され、それ以外の端末の通信が切断されてしまいましたが、これを修正しました。

4.12 ISAKMP 機能において、IKE のステータスやエラー情報を通知する Notify ペイロードを送信する際のバッファーの計算に誤りがあり、誤ったメモリーアクセスが発生し、本製品がリブートしていましたが、これを修正しました。

4.13 IPsec 機能の SA バンドルスペック設定において、IPsec SA の有効期限 (EXPIRYSECONDS) を設定し以下の両方の条件に合致した条件で通信した場合に、本製品がリブートしていましたが、これを修正しました。

- 本製品が IPsec のレスポンダーである場合。
- IPsec のイニシエーターから通知される IPsec SA の有効期限が、本製品に設定された IPsec SA の有効期限より長い場合。

4.14 IPSec SA 更新時に該当 IPsec ポリシーを使用した通信が発生していない状況において、対向機器から古い IPSec SA を削除する Delete メッセージを受信することにより IPSec SA が削除された場合、IP ルートテンプレートによって登録された経路が削除されていましたが、これを修正しました。

4.15 Re-KEY により新旧 2 つの ISAKMP SA が存在する状況で、古い ISAKMP SA が削除されるタイミングで新しい IPsec SA も削除してしまう場合がありましたが、これを修正しました。

4.16 ISAKMP/IPsec ポリシーの PEER に ANY または DYNAMIC を設定した場合、実際は行っていないにも関わらず名前解決に失敗したようなログが表示されてしまうことがありましたが、これを修正しました。

4.17 PEER=ANY で VPN が接続されている場合、VPN ピアが接続されている NAT 機器の IP アドレスが変わることによって、ISAKMP SA を通じて送信される Info メッセージ (IPsec DPD、ISAKMP ハートビートなど) は、AR ルーターで保持している送信元アドレスと異なる IP アドレスで受信します。この Info メッセージの破棄処理において、メモリーの解放漏れが発生していましたが、これを修正しました。

5 本バージョンでの制限事項・注意事項

ファームウェアバージョン 2.9.2-07 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

参照 **「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

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○ 複数のログフィルターにそれぞれ複数のログ出力インターフェースを使用する場合、フィルターによって分類されたログメッセージが 1 つのメールで送信されません。

○ 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 ETH 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」/「Ethernet インターフェース」

○ 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。

5.4 ポート認証

参照「コマンドリファレンス」/「運用・管理」/「ポート認証」

○ 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。

○ ENABLE/SET PORTAUTH PORT コマンドの SERVERTIMEOUT 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 TIMEOUT × (RETRANSMITCOUNT + 1) の値を SERVERTIMEOUT より大きく設定した場合は、SERVERTIMEOUT の設定が正しく機能します。

5.5 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 アドレス宛て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。

○ 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。

○ 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。

5.6 ダイナミック 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。

5.7 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。

5.8 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。

○ 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。

5.9 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 プロキシー機能使用時、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。

○ 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。

○ IPsec とファイアウォール併用時、IPsec 対向機器配下の端末から TELNET でマルチホーミングの設定（追加または削除）を行うと TELNET セッションが削除されます。

○ NAT ループバックの設定で FTP を行うと、3 ウェイハンドシェー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。

5.10 DHCPv6 サーバー

参照「コマンドリファレンス」/「DHCPv6 サーバー」

○ 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。

○ 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。

5.11 WAN ロードバランス

参照「コマンドリファレンス」/「WAN ロードバランス」

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ます。

5.12 GRE

参照「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。

5.13 L2TP

参照「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。

○ 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 の自動接続を開始しません。

5.14 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。

6 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.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、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 Web 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.C」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-telesis.co.jp/