



最初にお読みください

CentreCOM® AR450Sリリースノート

この度は、CentreCOM AR450S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（J613-M3069-00 Rev.A）とコマンドリファレンス（J613-M3069-03 Rev.L）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 2.9.1-20

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 2.9.1-19 から 2.9.1-20 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 ファイアウォールセッション数の制限（リミットルール）

 **参照**「コマンドリファレンス」 / 「ファイアウォール」


ファイアウォールセッション数の制限が可能です。

本製品はファイアウォールセッションを作成する際、すべてのリミットルールをチェックし、もし、対象となる通信を行う端末のセッション数が超過する場合、新たなセッションを作成しません。

コマンド

```
ADD FIREWALL POLICY=policy LIMITRULE=rule-id SRCIPLIMIT=0..10000  
[INTERFACE=interface] [GBLREMOTEIP=ipadd[-ipadd]]  
[IP=ipadd[-ipadd]]
```

2.2 新規サポートコマンドの追加

 **参照**「コマンドリファレンス」

以下の機能に新規コマンドを追加しました。詳細はコマンドリファレンスを参照してください。


- 運用・管理 / 記憶装置とファイルシステム
- 運用・管理 / ログ
- 運用・管理 / ターミナルサービス
- インターフェース / スイッチポート
- PPP/PPPoE AC
- IP
- IPv6
- IP マルチキャスト /IGMP
- IP マルチキャスト /PIM
- ファイアウォール
- ファイアウォール /UPnP
- VRRP

- DHCP サーバー
- L2TP
- IPsec

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 2.9.1-19 から 2.9.1-20 へのバージョンアップにおいて、以下の仕様変更が行われました。

3.1 Ethernet/VLAN インターフェースのリンクアップ・ダウン時のログ

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「ログ」

Ethernet/VLAN インターフェースのリンクアップ・ダウン時のログが記録されるようになりました。

3.2 MSS クランプ（書き換え）機能の拡張

 **参照** 「コマンドリファレンス」 / 「PPP」

MSS 調整機能は PPPoE 上で IP + TCP のパケットに対してのみ行われていましたが、IPsec 通信（PPPoE 上では IP + ESP）に対しても MSS 調整が行われるようになりました。

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 2.9.1-19 から 2.9.1-20 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 モジュールトリガーを作成する際に、SCRIPT パラメーターを複数設定しようとしてもエラーとなっていたが、これを修正しました。
- 4.2 SSH 機能を使用する場合、SSH 通信にて受信した 1584 バイト以上の暗号化データを処理する際に、リポートが発生していましたが、これを修正しました。
- 4.3 Unnumbered PPP インターフェースで、TTL=1 を持つ ICMP パケットを受信した場合、その応答パケットの送信元 IP アドレスとして 0.0.0.0 を使用していましたが、ローカル IP インターフェースが設定されている場合はその IP アドレス、設定されていない場合は、ICMP パケットの転送先インターフェースの IP アドレスを使用するように修正しました。
- 4.4 ICMPv6 Packet Too Big メッセージを受信した際、そのメッセージによって通知された MTU の値を、メモリー上の設定に動的に反映していましたが、これを反映しないように修正しました。
- 4.5 ルーター通知（RA）パケットの送信が無効のときに、受信したルーター通知パケットの Cur Hop Limit フィールドの値が本製品に設定されている値と異なる場合、本製品の設定内容を書き換えてしまっていたが、書き換えないように修正しました。
- 4.6 データ長が 1445 Byte から 1452 Byte のフラグメント化された IPv6 PING パケットを VLAN インターフェースで受信した時に応答できまなかったが、これを修正しました。

- 4.7 IPv6 フィルター機能において、フィルター対象をプロトコル番号で指定してもフィルター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。
- 4.8 SMTP プロキシを外部から内部への通信に対して動作させた場合に、外部と確立しているセッションに対し、TCP RST パケットを送信する場合がありますでしたがこれを修正しました。
- 4.9 PUBLIC 側でマルチキャストパケットを破棄した場合、PRIVATE 側での破棄としてファイアウォールのログに記録されていましたが、これを修正しました。
- 4.10 異なるファイアウォールセッションで同一の TCP ポートが使用されてしまう、または同一のファイアウォールセッションで異なる TCP ポートが使用されてしまう場合がありますでしたが、これを修正しました。
- 4.11 DELETE FIREWALL コマンドで NAT=ENAPT の設定を削除することができなくなりましたが、これを修正しました。
- 4.12 ファイアウォールにおいて、RST パケットを受信してファイアウォールセッションを切断した後、RST パケットを転送する際に、シーケンス番号または ACK 番号を不正な値で送信する場合がありますでしたが、これを修正しました。
- 4.13 PPP インターフェースに動的に IP アドレスを割り当てる設定の場合、PPP インターフェースに IP アドレスが割り当てられる前に IPsec ポリシーが作成されると、IPsec ポリシーのローカル IP アドレスに LAN 側 IP アドレスが設定されていましたが、正しく WAN 側の IP アドレスが設定されるように修正しました。
- 4.14 動的に IP アドレスを割り当てる PPP インターフェースがリンクダウンし、IPsec モジュールと ISAKMP モジュールが無効になった状態で PPP インターフェースのみ再度リンクアップすると、IPsec ポリシーのローカル IP アドレスに不正なアドレス 0.1.0.1 が設定されていましたが、これを修正しました。
- 4.15 ISAKMP ポリシーの PEER パラメーターに IPv6 のアドレスを設定する際に、本来であれば IP アドレスしか設定できないはずが、プレフィックスまで設定できてしまいましたが、これを修正しました。
- 4.16 IPsec ポリシーにて NAT-Traversal (NAT-T) を有効に設定した際、ESP パケットの TOS 値がランダムな値に設定されていましたが、これを修正しました。
- 4.17 IPv6 の IPsec VPN にて、セレクトターに ANY を指定すると、IKE フェーズ 2 (Quick モード) 時に、ペイロードに IPV4_ADDR_SUBNET を含むパケットを送出していましたが、これを IPV6_ADDR_SUBNET に修正しました。

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 2.9.1-20 には、以下の制限事項や注意事項があります。

5.1 IPv6

「コマンドリファレンス」 / 「IPv6」

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。

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（J613-M3069-00 Rev.A）とコマンドリファレンス（J613-M3069-03 Rev.L）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「J613-M3069-03 Rev.L」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/>