613-000275 Rev.E 070509

Allied Telesis

CentreCOM® AR570Sリリースノート

この度は、CentreCOM AR570S 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（613-000451 Rev.B）とコマンドリファレンス（613-000273 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　2.9.1-05

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 2.8.1-05 から 2.9.1-05 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　AT-FL-*-B

参照「コマンドリファレンス」/「運用・管理 / ソフトウェア」

固定パスワードによる、下記のフィーチャーライセンスの使用が可能となりました。
新たなライセンスのご購入は、末尾に「-B」のついたものをご購入ください。すでに、下記の旧ライセンスをご使用の場合はそのままご使用ください（AR570S では旧ライセンス AT-FL-15 に対応しておりません）。

○　AT-FL-04-B（SMTP プロキシー）
○　AT-FL-05-B（HTTP プロキシー）
○　AT-FL-06-B（PKI）
○　AT-FL-08-B（BGP-4）
○　AT-FL-15-B（WAN ロードバランス）

2.2　IGMP プロキシー

参照「コマンドリファレンス」/「IP マルチキャスト /IGMP」

IGMP プロキシーをサポートしました。IGMP プロキシーは、ホストからの IGMP パケットを上位のルーターに転送する機能です。これに伴い、ADD IP INTERFACE コマンドに IGMPPROXY パラメーターが追加されました。

2.3　PPTP パススルー

参照「コマンドリファレンス」/「ファイアウォール」

PPTP（Point-To-Point Tunnelling Protocol）パススルーをサポートしました。本機能により、Private 側からの PPTP パケットをファイアウォールが検知すると、データ通信に使われる GRE（Generic Routing Encapsulation）の通信を自動的に許可します。これに伴い、ADD/SET FIREWALL POLICY RULE コマンドの PORT パラメーターの値として、サービス名 PPTP が追加されました。

Private 側からの PPTP の通信を許可しない場合、または Public 側からの PPTP 通信に本機能を使用する場合は、ファイアウォールルールの設定が必要です。

○ Private 側からの PPTP の通信を許可しない場合

```
add firewall policy=policy-name rule=rule-id action=deny inter-
face=interface protocol=tcp port=pptp [other-parameters]
```

○ Public 側からの PPTP 通信に本機能を使用する場合

```
add firewall policy=policy-name rule=rule-id action=allow inter-
face=interface ip=ipadd[-ipadd] protocol=tcp port=pptp gblip=ipadd
gblport=pptp [other-parameters]
```

2.4 ファイアウォール・セッション・モニタリング

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・モニタリングをサポートしました。本機能により、ファイアウォールを通過するパケットをコピーし、キャプチャー端末で受信することが可能となります。ファイアウォールで破棄されたパケットはモニターの対象になりません。
これに伴い、ENABLE/DISABLE FIREWALL MONITOR、ADD/SET/DELETE FIREWALL MONITOR、SHOW FIREWALL MONITOR コマンドが追加されました。

本機能は、ファイアウォールを通過したパケットをコピーし、copyto に指定したインターフェースからブロードキャストパケット（FF:FF: FF:FF:FF:FF）として送信します。そのため、copyto に設定されるインターフェースがスイッチインターフェースの場合、VLAN を分ける必要があります。
モニター数に上限はありませんが、スループットに影響します。すべてのセッションをモニターした場合、スループットは半分程度になります。また、コマンド入力の際に、設定内容が部分的に重複していると、後から入力したコマンドによりオーバーライドされます。

2.5 DHCPv6

参照「コマンドリファレンス」/「DHCPv6 サーバー」

DHCPv6 サーバー、Prefix Delegation サーバーをサポートしました（リレーエージェント、クライアントは未サポートです）。

2.6 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 ロードバランスをサポートしました。WAN ロードバランスをご使用いただくためには、フィーチャーライセンス AT-FL-15-B のご購入が必要です。

注意 AR570S のもとで WAN ロードバランスをご利用いただく場合、機器の処理負荷が高くなるため充分な実行速度を得られない可能性がありますので、あらかじめご了承ください（PPPoE、Firewall、ENAT、WAN ロードバランスを併用し、パケット長 1518Byte における当社計測値は主 / 副回線合計で 667Mbps です）。

2.7 IPsec の IPv6 対応

参照 「コマンドリファレンス」/「IPsec」

IPsec が IPv6 に対応しました。これに伴い、CREATE IPSEC POLICY コマンドに ICMPTYPE パラメーターが追加されました。値として「ndall」を指定すると、IPv6 近隣探索で使用する ICMP タイプ 133-136 がすべて選択され、IPsec ポリシーのアクションは「permit」に自動的に切り替わります。

下記機能は、IPv6sec では未サポートとなります。

○ IPsec
UDPTunnel 関連機能

○ ISAKMP
XAUth 関連機能
ISAKMP HEARtbeat 関連機能
PKI 関連機能

3 本バージョンで仕様変更された項目

ファームウェアバージョン 2.8.1-05 から 2.9.1-05 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 BGP-4

参照 「コマンドリファレンス」/「IP/ 経路制御（BGP-4)」

BGP-4 ループバックインターフェース（ローカルインターフェース）を設定することにより、ルーターが生成する BGP-4 パケットのソースアドレスとして使用できるよう仕様を変更しました。下記コマンドで設定します。

```
ADD IP LOCAL=[1..15][FILTER={filter-number|NONE}]
[GRE=[0..100|NONE}][IPADDRESS=ipadd] [POLICYFILTER={filter-num-
ber|NONE}][PRIORITYFILTER={filter number|NONE}]

ADD BGP PEER=ipadd <other parameters> [LOCAL={NONE|1..15}]
```

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 2.8.1-05 から 2.9.1-05 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 ごく稀に内部エラーのリカバリー動作に問題が発生し、リブートすることがありましたが、これを修正しました。

4.2 SNMP の switch ポートの一部のエラーカウンターがランダムな値を返すことがありましたが、これを修正しました。

4.3 Telnet サーバーの応答に時間がかかっていましたが、これを修正しました。

4.4 フラグメントパケットを高負荷で受信すると、稀にインターフェースが応答しなくなることがありましたが、これを修正しました。

4.5 PPP において FCS のフラグ及び FCS が付加されたパケットを受信した場合、FCS を削除せずにブリッジを行っていましたが、これを修正いたしました。

4.6 PPP インターフェースのダウンにより経路が切り替わると、その PPP インターフェースが再びアップしても、経路が切り替わったままとなっていましたが、これを修正しました。

4.7 IPCP で無効な IP アドレスが与えられても、IP アドレスの再割り当て要求以降の処理が正常に行われるよう修正しました。

4.8 PPPoE インターフェース上で QoS（SQoS）を有効にしているにも関わらず、パケットの破棄が発生することがありましたが、これを修正しました。

4.9 タグ VLAN を有効に設定されている場合、VLAN から送信する ARP リクエストにタグが付加されませんでしたが、これを修正しました。

4.10 BGP-4 によってルーティングテーブルが更新された場合、IP フローが更新されませんでしたが、これを修正しました。

4.11 Port Restricted Cone NAT を使用すると、ファイアウォールルール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。

4.12 ファイアウォールと ENAT が併用されている場合、Linux、Mac OS などで TCP の Windows Scaling のオプションが有効になっていると、ルーター越しの TCP セッションのスループットが著しく低下していましたが、これを修正しました。

4.13 レンジ NAT とファイアウォールを併用すると、サーバー、クライアント間でセッションが正常にクローズしているにもかかわらず、TCP のセッションが Establish のまま取り残されていましたが、これを修正しました。

4.14 プリエンプトモード OFF かつ優先度 231 以上でバックアップルーターとして動作している場合、マスタールーターがダウンしてもマスターに移行しませんでしたが、これを修正しました。

4.15 ripmetric を 2 以上に設定すると、DHCP サーバーがインターフェース直下の DHCP クライアントにアドレスをリースしませんでしたが、これを修正しました。

4.16 LAC、LNS 間において無通信状態が 60 秒経過し、Hello パケットが送信されると、それ以降 Hello に応答しなくなることがありましたが、これを修正しました。

4.17 L2TP トンネル確立時にタイブレーク値に対する処理が正しく行われていませんでしたが、これを修正しました。

4.18 SET IPSEC POLICY コマンドを実行するとき、事前に設定された respondbadspi の値を継承していませんでしたが、これを修正しました。

4.19 長さが 2048 ビット（256 バイト）以上の公開鍵を含む証明書を証明書データベースへ登録するとリブートしていましたが、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 2.9.1-05 には、以下の制限事項や注意事項があります。

5.1　「show interface=ppp0 counters」「show interface=eth0 counters」で表示される「ifInOctets」「ifOutOctets」の値に誤りがあります。

5.2　ファイアウォールにおいて Private インターフェースとしてループバックインターフェースを指定し、Private 側のコンピューターから Telnet を実行すると接続ができません。

5.3　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。

5.4　「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、更に「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。

5.5　ISAKMP ポリシーの設定で PRENEGOTIATE を有効にすると、Phase-1 の Rekey が発生するまで通信ができません。「disable isakmp」「enable isakmp」コマンドを順に実行し、強制的に Rekey させることで通信は復旧します。

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（613-000451 Rev.B）とコマンドリファレンス（613-000273 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「613-000273 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/