613-000275 Rev.M 101130

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.E）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　2.9.2-00

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 2.9.1-21 から 2.9.2-00 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　PPP VJ 圧縮

参照 「コマンドリファレンス」/「PPP」

CREATE/SET PPP TEMPLATE コマンドで PPP テンプレートを作成する際、TCP/IP ヘッダーを圧縮して転送効率を向上させる、VJ 圧縮の有効 / 無効を指定できるようになりました。

コマンド

```
CREATE PPP TEMPLATE=template [VJC={ON|OFF}]
```

パラメーター

VJC: VJ 圧縮を行うかどうか。ON（行う）、OFF（行わない）から選択する。VJ 圧縮を行う場合、PPP テンプレートで作成されるダイナミック PPP インターフェースの IPCP Configuration Request に VJ 圧縮オプションを付与して送信します。デフォルトは OFF。

2.2　アプリケーション検出・遮断機能（Application Detection System：ADS）

参照 「コマンドリファレンス」/「ファイアウォール」

ファイル共有ソフトによる P2P 通信は、特定のホストが大量の TCP セッションを使用するため、帯域を占有してしまうことになります。また、ファイル共有ソフトの使用により、意図せず有害なファイルや企業の極秘情報等を拡散させてしまう恐れがあります。
ADS(Application Detection System) 機能は、このような P2P 通信を検知し、必要に応じてブロックすることができる機能です。
以下のコマンドが追加されました。

```
ENABLE FIREWALL POLICY=policy P2PFILTER={WINNY} ACTION={NOTIFY|DENY}
[THRESHOLD=number]

DISABELE FIREWALL POLICY=policy P2PFILTER={WINNY}

SHOW FIREWALL POLICY[=policy] P2PFILTER
```

2.3 IPsec 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」

IPsec パススルー機能とは、NAT 機器配下にある IPsec 端末が、NAT 機器の先にある IPsec 端末と IPsec 通信ができるようにするための機能です。
通常、エンハンスト NAT では、送信元アドレスに加えて、送信元ポート番号の変換も行いますが、IPsec 通信で使用される ESP パケットにはポート番号の概念がないため、NAT 機器配下に複数の IPsec 端末が接続されている場合、最初に接続してきた IPsec 端末だけしか接続できません。
しかし、エンハンスト NAT を使用する際に、PROTOCOL パラメーターで ESP を指定することによって、NAT 機器配下の複数の IPsec 端末が NAT 機器の先にある IPsec 端末と IPsec 通信ができます。
以下のコマンドが追加されました。

```
ADD/SET FIREWALL POLICY=policy RULE=rule-id PROTO-
COL={protocol|ALL|GRE|OSPF|SA|TCP|UDP|ICMP|ESP}

SET FIREWALL POLICY=policy [ESPTIMEOUT=0..43200]

SHOW FIREWALL SESSION
```

2.4 IPsec DPD

参照 「コマンドリファレンス」/「IPsec」

IPsec DPD は、IPsec の対向側の接続断を検知する機能です。
本機能では、IPsec SA 上にトラフィックがある限り、対向側が動作していることを証明し、DPD メッセージを送る必要はないと認識するトラフィックベースの検知方法を使用しており、一定時間トラフィックが止まると、対向側の状況が不明と認識し、DPD メッセージを送信します。
また、DPD メッセージを受信した対向側は、送信側に DPD ACK メッセージを返信することにより、自身が動作していることを証明します。
以下のコマンドが追加されました。

```
CREATE/SET ISAKMP POLICY=policy [DPDIDLETIMER=1..86400] [DPD-
MODE={BOTH|NONE|RECEIVE}]

SHOW ISAKMP COUNTER=DPD
```

3 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 2.9.1-21 から 2.9.2-00 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。

3.1 MAC ベース認証ポートに指定しているインターフェースをブリッジポートに指定すると、不正なユーザー名の認証リクエストが送出されていましたが、これを修正しました。

3.2 DHCP クライアント機能使用時、DHCP サーバーから新しい DNS サーバーアドレスを通知されても DNS サーバーリストを更新せず、以前に通知された DNS サーバーアドレスを使い続けていましたが、これを修正しました。

3.3 RIP 使用時、スタティック経路が削除されても該当経路をメトリック 16 で通知しませんでしたが、これを修正しました。

3.4 RIP 使用時、インターフェースがリンクアップしてもトリガーアップデートを送信しませんでしたが、これを修正しました。

3.5 RIP 機能において、複数に分割された RIP response パケットを正常に受信することができず、最初の 1 パケットのみしか受信することができませんでしたが、これを修正しました。

3.6 OSPF ルーターとして動作する場合、LSA を作成、通知を行った後、同じ LSA を再度通知することによって、一時的な LSA の不一致が発生することがありましたが、これを修正しました。

3.7 ファイアウォールポリシーに MAC アドレスリストを登録するとき、先頭文字が a ～ f の MAC アドレスが登録されませんでしたが、これを修正しました。

3.8 ダブル NAT を使用した状態で WAN インターフェースをリンクダウンさせ、ダブル NAT ルールに合致する通信を行うと、本製品がリブートする場合がありましたが、これを修正しました。

3.9 ファイアウォール有効時に RTSP の Continuation パケットの遅延が発生し、動画配信が止まることがありましたが、これを修正しました。

3.10 DHCP レンジの範囲外にある IP インターフェースで DHCP Discover メッセージを受信したとき、dhcpRangeExhaustedTrap トラップ（プライベート MIB）を送信していましたが、これを修正しました。

3.11 ソフトウェア QoS の仮想帯域を越えるトラフィックが発生することによって、フラグメントパケットが破棄されると、ソフトウェア QoS の送信インターフェースがリセットされる場合がありましたが、これを修正しました。

3.12 IPSec の IPv6 構成で、高負荷の UDP パケットを処理すると再起動することがありましたが、これを修正しました。

4 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 2.9.2-00 には、以下の制限事項や注意事項があります。

4.1 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。

4.2 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一つのメールで送信されません。

4.3 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。

4.4 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。

4.5 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。

4.6 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。

4.7 ポリシーフィルター（ポリシーベースルーティング）

参照「コマンドリファレンス」/「IP」/「IP フィルター」

ポリシーベースルーティングを使用し、WAN ロードバランスに該当しない IPsec 通信を行う際、TCP の RST/ACK パケットのみ、ポリシーベースルーティングで設定した先とは異なる PPP インターフェースへ送出されます。

4.8 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。

4.9 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。

4.10 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一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。

4.11 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。

4.12 ソフトウェア QoS

参照「コマンドリファレンス」/「QoS」

複数のトラフィッククラスの優先制御方式を DWRR に設定し、かつ、各トラフィッククラスをプライオリティーと重み付けにて制御（併用）すると、送信エラーが発生し、最優先にて処理されるべきパケットがロスする場合があります。

4.13 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。

4.14 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。

4.15 IPsec

参照「コマンドリファレンス」/「IPsec」

ISAKMP フェーズ 1 で使用する IKE 交換モードを AGGRESSIVE モードに設定し、ピアのアドレスを FQDN で設定すると、その FQDN から ISAKMP パケットを受信しても応答しません。

5 取扱説明書・コマンドリファレンスの補足

取扱説明書（613-000451 Rev.B）とコマンドリファレンス（613-000273 Rev.E）の補足事項です。
取扱説明書の補足事項です。

5.1 STATUS LED

参照「取扱説明書」18 ページ

本製品の STATUS（SYSTEM）LED には、以下の状態も含まれます。

LED	色	状態	表示の内容
SYSTEM	橙	短い 3 回点滅の繰り返し	内部電源ユニットに異常が発生しています。

5.2 DISABLE SWITCH PORT コマンド

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」

"DISABLE SWITCH PORT=xx" で特定のポートを指定しても FDB に登録されたすべてのエントリーが消去されます。

5.3 ダイナミックインターフェースと HTTP プロキシーの併用

参照「コマンドリファレンス」/「ファイアウォール」

ADD FIREWALL POLICY INTERFACE コマンドで設定するダイナミックインターフェースと HTTP プロキシー機能（ADD FIREWALL POLICY PROXY=HTTP で設定）は併用できません。

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