613-000275 Rev.J 090731

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.D）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　2.9.1-20

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　ダイナミック DNS クライアント機能

参照「コマンドリファレンス」/「IP」/「名前解決」

固定の IP アドレスが割り当てられなくても特定のドメイン名を利用できる、ダイナミック DNS をサポートします。この機能は、ISP より割り当てられた IP アドレスに変更があった場合などに、インターネット上に存在するダイナミック DNS サーバーに対し通知し、DNS データベースを更新します。
この機能により、ダイナミック DNS サーバーが常に最新の情報を保持でき、またサーバーに登録されたドメインから接続したいルーターの IP アドレスを検索できるようになるため、固定 IP アドレスを持たないルーターへのアクセスが可能です。
これに伴い、CREATE/SET ISAKMP POLICY および CREATE/SET IPSEC POLICY コマンドの PEER パラメータをドメインで指定できるようになり、固定の IP アドレスが割り当てられていない拠点同士でのインターネット VPN が可能になります。

コマンド

```
ACTIVATE DDNS UPDATE

DISABLE DDNS

DISABLE DDNS DEBUG

ENABLE DDNS

ENABLE DDNS DEBUG

SET DDNS [SERVER=server] [PORT=port] [USER=userid]
[PASSWORD=password] [DYNAMICHOST=hostnames]
[PRIMARYINT=ipinterface] [SECONDARYINT=ipinterface]
[WILDCARD={YES|NO|ON|OFF}] [OFFLINE={YES|NO|ON|OFF}]

SHOW DDNS
```

ヒント 本製品のダイナミック DNS クライアント機能は、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 サービスのみに対応しています。

2.2 タグ付きフレームのブリッジ機能

参照「コマンドリファレンス」/「ブリッジング」

ブリッジ対象フレームに対し、VLAN タグ（IEEE 802.1Q）を付けたまま送出できる機能が追加されました。
L2TP を使用したリモートブリッジでも使用可能です。

コマンド

```
SET BRIDGE STRIPVLANTAG={YES|NO|ON|OFF|TRUE|FALSE}
```

2.3 VID に基づいたリモートブリッジ機能（タグ VLAN-to-WAN ブリッジング）

参照「コマンドリファレンス」/「ブリッジング」

リモートブリッジ設定時に VLAN タグ（IEEE 802.1Q）の VID に基づいたブリッジングが可能になりました。
複数 VLAN（または単一 VLAN）設定時に VLAN タグ（IEEE 802.1Q）をチェックし、VID やタグの有無によりパケットの通過または破棄を行うリモートブリッジ設定が可能です。

コマンド

```
ADD VLAN={vlan-name|1..4094} BRIDGE [DEVICELIMIT={NONE|1..250}]
[AGEINGTIMER={NONE|0..1000000}]

DELETE VLAN={vlan-name|1..4094} BRIDGE

SET BRIDGE CHECKVLANTAG={YES|NO|ON|OFF|TRUE|FALSE}

SET BRIDGE STRIPVLANTAG={YES|NO|ON|OFF|TRUE|FALSE}

SET VLAN={vlan-name|1..4094} BRIDGE [DEVICELIMIT={NONE|1..250}]
[AGEINGTIMER={NONE|0..1000000}]

SHOW VLAN={vlan-name|1..4094} BRIDGE
```

2.4 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」

スイッチポート単位、Ethernet インターフェース（eth）で LAN 上のユーザーや機器を認証する、ポート認証をサポートします。認証に成功したユーザー、機器の通信を許可します。また、認証に成功したユーザー / 機器を特定の VLAN にアサインすることも可能です。また、Supplicant MAC 機能に対応し、特定の送信元 MAC アドレスを持つ機器を常に認証済み / 非認証の Supplicant として登録することが可能です。
ポート認証方式として、IEEE 802.1X 認証方式 /MAC アドレスベース認証方式をサポートします。

○ 802.1X 認証
802.1X 認証は、EAP（Extensible Authentication Protocol）パケットを使用し、ユーザー単位の認証を行います。Authenticator、または Supplicant として設定可能です。
802.1X 認証モジュールが現在サポートしている EAP 認証方式は以下のとおりです。

- Authenticator： EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-OTP（MD4/MD5）
- Supplicant： EAP-MD5、EAP-OTP（MD4/MD5）

○ MAC アドレスベース認証
機器の送信元 MAC アドレスに基づいて機器単位で認証を行います。Authenticator 設定が可能です。

2.5 IPv6 マルチキャスト

参照「コマンドリファレンス」/「IPv6 マルチキャスト」

IPv6 マルチキャストルーティング機能として以下の機能をサポートします。

○ MLDv1
MLDv1（RFC2710、Multicast Listener Discovery（MLD）for IPv6）をサポートします。
MLD（Multicast Listener Discovery：マルチキャスト受信者探索）は、LAN 上の IPv6 ルーターが IPv6 ノードとメッセージを交換しあい、LAN 上にどのマルチキャストグループの受信希望者（メンバー）がいるかを把握するためのプロトコルです。MLD は、IPv4 における IGMPv2（Internet Group Management Protocol v2）と同等の機能です。

○ PIM
PIM（Protocol Independent Multicast PIM-SM: draft-ietf-pim-sm-v2-new-05、PIM-DM: draft-ietf-pim-dm-new-v2-01）をサポートします。PIM（Protocol Independent Multicast）は、ユニキャスト用のルーティングプロトコル（EIGRP や OSPF など）から独立（Independent）した、マルチキャスト用のルーティングプロトコルです。
PIM には PIM-DM（Protocol Independent Multicast - Dense Mode）と PIM-SM（Protocol Independent Multicast - Sparse Mode）があり、本製品は両方をサポートしています。PIM の基本動作は IPv4 と同じです。

2.6 MLD プロキシー

参照「コマンドリファレンス」/「IPv6 マルチキャスト」

本機能はホストからの MLDv1/v2 パケットを上位のルーターに転送する機能です。

2.7 SNMPv3

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

セキュリティーと遠隔管理方法について拡張された SNMPv3 をサポートします。

2.8 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]]
```

2.9 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。

3.3 経路選択時の優先度変更機能の追加

参照「コマンドリファレンス」/「IP」/「経路制御（スタティック）」

経路制御プロトコルによって学習した経路の優先度（preference）の変更が可能になりました。

コマンド

```
SET IP ROUTE PREFERENCE={DEFAULT|1..65535}
PROTOCOL={BGP-EXT|BGP-INT|OSPF-EXT1|OSPF-EXT2|OSPF-INTER|
OSPF-INTRA|OSPF-OTHER|RIP}
```

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ましたが、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、リブートが発生しておりましたが、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 Ethernet インターフェースがリンクダウンしている状態で Ethernet インターフェース向けのパケットを受信すると、リンクアップするまで CPU 使用率が上昇したままの状態となっておりましたが、これを修正しました。

4.5 ICMPv6 Packet Too Big メッセージを受信した際、そのメッセージよって通知された 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。

4.6 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ましたが、書き換えないように修正しました。

4.7 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せんでしたが、これを修正しました。

4.8 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。

4.9 SMTP プロキシー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したがこれを修正しました。

4.10 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。

4.11 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したが、これを修正しました。

4.12 DELETE FIREWALL コマンドで NAT=ENAPT の設定を削除することができませんでしたが、これを修正しました。

4.13 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したが、これを修正しました。

4.14 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。

4.15 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。

4.16 ISAKMP ポリシーの PEER パラメータに 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っていましたが、これを修正しました。

4.17 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。

4.18 IPv6 の IPsec VPN にて、セレクターに 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 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 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。

5.3 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。

5.4 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。

5.5 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。

5.6 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。

5.7 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。

6 取扱説明書の補足

取扱説明書の補足事項です。

6.1 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。

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