613-000275 Rev.S 130920

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.J）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　2.9.2-11

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 2.9.2-09 から 2.9.2-11 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　Telnet セッション数の制御

参照「コマンドリファレンス」/「運用・管理」/「ターミナルサービス」

SET TELNET コマンドの MAXSESSIONS パラメーターにより、Telnet 同時接続セッション数の制御が可能になりました。

書式・パラメーター：

SET TELNET [MAXSESSIONS={1-32}]

MAXSESSIONS: 同時接続可能な Telnet セッション数。ここで設定した値のセッション数になると、次に張ろうとするセッションが破棄される。また、設定する際に確立されているセッション数以下の値は設定できない。デフォルトは 32。

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 2.9.2-09 から 2.9.2-11 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　ログメッセージタイプの名称変更

参照「コマンドリファレンス」/「運用・管理」/「ログ」

DNS 関連のログメッセージタイプの名称が、IPDNS から DNS に変更になりました。
本仕様変更にともない、以前のバージョンの設定で以下のコマンドの MODULE パラメーターに IPDNS を指定している場合は、DNS へ変更してください。

○　以前のバージョンでの設定（変更前）
ADD LOG OUTPUT [MODULE=IPDNS]
SET LOG OUTPUT FILTER [MODULE=IPDNS]
SHOW LOG [MODULE=IPDNS]

○　本バージョンでの設定（変更後）
ADD LOG OUTPUT [MODULE=DNS]
SET LOG OUTPUT FILTER [MODULE=DNS]
SHOW LOG [MODULE=DNS]

3.2　SHOW IP DNS / SHOW IP DNS CACHE コマンドの表示変更

参照「コマンドリファレンス」/「IPv6」/「名前解決」

該当コマンドの表示項目が一部変更になりました。

○　SHOW IP DNS コマンド

```
Manager > show ip dns

DNS Server Configuration
------------------------------------------------------------------------------
Domain                       Int/Status    Server Addr Preference         Requests
 Primary (v4)                           Primary (v6)
 Secondary (v4)                         Secondary (v6)
------------------------------------------------------------------------------
ANY*                         ppp0/Up       Prefer IPV4                         3
 200.100.10.1                           Not set
 200.100.10.2                           Not set
------------------------------------------------------------------------------

Cache:
  Maximum entries ................... 30
  Current entries ................... 2 (592 bytes)
  Timeout (minutes) ................. 10
  Cache hits ........................ 1

Global configuration:
  IP RR Type query preference ....... IPv4
```

以下は変更／追加された項目です。

Primary (v4)	プライマリー DNS サーバーアドレス。未設定の場合は 0.0.0.0 と表示される。サーバーアドレスを動的に取得しているときは、該当インターフェースがダウンだとアドレスは未設定状態となる
Secondary (v4)	セカンダリー DNS サーバーアドレス。未設定の場合は 0.0.0.0 と表示される
Primary (v6)	未サポート
Secondary (v6)	未サポート
Server Addr Preference	未サポート (Prefer IPV4 のみ表示)
Global configuration セクション	DNS の全体設定が表示される
IP RR Type query preference	未サポート (IPv4 のみ表示)

○　SHOW IP DNS CACHE コマンド

表示項目名の「IP Address」が「IPv4 Address」へ変更されました。

3.3 DHCPv4 サーバーの仕様変更

参照「コマンドリファレンス」/「DHCP サーバー」

DHCPv4 サーバー機能において、DHCP クライアントに配布した IP アドレスが重複していた場合、DHCP クライアントが送信する DHCP DECLINE メッセージを受信しても同じ IP アドレスを再配布することがありましたが、異なる IP アドレスを再配布するように仕様変更しました。

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 2.9.2-09 から 2.9.2-11 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 確立済みの PPPoE インターフェースを削除することによって、リブートが発生する場合がありましたが、これを修正しました。

4.2 2.9.2-00 以降のファームウェアにおいて IP NAT 機能を使用する場合、TCP 通信が繰り返されることによって、少しずつメモリーリークが発生していましたが、これを修正しました。

4.3 PUBLIC 側からの TCP SYN パケットに対する代理応答機能（TCP セットアッププロキシー）を使用し、PRIVATE 側に位置する HTTP サーバーを PUBLIC 側に公開する場合、アクセスが集中すると PUBLIC から HTTP サーバーにアクセスできなくなることがありましたが、これを修正しました。

4.4 2.9.2-00 以降のファームウェアにおいて P2P Filter（ADS 機能）を使用する場合、TCP の通信が行われることによって、少しずつメモリーリークが発生していましたが、これを修正しました。

4.5 FTP クライアントが FTP アクティブモードを使用したとき、送信した FTP 制御コマンドに対して FTP サーバー側からエラー応答された場合、ファイアウォールが誤ってデータコネクションを削除することがあり、その場合 FTP データが破棄されていましたが、これを修正しました。

4.6 PPP テンプレートを使用して動的に作成されるインターフェース（ダイナミック PPP インターフェース）に設定されたファイアウォールルールは、ルールの削除コマンドで削除できない場合がありましたが、これを修正しました。

4.7 DHCPv6 サーバー機能において、DHCP クライアントに配布した IP アドレスが重複していた場合、DHCP クライアントが送信する DHCP DECLINE メッセージを受信しても同じ IP アドレスを再配布していましたが、これを修正しました。

4.8 QoS 機能において、MINBURST パラメーターを設定した場合、転送遅延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 L2TP トンネルの確立を行うとき、L2TP トンネルの接続処理のやり直しが繰り返し発生することにより、長時間完了できない場合がありましたが、これを修正しました。

4.10 IPv6 IPsec 接続時に高負荷が発生している場合、まれに本製品がリブートすることがありましたが、これを修正しました。

4.11 受信した ESP パケットに対して復号化を行った際に、エラーを検出することによって IPsec 通信ができなくなる場合がありましたが、これを修正しました。

4.12 IPv6 IPsec 構成において、AR ルーターから送信される ESP パケットが対向ルーターで破棄される場合がありましたが、これを修正しました。

4.13 IPv6 IPsec トンネルを通過する IPv6 パケットにフラグメントヘッダーが付与されている場合、これを破棄していましたが、ルーティングするように修正しました。

4.14 L2TP/IPsec 使用時、対向機器が不在などの理由により接続ができない状況が続くことによって、まれにリブート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 2.9.2-11 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」

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」

○ 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。

○ 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。

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 OSPF

参照「コマンドリファレンス」/「IP」/「経路制御（OSPF)」

MD5 認証を行う OSPF インターフェースにおいて、大量の LSU（Link State Update）パケットを受信した場合、「MD5 authentication Fails」のログが出力されます。

5.7 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。

○ IPsec/ISAKMP 使用時、対向機器のアドレスを FQDN で指定する場合は、DNS キャッシュ機能との併用はできません。

5.8 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。

5.9 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。

○ 6to4 トンネルは、本製品 1 台につき 1 個だけをサポートします。

○ 6to4 トンネルコマンドを保存し、再起動するとエラーメッセージが出力されます。（動作に問題はありません。）

○ 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。

5.10 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 1 つ多くカウントされます。

○ 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。

○ ファイアウォールでダイナミックインターフェーステンプレートを使用する構成において、ADD FIREWALL POLICY RULE コマンドで既存ルールの番号を指定した場合、重複しないようにルール番号の再設定が行われますが、異なるルールに対して、同じルール番号が設定される場合があります。重複する番号を持つルールは、どちらも動作しており、表示上の問題となります。

5.11 DHCPv6 サーバー

参照「コマンドリファレンス」/「DHCPv6 サーバー」

○ 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。

○ 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。

5.12 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。

5.13 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。

5.14 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。

○ 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。

5.15 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。

○ 拠点側の IP アドレスが不定であり、ISAKMP フェーズ 1 の IKE 交換モードが Aggressive モードである環境において、センター側の設定に ISAKMP ポリシーが以下の順で登録されていると、拠点側からの ISAKMP ポリシーによる相手ルーターの検索時、本来適合させたい ISAKMP ポリシー (2) に適合せず、リモート ID 未設定のポリシー (1) にマッチしてしまいます。
(1) ISAKMP の相手ルーターの ID（リモート ID）が未設定の ISAKMP ポリシー
(2) 本来適合させたい ISAKMP ポリシー
この現象は IPsec DPD、ISAKMP ハートビートのどちらを使用している場合でも発生します。
たとえば、以下の設定を利用した場合、IKE ネゴシエーションが行われると、センター側では ISAKMP ポリシー i_a が誤って選択されます。
＜センター側 : アドレス固定＞
CREATE ISAKMP POLICY="i_a" PEER=ANY MODE=AGGRESSIVE KEY=1 MSGRETRYLIMIT=3 DELETEDELAY=10
CREATE ISAKMP POLICY="i_b" PEER=ANY MODE=AGGRESSIVE KEY=1 SENDNOTIFY=TRUE DELETEDELAY=10 HEARTBEATMODE=BOTH REMOTEID="id_b"
＜拠点側 : アドレス不定＞
CREATE ISAKMP POLICY="i_b" PEER=10.0.0.1 MODE=AGGRESSIVE KEY=1 SENDNOTIFY=TRUE HEARTBEATMODE=BOTH LOCALID="id_b"
これを回避するには、コマンドリファレンス（「IPsec」/「概要・基本設定」）に示されているように、相手ルーターの ID を正しく設定してください。

○ センター側ルーターの ISAKMP ポリシーの設定に相手ルーター（拠点側）のリモート ID を追加し、正しい設定を行っても、ISAKMP ポリシー適合時のポリシー名が誤って表示されます。この現象は IPsec DPD、ISAKMP ハートビートのどちらを使用している場合でも発生します。

6 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.J）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。

6.2 CREATE ENCO KEY コマンド

参照「取扱説明書」97,101,108,112 ページ

取扱説明書の記載に誤りがありましたので、下記のとおり訂正いたします。
誤：「CREATE ECHO KEY」コマンド
正：「CREATE ENCO KEY」コマンド

6.3 ICMP

参照「コマンドリファレンス」/「IP」

本体宛 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、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します。

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.J）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.J」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/