



613-000669 Rev.E 081217



最初にお読みください

CentreCOM® AR415S リリースノート

この度は、CentreCOM AR415S 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（613-000666 Rev.B）とコマンドリファレンス（613-000667 Rev.B）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 2.9.1-17

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 2.9.1-11 から 2.9.1-17 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 SNMP のエンコード方式の設定

 「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」

SNMP マネージャーからの Get 要求に対し、返信する値（カウンター値）が特定の範囲にある場合の動作を設定できます。以前のバージョンのファームウェアでは、カウンター値の先頭 1Byte が省略されるため、SNMP マネージャーによっては正しい値が表示されないことがありました。本設定（デフォルトで ON）により、省略しない値を出力できます。設定は、追加された SET SNMP ASNBERPADDING コマンドで行います。


コマンド

```
SET SNMP ASNBERPADDING={ON|YES|TRUE|OFF|NO|FALSE}
```

パラメーター

ASNBERPADDING: SNMP マネージャーからの Get 要求に対し、返信する値（カウンター値）が特定の範囲にある場合、カウンター値の先頭 1Byte を省略するかどうかを示す。（特定の範囲とは、2 進数で表記した場合に先頭 9bit がすべて 1 となる数値。32bit カウンターの場合は 4286578688 ~ 4294967295。）ON（デフォルト）の場合、カウンター値の先頭 1Byte を省略しない。OFF を指定すると、カウンター値の先頭 1Byte を省略する。ON、YES、TRUE および OFF、NO、FALSE はそれぞれ同じ意味。

2.2 SNMP トラップ送信遅延時間の設定

 「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」

起動時におけるすべての SNMP トラップを送信するタイミングを任意に遅らせることができようになりました。設定は、新しく追加された SET SNMP TRAPDELAY コマンドで行います。

コマンド

```
SET SNMP TRAPDELAY=10..600
```

パラメーター

TRAPDELAY: すべての SNMP トラップを送信するタイミングを遅らせる時間 (秒)。
デフォルトは 10 秒。

2.3 SNMP リンクトラップ送信遅延時間の設定

 「コマンドリファレンス」 / 「インターフェース」

SNMP リンクアップ / リンクダウントラップを送信するタイミングを任意に遅らせることができるようになりました。設定は、新しく追加された SET INTERFACE TRAPDELAY コマンドで行います。

コマンド

```
SET INTERFACE={ifIndex|interface} TRAPDELAY=0..60
```

パラメーター

INTERFACE: インターフェースの ifIndex またはインターフェース名。

TRAPDELAY: SNMP リンクアップ / リンクダウントラップを送信するタイミングを遅らせる時間 (秒)。デフォルトは 0 秒。

2.4 ファイアウォールにおけるフラグメント化パケット透過の最大数設定

 「コマンドリファレンス」 / 「ファイアウォール」

ファイアウォールによってフラグメント化パケットを透過させる場合、「ENABLE FIREWALL POLICY FRAGMENT=UDP」コマンドによって設定可能ですが、このコマンドを実行した場合、透過させることができるフラグメント化パケットの個数は 20 個までとなっていました。本バージョンより、透過できるフラグメント化パケットの個数の上限を変更できるようになりました。設定は、新しく追加された SET FIREWALL MAXFRAGMENTS コマンドで行います。

コマンド

```
SET FIREWALL MAXFRAGMENTS=8..50
```

パラメーター

MAXFRAGMENTS: 透過させるフラグメント化パケットの最大数。

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 2.9.1-11 から 2.9.1-17 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 ファイアウォールにおいて、フラグメントされた TCP 再送パケットの取り扱いに問題があり、メモリーリークが発生する場合がありますでしたが、これを修正しました。
- 3.2 トンネルインターフェースのダウン時にレポートが発生する場合がありますでしたが、これを修正しました。
- 3.3 ごくまれに RENAME コマンドによりフラッシュメモリー上のファイルが削除される場合がありますでしたが、これを修正しました。


- 3.4 PPP の Magic Number オプションを使用しない設定の機器からの LCP Echo Request に応答できませんでしたが、これを修正しました。
- 3.5 ブリッジフィルター設定時、不要な SET BRIDGE FILTER=1 ENTRY=1 PORT=ALL コマンドが追加されてしまい、ブリッジフィルター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。
- 3.6 BGP 脆弱性 (JVNVU#929656) への対策を行いました。
- 3.7 レンジ NAT 使用時に、グローバル側からの TCP パケットを不正に書き換え、通信が行えませんでした。これを修正しました。
- 3.8 DNS に関するキャッシュポイズニング脆弱性 (JVNVU#800113) への対策を行いました。
- 3.9 IPv6 近隣通知 (NA) パケットの受信を待っているときに、Target link-layer address オプションの値が 00-00-00-00-00-00 の不正な NA パケットを受信するとリポートしていましたが、これを修正しました。
- 3.10 PIM-SM 使用時、ルーティング済みのマルチキャストパケットを筐体内に保持し続け、メモリーリークが発生する場合がありますでしたが、これを修正しました。
- 3.11 ファイアウォール使用時、TCP オプションヘッダーを正しく認識できず、スルーブックが低下する場合がありますでしたが、これを修正しました。
- 3.12 L2TP とファイアウォールを併用している場合、トンネル確立後、ファイアウォールセッションを削除し L2TP の再送処理が行われるまで通信が行えませんでした。これを修正しました。
- 3.13 UPnP で使用する TCP セッションが保持され続け、本製品との TCP 通信が行えなくなる場合がありますでしたが、これを修正しました。
- 3.14 VRRP のバーチャル IP アドレスとして自身のインターフェースの IP アドレスを使用している場合 (優先マスタールーターとして設定している場合)、インターフェース監視機能 (ADD VRRP MONITOREDINTERFACE コマンドで設定) によってマスタールーターからバックアップルーターに移行した後も、バーチャル IP アドレス宛での ARP Request に対し、自身の MAC アドレスで応答することがありましたが、これを修正しました。
- 3.15 ファイアウォールルールに VRRP のバーチャル IP アドレスを指定した場合、バーチャル IP アドレス宛での ARP に VRRP のバックアップルーターも応答していましたが、これを修正しました。
- 3.16 DHCP サーバーとマルチホーミングを併用した場合、DHCP クライアントに IP アドレスを割り当てたあと、再度、DHCP クライアントから DHCP DISCOVER パケットが送信されると、すでに割り当てた IP アドレスと異なる IP アドレスを割り当てていましたが、これを修正しました。

- 3.17 インターフェースダウンなどにより、リモート装置までの経路が確立されていない状態でL2TPの発呼が行われた場合、インターフェースアップ後にトンネルが確立されてもトンネル作成のためのSCCRQパケットが続けて送信される場合がありますでしたが、これを修正しました。
- 3.18 SHOW L2TP TUNNEL CALL コマンドを実行するとリポートする場合がありますでしたが、これを修正しました。
- 3.19 インターフェースダウン時、L2TPでカプセリングされたパケットを送信する際にリポートする場合がありますでしたが、これを修正しました。
- 3.20 L2TPにおいてリモート側の装置が再起動しトンネルの不整合が発生した場合、新たにトンネルを作成できませんでしたが、これを修正しました。
- 3.21 リモート側の装置よりL2TP接続の切断が開始される際に、受信したパケットの結果Codeによっては、機器がリポートする場合がありますでしたが、これを修正しました。
- 3.22 センター経由の拠点間IPsec通信において、拠点間通信時にセンター側ルーターからICMP Redirectが送出されていましたが、これを修正しました。
- 3.23 IPsec SA未確立時に受信したパケットをSAが確立するまで保持していましたが、これを修正しました。
- 3.24 ポリシー名とインターフェース以外の値が同じIPsecポリシーを複数設定した場合、先に設定したIPsecポリシーが常に優先され、設定どおり動作していませんでしたが、これを修正しました。

4 本バージョンでの制限事項


ファームウェアバージョン **2.9.1-17** には、以下の制限事項があります。

4.1 ADD DHCP6 POLICY コマンド

 「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。

4.2 ADD DHCP6 KEY コマンド

 「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。

5 取扱説明書・コマンドリファレンスの誤記訂正

取扱説明書（613-000666 Rev.B）・コマンドリファレンス（613-000667 Rev.B）の誤記訂正です。

5.1 WAN ポート仕様および SET ETH コマンド

 「取扱説明書」 135 ページ

 「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」

- 取扱説明書に記載の製品仕様について、以下のように訂正してお詫びします。

A.7 製品仕様 / ハードウェア / インターフェース / WAN ポート

【誤】 10BASE-T/100BASE-TX × 1（オートネゴシエーション、Full Duplex/Half Duplex/10Mbps/100Mbps 手動設定、常に MDI/MDI-X 自動切替）

【正】 10BASE-T/100BASE-TX × 1（オートネゴシエーション時 MDI/MDI-X 自動切替、Full Duplex/Half Duplex/10Mbps/100Mbps 手動設定時は MDI 固定）

- SET ETH コマンドの SPEED パラメーターの設定および備考・注意事項は、正しくは以下のとおりです。訂正してお詫びします。

表 1：SPEED パラメーターの設定

AUTONEGOTIATE	オートネゴシエーション
10MHALF	10M Half Duplex 固定
10MFULL	10M Full Duplex 固定
100MHALF	100M Half Duplex 固定
100MFULL	100M Full Duplex 固定

備考・注意事項

オートネゴシエーション（AUTONEGOTIATE）の場合、Ethernet インターフェースは MDI/MDI-X 自動切替が有効となる。固定設定（AUTONEGOTIATE 以外）の場合、Ethernet インターフェースは MDI 固定となる。

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（613-000666 Rev.B）とコマンドリファレンス（613-000667 Rev.B）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きますので、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はない場合は、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「613-000667 Rev.B」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-teleasis.co.jp/>