



最初にお読みください



CentreCOM® AR260S V2 リリースノート

この度は、CentreCOM AR260S V2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（613-001298 Rev.A）、リファレンスマニュアル（613-000685 Rev.F）および設定例集（613-000902 Rev.E）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 3.3.0

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 3.1.0 から 3.3.0 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 アプリケーション検出機能



「リファレンスマニュアル」/
「5 ファイアウォール/NATの設定」/
「5.10 DoS 検出の設定」

ADS(Application Detection System: アプリケーション検出システム)機能として、下記の検出が可能になりました。なお、検出はWAN側インターフェース(EthernetまたはPPPoE)にて受信した場合に行われ、検出後の動作として「破棄」もしくは「通過」を設定できます。

- Winny(Version2のみ)

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 3.1.0 から 3.3.0 へのバージョンアップにおいて、以下の項目が仕様変更されました。

3.1 かんたんVPN



「取扱説明書」/
「6 かんたんVPN」/
「6.2 多拠点間のVPN接続」

これまでの「かんたんVPN」設定が「1対1接続」に変更され、新たに「多拠点接続」が追加されました。閉域網サービスを利用したセンターと各拠点を、ハブ&スポーク型で接続するVPNを構築します。接続形態ごとに以下のメニューが選択可能です。

- センタールーターとして設定
- 拠点ルーターとして設定



・ 拠点となるルーターは、他拠点およびインターネット宛の packets をセンタールーター経由で送るように設定されます。
・ フレッツ・VPNワイド等のCUGサービスで使用する場合、事前に管理者によるIPアドレスの割当等を行ってください。

3.2 Web GUI に関する変更

Web GUI に対して以下の修正、および改善を行いました。

- Web GUI 使用時のブラウザとして、Microsoft Internet Explorer 8 (Windows 版) に対応しました。
- かんたん接続に、フレッツ光ネクストの「サービス情報サイト」設定画面を追加しました。
- かんたん接続で設定される NTT 東日本のフレッツ・スクウェアの経路情報を更新しました。(平成 21 年 3 月 13 日現在の内容)
- DHCP に、任意の動的 DHCP クライアントを固定クライアントに登録できる設定を追加しました。
- アクセス制御で設定されるアクセスリストのプロトコル設定画面で、プロトコル番号を指定できるようにしました。
- Telnet サーバー機能を有効 / 無効にする設定画面を追加しました。これに伴い初期設定値を無効にしました。(ただし、本機能は未サポートです)

3.3 ファイアウォール、NAT 機能の拡張



「リファレンスマニュアル」/
「5 ファイアウォール / NAT の設定」 /

- ファイアウォール / NAT の FTP ALG 機能が、FTP Extensions (EPRT、EPSV コマンド) に対応しました。
- ファイアウォール / NAT のキャッシュ数が最大値を超えた場合、古いキャッシュを削除して新しいキャッシュを作成するようにしました。

3.4 ファイアウォール、セルフアクセス機能の拡張



「リファレンスマニュアル」/
「5 ファイアウォール / NAT の設定」 /
「5.3 ステルスモードの設定」

- セルフアクセス制御の有効 / 無効をインターフェース単位でも設定できるようにしました。これにより、システム全体でのセルフアクセス [有効 / 無効] および、インターフェース単位でのセルフアクセス [有効 / 無効] の組み合わせによる動作が、以下のようになります。

システム	インターフェース	動作結果
有効	有効	有効
	無効	無効
無効	有効	無効
	無効	無効

システム：「システム管理」内のセルフアクセス
インターフェース：「セルフアクセス」内のインターフェース単位のセルフアクセス

3.5 Windows 7 に対応

Windows 7 がインストールされた端末からのルーター機能の利用をサポートしました。

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 3.1.0 から 3.3.0 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 JVN#410676 「ISC DHCP dhclient におけるバッファオーバーフローの脆弱性」の対策を実施しました。
- 4.2 ファイアウォールが有効な際に、通信負荷が高い状態でアクセスリストのキャッシュや、NAT キャッシュの削除を行うとリポートすることがありましたが、これを修正しました。
- 4.3 ファイアウォールが有効な際に、"Sequence number error" がログに記録され、通信が中断されることがありましたが、これを修正しました。
- 4.4 ENAT を設定した構成において、NAT 変換後の IP アドレス（WAN 側インターフェースの IP アドレス）を送信元 IP アドレスに持つパケットを LAN 側インターフェースで受信した場合、WAN 側に転送していましたが、これを破棄するようにしました。
- 4.5 高負荷状態で IPsec の Rekey が発生すると、まれに IPsec 通信が一時的に不安定になることがありましたが、これを修正しました。
- 4.6 IPsec を使用した際、通信負荷が高い状態が続くと、通信に使用していた IPsec/ISAKMP SA が削除された場合、通信できなくなることがありましたが、これを修正しました。
- 4.7 IPsec を使用した際、通信負荷が高い状態が続くと確立済みの IPsec SA の SPI を持つ ESP パケットが未学習の SPI パケットとなり通信できなくなることがありましたが、これを修正しました。
- 4.8 IPsec の Rekey の際に更新された SPI の ESP パケットを受信すると、未学習の SPI と認識されてしまいパケットが破棄される場合がありましたが、これを修正しました。
- 4.9 IPsec の内部 NAT を使用している際に、"BLOCKED (match NAT address)" とログに記録され、しばらくの間拠点間の通信が行えなくなることがありましたが、これを修正しました。

5 本バージョンでの制限事項

ファームウェアバージョン 3.3.0 には、以下の制限事項があります。

5.1 PPPoE インターフェース複数使用時の IPsec 経路変更



「リファレンスマニュアル」/
「3 WAN 側インターフェースの設定」/
「3.3 PPPoE を使用した WAN 側ネットワークへの接続」

PPPoE インターフェースを複数設定し、仮想トンネルインターフェースを使用する IPsec 環境において、IPsec 対向機器に対する経路（ルーティングテーブル）を変更する場合は、一度「切断」ボタンを押して PPPoE インターフェースを切断してから行ってください。

5.2 MSS クランプ値の手動設定時の MSS 値



「リファレンスマニュアル」/
「3 WAN 側インターフェースの設定」/
「3.6 「WAN」 ページの解説」

WAN 側インターフェースの設定において MSS クランプ値を手動設定にした場合、MTU 値が 1454Byte 以外の時に MSS 値が正しく設定されないことがあります。そのため、自動設定を使用するか、正しい MSS 値になるように MSS クランプ値を調整してください。

5.3 デフォルトルートの出カインターフェース



「リファレンスマニュアル」/
「6 VPN の設定」/
「6.2 VPN の設定」

トンネルインターフェースを利用した IPsec 構成において、デフォルトルートの出カインターフェースをトンネルインターフェースにしている場合、WAN 設定の内容を変更すると、デフォルトルートの出カインターフェースが、PPPoE インターフェースに変更されてしまいます。「ルーティング」設定にてデフォルトルートの出カインターフェースを再設定してください。

6 取扱説明書とリファレンスマニュアルについて

最新の取扱説明書（613-001298 Rev.A）、リファレンスマニュアル（613-000685 Rev.F）および設定例集（613-000902 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、リファレンスマニュアルおよび設定例集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、リファレンスマニュアル、設定例集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。

<http://www.allied-teleasis.co.jp/>