MUCHO-EX,EV,EV/PK ファームウェア拡張のお知らせ

このたびは、MUCHO-EX,EV,EV/PK をお買い上げいただき、まことにありがとうございます。

今回お買い上げいただきました MUCHO-EX/EV のファームウェアでは、以下の機能がサポートされています。

- **i・ナンバー対応**
- **VoIP 中継機能**
- **PIAF 2.1（ベストエフォート）対応**
- **フレームリレーEncapsulation 拡張**
- **Hotline 機能**
- **DN(Distinguished Name)識別**
- **IPSec の拡張認証に対応**
- **IPsec の VPN 対象データ指定方法の拡張**
- **IPsec の NAT 動作モード拡張**
- **初期化設定の拡張**
- **学習 IP フィルタリング機能**
- **VPN 機能拡張**
- **フレッツ ISDN 接続**

これらの機能につきましては、取扱説明書に関連する記載がありませんので、この資料を参照し、設定／運用を行ってください。

１．ｉ・ナンバー対応

NTT グループよりサービスが提供される「ｉ(アイ)・ナンバー」に対応いたしました。

ｉ･ナンバーを利用すると、INS ネット 64／INS ネット 64 ライトの２本のチャネルに別々の番号を割当てることができます。つまり、MUCHO-EX/EV に接続した２台の電話が別々の番号をもてることになります。

・家族用／子供用といった着信者別
・電話用／FAX 用といったメディア別
・仕事用／家庭用といった目的別

等の使い分けも簡単に行うことができます。

ｉ・ナンバーを契約している場合は、MUCHO-EX/EV で以下の設定を行ってください。

① 追加番号を登録します。

ｉ・ナンバーでは、契約時に「契約者回線番号」「追加番号」を割当てられます。

MUCHO-EX/EV には、「追加番号」を登録しておきます。

MUCHO-EX/EV に接続した電話（TEL ポートはどちらでも良い）で

３＊８「追加番号」＃

と押します。追加番号は市外局番を入れないで登録します。

例えば、追加番号が 03-1234-5678 である場合は、

３＊８１２３４５６７８＃

と押します。("03"は市外局番のため入力しない)

② 電話の鳴らし方を設定します。

「契約者回線番号だけ鳴らす」「追加番号だけ鳴らす」「契約者回線番号・追加番号とも鳴らす」の中から、設定します。この設定は、各 TEL ポートに設定します。

契約者回線番号だけ鳴らす	５＊＊＃と押す
追加番号だけ鳴らす	５＊＊追加番号＃と押す
契約者回線番号 追加番号　とも鳴らす	５＊＃と押す

MUCHO-EX/EV で、すでにダイヤルインを利用している場合で、ｉ・ナンバーに移行した場合は、②の設定変更は必要ありません。

２．VoIP 中継機能

音声データを中継する際の品質を向上させることができるようになりました。

MUCHO-EX/EV で、VoIP 中継機能を使用するには、以下の２点の設定が必要になります。

① MTU 長の変更

② データ別優先制御機能による音声データの優先

① MTU 長の変更

MTU 長の変更は、コンソールより以下の方法で行います。

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password: ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# mtu on size=256 ←MTU コマンドでサイズを指定
```

MTU 長は、256byte～1500byte の範囲で指定します。

② データ別優先制御機能による音声データの優先

データ別優先制御の設定により、音声データを優先させます。

データ別優先制御の設定は、コンソールより以下の方法で行います。

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password: ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# prioritycontrol on fast=97 medium=2 ・・・i
conf# hostpriority add ip=192.168.1.1 fast・・・ii
conf# protocolpriority add ip=all,udp fast・・・iii
```

i) prioritycontrol コマンドで、優先度を指定

ii) hostpriority コマンドで音声データを指定

上記例では、 VoIP サーバの IP アドレスが、192.168.1.1 の場合

iii) protocolpriority コマンドで音声データを指定

上記例では、 音声データが使用するプロトコルが UDP の場合。

Microsoft NetMeeting※では、音声データは UDP を使用しています。

※："Microsoft" ならびに "NetMeeting" は，米国およびその他の国における Microsoft Corporation の登録商標です。

３．PIAF 2.1（ベストエフォート）対応

DDI ポケットよりサービスが提供される「PIAF 2.1（ベストエフォート)」に対応いたしました。

PIAF2.1（ベストエフォート）とは、基地局の利用状況により通信速度を適宜 64kbps←→32kbps に適切に切り替える通信方式です。

PIAF 2.1（ベストエフォート）の選択はコンソールより、以下の方法で行います。

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password: ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# target add name=Osaka dial=06xxxxxxxx speed=piafs64b
                                                ←piafs64b を指定
conf#
```

※：*PIAF2.1 は、DDI ポケット専用です。DDI ポケット以外は対応していません。*

４．フレームリレーEncapsulation 拡張

CISCO 社製ルータが独自で採用している、フレームリレーのエンカプシュレーション方式に対応いたしました。フレームリレーで接続する相手のルータがCISCO社製である場合、CISCO 社製ルータのエンカプシュレーション方式が独自方式か RFC1490 方式かを確認し、エンカプシュレーション方式が同じになるように設定してください。

エンカプシュレーション方式の設定は、以下のように行います。

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password: ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# dlci 16 encap=other  ←ｴﾝｶﾌﾟｼｭﾚｰｼｮﾝ方式を選択します
conf#
```

エンカプシュレーション方式は、"encap="で指定します。RFC1490 方式を使用する場合は"encap=rfc"、CISCO 社独自方式を使用する場合は"encap=other"を指定します。

上記画面例では、DLCI=16 でのエンカプシュレーション方式を、CISCO 社製独自方式としています。

５．Hotline 機能

MUCHO に接続した電話機の受話器をあげただけで，設定した相手に電話をかけることができるようになりました（Hotline 機能)。

従来よりサポートしていた，オフフック発信との違いを以下に示します.

オフフック発信	装置のディスプレイに発信履歴／着信履歴が表示されている状態で MUCHO に接続した電話機の受話器をあげると，表示されている相手に発信します.
Hotline 機能	MUCHO に接続した電話機の受話器をあげると,MUCHO の短縮登録 00 番に設定してある相手に発信します.

Hotline 機能の設定は、以下のように行います。

① ディップスイッチの 4 番を OFF にします。（工場出荷状態では OFF になっています）

② Hotline 機能で接続する相手を登録します.

Hotline 機能を使用するアナログ通信機器ジャックに接続した電話機より

０＊００接続する相手の電話番号＃

と押します。

例えば、Hotline 機能で接続する相手の電話番号が 03-1234-5678 である場合は、

０＊０００３１２３４５６７８＃

と押します。

※：短縮 00 番は，ホットライン専用になります。

③ Hotline 機能を有効にします.

Hotline 機能を使用するアナログ通信機器ジャックに接続した電話機より

９＊＊４

と押します。

※： オフフック発信の場合は「９＊＊３」，Hotline 機能を解除する場合は「９＊＊２」を押します.

６．DN(Distinguished Name)識別（MUCHO-EV/PK）

MUCHO-EV/PK の電子証明書による認証で、従来は、Email アドレス／ドメイン名／IP アドレスのいずれかで VPN ピアを識別していましたが、DN(Distinguished Name)で識別できるようになりました。

７．IPSec の拡張認証に対応

IPsec の Phase1 終了後、Phase2 に移行する前に行う、拡張認証（相手を認証する／相手に認証される）に対応いたしました。拡張認証を行うかどうか、拡張認証の ID/パスワードを設定することで、拡張認証を使用することができます。拡張認証の設定は、vpnikepolicy,vpnpeer コマンドで行います。

（１）vpnikepolicy の設定

```
conf#vpnikepolicy add id=1 method=prekeyxauth
                    ← 拡張認証を使用するmethod を選択
                       Pre-shared key で拡張認証する場合は”prekeyxauth ”
                       RSAsignature で拡張認証する場合は”rsasigxauth ”（EV/PK
                       のみ）
```

（２）vpnpeer の設定（相手に認証される場合）

```
conf#vpnpeer add addr=x.x.x.x myname=MUCHO-EV
myname_xauth=admin-MUCHOEV mypasswd=secret ikepolicy=1 ・・・・・
                    ← 拡張認証される設定
                       myname_xauth は、自身の名称
                       mypasswd は、自身のパスワード
                       ikepolicy は、拡張認証を指定した vpnikepolicy 識別
                       子
```

（３）vpnpeer の設定（相手を認証する場合）

```
conf#vpnpeer add addr=1.1.1.1 name=peername passwd=peersecret
xauth=on ikepolicy=1 ・・・・・
                    ← ←拡張認証する設定
                       name は、認証する相手の名称
                       passwd は、認証する相手のパスワード
                       xauth=on は、相手を認証する設定
                       ikepolicy は、拡張認証を指定した vpnikepolicy 識別
                       子
```

８．IPsecのAggressiveモード機能拡張

本装置をAggressiveモードで使用する場合は、相手に対してnameの情報を通知しますが、従来のMUCHO-EV／MUCHO-EV/PKではuserFQDN形式で通知していました。IPsecの相手によっては、FQDN形式で受信するものがあるため、nameを通知する形式を選択できるようになりました。Aggressiveモードで使用する場合は、IPsecの相手の仕様を確認してください。

（１）MUCHO-EV の場合

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password:←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# vpnpeer add addr=x.x.x.x myname=MUCHO-EV kye=a,xxxx
idtype=userfqdn ・・・・←name を通知する形式を選択
conf#
```

（２）MUCHO-EV/PK の場合

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password:←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# vpnpeer add addr=x.x.x.x myname=MUCHO-EV kye=a,xxxx
idtype-pre=userfqdn ・・・・←name を通知する形式を選択
conf#
```

※： MUCHO-EV/PK では、V40.06 以前で設定していた「idtype」のパラメータが「idtype-rsa」に変更になります。

９．IPsecのVPN対象データ指定方法の拡張

VPN対象データの設定で、全てのパケットを対象とするように設定した場合、IPsecの相手には255.255.255.255（マスク：0.0.0.0）で通知していました。IPsecの相手によっては、0.0.0.0 （マスク：0.0.0.0）で受信するものがあるため、MUCHO-EV V20.32以降／MUCHO-EV/PK V40.07以降では、全てのパケットを通知する形式を選択できるようになりました。全てのパケットを対象とする場合は、IPsecの相手の仕様を確認してください。

全てのパケットの指定方式は、コンソールより以下の方法で行います。

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password:←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# vpnselector add dst=all0 src=all0 ・・・・・
                        ←ホスト部オール0 で通知する場合は”all0 ”を指定
conf#
```

all0とした場合 ：0.0.0.0（マスク：0.0.0.0）で通知

all とした場合 ：255.255.255.255（マスク：0.0.0.0）で通知

１０．IPsec のNAT 動作モード拡張

１０．１　NAT変換後のセレクタ情報設定

NAT 動作モードが”nat ”（1対1変換）の場合で、変換後のアドレスが複数存在する場合に、VPNセレクタ情報で変換後のアドレスが設定できるようになりました。ここで変換後のアドレスを設定することにより、NAT 動作モードが”nat ”の場合でも、IPsecの通信を行うことができます。

VPN セレクタ情報の変換後アドレス設定方法は、コンソールより以下の方法で行います。

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password:←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# vpnselector add dst=all src=xxx.xxx.xxx.xxx ・・・・・
srcp2id=yyy.yyy.yyy.yyy,255.255.255.254
                        ←NAT変換後のアドレス（マスクつき）を指定
conf#
```

例）

NAT 変換範囲（natrange）：start=158.xxx.xxx.1 end=158.xxx.xxx.2 の場合

srcp2id=158.xxx.xxx.1,255.255.255.254 と指定

１０．２　VPNピア毎のNATスタティック登録（MUCHO-EV/PK）

VPN を使用する場合、NAT の設定は vpnpeer コマンドの natmode の設定にしたがっていましたが、VPN で NAT+/peernat/modeconfig とした場合にも、NAT スタティックを使うことができます。

natstatictable コマンドで、vpnpeer コマンドで設定した VPN ピアの IP アドレスまたは名称を指定した後、NAT スタティックテーブルを登録します。

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password:←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# natstatictable peeraddr=192.168.100.1 add local=・・・・
conf#
```

１１．初期化設定の拡張（MUCHO-EV/PK）

設定を初期化状態にする際、VPNで使用する電子証明書の情報（自身の証明書/CAの証明書）はクリアせず、その他の情報（パスワードを含む）を工場出荷時の設定に戻してからリセットします。

初期化設定の拡張は、コンソールより以下の方法で行います。

```
# reset -l
Configuration password:←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
Do you want to continue (y/n)?:←y を入力
```

１２．学習IP フィルタリング機能

学習IP フィルタリング機能とは、LAN →WANに中継する際に、そのパケットの宛先IPアドレスを学習し、学習したIPアドレスからのパケット以外は廃棄する機能です。インターネットに接続する場合などでは、どこからでも本装置にアタックが可能になりますが、このフィルタリングを利用し、セキュリティを強化することができます。

WAN →LANへの中継を許可するWAN側の装置のIPアドレスを設定します。

この登録を有効にするためには、iproutingコマンドのsealedをon に設定する必要があります。

WAN 側のxxx.xxx.xxx.xxxからの中継を許可する設定方法は、コンソールより以下の方法で行います。

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password:←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# sealed add addr=xxx.xxx.xxx.xxx 255.255.255.0
                    ←中継を許可するWAN 側のアドレス（マスクつき）を指定
conf#
```

１３．VPN 機能拡張

VPN 機能拡張により以下のコマンドおよびパラメータが追加されました。

① vpnpeerコマンドにおいてセキュリティ向上のため、登録済み鍵データ（key）が表示されなくなりました。

② transaction exchangeにより相手からもらったアドレスを使用してNAT+モードとして動作するモード（mode-config）が追加されました。vpnpeerコマンドにおいてnatパラメータでmodeconfigを選択することで使用することができます。

③ 従来はWANにアドレスを設定する場合はMain Mode、PPPでアドレスを取得する場合は、Aggressive Modeで動作していましたが、設定で指定することができるようになりました。vpnpeerコマンドにおいて新規パラメータ”mode ”にて指定します。また、autoを指定した場合は、従来の動作となります。

④ keepalive機能が追加になりました（IKE/ICMP）。vpnpeerコマンドにおいて新規パラメータ”keepalive ”を設定することによりkeepaliveを行うかどうか選択することができます。また、ICMPのkeepaliveを行なう場合は、送信元アドレスにつけるアドレスも指定することができます。

⑤ WAN回線が切断した時にSAを消去するかどうかを指定することができるようになりました。vpnpeerコマンドにおいて新規パラメータ”release ”で設定します。

⑥ インタフェースup時に自動でSAを張りにいくかどうかを指定することができるようになりました。vpnselectorコマンドにおいて新規パラメータ”ifupnego”で設定します。

⑦ SA が張れるまでリトライし続けるかどうかを指定することができるようになりました。vpnselector コマンドにおいて新規パラメータ”retrynego ”で設定します。

⑧ アドレスが不定のインタフェースに対して、自局発のパケットをIPsec通信することができるようになりました。vpnselectorコマンドにおいてsrcパラメータでmyaddrを指定することで使用することができます。
この場合、VPN対向装置のVPNセレクタ設定においては、アドレス不定に対するdstパラメータを指定する必要があります。古河電工VPN製品（MUCHO-EV、EV/PK、INFONET-VP100、FITELnet-F40）では、dstパラメータにpeerを指定することで、アドレス不定の相手に対してもVPN通信を行うことができます。

１４．フレッツ ISDN 接続設定

設定する接続相手（target）が、フレッツ ISDN 契約かどうかの設定が追加になりました。

target コマンドで、指定した相手がフレッツ ISDN 接続の相手の場合に、type=flets を指定します。

```
#conf ←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾓｰﾄﾞに移行
Configuration password:←ｺﾝﾌｨｸﾞﾚｰｼｮﾝﾊﾟｽﾜｰﾄﾞを入力
conf# target add name=・・・・・ type=flets・・
conf#
```

最新のマニュアルは、
http://www.furukawa.co.jp/network/mucho/HOWTO/mucho-manual.htmlにもあります。

130-M0443-N