SIPとIPv6でつくるオンデマンドVPN

IP電話の呼制御に使うSIPをベースにした技術によって，オンデマンドに接続先が変更可能なサービスが，「マルチポリシーVPN for OCN」です．これまでのVPNサービスと違い拠点間接続のみならず端末どうしまたはセグメントどうしといった細かな単位でのVPNの構築が可能であり，エクストラネット等の企業間通信やファシリティの管理・保守等，さまざまな分野での適用が期待できるこれまでになかったサービスです．

次世代VPNの重要性

考えつく限りのあらゆるものが，シームレスにネットワークへ接続される．そんな未来のネットワークでは，現在の接続サービスや形態よりも柔軟な構成で，誰もが必要最小限の手続きで簡単に接続でき，かつセキュリティを確保することが重要となります．

次世代VPNでは，このようなm2mで利用されることを前提とし，ユーザビリティやセキュリティを考慮したサービスを展開する必要があり，「マルチポリシーVPN for OCN」はまさにそのさきがけのサービスです．

既存のVPNサービスは企業間通信が苦手

取引先企業とエクストラネットを構築する場合や，オフィス内の監視やエレベータの保守点検といったファシリティ管理・制御で業者の代行サービスを受ける場合，どちらのケースでも外部の企業との通信が発生するが，ユーザ企業は社内のセキュリティを守りながら外部企業と接続するネットワークを整備しなければなりません．

すでにある社内ネットワークを流用し，必要なセキュリティを確保して外部企業と接続するのが望ましいのですが，用途ごとに回線を敷設する必要がありました．

既存のVPNサービスで，「社内」と「企業間」といった複数の運用ポリシーを適用するには，複数の物理回線を敷設し，それぞれにVPNをつくる必要がありましたが，それでは運用コスト・運用の負荷が高くなり導入をためらう企業も多くありました．

専用の暗号化装置で個別のVPNを構築可能

マルチポリシーVPN for OCNでは，専用の暗号化装置「CPE」と，OCN側に設置してある「ポリシーマネジメントサーバ」で，セキュア通信を行うための手順を実装し，対向のCPEとの間でIPsecによるセキュア通信を実現します．

マルチポリシーVPN for OCNでは，従来のVPNでは難しかった4点の特性を備えています（**図1**，**2**）．

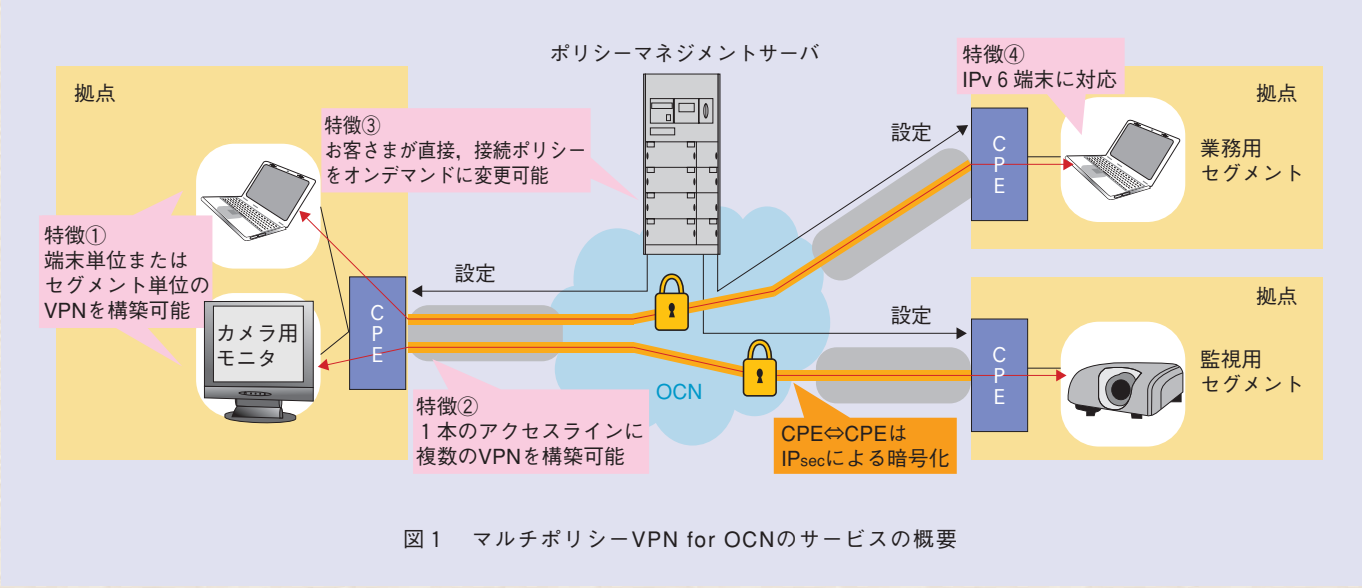

図1　マルチポリシーVPN for OCNのサービスの概要

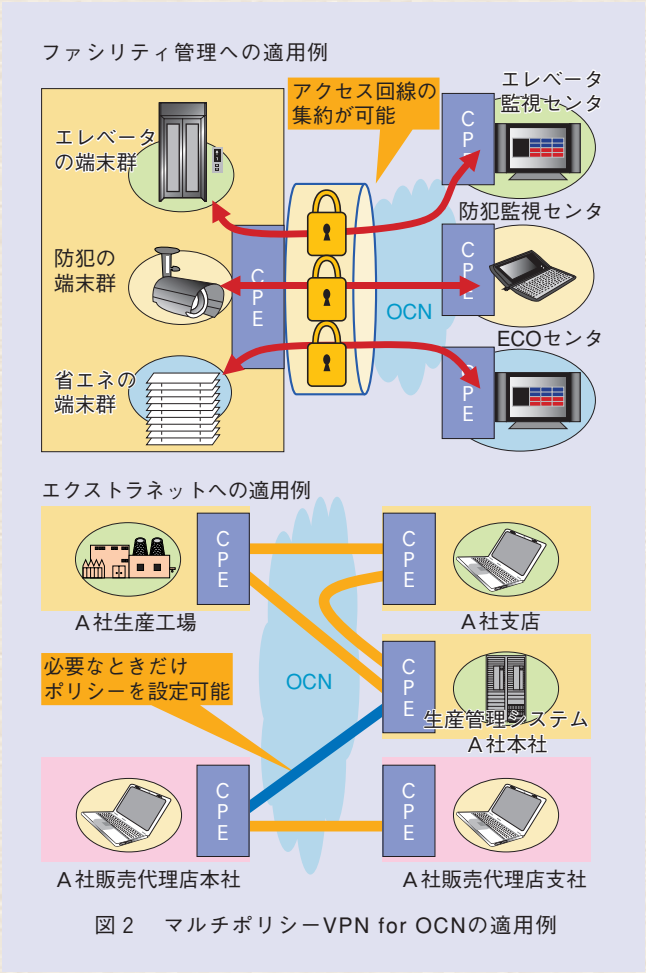

図 2　マルチポリシーVPN for OCNの適用例

① 端末単位やセグメント単位でのVPNの構築が可能：CPEのLAN側に，端末単位やセグメント単位で複数のVPNを構築可能．またCPEはLANの任意の場所に複数台設置可能．

② 1本の物理回線に複数のVPNの構築が可能：CPEのLAN側に，端末単位やセグメント単位のグループを複数設定可能．その個々のグループに対し，接続ポリシーを設定可能であり，1本の物理回線に複数のVPNの構築が可能．

③ ユーザがコントロールパネルにて，簡単にオンデマンドにVPNを設定可能：ポリシーマネジメントサーバと連動し，お客さまが直接操作可能な「コントロールパネル」を備えており，お客さまはオンデマンドで設定変更が可能．

④ IPv6を利用したVPN：CPEの配下のIPv6端末に対しVPNの設定が可能であり，既存のIPv4アドレスを使ったネットワークとの共存が可能．

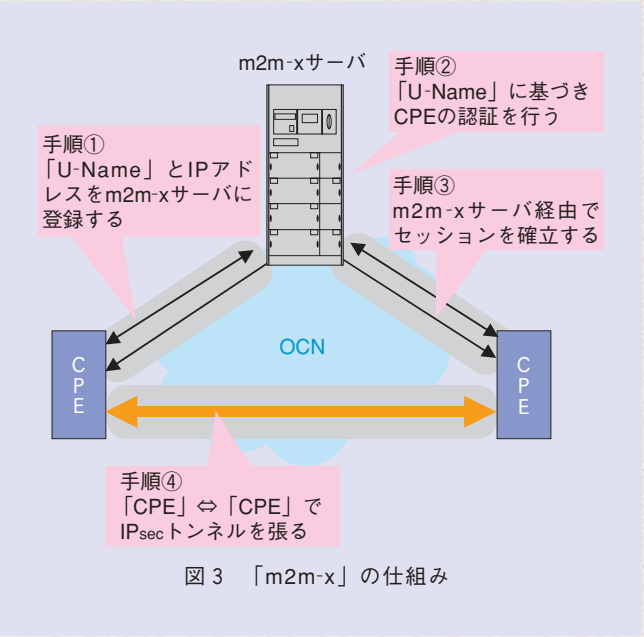

図 3　「m2m-x」の仕組み

SIPをベースにした独自の暗号化通信

マルチポリシーVPN for OCNでは，IP電話の呼制御などに使われる「SIP（Session Initiation Protocol）」をベースに，NTTコミュニケーションズが独自に開発した「m2m-x」という技術が利用されています．これは，端末どうしがエンド・ツー・エンドで安全かつリアルタイムに通信するために開発された技術であり，エンド・ツー・エンドでIPsecトンネルを張り，セキュリティを確保する仕組みとなっています（**図 3**）．

まずCPEは，自分に割り当てられた「U-Name」とIPアドレスを，m2m-xサーバに登録します．通信相手の端末も同様に登録します．このやり取りによりCPEとm2m-xサーバの間に通信路を確立します．

m2m-xサーバへの登録時には，各CPEが正規のユーザであるかどうかの認証を行い，正しいユーザの場合には，CPEとm2m-xサーバとの間で確立された通信路をIPsecで暗号化します．

CPEはm2m-xサーバに正しく登録されると，ポリシーマネジメントサーバで設定された「接続ポリシー」に基づき，通信相手先のCPEとの間にIPsecを確立し，セキュア通信が可能となります．

m2m-xサーバは，CPE間のIPsecトンネルを張る際の鍵情報等を自動で設定し，定期的に交換するため，安全性の確保に一役買っています．

いったん確立したセッションは，基本的にそのまま使い

続けることが可能ですが，エクストラネットのように必要なときだけ通信したい場合は，コントロールパネルを操作し，その都度セッションの管理をすることが可能です．

リアルタイムにポリシー変更が可能

ポリシーの設定はお客さま自身がコントロールパネルを操作することで実施します．１つひとつポリシーを設定する必要があるため，操作に多少の手間は掛かりますがGUIのため操作自体は簡単にできます（**図 4**）．

お客さまはコントロールパネルにログイン後，設定を行うCPEを選択し，「グループ」に含める端末（IPv6端末）を登録します．グループを複数設ける場合，すべてのグループに対して端末を登録します．

グループ登録後，通信先のCPEとグループを指定し接続ポリシーを規定します．すべての通信させたいグループに対し接続ポリシーを設定したら，最後にその設定を有効にするためにCPEにポリシーを反映させます．

CPEは，コントロールパネルから送られてきた接続ポリシーに基づき動作し，接続先との接続ポリシーと合致した場合のみ，IPsecによるセキュア通信を行うことができます．

マルチポリシーVPN for OCNのサービス仕様

マルチポリシーVPN for OCNでは，これまで述べたとおりCPE配下のIPv6端末に対して，オンデマンドに個々の

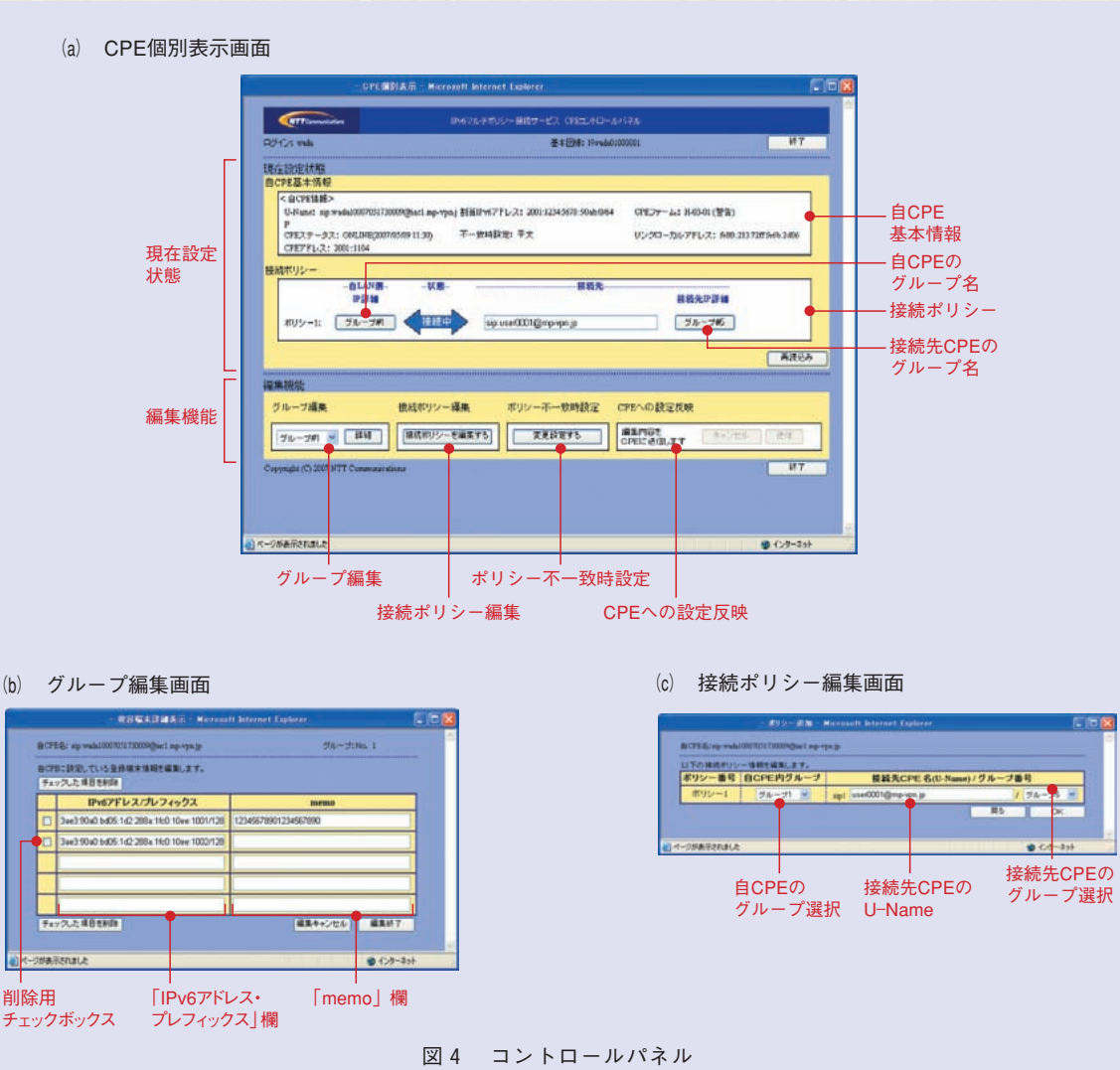

図 4　コントロールパネル

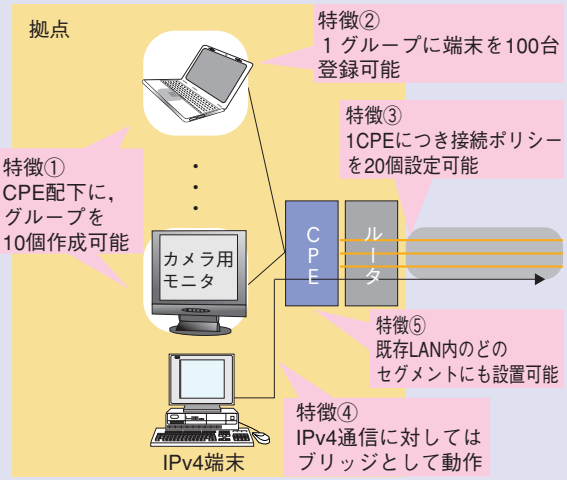

図5　マルチポリシーVPN for OCNの仕様

VPNを設定可能です．

CPE配下のIPv6端末を，複数のグループに分けて管理しますが，1グループ当り最大100台の端末を登録できます．また1台のCPEでは，最大10グループまで管理でき，そのグループごとに接続ポリシーを設定することが可能です．1台のCPEでは，最大20の接続ポリシーを設定できます．

また既存のIPv4端末に対しては，ブリッジとして動作するため，現在利用しているネットワークのLAN内のどのセグメントにもCPEを設置することができます（**図5**）．

マルチポリシーVPN for OCNは，VPNサービスとしてはめずらしい片端契約で，1拠点からの契約が可能です．グループ企業間での通信など，これまで構築の難しかったエクストラネットでの利用も可能です．

現在利用できるネットワークは「OCN」であり，FTTHを使う「OCN光アクセス」等の主要なサービスに対応しています．

マルチポリシーVPN for OCNのサービス拡張

現状のマルチポリシーVPN for OCNのサービスでは，

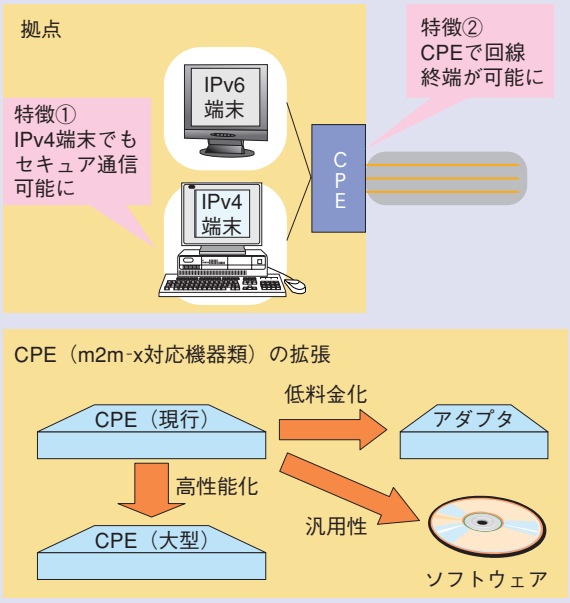

図6　サービス拡張予定

VPNの設定をできるのがIPv6端末に限られていますが，近い将来，仕様は同じでIPv4端末に対応させる予定です（**図6**）．

IPv4グローバルアドレスの枯渇問題もあり，これからIPv6がネットワークの主流となる際の，IPv4⇒IPv6へのマイグレーションを誘導するための起爆剤となるサービスに成長させたいと考えています．

また現状CPEは1種類しかありませんが，現状よりも大型でより高性能のCPEの開発や，端末収容を1台に限定した「アダプタ型CPE」の開発も順次行っていく予定です．

さらに端末にm2m-xに対応するソフトウェアを導入することによりCPEの設置なしに暗号化通信が可能な「ソフトウェアタイプ」の開発も行う予定です．

◆問い合わせ先

NTTコミュニケーションズ
ブロードバンドIP事業部
TEL　03-6700-8344
E-mail　ipv6mp-info@ntt.com
URL　http://www.ocn.ne.jp/business/vpn/mpvpn/