ブロードバンド時代のネットワーク・セキュリティ・テクノロジについて

- IPsecとMPLSの動向について-

平成14年 4月 25日

古河電気工業株式会社
黒田政彦

ブロードバンド時代の到来

2001年はブロードバンド元年

●真のインターネット利用環境への本格的移行へ

- DSLの本格的普及の加速（10M以下）
  NTT東西、YAHOO-BB等による全国展開により、
  2001年度末時点で346万世帯へ増加（前年度比３．８倍）

●高速ブロードバンドインフラの多様化

- 無線サービス（ホットスポットサービス、FWA）
- FTTH（光ファイバ網による100M超サービスの登場）
  NTT東西（Bフレッツ）、有線ブロードネットワーク
  電力各社によるサービス開始（K-opti、QTNET等）
- CATVインタネットの普及

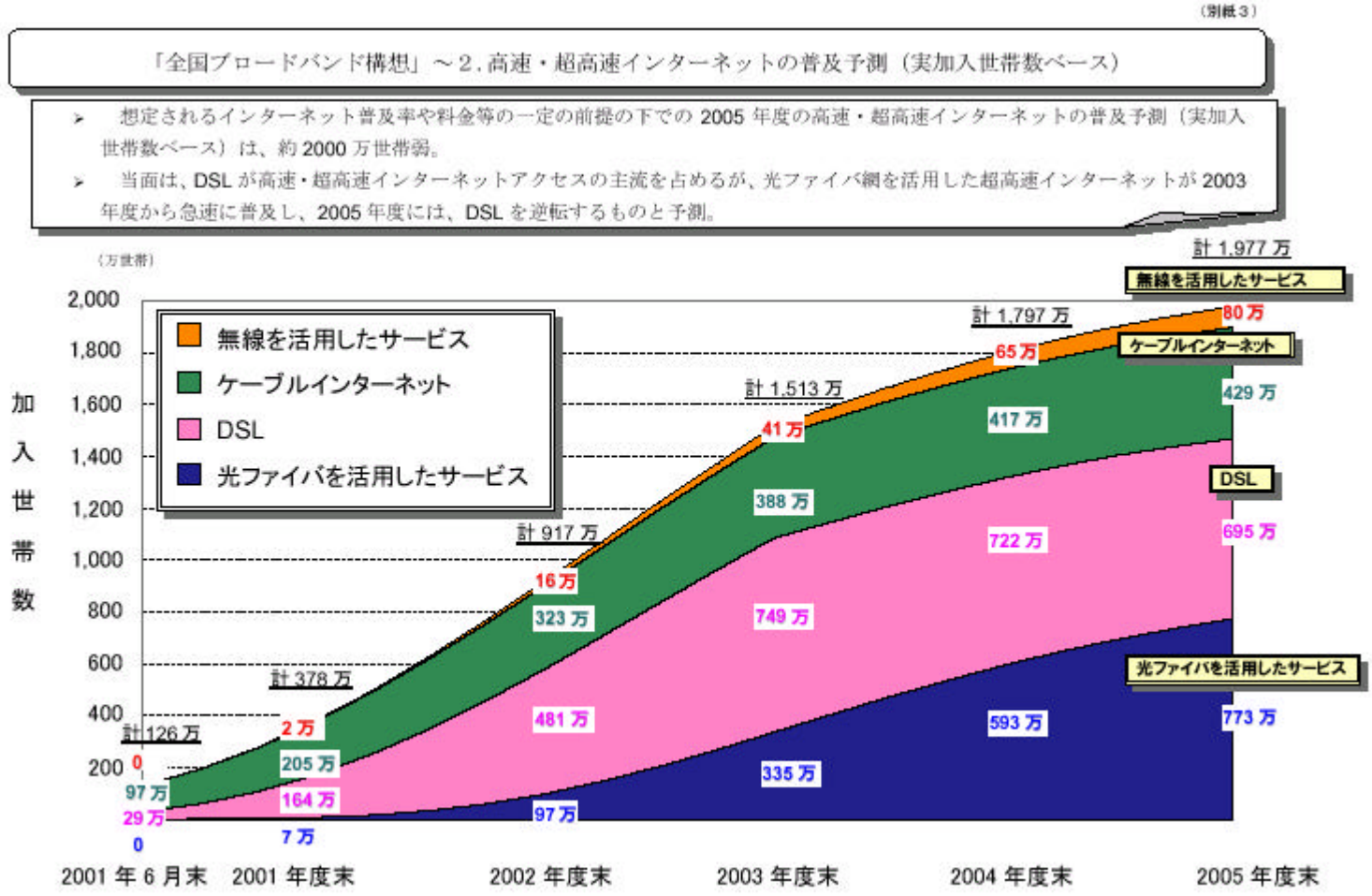
総務省　全国ブロードバンド構想

http://www.soumu.go.jp/s-news/2001/011016_2.html#betten

●目的

- 2005年度までに少なくとも3000万世帯が高速インターネットアクセス網に、1000万世帯が超高速インターネットアクセス網に常時接続可能な環境を整備
- 地理的要因によるデジタル・ディバイドの発生を防止
- 2005年度までに地域公共ネットワークの全国整備を図る

ブロードバンドインタネット普及予測



抜粋 :総務省ホームページ

古河電工

BtoBネットワークに求められるもの

Wecan.

・安定した運用
・高い信頼性
・高度な機密性
（専用線、F／R等）

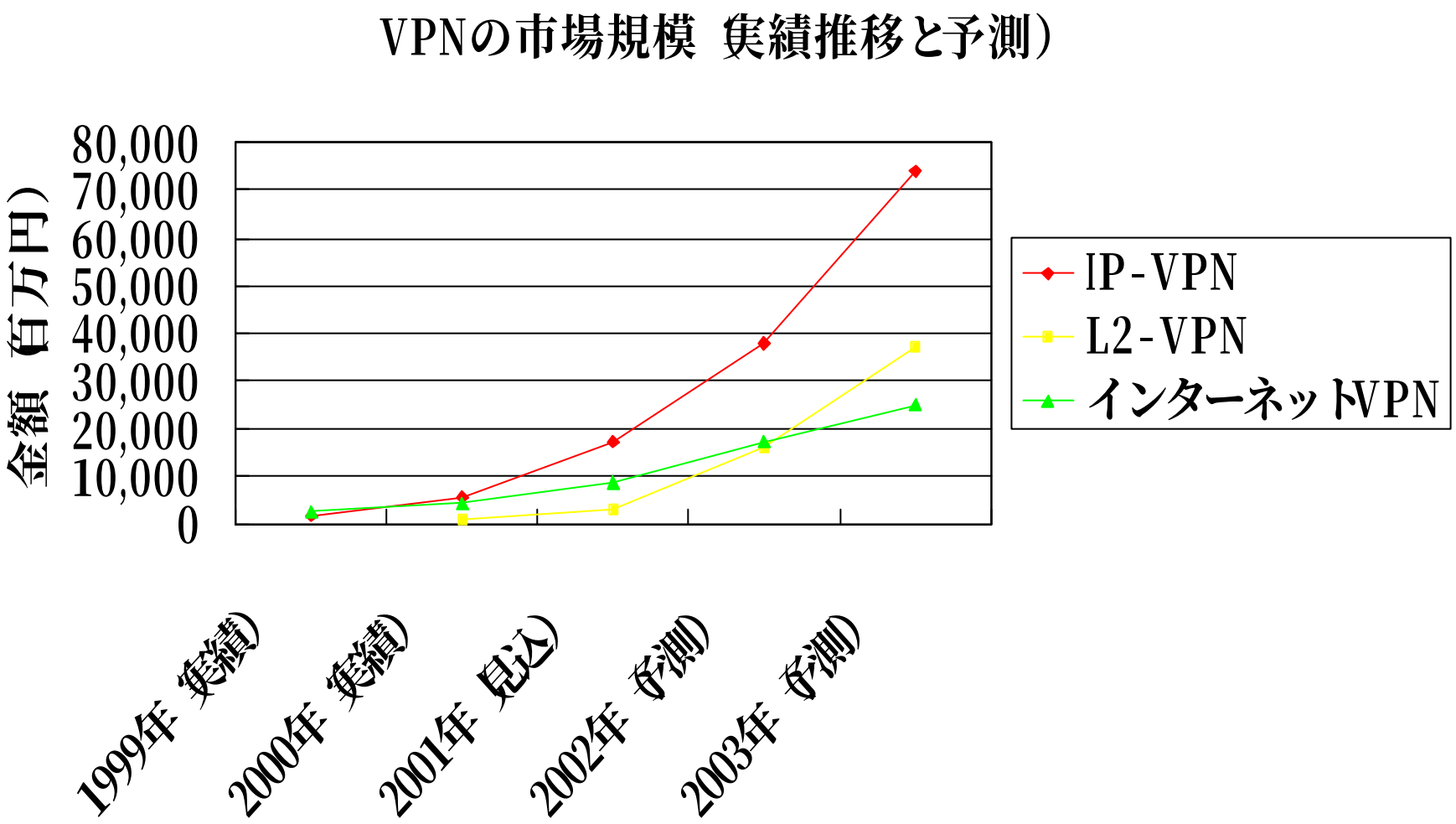
・安価な運用コスト

相反する要求を実現するためのトレンドソリューション

IP-VPNソリューション

古河電工

IP-VPNの市場規模



出典：㈱富士キメラ総研

IP-VPNの方式

インタネットVPN

●ユーザ実現型VPN

・公衆網であるインターネットを、暗号化やトンネリング技術を用いてセキュリティを確保し、あたかも専用線のように使うことを可能にする技術。
・接続各拠点には、IPSEC対応のセキュリティ装置をユーザが用意。

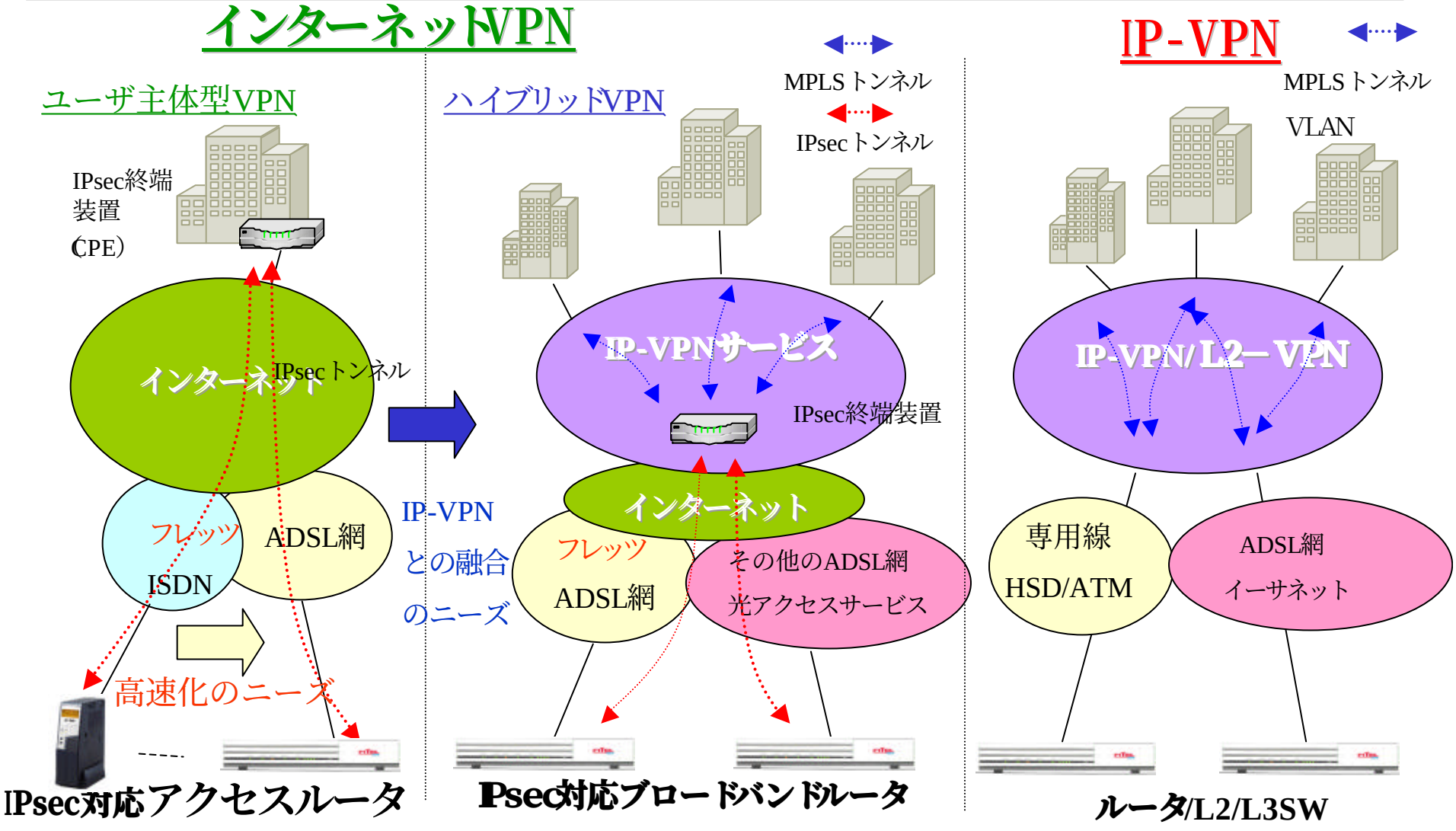
●ハイブリットVPN

・MPLSﾍﾞｰｽのIP-VPNとIPsecﾍﾞｰｽのｲﾝﾀｰﾈｯﾄVPNの統合
・アクセス回線はインタネットを利用し、IPsecで暗号通信し、中継網はIP-VPNサービスを利用することで、接続拠点規模に応じたネットワーク構築が可能
・主要拠点のNW運用コストの削減が可能。

IP-VPN

・従来の専用線で構築していたネットワークを安価に移行できるソリューション
・QOSやSLAによる高品質な通信が可能（Voip等への併用）
・L2ー VPNによる広域LANサービス

IP-VPNの分類


インターネットVPN
ユーザ主体型VPN
IPsec終端
装置
(CPE)
インターネット
IPsecトンネル
フレッツ
ISDN
ADSL網
高速化のニーズ
IPsec対応アクセスルータ
IP-VPN
との融合
のニーズ
ハイブリッドVPN
MPLSトンネル
IPsecトンネル
IP-VPNサービス
IPsec終端装置
インターネット
フレッツ
ADSL網
その他のADSL網
光アクセスサービス
IPsec対応ブロードバンドルータ
IP-VPN
MPLSトンネル
VLAN
IP-VPN/L2-VPN
専用線
HSD/ATM
ADSL網
イーサネット
ルータ/L2/L3SW

IP-VPNのキーテクノロジ

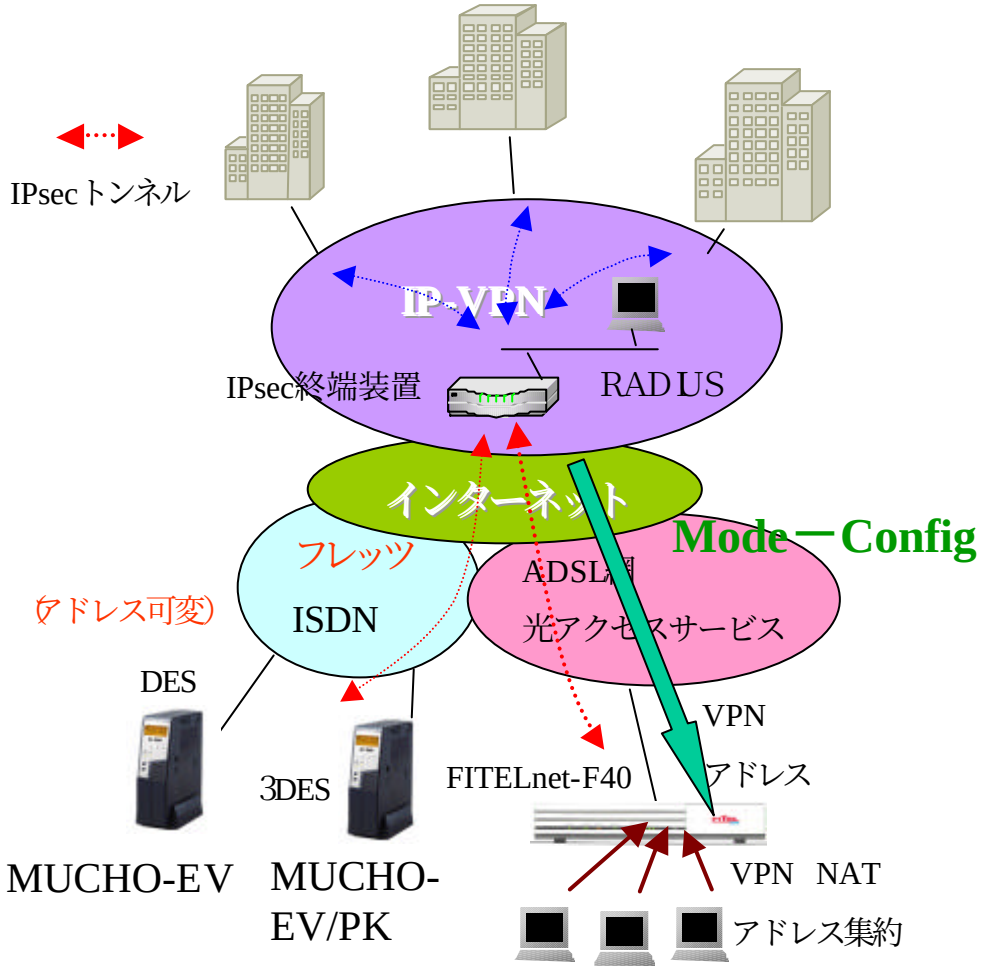
IPsec：Security Architecture for the Internet Protocol

- TCP／IPの通信における、セキュリティを確保するための技術
  ＜トンネリング＞、＜暗号化＞、＜自動鍵交換方式＞、<etc.>
- インタネットVPNに必要なIPsec応用技術動向
  - ダイナミックIPアドレスアサインに対する対応
  - NAT Traversal
  - AES

MPLS＝Multi Protocol Label Switching

- IP-VPN（RFC2547bis）
- MPLSベースのL2-VPN
- トラヒックエンジニアリング

IPSec Aggressive Mode 「Mode-Config」



・拠点側アドレス可変を想定した構成

IPSec Aggressive Mode

・センター（IP-VPN内）IPSec終端装置から

VPNアドレスをダイナミックアサイン

→ Mode－Config

・拠点側 IPSec装置でVPN NAT機能ON

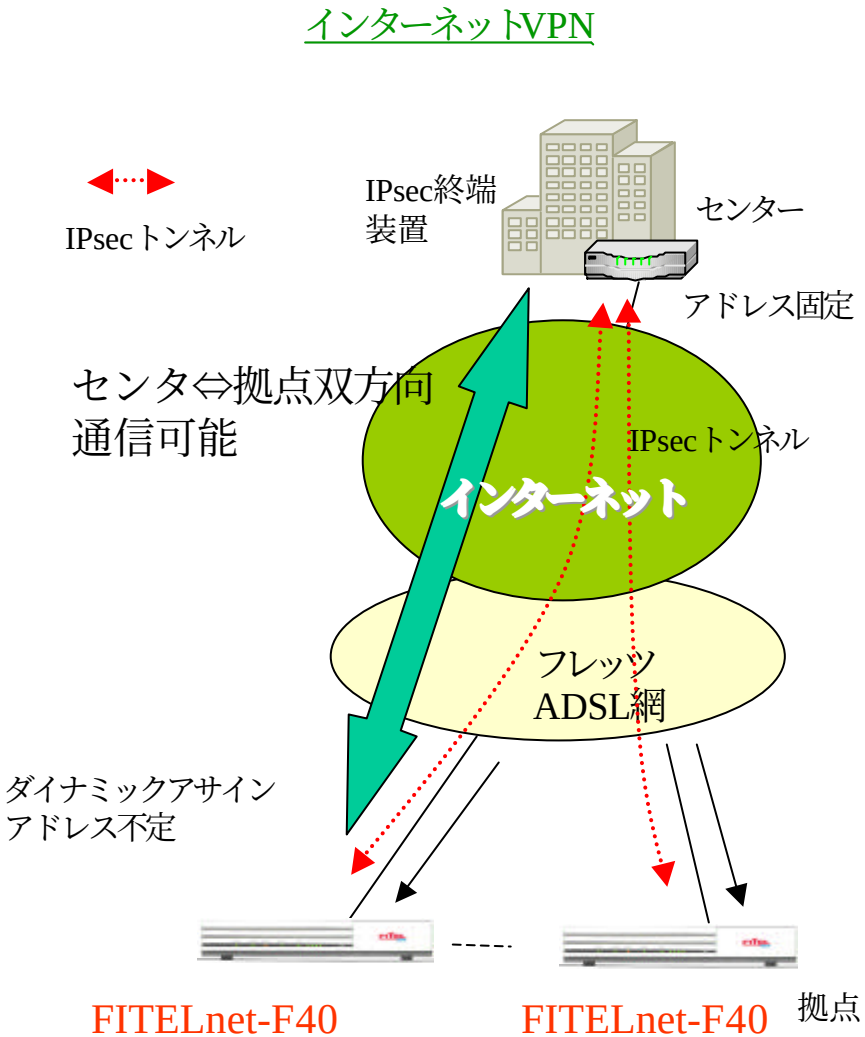
→IP-VPN事業者様側ではアドレス管理

項目が削減できる。

→ダイアルアップアドレスアサインのシステム

(RADIUS) にマージしやすい。

通信コスト削減　IPsec　フレッツADSL　アドレス不定への対応



●アドレス不定環境でのIpsec通信

IPsec Aggressive Modeを利用して、フレッツADSLの一般的な契約である「アドレス不定」でもVPN(IPsec)の通信が実現でき、通信ランニングコストを削減することができます。

※プロバイダA　サービス料金

通常サービス（アドレス不定）　1,950円/月

アドレス固定サービス　6,800円/月

●常時接続の対応

従来では、拠点側「アドレス不定」環境でのVPN(IPsec)の通信では、データ通信契機は、拠点→センター方向に限定されていましたが、

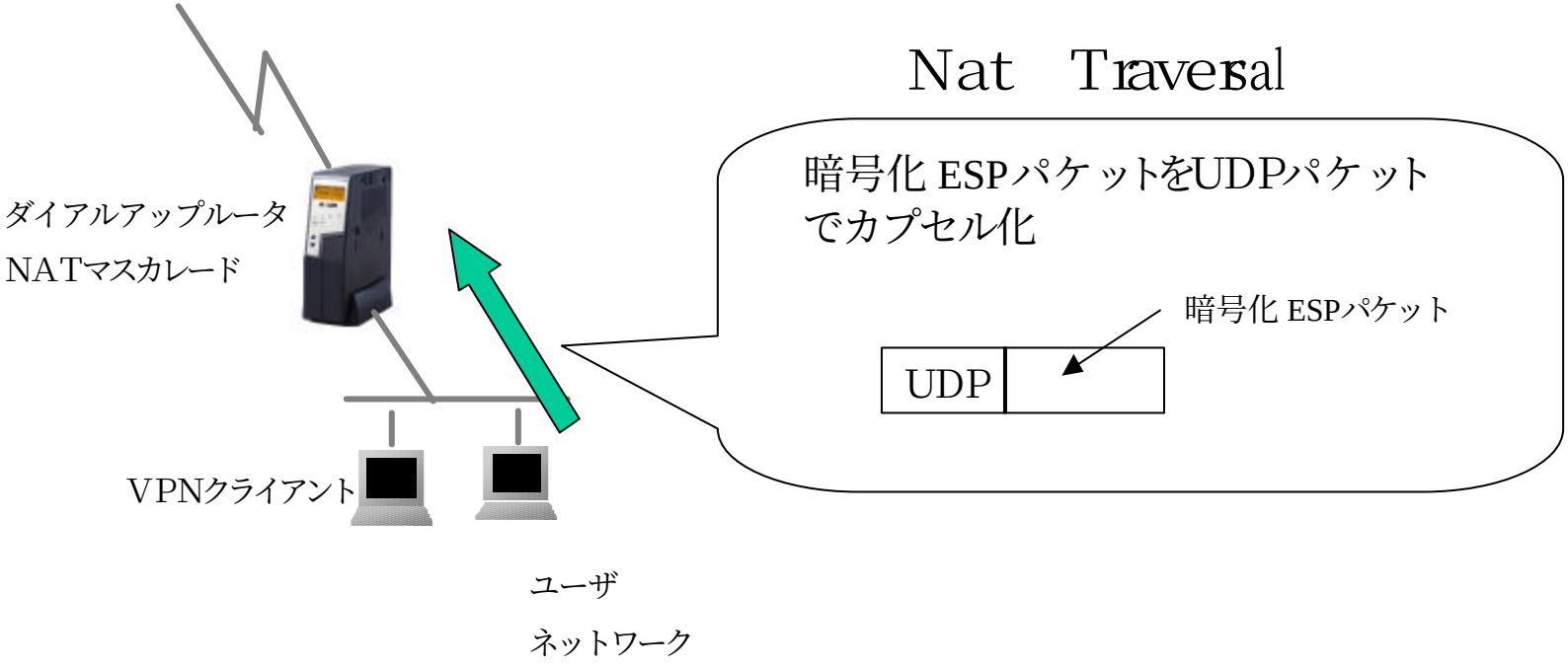
装置（FITELnet-F40）リセットや ADSLの ダウン→アップが発生しても、データの発生契機、方向に関わらず、VPN(IPsec)の通信を自動的に再開できる機能がサポートされ、拠点側「アドレス不定」環境での双方向通信を実現します。

NAT　Traversal

「NAT　Traversal」

経路上でNATマスカレード変換される場合のIPsec通信ができない問題を解決

－暗号化（ESP）パケットにはポート情報がない



次世代暗号化方式　AES

AES

「Advanced Encryption Standard」

DES、3DES

AESへ

暗号強度の改善

–DES（56bit）の「強度」

»1999年1月の解読コンテストでは22時間15分で解読

–3DES（168bit）の「強度」

»概ね80bitから112bit程度の鍵を用いたDESと同等

－米商務省技術標準局(NIST)が「DES (Data Encryption Standard)」の後継となる次世代暗号標準技術「Advanced Encryption Standard(AES)」に「Rijndael」を選定

－Rijndaelとは、ベルギーの暗号専門家であるJoan Daemen氏とVincent Rijmen氏が開発した暗号アルゴリズム

－AESは128、192および256ビットの暗号鍵に対応する暗号技術。米政府が従来、暗号標準技術として用いてきたDESの56ビットに比べて鍵長が長いため遙かに強力

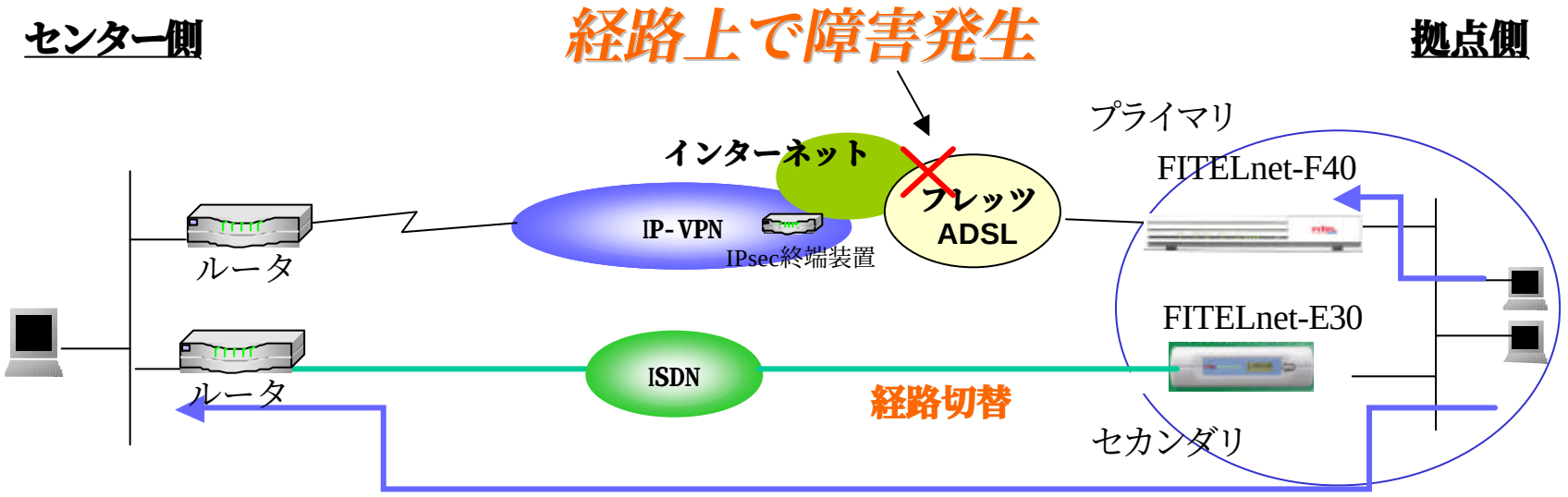
－さらに、DESの強化版である3 DESの168ビットに比べても、192ビットと256ビットのAESでは暗号機能が強化されていることと、3DESの問題であった装置の暗号処理負荷が大きいことについて改善が図られている

ブロードバンドルータFITELnet-F40

- 高速なIPsec
  - 多くの導入実績やノウハウを持ち，相互接続性も実証されているIPsec技術を搭載
  - IPsec動作時でもADSLの速度を損なわないスループットを実現
- 冗長性
  - アクセスルータFITELnet-E30と組み合わせた冗長構成をサポートし，ADSL側から任意のIPホストまでの到達性が損なわれた場合，ISDN側に切り替わるバックアップ動作が可能

FITELnet-F40の特長　冗長構成 ～ADSL網ダウンに対応～

ブロードバンドルータとISDNルータの組み合わせ。当社独自のホットスタンバイ＋L3監視機能を利用し、拠点側からの経路切り替えを実現します。



・セカンダリのルータは、スタンバイ状態で待機している。

・拠点側にあるPCからは、ルータは一台に見える。

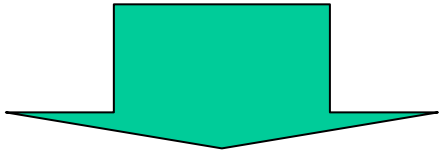
・経路に障害が発生した場合、セカンダリISDNルータがバックアップ動作を開始、経路の切り替えを行います。

・拠点側では、引き続きセンタ側への通信が可能となります。

何故、ブロードバンド→MPLSか？

ブロードバンドの特徴的傾向

- 低価格で広帯域の確保があらゆるユーザ層へ
- 常時接続
- サービスの多様化
  トラフィックの多様化→ストリーミング、VoIP、IP-VPN…



ネットワークの効率良い運用の必要性

- トラフィックエンジニアリング
- セキュリティ
- 顧客ニーズに対応したマルチサービスの実現

IP-VPNの主要技術　MPLS

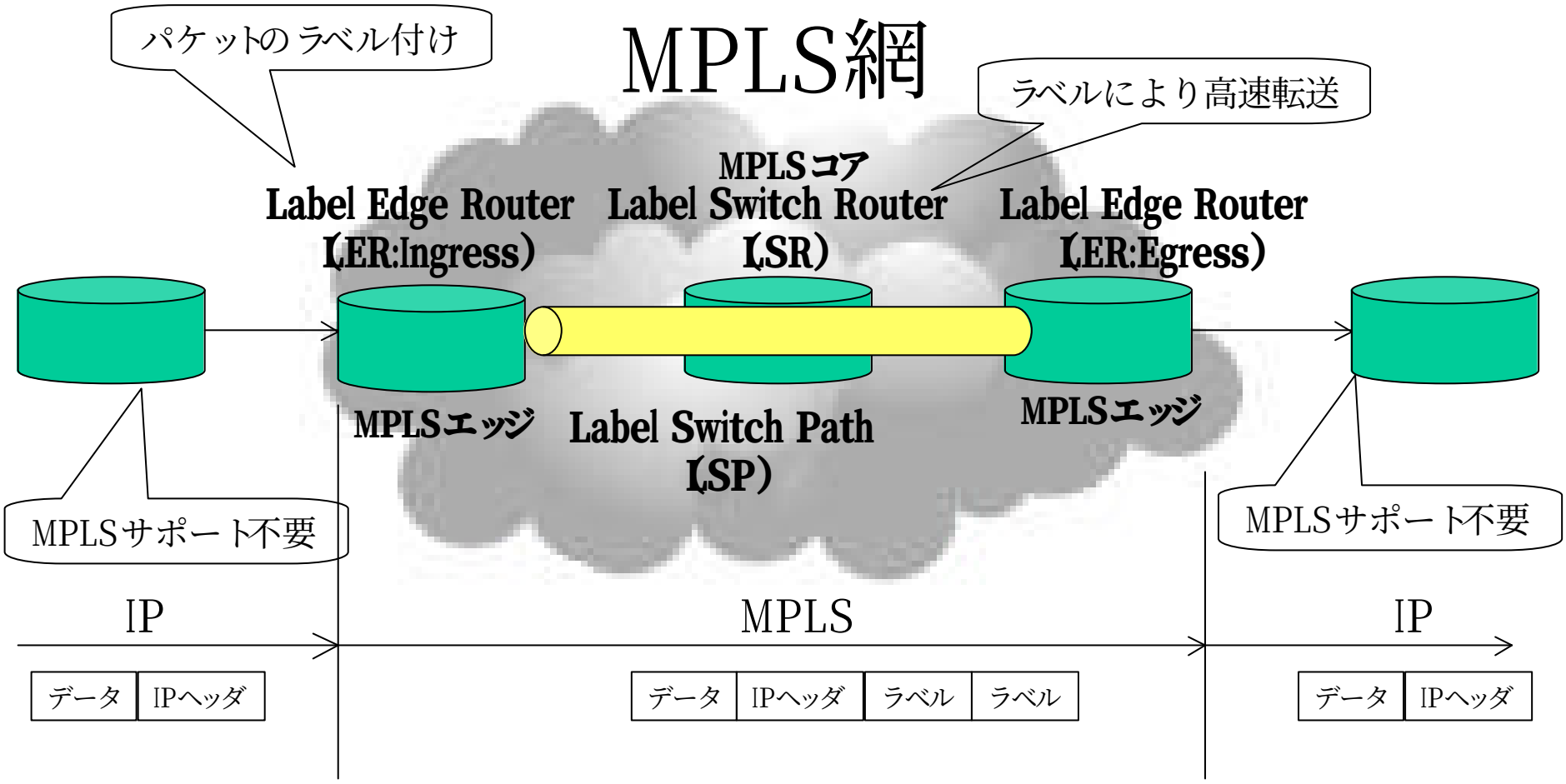
- **MPLS＝Multi Protocol Label Switching**

  従来のIP中継技術は、IPヘッダ内の宛先IPアドレスをもとに中継先を決定したのに対して、ヘッダに付加されたラベルをもとに中継先を決定する中継技術（ラベルスイッチ）

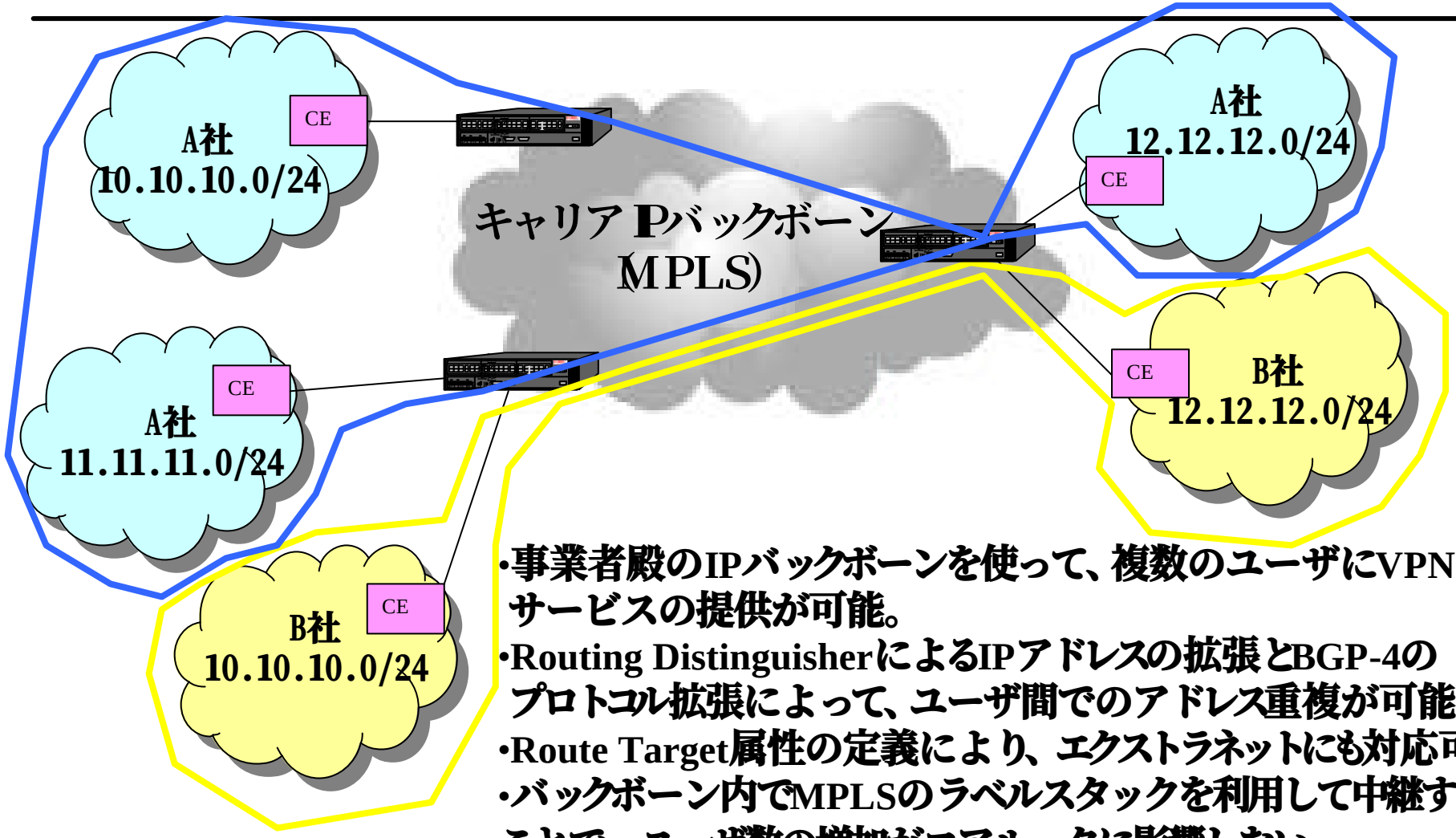
- **ラベルについてはシグナリングプロトコルによって交換し、ラベルスイッチパス（LSP）を決定する。**

  シグナリングは、LDP（Label Distribution Protocol）とRSVP（Resource Reservation Protocol）の2種類が標準化

MPLSの仕組み


パケットのラベル付け
MPLS網
ラベルにより高速転送
MPLSコア
Label Edge Router
（LER:Ingress）
Label Switch Router
（LSR）
Label Edge Router
（LER:Egress）
MPLSエッジ
Label Switch Path
（LSP）
MPLSエッジ
MPLSサポート不要
MPLSサポート不要
IP
MPLS
IP
データ
IPヘッダ
データ
IPヘッダ
ラベル
ラベル
データ
IPヘッダ

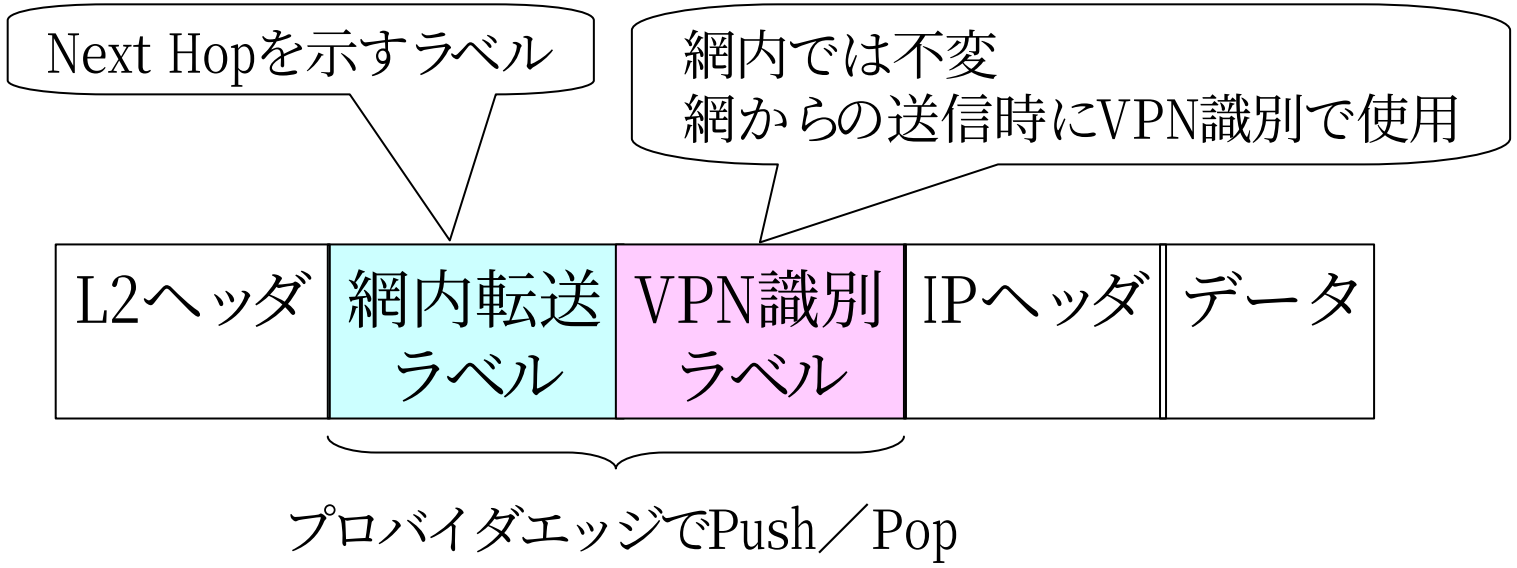
IP-VPN（RFC2547bis方式）



- 事業者殿のIPバックボーンを使って、複数のユーザにVPNサービスの提供が可能。
- Routing DistinguisherによるIPアドレスの拡張とBGP-4のプロトコル拡張によって、ユーザ間でのアドレス重複が可能。
- Route Target属性の定義により、エクストラネットにも対応可能。
- バックボーン内でMPLSのラベルスタックを利用して中継することで、ユーザ数の増加がコアルータに影響しない

IP-VPNの技術

- MPLS :Multi Protocol Label Switching
  - IPパケットの トンネリング技術の1つ
  - ラベルパスによりIPレベルでのコネクションを実現
  - IP-VPNではラベルを2スタックで使用



VLANベースL2-VPN（広域LANサービス）

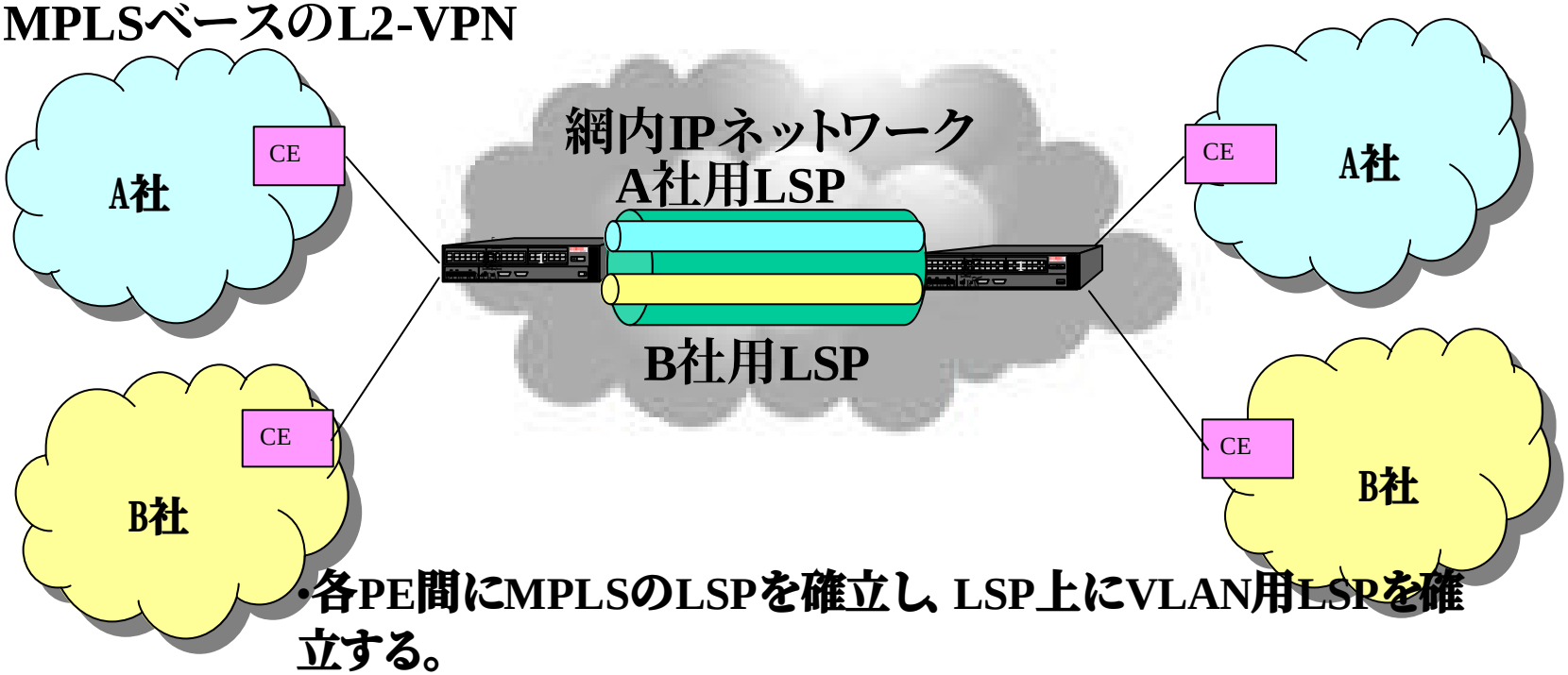
VLANベースのL2-VPN

•VLANベースのL2-VPNでは、網内のL2ネットワーク内にTag-VLAN機能を利用して各ユーザ用のVLANを構築する。

網内でサービス可能なユーザ数がTag-VLANの数（≦4096）に制限される。

MPLSベースのL2-VPNとの比較

MPLSベースのL2-VPN



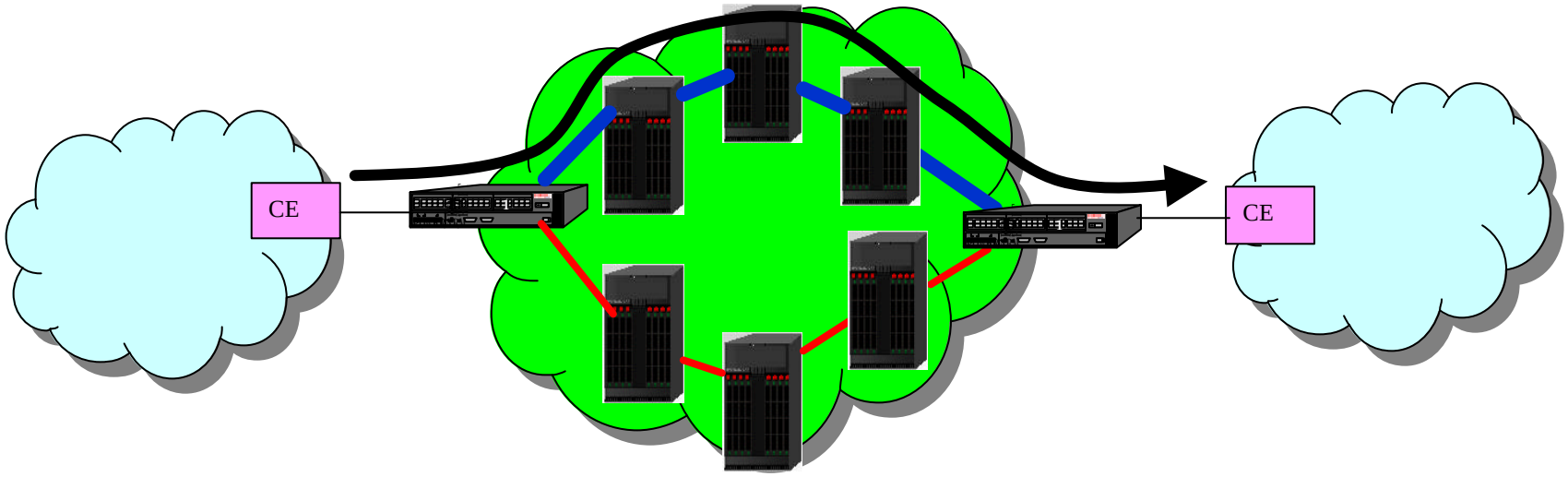
- 各PE間にMPLSのLSPを確立し、LSP上にVLAN用LSPを確立する。
- 各拠点間を同一LANで接続する（PE間はブリッジ中継）。
- 拠点間はマルチプロトコルデータの中継が可能。
- PEでは拠点間のLSP毎にMACアドレスの学習を行う。

網内でサービス可能なユーザ数は、MPLSのラベル数（約100万ラベル）まで設定可能

MPLSベースのL2-VPN

- Point-to-Point ⇒ VLL (Virtual Leased Line)
  - 従来のFrameRelay、ATM専用線網と等価なサービスをMPLS網経由で実現
  - Draft-Kompella
    - BGP-4 MPを使用
  - Draft-Martini
    - LDPを使用
- Point-to-Multipoint ⇒TLS (Transparent Lan Service)
  - 広域Ethernet LAN間接続サービスをmpls網経由で実現
  - Draft-VKomprlla

トラフィックエンジニアリング



- RSVP-TEを用いて、帯域に見合った経路を選択してLSPを確立する。
- 経路の選択方法として、Ingressルータでスタティックに設定する方法とOSPF-TE/IS-IS-TEでダイナミックに選択する方法が可能。
- LSR-MIBを利用して、パスごとにトラフィックの監視が可能。

Qos/Cosの実現　～DS-TE機能の概要～

Wecan.

- **同一LSP上でEXPの値によって優先制御（E-LSP）**

- **Ingressでは、IPアドレス、TOS/Precedence、TCP/UDPポート番号、IEEE802.1p/802.1qのヘッダでデータをクラス分け可能**

- **Ingressでは、クラス毎のrate-limitおよびDiff-Servクラスに従ったキューイングが可能**

- **CoreおよびEgressでは、Diff-Servクラスでのキューイングおよびフォワーディングが可能**

古河電工

ＭＰＬＳ最新動向

- **Fast Reroute**
  リンク障害時の高速切り替え技術（リンクプロテクション）

- **QoS/CoS**
  Diffservとの連携
  Diffserv-aware-TE

- **Layer2 IP-VPN**
  Layer2サービスをMPLSコア網上にエミュレーション

- **IPv6　over　MPLS**

- **GMPLS**

標準化の動向

- 基本的なプロトコルは標準化済み
  RFC3031:Multiprotocol Label Switching Architecture
  RFC3032:MPLS Label Stack Encoding
  RFC3036:LDP Specification
  RFC3209:RSVP-TE: Extensions to RSVP for LSP Tunnels
- 付加機能の検討
  MPLS　TEの継続検討
    Fast　Reroute
  Diff-servとの連携
    Label-inferred LSP(L-LSP)
    EXP-inferred LSP(E-LSP)
    Diff-Serve aware TE
- その他
  次世代IX研究会による相互接続試験の推進

メトロエッジルータFITELnet-Gシリーズ

- フルワイヤースピード
  - GbEポート，アクセスリスト，QoSの設定時，IP Multicastにおいてもフルワイヤースピード
- RIC※の成果を実現したQoS
  - 1000フロー／ GbEポート，64フロー／ FEポートの高速処理
  - マルチキャストでのダイナミックなQoS保証と経路制御を可能にするHQLIP+SRSVP方式
- MPLS
  - エッジとコアの両機能をサポートしMPLSにおいてもフルワイヤースピード

※RIC（Real Internet Consortium）：http://www.real-internet.org/
超高速・高機能次世代インターネットコンソーシアム．古河電工はプロトコル方式の開発並びに実装および検証を担当．

カスタマエッジルータFITELnet-Bシリーズ

- IP-VPN/L2-VPN等のイーサネット・アクセスに最適な、カスタマエッジルータ
- フルワイヤースピード
- 高速キューイング技術であるPPQにより32フロー/ポートのQos制御が可能
- IPv6対応（FITELnet-B4）
- BGP-4サポートにより、IP-VPN利用時の冗長構成を実現

装置名	中継インタフェース	
	Gigabit Ethernet	Fast Ethernet
FITELnet-B10	2	16
FITELnet-B4	—	8