

ご参考 (BPセキュリティ・ソリューション・フォーラム資料)
VPN (Virtual Private Network) の構築

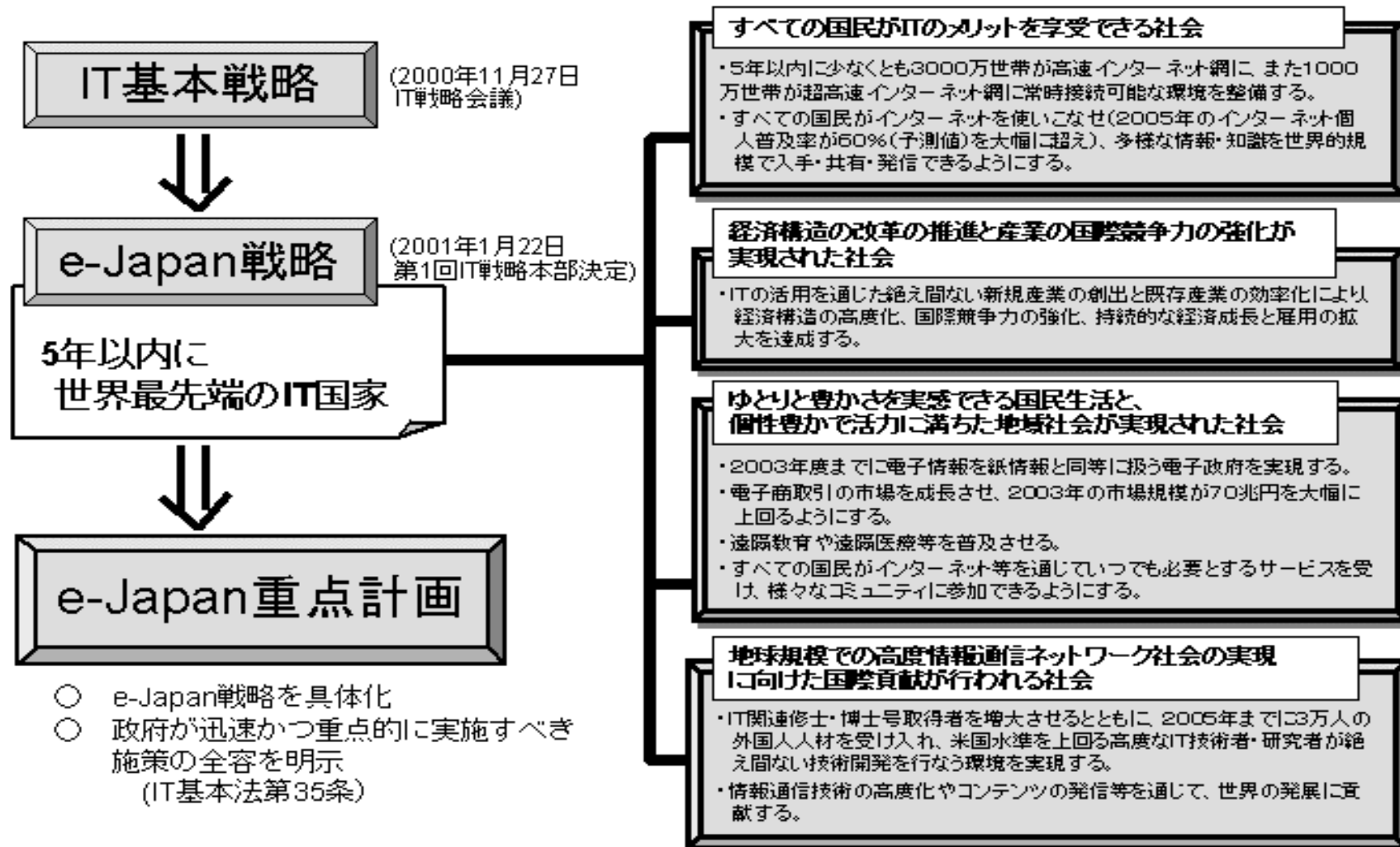
-ブロードバンド時代にセキュリティとスピードを両立させる-

2001年12月4日 13時40分～14時20分

古河電気工業株式会社

安田圭一

e-Japan戦略の基本的な方針



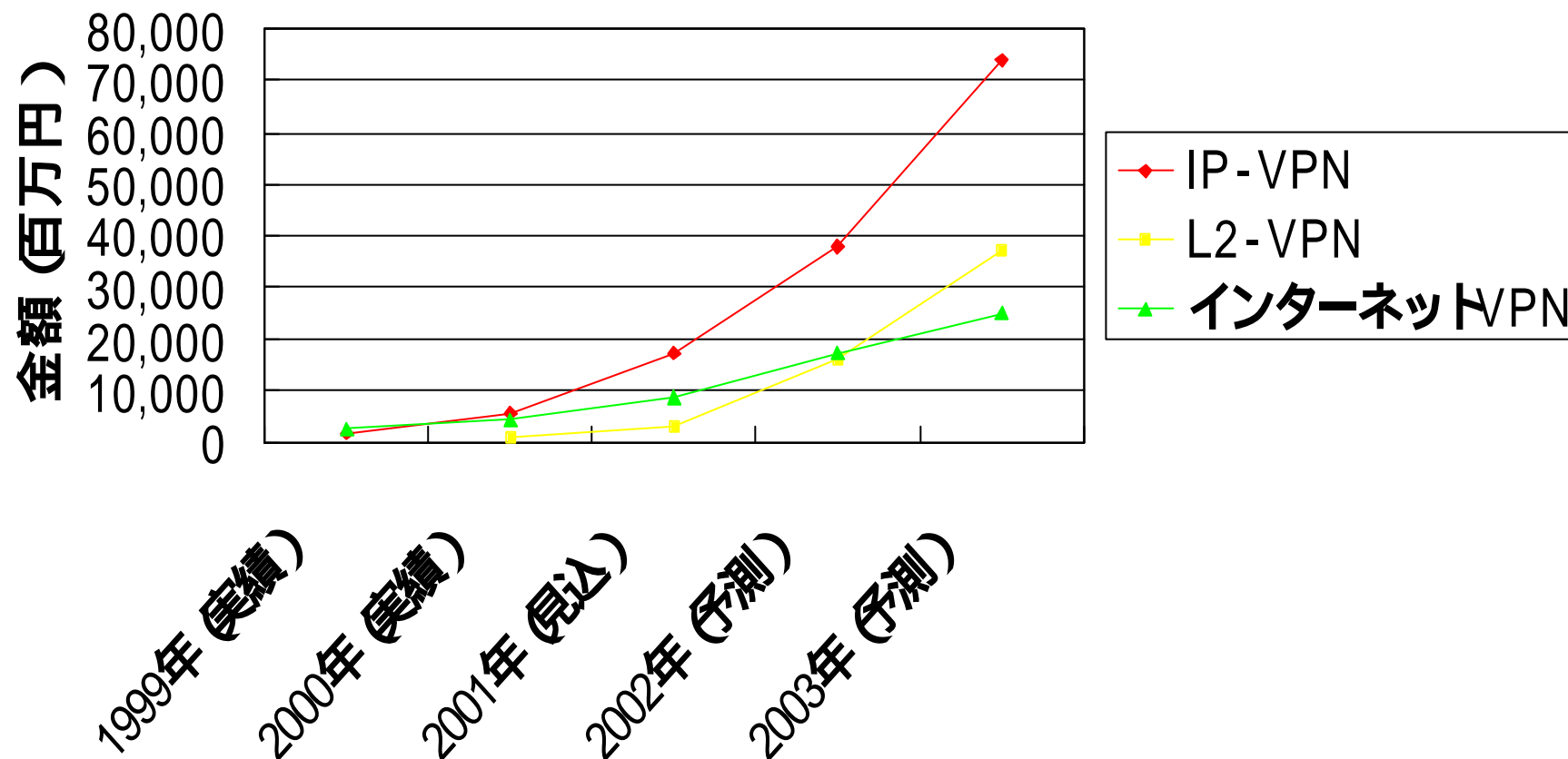
抜粋 : 首相官邸ホームページ

VPNの種類

- IP-VPN
- L2-VPN (広域LANサービス)
- インターネットVPN
- ハイブリッドVPN
 - IP-VPN + インターネットVPN

VPNの市場規模

VPNの市場規模 (実績推移と予測)



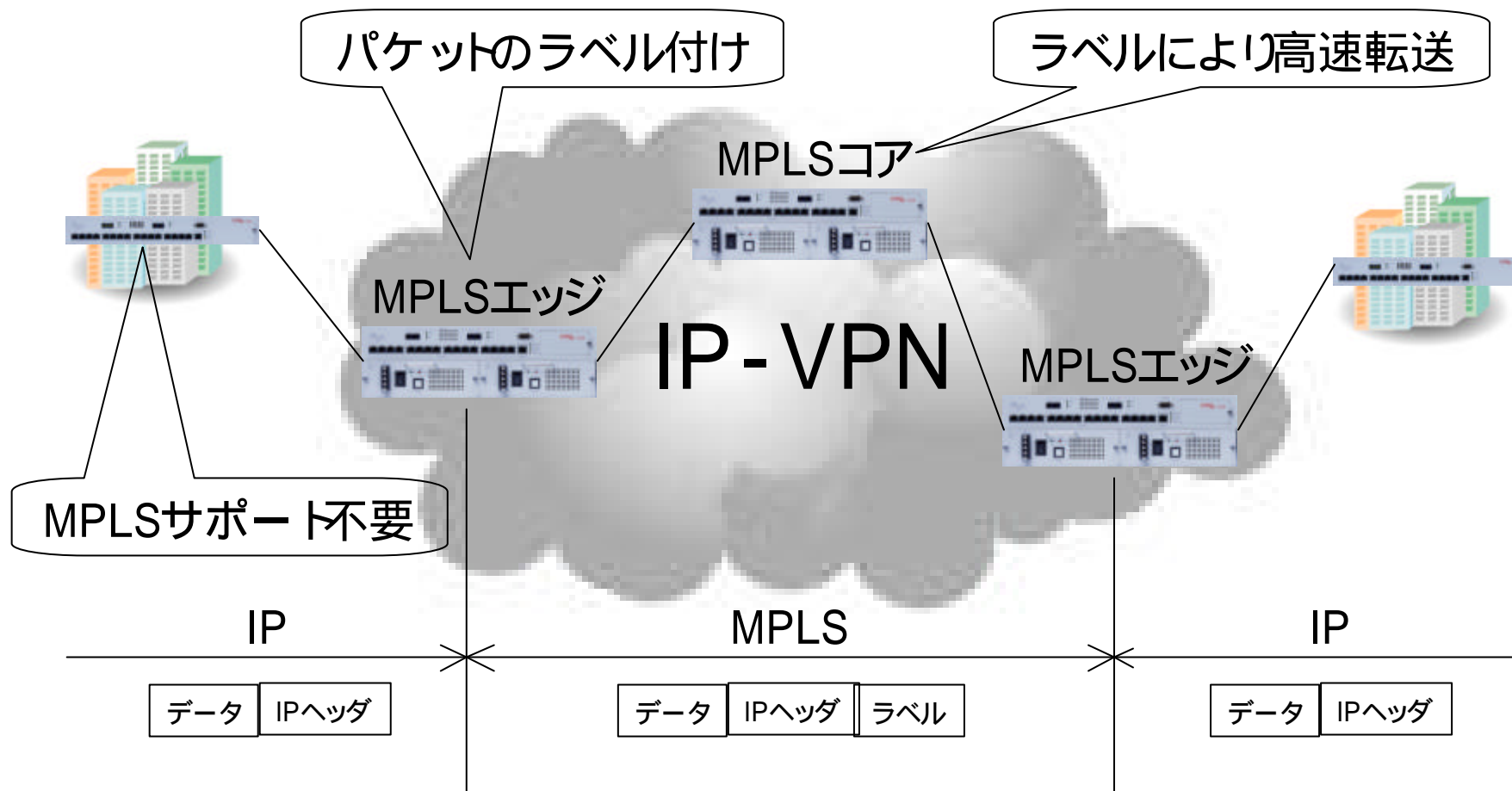
出典：(株)富士キメラ総研

VPNの比較

VPN	IP-VPN	L2-VPN (広域LANサービス)	インターネットVPN
網	キャリア	キャリア	インターネット
ユーザー インタフェース	レガシー (BRI ,PRI ,ATM) イーサネット	イーサネット	レガシー (BRI ,PRI ,ATM))
セキュリティ	MPLS	VLAN	IPsec
ネットワーク プロトコル	IPのみ	IP以外も利用可	IPのみ
ルーティング プロトコル	BGP-4等の制限あり	制限なし	Staticのみ
QoS / CoS	あり	なし	できない
運用コスト	比較的安価	比較的安価	安価

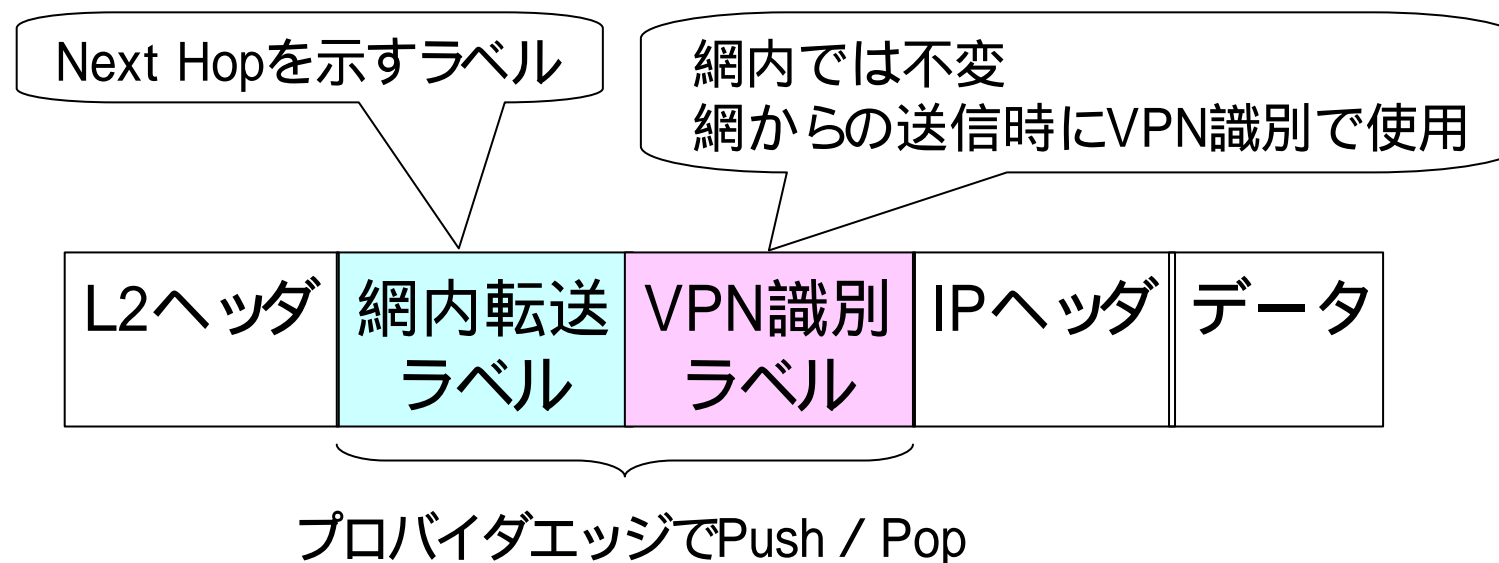
IP-VPN網の構成

- MPLSのコアルーターとエッジルーターで構築



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



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UMPLSにおいてもフルワイヤースピード



ボックス型
FITELnet-G12



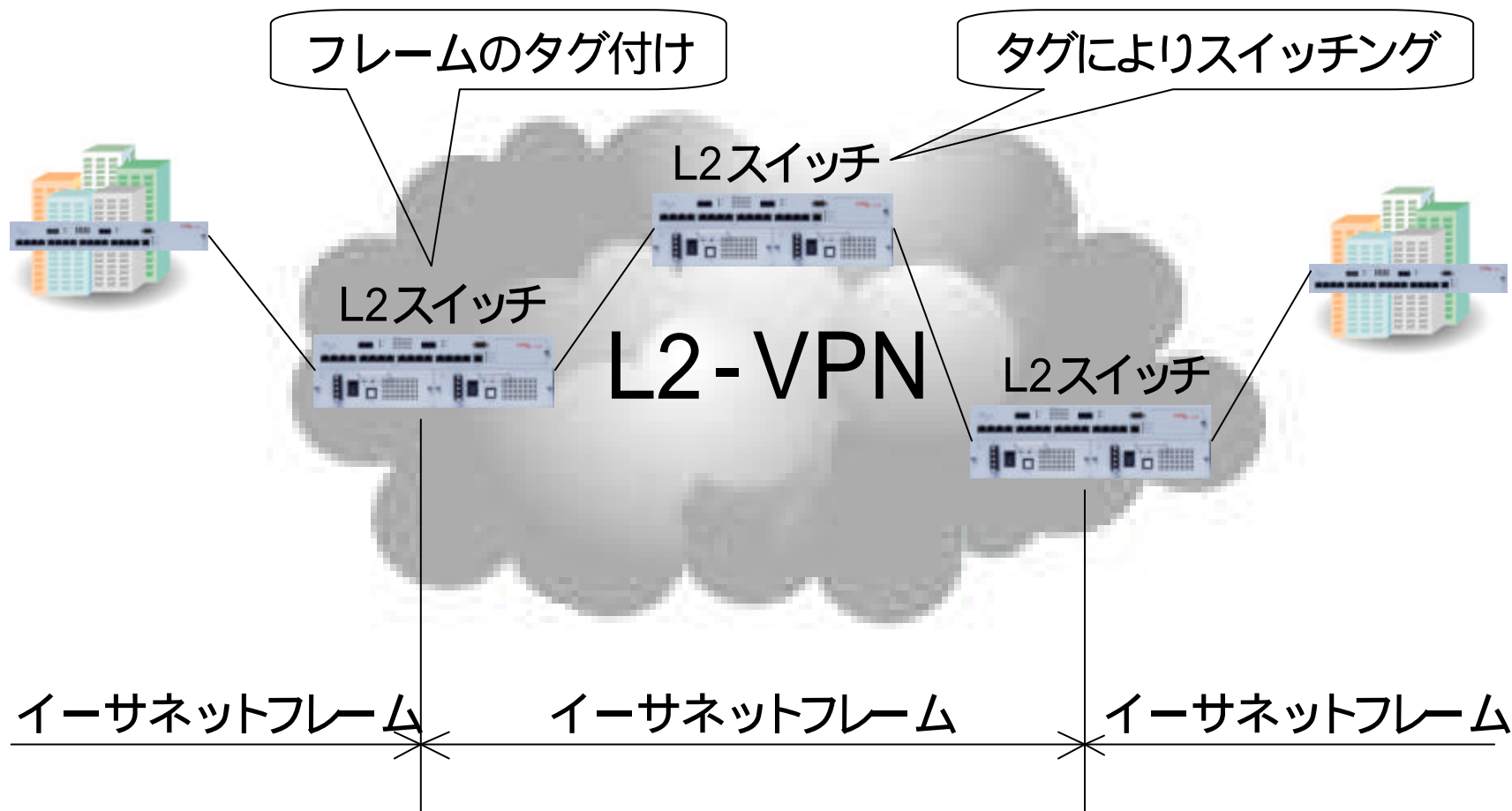
シャーシ型
FITELnet-G40

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。

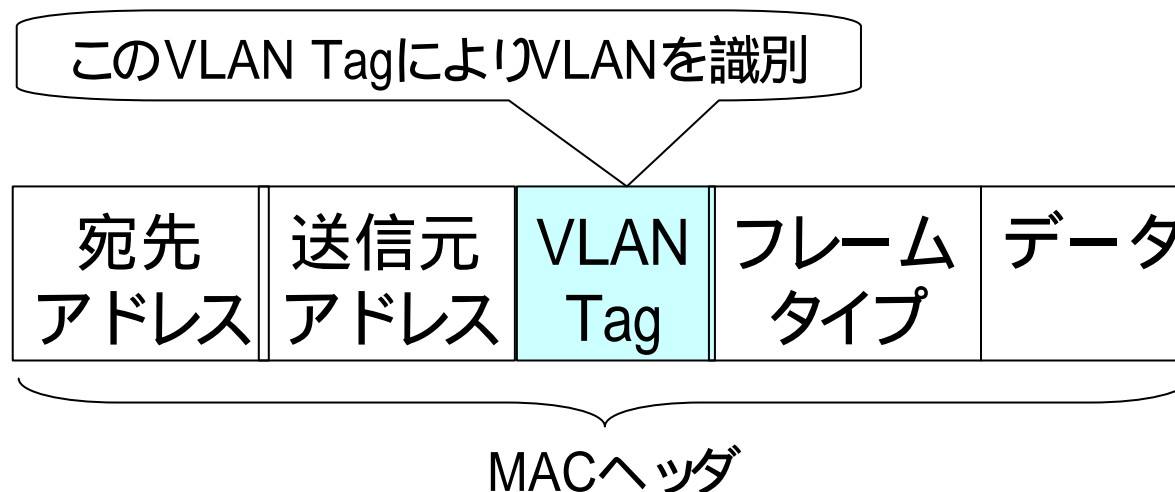
L2-VPN網の構成

- L2スイッチで構築



L2-VPNの技術

- VLAN :Virtual Local Area Network
 - 仮想的なLAN構築技術の1つ
 - VLAN TagでVLANを識別
 - 1つの物理ポートに複数のVLANを割り当て可能
 - Tag VLAN



インターネットVPNの構成

- IPsec終端装置で構築

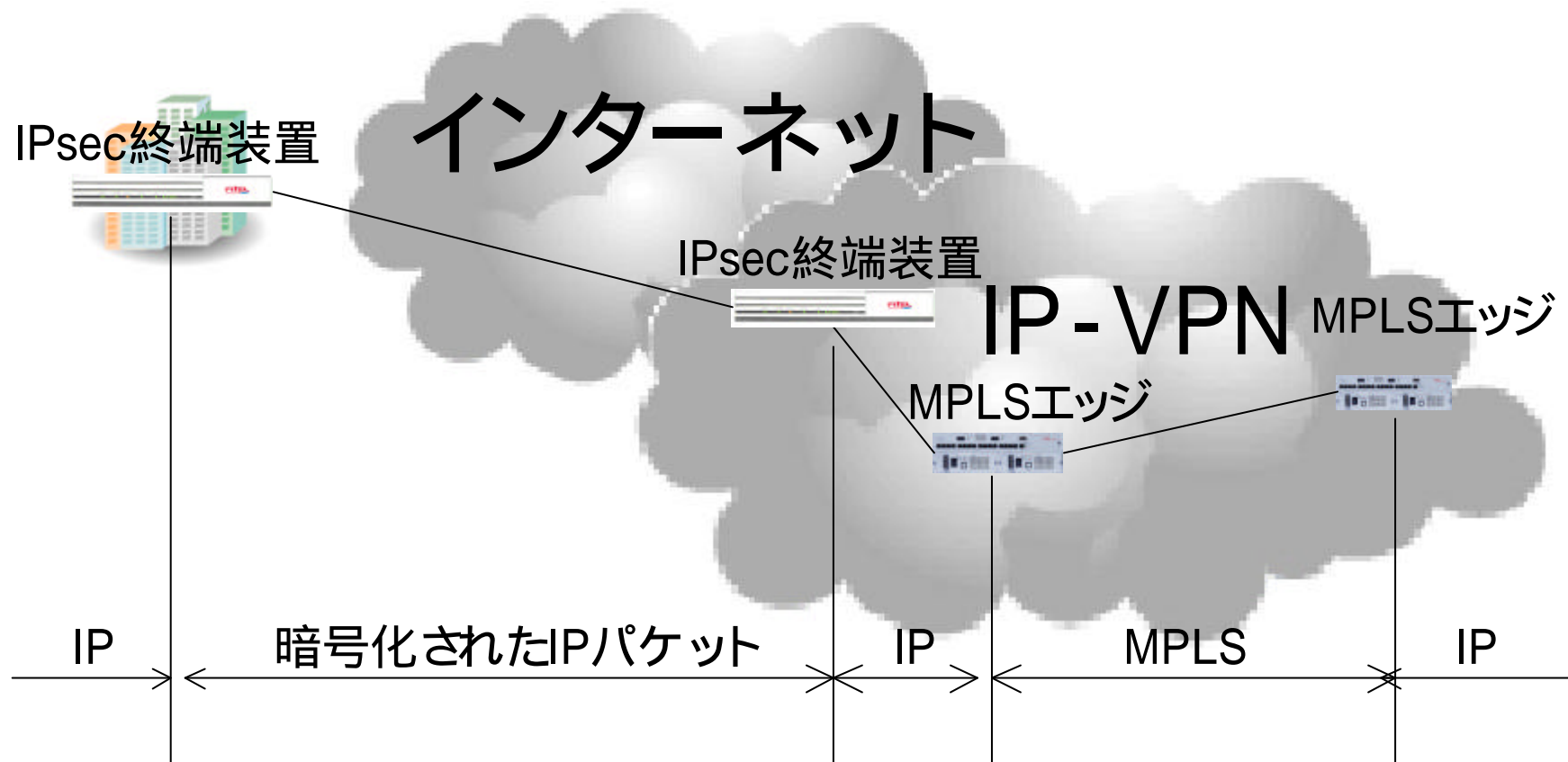


インターネットVPNの技術

- IPsec :Security Architecture for the Internet Protocol
 - IPパケットのトンネリング技術の1つ
 - ESP :Encapsulating Security Payload
 - 通信ホストの相互認証
 - 送信データの暗号化
 - 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

ハイブリッドVPN

- IP-VPNへのアクセス手段としてインターネットVPNを使用



VPN導入の目的

- コスト削減
 - 回線コストの削減
 - 管理コストの削減
 - 自営網からキャリアへのアウトソーシング
- 帯域拡大
 - 同一コストでの帯域拡大
- イン트라ネット/ エクストラネット構築

VPN導入時の検討項目

- ネットワーク構成
 - イン트라ネット/エクストラネット
 - ネットワーク機器
 - プロトコル

- セキュリティ

- 通信品質

IP-VPN導入時の留意点

- ルーティングプロトコル
 - 網側のルーティングプロトコルに制限あり
 - BGP-4等カスタマエッジでの対応が必要

- 優先制御
 - ToSフィールドに値を設定する必要あり
 - カスタマエッジでの対応が必要

L2-VPN導入時の留意点

- 網は「土管」
 - カスタマエッジ側でQoS等を考慮する必要あり
 - カスタマエッジはL2スイッチやL3スイッチではなく、ルータ機能の充実した機器が必要

カスタマエッジルータFITELnet-B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
 - 256フロー / GbEポート,32フロー / FEポートの高速処理



FITELnet-B12

インターネットVPN導入時の留意点

- 導入する機器
 - 接続性
 - 他ベンダーとの接続性
 - IPsecでの性能
 - ブロードバンドでは暗号化 / 復号化の性能差が顕在化

ブロードバンドルーター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
 - アクセスルーター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