We can.

VPN(IPSEC)の動向と構築時のポイントについて

2001年7月

古河電気工業株式会社
ネットワーク事業部
ネットワークインテグレーションチーム
宮坂　行真（miyasaka@ni.furukawa.co.jp)

古河電工

内容

- VPNのニーズ、動向
- 古河電工　VPN (IPSEC)ソリューション

  ～製品ラインナップ、導入事例～
- VPN (IPSEC)構築時のポイント

VPNのニーズ、動向

VPNの種類

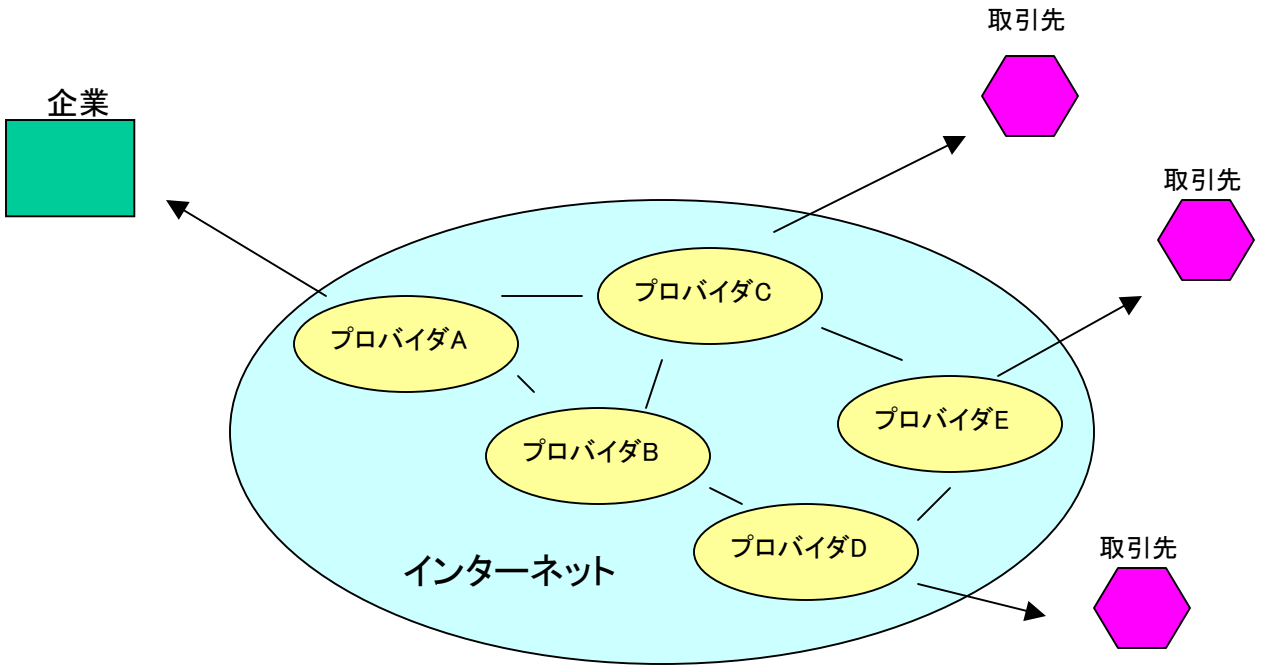
・インターネットVPN

・IP－VPN

VPNの種類

・インターネットVPN

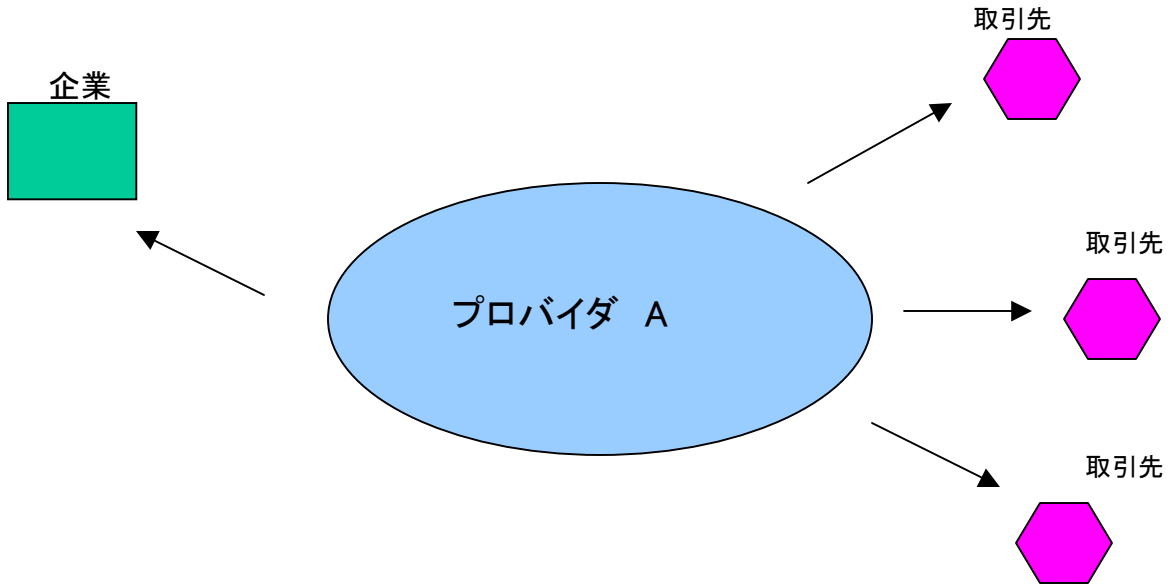
既存のインターネット接続を利用できる
アクセスポイントが多い



VPNの種類

- IP-VPN

  インターネットとは独立した専用のIPネットワーク上で提供される閉域IP網
  ユーザサイトで暗号化などの特別な装置は必要がない
  アクセスポイントは少ない



インターネットVPNとIP－VPN

インターネットVPN　　IP－VPN

インターネット	使用するネットワーク	閉域のIP専用ネットワーク
○（各拠点よりインターネット接続）	VPNと インターネット接続併用	×（センターからのインターネット接続）
IP-VPNより安い	ランニングコスト	インターネットVPNより高い
遅延、スループットは保証されない	通信品質	遅延、スループットの保証、目標値がある

VPNのニーズ、動向

・通信コスト削減

・既存インターネット接続から変更が容易（インターネットVPN）

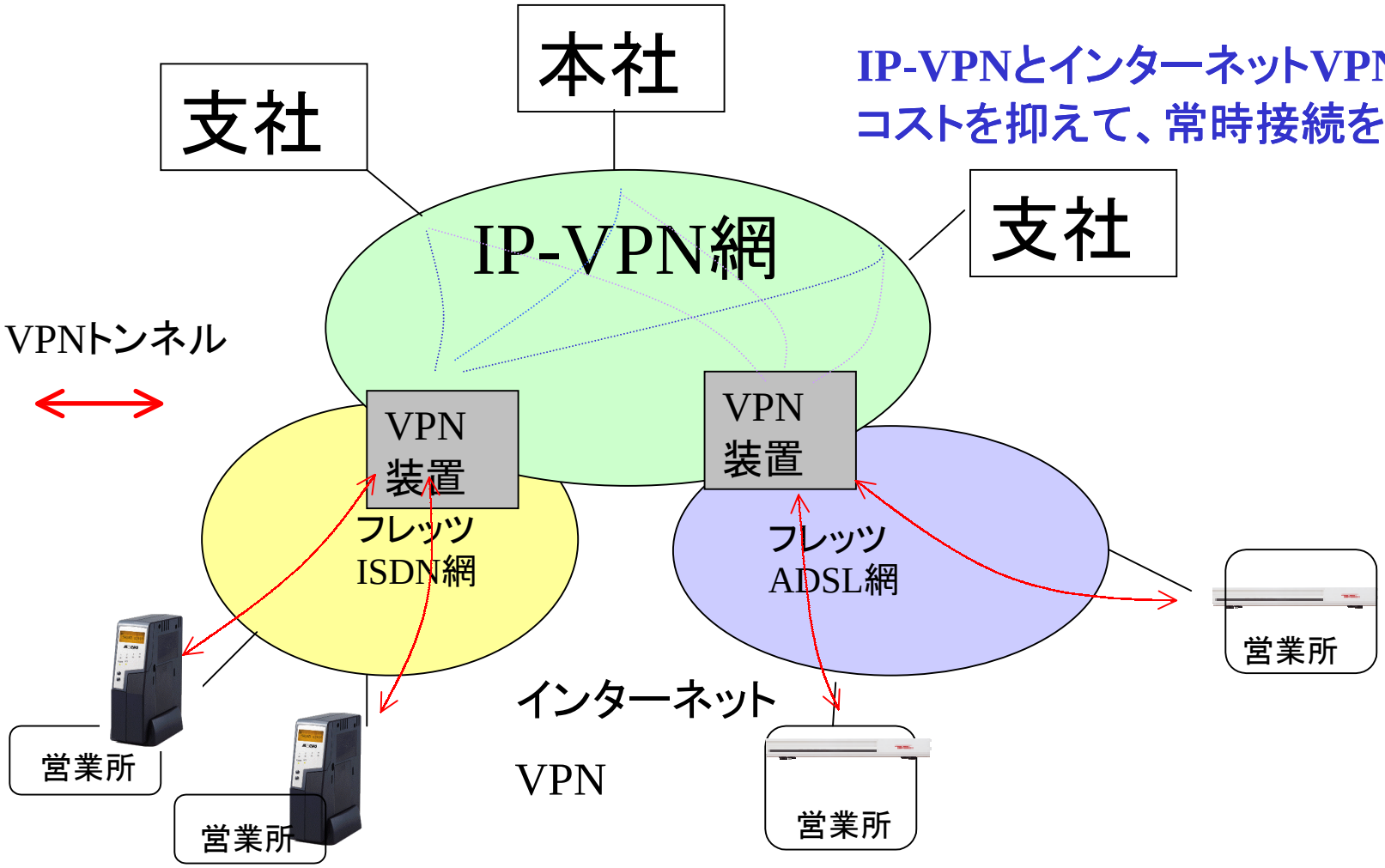
・積極的なセキュリティ確保の手段　ex.改竄防止

・フレッツサービスで閉域ネットワーク　ハイブリッド型

・キャリアサービスで積極的に採用、検討

黒字：従来からのニーズ　赤字：最近の動向

ハイブリットVPN



IP-VPNとインターネットVPNを融合
コストを抑えて、常時接続を実現

IPSEC

- インターネットVPNでは、IPSECが使われているケースが多い

- IP－VPNでも、キャリアが積極的に検討、採用
  - －セキュリティ確保としての負荷価値サービス　暗号化
  - －ハイブリッド型でのサービスコスト削減、提供エリア拡大
  - －エキストラネットでの採用　　ex. JNX

古河電工　VPN (IPSEC)ソリューション

古河VPN基本コンセプト

古河電工は、実績の高い国産ルータシリーズの開発で培ったノウハウを基盤とし、多拠点リモートアクセスネットワークVPNソリューションをご提供させていただきます。

•IPSecの標準に準拠した自社開発VPN装置と、実績のある他社IPSecコンポーネントとの相互接続性確保により、ネットワーク規模に応じたマルチベンダトータルシステムのご提供

•LAN環境からのダイアルアップVPN接続、フレッツISDN対応など、国内サービスに適合した、安価なセキュリティネットワークの実現に貢献

古河電工VPN対応製品ラインアップ

（センター側）

VPNボックス
古河電工
INFONET－VP100
標準価格498，000円
同時接続：100拠点
登録拠点数：500拠点

（拠点側）

VPNクライアントソフト
古河電工
INFONET－VPN　Client

VPN対応アクセスルータ
古河電工
MUCHO－EV
標準価格98，000円
同時接続：16拠点

PKI対応アクセスルータ
古河電工
MUCHO－EV/PK
標準価格118，000円
同時接続：16拠点

価格

接続拠点数

相互接続性(1)

・NTTコミニュケーションズ主催による第三回IPSce相互接続試験（１９９９．５～６月）にて１５製品中第２位のポイントを獲得

→http://www.secio.bch.ntt.ocn.ne.jp/ipsec/

（MUCHO-EV接続確認機種）

・VPNetテクノロジーズ「VSU1010」	（VPN専用装置）
・インターネット・デバイシーズ（IDI）「FortKnox」	（VPNファイアーウオール）
・タイムステップ「PERMIT/Gate　4520」	（VPN専用装置）
・米IRE「SafeNet/Soft-PK」	（VPNソフトウエア）
・シスコ・システムズ「CISCO1720」	（VPNルータ）
・インテル「VPN Gateway Plus」	(VPN専用装置）
・ノーテル・ネットワークス「Conivity　Extranet　Switch」	（VPN専用装置）
・ラドガード「ClPro-VPN」	（VPN専用装置）
・レッドクリーク・コミュニケーションズ「Ravlin10」	（VPN専用装置）
・スターネット「STAR-Gateware」	（VPN専用装置）
・ウオッチガード・テクノロジーズ「FireBox Ⅱ」	（VPNファイアーウオール）
・アクセント・テクノロジーズ「RaptorFirewall」	（VPNファイアーウオールソフトウエア）
・セキュア・コンピューティング「Sidewinder Security Server」	（VPNファイアーウオールソフトウエア）

相互接続性(2)

・VPN　Interoperability　Workshop
　　期間：January 10-14,2000　　場所：Sandiego

・HATS（高度通信システム相互接続推進会議）　2000年9月

アライドテレシス㈱：CentreCOM AR300V2
NTTコミュニケーションズ㈱：Cisco1750
住友商事㈱：ヤマハRT103i
セイコーインスツルメンツ㈱：試作機（型式未定）
㈱フジクラ：FNX0531
富士通㈱：NetShelter/FW
古河電気工業㈱：INFONET-VP100

とくにPERMIT/GateとMUCHOーEVでは、
(preshared-key)ダイアルアップ
VPN接続を実現

・JNSA相互接続試験　2000年11月～

・JNXベンダー試験　2001年6月～
　　PERMIT/Gate、VPN-1、VSU、MUCHO-EV/PK（PKI)

ICSA認定取得

・INFONET-VP100

ICSAの認定を取得　　国内初！！

旧：International Computer Security Association

→TruSecure Corporation

http://www.icsa.net/html/communities/ipsec/certification/certified_products/index.shtml

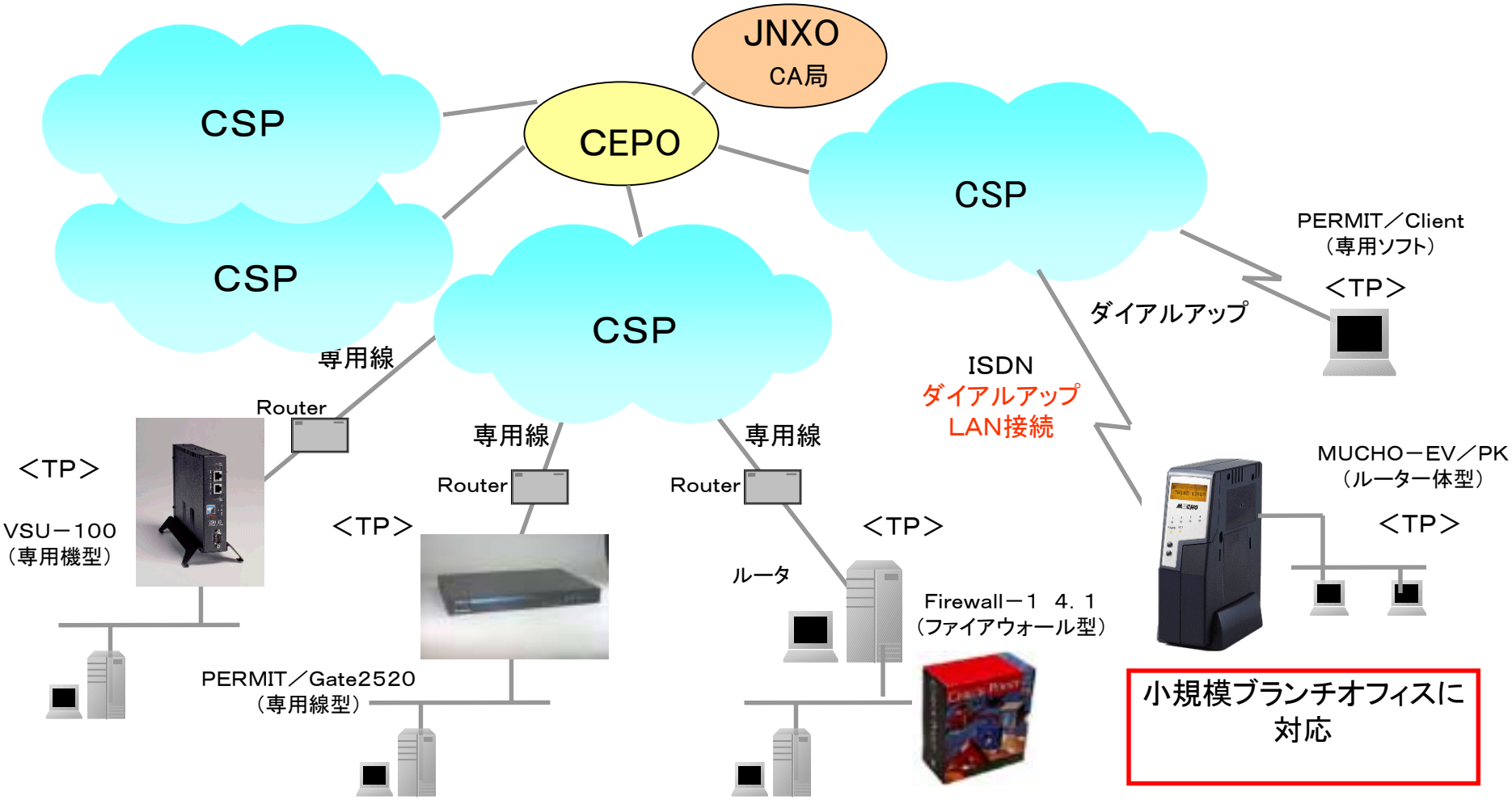
ICSA（International Computer Security Association）は、認証システムやコンピュータ･ウイルス対策、不正アクセス対策など、セキュリティを中心にした調査･研究及び監査サービスを行う米国の企業です。

・MUCHO-EV/PK　認定取得

・VPNクライアントソフト INFONET－VPN　Client

米国**SafeNet,Inc**の**SafeNet/Soft-PK**で取得済み

ＪＮＸ(Japanese Automotive Network eXchange)への取り組み

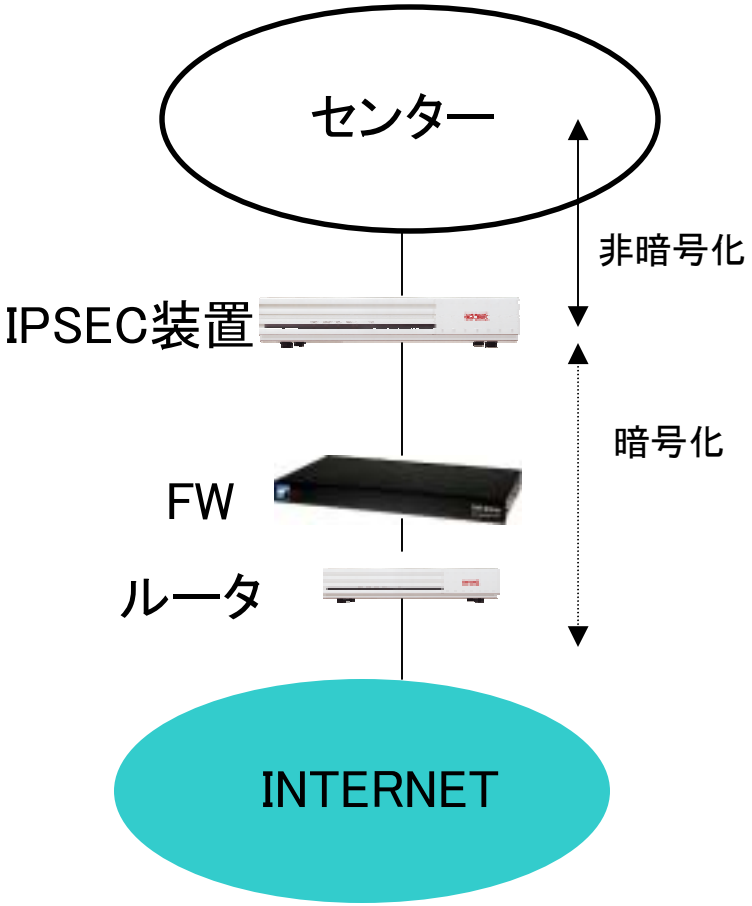


MUCHO-EV/PK JNX認定に向けての状況
今後の予定

項目	日程
JNSA相互接続試験（済み）	2001年3月
JNXベンダー試験	6月末～7月初
CSP持ち込み試験	7月初～7月末
JNXベンダー試験認定	7月31日

VPN (IPSEC)構築時のポイント

Firewallとの併用：直列（1）



・暗号化パケットを通過させる設定がFWに必要

・FWで細かいアクセス制限がかけにくい

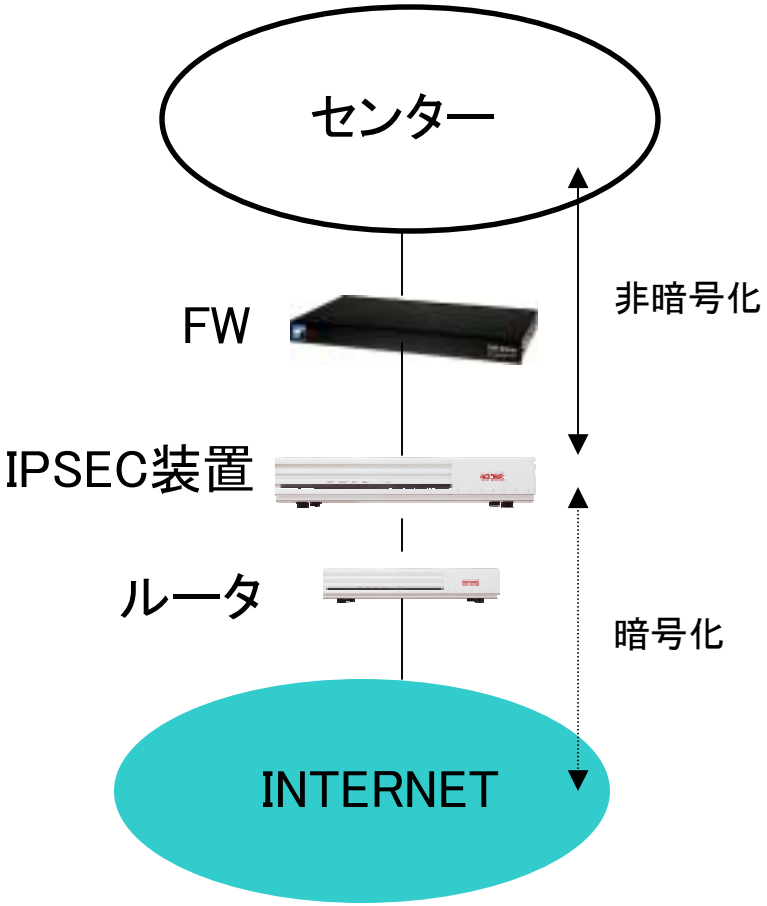
・FWがNATを行う場合
（IPSEC経路上のNAT問題）

main mode		NG
agrresive mode	1対1NAT	OK
agrresive mode	1対多NAT	NG

・IPSEC装置、FWどちらかダウンすると
全通信が停止

「この設置方法は避けたほうが賢明」

Firewallとの併用：直列（2）

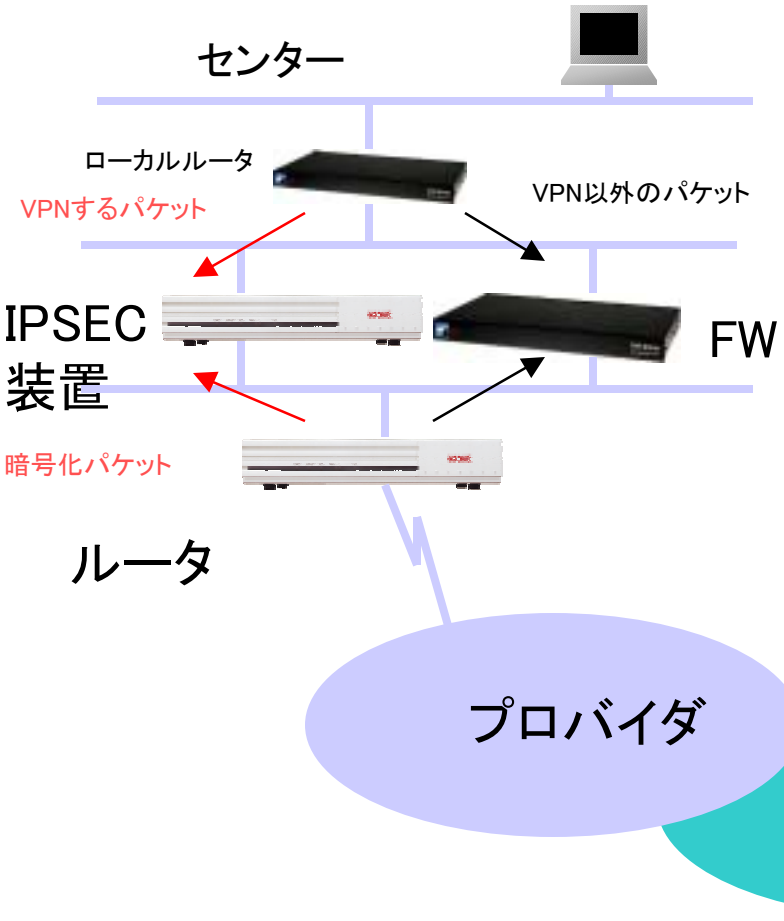


・FWに到達する前にデータは復号化される。
　FWの設定への影響はすくない。

・FWがNAT（1対多）している場合、センターホストのIPアドレスを元にしたセキュリティポリシーの設定がむずかしい。

・IPSEC装置、FWどちらかダウンすると
　全通信が停止

Firewallとの併用：並列



・VPNは、IPSEC装置を経由、その他インターネットアクセスFWを経由

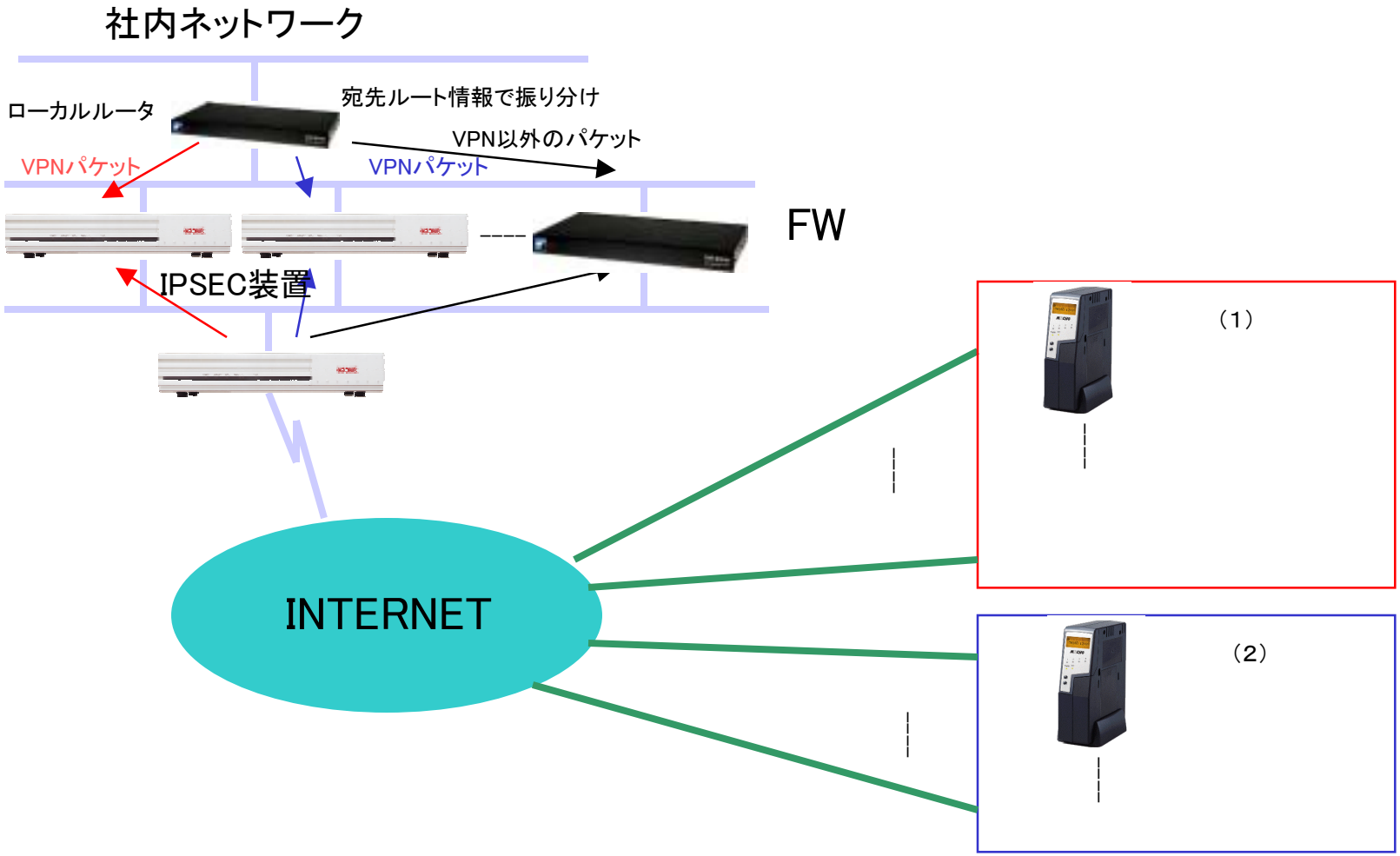
・ルータでの経路制御が必要

・VPN導入時に、FWの設定変更が少ない

「並列形態で導入するユーザが多い」

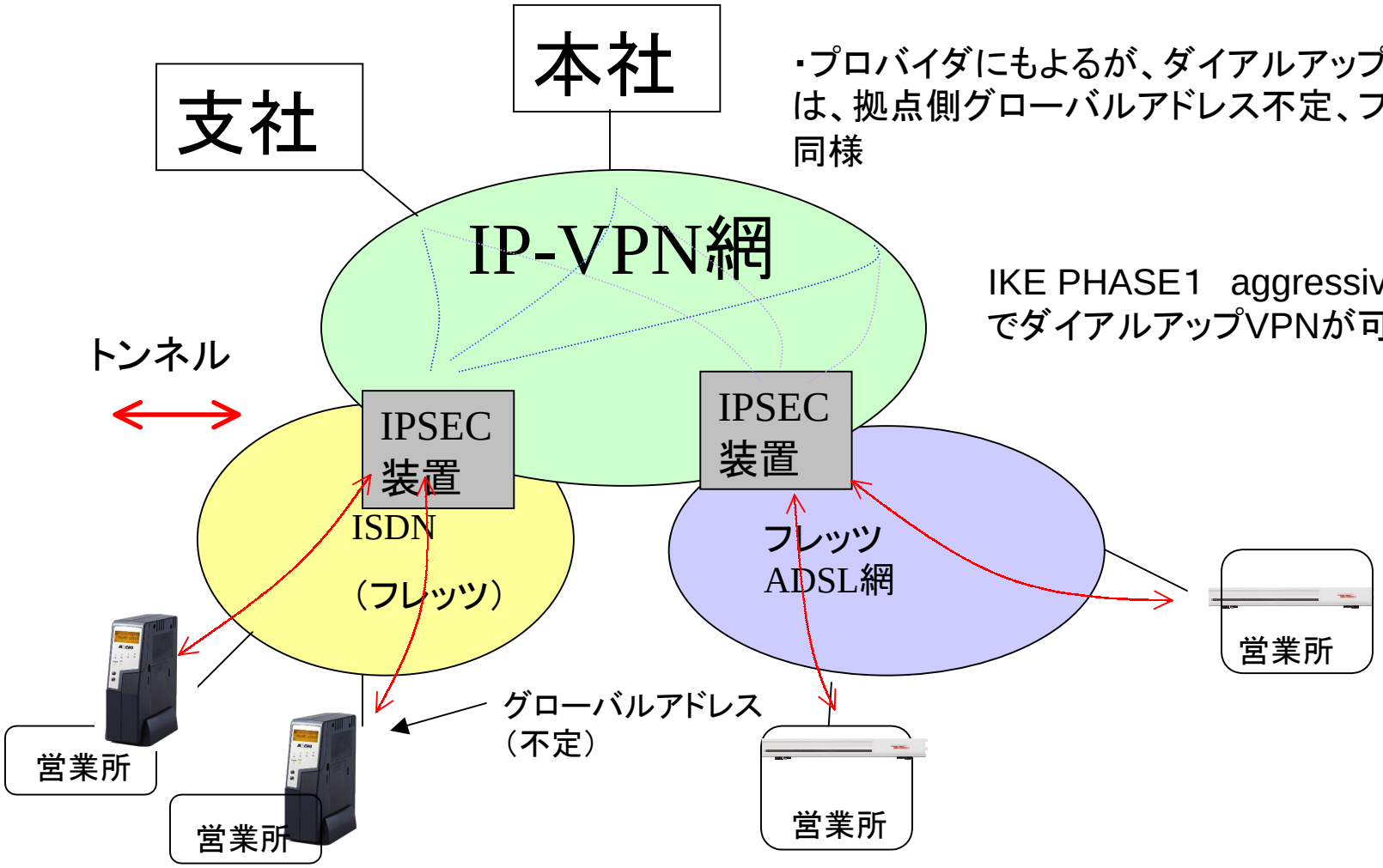
拠点側プライベートアドレスのアグリゲートは必要

Firewallとの併用：並列～VPN帯域拡張～



拠点側プライベートアドレスのアグリゲートは必要

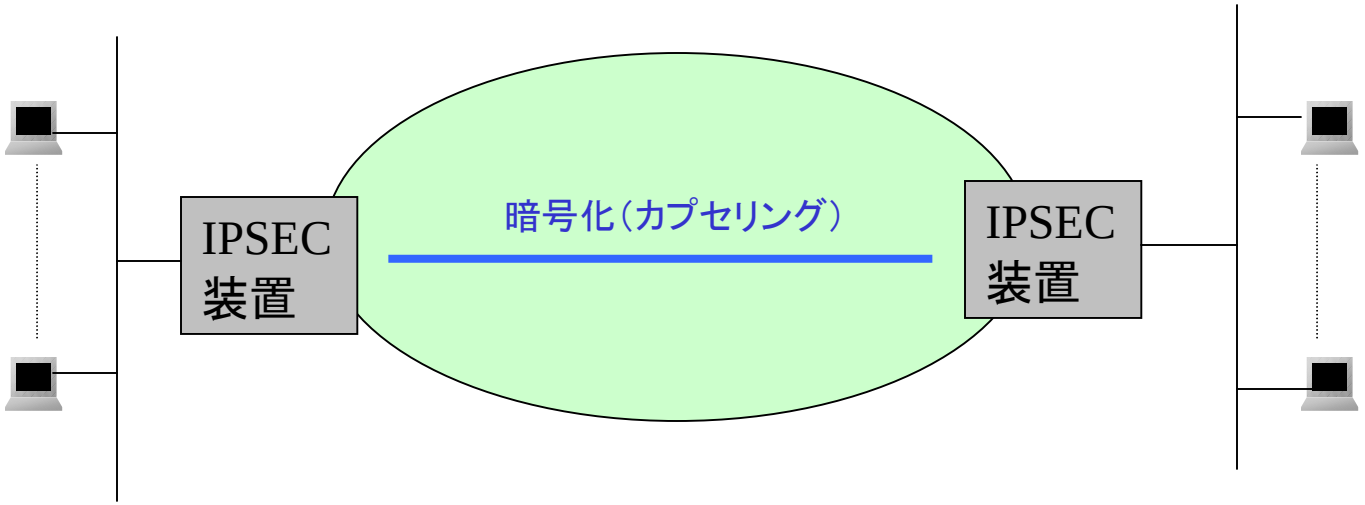
ダイアルアップVPN(IPSEC)



・プロバイダにもよるが、ダイアルアップ（フレッツ含む）は、拠点側グローバルアドレス不定、フレッツADSLも同様

IKE PHASE1　aggressiveモードでダイアルアップVPNが可能

IPSEC　優先制御(QOS)が困難



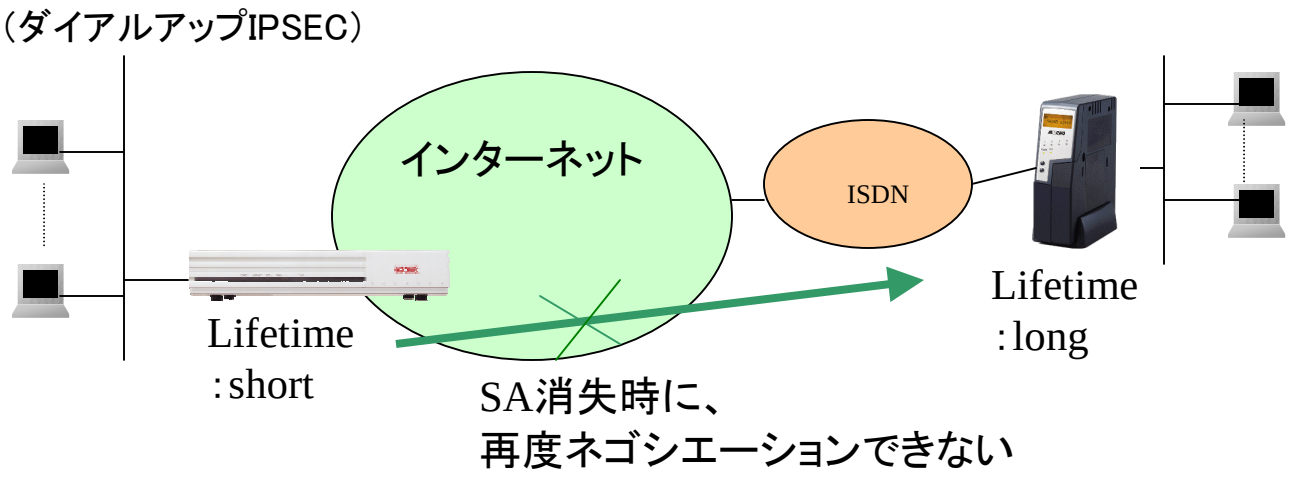
インターネットの問題
・インターネットなど帯域保証がない場合が多い
・途中経路上のルータ、Gateway装置で優先制御が難しい

IPSEC　優先制御を行うには？？
→プロバイダとのSLA確認
→TOSフィールドでの優先制御方式
アプリケーションでのTOSフィールドセット、暗号化処理でのTOSフィールドコピー、経路上での
TOSフィールド優先制御を組み合わせて行う必要がある → （現状では、実現が非常に困難）

IPSEC　SA Lifetimeの設定

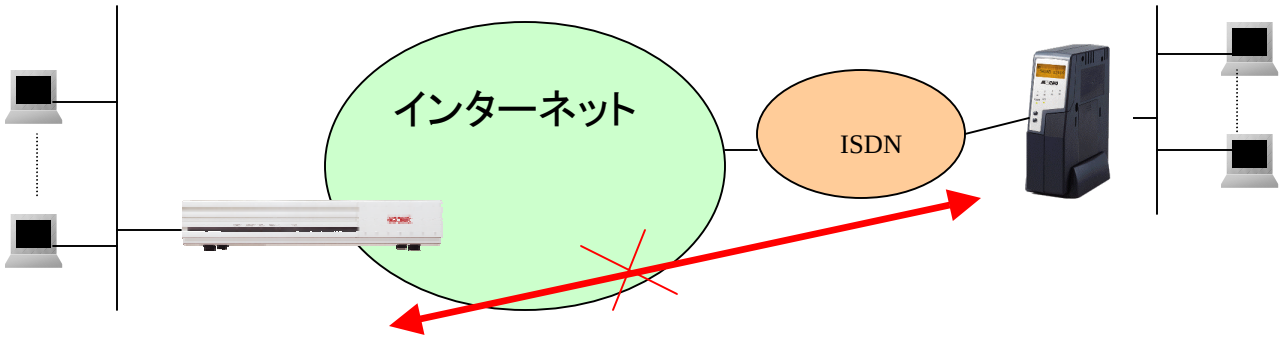
基本的な考え方
　何らかの問題（Ex.リブート）でSA状態不一致が発生。送信元のSAが残った場合には、データ中継できない。

→各ベンダーでそれぞれ対策を講じているが、相互接続の観点からは、？？の状態



「Lifetimeの設定は双方で同じにすることが望ましい」

IPSEC　経路上のフィルタリング



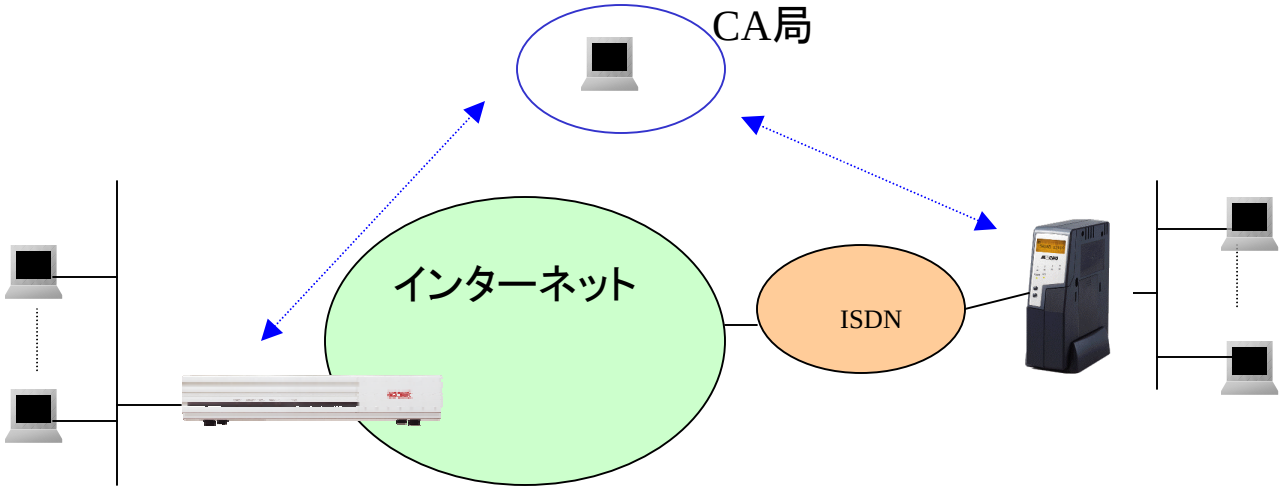
IPSECの経路上、とくにプロバイダでフィルタリングされていないか注意！
事前に申し入れることを推奨

－IPSEC

UDP	500	IKE
IP	ProtNo.50	ESP

－その他、
CA局で使用するプロトコル
ディレクトリサービス(LDAP)
製品毎の管理アプリケーションプロトコルに注意

IPSEC（PKI）でのネットワーク運用保守



IPSEC装置への証明書インストール手順概要

IPSEC装置で秘密鍵、公開鍵を作成→CA局に証明書リクエスト→CA局で証明書発行→IPSEC装置にインストール

「ネットワークの運用保守を検討する際には、CA局との連携、証明書インストールの時間を考慮する必要がある。」