INTERNET WEEK 2002

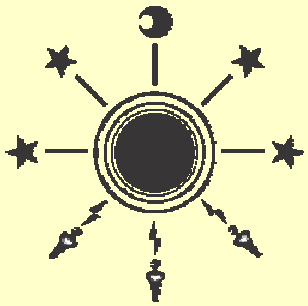
T20 : IPSec～技術概要とセキュアなネットワークの実現手法～

第1部　IPsecの概要

Secure Virtual Private Network

2002/12/20

株式会社ディアイティ
山田　英史



内容

1. SVPNとは
2. IPsecによるSVPNの構築事例
3. IPsecの技術概要

1. SVPNとは

ネットワークに対する脅威と防御法

攻　撃	防御策
不正アクセス	アクセスログ・Firewall・Onetime Password
盗　聴	暗号化
なりすまし	認　証
改ざん	電子署名
ウィルス	ウィルスチェックソフト

SVPN = 通信経路上のデータを守る技術

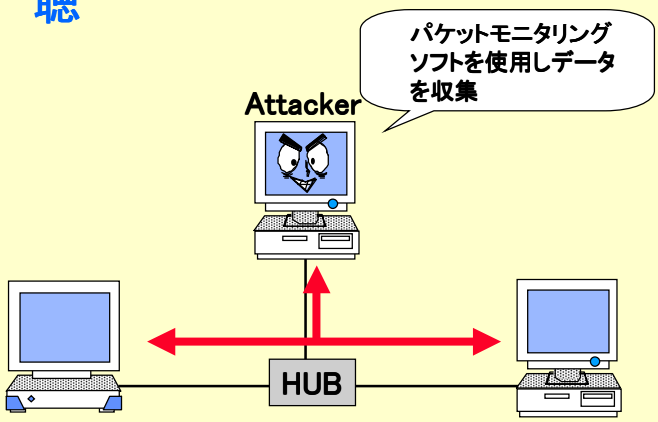
- ファイアウォールは侵入を防御できても、通信経路上のデータは守れません。
- ユーザの手許を離れて通信経路上を飛び交うデータを保護するのがSVPNの役目です。

通信経路上におけるアタック

- 盗　聴
- なりすまし
- 改ざん

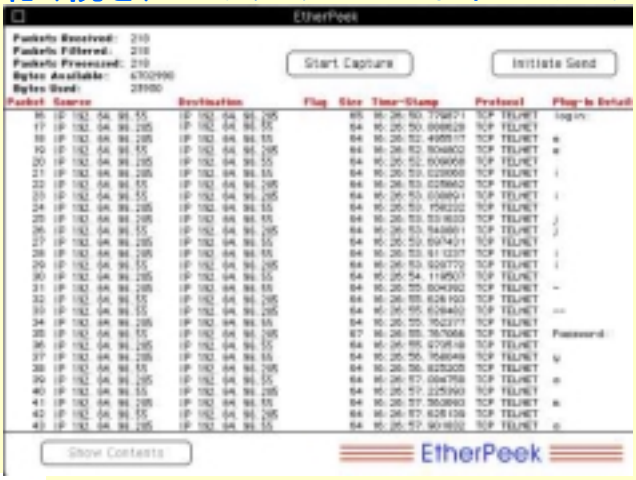
通信経路上におけるアタック（1）

- 盗　聴



通信経路上におけるアタック（1）

- 盗聴（続き）モニタリングソフトで収集したデータ

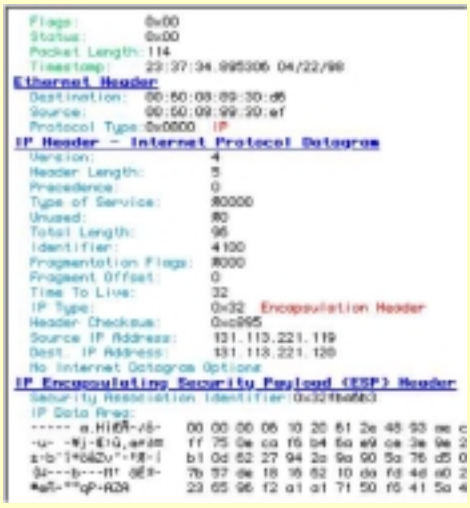


通信経路上におけるアタック（1）

- 盗聴（続き）モニタリングソフトで解析したパケット

暗号化されたデータ

- 暗号化されたパケットのサンプル

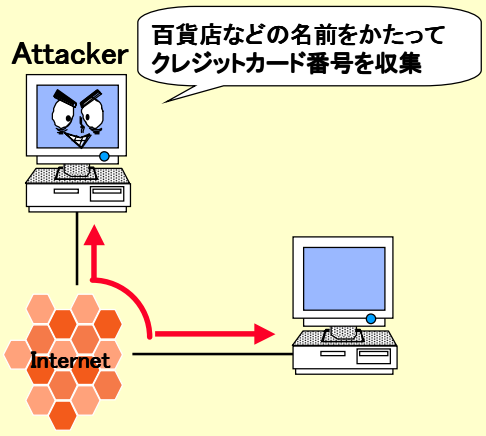


通信経路上におけるアタック(1)

- 盗聴(続き)
  - スニファーソフト、パケットモニタリングソフト、監視ソフト
  - 社内LAN上
  - ISP内の設備上
  - ルーティング設定ミスによる漏洩:社内LAN、ISP

通信経路上におけるアタック(2)

- なりすまし

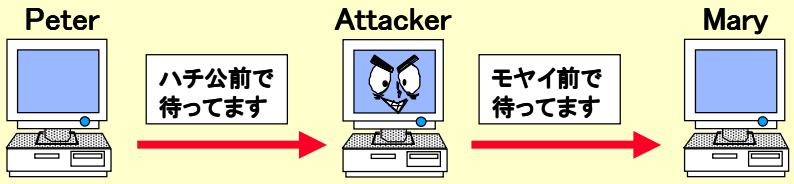


通信経路上におけるアタック(2)

- なりすまし(続き)
  - パソコン通信の架空登録による、アカウント/パスワードの収集
  - 偽った電子メールの送信元

通信経路上におけるアタック(3)

- 改ざん



通信経路上におけるアタック(3)

- 改ざん(続き)
  - 振込先／振込金額の書き替え
  - ブロック暗号では、提携フォームの各項目が予想可能？　金額欄、振込先欄

SVPNの基礎技術

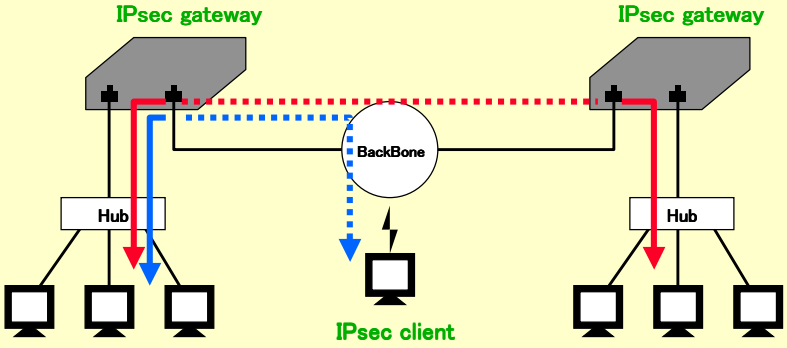
- トンネリング
  - 仮想的な専用経路の構築
- 暗号技術
  - 通信データの秘匿
- 電子署名による認証
  - 身元保証
  - 完全性
- 認証局（PKI）
  - 第三者による身元保証
  - 否認防止

SVPNのニーズ

- コスト削減
  - 専用線　→　安価なインターネットへ
  - 用途別の配線　→　VPNで1本に統括
- 情報の守秘
  - 取引先との電子決済
  - CAD/CAMデータ等製造データ
  - 人事データ、経理データその他
  - 個人データ
    - 銀行・証券の顧客データ
    - 病院の患者データ
    - 行政などの住民データ

2.　IPsecによるSVPNの構築事例

IPsec-VPNの構成



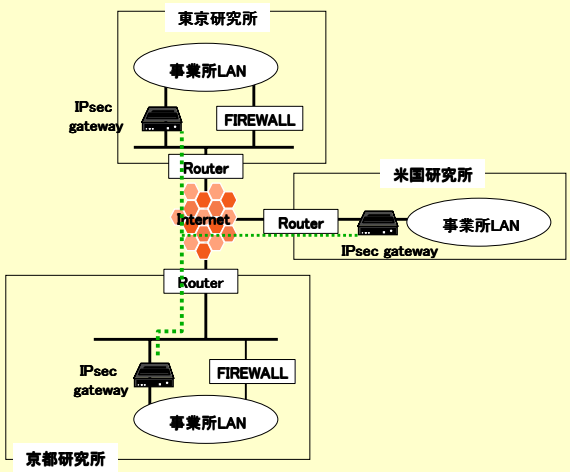
O社海外拠点とのインターネットVPNの事例

システム概要

- 国内と米国の研究所をインターネットで接続。
- 従来の専用線に比較して年間約1500万円の通信費用を削減。
- 同様の事例で弊社が納入した実績のある国は以下の通り。
  - 北米、カナダ、英国、アイルランド、オランダ、フランス、ドイツ、タイ、シンガポール、マレーシア、フィリピン、韓国、香港、台北、韓国、インド(注)、中国(注)

(注)輸出規制有り

構成

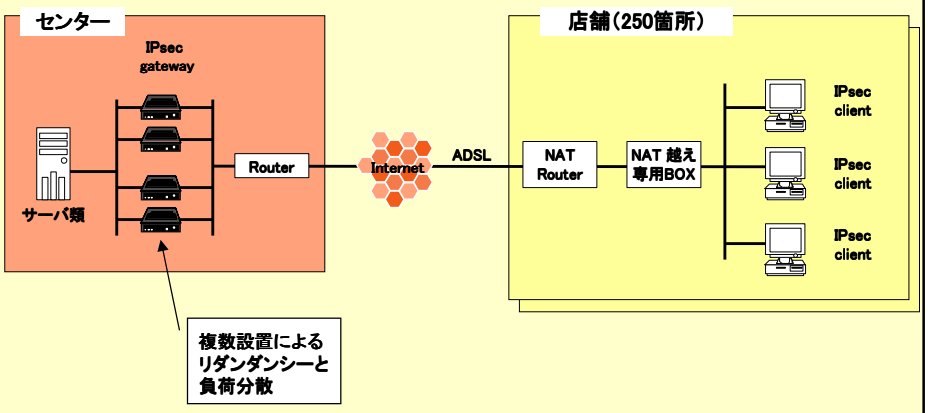


N社直営店ネットワークのVPN事例

概要

- 250店舗の直営店とセンターをインターネットで接続。
- 各店舗にはADSLを敷設し、情報保護のために店舗端末にはIPsec clinetを実装。NATルータを超えるために専用BOX（弊社製品）を設置。
- 店舗からのアクセスを受けるセンター側にはIPsec gatewayを設置しインターネット上の情報を保護。
- 既存のFRからインターネットへ置き換えることで、年間通信費が数千万円削減できる。

構成

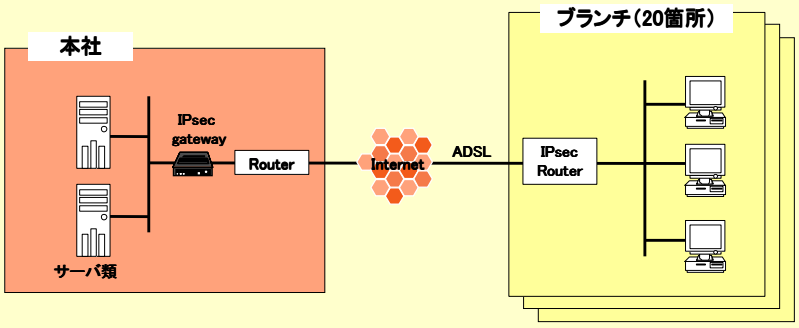


B社ADSLによるリモートオフィスの事例

概要

- 本社と各ブランチ間をインターネット接続。
- 本社側には高パフォーマンスでセキュアトンネル（SA）のキャパの大きいIPsec専用 gatewayを設置し、規模の小さいブランチには安価なIPSecルータを設置。
- ブランチ側はフレッツADSLで接続し、通信コストの削減を狙う。

構成

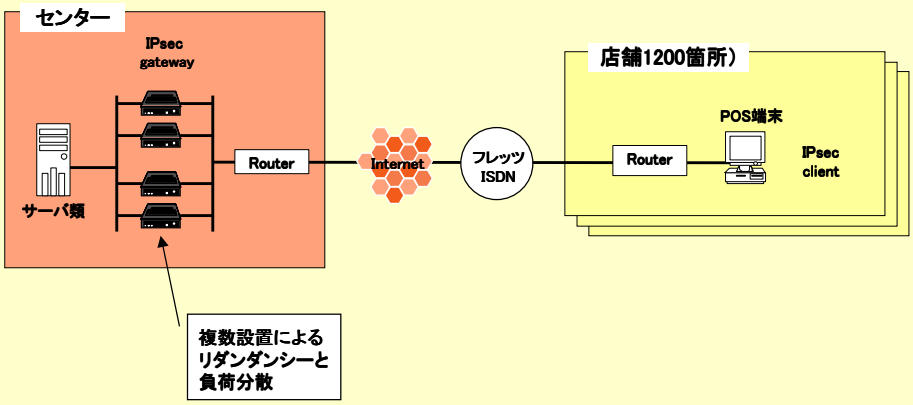


T社POS端末系インターネットVPNの事例

システム概要

- T社の1200店舗に配置するPOS端末にIPsec clientを実装。POS端末がWindowsベースのため、大きな変更無くIPsec clientが適用可能。
- T社の本部にはIPsec gatewayを設置し各店舗からのアクセスを受ける。セキュアなトンネル（SA）の数が多いため、

構成



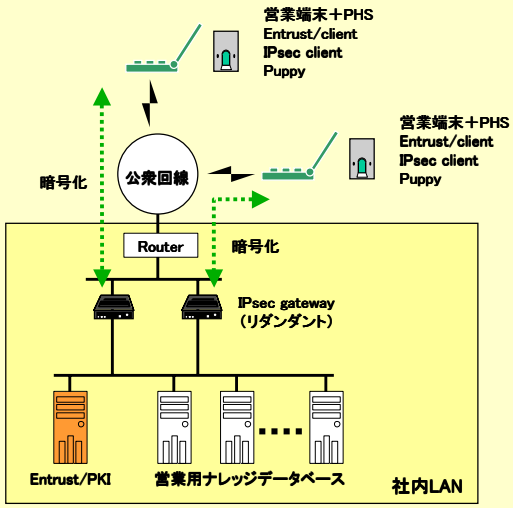
S社モバイルVPNの事例

サービスの目的と特徴

- モバイル環境の有効活用により営業活動のスピード化。
- 開発 ⇔ 営業　相互の情報をリアルタイムに交換。
- 指紋認証とPKIによる高度な認証。
- IPSec-VPNによる通信データの暗号化。

PKI: Public Key Infrastructure

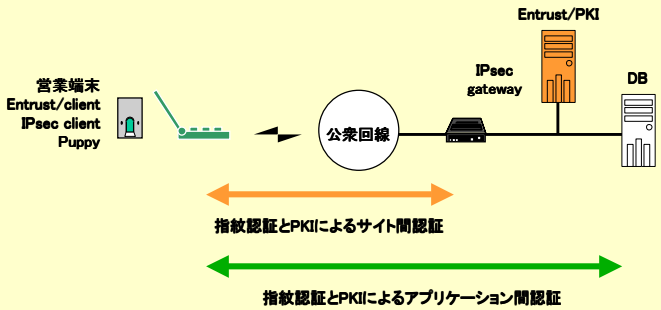
構成



Puppyの特徴

- 指紋認証と電子証明書の併用
- 各種プログラムの提供
  - シングルサインオン
  - アプリケーションの自動起動

多重認証



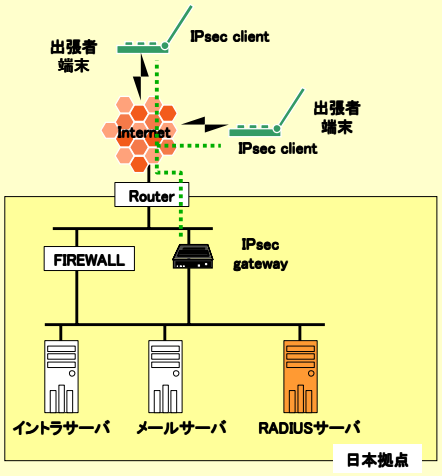
※ アプリケーションの作り方によってはシングルサインオンも可能

S社モバイル環境での社内情報へのアクセス事例

システム概要

- 海外出張者がインターネット経由で、安価に安全に日本社内のイントラサーバにアクセス。
- 社内サーバへアクセスし、メールの利用、スケジュール管理などが可能。
- 日本側のIPsec gatewayから出張者の端末に社内LANのプライベートアドレスを割り振ることで(PAR機能)、出張者はあたかも社内LANに存在するかのように、各種サーバへのアクセスが可能。

構成

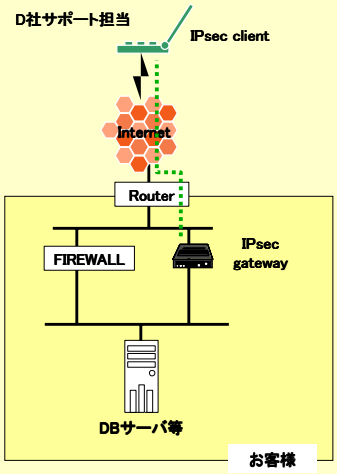


D社リモートメンテナンスの事例

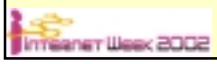
システム概要

- D社がお客様先に納めたシステム（DBなど）を遠隔からメンテナンス。
- お客様先にIPsec gatewayを設置してもらうことで、D社のサポート担当者はどこにいようともインターネット経由で安全にお客様のシステムにリモート接続。
- サポート担当者の移動時間を削減し、メンテナンス費用を低減。

構成



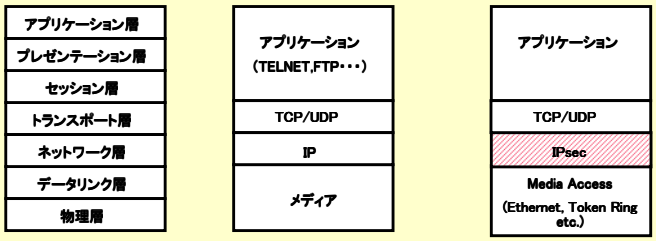
3. IPsecの技術概要



IPsecの基本技術

IPsecの概要

- IPsec(IP Security Protocol)
  - IETF(Internet Engineering Task Force)が標準化をすすめている、IPトラフィックを安全に保つための技術です。
  - 認証ヘッダ(AH)、IPカプセル化(ESP)、鍵の交換と管理の方式(IKE)などの技術です。



OSI参照モデル　IP　IPsec

IPsecに関連するRFC

- Proposed StandardとしてRFC番号が与えられました。
  - RFC 2401: Security Architecture for the Internet Protocol
  - RFC 2402: IP Authentication header
  - RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
  - RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
  - RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV
  - RFC 2406: IP Encapsulating Security Payload (ESP)
  - RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
  - RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
  - RFC 2409: The Internet Key Exchange (IKE)
  - RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec
  - RFC 2411: IP Security Document Roadmap
  - RFC 2412: The OAKLEY Key Determination Protocol
  - RFC 2451: The ESP CBC-Mode Cipher Algorithms
  - RFC 2457: The Use of HMAC-RIPEMD-160-96 with ESP and AH

IPsecに関連するRFC

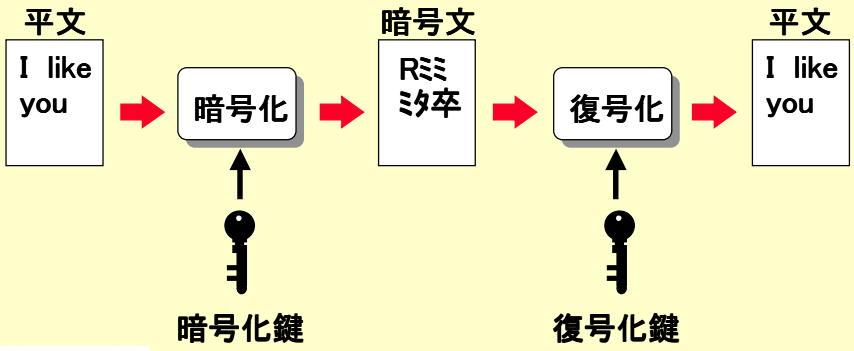
- IP Compressionについて
  - IPsecの技術を応用したもの
    - RFC 2393: IP Payload Compression Protocol (IPComp)
    - RFC 2394: IP Payload Compression Using DEFLATE
    - RFC 2395: IP Payload Compression Using LZS
    - RFC 3051: IP Payload Compression Using ITU-T V.44 Packet Method

IPsecの基本技術

- 暗号技術
- 認証技術
- 鍵交換、管理技術

暗号化技術

- 暗号化の考え方
  - デジタルデータの暗号化技術は純粋に数学の問題。
  - 強度の向上
    - 鍵長の増長、アルゴリズムの強化、定期的な鍵を変更(Re-key)

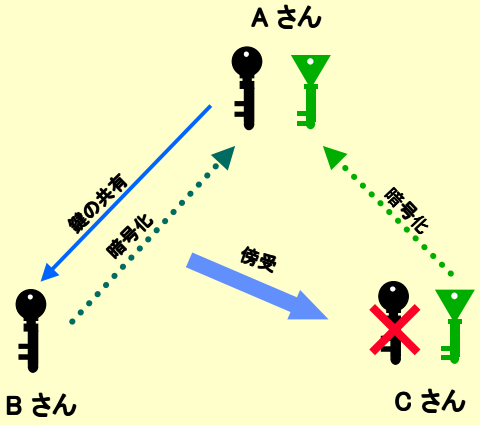


暗号化技術

- 共通鍵暗号方式(対称暗号)
  - 暗号化鍵と復号化鍵が同じ
  - 暗号化処理が高速
  - 通信相手毎に異なった鍵を生成するので、鍵の管理が繁雑
  - 復号化鍵がばれると暗号化鍵もばれる「どうやって相手に届けるか？」
  - DES, 3-DES, RC5, IDEA, FEAL, MISTY

暗号化技術

- 共通鍵暗号方式（対称暗号）

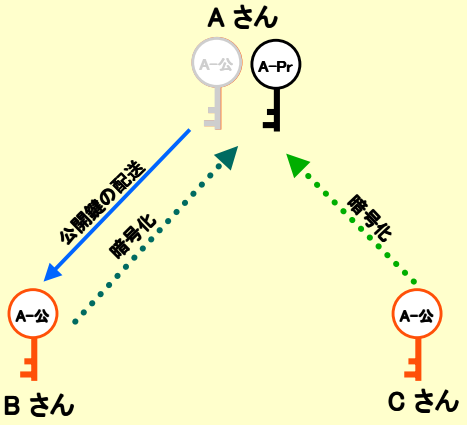


暗号化技術

- 公開鍵暗号方式（非対称暗号）
  - 暗号化鍵と復号化鍵が異なる
  - 自分の所持する非公開の鍵をプライベート鍵、相手に配布する鍵を公開鍵という
  - 公開鍵からプライベート鍵を予測するのは数学的に困難なので配布の方法は気にする必要なし
  - すべての通信相手に同じ鍵（公開鍵）を配布できるので鍵の管理が容易
  - 暗号化と認証（電子署名）の機能を持つ
  - 暗号化処理が遅い
  - RSA

暗号化技術

- 公開鍵暗号方式（非対称暗号）



IPsecで使用する暗号

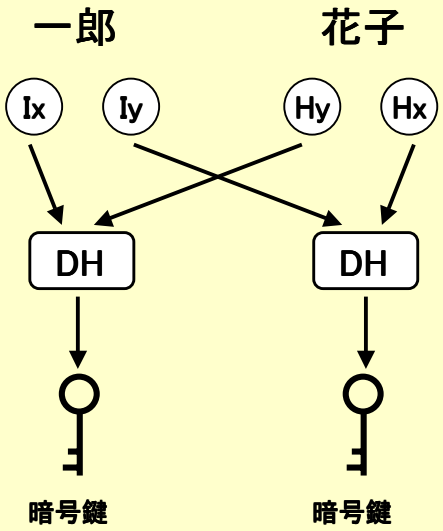
- 標準としては共通鍵暗号方式を使用
  - DES, Triple-DES, AES
- 公開鍵暗号は認証用に使用
  - 公開鍵認証, PKI

IPsecにおける鍵の交換方式： Diffie-Hellman

Ix：一郎の秘密鍵
Iy：一郎の公開鍵

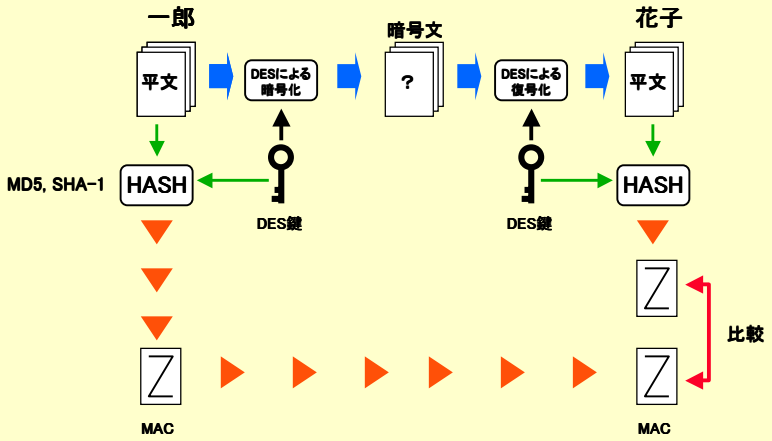
Hx：花子の秘密鍵
Hy：花子の公開鍵

・秘密鍵から公開鍵を導き出す。



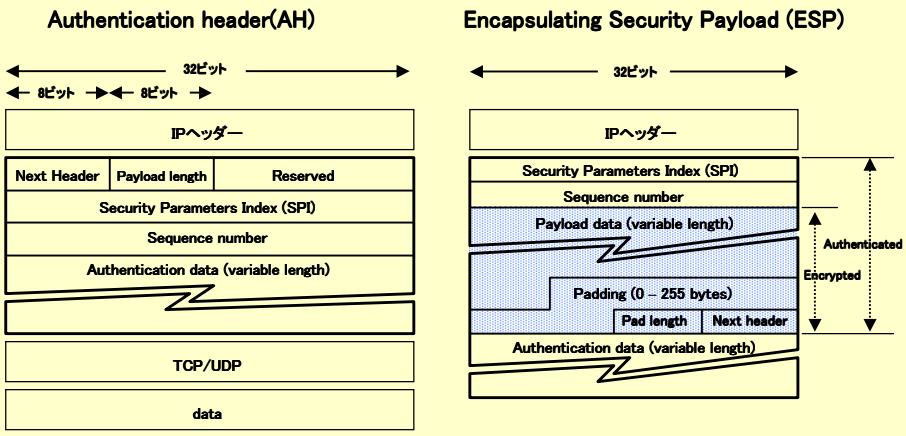
ハッシュによるメッセージ認証

- HMAC（Hash-Message Authentication Code）



送信者の身元確認と改ざんの検出

IPv4におけるIPsecヘッダー



AHとESP

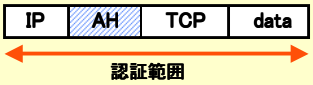
- AH
  - パケットの改ざんの検出
  - 発信元のなりすましの回避
  - リプライ攻撃への対処
- ESP
  - データ部の暗号化
  - IPアドレスの秘匿
  - パケットの改ざんの検出
  - 発信元のなりすましの回避
  - リプライ攻撃への対処

認証範囲

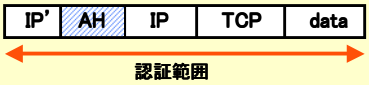
AHとESPの暗号化・認証の範囲

- AH

AH Transport Mode



AH Tunnel Mode



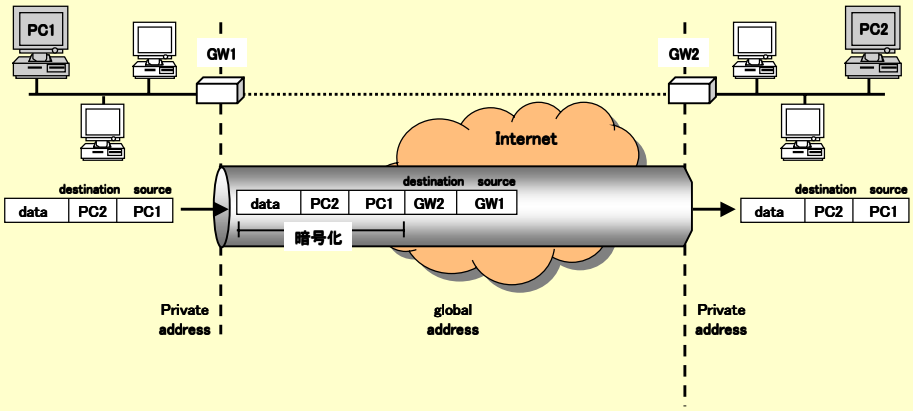
- ESP

ESP Transport Mode

ESP T Tunnel Mode

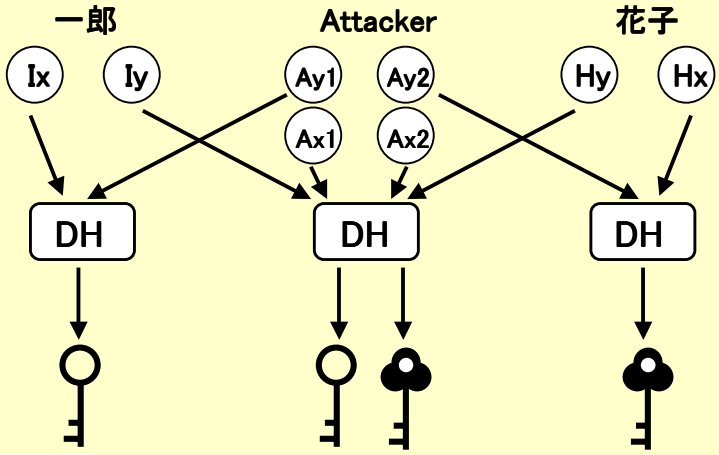
トンネリング

- トンネルモード



身元確認の強化の必要性

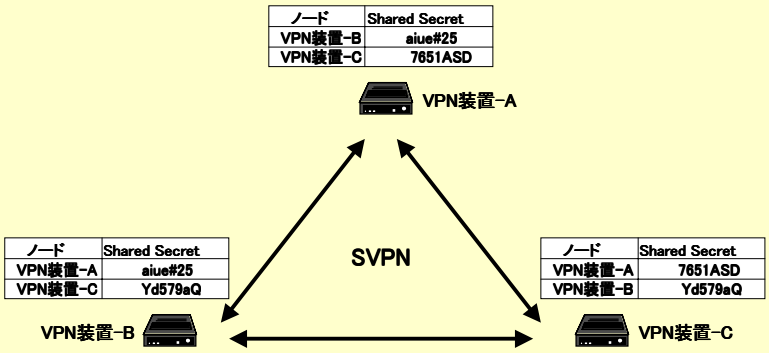
- 鍵情報交換時のなりすまし



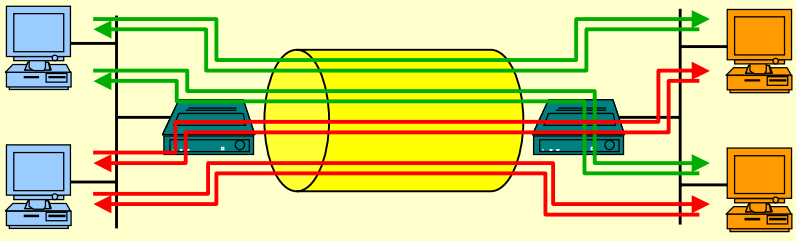
Pre-Sharedによる認証

- Pre-Shared
  - IPsec標準認証機能。
  - ノード同士が秘密を共有（Shared-Secret）し直接認証
    - 設定が容易
    - 分散管理のため大規模VPNには向かない

Pre-Shared



IPsecにおけるSA(Security Association)



Phase 2 SAはプロトコル(AH, ESP)毎に両方向に2本確立。

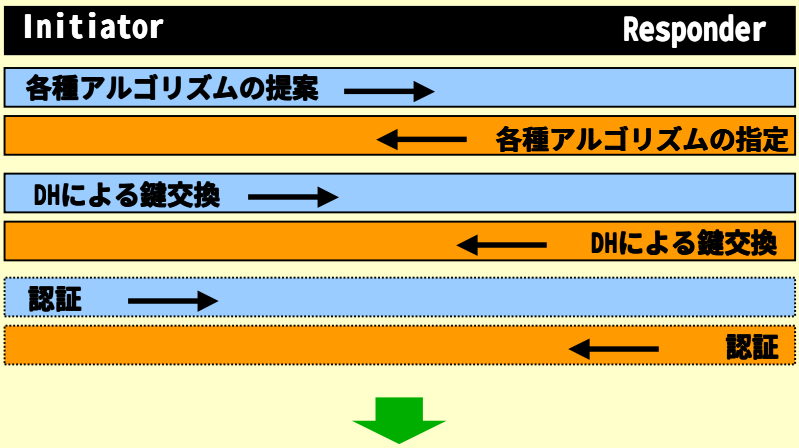
SAとは

- IPsec標準では通信するIPsec製品間でSA(Security Association)というセキュアなトンネルを生成。
- SAは定期的に更新され再構築されます。再認証による身元の確認と暗号鍵の更新(Re-key)による安全性の向上がその目的です。
- SAの再構築にはIKE(Internet Key Exchange)という手順が用いられます。IKEはISAKMP/Oakleyを基にしています。UDP500が割り当てられています。
- IKEには以下のような役割があります。
  - ポリシーやアルゴリズムのネゴ
  - Diffie-Hellmanによる暗号鍵の交換
  - 相互認証
- IKEはPhase 1とPhase 2という段階を経て確立します。

IKE Phase 1

- Phase 1は安全に IKE のコミュニケーションを確立するための手順です。
- Main ModeとAggressive Mode
  - Main Mode
    (1)暗号化アルゴリズムやハッシュアルゴリズム等のネゴ (2)DHによる鍵 (3)情報の交換相互認証
    - 3往復のメッセージ交換で確立
  - Aggressive Mode
    - アルゴリズムなどの提案、DH公開値、身元情報を1メッセージで送信
    - 1.5往復のメッセージ交換で確立
    - リモートアクセスなど、選択オプションが予めわかっている場合に適用
- 認証方式
  - Pre-Shared
  - 公開鍵認証
  - 拡張(RADIUS、PKI ・・・)

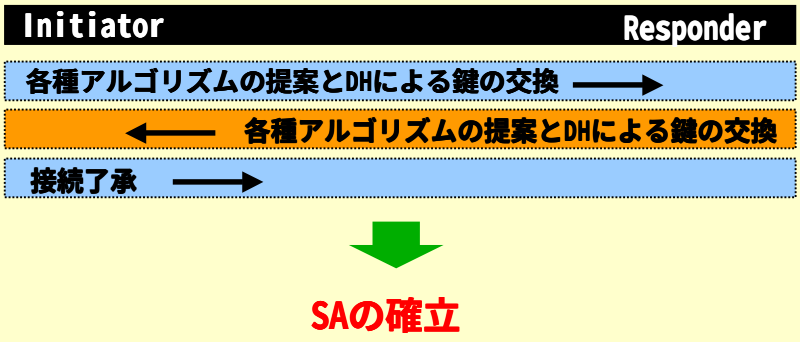
IKE Phase 1のフロー



IKE Phase 2

- IPsecの ESP & AHを確立するための手順です。
- Quick Mode
  - 暗号化アルゴリズムやハッシュアルゴリズム等のネゴと鍵の生成
  - Phase 1(IKE SA)で保護された通信。
- Perfect Forward Secrecy (PFS)のサポート
  - PFS = off: Phase 1で生成した鍵をそのまま利用
  - PFS = on: 再度DHにより新たな鍵の共有を行ない、Phase 1で生成した鍵を廃棄

IKE Phase 2のフロー



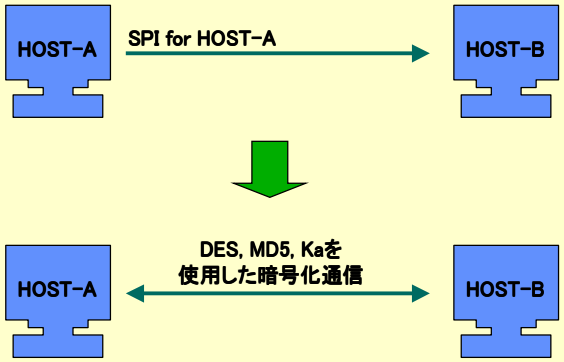
SAとSPI

HOST-AのSAテーブル

送信先	暗号化アルゴリズム	認証アルゴリズム	鍵情報	…
HOST-B	IDEA	MD5	Kb	…
HOST-C	3-DES	SHA	Kc	…
HOST-D	DES	SHA	Kd	…

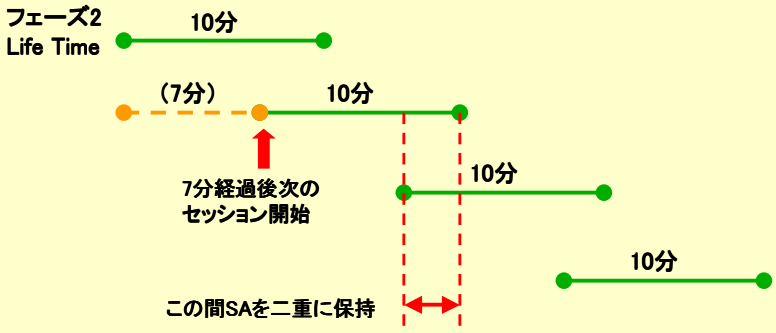
HOST-BのSAテーブル

送信先	暗号化アルゴリズム	認証アルゴリズム	鍵情報	…
HOST-A	DES	MD5	Ka	…
HOST-B	3-DES	SHA	Kc2	…
HOST-C	DES	SHA	Kd2	…



Re-Key

- SAの更新
  - フェーズ1、フェーズ2それぞれにLifeTimeを設定
  - LifeTime： 時間単位、パケット数単位



※フェーズ1はLife Timeの時点でいきなりRe-Key

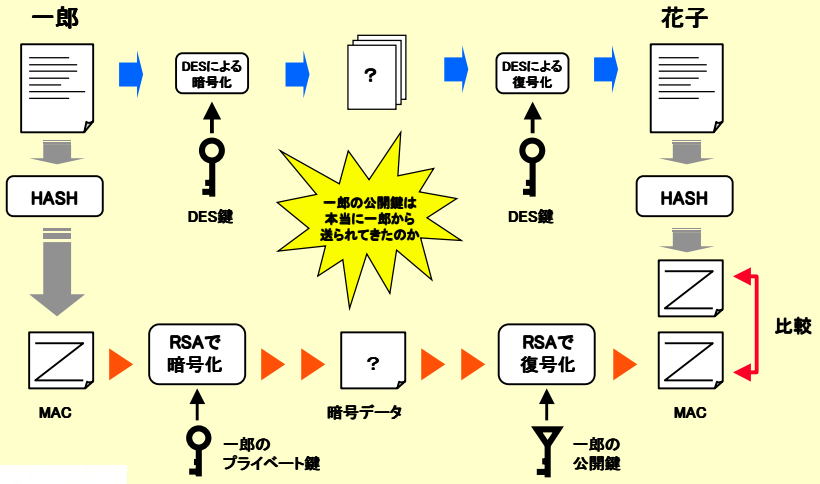
Secure Mapによるルール設定

```
Version 1

begin static-map
        Name"Lab station"
        Target"192.169.211.[1-10]"
        Mode"ISAKMP-Cert"
        ID "CN=yamada,OU=sales,O=dit,C=JAPAN"
end

begin static-map
        Name"Sales Laptop"
        Target"207.181.174.2"
        Mode"ISAKMP-Shared"
end

begin static-map
        Name"Support"
        Target"155.194.204.3"
        Tunnel"192.169.211.14"
        Mode"ISAKMP-Shared"
end
```

IPsecの拡張機能

認証の強化

- RSA電子署名による認証



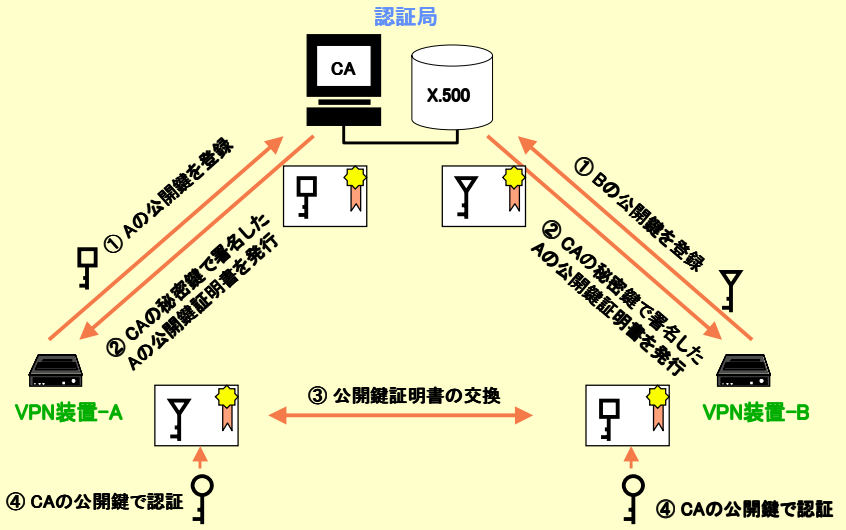
CAの必要性

- 認証サーバ(CAサーバ)による認証
  - CA(Certification Authority:認証機関)
  - 端末が発行する電子署名だけでは認証が不十分:なりすまし・改ざんの危険性
  - 信用がおけ、かつ中立な立場の認証機関を設置。
  - 認証機関から各ユーザへ証明書(RSAなどで署名された)を発行し身元を保証。
    - RSA電子署名、X.509公開鍵証明書による強力な認証。
    - 第三者(CA)による確かな身元保証。
    - 集中管理。大規模VPN向き。
  - PKI(Public Key Infrastructure)として標準化中

X.509証明書

- ISO/IEC DIS9594-8 X.509
- 証明書の管理・配布の標準的な構造について定義されています。
  - 以下の様な情報を含みます。
    - ユーザID
    - ユーザIPアドレス
    - 証明書の発行日
    - 証明書の期限
    - ユーザの公開鍵
    - CAの電子署名
    - 証明書のシリアル番号
    - CAのIPアドレス
    - CAの認証シリアル番号
    - 認証機構のバージョン
    - 各アルゴリズム(ハッシュや電子署名)のバージョン

PKIによる認証

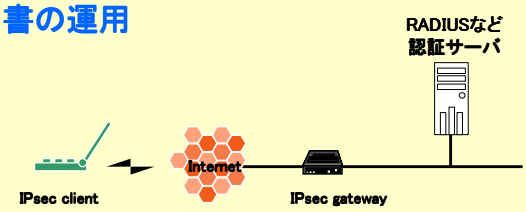


PKIによる認証

- PKIサポート
  - 標準的なPKIに対応
    - Verisign, Entrust、BALTIMORE、SSH、Netscape
    - PKCS 10/7 オフライン認証 (gateway)
    - PKCS 12 認証、プライベート鍵の組み込みと管理 (client)
    - SCEP (Simple Certificate Enrolment Protocol) : Webベースの証明書要求プロトコル

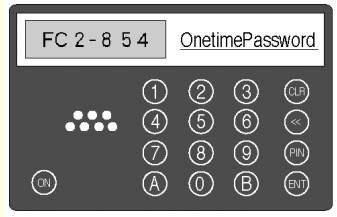
その他 認証機能の拡張

- Hibrid Auth / XAuth
  - 拡張されたIKE認証
  - PKIより安価で簡易、PKIに至る前段階
  - リモートアクセスに適する
    - RADIUS認証による個人認証とアクセス制御
      - ACE/SecurID, SafeWord, NT Domain, …のサポート
    - 容易な証明書の運用



個人認証デバイス

- ワンタイムパスワード
- ICカード
- i-key
- バイオメトリックス



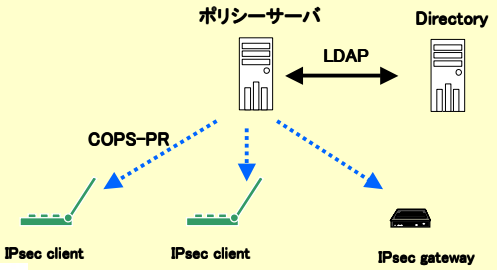
ワンタイムパスワード

i-key

PUPPY（指紋認証）

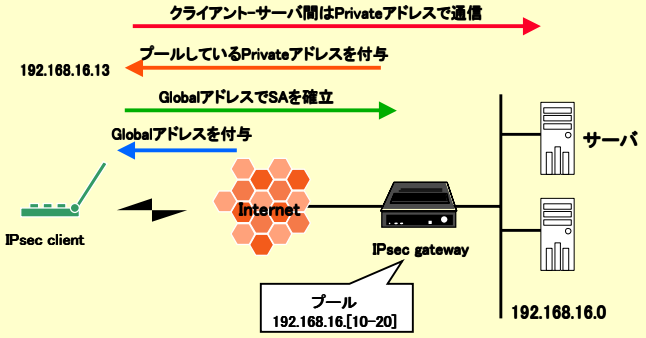
ポリシー管理機能の拡張

- ポリシー サーバの運用
  - SSP(Security Policy Protocol): 接続先Gateの発見とセキュリティポリシーの取得
  - IPsecデバイス側: IPsec PIB(Policy Information Language)の実装
  - ポリシーサーバ側: COPS-PR(Common Open Policy Service Protocol and Support of policy provisioning)の実装



アドレス管理機能の拡張

- ダイナミックリモート管理
  - IKE Configuration
  - Private address request (PAR)

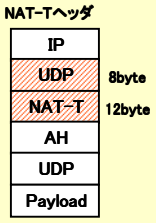


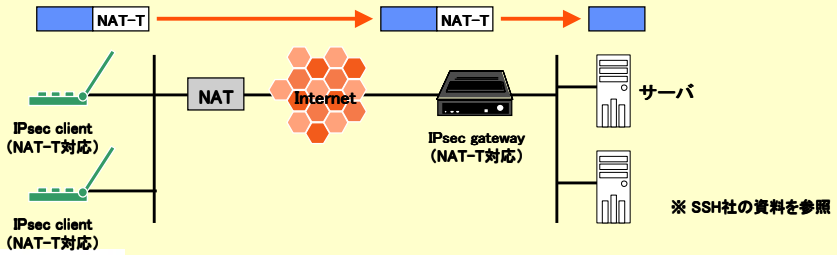
アドレス管理機能の拡張

- ISAKMP-Config
  - リモート端末に対し、社内アドレスの割り当て、ネットマスク、内部DNSサーバアドレスなどを知らせる
- IPsec-DHCP
  - 社内DHCPサーバから社内アドレスの割り当て

トンネル技術の拡張

- NAT Traversal（NATを超える取り組み）
  - IKEによるネゴ
    1. 対向でNAT Traversalを持つかの確認
    2. NAT Traversalでカプセリング
    3. ハートビートでとらフィックを維持
    4. 相互でプライベートアドレスの重複も回避





他のVPN技術とIPsecの比較

各種VPNの比較 （一部はデータ暗号技術）

	L2TP	IPSec	MPLS	SSL
実装レイヤ	レイヤ2	レイヤ3	レイヤ2,3	レイヤ4,5
対応プロトコル	マルチプロトコル	IP	マルチプロトコル	HTTP、FTP 等
適用範囲	End to End	End to End	キャリア網内	End to End
認証機能	あり	あり	なし	あり
暗号機能	オプション	あり	なし	あり
VPN機能	トンネリング +認証	トンネリング +認証 +暗号化	ラベルによる 認証 トラフィックの 分離	+暗号化

L2TP : Layer 2 Tunneling Protocol
IPSec : IP Security Protocol
MPLS : Multi-Protocol Label Switching
SSL : Secure Sockets Layer

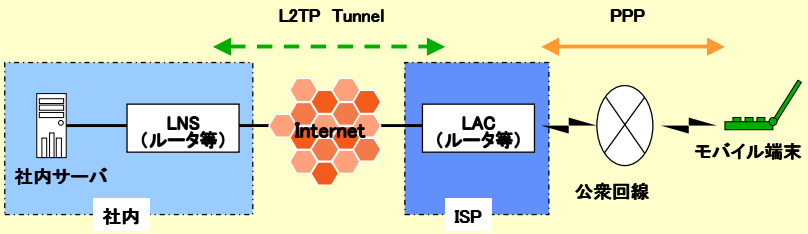
IPsecが普及した理由

- 通信データの暗号化、送受信相互の認証といったセキュリティ機能が標準実装
- 企業ネットワークが内外ともIP系で設計されることが多くIPのみに対応していれば十分である
- 専用ゲートウェイ、ルータ、ファイアウォール、クライアントソフトといった様々な製品バリエーションがあり使用目的や予算に合わせて製品が選択できる
- キャリアを選ばない
- 異機種間相互接続が可能

L2TPによるVPN

- L2TP（ Layer 2 Tunneling Protocol）
  - PPTPとL2Fの統合
  - IETF RFC2661
  - マルチプロトコル対応
  - PPPの拡張機能
  - リモート端末 – LAN間
  - コネクション型トンネリング プロトコル
  - 暗号機能はオプション
  - パケット形態が若干複雑

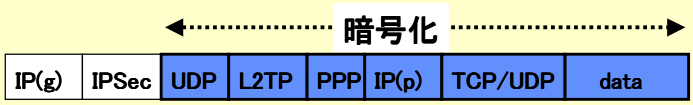
L2TPによるVPNの構成



- LAC（L2TP Access Concentrator）
  - モバイル端末からアクセスを受ける装置。一般的にはISP内に設置されるリモートルータ（アクセスサーバ）がLAC機能を実装。
- LNS（L2TP Network Server）
  - LACとの間にL2TPトンネルを確立する装置。受信したL2TPカプセルを解きアクセスサーバとしてPPPの確立を行なう。

L2TPのパケット構造

- Windows 2000のL2TP
  - LAC機能とL2TPクライアント機能
  - IPSecとの併用による暗号機能の実現

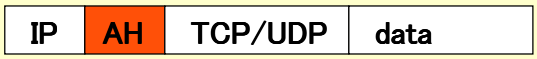


L2TP over IPSec

IPSecのパケット構造

- AHとESP

Authentication header(AH)
AHは認証機能のみ



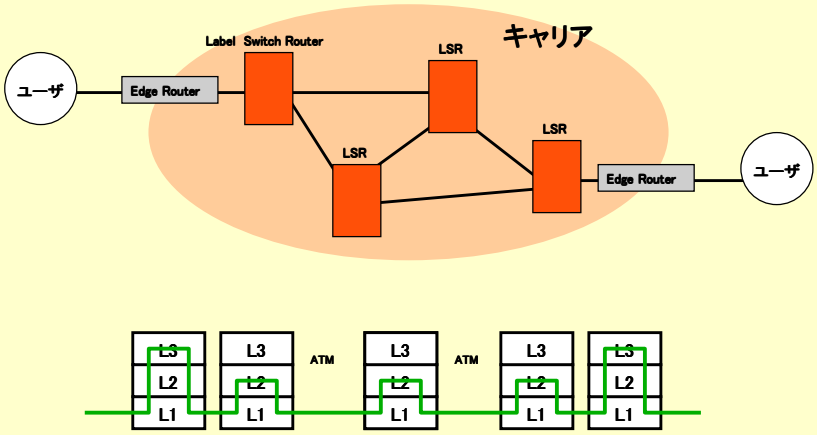
Encapsulating Security Payload (ESP)
ESPは認証機能と暗号機能を実装

※上図AH,ESPともトランスポートモードの場合

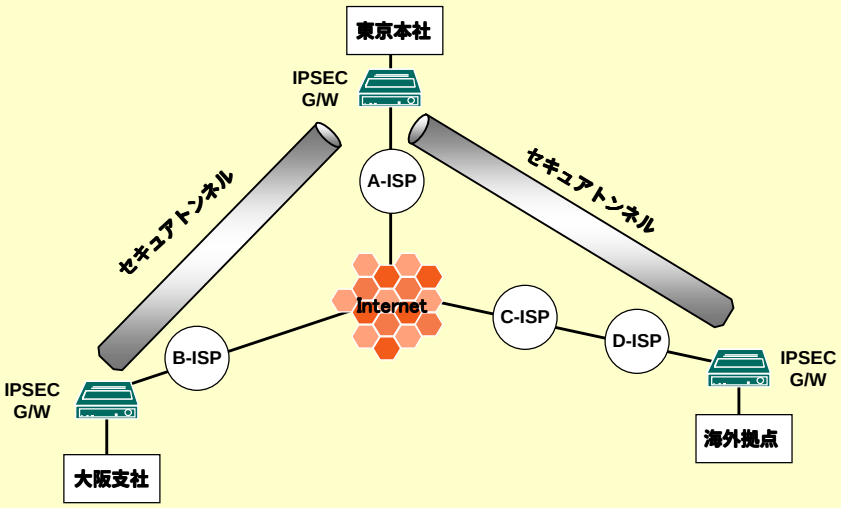
MPLSによるVPN

- MPLS(Multi-Protocol Label Switching)
  - キャリアのIP-VPNサービスで使用
  - レイヤ3のルーティングとレイヤ2のスイッチングの統合
  - マルチプロトコル
  - キャリア網内(交換機間)に適用
  - ラベルによるトラフィックの分離
  - 高品質なサービス
    - レイヤ3ルーティングのオーバヘッドを軽減
    - QoS

MPLSによるVPNの構成



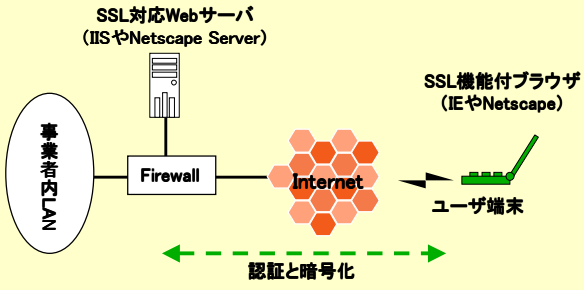
IPsecのEnd to End トンネリング



SSLによるVPN

- SSL（Secure Sockets Layer）
  - HTTP、TELNET、SMTP、FTP等特定のアプリケーションの安全性
  - IETF RFC 2246
  - End to Endの認証機能、暗号機能
  - Webブラウザ等に標準装備
  - BtoCで普及
  - UDPは扱えない

SSLによるVPNの構成

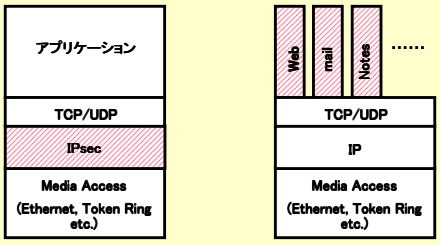


その他アプリケーションレベルのVPN

- PGP、SMIME
  - メールの暗号化、認証機能
  - PGPはフリーソフトとして普及
- SSH セキュアシェル
  - TELNET、FTPなどリモートコマンドベースの通信を暗号化
  - フリーソフトとして普及したが市販版により企業向けの展開

SSLとIPsecの比較

- アプリケーションレベルとIPSecの比較
  - PGP・SSLはアプリケーションに実装
    - 適用サービスが限定される
    - サーバ側の作りこみが必要
  - SSLとIPSecの共存
    - インフラはIPSecで保護、サービスのセキュリティをSSLで向上



IPSEC　　PGP, SSLなど

付録

主なIPsec製品一覧

カテゴリ	メーカ	製品
専用gateway	Alcatel	Alcatel SecureVPN シリーズ
	AVAYA	VPN wareシリーズ
	Nokia	IPシリーズ
	Notel Networks	Contivity Extranet Switch
ファイアウォール	Checkpoint	VPN-1
	NetScreen	NetScreenシリーズ
	Symantec	Symantec Gateway Security
	WatchGuard	FIREBOX VCLASS
ルータ	Allied Telesis	CentreCOM AR740 他
	Cisco	VPNシリーズ
	古河電工	MUCHOシリーズ、FITELnetシリーズ
	ヤマハ	RTシリーズ
OS	Microsoft	Windows 2000, XP
		KAME for BSD UNIX
		S-WAN for Linux

参考文献

Internet Week 2000 セミナー資料
IPsecによるVPN構築
ネットワンシステムズ(株)　白橋　明弘 著

マスタリング IPsec
馬場　達也 著
オライリー・ジャパン

ネットワークセキュリティ
チャーリー・カウフマン、ラディア・パールマン、マイク・スペシナー　著
石橋　啓一郎、菊池　浩明、松井　彩、土井　裕介　訳
株式会社プレンティスホール出版

ポイント図解式　VPN/VLAN教科書
是友　春樹　監修
マルチメディア通信研究会
アスキー出版局

IPsec導入の手引き
Elizabeth Kaufman, Andrew Newman 著
SE編集部　訳
笠野　英松　監修
翔泳社

オープンデザイン　1996年6月号
特集　最新の暗号技術によるセキュリティの実現
CQ出版社

日経コミュニケーションズ　1998年6月15日号
検証テクノロジ IPSEC　インターネットVPNの基本技術 既設機器との相互運用が課題

IPSec～技術概要とセキュアなネットワークの実現手法～

第1部 おわり

株式会社ディアイティ
山田　英史
eiji@dit.co.jp