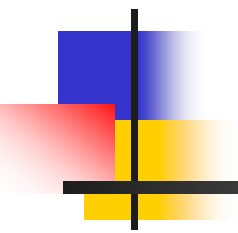
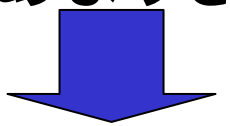


マスタリングIPSEC

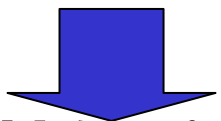
00J139　**柳沢信成**

IPSECの歴史

- インターネットは、歴史上の理由からセキュリティに対する考慮があまりされてこなかった



- インターネットをビジネスで使う場合には、セキュリティの弱さが非常に大きな問題



- インターネットの基盤プロトコル(IP)にセキュリティ機能を持たせることにより、インターネット上を流れるデータを保護する必要性がある

IPSECの歴史

- 1992年　IETF(Internet Engineering Task Force)ミーティングでIPにセキュリティを追加するIPSECについて議論を行うIPSEC BOFが発足
- 1993年　正式なWG (Working Group)と認められ、IPSEC WG本格的な活動
- 1995年8月　IPSECバージョン1の仕様公開
- 1998年11月　自動鍵管理プロトコルの使用と更なる機能を盛り込んだIPSECバージョン2の仕様を公開

IPSECの特徴

- ネットワーク上のデータの機密性を確保することが可能
- ネットワーク上のデータの完全性を確保することが可能
- データの送信元を認証することが可能
- IPSECは標準プロトコルである
- 約束された将来性
- アルゴリズム選択の柔軟性
- IPによる通信を全て保護することが可能
- VPNを構築することが可能
- エンドユーザに透過的である

鍵管理プロトコル

- IKE (Internet Key Exchange)
  - IPSEC**で用いるインターネット標準の鍵交換プロトコル。**ISAKMP(Internet Security Association and Key Management Protocol)**に基づいて，モードと呼ばれる各鍵交換方法を規定したOakleyを使用するプロトコル。**

暗号アルゴリズム

- **現在は、米国の連邦情報処理標準規格となっている**DES（Data Encryption Standard)**や**3DES(Triple DES)**が主流**

- **今後は**AES（Advanced Encryption Standard)**が主流になると考えられている**

暗号アルゴリズム

- DES(Data Encryption Standard)
  - **一番広く利用されている方式**
  - **６４ビットブロックで動作するブロック暗号であり、６４ビットの固定長鍵を使用している（実際は、８ビットに１ビットのパリティビットを含んでいるので、鍵の実行長は56ビット）**
- 3DES (Triple DES)
  - **DESでは強度が不十分として生まれた**
  - **DESの処理を３回繰り返すことによって安全性を高めた**
  - **実用上解読不可能と言われているが，方式上処理がかなり重くなる。**

暗号アルゴリズム

- AES (Advanced Encryption Standard)
  - **ＤＥＳが開発されてから20年以上経過し、56ビットの鍵を使用するＤＥＳでは、セキュリティを保つのが不十分だとして生まれた**
  - **128ビットブロックを動作するブロック暗号で、128ビット、192ビット、256ビットの長さの鍵を使用する。**

認証アルゴリズム

- **代表的なものには**
  - MD5(Message Digest Five)
  - SHA-1(Secure Hash Algorithm)

  がある

認証アルゴリズム

- MD5(Message Digest Five)
  - **暗号アルゴリズムの一つで，アルゴリズムの簡潔さ，安全性，速度を重視している。** 128**ビットの固定長鍵をサポート。**128bits**の認証様データを生成。**
- SHA-1(Secure Hash Algorithm)
  - MD5**とほぼ同じアルゴリズム。より安全性に優れるが，**MD5**より処理が重くなる。** 160**ビットの固定長鍵をサポート。**160bits**の認証様データを生成。**

セキュリティプロトコル

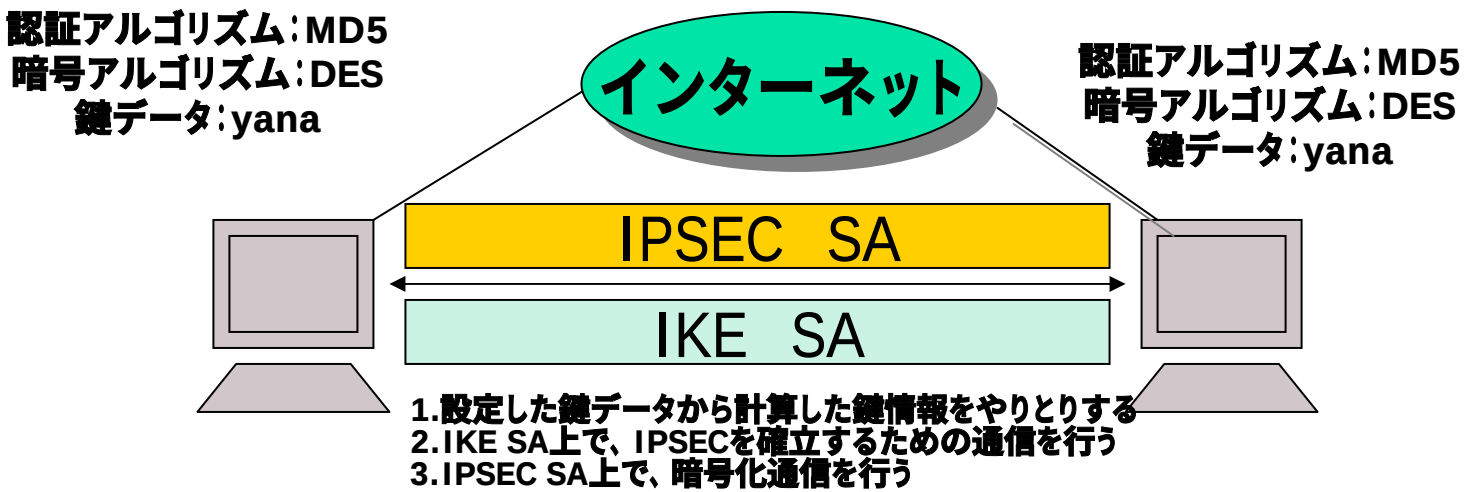
- AH(Authentication Header)
  - **発信元の認証、データの完全性（改ざんされていないこと）認証、リプレイ・アタックの阻止などの機能を提供する。**
- ESP(Encapsulation Security Payload)
  - **AHの機能に加えてデータの暗号化機能を提供する**

SA(Security Association)

- IPSEC通信を行うために，通信相手（ピア）との間でSAと呼ばれる論理的なコネクションを確立する
- SAはVPN通信を行うトラフィック毎に確立され，トラフィック情報と，暗号アルゴリズム，認証アルゴリズム等のトラフィックに適用するセキュリティ情報を含んでいる。従ってSAを確立した後，ルータはSAの情報に基づいてVPN通信処理を行う。自動鍵管理プロトコルを使用した場合，対象パケットデータ受信を契機に自動的にピアとネゴシエーションを行って鍵を交換し，SAを確立する。

SAの流れ

1. IKE SAの確立（鍵交換用のトンネル）
2. IPSEC SAの確立（データ通信用のトンネル）
3. **暗号化通信**

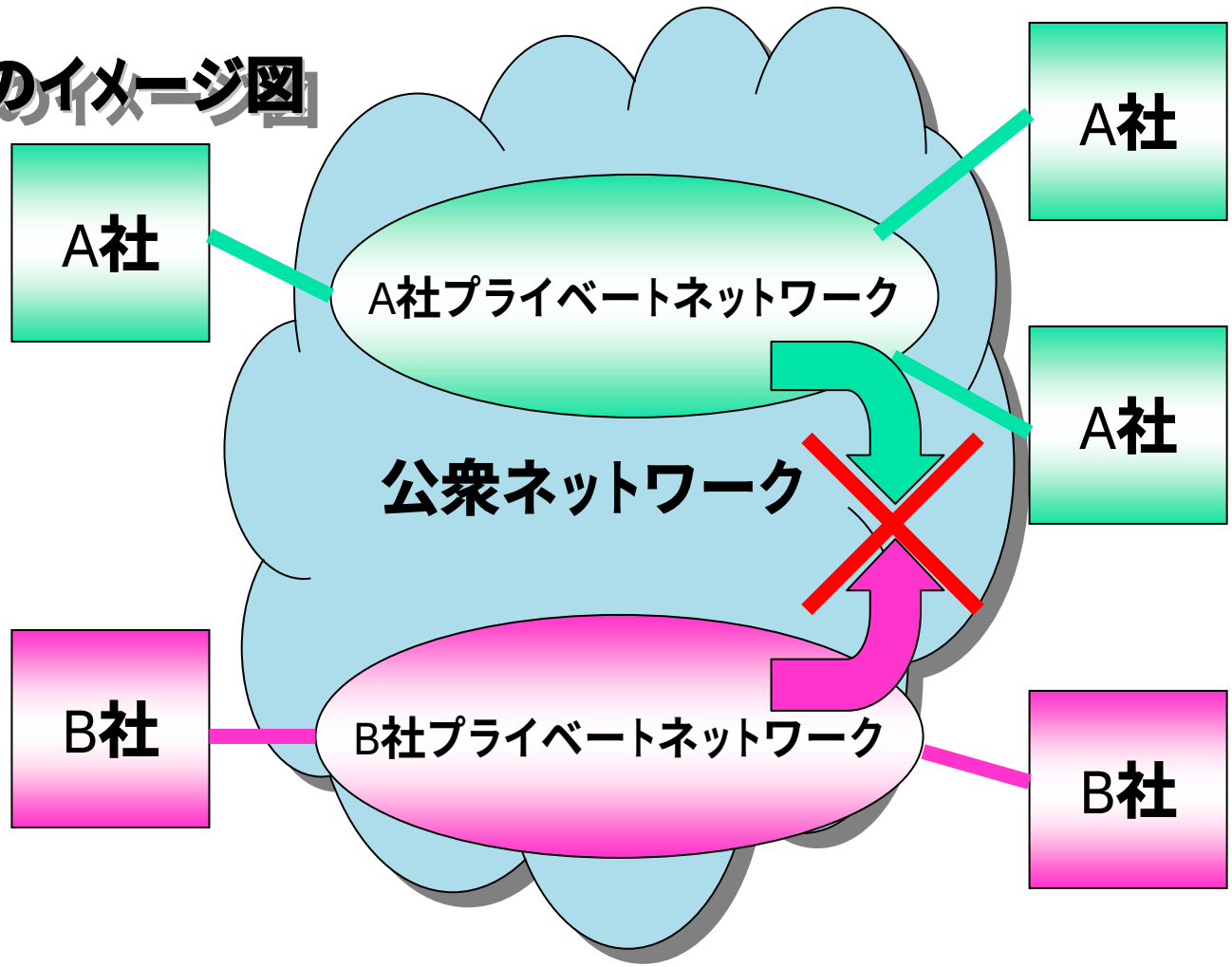


IP-VPN (IP Based Virtual Private Network)

- 拠点間のネットワーク接続や、モバイル端末から企業ネットワークへのリモートアクセスを実現するために欠かせない技術
- IPSECは、このIP-VPNを構築するための標準プロトコルとして使用されている
- VPNとは、インターネットなどの公衆ネットワーク上に、トンネリング技術や暗号技術などを使用して構築された安全な経路のこと

VPN

VPNのイメージ図



VPNのメリット

- VPNでは，インターネットを利用するため，
  - 月々の通信コストを削減
  - 距離の影響を受けないネットワーク構築が可能
  - 接続相手が海外であっても容易で，安価に構築可能
  - 各拠点でイントラネットとインターネットの共有が可能
  - SOHO環境，モバイル環境からのアクセスも容易

  など，様々なメリットがある。

VPNのデメリット

- 複数のインターネット接続点でのセキュリティは甘くなり、ファイアウォールによるネットワークセキュリティの確保が必須。また、通信速度や通信帯域は必ずしも保証はなく，現状では，帯域保証が要求されるネットワークでは不向き。
- 帯域が保証された安定した通信を実現するためには，インターネット接続の際のQoS(Quality Of Service) などのサービスを付加する必要。

IP-VPN

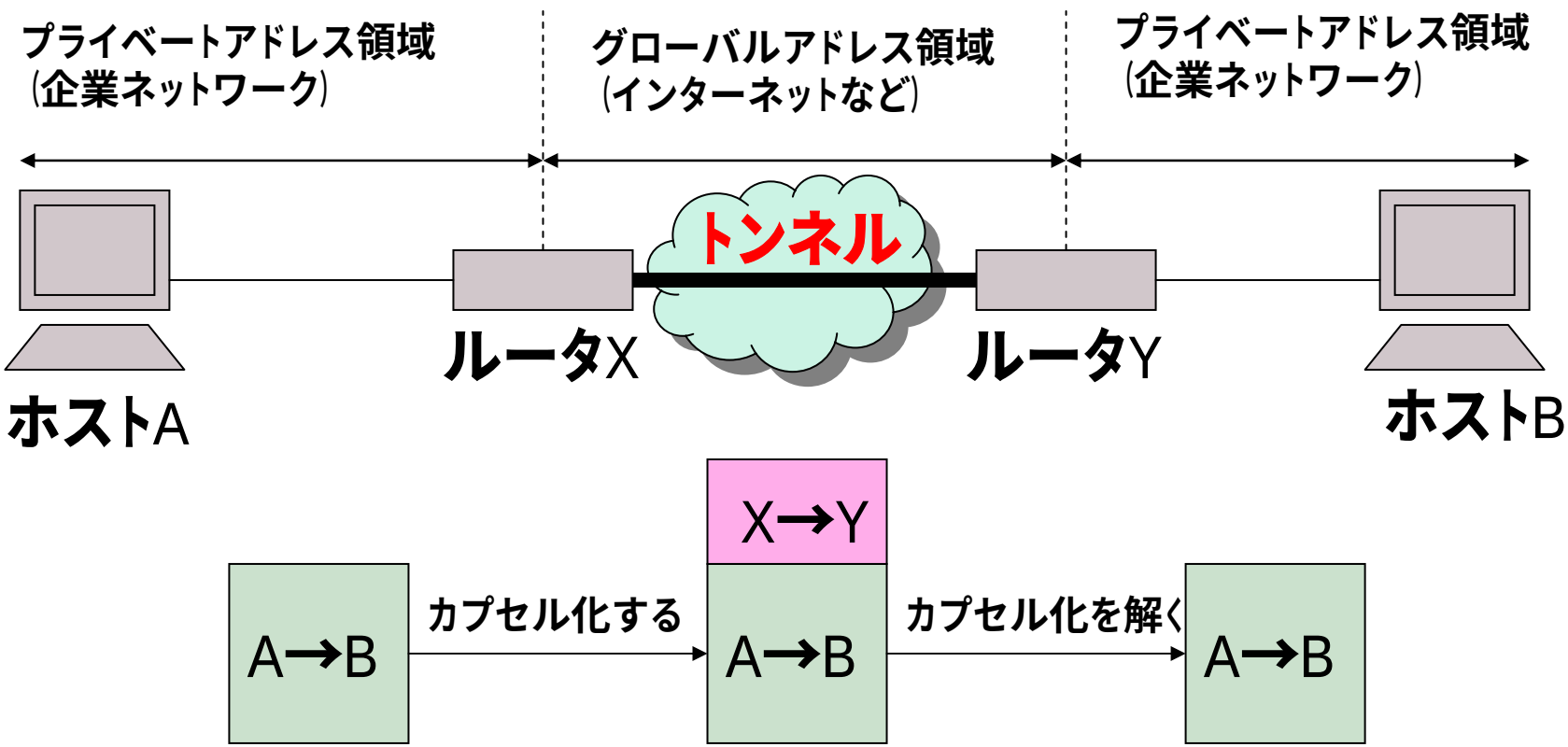
- IP-VPNで必要となる機能
  - トンネリング機能
  - データのセキュリティ確保
  - マルチプロトコル転送
  - サービス品質（QoS：Quality of Service）の保証
  - シーケンス保証
  - トラフィック情報の機密性確保

IP-VPN

- トンネリング機能
  - ネットワーク上に2拠点間を結ぶ仮想的な通信路（トンネル）を構築すること
  - トンネルの入り口となるルータで相手に送信したいデータに、トンネルの出口となるルータまで運ぶための別のIPヘッダをつけて送信する。このように別のIPヘッダを付加する処理をカプセル化という。

IP-VPN

- トンネリング処理



IP-VPN

- **トンネリング機能**
  - **IP-VPNを経由して送信するデータにはインターネット上では利用できないプライベートアドレスが含まれている可能性があるが、トンネリングによってプライベートアドレスを含んだIPパケット全体がカプセル化されるため、プライベートアドレスを隠蔽することが可能**
  - **トンネリングはIP-VPNを実現するためには必須の機能**

IP-VPNの形態

- **拠点間接続**VPN
  - **離れた拠点同士で**VPN**接続すること**
  - **仮想専用線** (VLL)、**仮想プライベートネットワーク** (VPRN) 、**仮想プライベート**LAN**セグメント** (VPLS)**がある**
- **リモートアクセス**VPN
  - **プロバイダのアクセスポイントなどにダイアルアップ接続した端末と企業ネットワークとの間で**VPN**を構築する形態**
  - **仮想プライベートダイアルネットワーク** (VPDN)**とも呼ばれる**

IP-VPNの形態

- トンネリングプロトコル
  - VPNを構築するために必要なトンネリング機能をもつプロトコル
  - IPSECの他に、L2TP（Layer 2 Tunneling Protocol)や、MPLS(Multiprotocol Label Switching)などがある

IPSEC-VPN

- IPバックボーン（インターネットやISPが提供する閉域IPネットワーク）にIPSECトンネルを構築することによって実現する。
- ISPなど事業者のサービスを利用することによって実現することも可能だが、インターネットへのアクセス環境が整っていれば、IPSECに対応した機器やソフトウェアを導入することによって、自組織でVPNを構築することが可能

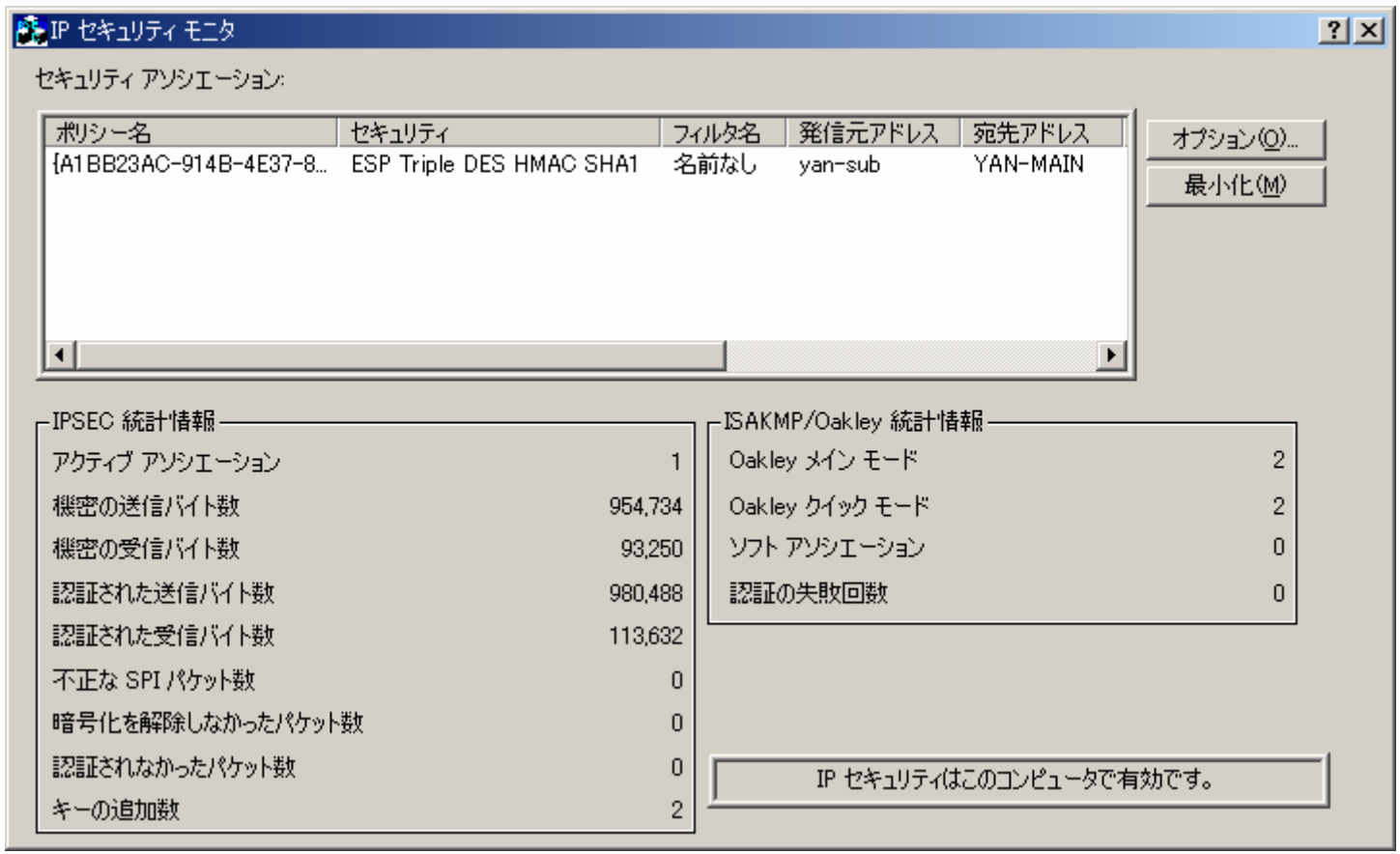
IP-VPN実現方式の比較

機能および特徴	IPSEC-VPN	L2TP-VPN	MPLS-VPN
トンネリング機能	○	○	○
データのセキュリティ確保	○ 暗号技術により確保	× IPSECを利用	△ 閉域性により確保
マルチプロトコル転送	×（IPのみ）	○	×（IPのみ）
シーケンス保証	×	○	○
QoS保証	× RSVP/DiffServを利用	× RSVP/DiffServを利用	× RSVP/DiffServを利用
トラフィック機密性の確保	△ 部分的に確保	× IPSECを利用	○ 閉域性により確保
主な利用形態	VPRN、VPDN	VPDN	VPRN
実現形態	自前の機器またはプロバイダの機器を利用	自前の機器またはプロバイダの機器を利用	プロバイダが提供する網と機器を利用

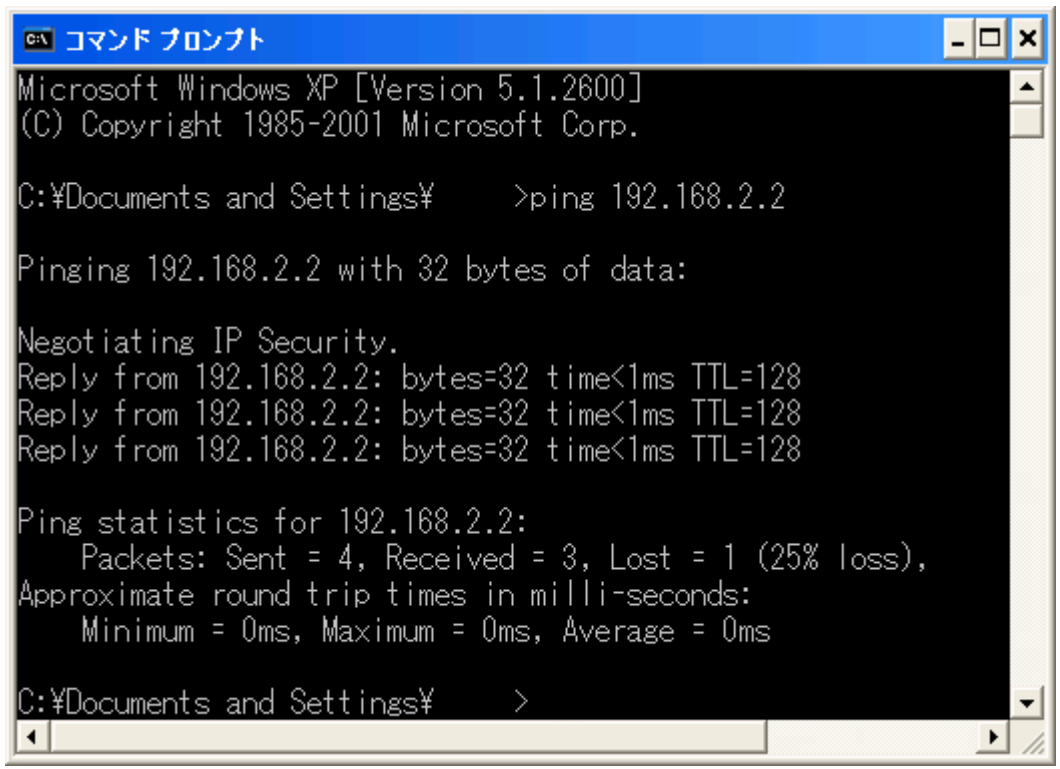
IPSECの導入

- Windows2000およびXPにIPSECを導入する
- Windows2000だとSP2以降がインストールされている必要がある
- IPSECが導入していないと通信を拒否するよう設定した

IPSECの導入


IP セキュリティ モニタ
セキュリティ アソシエーション:
ポリシー名
セキュリティ
フィルタ名
発信元アドレス
宛先アドレス
{A1BB23AC-914B-4E37-8...
ESP Triple DES HMAC SHA1
名前なし
yan-sub
YAN-MAIN
オプション(O)...
最小化(M)
IPSEC 統計情報
アクティブ アソシエーション 1
機密の送信バイト数 954,734
機密の受信バイト数 93,250
認証された送信バイト数 980,488
認証された受信バイト数 113,632
不正な SPI パケット数 0
暗号化を解除しなかったパケット数 0
認証されなかったパケット数 0
キーの追加数 2
ISAKMP/Oakley 統計情報
Oakley メイン モード 2
Oakley クイック モード 2
ソフト アソシエーション 0
認証の失敗回数 0
IP セキュリティはこのコンピュータで有効です。

IPSECの導入



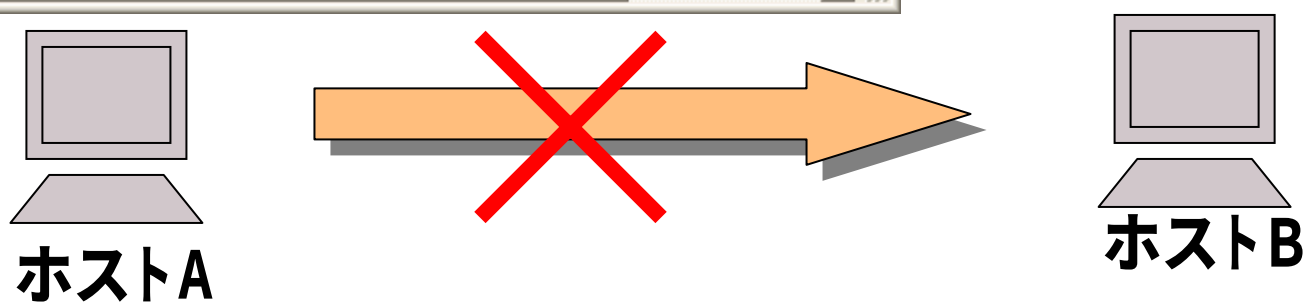
A，B共にIPSECを導入した場合

IPSECの導入

コマンド プロンプト

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:¥Documents and Settings¥     >ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:¥Documents and Settings¥     >
```

AはIPSECを導入していない場合 (Bのみ)



IPSEC導入への課題

- IPSECを導入するには解決すべき、さまざまな課題が残されている
  - PKIの利用
  - NAT環境への適用
  - リモートアクセス環境への適用
  - QoS制御
  - マルチプロトコル環境への適用
  - マルチキャストへの対応
  - Kerberos環境での利用
  - セキュリティーポリシーの管理
  - 相互接続

参考文献

- 「マスタリングIPsec」のサポートページ
  (http://www.tatsuyababa.com/MasteringIPsec/)
- TOM のネットワーク勉強 ノート
  (http://www.tomnetwork.net/index.htm
)

おわり