おや？こんなところにIPsec？
～Windowsで使うIPsecとその罠

2003/03/22

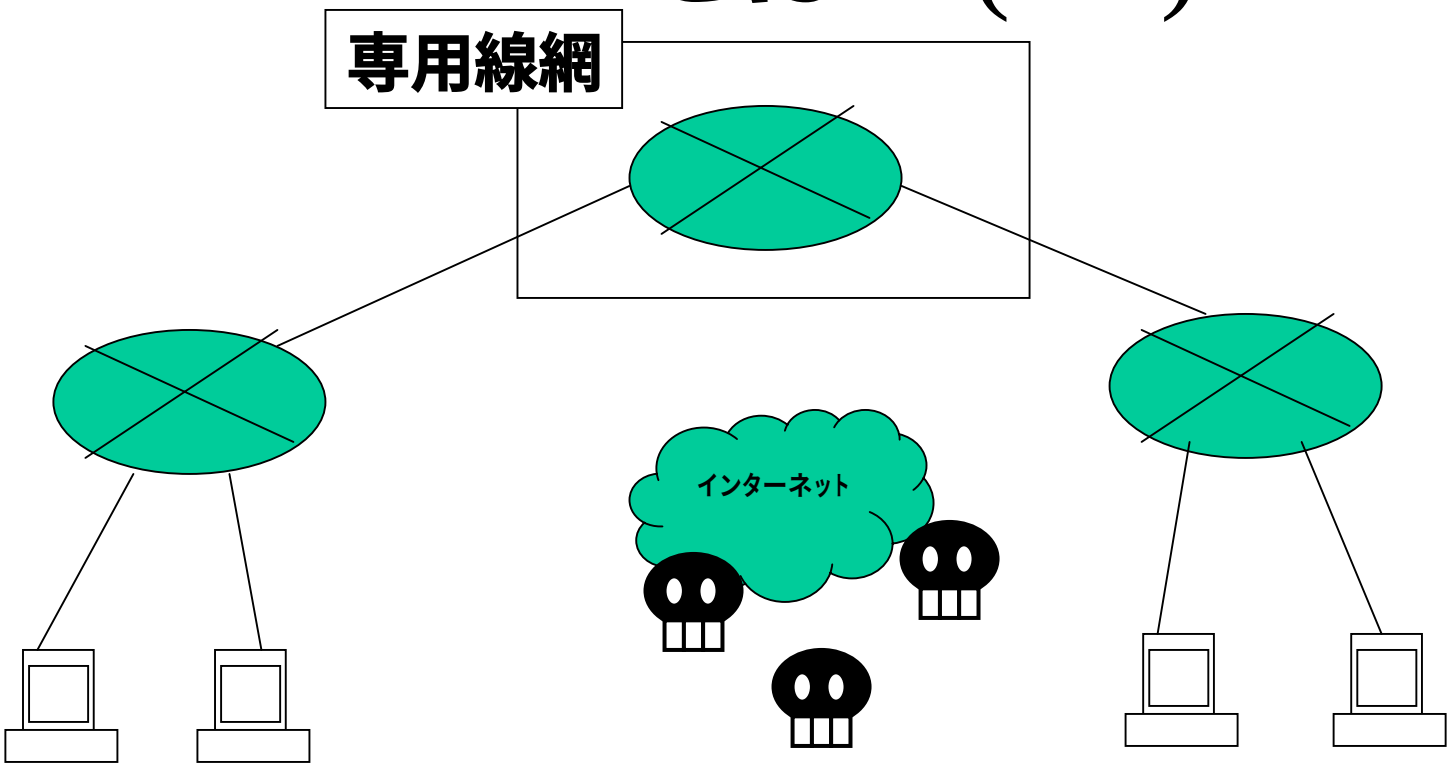
宮本 久仁男

wakatono@todo.gr.jp

IPsecとは？

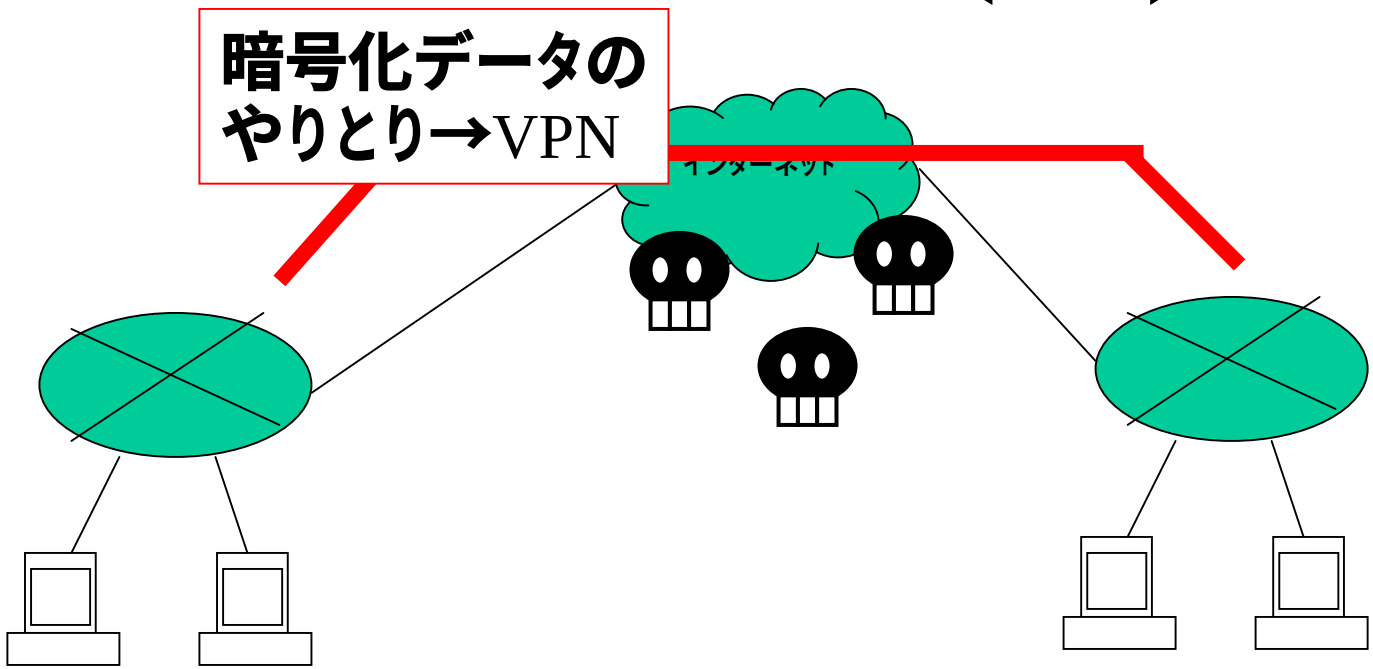
- VPNで使用される標準的なプロトコルの1つ
  - PPTPもその1つ
- ホスト/GW間の安全な通信のためのしくみ
  - ユーザ（資格）は考慮しない（PPTPはユーザ認証込み）
- TCP/IPを使った暗号化通信のための規約／実装
  - 上位アプリケーションには影響を与えない
- 暗号化通信の鍵交換方式について規定
  - IKEと呼ばれている（古くはISAKMP/Oakleyと呼称）
  - IKEとIPsec暗号化通信は独立の規約／実装
- 暗号化方式等について、最低限は規定
  - DES, MD5,SHA1,Oakley Group 1 等必須

VPNとは？(1/3)



- 会社の拠点間ネットワークなどはインターネットとは独立した専用線で構築
- インターネットからの侵入は本質的には無関係
- 当然維持コストは高い

VPNとは？(2/3)



- 専用線を使わず別の方法で（機能的に）専用線とみなせる（仮想的な）網を構築
  - たとえばインターネット経由
  - IPsec等を使ってデータを暗号化

VPNとは？(3/3)

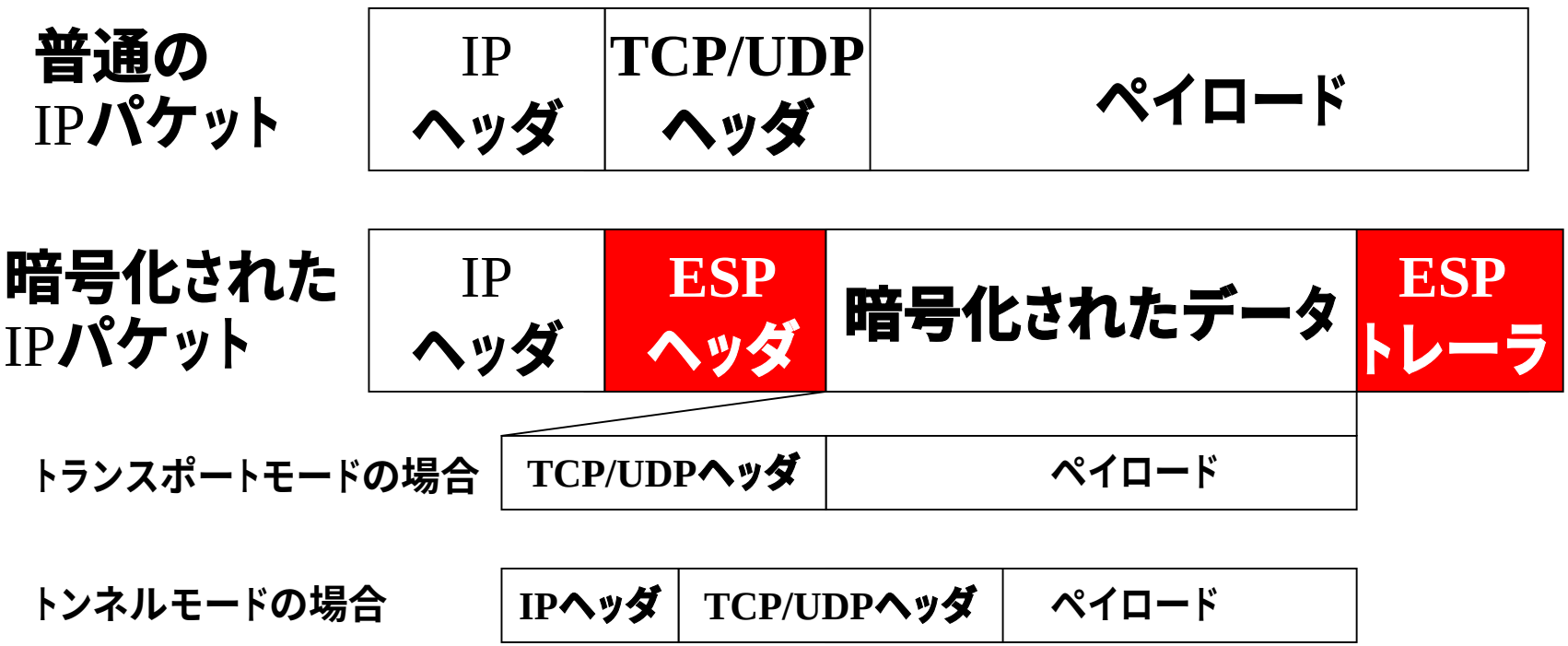
- 専用線とVPNの相違点
  - 見られないようにする（専用線）
    - 網側で外部からのアクセスがないことを保障
    - そもそも網自体にアクセスするのが困難
  - 見られても大丈夫なように暗号化する（VPN）
    - 網はアクセス可能（インターネット）
    - トラフィックを見ることも可能
    - でも、トラフィックが何を意味するかは不明

IPsecの特徴

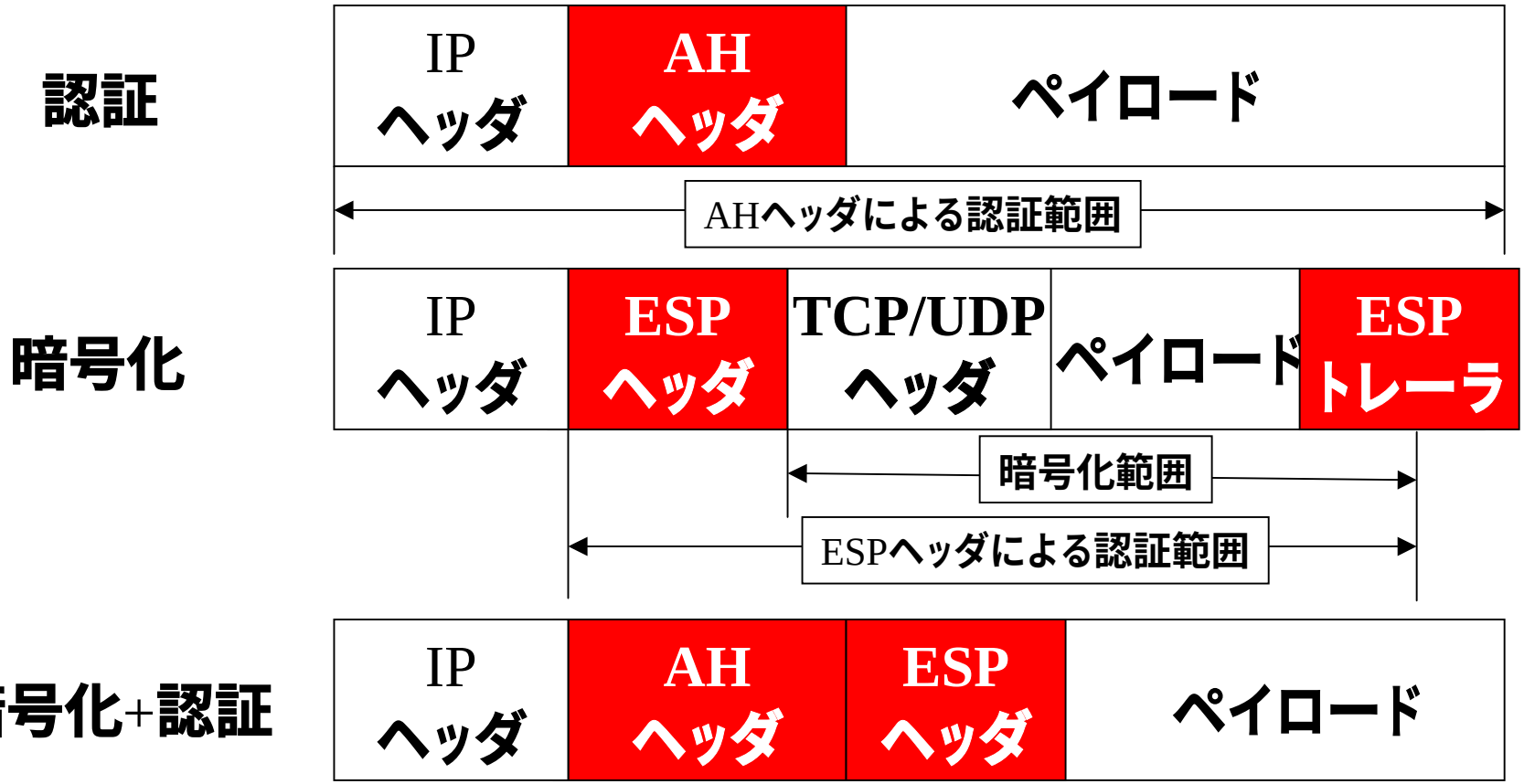
- IP プロトコルのセキュリティ拡張
  - 認証と暗号化
    - 認証に使うAH (Authentication Header)
    - 暗号化に使うESP (Encapsulated Security Payload)
- 2つの通信モード
  - トランスポートモード (1対1/エンドツーエンドの暗号化)
  - トンネルモード (m対n/ゲートウェイでの暗号化)
- レイヤ3での実装
  - 実装はOSのプロトコルスタック (例外も存在)
  - 強力な認証／暗号化方式を採用することも可能

IPsecのパケット構造(1/1)

- IP Security (データを暗号化したIP)

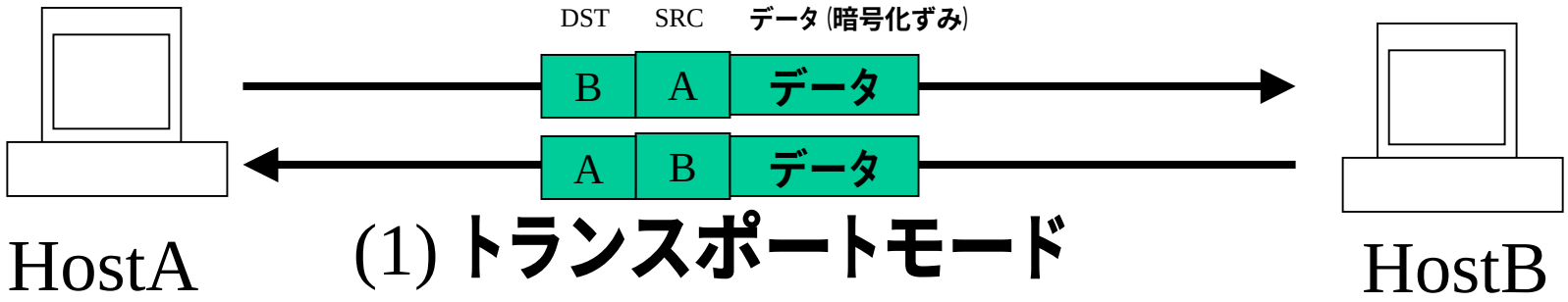


IPsecのパケット構造(2/2)

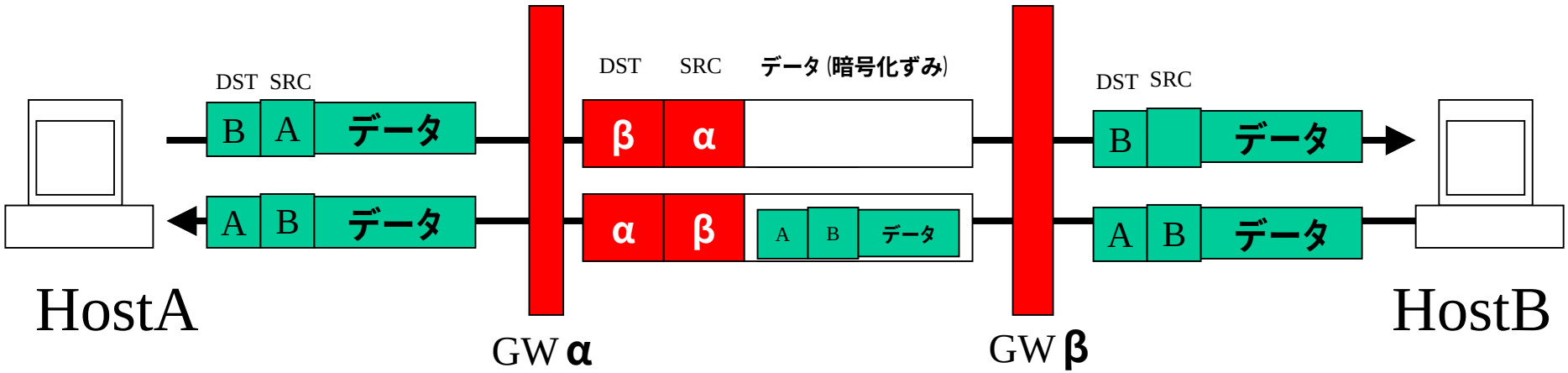


- 認証のみ（暗号化をしてはいけないようなところで使う）
- 暗号化のみ（実用上はESPで認証も行う）
- 暗号化＋認証（厳密）

IPsec の通信モード



(1) トランスポートモード



(2) トンネルモード

IPsecの通信でやりとりするもの

- SPIと暗号化データ
  - SPI: Security Parameter Index
    - 暗号化通信ノードで、SPIに対応して
      「暗号化方式＆秘密鍵」や「相手のIPアドレス」
      等を保持
  - 暗号化データ
    - SPIに対応する暗号化アルゴリズム＆鍵で暗号化
    - データが漏れても解読するための手がかりは
      パケット内になし

IPsec通信の例

- SPIに対応する暗号化方式（CIPHER）やKEYなどは、ISAKMP SA を通じてやりとりされる

IKEのはたらき

- SPIに対応付けられる暗号化方式や鍵等を交換
- IKEの通信時も暗号化通信路を開設
- 認証方法はいろいろ
  - 仮共有鍵（Windows上の呼称）による認証（秘密鍵）
    - IPsec的には仮共有鍵は事前共有鍵(Pre-Shared Key と呼ぶ)
  - X.509v3証明書による認証（公開鍵暗号方式）
  - Kerberos

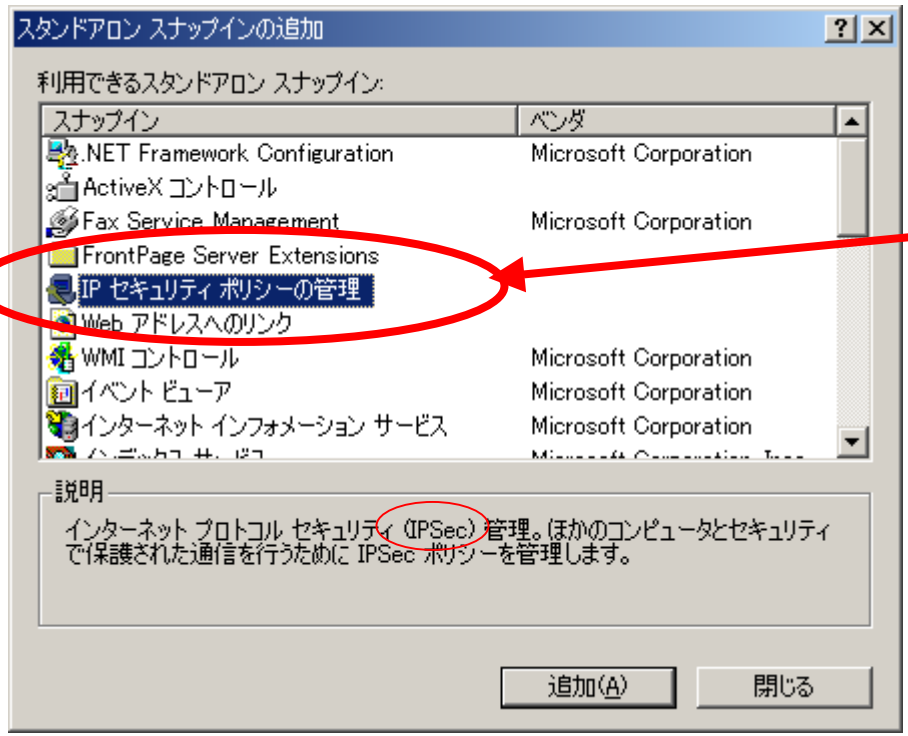
Windows系OSのIPsec対応(1/2)

- Windows 2000 Family
  - **最初からサポート**
- Windows XP Home / Professional
  - **最初からサポート**
- Windows Server 2003
  - **最初からサポート**

Windows系OSのIPsec対応(2/2)

- Windows 98/Me/NT4.0
  - **標準では未対応**
  - SafeNet**作成のクライアントキットが**MS**から配布されている**
    - http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp

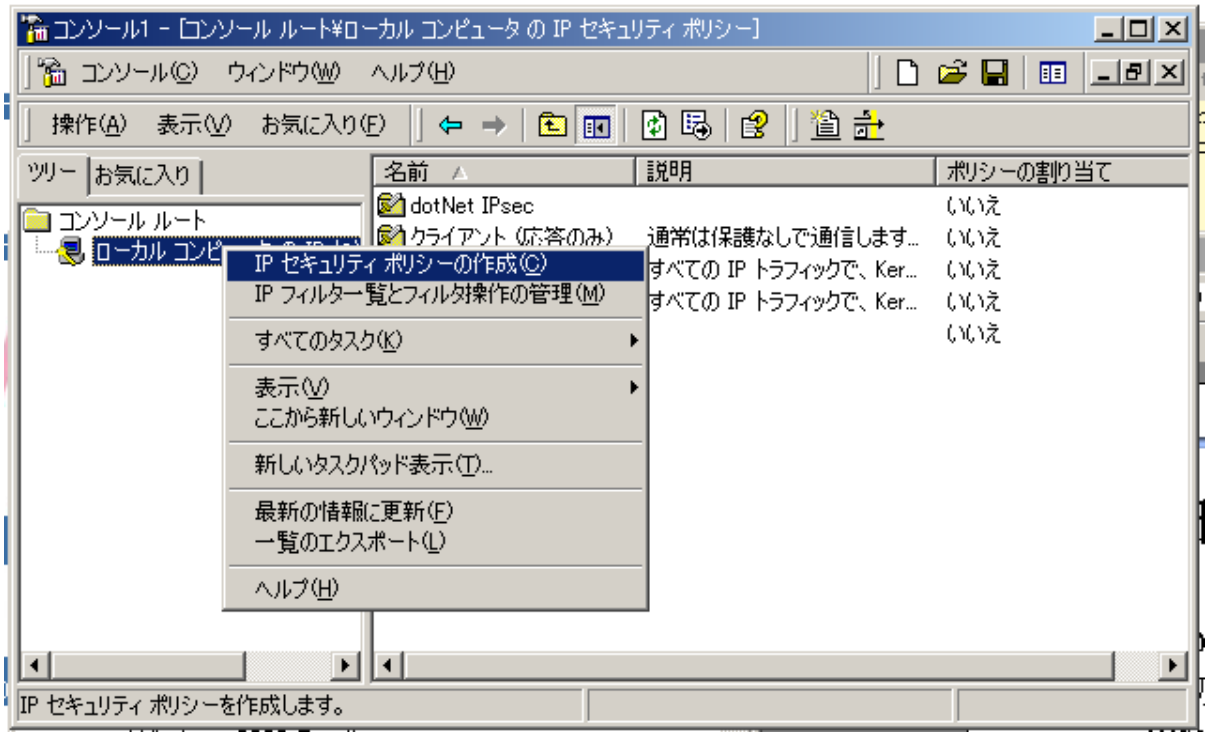
Windows2000での例(1/2)



こんなところにIPsecの設定スナップインが…

MMCコンソールにてスナップインを追加

Windows2000での例(2/2)



- こんな感じの設定画面がつかえます
  - Windows XP Homeでも使用可能
    - mmcコマンドを起動し、スナップイン追加

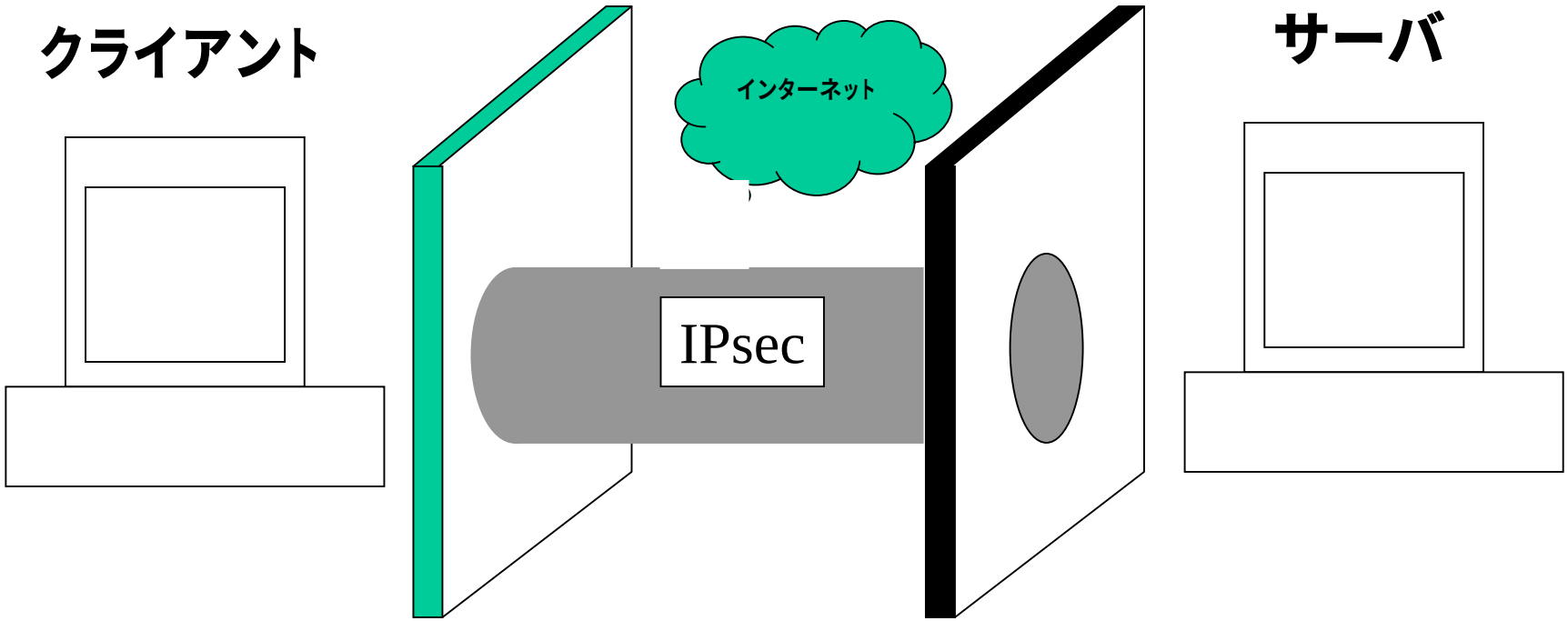
IPsecの弱点

- NAPTによるIPヘッダ書き換え等が入る環境では事実上使えない
  - NATならばESPのみ使う場合はOK
- プロトコルやポートの制限が入ると使えない
  - 後述
- これらの制限は、IPsecでの通信を出来なくする
  - 相互接続性は（意外に）ある
    - 参考文献を参照のこと（汗）
- でも、他にも脅威が…

IPsecのVulnerability(?)

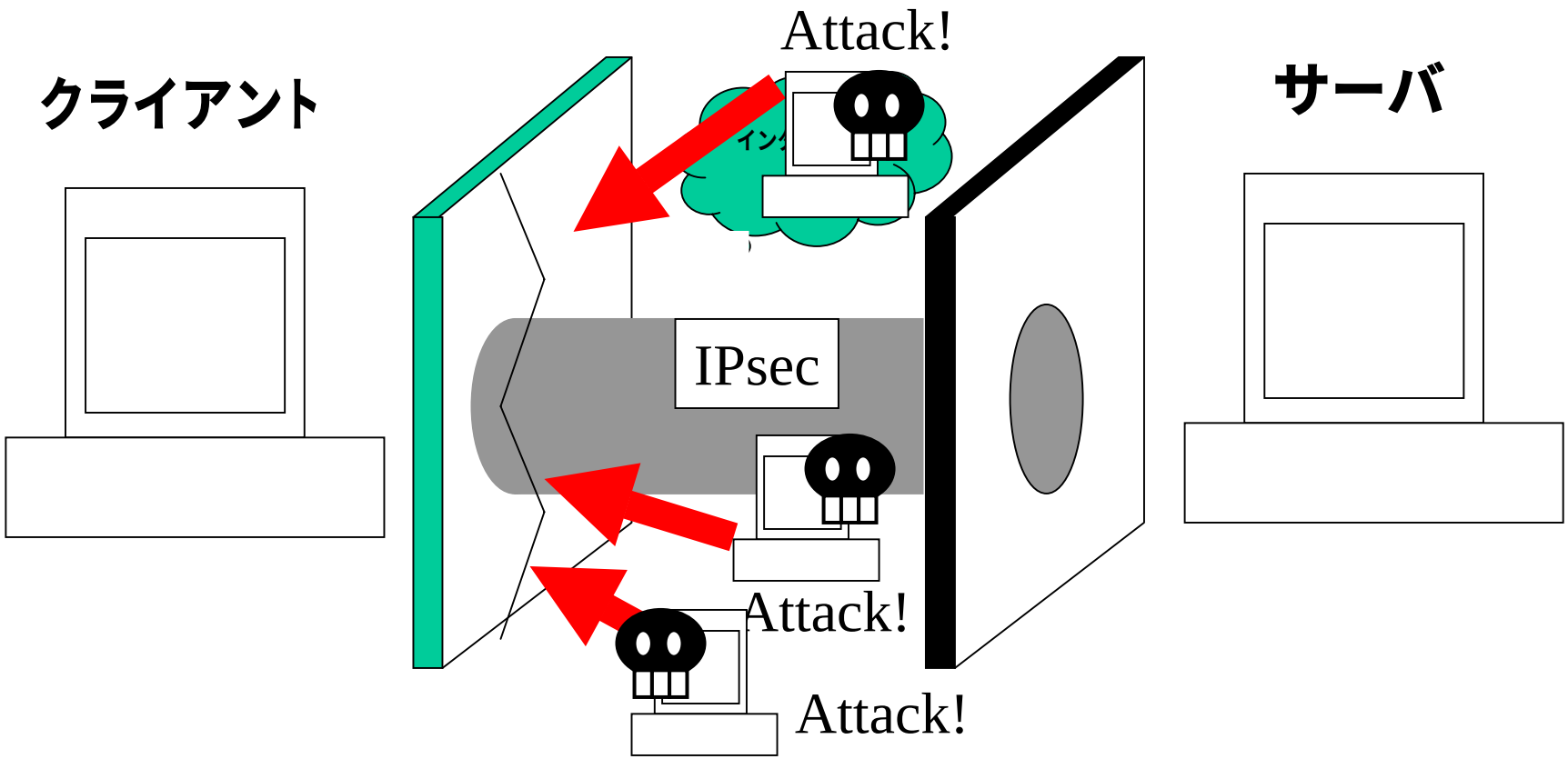
- IPsecパケットそのものは比較的セキュア
  - 暗号化方式の手掛かりはSPI以外ない
  - ホストも、IPsecとは無関係にセキュアにできる
- でもIKEネゴシエーションは…
  - 暗号化はされるものの、IPsecそのものより強力とは言えない
    - SSL相当（それでも強力だが…）
  - IKEを狙うためのツールも存在
    - IKECrack,IKEScan
  - IKEの認証方式によってはガンガン弱くなる
    - Pre-shared Key等
    - クライアントの実装によっても強弱が変わる…（→実例は？）

鋼鉄のパイプにも弱点が…



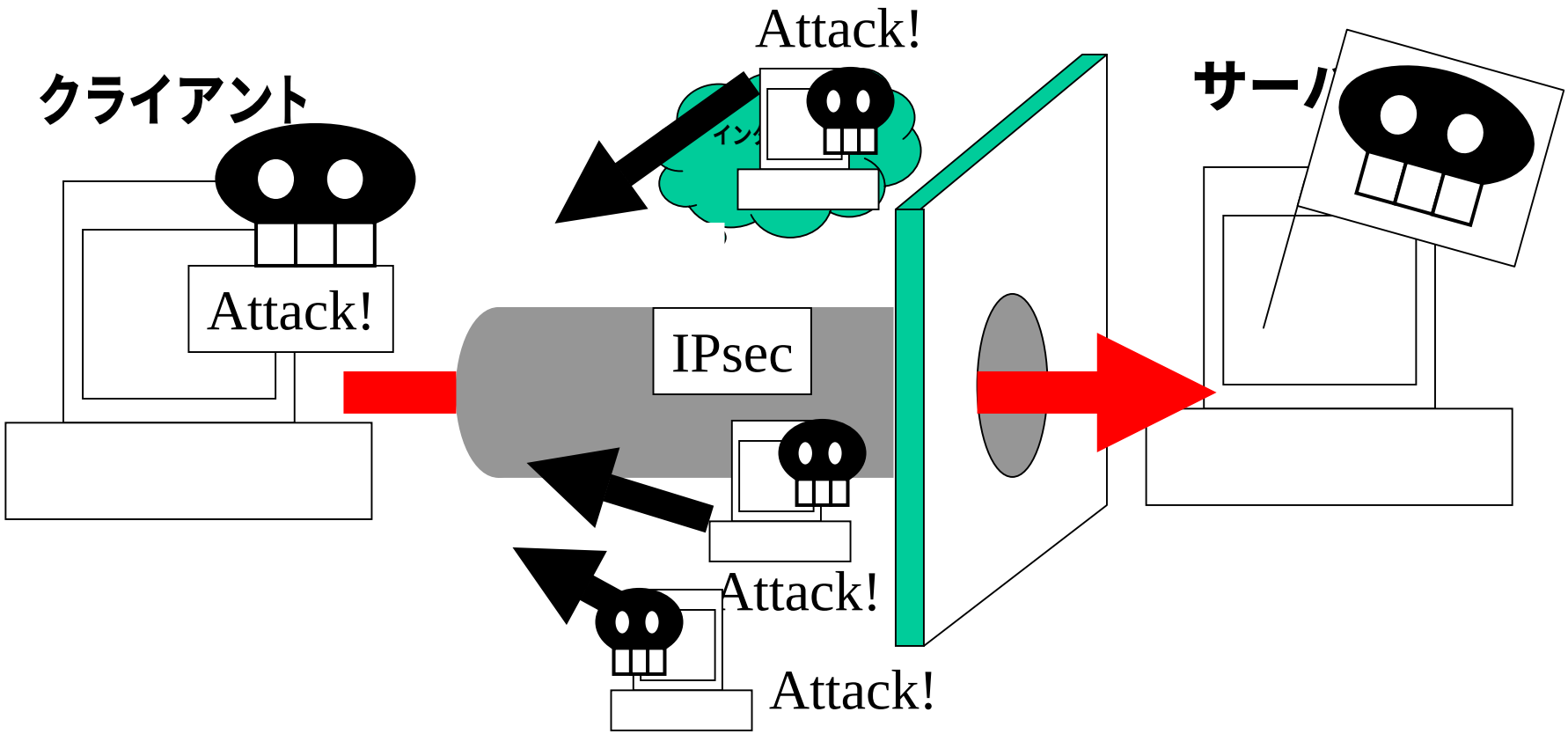
- IPsecにより守られた（仮想）通信路は
  「鋼鉄のパイプ」と呼ばれることもある。が…

守りの弱いマシンが狙われる



- マシンの守りが**ベニヤ板**じゃ意味なし…
- セキュリティ的に弱いマシン = システムの弱点

あわれクライアントは踏み台に



- そしてサーバの運命はいかに…

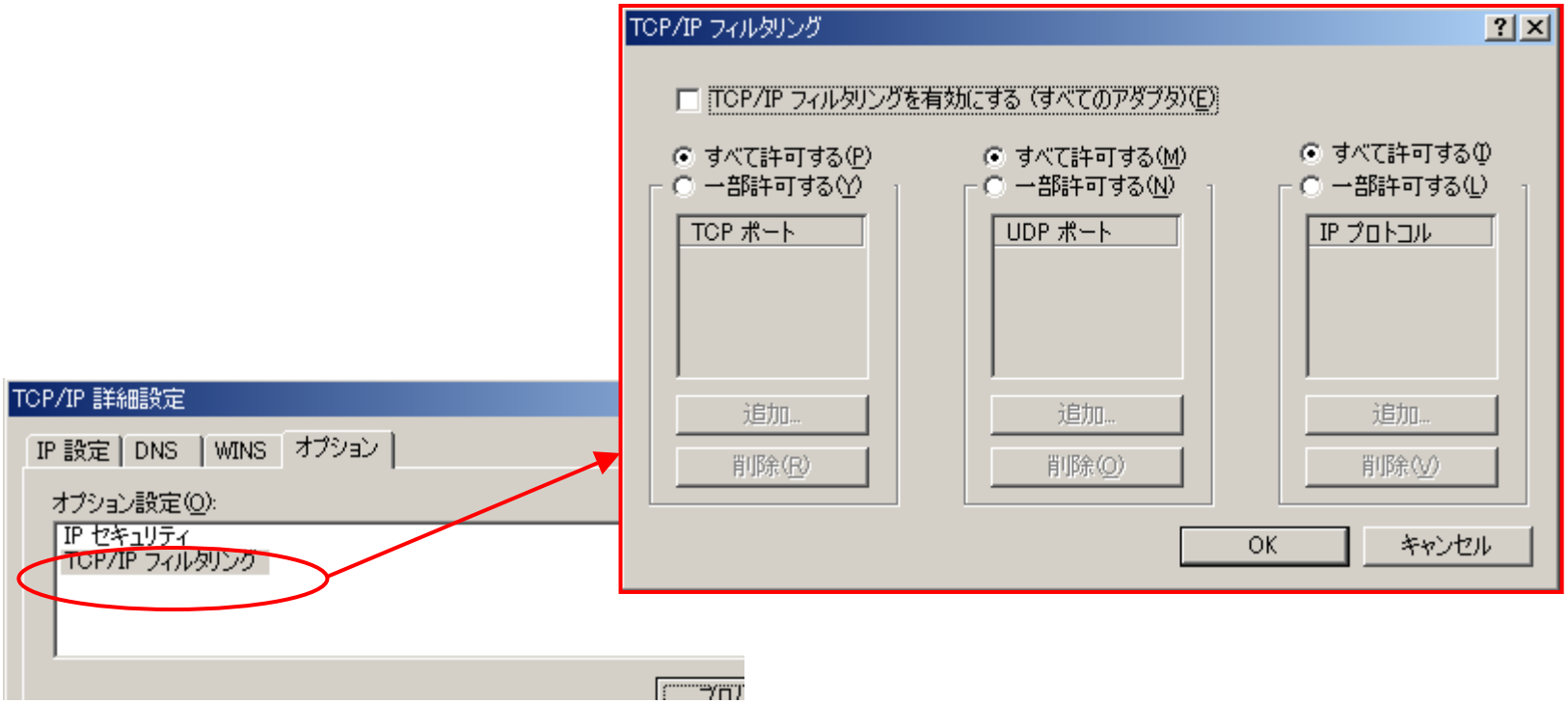
3つの鉄則その1&その2

- IPsecは盗聴と改ざんに強いとされているが**万能ではない**
  - 仮共有鍵を変えなければいつかは破られる
    - 仮共有鍵はマメに変更
    - 願わくば是非、公開鍵暗号を（やぶるのに時間がかかる）…
- 盗聴に強いのと侵入されづらいのは**別問題**
  - システム中でセキュリティの弱い端末が弱点に
    - ゲートウェイやクライアントに侵入されたら終了
      - 鍵がわからなくても通信が出来る
      - もちろん鍵も割り出せる

IPsec+ α

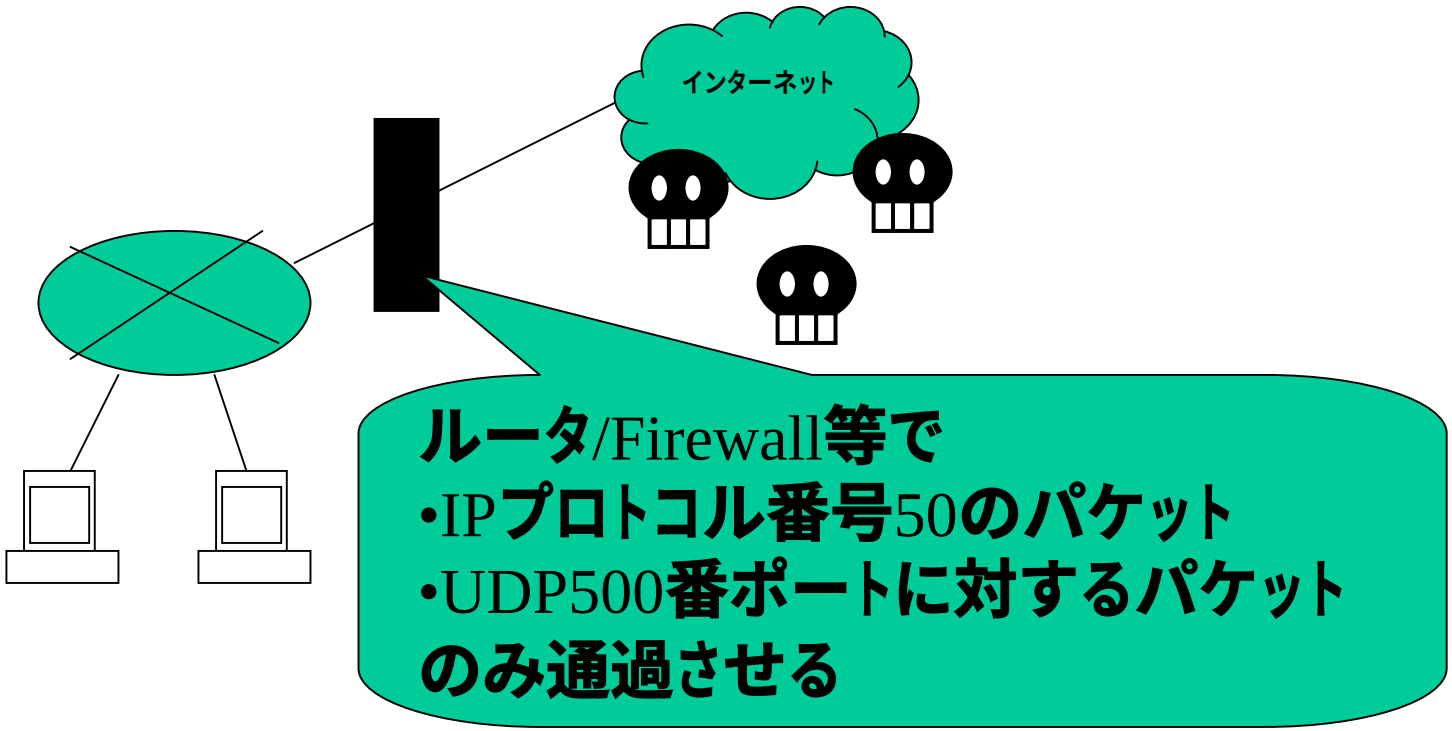
- Windows 2000 の場合
  - IPsecのスタックを経由しない通信もあるケース
    - Kerberosのトラフィック等はIPsec経由せず
      - レジストリの設定による
      - http://support.microsoft.com/default.aspx?scid=kb;ja;253169
    - これを悪用されると、送信元ポートがTCP88番のパケットは素通し
      - 大いなる罠…
  - レジストリを編集することで回避
    - http://www.securityfocus.com/infocus/1528
    - http://support.microsoft.com/default.aspx?scid=kb;en-us;Q254728&sd=tech
      - HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥IPSEC¥NoDefaultExempt のType値を1に(Windows 2000, Windows XP)
      - Regedt32等のツールを使用してキーを追加

IPsec+α(1/3)



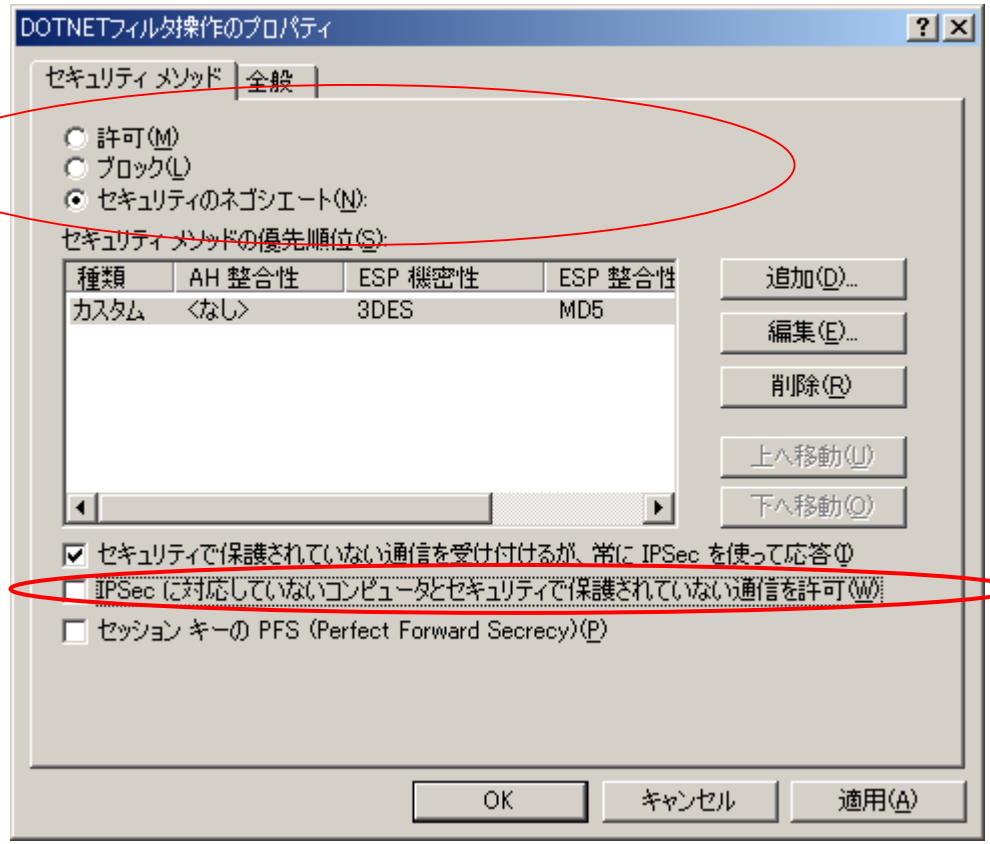
- TCP/IP**フィルタリング等も使ってみよう**
  - IP**プロトコル番号**50&UDP500**番向けパケットのみ通過させるような感じ**

IPsec+α(2/3)



- ルータ等でもなんとかなることも多い
  - 私はRTA54iのフィルタ機能を使ってた経験あり…

IPsec+ α (3/3)



- IPsecでしか通信しないように仕向ける

3つの鉄則その3

- IPsec以上にシステムのトータルセキュリティの方が重要
  - ルータやFirewallでフィルタするだけでも違う
  - IKEネゴシエーションに失敗したら通信しないというのも手

まとめ（？）

- 盗聴と改ざんと侵入は「別！」
  - 通信内容の盗聴も改ざんも出来なくても、侵入は可能
- 暗号化や認証を過信するな
  - 侵入は別だってば
  - DoSも別かな
- IPsecに多くを期待するな
  - 強力な暗号化通信/認証手段を提供するが
    万能ではない（過信は禁物）
  - 使いどころだよねぇ

参考文献(1/2)

- Linux以外のIPSecスタックとの相互接続
  - Windowsを含むいくつかのIPsec実装相互接続検証
  - http://www.atmarkit.co.jp/flinux/special/ipsec2/ipsec02a.html
- マスタリングIPsec (オライリージャパン)
  - IPsecについてはこれ1冊で十分なほどの情報量を誇る
    - 当然私も持ってます (そして読んでます)
    - プラットフォームごとの設定方法についても言及
    - 相互接続のヒントまで記述
    - 最新の動向にも追従
      - 筆者のページでサポートが

参考文献(2/2)

- IKECrack
  - http://ikecrack.sourceforge.net/
- IKEScan
  - http://www.nta-monitor.com/ike-scan/