オフィス環境での無線セキュリティ

JNSA相互接続WG
㈱ディアイティ　関

JNSA 相互接続WG

- 802.1xを使って構築する802.11無線LAN セキュリティの接続性
- 実機を使った構築と接続試験を実施中

有線LANとオフィス環境

- 重要な端末や、ケーブルにはアクセスできない物理的に守られた環境
- 盗聴やデータ改ざん、なりすましは内部犯行に限られる。

無線と施設のセキュリティ

- 電子錠前付きドア
- 警備員
  ------人や物の移動を制限
- 電波を使った無線通信
- あらゆる方向に拡散する
  「何時でも何処でも」
  -------従来のセキュリティでは制限できない

電波の性質とセキュリティ

- 「不審な電波を除外できない」
  論理的に(結果として) 不審者を
  除外する方法を用意しなければならない
- 「電波は拡散してしまう」
  何処にでも広がる電波
  壁などで減衰させることは可能

無線LAN環境の脅威

- 情報の漏洩
  簡単にできるパケットキャプチャー
- ネットワークへの侵入
  イントラネットへの不正侵入、情報改ざん
- ネットワーク犯罪への加担
  侵入者のID隠蔽に利用される

便利で危険な無線LAN

- すでに普及が始まっている
  「会議室へ移動して･･･」
  「配線が面倒･･･」

- 無線LAN環境を配備していなくても
  意識しなければならない無線セキュリティ

不審者を除外＝信頼を確認

- 通信相手の信頼性を確認する
  「より確実で安全な認証」
- より安全な暗号通信を行う
  「解けない」「ばれない」
- 非暗号の通信を拒否する
  アクセスポイント、基地局？

安全な通信　IPsecの考え方

- 長い鍵(128、168bit)を使う
- より安全な暗号方式(DES,AESなど)

- 鍵をネットワークへ送信しない　(DH)
- 鍵を更新する
- 暗号処理をしてIDを確認する

無線セキュリティの現状

- MACアドレス(物理アドレス)フィルタ
- WEP
- IEEE802.1x　(認証手順)

- ベンダー独自方式

物理アドレスによるフィルタ

- MACアドレス(物理アドレス)を使うので
  ノートPCの固体認識が簡単に可能
- スキルがあればアドレスの詐称が可能
- 情報の機密性は守れない

WEP

- 64(40),128(104)ビットの暗号処理
- すべてのPCで同じ鍵を使う
  誰かが漏洩したら安全でなくなる
- 固定的に同じ鍵を使う
  一度ばれたら安全でない
- 暗号処理が弱い
  特定の条件で暗号を解ける(RC4を問題のある実装で使う)

IEEE802.1x

- MS Windows XPに標準搭載
- 認証方式を定めた標準技術
- 無線LANではWEPと組み合わせる

- WEPとの連携は厳密に定めていない
  無線LANでは製品ごとに
- パスワードやPKIなど選択肢によって
  セキュリティレベルが変わる

独自のセキュリティ方式

- 標準技術だけでは実現できない
  セキュリティレベル

- 互換性が期待できない
- セキュリティレベルも
  ベンダーごとにまちまち
- 標準技術ではない

次世代の方式

- 現在検討中の規格
  IEEE802.11i等

安定している802.11bとWEP

- 広く流通している機材
- 高い相互接続性
- 無線の特性を生かした使い方

- 簡単に使用できる=セキュリティに疑問

既存製品の適用範囲

- 受け付け、会議室などの
  パブリックよりのサービス

- 困難なのはイントラネットへの直結
  →独自方式を採用した製品の検討
  →IPsecなどの暗号処理を併用
  →端末PCの保護にパケットフィルタを設定

組み合わせでのセキュリティ

- WEPの設定
  鍵長128ビット、定期的に変える
- ESSIDの設定
  ANYの禁止
- MACアドレスフィルタ
- 不使用時の電源OFF

イントラネットへのアクセス

- MACアドレスによるフィルタリング
- ESSIDのセキュリティ設定
  ANYの拒否
  ビーコンの停止
  プローブ要求に対するESSIDの隠蔽応答
  プローブ要求の無視
- IPsecゲート機器などの併用
- 独自方式を採用した製品の配備

VPN機器の併用

- IPsec
- PPTP、L2TP

- PCにインストールするクライアントソフト
  トンネル外側のフィルタ機能

  システム全体の使い勝手を評価する必要

勝手に設置されるAPの危険性

- 「マネジメント」されないAP
  危険があるまま「放送」される
- クライアント間での通信による危険

無線パトロール

- 不適切なAPの排除
  「APは簡単に設置できる」
- 使いやすい=セキュリティが弱い
  見つけるのが簡単
  「アナライザ」
  「ウォードライビングツール」

まとめ

- 未熟な無線LANのセキュリティ
- 必要とされるオフィスでの無線LAN環境

- 有線とは区別して使うこと