IW2002-B5

1

家庭内ネットワーク・セキュリティ入門
～常時接続時代を迎えて～

Internet Week 2002
2002年12月18日(水) 9:30～12:30

(株)電通国際情報サービス
熊谷誠治
kuma@isid.co.jp

IW2002-B5

2

セッション概要

- ADSLやFTTHのサービスが全国に広がる中、家庭でのインターネット常時接続の普及が進んでいる。24時間・定額で広帯域を利用できるブロードバンド・インターネットは、多くの利用者が理想とするサービス形態である。固定IPアドレスが割り当てられればなおよい。さらに、自宅内では、配線の手間を省く無線LANの普及が始まっている。ノートパソコンも無線LANクライアント機能を内蔵する製品が増えており、アクセス・ポイントを購入し、自宅のネットワーク接続するだけなので、手軽に利用を始めることが可能である。
- しかし、これらはセキュリティ的に大きな問題を抱えている。注意を怠ると、個人情報が漏れたり、他のサイトへの進入経路として利用されたり、他のサイトへの攻撃の拠点として悪用されることもある。
- 本セッションでは、家庭の常時接続インターネットや無線LANが抱える問題を解説し、被害者とならないだけでなく、知らぬ間に加害者とならないための方法を検討する。家庭に広がる常時接続インターネット利用者のための入門講座という位置づけである。
- **対象者**
  - 常時接続を考えているインターネット初心者
  - 常時接続を利用していてセキュリティが気になる人
  - 社員が自宅で常時接続を利用している企業のネットワーク管理者

IW2002-B5
3

なぜセキュリティなのか？

- インターネットの普及が進む
  - 技術的知識がなくてもインターネットは使える
  - セキュリティ意識の低い利用者が増える
  - 利用者が増えれば犯罪者も増える
  - 当然守りが弱い
- 実際に被害が急増中
  - 守らないとやられる
  - 守りが弱いとやられる
  - 守り方がわからない利用者が急増中
  - 誰かがやられるとそこから攻撃が行われる
- 「守る」ことがセキュリティ
  - 被害に遭ってまで使うようなものか？

IT Solution Innovator iSiD

IW2002-B5
4

常時接続時代に突入

- 常時接続とは
  - つねにインターネットに接続されている
  - 利用のたびに接続する必要がない
- 個人も常時接続へ
  - 安価なサービスが登場
  - 使いたいときに使いたいだけ費用を考えずに使える
  - ダイアルアップに比べて高速
  - 「あたりまえ」になりつつある
- e-Japanの目標
  - 2005年に3000万世帯が高速インターネット接続
  - 2005年に1000万世帯が超高速インターネット接続

IT Solution Innovator iSiD

IW2002-B5

5

ブロードバンド時代ともいう

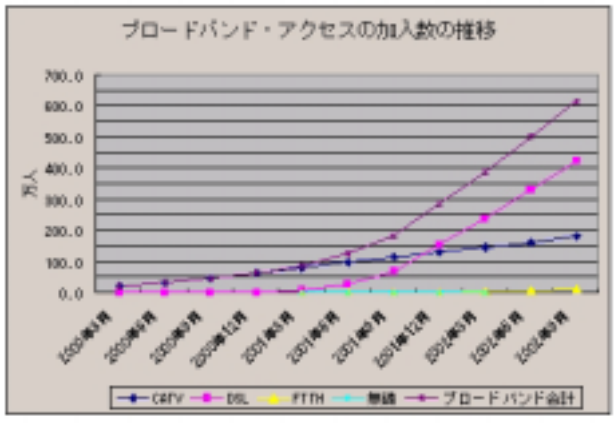
- ブロードバンドとは
  - 広帯域
  - 常時接続
  - 固定料金
  - 固定IPアドレス
- 速いことはいいこと
  - 無駄な時間をなくしてインターネットアクセス
    - » イライラがなくなって気分爽快
  - これまでできなかったことができるようになる
    - » なんでもインターネットで調べてしまう
- 日常生活にとけ込んでくると…
  - もう止められない

IW2002-B5

6

急増するブロードバンド利用者

- 多彩な接続方式
  - CATV
  - DSL
  - FTTH
  - 無線LAN



- 約620万人(2002年9月末現在)
  - CATV 180万、DSL 422万、FTTH 12万

総務省平成14年度版情報通信白書より

IW2002-B5
7

ブロードバンドでできること

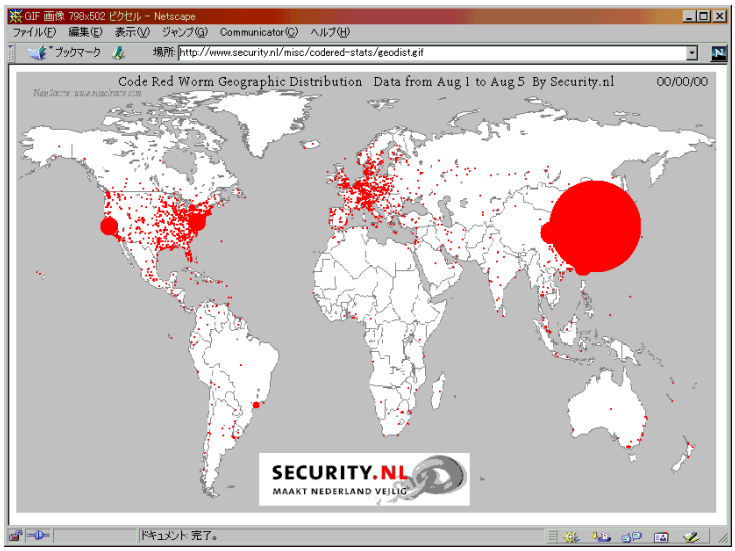
- ファイルダウンロード
  - MP3、CDデータ、映画、プログラム
- インターネット放送
  - イベント中継、スポーツ中継
  - CM、ニュース
- 映像や音楽のリッチコンテンツ
  - ビデオクリップ、マニュアル、観光案内、VoD
- 楽しくお買い物
  - 動画がナビゲーション
- その他
  - テレビ電話、テレビ・チャット

IW2002-B5
8

リスクも大きくなる

- 高速回線で攻撃力が向上
  - 回線速度が100倍になると…
    - » 1分間に5回しかできなかった攻撃が500回可能に
- 常時接続で被害を受ける機会が増える
  - 1日24時間接続していると…
    - » 1日1時間接続の24倍の危険
- たとえば2001年に発生したCodeRed
  - 韓国での被害拡大が有名
    - » ブロードバンドの普及
    - » セキュリティ意識の不足
  - これまでになかった傾向

CodeRedの被害状況



URL=http://www.security.nl/misc/codered-stats/

CodeRedのしくみ

- 自己増殖するワーム(Worm)だった
  - ワームがサーバーに攻撃をしかける
  - セキュリティ・ホールがあると被害に遭う
  - 被害者が他のサーバーに攻撃を始める
- 無差別に攻撃を行う
  - IPアドレスを勝手に選んで攻撃
  - 攻撃先のIPアドレスを高速で変更しながら攻撃
  - 自動的にどんどん攻撃を繰り返す
- 亜種も登場
  - CodeRed II は近傍のIPアドレスを攻撃
  - 同一ISPの顧客に広がる

IW2002-B5
11

セキュリティ・モデルの変化

- 昔
  - 狙われるのは大企業や官公庁だった
    - » 重要な情報がありそうだから
    - » 損害を与えることができる
    - » 守られているはずだから破る楽しみ
- 今
  - インターネットに接続していれば攻撃される
    - » 企業も個人も関係なし
    - » 攻撃を逃れることはできない
    - » 防衛していないと被害に遭う
- 自分の責任で守らなければならない
  - 知らなかったでは済まない
  - 実質的な被害に至ることも

IW2002-B5
12

今そこにある危機

- 多彩な攻撃パターンと急増する攻撃者
  - ウイルス
  - ワーム
  - スパイウェア
  - 不正アクセス
- 無差別に攻撃を受ける
  - 攻撃者は「相手」を気にせずに攻撃
  - 個人でも家庭でも攻撃を受ける
- 守っていないと被害を受ける
  - 被害内容はさまざま
  - クライアントでも被害を受ける

IW2002-B5

13

今そこにある危機(つづき)

- 通信内容漏洩の可能性
  - CATV
  - マンション・インターネット
  - 無線LAN
- 個人情報特定の可能性
  - クッキー
  - 固定IPアドレス
- 「受動的攻撃」
  - ワナをしかけられている
  - インターネットを使うだけで被害に遭う

IW2002-B5

14

注意喚起が続く(JPCERT)

- 2002-09-17 OpenSSL の脆弱性を使って伝播する Apache/mod_ssl ワーム
- 2002-06-28 DNS resolver の脆弱性に関する注意喚起
- 2002-06-27 OpenSSH サーバプログラムの脆弱性に関する注意喚起
- 2002-06-20 Apache Web サーバプログラムの脆弱性に関する注意喚起
- 2002-05-24 TCP 1433番ポートへのスキャンの増加に関する注意喚起
- 2002-02-14 SNMPv1 の実装に含まれる脆弱性に関する注意喚起
- 2001-10-09 CDE ToolTalk に含まれる脆弱性に関する注意喚起
- 2001-09-19 80番ポート (HTTP) へのスキャンの増加に関する注意喚起
- 2001-08-31 BSD 系 OS の lpd に含まれる脆弱性に関する注意喚起
- 2001-08-21 Linux の telnetd に含まれる脆弱性に関する注意喚起
- 2001-08-08 Microsoft IIS の脆弱性を使って伝播するワーム "Code Red II"
- 2001-08-06 "Code Red" Worm の変種に関する注意喚起
- 2001-07-30 "Code Red" Worm の伝播活動再開に関する注意喚起
- 2001-07-27 telnetd に含まれる脆弱性に関する注意喚起
- 2001-07-27 SSH のパスワード認証の脆弱性に関する注意喚起
- 2001-07-25 Microsoft IIS の脆弱性を使って伝播するワーム
- 2001-07-19 Microsoft IIS の脆弱性を使って伝播する Worm に関する注意喚起
- 2001-07-04 Solaris の NIS プログラム ypbind に含まれる脆弱性に関する注意喚起
- 2001-06-27 Solaris のプリンタデーモンに含まれる脆弱性に関する注意喚起
- **http://www.jpcert.or.jp/at/**

IW2002-B5
15

ひとごとでなくなった被害

- 狙われるのは官公庁、有名企業だけではない
  - 企業規模を問わない
  - 個人かどうかも関係ない
  - 目標の考え方が変わった
- これまでは目標を持つ犯罪が多かった
  - 官公庁Web改ざん
  - 軍、研究所に侵入して機密情報入手
- 最近は無差別攻撃
  - ランダムにIPアドレスを選んで攻撃
  - 被害を広めることが目的
- 毎日のように攻撃を受けている !!

IW2002-B5
16

不正アクセスによる被害

- コンピュータに侵入
  - 侵入そのものが犯罪 → 不正アクセス防止法
  - トロイの木馬をしかける
- ファイルを破壊
  - データが消失
  - コンピュータを再インストール
- ファイルを窃盗
  - 盗んだファイルを公開
  - 盗んだクレジットカード番号を悪用
- SPAMメールの中継に使用
- 踏み台にしてほかに侵入

トロイの木馬とは

- ギリシャ神話の「あれ」
  - 門前に置かれていた木馬
  - 「贈り物」と思った
  - ありがたく受け取り城内に持ち込んだ
  - 「贈り物」の木馬に兵士が潜んでいた
- インターネットの世界では
  - ユーザーが予測しない働きをするプログラム
  - ハッカーが何らかの手段でしかける
  - 「受動的攻撃」でもトロイの木馬を利用

ダウンロードによる被害

- ウイルスに感染
- 勝手に電話をかけられる
  - ダイヤルQ2
  - 国際電話
- ハードディスク内のデータを破壊
- 外部の第三者がコンピュータを操作
  - 破壊、窃盗
  - 踏み台
- コンピュータ内のファイルを窃盗
  - 外部に送出

不正侵入による被害

- 重要情報の持ち出し
  - 年賀状住所録、画像
  - 銀行口座番号、クレジットカード番号
  - 日記、家族情報
- 持ち出した個人情報を公開・悪用
  - 友人に大きな迷惑をかける
  - 金銭的被害を受けることも
- 重要情報を破壊・消去
  - 持ち出されたり公開されるよりまし？
  - バックアップを取っていなければ大変かも

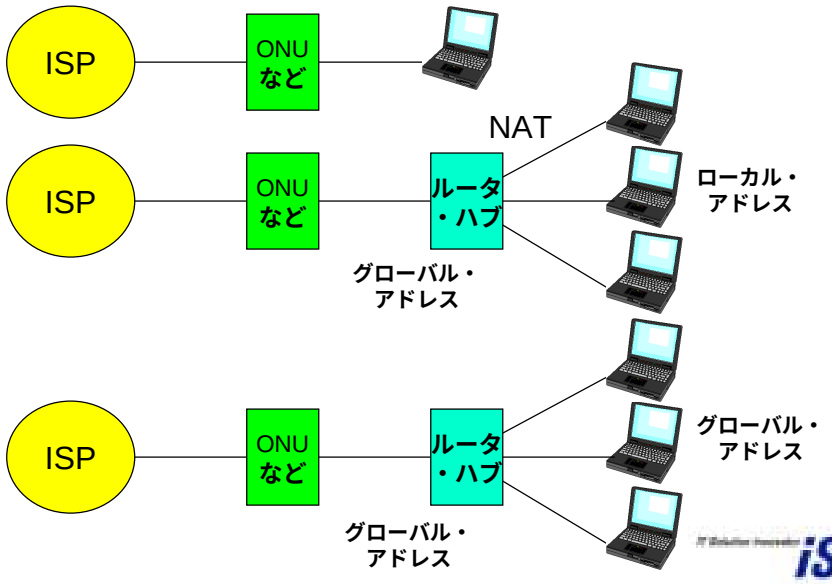
「受動的攻撃」とは

- Passive Attack
  - 自らが外部をアクセスして被害を受ける
  - ファイアウォールが機能しない
- Webアクセスに対し悪意のある情報が返される
  - セキュリティホールが突かれてトロイの木馬が稼働
  - サーバでなくても被害を受ける
  - データ破壊やデータ送出や外部攻撃
- 「変なWebサイト」じゃなくても感染
  - Webサイトが改ざんされて悪意のある情報が置かれることもある

常時接続の実際

- CATV
  - ケーブルモデムにEthernet端子
- DSL
  - DSLモデムにEthernet端子
- FTTH
  - ONU(Optical Network Unit)にEthernet端子
- これらのEthernet端子にPCやルータをつなぐ
  - 1台のPCしか接続できないサービスもある
  - IPアドレスの割り当て方法はいろいろ
  - PPPoEを使うサービスも

常時接続の構成例



IW2002-B5
23

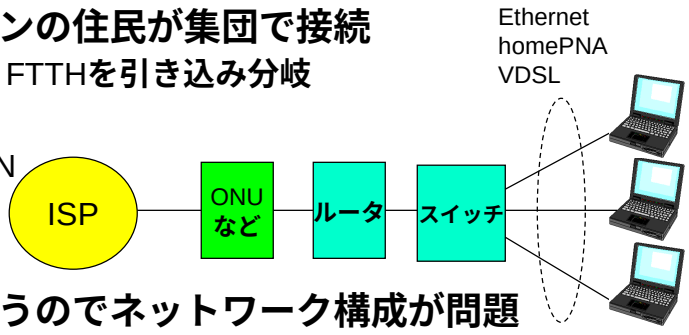
NATとは？

- Network Address Translation
  - ひとつのグローバルIPアドレスをみんなで使う
  - ルータの内側はローカルアドレス
  - インターネットからアクセスを受けるもの以外
- IPアドレス不足を解消
  - グローバルアドレスは少なくて済む
- セキュリティにも役立つ
  - 内部のマシンへは外部から直接アクセスできない
- インターネットからのアクセスを受けられない
  - 特定ポートへのアクセスを特定のマシンへ
  - 特定のマシンしか対応できない
- NATの能力に注意

IW2002-B5
24

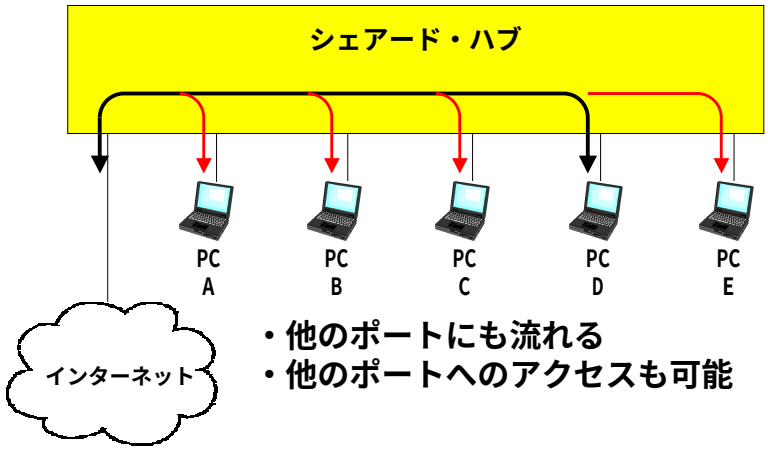
集合住宅でのブロードバンド

- マンションの各戸が単独で接続
  - ADSL
  - FTTH
  - 無線LAN
- マンションの住民が集団で接続
  - ADSL、FTTHを引き込み分岐
  - CATV
  - 無線LAN



- 他人も使うのでネットワーク構成が問題

シェアードハブは情報が漏れる



・他のポートにも流れる
・他のポートへのアクセスも可能

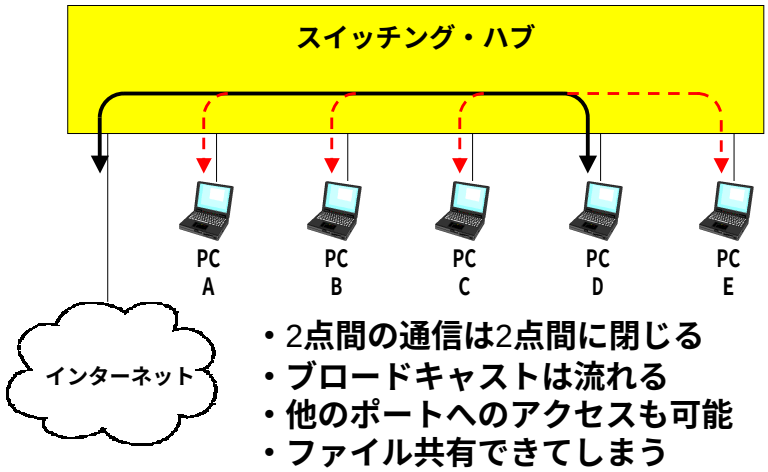
シェアード・ハブの問題点

- メディア共有は怖い
  - 同じ通信路に複数の利用者のデータが流れる
- 生のデータが見えると…
  - メールが盗聴される
  - パスワードが盗聴される
- 同様なしくみのシステムも存在
  - CATV
  - 無線LAN
  - すべてとは限らないが…
- 使い物にならないか？
  - そのままではかなり危険

IW2002-B5

27

スイッチング・ハブは？

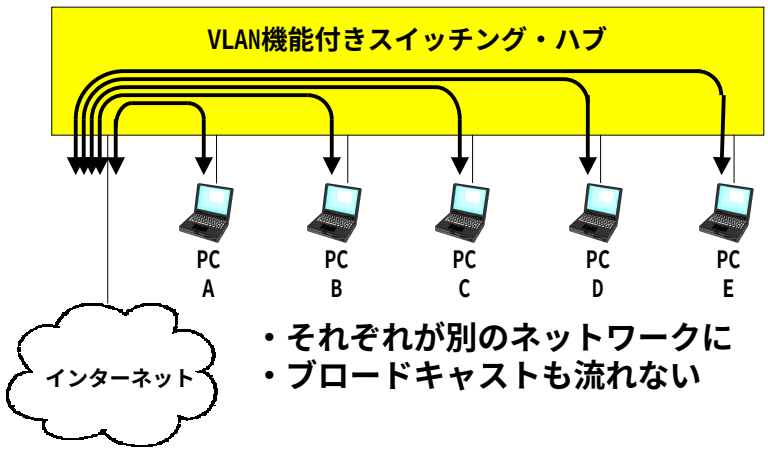


- 2点間の通信は2点間に閉じる
- ブロードキャストは流れる
- 他のポートへのアクセスも可能
- ファイル共有できてしまう

IW2002-B5

28

VLANが設定できると…



- それぞれが別のネットワークに
- ブロードキャストも流れない

IW2002-B5
29

家庭ネットワークの危機

- 危機のいろいろ
  - どんどん届くウイルスつきメール
  - ガンガンやってくる不正アクセス
  - 覗かれる無線LAN
- 多くの人がこれらの危険に気づいていない
  - 届いたメールを読むだけで感染するウイルス
  - Webサイトをアクセスするだけで感染も
  - 次々と発見される脆弱性
- 利用者の知識も意識も低い

IW2002-B5
30

パソコンはひとり1台

- 家庭でもひとり1台へ
  - 一家に1台の時代は終わる
  - 家庭内ネットワークが必要に
- セキュリティはどうするのか？
  - 守るべき機器が増える
  - ひとり一人が自分のパソコンを守るの？
  - 子供や高齢者に任せされるの？
  - ネットワークも守らなくちゃ
- 何を考えればいいのだろうか？
  - ネットワーク管理
  - 個々のパソコンのセキュリティ管理

IW2002-B5

31

外部との境界で守る

- 境界は2か所
  - ネットワークの接続点
  - パソコンの接続点
- ファイアウォール
  - 通信状況を検査する
  - 外部からのアクセスを制限
  - 内部からのアクセスを制限
  - アドレス変換(NAT)
- ウイルスチェック
  - やってくるデータを検査する
  - メール添付ファイル
  - ダウンロードファイル

IW2002-B5

32

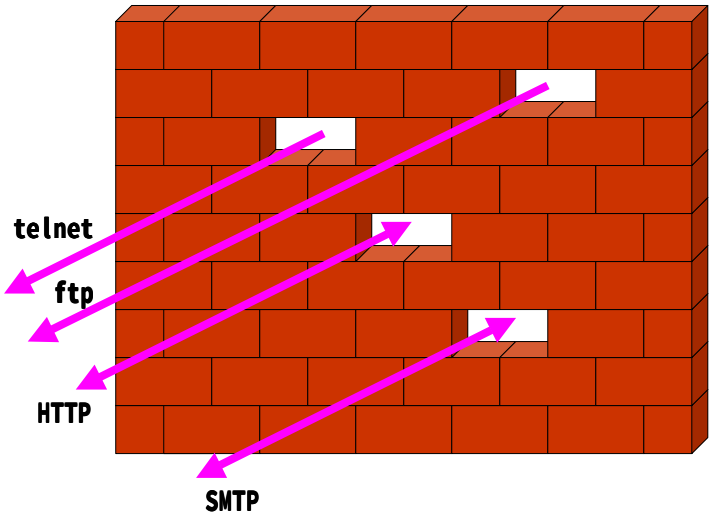
ファイアウォールとは？

- 防火壁
  - 火災が発生するとそこでくい止める
  - 普段は楽に通れる
- インターネットから家庭内ネットワークを守る
  - つながないのが一番安全
  - つながないとインターネットが使えない
  - インターネットを安全に使うための解決策
- どこに設置して何を通す(止める)かが問題
  - 管理者がしっかりと判断して設定する
  - 使い易さと安全性のトレードオフ
  - フィルタリングとSPI
    - » State-full Packet Inspection

IW2002-B5

33

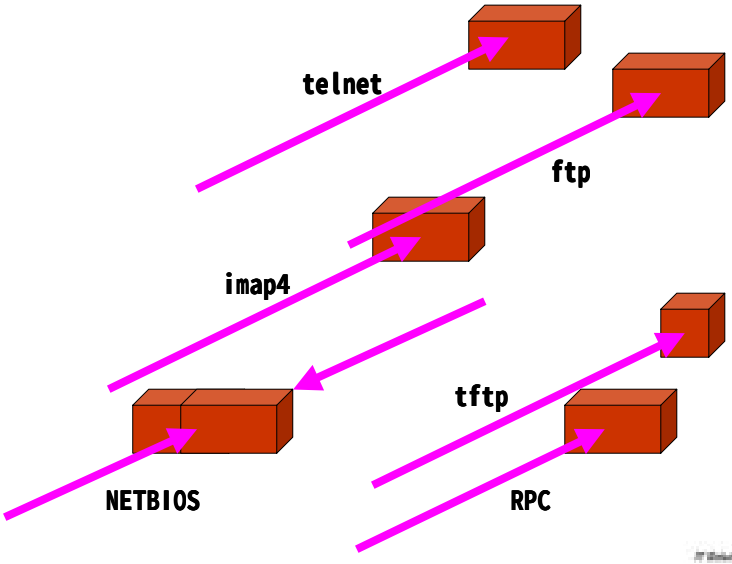
必要な通信のみを通す



IW2002-B5

34

危険な通信を止める

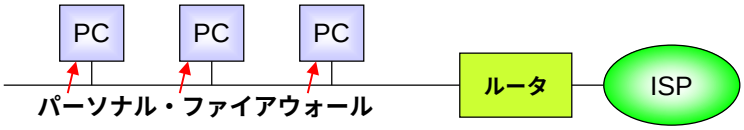


SPI

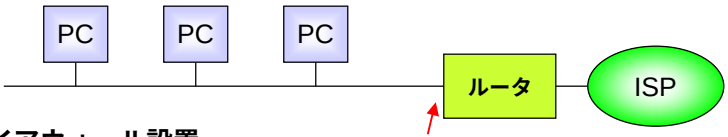
- ステートフル・パケット・インスペクション
  - IPアドレスやポート番号でフィルタリングするだけじゃダメ
  - 通信手順を理解した上でそのやりとり状況を監視
  - 偽装パケットも発見できる
- 家庭用のルータにも搭載が始まる
  - しっかり守れることが重要
  - デフォルト設定がしっかりしていないと難しい
  - 参考文献「ADSLに最適なルータはこれだ！」
    - » インターネットマガジン2002年12月号 インプレス

ファイアウォールの構成例

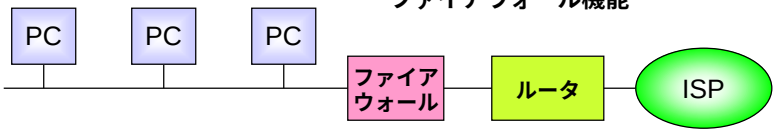
A．ファイアウォールなし



B．ルータで対応



C．ファイアウォール設置



パーソナル・ファイアウォール

- パソコン内にファイアウォール機能を載せる
  - パソコン単体で外部からのアクセスを制限できる
  - パソコン単体で外部へのアクセスを制限できる
- 個々のパソコンで守る
  - 1台が被害を受けてもほかに広がらないように
  - 必要に応じて設定を変更
  - 設定が面倒な場合が多い
  - ウイルス検知と合体していることも
- 予期しないデータ伝送を検知
  - スパイウェア対策

スパイウェアにご注意

- フリーウェアなどに組み込まれた悪質な機能
  - パソコン内の情報などを外部に送る
  - 不正行為とは限らない
  - 通常、利用規約に「情報を送ることがある」などと書かれている
  - もちろん、不正なものもある
- 安易にフリーウェアをインストールしない
  - あたりまえのこと
  - ウイルスではないので使っても危険性を感じない
  - 便利なので友人に勧めてしまうことも

IW2002-B5

39

ウイルスも凶悪化

- 伝染性を持つ悪質なプログラム
  - メールやデータファイルなどに添付されて感染
  - プログラムに組み込まれて感染
  - Webアクセスだけで実行されて感染することも
- 次第に悪質に、そして巧妙に
  - 知人からのメールなら疑わない
  - メールを読むだけで感染することも
- ウイルス・チェック・プログラムが存在
  - ウイルス・パターンでチェック
  - 発見されてからパターンが作られる
  - 新規のウイルスでは間に合わないことも

IT Solution Innovator iSiD

IW2002-B5

40

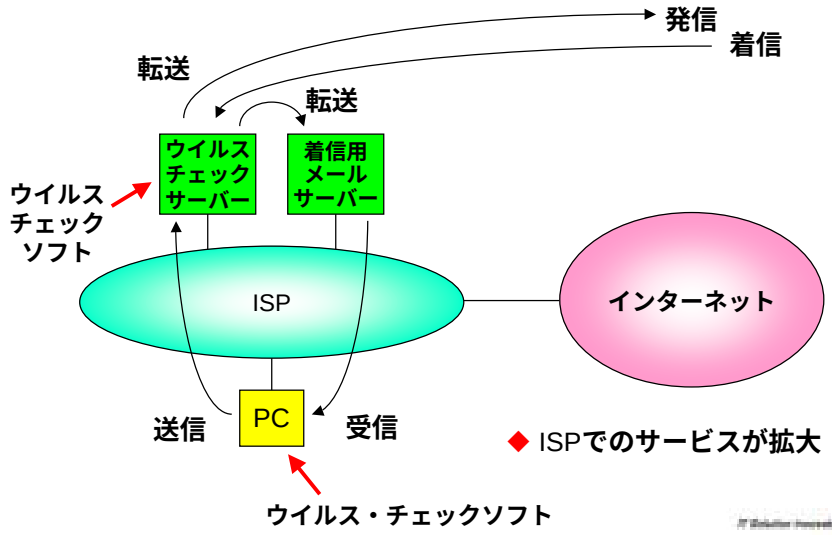
ウイルスを防ぐ

- メールゲートウェイなどでチェック
  - 家庭に入る前に感染していないか調べる
  - ISPのメール・サーバ確認
- パソコンでチェック
  - 届いたメールやファイルが感染していないか
  - 読む前に確認
- ウイルス・チェックソフトが存在
  - 新たに生まれるウイルスに関する情報を更新
  - 更新されるのはウイルスが出回ってから
- 完璧ではない
  - 怪しいメールはしばらく寝かしてから読む

IT Solution Innovator iSiD

IW2002-B5
41

メールのウイルス・チェック



◆ ISPでのサービスが拡大

IW2002-B5
42

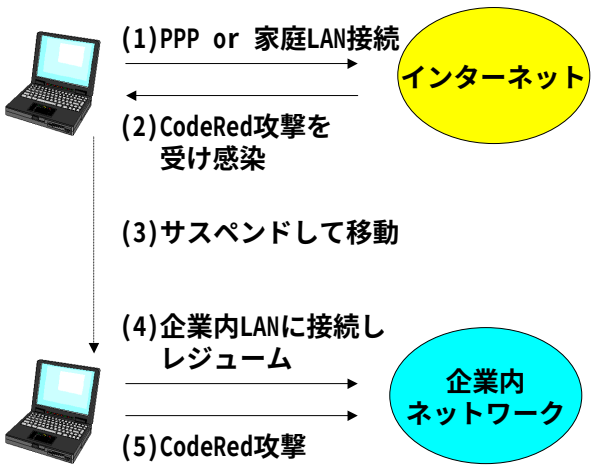
猛威をふるったCodeRed

- ◆ ウイルスではなく「ワーム」
  - 2001年7月19日にCERT/CCなどから緊急警報
    - » http://www.cert.org/advisories/CA-2001-19.html
  - 26億ドル以上という莫大な被害
- ◆ IISとIndex Serverのセキュリティホールを突く
  - すでにセキュリティ・パッチはでていた
  - CERT/CCからアナウンス 2001年6月19日
    - » http://www.cert.org/advisories/CA-2001-13.html
  - マイクロソフトからアナウンス 2001年6月18日
    - » http://www.microsoft.com/japan/technet/security/prekb.asp?sec_cd=MS01-033

被害は企業内に広がった

- 企業はファイアウォールで守られていた
  - 当然、攻撃をうけるはずがない
  - 誰もがそう信じていた
  - もちろん、セキュリティ・パッチは当てていない
  - インターネットに接続していないLANでも被害
- 被害は「裏口」から広がっていた
  - 社員が持ち込んだPCが犯人
  - インターネットに接続して感染したPCが原因
  - 社内LANにつなぐと攻撃を始める
  - 被害は急激に拡大
- 破壊行動を起こさなかったのが不幸中の幸い
  - このつぎは…

盲点だったCodeRedの感染経路



そのつぎはNimda

- Nimdaはさらに深刻
  - サーバーとクライアントを攻撃する複合型
    - » http://www.ipa.go.jp/security/topics/newvirus/nimda.html
  - ウイルス+ワーム
- InternetExplorer、OutLook、IISを攻撃
  - メールを読んだりWebアクセスだけで感染
  - 感染したクライアントがサーバーを攻撃
  - 感染したサーバーがクライアントを攻撃
  - 感染したクライアントがメールでウイルスを送る
- いずれも公表済みのセキュリティ・ホール
  - CodeRed IIが残した「裏口」も攻撃
  - CodeRed直後なのに被害が多発

Sircam

- ウイルス
  - http://www.ipa.go.jp/security/topics/sircam.html
- 感染すると以下の被害が発生
  - 10月16日に Cドライブのすべてを削除
  - 起動時にハードディスクの未使用スペースを埋める
  - MS-Word、MS-Excel などのデータファイルに感染
    - » 添付ファイルとして送信するので、 秘密情報などが漏洩
- ウイルスつきメールの送信先は
  - Outlook, Outlook Express のアドレス帳を参照
  - Webブラウザのキャッシュ内のメール・アドレス

Klez

- ウイルス
  - http://www.ipa.go.jp/security/topics/newvirus/klez.html
  - Windows32ビット環境で動作
  - Outlookのアドレス帳アドレスにメールを送信
  - ウイルスを添付
- 既知のセキュリティホールを悪用
  - Outlook ではメールを開いただけで感染
  - OutlookExpress ではプレビューしただけで感染
- 具体的な被害
  - 毎月6日に発病
  - Cドライブのファイルを削除

BugBear

- ウイルス
  - http://www.ipa.go.jp/security/topics/newvirus/bugbear.html
  - トロイの木馬
  - 自分自身のコピーをメールに添付して送信
  - 感染するとメールアドレスを収集
    - » 受信トレイや送信トレイ
    - » 特定の拡張子のファイル(tbb,eml,mbx,nch等)
  - 取得できたアドレス宛にメールを送信
- 大きな被害
  - ネットワーク共有のパソコンに感染
  - アンチウイルス製品の動作を終了
  - バックドアを仕掛けてキー入力情報を第三者が取得

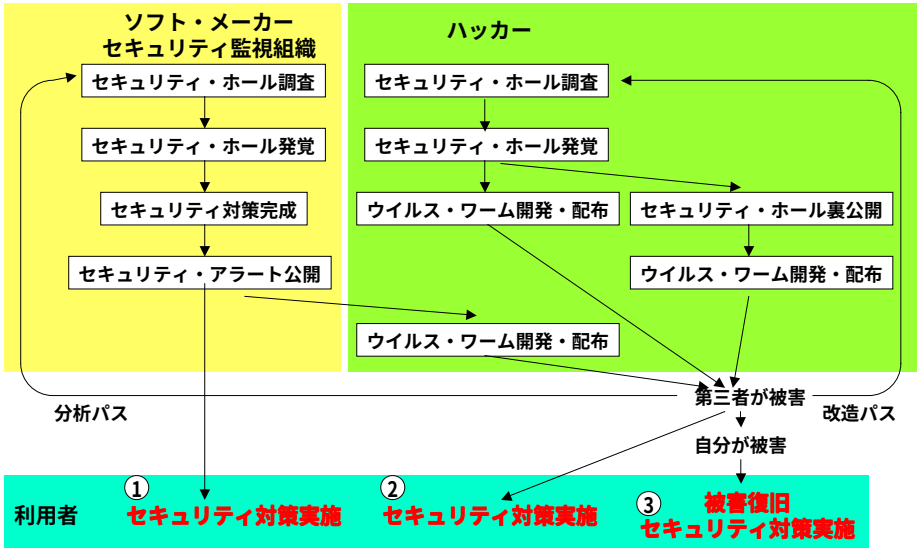
Microsoft製品が弱いのか？

- YES !?
  - いつまでたってもセキュリティ・ホールがある
  - 同社のいろんな製品で見つかる
  - 大量に使われているから狙われるという意見も
- 考えられる原因
  - プログラム規模が大きすぎて管理できていない
  - 開発段階でセキュリティが十分検討されていない
  - 新製品開発が忙しくセキュリティを考えられない
- セキュリティホールがなければ攻撃を受けない
  - セキュリティ情報がでるのが救い !?
- 方針転換で現在対策中とのこと
  - 成果を「期待」

セキュリティ情報

- ソフトウェア・メーカーや専門家が公開
  - 製品の脆弱性
    - » 自社で発見
    - » 第三者が発見
  - 脆弱性情報はハッカーにも届く
    - » この情報をもとにウイルスやワームを開発できる
- 対策ができてから公開されるのが一般的
  - 対策なしで公開されれるのはかなり危険な状態
- 脆弱性が大きいほどハッカーが喜ぶ
  - ウイルスやワームの開発にも熱が入る
- セキュリティ情報を出さないメーカーも
  - 対策を出さないメーカーは最悪

ハッカー vs. ソフト・メーカー



セキュリティ・ホール

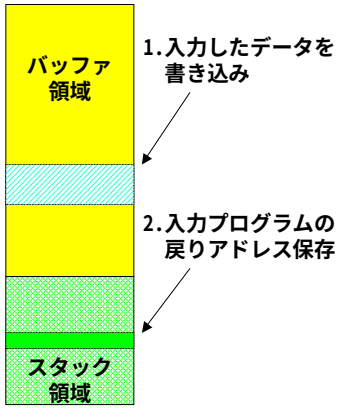
- プログラムのセキュリティ的「穴」
  - 本来は存在してはいけないバグの一種
  - 特定のデータを送り込むと予定されていない動き
  - これを利用してハッカーが侵入や命令実行
- なぜ「穴」が存在するのか
  - 安全教育が十分に行われていない
  - プログラムの規模が大きいと確認・検査が難しい
  - ハッカーはこの「穴」を探している
- 「穴」が見つかると…
  - 「穴」のふさぎ方がわかってから公表が一般的
  - すぐには公表されなかったが…
  - 最近は公表が早まる傾向

IW2002-B5

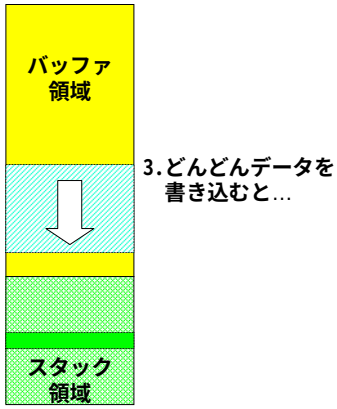
53

バッファ・オーバー・フロー

A)チェックが十分でない
入力プログラムを悪用



B)想定を越えたデータを
与えていく

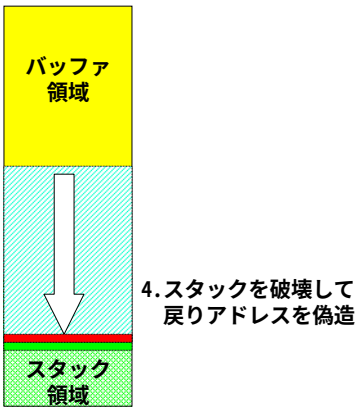


IW2002-B5

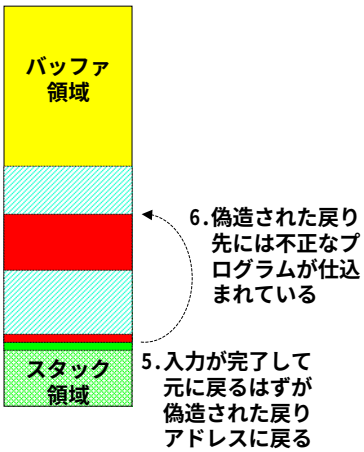
54

バッファ・オーバー・フロー

C)ついにはスタックを
破壊



D)不正なプログラムが
実行される



IW2002-B5
55

パソコン自身で守る

- 軟弱なパソコンは攻撃に弱い
  - パソコンを丈夫にする
  - 弱点をなくす
- 実際はあちこちに弱点が潜む
  - ときどき発見されて対策が公開される
  - きっちりと対策していくことが重要
  - それがセキュリティ・パッチ
- 普段から弱点情報に注目する
  - 問題があれば改善する
  - 古いOSは捨てた方がいいかも
- セキュリティ・ホールがなくなればかなり安全
  - もちろん利用者の注意は必要

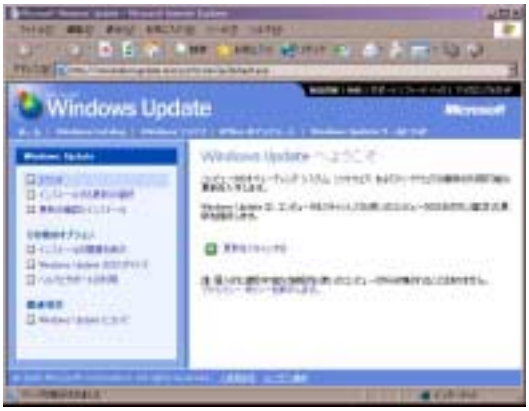
IW2002-B5
56

セキュリティ・パッチ

- どんどんでてくるセキュリティ・パッチ
  - 毎日のように確認しなければならない
  - どれを当てればいいのか分からない
- これまでは…
  - 被害の報告がでてからでも間に合った
  - 最初に攻撃を受けるのは官公庁や大企業だった
- ランダムに攻撃されると1番目は自分かも
  - 「備えなければ憂いあり」
- セキュリティ・パッチを当てれば安心？
  - バージョンアップで元に戻ることも
  - セキュリティ・パッチで動かなくなるアプリも

Windows Update

- いつもWindowsを最新の状況に
  - 最近のWindowsの基本機能
  - 自動的に更新情報を探してくれる



家庭にもサーバーを

- せっかくだからWebサーバーを置きたい
  - 自分のホームページを自宅で運用
  - 家族の写真を見てほしい
  - 趣味を知ってほしい
- 家庭内の情報を外出先から利用したい
  - 友人の住所録や電話番号
  - 自分の銀行口座番号やクレジットカード番号
  - 手帳を持って歩くのは面倒
  - インターネットからアクセスできると便利
  - ファイル共有できるとめちゃくちゃ便利

IW2002-B5
59

サーバーは狙われている

- 外部からアクセスできるマシンは危ない
  - ファイアウォールの内側のマシンでも攻撃
  - 特定のポートしか開いていなくてもそこから攻撃
- 攻撃のパターン
  - セキュリティ・ホールを突く
  - 設定ミスを突く
  - 甘いCGI(Common Gateway Interface)を攻める
- ファイアウォールだけでは防ぎきれない
  - 正しい設定
  - 確実な監視
  - それなりの知識が必要

IW2002-B5
60

ポート・スキャンが襲う

- サーバーで動いているプログラムを探し出す
  - プログラムが稼働していないと攻撃は不可能
  - 稼働しているプログラムの弱点をつく
  - プログラムごとに利用するポートが違う
- ポートを探すからポート・スキャン
  - ポートに順番にアクセスして答えるポートを探す
  - そこに攻撃を仕掛ける
- 攻撃用フリーウェアが配布されている
  - だれでもが簡単にポート・スキャンできる
  - 自分のサイトをスキャンしてチェック
  - 他人をスキャンすると「攻撃」と見られる

IW2002-B5

61

サーバーを守ろう

- ファイアウォールで守る
  - 不要な通信を許さない
  - 必要な通信だけを通す
- サーバー自身で守る
  - 通信を許さないと通信できないのでそこが狙われる
  - セキュリティ・ホールをふさぐ
  - 不要なプロセスを止める
  - 攻撃を検知する
    - » ログでアクセス状況を監視
- 知らないうちにサーバーが稼働していることも
  - 自分のマシンは自分で「管理」する

IW2002-B5

62

より安全なサーバーに

- サーバーは攻撃を受ける
  - アクセスを待ち受けているから
  - サーバーにセキュリティ・ホールがあることを期待
- 使っていないサービスが危ない
  - ちゃんと管理していないから
  - 動いていることに気づかないことも
  - 自分で調べて止める
- よく分からなければサーバーを立ち上げない
  - 結局、家族に跳ね返ってくる
  - どうしても使いたければ「勉強」する

IW2002-B5

63

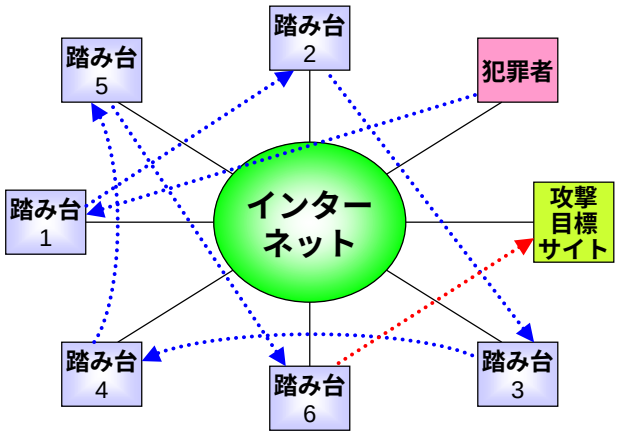
踏み台に注意

- 踏み台って何？
  - 誰かが侵入するが、破壊も盗みもしない
  - そこからさらにほかへ侵入する
- 被害はないのか？
  - 踏まれただけでは表面的な被害はゼロ
  - これだけでは痛くもかゆくもない
  - だから気づきにくい
- それで…
  - つぎに侵入されたところからは侵入者に見える
  - 犯人扱いされてしまう→告訴される危険もある
  - 他の組織に大きな迷惑をかけることになる

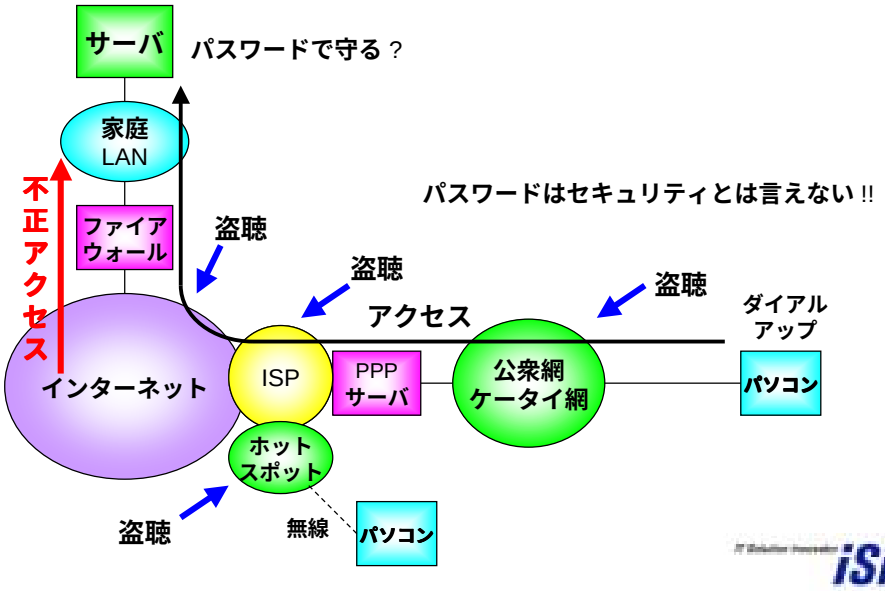
IW2002-B5

64

踏み台の実際



外から自宅をアクセスしたい



認証と暗号化

- 外部からの接続は危険
  - 自分が接続できるということは他人も接続可能
  - 本人を確認するしくみが重要
  - パスワードだけではダメ → 繰り返して試せるから
  - 例えばワンタイム・パスワード
- インターネットの通信は盗聴可能
  - 安全な認証の後に通信路を暗号化したい
  - 暗号の強度が十分であれば安心
  - 例えばセキュア・シェル(SSH)
    - » http://www.ipsec.co.jp/
  - 例えばSSL
    - » http://www.orangesoft.co.jp/wstunnel/index.html

IW2002-B5

67

SSLの機能

- 通信路を暗号化
  - Secure Sockets Layer
    - » サーバーとブラウザ間の通信を暗号化する
    - » クレジットカード情報などを暗号化して送る技術
  - Web用ということではない
    - » いろんな用途に使える
- サーバーが本物であることを証明
  - 電子署名によって
  - 証明者が信用できなければ意味がない
  - ショッピングサイトが信用できなければ意味がない
  - 利用する都度確認することが必要
- クライアントが本物であることを確認

IW2002-B5

68

盗聴による被害

- メールを読まれる
  - なぜそのことを知っているの？
  - どうもおかしい
- パスワードを盗まれる
  - いろいろと悪用が可能
  - メール、コンピュータ、…
- クレジットカード番号を盗まれる
  - 勝手に使われてしまうと
- 盗聴されても分からない
  - 証拠が残らない
  - 気づかない

IW2002-B5
69

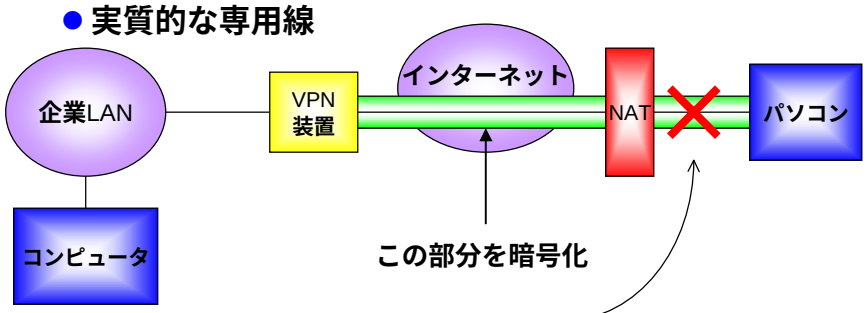
盗聴は可能なのか？

- 何を盗聴するのか？
  - メール
  - クレジットカード番号
  - すべての通信
- 盗聴場所は
  - 接続しているISP
  - 経路のISP
  - 相手のマンション内LAN
  - 通信会社
  - ホットスポット
  - サーバー

IW2002-B5
70

VPN

- Virtual Private Network
  - インターネットの通信路を暗号化
  - 実質的な専用線

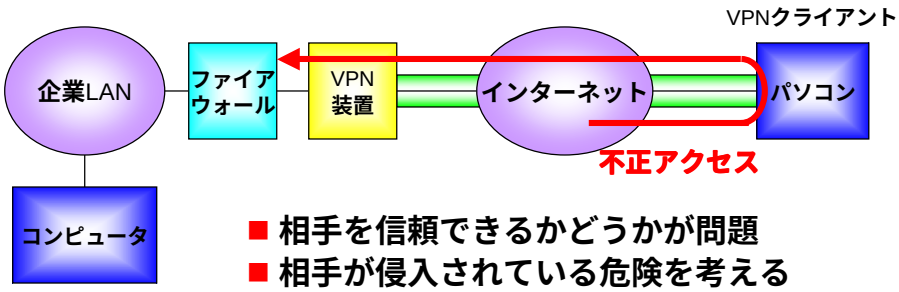


■NATの壁が越えられない
  ✧ホテルや自宅で
  ✧ポートフォワーディングでできる場合も
■グローバルアドレスがほしい

IW2002-B5
71

VPNって大丈夫？

- 外出先と自宅
- 自宅と会社



- 相手を信頼できるかどうかが問題
- 相手が侵入されている危険を考える
- VPNの内側もファイアウォールで守ろう
- 許可するアクセスを考えよう

IW2002-B5
72

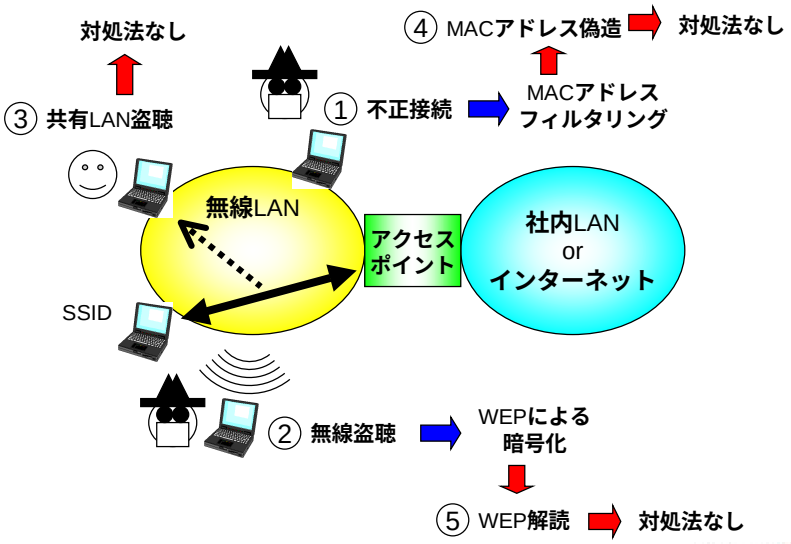
無線LANも怖い

- 802.11bは2.4GHz(IMS)帯を利用
  - 11Mbpsと高速
  - PCMCIAやUSBで接続　→　簡単で便利
  - 免許不要で使用している機器も多い
  - 大量生産で低価格化が進む
- 便利だけれど…
  - 電波はけっこう遠くへも届く
  - 盗聴が心配
  - 不正アクセスが心配
  - 暗号機能に脆弱性があるという話も
    - » RC4という暗号方式の弱点
    - » http://airsnort.sourceforge.net/

IW2002-B5

73

無線LANの脆弱性



IW2002-B5

74

脆弱性の指摘はいろいろ

- **カリフォルニア大学バークレイ校ISAACが警告**
  - 2001年1月30日
  - Internet Security, Applications, Authentication and Cryptography
  - http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- **メリーランド大学が警告**
  - 2001年3月30日
  - http://www.cs.umd.edu/%7Ewaa/wireless.pdf
  - **シスコ社の解説が分かりやすい**
    http://www.cisco.com/japanese/warp/public/3/jp/product/product/wireless/ao350ap/prodlit/1327_pp.html#a002

IW2002-B5

75

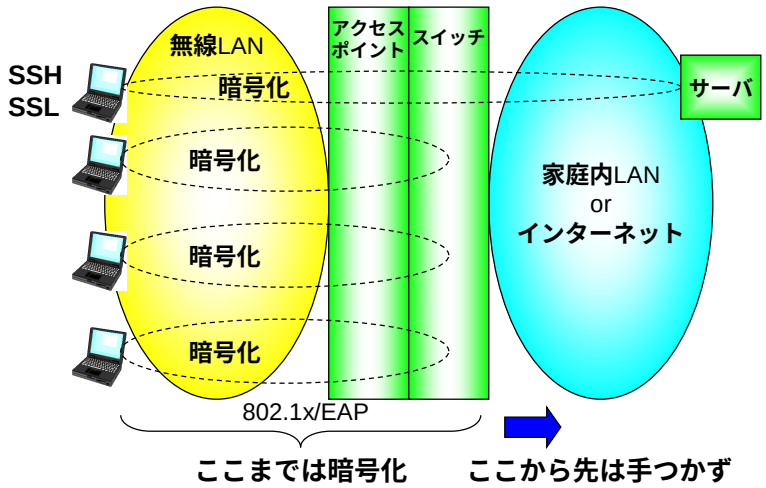
実際あちこちで電波を拾える

- つながってしまう親機も多い
  - 勝手に使ってもいいのか？
  - 個人が無料開放する親機もある
  - 盗聴されている危険もある
- 設定ミスも多い
  - 不正アクセスになるのか？
  - 誰かが勝手にアクセスしているかも
- ホットスポットは怖い
  - 共有ネットワークで盗聴の危険
  - 喫茶店で大声で打ち合わせするのと同じ
  - 誰かがとなりで聞き耳を立てているかも

IW2002-B5

76

802.1x/EAP

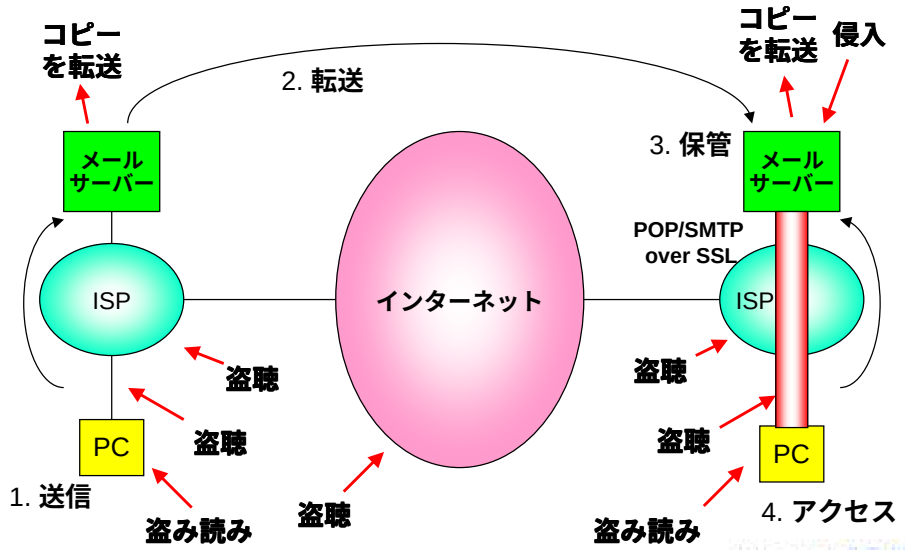


これでも安全ではない !!

IW2002-B5

77

メールを盗聴から守る



IW2002-B5

78

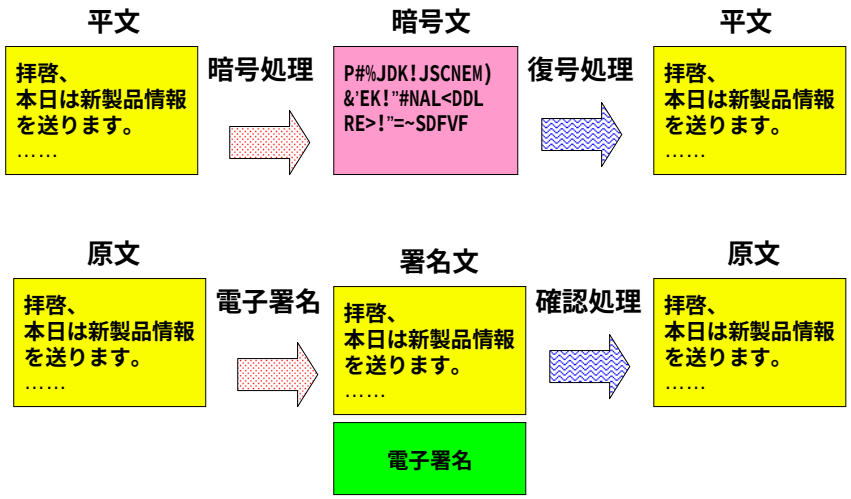
メールシステムは脆弱

- メールに多くのリスクが存在
  - 暗号化されていないから盗聴される
  - 発信者を確認できないからなりすまされる
  - 書き替え可能だから改ざんされる
  - 管理者なら読めてしまう
- 暗号電子メールもあるが普及していない
  - PGP(Pretty Good Privacy)
  - S/MIME(Secure/MIME)
    - » MIME → Multipurpose Internet Mail Extensions
- メーラで暗号処理
  - 電文の暗号化
  - 電子署名で発信人確認と改ざん検出

IW2002-B5

79

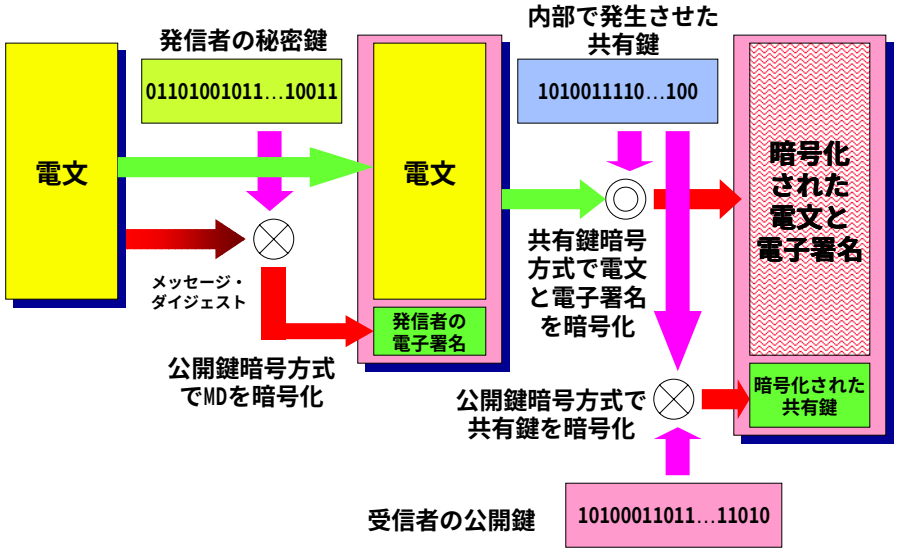
暗号メールの使い方



IW2002-B5

80

暗号化メールのしくみ



IW2002-B5

81

インターネットで使う暗号技術

- 暗号の利用方法
  - 通信経路で盗聴されても分からない ー 暗号
  - ネットワーク越しは相手が見えない ー 認証
  - 電子情報は書き換えても分からない ー 改ざん発見
- 共有鍵暗号方式
  - 電文の暗号化に利用する
    - » DES, TripleDES, ISEA, RC2, RC4, MISTY, FEAL, CAST
- 公開鍵暗号方式
  - 認証と共有鍵の暗号化に利用する
    - » RSA, Diffie-Hellman, ElGamal
- メッセージ・ダイジェスト
  - 改ざん発見に利用する
    - » SHA-1,MD5

IW2002-B5

82

暗号を破る

- もともと復号できるものだから
  - 関係者は解読できて当たりまえ
  - 第三者が解読すると「暗号破り」
- どのように破るのか？
  - 力ずく → すべての組み合わせを試せば必ず解ける
  - しくみの弱点を突く → 錠は上部でも蝶番が弱い
  - バグを突く → 暗号は強力だけど実装を間違えた
- 安全性の確認されていない暗号は危険
  - この暗号は破られていない → 誰も挑戦していない

IW2002-B5

83

暗号鍵の長さと組み合わせの数

40ビット	1,099,511,627,776
56ビット	72,057,594,037,927,936
64ビット	18,446,744,073,709,551,616
128ビット	340,282,366,920,938,463,463,374,607,431,768,211,456

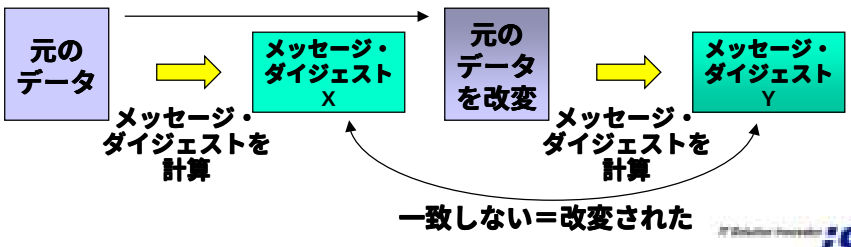
・力ずくで解読するには組み合わせが多いほど難しい

IW2002-B5

84

電子署名とは

- 電子的な署名で発信者が本物であることを確認
  - 署名があるから成りすましができない
  - 公開鍵暗号技術を使用
- メッセージ・ダイジェストで改ざんを発見
  - 電文に計算処理をして128～160ビットの数値を得る
  - この数値を変えないように電文を変えるのは困難



IW2002-B5

85

PKIを利用する

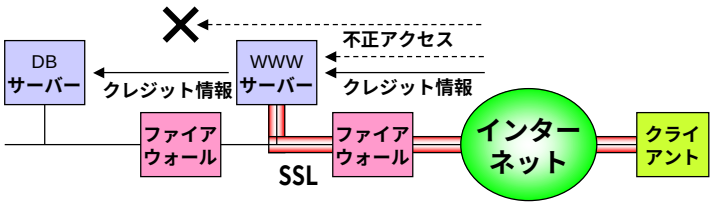
- Public Key Infrastructure
  - 公開鍵暗号基盤 と訳す
  - 電子認証のためのインフラ
- 認証
  - Webサーバーが本物である
  - 電子メールの発信人が本物である
  - ネーム・サーバー情報の発信人が本物である
  - ルーティング情報の発信人は本物である
  - ドライバの作成者が本物である
  - VPNの相手が本物である
- インターネット経由のあらゆる認証で使われる
  - 利用はどんどん広がるはず

IW2002-B5

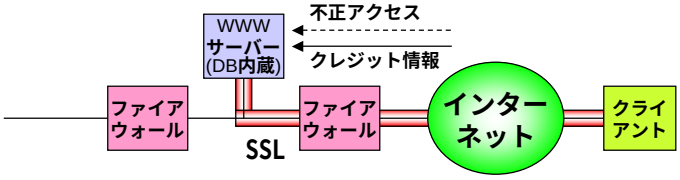
86

インターネットでお買い物

A．一般的な構成



B．危険な構成



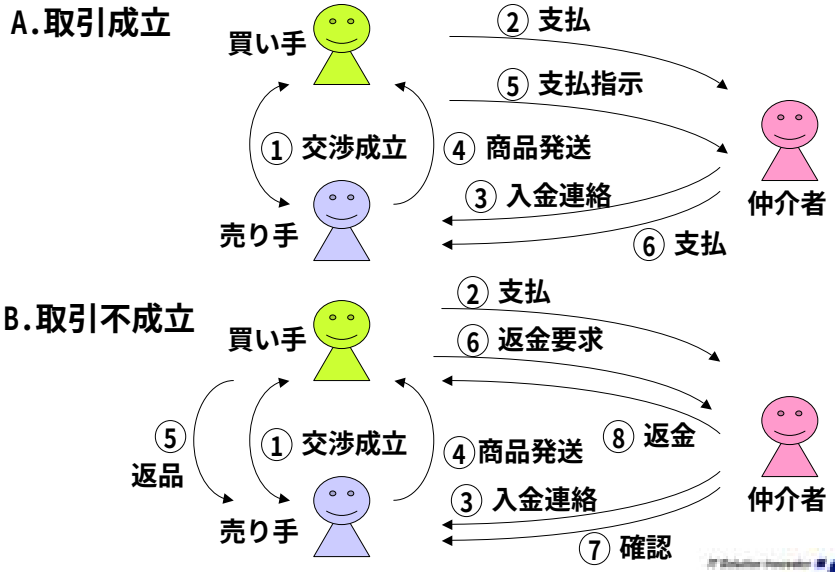
SSLを使えば安心？

- 「当サイトはSSL対応なので安心です」
  - 通信路での盗聴は難しいが…
  - ショッピング・サイトに届いてからが問題
    - » 侵入や攻撃によるファイルの窃盗
    - » 従業員による顧客DBの持ち出しなど
- 詐欺が目的のショッピングサイトの可能性も
  - 企業としての信用力
  - サイトを守れるそれなりの技術力
  - どうしても買いたければそれなりの覚悟で
    - » 代引きを活用するとか
  - インターネットで買わないといけないのか？
  - 相手が個人ならなおさら
    - » たとえばオークション

詐欺による被害

- 購入した「はず」の商品が届かない
  - 売り主に連絡が取れない
  - 売り主の連絡先がわからない
  - 売り主が倒産
  - オークション・サイトが責任をとってくれない
- 「試用」は無料といわれたのに課金された
  - 「試用」でカード番号を教えてしまった
  - キャンセルする方法がわからない
- クレジットカードに身に覚えのない課金
  - カード会社はとりあってくれない

エスクロウのしくみ



Unsolicited Commercial Email

- 一般にはSPAMと呼ばれている
  - SPAMはハムの缶詰
  - インターネットとの関係は？
- 勝手に送られてくる広告メール
  - メール・アドレスが販売されている
  - 効果があると勘違いしている
- 受信者に通信コスト負担を強いる
  - 発信コストは安いが受信者は迷惑
  - FAXによるDMと同じように問題
- 勝手に広告を送りつける企業からは買わない
  - 効果がなければなくなる？

IW2002-B5
91

SPAMer保護法成立

- 特定電子メールの送信の適正化等に関する法律
  - 「未承諾広告※」をつければ勝手に送れる
  - SPAMの送信が法律で認められた
  - フィルタリングできるはずだが…
- 到達性が不確実なメールアドレスに送る
  - 不要なのでメールアドレスをSPAMerに通知すると…
  - SPAMerは到達性のあるメールアドレスを収集
  - SPAMerは名前を変えればそこに送信可能
  - メールアドレスを他の業者に転売
- オプト・インとすべき
  - 広告メールをほしいという人だけに送るべき
  - とりあえず送るというのはやめてほしい

IW2002-B5
92

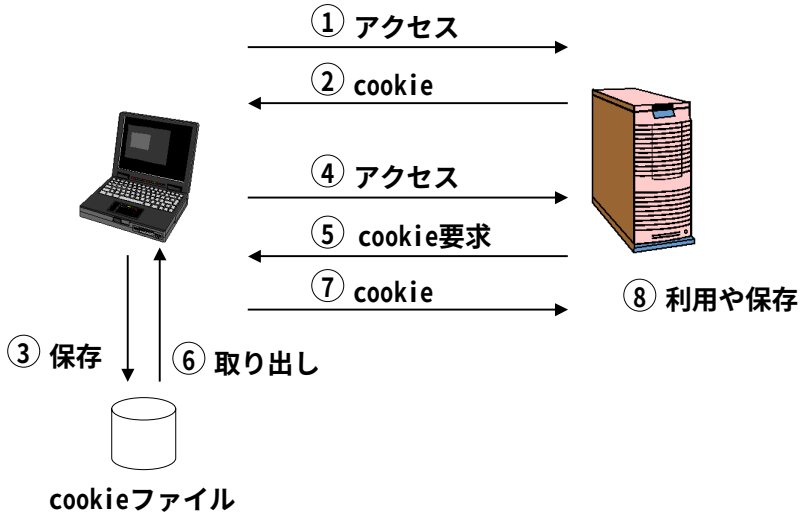
プライバシーと住基ネット

- 妙な妥協が意味のないシステムを作った
  - 変更可能な「背番号」
  - 民間活用ができない法規制
  - 「稼働」が最大の目的になってしまった
- 根本的な問題が放置された
  - システムが個人情報保護に無頓着
  - 窓口の「人」のレベルが低いという現実を無視
  - 勝手に機能が肥大するという国民の危機感を無視
- のど元過ぎれば…
  - すでにマスコミは忘れているかも
  - このままでは、プライバシーが危ない

プライバシーが狙われている

- Cookieでクライアントを特定
  - Webをアクセスするとクライアントに送られる
- どうなるの？
  - アクセス状況をサーバー保有者に把握されてしまう
  - アンケートなどに答えて氏名を明かしていると…
    - » アクセス状況が個人にひもづけされる
- 拒否したほうがいいの？
  - プライバシーに関する考え方次第
  - 拒否するとアクセスできないサイトもある
  - 保存されないCookieも
- 固定IPアドレスはもっと危険

クッキーのしくみ



ブラウザ側で扱いを決める

Netscape7.0の例

固定IPアドレスの問題

- 固定IPアドレスは便利
  - サーバーを設置できる
  - 相手からアクセスを受けつけられる
  - ドメイン名を登録できる
- サイト情報がJPNICに登録される
  - 電話帳のように非公開にできない
  - 一部の情報は非公開だが
- 何が起こるのか？
  - アクセス元を「登録情報」として把握される
  - 技術連絡担当者の連絡先も把握される
    - » 氏名、電話番号、メール・アドレス
    - » 勤務先が分かることも

IW2002-B5
97

プライバシーを守る

- 日本人はプライバシーに無頓着？
  - 電話帳、各種名簿、Web、アンケート、プレゼント
    - » すぐに情報を出してしまう
  - 個人情報が簡単に集められる
- 個人情報の公開範囲を決める
  - 公開する相手、内容、得られる効果を見極めて
- 二次的、三次的影響も考える
  - どのように利用されるのか
  - どこまで流用されるのか
  - 流れ出すと止められない
- クレジットカード情報は特に注意
  - インターネットだけとは限らない

IT Solution Innovator iSiD

IW2002-B5
98

プライバシーとサービス

- プライバシーを渡してサービスを得る
  - 個人情報を渡してポイントやプレゼントをもらう
  - 個人情報で細かいサービスができる
- ご用聞きモデル
  - 顧客の特性を把握している
  - これがほしいという前に手を打ってくれる
  - 他でしゃべられると困る
- Self Service Gas Stationモデル
  - 自分のことは自分でやるから放っておいてほしい
- マクドモデル
  - 「ポテトもどうですか？」

IT Solution Innovator iSiD

プライバシー・ポリシーとは

- プライバシーを守るための方針
  - どのような情報を集めるのか
  - どのような情報は集めないのか
  - どのような目的で情報を集めるのか
  - どのような手段で情報を集めるのか
  - その情報をどのように利用するのか
  - 集めた情報をどのような危機から守るのか
  - 利用し終わった情報はどのように廃棄するのか
  - その企業が存続しなくなったときにどう扱うのか
- 最近は「ポリシー」を掲げる企業が急増

プライバシー・マーク

- 財団法人日本情報処理開発協会が認定
  - http://www.jipdec.or.jp/security/privacy/
    - 「電子計算機処理に係る個人情報の適切な保護のための体制を整備している事業者に申請により認定し付与」
  - JIS Q15001
    - 個人情報保護に関するコンプライアンス・プログラムの要求事項
  - 国内に活動拠点を持つ民間事業者
    - JIS Q 15001に準拠したコンプライアンス・プログラムを定めていること
    - コンプライアンス・プログラムに基づき実施可能な体制が整備されて個人情報の適切な取扱いが行なわれていること
- マークがあるから完璧とは限らないかも ？
  - 目安のひとつ

セキュリティは危機管理の一部

- 危機管理の実際
  - 危機を認識する
  - 危機発生時の被害を予測する
  - 危機に陥らない方法を考える
  - 逃れられない危機であれば，被害を最小限に抑える方法を考える
  - 危機に陥ったなら状況を分析する
  - 危機に陥ったなら被害を最小限に抑える措置を講じる
  - 危機から最短で復旧する方法を考える
- 個人や家庭においても危機管理は重要

参考URL・参考文献

- 情報処理振興事業協会セキュリティセンター
  - http://www.ipa.go.jp/security/index.html
- JPCERT/CC
  - http://www.jpcert.or.jp/
- 首相官邸高度情報社会推進本部
  - http://www.kantei.go.jp/jp/it/security/index.html
- 経済産業省情報セキュリティ政策関連のページ
  - http://www.meti.go.jp/kohosys/topics/10000098/
- 日経ネットワークセキュリティ2003
  - 日経BPムック 日経BP社 本体1,480円