常時接続時代の セキュリティ入門

Internet Week 2001

(株)電通国際情報サービス

熊谷誠治

kuma@isid.co.jp

セッション概要

- ブロードバンドが注目を集める中、家庭へもインターネットの常時接続が浸透し始めている。だれでもが常時接続を手に入れられることで、インターネットの便利さを享受できるようになる。一方で、常時接続はインターネット側からアクセスがやってくる可能性が高くなるため、CodeRedで明らかになったように、正しく防御していないとリスクが伴うことを忘れてはならない。本セッションでは、家庭に常時接続インターネットがやってくるときに発生するであろうセキュリティ問題に関して、その重要性と危険性をやさしく解説し、セキュリティ意識を持つための発想法を提案する。
- 具体的なセキュリティ対策には触れないが、用語の意味を含め、常時接続にあたって知っておいた方がいいセキュリティの概要やプライバシー問題をひととおり説明する。常時接続を考えているインターネット初心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
  - 社員が常時接続を利用している企業のネットワーク管理者

IW2001-B2
3

セキュリティとは

- 辞書(EXCEED 英和辞典)で引くと…
  - se・cu・ri・ty
  - n.安全(from); 安心;[古]油断; 確実; 保護, 保安; 防衛(策) (against; from);
  - 【コンピュータ】安全保護(無断でデータにアクセスできないようにすること); 保証(金・人); 担保(品); 借用証(for); (pl.)証券, 証書, 債券.
- 安全を守ることらしい
  - 安全といわれると重要かと思うが…

IW2001-B2
4

なぜセキュリティなのか？

- インターネットの普及で意識が高まる
  - 利用者が増えれば犯罪者も増える
  - 犯罪だという認識がない犯罪者も
- 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も急増
- しっかり守れといわれても…
  - どうすればいいかわからない
  - 独学では限界も
  - 素人が学ぶスピードよりも犯罪者の進歩が早い
  - 本当に危険なの？

IW2001-B2
5

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
  - 月額固定料金制
  - 着信可能
- 企業はこれまでも常時接続
  - 予算化が楽な定額制
  - Webサーバーを設置可能
- 最近は個人も常時接続へ
  - 安価なサービスが登場
  - 個人にとっても便利

IW2001-B2
6

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
- 会社よりも自宅のインターネットの方が速い
  - 速いことはいいことだ
  - 会社はWebとメール程度
  - インターネット中継やMP3は「あそび」

IW2001-B2

7

個人をとりまく環境

- 会社よりも自宅のインターネットが速い
  - 会社は1.5Mbps、自宅は8Mbps
  - 会社は500人、自宅はせいぜい数人
  - この差は大きい
- 低価格で利用可能
  - 競争のおかげでコストが低下傾向
  - 投資の拡大で利用可能範囲が拡大
- 速いことはいいこと
  - 無駄な時間をなくして仕事の効率アップ
  - イライラがなくなって気分爽快
  - 乗っ取られると攻撃も高速にできる

IT Solution Innovator iSiD

IW2001-B2

8

ブロードバンドでできること

- ファイルダウンロード
  - MP3、映像コンテンツ、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

IT Solution Innovator iSiD

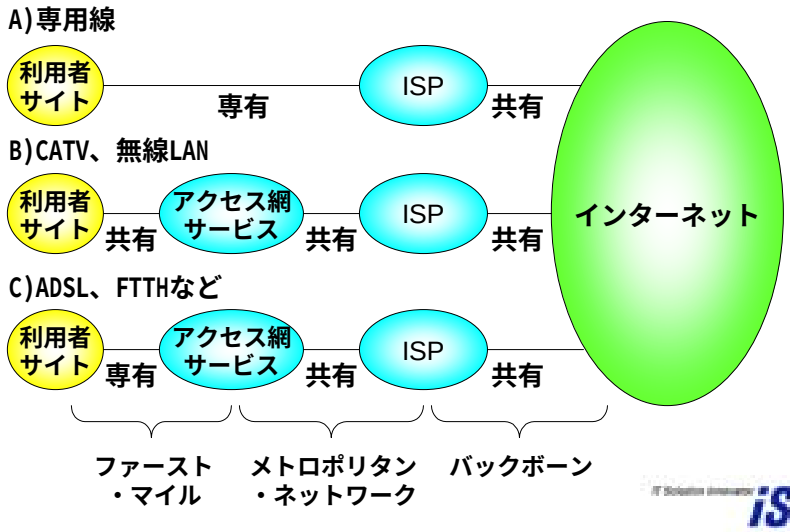
IW2001-B2
9

ファースト・マイルの技術

- ADSL (Asymmetric Digital Subscriber Line)
  - 電話線(銅線)
- CATV
  - 同軸ケーブル、光ファイバ
- 衛星
  - 電波
- FWA (Fixed Wireless Access)
  - 電波
- FTTH (Fiber To The Home)
  - 光ファイバ
- Ethernet
  - 光ファイバ

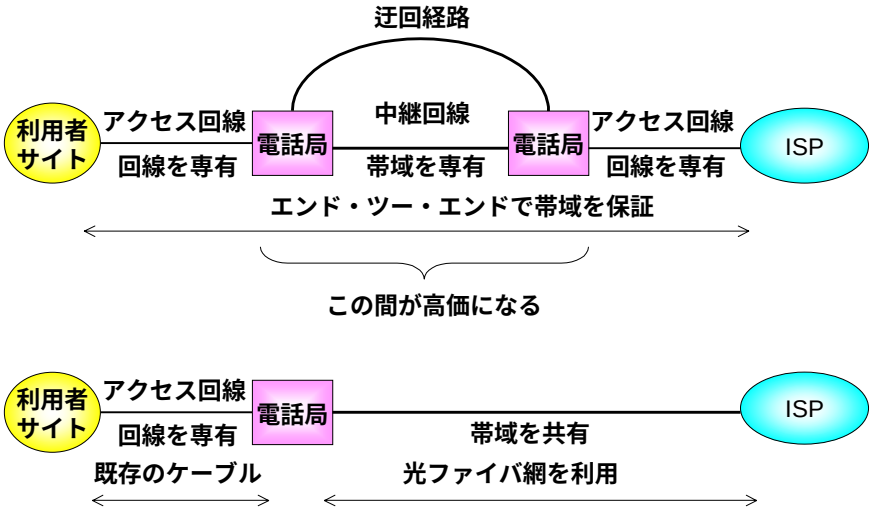
IW2001-B2
10

通信路を共有してコストダウン



IW2001-B2
11

電話システム(専用線)は高価



IW2001-B2
12

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
- 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
- 既設のマンションでは難しいことも
  - 建物本体に貫通工事やケーブル敷設が必要なことも
  - 共有スペースへの機器設置が必要なことも

IW2001-B2

13

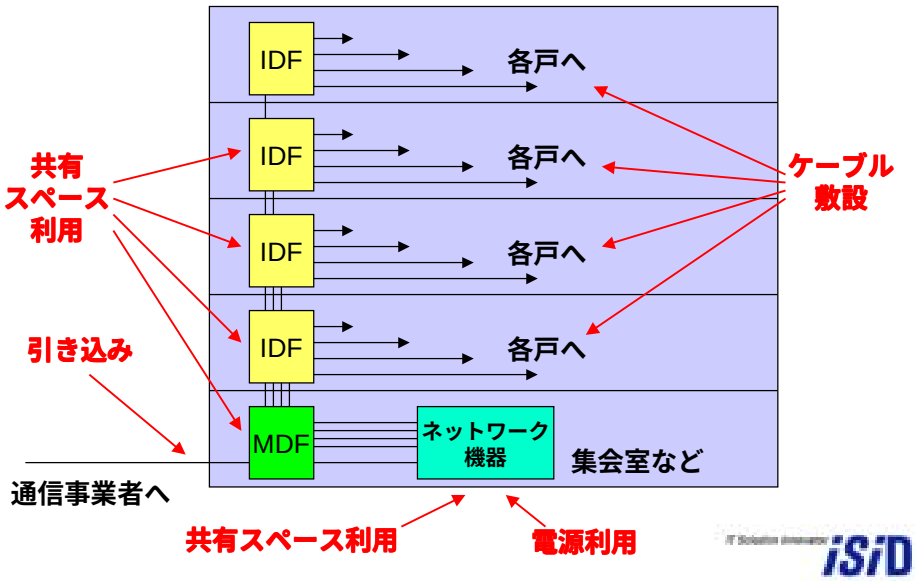
集合住宅での注意点

- 引き込み路が用意されていない
  - 新たな管路の設置
  - 構造体である壁の貫通
  - ケーブルを露出配線
- ネットワーク機器を集会室に設置する
  - 一部の住民が集会室などの一部を占拠することに
  - 電気代の支払い
  - セキュリティ
- 利用のためには住民の合意が必要なケースが
  - 1/2とか2/3とか全員とか
  - なかなかタフ

IW2001-B2

14

集合住宅での問題



IW2001-B2

15

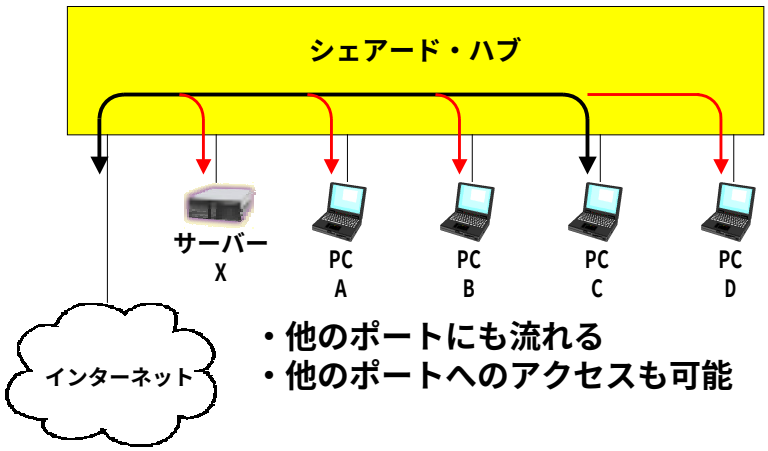
新築マンションの問題点

- 導入されているサービスが貧弱なことがある
  - マンション全体で1.5Mbpsとか128kbpsとかも
  - 100Mbpsでも300戸で使うと…
- 管理費に組み込まれている
  - コストダウンに追従してもらえない
  - 性能向上に追従してもらえない
  - 管理業務委託企業が利益確保に走る
- 利用者の大半が技術に疎い
  - 変更には管理組合の合意が必要
  - 管理業務委託先も技術に疎い
  - シェアード・ハブを使っているマンションも

IW2001-B2

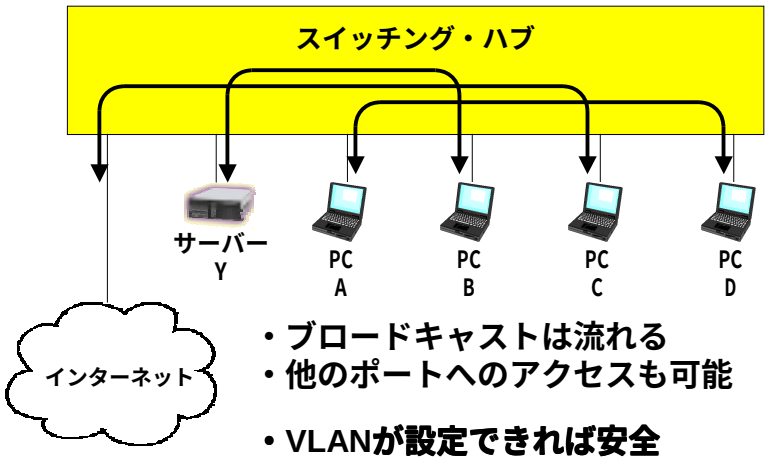
16

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

スイッチング・ハブで守る



- 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
- VLANが設定できれば安全

メディア共有の問題点

- シェアード・ハブと同じしくみのシステムも
  - ケーブル・テレビ
  - 無線LAN
  - すべてとは限らないが…
- 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
- 使い物にならないか？
  - そのままでは盗聴の危険がある
  - そのままではファイル共有される危険もある
  - 「そのままに」しない方法は？

IW2001-B2

19

無線LAN

- 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/

IW2001-B2

20

セキュリティ・モデルの変化

- 狙われるのは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
- 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

IW2001-B2

21

攻撃が変わる

- 2000年1月　官公庁Web改ざん事件
  - セキュリティ・ホールを突く
  - 目標を定めて攻撃
  - 相手の信用失墜と自己顕示
- 2001年7月　Sircam
  - メールの添付ファイルで伝搬
  - PC内部の情報を外部へメールで送信
- 2001年8月　CodeRed
- 2001年9月　Nimda
  - セキュリティ・ホールを突く
  - 無差別に攻撃
  - 自動的に攻撃

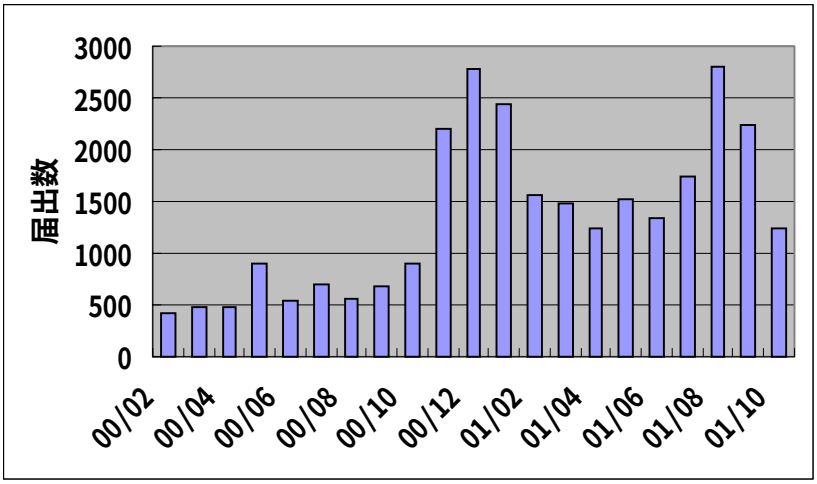
IW2001-B2

22

ウイルスとは

- 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

多発するウイルス被害



http://www.ipa.go.jp/security/txt/2001_11.htmlなどからデータを入手

Sircam

- Sircamはウイルス
  - 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

IW2001-B2

25

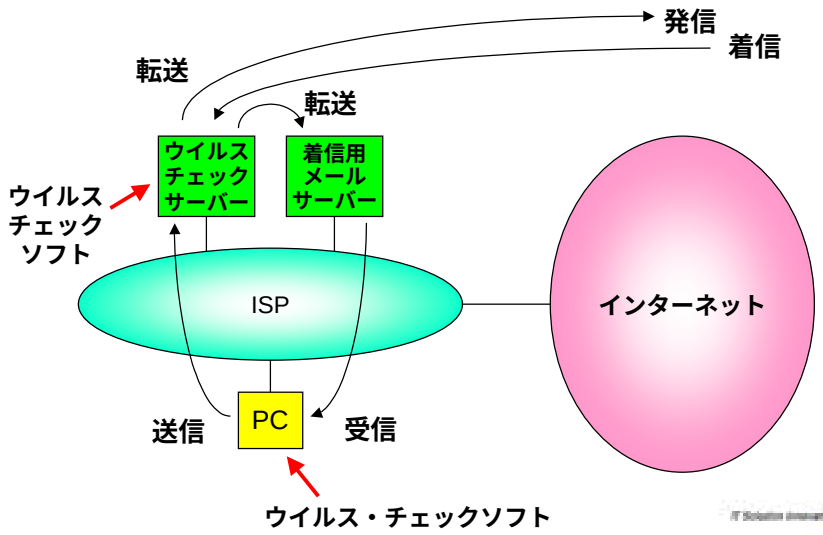
ウイルスを防ぐ

- メールゲートウェイなどでチェック
  - 企業内に入る前に感染していないか調べる
  - 社外から届く前に確認
- 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

IW2001-B2

26

メールのウイルス・チェック



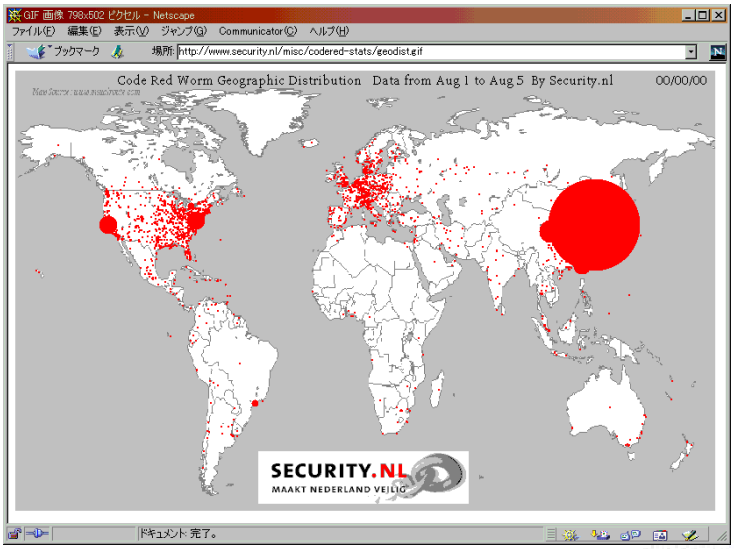
猛威をふるったCodeRed

- 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

CodeRedのしくみ

- ワームは自己増殖
  - 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
  - ワームが増殖していく
- 無差別に攻撃を行う
  - IPアドレスを勝手に選んで攻撃
  - 高速で攻撃するIPアドレスを変更
  - 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
  - 社内LANにとっては致命的

CodeRedの被害状況



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

セキュリティ情報に誤りも

- 「クライアントには感染しません」
  - 一部のセキュリティ管理組織がアナウンス
  - 「CodeRedは，PCウイルスではありません。IISサーバーをご使用でない個人ユーザーの方には，重大な危険はありません。」
- 実際は…
  - クライアントであるはずのパソコンにも感染
  - 多くのWindows 2000 ProfessionalでIISが動いていた
  - しかも、利用者が知らないうちに
  - 当然、みんながセキュリティ・パッチを当てない
  - そして個人のPCが被害に遭う
  - ダイアルアップ接続でも

IW2001-B2

31

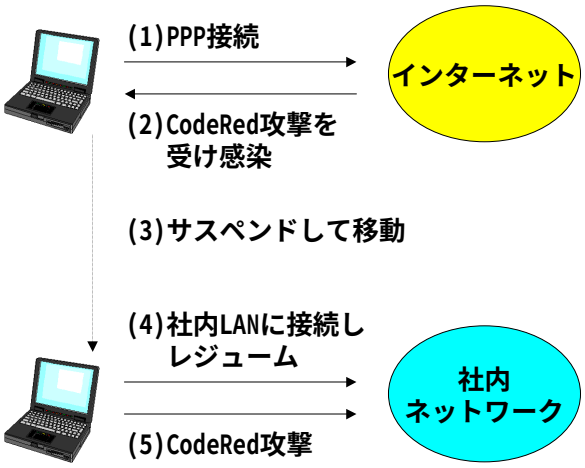
被害は企業内に広がる

- 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…

IW2001-B2

32

盲点だったCodeRedの感染経路



IW2001-B2
33

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

IW2001-B2
34

Microsoft製品が弱いのか？

- たぶん!?
  - いつまでたってもセキュリティ・ホールがある
  - いろんな製品で見つかる
- 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
- 大量に使われているから狙われるという意見も
  - 狙う側にとっては効果が大きい
  - 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!?

IW2001-B2

35

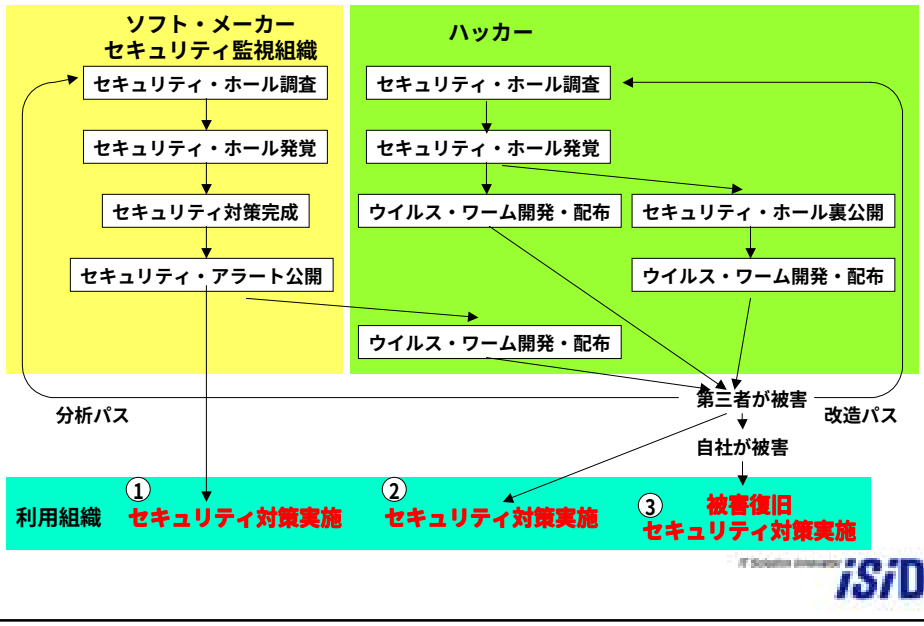
セキュリティ・パッチ

- 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

IW2001-B2

36

ハッカー vs. ソフト・メーカー



セキュリティ情報

- ソフトウェア・メーカーが公開
  - 自社製品の脆弱性
    - » 自社で発見
    - » 第三者が発見
  - 脆弱性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ばかなり危険な状態
- 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

セキュリティ・ホール

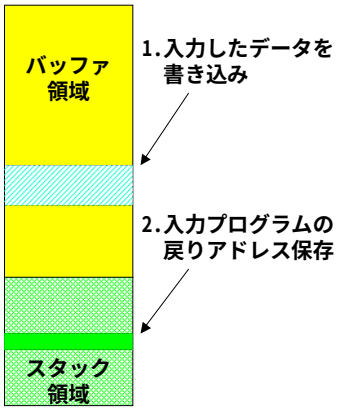
- プログラムの「穴」
  - 本来は存在しないはずのバグの一種
  - 特定のデータを送り込むと予定されていない動き
  - これを利用してハッカーが侵入や命令実行
- なぜ「穴」が存在するのか
  - 安全教育が十分に行われていない
  - プログラムの規模が大きいと確認・検査が難しい
  - ハッカーはこの「穴」を探している
- 「穴」が見つかると…
  - すぐには公表されない
  - 「穴」のふさぎ方がわかってから公表

IW2001-B2

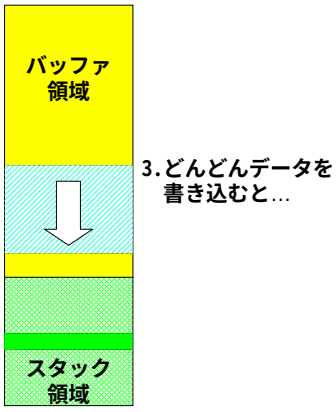
39

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

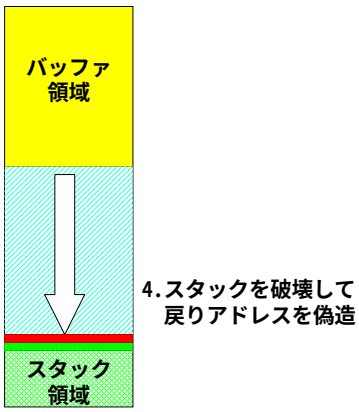


IW2001-B2

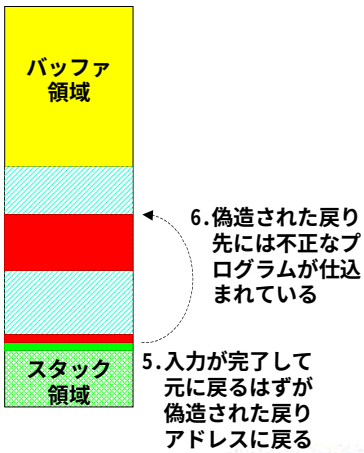
40

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



IW2001-B2

41

企業の守り方が変わる

- ファイアウォールだけでは守れない
  - いろいろな裏口が考えられる
  - すべてに対応することは可能なのか
- 社外に持ち出したPCは社内LANにつながせない
  - そんなことが可能なのか？
  - 持ち出してもインターネットにつながなければOK？
- すべてのPC最新パッチをあてる
  - 誰が管理するのか？
  - 現実的なのか？
- すべてのPCにウイルス・チェックを導入する
  - 最新でないと意味がない
  - 現実的なのか？

IW2001-B2

42

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
- 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

IW2001-B2

43

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

IW2001-B2

44

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
  - トロイの木馬自身は増殖しない
  - ハッカーが何らかの手段でしかける
  - たとえばリモート接続プログラム
    - » ユーザーIDとパスワードの入力を求める
    - » 実はニセのプログラム → パスワードを盗む

IW2001-B2

45

官公庁Web改ざん事件

- 2000年1月に発生
  - 官公庁のホームページをつぎつぎと改ざん・消去
  - 海外からの攻撃だといわれている
- 守りが不十分なサイトが多数存在
  - ファイアウォールがないもの
  - セキュリティ・ホールをついたもの
  - 外部からアクセス可能なもの
- 被害は
  - 信用失墜
  - 緊急対応費用
- 原因は
  - 危険性認識の甘さ
  - 守るしくみが用意されていなかった

IW2001-B2

46

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

IW2001-B2

47

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

IW2001-B2

48

なりすましによる被害

- 身に覚えのない「クレーム」のメール
  - だれかが名をかたって掲示板に悪口
  - だれかが名をかたってSPAMを送信
- エラーメールが大量に届く
  - SPAMの発信人としてメール・アドレスをかたられた
  - ひどいときには何万通も
- 身に覚えのない商品が届く
  - だれかが名をかたって注文
- おかしな電話がかかったり、メールが届く
  - 電話番号やメール・アドレスを公表された
  - 個人情報が流出している !!

IW2001-B2

49

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

IW2001-B2

50

不正侵入による被害

- 重要情報の持ち出し
  - ショッピング・サイトからクレジットカード情報
  - ショッピング・サイトから個人情報
  - 企業サイトから顧客情報
- 持ち出した個人情報を公開
  - 顧客に大きな迷惑をかける
  - 利用者が防衛策を講じる必要も
- 重要情報を破壊・消去
  - 顧客としては持ち出されたり公開されるよりまし？

IW2001-B2

51

インターネットは危険なのか？

- インターネットだから危険ということはない
  - それなら安全なのか？
  - インターネットは安全ではない
- 実社会と同じ!!
  - 実社会の危険性を理解できていない人も多い
  - 危険を理解していないのが一番危ない
- 実社会は危険なのか？
  - 大変危険
  - それを理解していないともっと危険
- だからインターネットも危ない
  - 実社会の延長だから

IW2001-B2

52

実社会の危なさ

- テロ
  - 国際テロ
  - 犯罪組織
- 強盗
  - ハイジャック
  - 集団スリ
  - おやじ狩り
- 窃盗
  - ピッキング
  - 置き引き
  - ケチャップマン

IW2001-B2
53

実社会の危なさ(つづき)

- 詐欺
  - 集団催眠、宗教まがい団体
  - ネズミ講、高配当投資、M資金
  - 取り込み詐欺
  - ワイン・マン
- カード詐欺
  - 偽造カード
  - スキミング、番号窃盗
  - 盗難カード利用
- ぼったくり
  - 店
  - タクシー

IW2001-B2
54

実社会の危なさ(つづき)

- 盗撮・盗聴
  - トイレ、更衣室
  - 会議室、役員室
- 事故
  - 火災
  - 衝突
  - 墜落
- 落書き
  - 建物
  - 乗り物
- 通り魔

IW2001-B2
55

インターネット上で身を守る

- 実社会で身を守れない人は…
  - インターネットでも身を守れるわけがない
- 危険を認識できないと被害は拡大
  - 自分だけは大丈夫？
  - 手口がわかれば防ぎ方もわかるはず
- 「身を守る」と「運がいい」とは意味が違う
  - でも、結果は同じ
  - 身を守る心構えが重要
- かならず被害に遭うとは限らない
  - 運がよければ被害に遭わない
  - 今日は大丈夫でも明日は不明

IW2001-B2
56

インターネットの犯罪者

- プロ
  - 極秘情報を目的とした産業スパイ
  - 軍事情報、先端技術情報を目的とした国際スパイ
  - 情報破壊・システム破壊による営業妨害
- アマ
  - 技術力の誇示
  - 他人につられて
  - 楽しみのひとつ
- 社内
  - 不満分子 → 「いつかはこういうことになると…」
  - 金銭に困って → 「えっ、あの人が」
  - 派遣社員・アルバイト

IW2001-B2

57

サーバーは狙われている

- 外部からアクセスできるので危ない
  - ファイアウォールの内側のマシンは攻撃しにくい
  - 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

IW2001-B2

58

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
  - スキャンされた方にとっては攻撃と見られる
  - 自分のサイトをスキャンしてチェック

IW2001-B2

59

サーバーを守る

- 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
    - » 一種のバグ
    - » バッファ・オーバー・フローなど
  - 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

IW2001-B2

60

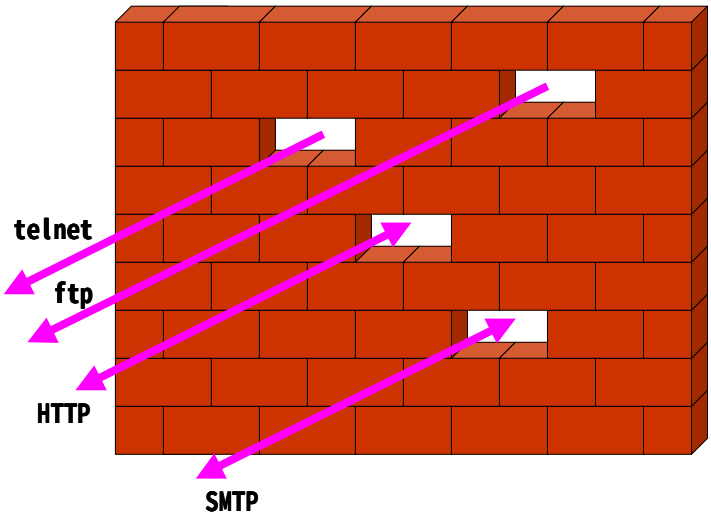
ファイアウォールとは？

- 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
  - 何も通さない壁では意味がない
- インターネットからホームLAN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

IW2001-B2

61

必要な通信のみを通す

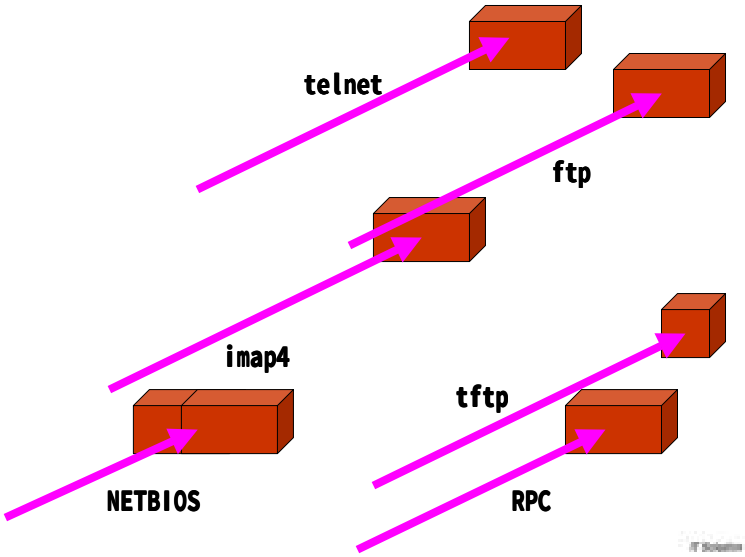


iSiD

IW2001-B2

62

危険な通信を止める



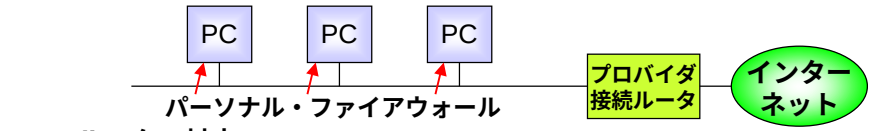
iSiD

IW2001-B2

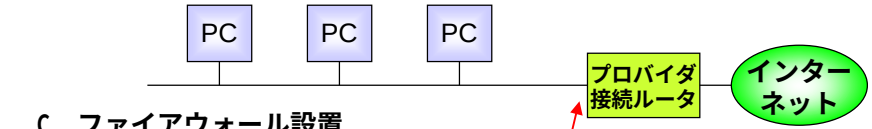
63

ファイアウォールの構成例

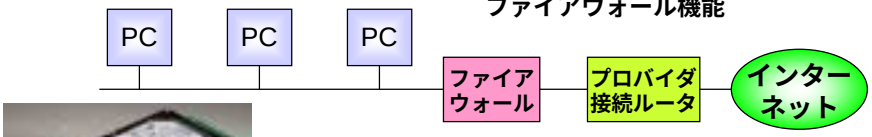
A．ファイアウォールなし



B．ルータで対応



C．ファイアウォール設置



← 超小型PCでファイアウォール構築
スループットが問題に……
2.5インチHDサイズで50Mbps以上
という製品も

IW2001-B2

64

ファイアウォールで安心？

- 設置しただけでは安全は守れない
  - 攻撃手段はどんどん進化する
  - ファイアウォールでの守り方も進化させる必要あり
- セキュリティホールのあるファイアウォールも
  - どの製品を使うかは重要な選択
  - 機能、性能、使い勝手、信頼性などで判断
- それでも安心してはいけない
  - つねにセキュリティ情報に注目しておく
  - ログを調べて大丈夫なことを確認する
  - 自分たちでできなければ専門家に任せる
- フェイル・セイフという考え方を忘れずに

IW2001-B2

65

不要なサービスを停止する

- サーバーに対して攻撃をしかける
  - 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
  - CodeRedのIISのようなことも
  - 分からなければ止めてみる
    - » 悪影響がでれば再度起動する
  - 知らないサービスは危険
  - ハッカーが起動していたかも

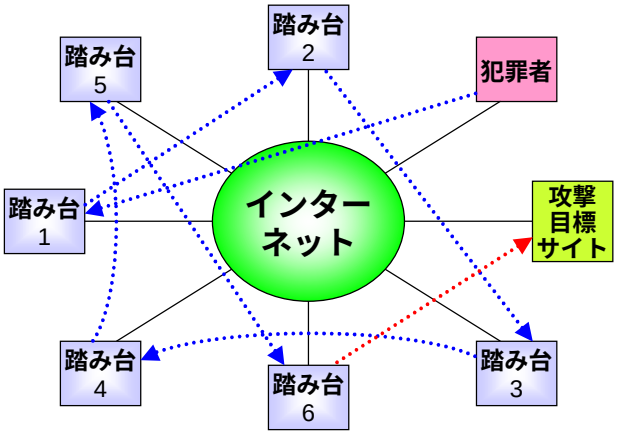
IW2001-B2

66

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

踏み台の実際



Denial of Service

- DoS
  - サービス妨害
  - サービス不能攻撃
  - 過負荷などでサービスを提供できなくする
- DDoS
  - Distributed DoS
  - 複数のコンピュータからDoSをしかける
  - 負荷が大きくなる
  - 高帯域ネットにつながっていても被害を受ける
- 通常、踏み台を利用して攻撃
  - 踏み台にされないことが重要

IW2001-B2

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
  - サーバー

IW2001-B2

70

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 ― 暗号
  - ネットワーク越しは相手が見えない ― 認証
  - 電子情報は書き換えても分からない ― 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

IW2001-B2

71

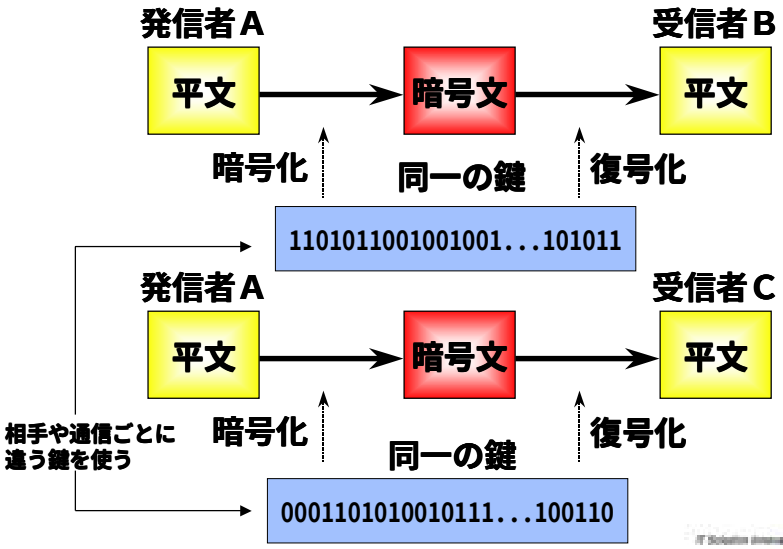
共有鍵暗号方式

- 送信者と受信者は暗号、復号に同じ鍵を使う
  - 鍵を共有するから「共有鍵暗号」
- 処理速度が速い
  - 大量のデータを処理可能
- 送信者と受信者の間で鍵を受け渡す
  - 相手ごとに違う鍵が必要
    - » 同じ鍵を使うと暗号化の意味がない
  - 安全な鍵交換の方法が問題
    - » 鍵が盗まれては意味がない
- 鍵の強度が問題
  - 総当たりで試せば必ず破れる

IW2001-B2

72

共有鍵暗号方式



IW2001-B2

73

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

IW2001-B2

74

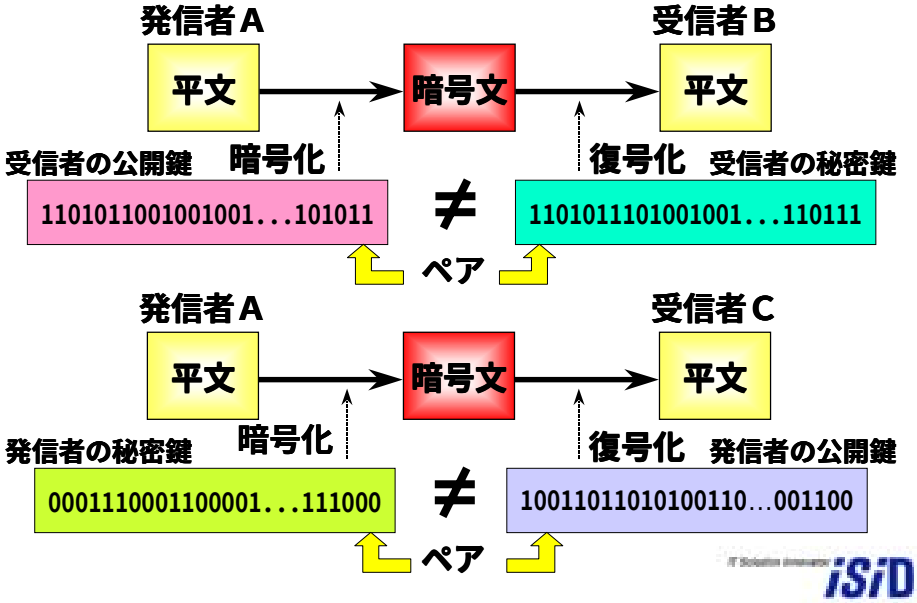
公開鍵暗号方式

- 暗号化鍵と復号化鍵が異なる
  - ふたつの鍵(公開鍵と秘密鍵)がペアになっている
  - 片方を公開(公開鍵)し、片方を秘密(秘密鍵)に
  - 公開鍵で暗号化 → 秘密鍵でのみ復号可能
  - 秘密鍵で暗号化 → 公開鍵でのみ復号可能
- 処理速度は遅い
  - メッセージ全体の暗号には不向き
- こちらも強度が問題
  - 1024ビット程度の鍵が用いられる
  - 認証局では、2048〜4096ビット

IW2001-B2

75

公開鍵暗号方式



IW2001-B2

76

Virtual Private Network

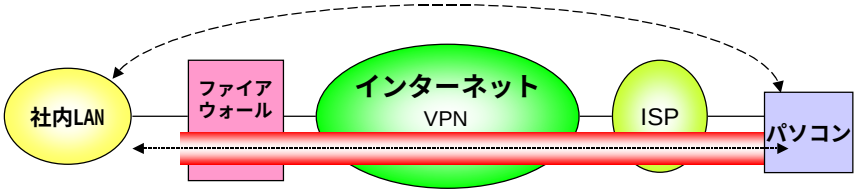
- 実質的なプライベート・ネットワークを作る
  - インターネットを使って
  - 暗号技術で盗聴を防ぐ
  - 「仮想」ではなく「実質的な」
- あたかも専用線のように
  - いくつかのパターンが存在
    - » ネットワーク ⟷ ネットワーク
    - » ネットワーク ⟷ コンピュータ
    - » コンピュータ ⟷ コンピュータ
- メリットは
  - 通信費の削減が可能
  - 社外から安全に通信可能

IW2001-B2

77

Virtual Private Network(つづき)

- 注意点
  - 接続相手のリスクがそのままやってくる
  - 接続が信頼できないと危険
  - VPNの中にもファイアウォールを設けよう



IW2001-B2

78

盗聴に備える

- インターネット通信路上の盗聴は難しいが…
  - 155Mbpsなら1時間で72Gバイト(1.7TB/日)
  - 流れるデータを選択的に取り込む
- 絶対に不可能ということではない
  - 国家レベルで取り組めば
  - 探偵に頼まれた通信会社職員が荷担すれば
- どのように備えるのか
  - 重要な情報をインターネットで送らない
    - » 電話はもっと危ない
  - 通信路を暗号化する
  - 電文を暗号化する

IW2001-B2

79

自分自身を証明する

「わたしは“くまがい”です」と宣言する
- 誰にでも宣言することは可能
- 本物であることを示したことにはならない

◆ 何を根拠に証明するのか？
- 免許証 → 公安委員会が証明
- パスポート → 外務省が証明
- 指紋 → どこにも登録されていない？

◆ 本物であることを示すしくみが重要
- 信頼のおける人に保証してもらう
- 信頼のおける組織に保証してもらう
- 印籠を持っていることを確認する

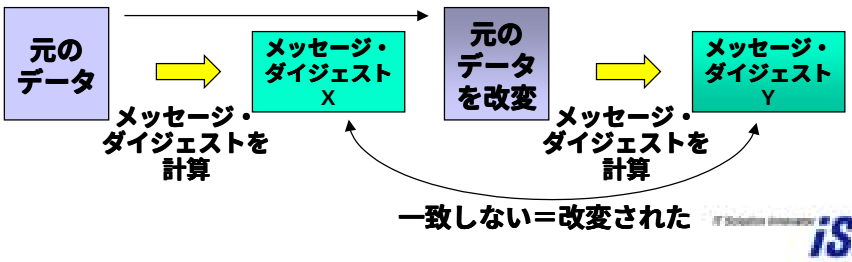
IW2001-B2

80

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

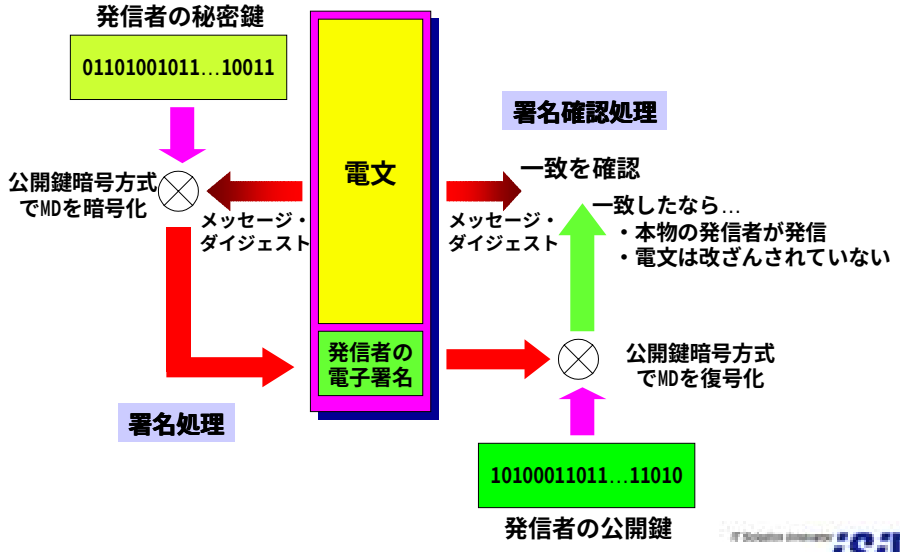
◆ メッセージ・ダイジェストで改ざんを発見
- 電文に計算処理をして128～160ビットの数値を得る
- この数値を変えないように電文を変えるのは困難



IW2001-B2

81

電子署名のしくみ



IW2001-B2

82

Public Key Infrastructure

- PKI
  - 公開鍵暗号基盤 と訳す
  - 電子認証のためのインフラ
- 公開鍵暗号技術を利用して本人証明
  - 利用者の公開鍵を認証局の秘密鍵で暗号化
  - 配布されている認証局の公開鍵で復号できれば本物
  - 印鑑証明書に押された市長印のようなもの
- 認証局とは
  - 英語ではCA (Certificate Authority)
  - 印鑑証明書の発行組織のようなもの
- 証明書とは
  - 利用者の公開鍵に認証局が電子署名したもの

IW2001-B2

83

PKIを利用する

- 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
  - ますます重要なものになっていく

IW2001-B2

84

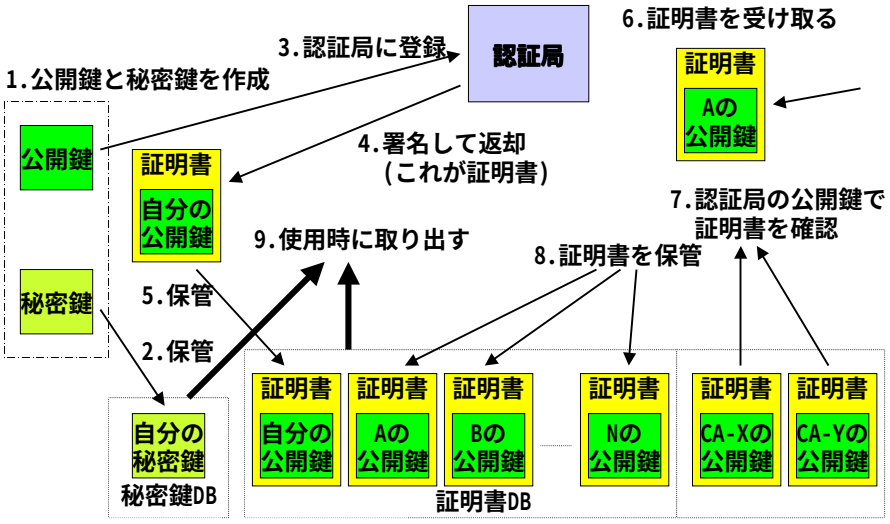
証明書の信頼性は？

- 確実な認証にはコストがかかる
  - 簡単な認証でいい場合もある
  - 完璧な認証を求める場合もある
- 完璧さとコストを秤にかけて複数のレベルを
  - クラス１ メール・アドレスが正しい(誰かに届く)
  - クラス２ 第三者機関を通して個人情報を確認
  - クラス３ 戸籍謄本など公的書類で確認
  - クラス４ 所属組織も含めて調査し確認
- レベルによって発行料金が違う
  - 1,500円/年 ～ 数千円/年
  - ちょっと高すぎないか !!

いろいろな認証局

- 証明書発行機関
  - 公開鍵が正しいことを証明する組織
    - » 印鑑証明書
- 商用サービス
  - 日本ベリサイン などなど
- プライベート認証局
  - 自社で運営する認証局
  - 誰の権限で証明書を発行するか？
  - 他の認証局に認証を受けるのか？
- 認証局の秘密鍵管理が重要
  - 盗まれると大問題に

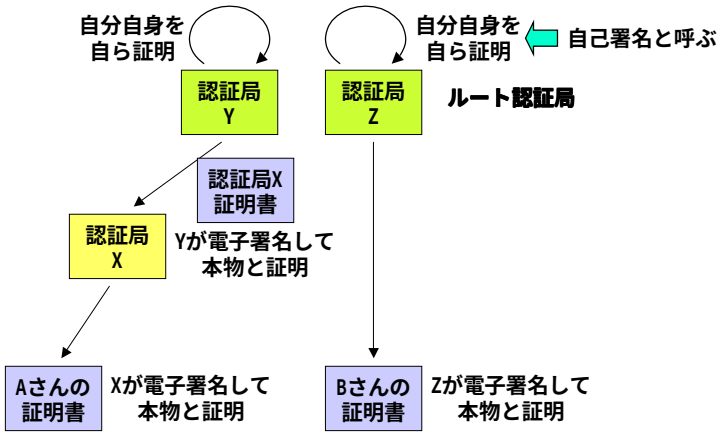
認証局のしくみ



IW2001-B2

87

認証局の構造

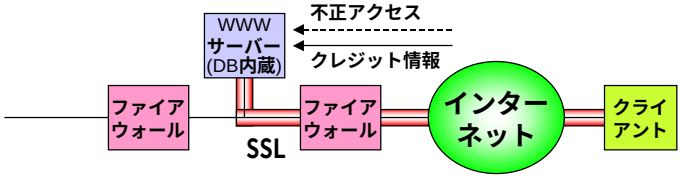


IW2001-B2

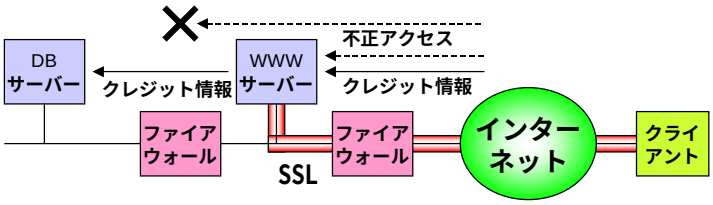
88

ショッピングサーバーの構成例

A．危険な構成



B．一般的な構成



IW2001-B2

89

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
  - 暗号強度が問題
- サーバーが本物であることを証明
  - 電子署名によって
  - 誰が証明しているかが問題
  - 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

IW2001-B2

90

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

IW2001-B2

91

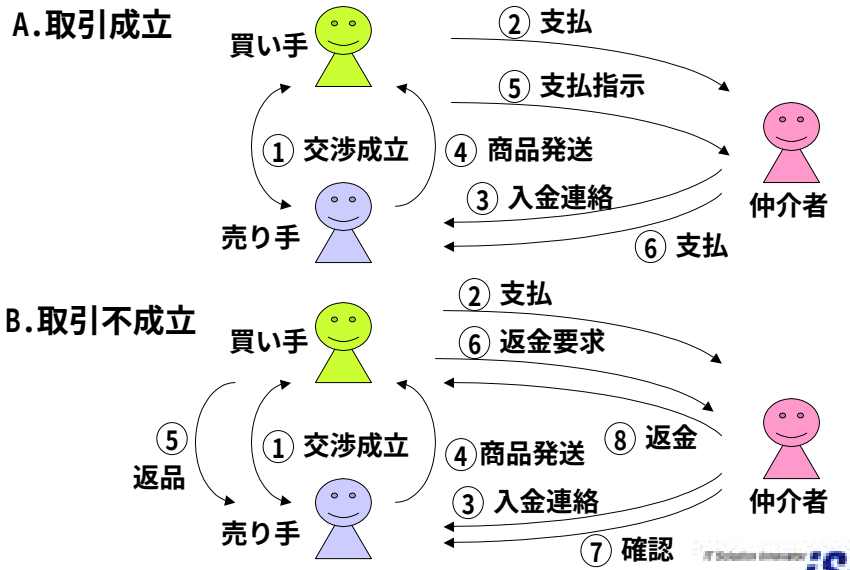
相手の顔が見えない

- ネットワークの向こうはモモンガかもしれない
  - 顔も見えないし声も聞こえない
  - 顔が見えても相手を知らなければ偽物かもしれない
- 契約書に印鑑を押してもらうわけにもいかない
  - 物理的に「もの」を交換できない
  - 印鑑が押されても詐欺目的ならどうしようもない
  - なにを信じればいいのかが難しい
- 電子的な情報で相手を確認する手段が必要
  - そこで登場するのが電子署名
  - 暗号技術を駆使することで解決できる
- 第三者が取引を仲介することも
  - 第三者が信用できないと意味がない

IW2001-B2

92

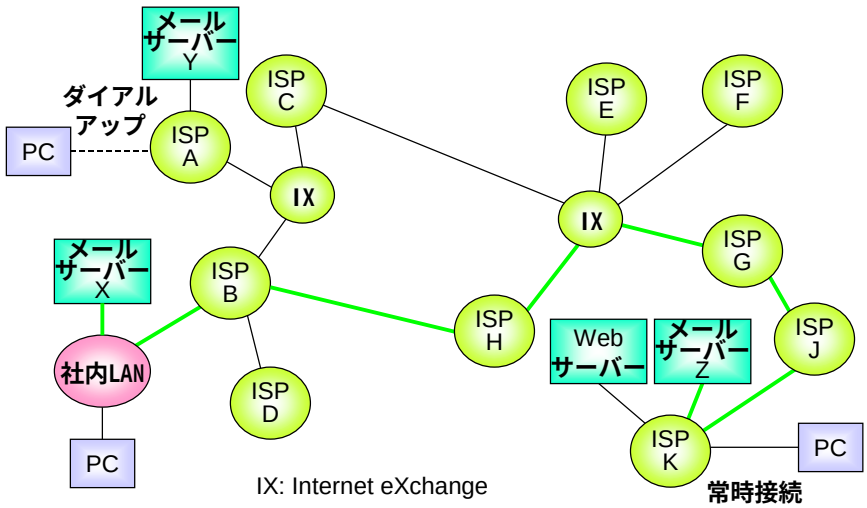
エスクロウのしくみ



IW2001-B2

93

メール転送のしくみ



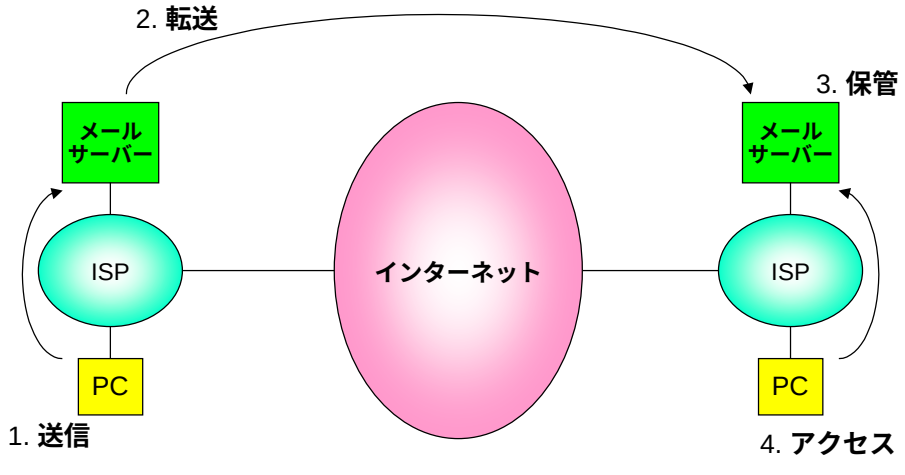
IX: Internet eXchange

ISP: Internet Service Provider

IW2001-B2

94

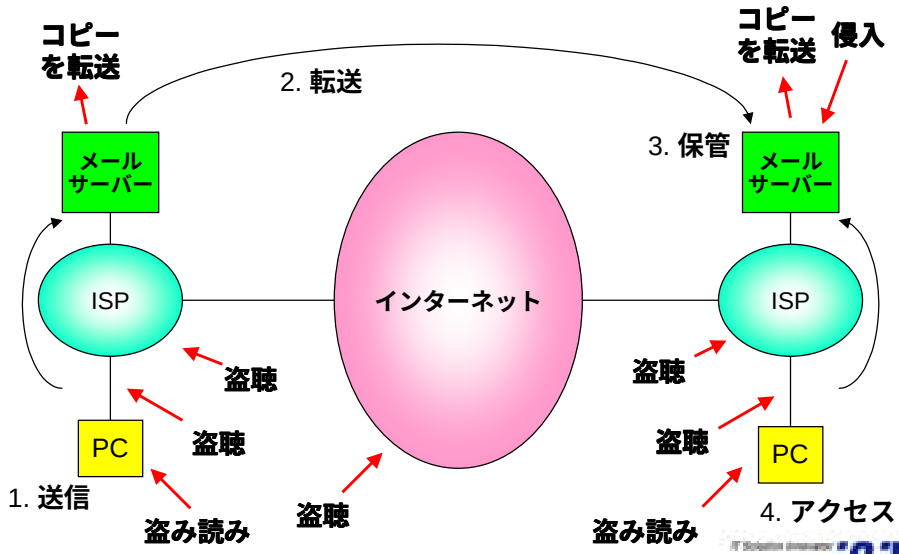
メールを送信する



IW2001-B2

95

メールを盗聴する



IW2001-B2

96

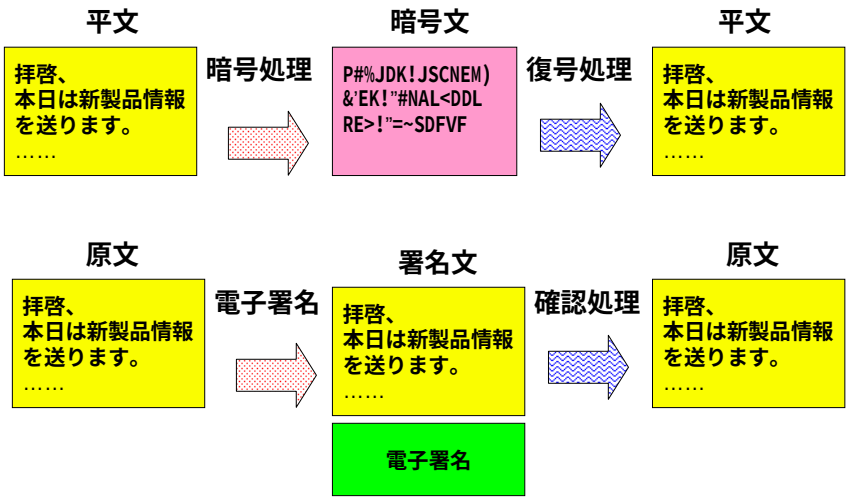
メールシステムは脆弱

- 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

IW2001-B2

97

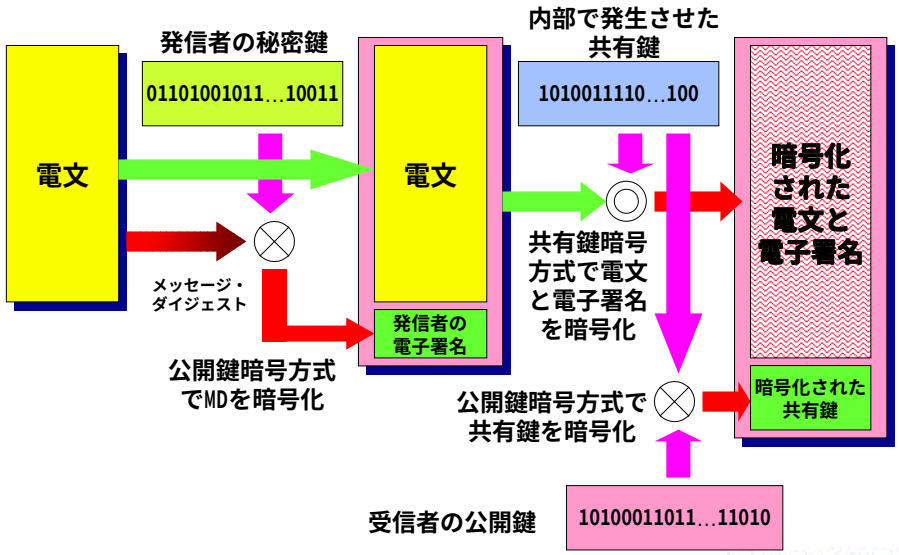
暗号メールの使い方



IW2001-B2

98

暗号化メールのしくみ



IW2001-B2

99

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？

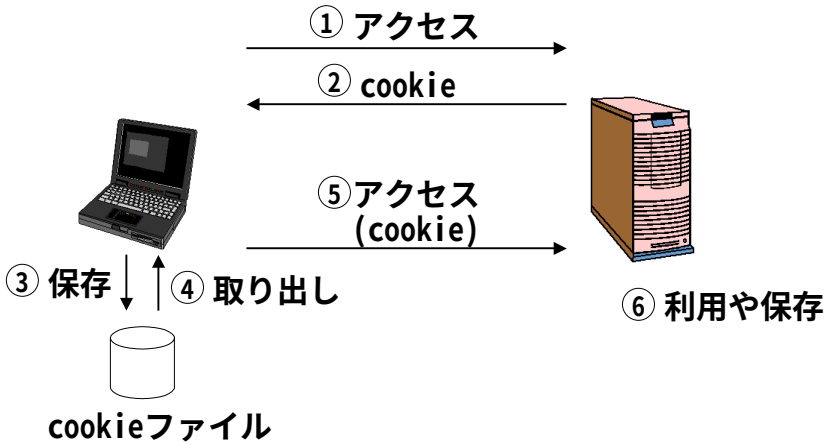
IW2001-B2

100

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

IW2001-B2
103

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

IW2001-B2
104

顧客の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
- 個人情報を守るための方針や方法を決める
  - どのような組織体制で守るのか
  - どのように監査していくのか
  - 問題をどのように見直していくのか
- 不要な情報は集めない
  - 「あれば使えるだろう」は危険
  - 集める「目的」を明確に
- 企業側の意識が低すぎる

IW2001-B2

105

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
- SSGS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
  - うるさいだけ

IW2001-B2

106

正しい顧客情報管理

- 外部からの不正アクセスを防ぐ
  - インターネットからアクセスできるマシンは危険
  - ネットワークから切り離すと不便
- 内部からの不正アクセスを防ぐ
  - アクセス権限を制限
  - アクセスログを残す
  - ログを監査して不正なアクセスを防ぐ
- 使い終わった情報はすぐに廃棄する
  - 保持していると漏えいのもとに
  - たとえばクレジットカード番号
  - 利用目的以外に使わない
- 外部から見極めるのは難しい

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

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
- 申請も調査もマーク使用も有料

IW2001-B2
109

最近気になるIDN

- International Domain Name
  - 日本語.jp とか 日本語.com とか 日本語 など
  - 日本語でURLを書くと関係するWebサイトに行ける
- いろいろな方法で変換
  - いろいろな企業が参入しアクセスをさばく
  - IDNサービス企業に一度アクセスが行われる
  - アクセス状況がすべて記録される
  - 記録を残しているIDNサービス企業も
- その情報がどのように利用されているのか心配
  - 企業活動に利用されていないのか？
  - どこかに売られていないのか？
  - これもプライバシーの一部

IW2001-B2
110

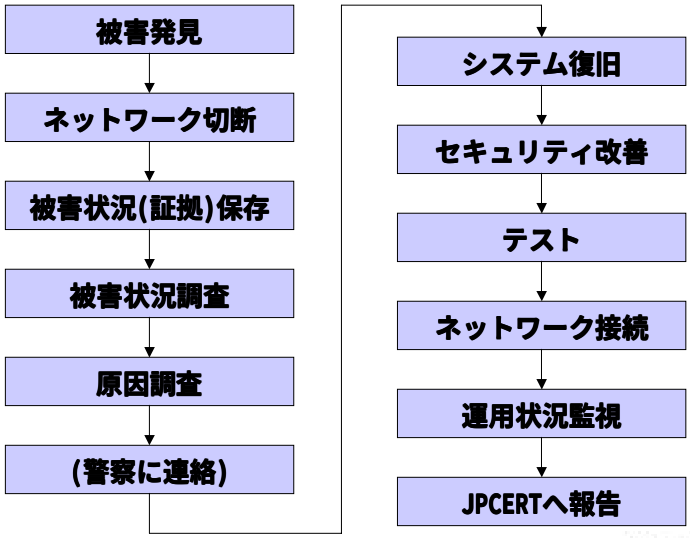
セキュリティは危機管理の一部

- 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

IW2001-B2

111

被害が発生したときには



IW2001-B2

112

犯罪から身を守るために

- 危険な場所を知る
  - 国、地域
  - 都市、地区
  - 店、部屋、トイレ
- 危険な手口を知る
  - ケッチャップ・マン、ワイン・マン
  - 路地に引きずり込む
  - ホテル客室の金庫にドリルで穴
- ことば巧みに
  - 「いい品物ですがお金が必要なので安く売ります」
  - 「もうかりまっせ」、「当社は絶対安全です」

IW2001-B2
113

法律は守ってくれない!?

- 「情報」を盗んでも罪を問えないことも
  - プリントアウトした紙、コピーに使ったFD
  - ネット経由なら、不正アクセス防止法が適用
- にせクレジットカードの保有もOK
  - 偽造団が日本に押し寄せる
- 個人情報を漏らしても罪に問われるのは一部
  - 国家公務員やNTTの社員などのみ
  - 金融機関などは法制化に反対しているらしい
- 相談する相手もいない？
  - 警察も消費者センターも理解が不十分？
- 自分の身は自分で守るしかない

IW2001-B2
114

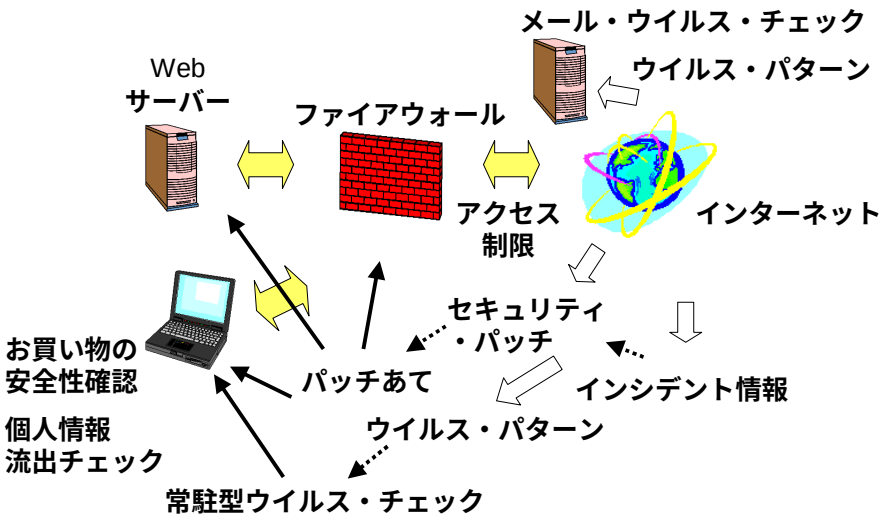
社会情勢の変化に対応する

- 海外へ出かける人が増加
  - 危険な地域が多い
  - 海外の危なさを認識していない人が多い
- 海外から流入する犯罪組織
  - 「国内は安全」という認識を逆手に
  - 海外の手口を国内に
  - 密入国が増加中
- 国内の犯罪組織も過激化
  - 海外からの流入組に負けられない
  - 資金源の確保のために
- インターネットも同じ

IW2001-B2

115

セキュリティ対策の数々



IW2001-B2

116

自宅のネットワークを守る

- インターネットにつなぐと攻撃を受ける
  - IPアドレスがついた時点で攻撃対象
  - しっかり守らないと
- 対象機器は無差別
  - PC
  - ルータ
  - プリンタ
- 攻撃を防ぐには
  - ファイアウォールの構築
  - セキュリティ・ホールをふさぐ
  - 不要なサーバー・プログラムを停止する
  - 自分自身をポート・スキャンする

IW2001-B2

117

個々のパソコンを守る

- パーソナル・ファイアウォールを導入する
- ウイルス・チェックを導入する
- ウイルス・チェックを常駐させる
- ウイルス・パターンを最新に保つ
- セキュリティ・ホールをふさぐ
- 安全性を確信できないメールを読まない
- 安全性を確信できない添付ファイルを開かない
- 安全性を確信できないファイルをダウンロードしない
- 安全性を確信できないプログラムを実行しない

IT Solution Innovator iSiD

IW2001-B2

118

プライバシーを守る

- 個人情報の公開範囲を決める
  - 公開する相手を見極めて
  - 公開する内容を見極めて
  - 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
  - 利用されたときの法的拘束力は
- 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

パスワードにもご注意

- やさしいパスワードは危険
  - 辞書に載っている文字列
  - 人名、製品名、グループ名なども
- 難しいパスワードも実は危険
  - 総当たりすればいずれ当たる
  - 総当たりには時間がかかるが…
- ひとつのパスワードを流用しない
  - 目的にあわせてパスワードを変える
  - 重要度にあわせてパスワードを決める
- パスワードを共有しない
  - ひとつのIDを共有すると責任が不明確に

参考URL

- 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/
- The SANS (System Administration, Networking, and Security) Institute
  - http://www.sans.org/