情報セキュリティとクラッキングの実際

― どのような脅威があるのか ―

東大理　　民井　淳

目次

I. 情報セキュリティ

情報セキュリティの概要

1. 守るべき対象の明確化（分類）
2. 対象の何を確保するのか（対象によって重みが異なる）
    1. 機密性 (Confidentiality)
    2. 完全性 (Integrity)
    3. 可用性 (Availability)
3. 脅威、脆弱性とリスクの評価
4. セキュリティに対するコスト
   安全性、利便性、コスト

脆弱性×脅威＝被害発生（リスク）

100%のセキュリティは実現できない。
100%に近づけることは可能
⇔ 利便性の低下、コストの増大

セキュリティは構成員全員で確保する

参考 (セキュリティ標準規格)： BS7799, ISO17799, JIS X5080

セキュリティの対象
（何を守るのか）

例：

- 解析データ、ファイル（可用性、完全性）
- メイルの内容 (可用性、機密性)
- ネットワーク機器、サーバーPC (可用性)
- 解析用 CPU (可用性)
- 成績表 (機密性)
- 研究室および大学の社会的信頼
  (外に対して攻撃をしない。ホームページが改竄されない、悪用されない、...)

セキュリティの要件
（対象の何を確保するか）

1. 機密性 (Confidentiality)
   対象者以外には内容が漏れないこと
   Privacy　を含む

2. 完全性 (Integrity)
   内容が改竄されていないこと
   故意の改竄に限らず事故を含む

3. 可用性 (Availability)
   資源(resource)が利用可能であること
   （必要な時に必要な量）

その他のセキュリティ上の関心事(Security Concern)：
非否認性 (Non-Repudiation), 説明可能性 (Accountability), 真正性 (Authenticity)

脅威(Threat)
(何から守るのか)

1. 事故

- サーバー、ディスクのクラッシュ
- 操作ミス
- プログラムのバグ
- 停電、火事などの災害

2. 悪意のある者による脅威

- 外部からの不正行為 (ネットワーク)
- 内部からの不正行為 (内部端末)
- ウィルス、ワーム、トロイの木馬
- サーバー、ディスクの物理的破壊

脆弱性(Vulnerability)
（脅威に対する非耐性）

- OS･アプリケーションのバグの存在、およびパッチを当てていないこと
- データのバックアップをとっていない
- 侵入者に対する防御が弱い　(ソフトウェア的に、物理的に)
- 利用者の教育が不十分
- ウィルスの検出･駆除を行っていない

リスク(Risk)
(どのような被害が起きるか)

- メイル、データ、ソフトウェア資産の喪失
- データの改竄
- データ解析・理論計算の停止、遅延
- 機密文書の漏洩 (メイルの内容、成績表、実験計画・結果、...)
- 社会的信頼の喪失

被害発生(リスクの現実化)のメカニズム

脆弱性　×　脅威　＝　被害発生

- バックアップをとっていない　×　ディスクのクラッシュ　＝　データの損失
- 侵入者に対する防御が甘い　×　侵入者による侵入　＝　機密の漏洩、...
- バックアップ機器がない　×　サーバーのクラッシュ　＝　サービスの停止
  (メール、WWW、CPU,...)
- ウィルス検出の不足　×　ウィルスの伝播　＝　外部への感染、攻撃
  (信用の低下・喪失)

脆弱性を減らすことによりセキュリティ向上を図る

コスト(Cost)
(リスク回避の為のコスト)

- バックアップ機器(ディスクなど)の整備(費用)
- バックアップ機器(サーバやネットワーク機器の代替機)の整備(費用)
- 人的コスト(費用＋マンパワー)
  日々のセキュリティ診断、バックアップ作業、セキュリティホールの除去
  機器の整備、緊急時の対応

セキュリティは日々の努力のたゆまぬ積み重ねである。

もはや全てボランティアで運用できる時代ではない。

ボランティアで運用するのであれば相応のリスクを覚悟すべき。

II. クラッキングの実際

セキュリティ侵害の分類

1. 悪意コード(Malware: Virus, Worm, Trojan Horse)
2. サービス拒否攻撃(Denial of Service: DoS)
3. 不正侵入
4. 機密性(Confidentiality), プライバシー, あるいは匿名性の侵害

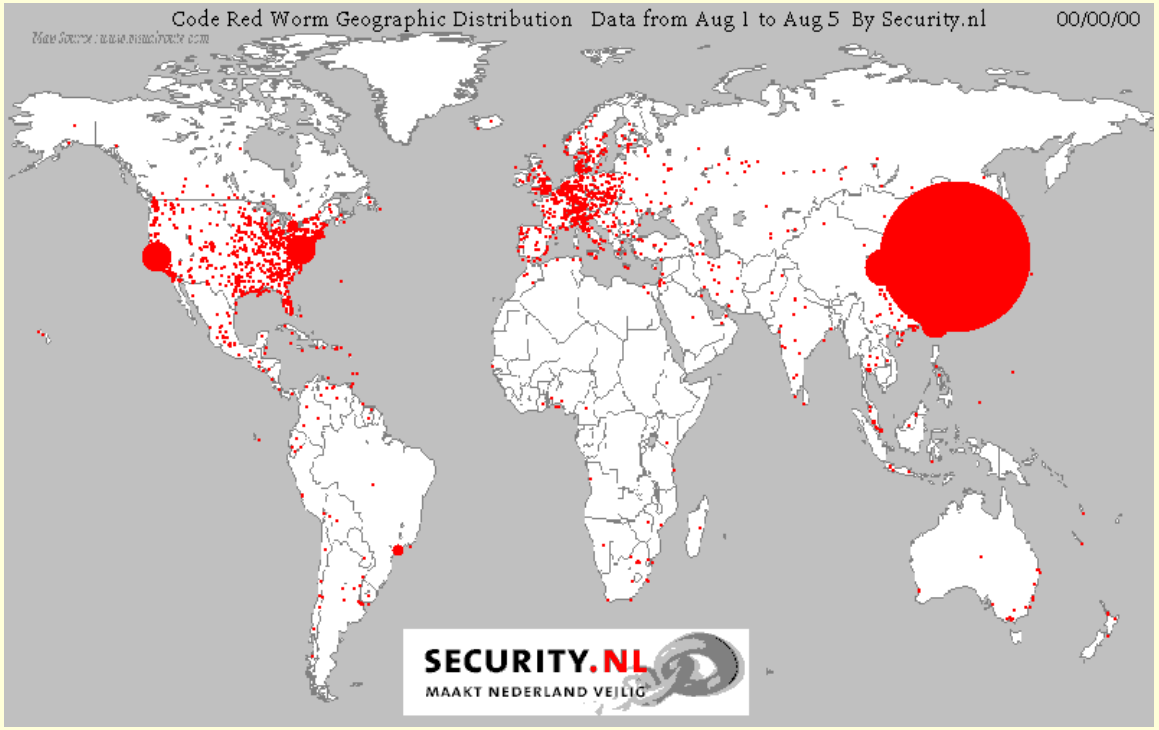
かならずしも綺麗に分類できる訳ではないが。

悪意コード

2001年7月16日にワーム「コードレッド」が発見される。

→ Microsoft IIS のバッファオーバーフローの脆弱性を利用して広がる。
この脆弱性は既に(2001.6.19)知られていたが、セキュリティパッチを当てていなかった多くのサーバーに感染が広がった。

→ 2001年8月オランダの Security.nl 社が被害状況世界地図を作成して公開。



実際には被害が大きかったのは韓国であった。

悪意コード

1. ウィルス(Virus)
   - 他のプログラムにとりつくことで増殖し、不正行為を働く。
   - 現在出回っているウィルスは数百種程度。
   - ほとんどはマクロウィルス（他にファイル感染、ブートセクタウィルス）
     1985年にマイクロソフトワードのマクロウィルス「コンセプト」が発見される。
   - メリッサ(1999年, 100万台に感染、被害額8000万ドル) 米、D.L.スミス30歳
   - ILOVEYOU（2000年, 数100万台に感染、被害額1-100億ドル)フィリピンの学生
     → メイル(アウトルック)による感染。

2. ワーム（Worm）
   - 自立して増殖する。
   - 1988年コーネル大学の博士課程の学生ロバート.T.モリスがワームを作成。6000台のコンピュータをクラッシュさせた。当時のインターネット上コンピュータの10％）。
     (3年間の保護観察処分、400時間の地域奉仕、および 10,500ドルの罰金)
     コードレッド(2001年)
     → マイクロソフトIIS(WWWサーバ)への感染
     WWW頁の改竄、特定のサーバー(ホワイトハウスなど)への攻撃

悪意コード

3. トロイの木馬(Trojan Horse)

- 通常のプログラムを装う悪意をもったプログラム。
  パスワードを盗む、外部からキーストロークや画面を読み取る、計算機を操るなど。
- 1999年Microsoft Internet Explore のアップグレードのトロイの木馬が配布される。
- 1999年TCPWrappers のトロイの木馬版が配布される。
- 2002年OpenSSHのトロイの木馬が配布される。

- その他リモートコントロールデーモン、BackOrifice, NetBUS など
  → コンピューターはほぼ完全にのっとられる。

悪意コードに対する対応:

- メイルはウィルスチェッカを通す(常に最新版に)。
- 各ホストにアンチウィルスソフトを入れる(常に最新版に)。
- 少しでも怪しいプログラム、プラグインはダウンロードしない。
- 常に最新版のパッチをあてる。
- 不用意に添付ファイルを開かない。
  ただし、OutlookExpress, ActiveX などでは、ファイルが選択されただけでプレビューが表示されてウィルスに感染する可能性がある。

サービス拒否(DoS)攻撃

- WWW サーバーへの DoS 攻撃
  → WWW サーバー管理者の信頼失墜、クラッカーの売名行為。
  ひたすらアクセスを送りつける。
  DNS ハッキング (DNS Spoofing) 閲覧者を別の(クラッカーの)頁へ誘導する。

- メイルサーバーへのDoS攻撃
  メイル爆弾攻撃 ... ひたすら大量のメイルを送りつける。SPAM ホストなども利用。

- 分散型 (Distributed) Dos攻撃(DDoS)
  トロイの木馬やウィルスを利用して大量のホストから集中的に標的を攻撃する。
  → コードレッドワームはホワイトハウスを攻撃。IEのトロイの木馬はブルガリアテレコム社を攻撃。

- SYN Flooding 攻撃
  標的に大量の接続要求パケットを送りつける(送り元は存在しないホスト)。
  標的コンピュータは接続用リソース(メモリ)を食いつぶしてダウンする。
  (Tiny Fragment 攻撃、Overlapping 攻撃)

- 標的のOSの脆弱性をついてシステムダウンを引き起こす(teardrop 攻撃, ping of death 攻撃など)。
- ネットワーク機器をダウンさせる。
- 接続可能なセッション数全てを占有する。

外部ネットワークからの脅威

- Password Cracking
- Social Engineering
- IP Spoofing
- DNS Spoofing
- SYN Flooding 攻撃
- Tiny Segment 攻撃、Overlapping 攻撃
- Virus, Worm, Trojan Horse
- Mail Bomb, SPAM
- SPAM
- Tempest
- WWW のセキュリティ
- Cross Site Scripting
- Port Scanning, half scan, stealth scan, slow scan
- Back Door
- Log Bassing
- Sniffing
- War Dialing
- 暗号の安全性
- Buffer Overflow
- 種々のDoS攻撃
- 認証方式

- スーパーユーザーによる脅威
- 政府による脅威

不正侵入の一般的手順

1. 標的に関する情報の収集
   - WWW による検索など
   - Host IP 、ネットワーク構成の推測、管理者の名前・連絡先の取得

2. 侵入方法の確立(ユーザー権限取得)
   - Social Engineering
   - WEB サーバへの攻撃
   - Port Scanning, OS・アプリケーションの推測, 各種攻撃の実施
   - 他ホストからの芋づる式侵入

3. (ルート権限取得)
4. 侵入目的の実行
   データのコピー、改竄、消去、システムクラッシュ。
   踏み台攻撃

5. 事後処理
   - バックドアの生成
   - ログの消去(log basher)

6. 撤退

- パスワードファイルの取得
- 既知の脆弱性の悪用による権限取得

Social Engineering

人間をだまして情報を得る、あるいは不正に必要な操作をさせる行為。
クラッカーはかなりの頻度でこの手法を用いる。

- 1993年ニューヨークのインターネットプロバイダ Phantom Access の利用者は以下のような偽のメールを受け取った。「最近の調査によりお客様のアカウントが外部の何者かによりハッキングされたことが判明しました。これにより多額の追加料金が発生しています。被害を見積もるためにお客様のパスワードを一時的に『DPH7』に変更してください....。」
- 1999年 AOI の利用者が以下のようなメッセージを受け取った。「データベースのエラーによりお客様のアカウントが削除されてしまいました。バックアップデータの復旧にはお客様のパスワードが必要です...。」

- 計算機会社の職員らしいらしい服装とバッジをつけて現場に現れ、しばらく端末を使用して作業したいと要求する。
- 権威を装う。「あなたのコンピュータから当方に攻撃が仕掛けられている。今すぐ添付のパッチプログラムをインストールするように！」。あるいは「こちらで対処するので大至急パスワードを教えるように！」。
- 新規ユーザを装う。新規の派遣社員を装い、ユーザー名とパスワードを要求する。

事前に十分に下調べを行い、担当職員の名前や会社、部門の名前などを伝える。

パスワードの安全性

1. UNIX システムでは、パスワードのハッシュ値が登録されている(ハッシュアルゴリズムは公開)
   → パスワードファイルの中身からパスワードは引き出せない。
   しかし、近年の CPU パワーの増大により、辞書攻撃やブルートフォース攻撃が非常に有効になっている

Pentium II 400Hz ×4 による WindowsNT 7 文字のパスワードのクラッキング例(L0phtcrack):

- アルファベットと数字の組み合わせ ... 5.5 時間
- ＋よく使う記号の組み合わせ ... 45 時間
- キーボードから入力可能なあらゆる文字 ... 480 時間

実際に使われているパスワードの調査

16 % ... 3 文字以下

86 % ... クラック可能なパスワード(3文字以下を含む)

悪いパスワード

以下のようなパスワードはすぐに解読される。

- 人名、地名、商品名、固有名詞
- 小説、映画、テレビなどの名前
- 誕生日、住所
- 電話番号、ナンバープレート、証明書番号
- 辞書に載っている単語(日本語でもだめ！)
- 以上のものを逆に綴ったもの
- 以上のものの前後または途中に、数字や記号を1文字を挿入したもの
- 7文字以下のパスワード

悪いパスワードの使用法

- WWW 等で使用するアカウントと同じパスワードを用いてはいけない
- パスワードを書きとめてはいけない。どうしても書き留める必要があるときは、
  - パスワードとは分からないように書き留める
  - 他の文字の間にはさんだり、自分だけがわかる方法で組替えたりする
  - アカウント名、コンピュータ名と一緒に記録しない

良いパスワード

良いパスワード

- 大文字と小文字が混在している
- 数字、句読点、記号などを含んでいる
- 覚えやすい(書き留めておく必要がない)
- 最低8文字以上である
- 肩越しに覗かれないようにすばやく入力できる。

良いパスワードの例:

- 単語2つの間に記号や数字をはさんだもの
- 自分にとって意味のある言葉の頭文字をとったもの

機密性に関する防御
---果たしてPrivacyは守れるか？---

自分以外は全て敵

- データの機密性

  個人 PC のみにデータを置く。

  → 個人 PC の管理の厳重化(内部・外部に対して)

  → バックアップデータの安全性も重要

  暗号化 (PGP, GnuPG)

  → 暗号化データの安全性

  → データ復号の安全性

- メイル通信の(ネットワーク上での)機密性

  S/MIME

- WWW 通信の機密性、匿名性

  SSL (Secure Socket Layer)

  → 公開鍵証明書の安全性

- ネットワーク通信(盗聴)に関する機密性

  SSH (Secure Shell) ... 暗号化通信

  IPSec (IP Security) ... 暗号化 IP (機密性、認証)

  → トラフィック分析による攻撃はさけられない

暗号の安全性(1/2)

1. 暗号データの安全性
   - いつまで秘匿できる必要があるか（永遠？）
   - アルゴリズムの安全性

     公開アルゴリズムの若(し)くはなし:

     専門家による大規模な分析とレビューが行われてきている。

     RSA, Elgamal, 楕円暗号

     非公開アルゴリズムは早晩破られる:

     DVD暗号、Firewire 暗号, マイクロソフト暗号アルゴリズム、スマートカード用商取引プロトコル、セキュアIDの秘密ハッシュ関数、携帯電話アルゴリズム、...
   - 鍵の長さ

     長い方が破られにくいが、実質鍵長が重要。

     Netscape Navigator 1.1 ... 128ビットの鍵を生成する暗号アルゴリズムに欠陥。実質鍵長は20ビットであった。

     欧州のGSM携帯電話 ... A5/1 アルゴリズム。64ビット鍵の実質鍵長は30ビットであった。
   - パスワードの安全性

     秘密鍵が盗まれた時、パスワードの実質鍵長が短ければ破られる。

     英文で 128 ビットの実質鍵長を得るには 98 文字のパスフレーズが必要
   - プログラムの安全性
   - システム(OS)の安全性

     システムが破られれば(そしてそれが認識されていなければ)暗号は簡単に破られる。

暗号の安全性(2/2)

2. 復号の安全性
   - パスワードの記憶
   - 秘密鍵の安全性

     秘密鍵が失われれば二度と復号できない

データマイニング

個人情報データベースには大きな価値がある。

例：クレジット会社は個人に対する多大なデータベースを作成している。
(消費の嗜好、食べ物、旅行先などありとあらゆる情報)
個人データベースは合法的に売買される。お金を出せば誰でも買える。
米国では、データベースの所有権はデータを集めた企業にあり、データベースの対象である個人には何の権利もない。

例：マイレージカードなども同様。
航空便のみならずホテル、ショッピング等々に関しても情報を集める。

例：一部のレンタルビデオチェーンは客が借りたビデオ全てを記録したデータベースを持っている。

このような情報を収集して分析する作業をデータマイニングと呼ぶ。
インターネット上の情報は、データマイニングの格好の標的である。

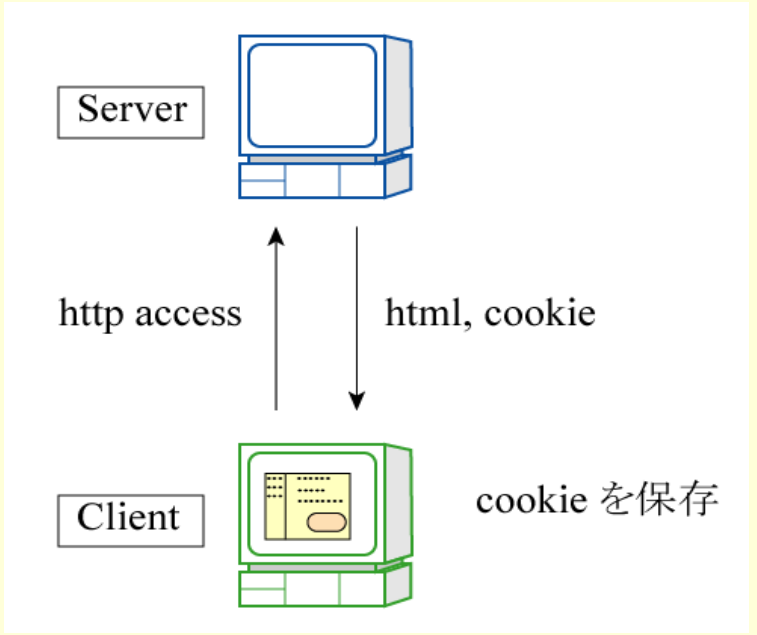
WWW閲覧の匿名性(1/2)

クッキー： WWW ブラウザ識別のため、WWWサーバが閲覧者に与える ID。
閲覧者との接続を維持する。ブラウザはクッキーを期限まで保存する。
例： ショッピングカート

クッキーの悪(?)用：
クッキーを利用してブラウザの閲覧を関連付けることができる。
場合によっては個人を特定することも可能。

Double Click 社
WWWサイトの広告メッセージを仕切っている。
あるページの広告でBrowserにクッキーを渡し、別のページの広告でクッキーを返すことを要求。
→両者が一致すれば閲覧を関連付けられる。
→あるページで個人情報を入力し、それが Double Click 社に流れていれば、個人の特定も可能。

・個人の閲覧嗜好に基づいて絞り込み広告を行う。
・個人情報の売買



WWW閲覧の匿名性(2/2)

メイルアドレス識別タグ付きの URL をダイレクトメイルで送る。

→ メイルを受信した人が URL をアクセスするとクッキーを渡し、個人情報とクッキーを関連付ける。

WEBハッキング

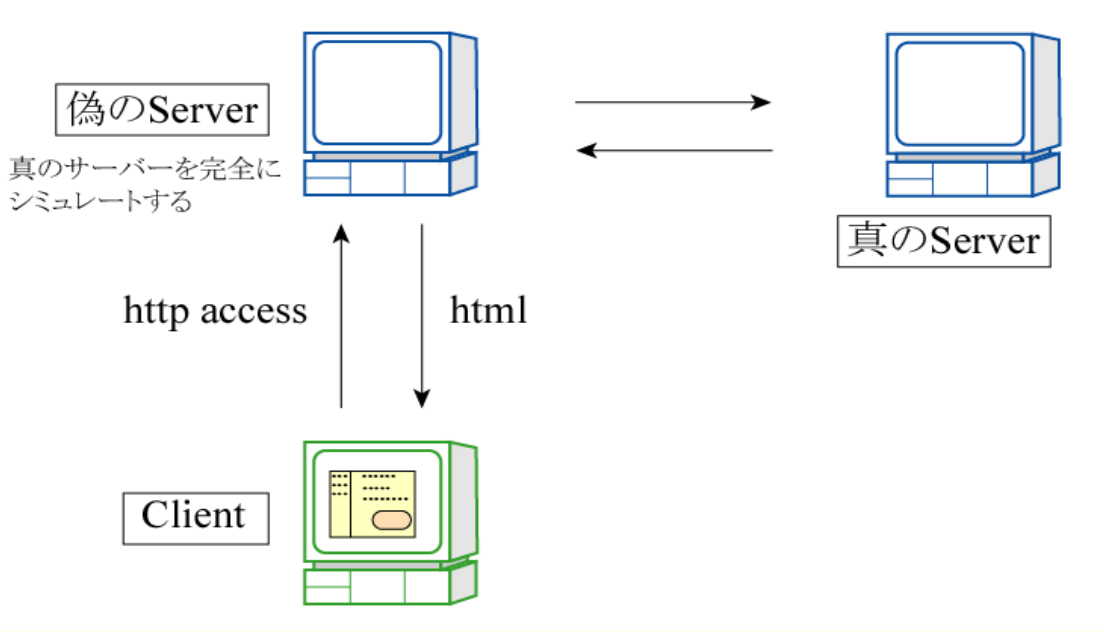
WEB ハッキング

（中間者攻撃の一種）

- ダイレクトメイルや検索エンジンなどでブラウザを偽のWWWサーバーに誘導する。
- 偽サーバーは本物のサーバーを完全にシミュレートする。必要であれば真のサーバーとの通信を行う。
- 偽サーバーはブラウザで入力した全ての情報を盗聴することができる。

  → クレジットカードデータの悪用、商品注文数や配送先の書き変え
- 公開鍵証明書を用いた SSL 通信で防御可能

  (但し公開鍵をユーザーがチェックしなければ無意味)



クロスサイトスクリプティング

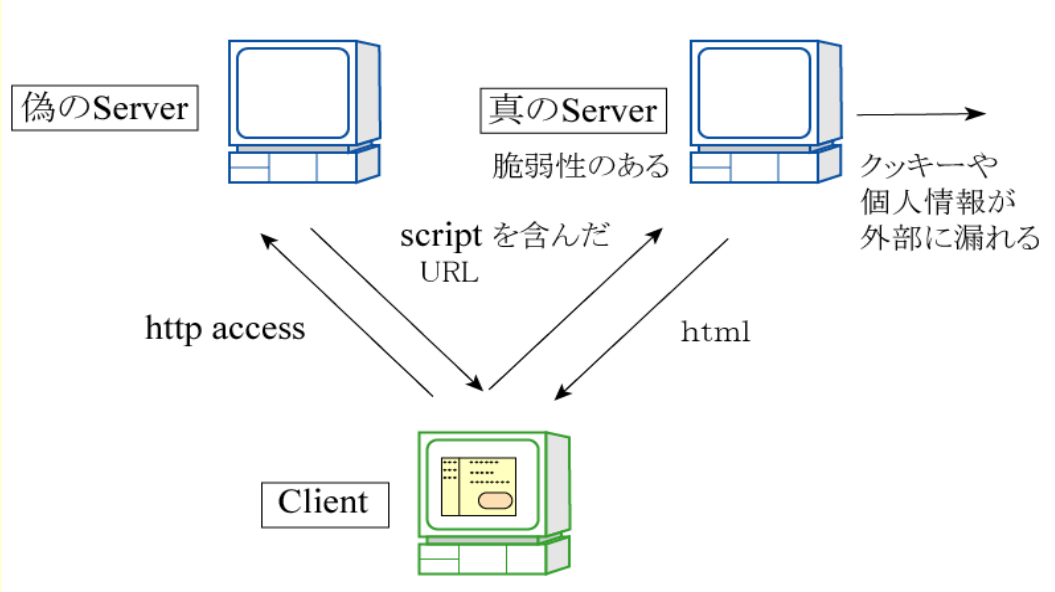
顧客情報が外部に流出事件

- ソニーミュージックグループの化粧品メーカーサイトで、約1万人分の個人情報が流出。
  顧客の氏名、住所、メールアドレスなど。
- パソコン関連機器販売会社「サクセス」の通販用ページから、通販を利用した顧客の住所や
  氏名、電話番号、メールアドレス、購入商品名が流出。

…

手法:

- 検索エンジンなどでブラウザを偽のWWWサーバーに誘導。
- スクリプトを含んだ URL により真の
  (脆弱性のある)サーバにアクセス
  させる。
- クッキーや個人情報を外部(電子掲
  示板など)に送信
- 公開鍵証明書+SSLでは防御できない。



その他の盗聴

電磁波漏洩(tempest)

コンピュータ機器を使用する際に生じる電磁波を盗聴する手法

- Ethernet ケーブル
- 電源ライン
- 水道管
- モニタ画面の読み取り

企業による介入

- マイクロソフト（に限らず）のアプリケーションデータにはソフト所有者の ID が入っている。
- Pentium III CPU には固有シリアル番号が埋め込まれている。

- ISPによるデータアクセスの記録、通信の傍受、個人情報の収集。
  → AOLを通じてウィルスを広めた人物が、アクセス記録により捕まった例がある。

政府による介入

政府は決して個人プライバシーの味方ではない。

- 米政府は標準共通鍵暗号 DES を認可する時に暗号鍵の長さを 112 ビットから 56 ビットに縮めさせる(1976年)。
- 米政府は暗号化製品の輸出と使用を規制している。
- 米政府は鍵預託(Key Escrow)システムの開発を進めている。
  秘密鍵の政府に対する預託、あるいは復号のための回復鍵機能を付ける。

- 米国の主導で全地球自動傍受システム（Echelon）を運営している。
  （アメリカ、イギリス、カナダ、オーストラリア、ニュージーランド）
- 同時多発テロを機に米 FBI は主要 ISP に電子メイル傍受システムを設置。
- 中国、シンガポール政府は自国のインターネット通信を盗聴している。

- 欧州議会で携帯電話の通話場所について警察機関に情報を提供する法案が通る。

- 米諜報機関は、電源を切った後に RAM に残ったデータの痕跡や、10回上書きされた後のハードディスクのデータの一部を読み出す技術を持っている。

無線LANの安全性

無線ラン (IEEE802.11) の問題点

○ WEP(Wired Equivalent Privacy)

・暗号化初期ベクトルの選択が脆弱

・ユーザーごとに共通鍵を与える手段を示していない（全てのユーザーが同じ共通鍵を共有する）

・暗号化初期ベクトルの選択が脆弱

・鍵長が24bitしかない(リアルタイムでは不可能でもオフラインでは解読される可能性がある)

対応： AES を使用する。ホスト側での暗号機能を利用(IPSec, SSL)。

○ 誰でも接続が可能であることの問題

対応： MAC アドレスによるフィルタリング、RADIUSサーバーによる認証

結論
--- 如何に自衛すべきか ---

本当に有能なクラッカーが襲ってくれば防御することはほぼ不可能。
→ 防御は諦めてデータ(のバックアップ)を死守する。
多くの攻撃はスクリプトを利用したもの
→ 既に知られている脆弱性を塞ぐことで大部分の攻撃を回避できる。
セキュリティに力を入れていることを知らせることで、別の標的に向けさせる。

1. データの確保
- 定期的にバックアップをとるべし。
- 火事など災害の場合も考慮に入れる。

2. 機密性の確保
- 個人PC上で 暗号化するべし。
- 強いパスフレーズを使い、秘密キーのバックアップも忘れない(決してパスフレーズを忘れないこと)。
- バックアップ媒体の機密性にも注意。

3. 集団的自衛のために
- ログインパスワードを強くする。WWW サイトのログイン等で同じパスワードを使わない。
- Social Engineering に引っかからない。
- 怪しい添付ファイルを開かない(特に Windows)。
- 最新のパッチをあてる(CERT 等セキュリティ情報やWindows Updateを利用)。

References

- 暗号の秘密とウソ, Bruce Schneier (翔泳社,2001).
- CODE, Lawrence Lessig (翔泳社,2001).
- 大学におけるセキュリティポリシーの考え方 (国立情報学研究所, 2002).
- インターネットセキュリティの基礎 (NEC, 2002).
- クラッカー迎撃完全ガイド、Anonymous (インプレス, 2000).
- ハックアタック徹底解析, John Chirillo (ソフトバンク, 2002).
- UNIX & インターネットセキュリティ, G. Spafford and S. Garfinkel (O'Reilly, 1998).
- スーパーハッカー入門, Vladimir (Data House, 2000).
- JIS X5080 ドラフト, 日本工業標準委員会, 2002.
- Site Security Handbook (RFC2196), Barbara Fraser, 1997.

セキュリティ関連サイト

- CERT (Computer Emergency Response Team) http://www.cert.org/
- IPA (The Information-Technology Promotion Agency) http://www.ipa.go.jp/security/
- CIAC (Computer Incident Advaisory Capability) http://ciac.llnl.gov/ciac/
- JPCERT (JaPan CERT) http://www.jpcert.or.jp/

- シマンテック(Symantec) http://www.symantec.com/region/jp/
- トレンドマイクロ(Trend Micro) http://www.trendmicro.co.jp/