

不正アクセスとその傾向

ソフトウェア・コンサルタント

鈴木裕信

hironobu@h2np.suginami.tokyo.jp

IRTへの報告

1年間の不正アクセス報告数

- JPCERT/CC (96/10 - 97/9)
 - 不正アクセス情報提供**383**件
- CERT/CC (96)
 - 不正アクセス処理件数**2573**件
 - 問い合わせ件数
 - email 31268 件
 - hotline 2062 件

不正アクセスの警告

CERT/CC, JPCERT/CC のレポート

- 多種多様
 - sendmail,inn,cgi-bin/phf
 - SPAM, Mail Bombing
 - Trojan horse
 - Packet sniffers
 - Password Cracking

インターネットの現状

急速な拡大によるひずみ

- コンピュータは家電ではない
 - 数億のシステムが数十万で手に入る
- 管理には専門知識が必要である
 - システム管理者の質的 / 量的不足
 - 導入、運用に対する無理解

誰でも使えるはウソ

十分なスキルが必要

- 無免許の自動車ドライバー
 - 自分のコンピュータが何をしているのかわからない
- 無免許のバス運転手
 - いったい何パーセントのISPがまともに管理できているのか
 - そもそも数が多すぎるISP

背景知識の欠如

コンピュータ技術や文化の知識の欠如

- 技術的ギャップ
 - 柔軟で多目的なシステム
 - 利用者以上に賢くはならない
- 文化的ギャップ
 - 技術はリスクを負いつつ急速に先に進む
 - 少数のフロンティアに立つ人たちが牽引
 - ハッカーの意味すら正しく伝わっていない

最大のターゲット

無防備なシステム

- まったく何もしていない
- 技術的に役に立っていない
- 古すぎて役にたたない

絶対的な数の増加

たとえ 0.1% でも

- 全体の数が数十万であれば

機械は疲れない

無差別にスキャンしてゆく

- DNS
- WWW Server Log
- etc.

すべてのサイトが対象

インターネットからアクセスできるマシン

- 成功・不成功を問わず
- 情報収集
 - マシンの種別
 - OS種別 / バージョン
 - 動作ソフトウェアのバージョン

踏み台の入手

価値のないサイトも価値がある

- 管理がずさん
- あまり使われていない
- 入手が簡単 / 発見されない

パスワード破り

破りと盗み

- ユーザのパスワードを破る
 - パスワードファイルなし
 - パスワードファイルあり
- パスワードを盗む
 - ネットワーク盗聴
 - ペテンにかける

ソフトウェアの脆弱(ぜいじゃく)性

バグはソフトウェアの宿命

- バグの発見 / 攻撃の発覚
 - 修正版リリース バージョンアップ
- タイムリーな情報収集
 - すぐに対応
- 運用技術不足・無関心
 - 不正アクセスの温床

ネットワーク盗聴

ほとんどの組織で考慮されていない

- 現状のイーサネットの欠点
 - 大学内
 - 企業内
- 防御
 - スイッチングハブ
 - IPv6

E-Mail Bombing

電子メールを大量に送り付ける

- 単純かつ簡単
- 攻撃側はトラッキングされやすい
 - 攻撃は短期的(すぐにブロックされる)
 - リスクが多く、果実が少ない

実際のクラッキングの技術レベル

高度な知識は不必要

- ありふれた手法
- 数撃ちや当たる方式
- マニュアル化 / パッケージ化
- ルーチンワーク

コンピュータ技術はいらない

詐欺師の才能があればいい

- パスワードを聞きだす
- 内部犯行
- 狂言

守る側と攻める側

攻める側が絶対的に有利

- 攻める側は、なんとかの1つ覚えで構わない
- 守る側は、オールマイティーな知識が必要
 - セキュリティは、典型的な応用技術
- ソースコードのないシステムは、絶対的に不利
 - ベンダーまかせで自分で動けない

防御と発見

やるべきことをやる

- ファイアウォールの正しい運用
- tcp_wrapper などによる記録
- ワンタイム・パスワードの導入
- SSL/SSH の導入
- 最新のセキュリティ情報を収集する
- 安全なバージョンで運用

やるべきことをやる人材を育てる

すべては技術者教育の問題に還元される

- 啓発活動
- 情報の公開
- 必要な技術の習得
 - 技術を理解できるだけのバックグラウンドが必要

インターネット・セキュリティ情報

JPCERT/CC

- URL <http://www.jpccert.or.jp>