abuse

~インターネット上の迷惑行為~

メディアエクスチェンジ株式会社
三ツ木 絹子(mitsugi@mex.ad.jp)

目次

- インターネット上の過去と現在
- どうして事件はおこるの?
- Abuseとその対策
- 防御のための技術
- 誰が頑張るの?

インターネットの過去と現在

昔々のインターネット

- 研究者のためのネットワーク
  - 利用者≒技術者
  - 相手の顔がわかる
  - 自己責任
- たかがしれたトラヒック
  - ほそーい回線
  - テキストベースの通信

昔の事件

- 研究者としての興味？
- 自己研鑽？
- 愉快犯
- 自己顕示欲
- セキュリティホールを教えてあげる

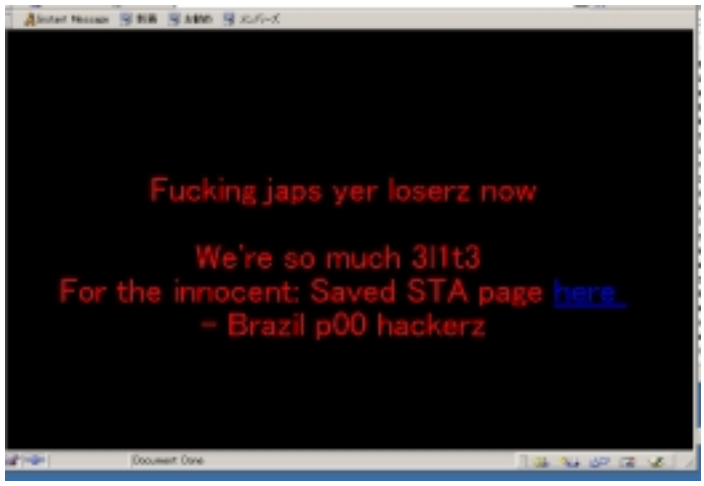
商用インターネット時代

- 商用プロバイダの出現
  - 利用者層の拡大
    - 誰が使うかわからない
    - プロも使う、素人も使う
    - 教育が追いつかない
  - ビジネスに群がる人たち
    - お金にかかわる情報のやりとり(EC)
    - お金儲けのためのコンテンツ(マルチメディア)

今までのインターネット上の事件

- サーバに侵入
  - クレジットカード情報を盗む(1985年)
  - 湾岸戦争に関する軍の情報を盗む(1990～1年)
- Webページの書き換え
  - 朝日放送Webページ書き換え(1997年)
  - 中国語圏クラッカーによる中央省庁のWebページ書き換え(2000年2月ころ、2001年2月ころ)
  - CIAなど、米国政府のWebページ書き換え(1996年ころ)

中央省庁攻撃事件



近頃のインターネット

キーワードは、
- ブロードバンド
- 常時接続
  - ADSL
    1.5Mから8M、12Mへ
  - CATV
  - FTTH
    .....

利用者も
利用アプリケーションも
増えたけれど、

! 苦情も増えました

利用者のスキル
が格段にアップし
たわけでは…

最近多い苦情

No.1 迷惑メール(広告メールを含む)

No.2 ポートスキャン

- ワーム等による侵入の試みとさらなる感染
- (D)DoS
- コンテンツの内容に関する苦情
  - 誹謗中傷・ワイセツ画像
  - 著作権侵害

どうして事件はおこるの?

事件をおこす人は誰?

- 産業スパイ
- テロリスト

プロ
お金は潤沢

- いたずら(自己顕示欲)
- いたずら(できごころ？)

アマチュア

- お仕事

広告目的

何を狙うの?

- 会社の資産
  - 顧客情報
  - 設計データや会議資料
  - 人事情報
  - 会社の計算機資源
- 提供しているサービス
  - Webサーバ、ネットワーク
- 私個人の情報

何をされるの?

- 通信の盗聴(のぞき見)
- ホスト上のデータの
  のぞき見/改ざん/削除
- なりすまし
- 踏み台
- サービス妨害
- 計算機資源や時間の浪費

どうして困るの?

- 情報が流出する
- 情報を失う
- 何が正しいか、わからなくなる
- 信用を失う
- お金を失う

どうして侵入されるの?

- プログラムのバグ
- プログラム/通信上の仕組みの仕様上の問題
- ユーザの操作ミス
- セキュリティ意識の甘さ

どうしたら防げるの?

- プログラムのバグがわかったら直す
- プログラム/通信上の仕組みの問題点を、できるだけ少なくする
- 必要ない通信を遮断する(アクセス制御)
- 本人であることを確認する(認証、認証局・証明書、署名)
- 他人から通信を見られないようにする(暗号化)
- 他人がデータを書き換えられないようにする(暗号化)
- 操作ミスをしないようにする(確認を何重にもする)
- 操作ミスできないような仕組みを作る(XXよけ)
- セキュリティ教育をする
- インターネットに繋がない

Abuseとその対策

ネットワーク関連のセキュリティ侵害

- ソーシャルエンジニアリング
- 個人情報流出
- ネットワークを介したセキュリティ侵害
  - ポートスキャン
  - 迷惑メール
  - ウィルス・ワーム・トロイの木馬
  - Denial of Service Attack (DoS)
  - その他

今回の話題

ソーシャルエンジニアリング

- 詐欺まがいの手口や、心の隙を突いた方法で侵入の糸口を得る
  - ゴミ箱のごみを漁る(パスワードを入手)
  - 肩越しにパスワードを盗み見る
  - 緊急を装って外部から入れるようにしろと言う
  - 業者を装う
  - 落し物から秘密情報を探る

ソーシャルエンジニアリングを防ぐ

- パスワード
  - 忘れにくいものをつけ、メモ書きを残さない
  - メモはシュレッダーする
  - 推測しにくく、かつ、キー入力しやすいものにする
- 身元確認
  - 作業フローを明確にし、緊急の用向きでも、身元確認を必ず行う(例：コールバック)
- ごみ管理
  - PC廃棄の際はディスクの中身を消す

ソーシャルエンジニアリング(まとめ)

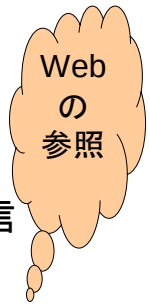
- 詐欺まがいの手口や、心の隙を突いた方法で侵入の糸口を得る
- ごみ漁り・業者のふり
- 緊急を装い、あわてさせる
- いつでも、身元確認をきちんとする必要有り
- 機器や紙の廃棄は完璧に

個人情報の流出

- 流出した個人情報を使われると
  - 個人の信用失墜・濡れ衣
  - 知らない間に名前を使われて契約
  - ストーカー?・嫌がらせ
  - なりすまして他人を誹謗中傷
- どこから漏れるのか？
  - ウイルス等によってPC上のデータを盗まれる
  - 企業・友人・知人・自分が原因
  - インターネット上のサービス

なぜ漏れる?

- 個人の場合は
  - 自分、友達のPCに侵入される
  - 懸賞サイト、アンケート、掲示板
  - うっかりミスで公開・送付
- 企業の場合は、
  - 盗まれる(お金になる)
  - うっかりミスで公開・送付
    - To:にユーザを列記してメールを送信
    - 見えるところに顧客情報を置いた
  - データの入ったPCを安易に廃棄



Webの参照

- UserAgent
  - Webを参照時に、自分の使っているOS、ブラウザ名がWebサーバへ送られる
- Cookie
  - セッション管理にCookieを使っていると、自分が過去にそのWebサイトにアクセスしたことが相手にわかってしまう
- Referer
  - Webサーバを参照すると、直前に参照していたURLがWebサーバに送られる。

個人情報流出の対策

- 少なくとも自分はセキュリティパッチを当て、ウィルスチェックをする
- 自分が信じても良いと思ったところにしか個人情報を書き込まない
- Webの参照については、
  - Cookie を Off にする
  - HTTP Proxyサーバ(代理サーバ)や、パーソナルファイアウォールを利用し、UserAgent や refererをWebサーバに送らない

個人情報の流出(まとめ)

- オンラインデータの個人情報が漏れることがある
- ユーザ自身がどんなに気をつけても漏れる
  - データを提供された側の不注意
  - データを提供された側への侵入
- Webをみるだけで、わかってしまう情報
  - クライアントのOSやブラウザ
  - 参照していたサイト

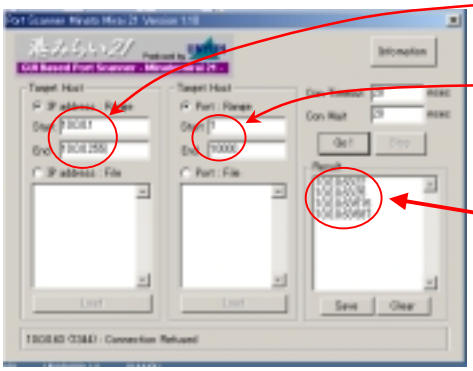
Cookieを受け付けない。
Refererを止める

ポートスキャン

- どのホストにどんなサービス(ポート)が提供されているか
  - セキュリティホールのあるサービスが上がっていないか?
    接続時のプロンプトメッセージからサービス(デーモン)のバージョンを推測
- OSの種類とバージョンを推測
  - セキュリティホールのあるOSを使っていないか？

ポートスキャンツール

- 例えば、10.0.0.0/24 に対して、ポートスキャンしてみる



スキャンするIPアドレスを指定(10.0.0.0/24)

スキャンするポートを指定(1～10000)

開いているポート
この場合、10.0.0.63の22(ssh)、25(smtp)、515(printer)、587が開いている

ポートスキャンの対策

- 必要の無いサービスを停止
  - インストールしたままで、なんでもかんでもサービスがあがっているのは危険
  - テストで立ち上げたサービスをそのままにしていないか？
  - サービスのバージョンを隠すのも有効
- 適切な相手に、適切なサービスを
  - 適切なアクセス制御
    - tcpwraper などの利用
      例：Webは全インターネットへ提供、
      ftpは会社からだけ

ポートスキャン(まとめ)

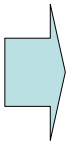
- 侵入のためのファーストステップ
- ネットワークに存在するホストを探索
- 口を開けて待っているサービスを探索
  - セキュリティホールのあるサービスを探索
- 不要なサービスは止める
- アクセス制御を行う
- セキュリティホールを塞ぐ
- サービスのバージョンを隠すのも有効

迷惑メールとは?

- 広告メール(迷惑メール)
  - 無差別に
  - "広告"らしき内容のメールを送付
  - 携帯電話のメールアドレス(特にiモード)へ
  - 身元を隠すために Open Relay を行うメールサーバを利用
  - メールの発信を専用に行なう業者
  - メールアドレスリストの売買

悪用されるOpen Relay

- メールの不正中継
  - どこからきたメールでも中継
  - 自分と関係ないサイトのメールを中継

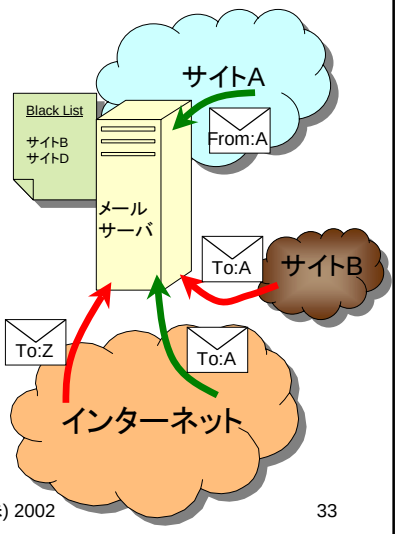


問題点

- 計算機リソースの無駄使い
- 迷惑メールの温床に
- 加害者として扱われる

Open Relayの対処方法

- 関係あるサイトのメールのみ転送
  - メール配送プログラムの設定
  - メール送信時に認証機構を導入
    (SMTP_AUTHなど)
- ブラックリストに載っているサイトからのメールを拒否

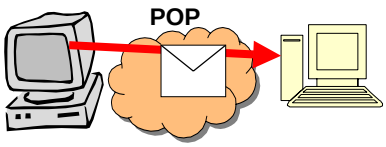


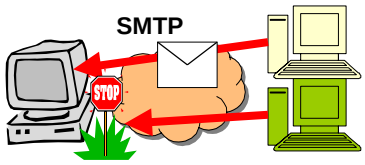
メール配送プログラムの設定

- たとえばsendmail の設定
  - Sendmail 8.8.X 以上でないと、迷惑メール対策ができない(check_relay ルーチンの利用)
  - Sendmail 8.9.X 以降は、デフォルトでメールのリレーは無効に
  - From:が自分のドメイン名(例:yyy.co.jp)ならリレーする、にしてしまうと、From:をyyy.co.jpと偽造されると、メールをリレーしてしまうので注意
  - ブラックリスト(ORBSなど)を利用も可

認証機能付のメール送信

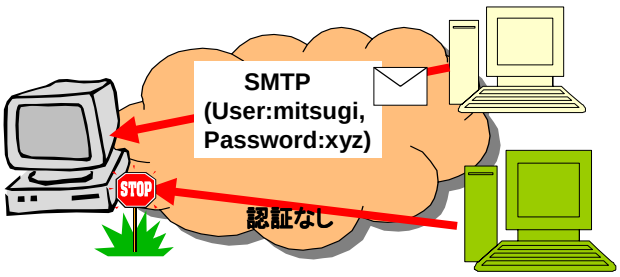
- POP before SMTP
  - メールの配送を行う前に、POPで認証を行う。
  - POPで認証を行った後、POP元のアドレスからのSMTPを許可





認証機能付のメール送信

- SMTP__AUTH
  - メールの送信を行う前に、認証を行う(時間は関係なし)



Open Relay修正の確認

- 自分で確認する

```
% telnet mail.xxx.co.jp smtp
Trying 10.10.140.5...
Connected to mail.xxx.co.jp.
Escape character is '^]'.
220 mail.xxx.co.jp IMS SMTP Receiver Version 0.83 Ready
helo mex.ad.jp
250 OK
mail from: <abuse@mex.ad.jp>
250 abuse@mex.ad.jp OK
rcpt to: <abuse%mex.ad.jp@mail.xxx.co.jp>
250 abuse@mex.ad.jp OK
quit
221 mail.xxx.co.jp closing
Connection closed by foreign host.
```

ここが、Rejectedにならないとだめ

- Webサイトで確認をする
  - 例: http://www.nanet.co.jp/rlytest/relaytest.html

迷惑メールのフィルタ

- プロバイダによるメールフィルタ
  - ヘッダ情報から明らかな迷惑メールの破棄
  - From 等により、迷惑メールをフィルタ(個別)
- メーラによるメールフィルタ
  - メーラの設定により要らないメールを選別/削除
    From や 特定の文字列で判別
- 個人でメールフィルタソフトの導入

迷惑メールを受け取った

- 迷惑メールの送り主への連絡
  - From: の宛先へ
  - 本文内のURLに掲載されている問い合わせ元へ
  - Whoisに登録されている連絡担当者へ
  - 中継しているメールサーバの管理者へ
    - Postmaster や abuse 宛
  - JPCERT/CCではサポート外
- 相談窓口・情報提供窓口へ(後述)

連絡する内容

- 私は〇〇です。
- 受け取ったメールの内容(ヘッダも含めて)
  - 受け取ったメールをヘッダも含めて添付するのがベスト
- どうして欲しいかを書く

連絡仲介ツールの利用

- SpamCop (http://spamcop.net)
  - 問い合わせの際、相手が何者かわからないため、名乗りたくない
  - 誰に対応を依頼すればよいかわからない
    - 迷惑メールをSpamcopに登録すると、Spamcopが本文やヘッダを手がかりに問い合わせ元を調べ、メールで対応を依頼

不親切なメーラ

- ヘッダを消してしまうメーラ
  - たとえば i-mode
    - メール送付の経路が全くわからない
    - 問い合わせをする場合は、メール本文のURLから送り主を想像する
- From:を消してしまうメーラ
  - たとえば i-mode
    - 送り主は、「きぬこ」
    - メールアドレスすらわからない

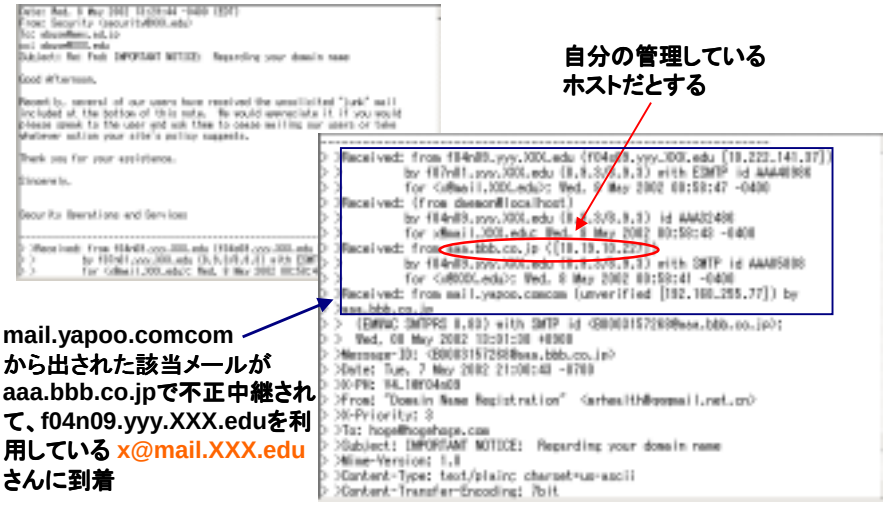
問い合わせメールを受け取ったら

- 何を依頼されているかを確認する
  - 迷惑メールの場合は、迷惑メールの停止
  - 迷惑メール発信者の特定と連絡
    などを依頼されることが多い
    ただし、発信者の詳細についてはプライバシーに関わることもあるので注意
- 調査すべき対象の確認
  - ヘッダや本文に記述のある、IPアドレスやURLを確認

対応のポイント

- 問い合わせ元は、イライラしている
  - 調査を開始したことをできるだけ速やかに伝える
  - こちらの立場を客観的に伝える
  - あまりへりくだらず、事務的にかつ丁寧に伝える
  - 過度の期待は持たせないような文面にする
  - 疑問点、情報不足があれば質問する
  - 対応できない点があれば、あらかじめ伝える

調査の具体例



自分の管理している
ホストだとする

mail.yapoo.comcom
から出された該当メールが
aaa.bbb.co.jpで不正中継され
て、f04n09.yyy.XXX.eduを利
用している x@mail.XXX.edu
さんに到着

HotmailなどのWebメールの場合

```
Return-Path: <XXXXXX7482@hotmail.com>
Received: from  XXX-YYY.mx.aol.com (XXX-YYY.mail.aol.com [172.16.105.229]) by
X-YYY.mail.aol.com (v90.10) with ESMTP id MAILINXF51-1213005328; Fri, 13 Dec
2 00:53:28 -0500
Received: from  hotmail.com (AAA.BBB.hotmail.com [207.68.xxx.xx]) by XXX-YYY.
aol.com (v90.10) with ESMTP id MAILRELAYINXF54-1213005323; Fri, 13 Dec 2002 0
3:23 -0500
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
         Thu, 12 Dec 2002 21:48:49 -0800
Received: from 10.15.147.133 by AAA.BBB.hotmail.msn.com with HTTP;
        Fri, 13 Dec 2002 05:48:49 GMT
X-Originating-IP: [10.15.147.133]
From: "Cabrera Guevara" <>
To: x
Cc: x, x, x, x,
        x, x, x,
        x, x
Subject: Increase Your Sales Today!
Date: Fri, 13 Dec 2002 05:48:49 +0000
Mime-Version: 1.0
```

クライアントのアドレス
(10.15.147.133)が
しっかりと。

立場の違い

- 迷惑メールの感じ方は立場によって違う
  - インターネットでダイレクトメールを送る業者
    - 郵便で来るダイレクトメールと同じ
    - 街で配られるチラシと同じ
  - 受け取る側は不快
    - 特に出会い系サイトへの誘い(生理的に嫌)
    - 受け取り側へのメール課金問題
    - 重要なメールが埋もれる
    - メールボックスが溢れてメールを受け取れない

迷惑メール関連法案の問題

- 元々、特定商取引法を守っていない業者が問題
- 名前を書けば送ってよいのか？
- 「未承諾広告※」と書かれたメールがたくさん届くようになっただけ…
  - プロバイダ側がフィルタをしてくれないと意味なし
  - フィルタしにくいパターンマッチ文字列

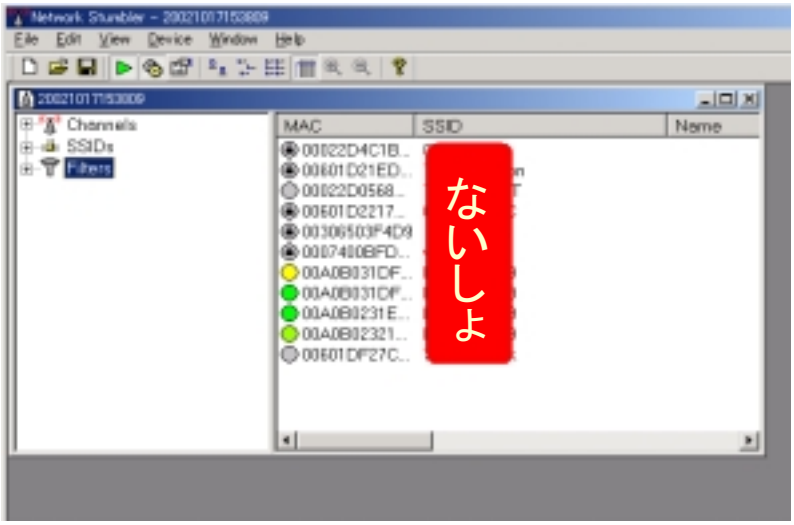
「未承諾広告※」

- プロバイダがフィルタしようとしても。。。
  - 明らかな違反表示
    ※未承諾広告
  - 微妙に守られていない表示
    冒頭から連続して 未承諾広告※ と記述が◎
    未承諾 広告※　未承諾広告 ※ 末承諾広告※
- 受信ドメイン指定と未承諾広告が排他

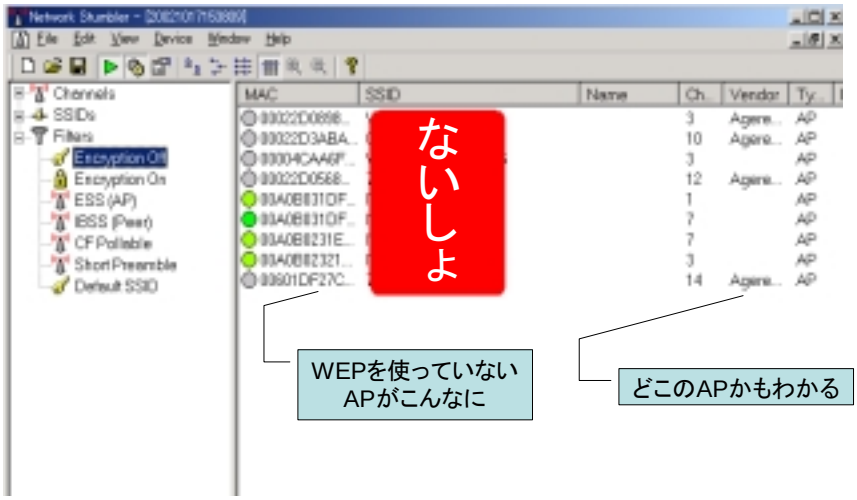
無線LANの悪用

- 無線LAN
  - 認証機構を利用していないアクセスポイント
    - 使ってくださいと言っているようなもの
    - 繋がってしまえば、正規ユーザと同様に利用
    - アクセスポイントをごそごそ探す、ケーブルを繋ぎこむという不審な行動をしなくてよい
  - 無線LANの認証機構
    - WEP キーの利用(通信の暗号化も可能)
    - Mac アドレスの登録　　etc…

とあるところの無線LANの状況



WEPを利用していないAP



迷惑メール相談窓口

- 相談窓口
  - 日本データ通信協会
    「迷惑メール相談センター」
    - 電話番号　03-5815-7201
    - 受付時間　10:00～17:00
      （土日・祝日、年末年始を除く）
    - 電話でのみ受付
    - 内容は、迷惑メールに関してのみ

違反メールの情報提供窓口

- 特定商取引法
  （財）日本産業協会
  03-3501-3344
  http://www.nissankyo.or.jp/
  mailagain@nissankyo.jp
- 特定電子メール法
  （財）日本データ通信協会 「迷惑メール相談センター」
  03-5815-7201
  http://www.dekyo.or.jp/
  mailagain@dekyo.or.jp

迷惑メール(まとめ)

- 迷惑メール=広告メールがほとんど
- 少なくとも自分は不正中継に加担しない
  - Open Relay サーバにならない設定
  - 認証付 SMTP の利用
- 迷惑メールを受け取った場合
  - 情報を隠しすぎても対応はできない
  - 受信者課金タイプのメールシステム側の対策

確信犯もいるので、現状では抜本的対策は困難

ウィルス・ワーム・トロイの木馬

- ウィルスとは、プログラムのこと
- ワームやトロイの木馬も広義のウィルス
  - ワームは、自分のコピーを作って次々に伝播
  - トロイの木馬とは、送り込まれたプログラムを実行してしまうことにより
    - パスワードなどホスト上の情報を盗まれる
    - 自分のホストの制御を奪われる

      BO2K、Netbus etc…

ウィルス・ワーム対策

- セキュリティホール対策のパッチを当てる
- 知らない人からのメールは読まない
- 知っている人からのメールでも、いつもと雰囲気が違うものは読まない
- 添付ファイルを安易に開けない
- 信用できるか不安なサイトを閲覧しない

自分を守るのは自分でしかありません！

最近のウィルスやワームの傾向

- 手口が巧妙に
  - 2重拡張子を用いる
    - 危なそうな拡張子をわざとわからなくする
      bbb.txt.shs　　見かけ上は、bbb.txt
  - ソーシャルエンジニアリング的手口
    - I Love You ウィルス
      もし、社内の素敵なあの人から来たら？
    - Happy99
      直前のメールに添付し忘れました風を装う

2001年の大騒ぎ

- 自立分散型ワーム(CodeRed、Nimda)
  - 自動的に次々に感染、仲間を増やす
  - 感染手法が複合型に
    - メールの添付ファイル
    - Exploreのプレイメージ表示
  - 感染した後に、集団でターゲットホスト攻撃
    - DDoS 攻撃へ
  - 人手を介さないので、対策をとられるまで感染の勢いはおさまらない

ウィルスチェッカ

- ウィルスチェッカ
  - エンドユーザの端末へインストール
  - メールサーバ等のゲートウェイにインストール
- 利用上の注意点
  - ウィルスデータベースを最新版にする
  - リアルタイムスキャン(常にチェックする)にする
  - 定期的に全てのディスクやFDをチェックする
  - メールサーバ適用タイプの場合は、感染メールの取り扱いに注意

ウィルス(まとめ)

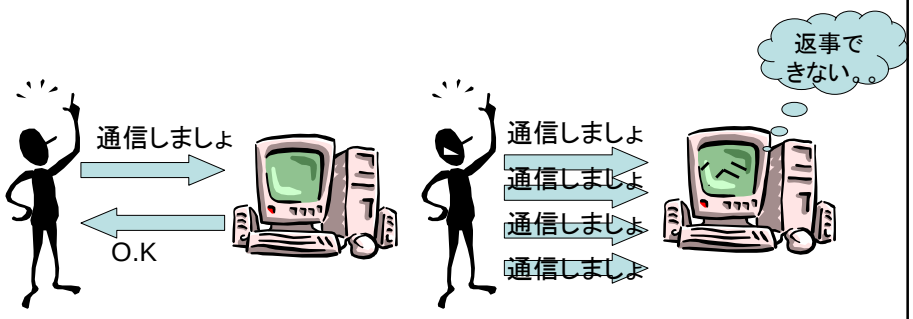
- ウィルスは、システムに故意に悪影響を与えるプログラム
  - ワーム、トロイの木馬も広義のウィルス
- 最近の感染経路は、
  - メールの添付ファイル
  - Webの閲覧

興味本位のWeb閲覧、知らない人からのメール添付ファイルの開封はとっても危険

- セキュリティホールを塞ぐことが重要
- ウィルスチェッカは、最新ウィルスDBで利用

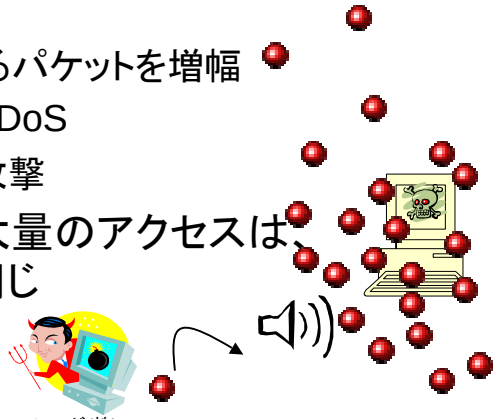
DoS

- 負荷をかけて、通常のサービスが提供できないようにする



(D)DoS

- DoS(Denial of Service Attack)
  - 送信元を偽造
  - ターゲットへ送信するパケットを増幅
  - 分散型(Distributed)DoS
  - 不特定多数からの攻撃
- 攻撃ではなくても、大量のアクセスは、見かけ上はDoSと同じ



ワーム・DoS連係型

- ワームにより感染、ターゲットを攻撃する
  - 手先をたくさん作っておく
  - 攻撃の首謀者がわからなくなる
  - 苦労なく大量のアクセスを発生
    - 塵も積もれば。。。

      ブロードバンドネットワーク時代

DoSを防ぐ

- サーバについて
  - セキュリティホールを塞ぐ
  - 必要のないサービスを停止する
    DoSの対象となる要因をできる限り削減する
  - ロードバランシングをして、負荷を分散する
- ただし、抜本的な対策はない

DoS(まとめ)

- 大量のアクセスやプロセスを発生させ、正常にサービス提供をできないようにする
- 犯人は身元がわからないようにする
  - 送信元を偽る
  - 踏み台(手下)を作る
    - アクセス数も増える
    - 分散型のDoS（DDoS)

  ブロードバンド化が進みトラヒックも莫大に
- 不要なサービスを停止
- セキュリティホールを塞ぐ

⇒ **ただし、抜本的な対策なし**

攻撃を受けている

- 攻撃をしている相手への連絡
  - 相手の利用しているISPへ連絡
    - Whoisや、tracerouteを利用
  - 相手に直接連絡
    - Whoisや、abuse@ xxx.co.jpへ
    - 攻撃相手は、**本当に悪い人**かもしれないことに注意
  - JPCERT/CCへ連絡、仲介を依頼する
    - info@jpcert.or.jp

調査依頼する内容

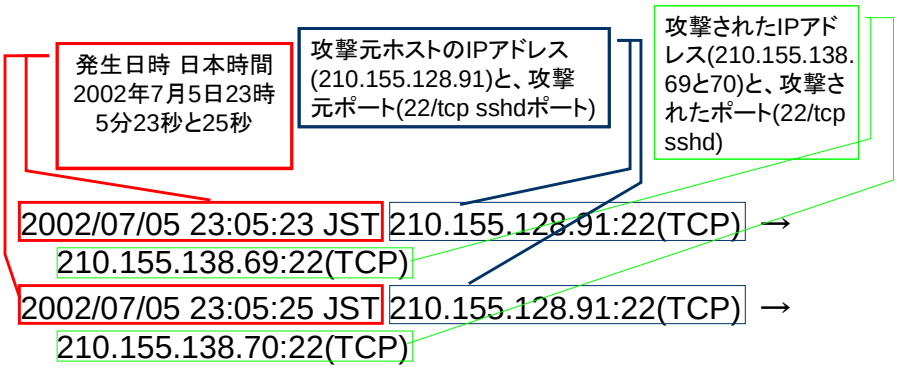
- 私は〇〇です。
- ××をされました。
  - 〇月×日　△時□分～☆時△分まで
  - XXXからYYYの、ZZZに対してアクセスを受けた
- △△をしてください。
- アクセスログを添付すること

困った問い合わせ

- 攻撃を受けました。なんとかしてください。
  - いつ攻撃を受けたのかわからない
  - どんな攻撃を受けたのかわからない
  - 誰が攻撃したのかわからない

•問い合わせを受けた側はたくさんのホストを持っているかもしれない
•問い合わせを受けた側が調査をできるような情報提供を

対応の例



ログを解析上の注意

- 発生時刻について
  - ロケーションの確認
    日本時間にしたら何時なのか？
  - 時刻は合っていないこともある
    合っていないこともあるのでそれを念頭に調査
- 攻撃元について
  - 詐称されている可能性がある
  - 自分のホストのログの検証をきちんと行う

ISPの場合

- 該当時刻の攻撃元ホストを調べる
  - 攻撃元ホストは誰(顧客)の管理下か?
    - まずは、現在稼動しているか?
    - 顧客情報から担当者を特定
    - ダイアルアップの場合はログから顧客を特定
  - 該当者に、調査依頼を行う
    - 問い合わせメールを添付
    - 問い合わせメールの内容を簡単に解説

攻撃元ホストの管理者

- 該当時刻に対象ホストが稼動していたか？
- 対象ホストの現状を確認
  - 今も攻撃していないか？
  - ログを確認、自分が本当に攻撃したのか？
    - messages
    - acct
    - syslog

インシデント対応

- 調査対象を特定
- 現在の状況は？
  - 現在も攻撃しつづけている
  - 自ホストを破壊している
- ログはあるのか?
- 関係者への連絡
- 復旧プラン

調査と復旧

- 状況調査のために必要なことをあらかじめ用意しておく
  - ネットワーク構成図
  - 設定情報
  - 関係者連絡先
- 復旧しやすいようなシステム構成をとる
  - 機能単位ごとに分割してシステム構築
  - 冗長構成

警察の方から連絡があったら

あれやこれやと言われますが、、、、

- 弁護士に相談しましょう
- 安易に答えるのは危険です
  - 捜査関係事項照会書
- 必要以上に抵抗するのも危険です
  - 差し押さえ令状 → ブツ差し押さえ

防御のための技術

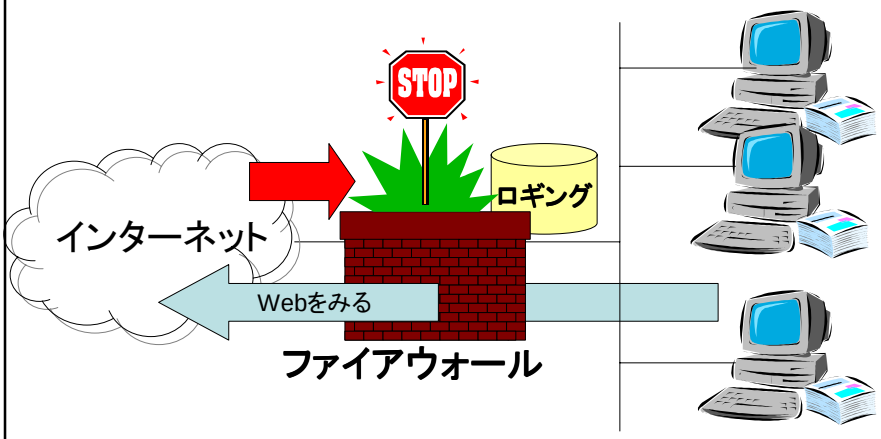
Abuseを防ぐ/減らす技術

- サーバ側
  - (いわゆる)Firewall
    - 不必要なアクセスを遮断する
  - IDS (Intrusion Detection System)
    - 不正と思われるアクセスを検出、通知する
  - その他
    - パッチ（修正プログラム）の適用
    - 設定確認 etc...

Abuseを防ぐ/減らす技術

- クライアント側
  - ウィルスチェッカ
  - パーソナルファイアウォール
    ウィルスチェッカ＋
    パーソナルファイアウォールの製品も販売
  - ブロードバンドルータ
  - セキュリティパッチ
  - (自制心)

ファイアウォール



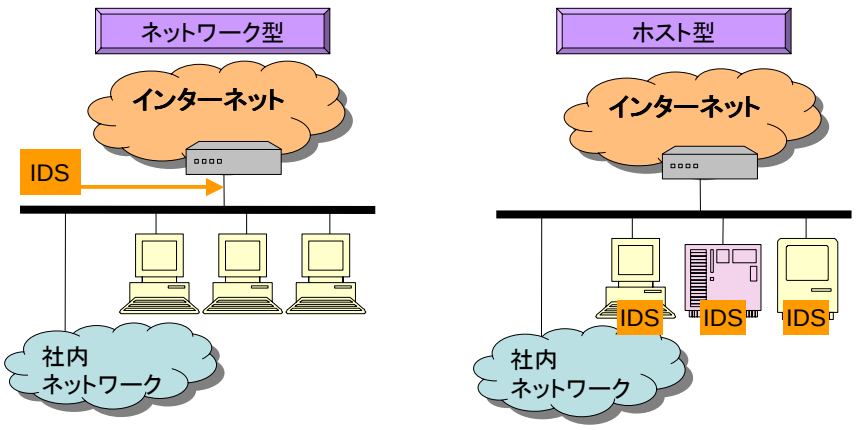
ファイアウォールがあれば！

- 万全か？
  ファイアウォールが無いから侵入された?
  - 許可したサービスで侵入される
  - メール経由でウィルスやワームに感染
  - Webの閲覧をしたらウィルスやワームに感染
  - DoSで回線真っ黒け

  ファイアウォールを守る努力
  - ファイアウォールのバグをつぶす
  - 設定ミスを減らす

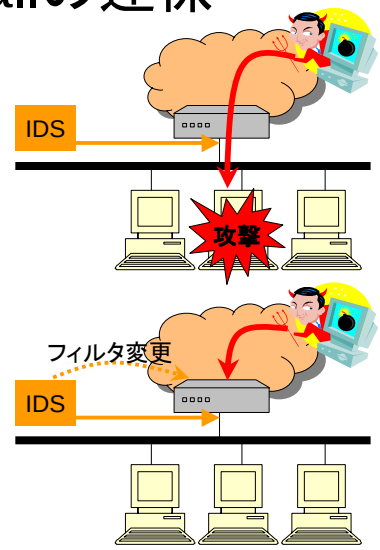
IDS

- 攻撃されていることを検出、通知する



IDSとFirewallの連係

- IDSで攻撃を発見
  - 該当セッションをFirewallで切断
  - 該当ネットワークからのアクセスを遮断するため、Firewallのフィルタを動的に変更



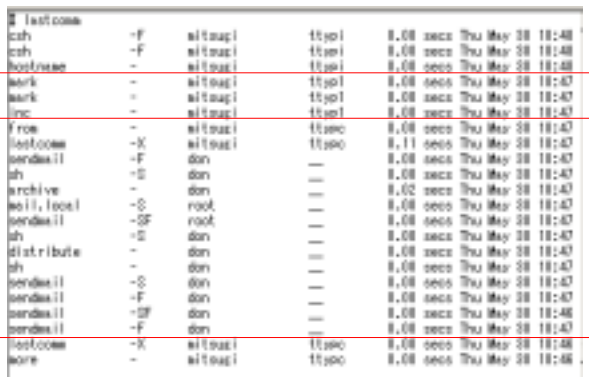
設定の確認

- 自分で、複数人数で何度も確認する
- 設定を変更したことの記録を残す
  - sudo などの活用
- 設定の履歴を残す
  - CVS、RCS
- 擬似的に自分のサイトを攻撃してみる
  - nmap などの活用
- 設定が変更されていないことの確認

ユーザの行動記録

- 何が行われたのかを知るためにとっておく
  UNIX 系 OS
  – acct (コマンドと、IDだけ)
    # acct /var/adm/pacct
      acct を /var/adm/pacct に採取する
    # lastcom
      acct 情報を出力
  – C2audit
    Openされたファイル名までわかる

Acctを見る



rootの行動を記録

- sudoコマンド
  - rootになれる人を限定
  - 利用できるコマンドを限定
  - 利用したコマンドを記録

    インシデントがあった場合には、この記録を参照
    - 誰が行ったのか
    - 何が行われたのか

sudoのログ

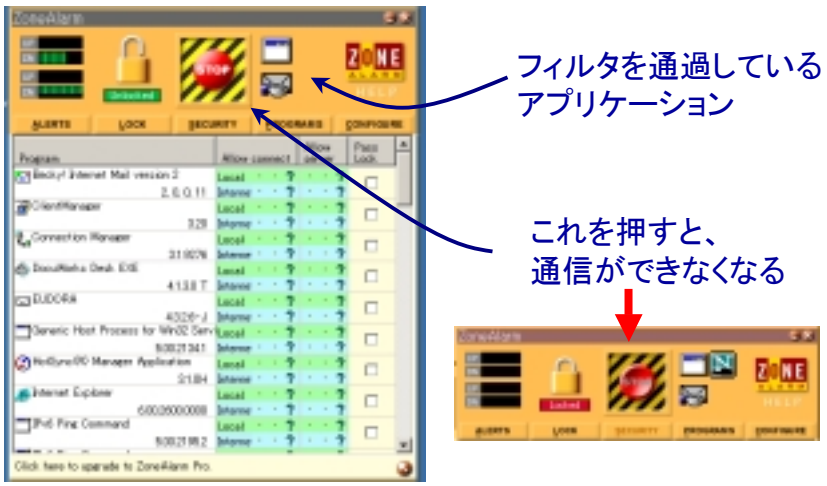
```
sudo access:
Jun 15 15:35:21 mail /usr/local/bin/sudo:  mitsugi : TTY=ttyp0 ; PWD=/etc ;
 USER=root ; COMMAND=/usr/bin/co -l aliases
Jun 15 15:35:28 mail /usr/local/bin/sudo:  mitsugi : TTY=ttyp0 ; PWD=/etc ;
 USER=root ; COMMAND=/usr/bin/vi aliases

Jun 17 22:32:56 mail sudo:  mitsugi : TTY=ttyp0 ; PWD=/var/home/mitsugi ; U
SER=root ; COMMAND=/usr/sbin/vipw
Jun 17 22:35:00 mail sudo:  mitsugi : TTY=ttyp0 ; PWD=/var/home/mitsugi ; U
SER=root ; COMMAND=/bin/cat /etc/master.passwd
Jun 17 22:35:28 mail sudo:  mitsugi : TTY=ttyp0 ; PWD=/var/home/mitsugi ; U
SER=root ; COMMAND=/usr/bin/passwd don
```

パーソナルファイアウォール

- エンドユーザのホスト毎に入れるアクセスフィルタとログ機能
  - 内→外、外→内 のアクセスを制限

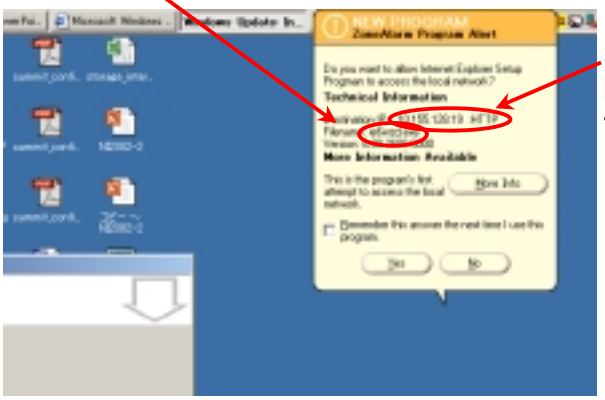
    内→外のアクセスを監視するので、自分がワーム、トロイの木馬にかかった時の発見にも役立つ
  - フィルタをビジュアルに、インタラクティブに設定
  - 許可していないアクセスがあると、アクセスはブロックされ、警告が画面に表示される

パーソナルファイアウォール



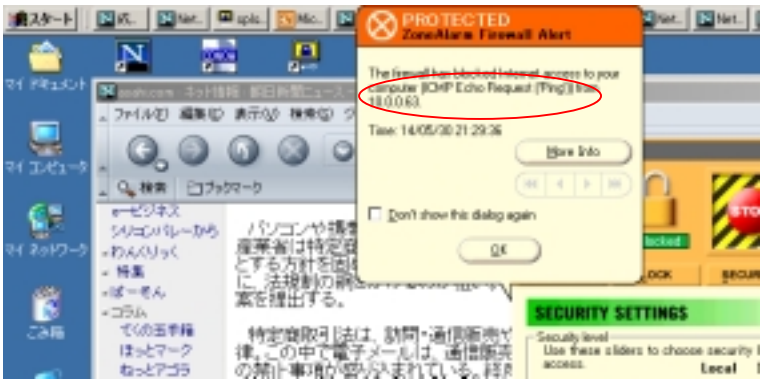
パーソナルファイアウォールの利用例

- 新しいアプリケーションを起動した例



パーソナルファイアウォールの利用例

- 10.0.0.63 からPingを受けて、ブロックした例



ブロードバンドルータ

- ブロードバンドの機能をうまく使って、インターネットからのアクセスを制限する
  - NAT
  - フィルタ機能
  - IDS機能
  - ログ書き出し機能
  - Ping不応答機能

機種によっては サポートされて いない機能もある

- 設定はGUIでわかりやすい(はず)

クライアント側の防御の問題点

- 設定ミス
  - 勘違い、オペレーションミス
  - どのフィルタを開ける必要があるか?

    初めは怖いから全部閉じる

    »通信できない→ 結局開けてしまう
- 警告やログの読み方がわからない
- 調査のため、ログをお願いしてもログの送付方法がわからない

とんちんかんな問い合わせ

- 送信元とあて先を勘違いした問い合わせ
  - 不正なHTTPアクセスを受けています
    自分がHTTPでアクセスしているんじゃない?
    自分が見ている.html内の参照先じゃない?
- ICMPに関する問い合わせ
  - ICMPの警告 ＝ Pingされたのだ！
    実は、単に Host Unreach が返っていたりする

結局、ログを見せてもらい、
問い合わせを受けた側が解析

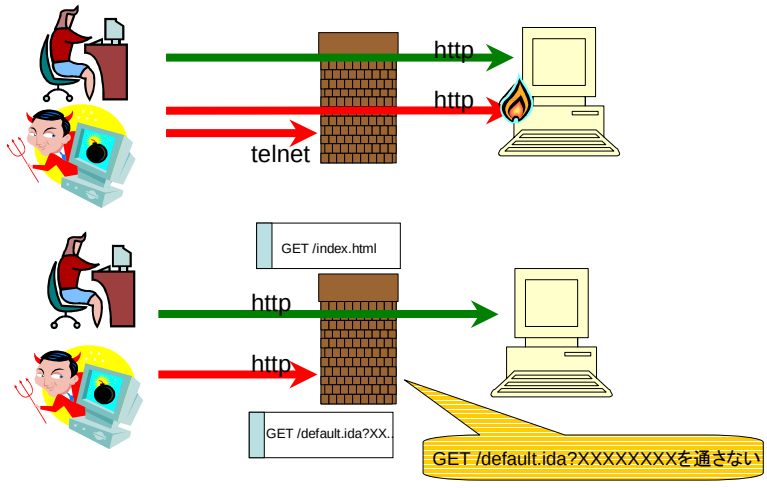
誰ががんばるか?

ISPが頑張ればなんとかなる?

- ネットワークの接続元でなんとかできるか？
  - ISPは、検閲を禁止されている

- ISPは通信状況を把握しないといけない
- ペイロードを解析したくなることも…
  - ISPで対応できることの限界
  - ログをとることを推奨する警察との整合性は？

ペイロードを解析する必要性



役割分担と協力