スパマ・アタッカは
他人ゴトにアラズ

～ 加害者に仕立てあげられないための予防と
インシデント対応～

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

- 今年の話題とその背景
- インターネットセキュリティと迷惑行為
- スパマ・アタッカにならないために
- 問い合わせへの対応
- まとめ

今年の話題

- blaster worm
- MS SQL
- SSH、SSL
- sendmail
- IOS

etc...

その一方で、相変わらずCodeRedなど、
従前の問題に関する被害の問い合わせも

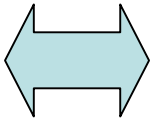
背景

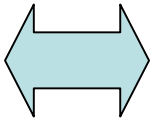
- インターネット利用者層の拡大
  - 平成14年末で全人口の50%を超える
    (携帯電話、ゲーム機含む)
- エンドユーザの接続帯域の増加
  - ADSL 8M，12M，24M，40M?!
  - FTTH

    http://www.soumu.go.jp/s-news/

インターネットの浸透

- 生活基盤として定着
  インターネットで成り立つ金儲け
- 誰もが使うインターネット


誰もが危険、迷惑にさらされる可能性


誰もが悪者になる可能性

過去は平和だったのか？

- 最初の事件
  - モリスのワーム
    - CERT/CC 設立のきっかけに
- 特徴
  - いたずら(愉快犯)
  - 自己研鑽
  - 自己顕示
  - セキュリティホールを教えてあげるため

あのころのインターネット

- 主に研究者が利用するネットワーク
  - 相手の顔がわかるくらいの利用者数
  - 自己責任
  - トラヒックもたかがしれている
  - テキストベースの通信
  - ほそい回線(T1の回線があれば天国)

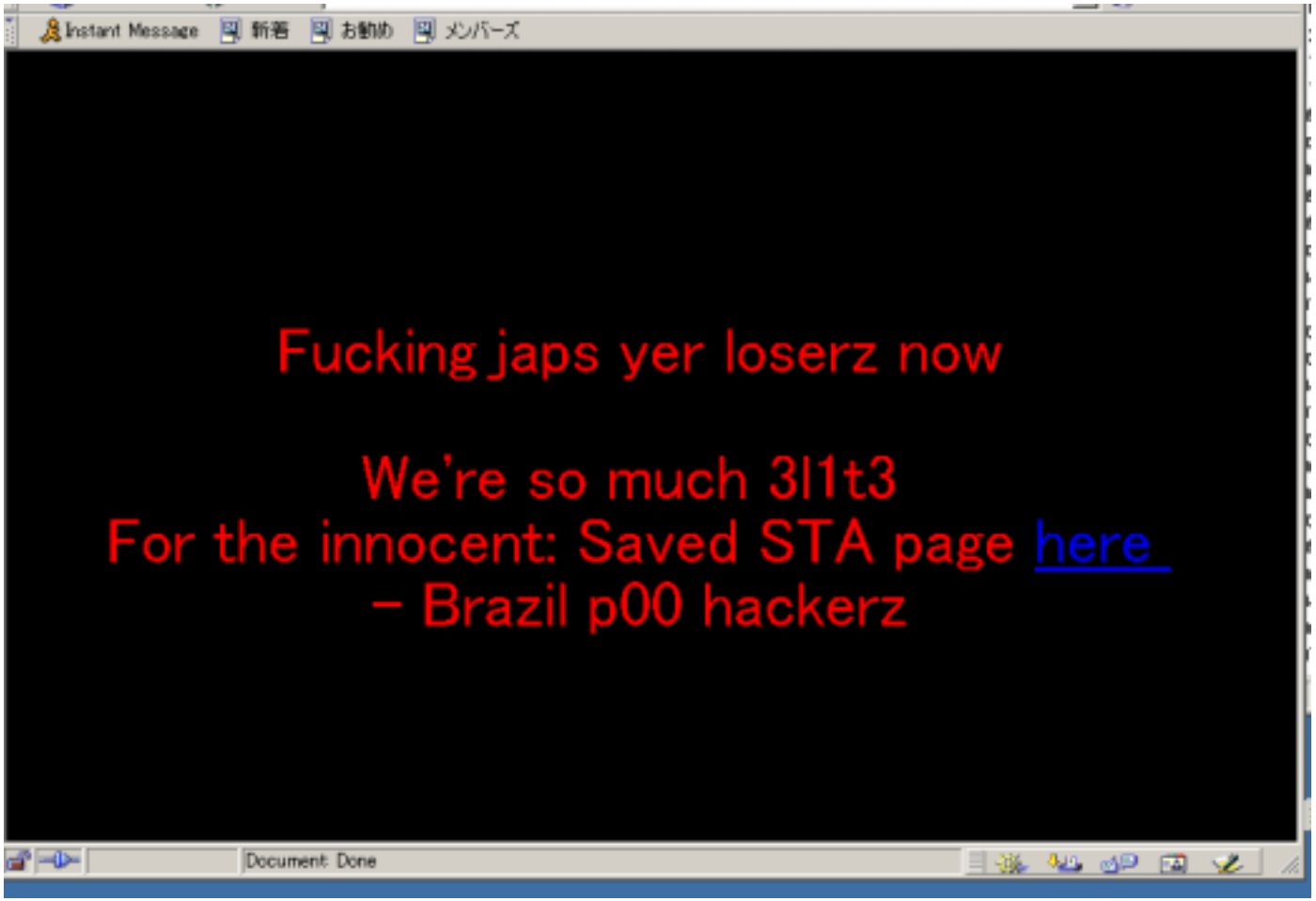
WorldWideWebの登場

- 特にWWW
  - 組織の"顔"、"玄関"としてのWebページ
  - Webページを書き換える

    インパクトが強い、目立つ

- 2000年、2001年に中央省庁等の Web ページ書き換え事件が多発

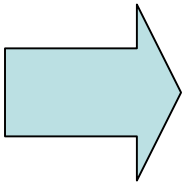
中央省庁攻撃事件



各組織がインターネットに接続

- インターネットを介したビジネス
- インターネットを利用したビジネス
- 拠点間をインターネットで結ぶ
  - お金になる
  - 機密

情報が
インターネット上に存在



お金目当ての犯罪
政治的な犯罪

現実社会とインターネット

- 現実社会で起こること
  インターネットでも起こる
- 特徴
  - 匿名性が高い
  - 技術の進歩が早い
  - 法整備不足
  - リアリティがない
    (危機感を持ちにくい)

インターネットセキュリティ
と
迷惑行為

セキュリティが必要になる理由

- 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

何をされるのか

- 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

どうして困るのか

- 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か

- プログラムのバグ
- プログラム/通信の仕様上の問題
- 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か

- プログラムのバグがわかったら直す
- プログラム/通信の仕様の問題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

迷惑行為

- 誹謗中傷
- 著作権侵害
- ワイセツブツ?陳列
- 詐欺
- 迷惑メール(広告メール含む)

etc...

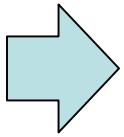
迷惑メールとは?

- 広告メール(迷惑メール、スパム)
  - 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

スパマ・アタッカに
ならないために
<スパム編>

スパマにならないために

- ネットワークで行なうこと
- 計算機で行なうこと

   一般的なセキュリティ対策(後述)

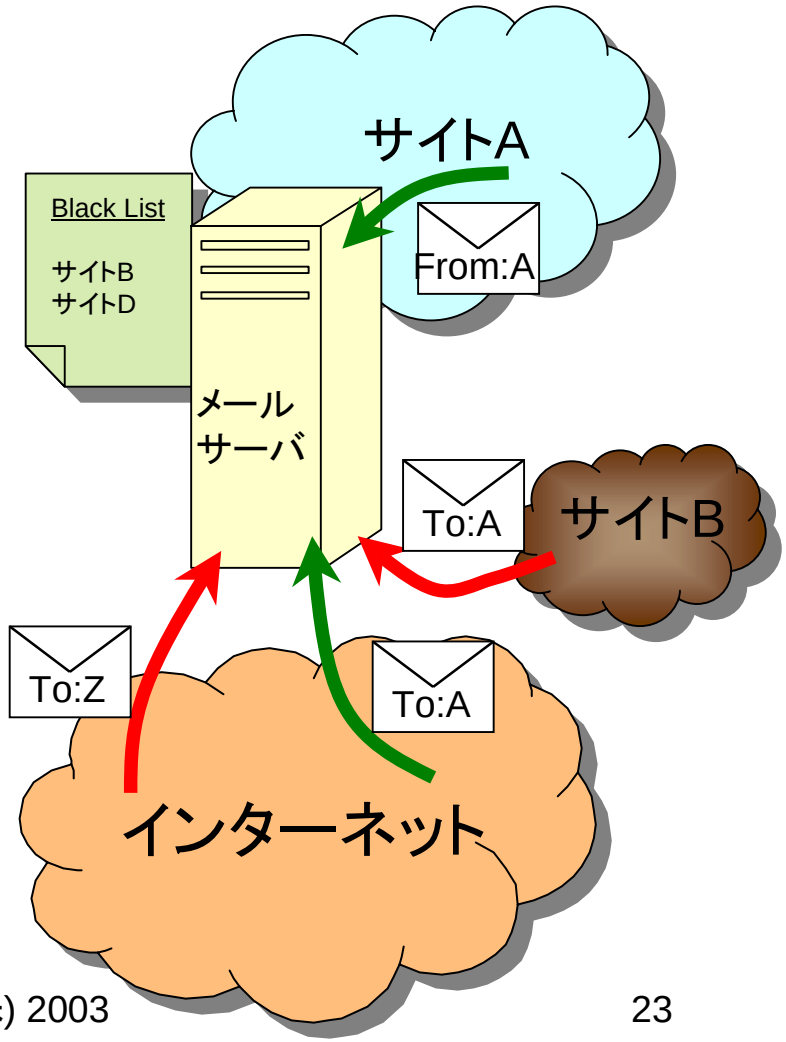
- メール配送システムで行なうこと
  (Open Relay対策)
- サービスで気をつけること

Open Relayとは

- メールの不正中継をしてしまう
  - 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

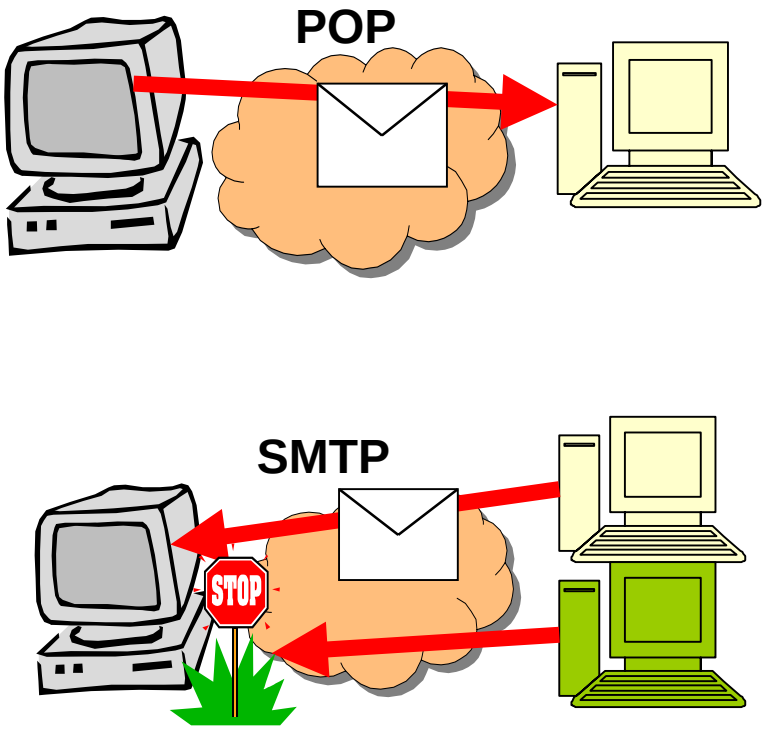


メール配送システムの設定

- 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(ORDBなど)を利用も可

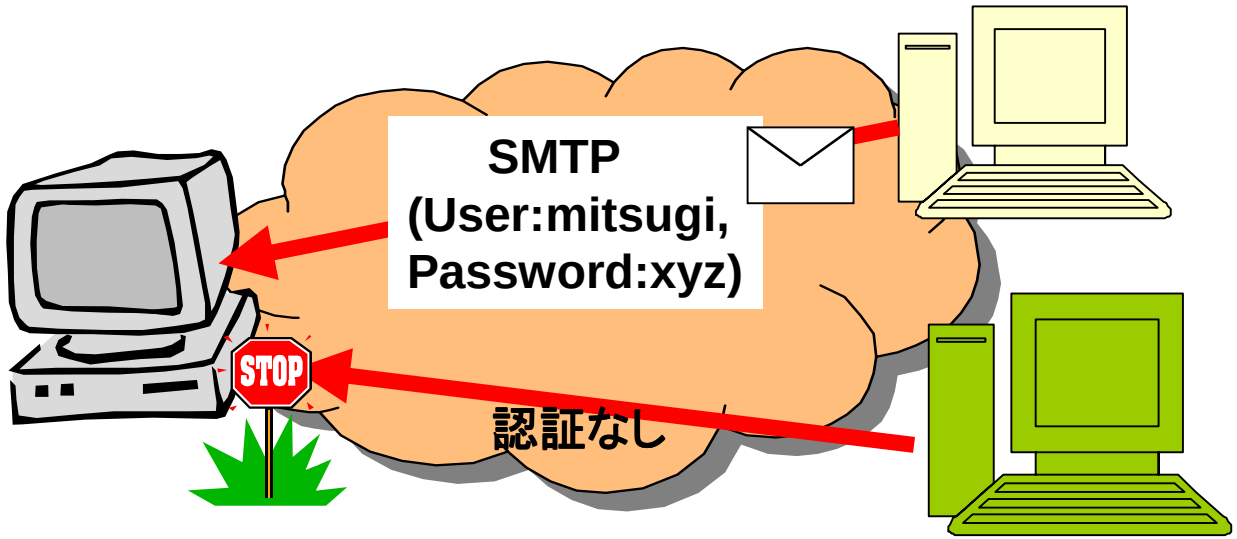
認証機能付のメール送信

- 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



ブラックリストの利用

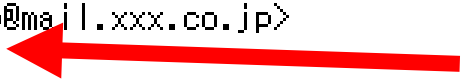
- sendmail.cf などで指定
  - ブラックリストに載っている
    ドメイン、
    アドレスブロック
    からの配送を
    拒否

- 無実のドメインやアドレスが載っていることも
- OpenRelay対策後に削除依頼を

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

サービス上気をつけること

- 立場の違いを理解する
  もし、未承諾なら「未承諾広告※」表記
- メールマガジンの登録方法
- 「登録をすると広告メールが送られる
  ことの周知
- 登録解除をしたい場合の手間

登録方法

メールアドレス登録の際には、第三者によるいたずらも考慮して

例

1. メールアドレス登録
2. 確認メールの送信
3. 確認メールの内容を利用して再度確認
4. 登録終了

広告メールが送られることの周知

- 目につくところへの表記
  - 能動的に、了解させる
  - 「同意する」「同意しない」の選択
- 送付する広告メールにも
  「何に登録したから
  このメールが送られているか」
  を明記

登録解除

- 登録情報を忘れた場合でも、
  簡単に登録を解除できる仕組みも検討
  - 登録アカウント忘れ
  - 登録メールアドレス忘れ

  例「解除は、このURLにアクセスして下さい」

  http://xxx.yyy.zzz/ほにゃらら…
- スパムと認識されるとアクセスしてもらえないことも

スパムを受ける側の対策
<参考>

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
  - メーラの設定で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
  - UNIXではspamassassinなど
    (http://www.spamassassin.org)

スパマ・アタッカに
ならないために
<アタック編>

アタッカにならないために

- 設計時に考えること
- 運用時に行なうこと
- ネットワークで行なうこと
- 計算機上で行なうこと

設計・運用で行なうこと

- セキュリティポリシを決める
- 侵入されにくい
  - ネットワーク構成
  - システム構成
- セキュリティ情報収集
- 運用時の相互確認
  (ミスを軽減するために)

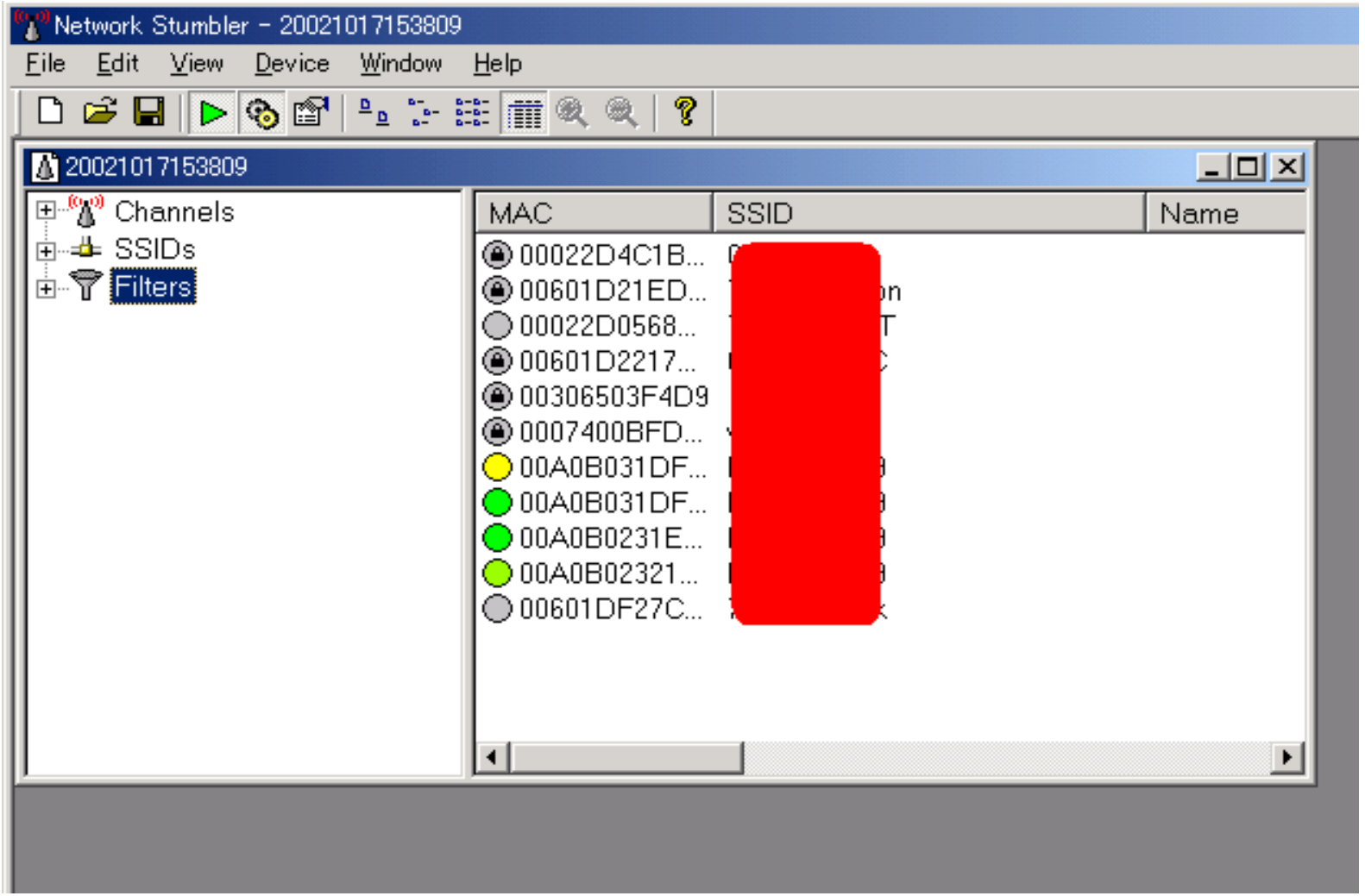
侵入されにくいネットワーク構成

- インターネットに向けてする提供する
  サービスと、組織内向けサービスの分離
- 重要なシステムを置くネットワークは
  内側かつ奥側へ
- 誰でも使えるネットワークは危険
  - オープンスペースに置いてあるハブ・
    スイッチ
  - 認証無しの無線LANも危険

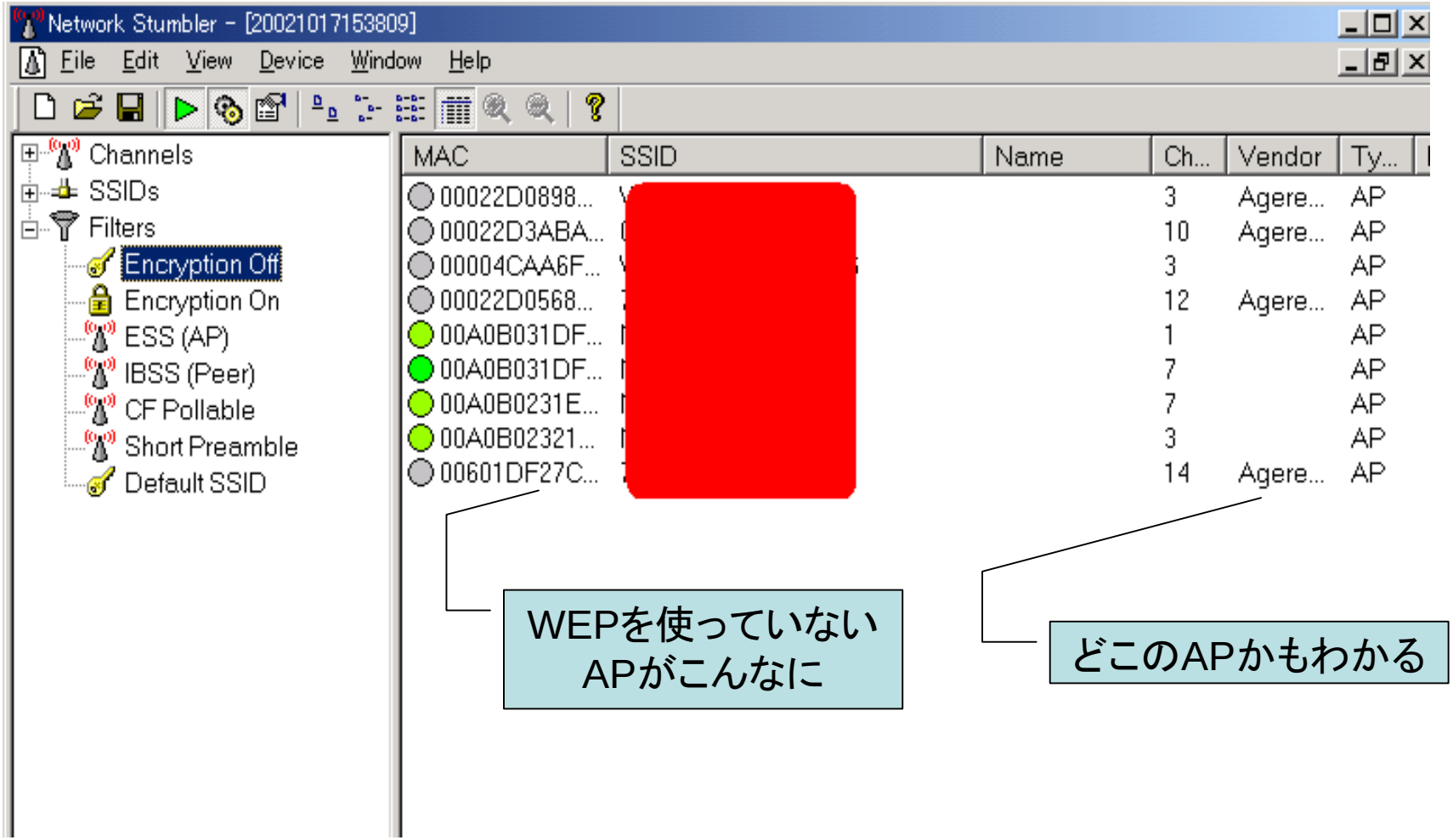
無線LANの悪用

- 認証機構を利用していないアクセスポイント
  - 繋がれ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…

無線LANの状況



WEPを利用していないAP



侵入されにくいシステム構成

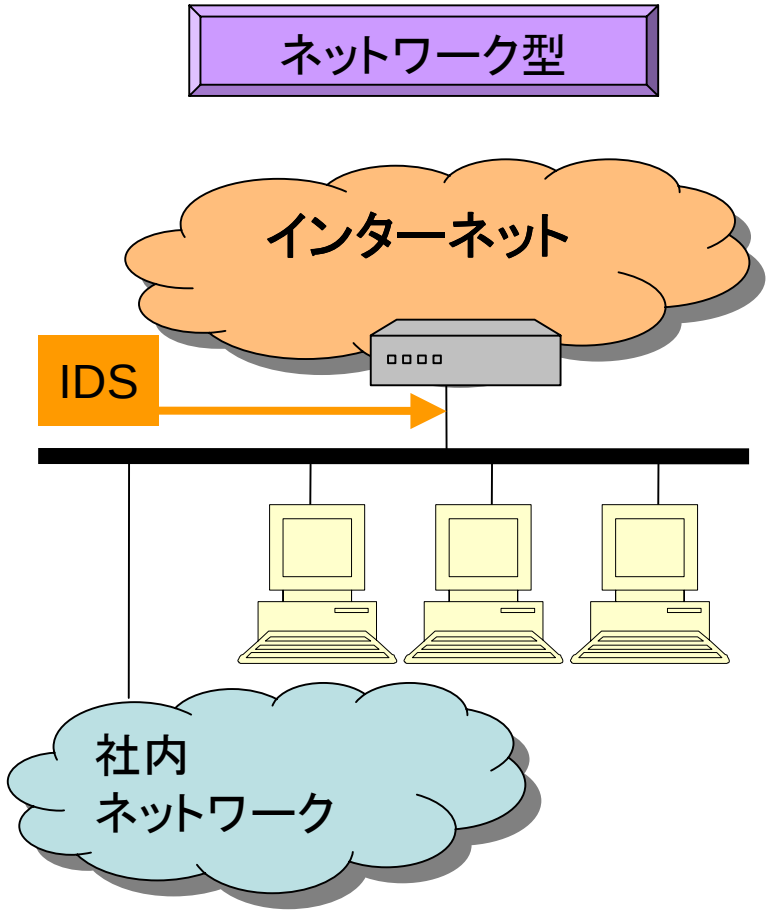
- 各ホストの役割を
  - 明確に
  - 構成を簡素化する
  - 守りやすい OS の選択
  - 守りやすいアプリケーションの選択

ネットワークで行なうこと

- Firewall
  - 外->内への不必要なアクセスを遮断
  - 内->外へもアクセスを制限
    - 踏台になった場合被害を軽減
- Firewall があっても
  - 許可したサービスで侵入
  - メール、Web閲覧でウィルス・ワーム感染
  - 大量のアクセスによるDoS攻撃

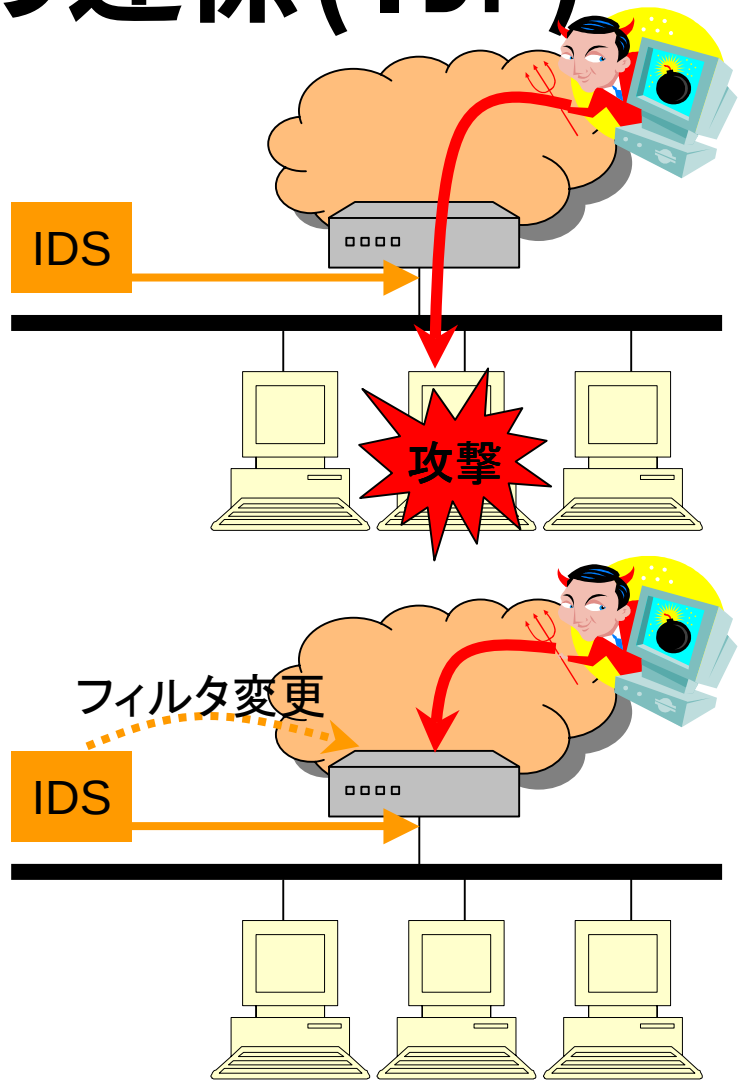
IDS・IDP

- 不正と思われるアクセスを検出、通知
- 攻撃パケットを破棄
- 攻撃セッションのリセット



IDSとFirewallの連係(IDP)

- 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



計算機で行なうこと

- パッチ(修正プログラム)の適用
- ウィルスチェック
- フィルタリング
- 特権ユーザが利用可能なコマンドを制限
- 設定確認
- ログの採取

フィルタリング

- 接続可能なサービス、接続元のIPアドレスを制限する
  - UNIX系、Linux サーバ機
    - TCPwrapper, xinetd
    - ipfw,sunscreen など
  - Windows クライアント
    - パーソナルファイアウォール
    - ウィルスチェッカと統合されたツールも

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

ログの採取

- ユーザの行動記録
  UNIX系OS(acct, C2auditなど)
- rootの行動記録(sudo)
- サービスへのアクセス記録(syslogなど)
- サービスの利用記録(syslogなど)
- カーネルの出すメッセージ
  (messagesなど)

ユーザの行動記録

- 何が行われたのかを知るために

  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

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
      - 該当時刻に誰が何をしたか確認
  - sudoを使わずにroot権限とを得た場合は記録されない

Windowsクライアントで行う
アクセス制御
<参考>

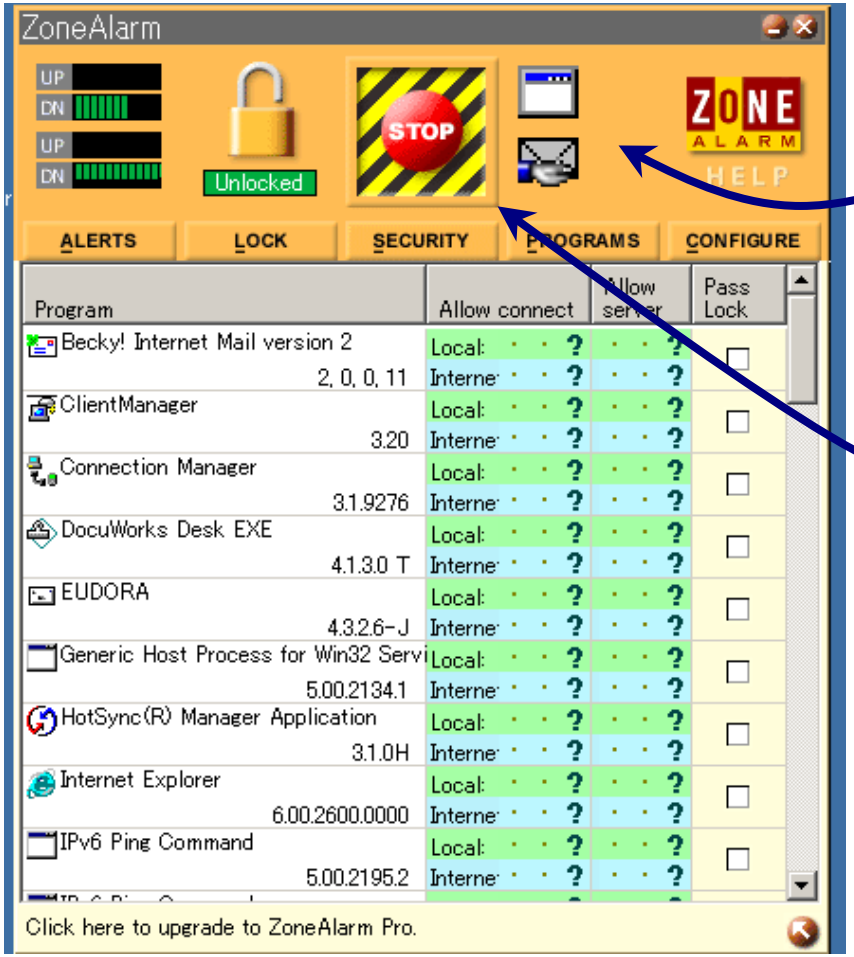
パーソナルファイアウォール

- 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

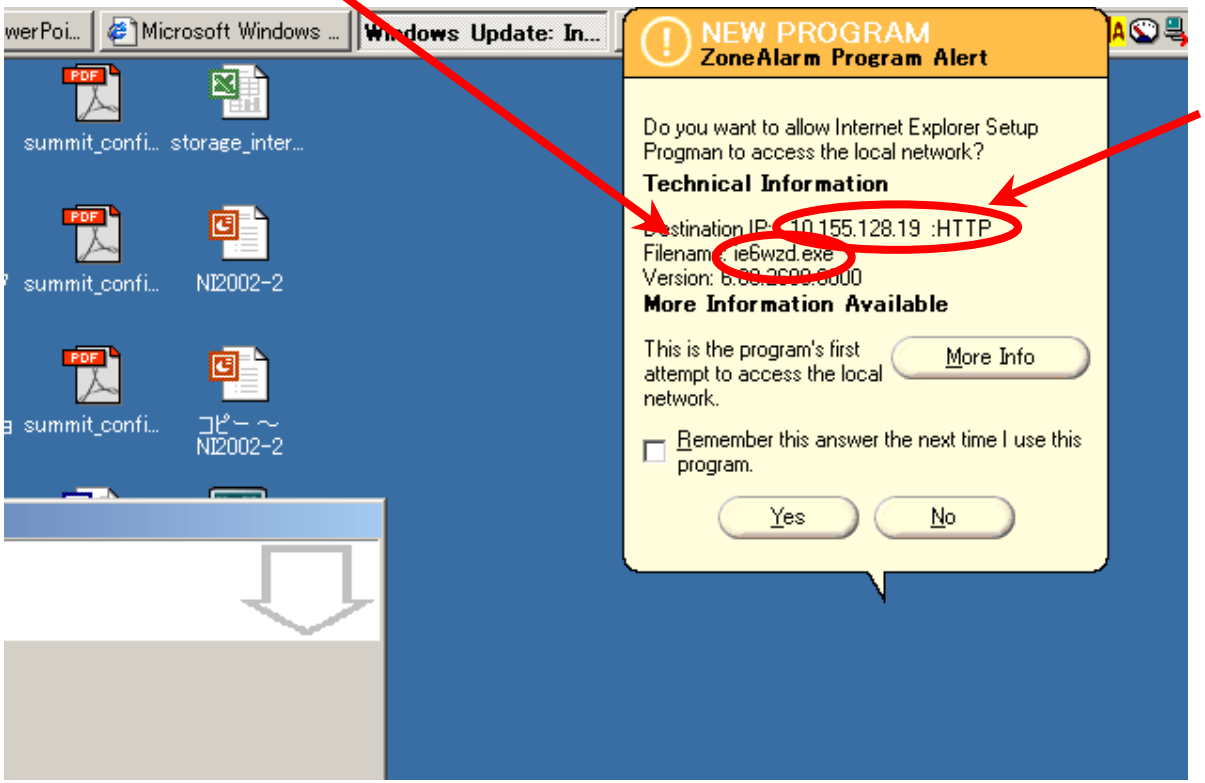


フィルタを通過している
アプリケーション

これを押すと、
通信ができなくなる

パーソナルファイアウォールの利用例

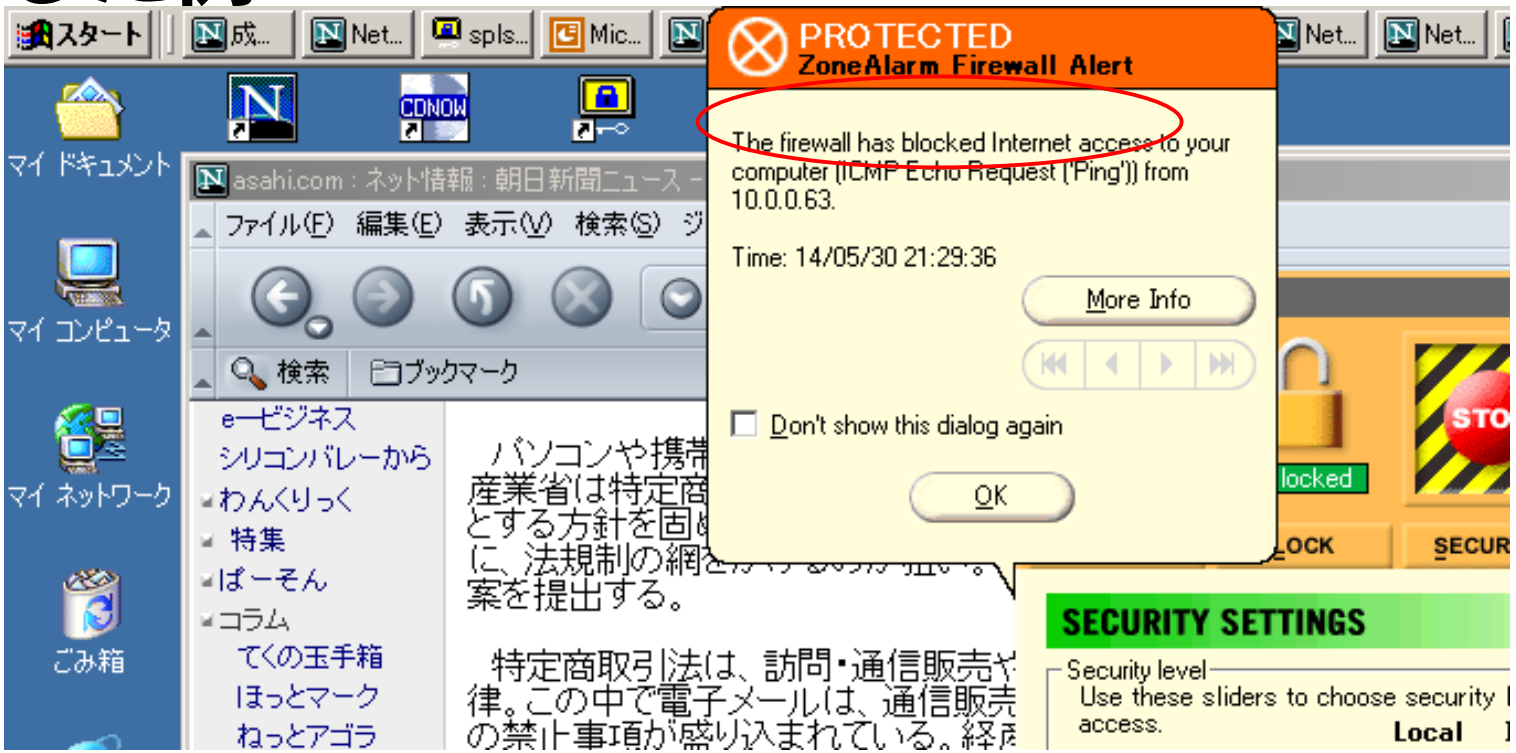
- 新しいアプリケーションを起動した例



10.155.128.19のHTTPポートへアクセス

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



問い合わせへの対応
<スパム編>

問い合わせメールを受け取ったら

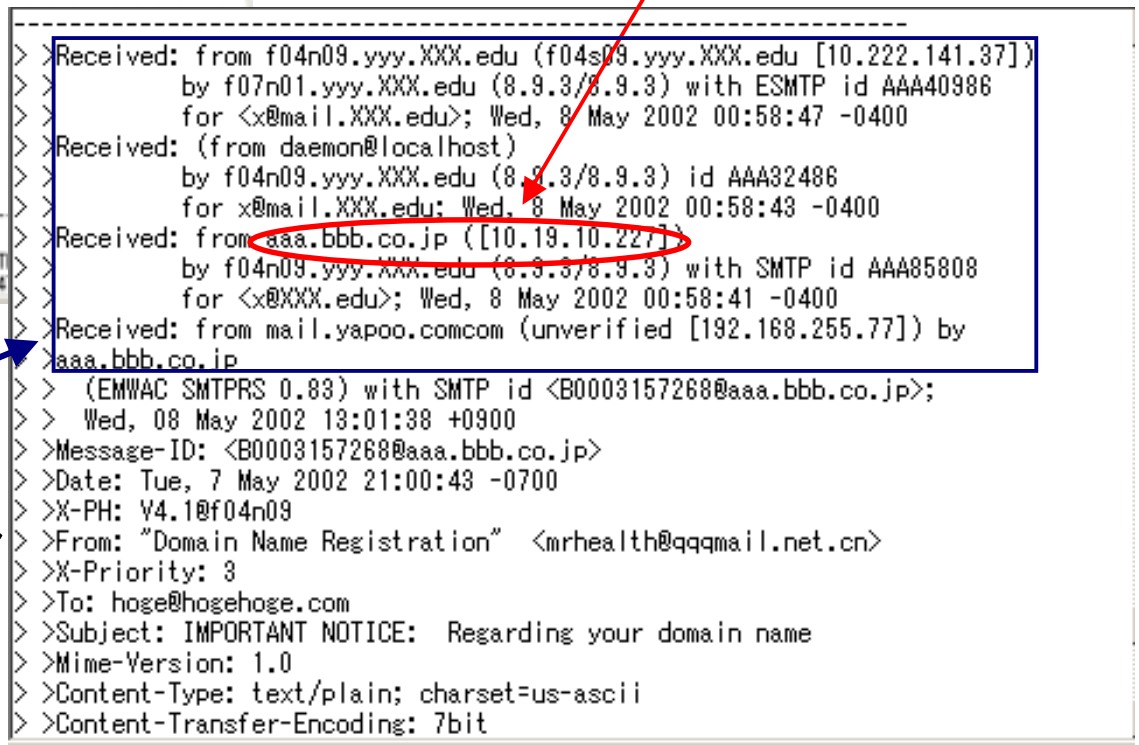
- 何を依頼されているかを確認する
  - 迷惑メールの停止
  - 迷惑メール発信者の特定と連絡
    ただし、発信者の詳細については
    プライバシーに関わることもあるので注意
- 調査すべき対象の確認
  - ヘッダや本文のIPアドレスやURLを確認

対応のポイント

- 問い合わせ元は、イライラしている
  - 調査開始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
  - 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。

対応の難しさ

- ヘッダの改ざん
- なりすまし
- ユーザ情報の取り扱い
- ユーザのそのまたユーザが対象の場合
- 嫌がらせのためのURL引用
- 問い合わせ元（被害者）を本当に信用できるのか?

迷惑メール関連法案はあるが

- 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…
- 友達を装ったメールも増加

確信犯に対しては、抜本対策は困難

問い合わせへの対応
<アタック編>

アタックされたら

- 対象の特定
- 現在の状況
  - アタックされ続けている
  - 破壊されている
- ログはあるか？ ⇨ ログの確認
- 関係者への連絡
- アタック元への調査依頼
- 復旧プラン

アタック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

- アタックされた時刻
- 自分の
  - アドレス、ポート番号
- アタックしてきた相手の
  - アドレス、ポート番号
- アクセスログを添付する

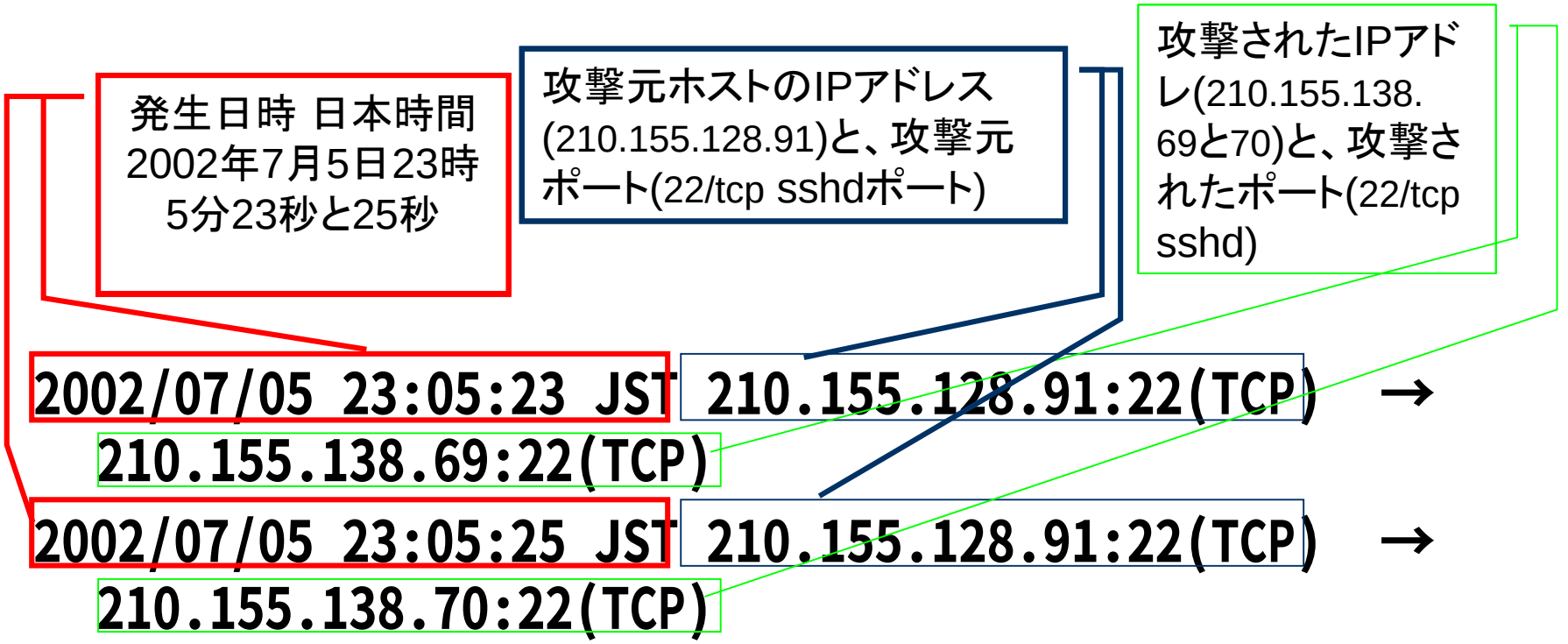
アタックしているという問い合わせがきたら

- 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

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
- 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を確認

対応の例



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?
    - 現在稼動しているか?
    - 顧客情報から担当者を特定
    - 接続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
  - 誰がやったのか?
  - 間違ったのか?
  - 踏み台か?

Acct

```
# lastcomm
csh              -F      mitsugi          ttypi      0.00 secs Thu May 30 18:48
csh              -F      mitsugi          ttypi      0.00 secs Thu May 30 18:48
hostname         -       mitsugi          ttypi      0.00 secs Thu May 30 18:48
mark             -       mitsugi          ttyp1      0.00 secs Thu May 30 18:47
mark             -       mitsugi          ttyp1      0.00 secs Thu May 30 18:47
inc              -       mitsugi          ttyp1      0.00 secs Thu May 30 18:47
from             -       mitsugi          ttypc      0.00 secs Thu May 30 18:47
lastcomm         -X      mitsugi          ttypc      0.11 secs Thu May 30 18:47
sendmail         -F      don              __         0.00 secs Thu May 30 18:47
sh               -S      don              __         0.00 secs Thu May 30 18:47
archive          -       don              __         0.02 secs Thu May 30 18:47
mail.local       -S      root             __         0.00 secs Thu May 30 18:47
sendmail         -SF     root             __         0.00 secs Thu May 30 18:47
sh               -S      don              __         0.00 secs Thu May 30 18:47
distribute       -       don              __         0.00 secs Thu May 30 18:47
sh               -       don              __         0.00 secs Thu May 30 18:47
sendmail         -S      don              __         0.00 secs Thu May 30 18:47
sendmail         -F      don              __         0.00 secs Thu May 30 18:47
sendmail         -SF     don              __         0.00 secs Thu May 30 18:46
sendmail         -F      don              __         0.00 secs Thu May 30 18:47
lastcomm         -X      mitsugi          ttypc      0.00 secs Thu May 30 18:46
more             -       mitsugi          ttypc      0.00 secs Thu May 30 18:46
```

mitsugi がログイン

mitsugiがメールを読んでいる

donがオーナのメーリングリストにメールが届き、アーカイブの処理がされた

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
```

さらなる調査と復旧

- 侵入経路や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

警察からの連絡

- 最初の問い合わせは電話でくることも
- 何の件か確認する
  - 攻撃した(不正アクセス禁止法関連)
  - 誹謗中傷
  - 児童ポルノ系
  - 詐欺
- 顧客情報等を聞かれる
- 「警察だから」と安易に電話で答えない
- 書面での問い合わせを要求する

書面での問い合わせ

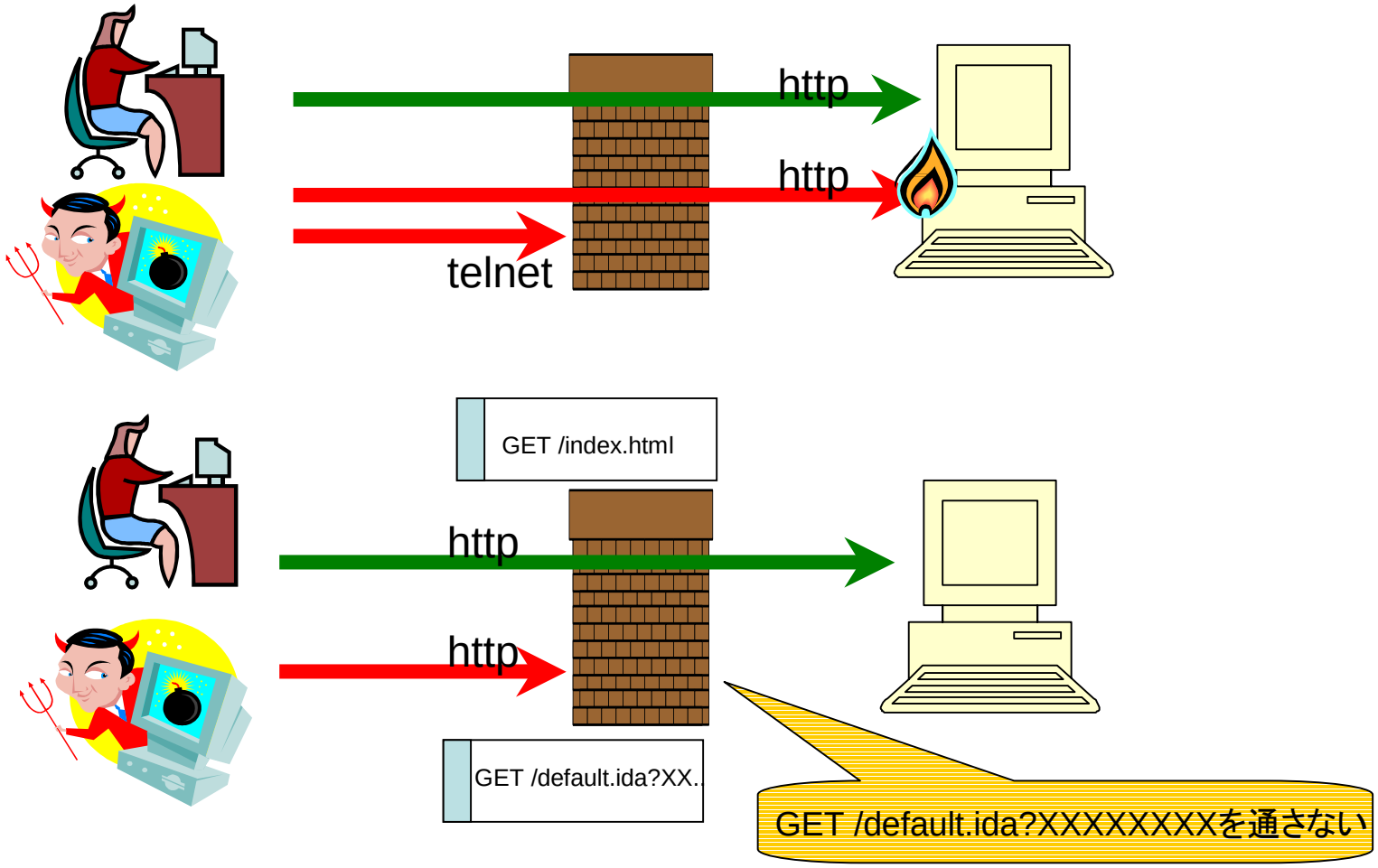
- 捜査関係事項照会書が届いたら
  - 照会内容に関して返答を
    - 契約者の名前、設置場所など
  - ただし、詳細については、弁護士と相談する
- 場合によっては "証拠" を保存、提出

いまできることの限界点

ISPの限界

- トラヒックの内容を区別してはいけない
  - 検閲の禁止(電気通信事業法 第三条)
  - 秘密の保護(同 第四条)
- フィルタをすることは良いことか？
- 問い合わせメール自体の正当性
- 状況証拠だけで罪に問えるのか？
- 確信犯とのいたちごっこ

ペイロードを解析する必要性



何もしないわけにはいかない

- ◆うっかり片棒を担がないように
  - – セキュリティ対策
    - ・セキュリティパッチ
    - ・アクセス制御、フィルタ
    - ・ロギング　　etc…
  - – スパムのためのOpenRelay対策
- ◆何かあった場合の状況説明

ご清聴ありがとうございました