今、企業のセキュリティ対策は、何を求められているのか

2007/11/28 “Email Security Conference” ベルサール神田

有限責任中間法人
JPCERT コーディネーションセンター
小宮山 功一朗

最初に

- 左上隅の青い三角は...
- JPCERT/CCとは...
  - インシデント報告してください。
  - 貴社内にCSIRTを作りませんか？
  - Cyber Clean Centar プロジェクトでがんばってます。
- 私は...

Agenda

- 内外に存在するリスク
  - 外部からの脅威
    - メールを使った、様々な攻撃手法の傾向
  - 内部の脅威
    - メールを介した企業の情報漏洩
- 対策
  - サーバサイド(MTA)の対策
  - クライアントサイド(MUA)の対策

無料かつ、導入が容易なものだけ。

メールはインフラ

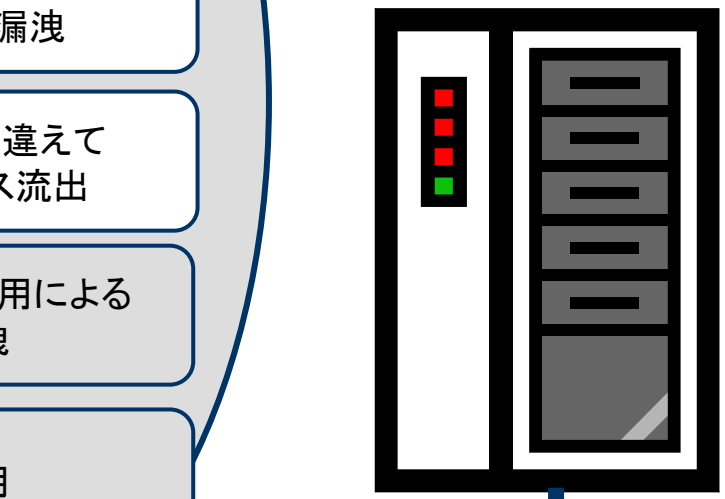
- ハイレベルな可用性、拡張性が要求される
  - ユーザの増加、ストレージ容量の増加、バージョンアップ、パッチ対応
  - 可用性を保つための運用・検証
- メールの保存(ストレージ)
  - 増え続けるメールをいかに保存するか?
- メンテナンス
  - JVN#19445002: APOP におけるパスワード漏えいの脆弱性
    http://jvn.jp/jp/JVN%2319445002/index.html

組織内に存在するリスク

- アドレスの入力ミス による誤送信
- 間違った添付ファイルを 送付し情報漏洩
- BCCとCCを間違えて メールアドレス流出
- Webメールの使用による 情報漏洩
- 私的利用

外部の脅威

- スパム
- フィッシング
- ウイルスメール
- ゼロデイ攻撃
- 標的型攻撃



メールはインフラ
メールシステムは動き続けて当たり前
ユーザの増加、ストレージ容量の増加、バージョンアップ、パッチ対応

外部の脅威

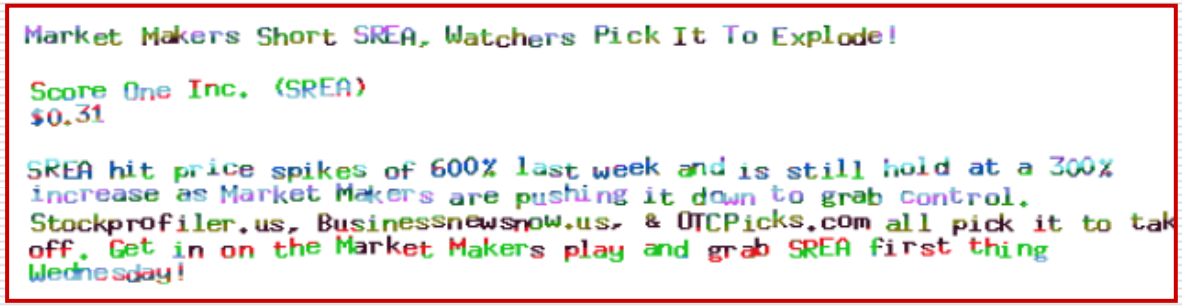
1. スパム
2. 株価操作スパム
3. フィッシング
4. 標的型攻撃
   - スピアフィッシング
   - Targeted Trojan Attack
5. ウイルスメール(ウイルスが添付されたメール)

外部の脅威① スパム

- Botによるスパム送信

  Cyber Clean Center サイバークリーンセンター

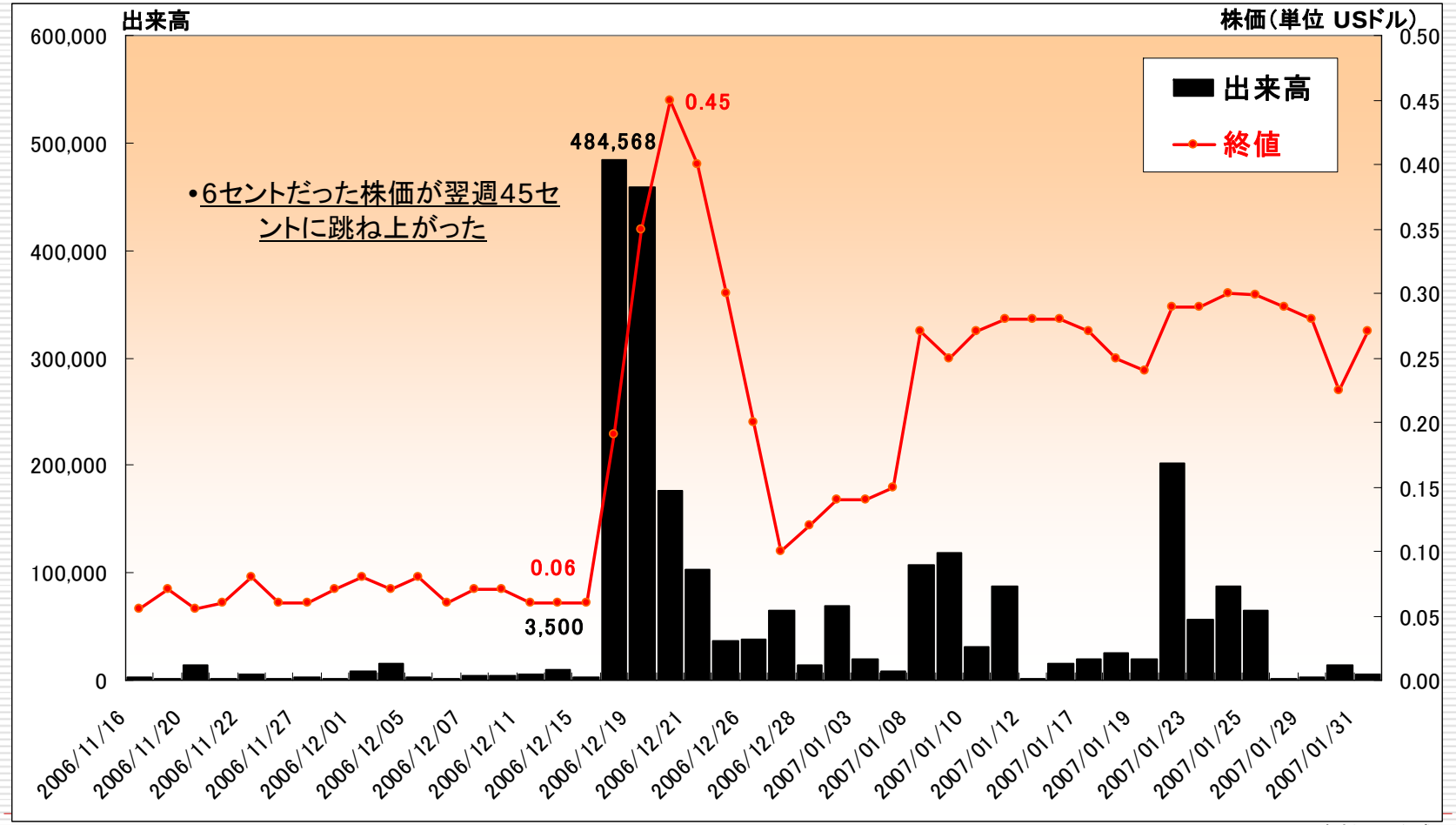
  - www.ccc.go.jp
- 様々な形式のファイルが届きます
  - 画像(jpg, gif, png)
  - PDF
  - MS Office文書 (xls)
  - MP3
- 共通するのは:文字認識技術による検知を回避するための工夫



外部の脅威② 株価操作スパム

- Pump and Dumpなどと呼ばれる
- 特定銘柄の株式を購入することを推奨するメールなどを送り株価を不正につりあげた上で、自分が所有していた株式を売り抜ける行為
- 2007年3月、米国証券取引委員会(SEC)により特定銘柄の取引が停止させられるという処置もとられた
- 特徴
  - 狙われるのは米国のピンクシート銘柄とよばれる小規模の株式
  - 株価操作から売り抜けまでは長くて1ヵ月

外部の脅威② 株価操作スパム 続き



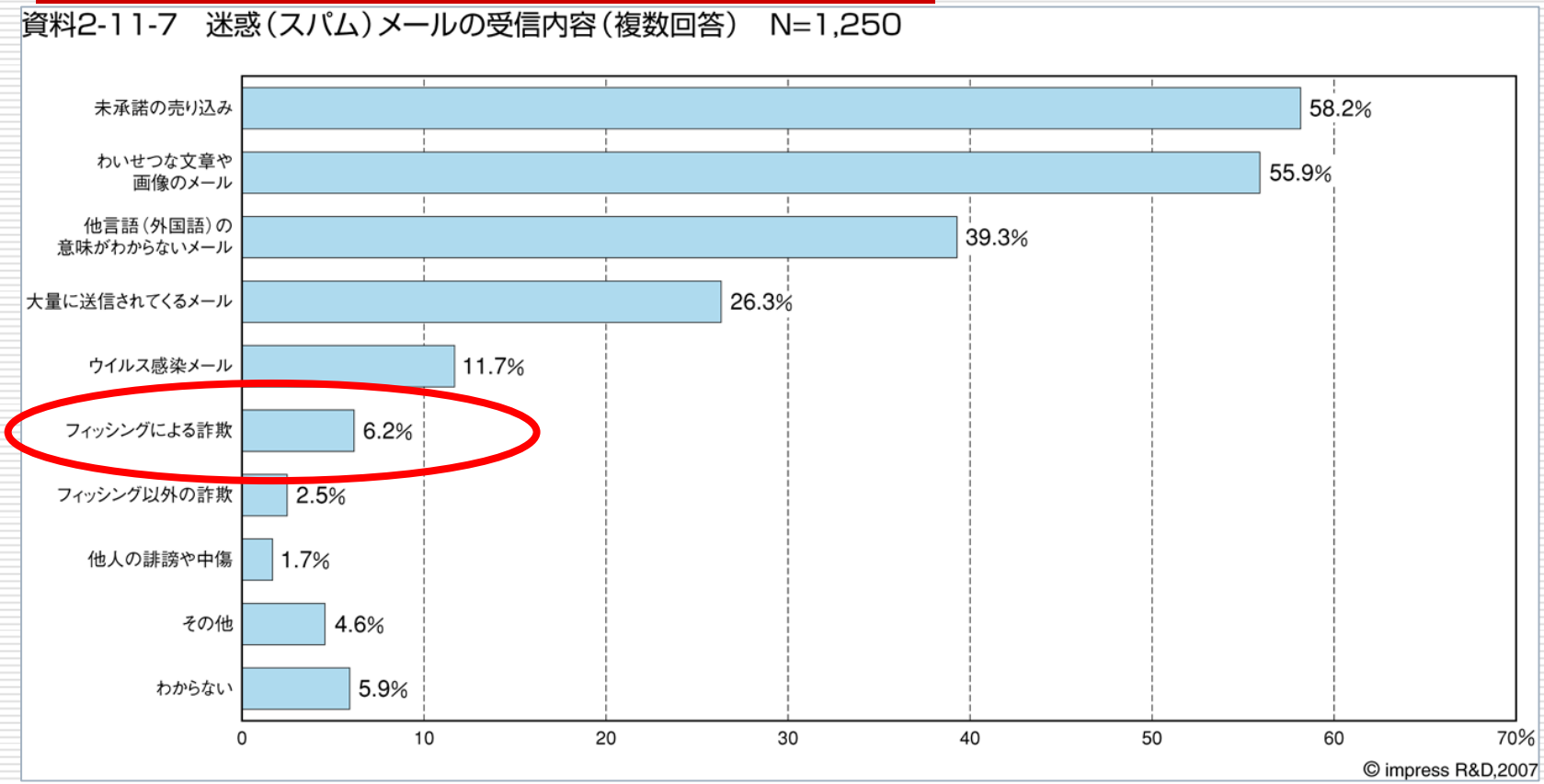
SEC公開資料より作成

外部の脅威③ フィッシング

- 国内企業を狙うフィッシング詐欺
  - 銀行、消費者金融が中心
- フィッシングサイトを用いて認証情報を盗むという事例は、2006年の1件から220件に増加

(経済産業省『不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況について』)

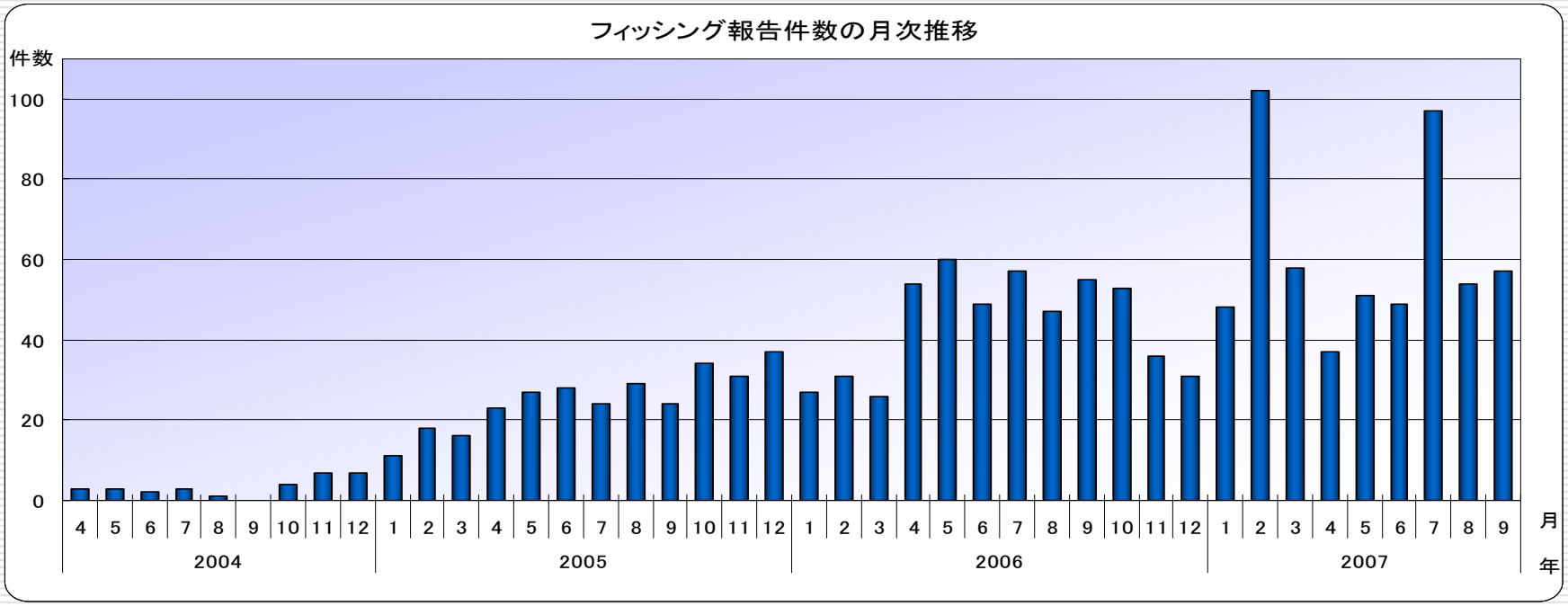
外部の脅威③ フィッシングメールは増えているか?



- スパム全体の6.2%強 『インターネット白書2007』より

外部の脅威③ フィッシング 報告

- JPCERT/CCに寄せられるフィッシング報告のほとんどが、国内のサーバが侵入されフィッシングサイトとして使用されているケース
- 増加傾向に鈍りが見えたか?



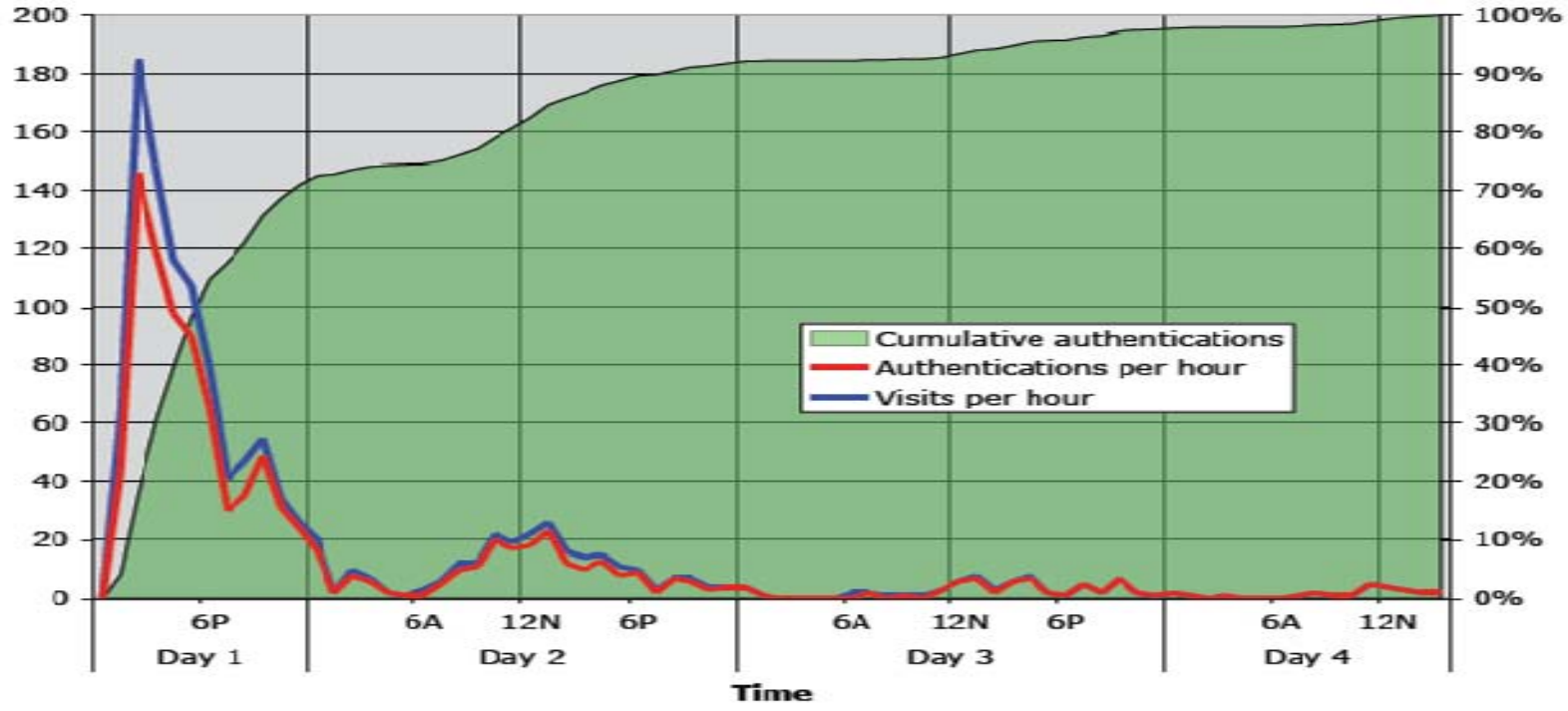
JPCERT/CCへのフィッシング報告 : 2004/4 ~ 2007/9

外部の脅威③ フィッシング対応の難しさ

- フィッシング対応の難しさ
  - 減らない、放置されているテストサーバ
  - 何度も蘇るフィッシングサイト
  - ISPの対応にばらつき
  - 各国にフィッシングサイト
    - 国境を跨るコーディネーションのややこしさ

外部の脅威③ フィッシング対応の難しさ 続き

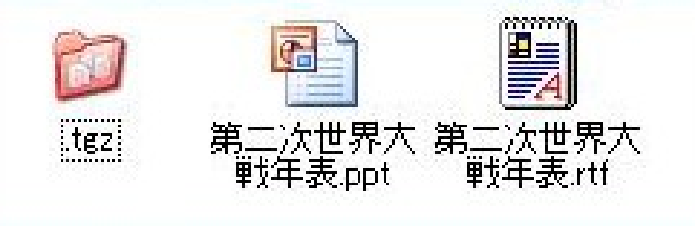
- 被害の70%は最初の12時間で起こっている



出典: **Social Phising, Indiana University (Dec 12, 2005)**
http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf

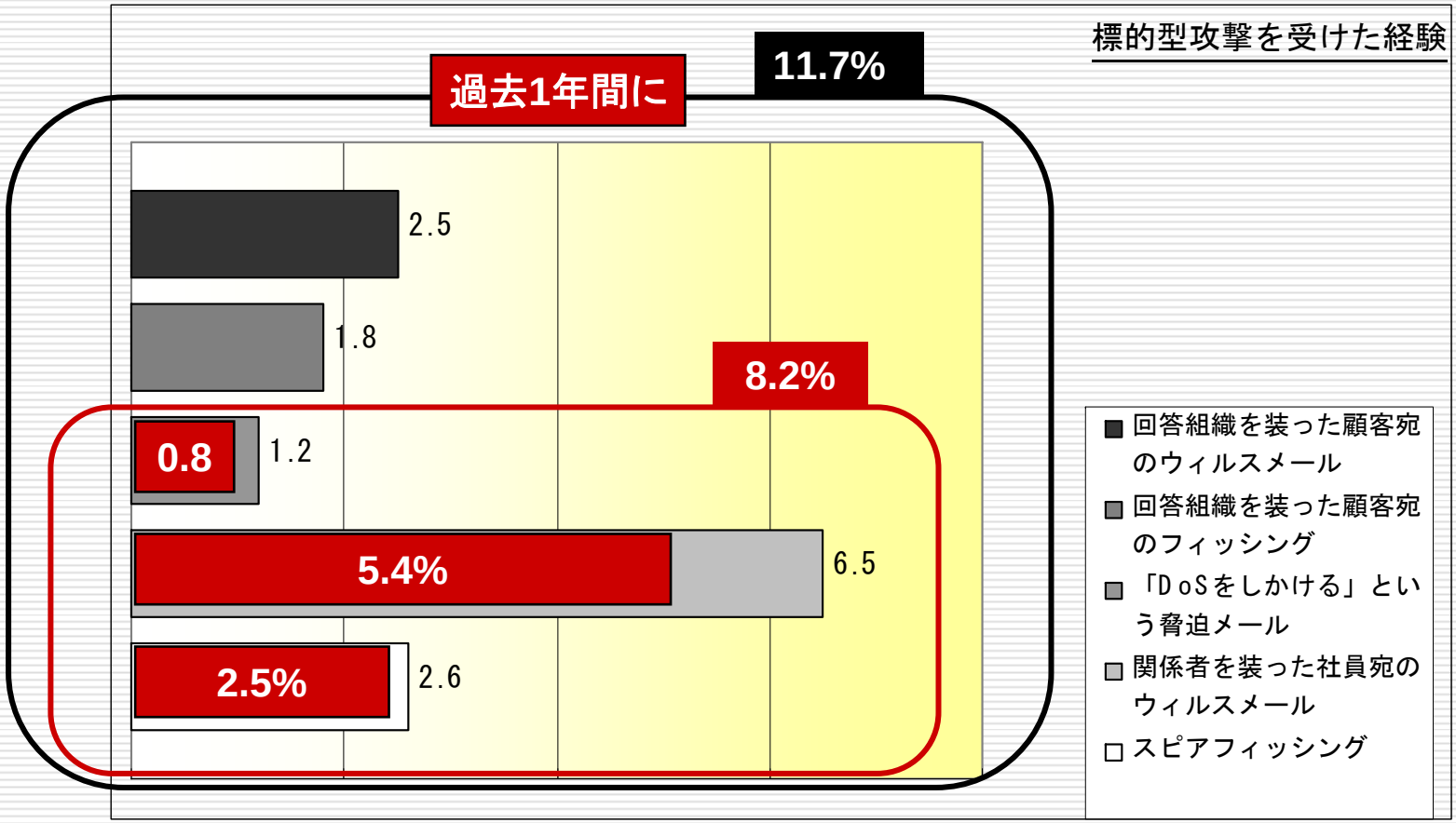
外部の脅威④ 標的型攻撃

- 標的型攻撃とは?
- スピアフィッシングとは?
- ケーススタディ: Lhazへのゼロデイ攻撃
  - 時期:2007/8/17
  - メール受信: 日本の一部組織
  - 添付ファイル: lhazをインストールしていると開いた瞬間にマルウェアがインストールされる



画像出典: Malware Blog - by Trend Micro
http://blog.trendmicro.com/yet-another-japanese-zero-day-trojan-discovered/

外部の脅威④ 標的型攻撃



JPCERT/CC『標的型攻撃についての調査』
http://www.jpcert.or.jp/research/2007/targeted_attack.pdf

外部の脅威⑤ ウイルスメール

- 昔ながらの手口
  - 送信者が・・・
    - 大統領候補、福田首相
  - セキュリティプログラムを装う

内なる脅威

- 「つい、うっかり・・・」
  1. 大量のTo、Ccでメールアドレス漏洩
  2. 添付ファイルを間違える
  3. 誤った宛先へ送信
- 社内ポリシーが問われる
  - メールの私的利用
    - 関連:個人契約のメールサービスを業務に使用しない
      http://www.jpcert.or.jp/wr/2006/wr063401.html
  - 無料のWebメール使用

内なる脅威① 大量の同報送信

- ToやCcに複数のアドレスを入力して送信
  - 本来であればBccを使うべき

内なる脅威② 添付ファイルを間違える

- 送る必要のないファイルを送ってしまう

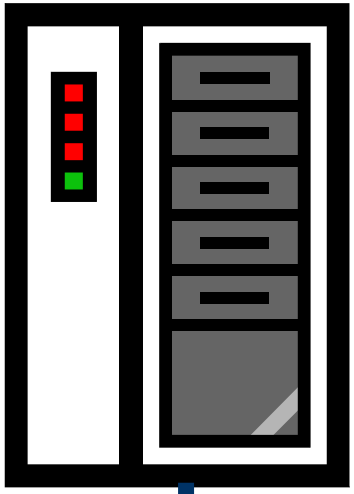
内なる脅威③ アドレスの入力ミス

- 社内に送るはずのメールを、取引先に・・・

組織内に存在するリスク

- アドレスの入力ミス による誤送信
- 間違った添付ファイルを 送付し情報漏洩
- BCCとCCを間違えて メールアドレス流出
- Webメールの使用による 情報漏洩
- 私的利用

メールサーバ管理者にしか 出来ない対策がある・・・



外からの攻撃

- スパム
- フィッシング
- ウイルスメール
- ゼロデイ攻撃
- 標的型攻撃

メールはインフラ
メールシステムは動き続けて当たり前。
ユーザの増加、ストレージ容量の増加、バージョンアップ、パッチ対応

再掲

対策

海外での対策

- アメリカ
  - SPF
    - Fortune Top 500企業でのSPF導入率
  - DKIM
    - Yahoo, Gmailなどが採用
- 韓国
  - KISA-RBL
    - http://www.kisarbl.or.kr
  - Sinkhole (Bot対策)
    - http://www.cert.org/archive/pdf/BotSinkhole_KrCERTCC.pdf

サーバサイド(MTA)の対策

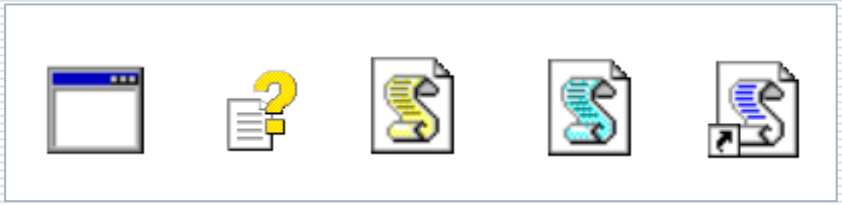
- 無料で効果が高そうなもの
  - 同時送信数の制限
  - 添付ファイルのフィルタ
  - 送信ドメイン認証 SPF
- 「コンピュータにできることはコンピュータに!」

同時送信数の制限

- MTAに以下の設定を行う
  - Sendmail
    - *define(confMAX_RCPTS_PER_MESSAGE', `<設定値>')*
  - Postfix
    - *smtpd_recipient_limit = <設定値>*
    - デフォルト 1000
  - Exchange Server 2007
    - *MaxRecipientPerMessage* を変更する
    - デフォルト 200
- Max値を越えるとエラー”452 Too many recipients”

添付ファイルの制限

- その添付ファイル、本当に必要ですか?
- 過去に悪用されたことのある拡張子
  - 止めても良いのでは?
    - exe chm scr wmf vbs wsh hta com mp3 js
  - 悪用されるけど、フィルタは難しい
    - doc ppt pdf xls zip lzh



送信ドメイン認証 SPF

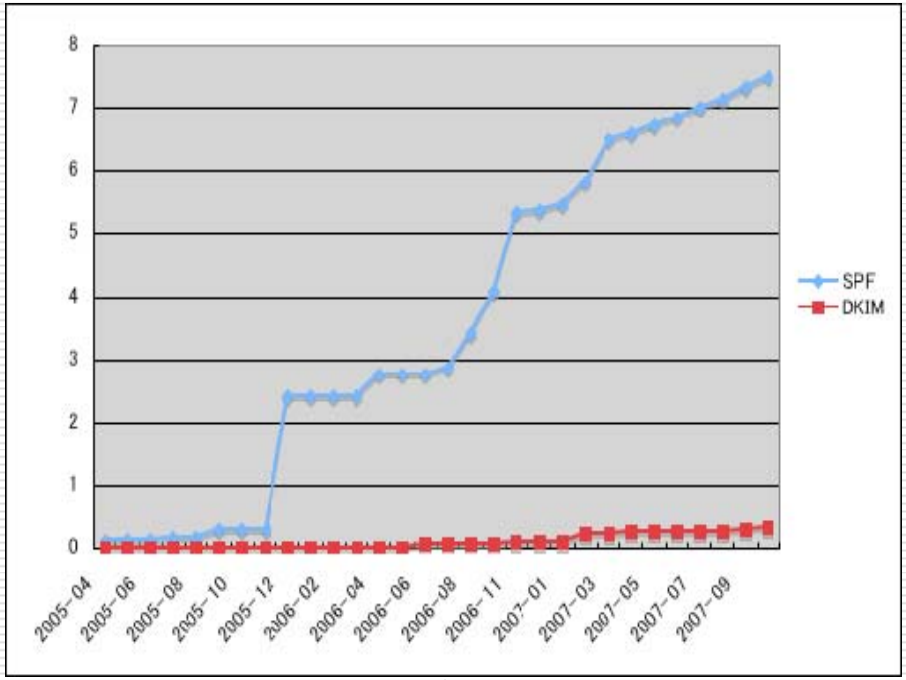
- なりすましを見破ることが可能
  - スパム対策・フィッシング対策に

```
-bash-2.05b$ dig TXT jpcert.or.jp
; <<>> DiG 8.3 <<>> TXT jpcert.or.jp
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51445
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;     jpcert.or.jp, type = TXT, class = IN
;; ANSWER SECTION:
jpcert.or.jp.  1H IN TXT  "v=spf1 ip4:210.148.223.5
ip4:210.148.223.6 ~all"
```

jpcert.or.jpでのSPFレコード設定例

送信ドメイン認証 SPF

- 普及状況
  - .jpドメインの7.47%が対応済み
    (2007/10 現在)
    - ドメイン認証の普及率に対する測定結果
      http://member.wide.ad.jp/wg/antispam/stats/index.html.ja
- 設定を確認したい?
  - http://www.seoconsultants.com/tools/spf/



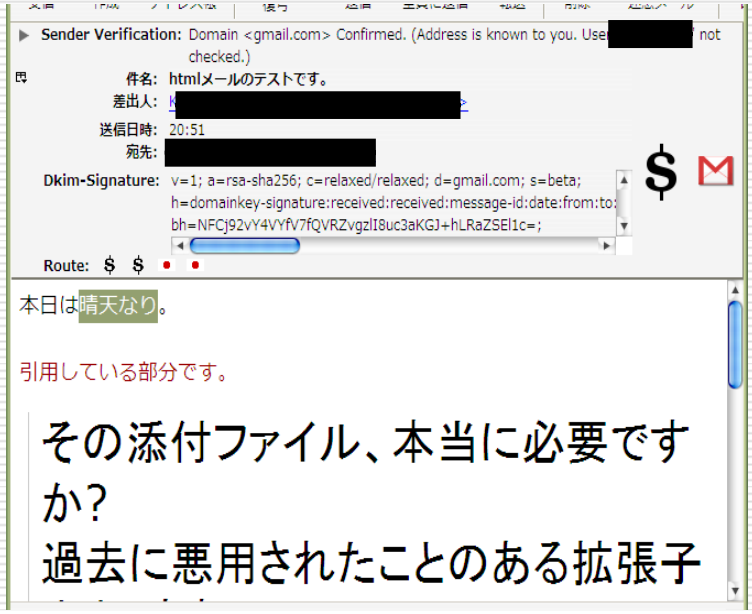
WIDEプロジェクト ドメイン認証の普及率に対する測定結果

クライアントサイド(MUA)の対策

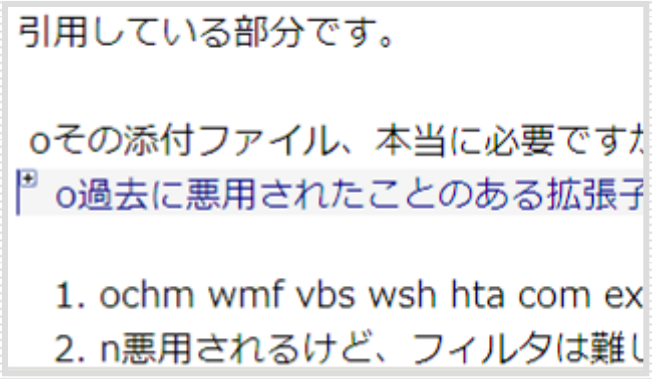
- Mozilla Thunderbirdとアドオンを使ってメール環境をセキュアにするTips
  1. HTMLメールを表示しない
  2. SPFレコードをチェックする
  3. このメールはどこの国から?

HTMLメールを表示しない

- デフォルトでテキスト表示。必要に応じてHTML表示に切り替え
  - Allow HTML temp
    https://addons.mozilla.org/ja/thunderbird/addon/1556

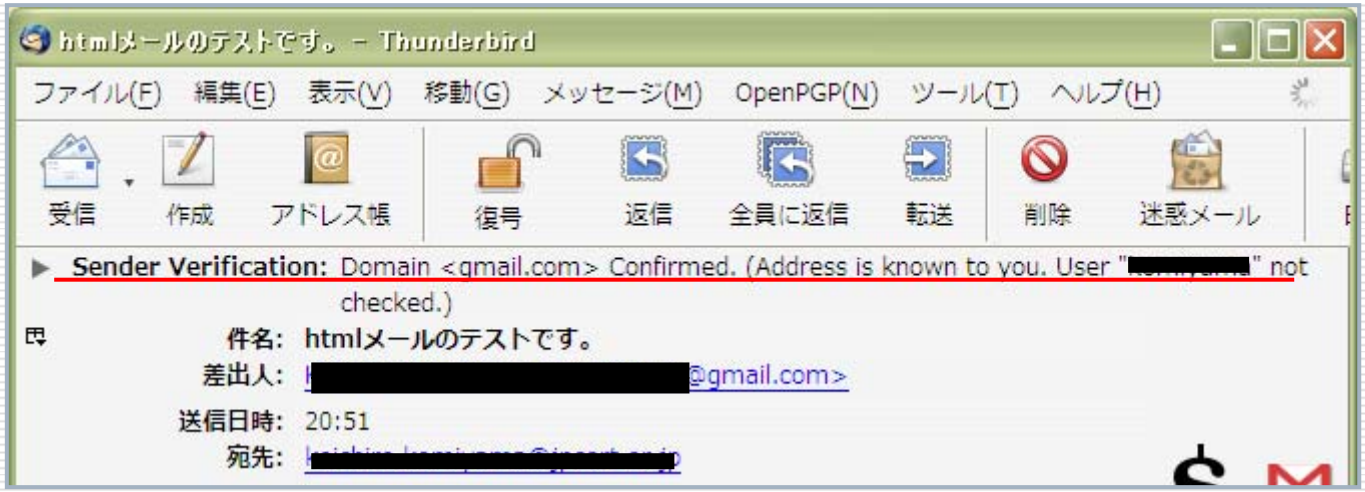


ワンクリックで切り替え



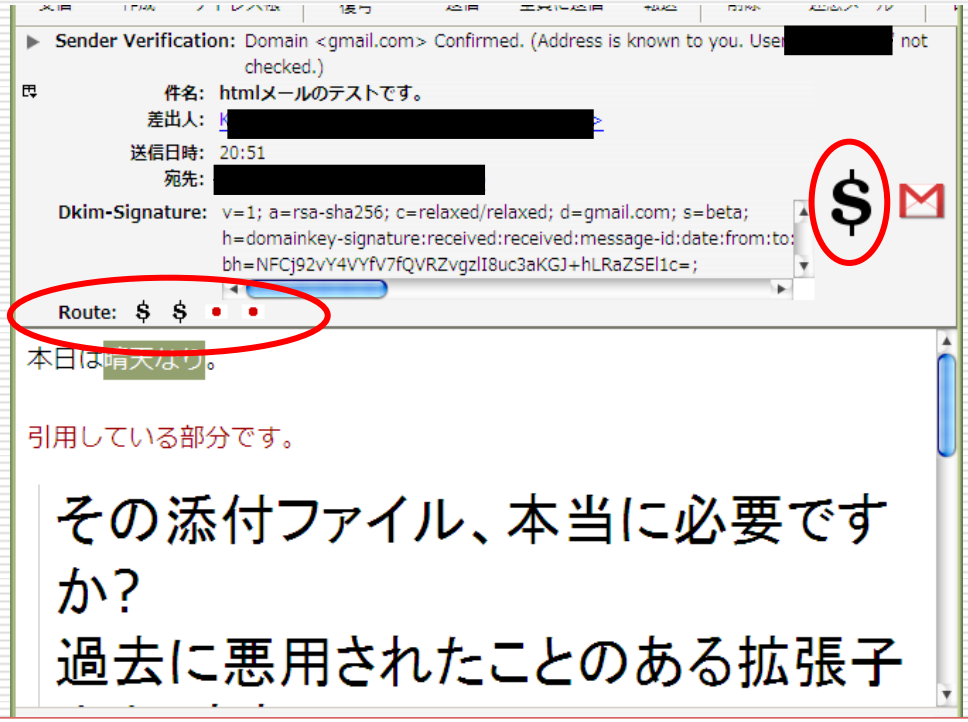
SPFレコードをチェックする

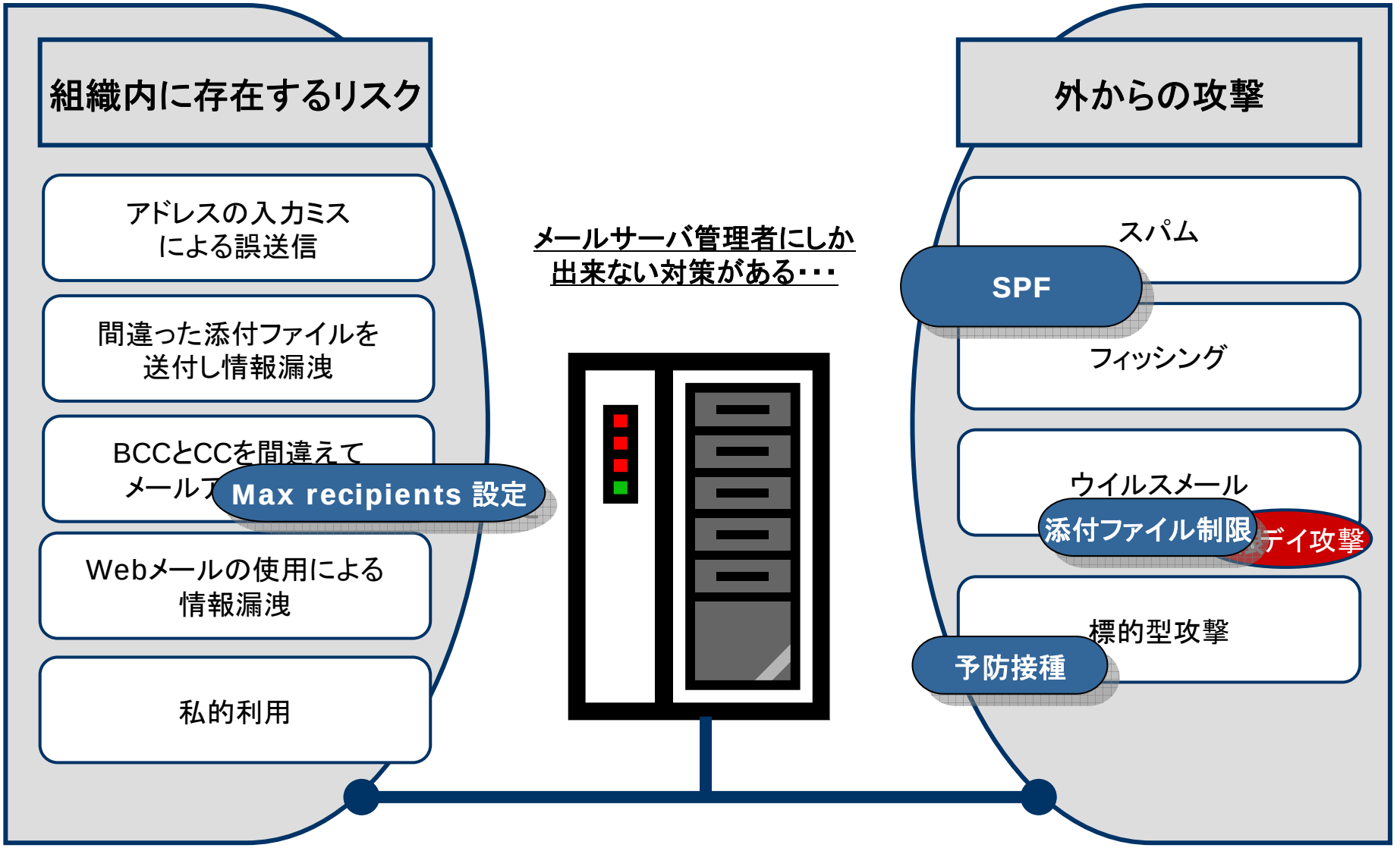
- メールのヘッダーとドメインのSPFレコードを照合する
  - Sender Verification Extension
    https://addons.mozilla.org/ja/thunderbird/addon/345



このメールはどこの国から?

- メールが経由した国を表示する。経由したSMTPサーバのIPアドレスで判断
  - Display mail route
    https://addons.mozilla.org/ja/thunderbird/addon/1244





メールはインフラ
メールシステムは動き続けて当たり前
ユーザの増加、ストレージ容量の増加、バージョンアップ、パッチ対応

再掲

協力のお願い

- 標的型攻撃への訓練＝予防接種
  - 社員や職員を対象に疑似攻撃
    - New York State Office (アメリカ)
    - IRS (アメリカ)
    - TWNCERT (台湾)

お問い合わせ先

- JPCERTコーディネーションセンター
  - Email：office@jpcert.or.jp
  - Tel：03-3518-4600
  - http://www.jpcert.or.jp/

- インシデント報告
  - Email：info@jpcert.or.jp

    PGP Fingerprint ：BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8
  - 報告様式

    http://www.jpcert.or.jp/form/