その情報って本物?
あるいは、なぜ未だにこうなのか

小島　肇
kjm@rins.ryukoku.ac.jp

たとえばベンダーのセキュリティ情報

- 例:
  http://www.microsoft.com/japan/technet/security/
- これって改ざんされてたりするんじゃないだろうか?
- これって偽サイトだったりするんじゃないんだろうか?

たとえば FreeBSD をインストール

- ftp://ftp.jp.freebsd.org/pub/FreeBSD/ から .iso を get
- CD-R に焼き焼き
- そいつで boot
- インストール

ところでその .iso、ほんものですか?

確認方法

- 偽サイトかどうか – SSL
- 改ざんされていないかどうか – 電子署名
- SSL は必要?
  - SSL は通信路上の改ざんが行われていないことも保証する → 本物が偽物にされる危険性の排除
  - センシティブ情報 (パスワード等) のやりとりなどがある場合

ダメな例

- MD5 digital signature 置きました
  - その MD5 値が改ざんされていないという保証はどこにもない。
- SSL つけました
  - 本物サイトである、ことしか保証しない。そのサイトに格納された文書が改ざんされていないことを保証しているわけではない。
  - CSS 穴があった日には (後略)

ダメな例 (つづき)

- PGP/GPG で署名しました
  - PGP/GPG 鍵の保証をどうするか、がやっかい。
  - PKI だって「ほんとにちゃんとやってんのか XXXXXXXX !」とかいう話があるけど…
- インターネットは使ってません
  - 利用している別のネットワーク上 (例: 郵便) で改ざんされていないという保証はない。特に、国家権力がらみの場合は…

事例 - Microsoft

- web page SSL – good
- 電子署名 – no good
  - web ドキュメントには署名なし
  - 昔、U.S. のメール版セキュリティ情報は PGP 署名してあったりしましたが、…
    - 署名が壊れてたりもした (^^;;)
  - Patch やプログラムファイルについては署名がある

事例 – Red Hat

- web page SSL – good
- 電子署名 – no good
  - web ドキュメントには署名なし
  - rpm については GPG 署名がある
    gpg –import /usr/share/rhn/RHNS-CA-CERT
    rpm –checksig package.rpm
  - この GPG 署名の正しさはどうやって確認する?

事例 – JPCERT/CC

- 電子署名 – (half?) good
  - 注意喚起、JPCERT/CC レポート等、主要なものには PGP 署名あり。全てではない。
  - 署名の確認方法: JPCERT/CC 関係者から名刺をかっぱらい、名刺に刷られた Fingerprint を見る
- web page SSL – no good
  - 設置予定なし (T_T)。センシティブ情報のやりとりは、今のところはないようだが…

事例 - FreeBSD

- web page SSL – no good
- **電子署名** – no good
- **似たような感じのところは多い…**
  - *BSD, Vine, Turbo, …
  - **事例: トロイの木馬版** OpenSSH **配布事件**
    http://www.openssh.com/txt/trojan.adv
- **そこらじゅうに存在するブツを集めまくった上で比較し、「どうやら本物っぽい」と言うことはできるかも**

問題点いろいろ

- SSL を入れていないところは多い
- なぜ普及しない?
  - 重い
  - 高い
  - ウザい
  - 個人じゃ取れない

個人向けの証明書サービスを!

- 個人で (いくつも) ドメインを持つ時代にサービス内容が適合していない
- 「そのサイトが確かにそのドメインのものである」ことを保証してくれれば、多くの人にとってはそれでいいのでは?
  - 住所だの何だのがどうだというのか
  - あまりにも EC 方面に向きすぎ
- ドメイン屋さんがやってくれないかなあ…

問題点いろいろ (つづき)

- Akamai などを使ってると、「セキュリティ証明書の名前が無効であるか、またはサイト名と一致しません」と言われる
  例: HP, Symantec, NAI, 読売
- SSL を入れていても、ブラウザで鍵アイコンが出ないところが結構ある
  例: IBM, Sony, Oracle, ISSKK

問題点いろいろ (つづき)

- 電子署名されたコンテンツはほとんどない
  - 普及してない?
  - いや、俺も署名してないが (^^;)
    しょせん 2 次情報サイトだし…
- 動的な web page はどうするのがいいんだろう
  - web サービスの時代 (XML 署名) を待つ?
  - それまでは、サイトをまるごと信用する・しないしかない?

個人的 to do

- SSL 導入
  - 手続きはやっぱりウザそう…
- 署名方面
  - ちょっと考え中…
  - PKI 大規模導入、なんてのは絶対ムリ

Appendix

- SSL なページがあるかどうか、ちょっと調べてみた結果を
  http://www.st.ryukoku.ac.jp/~kjm/security/memo/ssl-enable-sites.txt
  に置いておきます。
- 署名してません (^^;)