EV SSLとは？

有限責任中間法人 日本電子認証協議会(JCAF)

http://www.jcaf.or.jp/

SSLの基礎知識

- Secure Socket Layerの略でNetscape Communication社が1994年に発表
- インターネット上で最も広く使われている暗号化・認証のためのプロトコル
- ブラウザでは「https://～」と 鍵マーク
- X.509準拠のデジタル証明書を使用
- 近年ではWeb以外にも利用範囲を拡大
  (XXX over SSL、SSL-VPN等)

参考：XXX over SSL

- Web以外へと用途の広がるSSL

サービス名	ポート番号	詳細
https	443	HTTP over SSL
nntps	563	NNTP over SSL
ldaps	636	LDAP over SSL
ftps	989/990	FTP over SSL
telnets	992	TELNET over SSL
imaps	993	IMAP4 over SSL
pop3s	995	POP3 over SSL

SSLの2つの（本来の）機能

- 暗号化
  - 第三者によって盗聴、改ざんされていないか？
- 身元確認
  - 通信をしているのが正しい相手か？
  - ではもし、予め正しい相手だとわかっていたら？
    （⇒例：社内メールサーバへの接続）

SSL証明書の種類（1）

- 組織認証（本来のSSL）
  - サイト運営者の実在性を確認して発行される
- ドメイン認証
  - ドメインの所有者を確認して発行される
- 自己署名
  - 組織内で独自に認証局を立てて発行される

SSL証明書の種類（2）

認証区分	第三者認証	実在認証	使用範囲
組織認証	Y	Y	不特定多数
ドメイン認証	Y	N	組織内
自己署名	N	N	組織内（鍵配送）

※認証区分と暗号強度は無関係！

SSLの抱える課題

- 利用範囲の拡大とともに、発行基準が多様化する一方で、一般のエンドユーザにはその区別が困難な状況にある

↓

- 鍵マークへの信頼を逆手に取り、フィッシングサイトに悪用されるケースが発生

ここまでのまとめ

- SSLは通信の暗号化だけでなく、本来は同時に通信相手の身元確認をするためのプロトコルだった
- しかし近年、利用範囲の拡大により、結果的に匿名でも取得可能な証明書も市場で提供されるように
- また、暗号化の機能だけが強調され、身元確認の重要性については忘れられがち…
- 従来のブラウザでは、身元確認の有無を一般ユーザが識別困難⇒フィッシングに悪用される事態に

EV SSLの登場

- CA/Browser Forum（CABF）の設立
  ⇒EVガイドラインの制定（2006/10、Draft11）
- EV SSL対応ブラウザの登場
  ⇒IE7、Firefox3
- JCAFの設立とCABFへの提案
  ⇒日本語版ガイドラインの作成、国内での標準化
  ⇒日本の法体系に沿う運用の提案（Appendix F）

EV SSLを一言でいえば

SSL証明書の審査発行基準の標準化　＋
一般エンドユーザに一目でわかるしくみ

＝ EV SSL
（Extended Validation SSL）

審査発行基準の標準化

- 20社以上の認証局＋ブラウザベンダーが参加し、世界共通の発行ガイドラインを制定
- より厳格な審査基準（実在証明）を定義
  - 法的実在　（Legal Existence）
  - 物理的実在（Physical Existence）
  - 運用実在　（Operational Existence）
- 審査発行に関する外部監査が義務

一般のユーザに分かりやすく

- 対応ブラウザでEV SSLが導入されたサイトにアクセスするとアドレスバーが緑に

EV SSLの先にあるもの

- EV適用範囲の拡大
  - コードサイニング、S/MIME…
- 全世界標準の企業認証の枠組み
- 「ホワイトリスト」ではなく「トレーサビリティ」
- ネット上の存在と実社会の存在を、信頼できる第三者が結びつける枠組みの必要性

PKI（セキュリティ）は運用がキモ！

- どんなに技術的に［優れて｜枯れて］いても、運用が伴わないと「インフラ」たり得ない
- 「標準化」と「公開」がキーワード
  - 標準制定プロセスの公開
  - 制定された標準そのもの
  - 本当に標準が守られているか（外部監査）