SSLサーバー証明書の動向

一般社団法人 日本電子認証協議会 (JCAF)
代表理事 秋山卓司

SSLの基礎知識

- Netscape Communication (1994年)
- インターネット上で最も広く使われている暗号化／認証プロトコル
- ウェブ以外にも利用範囲を拡大
- 認証レベルによってEV/OV/DVの３種類

認証レベルの違い

レベル	第三者認証	実在審査	グリーンバー
EV	Y	国際標準	Y
OV	Y	各CA基準	N
DV	Y	N	N
自己署名	N	N	N

EV SSL 最新動向

- 国内及び海外の普及状況
- PC上の主要５ブラウザが対応を完了
- 10/1に最新ガイドラインV1.2が公開
- 暗号アルゴリズムの2010年問題対応

2011年以降のEV SSL

- EVガイドラインのAppendix Aに記載
- RSA2048/SHA-1以上が義務化
- OCSPレスポンダが必須に

EV技術仕様の移行

項　目	2010年末まで	2011年以降
ルートCAのハッシュ	MD5を許容	SHA-1以上
サブCAのハッシュ	SHA-1	SHA-1以上
サブCAの鍵長	1024以上	2048以上
証明書のハッシュ	SHA-1	SHA-1以上
証明書の鍵長	1024以上	2048以上
OCSP対応	推奨	必須

SSLの課題（世界）

- EV SSLの普及
- SHA-2（あるいはSHA-3）への移行
- EV以外（OV/DV）の最低基準
- 脆弱性が顕在化した場合の対処

SSLの課題（国内）

- EV 審査の最適化
- 携帯や他の機器の対応（EV/SHA-2等）
- 日本語対応（CNの記述をどうするか）