番号制度とPKI

JNSA PKI-DAY 2010
2010年6月29日

クロストラスト株式会社　秋山卓司

CrossTrust

はじめに

- 「番号制度とPKI」というお題を頂きましたので、EV SSL証明書とのからみでPKI の What? について考えてみました
- そもそも我々認証ベンダーは「何のために」「何を」証明しているのでしょうか？

CrossTrust

認証局の仕事

ものすごくシンプル言い方をすれば
信頼できる第三者として、

「ネットとリアルの
結びつきを保証する」

ことが認証局の仕事です

CrossTrust

結びつけるために

- 技術的な話（How?）
  - 2010年問題に代表される暗号の話等
- 制度の話（What?）
  - そもそも、何のために何を証明しようとしているのか？

CrossTrust

SSLサーバ証明書は

- 何のために
  - ネット上の円滑な取引（特にBtoC）のために
- 何を
  - ウェブサイト運営者の実在を証明

CrossTrust

SSLの2つの機能

- 「第三者による実在証明」
- 「通信経路の暗号化」

CrossTrust

EV SSL

- 世界的に標準化された審査プロセス
- 審査発行に関しても外部監査が必須
- 最新版の主要なブラウザ（IE, Firefox, Opera, Safari, Google Chrome）で採用
- アドレスバーが緑に表示される

CrossTrust

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

CrossTrust

EV SSL策定時の議論

- 認証レベルをどうするのか？
- 誰が認証レベルを確認するのか？

✓何を証明しているのか？

- ユーザーがどうやって確認するのか？

CrossTrust

法人が対象

- EV SSLガイドラインにおいては、原則として法的実在（法人）が証明書の発行対象とされている
- 法人の定義は国によって違う
- ネット上のBtoC取引において、どこまで厳格に定義することが適当か？

CrossTrust

法人とは

- 法律の規定によって権利義務の帰属者となるもの（法的主体）
- 民法33条「法律の規定によらなければ、成立しない」（法人法定主義）
- 法人擬制説 ⇔ 法人実在説

EVにおける登録番号

- EV SSLでは、証明書のフィールド：
  Subject:serialNumber (OID 2.5.4.5) に、
  法人設立/登録管轄地の法人設立機関が
  サブジェクトに割り当てた登録番号を
  記載することが必須

- 日本においては「会社法人等番号」

CrossTrust

会社法人等番号

登記所番号(6桁)＋種類(2桁)＋シリアル(6桁)

- 登記所が変わると番号が変わる
- 会社の移転や組織変更だけではなく、
  登記所の統廃合等でも変わってしまう
- 利用者側よりも管理者側の視点で付番

CrossTrust

番号の必要性

- 企業は国の枠を超えたところで、自らを証明する必要があるため、国際的な枠組が不可欠
- その一方で、法人は各国の法律によって規定されるので、必然的に法人番号もその国の法制度に依存することになる
- 適切な法制度がないと、企業はその存在をネット上で証明することができない時代に

CrossTrust

EV SSL策定時の議論

- 認証レベルをどうするのか？
- 誰が認証レベルを確認するのか？
- 何を証明しているのか？

✓ユーザーがどうやって確認するのか？

CrossTrust

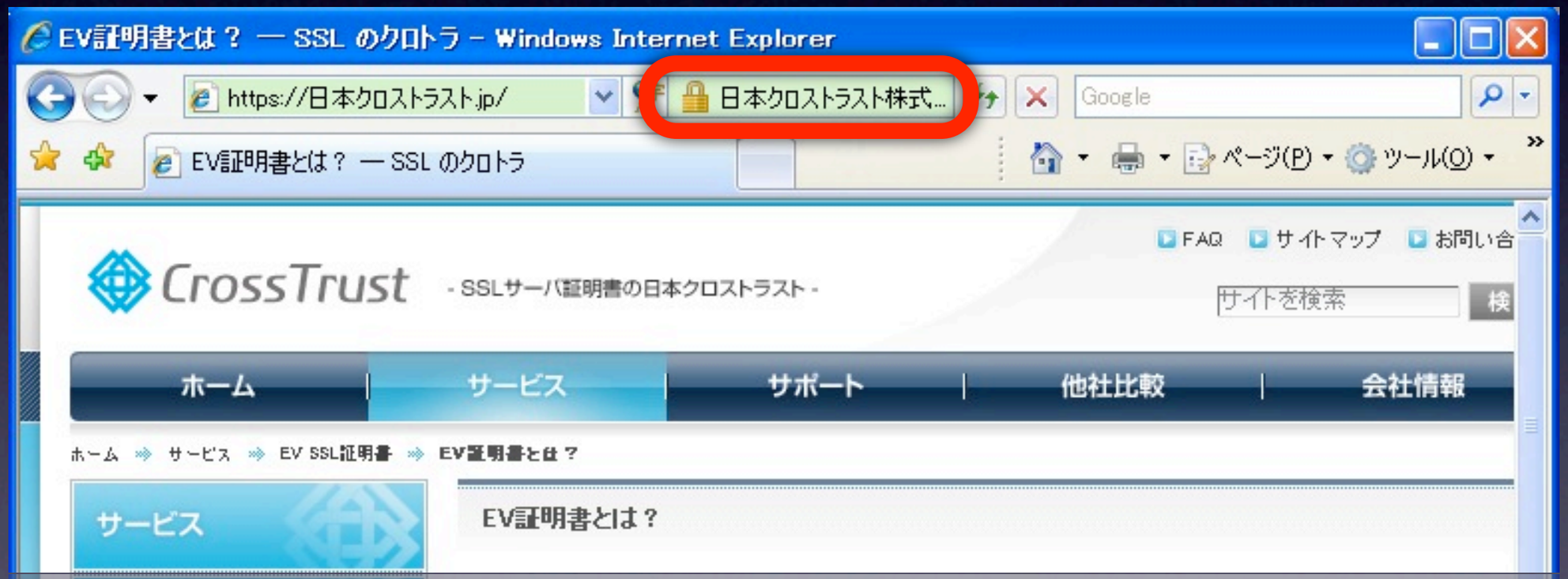
EVにおける組織名

- EV SSLでは、証明書のフィールド：
  Subject:organizationName (OID 2.5.4.10)
  に、「完全な法的組織名」
  を記載することが必須になっている
- 日本は例外が認められたものの…

CrossTrust

EV SSL

Internet Explorer 7 での表示例：



CrossTrust

英文社名の問題

- 日本語が読めないユーザーに、日本語で記載された法人名を表示することが適切かどうか？
- 英文社名と法人の結びつきをどう担保するべきか？

案1:会社法の改正

経済産業省アイディアボックス（OpenMETI）への投稿（05.社会制度総論、@00489）

法人登記事項に読み仮名と英文社名を追加する

現在の登記制度では、社名の読み仮名が登録されていません。例えば「日本」が「にほん」なのか「にっぽん」なのかについて公的に確認できる手段が存在しません。英文社名については、上場企業についてのみ金融庁管轄のデーターベース（EDINET)で確認することができる状況です。

今後、中小企業においてもインターネット経由での海外取引が拡大することを考えると、法人の一意性を確認する手段として公的情報を参照しても社名の発音がわからない、あるいは、アルファベットによる表記を確認できないという現在の状況は改善されるべきであると考えます。（英文社名については、希望する法人だけが登録する選択制としても良いかと思います）

CrossTrust

案2: 英文社名DB

CA/Browser Forum への提案 (2010-05-12)

非ラテン文字地域における
英文組織名データベースの提案

CA/Browser Forum

Japanese database of Latin-character versions of corporate names

日本においては、登記上の社名が非ラテン文字(漢字)で表記されてい るため、EVガイドラインの Appendix Fに記載されているガイドラインに 沿って証明書に記載される英文組織名が審査される必要がある。また、 国ごとの方法としてQIISもしくは弁護士の意見書によって確認された ローマ字名の使用や、あるいは、金融庁のデータベース、定款の参照な ど、日本における制度・習慣を反映した複数の手段が容認されている。
しかしながら、これらの方法によって対応可能な日本国内の組織はごく 限られており、EV証明書の普及を阻害する最も大きな要件の一つとなっ ている。

※詳細は別資料→

CrossTrust

ネット上の組織名

- 組織名の取り扱いについては言語と各国の制度の違いから課題を残している
- 法制度の対応には時間がかかるだろう
- 番号制度によって法的実在との結びつきが担保されることを前提に、組織名の多言語化の可能性を考えたい

CrossTrust

官民連携の可能性

- 日本には商業登記に基づく電子認証制度がある
- 技術的には、証明書発行時に不可欠な、法的な実在の証明と、意思・権限の確認が一括して電子的に実現可能である
- さらには、これまでのSSLでは見過ごされてきた、登記情報変更時の対応も可能になる

CrossTrust