トラストサービス検討WG発表資料

資料5－2

webサーバ証明書に関連する課題

伊藤 忠彦
セコム株式会社　IS研究所

2019/4/15

Web サーバ証明書における課題

①現状
- ブラウザのトラストリストが信頼の基点

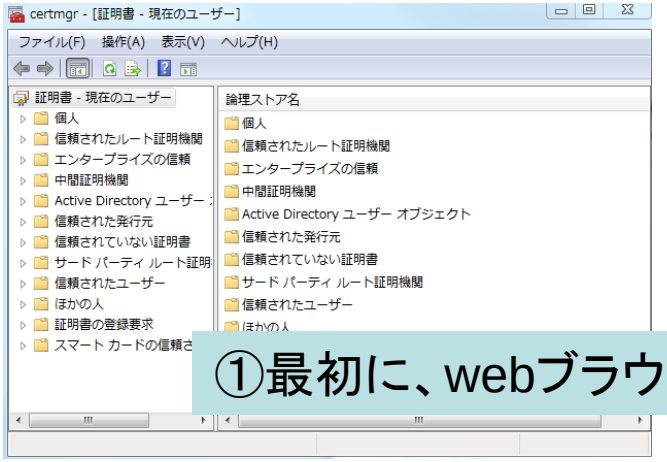
②CA/BForumによる認証局への要求
- 迅速性、透明性、厳格性

③課題

④国際動向

⑤むすび

①現状：ブラウザのトラストリストが信頼の基点



①最初に、webブラウザのトラストリストを使いアクセス

②データやアプリをDL

Webブラウザ
（のトラストリスト）

【制度的（根本的）課題】
最初にアクセスする対象がブラウザである以上、webサーバ証明書は
ブラウザを提供する主体のポリシに依存せざるをえない

実質的に、ブラウザのトラストリストが信頼の基点

①現状：ブラウザのトラストリストを守る事は非常に重要

Webブラウザ
（のトラストリスト）

- 安全なトラストリストは、ブラウザに必要な機能
- ブラウザのトラストリストに不備があると、webやInternet 全体へ脅威が波及する

- 日々高度化するサイバー攻撃に備える為、ブラウザトラストリストに記載される認証局には、以下が求められるようになった
  - より迅速なレスポンス体制
  - より透明な運用体制や運用実態
  - より厳格な本人確認

- ブラウザベンダに求められる迅速な対応ができず、トラストリストへ搭載されなかった民間企業や政府機関の証明書（GPKIなど）も存在する

多くの政府機関も商用認証局を利用する事になった

②CA/BForumの認証局への要求

迅速性

透明性

厳格性

② 認証局への要求：迅速性

- 要求変更等に、迅速に対応する事を求める

- 体制に不備が有った場合、速やかな改善を求める
  - 監査等の手続きが必要な場合もある（場合によっては非常にコストがかかる）

- 証明書の有効期間を5年⇒3年⇒2年と短縮
  （今後の技術動向により、さらに短くなる可能性もある）
  - 暗号アルゴリズムsha-1移行では、利用者への影響を鑑み、
    Sha-1証明書の新規発行を停止しつつ、発行済み証明書の期限切れを待った
  - 証明書の有効期限が長い事に起因し、移行に想定以上の時間を要した
  - NISTガイドラインは当初2010年までの移行を求めたが、
    CA/BForumが移行を完了したのは2017年

② 認証局への要求：透明性

- 要求全体の厳格性を確保する為、透明性を要求
- Certificate Transparency Log
  - 認証局が発行した全ての証明書を第三者に公開する
    - 組織内のドメインの構成等も露見する
- プロセスの透明性
  - 認証局の運用体制やインシデント対応を迅速に報告する

② 認証局への要求：厳格性（証明書発行に関して）

- 証明書発行における確認事項

  – ドメインを確認し、なりすましを防ぐ
    - CA/BForumでは、新技術等を採用しつつ改善を図った

  – 審査を行い、なりすましを防ぐ
    - 申込者の法人名等をきちんと確認する

  – 法人名とドメインの結びつきを確認
    - 各国の法人データシステムに応じて、独自の難しさがある（後述）

採用した技術

【DNS CAAリソースレコード】
DNSで配信する情報に、証明書発行を許可する認証局を記載する事ができる
【DNSSEC】
電子署名を利用し、DNS間で転送される情報の改ざんを防ぐ
【本人確認にもDNSを利用】
DNSで配信する情報に、本人確認時の連絡先や連絡方法を記載する事ができる（ルール策定中）

③課題

- 認証局は、CA/BForumの要求に対応する際に、
  各種コストの上昇にも対応しなければいけない。
  - 業務体制や業務システムの継続的かつ迅速な改善
  - 変化についての顧客説明

- 日本独自の課題
  - 法人名を日本語で記載すると、海外の人には読めない。
    - 世界において、「田」と「由」が入れ替わっていた時、判断できる人の比率は少ない
  - 英字で表記したいが、登記簿には英字表記は存在しない
    - 現状） 英字ト表記の妥当性の確認が必要
  - 臨機応変に対応しているが、全体的に「人手」がかかる

国際的な利用を考慮すると、海外のブラウザ利用者にとっても、証明書に記載されている法人を一意に同定可能な仕組みが望ましい
海外のブラウザ利用者が登記情報等にアクセスするのは難しく、また英字表記を元にした検索は必ずしもうまくいかない
法人登記に紐づく登記事項を、法人番号をもとに電子的に確認する仕組みが整備され、英字での表示にも対応すれば、上記のような問題は解決すると考えられる
加えて、利用者の発行申請の手間削減や、認証局の審査機械化が期待される

④各国動向：CA/BForumを取り巻く状況

中国

qihoo 360(独自ブラウザと独自トラストリスト)
民間向けと政府向けの2種類のトラストリスト
民間向けはWebTrust準拠も存在

【中国の方針】
独自ブラウザや独自トラストリストを開発し、
米国のブラウザに依存しない体制を構築中

迅速性・透明性・厳格性の要求
ローカリティへの配慮は存在する

CA/BROWSER FORUM

【EUの方針】
継続的に、様々なチャネルを利用した対話を行ってきた
現在は、米国ブラウザへEU独自トラストリスト搭載の為の摺合せ中
【現状】
EUは認定基準を作成し、CA/Forumは大枠で受け入れた
※EUのトラストリストに記載されていれば無条件で受け入れるわけではない

EU

FESA
Forum of European Supervisory Authorities for Electronic Signatures

ACAB'c

enisa
European Union Agency for Network and Information Security

ETSI

cen

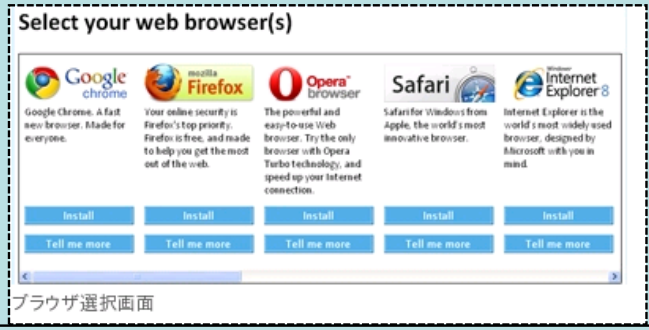
欧州標準化委員会

QUALIFIED TRUST SERVICE PROVIDER

各トラストサービスプロバイダ

https://www.enisa.europa.eu/events/tsforum-caday-2018/presentations/02_04_Gonnot.pdfをもとに構成

極端な例であるが、過去EUは、ブラウザの
選択画面必須化（2009）等も行っている（私見）



ブラウザ選択画面

https://www.itmedia.co.jp/news/articles/1303/07/news027.html

⑤むすび

- 利用者が最初に利用する信頼点は、
  Microsoft、Mozilla、Apple等のトラストリスト
  - ブラウザを提供する主体のポリシに依存せざるをえない構造になっており、
    回避する場合は利用者に負担を強いる事になりうる
- 日本には欧米と異なる制度もある（漢字利用、戸籍、法人登記、プライバシ、etc.）
  - 日本の制度と、CA/BForumのポリシが背反した場合、対応できない

- 提言
  - CA/BForum等に積極的に関わる事も検討すべき
    （独自の認定基準及び独自トラストリストを作成したETSIの活動が参考になると考えられる）

    - （私見）フォーラム標準での活動では、ユースケースの明確化が重要
      - 日本独自の要件が存在するか、トラストリストの利用目的は何か、等の検討を予め行う事が望ましい