CrossTrust

暗号アルゴリズム２０１０年問題

事例：電子証明書の国際標準化の動きと日本の携帯

日本クロストラスト株式会社

代表取締役 秋山卓司

PKI-DAY 2008

CrossTrust

SSL証明書の国際標準化までの道のり(1)

- SSLがNetscape Communication社によって1994年に発表された時点では、「暗号化」と「実在証明」の2つの機能があった
- その後、SSLの利用範囲が拡大するとともに「実在証明」の機能を省いたものが登場
- エンドユーザが「実在証明」の有無をブラウザ上で簡単に識別する方法がなかったため、フィッシングサイト等に悪用されはじめる

SSL証明書の国際標準化までの道のり(2)

- 米CA/Browser Forum (CABF) の発足 *1)
- 証明書の審査方法の標準化と、わかりやすいユーザインターフェースをブラウザに搭載
  ⇒ EV SSLの誕生(2007/1)
- 日本における普及と標準化のために
  日本電子認証協議会 (JCAF)が発足 *2)
- JCAFからの提案がEVガイドライン V1.0で採用される (2007/6、Appendix F)

*1) http://www.cabforum.org/
*2) http://www.jcaf.or.jp/

CrossTrust

新しい世界標準「EV SSL」

- ガイドライン策定には、世界30以上の認証局と、主要なブラウザベンダーが参加
- 全世界共通の厳格な審査・発行基準
- 監査法人による審査プロセスの認証
- ひとめでわかる「緑のアドレスバー」
- IE7、Firefox3、Opera9.5以降が対応

EV SSLの暗号アルゴリズム移行

- EV SSL Certificate Guidelines（V1.1）の Appendix A において：

> “…subscriber certificates containing a 1024 bit RSA key MUST expire on or before 31 Dec 2010.”

「1024ビットRSA鍵を含む加入者証明書については、2010年12月31日以前に失効させなければならない」

CrossTrust

ところが．．．

- 日本で発売された一部の携帯はRSA1024のみに対応している
- ルート証明書の入れ替えでは解決せず、新しい機種に買い換えてもらう必要がある
- 平均的な耐用年数から考えても、ほとんどの携帯端末が買い換えられるまでには長い期間がかかる

その一方で．．．

- EVガイドラインは、2006年10月に発表されたDraftの時点で、2010年末までは移行措置のため、従来のRSA1024のルート証明書及び、RSA1024の中間証明書とも繋げることが許されている。

- EVガイドラインV1.0制定の際に、「EVはRSA2048に統一するべき」との意見が出たが、これを日本市場の携帯対応を理由に一旦延長。

日本の選択は？

EV SSLにおいて：

A) 2010年末でRSA1024を切り捨てる

B) CABFに移行期限の延長を提案する

JCAFのプロポーザル案

- JCAFでは、「2010年問題対策WG」を設置し CABFに対してのプロポーザルを現在検討中

（具体的内容は本原稿提出の時点では未定）

CrossTrust

プロポーザルの是非

1) 延長するだけの理由があるか？

2) 期限を延長しても十分に安全なのか？

3) 延長することで、本当に移行が可能なのか？

1) 十分な理由があるか？

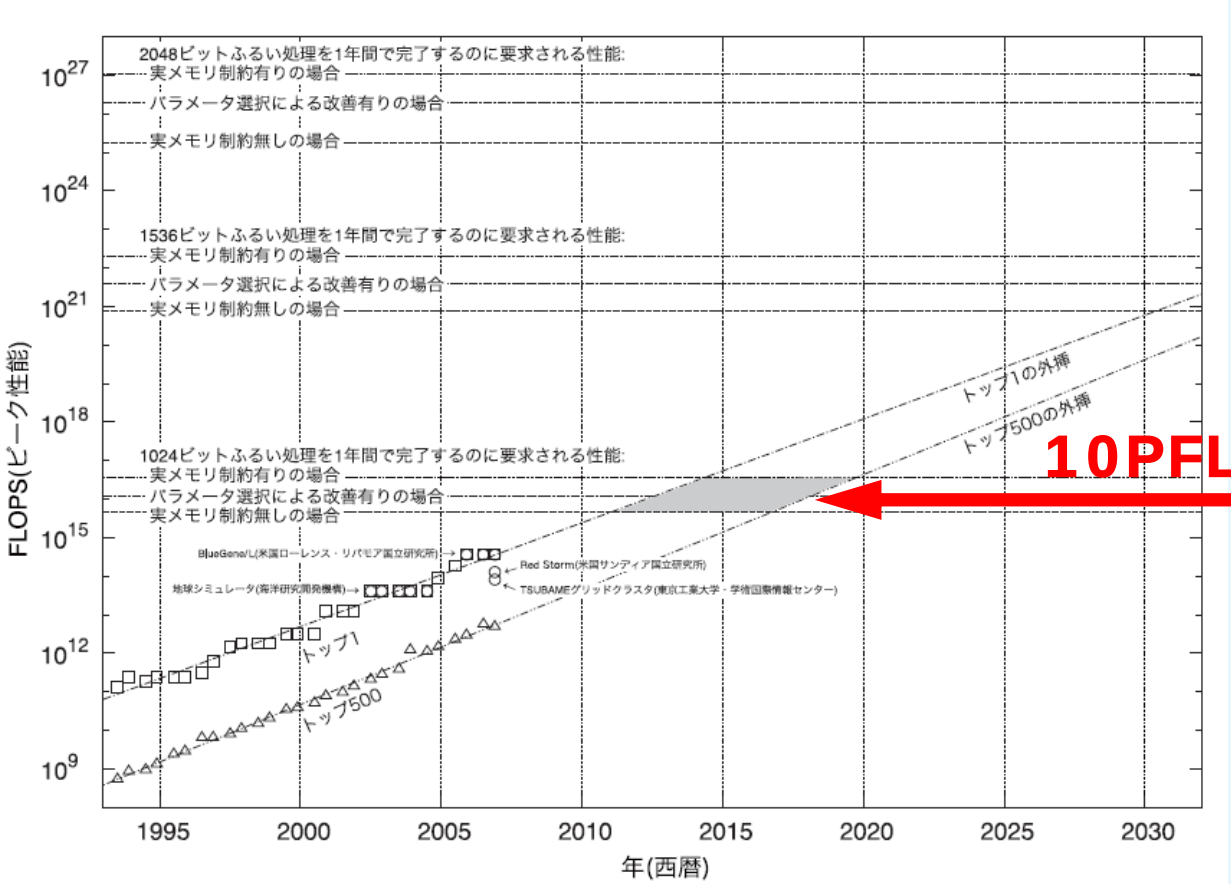
- 日本においては、インターネット上のトランザクションの多くの部分が携帯によるもの

- EV SSLの普及のために携帯対応が不可欠

  ⇒携帯用、PC用にSSLを使い分けるためだけに2つのサイトを立てなければならなくなる

CrossTrust

2) 移行期限を延長しても安全か？



*1)暗号技術検討会 2006年度報告書 (2007/3)、14p「1年間でふるい処理を完了するのに要求される処理性能の予測」

CrossTrust

思わぬ朗報 (?)

- 本年4月に内閣官房情報セキュリティセンターが、政府機関の情報システムにおいては、暗号アルゴリズム移行の期限を2013年度内とする方針を発表

- RSA2048への移行期限を延ばしてもらう大義名分ができた？

3) 移行は可能なのか？

- 携帯については、今後は全てRSA2048に対応可能な機種のみが発売され、今後も今まで同様な買い替えのサイクルが続くと仮定すれば2012年までには、市場に与える影響は最小化されると予想。

CrossTrust

残される課題

- CABFへのプロポーザルが受け入れられても、受け入れられなくても、移行を進めていかなければならない状況は変わらない
- SHA-1については先送り
- 間違ったメッセージとして受け取られないか？
- 次に移行が必要になった時は？

日本以外でのコンセンサス

- RSA2048及びSHA-256への移行については、NISTの影響力が極めて大きい
- PCでの利用を前提としているためRSA2048に移行しても、処理能力の問題は特に無い
- オンラインアップデートで移行可能
- 過去の互換性よりもセキュリティが重要

CrossTrust

日本の理解されにくい現状

- 民間の暗号アルゴリズム移行について、方向性やスケジュールを誘導する政策・組織がない
- インターネット上のトランザクションにおける携帯のシェアが極めて大きい
- 携帯や組み込み系機器においてはRSA2048の処理はまだまだ重たい場合もある
- 必ずしもオンラインアップデートが可能でない
- 既にメンテされていなくても、今は捨てられない

デッドロック状態 (by JNSA松本さん)

- 暗号研究者
- 標準仕様策定関係者
- PKIミドルウェア開発ベンダー
- アプリケーションベンダー
- 認証局、証明書発行ベンダー

CrossTrust

ワーストシナリオ

- 市場環境の特殊性から、他国と比較してより早い、また長期にわたる移行期間が必要とされるにも関わらず、移行開始そのものが遅れる。
- 日本vs海外、また国内においても携帯vsその他のインターネット等、複数の標準が継続して存在し、かつそれらを維持するためのコスト増。
- PKIという選択肢そのものへの不信感が増大。

CrossTrust

本来取るべきアプローチ

- 「ロングタームセキュリティ」
- レイヤーを跨いだ情報交換と相互啓発
- アルゴリズムの移行を前提としたシステム及び制度設計、技術者への注意喚起
- 民間においても、全てのレイヤーに属する関係者が協調、連携して問題に取り組むべき