EV SSLと暗号の2010年問題

－ 新たな国際標準化の流れと日本市場への影響 －

日本クロストラスト株式会社
代表取締役　秋山　卓司

1. EV SSL 登場の背景

インターネット上で最も広く使われている暗号プロトコルの一つにSSLがあります。SSLは米Netscape Communication社によって、インターネットというお互いの顔の見えない、オープンなネットワーク上で重要な情報をやり取りするために提案されたもので、通信経路の暗号化とWebサイト運営者の実在確認という2つの機能があります。インターネット上でのBtoC取引の拡大とともにSSLの需要も伸び、広く普及することとなりましたが、近年ではさらにその利用範囲も拡大し、メールの送受信(SMTP/POP over SSL)や、SSL-VPNなど、同一組織、あるいはグループ内で利用されるケースも増えてきました。

このような用途では、不特定多数を対象とするWebの場合と異なり、サーバ運営者の身元確認は特に必要ないため、通信経路の暗号化のみを目的とした低コストのSSLサーバ証明書が市場に提供されるようになったのです。またこれらの証明書はサーバ運営者の身元は確認せず、ドメインの所有者か否かを審査の対象としているため、匿名での取得も可能です。

これらの実在証明の審査を省いた証明書は、同一企業内、もしくはサーバ運営者とそれを利用するユーザーの間にあらかじめ信頼関係があること(例えば自社で管理しているメールサーバへのアクセスに利用するなど)を前提にしていましたが、不特定多数からのアクセスを前提とした通常のWebサーバに導入された場合であっても、実在証明のあるSSL証明書と同様にユーザーのブラウザには南京錠マークが表示されるため、一般のユーザーが実在証明の有無を見分けることは事実上困難であるという問題を抱えていました。

各種調査等によるとユーザー側の南京錠マークに対する信頼度は非常に高く、例えばネットショッピングの際「南京錠マークがあれば安心」という認識が広がっている一方で、このユーザーの南京錠マークへの信頼感を逆手にとって、実在証明の無いSSLサーバ証明書を使ったフィッシングサイトが多数報告されるに至ったのです。

この事態を受け、主要なブラウザベンダーと世界各国の認証局が中心となり、証明書発行に際するサーバ運営者の審査基準を標準化することと、またその標準化された証明書を、一般のユーザーが容易に確認できる手段を提供することを目的として米国で設立されたのがCAブラウザフォーラム(CABF)です。(http://www.cabforum.org/)

CABFでは、これまで各認証局が個別に定めていた審査プロセスについて、全世界で統一された非常に厳格なガイドライン(EVガイドラインと呼ばれる)を定め、さらに、第三者である監査法人が、認証局がEVガイドラインを厳守していることを確認することを義務付けました。このEVガイドラインに沿って発行された証明書がEV SSLサーバ証明書と呼ばれるもので、IE7やFirefox3、Opera9.5、あるいはGoogle Chrome等の最新ブラウザでこの証明書を取得したWebサイトにアクセスすると、アドレスバーが緑に変色するため、一般のユーザーにも一目で見分けることが可能になっています。

また、日本でも国内の認証ベンダー及びブラウザベンダーが発起人となって2006年1月に日本電子認証協議会(JCAF)が設立され、日本におけるEV SSLの標準化と普及促進を目的とした活動が開始されています。(http://www.jcaf.or.jp/)

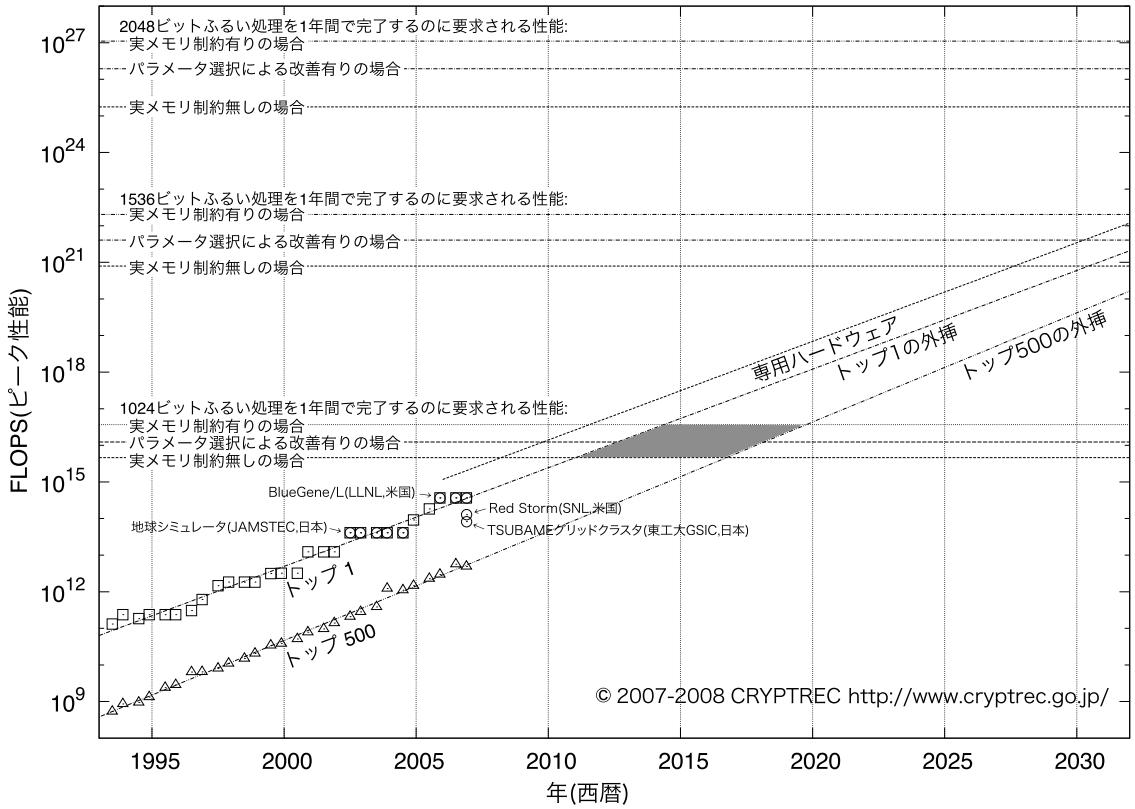
2. 暗号の 2010 年問題とは

前述の通り、一般のユーザーにとってより安心、安全なインターネット環境を実現するために、世界各国30社以上の認証局と、主要なブラウザベンダーが参加して策定されたEV SSLですが、そのガイドラインには発行時の審査プロセスと合わせて、証明書の技術的仕様についても言及されており、特にSSLに使われている公開鍵暗号の鍵長については、

2010年末を期限として、従来広く使われていた1024ビットRSA鍵から2048ビットRSA鍵へと移行することが義務づけられています。

暗号は解読に使われる計算機の性能向上や、特定のアルゴリズムについての研究が進むに従い、徐々にその相対的な強度は弱まっていくことになります。従って、長期間の利用が想定される場合には、将来的な強度低下をあらかじめ想定した上で暗号の仕様が選定され、また定期的にその強度が検証されなければなりません。

では、暗号はどれくらいの強度を持つべきなのでしょうか？それに答えるのは簡単なことではありませんが、政府の暗号技術検討会2006年度報告書に掲載された次のグラフが参考になるかと思います。



グラフの縦軸には解読の対象となる暗号の強度が示されており、斜めの線は各年代における計算機の処理能力向上を表しています。そして、2015年を中心とした赤い平行四辺形として示された部分が、従来広く使われてきた1024ビットRSAが計算機の処理能力向上とともに、解読の危険性が高まるであろう時期を示していることが、このグラフから読み取って頂けるかと思います。

つまり2010年は何十年に一度の暗号アルゴリズムの世代交代という大きな節目にあたり、その移行についてはコストや相互運用性の確保など、さまざまな困難が予想されています。これがいわゆる「暗号の2010年問題」です。そしてこの「暗号の2010年問題」は、日本において、より深刻な問題となる可能性があります。

3. 日本特有の問題

EV SSLの場合には、日本市場において一部の携帯端末が2048ビットRSA鍵に対応していないことが、移行における大きなハードルの一つとして指摘

されていました。現在、EV SSLのガイドラインでは、互換性確保のために1024ビットRSA鍵の利用が許されていますが、前述の通り、このまま行けば2011年以降は2048ビットRSA非対応の携帯端末からは、EV SSLサーバ証明書を採用したサイトとのSSL接続ができなくなってしまいます。また、2048ビットRSAに対応した携帯であっても、現時点ではEV SSL対応のブラウザが搭載された機種はありません。

ご存じの通り、日本では多くのユーザーが携帯端末経由で日常的にインターネットにアクセスしており、携帯コンテンツについては、その絶対的規模と成長率において、世界でも類を見ない最先端の市場です。また、総務省の調査によると、Eコマースの実に20%が携帯を使用しているとのことです。

その一方で、世界的に最先端であることは、「特殊」であり、海外ではなかなか理解されにくいということでもあります。事実、当初のEVガイドライン策定段階においては、日本のベンダーが議論に参加していなかったこともあり、携帯端末をはじめとする組み込み系の機器でのSSL利用については元々想定されていませんでした。つまり、あくまでPCでの利用が前提ですから、暗号アルゴリズムの移行等に関してもオンラインアップデートで対応可能だろうと考えられていたのです。ところが、携帯端末にオンラインアップデートの仕組みはありません。新しい暗号アルゴリズムに対応するには、基本的にはユーザーに端末を買い替えてもらう必要があるのです。

JCAFでは、このように携帯がPCと比較して移行に長い期間が必要なことと、日本市場における携帯の重要性、また後述の通り日本政府が2048ビットRSAへの移行を2013年度までに完了させるという指針を出したことなどから、1024ビットRSAにしか対応していない携帯にも対応するEV SSL証明書の利用可能期間延長をCABFに対して提案しましたが、結果的に受け入れてはもらえませんでした。

4. 政府と民間の取り組み

2010年末に暗号アルゴリズムを移行させるようにとの勧告を出しているのは、アメリカ国立標準技術研究所(National Institute of Standards and Technology、以下NIST)という組織です。NISTは本来、米国政府の調達基準を定める機関ですが、民間にも極めて大きな影響力があり、暗号等についても事実上の標準となっています。CABFが定めたEV SSLのガイドラインも暗号の技術的仕様については、NISTの勧告に準拠しています。

一方日本では、本年4月に内閣官房情報セキュリティセンター（NISC）が、政府の情報システムで使用する暗号アルゴリズムを2013年度を目途に移行する方針を発表しました。しかし残念ながら、日本の場合は民間の規範となるべく発表されたものではなく、あくまで「政府の政府による政府のための」基準にすぎません。

つまり民間は、それぞれ独自に暗号に関する基準や移行のスケジュールを決定する必要に迫られるわけですが、個々の事業者が最新の学術的研究結果と実際に採用した場合の費用対効果、さらには相互運用性等のバランスを取って暗号アルゴリズムを適切に選定することはかなり困難な作業となることが予想されます。

前述の通り、日本市場においては、携帯をはじめとする組み込み系機器における暗号の利用も多く、移行には諸外国に比べてより長い期間が必要であると考えられます。従って本来は、より早い時期から準備を進めるべきなのですが、このまま民間における標準化やスケジュールのコンセンサスをとる動きが出ないまま進んだ場合、諸外国に比較して移行が著しく遅れることも危惧されます。そして、その結果としてもたらされるものは、単なる暗号の安全性の低下だけではありません。

相互運用性を考えなくて良い、閉じたシステムはともかく、そうでないシステムで移行が長期間にわたるということは、必然的に両方の標準を運用し続けるということになります。しかも、下位にあたる基準は日本国内でしか使えないとすれば、このダブルスタンダードを維持するコストは、国内の事業者およびユーザーが負担することになってしまいます。社会全体のコストを最小化するためにも、民間にお

けるプレーヤーの整理と情報共有、そしてアクションプランの策定が必要なのではないでしょうか。

5. 最後に：「公開と標準化」によるセキュリティ

今回はEV SSLを例にして、運用基準と技術仕様の両方が世界的に標準化されることによって、SSLが新たなセキュリティの枠組みとして次の段階に進もうとしていることをお伝えしました。海外では、公開された標準ができることを新たなビジネス参入の機会として捉え、標準策定に積極的に関与しようとする動きが見受けられます。「公開と標準化」これはSSLに限らずセキュリティの様々な分野においても大きな流れであるかと思います。

しかし残念ながら日本においては、標準が決まった後でそれを「ローカライズ」することで手一杯で、一番重要な標準化の際の議論に直接参加していなかったり、あるいは、日本国内だけのための仕様策定に終始し、そこで標準化された成果を海外に送り出そうという動きが少ないように感じられます。また特にセキュリティの分野で「公開と標準化」の重要性があまり認識されていないと感じるのは筆者だけでしょうか。

2006年2月、政府は情報セキュリティ政策会議において「情報セキュリティ立国」の理念を掲げ、世界一安全な国として「ジャパンモデル」の確立を目指すとしました。暗号の研究において日本は世界有数の実力を持っているはずですが、その成果を社会が享受できるまでには、まだまだ道半ばと言わざるを得ません。今後の日本の取り組みが、将来他の国からお手本とされるような「ジャパンモデル」として実現されることをぜひ期待したいと思います。

参考

「CRYPTREC Report 2006 暗号技術監視委員会報告書」
http://www.cryptrec.go.jp/report.html

「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」
http://nisc.go.jp/active/general/pdf/crypto_pl.pdf

「次期情報セキュリティ基本計画に向けた第1次提言」説明資料
http://www.nisc.go.jp/conference/seisaku/strategy/dai10/pdf/10siryou_ref01.pdf