IPA Technical Watch

IPA

IPA テクニカルウォッチ

『暗号をめぐる最近の話題』に関するレポート

～　SSL/TLS や暗号世代交代に関連する話題から　～

2011 年 5 月

IPA テクニカルウォッチ：『暗号をめぐる最近の話題』に関するレポート
～　SSL/TLS や暗号世代交代に関連する話題から　～

目次

IPA テクニカルウォッチ：『暗号をめぐる最近の話題』に関するレポート
～　SSL/TLS や暗号世代交代に関連する話題から　～

2011 年 5 月 11 日
IPA（独立行政法人　情報処理推進機構）
セキュリティセンター

1. はじめに

最近、社会生活に影響を与えるような暗号をめぐる話題がいくつか立て続けに起こっている。しかも、そのいずれもがいまや社会インフラともなっている SSL/TLS (Secure Socket Layer/Transport Layer Security) プロトコルを主な舞台としており、セキュリティ専門家ではないごく一般のユーザにも少なからず影響を与えている。

本レポートでは、一般ユーザへの警鐘の意味も込め、暗号をめぐる最近の話題と題して俯瞰的に取りまとめる。

2. SSLでのセキュリティ事故

オンラインショッピング、インターネットバンキング、ネットトレード ― これらのサービスを利用するときにほぼ確実に使うのが SSL/TLS プロトコルである。そして、そのようなサイトの「セキュリティ」の項目をみるとほぼ例外なく「お客様の情報を守るために“SSL という暗号化技術”を採用」と書かれているはずである。ところが、その SSL/TLS プロトコルで最近事故が複数発生している。

2.1 不正SSLサーバ証明書が発行された事件 – Comodo社のケース

SSL プロトコルで使われる SSL サーバ証明書は、ブラウザが接続する相手のサーバ自体が正当なものであるかという「サーバ認証」と暗号通信を行うための「鍵交換」に使われる。

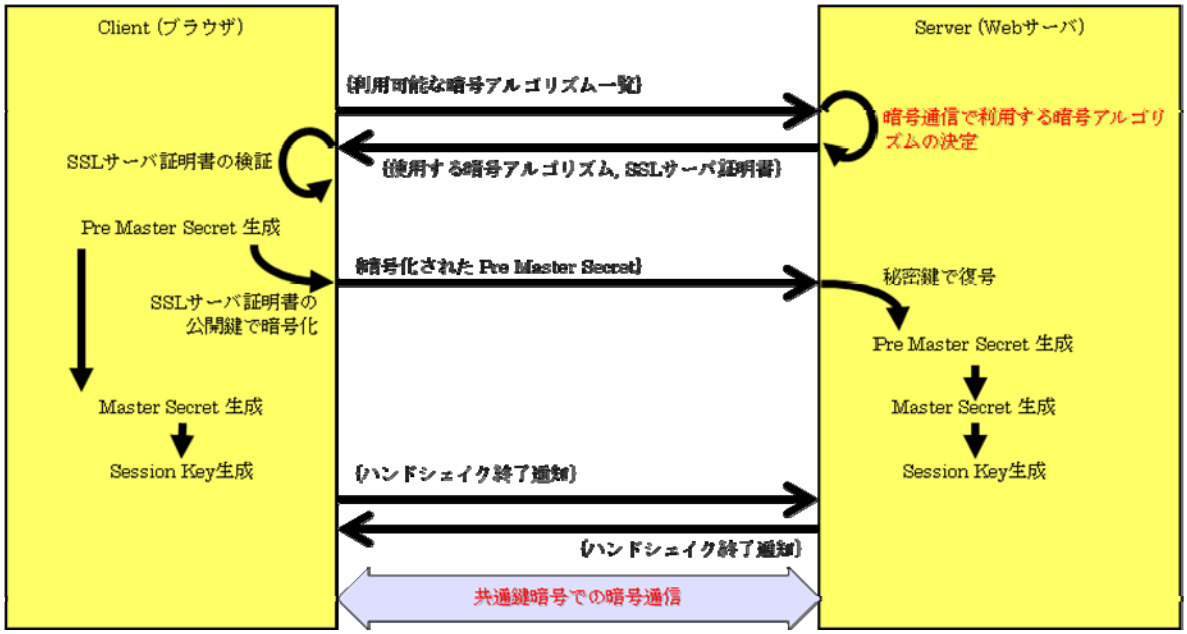

図 1. SSL プロトコルの仕組み

そのため、SSL プロトコルを使ったサービスを利用するということは、SSL サーバ証明書が信頼できるものであることを暗黙の前提とする。その一方、SSL サーバ証明書そのものは仕様が決まっており、誰にでも発行することができるものなので、SSL サーバ証明書の信頼性を何らかの手段で確認する必要がある。

公開鍵暗号基盤 PKI (Public Key Infrastructure)は、信頼できる第三者機関である認証局 CA (Certification Authority)が SSL サーバ証明書を発行することで SSL サーバ証明書の信頼性を保証する仕組みである。利便性を考慮し、例えば WebTrust for CA に基づく第三者監査を取得した CA は「信頼できる第三者機関である認証局」として、Internet Explorer（正確には MS-Windows が管理）や Firefox などのブラウザにあらかじめ登録されている。これにより、WebTrust for CA を取得した CA が発行する SSL サーバ証明書の信頼性は、ユーザが意識することなく、ブラウザの中で自動的に検証される。

今回の事件は、WebTrust for CAを取得している Comodo 社の CA から不正 SSL サーバ証明書が“通常の手続き”を経て発行されたことである。Comodo 社の Incident report [1]によれば、その経緯は以下のとおりである。

1. 2011 年 3 月 15 日、SSL サーバ証明書の発行にあたって身元を確認する Comodo 社の登録機関 RA (Registration Authority)の一つで、あるユーザアカウントがクラックされる（その攻撃では主にイランに割り当てられている IP アドレスが使われた）
2. クラックされたユーザアカウント上に新たなユーザ ID が作られる
3. 2.で作った新たなユーザ ID を使って、（見掛け上正当な）証明書署名要求 CSR (Certification Signing Request)が 9 つ（ドメインとしては 7 つ – mail.google.com, www.google.com, login.yahoo.com, login.skype.com, addons.mozilla.org, login.live.com, global trustee）不正に作られる
4. 3.で不正に作られた 9 つの CSR に対して、Comodo 社の CA に（不正な）SSL サーバ証明書の発行依頼が通常の手続きに従って行われる
5. 受け付けた CSR のいくつかについて（不正な）SSL サーバ証明書を通常の手続きに従って発行

この攻撃に関連して犯人が手口を公表したとの報道[2]もある。真偽のほどは完全に確認されているわけではないが、今のところ状況的に矛盾するところは見つかっていないようである。ここでのポイントは以下の点である。

① 当初ハッキングのために RSA アルゴリズムを破ろうとしたが、RSA アルゴリズムを破る前にハッキングに成功している。これは、Comodo 社の CA の鍵情報の漏えいはなく、また別の RA にも問題がないとの Incident report での記述と矛盾していない
② CSR 提出プロセスの一部でテキスト形式のユーザ名とパスワードが使われていることを発見し、その脆弱性を利用して SSL サーバ証明書の発行依頼を行っている。つまり、パスワードの取り扱いの問題に起因した事件である可能性が極めて高い

このように事件の形としては、比較的単純なものである。しかし、経緯がどのようなものであれ、WebTrust for CAを取得している CA から不正 SSL サーバ証明書が通常の手続きに則って発行されてしまった影響は大きい。先に述べたように、WebTrust for CAを取得している CA が発行する SSL サーバ証明書の信頼性は、ブラウザの中で自動的に検証されるため、通常の手続きに則って発行された

SSL サーバ証明書は基本的に信頼できるものとして扱われてしまうためである。

そこで、不正 SSL サーバ証明書をブロックするために、Comodo 社では、不正 SSL サーバ証明書が発行されたことを認識した後に、速やかにそれらの SSL サーバ証明書を失効させ、証明書失効リスト CRL (Certificate Revocation List)に登録した。合わせて、Microsoft や Mozilla をはじめとする主要なブラウザベンダに対してセキュリティアラートを通知している。

これを受けて、例えば、Microsoft は 2011 年 3 月 24 日にセキュリティアドバイザリ(2524375) [3]を公表し、Windows update 向け更新プログラムをリリースした。Mozilla も、同 22 日に Mozilla Foundation Security Advisory 2011-11 [4]を公表し、Firefox 向け更新プログラムをリリースしている。どちらの更新プログラムも、緊急度が高いため、月 1 回行われる定期リリースによらないアップデートの対象としており、OS やブラウザが自動アップデートするように設定されていれば、比較的早期に自動的に更新される。このほかの主要なブラウザベンダも同様の対応を行っている。

実際に正規のドメイン名を使った不正な SSL サーバ証明書でフィッシングを成功させるためには、DNS キャッシュポイズニングによって詐称したドメインに誘導するなどが必要となるため、現時点までに本件を原因とする不正行為は報告されていない。

しかし、いかなる理由であれ、WebTrust for CA を取得している CA が不正 SSL サーバ証明書を発行することは本来あってはならない事象であり、何ら対策をしていなければ不正な Web サイトを信頼できる Web サイトであるとブラウザが誤認する恐れがある。それを避ける意味でも、特に自動アップデートを設定していないブラウザについて、各々のブラウザベンダが作成した、本件に対処するための更新プログラムが必ず適用されていることを確認していただきたい。

2.2 オンラインショッピングでSSLプロトコルが動作せず – 大手百貨店のケース

2011 年 3 月 4 日、大手百貨店が運営するオンラインショッピングサイトで、「個人情報は、信頼性の高いセキュリティ技術の SSL を使用し暗号化しています。」と表示しておきながら、Web サーバの設定ミスにより SSL プロトコルが動作しないまま運用が続いていた、と発表した。

ホームページ上に公開された情報によれば、本件での該当案件は以下の通りである。つまり、本件の事象による直接的な影響は、個人情報である、顧客の氏名、住所、電話番号、メールアドレスが暗号化されずに顧客の端末から大手百貨店オンラインストアのサーバにインターネットを経由して送信されていたことである。

該当ページ	カタログ申し込みページ
対象カタログ	通信販売カタログ、中元カタログ、歳暮カタログ、おせちカタログ、ギフトカタログ
該当期間	平成 22 年 5 月 19 日～平成 23 年 3 月 2 日
該当件数	7,444 件 6,064 名
該当する個人情報	氏名、住所、電話番号、メールアドレス

ここで注意してほしいのは、Web サーバの設定ミスからオンラインショッピングサイトで SSL プロトコルが使われていなかった事故が起きたという理由だけで本件を取り上げているわけではないということである。もちろん、「SSL を使っている」と表示しながら実際には「SSL を使っていなかった」ということに対して Web サーバ管理者に過失があったことはいうまでもない。

しかし、本件には、そのこと以上にもっと深刻な問題が 2 つ含まれている。

一つは、Webサーバ管理者側からの視点の問題であり、本件が“約 9 ヶ月もの間、発覚しなかった”ということである。

対象カタログで「中元」「歳暮」「おせち」というように明らかに販売時期が異なるものが掲載されていることから見て、この期間中に何度かページ更新されたはずである。それにも関わらず発覚しなかったということは、ホームページ完成時の確認を怠っただけではなく、実際の稼働を始めた後も一度たりとも SSL プロトコルの動作確認を自らしていない、ということである。しかも、顧客からの指摘で判明したとの報道もあることから、もしその指摘がなければ未だに継続していた可能性さえある。

SSL プロトコル設定の確認漏れが起きた理由として、http://で始まる暗号化をしていないページとhttps://で始まる暗号化をしているページが混在していることが影響していたことも可能性として考えられる。オンラインショッピングなどではよくあるサイト構成ではあるが、http://から https://に切り替わったことが分かりづらい表示方法であると設定ミスを見落とす可能性が高まる。

もうひとつは、利用者側からの視点の問題であり、“約 9 ヶ月間に6,064 名もの顧客が利用していた”ということである。

SSL プロトコルが使われているかどうかを確認する手段として、ブラウザの URL アドレスバーでの「https://」表示と「南京錠」表示がある。オンラインショッピングに限らず、Web ページに個人情報やパスワード、クレジットカード番号などを入力する場合には、それらの表示を見て SSL プロトコルが使われていることを確認するよう、様々なところで啓発されている。

しかし、本件の場合、実際にはSSLプロトコルを使っていなかったことから、当然ブラウザには「https://」表示も「南京錠」表示もなかったはずである。それにも関わらず、多数の顧客が利用していたという事実は、顧客側も、大手百貨店のWebサイトでSSLプロトコルが実際に使われているかを確認してから行動していたのではなく、大手百貨店のWebサイトなのだから安心に違いないという思い込みで行動をしていたことを図らずも示したことになる。

今回は、たまたま本物の大手百貨店の Web サーバでの設定ミスが原因であったために、顧客に被害が及ぶリスクは相対的に低いと考えてよい。しかし、仮にこれが本物の大手百貨店の Web サーバに似せたフィッシングサイトであったとしたらどうであろうか。想像したくないことではあるが、多数の顧客の個人情報がフィッシングサイトに流れていた可能性は否定できない。

SSL プロトコルというと「個人情報を暗号化する」ための技術というイメージが強いが、オンラインショッピングでは、ブラウザが接続する相手のサーバ自体が正当なものであるかという「サーバ認証」も同じように重要な機能である。とりわけブランド力がある企業の Web サイトはフィッシングサイトの標的になる恐れがあり、サーバ認証には「フィッシングサイトから顧客を守る」という役割もある。

Web サイトの構築・運用にあたっては、単に個人情報を保護するために暗号化するという目的だけのために SSL プロトコルを導入すればよいと考えるのではなく、フィッシングサイトから顧客を守るという観点を含めて SSL プロトコルの重要性を認識し、顧客への啓発を進めていただきたい。

その意味で、Web サイト構築者は、Web サイトでの見栄えを重視し、同一ページ上に SSL プロトコルで暗号化する部分とそうでない部分が混在するような作りはやめることを検討していただきたい。このような作りをしたページでは、「https://」表示がありながら「南京錠」表示が出ないといったことが起きるため、SSL プロトコルが正しく動作しているかを利用者が確認する際の障害となる場合がある。

図 3. Internet Explorer 8（上）と Firefox 3（下）における SSL プロトコル動作中の表示例
（〇の部分の表示を確認。EV SSL サーバ証明書なら URL のアドレスバーが緑色になる）

また、利用者も、たとえ有名な企業の Web サイトだとしても、少なくとも個人情報やパスワード、クレジットカード番号などを入力するページでは、「https://」表示と「南京錠」表示を確実にチェックすることで SSL プロトコルが正しく動作しているかを確認する癖をつけていただきたい（図 3 参照）。

2.3 SSLサーバ証明書を使ったフィッシングサイトにも注意

前節でフィッシングに遭わないためにも SSL プロトコルが正しく動作しているかを確認するようにと記述したが、これはあくまで最低ラインの行為である。それというのも、SSL サーバ証明書の信頼性にはやや問題があるからである。

2011 年 2 月 25 日、シマンテックは、SSL サーバ証明書を利用した大規模なフィッシングが発見されたと同社のセキュリティブログに掲載した[5]。最近でこそ珍しくなった手法ではあるが、ユーザにあえてサーバ認証をさせることで本物の信頼できるサイトであると誤認させ、個人情報や信用情報などを盗もうとした事例である。もっとも、今回の事例は、スイスのユーザを標的としてフランス語で書かれたサイトであり、また使われた SSL サーバ証明書の有効期限も切れているためブラウザから警告が出るケースである。したがって、日本人が本件に巻き込まれる可能性は低いといえる。

ただ、以前は SSL サーバ証明書を使ったフィッシングサイトは決して珍しいものでなかった。それというのも、SSL サーバ証明書発行の審査内容は CA によって、また Class によって異なるのに、ブラウザにはそれらの違いを区別して表示する機能はないため、審査の緩い SSL サーバ証明書を使ってフィッシングサイトを作ることができたためである。具体的には、DV SSL 証明書(Domain Validated Certificate)と呼ばれる、実在確認を行わないで発行される SSL サーバ証明書を利用するケースである。

本件の事象をここで取り上げた理由は、今後日本でも SSL を使ったフィッシングサイトが出現しないとは言い切れないためである。何よりも注意する必要があるのが、現在、甚大な被害が発生した東日本大震災への義援金募金サイトが国内外で数多く設立されていることであり、残念なことではあるが、そのなかにはフィッシングサイトと疑われるものが紛れ込んでいることである[6]。

警鐘の意味も込め、もしインターネット募金を考えているならば、せっかくの善意を無駄にせず、またフィッシングによる被害に遭わないためにも、信頼できる企業や団体の Web サーバを利用していただきたい。

その際、EV SSL サーバ証明書(Extended Validation Certificate)を利用した Web サイトであれば、実在する信頼できる企業や団体であると考えてよい。従来の SSL サーバ証明書の場合とは異なって、企業や団体の実在確認が規定されるなど、CA とブラウザベンダで構成する業界団体「CA/Browser フォーラム」によって策定された厳格な審査基準に沿って審査されたうえで EV SSL サーバ証明書が発行される。また、従来の SSL サーバ証明書と区別するために、EV SSL サーバ証明書を利用した Web サイトではブラウザの URL アドレスバーが緑色で表示され、一目で確認できるメリットもある。

従来の SSL サーバ証明書を利用している Web サーバであれば、ブラウザが警告表示しないことは絶対条件として、念のため URL と SSL サーバ証明書の発行 CA がどこであるかも検証し、十分に信頼できる Web サイトであることを確認していただきたい。

3. 暗号アルゴリズムの世代交代の最新動向

3.1 暗号アルゴリズム移行への最近の米国の動き

「暗号アルゴリズムの 2010 年問題」や「暗号アルゴリズムの世代交代」の出発点は、もともと 2005 年当時ハッシュ関数に対する攻撃が相次いでいた事を受けて、米国立標準技術研究所 NIST（National Institute of Standards and Technology)が発表した暗号アルゴリズムの移行計画が契機となっている。

具体的には、NIST は、2010 年末を期限として、米国政府システムで利用する暗号を当時主流であった暗号アルゴリズム（Triple DES, 1024 ビット RSA, SHA-1; 80 ビット安全性の暗号アルゴリズム）を次世代の暗号アルゴリズム（AES, 2048 ビット RSA, SHA-2 など; 112 ビット安全性以上の暗号アルゴリズム）に変更するためのガイドライン SP800-57 [7]を公表した。

2011 年 1 月 13 日、最近の暗号解読の進展状況を踏まえ、NIST は SP800-57 の移行計画を一部修正したガイドライン SP800-131A [8]を公表した。基本路線としては SP800-57 が引き続き移行計画のベースとなっているが、SP800-131A ではより詳細な移行方針が打ち出されている。

なお、SP800-131A は SP800-57 全体を無効にするものではなく、取り扱いの一部を変更するだけに過ぎないことに注意されたい。つまり、暗号アルゴリズム移行についての全体的な思想は今でも SP800-57 である。

SP800-57 と SP800-131A との具体的な違いは表 1～表 3 の通りである。

両者の違いの大きなポイントとしては、現時点での解読リスクをベースに移行期限を再評価した点と、使用形態の違いによる取り扱いを考慮した点にある。その結果、2010 年末までに運用を終了するとしていた 80 ビット安全性の暗号アルゴリズムについて、解読リスクを許容したうえで今後数年間（おおむね 2013 年末まで）継続利用を認めることになった。また、SHA-1 が継続利用できるアプリケーションの範囲が、SP800-57 では極めて限定的な取り扱いだったのに対し、SP800-131A では署名以外はすべて認められるようになった。

ちなみに、SP800-57 に従い、認証局の多くは 2010 年当初から 1024 ビット RSA を使った SSL サーバ証明書の発行を 2010 年末までに終了する旨のアナウンスを出していた。しかし、2013 年末までの継続利用が認められる方向性が打ち出された後は、予定を変更して、1024 ビット RSA を使った SSL サーバ証明書の発行を継続するところがほとんどである。現時点では、SP800-131A に従い、SSL サーバ証明書の有効期限が 2013 年末を越えないことを条件としているところが多い。

表 1: SP800-57 と SP800-131A での用語定義の違い

<table>
<tr><th>SP800-57</th><th>SP800-131A</th></tr>
<tr><td>Approved:
FIPS もしくは SP で承認された暗号アルゴリズム</td><td>Approved:
FIPS もしくは SP で承認された暗号アルゴリズム</td></tr>
<tr><td rowspan="5">Algorithm security lifetimes:
暗号アルゴリズムが安全に使えると考えられる残存期間で区分。区分分けの指標として等価安全性を利用。具体的には以下の通り。

80 ビット安全性：2010 年末まで
112 ビット安全性：2030 年末まで
128 ビット安全性：2030 年末以降も可

十分な安全性を保っているうちに新たな暗号アルゴリズムに移行するやり方であり、システムの運用期限から逆算して採用する暗号アルゴリズムを決める</td><td>Acceptable:
安全に使える（解読リスクが表面化していない）と考えられる暗号アルゴリズム</td></tr>
<tr><td>Deprecated:
ある程度の解読リスクはあるものの、短期的には（データ暗号化や署名生成にも）使ってもよいと考えられる暗号アルゴリズム</td></tr>
<tr><td>Restricted:
解読リスクを回避するために利用する際の制約条件を付けた上で、短期的には（データ暗号化にも）使ってもよいと考えられる暗号アルゴリズム</td></tr>
<tr><td>Legacy-use:
すでに暗号化された情報について処理(データ復号や署名検証)するためだけに利用する暗号アルゴリズム</td></tr>
<tr><td>Disallowed:
利用を禁止する暗号アルゴリズム</td></tr>
</table>

表 2: SP800-57 と SP800-131A での暗号アルゴリズム区分の違い

SP800-57（暗号アルゴリズム主体での区分）		SP800-131A（利用用途主体での区分）	
共通鍵暗号		暗号化	共通鍵暗号
		鍵配送	
		鍵生成関数(KDF)	
		メッセージ認証子(MAC)	
公開鍵暗号	素因数分解型	署名生成	公開鍵暗号
	離散対数型	署名検証	
	楕円曲線型	鍵交換	
		鍵配送	
ハッシュ関数	署名 ハッシュ利用アプリケーション	署名生成	ハッシュ関数
		署名検証	
		署名以外のアプリケーション	
	疑似乱数生成(RNG)	疑似乱数生成(RNG)	
	鍵生成関数(KDF)	鍵生成関数(KDF)	
	HMAC	メッセージ認証子(MAC)	

表 3: SP800-57 と SP800-131A での代表的な暗号アルゴリズムの取り扱いについて

	SP800-57	SP800-131A
2-key Triple DES	2010 年末まで	2010 年末まで Acceptable 2015 年末まで Restricted 2016 年以降は Legacy-use（復号以外の利用について Disallowed）
3-key Triple DES	2030 年末まで	Acceptable
AES	2030 年以降も利用可	Acceptable
1024 ビット RSA	2010 年末まで	2010 年末まで Acceptable 2013 年末まで Deprecated 2014 年 1 月以降は Legacy-use（署名検証以外の利用について Disallowed）
2048 ビット RSA	2030 年末まで	Acceptable
160 ビット ECDSA	2010 年末まで	2010 年末まで Acceptable 2013 年末まで Deprecated 2014 年 1 月以降は Legacy-use（署名検証以外の利用について Disallowed）
256 ビット ECDSA	2030 年以降も利用可	Acceptable
SHA-1	HMAC, KDF, RNG を除き、2010 年末まで HMAC, KDF, RNG については 2030 年以降も利用可	署名での利用に関して： 2010 年末まで Acceptable 2013 年末まで Deprecated 2014 年 1 月以降は Legacy-use（署名生成での利用について Disallowed）
		署名以外の利用に関して：Acceptable
SHA-256	2030 年以降も利用可	Acceptable

3.2 ハッシュ関数をめぐる最近の米国の動き

NIST は、2012 年末頃に新しい米国政府標準ハッシュ関数 SHA-3 を決めるためのコンペティションを進めている。2007 年 11 月から始まった公募、2008 年 12 月から始まった第 1 次評価、2009 年 9 月から始まった第 2 次評価を経て、2010 年 12 月 9 日に最終評価に臨む 5 つの最終候補が発表された。最終候補に選定されたハッシュ関数は以下のとおりである。

- BLAKE（産学連携型 – スイス、英国）
- Grøstl（大学連携型 – デンマーク、オーストリア）
- JH（国立研究所型 – シンガポール）
- Keccak（半導体企業連携型 – スイス、オランダ）
- Skein（産学連携型 – 米国、英国、ドイツ）

NIST が公表した最終候補の選考にあたっての判断レポート[9]によれば、選考基準として「安全性：少なくとも選定後 20 年以上安全性が維持できること」「処理性能：SHA-2 よりは処理性能が良いことは最低条件」「その他」を挙げており、その選考基準に従って上記 5 つのハッシュ関数を選定したことになっている。ちなみに、第 2 次評価対象となったハッシュ関数 14 個について、明確に安全性上の問題があったと判断されたものはなく、処理性能に関して IC カードのような制限された環境での性能やハードウェア性能で大きな差がついたとのことである。

ただ、この判断レポートをよく読むと、評価だけで判断しているのではなく、選考に当たっての NIST の考え方が色濃く影響していることが分かる。キーワードは“conservative（保守的）”である。

「選定後 20 年以上安全性を維持」したいとの考えからだと推測されるが、候補となっているハッシュ関数自体の安全性評価結果そのものもさることながら、そのハッシュ関数の設計思想に対する今までの研究成果の厚みも重要との立場を NIST はとっている。つまり、「性能が非常によいが従来にはない斬新な設計思想に基づくハッシュ関数」と「性能は飛びぬけていいわけではないが従来からある設計思想を踏襲しつつ改善されたハッシュ関数」とがあれば、同程度の安全性評価結果であるならば、性能が良い前者ではなく、安全性に信頼感のある後者をあえて選ぶということである。

この選定手法は、技術的に斬新な設計思想で非常に素晴らしいハッシュ関数を排除するリスクを持っている。一方で、斬新な設計思想である以上、単に研究がされていないので脆弱性が露見していないだけかもしれないという潜在的なリスクがある。両者のリスクを考えた際、NIST は米国政府標準暗号アルゴリズムの安定性の観点から、後者のリスクのほうが大きいと判断していると考えられる。その意味では、暗号学会からあまり注目されず安全性評価結果が少ないと判断されたハッシュ関数も選考対象外となる。

ところで、最近、NIST はハッシュ関数の取り扱いについてスタンスを変えつつあるのではないかと思わせる動きを見せている。

もともと SHA-3 コンペティションを始める動機にもなったのが、2005 年当時は SHA-1 をはじめとしたハッシュ関数に対する攻撃が相次いでいたこともあり、同じ設計思想で作られている SHA-2 ファミリーに対しても安全性について疑いの目が向けられたことである。つまり、「SHA-2 ファミリーとは異なる設計思想のハッシュ関数を作るべきではないか」という意見が暗号学会を中心に広まったことが契機となった。

しかし、それから 5 年以上が経過したものの、SHA-2 ファミリーはおろか、SHA-1 についても 2005 年当時に想定されたような安全性低下は見られず、実際 SHA-1 の衝突が見つかったという報告もない。このことが、安全性に関する研究成果の厚みという点で、SHA-2 ファミリーの安全性に問題がないので

はないかとの NIST の判断に変わってきているのではないかと推測される。

これまで、SHA-2 ファミリーは SHA-3 ができるまでのワンポイントリリーフ的な扱いになるかもしれないという意見が少なからずあった。しかし、現在の NIST の動きを見る限りは、AES が DES/Triple DES の代替方式という明確な位置づけを与えられていたのとは異なり、むしろ SHA-2 ファミリーのほうこそ今後の本命であり、SHA-3 は SHA-2 の代替どころか補完もしくはバックアップとして位置づけるように見直してきている節がある。

事実、NIST は、SHA-3 コンペティションを計画通り進める一方で SHA-2 の拡充にも乗り出し、2011 年 2 月 11 日、新しい SHA-2 ファミリーとして SHA-512/224 と SHA-512/256 のドラフトを公開した[10]。これらは、簡単に言うと、SHA-2 ファミリーの一つである SHA-384 と同じ考え方で作られたアルゴリズムで、SHA-512 をベースに計算したのちハッシュ長としてそれぞれ 224 ビット、256 ビットに切り出すハッシュ関数である。

SHA-224 や SHA-256 は 32 ビット CPU で高速に演算できるように作られているのに対し、SHA-512 は 64 ビット CPU で高速に演算できるように作られている。その SHA-512 を使って 224 ビットや 256 ビットのハッシュ関数を新たに作るということは、最近数を増やしつつある 64 ビット CPU 向けに SHA-2 ファミリーが使える環境を拡充することを意味している。

参考文献

[1] Comodo Report of Incident, http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

[2] ITmedia, 不正 SSL 証明書の発行事件で「犯人」が手口公表,
http://www.itmedia.co.jp/news/articles/1103/29/news017.html

[3] マイクロソフトセキュリティ アドバイザリ (2524375) ,
http://www.microsoft.com/japan/technet/security/advisory/2524375.mspx

[4] Mozilla Foundation Security Advisory 2011-11,
http://www.mozilla.org/security/announce/2011/mfsa2011-11.html

[5] Symantec, Mass Phishing on Credit Card Services Brand Using Fake SSL,
http://www.symantec.com/connect/ja/blogs/mass-phishing-credit-card-services-brand-using-fake-ssl

[6] フィッシング対策協議会、日本赤十字社を騙るフィッシング、http://www.antiphishing.jp/

[7] NIST, SP800-57 Recommendation for Key Management – Part 1: General

[8] NIST, SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

[9] NIST, Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition

[10] NIST, DRAFT FIPS PUB 180-4 Secure Hash Standard (SHS)