資料３－２

2008-3-5

「電子署名及び認証業務に関する法律の施行状況に係る検討会」
への回答

暗号技術検討会

「電子署名及び認証業務に関する法律の施行状況に係る検討会」（以下「電子署名法検討会」という。）への回答は、以下のとおりである。

初めに、

二　RSA1024bit については、概ね 2015 年前後以降に、危殆化のおそれが高まってくることが示されていること。

についての見解を述べる。

【暗号技術検討会としての見解】

RSA 暗号の安全性の根拠は、2 つの大きな素数の積である「モジュラス」だけが与えられたとき、元の 2 つの素数が容易に計算できないこと（一方向性が確保されていること）である。言い換えれば、与えられた「モジュラス」が容易には素因数分解できないこと（素因数分解問題の困難性）が求められている。

素因数分解問題は、過去から活発に研究活動が行われており、近年では「一般数体ふるい法」等の新しい知見も得られているところである。

暗号技術検討会としても、公開鍵暗号の安全性の根拠となる素因数分解問題の動向には、関心を払っており、昨年度（2006 年度）には、下位組織の暗号技術監視委員会にて、監視活動の一環として、1024 ビットの「モジュラス」の素因数分解に対する予測を行ったところである。

暗号技術監視委員会では、素因数分解が所定の時間内に可能になるものと推測される時期について、以下のような前提の下に検討を行った。

１．n=pq 型素因数分解問題の攻撃に必要な計算量に関する前提

前提 1: ふるい処理の計算量見積もりについては、CRYPTREC REPORT 2006 暗号技術監視委員会報告書 14 ページ表 2.4 の値（以下のとおり）を採用する。

表 2.4　ふるい処理時間の推測（単位は、AMD Athlon 64 2.2GHz x 年）

法パラメータのサイズ（ビット）／ふるい処理のパラメータ選択の最適さ	768	1024	1536	2048
実メモリに制約（2GB RAM）がある場合の見積もり	1108	8.4×10^{6}	4.5×10^{12}	25×10^{16}
ふるい処理に関するパラメータ選択をより改善した場合の見積もり	-	2.8×10^{6}	0.92×10^{12}	4.4×10^{16}
実メモリにそれほど制約がない場合の見積もり	-	1.05×10^{6}	0.18×10^{12}	0.4×10^{16}

前提 2: 素因数分解のアルゴリズムに関しては、これから 30 年間はブレークスルーがなく、一般数体ふるい法よりも効率の良いアルゴリズムが発見されないものとする。また、アルゴリズム等の大きな改良もないものとする。つまり、計算機性能の向上による計算能力の増大が、安全性を脅かす主な要因とみなす。

前提 3: ふるい処理の計算が 1 年間で処理し終えることをもって、素因数分解が完了したものとみなす。漸近的な実行時間の評価において、ふるい処理と線形代数処理は同じオーダーであること、一般数体ふるい法により分解された合成数の世界記録において、これまでのところふるい処理の方が線形代数処理より多くの時間を要していることから、このように仮定した。

２．計算機性能の将来予測に関する前提

前提 4: 計算機性能の将来予測に関しては、スーパーコンピュータのベンチマーク結果の 1 位から 500 位を 1993 年から半年毎に集計している Web サイト TOP500.org に過去掲載された計算機における FLOPS(ピーク性能)の統計値を外挿することにより算出する。これを取り上げたのは、このような情報を収集している場所が他にはなく、実際に構築されたスーパーコンピュータのうち、高性能なものの代表として相応しいと考えられるからである。

前提 5: 近年の汎用 CPU 及びスーパーコンピュータにおける整数演算性能と浮動小数点演算性能については、ほぼ同等（1 対 1）であるとした。

３．計算量の換算に関する前提

前提 6: 一般数体ふるい法の処理は専ら CPU の整数演算を用いるものなので、計算能力の比較には、整数演算性能を用いるのが適当であるが、前提 5 によ

り、CPU における浮動小数点演算性能への換算を行った。

前提 7: 基準点として用いる Athlon 64(2.2 GHz)の FLOPS(ピーク性能)値は、(クロック周波数)x(浮動小数点演算ユニット数)によって見積もる。Athlon64(2.2 GHz)の場合は、4.4 GFLOPS である。

このような前提の下、将来獲得されると予測される計算処理能力の推移と n=pq 型素因数分解問題を用いた攻撃に必要な計算量の関係をグラフにすると、図１のようになる。

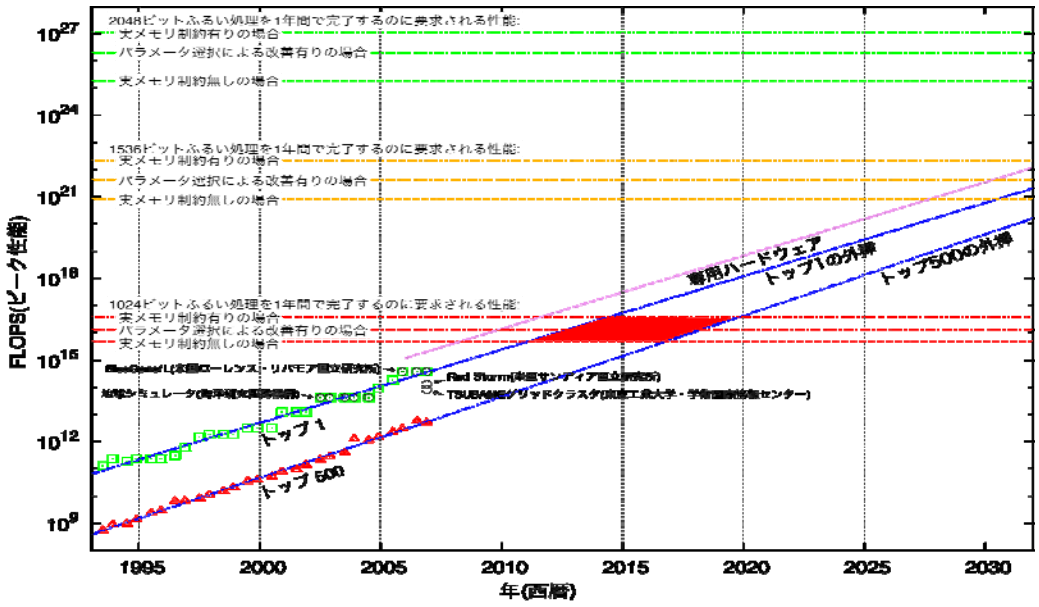

図１　1 年間でふるい処理を完了するのに要求される処理性能の予測

図１において、横軸は時間軸（年）であり、縦軸は計算機の性能（FLOPS）である。

想定する計算量としては、使用できる実メモリの量に制約がない場合（最下位の赤破線)、使用できる実メモリの量が現実的な制約（数 GB 程度）を受ける場合（最上位の赤破線)、使用できる実メモリ量を一般数対ふるい法のパラメータで最適化した場合（中位の赤破線）であり、斜線は、世界最高性能の計算機（トップ１）と性能はやや低下するもののより入手しやすい計算機（トップ 500）の計算能力の向上を推測した結果を示している。この実メモリ制約がある場合の計算量と、制約のない場合の計算量およびトップ１の計算機性能予測、トップ５００の計算機性能予測で囲まれた中央の赤い菱形部分が、1024bit の素因数分解に成功するであろう危険領域を示している。

より現実的な、実メモリに制約がある場合において、世界最高性能の計算機（トップ１）であれば、2015 年前後に 1024bit のモジュラスの素因数分解に成功すると想定され、やや入手しやすいトップ 500 位レベルの計算機環境であれば、2020 年頃までには素因数分解に成功すると予測できる。

したがって、暗号技術検討会としては、「二　RSA-1024 bit については、概ね 2015 年前後以降に、危殆化のおそれが高まってくることが示されていること。」との見解が妥当なものであると考える。

次に、

一　SHA-1 については、国内最高速のスーパーコンピュータを用いれば 462 年以下で衝突発見されるおそれがあることが 2007 年春に示されているが、今後コンピュータの計算処理能力の向上だけでなく、新たな攻撃手法が発見されることによって、危殆化までの時間が格段に短縮されるおそれがあること。

についての見解を述べる。

【暗号技術検討会としての見解】

SHA-1 の安全性に関する暗号技術検討会としての見解は、平成 18 年 6 月 28 日付、暗号技術監視委員会による「SHA-1 の安全性に関する見解」（別添参照のこと）のとおりであるが、改めて将来獲得されると予測される計算機の計算処理能力の推移と SHA-1 の実行に必要な計算量の関係をグラフにすると、以下の図２のようになる。

なお、SHA-1 の実行に必要な時間の推測に関しては、623 cycles/blockを参考とした[1]。また、計算機性能の将来予測に関する前提はRSA-1024 bitの危殆化に関する見解で既に述べたとおりである。

図２において、横軸は時間軸（年）であり、縦軸は計算機の性能（FLOPS）である。

想定する計算量として、赤波線のうち上位の線が2^{69}回のSHA-1の実行回数を、同じく下位の線が2^{63}回のSHA-1の実行回数を１年間で完了するのに要求される性能を示している。

斜線は、世界最高性能の計算機（トップ１）とやや入手しやすい計算機（トップ500）の計算能力の向上を推測した結果である。

2^{69}回の SHA-1 の実行回数については、世界トップ１の計算機環境で 2012～13 年頃、トップ 500 位レベルの計算機環境であれば、2020 年頃までには衝突発

[1] Parallel Implementations of Dedicated Hash Functions, J.Nakajima,　M.Matsui, pp.165-180, EUROCRYPT 2002

見が現実のものとなると予測できる。

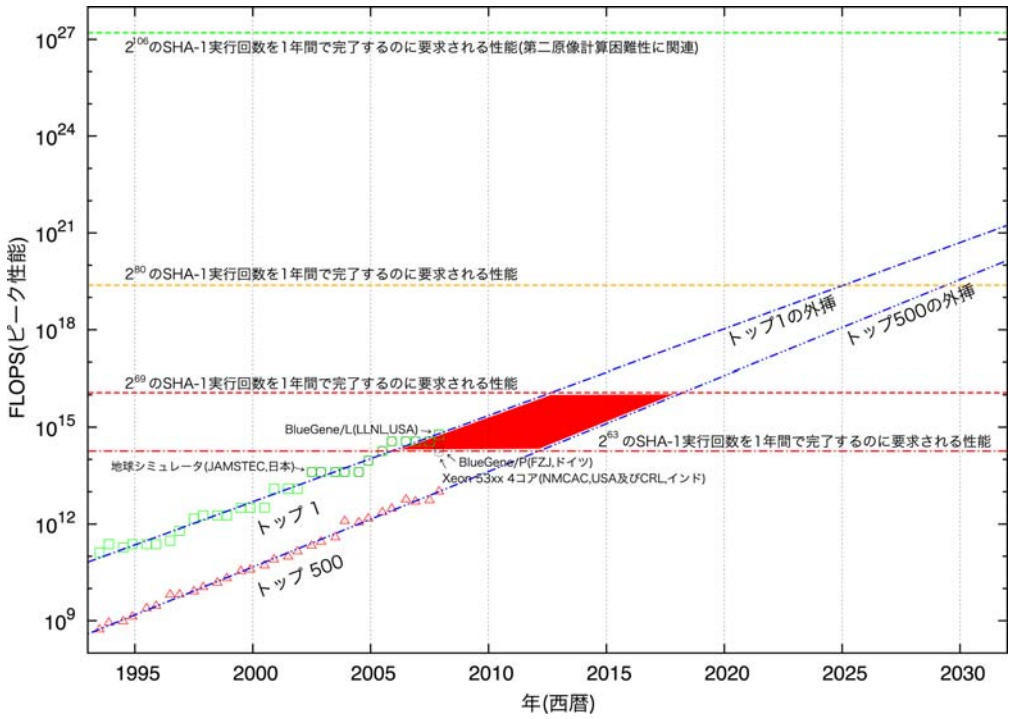

図２　SHA-1 の実行回数と計算機の処理性能の関係

しかしながら、２^{63}回の SHA-1 の実行回数で衝突が発見されることとなれば、世界トップ 500 の計算機環境で 2012～13 年頃、世界トップ１の計算機環境であれば、現在、既に 1 年間計算すれば衝突が発見できてしまうことになる。また、２^{63}回よりもさらに少ない実行回数で衝突が発見される可能性も否定できない。

したがって、署名利用者が使用する電子文書に対する署名アルゴリズムについては、2015 年前後以降に衝突計算攻撃が現実的なものになると考えられるので、暗号技術検討会としては、

「一　SHA-1 については、国内最高速のスーパーコンピュータを用いれば 462 年以下で衝突発見されるおそれがあることが 2007 年春に示されているが、今後コンピュータの計算処理能力の向上だけでなく、新たな攻撃手法が発見されることによって、危殆化までの時間が格段に短縮されるおそれがあること。」との見解が妥当なものであると考える。

なお、直接的な脅威となるSHA-1 の第二原像計算困難性[2]に関しては、現時点ではまだ脅威となる攻撃手法は発見されていない。これは、衝突発見によって同じハッシュ値を持つ異なる電子文書の生成可能性はあるものの、任意の文書

[2] 既に与えられているデータとそのダイジェスト値に対して、別のデータで同じダイジェスト値を生成する計算困難性

を作成できる訳ではないことを意味している。ただし、電子署名者による否認を防止するためには、衝突計算攻撃による脅威も考慮する必要があり、電子署名法報告書案にはその旨必要に応じて説明を加えることが適切である。

（別添）

SHA-1 の安全性に関する見解

平成 18 年６月 28 日
暗号技術監視委員会

電子政府における情報セキュリティ確保のために、各府省の情報システム構築において暗号を利用する場合には、「各府省の情報システム調達における暗号の利用方針」（平成 15 年 2 月 28 日 行政情報システム関係課長連絡会議了承）において、必要とされる安全性・信頼性などに応じ、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとされている。
また、情報セキュリティ政策会議から出された「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版（全体版初版））」（平成 17 年 12 月 13 日）においても、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択することが基本遵守事項として明記されている。

電子政府推奨暗号リストでは、ハッシュ関数の SHA-1 は注釈において、『（注 6）新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。』と規定している。

SHA-1については、最近の研究動向によれば、Wangらにより2^{69}回以下のSHA-1の実行回数で同じハッシュ値を持つ2つのメッセージが発見できる衝突探索攻撃アルゴリズムが発表され、CRYPTRECで検証した結果、2^{69}回のSHA-1の実行回数で衝突発見できることの妥当性は検証された。また、近い将来に2^{63}回以下のSHA-1の実行回数で衝突発見できることも妥当性があるとの結論を得た。このことは、SHA-1を長期間にわたって利用する電子署名やタイムスタンプなどは、近い将来にSHA-1の衝突発見が現実的な問題に発展する可能性を示唆している。
このようなことから、電子署名やタイムスタンプのように長期間にわたって利用するシステムでは、新規（更新を含む）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、SHA-256 ビット以上のハッシュ関数の使用を薦める。

＊参照：CRYPTREC Report 2005「暗号技術監視委員会報告」
http://cryptrec.jp/

（参考）

各種文献等を踏まえ、以下の参考情報を提供する。ただし、CRYPTREC として、ここで引用した文献等の内容の正確性、信頼性、妥当性を保証するものではない。

ハッシュ関数のSHA-1 を利用している電子署名システムにおいて、仮に 2^{63}回のSHA-1の実行回数で衝突が起こるということになれば、例えば、一般に用いられているCPUで構成される「PCクラスタ型」[i]のスーパーコンピュータのうち 2006 年 4 月現在で国内最高速のもの[ii]を使用して約 7 年間計算すると、同じハッシュ値を生成する異なる文書などが作成できる可能性がある。

具体的には、電子署名された原文と同一の電子署名を生成できる別の文書が作成（偽造）され得るということであり、電子署名された文書（原文）の真がんの判断ができなくなるおそれがある。

現時点では、電子署名された文書の有効性に疑問は生じていないが、SHA-1 の衝突に関する最近の研究結果は、今後、暗号研究の進歩やコンピュータ処理能力の向上[iii]などによって、文書の有効期間が本来よりも著しく短縮され、電子署名された文書であっても、否認、なりすまし又は改ざんといった脅威にさらされる危険性があることを示唆している。

衝突発見に要する時間の目安（推定）

SHA-1 の実行回数	2006 年 4 月現在
2^{69}回	・国内最高速のスパコンで約 462 年以下
2^{63}回	・国内最高速のスパコンで約 7 年以下

処理時間については、計算アルゴリズムや計算機のアーキテクチャなどに依存して大きく変わり得るため、この年数はあくまで推定である。なお、今後の進歩によっては、スーパーコンピュータだけではなく、インターネットを利用して世界中の国々で分散処理を行う分散コンピューティングシステム[iv]によっても、本推定以上の衝突発見能力を実現できる可能性がある。

---

[i]クラスタとは、複数のコンピュータをネットワークを介して相互に接続して統合し、より高い性能を求めたコンピュータ・システムのこと。

[ii]東京工業大学 学術国際情報センター スーパーコンピューティング・グリッドシステム「TSUBAME (Tokyo-tech Supercomputer and UBiquitously Accessible Mass-storage Environment)」(http://www.gsic.titech.ac.jp/Japanese/Publication/pressrelease04032006.html.ja)

[iii]たとえば、ムーアの法則(http://www.intel.co.jp/jp/developer/technology/silicon/mooreslaw/index.htm)など。

[iv]たとえば、distributed.net(http://distributed.net/)など。