暗号の安全性評価

盛合 志帆（もりあい しほ）
ネットワークセキュリティ研究所　セキュリティ基盤研究室長

1993年大学卒業。日本電信電話（株）、ソニー（株）を経て2012年、NICTに入所。
暗号技術の設計および安全性評価に関する研究や国際標準化に従事。博士（工学）。

暗号の安全性評価の重要性

ネットワークの発展にともない、暗号技術は現代社会の根幹を支える技術となっています。暗号技術は、インターネットや携帯電話における通信の秘密保持のみならず、鉄道の自動改札システム、高速道路の自動料金収受システム、電子書籍などのコンテンツ配信、ブルーレイディスクの著作権保護、ICチップによるパスポート偽造防止などに用いられており、もはや暗号技術なしでは通信・交通・ビジネスの安全・安心な運用は考えられないと言っても過言ではないでしょう。

しかしながら、現在、社会で広く使われている暗号技術は、一度安全性が確認されれば永遠に安全であるというわけではなく、暗号解読技術の進歩により急激な安全性の低下が起こることもあります。このため、NICTネットワークセキュリティ研究所 セキュリティ基盤研究室では、日々進歩する暗号解読技術や計算機性能の向上を考慮に入れ、継続的に暗号技術の安全性評価の研究を行っています。

暗号の安全性指標

「暗号の安全性を評価する」とはいったいどのようにすればよいのでしょうか。暗号の安全性は、その暗号を最も効率のよいアルゴリズムで解読したときに必要な計算量を指標として定義されています。ある暗号の解読計算量が2^kのオーダーであった場合、その暗号の安全性はkビットセキュリティであるといいます。例えば、暗号Aが2^{112}回の復号演算処理で鍵が見つかる場合、暗号Aの安全性は 112ビットセキュリティとなります（図1）。暗号の安全性を評価するには、最も効率のよい解読アルゴリズムを見つけ、その方法で解読にどれくらいの手間が必要かを見積もればよいということになります。

米国標準技術研究所（National Institute of Standards and Technology: NIST）では暗号解読技術の進歩や計算機性能の向上を考慮に入れ、米国の政府調達において、何年にどれくらいのセキュリティレベルをもつ暗号技術を利用すべきかの指針を出しています。図2に2007年にNISTが発表した推奨鍵長・パラメータを示します。これによると、2011年以降は最低112ビットセキュリティの安全性指標をもつ暗号技術を利用すべきであり、このレベルと等価な共通鍵暗号は鍵長112ビット、RSAなど素因数分解問題に基づく公開鍵暗

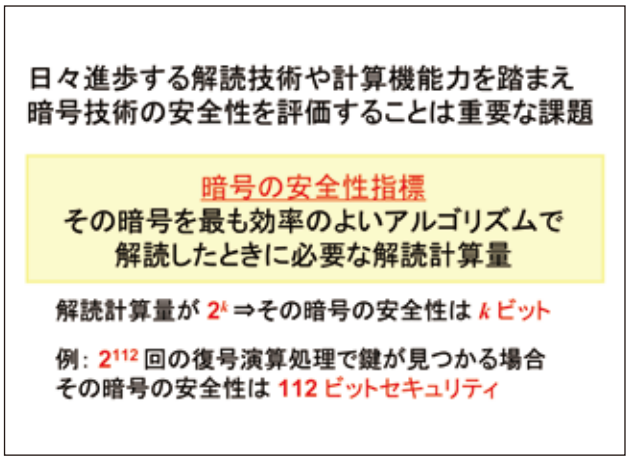

図1　暗号の安全性評価

		安全性指標に相当する鍵長・パラメータ（bit）				
		～2010年	2011～2030年	2031年～	2031年～	2031年～
暗号の安全性指標		80 bit セキュリティ	112 bit セキュリティ	128 bit セキュリティ	192 bit セキュリティ	256 bit セキュリティ
共通鍵暗号（AESなど）		80	112	128	192	256
公開鍵暗号 デジタル署名	素因数分解問題に基づく方式（RSAなど）	1024	2048	3072	7680	15360
	離散対数問題に基づく方式（DSA, DHなど）	1024	2048	3072	7680	15360
	楕円曲線上の離散対数問題に基づく方式（ECDSA, ECDHなど）	160	224	256	384	512
ハッシュ関数（SHA-2など）		160	224	256	384	512

Recommendation for Key Management - Part 1: General (Revised), NIST SP 800-57, 2007.

図2　暗号の安全性指標

号は鍵長2048ビット、DSAなど離散対数問題に基づく公開鍵暗号は鍵長2048ビット、ECDSAなど楕円曲線上の離散対数問題に基づく公開鍵暗号は鍵長224ビット、ハッシュ関数はハッシュ長224ビットであることが示されています。なお、この指標は漸近的な計算量評価に基づきNISTが2007年に示したものであり、日々進歩する技術や実際の計算機実験による評価結果に基づいて変わっていきます。また、NIST以外のいくつかの国の研究機関等も指針を出しており、NISTとは異なる推奨鍵長・パラメータを示しているところもあります。

セキュリティ基盤研究室でのこれまでの成果

セキュリティ基盤研究室でこれまで行ってきた暗号の安全性評価の1つに、現在最も広く使われている公開鍵暗号であるRSA暗号や楕円曲線暗号の評価があります。特に、1024ビットRSA暗号の解読は従来考えられていたよりも容易で、現在では、スーパーコンピュータ京を使うと1年程度で解けてしまうという評価を得ています（図3）。この評価結果は、我が国の電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトであるCRYPTREC（Cryptography Research and Evaluation Committees）を通じて公開され、誰もが参照できるようになっています。当研究室では、電子政府推奨暗号リストの改訂のための暗号の安全性評価やCRYPTRECの事務局運営の面で貢献を行っています。詳細は本号p6で紹介します。

また、現在使われている暗号技術にとどまらず、クラウドコンピューティングにおいて、他に内容を一切知らせることなく計算作業などを託することができるよう、データを暗号化したまま種々のデータ処理を行うことが可能な次世代暗号の安全性評価も行っています。次世代暗号においてどのようなパラメータを選択すれば安全に利用できるかがわかるので、次世代暗号の実用化や標準化に役立ちます。次世代暗号の安全性評価に関して、当研究室では、これまでに、高度なプライバシ保護機能を実現する「ペアリング暗号」の解読で世界記録を達成しました（NICT NEWS 2012年9月号に掲載）。また、格子暗号の安全性評価でも世界記録を達成しております。詳細は本号p3-5で紹介します。

NICTが行っている暗号の安全性の評価結果は、我が国の電子政府システムをはじめ、世界中で広く利用されている暗号技術を安全に利用する際の適切な鍵長やパラメータを選択するための技術的根拠を与えており、極めて重要な貢献となっています。

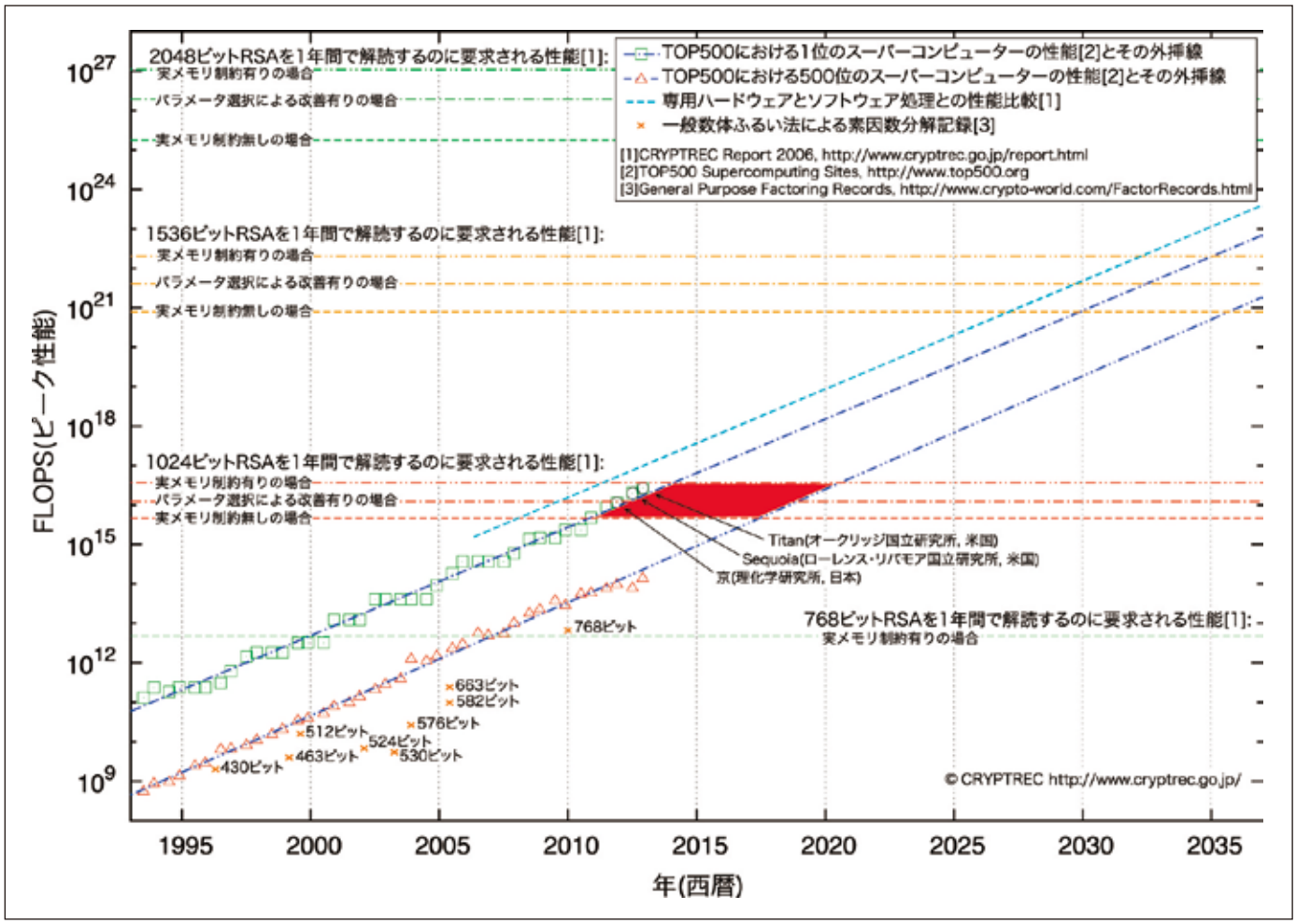

図3　RSA暗号の安全性評価

縦軸は計算機能力を表し、グラフの水平破線は下から順に768ビット、1024ビット、1536ビット、2048ビットのRSAを1年間で解読するのに要求される性能を示している。但し、この性能は実メモリ制約の有無により幅があり、例えば同じ1024ビットRSAについて複数の破線で表されている。一方、グラフの左下から右上にのびる線は年とともに推移する計算機性能の向上を示しており、スーパーコンピュータの演算処理速度のランキング上位500位を発表する「TOP500」における1位（□）および500位（△）のスーパーコンピュータの性能とその外挿線となっている。こちらも1位と500位で性能に幅がある。この水平線と斜め線が交わるところが赤く塗られているが、これが1024ビットRSAがスーパーコンピュータを用いて1年で解読される時期を表している。2013年現在、1024ビットRSAがスーパーコンピュータを用いて1年で解読される時期に入って来たことがわかる。