情報セキュリティ歳時記 12

暗号に関する輸出規制

前川　徹
早稲田大学 国際情報通信研究センター

➲ 大幅に緩和された暗号輸出規制

1999年9月に米大統領府が暗号技術に関する規制をさらに緩和すると発表してから4カ月，米商務省は2000年1月12日，ようやく新しい暗号技術輸出規制を発表した．これは暗号技術や暗号製品の輸出規制を大幅に緩和するもので，長い間，IT（Information Technology）業界が待ち望んでいたものである．これによって実質的に暗号技術に関する米国の輸出規制はほとんど撤廃されたことになる．

この新しい規制によれば，米国企業は，その製品の技術審査を一度受ければ，米輸出管理局のライセンスがなくても，キューバ，イラン，イラクなど7カ国を除く全世界の一般企業，個人，非政府ユーザに暗号製品を輸出でき，市場に広く出回っている暗号製品であれば，外国政府を含むすべてのユーザに対して輸出できる．暗号アルゴリズムや鍵長による制限はまったくない．また，一般に入手可能な暗号ソフトウェアのソースコードについては，ライセンスも技術審査も不要で，輸出管理局にソースコードそのものか，ソースコードが公開されているインターネット上のアドレスを届ければよくなった．

暗号に関する規制の全面撤廃を訴えている市民団体の中には，まだ完全な勝利ではないという声もあるが，米国のIT企業のほとんどは，この規制緩和を歓迎していると伝えられている．将来，逆に規制が強化される可能性は否定できないが，おそらくこれが暗号輸出規制に関する長い論争の終着点になるのではないだろうか．

➲ 米国はなぜ暗号輸出を規制してきたのか

1995年8月まで米国は暗号技術について厳しい輸出規制を行ってきた．当時は，共通鍵暗号の場合，鍵長が40ビットを超える暗号については，原則輸出禁止であった．それは，強い暗号技術が世界中に広まると，一部の連邦政府機関が行っている諜報活動が制約を受けることになり，国家安全保障に悪影響すると言われてきたからである．つまり，世界中の電波を傍受して国家安全保障に関する情報を収集している国防総省傘下のNSA（National Security Agency）は，鍵長が40ビットを超える強い暗号が利用されるようになると，暗号化された通信内容を有効な時間内に解読することが一層困難になり，その情報収集能力が大幅に落ちてしまうことを懸念していたのである．

少し話はそれるが，暗号の強度はアルゴリズムと鍵の長さで決まる．共通鍵暗号を例にして簡単に説明しよう．共通鍵暗号を解読する方法として，さまざまな方法が提案されているが，暗号アルゴリズムに関する情報以外を持たない第三者にとって一番現実的な解読方法は，可能性のある鍵を片っ端から試してみるというbrute-force exhaustive searchと呼ばれる方法である（「線形解読法」や「差分解読法」などは相当量の情報を持っていることが前提になっている）．この方法では，最大2の「鍵の長さ」乗の試行が必要とされる．1970年代に連邦政府の暗号標準として採用されたDES（Data Encryption Standard）を例として考えれば，鍵長が56ビットなので，「2の56乗」回以内で解読できることになる．期待値はこの半分なので，平均的に「2の55乗」回（約3.6京回）でDESが破れるという計算になる．1秒間に10万回の試行が可能と仮定しても1万年かかる計算になり，素人目には安全なように見える．しかし情報技術の進歩により，もはやDESは安全ではないというのが定説である．実際に1999年1月にはわずか22時間15分で解読されている．

➲ 米国の暗号政策の変遷

DESの安全性が疑わしくなることを予期していた連邦政府は，1993年に悪名高い「クリッパーチップ計画」を発表した．暗号アルゴリズムにはSkipJackという80ビット長の共通鍵暗号が使用され，鍵を政府に預けさせるというKey Escrowという仕組みがチップに組み込まれた．ホワイトハウスから発表されたプレス資料によれば，クリッパーチップの民間における採用は任意であった．しかし，市民団体や情報産業界は，政府による通信監視につながる懸念があることや新しい暗号の信頼性に問題があることなどを理由として，激しい反対運動を繰り広げた．

こうしたクリッパーチップへの批判が続く中，連邦政府は1995年8月に最初の暗号技術に関する輸出規制緩和策を発表した．これは，政府が定めたキー・エスクロー基準を満たせば鍵長が64ビットまでの暗号技術製品の輸出が可能になるというものであった．

さらに連邦政府は1996年3月，新しく「キー・リカバリー・システム（KRS）」の整備（あるいは整備計画の推進）を条件にした規制緩和策を発表した．KRSとは，復号に必要な鍵を紛失に備えて信頼できる第三者に預けておく仕組みである．しかし，当事者が鍵を紛失した場合に鍵を回復できるということは，司法当局が（裁判所の許可を得た上で）合法的に復号鍵を入手できるということでもある．したがって政府が新しく打ち出した「キー・リカバリー」という概念は，従来の「キー・エスクロー」と本質は変わっていないという批判を浴びることになった．

結局，連邦政府はKRS構想を半ばあきらめ，1998年7月，9月と連続して新たな規制緩和策を発表した．まず7月に発表された規制緩和策によって，主な先進国をほとんど含む45カ国の金融機関が電子取引のために利用する場合は，鍵長や暗号方式，KRS機能の有無にかかわらず，技術審査を一度受ければ，以降はライセンスなしで輸出できることになった．ついで9月の規制緩和策は，7月に発表した緩和策を金融機関以外の保険会社，医療機関，オンライン通販会社に拡大すると同時に，56ビットのDESおよび同等の暗号製品については，イラン，イラク，リビアなどの7カ国を除き，1回技術審査を受ければ以降はライセンスなしで輸出できることになった．

➲ 暗号規制は有効なのか

暗号技術に関する規制緩和に反対してきた連邦政府機関はNSAだけではない．米国内の重大犯罪の捜査を担当しているFBI（Federal Bureau of Investigation）は，国内の犯罪捜査のために米国内における暗号技術の利用も規制すべきであると主張してきた．つまり組織的犯罪者が通信などに強力な暗号を利用していると捜査に支障が生じ，国民の安全を守れないというのである．しかし暗号技術は武器等に該当するという解釈によって武器等の輸出規制を適用してきた輸出と異なり，国内利用を規制するためには新たな立法が必要となる．これに対して，プライバシー保護や言論の自由に高い関心を持つ市民団体等は，強く反発してきた．実際に連邦政府内では暗号技術の国内利用を規制しようという法案が何度も検討され連邦議会に提案されてきたが，毎回廃案になってきた．

暗号を規制すべきか，すべきでないかの議論はさておき，果たして暗号の規制は可能なのだろうか．仮に政府が暗号の利用まで規制したとして，その規制は有効に働くだろうか．国境のないインターネットによって，地球の裏側からでもディジタル・コンテンツが簡単に入手できることを考えると，暗号規制は全世界で歩調を合わせて行わないと有効にはならない．仮にそれが可能であったとしても，すでにインターネット上に存在する高度な暗号プログラムの流通と利用を規制できるだろうか．正直者の市民は規制に従ったとしても，組織的犯罪者やテロリストが強力な暗号を利用することを止められるだろうか．

1997年10月に欧州理事会（European Commission）が発表したレポートは「インターネット上にある強力な暗号ソフトへのアクセスを効果的に阻むことは不可能である」と指摘し，「暗号の利用を制限すれば，法律を遵守している企業・市民から自衛手段を奪うことになりかねず，しかもそうした制限を行ったからといって，犯罪者の（強力な）暗号利用を完全に阻止できるものでもない」と述べている．

米国政府が，暗号規制に関する長い論争の果てに，ほとんど規制を撤廃するような結論を出した理由は，ここにあるのではないだろうか．

➲ 日本における暗号輸出規制

米国と同様，多くの先進国も暗号技術の輸出を規制している．その輸出規制の基本になっているのがワッセナー・アレンジメントであり，日本の暗号輸出規制の内容もこれを基本としている．ワッセナー・アレンジメントは，1996年7月に発足した輸出管理に関する国際的な枠組みで，地域の安定を損なうおそれのある通常兵器とその関連製品の輸出管理を目的としており，現在33カ国が参加している．

1998年12月2，3日に開催されたワッセナー・アレンジメントの総会において，暗号技術製品については，大幅な規制緩和を行う一方，2年間の期限付きではあるものの，64ビット超の大衆市場製品を新たに規制の対象とするという新しい合意が行われた．この合意によれば，まず56ビット以下の共通鍵暗号，512ビット以下のRSA暗号，112ビット以下の楕円暗号は規制の対象外となる一方，従来は規制の対象外とされてきた「店頭等で入手可能な64ビット超の暗号ソフトウェア」が規制の対象とされることになった．この決定を受けて，日本でも関連法令の改正が行われ，1999年6月に施行されている．

この項の最初で取り上げた米国の輸出規制緩和は，このワッセナー・アレンジメントにおける決定以上の大幅な緩和である．今回の米国の決定が，このワッセナー・アレンジメントにどのような影響を与えるのかはよく分からないが，日本の規制も米国並みに緩和されることを期待したい．

今月の参考文献等
1) Commerce Announces Streamlined Encryption Export Regulations: Department of Commerce, http://204.193.246.62/public.nsf/docs/60D6B47456BB389F852568640078B6C0
2) 前川　徹: 米国の暗号政策をめぐる論争を考える, 情報処理, Vol.40, No.6, pp.600-605 (June 1999).
3) 近藤賢二: 国際合意と我が国の新たな暗号輸出規制, 情報処理, Vol.40, No.6, pp.606-609 (June 1999).

（平成12年1月17日受付）