暗号規制の歴史

平井進

規制する目的

政府・軍当局の暗号通信が敵対勢力に解読されないようにする。
敵対勢力が政府・軍当局に解読できない暗号通信を行う能力を持たせないようにする。

規制に関する政策的対立

政府が管理したい通信に関しては暗号の使用を規制すべきという姿勢となる。
一方、国民の情報の電子的なやりとりを正しくするには暗号化して保護するしかない。アメリカでも国民が使用すべき安全な暗号規格を政府が推奨している（DES、AES）。

何故、輸出を規制するのか

フランス、中国では公安の取締のために国内での暗号使用を規制している。公安当局の目的からすれば国内を規制したい意向がある。
しかし、一般の先進国では平時に国内通信を規制すべき法的な根拠に問題があるのであろう。輸出についてはココム以来の伝統により規制できる権限がある。また、アメリカは輸出規制を外交政策に用いている面もある。
一般的に、先進国向けに比べてその他の地域への輸出の方が規制が強い。

CoCom と Wassenaar の規制の変遷

1991 年９月のコア・リストは従来の規制体系を一新したものである[1]。5.A.2.で暗号技術はすべて規制し、Note においてスマートカード、固定式、特定加入者 TV 放送の復号、携帯電話(使用者が携帯して輸出する場合)、コピー防止されたソフトウェアの復号等の機能が除外された（これらの用途による除外規定は 1998 年に Decontrol Note となる）。
（1994 年 3 月にココムが終了し、1996 年 9 月に新たに Wassenaar Arrangement が発足した。）
(1996 年 8 月に日本の暗号開発の件がアメリカで報道され[2]、日本で突然、暗号規制が厳しく運用され、上記で除外されている製品を欧米で生産するための部品の輸出が止まった。)
従来、アメリカでは暗号アイテムの規制は武器と見なされて国務省で管理されていたが、1996 年 11 月の Executive Order 13026[3]（Sec.1, (a)）により民生分野のものは同年 12 月に商務省の管理に移管された。このときに鍵長が 40 ビット以下のものであれば許可され得るようになった。
（1997 年 10 月に発売された Internet Explorer 4.の暗号機能（鍵長 128 ビット）によりそれを組み込んだ Windows が規制されるようになった。）

General Software Note

ココム規制においては、民生用に市場で流布する製品は controllable ではないために規制しないという一つの原則があった。技術・ソフトウェアに関しては General Technology Note があり、in the public domain にあるものまたは basic scientific research によるものは規制しないとされていた。

一方、ハードウェアに関してはココム以来、リストで個別に規定する方針となっており、このように共通の除外規定は存在していない。

上記のコア・リスト制定時にソフトウェアに関しては General Software Note が分離された。In the public domain に加えて generally available to the public であるものも規制から除外され、その条件として市販されていること、供給者のサポートなくインストールできることとされた。ただし、規定上は見あたらないが、運用上は General Software Note は暗号ソフトウェアには適用されていなかった。

Wassenaar の規制の変遷

（アメリカの RSA 社が 1997 年に行った DES 暗号（鍵長 56 ビット）の解読コンテストにおいて 6 月に解読された。また 1999 年 11 月に DVD の CSS 暗号（鍵長 40 ビット）が解読された。）

Wassenaar で 1998 年 12 月に対称型暗号の鍵長が 56 ビット以下のものは規制から除外された。また、用途によらない除外規定が設けられ（Cryptography Note）、暗号に関しては generally available to the public であって鍵長が 64 ビット以下であること、ユーザーによって暗号機能が容易に改変できないこととされた。

暗号はそれまでは Wassenaar の規制リストにおいて Sensitive List といわれる厳しい規制レベルに分類される対象であったが、1998 年 12 月により緩い規制レベルである Basic List の対象となった。

（2000 年 2 月に Windows 2000 が発売された。同年 3 月に日本のゲーム用コンピュータが発売され、その輸出規制の件が 4 月にアメリカで報道された[4]。）

Wassenaar で 2000 年 12 月に Cryptography Note における 64 ビットの制限が撤廃された。

EU では、2000 年 9 月に先進国向けの輸出規制を事実上なくすような規則を施行した。

日本では、暗号関係は 1998 年 8 月に衛星放送 TV 受信機と DVD 再生機の分野を限定して一般包括許可の対象とされた。1999 年 6 月に欧米等の先進国向けの輸出は暗号関係全般が一般包括許可の対象となり、また Cryptography Note の 64 ビット以下の規制緩和がいわゆる市販特例の告示によって施行された（該当であるが許可不要とする）。2000 年 12 月にこの 64 ビットの制限は撤廃された。

General Software Note と暗号ソフトウェアの関係

上記の 1998 年の Cryptography Note の generally available to the public における鍵長 64

ビット等の条件は、General Software Note にこの制約を加えて暗号ソフトウェアに適用したものといえる。上記のように 2000 年にこの制約もなくなったことにより、暗号ソフトウェアの規制もある程度他のソフトウェアに近いレベルとなった。
この規制緩和の議論は General Software Note によるアプローチであったため、当初はソフトウェアが対象であったが、最終的にハードウェアも含めて対象とされた。
アメリカでは当初から General Software Note は暗号ソフトウェアに適用されておらず、現在でも鍵長が 64 ビットを超えるマス・マーケットの暗号ソフトウェアについて規制対象としており（734.3(b)(3), 740.13(d)(2)）、web site 上に公開する場合はその時またはその前に当局に notification（URL またはソースコード）を行うことが求められている（734.2(b)(9)(ii), 740.13(e)(3)）。

日米の産業構造と規制緩和

ココム規制以来、エレクトロニクス分野の規制緩和の動きはアメリカのコンピュータ、マイクロプロセッサ、通信、ソフトウェア等の産業の意向を受けて行われている。上記のコア・リストでの暗号の特定用途の規制除外も、当時、アメリカにおいて民生用製品が存在していた分野である。
暗号関連ではアメリカの産業構造はコンピュータとソフトウェアにあり、日本はコンスーマー・エレクトロニクス製品であるハードウェアにある。
日本の産業が強い分野での規制緩和の動きはアメリカと同様ではない。例えば、アメリカが得意である音楽・映画のコンテンツの分野について、その著作権保護管理の技術を開発・実施しているのは日本であるが、著作権保護管理に関して Wassenaar で規制緩和が実現したのは 2003 年 12 月であった。

ソースコード規制と言論の自由との関係

アメリカでは暗号研究におけるソースコードの規制について言論の自由の観点による議論がある。裁判所（最初の判決は 1996 年 4 月の Bernstein v. U. S. Department of State, 922 F. Supp. 1426 (N.D. Cal. 1996)）はソースコードは言論と判断した[5]。
これに対して、上記の 1996 年 11 月の Executive Order 13026（Sec.1, (c)）にあるように暗号ソフトウェアは技術としては扱われず、輸出管理規則では暗号ソフトウェアは情報または理論的な価値としてではなく、ハードウェアの場合と同様にコンピュータ・システム上での電子的機能として規制されている（742.15）。ソースコードは印刷物としては規制されないが、電子的な形態またはメディア（ディスク等）にあるものは規制対象とされる（734.3(b)Note）。上記の判例により、国内の外国人に対するソフトウェアの教示はみなし輸出の対象から除外された（734.2(b)(9)(i)）。

[1] 暗号は 1991 年以前はココムリストの 1527 項で規制されていた。

[2] http://www.cjmag.co.jp/magazine/issues/1996/aug96/08cipher.html

[3] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1996_register&docid=fr19no96-98.pdf

[4] http://news.com.com/2100-1040-239322.html?legacy=cnet

[5] Bernstein 裁判のその後について、
http://www.cand.uscourts.gov/cand/judges.nsf/0/77a88a5a349a6d2f88256e7b006d6c99/$FILE/Bernstein.order.pdf