暗号技術に係る政策動向調査
報　告　書

平成１２年２月

情報処理振興事業協会

目　次

＜本編＞

＜資料編＞

本　　編

0．はじめに

0.1 調査の背景と目的

近年、インターネットの急速な普及を背景に、ネットワークを活用した様々なビジネスへの取り組みが活発化している。しかし、インターネットをインフラとして事業を展開するには、充分なセキュリティの確保が不可欠とされる。

暗号技術は、インターネット上での安全な情報流通を実現するキーテクノロジーであり、電子商取引時代を支える基盤技術として注目されている。その一方、軍事や外交の目的で発展してきたという歴史的経緯もあって、国防上の理由から輸出規制の対象とされる側面も持ち合わせている。冷戦時代の COCOM（Coordinating Committee on Multilateral Export Controls：対共産圏輸出統制委員会）の流れを継ぐワッセナー条約（Wassenaar Arrangement）では、日米欧の他、ロシアやポーランド等旧東側の国も含む 33 カ国が、テロ支援国や懸念国、紛争地域等への暗号製品の輸出規制を実施することで合意している。しかし、このような輸出規制は、企業のグローバルなビジネス展開を阻害するという影響もあるため、アメリカでも産業界からの反発が大きかった。

そして、フランスの暗号使用の自由化（1999 年１月）、アメリカ政府による暗号輸出規制の緩和（2000 年１月）など、暗号技術をとりまく状況は急速に動きつつある。さらに、アメリカの AES（Advanced Encryption Standard）やヨーロッパの NESSIE（New European Schemes for Signature, Integrity, and Encryption）、ISO/IEC JTC1 SC27（ International Organization for Standardization / International Electronical Comission Joint Technical Committee 1 Sub-Committee 27：国際標準化機構/国際電気標準会議　技術専門委員会１　分科委員会 27）における国際標準の検討といった、暗号の標準化を巡る動きも注目される。

我が国においても、今後、電子政府向けの機器調達を控え、暗号製品の調達基準の策定、また、産業活性化施策やプライバシー保護、国家安全保障、犯罪防止等の適正なバランスをとった暗号政策が求められることになる。

本調査では、諸外国の暗号技術に係る政策動向を把握することにより、安全な情報化社会の実現をめざすとともに、我が国の暗号関連事業の振興に寄与することを目的とする。具体的には、高強度の海外暗号製品の輸入に関する実現可能性や海外暗号技術の国内製品への適用可能性、国内暗号製品の海外への輸出に関する実現可能性に関する検討に資するため、暗号技術・製品に対する欧米諸国（アメリカ、カナダ、ドイツ、フランス、イギリス）の規制や審査基準について調査した。また、そのような規制が市場に及ぼす影響の検討に資するため、規制に対する産業界の意識について調査した。

0.2 調査の概要

本調査では、アメリカ、カナダ、ドイツ、フランス、イギリスの計 5 カ国の政策を対象としている。

（1）暗号の利用と貿易に関する諸外国の政策動向

暗号技術及び暗号製品の利用や輸出入に関する規制について、欧米各国の状況を調査した。暗号技術及び暗号製品の利用や輸出入に関する規制がある場合には、それを管轄する機関や、申請手続・許認可のプロセス、審査基準、暗号標準化活動について調査した。

①アメリカ

・輸出・輸入・使用のうち「輸出」のみ規制有り

・2000 年 1 月に暗号輸出規制を緩和：

- 技術審査（ワンタイム・レビュー）により申請手続を簡略化
- 鍵長 64bit 超の暗号製品を非米国企業に輸出する場合は事後報告が必要
- すべての暗号製品は技術審査の後、政府機関以外のいかなる最終ユーザに対しても許可例外として輸出可能（除テロ支援国家 7 カ国）
- 市販暗号製品は、いかなる最終ユーザに対しても許可例外として輸出可能（除テロ支援国家 7 カ国）
- 米国企業の海外子会社に対する暗号製品の輸出は、技術審査は不要

・輸出申請の審査機関：商務省（DOC）の輸出管理局（BXA）

・BXA の依頼で、国家安全保障局（NSA）が暗号の技術審査（独自基準）を実施

・暗号標準化の取り組み：

- 連邦政府の暗号調達標準（FIPS46）として、DES, Triple-DES を策定
- 次世代連邦政府調達標準として AES を策定中
- 国際標準化機構/国際電気標準会議（ISO/IEC）が暗号アルゴリズムの標準化検討に着手

②カナダ

・輸出・輸入・使用のうち「輸出」のみ規制有り

・1998 年 10 月に暗号政策を発表：

輸入・使用の自由、国際協定と調和した輸出、法執行機関の支援等

・輸出申請の審査機関：外務・国際貿易省（DFAIT）の輸出管理課（ECD）

・技術審査は CSE（Communication Security Establishment）がサポート（独自基準）していると考えられる

・暗号標準化の取り組み：ISO/IEC が暗号アルゴリズムの標準化検討に着手

③ドイツ

・輸出・輸入・使用のうち「輸出」のみ規制有り

・1999 年 6 月に暗号政策発表：

規制の縮小、安全な暗号の普及の積極的支援

・連邦輸出局（BAFA）が輸出申請の審査機関

・技術審査は連邦安全情報局（BSI）がサポート（独自基準）していると考えられる

・暗号標準化の取り組み：

- 欧州委員会のプロジェクト NESSIE（New European Schemes for Signature, Integrity, and Encryption）において暗号方式を公募
- ISO/IEC が暗号アルゴリズムの標準化検討に着手

④フランス

・輸出・輸入・使用のうち「輸出」「使用」に規制有り（「使用」は 1999 年１月に規制撤廃を発表したが、法改正が必要なため、当面は鍵長の上限を 40bit から 128bit まで引き上げることで改善を図る）

・1999 年 1 月に暗号政策の変更発表：

暗号使用の自由化、第三者信用機関（TTP：Trusted Third Party）利用強制の廃止、法執行機関の支援

・輸出申請の審査機関：中央情報システム安全部（SCSSI）

・技術審査も SCSSI（独自基準）が実施

・暗号標準化の取り組み：

- 欧州委員会のプロジェクト NESSIE において暗号方式を公募
- ISO/IEC が暗号アルゴリズムの標準化検討に着手

⑤イギリス

・輸出・輸入・使用のうち「輸出」のみ規制有り

・1999 年 7 月に電気通信法案及び「電子商取引の促進」を発表：

捜査のための暗号鍵の開示要請、法執行機関の支援

・輸出申請の審査機関：貿易産業省（DTI）の輸出管理局（ECO）

・暗号技術審査は通信電気セキュリティグループ（CESG）が実施（独自基準）

・暗号標準化の取り組み：

- 欧州委員会のプロジェクト NESSIE において暗号方式を公募
- ISO/IEC が暗号アルゴリズムの標準化検討に着手

図表 0-1　欧米の暗号関連施策の現状

項　目		アメリカ	カナダ	ドイツ	フランス	イギリス
暗号関連施策の動向		暗号輸出規制緩和（2000年1月）	暗号政策発表（1998年10月）	暗号政策発表（1999年6月）	暗号政策変更（1999年1月）	電気通信法案/電子商取引の促進（1999年7月）
暗号の法的規制の有無	輸出	あり	あり	あり	あり	あり
	輸入	なし	なし	なし	なし	なし
	使用	なし	なし	なし	あり*	なし
輸出審査機関		商務省（DOC）の輸出管理局（BXA）	外務・国際貿易省（DFAIT）の輸出管理課（ECD）	連邦輸出局（BAFA）	中央情報システム安全部（SCSSI）	貿易産業省(DTI)の輸出管理局（ECO）
技術審査		NSA	[CSEのサポート]	[BSIのサポート]	SCSSI	CESG
暗号標準化の取り組み		・FIPS46-2,3 ・AES ・ISO/IEC JTC1 SC27	・ISO/IEC JTC1 SC27	・NESSIE ・ISO/IEC JTC1 SC27	・NESSIE ・ISO/IEC JTC1 SC27	・NESSIE ・ISO/IEC JTC1 SC27

*)規制は廃止する方針だが、法改正までは鍵長の上限を40bitから128bitまで引き上げることで対応。
[]は公式な形では記載がない

（2）暗号の規制に対する産業界の考え方

(1)で示した、暗号技術及び暗号製品の利用や輸出入に関する規制施策について、各地域の産業界がどのような考えを持っているかを調査した。

・アメリカ政府による暗号技術及び暗号製品の輸出規制緩和（2000 年 1 月）は、ネットワーク配布やオープンソースコードへの配慮も含め、関連業界からは概ね歓迎される結果となった。ただし、まだ既成のしくみが複雑であること、政府の影響力も維持されていることなどを指摘する意見も見られた。

・フランスの産業界では、1999 年 1 月の暗号政策変更を受けて、使用できる暗号の鍵長が 40bit から 128bit まで引き上げられた結果、セキュリティレベルが向上することを歓迎している。

・イギリスの RIP（Regulation of Investigatory Powers）法案[1]に対し、プライバシー保護団体等の反発が高まっている。

（3）国内において利用可能な暗号製品

諸外国の暗号輸出規制を踏まえ、我が国において現在利用可能な暗号製品に関する情報を収集し、そのリストを作成した。

・本調査で採り上げた暗号製品数　　253 製品

・該当するメーカまたは販売代理店数　　123 社

[1] 2000 年 2 月にイギリス政府が提案した法案。法執行機関に通信を傍受したり、暗号文の復号に必要な鍵の開示を利用者に要求できる権利を与える。

1．暗号の利用と貿易に関する諸外国の政策動向

本章では、アメリカ、カナダ、ドイツ、フランス、イギリスの各国における暗号技術及び暗号製品に関する規制や、許認可のしくみについて解説する。

1.1 アメリカ

1.1.1 暗号技術及び暗号製品に関する規制の概要

アメリカでは、暗号技術・製品の使用や輸入に関する規制は存在しないが、輸出については、従来、国家安全保障や犯罪防止を重視した政府の規制と、それに対する産業界の反発という構図が続いていた。しかし、1999 年９月、Clinton 政権は輸出認可方式を変更する方針を打ち出し、これを受けて、商務省輸出管理局（BXA：Bureau of Export Administration）では 11 月に暗号技術輸出規則の草案を公開、パブリックコメントを受け付けた上で翌 12 月には同草案を改訂、さらに 2000 年１月にはそれまでの検討を踏まえた新しい暗号技術輸出規則を発表した。

この規則の主な要点は以下の通りである。

●個人、企業、などの非政府組織のエンドユーザに対する海外輸出

すべての暗号製品や暗号ソフトウェアは、いかなる鍵長でも、技術審査を受けた後、テロ支援国家７カ国[2]を除くすべての国のエンドユーザ（政府機関を除く）に向けて輸出が可能である。これまで輸出は企業内使用にのみ許可されていたが、他社や部品調達などの関連会社、顧客との連絡を含むあらゆる用途に可能となった。銀行、金融機関、また、既にライセンスを受けた企業に対するこれまでの優遇措置はそのまま継続し、「ライセンスの例外」の位置づけで認可される。ただし、政府使用のための輸出はライセンスが必要となる。

●市販暗号製品の海外輸出

市販用の暗号製品及び暗号ソフトウェアという新たな製品のカテゴリーは、いかなる利用者（テロ支援国家を除く）に対しても輸出可能である。市販暗号製品及び暗号ソフトウェアとは、広く利用され、輸出や再輸出が誰（インターネットサービスプロバイダや通信事業者を含む）に対しても可能で、あらゆる製品やサービス（例：電子商取引、クライアント／サーバーの申請やソフトウェアの購入）の提供に利用可能なものである。

どの製品を「市販」に分類するかは、製品の機能や販売量、配布方法に関する BXA

[2] キューバ、イラン、イラク、リビア、北朝鮮、スーダン、シリア

の審査で決定する。市販製品と同じ機能を持つ製品も同様に市販用と考える。512bit や 1024bit 以上の鍵交換機能を持つ、金融に特化した 56bit 鍵の非一般市場向け製品、ネットワークアプリケーションやその他の製品も、機能的に市販製品と同様であれば、市販製品とみなされる。

●インターネットサービスプロバイダおよび通信事業者

インターネットサービスプロバイダおよび通信事業者は、暗号サービスを一般の人に提供する目的であれば、PKI（Public Key Infrastructure）を提供することも含めて、いかなる暗号製品についても認可なく保有及び使用することができる。ただし、政府に対するサービスの提供（例：政府機関の非公開ネットワークの運営）には、認可を要する。

●利用制限のない暗号ソースコードの海外輸出

一般に利用可能で、商業製品のライセンス料や特許権使用料、またはそれを組み込んで開発された製品の販売に関する契約書を必要としない暗号ソースコード（ここでは「利用制限のない暗号ソースコード」と呼ぶ）は、政府の技術審査やライセンスなしで輸出が可能である。輸出業者はソースコードのコピーもしくはソースコードにアクセスできる URL を記した文書を輸出時までに BXA へ提出しなければならない。利用制限のないソースコードを使って開発された海外の製品は、再輸出の際、アメリカ政府による審査や分類が必要ない。この処置は、多くのオープン・ソース・ソフトウェアの輸出に適用される。

商業製品のライセンス料や特許権使用料、またはそれを使って開発された製品の販売に関する契約書を必要とする商業用の暗号ソースコードや暗号ツールキットについても、技術審査を必要とせず、いかなる利用者に対してもライセンスなしで輸出が可能である。ただし、輸出の際に、輸出業者はコピーもしくはソースコードにアクセスできる URL を記した文書を BXA へ提出しなければならない。

その他の全てのソースコードは、技術審査を受けた後、政府機関以外のエンドユーザに向けて輸出することができる。アメリカの輸出業者は、商業用ソースコードを使用して、商業販売用に開発された外国製品については一般情報を提供しなければならないが、アメリカで開発されたソースコードやツールキットを使用して作られた海外製品については、技術審査は不要である。

●アメリカの関連会社

いかなる鍵長の暗号製品、暗号ソフトウェア、暗号技術についても、アメリカ企業の海外関連会社に輸出または再輸出する場合、技術審査は不要である。また、アメリカで働く外国人は、アメリカ企業で働く際に暗号を使用することについて認可を必要としない。これは、アメリカ企業の海外関連会社で外国人が働くことを「ライセンスの例外」として認める、1999 年のドラフト最終版に採用された政策を拡大したもので

ある。ただし、この「ライセンスの例外」として認められた暗号製品や暗号ソフトウェア、暗号技術を組み込んで開発された全ての製品は、技術審査を要する。

●輸出報告

64bit 超の製品を海外に輸出する際には、輸出後の報告が必要となる。しかし、製品が金融に特化した製品、もしくは個人消費者向けに輸出された市販製品である場合、報告は不要である。加えて、製品が無料で輸出されたり匿名でダウンロードできる場合や、銀行業務や財務業務の目的で、アメリカの銀行から金融業者やその関連会社、支社、顧客、契約者に輸出される場合も、報告は必要ではない。報告は規則が履行されているかを確認し、ライセンスのための要件を減らすために用いられる。

●ワッセナー条約改訂（1998 年 12 月）の履行

1998 年、ワッセナー条約（暗号も含む輸出に関して共通の規制を持つ 33 カ国の参加による）は、多国間の暗号規制を更新するため大幅な改訂を行った。この改訂により、56bit の DES や同等の製品（ツールキット、チップも含む）は、技術的審査後には、テロ支援 7 カ国を除くあらゆる利用者に対して、ライセンスなしで輸出可能となった。ワッセナー条約の暗号に関する新要旨では、64bit またはそれ以下の鍵長の、一般市場向けの暗号製品や暗号ソフトウェアは、技術的審査後にはライセンスなしで輸出可能であるとしている。

暗号輸出規制緩和に伴う取扱いの変化を図表 1-1に示す。

図表 1-1　アメリカの暗号輸出規制緩和に伴う変化

製品の分類	改訂前	2000 年 1 月 14 日改訂後		
	ライセンス	ライセンス	技術審査	輸出報告
56bit 以下の鍵長もしくは 1024bit 以下の鍵交換の一般市場向けソフトウェア	TSU	NLR	Yes[1,2]	No
56bit 以下の鍵長もしくは 1024bit 以下の鍵交換の一般市場向けハードウェア	ENC	NLR	Yes[1,2]	No
64bit 以下の鍵長の一般市場向けハードウェア及びソフトウェア	IL/ELA	NLR	Yes[1,2]	No
56bit以下の鍵長もしくは512bit鍵までの交換の非一般市場向けハードウェア及びソフトウェア	ENC	NLR	Yes[1,2]	No
56bit 以下の鍵長で 512bit 超 1024bit 以下の非一般市場向けハードウェア及びソフトウェア	ENC	ENC	Yes[1,2]	No
56bit 以下のコンポーネント（クリップ、ツールキット）	IL/ELA	NLR	Yes[1]	No
市販製品	IL/ELA /L.E.	ENC	Yes	Yes, except to individuals
56bit 超のコンポーネント（クリップ、アプリケーション、専用ツールキット）	IL/ELA	ENC	Yes[1,3]	Yes
一般的な用途のツールキット	IL/ELA	ENC	Yes[1,3]	Yes
ソースコード（一般に入手可能、利用制限なし）	IL/ELA	TSU	No[3,4]	No
ソースコード（制限付きだが一般に入手可能）	IL/ELA	ENC	No[3,4]	Yes
ソースコード（その他）	IL/ELA	ENC	Yes[1,3]	Yes

注）1. 以前のレビューでライセンスを受けたかライセンスの例外であったなら、それに倣う
2. 以前にレビューしていて、鍵長が拡大した場合であればそれを通知するだけで可
3. 海外製品はレビューしない
4. 輸出時に BXA への報告が要求される

ELA：Encryption Licensing Arrangement（暗号ライセンス締結）
IL：Individual License（個別のライセンス）
L.E.：License Exception（ライセンスの例外）
NLR：No License Required（ライセンスは要求されない）
TSU：Lisense Exception – Technology and Software, Unrestricted
（ライセンスの例外 – 制限なしの技術及びソフトウェア）
ENC：License Exception – Encryption Commodities and Software
（ライセンスの例外 – 暗号商品及びソフトウェア）

1.1.2 許認可の申請先、審査機関

（1）審査機関

暗号技術及び暗号製品の輸出申請に関する主要な審査機関は BXA である。

（名　称）Bureau of Export Administration（商務省輸出管理局）

（連絡先）Office of Strategic Trade and Foreign Policy Controls
Bureau of Export Administration, Department of Commerce
14th Street and Pennsylvania Ave, N. W., Room 2705,
Washington, DC 20230
TEL: (202) 482-0092　URL：http://www.bxa.doc.gov/

また、申請時には、NSA（National Security Agency：国家安全保障局）、DoJ/FBI（Department of Justice：法務省, Federal Bureau of Investigation：連邦捜査局）、DoD（Department of Defense：国防省）、DoE（Department of Environment：環境省）にも申請書類のコピーが回され、それぞれの立場からレビューがなされる。暗号技術については、NSA がレビューを行う（ただし、最終的な判断は BXA が下す）。

（名　称）National Security Agency（国家安全保障局）

（連絡先）　9800 Savage Road Suite 6779, Fort Meade, MD 20755-6779
TEL: (301)688-6524　（NSA Public Affairs Office）
URL: http://www.sna.gov/

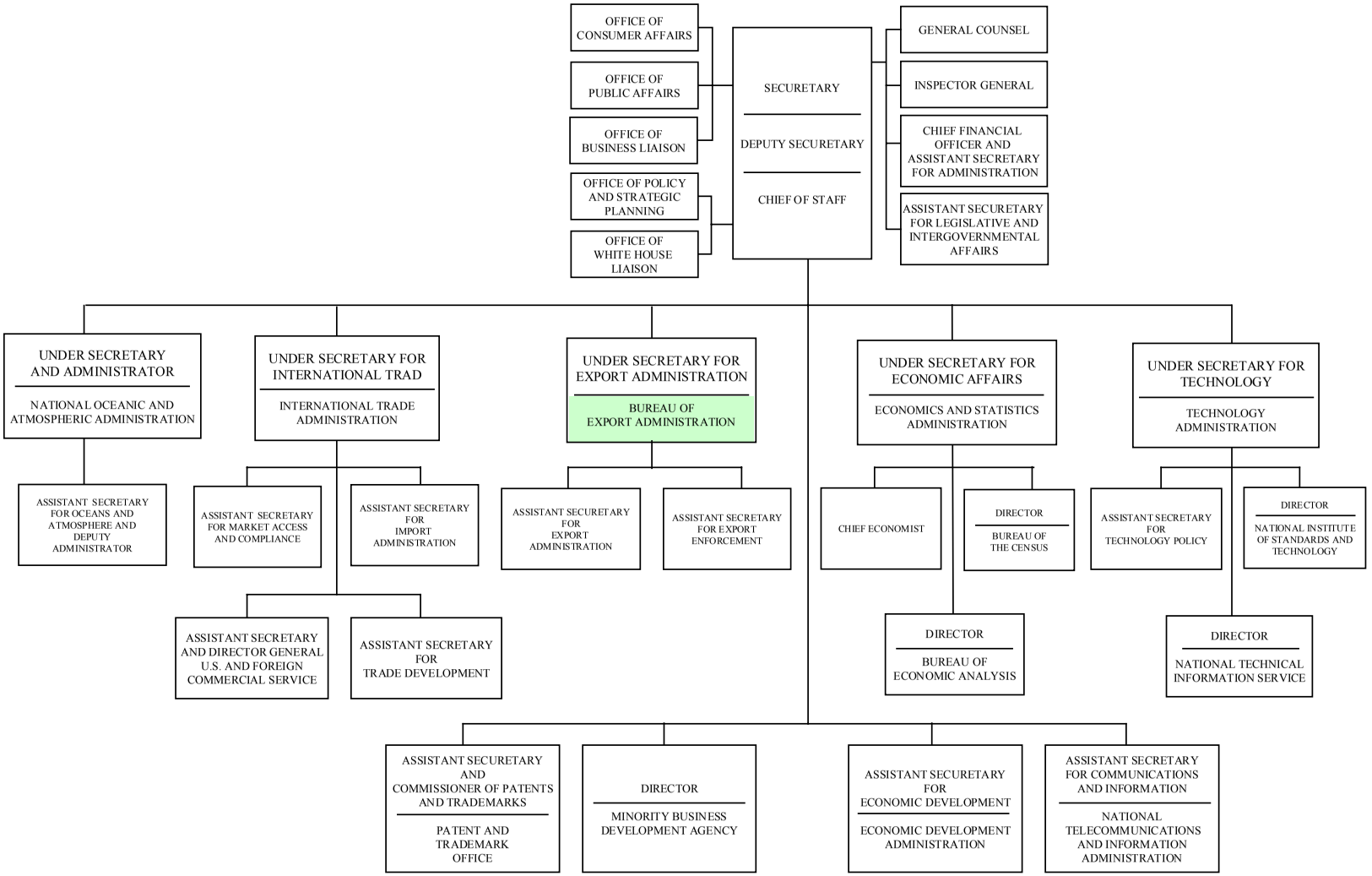
NSA は CSS（Central Security Service）と統合的に活動するケースが多い。CSS は、NSA と軍の暗号関連組織とのパートナーシップを促進するため、1972 年に大統領指令で設立された機関で、海軍、空軍、海兵隊に係る横断的な存在である。NSA と CSS の協力体制を強化するため、NSA の局長は CSS の長を兼ねている。

（2）組織編成

a) BXA

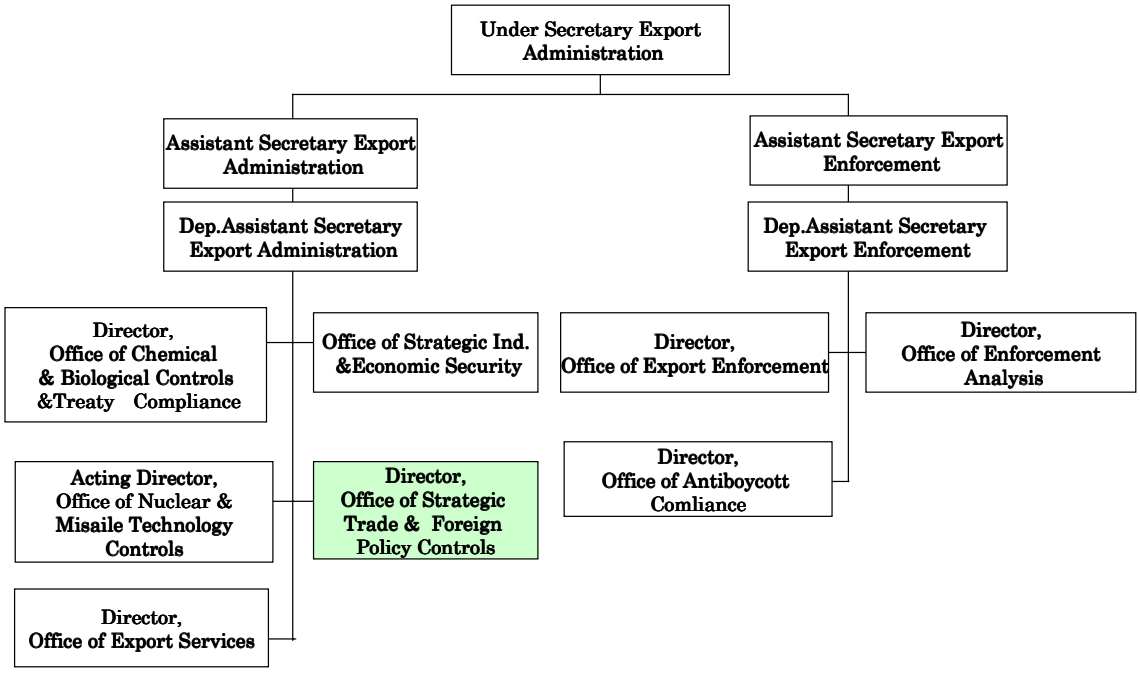
BXA が属する商務省の組織概要を図表 1-2に示す。BXA は、商務省長官室の下に置かれる。

図表 1-2　アメリカ商務省（Department of Commerce）の組織概要



また、BXA の組織構成は図表 1-3の通りである。このうち、輸出規制は、戦略的貿易・外交政策管理課(Office of Strategic Trade & Foreign Policy Controls)が担当する。

図表 1-3　BXA の組織構成



BXA には現在 490 名が勤務しており、そのうち輸出申請の審査を担当する戦略的貿易及び外交政策管理課には、33 名が配置されている。

b) NSA

NSA/CSS の雇用や予算の規模に関する情報は機密扱いとされている。

公開情報によると、「NSA/CSS の支出、フロアスペース、雇用規模は、企業にたとえるとフォーチュン 500 社の上位 10%に相当」とされている。なお、NSA を含むアメリカ政府の情報機関及び活動に関する総合予算は、1997 年に 266 億ドル、1998 年に 267 億ドルであった（1999 年は未公開）。

また、NSA の職員は、軍人と非軍人が 50%ずつで構成される。主要な職種として、アナリスト、エンジニア、物理学者、数学者、言語学者、コンピュータ科学者、リサーチャー、セキュリティ・オフィサー、データフローの専門家、マネージャ、管理・事務の専門家などが挙げられている。

なお、フランスの SCSSI に関する情報から、NSA の情報システムセキュリティの担当部署の規模を 300 名超と推測する見解がある。

（4）ミッション

a) BXA

BXA のミッションは次のように規定されている。

『BXA は、商務省が策定するセキュリティ関連の貿易および競争力強化計画を管理統制し、アメリカ合衆国の国家と経済の安全ならびに外交政策の権益確保に努めている。BXA は、国家安全保障、核拡散の防止、輸出拡大、先端技術を含む諸問題への対応において重要な役割を果たす。BXA の継続的な使命は、アメリカの輸出をさらに拡大する一方、大量破壊兵器の拡散防止に努めることである。これは世界経済の競争が激化する中で、アメリカがリーダーシップを維持する上でも重要である。』

また、ビジョン教書には「世界状況の変化に伴うわが国の戦略的貿易政策および計画の転換点において、われわれは変革の主導的役割を果たすつもりである」とある。

BXA の主な計画と活動は、以下の通りである。

・輸出管理規則（ERA：Export Administration Regulations）を通して、輸出管理法（EAA：Export Administration Act）を施行する。EAA は、兵器の拡散防止をはじめ、国家安全保障上の問題、供給不足、外交政策上の課題（テロ対策など）の追求といった目的で、デュアルユース[3]の輸出管理を規定する。冷戦の終結に伴う規制の簡素化や更新は、BXA の主要な業務である。

・EAA に基づく輸出管理および反ボイコット規制を施行する。EAA は様々な行政処分や民事・刑事罰を通して実施される。

・国防生産法（Defense Production Act）など各種法令に基づき、国防産業および国防技術の下部構造を分析し保護する。経費削減策の影響で軍事・民生両用高度先端技術に対する国防省の依存度が高まる中、この分野ならびに関連領域において競争力を維持することが、アメリカの国家安全保障にとって極めて重要である。

・ウクライナ、カザフスタン、ベラルーシ、ロシアやその他の新興国が、有力な輸出管理機構を構築する手助けを行う。「無法国家」やテロリストが支援国から国家機密に関わる製品や先端技術を入手する事態になれば、アメリカの輸出統制力は著しく低下すると考えられる。

・旧ソ連の新独立国家におけるかつての軍需工場に協力し、民間の平和有効利用への移行を支援する。また、貿易や投資に関わる不必要な障壁を取り除き、米企業との共同事業の機会が得られるよう援助を行う。

・アメリカの国防企業が、民需品への生産転換と輸出市場の開拓を通じて、国防支出削減に対処できるよう支援する。これによりアメリカ人労働者の職を確保すると同時に、防衛産業の下部構造を維持することができる。BXA の 2 つの主要作業部門、

[3] 軍事・民生両用の製品及び技術（主に商品として販売されるが軍事目的に転用可能なもの）

輸出管理部と輸出統制法執行部は、BXA の管理課（Office of Administration）と同様、国家勤務評定（NPR：National Performance Review）ならびに貿易促進協調委員会（TPCC：Trade Promotion Coordinating Committee）の勧告に基づき、輸出管理体制の改革および合理化目標に沿って、この数年間に大幅な再編成と人員削減を行った。なお、BXA は、NPR の改革モデルの 1 つに指定されている。

戦略的貿易および外交政策管理課は、通常兵器および関連のデュアルユースに対応するワッセナー条約に基づき、多国間の輸出管理を管轄する。具体的には、BXA における暗号政策の展開、商用暗号製品の輸出許可の裁定、および鍵回復機関の規制を主導する立場にある。

b) NSA

NSA は、暗号分野におけるアメリカ最大の専門機関である。NSA は、次の 2 つのミッションを遂行するために組織された。

・アメリカの情報システムの防衛

情報セキュリティ（INFOSEC）のミッションは、政府の機密情報を含むアメリカの情報システムを防衛することである。具体的には、ソリューションや製品、サービスを提供し、国家安全保障の利益につながる情報インフラの評価認証を達成する情報関連の運用を指揮することである。INFOSEC の専門家は、政府のシステムが侵入不可能である状態を維持するためにあらゆる努力を行う。

・海外情報機関による情報の生成

海外情報機関は、アメリカの優位性を維持するために活動を続けている。情報機関の活用により、太平洋戦争を 1 年以上短縮することができたと考えられている。

1.1.3 許認可の審査方法

BXA の暗号輸出申請に係る審査プロセスを図表 1-4に示す。

申請フォームや関連の情報が BXA に送られた場合、それがライセンスの申請であれば、BXA から DoJ、DoD、NSA にコピーが回され、各機関にコメントが求められる。BXA は、各機関から得られたコメントを基に輸出許可の可否を決定する。また、分類の申請であれば、NSA のみに情報が提供される。BXA の決定は、プライバシー、国家安全保障、法執行の検討に関する評価者の判断や関連情報を考慮して、ケースバイケースになされる。

暗号の技術審査については、NSA が実施し、その結果を BXA が活用している。NSA では、技術審査に際し何らかの独自基準を適用していると考えられるが、その内容や審査方法については一切公開されていない。

申請者が暗号製品の分類を申請する場合、以下の情報が要求される。

1)審査を依頼する製品もしくはソフトウェアの名称

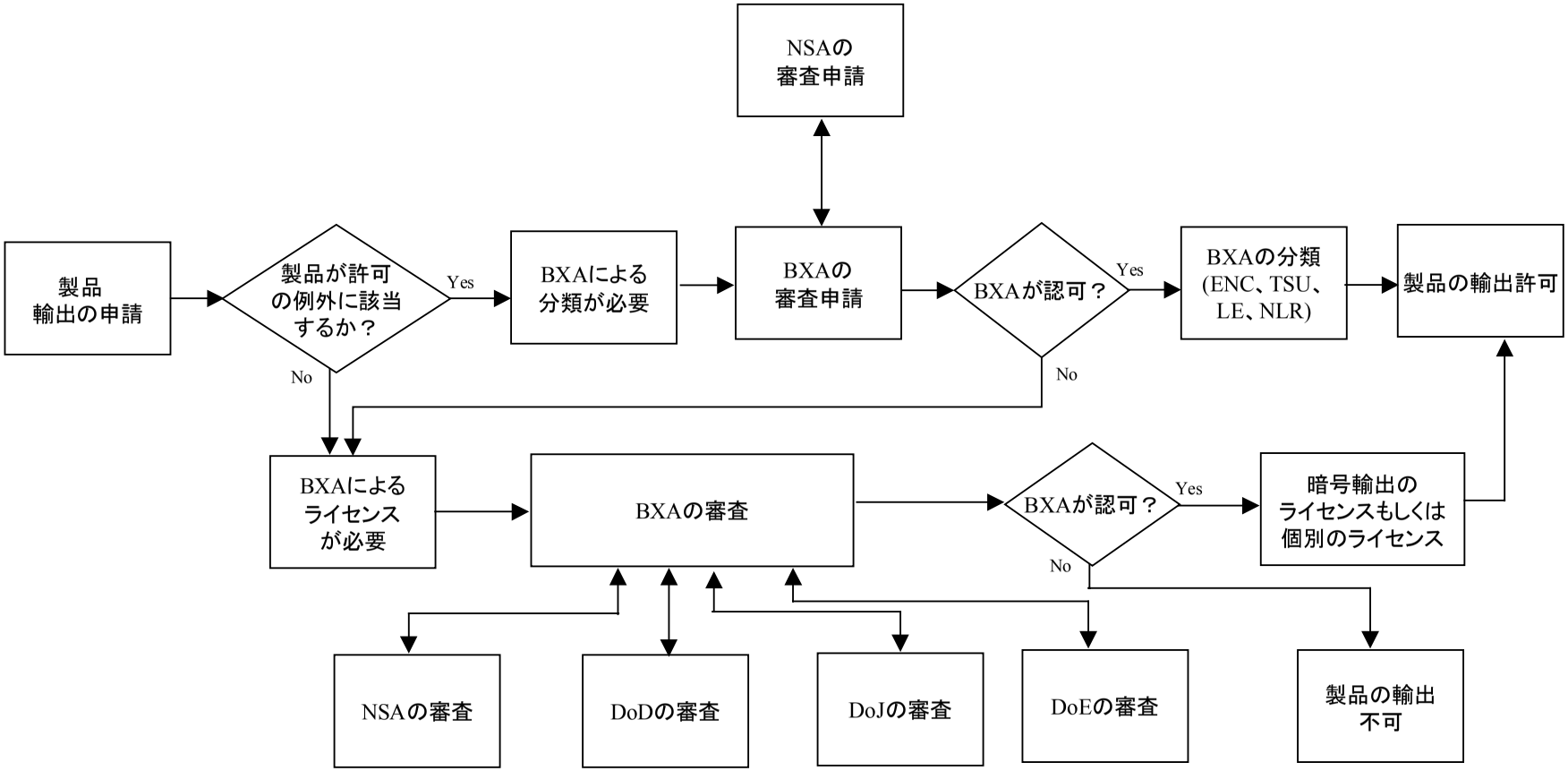
2)製品もしくはソフトウェアの暗号アルゴリズム、鍵管理機構、鍵容量についてユーザの修正を不可能にする方法

3)ライセンスの例外に関する申請窓口へのコピーの送付

4)製品もしくはソフトウェアに関する以下の情報：

- 暗号アルゴリズムや鍵長の特徴
  同じ製品で複数のアルゴリズムが利用されている場合はそれぞれの適用方法
- 平文データを暗号化する前に行う処理（例：データ圧縮）
- 平文データを暗号化した後に行う処理（例：暗号データのパケット化）
- オブジェクトコードや Java のバイトコードに関する要求として、解読や誤用に対するプロテクトに用いられる技術
- コンポーネントに関する要求：
  - （既知の場合）コンポーネントとアプリケーションの関係
  - コンポーネントに対する一般的なプログラミングインタフェースの有無
  - コンポーネントが機能によって強制される点
  - コンポーネントに適用される標準やプロトコル
  - すべての機能性や接続性に関する説明
  - 製造者の名称、コンポーネントの型式番号、その他明確な識別情報の適用
- ソースコードに関する要求：
  - （該当する場合）技術審査を既に受けた製品の実行可能性に関する言及
  - ソースコードが修正可能か、可能な場合には修正方法の技術的な詳細の提供
  - 暗号アルゴリズム、鍵管理ルーチンおよびその呼び出しを含むソースコードのセクションのコピー

図表 1-4　BXA の暗号製品の輸出申請許可に係る審査手順



ENC: License Exception - Encryption Commodities Software
TSU: Licence Exception - Technology and Software, Unrestricted
NLR: No License Requiired
LE: Licence Exception

1.1.4 暗号の標準化動向

（1）暗号の評価基準

①暗号輸出規制に基づく技術審査の評価基準

暗号技術の技術審査については、BXA の依頼を受け NSA が実施し、その結果を BXA が活用している。NSA では、技術審査に際し何らかの独自基準を適用していると考えられるが、その評価基準については一切公開されていない。今回の調査でも、そのような情報については入手が極めて困難であった。

②ISO/IEC15408（Common Criteria）

アメリカで用いられるセキュリティ製品の評価基準として、ISO/IEC15408（CC：Common Criteria）がある。CC では、EAL（Evaluation Assurance Level）と呼ばれるセキュリティ評価の尺度を設定して、保証要件に関するランク付けを行う。評価は公的機関が行い、その結果を認証する。その認証は、当初 NSA が占有的に行っていたが、1992 年 EAL4 以下を扱う NIAP（National Information Assurance Program）が設立され、権限が委譲された。

CC の源流は、アメリカの TCSEC（Trusted Computer Security Evaluation Criteria, 通称”Orange Book”）である。TCSEC は、国防機関において利用されるセキュリティ関連製品の評価基準として 1985 年に策定され、これに基づいて NCSC（National Computer Security Center）が情報セキュリティ関連製品の評価・認定を行っている。また、TCSEC は、ヨーロッパの ITSEC（Information Technology Security Evalution Criteria）やカナダの CTCPEC（Canadian Trusted Computer Product Evaluation Criteria）の策定にも影響を与えた。国立標準技術院（NIST：National Institute of Standards and Technology）と NSA は、TCSEC、ITSEC の統合を目指して、国防関連機関以外の政府機関を対象とした新評価基準 FC（Federal Criteria for Information Technology Security）を 1993 年起草した。FC は実用されるには至らなかったが、これをもとに 1993 年 6 月、アメリカ、カナダ、イギリス、ドイツ、フランス、オランダの 6 カ国の代表者が ISO 標準を目指した評価基準 CC の策定について合意、CC プロジェクトが発足した。アメリカからは NIST、NSA の 2 機関が CC プロジェクトに参加した。CC は 1996 年 1 月に第 1 版、1997 年 10 月に第 2 版ベータ版がまとめられた。1998 年 10 月には、アメリカ、カナダ、フランス、ドイツ、イギリスの 5 カ国間で 1998 年 10 月に相互承認された（オランダは制度がないため不参加）。さらに、ISO/IEC において 1999 年 6 月国際規格 ISO/IEC15408 として承認、同年 12 月に告示された。

CC では、「暗号機能については、最低限、その時点での技術動向等を考慮し、安全と思

われるアルゴリズム・鍵長等を、データの重要度・暗号化速度・コスト等に応じて選択すること。暗号鍵の生成方法、配布と確認、運用時の保管、有効期限、バックアップに関して、安全性を考慮すること。」と解説されている。

（2）暗号の標準化

①DES, Triple-DES

DES は、1974 年に米 IBM 社が開発した共通鍵暗号アルゴリズムである。1977 年 NIST によって政府の調達標準（FIPS46）に認定され（1993 年には FIPS46-2 として再認定）、金融機関をはじめとする産業界のアプリケーションにも広く採用されている。ただし、鍵長が 56bit の DES については、近年の CPU の高速化やネットワークを介した複数のコンピュータの連携により飛躍的に向上した計算能力が解読の危険性を高めており、1998 年の見直しで FIPS の認定が終了した。

一方、DES を三重化した Triple DES は、1998 年に ANSI（American National Standards Institute）で X9.52 として認定され、これを受けた NIST にも 1999 年 11 月、FIPS46-3 として認定されている。ISO でも、ANSI9.52 の認定を受け、ISO/TC68（金融専門委員会）において Triple DES の国際標準化を進めている。

図表 1-5　主要標準化機関による DES、Triple DES の標準

標準化機関	ANSI	ISO/TC68	NIST
Triple DES の 利用モードの標準名	ANSI X9.52	未定	FIPS46-3
DES の標準名	ANSI X9.52	ISO8731-1, 9564-2 10126-2	FIPS46-2
DES の 利用モードの標準名	ANSI X9.52	ISO8372(ISO/IEC JTC1 SC27 の標準)	FIPS81
位置付け	米国金融業界の標準	金融業界の国際標準	米国政府機関に おける標準

（資料：谷口文一, 大田和夫, 大久保美也子, “Triple DES を巡る最近の標準化動向について”, 日本銀行金融研究所/金融研究, 1999 年 9 月）

②AES

AES (Advances Encryption Standard) は、NIST が策定を進めている次世代のアメリカ政府標準暗号である。1997 年 1 月～1998 年 6 月の期間公募され、15 のアルゴリズムが提案された。AES は、DES の後継となる位置づけであり、DES 同様、多様なアプリケーションに採用され、世界中で利用される可能性がある。

AES アルゴリズムの公募要件は、次の通りである。

・共通鍵ブロック暗号であること

・鍵長は 128bit、192bit、256bit のいずれも利用可能であること

・ロイヤリティ・フリーで使用できること

また、アルゴリズムの評価基準として以下の項目を設定している。

・安全性（解読の困難性：暗号文のランダム性、暗税制に関する理論的根拠、評価プロセスにおいて指摘された問題点）
・コスト（鍵のセットアップ、暗号・復号の処理速度、メモリ容量）
・その他アルゴリズムの特徴（アプリケーションへの利用可能性、ハードウェア・ソフトウェアへの適用性、構造の単純性）

NIST はこれらの基準に基づく評価を行うにあたり、外部の暗号研究者や技術者による独自の分析結果を参考にするとしている。

AES の検討ステップは、以下の通りである。計画通りに進めば、2001 年夏には標準化が終了する。

・1997 年１月　NIST が AES 開発の開始を宣言
・1997 年９月　暗号アルゴリズムの募集開始
・1998 年８月　第一回会議；AES 候補アルゴリズム（15 件）の公開
・1999 年３月　第二回会議；候補アルゴリズムの分析・検討
・1999 年４月　分析、コメントの公募受付終了、最終候補（５件）の選定
- MARS（IBM）
- RC6（RSA Lab）
- Rijndael（J.Daemen、V.Rijmen）
- Serpent（R.Anderson、E.Biham、L.Knusen）
- Twofish（B.Schneider、J.Kelsey 他）

このうち、MARS、RC6、Twofish はアメリカ、Rijndael と Serpent はヨーロッパからの応募である。

・2000 年４月　第三回会議；候補アルゴリズムの分析・検討
・2000 年９月　分析、コメントの公募受付終了、AES（１件以上）の選定
　～　分析、コメントの公募、コメントへの回答、アルゴリズムの改修
・2001 年夏　AES の標準化終了

③ISO/IEC JTC1 SC27 による国際標準暗号

1999 年秋に ISO/IEC JTC1 SC27 の会議において、暗号アルゴリズムの国際標準を策定する提案がなされ、翌 2000 年３月の会議でこれを業務項目として登録することが承認された（NP 承認）。そこで、翌４月のロンドン会合において、各国からアルゴリズムの候補を提案することとなった。アメリカからは、AES の最終５候補がそのまま提案された。その他では、日本、韓国、ノルウェー、ドイツ（スイスからの寄書もあり）、カナダ、ベルギーからアルゴリズムの提案がなされた。

暗号の評価基準については、現段階では白紙の状態であり、今後はまず暗号のタイプ（共

通鍵暗号（ブロック暗号、ストリーム暗号)、公開鍵暗号）ごとに評価基準の策定を進め、2000 年秋に決定するという展開が予想される。さらに、その上で公募も含めた候補アルゴリズムの提案・分析が行われ、最終的に標準化されるのは早くても 2002 年 3 月以降になるものと考えられる。

1.2 カナダ

カナダにおける暗号政策の特徴は次のように整理できる。

・国際的なワッセナー条約の枠組みに従って暗号輸出規制を実施
・輸出許可の決定を下す際には、他国の輸出の実態と類似の製品の入手可能状況を考慮
・輸出許可申請手続きをよりわかりやすく、既存の手続きでは規制は必要最低限とするよう合理化することをめざす

1.2.1 暗号技術及び暗号製品に関する規制の概要

カナダには暗号の私的な使用を取り締まる法はない。1998 年 10 月、John Manley 産業大臣（Minister of Industry）は、カナダの暗号政策の内容を発表した。この政策では、カナダ人に対して、どのような暗号製品についても開発、輸入、使用を認め、強制的なキーリカバリーの要件や許可制度は課さないとしている。

カナダ政府が具体的に推進している暗号政策の方針は、次の通りである。

・ 電子商取引の発展を支援する
・ カナダの製造業者が自社製品を国際的な協定の枠組みに則って世界中に輸出することを認める
・ 公共の安全性を確保するために、法施行機関の能力を維持するための立法措置を導入する

以下にこれらの方針の内容を示す。

①電子商取引の支援

カナダ人は、どのような暗号製品についても自由に開発、輸入、使用することができる。政府は、強制的なキーリカバリーの要件や、許可制度を実施しない。また、政府は、保管データに対するキーリカバリー技術のような、責任のある業務を産業界が確立することを支援する。さらに、政府は、カナダ政府 PKI（GOC PKI：the Government of Canada Public Key Infrastructure）の実施を通して、模範的な暗号ユーザの役割を務めると同時に、民間の認証機関による産業界主導の認定を促進し、支援する。

②輸出・国際協定

カナダは、ワッセナー条約の枠組みと調和するように、暗号輸出規制を維持している。カナダでは、輸出許可の決定を下す際、他国の輸出の実態や、類似製品の入手が可能な状況か否かを考慮に入れる。今後、輸出許可申請手続きはよりわりやすく、既存の手続きでは規制は必要最低限となるよう合理化されるであろう。

③公共の安全性

政府は、以下の項目のために必要であれば、刑法や他の法規の修正を提案する。

- 暗号鍵の不法な公開の違法化
- 犯罪の遂行における暗号使用の阻止
- 証拠隠滅のための暗号使用の阻止
- 暗号が用いられる状況や環境に対する既存の傍受、捜索、没収、支援手続きの適用

1.2.2 許認可の申請先、審査機関

（1）審査機関

カナダの輸出業者は、外務・国際貿易省（DFAIT：Department of Foreign Affairs and International Trade）に個別の輸出許可を申請する。許可を得るために、輸出業者はまず申請書を記入し、DFAIT に送らなくてはならない。要求される書式は DFAIT フォーム EXT-1042「製品の輸出許可申請書」である。

審査を行うのは、DFAIT の輸出入管理局輸出入管理課（the Export Control Division of the Export and Import Control Bureau）であり、申請の許可／不許可を決定する。

（名　称）Export Controls Division (ECD)
The Department of Foreign Affairs and International Trade
（連絡先）125 Sussex Drive, Ottawa, Ontario, K1A 0G2
TEL: (603) 996-2387　Fax: (613) 996-9933
URL: http://www.dfait-maeci.gc.ca/

なお、DFAIT から要求される許可に加え、税関の書類（Customs Form）も要求される。製品の輸出を許可する前に、税関の役人は輸出入許可条例（EIPA: Export and Import Permits Act）と税関条例（Customs Act）に従って、その輸出が EIPA を違反しないか確かめなければならない。輸出用に製品が提出されるときには、輸出許可書と税務署申告書（Customs and Excise Declaration form）B-13/B-13A を提出しなければならない。

また、審査時における暗号の強度評価は、カナダ政府における情報セキュリティ分野の先導的機関である CSE（Communications Security Establishment）[4]がサポートしているものと考えられる。CSE は、Common Criteria の評価機関としての機能もあり、GOCPKI でも中心的な役割を担っている。

（名　称）Communications Security Establishment (CSE)
（連絡先）Canadian Central Facility(T1B), Communications Security Establishment
P. O. Box 9703, Terminal, Ottawa, Canada. K1G3Z4
TEL: (613)991-8797
URL: http://www.cse-cst.gc.ca/

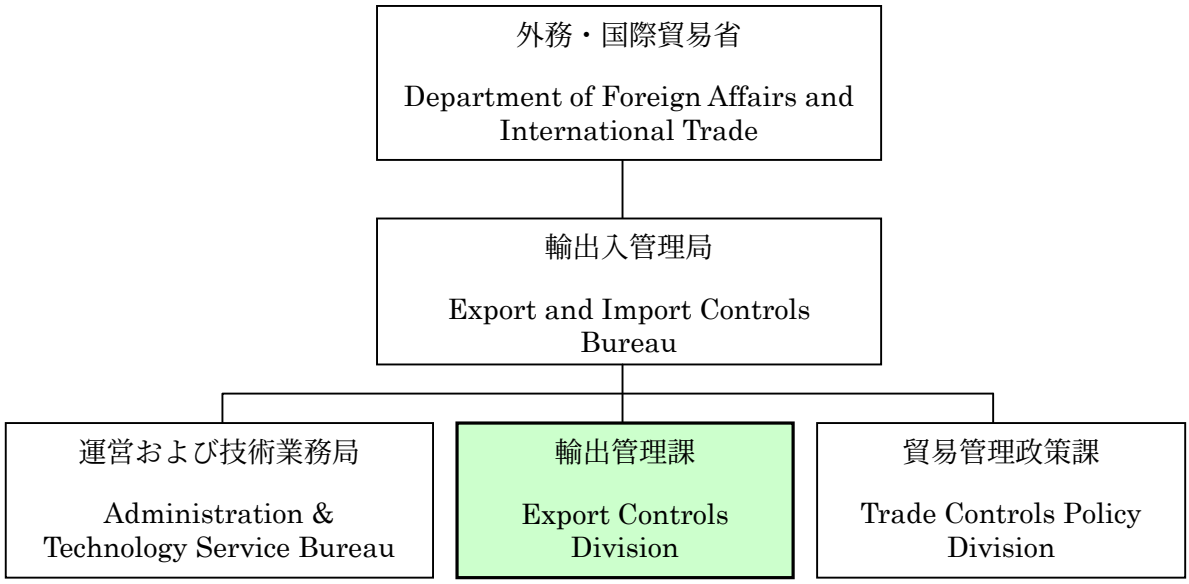
（2）組織編成

審査機関は輸出管理課（Export Controls Division）であり、これは外務・国際貿易省（Department of Foreign Affairs and International Trade）の輸出入管理局（Export and

[4] URL: http://www.cse-cst.gc.ca/cse/

Import Controls Bureau）に属する 3 部局のうちの 1 つである。他の 2 つは、運営および技術業務局（Administration and Technology Service Bureau）、貿易管理政策課（Trade Controls Policy Division）である。図表 1-6にその構成を示す。

図表 1-6　カナダにおける暗号審査機関の位置付け



輸出管理部の名簿には、部長から受付係まで 17 名が記載されている。
また、CSE については、組織編成、人員等の情報が得られなかった。

（3）ミッション

輸出入管理局（EPD：Export and Import Controls Bureau）は、1947 年に成立した輸出入許可法（EIPA：Export and Import Permits Act）の施行責任を負う。EIPA に従って製品の一覧が作成され、外務大臣には記載製品の流通を統制する広範な自由裁量権が与えられる。また、外務・国際貿易省法（Department of Foreign Affairs and International Trade Act）に基づき、国際貿易担当相（the Minister for International Trade）は市場参入から外交政策まで大半の分野で政策指針を示す。

自由貿易に伴う経済的利益は、カナダにとって最も重要な資産の 1 つとみなされているが、その一方で貿易統制は必要不可欠との判断が示されてきた。それには以下のように様々な理由がある。

- 多国間協定に伴う責務を全うするため、軍備と戦略に関わるデュアルユースの貿易を規制、大量破壊兵器の拡散防止に努める。
- カナダの国家安全保障において脅威となる、国連の制裁を受けている、国内または対外的紛争の当事国である、人権侵害を行っているなどの理由により、特定の国家に対

する軍事物資の供給を禁止する。

- 衣料品製造業など競争力のない国内産業を保護する。
- 国際協定から得られる交渉利益を確保する。
- カナダの供給管理計画に対する支援策として、貿易制限を行う。
- その他の国際的責務を果たす。
- 国連安全保障理事会の貿易制裁を実行する。

EIPA の規定により、行政長官の諮問委員会（Governor-in-Council）が、輸入統制品リスト（ICL：Import Control List)、輸出統制品リスト（ECL：Export Control List)、および地域統制リスト（ACL：Area Control List）を定める。ECL は製品一覧で構成され、記載されたすべての製品の輸出に許可が必要となる。輸出統制の対象製品は以下の通りである。

- 農産物（精製砂糖、砂糖を含有する製品、ピーナッツバター）
- 繊維、衣料品
- 軍需および戦略に関わるデュアルユース物資（暗号製品を含む）
- 核エネルギー関連の物質およびテクノロジー
- 拡散が懸念されるミサイル、化学、または生物関連物資
- 軟質木材、未処理の丸太、その他数種類の林産品
- アメリカ原産品、医療効果を有する数種類の品目を含む種々雑多な物資
- ACL に記載された国家に輸出されるあらゆる物資

大部分の統制品は輸出入の際に個別許可を要する。ただし、汎用許可により手続きを簡素化できる場合がある。汎用許可は個別許可と異なり、個々の輸出入業者に限定されない。汎用許可は、あらかじめ認定を受けた特定の適格国間との輸出入に対して、簡素化された手続きにしたがって許可を与える。たとえば、家庭用品は汎用許可の対象品目の一例である。輸出管理課（Export Controls Division）は輸出入許可の審査を行い、許可／不許可を決定する。

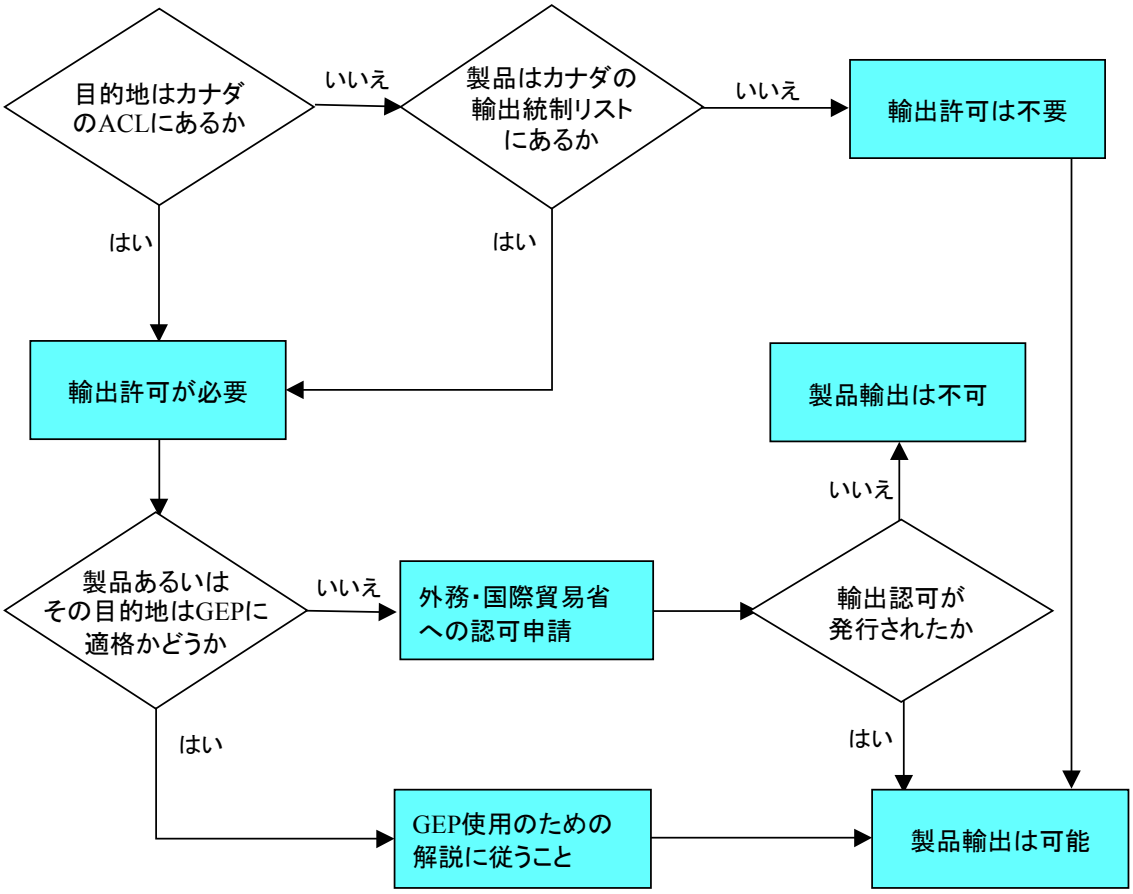
ECL に記載される製品や技術の輸出には、DFAIT の認可を必要とする。

1.2.3 許認可の審査方法

（1）申請・許認可のプロセス

輸出認可の申請は DFAIT 宛に提出される。カナダは、以下の図表 1-7のような申請手続きのフローチャートを公表している。

図表 1-7　カナダにおける輸出申請手続きの流れ



ACL：Area Control List　地域統制リスト（現在はアンゴラ、ビルマ（ミャンマー）、リビア）
GEP：General Export Permit　一般輸出許可

また、審査基準として、以下の項目が規定されている。

・アメリカへの暗号製品及び技術の輸出は認可を必要としない。

・鍵長が 128bit 以内の共通鍵アルゴリズムを組み込んだ一般市場向けのソフトウェアには一般輸出認可が発行される。

・カナダでは、1998 年 10 月に Manley 産業大臣によって発表された政府暗号政策に合わせて、暗号の多目的用途向け認可を設定し、規制製品に関する情報（カタログ）

をメンテナンスすることによって、規制されている暗号製品の認可発行プロセスを簡素化した。

・特定の製品または製品群の輸出を許可するため、DFAIT は特定の国々の承認済みの該当部門向けに暗号の多目的用途向け認可を発行する。輸出業者は、厳重に管理された暗号を

a)個人の利用者には認可を要することなしに、

b)銀行や金融業者、純粋なカナダやアメリカ企業のような既に承認を受けた該当部門に対して、

ⅰ）軍の利用者向けの輸出を許可しないこと

ⅱ）輸出業者は利用者に全ての条件や状況を通知することを保証すること

という前提で、輸出することができるようになる。

・カタログ化では、輸出許可発行時に規制製品の暗号能力や機能を規定する。製品が最後にカタログ化されてから変更されていない場合、以後の認可申請における認可協議過程は利用者や製品の利用目的を中心に議論される。

1.2.4 暗号の標準化動向

（1）暗号の評価基準

①暗号輸出規制に基づく技術審査の評価基準

暗号の技術審査については、明確な審査基準は公開されていない。ただし、カナダは、規制を最低限の水準にとどめることを政策として打ち出しており、アメリカに比べ強度の高い暗号の輸出が容易であった[5]（アメリカの大幅な輸出規制緩和（2000 年 1 月）より前）。その意味で、CSE の基準がアメリカの NSA に比べ緩やかである可能性はある。

②ISO/IEC15408（Common Criteria）

カナダで用いられるセキュリティ製品の評価基準として、ISO/IEC15408（CC：Common Criteria）がある（CC の概要は 1.1.4 参照）。カナダでは、1993 年、アメリカの TCSEC やヨーロッパの ITSEC を参考に、CTCPEC を策定した。

CC 策定に際して、カナダからは CSE が参加した。現在は、CSE が CC の認証機関として機能している。

（2）暗号の標準化

①ISO/IEC JTC1 SC27 による国際標準暗号

ISO/IEC JTC1 SC27 の暗号アルゴリズム国際標準の検討（概要は 1.1.4 参照）において、カナダは、2000 年４月のロンドン会合で、暗号アルゴリズムの候補を提案した（詳細については 4 月 14 日現在で未公開）。

---

[5] Marc Plumb; “A smmary of Canada’s export controls on cryptographic software”, June 25, 1996 （http://insight.mcmaster.ca/org/efc/pages/doc/crypto-export.html）

1.3 ドイツ

ドイツは暗号化の規制に対する反対派の最前線にあり、キーエスクローや国際的規制の推進を図っていたアメリカとは正反対の立場にいた。ドイツは、EU の 1997 年の暗号化とデジタル署名に関する EU 文書に重要な役割をなした。1998 年には、ドイツの努力によってキーエスクローはワッセナー条約の一部になることを免れたとも言われている。

1.3.1 暗号技術及び暗号製品に関する規制の概要

在米のドイツ大使館や連邦経済技術省（Federal Ministry of Economics and Technology）によると、暗号の使用や輸出入に関する方針は次の通りである。

- 暗号化のソフトウェアやハードウェアの使用に対する規制はない。
- 暗号の輸入に対する規制はない。

ドイツでは、1997 年 6 月、電子署名法が成立した。法的拘束力を持った電子署名システムは公開鍵暗号を使用しており、署名者の持つ秘密鍵と認証局によって定められた公開鍵が必要とされる。使用する暗号アルゴリズムについては、法律による規定がない。法律は認証局を特定していないが、そのような団体は政府の通信行政局（Communications Authority）から認可を受ける必要がある。通信行政局が認証局を認証し、公開鍵証明を目的とした信頼のデジタルチェーンを作ることになる。

経済協力開発機構（OECD：Organization for Economic Cooperation and Development）に対するドイツの報告によると、連邦政府の電子商取引イニシアチブ（Electronic Commerce Initiative of the Federal Government）は、「ドイツ政府には、暗号製品の売買や使用を法令によって規制する計画はない。ドイツでは、暗号システムを自由に選択、使用することができる。」と述べている。ドイツ行動計画（1997 年秋）に関するレポートにおいて政府が述べている政策は、次の通りである。

- 持続可能な基盤に基づく、ドイツの信頼できる強い暗号の可用性の確保
- ドイツの国家安全保障や犯罪に係る検察当局の権利の保護
- 暗号システムに関するドイツの製造業者の市場における影響力の強化

暗号の輸出は、EU のデュアルユース規制の履行によって規制されている。暗号製品は、ドイツの輸出リストに個別に掲載される。

1998 年 12 月に改訂されたワッセナー条約の輸出規制をドイツは容認した。

1999 年 6 月、ドイツ政府は「ドイツの暗号政策における要点」を発表した。この発表には、５つの要点が示されている。

1) 政府は、暗号の実用性に対する規制を意図しない。政府は、ドイツにおける安全な

暗号の普及を積極的に支援する。

2) 政府は、安全な暗号のための信頼のフレームワークを構築する施策を実施する。

3) 政府は、安全で強力な暗号製品を開発するために暗号製造業者の能力が必要不可欠であると考える。

4) 強い暗号の普及によって、政府の傍受能力が侵害されるべきではない。政府は、法の執行と安全保障機関の技術的能力を高めるために努力する。

5) 政府は、暗号政策における国際協力を重んじる。それによって、市場主導型のオープンな標準や互換性のあるシステムを支持する。

また、経済省による 1999 年８月の報道発表では、一般市場向けの暗号に対する輸出規制は必要最小限にされる、という新しい輸出規制が発表されている。既に EU では、EU 内における一般市場向け暗号の輸出を自由化している。少数の国や機密を扱う（軍事的な）アプリケーションに対する輸出を除き、製品が一般的なライセンスで充分な一般市場向け暗号に分類されるかどうかは、輸出事業者自身の判断にまかされている。その場合、一般的な申請の必要はない。ただし、輸出事業者は、要請に応じて輸出の詳細を提出できなければならない。

ドイツにおける暗号製品の輸出に対する規制は、このような EU 規制とワッセナー条約に沿って、1999 年９月に施行された General License Nr.16 に従って改訂された規則に基づいて実施されている。

1.3.2 許認可の申請先、審査機関

（1）審査機関

ドイツにおける輸出の許可申請と資格審査機関の住所は、以下の通りである。

（名　称）Bundesausfuhramt（BAFA：連邦輸出局）

（連絡先）Frankfurter Str. 29-35, 65760 Eschborn, Germany

TEL: (06196)908－712　　FAX: (06196)908-859

E-mail: poststelle@bundesausfuhramt.de

URL: http://www.bundesausfuhramt.de

また、ドイツにおける Common Criteria の認証機関である BSI（Bundesamt fur Sicherheit in der Informationstechnik：連邦安全情報局）は、直接的な関与はないが、助言的な役割を担うと推測される。

（名　称）Bundesamt fur Sicherheit in der Informationstechnik（BSI）

（連絡先）Godesberger Allee 183, Postfach 20 03 63, 53133 Bonn, Germany

TEL: (49) 228-9582-0　　FAX:(49) 228-9582-400

URL: http://www.bsi.de

（2）組織編成

BAFA は、連邦経済技術省に属する上級官庁である。BAFA は 3 部局から構成され、内部管理を担当する本部である第 1 部局、通常軍備および輸出手続を担当する第 2 部局、国際制度およびデュアルユースを担当する第 3 部局に分かれている。BAFA の構成を図表 1-8に示す。構成暗号化関連事項の審査は、第 3 部局の 321 課が担当する。

図表 1-8　ドイツにおける連邦輸出局の構造

Federal Export Office-Direction - President - Vice-President - Press and Public Relations - Internal Auditing, Quality Assurance	連邦輸出局 - 局長 - 副局長 - 報道、渉外 - 内部監査、品質保証
Division 1-Administration - Section 101-Personnel - Section 102-Legal Affairs - Section 103-Budget, Internal Services, Licence Registration - Section 104-Data Processing, EDP Operation - Section 105-Organization - Section 106-Security Protection	第 1 部局 - 管理 - 101 課 - 人事 - 102 課 - 法律問題 - 103 課 - 予算、内部業務、許可登録 - 104 課 - データ処理、電子データ処理 - 105 課 - 組織化 - 106 課 - セキュリティ保護
Division 2-Conventional Armaments, Export Procedures > Subdivision 21-Export Procedures, Export Monitoring - Section 211-Principles and Procedural Questions, Collective Export Licenses - Section 212-Information Analysis, Reports, Reliability Verification - Section 213-Cooperation with Monitoring and Investigating Authorities - Section 214-Non-Listed Goods, Embargoes > Subdivision 22-Licences, Conventional Armaments, Simplified Procedures, War Weapons Control -Section 221-Licences for Conventional Armaments -Section 222-Licences for OECD-Countries, Firearms -Section 223-War Weapons Control -Section 224-Control of Compliance with Obligations, General Licenses (Declaration Procedure), End-Use Certificates	第 2 部局 - 通常軍備品、輸出手続 > 21 部 - 輸出手続、輸出監視 - 211 課 - 原則および手続き上の問題、集合輸出認可 - 212 課 - 情報分析、報告書、信頼性検証 - 213 課 - 監視調査当局に対する協力 - 214 課 - リスト外物資、禁輸措置 > 22 部 - 許可、通常軍備品、簡易手続、兵器統制 - 221 課 - 通常軍備品に対する許可 - 222 課 - OECD 諸国向け許可、火器に対する許可 - 223 課 - 兵器統制 - 224 課 - 義務遵守の管理､汎用許可(申告手続)、最終用途証明書
Division 3-International Regimes, Dual-Use Goods > Subdivision 31-Aviation and Space Technology, Nuclear Technology, Industrial Goods -Section 311-1-Basic Technical Questions, International and National Lists of Goods -Section 311-2-Special Tasks -Section 312-Aviation and Space	第 3 部局 - 国際レジーム、デュアルユース > 31 部 - 航空宇宙技術、核技術、工業製品 - 311-1 課 - 基本的な技術的問題、国際および国内向け製品リスト - 311-2 課 - 特殊任務(special tasks) - 312 課 - 航空宇宙部品、ミサイル技術(MTCR､ミサイル関連技術輸出規制) - 313 課 - 核技術(NSG、原子力供給国グループ)、放射性物質 - 314 課 - 電子装置、情報セキュリティ - 315-1 課 - 機械装置、生産技術 - 315-2 課 - コンピュータ、ソフトウェア、システム･セキュリティ >32 部 - 化学、生物、化学兵器禁止条約(CWC)、ライセンス **- 321 課 - デュアルユース製品に対するラ**

Components, Missile Technology (MTCR) -Section 313-Nuclear Technology (NSG), Radioactive Substances -Section 314-Electronical Systems, Information Security -Section 315-1-Mechanical Systems, Manufacturing Technology -Section 315-2-Computers, Software, Systems Security > Subdivision 32-Chemistry, Biology, Chemical Weapons Convention (CWC), Licenses **-Section 321-Licences for Dual-Use Goods** -Section 322-Chemicals, Biological Agents, Materials, (Australia Group) -Section 323-Chemical Weapons Convention –Principles, Inspections-, Chemical and Biotechnological Units, BWC Project -Section 324-Chemical WeaponsConvention -Declarations, Special OPCW Issues-	**イセンス** - 322 課 - 化学、生物関連の薬品と物質、(オーストラリア・グループ) - 323 課 - 化学兵器禁止条約－綱領､査察－、化学および生物工学ユニット、BWC（生物兵器条約)プロジェクト - 324 課 - 化学兵器禁止条約－申告、OPCW(化学兵器禁止機関)の特別問題(OPCW 問題)-

BAFA には約 340 名が勤務する。

（3）ミッション

ドイツ連邦共和国は､政府が実施する審査に関する包括的なミッションを規定している。以下はその内容の一部に基づいている。

ドイツ連邦共和国は、要注意製品に対する輸出統制を政策の最優先事項と位置付けている。軍事目的への転用が懸念される製品の輸出を統制して、ドイツ連邦共和国の国家安全保障を脅かす要因を排除し、外交関係の混乱を防止して各国との平和的共存関係を維持する。特に、大量破壊兵器および関連ミサイル技術の拡散防止に力を入れる。

BAFA の主な職務は、所定の認可手続に基づき軍事目的に転用可能な製品、テクノロジー、またはソフトウェアの輸出に対する認可の必要性を調査し、輸出許可を与えるかどうか決定することである。輸出許可は軍事装備（例：兵器や兵器の生産設備）およびデュアルユースの双方に対して適用される。

BAFA の業務のうち暗号化に関わる職務の概要は、以下の通りである。

①輸出管理システムにおける BAFA の職務

輸出管理システムにおける BAFA の職務には、まず認可要件の審査が挙げられる。所定の輸出管理体制に基づいて、BAFA は特定の商品に輸出許可が必要か否か審査する。原則として、デュアルユースの輸出は欧州連合（EU）の法令（デュアルユースの輸出規制に関するコミュニティ制度を設定した会議規定：EC 規定 No.3381/94,

1994 年 12 月 19 日）により規制される。なお、EU では、軍事装備や他の特に重要な数種類のデュアルユースについては、移動にも許可が必要となる。数項目の国内規定の例を除けば、EU の製品リストとドイツの輸出リストに記載される項目は、ワッセナー条約の統制品リストに従って定められる。

ワッセナー条約に基づく商品リストは、最新の技術進歩に合わせて定期的に更新される。BAFA の職員は、これらの一覧表の更新作業にも加わる。ワッセナー条約のような国際制度は国際法のもとでは拘束力を持たないものの、参加各国に対して重大な政治的義務を課す。商品一覧を含め国際制度の決議は、各国の外国貿易法や EU の法令に組み込まれなければならない。

②輸出許可の交付に関する審査

外国貿易ならびに貿易決済における取引の基本的権利が、厳密な法規制の範囲内で制限を受けることがある。ドイツ連邦共和国は国家安全保障、諸外国との平和的共存関係の混乱防止を目的とする規制を施行することができる。また、ドイツ連邦共和国の対外関係に支障を来たす事態を回避する義務がある。EC 規定に基づく輸出許可書交付についても、同等の基準が当てはまる。EC 加盟国は輸出許可書の交付に際し、以下の点を特に考慮することで合意に達した。

- 国際的核兵器非拡散合意および要注意製品統制の枠組みに基づく加盟国の義務
- 国連安全保障理事会が課す、または他の国際機構が合意した制裁の枠組みに基づく責務
- 自国の外交および安全保障政策の検討
- 予定されている最終的な用途と転用リスクの検討

BAFA の主要職務は、輸出申請に対して以上の点を検討した上で、戦略的に重要な製品の輸出の可否を決定することである。多くの場合、連邦経済技術省および連邦外務省(Federal Foreign Office)と綿密に協力する必要がある。BAFA は許可を要する製品について、その用途、輸出先、購入者およびエンドユーザ、種類、さらに場合によっては数量を調査し､輸出業者の信用情報も考慮した上で輸出許可の発行を決定する。

デュアルユースに関わる法的および行政上の問題は、とりわけ複雑である。デュアルユースは主に民生用途で利用されるが、軍事目的にも転用できる（例：工作機械)。毎年ドイツ国境を越える無数の輸出品の中でもこの種の製品は例外的だが、通常その最終的な用途が直ちに明らかになることはない。BAFA の業務は、製品の用途に関する情報を可能な限り多く入手した上で、その情報に基づき輸出許可交付の可否を決定することである。その際、輸出業者は輸出する製品の用途について、納得のいく説明を行う義務がある。一方、連署人（cosignee）は、製品の最終用途が輸出許可申請書

の記載に一致しているかどうか、最終用途証明書により確認しなければならない。さらにユーザは、連邦輸出局の事前承認なしに個々の製品を再輸出しないことを確約しなければならない。

③その他の輸出管理関連の職務

輸出管理に関する国際協力体制に基づき、連邦輸出局は国際輸入証明書（IC）を発行する。この証明書は外国のサプライヤが輸出にこの種の書類を必要とする場合、ドイツの輸入業者に対して発行される。IC は、国際貿易の流れを統制する手段であると同時に、通常は供給国側の輸出許可を取得するのに必要である。また、連邦輸出局は申請に基づき配達証明書（DVC）を発行する。

1.3.3 許認可の審査方法

"Limits of Trust, Cryptography, Governments, and Electronic Commerce"[6]では、ドイツで行われている申請の審査手続きについて解説している。以下は同書からの引用である。

輸出許可を得るためには、ドイツ行政法の一般原則が適用され、申請は BAFA に対してなされる。輸出業者がドイツ国内に拠点を持つ場合、BAFA は EU 内の他の国に置かれた輸出品に対しても管轄権を有する。輸出業者が法人である場合は、本部事務所あるいは本部のみが輸出許可を申請できる。輸出業者が商品のある場所以外に位置している場合、EU デュアルユース規制のもとで、複数の EU 加盟国が輸出に対する管轄権を有するケースが生じうる。商品が輸出業者とは異なる国に位置している場合、BAFA は輸出禁止権を有する EU 内の当該国の適当な関係当局と協議する。

オンラインでのソフトウェアの伝送が「輸出品」とされること、例えば、暗号機能を持つソフトウェアのインターネット上での伝送が輸出と考えられることには注意すべきである。ただし、ドイツでは一般ソフトウェア通告（GSN： General Software Note）を完全に履行しており、店頭で売られるソフトウェアや自由に入手可能なソフトウェアについては輸出認可を取得する必要がない。インターネット上で配布されるソフトウェアは「自由に入手可能」とみなされる傾向があるため、オンラインで配布される暗号ソフトウェアに対しては一般的に輸出認可は必要でない。GSN のもとでは、暗号ソフトウェアのサンプルを見本市で配布することも認められている。しかし、対象となる配布形態が輸出許可の不要なケースに該当するか、GSN を入念に吟味することが重要である。BAFA は、例えば、特定のハードウェアに追加するだけのソフトウェアや、不慣れなエンドユーザではインストールできない複雑なソフトウェアのように、顧客層が限定されている暗号ソフトウェアの配布は、輸出許可が不要なケースに該当しないという立場をとっている。

事前の許可申請なしに製品の輸出を認める、いわゆる「一般的例外」も存在する。暗号製品は、「コンピュータ」や「電話通信」の一般的例外の事例について厳密に検討すべきである。もし一般的例外が適用できるならば、それによって輸出業者は大半の国々に対する輸出の認可を取得する必要がなくなり、GSN にあてはまらない場合でも暗号のオンライン配布が認められるようになる。しかし、他国に存在しているような、利用可能な「一般的なライセンス」が存在しないため、一般的には暗号を輸出する度に輸出認可を取得する必要がある。

個々の製品に対して輸出認可が必要であるかどうかを決定するのは容易ではない。このような場合、輸出業者は、「商品の認可取得の義務がない」という法的拘束力のある BAFA

---

[6] Stewart A. Baker and Paul R. Hurst, “The Limits of Trust, Cryptography, Governments, and Electronic Commerce ”, Kluwer Law International, The Hague, 1998

の決定を申請することができる。個々のライセンスや決定は許可された特定の場合にのみ適用されるが、ひとたび特定の商品や輸出先についてのライセンスが得られると、BAFAは将来的にもそれを利用し、輸出業者にさらなる輸出が可能となる法的保証を与える。

輸出認可の申請にどの程度の時間がかかるかということについて確実なことは言えないが、BAFA は OECD 加盟国への輸出許可申請については二週間以内で決定しようとしている。非 OECD 加盟国への輸出は、様々な政府機関との協議が必要であることから、時間がかかる。暗号製品の鍵長は、ライセンスを与えるかどうかの決定において重要ではない。

1.3.4 暗号の標準化動向

（1）暗号の評価基準

①暗号輸出規制に基づく技術審査の評価基準

暗号の技術審査については、明確な審査基準は公開されていない。ただし、ドイツは、規制反対派の主導的立場であり、NSA のスタンスに近いと思われる BSI が前面に出てきていないこと、暗号の強度が許可の可否の決定において必ずしも重要視されていないことから、暗号技術審査の位置づけが他の国に比べ軽いと推測される。

②ISO/IEC15408（Common Criteria）

ドイツで用いられるセキュリティ製品の評価基準として、ISO/IEC15408（CC：Common Criteria）がある（CC の概要は 1.1.4 参照）。ドイツがイギリス、フランス、オランダと協力して策定したヨーロッパの統一評価基準 ITSEC は、1991 年に欧州委員会から発行された。

CC 策定に際して、ドイツからは BSI が参加した。BSI は CC の認証機関として機能している。

（2）暗号の標準化

①ISO/IEC JTC1 SC27 による国際標準暗号

ISO/IEC JTC1 SC27 の暗号アルゴリズム国際標準の検討（概要は 1.1.4 参照）において、ドイツは、2000 年４月のロンドン会合で、暗号アルゴリズムの候補を提案した（詳細については 4 月 14 日現在で未公開）。ドイツは自国の提案の他、スイスの提案分（IBM チューリッヒ研究所）も併せて提出している。

②NESSIE

NESSIE（New European Schemes for Signature, Integrity, and Encryption）は、欧州委員会の IST Programme の一環として、2000 年１月から始まった３カ年計画のプロジェクトである。NESSIE プロジェクトの主要な目的は、多様なプラットフォーム向けの強い暗号方式によるポートフォリオの策定である。その実現のため、暗号方式を公募し、透明性の高いオープンなプロセスで評価することを予定している。

本プロジェクトの主要なメンバー８機関のうち、ドイツからは Siemens が参加している。

NESSIE では、2000 年３月８日から 2000 年９月 29 日までの期間、暗号方式を公募している。公募の対象は、共通鍵暗号（ブロック暗号）に限定した NIST の AES より広範である。図表 1-9に公募の対象と要件をまとめる。

図表 1-9　NESSIE プロジェクトの暗号方式の公募対象

公募対象		公募要件
1	Block ciphers	a) High.　Key length of at least 256 bits.　Block length at least 128 bits b) Normal.　Key length of at least 128 bits.　Block length at least 128 bits. c) Normal-Legacy.　Key length of at least 128 bits.　Block length 64 bits
2	Synchronous stream ciphers	a) High.　Key length of at least 256 bits.　Internal memory of at least 256 bits. b) Normal.　Key length of at least 128 bits.　Internal memory of at least 128 bits.
3	Self-synchronising stream ciphers	a) High.　Key length of at least 256 bits.　Internal memory of at least 256 bits. b) Normal.　Key length of at least 128 bits.　Internal memory of at least 128 bits
4	MACs（Message Authentication Codes）	The primitive should support all output lengths (in multiples of 32 bits) up to the key length (inclusive). a) High.　Key length of at least 256 bits. b) Normal.　Key length of at least 128 bits.
5	Collision-resistant hash functions	a) High.　Output length of at least 512 bits. b) Normal.　Output length of at least 256 bits.
6	One-way hash functions	These hash functions shall be preimage resistant and second preimage resistant. a) High.　Output length of at least 256 bits. b) Normal.　Output length of at least 128 bits.
7	Families of pseudo-random functions	Fixed block length of at least 128 bits. a) High.　Key length of at least 256 bits. b) Normal.　Key length of at least 128 bits.
8	Asymmetric encryption schemes	The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions.
9	Asymmetric digital signature schemes	The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions.
10	Asymmetric identification schemes	The minimal computational effort for an attack should be of the order of 2^{80} 3-DES encryptions. The probability of impersonation should be smaller than 2^{-32}.

（資料：NESSIE 暗号公募資料 https://www.cosic.esat.kuleuven.ac.be/nessie/call/）

また、この公募に合わせて、その評価基準を提案している。評価基準は、セキュリティ、インプリメンテーション、その他の３つの方向が想定されている。

［セキュリティ］

・一般的攻撃（例：exhaustive search, birthday attack）と少なくとも同程度の攻撃

・提供者によるセキュリティ上の主張に基づく評価

・固定的な環境での評価

［インプリメンテーション］

・ソフトウェアやハードウェアの能力に関する同様の提案や既存の方式との比較

・実行コードやメモリのサイズの査定

・提案された方式に関するパフォーマンスの査定

［その他］

・設計のシンプルさ、明快さ

1.4 フランス

1.4.1 暗号技術及び暗号製品に関する規制の概要

1999 年 1 月、フランスの Lionel Jospin 首相は、暗号政策の劇的な変更を発表した。新しい政策は、暗号の輸入や国内使用に関する複雑な免許制度や、暗号の国内使用における鍵登録の義務付け、政府認可による信用された第三者機関（TTP: Trusted Third Party）のシステムを廃止した。

Jospin 首相の発表は以下の通りである。「政府は自身を省みた。専門家や国際的なパートナーなど関係者との協議の結果、1996 年の法律がもたらした性質はもはや適切ではないと確信した。暗号化によって潜伏を容易にしている犯罪行為と効率的に闘うべき当局への許可を除き、フランスにおける暗号の使用は厳しく規制されている。フランスが主要な同盟国から孤立する危険性も表面化している。それゆえ政府は、フランスにおける暗号使用の完全自由化をめざす方向への抜本的な変更という選択を決断した。一方、この新しい環境における公的自由を保証し、暗号の不正使用と闘うために、当局による対処という方法を採用した。」

国会に提出された法案の要点を以下に示す。

- ワッセナー条約に基づく輸出規制の維持を目的とした規則を除き、暗号製品の使用の完全自由化を提供する。
- 暗号鍵の寄託を TTP に依存しなければならないという強制的性質は撤廃される。TTP の役割は鍵管理に限定されず、電子署名の認証のような他の機能まで拡大することができる。そのような手段や自動寄託機構へ頼ることが奨励される。TTP は、特に当局による認証を申請することができる。
- 当局が暗号の不正使用と効率的に闘うことを容認する。これに向けて、法執行機関が要求した場合、暗号化された文書の暗号化されていない写しが提出されるように、刑事上の制裁と同様の義務を設定することによって、現在の法機構を補うものとする。更に、当局の技術的能力を絶大に強化する。

それゆえ、法律は変更されなければならないが、それには数ヶ月かかる。しかし政府は、取引の機密性の保護を切望する市民を不利な立場に陥れ、電子商取引の発展を妨げる障害が、遅滞なく取り除かれることを望んでいる。そこで、政府は法改正が発表されるのを待つ一方、許容されている暗号方式の敷居値を、40bit から、専門家が高いセキュリティを保証できると考える 128bit まで引き上げた。

1.4.2 許認可の申請先、審査機関

（1）審査機関

中央情報システム安全部（SCSSI：Service Central de la sécurité des systémes d'information）は、暗号法に関するフランスの法的機関であり、申請を受け取り、資格審査を行っている。SCSSI は国防事務局（SGDN：Secretariat General De la Deffense Nationale）の傘下にあり、フランス首相の事務所に直接報告を提出している。住所は以下の通りである。

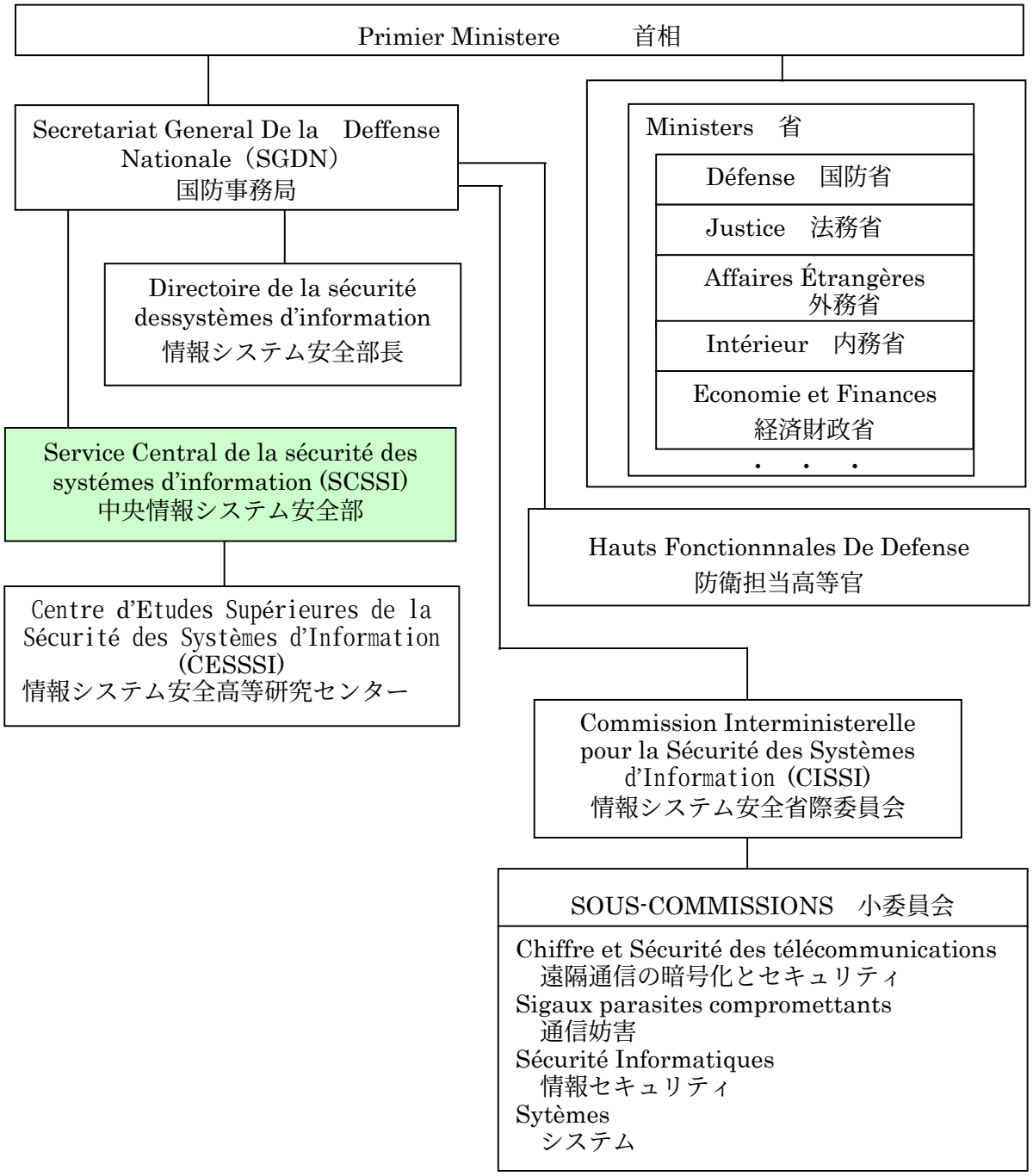
（名　称）Service Central de la sécurité des systémes d'information（SCSSI）
（連絡先）18,rue du docteur Zamenhof, 92131 lssy-les-Marlineaux, France
URL: http://www.scssi.gouv.fr

（2）組織編成

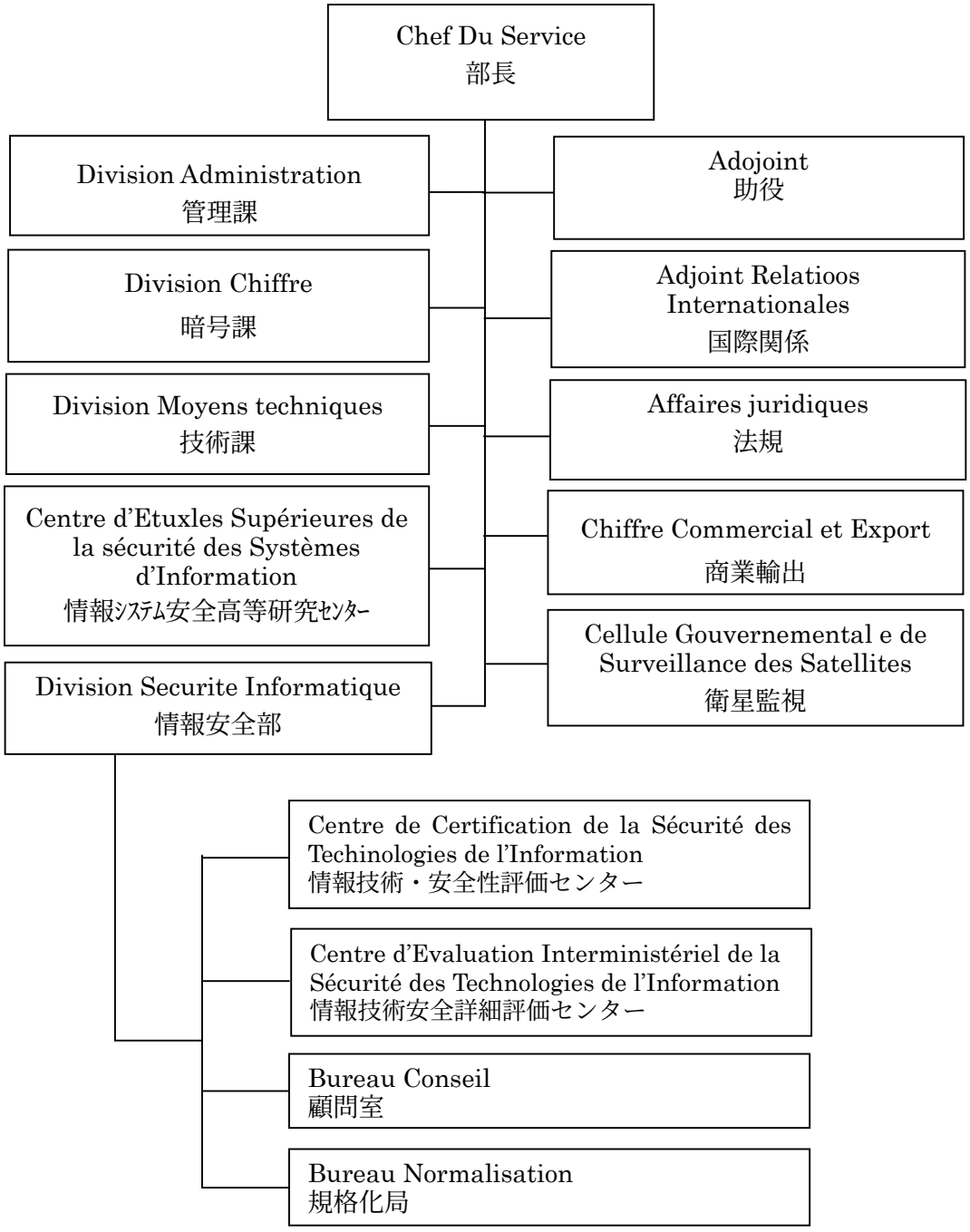
フランスでは 1986 年 3 月 3 日の政府命令により、情報システムのセキュリティは首相の管轄下に置かれることになった。当初、情報システム安全省際代表部（DISSI：Delegation Interministerielle pour la Securite des Systemes d 'Information）が設置されたが、1996 年に SGDN に全権を委譲している。「フランスの技術および産業の生産力開発と維持」を担当した DISSI は、組織としてはかなり小規模ながら、情報セキュリティの面で行政と民間のニーズに応えるよう努めた。SGDN では、防衛関連省庁の高官が各 1 名ずつ事務局を代表して政府の各部門に対応する。また、SGDN は情報システム安全省際委員会（CISSI：Commission Interministerelle pour la Sécurité des Systèmes d'Information）の政策を定める。CISSI は 4 つの小委員会（遠隔通信の暗号化とセキュリティ、通信妨害、情報セキュリティ、システム）によって構成され、構想、方法、および調達計画の調和を図る。さらに、SCSSI の情報システム安全高等研究センター（CESSSI：Centre d 'Etudes Supérieures de la Sécurité des Systèmes d'Information）が、職員の教育と科学的調査の監督にあたる。

図表 1-10に SCSSI の母体組織内の構造を、図表 1-11に SCSSI の組織図を掲載する。

図表 1-10　フランスにおける SCSSI の組織内での位置付け



図表 1-11　SCSSI の組織図



SCSSI に職員数を問い合わせたが、この点は明らかにされなかった。

しかし、1998 年 7 月に発表された記事によれば、フランス政府は中央情報システム安全部（SCSSI）の拡大を考えており、コンピューター・セキュリティの強化、暗号ソフトウェアの評価、信託を受ける第三者機関の承認、および国際指標（international measures）の調整など、増大する一方のニーズに対応できるよう支援する模様である。

SCSSI が設置された 1986 年当時は、情報システムが今日のように急速に拡大するとは誰も予想していなかったため、職員数はわずか 70～80 人に過ぎなかった。一説によると、1995 年 5 月に Gen. Jean-Louis Desvignes が指揮を取り始めて以来、SCSSI の職員数は増加中で、将来的に 300 名を超える可能性があるという。その結果、SCSSI は NSA（より正確には、NSA の中で情報システムセキュリティを担当する部署）あるいはイギリスの CESG（Communications Electronics Security Group）に匹敵する規模に達すると予想される。

また、インテリジェンス・ニュースレター（1999 年 4 月）は、SCSSI の役割および予想される職員構成について、以下のように述べている。

「（情報システム保護の）技術的側面については、SCSSI が監視を行ってきたが、今後さらに重要な役割を果たすと考えられ、独立した省庁に昇格、独自の予算とより多くのスタッフを持つようになると考えられる。」

事実、こうした大きな変化が今春にも始まる可能性がある。複数の情報筋によれば、SCSSI の職員数は 2000 年中に現行の 60 人から 50%増員される見通しである。それに伴い、パリ南部の Issy les Moulineaux を離れ、より広い事務所に移動する予定だという。

（3）ミッション

以下はホームページ上に公開されている SCSSI の職務内容である。

- 暗号保護のプロセス、情報技術に依存する製品とサービス、および違法な通信妨害への対抗措置を評価する。
- 防衛機密情報の処理に使用する機器、製品、システムの承認と認可を行う。所定の査定と認可の体制に基づき、情報技術のセキュリティの評価機関を認定する。
- 認定された評価機関が査定した製品を認証する。
- 暗号化技術と暗号化サービスの提供、ならびに使用を目的とした認定申請を査定する。
- テクノロジー、製品、システムの輸出を審査する。
- 暗号鍵を作成して、公共団体および民間団体に配布、技術サポートを行う。
- 情報システム安全高等研究センター(CESSSI)を通して、公共団体および民間団体に所属する専門家をトレーニングする。
- 公共団体および特定の企業に対して、情報システム保護に関するアドバイスを供与する。
- 情報システム保護に関する国内外の標準化活動に参加、規制に関する最新の研究を把握する。

1.4.3 許認可の審査方法

フランスは、1998 年以前の一般ソフトウェア通告を除いて、輸出管理のためのワッセナー条約に署名している。

EU と EEA（ヨーロッパ経済地域）以外の国からの暗号の輸入と輸出は 1996 年 7 月 26 日の法律とそれを履行するための法令によって規制されている。EU、EEA 内からの輸入は自由である。

輸出に関しては、暗号が個人によって私的な利用のために使われる場合は、ユーザの申請が輸出の申請となる。つまり、出荷時の申請は仮の輸出申請となる。

1999 年 3 月 17 日の法令 99-200 は、事前の手続きを必要としない暗号のカテゴリーを記している。1999 年 3 月 17 日の法令 99-199 では、（もはや事前の許可でなく）事前の申告が必要とされるカテゴリーが記されている。これらの法令は 1998 年 3 月 23 日の法令 98-206 と 98-207 に置き換えられたものであり、以下の図表 1-12にまとめられている。

図表 1-12　フランスの暗号製品の扱い（2000 年 2 月 17 日時点）

機能	手続不要	申告	認可
認証のみ	使用	輸入、輸出、供給	
鍵長が 40bit 以下の機密性のある暗号	使用、輸入	供給	輸出*
鍵長が 40～128bit の長さまでの機密性のある暗号	使用、輸入（私的な使用に限る）	使用、輸入（私的でない使用）、供給	輸出
アナログ暗号 （例：ファックス機器）	使用、輸出、輸入	供給	
データを暗号化する際ユーザが暗号を利用できない場合の様々な特別のアプリケーション	供給、使用、輸出、輸入		
国による公的招聘に伴う暗号装置	使用、輸出、輸入		
その他			供給、利用、輸出、輸入

*）出典元では、「確証がない」としている

（資料：Bert Jaap Koops; ”Crypto Law Survey”, http://cwis.kub.nl/%7Efrw/people/koops/cls2.htm）

1.4.4 暗号の標準化動向

（1）暗号の評価基準

①暗号輸出規制に基づく技術審査の評価基準

暗号の技術審査については、明確な審査基準は公開されていない。なお、フランスでは、他の国と異なり、輸出ライセンスの許可・不許可の判定と暗号の技術審査の両方を SCSSI が行う。

②ISO/IEC15408（Common Criteria）

フランスで用いられるセキュリティ製品の評価基準として、ISO/IEC15408（CC：Common Criteria）がある（CC の概要は 1.1.4 参照）。フランスがイギリス、ドイツ、オランダと協力して策定した統一評価基準 ITSEC は、1991 年に欧州委員会から発行された。CC 策定に際して、フランスからは SCSSI が参加した。SCSSI は CC の認証機関として機能している。

（2）暗号の標準化

①ISO/IEC JTC1 SC27 による国際標準暗号

ISO/IEC JTC1 SC27 の暗号アルゴリズム国際標準（概要は 1.1.4 参照）において、2000 年４月のロンドン会合で、フランスは暗号アルゴリズムの候補を提案しなかった（詳細については 4 月 14 日現在で未公開）。

②NESSIE

NESSIE（概要は 1.3.4 参照）では、本プロジェクトの主要なメンバー８機関のうち、フランスからは Ecole Normale Superieure が参加している。

1.5 イギリス

1.5.1 暗号技術及び暗号製品に関する規制の概要

現在のイギリスでは、国内における暗号製品の使用や輸入に関する規制はない。

イギリスは、暗号に対する規制やキーエスクローを推進しているアメリカを最も強く支持してきた。しかし、1999 年 3 月、Tony Blair 首相は産業界の代表者と会見し、政府がキーエスクローをライセンシングの条件に結びつける施策を止めることを発表した。産業界と政府によるタスクフォースは､法の施行を助けるための他の方法を検討する｡ただし、他の方法十分でない場合には、キーエスクローが採用される可能性もある。

イギリスは、ワッセナー条約と EU デュアルユース規制リストの堅持のため、暗号に関する輸出規制を維持している｡イギリスは 1998 年 12 月に発表されたワッセナーデュアルユース規制リストに関する改訂を強く支持した｡輸出規制は、1994 年制定の製品輸出に関する制度（1996 年の「デュアルユースと関係製品に関する規制」によって改訂）に基づいて実行されている。

許認可の担当局は、貿易産業省（DTI：Department of Trade and Industry）の輸出管理局（ECO：Export Control Organization）である。”Strategic Export Control White Paper”によると、有形の暗号製品からインターネット上の暗号化プログラムという無形の輸出まで規制対象を広げる段階に至った、と説明されている。

1998 年 1 月､DTI は､暗号機能を含むパソコンのための‘ Open General Export License ’を公認した。ただし、この特別許可には、オンラインの音声暗号化／復号プログラムは含まれていない。

1999 年 7 月、政府は、電気通信法案（Electronic Communications Bill）の草案と一緒に、「電子商取引の促進:貿易産業委員会の報告に対する政府の回答及び法案草案に関する解説」という新しい協議文書を発行した。本法草案の第 10 条は、暗号鍵の開示を要求する権限を含んでいる。暗号化された資料の合法的な入手を目的として、暗号化された情報を明瞭な形（つまり、暗号化や同様の処理がなされる前の状態）で提出することや、鍵を開示することを要求する通知を、鍵の持ち主に送ることができる。ただし、認証専用で、他の目的（例えば機密保持）には事実上使われない鍵については、開示を要求できない。通知は、国務大臣や判事、警察官のような適切な当局（暗号化された資料がどの権限に基づいて得られたかに依存する）によって認可される必要がある。そのような通知に従わない場合は、懲役 2 年以下の犯罪となる。鍵の所有の可能性を示す十分な情報を提供していた場合には、鍵を持っていないことの証明が弁護になる。また、鍵を開示するのが実現可能になり次第すぐにそれを提出する意向であれば、今は理論上実現不可能であることの証

明が弁護になる。

鍵を提出させる通知が、通知を送付した事実や通知の内容、その遂行時になされたことについて秘密にするよう要求している場合、他人にこのことを内報するのは懲役５年以下（法的助言者に情報を流すような弁護行為も含めて）の罪に当たる。通知を通して得られた鍵の使用を制限するために、多用な安全保護策が提案されている。この権限の履行に際しては実行の規範が示され、権限の使用を監視するために委員が任命されるだろう。

政府は、法の執行を助け、適正な認証のもとで復号鍵にアクセスする技術支援センター（Technical Assistance Center）の設立を決定した。

キーエスクローは法案草案に含まれていないが、登録済み暗号サービスプロバイダ（Registered Cryptography Service Provider）に認証される条件として、キーエスクローへの対応が採り上げられる可能性もある。

1.5.2 許認可の申請先、審査機関

（1）審査機関

イギリスにおいて輸出申請する機関の住所は、以下の通りである。

（名　称）DTI（Department of Trade and Industry）　（貿易産業省）
ECO（Export Control Organization）　（輸出管理局）

（連絡先）4 Abbey Orchard Street, London, SWIP 2HT
TEL: 020-7215-8070　FAX: 02-0-7215-0558
URL: http://www.dti.gov.uk/export.control

また、その際、暗号の技術審査をサポートするのが、CECG（Communications-Electronic Security Group：通信電気セキュリティグループ）である。

（名　称）CECG（Communications-Electronics Security Group）

（連絡先）The Marketing Group
Communications-Electronics Security Group
PO Box 144, Cheltenham, Gloucestershire GL52 5UE
Tel: 01242 237323　Fax: 01242 257520
Email: enquiries@cesg.gov.uk - for general enquiries
brochures@cesg.gov.uk - to request copies of our brochures
policy@cesg.gov.uk - for further information about our policy documentation
URL://www.cecg.gov.uk/

（2）組織編成

ECO の組織図の概要は図表 1-13の通りである。ECO には約 20 名が勤務する。
また、CECG については、明確な情報が得られなかった。

図表 1-13　ECO の組織構成

輸出管理局（局長）
●認可グループ
・認可グループ長
・軍事物資、小火器、個別オープンライセンスなどの認可部門担当
・産業用のデュアルユースの認可部門、国連制裁などの担当
・ビジネス支援チーム、ビジネス・プラニング品質と統計、認可受付、保管と検索
●テクノロジー・チーム
・テクノロジー・チーム長
・認可手続作業、格付けサービス担当
・非拡散関連の技術サポート、申請受諾およびサービス担当
・告知活動、ヘルプライン(020 7 215 8070)、オープンライセンス準拠、苦情受付
●政策
・戦略的貿易管理、武器の禁輸措置と貿易制裁、補助立法、
MPST（多目的支援チーム）ケースワーク、一般オープンライセンス、
および輸出許可情報の開示に関するイギリスおよび欧州連合の政策展開に対する
DTI（貿易産業省）の取り組みの調整
輸出管理および非拡散法案担当チーム
・戦略的輸出管理に関する主要法規の検討、戦略的輸出管理白書、
不可避手段を用いた技術移転に対する施策
●統制
・輸出管理の統制に関する問題、関税および物品税との連携
●運営サポート
・理事会、財政予算の管理、監視、調達、人事、登録、設備に対する運営サポート

（3）ミッション

a)ECO

ECO は、多種多様な製品、構成部品、予備部品、およびテクノロジーの輸出許可を検討し、承認または不承認を決定する。以下の項目が対象となる。

－　武器、弾薬、爆弾、戦車、画像化装置などの軍用装備
－　軍用機および軍艦、核物質を含む核関連物資、原子炉および核燃料加工工場
－　デュアルユース、すなわち、特定の物質、工作機械、電子装置、コンピュータ、遠隔通信装置、暗号製品、センサーおよびレーダー、航行および航空電子工学機器、海洋機器および宇宙推進装置など、民間向け設計ながら軍事目的に転用可能な製品
－　化学兵器用前駆物質、その関連装置とテクノロジー
－　特定の微生物、生物機器とその関連技術、
－　大量破壊兵器およびその発射用ミサイル用プログラムの作成に使用する製品

輸出その他の活動のなかに、特定の出荷先にのみ規制が行われるケースがある。たとえば、国連(UN)の武器禁輸措置、ならびに欧州連合(EU)や国連(UN)の貿易制裁適用地域がこれにあてはまる。

b)CESG

CECG は、GCHQ（Government Communications Headquarters：政府通信本部）に属する機関であるが、セキュリティの保護という役割が明確に定義された独自のグループとして運営されている。

CECG のタスクは、暗号技術やセキュリティを軸にした政府のサポートであり、具体的には以下の項目が挙げられている。

・イギリス政府の情報セキュリティポリシーの策定支援
・ポリシーの実現について、政府や公的機関のオフィシャルなユーザに対するアドバイスやコンサルティングの提供
・政府が使用する暗号製品の開発
・政府の仕様に合わせた暗号製品を使った、商用開発者への支援
・トレーニングコースの運用
・政府向けの暗号製品やシステムについての消費者への供給

1.5.3 許認可の審査方法

DTI によると、「輸出の認可は DTI に申請することによって得られる」としている。しかし、決定プロセスを早めるため、DTI に対する申請を伝えると同時に、CESG に申請のファックスを送るケースも実際には見られる。CESG は申請内容を検討し、DTI の見地についてアドバイスする。

DTI は一般的に CESG の忠告に従い、CESG が認めない輸出項目を認可することはない。1998 年 1 月に、DTI は暗号化機能を備えたパソコンに対して公開一般輸出許可証を認可した。この認可はオンラインの音声による暗号化／解読プログラムを扱っていない。

1.5.4 暗号の標準化動向

（1）暗号の評価基準

①暗号輸出規制に基づく技術審査の評価基準

暗号の技術審査については、明確な審査基準は公開されていない。

②ISO/IEC15408（Common Criteria）

イギリスで用いられるセキュリティ製品の評価基準として、ISO/IEC15408（CC：Common Criteria）がある（CC の概要は 1.1.4 参照）。イギリスがフランス、ドイツ、オランダと協力して策定した統一評価基準 ITSEC は、1991 年に欧州委員会から発行された。CC 策定に際して、イギリスからは CESG が参加した。CESG が CC の認証機関として機能している。

（2）暗号の標準化

①ISO/IEC JTC1 SC27 による国際標準暗号

ISO/IEC JTC1 SC27 の暗号アルゴリズム国際標準（概要は 1.1.4 参照）については、2000 年４月のロンドン会合で、イギリスは、暗号アルゴリズムの国際標準化を提案したにもかかわらず、候補を提案しなかった（詳細については 4 月 14 日現在で未公開）。

②NESSIE

NESSIE（概要は 1.3.4 参照）では、本プロジェクトの主要なメンバー８機関のうち、イギリスからは Royal Holloway, University of London が参加している。

2．暗号規制に対する産業界の考え方

本章では、多方面の産業界が、暗号技術や暗号製品の輸出入の規制に対してどのように考えているのかを説明したものである。文献やインターネットから得た専門家らのコメントや関連企業の意見が含まれている。多くは、アメリカ政府の政策の変更から生じたものであるが、明白に国際的な意見を反映している。それによると、暗号技術や製品の輸出入への規制緩和もしくは撤廃を望む傾向が明白である。

2.1 米州（アメリカ、カナダ）

以下に、米州における業界関係者のコメントを紹介する。

●Jim Bizos（RSA Secrurity 会長）
「コンピュータ業界が暗号技術規定を心配する必要はなくなる。政府は今回、後戻りできないところまで来てしまった。」

●ハイテク産業の職員
「強い暗号の輸出規制の緩和は、ただ単にソフト企業の進展だけでなく、詮索好きな者たち、たとえそれが犯罪者や政府の役人であろうとも、彼らからプライベートのデジタル情報を保護する方向への歴史的な変化である。それが、水曜日の発表を祝った、ハイテク産業の職員や成長を続けるインターネットプライバシーの動向筋の見解である。」

●Ed Gillespie 氏（先導的な暗号の専門グループの一つである Americans for Computer Privacy の エグゼクティブディレクター）
「新しい規制は、アメリカにとってきわめて重要であるセキュリティと警察機構の双方のニーズを保護する一方で、情報化時代における経済的な現実を浮き彫りにしたものになった。」

●Piper Cole 氏（Sun Microsystems 社副社長）
「新しい規制は、ワシントンで徐々に強力な力をつけている技術産業の影響力を証明している。ハイテクのロビイストは、インターネットにアクセスできる人ならば暗号化のソフトはアメリカ以外の国でもう入手できると､政府をうまく説得した。『今だに暗号化を使用していない犯罪者はかなり頭が悪いと思っていい』」
「産業界の専門家らは、商務省の輸出管理事務局の変化で、データスクランブリング製品

をより広い範囲で使用すること、簡単に使えるようにすることを促進するであろう。今、もっとも普及している暗号製品でもまだ扱いにくく、詮索好きな他者から電子メールを守りたい消費者がすぐに使える製品ではない。」

●Eric Schmidt 氏（Novell 社会長）
「この発表は、インターネットの次の大成長時代への段階を明白に位置付けた。これからも政府は、暗号技術を外国の政府や軍に販売する際、企業に許可を求めるよう要求し、また、テロリズムを援助していると非難されている７カ国（イラン、イラク、リビア、シリア、スーダン、北朝鮮、キューバ）に対する販売の禁止を継続するであろう。以前、政権は、最も強力な暗号技術について、海外における特定の産業への販売許可しか与えず、他の海外の顧客への販売は、通常の 128bit プログラムに比べ極めて弱い、いわゆる 56bit の暗号製品に限られていた。」

●アメリカ連合通信社（AP 通信）及びロイターによる本調査への寄稿
「新しい規定は、Linux オペレーティニグシステムを使用している人達のような、プログラムのソースコードを作ることができるコンピュータープログラマの中で増大するオープン・ソース・ムーブメントをも扱おうと努めている。新しい規定の下では、暗号のソースコードが公に入手でき、その使用に際してロイヤリティが課金されないのであれば、暗号は輸出規制の対象にはならない。暗号のオープン・ソースプログラムを公開している人達は、暗号、またはその暗号が公開されている Web サイトのアドレスを政府に送る必要がある。議会は、古く厳しい輸出規定をくつがえすと脅していたが、改訂された規定が立法措置に向けたどのような勢いをも排除したように見えた。Bob Goodlatte 議員や R-Va 議員は、古い輸出規制を緩和する法案の主な後援者だが、立法者は引き続き政権の行動を監視続けるであろうと語った。『議会は、今日発表された規定が正しく、またよりよい方法で実行されるか、引き続き注意深く監視していく。そのために、もし規制のためにアメリカの企業が世界市場で十分に競争できないのであれば、議会は、下院 850（輸出改正立法措置）をいつでも取り上げる姿勢を取っている。』」

シリコンバレーからの強力な圧力に屈し、Clinton 政権は、データ暗号技術 ― 内密にするために電子メールをスクランブルするソフトウェア ― に対する輸出規制の大半を撤廃した。ハイテク産業の重役やロビイスト達は、暗号が簡単に手に入るようになることによってテロリストや他の犯罪者による情報のやり取りが秘匿化されてしまうのを恐れた法執行機関や国家安全保障機関の役人達と、内幕で戦いを繰り広げていた。おおかたの産業界の代表者達は、この新しい規制に満足の意を表わし、これらは、アメリカの企業がもっと効率よく世界市場で競争できる手助けをするであろうと述べている。

改正された規定は、多くのアメリカ企業にとってコスト削減や新しいビジネスの機会を意味している。

●Rick Miller 氏（Microsoft 社スポークスマン）

「以前の政府の暗号輸出規制は、オペレーティングシステムのWindows95やWindows98、またはブラウザの Internet Explore 用に、アメリカ国内版と海外版の異なるバージョンを制作せざるをえず、ソフト開発に多大なるコストがかかった。我々は、失った製品販売額を計算することはできないが、海外の顧客が本当に暗号を求めていたこと、また、我々がそれらの製品を持っていなかったため彼等が我々の製品を買えなかったこととを知っている。」

また、ハイテク企業の職員達は、古い規定が、厳重な輸出統制のない他国のソフト開発者達との競争を妨げたため、彼等を不利にしたと不平を訴えていた。

●Bill Larson 氏（Network Associates 社会長兼最高経営責任者）

「古い規定が、メキシコにある銀行にデータ暗号技術の販売を禁じたため、1999 年の第４四半期だけで当社は数十万ドルの損をした。また、古い規定は、海外に基盤がある多国籍企業、例えば、Sony 社や Daimler Chrysler 社に提供するのを妨げた。」

変化していくソフト市場の眺望を反映し、産業界は、“ 市販ソフト ”の定義に、一括の製品だけでなく、インターネットで販売されているソフトや、ネットワークサーバにあり顧客が使用につき支払う基準で販売されているソフト（両方とも増加しつつあるよくある現象）を含むように強く圧力をかけた。最後には、Clinton 政権はその大半を受諾した。

●Dan Cooperman 氏（Oracle 社首席副頭取兼総顧問）

「これは躍進である。新しい政策は、初めてオンラインの流通ルートを容認した。オンラインでの販売やオンラインの流通ルートは、我らの未来のビジネスを活発にしていくであろう。これで、我々は、全製品の一つ一つに世界的モデルを履行できるようになる。」

いくつかの産業代表者達は、まだ、輸出規制の複雑さに懸念を示している。

●Piper Cole 氏（Sun Microsystems 社世界公共政策副総裁）

「確かに、大きいステップだが、私は完全勝利だとは思わない。規制は、まだ少し複雑で、顧客が政府か非政府か、市販製品か非市販製品か、それぞれによって異なった手続きや調査期間がある。私は、さらなる大きな変更は必要ないと思うが、合理化また簡素化する余地は十分にある。Clinton 政権は、一年以内に再検討することを約束した。」

市民自由意志論者達も同じ論点を上げた。

●David Sobel 氏（Electronic Privacy Information Center　総顧問）
「私は、この前進の意味を過小評価したくはない。しかし、我々の結論としては、これは、統制解除ではない。まだ、とても複雑な認可までの過程が残っている。我々の考えでは、暗号ソフトは、ワードプロセッサやスプレッドシートのソフトと異なって扱われるべきではない。昨日発表された変更は、すべて例外として記載されている。それらの詳細に述べられている例外に当てはまらなければ、まだ古い制度の中である。」

●Cindy Cohn 氏（Electronic Frontier Foundation と仕事をしている弁護士、かつオンライン市民自由論者のロビイスト）
「新しい規制は、インターネットで新しい暗号ソフトを自由に共有することを妨げている。」
　Cohn 氏は、インターネットに新しい暗号ソフトを載せるのに政府の許可が必要という規定のため、憲法第一箇条が侵害されているとして、６年前政府を告訴したカルフォニア州立大学バークレー校の数学者 Dan Bernstein 氏の代理人でもある。

●Barry Steinhardt 氏（ACLU　全米市民自由連合　アソシエートディレクター）
「強力な暗号技術を使って製品をどう輸出し、どう利用するかを、米政府が監視できる力はそのまま残っている。米政府はごくシンプルな規制撤廃に踏み切るのをいやがっている。幻を追いかけることをやめようとしない NSA や FBI からの圧力のせいだろう。今回の規制新ルールは、一歩前進だが、迷路を築いている。その迷路を歩けるのは弁護士の一群を抱えた者だけだ。」

●Cole 氏（Sun Microsystems 社）
「新しい規定は、研究者やインターネット上で公開された新しいアルゴリズムを選択する研究者や他の人々を保護するであろう。」
　彼女は、掲示者が政府にインターネットのアドレスを送付さえすれば、そこに掲示されている“ オープンソース ”ソフトへの統制が特別に取り除かれるという一部節を例証した。

　共和党が支持する、暗号化輸出を自由化する法案が提出された 1995 年から、法案は徐々に強い支持を得てきた。共和党の Bob Goodlatte 議員、R-Va 議員が著した一つの法案は、Zoe Lofgrent 議員のような著名なベイエリアの民主党員も含めた、285 人の支援者により議員評決への態勢ができた。Goodlatte 議員は、政権が暗号の問題について 180 度転換したことを賞賛した。しかし、彼は、最後の突きを逃すわけにはいかなかった。「私は、彼等がこの問題に対して２～３年遅かったことが残念である。彼等は、イスラエルのような国にアメリカの強力な競争相手を作らせてしまったからだ。」と言った。

2.2 欧州（ドイツ、フランス、イギリス）

以下に、欧州の暗号政策に対する業界関係者のコメントを紹介する。

●Institutional Investor, Inc.記者, 1999 年 8 月 30 日
「つい先日の国内法改正にともない、フランス企業は鍵長 128bit までの暗号を使用できるようになった。1996 年に制定された暗号法のもとで、これまでフランス企業は、最長 40bit の暗号しか使用できずにいた。パリの Baker & McKenzie 社で、電子商取引を担当する Pascal Gaudillere 弁護士は、『オンライン・セキュリティを強化するには、使用する暗号レベルを高める必要がある』と述べた。また、同社の他の弁護士によれば、金融サービス関連企業は需要さえ見込まれるなら、さらに高いレベルの暗号化を認可するよう、フランス政府に働きかけるだろうという。アメリカ政府のスポークスマンの一人は、ヨーロッパには経済協力開発機構（OECD）のように、強力な暗号化技術の利用と市場主導による暗号手法の開発を支持するグループが存在すると指摘した。

電子商取引を促進しセキュリティを強化するため、より信頼性の高い暗号を導入することでは、ヨーロッパ諸国はアメリカより意欲的である。『現在のところ、フランスで鍵長 128bit の暗号を導入する企業は、このような高レベルの暗号使用の認可を受けた第三者機関を利用しなければならない』と Gaudillere 弁護士は述べた。暗号を巡るフランス国内の議論は、アメリカで盛んになりつつある議論に生き写しである。多くのアメリカ企業は、重要な財務データの送信に高レベルのセキュリティを導入すれば、顧客の信頼を獲得できるため、強力な暗号技術の輸出を望んでいる。一方、法執行機関はセキュリティ上の理由から、強力な暗号を解読する手段を望んでいる」

「6 月 2 日、Gerard Schroder 独首相は閣議を召集した。この閣議で、ドイツの暗号政策の指針を策定する 4 頁の文書が仕上がり、暗号化規制の緩和が明確に打ち出された。ドイツの“ Eckpunkte der Deutschen Kryptopolitik ”というこの法案は、内務省と経済技術省のスタッフが共同で草案を作成、5 つの点を改正して政策にまとめあげた。第 1 に、『連邦政府は、ドイツ国内における暗号ソフトウェア利用に制限を加える意図を持たない。これは、暗号化技術がより効率的な情報保護手段を提供し、ひいてはオンライン商取引を促進するとともに、業務上の機密をさらに堅固に保護するという認識による』と明記している。第 2 に、連邦機関が市場に出回るソフトを管理する形で、暗号ツールの信頼性を確保するという政府方針を打ち出した。第 3 に、民間部門に主導権を握らせるという政府の意向が示された。ただし、その詳細は明らかにされていない。経済技術省のインテリジェン

ス・ニュースレター（Intelligence Newsletter）によれば、『暗号技術に特化した新興企業に対し、財政支援を行うための法整備も含まれるだろう』という。第 4 のポイントは、長距離通信を監視する政府機関に関するもので、それらの機関の業務に規制緩和が支障を及ぼさないよう配慮した。今後 2 年間、政府は規制緩和に伴う問題点を検討して、ゆくゆくは見直しを行う方針である。最後のポイントでは国際協力に触れており、この点に関するドイツ内閣の積極的な姿勢がうかがえる。ブリュッセルの外交筋によれば、ドイツの政策は、Lionel Jospin 仏首相が派遣した代表団と合同で練り上げられた。置かれた状況はそれぞれ異なるものの、わずか数ヶ月の間に、フランスとドイツはきわめて似かよった基本政策を取り入れたことになる。」

●Samoera Jacobs 氏（Global Sign 法務担当副社長）
［フランス政府が使用できる暗号製品の鍵長を 40bit から 128bit に上げ、管理機関の従業員に対するセキュリティ上の条件をなくすことについて］
「われわれは顧客の電子鍵を保管しない。我々のような資格認証機関が鍵を保管することは、セキュリティの侵害になりかねない（つまり、法律上の進歩はわずかな影響力しか持たない)」
「政府は、認証機関がメッセージの復号技術をを持つ個人（例：ユーザ本人）の協力を要請する権利を与えるような法律の制定を促進し、それによって、重要なデータを引き出すことができるような制度を整える可能性がある。そして、非協力者に対して法的な罰則を適用することも考えられる」

●Fridiric Saint-Joigy 氏（Data Fellow French　ゼネラルマネージャ）
［暗号政策変更後のフランスにおいて暗号製品販売に乗り出して］
「ルールが簡単になった結果、フランスで 128bit の暗号技術を販売することに青信号が灯った。」

（Steve Gold; Newsbytes1999.10.1）

●Yaman Akdeniz 氏（Cyber-Rights & Cyber-Liberties(UK)ディレクター）
［イギリスで Key Escrow が検討されていることについて（1999/11/03 現在)］
「電子通信法のパートⅢは法執行機関の意見が取り扱われて、議論を呼ぶだろう。政府からは、暗号は法執行機関にとって大きな問題であることを示すため、特に、実質上証拠がないことが採り上げられるだろう。」

（NEWSWIRE1999.11.03）

●Caspar Bowden 氏（Foundation for information Policy Research　ディレクター）

［イギリス政府が提案した RIP[7]（Regulation of Investigatory Powers）法案について］

「この法案はインターネット上でのプライバシーを守る暗号を使う人をだれでも犯罪者にすることができる。」

（The Daily Telegraph,2000.02.24）

「もし、あなたが復号鍵をなくしたら、あなたは２年まで投獄されるのだ。」

「e-ビジネスにとって法案が意味することは、暗号を使うどの企業でも法的に有罪となる危険性があるということだ。e-ビジネスの法律家たちは企業に自らを覆い隠すようアドバイスしなければならない。ここにはキーエスクローも組み込まれるだろう。」

（James Middleton; Network News, 2000.03.8）

[7] 2000 年 2 月にイギリス政府が提案した法案。法執行機関に通信を傍受したり、暗号文の復号に必要な鍵の開示を利用者に要求できる権利を与える。

3．国内において利用可能な暗号製品

諸外国の暗号輸出規制を踏まえ、我が国において現在利用可能な暗号製品に関する情報を収集し、そのリストを作成した。暗号製品の構成は以下のように設定した。

＜暗号製品の構成＞

（１）暗号製品

①電子メール

②暗号 Web／ブラウザ

③データ／ファイル暗号化、暗号化装置等

④暗号ライブラリ・暗号ツールキット

（２）VPN（Virtural Private Network）

（３）認証製品

①PKI（Public Key Infrastructure）

②電子署名

③ワンタイムパスワード

（４）IC カード

（５）電子商取引

①電子決済ツール

②不正コピー防止

また、各製品の属性情報として、以下の項目を調査した。

（１）製品名

（２）開発元

（３）国内販売窓口（複数の事業者と契約している場合は、代表例を示す）

（４）暗号アルゴリズム・鍵長

（５）標準化対応

（６）製品概要

調査結果を図表３－１に示す。なお、調査結果は 1999 年 11 月実施時点の情報であり、最新の情報ではないことに留意する必要がある。ただし、開発元・国内販売窓口については、利用者のアクセスメリットを考慮し、可能な限り 2000 年２月時点の情報にアップデートしている。

図表３－１　国内で利用可能な暗号製品リスト（1999 年 10 月時点）

（1）暗号化製品

①暗号メール

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	AsGentIT	CYLINK, Algorithmic Reserach	アズジェント	共通鍵 公開鍵	DES(56bit) RSA(1024bit)		暗号メール ソフトウェア 無償ダウンロード可
	CryptoPlug for EUDORA for MS Exchange / Outlook	アドバンス	アドバンス	共通鍵 鍵共有	DES(56bit) KPS		EUDORA PRO のプラグイン
	F*ENCRY	富士通ビー・エス・シー	富士通ビー・エス・シー	共通鍵	DES（56bit）		セキュア活性化方式
	FEAL for EUDORA PRO	NTTアドバンステクノロジ	NTTアドバンステクノロジ	共通鍵 公開鍵 署名	FEAL(128bit) 楕円DH(256bit) ESIGN(768bit)	MOSS PERSEUS	EUDORA PRO のプラグイン
	FJPEM	WIDE プロジェクト	－	共通鍵 公開鍵	DES（56bit） RSA	PEM	暗号メール ソフトウェア 無償ダウンロード可
	MAIL guardian	Vanguard Security	Vanguard Security Technologies	共通鍵 ハッシュ	DES(56bit), TripleDES, Blowfish MD5, SHA-1	S/MIME	暗号メール ソフトウェア
	MailSecure	Baltimore Technologies	NSJ	共通鍵 公開鍵	TripleDES RSA(512,768,1028,2048bit)	PKCS S/MIME X.509 LDAP	暗号メール ソフトウェア
	MailSecure Enterprise	Baltimore Technologies	NSJ	共通鍵 公開鍵	TripleDES(112bit) RSA(2048bit)	S/MIME X.509 LDAP	暗号メール ソフトウェア
	Misty Guard/ CryptoSign	三菱電機	三菱電機	共通鍵 公開鍵 ハッシュ	MISTY（128bit）, DES（64bit), TripleDES（192bit）, RC2（40bit） RSA（鍵長は認証書に依存） SHA-1, MD5	S/MIME X.509	暗号メール ソフトウェア 魔法便Ⅱと相互通信可能
	Netscape Messenger	Netscape Communications	日本ネットスケープコミュニケーション	共通鍵 公開鍵	RC2, RC4, RC5(各40bit) RSA(512bit)	S/MIME	ブラウザのメール機能として普及
	Outlook Express	Microsoft	マイクロソフト	共通鍵 公開鍵	RC2(40bit) RSA(512bit)	S/MIME	メールソフトとして普及
	PGP for Bisiness Security	Network Associates	ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120～168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4048bit)	PGP	メール／ファイル暗号化ソフトウェア EUDORA PROへプラグイン可能
	PGP for Personal Edition	Network Associates	ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120～168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4048bit)	PGP	メール／ファイル暗号化ソフトウェア
	PGP Policy Management Agent for SMTP	Network Associates	ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120～168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4048bit)	PGP	企業内メールのポリシー設定
	SecureWare/電子メール SecureWare Plugin for EUDORA PRO	日本電気	日本電気	共通鍵 公開鍵	DES RSA	PEM X.509	EUDORA PRO のプラグイン
	Secure Messenger	Worldtalk	アイフォー	共通鍵 公開鍵 ハッシュ	RC2(40bit) RSA(512bit) SHA1,MD5	S/MIME	MS Exchange, EUDOEA PRO等のプラグイン
	WorldSecure Serever	Worldtalk	アイフォー	共通鍵 公開鍵 署名 ハッシュ	RC2(40bit), DES(56bit) RSA(512bit) RSA(512/2048bit) SHA1, MD5	S/MIME	電子メール総合管理支援ツール ソフトウェア
	あやとり	キヤノン	キヤノン販売			MOSS	暗号メール ソフトウェア
	インターネット安心便システム	トランスコスモス	トランスコスモス	共通鍵 鍵共有	(128bit) 動的鍵教共有アルゴリズム(1024bit)		メール／ファイル暗号化ソフトウェア
	カオスメール	国際情報科学研究所	国際情報科学研究所	共通鍵	GCCカオス暗号（320bit）	S/MIME	暗号メール ソフトウェア
	セキュア電子メール	NTTアドバンステクノロジ	NTTアドバンステクノロジ	共通鍵 署名	FEAL ESIGN	MOSS	暗号メール ソフトウェア
	秘文/メール	日立ソフトウェアエンジニアリング	日立ソフトウェアエンジニアリング	共通鍵	顧客の要望に応じて対応		暗号メール ソフトウェア
	魔法便Ⅱ	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵 公開鍵	DES, RC2, RC5, Tri-DES, FEAL, MISTY（全て最大168bit） RSA(最大2048bit)	S/MIME	MS Exchange, EUDOEA PRO等のプラグイン
	魔法便ver2	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵 署名 ハッシュ	RC2(40bit) RSA(512bit) SHA-1, MD2, MD5	S/MIME	暗号化メール ソフトウェア

②暗号web/ブラウザ

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	Entrust/Direct	Entrust	エントラストジャパン				Web セキュリティプロダクト
	Internet Explore	Microsoft	マイクロソフト	共通鍵 公開鍵 鍵配送	RC2, RC4, DES(40bit) RSA Diffie-Hellman	SSL PCT PKCS	無償ダウンロード可
	MistyGuard/ TRUSTWEB	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit) RSA(1024bit)		セキュアWebアクセス
	Netscape Navigator	Netscape Communications	日本ネットスケープコミュニケーションズ	共通鍵 公開鍵 鍵配送	RC2(40bit), RC4(128bit), DES, TripleDES RSA	SSL PKCS	無償ダウンロード可
	SecureWeb Payments ToolKit	Terisa Systems	SPYRUS 東洋情報システム	共通鍵 公開鍵、 鍵配送、 署名	DES, TripleDES, RC2(40bit), RC4 RSA(512～1024bit) MD2,MD5,SHA-1	S-HTTP SSL SET X.509 PKCS	暗号ツールキット
	Stronghold Secure Web Server	C2NET	C2NET 日本ベリサイン	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES(168bit), RC4, RC2, IDEA RSA SHA,MD5		暗号機能対応Web
	WebSecure	Baltimore Technologies	NSJ	共通鍵 公開鍵 ハッシュ	RC4(40bit) RSA(512,768,1024bit) MD5	PKCS SSL	webセキュリティ

③データ/ファイル暗号化、暗号化装置等

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	4755 暗号化 アダプタ	IBM	日本IBM	共通鍵 公開鍵、 鍵配送	DES(56bit) RSA		暗号化アダプター・カード
	4758-001 PCI 暗号化コプロセッサ	IBM	日本IBM	共通鍵 公開鍵、 署名	DES(56bit) RSA(512,768,1024bit)		暗号化PCIバス・アダプターカード
	ActiveGate	Security7	アズジェント				統合型ソフトウェア
	AR CryptoCom-J	Algorithmic Research	フォーバルクリエーティブ	共通鍵 公開鍵、 鍵配送	DES(56bit) RSA		ファイル暗号化ソフトウェア
	AR KGU	Algorthmic Research	フォーバルクリエーティブ				鍵生成ソフトウェア
	Atalla A10000E NSP	Compaq Computer	コンパックコンピュータ	共通鍵	DES(56bit)		暗号化プロセッサ
	Atalla TrustMaster CSP	Compaq Computer	コンパックコンピュータ	共通鍵 公開鍵、 鍵配送 署名 ハッシュ	DES, RC2, RC4(各40bit) RSA(公開鍵 256～2048bit 鍵配送 256～512bit) DSA MD2, MD5, SHA1	FIPS140-1 Level3, UL, CSA, TUV	CryptoAPI用暗号化ハードウェア
	BOS	ビーオーエス・ネットワーク研究	ビーオーエス・ネットワーク研究所	共通鍵	TripleDES		暗号、認証、署名システム
	Choas InforGuard v3.0,v4.0	国際情報科学研究所	国際情報科学研究所	共通鍵	GCCカオス暗号(320bit)		ファイル暗号化ソフトウェア
	CryptoSwift	RAINBOW Technologies	RAINBOW Technologies	公開鍵 鍵配送 署名	RSA(384～1024bit) DSA Diffie-Hellman	SSL, X.509, S/MIME, PKCS, SET, SSH, IKE, IPSec, TLS,	暗号PCIバスボード
	D-RANS	KENWOOD, ローレルインテリジェントシステム	ローレルインテリジェントシステムズ	共通鍵 公開鍵 鍵共有	DES, SXAL/MBAL, MISTY, MULTI, FEAL RSA KPS		暗号化ソフトウェア
	DBMSセキュアアドインソフトウェア	NTTアドバンステクノロジ	NTTアドバンステクノロジ	共通鍵	FEAL		DBMS-端末間の暗号通信ミドルウェア
	FastMAP	RAINBOW Technologies	RAINBOW Technologies	公開鍵 鍵配送 署名	RSA(4～4096bit) Diffie-Hellman DSA	IPSec, IKE, ISAKMP, SSL, SET	暗号LSI
	FEAL暗号装置	NTT エレクトロニクス	NTT エレクトロニクス	共通鍵	FEAL		ハードウェア
	F-Secure Desktop	F-Secure	山田洋行	共通鍵	3key TripleDES(168bit), Blowfish(128bit)	SSH	ファイル暗号ソフトウェア
	F-Secure SSH2 /Server for UNIX /Client for Windows, Macintosh, UNIX	F-Secure	山田洋行	共通鍵 公開鍵	TripleDES(168bit), IDEA(128bit), Blowfish(128bit) RSA(1024bit)	SSH2	ソフトウェア

	FSS with VirusScan 防人	ローレルインテリジェントシステムズ	ノア・ビジネス	共通鍵	SXAL/MBAL		暗号化とアンチウィルスによるPC保護ソフトウェア
	IKEVIEW	松下電工	松下電工	共通鍵 鍵配送	DES(40,56bit), TripleDES(112,168bit) Deffie-Hellman	IPSec	リアルタイムIPSec, ISAKMP解析ソフトウェア
	InstaGate	Technologic	Technologic	共通鍵 ハッシュ	DES(56bit), TripleDES(168bit), RC2(40bit), RC4(40,128bit), Safer(128bit) MD5	ICSA S/WAN	ハードウェア
	Interceptor	Technologic	Technologic	共通鍵 ハッシュ	DES(56bit), TripleDES(168bit), RC2(40bit), RC4(40,128bit), Safer(128bit) MD5	ICSA S/WAN	ハードウェア
	interConclave	Internet Dynamics	アズジェント		RC4, RC2, DES(56bit)	X.509 SKIP	統合セキュリティソフトウェア
	Internet SR	日新電機	日新電機	共通鍵	IDEA(128～384bit)		暗号ルータ
	InterVerse	セコム情報システム	セコム情報システム	共通鍵	DES(56bit)	X.509	統合ネットワークソフトウェア
	KPS CipherPRO	アドバンス	アドバンス	共通鍵 鍵共有	DES(56bit) KPS		ファイル暗号ソフトウェア
	KPS Cipher PC Guard	アドバンス	アドバンス	共通鍵 鍵共有	DES(56bit) KPS		KPS対応暗号通信用PCカード
	KPSAGS	アドバンス	アドバンス	鍵共有	KPS		KPS鍵配送方式のIDを生成するソフトウェア
	MELWALL A3000-1	三菱電機	三菱電機	共通鍵	MISTY(128bit)		暗号アダプタハードウェア
	MELWALL H3000-1	三菱電機	三菱電機	共通鍵	MISTY(128bit)		集線型暗号装置ハードウェア
	MELWALL P3000CL	三菱電機	三菱電機	共通鍵	MISTY(128bit)		暗号ドライバソフトウェア(LAN対応)
	MELWALL P3000	三菱電機	三菱電機	共通鍵	MISTY(128bit)		暗号ドライバソフトウェア(WAN対応)
	MELWALL Mgr	三菱電機	三菱電機	共通鍵 公開鍵	MISTY(128bit) RSA(512bit)		鍵管理ソフトウェア
	MistyGuard/ CRYPTOFILE	三菱電機	三菱電機	共通鍵	MISTY(128bit)		ファイル暗号化ソフトウェア
	MY-ELLTY	松下電器産業	松下電器産業	公開鍵	松下楕円曲線暗号(160bit)		高速楕円曲線暗号ハード モジュール
	NE-Secure	ソリトンシステムズ	ソリトンシステムズ	共通鍵 公開鍵	FEAL, DES RSA		LAN間接続の暗号ルータ
	NetCryptor	RADGUARD	千代田情報機器	共通鍵 公開鍵 署名 鍵配送	DES(56bit) RSA DES-MAC Deiffie-Hellman	IPSec	暗号化専用装置
	NetLOCK	Sterling Software	日新電機	共通鍵	RC2, RC4, 独自暗号		端末間暗号通信
	NetSwift 1000 PCI Card	RAINBOW Technologies	RAINBOW Technologies	共通鍵 公開鍵 署名 鍵配送 ハッシュ	DES(56bit), TripleDES, RC4 RSA(384～1024bit) DSA Diffie-Hellman MD5, SHA-1, HMAC	IPSec DMA ISO	暗号PCIカード
	NSS-10ENI	SEMAPHORE	日本電子計算	共通鍵 公開鍵	DES(56bit) RSA		ノード間通信用暗号ボード
	nFast Crypto Accelerators	nCipher	nCipher	公開鍵 署名 鍵配送	RSA DSA Diffie-Hellman	SSL, SET, S/MIME, PKCS,	暗号ハードウェア
	nFast PCI Crypto Accelerators	nCipher	nCipher	共通鍵 公開鍵 署名 ハッシュ 鍵配送	DES(56bit), TripleDES, CAST RSA, El Gamal DSA MD2, MD5, SHA-1, HMAC, RIPEMD-160 Diffie-Hellman	SSL SET S/MIME PKCS FIPS140-1 ISO	暗号PCIハードウェア
	nFast/CA Crypto Accelerators	nCipher	nCipher	共通鍵 公開鍵 署名 ハッシュ 鍵配送	DES(56bit), TripleDES, CAST RSA, El Gamal DSA MD2, MD5, SHA-1, HMAC Diffie-Hellman	SSL SET S/MIME PKCS FIPS140-1 ISO	暗号ハードウェア
	nFast/KM Crypto Accelerators	nCipher	nCipher	共通鍵 公開鍵 署名 鍵配送 ハッシュ	DES(56bit), TripleDES, CAST RSA, El Gamal DSA MD2, MD5, SHA-1, HMAC Diffie-Hellman	SSL SET S/MIME PKCS FIPS140-1 ISO	暗号ハードウェア

	NLC0033T	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵	FEAL-8, FEAL-32	ITU-T H.233	暗号ボード ハードウェア
	NLC0061T	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵	DES(56bit), TripleDES(112bit)	ITU-T H.233	暗号ボード ハードウェア
	NSOC3	RAINBOW Technologies	RAINBOW Technologies	共通鍵 公開鍵 署名 鍵配送	DES(56bit), TripleDES, RC4 RSA DSA, 楕円DSA Diffie-Hellman, 楕円Diffie-Hellman	IPSec IKE	暗号PCIカード
	NX7000 暗号ボード	日本電気	日本電気	共通鍵 公開鍵	DES(56bit), TripleDES RSA	FIPS140-1	暗号ボード
	Page Vault	Authentica Security	ディアイティ	共通鍵	RC4(128bit)		暗号化ソフトウェア
	PGP Certificate Server	Network Associates	ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120～168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4048bit)	PGP	鍵管理サーバ ソフトウェア
	PGP for SDK	Network Associates	ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120～168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4048bit)	PGP	PGPシステム開発 モジュール
	Private Internet Exchange	Cisco Systems	日本シスコシステムズ	共通鍵	DES(56bit)	NAT	ハードウェア
	PrivateWire	Algorithmic Rsearch Cylink Company	アズジェント	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES, RC4(128bit) RSA(1024bit) SHA-1	X.509 FIPS ANSI	認証、暗号、ファイアーウォール統合 ソフトウェア
	Protect Plus	DECROS	東芝情報システム				ファイル暗号化ソフトウェア
	RSA SecurPC	RSA Security	RSAセキュリティ	共通鍵	RC4(40, 128bit)		ファイル暗号化ソフトウェア 鍵回復が可能
	SecureExplorer 防人	ローレル インテリジェントシステムズ	ローレル インテリジェントシステムズ	共通鍵	SXAL/MBAL		暗号化ソフトウェア
	SECURE PC CARD	富士通ビー・エス・シー	富士通ビー・エス・シー	共通鍵	DES(56bit)		PCカード 指紋認証版、ハードウェア版、ソフトウェア版等がある
	SecurityPack'98	システムニーズ	システムニーズ		KOAカオス暗号		PCカード
	SecureWare/ 暗号ボードマネージャ	日本電気	日本電気	共通鍵 公開鍵	DES(56bit), TripleDES RSA		暗号ボードの制御 ソフトウェア
	SecureWare/ 秘密鍵マネージャ	日本電気	日本電気	公開鍵	RSA		秘密鍵管理ソフトウェア
	SmartSafe for Notes	BIGベスト情報システム	ノア・ビジネス		SXAL/MBAL		Lotus Notes対応 ソフトウェア
	Soliton IPSec	ソリトンシステム	ソリトンシステムズ	共通鍵	DES, TripleDES, FEAL	IPSec	暗号化ソフトウェア
	SSH Internet Key Exchange	SSH Communications Security	SSH Communications Security	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES(168bit), Blowfish(40～4467bit), CAST(80bit以上) RSA SHA-1, MD5	X.509, IKE, ISKAMP, PKCS	鍵管理ソフトウェア
	TF1aEsafeD	ビー・ユー・ジー東京エレクトロンRSAセキュリティ	東京エレクトロン	共通鍵	DES(56bit)		フラッシュメモリカード
	TF1aEsafeR	ビー・ユー・ジー東京エレクトロンRSAセキュリティ	東京エレクトロン	共通鍵	RC5(0～2040bit)		フラッシュメモリカード
	VerSecure	Hewlett Packard	日本HP	共通鍵 公開鍵 鍵配送	DES(56bit), TripleDES(128bit), RC2(40～128bit), RC4(40～128bit) RSA(256～2048bit) Deiffie-Hellman(512～2048bit)	IPSec	ハードウェアベース 暗号フレームワーク
	あい言葉 「Only You」	システムニーズ	システムニーズ	共通鍵	KAO暗号		ICカード対応データ暗号化ソフトウェア
	FEAL	NTTアドバンストテクノロジ	NTTアドバンストテクノロジ	共通鍵	FEAL(128bit)		暗号化ソフトウェア
	安心金庫PRO Group Edition	トランスコスモス	トランスコスモス	共通鍵	TEE128(128bit), GOST, DES(56bit), TripleDES(168bit), Blowfish(128/160bit)		動的鍵共有アルゴリズム(1024bit)使用 ソフトウェア
	クリプティボード 710B	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵 公開鍵	DES(56bit), TripleDES 公開鍵(最大2048bit)	FIPS140-1 Level3	暗号ボード
	セキュアサービスプラットフォーム	NTTアドバンステクノロジ	NTTアドバンステクノロジ	共通鍵	FEAL, DES		認証、権限、暗号化のプラットフォーム
	秘文/SAFE	日立ソフトウェアエンジニアリング	日立ソフトウェアエンジニアリング	共通鍵	IDEA(128bit)		自動ファイル暗号ソフト

	カオスリモコンv2.2	国際情報科学研究所	国際情報科学研究所	共通鍵	GCCカオス暗号(320bit)	S/MIME PGP	暗号リモコンソフトウェア
	ノキアIPシリーズ	NOKIA	NOKIA ネットワールド インテック KDD 東芝情報システム	共通鍵	DES(56bit), RC4(40bit), FWZ-1		統合型ファイアウォール、ルータ

④暗号ライブラリ・暗号ツールキット

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	AR CryptoKit-J	Algorithmic Research	フォーバルクリエーティブ	共通鍵 公開鍵	DES RSA(最大1024bit)		暗号ツールキット
	BCERT	Technologic	RSAセキュリティ	公開鍵 ハッシュ	RSA(2048bit) MD2, MD5, SHA-1	X.509	暗号ツールキット
	BSAFE CryptoC	RSA Security	RSAセキュリティ	共通鍵 公開鍵 署名 ハッシュ 鍵配送	DES(56bit), RC2, RC4, RC5 RSA(2048bit) DSA,DSS, 楕円DSA MD,MD2,MD5,SHA-1 Diffie-Hellman	ANSI FIPS140-1 PKCS ISO IEEE ITU-T	暗号ツールキット
	BSAFE CryptoJ	RSA Security	RSAセキュリティ	共通鍵 公開鍵 署名 ハッシュ 鍵配送	DES(56bit), RC2, RC4, RC5 RSA(2048bit) DSA MD2, MD5, SHA-1 Diffie-Hellman	S/MIME PKCS IPSec SET SSL	暗号ツールキット
	BSAFE S/MIME -C	RSA Security	RSAセキュリティ	共通鍵 公開鍵 ハッシュ	DES(56bit), RC2, RC4 RSA MD5, SHA-1	S/MIME PKCS X.509	暗号ツールキット
	BSAFE SSL-C	RSA Security	RSAセキュリティ	共通鍵 公開鍵 鍵配送 ハッシュ	DES(56bit), RC4 RSA Diffie-Hellman MD5, SHA-1	S/MIME PKCS X.509	暗号ツールキット
	BSAFE SSL-J	RSA Security	RSAセキュリティ	共通鍵 公開鍵 鍵配送 ハッシュ	DES(56bit), RC4 RSA Diffie-Hellman MD5, SHA-1	SSL X.509 S/MIME	暗号ツールキット
	C/SSL	Baltimore Technologies	NSJ	共通鍵 公開鍵 ハッシュ	DES(40,56bit), TripleDES, RC4(40,128bit) RSA(1024bit) MD5, SHA	PKCS#7, #12 TLS	暗号化クラスライブラリソフトウェア
	Certicom Security Builder SDK	Certicom	Certicom	共通鍵 公開鍵 鍵配送 署名 ハッシュ	DES(56bit), TripleDES(112bit), RC4 楕円曲線暗号 Diffe-Hellman, 楕円Diffie-Hellman DSA, 楕円DSA SHA-1	ANSI X9.62, ANSI X9.63, S/MIME, TLS, PKIX, IEEEP1363	暗号ツールキット
	Certicom SSL Plus Toolkit	Certicom	Certicom	共通鍵 公開鍵 鍵配送 署名 ハッシュ	DES(56bit), TripleDES, RC4 RSA, 楕円曲線暗号 Diffie-Hellman DSA MD5, SHA-1	X.509, SSL, TLS, PKIX, ANSI X9.62, ANSI X9.63, IEEEP1363	SSL対応暗号ツールキット
	Crypto System Toolkit for Visual Basic	Baltimore Technologies	NSJ	共通鍵 公開鍵 署名 ハッシュ	DES(56bit), TripleDES(112bit), IDEA(128bit), RC2, RC4, BSA4, BSA5 RSA DSA SHA-1, MD2, MD5, BHF, BSAH, RIPEMD, RIPED-160, MDC2, HMAC	PKCS#1,#3,#5, #8,#12	暗号化クラスライブラリ
	Crypto System Toolkit v7.2	Baltimore Technologies	NSJ	共通鍵 公開鍵 署名 ハッシュ	DES(56bit), TripleDES(112bit), IDEA(128bit), RC2, RC4, BSA4, BSA5 RSA DSA SHA-1, MD2, MD5, BHF, BSAH, RIPEMD, RIPED-160, MDC2, HMAC	PKCS#1,#3,#5, #8,#12	暗号化クラスライブラリ
	CryptoWsift SoftWare Developer's Kit	RAINBOW Technologies	RAINBOW Technologies	公開鍵 署名 鍵配送	RSA(384～1024bit) DSA Diffie-Hellman	SSL, X.509, S/MIME, PKCS, SET, SSH, IKE, IPSec, TLS,	暗号ツールキット
	Entrust/Toolkit	Entrust	エントラストジャパン セコム情報システム	共通鍵 公開鍵 署名 ハッシュ 鍵配送	DES(56bit), TripleDES, CAST(40,64,80,128bit), RC2(40,128bit) RSA DSA MD5, SHA-1 Diffie-Hellman	PKCS FIPS140-1 RFC LDAP	暗号ツールキット

	IAIK-JCE	IAIK	IAIK	共通鍵 公開鍵 署名 鍵配送 ハッシュ	DES(56bit), TripleDES112bit), IDEA(64bit), Blowfish(64～448bit), GOST(64～256bit), CAST128(64～ 128bit), RC2(64bit), RC4 RSA DSA Diffie-Hellman	PKCS ANSI X.509 FIPS PUB	Javaアプリケーション用暗号ツールキット
	J/CRYPTO	Baltimore Technologies	NSJ	共通鍵 公開鍵 署名 鍵配送	DES(56bit), TripleDES(112bit), RC2, RC4(128bit) RSA(512,1024bit) DSA(512,768,1024bit) Diffie-Hellman(256,512,768,1024bit)	PKCS X.509 HMAC FIPS-186	Javaアプリケーション用暗号化クラスライブラリ
	J/SSL	Baltimore Technologies	NSJ	共通鍵 公開鍵 ハッシュ	DES(40,56bit), TripleDES, RC4(40,128bit) RSA(1024bit) MD5, SHA	PKCS TLS	暗号化クラスライブラリ
	Keymate/Crypt	日立製作所	日立製作所	共通鍵 公開鍵	MULTI2(256bit) 楕円曲線暗号		暗号ライブラリ/ソフトウェア
	Keymate/Multi Ver2	日立製作所	日立製作所	共通鍵	MULTI2(256bit)	GSS-API	暗号ライブラリ&ユーティリティソフトウェア
	KPSSDK	アドバンス	アドバンス	共通鍵 鍵配送	TripleDES(112bit), DES(56bit) KPS		KPSソフトウェア開発キット
	MY-ELLTY	松下電器産業	松下電器産業	公開鍵	松下楕円曲線暗号		暗号ソフトウェア
	PKCS暗号ソフトウェア標準キット	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵 公開鍵 ハッシュ	DES（56bit), TripleDES(168bit), RC2(50～ 1024bit), RC4（40～2048bit), MISTY1 （128bit) RSA(512～2048bit) MD2(128bit), MD5(128bit), SHA-1(160bit)	X.509 PKCS S/MIME	暗号ソフトウェアツールキット
	PowerMISTY for Windows/HP-UX	三菱電機	三菱電機	共通鍵 公開鍵 ハッシュ 署名	MISTY(128bit), DES(56,112,168bit), RC2 RSA, 楕円ELGamal MD5,MD2,SHA1,SHA RSA,DSA,楕円DSA		暗号ライブラリソフトウェア
	S/MIME暗号ソフトウエア標準キット	NTTエレクトロニクス	NTTエレクトロニクス	共通鍵 公開鍵 ハッシュ	FEAL（64,128bit), DES（56bit), TripleDES （56×3bit),RC2（40,128,256bit), RC4 （40,128,256bit), MISTY（128bit) RSA(512,768,1024,2048bit) MD2(128bit), MD5(128bit), SHA-1(160bit)	S/MIME PKCS X.509v3	S/MIMEをベースとする暗号通信ツールキット（開発中）
	Secure Messaging Toolkit	Baltimore Technologies	NSJ	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES, RC2(40,64,128bit) RSA(512～2048bit) MD5, SHA-1	S/MIME X.509 PKCS#1,#5,#7	S/MIMEをベースとする暗号通信ツールキット
	SecureWare/開発キット	日本電気	日本電気	共通鍵 公開鍵 ハッシュ	DES(56bit) RSA MD5		ソフトウェア
	Soliton IPSEC	ソリトンシステムズ	ソリトンシステムズ	共通鍵	DES(56bit), TripleDES(168bit), FEAL(64bit)	IPSEC	IPレベルの暗号ツール
	SSH IPSEC Express Tollkit	SSH	SSH			ISKAMP IPSec IKE X.509	暗号ツールキット
	SunScreenSKIP エクスポータブル版 グローバル版	Sun Microsystems	サン・マイクロシステムズ	共通鍵 ハッシュ	RC2(40bit), DES(56bit), RC4(40bit) KeyedMD5	SKIP	暗号ソフトウェアモジュール
	セキュリティライブラリ開発環境	日立製作所	日立製作所				セキュリティライブラリイ開発ソール ソフトウェア
	認証サーバ/ セキュリティライブラリ	日立製作所	日立製作所			X.509 PKCS#7 PKCS#10	セキュリティライブラリイ ソフトウェア

（2）VPN

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	AccessMaster	Bull	ブル			X.509,PKCS,PKC11	PKI,VPN ソフトウェア
	AltaVista Tunnel 98	AltaVista Software	アクセントテクノロジー	共通鍵 公開鍵 ハッシュ	RC4(40,56,128bit) RSA(512bit) MD5		ソフトウェア
	AltaVista Tunnel with FEAL	AltaVista Software	NTTアドバンストテクノロジ	共通鍵 署名	FEAL(128bit) ESIGN		VPN

	Altiga C50,C20,C10	Altiga Networks	Altiga Networks	共通鍵 公開鍵 鍵配送 ハッシュ	DES(56bit), TripleDES(168bit), RC4(40,128bit) Deiffie-Hellman MD5, SHA-1, HMAC	X.509 IPSec IKE LDAP	VPNハードウェア
	Cisco IOS Firewall	Cisco Systems	日本シスコシステムズ	共通鍵	DES(56bit), TripleDES(168bit)	IPSec	VPN対応ファイアウォールシステムソフトウェア
	CiscoPIX FireWall 500	Cisco Systems	日本シスコシステムズ	共通鍵 ハッシュ	DES(56bit), TripleDES(168bit) MD5	IPSec	暗号化 ファイアーウォール
	CRP-LANGW	NTT エレクトロニクス	NTT エレクトロニクス	共通鍵	FEAL		暗号ゲートウェイ装置
	CryptoSystem	RADGUARD	千代田情報機器	共通鍵 鍵配送 署名	DES(56bit) RSA(256bit), Deiffie-Hellman DES-MAC		VPN構築 ハードウェア
	CyberGuard Firewall	CyberGuard	日立ソフトウェアエンジニアリング			NCSC-B2認定	ファイアウォール VPN機能をオプションでサポート
	Entrust/Access	Entrust	エントラストジャパン			IPSec	リモートアクセス
	Fireless FL-50A/FL-80A	コンテック	コンテック	共通鍵	DES(56bit), RC5		ハードウェア,ソフトウェア一体型FW
	FireWall Plus V4.0	Network-1 Security	三井物産	共通鍵 ハッシュ	DES(56bit) MD4,MD5	CAPI	
	FireWall-1	CheckPoint	チェックポイント・ソフトウェア・テクノロジーズ,フォーバルクリエーティブ	共通鍵 ハッシュ	DES(56bit), TripleDES(112,168bit) SHA-1, MD5	X.509 IKE	VPN,PKI対応 ソフトウェア
	FortKnox F-1000v	Alcatel	日本アルカテル,クボタシステム開発	共通鍵	DES(56bit)	IPSEC,ISAKMP	VPNハードウェア
	F-Secure VPN	F-Secure	山田洋行	共通鍵 公開鍵	TripleDES(168bit), IDEA(128bit), Blowfish(128bit) RSA(1024bit)	SSH	VPN構築ソフトウェア
	Guardian IPSec Client	NetGuard	NetGuard	共通鍵 ハッシュ	DES(40,56bit), TripleDES(168bit) SHA	X.509 IPSec IKE	VPNソフトウェア
	Guardian IPSec VPN soft	NetGuard	NetGuard	共通鍵	DES(40,56bit), TripleDES(168bit)	X.509 IPSec IKE	VPNソフトウェア
	Guardian IPSec VPNNodeManager	NetGuard	NetGuard	共通鍵 ハッシュ	DES(40,56bit), TripleDES(168bit) SHA	X.509 IPSec	VPNソフトウェア
	IBM FireWall v3.3 AIX/WindowsNT	IBM	日本IBM	共通鍵	DES(56bit) CDMF(40bit)	IPSec	VPN対応 ファイアーウォール
	LANBASE SX20	日新電機	日新電機	共通鍵 ハッシュ	IDEA(128bit), DES(56bit:対応予定) 鍵付きMD5	IPSec	VPN対応暗号装置 ハードウェア
	net GUARDIAN	Net Guard	datacontrol 日立ソフトエンジニアリング	共通鍵 公開鍵	RC2, RC4(各40bit) RSA		VPN対応FireWall ソフトウェア
	NetCocoon Client/Server	松下電工	松下電工	共通鍵 鍵配送	DES(40,56bit), TripleDES(112,168bit) Deffie-Hellman	IPSec	VPN対応 ソフトウェア
	NetDefender	Technologic	ダイナラブ・ジャパン			IPSec X.509	ファイヤーウォール
	NEU-10ENI-BOX	SEMAPHORE	日本電子計算	共通鍵 公開鍵 ハッシュ	DES(56bit) RSA(512bit) MD5		VPN暗号化装置 ハードウェア
	OmniGuard/ PowerVPN	Axent Technologies	ソリトンシステムズ 千代田情報機器	共通鍵 鍵配送 ハッシュ	DES(56bit) TripleDES(112,168bit) Diffie-Hellman MD5		ワンタイムパスワード・暗号化VPN
	PERMIT/Client	TIMESTEP	ディアイティ	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES, RC5, Blowfish, CAST, IDEA(128bit) RSA HMAC, MD5, SHA-1	IPSEC X.509 DSA PKCS#11	VPNソフトウェア
	PERMIT/Gate	TIMESTEP	ディアイティ	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES, RC5, Blowfish, CAST, IDEA(128bit) RSA HMAC, MD5, SHA-1	IPSEC DSA FIPS-140 X.509	VPNハードウェア ゲートウェイ
	PowerVPN	AXENT Technoogies	日新電機	共通鍵	DES(56bit)		暗号通信ソフトウェア
	PusBuilder トンネルスイッチ	3com	3com	共通鍵 ハッシュ	DES(56bit), TripleDES, RC4, RC5 MD5, SHA-1	IPSec	VPNハードウェア

	Raptor FireWall RaptorRemote RaptorMobile	AXENT Technoogies	日立インフォメーションテクノロジー	共通鍵 ハッシュ 鍵配送	DES(56bit), Triple DES(米国内のみ), RC2(40bit) Keyed MD5, SHA-1, MD5 Deffie-Hellman	IPSec IKE swIPe X.509	VPN対応FireWall ソフトウェア
	Secure Connect Firewall + VPN	Lucent Technology	アセンドコミュニケーションズジャパ	共通鍵 ハッシュ	DES(56bit), TripleDES(168bit) MD5(128bit), SHA-1(160bit)	IPSec SSL	VPN構築
	SC-W001	ステラクラフト	ステラクラフト		Odo2(56bit:独自暗号)		VPN
	Secure Socket	日立製作所	日立製作所	共通鍵	MULTI2(256bit)	ISO/IEC9798 X.509	VPNシステム ソフトウェア
	SecureWare BNE	Bull	ブル	共通鍵 公開鍵	DES(56bit), TripleDES(168bit) RSA(2048bit)		VPN構築ハードウェア
	Sidewinder Security Server	Secure Computing	ネットワンシステムズ			IPSec(オプション)	VPN対応ファイアウォール
	SmartGate	V-ONE	V-ONE アスキーNT	共通鍵 公開鍵	DES(56bit) RSA		VPN アプリケーション
	SOCKSVPNver2.1	日本電気	日本電気	共通鍵 公開鍵	DES(56bit) RSA(512,768,1024bit)	ISO/IEC11770	VPN構築ソフトウェア
	SonicWALLPro	住友金属 システム開発	住友金属 システム開発	共通鍵	DES(56bit), TripleDES(168bit), RC4	Ipsec	VPN,FireWall対応 ハードウェア
	VPN-1 Accelerator Card	CheckPoint	日本IBM 日立ソフトウェアエンジニアリング 日本電気	共通鍵 ハッシュ	DES(56bit), TripleDES(168bit) MD5, SHA-1	IKE IPSec	VPN対応 ハードウェアカード
	VPN-1 SecuRemote	CheckPoint	日本IBM 日立ソフトウェアエンジニアリング 日本電気	共通鍵 公開鍵 鍵配送	DES(56bit), TripleDES(168bit), FWZ-1(48bit), CAST(40bit) RSA(512～1024bit) Diffie-Hellman(512～1024bit)	IKE SKIP IPSec X.509	リモートVPN ソフトウエア
	VPN-1 Appliance	CheckPoint	日本IBM 日立ソフトウェアエンジニアリング 日本電気	共通鍵 公開鍵 鍵配送	DES(56bit), TripleDES(168bit), FWZ-1(48bit), CAST(40bit) RSA(512～1024bit) Diffie-Hellman(512～1024bit)	IKE SKIP IPSec	VPNハードウェア
	VPN-1 GatewaySolutions	CheckPoint	Advanced Rserach of Tecnologies 日本IBM 日立ソフト 日本電気	共通鍵 公開鍵 鍵配送	DES(56bit), TripleDES(168bit), FWZ-1(48bit), CAST(40bit) RSA(512～1024bit) Diffie-Hellman(512～1024bit)	IKE SKIP IPSec X.509	VPN対応 ゲートウェイ ソフトウェア
	VPN-1 SecureClient	CheckPoint	日本IBM 日立ソフトウェアエンジニアリング 日本電気	共通鍵 公開鍵 鍵配送	DES(56bit), TripleDES(168bit), FWZ-1(48bit), CAST(40bit) RSA(512～1024bit) Diffie-Hellman(512～1024bit)	IKE SKIP IPSec X.509	VPNソフトウェア
	VPN210 VPN220 VPN230 VPN240	NOKIA	NOKIA ネットワールド インテック KDD 東芝情報システム	共通鍵	DES(56bit), RC4(40bit), FWZ-1	IPSec	VPNハードウェア
	VSU-1010/ VSU-10	ネットワールド	ネットマークス	共通鍵 ハッシュ	DES(56bit) MD5	SKIP IKE IPSec X.509	VPN対応 ハードウェア
	WatchGuard Firebox-Ⅱ	WatchGuard	千代田情報機器	共通鍵	DES(56bit), RC4	IPSec IKE	VPN対応 ファイアーウォール ソフトウェア
	WebTrends for FierWall and VPNs	WebTrends	アズジェント				VPN,FireWall対応 ソフトウェア
	秘文/SC	日立ソフトウェアエンジニアリング	日立ソフトウェアエンジニアリング	共通鍵 公開鍵	IDEA(128bit) RSA	SSL X.509	VPN構築ソフト

(3)認証製品

①PKI

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	AR Crypto Server-J	Algorithmic Research	フォーバルクリエーティブ	共通鍵 公開鍵、署名	DES RSA(512,768,1024,2048bit)		CA構築ツール
	Carassuit	日本電気	日本電気			PKCS#10, #11, #12 X.509 LDAP	PKIサーバ CA、RA機能を提供
	CertMISTY for Windows	三菱電機	三菱電機	共通鍵 ハッシュ 署名	MISTY(128bit), DES(56, 168bit), RC2(40bit) MD5, MD2, SHA1	X.509 PKCS#7, #10, #12	認証ライブラリ ソフトウェア

	Entrust/PKI	Entrust	エントラストジャパン セコム情報システム	共通鍵 公開鍵、 鍵配送 ハッシュ	CAST(64,80,128bit), DES, TripleDES, RC2(40,128bit) RSA(1024bit), DSA, Diffie-Hellman SHA-1, MD2, MD5	FIPS140-1 ISO IS15408, CC EAL3 X.509, PKIX PKCS#7, #10, #11 S/MIME IPSec ISAKMP	コンポーネント製品群の総称
	FibeCrypt	日本発条	日本発条		非公開		機械認識ファイバハードウェア
	iKey	RAINBOW Technologies	RAINBOW Technologies	公開鍵 ハッシュ	RSA MD5	IPSEC/IKE SET,SSL PKCS MilliCent eWalllet X.509 S/MIME	認証デバイス
	MistyGuard CERTMANAGER	三菱電機	三菱電機	公開鍵 署名 ハッシュ	RSA(512,1024,2048bit) RSA MD5,SHA1	X.509, PKCS, SSL,S/MINE, LDAP	認証サーバシステム
	PERMIT/Detector suite	TimeStep	ディアイティ	公開鍵、 署名	RSA(768～1024bit), DSA(option)	IPSEC PKIX X.509	認証局、 ポリシー管理 アプリケーション
	PGP Certificate Server	Network Associates	ネットワークアソシエイツ	共通鍵 公開鍵 鍵配送	TripleDES(120～168bit), IDEA(128bit), CAST(128bit) RSA(最大2048bit) Diffie-Hellman(最大4048bit)	PGP	企業向け鍵管理サーバ
	PKI-Plus SDK	Baltimore Technologies	NSJ	共通鍵 公開鍵 鍵配送 署名	DES(56bit), TripleDES(112bit), IDEA(128bit), RC2, RC4 RSA(1024,2048bit) Diffie-Hellman DSA	PKCS X.509	PKIソフトウェア
	RSA Keon Desktop	RSA Security	RSAセキュリティ	共通鍵 公開鍵	DES(56bit), TripleDES(112bit), RC5(128bit)	X.509 PKCS	PKI
	SecureWare/ 認証プラグイン	日本電気	日本電気	共通鍵 公開鍵	DES(56bit) RSA	GSS-API ISO-IEC	ソフトウェア
	UniCERT	Baltimore Technologies	NSJ	公開鍵 署名	RSA DSA, 楕円DSA	X.509 SET S/MIME SSL SEIS PKCS	PKI
	UXP/DS InfoCA V12	富士通	富士通			X.509 IKE PKCS	PKI構築ソフトウェア
	UXP/DS PKI Manager v1.0	富士通	富士通	共通鍵 ハッシュ	RSA(56bit), RC2 MD5		PKI
	イントラキーセンタ	NTTアドバンス テクノロジ	NTTアドバンス テクノロジ	共通鍵 公開鍵 署名	FEAL(128bit) 楕円Diffie-Hellman(256bit) ESIGN(768bit)	PERSEUS	プライベートCA ソフトウェア
	鬼刑事ver 2.1	横河デジタル コンピュータ	横河デジタル コンピュータ	ハッシュ	MD5		ワンタイムパスワード
	プライベートCAビルダー S/MIME用 / WEB用	NTTエレクトロニクス	NTTエレクトロニクス	公開鍵、 署名 ハッシュ	RSA(512～2048bit) SHA1,MD5(各160,128bit)	X.509 PKCS#7,#10	証明書発行局 ソフトウェア

②電子署名

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	Atalla SignMaster ISP Atalla SignMaster/PCI ISP	Compaq Computer	コンパックコンピュータ	署名 ハッシュ	RSA, MAC, DSA(各256～2048bit) MD2, MD5, SHA-1	FIPS140-1レベル3 UL CSA TUV	署名, 認証 暗号化ハードウェア BOX/PCI
	ESIGN	NTT	NTT	署名	ESIGN		電子署名ソフトウェ
	Keymate/Sign	日立製作所	日立製作所				電子署名ソフトウェ

③ワンタイムパスワード

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	OmniGuard/ Defender	AXENT Technologies	ソリトンシステムズ 千代田情報機器	共通鍵	DES(56bit)		
	CRYPTOCard	CRYPTOCard	イノテック	共通鍵	DES(56bit)		
	CrypToken for Web	アドバンス	アドバンス	鍵共有	KPS		Webへのアクセスを管理

	SAFEWORD	Secure Computing	メトロ	共通鍵	DES(56bit)	ANSI	
	SecurID	RSA Security	ニチメンデータシステム				
	SecureNet Key/ Defender	AXENT Technologies	日新電機	共通鍵	DES(56bit)		

(4)ICカード

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	ActivCard Gold	ActivCard	エヌ・シー・エルコミニケーション	共通鍵 公開鍵	DES(56bit) RSA(512,768,1024bit)	PKCS#11 X.509 SSL S/MIME	ICカード
	ARCACLAVIS for CIPHER,LOCK, NOTES,VPN	ネットタイム	ネットタイム、セコム情報システム				ICカード
	Certicom Smart Card Evaluation Toolkit	Certicom	Certicom	署名	楕円DSA(163～1024bit), DSA(163～1024bit)	ANSI X9.62 PKCS IETF X.509 ISO IEEE FIPS140-1	電子署名 ICカード
	CZ-3017	東芝	東芝	公開鍵	RSA(1024,2048bit)	ISO/IEC7816	ICカード
	GemSAFE	Gemplus	NSJ	公開鍵	RSA(512,1024bit)	PKCS#11, X.509, SSL, S/MIME, ISO7816	ICカード
	KPS Cipher Card	アドバンス	アドバンス	共通鍵 鍵共有	DES(56bit) KPS		KPS対応暗号ICカード
	各種Icカード	凸版印刷	凸版印刷			ISO7816 JISSSAP	ICカード
	SafePad	Bull	ブル	共通鍵 公開鍵	DES(56bit) RSA(1024bit)	SET C-SET	ICカード リーダ・ライタ
	SecureWare /ICカード発行キット	日本電気	日本電気	共通鍵	DES(56bit)	ISO7816 PKCS#11	ソフトウェア
	SmartAuth	ローレルインテリジェンスシステム	ローレルインテリジェンスシステムズ		独自暗号		ICカード

(5)電子商取引

①電子決済ツール

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長		標準化対応	製品概要
	Atalla PayMaster ISP Atalla PayMaster/PCI ISP	Compaq Computer	コンパックコンピュータ	共通鍵 公開鍵、署名 ハッシュ	DES(40～128bit) RSA(鍵配送:256～1024bit、署名:256～2048bit) MAC	SET FIPS140-1 Level3	クレジットカード決済 暗号化ハードウェアBOX/PCI
	Atalla WebSafe2 ISP Atalla WebSafe2/PCI ISP	Compaq Computer	コンパックコンピュータ	共通鍵 公開鍵、署名 ハッシュ	DES, RC2, RC4(各40～128bit) RSA(256～2048bit), DSA MD5, SHA1 Diffie-Hellman(鍵共有)	FIPS140-1 Level3 SSL PEM S/MIME UL CSA TUV	電子商取引 暗号化ハードウェアBOX/PCI
	CyberCash Wallet	CyberCash	サイバーキャッシュ				無償ダウンロード可
	DOSET	東洋情報システム	東洋情報システム	共通鍵 公開鍵	DES(56bit) RSA	JPO SET	クレジット用電子決済ソフトウェア
	Globeset Wallet	Globeset	Globeset			SET	WWWブラウザ等のプラグイン
	IBM Consumer Wallet	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応電子決済ソフトウェア
	IBM Payment Gareway	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応ゲートウェイソフトウェア
	IBM Payment Server	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応電子決済ソフトウェア
	IBM Payment Registry	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応電子決済ソフトウェア

	InstaBuy	CyberCash	サイバーキャッシュ				サーバ側でWallet情報を保有
	Infomerce Mail	沖電気工業	沖電気工業			SET SSL	クレジットカードによるオンライン決済
	Infomerce Store	沖電気工業	沖電気工業			SET	仮想店舗構築ソフトウェア
	Microsoft Wallet	Microsoft	マイクロソフト				WWWブラウザへのプラグイン 無償ダウンロード可
	MilliCent Wallet	MilliCent	MilliCent				無償ダウンロード可
	Net.Commerce V3	IBM	日本IBM	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応仮想モール 構築ソフトウェア
	NetPay	METHEAN	METHEAN	共通鍵 公開鍵	DES(56bit) RSA(最大2048bit)	SET JPO	SET対応電子決済ソフトウェア
	NetPay Gateway	METHEAN	METHEAN	共通鍵 公開鍵	DES(56bit) RSA	SET ISO SSL X.509 JPO PKCS CAPI/CPS	SET対応 電子財布ソフトウェア
	NetPay Marchant	METHEAN	METHEAN	共通鍵 公開鍵	DES(56bit) RSA	SET ISO SSL X.509 HTTP/MIME CAPI/CSP VAP	SET対応 ゲートウェイ ソフトウェア
	NetPay Wallet	METHEAN	METHEAN	共通鍵 公開鍵	DES(56bit) RSA	SET ISO SSL X.509 PKCS ASN1	SET対応 マーチャント ソフトウェア
	PayGateway	Trintesh	Trintesh	共通鍵 公開鍵	DES(56bit) RSA	SET	SET対応 ゲートウェイ ソフトウェア
	PayPurse	Trintesh	Trintesh			SET	SET対応電子財布ソフトウェア
	PayWare	Trintesh	Trintesh	共通鍵 公開鍵	DES(56bit) RSA	SET SSL	SET対応コマースサーバーソフトウェ
	S/PAY SET ToolKit	RSA Security	RSAセキュリティ	公開鍵	RSA	SET CCITT ISO IEEE ANSI	SET開発 ツールキット
	SecureWare/ 電子取引	日本電気	日本電気	共通鍵 公開鍵 ハッシュ	DES(56bit) RSA MD5	CII EDI	ソフトウェア
	SecureWeb Payment Source	Terisa Systems	SPYRUS 東洋情報システム	共通鍵 公開鍵 ハッシュ	DES(56bit), TripleDES, RC2(40bit), RC4 RSA(512～1024bit) MD2,MD5,SHA-1	S-HTTP SSL SET X.509 PKCS	アドオンソフト
	vGATE	VeriFone	VeriFone	共通鍵 公開鍵	DES(56bit) RSA	SET SSL	SET対応 ゲートウェイ ソフトウェア
	vPOS	VeriFone	VeriFone	共通鍵 公開鍵	DES(56bit) RSA	SET SSL	SET対応 コマース・サーバー・
	vWALLET	VeriFone	VeriFone	共通鍵 公開鍵	DES(56bit) RSA	SET SSL	SET対応電子財布ソフトウェア
	WebWallet	SPYRUS	SPYRUS			SET	電子財布ソフトウェ
	日立コマース・ ソリューション	日立製作所	日立製作所	共通鍵 公開鍵	DES(56bit) RSA	SET SECS	SET対応電子決済ソフトウェア

②不正コピー防止

	製品名	開発元	国内販売窓口	暗号アルゴリズム・鍵長	標準化対応	製品概要
	CXD3201R	Sony Electronics	Sony Electronics	共通鍵 M6(56/64bit), DES(56bit), 署名 Blowfish(56,64bit) 楕円DSA(署名)	DTCP IEEE1394 MPEG2	IEEE1394LSI
	CXD3204R CXD3205R	Sony Electronics	Sony Electronics	共通鍵 M6(56/64bit), DES(56bit), 署名 Blowfish(56,64bit) 楕円DSA(署名)	DTCP IEEE1394 MPEG2	1チップ i.LINC コントローラLSI
	MN864501	松下電器産業	松下電器産業	共通鍵 M6(56/64bit), DES(56bit), 署名 Blowfish(56,64bit) 楕円DSA(署名)	DTCP IEEE1394 MPEG2	IEEE1394LSI
	Internet secureEDI	NSJ	アドバンストシステムコンサルティング	共通鍵 RC2,RC4(各128bit) 公開鍵 RSA(1024,2048bit)		EDIソフトウェア・パッケージ

※本データは1999年11月現在で収集可能な情報から作成した。
ただし、開発元・国内販売窓口の一部については、2000年2月17日現在の情報に基づく。
※個人の提供によるもの(例:SSLeayなど)は掲載していない。

資　料　編

付録 A　最終用途の証明書、許可証及び申請

カナダと主な産業国の貿易パートナーは、許可していない最終使用、または、最終目的地への規制商品の流用や積み替えを防ぐための輸出管理制度の大部分で一致した。ただし、核また核関連の二次使用可能な品目用の必要書類は多少異なる。ある場合には、最終使用者からの政府間の保障が必要となることもある。輸出許可の資格を得ようと考えるのなら、申込者は、このような考慮をも留めておかなけれえばならない。しかし、一般に、カナダはいくつかの国際的許認可形式を最終使用保障制度に導入している。

・国際輸入証明書　[International Import Certificates (IIC)]
・最終使用証明書および／もしくは輸入許可書
　[End-use Certificates (EUC), and/or Import Licenses (IL)]
・配達確認証明書　[Delivery Verification Certificates (DV)]
・最終用途申告書　[End-use Statements (EUS)]

輸出許可申請書の手続きを手早く処理できるようにするために、輸出者は、輸出許可書を申請する前に、あらかじめ輸入者から IIC, DV, EUC, IL, または、EUS を取得するよう奨励する。これは、申請書が最短の遅れで手続きされることを確保するものである。

ある特定の状況の場合、IIC, DV, EUC, IL, または、EUS の必要性が免除されることがある。免除に関しては、詳細に説明されている以下の小区分５を参照してください。

1.　国際輸入証明書　[International Import Certificates (IIC)]

IIC が必要な時は、輸出者が、輸入者もしくは受託者に輸入国の政府から IIC を取得するよう要請しなければならない。この IIC は輸入国の政府が、出荷される商品を承知したということを意味する。さらに、IIC は、輸入国の政府に対して、商品が途中でまたは到着時に流用されないよう確保するよう警戒させる。

輸入国の当局が IIC を確認すれば、オリジナルと輸入局のコピーが輸入者に返却される。その後、輸入者はオリジナルを、カナダの輸出者に送還し、カナダの輸出者は、そのオリジナルと輸出許可申請書を共に輸出管理局（Export Controls Division）に転送しなければならないなければならない。そこで初めて、輸出許可書の手続きが始まる。輸出者は、IIC にはたいてい制限された有効期限（通常６ヵ月）があることを注意しておかなければ

ならなく， また、その有効期限内に輸出管理局（Export Controls Division）に提出しなければならない。

カナダへ輸出する際は、外国の政府がカナダの IIC を、その国の輸出許可書／免許書を発行する前に、必要とする場合がある。その際は、カナダの輸入者は、輸出管理局（Export Controls Division）に IIC を申し込む。

2. 配達確認書 [Delivery Verification Certificates (DV)]

多くの国では、IIC を発行する際、配達確認書 [Delivery Verification Certificates (DV)] をも発行する。DV は、製品が輸入国に到着したことを証明する。カナダの輸出者は、輸入国の政府から DV を取得する必要がある場合もある。DV は通常最終目的地の国の輸出または輸入管理局（Export Controls Division）が発行する。DV は、製品がカナダの輸出許可と海外で発行された IIC 両方の条件に従って配達されたことを公的に認確するものである。

カナダへの輸出の場合、外国の政府はカナダの DV を必要とするかもしれない。DV は、輸出者が、カナダの輸入者に要請し、輸入者が DV 申請書を記入し輸出管理局（Export Controls Division）に手続きのための提出する。

3. 最終用途証明書／輸入許可書 [End-use Certificates (EUC) / Import Licenses (IL)]

カナダの輸出者は、輸入者に EUC または IL の必要などちらかを指定された当局で取得するよう要請する。海外の輸入者は、その書類を、カナダの輸出者に転送し、カナダの輸出者が輸出許可申請書と共に輸出管理局へ提出する。

4. 最終用途申告書 [End-use Statements (EUS)]

どんな種類の最終用途証明書、または、他の最終用途についての公的保証書も発行しない政府もある。そんな場合は、輸入者からの最終用途申告書が受諾可能である。申告書は、輸出者のレターヘッド（コピー不可）に記載されてなければならない。また、

i. 最終使用者と輸入製品の目的、また、使用方を明らかにすること
ii. 輸出許可申請書に記述されている商品と一致すること
iii. 製品の使用が民間用か軍用かを明らかにすること
iiii. 輸入製品が流用、または、再輸出されないことを示すこと

5. 証拠書類の一般的免除

輸出管理局の考え次第では、証拠書類の必要性は免除される、特定の製品を輸出の申請者の対して以下に記載されていない限り、免除は ECL のグループ１の製品(HYPERLINK "http://www.dfait-maeci.gc.ca/~eicb/export/gr1_e.htm") にしか該当しない。輸出者は、特定の商取引が免除の対称になると思うのなら、そのように輸出許可申請書の本文に述べるべきである。

i. 個々の出荷が６千カナダドル以下

ii. 政府の省、または、機関 （すべて ECL のグループ）
政府の省とは、政府に雇われた人員で政府の行政上の機能を遂行するために働いている団体 (e.g. 防衛省や保健省)。
政府機関とは、政府が監督している公益事業団体（５０%以上政府が所有)、例えば、交通機関網、郵政、電話、電報、放送、水力発電

iii. 救助機関、救済事業のための

iv. 教育機関（e.g. 大学、学会、専門学校、研究所）

v. 一時的許可（すべて ECL のグループ）
展示会、デモンストレーション、試験目的のために製品を輸出をする際の申請用

vi. 小火器（ECL Items 2001 だけ
HYPERLINK "http://www.dfait-maeci.gc.ca/~eicb/export/gr2_e.htm" ）
ライフル銃、カービン銃、レボルバー銃、ピストル銃（ECL Items 5500 に入っているもの以外
HYPERLINK "http://www.dfait-maeci.gc.ca/~eicb/export/gr5_e.htm" ）
これらの小火器の全出荷が１５丁を越えない場合に限る。

vii. 整備／修理パーツー‐商業用航空機

viii. 整備／修理パーツー‐その他の製品

ix. 返品

返品とは：

- カナダから海外の国に修理や交換のために返されて製品
- カナダでの修理が終わり返された製品、または、
- カナダから以前輸出されたが交換のためにカナダに返された取り替え用の製品

注意：

ある特定の場合、GEP NO.EX.1 は、上の段落 vii,viii,ix で記載された状況においては輸出に該当することがある可能性がある。

6. IIC, DV, EUC, や IL が要求される国

国名	要求している書類
オーストラリア（Australia）	IIC/DV
オーストリア（Austria）	IIC/DV
ベルギー（Belgium）	IIC/DV
ボリビア（Bolivia）	DV
ブルネイ（Brunei）	IL
チリ（Chile）	IIC/Dv と同等のもの(equivalents)
中華人民共和国（PRC）	EUC/MOFERT
デンマーク（Denmark）	IIC/DV
フィンランド（Finland）	EUC
フランス（France）	IIC/DV
ドイツ（Germany）	IIC/DV
ギリシャ（Greece）	IIC/DV
香港（Hong Kong）	IIC/DV
ハンガリー（Hungary）	IIC
アイルランド（Ireland）	IIC/DV EUC
イスラエル（Israel）	IIC/CC**
イタリア（Italy）	IIC/DV
日本（Japan）	IIC/DV
大韓民国（Republic of Korea）	IICC/DV
リヒテンシュタイン（Liechtenstein）	Swiss Blue
ルクセンブルク（Luxembourg）	IIC/DV
マカオ（Macau）	IL
マレーシア（Malaysia）	IIC/DV
ミャンマー（ビルマ）」（[Myanmar (Burma)]）	EUC
オランダ（Netherlands）	IIC/DV
ニュージーランド（New Zealand）	EUC
ナイジェリア（Nigeria）	IIC
ノルウェー(Norway)	IIC/DV
パキスタン（Pakistan）	IIC/DV
ポルトガル（Portugal）	IIC/DV

シンガポール（Singapore）	IIC/DV
スペイン（Spain）	IIC/DV
スウェーデン（Sweden）	IIC/DV
スイス（Switzerland）	Swiss Blue
トルコ（Turkey）	IIC/DV
英国（United Kingdom）	IIC/DV
アメリカ合衆国（United States）	IIC/DV
ユーゴスラビア（Yugoslavia）	EUC

* PRC = People's Republic of China

**DV の代りに通関証明書（Customs Certificate in lieu of a DV)が要求される

付録 B　ワッセナー条約

以下のワッセナー条約の説明は、カナダの外務・国際貿易省から提供された。

ワッセナー条約は、通常兵器と二次使用可能な製品や技術の移動の透明性と信頼性の向上を促進させ、不安定な蓄積を防ぐことによって、地域的また国際的な平和と安全に貢献するために制定された。ワッセナー条約に参加している 33 の国は、これらの製品や技術の移動が軍事能力の発展や向上につながらないよう、また、その能力を支える方向に向けたものではないように確保しようとし、ワッセナー条約の目的を傷つけないように努めている。さらに、ある地域の状況や国の行動が重大な懸念になったり、懸念の原因になることがもしあれば、この協定は、軍備や最終的に軍使用を目的としたデュアルユースが可能な微妙な品目の獲得を防ぐための協力を高めることをも意図している。この協定は、直接的にいかなる国や国々に対して反対しているわけではなく、また、誠実な民間の取り引きを妨げるものでものない。

この協定の制定に伴い、どの鍵長の暗号でも使用できるようにデザイン、または、変更されたすべての製品は、特定の免除もしくはジェネラルソフトの覚書（General Software Note）に従ったもの以外は、情報の安全を確保するため規制されている。安全確保に関心の注意を払いながら今の技術の発展と電子商業に遅れをとらないように、ワッセナー条約参加国は、1998 年 12 月 3 日のウィーンでの会議で、暗号製品と技術に対する輸出管理の改正への同意決議に達した。これらの改正版（詳細はワッセナー条約の Web サイト（"http://www.wassenaar.org/" で入手可能））は、電子商取引のいっそうの発展の促進を手助けするという意味のある緩和を提供した。一般に、変更は、ハードとソフト製品が同等に制定され、大量販売用製品には規制が履行され、また、様々な範囲の製品の規制が取り除かれた。

（１）規制緩和

ワッセナー条約参加国は、以下の製品を規制の対象から外すことに同意した。

(a)　批准の機能を行っている製品

(b)　デジタル署名の機能を行っている製品

(c)　パスワード保護、個人識別番号、もしくは、類似データの不正アクセスを防ぐのに直接関係している以外のファイルやテキストの暗号がないアクセス制御製品

(d)　デジタル技術で履行されてない時にアナログの原理を使用している製品

(e)　56bit 以下の鍵長の対称アルゴリズムを使用している製品

(f)　アルゴリズムのセキュリティが以下のどれかに基づいた場合の非対称アルゴリズムを使用している製品：

i.　整数の因数分解が 512bit 以上でないもの（e.g. RSA）

ii.　有限領域の範囲の乗法グループ内の離散対数の演算が 512bit 以上でないもの（e.g. Diffie-Hellman over Z/Pz）

iii.　離散対数のグループが上記に記載されている（ii）以外で、112bit 以上でないもの（e.g. Diffie-Hellman over an elliptic curve）

(g)　デジタル暗号が、支払いまたはプログラムに関して情報を放送供給者に送る時以外では全く使用されていない、ラジオ放送や有料テレビ、もしくはそれに類似した消費者用のタイプで視聴者が制限されているテレビの受信装置

(h)　暗号の権限がユーザにはアクセス不可能で、以下のどれかの使用ができるように特別にデザインされ制限された製品：

i.　複製不可のソフトの制作

ii.　以下のどれかにアクセスできるもの

a.　複製不可の読み専用メディア

b.　公に同等のセットが販売用に供給された時に、暗号化された形式で情報が入っているメディア（e.g. 知的所有権保護との関連で）

c.　一回だけ複製できる、著作権で保護された音楽や映像のデータ

(i)　銀行業務、もしくは通貨取引用に特別にデザインされ制限された製品

(j)　コードレス操作の最高有効距離が 400m 未満で、端末間暗号が不可能なコードレス電話器具（i.e. ターミナルとホームベースステイション間での中継のない単一の通信）

さらに、ワッセナー条約参加国は、以下の事項についても同意した。

(a)　輸出者に対する半年ごとの報告義務を廃止すること

(b)　権利不在状態のソフトに対するこれまでの免除を引き続き維持すること

（２）提案された輸出規制リストの変更

ワッセナー条約参加国は、大量販売用の暗号化ソフトのためのジェネラルソフトの覚書(General Software Note）の記載事項１を、以下のすべてを満たすハード・ソフト両方の製品に適切な暗号の覚書（Cryptography Note）と書き換えることに同意した。

(a)　以下のどのような方法についても小売販売されている先の在庫から、制限無しに一般の誰にでも販売されていること

i.　店頭取引

ii. 通信販売取引
iii. 電子取引
iv. 電話取引

(b) 暗号化の機能は簡単にユーザによって変えられないこと
(c) 供給者の実質的な手助けなしに、ユーザがインストールできるようデザインされたもの
(d) 鍵長 64bit 以上を使用の対称アルゴリズムが含まれていないもの
(e) 必要ならば、製品の詳細が入手可能で、また、上記の a～d に記述されている条件に従っているか確かめるために、輸出国の適切な当局に要請に応じて提供できること

技術変更に加えて、ワッセナー条約参加国は、上記の（d）で定義されている大量販売用製品への規制の効力は２年間であり、また、それらの規制の継続的なる更新はワッセナー条約参加国の満場一致が必要であることに同意した。

ワッセナー条約の現在の参加メンバーは以下の通りである。

アルゼンチン （Argentina）	ルクセンブルク （Luxembourg）
オーストラリア （Australia）	オランダ （Netherlands）
オーストリア （Austria）	ニュージーランド （New Zealand）
ベリギー （Belgium）	ノルウェー （Norway）
ブルガリア （Bulgaria）	ポーランド （Poland）
カナダ （Canada）	ポルトガル （Portugal）
チェコ共和国 （Czech Republic）	ルーマニア （Romania）
デンマーク （Denmark）	ロシア連邦 （Russian Federation）
フィンランド （Finland）	スロバキア共和国 （Slovak Republic）
フランス （France）	スペイン （Spain）
ドイツ （Germany）	スウェーデン （Sweden）
ギリシャ （Greece）	スイス （Switzerland）
ハンガリー （Hungary）	トルコ （Turkey）
アイルランド （Ireland）	ウクライナ （Ukraine）
イタリア （Italy）	英国 （United Kingdom）
日本 （Japan）	アメリカ合衆国 （United States）
大韓民国 （Korea, Republic of）	

付録Ｃ　鍵寄託／鍵回復制度に関する諸外国の動向（1999 年 9 月時点）

本稿は、鍵寄託／鍵回復制度（キーエスクロー／キーリカバリー）に関する諸外国の道央を、1999 年９月時点までの情報をもとに整理したものである。

１．背景

暗号技術の用途は、従来、軍事もしくは金融分野が中心であり、政策上の管理や規制も比較的容易であった。しかし、近年のインターネットの飛躍的な普及や電子商取引の発展を背景に、その応用範囲は急速に広がりつつある。インターネット上での安全な取引の実現に暗号技術は不可欠であり、昨今の情報システムの性能向上を受けて、暗号の強度に対する要求水準は日増しに高まっているといえよう。

その一方、高度な暗号技術が犯罪情報の隠蔽に利用され、犯罪捜査に悪影響を及ぼすことも懸念される。そこで、暗号装置に鍵寄託／鍵回復（Key Escrow/Key Recovery）のスキームを導入し、犯罪捜査等において必要な場合に、暗号解読を可能にする施策が提案されている。

寄託／鍵回復とは、利用者が秘密鍵もしくはそれを復元するための情報を第三者機関に寄託し、必要が生じた場合にその秘密鍵を提供もしくは復元することで、暗号文を解読することができるようにするしくみである。1993 年のアメリカ政府によるキーエスクロー構想の提案から始まり、その後、幾度かの軌道修正を経て、1996 年 10 月のゴア副大統領の公式声明以降、そのコンセプトは「犯罪捜査」から「鍵紛失時の対応」に重点を移し、その呼称も「キーリカバリー」が主流となった。しかし、政策上の焦点が、法律執行機関による暗号文の解読の合法化であることに変わりはなく、法制化をめざす政府機関とプライバシー保護団体等との論争が続いている。

鍵寄託／鍵回復制度について検討する上で重要となる視点として次の項目が挙げられる。

⑴鍵寄託／鍵回復のしくみを実現する制度、システムの導入と法的裏付け

⑵法律執行機関による暗号化されたデータの平文または暗号鍵へのアクセスの合法化

⑶国際協調

⑴については、アメリカでは輸出規制や政府調達品を盾に世界市場の大半をカバーする国内の製品ベンダに鍵寄託／鍵回復機能を搭載させるアプローチ、欧州では鍵管理を請け負う機関に対し、認可の条件として秘密鍵の提供を義務づけるアプローチが採られたが、鍵寄託／鍵回復システムの採用や利用者による鍵寄託の義務化については反発も大きく、トーンダウンの方向にある。また、アジアでは、鍵寄託／鍵回復のしくみを実現する制度

やシステムの導入に向けた取り組みについての情報が乏しく、まだ具体的な動きはないと思われる。

また、⑵については、キーリカバリー政策の普及をめざしたアメリカ政府の積極的なロビー活動により、1997 年 3 月に採択された OECD（Organization for Economic Cooperation and Development）暗号政策ガイドラインにおいて、「国家の暗号政策は暗号化されたデータの平文または暗号鍵への合法的アクセスを認めることができる。このような政策は、このガイドラインに納められた他の方針を最大限尊重しなければならない。」という一条が加えられた。この合法的アクセスの導入に係る判断は各国の政策に委ねられており、欧州やアジア諸国で法制化に向けた取り組みが見られる。

⑶については、上記の OECD 暗号政策ガイドラインの他、アメリカの GII 構想における KMI スキームの導入（後述）、欧州連合の「情報技術に関連する刑事訴訟法の問題に関する勧告」（1995 年 9 月）、ETSI（欧州電気通信標準化機構）における TTP の欧州標準化検討等で、⑴や⑵に関する国際協調が提言されている。

以下の節では、⑴や⑵を中心に鍵寄託／鍵回復制度に関する各国の動向を紹介する。

２．アメリカ

アメリカでは、1993 年に発表した Clipper Chip や Skipjack をベースとするキーエスクロー構想以降、法制化をめざす政府機関とそれに反発するプライバシー保護団体や暗号製品ベンダとのせめぎ合いが続いている。

（１）輸出規制と KMI

アメリカ政府は、1995 年 12 月には、鍵寄託機能を採用した暗号製品の輸出規制を緩和する方針を発表し、鍵寄託制度を推進する方策として暗号製品の輸出規制を利用するアプローチをとった。さらに、同年 10 月には、これまでの施策の軌道修正を踏まえたゴア副大統領の公式声明において、「キーエスクロー」から「キーリカバリー」への方向転換と、2 年以内の鍵回復機能の登載を前提として、鍵長 56bit 以下の暗号製品の輸出を許可する方針が明らかにされた。こうした動きをうけて、暗号製品の主要ベンダ側は Key Recovery Alliance を組織し、技術の標準化や提携に取り組む姿勢を示している。

ところが、1998 年７月には暗号製品の輸出規制が緩和され、金融機関の場合、鍵回復機能を持つ暗号製品を使わなくてもよいことになった。これは、鍵回復機能の導入による経費の増大がアメリカ企業の国際競争力を低下させることを懸念したためといわれる。さらに、同年９月には、この特例措置が、金融以外の健康、医療、保険業界にも適用されることとなった。プライバシー保護団体や暗号製品ベンダを中心とする IT 業界の圧力もあり、長期的に見れば、輸出規制はさらに緩和される方向に向かうものと考えられる。

また、国内については、1996 年 5 月に「鍵管理インフラ（KMI：Key Management Infrastructure）」として、公開鍵インフラに鍵寄託機関の概念を織り込む形で、捜査当局の秘密鍵への合法的アクセスを可能にする構想を提案した。さらにアメリカ政府は、OECD 等を通じて諸外国に対してもロビー活動を展開することにより、海外政府における鍵回復制度の採用を促し、国際協力の観点から KMI の実現に寄与する布石を打っている。

（２）鍵寄託／鍵回復制度を巡る法制化の動向

1997 年 3 月には KMI 構想を含む Electronic Data Security of Act 1997 と呼ばれる法案が発表された。この法案は、鍵回復機能を含む PKI を推進するものであった。実施にはいくつかの障害もあり、修正を経た法案は、いかなる暗号の使用も法律で提示された場合を除き合法であること、鍵回復インフラの使用は自発的なものであることが断言されたが、政府はもはやドラフト法案のスポンサーを探していない。ゴア副大統領は 1998 年 3 月 Senatory Daschle に宛てた手紙の中で、自発的な鍵回復制度を奨励するという政府の約束を繰り返し、政権が鍵回復制度の義務化を追求せず、産業と法執行の間の対話に従事することを確言した。

また、1997 年には、鍵回復システムの構築を指向する SPNA 法案（Secure Public Network Act）も提案されている。この法案では、登録を受けた認証機関が公開鍵証明書を発行する要件として、暗号化データの回復に必要なデータの預託や法律執行機関の鍵回復要請への対応が義務づけられている。

一方、1996 年には、暗号製品の輸出規制を緩和し、政府による鍵寄託／鍵回復システムの使用を禁止する SAFE 法案（Security and Freedom through Encryption Act）や Pro-CODE 法案（Promotion of Commerce On-line in the Digital Era Act）、ECPA 法案（Encrypted Communications Privacy Act）など、アメリカ政府の暗号政策に対抗する法案も相次いで提出された。これらは同年には成立せず、1997 年に再提出されたが、そのうち SAFE 法案（Goodlatte 案）は、いくつかのグループでそれぞれ改正案が検討された。その結果、キーリカバリー機能のない暗号製品の輸出の制限（Weldon – Delms 修正案）、アメリカ内におけるキーリカバリー機能のない暗号製品の生産、販売、輸入の禁止（Oxley - Manton 修正案 、Markey - White 修正案）、法律執行機関の研究等を補助する NET（National Electronic Technologies）Center の設置（Markey - White 修正案）など、実質的には鍵寄託を強いる方向の修正も含め、複数の競合案が提出された。しかし、House Roles Committee の Solomon 議長は、「もしその案が鍵寄託を義務づける規定を含むのであれば、法案を提出しない」と宣言、SAFE 法案は当初の提案者である Goodlatte 議員により、1999 年に議会に再提出されることとなった。SAFE 法案は、暗号を用いる全ての人間の権利を保護し、政府が鍵回復を義務化することを禁止すること、また、犯罪行為を隠すために暗号を用いた場合は罰せられることを示した。Commerce Committee は、1999 年 6 月、「解読の命令に応じない場合は、10 年を限度とする懲役が課せられる」という修正案を提案した。

また、1998 年 5 月、犯罪情報を隠すために暗号を用いた場合、連邦犯罪委員会によって 5～10 年の懲役が課せられるという項目を含む E-PRIVACY 法案が議会に提出された。また、この法案は、SAFE 法案（Markey- White 修正案）のように、法律執行機関のために NET センターを設立する項目も含む一方、政府による鍵寄託／鍵回復を禁止している。

また、MaCain 上院議員が 1999 年 4 月に提出した PROTEST（Promote Reliable On-Line Transactions to Encryption Act）法案は、政府が鍵回復を義務づけることを禁止しているが、犯罪を隠すための暗号の使用に対する刑事上の罰規定については含まれていない。

３．欧州

欧州では、鍵寄託機関、鍵復元機関、認証機関の役割を担う TTP（Trusted Third Party）という概念を打ち出し、これに基づく鍵寄託／鍵回復制度の導入を図る取り組みがなされてきた。国の認可を受ける TTP に秘密鍵提出を義務づけることで、アメリカ型の「製品供給側への規制」とは異なるアプローチの合法的アクセスが可能となる。

ただし、現段階では、TTP 導入に積極的であったフランスやイギリスでも、TTP への鍵寄託を義務づけるアプローチはトーンダウンしている。また、ETSI（欧州電気通信標準化機構）でも、TTP に関する欧州標準を策定する動きが見られたが、現在は凍結されている。

一方、法律執行機関による暗号データの平文または秘密鍵への合法的アクセスについては法律執行機関側のニーズが高く、フランスやイギリスでも法制化が進んでいる。

３．１　フランス

フランスでは、国が指定した暗号システム以外は利用を認めないなど、従来から統制色の強い施策を実施していた。しかし、90 年代後半からは暗号施策の規制緩和を進めつつある。その一方、鍵寄託制度の導入には意欲的で、1996 年７月に公布された電気通信法の一部改正において、

・情報の秘匿を目的とする暗号装置を利用する場合には、その暗号鍵を政府によって承認された組織に寄託すること

・暗号通信サービスを提供する事業者は、法律執行の枠組みに基づいて、管理する秘密鍵を法律執行機関に提出すること

が義務づけられている。その後、1998 年２月の法令では鍵寄託機関に求められる要件を示し、翌３月には、

・鍵寄託機関及び鍵寄託法案が承認された場合、鍵寄託機関に暗号鍵を寄託したユーザはそれらの鍵で暗号スキームを自由に使うことが可能になること

・鍵寄託機関はある特定の状況下で法律執行機関に鍵を渡すよう要求されること

等を示した法令を施行した。このとき、鍵寄託機関として唯一承認されたのは SCSSI（service central de la securite des systemes d’information）であった。

しかし、Jospin 首相による国内の暗号法の自由化に関する発表（1999 年１月）では、TTP への鍵寄託の義務的な性質を廃止する一方、法律執行機関の要求に応じて、暗号化文書の平文を司法局に提出するよう人々に要求できるしくみを法制化する方針が示された。これらの改正は同年３月の法令 99-199、99-200 として施行されている。

３．２　ドイツ

ドイツでは、1996 年 12 月に電子署名法が定められ、その中で「法律執行機関は必要に応じて認証機関の管理する個人情報を入手することができる」（第 12 条）という合法的アクセスの項目が明記された。

一方、暗号政策については、多くの政治家が規制への要望を表明しているが、今のところ具体的な施策は実施されていない。ただし、政府は暗号規制について３つの選択肢を考えていると言われる。

⑴暗号サービス供給者は寄託鍵を所有し、必要があればその鍵を法律執行機関に提出しなければならない。

⑵（⑴に加えて）暗号製品の取引に関しては許可証を必要とする。

⑶（⑴及び⑵に加えて）非認可または非寄託の暗号を禁止する。

1996 年 12 月には連邦と州の長官らが、暗号規制について話し合い、認可を受けた暗号のみ使用できること、暗号制作者と分配者は法律執行機関に暗号のソースコードと個人の寄託鍵を預けることなどの提案がなされた。

また、同月、内務相は、「犯罪者が認可を受けた（寄託鍵を持つ）暗号を用いるとは思えないが、許可されていない暗号を用いること自体に犯罪の疑いがあり、犯罪組織を発見するため取引経路を分析するのを容易にする」と述べ、法律執行機関と国家の安全を守るために、暗号規制に賛成であることを表明した。

1997 年 4 月、連邦内務省の Kanther は、暗号制作者と法律執行機関に鍵を共有させる技術のみを認めることによって暗号を規制したいと述べた。しかし、1997 年 6 月、内務省は鍵寄託の随意の使用を認め、政府は鍵寄託を取り入れた暗号製品に保証を与えた。このような製品は自発的に用いられている。

一方、経済事務相 Rexrodt や法務相の Schmidt-Jortzig は、暗号の規制には反対の意を示している。また、1998 年 1 月の RSA データセキュリティ会議において、外務省の Ulrich Sandl は、今年の終わりには GAK システムを認めないようにすると述べた。さらに彼は、アメリカの鍵回復製品はドイツのプライバシー法に違反するかもしれないとも述べた。

1998 年、ドイツ議会の調査委員会「メディアの将来」は、暗号は禁止すべきではないと勧告した。委員会は、利用者が自分を暗号によって守ることを法によって規制すべきではなく、このような技術の自由な使用を禁止することは、コストベネフィットの理論によって正当化されるべきではないとも述べた。

３．３　イギリス

イギリスでは、1997 年 3 月、貿易産業省（DTI:Department of Trade and Industry）が、暗号サービスの規定のために TTP の認可に関する調査書を発表した。この調査書は、1996 年 6 月の調査書に従っており、規制の対象を公共ネットワークでの暗号の使用から一般的な暗号の使用にまで拡大したものである。その主な目的は、TTP が行うサービスへ

の信頼を生じさせることである。その結果を踏まえた政策が 1998 年 4 月に発表された。提案された法律は、暗号サービスを提供する CA（Certification Authorities）、KEA（Key Escrow Agencies）等の TTP への DTI による認可を規定するものであった。これによって、個人ではなく組織によって公共や事業に提供される全ての暗号サービス（企業内 TTP やペイＴＶへの暗号サービスは除く）は、政府の支配を受け、認可を受けていないサービスの提供は禁じられる。

また、TTP は、大臣によって法的に発行された委任状に従って、個人の寄託鍵を提出することが求められる（暗号鍵のみが対象であり、署名鍵の提出は不要。デュアルユースの鍵の区別については言及していない）。また、この報告書は鍵寄託について記述しており、法律執行機関はセッション鍵でなく個人の秘密鍵を受け取ることになっているが、鍵を受け取った機関が、委任状失効の後、秘密鍵を破棄して個人情報を保護することを保証するとは明確に述べられていない。

この報告書では、認可を受けた TTP を用いるかどうかは随意であり、暗号の使用そのものを禁止しているわけではない。しかしながら、利用者にとっては認証局が必要であり、認証局は政府の支配下にあるので、政府が秘密鍵の寄託を求めずに設立された PKI をどの程度認めるかどうかは明らかでない。

1998 年 2 月、DTI の報告書に従った新たな政策の発表が計画された。それは、DTI の報告書とほぼ同じものと思われたが、デジタル署名鍵を強制的に預けさせることを控える内容であった。しかし、その発表は結局延期され、1998 年 4 月に行われた。TTP の認可は随意であり、暗号サービス提供者は認可を受けるのも受けないのも自由になった。また、この政策は、デジタル署名と秘匿目的の暗号を明確に区別し、認証局と KEA も区別した。鍵回復や鍵管理等の秘匿化暗号サービスを提供する組織は、認可を受けるよう奨励され、認可を受けたサービス提供者は鍵回復のための「適切な保管用の配列」を求められたが、これは鍵回復技術より鍵寄託技術と言えるものであった。法律は、法律執行機関が暗号鍵への合法的なアクセスの権限を得るように制定された。暗号鍵へのアクセスを可能にする法律は、認可を受けているかどうかに関わらず、暗号鍵を持つ全てのサービス提供者に適用される。これらの政策の原則は、1998 年 10 月の国際商取引会議の Barbara Roche の演説でも繰り返され、OFTEL が暗号サービスの認可機関になるであろうと述べた。

また、1999 年 3 月には、「電子商取引における信頼性の確立」という調査報告書が DTI から発表された。これは、以前の提案を踏まえてはいるものの、いくつかの変更がなされ、秘密性が重要なサービスの提供者は、鍵寄託や鍵回復の使用を推奨されることはあるが、強制されることはないということが示された。この政策は、以下の 3 つの方針からなる。

⑴作成された平文・解読鍵・鍵を保護するパスワードを作成者に求めることができる権力を確立する。この権力は提供者と利用者のどちらにも適用される。

⑵鍵寄託と鍵回復の使用を奨励する。

(3)政府は、犯罪者による暗号使用の影響を軽減する方法を他の団体等と調査する。

さらに、1999 年 7 月には「電子商取引の促進」と題された電気通信関連法案が提出された。TTP に対する暗号鍵保管の義務付けは見送られたが、法律執行機関に暗号鍵使用の権限が与えられている。

３．４　オランダ

オランダでは、1994 年 3 月、暗号化に関する法律の原案が出された。これは、政府が全ての通信チャネルから情報を得られるように、国民が強い暗号の所持・使用・売買することを禁じるもので、暗号化は政府に暗号鍵を登録した企業だけが許可された。提案された法案は、多くの抗議によって撤回された。しかし、1996 年 12 月に提案された法案では、暗号に対する命令は暗号化された電話通信にも拡大された。この影響はコンピュータ犯罪法Ⅱの草案にも及び、警察が盗聴器に暗号を発見した場合、会話をしている団体に解読への協力を命令することができることとなった。コンピュータ犯罪法Ⅱの草案は、警察の権限をより拡大したものであり、容疑に対する厳密な証拠を得る場合や事実発見のために緊急の必要がある場合には、解読の要求ができるようになっている。家宅調査によってコンピュータ内に暗号化された情報が見つかった場合、警察は暗号化の方法を知っている人にその情報を解読させることができる。ただし、容疑者の段階では、この命令は適用されない。

また、政府は TTP の政策策定に取り組んでおり、TTP が行う合法的アクセスについて定めようとしているが、未だその前提条件は定義されていない。なお、1998 年 2 月に発表された政府の政策に関する文書「電子ハイウェイのための規制」では、「暗号の使用は自由である」とする条項が含まれている。

４．アジア

アジア諸国では、鍵寄託／鍵回復制度の導入に係る施策はまだ見られない。しかし、いくつかの国では、OECD 暗号施策ガイドラインの公示と前後して、法律執行機関による暗号文解読を合法化する動きが見られる。

４．１　韓国

韓国では、金融分野も含めた暗号装置の輸入規制がなされてきた。ただし、暗号の使用についての制限はない（公共電話ネットワークを用いた暗号化サービスを除く）。

電子取引分野における国内市場の活性化と国際競争力の確保、電子取引の活性化や信頼性の構築、消費者保護の規定をめざして、1999 年 7 月に施行された電子取引基本法では、「電子取引当事者等は、電子取引の安全性及び信頼性を確保するために暗号製品を使用することができる」とした上で、「政府は国家安全保障等のために必要であると認められる場合には、暗号製品の使用を制限することができ、暗号化された情報の原文または暗号技術への接近に必要な措置をとることができる」と明示されている（第 18 条）。

４．２　シンガポール

シンガポールでは、暗号に関する法律がなく、暗号化は合法と位置付けられる。ただし、Singtel との協定によると、シンガポールの電話線を通して暗号化されたメッセージを送る場合には、署名者はシンガポール電信電話局（TAS：Telecommunications Authority of Singapore）から優先的に許可を受けなければならない。TAS は貿易発展委員会（TDB：The Trade Development Board）によって輸入許可の旨を伝えられる。ただし、暗号化の使用が許可されても、暗号製品が使用したアドレスは制限される可能性がある。また、TDB もしくは TAS の許可なしに暗号を売ることは禁じられている。

なお、国家プロジェクトである「シンガポールワンプロジェクト」では、Entrust 社の PKI システムを導入して、国民全員に暗号鍵を配布する計画がある。

４．３　マレーシア

マレーシアでは、1997 年に制定されたデジタル署名法において、認可証明書機関の保有する暗号化データの平文または暗号鍵への法律執行機関による合法的アクセスが明文化されている。

第 77 条

判事は、法律違反が行われているまたは行われたと信じる妥当な原因があると判断した場合、警部以上の立場の警察官あるいは権限を与えられた職員が昼夜妥当な時間に現場に立ち入り、必要上がれば強制的に捜索し、押収することを承認する令状が発

行できる。

第 78 条

第 77 条に基づく令状取得の遅れにより、調査への悪影響や法律違反の証拠の異動、損傷、破壊の危険性がある場合には、現場に立ち入り、第 77 条に関するすべての権限を行使できる。

第 79 条

第 77 条、第 78 条に基づいて捜索を行う警察官または権限を与えられた職員は、コンピュータ化されたデータへのアクセスが認められる。アクセスは必要なパスワード、暗号化コード、復号コード、ソフトまたはハード、コンピュータ化されたデータを理解するのに要求される他の手段も提供されることを含む。

諸外国における鍵寄託／鍵回復の概要

国名	キーリカバリーシステム	鍵回復機関	認証機関	暗号製品等の輸出入規制	その他
アメリカ	輸出暗号製品に鍵寄託機能搭載（計画可）を義務付け。1999 年 12 月に撤廃予定。	鍵寄託機関の枠組みは制作中。 非寄託鍵の利用は自由。 警察は、第三者が保存している暗号文を解読するための鍵の使用許可を法廷に要求できる。	連邦政府レベルでは法案段階。 ユタ州、ワシントン州では認証機関に対する任意の資格制度を導入。カリフォルニア州では免許制を義務づけ。	輸出－ - 64bit 以下 事前製品提出 - 64bit 超 事前審査必要 テロの恐れがある 7 カ国には輸出禁止。	犯罪情報の秘匿化目的の暗号利用を罰する法案[*1]を提出。 FBI 内に暗号解読技術を研究するセンターを設立。
フランス	寄託鍵利用者は、その鍵で自由に暗号使用利用。	KEA は必要に応じて寄託鍵を法執行機関へ引き渡す必要あり。 認可 KEA の候補は SCSSI。	認証機関に対する免許制度の義務づけはしない方向。EU 諸国及び他の国際機関の方向性に倣う方針。	- 証明目的製品 ベンダの申請で無制限。 - 40bit 以下 ベンダの申請で無制限。 - 40bit 超 供給、輸出入－首相の許可必要 利用－事前の許可、SCSSI 検査	従来は暗号の使用に首相の許可が必要であったが、1996 年、1998 年の法改正で緩和。
ドイツ	鍵寄託技術を用いた製品に保証付与。随意で使用。	－	認証機関に対する任意の資格制度を導入。	輸出－自由化 高度な暗号技術を含むソフトウェア製品[*2]	基本的には、暗号を利用する自由を保障。 法律執行機関は必要に応じて認証機関の個人情報を入手可能。
イギリス	鍵寄託／鍵回復制度を奨励。義務はなし。	TTP は必要に応じて寄託鍵の政府への提出が必要。	認証機関と KEA を区別。どちらも任意の資格認定制度を導入する方向。	輸出－認可必要	平文･解読鍵･ﾊﾟｽﾜｰﾄﾞの要求権あり。
オランダ	暗号利用者は、随意で鍵寄託利用可能。	TTP が行う合法的アクセスについて審議中。	商務省の Afdeling Exportcontrole en Sanctiebeleid	輸出－認可必要 ベネルクス三国内および電子的手段の輸出は規制なし	暗号－登録すれば利用可。緊急の場合、警察は暗号解読可能(盗聴器も含む)。
韓国	暗号鍵を政府と共有する義務について議論中。	－	認証機関に対する任意の資格制度を導入。 規定違反に対する罰則あり。	輸入制限－あり 暗号ｿﾌﾄｳｪｱは規制なし 暗号化政策の法律化予定なし。	暗号規制－なし 緊急時のみ、政府は暗号文の解読可能。
シンガポール	－	－	認証機関に対す	輸出規制－なし	暗号取引には

			る任意の資格制度を導入。 シンガポールワンプロジェクトでは PKI 導入を計画。	輸入－許可必要	TDB/TAB の許可が必要。 暗号利用に TAS を利用する場合認可必要。
マレーシア	－	－	認証機関に対する義務的免許制度を導入。	暗号規制－なし	必要があれば警察は認証機関の保有する暗号データの平文または暗号鍵へのアクセスが可能。

*1　Cyberspace Electronic Security Act 1999

*2　武器輸出を規制するワッセナー条約を違反しているとされる（1999 年 9 月 1 日）