暗号利用環境に関する動向調査

－ 調査報告書 －

2015 年 6 月

独立行政法人 情報処理推進機構
セキュリティセンター

目次

1. はじめに

独立行政法人情報処理推進機構(以下「IPA」という。)では、総務省、経済産業省、独立行政法人情報通信研究機構(以下「NICT」という。)とともに、CRYPTREC を運営している。2012 年度の CRYPTREC 活動において、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」が策定されたことにより、CRYPTREC 暗号リスト、とりわけ電子政府推奨暗号リストに掲載されている暗号アルゴリズムの普及が促進し、ひいては日本のセキュリティ産業の競争力強化につながることが期待されている。

しかし、現実には「優れた暗号アルゴリズムがセキュリティ産業の競争力強化に直接的に繋がる」という関連性について、CRYPTREC 委員ならびに CRYPTREC シンポジウム 2013 でのパネリストから極めて懐疑的であるという意見が多数出された。また、2012 年度に IPA が実施した暗号技術の利用状況に係る調査結果からは、旧電子政府推奨暗号リスト策定から 10 年経過していたにもかかわらず、旧リストに掲載されていた国産の暗号アルゴリズムの普及がほとんど進んでいない実態も明らかとなった。

そこで、我が国の暗号政策に係る中長期の視野に立った方針を検討するために、暗号アルゴリズムの普及促進やセキュリティ産業の競争力強化に向けた障壁が何かを明らかにすることを目的として、幅広く現況を俯瞰するために暗号利用環境に関する動向(以下「本調査」という。)を調査した。

本調査結果を報告書として取りまとめ公開すると共に、CRYPTREC での「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析・検討、並びに経済産業省等による暗号政策立案における基礎資料として活用する。

2. 調査方法

本調査では、以下のような構成により、暗号利用環境に関する動向について調査を実施した。

- 各国政府における暗号利用に関する政策動向の調査
- セキュリティ認証取得製品に関する動向の調査
- 国内暗号製品市場に係る動向の調査

「3 章 各国政府における暗号利用に関する政策動向の調査」では、米国、英国、フランス、ドイツ、エストニア、ロシア、中国、韓国、オーストラリア、EU の暗号に関わるセキュリティ政策に関する組織体制、役割、法制度、最新の政策動向について文献・Web 調査を実施した。さらに米国、英国、フランス、ドイツ、エストニア、オーストラリア、EU については政府機関や有識者等へのヒアリング調査を実施した。ヒアリングの際には以下の項目を確認した。

- 暗号に関わるセキュリティ政策に関する組織体制・役割
- 暗号に関わるセキュリティ政策の遂行に関連する法制度(特に、組織の設置根拠や権限・役割を定めたもの)。
- 利用すべき暗号方式の指定があるか否か(政府向け、民間向け等を区別する)。また、指定がある場合には、根拠法等の法規制があるか否か。
- セキュリティ認証制度が構築されているか否か。また、どの程度活用されているか。
- 政府の調達要件に関連する事項。
- 最新の政策動向。
- 暗号研究の遂行(研究予算や体制など)及び研究成果の活用に向けた政府としての関与の在り方。
- 暗号に関連する輸出入規制ならびに利用規制の有無。規制がある場合には、どのような規制か。

ヒアリング対象組織については表 2-1 の通りである。

「4 章 セキュリティ認証取得製品に関する動向の調査」では、CMVP/JCMVP の認証取得製品数の経年推移を日本と米国について調査し、推移の違いの原因の分析・検討を行った。また、CC の認証取得製品数についてグラフ化し、推移の違いの原因を分析・検討した。

「5 章 国内暗号製品市場に係る動向調査」では、暗号ライブラリ、暗号製品、情報セキュリティ製品の 3 つの国内市場にわけて、それぞれの市場規模の経年推移を文献・Web 調査にてグラフ化した。また、今後 5 年の市場規模の推移予測について国内セキュリティ製品ベンダ 9 社(表 2-2)へのヒアリング、30 社へのメールアンケートを実施し分析を行った。

「6 章 まとめと今後の課題」では、各章における調査結果を総括するとともに、暗号アルゴリズムの普及促進やセキュリティ産業の競争力強化に向けた障壁といった観点から今回の調査結果の分析を行なった。

表 2-1 ヒアリング対象組織

国	ヒアリング対象組織	件数
米国	政府機関	1
	大学	1
英国	政府機関	2
	大学	1
フランス	政府機関	1
	大学	1
ドイツ	研究機関	1
エストニア	政府機関	1
	研究機関	1
オーストラリア	政府機関	1
EU	大学	1

表 2-2 ヒアリング対象セキュリティ製品ベンダ

カテゴリ	(小カテゴリ)	対象企業	視点
暗号ライブラリ		A 社	暗号ライブラリ市場の状況、変遷 (セキュリティ製品・暗号製品市場も踏まえ)
		B 社	暗号ライブラリ市場の状況、変遷
		C 社	暗号ライブラリ市場の状況、変遷 メール暗号化・誤送信防止製品の状況
暗号製品	メール暗号化	D 社	メール暗号化・誤送信防止製品の状況 クラウドサービスへの提供、ニーズの状況 製品における暗号技術の位置付け
	ファイル･ディスク暗号化	E 社	ファイル・ディスク暗号化市場の状況 シンクライアント等、競合製品・サービスとの関係 製品における暗号技術の位置付け
	DRM　他	F 社	DRM 製品市場動向、アプリケーションと暗号化機能の関係 OS と暗号化機能の関係
セキュリティ製品	ウィルス対策ツール、DLP	G 社	ウイルス対策ツール、DLP 等市場動向 セキュリティ製品全体の市場動向 サービスとの関係、ニーズの状況
	ファイアウォール・VPN	H 社	ネットワークセキュリティの動向 ファイアウォール・VPN 製品市場動向
	シンクライアント	I 社	暗号製品との関係、DaaS 等サービスとの関係

3. 各国政府における暗号利用に関する政策動向調査

本章では、欧米・アジア各国における、暗号に関わるセキュリティ政策に関する組織体制・役割、法制度、最新の政策動向等について示す。

3.1. 米国

米国における暗号政策の原則は、暗号技術の利用に対しては規制を行わない一方で、戦略的な技術としてその開発を行い、対外的には輸出規制等を通じて厳格な管理を行うというものであった。

連邦政府における機密ではないが取り扱いに注意を要する情報(機微情報)の標準暗号アルゴリズムとして 1977 年に FIPS PUB 46 として策定された DES も当初は厳格な輸出管理が行われており、民間では金融業界などにおいてのみ標準暗号の地位を確立した。1996 年には大統領令[1]により暗号輸出規制が商務省管轄に移され、さらに 2000 年にはテロ支援国家以外への輸出が自由化された。

1990 年代後半には、DES の安全性に疑問が呈されるようになってきたことから、NIST により DES の後継アルゴリズムの募集が開始され、2001 年に FIPS 197 として AES が策定されている。AES については当初より輸出規制は緩和されており、暗号技術の囲い込みによる安全保障よりも、インターネット経済の加速化を狙いとした相互接続性重視に大きく戦略を転換した。

3.1.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

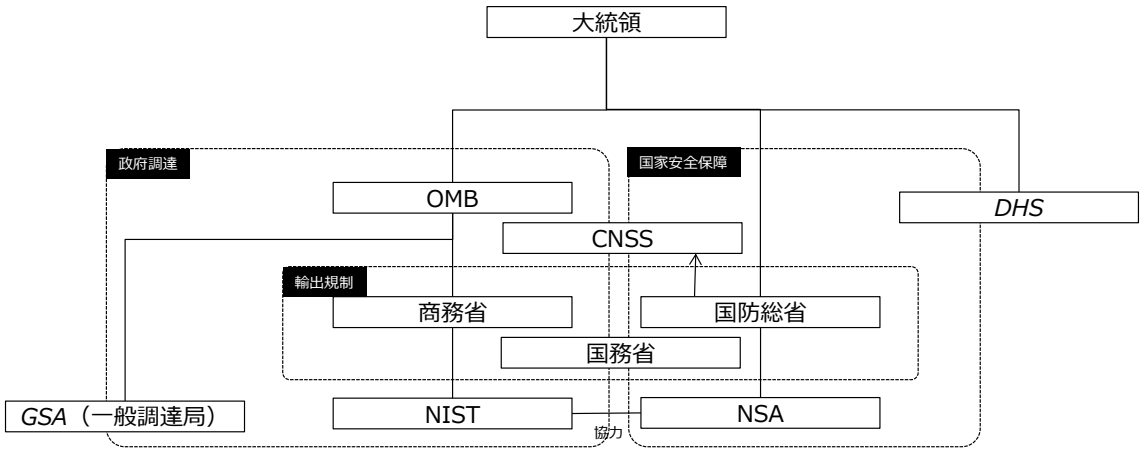
米国における暗号に係るセキュリティ政策に関する組織体制を図 3-1 に示す。

大統領が安全保障政策を大統領令のような形式で示し、国家安全保障局(NSA)と国立標準技術研究所(NIST)が政策遂行機関として暗号政策を具体化する構造となっている。

- NSA (国家安全保障局)
  NSA は国防総省の下に置かれた諜報機関であり、米国の機密情報の保護と、外国の通信傍受・暗号解読を任務としている。この目的のため、NSA は暗号技術の研究開発、暗号解読技術の研究開発を行っているとされ、国家安全保障の観点から暗号政策に大きな力を持っている。

- CNSS (国家安全保障システム委員会)
  国家安全保障に係るような機密情報に関する情報セキュリティの確保については、関係各省庁の代表者から構成される国家安全保障システム委員会(CNSS)がポリシーを策定することとなっており、CNSS の議長は国防総省が、事務局は NSA が務めている。

[1] Executive Order 13026, “Administration of Export Controls on Encryption Products”



OMB：Office of Management and Budget (行政管理予算局)

DHS：Department of Homeland Security (国土安全保障省)

NSA：National Security Agency (国家安全保障局)

GSA：General Service Administration (一般調達局)

NIST：National Institute of Standards and Technology (国立標準技術研究所)

CNSS：Committee on National Security Systems (国家安全保障システム委員会)

図 3-1 暗号政策に係る組織体制(アメリカ)

- 商務省
  商務省は NIST の上位機関として、NIST に予算を与え監督する。また商務省は暗号輸出規制にも関与している。

- NIST (国立標準技術研究所)
  NIST は商務省傘下の試験研究機関であり、政府機関向けの暗号標準を策定している。連邦政府機関の機微情報に関する情報セキュリティ確保に関しては、行政管理予算局(OMB)が責任を持っているが、NIST が情報セキュリティについて政府機関のための標準(暗号を含む)を策定することが法律によって定められている。NIST は OMB からも活動の方向性を示され、予算に関して NIST と OMB が直接の関係にあることが特徴的である。NIST のコンピュータセキュリティ部門の 2014 年度概算要求は約 60 百万ドルである(2012 年度実績は 45 百万ドル)。

- OMB (行政管理予算局)
  OMB は全ての連邦政府機関に適用される覚書(メモランダム)を発行する。NIST が策定する標準は OMB メモランダムを実装するために必要となるものである。

- GSA (一般調達局)
  政府調達の文脈では、サービス組織としての一般調達局(GSA)が関係する。GSA の役割は、FIPS を実装し、コンプライアンスを確保することである。例えば、NIST が策定した技術仕様に基づき省庁共通の入退室 ID カードシステムを導入するなどである。

NIST と NSA は、取組の重複がないことを確認するため、相互に協力することが法的に求められている。NSA は自身の目的達成のために、NIST のガイドラインのサブセットを利用することができる。NIST の資源は限られているため、技術指導と専門知識を得るために NSA と協議することができる。しかし、NSA と NIST の協力は厳密には機微情報が中心である。NIST と NSA は毎月ミーティングを行っている。また、NSA と NIST は多くの標準化団体に並んで参加しており、NSA はこの参加についてオープンにしている。

3.1.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

米国においては、情報保証(Information Assurance : IA)の考え方に基づき、NSA が主要な役割を果たしていることから国家安全保障のプライオリティが高い。また、政府のセキュリティ確保にも力を注いでおり、その一環として暗号技術の導入を政府調達基準等を通じて積極的に進めている。

米国における暗号に係るセキュリティ政策の遂行に関連する法制度及び政策文書(表 3-1)は主に以下のような種類に分類できる。

- 機密情報に係るもの
- 暗号輸出に係るもの
- 連邦政府の情報セキュリティに関するもの(機微情報)
- その他

諜報・防諜(機密情報)に係る法制度については、米国における国家安全保障に関する大統領令等は非公開にされる場合が多いため、法制度の全体像を把握することは困難である。

主な暗号政策について分類整理したものが図 3-2 である。

- 連邦情報セキュリティ管理法 (FISMA : Federal Information Security Management Act)
  2002 年に成立した電子政府法の一部であり、連邦政府機関における情報セキュリティ確保について定めたものである。FISMA 自体は暗号について触れていないが、NIST に対して情報セキュリティに関する標準とガイドラインの策定を求めている。

- 情報技術管理改革法 (Information Technology Management Reform Act (Clinger–Cohen Act))
  1996 年に成立した法律であり、それ自体は政府調達の改革を大きな目的としたものである。その一部として、NIST に対して連邦政府の情報システムに関する標準とガイドラインの策定を求めている。

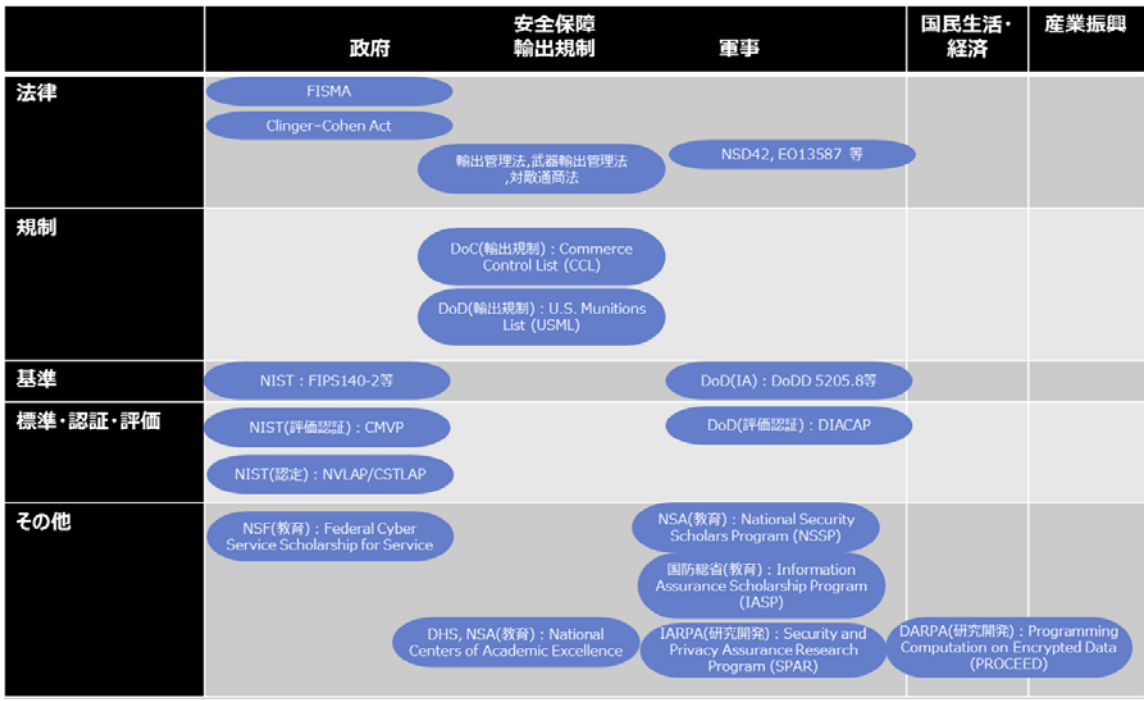
- NSD 42, “National Policy for the Security of National Security Telecommunications and Information Systems”
  CNSS の前身である NSTISSC を設立し国家安全保障上重要なシステム(national security systems)に関する運用ポリシーやガイドライン等の策定することを求めるなど、国家安全保障のセキュリティ確保に関するブッシュ大統領(父)の大統領指令である。

その後の大統領においてもCNSSがポリシーを策定しNSAが実際に政策を遂行するという体制が維持されている(最新はオバマ大統領の大統領命令 Executive Order 13587)。

- CNSS Policy No.3, “National Policy for Granting Access to U.S. Classified Cryptographic Information”
  米国連邦政府の暗号化された秘密あるいは極秘情報に対するアクセス権の付与に関するポリシーを定めたもの。具体的には、政府機関職員もしくは政府の委託先である米国市民であり、セキュリティクリアランスが与えられた者のみに当該アクセス権を付与することができる事などを定めている。また暗号化された秘密あるいは極秘情報に対するアクセス権を付与された者(暗号エンジニアも含む)に対する義務を定めている。

表 3-1 米国における暗号関連の法律及び政策文書

分野	名称	関係組織
上位政策・戦略	連邦情報セキュリティ管理法 (FISMA), 2002	OMB, NIST
	Information Technology Management Reform Act (Clinger–Cohen Act), 1996	OMB, NIST
暗号政策・設置法	NSD 42, “National Policy for the Security of National Security Telecommunications and Information Systems”, 1990	NSA
	CNSS Policy No.3, “National Policy for Granting Access to U.S. Classified Cryptographic Information”, 2007	NSA
	Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information”, 2011	NSA
	(廃止) NTISSP No.2, “National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems”, 1986	NSA
輸出入規制	輸出管理法(Export Administration Act, EAA), 1979	DoC
	武器輸出管理法(Arms Export Control Act, AECA), 1976	DoD
政府調達	(再掲) 連邦情報セキュリティ管理法 (FISMA)	OMB, NIST
	(再掲) Information Technology Management Reform Act (Clinger–Cohen Act)	OMB, NIST
	CNSS Policy No. 11, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products”, 2000	CNNS, NIST
標準・基準	FIPS140-2, 2001	NIST
	FIPS 197 等	NIST
	DoDD 5205.8, “Access to Classified Cryptographic Information”, DoDI 5025.01, DoDD 5143.01 等々	DoD
その他	National Defense Education Act, 1958	DoD



IARPA : Intelligence Advanced Research Projects Activity

図 3-2 米国における暗号関連政策マップ

- Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information”
機密情報の管理体制について定めたオバマ大統領の大統領指令であり、各政府機関内における管理体制を定めたものである。具体的には、政府機関内における機密情報共有のためのコンピュータネットワークのセキュリティ確保を目的として Senior Information Sharing and Safeguarding Steering Committee と Classified Information Sharing and Safeguarding Office (CISSO)等を設置した。OMB と国家安全保障会議の上級職が議長を務める Senior Information Sharing and Safeguarding Steering Committee は、機密情報の共有と保護に関する政府全体の目標設定と年次レビューを行い、コンピュータネットワーク上の機密情報を保護するための優先順位、ポリシー、技術標準について省庁間の調整を行う権限を持っている。CISSO は同 Steering Committee の事務局を務めている。また、コンピュータネットワーク上の機密情報保護のため、国防総省及び NSA に技術ポリシー等を策定する権限を引き続き認めた。

- NTISSP No.2, “National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems
連邦政府が管理する機微情報(Sensitive, but Unclassified Information)に関するポリシーを定めたものである。1987 年に廃止された。

- 輸出管理法 (Export Administration Act, EAA1979)
  主に商務省に対して国家安全保障に係る製品に関する輸出規制を行う権限を付与したもので、暗号などのデュアルユース製品もこの規制対象に含まれる。なお輸出管理法は、2001 年に失効したが、大統領令(Executive Order 13222)により規制の継続が認められた。

- 武器輸出管理法 (Arms Export Control Act, AECA
  武器等の防衛物品の輸出規制を定めたものであり、同盟国以外への輸出には大統領の同意を要する。いわゆる兵器、武器等の防衛物品を対象とした規制であり、軍用の暗号システム、軍用の暗号解読装置が含まれる。

- CNSS Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products"
  GOTS /COTS 製品[2]の調達に関して、NIAP[3]にて認証された製品の調達を求めている。

- FIPS140-2, "Security Requirements for Cryptographic Modules"
  NIST が定めた暗号モジュールに関するセキュリティ要件を規定した米国連邦標準であり、CMVP は本標準に基づく制度である。

- FIPS 197, "Advanced Encryption Standard" 等
  FIPS 197 は NIST が定めた暗号アルゴリズム Advanced Encryption Standard (AES)を規定した米国連邦標準である。同種の規格として、FIPS 180-4, "Secure Hash Standard"、SP800-67, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher"などがある。

- DoDD 5205.8 "Access to Classified Cryptographic Information"
  CNSS Poicy No.3 の施行令であり、暗号化情報へのアクセス権限等を定めている国防総省令である。

- National Defense Education Act
  科学、数学、外国語教育に関する政府の支援を定めた法律である。本法律の下で SMART (Science, Math and Research for Transformation)という奨学金プログラムが実施されていた(2011 年まで)。

[2] COTS(commercial off the shelf)とは既成品のソフトウェアやハードウェアを利用してシステムを構築することである。GOTS (government off the shelf)とは政府向けに製造されたソフトウェアやハードウェアをライブラリ化等することで利用可能なようにしたものである。

[3] NIAP (National Information Assurance Partnership)とは NIST と NSA により設立された認証機関で、IT セキュリティ評価認証制度 (Common Critera)に基づく情報セキュリティ製品の認証を実施。

3.1.3. 暗号に関わる各種制度及び規制

米国における暗号に関わる各種制度及び規制は多岐にわたる。また米国で構築され、世界中に広がった制度も多い。

3.1.3.1. 利用すべき暗号方式

米国政府においては、国家安全保障に係る機密情報の暗号方式と、それ以外の機微情報の暗号方式は別々の体系で規定されている。

国家安全保障に係る機密情報の暗号方式については NSA が定めており、その詳細は不明である。

一方で、機微情報の暗号方式は NIST が FIPS 及び SP として定めている(表 3-2)。この法的根拠は FISMA により NIST に与えられた権限である。連邦政府機関は NIST の定めた技術的標準に従うことが法的に求められている。

表 3-2 米国において利用すべき暗号方式を定めた規格

規格番号	名称
FIPS 46-3 (廃止)	Data Encryption Standard (DES); specifies the use of Triple DES
FIPS 180-4	Secure Hash Standard (SHS)
FIPS 186-4	Digital Signature Standard (DSS)
FIPS 197	Advanced Encryption Standard
FIPS 202 (Draft)	DRAFT SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
SP800-57	Recommendation for Key Management
SP800-67	Recommendation forthe Triple Data Encryption Algorithm (TDEA) Block Cipher
SP800-131A	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths

米国連邦政府において利用可能な暗号方式は、暗号危殆化にともない変更が加えられているが、SP800-57 及び SP800-131A に暗号移行方針が定められている。これによれば 2014 年時点で利用可能な暗号方式及び鍵長は表 3-3 の通りである。

3.1.3.2. セキュリティ認証制度

米国における主なセキュリティ認証制度は暗号モジュール認証制度(CMVP)とコモンクライテリア認証制度(CC)がある。連邦政府は、情報技術管理改革法や FISMA 等に基づき CMVP または CC の認証取得製品を調達しなければならないこととなっている。

表 3-3 2014 年時点で利用可能な暗号方式及び鍵長

種別	名称	備考
暗号化・復号	2Key Triple DES	2016 年以降の暗号化は利用禁止(2015 年までは限定的に利用可)、復号はレガシーユース[4]のみ利用可
	3Key Triple DES	利用可
	AES	AES-128、AES-192、AES-256 のいずれも利用可
	SKIPJACK	暗号化は利用禁止、復号はレガシーユースのみ利用可
ハッシュ関数	SHA-1	署名生成は利用禁止、検証はレガシーユースのみ利用可 電子署名以外の用途は利用可
	SHA-2	SHA-224、SHA-256、SHA-384、SHA-512 のいずれも全ての用途に利用可
電子署名	RSA/DSA	2048 ビット以上が利用可、1024～2047 ビットは署名検証のレガシーユースのみ利用可
	ECDSA	224 ビット以上が利用可、160～223 ビットは署名検証のレガシーユースのみ利用可

(1) 暗号モジュール認証制度（CMVP)

暗号モジュール認証制度(CMVP : Cryptographic Module Validation Program)とは、1995 年に NIST が開始した制度であり、連邦政府が利用する暗号モジュール(ハードウェア・ソフトウェア)を認証するプログラムである。暗号モジュールのセキュリティ要件は NIST が策定した FIPS 140-2 Security Requirements for Cryptographic Modules で規定されている。

(2) 暗号アルゴリズム認証制度（CAVP)

CMVP 取得のためには暗号方式の実装について暗号アルゴリズム認証制度(CAVP : Cryptographic Algorithm Validation Program)による認証を取得しなければならない。これは CMVP の一部であった暗号方式、乱数生成器及び鍵確立技術の実装を対象とした認証プログラムである。CAVP 認証のみを取得することも可能である。

(3) コモンクライテリア(CC)認証制度

コモンクライテリア(CC : Common Criteria)認証制度とは、情報技術を用いた製品やシステムのセキュリティ機能を対象として、ソフトウェア、ハードウェア、システム全体のセキュリティ機能の評価を行う。評価基準は ISO/IEC 15408 として国際標準化がなされている。CC は NSA と NIST の共同プログラムである NIAP (National Information Assurance Partnership)により運営されている。

[4] レガシーユースとは、すでに暗号化か署名された情報の処理に用いること

3.1.3.3. 政府の調達要件

1996 年の情報技術管理改革法を根拠法として、連邦政府機関における調達においては FIPS に準拠することが求められている。また FISMA により、情報技術管理改革法に含まれていた免除規定が廃止されたことから、FIPS の強制力はより高まっている。

具体的には、連邦政府機関は機微情報(≠機密情報)を扱う計算機及び通信システムのセキュリティシステムにおける暗号モジュールは CMVP の認証を取得することとなっている。

また、CNSS Policy No. 11 により GOTS/COTS 製品については、NIAP にて認証された CC 認証製品の調達を求めている。なお、政府調達において CC 認証製品を導入する根拠は以下のような指令・規則等による。

- National Security Directive 42
- CNSS Policy No.11
- CNSS Directive (CNSSD) 502, "National Directive on Security of Natonal Security Systems"
- DoDD 5100.2, "National Security Agency/Central Security Service"
- DoDD 8500.01E, "Information Assurance"
- DoDI 8500.02 "Information Assurance Implementation"

3.1.3.4. 暗号の輸出入規制

米国においては暗号の輸入規制は存在しないが、暗号の輸出規制は存在する。暗号規制の考え方は 1994 年に終了した COCOM[5]の後継として 1996 年に発足したワッセナー・アレンジメント(Wassenaar Arrangement)[6]に基づいている。暗号製品の輸出許可を所管するのは商務省産業安全保障局である。

2010 年に大幅に改定[7]された暗号輸出規制の詳細は Federal Register / Vol. 75, No. 122, "15 CFR Parts 730, 734, 738, et.al[8]"で説明されている。また、最新の規制は商務省産業安全保障局の Export Administration Regulation で規定されている。

Federal Register / Vol. 75 に示された暗号輸出規制の詳細は複雑であるが、概要としては以下のような規制である。

---

[5] COCOM：Coordinating Commmittee for Multilateral Export Controls（対共産圏輸出統制委員会）とは冷戦期に共産主義諸国への輸出規制を行うために設立された。

[6] すべての国家・地域及びテロリスト等を対象とした武器、デュアルユース品の輸出を規制する協約である。暗号はデュアルユース品として輸出規制の対象となっている。法的な拘束力を有する国際体制ではなく、紳士的な申し合わせとして、参加国が国内法で実装する努力をするものとなっている。General Software Notes(GSN)により、マスマーケットとパブリックドメインソフトウェアは規制対象外としている。COCOM の後継として 1995 年に合意された協約であり、当初 31 カ国により締結された。

[7] 2010 年 6 月 25 日の改定により、暗号品目のしての規制対象から多くの品目を削除するとともに、企業の自主判定が大幅に認められるようになった。

[8] http://www.gpo.gov/fdsys/pkg/FR-2010-06-25/pdf/2010-15072.pdf

- 暗号技術が医療用や著作権保護に用いられている場合は規制対象外
- 暗号の強度が一定以上(下記)の製品であってマスマーケット品目でないものは規制対象となる。
  - ✧ 対称アルゴリズム：64 ビット超
  - ✧ 非対称アルゴリズム：768 ビット超
  - ✧ 楕円暗号アルゴリズム：128 ビット超

3.1.4. その他

3.1.4.1. 標準化活動

米国における暗号分野における標準化活動としては、政府向け標準を策定する NIST、民間向け標準を策定する ANSI、IETF などがある。

OMB Circular No. A-119[9]によれば、民間の標準が連邦政府でも用いることができるよう、連邦政府機関は積極的に民間標準化活動を奨励することが求められるとともに、民間標準が利用可能な場合は政府機関もこれを用いることが求められている。

OMB Circular No. A-119 に基づき、NIST は ANSI や IETF などの標準化団体でのグループチェアとして作業することもある。また NIST は FIPS の発行時はいつでも標準化団体と協力することができる。NIST が既存の標準を使う場合や、反対に NIST が新しい標準の策定に貢献する場合もある。例えば、NIST は FIPS 201-1 の発行時、非接触 IC カードのための ISO/IEC 14443 を活用したことがある。

3.1.4.2. 人材育成

米国における暗号関係の人材育成策としては、例えば以下のようなものがある。

- National Initiative for Cybersecurity Careers and Studies (NICCS)
  DHS が中心となって構築したサイバーセキュリティに関する普及啓発、教育、トレーニング等のポータルサイトである。

- NDEA SMART (Science, Math and Research for Transformation) (2011 年に終了)
  国防総省が中心となって実施した National Defense Education Act に基づく大学生を対象とした奨学金プログラムである。暗号に特化したプログラムではないが、科学や数学に強い人材の育成を目的としている。

- National Security Scholarship Program (NSSP)
  NSA と民間企業が出資する奨学金プログラムで、諜報機関や防衛産業のニーズに対応した人材育成を目的としている。これまでに 15 年以上継続しており、200 人以上の学生に約 275 万ドルの奨学金を支給した実績がある[10]。

[9] Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities
[10] https://www.washcoll.edu/offices/career-development/internships/NSSP/

- Federal Cyber Service Scholarship for Service (CyberCorps)
  科学技術分野の基礎研究･教育のファンディング等を行う連邦政府機関 NSF (National Science Foundation)が実施している奨学金プログラムで、連邦政府における情報保証(Information Assurance)の専門家を育成することを目的としている。対象は学部学生(年 2 万ドル)、修士課程(年 2.5 万ドル)、博士課程(年 3 万ドル)の学生である。奨学金受給期間に応じた政府機関における就業義務がある。

- Information Assurance Scholarship Program (IASP)
  国防総省の助成・奨学金プログラムであり、NSA、DHS 等と共同して、国防総省が指定する大学への助成を行っている。軍及び国防総省で勤務する情報保証に関する専門家の育成を目的としている。

- National Centers of Academic Excellence (CAE)
  NSA と DHS の共同プログラムで情報保証に関する教育研究拠点を選定し、人材育成を行うものである。IA Education (CAE/IAE)、IA 2-year Education (CAE/2Y) 、IA Research (CAE/R)の三種類の CAE を選定している。

3.1.4.3. 研究開発

米国政府における暗号研究は、NSA と NIST を中心に行なわれている。NSA が自ら行なう暗号研究体制、研究内容は機密のため明らかになっていない。

- NIST
  NIST が実施している暗号の研究開発は、Cryptographic Technology Group において実施されている。同グループには 14 名の研究員が所属している。具体的な研究テーマとしては以下のようなものがある。
  - 軽量暗号
  - Randomness Beacon
  - ストリーム暗号

それ以外の米国における暗号分野の研究開発プログラムには以下のようなものがある。

- Independent Research and Development Program (IR&DP)
  NSA が実施している研究開発助成プログラムで、対象としては以下のような分野があげられている。
  - 未来の情報保証(IA)システム及び要素技術
  - 情報保証(IA)システムのライフサイクルコスト低減
  - 米国の暗号産業技術基盤の強化
  - 米国の産業競争力強化
  - 効率的かつ効果的なデュアルユーステクノロジーの開発と普及

- Intelligence Advanced Research Projects Activity (IARPA)
  国家情報長官局(Office of the Director of national intelligence)が実施している研究開発プログラムで、米国の諜報コミュニティにおける課題解決のためのハイリスクな研究開発プロジェクトに対して投資を行うものである。暗号技術には限定されないが、IARPA の Security and Privacy Assurance Research Program (SPAR)では、準同型暗号を利用したデータベース技術の開発などを行っている [11]。

- Defense Advanced Research Projects Agency (DARPA)
  国防総省傘下の研究開発機関であり、様々な研究開発プロジェクトを実施している。暗号技術関連の研究開発としては、Programming Computation on Encrypted Data (PROCEED)プロジェクト [12]などが挙げられる。本プロジェクトでは完全準同型暗号を利用して、クラウドとのやり取りを暗号化されたデータのみで行うことでセキュリティを確保するというアイデアである。

3.1.4.4. サービスにおける暗号利用

NIST SP800-144 “Guidelines on Security and Privacy in Public Cloud Computing”や SP800-146 “Cloud Computing Synopsis and Recommendations”では、クラウドコンピューティングでのデータの暗号化や適切な暗号鍵管理、FIPS140 を満たす製品の採用が推奨されている。

[11] http://www.iarpa.gov/index.php/research-programs/spar
[12] http://www.darpa.mil/program/programming-computation-on-encrypted-data

3.2. 英国

英国における暗号政策は、主に CESG (Communications-Electronics Security Group : 通信電子セキュリティグループ [13])が所管しており、暗号要件の策定、製品の認証を行うと共に、輸出規制、安全保障等を所管する他の省庁に対して技術的助言を行っている。

暗号要件については、HMG Cryptographic Standards が規定され、政府調達において適用される。セキュリティ認証制度としては、最も高いセキュリティ水準を要求する CAPS をはじめ、水準に応じた複数の認証制度が整備されている。輸出規制に関しては、ワッセナー・アレンジメントに加盟しており、それに準拠した The Dual-Use Items Regulations 2000 等により規制されている。

3.2.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

英国では､多くの政府機関が情報セキュリティ政策に関係するが､OCSIA を中心として、内務省(HO)、防衛省(MOD)、CESG など情報セキュリティ関連省庁の連携により戦略的方向性が示されている。暗号政策に関しては、CESG が中心となり、政府調達、輸出規制、電子署名等の分野ごととの関係機関と連携している。内閣府(Cabinet Office)が英国政府の電子政府政策についての政治的責任を持っている。

図 3-3 に関連組織の全体像を示す。

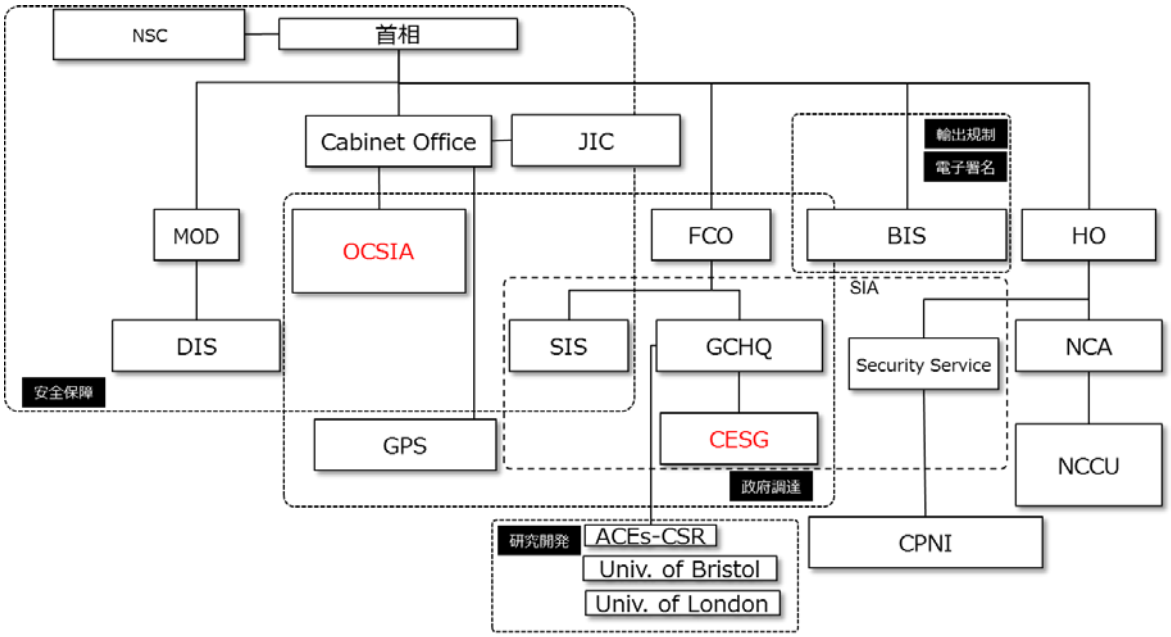
主な組織の要点をまとめると以下のようになる。

- OCSIA (サイバーセキュリティ&情報保証室)[14]
  首相および国家安全保障委員会によるサイバーセキュリティ政策の優先付けを支援し、英国におけるサイバーセキュリティ戦略的方向付けを行い、政府のサイバーセキュリティ政策の総合調整を行う。国の基本戦略 The national security strategy を担当する。
  教育、意識啓発、研修も所管し、セキュリティ情報提供サイト Get Safe online や、Cyber Security Challenge などのサイトを運営する。
  以下の組織と連携し、政府全体の総合調整を行っている：内務省、防衛省、GCHQ、CESG、CPNI、外務連邦省、ビジネス・革新・技術省

- Cabinet Office (内閣府)
  サイバーセキュリティ政策の優先付け、サイバーセキュリティ戦略の方向付けを推進する OCSIA を含む組織である。

- NSC (国家安全保障委員会)
  国家安全保障に関する包括的、戦略的な検討し、政府の基本的な方向性を定める大臣級の会議である。首相が議長を勤める。

[13] CESG は、設立当初は、Communications-Electronics Security Group の略称の意味を持っていたが、現在は、CESG が正式名称である。
http://www.cesg.gov.uk/Pages/homepage.aspx
[14] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance



NSC：National Security Council（国家安全保障委員会）
OCSIA：Office of Cyber Security & Information Assurance（サイバーセキュリティ&情報保証室）
JIC：Joint Intelligence Committee（統合諜報委員会）
MOD：Ministry of Defence（防衛省）
DIS：Defence Intelligence Staff（国防情報参謀部）
FCO：Foreign Foreign and Commonwealth Office（外務連邦省）
GCHQ：Government Communications Headquarters（政府通信本部）
CESG：Communications-Electronics Security Group（通信電子セキュリティグループ）
SIS：Secret Intelligence Service（機密情報部）
GPS：Government Procurement Service（国防情報参謀部）
SIA：Security and Intelligence Agencies
BIS：Department for Business, Innovation & Skills（ビジネス・革新・技術省）
HO：Home Office（内務省）
CPNI：Centre for Protection of National Infrastructure（国家インフラ防護センタ）
NCA：National Crime Agency（国家犯罪局）
NCCU：National Cyber Crime Unit（国家サイバー犯罪ユニット）
ACEs-CSR：Academic Centres of Excellence in Cyber Security Research

図 3-3 暗号政策に係る組織体制(イギリス)

- GCHQ（政府通信本部）[15]
  現代の通信環境の脅威の中で、英国の国家安全保障を保つために必要とされる諜報活

[15] http://www.gchq.gov.uk/who_we_are/Pages/index.aspx

動、セキュリティ対策を進める組織である。
偵察衛星や電子機器を用いた国内外の情報収集・暗号解読業務(SIGINT)を担当する。

- CESG (電子安全通信局)
  GCHQ の情報セキュリティに関する執行組織であり、情報保証に関する国家の技術的な規制機関(National Technical Authority)である。つまり、政府の情報セキュリティに関する技術的な観点について明確な発言権を持っている。
  企業、大学、CPNI、Security Service (MI5)、SIS と連携し以下の役割を遂行する。
  - 政府に対して IT システムのセキュリティリスクおよび対策に関する助言を行う。
  - 標準やガイドラインの提供によりセキュリティ対応能力の強化、企業と連携し、製品・サービス、人のセキュリティ確保
  - 組織におけるセキュリティ専門家の育成
  - 脅威や脆弱性に関する警告の提供、インシデント対応、機微情報を保護するための暗号鍵等の技術的ソリューションを提供する。

- SIS (機密情報部(通称 MI6))[16]
  英国の諜報活動を行う。グローバルな諜報能力を持つ。

- BIS (ビジネス・革新・技術省)
  貿易・産業を所管する貿易・産業省(DTI)が改称された組織で、暗号政策に関しては、輸出入規制、電子署名を所管している。

- CPNI (国家インフラ防護センタ)
  国家インフラに対してセキュリティの助言を与えることにより、国家安全保障を確保する。

- SIA (Security & Intelligence Agencies)
  セキュリティや諜報に係る GCHQ、CESG、SIS、Security Service 等の機関の連合体である。

- ACEs-CSR (Academic Centres of Excellence in Cyber Security Research)
  ケンブリッジ大学、キングスカレッジなどの 7 つの大学が参加するサイバーセキュリティに関するプロジェクトであり、CESG と連携している。

3.2.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

英国においては、情報セキュリティを含む包括的な概念である情報保証(Information Assurance：IA)の考え方が重視されている。IA の対象領域は図 3-4 のようになる。IA の考え方に基づいた政府調達基準および研究開発戦略により、自国企業による暗号技術を確

[16] https://www.sis.gov.uk/

保することを前提とした政策を進めている。
主な暗号政策について分類整理したものが表 3-4 と図 3-5 である。

主な制度の要点をまとめると以下のようになる。

- The UK Cyber Security Strategy[17]
  インターネットによる経済成長、新たな脅威を踏まえた英国のサイバーセキュリティ政策と 2015 年のビジョンを示す戦略である。暗号に関して直接言及は無いが、暗号と関連性の高い情報保証に関するサイバーセキュリティ専門家の認証のためのスキームを確立する目標が掲げられている。本戦略中に、サイバーセキュリティプログラム投資予算総額 6.5 億ポンド(2011～2015 年度の 4 年間)において、情報保証に関する予算が 59%であることが示されている。

- Keeping the UK safe in cyber space[18]
  基本戦略"The UK Cyber Security Strategy"に基づき、サイバーセキュリティが国家安全保障にとって最大の課題と位置づけ、サイバー犯罪対策組織の設立等を掲げて、2014 年に発表された戦略である。

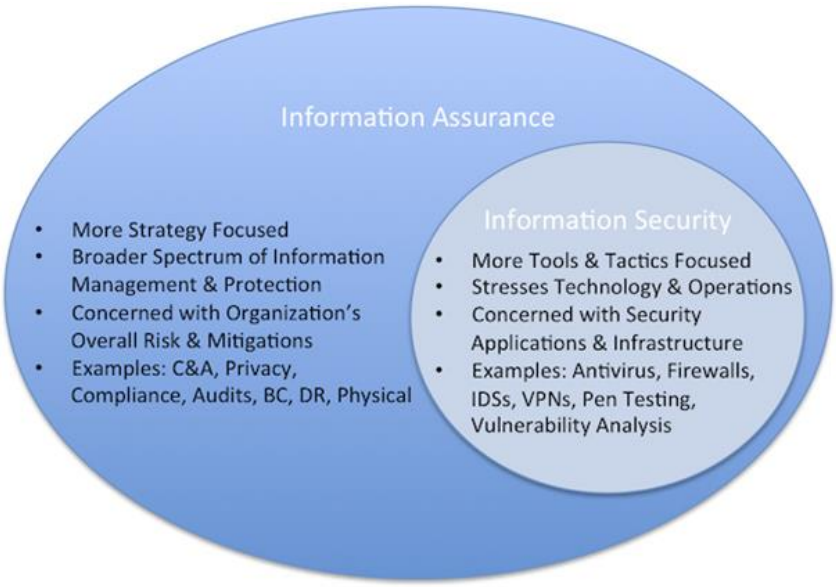


図 3-4 情報保証(Information Assurance)と情報セキュリティの関係

(出典：Information Assurance versus Information Security, NoVAC infosec[19])

[17] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
[18] https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security
[19] https://www.novainfosec.com/2011/08/30/information-assurance-versus-information-security/

表 3-4 英国における暗号関連の法律及び政策文書

分野	名称	関係組織
上位政策・戦略	The UK Cyber Security Strategy	OCSIA、内閣府
	Keeping the UK safe in cyber space	OCSIA
暗号政策・設置法	Security Policy Framework - April 2014	OCSIA、内閣府
	Regulation of Investigatory Powers Act 2000	
	Paper on regulatory intent concerning use of encryption on public networks.1996	BIS (旧 DTI)
	Intelligence Services Act 1994	GCHQ, SIS
	Electronic Signatures Regulations 2002	BIS (旧 DTI)
	Electronic Communications Act 2000	BIS (旧 DTI)
輸出入規制	Regulations 2000 (SI 2000/2620)	BIS (旧 DTI)
	Open General Export License of 1 May 2004	BIS (旧 DTI)
	White Paper on Strategic Export Controls, 1998	BIS (旧 DTI)
政府調達	eGIF (e-Government Interoperability Framework) Technical Standards Catalogue	CESG、内閣府
	HMG Cryptographic Standards	CESG
	HMG Information Assurance Standards	CESG
標準・基準	CAPS (CESG Assisted Products Service) Cryptographic Products	CESG
	CPA (Commercial Product Assurance) Commercial Products	CESG

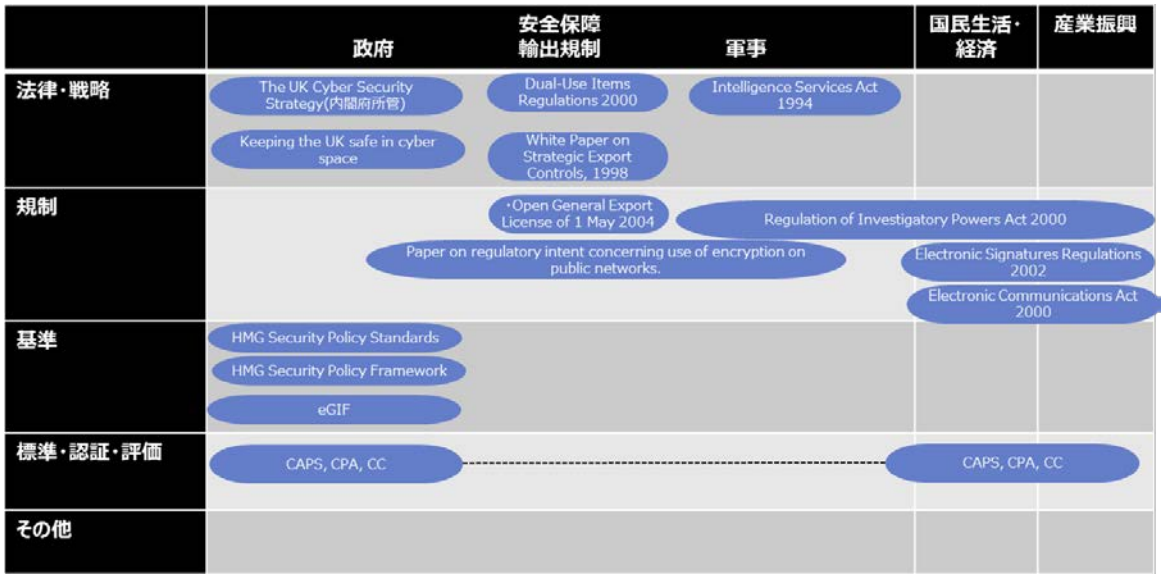


図 3-5 英国における暗号関連政策マップ

- Security Policy Framework - April 2014[20]
  英国政府の資産を保護するために必要な標準、ベストプラクティスガイドライン、アプローチを定めている。暗号について具体的には触れていないが、データ保護に関する記述がある。

- Regulation of Investigatory Powers Act 2000[21,22]
  暗号データに対する開示命令権を規定する。インテリジェンスサービス、警察、税関が合法的に取得した暗号データに対して、安全保障、犯罪防止、英国経済の利益のために復号が必要な場合に、当事者に開示命令を行える。

- Paper on regulatory intent concerning use of encryption on public networks.1996
  Trusted Third Parties (TTPs)のライセンスと規制に関する法制度に関する指針を示す文書である。TTP は、当局に秘密鍵の開示を義務付ける点について言及する。

- Intelligence Services Act 1994
  SIS と GCHQ の活動に関する保証と認可に関する情報､不法行為に対する SIS､GCHQ による捜査などの条項を定めている。SIS や GCHQ の直接的な設置法ではないが、活動に関する制約などが規定されている。

- The Electronic Signatures Regulations 2002[23]
  電子証明の有効性について規定する。EU 電子署名指令(Electronic Signatures Directive)の条項を英国法に反映させるために立法化された。証明書サービスプロバイダ(CSP)の監督や責任、有効な証明書の要件を規定している。

- Electronic Communications Act 2000[24]
  政府は、電子データの暗号鍵の預託を強制する権利を持たないことを規定している。また、暗号サービスプロバイダの登録と要件に関する条項(Section 14 prohibition of key escrow requirements)を含む。

- Regulations 2000 (SI 2000/2620)／Open General Export License of 1 May 2004／White Paper on Strategic Export Controls, 1998
  輸出入に関する規制で、3.2.3.4. 章にまとめる。

- eGIF(e-Government Interoperability Framework) Technical Standards Catalogue／HMG Cryptographic Standards／HMG Information Assurance Standards
  政府調達に関する規制で、3.2.3.3. 章にまとめる。

---

[20] https://www.gov.uk/government/publications/security-policy-framework
[21] http://www.legislation.gov.uk/ukpga/2000/23/contents/enacted
[22] http://www.cryptolaw.org/cls2.htm#uk
[23] http://www.legislation.gov.uk/uksi/2002/318/contents/made
[24] http://www.legislation.gov.uk/ukpga/2000/7/contents

- CAPS Cryptographic Products／CPA Commercial Products
  標準・基準に関するものであり、3.2.3.2. 章にまとめる。

3.2.3. 暗号に関わる各種制度及び規制

3.2.3.1. 利用すべき暗号方式

暗号方式について規定した主な標準は以下である。

- HMG Cryptographic Standards[25]（英国政府暗号標準）
  情報保証を確保するために暗号システムに関するガイダンスを与えるもので、以下の項目を定めている：
  - CS1 – 暗号メカニズム、アルゴリズム、プロトコル（Issue 1.0, Jul 2010）
  - CS2 - 「制限(Restricted)」マーク付きの情報のための暗号システム(Issue 1.0, Aug 2008)
  - CS3 – 暗号標準 – 機密性の保証グレードがハイグレードである製品の暗号実装標準（Issue 1.0, Aug 2012）
  - CS4 – ランダムビット生成（Issue 1.2, June 2012）
  - CS5 – 暗号標準- ローカルアクセスコントロール製品(Issue 1.0, 0ct 2012)

  HMG Cryptographic Standards は、英国情報保証標準(HMG IA Standards)の一部を構成するものである。これらの文書情報の開示は制限されているものがあり、CS1～CS5 はいずれも開示制限の対象となっている。

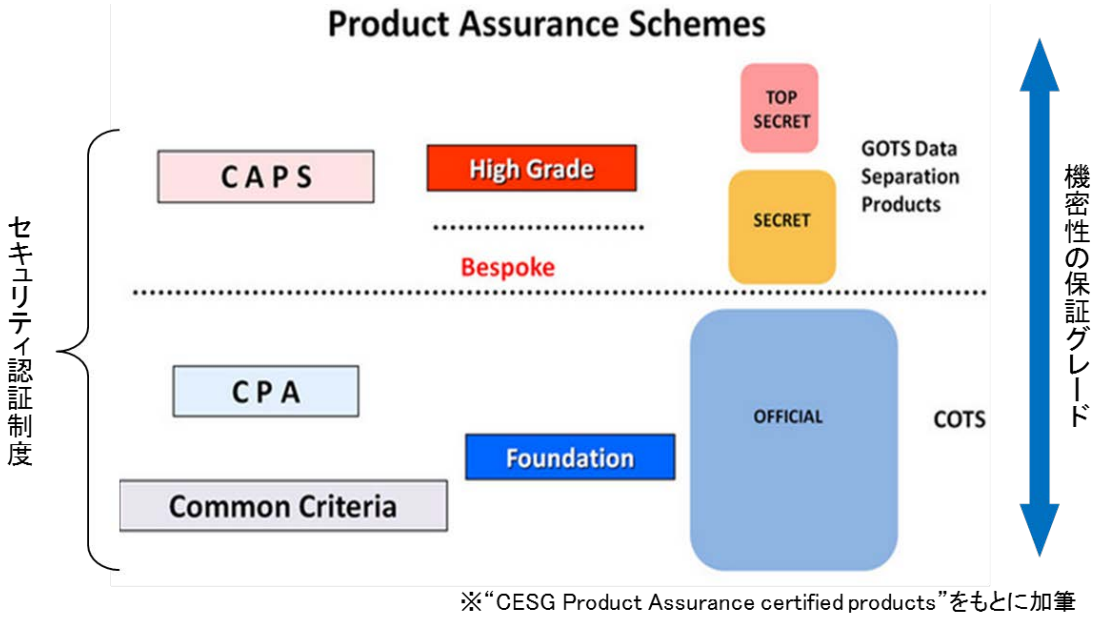
3.2.3.2. セキュリティ認証制度

セキュリティ認証制度は、CESG が所管している。CESG では、CC 認証制度を含め、複数のセキュリティ認証制度を実施している。CESG のセキュリティ認証制度の全体像は図 3-6 の通りである。

- CAPS Cryptographic Products
  特注の、産業設計による製品に対する頑健で詳細な製品認証である。英国政府の新しい方針 Government Security Classification Policy[26]に基づく 3 段階の保証グレードである最高機密(TOP SECRET)、機密(SECRET)、公的(OFFICAIL)のうち、上位 2 段階の最高機密(TOP SECRET)、機密(SECRET)に相当する高いグレードの評価を行い、製品認証する。

[25] Her Majesty Government Cryptographic Standards,
http://www.platinumsquared.co.uk/IAStandardsPages/CryptographicStandards.aspx

[26] 2012 年に改訂された政府情報セキュリティの分類方針であり、最高機密(TOP SECRET)，機密(SECRET)、公的(OFFICIAL)の 3 つの保証グレードに分けられる。これらに基づき上位 2 段階の保証グレードに相当する情報システムはハイグレード、それ以下を基盤の 2 種類に分割される。



※“CESG Product Assurance certified products”をもとに加筆

図 3-6 CESG の製品保証スキームの全体像

- CPA Commercial Products
  英国政府の機密に関する 3 段階の保証グレードのうち下位の公的(OFFICAIL)に相当するセキュリティ特性に対して、商用製品の評価を行う。現状の CPA と CC の関係[27]において、CC は CPA の保証グレードと等価であるとみなすには不十分であるとの立場をとっており、現時点では CC で CPA を代用することはできない。しかし、将来的には CC と CPA を同格に扱いたい意向を持っており、新 CCRA に基づく cPP の作成などに CPA の知見を入れる活動をしている。

- Common Criteria (CC)と ITSEC Products
  IT セキュリティに関する英国国内標準に基づく製品認証 ITSEC があったが、現在は、国際標準によるセキュリティ機能要求に基づく製品認証 CC に代替されている。
  英国における CC 認証は、CESG の監督下で、民間評価機関(Commercial Evaluation Facilities : CLEF)によって実施される。現在、英国においては、CSEG が任命し、英国認定サービス(UK Accreditation Service :UKAS)に認定された 5 つの民間評価機関がある。CLEF は、決められたセキュリティ基準に対して、暗号製品の設計、開発、実装、生産および流通の分析を行う。

他に以下のような製品認証がある：

- PRIME Conformance
  IP 暗号デバイスに関して、PRIME 標準に基づく認証を行う。PRIME 標準は、IP ネットワーク上の暗号通信に関して CESG の戦略的ソリューションとして定めた標準で

[27] International Aspects of Commercial Product Assurance

ある。

- SSCD 評価
  欧州において規定される署名生成機器 Secure Signature Creation Devices (SSCD)に組み込まれる暗号モジュールについての欧州ガイド CWA 14924 2004-03[28]に基づく評価である。強制力は持たない[29]。

3.2.3.3. 政府の調達要件

HMG IA Standards[30] (英国政府情報保証標準)は、英国政府の情報に係る IT システムの開発時に考慮しなければならない点を規定するもので、内閣府と CESG の共管である。英国政府セキュリティポリシーフレームワーク(HMG Security Policy Framework : SPF)における義務的要件に従う情報保証に関する法的拘束力のあるポリシーとして提供される。

HMG Cryptographic Standards は、民間の情報システムも含む情報保証を確保するために求められるより広い範囲を対象とする標準である。

この他に、政府と民間セクタとやり取りをするための電子政府相互運用フレームワークである eGIF (e-Government Interoperability Framework)[31]があり、ここでのポリシーや技術仕様の遵守は義務的なものである。

eGIF に基づく暗号アルゴリズムのリストとしては、2005 年 9 日発行の Technical Standards Catalogue[32], Version 6.21 に挙げられている。

- eGIF (e-Government Interoperability Framework) Technical Standards Catalogue
  eGIF で規定される技術方針に準拠するための最小限の仕様一式を定義するもので、相互接続の技術指針として、暗号化(AES, Triple DES)、署名(RSA, DSA, DSS)、鍵交換(RSA, DSA)、ハッシュ関数(SHA-512, SHA-256)等のアルゴリズムを規定している。また、スマートカード ID 認証の方式を規定している。スマートカードについては、ISO/IEC 7816-15 を参照し、暗号情報の保管、利用、取得等に関して規定している。

3.2.3.4. 暗号の輸出入規制

ワッセナー・アレンジメントをベースとして、各種規制が規定されている。

- The Dual-Use Items (Export Control) Regulations 2000[33]
  暗号輸出は、EU デュアユース規制(EU dual-use regulation)およびワッセナー・アレ

[28] CWA 14924 2004-03 European guide to good practice in management knowledge
[29] Study on Promotion Strategy of Conformity Assessment System of Information Security Promotion, 2004, IPA, Fraunhofer
[30] http://www.platinumsquared.co.uk/IAStandards.aspx
[31] http://edina.ac.uk/projects/interoperability/e-gif-v6-0_.pdf
[32] http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/UK_CBNET/C050901T.pdf
[33] http://www.legislation.gov.uk/uksi/2000/2620/contents/made

ンジメントに基づき規制されている。

- Open General Export License of 1 May 2004[34]
  暗号製品輸出入規制に関して個人利用、コミュニティライセンスの免除を規定する。このライセンスは、「自身による商用暗号製品開発活動」[35]という点において、下位機関、協力者による利用や個人的に関しては、多くの国に対する輸出が許可されている。

- White Paper on Strategic Export Controls, 1998 (DTI)
  輸出規制に関して暗号ソフトウェアを無形の転送に拡張することを提言している。

3.2.4. その他

3.2.4.1. 産業振興

産業振興については、BIS が所管しており、CESG と連携して暗号政策を推進している。UK CDF (Crypto Developers Forum)は、暗号製品開発の振興に取組んでいる。TechUK[36]は、技術系企業の集まりで、暗号を含む技術について、政府と民間の連携を推進している。また、産業振興策である Cyber Growth Partnership (CGP)の取組には、BT (British Telecom)、Thales、QinetiQ などが参加している。

グッドプラクティスである Cyber Essential は、中小企業など能力が限られる組織に対するサイバーセキュリティに関してまとめたものである。CREST は、情報セキュリティの技術的なサービスを提供する組織で、企業に対して侵入テスト(penetration test)などを提供している。CREST は、英国政府の Cyber Essentials を支援するものである。

ENISA には、加盟国のポストが用意されており、英国からは BIS が参加し、GCHQ がその支援を行っている。また、HORIZON2020 では、BIS が英国の研究開発の取りまとめをしている。

3.2.4.2. 人材育成

The UK Cyber Security Strategy において、暗号と関連性の高い情報保証についてスキル向上の重点化が掲げられている。関連して以下のような制度や取組がある。

- CESG Certified Professionals (CCP) Scheme
  英国のサイバーセキュリティ専門家の標準を規定する。英国の情報保証に関する監督省庁として、スキルの需要と供給に関するギャップの解消、英国のサイバーセキュリティ能力の構築を図るものである。

---

[34] https://www.gov.uk/government/publications/open-general-export-licence-cryptographic-development

[35] "their own commercial cryptographic product development activities"

[36] http://www.techuk.org/

- CESG Listed Advisor Scheme (CLAS)
  CESG により認定された民間セクタのコンサルタントの人材バンクであり、公共セクタに対して情報保証に関する助言を提供する役割を果たす。公共セクタに対して情報保証コンサルティングを提供したいと考える専門家に対して提供される機会であり、一定の要件を満たす専門家が対象となる。

また、情報セキュリティ政策全体を統括する OCSIA は、教育、意識啓発、研修も所管しており、人材育成に関連して、セキュリティ情報提供サイト Get Safe online や Cyber Security Challenge などのサイトを運営などの取組みを行っている。

CESG は、暗号分野の研究開発ファンディングを行っているが、対象者はイギリス国籍を持つことが条件となっている。暗号教育においては、暗号を適切に理解し、利用し、システムに組み込む方法や、グッドプラクティスの習得など、幅広い範囲をバランスよく網羅する人材の育成が重視されている。また、安全保障の観点から、国内に暗号専門家を維持するために、戦略的に研究教育の予算が割り当てられている。

3.2.4.3. 研究開発

英国における研究開発の主要なプレイヤーとしては、ECRYPTII 実施時のパートナーである以下の機関を挙げることができる。

- Royal Holloway, University of London, UK
  Information Security Group (ISG) [37]
  英国政府ファンディング機関 EPSRC[38]および GCHQ から 8 つのサイバーセキュリティ研究における学術拠点(Academic Centers of Excellence)の 1 つとして高く評価されている。グループの研究は、純粋な理論研究、理論と応用をつなぐ研究、応用研究に分けられ、純粋な理論研究は 4～5 名程度が行っている。暗号解析、組合せ論的暗号、証明可能セキュリティ、メッセージ認証コード(MAC)など研究テーマについて高い専門性を持つ。ISG に含まれる Smart Card Centre (SCC)は、ボーダフォンなどの関心を引きファンディングを受けている。教授、准教授、講師、研究アシスタント、アカデミックスタッフなど 31 名から構成される。

- University of Bristol, UK
  Bristol Cryptography Group[39]
  研究の焦点は、暗号システムの安全性を証明する技法、効率的な実装である。また、セキュリティ監査やコンピュータフォレンジックスも対象としている。研究グループに対して、Industrial Advisory Board (IAB)を設置し、外部専門家による研究ポートフォリオと方向性の決定を行っている。
  暗号研究の国際的な団体 International Association for Cryptologic Research

[37] https://www.royalholloway.ac.uk/isg/home.aspx
[38] 工学、物理化学分野の研究ファンディングを行う英国政府機関。
[39] http://www.cs.bris.ac.uk/Research/CryptographySecurity/

(IACR)の Vice President である Nigel Smart、事務局長の Martijn Stam はブリストル大学の教員であり、ブリストル大学が暗号研究において国際的なイニシアチブを持っている。

3.2.4.4. サービスにおける暗号利用

CESG が公開するクラウドサービスに関するガイダンス”Cloud Security Guidance: Separation” (2014 年発行)[40]において、暗号に関する留意点について記載している。本ガイダンスは、クラウドサービスを利用する公共セクタ機関およびサービスプロバイダ向けにセキュリティに係る留意点を示すものである。

本ガイダンスにおける IaaS 利用者に対するガイドでは、転送データの保護、保存されるデータの保護、利用者間のデータの隔離、サプライチェーンに係るデータ保護に関して暗号の利用を挙げているが、具体的な暗号アルゴリズムは規定していない。

[40] https://www.gov.uk/government/collections/cloud-security-guidance

3.3. フランス

フランスにおいては、ANSSI により情報セキュリティ政策全体が推進されており、その中に、暗号に係わる規制、セキュリティ製品認証制度が含まれている。ANSSI は、約 390 名の組織であり、政策立案に加え執行部門を持つなど機能が集約されている。

認証制度に関しては、コモンクライテリア(CC)認証とは別に、フランス独自の CSPN を実施し、審査日数を限定し、CC 認証に比べて安価に認証取得が可能な制度を整備することで、産業振興の観点で企業から評価されている。研究開発については、CNRS、ENS、INRIA の研究者が参加する CASCADE チームが中心的であり、クラウドの暗号技術として FHE に焦点を当てている。

3.3.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

フランスにおいては DCSSI の機能を拡大して設置された ANSSI により情報セキュリティ政策全体が推進されている。ANSSI は、暗号に係わる規制、輸出規制、CC 認証を含む製品のセキュリティ評価認証制度など国家の ICT セキュリティを所管している。DGCIS は、ICT の経済・貿易の促進等を所管している。ANSSI と DGCIS は、研究開発で協力している。

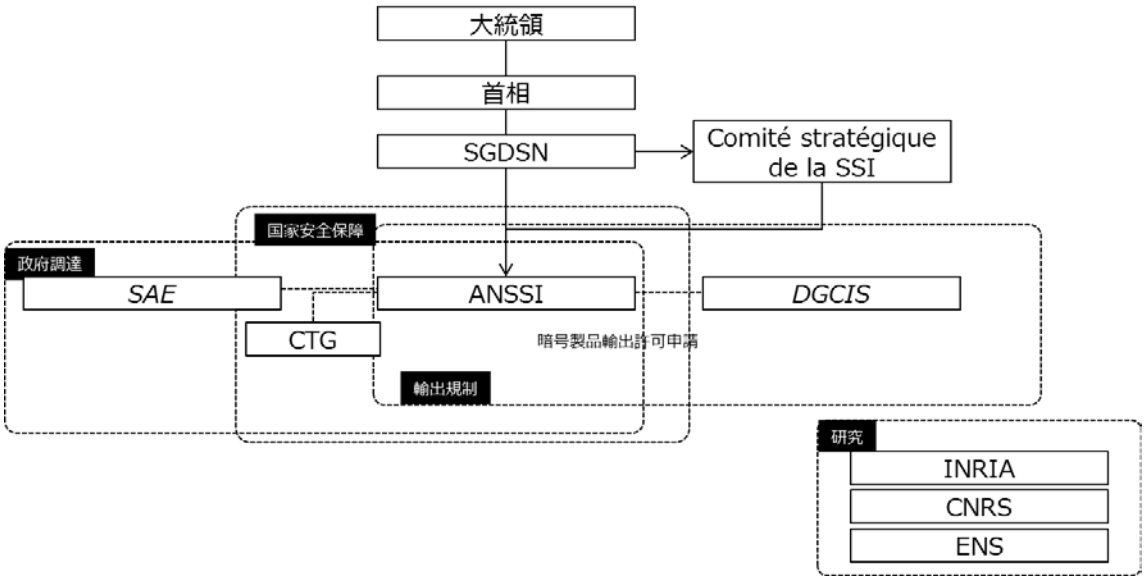
関連組織の全体像をまとめたものが図 3-7 である。

- ANSSI[41] (国立情報システムセキュリティー庁)
  国防安全保障白書により、French Network and Information Security Agency (ANSSI in French, standing for "Agence Nationale de la Sécurité des Systèmes d'Information")の設立が計画され、2009 年に、首相、SGDSN[42]の下に設置された。前身の Central Directorate for Information System Security (DCSSI)を代替し、より広い役割を担う。現在 390 人が勤務している。設置法 Décret n° 2009-834 du 7 juillet 2009 により、ANSSI は、情報システムセキュリティに関する規制機関であることが定められ、国防の関する情報システム機能の監督権限を持つことが定められている。また、暗号サービスの管理やライセンスに関する責任をもつことが示されている。情報システムセキュリティに関する課題へのフランスの対応能力を高めるためることを目的とする。暗号に係わる規制、CC 認証、First level security Certification (CSPN) 認証なども実施している。主なミッションは以下のものである：
  - サイバー攻撃の早期検出、早期対応
  - 政府、民間に対する脅威への対抗のための信頼できる製品・サービスの開発支援
  - 政府、重要インフラ事業者を支援するための助言
  - 積極的なコミュニケーションポリシーに基づき、情報セキュリティ脅威について企業や一般国民への情報提供

[41] http://www.ssi.gouv.fr/
[42] http://www.sgdsn.gouv.fr/site_rubrique88.html

ANSSI の前身である DCSSI は、暗号の選択、パラメータサイズと強度に関する規則と推奨に関する文書[43]を公開している。ANSSI において改訂した文書は見当たらないが、DCSSI の文書を引き継いでいると考えられる。フランスの政府 CSIRT である CRRTA は ANSSI 内に設置される。

ベルサイユ大学や、UPMC(ピエール・マリー・キュリー大学、パリ第 6 大学)、ナンシー大学などの外部の研究機関との協力を行っている。また、ENISA が暗号のガイドラインをまとめる際に、ANSSI は諮問委員会に参加するなどの協力関係にある。



SGDSN：Secrétaire général de la défense et de la sécurité nationale （国防安全保障事務局）

ANSSI：Agence nationale de la sécurité des systèmes drité nationale (国立情報システムセキュリティー庁)

Comité stratégique de la SSI：comité stratégique de la sécurité des systèmes d'information (情報システムセキュリティ戦略委員会)

DGCIS：Direction générale des douanes et droits indirects (生産再建省 競争・産業・サービス総局)

SAE：Le service des achats de l 'Etat, Ministre de l 'Economie, des Finances et de l' Industrie (経済・財政・産業省 国家調達局)

CTG：Le Centre de transmissions gouvernemental (政府伝送センター)

INRIA：Institut National de Recherche en Informatique et en Automatique (フランス国立情報学自動制御研究所)

CNRS：Centre national de la recherche scientifique (フランス国立科学研究センター)

ENS：Ecole normale supérieure (高等師範学校)

図 3-7 暗号政策に関する組織体制(フランス)

[43] Référentiel général de sécurité

- SGDSN
  国防および安全保障に関する上位戦略を検討するための事務局である。

- Comité stratégique de la sécurité des systèmes d'information
  フランスの情報システムセキュリティに係わる国家戦略を決定する委員会である。

- DGCIS (生産再建省　競争・産業・サービス総局)
  輸出入管理を所管しており、デュアルユース物品及びテクノロジーの輸出に関するガイドラインを公開している。

- SAE
  政府の調達を管理する経済・財政・産業省内の部局である。

3.3.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

フランスにおいては、ANSSI は首相府付きの SGDSN に直属する。ANSSI が所管する規制として暗号が代表的であるため、暗号政策のプライオリティは高く、それと相補的に、複数の製品認証制度を整備することにより産業振興にも重点を置いている。

フランスにおける主な法制度を分類整理すると表 3-5 と図 3-8 のようになる。

主な法制度の概要は以下の通りである。

- Livre blanc sur la défense et la sécurité nationale 2013 (FRENCH WHITE PAPER, DEFENCE AND NATIONAL SECURITY, 2013 国防安全保障白書)
  国防の将来像を示す白書である。オランド大統領就任直後に、新しい戦略ガイドラインの必要性から 5 年ぶりに改訂されたもの。暗号については、白書が示す戦略の実現に必要なリソース（技術）として、サイバー脅威への対抗策としてその必要性が示されているが、アルゴリズム等の具体的な内容は規定していない。

- Information systems defence and security France's strategy (情報システム防衛とセキュリティに係るフランスの戦略), ANSSI, 2011
  国防安全保障白書に基づき規定された戦略で、市民、企業、国のサイバー空間を防衛するための戦略概要を示すものである。暗号については、「国家主権に係わる情報保護による意思決定能力の確保」の章において、国家主権に係わる情報の主要な保護手段として重要性を指摘しており、戦略的な独立性を確保するためには暗号技術を自国の技術として確保しているか否かに依存することを示している。そのため、暗号技術の専門性が国から失われることを避け、若い世代が情報システムセキュリティ分野に魅力を感じるような取組が必要であることを示している。
  フランスは暗号と形式手法分野で世界クラスの研究チームを持っているが、セキュリティアーキテクチャ、情報システムの分野はまだ不十分であるため、サイバー防衛研究センターの設立を検討し、その研究センターにおいて、暗号研究、暗号攻撃等を含むセキュリティの研究を行うことを戦略に挙げている。

表 3-5 法制度の分類と一覧(フランス)

分野	名称	関係組織
上位政策・戦略	Livre blanc sur la défense et la sécurité nationale 2013 (国防安全保障白書)	大統領
	Information systems defense and security France's strategy (情報システム防衛とセキュリティに係るフランスの戦略)	ANSSI
暗号政策・設置法	Décret n° 2009-834 du 7 juillet 2009 (政令 No 2009-834, 2009 年 7 月)	ANSSI
輸出入規制	Law no. 2004-575, 21 June 2004 on confidence in the digital economy (デジタル経済における信頼のための 2004 年 6 月 21 日付けの法律)	DCSSI (現 ANSSI)
	Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° (政令 2007-663 2007 年 5 月 2 日付 条項 30,31, 36)	DCSSI (現 ANSSI)
	guide de l'exportateur de biens à double usage (デュアルユース物品及びテクノロジーの輸出に関するガイドライン(暗号技術については ANSSI))	DGCIS
政府調達	(再掲) Law no. 2004-575, 21 June 2004 on confidence in the digital economy (デジタル経済における信頼のための 2004 年 6 月 21 日付けの法律)	DCSSI (現 ANSSI)
	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (行政システムにおける情報セキュリティを規定 (Article 9))	DCSSI (現 ANSSI)
	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (上記 Ordonnance に対する施行令)	ANSSI
	Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information (政令 2002-535 2002 年 4 月 18 日付 IT 製品のセキュリティに関する評価と認証)	DCSSI (現 ANSSI)
標準・基準	Référentiel général de sécurité (セキュリティに関する一般基準)	DCSSI (現 ANSSI)
	Mécanismes cryptographiques (暗号技術)	DCSSI (現 ANSSI)
	Gestion des clés cryptographiques (暗号鍵管理)	DCSSI (現 ANSSI)
その他	Law 2001-1062 of 15 November 2001 on daily security	ANSSI

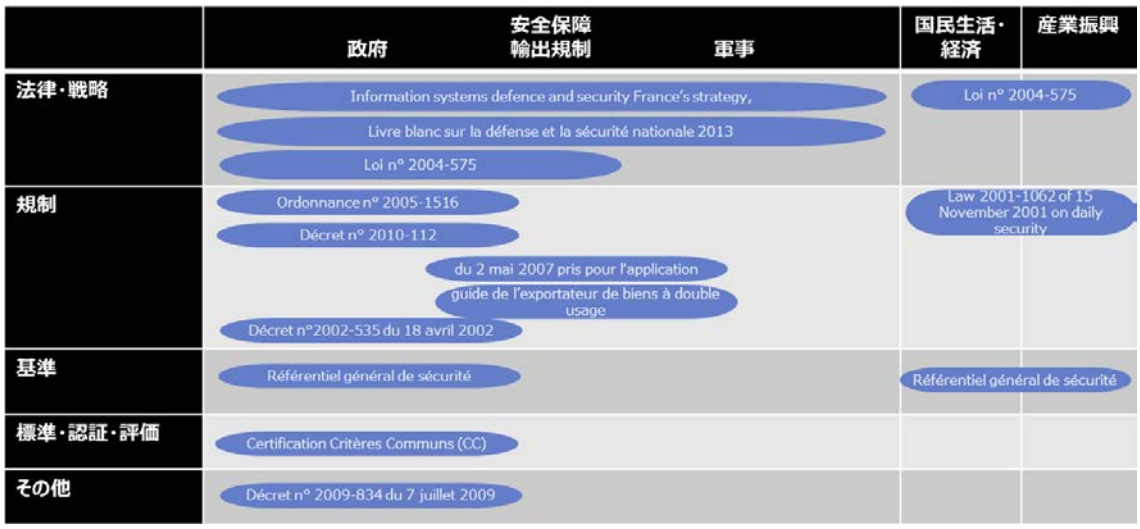


図 3-8 フランスにおける暗号関連政策マップ

- Law No. 2004-575 of 21 June 2004 on confidence in the digital economy[44]
  国内における暗号の利用は長い期間規制されていたが、1999 年に規制は取り除かれた。現在、law No. 2004-575, article 30(I)に基づき暗号の国内利用の規制はなくなっている。通信の暗号化などの暗号サービスの提供には規制があり、安全保障、国防に関係するものは申告が必要である。

- Décret n° 2007-663 du 2 mai 2007／Guide de l'exportateur de biens à double usage
  輸出入に関する規制であり、3.3.3.4. 章にまとめる。

- Law no. 2004-575, 21 June 2004 on confidence in the digital economy／Ordonnance n° 2005-1516 du 8 décembre 2005／Décret n° 2010-112 du 2 février 2010／Décret n° 2002-535 du 18 avril 2002
  政府調達に関する規制であり、3.3.3.3. 章にまとめる。

- Référentiel général de sécurité／Mécanismes cryptographiques（暗号技術）／Gestion des clés cryptographiques (暗号鍵管理)
  標準・基準に関するものであり、3.3.3.1. 章にまとめる。

- Law 2001-1062 of 15 November 2001 on daily security[45]
  復号支援(decryption assistance)と復号命令(decryption order)について定めている。復号支援について、捜査において暗号解読が必要な場合、適格な人物が、暗号解読または暗号鍵の引渡し要求権などを定める。復号命令については、命令に反する場合の罰

[44] http://www.wipo.int/wipolex/en/details.jsp?id=12761
[45] http://www.cryptolaw.org/cls2.htm#fr

金や懲役などの罰則を定めている。

3.3.3. 暗号に関わる各種制度及び規制

3.3.3.1. 利用すべき暗号方式

ANSSI／前身 DCSSI が暗号強度に関するルールと推奨についてまとめている。

- Référentiel Général de Sécurité (RGS)[46]
  セキュリティ全般の標準を規定している。政府システムへの適用が遵守事項となっているが、現状では完全に準拠されている訳ではない。第 2 版 [47]が 2014 年 6 月 13 日のアレテ(省令)で発表され、7 月 1 日に適用開始された。RGS の遵守事項のうち、暗号に関しては、Annex B1 に暗号技術（表 3-6)、Annex B2 に暗号鍵管理が記載される。
  - Mécanismes cryptographiques (暗号技術)
  - Gestion des clés cryptographiques (暗号鍵管理)

  Annex B1 では、暗号アルゴリズムとして、対称暗号(AES, Triple DES)、非対称アルゴリズム(RSAES-OASP)、署名(ECDSA, RSASSA-PSS)、ハッシュ関数 SHA-256 が例としてあげられている。

- “Cryptographic mechanisms Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level Version 1.10”, PRIME MINISTER General Secretariat for National Defence Paris, 2007 September 14 DCSSI,No. 1904/SGDN/DCSSI/SDS/LCR
  暗号強度に関する 2 つのレベル定義である「標準レベル」(第 1 レベル)、「強化レベル」(第 2 レベル)のうち、前者に関するルールと推奨についてまとめている。ルールに関しては、2010 年以降の対称暗号の最低鍵長を 100 ビット、非対称暗号の最低鍵長を 2048 ビット(2020 年以降を 4096 ビット)、楕円曲線暗号の最低鍵長を 256 ビット、最低ハッシュ値を 256 ビットとしている。

- “Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, Version 1.10”, 2006 , N° 2741/SGDN/DCSSI/SDS/LCR (Remplace la version 1.02 N°2791/SGDN/DCSSI/SDS/AsTeC/CD-SF du 19 novembre 2004)
  上記の英語文書のフランス語版である。

---

[46] http://www.ssi.gouv.fr/entreprise/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs/

[47] http://www.ssi.gouv.fr/entreprise/reglementation/administration-electronique/liste-des-documents-constitutifs-du-rgs-v-2-0/

表 3-6 ルールと推奨

	ルール	推奨
ブロック暗号	2020 年までの最低鍵長は 100 ビット、最低ブロック長は 64 ビット、100 ビット安全性を有する。 2020 年以降の最低鍵長は 128 ビット、ブロック長は 128 ビット、128 ビット安全性を有する。	推奨の最低鍵長は 128 ビット、ブロック長は 128 ビットで、かつ暗号学会で広く評価された暗号
ストリーム暗号	2020 年までは 100 ビット安全性を有する。 2020 年以降は 128 ビット安全性を有する。	ブロック暗号の利用を推奨
素因数分解	2030 年までは最低鍵長 2048 ビット 2030 年以降は最低鍵長 3072 ビット	推奨鍵長は 3072 ビットで、安全性証明が付いている
離散対数	2030 年までは最低鍵長 2048 ビット 2030 年以降は最低鍵長 3072 ビット	推奨鍵長は 3072 ビット、安全性証明が付いている
楕円曲線上の離散対数	2020 年までは最低鍵長 200 ビット 2020 年以降は最低鍵長 256 ビット	同左、かつ安全性証明が付いている
ハッシュ関数	2020 年までは最低ハッシュ値 200 ビットで、100 ビット安全性を有する 2020 年以降は最低ハッシュ値 256 ビットで、128 ビット安全性を有する	アタックが見つかっていない

3.3.3.2. セキュリティ認証制度

フランスにおけるセキュリティ認証制度は ANSSI が所管している。認証制度としては、CC 認証、CSPN、SSCD 評価、国防・国家安全保障に関する情報保護のための製品に与えられる「agrément」(承認)がある。

- コモンクライテリア認証(CC 認証)
  CC 国際承認アレンジメント(CCRA)の認証国として、CC 認証を行っている。ANSSI が認証および評価機関である Information Technology Security Evaluation Facilities (ITSEF)の認定を行っている。保証レベル EAL を決めて、要件を満たさない部分は、繰り返し改善する。ITSEF の評価に基づき、ANSSI は、製品認証を行う。認証製品およびプロテクションプロファイルは、ANSSI サイト [48,49]において公開されている。

[48] http://www.ssi.gouv.fr/administration/produits-certifies/cc/produits-certifies-cc/
[49] http://www.ssi.gouv.fr/administration/produits-certifies/cc/profils-de-protection/

- CSPN (First level security certification for information technologies)[50]
  フランス独自の認証プログラムで、ANSSI により開発された規準、技術、プロセスに基づき認証される。特に、サイバー攻撃に対する耐性に焦点をあてた評価を行う。評価を行う研究所において書類および製品について攻撃に耐えられるかどうかの評価を経た後、最後にプレゼンテーションによる審査が行われる。評価期間は、50 日と追加の 10 日までと限られており、一定の期間で結果が決まる。ANSSI によりライセンス付与された機関が評価を行う。

- SSCD 評価
  署名生成機器 Secure Signature Creation Devices (SSCD)に組み込まれる暗号モジュールについて、欧州について規定される要件として、欧州ガイド CWA 14924 2004-03[51]に基づき評価を行っている。CC, CSPN は、暗号モジュールについて明確に切り出していないが、SSCD 評価は暗号モジュールに焦点を当てたものである。

- 「agrément」
  ANSSI が付与する製品ラベルの一種であり、国防、国家安全保障に関する情報保護のためのラベルである[52]。

CC 認証、CSPN、SSCD 評価の関係比較

CC 認証は国際標準に基づく認証制度であり、CSPN は、フランス独自の基準に基づく認証である。CC 認証と比べて低価格で認証が取得できるように、評価項目を特定のサイバー攻撃に限定している。CC 認証よりも CSPN の方が手頃に利用できるため、特に、スマートカードやハードウェア関連製品については、民間からの評判は良く、マーケティング上の評価の向上につながるなど、産業振興の点で成功している[53]。CSPN は、CC 認証を取得する前段階としても、導入できるように設計されている。

また、CC 認証を補完するものとして、政府システムで用いられる製品に対する「資格証(qualification)」[54]がある。これは、政府が、ソースコードへのアクセスができるようにソースコードを開示しているかどうかや、どこで開発・製造が行われたか(仏製製品のみを採用するなど)といった点が検証される。CC と組合せて利用される場合もある。

暗号モジュールに関する認証制度 CMVP はフランスでは実施していないが、それに代わるものとして SSCD 評価が行われている。

3.3.3.3. 政府の調達要件

RGS に基づき、政府システムにおいては、システムに応じて ANSSI が実施する製品認

[50] http://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/
[51] CWA 14924 2004-03 European guide to good practice in management knowledge
[52] ANSSI ヒアリングによる。
[53] ANSSI ヒアリング結果による。
[54] http://www.ssi.gouv.fr/administration/qualifications/

証(CC 認証、CSPN 等)が義務化されている。政府調達に関する暗号要件に関連するものとして以下のような法令がある。

- Law No. 2004-575 of 21 June 2004 on confidence in the digital economy
  デジタル著作物に対する著作権に関して ID 認証が可能であるようにする必要性があることを規定している。

- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
  行政システムにおける情報セキュリティを規定している（Article 9)。

- Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
  上記 Ordonnance(規定)の行政システムにおける情報セキュリティの規定に対する施行令を定めている。

- Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information[55]
  セキュリティ製品・システムに関するフランスの認証フレームワークを規定する。

3.3.3.4. 暗号の輸出入規制

ワッセナー・アレンジメントに署名し、「一般ソフトウェアに関する注記(General Software Note : GSN）」付きの輸出規制を行っている[56]。輸出入は、Law No. 2004-575[57]、Decree No. 2007-663 of 2 May 2007[58] に基づき規制されている。認証や Decree No. 2007-663 Annex に挙げられる暗号は規制対象外である。EU/EEA からの輸入は自由。特定のカテゴリ以外については輸出は認可性であり、懲役、罰金等の罰則規定がある。

- Law No. 2004-575 of 21 June 2004 on confidence in the digital economy
  条項 Article 30-I において、フランス国内における暗号化手段の利用が自由とされている[59]。

[55] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005632663
[56] http://www.cryptolaw.org/cls2.htm#fr
[57] Law no. 2004-575, 21 June 2004 on confidence in the digital economy
[58] Decree No. 2007-663, 2 may 2007, in application of the law (no. 2004-575, 21 June 2004 on confidence in the digital economy).
[59] Regulation, Cryptology, ANSSI, http://www.ssi.gouv.fr/en/regulation/cryptology/

- Décret n°2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie.
  EU, EEA(欧州経済圏)の域外からの暗号輸入と輸出を規制する政令である。Annex には、規制の免除対象として、56 ビット鍵長以下の対称暗号、512 ビット以下の素因数分解に基づく非対称暗号が挙げられている。

- Guide de l'exportateur de biens à double usage
  デュアルユース物品及びテクノロジーの輸出に関するガイドラインを規定する。暗号技術については ANSSI が所管する。

3.3.4. その他

産業振興に関して、ANSSI は基本的に政府機関および重要インフラのサイバーセキュリティを担当するが、民間とはパスポート、ID カード、銀行カード、有料 TV といった分野での協力を行っている。具体的方法としては、銀行カードや有料 TV のセットトップボックスのセキュリティ認証や、業界団体と規格に関するワーキンググループを作るといった形での協力を行なっている。

3.3.4.1. 人材育成

新たな課題として、エンジニアの教育、学生の教育などが挙げられる。これは、国防安全保障白書に示されている暗号専門家の不足に対する解決法として挙げられるものである。教育的プログラムの責任を追うのは教育省であるが、ANSSI でも行政機関用の研修を行っている。

ANSSI 内には、information center、training center を設置している。これらは基本的には、政府機関を対象とした人材育成であるが、次第にオープン化しつつある。また、新しいガイドブックとして、2011 年に ANSSI が Information systems defence and security France's strategy を発行しており、その文書においてセキュリティオフィサーの設置などを挙げている。

一方、ENS の研究チームの業務は研究が中心であり、スタッフに課される教育業務は少ない。CNRS、INRIA の研究者は研究することだけが契約内容となっている。

暗号の授業としては、暗号の基礎クラスが 1 つ(Licence (学士課程)3 年目において)、暗号に関するアドバンスト・コースが 2 つ(Master(修士)2 年目において)があるのみ。これらの授業は、ほかの学校(大学、グランゼコール)の学生にも開かれている。修士の授業は、ENS、エコール・ポリテクニーク、パリ第 6、第 7、第 11 大学が共同開催している。

暗号研究においては、フランスでは CASCADE チームが中心的であり、多くの研究者は CASCADE チームからはじめ、他の大学に行くものがほとんどである[60]。

[60] 有識者ヒアリングによる。

3.3.4.2. 研究開発

フランスにおける暗号研究開発の中心的な組織として、CNRS、ENS、INRIA(国立情報学自動制御研究所)から研究者が参加している CASCADE チームがある。CASCADE チームのすべての研究者は ENS に集まり研究を行っており、ECYRPT II パートナーとしても参加した。チームリーダーは CNRS、ENS、INRIA を兼任する Pointcheval 氏である。

CASCADE チームは、常勤研究者 6 人、学生約 15 名から構成される。ANRT (Association Nationale Recherche Technologie; 国立テクノロジー研究協会)が実施する CIFRE (Conventions Industrielles de Formation par la REcherche; 研究を通じた研修に関する産業協定)を通じた奨学金により、企業からの研究者を受け入れて研究を実施している。

CASCADE チームの研究連携先として、ベルサイユ大学、ENS リヨン(リヨン高等師範学校) 、リモージュ大学、ボルドー大学、ENS カシャン(カシャン高等師範学校、数論、フォーマルメソッド)、ANSSI、パリ第 6 大学がある。

CASCADE チームでは、公開鍵暗号の設計と証明を中心として、暗号のランダム性、格子暗号、インターネットの並列性におけるセキュリティなど幅広く暗号の研究をしている。近年は、CASCADE チームでは、クラウドの暗号技術に焦点をあてている。特に、クラウド環境で、相手にデータの中身を秘匿したまま、復号せずに平文を処理した結果の暗号文を得られる暗号である FHE (Fully homomorphic encryption)に重点を置いている。

3.3.4.3. サービスにおける暗号利用

フランスにおいては、暗号化政策と個人情報保護政策は明確に区別されており、個人情報保護に関しては、CNIL(情報処理・自由全国委員会)が担当している。個人情報保護に関連して CNIL は、公開するクラウドサービスに関する以下の 2 つの勧告文書を公開している[61]。

- Summary of responses to the public consultation on Cloud computing
- Recommendations for companies planning to use Cloud computing services

前者の文書においては、クラウドサービスプロバイダと利用者間の通信における暗号化だけでなく、利用者側のレベルで暗号化を行うことでリスクを低減する必要性を挙げている。暗号化に使うアルゴリズムについては言及していない。

[61] http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-cnils-recommendations-for-companies-using-these-new-services/

3.4. ドイツ

ドイツにおける情報セキュリティ政策は BSI が中心的な役割を果たしている。また各州政府の IT 担当者による IT-Rat の意見も BfIT の調整によって反映される。暗号要件を含む主なセキュリティ基準・標準である Standards and Architectures for eGovernment Applications (SAGA)が連邦政府の調達おける最上位の文書[62]であり、BSI が主管している。

3.4.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

ドイツにおいて、暗号技術を含む IT 製品の連邦政府の調達は BFI 管理のもと BMI と IT-SB が方針を決定している。一方、州政府の調達方針等は IT-Rat を通じて調整されている。IT-SB と IT-Rat 間を BfIT がコーディネーションしている。安全保障に関わる政府調達については BSI が取り扱っている。

研究開発、人材育成に関しては DFG と連携しつつ、BSI が主に取り扱っている。また、武器や民生品とのデュアルユース製品については BAFA による輸出規制がある。電子署名については BnetzA が担当してる。

図 3-9 に関連組織の全体像を示す。主な組織の要点をまとめると以下のようになる。

- BMI (連邦内務省)
  国内治安の維持やパスポートや ID カードの発行に関わる法律を主管している。IT 製品の調達を BFI 管理の下、統括している。

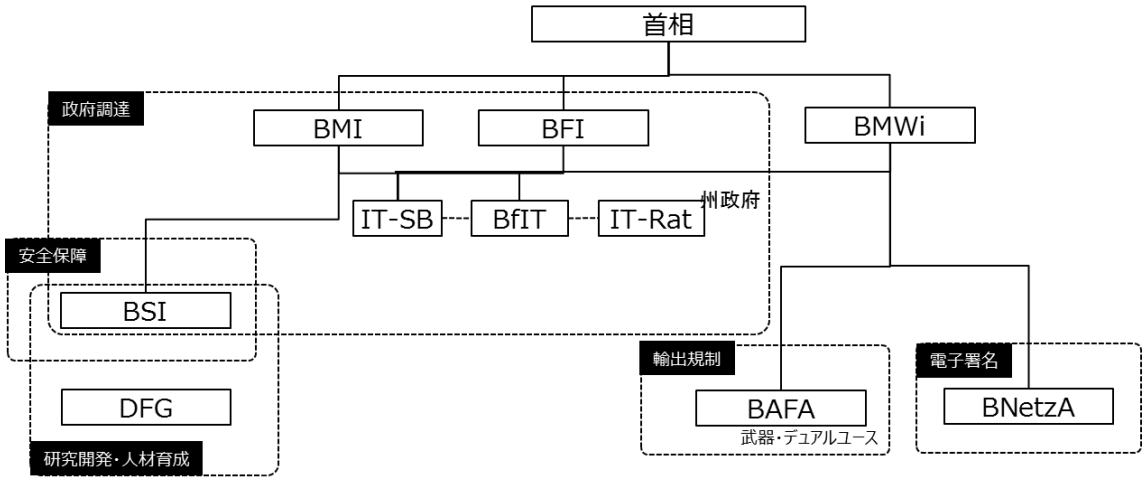
- BSI (連邦情報セキュリティ局)
  ドイツにおける暗号政策を主管する部署で、BMI の直下に設置されている。情報技術のセキュリティ促進が設立趣旨であり、具体的にはドイツの情報技術の防護、IT セキュリティリスクの情報収集・分析、IT セキュリティ研究、暗号アルゴリズムの研究等である。

- BfIT (連邦情報技術長官)
  2007 年の閣議決定 IT-Steuerung Bund に基づき設置。州政府 IT 担当者協議会の代表であり、スーパーバイザーである。IT セキュリティ戦略の策定や、政府の IT セキュリティ管理、アーキテクチャ・基準や手法の開発等の IT 関連の課題の方針を決定する。

- BFI (財務省)
  政府調達も財務省の管理下で行われる。

- BMWi (ドイツ連邦経済・技術省)
  政府調達へ直接的には関係していないが、IT 関連の政策方針には IT-SB を通して権限を持っている。

[62] IT-Rat の決議により、SAGA Var.5 が連邦政府の必須要件となっている。強制力を持つ。
http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/saga_node.html



BMI：Bundesministerium des Innern (Federal Ministry of the Interior：連邦内務省)

BSI：Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security ：連邦情報セキュリティ局)

BfIT：Die Beauftragte der Bundesregierung für Informationstechnik (the Federal Government Commissioner for Information Technology：連邦情報技術長官)

BFI：Bundesministerium der Finanzen (Federal Ministry of Finance：財務省)

BMWi：Bundesministerium für Wirtschaft und Energie (Federal Ministry for Economic Affairs and Energy：ドイツ連邦経済・技術省)

BNetzA：Bundesnetzagentur (Federal Network Agency：連邦ネットワーク庁)

BAFA：Bundesamt für Wirtschaft und Ausfuhrkontrolle (Federal Office for Economic Affairs and Export Control：経済・輸出管理局)

IT-SB：IT-Steuerungsgruppe des Bundes (Federal IT-Steering group 連邦 IT ステアリンググループ)

IT-Rat：Rat der IT-Beauftragten (Council of IT Officer：州政府 IT 担当者協議会)

DFG：Deutsche Forschungsgemeinschaft (German Research Foundation)

図 3-9 暗号政策に係る組織体制(ドイツ)

- BnetzA (連邦ネットワーク庁)
  BMWi の下に設置された、電気、ガス、通信、郵便及び鉄道分野を主管する。電子署名法に基づくルート CA(ルート認証局)である。

- BAFA (経済・輸出管理局)
  BMWi の下に設置された輸出管理を行う組織。

- IT-SB (連邦 IT ステアリンググループ)
  2007 年の閣議決定 IT-Steuerung Bund に基づき設置。連邦政府の IT 関連政策と予算の連携を強化することを目的とする。現在は BMI と BFI、BMWi の権限の下に設置されている。

- IT-Rat (州政府 IT 担当者協議会)
  2007 年の閣議決定 IT-Steuerung Bund に基づき設置。各州政府の IT 担当者による協議会。州政府の調達等について権限を持つ。

- DFG (German Research Foundation)
  ドイツの大学、大学以外の研究機関、科学および人文科学アカデミーにより構成された学術研究のための財団。州や連邦政府からの補助金によって運営されている。

3.4.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

ドイツの暗号政策は安全保障にプライオリティがあると考えられる [63]。市民の利用を規制する意図はないとしているが、政府の諜報能力が損なわれないように監視を行うとされている。また、ドイツにおける政府調達は Standards and Architectures for eGovernment Applications (SAGA)である。暗号アルゴリズムの選定に関しても強制力を持つ。この SAGA のうち暗号方式について具体化したものが Kryptographische Verfahren (暗号方式・鍵長推奨リスト)である。

ドイツにおける主な法制度を分類整理すると表 3-7 と図 3-10 のようになる。

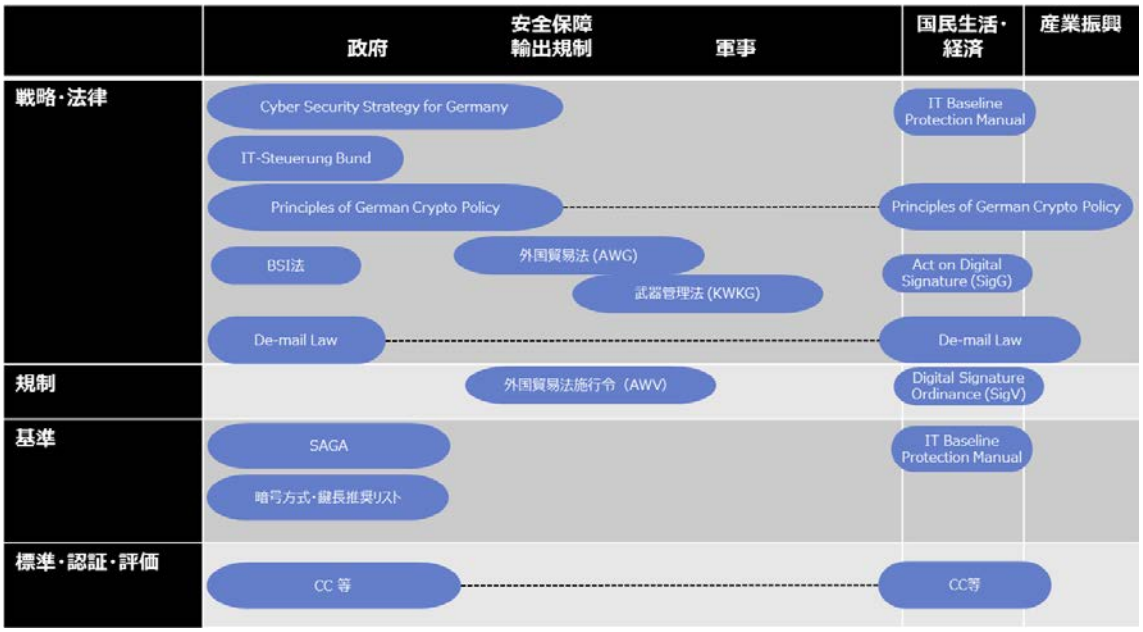


図 3-10 ドイツにおける暗号関連政策マップ

[63] Eckpunkte der deutschen Kryptopolitik 1999 (Principles of German Crypto Policy：ドイツにおける暗号政策の要点)に記載されている。

表 3-7 法制度の分類と一覧(ドイツ)

分野	名称	関係組織
上位政策・戦略	Cyber Security Strategy for Germany	BMI, BSI
	IT-Steuerung Bund （Federal IT Control/Governance)	閣議決定
暗号政策・設置法	Eckpunkte der deutschen Kryptopolitik 1999 （Principles of German Crypto Policy)	閣議決定
	Act on Digital Signature (SigG), Digital Signature Ordinance (SigV)	BNetzA
	Act to Strengthen the Security of Federal Information Technology(BSI 法)	BSI
輸出入規制	外国貿易法（AWG）、外国貿易法施行令（AWV)	BAFA
	武器管理法 (KWKG)	BAFA
政府調達	Standards and Architectures for eGovernment Applications (SAGA)	BMI, BfIT, BSI
	Technische Richtlinien Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102-1)	BSI
	Verwendung von Transport Layer Security (TLS) (BSI TR-02102-2)	BSI
	Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2) (BSI TR-02102-1)	BSI
標準・基準	IT Baseline Protection Catalogues (IT-Grundschutz)	BSI
	Guidelines for Developer Documentation according to Common Criteria Version 3.1	
	BSI 7138 Technical information on the IT security certification of products, protection profiles and sites	BSI
その他	De-mail Law	BMI

主な法制度の概要は以下の通りである。

- Cyber Security Strategy for Germany[64]

  2011 年 2 月に策定された社会、企業、行政に大きな影響を与える可能性のあるサイバー攻撃に対処するための戦略的フレームワークである。目的は以下の通り。
  - 重要インフラ防護
  - ドイツの IT システムの安全確保
  - 行政 IT システムの強化
  - 国家サイバー対応センターの設置
  - 国家サイバーセキュリティカウンシルの設置

[64] Cyber Security Strategy for Germany
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile

- サイバー空間における犯罪のコントロール
- 欧州、世界におけるサイバーセキュリティ強化のための効果的な協力体制
- 信頼できる情報技術の利用
- 連邦当局における人材育成
- サイバー攻撃対応ツールの確保

- IT-Steuerung Bund (Federal IT Control/Governance)
  2007 年 10 月の閣議決定。BfIT や IT-Rat、IT-SB の設置を規定し、IT に関する政策的課題に関して BfIT が連邦政府及び州政府の方針を調整することとしている。

- Eckpunkte der deutschen Kryptopolitik 1999 (Principles of German Crypto Policy : ドイツにおける暗号政策の要点)
  1999 年 2 月に制定された連邦政府による暗号政策に関する声明であり、以下のようなドイツにおける暗号分野の競争力強化等を謳っている。改訂作業は進められていないようである[65]。
  - 市民による暗号製品の自由な利用の保証(政府による規制をしない)
  - 連邦政府による暗号化製品のテスト等を通じた信頼のフレームワークの構築及び認定製品の利用推奨
  - 安全保障確保のため、連邦政府による暗号関連ベンダーの国際競争力強化措置
  - 強力な暗号技術の普及による法執行機関・治安当局の諜報能力が損なわれないように、監視を行う
  - 暗号政策における国際協力の重視(オープンスタンダード、相互運用性の重視)

- Act on Digital Signature (SigG)／Digital Signature Ordinance (SigV)
  1997 年に制定された電子署名の有効性を規定する法律とその施行令である。ルート認証局を BNetzA と規定している。暗号アルゴリズムに関する記述はない。

- Act to Strengthen the Security of Federal Information Technology (BSI 法)
  2009 年に公布された BSI の設置法である。情報技術のセキュリティ促進が設立趣旨であり、具体的にはドイツの情報技術の防護、IT セキュリティリスクの情報収集・分析、IT セキュリティ研究、暗号アルゴリズムの研究等である。

- 外国貿易法 (AWG) ／外国貿易法施行令 (AWV)／武器管理法(KWKG)
  3.4.3.4. 章にて記載。

- Standards and Architectures for eGovernment Applications (SAGA)／Technische Richtlinien Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102-1)／Verwendung von Transport Layer Security (TLS) (BSI TR-02102-2)／Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange

[65] ドイツの研究機関へのヒアリングによる。

(IKEv2) (BSI TR-02102-1)
3.4.3.1. 章にて記載。

- IT Baseline Protection Catalogues (IT-Grundschutz)[66]
  組織の IT システムに関する標準的なセキュリティ対策、実装上のアドバイス、IT システムの設定に関する支援などを示すマニュアルである。暗号アルゴリズムの選択方法、鍵長、暗号製品の選択方法などについて規定している。IT-Grundschutz は、複数の言語で公開されており、エストニアにおけるセキュリティ対策基準 ISKE の策定のベースとして利用されるなど国際的にも参考とされている。

- Guidelines for Developer Documentation according to Common Criteria Version 3.1 ／BSI 7138 Technical information on the IT security certification of products, protection profiles and sites
  3.4.3.2. 章にて記載。

- De-mail Law
  3.4.4.4. 章にて記載。

3.4.3. 暗号に関わる各種制度及び規制

3.4.3.1. 利用すべき暗号方式

ドイツにおける暗号方式を含む電子政府システムの実質的な標準として SAGA がある。更に BSI が一般システム開発者向けのガイドライン(テクニカルガイドライン：BSI TR-02102-1, 2, 3)を公開している。

- Standards and Architectures for eGovernment Applications (SAGA)[67] (電子政府アプリケーションにおける標準とアーキテクチャに関する文書)
  BfIT によるドイツにおける電子政府のアプリケーションについて、相互運用性や拡張性等のための標準、アーキテクチャ、インフラ、仕様や技術についての推奨事項について説明した文書であり、強制力を持つ。機密情報の送信における暗号化、電子署名における暗号アルゴリズムの要件や義務を規定している(表 3-8)。現在は 2011 年に発行された SAGA5.1[68]が最新である。

[66] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
[67] Standards and Architecture for eGovernment Applications
http://www.egov-conference.org/glossary/standards-and-architecture-for-egovernment-applications
[68] SAGA 現行版
http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/SAGA%205-aktuelle%20Version/saga_5_aktuelle_version_node.html

表 3-8 SAGA 指定暗号

区分	義務	推奨	継続利用
非対称暗号	—	RSA	－
対象暗号	AES	—	IDEA, Triple DES, Chiasmus
電子署名	—	RSA、DSA	－
ハッシュ関数	SHA-2	—	SHA-1, RIPEMD-160

- Technische Richtlinien Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102-1) (暗号方式：推奨暗号方式及び鍵長)[69]
  (電子政府システム以外の)システム導入を計画する開発者を対象とし、一般的な設定における暗号の適切な使用に関する推奨事項を記載した2014年に改訂された指針である。強制力を持たないことを冒頭で宣言し、2 章から 5 章にわたり推奨暗号を示している。主な推奨暗号は表 3-9 のとおりである。

表 3-9 推奨暗号方式

区分	推奨暗号
非対称暗号	ECIES (250bit)、DLIES (2000bit)、RSA-OAEP (2000bit)
対称暗号	AES-128, AES-192, AES-256
メッセージ認証	CMAC、HMAC、GMAC
電子署名	DSA (2000bit)、RSA-PSS (2000bit)、ECDSA (250bit)、EC-KDSA (250bit)、EC-GDSA (250bit)
ハッシュ関数	SHA-224、SHA-512/224、SHA-256、SHA-512/256、SHA-384、SHA512
	(2016 年から) SHA-256、SHA-512/256、SHA-384、SHA-512

- Verwendung von Transport Layer Security (TLS) (BSI TR-02102-2) (TLS の使用方法)[70]
  TLS における推奨暗号は TR-02102-1 に準じる。

[69] Kryptographische Verfahren: Empfehlungen und Schlüssellängen
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf.html
[70] Verwendung von Transport Layer Security (TLS)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.html

- Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2) (BSI TR-02102-3) (IPsec 及び鍵交換(IKEv2)の使用方法)[71]
  IPSec 及び IKE における推奨暗号は TR-02102-1 に準じる。

また、電子署名における最適な暗号アルゴリズムについては、以下の文書が公開されている。

- Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, version of 13th January 2014 (電子署名法及び電子署名規則の公示)[72]
  電子署名に関するアルゴリズム（署名・ハッシュ関数)、鍵長や乱数生成とそのスキームについて述べられている。推奨されているアルゴリズムは表 3-10 の通りである。

表 3-10 推奨アルゴリズム

種類		2015 年まで推奨	2020 年まで推奨
ハッシュ関数		SHA-224 (SHA-1, RIPEMD-160)* *：署名には利用不可	SHA-256 SHA-384, SHA-512 SHA-512/256
電子署名	RSA-PSS	－	最低鍵長 1976bit 推奨鍵長 2048bit
	DSA	最低鍵長 2048bit 最低qパラメータ 224bit	最低鍵長 2048bit 最低qパラメータ 256bit
	ECDSA、 EC-KCDSA 、 EC-GDSA 、 Nyberg-Rueppel-Signaturen	最低鍵長 224bit	最低鍵長 250bit

3.4.3.2. セキュリティ認証制度

ドイツは、CCRA での CC 認証国となっており、CC に基づくセキュリティ製品認証は BSI が所管している。なお、米国における CMVP に対応する暗号モジュールに関する認証制度はない[73]。

[71] Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3_pdf.html

[72] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung, version of 13th January 2014
http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2014Algorithmenkatalog.pdf

[73] ドイツの研究機関へのヒアリングでも確認済み。

CC 認証についての文書および基準等には、以下のものがある。

- BSI 7138 Technical information on the IT security certification of products, protection profiles and sites(including confirmations pursuant to the SigG)[74]
  IT セキュリティに係わる政府による認証方針について、ベンダ等に対する技術的な情報を提供する。Digital Signature Act に係わる製品に関しては、評価認証に先立ち、定められた要件を満たしているか検査される。

3.4.3.3. 政府の調達要件

暗号技術を含む IT 製品の連邦政府の調達は BFI 管理のもと BMI と IT-SB が方針を決定している。安全保障に関わる政府調達については BSI が取り扱っている。
政府情報システムの調達に関する主な文書には以下のものがある。

- Standards and Architectures for eGovernment Applications （SAGA）
  電子政府のシステム調達要件であり、調達要件における実質的な国家方針と言える。
  暗号方式の要件は 3.4.3.1. 章に記載。
- IT-Steuerung Bund （Federal IT Control/Governance）
  連邦政府 IT システムの管理とガバナンスに関する基準を定めている。

なお、CC 認証に関しては、公式サイト[75]に関連文書がまとめられているが、これらの情報から CC 認証が政府調達において義務か任意であるかについては情報は確認できなかった。

3.4.3.4. 暗号の輸出入規制

暗号技術の輸出入規制は、EU 輸出規制およびワッセナー・アレンジメントに基づいており、ドイツ固有のものは無い。EU 域内のマスマーケット暗号システムの輸出は自由化されている。輸出に係わる法律には以下のものがある。

- 外国貿易法（AWG）
- 外国貿易法施行令（AWV）
- 武器管理法（KWKG）

---

[74] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/7138_e_pdf.pdf?__blob=publicationFile

[75] BSI 製品認証公式サイト
https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html

3.4.4. その他

3.4.4.1. 産官連携

セキュリティ分野における産官連携の取組みとしてはAlliance for Cyber Securityがある。また、国民IDカード(German ID card)には電子署名等で暗号技術が利用されている。これらの暗号技術は民間により提供されている。

- Alliance for Cyber Security[76]
  ドイツ全土の参加者間でサイバーセキュリティに関する知見を共有することを目的とし、BSI及びBITCOM[77](Federal Association for Information Technology, Telecommunications and New Media)の主導のもと設立されたアライアンス。アライアンスの目的としては、サイバーセキュリティの向上に資する最新かつ有効な情報を提供することである。アライアンスには1000団体以上が参加し、Fraunhofer研究所をはじめとする研究機関や、IBMドイツ支社といった民間企業、ベルリン工科大学等の教育機関が参加している[78]。参加者のうち、サイバーセキュリティ分野でより専門性の高い知見を有する団体が「パートナー」となり、パートナーからの情報発信や、参加者間で知見を交換するために定例のフォーラムやワーキンググループが開催されている。ウェブサイトにはパートナー企業の作成した報告書等が収集され、検索できるようになっている。全てドイツ語で公開されている。

- German ID card
  ドイツの新しい国民IDカードである。2011年頃より配布が開始され、2021年に100%普及させる計画で進められている。IDカードに搭載されている電子署名は政府からではなく、民間から提供されているとのことである。ID cardにおける暗号の利用としては、VoIPの認証、暗号化などが挙げられる[79]。

3.4.4.2. 人材育成

基本戦略"Cyber Security Strategy for Germany"において、連邦政府機関の人材育成について規定している。サイバーセキュリティの目的で、行政機関内にスタッフの増員が必要かどうかを優先事項として検討する必要性があることをあげている。さらに、連邦政府機関内のスタッフの人材交流と研修は、省庁協力の強化に繋がることをあげている。

---

[76] Alliance for Cyber Security
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html
[77] Federal Association for Information Technology, Telecommunications and New Media
http://www.bitkom.org/en/
[78] Alliance for Cyber Securityの参加者リスト
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/Teilnehmer/teilnehmer.html
[79] ドイツの研究機関へのヒアリング情報による。

3.4.4.3. 研究開発

Fraunhofer 研究所は政府組織 BSI、BMWi と密接に連携し、研究調査ファンディングを獲得を行っている。Fraunhofer 研究所は多数の研究所から構成され、そのうち ICT をテーマとしたグループの一つである SIT がある。SIT は 163 名の専門家が多様な分野を対象に研究を行っている。年間予算は 930 万ユーロ、研究の 15-20% は基盤としての暗号に関連するとされる [80]。暗号分野に限った話ではなく、SIT 全体としては、共同研究等を通して、TU Darmstadt CASED (Center for Advanced Research Darmstadt)や HAD EC SPRIDE 等の大学との関係が深い。

Fraunhofer 研究所のセキュリティに関する基礎調査・研究は、BSI のガイドラインや法律に影響を与えている。例えば、“De-Mail Law”は、約 10 年前の調査が影響を与えている。

3.4.4.4. サービスにおける暗号利用

De-mail サービス 81はドイツの電子政府におけるコミュニケーションサービスであり、市民、行政機関や企業の間で公的な電子文書をインターネットを介して交換できる。E-mail と異なり、送信者と受信者の身元確認と送受信の確認を行うことができる。

- De-mail law[82]
  2011 年 5 月に施行。De-mail サービスを取り扱うプロバイダに、最低限の基準として暗号化等を強制し、ユーザがどのプロバイダを選択しても、均一なセキュリティレベルが保証される。ただしエンド間の暗号化ではない [83]。具体的な暗号アルゴリズムについては指定していない。

[80] ドイツの研究機関へのヒアリング情報による。
[81] De-Mail http://www.bmi.bund.de/EN/Topics/IT-Internet-Policy/De-Mail/de-mail_node.html
[82] De Mail Law http://www.gesetze-im-internet.de/de-mail-g/
[83] ドイツの研究機関へのヒアリング情報による。

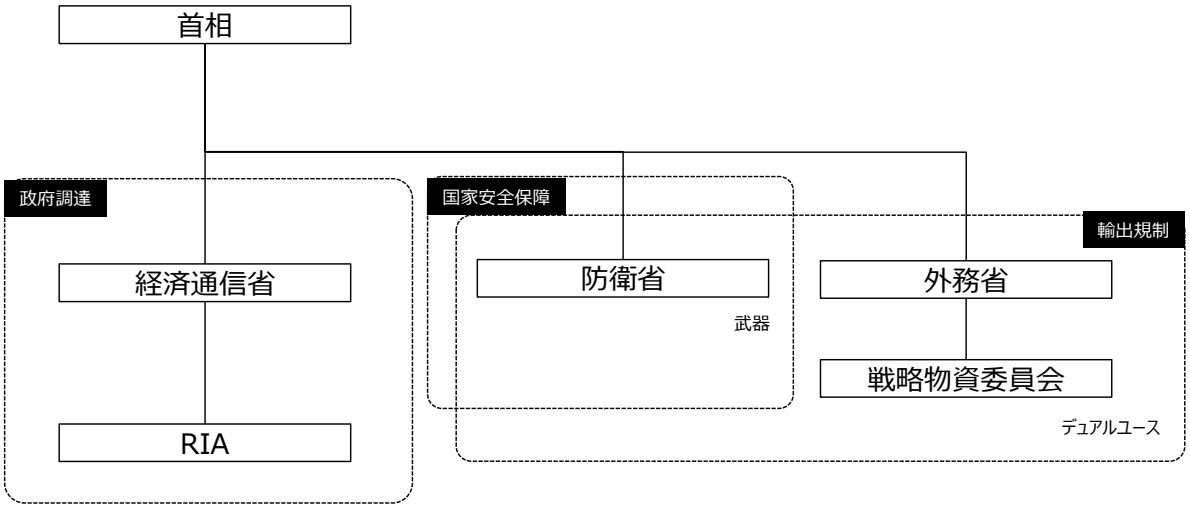
3.5. エストニア

エストニアではICチップを搭載した国民IDカードが普及しており、IDカードを利用した電子行政の利用も進んでいる。そのため、政府の情報や個人情報の大部分が電子データ化されていることや、電子署名が広く使用されていることから、サイバーセキュリティを国家レベルで重要視している。2008年には重要インフラ防護等を主目的とするサイバーセキュリティ戦略を策定し、2011年には情報システム局(RIA)を経済通信省の下へ設置し、政府の重要システムの防護やサイバーインシデント対応を行っている。

3.5.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

エストニアにおける暗号政策、特にITシステムに関わる政府調達については、RIAとその上部組織である経済通信省が主管であり、連携して取り扱っている。一方、国家安全保障に関わる調達については防衛省が主管し、輸出規制は防衛省及び外務省とその直下にある戦略物資委員会が主管している。

関連組織の全体像をまとめたものが図 3-11である。



経済通信省：Ministry of Economic Affairs and Communications
RIA (エストニア情報システム局)：Estonian Information System Authority
防衛省：Ministry of Defence (Kaitseministeerium)
外務省：Ministry of Foreign Affair (Välisministeerium)
戦略物資委員会：Strateegilise kauba komisjon

図 3-11 暗号政策に係る組織体制(エストニア)

- 経済通信省
  RIA の上部組織。IT システムの管理(政府調達を含む)を RIA とともに主管する。2013 年度予算は 5.8 億ユーロである [84]。

- RIA
  非機密レベルの文民系政府情報システムを主管し、その調達や運用、またインシデント対応や PKI の機能調整等を行っている。また、政府省庁のための意識啓発プログラムや情報セキュリティプログラム等を提供している。体制としては 83 名のスタッフである。

- 防衛省
  防衛系の情報システム(例えば National Security Agency、Information board 等)を所管している。

- 外務省
  戦略的通商法を主管している。内部に戦略物資委員会をもつ。

- 戦略物資委員会
  戦略物資リストの作成を行う。

3.5.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

エストニアではサイバーセキュリティ戦略が上位政策であり、定期的に見直され、更新されている。ただし暗号に関する記述はなく、具体的に暗号政策に関する文書としては RIA と研究機関である CYBERNETICA AS[85]が執筆した暗号アルゴリズムライフサイクルとなる。

エストニアにおける主な法制度を分類整理すると表 3-11 と図 3-11 のようになる。

主な法制度の概要は以下の通りである。

- Küberjulgeoleku strateegia (サイバーセキュリティ戦略)[86]
  サイバーテロからの防護を目的として政府横断的な対応体制をとるために定められた。サイバーセキュリティ戦略は、防衛省が主管となり、経済通信省、総務省、外務省、法務省、文部省、国防軍(Estonia Defence Force)、RIA、CERT-EE、民間の専門家等から構成される委員会にて承認される。現在、2014～2017 年の戦略の審議中である。2008～2013 年版の目的は以下の通り

[84] エストニアの予算
http://www.fin.ee/budgeting/?order=title_asc
[85] CYBERNETICA AS 政府系研究機関を前身とする、半官半民のソフトウェアやセキュリティ分野の研究開発機関である。
http://cyber.ee/
[86] Estonian Atlantic Treaty Association
http://www.eata.ee/eesti-nato-s/kuberjulgeoleku-strateegia

- 重要な情報インフラを防護する国家体制の確立
- 情報セキュリティに関する専門知識の増強
- サイバーセキュリティに必要な司法制度の確立
- 国際協力
- サイバーセキュリティ関連の国民意識啓発

- Krüptograaeku algoritmide kasutusvaldkondade ja elutsükli uuring (暗号アルゴリズムライフサイクル)
  3.5.3.1. 章にて記載。

- Majandus- ja Kommunikatsiooniministeeriumi põhimäärus Vastu võetud 23.10.2002 nr 323[87] (経済通信省設置法)
  経済通信省の設置法。政府情報システムの管理を行うことが示されている。

表 3-11 法制度の分類と一覧(エストニア)

分野	名称	関係組織
上位政策・戦略	Küberjulgeoleku strateegia 2008-2013 (サイバーセキュリティ戦略)	防衛省、関連省庁
暗号政策・設置法	Krüptograaeku algoritmide kasutusvaldkondade ja elutsükli uuring (暗号アルゴリズムライフサイクル)	RIA, CYBERNETICA AS
	Majandus- ja Kommunikatsiooniministeeriumi põhimäärus Vastu võetud 23.10.2002 nr 323 (経済通信省設置法)	経済通信省
	Riigi Infosüsteemi Ameti põhimäärus Vastu võetud 25.04.2011 nr 28 (RIA 設置法)	RIA
輸出入規制	Strateegilise kauba seadus, Vastu võetud 07.12.2011 (戦略的通商法)	外務省、防衛省
政府調達	Infosüsteemide turvameetmete süsteemi kehtestamine Vastu võetud 12.08.2004 nr 273 (情報セキュリティ体制; Government of the Republic Regulation no. 273 of 12 August 2004) (廃止)	RIA
	Infosüsteemide turvameetmete süsteem, 20.12.2007 nr 252 (情報システムセキュリティ)	RIA
	Infoturbe juhtimise süsteem, 15.03.2012 nr 26 (情報セキュリティマネジメントシステム)	RIA
標準・基準	ISKE (IT Security Standard)	RIA
その他	Digital Signatures Act	経済通信省、RIA

[87] Riigi Teataja https://www.riigiteataja.ee/akt/125062013005

図 3-12 エストニアにおける暗号関連政策マップ

- Riigi Infosüsteemi Ameti põhimäärus Vastu võetud 25.04.2011 nr 28[88]（RIA 設置法）
  RIA の設置法。以下の政府情報システムの管理を行うことが示されている。

  (1) サイバーセキュリティ
  - CIIP (Critical Information Infrastructure Protection)
    ヘルスケア、保安、経済活動等に関わる 42 のサービスを重要な情報システムインフラと設定し、これらを防護する目的で RIA 内部に設けられた部署である。
  - CERT-EE (Computer Emergency Response Team of Estonia)
    2006 年に立ち上げ、「.ee」ネットワークにおけるセキュリティインシデントへの対応(情報収集、分析、技術的サポート等)を行っている。

  (2) 国立 PKI (national Public Key Infrastructure)
  エストニアでは国立 PKI を設置しており、国家レベルで PKI の機能の確保を保証している。PKI はエストニアにおいて、IID カード、モバイル ID 等の基盤となっているため、ID カードにおけ基本的なソフトウェアの開発等も RIA が担っている。ただし ID カードの発行等は総務省が担当している。

- Strateegilise kauba seadus, Vastu võetud 07.12.2011 (戦略的通商法)
  3.5.3.4. 章にて記載。

- Infosüsteemide turvameetmete süsteemi kehtestamine Vastu võetud 12.08.2004 nr 273 (情報セキュリティ体制)／Infosüsteemide turvameetmete süsteem, 20.12.2007

[88] Riigi Teataja
https://www.riigiteataja.ee/akt/128042011001?tegevus=telli-teavitus

nr 252 (情報システムセキュリティ)／ISKE (IT Security Standard)
3.5.3.3. 章にて記載。

- Infoturbe juhtimise süsteem, 15.03.2012 nr 26 (情報セキュリティマネジメント体制)[89]
  政府機関における情報セキュリティマネジメント体制及び、首相や大臣の情報セキュリティ責任者としての任務について制定した規制である。インシデント発生時には、情報システムセキュリティ体制(Infoturbe juhtimise süsteem, 15.03.2012 nr 26)に則り、CERT-EE への報告や 3 ヶ月毎のレポート提出が義務付けられている。2012 年発効、2013 年改正。

- Digital Signatures Act[90]
  デジタル署名が手書きの署名と同様に扱われることを定めた法律である。デジタル署名に使用される秘密鍵と公開鍵は、本人の同意のもと認証サービスプロバイダや機関から発行されるとしている。使用される暗号方式についての言及はなされていない。

3.5.3. 暗号に関わる各種制度及び規制

エストニアでは、政府情報システムの大部分を RIA が所管しており、ISKE 標準に則ることが定められている。また、「暗号アルゴリズムライフサイクル」に推奨暗号が記載されている。

3.5.3.1. 利用すべき暗号方式

エストニアにおける推奨暗号に関する文章は以下のものがある。

- Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring (暗号アルゴリズムライフサイクル)[91]
  RIA と Cybernetica AS が民間や国家機関のシステム向けの推奨暗号方式についての国際レポートや論文を総括している。安全性に基づいた推奨であり、強制力はなく、また ISKE と直接的な連携はしていないと考えられる。表 3-12 に示す通り、2 年以内に SHA-1 と RSA-1024 を一新することになる。本文献において、RSA-1024 や Triple DES が 2011 年以前に発行された ID カード類に採用されていることに触れられている（エストニア語でのみ)。

[89] Riigi Teataja https://www.riigiteataja.ee/akt/119032012004
[90] Riigi Teataja https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/530102013080/consolide
[91] Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring (2013) http://www.id.ee/index.php?id=36589

表 3-12 推奨暗号リスト

推奨できない暗号	DES, A5/1, A5/2, RC4, RSA-512, RSA-768, MD5, RIPEMD-128
(2013 年から) 2 年間利用可能	SHA-1, RSA-1024,
(2013 年から) 5 年間利用可能	Triple DES, Kasumi
(2013 年から) 5 年間安全	Blowfish, AES, RSA-2048, SHA-2, SHA-3, RIPEMD-160

3.5.3.2. セキュリティ認証制度

エストニアはコモンクライテリア(CC)認証制度、暗号モジュール認証制度ともに対応していない。制度運用における資金の制約が理由であるが、CC については現在対応のためのレビュー段階にある。

3.5.3.3. 政府の調達要件

エストニアの電子政府システム、及び国防系以外の情報システムの調達は、経済通信省と RIA で主管している。政府系システムの調達基準としては ISKE へ則ることが義務となっている。

なお、ID カードシステムについては新システムへ抜本的な移行を計画しており、2016 年に調達にかけられる予定となっている。この新システムについて、政府は現在関係企業へ助言を求めている。

- IT Baseline Security System ISKE (ISKE 標準)[92]
  2003 年に策定された、エストニアの政府情報システムのセキュリティ標準。その後 1~2 年ごとに更新されている。2004 年にデータベース等を取り扱う地方公共団体や国家機関での利用が義務付けられた。扱うデータやシステムの重要度に基づき情報システムのセキュリティ要件を 3 段階のベースラインにて提示している。
  ドイツの「IT Baseline Protection Manual (IT ベースライン保護マニュアル：IT-Grundschutz[66])」を基に策定したものであり、ISO1335/17799 に整合しており、ヨーロッパにおける標準や米国 NIST SP 800 シリーズにも対応している。暗号アルゴリズムに関する具体的な記述はないと考えられる [93]。

- Infosüsteemide turvameetmete süsteemi kehtestamine Vastu võetud 12.08.2004 nr 273 (情報セキュリティ体制)[94]／Infosüsteemide turvameetmete süsteem, 20.12.2007 nr 252 (情報システムセキュリティ体制)[95]
  データベースとそれに関連する情報資産を扱う情報システムにおけるセキュリティ要

[92] ISKE https://www.ria.ee/iske-en
[93] エストニアの研究機関へのヒアリングによる。
[94] Riigi Teataja https://www.riigiteataja.ee/akt/12794423
[95] Riigi Teataja https://www.riigiteataja.ee/akt/13125331

件等を ISKE に則ることを制定した規制である。ただし国家機密レベルのシステムは対象外としている。nr 273 は 2004 年発行、2008 年廃止。替わって、nr252 が 2008 年発効、2009 年改正。

3.5.3.4. 暗号の輸出入規制

エストニアにおいて、輸入に関する規制はないが、輸出に関してはワッセナー・アレンジメントに則っている。参考となる文書は以下のものがある。

- Strateegilise kauba seadus, Vastu võetud 07.12.2011 (戦略的通商法)[96]
  戦略的物資の出荷を規制するための法律。戦略的物資委員会の設置についてもこの法律で定められている。

- Strateegiliste kaupade nimekiri (戦略物資リスト)[97]
  戦略的物資リストは上述の戦略的通商法にて定められている、①軍事品、②国防関連リスト、③人権侵害に関わる物品、④デュアルユース品から構成される。③人権侵害に関わる物品とは、死刑や拷問、その他の残虐な行為にて使用される物品であり、EC 規則 No 1236/2005 に準拠している。④デュアルユース品は、EC 規則 No 428/2009 に準拠してている。

3.5.4. その他

エストニアでは電子政府の活用が非常に進んでおり、電子政府システムを国外へ積極的に輸出する動きも起こっている。安全な電子政府を運用のためにもサイバーセキュリティ分野の研究が重視されている。全体の研究者数が限られているため、暗号分野に特化した研究室や研究プログラムはないと考えられる。

3.5.4.1. 産官連携

産官学の連携についてはあまり行われていないが、電子政府システムの開発や利用者として民間企業が関与している。また、サイバーセキュリティに関する産業界と RIA の定例会議も設定されていると言われいてる [98]。

- 電子政府システム
  電子政府システムで個人や政府機関、民間企業等のデータ連携を可能とするシステムが X-road[99]である(図 3-13)。2013 年時点では 170 のデータベースと 2000 以上のサービスが X-road 上で連携しており、900 以上の団体が日常的に X-road を利用している。

[96] Riigi Teataja 「Strateegilise kauba seadus」(2011 年 12 月 7 日)
[97] Riigi Teataja https://www.riigiteataja.ee/akt/128122011054&leiaKehtiv
[98] エストニアの研究機関へのヒアリングによる。
[99] X-road http://e-estonia.com/component/x-road/

X-road で使用されている暗号アルゴリズムとハッシュアルゴリズムの組み合わせとしては、Diffie-Hellman 鍵交換プロトコル、RSA-2048bit 認証、3key Triple DES による暗号化通信、ハッシュ関数 SHA-1 (EDH-RSA-DES-CBC3-SHA)が使用されている。

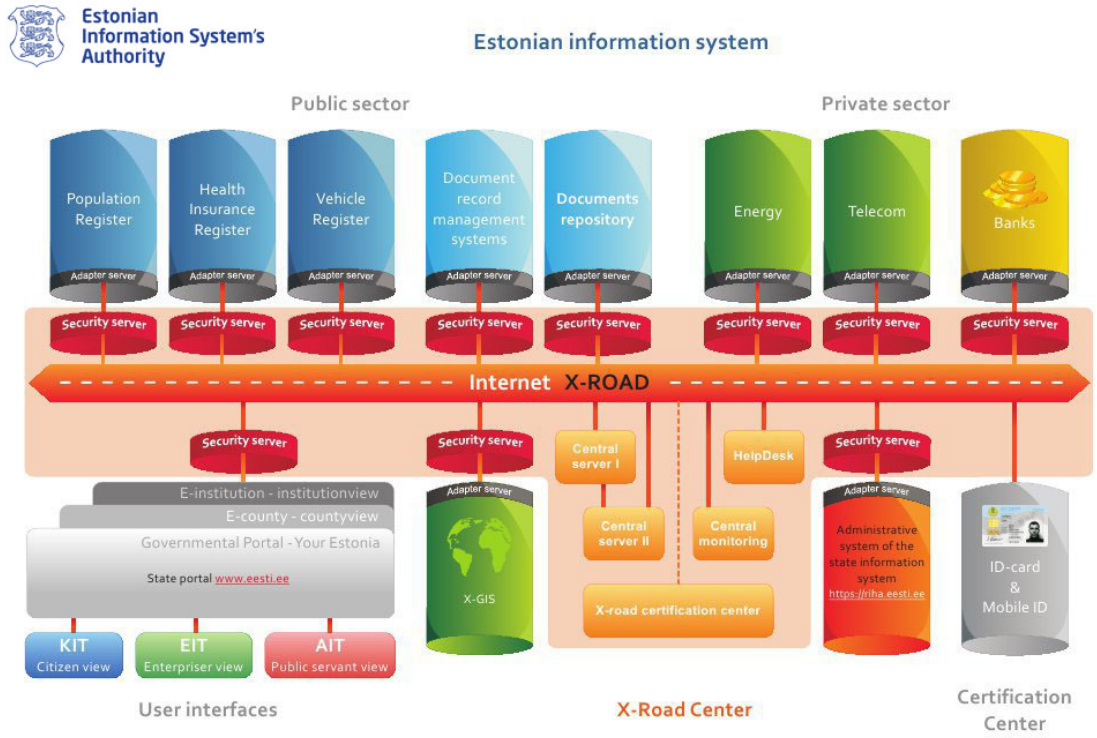


図 3-13 X-road を中心とする電子政府システムの構成図

- 国民 ID[100]
  原則、全国民に配布されている ID カードと国民 PKI システムがある。開発環境が公開されていることから銀行を始め、民間企業による ID カード利用も進んでいる。国民 ID カードはスマートカードリーダの設置が必要であったが、Mobiil-ID (Mobile-ID)と呼ばれる SIM カードに搭載した電子署名の普及が進んでいる。利用するにはエストニアのモバイル通信会社である EMT/Elion、Elisa、Tele2 の 3 社を通じて申し込み、Mobiil-ID を搭載した SIM カードを利用する端末へ挿入する。Mobiil-ID によってスマートカードリーダを使わずにスマートフォンと PIN コードだけで認証が可能となっている。

[100] https://www.ria.ee/id-card/

- 電子投票
  E-voting が 2005 年より運用されている。エストニアでは、政府は国民から信用されているため、政府による不正行為はあまり懸念されていないが、特に海外にシステムを輸出しようとすれば、投票プライバシーを保護しつつ分散システム上で集計する手法が有望と考えられており[101]、研究開発が行われている。

3.5.4.2. 人材育成

暗号分野に特化した人材育成プラグラムはないが、セイバーセキュリティ分野の人材育成プログラムがある。

- サイバーセキュリティ専攻大学院生奨学金
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)[102]
  NATO のサイバー防衛協力研究拠点。セイバーセキュリティ分野への奨学金やプログラムを提供している。
- MOE (Ministry of Education and Research：文部科学省)によるサイバーセキュリティに関する研究ファンディングも行われている[103]。

3.5.4.3. 研究開発

2007 年にエストニア政府機関に対する大規模な DDoS 攻撃[104]が発生した経験から、サイバーセキュリティ分野の研究は重視されているが、暗号分野に特化したプログラム等は無い。

- 大学
  エストニア国内における暗号分野の研究は、主にタリン工科大学(Tallinn University of Technology)[105]及びタルトゥ大学(University of Tartu)[106]で行われているが、暗号だけを専門とする研究室は設置されておらず、情報セキュリティの一分野として位置づけられている。暗号分野に限定した政府からの出資はないが、サイバーセキュリティを学ぶ両大学の学生への奨学金等がある[107]。

- 研究機関
  大学以外の研究機関でも、政府とは電子署名等に関する WG への出席、ID システムや電子政府の構築への協力等だけでなく、暗号プロトコルの開発も行っている[101]。

---

[101] エストニアの研究機関へのヒアリングによる。
[102] CCDCOE https://www.ccdcoe.org/index.html
[103] エストニアの政府機関へのヒアリングによる。
[104] The Guardian World News, http://www.theguardian.com/world/2007/may/17/topstories3.russia
[105] Tallinn University of Technology http://www.ttu.ee/en
[106] University of Tartu http://www.ut.ee/en
[107] エストニアの政府機関及び研究機関へのヒアリングによる。

3.5.4.4. サービスにおける暗号利用

主に電子政府の取り組みとして、3.5.4.1. 章にて記載している。

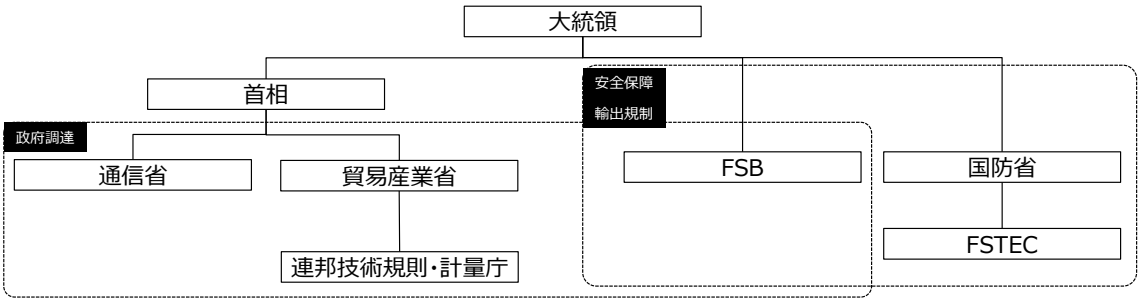
3.6. ロシア

ロシアは伝統的に厳格な暗号政策をとっている国であり、暗号の利用、開発、輸出、輸入等について法律あるいは大統領令により規制を行っている。

3.6.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

ロシアの暗号政策では、大統領直属の FSB (ロシア連邦保安庁)及び国防省の系統と、首相が所管する貿易産業省などの行政府の系統があり、主に輸出規制を含む安全保障に関する暗号施策については FSB を中心に実施されている。政府調達に関しては貿易産業省に設置されている連邦技術規制・計測庁が標準を定めている。

関連組織の全体像をまとめたものが図 3-14 である。



FSB：Federal Security Bureau (ロシア連邦保安庁) ※旧：KGB

通信省(通信・マスコミュニケーション省)：Министерство связи и массовых коммуникаций Российской Федерации

連邦技術規則・計量庁：Federal Agency on Technical Regulating and Metrology (Gosstandart)

FSTEC：Federal Service for Technical and Export Control of Russia (ロシア連邦技術・輸出管理局)

図 3-14 暗号政策に係る組織体制(ロシア)

- FSB
  防諜、犯罪対策を行う治安機関であり、暗号政策に関する広範な権限を有している。旧ソ連時代は KGB と呼称されていた組織である。また、傘下に暗号・通信･情報学研究所を設置している。
  主な権限は以下の通りである。
  - 暗号化サービスの提供、暗号化ツールの開発・製造・提供・配布に関するライセンスの発行(輸出入のライセンスも含む)
  - 暗号化ツールの認証

- 連邦技術規則・計量庁
  GOST と呼ばれる技術標準を発行するとともに認証制度を運営しており、主に輸入に関する認証に用いられる。ただし、連邦技術規制・計測庁自身は検査・認証を行わず、

民間企業(認証機関)にライセンスを与える。
暗号に関しては以下の標準を作成している。

- GOST 28147-89 (ブロック暗号)

- FSTEC
  国防省傘下に設置された、安全保障の観点から技術・サービスの輸出管理を行う組織である。単なる輸出管理にとどまらず、情報セキュリティの確保、技術情報に関する防諜、機密情報の保護、技術データの漏洩防止などを担当している。ただし、暗号技術については所掌分野から除外されている。

- 通信省
  国内の通信について所管する省である。暗号通信に関する捜査を所管する FSB、標準化や認証制度については、連邦技術規則・計量庁が所管しており、通信省と協力関係にあると考えられる。

3.6.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

ロシアの暗号政策は安全保障と治安維持にプライオリティがおかれている。これは暗号政策の主管官庁が安全保障と治安維持を所管する FSB であることから判断することができる。ロシアには暗号関係の法規制だけで数十存在するとされており、暗号規制が最も厳格に行われている国の一つである。一方で、政府機関(特に FSB)による制度の運用(定義等)があいまいで、特に外国企業からはわかりにくいとの意見も存在する。

ロシアにおける主な法制度を分類整理すると表 3-13 と 図 3-15 のようになる。

主な法制度の概要は以下の通りである。

- 149-FZ “On Information, Information Technologies, and Information Security”
  「情報」の定義と、情報のオーナーの法的能力、情報へのアクセス手段等について規定している。また、「情報システム」を定義すると共に、情報技術に関する国のポリシーガイドラインを示している。また機微情報(confidential information)についての技術的保護についても示している。

- 40-FZ “On the Federal Security Service”
  FSB の設置法であり、FSB に対して暗号分野に関する包括的な権限を付与している。FBS に付与されている暗号に関する主な権限は以下の通り。
  - 情報セキュリティ政策の立案と実装(暗号技術を含む)
  - 暗号化によるロシア連邦内の通信及びロシア連邦領域外との通信のセキュリティの確保
  - ロシア連邦から発信された暗号化された機密情報に対する諜報活動
  - ロシア連邦内の暗号化された機密情報に対するセキュリティ保護
  - 連邦政府内における暗号利用が規則通り行われているかのモニタリング
  - 暗号技術に関する開発、生産、実装、運用の規制
  - (必要に応じて)暗号装置の開発、生産、実装、運用

- 99-FZ “On Licensing Certain Activities”
  暗号利用等に関して特に重要な法律である。本連邦法では、ロシアにおいてライセンスが必要とされる活動について規定しており、以下の暗号関係についてもライセンスの対象とされている。ライセンスは FSB により発行される。
  - 符号化(暗号化)機能・手段(facilities)の流通
  - 符号化(暗号化)機能・手段の維持(maintain)
  - 情報暗号化サービスの提供
  - 符号化(暗号化)機能・手段の開発製造

表 3-13 ロシアにおける暗号関連の法律及び政策文書

分野	名称	関係組織
上位政策・戦略	149-FZ “On Information, Information Technologies, and Information Security”	FSB
暗号政策・設置法	(再掲)149-FZ “On Information, Information Technologies, and Information Security”, 2006	FSB
	40-FZ “On the Federal Security Service”, 1995	FSB
	99-FZ “On Licensing Certain Activities”, 2011	FSB
	Russian Government Resolution N 587 “On Licensing of Certain Activities Associated With Encryption (Cryptographic) Means”	FSB
	Decree No. 649, “Issues of Federal Executive Bodies Structure”, 2004	連邦技術規制・計測庁
	Decree No. 294 "On Federal Agency on Technical Regulating and Metrology",2004	
輸出入規制	164-FZ “On Fundamental Principles of State Regulation of Foreign Trade Activity”,1999 (外国貿易活動の国家規制原則)	
	183-FZ “On export control”, 1999	
	2005 年 6 月 9 日付連邦政府決定第 364 号「商品の貿易における許可制について」	
政府調達	184-FZ “On Technical Regulation”, 2002	FSB
	(再掲) 99-FZ “On Licensing Certain Activities”	
	Decree No.334 “Data Encryption”, 1995	
標準・基準	Decree No.351, 85-FZ “On Participation in international exchange of information”, 1996	FSB
	PKZ-2005 “Order on Approval of the Provision on the Development, Manufacturing, Sale, and Operation of Encryption(Cryptographic) Tools of Information Protection”	FSB, 法務省
	GOST 28147-89 (ブロック暗号)等	連邦技術規制・計測庁

Decree: 大統領令　　FZ: ロシア連邦法

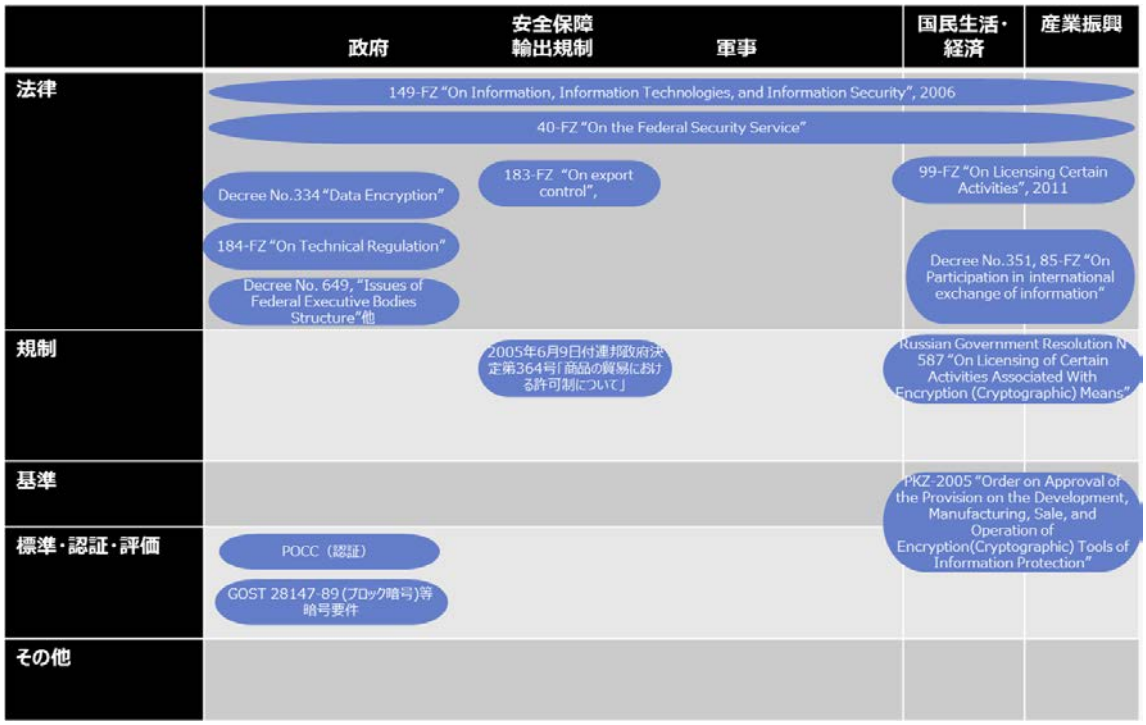


図 3-15 ロシアにおける暗号関連の政策マップ

- Russian Government Resolution N 587 "On Licensing of Certain Activities Associated With Encryption (Cryptographic) Means"
  暗号ライセンスに関する対象技術等について定義したもの。情報入手ができないため、詳細は不明

- Decree No. 649, "Issues of Federal Executive Bodies Structure"
  連邦技術規制・計測庁の設置法であり、権限を規定している。暗号についての明示的な規定はない。

- Decree No. 294 "On Federal Agency on Technical Regulating and Metrology"
  連邦技術規制・計測庁が連邦政府の国家標準化団体であることを規定している。

- 164-FZ "On Fundamental Principles of State Regulation of Foreign Trade Activity"
  外国貿易管理に関する原則を定めるとともに連邦と地方当局の権限等を定めた法律

- 183-FZ "On export control"
  ワッセナー・アレンジメントに基づく輸出規制について定めた法律

- 2005 年 6 月 9 日付連邦政府決定第 364 号「商品の貿易における許可制について」
  輸入許可に関する政府決定であり、「暗号解読に使われる機器」について輸入許可の取得を求めている

- 184-FZ “On Technical Regulation”
  ロシアにおける適合性評価について定めたもの。国家安全保障や国家機密保護に関する製品の要求仕様や性能は連邦政府機関が決定し、適合性評価を行わなければならない事が定められている

- Decree No.334 “Data Encryption”
  連邦政府機関において FSB が認可していない暗号化ソフトウェア・ハードウェアの利用は違法とされた

- Decree No.351, 85-FZ “On Participation in international exchange of information”
  国際的な情報交換における条件を定めたもの。FSB が承認した暗号ツールの利用が求められている

- PKZ-2005 “Order on Approval of the Provision on the Development, Manufacturing, Sale, and Operation of Encryption(Cryptographic) Tools of Information Protection”
  FSB による政令で、暗号化ツールの開発、製造、販売、運用等に関する詳細を定めたもの

- GOST 28147-89 (ブロック暗号)等
  連邦技術規制・計測庁が標準化している GOST 標準暗号。詳細は 3.6.3.1. 章に記載

3.6.3. 暗号に関わる各種制度及び規制

3.6.3.1. 利用すべき暗号方式

ロシアにおいて利用されている暗号方式については、連邦技術規制・計測庁が標準化している以下のものが GOST 標準暗号として知られている。

- GOST 28147-89：ブロック暗号
- GOST R 34.10-94：公開鍵暗号(署名)
- GOST R 34.10-2001：公開鍵暗号(署名)
- GOST R 34.11-94：ハッシュ関数(メッセージダイジェスト)

3.6.3.2. セキュリティ認証制度

暗号に関する認証制度には FSB による以下の二種類の制度が存在する。ただし、GOST 標準を実装した暗号システムだけが認証の対象となる。

- РОСС RU.0001.030001[108]：暗号ハードウェア(CMVP に相当)
- РОСС RU.0003.01БИ00：機密情報を処理するための情報保護ツール(CC に相当)

[108] http://www.libertarium.ru/15357

3.6.3.3. 政府の調達要件

連邦法184-FZ "On Technical Regulation"に基づき技術標準(GOST等)への適合が求められている。FSB によるライセンスを取得した組織が設計・開発した暗号化ツールを用いることとされているが詳細は不明である。それ以外にも認証取得済みの暗号化ツールの利用が求められている規則に以下のようなものがある[109]。

- Decree No. 351, FZ-85 “on participation in international exchange of information”
- Government regulation (PP-424) “on connection of the Federal state information systems to Internet”
- FSS Order No. 487 “on the Russian segment of Internet”
- Order of the Ministry of Communications No. 104 “on state-owned IS in public use”
- Government regulation (PP-330) “on specific features of assessment of compliance of protection tools for state-owned Information Systems and Personal Data Information Systems”
- Order of the Ministry of Economic Development No. 54 “on electronic sales areas”
- Government regulation (PP-781) “on protection of personal data”
- PP-608, Special requirements on technical protection of confidential information
- Decree No. 334, Gidelines of FSTEC on Key systems of information infrastructure

3.6.3.4. 暗号の輸出入規制

輸出規制に関して、ロシアもワッセナー・アレンジメントに参加しているが、より厳格な管理をしている。

基本的な輸出入規制の法体系としては、164-FZ “On Fundamental Principles of State Regulation of Foreign Trade Activity”及び183-FZ “On export control”がある。これらの法体系の下で、2005年6月9日付連邦政府決定第364号「商品の貿易における許可制について」に基づき、暗号解読に使われる機器の輸出入に際し許可の取得が必要とされている。具体的な手続きについては、2008年9月15日付連邦政府決定第691号「輸出管理対象である商品、情報、役務、サービス、知的活動の成果(権利)に関する対外貿易取引の許認可の規則の承認」が適用される。

輸入規制については、簡易的な方法(通知(notification))に基づく方法と、FSB ライセンスに基づく方法ある。簡易的な方法の対象となるのは、以下のような条件のいずれかを満たした暗号製品である。

[109] Alexey Lukatsky, CISCO, ”Regulation of Cryptography in Russia”, http://www.slideshare.net/lukatsky/crypto-regulations-in-russia

- 共通鍵アルゴリズムの場合で鍵長 56 ビット以下、公開鍵暗号アルゴリズムの場合で鍵長 512 ビット(素因数分解・離散対数)以下のもの
- 一般に提供されている OS のコンポーネントでありユーザが変更不可なもの
- 金融機関などの利用に限定されるもの
- 無線通信装置(伝達距離 400m 以下)、等

それ以外の輸入規制対象の暗号ツールは、FSB の許可を得た上で貿易産業省のライセンスが必要である。

3.6.4. その他

3.6.4.1. 研究開発・人材育成

FSB は傘下に暗号・通信・情報学研究所(ICSI : Institute of Cryptography, Telecommunications and Computer Science in the FSB Academy)を設置し、専門教育及び研究を実施している[110]。200 人以上の教員を擁している。

トレーニングコースは、暗号、情報セキュリティ、通信システムの情報セキュリティ、コンピュータセキュリティ等から構成されている。暗号に関してはモスクワ大学と連携している。また学生を対象に、「数学と暗号におけるオリンピック」を主催している。

3.6.4.2. サービスにおける暗号利用

ロシアにおける暗号利用は厳しく制限されており、クラウドサービスなどにおいて暗号技術を利用する場合、原則として FSB の許可が必要である。具体的には、99-FZ “On Licensing Certain Activities”で示されているように、以下の暗号関係の活動についてもライセンスの対象とされている。ライセンスは FSB により発行される。

- 符号化(暗号化)機能・手段(facilities)の流通
- 符号化(暗号化)機能・手段の維持(maintain)
- 情報暗号化サービスの提供
- 符号化(暗号化)機能・手段の開発製造

[110] http://www.academy.fsb.ru/index_i.html

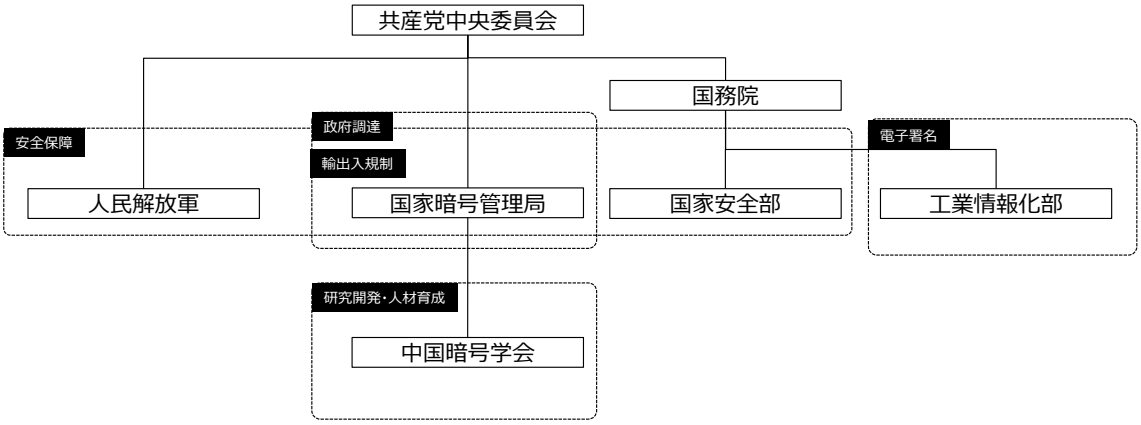
3.7. 中国

中国における暗号政策は、1999 年に公布された商用暗号管理条例(中華人民共和国国務院第 273 号令)に基づき、共産党中央委員会の下に設立された国家暗号管理局が主導しており、国家安全保障の一環として暗号政策を捉えている。

3.7.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

中国における暗号政策は、行政府である国務院ではなく、共産党中央委員会の下に設置された国家暗号管理局が主導しており、共産党主導の組織体制となっている。

関連組織の全体像をまとめたものが図 3-16 である。



国家暗号管理局：国家密码管理局もしくは中央密码工作领导小组办公室(中央暗号工作指導小組弁公室)(1 組織に二通りの名称がつけられている)
中国暗号学会：中国密码学会

図 3-16 暗号政策に係る組織体制(中国)

- 国家暗号管理局
  商用暗号管理条例(中華人民共和国国務院第 273 号令)に基づき共産党中央委員会の下に設置された商用暗号に関するポリシーの策定等を行なう組織であり、各省に支部を設置している。主な役割は、商用暗号の研究、生産、販売、使用の管理を実施し、これらの目的のための許可証を発行することである。
  一つの組織であるが、以下の二通りの呼称がある。
  - ✧ 国家密码管理局(国家暗号管理局)
  - ✧ 中央密码工作领导小组办公室(中央暗号工作指導小組弁公室)

  前者の名称が一般には用いられている。便宜上、行政府である国務院の下に位置づけられる場合もあるが、国務院の指揮下にはない。後者の名称は共産党内のものと思われる。

- 中国暗号学会
  国家暗号管理局の下に設置された暗号学会である。

- 国家安全部
  国務院に所属する諜報機関である。暗号政策に関する直接的な言及はないが、人事面で国家暗号管理局との交流があるとの情報がある[111]。

- 工業情報化部
  工業分野における情報化を推進する省であり、電子署名法等の所管において暗号政策に係わっている。

- 人民解放軍
  軍用の暗号について管理を行なっているものと思われるが詳細は不明である。

3.7.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

中国の暗号政策は安全保障と治安維持にプライオリティがおかれている。これは行政府である国務院ではなく、共産党中央委員会の下に設置された国家暗号管理局が主導していることから判断することができる。国家暗号管理局の設置及び権限を定めた商用暗号管理条例、国家暗号管理局が発行する公告、その他関連法令から構成される。

中国における主な法制度を分類整理すると表 3-14 と図 3-17 のようになる。

主な法制度の概要は以下の通りである。

- 商用暗号管理条例(中華人民共和国国務院第 273 号令)
  国家安全保障を目的とし商用暗号の管理を行なうことが宣言されている。商用暗号の定義とは、「国家機密の暗号化に用いられないもの」であり、政府における暗号のみならず、民間で用いられる暗号も対象としており広範である。
  本条例では、国家暗号管理局を設置すると共に、同局に商用暗号の研究、生産、販売、使用の管理に関する許認可権限を与えている。

- 商用暗号製品使用管理規定(国家暗号管理局公告(第 8 号))
  商用暗号の使用を規制するもの。中国公民、法人が使用できるのは国家暗号管理局が許可した商用暗号製品のみに限定される。また、商用暗号化製品の購入には ID 等の提示などが要求されている。外国企業が暗号化製品を持ち込む場合は、暗号製品輸入許可申請を行なわなければならない。

- 電子署名法
  電子署名の有効性、満たされるべき条件(電子署名作成データの適切な管理等)などが規定されている。電子署名は第三者(電子認証サービス提供者)による認証が必要である。

[111] 社団法人日本機械工業連合会、平成 19 年度「国際的制度調和に向けた安全保障貿易管理制度の比較・分析に関する調査研究報告書」

国務院信息産業主管部門が電子認証サービス提供者の認可を行なう。電子認証局は国家暗号管理局の暗号使用同意証明書類を取得しなければならない。

- 対外貿易法
  外国との輸出入に関する規制について規定したもの。「国の安全、社会公共利益または公共道徳を守る」目的で、関連貨物、技術の輸入または輸出を規制できるとされている。

表 3-14 中国における暗号関連の法律及び政策文書

分野	名称	関係組織
上位政策・戦略	商用暗号管理条例(中華人民共和国国務院第 273 号令)	国務院、国家暗号管理局
暗号政策・設置法	(再掲)商用暗号管理条例(中華人民共和国国務院第 273 号令)	国務院、国家暗号管理局
	商用暗号製品使用管理規定(国家暗号管理局公告(第 8 号))	国家暗号管理局
	電子署名法, 2004	国務院工業情報化部
輸出入規制	対外貿易法, 2004	商務部
	(再掲)商用暗号管理条例(中華人民共和国国務院第 273 号令)	国務院、国家暗号管理局
	連合公告 2009 年第 18 号	国家暗号管理局・税関総署
	(再掲)商用暗号製品使用管理規定(国家暗号管理局公告(第 8 号))	国家暗号管理局
	国外組織及び個人の中国での暗号製品使用に関する管理弁法(国家暗号管理局公告(第 9 号))	国家暗号管理局
政府調達	政府調達法, 2002	財政部
	情報セキュリティ製品強制性認証実施要求の調整に関する公告、2009	国家品質検査検疫総局・国家認証認可監督管理委員会
標準・基準	商用暗号科学研究管理規定(国家暗号管理局公告(第 4 号))	国家暗号管理局
	商用暗号製品生産管理規定(国家暗号管理局公告(第 5 号))	国家暗号管理局
	商用暗号製品販売管理規定(国家暗号管理局公告(第 6 号))	国家暗号管理局
	電子認証サービスにおける暗号管理方法(国家暗号管理局公告(第 17 号))	国家暗号管理局
	(再掲)電子署名法, 2004	国務院工業情報化部
	SM2 電子署名用楕円曲線公開鍵暗号アルゴリズム(国家暗号管理局公告（第 21 号))	国家暗号管理局
	SM3 ハッシュアルゴリズム(国家暗号管理局公告(第 22 号))	国家暗号管理局

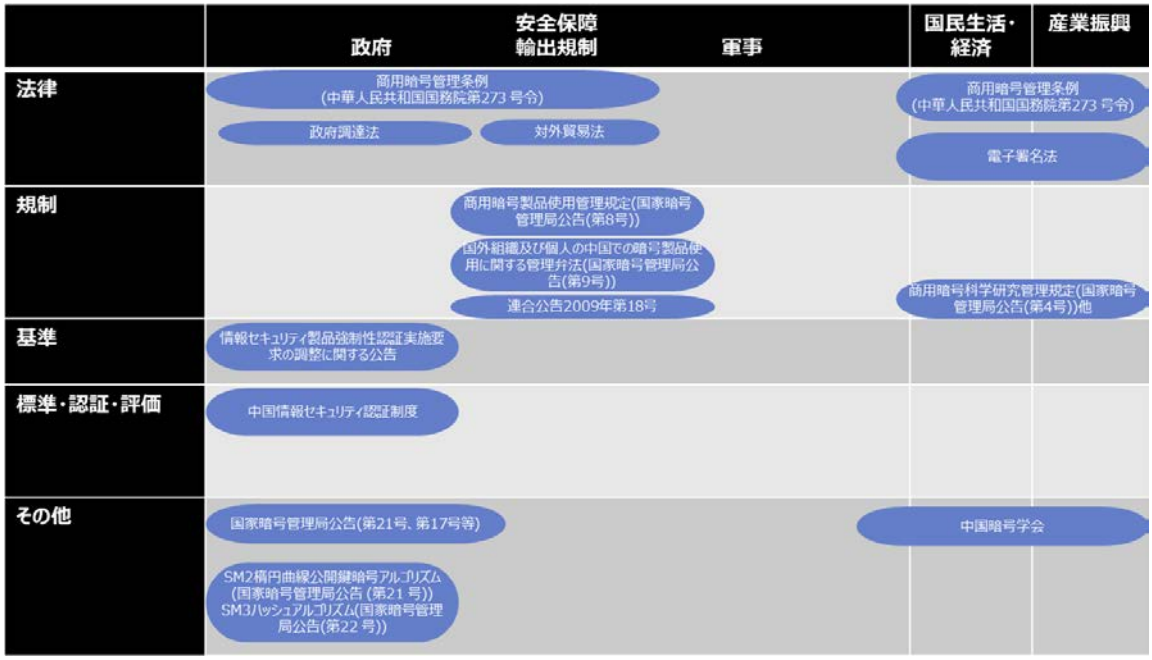


図 3-17 中国における暗号関連政策マップ

- 連合公告 2009 年第 18 号
  輸入商品に暗号技術が含まれる場合、「暗号製品と暗号技術を含む設備の輸入管理目録」に含まれていないコンピュータ、ソフトウェアであっても、輸入時に税関に対し自主的に暗号輸入許可証を提出する必要がある。

- 国外組織及び個人の中国での暗号製品使用に関する管理弁法(国家暗号管理局公告(第 9 号))
  国外組織及び個人による中国国内における暗号利用について規定したもの。国外組織等が暗号製品を中国に輸入しようとした場合、「暗号製品輸入許可証」の申請が必要である。

- 政府調達法
  政府調達の適用範囲、調達方式、調達手続きについて定めたもの。国産品の優遇について明記されている。また、暗号に関する強制認証制度の適用対象は政府調達法の範囲とされている。これについては 3.7.3.2. 章で詳しく述べる。

- 情報セキュリティ製品強制性認証実施要求の調整に関する公告
  強制認証制度(CCC)の一部として実施される中国情報セキュリティ認証制度の対象を当面政府調達に限るとした公告。

- 商用暗号科学研究管理規定(国家暗号管理局公告(第 4 号))
  商用暗号研究開発を規制するもの。商用の暗号研究を行なおうとするものは、事前に国家暗号管理局に申請を行ない許可を得る必要がある。

- 商用暗号製品生産管理規定(国家暗号管理局公告(第 5 号))
  商用暗号を製造を規制するもの。商用暗号の製造を行なおうとするものは、事前に国家暗号管理局に申請を行ない許可を得る必要がある。

- 商用暗号製品販売管理規定(国家暗号管理局公告(第 6 号))
  商用暗号の販売を規制するもの。商用暗号の販売を行なおうとするものは、事前に国家暗号管理局に申請を行ない許可を得る必要がある。

- 電子認証サービスにおける暗号管理方法(国家暗号管理局公告(第 17 号))
  電子認証サービスを行なおうとする者に対する要件を定めたもの。技術基準は本公告とは別に定められている。国家暗号管理局公告(第 2 号)を置き換えたもの。

- SM2 電子署名用楕円曲線公開鍵暗号アルゴリズム(国家暗号管理局公告（第 21 号))
  電子署名用の楕円曲線公開鍵暗号アルゴリズム SM2 について規定したもの。

- SM3 ハッシュアルゴリズム(国家暗号管理局公告(第 22 号))
  ハッシュアルゴリズムについて規定したもの。

3.7.3. 暗号に関わる各種制度及び規制

3.7.3.1. 利用すべき暗号方式

以下の暗号アルゴリズムが国家暗号管理局より定められている。

- 国家暗号管理局公告第 21 号:SM2 電子署名用楕円曲線公開鍵暗号アルゴリズム。鍵長は 256 ビット。
- 国家暗号管理局公告第 22 号：SM3 ハッシュアルゴリズム

また、国家暗号管理局により公告に関連して中国の標準として制定されている。

- GM/T 0001-2012：ストリーム暗号アルゴリズム
- GM/T 0002-2012：SM4 ブロック暗号
- GM/T 0003-2012：SM2 電子署名用楕円曲線公開鍵暗号アルゴリズム
- GM/T 0004-2012：SM3 ハッシュアルゴリズム

なお、商用暗号管理条例では「国家機密とされる商用暗号技術(第二条)」との記載もあるため、2012 年に公開された上記の「国家暗号管理局が定めた暗号方式(第三条)」とは異なる商用暗号技術が存在している可能性は否定できない。

3.7.3.2. セキュリティ認証制度

中国情報セキュリティ認証制度(CC-IS; China Certification of Information Security)は、中国政府の中国情報セキュリティ認証センター(ISCCC：China Information Security

Certification Center)が実施しているITセキュリティ認証制度であり、強制認証制度(CCC)の一部として実施されている。政府調達法に基づき、情報セキュリティ製品について認証の取得を義務づける制度である。

ISO/IEC 15408に対応した中国標準GB/T18336-2008に基づき、CCに類する認証スキームとして運用されている。評価基準的にはCCとほぼ差は無いが、評価方法については工場査察が入るなど、一部独自な部分も存在している。対象となる13品目のうち、6品目が暗号認証の対象となり、それについては国家暗号管理局がテストを行なう[112]。

2008年1月28日に国家品質監督検査検疫総局および国家認証認可監督管理委員会は「一部の情報セキュリティ製品に対して強制認証を実施することに関する公告」を公布し、翌2009年5月1日から、13品目の情報セキュリティ製品をCCC認証の対象とすることを発表した。これにより、当該情報セキュリティ製品はCCCを取得しなければ中国への輸入ができなくなるが、CCC の取得に際して技術情報(ソースコードを含む)の開示が必要となる可能性があったことから、日米欧などは強く反対した。

2009年4月29日に国家品質検査総局、財政部、国家認証認可監督委員会は「情報セキュリティ製品強制認証実施要求の調整に関する公告」及び「情報セキュリティ強制認証実施細則」(上述13品目の分野)を公布し、実施時期を延期すると共に、認証範囲を政府調達に限定する妥協を行なった。さらに、2010年7月14日には、国家認証認可監督管理委員会より「情報セキュリティ製品認証制度実施要求に関する公告」が公布され、情報セキュリティ製品の「CCC認証制度」は「国家情報セキュリティ製品認証制度」と名称が変更された。

3.7.3.3. 政府の調達要件

政府調達法に基づき、中国情報セキュリティ認証制度で認定された情報セキュリティ製品の調達が義務付けられている。また、暗号に関しては商用暗号管理条例等を根拠として国家暗号管理局が許可した暗号のみが利用可能である。

3.7.3.4. 暗号の輸出入規制

商用暗号製品使用管理規定(国家暗号管理局公告(第8号))、国外組織及び個人の中国での暗号製品使用に関する管理弁法(国家暗号管理局公告(第9号))及び国家暗号管理局・税関総署の連合公告2009年により暗号の輸入規制が行なわれている。暗号製品の輸入には国家暗号管理局が発行する暗号輸入許可証の取得が必要である。

また、輸出に関しては商用暗号製品販売管理規定(国家暗号管理局公告(第6号))により国家暗号管理局の許可が必要とされる。

なお、中国はワッセナー・アレンジメントに参加していない。

[112] http://www.ccilc.pt/sites/default/files/docs/CC-IS_CHINA_CERTIFICATION_OF_INFORMATION_SECURITY_%5BEN%5D_%5BEUSMECENTER%5D.pdf

3.7.4. その他

3.7.4.1. 研究開発

国家暗号管理局の下に中国暗号学会が設立されており、国が暗号研究をコントロールしている。

また、国家暗号管理局公告(第 4 号)によれば、商用暗号研究開発は政府により規制されている(学術・理論研究は規制対象外と見られる)。具体的には暗号研究ユニットの国家暗号管理局に対する事前申請を求めており、申請内容により国家暗号管理局が研究ユニットの指定を行い証明書を発行する。また研究ユニットとして指定された後に、研究開発プロジェクトについて、研究の概要、研究プロセスとスケジュール、安全性分析レポートを提出しなければならない。また、プログラムのソースコードやアルゴリズムの説明の提出も求められる。

3.7.4.2. サービスにおける暗号利用

商用暗号管理条例(中華人民共和国国務院第 273 号令)により、いかなる企業も個人も国家暗号管理局が認可した商用暗号製品のみを使用することができ、自ら開発製造した暗号製品や海外で生産された暗号製品を使用してはならないとされている。同種の規定として、商用暗号製品使用管理規定(国家暗号管理局公告(第 8 号))等により、中国国内で利用可能な暗号の規制が行なわれている。これらの規定により、サービスにおける暗号利用に際しても、中国公民、法人が使用できるのは国家暗号管理局が許可した商用暗号製品のみに限定される。

また、商用暗号科学研究管理規定(国家暗号管理局公告(第 4 号))、商用暗号製品生産管理規定(国家暗号管理局公告(第 5 号))に基づき、暗号製品の研究開発・生産についても国家暗号管理局の許可が必要である。

なお、2000 年 3 月に当時の国家暗号管理委員会弁公室が発行した「商用暗号管理に関する問題についての通知」によれば、『商用暗号管理条例の範疇に帰属する「暗号製品及び暗号技術を含む設備」とは、暗号化と復号化をその中核機能とする専用のハードとソフトの範囲に限定し、その他、例えば無線携帯電話、Windows ソフト、ブラウザソフト等は全てこの範疇から除外する。』とされており[113]、OS 等の機能として含まれる暗号機能の利用は除外されているとの解釈もあるが、明確な線引きについては不明点が多い。

[113] JETRO、“中国の商用暗号管理制度”、 2008 年 3 月、
http://www.jetro-pkip.org/upload_file/2008053080829801.pdf

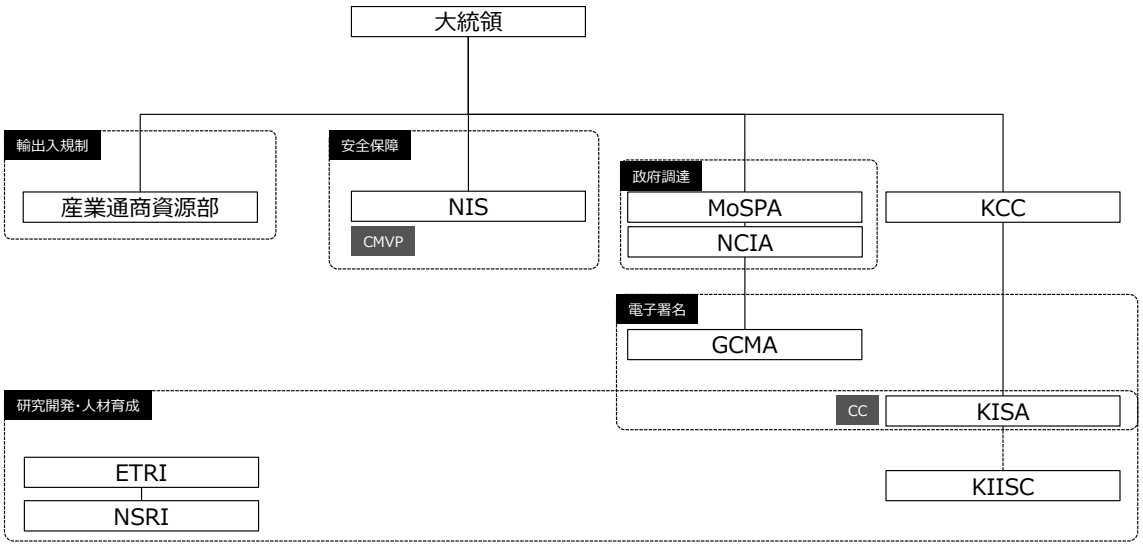
3.8. 韓国

韓国における暗号を含む情報セキュリティ政策の特徴は、主に政府機関を対象とした政策・組織と民間向けの政策・組織に分かれており、他国に比較して民間向けの政策・組織に力を注いでいる点である。一方で、組織改変が極めて頻繁に行なわれることは、政策の継続性という観点からは不利と思われる。

3.8.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

韓国における暗号政策の中心となるのは、大統領直属の情報機関である国家情報院(NIS)と、放送通信委員会の下に設置された韓国インターネット・安全振興院(KISA)が中心的な役割を果たしている。

関連組織の全体像をまとめたものが図 3-18 である。



NIS：National Intelligence Service (国家情報院)

MoSPA：Ministry of Security and Public Administration (安全行政部 (旧)行政安全部)

産業通商資源部：(旧)知識経済部

KCC：Korea Communications Commission(放送通信委員会)

KISA：Korea Internet & Security Agency (韓国インターネット振興院)

KIISC：Korea Institute of Information Security and Cryptology (韓国情報セキュリティ・暗号研究所)

ETRI：Electronics and Telecommunications Research Institute(電子通信研究院)

GCMA：Government Certificate Management Authority (政府認証局)

NCIA：National Computing and Information Agency (政府統合電算センター)

NSRI：国家保安技術研究所 (現在存続しているか否か不明)

図 3-18 暗号政策に係る組織体制(韓国)

- NIS

  大統領直属で設置された情報機関であり、以前は韓国中央情報部(Korean Central Intelligence Agency: KCIA)と呼称されていた。NIS における暗号関係の業務は以下のようなものがある。また、NIS の下に重要事項を審議する国家サイバー安全戦略会議(議長：国家情報院長、委員：関連省庁の次官)を置くと共に、サイバー安全センターが設置されている。

  - 情報セキュリティ製品の評価(いわゆる CC)
    - NIS の下に設置されている IT Security Certification Center (ITSCC)が Korea Evaluation and Certification Scheme (KECS)の認証機関となっている。
  - 暗号モジュール実装評価(いわゆる韓国版 CMVP)

- KISA

  1996 年に「情報化促進基本法」に基づき韓国情報保護センターとして設置され、2001 年の「情報通信網利用促進及び情報保護等に関する法律」により韓国情報保護振興院となり、2009 年に KISA(韓国情報保護振興院)、NIDA(韓国インターネット振興院)、KIICA(情報通信国際協力振興院)が合併し、放送通信委員会の下に新生 KISA(韓国インターネット振興院)として設置された。KISA の役割は極めて多岐に渡るが、暗号関係の業務としては以下のようなものがある。

  - 情報セキュリティ製品の評価(いわゆる CC)
    - KECS における評価機関
    - 認証評価関連規程の策定及び施行
    - 情報セキュリティ製品の評価
    - 評価技術及び方法論の開発
    - 共通評価基準解説書とガイドラインの開発
    - 国際相互承認協定(CCRA)に関する研究や活動
  - 暗号技術の開発及び利用基盤拡大
    - 韓国版 CMVP における評価機関
    - 暗号利用拡大のための技術/政策開発
    - 国産暗号技術(SEED、HIGHT、ARIA)基盤の拡大
    - 情報保管のセキュリティ強化方策
    - 暗号安全性検証ツールの開発と普及
    - 暗号ガイドラインの作成と普及
  - 電子署名認証管理
    - Root CA の運用管理
    - 電子署名認証技術の開発

- MoSPA

  行政の電子化を所管する

- 産業通商資源部

  対外貿易法、対外貿易法施行令、戦略物資輸出入告示などに基づき暗号の輸出規制に

ついて所管している。

3.8.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

韓国の暗号政策は安全保障にプライオリティが置かれている。これは大統領直属の情報機関である NIS が暗号政策の中核であることからうかがうことができる。韓国における暗号関連の法制度は多岐に渡る。表 3-15 と図 3-19 に韓国における主な暗号関連の法律及び政策文書を示す。

- 国家サイバー安全管理規定(大統領訓令第 316 号)
  サイバーセキュリティに関する最上位の規定であり、各省庁の役割を規定したもの。2004 年に制定(大統領訓令第 141 号)されたものの改定。各省庁と協議のうえ、NIS が国家サイバーセキュリティに関する政策を統括する。この目的のため、NIS の下に重要事項を審議する国家サイバー安全戦略会議(議長：国家情報院長、委員：関連省庁の次官)を置くと共に、サイバー安全センターを置き、国家サイバー安全政策の立案、国家サイバー安全マニュアルの作成、サイバー脅威に関する情報収集・分析・伝達、情報通信網の安全性確認、サイバー攻撃事案の調査・復旧等を行なう。また各省庁は所管の情報通信網を保護する責任をもつ。

- 情報通信網利用促進及び情報保護等に関する法律
  2001 年に改定された本法律では、韓国情報保護センター(=KISA)を設置すると共に、その事業として「情報保護のための暗号技術の開発」を行なうことを規定している。情報保護システムの研究・開発及び試験・評価、情報保護システムの性能と信頼度に関する基準策定及び標準化支援を行なうもとのされている。

- 国家情報化基本法
  1995 年に制定された本基本法には、1999 年の改正で情報保護に関して、「政府は情報の安全な流通のため情報保護に必要な施策を講じなければならない。」とした上で「政府は暗号技術の開発と利用を促進し、暗号技術を利用し情報通信サービスの安全を図る措置を講じなければならない。」とする条項が含まれている。

- 電子取引基本法
  電子商取引事業者による暗号の使用、国家安全保障のための暗号製品の使用制限、暗号解読等について定めている。具体的には、電子取引当事者は電子取引の安全性・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一方で、政府は国家安全保障のために必要な場合、暗号製品の使用制限、平文へのアクセス、暗号技術へのアクセス等を行うことができる。

表 3-15 韓国における暗号関連の法律及び政策文書

分野	名称	関係組織
上位政策・戦略	国家サイバー安全管理規定(大統領訓令第 316 号), 2010	
暗号政策・設置法	情報通信網利用促進及び情報保護等に関する法律, 2001	KISA
	国家情報化基本法, 2000	KISA
	電子取引基本法, 1999	
	個人情報保護法, 2011 (個人情報保護法施行令・個人情報保護ガイドライン)	安全行政部
	電子署名法, 1999	安全行政部、KISA、GCMA
	国家情報院法, 1999	NIS
暗号利用	保安業務規定	NIS
輸出入規制	対外貿易法, 1989 (対外貿易法施行令、戦略物資輸出入告示)	産業通商資源部
政府調達	電子政府法, 2007	安全行政部
	電子政府法施行令及び電子文書保安措置施行指針	NIS
標準・基準	Guideline on utilization of cryptographic algorithm and key length	KISA、KCC
	Guideline on implementation of cryptographic algorithms for protecting personal Information	KISA、KCC

図 3-19 韓国における暗号関連政策マップ

- 個人情報保護法(個人情報保護ガイドライン)
  個人情報保護ガイドラインの中で、安全管理措置の一環として「暗号アルゴリズムなどを利用して、ネットワークに個人情報を安全に電送できる保安装置」の利用が求められている。個人情報保護法施行令では、固有識別情報の安全性確保措置についても暗号利用が求められるとともに、電子媒体に保存している個人情報の暗号化が要求されている。これについて、KISA では Guideline on implementation of cryptographic algorithms for protecting personal Information を作成し公開している。

- 電子署名法
  電子署名の効力、公認認証機関等について定めている。

- 国家情報院法
  NIS の権限として、刑法のうち、内乱罪、外患罪、軍刑法のうち反乱罪、暗号不正使用罪、軍事機密保護法に規定された罪、国家保安法に規定された罪に対する捜査を行える旨を規定。

- 保安業務規定
  暗号資材の定義、必要な機関に対する NIS からの暗号資材の提供等が定められている。

- 対外貿易法／対外貿易法施行令／戦略物資輸出入告示
  ワッセナー・アレンジメントに基づく暗号製品の輸出規制。

- 電子政府法
  電子政府実現促進のための法律。政府等における情報通信網の安全性及び信頼性確保のための保安対策を用意するように求めている。

- 電子政府法施行令及び電子文書保安措置施行指針
  行政機関は電子文書の保管や流通に当たって保安措置を講ずることを義務付けるとともに、これらの保安機能や適合性についての規格を定める権限を NIS に与えている。

- Guideline on utilization of cryptographic algorithm and key length
  KISA が 2010 年に公開した暗号アルゴリズムと鍵長に関する推奨事項を示したガイドライン。2013 年に改訂された[114]。

- Guideline on implementation of cryptographic algorithms for protecting personal Information
  KISA/KCC が公開した個人情報保護における暗号アルゴリズムの実装に関するガイド

[114] KISA,
http://seed.kisa.or.kr/iwt/ko/guide/EgovGuideDetail.do?bbsId=BBSMSTR_000000000011&nttId=31&pageIndex=1&searchCnd=&searchWrd=

ライン(韓国語)[115]。

3.8.3. 暗号に関わる各種制度及び規制

3.8.3.1. 利用すべき暗号方式

韓国では電子政府法施行令及び電子文書保安措置施行指針等を根拠とし、対国民行政業務用で利用可能な暗号アルゴリズムのリストを作成するため、NIS の下に暗号検証委員会が設置されている[116]。対国民行政業務用システムの場合、韓国版 CMVP 認証を取得しなければならないが、韓国版 CMVP での利用が認められている暗号アルゴリズムは表 3-16 の通りである[117]。

また、国家サイバー安全管理規定に基づき NIS が策定している国家サイバー安全マニュアルにも政府機関が使用すべき暗号機器等に関する記載があるが、詳細は非公開である。

表 3-16 韓国版 CMVP 認可暗号アルゴリズム

区分	アルゴリズム
ブロック暗号	ARIA, SEED
ハッシュ関数	SHA-224, SHA-256, SHA-384, SHA-512
公開鍵アルゴリズム	RSAES-OAEP
電子署名	RSASSA-PSS, ECDSA, KCDSA, EC-KCDSA
鍵交換	DH, ECDH

この他にも、パスワードや DBMS などを利用する際の一般的な暗号アルゴリズムと鍵長の選定に関するクライテリア・事例紹介など目的としたガイドラインも KISA が作成している[118]。

3.8.3.2. セキュリティ認証制度

韓国における認証制度は、国家情報化基本法第 38 条(情報保護システムに関する基準告示等)、国家情報化基本法施行令第 35 条(情報保護システムの補完など)、情報通信網利用促進等に関する法律第 52 条(韓国インターネット振興院)、情報システム評価認証指針、国家情報通信保安基本指針、電子文書保安措置施行指針を根拠としている。

---

[115] KISA, “개인정보 암호화 조치 안내서”, http://m.privacy.go.kr/cmm/fms/FileDown.do;jsessionid=580D828E3856A8A86A1B0FA60C31D8D6?atchFileId=FILE_000000000453933&fileSn=1

[116] IPA, “国家と暗号の関わり方に関する海外調査報告書”, http://www.ipa.go.jp/files/000013768.pdf

[117] Yongdae Kim, “The current Status of CMVP in Korea”, http://icmc-2013.org/wp/wp-content/uploads/2013/10/YongdaeKim.pdf

[118] https://www.kisa.or.kr/notice/press_View.jsp?cPage=21&mode=view&p_No=8&b_No=8&d_No=1164&ST=T&SV=

暗号関係の認証制度としては、以下の二種類が存在する。

- 情報セキュリティ製品の評価(いわゆる CC(KECS))
  - NIS の下に設置されている IT Security Certification Center (ITSCC)が Korea Evaluation and Certification Scheme (KECS)の認証機関となっている。
  - 評価機関は KISA である。
- 暗号モジュール実装評価(いわゆる韓国版 CMVP)
  - NIS が認証機関である。
  - 評価機関は NSRI (National Security Research Institute)及び KISA である。NSRI は公的機関向け、KISA は民間向けの評価機関である。

3.8.3.3. 政府の調達要件

政府調達において、暗号関係の調達要件を定める根拠は、電子政府法施行令及びその下位文書である電子文書保安措置施行指針におかれている。同指針では、行政機関は電子文書の保管や流通に当たって保安措置を講ずることを義務付けるとともに、これらの保安機能や適合性についての規格を定める権限を NIS に与えている。国家サイバー安全管理規定に基づき NIS が策定している国家サイバー安全マニュアルにも政府機関が使用すべき暗号機器等に関する記載があるが、詳細は非公開である。

民間企業の製品を電子政府に採用するためには、NIS の KECS の認証取得が必要である。さらに、暗号モジュールが搭載されている場合で政府内部の用途の場合は NIS が認証した国家機関用暗号モジュール(認可暗号アルゴリズムは非公開)を採用しなければならない。

電子政府の対国民行政業務用システムの場合、韓国版 CMVP 認証を取得した製品を採用しなければならない[119]。

3.8.3.4. 暗号の輸出入規制

暗号の輸出規制については、対外貿易法、対外貿易法施行令、戦略物資輸出入告示などに基づき産業通商資源部が所管している。韓国はワッセナー・アレンジメントに参加していることから、暗号製品についても一定の輸出制限が課せられているものと思われる。

暗号に関する輸入規制については特に存在しない。

3.8.4. その他

3.8.4.1. 国産暗号普及施策

国産暗号の普及施策として、KISA はスマートフォン用暗号ライブラリを開発し、ホームページ上で配布している[120]。これは、スマートフォンアプリ開発時に国産暗号アルゴリズ

[119] IPA, “国家と暗号の関わり方に関する海外調査報告書”, http://www.ipa.go.jp/files/000013768.pdf
[120] http://seed.kisa.or.kr/iwt/ko/sup/EgovMobileLb.do

ムを簡単に組み込めるように提供しているものである。
提供されている形態は以下のとおりである。

- 対象 OS：Android, iOS, Windows Mobile
- ブロック暗号：SEED, HIGHT
- ハッシュ関数：HAS-160
- 電子署名：KCDSA

3.8.4.2. 人材育成

- 韓国情報セキュリティ暗号学会(KIISC：Korea Institute of Information Security & Cryptology)
  1990 年に、情報セキュリティと暗号の研究開発を促進するために KISA が支援して設立された組織である。国際会議・セミナーの開催、出版、標準化のための研究、普及啓発等を行なっている。

3.8.4.3. 研究開発

韓国では、情報セキュリティや暗号の研究を KISA をはじめ、NSRI (National Security Research Institute)、ETRI (Electronics and Telecommunications Research Institute)などで国として実施している。

3.8.4.4. サービスにおける暗号利用

民間におけるサービスを対象とした包括的な規制は存在しないが、サービスの中で個人情報を扱う場合、個人情報保護法等で求められている電子媒体に保存している個人情報の暗号化が必要となる。

また、現在韓国国会で審議中のクラウドコンピューティングの発展及び利用者保護に関する法律案が可決された場合、放送通信委員会が定めるサービス安全指針への準拠が求められる。サービス安全指針の内容は確定していないが、サービス提供・利用に関する情報保護基準が示される予定である。

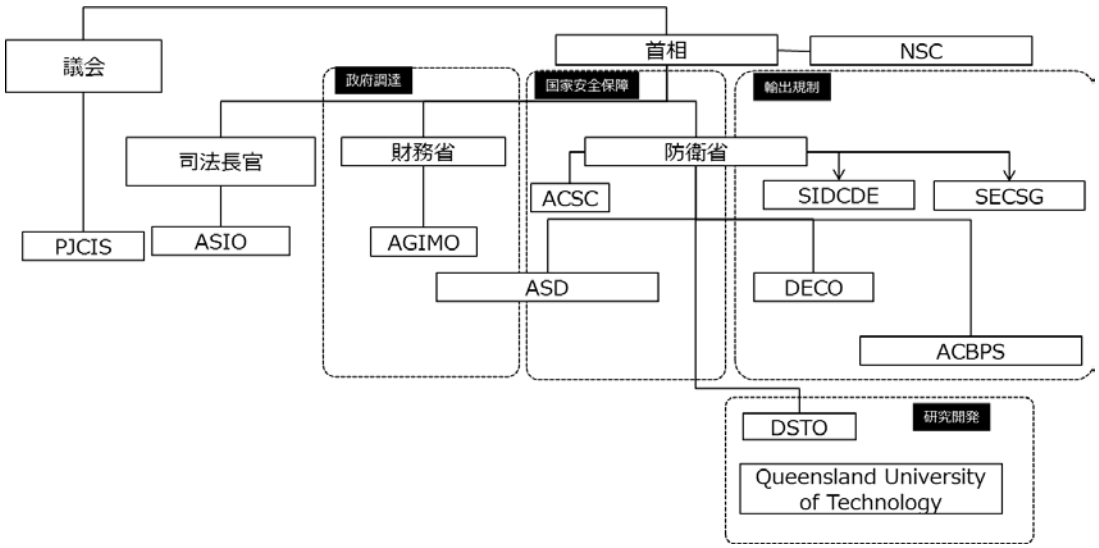
3.9. オーストラリア

オーストラリアにおいては、国防省傘下の ASD が、暗号政策の主導的な役割を担っている。ASD は、暗号の要件を含む政府システム要件の Information Security Manual (ISM)、製品認証制度 AISEP (Australasian Information Security Evaluation Program)、政府セキュリティフレームワーク Protective Security Policy Framework (PSPF)を所管すると共に、輸出規制を所管する DECO、政府調達を所管する AGIMO などに対して技術的な助言を行っている。

3.9.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

オーストラリアの暗号政策に係る組織は、諜報活動を含む安全保障を担当する防衛省内の ASD、輸出規制を所管する DECO、政府調達を所管する AGIMO が中心となる。暗号政策については、ASD がオーストラリアの主導的な役割を果たしている。

組織体制の全体像を示したものが図 3-20 である。



NSC：National Security Committee of Cabinet (内閣国家安全保障委員会)

ASD：Australian Signals Directorate (旧：defense Signals Directorate (DSD)) (オーストラリア信号局)

DECO：Defense Export Control Office (防衛輸出規制室)

ACBPS：Australian Customs and Border Protection Service (オーストラリア関税国境防衛サービス)

SIDCDE：Standing Interdepartmental Committee on Defense Exports (防衛輸出省庁横断常設委員会)

SECSG：Strengthened Export Controls Steering Group (強化輸出規制推進グループ)

AGIMO：Australian Government Information Management Office (オーストラリア政府情報管理室)

ASIO：Australia's national security intelligence service (オーストラリア国家安全諜報サービス)

PJCIS: Parliamentary Joint Committee on Intelligence and Security (国会諜報ｾｷｭﾘﾃｨ統合委員会)

ACSC ：Australian Cyber Security Centre (オーストラリア・サイバーセキュリティセンター)

DSTO：Defense Science and Technology Organization (防衛科学技術局)

図 3-20 暗号政策に関する組織体制(オーストラリア)

主な組織の役割及び関係は以下の通りである。

- ASD[121]
  オーストラリア防衛省の信号諜報機関であり、オーストラリアの国家安全保障を保つために必要とされる諜報活動、セキュリティ対策を進めることをミッションに掲げている。外国の信号情報の収集と分析を行い、連邦政府と州政府に対して情報通信セキュリティに関する助言と支援を行うことを役割としている。また、情報保証やその取組みの一つである ASD Cryptographic Evaluation などの製品認証に関する取組みにも重点を置いている。暗号製品の開発と配備のため企業と緊密に協力する。
  第 2 次世界大戦において日本の無線通信の傍受と解読を起源とする組織であり、2013 年に前身の Defence Signals Directorate (DSD)から改称された。

- NSC
  国家安全保障、国境防御、事案対処に関する基本戦略を審議、決定する。決定事項は、内閣の承認を得る必要はない。暗号政策に関しても、国家安全保障に係わる場合には審議事項となり、その決定事項は ASD の政策に影響を与える。

- ASIO[122]
  司法長官に対して責任を持つセキュリティ長官の指揮の下で運営される諜報機関である。セキュリティの脅威を特定し調査することを役割とし、オーストラリア政府や国民に対して助言を与える。ASD は信号諜報を役割とし、ASIO は信号以外を中心にセキュリティに係わる諜報全般を対象とする。

- DECO[123]
  防衛・戦略物資、技術の輸出規制を所管する防衛省の組織であり、輸出企業に対するライセンシングを担当している。規制の対象とするものは、軍事目的で設計・適合された物資、破壊性のあるもの、または商用品で軍事プログラムなどにも利用されるものである。暗号に関しては、Customs Act 1901 を修正する Defence and Strategic Goods List Amendment 2011 により規制されている。

- SECSG
  2015 年 5 月までの期限付きで、輸出規制に関して防衛省に対する助言を行うために設置されたステアリンググループで、防衛省が、産業界、研究機関、政府機関から代表者を任命して構成する。DECO は行政執行を所管し、SECSG は政策決定の助言を行う立場にある。

- SIDCDE
  防衛大臣に対して機微な輸出申請や輸出方針に関する助言を行う省庁横断型の委員会

[121] http://www.asd.gov.au/about/index.htm
[122] http://www.asio.gov.au/About-ASIO/Overview.html
[123] http://www.defence.gov.au/DECO/AboutUs.asp

である。

- AGIMO[124]
  ICT 全体の政策を担当しており、行政における情報通信技術の応用に関して政府機関を先導する役割を担う。財務省内の組織である。

- PJCIS[125]
  国会の委員会として、ASD などの政府諜報機関の活動に関する調査および支出の監視する。Intelligence Services Act 2001 にその役割が規定されている。

- ACSC[126]
  オーストラリアのネットワークが世界最高レベルのセキュリティを確保するためのイニシアチブである。防衛省、法務省、ASIO、連邦警察、オーストラリア犯罪委員会の政府のすべてのサイバーセキュリティ機能を集約する[127]ことを目的とする。サイバーセキュリティに関して政府、民間企業全体にわたる協力を推進している。

- DSTO
  国防に関する科学技術の応用を所管する機関で、大学等と連携し、情報セキュリティ技術の開発等を担っている。

- ACBPS
  オーストラリアの税関に関するセキュリティと完全性を確保するための組織である。

3.9.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

オーストラリアは、米、英、カナダ、ニュージーランドと共に、セキュリティ諜報活動 PRISM 等の連携関係にあり、信号諜報の中核となる暗号政策は、国家安全保障に関するプライオリティが高く、並行して政府調達にも重点を置いている。主な法制度を整理したものが表 3-17 と図 3-21 である。

- Cyber Security Strategy, 2009
  本戦略は、政府、企業、個人のセキュリティを守るために、リソースを如何に活用するか示す。Research Support for National Security Program などの研究開発プログラムにおいて、量子暗号に取り組むことを取り上げている。ASD の前身である DSD が、政府に対して暗号と通信の技術面の支援を行うことを挙げている。

[124] http://www.finance.gov.au/agimo/
[125] http://www.aph.gov.au/pjcis
[126] http://www.asd.gov.au/infosec/acsc.htm
[127] センターの運用開始は 2014 年後期を予定しており、集約の場所は、キャンベラの Ben Chifley Building が予定されている。

表 3-17 法制度の分類と一覧(オーストラリア)

分野	名称	関係組織
上位政策・戦略	Cyber Security Strategy, 2009	ASD
暗号政策・設置法	Intelligence Services Act 2001	ASD (旧 DSD)
輸出入規制	Customs Act 1901 (根拠法)	防衛省、ACBPS
	Defense Trade Controls Act 2012 (米豪軍事協力)	防衛省
	Customs (Prohibited Exports) Regulations 1958, 13E	防衛省
	defense and Strategic Goods List Amendment 2011	DECO
	Australian Export Controls for defense and Dual-Use Goods	防衛省
政府調達	Crimes Act 1914, Criminal Code 1995	Attorney-General (司法省)
	Directive on the security of Government business	Attorney-General (司法省)
	Protective Security Policy Framework (PSPF)	Attorney-General (司法省)
標準・基準	AISEP Policy Manual	ASD (旧 DSD)
	ASD Cryptographic Evaluation (ACE)(旧 DCE から改称))	ASD
	Information Security Manual	ASD (旧 DSD)
	Cybercrime Act 2001 / Crimes Act 1914	法執行機関

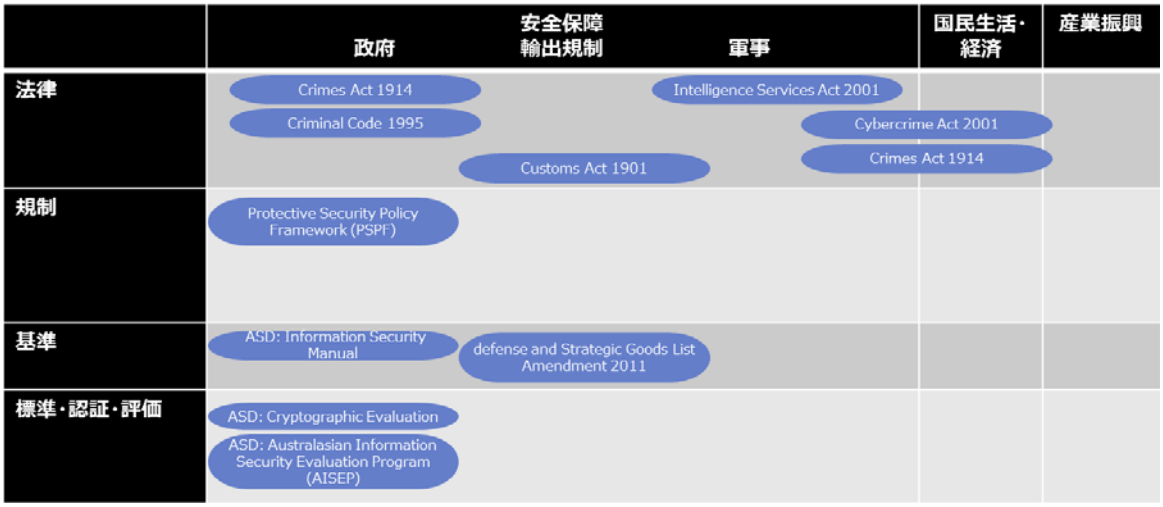


図 3-21 オーストラリアにおける暗号関連政策マップ

- Intelligence Services Act 2001
  ASD の活動を統制する法律(設置法)であり、ASD の機能を以下のように規定している:
  - 国外の人や組織の活動の能力と意図について信号諜報(SIGINT)を行う。
  - オーストラリア政府の要求に応じて諜報活動を行う
  - 連邦政府、州政府のセキュリティや情報の完全性について助言、支援を行う。
  - オーストラリア防衛軍の諜報活動に関する支援を行う。
  - 連邦政府、州政府の暗号、コンピュータ、通信技術に関する支援を行う。

- Customs Act 1901 (根拠法)／Defense Trade Controls Act 2012 (米豪軍事協力)／Customs (Prohibited Exports) Regulations 1958, 13E／Defense and Strategic Goods List Amendment 2011／Australian Export Controls for defense and Dual-Use Goods
  輸出入に関する規制を示したもので、具体的には 3.9.3.4. 章にまとめる。

- Crimes Act 1914, Criminal Code 1995
  政府機関の秘密保持を定めており、政府機関のセキュリティ確保の根拠としている。

- Directive on the security of Government business
  政府各機関の長に対して、各機関が機能するために必要な能力、政府に対する信頼性の確保などを確実にするためのセキュリティプログラムの実施を要求する。

- Protective Security Policy Framework (PSPF)
  政府機関のリスクレベルの設定、セキュリティ確保のための義務的事項の決定など政府業務のセキュリティポリシーを定めている。また、セキュリティ・ガバナンスを取り決めると共に、政府の情報セキュリティマネジメントを定めている。Tier3 政府の情報セキュリティマネジメントフレームワークのうち、”Australian Government Information Security Management Guidelines”において、機微情報、機密情報の特定と取扱いについて規定している。

- AISEP Policy Manual
  製品認証制度 AISEP を定める文書の一つで、セキュリティ製品等に関する基本的なフレームワークを示すものである。具体的には 3.9.3.2. 章にまとめる。

- Information Security Manual
  セキュリティ対策全般についての基準を定めたものである。、具体的には 3.9.3.1. 章に示す。

- ASD Cryptographic Evaluation
  オーストラリアとニュージーランドの政府が情報やシステムを守るために使う暗号製品の脆弱性等 の評価を行う制度である。、具体的には 3.9.3.2. 章にまとめる。

- Cybercrime Act, 2001, No. 161
  欧州理事会のサイバー犯罪条約に対応して立法化された法律で、行政官の命令があった場合に、暗号鍵の開示、または暗号データの復号を要求する(12 項)。命令に従わない場合は、6 か月の懲役等の罰則を持つ。

3.9.3. 暗号に関わる各種制度及び規制

3.9.3.1. 利用すべき暗号方式

Information Security Manual (ISM)は、セキュリティ対策全般についての基準を定めたものであり、その中で利用すべき暗号方式として ASD 認可暗号アルゴリズムを規定している。なお、ASD 認可暗号アルゴリズムは ASD Cryptographic Evaluation での評価対象である。

- Information Security Manual (ISM)[128]
  政府 ICT システムのセキュリティを統制するための国内標準で、セキュリティ認証制度 AISEP を補う位置づけである。政府の異なるレベルの組織に対応して情報セキュリティに対する意識啓発を促進するためのドキュメントとして整理している。
  構成文書の 1 つである Control Manual (2014)[129]において、ASD 認可暗号アルゴリズム(ASD Approved Cryptographic Algorithms) (表 3-18)、ASD 認可暗号プロトコル(ASD Approved Cryptographic Protocol)、鍵交換などについて規定している。

表 3-18 ISM で規定される ASD 認可暗号アルゴリズム

分類	アルゴリズム
非対称暗号	Diffie–Hellman (DH) 暗号化セッション鍵の合意
	Digital Signature Algorithm (DSA) 電子署名
	Elliptic Curve Diffie–Hellman (ECDH) 暗号化セッション鍵の合意
	Rivest–Shamir–Adleman (RSA) 電子署名と暗号化セッション鍵の合意
対称鍵暗号	AES (128, 192, 256 bits)
	Triple DES
ハッシュ関数	SHA-2 (SHA–224, SHA–256, SHA–384, SHA–512)

3.9.3.2. セキュリティ認証制度

セキュリティ認証制度については、AISEP (Australasian Information Security Evaluation Program)と、暗号製品に限定した認証制度として ASD cryptographic evaluation がある。両制度とも ASD が運営しており、認証結果は Evaluated Product List

[128] http://www.asd.gov.au/infosec/ism/index.htm
[129] http://www.asd.gov.au/publications/Information_Security_Manual_2014_Controls.pdf

(EPL)[130] として公開される。

- AISEP (Australasian Information Security Evaluation Program)
  オーストラリアとニュージーランドの両政府は、公的な業務等のセキュリティを確保する上で必要となる IT セキュリティ製品について、共同利用できる製品認証制度を整備している。ASD とニュージーランドの Government Communications Security Bureau (GCSB)が所管する。Common Criteria (CC)にも準拠し、さらに追加の要件を含んでいる。

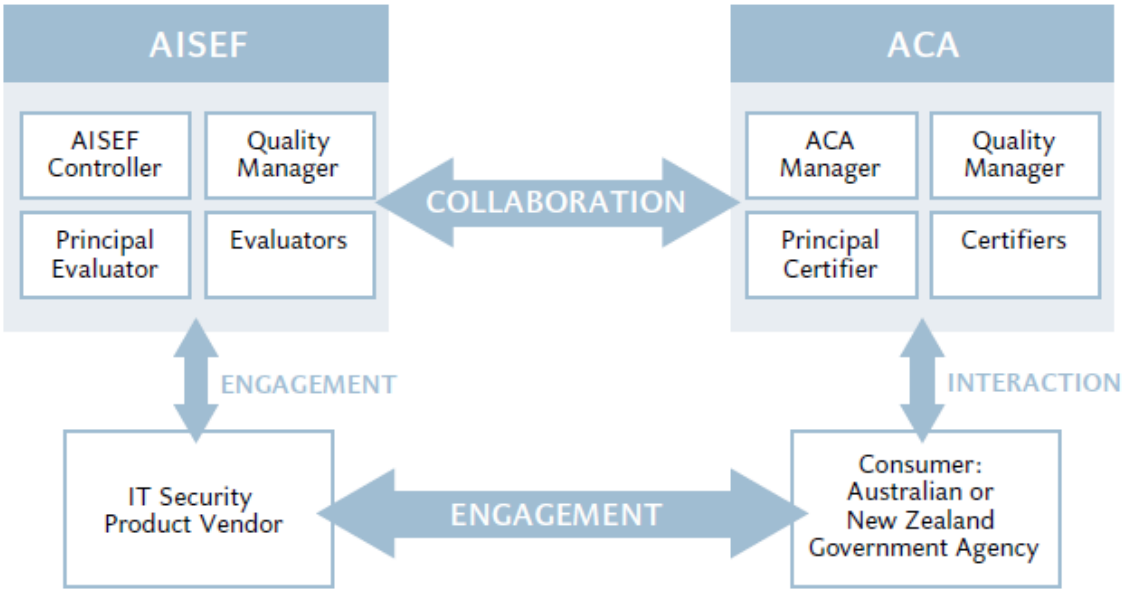


図 3-22 AISEP の関係組織

(出典:Australasian Information Security Evaluation Program (AISEP) AISEP Policy Manual)

ASD は、このプログラムの下で CC 評価を実施するための民間施設に対して Australasian Information Security Evaluation Facilities (AISEFs)としてライセンスを行っている。製品評価を受けたい IT セキュリティベンダは、AISEF の下で評価を受けなければならない。AISEF と認証全般を担当する Australasian Certification Authority (ACA)は協力して評価と認証を行っている(図 3-22)。
図中の AISEF controller, Quality Manager, Principal Evaluator, Evaluator は、AISEP 認証制度において、AISEF 内の評価を行うための役割を示している。また、ACA Manager, Quality Manager, Principal Certifier, Certifier は、ACA 内の認証を行うための役割を示している。

[130] http://www.asd.gov.au/infosec/epl/index.php

AISEP 制度の一環として、近年、Mobile PP (Protection Profile for Mobile Device Fundamentals[131])に基づく認証が開始されている。この Mobile PP は、collaborative Protection Profile に基づき国際共同で作られている。

- ASD Cryptographic Evaluation[132]
  セキュリティ全般を扱う AISEP に対し、ASD Cryptographic Evaluation では暗号製品を対象とし、オーストラリアとニュージーランドの政府が情報やシステムを守るために使う暗号製品の脆弱性等を評価・認証する。製品認証を得るためには、Information Security Manual (ISM)に規定された ASD 認可暗号アルゴリズムと ASD 認可暗号プロトコルを利用しなければならない。

3.9.3.3. 政府の調達要件

政府のセキュリティの基本フレームワークを定めるものとして、2013 年に改訂された Protective Security Policy Framework (PSPF)がある。

ISM は、PSPF の要件に準拠して作られており、機密情報を扱う政府システムに対して AISEP 認証取得を義務づけており、EPL にリストアップされる認証製品を使用するなどのガイダンスが示されている。なお、一般の政府システムについては EPL に代わって、条件に合致したレベルの CC 認証製品で代用することも可能である。

一方、機密情報(RESTRICTED information)以上を扱う政府システムの場合（CC 認証製品で代用している場合は、機密情報を扱う可能性があれば対象となる）には、ASD Cryptographic Evaluation 認証取得が必須である。なお、ASD Cryptographic Evaluation については、英国 UK CAPS、米国 FIPS-140、米国とカナダの CMVP など、他国で行われている同種の認証で代用することはできない。

3.9.3.4. 暗号の輸出入規制

ワッセナー・アレンジメントに従って輸出規制が行われている。

1999 年に Defence and Strategic Goods List が更新され、パブリックドメインソフトウェア、マスマーケットソフトウェア、個人利用製品は除外されている。また、インターネット上で電子的に送信される暗号ソフトウェアも規制対象外である。

- Defence and Strategic Goods List Amendment 2011 (No. 1)[133]
  CATEGORY 5 — TELECOMMUNICATIONS AND “INFORMATION SECURITY” において、輸出規制の対象となる鍵長及び暗号方式の要件について規定している。
  Defence and Strategic Goods List (DSGL)は、1996 年 Customs (Prohibited Exports)

---

131 http://www.asd.gov.au/publications/epl/Protection_Profile_for_Mobile_Device_Fundamentals_v1_1.pdf

132 http://www.asd.gov.au/infosec/aisep/crypto.htm

133 http://www.comlaw.gov.au/Details/F2011L02061

Regulations 1958 が改訂されてから、公開されたものである。

- Customs Act 1901
  関税に関する制度を定めた法律で、Defence and Strategic Goods List Amendment 2011 と組合せて暗号輸出に関する規制を定める。

- AUSTRALIAN EXPORT CONTROLS FOR DEFENCE AND DUAL-USE GOODS "Ensuring Australia Exports Responsibly" [134]
  暗号の輸出規制に関しては、個人利用の場合に規制対象外となることが記載されている。個人利用とは、販売、ローンなどでは提供されないもの、複製、コピーされないものなどである。輸出規制の対象となる暗号製品を海外で喪失した場合には、14 日以内に DECO (Defence Export Control Office)に報告する義務がある。

3.9.4. その他

3.9.4.1. 標準化

オーストラリアにおける国際標準に対する窓口機関(gateway body)が Standard Australia[135]である。ISO, ITEF における標準化の推進をしており、国内における国際標準の対応標準も策定している。

ASD も、Standard Australia のメンバーである。

3.9.4.2. 人材育成

暗号を含む研究教育に関しては防衛省内の DSTO (Defence Science and Technology Organisation)による Academic Scholarships Program があり、予算は年間 12,000AU ドルである。

ASD は、防衛省の部署にから依頼があれば、人材開発などの支援を行っている。依頼に応じて対応するアプローチ(Handoff approach)である。

3.9.4.3. 研究開発

暗号に関する研究開発については、以下の 2 つの代表的な大学が挙げられる。

- Queensland University of Technology
  Science and Engineering Faculty, Electrical Engineering, Computer Science, Information Security の Colin Boyd 教授 [136]は、暗号プロトコルの設計と解析を中心と

[134] AUSTRALIAN EXPORT CONTROLS FOR DEFENCE AND DUAL-USE GOODS," Ensuring Australia Exports Responsibly", Department of Defense, 2007
[135] http://www.standards.org.au/Pages/default.aspx
[136] http://staff.qut.edu.au/staff/boydc/

した研究に取り組んでいる。同学科の Ed Dawson 教授[137]は、データフォーマット、ソフトウェア、情報システムを専門とした研究を行っている。

- Macquarie University[138]
  Centre for Advanced Computing - Algorithms and Cryptography (ACAC)が、オーストラリアにおけるアルゴリズム、計算量理論(complexity)、暗号システムを先導する拠点として共同研究を推進している。

3.9.4.4. サービスにおける暗号利用

クラウドサービスに関する考慮事項を定めた以下の文書において暗号に関する留意事項を示している。

- Cloud Computing Security Considerations, 2012, CYBER SECURITY OPERATIONS CENTRE, 防衛省
  クラウドサービスにおけるリスクマネジメント、第三者、ベンダー顧客、ベンダー従業員からの不正アクセスに対するデータ保護等についての考慮事項を示している。

本文書において、暗号に関する考慮事項やチェックリストを示している。例えば、ASD 認可暗号アルゴリズムで暗号化が施されているかなどを考慮事項に挙げている。

[137] http://staff.qut.edu.au/staff/dawson/
[138] http://research.science.mq.edu.au/acac/

3.10. EU

欧州におけるサイバーセキュリティ政策については、ENISA が中心的な役割を果たしている。暗号評価および推奨リストに関しては、欧州研究開発プログラムである FP6 等において実施された ECRYPT II プロジェクトの成果を引き継ぎ、次期研究開発プログラムである HORIZON2020 への橋渡し的な位置づけとして、ENISA において暗号専門家を増強しメンテナンスが行われている。

輸出規制に関しては、ワッセナー・アレンジメントに準拠した、Council Regulation (EC) No. 1334-2000 等により規定されている。

3.10.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

欧州のサイバーセキュリティ政策は、EU により設立された諮問機関 ENISA による助言や支援に基づき、欧州委員会における ICT を担当する総局(DG CONNECT)などにより推進される。暗号の輸出規制に関しては EU 貿易総局(DG Trade)、研究開発については ICT を担当する総局(DG CONNECT)や EU 研究ファンディング機関である ERC が担当する。安全保障の暗号政策に関しては各国にゆだねられており、欧州レベルでは NATO が関連する。

図 3-23 は、EU における暗号政策に関係する機関の全体像を示したものである。

以下の関連する機関の概要をまとめる。

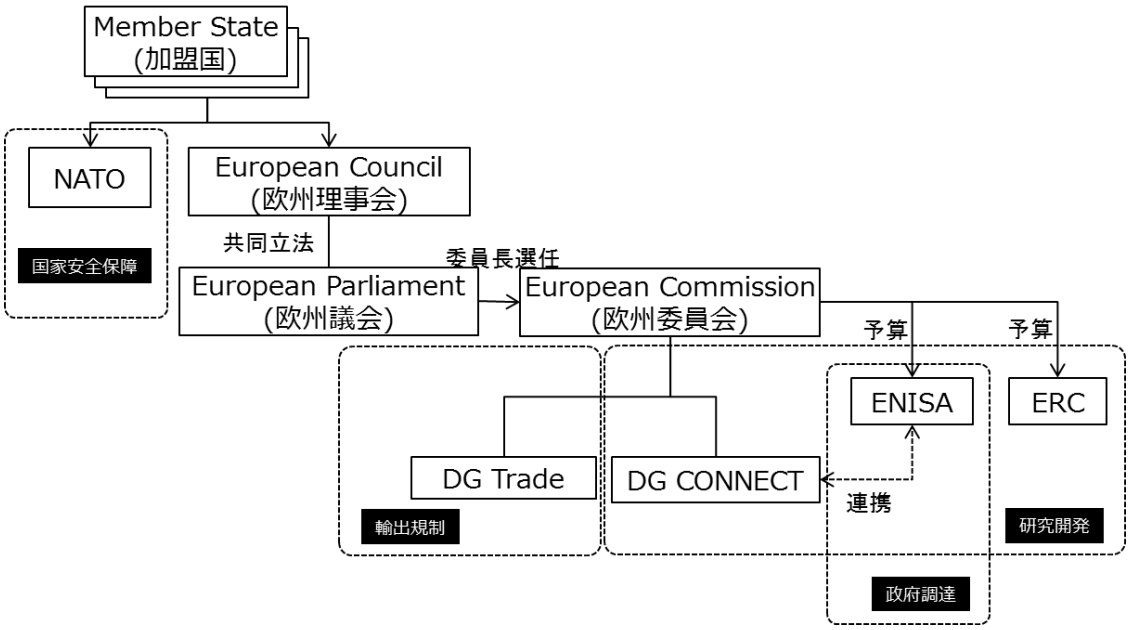
- 欧州委員会(European Commission)
  欧州連合条約により設立されたヨーロッパの地域統合体である欧州連合(European Union)の政策執行機関である。政策分野ごとに総局(Directorate General:DG)が設置され政策執行を行う。
  - DG CONNECT[139]
    欧州委員会における ICT 分野を所管する総局で、インターネットとそのサービス、市民のオンラインプライバシー、セキュリティを守るための活動に関する政策、研究やイノベーションのソリューションを開発している。以下のような取組が行われている。
    - ✧ Cybersecurity Strategy for the European Union
    - ✧ Cybersecurity, privacy and trustworthy ICT: research and innovation
    - ✧ ePrivacy
  - DG Trade
    欧州委員会における輸出入規制などを所管する総局である。

- ENISA
  ENISA 設置法(Regulation (EC) No 460/2004EU)に基づき、EU およびその加盟国に対してネットワーク・情報セキュリティに関する問題への対処を支援するために設立された機関である。EU のネットワーク・情報セキュリティに関する法制度を整備する

[139] http://ec.europa.eu/dgs/connect/en/content/dg-connect

際の技術的な支援を行う。
年間予算は、9,086,354 ユーロ(約 12.7 億円)[140]で、欧州委員会の一般予算から構成される。ミッションは、EU における高度で、効率的なネットワーク・情報セキュリティの達成である。EU 機関と加盟国とにより、ネットワーク・情報セキュリティに関する市民、消費者、企業、公共部門の文化を醸成するすることを目的とする。

- ERC[141]
  HORIZON2020, FP7 等の欧州研究開発プログラムの下で、すべての研究分野における先端研究(frontier research)へのファンディングと支援を通じて研究開発を推進する。ERC ファンディングスキームを実現し、HORIZON2020 の下で約 130 億ユーロの予算を配分する。



NATO：North Atlantic Treaty Organization (北大西洋条約機構)

DG Trade：Directorate General Trade (貿易総局)

DG CONNECT：Directorate General for Communications Networks, Content & Technology (通信ネットワーク・コンテンツ＆技術総局)

ENISA：European Union Agency for Network and Information Security (欧州連合ネットワーク・情報セキュリティ庁)

ERC：European Research Council (欧州研究会議)

図 3-23 暗号政策に関する組織体制(EU)

[140] Annual report

[141] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/european-research-council

3.10.2. 暗号に関わるセキュリティ政策の遂行に関連する法制度

EU においては、安全保障の暗号政策に関しては各国にゆだねられており、政府調達等の欧州共通のガイダンスに重点が置かれている。

主な法制度を分類整理したものが表 3-19 と図 3-24 である。

主な取組の概要は以下の通りである。

- EU Cyber Security Strategy – open, safe and secure[142],[143]
  インターネットやサイバー空間の影響が増大する中で、サイバーセキュリティに関する EU のビジョン、役割、責任を明確にした戦略を示している。その手段の一つとして暗号の開発の継続的な支援をあげている。暗号アルゴリズムに関する具体的な内容までは規定していない。

- Digital Agenda for Europe (DAE)[144]
  欧州経済を再生し、欧州の市民、企業がデジタル技術のメリットを十分に享受できるようにすることを目指す情報通信技術を含む戦略である。EU の上位の経済成長戦略 Europe 2020 の下に 7 つの旗艦イニシアチブが挙げられており、そのうちの情報通信基盤に係わる戦略が DAE である。

表 3-19 法制度の分類と一覧(EU)

分野	名称	関係組織
上位政策・戦略	EU Cyber Security Strategy - open, safe and secure	EC
	Digital Agenda for Europe (DAE)	EC
暗号政策・設置法	EC regulation (EU) No 611/2013	EC
	42 COM (2008) 798, COMMUNICATION FROM THE COMMISSION TO THE COUNCIL	欧州議会
	EU Directive 2002/58/EC	EC
	Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10	EC
	Convention on Cybercrime	EC
輸出入規制	Council regulation (EC) No. 428/2009 of 5 May 2009	EC
	Council Regulation (EC) No. 1334-2000.	EC
政府調達	Algorithms, Key Sizes and Parameters Report	ENISA
標準・基準	(再掲) Algorithms, Key Sizes and Parameters Report	ENISA
	The use of Cryptographic Techniques on Europe	ENISA

[142] http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm
[143] http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm
[144] http://ec.europa.eu/digital-agenda/digital-agenda-europe

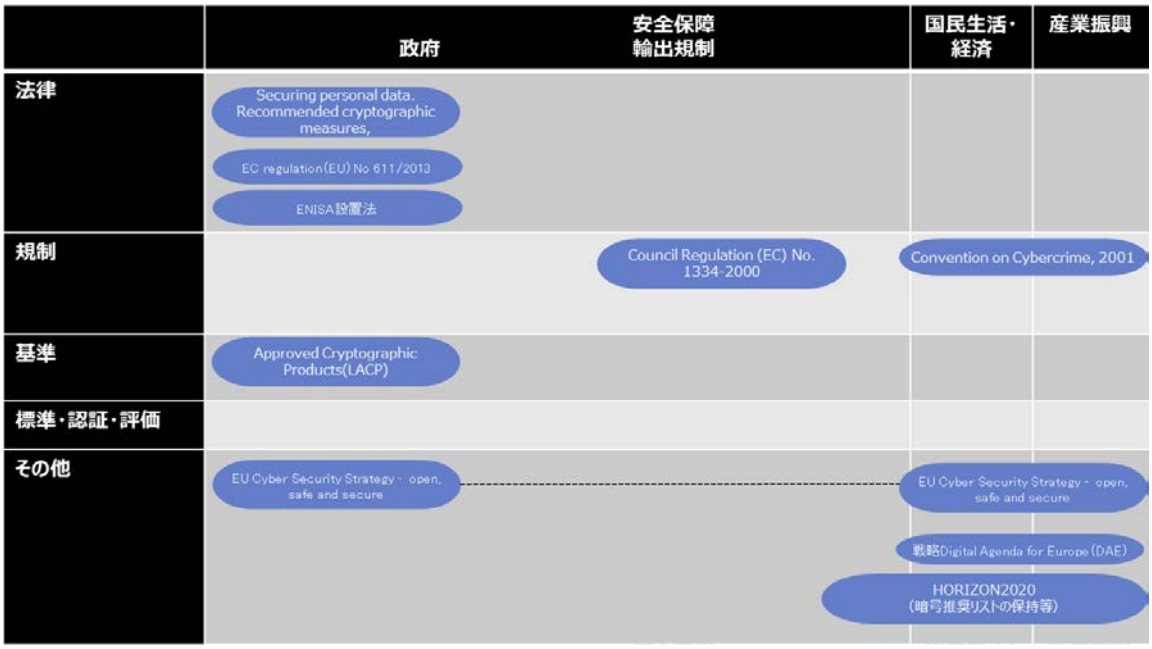


図 3-24 EU における暗号関連政策マップ

- EC regulation (EU) No 611/2013[145]
  プライバシーと電子通信に関する EU 指令 Directive 2002/58/EC on privacy and electronic communications の下で、個人情報漏えいの通報に関する規定をする。EU 指令 2002/58/EC に基づく個人情報漏えいにおける通報に関する EC の規制を規定。暗号対策の適切なリストの確立に関する諮問機関として ENISA を参照している。

- Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004[146]
  ENISA 設置法。欧州委員会からの予算により運営される法人格を持つ EC の傘下機関である。
  欧州委員会と EU 加盟国に対して、ネットワーク・情報セキュリティに関してレギュレーションが規定する問題について支援および助言を与える。また、ネットワーク・情報セキュリティに関する EU の法制度の更新、策定のための技術的な準備作業を支援する。さらに、欧州議会、欧州委員会、欧州および各国の所管機関に対して、要請に応じて助言を与える。

- Convention on Cybercrime, 2001[147]
  2001 年に採択されたサイバー犯罪に関しての対応を取り決めた国際条約。条約により

[145] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF
[146] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML
[147] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185

加盟国は、復号命令について、義務ではないが、法制度化することができる[148]。

- Council regulation (EC) No. 428/2009 of 5 May 2009／Council Regulation (EC) No. 1334-2000
  輸出入規制に関するものである。3.10.3.4. 章にまとめる。

- Algorithms, Key Sizes and Parameters Report
  利用すべき暗号方式に関するガイドラインを示す。具体的には 3.10.3.1. 章にまとめる。

- The Use of Cryptographic Techniques in Europe
  EU 加盟国の政策決定者への暗号要件に関する推奨をまとめている。3.10.3.2. 章にまとめる。

- Securing personal data. Recommended cryptographic measures, ENISA
  以下の点に関する対処について、非専門家向けの文書としてまとめている。
  - データ取得者が、機微データ、個人データについて保護すべきこと。
  - IT 利用者が、個人情報を保護するために暗号技術を利用する方法を示す。
  - EU と加盟国における個人情報、機微情報に対して、暗号化について最小限の要求を示す。

3.10.3. 暗号に関わる各種制度及び規制

3.10.3.1. 利用すべき暗号方式

利用すべき暗号方式については、NESSIE[149], ECRYPT, ECRYPT II といった欧州研究開発プログラムにおいて実施された暗号技術評価プロジェクトにおいて作成および改訂されてきた。これらの成果に基づき、現在有効な暗号方式の最新の文献およびリストには以下のものがある。

なお、ENISA がまとめた以下のレポートは、欧州における推奨暗号を示しているが、主要国は ENISA のレポートを参考にしつつ独自の暗号リストを定めている。つまり、参考情報として啓発的な効果がある[150]が、政府システムの調達における強制力はない。

- Algorithms, Key Sizes and Parameters Report, 2014, ENISA[151]
  暗号アルゴリズム、鍵長、パラメータに関する推奨についてまとめ、EU 加盟国が個人情報、機微情報の保護において対処すべき暗号に関する最小限の要件を示している。
  暗号アルゴリズム、鍵長、パラメータに関する推奨について ENISA によって公開され

[148] Crypto Law Survey
[149] The NESSIE project (New European Schemes for Signatures, Integrity and Encryption) (2000-2003)
[150] 政府機関ヒアリングの結果による。
[151] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014

た文書であり、アルゴリズムは表 3-20、鍵長は表 3-21 のものが推奨されている。
本レポートは、ECRYPT、ECRYPT II の年次レポートを継承するものであり、2013 年に初版発行、2014 年に改訂された。意思決定者向けの技術書で、専門化向けの文書としてまとめている。KU Leuven とブリストル大学の協力によりまとめられた。

表 3-20 推奨される暗号アルゴリズム

分類	推奨アルゴリズム（10-50 年以上の安全に利用できると期待される）	レガシーアルゴリズム（弱点は見つかっていないが優れた代替方式がある）
ブロック暗号	AES、	Triple DES 、 Kasumi 、 Blowfish
	Camellia	
ストリーム暗号	HC-128	Grain、Mickey 2.0、Rabbit、Trivium
	Salsa20/20	
	ChaCha	
	SNOW 2.0、SNOW 3G	
	SOSEMANUK	
ハッシュ関数	SHA-2 (SHA-256, SHA-384, SHA-512)	SHA-224、SHA-1、RIPEMD-160
	SHA-3	
	Whirlpool	
公開鍵暗号	RSA-OAEP	(none)
	RSA-KEM	
	PSEC-KEM	
	ECIES-KEM	
電子署名	RSA-PSS	RSA-PKCS#1 v1.5、RSA-FDH、RSA-DS3、(EC)DSA、(EC)GDSA、(EC)RDSA
	RSA-DS2	
	PV Signature	
	(EC)Schnorr	
	(EC)KDSA	

表 3-21 推奨される鍵長

分類	推奨の最低鍵長	レガシーの最低鍵長
素因数分解型	3072 bit 以上	1024 bit 以上
離散対数型	鍵長 3072 bit 以上でパラメータ q が 256 bit 以上	鍵長 1024bit 以上でパラメータ q が 160 bit 以上
楕円曲線上の離散対数型	256 bit 以上	160 bit 以上

- The Use of Cryptographic Techniques in Europe[152]
  EU 加盟国の政策決定者への暗号要件に関する推奨をまとめている。本文書では、EU 加盟国の電子政府サービスにとって、暗号技術の勧告、仕様が市民のプライバシーに直接的な影響を与えることを示している。また、加盟国の電子政府サービスにおいて保存、転送される機微情報の暗号化に関連する暗号文書と仕様についてまとめており、日本の CRYPTREC、米国 NIST の動向についても概要紹介している。

3.10.3.2. セキュリティ認証制度

EU における情報保証(Information Assurance)の考え方に基づき、欧州連合機密情報(European Union Classified Information ：EUCI)[153]が規定され、以下に示す機密区分に応じて、認証された暗号製品が求められる。機密区分は、機密性の高い順に EU TOP SECRET, EU SECRET, EU CONFIDENTIAL, EU RESTRICTED, and EU COUNCIL / COMMISSION の 5 段階に区分されている。

(a) 機密区分"SECRET UE/EU SECRET"以上に分類される情報の機密性については、セキュリティ委員会の推奨に基づき、Crypto Approval Authority (CAA)[154]により認証された暗号製品により保護されなければならない。
(b) 機密区分"CONFIDENTIEL UE/EU CONFIDENTIAL"または "RESTREINT UE/EU RESTRICTED"に分類される情報の機密性については、セキュリティ委員会の推奨に基づき、Crypto Approval Authority (CAA)の長官により認証された暗号製品により保護されなければならない。

これらの制度に基づく認証製品の一覧は、Approved Cryptographic Products (LACP)[155]により公開されている。

3.10.3.3. 政府の調達要件

暗号製品に関する政府の調達要件は、EU では規定せず、各国政府が EU、ENISA 等の情報を参考に独自に決める。

3.10.3.4. 暗号の輸出入規制

EU における暗号の輸出入規制に関しては、欧州委員会の DG Trade が担当しており、ワッセナー・アレンジメントに従い、EU の規制が定められている。関連する内容は以下の通

[152] https://www.enisa.europa.eu/activities/identity-and-trust/library/the-use-of-cryptographic-techniques-in-europe
[153] Information Assurance (IA), European Union Classified Information (EUCI) http://www.consilium.europa.eu/policies/information-assurance
[154] 暗号製品認証当局。
[155] http://www.consilium.europa.eu/policies/information-assurance/list-of-approved-cryptographic-devices?lang=en

りである。

- Council Regulation (EC) No. 1334-2000
  暗号を含むデュアルユース製品の輸出を規制するものである。この規制は、ワッセナー・アレンジメントに準拠する。

- Council regulation (EC) No. 428/2009 of 5 May 2009[156,157]
  デュアルユースアイテムの輸出に関する規制を目的としたもので、デュアルユースアイテムの転送、売買仲介に関する規制を定めている。

3.10.4. その他

3.10.4.1. 標準化

欧州における暗号に係わる標準化団体として以下のものがある。

- ETSI(European Telecommunications Standards Institute：欧州電気通信標準化機構)[158]
  ヨーロッパの電気通信の全般にかかわる標準化組織で、暗号に関連して、署名のみを対象にアルゴリズム、鍵長の標準を策定した取組[159]がある。署名に関する推奨アルゴリズムとして、RSA, DSA, EC-GDSA があげられている。民間企業等の参加組織の会費により標準化活動が運営されている。

- CEN(Comité Européen de Normalisation：欧州標準化委員会)
  ヨーロッパ経済の力を強め、ヨーロッパの市民の福祉や環境を高めることを目的とした欧州の標準化団体である。暗号に関しては、例えば、参照文書 CWA 14167-2 において、署名操作に関して触れている。

3.10.4.2. 人材育成

EU においては、欧州研究開発プログラムによるファンディングにより実施された暗号プロジェクトが人材育成の役割も担っていた。特に、FP7、FP6 においては、産業界と学術界の研究者ネットワークを継続させることに重点を置き、優先的に研究テーマが設定され人材育成に貢献した。特に、ECRYPT II においては、若手人材の育成、25 人の若手専門家を育成の成果が挙げられる。

EU における暗号に関するこれまでのプロジェクト等を比較したものが表 3-22 の通りで

---

[156] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF
[157] European Communities Official Journal L 134, 29 May 2009, page 1
[158] ETSI TS 102 176-1 V2.0.0 (2007-11), Technical Specification, Electronic Signatures and Infrastructures(ESI);Algorithms and Parameters for Secure Electronic Signatures
http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.00.00_60/ts_10217601v020000p.pdf
[159] ETSI TS 102 176-1 V2.0.0 (2007-11), Technical Specification, Electronic Signatures and Infrastructures(ESI);Algorithms and Parameters for Secure Electronic Signatures

ある。

表 3-22 EU における暗号に関するこれまでのプロジェクト等比較

プロジェクト等	HORIZON ICT 32 -2014 他	ECRYPT II	ECRYPT	NESSIE
期間	2014-2020	2008-2013	2004-2008	2000-2003
予算源	HORISON 2020 (2014 年暗号公募 100 万ユーロ)	FP7 (300 万ユーロ(4 年))	FP6 (暗号予算不明)	FP5 (暗号予算不明)
目的・対象範囲	ICT 環境の変化に対応し、ライフスパンにわたりセキュリティを確保する暗号の要件	暗号分野における EU の競争力を維持する為に、産業界と学術界の研究者ネットワークを継続させる。	暗号分野における EU の競争力を維持する為に、産業界と学術界の研究者ネットワークを継続させる。	安全な暗号プリミティブを特定する。
主な主体	Kath. Univ. Leuven	Kath. Univ. Leuven	Kath. Univ. Leuven	Kath. Univ. Leuven
成果物	ECRYPT Yearly Report の更新を継続	ECRYPT II Yearly Report on Algorithms and Key Lengths (推奨暗号アルゴリズム)	ECRYPT II Yearly Report on Algorithms and Key Lengths (推奨暗号アルゴリズム)	FINAL SELECTION OF CRYPTO ALGORITHMS

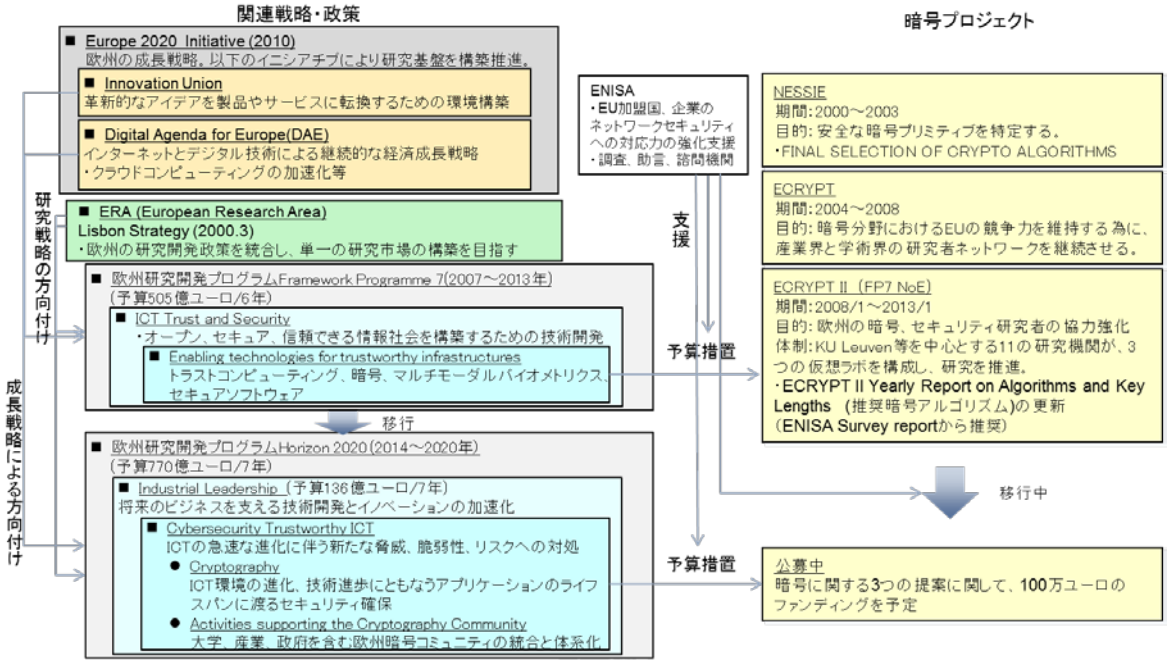


図 3-25 EU 戦略と暗号プロジェクトの全体像

3.10.4.3. 研究開発

EU における研究開発は、欧州研究開発プログラム(FP7, FP6)や 2014 年から開始された HORIZON2020 において実施されている。図 3-25 は欧州研究開発プログラムと暗号研究プロジェクトの関係について全体像をまとめたものである。

HORIZON2020 の 2014 年の行動計画における暗号関連の構成は以下の通りである。

- ICT 公募
  - ICT Cross-Cutting Activities(ICT 分野横断活動)
    - ICT 32 – 2014: Cybersecurity, Trustworthy ICT
      - Research & Innovation Actions(研究とイノベーション)
        - Cryptography
          ICT 環境の変化、ICT 技術の進歩に対応して、アプリケーションのライフスパンにわたりセキュリティを確保するための課題に取組まなければならい。課題には、以下のものを含む
          - ハードウェアベースのリソース効率の良い、高度に安全なリアルタイム技術
          - リソース効率が高く、高度に安全な、完全なホモモルフィック暗号
      - Activities supporting the Cryptography Community
        研究活動を補うために、以下の課題に取り組まなければならない：
        - 大学、産業、法執行機関、防衛省などの欧州暗号コミュニティの永続的な統合と構造化
        - 技術ギャップ、マーケットと実装の機会の特定。
        - 公的部門を含む欧州標準の開発。
        - セキュリティと実装ベンチマーキングによるオープンな競争の体系化

HORIZON2020 において、暗号関連の以下の研究公募が行われている。

(a) Research & Innovation Actions, Cryptography
ICT 環境の変化、ICT 技術の進歩に対応して、アプリケーションのライフスパンにわたりセキュリティを確保するための課題に取組まなければならい。

(b) Activities supporting the Cryptography Community
研究活動を補うために、大学、産業、法執行機関、防衛省などの欧州暗号コミュニティの永続的な統合と構造化などに取組む。

(a)に関しては、約 50 件の研究提案が行われており、そのうち 10～20 件の暗号に直接関連する研究である。まだ採択結果は決まっていないが、2～4 件程度が採択される見通しであ

る[160]。

(b)に関しては、1 件の CSA (Coordination and Support Action)に対するファンデングが予定されている。3 つのコンソーシアムが提案しており、その中の 1 件は、ECRYPT II の後継プロジェクトの提案が踏まれている[161]。現在審査中であり、結果は決まっていない。

以下に、その他の暗号関連プロジェクトの概要をまとめる。

- NESSIE
  欧州研究開発プログラム FP5 の予算により、安全な暗号プリミティブを特定することを目的として 2000～2003 年まで実施された。Kath. Univ. Leuven が中心的な役割を果たし、成果物として FINAL SELECTION OF CRYPTO ALGORITHMS がまとめられた。

- ECRYPT (2004-2008)
  4 年間の欧州研究イニシアチブで、2004 年 2 月 1 日に開始された。欧州の情報セキュリティの研究者の協力を促進することを目的として実施された。、特に、暗号とデジタル透かしに重点が置かれた。ストリーム暗号の公募等が行われた。

- ECRYPT II (European Network of Excellence in Cryptology II)(2008-2013)[162]
  ECRYPT に引き続き、欧州における情報セキュリティの研究者の共同研究をさらに強化することを目的として実施された。ECRYPT II の研究ロードマップは、暗号が利用される環境と脅威モデルの変化、暗号が根拠とする数学的な計算の困難性の退化、新しいアプリケーションと暗号実装に対する要求に動機付けられて策定された。
  以下の 3 つの仮想研究室により構成されたプロジェクトである：
  - 対称鍵アルゴリズム（SymLab)
  - 公開鍵アルゴリズムとプロトコル（MAYA)
  - ハードウェアとソフトウェアの実装（VAMPIRE)

  ECRYPT II プロジェクトにおいては、年次レポート ECRYPT II Yearly Report on Algorithms and Keysizes を公開し、推奨暗号リストを毎年更新を行っていた。
  欧州研究開発プログラムが FP7 から HORIZON2020 に移行したことにより、ECRYPT II において公開された暗号リストは、3.10.3.1. 章に記載した通り、ENISA が「Algorithms, Key Sizes and Parameters Report, 2013, ENISA」としてメンテナンスを行っている。この文書の更新・メンテナンスのために、ENISA は暗号担当者を 2 名増員している。

[160] 有識者へのヒアリング結果による。
[161] KU Leuven Professor Bart Preneel へのヒアリング結果による。
[162] http://www.ecrypt.eu.org/

- CAESAR(Competition for Authenticated Encryption: Security, Applicability, and Robustness) [163,164,165]
  新しい暗号を決定するためのプロジェクトであり、現在、暗号の提案を受け付けている段階である。暗号研究の国際コミュニティによって運営されており、中核メンバーは、ECRYPT の関係者が含まれる。ECRYPT II の仮想ラボ SymLab と VAMPIR が主催したワークショップ DIAC (Directions in Authenticated Ciphers)における検討が最初の起点となっている。CASEAR 委員会には、KU Leuven の Bart Preneel 教授が含まれており、全体の取りまとめは Univ. of Chicago and TU Eindhoven の Dan Bernstein 教授である。
  他のプロジェクトとは異なり、NIST からの予算を受けているため、HORIZON2020 で予定されるプロジェクトとは異なる位置づけとなる。CAESAR の暗号選定は、公開された暗号解析文書に基づき行われる。

3.10.4.4. サービスにおける暗号利用

欧州においては、ENISA が公開するクラウドサービスに関する以下のガイドラインにおいて暗号に係る確認事項を定めている。

- Cloud Computing: Information Assurance Framework
  クラウドコンピューティングを利用する企業(特に中小企業)、クラウドプロバイダを対象として、クラウドサービスを利用する際に、情報セキュリティ確保のために、クラウドプロバイダに対して確認すべき項目、利用者側・プロバイダ側の法的責任の範囲や責務の範囲をまとめている。確認すべき項目については、「人的セキュリティ」、「サプライチェーンにおける情報セキュリティの確保」、「データおよびサービスのポータビリティ」、「法的要求事項」等に分けてまとめている。

このガイドラインにおいて、暗号に係る情報セキュリティ確保の要件として、暗号化の利用場面、暗号化すべき対象、アクセス鍵の所有者、鍵の保護について確認すべきであることを示している。暗号アルゴリズムや認証制度については記載はない。

[163] http://competitions.cr.yp.to/index.html
[164] プロジェクトの予算の一部は、NIST grant 60NANB12D261, "Cryptographic competitions", 2013.01.01–2017.12.31.による。
[165] http://competitions.cr.yp.to/faq.html

4. セキュリティ認証取得製品に関する動向調査

セキュリティ認証制度として、暗号モジュール認証制度(CMVP/JCMVP)とコモンクライテリア(CC)認証がある。これらの認証制度は、欧米でスタートしてからすでに 20 年近くの運用実績があり、日本においても 10 年近くの運用実績がある。しかし、セキュリティ認証取得製品数などの利用実績においては、欧米と日本では相当な違いが生じている。

そこで、これらのセキュリティ認証取得製品数について以下のとおり経年推移を調査する。また、その推移の違いがなぜ起きるのかについて、セキュリティ認証製品の利用強制の有無や採用の動機づけの強弱、当該国での暗号製品競争力の強弱等の観点から、文献・Web 調査等により調査し、分析・検討する。

4.1. CMVP / JCMVP 認証取得製品数の経年推移

CMVP (Cryptographic Module Validation Program)とは、暗号モジュールに暗号アルゴリズムが正しく実装されていることを確認するとともに、暗号鍵、ID、パスワード等の重要情報の安全性が確保されていることを認証する制度として、米国 NIST とカナダ CSEC(Communications Security Establishment Canada：CMVP を NIST と共同で運営するカナダの政府機関)が認証機関として 1995 年 7 月から運営している。

CMVP では、NIST が定める暗号モジュールのセキュリティ要件についての規格である FIPS 140-2 に準拠しているかの確認のために、NISC 及び CSE から公式に認められた独立した第三者機関により暗号モジュール試験が行われる。試験では、FIPS 140-2 で規定される認定アルゴリズムの実装に関する評価のほか、FIPS 140-2 の評価分野において Level 1 から Level 4 までの評価が行われる。

FIPS 140-2 の評価分野は以下の通りである。

(1) 暗号モジュール仕様
(2) 暗号モジュールのポート及びインターフェース
(3) 役割、サービス、及び認証
(4) 有限状態モデル
(5) 物理的セキュリティ
(6) 動作環境
(7) 暗号鍵管理
(8) 電磁妨害／電磁両立性(EMI/EMC)
(9) 自己テスト
(10) 設計保証
(11) その他の攻撃の対処

また、暗号モジュールの各レベルの評価は以下の通りである。

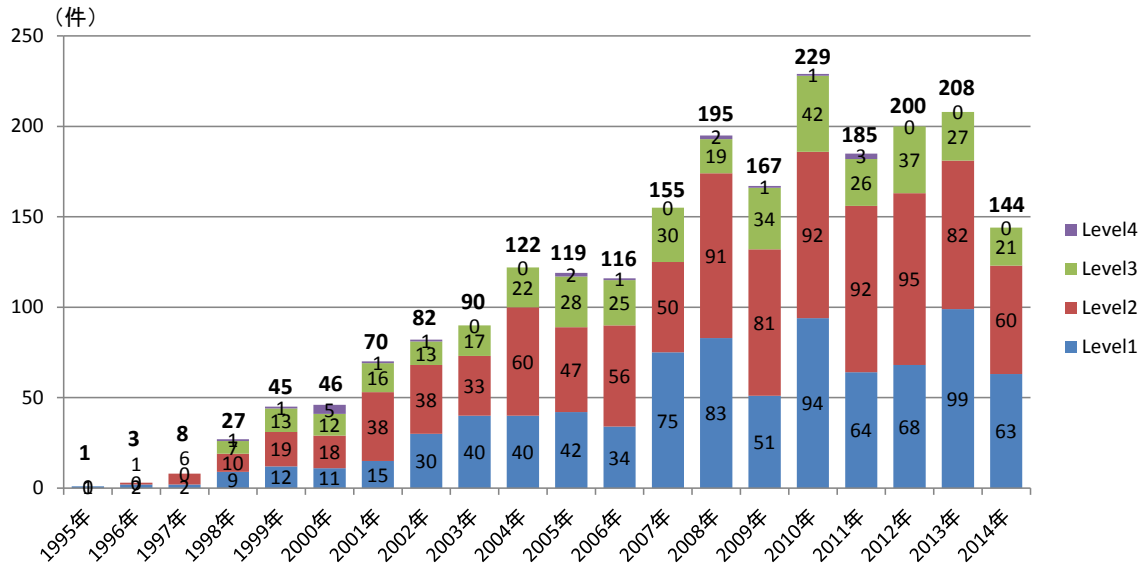
Level 1：基本的なセキュリティ要件を満たすレベル。セキュリティ確保のため特定の物理的なメカニズムは必要としない。

Level 2 : Level 1 に加え、タンパー証跡(暗号モジュールの開封跡が残るシール等)の要件を追加し、物理的なセキュリティメカニズムが強化されたもの。
Level 3 : Level 2 に加え、タンパー検出・応答(取り外し)の要件を追加したもの。
Level 4 : Level 3 に加え、いかなる物理的な攻撃に対してもタンパー検出・応答するよう完全に暗号モジュール部分を保護する物理的メカニズムを加えたもの。

FIPS 140-2 では、総合的な評価として各分野の評価のうち一番低いセキュリティレベル評価が適用される。Level 2 以上は物理的が保護が要件となるが、ソフトウェアの場合は暗号モジュールの物理的な保護に限界があるため、Level 1 での認定が一般的となる。

JCMVP (Japan Cryptographic Module Validation Program : 暗号モジュール試験及び認証制度)は、日本における CMVP と同等の制度で、IPA が認証機関として 2007 年 4 月から正式運用している。CMVP と JCMVP は独立した制度であり、認証対象の暗号アルゴリズムリストには差異があるが、2012 年度より共同認証が開始されている。

CMVP の認証取得製品は、1995 年制度設立以来増加傾向にあり、2014 年 7 月 11 日までの取得数は 2,212 件に達する(図 4-1)。暗号モジュール利用製品の米国及びカナダにおける政府調達には CMVP の認証取得が必須要件になっており、米国政府への製品導入を目指す世界各国のベンダにとって認証取得の動機づけとなること、また米国以外でも FIPS140-2 を採用する国々があることから、世界各国における認証取得が広まっている。
Level 別に見ると、認証取得製品数は Level 1 及び Level 2 が中心であり、総数では Level 1 が 835 件、Level 2 が 969 件である(図 4-2)。



注)2014 年の数値は、2014 年 7 月 11 日までの取得数

図 4-1 CMVP 認証取得製品数(経年変化・Level 別)

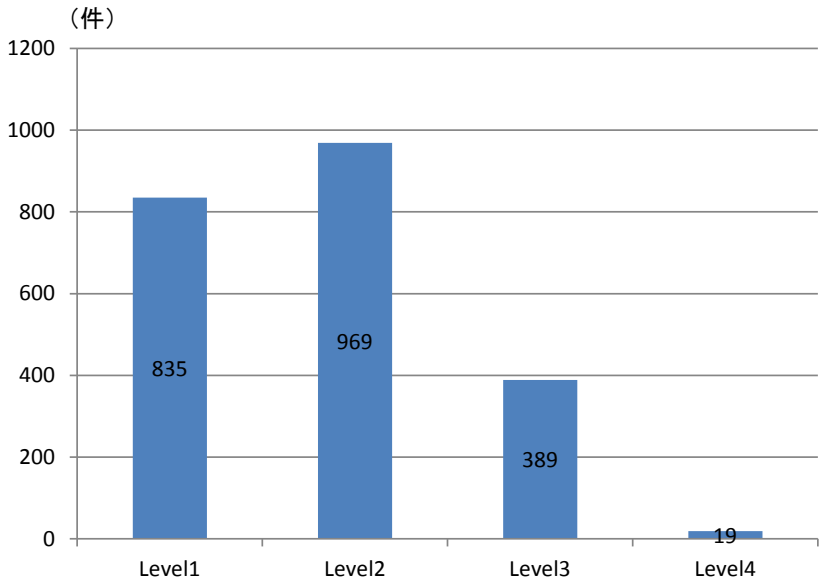


図 4-2 CMVP 認証取得製品数(Level 別)

CMVP の米国外への普及状況を確認するために、米国に本社がある企業における CMVP の認証取得状況を見ると、2014 年 7 月 11 日までの認証取得数は 1,737 件であり(図 4-3)、2014 年でみると CMVP 認証取得製品全体の約 70%を米国企業が占める(図 4-4)。1999 年 2011 年までは概ね 80%台であったが、ここ 3 年は 70%前半台となっており、米国企業以外の認証取得数がやや増えていることは、CMVP が米国以外にも広がっていることを示している。

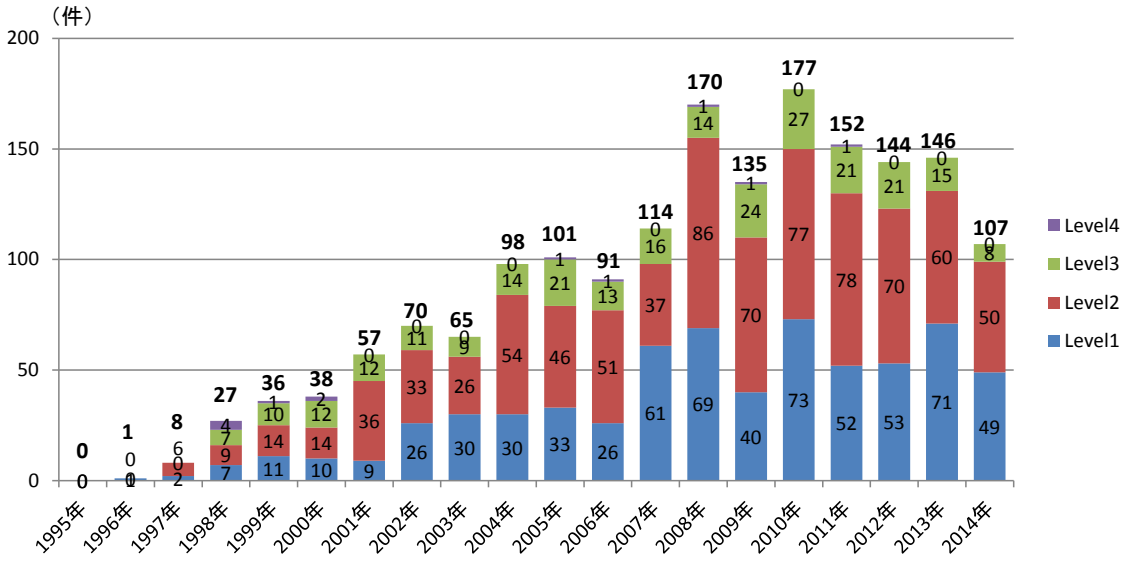


図 4-3 CMVP 認証取得製品数(米国企業のみ・経年変化・Level 別)

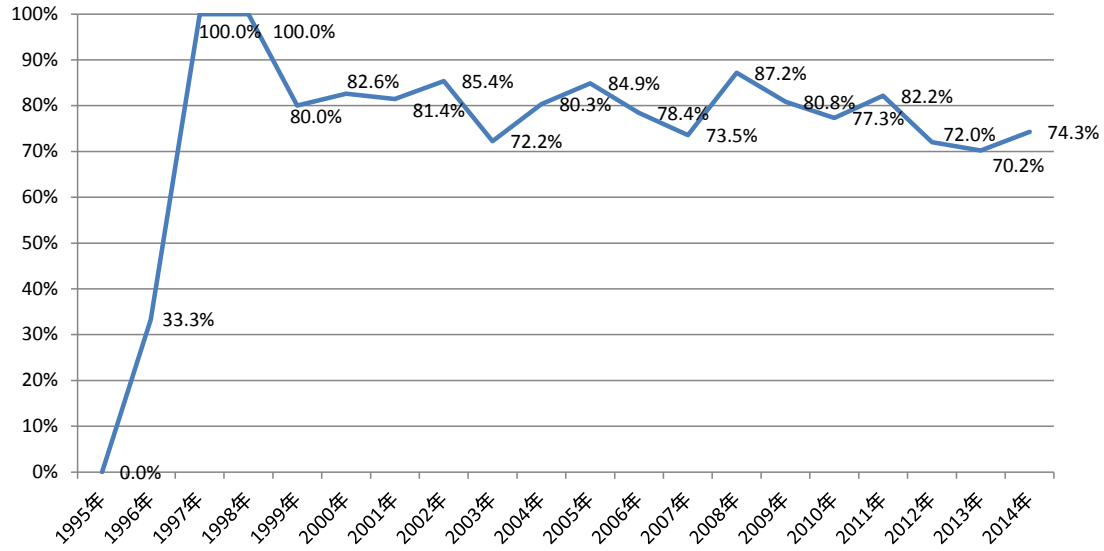


図 4-4 CMVP 認証取得製品数全体における米国企業の比率(経年変化)

一方、JCMVP 認証製品の取得数は、制度設立 2007 年以来年間 4 件が最大であり、2014 年 7 月までの取得数も 18 件に留まっている(図 4-5)。

レベル別に見ると、認証取得製品数はレベル 1 が最も多く、総数でレベル 1 が 14 件、レベル 2・3 は 2 件ずつ、レベル 4 は 0 件である(図 4-6)。2013 年に初のレベル 3 の認証取得製品が発現した。CMVP との共同認証制度を開始した 2012 年以降の認証取得製品 7 件のうち 5 件が、CMVP の認証も取得している。18 件のうち、海外企業による製品は 2 件のみである。

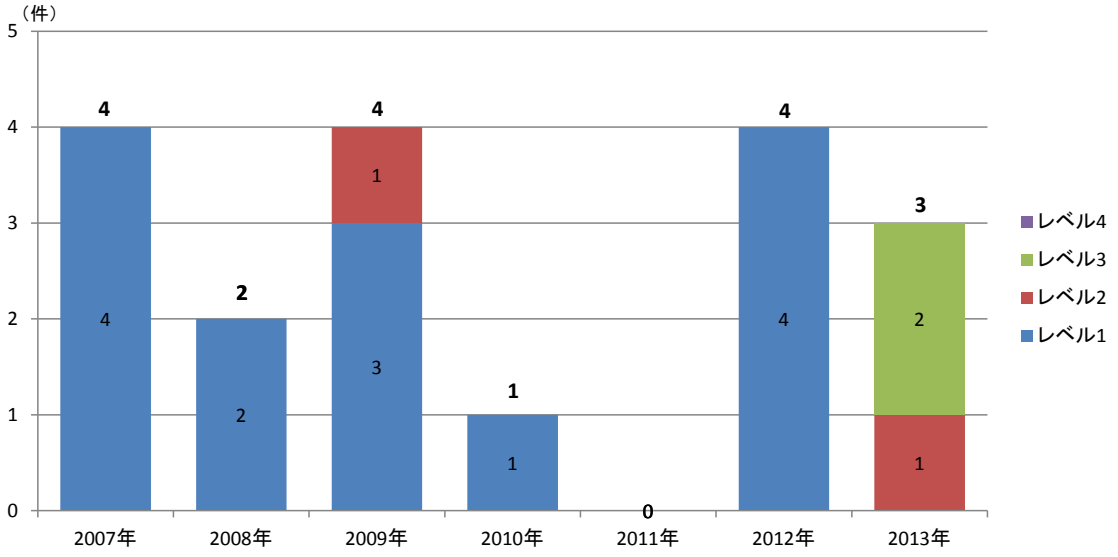


図 4-5 JCMVP 認証取得製品数(経年変化・レベル別)

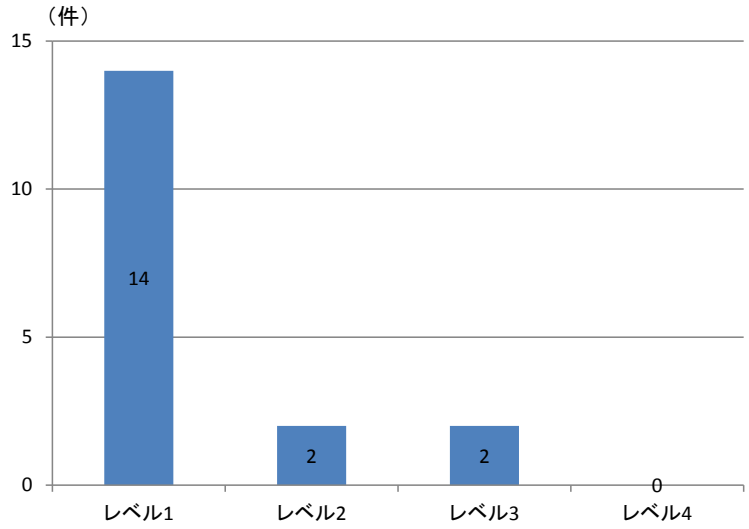


図 4-6 JCMVP 認証取得製品数(レベル別)

「政府機関の情報セキュリティ対策のための統一技術基準(平成 24 年度版)」(平成 24 年 4 月 18 日)においては、暗号と電子署名項目に関する遵守事項として、以下のように定められていた。

政府機関の情報セキュリティ対策のための統一基準(平成 24 年度版) (抄)

2.2.1.6 暗号と電子署名(鍵管理を含む。)

遵守事項(1)(e)

情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、以下のそれぞれの措置を講ずることの必要性の有無を検討し、必要と認めたときは、当該措置を講ずること。

(ア) 暗号モジュールの交換可能なコンポーネント化による構成

(イ) 複数のアルゴリズムを選択可能にする構成

(ウ) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品の選択

(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵の耐タンパー性を有する暗号モジュールへの格納

この遵守事項では、JCMVP 認証取得製品の利用はあくまでも「必要と認めた場合」に限られており、調達における必須要件でないことから、多くのツールベンダにとって、JCMVP の認証取得の強い強制力は働かなかったものと考えられる。

「政府機関の情報セキュリティ対策のための統一技術基準(平成 26 年度版)」は 2014 年 5 月 19 日の情報セキュリティ政策会議にて改訂され、新たに「府省庁対策基準策定のためのガイドライン」も同時に発行された。

しかし、「政府機関の情報セキュリティ対策のための統一基準(平成 26 年度版)」では政府機関における情報システムの調達及び利用において 2013 年 3 月に改定された電子政府推奨暗号リストを利用することを遵守事項に定める一方、「府省庁対策基準策定のためのガイドライン」では同遵守事項の基本対策事項の一例として「暗号モジュール試験及び認証制度に基づく認証を取得している製品の選択」を挙げているにすぎない。

このため、今後の JCMVP の利用拡大につながるかは不透明である。

府省庁対策基準策定のためのガイドライン(抄)

【 基本対策事項 】

＜6.1.5(1)(a)関連＞

6.1.5(1)-1 情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。

a) 情報システムのコンポーネント(部品)として、暗号モジュールを交換することが可能な構成とする。

b) 複数のアルゴリズムを選択することが可能な構成とする。

c) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装された製品であって、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれにひも付く主体認証情報等が安全に保護される製品を利用することを前提とするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。

d) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。

e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のある暗号プロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。

4.2. CC 認証取得製品数の経年推移

CC (Common Criteria)認証 とは、情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格である。CC 評価では、評価保証レベル(EAL: Evaluation Assurance Level)」を定めており、7 段階(EAL 1～EAL 7)が定義されている。EAL は評価対象の検証がどの程度まで行われたかを示す尺度であり、評価対象の保護資産の価値やセキュリティ機能に要求される信頼度によって EAL を選択する。

欧米諸国が、自国で保有している認証評価制度（欧州の ITSEC、米国の TCSEC）を基に、商用製品への活用や国際的な調達の目的から共通評価基準を策定するプロジェクトと

して CC 開発が始まった。1999 年、CC は ISO 標準（ISO/IEC 15408）となり、2000 年には JIS 標準（JIS X 5070）として制定された。

IT 製品等の安全性を客観的に評価した結果を国際的に相互承認する枠組みとして CCRA (Common Criteria Recognition Arrangement)が 2000 年 5 月に創設されており、日本は 2003 年 10 月に認証書生成国として加盟している。2014 年 7 月時点で、26 か国が CCRA に加盟している(表 4-1)。IT セキュリティ評価及び認証制度(JISEC：Japan Information Technology Security Evaluation and Certification Scheme)において承認された評価機関は IT 製品について CC に基づくセキュリティ評価を行い、認証機関は評価報告書並びに評価プロセスの妥当性について CC に基づき検証を行う。認証機関が適切と判断した場合に認証が授与され、認証された製品は CCRA 加盟国間で相互に通用する。

なお、2013 年 9 月に開催された ICCC (International Common Criteria Conference)にて、CCRA 新アレンジメントに関する基本合意が発表され、2014 年 9 月に CCRA 新アレンジメントが発行した。今後は、調達される IT 製品についてセキュリティ要件(cPP)を製品ベンダ、評価機関が中心となった国際的な技術者集団(iTC)が共同で開発する。CCRA では政府調達で考慮されるセキュリティ要件を共通の cPP として開発し、各国が共通の cPP に基づいて製品評価を行うことにより、効率よくセキュアな製品評価及び製品調達が可能となる。詳細は 4.3. 章を参照されたい。

表 4-1 CCRA 加盟国

認証国	アメリカ、イギリス、ドイツ、フランス、カナダ、日本、インド、マレーシア、トルコ、イタリア、スウェーデン、スペイン、韓国、ノルウェー、オランダ、ニュージーランド、オーストラリア
受入国	フィンランド、チェコ、ギリシア、シンガポール、イスラエル、デンマーク、オーストリア、パキスタン、ハンガリー

CC 認証取得製品数について、制度設立以来 2013 年度までの合計取得数をみると、ドイツが最も多く 529 件、次いで米国 484 件、フランス 442 件、日本 425 件、カナダ 203 件と続く。その他の国々は 100 件未満である(図 4-7)。

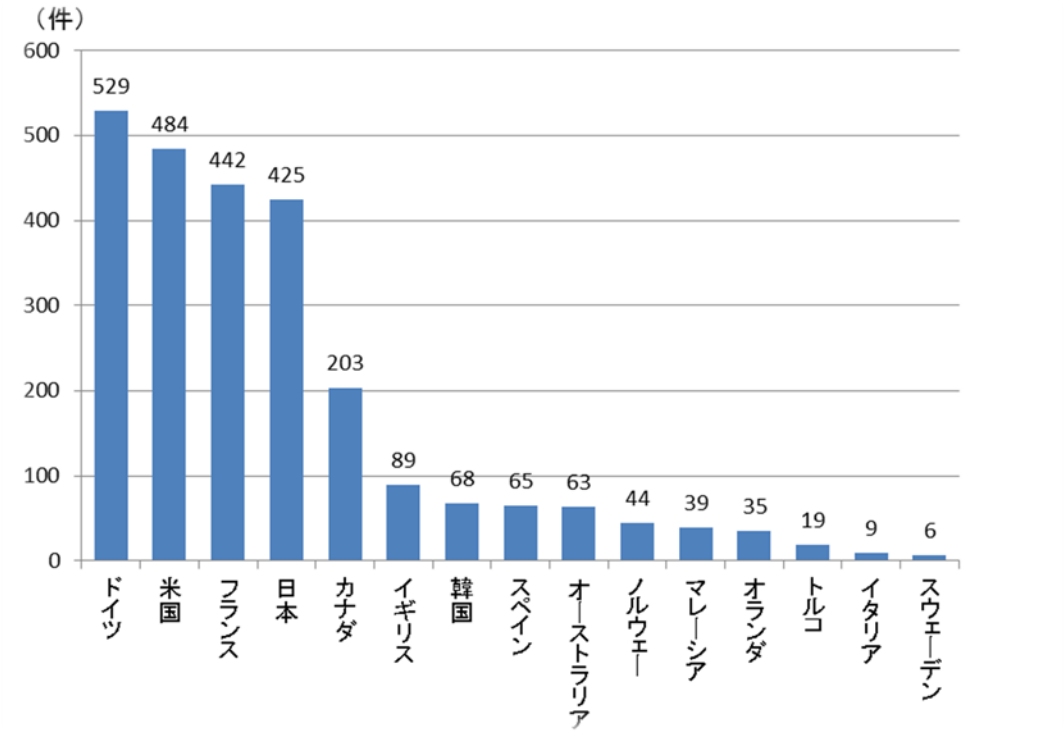


図 4-7 CC 認証取得製品数 ※2014/8/7 時点

4.2.1. 日本

日本政府では、IT 製品・システムの調達に関して、ISO/IEC 15408 (CC)に基づく評価・認証がされている製品の利用が推進されている。

「政府機関の情報セキュリティ対策のための統一基準(平成 26 年度版)」の「5.2.1 情報システムの企画・要件定義」でも、機器調達時には「IT 製品の調達におけるセキュリティ要件リスト」を参照し、適切なセキュリティ要件を策定することが求められている。また、経済産業省「IT 製品の調達におけるセキュリティ要件リスト」では、指定したセキュリティ要件が満たされていることの確認手段として、CC 認証のような国際基準に基づく第三者認証を活用することを推奨している。

政府機関の情報セキュリティ対策のための統一基準(平成 26 年度版) (抄)

5.2.1 情報システムの企画・要件定義
遵守事項(2) 情報システムのセキュリティ要件の策定
(c) 情報システムセキュリティ責任者は、機器等を調達する場合には、「IT 製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

日本における 2013 年度までの CC 認証取得数は 425 件であり、うち EAL 3 が 279 件で最も多いことが特徴的である(図 4-8)。認証取得数は、2007 年度に向け大幅に増加し、2010 年度までいったん落ち着いたものの、2011 年度の件数は再び増加した。

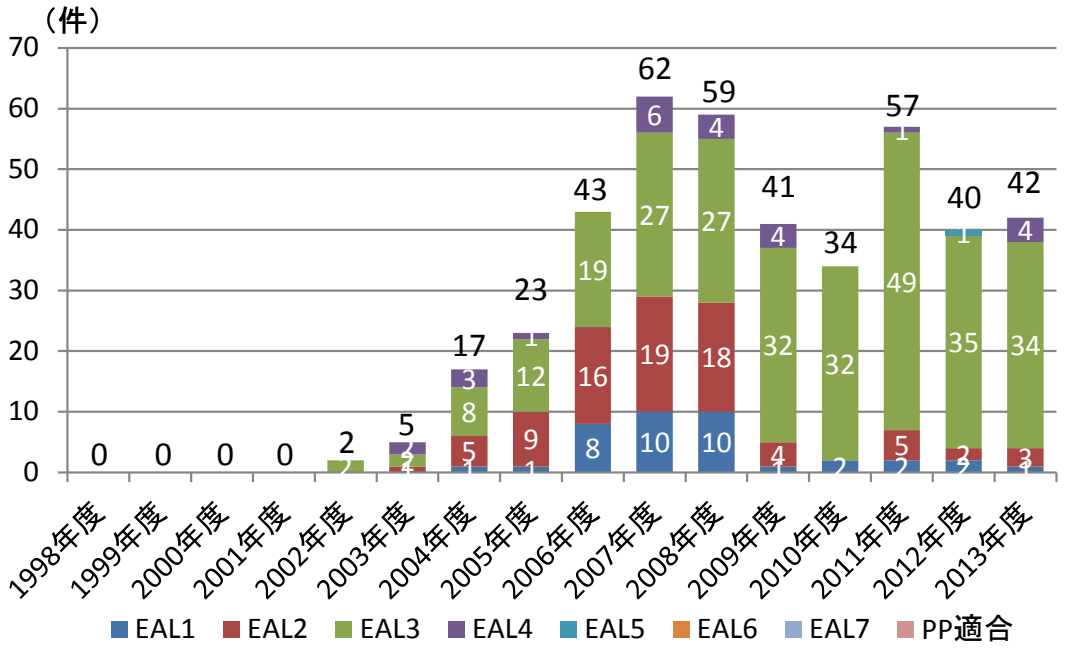


図 4-8 CC 認証取得製品数(日本・EAL 別) ※2014/8/7 時点

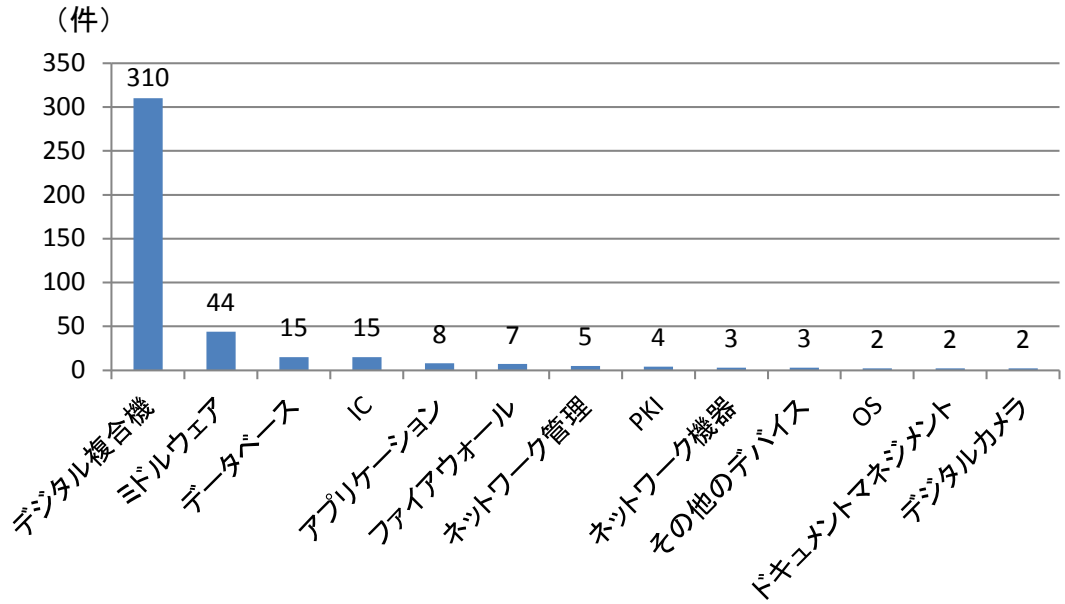


図 4-9 CC 認証取得製品数(日本・製品種別) ※2014/8/7 時点

製品種別でみるとデジタル複合機が最も多く、取得しているベンダは多くが日本の複合機メーカーである（図 4-9）。海外の政府調達ポリシーにより PP 適合評価が定着しているところもあるため、日本の複合機メーカーはグローバルで競争力が高く、特に米国向けの製品輸出を行っていることから、CC 認証取得の動機づけとなっていると想定される。また、政府統一基準により推奨されている 6 分野のうち、デジタル複合機、ファイアウォール、データベース管理ソフトウェア、IC チップについては、認証の実績がある。

4.2.2. 米国

米国における 2013 年度までの CC 認証取得数は 484 件であり、うち EAL 2 が 237 件で最も多い(図 4-10)。急激に取得製品数が増えた 2005 年度から 4 年間は高い水準で件数が推移したが、2009 年度に急激に下がり、再び上昇傾向を見せた。

製品種別でみると、IDS/IPS、複合型、機密データ保護等、多岐にわたっている(図 4-11)。

米国では、政府調達において CMVP または CC 認証取得製品の調達が義務化されており、ベンダにとって認証取得する動機が強くなっている。また、兵器・軍事システムのメーカーや戦闘機に搭載される組込型 OS の開発者などが EAL 6, 7 を取得する事例もみられる。

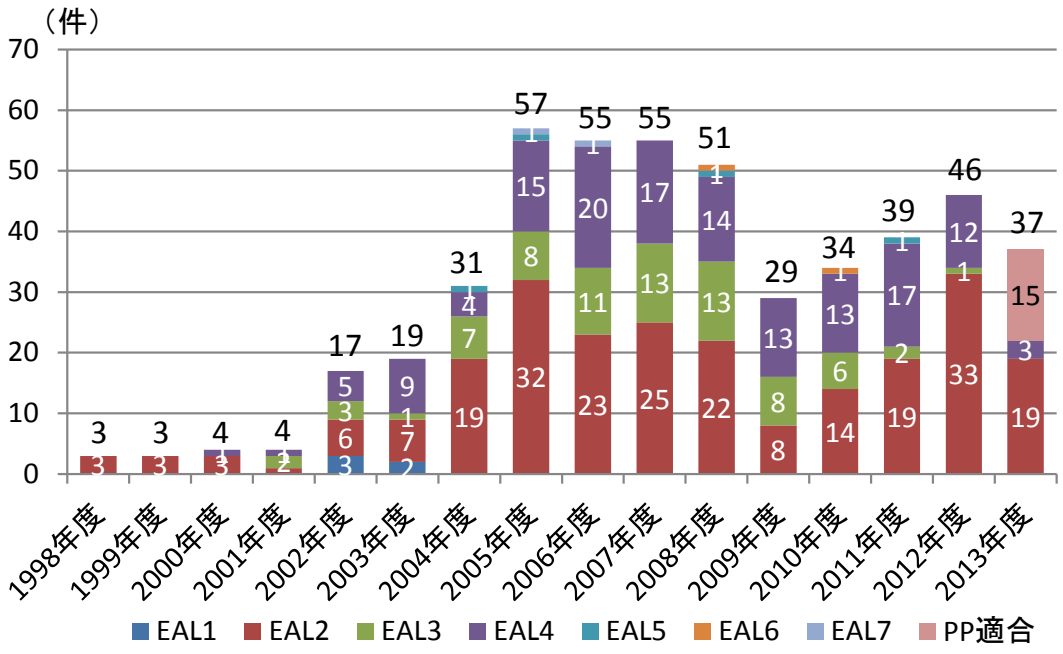


図 4-10 CC 認証取得製品数(米国・EAL 別) ※2014/8/7 時点

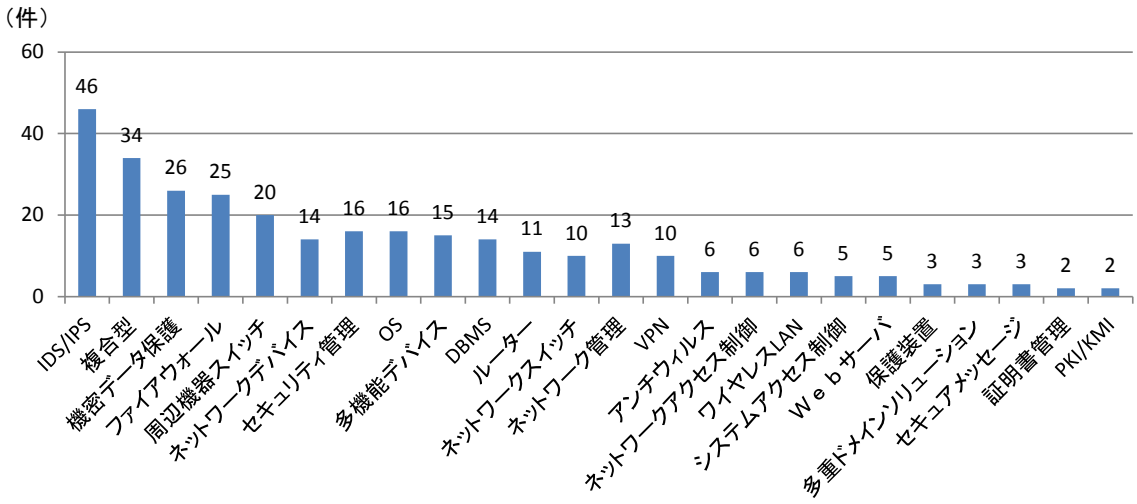


図 4-11 CC 認証取得製品数(米国・製品種別) ※2014/8/7 時点

4.2.3. イギリス

イギリスにおける 2013 年度までの CC 認証取得数は 89 件であり、うち EAL 4 が 47 件で最も多い(図 4-12)。2003 年度以降、5 件前後の定常的な認証件数で推移している。

製品種別でみると、ファイアウォール、OS、データベース、ネットワーク・通信機器等の取得製品が多い(図 4-13)。

イギリスでは、CC 認証制度の所管である CESG が暗号アルゴリズムから政府調達まで管轄している。

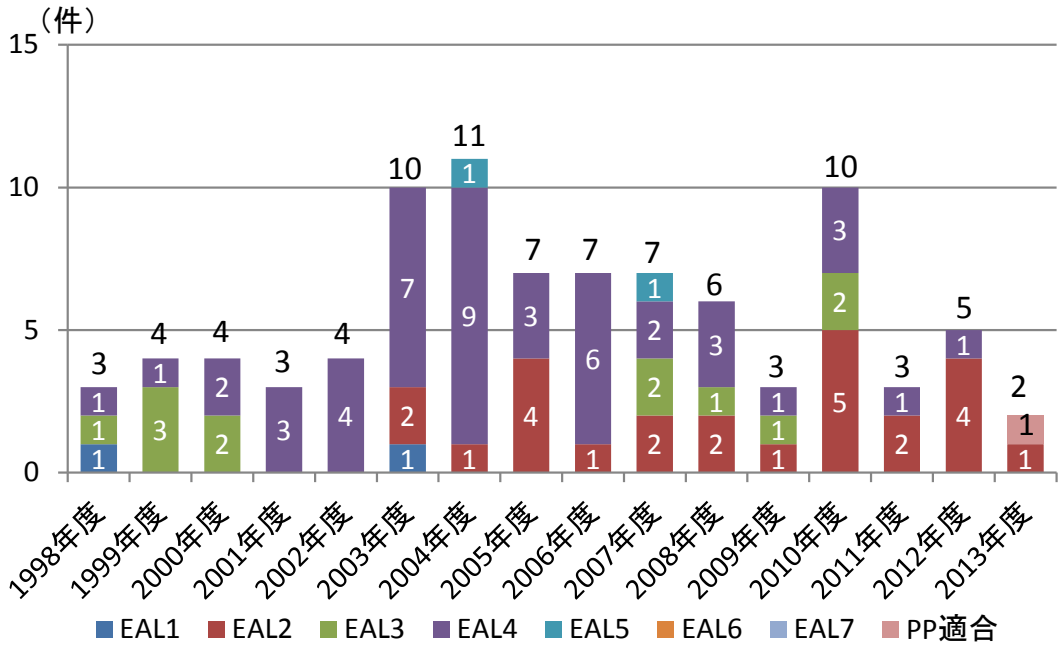


図 4-12 CC 認証取得製品数(イギリス・EAL 別) ※2014/8/7 時点

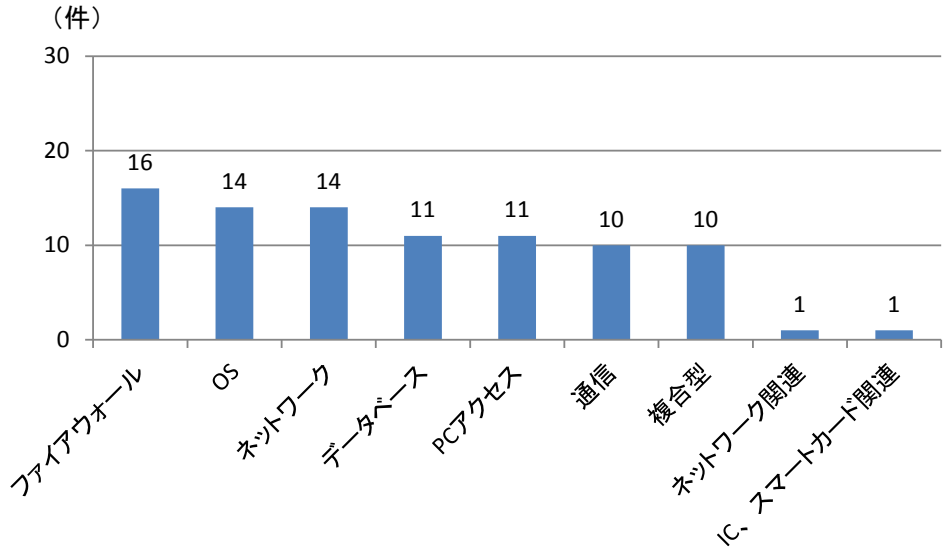


図 4-13 CC 認証取得製品数(イギリス・製品種別) ※2014/8/7 時点

4.2.4. フランス

フランスにおける 2013 年度までの CC 認証取得数は 442 件であり、うち EAL 4 が 231 件で最も多く、EAL 5 も 137 件、EAL 6 以上も 11 件と高レベルの認証取得製品が多い(図 4-14)。取得件数は順調に増加傾向にあり、評価機関が DCSSI から ANSSI に代わった 2009 年度に大きく増加、一時落ち着いたものの 2012 年度に再び大きく増加した。2013 年度の取得件数は 54 件で国別で最も多い。

製品種別でみると、スマートカードが 239 件で最も多く、次いで IC が 143 件であり、スマートカード及び IC で全体の 88%を占める(図 4-15)。スマートカードは EAL 4 以上の取得が主流であることから、国全体の取得数も EAL 4 が多くなっている。

フランスでは過去スマートカードのトップシェアであった企業があることなどから、実際に少数のトップベンダによる PP 適合した EAL 4、EAL 5 のスマートカードと IC に関する認証取得件数が多く全体の取得件数を上げている。また、IC チップにおける EAL6、スマートカード組み込みソフトウエアにおける EAL7 取得事例もみられる。さらに欧州では、スマートカードのチップセキュリティの評価・認証体制が構築されており、欧州 CC 認証機関やベンダ、ユーザが参加する ISCI (International smartcard certification initiative)で検討された評価方法が、ISCI 加盟各国の CC 認証制度で利用されていることが、スマートカードの認証件数が多い要因であるとも考えられる。

フランスでは、CC 認証より低コストな CSPN というフランス独自の認証制度が民間ニーズに対応して開発されているが、CSPN は CC 認証を取得する前段階としても導入できるように設計されている。政府の調達要件としては、ANSSI が規定する製品認証(CC 認証、CSPN 等)が要件化されており、CC 認証取得が広がることが予測される。

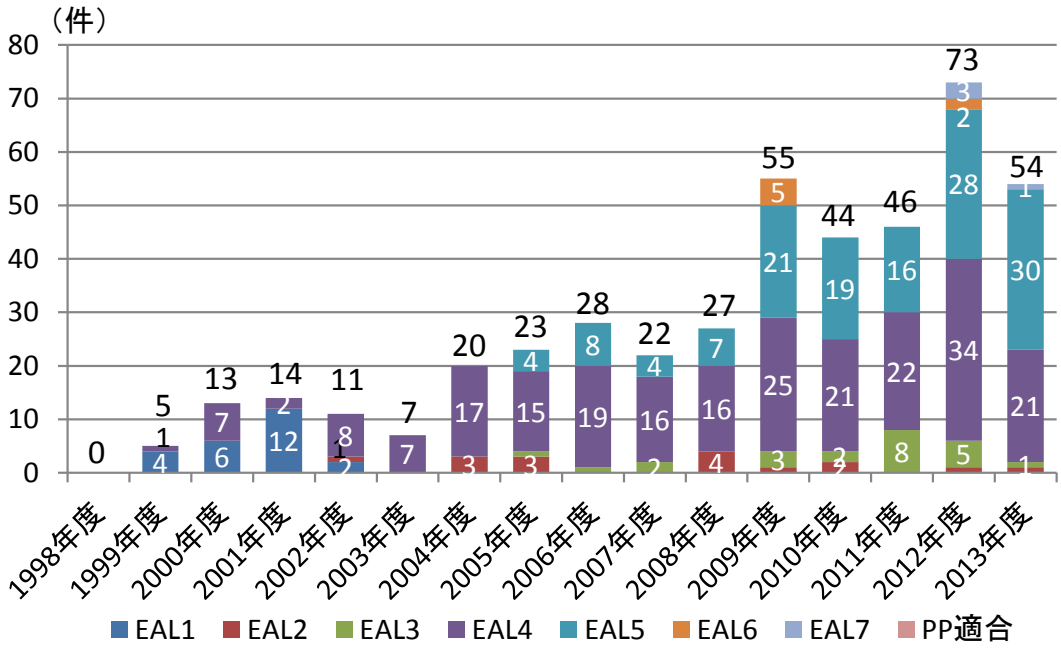


図 4-14 CC 認証取得製品数(フランス・EAL 別) ※2014/8/7 時点

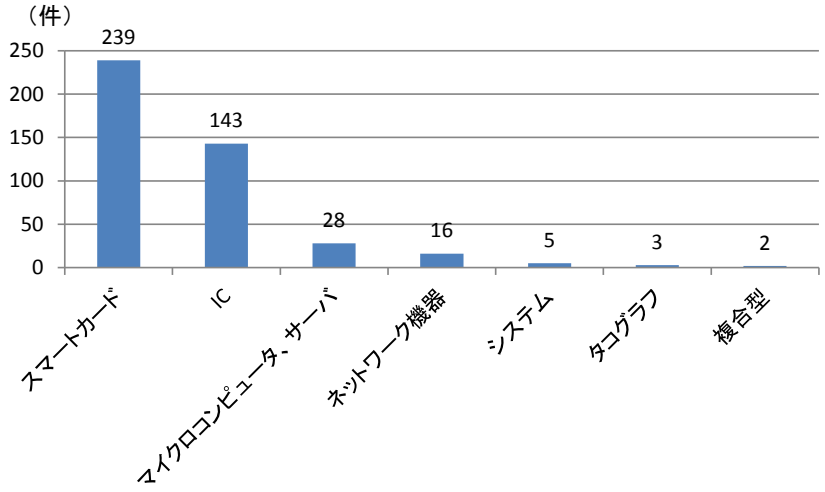


図 4-15 CC 認証取得製品数(フランス・製品種別) ※2014/8/7 時点

4.2.5. ドイツ

ドイツにおける 2013 年度までの CC 認証取得数は 529 件であり、うち EAL 4 が 276 件で最も多く、EAL 5 が 139 件、EAL 6 も 6 件ある(図 4-16) [166]。CC 認証制度は 2005 年頃

[166] German IT Security Certificates
https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html

までに立ち上がり、以降、毎年 50 件前後の認証件数で推移している。

製品種別でみると、スマートカードのコントローラー、公的ドキュメント、カードリーダー、電子医療カードを合わせ 300 件と多く、全体の 57%を占める(図 4-17)。

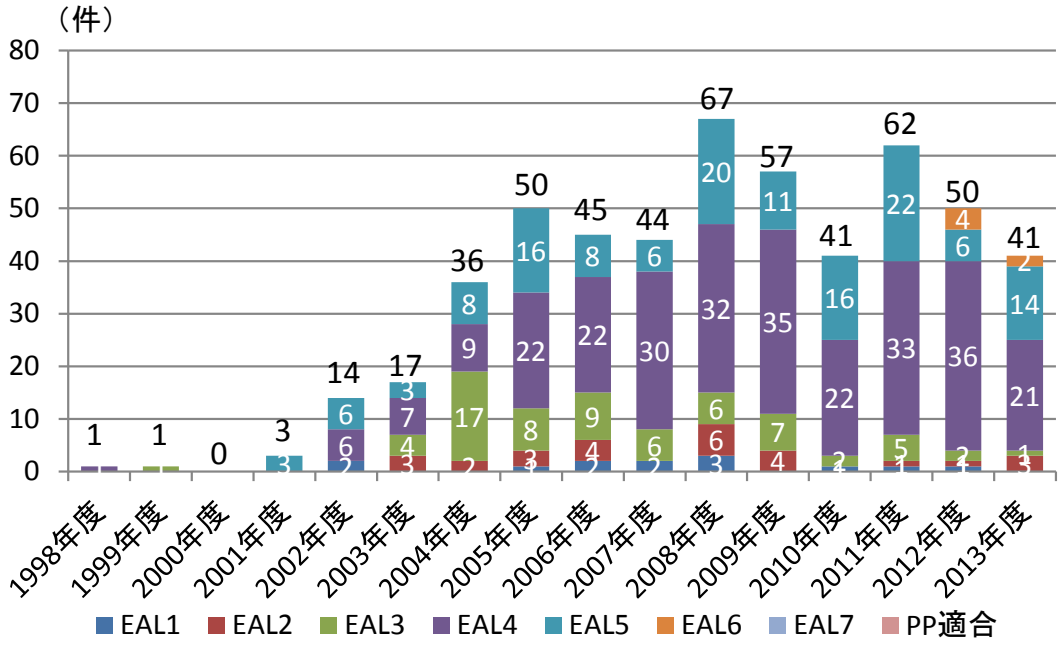


図 4-16 CC 認証取得製品数(ドイツ・EAL 別) ※2014/8/7 時点

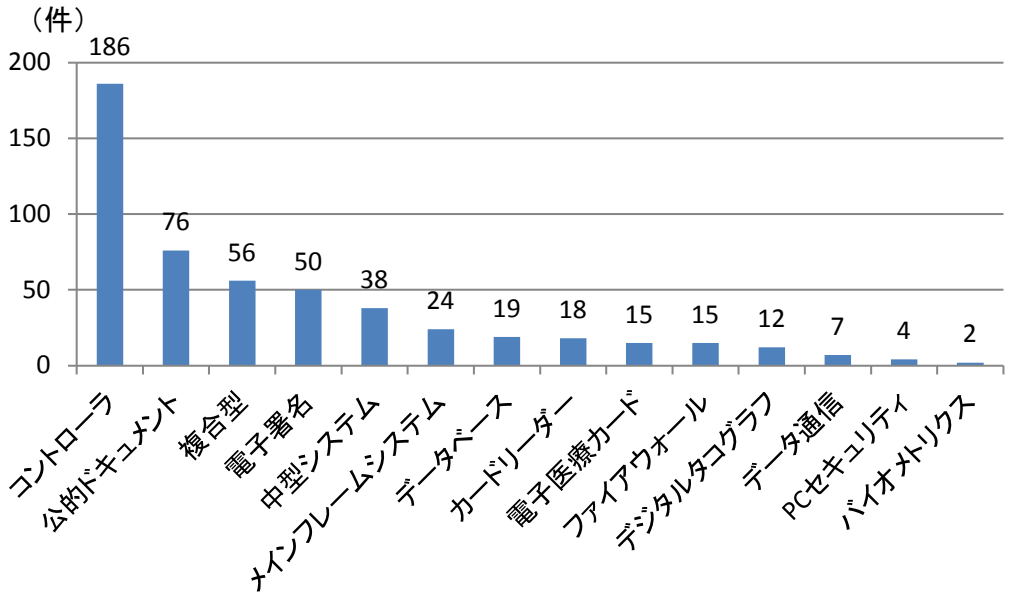


図 4-17 CC 認証取得製品数(ドイツ・製品種別) ※2014/8/7 時点

EAL 4、EAL 5 の認証製品はスマートカードに関するものが多く、申請者はスマートカード関連事業者が多い。スマートカードのセキュリティ評価では、BSI で認証された PP「BSI-PP-0035」が実質的な標準となっており、欧州で流通する多くのスマートカードがこの PP 適合認証を取得している。また、スマートカードは EAL 4 以上の取得が主流であることから、国全体の取得数も EAL 4 が多くなっている。

なお、政府調達は、CC 認証は義務化されていない。

4.2.6. 韓国

韓国における 2013 年度までの CC 認証取得数は 68 件であり、うち EAL 4 が 37 件で最も多い(図 4-18)。その他は、EAL 3 が 22 件、EAL 5 が 8 件で、EAL 3~5 内に収まっている。CCRA に加盟した 2006 年度から 3 年連続で 10 件を超える取得があり、その後年平均 7 件前後で推移している。

製品種別でみると、e-Passport COS、デジタル複合機、IPS が多い(図 4-19)。

韓国政府行政機関における電子文書の保安機能や適合性の規格を定めるのは NIS であり、その下の ITSCC が KECS (いわゆる CC 認証)の認証機関となっているが、CC 認証は政府調達において義務付けられていない。

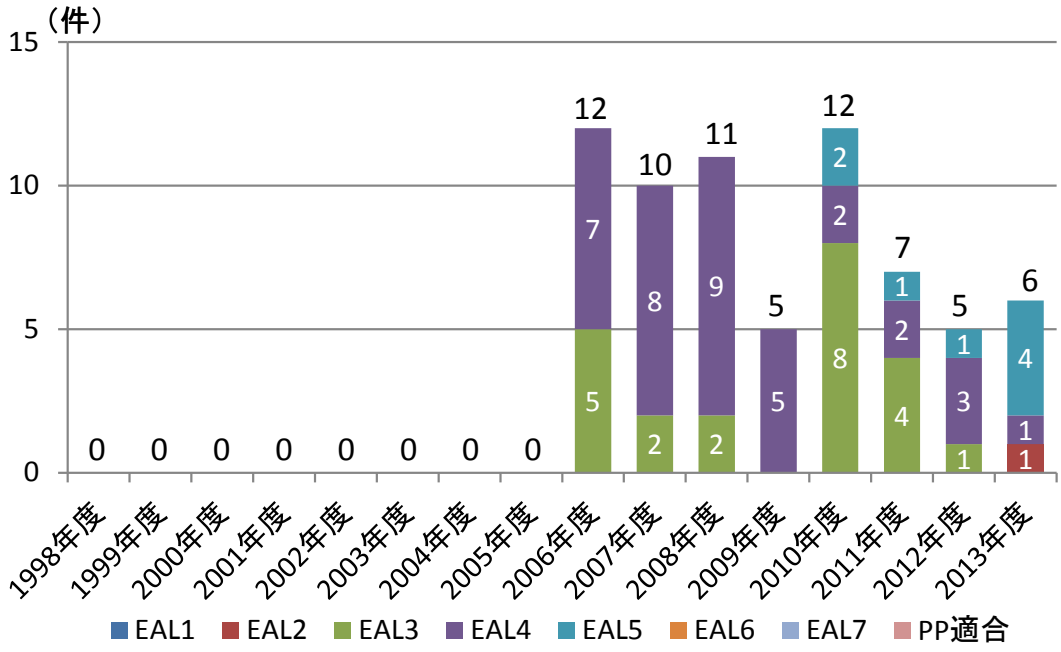


図 4-18 CC 認証取得製品数(韓国・EAL 別) ※2014/8/7 時点

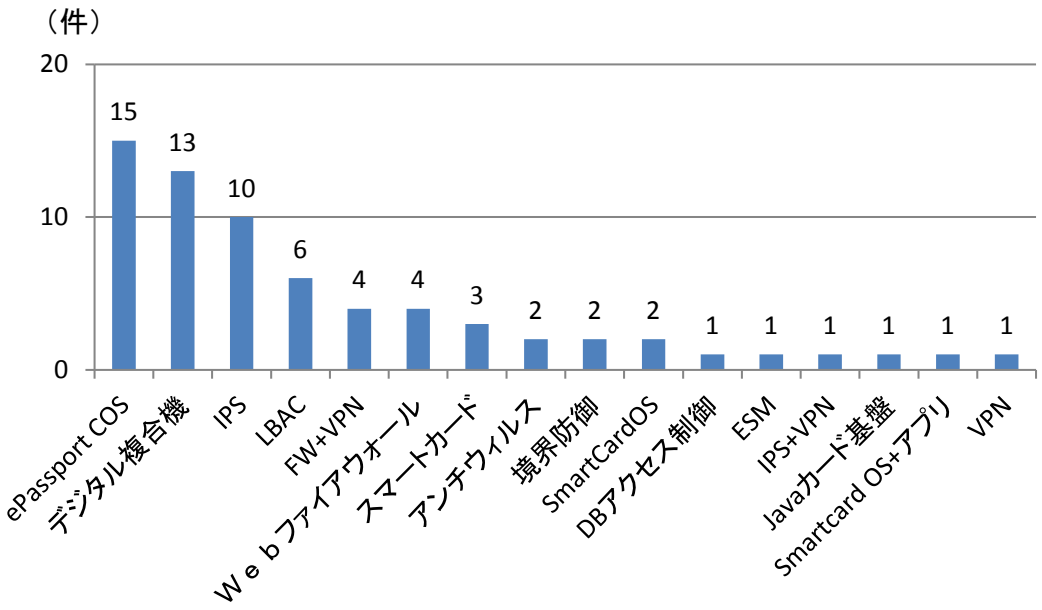


図 4-19 CC 認証取得製品数(韓国・製品種別) ※2014/8/7 時点

4.2.7. オーストラリア

オーストラリアにおける 2013 年度までの CC 認証取得数は 63 件であり、うち EAL 4 が 25 件で最も多く、EAL 2 も 20 件と多い(図 4-20)。取得件数は全体的には横ばいだが、2009 年度が大幅増となっている。また、2009 年度、2012 年度は特に EAL 4 以上の取得件数が増加しているが、2009 年度はモバイル製品やモバイルデバイス管理、2012 年度はアクセスコントロールやネットワーク関連システムでの EAL 4 の取得が多かった。

製品種別でみると、ネットワークが 29 件で最も多い(図 4-21)。

なお、暗号に係わるセキュリティ認証制度 AISEP (Australasian Information Security Evaluation Program)は、CC 認証に準拠しつつ追加の要件を含んでおり、政府システムに対しては AISEP が義務づけられており、2013 年度までの認証件数は 118 件である

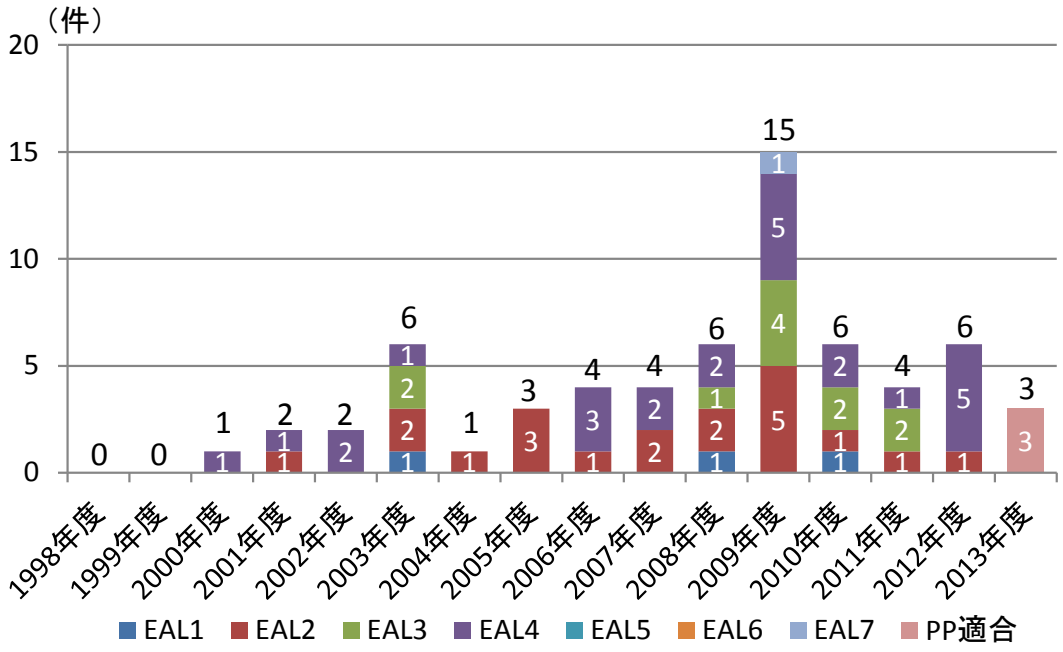


図 4-20 CC 認証取得製品数(オーストラリア・EAL 別) ※2014/8/7 時点

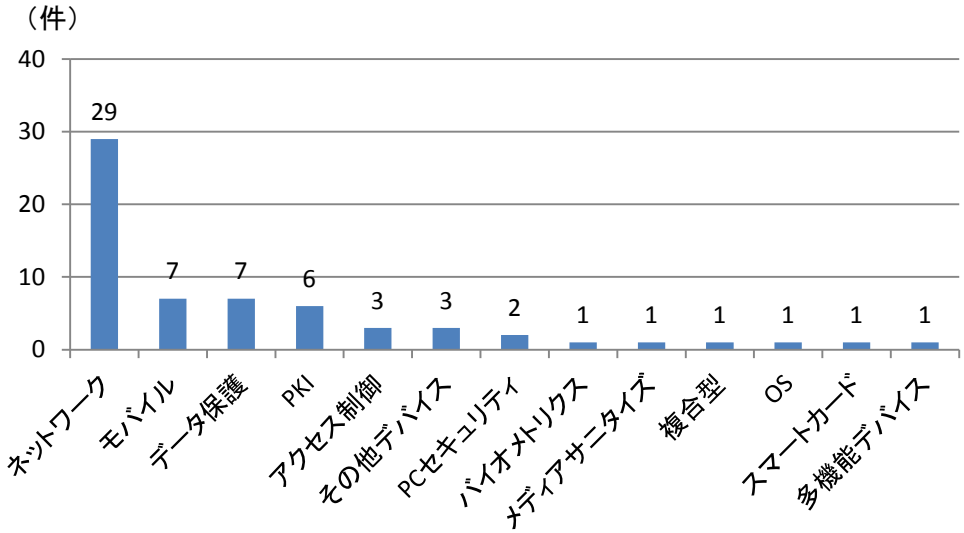


図 4-21 CC 認証取得製品数(オーストラリア・製品種別) ※2014/8/7 時点

4.2.8. その他の国々

4.2.1. ～4.2.7. 章で記載した以外の国々の EAL 別 CC 認証取得製品を図 4-22～図 4-29 に示す。

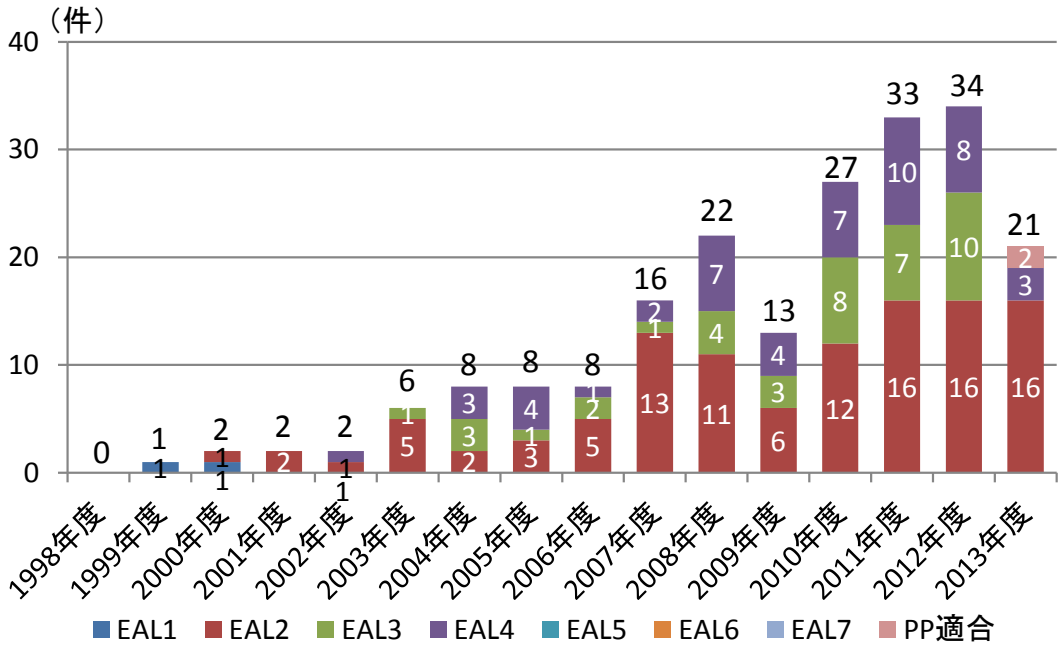


図 4-22 CC 認証取得製品数(カナダ・EAL 別) ※2014/8/7 時点

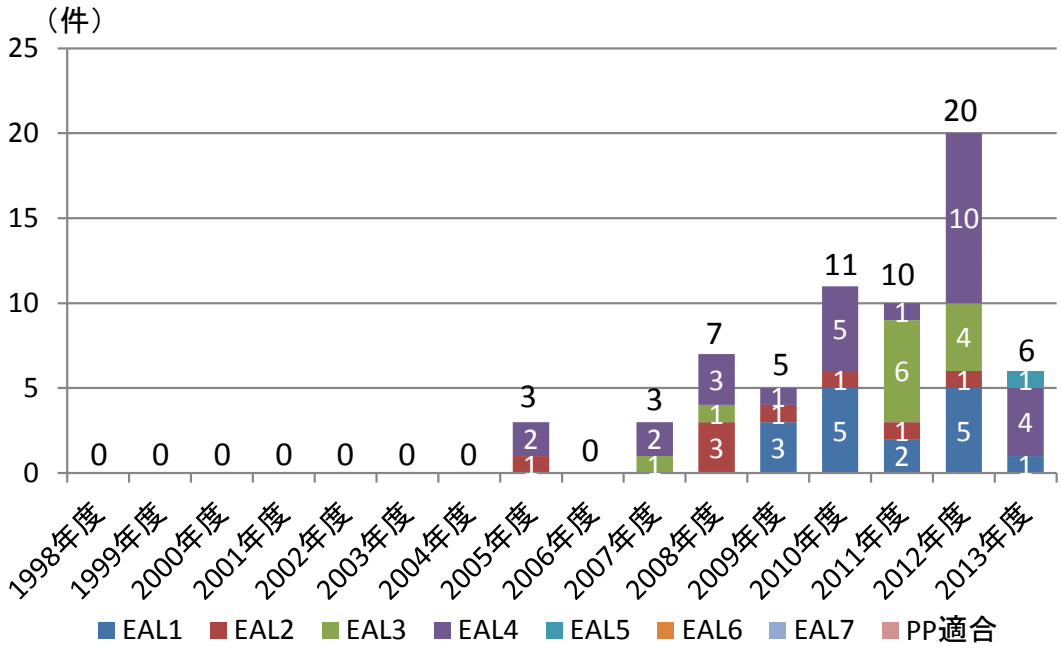


図 4-23 CC 認証取得製品数(スペイン・EAL 別) ※2014/8/7 時点

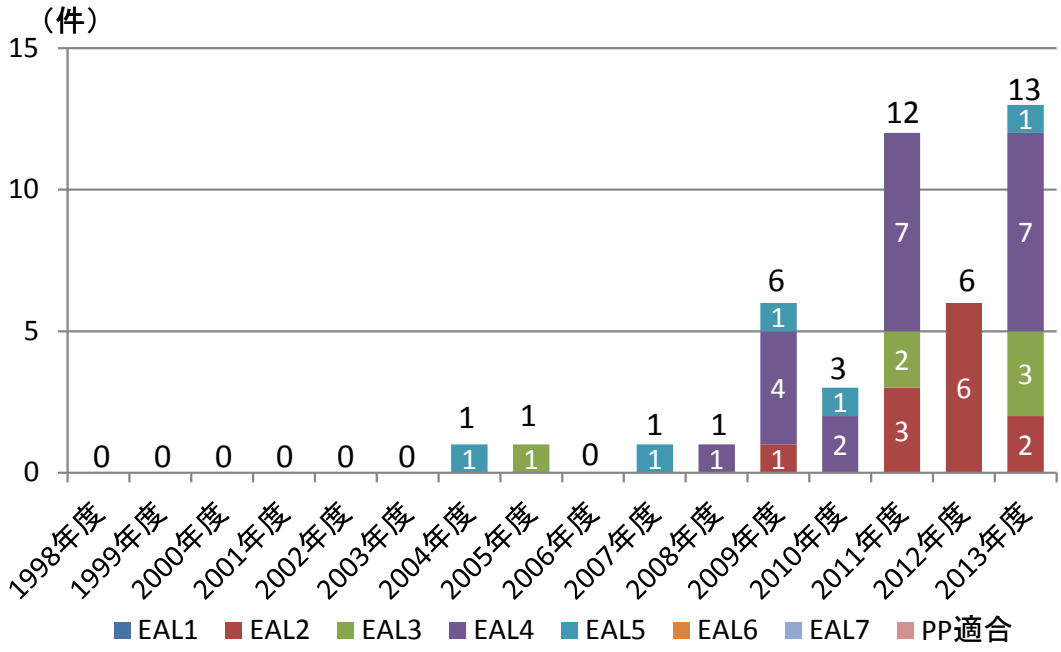


図 4-24 CC 認証取得製品数(ノルウェー・EAL 別) ※2014/8/7 時点

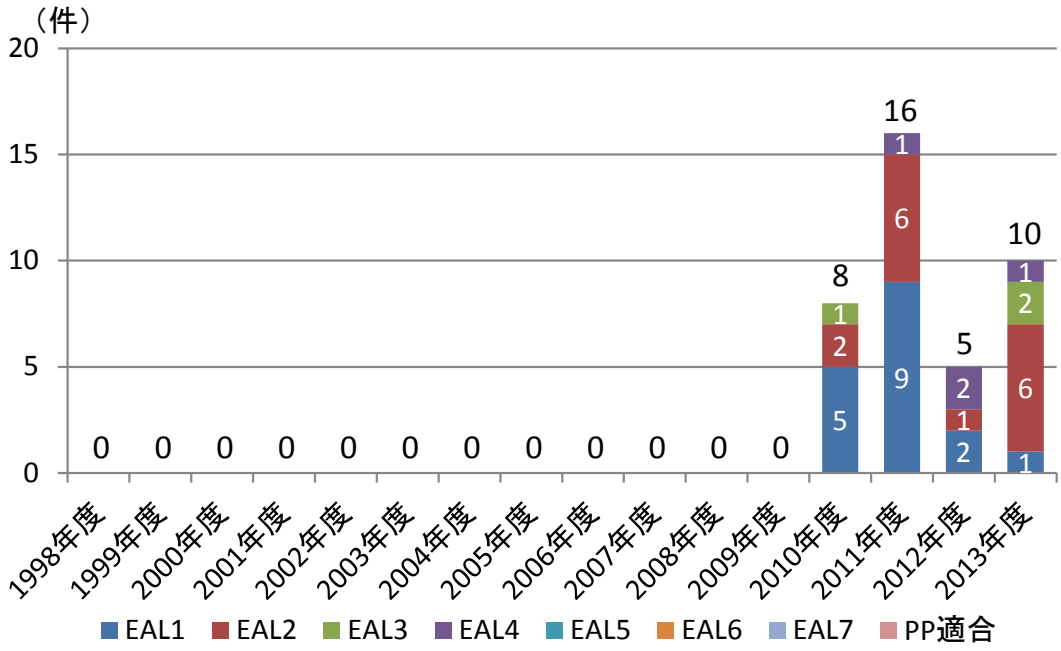


図 4-25 CC 認証取得製品数(マレーシア・EAL 別) ※2014/8/7 時点

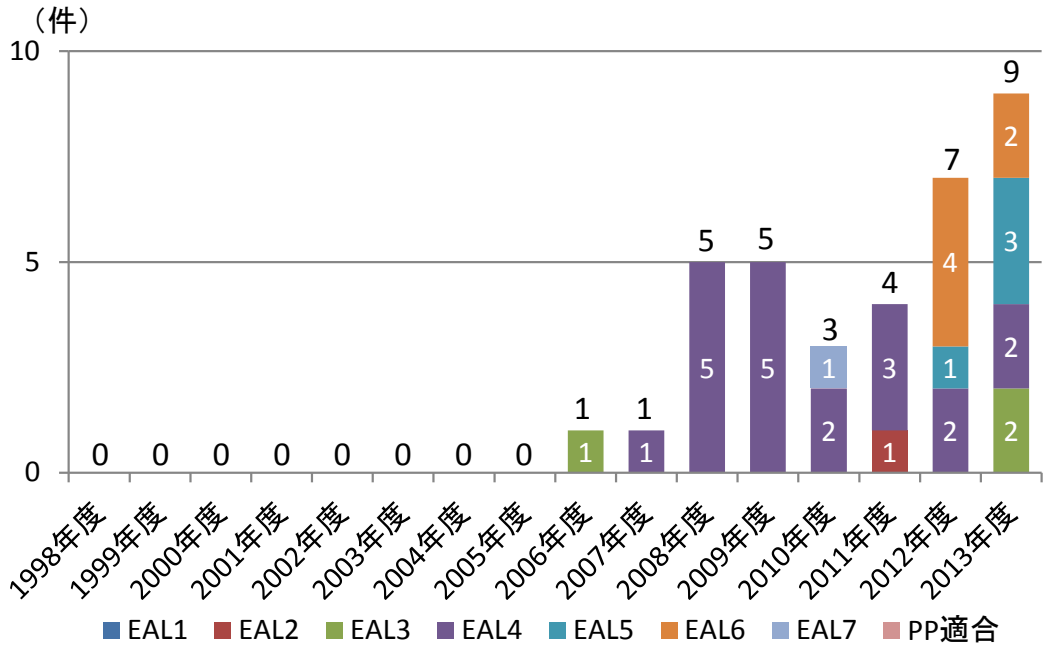


図 4-26 CC 認証取得製品数(オランダ・EAL 別) ※2014/8/7 時点

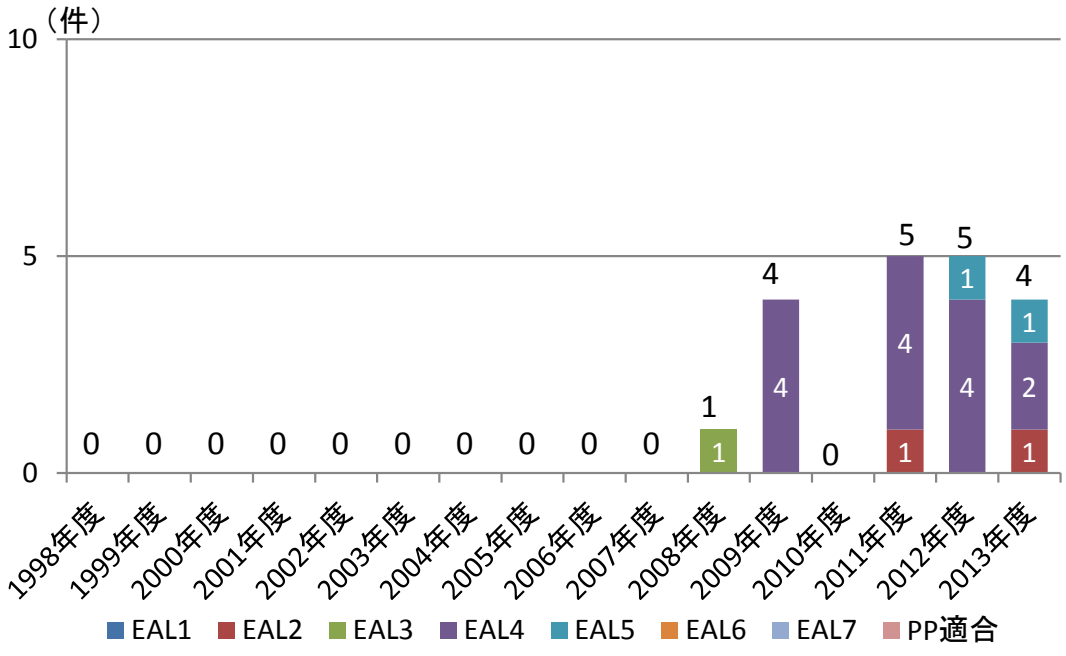


図 4-27 CC 認証取得製品数(トルコ・EAL 別) ※2014/8/7 時点

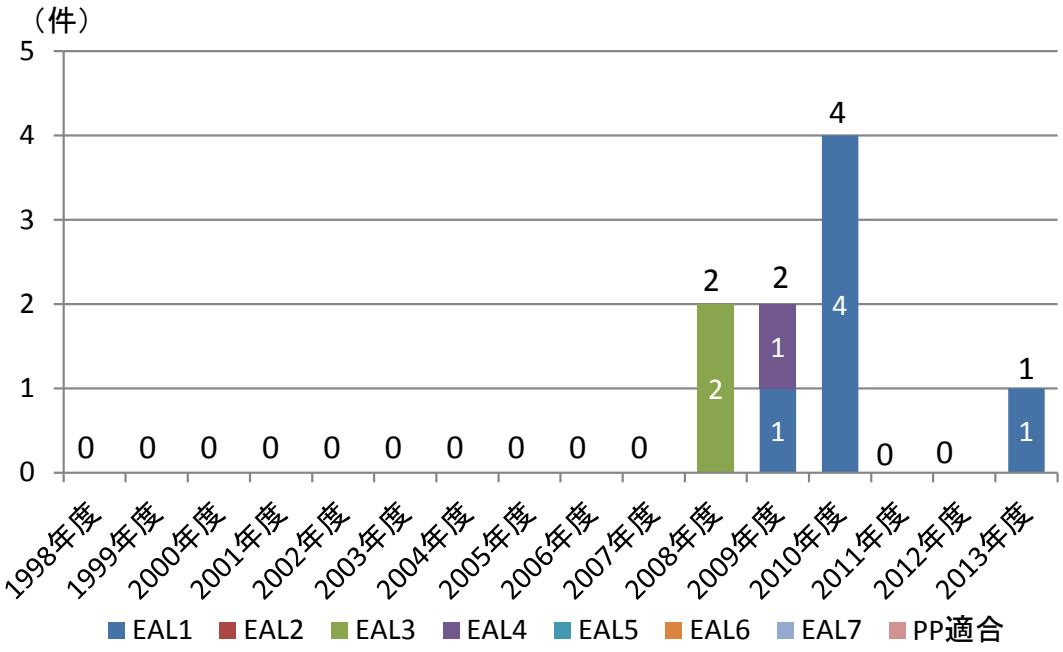


図 4-28 CC 認証取得製品数(イタリア・EAL 別) ※2014/8/7 時点

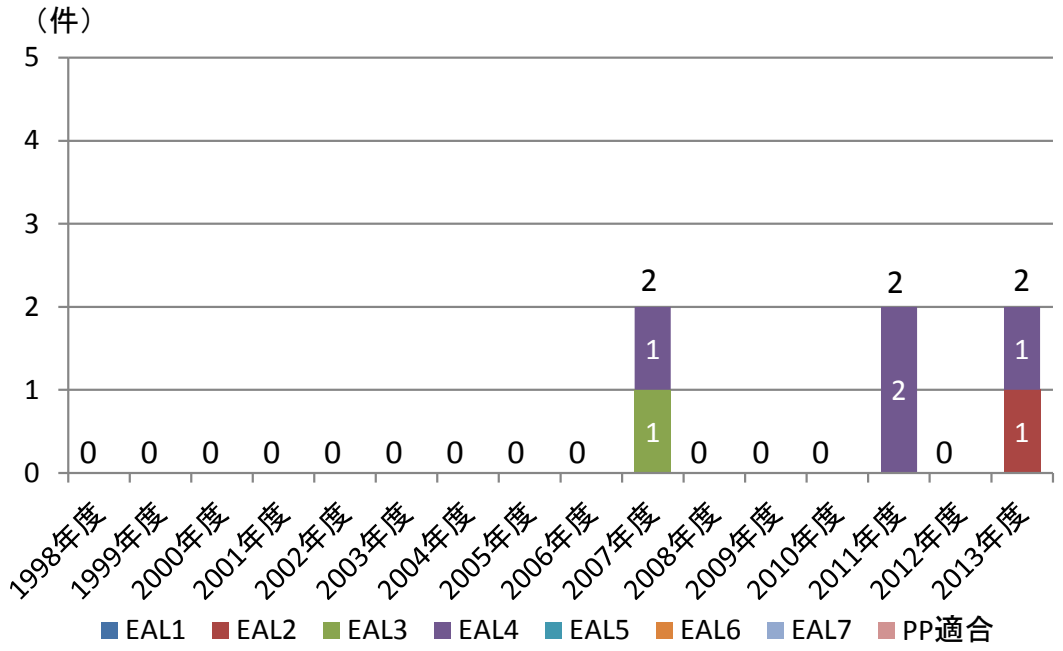


図 4-29 CC 認証取得製品数(スウェーデン・EAL 別) ※2014/8/7 時点

4.3. CCRA 新アレンジメント

2014 年 9 月 8 日付で CCRA 新アレンジメントが発行した。

これは、CCRA 加盟国での政府調達において、CC 評価を最大限に活用するための改訂であり、調達される IT 製品のセキュリティ要件(cPP; Collaborative Protection Profile)を製品ベンダ、評価機関が中心となった国際的な技術者集団(iTC)が共同で開発する。具体的には、政府調達で考慮されるセキュリティ要件を共通の cPP として開発し、各国が共通の cPP に基づいて製品評価を行うこととし、最長 3 年間(2017 年 9 月 8 日以内)の移行期間[167]をおいて、cPP に適合する IT 製品の評価結果が新しい CCRA での相互承認対象となる。

CCRA 新アレンジメントが作られた背景には、

① 各国が独自に PP (Protection Profile)を作成するため、結果として、ベンダは国ごとに別の PP 適合評価が求められた。
② PP が製品分野ごとに作られているため、複数の製品分野で共通の技術基盤についても別々の PP でセキュリティ要件が定められる。このため、要求されるセキュリティレベルにばらつきがある。
③ 政府調達において、EAL4 での評価を求めるケースが多く、評価に時間がかかり、タイムリーな調達ができない。
④ ベンダ独自の ST (Security Target)に基づく評価を認めているため、適切なセキュリティ機能がなくても評価認証が行われてしまう。

といった課題があった。これらの課題を踏まえ、CCRA 新アレンジメントでは、技術分野ごとに cPP を作成して共通基盤となる技術のセキュリティレベルの統一を図るとともに、複数の国の政府調達で利用できるように、原則ミニマム要件として規定する。

また、PP では暗号に関する評価は規定されていなかったのに対して、cPP では暗号に関するテスト方法が規定された。

現在、以下の cPP の開発が進んでいる。

- USB Portable Storage Device cPP
- Network Devices / Firewalls cPP
- Full Drive Encryption cPP

また、cPP 開発の先駆けとして

- Multifunction Printers PP

の開発も進んでいる。

[167] 移行期間中は従来の CC 認証も相互承認対象であるが、移行期間終了後は EAL1 または EAL2 の CC 認証のみに制限される

5. 国内暗号製品市場に係る動向調査

本章では、暗号と産業競争力の関連性を見る観点から、具体的には、暗号ライブラリ、暗号製品、セキュリティ製品の 3 つの国内市場に分けてそれぞれの市場規模の経年推移について示す。

5.1. 市場規模の経年推移

5.1.1. 市場分類

セキュリティ製品の市場は表 5-1 に示す製品カテゴリとする。そのうち、★印は暗号機能を主とする製品(暗号製品)にも該当する製品カテゴリである。

表 5-1 セキュリティ製品市場に該当する製品カテゴリ

ワンタイムパスワード	Web フィルタリングツール
デバイス認証ツール	メールフィルタリング
認証デバイス(IC カード、USB トークン、バイオメトリクス)	★メール暗号化(暗号機能、誤送信防止)
シングルサインオン	電子メールセキュリティアプライアンス
★PKI 関連製品	電子メールアーカイブ
統合 ID 管理ツール	Web セキュリティアプライアンス
特権ユーザ管理ツール	Web アプリケーションファイアウォール
検疫ツール(トークン、不正接続防止、検疫ツール)	データベースセキュリティ製品
フォレンジックツール	端末管理・セキュリティツール (IT 資産管理、端末操作ログ収集、持出制御、★ファイル暗号化 、★ディスク暗号化)
統合ログ管理ツール	★DRM
シンクライアント	DLP
ファイアウォール/VPN/UTM 関連製品	USB メモリセキュリティ
DDoS 対策ツール	モバイルウイルス対策
ウイルス対策ツール	モバイルフィルタリングツール
標的型対策ツール	★モバイル暗号化ツール
	★暗号ライブラリ(2010 年まで)

暗号製品市場は表 2-1 に示す製品カテゴリとする。

暗号ライブラリ市場は表 5-2 に示す製品カテゴリのなかの「暗号ライブラリ」のみを対象とする。

表 5-2 暗号製品市場に該当する製品カテゴリ

PKI 関連製品	DRM
メール暗号化(暗号機能、誤送信防止)	モバイル暗号化ツール
端末管理・セキュリティツール（ファイル暗号化 、ディスク暗号化)	暗号ライブラリ(2010 年まで)

5.1.2. セキュリティ製品市場

2013 年のセキュリティ製品市場規模は約 3,000 億円に達する。

セキュリティ製品市場は、図 5-1 に示すように、1999 年以降、インターネットの普及に伴い拡大し、2000 年代前半にワーム感染事例の多発や情報漏えい、Web サイトの改竄といったサイバーセキュリティインシデントが発生したこと、またセキュリティ関係法制度(個人情報保護法の全面施行、e-文書法の施行等)の動き出し(表 5-3)により企業や組織における情報セキュリティ関連製品の導入が進んだ。2008 年までは拡大してきたが、リーマンショックを機に一時縮小した。しかし、ここ数年は景気の好転による IT 投資の拡大と、サイバー攻撃の深刻化、そしてスマートデバイスの普及を背景に、再びセキュリティ製品市場が拡大しつつある。

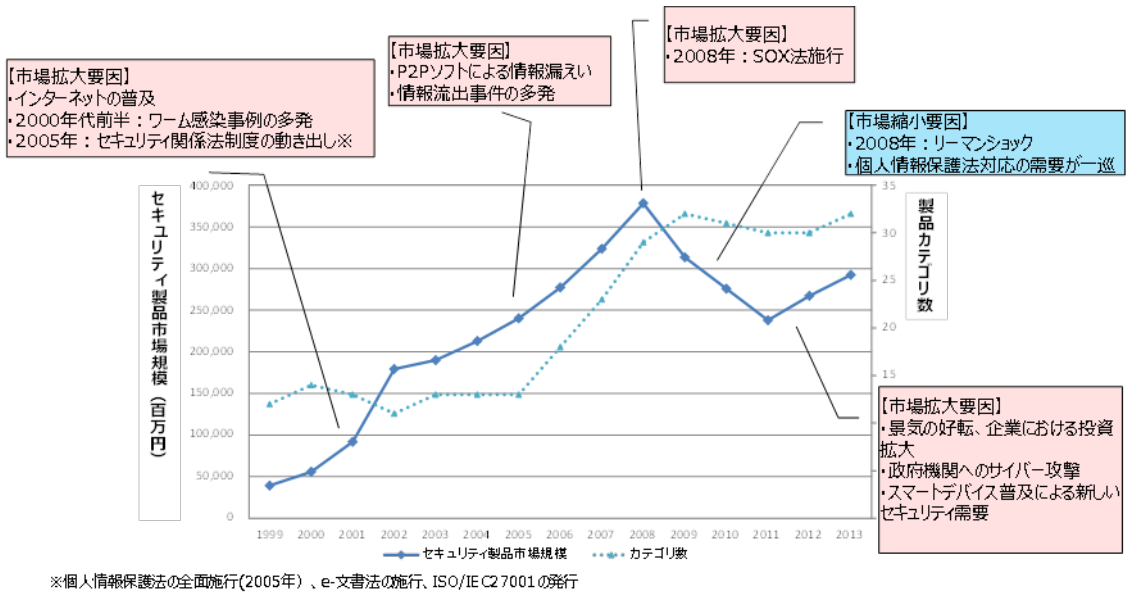


図 5-1 セキュリティ製品市場の推移(1999 年～2013 年)[168]

[168] 富士キメラ総研「ネットワークセキュリティビジネス調査総覧」(1999 年～2013 年)
なお、物理セキュリティ製品市場は除外した数値である。

表 5-3 セキュリティ製品市場へ影響するイベント

年代	(年)	イベント
～1999 年		インターネットの普及
	(1999 年)	不正アクセス禁止法
2000 年代前半		ワーム(LOVELETTER、Nimda、Slammer 等)感染事例の多発
		P2P ソフトによる情報漏えい
	(2000 年)	中央省庁の Web 改竄
	(2001 年)	電子署名法施行
		IT 書面一括法施行
		電子消費者契約法施行
		IT 基本法施行
	(2002 年)	ISMS 適合評価制度開始
	(2003 年)	IT 投資促進税制施行
		電子政府推奨暗号リスト公表
		情報セキュリティ監査制度　運用開始
		住民基本台帳ネットワーク本格稼働
	(2004 年)	脆弱性取扱に関する告示
		迷惑メール問題
2000 年代後半		企業による情報流出事故の多発
		e-コマースの加速
		SNS の登場と流行
	(2005 年)	個人情報保護法の全面施行
		e-文書法の施行
		ISO/IEC27001 の発行
	(2008 年)	リーマンショックによる景気の落ち込み
		日本版 SOX 法施行
		個人情報保護法対応の需要一巡
	(2009 年)	総務省が違法コピー対策徹底を各都道府県へ要請
		地域 ICT 利用高度化基盤強化税制
2010 年代		スマートデバイスの普及
		不正送金の増加
		政府機関や金融機関への大規模サイバー攻撃
		標的型攻撃の増加
	(2010 年)	制御システムへの攻撃
		Andoroid 初のボット型ウイルス
	(2011 年)	東日本大震災による景気の落ち込み
		サイバー刑法施行
	(2013 年)	中小企業情報基盤強化税
		中小企業投資促進税制
		電子政府推奨暗号リスト改定

5.1.3. 暗号製品市場

セキュリティ製品のうち、暗号を主たる機能とする製品(「ファイル暗号化・ディスク暗号化ツール」「メール暗号化／メール誤送信対策ツール」「モバイル暗号化ツール」「PKI 関連製品」「DRM」)と限定すると、2013 年の暗号製品市場規模は約 1,150 億円である。

暗号製品市場においては、図 5-2　暗号製品市場の推移(1999 年～2013 年)に示すように、セキュリティ製品市場と同様、1999 年以降順調に拡大し、2008 年をピークに縮小した。その後、セキュリティ製品市場が 2011 年を底に再び上昇傾向にあるのに対し、暗号製品市場は 2011 年以降も若干の縮小傾向にある。セキュリティ製品市場に占める暗号製品市場の割合をみると、1999 年～2001 年にかけて減少し、以降は 5%前後で推移したものの、ここ数年は再び減少に転じている。

1999 年から暗号製品市場の割合が低下したのは、ファイアウォールやワーム感染防止、ウイルス対策ソフト等、ネットワークセキュリティ製品の市場が拡大したことによる相対的な割合の縮小が理由である。その後、個人情報保護法の施行が企業の情報保護意識を高め、さらに J-SOX による監査の実施が暗号製品市場に影響を与え、暗号製品市場の割合はやや回復し、5%前後を維持していた。2010 年からの暗号製品市場規模、市場割合がともに減少傾向にあるのは、暗号ライブラリが集計対象から外れた影響のほか、セキュリティ製品やクラウドサービスなどで暗号機能が標準装備として提供されるようになり、暗号製品を追加で導入する必要性が薄れてきているためと推測される。

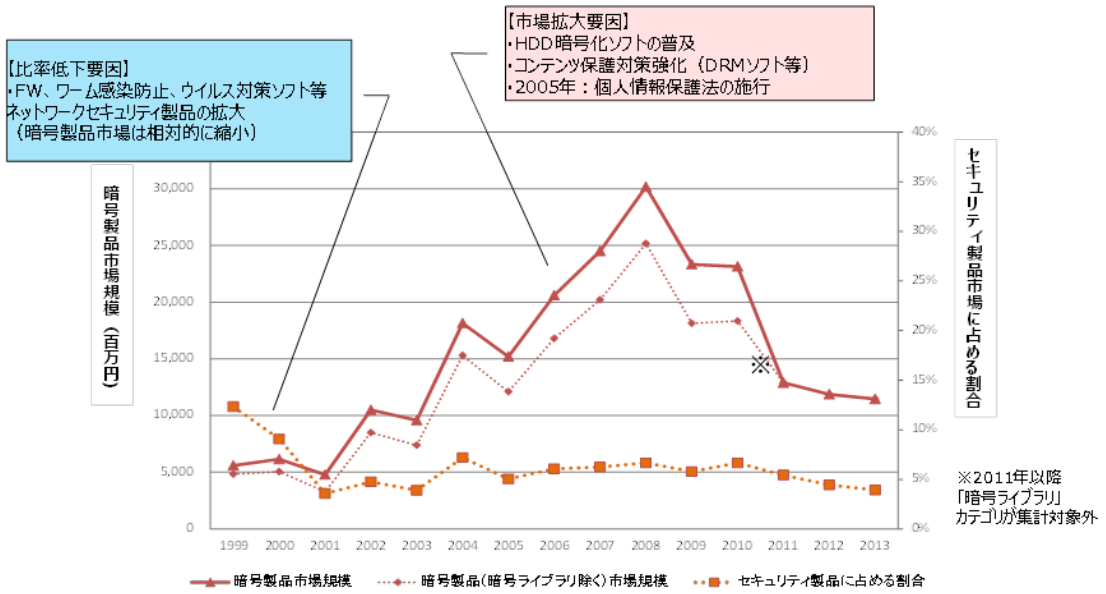


図 5-2　暗号製品市場の推移(1999 年～2013 年)[169]

[169] 富士キメラ総研「ネットワークセキュリティビジネス調査総覧」(1999 年～2013 年)

5.1.4. 暗号ライブラリ市場

暗号ライブラリは、主にアプリケーションや機器へ暗号機能を組み込む際に用いるソフトウェア製品であり、1999 年～2009 年まで単調増加傾向にあった（図 5-3）。しかし、暗号ライブラリ市場はトップ企業が圧倒的なシェアを持つ事実上の独占市場であるうえ、ゲーム機やプリンタ等の特定用途向けや組込み型が多い等の理由から、市場変動要因が少なく、2011 年以降は市場推計データが存在していない。

また、OS やスマートデバイスのアプリケーションの暗号機能の搭載が進み、ユーザは意識せずに暗号機能を利用する機会が増加しているものの、暗号ライブラリ単体の市場規模の拡大という形には表れない。例えば、OpenSSL のようにオープンソースでの暗号利用も広く普及しており、市場規模としては表れない部分で、暗号機能が広く利用されている実態もある。

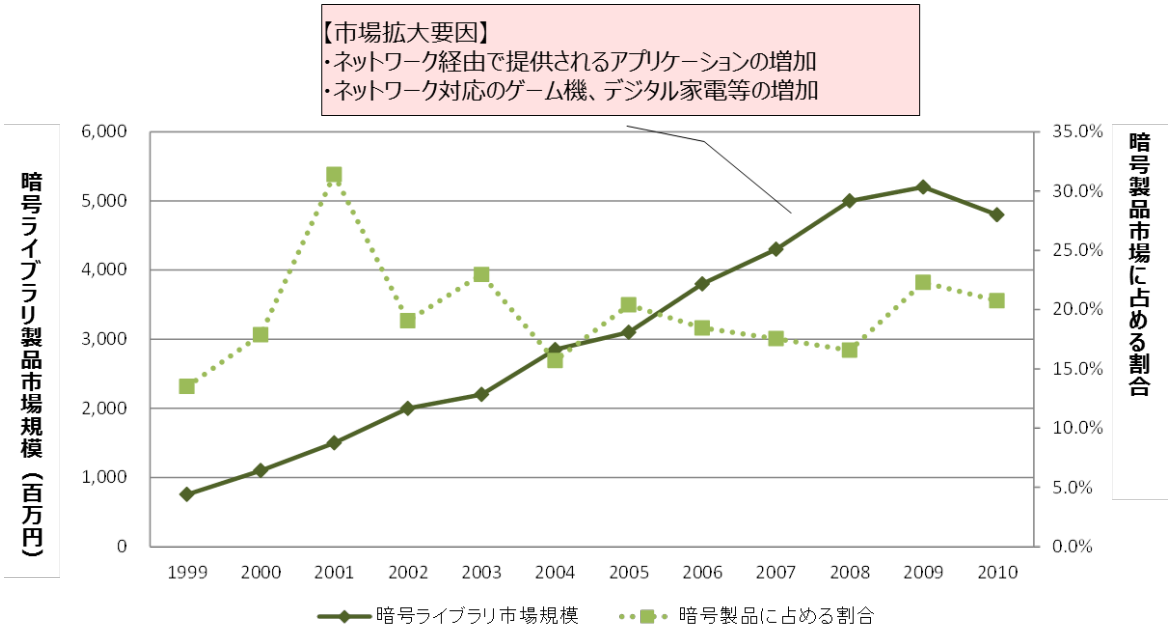


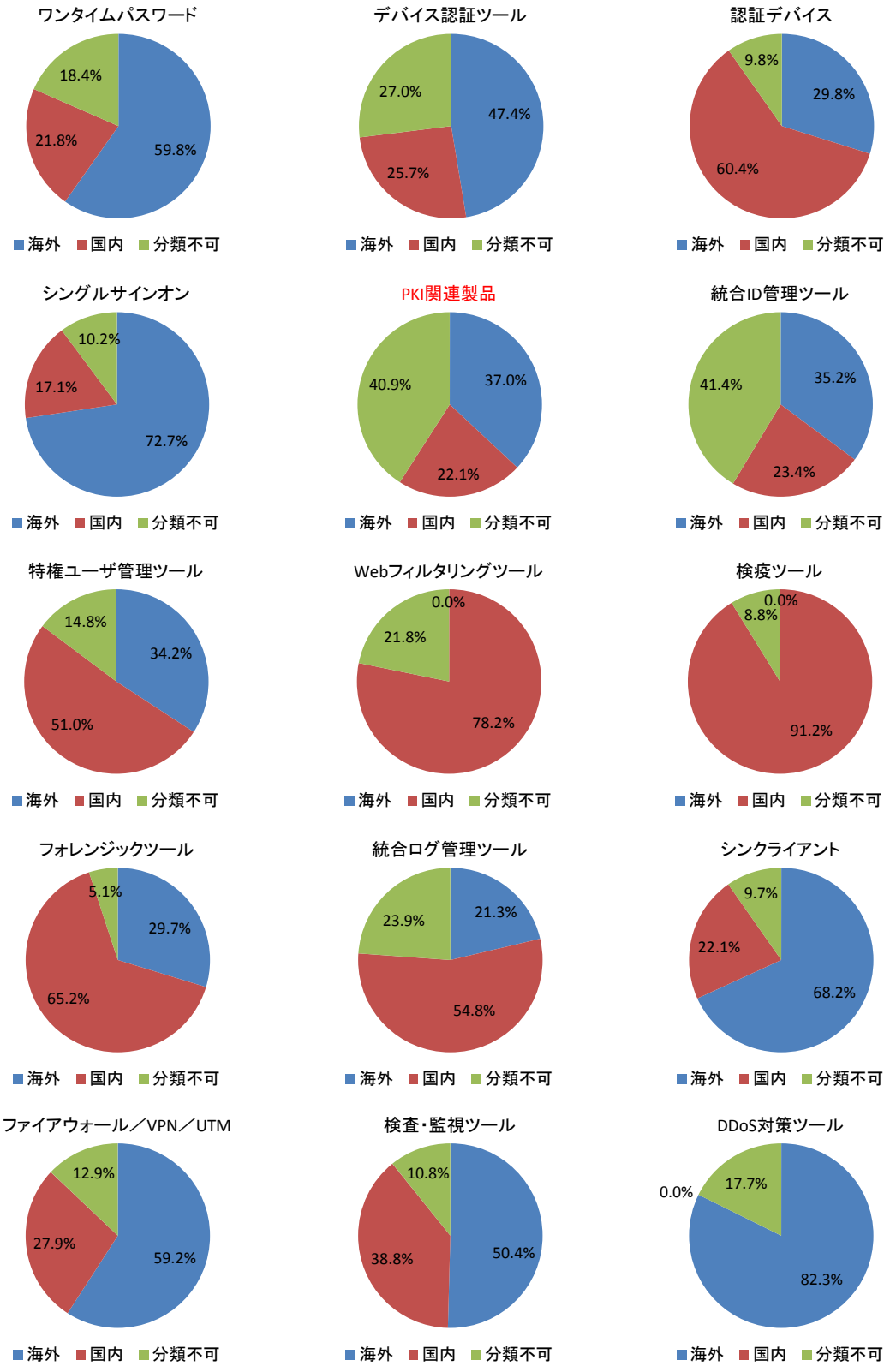
図 5-3 暗号ライブラリ市場の推移(1999 年～2010 年)[170]

5.2. セキュリティ製品ベンダから見る国内セキュリティ製品市場

5.2.1. セキュリティ製品市場における国内・海外ベンダ別のシェア

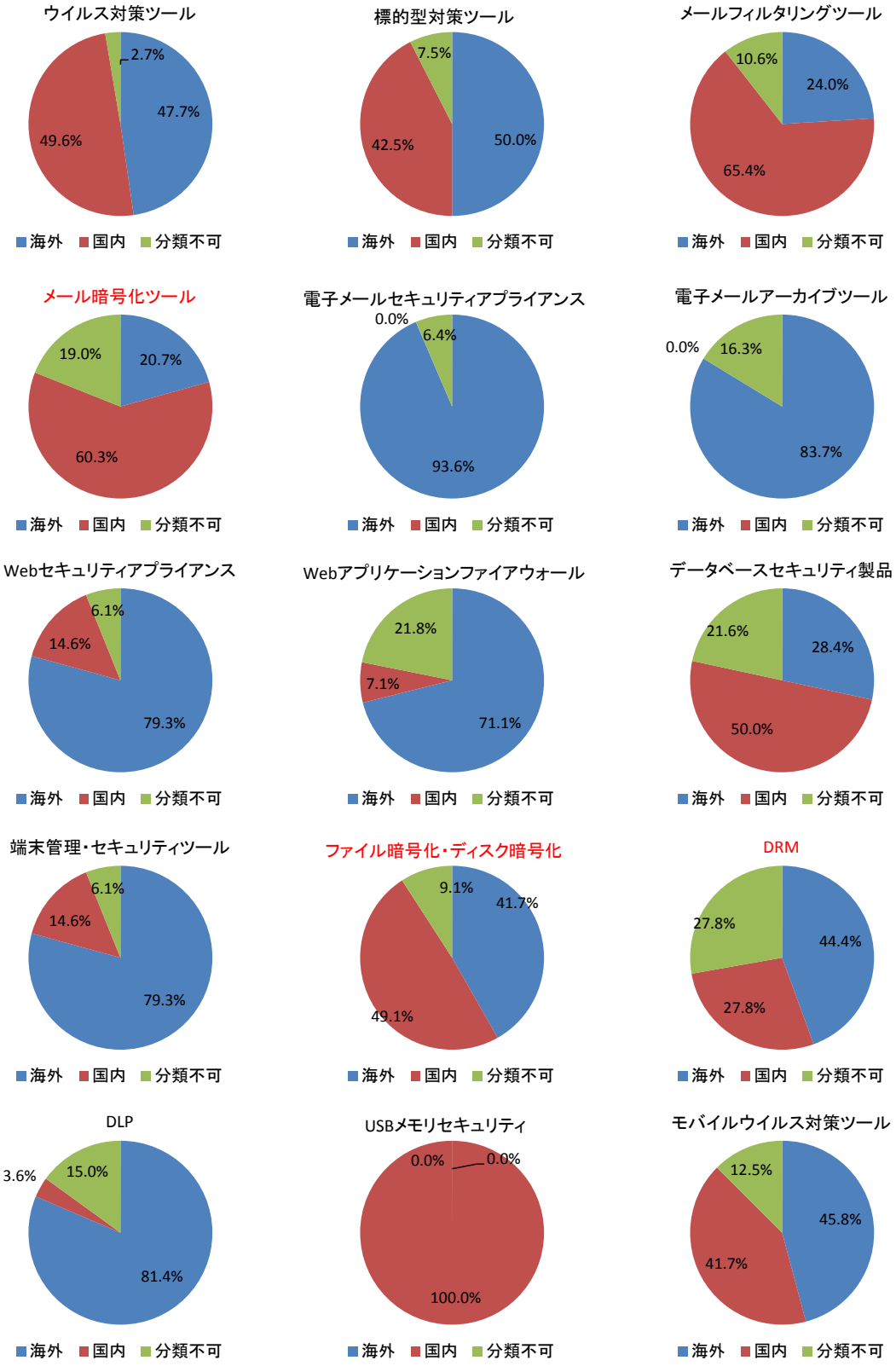
2013 年のセキュリティ製品市場の製品カテゴリ毎の国内ベンダ・海外ベンダ別のシェアは図 5-4 の通りである。

[170] 富士キメラ総研「ネットワークセキュリティビジネス調査総覧」（1999 年～2013 年）



注：「分類不可」は元データにおいて売上が小さく「その他」に分類されるもの

図 5-4 情報セキュリティ製品市場における国内・海外ベンダ別シェア(1)



注：「分類不可」は元データにおいて売上が小さく「その他」に分類されるもの

図 5-5 情報セキュリティ製品市場における国内・海外ベンダ別シェア(2)

富士キメラ総研「ネットワークセキュリティビジネス調査総覧 2013」で示された製品カテゴリ毎に示された上位ベンダの金額シェアを、本調査において国内・海外別に分類した。国内・海外の別は、企業設立が国内か海外かで分類しており、海外企業の日本法人・日本支社は海外に分類している。

全体でみると、電子メールセキュリティ製品、Web セキュリティ関連製品等、外部脅威に対するセキュリティ対策に関するカテゴリでは、海外ベンダの製品市場が大きい。一方、メール・Web フィルタリングツール等、主にコンテンツに関わるセキュリティ対策等については国内ベンダの製品市場が大きい。

暗号製品市場を見ると、PKI 製品、DRM については、海外ベンダが主要な技術開発を主導しており、市場シェアも海外ベンダが中心となっている。一方、ファイル暗号化・ディスク暗号化・メール暗号化等、業務で利用されるデータの暗号化を行うソフトウェアは、暗号化機能の使い勝手や業務アプリケーションとの親和性等を考慮する必要があり、国内ベンダの市場規模も大きくなっている。

5.2.2. セキュリティ製品ベンダへのヒアリング

今後のセキュリティ製品市場について、情報セキュリティ製品ベンダ 9 社(表 2-2)へヒアリング調査を行った。各ベンダへは、(1)市場成長率と市場成長率に影響を与える要因、(2)製品機能の変化(特に暗号機能を有する製品、サービスとの関係)、(3)国産暗号の普及について確認した。ヒアリングの結果得られた主な市場動向は以下のとおりである。

(1) 市場成長率と市場成長率に影響を与える要因

(ア) 情報セキュリティ製品市場

- 市場成長率

  市場成長率に関しては、今後数年間は数%から 10%程度の伸びるという意見が多かった。

- 市場成長率に影響を与える要因

  サイバー攻撃の増加、スマートデバイス（特に BYOD）の普及、クラウドの普及、内部情報漏えい等に関わる脅威の増大が挙げられている。

  具体的には、2011 年頃からのサイバー攻撃の増加に伴い、サイバー攻撃の多様化に対処するための新しいカテゴリの製品が伸びている。特に標的型攻撃対策製品や監視系の製品に対する需要が高い。

  また、クラウドセキュリティ製品・サービスが市場規模へ与える影響については、クラウドビジネスにより単価は下がるが、複数クラウドの認証等、クラウドセキュリティの利用数が増大するため、情報セキュリティ製品市場が落ち込むことはないとの見通しが示された。

  その他、リモートアクセス環境での利用デバイスの多様化により、防御側も様々な OS や製品に対応する必要があることから、各々に対応するセキュリティ製品が求められる点が市場成長に対するプラス要因として挙げられている。

(イ) 暗号製品市場

市場成長率に関して、暗号機能の利用は増加しているが、暗号製品単体では市場成長は止まってきている。これは、暗号機能が OS や様々な製品に統合されインフラ化するなどして初めからセキュリティ製品の機能として提供されるようになり、後から暗号機能を主としている専用製品を利用する必要性が減少したことによるとの指摘があった。

(ウ) 暗号ライブラリ市場

市場成長率に関して、暗号ライブラリに関しては製品に組み込まれているため、製品区分として捉えることは困難であり、市場規模の数値化は難しいとの指摘があった。特に、ベンダが独自にインプリメントしている暗号ライブラリは市場規模の数字には入ってこない。

ただし、暗号ライブラリの売り上げは導入デバイス数に比例するが、暗号ライブラリを組み込むデバイス数が減少してきており、国内の暗号ライブラリ市場は縮小してきている、との指摘があった。これは、暗号ライブラリのライセンス先であった携帯電話やゲーム機向けの市場が、スマートフォンの普及に伴い減少してきていることが理由である。スマートフォンの場合、OS 機能として暗号機能が実装されているため、暗号ライブラリを改めて導入する必要性がない。

(2) 要求される製品機能の変化

セキュリティ製品、特に暗号関連製品に関する要求される製品機能の変化について、以下のような傾向が指摘された。

(ア) 機能統合製品の増加

以前は単体で提供されていたような機能（例：VPN）については、現在は機能統合製品（次世代 FW 等の UTM）として提供される例が増えてきている。例えば、今では IPSec や SSL-VPN などは単体では売れず、ネットワークインフラ機能の一部として組み込まれてきている。

同様の事例として、メール暗号化が以前は独立の機能として提供されていたが、2008 年頃からは誤送信防止機能が追加されるなど統合的な製品となってきている。

(イ) ビッグデータへの対応

ビッグデータの普及に伴い、データは暗号化したままで、必要な情報検索をしたり、統計処理を行う技術が求められるようになってきている。

(ウ) 組み込みシステム（IoT）への対応、制御システム等への対応

組み込みシステム（IoT を含む）、例えば白物家電、家庭の中のリモコン、自動車、ロボット掃除機等も乗っ取りや踏み台にされる脅威が増大している。また制御システムについても、不正に操作されることで大きな被害が出る可能性が高まってきており、これらの製品・システムをサイバー攻撃から守る製品へのニーズが出てくる。

(エ) 暗号技術の改善

クラウド時代には個別機器に組み込まれた暗号技術よりも、クラウドインフラ側に組み込まれる暗号技術の方が影響力が大きく、また展開しやすい。

また、暗号技術はユーザからみるとデータの破損、鍵管理等で不安感があり、導入が進んでいない。特に、使いやすさや安心感を解消するような技術や、暗号を使うと今までできなかったことができる、というような付加価値が必要との意見が得られた。

例えば、暗号製品単体は儲けが少ないマーケットビジネスである。マーケットビジネスは売れるかわからない上に、売れた場合には保守の負荷が上がる。一方、アカウントビジネスとしての暗号機能の提供であれば、お客様が保守料を払ってくれるなど、セキュリティ市場のビジネススキームの変革を起こせる可能性がある。

(3) 国産暗号技術の普及

国産暗号技術の普及に向けた課題として、以下のような指摘があった。

(ア) デファクト標準暗号以外を使うメリットの少なさ

顧客から見て、暗号技術の差が製品の差別化に繋がることは少なく、また顧客から暗号方式に対して要求が来ることはない。したがって、デファクト標準である暗号方式を採用することが、顧客への説明も容易であり、(OS の標準機能となっている場合も多いため) コスト面でもメリットが大きい。ユーザは暗号強度よりも柔軟性や効率等使いやすさで選択する場合が大半である。

また、AES 等のデファクト標準であれば海外でも販売しやすいため、メーカはデファクト標準技術を採用する傾向にある。

(イ) 国の調達要件への盛り込みの是非

国産暗号が国の調達要件となると普及するという意見があった一方、日本政府は海外と接続する必要が少ないため、海外で国産暗号技術が導入される可能性はほとんどなく、ガラパゴス化する可能性があるのではないかとの意見もあった。

(ウ) 導入実績の積み上げの少なさ

民間などでの採用に際しては導入実績の有無が重要である。国産暗号技術の普及に向けては、先進的な企業における導入実績を積み重ねるか、まず国が導入し民間に展開するかなどの方策が考えられる。

(エ) デバイスを通じた普及

日本企業(特に大手企業)が海外へ進出する際に、自国技術を持っていくことで、関係する海外企業を通じて世界で利用される可能性はあるとの指摘もあった。また、我が国が強い競争力を持ったデバイスに国産暗号技術を搭載することで普及を図るという意見があった。

ただし一方で、近年は、国産デバイス自体の国際競争力が落ちてきており、デバイスを通じて普及を図るのは難しいとの意見もあった。

(オ) 安全保障観点の考慮

暗号は国家安全保障の側面もあるので、安全保障の観点から国産暗号技術の導入を進めるという割り切りも必要という意見もあった。例えば、政府内の機密文章用に AES と国産暗号を組み合わせて二重化するなどにより、AES が破られた場合の保険として国産暗号技術を利用してはどうかとの意見があった。

5.2.3. セキュリティ製品ベンダへのメールアンケート

国内セキュリティ製品ベンダ 30 社へメールアンケートを実施し、(1)取り扱っている製品カテゴリ、(2)今後 5 年の市場成長率予測(3)市場成長率に影響を与える要因を確認し、5 社より回答を得た。回答の結果は表 5-4 の通りである。

表 5-4 メールアンケート結果 [171]

製品カテゴリ	成長率予測	成長要因
検疫ツール	5～10%未満	モバイルデバイスの普及／サイバー攻撃(外部)の脅威の高まり
シンクライアント	20%以上	モバイルデバイスの普及/内部犯行等の脅威の高まり／運用管理の負荷低減など IT コスト全体の削減
ファイアウォール／VPN／UTM	5～10%未満	モバイルデバイスの普及／IT 投資の回復／マイナンバー等、政府施策による IT 案件の増加
メールフィルタリング	ほぼ横ばい	クラウドコンピューティングの進展／サイバー攻撃(外部)の脅威の高まり／内部犯行等の脅威の高まり
電子メールセキュリティアプライアンス	ほぼ横ばい	当該製品の需要の一巡
	ほぼ横ばい	クラウドコンピューティングの進展／サイバー攻撃(外部)の脅威の高まり／内部犯行等の脅威の高まり
電子メールアーカイブ	5～10%未満	クラウドコンピューティングの進展/内部犯行等の脅威の高まり／IT 投資の回復
Web セキュリティアプライアンス	5～10%未満	当該製品の需要の一巡／サイバー攻撃(外部)の脅威の高まり／モバイルデバイスの普及
	ほぼ横ばい	クラウドコンピューティングの進展／モバイルデバイスの普及／サイバー攻撃(外部)の脅威の高まり
Web アプリケーションファイアウォール	20%以上	サイバー攻撃(外部)の脅威の高まり／プライバシー保護意識の高まり
	10% ～ 15%未満	モバイルデバイスの普及／サイバー攻撃(外部)の脅威の高まり／内部犯行等の脅威の高まり
セキュリティ検査／監視ツール	0～5%未満	マイナンバー等、政府施策による IT 案件の増加／サイバー攻撃(外部)の脅威の高まり／内部犯行等の脅威の高まり

[171] 同一製品カテゴリに対して複数社からの回答を得ている場合は行を分けて示している。

各製品カテゴリによって差はあるものの、すべて横ばい以上との回答となっており、ヒアリングで確認したセキュリティ製品市場の動向と大きく離れるものではない。

また、成長要因だけを抜き出してみると、表 5-5 の通り、サイバー攻撃(外部)の脅威の高まり、モバイルデバイスの普及、内部犯行等の脅威の高まりが多く挙がっている。これらの要因はヒアリングでも成長要因として挙げられていた。

表 5-5 市場成長要因として挙げられた回数

成長要因	要因に挙げられた回数
サイバー攻撃の脅威の高まり	7
モバイルデバイスの普及	6
内部犯行等の脅威の高まり	5
IT 投資の回復	2
マイナンバー等、政府施策による IT 案件の増加	2
プライバシー保護意識の高まり	1

5.3. 今後の市場規模の推計

事業者ヒアリング（5.2.2. セキュリティ製品ベンダへのヒアリング）及び事業者に向けたアンケート回答の結果（5.2.3. セキュリティ製品ベンダへのメールアンケート）から、セキュリティ製品市場、暗号製品市場の成長率の予測を行なった（表 5-6）。

5.3.1. セキュリティ製品市場

事業者ヒアリング及びアンケート回答の結果などから推計した結果、セキュリティ製品市場については、今後も 5%前後の成長率を維持すると考えられる。

標的型攻撃、DDoS 攻撃、Web アプリケーション等、昨今の新しい脅威に対する対策ツールにおいては、成長率が高く見込まれている。また、モバイル系全般、情報漏えい防止の観点からシンクライアントや DLP 等も、成長率が高い。

なお、富士キメラ総研[172]によると、今後 5 年間、セキュリティ製品市場の成長率は 5%前後で推移し、市場全体は堅調に成長するものと推計されており、今回の調査結果と同様の傾向を示している。具体的には、現在の市場規模から類推すると 2017 年頃には 4 千億円近くになると予測される（図 5-6）。

拡大する要因としては、モバイル端末の業務利用の拡大やクラウド化の進展によって企業において利用される端末・システム形態が多様化する点が挙げられる。特にモバイル暗号化関連ツールは大きく伸びると予測される。また、大企業へのより高度なサイバー攻撃の増加により、外部脅威対策ツールやリスクの可視化ツールへの需要の拡大も要因として挙げられている。

[172] 富士キメラ総研「ネットワークセキュリティビジネス調査総覧」(2013 年)

表 5-6 セキュリティ製品市場の成長率

市場	製品カテゴリ	ヒアリング	メールアンケート	総合
セキュリティ製品市場	・ワンタイムパスワード ・デバイス認証ツール ・認証デバイス(ICカード、USBトークン、バイオメトリクス) ・シングルサインオン ・統合ID管理ツール ・特権ユーザ管理ツール ・検疫ツール(トークン、不正接続防止、検疫ツール) ・フォレンジックツール ・統合ログ管理ツール ・シンクライアント ・ファイアウォール/VPN/UTM関連製品 ・DDoS対策ツール ・ウイルス対策ツール ・標的型対策ツール ・Webフィルタリングツール ・メールフィルタリング ・電子メールセキュリティアプライアンス ・電子メールアーカイブ ・Webセキュリティアプライアンス ・Webアプリケーションファイアウォール ・データベースセキュリティ製品 ・端末管理・セキュリティツール(IT資産管理、端末操作ログ収集、持出制御) ・DLP ・USBメモリセキュリティ ・モバイルウイルス対策 ・モバイルフィルタリングツール	**今後数年間は数%～10%程度伸びる** (＋)サイバー攻撃の増加 (＋)スマートデバイス(特にBYOD)の普及 (＋)内部情報漏えい等に関わる脅威の増大	・検疫ツール: 5～10%未満 ・ファイアウォール／VPN／UTM関連製品: 5-10%未満 ・セキュリティ検査／監視ツール: 0-5%未満 ・標的型攻撃対策ツール: 20%以上 ・電子メールセキュリティ: ほぼ横ばい ・電子メールアーカイブ: 5～10%未満 ・Webセキュリティアプライアンス: 5～10%未満、ほぼ横ばい ・Webアプリケーションファイアウォール: 20%以上、10%-15%未満 ・端末管理・セキュリティツール: ほぼ横ばい	5%前後
暗号製品市場	・PKI関連製品 ・メール暗号化(暗号機能、誤送信防止) ・端末管理・セキュリティツール(★ファイル暗号化 、★ディスク暗号化) ・DRM ・モバイル暗号化ツール ・暗号ライブラリ(2010年まで)	**今後数年間は微増** (－)暗号機能を主とする製品が減少 (＋)拠点間の暗号通信(VPN)や企業クラウド利用の増加 (＋)リモートアクセスやBYODの普及によるデータ保護ソリューションへのニーズの高まり	・ファイル暗号化・ディスク暗号化: ほぼ横ばい	ほぼ横ばい
暗号ライブラリ市場	・暗号ライブラリ	**製品に組み込まれており、製品区分として捉えることが困難** (-)暗号ライブラリを組み込むデバイス(携帯電話やゲーム機)がスマートフォン普及などにより減少	－	－

5.3.2. 暗号製品市場

暗号製品市場は、今後 5 年はほぼ横ばいで推移すると考えられる（表 5-6)。

標的型攻撃への出口対策として金融や大手製造業でメール暗号化ツールの導入が進み、誤送信防止ツールや DRM 市場は幅広いユーザがいるため堅調に成長が見込まれる。しかし、ファイル暗号化・ディスク暗号化ツール、PKI 関連は機能統合製品へのリプレスが進むと考えられるため、市場はマイナス成長～若干のプラスに留まると考えられる。モバイル暗号化ツールは成長率としては大きな成長が見込まれるが、市場規模が小さいため暗号製品市場に与えるインパクトは小さいとみられる。

参考までに、富士キメラ総研による暗号製品市場の推移についてまとめた結果を図 5-7 に示す。

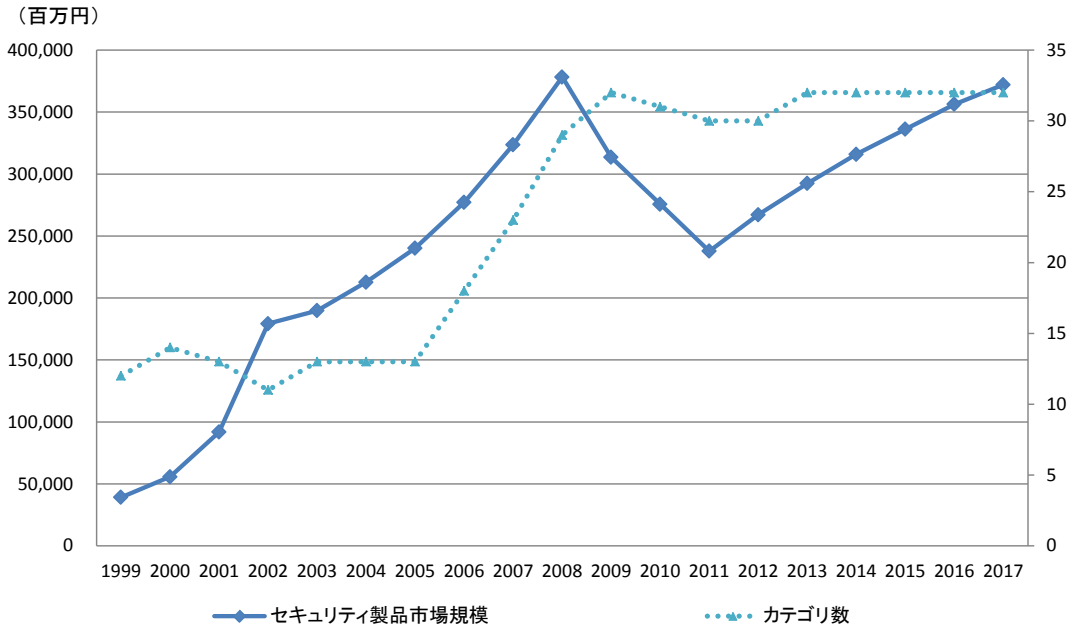


図 5-6 情報セキュリティ市場の推移(1999 年～2017 年)[173]

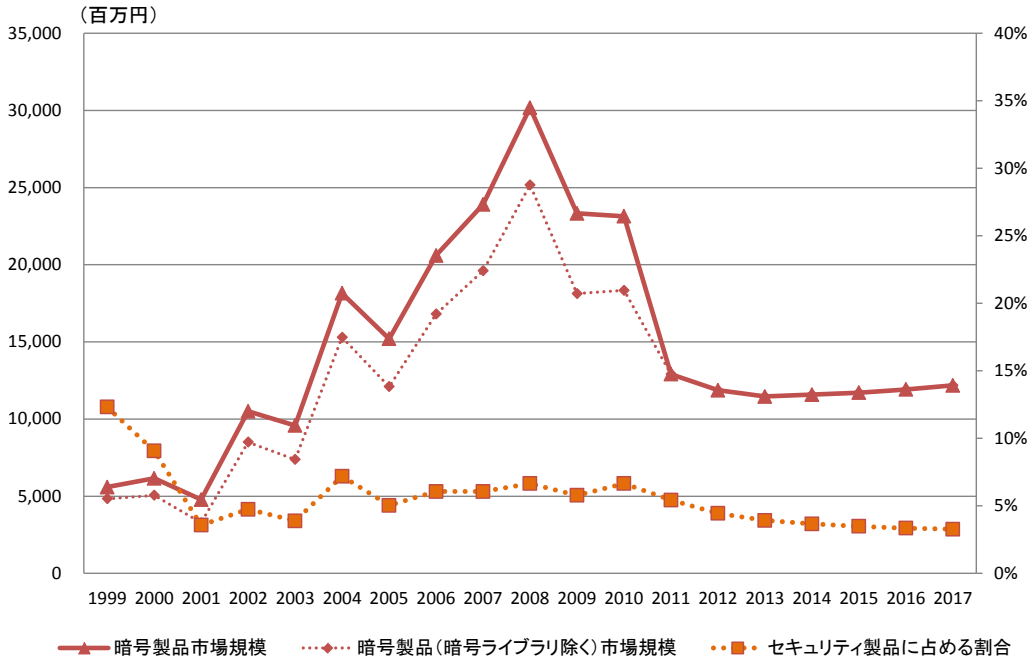


図 5-7 暗号製品の推移と予測(1999 年～2017 年)[174]

[173]富士キメラ総研「ネットワークセキュリティビジネス調査総覧」(1999 年～2013 年)より三菱総合研究よが作成 。2013 年～2017 年の値は富士キメラ総研の予測による。
[174]富士キメラ総研「ネットワークセキュリティビジネス調査総覧」(1999 年～2013 年)より三菱総合研究所が作成 。2013 年～2017 年の値は富士キメラ総研の予測による。

5.3.3. 暗号ライブラリ市場

暗号ライブラリ市場については、ヒアリング結果を踏まえると、従来、ゲーム機等ライセンス先となっていた端末機能がスマートフォンに集約され、スマートフォンの場合、暗号機能が OS 機能に組み込まれていることから市場は縮小傾向が見込まれる。一方、OpenSSL 等のオープンソースの普及や、暗号機能の OS への組み込み等、市場としては顕在化しないため、暗号自体の普及は進むものの市場成長へは寄与しないと見られる。

デジタル複合機など、スマートフォンに集約されない機器の場合は、機器市場の成長に伴い暗号ライブラリも成長すると見られる。その場合、成長市場は、飽和に近い国内市場より海外が有望と考えられる。

5.4. 情報セキュリティ製品市場における暗号技術の現状と今後

文献調査及びヒアリング調査結果より、国内の情報セキュリティ製品市場は今後数年間も年間数%程度の成長率を維持すると考えられる。これは企業におけるクラウドサービス利用の増加やリモートアクセス環境の整備、多様化するサイバー攻撃等を背景として新たな情報セキュリティ製品の導入が進む事により牽引されると予想されるためである。

暗号技術は情報セキュリティ製品に広く使われており、情報セキュリティ製品市場の成長と共に、暗号技術の利用は広がると考えられる。しかし、暗号技術に特化した暗号製品市場という単体のカテゴリとして見える市場規模は横ばいである。これは、情報セキュリティ製品の機能が単体で成り立つ市場が減少しており様々な機能を統合したものとなっていることや、情報活用をビジネス戦略の重要な位置付けと見る機運が高まる中、保護すべきデータを活用しながら暗号機能を含むセキュアな環境構築の必要性が高まっていることも背景にあると考えられる。

6. まとめと今後の課題

6.1. 各国の暗号政策

各国政府における暗号利用に関する政策動向調査について、各国政府における暗号利用に関する政策を表 6-1、表 6-2 にまとめた。

暗号政策の所管省庁については、今回調査対象とした 9 カ国のうち、6 カ国(英国・フランス・ドイツ・ロシア・中国・オーストラリア)が国家安全保障系機関(国防機関、諜報機関、治安機関等)であり、2 カ国が国家安全保障系機関と経済・科学技術系機関の共管(米国:NSA と NIST、韓国:NIS と KISA)であった。所管省庁が国家安全保障系機関ではないのは 1 カ国(エストニア)のみであり、電子政府系機関が担当している。

このことからわかることは、今回調査対象とした 9 カ国はいずれも暗号政策の所管省庁の役割・権限が明確に定められており、各国毎に政策の重点は微妙に異なっているものの、多くの国では国家安全保障の観点を重視して暗号政策を捉えている。

具体的な施策として、政府機関のセキュリティ向上のために、濃淡はあるものの、殆どの国では政府調達において、一定以上のセキュリティ水準が求められる情報システムでのセキュリティ認証取得製品の導入を義務付けたり、政府機関で用いることのできる暗号アルゴリズムを指定もしくは推奨している(表 6-1)。

安全保障の観点から敵性国家等に対する暗号技術の拡散を防止するための輸出規制は全ての国で実施されている。一方、暗号技術の国内利用の規制についてはロシアと中国が特に厳格な管理を行なっている。これは国内の治安政策を重視しているためである。

ただし、それ以外の国に関しても犯罪捜査やテロリスト対策などの観点から、裁判所の命令等に基づき暗号化されたデータの復号や、暗号鍵の開示を求めるなどを法律で定めている国が多い。

人材育成に関する各国の暗号政策の重点は、安全保障や政府機関のセキュリティ向上を目的とした人材の育成である。この目的のため、奨学金プログラム等が実施されている。暗号に特化したプログラムは少ないが、例えばロシアでは暗号・通信･情報学研究所を設置し、専門教育及び研究を実施すると共に、学生を対象に「数学と暗号におけるオリンピック」を主催するなど、暗号人材の育成に力を注いでいる。また、暗号に特化したプログラムではないが、米国やエストニアなどでは、サイバーセキュリティを専攻する学生に対する奨学金の給付や、それら学生の優先的な採用などの人材育成プログラムを持っている。

研究開発に関する各国の暗号政策では、国立研究所・国立大学における暗号研究の実施に加え、研究資金提供、暗号研究コミュニティの支援(中国・韓国)等が実施されている。

表 6-1 各国暗号関連政策の比較 (1/2)

国(所管省庁)		政府調達要件	評価認証	暗号要件
米国 (NSA/NIST)	制度等	情報技術管理改革法, FISMA, CNSSP 11	CMVP, CC	FIPS 197、FIPS 180-4 等
	特徴	連邦政府機関のセキュリティシステムについて CMVP, CC 認証製品の導入を義務づけ	CMVP は NIST が運営、CC は NIAP (NIST と NSA の共同)が運営。CMVP での対象は NIST が定めた暗号のみ	NIST が連邦政府機関で用いることのできる暗号を規定。 安全保障用途は NSA が別途規定(非公開)
英国 (CESG)	制度等	HMG Security Policy Framework, HMG IA Standards	CAPS, CPA, CC	HMG Cryptographic Standards
	特徴	OCSIA が定める HMG Security Policy Framework に基づき、CESG が IT システム開発時に考慮しなければならない情報保証に関する法的拘束力のあるポリシーとして HMG IA Standards を規定。 少なくともハイグレードの情報システムでは CAPS 認証が必須	CESG が運営。CAPS, CPA は英国独自の認証制度。 CAPS は上位 2 段階の保証グレート認証で、GOTS 製品が対象。CPA は最も低い保証グレード認証で、COTS 製品が対象。 なお、CC は CPA より低位に位置づけ	CESG が政府機関で用いることのできる暗号を規定(非公開)
フランス (ANSSI)	制度等	Ordonnance n° 2005-1516 du 8 décembre 2005, Référentiel Général de Sécurité (RGS)	CC, CSPN, SSCD, agrément	Référentiel Général de Sécurité (RGS)
	特徴	政府システムにおける情報セキュリティを義務的要件として ANSSI が規定。特に、RGS に基づき、システムに応じて ANSSI が実施する製品認証 (CC, CSPN 等)が義務づけ	ANSSI が運営。CC 以外はフランス独自の認証制度。 CC に加え、CC より低コストの CSPN を推進。SSCD は欧州ガイド CWA 14924 2004-03 に基づく暗号モジュール認証。 agrément は、国家安全保障に関する情報保護が対象	ANSSI (前身 DCSSI)が暗号強度に関するルールと推奨暗号についてとりまとめ。推奨暗号は例示
ドイツ (BSI)	制度等	SAGA, IT-Steuerung Bund	CC	SAGA, BSI TR
	特徴	IT 製品の連邦政府の調達は BFI 管理のもと BMI と IT-SB が方針を決定。これらは実質的な電子政府のシステム調達要件になっている。 なお、認証製品の導入が義務になっているかどうかは不明	CC は BSI が運営。 CMVP に相当する認証制度はない	SAGA では BfIT が電子政府システムでの暗号アルゴリズムの要件を規定。BSI TR では BSI が電子政府システム以外を対象に推奨暗号を例示

国(所管省庁)		政府調達要件	評価認証	暗号要件
エストニア (RIA)	制度等	ISKE (IT Security Standard), Infosüsteemide turvameetmete süsteem	なし	Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring
	特徴	政府システムにおける情報セキュリティを義務的要件としてRIA が規定。ドイツの「IT Baseline Protection Manual」がベース	CC を準備中	安全性に基づいた推奨暗号を例示。RIA と Cybernetica AS がレポートや論文を総括したもの
ロシア (FSB)	制度等	184-FZ "On Technical Regulation"	POCC RU.0001.030001, POCC RU.0003.01 Б И00	GOST 28147-89 等
	特徴	政府調達についてはGOST 標準への準拠が求められる。 FSB によるライセンスを取得した組織が設計・開発した暗号化ツールで、認証取得済みのものを用いることが必要。 なお、99-FZ "On Licensing Certain Activities"により、暗号利用等、様々な場面で FSB からライセンスの取得が必要	FSB が運営。どちらもロシア独自の認証制度。 POCC RU.0001.030001 が CMVP、POCC RU.0003.01 Б И00 が CC に類似する制度。なお、GOST 標準を実装した暗号システムだけが認証対象	連邦技術規制・計測庁が標準化
中国 (国家暗号管理局)	制度等	政府調達法	中国情報セキュリティ認証制度	国家暗号管理局公告 (第21 号)等
	特徴	政府調達において認証取得が義務付けられている。国家暗号管理局が許可した暗号のみ利用可能	ISCCC が運営。中国独自の認証制度。 中国標準 GB/T18336-2008 に基づいた CC に類似する制度	国家暗号管理局が標準としての商用暗号を規定。 なお、商用暗号管理条例では「国家機密とされる商用暗号技術(第二条)」との記載もあるため、それ以外の商用暗号がある可能性は否定できない
韓国 (NIS/KISA)	制度等	電子文書保安措置施行指針 国家サイバー安全管理規定	CC (KECS)、韓国版 CMVP	ARIA (国家標準(KS)), SEED, HIGHT 等 (TTAS KO-12)等
	特徴	政府向けにはKECS 認証取得が必要で、暗号モジュール搭載時は国家機関用暗号モジュール認証も必要。 対国民行政業務用システムでは韓国版 CMVP 認証取得が必要	CC (KECS)は ITSCC の運営で、CCRA の対象 韓国版 CMVP は NIS の運営で、韓国独自の認証制度。 他に、国家機関用暗号モジュール(認可暗号アルゴリズムは非公開)の認証制度がある	KISA が中心になって開発。 ARIA 以外は通信技術協会(TTA)にて標準化。ARIA のみ国家標準基本法に基づく国家標準 NIS が韓国版 CMVP 認可暗号アルゴリズムを規定

国(所管省庁)		政府調達要件	評価認証	暗号要件
オーストラリア (ASD)	制度等	Protective Security Policy Framework (PSPF) 2013	AISEP, ASD cryptographic evaluation	Information Security Manual, Control Manual
	特徴	機密情報を扱う政府システムでは AISEP 認証取得を義務的要件として規定。一般政府システムでは条件に合致したレベルの CC 認証で代用可能。 機密情報(RESTRICTED information)以上を扱う政府システムの場合、ASD Cryptographic Evaluation 認証取得が必須	AISEP は ASD がニュージーランドの GCSB と共同運営する両国政府共同認証制度。CC に準拠した制度になっているが、独自の追加要件を含む。 ASD Cryptographic Evaluation は暗号製品のみを対象とする独自の両国政府共同認証制度	ASD が政府機関で用いることのできる暗号を規定
EU (ENISA)	制度等	ー	Approved Cryptographic Products(LACP)	Algorithms, Key Sizes and Parameters Report
	特徴	EU では規定せず、各国政府が EU、ENISA 等の情報を参考に独自に決める	EU における情報保証(Information Assurance)の考え方に基づき、欧州連合機密情報(European Union Classified Information) を規定。機密区分に応じて、認証された暗号製品が求められる	暗号アルゴリズム、鍵長、パラメータに関する推奨について、EU 加盟国が個人情報、機微情報の保護において対処すべき暗号に関する最小限の要件を取りまとめたもの。強制力はない。 ECRYPT II を引き継ぎ ENISA が保守を行なっている

表 6-2 各国暗号関連政策の比較 (2/2)

国(所管省庁)		輸出入規制	国内利用規制	研究開発
米国 (NSA/NIST)	制度等	Export Administration Act, Export Administration Regulation	ー	NIST, NSA が中心。 その他の暗号研究開発プログラムとして、IARPA, DARPA などがある。 人材育成でも、NSA、国土安全保障省、国防総省などが関与した育成プログラム(主にファンディング)を実施
	特徴	輸出規制はワッセナー協定に基づく。2010 年に大幅に規制緩和され、暗号強度が一定以上でマスマーケット品でないもの以外は規制対象から除外された(※医療や著作権保護用途の場合は暗号強度に関わらず規制対象外)。 輸入規制はなし	明示的な国内利用の規制はなし	
英国 (CESG)	制度等	Dual-Use Items Regulations, Open General Export License, White Paper on Strategic Export Controls	Regulation of Investigatory Powers Act	ロンドン大学、ブリストル大学等が中心。 人材育成では、CESG がイギリス国籍を持つことを条件とした研究開発ファンディングを実施
	特徴	輸出規制は、EU デュアユース規制及びワッセナー協定に基づく。 暗号製品輸出入規制に関して、個人利用、コミュニティライセンスを免除	安全保障、犯罪捜査等を目的とした暗号データの復号命令権を規定	
フランス (ANSSI)	制度等	Law No. 2004-575, Decree No. 2007-663 of 2 May 2007	Law No. 2004-575, article 30(I)	CNRS, ENS, INRIA から研究者が参加している CASCADE チームが中心組織。国内および EU ファンディング機関からの資金援助を受ける
	特徴	輸出規制は、ワッセナー協定に基づく。 EU/EEA からの輸入は自由。 域外からの輸出入では暗号強度が一定以上の場合は規制あり	国内利用の規制なし。ただし、安全保障、国防に関係する暗号サービスでは申告が必要	
ドイツ (BSI)	制度等	AWG, AWV, KWKG	ー	DFG と連携しつつ、BIS が担当。実務として、Fraunhofe 研究所が、BSI、BMWi と密接に連携し研究
	特徴	暗号技術の輸出規制は、EU 輸出規制およびワッセナー協定に基づく。域内でのマスマーケット向けの暗号システムの輸出は自由化。 輸入規制はなし。	明示的な国内利用の規制はなし	
エストニア (RIA)	制度等	Strateegilise kauba seadus, Vastu võetud 07.12.2011	ー	タリン工科大学とタルトゥ大学が中心。 人材育成では、NATO のサイバー防衛協力研究拠点を活用したプログラム等がある
	特徴	輸出規制はワッセナー協定に基づく。輸入規制はなし	明示的な国内利用の規制はなし	

国(所管省庁)		輸出入規制	国内利用規制	研究開発
ロシア (FSB)	制度等	164-FZ"On Fundamental Principles of State Regulation of Foreign Trade Activity", 183-FZ "On export control", 連邦政府決定第 364 号「商品の貿易における許可制について」	99-FZ "On Licensing Certain Activities", Decree No.334 "Data Encryption", Decree No.351, 85-FZ "On Participation in international exchange of information"	FSB 傘下の暗号・通信・情報学研究所で研究が行なわれている
	特徴	輸出規制はワッセナー協定よりも厳格に管理。 一定以上の強度をもった暗号に関しては輸入規制が存在	暗号ツールの開発・製造・流通・販売・提供等にはライセンス許可が必要。FSB が認可していない暗号ツールや暗号製品は利用禁止	
中国 (国家暗号管理局)	制度等	商用暗号製品使用管理規定、商用暗号製品販売管理規定、対外貿易法、連合公告 2009 年第 18 号、国外組織及び個人の中国での暗号製品使用に関する管理弁法、等	商用暗号管理条例、商用暗号製品使用管理規定、国外組織及び個人の中国での暗号製品使用に関する管理弁法、等	国家暗号管理局の下に中国暗号学会を置き、暗号研究を管理している。 商用暗号開発には、国家暗号管理局からの認可が必要
	特徴	輸入規制、輸出規制ともに存在する。輸入規制に重点が置かれている。	商用暗号の研究・生産・販売・使用等の管理について様々な規制がなされている。国外組織も対象	
韓国 (NIS/KISA)	制度等	対外貿易法、対外貿易法施行令、戦略物資輸出入告示	ー	KISA、NSRI、ETRI を中心に研究開発が行なわれている
	特徴	輸出規制は、ワッセナー協定に基づく。輸入規制はなし	明示的な国内利用の規制はなし	
オーストラリア (ASD)	制度等	Customs Act 1901, Defence and Strategic Goods List Amendment 2011, Australian Export Controls for defense and Dual-Use Goods、等	Cybercrime Act, No. 161, 2001	Queensland University of Technology, Macquarie University 等が中心。 人材育成では、防衛省内の DSTO Academic Scholarships Program がある
	特徴	輸出規制は、ワッセナー協定に基づく。パブリックドメインソフトウェア、マスマーケットソフトウェア、個人利用は規制対象外。 輸入規制はなし	欧州理事会のサイバー犯罪条約に対応して立法化された法律で、暗号鍵の開示、または暗号データの復号権を規定	
EU (ENISA)	制度等	Council Regulation (EC) No. 1334-2000	Convention on Cybercrime, 2001	欧州研究開発プログラム(現在は HORIZON2020)のファンディングにより推進
	特徴	ワッセナー協定に準拠するEU規制を定める	サイバー犯罪に関する対応を取り決めた国際条約で、復号命令の立法化を容認	

6.2. セキュリティ認証取得動向

セキュリティ認証取得製品に関する動向調査では、各国の認証取得製品数の推移の分析を行なった結果、米国の CMVP 認証取得製品数に比較して我が国の JCMVP 認証取得件数が低調であることがわかった。これは政府調達で要件として求められていないことが大きな原因と考えられる。

CC 認証について、我が国はドイツに次いで認証取得件数が多いものの、内容は複合機関連などが多くを占めており、これは我が国から米国に製品を輸出する際に顧客から認証取得を求められているためと考えられる。米国では CMVP または CC 認証取得製品の政府調達が義務化されており、ベンダにとってセキュリティ認証を取得する動機が強く、取得件数も多くなっている。民間活用の事例では、欧州におけるスマートカードのチップセキュリティの評価・認証がスタンダードとなって、各国の CC 認証でも利用されていることから、スマートカードで高い競争力を有するフランスやドイツでのスマートカードの認証件数が多くなっている。

6.3. 国内暗号製品市場に係る動向

国内暗号製品市場に係る動向調査の結果から、暗号製品の市場は情報セキュリティ製品市場のおよそ 5%を占めており、経年的に見ても大きな変動はない事がわかった。

具体的には、情報セキュリティ製品市場全体として、数%の成長率を維持する見込みである。暗号機能単体の製品の導入よりも暗号技術を取り入れた機能統合的な製品にニーズが移っているため、見かけ上は暗号製品市場が縮小しているように見えるが、この傾向は今後も継続すると思われる。また暗号ライブラリ市場については製品への組込みが進んでおり、市場としての評価は難しい。

情報セキュリティ製品市場が数%の成長率を維持する要因としては、BYOD に代表されるスマートデバイスの利用増加により、各スマートデバイス向けのセキュリティサービスのニーズが高まる事やクラウドサービスの増加に対応するために新しいカテゴリの製品の導入が進展すること等が挙げられた。

今後の注目すべき市場の動向としては、機能統合型製品やサービスの導入の増加、ビッグデータの普及に伴う暗号化したまま処理のできる技術へのニーズの拡大、IoT の進展と制御システム向け製品やサービスへのニーズが高まりなどが挙げられる。

6.4. 今後の課題

暗号アルゴリズムの普及促進やセキュリティ産業の競争力強化に向けた障壁といった観点から今回の調査結果を分析すると以下のような課題があることがわかった。

(1) 今回調査対象となった諸外国では、暗号政策を国家安全保障の観点を重要な要素として位置づけている国が多かった。今後は、暗号を含む情報セキュリティ産業の維持・強化についても、国家安全保障上の意義といった観点からの検討が必要である。

(2) 暗号の利用促進によるセキュリティ水準の向上といった観点からは、米国などのように政府調達においてセキュリティ認証製品の調達を法的に義務付ける方向性に加え、フランスやドイツのように競争力を持つ自国産業であるスマートカードなど、特定分野における評価・認証を進めることで自国産業のさらなる競争力向上と併せてセキュリティ水準の向上を図るという方向性が考えられる。

(3) 暗号技術は今後も情報セキュリティ技術の中核を占めていくことは市場調査の結果からも明らかであるが、暗号技術による製品の差別化が困難である状況がより進展する可能性がある。ビッグデータに対応した準同系暗号技術の開発や、暗号技術が存在しないと実現できない新しい用途の開発など、製品差別化に繋がるような技術開発が今後必要になると考えられる。

今後の一つの方向性としては、暗号関連産業の維持・強化が国の安全保障戦略上重要であることについて、関係者間での認識の共有が重要になってくると考えられる。この目的のため、安全保障上どの程度の暗号関連産業(とそれを支える人材・学会等)を維持する必要があるかについて、合理的な仮説を構築し、関係者間で議論を行なうことが重要ではないかと考えられる。

以上