各国政府のセキュリティ政策に関する実施体制、法制度及び認証制度調査

― 調査報告書 ―

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan
2021 年 4 月

目　次

＜改訂履歴＞

2021.4.15	（P.15、P.21）誤植修正。 「ISO/IEC 24759:2014」→「ISO/IEC 24759:2017」

1. はじめに

1.1. 背景と目的

2014 年に、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、特に欧米・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調査を実施した。

その後、IoT や自動車の自動運転、個人データ流通に伴うリコメンドサービスの進展など、新たな産業構造の急速な変化に伴い、サービスそのものの安全性確保や個人のプライバシー保護などのセキュリティ課題も大きくなってきている。また、ビットコインに代表される国家管理から離れた暗号資産（crypto assets）の急速な普及、サイバーテロによるウクライナでの大規模停電、マルウェア Mirai による北米を中心とした大規模システム障害など、社会活動そのものに大きな影響を与えるセキュリティ関連の事象が世界中でますます多発している。このような社会的変化を受け、ここ数年でサイバーセキュリティに関連する実施体制や法制度等を大きく見直したり、新たな法規制等を設けたりした国も多い。

そこで、独立行政法人情報処理推進機構（以下「IPA」という。）では、各国政府、特に欧米中露を中心に、セキュリティ政策に関する実施体制、法制度及び認証制度に関して、2014 年 7 月以降の変化を踏まえた最新動向調査を実施した。

本調査結果を報告書として取りまとめて公開すると共に、経済産業省等による暗号に関わるセキュリティ政策等の立案における基礎資料として活用する。

2. 調査方法

IPA 及び経済産業省において、これまでに実施した欧米やアジア各国におけるセキュリティ政策や暗号政策に係る現状の調査を参考に、最新の動向を調査し、情報の更新を行った。具体的には、2014 年度暗号利用環境に関する動向調査[1]に記載している組織体制及び法令等について、2014 年 7 月以降に改正されているかどうかを確認し、改正されている場合には改正内容を調べた。また、調査対象期間に新規に施行された法令等についても調査対象に含めた。さらに、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、法制度以外の最新の政策動向等について、2014 年 7 月以降を重点的に調査した。

3 節に、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 調査結果を報告する。文献調査では、主に以下の項目を確認した。

- 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、並びに暗号やセキュリティの政策方針を定めたもの）
- 暗号方式の利用に関連する法制度やガイドライン等（特に、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、暗号の利用に関する条件があるか、所管官庁など）
- セキュリティ認証制度に関連する法制度やガイドライン等（特に、セキュリティ認証制度が構築されているか否か。構築されている場合には、どの程度活用されているか、など）
- 政府のセキュリティ製品の調達要件（もしくは調達ポリシー）に関連する法制度やガイドライン等（特に、セキュリティ認証製品の政府調達が強制されているか否か、など）
- 暗号に関連する輸出入規制についての法制度やガイドライン等（特に、輸出規制がワッセナー・アレンジメントに準拠したものか否か、輸入規制があるか否か。規制がある場合にはどのような規制か、所管官庁、など）
- その他、暗号又はセキュリティに関連するサービスに対する法制度やガイドライン等（例えば、暗号資産、電子商取引、不正アクセス禁止法、個人情報保護法など）

4 節に、3 節における調査結果を総括として、各国・地域の暗号要件・評価認証の比較、輸出入/利用規制の比較を行なった。

---

[1] 2014年度 暗号利用環境に関する動向調査
https://www.ipa.go.jp/security/fy27/reports/crypto_survey/index.html

3. 各国政府のセキュリティ政策の実施体制、法制度及び認証制度

3.1. 米国

ホワイトハウスは 2018 年 9 月に国家サイバー戦略を発表し、サイバーセキュリティ確保を基本的取り組みとして挙げ、ネットワークやシステムの機能や情報の保護、デジタル経済や新興技術の育成、サイバー攻撃の抑止、オープンなインターネットの拡大を 4 つの柱として掲げた。これに基づいた政策として、暗号製品及び技術の輸出規制、標準化が行われている。輸入及び利用は規制されていない。

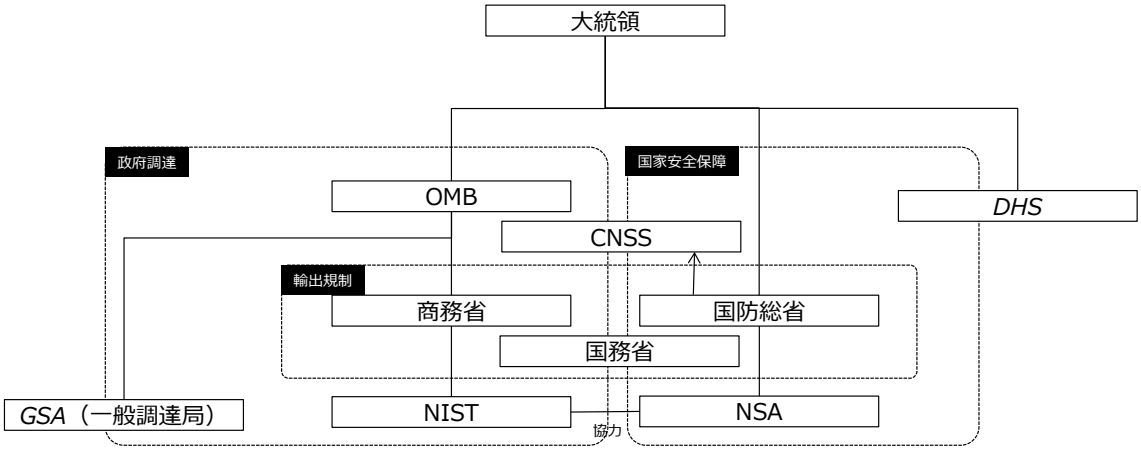
暗号製品や技術の輸出規制は安全保障と産業競争力の両立を目的として実施され、強い暗号や耐量子計算機暗号を使用した製品や技術、量子暗号を利用もしくは実現する機器を規制対象としている。

標準化については、NIST（National Institute of Standards and Technology、国立標準技術研究所）により、連邦政府機関向けの暗号技術やそれを利用するサイバーセキュリティ技術・手法の標準やガイドラインの策定・更新、公開が行なわれている。それらは連邦政府機関のみならず、民間や国外からも参照され広く利用されている。NIST は耐量子計算機暗号アルゴリズムの標準化作業を進めており、これは、国家サイバー戦略の、振興分野の技法・プロセスの開発及び標準の策定の優先実施項目としての指定に基づき実施されている。NIST はこの他にも、しきい値暗号やペアリング暗号といった高機能暗号の標準化を行なっている。

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として示し、NSA（National Security Agency、国家安全保障局）と 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。



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　米国における暗号政策に係る組織体制

暗号及びセキュリティ政策に関する組織の中で主要なものについて、その役割を以下に示す。

- OMB（Office of Management and Budget、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。情報管理についての覚書（OMB Circular A-130（後述））の中で、連邦政府機関にセキュリティ計画の策定・実施を求め、NIST が策定した標準やガイドラインに従うことを求めている。

- 商務省（Department of Commerce）
  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、暗号製品を含むデュアルユース品目の輸出規制を担当する。

- NIST（National Institute of Standards and Technology、国立標準技術研究所）
  NIST は商務省配下の試験研究機関であり、連邦政府機関向けの暗号標準を含むサイバーセキュリティ技術や手法を開発し、標準やガイドラインの策定を行なう。また、暗号モジュール、暗号アルゴリズムの試験認証制度を実施する。これについて、3.1.3.2 節で説明する。
  なお、NIST のサイバーセキュリティ・プライバシー部門の 2021 年度概算要求は約 79.4 百万ドルである（2020 年度実績は 77.5 百万ドル）[2]。

- 国防総省（DoD、Department of Defense）
  CNSS（Committee on National Security Systems、国家安全保障システム委員会）を通して政府の国家安全保障システム（NSS: National Security System）のセキュリティ政策に関わる一方、国防総省内のネットワークセキュリティに関して独自にポリシーを定め実施している。

[2] https://www.nist.gov/fy2021-presidential-budget-request-summary

- NSA（National Security Agency、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（Committee on National Security Systems、国家安全保障システム委員会）
  NSS の政策、指針、操作手順、ガイダンスを議論、策定、公表する。組織は連邦政府機関の代表者から構成され、国防長官が委員長を、NSA 長官が責任者を務める。

- 国務省（Department of State）
  軍用に開発された暗号機器などを含む軍需品の輸出管理を担当する。

- 国土安全保障省（DHS、Department of Homeland Security）
  連邦政府機関のサイバーセキュリティ対策の実施を管理、技術的支援等を行う。

- GSA（General Service Administration、一般調達局）
  FISMA（Federal Information Security Management Act（後述））の定めるセキュリティ要件に従い、NIST が発行する標準やガイドに準拠した情報技術関連製品の調達を行う。また国土安全保障省、国防総省とともに、連邦政府統一のクラウドサービス評価・認証制度 FedRAMP を実施する。これについて、3.1.3.3 節で説明する。

なお、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。また、NIST と NSA は多くの標準化団体に並んで参加している。

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。

諜報・防諜（機密情報）に係る法制度については、国家安全保障に関する大統領令や CNSS が発行する文書等が非公開とされるなどの理由から、その全体像を把握することは困難である。

主な暗号政策・情報セキュリティ政策について分類整理したものが表 3-1 及び図 3-2 である。

表 3-1　米国における暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	上位政策・戦略	Federal Information Security Management Act of 2002 (FISMA)[1]、 Federal Information Security Management Act of 2014 (FISMA2014、FISMA Reform)[2]	OMB、NIST	後継
2		OMB Circular A-130, “Managing Information as a Strategic Resource” [3]	OMB、NIST	―
3		Information Technology Management Reform Act (Clinger-Cohen Act)[5]	OMB、NIST	更新無
4	暗号政策・設置法	National Institute of Standards and Technology Act (NIST Act)[4]	NIST	―
5		NSD 42, “National Policy for the Security of National Security Telecommunications and Information Systems” [6]	NSA	更新無
6		CNSS Policy No.3, “National Policy for Granting Access to U.S. Classified Cryptographic Information” [7]	NSA	更新無
7		Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information” [8]	NSA	更新無
8	輸出入規制	Export Administration Act of 1979 (EAA)[9]、 Export Control Reform Act of 2018 (ECRA)[10]	商務省	廃止、 ―
9		Export Administration Regulation (EAR)[11]	商務省	後継
10		John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA2019)[12]	商務省等	―
11		Arms Export Control Act of 1976 (AECA)[13]、 The International Traffic in Arms Regulations (ITAR)[14]	国務省	更新無、 ―
12	政府調達	CNSS Policy No. 11, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products” [15]	NIAP、NSA	更新無
13		Memorandum for Chief Information Officers – Security Authorization of Information Systems in Cloud Computing Environments[16]	国防総省、 DHS、GSA	―
14	標準・基準	FIPS140-3, “Security Requirements for Cryptographic Modules” [17]	NIST	後継
15		DoDI 5205.8, “Access to Classified Cryptographic Information” [24]、DoDD 5143.01[19]等	国防総省	後継、 後継
16		SP 800-53 Rev. 5, “Security and Privacy Controls for Information Systems and Organizations” [33]	NIST	―
17	その他	Securities Clarity Act[25]、 Digital Commodity Exchange Act of 2020[26]、 Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets[27]	財務省、金融犯罪捜査網等	―、 ―、 ―
18		Electronic Signatures in Global and National Commerce Act (ESIGN Act)[28]、 Uniform Electronic Transactions Act (UETA)[29]	商務省、 財務省、 司法省 等	―、 ―
19		SP 800-88 Revision 1, “Guidelines for Media Sanitization” [36]	NIST	―
20		NISTIR 8105, “Report on Post-Quantum Cryptography” [37]	NIST	―

21		NISTIR 8114, “Report on Lightweight Cryptography” [38]	NIST	―
22		DA PAM 25-2-16, “Information Management: Army Cybersecurity Communications Security (COMSEC)” [39]	国防総省	―
23		Health Insurance Portability and Accountability Act of 1996 (HIPAA) [40]、 SP 800-66 Rev. 1, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule” [42]	保健福祉省、 NIST	―、 ―
24		NISTIR 8200, “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)” [43]	NIST	―

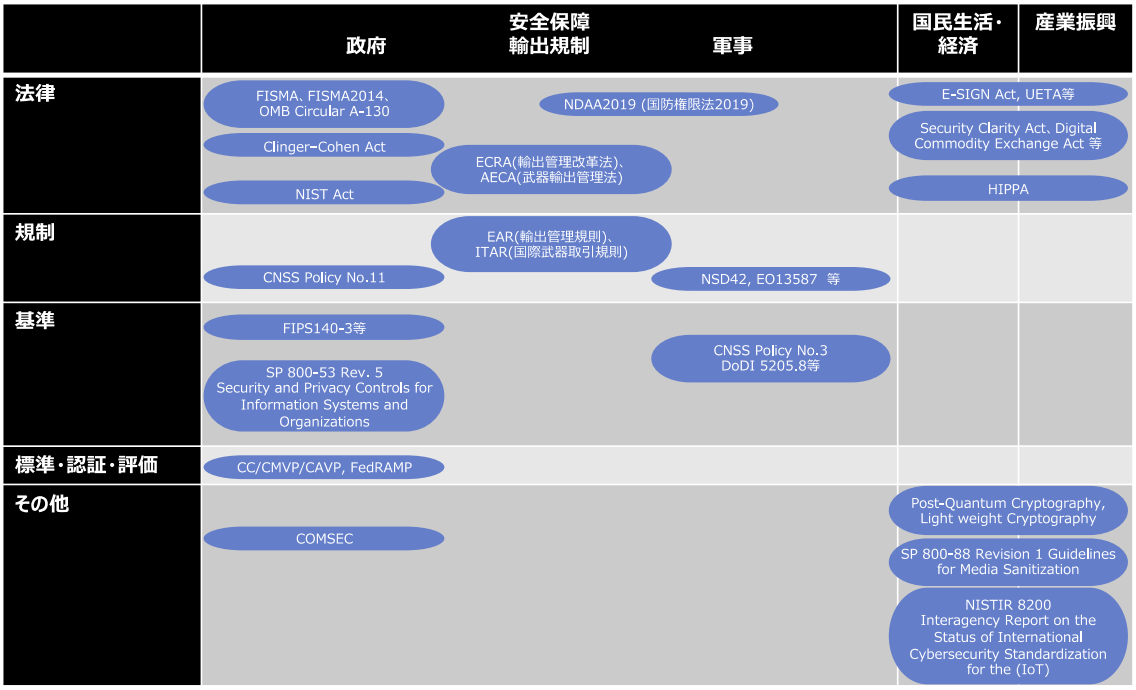


図 3-2　米国における暗号関連政策マップ

- Federal Information Security Management Act of 2002 (FISMA、連邦情報セキュリティ管理法) [1]、Federal Information Security Management Act of 2014 (FISMA2014、FISMA Reform、連邦情報セキュリティ近代化法) [2]

  FISMA は 2002 年 12 月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。2014 年 12 月、FISMA2014 を制定し FISMA を修正した。情報セキュリティの概念を更新、対象機関・組織を拡大するとともに、国土安全保障省に各機関・組織のセキュリティポリシー実施の管理や支援、連邦情報セキュリティ・インシデントセンターの設置などの権限を与え、情報セキュリティの強化等が行われた。

- OMB Circular A-130, “Managing Information as a Strategic Resource”（戦略資源としての情報管理）[5]
  OMB は連邦政府機関に対し、FISMA が連邦政府機関に求める情報リソース保護方針に対する具体的な方針の対策を指示する。Circular A-130 は、1985 年に発行され幾度か改正されてきた。2016 年の改正で連邦政府機関に対し FISMA への対応の強化を求めている。

- Information Technology Management Reform Act（Clinger-Cohen Act、情報技術管理改革法）[3]
  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。
  なお、2014 年度調査の後、改正は行われていない。

- National Institute of Standards and Technology Act（NIST Act）[4]
  NIST を設置し、その目的や機能、活動等について包括的に定めている。1901 年に NIST の前身である国立標準技術研究所（NBS: National Bureau of Standards）の設置法が制定され、1988 年の改正で組織の役割と責任を拡大するとともに NIST へ改名した。目的や活動等の変更に伴い度々改正されている。

- NSD 42, “National Policy for the Security of National Security Telecommunications and Information Systems”[6]
  CNSS の前身である NSTISSC を設立し、国家安全保障システム（NSS）に関する運用ポリシーやガイドライン等の策定を求めるなど、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。
  なお、2014 年度調査の後、改定は行われていない。

- CNSS Policy No.3, “National Policy for Granting Access to U.S. Classified Cryptographic Information”[7]
  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。暗号化された秘密あるいは極秘の情報に対するアクセス権は、アクセスが必要となる立場で一定の基準を満たす者にのみ与えられるものとする暗号アクセスプログラムの確立と確実な実施を、連邦政府部門・機関・契約者業者に義務付ける。
  なお、2014 年度調査の後、改定は行われていない。

- Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information”[8]
  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。具体的には以下を定める。
  - 機密扱いネットワークの運用及び利用機関代表の責任
  - 上級情報共有保護運営委員会及び機密情報共有保護オフィス設置
  - ネットワーク上の機密情報保護執行代理人に国防長官及び NSA 長官を指定
  - インサイダー脅威プログラムの開発を行うインサイダー脅威タスクフォースの設立

  なお、2014 年度調査の後、改定は行われていない。

- Export Administration Act of 1979（EAA、輸出管理法）[9]、Export Control Reform Act of 2018（ECRA、輸出管理改革法）[10]
  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、具体的な規制内容は輸出管理規則（EAR: Export Administration Regulation）で定めている。なお輸出管理法は、1994 年に失効した後、大統領令及び国際緊急経済権限法により EAR の運用が継続された。2018 年 8 月、輸出管理改革法が国防権限法の一部として制定され、EAR の法制化、規制の強化等が行われた。

- Export Administration Regulation（EAR、輸出管理規則）[11]
  輸出管理改革法に基づき、商務省産業安全保障局（BIS: Bureau of Industry and Security）[3]が実施するデュアルユース品目の輸出・再輸出・国内移転の規制を定めた規則である。輸出規制対象は規制品目リスト（CCL: Commerce Control List）[4]、貿易相手として好ましくないと判断された国外の組織・個人はエンティティリスト（Entity List）[5]で管理する。CCL にはワッセナー・アレンジメント基づく規制品が含まれ、暗号技術に関する品目が含まれる。EAR は随時更新される。これについて、3.1.3.4 節に記載する。

- John S. McCain National Defense Authorization Act for Fiscal Year 2019（NDAA2019、国防権限法（2019））[12]
  国防権限法は、国防総省の年間予算・支出を定めるため会計年度毎に可決・制定する連

[3] https://www.bis.doc.gov
[4] https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl
[5] https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

邦法である。2019 年度の国防権限法は、輸出管理改革法、外国投資リスク審査現代化法、中国企業の通信・監視等の機器・サービスの購入・利用の禁止と、それらを利用している企業等との契約を禁止する規定を含み、輸出入及び外国投資に対する規制を強化している。

- Arms Export Control Act of 1976（AECA、武器輸出管理法）[13]、The International Traffic in Arms Regulations（ITAR、国際武器取引規則）[14]
  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から権限を委任された国務長官の同意を要する。実施細目は国際武器取引規則で定められ、国務省国防貿易管理局がこれに基づき規制を管轄する。規制対象品目は、米国軍需品リスト（USML: The United States Munitions List）[6]で管理され、随時更新される。USML には暗号デバイス、ソフトウェア、コンポーネントが含まれる。

- CNSS Policy No. 11, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products”[15]
  国家安全保障システムの情報保護に使用する製品を調達する場合、COTS 製品[7]の場合は NIAP[8]の認証（CCEVS）を得たもの、GOTS 製品[9]の場合は NSA による評価・認証を得たもの、COTS 製品が選択できない場合のみ GOTS 製品を選択することを求めている。

- Memorandum for Chief Information Officers – Security Authorization of Information Systems in Cloud Computing Environments[16]
  連邦政府機関が利用するクラウド製品やサービスのセキュリティ評価・承認・継続的監視を標準化・共通化するプログラム、 FedRAMP（Federal Risk and Authorization Management Program）の実施について定めた OMB の覚書書である。これについて、3.1.3.7 節に記載する。

- FIPS 140-3, “Security Requirements for Cryptographic Modules”[17]
  NIST が定める暗号モジュールの評価のためのセキュリティ要件を規定する米国連邦情報処理標準であり、暗号モジュール認証制度（CMVP: Cryptographic Module Validation）は本標準に基づく制度である。2019 年 3 月に FIPS 140-2 からの改定として公開され同 9 月に有効となった。これに伴い、テスト要件などを定めた SP 800-140 サブシリーズ

[6] https://www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_itar_landing
[7] 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。
[8] 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 Criteria)に基づく情報セキュリティ製品の認証を実施する。
[9] GOTS (Ggovernment 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。

文書も更新されている。
FIPS 140-3 の最大の変更点は、国際標準規格 ISO/IEC 19790:2012（暗号モジュールのセキュリティ要件）、ISO/IEC 24759:2017（暗号モジュールのセキュリティ試験要件）の採用にあり、これにより国際標準への準拠が達成された。

- SP 800-57, “Recommendation for Key Management”[20]、SP 800-131A, “Transitioning the Use of Cryptographic Algorithms and Key Lengths”[21]
  SP 800-57 は暗号鍵の管理に関する三部構成のガイドラインであり、第一部に、暗号鍵の安全強度と鍵長の関係、暗号有効期間（Cryptoperiod）、保護要件等の説明がある。また、SP 800-131A は、より強力なアルゴリズムと鍵長への移行のためのガイドラインであり、推奨アルゴリズムと鍵長について示している。これについて、3.1.3.1 節で説明する。

- DoDI 5205.8, “Access to U.S. Classified Cryptographic Information”[24]、DoDD 5143.01, “Under Secretary of Defense for Intelligence and Security (USD(I&S))”[19]等
  DoDI 5205.8 は CNSS Policy No.3 の施行令であり、国防総省が所有・管理・作成した、もしくは国防総省のために作成された米国の機密暗号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。
  1991 年 2 月、DoDD 5205.8 として公開され、2007 年 11 月に DoDI 5205.8 へ変更・改訂、2020 年 9 月に改訂されている。いずれも管理上の理由によるものとなっている。
  一方、DoDD 5143.01 は、情報・安全保障担当国防次官の責任、機能、関係、権限を割り当てる国防司令であり、国防長官に代わり情報機関・安全機関の監督を行うと定め、機密情報へのアクセス管理の実施の監督等を行うとしている。
  2005 年 11 月に公開され、2014 年 10 月の改定で情報・安全保障担当国防次官の役割が改められた後、管理上の理由による改定が行われている。

- Securities Clarity Act[25]、Digital Commodity Exchange Act of 2020[26]、Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets[27]
  暗号資産の規制に関する 2020 年に提出された法案及び、金融犯罪捜査網・財務省が発表した規制案である。これについて、3.1.3.8 節に記載。

- Electronic Signatures in Global and National Commerce Act (ESIGN Act)[28]、Uniform Electronic Transactions Act (UETA)[29]等
  米国の電子署名法。連邦法の ESIGN 法は主に州間及び海外向け、UETA は各州が制定す

る統一州法であり州内に適用される。いずれも電子署名を定義し、紙の書類上の署名と同等の法的効力を持つと定めている。これについて、3.1.3.9 節に記載する。

- SP 800-53 Rev.5, “Security and Privacy Controls for Information Systems and Organizations”[33]
  組織や情報システムのセキュリティとプライバシーのリスク管理策をカタログ形式でまとめたものである。リスク策方法の中に暗号技術を利用するものが含まれている。FISMA、FedRAMP、HIPPA、国防総省のリスク管理フレームワーク等から参照されている。

- DoDI 8500.01, “Cybersecurity”[34]
  国防総省におけるサイバーセキュリティに関するポリシーを規定。機密情報や、国防総省が扱う情報を保護するための暗号アルゴリズムについての規定が含まれている。

- SP 800-88 Rev.1, “Guidelines for Media Sanitization”[36]
  組織やシステムの所有者が情報を消去する際、情報の機密性の分類に基づいて実用的な方法を選択するためのガイドラインである。暗号化消去（Cryptographic Erase）の説明が含まれている。

- NISTIR 8105, “Report on Post-Quantum Cryptography”[37]
  量子計算と耐量子計算機暗号の現状をまとめ、NIST による耐量子計算機暗号の標準化計画を説明した文書である。NIST による耐量子計算機暗号の標準化作業について 3.1.4.2 節で説明する。

- NISTIR 8114, “Report on Lightweight Cryptography”[38]
  軽量暗号についてのまとめと、NIST による標準化計画の説明した文書である。NIST による軽量暗号の標準化作業について、3.1.4.3 節で説明する。

- DA PAM 25-2-16, “Information Management: Army Cybersecurity Communications Security (COMSEC)”[39]
  機密情報を扱うことが認められた通信システム COMSEC の、米陸軍での利用・運用にあたっての手順を説明している。COMSEC についての情報は非公開のため詳細は不明であるが、このパンフレットから、その概要を垣間見ることができる。これについて、3.1.3.3 節で説明する。

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)[40]、SP 800-66 Rev.1, “An Introductory Resource Guide for Implementing the Health

Insurance Portability and Accountability Act (HIPAA) Security Rule”[42]
HIPAA は、医療の電子化の促進を目的として制定された連邦法。医療情報保護のためのプライバシールール及びセキュリティルールの国家基準策定を義務付けている。セキュリティルールのガイドとして SP 800-66 Rev.1 が策定されており、NIST の標準やガイドライン文書への対応を示している。

- NISTIR 8200, “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)”[43]
  IoT セキュリティについて国際的な標準化状況の調査結果レポートである。軽量暗号標準 ISO/IEC 29192 シリーズ Lightweight Cryptography を紹介している。

なお、前回の調査報告書に記載されていた以下の情報は、現在の暗号政策やサイバーセキュリティ政策とは関係がなかったことが分かった。

- 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が、1987 年に廃止されていた。

- DoDI 5025.01, “DoD Issuances Program”[18]
  DoD の発行物の作成、調整、承認、発行、レビュー方針の確立、責任の割り当てについて定めるものであり、暗号政策やサイバーセキュリティ政策とは関係がなかった。

3.1.3. 暗号に関わる各種制度、規制及びガイドライン

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(Federal Information Processing Standards)及び SP (Special Publication) 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。

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おり、SP 800-57 及び SP 800-131A に暗号移行方針が定められている[10]。これによれば、2021 年 1 月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。

また、NSA は、CNSA Suite（Commercial National Security Algorithm Suite）と呼ばれる暗号スイートを公開している[35]（表 3-4）。NIST が標準化・推奨した暗号アルゴリズム等から構成され、連邦政府の機密情報保護に利用できるもとして NSA が承認しているもので、国防総省は、機密情報だけでなく、国防総省の情報保護のために CNSA Suite の使用を求めている[34]。

表 3-2　米国において利用すべき暗号方式を定めた規格（2021 年 2 月）

規格番号	名称
FIPS 180-4	Secure Hash Standard (SHS)
FIPS 186-4	Digital Signature Standard (DSS)
FIPS 197	Advanced Encryption Standard (AES)
FIPS 198-1	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 202	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques
SP 800-38A Addendum	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
SP 800-38B	Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
SP 800-38E	Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices
SP 800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
SP 800-56A	Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography

[10] NIST が公開する文書はリビジョンを含めて管理されている。本報告書においては、リビジョンの指定が無い場合、最新のものを指すものとする。

SP 800-56B	Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography
SP 800-56C	Recommendation for Key-Derivation Methods in Key-Establishment Schemes
SP 800-57 Part1,2,3	Recommendation for Key Management
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-131A	Transitioning the Use of Cryptographic Algorithms and Key Lengths
SP 800-185	SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash

表 3-3　米国にて利用可能な暗号方式及び鍵長（2021 年 1 月）

種別	名称	備考
暗号化・復号	Two-key TDEA	暗号化は利用禁止、復号はレガシーユース[11]としてのみ利用可
	Three-key TDEA	暗号化は 2024 年以降利用禁止(2023 年までは限定的に利用可)、復号はレガシーユースとしてのみ利用可
	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としてのみ利用可
電子署名	RSA	2048 ビット以上が利用可、 1024～2048 ビットは署名検証のレガシーユースとしてのみ利用可
	DSA	(L, N)=(2048, 224)、(2048, 256)、(3072, 256)が利用可、 512≦L<2048 もしくは 160≦N<224 は署名検証のレガシーユースとしてのみ利用可
	ECDSA	224 ビット以上が利用可、 160～224 ビットは署名検証のレガシーユースとしてのみ利用可
Diffie-Hellman と MQV 鍵共有	有限体上の SP 800-56A DH と MQV スキーム	セキュリティ強度が 112 ビット以上で、次の条件を満たすものが利用可: ・ SP 800-56A 付録 D 掲載の安全素数のグループのリストを使用、もしくは、 ・ FIPS 186 形式のドメインパラメータ(112 ビットセキュリティ強度のみ): (len(p), len(q))=(2048, 224) もしくは (2048, 256)を使用
	楕円曲線上の SP 800-56A DH と MQV スキーム	セキュリティ強度が 112 ビット以上で、次の条件を満たすものが利用可:

[11] 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

		・ SP 800-56A に記載されている曲線を使用、もしくは、 ・ 「Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program」の A.2 の要件を満たす曲線を使用
RSA 鍵共有と鍵配送	SP 800-56B 鍵共有・鍵転送スキーム	len(n)≧2048 が利用可
	SP 800-56B 非準拠鍵共有・鍵転送スキーム	PKCS1-v1_5 パディングが 2023 年以降の利用禁止 (2013 年までは限定的に利用可)
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としてのみ利用可、 電子署名以外の用途は利用可
	SHA-2	SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、 SHA-512/256 のいずれも利用可
	SHA-3	SHA3-224、SHA3-256、SHA3-384、SHA3-512 のいずれも利用可
	TupleHash, ParallelHash	TupleHash は、複数の入力から任意長のハッシュ値を求める用途に限定して利用可、 ParallelHash は、非常に長い入力から並列処理により効率的に任意長のハッシュ値を求める用途に限定して利用可
メッセージ認証コード	HMAC	生成は鍵長 112 ビット以上が利用可 検証は鍵長 112 ビット以上が利用可、112 ビット未満はレガシーユースとしてのみ利用可
	CMAC	生成は、 ・ Two-key TDEA ベースは禁止、 ・ Three-key TDEA ベース 2024 年以降の暗号化は利用禁止（2023 年までは限定的に利用可） ・ AES ベースは利用可 検証は、 ・ Two-key TDEA ベース、Three-key TDEA ベースはレガシーユースとしてのみ利用可、 ・ AES ベースは利用可
	GMAC	生成、検証ともに AES ベースは利用可
	KMAC	生成、検証ともに鍵長 112 ビット以上が利用可

表 3-4　米国 NSA が定める暗号スイート「CNSA Suite」

アルゴリズム	種別	仕様	パラメータ
AES	暗号化・復号	FIPS 197	256 ビット
ECDH	鍵共有	SP 800-56A	P-384 曲線
ECDSA	署名	FIPS 186-4	P-384 曲線
SHA-3	ハッシュ関数	FIPS 180-4	SHA-384
DH	鍵共有	RFC 3526	3072 ビット以上
RSA	鍵共有	SP 800-56B Rev. 1	3072 ビット以上
RSA	署名	FIPS 186-4	3072 ビット以上

3.1.3.2.　セキュリティ製品認証制度・セキュリティサービス認証制度

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試験・認証制度（CMVP）とコモンクライテリア認証制度（CC）であり、CMVP と関連して暗号アルゴリズム試験制度（CAVP）が実施されている。連邦政府は FISMA 等に基づき CMVP 及び 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。

- 暗号モジュール試験・認証制度[12]（CMVP: Cryptographic Module Validation Program）
  CMVP は、1995 年に NIST が開始した、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）の試験・認証制度である。暗号モジュールのセキュリティ要件は NIST が策定した FIPS 140-3, “Security Requirements for Cryptographic Modules” で規定されている。FIPS 140-3 は、国際標準 ISO/IEC 19790:2012（暗号モジュールのセキュリティ要件）、ISO/IEC 24759:2017（暗号モジュールのセキュリティ試験要件）を参照する。

- 暗号アルゴリズム試験制度[13]（CAVP: Cryptographic Algorithm Validation Program）
  CAVP は NIST が実施する、暗号アルゴリズム（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制度である。CMVP 認証の取得に CAVP 認証の取得が求められる。CAVP 認証のみを取得することも可能である。

[12] https://csrc.nist.gov/projects/cryptographic-module-validation-program
認証取得モジュールを検索・一覧表示: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search
[13] https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program
認証取得アルゴリズムを検索・一覧表示: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation-search

- コモンクライテリア認証制度[14]（CC: Common Criteria）
  CC 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た、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制度である。NSA と NIST の共同プログラムである NIAP（National Information Assurance Partnership）が運営する。評価基準は ISO/IEC 15408（IT セキュリティ評価基準）として国際標準化されている。また、コモンクライテリア承認アレンジメント（CCRA: Common Criteria Recognition Arrangement）を通して、加盟国間で評価結果の相互承認が行われている。

これらの試験・認証制度について、所管、認証機関、評価機関、認証件数を表 3-5 に示す。

表 3-5　米国の認証制度と関連する機関（2021 年 2 月）

	CMVP	CAVP	CC
所管	NIST	NIST	NIST, NSA
認証機関	NIST	NIST	NIAP
評価機関	• Acumen Security • ADVANCED DATA SECURITY • AEGISOLVE, Inc. • Asia Pacific IT Laboratory, TUV NORD • atsec information security corporation • Booz Allen Hamilton Cyber Assurance Testing Laboratory • Cisco Systems Automated Cryptographic Validation Protocol Lab • COACT, Inc. Labs • CyberSecurity Malaysia Cryptographic Evaluation Laboratory • CygnaCom Solutions, Inc. • Dekra Testing and Certification S.A.U. • ECSEC Laboratory Inc. • EWA - Canada • Gossamer Security Solutions • IT Security Center		• Acumen Security • Atsec information security corporation • Booz Allen Hamilton Common Criteria Testing Laboratory • CygnaCom Solutions, Inc • Gossamer Security Solutions • Leidos Common Criteria Testing Laboratory • UL Verification Services Inc.

[14] https://www.niap-ccevs.org
認証取得製品を検索・一覧表示: https://www.niap-ccevs.org/Product/index.cfm

	• Leidos Accredited Testing & Evaluation (AT&E) Lab • Lightship Security Inc. • Penumbra Security, Inc. • SERMA SAFETY AND SECURITY • TUViT Evaluation Body for IT-Security • UL Verification Services, Inc.		
認証件数	2020 年 242 件 2019 年 358 件 2018 年 428 件	2020 年 1590 件 2019 年 1293 件 2018 年 4642 件	2020 年 101 件 2019 年 112 件 2018 年 101 件

※ CC の認証件数は「国内向け認証」と「CCRA 向け認証」の合計。

※ 認証件数は、それぞれの制度のウェブページが公開する認証製品リストに掲載された製品や技術の認証取得日より集計した。同一の製品が認証を再取得した場合、認証取得日が最新の日付で更新され過去の認証取得日を参照できないため、表の値は実際の認証件数より多少なくなっている。

なお、調査時点（2021 年 2 月）で CC Portal に掲載されている CCRA 向けの有効な CC 認証取得は、114 製品である。以下に認証取得と EAL を示す。

表 3-6 EAL ごとの Common Criteria 認証取得数（米国）[15]

EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	N※	Total
0	0	0	0	0	0	0	0	0	0	0	0	0	114	114

※N（None）: EAL の表記がない認証である。

3.1.3.3. 政府の調達要件

連邦政府機関は FISMA を根拠として、情報セキュリティ確保のために、NIST の定める標準やガイドラインに従うことが義務付けられている。これに基づき GSA は政府調達において、NIST の標準やガイドラインに準拠した製品の調達を行う[16]。

また、CNSS Policy No. 11 により 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。

[15] Certified Products List - Statistics : New CC Portal https://www.commoncriteriaportal.org/products/stats/
[16] Federal Acquisition Regulation, Part 7, Subport 7.1, Section 7.103 (w).

- National Security Directive 42
- CNSS Policy No.11
- CNSS Directive (CNSSD) 502, “National Directive on Security of National Security Systems”
- DoDD 5100.20, “National Security Agency/Central Security Service”
- DoDI 8500.01, “Cybersecurity”

なお、2014 年度調査報告書に掲載の「DoDD 8500.01E, “Information Assurance”」は「DoDI 8500.01, “Cybersecurity”」へ管理上の理由により更新。また、「DoDI 8500.02 “Information Assurance Implementation”」は 2019 年 10 月に廃止となっている。

2011 年 12 月に OMB が公表した覚書書[16]により FedRAMP（Federal Risk and Authorization Management Program）が開始された。FedRAMP はクラウド製品・サービスの安全性の評価・承認、継続的監視制度であり、連邦政府機関を通して評価基準・制度を統一することで、基準を明確化、評価手続きを簡略化する。事業者は、連邦政府に提供するクラウド製品やサービスに FedRAMP 認証取得が義務付けられ、連邦政府は承認済みのサービス・製品の調達が義務付けられる。評価基準として SP 800-53 [33]が用いられる。

COMSEC Equipment は、連邦政府の機密情報を扱うことが認められている機器や部品であり、NSA の製品タイプ分類における Type1（機密指定の国家安全情報を扱うもの）、Type 2（機密指定されていない国家安全情報を扱う）に該当する[17]。これらの機器は NSA の管理の元で開発が行われ、NSA が承認する。

COMSEC は、NSA が承認した暗号アルゴリズムの利用が義務付けられているが、その詳細は、アルゴリズムだけでなく COMSEC 自体が非公開であるため把握することができない。NIST が標準化・推奨している暗号が一部採用されている、NSA の開発した独自の暗号アルゴリムが利用されているなどという情報もあるが、定かではない。

3.1.3.4. 暗号の輸出入規制

米国においては暗号の輸入は規制せず、暗号の輸出を規制する。暗号規制の考え方は 1994 年に終了した COCOM[18]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）[19]に基づいている。

---

[17] CNSSI No. 4009, National Information Assurance (IA) Glossary の「Commercial COMSEC Evaluation Program (CCEP)」の説明で、COMSEC と Type 1, 2 の対応を確認できる:
https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

[18] COCOM：Coordinating Committee 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。

[19] ワッセナー・アレンジメント (Wassenaar Arrangement)は COCOM の後継として合意された協定で、すべての国家・地域及びテロリスト等を対象とした輸出管理の協定。

暗号製品の輸出規制は商務省産業安全保障局が行なう。規制の内容は、輸出管理改革法に基づき定められた管理規則、EAR[20]に定められている。

EAR は規制品目リストである CCL と、貿易相手として好ましくないと判断された国外の組織・個人を管理するエンティティリスト[21]を含む。CCL はワッセナー・アレンジメントに基づく規制品目を含み、そこに暗号製品が含まれる。EAR は随時更新され連邦官報（Federal Register）で公表され、また、商務省産業安全保障局のウェブページにも掲載される。

2021 年 2 月時点の CCL[22]は 10 のカテゴリに分類され、2019 年 12 月のワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）[23]」のなかのデュアルユース製品・技術に関するリストの各カテゴリにほぼ対応して作られている。そのなかで、デュアルユース製品・技術に関するリストのカテゴリ 5 パート 2（Category 5 Part II - Information Security）をベースに、輸出規制対象となる暗号製品を定めている。その概要は以下のようなものとなっている。

- 後に示す要件を満たす暗号アルゴリズムをデータの機密性確保のために使用し、暗号機能が、安全な「暗号アクティベーション」以外の手段で、利用できるようにされるかアクティベートされている、あるいはアクティベートすることができる以下の製品
  - 情報セキュリティを主な機能とする製品
  - デジタル通信、ネットワークシステム、機器、コンポーネント
  - コンピュータ、情報の保存・処理を主な機能等する製品、コンポーネント
  - 後に示す要件を満たす暗号アルゴリズムがデータの機密性確保のために利用され、暗号製品の主機能以外をサポートし、独立型の組み込み機器もしくはソフトウェアとして動作する製品
- 暗号アクティベーショントークン
- 量子暗号（量子鍵配送）を利用または実行する機器
- 暗号を利用した超広帯域無線通信機器
- 暗号を利用した拡散コードを用いたスペクトラム拡散装置

- 暗号アルゴリズムの要件
  - 共通鍵暗号アルゴリズム: 鍵長 56 ビット以上

[20] https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear
[21] https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list
[22] https://www.federalregister.gov/documents/2020/10/05/2020-18334/implementation-of-certain-new-controls-on-emerging-technologies-agreed-]at-wassenaar-arrangement-2019
[23] Public Documents, Vol II - List of Dual-Use Goods and Technologies and Munitions List: https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-II-2020-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-20-3.pdf

- 公開鍵暗号アルゴリズム:
  - 因数分解ベース: 512 ビット以上
  - 有限体の乗法群における離散対数ベース: 512 ビット以上
  - 上記以外の群上の離散対数ベース: 112 ビット以上
- 耐量子計算機暗号アルゴリズム
  - 格子の最短ベクトル・最近ベクトル問題ベース
  - 超特異楕円曲線の同種写像問題ベース
  - ランダム符号の復号問題ベース

なお、公開済みのソフトウェアや、マスマーケット品等は管理対象外とされる。

ただし、公開済みのソフトウェアは、事前にソースファイルの場所もしくはソースファイルそのものを、NSA 及び商務省産業安全保障局へメールで通知する必要がある。

また、マスマーケット品については、使用する共通鍵暗号アルゴリズムの鍵長が 64 ビット以上、公開鍵暗号アルゴリズムで因数分解ベース、有限体の乗法群における離散対数ベースの場合の鍵長が 768 ビット以上、それ以外の離散対数ベースの場合の鍵長が 128 ビット以上の場合、BIS に分類要求、もしくは自己分類報告書を提出する必要がある。

CCL の元となるワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト」は、「デュアルユース製品・技術のリスト」と「軍需品リスト」の 2 つのパートから構成され、「デュアルユース製品・技術のリスト」は 9 のカテゴリ、機密リスト、特別な機密リストから成る。暗号製品や技術の管理について、「デュアルユース製品・技術のリスト」のカテゴリ 5 のパート 2(Category 5 – Part 2 “Information Security”)で定められている。

ワッセナー・アレンジメントの「デュアルユース製品・技術のリスト」のカテゴリ 5 のパート 2 と CCL のカテゴリ 5 のパート 2 の内容を比較したところ、基本的に一致し、以下のような相違点があった。

- 管理対象外製品の条件が CCL で詳細化
  - パーソナル無線ネットワークの機密性を確保する製品のうち、仕様上の動作範囲が 30m を超えない、もしくは 7 台以上の機器と接続できないもので 100m を超えないものは管理対象外とする項目を追加
- EAR に基づく輸出管理を実施するための情報や参照を CCL で追加
  - 最終用途が軍事目的の CPU 及びソフトウェアや技術の輸出管理情報への参照を追加
  - 関連する管理項目や利用できる許可制度の情報や参照を追加

なお、前述の CCL における、公開済みのソフトウェアの通知、マスマーケット品の BIS への分類要求・分類報告書提出は、EAR に基づくものであり、ワッセナー・アレンジメントの「デュアルユース製品・技術のリストはそのような規定を含まない。

一方、武器輸出管理法、国際武器取引規則に基づき、軍需品の輸出規制も行われている。暗号デバイス、ソフトウェア、およびコンポーネントが規制対象に含まれている。

以下に、2020 年 12 月のワッセナー・アレンジメント会議で合意されたデュアルユース製品・技術のリスト[24]の Category 5 Part 2 に記載している規制の対象となる暗号技術の抜粋を示す。

Category 5 Part 2 に記載の規制対象となる暗号技術の抜粋

5.A.2.a
以下の情報セキュリティシステム、機器、及びコンポーネント
a　該当するセキュリティアルゴリズムを有する「データの機密性のための暗号」を使用するように設計又は変更されたもので、暗号機能が、安全な「暗号アクティベーション」以外の手段で、利用できるようにされるかアクティベートされている、あるいはアクティベートすることができるもの。
1. 情報セキュリティを主な機能とするもの。
2. 5.A.2.a.1.に規定されてない、デジタル通信、またはネットワークシステム、機器、コンポーネント。
3. 5.A.2.a.1.または 5.A.2.a.2.に規定されていない、コンピュータ、情報の記憶・処理を主な機能とするその他の物品、コンポーネント。
4. 5.A.2.a.1.～5.A.2.a.3.に規定されていない物品で、該当するセキュリティアルゴリズムを有する「データの機密性のための暗号」が以下の全てを満たすもの。
    a. 物品の主機能でないものをサポートするもの。
    b. カテゴリ 2 Part2 で規定される、独立型の組み込み機器、あるいはソフトウェアにより実施されるもの。

テクニカルノート:
1. 「データの機密性のための暗号」とは、デジタル技術を用いて以下のいずれかの暗号機能を実行する暗号である。
    a　認証

[24] Public Documents, Vol II - List of Dual-Use Goods and Technologies and Munitions List: https://www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-II-2020-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-20-3.pdf

b　デジタル署名

c　データの完全性保護

d　否認防止

e　コピー保護ソフトウェアの実行を含むデジタル著作権管理

f　娯楽、商業放送あるいは医療記録管理のサポートのための暗号化・復号

g　上記 a.から f.に記載される機能をサポートする鍵管理。

2. 該当するセキュリティアルゴリズムとは、以下のいずれかである。

a　パリティビットを含まず、56 ビットを超える鍵長を持つ対称アルゴリズム。

b　以下のいずれかのアルゴリズムのセキュリティに基づく非対称アルゴリズム。

1. 512 ビットを超える整数の因数分解（例： RSA）
2. 512 ビットを超える有限体の乗法群における離散対数の計算（例： Diffie-Hellman over Z/pZ）
3. 112 ビットを超える、上記 2 以外の群における離散対数(例: 楕円曲線 Diffie-Hellman 鍵共有）

c　以下のいずれかアルゴリズムのセキュリティに基づく非対称アルゴリズム。

1. 格子暗号における最短ベクトル・最近ベクトル問題（例： NewHope, Frodo, NTRUEncrypt, Kyber, Titanium）
2. 超特異楕円曲線間の同種写像（例： 超特異同種写像鍵カプセル化）
3. ランダム符号の復号（例： McEliece、Niederreiter）

Note 1

輸出元の国の管轄当局により必要と判断された場合は、以下のいずれかを立証するために、管轄当局が物品の詳細にアクセスできるようにするか、提供しなければならない。

a　物品が 5.A.2.a.1.から 5.A.2.a.4.の基準を満たすかどうか

b　5.A.2.a に規定されるデータの機密性に関する暗号機能が暗号のアクティベーションなしで利用できるかどうか。

Note 2

以下のいずれかに該当する場合、あるいは、特別に設計された情報セキュリティコンポーネントである場合、5.A.2.a.は適用されない。

a　以下のスマートカードおよびスマートカードリーダ/ライタ

1. スマートカードあるいは以下のいずれかを電子的に読める個人文書（Personal Documents）

a　以下の全てを満たす暗号機能：

1. 以下のいずれかに使用が制限されている。

a　5.A.2.a.1 から 5.A.2.a.4 に記載されない機器またはシステム

b　該当するセキュリティアルゴリズムを有するデータ機密性のための暗号を利用しない機器またはシステム

c　5.A.2.a の注釈の b.から f.で除外された機器またはシステム。

2. 他の用途にプログラムを作り直すことができないもの。

b　以下の全てを有するもの。

1. 保存された個人データの保護を許可するために特別に設計されたもの、あるいは制限されたもの。
2. 公的・商業的取引、あるいは個人の識別のためにパーソナライズされたもの。
3. 暗号機能にユーザがアクセスできないもの。

2. 本 Note の a.1.に規定される物品のために特別に設計・変更された、あるいは制限されたリーダ/ライタ

b　銀行での使用または金銭取引のために特別に設計された、あるいは限定された暗号機器。

c　暗号化されたデータを、直接、他の無線電話・機器（無線アクセスネットワーク（RAN）機器）に送信する機能を持たないもの、あるいは、RAN 機器（無線ネットワークコントローラ（RNC）または基地局コントローラ（BSC））を通じて暗号化されたデータを通信する、民間用のポータブル・モバイル無線電話機（商業用の民間セルラー無線通信システムと利用されるものなど）。

d　end-to-end 暗号機能を持たないコードレス電話機で、ブーストされていないコードレス操作の最大有効範囲（端末とホーム基地局との中継されていない単一のホップ）製造者の仕様に従い 400 メートル未満であるもの。

e　暗号ノート（Category 5 Part 2 Note 3）の a.2.から a.4 の規定を満たし、本来のカスタマイズされていないデバイスの暗号機能に影響を与えない特定の民需産業アプリケーション向けにカスタマイズされた、公開・商用暗号基準（非公開の場合もあるアンチパイラシ機能を除く）のみを実装した民間用のポータブル・モバイル無線電話および同様のクライアント無線デバイス。

f　情報セキュリティ機能が、公開・商用暗号基準のみを実装する無線パーソナルエリアネットワーク機能のみに限定されている物品。

g　暗号ノート（カテゴリ 5 Part 2 Note 3）の a.2 から a.4 を満たし、RF 出力電力が 0.1w（20 dBm）以下に制限されており、16 人以上の同時使用ユーザをサポートする、民間用に設計されたモバイル通信無線アクセスネットワーク（RAN）機器。

h　情報セキュリティ機能が公開・商用暗号基準のみを実装する運用、管理または保守（OAM）のみに限定されている、ルータ、スイッチ、ゲートウェイまたはリレー。

i　情報セキュリティ機能が以下の全てを満たす汎用コンピュータ機器またはサーバ。

1. 公開・商用暗号基準のみを使用する。
2. 以下のいずれかである。

a　Category 5 Part 2 Note 3 の規定を満たす CPU に統合されている

b　5.D.2 に規定されていないオペレーティングシステムに統合されている。

c　機器の OAM に限定される。

j　接続される民需産業アプリケーション用に設計され、以下の全てを満たすもの。

1. 以下のいずれかであること

a　以下のいずれかを満たすネットワークに接続できるエンドポイントデバイス。

1. 情報セキュリティの機能が、非恣意的データの保護、または運用、管理、保守（OAM）に限定されている。
2. デバイスが、特定の接続された民需産業アプリケーションに限定されている。

b　以下の全てを満たすネットワーク機器

1. j.1.a で規定されたデバイスと通信するために特別に設計されている。
2. 情報セキュリティの機能が j.1.a により規定されたデバイスの接続される民需産業用アプリケーションのサポート、あるいは j で規定されるネットワーク機器あるいはその他物品の OAM に限定されている

2. 情報セキュリティ機能が公開。商用暗号基準にのみ実装されており、暗号機能がユーザによって容易に変更されない。

テクニカルノート

1. 接続された民需産業アプリケーションとは、情報セキュリティ、デジタル通信、汎用ネットワーク・コンピューティング以外のネットワークに接続される消費者向けあるいは民需産業アプリケーションである。
2. 非恣意的データとは、システムの安定性、性能または物理的測定（温度、圧力、流量、質量、体積、電圧、物理的位置など）に直接関連するセンサーまたは計測データであり、デバイスのユーザが変更できないものである。

5.A.2.b.

暗号アクティベーショントークン

テクニカルノート

暗号アクティベーショントークンは、以下のいずれかのために設計または変更されたものである。

1. 暗号アクティベーション手段により、Category 5 Part 2 に規定されていないものを 5.A.2.a または 5.D.2.c.1 に規定されるものに変換し、暗号ノート（Category 5 Part 2 Note 3）に公開されていないもの。

2. 暗号アクティベーション手段により、Category 5 Part 2 で既に規定されているもので 5.4.2.a で規定される追加の機能を有効にする。

5.A.2.c.
量子暗号を利用または実行するために設計・変更されたもの。

5.A.2.d.
超広帯域変調技術を使用するシステム向けにチャネライジングコード、スクランブルコードまたはネットワーク識別コードを生成するために暗号技術を使用するために設計・修正され、以下のいずれかを有するもの

1. 500MHz を超える帯域幅
2. 20%以上の比帯域

5.A.2.e.
5.A.2.d で規定されないスペクトラム拡散システムの拡散コードを生成する暗号技術を使用するために設計・変更され、周波数ホッピングシステム向けのホッピングコードを含むもの。

3.1.3.5. プロトコル等での暗号方式

NIST は、連邦政府機関によるネットワークを介した通信のセキュリティリスクの低減を支援するため、TLS の利用・設定ガイドライン及び IPsec のガイドを公表している。

SP 800-52 Rev.2（TLS プロトコルの実装の利用・設定ガイドライン）[22]は、2019 年 8 月に改定、プロトコルバージョンやサポートすべき暗号方式、TLS 拡張等について詳細に説明している。概要は以下の通り。

- プロトコルバージョン
  - 連邦政府専用: TLS1.2 以上
  - 民間との接続あり: TLS1.2 以上（1.0, 1.1 も可）
  - 2023 年末までに TLS1.3 をサポート

- 暗号アルゴリズム
  - FIPS 標準、SP で推奨されているアルゴリズムを使用
  - サーバの場合、暗号モジュールは CMVP 認証取得済み、暗号アルゴリズムは CMVP 認証範囲内のものを利用、
    クライアントの場合、CMVP 認証範囲内のものを利用
  - 安全性: 112 ビットセキュリティ以上

一方、SP 800-77 Rev.1（IPsec VPN のガイド）[23]は、2020 年 6 月に改定版が公開され、VPN や IPsec の仕組み、導入計画・方法、IPsec に代わる選択肢等を紹介している。

3.1.3.6. 暗号利用に関する規則（利用ライセンス・暗号盗聴法など）

米国では、暗号の利用を規制する法令は制定されていないが、合法的に暗号化解除や迂回手段の提供を義務付けようとする動きがある。

- Lawful Access

  近年、エンドツーエンド暗号化技術を利用し、エンドユーザや端末の所有者だけが情報にアクセスできる製品やサービスが増加し、法執行機関の命令といった合法的な権限を持ってしてもコンテンツにアクセスできず、テロや児童虐待などの捜査を妨げることが問題となると法務局等が主張している。

  2020 年 10 月、米国、日本を含む 7 カ国の連盟で“International Statement: End-To-End Encryption and Public Safety”（国際声明:エンドツーエンド暗号化と公共の安全）[25]を発表し、テクノロジー企業に対し以下の 3 点を要求した。

  - 公共の安全を取り込んだシステム設計を行う
  - 可読かつ利用可能な形式で法執行機関によるコンテンツへのアクセスを可能とする
  - 政府やその他の利害関係者と合法的アクセスについての協議を行う

- 2020 年に同一の内容の以下の法案が上院・下院に提出された。2021 年 2 月時点では、いずれの法案も審議が行われていない。

  - H.R.7891[26]、S.4051[27] - Lawful Access to Encrypted Data Act（暗号化データへの合法的アクセス法案）

    暗号化通信及び暗号化ストレージを対象とし、法務行政機関によるコンテンツへのアクセスの支援、事業者がアクセスの支援提供能力を保有することを義務付ける等

3.1.3.7. クラウドサービス

3.1.3.3 節に示した通り、連邦政府機関が利用するクラウド製品・サービスは、FedRAMP 認証の取得が義務付けられている。他にも以下のようなガイドライン等がある。

[25] https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety
[26] https://www.congress.gov/bill/116th-congress/house-bill/7891
[27] https://www.congress.gov/bill/116th-congress/senate-bill/4051

- SP 800-144, “Guidelines on Security and Privacy in Public Cloud Computing”、SP 800-146, “Cloud Computing Synopsis and Recommendations”
  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、及び FIPS 140 を満たす製品の採用を推奨

- SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems”
  クラウドサービスを含む情報管理システムの構成管理において、通信やデータ保存の際に、FIPS140 検証済みの暗号モジュールやアルゴリズムの利用を推奨

3.1.3.8. 暗号資産

米国には、暗号資産を包括的に規制する法令は存在しない。既存の法律に基づいた規則が行われている。

- 暗号資産の取引で得られた損益は税法上の計上の対象となる（米国内国歳入庁（IRS））
  暗号資産の取引所及び管理者は銀行秘密法（Bank Secrecy Act）の対象であり、金融サービス事業の登録が必要（FIN-2013-G001）（FinCEN（Financial Crimes Enforcement Network, 金融犯罪捜査網））

2020 年に以下の 2 件の法案が議会に提出された。2021 年 2 月時点では、いずれの法案も審議が行われていない。

- Securities Clarity Act[28]
  暗号資産は有価証券ではなく、米国証券取引委員会の管理対象では無いことを確認する
- Digital Commodity Exchange Act of 2020[29]
  暗号資産取引所を「デジタルコモディティ取引所」として米国先物取引所の管轄下に置く

また、FinCEN 及び財務省は 2020 年 12 月に、新たなルール策定に向けての意見募集を行った。

[28] https://www.congress.gov/bill/116th-congress/house-bill/8378
[29] https://www.congress.gov/bill/116th-congress/house-bill/8373

- Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets[30]
  銀行及び金融サービス事業者は、金融機関にホストされていないウォレットもしくはFinCENが指定した国の金融機関がホストするウォレットとのトランザクションによる仮想通貨、デジタル資産に対して、一定の条件を満たすものは、顧客の身元確認、取引先の確認、記録保持、報告を求める。

一方、米国の中央銀行発行デジタル通貨（CBDC: Central Bank Digital Currency）、いわゆるデジタルドルについては、米国連邦準備制度理事会（FRB: Federal Reserve Board）が調査・研究を行っているが、早急な実現に向けての動きは見られない。

2020年8月、ボストン連邦準備銀行とMITのデジタル通貨イニシアチブがCBDCに関する技術研究開始について発表している[31]。3年をかけて、架空のCBDCプラットフォームの設計、構築し、テスト、評価を行うとしている。

3.1.3.9. 電子署名法

米国における電子署名は、連邦法のESIGN法[28]、州法のUETA[29], ESRA[30], ECSA[31]の4つの法律により管理されている。

- ESIGN法（Electronic Signatures in Global and National Commerce Act）
  2000年6月施行の連邦法。主に州間及び外国との関係を対象としているが、州内を対象外としていないため、米国全てを対象とする法律となっている。

- UETA（Uniform Electronic Transactions Act）
  ニューヨーク州、イリノイ州を除く全ての州とコロンビア特別区、プエルトリコ、米領バージン諸島が採用する統一州法[32]。1999年7月に、統一州法全国委員会（ULC: The National Conference of Commissioners on Uniform State Laws, The Uniform Law Commission）により策定され、以後、各州・地域が採用。

- ESRA（Electronic Signatures and Records Act）
  ニューヨーク州の電子署名法。2000年3月施行。

[30] https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets
[31] https://www.bostonfed.org/news-and-events/press-releases/2020/the-federal-reserve-bank-of-boston-announces-collaboration-with-mit-to-research-digital-currency.aspx
[32] https://www.uniformlaws.org/committees/community-home?communitykey=2c04b76c-2b7d-4399-977e-d5876ba7e034&tab=groupdetails

- ECSA (Electronic Commerce Security Act)
  イリノイ州の電子署名法。1999 年 7 月に施行。

ESIGN 法も UETA も、電子署名、電子記録の定義を概して以下のように定めている。

- 電子署名: 記録に添付もしくは論理的に関連づけられた電子音・記号・処理であり、記録への署名意思を持つ者が実行もしくは選択したもの
- 電子記録: 電子的な方法で作成、生成、送信、通信、受信、保存された記録

更に、電子署名、電子記録の法的効力について、以下のように規定している。

- 記録・署名は、電子形式であることで、法的効力・強制力を否定されない
- 契約は、電子記録が使われたことで、法的効力・強制力を否定されない
- 法律が紙の記録を要求する場合、電子記録は法律を満たす
- 法律が署名を要求する場合、電子署名は法律を満たす

いずれの法律も、電子署名の有効性を定めるが、暗号技術を用いた電子署名など、技術的な要件を規定しない。暗号技術を用いた電子署名は、これらの法律が定める電子署名の定義にあてはまる技術の一つとして位置付けられる。

ESRA、ECSA のいずれも、電子記録及び電子署名の法的効力を ESIGN や UETA と同様に定めている。ESRA は暗号技術に基づく電子署名についての規定を含み、州は電子証明書及び認証局の基準を定め、基準への準拠を確認する認証制度を実施する事などが定められている。

現在、多くの州がブロックチェーンなどの新しい技術を管理するため UETA の改正を実施、もしくは計画・検討している。そのような動きに対し、統一州法全国委員会は、技術中立性の原則に反することを理由に UETA の改正に反対し、改正せずに対応する方法を示している[32]。

3.1.3.10. 国民 ID 番号制度 (eID)

米国では、米国市民を識別する統一の ID カードは発行されていない。

米国で個人を識別する ID として利用されているものに、以下のようなものがあるが、いずれも電子化されていない。

- 運転免許証、非運転者身分証明書
  連邦政府ではなく州政府が発行するため、州ごとに外観・情報が不統一

- 社会保障番号（SSN: Social Security Number）カード
  米国市民や永住者等に発行される事実上の国民識別番号。顔写真など生態情報と関連づけされていない

運転免許証、非運転者身分証明書は、2005 年に制定された Real ID 法に基づき、登録情報、発行申請時の検証内容等が共通化され、また、州ごとに管理されていたこれらの登録情報データベースを連邦内で共有することが義務付けられた。

また、運転免許証に関して、携帯端末のモバイルアプリケーションを利用したデジタル運転免許証の実験が、Gemalto 社と一部の州及び NIST の協力で実施されている[33]。

社会保障番号については、社会保障局（SSA: Social Security Administration）が、番号、名前、生年月日の組が社会保障記録と一致するか確認するオンラインのサービス（eCBV: Electronic Consent Based Social Security Number Verification）[34]を提供している。

一方、米軍はスマートカード形式の共通アクセスカード（CAC: Common Access Card）[35]を身分証明書として利用している。これは、FIPS 201, “Personal Identity Verification (PIV) of Federal Employees and Contractors”に準拠している。

3.1.4. その他

3.1.4.1. 暗号化消去（Cryptographic Erase）

暗号化消去は、メディアにデータを保存する際、暗号化処理を行う手法である。データを消去する場合、データの暗号化に使用した暗号鍵を削除することで、メディア上の暗号化されたデータ全てを消去する作業が不要になり、消去処理を迅速に行える。SP 800-88 Rev.1, “Guidelines for Media Sanitization”で、仕組みや利用すべき場面などについて説明されている。

3.1.4.2. 耐量子計算機暗号標準化

量子計算技術の向上により、現在利用されている暗号アルゴリズムの危殆化が危惧されている。これに対し、NIST は 2016 年より耐量子計算機暗号アルゴリズムの標準化作業を進めている[36]。標準化の方法は、暗号化・電子署名・鍵共有のための候補となる耐量子計算機暗号アルゴリズムを募集し、セキュリティ、コストとパフォーマンス、アルゴリズムと実装

[33] https://www.nist.gov/itl/applied-cybersecurity/tig/pilots#gemalto
[34] https://www.ssa.gov/dataexchange/eCBSV/
[35] https://www.cac.mil/
[36] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

の特性を基準に複数回の Round で段階的に絞り込むというものであり、以下のスケジュールで作業が進められている。

- 2016 年 8 月 提出要件と評価基準に関するコメント要求
- 2016 年 12 月 耐量子計算機暗号アルゴリズム募集開始
- 2017 年 11 月末 募集終了
- 2017 年 12 月 Round 1 開始
- 2019 年 1 月 Round 2 開始
- 2020 年 1 月 Round 3 開始
- 2021 年 Round 4 開始予定
- 2023-2024 年 最終候補決定、意見募集予定
- 2024 年 標準決定予定

Round 1 には 82 件のアルゴリズムの応募があり、受理されたのは 69 件、Round 1 の絞り込みの結果 26 件が選ばれ、Round 2 で 15 件が残った。そのうちの 7 件が候補、8 件が次候補とされた（表 3-7）。その内訳を表 3-8 に示す。2021 年 2 月時点では Round 3 の結果は公開されていない。

表 3-7　米国 NIST の耐量子計算機暗号標準候補アルゴリズム数の変化

段階	候補アルゴリズム数
応募	82
Round 1 開始	69
Round 2 開始(Round 1 結果)	26
Round 3 開始(Round 2 結果)	15(候補 7、次候補 8)

表 3-8　米国 NIST の耐量子計算機暗号標準 Round 3 候補、次候補一覧

アルゴリズム	公開鍵暗号・鍵共有向け	電子署名向け
格子ベース	候補: CRYSTALS-KYBER、NTRU、SABER 次候補： FrodoKEM、NTRU Prime	候補: CRYSTALS-DILITHIUM, FALCON
符号ベース	候補: Classic McEliece 次候補: BIKE, HQC	
多変数多項式ベース		候補: Rainbow 次候補: GeMSS
ハッシュベース		次候補: Picnic, SPHINCS+
同種写像ベース	次候補: SIKE	

3.1.4.3. 軽量暗号標準化

IoT 機器の普及などに伴い、制約のある環境の限られたリソースでセキュリティを確保する必要があるが、NIST 標準の暗号アルゴリズムではパフォーマンスが許容できない可能性が問題と捉えられるようになった。これに対応するため、NIST は 2015 年から軽量暗号アルゴリズムの標準化を進めている[37]。

標準化の方法は、候補となるアルゴリズムを募集し、暗号学的安全性、制限のある環境での実装の特性（パフォーマンスとコスト）、サイドチャネル攻撃耐性などを基準に選別を行い、複数のラウンドで絞り込むものであり、以下のスケジュールで作業が進められている。

- 2015 年 7 月 軽量暗号研究会第 1 回開催
- 2017 年 5 月 NISTIR 8114 公開
- 2018 年 8 月 募集開始
- 2019 年 2 月 締め切り
- 2019 年 4 月 Round 1 開始
- 2019 年 8 月 Round 2 開始
- 2020 年 12 月 Round 3 開始予定（当初は 9 月の予定）
- 2021 年 最終決定予定

Round 1 に 57 件の応募があり 56 件が受理され、そのうちの 32 件が選ばれ Round 2 の対象となった。2021 年 2 月時点では、Round 2 の結果は公開されていない。

3.1.4.4. HIPAA（Health Insurance Portability and Accountability）

米国では、医療の電子化の促進を目的として 2 つの法令、HIPAA、HITECH Act が制定されている。HIPAA は 1996 年 8 月に制定され、医療情報を同意無く開示されることから保護するための国家基準策定を義務づけた連邦法、HITECH Act は 2009 年 2 月に制定された医療情報の電子化の促進とプライバシーとセキュリティを強化するための連邦法である。

保健福祉省（HHS: Department of Health and Human Services）は、HIPAA に基づき、プライバシールール、セキュリティルールを策定した。

プライバシールールは健康情報の保護、セキュリティルールは電子的に保護された健康情報の保護を目的とした基準となっている。セキュリティルールでは、電子的に保護された健康情報（EPHI: electronic protected health information）を保護するために行わなければならない対策を定めている。対策には、EPHI 保護、リスク分析と管理、アクセスコントロール、コンプライアンス確保が含まれる。

これに対し、NIST は、SP 800-66 Rev.1 を公表している。これは、HIPAA セキュリティル

[37] https://csrc.nist.gov/Projects/lightweight-cryptography

ールに対するガイドであり、セキュリティルールのテーマごとに、NIST が定める SP 800-53 が定めるセキュリティリスク対策カタログの項目と、NIST が定めるその他の標準・文書への対応を示す形式となっている。この中で、以下の文書を参照している。

- データ保存
  - SP 800-111, “Guide to Storage Encryption Technologies for End User Device”
- データ消去
  - SP 800-88, “Guidelines for Media Sanitization”
- データ転送
  - SP 800-52, “Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations”
  - SP 800-77, “Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs”
- 暗号モジュール認証
  - FIPS 140-2, “Security Requirements for Cryptographic Modules”

3.1.5. 米国の参考文献

[1] Federal Information Security Management Act of 2002 (FISMA)（連邦情報セキュリティ管理法）、Title III of E-Government Act of 2002:
https://www.govinfo.gov/app/details/PLAW-107publ347

[2] Federal Information Security Management Act of 2014 (FISMA2014, FISMA Reform)（連邦情報セキュリティ近代化法）
https://www.govinfo.gov/app/details/PLAW-113publ283

[3] OMB Circular A-130, “Managing Information as a Strategic Resource”（戦略資源としての情報管理）
Division E of the National Defense Authorization Act for Fiscal Year 1996:
https://www.govinfo.gov/app/details/PLAW-104publ106

[4] National Institute of Standards and Technology Act (NIST Act)
https://www.govinfo.gov/app/details/USCODE-2014-title15/USCODE-2014-title15-chap7

[5] Information Technology Management Reform Act (Clinger-Cohen Act)（情報技術管理改革法）
Division E of the National Defense Authorization Act for Fiscal Year 1996:
https://www.govinfo.gov/app/details/PLAW-104publ106

[6] NSD 42, “National Policy for the Security of National Security Telecommunications and Information Systems”
https://www.hsdl.org/?abstract&did=458706

[7] CNSS Policy No.3, “National Policy for Granting Access to U.S. Classified Cryptographic Information”
CNSSP 3 of https://www.cnss.gov/CNSS/issuances/Policies.cfm

[8] Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information”
https://www.federalregister.gov/documents/2011/10/13/2011-26729/structural-reforms-to-improve-the-security-of-classified-networks-and-the-responsible-sharing-and

[9] Export Administration Act of 1979 (EAA)（輸出管理法）
https://www.govinfo.gov/app/details/STATUTE-93/STATUTE-93-Pg503/

[10]Export Control Reform Act of 2018 (ECRA)（輸出管理改革法）
Subtitle B - Export Control Reform of
TITLE XVII - REVIEW OF FOREIGN INVESTMENT AND EXPORT CONTROLS of
The DIVISION A - DEPARTMENT OF DEFENSE AUTHORIZATIONS of

John S. McCain National Defense Authorization Act for Fiscal Year 2019: https://www.govinfo.gov/app/details/PLAW-115publ232

[11]Export Administration Regulation (EAR) (輸出管理規則) https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

[12]John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA2019) (国防権限法 (2019)) https://www.govinfo.gov/app/details/PLAW-115publ232

[13]Arms Export Control Act of 1976 (AECA) (武器輸出管理法) Title II of 90 Stat. 729 - International Security Assistance and Arms Exports Control Act: https://www.govinfo.gov/app/details/STATUTE-90/STATUTE-90-Pg729

[14]The International Traffic in Arms Regulations (ITAR) (国際武器取引規則) https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987

[15]CNSS Policy No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products" CNSSP-11 of https://www.cnss.gov/CNSS/issuances/Policies.cfm

[16]Memorandum for Chief Information Officers - Security Authorization of Information Systems in Cloud Computing Environments https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

[17]FIPS140-3, "Security Requirements for Cryptographic Modules" https://csrc.nist.gov/publications/detail/fips/140/3/final

[18]DoDI 5025.01, "DoD Issuances Program" https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/502501p.pdf

[19]DoDD 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))" https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/514301p.pdf

[20]SP 800-57, "Recommendation for Key Management" https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final

[21]SP 800-131A, "Transitioning the Use of Cryptographic Algorithms and Key Lengths" https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final

[22]SP 800-52 Rev. 2, "Guidelines for the Selection, Configuration, and Use of

Transport Layer Security (TLS) Implementations”
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final
[23]SP 800-77 Rev. 1, “Guide to IPsec VPNs”
https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final
[24]DoDI 5205.8, “Access to U.S. Classified Cryptographic Information”
https://fas.org/irp/doddir/dod/i5205_08.pdf
[25]Securities Clarity Act
https://www.congress.gov/bill/116th-congress/house-bill/8378
[26]Digital Commodity Exchange Act of 2020
https://www.congress.gov/bill/116th-congress/house-bill/8373
[27]Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets
https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets
[28]Electronic Signatures in Global and National Commerce Act (ESIGN Act)
https://www.govinfo.gov/app/details/PLAW-106publ229
[29]Uniform Electronic Transactions Act (UETA)
https://www.uniformlaws.org/committees/community-home?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034
[30]Electronic Signatures and Records Act (ESRA)
https://its.ny.gov/electronic-signatures-and-records-act-esra
[31]Electronic Commerce Security Act (ECSA)
https://www.ilga.gov/legislation/ilcs/ilcs5.asp?ActID=89&ChapterID=2
[32]Guidance Note Regarding the Relation Between the Uniform Electronic Transactions Act and Federal Esign Act, Blockchain Technology and “Smart Contracts”
https://www.uniformlaws.org/viewdocument/guidance-note-regarding-the-relatio?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034&tab=librarydocuments
[33]SP 800-53 Rev. 5, “Security and Privacy Controls for Information Systems and Organizations”
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[34]DoDI 8500.01, “Cybersecurity”
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

[35]CNSS Policy No. 15, “Use of Public Standards for Secure Information Sharing” CNSSP-15 of https://www.cnss.gov/CNSS/issuances/Policies.cfm
[36]SP 800-88 Revision 1, “Guidelines for Media Sanitization” https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
[37]NISTIR 8105, “Report on Post-Quantum Cryptography” https://csrc.nist.gov/publications/detail/nistir/8105/final
[38]NISTIR 8114, “Report on Lightweight Cryptography” https://csrc.nist.gov/publications/detail/nistir/8114/final
[39]DA PAM 25-2-16, “Information Management: Army Cybersecurity Communications Security (COMSEC)” https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN16678_DAPam25-2-16_FINAL.pdf
[40]Health Insurance Portability and Accountability Act of 1996 (HIPAA) https://www.govinfo.gov/app/details/PLAW-104publ191/
[41]Health Information Technology for Economic and Clinical Health Act (HITECH Act) TITLE XIII of American Recovery and Reinvestment Act of 2009: https://www.govinfo.gov/app/details/PLAW-111publ5/
[42]SP 800-66 Rev.1, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule” https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
[43]NISTIR 8200, “Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)” https://csrc.nist.gov/publications/detail/nistir/8200/final

3.2. 英国

英国では、2016 年 10 月より新しいサイバーセキュリティ戦略（2016 年～2021 年）が開始され、英国をサイバー攻撃の脅威から守るための担当組織として GCHQ（Government Communications Headquarters、政府通信本部）の一部として NCSC[38]（National Cyber Security Centre：国家サイバーセキュリティセンター）が設立された。NCSC の設立に伴い、従来 CESG（Communications-Electronics Security Group、電子安全通信局）が提供していた製品の認証 CAPS（CESG Assisted Products Service）および CPA（Commercial Product Assurance）も、NCSC の担当に変更となっている。

また、英国政府は、豪加印日米ニュージーランドと連名で、激化するテロ、サイバー攻撃への対応において、End-to-end で暗号化された通信が解読できないことについて懸念を表明している［24］。

一方、既存の暗号技術は、将来的に量子コンピュータの発展により危殆化することが予想されており、この対策として、耐量子計算機暗号の検討が進められている［25］。

なお、英国は Brexit の移行期間を 2020 年 12 月 31 日に終え、EU（European Union、欧州連合）から離脱した。この離脱に伴い、今後様々な領域で変更が生じる可能性がある。

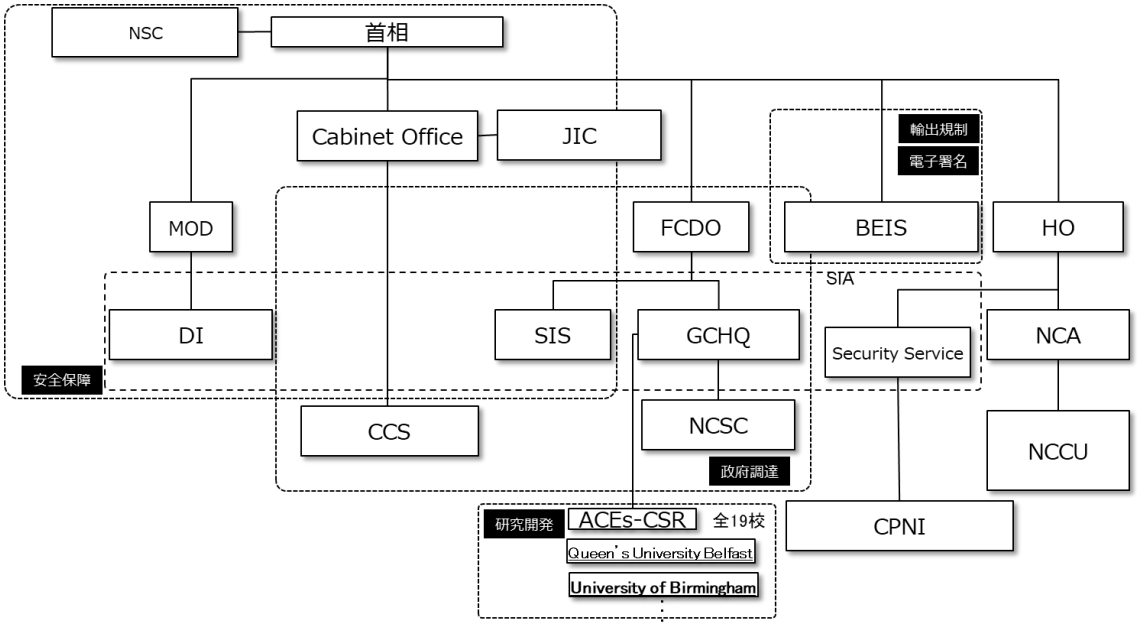
3.2.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

NCSC は、GCHQ を母体とし、英国の国家レベルでのサイバーセキュリティのための唯一の機関として設立された。NCSC は、既存の 3 つのサイバーセキュリティ組織である、GCHQ の情報セキュリティ部門である CESG、CERT-UK（Computer Emergency Response Team、コンピュータ緊急対応チーム）、CCA（Cyber Security Centre、サイバー評価センター）を統合し、これらに代わるものであり、国家インフラ保護センター（CPNI：Centre for the Protection of National Infrastructure）のサイバー関連の責任も含んでいる。[39]

主要な関係組織のセキュリティ政策における役割の要点は以下のようになる。

[38] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

[39] The launch of the National Cyber Security Centre, https://www.ncsc.gov.uk/information/our-history



Cabinet Office（内閣府）
NSC：National Security Council（国家安全保障委員会）
NCSC：National Cyber Security Centre（国家サイバーセキュリティセンター）
JIC：Joint Intelligence Committee（統合諜報委員会）
MOD：Ministry of Defence（防衛省）
DI：Defence Intelligence（国防情報参謀部）
FCDO：Foreign, Commonwealth & Development Office（外務・英連邦省）
GCHQ：Government Communications Headquarters（政府通信本部）
SIS：Secret Intelligence Service（機密情報部）
CCS：Crown Commercial Service（クラウン商業サービス）
SIA：Security and Intelligence Agencies
BEIS：Department for Business, Energy & Industrial Strategy
HO：Home Office（内務省）
CPNI：Center for Protection of National Infrastructure（国家インフラ防護センター）
NCA：National Crime Agency（国家犯罪対策庁）
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（英国）

- 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部門である。

- NSC（National Security Council、国家安全保障委員会）
  国家安全保障に関する政府の目標をどのように実現するかを、包括的、戦略的に検討する会議である。首相が議長を勤める。

- GCHQ（Government Communications Headquarters、政府通信本部）
  英国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組織である。

- NCSC（National Cyber Security Centre、国家サイバーセキュリティセンター）
  GCHQ の一部として、2016 年 10 月 1 日に発足したサイバーセキュリティ戦略の推進機関である。政府、産業界、市民との間でサイバーセキュリティのパートナーシップを構築し、英国のオンラインの安全性を確保する。

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

- BEIS（Department for Business, Energy & Industrial Strategy、ビジネス・エネルギー・産業戦略省）
  貿易・産業を所管するビジネス・革新・技術省（BIS）が改称された組織である。輸出入規制、電子署名を所管している。

- CPNI（Center for Protection of National Infrastructure、国家インフラ防護センター）
  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組織である。

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

- ACEs-CSR（Academic Centres of Excellence in Cyber Security Research）
  Queen’s University Belfast、University of Birmingham など 19 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、NCSC と連携している。

また、以下の組織は、廃止・移管された。

- CGSD（Cyber and Government Security Directorate、旧サイバー・政府セキュリティ局）[40]
  旧サイバー・政府セキュリティ局（CGSD）は、国家サイバーセキュリティ計画を調整し、

[40] https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

政府全体および国際的な個人、物理、情報セキュリティ政策を担当していた。NCSC の設立を支援し、2017 年 9 月に存在を終えた。その作業は、内閣府内で再編成された。

- OCSIA（Office of Cyber Security & Information Assurance、旧サイバーセキュリティ&情報保証室）
  英国の様々な組織と連携し、基本戦略 The national security strategy を担当していた。新しいサイバーセキュリティ戦略 NATIONAL CYBER SECURITY STRATEGY（2016-2021）に伴い、その機能は NCSC へ移管された。

- CESG（Communications-Electronics Security Group、旧電子安全通信局）
  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）であった。CESG は現在、NCSC の一部として再編成された。

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

英国では、2016 年に 2021 年のビジョンを示した新しいサイバーセキュリティ戦略が発表され、サイバーセキュリティ政策の推進機関として NCSC を設立し、£1.9billion の投資により、激化するサイバー攻撃に対抗する。

主な制度の要点をまとめると以下のようになる。

- National Cyber Security Centre Prospectus [1]
  英国のサイバーセキュリティを確保するために設立された NCSC のビジョンと目的を記載している。次の４つを目標としている。
  - サイバーセキュリティ環境を理解し、知識を共有し、その専門知識を活用してシステムの脆弱性を特定し、対処する。
  - サイバーセキュリティを向上させるために、公共部門や民間部門の組織と協力して英国のリスクを軽減する。
  - サイバーセキュリティインシデントに対応し、被害を軽減する。
  - 英国のサイバーセキュリティ能力を育成し、成長させ、国家の重要なサイバーセキュリティ問題でリーダーシップを発揮する。

- UK Digital Strategy 5. A safe and secure cyberspace – making the UK the safest place in the world to live and work online [2]
  英国のデジタル戦略（2017）のうち 5 番目の要素である「安全で安全なサイバースペース-英国をオンラインで生活し、働くための世界で最も安全な場所にする」を実現する

ための目標および要素を示している。以下の 3 つの目標が挙げられている。

- 防御　進化するサイバー脅威から英国を防御する
- 抑止力　敵対的な行動を検出、理解、調査、妨害し、犯罪者を追跡し、起訴する
- 開発　サイバーセキュリティ業界の研究開発により、公的部門と民間部門全体で、将来の脅威と課題に対応し、克服する

- NATIONAL CYBER SECURITY STRATEGY 2016-2021 [3]

  急激に変化するサイバー攻撃の脅威に対抗するためのサイバーセキュリティ戦略である。英国がサイバー攻撃の脅威に対して安全で回復力があり、デジタル世界で繁栄し、自信を持っていることをビジョンとしている。この戦略では、2016 年から 2021 年までの 5 年間に£1.9billion の投資を行い、NCSC の設立により迅速なインシデント対応を行ってビジネス及び個人への専門知識の中枢とすることが定められている。

表 3-9　英国における暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	上位政策・戦略	National Cyber Security Centre Prospectus	内閣府、GCHQ	ー
2		UK Digital Strategy	DCMS	後継
3		NATIONAL CYBER SECURITY STRATEGY 2016-2021	内閣府、National security and intelligence, HMT	後継
4	暗号政策・設置法	Security Policy Framework - May 2018	内閣府、National security and intelligence、Government Security Profession	更新有
5		The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016	法執行機関	後継
6		Regulation of Investigatory Powers Act 2000 (RIPA)	法執行機関	更新有
7		Intelligence Services Act 1994	GCHQ、SIS	更新無
8		Paper on regulatory intent concerning use of encryption on public networks.1996	BEIS（旧 BIS）	更新無
9		Electronic Communications Act 2000	BEIS（旧 BIS）	更新無
10	輸出入規制	Open general export licence (cryptographic development)	ECJU、DIT	後継
11		UK Strategic Export Controls annual report 2019	ECJU、DIT、FCDO、MoD	後継

12		Export controls: dual-use items, software and technology, goods for torture and radioactive sources	ECJU、DIT	―
13	政府調達	eGIF (e-Government Interoperability Framework) Technical Standards Catalogue	内閣府	更新無
14		HMG Information Assurance Standards	内閣府	更新無
15		Procurement Policy Note 09/14: Cyber Essentials scheme certification	内閣府	―
16		Government Security Classifications	内閣府	―
17	標準・基準	CAPS Assisted Products	NCSC	後継
18		Commercial Product Assurance (CPA)	NCSC	後継
19		Government Functional Standard GovS 007: Security	内閣府	―
20		Security Standard - Use of Cryptography (SS-007)	DWP	―
21	その他	Guidance Cloud guide for the public sector	GCF、GDS	―
22		Cryptoassets Taskforce: final report	HMT、FCA、BoE	―
23		Guidance on Cryptoassets	FCA	―
24		International statement: End-to-end encryption and public safety (accessible version)	英国、オーストラリア、カナダ、インド、日本、ニュージーランド、及び米国政府	―
25		Quantum security technologies, Preparing for Quantum-Safe Cryptography	NCSC	―

BoE：Bank of England（イングランド銀行）
DCMS：Department for Digital, Culture, Media & Sport（デジタル・文化・メディア・スポーツ省）
DIT：Department for International Trade（国際貿易省）
DWP：Department for Work and Pensions（労働・年金省）
ECJU：Export Control Joint Unit（輸出管理局）
FCA：Financial Conduct Authority（金融行動監視機構）
FCDO：Foreign, Commonwealth & Development Office（外務・英連邦省）
GCF：Government Commercial Function
GDS：Government Digital Service（政府デジタルサービス）
HMT：HM Treasury（大蔵省）
MoD：Ministry of Defence（防衛省）

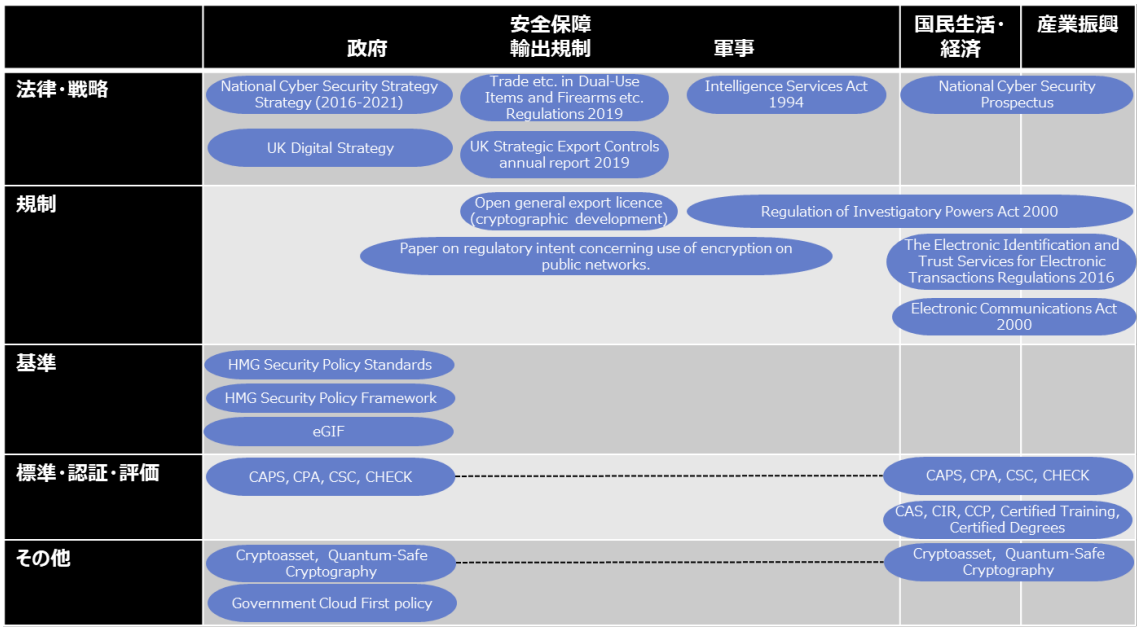


図 3-4　暗号政策に係る政策マップ（英国）

- Security Policy Framework - May 2018 [4]
  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。2018 年 5 月の改訂版は、EU の GDPR（General Data Protection Regulation 一般データ保護規則）の実装に対応した英国のデータ保護法（Data Protection Act 2018）に合わせて更新された。

- Regulation of Investigatory Powers Act 2000 (RIPA) [6]
  暗号利用に関する規制であり、3.2.3.6 節にまとめる。

- Paper on regulatory intent concerning use of encryption on public networks.1996 [8]
  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。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- Intelligence Services Act 1994 [7]
  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。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016（電子取引のための電子識別およびトラストサービスに関する規則）[5]

  The Electronic Identification and Trust Services for Electronic Transactions Regulations は EU の eIDAS 規則（Regulation（EU）910/2014）の監督機関及び罰則制度要件を英国法に反映させるために立法化された。

  eIDAS 規則（Regulation（EU）910/2014）は、企業、市民、および行政機関間の安全でシームレスな電子国境を越えた取引を可能にし、電子署名、電子シール、電子タイムスタンプ、電子文書およびウェブサイト認証の受け入れの相互認識のための体制を導入することを目的としている。

- Electronic Communications Act 2000 [9]

  政府は、電子データの暗号鍵の供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。

  なお、2014 年度調査以降に変更及び更新は見当たらない。

- Open general export licence（cryptographic development - from December 2019）[10]／UK Strategic Export Controls annual report 2019 [11]／Export controls: dual-use items, software and technology, goods for torture and radioactive sources [12]

  輸出入に関する規制で、3.2.3.4 節にまとめる。

- eGIF（e-Government Interoperability Framework）Technical Standards Catalogue [13]／HMG Information Assurance Standards[14]／Procurement Policy Note 09/14: Cyber Essentials scheme certification[15]／Government Security Classifications [16]

  政府調達に関する規制で、3.2.3.3 節にまとめる。

- CAPS（CESG Assisted Products Service）Cryptographic Products [18]／CAPS Assisted Products [17]／Government Functional Standard GovS 007: Security [19]／Security Standard - Use of Cryptography（SS-007）[20]

  標準・基準に関するものであり、3.2.3.2 節にまとめる。

- Guidance Cloud guide for the public sector [21]

  クラウドに関するものであり、3.2.3.7 節にまとめる。

- Cryptoassets Taskforce: final report [22] ／Guidance on Cryptoassets [23] 、及び補足として Cryptoasset promotions Consultation
  暗号資産に関するものであり、3.2.3.8 節にまとめる。

- International statement: End-to-end encryption and public safety (accessible version) [24]
  End-to-end の暗号化と公共の安全に関するものであり、3.2.3.6 節にまとめる。

- Quantum security technologies [25] ／Preparing for Quantum-Safe Cryptography [26]
  量子セキュリティ技術に関するものであり、3.2.4.1 節にまとめる。

3.2.3. 暗号に関わる各種制度、規制及びガイドライン

3.2.3.1. 利用すべき暗号方式

暗号方式、セキュリティに関する機能、および暗号セキュリティの管理策について規定した主な標準はそれぞれ以下のとおりである。

- HMG Cryptographic Standards（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、英国情報保証標準（HMG IA Standards）の一部を構成する。この文書情報の開示は制限されている。

- Government Functional Standard GovS 007: Security
  政府機関内および組織の境界を越えて、一貫して筋の通った作業を促進し、保証、リスク管理、能力向上のための安定した基盤を提供することを目的とした一連の機能基準の一部である。

- Security Standard – Use of Cryptography (SS-007)
  この暗号セキュリティ標準は、暗号を当局によって承認されたセキュリティレベルに安全に実装するために必要な管理策のリストを提供する。
  労働・年金省内部の暗号システムのセキュリティ基準である。

3.2.3.2. セキュリティ製品認証制度・セキュリティサービス認証制度

NCSC は、製品、サービス及び組織を対象とした多くの認証を提供している。このうち、製品に対しての認証として CAPS 及び CPA がある。これらは、従来は CESG が所管であった。

なお、保証サービス範囲の見直しにより、NCSC は、コモンクライテリア認証協定（CCRA）に基づく認証機関ではなくなった（2019 年 10 月 1 日）[41]。これに伴い、英国は CCRA 認証国から CCRA 受入国に変更となった。

セキュリティ製品認証制度

- CAPS Assisted Products

  CAPS は、HMG やその他の適切な組織が使用することを目的として、製品が HMG ポリシーの基準を満たしていることを評価する。HMG ポリシーは、政府の機密データを保護するために暗号化が使用される場合に採用される承認済みの標準を定めている。

  政府セキュリティ分類ポリシー[42]では、情報の機密性に応じて、OFFICIAL、SECRET、TOP SECRET の 3 段階に分類されている。

表 3-10　政府セキュリティ分類

TOP SECRET	最も深刻な脅威から最高レベルの保護を必要とする。例えば、人命を脅かしたり、国や友好国の安全や経済を脅かしたりする可能性がある場合など。
SECRET	強靭で非常に有能な脅威行為者から防護するために、保護措置を強化することが正当化される非常に機密性の高い情報。例えば、軍事力、国際関係、または重大な組織犯罪の捜査に重大な損害を与える可能性がある場合。
OFFICIAL	公共部門で作成または処理される情報の大部分を占める。日常的な業務運営やサービスで扱われる情報が含まれ、その中には、紛失、盗難、メディアへの掲載などにより損害を受ける可能性のあるものも含まれるが、脅威プロファイルの強化の対象とはならない情報。

  CAPS の従来のベースライングレードとエンハンスドグレードおよびハイグレードは、上表の分類に移行している。

  ○ OFFICIAL 層の製品

  CAPS による評価を受けなくなった。

  ○ Airwave 製品（無線通信製品）

  Airwave 製品の保証方法は、従来のベースライングレードとエンハンスドグレードに基づいて、AIRWAVE システムの寿命まで継続される。

[41] https://www.ncsc.gov.uk/information/common-criteria-0

[42] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

○ PRIME デバイス

PRIME とは、暗号化された IP 通信に関する英国の戦略的標準であり、インターネット標準の IPsec に基づいている。PRIME デバイスとは、PRIME 標準への準拠を検証するための独立したテストの後、NCSC によって認証された製品を指す。

- CPA（Commercial Product Assurance）

  CPA スキームでの新規製品の評価を受け付けは、スマートメータまたはスマートメータ製品のみに変更になった。ただし、既存の CPA 認証書を有する製品は、認証書に記載された期限まで有効である。

- Cyber Essentials

  Cyber Essentials は、組織がサイバー攻撃に対しての対策を講じていることを評価する政府支援のスキーム。スキームには、Cyber Essentials と Cyber Essentials Plus の 2 つのレベルがある。Cyber Essentials Plus は、認証の一部として脆弱性テストの実施が必要となるため、より厳格なものとなっている。

  一部の政府契では、Cyber Essentials 認証を取得していることを必須要件とする場合がある。

  なお、約 2020 年 4 月 1 日から、NCSC に代わって IASME コンソーシアムが Cyber Essentials スキームの運営を引き継いだ[43]。

セキュリティサービス認証制度

以下の７つの認証制度がある。

- CAS（Commodity Information Assurance Services）

  データの破壊とサニタイズサービスを提供している会社である場合、CAS は潜在的な顧客にそのサービスが優れていることを示すスキームであり、独立した評価者が、基準に照らして提供しているサービスを評価する。

- CIR（Cyber Incident Response）

  英国の重要なネットワークを持っている組織は、サイバーインシデントレスポンス（CIR）認証企業を使用して、標的型攻撃への対処を支援できる。NCSC は、サイバー攻撃の被害を受けた組織を支援できる企業を認証するために、サイバーインシデントレスポンス（CIR）スキームが設定されている。

[43] https://www.ncsc.gov.uk/blog-post/announcing-iasme-consortium-as-our-new-cyber-essentials-partner

- CSC（Cyber Security Consultancies）
  政府、より広範な公共部門、および重要な国家インフラストラクチャに対して、広範囲かつ複雑なサイバーセキュリティ問題のサポートを提供することを目的としており、認証を受けたコンサルタント会社は、顧客に対し、独立した専門家としてのアドバイスを提供する。

- CCP（Cyber Security Professionals）
  CCP に基づく専門資格は、サイバーセキュリティのスキル、知識、専門知識を実際の状況に適用する持続的な能力を実証した人に授与される。

- Certified Training
  質の高いトレーニングコースを保証するため、トレーニングを 2 つのレベルで評価する。
  - サイバーセキュリティを初めて学ぶ人に基礎を提供するための入門編
  - 専門的な開発のための詳細なコースを探している人のための応用編

- Certified Degrees
  サイバーセキュリティおよび密接に関連する領域の NCSC 認証の学士号、統合された修士号および修士号。

- CHECK（Penetration testing）
  NCSC が承認した企業が、公共部門および重要な国家インフラストラクチャシステムとネットワークに対し、認可された侵入テストを実施できるスキームである。

2021 年 2 月 2 日時点での各認証サービスにおける認証件数は以下の通りである。

表 3-11　英国認証サービス件数　一覧表

認証サービス [44]	認証件数	備考
CAPS	48	製品認証
CPA	41	製品認証
CAS	7	サービス認証
CIR	9	サービス認証
CSC	27	サービス認証

[44] https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?start=0&rows=20

CCP	―	制度変更中[45]
Certified training	2	サービス認証
Certified Degrees[46]	35	サービス認証
CHECK	46	サービス認証、侵入テストの提供企業数

CAPS (Certified Assisted Products)
CPA (Commercial Product Assurance)
CAS (Assured Services)
CIR (Cyber Incident Response)
CSC (Cyber Security Consultancies)
CCP (Cyber Security Professionals)

3.2.3.3. 政府の調達要件

HMG Information Assurance Standards [14] （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、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。

また、政府の機密データを保護するために暗号化が使用される場合は、CAPS 認証が必要となっている。

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）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 月発行の Technical Standards Catalogue Version 6.2 [13] 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、下表を規定している。

表 3-12 推奨仕様

暗号化アルゴリズム	AES, Triple DES
署名	RSA, DSA, DSS
鍵交換	RSA, DSA
ハッシュ関数	SHA-512, SHA-256

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、

[45] https://www.ncsc.gov.uk/section/products-services/ncsc-certification
[46] https://www.ncsc.gov.uk/information/ncsc-certified-degrees

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。なお、2014 年度調査以降に変更及び更新は見当たらない。

また、英国政府は、サプライチェーンにおけるサイバーセキュリティリスクのレベルを低減するため、Cyber Essentials スキームを策定し、採用を奨励している。このスキームは、個人情報の取り扱いや特定の ICT 製品・サービスの提供を特徴とする政府の契約の場合には、必須となっている。

- Procurement Policy Note 09/14: Cyber Essentials scheme certification [15]
  英国政府の調達時のサプライチェーンにおけるサイバーセキュリティリスクを軽減することを目的とした Cyber Essentials スキームの使用法を説明している。

英国政府と連携するすべての人が守るべき情報資産のポリシーとして、Government Security Classifications が定められている。

- Government Security Classifications [16]
  英国政府の情報資産の分類方法を説明したポリシー。政府が、外部パートナーから受信または外部パートナーと交換する情報を含め、提供されるサービスおよびビジネスを行うために政府が収集、保存、処理、生成、または共有するすべての情報に適用される。このポリシーに従って資産を保護する責任がある。

3.2.3.4. 暗号の輸出入規制

英国においては暗号の輸入は規制せず [47]、暗号の輸出を規制する。暗号規制の考え方は、ワッセナー・アレンジメント（Wassenaar Arrangement）に基づいている。規制対象となる暗号製品等は、ワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）」のなかのデュアルユース製品・技術に関するリストのカテゴリ 5 パート 2（Category 5 – Part 2 “Information Security”）がベースになっている。（参考：3.1.3.4 節のワッセナー・アレンジメント）

2021 年 2 月時点の CCL は、2019 年 12 月のワッセナー・アレンジメント会議で合意されたデュアルユース製品・技術のリスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）に基づいている [48]。合意リストは 9 のカテゴリに分類

[47] https://www.gov.uk/guidance/import-controls

[48] https://www.federalregister.gov/documents/2020/10/05/2020-18334/implementation-of-certain-new-controls-on-emerging-technologies-agreed-at-wassenaar-arrangement-2019

されたデュアルユース製品・技術のリスト、機密リスト、特別な機密リストから構成され、デュアルユース製品・技術のリストの各カテゴリは、CCL に対応するものが存在する。規制対象となる暗号製品はカテゴリ 5 パート 2(Category 5 – Part 2 “Information Security”)で定められている。

暗号製品の輸出規制は輸出管理局（ECJU）が行う。

- Open general export licence (cryptographic development – from December 2019)
  「情報セキュリティ機能」を有するソフトウェアおよびテクノロジーの輸出を許可するライセンス。対象となるアルゴリズム[49]は、以下の通り。

表 3-13　輸出規制対象の暗号アルゴリズム

分類	アルゴリズム
対称鍵暗号	鍵長 56 ビット（パリティビットを含まない）以上
非対称暗号	1. 512 ビットを超える整数の因数分解（例：RSA） 2. 512 ビットを超えるサイズの有限体の乗法群における離散対数の計算（例えば、Z/pZ 上の Diffie-Hellman） 3. 上記 2.以外の群の離散対数が 112 ビットを超える（例えば、楕円曲線上の Diffie-Hellman）
非対称暗号	1.格子の最短ベクトル問題または格子簡約問題（例 NewHope, Frodo, NTRUEncrypt, Kyber, Titanium）; 2.超特異楕円曲線間の等値性の発見 （例 超特異同種鍵のカプセル化）; or 3.ランダムコードのデコード(e.g., McEliece, Niederreiter).
量子暗号	—

- UK Strategic Export Controls annual report 2019
  2019 年 1 月から 12 月にかけての英国の戦略的輸出管理業務の詳細についてのレポート。

- Export controls: dual-use items, software and technology, goods for torture and radioactive sources
  管理されたデュアルユースアイテム、ソフトウェアとテクノロジー、拷問用商品、放射能源の輸出に関するライセンス手続きとその他の制限に関するガイド。

[49] https://www.gov.uk/guidance/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items, 5A002.a

3.2.3.5. プロトコル等での暗号方式

NCSC は、インターネット上での商取引と個人情報を保護するための TLS（トランスポート層セキュリティ）プロトコルとして、以下の暗号化プロファイルを推奨している[50]。

表 3-14 TLS での暗号化プロファイル

	Combination 1 of the Suite B profile	Foundation Profile
プロトコル	TLS v1.2	TLS v1.2
暗号化	GCM モードで 128 ビット鍵を使用する AES	CBC モードで 128 ビットキーを使用する AES
疑似乱数関数	TLS PRF（SHA-256 を使用）	TLS PRF（SHA-256 を使用）
認証	P-256 曲線上の SHA-256 を使用した ECDSA-256	RSA 署名（2048 ビット）および SHA-256 を使用した X.509 証明書
鍵交換	P-256 曲線を使用した ECDH	DH グループ 14（2048 ビット MODP グループ）
完全性	-	SHA-256

3.2.3.6. 暗号利用に関する規制（利用ライセンス・暗号盗聴法など）

激化するサイバー犯罪（テロや児童性犯罪など）の対策として、英国では、Regulation of Investigatory Powers Act 2000（RIPA）により、一定の要件の下で、暗号化された被保護情報を復号する鍵を所持している者に対して、暗号化された情報の開示を間接強制的に要求することができる。また、国際声明：End-to-end の暗号化と公共の安全（International statement: End-to-end encryption and public safety [24] ）が出され、法執行機関がエンドツーエンド暗号化された通信にアクセスできるように IT 企業へ要請している。

- Regulation of Investigatory Powers Act 2000（RIPA） [6]
  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。
  2000 年発行以降、数回の修正が行われている。最近では、Coronavirus Act 2020（コロナウィルス法）による変更等あり。

- International statement: End-to-end encryption and public safety (accessible version)
  英国、オーストラリア、カナダ、インド、日本、ニュージーランド、及び米国の政府に

[50] https://www.ncsc.gov.uk/guidance/tls-external-facing-services

よって署名された国際声明。

3.2.3.7. クラウドサービス

英国政府は、Government Cloud First policy[51]（政府クラウドファーストポリシー）により、サービス調達時に、先ずクラウドソリューションを検討し評価する必要がある。クラウドテクノロジーの活用により、速度、セキュリティを強化し、部門間のコラボレーションが可能となる。

- Guidance Cloud guide for the public sector [21]
  one government cloud strategy（1 つの政府クラウド戦略）とも呼ばれ、次の責任を負う公務員を対象としたガイダンスである。
  - クラウド戦略の決定と設定
  - クラウドへの移行の実装
  - クラウド使用の管理

  次の方法について説明している。
  - クラウドライフサイクル全体で部門間のコラボレーションを可能にする
  - ベストプラクティスのクラウドサービスの使用法を実現する
  - 商業、技術、セキュリティ、および人的能力を最大化する

3.2.3.8. 暗号資産

暗号資産の市場とその基盤となる DLT(Distributed Ledger Technology：分散型台帳技術)のテクノロジーは急速に発展しており、市場参加者は、問題点、当局の承認の是非、ビジネスに適用される規則や規制が理解できていないと言われており、これらに対応することが必要となっている。

- Cryptoassets Taskforce: final report[52]
  HMT（大蔵省）、FCA（金融行動監視機構）およびイングランド銀行による暗号資産タスクフォースの合同報告書。金融サービスにおける暗号資産と分散型台帳技術（ブロックチェーン技術）に対する以下のような英国のアプローチを示している。
  - 金融サービスでビジネスを行う上で安全で透明性の高い場所としての英国の国際的な評判を維持する。
  - 金融市場における高い規制基準を確保する。
  - 消費者を保護する。

---

[51] https://www.gov.uk/guidance/government-cloud-first-policy
[52] https://www.gov.uk/government/publications/cryptoassets-taskforce

- 将来出現する可能性のある金融安定性への脅威から保護する。
- 規則を遵守する金融セクタの革新者が繁栄することを可能にする。

- Guidance on Cryptoassets[53]
  暗号資産の市場参加者が採用する暗号資産が規制範囲内にあるかどうかを理解するためのガイダンス。これにより、市場参加者に関連する問題を警告し、承認が必要かどうか、およびビジネスに適用される規則や規制を理解できるようになる。

- Cryptoasset promotions Consultation[54]
  特定の暗号資産を金融振興規制の範囲に含める提案についての協議。

3.2.3.9. 電子署名法

EU の eIDAS 規則(Regulation (EU) 910/2014)を英国法に反映させるため、The Electronic Identification and Trust Services for Electronic Transactions Regulation が 2016 年 7 月に発効された。

3.2.3.10. 国民 ID 番号制度（eID）

英国では、2006 年に国民 ID 登録簿（National Identity Register）の構築と ID カードの発行を規定した ID カード法（Identity Cards Act 2006）が制定された。しかし、費用対効果およびプライバシーや市民的自由への懸念のため、2010 年 5 月に ID カードおよび国民 ID 登録簿は廃止された。

このため、英国では GOV.UK Verify[55]を使用して、特定分野間で個別にデータ連携基盤を用意することで、行政事務の効率化やワンストップサービス化を図ろうとしている。

GOV.UK Verify とは、オンラインで自分が誰であるかを証明するための安全な方法であり、これにより、税金の申告や運転免許証の情報の確認など、政府のサービスに安全、迅速、簡単にアクセス可能となっている。GOV.UK Verify を使用して政府サービスにアクセスする場合、最初に、政府が ID の検証を承認した ID プロバイダにより本人確認が行われる。

3.2.4. その他

3.2.4.1. 量子コンピュータの進展に伴う対応策

量子コンピュータの実用化に向け研究開発が進んでいる。現在のコンピュータを超える量子コンピュータの演算能力により、電子商取引の基礎となっている公開鍵暗号が危殆化

---

[53] https://europeanchamberofdigitalcommerce.com/wp-content/uploads/2019/06/Guidance-on-Cryptoassets-Consultation-Paper.pdf
[54] https://www.gov.uk/government/consultations/cryptoasset-promotions
[55] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

する恐れが指摘されているため、その対応策が検討されている。

- Quantum security technologies（量子セキュリティテクノロジ） [25]
  量子物理学に依存する 2 つのセキュリティテクノロジである QKD（Quantum Key Distribution、量子鍵配送）と QRNG（Quantum Random Number Generator、量子乱数生成）に関する NCSC の立場について説明している。
  従来の公開鍵暗号アルゴリズムは将来の大規模量子コンピュータに対して脆弱である可能性があるため、この脆弱性を共有しない新しいアプローチとして QKD プロトコルを、送受信者の認証を保証する暗号化メカニズムと一緒に展開する必要があり、量子コンピュータの脅威に対する最善の緩和策としては、量子セーフ暗号（quantum-safe cryptography）を勧めている。

  QKD は、２者間で暗号化鍵を合意するためのメカニズムであり、量子力学の基本原理に基づいて攻撃者を検出できる。
  QRND は、エントロピーを量子力学のみに基づいた構造に依存する RNG（乱数生成）であり、原理的に生成される乱数が予測不可能である。NCSC としては、多くの従来の RNG では、ハードウェアノイズ源が使用され、実用上十分な予測不可能性を満たしており、QRNG は、現在のところ実際には実現困難であり、研究課題があることを認めている。

- Preparing for Quantum-Safe Cryptography（量子セーフ暗号の準備） [26]
  量子コンピューティングの開発による暗号化への脅威の軽減に関する NCSC ホワイトペーパー。
  現在存在する量子コンピュータは、公開鍵暗号にとって、まだ脅威ではない。しかし、量子コンピュータは、攻撃者が過去に暗号化された情報を読み取り、将来情報を偽造することを可能にする。例えば、長い運用寿命を持つ高価値のルートレベルの公開鍵暗号で署名されたデジタル署名に対する脅威は、量子コンピュータにより、攻撃者が署名を「偽造」して正当な秘密鍵の所有者になりすましたり、デジタル署名によって信頼性が保護されている情報を改ざんしたりする可能性がある。
  QSC（Quantum-Safe Cryptography、量子セーフ暗号）は、PKC で使用される量子脆弱な数学的問題を、古典的なコンピュータと量子コンピュータの両方にとって扱いにくいと考えられている数学的問題に置き換える暗号方式。鍵共有とデジタル署名の両方を量子セーフにすることができる。耐量子計算機暗号（PQC: Post-Quantum Cryptography）ともいう。

  NCSC は、公開鍵暗号を QSC に置き換えることにより、量子コンピューティングの脅威を最も効果的に軽減できると考えており、2022 年から 2024 年に予定されている量子セ

ーフ暗号の米国 NIST 標準化に従う意向である。
新しい暗号インフラへの移行は、NIST 標準が利用可能になり、プロトコル（IPSec、TLS など）が QSC をサポートするように更新された後、標準に準拠した QSC 製品の開発を待って行うことが推奨されている。

3.2.5. 英国の参照文献

[1] National Cyber Security Centre Prospectus
https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus

[2] UK Digital Strategy
https://www.gov.uk/government/publications/uk-digital-strategy

[3] NATIONAL CYBER SECURITY STRATEGY 2016-2021
https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[4] Security Policy Framework - May 2018
https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework

[5] The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016
https://www.legislation.gov.uk/uksi/2016/696/contents

[6] Regulation of Investigatory Powers Act 2000 (RIPA)
https://www.legislation.gov.uk/ukpga/2000/23/contents

[7] Intelligence Services Act 1994
https://www.legislation.gov.uk/ukpga/1994/13/pdfs/ukpga_19940013_en.pdf

[8] Paper on regulatory intent concerning use of encryption on public networks.1996
https://webarchive.nationalarchives.gov.uk/19990127124859/http://www.dti.gov.uk:80/cii/encrypt/

[9] Electronic Communications Act 2000
https://www.legislation.gov.uk/ukpga/2000/7/contents

[10] Open general export licence (cryptographic development)
https://www.gov.uk/government/publications/open-general-export-licence-cryptographic-development

[11] UK Strategic Export Controls annual report 2019
https://www.gov.uk/government/publications/united-kingdom-strategic-export-controls-annual-report-2019

[12] Export controls: dual-use items, software and technology, goods for torture and radioactive sources
https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources

[13] eGIF (e-Government Interoperability Framework) Technical Standards Catalogue
https://www.immagic.com/eLibrary/ARCHIVES/GENERAL/UK_CBNET/C050901T.pdf

[14] HMG Information Assurance Standards

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.177.1833&rep=rep1&type=pdf
[15] Procurement Policy Note 09/14: Cyber Essentials scheme certification
https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification
[16] Government Security Classifications
https://www.gov.uk/government/publications/government-security-classifications
[17] CAPS Assisted Products
https://www.ncsc.gov.uk/information/products-cesg-assisted-products-service
[18] Commercial Product Assurance (CPA)
https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa
[19] Government Functional Standard GovS 007: Security
https://www.gov.uk/government/publications/government-functional-standard-govs-007-security
[20] Security Standard - Use of Cryptography (SS-007)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/882760/dwp-ss007-security-standard-use-of-cryptography-v1.1.pdf
[21] Guidance Cloud guide for the public sector
https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector
[22] Cryptoassets Taskforce: final report
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf
[23] Guidance on Cryptoassets
https://www.fca.org.uk/publication/consultation/cp19-03.pdf
[24] International statement: End-to-end encryption and public safety (accessible version)
https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety
[25] Quantum security technologies
https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
[26] Preparing for Quantum-Safe Cryptography
https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

3.3. フランス

フランスにおいては、国立情報システムセキュリティ庁（ANSSI/Agence nationale de la sécurité des systèmes d'information（French Agency for the Security of Information Systems））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、暗号に関わる規制、セキュリティ認証制度が含まれている。ANSSI は、前回調査時の 390 名の組織より、2019 年 6 月時点で約 600 名の組織となっており、成長を続けている。

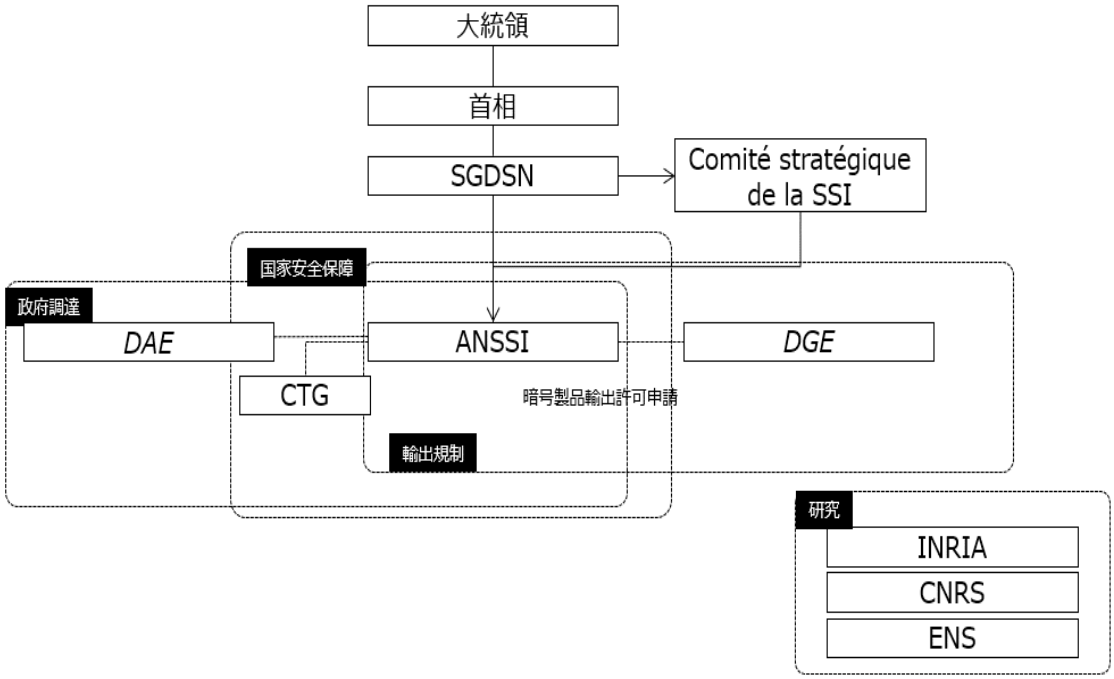
認証制度に関しては、コモンクライテリア(CC)認証とは別に、フランス独自の CSPN(First Level of Security Certification) を実施し、審査日数を限定し、CC 認証に比べて安価にかつ短期間で認証取得が可能な制度を整備することで、産業振興の観点で企業から評価されている。暗号に関する研究開発については、CNRS（French National Centre for Scientific Research）、ENS（École normale supérieure）、INRIA の研究者が参加するプロジェクトチーム CASCADE[56]が中心的であり、公開鍵アルゴリズムに焦点を当て、暗号アルゴリズムの実装・応用暗号学、アルゴリズムとプロトコルの設計・証明可能安全性、理論上・実際の攻撃の研究に取り組んでいる。

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

上述の通り、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、暗号に関わる規制、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を所管している。また、公的機関、公的サービスおよび企業が安全で信頼できるデジタル化を最大限活用できるよう尽力している。近年、サイバーセキュリティが国家的な優先事項になっており、国民一人一人に関わるものと考えられている。ANSSI の役割は、フランスのサイバーセキュリティに関する対応を促進し、協調的・意欲的・積極的な対応、意識向上のための措置、フランスのビジョンや専門知識、欧州の価値観を海外に広めることである。企業総局（DGE）（旧 DGCIS）は、産業、デジタル経済、観光、貿易、技能およびサービスに関連する公共政策を策定し、実施している。

関連組織の全体像をまとめたものが図 3-5 である。

[56] https://crypto.di.ens.fr/web2py



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）
DGE：DIRECTION GÉNÉRALE DES ENTREPRISES（企業総局）
DAE：Direction des Achats de l'État（国家購買部門）
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 3-5　暗号政策に係る組織体制（フランス）

- ANSSI（Agence Nationale de la Sécurité des Systèmes d'Information、国立情報システムセキュリティ庁）[57]

  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、国防安全保障事務局（SGDSN）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。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

[57] https://www.ssi.gouv.fr/

られ、国防に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持つことが示されている。2013 年の「国防・国家安全保障白書」の提案に従い、フランス及び欧州のサイバーセキュリティ研究の舵取りを行う役割を担っている。2013 年 12 月 19 日に採択された軍事計画法により ANSSI の機能が強化された。同法第 22 条では、国にとって極めて重要な事業者；利用できない場合に国家のセキュリティ・安全性を損なう恐れのある施設・設備、および原子力施設のセキュリティを高めるための措置を採用することを規定し、ANSSI が首相に代わり事業者の最も重要なネットワークや情報システムのセキュリティと管理策を強化することを可能にする特権を与えた。さらに、重要な事業者が、システムで検出されたインシデントを報告することを義務とした。[58]

規制の発行やその適用性の検証から、特に政府のネットワークにおけるアラートの監視や迅速な対応まで、幅広い規制・運用を行っている。主なミッションは以下のものである。

- サイバー脅威への理解と対応
- 政府機関向け製品開発の支援
- 情報提供・助言
- 行政、公共サービスおよび企業の支援
- デジタルリスクに対する市民の意識向上と教育に貢献
- 信頼できる製品やサービス提供者へのセキュリティビザの監督や発行

- SGDSN（Secrétariat général de la défense et de la sécurité nationale、国防安全保障事務局）

  国防および安全保障分野（軍事計画、抑止政策、国家安全保障、経済・エネルギーセキュリティ、テロリズムへの対抗、危機対応計画）における政治的意思決定を支援する役割を果たしている事務局である。

  SGDSN の主要なミッションの 1 つである、権限の管理、機密文書の管理、政府間情報システム運用者（OSIIC：Opérateur des Systèmes d’Information Interministériels Classifiés）を通じた政府通信、情報システムのセキュリティ、およびサイバー防衛を担当するのが下位組織である ANSSI である。

- Comité stratégique de la SSI

  フランスの情報システムセキュリティに係る国家戦略を決定する委員会である。

[58] http://www.sgdsn.gouv.fr/le-sgdsn/fonctionnement/lagence-nationale-de-la-securite-des-systemes-dinformation-anssi/

- DGE（Direction générale des Entreprises、企業総局）（旧 DGCIS（生産再建省　競争・産業・サービス総局））
  フランス経済財務省の一部門で、2014 年 9 月、DGCIS から DGE に変更され、産業、デジタル経済、観光、貿易等に関する公共政策の策定や実施を担当する。デュアルユースグッズ・テクノロジーの輸出認可の申請先となっている。デュアルユースグッズ・テクノロジーの輸出に関するガイドラインは、関税・間接税総局（DGDDI）が公開している。

- DAE（Direction des Achats de l'État、国家購買部門）（旧 SAE（国家調達局））
  フランス経済財務省の一部門で、2016 年 3 月 3 日付け条例により、SAE に代わり設立された部門であり、首相の権限の下で国の購買ポリシーを定義している。

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、ANSSI は首相府付きの SGDSN に直属する。暗号製品の輸出申告や認可については ANSSI が所管しており、フランス及び EU の法令に基づき、暗号機器やサービスの認可リクエストの申告を記録し、調査を行っている。

フランスにおける主な法制度を分類整理すると表 3-15 と図 3-6 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（国防安全保障白書 2013）
  国防の将来性を示す白書である。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である。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。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- French National Digital Security Strategy（フランス国家デジタルセキュリティ戦略）
  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）に代わる新たな国家サイバー戦略として、2015 年 10 月 16 日付けでマニュアル・ヴァルス首相により発表されたフランス社会のデジタル移行を支援する戦略である。デジタル移行は技術の革新や成長を促進するが、同時に国家、経済ステークホルダー、市民へのリスクを伴う。サイバー犯罪、スパイ活動、プロパガンダ、妨害行為、個人データの乱用はデジタルトラストとセキュリティを脅か

すものであり、以下の 5 つの戦略的優先事項に基づき集団的かつ協調的な対応を行っていくことを定めている。

1. 基本的利益、国家情報システムおよび重要インフラの防衛およびセキュリティ、経済・社会に必要不可欠な事業者、重大なサイバーセキュリティ危機
2. デジタルトラスト、プライバシー、個人情報、悪意あるサイバー攻撃
3. 意識改革、初期研修、継続した教育
4. デジタル技術ビジネスの環境、産業ポリシー、輸出および国際化
5. 欧州、デジタル戦略的自立性、サイバースペースの安定性

- Strategic review of cyber defence February 2018（サイバー防衛の戦略的レビュー、2018 年 2 月）[3]

  首相から SGDNS に委託され、2018 年 2 月に公開された本文書は上記の French National Digital Security Strategy を補足する戦略文書の一つである。サイバー危機を管理するための方針を定めたもので、国のサイバー防衛戦略のゴールを明確にし、フランスのモデルの妥当性とサイバー防衛における政府の主要な責任を確認するものである。

  サイバー脅威の概要、国家のサイバー防衛の改善するための提案、フランス社会におけるサイバーセキュリティを向上するための機会を浮き彫りにすること、の 3 つのパートに分かれている。

  本文書の 3.1.2 項「クラウドコンピューティング戦略」において、クラウド暗号化ソリューション、特に、クラウドにおいて暗号化されたデータの処理を許可する準同型暗号、が今後の優先分野であるべきであると提言されている。

- Stratégie internationale de la France pour le numérique（フランス国際デジタル戦略）[4]

  すべての関係省庁との協議により策定され、国際的なデジタル機関との協力やガバナンス等における、フランスの今後数年間の国際的アクションのロードマップとなる文書である。2015 年 12 月 15 日、ル・ドリアン　ヨーロッパ・外務大臣により、ザキャンプにて発表された。

  ガバナンス、経済、安全保障の 3 つの分野に焦点を当てている。

  - オープン、多様な、信頼できるデジタル世界を世界規模で推進すること
  - 経済的成長、基本的権利と自由およびセキュリティのバランスの取れた欧州モデルを支持すること
  - デジタル世界におけるフランスとフランスデジタルプレーヤーの影響力、魅力、セキュリティおよび商業的地位の強化すること。

本文書の 1.3 項「インターネット上での信頼の構築」の「国際レベルでのテロ目的で

のデジタル技術の使用の対策」において、パートナーであるドイツ、イギリスの協議の上で、以下を主な目的の一つとして定めている。

- 特に EU 域外で設立された電子通信サービス提供者である場合には、法執行当局とサービス提供者のコンタクトを設定し、電子通信サービス提供者との協力体制を強化すること
- 犯罪捜査における協力義務を強化すること
- 司法当局からの要請に迅速に対応すること
- 捜査目的、特にトラフィック・位置情報へのアクセスを保持・保護し、暗号化の禁止やバックドアを許可することなく、暗号化コンテンツへのアクセスを可能にすること
- 保存場所に関わらず、国境を越えた通信のデータやコンテンツへのアクセスを高速化すること。

表 3-15　フランスにおける暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	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	更新無
2		French National Digital Security Strategy(フランス国家デジタルセキュリティ戦略)	ANSSI	後継
3		Strategic review of cyber defence February 2018（サイバー防衛の戦略的レビュー　2018 年 2 月）	SGDSN	ー
4		Stratégie internationale de la France pour le numérique （French International Digital Stragegy）（フランス国際デジタル戦略）	Ministry for Europe and Foreign（ヨーロッパ・外務省）	ー
5	暗号政策・設置法	Décret n° 2009-834 du 7 juillet 2009（2009 年 7 月 7 日付けの政令 No 2009-834）	ANSSI	更新有
6	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）	ANSSI	更新有
7		Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n°（2007 年 5 月 2 日付けの政令 2007-663 条項 30, 31 および 36）	ANSSI	更新有
8		GUIDE SUR LES EXPORTATIONS DE BIENS ET TECHNOLOGIES A DOUBLE USAGE （デュアルユースグッズ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)）	DGE、DGDDI	後継
9		Décret n° 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au	ANSSI	ー

		transfert de biens et technologies à double usage（デュアルユース物品およびテクノロジーの輸出入および移動の管理に関する 2001 年 12 月 13 日付けの政令 No 2001-1192		
10	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）	ANSSI	更新有
11		Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives（ユーザと行政機関間、行政機関間の電子交換に関する 2005 年 12 月 8 日付け条例 No 2005-1516 (Article 9)）	ANSSI	更新有
12		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 12 に対する施行令）	ANSSI	更新有
13		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（IT 製品およびシステムが提供するセキュリティの評価と認証に関する 2002 年 4 月 18 日付け政令 No 2002 535）	ANSSI	更新有
14		Ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics（公的契約に関する 2015 年 7 月 23 日付け条例 No 2015-899）	ministre de l'économie, de l'industrie et du numérique	ー
15		Arrêté du 12 avril 2018 relatif à la signature électronique dans la commande publique et abrogeant l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics（公共調達における電子署名に関する 2012 年 6 月 15 日付け法令を廃止する 2018 年 4 月 12 日付け法令）	Ministère de l'Économie, des Finances et de la Relance	ー
16	標準・基準	Référentiel général de sécurité (RGS) version 2.0（セキュリティに関する一般基準 version 2.0）	ANSSI	更新無
17		Mécanismes cryptographiques（暗号技術）	ANSSI	更新無
18		Gestion des clés cryptographiques（暗号鍵管理）	ANSSI	更新無
19		décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes（システムセキュリティニーズに対応したセキュリティ製品および信頼できるサービスプロバイダの資格認定に関する 2015 年 3 月 27 日付け政令 No 2015-530）	ANSSI	ー

20	その他	LOI no 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1) (Personal Data Protection Act)（個人情報の保護に関する 2018 年 6 月 20 日付け法律 No 2018-493）	CNIL	ー
21		Should Quantum Key Distribution be Used for Secure Communications?（安全な通信のための量子鍵を使用するべきか？）	ANSSI	ー
22		LOI n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises（企業の成長と変革に関する 2019 年 5 月 22 日付け法律 No 2019-486）	閣議決定	ー
23		RÈGLEMENT GÉNÉRAL DE L'AUTORITÉ DES MARCHÉS FINANCIERS BOOK Ⅶ - TOKEN ISSUERS AND DIGITAL ASSETS SERVICES PROVIDERS	AMF	ー
24		Law 2001-1062 of 15 November 2001 on daily security（日常のセキュリティに関する 2001 年 11 月 15 日付け法律 2001-1062	ANSSI	更新有

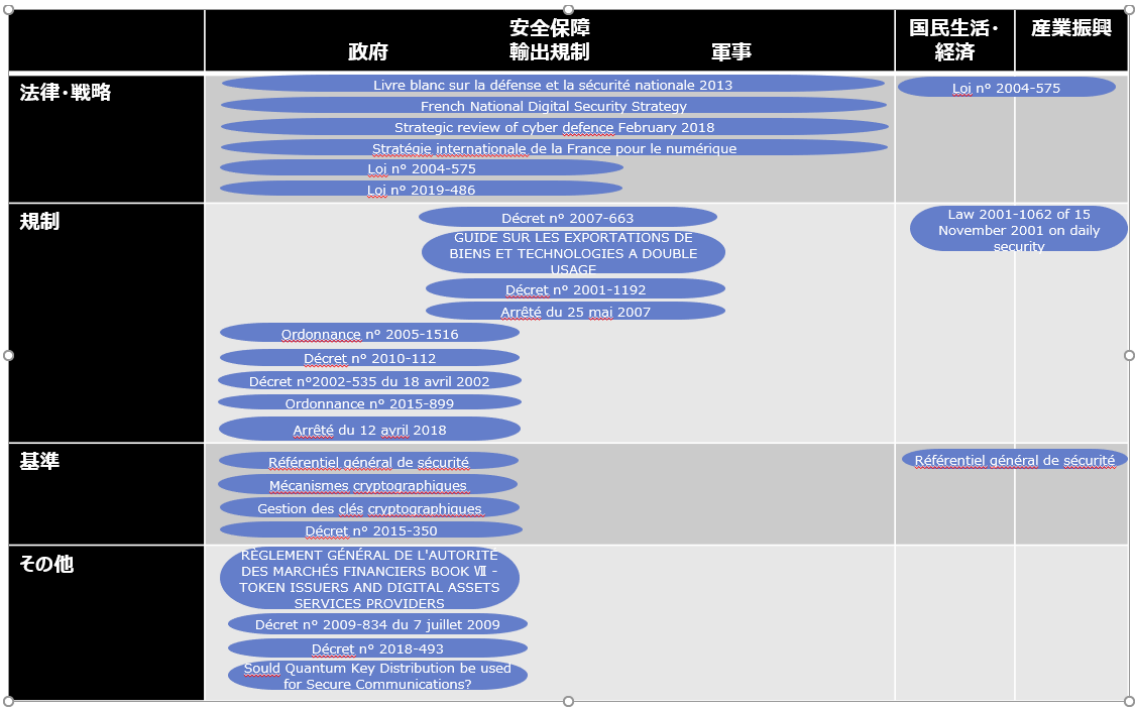


図 3-6　暗号に関連した政策マップ（フランス）

- Décret n° 2009-834 du 7 juillet 2009（2009 年 7 月 7 日付けの政令 No 2009-834）[5]

  ANSSI を情報システムセキュリティに関する規制機関とすることを定める政令である。この政令により、ANSSI が国家の情報システムのセキュリティに加えて、セキュリティ技術の研究開発やその推進することで情報社会のセキュリティに寄与し、管理者や運用者への助言やサポートを行うことを任務とすることを定めている。

2014 年 7 月以降、ANSSI の役割、任務、Comité stratégique de la SSI の構成員等に関する条項が改訂されている。

- 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）[6]
  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、安全保証、国防に関係するものは申告が必要である。
  2014 年 7 月以降、公衆にオンラインでの通信サービスへのアクセスを提供する事業者に対する要求事項、電子商取引を提供する事業者がアクセスを提供する必要がある情報、刑法の規定、本法律の適用地域に関する条項の改訂・一部廃止、テロ行為や未成年者の画像の流布等に行為に対する内容の撤回の要求に関する条項の追加、デジタルサービスの適用地域に関する条項の追加・改訂が行われた。

- Référentiel général de sécurité[15]／Mécanismes cryptographiques（暗号技術）[16]／Gestion des clés cryptographiques（暗号鍵管理）[17]
  暗号の標準・基準に関するものであり、3.3.3.1 節にまとめる。なお、2014 年 7 月以降に変更及び更新は見当たらない。

- décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes（システムセキュリティニーズに対応したセキュリティ製品および信頼できるサービスプロバイダの資格認定に関する 2015 年 3 月 27 日付け政令 No 2015-530）[18]
  情報システムセキュリティに関するセキュリティ製品（情報システムのセキュリティに関連するデバイス、ハードウェア、ソフトウェア及び機能）や信頼できるサービス提供者（情報システムのセキュリティに関連するサービスを提供する事業者）の資格取得手続きについて定める文書である。

- LOI no 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1)（Personal Data Protection Act）（個人情報の保護に関する 2018 年 6 月 20 日付け法律 No 2018-493）[19][59] [60]

[59] https://www.cnil.fr/fr/publication-de-lordonnance-de-reecriture-de-la-loi-informatique-et-libertes
[60] https://moirouxavocats.com/actualites/les-modifications-apportees-par-lordonnance-n-2018-1125-du-12-decembre-2018-a-la-loi-n-78-17-du-6-janvier-1978-relative-a-linformatique-aux-fichiers-et-aux-libertes/

情報処理、ファイルおよび自由に関する 1978 年 1 月 6 日付け法（ loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés）を欧州の個人データ保護規則（General Data Protection Regulation/GDPR）により制定された法的枠組みに適応させるために発行された法である。loi n° 78-17 の内容を大きく変更するものではなく、用語を GDPR に準拠したものへ修正、機密データの処理禁止の範囲（除外事項）の変更、GDPR によって確立された新たな権利に関する条文の追加などが行われている。

- Should Quantum Key Distribution be Used for Secure Communications?（安全な通信のための量子鍵配送を使用するべきか？）[20]
  QKD（量子鍵配送）が提供するサービスとその結果として得られるセキュリティ特性に焦点を当てた ANSSI のテクニカルポジションペーパーである。

- Law 2001-1062 of 15 November 2001 on daily security（日常のセキュリティに関する 2001 年 11 月 15 日付け法律 2001-1062）[23]
  フランスの安全保障について規定した法律である。
  2014 年 7 月以降、本法律の適用地域に関する条項が改訂された。

3.3.3. 暗号に関わる各種制度、規制及びガイドライン

3.3.3.1. 利用すべき暗号方式

ANSSI の前身 DCSSI により 2007 年に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) version 2.0（セキュリティに関する一般基準、version 2.0）
  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 3-16）、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。

なお、2014 年度調査以降に変更及び更新は見当たらない。

- “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、前者に関する規則と推奨についてまとめている。対称暗号として DES（鍵長推奨として 100 ビット以上）、非対称暗号として RSA 暗号を推奨している。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- “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。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- Gestion des clés cryptographiques（暗号鍵管理）
  なお、2014 年度調査以降に変更及び更新は見当たらない。

表 3-16 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 ビットで、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. セキュリティ製品認証制度・セキュリティサービス認証制度

フランスにおけるセキュリティ認証制度は ANSSI が所管しており、認可された検査機関による審査に基づきセキュリティビザと呼ばれるセキュリティに関する資格証（Qualification）、認証（Certification）を発行する。セキュリティビザは、市場に出回る様々なサイバーセキュリティソリューションの中で信頼性の高いものを簡単に特定できるようにするものである。国にとって極めて重要な事業者の情報システムにおけるセキュリティシステム及びサービス事業者の資格については、首相に認定権限が与えられているものの、同時に ANSSI がセキュリティ製品の資格及び認証制度を運営している。

資格証（Qualification）は、ANSSI により試験、あるいは承認されたサイバーセキュリティ製品・サービスとしてフランス国家が推奨していることを示すものである。製品の堅牢性やサービスプロバイダの適格性、製品・サービスサプライヤの信頼の基準への準拠を保証することで、ANSSI が促進する法的・技術的要件、あるいはセキュリティ要件を遵守していることを証明する。

認証(Certification)制度としては、コモンクライテリア(CC)認証、CSPN(Certification de Sécurité de Premier Niveau ）がある。ANSSI により認定された第三者機関がセキュリティニーズに合わせたスキームとベンチマークに従った適合性分析と侵入試験に基づき堅牢性を証明するものである。

- 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。評価保証レベル（EAL）に基づいて、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 のサイト[61,62]上において公開されている。2021 年 2 月時点の認証製品数は、スマートカード 181 件、マイクロチップ 108 件を含む 314 件、認証プロテクションプロファイル数は 42 件である。

[61] http://www.ssi.gouv.fr/en/products/certified-products/

[62] https://www.ssi.gouv.fr/administration/produits-certifies/cc/profils-de-protection/

なお、調査時点（2021 年 2 月）の CCRA 向けの有効な CC 認証取得は、310 製品である。以下に認証取得と EAL を示す。

表 3-17　EAL ごとの Common Criteria 認証取得数（フランス）[63]

EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6+	EAL7	Total
0	0	0	2	0	17	2	63	6	198	20	2	310

- CSPN[64]

  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。CSPN の評価機関は、基本的に、25 人日で、8 週間以内に完了しなければならないが、暗号アルゴリズムに基づくセキュリティ機能を持つ製品の場合、その分析の実施を可能にするために 10 人/日が追加される。

  2019 年 6 月 1 日時点で、141 の製品が CSPN 認証を取得している。

CC 認証、CSPN 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。CSPN ではブラックボックステストが実施されている。目的とする信頼度のレベルが低い場合、費用面と評価期間の負担が大きい CC 認証に代わるものとなる。

資格証（Qualification）とは、ANSSI が承認したサイバーセキュリティ製品およびサービスを、国家が推薦することである。製品の堅牢性とサービス提供者の能力を保証し、ソリューション提供者が適切な信頼の基準の遵守に責任を持つことで、ANSSI が推薦する規制、技術的及び安全性の要件を遵守することを証明するものである。

3.3.3.3.　政府の調達要件

CC 認証や CSPN 認証の取得製品、あるいは Qualification 取得の製品やサービスを調達するように定めている規則やルールは見当たらなかった。その他の政府の調達要件には、以下のものがある。

- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives（ユーザと行政機関間、行政機関間の電子交換に関する 2005 年 12 月 8 日付け条例 No 2005-1516（Article 9））

[63] Certified Products List - Statistics : New CC Portal https://www.commoncriteriaportal.org/products/stats/

[64] https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/presentation/

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。
2014 年 7 月以降、本条例における行政当局の定義および本条例の適用地域に関する条項が改訂され、電子的手段で行われる行政手続きの簡素化および国による電子証明書の検証に関する条項が廃止された。

- 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 12 に対する施行令）
  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。
  2014 年 7 月以降、セキュリティリファレンスシステム、情報システムのセキュリティ機能、トラストサービスプロバイダを認定する機関の権限、違反の場合の認定の一時停止または取り消し、トラストサービスプロバイダの認定に関する条項および雑則が改訂されている。

- 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（IT 製品およびシステムが提供するセキュリティの評価と認証に関する 2002 年 4 月 18 日付け政令 No 2002 535）
  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。
  2014 年 7 月以降、認証、審査センターの承認、本政令の適用地域に関する条項が改訂された。

- Ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics（公的契約に関する 2015 年 7 月 23 日付け条例 No 2015-899）[65]
  公的契約について定める条例であったが、2019 年 4 月 1 日に発効された公共調達コード（Public Procurement Code）に集約された。公共調達コードは、公共団体や事業者が、公共調達契約を締結・実施するために日常的に使用されていた約 30 の法や規制を統合したものである。2018 年 11 月 26 日付け条例 No. 2018-1074（Ordonnance n° 2018-1074）（公共調達コード（Public Procurement Code）の立法に関する条例）、2018 年 12 月 3 日付け政令（Décret n° 2018-1075）（公共調達コードの規制に関する政令）の発行により制定された。

[65] https://www.whitecase.com/publications/alert/first-french-public-procurement-code-has-entered-force

- Arrêté du 12 avril 2018 relatif à la signature électronique dans la commande publique et abrogeant l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics（公共調達における電子署名に関する 2012 年 6 月 15 日付け法令を廃止する 2018 年 4 月 12 日付け法令）
  これまで標準であった RGS 電子証明書から 2017 年 7 月 23 日付け規則 910/2014（eIDAS 規則）への移行を行うために発行された政令である。

3.3.3.4.　暗号の輸出入規制

フランスにおいてはワッセナー・アレンジメント（Wassenaar Arrangement）に署名し、輸出規制を行っている。そのため、規制対象となる暗号製品等は、ワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）」のなかのデュアルユース製品・技術に関するリストのカテゴリ 5 パート 2（Category 5 – Part 2 “Information Security”）がベースになっている。（参考：3.1.3.4 節のワッセナー・アレンジメント）

輸出入は、以下の Décret n° 2007-663 du 2 mai 2007 に基づき規制されている。暗号製品の輸出入規制は ANSSI が行う。

- 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（暗号のリソースとサービスに関するデジタル経済の信頼性に関する 2004 年 6 月 21 日付け法令 2005-575 の条項 30, 31, および 36 を実施する 2007 年 5 月 2 日付けの政令 2007-663）
  暗号手段・サービスの提供、輸送、および輸出入の際に必要となる事前の手続きについて規定する政令である。事前の手続きには、申告（Declaration）と認可（Authorization）の二種類があり、本政令の Annex に記載される場合と防衛法（Defence Code）第 L.2335-1 条から第 L.2335-3 に規定される輸出入の許可を受けた暗号手段の輸送・輸出入については、これらの手続きが免除される。
  以下の場合には、申告（Declaration）の対象となり、暗号手段またはサービスの提供・輸送、輸出入の少なくとも 1 か月前に、申告書類を ANSSI に提出しなければならない。
  - 事前の手続きが免除されない暗号手段・サービスのうち、EU 加盟国から提供、輸送される場合、および、認証または完全性の制御機能のみを提供しない暗号手段の輸入の場合。
  - 本政令の Annex 2 に記載される暗号手段の輸送または輸出の場合。
  - 本政令の Annex 1 に記載されない暗号サービスの提供。

  書類に不備がある場合や製品が認可（Authorization）の対象となると判断された場合、

ANSSI は、申告書類の受領から一か月以内にその旨を申告者に知らせる。1 か月以内に ANSSI より連絡がない場合、申告者は申告を行った暗号手段・サービスの提供、輸送、輸入を開始することができる。

事前の手続きが免除されない暗号手段・サービスであり、上記の申告の条件にもあてはまらない場合には、認可（Authorization）が必要である。認可リクエスト書類を ANSSI に提出し、書類に問題がなければ、ANSSI が書類の受領を確認した日より 4 か月以内に、ANSSI の長官による決定が通知される。

本政令の Annex は以下の通りである。

Annex 1： 事前の手続きを免除される EU 加盟国内における提供と輸送、輸入と輸出。

以下の暗号手段を、EU 加盟国内で提供、輸送する場合、または輸出入を行う場合：

- カテゴリ 1：消費者アプリ向けにパーソナライズされたスマートカード。
  - 以下のカテゴリ 2、3、4、5 に該当する機器のみとの使用のために暗号機能が設計され、制限されている場合。
  - ユーザが暗号機能にアクセスできない場合で、保存されているデータの保護を可能にするために特別に設計され、制限されたものである場合。
- カテゴリ 2：一般市民向けのラジオ・テレビ受信機であり、その暗号機能が請求書発行、管理または番組編成に限られ、復号が、ビデオ、オーディオ、技術管理機能に限定されるもの。
- カテゴリ 3:一般市民向けで、銀行、金融業務での使用のために特別に設計され、限定されたもので、ユーザが暗号機能にアクセスできないもの。
- カテゴリ 4：一般市民向けのモバイル無線通信機器であり、無線チャンネルを保護するためにネットワークオペレータによって実装された暗号機能のみを有し、無線機器間で直接暗号化を行うことができないもの。
- カテゴリ 5：一般市民向けのコードレス電話機で、直接、電話機間の暗号化を行うことができない、製造者の仕様では電話機とその基地局の距離が 400 メートルを超えないもの。
- カテゴリ 6:違法なコピーや使用からソフトウェアやコンピュータのデータを確実に保護するために特別に設計され、限定されたもので、ユーザがその暗号機能にアクセスできないもの。
- カテゴリ 7：暗号機能がなく、オーディオビデオデータの再生のために特別に設計され、限定されたもので、復号が、オーディオ、ビデオ、技術管理情報に限定された自動機器。

以下のカテゴリの暗号手段を、EU 加盟国内で輸送、または輸出入を行う場合：

- カテゴリ 8：以下により輸送される、暗号手段を有する機器。
  - 国家より正式な依頼を受けた外国人。
  - 自然人であり、その人物の使用のみを目的とした機器。

以下のカテゴリの暗号手段を、EU 加盟国内で提供、輸送、または輸入を行う場合：

- カテゴリ 9：一般市民向けのモバイル機器に接続するために設計された民間の商業用セルラー無線通信基地局で、モバイル機器間のデータ通信に、直接暗号機能を適用することを許可しないもの。
- カテゴリ 10：一般市民向けの機器で、無線通信によりデータを交換することを許可し、機器の暗号機能単体が、IEEE 802.15.1、IEEE 802.15.3、IEEE 802.15.4、IEEE 802.11a、IEEE 802.11b、IEEE 802.11g に従って設計されているもの。
- カテゴリ 11：システムの管理、設定に必要なデータのみを暗号化し、他の全てのデータを除外することを許可することを条件として、情報システムの管理、設定のために特別に設計され、限定された暗号手段。

以下のカテゴリの暗号手段を、EU 加盟国から提供、輸送、または輸入を行う場合：

- カテゴリ 12：以下専用の暗号手段：
  - 電子的手段によるものを含め、輸入または輸送する自然人が使用する場合。
  - 電子的手段によるものを含め、輸入または輸送する人物による開発、検証、実証を目的とする場合。

以下のカテゴリの暗号手段を、EU 加盟国へ輸送、または輸出する場合：

- カテゴリ 13：以下のいずれかの特性を有する暗号アルゴリズムを実装しない暗号手段。
  - 鍵長が 56 ビットを超える対称暗号アルゴリズム。
  - 512 ビットを超える整数の因数分解、または 512 ビットを超える有限体の乗法群または 112 ビットを超えるその他タイプの群における離散対数の計算に基づく非対称暗号アルゴリズム。
- カテゴリ 14：超広帯域変調システム用のチャネライゼーションコード、スクランブルコード、ネットワーク識別コードを生成するための暗号手段で、以下のいずれの特性も有しないもの。
  - 500MHz を超える帯域幅。
  - 電力が 3dB で一定に保たれる帯域幅として定義される比帯域を中心周波数で割って、20%以上のパーセンテージである場合。

以下のカテゴリの暗号サービスを提供する場合：

- カテゴリ 15：上記カテゴリ 1、2、3、4、5 に該当する暗号手段の実施を目的とした暗号サービスで、2001 年 3 月 30 日付け政令の第 1 条において電子証明書の発行またはその他の電子署名サービスの提供から構成されないサービスであること。

Annex 2： 宣言の対象となる、EU 加盟国への輸送と輸出。
以下のカテゴリの暗号手段を、EU 加盟国へ輸送、または、オーストラリア、カナダ、米国、日本、ニュージーランド、ノルウェー、スイスへ輸出する場合。

- カテゴリ 1： 認証又は完全性の管理機能を排他的に保証しない暗号手段であり、以下に実装されている場合。
  - 鍵長が 56 ビットを超える対称暗号アルゴリズム
  - 512 ビットを超える整数の因数分解、または 512 ビットを超える以上の有限体の乗法群または 112 ビットを超えるその他タイプの群における離散対数の計算に基づく非対称暗号アルゴリズム。
- カテゴリ 2： 超広帯域変調システム用のチャネライゼーションコード、スクランブルコード、ネットワーク識別コードを生成するための暗号手段で、以下のいずれかの特性を有する場合。
  - 500MHz を超える帯域幅。
  - 電力が 3dB で一定に保たれる帯域幅として定義される比帯域を中心周波数で割って、20%以上のパーセンテージである。

以下のカテゴリの暗号手段を、上記で記載する国以外に輸出する場合：

- カテゴリ 3： 上記のカテゴリ 1、2 に該当する暗号手段で、以下の条件を全て満たす場合。
  - 店頭、通信販売、電子取引または電話による販売のいずれの場合も、在庫から直接、制限なく小売店で販売され、市民が日常的に入手可能である場合。
  - ユーザが暗号機能を容易に変更することができない場合。
  - サプライヤからの大きなサポートなしで、ユーザがインストールできるように設計されている場合。

2014 年 7 月以降、暗号輸入と輸出を行う場合の事前の宣言、承認の取り消し、首相から ANSSI に与えられる権限に関する条項に改訂が行われた。

- GUIDE SUR LES EXPORTATIONS DE BIENS ET TECHNOLOGIES A DOUBLE USAGE[8] (GUIDE ON EXPORT OF GOODS AND DUAL-USE TECHNOLOGIES)

デュアルユースグッズや技術の輸出手続きを容易にするために、2015 年 2 月に関税・間接税総局（DGDDI）により作成されたガイドラインである。暗号製品のデュアルユースグッズの輸出については ANSSI が所管しており、事前の輸出許可を取得する必要がある。

- Décret n° 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage（デュアルユース物品およびテクノロジーの輸出入および移動の管理に関する 2001 年 12 月 13 日付けの政令 No 2001-1192）
  デュアルユースグッズおよびテクノロジーの輸出入に関する法令である。

3.3.3.5. プロトコル等での暗号方式

今回調査した文献の中では本節に該当する文献は発見できなかった。

3.3.3.6. 暗号利用に関する規制（利用ライセンス・反暗号法・暗号盗聴法など）

- （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）[6]
  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、安全保証、国防に関係するものは申告が必要である。
  2014 年 7 月以降に、公衆にオンラインでの通信サービスへのアクセスを提供する事業者に対する要求事項、電子商取引を提供する事業者がアクセスを提供する必要がある情報、刑法の規定、本法律の適用地域に関する条項の改訂・一部廃止、テロ行為や未成年者の画像の流布等に行為に対する内容の撤回の要求に関する条項の追加、デジタルサービスの適用地域に関する条項の追加・改訂が行われている。

3.3.3.7. クラウドサービス

- （再掲）French National Digital Security Strategy（フランス国家デジタルセキュリティ戦略）
  5 つ目の戦略的優先事項（目標）「欧州、デジタル戦略的自立性、サイバースペースの安全性」に、フランスが任意の EU 加盟国とともに、欧州における戦略的自立性の原動力となることが記述されており、その中で、ドイツとともに、クラウドコンピューティングおよび両国間の暗号化されたメールのやりとりに関する取り組みを行っていることが述べられている。

3.3.3.8. 暗号資産

- LOI n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises(企業の成長と変革に関する 2019 年 5 月 22 日付け法律 No 2019-486)[21][66] [67]

  PACTE 法と呼ばれ、中小企業の成長を促進するものである。2019 年 5 月 24 日に制定された。

  この法内で、デジタルファイナンスについて規定されている。仮想トークンの発行（イニシャルコインオファリング（ICO））は任意のビザ、デジタルアセットサービスプロバイダ（DASP）は任意の承認を、それぞれ AMF（Autorité des marches financiers/金融市場機関）から取得することができるようになった。これらの取得はオプション(任意)であるが、第三者へのデジタル資産保管サービス提供者や、法廷通貨と引き換えにデジタル資産の売買を希望するサービス提供者は、AMF への登録が義務付けられている。

- RÈGLEMENT GÉNÉRAL DE L'AUTORITÉ DES MARCHÉS FINANCIERS BOOK Ⅶ - TOKEN ISSUERS AND DIGITAL ASSETS SERVICES PROVIDERS[22]

  イニシャルコインオファリングを行うトークン発行者およびデジタルアセットサービスプロバイダに対して適用される規定が記述されている。

3.3.3.9. 電子署名法

今回調査した文献の中では本節に該当する文献は発見できなかった。

3.3.3.10. 国民 ID 番号制度（eID）

今回調査した文献の中では本節に該当する文献は発見できなかった。

---

66 https://www.amf-france.org/en/node/59937

67 https://www.kramerlevin.com/en/perspectives-search/with-the-enactment-of-the-loi-pacte-the-french-regulatory-framework-for-crypto-activities-and-icos-becomes-effective.html

3.3.4. フランスの参照文献

[1] Livre blanc sur la défense et la sécurité nationale 2013
http://www.livreblancdefenseetsecurite.gouv.fr/

[2] French National Digital Security Strategy
https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

[3] Strategic review of cyber defence February 2018
http://www.sgdn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

[4] Stratégie internationale de la France pour le numérique
https://et.ambafrance.org/La-strategie-internationale-de-la-France-pour-le-numerique

[5] Décret n° 2009-834 du 7 juillet 2009
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212

[6] Law no. 2004-575, 21 June 2004 on confidence in the digital economy
https://www.legifrance.gouv.fr/loda/id/LEGITEXT000005789847/2021-01-26/

[7] 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
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000646995/2021-01-26/#:~:text=juin%202004%20...-,D%C3%A9cret%20n%C2%B02007%2D663%20du%202%20mai%202007%20pris,et%20aux%20prestations%20de%20cryptologie.

[8] GUIDE SUR LES EXPORTATIONS DE BIENS ET TECHNOLOGIES A DOUBLE USAGE
https://www.douane.gouv.fr/sites/default/files/uploads/files/2019-04/2015-fevrier-guide-bdu.pdf

[9] Décret n° 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage
https://www.legifrance.gouv.fr/loda/id/LEGITEXT000005631830/2021-01-26/

[10] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/2021-01-26/

[11] 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
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000021779444/

[12] 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

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000412673?r=J3JObEbfcX
[13]Ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030920376/2021-01-26/
[14]Arrêté du 12 avril 2018 relatif à la signature électronique dans la commande publique et abrogeant l'arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036819 83#:~:text=Article%208-,L'arr%C3%AAt%C3%A9%20du%2015%20juin%202012%20relatif%20%C3%A0%20la%20signature,dispositions%20jusqu'%C3%A0%20leur%20expiration.
[15]Référentiel général de sécurité (RGS) version 2.0
https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/
[16]Mécanismes cryptographiques
https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf
[17]Gestion des clés cryptographiques
https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B2.pdf
[18]décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systems
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030405903/2021-01-26/
[19]LOI no 2018-493 du 20 juin 2018 relative à la protection des données personnelles
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952/
[20]Should Quantum Key Distribution be Used for Secure Communications?
https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/#:~:text=Although%20QKD%20can%20be%20used,next%20step%20for%20secure%20communications.
[21]LOI n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038496102/
[22]RÈGLEMENT GÉNÉRAL DE L'AUTORITÉ DES MARCHÉS FINANCIERS BOOK Ⅶ - TOKEN ISSUERS AND DIGITAL ASSETS SERVICES PROVIDERS
https://reglement-general.amf-france.org/eli/fr/aai/amf/rg/20200518/notes/en.pdf
[23]Law 2001-1062 of 15 November 2001 on daily security
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052&dateTexte=20200910

3.4. ドイツ

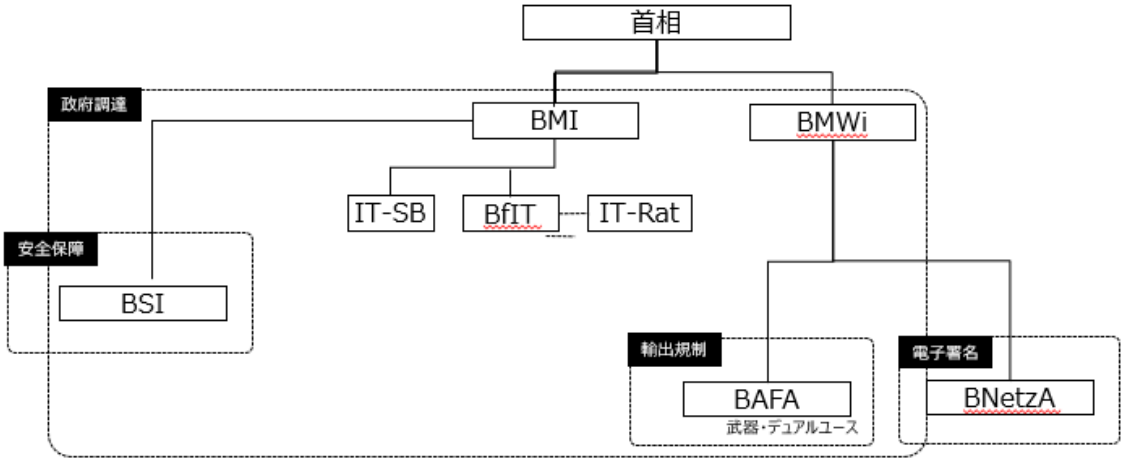
ドイツにおいては、BMI（連邦内務省/ Bundesministerium des Innern, für Bau und Heimat）の一部門である BSI（連邦情報セキュリティ庁/ Bundesamt für Sicherheit in der Informationstechnik）が、情報社会における IT セキュリティに関するあらゆる問題を取り扱っている。ドイツにおいては、2015 年に「Grobkonzept zur IT-Konsolidation Bund（Rough Concept for Federal IT Consolidation）」が閣議決定され、2025 年までに連邦政府の IT をバンドル化・標準化するプロジェクトが開始された。IT は、国家や行政の機能、経済・社会の発展のために重要な役割を果たしており、ドイツ連邦政府は、年間約 30 億ユーロを IT に費やしている。連邦政府の IT システムの政治的・戦略的な管理が必要となっており、この任務は BfIT（Beauftragten der Bundesregierung für Informationstechnik/連邦政府情報技術長官）と IT-Rat（IT Council/IT 担当者協議会）により実施されている。

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

BSI は、連邦政府、企業、民間のユーザに、IT システムの安全な利用のための推奨事項を、技術指針（TR）として提供している。また、DIN（ドイツ工業規格協会）NA 043-01-27 AA や SOG-IS との協力により、暗号分野における国際的なガイドラインや標準の策定・維持にも関与している。

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（連邦経済・輸出管理庁/Bundesamt für Wirtschaft und Ausfuhrkontrolle）による輸出規制がある。電子署名については BnetzA（連邦ネットワーク庁/ Bundesnetzagentur）が担当している。

図 3-7 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：Bundesministerium des Innern, für Bau und Heimat（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（連邦情報技術長官）
IT-Rat:Rat der IT-Beauftragten（州政府 IT 担当者協議会）
IT-SB：IT-Steuerungsgruppe des Bundes（連邦 IT 運営委員会）
BMWi：Federal Ministry for Economic Affairs and Energy（ドイツ連邦経済・技術省）
BNetzA：Federal Network Agency（連邦ネットワーク庁）
BAFA：Federal Office for Economic Affairs and Export Control（経済・輸出管理局）
DFG：German Research Foundation

図 3-7　暗号政策に係る組織体制（ドイツ）

- BMI（Bundesministerium des Innern, für Bau und Heimat、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。また、2015 年より開始された Federal IT Consolidation を主管している。

- BSI（Bundesamt für Sicherheit in der Informationstechnik、連邦情報セキュリティ庁）
  ドイツにおける IT セキュリティを主管する部門で、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、具体的には連邦政府ネットワーク保護やネットワークへの攻撃の検出、IT 製品およびサービスの試験・認証、マルウェアやセキュリティギャップの警告、IT セキュリティ標準の開発などである。

- BfIT（Beauftragten der Bundesregierung für Informationstechnik、連邦情報技術長官）
  2007 年の閣議決定 IT-Steuerung Bund に基づき設置された。BfIT の最も重要な任務は、IT-Rat 及び IR 担当官会議（Konferenz der IT-Beauftragten）とともに、省庁間の IT の連携を省庁間の IT の統制に拡大することである。連邦行政における IT 利用の戦略的課題に責任を持ち、行政における IT の設計に重大な影響を与える立法手続きや政府プロジェクトに関与する。

- BMWi（Bundesministerium für Wirtschaft und Energie、ドイツ連邦経済・エネルギー省）
  ドイツにおける政府調達の原則と法的枠組みを定義している。BAFA、BnetzA は BMWi の一部門である。

- BnetzA（Bundesnetzagentur、連邦ネットワーク庁）
  BMWi の下に設置され、電気、ガス、通信、郵便及び鉄道分野を主管している。電子署名

法に基づくルート CA(ルート認証局)である。

- BAFA（Bundesamt für Wirtschaft und Ausfuhrkontrolle 、経済・輸出管理庁）
  BMWi の下に設置された輸出管理を行う組織である。

- 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 に基づき設置された。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 に基づき設置された。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。

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[68]。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 3-18 と図 3-8 のようになる。

表 3-18 ドイツにおける暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	上位政策・戦略	Cyber Security Strategy for Germany	BMI	後継
2		Grobkonzept zur IT-Konsolidierung Bund	閣議決定	後継
3		IT-Strategie der Bundesverwaltung 2017-2021	BSI	―
4	暗号政策・設置法	Eckpunkte der deutschen Kryptopolitik 1999 (Principles of German Crypto Policy)	閣議決定	更新無
5		Vertrauensdienstegesetz (VDG)	BMWi	後継
6		Act on the Federal Office for Information Security (BSI Act - BSIG)	BSI	更新有

[68] 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。

7		Architekturrichtlinie für die IT des Bundes(Architecture Guideline for Federal IT)	BMI	—
8		Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)	BSI	—
9	輸出入規制	外国貿易法（AWG）、外国貿易法施行令（AWV）	BMWi	AWG のみ更新有
10		CHP Act 2016 (KWKG 2016)	BMWi	後継
11		Zertifizierungsverfahren nach § 9 AWG, 2 AWV und Art. 9 der Verteidigungsgüterrichtlinie (2009/43/EG)	BAFA	—
12	政府調達	Standards and Architectures for eGovernment Applications (SAGA) 5.1	BMI, BfIT, BSI	更新無
13		BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths	BSI	更新有
14		BSI TR-02102-2: Cryptographic Mechanisms: Recommandations and Key Lengths: Use of Transport Layer Security (TLS)	BSI	更新有
15		BSI TR-02102-3: Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)	BSI	更新有
16		IT Baseline Protection Catalogues (IT-Grundschutz)	BSI	後継
17	DGCIS 標準・基準その他	Guidelines for Developer Documentation according to Common Criteria Version 3.1	BSI	更新無
18		Produktzertifizierung: Programm IT-Sicherheitszertifizierung Common Critieria (CC)	BSI	更新有
19		Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 1: Telematikinfrastruktur	BSI	—
20		Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2: eID-Karten und hoheitliche Dokumente	BSI	—
21		Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3: Intelligente Messsysteme	BSI	—
22		Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4: Kommunikationsverfahren in Anwendungen	BSI	—
23		Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API	BSI	—
24		De-mail Law	BSI	更新有
25	その他	Kreditwesengesetz - KWG	BaFin[69]	—
26		Referentenentwurf des Bundesministeriums der Justiz und	BMI, BMJV	—

[69] Bundesanstalt für Finanzdienstleistungsaufsicht（連邦金融監督庁）

		für Verbraucherschutz und des Bundesministeriums der Finanzen, Entwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren		
27		Migration zu Post-Quanten-Kryptografie	BSI	—
28		Das Standard Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele Version 2.0		—

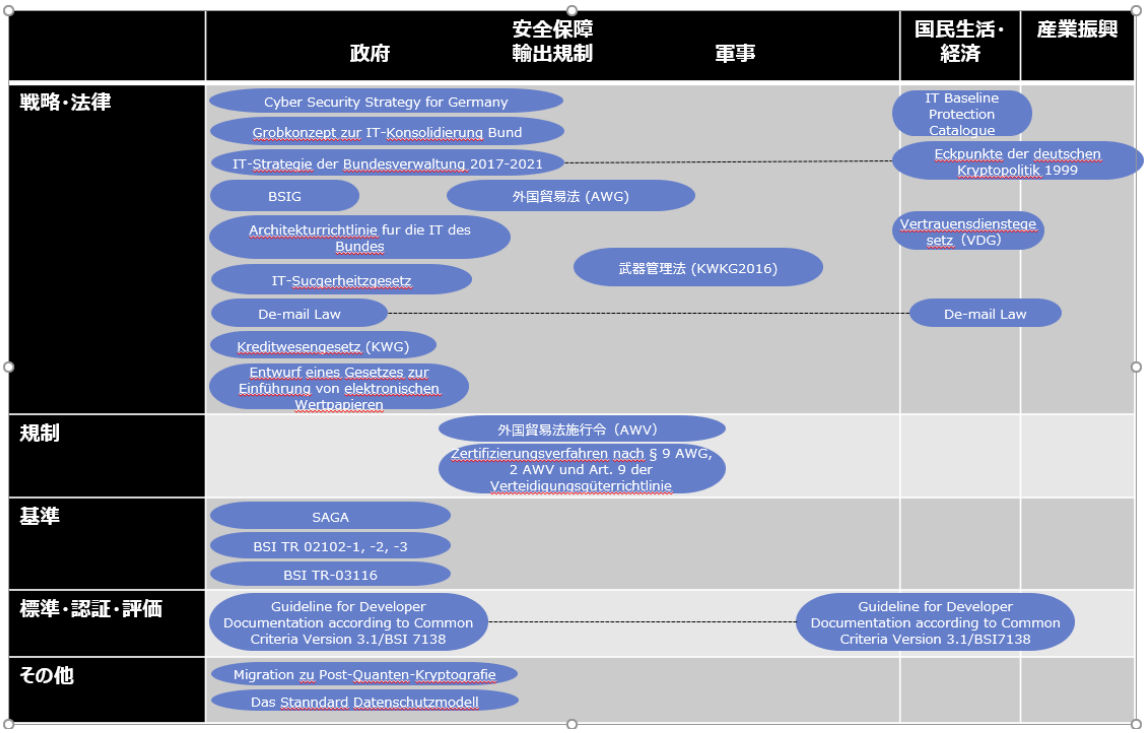


図 3-8　暗号に関連した政策マップ（ドイツ）

主な法制度の概要は以下の通りである。

- Cyber Security Strategy for Germany[1]
  2011 年 2 月に策定された戦略的フレームワークの後継として、2016 年 11 月に新たに発行されたサイバーセキュリティ戦略である。2011 年以降、サイバーセキュリティは、連邦政府の多くの戦略的計画や省庁間プロジェクトにおいて重要な要素となっている。2011 年の戦略は現在も有効なものであるが、常に変化する状況の中で、この戦略を拡大し、サイバーセキュリティの関連性と水平的な性質に注意を払い、この問題に包括的に対応する省庁間の取り組みに組み込む必要がある。本戦略は、サイバーセキュリティに関する連邦政府の活動に関する省庁間の戦略的フレームワークを提供するものである。

- Grobkonzept zur IT-Konsolidierung Bund[2]

  2015 年の閣議決定により開始された IT-Konsolidierung（IT コンソリデーション）プロジェクトの概要を示す文書である。

  プロジェクトは以下を目標としている。

  - 複雑化する環境における情報セキュリティの確保
  - IT に対する恒久的な主権と制御
  - 革新的な技術動向への柔軟な対応
  - 効率的・経済的・安定的で持続可能な運用の確保
  - IT スペシャリストにとって魅力的な雇用主であり続けること

  IT コンソリデーションは 4 つのアクションで構成される。

  - 事業の統合

    2023 年までに、連邦行政直属の IT 運用を少数のデータセンターに集約し、それに対応したシステムプラットフォームとセキュリティ基準の標準化を行うことを目標としている。これにより、コスト削減と適切なセキュリティレベルを確保することが可能になる。
  - サービスの統合

    2025 年までに、連邦政府の同様のユースケースを対象とする統一された、高性能で安全な IT ソリューションを開発することを目標としている。現在は、41 種類のサービスを統合する IT 施策として実施されているが、将来的には約 200 の政府機関が利用可能ものにし、IT の標準化と近代化だけでなく、業務プロセスのデジタル化や変更を可能にするものである。

    このプロジェクトは、BMI が一元管理をしているが、個々の IT 施策は各省庁により実施される。
  - サービス提供者の向上

    ITZBund[70]（Informations Technik Zentrum Bund）と BWI GmbH[71]は、業務とサービスを統合し、課題に対応できるようにする。
  - 調達のバンドル化

    連邦政府直属の IT 調達は、ZIB（Zentralstelle für IT-Beschaffung）が一括で管理を行う。

    ・ IT ハードウェア
    ・ ソフトウェア
    ・ 情報通信技術
    ・ IT サービスおよび IT 関連サービス

[70] https://www.itzbund.de/DE/home/home_node.html
[71] https://www.bwi.de/

- IT-Strategie der Bundesverwaltung 2017-2021[3][72]
  BMI の連邦政府情報技術委員会（Federal Government Commissioner for Information Technology）によって策定される政府の IT 戦略である。少なくとも 5 年毎に政治的・技術的な発展に合わせて更新される。全省庁における IT の戦略的目標を定義するものである。
  上記 Grobkonzept zur IT-Konsolidierung Bund に基づいて策定されおり、第 2 章に IT 戦略の原則、第 3 章に戦略的 IT 目標、第 4 章に行動分野、第 5 章に IT 戦略の継続と運用の見通しが述べられている。

- 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[73]。
  - 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）

  なお、2014 年度調査以降に変更及び更新は見当たらない。

- Vertrauensdienstegesetz（VDG）（Trust Service Act）[5][74]
  欧州における eIDAS 規則（Regulation No. 910/2014）の施行により、2017 年 7 月 18 日に、Act on Digital Signature (SigG)／Digital Signature Ordinance (SigV)に代わる法として施行された。本法の施行により、SigG/SigV は失効された。

- Act on the Federal Office for Information Security (BSI Act - BSIG)[75]
  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

---

[72] https://www.cio.bund.de/SharedDocs/Kurzmeldungen/DE/2017/20170628_it_strategie_der_bundesverwaltung.html

[73] 前回調査におけるドイツの研究機関へのヒアリングによる。

[74] https://www.secrypt.de/en/useful-information-and-legal-issues/

[75] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html

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。
2009 年 8 月 20 日の発効以降、料金に関する軽微な変更のみが行われたが、2015 年 7 月 25 日に施行された Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme（IT-Sicherheitsgesetz/IT セキュリティ法）により大きく改正され、BSI に、新たな任務と権限が与えられた。（詳細は以下の IT-Sicherheitsgesetz 参照）

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme（IT-Sicherheitsgesetz）[8]
  ドイツの IT システムとデジタルインフラを世界で最も安全なものにし、企業や連邦政府の IT セキュリティを強化し、インターネット上での市民の保護を強化するために、2015 年 7 月に施行された法である。
  この法の施行により、BSI の任務と権限が拡大された。障害が発生した場合にドイツの経済、国家、社会に影響を及ぼす可能性のある重要インフラ（KRITIS/ Kritischen Infrastrukturen）のネットワークセキュリティを向上することを目的とおり、また、KRITIS の事業者に対して、重大な IT セキュリティインシデントが発生した場合に BSI に報告することが義務付けている。
  2020 年 12 月 16 日、連邦政府は、BMI により提出された IT-Sicherheitsgesetz 2.0 の草案を可決した。この草案には、BSI の機能のさらなる強化、消費者保護の強化、企業の予防措置の強化、国家の保護機能の強化に関する規定が含まれている。BSI は、連邦政府の通信技術を脅威から保護するためにログデータの処理や、情報セキュリティに対する脅威が発生した場合に電気通信企業に対して対策を命令する権限を与えられる。

- Architekturrichtlinie für die IT des Bundes (Architecture Guideline for Federal IT)[7]
  連邦政府の IT コンソリデーションとって、包括的な IT アーキテクチャ管理が必要不可欠である。このガイドラインは、IT コンソリデーションを促進し、矛盾した開発を避け、各省庁の活動を積極的に支援することを目的として策定されたものである。2017 年に初めて策定され、以降、各省庁の関与により毎年更新されている。
  SAGA の仕様が本ガイドラインに統合され、必要に応じて更新されている。
  現在公開されている最新版は 2020 年 7 月 31 日付けの Version 2020 である。2020 年版の 4.7 章の”Architekturvorgaben zur Informationssicherheit”において、保護が必要とされる IT 手続きに、承認されている最新の技術に基づく暗号を利用することが規定されている。暗号の利用については、BSI の技術ガイドライン（BSI TR-02102-1）及び BSI TR-03116-X を考慮するよう要求している。トランスポートレイヤーセキュリティ（TLS）については BSI の MSO.APP.TLS、連邦国防省（Bundesministerium der

Verteidigung /BMVg）の分野においてはNATOの規定、特定のIT手続きにおけるアーキテクチャ要件では、DSGVO（EU一般データ保護規則）、VSA（VPSサービスアダプタ）による暗号化が要求されている。

- 外国貿易法（AWG）[9]／外国貿易法施行令（AWV）[10]／武器管理法（KWKG）
  3.4.3.4節にて記載。なお、2014年7月以降に更新があることに留意されたい。

- Zertifizierungsverfahren nach § 9 AWG, 2 AWV und Art. 9 der Verteidigungsgüterrichtlinie (2009/43/EG)[12]
  AWG、AWV、防衛機器の域内移動の容易化に関する指令（2009/43/EG）に従い、防衛機器を受け取る企業を認証する手続きを規定する文書である。

- Standards and Architectures for eGovernment Applications (SAGA)[13]／Technische Richtlinien Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102-1)[14]／Verwendung von Transport Layer Security (TLS) (BSI TR-02102-2)[15]／Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2) (BSI TR-02102-1)[16]
  3.4.3.1節にまとめる。なお、2014年度調査以降に変更及び更新は見当たらない。

- IT-Grundschutz-Catalogue 15. Version - 2015
  すべてのITシステムで考慮すべき標準的なセキュリティ保護策が記載されているカタログである。2016年に、2015年版としてBSIより公開されたが、ドラフト版であり、編集上のバグがある可能性があることが補足されている。本カタログには、以下が記載されている。
  - 典型的なビジネスプロセス、アプリケーション、および通常の保護要件のITシステムの標準的なセキュリティ保護策
  - 通常適用される脅威のシナリオの説明
  - 保護策の実施を容易にするための詳細な説明

  国際的にも参照されている文書である為、本カタログおよびその関連文書もデジタル形式で、英語のものが公開されている。
  2015年版では、サービス指向アーキテクチャ(SOA)に関するモジュールが追加された。各モジュールにおいて、暗号の使用や推奨する暗号メカニズムについて記述されている。

- Guidelines for Developer Documentation according to Common Criteria Version 3.1[18]/Produktzertifizierung: Programm IT-Sicherheitszertifizierung Common Critieria (CC)[19]
  3.4.3.2 節にて記載。なお、BSI 7138 Technical information on the IT security certification of products, protection profiles and sites については、2014 年 7 月以降に変更があることに留意されたい。詳細は 3.4.3.2 節参照のこと。

- Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 1: Telematikinfrastruktur[20]/Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2: eID-Karten und hoheitliche Dokumente[21]/Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3: Intelligente Messsysteme[22]/Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4: Kommunikationsverfahren in Anwendungen[23]/Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API[24]
  連邦政府のプロジェクトの暗号仕様について規定する技術ガイドラインである。
  - パート 1：テレマティクスインフラストラクチャ
    電子健康保険証、医療従事者カード、テレマティクスインフラストラクチャの技術コンポーネントへの暗号の使用に関するセキュリティ要件と仕様を定義する。
  - パート 2：身元確認文書
    電子パスポート、eID カード、電子滞在許可証、到着証明などの身元確認文書への暗号の使用に関するセキュリティ要件を定義する。
  - パート 3：スマートメータリングシステム
    スマートメータリングシステムへの暗号の使用に関するセキュリティ要件を定義する。
  - パート 4：アプリケーションにおける通信手段
    連邦政府のアプリケーションにおける通信手段の使用に関するセキュリティ要件を定義している。
  - パート 5：セキュアエレメント API のアプリケーション
    セキュアエレメント API のアプリケーションでの暗号の使用に関するセキュリティ要件を定義している。

- De-mail Law[25]
  3.4.4.2 節にて記載。なお、2014 年 7 月以降に変更があることに留意されたい。

3.4.3. 暗号に関わる各種制度、規制及びガイドライン

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情報システムの実質的な標準としてSAGAがある。更にBSIがSAGAを具体化する形で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)[76]（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 3-19）。現在は2011年に発行されたSAGA5.1[77]が最新である。
  なお、2014年度調査以降に変更及び更新は見当たらない。

表 3-19 SAGA指定暗号

区分	義務	推奨
非対称暗号	—	RSA
対象暗号	AES	—
電子署名	—	RSA、DSA
ハッシュ関数	SHA-2	—

- 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）[78]
  2020年3月24日に発行された最新版では、主に、2018年以降に新しい暗号システムの導入を計画する開発者を対象としている。 2014年7月以降、乱数生成や素数生成に関する項の改訂など4度の改訂が行われている。強制力を持たないことを冒頭で宣言している。

---

[76] Standards and Architecture for eGovernment Applications http://www.egov-conference.org/glossary/standards-and-architecture-for-egovernment-applications

[77] 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

[78] Kryptographische Verfahren: Empfehlungen und Schlüssellängen https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf.html

主な推奨暗号は表 3-20 の通りである。

表 3-20　推奨暗号方式

区分	推奨暗号
対称暗号	AES-128, AES-192, AES-256
非対称暗号	ECIES（250 ビット）,DLIES（2000 ビット）, RSA（2000 ビット） ※2022 年以降も使用される場合は、推奨されるすべての非対称暗号方式においてセキュリティレベルと統一するため、3000 ビットの RSA/DLIES 鍵の使用が推奨される。2000 ビットは、DLIES 鍵では 2022 年まで、RSA 鍵では 2023 年末まで、現在の技術指針に適合するとみなされる。
ハッシュ関数	SHA-256, SHA-512/256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512
メッセージ認証	CMAC, HMAC, GMAC
電子署名	RSA, DSA, DSA（ECDSA, ECKDSA, ECGDSA）, Merkle signatures

- Verwendung von Transport Layer Security（TLS）（BSI TR-02102-2）（TLS の使用方法）[79]/ 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）[80]
  本技術指針におけるすべての暗号技術のセキュリティレベルは、TR-02102-1 の 1.1 項に準じる。

- Architekturrichtlinie für die IT des Bundes（Architecture Guideline for Federal IT）[7]
  SAGA の仕様が本ガイドラインに統合され、必要に応じて更新されている。
  現在公開されている最新版は 2020 年 7 月 31 日付けの Version 2020 である。2020 年版の 4.7 章の”Architekturvorgaben zur Informationssicherheit”において、保護が必要とされる IT 手続きに、承認されている最新の技術に基づく暗号を利用することが規定されている。暗号の利用については、BSI の技術ガイドライン（BSI TR-02102-1）及び BSI TR-03116-X を考慮するよう要求している。トランスポートレイヤーセキュリティ（TLS）については BSI の MSO.APP.TLS、連邦国防省（Bundesministerium der Verteidigung /BMVg）の分野においては NATO の規定、特定の IT 手続きにおけるアーキテクチャ要件では、DSGVO（EU 一般データ保護規則）、VSA（VPS サービスアダプタ）による暗号化が要求されている。

[79] Verwendung von Transport Layer Security (TLS)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.html

[80] 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

- （再掲）Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 1: Telematikinfrastruktur[20]/Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2: eID-Karten und hoheitliche Dokumente[21]/Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3: Intelligente Messsysteme[22]/Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4: Kommunikationsverfahren in Anwendungen[23]/Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API[24]
  連邦政府のプロジェクトの暗号仕様について規定する技術ガイドラインである。
  - パート 1：テレマティクスインフラストラクチャ
    電子健康保険証、医療従事者カード、テレマティクスインフラストラクチャの技術コンポーネントへの暗号の使用に関するセキュリティ要件と仕様を定義する。
  - パート 2：身元確認文書
    電子パスポート、eID カード、電子滞在許可証、到着証明などの身元確認文書への暗号の使用に関するセキュリティ要件を定義する。
  - パート 3：スマートメータリングシステム
    スマートメータリングシステムへの暗号の使用に関するセキュリティ要件を定義する。
  - パート 4：アプリケーションにおける通信手段
    連邦政府のアプリケーションにおける通信手段の使用に関するセキュリティ要件を定義している。
  - パート 5：セキュアエレメント API のアプリケーション
    セキュアエレメント API のアプリケーションでの暗号の使用に関するセキュリティ要件を定義している。

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）[81]

[81] 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

電子署名に関するアルゴリズムとして推奨するハッシュ関数、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。ハッシュ関数として推奨されているものは表 3-21 の通りである。

表 3-21　推奨ハッシュ関数

2015 年まで推奨	2020 年まで推奨
SHA-224 (SHA-1, RIPEMD-160)	SHA-256 SHA-384 SHA-512 SHA-512/256

3.4.3.2.　セキュリティ製品認証制度・セキュリティサービス認証制度

ドイツは、国際承認アレンジメント（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[82]。

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。

- Produktzertifizierung: Programm IT-Sicherheitszertifizierung Common Critieria（CC）

  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。

  2014 年 7 月以降、7 度の改訂が行われており、version 3.5 が最新版となっている。

  2015 年 7 月の改訂により、BSI 7138 の更新版として文書の再構築が行われ、現在の文書名に変更になった。その他の改訂箇所としては、SigG の参照の削除、暗号関連の更新、プロテクションプロファイルの認証に関する更新、費用の更新などが行われている。

認証製品及びプロテクションプロファイルは、BSI のサイト[83,84]上で公開されている。2021 年 2 月時点で有効な認証製品数は、スマートカード 55 件を含む 182 件、認証プロテクションプロファイル数は 66 件である。

---

[82] 前回調査においてドイツの研究機関へのヒアリングでも確認済み。

[83] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Zertifizierte-Produkte-nach-CC/zertifizierte-produkte-nach-cc_node.html

[84] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Schutzprofile-Protection-Profiles-PP/SchutzprofileProtectionProfiles_Aktuell/schutzprofile_pps_aktuell_node.html

なお、調査時点（2021 年 2 月）の CC Portal に掲載されている CCRA 向けの有効な CC 認証取得は、240 製品である。以下に認証取得と EAL を示す。

表 3-22 EAL ごとの Common Criteria 認証取得数（ドイツ）[85]

B※	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6+	EAL7	N※	Total
2	2	0	9	6	5	14	7	88	1	51	50	0	5	240

※B（Basic）: ITSEC（Information Technology Security Evaluation Criteria）における E3（EAL4 相当）の認証である。

※N（None）: EAL の表記がない認証である。

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 BMWi が管轄している。

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。

- （再掲）Architekturrichtlinie für die IT des Bundes（Architecture Guideline for Federal IT)[7]

  連邦政府の IT コンソリデーションとって、包括的な IT アーキテクチャ管理が必要不可欠である。このガイドラインは、IT コンソリデーションを促進し、矛盾した開発を避け、各省庁の活動を積極的に支援することを目的として策定されたものである。2017 年に初めて策定され、以降、各省庁の関与により毎年更新されている。

  SAGA の仕様が本ガイドラインに統合され、必要に応じて更新されている。

  現在公開されている最新版は 2020 年 7 月 31 日付けの Version 2020 である。2020 年版の 4.7 章の”Architekturvorgaben zur Informationssicherheit”において、保護が必要とされる IT 手続きに、承認されている最新の技術に基づく暗号を利用することが規定されている。暗号の利用については、BSI の技術ガイドライン（BSI TR-02102-1）及び BSI TR-03116-X を考慮するよう要求している。トランスポートレイヤーセキュリティ（TLS）については BSI の MSO.APP.TLS、連邦国防省（Bundesministerium der Verteidigung /BMVg）の分野においては NATO の規定、特定の IT 手続きにおけるアーキテクチャ要件では、DSGVO（EU 一般データ保護規則）、VSA（VPS サービスアダプタ）による暗号化が要求されている。

[85] Certified Products List - Statistics : New CC Portal https://www.commoncriteriaportal.org/products/stats/

- Standards and Architectures for eGovernment Applications (SAGA)[86]（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）
  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 3.3.3.1 節に記載。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- 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[87]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の情報は確認できなかった。

3.4.3.4. 暗号の輸出入規制

ドイツにおいては暗号の輸出入規制は、EU 輸出規制およびワッセナー・アレンジメント（Wassenaar Arragement）に基づいている。規制対象となる暗号製品等は、ワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）」のなかのデュアルユース製品・技術に関するリストのカテゴリ 5 パート 2（Category 5 – Part 2 “Information Security”）がベースになっている。（参考：3.1.3.4 節のワッセナー・アレンジメント）

なお、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）
- KWKG 2020

3.4.3.5. プロトコル等での暗号方式

今回調査した文献の中では本節に該当する文献は発見できなかった。

3.4.3.6. 暗号利用に関する規制（利用ライセンス・暗号盗聴法など）

今回調査した文献の中では本節に該当する文献は発見できなかった。

---

[86] Standards and Architecture for eGovernment Applications http://www.egov-conference.org/glossary/standards-and-architecture-for-egovernment-applications

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

3.4.3.7. クラウドサービス

今回調査した文献の中では本節に該当する文献は発見できなかった。

3.4.3.8. 暗号資産

- Kreditwesengesetz – KWG[26]
  2020 年の改正において、暗号資産（crypto asset）が金融商品のカテゴリの 1 つとして定義され、金融サービスの 1 つとして暗号資産ビジネスが組み込まれた。本法の施行される 2020 年 1 月 1 日より、暗号資産ビジネスを提供する企業は、BaFin からの認可取得が必要となった。

- Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz und des Bundesministeriums der Finanzen, Entwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren[27]
  ドイツの証券法と関連監督法の近代化を目指し、ブロックチェーン技術を基盤とした証券のデジタル化を確立するフレームワークを整備するための電子証券法草案である。BMF（財務省／Bundesministerium der Finanzen）および BMJV（司法消費者保護省／Bundesministerium der Justiz und für Verbraucherschutz）により提案された本草案は、2020 年 12 月 16 日に連邦政府により承認されている。

3.4.3.9. 電子署名法

- （再掲）Vertrauensdienstegesetz（VDG）（Trust Service Act）
  欧州における eIDAS 規則（Regulation No. 910/2014）の施行により、2017 年 7 月 18 日に、Act on Digital Signature (SigG)／Digital Signature Ordinance (SigV)に代わる法として施行された。本法の施行により、SigG/SigV は失効された。

3.4.3.10. 国民 ID 番号制度（eID）

今回調査した文献の中では本節に該当する文献は発見できなかった。

3.4.4. その他

3.4.4.1. 量子コンピュータの進展に伴う対応策

- Migration zu Post-Quanten-Kryptografie[28]
  いつ、どのような場合に量子コンピュータに耐性のある手段に移行するかを、早い段階で検討する必要があり、本文書では、長期的には標準となるであろう耐量子計算機暗号への移行を開始する方法について示している。

3.4.4.2. その他特記すべき項目

- De-Mail Law

  De-Mail Lawは、De-Mailを介したメッセージの安全な電子通信のための最低限の要件を規定するもので、De-Mailサービスを提供するすべての事業者に適用される。De-Mail事業者の承認は、BSIが行っている。

  2019年の改訂により、De-Mailアカウントの作成、身元確認サービス、ディレクトリサービス、情報の明確化と情報提供の義務、アカウントのブロック・終了、データ保護、情報に関する権利、サービス提供者の認定の要件、De-Mail標準化委員会、罰則に関する条項が改訂され、文書化の条項が廃止された。

  De-Mailは、検証可能で信頼できる電子通信を可能する手段で、法的に安全な通信を提供している。De-Mailは、通信時は常に暗号化されており、また、暗号化された状態で保存されるため、読むこと、変更することができない。オプションでEnd-to-Endの暗号化も可能である。

- Das Standard Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele Version 2.0[29]

  GDPRの運用ルールである標準データ保護モデル（SDM）の第2版である。2019年11月5日から7日に開催された第98回ドイツ連邦と州のデータ保護監督機関で採択された。第2版では前版のSDMが抜本的に改訂され、GDPRの全ての要件をカバーするようになった。

3.4.5. ドイツの参照文献

[1] Cyber Security Strategy for Germany 2016
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany

[2] Grobkonzept zur IT-Konsolidierung Bund
http://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/it_konsolidierung_bund_grobkonzept.pdf?__blob=publicationFile

[3] IT-Strategie der Bundesverwaltung 2017-2021
https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/it_strategie_der_bundesverwaltung_download.pdf?__blob=publicationFile#:~:text=Die%20vorliegende%20IT%2DStrategie%20definiert,IT%2DBeauftragten%20der%20Ressorts%20verabschiedet.

[4] Eckpunkte der deutschen Kryptopolitik 1999 (Principles of German Crypto Policy)
https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2002-06-06/anlage-15.pdf?__blob=publicationFile&v=2

[5] Vertrauensdienstegesetz (VDG)
https://www.gesetze-im-internet.de/vdg/BJNR274510017.html

[6] Act on the Federal Office for Information Security (BSI Act - BSIG)
https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[7] Architekturrichtlinie für die IT des Bundes(Architecture Guideline for Federal IT)
https://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/architekturrichtlinie_it_bund_2020.pdf?__blob=publicationFile

[8] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1612123920750

[9] 外国貿易法 (AWG)
https://www.gesetze-im-internet.de/awg_2013/AWG.pdf

[10]外国貿易法施行令 (AWV)
https://www.gesetze-im-internet.de/englisch_awv/

[11]CHP Act 2016 (KWKG 2016)
https://www.bmwi.de/Redaktion/DE/Downloads/Energie/kwkg.pdf?__blob=publicationFile&v=6

[12]Zertifizierungsverfahren nach § 9 AWG, 2 AWV und Art. 9 der Verteidigungsgüterrichtlinie (2009/43/EG)

https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_zertifizierung.html
[13]Standards and Architectures for eGovernment Applications (SAGA) 5.1
https://joinup.ec.europa.eu/collection/eprocurement/discussion/saga-standards-and-architectures-egovernment-applications
[14]Technische Richtlinien Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102-1)
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=10
[15]Verwendung von Transport Layer Security (TLS) (BSI TR-02102-2)
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=10
[16]Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2) (BSI TR-02102-3)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.pdf?__blob=publicationFile&v=7
[17]IT Baseline Protection Catalogues (IT-Grundschutz)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/GSK_15_EL_EN_Draft.pdf?__blob=publicationFile&v=2
[18]Guidelines for Developer Documentation according to Common Criteria Version 3.1
https://www.commoncriteriaportal.org/files/ccfiles/CommonCriteriaDevelopersGuide_1_0.pdf
[19]BSI 7138 Technical information on the IT security certification of products, protection profiles and sites
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/7138_e_pdf.pdf?__blob=publicationFile&v=1
[20]Technische Richtlinie BSI TR-03116-1 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 1: Telematikinfrastruktur
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116.pdf?__blob=publicationFile&v=3
[21]Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2: eID-Karten und hoheitliche Dokumente
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-2.pdf?__blob=publicationFile&v=8
[22]Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3: Intelligente Messsysteme
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-3.pdf?__blob=publicationFile&v=10
[23]Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte

der Bundesregierung Teil 4: Kommunikationsverfahren in Anwendungen
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?__blob=publicationFile&v=7
[24]Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-5.pdf?__blob=publicationFile&v=6
[25]De-Mail Sicherer elektronischer Nachrichtenverkehr - einfach, nachweisbar und vertraulich
https://www.gesetze-im-internet.de/de-mail-g/BJNR066610011.html
[26]Kreditwesengesetz - KWG
[27]https://www.gesetze-im-internet.de/kredwg/Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz und des Bundesministeriums der Finanzen
https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Einfuehrung_elektr_Wertpapiere.pdf?__blob=publicationFile&v=1
[28]Migration zu Post-Quanten-Kryptografie
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=4
[29]Das Standard Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele Version 2.0
https://www.heise.de/downloads/18/2/7/8/9/2/0/7/SDM-Methode.pdf

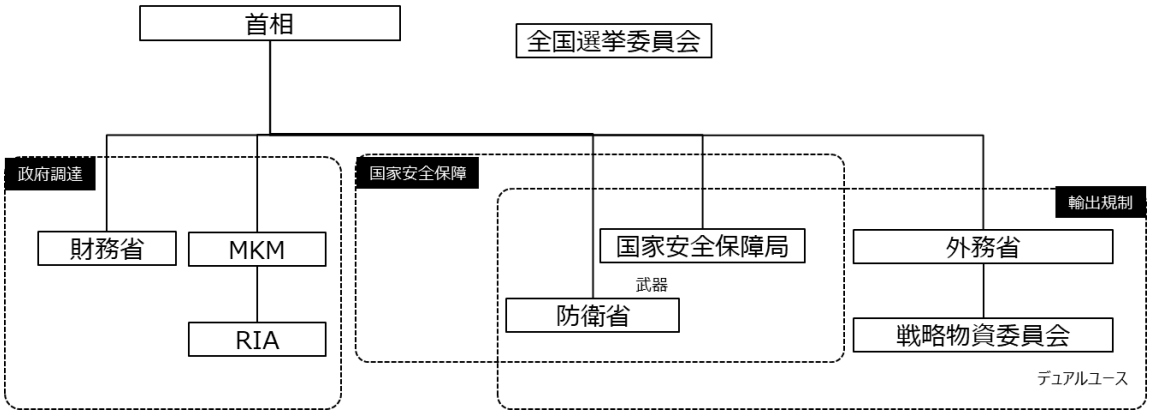
3.5. エストニア

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（Riigi Infosüsteemi Amet、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 3-9 である。

なお、2014 年度調査以降の変化として、財務省、国家安全保障局、全国選挙委員会を追加した。



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 (Riigi Infosüsteemi Amet)
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
財務省：Riigikassa
国家安全保障局：Estonian National Security Authority
全国選挙委員会：Vabariigi Valimiskomisjon

図 3-9 暗号政策に係る組織体制（エストニア）

- 経済通信省（Ministry of Economic Affairs and Communications）
  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。2021 年度の投資予算額は 131 億ユーロ[88]。

- RIA（Estonian Information System Authority：エストニア情報システム局）
  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。2019 年の体制としては 141 名のスタッフである。[89]

- 防衛省（Ministry of Defence（Kaitseministeerium））
  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（Ministry of Foreign Affair（Välisministeerium））
  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（Strateegilise kauba komisjon）
  戦略物資リストの作成を行う。

- 財務省（Estonia Ministry of Finance(Riigikassa)）[90]
  国家予算、資源管理、税金、税関および財務政策の計画と実施、会計、監査、公式統計、公共サービスおよび国家資産および公共調達を行う。

- 国家安全保障局（Estonian National Security Authority（Riigi julgeoleku volitatud esindaja））
  国内の機密情報の保護、及び外国の機密情報の受領と保護を行う。

- 全国選挙委員会（Vabariigi Valimiskomisjon）[91]
  電子選挙等に関する選挙主催者のモニタリング、立候補者の登録、投票と選挙結果の識別、投票結果の取消等を行う。また、電子投票システムのセキュリティまたは信頼性が

[88] エストニアの予算 https://www.rahandusministeerium.ee/et/eesmargidtegevused/riigieelarve-ja-majandus/riigieelarve-ja-majandusulevaated
[89] https://www.ria.ee/sites/default/files/content-editors/RIA/ria_aastaraamat_2020_eng.pdf
[90] https://www.rahandusministeerium.ee/en
[91] https://www.valimised.ee/et/korraldajad/vabariigi-valimiskomisjon/vabariigi-valimiskomisjoni-koosseis-padevus-ja-ulesanded

法律に定めた要件に従っていることを保証できない場合、電子投票を開始しない権利を有する。

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[92]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 3-23、図 3-10のようになる。

表 3-23 エストニアにおける暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	上位政策・戦略	KÜBERTURVALISUSE STRATEEGIA 2019－2022 (サイバーセキュリティ戦略)	防衛省、 関連省庁	後継
2	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	後継
3		Majandus- ja Kommunikatsiooniministeeriumi põhimäärus Vastu võetud 23.10.2002 nr 323 (経済通信省設置法)	経済通信省	更新有
4		Riigi Infosüsteemi Ameti põhimäärus Vastu võetud 25.04.2011 nr 28 (RIA設置法)	RIA	更新有
5	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	更新有
6		Procedure for Protection of State Secrets and Classified Information of Foreign States (国家機密および外国の機密情報の保護手順)	国家安全保障局	－
7	政府調達	Infosüsteemide turvameetmete süsteem, 20.12.2007 nr 252 (情報システムセキュリティ)	RIA	更新有
8		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	更新無
9		Public Procurement Act	財務省	－
10	標準・基準	ISKE (IT Security Standard)	RIA	更新無
11		Elliptilistele kurvidele kohandatud CDOCi spetsifikatsioon (楕円曲線に適合したCDOC仕様)	RIA	－
12		ID-kaardi rakenduse ESTEID spetsifikatsioon (IDカードアプリケーションEstEID仕様)	RIA	－
13	その他	Digital Signatures Act	経済通信省、RIA	更新無
14		Identity Documents Act(身分証明書法)	警察、国境警備局、外務省	－
15		ID-card	RIA	－

[92] CYBERNETICA ASは、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/

16		Development and application of cryptography in the Estonian public and private sectors REPORT 2019 （エストニアの公的および民間部門における暗号技術の開発・応用レポート 2019）	CYBERNETICA AS	―
17		Government Cloud - e-Estonia	RIA	―
18		KRÜPTOVARADE REGULEERIMISE VÄLJATÖÖTAMISKAVATUS （暗号資産規制　開発計画）	財務省	―
19		Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seadus	財務省	―
20		Referendum Act（国民投票法）	国家選挙局、 国家選挙委員会	―

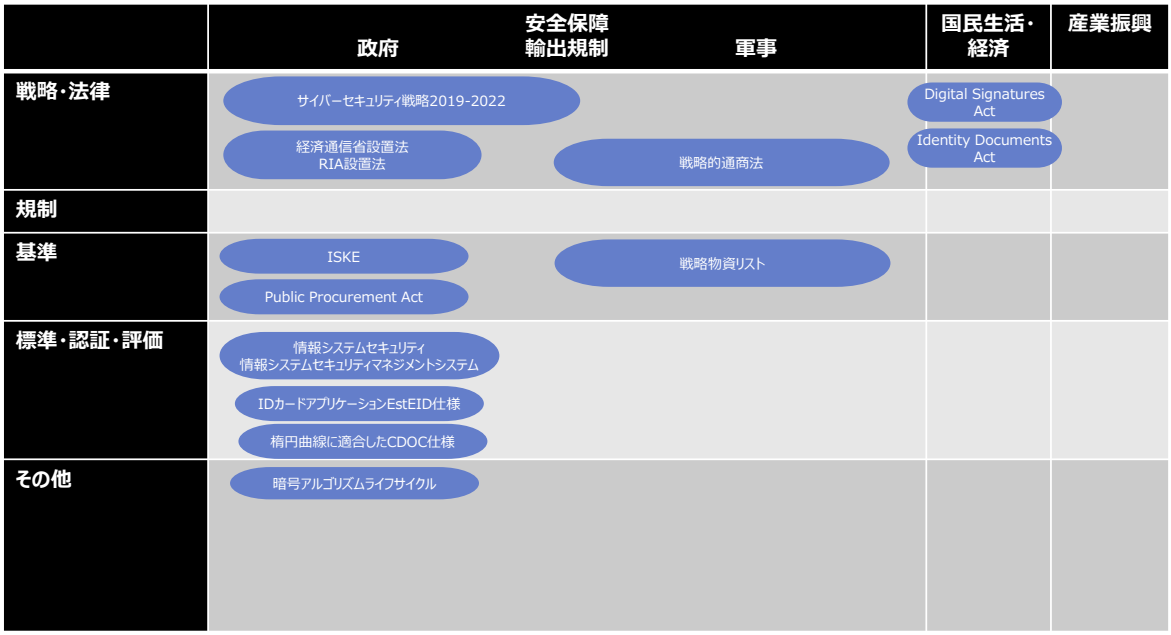


図 3-10　暗号に関連した政策マップ（エストニア）

- KÜBERTURVALISUSE STRATEEGIA 2019－2022（サイバーセキュリティ戦略）[1]
  サイバー脅威に効果的に対処し、公的機関の共同能力、知識豊富で参加している民間セクタ、優れた科学的能力を構築することで、デジタル社会の安全で円滑な機能を確保することである。国家の権限を指定し、サイバーインシデントに対応するための機能する運用ユニットとして Critical Information Infrastructure Protection（CIIP、重要情報インフラストラクチャ保護局）[93]を RIA 内に立ち上げ、国家サイバーセキュリティ戦略を確立する。2019～2022 年版の目的は以下の通り。
  - 現場の総合的な管理とコヒーレントコミュニティの形成
  - サイバーセキュリティ研究開発および研究ベースの起業家精神の支援と推進

[93] https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html

- 戦略的な外部パートナーとの連携の強化
- 持続可能なサイバー機能の国際的な推進
- 官民の需要に応える人材育成

- Krüptograaeku algoritmide kasutusvaldkondade ja elutsükli uuring（暗号アルゴリズムライフサイクル）[2]
  詳細は 3.5.3.1 節にて記載。なお、2014 年度調査以降で変更があることに留意されたい。

- Majandus- ja Kommunikatsiooniministeeriumi põhimäärus Vastu võetud 23.10.2002 nr 323（経済通信省設置法）[3]
  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。
  2014 年度調査以降の変更点としては、省内の構成変更及び部門に関する記述の一本化である。2014 年度調査時点では、省の構成（部門）として、運営部門、統合部門、サポート部門、実行部門、安全調査センターに分け規定していたが、新規に省安全調査センター部を設置し、その下部に安全調査センターを設置し、統合部門、サポート部門、実行部門等の記述を廃止し、省の部門と主な任務に記述を一本化した。

- Riigi Infosüsteemi Ameti põhimäärus Vastu võetud 25.04.2011 nr 28（RIA 設置法）[4]
  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。

  なお、2014 年度調査以降の変更点としては、州情報システム全般のセキュリティシステムの管理については、デジタル署名、暗号化ソフトウェア、インターネットにおける認証、電子管理について詳細化された。さらに、サイバーセキュリティの分野では、情報セキュリティ対策の実施に加え、サイバーセキュリティに関するリスクの監視、分析、対策について詳細化した。

(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、ID カード、モバイル ID 等の基盤となっているため、ID カードにおける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）[5]
  詳細は 3.5.3.4 節参照のこと。なお、2014 年度調査以降で変更があることに留意されたい。

- Infosüsteemide turvameetmete süsteem, 20.12.2007 nr 252（情報システムセキュリティ）[7]／ISKE（IT Security Standard)[10]
  詳細は 3.5.3.3 節参照のこと。なお、2014 年度調査以降で変更があることに留意されたい。

- Infoturbe juhtimise süsteem, 15.03.2012 nr 26（情報セキュリティマネジメント体制）[7]
  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。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

3.5.3. 暗号に関わる各種制度、規制及びガイドライン

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）[2]

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。2015 年のレポートでは 2013 年以降に、暗号解析に関する重大なブレークスルーがなかったこと、2017 年のレポートには、鍵長に関する推奨（表 3-24）の記載があるが、レポートの対象期間（2016～2017 年）に暗号解析に関する大きな進歩がなかったこと報告している。

なお、2017 年の主な調査テーマは以下の 3 点である。

- 暗号プリミティブとプロトコルのセキュリティレベル
- ID カードインシデントの説明
- 暗号アプリケーションとしてのブロックチェーンの概要

表 3-24　各暗号アルゴリズムの推奨鍵長

Security level	DSA, DH	RSA	ECC	Block ciphers	SHA-2, SHA-3
128	L = 3072, N = 256	3072	256 ... 383	128	256
192	L = 7680, N = 384	7680	384 ... 511	192	384
256	L = 15360, N = 512	15360	512+	256	512

3.5.3.2.　セキュリティ製品認証制度・セキュリティサービス認証制度

Development and application of cryptography in the Estonian public and private sectors REPORT 2019[16]において公的機関および民間における暗号技術の調査レポートを公表している。このレポートでは、エストニア国内にコモンクライテリア（CC）の認証機関を設立するために必要な要素を言及しているパートがある。そのパートでは、RIA は、より多くの組織的または監督的な作業を行う必要があり、実際の技術的能力においても ITSEF と同程度が要求されるため、エストニアには CC と同様の認証制度はないが、潜在的に Certification Body になる可能性があることが報告されている。また、公共の安全及び防衛の観点からエストニア国内の評価、認証制度は必要であるが、ビジネスの観点からエストニア国内に CC 認証機関を設立することは時期尚早であり、エストニア国内の認証よりも主要輸出市場での認証が恩恵を受けることを記載している。

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。

- IT Baseline Security System ISKE（ISKE 標準）[10]

  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)」を基に策定したものであり、ISO 1335/17799 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[94]。
なお、2014 年度調査以降に変更及び更新は見当たらない。

- Infosüsteemide turvameetmete süsteem, 20.12.2007 nr 252（情報システムセキュリティ体制）[7]
  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。2008 年発効、2009 年改正。
  なお、2014 年度調査以降の変更点として、第一章にデータベースのセキュリティ要件として国際標準 ISO/IEC 27001 に準拠すること、また適合性証明を RIA に提出することが追記された。

- Public Procurement Act[9]
  国家及び行政の公共調達は、財務省が監督する。また、国際標準の優先順位を以下のように定めている。
  (1) エストニアにて国内標準化した欧州規格
  (2) 欧州標準
  (3) 欧州連合加盟国の指定承認機関によって承認された欧州の技術文書
  (4) 欧州連合加盟国によって規定された欧州連合共通の技術仕様
  (5) 国際基準
  (6) 欧州標準化機関によって確立された技術参照システム
  (7) 旧エストニア標準、またはエストニアの承認技術文書またはエストニアの技術仕様

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（the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies）に則っている。規制対象となる暗号製品等は、ワッセ

[94] 前回調査におけるエストニアの研究機関へのヒアリングによる。

ナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）」のなかのデュアルユース製品・技術に関するリストのカテゴリ5パート2(Category 5 – Part 2 “Information Security”）がベースになっている。（参考：3.1.3.4 節のワッセナー・アレンジメント）

その他の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）[95]
  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。また、Procedure for Protection of State Secrets and Classified Information of Foreign States[6]にて国家機密と外国の機密情報の保護手順、国家機密の情報のサブカテゴリの分類とレベル及び条件を規定している。保護対象には、国防軍及び国防連盟の軍事兵器及び軍需品に関する情報に、二次レーダーの識別基準の確立を可能にする暗号装置と暗号鍵は、10年間の機密として分類されている。
  なお、2014 年度調査以降の変更点としては、戦略的商品の適用範囲の変更及び廃止、戦略的な商品やサービスの輸送の禁止の追加である。

- Strateegiliste kaupade nimekiri（戦略物資リスト）[96]
  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。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

3.5.3.5. プロトコル等での暗号方式

3.5.3.10 節で示す X-Road では、X-Road に連携するサーバやクライアント及びの TLS の設定を X-Road: System Parameters User Guide[97]に記載している。以下に概要を示す。

server.ssl.enabled-protocols：TLSv1.2

- server.ssl.ciphers
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

---

[95] Riigi Teataja 「Strateegilise kauba seadus」(2011 年 12 月 7 日)
[96] Riigi Teataja https://www.riigiteataja.ee/akt/128122011054&leiaKehtiv
[97] https://x-tee.ee/docs/live/xroad/ug-syspar_x-road_v6_system_parameters.html

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- client-tls-protocols：TLSv1.2
- Default value for proxy.client-tls-ciphers
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- Default value for proxy.xroad-tls-ciphers
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

3.5.3.6. 暗号利用に関する規制（利用ライセンス・反暗号法・暗号盗聴法など）

今回調査した文献の中では本節に該当する文献は発見できなかった。

3.5.3.7. クラウドサービス

Government Cloud - e-Estonia[17]において、エストニアの公的機関は、安全と品質の要件の遵守を確保するために、国家 IT セキュリティ基準（ISKE）に従って開発された新しい政府クラウドソリューションに、既存のレガシーシステムから移行することを示している。

3.5.3.8. 暗号資産

2019 年に KRÜPTOVARADE REGULEERIMISE VÄLJATÖÖTAMISKAVATUS（暗号資産規制開発計画）[18]を作成し、財務大臣が関係機関である金融監督局、経済通信省、法務省等との調整を行っていたが、2021 年に Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalväärtingute seadus（クラウドファンディングおよびその他の投資手段および仮想通貨に関する法律）[19]のドラフト版を公開し、意見募集を行っている。

なお、このドラフト版には、詳細な暗号アルゴリズムや鍵長に関する記載はない。

3.5.3.9. 電子署名法

- Digital Signatures Act[13]

  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。

  なお、2014 年度調査以降に変更及び更新は見当たらない。

3.5.3.10. 国民 ID 番号制度（eID）

- 国民 ID

  原則、全国民に配布されている ID カード[15]を利用し、政府の各種オンラインサービスや電子サービスへのアクセス、デジタル署名を提供している。また、SIM カードベースの Mobiil-ID に加え、スマートデバイス用の ID アプリであるスマート ID（Smart-ID）を提供している。さらに、これらの利用するためのデジタル署名用の Java ライブラリ（DigiDoc libraries）を公表し、ファイルの暗号化と復号が可能である。さらに、eID 導入ガイドである eID rakendusjuhend（eID アプリケーションガイド）を公表し、エストニアの ID カード、モバイル ID 等の利用方法、及びこれらを活用した情報システムの設計・構築に関する実装シナリオやテクニカルチュートリアルとサンプルコードを提供している。

  調査時点では、国民の 98%が ID カードを所持し、9 億以上のデジタル署名を発行している[98]。

  ID カード関連分野の規制として、Identity Documents Act [14]によってエストニアの主要な政府による身分証明書として ID カードの機能や要件を定めている。また、Electronic Identification and Trust Services for Electronic Transactions Act[99]によって電子識別および電子取引に必要な信頼サービスを定めている[100]。なお、Identification and Trust Services for Electronic Transactions Act は、Regulation (EU) No. 910/2014 及び Directive 1999/93/EC に対応している。

- Elliptilistele kurvidele kohandatud CDOCi spetsifikatsioon（Required modifications to CDOC for elliptic curve support）[11]

  エストニア政府発行の ID カード及びモバイル ID を利用して、利用者が任意のドキュメントファイルに電子署名やタイムスタンプを付与することができる。エストニアでは、これら仕様やテスト環境及び ID カードをするための DigiDoc ライブラリを公開している。ファイルフォーマットである DigiDoc encrypted container (CDOC)は、楕円曲線に対応し、暗号アルゴリズムや鍵長を規定している。具体的には、ECC Transport key encryption は、SP 800-56A Rev.2 を参照、Data Encryption は、SP 800-38D を参照している。

3.5.3.11. X-road による電子政府システム

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

[98] https://e-estonia.com/solutions/e-identity/id-card/
[99] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/527102016001/consolide
[100] https://www.ria.ee/en/state-information-system/eid/applications.html#digital-signing

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[101]。

- 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[102]である（図 3-11）。調査時点では 2691 サービスが X-road で連携しており、52,000 の組織が X-road を利用[103]している。

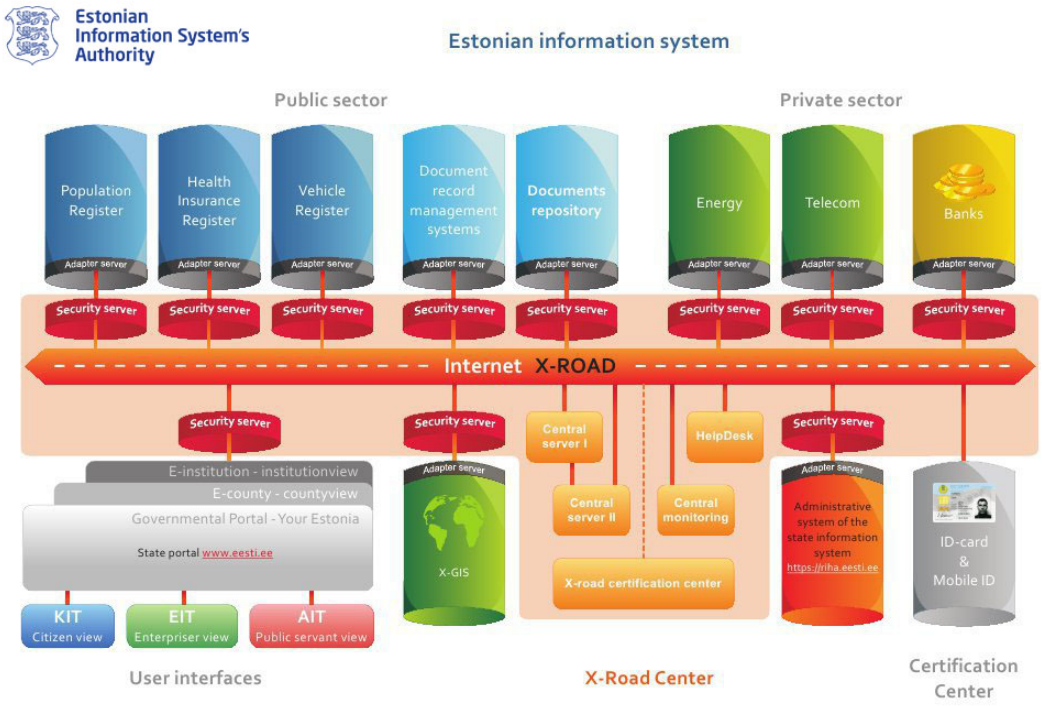


図 3-11　X-road を中心とする電子政府システムの構成図

3.5.4.　その他

3.5.4.1.　量子コンピュータの進展に伴う対応策

Development and application of cryptography in the Estonian public and private sectors REPORT 2019[16]において公的機関および民間における暗号技術の調査レポートを公表している。このレポートに記載されている量子コンピュータの進展に関するパートの概要を以下に示す。

101 前回調査におけるエストニアの研究機関へのヒアリングによる。
102 X-road　http://e-estonia.com/component/x-road/
103 https://e-estonia.com/solutions/interoperability-services/x-road/

- 耐量子計算機暗号の動向調査として、米国、中国、EU 等の投資額、及び米国 NIST の標準化活動の状況を報告している。
- 量子鍵配送の動向として、実用性には問題があるが、エストニアのような小国では、現在達成されている 400km の距離での量子鍵配送は有意義であることを報告している。
- 政府機関は公的調達によって、イノベーションに対して、より積極的な役割を果たす必要があり、イノベーション調達の候補製品として通信セキュリティソリューション、フェデレーション ID 管理に加え、耐量子 eID があることを報告している。

3.5.4.2. その他の特記すべき項目

- Referendum Act[20]
  電子投票については、電子取引のための電子識別および信託サービス法に従った電子署名（[はい]または[いいえ]）の回答マークの投票を確認することが規定されている。
- Support for development of new products, practices, processes and technologies[104]
  「エストニア農村開発計画 2014-2020」において定められた「新製品、慣行、プロセス及び技術の開発支援」活動において新しい製品、慣行、プロセスおよび技術の開発のためのサポートを使用するための条件と手順を定め、申請には電子署名が必要である。

[104] https://www.riigiteataja.ee/en/eli/ee/MRA/reg/512062018001/consolide

3.5.5. エストニアの参照文献

[1] KÜBERTURVALISUSE STRATEEGIA 2019－2022
https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf

[2] Krüptograaeku algoritmide kasutusvaldkondade ja elutsükli uuring
https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kruptograafiliste_algoritmide_elutsukli_uuring_ii.pdf

[3] Majandus- ja Kommunikatsiooniministeeriumi põhimäärus
https://www.riigiteataja.ee/akt/129122011157?leiaKehtiv

[4] Riigi Infosüsteemi Ameti põhimäärus
https://www.riigiteataja.ee/akt/125032020010

[5] Strateegilise kauba seadus
https://www.riigiteataja.ee/akt/StrKS

[6] Procedure for Protection of State Secrets and Classified Information of Foreign States
https://www.riigiteataja.ee/en/eli/ee/VV/reg/512092017002/consolide

[7] Infosüsteemide turvameetmete süsteem
https://www.riigiteataja.ee/akt/13125331?leiaKehtiv

[8] Infoturbe juhtimise süsteem
https://www.riigiteataja.ee/akt/119032012004

[9] Public Procurement Act
https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/513072020002/consolide

[10]ISKE (IT Security Standard)
https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html

[11]Elliptilistele kurvidele kohandatud CDOCi spetsifikatsioon
https://www.ria.ee/sites/default/files/content-editors/EID/cdoc.pdf

[12]ID-kaardi rakenduse ESTEID spetsifikatsioon
https://www.ria.ee/sites/default/files/content-editors/EID/ria-esteid-chip-app-v358_fix_form.pdf

[13]Digital Signatures Act
https://www.riigiteataja.ee/en/eli/530102013080/consolide

[14]Identity Documents Act
https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/504022020003/consolide

[15]ID-card
https://www.id.ee/en/rubriik/id-card-for-developer/

[16]Development and application of cryptography in the Estonian public and private sectors REPORT 2019
https://cyber.ee/research/reports/A-116-1-Development-and-application-of-

cryptography-in-the-Estonian-public-and-private-sectors.pdf
[17]Government Cloud - e-Estonia
https://e-estonia.com/solutions/e-governance/government-cloud/
[18]KRÜPTOVARADE REGULEERIMISE VÄLJATÖÖTAMISKAVATUS
https://adr.rik.ee/ram/dokument/6795482
[19]Ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seadus
http://eelnoud.valitsus.ee/main/mount/docList/a41d0022-7752-4009-9a08-1b97fc44be64#3toLfa8t
[20]Referendum Act
https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/513012020004/consolide

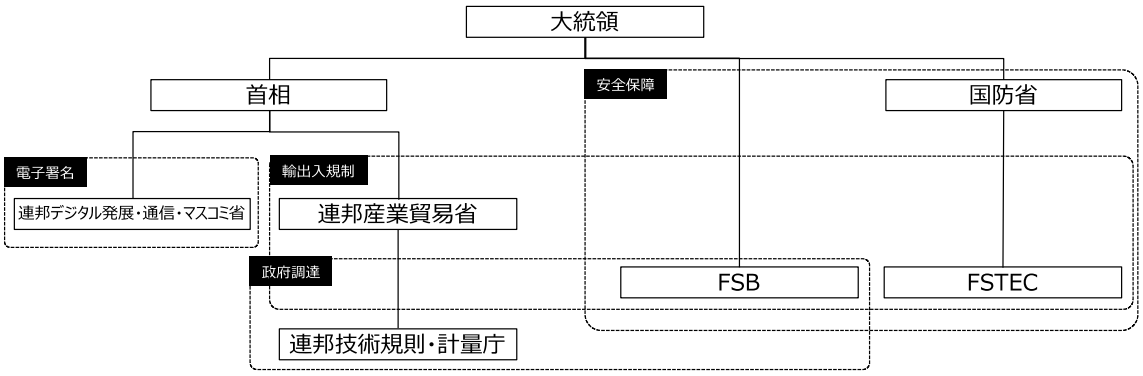
3.6. ロシア

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（Federal Security Service of the Russian Federation、連邦保安庁）であることから判断することができる。伝統的に厳格な暗号政策を実施しており、暗号の開発、製造、流通、利用、輸出入等について、法律あるいは大統領令による規制を行っている。

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

ロシアの暗号政策には、大統領直属のFSB及び国防省の系統と、首相が所管する連邦産業貿易省、連邦デジタル発展・通信・マスコミ省などの行政府の系統があり、主に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連邦産業貿易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 3-12 である。



FSB: Federal Security Service of the Russian Federation（連邦保安庁（旧 KGB））

FSTEC: Federal Service for Technical and Export Control（連邦技術・輸出管理局）

連邦デジタル発展・通信・マスコミ省（旧 通信・マスコミ省）

図 3-12 ロシアにおける暗号政策に係る組織体制

暗号及びセキュリティ政策に関する組織の中で主要なものについて、その役割を以下に示す。

- FSB（Federal Security Service of the Russian Federation、連邦保安庁）[105]
  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。旧ソビエト連邦時代はKGBと呼称されていた組織である。
  主な権限は以下の通りである。
  - 暗号サービスの提供、情報セキュリティツールの開発・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）
  - 情報セキュリティツールの認証
  - 暗号製品の輸出入許可(大量に使用されるもの、一時的なもの)

- 連邦技術規制・計測庁（Federal Technical Regulation and Metrology Agency (Nonstandard)）[106]
  GOST と呼ばれる技術標準を発行するとともに認証制度を主管している。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。暗号に関する標準について、3.6.3.1節に記載。

- FSTEC（Federal Service for Technical and Export Control、連邦技術・輸出管理局）[107]
  国防省配下に設置された組織であり、安全保障の観点から技術・サービスの輸出管理を行う。また、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。

- 連邦産業貿易省（Ministry of Industry and Trade of the Russian Federation）
  暗号製品に関して、輸出入管理を担当する。

- 連邦デジタル開発・通信・マスコミ省（Ministry of Digital Development, Communications and Mass Media of the Russian Federation）[108]
  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、連邦技術規制・計量庁が所管しており、互いに協力関係にあると考えられる。電子署名制度の所轄官庁である。
  2014年度調査の後、2018年5月に連邦通信・マスコミ省から改名した。

[105] http://fsb.ru/
[106] https://www.rst.gov.ru/
[107] https://fstec.ru/
[108] https://digital.gov.ru/

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

ロシアは暗号規制を厳格に行なっており、以下のような政策がとられている。

- 暗号に関する開発、製造、流通、利用に関するライセンス取得を義務付けている。
- 輸出入管理として、ロシアが加盟するユーラシア経済連合(Eurasian Economic Union、EEU、EAEU)[109]で統一の輸出入管理制度と、ワッセナー・アレンジメント・安全保障政策に基づく輸出管理を実施し、規制対象に暗号を含む。
- 暗号に関する認証制度として、国家機密等を扱う製品・サービスの強制認証、国家機密を扱う情報セキュリティツールの強制認証制度がある。
- インターネットを介した暗号化メッセージの送受信及び転送については、復号のための情報の提出を義務付けている。

ロシアにおける主な法制度を分類整理すると表 3-25 と図 3-13 のようになる。

表 3-25 ロシアにおける暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	上位政策・戦略	情報、情報技術、情報保護について (2006 年 7 月 27 日付連邦法 第 149-FZ 号)[1]	FSB	更新有
2	暗号政策・設置法	連邦保安庁について (1995 年 4 月 3 日付連邦法 第 40-FZ 号)[7]	FSB	更新有
3		特定の種類の活動のライセンスについて (2011 年 5 月 4 日付連邦法 第 99-FZ 号)[5]	FSB	更新有
4		暗号もしくは暗号を使用して保護された情報システムおよび通信システムの開発・製造・流通、暗号もしくは暗号を使用して保護された情報システムおよび通信システムの情報暗号化および保守の仕事を行うもしくはサービスの提供のためのライセンスに関する規則の承認について(法人または個人事業主の自己ニーズのための暗号もしくは暗号を使用して保護された情報システムおよび通信システムの保守の実施は除く) (2012 年 4 月 16 日付連邦政府決議 第 313 号))[6]	FSB	―
5		国家機密について (1993 年 7 月 21 日付連法 第 5485-I 号)[3]	FSB	―
6		国家機密を構成する情報の使用に関する企業、機関及び組織の活動、情報保護施設の設置、国家機密保護のための措置の実施及び(又は)サービスの提供の許可について (1995 年 4 月 15 日付連邦政府決議 第 333 号)[4]	FSB	―
7		連邦行政機関の構造に関する問題 (2004 年 5 月 20 日付大統領令 第 649 号)[8]	連邦技術規制・計測庁	更新有
8		連邦技術規制および計測庁について (2004 年 6 月 17 日付連邦政府決議 第 294 号)[9]	連邦技術規制・計測庁	更新有
9		連邦技術・輸出管理庁について (2004 年 8 月 16 日付大統領令 第 1085 号)[10]	FSTEC	―
10	輸出入規制政府調達	外国貿易活動の国家規制の原則について (2003 年 12 月 8 日付連邦法 第 164-FZ 号)[12]	連邦産業貿易省	後継
11		輸出管理について (1999 年 7 月 18 日付連邦法 第 183-FZ 号)[13]、 輸出規制の対象となる商品、情報、作品、サービス、知的活動の結果(権利)を伴う対外経済活動のライセンスに関する規則の承認について (2008 年 9 月 15 日付連邦政府決議 第 691 号)[19]、 輸出管理が実施される武器および軍事機器の開発に使用できるデュアルユース製品および技術のリストの承認について (2011 年 12 月 17 日付大統領令 第 1661 号)[17]	FSTEC	後継、 後継、 ―

[109] http://www.eaeunion.org/

12		商品の貿易における許可制について（2005 年 6 月 9 日付連邦政府決議 第 364 号）[18]	連邦産業貿易省	廃止
13		ユーラシア経済連合条約（2014 年 5 月 29 日）[14]、 個別商品の輸出入の許可の申請手続き並びに発行手続きについて（2014 年 11 月 6 日付ユーラシア経済委員会理事会決定 第 199 号）[15]、 非関税規制の措置について（2015 年 4 月 21 日付ユーラシア経済委員会決定 第 30 号）[16]	連邦産業貿易省、FSB	一、 —
14		技術規制について（2002 年 12 月 27 日付連邦法 第 184-FZ 号）[20]	連邦技術規制規則・計量庁、FSB	後継
15	政府調達標準・基準	暗号手段の開発、製造、販売、運用、および情報の暗号分野におけるサービスの提供の適法性遵守のための措置について（1995 年 4 月 3 日付大統領令 第 334 号）[21]	FSB	更新無
16		国際情報交換への参加について（1996 年 7 月 4 日付連邦法 第 85-FZ 号）[22]	FSB	廃止
17		情報保護の暗号手段の開発、生産、実装、運用に関する規則（規則 PKZ-2005）（2005 年 2 月 9 日付連邦安全保障局令 第 66 号）[24]	FSB、法務省	更新無
18	標準・基準	電子署名について（2011 年 4 月 6 日付連邦法 第 63-FZ 条）[25]	通信・マスコミ省	—
19		連邦国家情報システムについて「情報を提供するインフラストラクチャ内の統合された識別および認証システムと、電子形式で州および地方自治体のサービスを提供するために使用される情報システムの技術的相互作用」（2011 年 11 月 28 日付連邦政府決定決議 第 977 号）[30]	通信・マスコミ省	—

図 3-13　ロシアにおける暗号関連政策マップ

主な法制度の概要は以下の通りである。

- 情報、情報技術、情報保護について（2006 年 7 月 27 日付連邦法 第 149-FZ 号）[1]
  「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。
2014 年度調査後の改正で、インターネット上のサービス提供者に対し、送受信・転送・処理する情報を暗号化する場合、復号するための情報を当局に提供する義務があるという規定が追加された[2]。

- 連邦保安庁について（1995 年 4 月 3 日付連邦法 第 40-FZ 号）[7]
  FSB(連邦保安庁)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。FSB 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、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

  なお、2014 年度調査の後、暗号に関係がある部分の改正はない。

- 特定の種類の活動の許可について（2011 年 5 月 4 日付連邦法 第 99-FZ 号)[5]
  ロシアにおいて、許可の取得が必要とされる活動について定める。暗号に関する活動も含まれている。詳細を 3.6.3.6 節に記載。
  なお、2014 年度調査の後、暗号に関係がある部分の改正はない。

- 暗号もしくは暗号を使用して保護された情報システムおよび通信システムの開発・製造・流通、情報暗号化に関わる仕事の実施及びサービスの提供、暗号もしくは暗号を使用して保護された情報システムおよび通信システムの保守のためのライセンスに関する規則の承認について(法人または個人事業主の自己ニーズのための暗号もしくは暗号を使用して保護された情報システムおよび通信システムの保守の実施は除く）(2012 年 4 月 16 日付連邦政府決議 第 313 号)[6]
  特定の種類の活動のライセンスについて(2011 年 5 月 4 日付連邦法第 99-FZ 号)で定めた活動のうち、暗号に関する活動に対する許可制度を定める。詳細を 3.6.3.6 節に記載。

- 国家機密について（1993 年 7 月 21 日付連邦法 第 5485-I 号）[3]
  国家機密としての情報の区分、その指定と解除、ロシア連邦の安全確保のための国家機密の保護に関る事項を定めている。国家機密を保護する情報セキュリティツールの検査・認証を行う組織の設置を定めている。

- 国家機密を構成する情報の使用に関する企業、機関及び組織の活動、情報保護施設の設置、国家機密保護のための措置の実施及び（又は）サービスの提供の許可について（1995 年 4 月 15 日付連邦政府決議 第 333 号）[4]
  国家機密を構成する情報の使用、情報セキュリティツールの開発、サービスの提供等の活動に関するライセンス制度等を定める。

- 連邦行政機関の構造に関する問題（2004 年 5 月 20 日付大統領令 第 649 号）[8]
  連邦技術規制・計測庁の設置法であり、権限を規定する。暗号についての明示的な規定はない。
  なお、2014 年度調査の後、暗号に関係がある改定はない。

- 連邦技術規制・計測機庁について（2004 年 6 月 17 日付連邦政府決議 第 294 号）[9]
  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。
  なお、2014 年度調査の後、活動分野や権限を変更する改正が行われたが、暗号政策に関わるものは含まれていない。

- 連邦技術・輸出管理庁について（2004 年 8 月 16 日付大統領令 第 1085 号）[10]
  FSTEC の設置法であり、FSTEC を国家機密の保護、重要なインフラのセキュリティ確保、輸出の規制等を行う連邦執行機関と定める。FSTEC の活動の実施のため、広範囲の権限を与えるとともに、その活動について規定している。
  活動の中に、国家機密等を保護する製品やサービスの適合性評価を行う認証機関・試験機関の認定が含まれる。

- 外国貿易活動の国家規制の原則について（2003 年 12 月 8 日付連邦法 第 164-FZ 号）[12]
  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る。なお、2014 年度調査の後、暗号に関係がある改正はない。

- 輸出管理について（1999 年 7 月 18 日付連邦法 第 183-FZ 号）[13]、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（2008 年 9 月 15 日付連邦政府決議 第 691 号）[19]、輸出管理が実施

される武器および軍事機器の開発に使用できるデュアルユース製品および技術のリストの承認について（2011 年 12 月 17 日付大統領令 第 1661 号）[17]
ロシア連邦の利益の確保、国際条約に基づいた大量破壊兵器及び軍事・デュアルユース品の輸出管理、国際テロへの対応等を目的とした輸出規制について定める。規制対象は管理品目・技術リストで管理し、規制対象の製品や技術を輸出する場合は FSTEC の許可を得ること等が定められている。暗号製品の輸出入について、3.6.3.4 節に記載。
なお、2014 年度調査の後、暗号に関係がある改正はない。

- ユーラシア経済連合条約（2014 年 5 月 29 日）[14]、個別商品の輸出入の許可の申請手続き並びに発行手続きについて（2014 年 11 月 6 日付ユーラシア経済連合委員会決定第 199 号）[15]、非関税規制上の措置について（2015 年 4 月 21 日付ユーラシア経済連合委員会決定 第 30 号）[16]
ロシアが加盟するユーラシア経済連合で統一の輸出入管理制度を規定する。条約付属の「第三国に対する非関税措置に関する議定書」（付随文書 7）で制度を定め、「非関税規制の措置について」で規制対象品目リストを定めている。リストは暗号製品・技術を含む。
暗号製品の輸出入について、3.6.3.4 節に記載。

- 技術規制について（2002 年 12 月 27 日付連邦法 第 184-FZ）[20]
ロシアにおける適合性評価について定める。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を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。
なお、2014 年度調査の後、暗号に関係がある改正はない。

- 暗号手段の開発、製造、販売、運用、および情報の暗号分野におけるサービスの提供の適法性遵守のための措置について（1995 年 4 月 3 日付大統領令 第 334 号）[21]
連邦政府機関及び企業において FSB が認可していない暗号手段の利用を禁止している。また、法人、個人による FSB が許可していない暗号手段の開発、製造、販売、運用活動、および、情報の保存、処理、転送を保護する技術的な手段や情報サービスの提供も同様に禁止としている。
なお、2014 年度調査の後、改定は行われていない。

- 情報保護の暗号手段の開発、生産、実装、運用に関する規則（規則 PKZ-2005）（2005 年 2 月 9 日付連邦安全保障局令 第 66 号）[24]
FSB による政令で、情報セキュリティツールの開発、製造、販売、運用等に関する詳細を定めたもの。機密情報を保護する暗号化手段は「技術規制について（2002 年 12 月 27

日付連邦法 第184-FZ号）」で定められた要件を満たさなければならない。
なお、2014年度調査の後、改正は行われていない。

- 電子署名について（2011年4月6日付連邦法 第63-FZ号）[25]
  電子署名を定義し、電子署名された電子文書と署名された紙の文書を同等とする要件、電子署名の鍵の証明書を発行する認証センター及びその認定等を定めている。これについて、3.6.3.9節で述べる。

- 連邦国家情報システムについて「情報を提供するインフラストラクチャ内の統合された識別および認証システムと、電子形式で州および地方自治体のサービスを提供するために使用される情報システムの技術的相互作用」（2011年11月28日付連邦政府決議 第977号）[30]
  政府機関が提供する様々なオンラインサービスに対し、単一のアカウントを提供するための総合識別認証システム（ESIA）について定めている。これについて、3.6.3.10節で説明する。

また、2014年度調査の後に廃止された、もしくは廃止されていたことが判明した法制度の概要は以下の通りである。

- 商品の貿易における許可制について（2005年6月9日付連邦政府決議 第364号）[18]
  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。
  2016年11月に廃止された。

- 国際情報交換への参加について（1996年7月4日付連邦法 第85-FZ号）[22]
  国際的な情報交換における条件を定めたもの。FSBが承認した暗号手段の利用が求められている。
  2006年7月に廃止された。

3.6.3. 暗号に関わる各種制度、規制及びガイドライン

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 34.10-2018：公開鍵暗号（署名）
- GOST R 34.11-2012：ハッシュ関数（メッセージダイジェスト）
- GOST 34.12-2018：ブロック暗号
- GOST R 34.13-2015：ブロック暗号の動作モード

3.6.3.2. セキュリティ製品認証制度・セキュリティサービス認証制度

セキュリティ製品に関する認証制度は、国家機密情報保護製品の認証制度と、情報セキュリティツールの認証制度の二つが実施されている。

- 国家機密情報保護製品の認証制度

  国家機密もしくは法律により保護される情報に関する製品・サービスの検査・認証制度で、FSB の国家機密の許可・認証・保護センター[110]、FSTEC がそれぞれ実施している[33][34]。根拠法は「国防命令の下で供給される防衛製品、国家機密を構成する情報の保護に使用される製品、またはロシア連邦の法律に従って保護されるその他の制限情報に関連する製品、国家機密を構成する情報、および政府の特定の法律の改正に関するコンプライアンスの評価のための業務を行う試験所と認証機関の認定について（2014 年 11 月 3 日付連邦政府決議 第 1149 号）」[31]である。

  なお、FSTEC による実施については詳しい情報を見つけることができなかった。

- 情報セキュリティツールの認証制度

  国家機密の保護に使用可能な情報セキュリティツールの検査・認証制度[111]で、FSTEC が実施している。根拠法は「情報セキュリティツールの認証に関する規則の承認について（1995 年 6 月 26 日の連邦政府決議 第 608 号）」[32]である。

  FSTEC はセキュリティプロファイルや関連する資料を公開する[35][112]。プロファイルは国家基準 GOST R ISO/IEC 15408 に従い作成されている。なお、この情報セキュリティツールの開発には、国家機密を構成する情報を含む情報保護手段の作成活動の許可を FSB より取得する必要がある[3][4]。

一方、国家機密を含まない情報の保護のための暗号手段については、開発を行う際に FSB の許可を得る必要があり[1]、開発物がセキュリティ要件を満たすことを FSB が確認すると

---

[110] http://clsz.fsb.ru/
認定試験機関の一覧：http://clsz.fsb.ru/accred.htm
認証製品の一覧：http://clsz.fsb.ru/certification.htm

[111] 専用のウェブサイトは見つけることができなかった。
認証機関・認定試験機関の一覧：https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/588-perechen-ispytatelnykh-laboratorij-n-ross-ru-0001-01bi00
認証製品の一覧：https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

[112] https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty

定められている[24]。また、利用する暗号アルゴリズムは国家標準として承認されたものが推奨されている。

これらの試験・認証制度について、所管、認証機関、評価機関、認証件数を表 3-26 にまとめた。

表 3-26　ロシアの認証制度と関連する機関（2021 年 2 月）

	国家機密もしくは法律により保護される情報に関する製品・サービスの検査・認証制度		情報セキュリティツールの検査・認証制度
所管	FSB	FSTEC	FSTEC
認証機関	FSB	FSTEC	合資会社「BITK」 合資会社「NPO」エシェロン 非公開株式会社 NPP「ビット」 合資会社「PC ラボ」 有限責任会社「CBI」 合資会社「NIIAS」 連邦国家機関「ロシア連邦技術輸出管理局科学技術情報研究所」 合資会社「アトムザシテイン情報センター」
評価機関	・連邦国庫軍 高等教育機関 A.F.モジャイスキー軍事宇宙アカデミー ロシア国防省 ・国際情報電子センター（インターコンピューター） ・連邦州の単一企業「ロストフ・オン・ドン科学研究所無線通信」 ・地域間公的機関 基礎工学研究所 ・公共団体 「SYNCLITE」 ・高等教育の連邦国庫軍事教育機関 「ロシア連邦の連邦保安局のアカデミー」 等、全 59 箇所	不明	・ロシア連邦技術規制・計測局(FSTEK)の情報技術・ラジオエレクトロニクス国家研究所 等、全 23 箇所
認証件数	2020 年 163 件 2019 年 136 件 2018 年 233 件	不明	2020 年 152 件 2019 年 161 件 2018 年 184 件

3.6.3.3.　政府の調達要件

政府調達について包括的に定める法令は制定されていないが、「技術規制について（2002 年 12 月 27 日付連邦法 No.184-FZ）」に基づいた技術標準（GOST 等）への適合が求められる。また、政府調達において認証取得済みの暗号製品・サービスの利用が義務付けられている（3.6.3.2 節参照）。

この他に、国や地方自治体が使用する国家機密を含まない情報を扱うシステムについて、組織や状況に応じた個別のセキュリティ要件を定め実施すことが定められており[36]、そ

の中で、認証取得済みの情報セキュリティツールの使用を定めている。

3.6.3.4. 暗号の輸出入規制

ロシアにおいて暗号製品の輸出入を規制する法令は、ユーラシア経済連合の条約の下で定められた規制と法律「輸出管理について」の二つある。また、輸出入を行うにあたり、暗号手段の開発、製造、配布のための許可が求められる場合がある点にも注意が必要である。

ロシアはユーラシア経済連合に加盟しており、ユーラシア経済連合の条約[14]に付属する「第三国に対する非関税措置に関する議定書」（付随文書 7）に基づき、加盟国間統一の輸出入規制制度を実施している。暗号の輸出入に関する規制は、この議定書に基づき制定された「非関税規制上の措置について（2015 年 4 月 21 日付ユーラシア経済連合委員会決定第 30 号）」[16]の付録 9「暗号手段のユーラシア経済連合の税関地域への輸入およびユーラシア経済連合の税関地域からの輸出に関する規制」にある。この中で、通知、決定、許可、個人による輸出入の四つの制度を定めている。

- 通知

  「許可」を取得せず、主に大量に使用される暗号製品をユーラシア経済連合へ輸出入するための制度であり、ロシアでは FSB が実施する。対象となる暗号製品の分類は、「非関税規制上の措置について（2015 年 4 月 21 日付ユーラシア経済連合委員会決定 第 30 号）」の付録 9「暗号手段のユーラシア経済連合の税関地域への輸入およびユーラシア経済連合の税関地域からの輸出に関する規制」の付録 4「暗号ツール商品のカテゴリのリスト」にある。リストは以下の 12 項目からなる。

  - 弱い暗号を使用した製品
    - 共通鍵暗号アルゴリズム: 鍵長 56 ビット未満
    - 公開鍵暗号アルゴリズム:
      因数分解ベース: 512 ビット未満
      有限体の乗法群における離散対数ベース: 512 ビット未満
      上記以外の離散対数ベース: 112 ビット未満
  - 認証、電子署名（鍵配布きのを含む）機能を持つ製品
  - OS
  - スマートカード
  - デジタルラジオ・テレビ等の受信機器
  - ユーザが暗号機能を利用できない製品（コピープロテクト、読み取り専用、著作権保護）
  - 銀行・金融取専用の暗号機器（ATM など）

- エンドツーエンド暗号化機能を持たないモバイル無線機器
- 短距離無線機器（Wi-Fi, Bluetooth, NFC 等）
- ネットワーク機器
- 暗号機能がロックされている装置
- 上記以外で、市販され、暗号機能を変更できず、サプライヤのサポートなしでユーザ利用できる設計であり、それを確認できる製造者による技術資料を規制当局に提出できるもの

- 決定

「許可」を取得せず、一時的に暗号製品をユーラシア経済連合へ輸出入するための制度であり、ロシアでは FSB が実施する。個人が利用する製品の輸出入、税関の倉庫等への一時的輸出入、「許可」の取得手続きのためのサンプル製品の輸入のいずれかの場合に利用する。

対象となる暗号製品は、「非関税規制上の措置について（2015 年 4 月 21 日付ユーラシア経済連合委員会決定 第 30 号）」の付録 19「暗号手段とは」で定められている。

規制対象品以下の 17 項目からなる。

- 暗号機能を備えたプリンタ、コピー機、ファクシミリ機、およびそれらの電子モジュール
- 暗号機能を備えた計算機能を持つデータの記録、複製、表示を行う携帯機器
- 暗号機能を備えた携帯型コンピュータ
- 暗号機能を備えたコンピュータとその部品
- 暗号機能を備えたコンピュータのデバイス
- 暗号機能を備えた携帯機の電子モジュール及び部品
- 暗号機能を備えた加入者通信装置
- 暗号機能を備えた基地局
- 暗号機能を備えた通信機器およびその部品
- 暗号ソフトウェア（メディアを問わない）
- 重要なドキュメント（磁気、半導体、フィルム、紙、その他）
- 暗号機能を備えた放送またはテレビ機器とその部品
- 暗号機能を備えた無線ナビ受信機、遠隔操作装置およびその部品
- 暗号機能を備えたインターネットにアクセスするための機器、および通信機能を備えたテレビ受信機、それらの部品
- 暗号機能を備えた IC、または暗号機能を備えたストレージデバイス
- 暗号機能を備えた、個別の機能を備えたその他の電気機械および装置
- 上記の暗号機器のための規制、技術、設計、運用に関する文書（メディアを問わ

ない）

- 許可

  「通知」・「決定」に当てはまらない暗号製品をユーラシア経済連合へ輸出入するための制度であり、ロシアでは連邦産業貿易省が実施する。対象となる暗号製品は、「決定」と同一である。

  暗号製品の輸出入ライセンスの取得の条件に、暗号手段の開発、製造、配布のためのライセンスを取得していることが含まれる（3.6.3.6 節参照）。

- 個人による輸出入

  個人が利用する暗号製品を、「通知」・「決定」・「許可」手続きを行わず輸出入するための制度で、対象となる商品のリストが「非関税規制上の措置について（2015 年 4 月 21 日付ユーラシア経済連合委員会決定 第 30 号）」の付録 9「暗号手段のユーラシア経済連合の税関地域への輸入およびユーラシア経済連合の税関地域からの輸出に関する規制」の付録 5「許可証なしに個人が輸出入を許可されている商品のリスト」で公表されている。リストは以下の 8 項目からなる。

  - 大量使用を目的とした、広く提示され、自由に販売されている、あらゆる媒体で公開されているソフトウェア

    OS、インターネットブラウザ、メーラ、オンライン通信・通話ソフトウェア、アンチウイルスソフトウェア、翻訳ソフトウェア、アーカイバ、音楽・ビデオ再生、処理ソフトウェア、ファイル転送、ゲーム、インターネットバンキング支払いシステム、SNS サービス関連ソフトウェア
  - 電子署名手段（メディアを問わない）
  - コンピュータ等（PC、携帯ゲーム機、スマートフォン、スマートウォッチ等）
    - ソフトウェア無し、もしくは上記 2 項目のソフトウェアがプリインストール済み
    - 暗号機能が補助的でユーザが変更できず、上記 2 項目以外のプリインストールされた公開ソフトウェアを利用する
  - スマートカード（銀行カード、SIM カードなど、暗号機能をユーザが利用できないもの）
  - ラジオ・テレビ放送の受信機、部品
  - 携帯電話機、付属品（暗号化された専用電話やエンドツーエンド暗号化が可能なものを除く）
  - プリンタ、複合機、コピー機及びそれらの部品、および、LAN 用ルータ、無線モデム（接続範囲 400m 未満）で、暗号機能を有するもの

➢ 無線ナビ受信機、リモート制御装置とその部品

一方、輸出管理法に基づく輸出管理が、ロシア連邦の利益の確保、国際条約に基づいた大量破壊兵器及び軍事・デュアルユース品の輸出管理、国際テロへの対応を目的として実施されている。ロシア連邦からの輸出が対象となる。

規制対象品目は、連邦政府が作成し大統領が承認した「輸出管理が実施される武器および軍事機器の作成に使用できるデュアルユース製品および技術のリストの承認について（2011 年 12 月 17 日付大統領令 第 1661 号）」[17]として公表される。

規制対象の製品や技術を輸出する場合は「輸出管理対象である商品、情報、役務、サービス、知的活動の成果に関する対外貿易取引の許認可の規則の承認（2008 年 9 月 15 日付連邦政府決議 第 691 号）」[19]に基づき、FSTEC の許可を得る必要がある。

ロシアはワッセナー・アレンジメント加盟国であり、「武器および軍事機器の作成に使用できるデュアルユース製品および技術のリスト」は、ワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）」のなかのデュアルユース製品・技術に関するリストがベースになっている。（参考：3.1.3.4 節のワッセナー・アレンジメント）

リストは 5 つのセクションから成り、それぞれ、デュアルユース製品・技術のリスト、機密リスト、特別な機密リスト、国家安全保障のために管理される輸出製品・技術リスト、国家安全保障のために管理される輸入製品・技術リストとなる。

デュアルユース製品・技術のリストは 9 のカテゴリに分類され、輸出規制対象となる暗号製品はカテゴリ 5 のパート 2「情報セキュリティ」で定められている。

2021 年 2 月時点の概要は以下のようなものとなっている。

- 認証・デジタル署名以外の暗号化機能を有する機器で、後に示す要件を満たす暗号アルゴリズムを使用するもの
- 暗号解読装置
- 情報伝達時の情報漏洩を抑制するように設計された装置（健康保護目的、EMI 規格準拠目的を除く）
- 暗号を利用した拡散コードを用いたスペクトラム拡散装置
- 暗号を利用した超広帯域無線通信機器
- EAL-6 クラス以上の保護を保証すると評価された情報通信技術に関するセキュリティデバイス
- 有線通信システムにおいて電子的に不正アクセスを検出する機器
- 量子暗号（量子鍵配送）を利用または実行する機器

- 暗号アルゴリズムの要件
  - 共通鍵暗号アルゴリズム: 鍵長 56 ビット以上
  - 公開鍵暗号アルゴリズム:
    - 因数分解ベース: 512 ビット以上
    - 有限体の乗法群における離散対数ベース: 512 ビット以上
    - 上記以外の群上の離散対数ベース: 112 ビット以上

デュアルユース製品・技術のリストは、ワッセナー・アレンジメントで合意された「デュアルユース製品・技術リスト及び軍需品リスト」のなかのデュアルユース製品・技術に関するリストに基づいているが、いつの合意に基づくものか確認することができなかった。また、カテゴリ 5 のパート 2「情報セキュリティ」部分を 2019 年 12 月のワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト」のなかのデュアルユース製品・技術に関するリストのカテゴリ 5 パート 2（Category 5 – Part 2 "Information Security"）（米国の 3.1.3.4 節参照）と比較したところ、米国、韓国と比べ多くの異なる部分を確認した（耐量子計算機暗号アルゴリズムがロシアのリストに含まれない等）。

3.6.3.5. プロトコル等での暗号方式

暗号通信プロトコルの推奨される設定について定める文書やガイドラインについて、公的機関によるものは見つけることができなかった。暗号製品の認証制度が実施されているため、検査要件定義書などで定められている可能性があるが、そのような文書を参照できなかった。

3.6.3.6. 暗号利用に関する規制（利用ライセンス・暗号盗聴法など）

ロシアでは、インターネットでサービスを提供する者がメッセージを送受信・転送・処理する際に暗号化処理を行う場合は、復号に必要な情報を FSB に提供することが義務付けられている。これはテロ対策を目的としたもので、「情報、情報技術、情報保護について（2006 年 7 月 27 日付連邦法 第 149-FZ 号）」[1]の第 10^1 条 4^1 項に規定されている。

また、以下の暗号に関する活動を行う場合、FSB の許可を得る必要がある [113]。

- 暗号もしくは暗号を使用して保護された情報システムおよび通信システムの開発・製造・流通、情報暗号化に関わる仕事の実施及びサービスの提供、暗号もしくは暗号を使用して保護された情報システムおよび通信システムの保守のためのライセンスに関する規則の承認について（法人または個人事業主の自己ニーズのための暗号も

[113] ライセンスに関する一般情報(FSB の国家機密の認可・認証・保護センター): http://clsz.fsb.ru/license.htm

しくは暗号を使用して保護された情報システムおよび通信システムの保守の実施は除く）

すなわち、以下の「規制対象活動 1、2、3」が、規制対象となる活動である。

- 手段
  手段 1: 暗号[114]
- 対象
  - ✧ 対象 1: 手段 1
  - ✧ 対象 2: 手段 1 を使用して保護された情報システムおよび通信システム
- 規制対象活動
  - ✧ 規制対象活動 1: 対象 1、2 の開発・製造・流通
  - ✧ 規制対象活動 2: 情報の暗号化に関わる仕事の実施およびサービスの提供
  - ✧ 規制対象活動 3: 対象 1、2 の保守（ただし法人・個人の自己ニーズのための保守は除く）

これは、ロシアにおける様々な活動に対する許可制度を定める「特定の種類の活動のライセンスについて」[5]の第 12 条 1 項、及び、「暗号もしくは暗号を使用して保護された情報システムおよび通信システムの開発・製造・流通、情報暗号化に関わる仕事の実施及びサービスの提供、暗号もしくは暗号を使用して保護された情報システムおよび通信システムの保守のためのライセンスに関する規則の承認について（法人または個人事業主の自己ニーズのための暗号もしくは暗号を使用して保護された情報システムおよび通信システムの保守の実施は除く）（2012 年 4 月 16 日付連邦政府決議 第 313 号）」[6]で規定されている。

3.6.3.7. クラウドサービス

クラウドサービスを包括的に規制する法令、ガイドラインは見つけることができなかった。個別の法令の中で、クラウドサービスに関連する事項を規制するものがある。

- 情報、情報技術、情報保護について（2006 年 7 月 27 日付連邦法 第 149-FZ 号）
  国及び地方自治体の単一企業や機関が使用する情報システムの技術的手段は、ロシア連邦内に配置しなければならないことを定めている（第 13 条 21）。
- 個人情報について（2006 年 7 月 27 日付連邦法第 152-FZ）
  ロシア、個人情報保護に関するロシアとの条約締結国、個人情報の主体の権利を保障するとロシアに認められた国における個人データの国境を超えた移動を禁止・制限している（第 12 条 1）。

[114] ロシアの法令では「Encryption (Cryptography) method」のロシア語表記が使われているが、日本語ではこれらを区別した簡単な表記方法が見つからないため、本報告書では「暗号」とした。

3.6.3.8. 暗号資産

ロシアでは暗号資産を規制する法律、「デジタル金融資産、デジタル通貨、およびロシア連邦の特定の立法行為の改正について（2020 年 7 月 31 日付ロ連邦法 第 259-FZ）」[23]を 2021 年 1 月に施行した。この法律は、デジタル金融資産の発行システム・交換所の運営者及び、デジタル通貨の流通を規制する。この法律の施行により、デジタル通貨は財産として認められるが、支払い手段としては認められないことが明確になった一方で、暗号資産のマインニング等についての規定は含まれておらず、適法かどうか不透明な面が残されている。

一方、ロシア中央銀行は、デジタル通貨（デジタルルーブル）の発行に向けての活動を行なっている。2020 年 10 月に発行準備の発表とレポートを公表し、コメント募集を行った[115]。2021 年 2 月時点では、それ以降の動きは確認できていない。

3.6.3.9. 電子署名法

電子署名を規定する法令「電子署名について（2011 年 4 月 6 日付連邦法 第 63-FZ 号）」[25]が施行されている。電子署名の基礎概念、種類、署名された紙の文書と同等とみなすための要件を定めるとともに、電子署名を規制する行政機関の権限や電子署名を発行する認定認証センター等について、包括的に規定している。

この電子署名法では電子署名を、暗号技術を用いた物だけでなく、コードやパスワードなどを使用して特定の人物が電子署名を作成したことを確認できるものを含むものとし、暗号技術を使わないもの、暗号技術を用いたもの、暗号技術を用いたもので認定された認証センターが発行したものの 3 つに分類し、それぞれの効力を規定している。

電子署名の規制行政機関は、通信・マスコミ省としている[26]。電子署名の認証センターの認定基準は「認証センターの認定について（2011 年 11 月 23 日付通信省令 第 320 号）」で定められている[29]。

電子署名は、公共サービスの利用、銀行手続き、調達手続きの参加などで利用されている。公共サービスの種類に応じた使用すべき電子署名の種類が定められている[27][28]。

電子証明書は、法人向けの場合は税務局の認証センターが発行し、信用機関は中央銀行の認証センターが、行政機関は債務章の認証センターが、個人は認定認証センターが発行する。

3.6.3.10. 国民 ID 番号制度（eID）

ロシア市民が 14 歳に達すると所持が義務付けられている身分証明書（市民パスポート）を電子化する試みが内務省と関連する組織により進められている[116]。紙に情報が印刷された従来の身分証明書を、IC カードとそれを補う携帯端末のアプリケーションに置き換えるものである。

---

[115] https://cbr.ru/analytics/d_ok/dig_ruble/

[116] https://xn--b1aew.xn--p1ai/news/item/21989777/

総合識別認証システム（ESIA）[30][117]は、様々な行政機関が提供する情報システムに対し単一のアカウントを提供するシステムである。このアカウントは行政が持つ市民情報と関連づけられ(アクセス制御設定可)、オンライン行政サービス向けの電子 ID として利用できる。また、このシステムの利用を金融・商業組織等へ開放する計画もあり、2019 年 11 月の登録者数は 1 億人以上である[118]。

3.6.4. その他

3.6.4.1. 量子暗号・量子計算技術の研究状況

モスクワ州立大学、ITMO 大学、ロステレコム、NTI 量子コミュニケーションコンピテンスセンター等の大学・企業・研究機関が量子暗号・鍵配送技術の研究・開発を進めている。また、国立研究技術大学は 2019 年 10 月に国内初の量子コンピュータのプロトタイプの開発成功を発表するなど、量子暗号、量子計算の実用化に向けての活動は進められているが、国際的に比較すると遅れをとっている。このような背景を元に、2019 年、国営会社ロスアトムは量子コンピューティングの研究開発のロードマップを作成し、政府はそれを承認した。2024 年までの 5 年間で、236 億ルーブルの予算規模となっている。

量子計算機の実用化に備えた耐量子計算機暗号アルゴリズムの開発や、推奨暗号スイートの策定等の具体的な活動に関する資料は見つけることができなかった。

[117] https://www.gosuslugi.ru/esia-help
[118] https://digital.gov.ru/ru/events/39510/

3.6.5. ロシアの参考文献

[1] Об информации, информационных технологиях и о защите информации(Федеральный закон от 27.7.2006 N 149-ФЗ)
（情報、情報技術、情報保護について（2006 年 7 月 27 日付連邦法 第 149-FZ 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264

[2] О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности(6 июля 2016 года №. 374-ФЗ)
（テロ対策および公共の安全の確保のための追加措置の確立に関する連邦法「テロ対策」の改正およびロシア連邦の特定の立法行為について（2016 年 7 月 6 日付連邦法 第 374-FZ 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102404066

[3] О государственной тайне(Закон Российской Федерации от 21.07.1993 № 5485-I)
（国家機密について（1993 年 7 月 21 日付連邦法 第 5485-I 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102025035

[4] О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны(Постановление Правительства Российской Федерации от 15.04.1995 №. 333)
（国家機密を構成する情報の使用に関する企業、機関及び組織の活動、情報保護施設の設置、国家機密保護のための措置の実施及び（又は）サービスの提供の許可について（1995 年 4 月 15 日付連邦政府決議 第 333 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102035139

[5] О лицензировании отдельных видов деятельности(Федеральный закон от 4.5.2011 N99-ФЗ)
（特定の種類の活動の許可について（2011 年 5 月 4 日付連邦法 第 99-FZ 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102147413

[6] Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)(Правительство Российской Федерации Постановление от 16 апреля 2012 г. №. 313)
暗号もしくは暗号を使用して保護された情報システムおよび通信システムの開発・製造・流通、情報暗号化に関わる仕事の実施及びサービスの提供、暗号もしくは暗号を使用して保護された情報システムおよび通信システムの保守のためのライセンスに関する規則の承認について（法人または個人事業主の自己ニーズのための暗号もしくは暗号を使用して保護された情報システムおよび通信システムの保守の実施は除く）
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102155729

[7] О федеральной службе безопасности(Федеральный закон от 3.4.1995 N 40-ФЗ)
（連邦保安庁について（1995 年 4 月 3 日付連邦法 第 40-FZ 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102034880

[8] Вопросы структуры федеральных органов исполнительной власти(Указом Президента Российской Федерации от 20 мая 2004 г. № 649)
（連邦行政機関の構造に関する問題（2004 年 5 月 20 日付大統領令 第 649 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102086848
[9] О Федеральном агентстве по техническому регулированию и метрологии(Постановление Правительства российской федерации от 17 июня 2004 г. N 294)
（連邦技術規制・計測機庁について（2004 年 6 月 17 日付連邦政府決議 第 294 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102087354
[10]О Федеральной службе по техническому и экспортному контролю(Указом Президента Российской Федерации от 16 августа 2004 г. N 1085)
（連邦技術・輸出管理庁について（2004 年 8 月 16 日付大統領令 第 1085 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102088330
[11]О Министерстве промышленности и торговли Российской Федерации(Правительство российской федерации Постановление от 5 июня 2008 г. №. 438)
（ロシア連邦産業貿易省について（2008 年 6 月 5 日付連邦政府決議 第 438 号））
http://ips.pravo.gov.ru/?docbody=&nd=102122397
[12]Об основах государственного регулирования внешнеторговой деятельности(Федеральный закон от 8.12.2003 года № 164-ФЗ)
（外国貿易活動の国家規制の原則について（2003 年 12 月 8 日付連邦法 第 164-FZ 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102084509
[13]Об экспортном контроле(18 июля 1999 года N 183-ФЗ)
（輸出管理について（1999 年 7 月 18 日付連邦法 第 183-FZ 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102061053
[14]Договор о Евразийском экономическом союзе
（ユーラシア経済連合条約（2014 年 5 月 29 日））
https://docs.eaeunion.org/ru-ru/Pages/DisplayDocument.aspx?s=bef9c798-3978-42f3-9ef2-d0fb3d53b75f&w=632c7868-4ee2-4b21-bc64-1995328e6ef3&l=540294ae-c3c9-4511-9bf8-aaf5d6e0d169&EntityID=3610
[15]Об Инструкции об оформлении заявления на выдачу лицензии на экспорт и (или) импорт отдельных видов товаров и об оформлении такой лицензии и Инструкции об

оформлении разрешения на экспорт и (или) импорт отдельных видов товаров(06.11.2014 Решение №199)
（個別商品の輸出入の許可の申請手続き並びに発行手続きについて（2014年11月6日付ユーラシア経済連合委員会決定 第199号））
https://docs.eaeunion.org/docs/ru-ru/0053689/clcd_06112014_199
[16]О мерах нетарифного регулирования(21.04.2015 Решение Коллегии ЕЭК №30)
（非関税規制上の措置について（2015年4月21日付ユーラシア経済連合委員会決定第30号））
https://docs.eaeunion.org/docs/ru-ru/0157584/clcd_22042015_30
[17]Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль(Указом Президента Российской Федерации от 17 декабря 2011 года N 1661)
（輸出管理が実施される武器および軍事機器の開発に使用できるデュアルユース製品および技術のリストの承認について(2011年12月17日付大統領令 第1661号)）
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102153228
[18]О лицензировании в сфере внешней торговли товарами (УТВЕРЖДЕНО постановлением Правительства Российской Федерации от 9 июня 2005 г. N 364)
（商品の貿易における許可制について(2005年6月9日付連邦政府決議 第364号)）
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102098099 の付録1
[19]Об утверждении Положения о лицензировании внешнеэкономических операций с товарами, информацией, работами, услугами, результатами интеллектуальной деятельности (правами на них), в отношении которых установлен экспортный контроль(Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 691)
（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(2008年9月15日付連邦政府決議 第691号)）
http://ips.pravo.gov.ru/?docbody=&nd=102124267
[20]О техническом регулировании(федеральный Закон 27 декабря 2002 года № 184-

ФЗ)
（技術規制について（2002 年 12 月 27 日付連邦法 第 184-FZ））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102079587

[21]О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации(УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ 3 апреля 1995 года N 334)
（暗号手段の開発、製造、販売、運用、および情報の暗号分野におけるサービスの提供の適法性遵守のための措置について（1995 年 4 月 3 日付大統領令 第 334 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102034885

[22]Об участии в международном информационном обмене (4 июля 1996 года N 85-ФЗ)
（国際情報交換への参加について（1996 年 7 月 4 日付連邦法 第 85-FZ 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102042271

[23]О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации(Российская Федерация Федеральный Закон 31 июля 2020 года №. 259-ФЗ)
（デジタル金融資産、デジタル通貨、およびロシア連邦の特定の立法行為の改正について（2020 年 7 月 31 日連邦法 第 259-FZ 号））
http://ips.pravo.gov.ru/?docbody=&prevDoc=102038864

[24]Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)(Приказ Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. N 66)
（情報保護の暗号手段の開発、生産、実装、運用に関する規則（規則 PKZ-2005）（2005 年 2 月 9 日付連邦安全保障局令 第 66 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102097894

[25]Об электронной подписи(6 апреля 2011 года № 63-ФЗ)
（電子署名について（2011 年 4 月 6 日付連邦法 第 63-FZ 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102146610

[26]О федеральном органе исполнительной власти, уполномоченном в сфере

использования электронной подписи(Правительство Российской Федерации Постановление от 28 ноября 2011 г. N 976)
（電子署名の使用を許可された連邦執行機関について（2011 年 11 月 28 日連邦政府決議 第 976 号））
http://ips.pravo.gov.ru/?doc_itself=&nd=102152435
[27]О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг(Правительство Российской Федерации Постановление от 25 июня 2012 г. N 634)
（州および地方自治体のサービスを申請する際に使用が許可されている電子署名の種類について（2012 年 6 月 25 日付連邦政府決議 第 634 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102157582
[28]Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи(Приказ Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. N 795)
（州および地方自治体のサービスの提供における単純な電子署名の使用について（2011 年 12 月 27 日付 FSB 令 第 795 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102155745
[29]Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра(ПРИКАЗ Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. N 796)
（電子署名手段の要件および認証センターの手段の要件の承認について（2011 年 12 月 27 日の連邦安全保障局令 第 796 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102155746
[30]О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем,

используемых для предоставления государственных и муниципальных услуг в электронной форме"(ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПОСТАНОВЛЕНИЕ от 28 ноября 2011 г. No. 977)

（連邦国家情報システムについて「情報を提供するインフラストラクチャ内の統合された識別および認証システムと、電子形式で州および地方自治体のサービスを提供するために使用される情報システムの技術的相互作用」（2011 年 11 月 28 日付連邦政府決議 第 977 号））

http://ips.pravo.gov.ru/?docbody=&nd=102152436

[31]Об аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по оценке (подтверждению) соответствия в отношении оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, а также о внесении изменений в некоторые акты Правительства Российской Федерации в части оценки соответствия указанной продукции (работ, услуг)(ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПОСТАНОВЛЕНИЕ от 3 ноября 2014 г. No. 1149)

（国防命令の下で供給される防衛製品、国家機密を構成する情報の保護に使用される製品、またはロシア連邦の法律に従って保護されるその他の制限情報に関連する製品、国家機密を構成する情報、および政府の特定の法律の改正に関するコンプライアンスの評価のための業務を行う試験所と認証機関の認定について（2014 年 11 月 3 日付連邦政府決議 第 1149 号））

http://pravo.gov.ru/proxy/ips/?docbody=&nd=102361323

[32]Об утверждении Положения о сертификации средств защиты информации(Постановление Правительства Российской Федерации от 26

июня 1995 г. N 608)
（情報セキュリティツールの認証に関する規則の承認について（1995 年 6 月 26 日の連邦政府決議 第 608 号））
http://pravo.gov.ru/proxy/ips/?docbody=&nd=102036208
[33]О реализации пункта 2 постановления Правительства Российской Федерации от 3 ноября 2014 г. N 1149(ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИКАЗ(11 января 2016 г. N 1)
（2014 年 11 月 3 日付連邦政府決議第 1149 号の第 2 項の実施について（2016 年 1 月 11 日付 FSB 令 第 1 号））
http://pravo.gov.ru/proxy/ips/?docbody=&link_id=&nd=102391093
[34]ОБ УТВЕРЖДЕНИИ ПРАВИЛ ВЫПОЛНЕНИЯ ОТДЕЛЬНЫХ РАБОТ ПО АККРЕДИТАЦИИ ОРГАНОВ ПО СЕРТИФИКАЦИИ И ИСПЫТАТЕЛЬНЫХ ЛАБОРАТОРИЙ, ВЫПОЛНЯЮЩИХ РАБОТЫ ПО ОЦЕНКЕ (ПОДТВЕРЖДЕНИЮ) СООТВЕТСТВИЯ В ОТНОШЕНИИ ПРОДУКЦИИ (РАБОТ, УСЛУГ), ИСПОЛЬЗУЕМОЙ В ЦЕЛЯХ ЗАЩИТЫ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ ИЛИ ОТНОСИМЫХ К ОХРАНЯЕМОЙ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ИНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, И ПРОДУКЦИИ (РАБОТ, УСЛУГ), СВЕДЕНИЯ О КОТОРОЙ СОСТАВЛЯЮТ ГОСУДАРСТВЕННУЮ ТАЙНУ, В УСТАНОВЛЕННОЙ ФСТЭК РОССИИ СФЕРЕ ДЕЯТЕЛЬНОСТИ(ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПРИКАЗ от 10 апреля 2015 г. N 33)
（ロシアの法律に従って国家機密を構成する情報やその他の制限付き情報を保護するために使用される製品（工作物、サービス）の適合性評価（確認）を行う認証機関および試験所、およびロシア連邦保安庁が定めた活動分野の製品（工作物、サービス）、国家機密を構成する情報の認証に関する規則の承認について（2015 年 4 月 10 日付 FSTEC 令 第 33 号））
https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/118-prikazy/1015-prikaz-fstek-rossii-ot-10-aprelya-2015-g-n-33
[35]ПОЛОЖЕНИЕ О СИСТЕМЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ(Утверждено приказом ФСТЭК России от 3 апреля 2018 г. N 55)
（情報保護の認証システムに関する規制 （2018 年 4 月 3 日付ロシアの FSTEC 令 第

55 号））
https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/119-polozheniya/1594-polozhenie-utverzhdeno-prikazom-fstek-rossii-ot-3-aprelya-2018-g-n-55
[36]ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ(ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПРИКАЗ 11 февраля 2013 г. N 17)
（国の情報システムに含まれる国の秘密を構成しない情報の保護について（2013 年 2 月 11 日付 FSTEC 令 第 17 号））
https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17

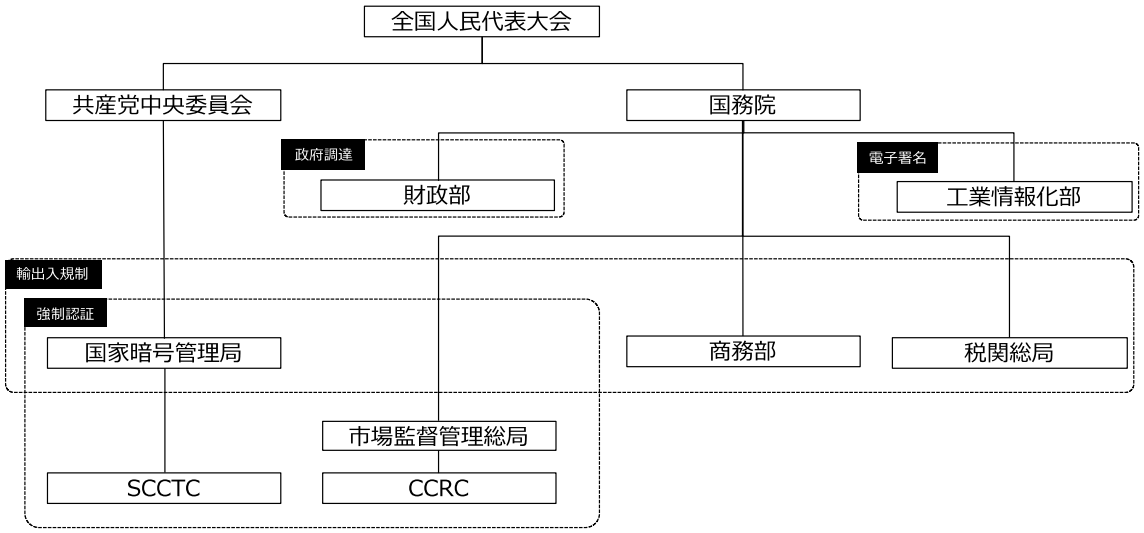
3.7. 中国

中国では、長らく 1999 年 10 月に施行された商用暗号管理条例[1]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の主導の下で暗号政策が実施されてきた。2020 年 1 月に暗号法が施行され、暗号に関する政策の体制・構造が大規模に変更されることとなり、関連する法令や行政規定、標準等の改訂・新規制定が進められている。

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 3-14 である。



CCRC: 中国サイバーセキュリティ審査技術・認証センター

SCCTC: 国家暗号管理局商用暗号テストセンター

図 3-14 中国における暗号政策に係る組織体制

暗号及びセキュリティ政策に関する組織の中で主要なものについて、その役割を以下に示す。

- 国家暗号管理局[119]
  暗号法及び商用暗号管理条例に基づき共産党中央委員会の下に設置された、暗号に関する政策の策定及び実施等を行なう組織であり、各省に支部を設置し、市、郡と連携し業務を分担している。主な役割は、商用暗号や商用暗号製品の管理であり、これらの目的のために商用暗号製品の検査・認定制度の規則の策定及び制度を実施する。

- 工業情報化部[120]
  工業分野における情報化を推進する部門であり、電子署名法等の所管において暗号政策に係わっている。

- 商務部[121]
  経済と貿易を担当する行政部門であり、商用暗号製品の輸出入の規制を担当する。

- 市場監督管理総局[122]
  市場の監督・管理を行う機関であり、商用暗号製品に関して、品質保証のための検査・認定制度の策定・監督を行う。

- CCRC（China Cybersecurity Review Technology and Certification Center、中国サイバーセキュリティ審査技術・認証センター）[123]
  市場監督管理総局配下の組織であり、サイバーセキュリティ製品・サービスの検査・認定などの業務を行う。商用暗号について、国家情報セキュリティ認証制度を実施する。

- SCCTC（State Cryptography Administration Commercial Code Testing Center、国家暗号管理局商用暗号テストセンター）[124]
  国家暗号管理局配下の組織であり、商用暗号製品認証制度を実施し、商用暗号の検査・認定を行う。

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

暗号に関する法制度は、1999 年 10 月に施行された商用暗号管理条例を上位法とし、国家暗号管理局が定める複数の管理規定、その他の関連法令から構成されていた。2020 年 1 月

[119] https://sca.gov.cn/
[120] https://www.miit.gov.cn/
[121] http://www.mofcom.gov.cn/
[122] http://www.samr.gov.cn/
[123] https://www.isccc.gov.cn/
[124] http://www.scctc.org.cn/

に暗号法が施行され、これを上位法とする構成へ移行の過程にある。

中国における暗号政策に関わる主な法制度を分類整理すると表 3-27 と図 3-15 のようになる。

表 3-27　中国における暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	上位政策・戦略	暗号法[2]	国務院、国家暗号管理局	―
2		商用暗号管理条例（国務院 第 273 号)[1]	国務院、国家暗号管理局	後継
3	暗号政策・設置法	商用暗号製品使用管理規定（国家暗号管理局 第 8 号)[7]	国家暗号管理局	後継
4		電子署名法[9]	工業情報化部	後継
5	輸出入規制	対外貿易法[12]、輸出管理法[13]	商務部	後継、―
6		商用暗号輸入許可リスト、輸出管理リストおよび関連する管理措置の発行に関する公告（商務部、国家暗号管理局、海関総署 2020 年第 63 号)[15]	商務部、国家暗号管理局、海関総署	後継
7		技術輸出入管理条例（国務院 2020 年第 4 号)[17]、輸出禁止・制限技術リスト（商務部・科学技術部 2008 年第 12 号)[18]、輸出禁止・制限技術リスト調整のお知らせ(商務部、科学技術部 2020 年第 38 号)[19]	商務部、科学技術部	―
8		信頼できない事業体リスト（商務部 2020 年第 4 号)[16]	商務部	―
9		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措置（国家暗号管理局 第 9 号)[8]	国家暗号管理局	廃止
10	政府調達	政府調達法[20]	財政部	後継
11		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（認証認定局 2010 年第 26 号)[21]	国家品質検査検疫総局、国家認証認可監督管理委員会	更新無
12	標準・基準	商用暗号科学研究管理規定（国家暗号管理局 第 4 号)[4]	国家暗号管理局	後継
13		商用暗号製品生産管理規定（国家暗号管理局 第 5 号)[5]	国家暗号管理局	後継
14		商用暗号製品販売管理規定（国家暗号管理局 第 6 号)[6]	国家暗号管理局	廃止
15		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 第 17 号)[10]	国家暗号管理局	後継
16		商用暗号製品の管理方法の調整について（国家暗号管理局、市場監督総局 第 39 号)[34]	国家市場監督管理総局、国家暗号管理局	―
17		「商用暗号製品の認証カタログ(初回)」および「商用暗号製品の認証規則」の公告（市場監督総局・暗号管理局 2020 年第 23 号)[35]	国家市場監督管理総局、国家暗号管理局	―
18	その他	国家情報法[36]	国家安全部	―
19		行政承認項目およびその他の事項の一括廃止および調整に関する国務院の決定（国発〔2015〕11 号)[28]	国務院	―
20		非行政許可承認事項の決定取り消しに関する国務院の決定（国発〔2015〕27 号)[29]	国務院	―

21		管理承認項目の公開カタログの調整に関する国家暗号管理局の通知[30]	国家暗号管理局	—
22		行政許可項目の一括取り消しに関する国務院の決定（国発〔2017〕46 号）[31]	国務院	—
23		商用暗号製品生産ユニットの承認を含む 4 つの管理ライセンスの廃止後の管理政策の継続に関する国家暗号管理局の通知（国家秘密局 2017 年第 336 号）[32]	国家暗号管理局	—
24		特定の行政規則の廃止と変更に関する国家暗号管理局の決定（国家暗号管理局 第 32 号）[33]	国家市場監督管理総局、国家暗号管理局	—

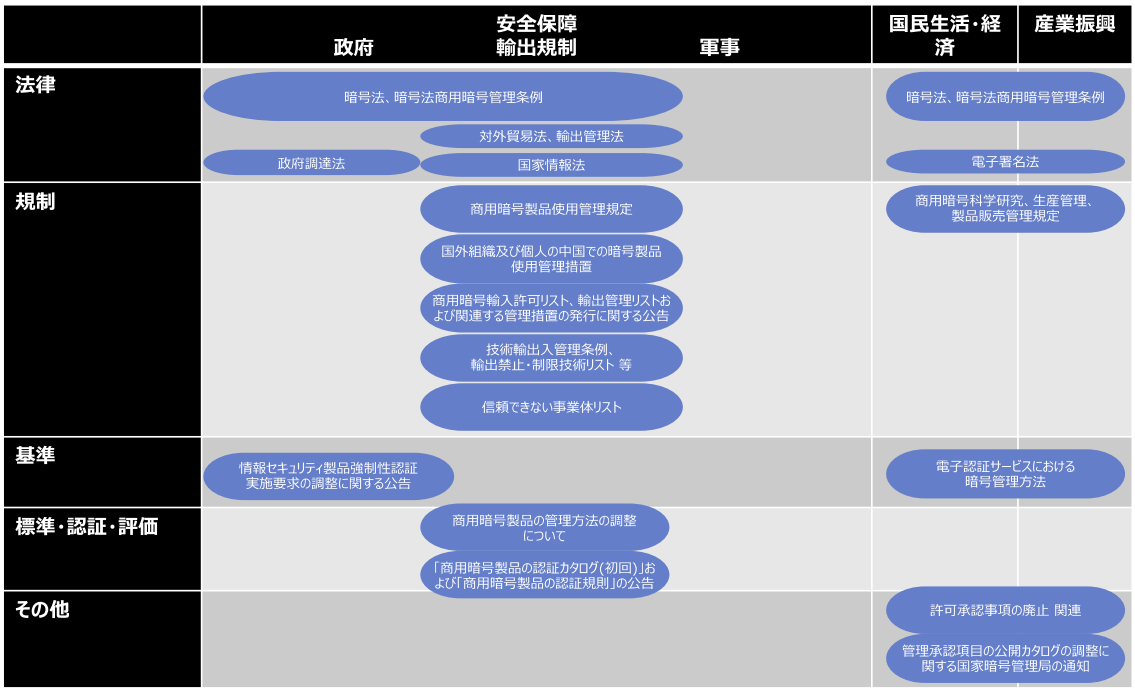


図 3-15　中国における暗号関連政策マップ

主な法制度の概要は以下の通りである。

- 暗号法[2]

  2020 年 1 月に施行、暗号の利用と管理について定める。国家暗号管理局の設置法でもある。

  暗号を核心暗号、普通暗号、商用暗号に分類し、以下のように定める。

  - 核心暗号、普通暗号

    国家機密情報の保護に利用、暗号管理局が厳格に管理、暗号自体が国家機密

  - 商用暗号

    国家機密以外の情報の保護に利用

また、商用暗号について、主に以下を定める。

- 暗号技術の標準化
- 暗号製品の検査・認証制度
- 国家安全保障に影響を与える可能性のあるネットワークが使用する製品・サービスの検査制度
- 重要な情報インフラの運用安全性評価制度
- 輸出入規制

- 商用暗号管理条例（国務院令 第 273 号)[1]
  暗号法制定以前の暗号に関する上位法。
  1999 年 10 月に施行された条例であり、国家安全保障の維持を目的とし、商用暗号の管理を行なうことを目的とする。商用暗号を、国家機密を含まない情報の暗号化・認証に利用する、国家機密指定の暗号と定める。また、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る。
  暗号法の制定により商用暗号の管理構造が再構築され、本条例は暗号法の要件を満たせなくなった。条例の改正に向けて、2020 年 8 月に商用暗号管理条例（意見募集草案）[3]が公開された。

- 電子署名法[9]
  電子署名の有効性、満たすべき要件などを定める。電子署名は第三者（電子認証サービス提供者）による認証が必要となる。電子認証サービス提供者は、暗号管理局より「電子認証サービスの暗号使用許可」を取得した上で、工業情報化部より「電子認証許可」の認可を得なければならない。
  なお、2014 年度調査の後、暗号に関係がある部分の改正はない。

- 対外貿易法[12]、輸出管理法[13]
  対外貿易法は外国との輸出入に関する規制について定める。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している。
  なお、2014 年度調査の後、暗号に関係がある部分の改正はない。
  一方、輸出管理法は 2020 年 12 月に施行された輸出管理の強化を目的とした法律であり、主にデュアルユース製品の輸出規制、信頼できない企業や個人に対する輸出規制、再輸出規制などを定める。報復条項を持ち、他国による輸出管理措置の濫用に対し、相応の措置を講じるとしている。

- 商用暗号輸入許可リスト、輸出管理リストおよび関連する管理措置の発行に関する公告（商務部、国家暗号管理局、海関総署 2020 年第 63 号）[15]

暗号法、輸出管理法、関税法に基づき輸出入管理措置を定める。規制対象品目をリストで管理し、該当する暗号製品・技術の輸出入を行う場合、商務部の許可が必要となる。2014 年度調査の後、根拠法が商用暗号管理条例から暗号法へ、また、主管する機関が暗号管理局から商務部へ変更された。これについて、3.7.3.4 節に記載する。

- 技術輸出入管理条例（国務院 2020 年第 4 号）[17]、輸出禁止・制限技術リスト（商務部・科学技術部 2008 年第 12 号）[18]、輸出禁止・制限技術リスト調整のお知らせ（商務部、科学技術部 2020 年第 38 号）[19]
  対外貿易法に基づき、国内の技術の権利や利益の保護を目的として実施される、技術の輸出入禁止及び制限について定める。輸出禁止・制限技術リストを商務部が作成し公開する。輸出禁止技術の輸出は許されない。輸出制限技術を輸出する場合、商務部による許可が必要となる。
  輸出が制限されている技術を輸出する場合、商務部による許可が必要となる。これについて、3.7.3.4 節に記載する。

- 信頼できない事業体リスト（商務部 2020 年第 4 号）[16]
  対外貿易法、国家安全法に基づき、中国の主権や国家安全保障、開発の利益を脅かす外国企業や個人を「信頼できない事業体リスト」で管理し、相応の措置を行うと定める。2021 年 2 月時点では、リストはまだ公開されていない。これについて、3.7.4.2 節に記載する。

- 政府調達法[20]
  政府調達の適用範囲、調達方式、調達手続きについて定める。国産品の優遇について明記している。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している。これについて、3.7.3.3 節に記載する。
  なお、2014 年度調査の後、暗号に関係がある部分の改正はない。

- 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（認証認定局 2010 年第 26 号）[21]
  強制認証制度の一部として実施される国家情報セキュリティ認証制度の対象を、政府調達に限るとした公告。
  なお、2014 年度調査の後、暗号に関係がある部分の改正はない。

- 商用暗号科学研究管理規定（国家暗号管理局 第 4 号）[4]
  商用暗号管理条例に基づき商用暗号研究開発を規制する。商用の暗号研究を行なおうとする者は、事前に暗号管理局に申請を行ない、「商用暗号科学研究指定ユニット」指

定を得る必要がある。研究結果は国家暗号管理局がレビュー・評価を行い、承認する。「商用暗号科学研究指定ユニット」指定制度は（国発〔2017〕11 号）により廃止された。

- 商用暗号製品生産管理規定（国家暗号管理局 第 5 号）[5]
  商用暗号管理条例に基づき商用暗号製品の製造を規制する。商用暗号製品の生産を行なおうとする者は、事前に暗号管理局に申請を行ない、「商用暗号製品生産指定ユニット」指定を得る必要がある。商用暗号製品の製造を行う者は、製品の製造開始前にサンプル品を作成して暗号管理局へ申請し、セキュリティレビューに合格し、商用暗号製品の「種類とモデル」指定を取得する必要がある。また、製品の販売を開始する前に、強制認証の対象となる製品は、国指定の組織により試験・認定される必要がある。対象外の製品は、暗号管理局によって指定された製品品質試験機関によって試験・認定されることが求められる。
  「商用暗号製品生産指定ユニット」指定制度は（国発〔2017〕46 号）により廃止された。「種類とモデル」指定項目は、国家暗号管理局・国家市場監督管理総局公告（第 39 号）により廃止され、「全国商用暗号認証制度」へ移行した。この制度は（国家市場監督管理総局・国家暗号管理局 2020 年第 23 号）で説明されている。

- 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 第 17 号）[10]
  電子署名法、商用暗号管理条例に基づき、電子認証サービスを行なう者に対する要件を定める。技術基準は本公告とは別に定められている。
  2017 年 12 月、(国家暗号管理局 第 32 号)により改正され、電子認証サービスの構築者の要件から「商用暗号製品生産指定ユニット」の指定が取り除かれる等の変更等が行われた。

- 商用暗号製品の管理方法の調整について（国家暗号管理局、市場監督総局 第 39 号）[34]
  暗号法の規定に従い、商業暗号製品の「種類とモデル」の指定を廃止し、市場監督総局・国家暗号管理局による「統一全国商用暗号認証システム」（全国商用暗号認証制度に相当）を開始すると説明している。詳細は（市場監督総局・国家暗号管理局 2020 年第 23 号）で規定されている。

- 「商用暗号製品の認証カタログ（初回）」および「商用暗号製品の認証規則」の公告（市場監督総局、国家暗号管理局 2020 年第 23 号）[35]

全国商用暗号認証制度[125]の実施のために策定された、認証規則と商用暗号製品の初回認証カタログを公開する。
認証規則は、制度実施のための基本原則と要件を定め、認証モデル、実施手順、関係者の責任等について定める。
一方、認証カタログには、認証対象となる暗号製品と対応する検証要件が一覧形式で記載している。検証要件は、いずれも業界標準（GM/T）として制定された標準を参照する。また、この認証カタログは、認証対象の暗号製品の使用する暗号アルゴリズの国内暗号への準拠を求めている。

- 国家情報法[36]
  中国の情報活動を強化・保護し、国家の安全と利益の維持を目的として制定された法律であり、情報活動の定義、実施体制、情報活動期間の機能と権限、国民の権利と義務について定める。
  全ての組織や国民は国家情報活動を支援・協力し、国の情報活動の秘密を守るものとする（第 7 条）、国家情報活動機関は、関連する個人や組織と協力関係を確立し、関連する活動を委託することができる（第 12 条）などの条文を含む。

- 行政承認項目およびその他の事項の一括廃止および調整に関する州議会の決定（国発〔2015〕11 号）[28]
  多数の承認項目を一括して取り消し調整する決定である。171 件の取り消し項目等の中に、商用暗号科学的研究管理規定の「商用暗号科学研究指定ユニット」指定が含まれる。

- 非行政許可承認事項の決定取り消しに関する国務院の決定（国発〔2015〕27 号）[29]
  多数の許可承認項目を一括して取り消し調整する決定である。133 件の取り消し項目の中に、電子署名法の「電子政府の電子認証インフラの安全性審査」許可承認項目が含まれている。

- 管理承認項目の公開カタログの調整に関する国家暗号管理局の通知[30]
  本通知の公開時点の国家暗号管理局の承認項目一覧「国家暗号管理局行政承認項目公開カタログ」を公開する。商用暗号管理条例と関連する管理規定の中で、商用暗号に関する多数の承認項目が定められているが、本通知の公開までに廃止・追加となった項目がある。最新のカタログは、国家暗号管理局のウェブサイトに掲載されている[126]。

[125] 商用暗号テストセンターが運用 http://service.scctc.org.cn/
[126] https://sca.gov.cn/sca/xxgk/index.shtml の「行政审批事项公开目录」より確認できる。

- 行政許可項目の一括取り消しに関する国務院の決定（国発〔2017〕46 号）[31]
  多数の許可項目等を一括して取り消し調整する決定である。 廃止される許認可項目の中に、「商用暗号製品生産指定ユニット」、「商用暗号製品販売許可」、「国外生産暗号製品の使用許可」、「外国組織・個人の暗号製品使用許可」が含まれる。

- 商用暗号製品生産ユニットの承認を含む 4 つの管理ライセンスの廃止後の管理政策の継続に関する国家暗号管理局の通知（国家秘密局 2017 年第 336 号）[32]
  （国発〔2017〕46 号）で暗号に関わる 4 つの承認項目が廃止となった後、以下が引き続き実施されることを公表された。
  - 製造・販売する暗号製品を登録し「種類とモデル」の指定を取得
  - 外国組織、個人が海外の暗号製品を利用する場合、「暗号製品輸入許可」を取得
  - 商用暗号製品の販売登録データの登録

- 特定の行政規則の廃止と変更に関する国家暗号管理局の決定(国家暗号管理局 第 32 号)[33]
  管理規定の廃止と修正について、国家暗号管理局の決定を通知する。以下の 3 つの規定が廃止となる。
  - 商用暗号製品販売管理規定（国家暗号管理局 第 6 号）
  - 商用暗号製品使用管理規定（国家暗号管理局 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措置（国号管理局 第 9 号）

  また、過去の承認項目の廃止時に修正されなかった管理規定を修正する。
  - 「商用暗号科学研究指定ユニット」指定の廃止: 商業暗号研究管理に関する規定（国家暗号研究行政発表第 4 号）
  - 「商用暗号製品生産指定ユニット」指定の廃止: 商用暗号製造管理に関する規定（国家暗号管理局の発表第 5 号）、及び、電子認証サービスの暗号管理措置（国家暗号管理局 第 17 号）

また、上記の公告等により、2014 年度調査の後に廃止された主な法制度の概要は以下の通りである。

- 商用暗号製品使用管理規定（国家暗号管理局 第 8 号））[7]
  （国家暗号管理局 第 32 号）により廃止された。
  商用暗号管理条例に基づき商用暗号の使用を規制する国家暗号管理局の管理規定である。中国公民、法人、その他の組織が使用できる商用暗号製品は、国家暗号管理局が許

可したのみに限定する。また、商用暗号製品の購入時に ID 等の提示などを要求する。外国企業は国外で生産された暗号製品の利用が可能であり、事前に暗号管理局より「国外生産暗号製品の使用許可」を取得する必要がある。外国企業が海外で生産された暗号製品を持ち込む場合は、事前に暗号管理局より「暗号製品輸入許可」を取得し、通関手続きの際に税関へ提出する必要がある。

「国外で生産された暗号製品の使用許可」は（国発〔2017〕46 号）により廃止された。

- 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措置(国家暗号管理局 第 9 号)[8]

  （国家暗号管理局 第 32 号）により廃止された。

  商用暗号管理条例に基づき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定める。中国国内で外国組織・個人が商用暗号製品を使用する場合、事前に暗号管理局に申請し、「外国組織・個人の暗号製品使用許可」を取得する必要がある。国外組織等が暗号製品を中国に輸入する場合、事前の「暗号製品輸入許可」の申請が必要である。

  「外国組織・個人の暗号製品使用許可」は、（国発〔2017〕46 号）により廃止された。

- 商用暗号製品販売管理規定（国家暗号管理局 第 6 号）[6]

  （国家暗号管理局 第 32 号）により廃止された。

  商用暗号管理条例に基づき商用暗号製品の販売について定める。商用暗号製品の販売を行なおうとするものは、事前に暗号管理局に申請を行ない、「商用暗号製品販売許可」を得る必要がある。商用暗号製品の販売を行なう者が販売できる商品は、強制認証または製品品質試験機関に認可されたものに限定される。商品の販売時に販売者は、製品の利用者の名前（氏名）、居住地、組織コード（住民 ID 番号）、製品名、モデル、目的、数量を確認し、暗号管理局へ登録する。商用暗号製品を海外で販売する場合は、輸出に関する規制に従うものとする。

  「商用暗号製品販売許可」は、（国発〔2017〕46 号）により廃止された。

3.7.3. 暗号に関わる各種制度、規制及びガイドライン

3.7.3.1. 利用すべき暗号方式

利用すべき暗号方式を明確に定めた文書は見つからなかった。

中国で販売される商用暗号製品は、国家暗号管理局が所管する全国商用暗号認証制度に基づく検査を受ける必要がある。この検査の要件で、暗号製品が使用する暗号アルゴリズムは国産暗号アルゴリズムに準拠することが求められている。

国産の暗号アルゴリズムは、国家暗号管理局により中国の業界標準として、国家標準化管理委員会により中国の国家標準として定められ、ISO 標準にも組み込まれている(表 3-28)。

表 3-28　中国の国産暗号アルゴリズムの業界・国家・国際標準一覧

区分	業界標準	国家標準	国際標準
SM2 楕円曲線公開鍵暗号アルゴリズム	GM/T 0003-2012	GB/T 32918-2016	ISO/IEC 14888-3:2018
SM3 暗号ハッシュアルゴリズム	GM/T 0004-2012	GB/T 32905-2016	ISO/IEC 10118-3:2018
SM4 ブロック暗号アルゴリズム	GM/T 0002-2012	GB/T 32907-2016	ISO/IEC 18033-3:2010/DAMD 1
SM9 ID ベース暗号アルゴリズム	GM/T 0044-2016	GB/T 38635-2020	ISO/IEC 18033-5:2015/DAMD 1 ISO/IEC 11770-3:2015/DAMD 2
ZUC ストリーム暗号アルゴリズム	GM/T 0001-2012	GB/T 33133-2016	ISO/IEC 18033-4:2011/AMD 1:2020

3.7.3.2.　セキュリティ製品認証制度・セキュリティサービス認証制度

商用暗号に関して、3 つの認証制度を実施している。国家情報セキュリティ認証制度、主要なネットワーク機器およびネットワークセキュリティ製品のセキュリティ認証制度、商用暗号製品認証制度である。いずれも、強制認証制度の一部として実施している。ISO/IEC 15408 に対応した中国標準 GB/T18336 に基づき、CC と同様の認証スキームとして運用している。評価基準は CC と大きな違いは無いが、評価方法については、製品のプロトタイプに対する型式試験、製品に対する初回工場検査、承認後の監督から構成され、独自な部分も存在している。

- 国家情報セキュリティ認証制度 [127]

  国家情報セキュリティ認証制度（CC-IS: China Certification of Information Security）は、商用暗号管理条例第 9 条及び商用暗号製品生産管理規定第 15 条に基づき、中国サイバーセキュリティ審査技術・認証センター（CCRC: China Cybersecurity Review Technology and Certification Center、旧:中国情報セキュリティ認証センター（ISCCC：China Information Security Certification Center））[128]が実施している情報セキュリティ認証制度である。政府調達法は、情報セキュリティ製品の認証取得を義務づけている。

  2008 年 1 月、一部の情報セキュリティ製品に対する強制認証の実施を、国家認証認可監督管理委員会等が公表[21]した後、2009 年 5 月に実施要件・実施開始日（2010 年 5 月 1 日）・認証範囲の政府調達への限定を公表した[22]。2010 年 4 月、政府調達に関する規則を明確化し[23]、2010 年 7 月、制度の名称を「国家情報セキュリティ認証制度」に決定、証明書の形式、認証マークを公表した[24]。

[127] https://www.isccc.gov.cn/zxyw/cprz/gjxxaqcprz/index.shtml

[128] 中国网络安全审查技术与认证中心 https://www.isccc.gov.cn/

- 重要なネットワーク機器およびネットワークセキュリティ製品のセキュリティ認証制度[129]

  重要なネットワーク機器およびネットワークセキュリティ製品のセキュリティ認証制度は、暗号法 26 条、サイバーセキュリティ法 23 条に基づき、CCRC が実施する情報セキュリティ認証制度である。この認証制度は CC-IS に基づき構成され、認証モデルや手順、認定マーク等、CC-IS と共通のものとなっている。認証制度の対象となる製品一覧、実施要件、検査・認証機関は公表されているが、製品ごとの認証要件を見つけることができず、詳細を把握することができない。対象となる製品は、重要なネットワーク製品としてルータやスイッチ等、ネットワークセキュリティ製品として、ファイヤーウォールや侵入検知システムなどを含む。

  2017 年 6 月、重要なネットワーク機器及びネットワークセキュリティ製品の一覧（初回）が公表された[25]。

  2018 年 3 月、セキュリティ認証・安全検査タスクを実施する組織の一覧（初回）が発表され[26]、CCRC を認証機関、その他 15 の機関を検査機関として指定している。

  2018 年 6 月、セキュリティ認証実施要件（CNCA-CCIS-2018）を公表し[27]、運用を開始した。

- 商用暗号製品認証制度[130]

  商用暗号製品認証制度は、国家暗号管理局商用暗号テストセンターが実施する商用暗号製品の認証制度である。

  暗号法の制定前に商用暗号管理条例第 8 条及び商用暗号製品生産管理規定第 12 条に基づき実施されてきた、暗号製品を生産する場合の商用暗号製品の種類とモデルの承認、製品の試験・認証制度を、暗号法のもと新たな制度として置き換えたもの。暗号管理局による集中管理から試験・認可形式へ移行し、強制認証制度化した。

  商用暗号製品認証規則及び、製品種類別の認証基準を示した認証カタログが公開されている。認証基準は業界標準（GM/T）を参照している。また、暗号アルゴリズムの国産暗号準拠を定めている。カタログの各製品の認定要件に「GM/T 0028 暗号モジュールのセキュリティ技術要件」が含まれており、GM/T 0028-2013 の中で ISO19790: 2012 を参照していることから、米国の CMVP に相当する検査も行われていると推測される。

  2019 年 12 月、暗号法施行に合わせて、暗号製品のモデルと承認制度を廃止し[34]、2020 年 5 月、商用暗号製品認証規則及び製品認証カタログを公開、認証制度を開始した[35]。

---

[129] https://www.isccc.gov.cn/zxyw/cprz/wlgjsb/index.shtml

[130] http://service.scctc.org.cn/

商用暗号製品認証一覧: http://service.scctc.org.cn/cer/cerall/list-c38.html

これらの試験・認証制度について、所管、認証機関、評価機関、認証件数を表 3-29 にまとめた。

表 3-29　中国の認証制度と関連する機関

	国家情報セキュリティ認証制度	重要なネットワーク機器およびネットワークセキュリティ製品のセキュリティ認証制度	商用暗号製品認証制度
所管	国家認証認可管理委員会	国家認証認可管理委員会	国家暗号管理局
認証機関	中国サイバーセキュリティ審査技術・認証センター	中国サイバーセキュリティ審査技術・認証センター	国家暗号管理局商用暗号テストセンター
評価機関	・情報産業部コンピュータセキュリティ技術試験センター ・国家機密局機密情報システムセキュリティ評価センター ・公安部コンピュータ情報システムセキュリティ製品品質監督検査センター ・国家暗号局商業暗号試験センター ・中国情報セキュリティ試験評価センター情報セキュリティ研究所 ・北京情報セキュリティ試験評価センター ・上海情報セキュリティ評価認証センター	・ 中国情報セキュリティ認証センター ・ 中国情報通信研究院/中国テレサービス研究所 ・ 全国コンピュータネットワーク・情報セキュリティ管理センター ・ 産業制御システム・製品安全国家品質監督検査センター ・ 中国電子技術標準化研究所賽西研究所 ・ 産業情報技術省 第五電子工学研究所 ・ 情報産業データ通信製品品質監理検査センター ・ 全国電話交換品質監理検査センター ・ 情報産業無線通信製品の品質監理検査センター ・ 情報産業有線通信製品の品質監理検査センター ・ 情報産業用光通信製品品質監理検査センター ・ 広州情報産業電話交換設備品質監督検査センター ・ 公安部コンピュータ情報システムセキュリティ製品品質監督検査センター ・ 公安警察省電子製品品質試験センター ・ 国立コンピュータウイルス緊急対策センター コンピュータウイルス対策製品試験所 ・ 情報産業試験評価センター	国家暗号管理局の商用暗号テストセンター 鼎軒商業暗号評価技術(深セン)株式会社 智巡暗号(上海)検査技術株式会社
認証件数	不明	不明	2020 年 431 件 2019 年 677 件 2018:年 273 件

※ 商用暗号製品認証制度の認証件数の年と後の件数は、認定日の情報が得られたかったため、有効期限を元に有効期間 5 年として集計。

3.7.3.3. 政府の調達要件

政府調達法に基づき、国家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を義務付けている[23]。これらの製品が利用する暗号は、認証制度の定める各製品の要件により、国の暗号管理要件に準拠することが求められる。

3.7.3.4. 暗号の輸出入規制

中国は、商用暗号の輸出入を、デュアルユース品目の輸出入管理制度、技術輸出入管理制度により規制している。いずれも商務部が主管する。

デュアルユース品目と技術の輸出入管理制度は、暗号法、対外貿易法、関税法に基づき実施される制度で、国家安全保障と社会的公益の維持を目的とする。

規制対象品目は、商用暗号輸入許可リスト・輸出管理リストとして、商務部・国家暗号管理局、海関総署より公開され[15]、掲載されている製品や技術を輸入・輸出する場合、商務部の許可が必要となる。リストの概要を表 3-30 に示す。ただし、マスマーケット向け製品の商用暗号は輸出入管理の対象に含まれない。マスマーケット向け製品の具体的範囲は明確に定義されておらず、国家暗号管理局ウェブサイトの暗号政策に関する質問・回答ページに、「個人利用の制限なく、従来の小売ルートで一般の人々が購入できる製品や技術であって、暗号機能を容易に変更できないもの」との説明がある[131]。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。

技術輸出入管理制度は、対外貿易法、技術輸出入管理条例に基づき実施される制度で、技術の輸出入秩序の維持、経済・社会の発展の促進を目的とするものである。

規制対象品目は、輸出禁止・制限技術リストとして、商務部・科学技術部より公開され[18][19]、記載されている製品や技術を輸出する場合、商務部の許可が必要となる。リストの項目のうち暗号に関連するものの概要を表 3-31 に示す。

なお、従来の商用暗号製品の輸出入管理制度は、2020 年 1 月の暗号法の制定により、大きく変更された。

暗号法施行以前、商用暗号製品の輸出入管理制度は、商用暗号管理条例の規定（第 13 条）と関連する施行規則に基づき、国家暗号管理局により行われてきた[6][7][8]。

国家暗号管理局は輸入規制対象品目リストを公開し、該当する製品・技術を輸入する場合、国家暗号管理局の許可が必要となる。輸出の場合は、品目リストは存在せず、すべての商用暗号製品を対象として、輸出の場合と同様に、国家暗号管理局の許可が必要であった。

輸入規制対象品目リストは 2009 年 12 月に初回のリストが公開、2013 年 12 月に更新され

[131] https://sca.gov.cn/sca/xxgk/2020-04/02/content_1060694.shtml

ている[29]。また、この施行規則は 2017 年 9 月に修正[31]、2017 年 12 月に廃止[33]されたが、制度は継続された[32]。

暗号法施行後、商用暗号製品の輸出入規制管理の根拠は暗号法の規定（第 28 条）となった。暗号の輸出入管理は、商務部が実施するデュアルユース品目と技術の輸出入管理承認制度によるものとなり、2021 年 1 月にこれまでの制度は廃止、前述の通り、新たな制度の下で輸出入管理対象となる暗号製品及び技術のリストが公開された[14][15]。

表 3-30　中国の商用暗号輸入許可リスト・輸出管理リストの概要（2021 年 1 月）

リスト	規制対象品目	規制対象となる条件
輸入許可リスト	暗号電話	
	暗号ファクシミリ	
	暗号装置(暗号ボード)	共通鍵暗号アルゴリズムで暗号化・復号速度 10Gbps 以上
	暗号 VPN 設備	暗号通信速度 10Gbps 以上
輸出管理リスト	セキュリティチップ	電力、税務、公安、金融等の分野専用の暗号アルゴリズムを含む 共通鍵暗号アルゴリズムで暗号化・復号速度 10Gbps 以上もしくは 公開鍵暗号アルゴリズムの署名速度 50,000 回/秒以上
	暗号装置(暗号ボード)	共通鍵暗号アルゴリズムで暗号化・復号速度 10Gbps 以上もしくは 公開鍵暗号アルゴリズムの署名速度 50,000 回/秒以上
	IPsec/SSL VPN 設備	暗号通信速度 10Gbps 以上
	暗号鍵管理製品	サポート管理対象数 10,000 以上
	暗号専用設備	電力、税務、公安、金融等の分野専用の暗号アルゴリズムを含む設備
	量子暗号設備	
	暗号分析設備	
	暗号の研究・生産設備	上記商用暗号輸出管理リスト品目の研究・生産設備
	暗号の試験検証設備	上記商用暗号輸出管理リスト品目の測定・試験・評価・検証設備
	ソフトウェア	上記商用暗号輸出管理リスト品目の研究・生産、使用に用いるソフトウェア
	技術	上記商用暗号輸出管理リスト品目の研究・生産、使用に用いる技術

※ いずれの品目も、使用される暗号アルゴリズムの条件が、共通鍵暗号：鍵長 64 ビット以上、RSA 暗号：768 ビット以上、楕円曲線暗号：128 ビット以上であることとされている。

表 3-31　中国の輸出禁止・制限技術リスト上の暗号に関連する項目（2020 年 8 月末）

リスト	技術名	規制対象となる条件
輸出禁止技術リスト	宇宙船の測定制御技術	人工衛星と、その無線遠隔制御における符号化・暗号化技術
	宇宙データ伝送技術	以下の衛星情報暗号化技術のいずれかを含む 1. 機密保護の原理、方法、回路設計技術 2. 暗号化・復号ソフトウェアおよびハードウェア
	衛星応用技術	北斗衛星ナビゲーションシステムの情報伝送暗号化技術

輸出制限技術リスト	通信伝送技術	テレビおよび電話のセキュリティ技術に含まれる暗号設計技術
		中国で開発され軍事分野で使用される情報送信、暗号化・復号技術
	水中低周波電磁通信技術	水中低周波電磁通信技術に含まれる通信セキュリティ技術で、中国のために特別に開発、設計、製造された通信セキュリティ機器及び通信暗号化技術
	情報処理技術	情報アクセスの暗号化・復号技術
	暗号セキュリティ技術	暗号化チップの設計と実装技術(高速暗号アルゴリズム、並列暗号技術、暗号化チップのセキュリティ設計技術、SoC)の設計と実装技術、高速アルゴリズム標準に基づく高速チップ実装技術)
		量子暗号技術(量子暗号実現法、量子暗号伝送技術、量子暗号ネットワーク、量子暗号工学的実装技術)

3.7.3.5. プロトコル等での暗号方式

商用暗号製品認証制度による強制認証対象製品の認定基準として GM/T 0024「SSLVPN 技術仕様」、GM/T 0022「IPSecVPN 技術仕様」を策定し、TLS、IPsec に関する暗号アルゴリズムや設定を定めている。いずれの仕様書も暗号アルゴリズムは、国の暗号管理要件に準拠した以下の暗号アルゴリズムに準拠すること定めている。

- GM/T 0001 ZUC ストリーム暗号アルゴリズム
- GM/T 0002 SM4 ブロック暗号アルゴリズム
- GM/T 0003 SM2 楕円曲線公開鍵暗号アルゴリズム
- GM/T 0004 SM3 暗号ハッシュアルゴリズム
- GM/T 0044 SM9 ID ベース暗号アルゴリズム

3.7.3.6. 暗号利用に関する規制（利用ライセンス・暗号盗聴法など）

中国では、暗号の利用は規制されていない。

ただし、国家情報法に「全ての組織や国民は国家情報活動を支援・協力し、国の情報活動の秘密を守るものとする」（第 7 条）という条文があり、中国製の情報機器・通信機器の製造者やサービス提供者が当局に取扱う情報を提供する可能性があると考えられている。

3.7.3.7. クラウドサービス

クラウドサービスを含むサイバーセキュリティの安全性確保、国家の主権、公益の保護などを目的とし、サイバーセキュリティ法を 2017 年 6 月に施行している。多くの規定を含むが、特に重要な項目を以下に示す。

- サイバーセキュリティ等級保護

  サイバーセキュリティに関するリスクの影響度とシステムの重要度に応じて対策や管

理を行う方法を定めた国家標準の改正について、「サイバーセキュリティ等級保護規制（意見募集草案）（公安部 2018 年）[37]」を公表した後、以下を含む国家標準を改正した。

- GB/T 22239　サイバーセキュリティ級保護基本要件
- GB/T 22240　サイバーセキュリティ等級保護分類ガイド
- GB/T 25058　サイバーセキュリティ等級保護実施ガイド
- GB/T 25070　サイバーセキュリティ等級保護セキュリティ設計技術要件
- GB/T 28448　サイバーセキュリティ等級保護評価要件

- 重要な情報インフラ

  重要な情報インフラの運営者にセキュリティ保護義務を課し、国家サイバースペース局が実施する国家安全保証審査を受け、ネットワーク製品やサービスの購入時に秘密保持契約の締結を義務付けている。サイバーセキュリティレビュー方法（中国国家ネットワーク情報弁公室、その他 11 組織による命令 2020 年第 6 号）[38]を公表し、国家標準として以下を策定した。

  - GB/T 39204　ネットワークセキュリティ保護の基本要件
  - 20173587-T-469　検査および評価ガイドライン
  - 20173586-T-469　保証指標体系
  - 20173588-T-469　セキュリティ制御要件

3.7.3.8.　暗号資産

中国では、いわゆるデジタル人民元の研究・開発が進み、いくつかの地域で実証実験が行われている。商務部は、2020 年 8 月にサービス貿易の革新的と発展のための試行の包括的深化の全体計画[41]を公表し、その中でデジタル人民元の実験を 2022 年の冬季五輪の会場となる地域（深圳、成都、蘇州、熊安新区）で先行的に開始し、適宜他の地域に拡大していくと表明した。これらの地域では、順次、一部の市民にデジタル人民元が配られ、携帯端末に導入したウォレットアプリケーションを通して利用されている。

この他にも実証実験が行われているが、いずれも関連する法令や技術的な資料を見つけることができなかった。

一方、中国人民銀行は、2020 年 10 月に、中国人民銀行法（意見募集草案）[42]を公表した。以下の条文を含み、デジタル通貨の発行の法的根拠を用意し、また、組織や個人によるデジタルトークンの作成・販売を禁止するものとなっている。なお、トークンの発行は 2007 年 9 月の中国人民銀行等の共同広告[43]により禁止されており、これを法令化するものとなっている。

- 第 19 条（人民元の単位）の 2 項: 人民元には、物理形式とデジタル形式が含ま

れる。

- 第 22 条(トークン): ユニットまたは個人は、市場で流通している人民元に代わるトークン、クーポン、およびデジタルトークンを作成または販売することはできない。

また、国家インターネット情報局は、サイバーセキュリティ法に基づき「ブロックチェーン情報サービス管理規定」[44]を制定し、ブロックチェーン技術やシステムに基づく情報サービスを監督している。それらのサービス提供者に、利用者の本人確認、コンテンツやログの保存、法務執行機関からの要請に応じた情報の提供を義務付けている。

3.7.3.9. 電子署名法

中国の電子署名法は、2005 年 4 月に施行され、2019 年 4 月に改正されている。

電子署名は、電子署名を以下のように定めている。

- 電子的形式のデータメッセージに含まれ、署名者を識別し、署名者の承認を示す目的で添付されたデータ（第 2 条）
- 契約書やその他の文書として電子的形式の電子署名とデータメッセージの利用を当事者が同意した場合に法的に有効（第 3 条）
- 電子署名とデータメッセージの形式であるという理由だけで否定されない（第 3 条）
- 信頼できる電子署名は、手書きの署名または印鑑と同じ法的効力を持つ（第 14 条）

信頼できる電子署名は、電子署名作成データ（鍵）が以下の条件を満たす、もしくは、合意された信頼条件を満たすもの（第 13 条）としている。

- 電子署名用データは署名者専用
- 電子署名用データは署名者のみが制御
- 署名後、電子署名への変更を検出できる
- 署名後、データメッセージの変更を検出できる

電子署名の第三者認証のため、電子認証サービス機関は認証サービスを提供できる（第 16 条）とされ、その詳細は、電子認証サービスの暗号管理措置（国家暗号管理局 第 17 号）、電子認証サービスの管理措置（工業情報化部 2015 年第 29 号）[11]で定められている。概要は以下の通り。

- 電子認証サービス機関の暗号利用は国家暗号管理局が監督する
- 電子認証サービス及びサービス機関は工業情報化部が監督する
- 電子認証サービス機関は、暗号管理局から「電子認証サービスの暗号使用許可」

を取得する必要がある

- 電子認証サービス機関は、工業情報化部から「電子認証サービス許可」を取得し、工業情報化部が定めた「電子認証事業規則及び規則」に従う必要がある

関連する技術基準に以下がある。

- GB/T 25056　証明書認証システムの暗号および関連する安全技術仕様
- GB/T 25064　PKI 電子署名フォーマット仕様
- GB/T 20520　PKI タイムスタンプ仕様

3.7.3.10.　国民 ID 番号制度（eID）

中国では、身分証明書として居住者 ID カードが発行されている。ID カードの表面には、所有者の氏名、生年月日、公民身分番号、顔写真等が印刷されている。公民身分番号は個人ごとに一意で永続な ID コードである。2004 年より非接触 IC チップ内蔵カード型のカードが交付され、2013 年にチップ非搭載のカードが無効とされた。

公民身分番号は国家標準として、居住者 ID カードに関する標準は業界標準として仕様・要件が定められている。

- GB 11643 公民身分番号
- GA 448 居住者 ID カードの一般的な技術要件
- GA/T 449 居住者 ID カードの条件
- GA/T 451 居住者 ID カード本体の技術仕様
- GA/T 455 居住者 ID カードの印刷要件
- GA 456 居住者 ID カードを視覚的に読み取るための個人情報配置フォーマット
- GA/T 457 居住者 ID カードのコンポーネントレイヤーの技術仕様
- GA/T 458 居住者 ID カードの品質要件
- GA/T 490 ID カード機械読み取り可能情報仕様

2017 年に Wechat（ウィーチャット）が WeChatID, 2018 年に Alipay（アリペイ）が「住民票のオンライン居住者 ID カードオンライン認証機能」と呼ばれるスマートフォンを利用したネットワーク証明書サービスを試験的に開始している。スマートフォンで顔や指紋をスキャンしたり居住者 ID カードを撮影したりすることで、スマートフォンのアプリ上に証明書が登録され、本人確認などの場面で利用できるというものである。

これらいずれも CTID プラットフォーム（信頼できる ID 認証プラットフォーム）と呼ばれる中国公安部第一研究所が研究・開発、関連組織が運用する ID 認証プラットフォームを利用している。WeChatID、住民票のオンライン居住者 ID カードオンライン認証機能、CITD プラットフォームのいずれについても詳しい情報は見つけることができなかったが、生体情報や居住者 ID カード情報を個人の識別に利用し、CITD プラットフォームにより ID 認証をオンラインで利用可能としたものであると推測される。

3.7.3.11. サイバーセキュリティ法における個人情報保護及び越境データ移転の規定

3.7.3.7 節で参照したサイバーセキュリティ法は、クラウドサービスに関する規定だけでなく、個人データの保護、越境データの移転についても定めている。

- 個人情報保護

  個人情報の保管と使用に関して、収集したユーザの情報の機密を厳守すること、収集した個人情報の開示、改竄、破壊、同意のない他者への提供は禁止とし、漏洩、破壊、紛失対策を講じること等を義務付けている。データセキュリティ管理措置（意見募集草案）（国家インターネット情報局(2019)）[38]を公開し、以下の国家標準を策定している。

  - GB/T 35273　個人情報安全規範
  - GB/T 39335　個人情報安全影響評価ガイドライン
  - GB/Z 28828　公的および商用サービス情報システム個人情報保護ガイドライン
  - 20190914-T-469　個人情報安全工程ガイドライン

- 越境データ移転

  中国国内で収集・生成した個人情報や重要情報は中国国内に保管し、越境する場合には、国や社会に与える影響に応じた安全評価を行う必要がある。個人情報国外移転の安全性評価法（意見募集草案）(国家インターネット情報局の通知（2017）)[40]及び以下の国家標準を策定している。

  - 20173853-T-469　データ越境セキュリティ評価ガイドライン

3.7.4. その他

3.7.4.1. 規制の動向

中国の暗号政策は、2020 年 1 月に暗号法が施行されるまで、1999 年 10 月に施行された商用暗号管理条例に基づき実施されてきた。この条例は、商用暗号技術や製品の活動を科学的研究、生産、販売、使用、輸出入に分類し、国家暗号管理局はこれら全ての活動を管理・統制する行政機関として定めている。

国家暗号管理局は商用暗号に関する活動ごとに、管理規定及び措置を定め制定している。それらは、暗号に関する活動の重要なポイントで暗号管理局が検査・確認を行い、許可・承認する制度となっている。この、管理規定と許可・承認項目の対応を表 3-32 に示す。暗号管理局はこれらの規定に基づき商用暗号の管理を実施していた。

表 3-32　中国の商用暗号管理条例に関連する規定・措置と許可・承認項目等一覧

公布・施行日	管理規定(措置を含む)	許可・承認制度等
2005 年 12 月 11 日公布 2006 年 1 月 1 日施行	商用暗号科学研究管理規定	商用暗号科学研究指定ユニット (2015 年 2 月 24 日廃止)
		商業暗号の科学的研究結果のレビューと評価
2005 年 12 月 11 日公布 2006 年 1 月 1 日施行	商用暗号製品生産管理規定	商用暗号製品生産指定ユニット (2017 年 9 月 22 日廃止)
		商用暗号製品の「種類とモデル」指定
		商用暗号製品品質検査機関の承認
2005 年 12 月 11 日公布 2006 年 1 月 1 日施行	商用暗号製品販売管理規定 (2017 年 12 月 1 日廃止)	商用暗号製品販売許可 (2017 年 9 月 22 日廃止)
2007 年 3 月 24 日公布 2007 年 5 月 1 日施行	商用暗号製品使用管理規定 (2017 年 12 月 1 日廃止)	暗号製品輸入許可
		商用暗号製品の輸出許可
		国外生産暗号製品の使用許可 (2017 年 9 月 22 日廃止)
2007 年 3 月 24 日公布 2007 年 5 月 1 日施行	外国組織及び個人による中国における暗号製品の使用管理措置 (2017 年 12 月 1 日廃止)	外国組織・個人の暗号製品使用許可 (2017 年 9 月 22 日廃止)

2015 年以降、暗号分野の成長、市場の自主規制機能の発達、管理の効率化への期待などの理由から、商用暗号活動の管理体制は、これまでの厳格なものから緩和へと方針が変更された。これに伴い、許可・承認制度や管理規定の多くが廃止となった（表 3-33）。

表 3-33　中国の許可・承認制度の廃止を公表した公告・通知一覧

公布日	廃止を公表する公告、通知等	廃止された許可・承認制度
2015 年 02 月 24 日	行政承認項目およびその他の事項の一括廃止および調整に関する国務院の決定 (国発〔2015〕11 号)	商用暗号科学研究指定ユニット
2015 年 05 月 14 日	非行政許可承認事項の決定取り消しに関する国務院の決定 (国発〔2015〕27 号)	電子政府の電子認証インフラストラクチャのセキュリティレビュー
2017 年 9 月 22 日	行政許可項目の一括取り消しに関する国務院の決定 国発〔2017〕46 号)	商用暗号製品生産指定ユニット
		商用暗号製品販売ユニットの承認
		国外生産暗号製品の使用許可
		外国組織・個人の暗号製品使用許可
2017 年 12 月 1 日	特定の行政規則の廃止と変更に関する国家暗号管理局の決定 (国家暗号管理局 第 32 号)	商用暗号製品販売管理規定
		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措置
2019 年 12 月 30 日	商用暗号製品の管理方法の調整について (国家暗号管理局、市場監督総局 第 39 号)	商用暗号製品の「種類とモデル」指定 (商用暗号製品認証制度開始)

※「廃止を公表する公告、通知等」列の公告・通知が「廃止された許可・承認制度」列の許可・認証制度を廃止。

2020 年 1 月、暗号法の施行により、商用暗号の管理体制が再構築されることとなった。これまで商用暗号管理条例に基づき規定されていた管理規則等が、暗号法を根拠とする形へ置き換えられつつある。

商用暗号製品生産管理規定の商用暗号製品の種類とモデルの承認制度は暗号法の制定に合わせて廃止され、新たに商用暗号製品認証制度へ置き換えられた。前者は商用暗号管理条例に基づき暗号管理局が検査・認定を行っていたが、後者は強制認証制度に基づいた制度となっている。また、商用暗号条例は暗号法との整合性が取れなくなっていることから、改正に向けて、2020 年 8 月、国家暗号管理局より商用暗号管理条例（意見募集草案）が公開されている。

3.7.4.2. 国外からの圧力に対する対応措置

米国が 2018 年 8 月中国製通信機器の政府調達を禁止、2019 年 5 月に中国の企業をエンティティリストに追加し輸入を禁止した。その根拠の一つとして、2017 年 6 月より施行されている国家情報法が指摘された。この法律は中国の情報活動について定めたものであり、「全ての組織や国民は国家情報活動を支援・協力し、国の情報活動の秘密を守るものとする」（第 7 条）とある。この規定により、中国製の機器・サービスにより集められた情報が中国当局に送られる可能性が否定できないと考えられている。

このような状況を踏まえ、中国は輸出管理法を 2020 年 12 月より施行し、輸出規制を大幅に強化した。この法律には、「如何なる国或いは地域が輸出管理措置を濫用して、中華人民共和国の国家安全と利益に危害を及ぼした場合は、中華人民共和国は、実際の状況に基づき、当該国或いは地域に対し相応の措置を講じることができる。」（第 48 条）といった報復条項が含まれている。

更に、2020 年 9 月、信頼できない事業体リスト（商務部省令 2020 年第 4 号）制度が実施され、差別的措置や、正常な市場取引原則に違反、中国の主権や安全、利益に危害を及ぼすものなどをリストで管理し、貿易、投資、入国、ビザ発給を禁止する措置をとる事となった。2021 年 2 月時点でリスト自体はまだ公開されていない。

また、中国の北京字節跳動科技（バイドダンス）社が提供する短編動画共有サービス TikTok（ティックトック）について、同様の理由から、米国における事業の 2020 年 11 月 12 日まで（その後、期限が延長され 12 月 4 日まで）の米国企業への売却が米大統領より要求され [132]、複数の企業との売却・提携交渉が進められていた。このような状況の中で、2020

[132] https://www.federalregister.gov/documents/2020/08/19/2020-18360/regarding-the-acquisition-of-musically-by-bytedance-ltd

年 8 月に中国は技術輸出入管理条例に基づく輸出禁止・制限技術リストを改定し[19]、TikTok のサービスが使用するとされている AI やデータ解析に基づくパーソナライズ技術を規制の対象に追加した。これにより、たとえ事業の売却が成功したとしても、実際の事業売却のためには中国当局の許可が必要となると考えられている。

その後、2020 年 9 月、バイドダンスと Oracle、Walmart の提携案を大統領が概ね承認し[133]、交渉が続けられたが、12 月 4 日の期限までにまとまらず、司法省による強制売却命令が施行されうる状態となった中で、引き続き協議が続けられているとされている。

2021 年 2 月、米国新政権は国外企業の提供するソフトウェアのセキュリティリスクについての調査を実施するとし、その期間の強制売却の取り組みを停止すると報道された[134]。また、バイドダンスと Oracle、Walmart の提携計画が破棄されたとも報道されている[135]。

[133] https://www.govinfo.gov/content/pkg/DCPD-202000707/pdf/DCPD-202000707.pdf
[134] https://www.wsj.com/articles/tiktok-sale-to-oracle-walmart-is-shelved-as-biden-reviews-security-11612958401
[135] https://www.scmp.com/news/china/diplomacy/article/3121383/tiktok-continues-negotiations-us-government-concerning-sale-us

3.7.5. 中国の参照文献

[1] 商用密码管理条例（中华人民共和国国务院令 第 273 号）（商用暗号管理条例（国務院 第 273 号））
http://www.gov.cn/zhengce/gongbao/guowuyuan1954-1999.htm の中華人民共和国務院広報(1999 年)第 36 号より

[2] 中华人民共和国密码法（暗号法）
http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml

[3] 商用密码管理条例（修订草案征求意见稿）（商用暗号管理条例（意見募集草案））
https://www.oscca.gov.cn/sca/hdjl/2020-08/20/content_1060779.shtml

[4] 商用密码科研管理规定（国家暗号管理局公告 第 4 号）（商用暗号科学研究管理規定（国家暗号管理局 第 4 号））
http://sca.gov.cn/sca/xwdt/2005-12/11/content_1002351.shtml

[5] 商用密码产品生产管理规定（国家暗号管理局公告 第 5 号）（商用暗号製品生産管理規定（国家暗号管理局 第 5 号））
http://sca.gov.cn/sca/xwdt/2005-12/11/content_1002352.shtml

[6] 商用密码产品销售管理规定（国家密码管理局公告 第 6 号）（商用暗号製品販売管理規定（国家暗号管理局 第 6 号））
http://sca.gov.cn/sca/xwdt/2005-12/11/content_1002354.shtml

[7] 商用密码产品使用管理规定（国家密码管理局公告 第 8 号）（商用暗号製品使用管理規定（国家暗号管理局 第 8 号））
http://sca.gov.cn/sca/xwdt/2007-03/24/content_1002356.shtml

[8] 境外组织和个人在华使用密码产品管理办法（国家密码管理局公告 第 9 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措置（国家暗号管理局 第 9 号））
http://sca.gov.cn/sca/xwdt/2007-03/24/content_1002357.shtml

[9] 中华人民共和国电子签名法（電子署名法）
http://www.npc.gov.cn/wxzl/wxzl/2004-10/20/content_334609.htm

[10]电子认证服务密码管理办法（国家密码管理局公告 第 17 号）（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 第 17 号））
http://www.jsmm.gov.cn/smcms/xzgz/55223.jhtml

[11]电子认证服务管理办法（中华人民共和国工业和信息化部令 第 29 号）（電子認証サービスの管理措置（工業情報化部 2015 年第 29 号））
http://sso.sz.gov.cn/pub/szscjg/xxgk/zcwj/scjgfg/200911/t20091105_1219510.htm

[12]中华人民共和国对外贸易法（対外貿易法）

http://tradeinservices.mofcom.gov.cn/article/zhengce/flfg/201710/2543.html
[13]中华人民共和国出口管制法（輸出管理法）
http://www.npc.gov.cn/npc/c30834/202010/cf4e0455f6424a38b5aecf8001712c43.shtml
[14]国家密码管理局 商务部 海关总署公告 2019 年第 38 号（国家暗号管理局、商務部、海関総署 2019 年第 38 号）
http://www.mofcom.gov.cn/article/b/e/201912/20191202926887.shtml
[15]关于发布商用密码进口许可清单、出口管制清单和相关管理措施的公告（商务部 国家密码管理局 海关总署公告 2020 年第 63 号）（商用暗号輸入許可リスト、輸出管理リストおよび関連する管理措置の発行に関する公告（商務部、暗号管理局、海関総署 2020 年第 63 号））
http://aqygzj.mofcom.gov.cn/article/zcgz/202012/20201203019733.shtml
[16]不可靠实体清单规定（商务部令 2020 年第 4 号）（信頼できない事業体リスト（商務部 2020 年第 4 号））
http://www.mofcom.gov.cn/article/i/jyjl/l/202009/20200903002868.shtml
[17]中华人民共和国技术进出口管理条例（中华人民共和国国务院令 第 331 号，2011 年 1 月 8 日，2019 年 3 月 2 日修订）（中華人民共和国の技術輸出入管理条例（国務院 331 号，2011 年 1 月 8 日，2019 年 3 月 2 日改訂））
http://fms.mofcom.gov.cn/article/a/ae/200403/20040300198763.shtml
[18]中国禁止出口限制出口技术目录（商务部、科技部令 2008 年第 12 号）（輸出禁止・制限技術リスト（商務部・科学技術部 2008 年第 12 号））
http://tradeinservices.mofcom.gov.cn/article/zhengce/flfg/201808/68289.htm
[19]关于调整发布《中国禁止出口限制出口技术目录》的公告（商务部科技部公告 2020 年第 38 号）（輸出禁止・制限技術リスト調整のお知らせ（商務部・科学技術部 2020 年第 38 号））
http://www.gov.cn/zhengce/zhengceku/2020-08/29/content_5538299.htm
[20]中华人民共和国政府采购法（中華人民共和国の政府調達法）
http://www.npc.gov.cn/wxzl/gongbao/2014-11/18/content_1892150.htm
[21]关于部分信息安全产品实施强制性认证的公告（国家质检总局 国家认监委 2008 年第 7 号公告）（特定の情報セキュリティ製品の強制認証の実施に関する発表（国家品質監督検査検疫総局、国家認証認可監督管理委員会 2008 年第 7 号））
http://www.cnca.gov.cn/zl/qzxcprz/mlmsyjd/202007/t20200715_59748.shtml
[22]关于调整信息安全产品强制性认证实施要求的公告（国家认证认可监督管理委员会公告 2009 年第 33 号）（情報セキュリティ製品の強制認証の実施要件の調整に関する公告（国家認証認可監督管理委員会 2009 年第 33 号））
http://www.cnca.gov.cn/zw/gg/gg2009/202008/t20200818_62969.shtml

[23]财政部 工业和信息化部 质检总局 认监委关于信息安全产品实施政府采购的通知（财库〔2010〕48号）（財政部、工業情報化部、国家品質監督検査検疫総局、国家認証認可局の情報セキュリティ製品の政府調達の実施に関する通知（財庫〔2010〕48号））
http://cgzx.jgj.sh.gov.cn:8090/new_web/2004_year/yuandi/peixun/fagui/2013-10.htm

[24]关于信息安全产品认证制度实施要求的公告（国家认监委2010年第26号公告）（情報セキュリティ製品認証システムの実施要件に関する公告（認証認可局 2010年第26号））
http://www.cnca.gov.cn/zl/qzxcprz/mlmsyjd/202007/t20200715_59750.shtml

[25]关于发布<网络关键设备和网络安全专用产品目录（第一批）的公告（国家网信办 工信部、公安部、国家认监委公告 2017年第1号）（重要なネットワーク機器およびネットワークセキュリティ特別製品カタログ（初回）」のリリースに関する公告（インターネット情報局、工業情報化部、公安部、国家認証認可監督管理委員会 2017年第1号））
https://www.isccc.gov.cn/zxyw/cprz/wlgjsb/tzgg/2018/07/891612.shtml

[26]关于发布承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录（第一批）的公告（国家认监委 工业和信息化部 公安部 国家互联网信息办公室2018年第12号）（安全認証・安全検査業務を実施する組織の一覧（初回）についての公告（国家認証認可監督管理委員会、工業情報化部、公安部、国家インターネット情報局 2018年第12号）
https://www.isccc.gov.cn/zxyw/cprz/wlgjsb/tzgg/2018/06/891506.shtml

[27]认监委关于发布网络关键设备和网络安全专用产品安全认证实施规则的公告（转发国家认监委公告2018年第28号）（重要なネットワーク機器および特別なネットワークセキュリティ製品の安全認証の実施規則の発行に関する国家認証認可監督管理委員会の公告（国家認証認可監督管理委員会 2018年第28号））
https://www.isccc.gov.cn/zxyw/cprz/wlgjsb/tzgg/2018/07/891611.shtml

[28]国务院关于取消和调整一批行政审批项目等事项的决定（国发〔2015〕11号）（行政承認項目およびその他の事項の一括廃止および調整に関する国務院の決定（国発〔2015〕11号））
http://www.gov.cn/zhengce/content/2015-03/13/content_9524.htm

[29]国务院关于取消非行政许可审批事项的决定（国发〔2015〕27号）（非行政許可承認事項の決定取り消しに関する国務院の決定（国発〔2015〕27号））
http://www.gov.cn/zhengce/content/2015-03/13/content_9524.htm

[30]国家密码管理局关于调整行政审批事项公开目录的通知（管理承認項目の公開カタログの調整に関する国家暗号管理局の通知）
http://www.sca.gov.cn/sca/xwdt/2015-06/01/content_1002353.shtml

[31]国务院关于取消一批行政许可事项的决定（国发〔2017〕46号）（行政許可項目の一括取り消しに関する国務院の決定（国発〔2017〕46号））
http://www.gov.cn/zhengce/content/2017-09/29/content_5228556.htm

[32]国家密码管理局关于做好商用密码产品生产单位审批等 4 项行政许可取消后相关管理政策衔接工作的通知（国密局字 〔2017〕336号）（商用暗号製品生産ユニットの承認を含む 4 つの管理ライセンスの廃止後の管理政策の継続に関する国家暗号管理局の通知（国家秘密局 2017年第336号））
http://www.sic.gov.cn/News/91/8562.htm

[33]国家密码管理局关于废止和修改部分管理规定的决定(国家密码管理局公告 第32号)（特定の行政規則の廃止と変更に関する国家暗号管理局の決定（国家暗号管理局 第32号））
http://www.jsmm.gov.cn/smcms/gsgg/54904.jhtml

[34]国家密码管理局 市场监管总局 关于调整商用密码产品管理方式的公告 第39号
(商用暗号製品の管理方法の調整に関する公告（国家暗号管理局、国家市場監督管理総局 第39号)
http://nca.zj.gov.cn/art/2019/12/30/art_1475643_41566020.html

[35]《商用密码产品认证目录（第一批）》《商用密码产品认证规则》的公告 市场监管总局 国家密码管理局公告2020年第23号
(「商用暗号製品の認証カタログ(初回)」および「商用暗号製品の認証規則」の公告(国家市場監督管理総局、国家暗号管理局 2020年第23号))
http://www.gov.cn/zhengce/zhengceku/2020-05/11/content_5510753.htm

[36]中华人民共和国国家情报法（中華人民共和国の国家情報法）
http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml

[37]公安部关于《网络安全等级保护条例（征求意见稿）》 公开征求意见的公告（公安部2018年6月27日）（サイバーセキュリティ等級保護規制（意見募集草案）（公安部2018年6月27日））
http://www.djbh.net/webdev/web/HomeWebAction.do?p=getGzjb&id=8a818256641b29b90164409250320021

[38]网络安全审查办法(国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局令2020年4月13日第6号）（サイバーセキュリティレビュー方法（中国国家ネットワーク情報弁公室、その他11組織による命令2020年第6号））
http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

[39]国家互联网信息办公室关于《数据安全管理办法（征求意见稿）》公开征求意见的通知

（国家互联网信息办公室 2019 年 5 月 28 日）（国家インターネット情報局の「データセキュリティ管理措置（意見集草案）」の公告（インターネット情報局 2019 年 5 月 28 日））
http://www.cac.gov.cn/2019-05/28/c_1124546022.htm

[40]国家互联网信息办公室关于《个人信息出境安全评估办法（征求意见稿）》公开征求意见的通知（国家互联网信息办公室 2019 年 6 月 13 日）（国家インターネット情報局の「個人情報国外移転の安全性評価法（意見募集草案）」の公告（インターネット情報局 2019 年 6 月 13 日））
http://www.cac.gov.cn/2019-06/13/c_1124613618.htm

[41]商务部关于印发全面深化服务贸易创新发展试点总体方案的通知（商服贸发〔2020〕165 号）（サービス貿易の革新的と発展のための試行の包括的深化の全体計画の通知（商服貿発〔2020〕165 号））
http://www.gov.cn/zhengce/zhengceku/2020-08/14/content_5534759.htm

[42]中国人民银行关于《中华人民共和国中国人民银行法（修订草案征求意见稿）》公开征求意见的通知（「中華人民銀行に関する中華人民共和国法（意見募集草案）」に関する公開協議に関する中華人民銀行の通知）
http://www.gov.cn/zhengce/zhengceku/2020-10/24/content_5553847.htm

[43]中国人民银行 中央网信办 工业和信息化部 工商总局 银监会 证监会 保监会关于防范代币发行融资风险的公告 （中国人民銀行中央サイバースペース産業情報技術局、産業情報技術省、中国銀行監督管理委員会、中国証券監督管理委員会、中国保険監督管理委員会の広告）
http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html

[44]区块链信息服务管理规定（国家互联网信息办公室令 2019 年第 3 号）（ブロックチェーン情報サービス管理規定（インターネット情報局 2019 年第 3 号））
http://www.cac.gov.cn/2019-01/10/c_1123971164.htm

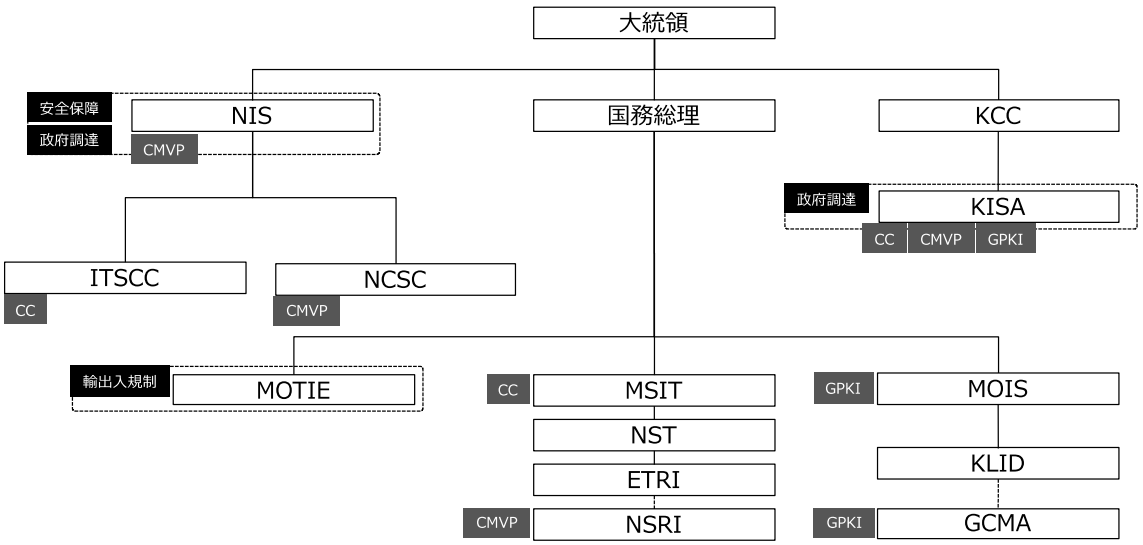
3.8. 韓国

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・組織に力が注がれている。一方で、法改正や組織改変が極めて頻繁に行なわれており、状況の変化へいち早く対応できる反面、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は、大統領直属の情報機関である NIS（National Intelligence Service、国家情報院）と、KISA（Korea Internet and Security Agency、韓国インターネット振興院）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 3-16 である。



ETRI: 電子通信研究院
GCMA: 行政電子署名認証管理センター
ITSCC: IT セキュリティ認証事務局
KCC: 放送通信委員会
KISA: 韓国インターネット振興院
KLID: 韓国地域情報開発院,
MOIS: 行政安全部（旧 MOI:行政自治部, MoSPA: 安全行政部）

MOTIE: 産業通商資源部
MSIT: 科学技術情報通信部
NCSC: 国家サイバーセキュリティセンター
NIS: 国家情報院
NSRI: 国家安全保障技術研究所
NST: 国家科学技術研究会

図 3-16 韓国における暗号政策に係る組織体制

暗号及びセキュリティ政策に関する組織の中で主要なものについて、その役割を以下に示す。

- NIS（National Intelligence Service、国家情報院）
  大統領直属に設置された情報機関であり、国の安全保障に関わる情報の収集や公開、サイバー攻撃の予防や対応、サイバーセキュリティ政策の計画・調整などを職務範囲とする。NIS の組織や職務は国家情報院法[8]、サイバーセキュリティに関する業務は保安業務規定[9]で定めされている。
  NIS は、暗号・セキュリティに関する以下の認証制度の保護基準の策定や評価・認定機関としての業務を行う。
  - KCMVP（韓国版 CMVP）の制度・基準策定
  - セキュリティ適合性検証（政府調達）の制度策定、認証・試験機関
  - セキュリティ機能試験（政府調達）の制度策定、認証機関

- KISA（Korea Internet and Security Agency、韓国インターネット振興院）
  インターネットの振興、安全な利用の促進、国際協力・海外進出の推進を目的に設立された公共機関であり、情報通信網利用促進及び情報保護等に関する法律第 52 条を根拠法とする。KISA の役割は極めて多岐に渡るが、暗号や情報セキュリティに関する業務に以下のようなものがある。
  - MSIT と共同で情報セキュリティに関するガイドラインを作成
  - 情報保護製品評価・認証制度（CC）の評価機関
  - 暗号モジュール試験（KCMVP）の試験機関
  - セキュリティ機能試験（政府調達）の試験機関
  - クラウドセキュリティ認証制度（CSAP）の認証・評価機関
  - IoT セキュリティ認証制度（IoT-SAP）の認証・評価機関

- MSIT（Ministry of Science and ICT、科学技術情報通信部）
  科学技術政策や科学技術の研究開発に関わる業務を行う行政機関。暗号や情報セキュリティに関して以下の業務を行う。
  - KISA と共同で情報セキュリティ等に関するガイドラインの作成
  - CC の制度・基準策定
  - クラウドセキュリティ認証制度（CSAP）の制度・基準策定
  - IoT セキュリティ認証制度(IoT-SAP)の制度・基準策定

- MOIS（Ministry of the Interior and Safety、行政安全部）（旧 行政自治部（MOI）、安全行政部（MoSPA））
  国、政府、電子政府の管理、地方自治の促進などを行う中央行政機関。暗号や情報セキュリティに関する業務として、政府電子認証基盤（GPKI）の制度・基準策定を行う。
  2014 年 11 月に MoSPA から MOI へ、2017 年 7 月に MOIS へ改編された。

- MOTIE（Ministry of Trade, Industry and Energy、産業通商資源部）
  商業、貿易、工業、外国人投資、産業技術研究開発政策、エネルギー・地下資源輸出入を所管する行政機関。

- ETRI（Electronics and Telecommunications Research Institute、電子通信研究院）
  情報、通信、電子、放送の分野の基盤技術の研究開発を行う研究機関。セキュリティ機能試験（政府調達）の試験機関である。

- NCSC（National Cyber Security Center、国家サイバーセキュリティセンター）
  NIS の下に設置された KCMVP の認証機関。

- NSRI（National Security Research Institute、国家安全保障技術研究所）
  国の安全保障システムやサイバーセキュリティ技術の研究開発などを行う研究所。国家情報セキュリティに関する業務を行う研究機関であるため詳細は不明。KCMVP の試験機関である。

- ITSCC（IT Security Certification Center、IT セキュリティ認証事務局）
  CC 認証機関であり、認証に関する業務の他、CCRA 関連活動も行う。

- GCMA（Government Certification Management Authority、行政電子署名認証管理センター）
  政府電子認証基盤 GPKI の Root CA であり、GPKI の運用を行うとともに、下位の認証局の評価・認定を行う。

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 3-34 と図 3-17 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。

表 3-34 韓国における暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	上位政策・戦略	国家サイバーセキュリティ管理規定[1]	NIS、政府機関	更新無

2	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[2]	KISA	後継
3		知能情報化基本法（旧:国家情報化基本法)[3]	KISA	後継
4		電子文書と電子取引基本法（旧:電子取引基本法)[4]	KISA	後継
5		個人情報保護法[5]、個人情報保護法施行令[6]	MOIS、KISA	後継、後継
6		電子署名法[7]	MOIS、KISA	後継
7		国家情報院法[8]	NIS	更新無
8	暗号利用	保安業務規定[9]	NIS	後継
9	輸出入規制	対外貿易法[10]、対外貿易法施行令[11]、戦略物資輸出入告示[12]	MOTIE	後継、後継、後継
10	政府調達	電子政府法[13]	NIS、MOIS, KISA、GCMA	後継
11		電子政府法施行令[14]、電子文書保管などの標準業務準則[15]	MOIS	後継、ー
12	標準・基準	暗号アルゴリズムと鍵長の利用ガイドライン[16]	KISA、MSIT	後継
13		個人情報の暗号化措置ガイドライン[17]	KISA、MSIT	後続
14		量子コンピューティング環境における暗号技術利用ガイドライン[18]	MSIT、KISA	ー
15	その他	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[19]	MSIT、KISA	ー

図 3-17　韓国における暗号関連政策マップ

- 国家サイバーセキュリティ管理規定[1]
  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。2005 年 1 月に制定（大統領訓令第 141 号）。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

る国家サイバーセキュリティ戦略会議（議長：国家情報院長、委員：関連省庁の次官や次官級公務員）を置く（第 6 条）と共に、サイバーセキュリティセンターを置き、国家サイバーセキュリティ政策の立案、国家サイバーセキュリティマニュアル（非公開）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（第 8 条）。また各省庁は所管の情報通信網を保護する責任をもつ（第 9 条）。
なお、2014 年度調査の後、改正は行われていない。

- 情報通信網利用促進及び情報保護等に関する法律（情報通信網法）[2]
情報通信網の利用促進、利用者の保護、安定性の確保等について定めた法律。1987 年 1 月施行。KISA を設置し、その事業として、情報通信網の利用と保護等のための法令・政策・制度の調査と研究、情報保護認証・評価等の実施およびサポートを含む多数を指定（第 52 条）。KISA の前身である情報保護振興院の事業に暗号技術の開発が含まれていたが、2009 年 7 月の改正で除かれている。
なお、2014 年度調査の後、暗号に関係がある部分の改正はない。

- 知能情報化基本法（旧: 国家情報化基本法）[3]
2020 年 6 月に国家情報化基本法から全部改正。AI 技術などを活用した知能情報化社会の実現のための政策樹立・推進を目的とする。情報保護に関して、政府は暗号技術の開発と利用の促進、暗号技術を利用し知能情報サービスの安全を図る措置を講じなければならない（第 57 条②）。また、MSIT は情報保護システムの性能や信頼性の基準を策定し､情報保護システムの製造･輸入者にその基準を守ることを勧告できる(第 58 条)。これに基づきは CC 認証制度が実施されている。

- 電子文書と電子取引基本法（電子文書法）（旧: 電子取引基本法）[4]
電子文書と電子取引の法的関係を明確化し、安全性・信頼性を確保、利用促進基盤の造成を目的とした法律。暗号に関して、「電子取引事業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。」（第 14 条①）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、平文や暗号技術へのアクセスに必要な措置を行うことができる。」（第 14 条②）としている。
なお、2014 年度調査の後、暗号に関係がある部分の改正はない。

- 個人情報保護法[5]、個人情報保護法施行令[6]
個人情報保護法は、個人情報の処理と保護について包括的に定め、個人を一意に識別する固有識別情報の処理、住民登録番号の保管の際の安全確保に、暗号化措置の実施を求める。また、個人情報保護法施行令は、個人情報の転送の際の暗号化もしくは同等の措

置を求める。
2014 年度調査の後、個人情報保護法、施行令共に管理の厳格化、被害救済・制裁の強化等の改正が繰り返し行われている。

- 個人情報の暗号化措置ガイドライン[17]
  MOIS､KISA が公開する､個人情報保護における暗号技術の利用に関するガイドライン。法令、暗号アルゴリズム、情報の転送・保存時に使用する暗号化方式、鍵管理方法等について広く解説し、個人情報を扱うシステムの構成に合わせた適切な暗号化措置について説明する。
  2017 年 1 月の改定で、暗号アルゴリズム別の安全性、暗号鍵の管理、暗号化の導入手順と事例紹介等が追加された。

- 電子署名法[7]
  電子文書の安全性と信頼性を確保、利用の有効化を目的として、電子署名に関する基本的事項を定めている。この法令に基づき、民間の電子署名認証基盤（NPKI）を利用した公認認証制度が実施されている。
  2020 年 10 月、全部改正により公認認証制度を廃止、新たに電子署名認証業務評価・認定制度を導入し、民間中心の制度へ変更された。
  これについて、3.8.4.2 節に記載する。

- 国家情報院法[8]
  NIS の組織と職務範囲等を定める法律。NIS の職務範囲を国家安全保証に関わる国内外の情報の収集、国家機密を保護、行政機関のサイバーセキュリティ対策、情報セキュリティ業務の企画・調整等と規定している（第 4 条）。
  2021 年 1 月に全部改正され、政治中立性の維持、国家安全保障を促進するものとなっている。

- 保安業務規定[9]
  国家情報院法に基づき、NIS のセキュリティ業務遂行に必要な事項を定める。秘密の保護、国家安全保障施設や国の保護装置の保護、中央行政機関のセキュリティ監査等について定めており、秘密の保護に関して、秘密の重要性や価値に基づく区分方法、暗号資材と呼ばれる秘密保護のための装置や手段の開発・管理、秘密や暗号機材の取り扱い方等を定めている。
  なお、2014 年度調査の後の改正で、秘密管理の効率性向上、秘密の管理強化、暗号資材の取り扱いや管理の厳格化等が行われている。

- 対外貿易法[10]、対外貿易法施行令[11]、戦略物資輸出入告示[12]
  対外貿易における公正な取引の秩序の確立、国際収支の均衡と通商の拡大を目的とした法律。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を含む。産業通商資源部より戦略物資輸出入告示として二重用途品目、軍用物資品目リストが公表される。
  なお、2014 年度調査の後、暗号に関係がある部分の改正・改定はない。
  これについて、3.8.3.4 節に記載する。

- 電子政府法[13]
  行政業務の電子的処理のための基本原則・手順・推進方法などを定める。国民向けの電子サービスのセキュリティ対策や情報通信網などのセキュリティ対策の樹立・施行を求める。行政の電子署名の認証業務遂行に関する規定があり（第 29 条②）、これに基づき行政機関向けの電子署名認証基盤（GPKI）が運用されている。
  なお、2014 年度調査の後、暗号に関係がある部分の改正はない。

- 電子政府法施行令[14]、電子文書保管などの標準業務準則[15]
  電子政府法施行令は電子政府法の関連事項を規定する。行政機関に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、NIS に、これらの保安機能や適合性の規格を定める権限を与える（第 69 条）。これに基づき KCMVP 制度が実施されている。
  電子文書保安措置施行指針は、電子文書と電子取引基本法に基づき公認電子文書センターの業務の具体的規則を定め、セキュリティ対策（第 3 章）に関する規定を含む。
  2014 年度調査報告書で参照していた「電子文書保安措置施行指針」は参照できなかった。
  いずれも 2014 年度調査の後、暗号に関係がある部分の改正・改定はない。

- 暗号アルゴリズムと鍵長の利用ガイドライン[16]
  KISA、MSIT が 2019 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。
  2018 年 12 月の改定で、国内推奨暗号アルゴリズムの情報が更新された。
  これについて、3.8.3.1 節に記載する。

- 量子コンピューティング環境における暗号技術利用ガイドライン[18]
  MSIT、KISA が 2017 年 12 月に公開した推奨耐量子計算機暗号を示したガイドライン。
  量子コンピューティング環境における推奨耐量子計算機暗号アルゴリズムだけでなく、量子コンピュータの特徴の紹介、国内・国外の量子情報通信技術の研究の現状、現代暗号の安全性、耐量子計算機暗号活用事例とオープンソースのライブラリ、耐量子計算機暗号公開鍵暗号アルゴリズムについても説明している。

これについて、3.8.4.1 節に記載する。

- 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（クラウドコンピューティング法）[19]
  クラウドコンピューティングの発展と利用の促進、サービスの安全な利用環境の確保を目的として 2015 年 9 月より施行されている法律。
  MSIT は 3 年ごとに基本計画を策定・実施し（第 5 条）、クラウドコンピューティングの発展を計画的に進める事、クラウドコンピューティングサービスの品質・性能・情報保護基準を MSIT が策定しプロバイダに従わせること（第 23 条）、事故や障害発生時の通知（第 25 条）や、利用者情報の同意の無い第三者提供や目的外利用は禁止（第 27 条）等による信頼性向上と利用者保護等を定めている。
  これについて、3.8.3.7 節に記載する。

3.8.3. 暗号に関わる各種制度、規制及びガイドライン

3.8.3.1. 利用すべき暗号方式

KISA、MSIT は「暗号アルゴリズムと鍵長の利用ガイドライン」を公開し、推奨暗号アルゴリズムを示すとともに、暗号アルゴリズムと鍵長の選定に関する基準や事例紹介などを行っている。また、KISA が実施する暗号モジュール試験制度（KCMVP）の試験対象とされている暗号アルゴリズムも利用が推奨されていると考えられる。これらをまとめた結果は表 3-35 となる。

韓国の国産暗号は国内・国際規格として標準化されている（表 3-36）。

また、国家サイバーセキュリティ管理規定に基づき NIS が策定している「国家サイバーセキュリティマニュアル」に政府機関が使用すべき暗号等に関する記載があることが窺えるが、非公開資料のため確認できない。

表 3-35 韓国の推奨暗号アルゴリズム（2018 年 12 月）

区分	アルゴリズム
ブロック暗号	SEED、HIGHT、ARIA、LEA
ハッシュ関数	SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224(※)、SHA-512/256(※)、SHA3-224、SHA3-256、SHA3-384、SHA3-512、LSH-224、LSH-256、LSH-384、LSH-512、LSH-512-224、LSH-512-256
鍵共有	DH、ECDH
公開鍵	RSAES
電子署名	RSA-PSS、KCDSA、ECDSA、EC-KCDSA

※ 暗号アルゴリズムと鍵長の利用ガイドラインにのみ記載 KCMVP の対象に含まれていない。

表 3-36　韓国の国産暗号アルゴリズムの業界・国家・国際標準一覧

区分	業界標準	国内標準	国際標準
ARIA	－	KS X 1213-1、KS X 1213-2	－
SEED	TTAS.KO-12.0004/R1	KS X ISO/IEC 18033-3	ISO/IEC 18033-3:2010
LEA	TTAK.KO-12.0223	KS X 3246	ISO/IEC 18033-3:2010/DAMD 1
HIGHT	TTAS.KO-12.0040/R1	KS X ISO/IEC 18033-3	ISO/IEC 18033-3:2010
LSH	－	KS X 3262	－
KCDSA	TTAK.KO-12.0001/R4	KS X ISO/IEC 14888-3	ISO/IEC 14888-3:2008
EC-KCDSA	TTAK.KO-12.0015/R3	KS X ISO/IEC 14888-3	ISO/IEC 14888-3:2008

3.8.3.2.　セキュリティ製品認証制度・セキュリティサービス認証制度

韓国における暗号に関する試験・認証制度は「情報保護製品評価・認証制度（CC）」、「暗号モジュール試験・認証制度（KCMVP）」の 2 つあり、また、情報セキュリティに関して「セキュリティ機能試験制度」、「IoT セキュリティ認証制度（IoT-SAP）」等が実施されている。

- 情報保護製品評価・認証制度（CC）[136]

  韓国は、2006 年 5 月にコモンクライテリア承認アレンジメント(CCRA: Common Criteria Recognition Arrangement）に加盟しており、NIS の下に設置されている ITSCC が情報保護システムの評価・認証指針（KECS: Korea Evaluation and Certification Scheme）の認証機関となっている。KISA は評価機関の一つに指定されている。

  法的根拠は以下の通り。

  - 知能情報化基本法第 58 条（情報保護システムに関する基準告示等）
  - 知能情報化基本法施行令第 51 条（情報保護システムに関する基準告示等）
  - 情報保護システムの共通の評価基準（未来創造科学部告示第 2013-51 号）
  - 情報保護システムの評価・認証指針（科学技術情報通信部告示第 2017-7 号）
  - 情報保護製品評価・認証の実行規定（科学技術情報通信部・IT セキュリティ認証事務局 2017-9-12）

[136] https://itscc.kr/
認証製品一覧: https://itscc.kr/certprod/list.do?product_class=1

- 暗号モジュール試験・認証制度（KCMVP）[137]

  韓国では、暗号モジュール試験・認証制度（KCMVP: Korean Cryptographic Module Validation Program）が実施されている。米国・カナダで実施されている CMVP (Cryptographic Module Validation Program)と同様の制度で、認証機関は NIS 下に設置されている NCSC、試験機関は NSRI 及び KISA となっている。NSRI は公的機関向け、KISA は民間向けの評価機関である。

  法的根拠は以下の通り。

  - 電子政府法第 56 条（情報通信網などのセキュリティ対策樹立・施行）
  - 電子政府法施行令第 69 条（電子文書の保管・流通関連のセキュリティ対策）
  - 暗号モジュール試験及び試験の手順（行政自治部告示第 2004-45 号）

  また、セキュリティ要件、試験要件は以下の通り。

  - KS X ISO/IEC 19790：2015（暗号モジュールのセキュリティ要件）
  - KS X ISO/IEC 24759：2015（暗号モジュール試験要件）

- セキュリティ機能試験制度[138]

  セキュリティ機能試験制度は、情報保護システム及びネットワーク機器などの IT 製品について、NIS が定める「国のセキュリティ要件」に基づき安全性を確認する制度であり、CC 認証制度に比べ、セキュリティ適合性検証手続きが簡素化されている。認証機関は NSRI、試験機関には KISA、ETRI などが含まれる。

- IoT セキュリティ認証制度（IoT-SAP）[139]

  KISA は、IoT 製品及び、それと連携するモバイルアプリケーションの安全性の検証制度 IoT-SAP を実施している。人々の生活の中で身近に利用されている IoT 製品に内在するセキュリティ上の問題を解消し、安全性を確保することを目的としている。

  MSIT が策定した制度の下で、KISA が試験・評価・認定を行う。対象の IoT 機器は種類に応じて Lite、Basic、Standard に区分され、いずれも、認証、暗号、データの保護、プラットフォームの保護、物理的な保護についての試験・評価を行う。試験・検査項目数は合わせて最大 40 件程度となっている。認証の有効期限は設けられていない。

  認定基準についての解説書や、その他の資料は、IoT-SAP に関する Web ページで公開されている。

---

[137] https://www.nis.go.kr:4016/AF/1_7_3_1.do
https://seed.kisa.or.kr/kisa/kcmvp/EgovSummary.do
認証暗号モジュール一覧: https://www.nis.go.kr:4016/AF/1_7_3_3/list.do

[138] https://www.nis.go.kr:4016/AF/1_7_2_2/list.do

[139] https://www.ksecurity.or.kr/kisis/subIndex/307.do

これらの試験・認証制度について、所管、認証機関、評価機関、認証件数を表 3-37 にまとめた。

表 3-37　韓国の認証制度と関連する機関

	CC	KCMVP	セキュリティ機能試験制度	IoT-SAP
所管	MSIT	NIS	NIS	MSIT
認証機関	ITSCC	NIS	NSRI	KISA
評価機関	KISA 韓国システム保証(KoSyAs) 韓国安全保障評価院(KSEL) 韓国情報セキュリティ技術院(KOIST) 韓国情報通信技術委員会(TTA) 韓国機械電気電子試験研究院(KTC)	NSRI, KISA	KISA 韓国システム保証(KoSyAs) 韓国安全保障評価院(KSEL) 韓国情報セキュリティ技術院(KOIST) 韓国情報通信技術協会(TTA) 韓国機械電気電子試験研究院(KTC) 韓国産業技術試験院(KTL) 韓国電子通信研究院(ETRI)	KISA
認証件数	2020 年 84 件 2019 年 74 件 2018 年 56 件	2020 年 17 件 2019 年 11 件 2018 年 18 件	不明	2020 年 40 件 2019 年 35 件 2018 年 7 件

CC, KCMVP の認証件数の値は認定日により分類

CC の認証件数は「国内向け認証」と「CCRA 向け認証」の合計

MSIT の認証件数は KISA の発表による（2020 年は、12 月第 1 週までの値）

なお、調査時点（2021 年 2 月）の CCRA 向けの有効な CC 認証取得は、41 製品である。以下に認証取得と EAL を示す。

表 3-38　EAL ごとの Common Criteria 認証取得数（韓国）[140]

EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	N※	Total
7	0	3	3	0	0	0	1	0	5	0	0	0	22	41

※N(None)：EAL の表記がない認証である。

[140] Certified Products List - Statistics : New CC Portal https://www.commoncriteriaportal.org/products/stats/

3.8.3.3. 政府の調達要件

政府調達において、暗号に関連する調達要件を定める根拠は、電子政府法第 56 条、電子政府法施行令第 69 条におかれている。

これらは、行政機関に電子文書の保管や流通にあたり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。この権限に基づき、NIS は「セキュリティ適合性検証」制度を実施している。

セキュリティ適合性検証制度[141]は、国家情報院法第 4 条及び電子政府法第 56 条に基づき実施されている制度であり、国や公共機関が情報保護システム及びネットワーク機器を導入後、NIS によるセキュリティ適合性検証を受ける事を義務付け、その過程で発見された脆弱性を排除した後に運用を開始するというものである。ここで導入する情報保護システム及びネットワーク機器は、CC 認証もしくは「セキュリティ機能試験」の認定の取得が求められる。また、CC の保護プロファイルの中で、KCMVP 認証済み暗号モジュールやアルゴリズムの利用を求めている。セキュリティ機能試験のプロファイルは参照することができなかった。

3.8.3.4. 暗号の輸出入規制

韓国における輸出入管理は産業通商資源部が所管し、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監視、規制が行われている。

暗号に関する輸入規制は行われず、輸出に関してワッセナー・アレンジメントに基づいた規制が行われている。規制対象は、デュアルユース品目リストとして戦略物資輸出入告示により公開される。

2021 年 2 月時点のリストは、デュアルユース管理リスト、機密リスト、特別な機密リストから構成され、2019 年 12 月のワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）」のなかのデュアルユース製品・技術に関するリストにほぼ対応して作られている（参考：3.1.3.4 節のワッセナー・アレンジメント）。そのなかで、デュアルユース管理リストのカテゴリ 5 パート 2（Category 5 Part 2 - “INFORMATION SECURITY”）をベースに、輸出規制対象となる暗号製品を定めている。その概要は以下のようなものとなっている。

- データの機密性確保のために、後に示す要件を満たす暗号アルゴリズムを使用し、暗号機能が、安全な「暗号アクティベーション」以外の手段で、利用できるようにされるかアクティベートされている、あるいはアクティベートすることができる以下の製品

[141] https://www.nis.go.kr:4016/AF/1_7_2_1.do

- 情報セキュリティを主な機能とする製品
- デジタル通信、ネットワークシステム、機器、コンポーネント
- コンピュータ、情報保存・処理を主な機能等する製品、コンポーネント
- 後に示す要件を満たす暗号アルゴリズムがデータの機密性確保のために利用され、暗号製品の主機能以外をサポートし、独立型の組込機器もしくはソフトウェアとして動作する製品

- 暗号アクティベーショントークン
- 量子暗号（量子鍵配送）を利用または実行する機器
- 暗号を利用した超広帯域無線通信機器
- 暗号を利用した拡散コードを用いたスペクトラム拡散装置

- 暗号アルゴリズムの要件
  - 共通鍵暗号アルゴリズム: 鍵長 56 ビット以上
  - 公開鍵暗号アルゴリズム:
    - 因数分解ベース: 512 ビット以上
    - 有限体の乗法群における離散対数ベース: 512 ビット以上
    - 上記以外の群上の離散対数ベース: 112 ビット以上
  - 耐量子計算機暗号アルゴリズム
    - 格子の最短ベクトル・最近ベクトル問題ベース
    - 超特異楕円曲線の同種写像問題ベース
    - ランダム符号の復号問題ベース

なお、マスマーケット品等は管理対象外とされている。

2021 年 2 月時点のデュアルユース管理リストのカテゴリ 5 パート 2 が、2019 年 12 月のワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト」のなかのデュアルユース製品・技術に関するリストのカテゴリ 5 パート 2（Category 5 – Part 2 "Information Security"）（米国の 3.1.3.4 節参照）とほぼ一致することを確認した。

3.8.3.5. プロトコル等での暗号方式

暗号通信プロトコルの安全な運用のための設定ガイライン等の文書は見つけることができなかった。

3.8.3.6. 暗号利用に関する規制（利用ライセンス・暗号盗聴法など）

韓国は、暗号の利用を規制していない。

電子文書と電子取引基本法の第 14 条（暗号製品の使用）②「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、平文や暗号技術へのアクセスに必要な措置を行うことができる。」の規定から、暗号化された情報に対する政府によるアクセスが可能となっている。

3.8.3.7. クラウドサービス

韓国では、クラウドコンピューティングの発展と利用者保護に関する法律（クラウドコンピューティング法）が施行されている。

この中で、MSIT が 3 年ごとに基本計画を策定し、実施することが定められている（第 5 条）。MSIT は以下の文章を策定・公開し、これに基づいた政策によりクラウドコンピューティングの発展が計画的に進められている。なお、これらの文章は見つけることができなかった。

- 第 1 回クラウドコンピューティングの基本計画('16～'18)
- 第 2 回クラウドコンピューティングの基本計画('19～'21)

また、MIST は、クラウドコンピューティングサービスの品質・性能・情報保護基準のレベルを向上させるため、基準を策定し、プロバイダに守らせることを勧告できる（第 23 条）と定められている。これに基づき、MIST は以下の基準を策定・公開し、KISA を評価・認証機関としてクラウドセキュリティ認証制度（CSAP: Cloud Security Assurance Program）[142] を実施している。

- クラウドコンピューティングサービス情報の保護に関する基準[20]
- クラウドコンピューティングサービスの品質・性能に関する基準[21]

CSAP はクラウドサービスの安全性評価・認定制度であり、MSIT が定めた検査・試験の基準に従い、KISA が評価・認定を行う。クラウドサービスの種類により IaaS, DaaS, SaaS（標準/簡単）の 4 種類に区分され、いずれも管理的・物理的・技術的保護対策及び公共機関特有のセキュリティ要件について、合わせて 100 件程度の項目が含まれる。

認証の有効期間は 5 年（SaaS の簡単検証は 3 年）であり、期間中は毎年 1 度の事後調査を受け、期間中に更新評価を受ける事で有効期間を延長できる。

この制度を利用し発行された証明書は、制度が開始された 2016 年から 2020 年の 5 年間の間に 27 件で、執行せず維持されているものは 26 件となっており、2019 年に利用数が少ないことが指摘されている [143]。

---

[142] https://isms.kisa.or.kr/main/csap/intro/index.jsp

[143] 「ミンウォンギ次官『中小企業の負担を減らすクラウドセキュリティ認証制度を検討』 実効性の低い制度を国政監査で指摘、改善の意志を明らかに」ZDNet Korea 2019 年 10 月 15 日 https://zdnet.co.kr/view/?no=20191015112229

3.8.3.8. 暗号資産

暗号資産を規制する法律として、以下の法律が施行されている。

- 特定の金融取引情報の報告および利用などに関する法律[22]

資金洗浄行為や脅迫資金調達行為の規制のための金融取引情報の報告・利用などについて定めており、2020 年 5 月の改正で、暗号資産に関する規制が追加された。これにより仮想資産事業者は金融委員会(FSC)[144]の規制を受けることとなった。

この法律は、仮想資産事業者は、FSC へ代表者名・住所等の申告（7 条）、不法疑いのある取引や高額取引の報告（第 4 条、第 4 条の 2）、また、取引の記録の保有（第 4 条の 4）、顧客ごとに取引記録を分離して管理（第 8 条）等を義務付けている。

また、銀行等の金融機関は、顧客が仮想資産事業者である場合、資金管理体制、システムのセキュリティ認証取得状況、不法疑いのある取引防止体制等を確認し、不適切と判断した場合は口座開設の拒否や終了を行うことができるとしている（第 5 条②）。

3.8.3.9. 電子署名法

韓国の電子署署名法は、1999 年 7 月に施行された法律であり、電子署名を定義し、紙の上の署名・捺印等と同等の効力を持つと定め、電子証明書と認証機関についても規定している。

2020 年 10 月に全部改正され、証明書の認証機関に関する仕組みが大きく変更された。

改正以前の電子署名法には、公認認証局と呼ばれる国や地方自治体の機関の組織が管理する認証局と、それが発行する公認認証書についての規定があり（第 2 章、第 3 章）、それらに基づき、政府公認の民間向けの電子認証基盤（NPKI）が運用されていた。

全部改正は、この公認認証局・公認認証書に関する規定を削除し、新たに、MSIT が電子署名認証業務運用基準を定め（第 7 条②）、電子署名認証事業者の評価・認定制度（第 8 条①）及び認定機関を KISA とする規定（第 9 条）が追加された。この改正により、NPKI は廃止となり、民間の電子署名認証サービスへ移行することとなった。公認認証書制度が市場独占をもたらしていることが改正の理由として挙げられている。

また、この改正で「国は、生体認証、ブロックチェーンなど、さまざまな電子署名手段の利用活性化のために努力しなければならない。」（第 6 条）という条文が追加された。

民間による様々な技術とサービスに基づいた認証手段の提供、信頼性の向上、サービス選択の幅の拡大が期待される。

3.8.3.10. 国民 ID 番号制度（eID）

韓国では全ての国民に固有の住民登録番号が割り振られており、17 歳以上の国民に発給

[144] FSC: Financial Services Commission http://www.fsc.go.kr/

される住民登録証に氏名や生年月日等と共に記載されている。この住民登録証は電子化されておらず、eID として利用されていない。

韓国では電子署名法に基づいた公的な電子証明書が、ネット上のサービスにおいて身分証明書として利用されてきた。しかし 2020 年 10 月の電子署名法全部改正で根拠となる規定が削除され、公的な電子証明書制度は廃止され、民間が提供する電子署名認証サービスへと移行することとなった。2021 年 2 月時点では、新たサービスの開始は確認されていない。

2020 年 6 月より、韓国の通信 3 社（SK テレコム、KT、LGU+）と警察庁による、モバイル運転免許確認サービスの運用が開始された。携帯端末に専用アプリケーションを導入し、生体認証による本人確認と運転免許書を撮影することで登録でき、本来の運転免許書と同様に身分証明書としても利用可能となっている。規制サンドボックスと呼ばれる新たな技術やサービスのテストのための制度の下で実験的に実施されており、今後の展開は不明である。

3.8.4. その他

3.8.4.1. 耐量子計算機暗号

KISA は 2017 年 12 月「量子コンピューティング環境における暗号技術利用ガイドライン」を公開し、推奨される耐量子計算機暗号アルゴリズムを紹介している。取り上げられているアルゴリズムを表 3-39 に示す。なお、ガイドラインは耐量子計算機暗号アルゴリズムの出典を示していない。

表 3-39 韓国の推奨耐量子計算機暗号アルゴリズム

種類	耐量子計算機暗号アルゴリズム
多変数多項式ベース	Gui、HFE、Rainbow、UOV、ZHFE
符号ベース	MCPC-McEliece、McBits、McEliece、Modern McEliece、Niederreiter、QC-MDPC、Wild McEliece
格子ベース	BLISS、LWE-Frodo、NTRU、NTRU Prime、New Hope、SS-NTRU
同種写像ベース	Diffie-Hellman-like protocol、SIDH
ハッシュベース	HORS、SPHINCS、W-OTS、W-OTS+、XMSS

また、各種類から代表的なアルゴリズムを一つ選び、推奨パラメータを示している（表 3-40、表 3-41、表 3-42、表 3-43、表 3-44）。

表 3-40　韓国で推奨される耐量子計算機暗号 Rainbow のパラメータ

セキュリティ強度	推奨パラメータ (v, o_1, o_2)	鍵長(ビット)
80	(21, 20, 20)	312,115
112	(29, 28, 28)	838,041
128	(33, 32, 32)	1,241,907
192	(36, 24, 24)	1,471,283
256	―	―

表 3-41　韓国で推奨される耐量子計算機暗号 QC-MDC McEliece のパラメータ

セキュリティ強度	推奨パラメータ (n0, n, r, w, t)	鍵長(ビット)
80	(2, 9602, 4801, 90, 84)	4,801
	(3, 10779, 3595, 153, 53)	7,186
128	(2, 1974, 9857, 142, 134)	9,857
	(3, 22299, 7433, 243, 85)	14,866
256	(2, 65542, 32771, 274, 264)	32,771
	(3, 67593, 22531, 465, 167)	45,062

表 3-42　韓国で推奨される耐量子計算機暗号 NTRU のパラメータ

セキュリティ強度	推奨パラメータ (N, p, q)	鍵長(ビット)
112	ees401ep2: (401, 3, 2048)	4,411
128	ees439ep1: (439, 3, 2048)	4,829
192	ees593ep1: (593, 3, 2048)	6,523
256	eex743ep1: (743, 3, 2048)	8,173

表 3-43　韓国で推奨される耐量子計算機暗号 SIDH のパラメータ

セキュリティ強度	推奨パラメータ ($p=l_A^a, l_B^b, f\pm1$)	鍵長(ビット)
123	$p=2^{251}3^{155}5-1$	1,996
189	$p=2^{382}3^{238}79-1$	3,073

表 3-44　韓国で推奨される耐量子計算機暗号 SPHINCS のパラメータ

セキュリティ強度	推奨パラメータ (n, m, h, d, w, t, k)	鍵長(ビット)
128	(256, 512, 60, 12, 16, 2^{16}, 32)	2,144

3.8.4.2.　公開鍵認証基盤

韓国には NPKI（民間認証基盤, National PKI）と GPKI（政府認証基盤, Government PKI）との 2 つの公開鍵基盤があり、これらから発行された電子証明書がオンライン上で ID とし

て利用されてきた。

NPKI は一般市民向けの認証基盤であり、電子署名法（2020 年 10 月改正以前の第 25 条）を法的根拠とし、MSIT が制度を定め、KISA の電子署名認証管理センター[145]がルート認証局を運営し、システムの構築や運用、関連サービスの運営を行なってきた。証明書は公認認証書と呼ばれ、公認認証機関もしくは金融機関で申請することで発行された。2020 年 10 月電子署名法が全部改正され、NPKI は廃止された。

GPKI は政府機関向けの認証基盤であり、電子政府法第 29 条②及び電子政府法施行令第 28 条を法的根拠とし、MOIS の下、KLID の GCMA[146]がルート認証局を勤め、システムの運用、サービスの運営を行っている。証明書は行政電子署名証明書と呼ばれ、KLID の情報認証部へ申請することで GCMA より発行される。

[145] https://www.rootca.or.kr/kor/main.jsp
[146] https://gcert.gpki.go.kr/main/PreMainAction.action

3.8.5. 韓国の参照文献

[1] 국가사이버안전관리규정（대통령훈령 제316호）（国家サイバーセキュリティ管理規定（大統領訓令第316号））
https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2000000100482

[2] 정보통신망 이용촉진 및 정보보호 등에 관한 법률（정보통신망법）（情報通信網利用促進及び情報保護等に関する法律（情報通信網法））
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=218937

[3] 지능정보화 기본법（知能情報化基本法）
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=218737

[4] 전자문서 및 전자거래 기본법（전자문서법）（電子文書と電子取引基本法（電子文書法））
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=218883

[5] 개인정보 보호법（個人情報保護法）
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=213857

[6] 개인정보 보호법 시행령（個人情報保護法施行令）
https://www.law.go.kr/lsInfoP.do?lsiSeq=220409

[7] 전자서명법（電子署名法）
https://www.law.go.kr/lsInfoP.do?lsiSeq=218885

[8] 국가정보원법（国家情報院法）
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=224235

[9] 보안업무규정（保安業務規定）
https://www.law.go.kr/lsInfoP.do?lsiSeq=220563

[10]대외무역법（対外貿易法）
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=213853

[11]대외무역법시행령（対外貿易法施行令）
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=223713

[12]전략물자 수출입고시（戦略物資輸出入告示）
http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000190108

[13]전자정부법（電子政府法）
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=225099

[14]전자정부법 시행령（電子政府法施行令）
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=223831

[15]전자문서보관등 표준업무준칙（電子文書保管などの標準業務準則）
https://www.law.go.kr/LSW/admRulLsInfoP.do?admRulSeq=2100000099395

[16]암호 알고리즘 및 키 길이 이용 안내서（暗号アルゴリズムと鍵長の利用ガイドライン）
https://kisa.or.kr/public/laws/laws3_View.jsp?mode=view&b_No=259&d_No=82
[17]개인정보 암호화 조치 안내서（個人情報の暗号化措置ガイドライン）
https://kisa.or.kr/public/laws/laws3_View.jsp?mode=view&b_No=259&d_No=78
[18]양자컴퓨팅 환경에서의 암호기술 이용 안내서（量子コンピューティング環境における暗号技術利用ガイドライン）
https://kisa.or.kr/public/laws/laws3_View.jsp?mode=view&b_No=259&d_No=96
[19]클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률（클라우드컴퓨팅법）（クラウドコンピューティングの発展と利用者保護に関する法律（クラウドコンピューティング法））
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=218773
[20]클라우드컴퓨팅서비스 정보보호에 관한 기준（クラウドコンピューティングサービス情報の保護に関する基準）
https://www.law.go.kr/LSW//admRulLsInfoP.do?admRulSeq=2100000095223
[21]클라우드컴퓨팅서비스 품질·성능에 관한 기준（クラウドコンピューティングサービスの品質・性能に関する基準）
https://www.law.go.kr/LSW//admRulLsInfoP.do?admRulSeq=2100000095957
[22]특정 금융거래정보의 보고 및 이용 등에 관한 법률（특정금융정보법）（特定の金融取引情報の報告および利用などに関する法律（特定の金融情報法））
https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=228209

3.9. オーストラリア

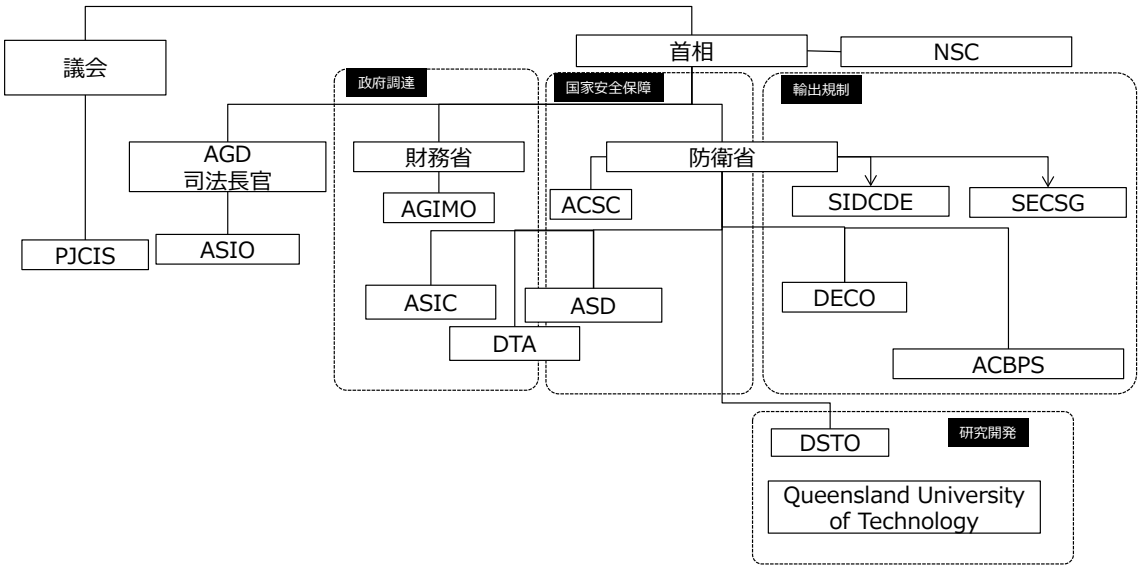
オーストラリアにおいては、国防省傘下の ASD（Australian Signals Directorate）が、暗号政策の主導的な役割を担っている。ASD は、暗号の要件を含む政府システム要件の Information Security Manual（ISM)、製品認証制度 AISEP（Australasian Information Security Evaluation Program)、政府セキュリティフレームワーク Protective Security Policy Framework（PSPF）を所管すると共に、輸出規制を所管する DECO（Defense Export Control Office)、政府調達を所管する AGIMO（Australian Government Information Management Office）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 3-18 である。

なお、2014 年度調査以降の変化として、DTA、ASIC、AGD を追加した。



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）
DTA：Australian Government Digital Transformation Agency（デジタル変換庁）
ASIC：Australian Securities and Investments Commission（オーストラリア証券投資委員会）
AGD：Australian Government Attorney-General's Department（司法省）

図 3-18　暗号政策に係る組織体制（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（Australian Signals Directorate、オーストラリア信号局）[147]
  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（National Security Committee of Cabinet、内閣国家安全保障委員会）
  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（Australia's national security intelligence service、オーストラリア国家安全諜報サービス）[148]
  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。

147 http://www.asd.gov.au/about/index.htm
148 http://www.asio.gov.au/About-ASIO/Overview.html

- DECO（Defense Export Control Office、防衛輸出規制室）[149]
  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（Strengthened Export Controls Steering Group、強化輸出規制推進グループ）
  2015 年 5 月に廃止されたグループである。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活動していた。SECSG の活動は、DECO が行政執行を所管していた。SECSG が廃止後は、DECO が継続して、産業省と協議、ステークホルダーとのネットワークの確立を行っている。

- SIDCDE（Standing Interdepartmental Committee on Defense Exports、防衛輸出省庁横断常設委員会）
  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である。

- AGIMO（Australian Government Information Management Office、オーストラリア政府情報管理室）[150]
  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（Parliamentary Joint Committee on Intelligence and Security、国会諜報セキュリティ統合委員会）[151]
  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を監視する。Intelligence Services Act 2001 にその役割が規定されている。

- 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）[152]
  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

[149] http://www.defence.gov.au/DECO/AboutUs.asp
[150] http://www.finance.gov.au/agimo/
[151] http://www.aph.gov.au/pjcis
[152] http://www.asd.gov.au/infosec/acsc.htm

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[153]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（Defense Science and Technology Organization、防衛科学技術局）
  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（Australian Customs and Border Protection Service、オーストラリア関税国境防衛サービス）
  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。

- DTA（Australian Government Digital Transformation Agency、デジタル変換庁）
  政府のデジタルサービスの推進、改善、支援を行う。政府サービスを設計に関するデジタルサービス規格、政府サービスをオンラインで利用ためのデジタルアイデンティティ及び信頼できるデジタルアイデンティティフレームワークを推進している。

- ASIC（Australian Securities and Investments Commission、オーストラリア証券投資委員会）
  Australian Securities and Investments Commission Act 2001 基づいて設立したオーストラリア証券投資委員会であり、ライセンスが必要となるオーストラリアの金融サービス（Australian financial services：AFS）のライセンス発行機関である。

- AGD（Australian Government Attorney-General's Department、司法省）
  オーストラリアの法律を維持、改善し、オーストラリア政府の弁護士を通じて、法的助言や連邦への法的サービスを提供している。

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 3-45 と図 3-19 である。

[153] 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 3-45　オーストラリアにおける暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	上位政策・戦略	Cyber Security Strategy, 2020 サイバーセキュリティ戦略	ASD	後継
2	暗号政策・設置法	Intelligence Services Act 2001 (Includes amendments up to: Act No. 88, 2020) インテリジェンスサービス法	Australian Government	更新有
3		Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 電気通信およびその他の法律改正(支援とアクセス)法案 2018	連邦議会	―
4		ELECTRONIC TRANSACTIONS ACT 1999 1999 年電子取引法	法務省、連邦議会	―
5	輸出入規制	Customs Act 1901 1901 年税関法（基本法/根拠法）	防衛省、ACBPS	更新有
6		Defense Trade Controls Act 2012 2012 年防衛貿易管理法（米豪軍事協力）	防衛省	更新無
7		Customs (Prohibited Exports) Regulations 1958, 13E 税関（輸出禁止）規則 1958、13E	防衛省	更新有
8		Defence and Strategic Goods List 2019	DECO	後継
9		Australian Export Controls and ICT	防衛省	―
10	政府調達	Crimes Act 1914, Criminal Code 1995	AGD	更新有、更新有
11		Directive on the security of Government business 政府事業の安全に関する指令	AGD	更新無
12		Protective Security Policy Framework (PSPF) 保護セキュリティポリシーフレームワーク (PSPF)	AGD	更新無
13	標準・基準	Australasian Information Security Evaluation Program(AISEP) Policy Manual (August 2011) オーストラリアの情報セキュリティ評価プログラム	ASD	更新無
14		ASD Cryptographic Evaluation (ACE)	ASD	更新無
15		Australian Government Information Security Manual (ISM) (December 2020)	ASD	後継
16		Guidelines for Cryptography (December 2020)	ASD	―
17		Cybercrime Act 2001 / Crimes Act 1914	法執行機関	更新有／更新無
18		Cloud Security Guidance	ASD	―
19		Trusted Digital Identity Framework (TDIF)	DTA	―
20	その他	Initial coin offerings and crypto-assets	ASIC	―

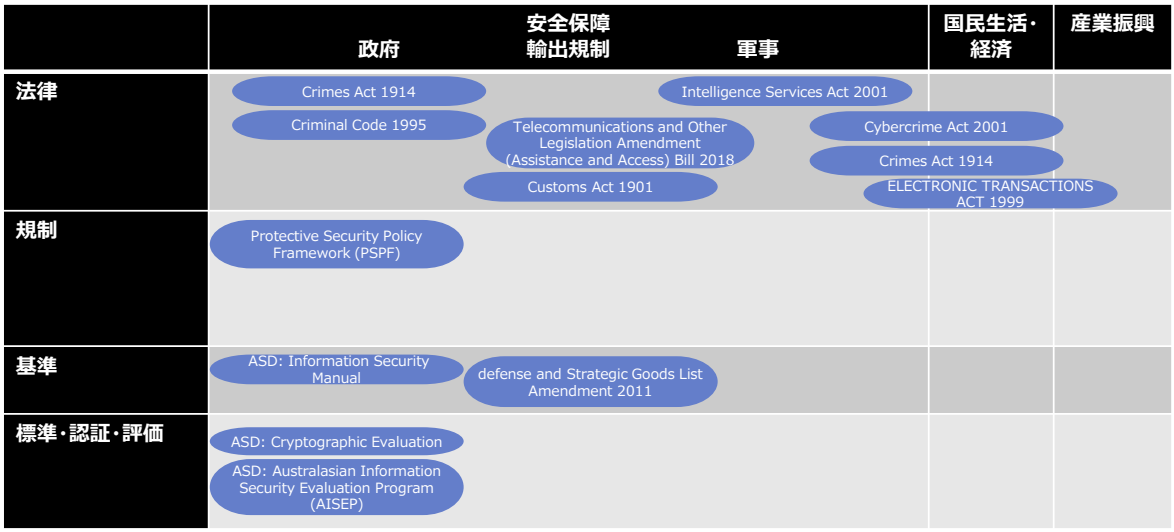


図 3-19　暗号に関連した政策マップ（オーストラリア）

- Cyber Security Strategy, 2020[1]
  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。特に、法執行機関がサイバー犯罪の減少に取組むため、ダークウェブと暗号化技術による匿名性に取り組む能力の強化が必要であり、オーストラリア政府は、法執行機関がダークウェブを含むサイバー犯罪を捜査し、阻止するための権限と能力を確保するために取り組むことを挙げている。

- Intelligence Services Act 2001[2]
  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。

  なお、2014 年度調査以降の変更点としては、法令に基づく ADS の設置・管理、及び ADS 事務局長に関する行政の規程、ADS 従事者の詳細規則等を追加している。

- Customs Act 1901（根拠法）[5]／Defense Trade Controls Act 2012（米豪軍事協力）[6]／Customs (Prohibited Exports) Regulations 1958, 13E[7]／Defense and Strategic Goods List Amendment 2011
  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 節にまとめる。

なお、2014 年度調査以降に更新したものは、Customs Act 1901（根拠法）と Customs (Prohibited Exports) Regulations 1958, 13E であり、Defense and Strategic Goods List Amendment 2011 は廃止している。
Customs Act 1901（根拠法）については、2014 年度調査以降に、関税、輸出に関する詳細項目の変更があり、Customs (Prohibited Exports) Regulations 1958, 13E については、液化天然ガスを追加しているが、暗号技術や暗号製品に関する変更はない。また、Defense Trade Controls Act 2012 は 2014 年度調査以降に変更及び更新は見当たらない。

- Crimes Act 1914, Criminal Code 1995[9]
  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。
  なお、2014 年度調査以降の変更として、Crimes Act 1914 は犯罪者に関連した身分証明の保持および開示等の行動に関する変更、Criminal Code 1995 は会計処理の虚偽に関する変更があったが、暗号技術や暗号製品に関する変更は見当たらない。

- 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。
  なお、Directive on the security of Government business は 2014 年度調査以降に変更及び更新は見当たらない。

- Protective Security Policy Framework（PSPF）[154]
  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。
  なお、PSPF は 2014 年度調査以降に変更及び更新は見当たらない。

- AISEP Policy Manual[10]
  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。
  なお、2014 年度調査以降で変更があることに留意されたい。詳細は 3.9.3.2 節にて記載する。

[154] https://www.protectivesecurity.gov.au/

- Information Security Manual[12]
  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。
  なお、2014 年度調査以降で変更があることに留意されたい。詳細は 3.9.3.1 節にて記載する。

- ASD Cryptographic Evaluation[11]
  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。
  なお、2014 年度調査以降で変更があることに留意されたい。詳細は 3.9.3.1 節にて記載する。

- 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。
  なお、Cybercrime Act は 2014 年度調査以降に変更及び更新は見当たらない。

3.9.3. 暗号に関わる各種制度、規制及びガイドライン

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）[12]
  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。

- Guidelines for Cryptography (DECEMBER 2020)[13]
  上記の ISM の構成文書の 1 つである Guidelines for Cryptography において、ASD 認可暗号アルゴリズム（ASD Approved Cryptographic Algorithms）（表 3-46）、ASD 認可暗号プロトコル（ASD Approved Cryptographic Protocol、AACP）、鍵交換などについて規定している。なお、3-key Triple DES の利用はオプションであり、AES の利用が推奨されている。

表 3-46　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 ビット）
	3-key Triple DES
ハッシュ関数	SHA-2（SHA-224, SHA-256, SHA-384, SHA-512）

また、Guidelines for Cryptography では、保護する情報を SECRET と TOP SECRET に分け、利用する暗号アルゴリズムと鍵長を定めている。なお、暗号アルゴリズムと鍵長については、Commercial National Security Algorithm（CNSA）Suite との相互運用性を確保するために、推奨するアルゴリズムと鍵長を優先することを記載している。

表 3-47　ASD 認可暗号アルゴリズム及び鍵長の詳細

目的	アルゴリズム	Approved for SECRET	Approved for TOP SECRET	Recommended
暗号化	AES	AES-128 AES-192 AES-256	AES-256	AES-256
ハッシュ関数	SHA-2	SHA-256 SHA-384 SHA-512	SHA-384 SHA-512	SHA-384
デジタル署名	ECDSA	NIST P-256 NIST P-384 NIST P-521	NIST P-384 NIST P-521	NIST P-384
	RSA	3072 ビット鍵以上	3072 ビット鍵以上	3072 ビット鍵
鍵交換	DH	3072 ビット鍵以上	3072 ビット鍵以上	3072 ビット鍵
	ECDH	NIST P-256 NIST P-384 NIST P-521	NIST P-384 NIST P-521	NIST P-384
	RSA	3072 ビット鍵以上	3072 ビット鍵以上	3072 ビット鍵

3.9.3.2.　セキュリティ製品認証制度・セキュリティサービス認証制度

セキュリティ認証制度については、AISEP（Australasian Information Security

Evaluation Program)、暗号製品に限定した認証制度として ASD cryptographic evaluation がある。

- 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。

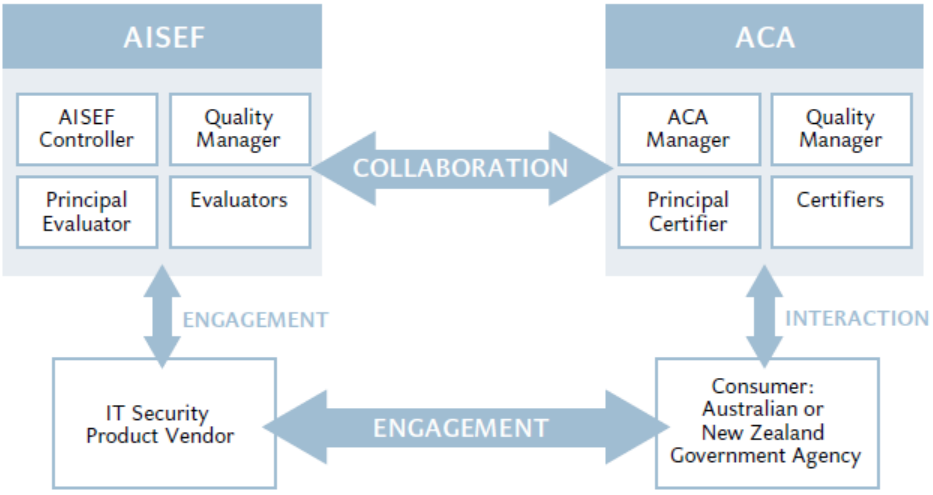


図 3-20　AISEP の関係組織

(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 3-20)。
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。

ACA は、Common Criteria Web サイトにリストされているすべての collaborative

Protection Profile を承認し、さらに、AISEP 内での評価のために ACA によっても承認されている以下の Protection Profile がある。

表 3-48　AISEP 内評価のための Protection Profile

Protection Profile	Version	Published
PP-Module for Virtual Private Network (VPN) Gateways (Mod_VPNGW_v1.1)	V1.1	2020-07-01
PP-Module for Virtual Private Network (VPN) Gateways (Mod_VPNGW_v1.0)	V1.0	2019-11-22
Extended Package VPN Gateway (GW EP)	V2.1	2017-06-15
Extended Package Intrusion Prevention Systems (IPS EP)	V2.11	2017-03-08
Extended Package MACsec Ethernet Encryption (MACSEC EP)	V1.2	2016-05-10

なお、AISEP で CC 認証を取得した製品はすべて CCRA に登録しており、調査時点（2021 年 2 月）の有効な CC 認証取得は、32 製品である。以下に認証取得と EAL を示す。

表 3-49　EAL ごとの Common Criteria 認証取得数（オーストラリア）[155]

EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6+	EAL7	N※	Total
0	0	5	6	0	0	0	0	0	0	0	0	21	32

※N(None)：EAL の表記がない認証である。

- ASD Cryptographic Evaluation[11]

  ASD は、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い、その結果を AISEP として公開している。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。

  さらに、3.9.3.7 節に示すクラウドサービス、3.9.3.10 節に示す The Trusted Digital Identity Framework（TDIF）においても ASD 認証暗号アルゴリズム及び ASD 認証暗号プロトコルの利用を求めている。

  なお、認証取得製品は、表 3-49 に示した通りである。

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

[155] Certified Products List - Statistics : New CC Portal https://www.commoncriteriaportal.org/products/stats/

Protective Security Policy Framework（PSPF）がある。前述の 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いる。

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。規制対象となる暗号製品等は、ワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）」のなかのデュアルユース製品・技術に関するリストのカテゴリ 5 パート 2（Category 5 - Part 2 “Information Security”）がベースになっている。（参考：3.1.3.4 節のワッセナー・アレンジメント）

また、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 2019[8]
  2014 年度調査に記載した Defence and Strategic Goods List Amendment 2011 (No.1) では、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たが、2019 年発行の Defence and Strategic Goods List 2019 では、同項目の情報セキュリティ（システム、機器およびコンポーネント）の規制対象である Authentication、Digital signature に加え、Data integrity、Non-repudiation、Digital rights management 等が追加された。また、規制対象の暗号の条件を以下に示す。
  - パリティビットを含まず鍵長 56 ビットを超える対称アルゴリズム
  - 鍵長 512 ビットを超える素因数分解に基づく非対称アルゴリズム（RSA 等）
  - 鍵長 512 ビットを超える離散対数に基づく非対称アルゴリズム（DH 等）
  - 上記以外の鍵長 112 ビットを超える離散対数に基づく非対称アルゴリズム(ECDH 等)

- Australian Export Controls and ICT[19]
  7.4「情報セキュリティ」においてシステム、試験、検査、生産設備において規制対象として以下が規定されている。
  - デジタル技術を採用した暗号化及び復号するように設計または変更するもの。
  - 量子暗号を使用または実行するように設計または変更するもの。

3.9.3.5. プロトコル等での暗号方式

ASD 認可暗号プロトコル（ASD Approved Cryptographic Protocol）[14]を規定している。ASD 認可暗号プロトコルで利用する暗号アルゴリズム及び鍵長は、基本的には ASD 認可暗号アルゴリズム（ASD Approved Cryptographic Algorithms）に限定している。以下に、ASD 認可暗号プロトコルとして定めているプロトコルと ASD 認可暗号アルゴリズム以外で規定している暗号アルゴリズム及び鍵長を示す。

- Transport Layer Security（TLS）
  - AES in Galois Counter Mode の利用
  - Anonymous DH の利用禁止
- Secure Shell（SSH）
- Secure/Multipurpose Internet Mail Extension（S/MIME）
- Open PGP Message Format
- Internet Protocol Security（IPsec）
  - HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 の利用
- Wi-Fi Protected Access 2（WPA2）

3.9.3.6. 暗号利用に関する規制（利用ライセンス・反暗号法・暗号盗聴法など）

暗号の利用を規制していない。一方、Telecommunications and Other Legislation Amendment（Assistance and Access）Bill 2018[3]において警察機関や国家安全保障機関が暗号通信の内容を読み取れるように定めた法律を制定している。

3.9.3.7. クラウドサービス

2020 年発行の Cloud Security Guidance[15]には、情報セキュリティ登録査定プログラム（Information Security Registered Assessors Program、IRAP）によって、クラウドサービスの関係組織、クラウドサービスプロバイダー（CSP）及びクラウドサービスの評価手法を示し、組織のデータ処理に対するリスクに基づいてサービスを選択することを解説している。また、同ガイダンスのクラウドサービスプロバイダー向けの分冊である Cloud Computing Security for Cloud Service Providers、テナント向けの分冊である Cloud Computing Security for Tenants には、ASD 承認暗号機能のサポートを求める項目がある。

3.9.3.8. 暗号資産

Australian Securities and Investments Commission（ASIC）が初期コインオファリングと暗号資産について情報シート（INFO 225）[18]を発行し、関係者に掛かる規制、規制ガイド、関連法等（会社法、ASIC 法、オーストラリア消費者法、マネーロンダリング防止法（AML）、顧客（KYC）の義務）、及びトークンなどの暗号資産を発行者が保持すべき金融サービスラ

イセンス（Australian financial services licence、AFSL）について解説している。なお、同情報シートには、暗号アルゴリズム及び鍵長の記述はない。

3.9.3.9. 電子署名法

ELECTRONIC TRANSACTIONS ACT 1999[4]において連邦法によって課せられる電子署名の要件を定義している。この要件は、電子署名を利用するために、書面で情報を提供する要件、署名を提供するための要件、文書を作成するための要件、情報を記録するための要件、文書を保持するための要件という5つであり､アルゴリズムや鍵長についても記載はない。

3.9.3.10. 国民ID番号制度（eID）

Australian Government Digital Transformation Agency[16]が、The Trusted Digital Identity Framework（TDIF）においてフレームワークを構成する13のポリシーを定め､TDIF認定（TDIF accredited）を実施している。このポリシーにはISMに規定されたASD認証暗号アルゴリズムとASD認証暗号プロトコルを利用が義務付けられている。

また、これらのフレームワークを利用し、政府サービスにアクセスするためのMyGov[17]を提供している。MyGovは他の住民制度とは関係なく、税務関連、保険制度等の各種の政府機関サービスにアクセスするためのアカウントである。

表 3-50 TDIFのドキュメント構成

ドキュメント分類	No	ドキュメント名称
Governance documents	1	01 - Glossary of Abbreviations and Terms
	2	03 - Accreditation Process
	3	06D - Attribute Profile
Requirements documents	4	04 - Functional Requirements
	5	05 - Role Requirements
	6	06 - Federation Onboarding Requirements
	7	06B - OpenID Connect 1.0 Profile
	8	06C - SAML 2.0 Profile
	9	07 - Annual Assessment
Guidance documents	10	02 - Overview
	11	04A - Functional Guidance
	12	05A - Role Guidance
	13	06A - Federation Onboarding guidance

3.9.4. その他

3.9.4.1. 量子コンピュータの進展に伴う対応策

ASD Approved Cryptographic Algorithms において NSA 発行の CNSA Suite 及び Quantum Computing の FAQ を参照[156]している。

[156] https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm.

3.9.5. オーストラリアの参照文献

[1] Cyber Security Strategy, 2020
https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

[2] Intelligence Services Act 2001 (Includes amendments up to: Act No. 88, 2020)
https://www.legislation.gov.au/Details/C2020C00300

[3] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018
https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195

[4] ELECTRONIC TRANSACTIONS ACT 1999
http://www6.austlii.edu.au/cgi-bin/viewdb/au/legis/cth/consol_act/eta1999256/

[5] Customs Act 1901
https://www.legislation.gov.au/Details/C2018C00379/Download

[6] Defense Trade Controls Act 2012

[7] Customs (Prohibited Exports) Regulations 1958, 13E
https://www.legislation.gov.au/Details/F2017C00597/Download

[8] Defence and Strategic Goods List 2019
https://www.legislation.gov.au/Details/F2019L00424

[9] Crimes Act 1914, Criminal Code 1995
https://www.legislation.gov.au/Details/C2017C00297/Download

[10]Australasian Information Security Evaluation Program AISEP Policy Manual (August 2011)
https://www.cyber.gov.au/acsc/view-all-content/programs/australasian-information-security-evaluation-program

[11]ASD Cryptographic Evaluation Program
https://www.cyber.gov.au/acsc/view-all-content/programs/australasian-information-security-evaluation-program

[12]Australian Government Information Security Manual (December 2020)
https://www.cyber.gov.au/acsc/view-all-content/ism
https://www.cyber.gov.au/sites/default/files/2020-12/Australian%20Government%20Information%20Security%20Manual%20%28December%202020%29.pdf

[13]Guidelines for Cryptography (December 2020)
https://www.cyber.gov.au/sites/default/files/2020-12/22.%20ISM%20-%20Guidelines%20for%20Cryptography%20%28December%202020%29.pdf

[14]ASD Approved Cryptographic Protocols

https://www.cyber.gov.au/acsc/view-all-content/guidance/asd-approved-cryptographic-protocols
[15]Cloud Security Guidance
https://www.cyber.gov.au/acsc/government/cloud-security-guidance
[16]Trusted Digital Identity Framework (TDIF)
https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework
[17]MyGov
https://my.gov.au/mygov/content/html/about.html
[18]Initial coin offerings and crypto-assets
https://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-crypto-assets/
[19]Australian Export Controls and ICT
https://cecs.anu.edu.au/sites/default/files/staff/announcement/australian_export_controls_and_ict.pdf

3.10. EU (European Union、欧州連合)

欧州では、2016 年に施行された eIDAS(Electronic Identification and Trust Services)規則により、「デジタル単一市場」の構築のため、欧州全域で電子署名等のトラストサービスの法制化および標準化とデジタル ID の相互承認が図られている。

一方、テロ、サイバー犯罪は激化しており、End-to-end の暗号化における加害者の追跡困難性が懸念されている。また、量子コンピューティングにより、トラストサービスの基礎を為す現在の暗号技術の危殆化の恐れも予想されており、対策が検討されている。

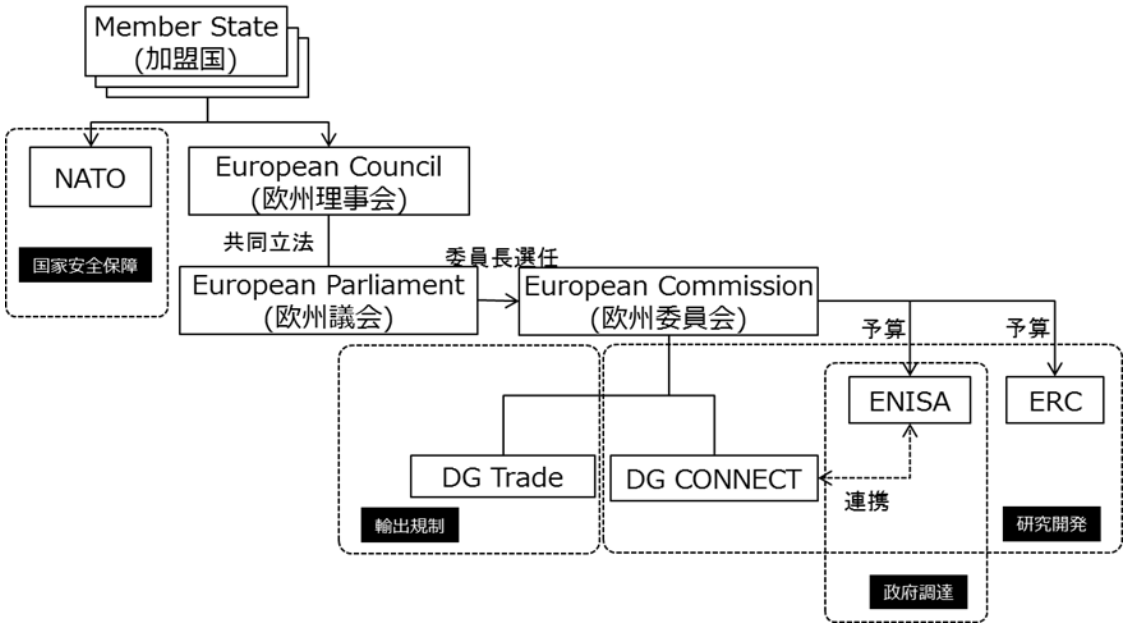
3.10.1. 暗号に関わるセキュリティ政策に関する組織体制・役割

欧州のサイバーセキュリティ政策は、EU（European Union、欧州連合）により設立された諮問機関 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)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、Directorate General 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 DG CONNECT や EU 研究ファンディング機関である ERC（European Research Council、欧州研究会議）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（North Atlantic Treaty Organization、北大西洋条約機構）が関連する。

図 3-21 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。



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 3-21　暗号政策に係る組織体制（EU）

- EC（European Commission、欧州委員会）
  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（EU：European Union）の政策執行機関である。政策分野ごとに総局（DG：Directorate General）が設置され政策執行を行う。
  - DG CONNECT（Directorate General CONNECT、通信ネットワーク・コンテンツ&技術総局）[157]
    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（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）
  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 2004 年に設立された機関である。ENISA は、任期が定められた、他の EU 機関と比較して、予算、人員が少ない小さな機関であったが、2019 年のサイバーセキュリティ法（Regulation（EU）2019/881）により、EU サイバーセキュリティ庁（EU Agency for Cybersecurity）として恒久的な権限を与えられた。これにより ENISA は、認証スキームの技術的根拠を準備し、ヨーロッパのサイバーセキュリティ認証フレームワークを構築および維持する上で重要な役割を果たす。また、EU レベルでの協力体制を強化し、サイバーセキュリティインシデントの支援を求める EU 加盟国を支援し、大規模な国境

[157] http://ec.europa.eu/dgs/connect/who-we-are

を越えたサイバー攻撃や危機に際して EU 加盟国間の調整をサポートすることを義務付けられている。
2019 年の年間予算は、約 1700 万ユーロ(約 21.42 億円)[158]で、欧州委員会の一般予算、ギリシャ共和国政府からの家賃補助金、および ENISA の活動に参加している第三国からの寄付により構成されている。

- ERC (European Research Council、欧州研究会議) [159]
  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。

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 3-51 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 [1]
  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。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- The EU's Cybersecurity Strategy for the Digital Decade [2]
  2020 年 12 月に発表された新しいサイバーセキュリティ戦略。この戦略の目的は、サイバー脅威に対するヨーロッパの集合的な回復力を強化し、すべての市民と企業が信頼できる信頼できるサービスとデジタルツールから完全に利益を得ることができるようにすることである。主要な手段として、次の 3 つが挙げている。
  - レジリエンス、技術的主権およびリーダーシップ
  - 防止、抑止、対応するための運用能力

158 https://www.enisa.europa.eu/about-enisa/accounting-finance

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

➢ グローバルでオープンなサイバースペースを推進するための協力

- Digital Agenda for Europe (DAE) [3]
  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。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- The European Agenda on Security (2015-2020) [4]
  2015 年から 2020 年にかけての安全保障上の脅威に対する EU の効果的な対応を確保するために、欧州委員会が想定している主な行動を定義している。
  緊急行動のための 3 つの優先事項は、(1)オンラインを含むテロリズムへの取り組みと過激化の防止、(2)組織犯罪の撲滅、(3)サイバー犯罪との戦いである。

- The EU Security Union Strategy (2020-2025) [5]
  The European Agenda on Security の後継として欧州委員会が発表した、新たな EU 安全保障連合戦略である。テロリズムや組織犯罪との戦いから、複合的な脅威の防止と検出、重要インフラの回復力の向上、サイバーセキュリティの促進、研究とイノベーションの促進に至るまで、物理的およびデジタル環境におけるセキュリティを確保するために、今後 5 年間に開発されるべきツールと対策を示している。

表 3-51 EU における暗号関連の法律及び政策文書

No	分野	名称	関連組織	前回調査差分
1	上位政策・戦略	EU Cyber Security Strategy - open, safe and secure Cyberspace	EC	更新無
2		The EU's Cybersecurity Strategy for the Digital Decade	EC	—
3		Digital Agenda for Europe (DAE)	EC	更新無
4		The European Agenda on Security (2015-2020)	EC	—
5		The EU Security Union Strategy 2020-2025	EC	—
6	暗号政策・設置法	Cybersecurity Certification: EUCC Candidate Scheme	ENISA	—
7		NIS Directive	EC	—
8		REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)	EC	—

9		The EU cybersecurity certification framework	ENISA	—
10		Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937	EC	—
11		ETSI TR 103 619 V1.1.1 (2020-07) CYBER; Migration strategies and recommendations to Quantum Safe schemes	ETSI	更新無
12		REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	EC	後継
13		The Budapest Convention on Cybercrime: benefits and impact in practice	欧州評議会	—
14		42 COM (2008) 798, COMMUNICATION FROM THE COMMISSION TO THE COUNCIL	欧州議会	更新無
15		EC regulation (EU) No 611/2013	EC	更新無
16		EU Directive 2002/58/EC	EC	更新無
17		EU strategy for a more effective fight against child sexual abuse	EC	—
18	輸出入規制	Council regulation (EC) No. 428/2009 of 5 May 2009	EC	更新有
19	政府調達	Algorithms, Key Sizes and Parameters Report	ENISA	更新無
21	標準・基準	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms	SOGIS	—
22		The use of Cryptographic Techniques on Europe	ENISA	更新無
23		(再掲) Algorithms, Key Sizes and Parameters Report	ENISA	更新無
24	その他	Baseline Security Recommendations for IoT	ENISA	—
25		the Effect of Encryption on Lawful Access to Communications and Data	CSIS	—
26		Quantum Safe Cryptography and Security	ETSI	—

CSIS：Center for Strategic and International Studies
ETSI：European Telecommunications Standards Institute（欧州電気通信標準化機構）
SOGIS：Senior Official Group Information Systems Security

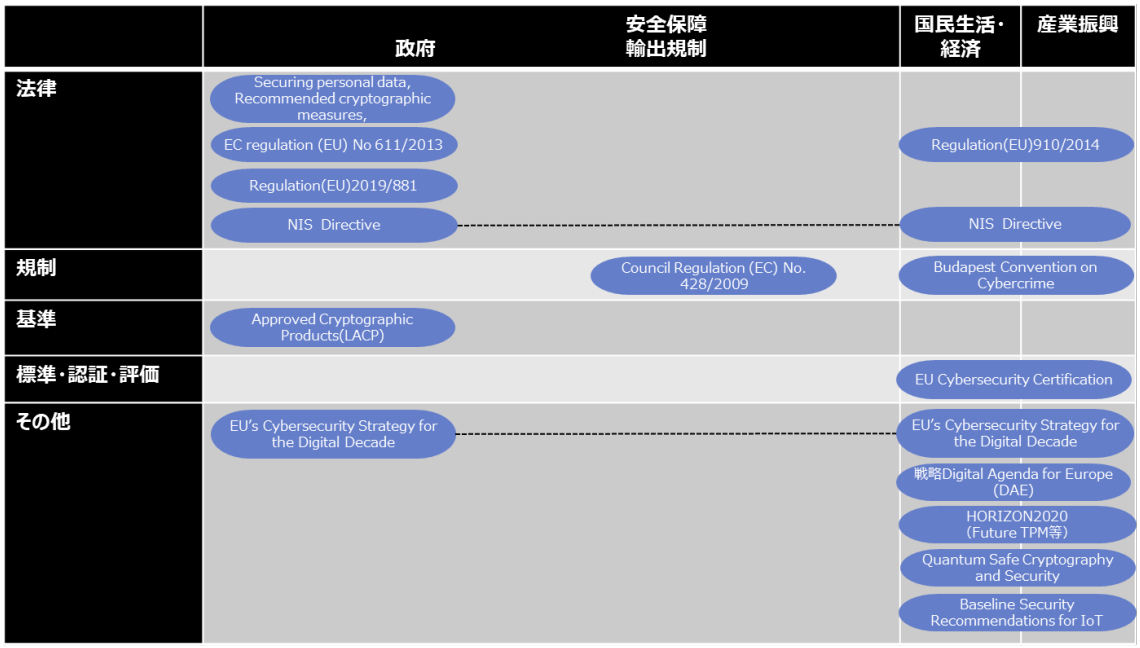


図 3-22　暗号政策に係る政策マップ（EU）

- Cybersecurity Certification：EUCC Candidate Scheme [6]
  サイバーセキュリティ認証：EUCC 候補スキーム。3.10.3.2 節にまとめる。

- NIS Directive（NIS 指令） [7]
  EU サイバーセキュリティ戦略の一環として 2016 年 8 月に発効した EU のネットワークや情報システムのセキュリティに関する指令。EU 指令では、
  - 加盟国の NIS 当局やコンピュータセキュリティー・インシデント・チーム(CSIRT)などを通じたサイバーセキュリティの能力の向上
  - 加盟国間の戦略的協力と情報交換体制の整備
  - 経済や社会に重要なサービス（エネルギー、交通、水、金融、医療など）提供者と、検索エンジン、クラウドコンピューティングサービス、電子商取引などのデジタルサービス提供者（DSP）に適切なセキュリティ対策を講じさせ、サービスに重大な影響を与えるインシデント報告の義務付け

  なお、2020 年 12 月に、NIS Directive の改訂案[160]が提案されている。

[160] https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

- REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 (EU Cybersecurity Act)
  サイバーセキュリティ法（Regulation (EU) 2019/881）は、欧州初の統合されたサイバーセキュリティ認証の枠組み。ENISA の刷新と強化および EU の ICT 製品のセキュリティ認証規格を制定するため、2019 年 6 月 28 日に施行された。

- The EU cybersecurity certification framework [9]
  EU サイバーセキュリティ認証フレームワーク。3.10.3.2 節にまとめる。

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 [10]
  暗号資産の市場に関する欧州議会および理事会の規制の提案、および指令（EU）2019/1937 の修正。3.10.3.8 節にまとめる。

- ETSI TR 103 619 V1.1.1 (2020-07) CYBER; Migration strategies and recommendations to Quantum Safe schemes [11]
  耐量子スキームへの移行戦略と推奨事項。3.10.4.1 節にまとめる。

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [12]
  EU 域内市場における電子取引のための電子識別子およびトラストサービスならびに指令 1999/93/EC の廃止に関する 2014 年 7 月 23 日の欧州議会および理事会規則（EU）No 910/2014（eIDAS 規則）。
  2016 年 7 月に施行された EU 域内の電子商取引を促進するため、eID およびトラストサービスを定めた規則。

- The Budapest Convention on Cybercrime: benefits and impact in practice, 13 July 2020 [14]
  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による利点と影響を説明している。3.10.3.6 節にまとめる。

- EC regulation (EU) No 611/2013[161]
  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

[161] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

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。
なお、2014 年度調査以降に変更及び更新は見当たらない。

- EU strategy for a more effective fight against child sexual abuse [18]
  EU レベルで、包括的に、児童の性的虐待との闘いに効果的な対応を提供することを目的とする戦略。3.10.3.6 節にまとめる。

- Council regulation (EC) No. 428/2009 of 5 May 2009 [19]
  輸出入規制に関するものである。3.10.3.4 節にまとめる。
  なお、2014 年度調査以降に変更があることに留意されたい。詳細は 3.10.3.4 節参照のこと。

- Algorithms, Key Sizes and Parameters Report, 2013 [21] ／Securing personal data. Recommended cryptographic measures
  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 節にまとめる。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [22]
  SOG-IS 参加者が相互に合意した、IT 製品のコモンクライテリアセキュリティ評価の暗号的側面に関連する要求事項と評価手順のセットを示す。
  暗号の開発者、意思決定者、利用者が、どの暗号メカニズムが最新のものであるかを決定するのに役立つ。

- The Use of Cryptographic Techniques in Europe [23]
  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 節にまとめる。
  なお、2014 年度調査以降に変更及び更新は見当たらない。

- Baseline Security Recommendations for IoT [24]
  IoT のベースラインセキュリティの推奨事項。3.10.4.2 節にまとめる。

- the Effect of Encryption on Lawful Access to Communications and Data [25]
  暗号化が法執行機関のデータへのアクセスに与える影響についての報告書。3.10.3.6 節にまとめる。

- Quantum Safe Cryptography and Security, June 2015 [26]
  現在の暗号技術にとって脅威となる量子コンピューティングの攻撃からセキュリティシステムを保護する暗号技術の紹介。3.10.4.1 節にまとめる。

- 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こと
  - 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こと

  なお、2014 年度調査以降に変更及び更新は見当たらない。

3.10.3. 暗号に関わる各種制度、規制ガイドライン

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[162]、ECRYPT[163]、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。

- Algorithms, Key Sizes and Parameters Report, 2013, ENISA
  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 によって公開された最初の文書である。アルゴリズムに関しては、表 3-52 のものが推奨されている。
  本レポートは、ECRYPT、ECRYPT2 の年次レポートを継承するものである。意思決定者向けの技術書で、専門家向けの文書としてまとめている。KU Loeven とブリストル大学の協力によりまとめられた。

[162] The NESSIE project (New European Schemes for Signatures, Integrity and Encryption) (2000-2003)
[163] https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

表 3-52　推奨される暗号アルゴリズム

分類	アルゴリズム
ブロック暗号	AES
	Camellia
ストリーム暗号	Rabbit
	SNOW 3G
ハッシュ関数	SHA-2 (SHA-256, SHA-384, SHA-512)
	SHA-3
	Whirlpool

- The Use of Cryptographic Techniques in Europe [23]
  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。
  政府システム間のデータを公共ネットワークを用いてやり取りする場合に利用すべき暗号技術として表 3-53 のものが挙げられている。

表 3-53　利用すべき暗号

共通要素(技術)	コメント
鍵交換アルゴリズム- Ephemeral Diffie Hellman、RSA 署名スキーム（SHA-2 以上のハッシュ関数）	ECRYPT 推奨に準拠
データ暗号化アルゴリズム - AES-128 又は AES-256	ECRYPT レポートに準拠

3.10.3.2.　セキュリティ製品認証制度・セキュリティサービス認証制度

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）[164]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、

[164] Information Assurance (IA), European Union Classified Information (EUCI)
https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/

EU SECRET、EU CONFIDENTIAL、EU RESTRICTED の 4 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)[165]又は、欧州議会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)又は、欧州議会の事務局長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) [166]により公開されている。認証件数を表 3-54 に示す。

表 3-54 EUCI を保護するための認証された暗号製品件数（2020 年 1 月 13 日時点）

強度レベル	機密区分	認証件数	備考
HIGH	SECRET UE/EU SECRET レベルまでの EUCI を保護する	17	CAA による認可
ENHANCED	CONFIDENTIAL UE/EU CONFIDENTIAL レベルまでの EUCI を保護する	2	CAA の事務局長による認可
STANDARD	RESTREINT UE/EU RESTRICTED レベルまでの EUCI を保護する	60	CAA の事務局長による認可

- EU サイバーセキュリティ認証フレームワーク [167]
  サイバーセキリティ法により、ICT デジタル製品、サービス、およびプロセスの EU 認証フレームワークを確立が図られている。現在、EU には ICT 製品のさまざまなセキュリティ認証スキームが存在するが、EU 全体で有効なサイバーセキュリティ証明書の共通のフレームワークがなければ、欧州単一市場での断片化と障壁のリスクが高まる。
  認証フレームワークは、EU 全体の認証スキームを、包括的なルール、技術要件、標準、および手順のセットとして提供する。
  ENISA は、利害関係者が EUCS 候補スキーム案に関するフィードバックを共有するための公開協議を開始している［9］（2021 年 2 月 7 日まで行われる）。

165 暗号製品認証当局。
166 https://data.consilium.europa.eu/doc/document/ST-5039-2020-INIT/en/pdf
167 https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

- Cybersecurity Certification: EUCC Candidate Scheme, 1 July 2020
  サイバーセキュリティ認証：EUCC 候補スキーム。
  サイバースセキュリティ法に基づき、欧州委員会からの要請を受け、SOG-IS MRA（Senior Officials Group Information Systems Security Mutual Recognition Agreement）の下で運用されている既存スキームの後継となる EU サイバーセキュリティ認証スキーム候補を検討し、まとめた候補スキーム。

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 においては暗号の輸出入規制はワッセナー・アレンジメント（Wassenaar Arrangement）に基づき、規制が定められている。規制対象となる暗号製品等は、ワッセナー・アレンジメント会議で合意された「デュアルユース製品・技術リスト及び軍需品リスト（List of Dual-Use Goods and Technologies and Munitions List）」のなかのデュアルユース製品・技術に関するリストのカテゴリ 5 パート 2（Category 5 – Part 2 “Information Security”）がベースになっている。（参考：3.1.3.4 節のワッセナー・アレンジメント）

また、暗号製品の輸出入規制は欧州委員会の DG Trade が行う。関連する内容は以下の通りである。

- Council regulation (EC) No. 428/2009 of 5 May 2009[168]
  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。
  数回に渡り改正が行われている。2016 年には制度改訂案[169]が出され、その中では、サイバー監視技術（Cyber-surveillance technology）関連品目に対する規制も新たに盛り込まれた。
  「情報セキュリティ」システムに関連して、表 3-55 の暗号が規定されている。

[168] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF

[169] https://eur-lex.europa.eu/resource.html?uri=cellar:1b8f930e-8648-11e6-b076-01aa75ed71a1.0013.02/DOC_1&format=PDF

表 3-55　規制対象の暗号アルゴリズム

分類	アルゴリズム
対称鍵暗号	鍵長 56 ビット以上
非対称暗号	1. 512 ビットを超える整数の因数分解（例：RSA） 2. 512 ビットを超えるサイズの有限体の乗法群における離散対数の計算（例えば、Z/pZ 上の Diffie-Hellman） 3. 上記 2.以外の群の離散対数が 112 ビットを超える（例えば、楕円曲線上の Diffie-Hellman）
量子暗号	—

3.10.3.5.　プロトコル等での暗号方式

- eIDAS Cryptographic Requirements for the Interoperability Framework[170]

  eIDAS 規則に従った eIDAS ノード間の通信を保護するために、暗号化された SAML メッセージが用いられ、トランスポート層の保護のために TLS が使用される。この SAML 通信の保護のための暗号化要件と、この通信内での TLS の使用法を以下に示す。

  - 暗号化要件
    - ✧ TLS 1.2（それ以前のバージョンは使用禁止）
    - ✧ 推奨暗号スイート

表 3-56　推奨暗号スイート

	Key agreement and authentication mechanisms		Encryption	Mode of operation	Hash
TLS_	ECDHE_ECDSA_	WITH_	AES_128_	CBC_ GCM_	SHA256
			AES_256_	CBC_ GCM_	SHA384
	ECDHE_RSA_	WITH_	AES_128_	CBC_ GCM_	SHA256
			AES_256_	CBC_ GCM_	SHA384
	DHE_RSA_	WITH_	AES_128_	CBC_ GCM_	SHA256
			AES_256_	CBC_	SHA256
				GCM_	SHA384

（出典：eIDAS Cryptographic Requirements for the Interoperability Framework）

170 https://ec.europa.eu/cefdigital/wiki/display/cefdigital/eidas+eid+profile?preview=/82773108/148898849/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf

3.10.3.6. 暗号利用に関する規制（利用ライセンス・暗号盗聴法など）

EU では、個人のプライバシー保護の観点から、通信の暗号化を推奨しているが、一方、テロ、サイバー攻撃の脅威に対抗するため、End-to-end 暗号化をサービスプロバイダ側で解読し、加害者の情報に政府がアクセスすることを可能にするよう要請を行っている。

- EU strategy for a more effective fight against child sexual abuse
  児童の性的虐待との闘いに効果的な対応を提供することを目的とする戦略。
  欧州評議会は、EU では 5 人に 1 人の子供が何らかの形の性的暴力の犠牲になっていると推定している。容疑者が End-to-end 暗号化を使用すると、加害者の特定がより困難になる。End-to-end 暗号化の導入は、通信のプライバシーとセキュリティを確保する上で有益であると同時に、画像やビデオの取引など、加害者が、法執行機関から行動を隠すことができる手段になる。
  このため、犯罪目的での暗号化技術の使用は、企業が End-to-end の暗号化された電子通信で児童の性的虐待を検出して報告できるようにする可能性のあるソリューションを通じて、直ちに対処する必要がある。

- The Budapest Convention on Cybercrime: benefits and impact in practice, 13 July 2020
  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による利点と影響を説明している。

- the Effect of Encryption on Lawful Access to Communications and Data
  暗号化が法執行機関のデータへのアクセスに与える影響についての報告書。
  暗号化の使用は急速に増加している。世界の通信トラフィックの推定 18%が End-to-end で暗号化されている。2019 年までには、通信トラフィックの 22%が End-to-end で暗号化されると推定されている。この比率が上昇するとユーザの合意なしには法執行機関が復元不可能な暗号化が増大することになる。End-to-end の暗号化は、犯罪捜査を困難にするため、懸念を抱いている国も多い。

3.10.3.7. クラウドサービス

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の記載はない。

3.10.3.8. 暗号資産

欧州の暗号資産市場に関する規制について、提案が行われている。

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937
  暗号資産の市場に関する欧州議会および理事会の規制の提案、および指令（EU）2019/1937 の修正。

3.10.3.9. 電子署名法

欧州の人々と企業が独自の国内電子識別スキーム（eID）を使用して、他の EU 諸国でもオンラインで公共サービスにアクセスができるように eIDAS 規則が 2016 年 7 月に施行された。トラストサービス（電子署名、電子シール、タイムスタンプ、電子配信サービス、Web サイト認証）のヨーロッパの内部市場を形成し、国境を越えて、従来の紙ベースの同等物と同じ法的ステータスを持つことが保証された。

3.10.3.10. 国民 ID 番号制度（eID）

eID[171]は、欧州全土のユーザを電子的に識別するサービスとして、国境を越えた国内電子識別スキーム（eID）の相互承認を可能にするために欧州委員会によって提供される一連のサービス。これにより、欧州市民は他の欧州諸国からのオンラインサービスにアクセスするときに自国の eID を使用できる。

[171] https://ec.europa.eu/cefdigital/wiki/display/cefdigital/eid, https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification

3.10.4. その他

3.10.4.1. 量子コンピュータの進展に伴う対応策

現在の暗号技術は、量子攻撃に対抗するように設計されていない。ここ数十年の間に、量子攻撃の脅威から保護する新しい暗号技術が登場した。この技術は「量子セーフ（Quantum Safe）」と呼ばれており、この状態への移行が検討されている。

なお、HORIZON2020 のプロジェクトの１つとして、FutureTPM というプロジェクトで Quantum-Resistant Trusted Platform Module（耐量子トラステッドプラットフォームモジュール）[172]の研究が行われている。この研究では、TPM（Trusted Platform Module）に含めるのに適した QR（Quantum Resistant、量子耐性）アルゴリズムを設計および開発することにより、量子耐性（QR）の信頼できるプラットフォームモジュール（TPM）を設計することを目標としている。

- Quantum Safe Cryptography and Security, June 2015
  現在の暗号技術にとって脅威となる量子コンピューティングの攻撃からセキュリティシステムを保護する暗号技術の紹介および量子セーフな状態にアップグレードするための実用的な推奨事項が示されている。

- ETSI TR 103 619 V1.1.1 (2020-07) CYBER; Migration strategies and recommendations to Quantum Safe schemes
  非量子セーフ暗号状態から完全量子セーフ暗号状態（FQSCS：Fully Quantum-Safe Cryptographic State）の環境への移行の問題と安全な遷移を確保するためのガイダンスを提供している。

3.10.4.2. その他の特記すべき項目

- Baseline Security Recommendations for IoT
  重要な情報インフラのコンテキストにおける IoT のベースラインセキュリティの推奨事項。重要な資産と関連する脅威をマッピングし、可能性のある攻撃を評価し、IoT システムを保護するために適用すべき潜在的な優良事例とセキュリティ対策を特定している。IoT のベースラインセキュリティ対策を定義する分野として、以下がカバーされている。
  - スマートホーム
  - スマートシティとインテリジェント公共交通
  - スマートグリッド
  - スマートカー

[172] https://futuretpm.eu/

- スマートエアポート
- e ヘルスとスマートホスピタル

3.10.5. EU の参照文献

[1] EU Cyber Security Strategy - open, safe and secure
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=en

[2] The EU's Cybersecurity Strategy for the Digital Decade
https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy

[3] Digital Agenda for Europe (DAE)
https://op.europa.eu/en/publication-detail/-/publication/27a0545e-03bf-425f-8b09-7cef6f0870af

[4] The European Agenda on Security (2015-2020)
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[5] The EU Security Union Strategy 2020-2025
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

[6] Cybersecurity Certification: EUCC Candidate Scheme
https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme#:~:text=This%20has%20been%20named%20EUCC,%2C%20and%20corresponding%20standards%2C%20respectively%2C

[7] NIS Directive
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[8] EU Cybersecurity Act
https://eur-lex.europa.eu/eli/reg/2019/881/oj

[9] The EU cybersecurity certification framework
https://www.enisa.europa.eu/topics/standards/certification/certification_graph_08.jpg/view

[10] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

[11] ETSI TR 103 619 V1.1.1 (2020-07) CYBER; Migration strategies and recommendations to Quantum Safe schemes
https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[12] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[13] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004R0460
[14] The Budapest Convention on Cybercrime: benefits and impact in practice
https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac#:~:text=The%20Budapest%20Convention%20provides%20for,crime%3B%20and%20(iii)%20efficient
[15] 42 COM (2008) 798, COMMUNICATION FROM THE COMMISSION TO THE COUNCIL
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF
[16] EC regulation (EU) No 611/2013
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0611
[17] EU Directive 2002/58/EC
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
[18] EU strategy for a more effective fight against child sexual abuse
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf
[19] Council regulation (EC) No. 428/2009 of 5 May 2009
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32009R0428
[20] Council Regulation (EC) No. 1334-2000.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000R1334
[21] Algorithms, Key Sizes and Parameters Report
https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
[22] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms Version 1.2 January 2020
https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf
[23] The use of Cryptographic Techniques in Europe

https://www.enisa.europa.eu/publications/the-use-of-cryptographic-techniques-in-europe

[24] Baseline Security Recommendations for IoT
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[25] the Effect of Encryption on Lawful Access to Communications and Data
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf

[26] Quantum Safe Cryptography and Security
https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

4. まとめ

4.1. 各国・地域の暗号要件・評価認証の比較

以下に各国暗号関連政策の比較として、政府調達要件、暗号要件、評価認証の概要を報告する。

表 4-1 各国暗号関連政策の比較（政府調達要件・暗号要件・評価認証）

国(所管省庁)		政府調達要件	暗号要件	評価認証
米国	制度等	FISMA、情報技術管理改革法、Memorandum for Chief Information Officers – Security Authorization of Information Systems in Cloud Computing Environments	連邦政府標準・推奨暗号、NIST SP 800-57、SP 800-131A、CNSA Suite	CMVP、CAVP、CC
	特徴	FISMA や情報技術管理改革法に基づき、連邦政府調達品が使用する暗号モジュールの CMVP 認証取得や CC 認証取得を求める。 CNSS Policy No. 11 は、国家安全保障システムでの政府調達品の CC 認証取得を求める。 Memorandum は、連邦政府機関が使用するクラウドサービスや製品に FedRAMP 認証の取得を求める。	連邦政府標準・推奨暗号は、NIST が策定する連邦政府機関が利用すべき暗号アルゴリズム。FIPS、SP として公開。 SP 800-57、SP 800-131A は、NIST が定める、連邦政府機関が利用すべき暗号アルゴリズムの要件。 CNSA Suite は、NSA が定める、機密情報の保護に利用可能な暗号アルゴリズムの要件。	CMVP は NIST が実施する暗号モジュールの試験・認証制度。セキュリティ要件は FIPS 140-3 で定められており、ISO/IEC 19790:2012 を参照する。 CAVP は NIST が実施する暗号モジュール・アルゴリズムの試験制度。 CC は NSA と NIST が共同で設立した NIAP が実施する暗号製品の認証制度。評価基準は ISO/IEC 15408。
英国	制度等	HMG IA Standards、eGIF Technical Standards Catalogue、Cyber Essentials	HMG Cryptographic Standards	CAPS、CPA、Cyber Essentials 、CAS、CIR、CSC、CCP、Certified training、Certified Degrees、CHECK
	特徴	HMG IA Standards は、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規定。 eGIF Technical Standards Catalogue は、政府と民間セクタ間の電子政府相互運用フレームワークであり、ポリシー及び技術仕様の遵守が必要。 また、政府の機密データを保護するために暗号化が使用される場合は、CAPS 認証が必要。	HMG Cryptographic Standards は、政府機関で用いることのできる暗号を規定(非公開)	NCSC が運営。すべて英国独自の認証制度。 CAPS、CPA は、セキュリティ製品認証。 Cyber Essentials は組織のサイバー攻撃に対する対策を評価する政府支援のスキーム。 これ以外は、セキュリティサービス認証。
フランス	制度等	軍事計画法	Référentiel général de sécurité (RGS) version 2.0（セキュリティに関する一般基準 version 2.0）	CC, CSPN, Qualification
	特徴	ANSSI に、国にとって極めて重要な事業者の情報システム	政府システムへの適用が遵守事項となっているセキュリテ	ANSSI が管轄する認証制度は CC, CSPN 等の第三者機関によ

		等におけるセキュリティに対して、首相に代わって対応策を実行させる権限を付与。同時に ANSSI がセキュリティ製品の資格及び認証制度を運営している。	ィ基準であり、Annex B1 に暗号技術、Annex B2 に暗号鍵管理が記載される。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。	る評価をベースとした Ceritifcation と、ANNSI 自身が試験及び承認を行う Qulalication がある。
ドイツ	制度等	SAGA, IT-Stuerung Bund	SAGA, BSI TR	CC
	特徴	IT 製品の連邦政府の調達は BMWi が管轄している。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。	SAGA はドイツにおける電子政府アプリケーションにおける機密情報の送受信における暗号アルゴリズム及び署名アルゴリズムの要件や義務を規定した文書である。TR は強制力を持たないガイドラインであり、推奨暗号方式を示しており、TLS や IPsec 等に関する適用法法も整備されている。	BSI が運営。国際承認アレンジメント（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
エストニア	制度等	ISKE（IT Security Standard）	暗号アルゴリズムライフサイクル	-
	特徴	行政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規定。	暗号アルゴリズム及び推奨鍵長を規定	評価認証制度はない。
ロシア	制度等	連邦法「技術規制について」、国家機密情報保護製品の認証制度、情報セキュリティツールの認証制度	GOST 標準暗号	国家機密情報保護製品の認証制度、情報セキュリティツールの認証制度、情報保護の暗号手段の開発、生産、実装、運用に関する規則
	特徴	連邦法「技術規制について」は、GOST 等の技術標準への準拠を求める。 国家機密情報保護製品の認証制度、及び、情報セキュリティツールの認証制度の根拠法は、政府調達品がそれぞれの認証を取得することを求める。	GOST 標準暗号は、連邦技術規則・計測庁が標準化する利用が推奨される暗号。	国家機密情報保護製品の認証制度は、FSB、FSTEC が実施する、国家機密及び法律により保護された情報を扱う機器・サービスの認証制度。 情報セキュリティツールの認証制度は、FSTEC が実施する、国家機密の保護に利用可能な情報セキュリティツールの認証制度。 情報保護の暗号手段の開発、生産、実装、運用に関する規則は、国家機密を含まない情報を扱う情報セキュリティツールを規制。製品開発時に FSB がセキュリティ要件を満たすか確認。
中国	制度等	政府調達法	暗号法、業界標準暗号・国家標準暗号、全国商用暗号認証制度	国家情報セキュリティ認証制度、重要なネットワーク機器およびネットワークセキュリティ製品のセキュリティ認証制度、商用暗号製品認証制度。
	特徴	政府調達法は、国家情報セキュリティ認証制度認定品の調達を義務付ける。	暗号法により、核心暗号、普通暗号、商用暗号に分類。商用暗号以外は非公開。 商用暗号は、業界標準暗号として国家暗号管理局が、国家標準暗号として国家標準化管理委員会がそれぞれ標準化し、暗号製品での利用が求め	国家情報セキュリティ認証制度と、重要なネットワーク機器およびネットワークセキュリティ製品のセキュリティ認証制度はいずれも中国サイバーセキュリティ審査技術・認証センターが実施する、情報セキュリティ製品、重要なネ

			られる暗号。 全国商用暗号認証制度は、国家暗号管理局が行う暗号製品の強制認証制度で、業界標準暗号への準拠を求めている。	ットワーク機器およびネットワークセキュリティ製品の強制認証制度。 商用暗号製品認証制度は、国家暗号管理局商用暗号テストセンターが実施する、商用暗号製品の強制認証制度。
韓国	制度等	電子政府法、セキュリティ適合性検証制度	国内標準暗号、暗号アルゴリズムと鍵長の利用ガイドライン、KCMVP、国家サイバーセキュリティマニュアル(非公開)	CC、KCMVP、セキュリティ機能試験制度、IoT-SAP
	特徴	電子政府法は、政府機関の扱う電子文書の保安措置を義務付け、それに基づき NIS はセキュリティ適合性検証制度を実施する。 セキュリティ適合性検証制度は、連邦政府機関が情報保護システム及びネットワーク機器を導入し運用開始前に実施が義務付けられている制度。 導入システム・機器は CC 認証、もしくは「セキュリティ機能試験」制度の認証取得が必要。	国内標準暗号は、利用が推奨される暗号アルゴリズム。国内標準化(KS X)されている。 暗号アルゴリズムと鍵長の利用ガイドラインは、利用が推奨される暗号アルゴリズムの要件を定める。 国家サイバーセキュリティマニュアル(非公開)でも、利用が推奨される暗号アルゴリズムについての規定を含むことが窺えるが、確認できていない。	CC は、NIS の下に設置された ITSCC が実施する情報保護システムの評価・認証制度。韓国は 2006 年より CCRA に加盟。 KCMVP は暗号モジュール試験・認証制度、米国カナダの CMVP の韓国版の制度。NIS の下に設置された NCSC が実施、KS X ISO/IEC 19790:2015, ISO/IEC 24749:2015 を要件とする。KCMVP では、利用が推奨される暗号アルゴリズムを対象とする。 IoT-SAP(セキュリティ機能試験制度)は NIS が実施する、手続きが簡略化された簡易版 CC。 IoT-SAP は KISA が実施する IoT 機器と連携アプリケーションの安全性検証制度。
オーストラリア	制度等	Protective Security Policy Framework (PSPF)、Information Security Manual (ISM)	Information Security Manual (ISM) 、Information Security Registered Assessors Program(IRAP)、The Trusted Digital Identity Framework (TDIF)	AISEP、ASD Cryptographic Evaluation(ACE)、TDIF accredited
	特徴	PSPF の要件に準拠した ISM において AISEP 認証取得を義務付けている。	ASD が政府機関で用いることのできる暗号を ISM で規定している。さらに、ISM を参照し、クラウドサービス、TDIF 等で暗号を指定している。	AISEP によって CC に準拠した製品を評価、ACE によって暗号モジュールを評価する。さらに、ACE を含んだ TDIF を認証する。
EU	制度等	-	Algorithms, Key Sizes and Parameters Report、The Use of Cryptographic Techniques in Europe	Approved Cryptographic Productts (LACP) 、EUCC
	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	Algorithms, Key Sizes and Parameters Report は、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。 The Use of Cryptographic Techniques in Europe は、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。	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。LACP (List of approved cryptographic products) はその製品リスト。 EUCC は、EU 共通基準に基づく欧州サイバーセキュリティ認証。そのスキームは現在検討中。

4.2. 各国・地域の輸出入/利用規制

以下に各国暗号関連政策の比較として、輸出入規制、国内利用規制の概要を報告する。

表 4-2 各国暗号関連政策の比較（輸出入規制・国内利用規制）

国(所管省庁)		輸出入規制	国内利用規制
米国	制度等	輸出管理改革法、EAR、武器輸出管理法、国際武器取引規則	International Statement: End-To-End Encryption and Public Safety、Lawful Access to Encrypted Data Act(法案)
	特徴	ワッセナー・アレンジメントの合意に基づき、暗号製品を含むデュアルユース製品の輸出規制が行われている。その規則や対象品目は輸出管理改革法の実施規則、EAR が定める。 暗号が利用されている軍事品の輸出規制は、武器輸出管理法の下で定められた国際武器取引規則に従い実施されている。 暗号製品の輸入は規制されていない。	暗号利用は制限されていない。 ただし、合法的に暗号化解除や迂回手段の提供を義務付けようとする動きがある。 International Statement: End-To-End Encryption and Public Safety は米国、日本を含む 7 カ国の連盟の国際声明で、テクノロジ企業へ公共の安全を取り込んだシステム設計、法執行機関によるコンテンツへのアクセス手段の提供、政府やその他の利害関係者との協議の参加を求めている。 Lawful Access to Encrypted Data Act は、2020 年に議会へ提出された法案で、暗号化通信及び暗号化ストレージのコンテンツへの法務行政機関によるアクセス支援、アクセスの支援提供能力の保有を義務付ける。
英国	制度等	Open general export licence (cryptographic development、UK Strategic Export Controls annual report 2019、Export controls: dual-use items, software and technology, goods for torture and radioactive sources	Regulation of Investigatory Powers Act 2000 (RIPA)
	特徴	ワッセナー・アレンジメントの合意に基づき、暗号製品を含むデュアルユース製品の輸出規制が行われている。EU 離脱により、規則が変わる可能性がある。 暗号製品の輸入は規制されていない。	暗号の利用は規制されていない。 ただし、暗号データに対する開示命令権を規定している。 International Statement: End-To-End Encryption and Public Safety は米国、日本を含む 7 カ国の連盟の国際声明の参加国。
フランス	制度等	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 GUIDE SUR LES EXPORTATIONS DE BIENS ET TECHNOLOGIES A DOUBLE USAGE[8] (GUIDE ON EXPORT OF GOODS AND DUAL-USE TECHNOLOGIES)	Law no. 2004-575
	特徴	輸出規制はワッセナー・アレンジメントに基づく。 デュアルユースを含む暗号製品の輸出入に関しては ANSSI が所管している。	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である。
ドイツ	制度等	AWG, AWV, KWKG 2020	-
	特徴	ワッセナー・アレンジメントの合意に基づき、暗号製品を含むデュアルユース製品の輸出規制が行われている。なお、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。 暗号製品の輸入は規制されていない。	明示的な国内利用の規制はなし。

エストニア	制度等	Strateegilise kauba seadus, Vastu võetud 07.12.2011	-
	特徴	ワッセナー・アレンジメントの合意に基づき、暗号製品を含むデュアルユース製品の輸出規制が行われている。 暗号製品の輸入は規制されていない。	明示的な国内利用の規制はなし。
ロシア	制度等	暗号手段のユーラシア経済連合の税関地域への輸入およびユーラシア経済連合の税関地域からの輸出に関する規制、輸出管理について	情報、情報技術、情報保護について、特定の種類の活動のライセンスについて
	特徴	輸出・輸入のいずれも規制される。 ロシアはユーラシア経済連合の加盟国であり、加盟国間統一の輸出入規制制度が実施され、「暗号手段のユーラシア経済連合の税関地域への輸入およびユーラシア経済連合の税関地域からの輸出に関する規制」が、暗号の輸出入を規定する。 「輸出管理について」は、ロシア連邦の利益の確保、国際条約に基づいた武器等の輸出管理を定め、暗号製品は、ワッセナー・アレンジメント合意に基づいたデュアルユース製品として輸出が規制される。	「情報、情報技術、情報保護について」は、インターネットでメッセージを暗号化してやり取りする場合、復号に必要な情報のFSBへの提供を義務付けている。 「特定の種類の活動のライセンスについて」は、暗号や暗号利用システム等の開発、製造、流通、サービスの提供などの活動には許可が必要としている。
中国	制度等	対外貿易法、輸出管理法、技術輸出入管理条例、暗号法、(商用暗号管理条例)	国家情報法
	特徴	暗号製品・技術の輸出入は、輸出管理法及によりデュアルユース品目の輸出入管理制度、技術輸出入管理制度が暗号の輸出・輸入のいずれも規制される。 デュアルユース品目の輸出入管理制度は、対外貿易法、暗号法等に基づき、国家安全保障と社会的公益の維持を目的に実施される。規制対象品目は、商用暗号輸入許可リスト・輸出管理リストとして公開。 技術輸出入管理制度は対外貿易法、技術輸出入管理条例に基づき、先端技術（宇宙開発、通信、量子暗号等）の輸出を規制する。 いずれも商務部が実施。 なお、2020年1月の暗号法制定以前は、商用暗号管理条例とその施行規則に基づき、暗号管理局により暗号の輸出入規制が行われていたが、2020年1月の暗号法の制定により大きく変更されたことに留意されたい。 また、中国はワッセナー・アレンジメントに参加していない。	暗号の利用は規制されていない。 ただし、国家情報法には「全ての組織や国民は国家情報活動を支援・協力し、国の情報活動の秘密を守るものとする」(第7条)という規定があり、中国製の情報通信機器やその製造者やサービス事業者から当局へ情報が受け渡される可能性があると考えられている。
韓国	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	電子文書、電子取引基本法
	特徴	輸出の規制は、対外貿易法、対外貿易法施行令の下、戦略物資輸出入告示により、ワッセナー・アレンジメントの合意に基づいたデュアルユース品目として実施される。 暗号製品の輸入は制限されていない。	暗号の利用は規制されていない。 ただし、電子文書と電子取引基本法に、「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、平文や暗号技術へのアクセスに必要な措置を行うことができる。」（14条（暗号製品の使用）②）という規定がある。
オーストラリア	制度等	Defence and Strategic Goods List 2019、Australian Export Controls and ICT	Cybercrime Act, No. 161, 2001、Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018
	特徴	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。 さらに、防衛・戦略物資リスト2019においてAuthentication、Digital signatureに加え、Data integrity、Non-repudiation、Digital	暗号の利用を規制していない。 ただし、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。 また、警察機関や国家安全保障機関が暗号通信の内容を読み取れるように定めた法律がある。

		rights management 等が追加し、輸出規制の対象となる暗号アルゴリズムと鍵長を規定している。 暗号製品の輸入は制限されていない。	International Statement: End-To-End Encryption and Public Safety は米国、日本を含む 7 カ国の連盟の国際声明の参加国。
EU	制度等	Council Regulation (EC) No. 428/2009	EU strategy for a more effective fight against child sexual abuse、The Budapest Convention on Cybercrime、the Effect of Encryption on Lawful Access to Communications and Data
	特徴	ワッセナー・アレンジメントに基づき、デュアルユース品目の輸出に関する規制を定めている。	EU strategy for a more effective fight against child sexual abuse は、児童の性的虐待との闘いに効果的な対応を提供することを目的とする戦略。End-to-end 暗号化の導入は、犯罪を隠蔽する懸念がある。 The Budapest Convention on Cybercrime:は、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による利点と影響を説明している。 the Effect of Encryption on Lawful Access to Communications and Data は、暗号化が法執行機関のデータへのアクセスに与える影響についての報告書。End-to-end の暗号化の比率が進むと、ユーザの合意なしには、法執行機関が復元不可能な暗号化が増大し、犯罪捜査が困難になることに懸念を抱いている国も多い。