国家と暗号の関わり方に関する
海外調査

調査報告書

平成 18 年 3 月

ジェトロニクス株式会社

目 次

I. 調査の概要

1 本調査の概要

1.1 背景

独立行政法人 情報処理推進機構（以下 IPA）および、独立行政法人 情報通信研究機構（以下 NICT）では情報セキュリティ対策の強化、整備の一環として、CRYPTREC(Cryptography Research and Evaluation Committee)の運営を行っている。CRYPTREC は電子政府推奨暗号の安全性を評価･監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。日本における電子政府推奨暗号リストを作成し、電子政府システムに使用する暗号技術として推奨している。一方で、ISO/IEC において暗号技術の国際標準化が進められているが、国際標準暗号と CRYPTREC の推奨暗号との間で差異が発生しつつあり、今後は両者の関連を整理した上で、国際関係の中での CRYPTREC のあり方や、ISO/IEC の国際標準化に対する働きかけ方、政府調達の標準暗号についての方針見直しの必要性の有無などを検討することが課題になってきている。

1.2 目的

本調査は、海外主要国における最新の標準暗号技術政策の動向を把握し、比較することにより、日本にとって今後の課題である、CRYPTREC 推奨暗号技術の国際標準暗号との関係や他国との国際関係の中でのあり方等を検討するための、基本的な参考情報に資することを目的とした。
そのために、

- 海外主要国の暗号標準化に関する調査
- 海外主要国の暗号製品の政府調達に関する調査
- 海外主要国の国際標準暗号への対応に関する調査

を行うこととした。

1.3 調査対象

本調査では IPA および NICT が指定する主要7カ国の、標準暗号政策を主管する以下の政府機関を主な対象とした。

- 米国：NIST (National Institute of Standards and Technology)
- カナダ：CSE (Communications Security Establishment)
- 英国：CESG（Communications-Electronics Security Group)

- フランス：DCSSI(Direction Centrale de la Securite des Systemes d’Information)
- ドイツ：BSI(Bundesamt fur Sicheit in der Informationstechnic)
- オーストラリア：DSD (Defense Signals Directorates)
- 韓国：KISA (Korea Information Security Agency)

また、可能な範囲で、これらの国の電子政府システムで調達される暗号製品のベンダやシステムインテグレータを補足的な調査対象とした。

1.4 調査方法

調査方法は以下の通りであった。

1.4.1. 文献調査

暗号技術標準化、暗号技術の政府調達、国際標準暗号への対応に関する文献、Web 等の調査を実施した。調査対象には以下のウェブサイトを含んだ。

- http://www.cryptrec.jp/ (CRYPTREC)
- http://www.ipa.go.jp/security/ (IPA)
- http://www.cosic.esat.kuleuven.ac.be/nessie/ (NESSIE)
- http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=1 (ISO/IEC JTC 1/SC 27)
- http://ts.nist.gov/ts/htdocs/210/its.htm (NIST)
- http://www.cse-cst.gc.ca/index-e.html (CSE)
- http://www.dsd.gov.au/infosec (DSD)
- http://www.cesg.gov.uk/ (CESG)
- http://www.ssi.gouv.fr/fr/dcssi/ (DCSSI)
- http://www.bsi.de/bsi/index.htm (BSI)
- http://www.cyberprivacy.or.kr/privacy.html (KISA)

1.4.2. ヒアリング調査

暗号技術標準化、暗号技術の政府調達、国際標準暗号への対応に関して面談によるヒアリング（不可の場合は、電話によるヒアリングまたは質問票へのメールによる回答による）調査を実施した。調査対象は以下を含む各国の暗号技術政策主管政府機関および、可能な範囲で政府の情報システムへの納入をするシステムインテグレータまたは暗号製品ベンダとした。

- 米国：NIST(National Institute of Standards and Technology)
- カナダ：CSE(Communications Security Establishment)
- 英国：CESG(Communications-Electronics Security Group)
- フランス：DCSSI(Direction Centrale de la Securite des Systems d’Information)
- ドイツ：BSI(Das Bundesamt fur Sicheit in der Informationstechnic)
- オーストラリア：DSD(Defense Signals Directorates)
- 韓国：KISA(Korea Information Security Agency)

1.4.3. 調査の進め方

本プロジェクトは、以下のタスクに分けて作業を進めた。

タ ス ク	作　業	方　法
タスク 0	キックオフ：スケジュールや進捗報告、作業の進め方、作業分担などの確認を行った。	ミーティングまたは電話会議
タスク 1	質問票の作成－：IPA/NICT の調査要求項目をもとに調査対象機関への質問項目を検討整理し、質問票を作成した。	チーム討議、チームレビュー
タスク 2	文献調査：対象国政府機関の暗号技術政策に関する情報収集を文献ベースで行った。	文献検索、サイト検索、レポート作成、チームレビュー
タスク 3	直接調査：タスク 1 で作成した質問票をもとに、対象政府機関、民間企業にインタビューまたはアンケートを実施し結果をまとめた。	電話、電子メール、訪問インタビュー、アンケート（代替）、レポート作成、中間報告
タスク 4	報告書作成：タスク 0 から 3 までの結果を日本語に翻訳し、報告書を作成した。	スタッフ作業、チームレビュー、最終報告

1.4.4. 実施期間

調査開始は 2006 年 1 月上旬、最終報告は 2006 年 3 月下旬で、本調査プロジェクトを約 12 週間で実施した。

1.5 調査項目

調査項目は以下の通りであった。

1.5.1. 暗号標準化に関する調査

本調査項目では、対象国における、CRYPTREC の電子政府推奨暗号に相当する標準暗号の動向に関して調査を行い、選定・変更のルールの観点から比較分析を行うこととした。このため、以下の調査を実施した。

- 推奨暗号リストに関する調査：
  対象国での推奨・標準暗号リストの有無、暗号の概要、およびリストの位置づけ

- 推奨暗号選定に関する調査：
  対象国での推奨・標準暗号の選定基準、規定、手順

- 推奨暗号変更に関する調査：

対象国での推奨･標準暗号の変更基準、規定、手順、および今後の展望

1.5.2. 暗号製品の政府調達に関する調査

本調査項目では、対象国における、電子政府の情報システムへの暗号技術の導入に関して調査を行い、調達ルールの観点から比較分析を行うとした。このため、以下の調査を実施した。

- 電子政府の実現状況：
  対象国での電子政府の具体的なシステム導入状況

- 電子政府への暗号製品導入に関する調査：
  対象国での電子政府への暗号技術導入実績

- 電子政府での暗号製品調達ルールに関する調査：
  対象国での調達のルールやその元となる法律･規則

1.5.3. 国際標準暗号への対応に関する調査

本調査項目では、対象国における ISO/IEC 標準暗号等、国際暗号標準への対応に関して以下の調査を行い、国内の推奨暗号･標準暗号との差異の観点から比較分析を行うこととした。

- 暗号技術の国際標準化の状況に関する調査：
  ISO/IEC 等での暗号技術を対象とした国際標準化の状況

- 暗号技術の国際標準化活動への参加に関する調査：
  対象国での暗号技術を対象とした国際標準化活動への参加状況

- 国際標準と国内標準暗号の差異に関する調査：
  対象国での推奨･標準暗号と国際標準暗号の差異

- 国際標準暗号の政府調達に関する調査：
  対象国での国際標準暗号の政府調達の方針、規定、手順、および今後の展望

2 本調査の結果概要

2.1 各国暗号政策の比較

調査対象7ヶ国の暗号政策の特徴を以下にまとめた。

調査対象国	暗号政策組織	推奨・標準暗号の例	推奨・標準暗号に関する規格	ISO/IEC対応例（ブロック暗号）	特徴
米国	OMB, NIST-STG, NSA-CSS	AES, RSA	FISMA, FIPS 140-1/-2	AES	FIPSに採用された暗号の国際標準化
カナダ	CSE-ITS, CIOB	CAST5, El-Gamal	MITS	CAST5	FIPS指向
英国	CESG	AES, DSA	e-GIF	AES	CAPS（官民協業）
フランス	DCSSI	RSA-OAEP, SHA-256	PRIS	AES	ADELEプログラム（電子政府戦略）
ドイツ	BSI	AES, ECDSA	SAGA	AES	三段階暗号リストとライフサイクル
オーストラリア	DSD	AES, DH	ACSI-33	AES	デファクト採用による効率性
韓国	NIS,NSRI, KISA,ETRI	SEED, ARIA	NIS	SEED	暗号アルゴリズム試験制度開始

2.2 調査結果から得られた知見

本調査の結果より、今後の日本での暗号政策検討のために参考となる知見として、以下のポイントが得られた。

- **政府調達における推奨暗号の役割**
  今回調査した全ての国で、政府調達における推奨または標準の暗号アルゴリズムの存在が確認された。商用レベルの暗号が要求されている場合では、韓国を除き、殆どの国で推奨・標準暗号アルゴリズムが公開されていた（韓国では KISA に依頼して入手）。その強制力については、各国で表現の違いはあるものの、基本的には推奨されたアルゴリズムを実装した製品が政府調達の対象となり、「標準」とは明示していないものの、実質的な標準アルゴリズムとなっている。実際の政府調達では、推奨・標準アルゴリズムの採用はあくまで前提条件であって、実装レベルで検証される必要がある。

- **政府調達における推奨・標準暗号以外の暗号の電子政府への使用可能性**
  米国では推奨・標準以外は暗号として認めていない。推奨・標準以外の暗号の電子政府システムへの使用を可能とする国でも、独自の評価（コスト・時間がかかる）を必要としている（カ

ナダ、英国、フランス、ドイツ、オーストラリア）。日本の場合、CRYPTREC との整合性を取り、方針を決定する必要がある。

- **国際標準暗号の政府調達における推奨・標準暗号への採用可能性**
  ISO/IEC 国際標準暗号も、政府調達における推奨・標準になっていなければ新規暗号と同様に独自の評価が必要、即ち、そのまま国内標準にはならない、としている国が多かった。この場合、EU 加盟諸国（フランス、ドイツ）ではコモンクライテリア相互認証制度での評価が、カナダ、オーストラリアでは米国の FIPS（Federal Information Processing Standards：連邦情報処理規格）の評価が、重要な判断基準として位置付けられている。

- **電子政府用暗号の階層化**
  電子政府用の暗号として、G2G（Government to Government：政府内および政府間）と G2C（Government to Consumer：政府と国民・市民間）を区別して使い分けることは、一般には行われていないが、一部の国（韓国、米国、英国）では、G2G の中でもより機密性の高い領域で使われるをアルゴリズムを非公開にしたり、一般の G2G や G2C と階層を区別して評価・管理する例がある。

- **国内推奨・標準暗号リストのライフサイクル・モデル**
  国内推奨暗号リストを定期・不定期的に見直すとしている国は多かったが、暗号リストを三段階のクラスに分けてライフサイクル管理を行うドイツのモデルが注目に値する。日本でも、暗号の危殆化やデファクト・スタンダード暗号への対応のためにも、推奨リストの見直しの方法を検討することは必要であろう。

II. 調査結果

1 暗号の国際標準化動向

1.1. 暗号国際標準化の背景

1.1.1. 暗号規制

インターネットが普及する以前、暗号は軍事的に重要な技術であり、民間での開発や利用はどこの国でも規制されていた。暗号の輸出は、他の国による軍事利用を警戒して特に規制されていた。その代表的な例は COCOM による規制である。しかし、インターネットの利用が始まり、個人や企業が通信に利用し始めると、情報の機密を守るために暗号を利用したいという要求が高まった。当時米国は暗号鍵の「第三者預託（エスクロー）」あるいは「鍵回復可能（キー・リカバブル）」を要求し、英国とフランスはこれに同調したが、日本、カナダ、ドイツなどが反対した結果、1997 年に発表された OECD の「暗号政策ガイドライン」[1]では以下のような内容が示された。

- 情報通信システムを利用する上での暗号技術は重要である。
- 市場要求にもとづいた暗号技術の開発を進める。
- 国内および国際レベルで暗号技術の標準・基準・プロトコルの開発を進め、公布する。
- 国あるいは国際的な暗号政策において、個人の通信の秘密、個人データの保護といったプライバシーを尊重する。
- 法令に基づいて、平文、暗号鍵、暗号化されたデータ、にアクセスすることを許す。
- 暗号サービスを提供し、暗号鍵を保持し、あるいは暗号キーにアクセスする個人あるいは団体は、契約または法律によりその責任を明確に記述しなければならない。
- 暗号が国際的に受け入れられるよう、一国は採用した暗号政策を出来る限り他の国の同様の政策と（一致させるよう）調整しなければならない。

但し、1997 年 6 月の G8 デンバー・サミットではテロを防止し捜索するために、法令に基づいて暗号データにアクセスすることは各国の支持を得た。

1.1.2. ワッセナー・アレンジメント

1994 年 3 月末に冷戦時代から続いていた旧共産圏諸国への戦略物資輸出統制システムである COCOM が解消された。その後、1995 年 12 月に新たな輸出管理体制の設立に関する合意が成立

[1] Cryptography Policy Guidelines, http://www.oecd.org/document/11/0,2340,en_2649_201185_1814731_1_1_1_1,00.html

し、会議の行われたオランダのワッセナー市にちなみ「ワッセナー・アレンジメント」（The Wassenaar Arrangement）とよばれている。[12]
ワッセナー・アレンジメントは法的な拘束力を有する国際体制ではなく、通常兵器及び機微な関連汎用品・技術の供給能力を有し、かつ不拡散のために努力する意思を有する参加国による紳士的な申し合わせとして存在する。日本国内ではこの精神に基づいて、輸出貿易管理令および貨物等省令により輸出の規制を行っている。暗号はこの規制の対象となっていて、機能・性能により特定の国へは輸出が規制されている。他の参加国も同様の規制を行っている。
現在の参加国は以下に示す 40 ヶ国である。

- アルゼンチン、米国、カナダ
- オーストリア、ベルギー、ブルガリア、クロアチア、チェコ、デンマーク、エストニア、フィンランド、英国　フランス、ドイツ、ギリシャ、ハンガリー、アイルランド、イタリア、ラトビア、リトアニア、ルクセンブルク、マルタ、オランダ、ノルウェー、ポーランド、ポルトガル、ルーマニア、スロバキア、スロベニア、スペイン、スウェーデン、スイス
- 日本、韓国、ニュージーランド、オーストラリア
- ロシア、トルコ、ウクライナ
- 南アフリカ

1.1.3. 金融分野におけるセキュリティ技術国際標準化

民間で早くからセキュリティ技術の国際標準が必要であることを認めたのは金融分野であった。クレジットカードや大口金融取引などで暗号化が必要となり、しかも、それが国際的に通用しなければならなかったからである。ISO TC 68 は金融業務のセキュリティ国際標準を 1990 年代の初めから進めてきた。その状況を以下の表で示す。
この表では当時の ISO 番号を用いているが、その内の相当数は新たな標準で置き換えられているので注意が必要である。

標準暗号などに　金融関連の国際標準

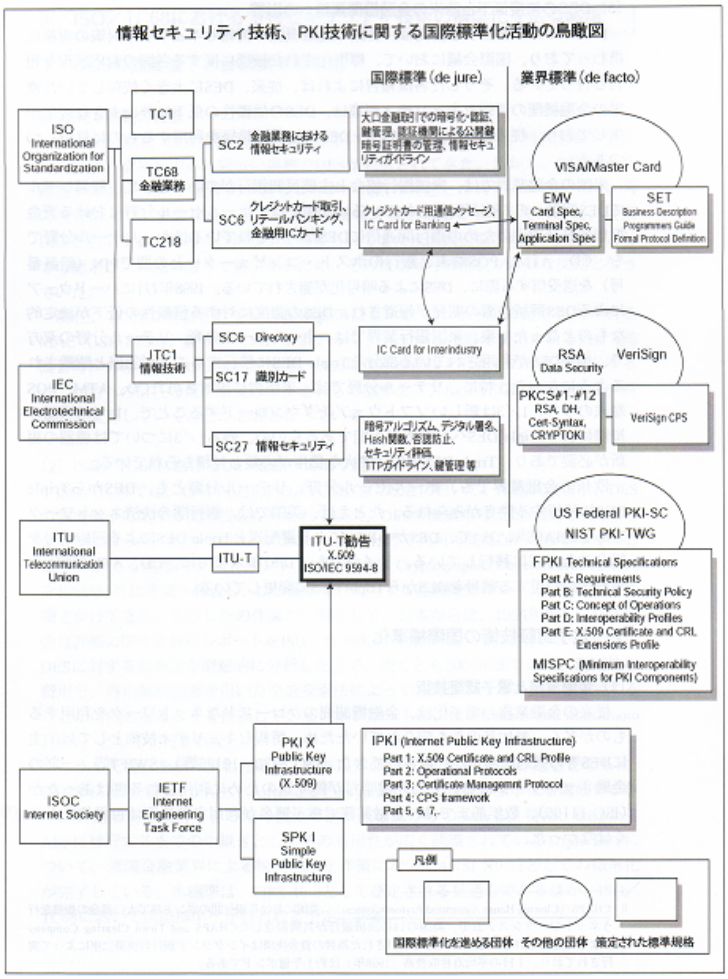
国際標準の番号	名称
ISO 8730	メッセージ認証のための必要案件
ISO 8731	メッセージ認証のためのアルゴリズム
ISO 8732	暗号鍵の管理
ISO 9564-1	PIN 管理とセキュリティ
ISO 9564-2	PIN　管理とセキュリティ：暗号アルゴリズム
ISO 9992	IC カードと端末間のメッセージ
ISO 10126-1	メッセージ暗号化手順
ISO 10126-2	メッセージ暗号化手順：暗号アルゴリズム
ISO 10202	IC カードを利用した金融取引システムのセキュリティ対策
ISO 11131	サイン・オン認証
ISO 11166-1	公開鍵アルゴリズムの利用による鍵管理
ISO 11166-2	公開鍵アルゴリズムの利用による鍵管理：RSA 暗号アルゴリズム
ISO 13491	安全な暗号装置

[1]通常兵器及び関連汎用品・技術の輸出管理に関するワッセナーアレンジメント
http://www.mofa.go.jp/mofaj/gaiko/arms/wa/index.html

[4] http://www.imes.boj.or.jp/japanese/zenbun99/yoyaku/kk18-2-3.html

この標準化作業は ISO と IEC の合同委員会（JTC 1/SC 27）や ITU（ITU-T）および ISOC（IETF）と協力しながら進められた。PKI 技術に関するこれらの国際標準化機関の関連を以下の図に示す。（「金融分野における情報セキュリティ技術の国際標準化動向」日本銀行金融研究所、金融研究／1999.4 PP33-56[4]）

金融関連国際標準の制定における協力関係



PKI では ISO(国際標準化機構)、IEC（国際電気標準会議）、ITU（国際電気通信連合）、ISOC（インターネット学会）が協調して規格の標準化を進めた。
（左図は「金融分野における情報セキュリティ技術の国際標準化動向」から引用 ）

1.1.4. AES 暗号の開発プロセス

米国では 1977 年に開発された共通鍵暗号である DES（鍵長 56 ビット、ブロック長 64 ビット）を長らく使っていたが、暗号研究や計算機性能の発展により、解読の危険性が現実的なものとなった。また、様々な機器やソフトウェアに組み込めるコンパクトで強力な暗号の必要性も高まり、NIST（米国標準技術局）が 128 ビットブロック暗号アルゴリズムを公募した。
DES は NBS（米国標準局、NIST の前身）が公募で選んだ暗号を改変して出来た暗号であり、改変プロセスを秘密にしたことが学会などから激しく批判された。そこで NIST はこの時の反省を教訓に、AES の公募において、候補暗号の評価方式および評価プロセスをすべて公開で行った。その結果 2000 年 10 月 2 日に最終選択が発表され、IBM, RSA, Counterpane などの米国企業の提案を抑えて Rijndael（ベルギー）が採用された。米国政府はこの暗号を AES(Advanced Encryption Standard) 暗号と名づけ、AES を連邦情報処理規格（FIPS:Federal Information Processing Standards）に採用

する方針を示し、2001 年 4 月に FIPS 197 として正式登録された。NIST は AES 暗号が他の政府及び民間標準として採用されることを希望すると表明した。[1]

1.1.5. EU の暗号標準化

ヨーロッパの標準化機関として暗号に関わるのは、次の 3 機関がある。
CEN (Europian Standadization Organization)[2]
CENELEC (Europian Committee for Electrotechnical Standardization)[3]
ICTSB (Information and Communications Technologies Standard Board)[4]
ICTSB は情報技術及びネットワーク技術に特化していて、以下に述べる NESSIE プロジェクトでは実質的な母体となった。

EU は電子商取引の発展にともない、暗号標準化の必要性を強く感じ 1999 年に暗号標準化プロジェクト NESSIE（New European Schemes for Signatures, Integrity, and Encryption IST-1999-12324 ）を立ち上げた。[5]
このプロジェクトの主な目的は公募した暗号アルゴリズムを公正に評価し、強い暗号アルゴリズムの一覧を作ること、そして米国の NIST が提唱する「AES ブロック暗号標準化プロセス」に寄与することであった。一方、データの機密性、完全性を高め、認証に使える暗号アルゴリズムの公募も行った。暗号アルゴリズムとしてはブロック暗号、ストリーム暗号、ハッシュアルゴリズム、MAC アルゴリズム、ディジタル署名方式及び公開鍵方式が含まれている。プロジェクトの目的は、これらのアルゴリズムや方式を評価する方法及びソフトウェアを開発することであった。さらに、この結果を公表し、共通認識を高め、ヨーロッパの暗号産業の地位を高めることも最終的なゴールであった。

プロジェクトは第一フェーズ（2000 年 3 月～2001 年 6 月）と第二フェーズ（2001 年 7 月～2003 年 3 月）に分けて進められた。参加企業は以下の通りである。

- Algorithmic Research (イスラエル)
- Amtec SpA (イタリア)
- Baltimore Technologies (アイルランド)
- Cryptomathic (デンマーク)
- Deutsche Telekom AG(ドイツ)
- Entrust Technologies (スイス)
- Ericsson Radio System AB (スエーデン)
- Europay International (ベルギー)
- Gemplus (フランス)
- Hewlett-Packard Laboratories (イギリス)

---

[1] AES: Who won?, Discover the results of the Advanced Encryption Standard contest
http://www.javaworld.com/jw-10-2000/jw-1027-aes.html

[2] CEN
http://www.cenorm.be/cenorm/index.htm
[3] CENELEC
http://www.cenelec.org/Cenelec/Homepage.htm
[4] ICTSB
http://www.ictsb.org/
[5] NESSIE, New European Schemes for Signature, Integrity, and Encryption
https://www.cosic.esat.kuleuven.be/nessie/

- Isabel (ベルギー)
- KPN Reseach (オランダ)
- NDS (イスラエル)
- Nokia (フィンランド)
- Oberthur Card System (フランス)
- RSA Laboratories Europe (スェーデン)
- Security Design International (イギリス)
- STMicroelectronics (フランス)
- S.W.F.T. (ベルギー)
- Telenor Research (ノルウェー)
- Telsy Elettoronica SpA (イタリア)
- Thomson CSF (フランス)
- Utimaco (デンマーク)
- Vodafone (イギリス)
- Zaxus (イギリス)

NESSIE プロジェクトの成果は「NESSIE security report」としてまとめられた。[1] その骨子は以下の通りである。

- 64 ビットブロック暗号：MYSTY1 を採用
- 128 ビットブロック暗号：AES および Camellia を採用
- 256 ビットブロック暗号：SHACAL2 を採用
- ストリーム暗号と擬似乱数：採用決定なし。
- 衝突困難ハッシュアルゴリズム：Whirlpool、SHA-256、SHA-384、SHA-512 を採用
- メッセージ認証コード：UMAC、TTMAC、EMAC、HMAC を採用
- 非対称暗号スキーム：PSEC-KEM、RSA-KEM、ACE-KEM を採用

この NESSIE プロジェクトは ISO/IEC 18033 の暗号標準化と並行して進められ、国際標準に大きな影響を与えた。

1.2. ISO/IEC JTC1

ISO/IEC の合同技術委員会 1（JTC 1）では、暗号関連の標準化を SC 27 小委員で審議している。SC 27 は情報技術のセキュリティ全般について、

- 情報システムのセキュリティ・サービスに対する要求の定義
- セキュリティ技法と機構の開発
- セキュリティ・ガイドラインの開発
- 管理支援文書と標準（用語集やセキュリティ評価基準）制定

を活動対象としている。但し、以下は対象外となっている。[2]

[1] NESSIE security report, Deliverable Number D20
https://www.cosic.esat.kuleuven.be/nessie/deliverables/D20-v2.pdf

[2] ISO/IEC JTC 1 SC 27 – IT Security Techniques, IEEE Computer Society
http://ieeeia.org/iasc/iso.html

- アプリケーションへの機構組み込み

JTC 1/SC 27 への参加国は以下の 31 カ国およびオブザーバ 11 カ国の合計 42 カ国となっている。
（括弧内は国数）

- 欧州(17)　英、独、仏、ベルギー、スイス、ノルウェー、オランダ、フィンランド、オーストリア、デンマーク、イタリア、ルクセンブルグ、スェーデン、ルーマニア、チェコ、スロベニア、ウクライナ
- アジア（6）日本、韓国、中国、インド、シンガポール、マレーシア
- 北米(2)　米国、カナダ
- アフリカ(3) 南アフリカ、エジプト、ケニヤ
- 中南米（1）ブラジル
- 大洋州（2）オーストラリア、ニュージーランド

SC 27 が制定した暗号関連の規格は現在以下の表 2 の通りである。
暗号標準選定に当たっては、予め次に示すような選択基準を定め、各国から提案された候補案をその基準に照らして審議した。

暗号の選考基準[1]

1.) 暗号の安全性：暗号分析攻撃に対し強固であること。
2.) 暗号の性能：様々なプラットフォーム上で時間的及び空間的に優れていること。
3.) 認可問題：認可に係る問題が無いこと。
4.) 暗号の成熟度：どれだけ広く使われ、分析結果が公にされ、吟味されたか。
5.) 権威ある機関による保証：標準化機関や政府のセキュリティ機関による保証がある。
6.) 暗号の採用度：特段の条件が無い限り、デファクトスタンダードは有利である。
7.) 暗号の数：この標準に含める暗号の数はできるだけ少なくする。

[1] ISO/IEC 18033-1
[3] Official Internet Standard

ISO/IEC JCT 1/ SC 27 が制定した暗号関連規格 (2006 年1月 20 日現在)

規格番号,	内容,	状態、
ISO/IEC 9796-2:2002	メッセージ回復を伴うディジタル署名のスキーム:素因数分解によるメカニズム	発行済み
ISO/IEC 9796-3:2002	メッセージ回復を伴うディジタル署名のスキーム:離散対数に基づくメカニズム	発行済み
ISO/IEC 9797-1	メッセージ認証コード－ブロック暗号を使うメカニズム	発行済み
ISO/IEC 9797-2	メッセージ認証コード－専用ハッシュ関数を使うメカニズム	発行済み
ISO/IEC 9798-1	主体認証－全般	発行済み
ISO/IEC 9798-2:1999	主体認証－対称暗号アルゴリズムを使ったメカニズム	発行済み
ISO/IEC 9798-2:1999/Cor1:2004	主体認証－対称暗号アルゴリズムを使ったメカニズム	発行済み
ISO/IEC 9798-3	主体認証－ディジタル署名を使ったメカニズム	発行済み
ISO/IEC 9798-4	主体認証－暗号チェック関数を使ったメカニズム	発行済み
ISO/IEC 9798-5	主体認証－ゼロ知識を使った技法	発行済み
ISO/IEC 9798-6	主体認証－手動伝送を使ったメカニズム	発行済み
ISO/IEC 9979	暗号アルゴリズム登録の手順	発行済み
ISO/IEC 10116:1997	N-ビットブロック暗号アルゴリズムの利用モード	発行済み
ISO/IEC 10116	N-ビットブロック暗号アルゴリズムの利用モード	開発中
ISO/IEC 10118-1	ハッシュ関数－全般	発行済み
ISO/IEC 10118-2	Nビットブロック暗号を用いたハッシュ関数	発行済み
ISO/IEC 10118-3:2004	専用ハッシュ関数	発行済み
ISO/IEC 10118-3:2004/Amd1	専用ハッシュ関数	開発中
ISO/IEC 10118-4:1998	剰余演算を用いたハッシュ関数	発行済み
ISO/IEC 11770-1	鍵管理－枠組み	発行済み
ISO/IEC 11770-2	鍵管理－対称技法を使ったメカニズム	発行済み
ISO/IEC 11770-3	鍵管理－非対称技法を使ったメカニズム	発行済み
ISO/IEC 14888-1	付録を伴う文書のディジタル署名－全般	発行済み
ISO/IEC 14888-2	付録を伴う文書のディジタル署名－識別に基づくメカニズム	発行済み
ISO/IEC 14888-3	付録を伴う文書のディジタル署名－証明書に基づくメカニズム	発行済み
ISO/IEC 15946-1	楕円アルゴリズムによる暗号化技術－全般	発行済み
ISO/IEC 15946-2	楕円アルゴリズムによる暗号化技術－ディジタル署名	発行済み
ISO/IEC 15946-3	楕円アルゴリズムによる暗号化技術－鍵生成	発行済み
ISO/IEC 18033-1	暗号アルゴリズム－全般	発行済み
ISO/IEC 18033-2	暗号アルゴリズム－非対称暗号	開発中
ISO/IEC 18033-3	暗号アルゴリズム－ブロック暗号	発行済み
ISO/IEC 18033-4	暗号アルゴリズム－ストリーム暗号	発行済み

1.3. ISOC-IETF

2006 年 1 月インターネット･エンジニアリング･タスクフォース（IETF）とインターネット協会（ISOC）は発足 20 周年を祝った。IETF はインターネットプロトコルの標準を決めているが、その実態は任意の会員（企業及び個人）による非営利団体である。会員同士の貢献、了解ならびに協力によって標準を決めるという方法は他にはないやり方である。しかし、その反面時間がかかることも事実である。標準はその審議過程で「標準提案（Proposed Standard）」、「標準草案（Draft Standard）」と進み、最終的に「標準（Internet Standard）」となるのだが「標準」として登録されているのは 66 項目で「標準草案」は 77 項目、「標準提案」が約 1030 項目ある。暗号に関する標準はまだ「標準提案」レベルであるが、すでに実用化されているものが多い。
IETF では暗号をプロトコルに組み込んで使うことに重点を置いていて、暗号の評価･選定には重点を置いていない。プロトコルとしては以下に示すものがある。

- TLS (Transport Layer Security)
- ESP (Encapsulating Securiy Payload)
- IKE (Internet Key Exchange)
- SNMP (Simple Network Management Protocol)
- CMS (Cryptographic Message Syntax)
- X.509 (Internet X.509 Public Key Infrastructure)
- SIP (Session Initiation Protocol)

使われている暗号は、DES、Triple DES、AES、SHA-1、Camellia、Diffie-Hellman などで、新しい暗号は余り使われていない。次ページに暗号に関係する RFC の一覧を表 3 に示す。[3]

表 1 暗号関連 RFC

プロトコル	規格番号	内容	状態
TLS	RFC 4279	TLSの共通鍵。第一のセットは認証に対称鍵のみを使う。第二のセットは共通鍵で認証したディフィー・ヘルマン鍵交換アルゴリズムを使う。第三のセットはサーバー認証に公開鍵を使いクライアントの認証に共通鍵を使う。	標準草稿
ESP	RFC 4305	カプセル化セキュリティペイロード(ESP9と認証ヘッダー(AH)	標準草稿
	RFC 4309	AES暗号をESPに用いる方法	標準草稿
	RFC 4312	CamelliaをESPに用いる方法	標準草稿
IKE	RFC 3526	インタネットキー交換 (IKE)における追加Moduler Exponential (MODP) Differ-Hellman グループ	標準草稿
	RFC 4307	IKEv2、かならず具備すべき暗号アルゴリズムー3DES-CBC, SHA1	標準草稿
	RFC 4308	IPsecで使う暗号、DES3-CBC, HMAC-SHA1, 1024 MODP	標準草稿
SNMP	RFC 3826	ユーザベースセキュリティモデルのSNMPに使うAES暗号	標準草稿
CMS	RFC 3537	鍵つきハッシュ関数をDES3またはAES暗号鍵で暗号化する	標準草稿
	RFC 3602	AES-CBC 暗号化アルゴリズムをIPsecで用いる	標準草稿
	RFC 3657	暗号メッセージシンタックスにCamellia暗号アルゴリズムを用いる。	標準草稿
	RFC 3852	暗号メッセージシンタックス	標準草稿
X.509	RFC 3279	PKIで使われる公開鍵及びASN.1で書いたディジタル署名のアルゴリズム判別	標準草稿
	RFC 3280	PKIの証明書取り消しリスト	標準草稿
	RFC 4055	RFC 3279の補足	標準草稿
SIP	RFC 3853	セッションイニシエーションプロトコル(SIP)におけるS/MIMEのAESによる暗号化	標準草稿

2 米国

2.1. 米国の概要

2.1.1. 電子政府普及の状況

電子政府への取り組み

「電子政府法（The “E-Government Act of 2002” (H.R. 2458/S.803)」 は 2002 年 12 月 17 日にブッシュ大統領が署名して成立し、2003 年 4 月に発効した（Public law 107-347）。これに先立ちブッシュ政権は 25 項目の重要項目を挙げた「大統領重点項目（President Management Agenda [PMA]）」を掲げ奨励した。電子政府法では行政予算管理局（OMB）を電子政府の主管と定めている。北アメリカ、ヨーロッパ、アジア地域に対して 2005 年にアクセンチュアがおこなった評価では、米国はカナダにつぐ 2 位となった。また、同年に行われたブラウン大学による評価では台湾、シンガポールに次ぐ 3 位であった。
内部評価では、電子政府の状態は政府の「点数表」と PMA で定義された 25 項目の進捗度によって測定される。2005 年 9 月の時点では次のような評価であった。

- 連邦政府の 26 省庁のうち 15%が成功という評価であった
- 50%は成否入り混じった評価であった。
- 35%は不成功という評価を受けた。

電子政府展開の現状

26 省庁の内 23 省庁は OMB に認可され、それぞれの省庁が受け入れた電子政府達成プログラムを遂行した結果、オンライン購買（SmatBUY）及び業務系統は 2005 年第四半期に 97%が完成した。以下のような事例がある。

- 連邦所得税申請オンラインサービス（Internal Revenue Service Free File）は 510 万人が 2005 年中に利用した。
- E-規則作成（ディジタル技術を規則作成に使うもの）は多くのサービスチャンネルで規則作成に携わる人々に使われ、2005 年中におよそ 160 万人の人々が利用した。
- オンライン認許では 2005 年中に 1500 の認許プログラムがオンラインで使えるようになった。
- 連邦政府のオンライン・ジョブサイトは「リクルート・ワンストップ」としてまとめられ、各省庁が独自に出していた求人サイトが閉じられた。その結果 2005 年に 880 万人がこのサイトを訪れ、80 万人以上の履歴書がオンラインで作られた。
- 「E-給与」は 26 の連邦給与システムを 2 プロバイダに集約し、簡素化しようとするものであるが、2004 年にはすでに 7 省庁が新システムに移行した。

セキュリティ実装の事例

省庁横断の情報セキュリティ計画としては OMB の E-認証がある。この計画の主要な実装は以下のとおりである。

- 総合サービス局がオンライン入札を行うための、E-提案及び E-修正システム
- 環境保護局が機密データの伝送を行う、中央データ交換プログラムの認証
- 司法省が実施する、初めての主要な PKI 認証―BATS(Bomb Arson Tracking System)
- 総合サービス局と財務省が、各省庁におこなう財務管理サービスで認証を行う。

2.1.2. 暗号政策の担当政府機関

OMB (Office of Management and Budget[1])

- OMB の使命：大統領を補佐し、予算、政策、の作成と実施及び運用をおこなう。
- 政府部内における位置づけ：行政府の一部であり直接大統領に報告する。
- 暗号政策への関与：OMB は 2002 年成立の電子政府法のタイトルIII、FISMA (Federal Information Security Management Act) で定められたように、その電子政府システムアーキテクチャで使われる暗号を選定する。

DHS (Department of Homeland Security[2])

- 使命：テロリストの攻撃を防ぎ、脅威や危険に対応し、国境の安全を確保する。
- 政府部内の位置づけ：大統領官邸の 15 部局のひとつである。
- 暗号政策への関与：国土防衛に関する大統領指示 (Homeland Security Presidential Directives [HSPD]) を通じて IT セキュリティのガイダンスを与える。例えば、2004 年 8 月に出された HSPD-12 は、すべての連邦政府職員及び契約者は情報システムや施設を使うに際し、PKI ディジタル認証を受けるためのスマートカードを持たなければならない、と規定した。この指示は OMB が監督している。

NIST (National Institute of Standards and Technology[3])

- 使命：IT リスクの認識を高め、情報システムのセキュリティを高めること。そのために IT リスクの研究を行い、助言をする。また、標準、評価指数、試験や実証方法を開発し、IT セキュリティを高めるために計画・実装・管理・運用についてのガイドラインを開発する。
- 政府部内における位置づけ：コンピュータセキュリティ部門は NIST の情報技術研究所の中にある。NIST は商務省の傘下にある 15 部局のひとつである。
- 暗号政策への関与：コンピュータセキュリティ部門は 4 つの重要分野を持っている。その内のひとつが連邦政府の情報の機密性、完全性および真正性を守るための暗号手法を開発することである。これを扱っているグループの名前は STG(Security Technology Group)である。このグループは連邦政府のために暗号を開発し保守する責任を直接持っている。

NSA/CSS (National Security Agency/ Central Security Service[4])

1 http://www.whitehouse.gov/omb/
2 http://www.dhs.gov/dhspublic/
3 http://www.nist.gov/
4 http://www.nsa.gov/

- 使命：米国政府の情報システムを守るために、各部門との調整を行い、指示しあるいは直接行動する。外国の信号を傍受して諜報情報を作り、暗号化文書を作成し、あるいは暗号解読を行う。
- 政府部内の位置づけ：行政府の中の 1 部局
- 暗号政策への関与：NSA は軍及び諜報部門のクラシファイド情報に対し、安全性の高い暗号を開発し保守する責任を持つ。NSA は場合により STG と協業する。

2.1.3. 電子政府システムでの暗号の使用

政府部内で使われる暗号は、次の項目が規定されている。

- 乱数発生
- キー管理
- 暗号化
- メッセージ認証
- ディジタル署名
- ハッシング
- オペレーションモード

2.1.4. 電子政府における非 ISO/IEC 暗号の利用

原則的には、各省庁が電子政府実現のために非 ISO/IEC 暗号を利用することが出来る。唯一の判断基準はその暗号が FIPS に採用されているかどうかである。インタビューした米国政府職員は残念ながら FIPS 標準が ISO/IEC 標準とどのように対応が取れるのかといった記録を持っていなかったため、ISO/IEC 標準に含まれない暗号が使われている実例を挙げることは出来なかった。

2.1.5. 電子政府における ISO/IEC 暗号の利用

インタビューした米国政府職員は FIPS と ISO/IEC の対応表を持っていなかったが、FIPS で採用されている暗号のほとんどは ISO/IEC 標準になっているという認識を示した。
一例を挙げれば米国政府が使用している AES は ISO/IEC 18033-3 に採用されている。

2.1.6. 電子政府システム向け暗号製品のサプライヤ

電子政府の暗号製品納入事例

会社名：Entrust
製品名：GetAccess
アプリケーション：財務省のセキュア・ウェブ・ポータルの認証に使われている。

会社名：Entrust
製品：(製品名は不詳)　ディジタル署名のソリューション
アプリケーション：労働省

会社名：VeriSign
製品：VeriSign’s managed PKI
アプリケーション：内務省土地管理局の電子認証

2.1.7.　電子政府のシステムインテグレータ

電子政府のシステムインテグレーション事例

会社名：CygnaCom (Entrust の 100%子会社)
製品：Entrust、VeriSign、HP および IBM Trust Authority が供給する PKI システム
アプリケーション：エネルギー省の PKI ディジタル署名

会社名：Enspier Technologies
製品：製品名不詳
アプリケーション：労働省運営管理補佐官の連邦識別管理イニシアティブ

会社名：ORC (Operations Research Consultant)
製品：製品名不詳
アプリケーション：総合サービス局調達サービスの電子提案と電子変更システム

2.2. 米国の暗号政策

2.2.1.　暗号技術政策を主管する政府機関

前節で概要を述べたとおり、国の暗号標準を決め、実装してゆく役割を負った組織はいくつかある。最も主要な役割を果たすのは NIST の傘下にある STG（Security Technology Group）[1]である。但し、STG は技術的な情報を政策決定のための準備をするが、政策の決定者ではない。
多くの国で軍事用及び非軍事用暗号が同一の組織で扱われている。しかし、米国では軍事と非軍事では明確な線引きがされ、軍事用暗号は NSA（National Security Agency）が扱い、非軍事用暗号は STG が扱う。暗号政策や標準の開発途中では、NSA から STG へ情報が供給され、共同作業をすることもある。例えば、楕円曲線の開発では、STG は NSA と密接な協力を行った。NSA はしばしば国際標準化機関で米国を代表することがある。
インタビューは STG 職員にのみ行ったので、以下の記述は STG だけをカバーしている。

組織名称：Security Technology Group (STG)

目的と使命：

[1] STG
http://csrc.nist.gov/pki/

- 暗号アルゴリズム、認証機構、およびセキュリティ基盤といったセキュリティのツールに責任を持つ。
- 認可された暗号とその実装に関し、標準およびガイドラインを開発する。
- STG は連邦 PKI の開発と標準化を主導する。

政府部内における位置づけ:

STG は NIST のコンピュータセキュリティ・ディビジョン（CSD）に置かれている。CSD は調査・研究によって情報システムのセキュリティを改善し、各省庁に IT セキュリティに関する助言を行い、標準やガイドラインを開発する。STG は CSD の 4 つのプログラムのうちのひとつである。他の 3 つとは、セキュリティ試験、セキュリティ研究と最新技術、およびセキュリティ管理と指導、である。

一方 CSD は NIST の情報技術研究所（ITL）の傘下にある 8 つの研究所のひとつだが、ITL は商務省（DoC）の技術管理局(TA)の一部でもある。

暗号政策への関与:

- STG は世界中で開発中の暗号（基本アルゴリズムと重要なアプリケーション）のレビューと分析を行う。
- 重要なプロジェクトの分野
  - 認証
  - バイオメトリクス
  - 公開鍵基盤
  - 暗号化が可能なアプリケーション
- 歴史：初期の歴史については情報を得ることが出来なかった。STG の地位は FISMA (Federal Information Security Act 2002) によって急激に上がってきた。FISMA ではすべての連邦政府省庁は IT セキュリティ製品に承認された暗号モジュールとアルゴリズムを使うことを義務付けている。
- 拠点：ワシントン DC
- 職員数：15 名
- 予算規模：不明
- 最近の活動：
  - 個人の識別と証明（PIV）を FIPS 201 として制定 （大統領令 12 が発行された 2004 年 8 月から標準が制定された 2005 年 10 月まで）
  - NSA と協力して、将来 ECC の基づいた記録が使われることを念頭に置いた楕円曲線暗号の開発をレビュー
  - 攻撃によって破られる可能性がある SHA-1 アルゴリズムを除去
  - FIPS 140-2 の次の版（FIPS 140-3）に更新
  - 連邦 PKI 基盤の開発と実装

2.2.2. 国内推奨・標準暗号の選択方針と手順

NIST は 5 年ごとにアルゴリズムと暗号標準を見直すことを要求している。実際に STG は次のような継続した活動をおこなっている。

- 新しい暗号を開発するために内部の暗号専門家が継続的に作業を行っている。
- NSA と暗号開発の共同作業を行っている。

- NIST が支援する講演会、ワークショップあるいはセミナーを通じて世界中で開発された暗号のレビューを行っている。
- ANSI（American National Standards Institute）IETF、IEEE と協力して世界中の開発状況をレビューしている。
- 世界的な暗号学会がもたらす現行の暗号の弱点についての情報に応える。

STG が行っている様々な活動の例として、AES 暗号アルゴリズム開発のプロセスは独創的で将来の暗号開発のモデルケースと考えられる。以下に AES 開発の経緯を記す。

- 1997 年に NIST は AES 開発計画を発表。その年の後半に共通鍵暗号とブロック暗号のアルゴリズムが公募された。
- 世界中の暗号専門家、企業、学者がアルゴリズムを提案し、また、レビューに参加するよう会議が招集された。
- STG の暗号専門家グループが提案したのは、ブロックサイズが 128 ビットで鍵の長さが 128、192、256 ビットの暗号であった。
- 提案されたアルゴリズムは 1 年後に NIST AES 暗号候補の会議で発表された。
- 会議では公開コメントを歓迎すると同時に政府広報でも発表がされた。
- 第二回目の会議を開き、公開コメントや内部での分析結果をもとに討議が行われた。
- こうしてでてきた分析やコメントに基づき、NIST は最後の 5 つを候補に選択した。
- 第二回目のより詳細なレビューをこの 5 候補について行い、公開コメントや NIST 後援の非公式検討会が行われた。また、第三回目の AES 会議が召集され選択された暗号の製作者等が集まって検討を行った。
- 最後に NIST が決定を下し、ドラフト FIPS 標準を発表し、コメントを求めた。
- 最後に公開で求めたコメントをレビューし、必要な修正を加えた後に標準として承認され、商務省により認可された。

FIPS 201 個人識別の立証（PIV）の開発では一層標準開発プロセスが考慮された。以下にその経緯を示す。

- 2004 年 8 月付けの国土安全に関する大統領令 12（連邦職員と連邦契約職員の共通識別標準）が公布された。NIST は 6 ヶ月以内に標準を公布しなければならなかった。
- 2004 年 9 月に、PIV 標準に関する案が PIV ウェブサイトで公開された。
- 標準の検討を行うために 4 回のワークショップが開かれた。（その内 1 回は政府関係者のみが参加。）
- 公開レビューのためにドラフトが公布された。
- 内部ではスマートカードに関する省庁間のアドバイザリー委員会と連邦識別委員会に諮問した。
- さらに、国務省、国防省、科学技術政策局、行政管理予算局、国土安全省、司法省に対し諮問した。
- この結果 90 の組織から 1900 のコメントを受け、それを反映した。
- 標準は 2005 年 2 月に商務省から発表された。

NIST は、ベンダやシステムインテグレータに対し、ガイドラインとして多くの出版物を交付する。

- 暗号標準（FIPS 刊行物）
- セキュリティ・ガイドライン（標準の安全な実装を呼びかける SP（Special Publication） 800 シリーズ）

- ガイドラインや標準のドラフト（ユーザーがレビューの段階でコメントを付け易いように提案された変更と共に標準のドラフトを公布する。）
- CMVP により暗号をテストするためのガイドライン
- 証明されたベンダや製品のリスト（CMVP プログラム）

NIST は DES のみならず、SHA-1 および FIPS 171(キーマネジメント。この標準は ANSI X9.17 に基づいているが、これは既に撤回されている）を廃却しようとしている。以下の DES に関する経緯から、NIST が古くなったアルゴリズムの撤回と廃却をする場合のプロセスが説明できる。

- NBS (National Bureau of Standard、現在の NIST) が 1977 年に DES を制定した。
- NSA は、1990 年代半ばまでにはこの暗号を破ることが可能であると判断した。 公開鍵方式開発者の一人であるスタンフォード大学の Martin Hellman 博士は DES の問題をより強力な計算機が現れた場合について議論した。
- この警告に対応し、NIST は 1997 年に DES を置き換えるアルゴリズムを募集した。一方 DES は 1998 年までに破られてしまった。
- DES の後継である AES 標準は 2001 年に制定された。
- 2004 年 9 月に商務省が DES の公式な撤回を求めた。この発表は Federal Register に掲載された。
- 2005 年 5 月 NIST は商務省の承認の下に DES の移行方針を発表した。
- この移行方針は以下の指示を含んでいる。
  ･DES を使う場合は Triple DES の一部としてのみ認める。
  ･省庁はより強力なアルゴリズム、例えば AES へ移行することを推奨する。
  ･過渡期間は 2005 年 5 月から 2007 年 5 月までである。
  ･この過渡期間中に DES を使用するシステムは、認識されていなければならない。
  ･渡期間終了後 DES 標準は FIPS 140-2 Annex A からはずされる。

2.3. 電子政府での暗号製品の調達

2.3.1. 暗号製品調達の政府方針と手順

米国政府が暗号製品を調達する場合、次の法律が適用される。

- FISMA 2002[1]：この法律では各省庁は連邦の情報システムには、NIST 標準および勧告に従うことが義務付けられている。
- OMB の公告 A-130 Appendix III[2]（連邦政府の情報自動処理資源の安全）では諸省庁がセキュアなシステムに責任を持つことおよび暗号を使用することが述べられている。

各省庁の責任

- セキュリティポリシーを制定し、業務内容に見合ったセキュリティのレベルを決めること。
- NIST のガイダンスに従ってリスクレベル及び被害規模に応じた十分なセキュリティを達成すること。

[1] http://csrc.nist.gov/policies/FISMA-final.pdf
[2] http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

GSA（General Services Administration）[1]の責任

- 自動情報処理機器を調達する場合は、配慮すべきセキュリティに関するガイダンスを用意すること。
- コスト効率が許す限り、GSA は各省庁が特定のセキュリティ・サービスを調達する場合の省庁横断的契約手段を確立すること。

NIST の責任

- 連邦政府システムに暗号を実装する場合のガイドラインを用意する。
- 暗号モジュールの試験と実証サービスを用意する。
- 認可した暗号モジュール、アルゴリズムおよび暗号製品のリストを用意すること。

暗号選定の手順

各省庁は以下のガイドラインに従ってセキュリティレベルを決定する。

- 脅威およびリスク環境
- コスト効率
- 保証レベル
- セキュリティ機能の仕様

各省庁は NIST のリストに従い、既認可暗号モジュール及び製品を見つける。

- CMVP リストから実証済み暗号モジュールを探す。
- NIAP／コモンクライテリア[2]のリストから認可済み製品を探す。

GSA プロセスでは次のことが要求される。

- IT 製品および IT の個別分類に対応する既認定供給者に対しスケジュール 70 を適用する。（すなわち、E-認証）
- 製品の適合性に関するガイダンスを用意する。
- 購買のための複数手段を用意する。
  - E-Offer（電子入札）
  - 直接調達
  - GSA を通じた紙ベースの通常購入

電子政府向け暗号アルゴリズムの標準と勧告

標準の目的

NIST 標準に適合する製品を使って最高レベルのセキュリティを確保する。

強化の方法

- OMB は、適時に各省庁が標準を適用し標準に適合すること、に対し責任を持つ。
- 連邦各省庁は毎年 FISMA 報告書を OMB に提出し、それぞれがセキュリティ要求を満たしていることを明らかにしなければならない。

2.3.2. 電子政府のための推奨･標準暗号アルゴリズム

暗号

- AES

[1] http://www.gsa.gov/Portal/gsa/ep/home.do?tabId=0

[2] NAIP/コモンクライテリア
http://niap.nist.gov/

- Triple DES
- Skipjack

メッセージ認証

- MAC
- HMAC

ディジタル署名

- DSA
- RSA
- EC-DSA

ハッシュ関数

- SHA-224/-256/-384/-512（SHA-1 は現在削除プロセスにある。）

2.3.3. 電子政府での暗号製品利用の現状

データ暗号化とディジタル署名

- 製品：Pitney Bowes Cygnus X-1 ポータルセキュリティ装置
- アルゴリズム：Triple DES、ECDSA、DSA、SHA-1
- 機能：暗号化、復号、ディジタル署名
- システム：USPS 郵便料金メーター

PKI ブリッジ

- 製品：Entrust Authority PKI
- アルゴリズム：ディジタル署名のための ECDSA
- 機能：ディジタル署名と暗号化
- システム：安全に部局間で通信ができるための PKI 認証をおこなう「PKI ブリッジ」。「PKI ブリッジ」は「GSA 連邦技術サービス」により運営されている。

2.3.4. 電子政府での推奨･標準、非国際標準製品に対する方針

米国連邦各省庁はそれが国際標準であるかどうかに関わらず、米国標準を使わなければならないとしている。

2.3.5. 電子政府での推奨･標準でない暗号を使用した国際標準製品に対する方針

米国連邦省庁は米国標準を使わなければならないとしている。

2.4. 暗号の国際標準に関する方針

2.4.1. 暗号の国際標準に関する政策

電子政府と電子商取引

インタビューを行った米国政府職員は電子政府と電子商取引に対する違いを次のように述べた。すなわち、電子商取引に関する限り米国は国際標準の適用を積極的に支持する。一方、電子政府システムは国益のために最良のセキュリティを実現しなければならない。

以下に述べることは国際標準と電子政府の情報システム及び暗号との関係である。

注記：米国政府は ANSI を情報システム分野の正式な ISO/IEC 代表としている。ANSI は商務省ならびに、国際及び国内の主要な標準化機関と密接に協力している。ANSI は INCITS（InterNational Committee on Information Technology Security）[1] のメンバーとなっている。一方 ANSI は ISO/IEC の米国代表であり、ISO/IEC JTC 1/SC 27 情報技術セキュリティ委員会のメンバーである。INCITS は NIST および CSD と特に緊密な協力を行っている。

情報システム全般

- 国際標準は電子政府システムの開発に有用ではあるが、必ずしも必要ではない。
- 商務省は国際標準に責任を持ち、その傘下の ANSI は ISO/IEC の情報システム標準化に対し、他の多くの組織と同様積極的である。
- 米国は WTO の「TFT（通商に対する技術的障害）条約」を遵守する。

暗号

- 電子政府システムにとって暗号の国際標準は有益かもしれないが必要ではない。
- 現実的には NIST の CSD 傘下にある STG は暗号開発を行っているが、IETF や IEEE および ANSI と密接に協力をしている。これらの人たちは ISO/IEC JTC 1/SC 27 の情報セキュリティについては絡んでいない。
- CSD のほかのグループが ISO/IEC と密接に仕事をしている。
- INCITS CS1 は ANSI に加わっていて、したがって米国の SC27 情報セキュリティの代表になっている。INCITS CS1 の議長は NIST の上級職員が務めている。

米国暗号と国際暗号の扱いの違いに対する方針

- 出来る限り米国は米国標準を奨励する。
- 米国は WTO の「TFT（通商に対する技術的障害）条約」に署名し、その一般原則を支持する。しかし、電子政府の暗号標準に関しては米国標準が優先である。

ISO/IEC 19790 に対する取組み

ISO/IEC 19790 は FIPS 140-2 に対応する。米国は FIPS 140-2 を変更し ISO/IEC 標準に変換できるようにする。

[1] INCITS
http://www.incits.org/

2.4.2. 国際暗号標準化活動

NIST の CSD が行っている活動は以下のとおりである。

ISO/IEC
FIPS 140-2 に ISO/IEC 標準への変換を可能にするよう訂正をしている。

- ISO/IEC の用語と定義の取込み
- ISO/IEC 参照の挿入
- EMI/EMC 項目の削除（これは米国 FCC の要求事項）
- ISO/IEC 標準に合わせ乱数発生試験（RNG）を改定

NIST 上級職員の役割

- INCITS CS 1 の議長 （SC27 の米国代表）
- ISO/IEC JTC 1 の事務局
- ISO/IEC 19790 の編集者
- ISO/IEC 19790 Derived Technical Document の副編集者

IETF

- IETF SEC セキュリティ分野（IP プロトコル、S/MIME, X.509 を用いた PKI）への参加
- IETF SEC PKI X.509 ワーキンググループへの参加

IEEE

- P1700 情報セキュリティ保証アーキテクチャへの参加
- 802.11 委員会への参加

2.4.3. 電子政府での ISO/IEC 標準暗号の利用と計画

現在は無い。

2.5. 電子政府のサプライヤ

2.5.1. Entrust

インタビュー相手：Entrust 社技術担当副社長

所在地：本社―カナダ、オタワ、インターナショナル本社―テキサス州ダラス

暗号事業の内容：

ID 管理および PKI，ディジタル署名のソリューション、認証、暗号化によるデータ保護、およびシステムインテグレーション（これは子会社の Cygnacom が担当している。）

電子政府納入実績：

- 米国 PKI を用いたインターネット利用
- カナダ
  - カナダ政府の IT セキュリティ基盤である「セキュアチャネル」に PKI を納入、

- ID 管理のソリューション PASS を納入し、下記の組織で使われている。
  - 退役軍人局
  - カナダ警察
  - 統計局
  - 運輸省

政府標準あるいは推奨暗号について

ビジネスへの影響：

基本的には政府が望むアルゴリズムを製品化するつもりであるが、すべての要求に応えることは出来ない。要求の度合いが強いかあるいは需要があるレベルに達しないと応じることは出来ない。現在は要求を満足していると考えている。

標準・推奨暗号の選択プロセスへの関与：

現在は SHA-1の置き換えと、新しい公開鍵の楕円関数アルゴリズムのアプリケーションに関与している。NIST および CSE と協力している。

政府のガイドラインに対する評価：

良いと思う。官・民協力という考えをしっかり持っている。

標準・推奨暗号の強制力：

ガイダンスに従っていない省庁は無い。しかし、それは我々の関心事ではなく、我々は出来るだけエンドユーザが選択肢を沢山もてるようにしている。一方製品は出来る限り標準アルゴリズムを使うような仕組みにしている。

電子政府等への納入実績

米国政府にインストールされた例

- パスポートの電子署名。米国政府は 2005 年中に百万枚の新しいパスポートを発行する予定であった。
- GSA (General Service Administration) によって承認された ID 管理ソリューション

カナダ政府にインストールした例

- 運輸省へ PKI 認証ソフトウェアを納入。
- TruePass を使った認証サービス、2006 年までにカナダ政府の 772,000 人に利用してもらう、
- 政府部内の「セキュアチャンネル」利用者数は 74%に達している

民間での納入実績

- 米国チェースマンハッタン銀行の ECGateway™ に PKI システムを納入。また、ブルーシールドに e-Pass を納入した。
- カナダマッケンジー証券に「セキュアチャンネル」を納入した。

推奨・標準暗号の選択

米国とカナダでは選択のプロセスに大学の暗号研究者や民間企業の暗号開発者を参加させている。この方法は良い暗号を作り出すのに役立っている。

ISO/IEC 標準

我々の暗号製品は ISO/IEC に広く対応している。たとえば PKI 製品では FIPS, IETF, ANSI, ISO/IEC の標準に準拠している。国際標準は相互運用性を高めると信じている。しかし、積極的に ISO/IEC 標準製品を作ろうとしているわけではない。

2.5.2. Certicom

インタビュー相手：製品開発部門上級役員

所在地：1800 Alexander Bell Dr Suite 400 Reston, Verginia 20191, USA
事業内容：暗号製品製造およびコンサルティング
暗号製品：暗号モジュール、セキュリティ・アーキテクチャ、コンサルティング・サービス
電子政府納入実績：現在米国政府むけに製品を作っている。

政府推奨・標準暗号について
国際標準製品は CC の認可を受けている場合は使えるが、暗号のモジュールレベルでは使うのは難しい。FIPS はほとんど国際標準と同じだと思っている。当社は暗号アルゴリズムの開発と、暗号モジュールの開発をしていて、NIST、CSE とは緊密な連携を保っている。

電子政府等への納入実績
- 連邦航空局（FAA）：Certicom Trustpoint/CA および Trustpoint/PKI Portal を航空管制官とパイロットの通信保護機構として認可した。
- 国家安全省（NSA）：Certicom の公開鍵を認可製品として、国のセキュリティ・アプリケーションに使用してよいと認許した。

民間での納入実績
- 携帯端末：当社の暗号モジュール（たとえば、GSE）は FIPS-140-2 認可製品として PALM OS や Windows CE に取り入れられ使われている。
- Sierra Wireless は Certicom’s movian VPN™ を自社のワイヤレスメールのソリューションである、Voq Mail Pro に採用した。

標準暗号選択への関与
Certicom は米国およびカナダ政府と緊密な協力をしている。Certicom の MQV プロトコルは NIST の推奨となり、SP 800-56 で公開鍵のひとつに取り入れられた。また、Certicom の楕円関数ディジタル署名（ECDSA）は FIPS 186-2 の 3 種類のディジタル署名のひとつになっている。

ISO/IEC 標準暗号について
我々は ISO/IEC 標準化活動にはあまり注目していない。それよりも IETF や ANSI の暗号標準化に関わっている。

3. カナダ

3.1. カナダの概要

3.1.1. 電子政府普及の状況

2004 年にカナダの電子政府（GOL あるいは Government-Online と呼ばれる）はアクセンチュアが 4 年前から始めた世界的な調査で第一位となった。アクセンチュアは成熟度、サービスの広さ･深さ、および、カストマー･リレイションシップ･マネジメントについて採点を行った。カナダの GOL は他の多くの国からも電子政府の役割モデルとして良いものだとみなされている。GOL は 2005 年までに最も普通に使われるサービスをオンライン化することを狙っている。
2004 年時点で GOL はおよそ 130 種類のサービスを様々なレベルの機能で提供しているが、それらは大まかに情報提供と業務処理とに分かれる。GOL のサービスの例を以下に示す。

- 雇用記録ウェブ（Web Record of Employment）によりカナダの企業は雇用保険を受けるための申請書類をオンラインで作ることが出来る。2004 年には 8,000 以上の企業の 46 万人に上る従業員登録がこのウェブサイトを使って行われた。
- 購買ボタン(Receiver General Buy Button)はカナダ市民や企業が政府から物やサービスを購入したときの支払いに使うオンライン決済システムである。265,000 件の支払いでで総額 20 百万ドルが決済された。
- カナダ市民は個人所得税をオンラインで申告できる。2003 年にはオンライン申告が40％であったが、2007 年までには 70％がオンライン申告を選ぶものと思われる。

電子政府のポリシーは「公共事業･政府サービス省（PWGS）」が管理しているが、電子政府のポリシーは財務省が預かっている。

3.1.2. 暗号政策の担当政府機関

カナダでは暗号政策に二つの部門が関わっている。

- CSE（Communications Security Establishment[1]）の一部門である ITS（Information Technology Security）
- CIOB (Chief Information Officer branch[2])

組織名称：ITS
組織の使命：ITS はクラシファイドおよび非クラシファイドシステムの暗号開発と承認に責任を持つ。また政府に情報セキュリティのソリューション（製品･サービス）を提供し、政府の情報

[1] http://www.cse-cst.gc.ca/
[2] http://www.ciob.org.uk/ciob/siteRoot/Regional/Branches/Canada/default.aspx?bid=40&bname=Canada

通信に係る脆弱性を分析する。サイバー攻撃を予測し予防する。通信のセキュリティについて研究する。

政府の中の位置づけ： CSE の二つの部局の一つで、もうひとつの部局は諜報情報収集を任務としている。CSE 自体は国防省に属している。

暗号政策に関する役割：ITS は国の暗号標準に技術的な情報を提供することである。

組織名称：CIOB
組織の使命：IT および IT セキュリティと暗号標準ならびに政策の開発
政府部内の位置づけ：CIOB は財務省の 16 部局のひとつである。
暗号政策に関する役割：非クラシファイド政府情報システムに対し、暗号標準や暗号政策を用意する。

3.1.3. 電子政府システムでの暗号の使用

カナダ政府は暗号とアルゴリズムのリストを承認しているがオンラインサービスを構築する場合省庁がこのような推奨暗号や認証製品を使うことは要求されていない。

暗号は GOL でよく使われているセキュリティツールである。暗号は以下のような使い方をされている。

- PKI あるいは電子認証
- 暗号化
- ディジタル署名
- ハッシュ関数
- データ保護（メッセージ認証）

暗号使用の代表的な例

- PKI 電子認証
- セキュアチャネル：これは GOL のインフラであり、PKI, ディジタル署名およ認証で構成される。
- 政府の PKI システムはセキュアチャネル内で動作する。
- ePass と呼ばれるディジタル署名ベースの認証が GOL の 85%の業務処理で必要となる。
- 暗号はディジタル署名と双方向のデータ暗号化に使われる。

暗号を使う具体的なアプリケーションの事例は以下の通りである。

- カナダ人材及び技術開発(HRSD: Human Resources and Skills Development)は ePass を使ってオンラインで従業員記録ファイルを提出できる。
- カナダの放送および通信会社は ePass を使って当該省庁とオンラインで申請書や許可証をやり取りできる。
- カナダ税務省（Canada Revenue Agency）は ePass を使って納税者がオンラインで住所変更届を出せるようにしている。
- 退役軍人省は ePass を使って ID とディジタル署名の検証を行い、退役軍人が情報の利用や、手当ての申請を行えるようにしている。
- カナダ統計局は暗号ログインをセキュアチャネル経由でおこなっている。

3.1.4. 電子政府における ISO/IEC 標準暗号の利用

カナダ政府は GOL で使う暗号が ISO/IEC 互換であるかどうかといった暗号一覧表を提供することは出来ない。
一般的な方針は以下の通りである。

- カナダは国際通商を促進するために、ISO/IEC のような国際標準を支持する。また、標準が通商障壁とならないようこれらの標準をカナダの国家標準として認める。
- しかし、電子政府については電子政府システムに最適なツールを見出すことに重点が置かれる。国際標準は必ずしも電子政府のための標準開発に参照されないかもしれない。参照はむしろ米国の FIPS 標準となるが、これはしばしば ANSI 標準およびカナダがコモンクライテリア方式に沿って開発した標準に従っている。

カナダの ISO/IEC を含めた国際標準団体への加入は CSA（カナダ標準協会、Canadian Standard Application）が統括する。CSA は ISO/IEC JTC1/SC 27 への情報提供や役割分担などに CAC-ITS (Canadian Advisory Committee[1])を利用する。

3.1.5. 電子政府の暗号製品のサプライヤ

TEAM BCE はセキュアチャネルを用意するために政府と契約をした企業の団体である。この団体には以下のようなベンダやシステムインテグレータが加わっている。

- ベル・カナダ（BCE）：主契約者
- CGI：システムインテグレータ、アーキテクチャの監督
- エントラスト（Entrust）：キーとなるセキュリティ製品や PKI、認証、ディジタル署名 のような暗号モジュールの供給者。エントラストオーソリティ（PKI）や TruePass（認証とディジタル署名）などもこの会社の製品である。

カナダ政府は積極的な電子政府むけの暗号製品開発者育成プログラムを持っていて、以下のような項目が含まれている。

- 「ITS 製品既認定プログラム」は IT セキュリティ製品を政府が使用する場合、FIPS あるいはコモンクライテリアなどですでに認定されたものを既認定品として扱う。
- 「暗号承認プログラム」は FIPS 140-1/-2 で検証された製品の評価をおこなう。
- 「情報技術のセキュリティ評価及びリスクアセスメントプログラム」によりカナダ政府は下に示す 4 企業との間で「国家主供給契約(National Master Supply Arrangement)」を結んだ。
    - AEPOS Technology Corp
    - CGI Information Systems and Management Consultants
    - Cinnabar Networks
    - TRM Technologies

既認定製品の供給会社としては以下の企業が選定されている。

- Chrysalis-ITS Inc.
- ViaSafe
- Admiral Secure Products
- Eracom Technologies Group (最近 SafeNet に買収されたオーストラリアの企業、暗号化アクセラレータを作っている。)

[1] http://www.scc.ca/en/nss/success_stories/storydetails_10.shtml

- SafeNet (暗号化アクセラレータ)
- nCipher (暗号化アクセラレータ)
- Pointsec Mobile Technologies (ディスク暗号化)
- Kasten Chase Technologies (ディスク暗号化および e-ビジネス・アプリケーション・ツール)
- WinMagic (ディスク暗号化)
- Cisco (e-ビジネス・アプリケーション・ツール – 侵入検知)
- Logistics Software Corp (e-ビジネス・アプリケーション・ツール-インターネット・ゲートウェイ・エクスチェンジ; カナダ税関が貨物の運送業者データ交換用に使っている EDI のゲートウェイ)
- Okiok (e-ビジネス・アプリケーション・ツール- シングルサインオン)

3.2. カナダの暗号政策

3.2.1. 暗号技術政策を主管する政府機関

カナダでは二つの部門が非軍事目的の暗号生成に責任を持っている。

- 財務省 (TB) の情報局 (CIOB) が情報セキュリティと暗号に関する標準と政策に対し責任を持っている。
- CSE の一部門である ITS が暗号アルゴリズム、製品、その他セキュリティ関連製品の分析と検定に責任を持っている。ITS は暗号政策の専門家であるとみなされている。

他の組織で情報システムのセキュリティについて標準化や政策に関与する部門は、

- RCMP (Royal Canadian Mounted Police) 米国の FBI 相当[1]
- PWGSC (Public Works and Government Services Canada)[2]
- OCIPEP (Office of Critical Infrastructure Protection and Emergency Preparedness)[3]

CIOB の任務と責任

CIOB は IT および IT セキュリティの標準と政策に責任を持つ。政策に責任を持つ部門は IPSP(Information, Privacy, and Security Policy) 部門で標準に責任を持つのは
EAS (Enterprise, Architecture and Standards) 部門である。これらの部門が ITS (Information Technology Security) プログラムを推進している。

組織名:IPSP 部門
使命:

- ITS の運用と技術に関するガイドを作る。
- 情報技術のセキュリティに関して戦略的な助言を行い、政府機関に対し政策やガイドライン及び標準を用意する。
- カナダ政府の情報、プライバシー、及び情報セキュリティ政策と標準について監視と更新を行う。

[1] RCMP
http://www.rcmp-grc.gc.ca/index_e.htm
[2] PWGSC
http://www.pwgsc.gc.ca/text/index-e.html
[3] OCIPEP
http://www.psepc-sppcc.gc.ca/abt/in-en.asp

政府部内の位置づけ：CIOB の 9 部局の内のひとつ
暗号政策への関与：

IPSP は MITS（Management Information Technology Security）について運用ガイドをつくる。この中には暗号使用に関するポリシーが述べられている。

- 暗号はあるアプリケーションでは必ず使わなければならないが、ほかのアプリケーションでは予防策として薦める程度である。
- 識別と認証は必ず使用しなければならず、より強固な認証が必要な場合は、暗号を使った認証を薦めている。

歴史／職員数：情報を入手できず。
所在地：カナダ、オンタリオ州オタワ

組織名：EAS 部門
使命：

- 政府のセキュリティポリシーを支援するために、IT セキュリティ、標準、情報技術の開発に責任を持つ。
- 政府認可の標準利用者に統一窓口を用意する
- カナダ政府内の情報技術セキュリティ標準について行われるすべての作業に対し、重点目標を与える。

政府部内の位置づけ：CIOB の 9 部局の内のひとつ
暗号政策への関与：カナダ政府内で情報セキュリティ標準化の調整を行う。
歴史／職員数：情報を入手できず。
所在地：カナダ、オンタリオ州オタワ

組織名：ITS チーム
ITS は CSE 内の組織である。
使命：

- カナダ政府の情報システムで処理されるアプリケーションの保護、認可及び認証に使う暗号アルゴリズムの評価と承認をおこなう。
- 情報セキュリティのソリューション（製品・サービス）を政府のために準備する。
- 政府の情報通信に関する脆弱性を分析する。
- サイバー攻撃を予測し予防する。
- 通信のセキュリティを研究する。

政府部内における位置づけ：

- ITS は CSE の一部門である。CSE はカナダ政府の機密文書や保護すべき文書を暗号化すること、及び暗号キーの管理に対し責任を持つ。CSE の米国における相当部門は NSA (National Security Agency)である。

暗号政策への関与

- PKI の実装を調整する。
- カナダ企業と共同で必要な暗号製品の開発をおこなう。また、米国の NIST と共同で「暗号モジュール評価プログラム（CMVP）」を管理する。
- カナダのコモンクライテリアチームに場所を提供する。
- 政府職員にセキュリティ教育とトレーニングプログラムを用意する。
- 連邦政府のために情報通信システムの運用標準の開発を支援する。
- 政府機関が上記の標準を達成できるよう助言とガイダンスを提供する。

歴史：

- 機密文書の保護および保護された情報の保護という二つの役割があるが、CSE の歴史的な根源はカナダの諜報機関である。

- CSE は 1964 年に CBNRC (Communication Branch of the National Research Council) として作られた。 1975 年に CSE と名前を改め、国防省の傘下に入った。ITS はさらに、2001 年に成立した「反テロリスト法（Anti-terrorism Act in 2001）に基づいて改編された。また、この法律により、CSE の役割、責任、及び機能が規定されている。

所在地：Ottawa, Ontario, Canada
職員：1450 名（2005 年 9 月現在）
予算：$200M（カナダドル）

3.2.2. 政府調達における推奨･標準暗号の選択方針と手順

暗号選択の方針

アルゴリズムはカナダ政府 IT セキュリティ基準に適合しなければならない。

選択プログラム

- CIOB の中にある多組織会議に対し技術的評価や試験結果を提供する「ITS セキュリティプログラム（ITS）」がある。
- CIOB はカナダ政府各省庁、内部専門家のキーグループ、ITS 専門家、電子政府サービスを行っている各省庁の IT セキュリティ専門家などからの報告をまとめる。
- 多組織会議は ITS の勧告に従って新しいアルゴリズムを決める。

選択基準

- 米国 FIPS 140-1/-2 標準に合致する
- CC（コモンクライテリア）標準に合致する
- 政府への主要な供給者である Entrust がサポートしている
- ISO/IEC 標準である

選定と評価手順

- カナダ政府内の関連組織は、それぞれが利用中のアルゴリズムの評価を行う。
- ITS はアルゴリズムの評価と試験で主導的に活動する。
- 提案された新しいアルゴリズムについての情報は CIOB に提出される。
- CIOB は認可を行う。

情報製品ベンダやシステムインテグレータへの公表とガイドライン

- ITS は認可したアルゴリズムと製品のリストを維持する。
- ITS は民間及び政府部門と次のような方法で連絡をとる。
  - ITS アラート：直ちに対応が必要な緊急情報
  - ITS セキュリティ公示：新しい製品や廃止品、新しい COMSEC 手順、講習会予定、講習内容、FAQ などを定期的に発行する。
  - IT セキュリティ指示：民間および政府省庁にたいする CSE に関係するレベルの高い長期にわたる指示
  - ITS セキュリティ･ガイドライン：技術的な指示をふくむガイドライン
  - ITS セキュリティ製品報告：ITS の一般的な知識や原理および実践情報で ITS の専門家に市場での技術開発状況を知らせる報告

3.3. 電子政府での暗号製品の調達

3.3.1. 暗号製品調達の政府方針と手順

カナダ政府の調達に関し、能率的な方式が開発され「オンライン政府に関する法的ならびに政策的枠組み」が定められた。それによれば次の手順で購買が行われる。

- 購入要求を MERX システム[1]にポストする。
- ベンダはオンラインで提案を出し、評価を受け、契約を結ぶ。

MITS によれば「各省庁は ISO/IEC 15408 (コモンクライテリア)により認可された製品を利用しなければならない。MITS はクラシファイド情報及び保護レベル C（非クラシファイド情報の中で最もセキュリティレベルが高い）の情報は CSE が許可または認証した暗号を用いなければならない、と決めている。しかし、インタビューのなかで政府関係者は、法的には CSE が認許した暗号を使用するよう求められてはいない、と語った。
「オンライン政府に関する法的ならびに政策的枠組み」ではセキュリティが必要な場合は PKI を使うことを決めていて、PKI のインフラは PWGSC[2]が運用するセキュアチャンネルによって実装される、としている。この PKI のインフラは Entrust によって運用されているが、諸省庁は PKI インフラおよびセキュアチャンネルに属するベンダが供給する製品を使うようにとは要求されていない。

3.3.2. 電子政府のための推奨･標準暗号アルゴリズム

カナダ政府は「オンライン政府に関する法的ならびに政策的枠組み（Canada's Legal and Policy Framework for Government On-line）[3]」を決めた。しかし、FISMA のように政府でのセキュリティを規定するような法律は制定されていない。MITS (Management of Information Technology Security)は FISMA 2002 に似ているが、法的な規制力はない。

CSE は政府内部で使用する暗号について暗号アルゴリズムを認可し、2003 年 4 月 1 日付けでアラートを発行した（ITSA-11(b)）。対象とする範囲は暗号アルゴリズム、鍵確立、ディジタル署名、ハッシング、パッディングスキームおよびデータ保護アルゴリズムである。
DES については危殆化を認め、2005 年までにすべて段階的移行をすることを求めている。

- 暗号アルゴリズム: AES（鍵長 128, 192, 256 ビット）、Triple DES、CAST5(鍵長 80, 128 ビット)、SKIPJACK
- 鍵確立アルゴリズム：RSA、KEA、Diffie-Hellman のような指数暗号、及び楕円曲線アルゴリズム
- ディジタル署名：RSA、DSA、El-Gamal のような指数アルゴリズム、ECDSA
- ハッシュ関数：SHA-1, SHA-224/-256 /-384 /-512 (但し SHA-1 は 2008 年までに段階的に移行)
- データ保護アルゴリズム：HMAC

---

[1] MERX
http://www.merx.com/English/nonmember.asp?WCE=Show&TAB=1&State=1&hcode=DSmmOnl5zU6FVjU16CWLSQ%3d%3d

[2] http://www.pwgsc.gc.ca/text/index-e.html

[3] http://www.solutions.gc.ca/pki-icp/gocpki/frame/frame00_e.asp

- 鍵確立パディングスキーム：RSAES-PKCS1-v1_5、RSAES-OAEP
- ディジタル署名パディングスキーム：RSASSA-PKCS1v1_5、RSAES-PSS

3.3.3. 電子政府暗号製品利用の現状

セキュアチャネル

PKI、ディジタル署名、認証、および暗号化には Entrust 製品を使っている。Entrust は米国標準、カナダ標準、ISO/IEC 標準など幅広い製品を持っているが、各省庁はその中から、望むものを選んでいる。その利用例としては以下のシステムがある。

- サービス・カナダ
  雇用保険のオンライン加入のための認証と暗号化。
- ACOA（Atlantic Canada Opportunities Agency）
  オンラインでビジネスを行う。
- カナダ統計局
  2006 年の国勢調査は PKI を利用し、オンラインで行うよう働きかけている。
- カナダ通関
  パスポート申請をオンラインで行う。

3.4. 国際標準暗号に関する方針

3.4.1. 暗号の国際標準への対処政策

カナダは ISO/IEC JTC 1 を強力にサポートしている。暗号関係では SC 27（IT セキュリティ）、SC 37（バイオメトリクス）及び SC 17（スマートカード）で活動をしている。

SC27 のカナダ代表にインタビューしたところ、国際標準への対応について次のように述べた。

- 政府は暗号標準についてその場合ごとに最適なものを選択する。しかし、暗号の国際標準化は重要であり、ビジネスの取引のみならず、政府間でも相互運用性が必要である。同時に暗号ベンダが複数の政府と取引する場合の負荷についても考慮しなければならない。

一方、CSE の CMVP 責任者は次のように述べた。

- 電子商取引と電子政府とは、はっきり分けて考えるべきである。電子商取引では相互運用性が鍵となるので、国際標準が必要となる。しかし、電子政府では、政府にとって最も利益になる選択をすべきである。

カナダが独自の暗号を選択した事例は CAST5 および SKIPJACK である。CAST5 は Entrust が開発した暗号だが、カナダ政府がセキュアチャネルに Entrust を採用した時、CAST5 を正式な認可暗号として採用した。CAST5 は FIPS 140-2 で認可されたはずである。また、SKIPJACK は米国の NSA が開発した暗号である。NIST にインタビューした時に面談者は次のように語った。「NSA は時々非常に丁重に NIST に対して NSA が開発したアルゴリズムを採用するように働きかけてくる。自分にはなぜ NSA が SKIPJACK を NIST 認可アルゴリズムにしたいのかわからない。NIST は AES に重きをおいているので SKIPJACK は余り使われていないのではないか。」数年前にカナダは CAST5 を

ISO/IEC 標準にしようと運動したことがある。だが、そのほかにはカナダ標準を ISO/IEC 標準に合わせようという努力はされていない。

3.4.2. 国際暗号標準化活動への対応

ISO/IEC に対する方針と活動

ISO/IEC JTC 1/SC 27 へは CAC-ITS（Canadian Advisory Committee for Information Security）が代表として出席している。この委員会の議長は Alice Sturgeon (EAS ディレクター)が務めている。カナダの SC 27 における貢献実績は以下のとおりである。

- WG1： ISO/IEC TR 13335 および ISO/IEC 17799 改定でリーダシップをとった。
- WG2：ISO/IEC 18031 のドラフトスタンダードで主編集者を務めた。
- WG3: ISO/IEC TR 15443-1/-3 のドラフトを編集した。

インタビューに対し、国際標準化活動への対応に対する考え方が次のように示された。

- それぞれの標準化団体が異なった役割を担っている。例えば IETF が電子政府での PKI 標準（X.509, IETF PKIX）を作り、それを ISO/IEC が標準化している。
- 米国では FIPS がある。カナダは公式に米国 NIST と協力し FIPS 140-2 を暗号実証基準とした。

ITU-T の活動の多くのものは IETF に、ひいては ISO/IEC に取込まれている。したがって、カナダが ITU-T で何をしたかということを定義するのは難しい。

4. 英国

4.1. 英国の概要

4.1.1. 電子政府普及の状況

英国では内閣官房室（Cabinet Office）が英国政府の電子政府政策についての政治的責任を持っている。内閣官房室内の電子政府局（e-Government Unit: eGU）[1]が電子政府計画を推進し、IT 戦略や政策の策定を担当している。

電子政府局の中で、e-Delivery Team (EDT)が中央および地方政府に製品やサービスを提供し、インターネットが国民・市民と政府とのやり取りの主な手段となるようにしている。EDT は、Direct.gov.uk という市民情報ポータルや政府ゲートウェイ・セキュア・トランザクション・ハブ（the Government Gateway secure transaction hub）[2]などのような国レベルの電子政府基盤の主要な部分の運用に責任を持っている。政府ゲートウェイは、インターネット上で安全に認証された電子政府トランザクションを可能とするように 2001 年 2 月に立ち上げられたセンター登録・認証のエンジンである。ユーザーはこのゲートウェイに登録して、オンライン行政サービスを使ったり、政府各部門とのやり取りを安全にできるようになる。ゲートウェイは現在 25 の政府部門から 100 以上のオンラインサービスを提供している。個人や法人が利用可能なオンラインサービスの例は以下である。

- 税金や国民保険料の支払い
- パスポート、ビザ、運転免許証の申請
- 国民年金見積
- 貿易産業省（DTI）輸出許可証の申請
- 付加価値税や源泉徴収税の還付

英国の国民に提供されている電子政府サービスのリストは eGovernment Observatory で公表されている。[3]

2004 年のヨーロッパにおけるオンラインサービスやインターネットの使用状況を比較分析した Eurostat の統計（Online Availability of Public Services: How is Europe progressing）[4]によれば、英国は 25 カ国の EU 加盟国中、電子政府サービスの企業による利用の調査において、最下位であった（章末の文献を参照）。ヨーロッパ全体平均で 45%の企業が電子政府サービスを使ったことがあるのに対して、英国では 3 分の 1 以下であった。ヨーロッパで 45%の企業が電子政府ウェブサイトから書類フォーム類をダウンロードしたのに対して、英国の企業は 27%で、わずか 11%が政府のオンラインのフォームを使ったに過ぎない。英国の国民のうち、政府のオンライン情報を取得したことがあるのは 5 分の 1 に過ぎず、政府ウェブサイトから書類フォーム類をダウンロードしたことがあるのは 7%だけであり、実際にオンラインのフォームを使ったことがあるのはわずか 3%だった。

---

1 http://www.cabinetoffice.gov.uk/e-government/
2 http://www.gateway.gov.uk/
3 http://europa.eu.int/idabc/en/chapter/417/
4 http://europa.eu.int/information_society/soccul/egov/egov_benchmarking_2005.pdf

電子政府の普及が他国に比べて遅れているため、英国政府は情報通信技術を使って継続的に公共サービスを変革してゆくための戦略を策定し、2005 年 11 月に「技術により変革する政府(Transformational Government - Enabled by Technology)」[1]と題する新しい文書を発表した。新しいアプローチは、単に公共サービスをインターネットを介して提供するだけではなく、人々の生活に浸透してきている技術の進化を政府が最大限に利用することができるように大きな変化を狙った、もっと意味深長なものである。例えば、モバイル技術やデジタルテレビを介した公共サービスの近未来的な提供などが記述されている。

4.1.2. 暗号政策の担当政府機関

ハイテク犯罪対応から、企業に対する情報セキュリティの推進まで、英国の情報システム保護の全ての局面に、多くの重要な政府組織が関与している。これらの組織には、内閣官房室内の 情報保証中央スポンサー(Central Sponsor for Information Assurance：CSIA)、 内務省(Home Office),国家インフラストラクチャ安全調整局(National Infrastructure Security Co-ordination Centre：NISCC)、ハイテク犯罪ユニット(National Hi-Tech Crime Unit：NHTCU)、貿易産業省(Department of Trade and Industry：DTI)、通信電子セキュリティグループ(Communications-Electronics Security Group：CESG)[2]などがある。CESG は、政府通信司令部(Government Communications Headquarters：GCHQ) の情報セキュリティ実行組織であると同時に、軍事・非軍事用の暗号の公式使用に対して、国として許可を与える存在である。

CESG は Gloucestershire の Cheltenham に位置し、通信や電子データのセキュリティについてアドバイスや援助を提供することにより、英国の国益を保護・推進することを目的としている。公的な IT 通信の保護に関する全ての技術面を担当することに加え、コモンクライテリアや英国独自の IT セキュリティ評価基準である ITSEC に基づいて、IT 製品の公式な評価や認証を実施する、認定された認証機関(Certification Body)でもある。CESG は、以前は予算を全て中央政府から得ていたが、1997 年より殆どの情報セキュリティや保証サービスを有料で提供するコンサルティング組織となっている。

CESG Assisted Products Scheme(CAPS)[3]は、英国政府市場向けに特化したセキュリティ製品認証スキームである。CAPS は、政府および国防省ユーザーに対して、調達するセキュリティ製品が最高の基準で検証されたことを保証するものである。

4.1.3. 電子政府システムでの暗号の使用

CESG が推奨する、電子政府システム構築のための暗号アルゴリズムが、2005 年 9 日発行の eGIF(e-Government Interoperability Framework) の Technical Standards Catalogue, Version 6.2[4] にリストされている。

[1] http://www.cio.gov.uk/
[2] http://www.cesg.gov/
[3] http://www.cesg.gov.uk/site/caps/index.cfm
[4] http://www.govtalk.gov.uk/schemasstandards/egif_document.asp?docnum=957

- 暗号化—Triple DES、AES (FIPS 197)、Blowfish
- 電子署名—RSA、DSA、DSS (FIPS 186-2)
- 鍵配送—RSA、DSA
- ハッシュ関数—SHA-512, SHA-256 (FIPS 180-2)、下位互換性のため、SHA-1、および MD5 のサポートも推奨

CESG は、このアルゴリズムのリストは完全なものではなく、ダイナミックに追加･修正･削除されるものとしている。特定の実装やアルゴリズムについてのより詳細なアドバイスは、CSIA に問い合わせれば、提供される。

Catalog V6.2 では、また、スマートカードに ISO/IEC 7816-8 と ISO/IEC 7816-9 の使用を推奨しており、ISO/IEC 7816-11 と ISO/IEC 7816-15 の将来の採用を検討中としている。しかし、このリストも完全ではなく、セキュリティ関連の追加の規格は、2004 年 1 月発行の“Security Standards for Smart Cards Issue 1.1”[1]に含まれている。この文書によると、

- 暗号によるプライバシーの保護が想定される場合には、FIPS 140 が推奨される。FIPS 140 は、DES、Triple DES または AES の中から少なくとも一つを使用することを要求している。
- アクセス制限を伴った保護が必要な場合は、CESG Assisted Products Scheme (CAPS) を通じたベースライン承認か、CESG が認める他の方法が要求される。ベースライン承認を必要とする CESG 製品で使用が許されているアルゴリズムには、Triple DES、AES、そして TETRA システムで実装される一群の TETRA アルゴリズムが含まれる。
- 電子署名—CESG は FIPS 180-2 に詳細がある電子署名の規格を承認している。それには、DSA、RSA、そして ECDSA の 3 つのアルゴリズムが含まれる。
- ハッシュ関数—FIPS 180-1/-2, Secure Hash Stand (1995)によると、 SHA-1 (160 ビット)の ベースラインと強化グレードでの使用が CESG に認められている。
- 鍵配送—CES はベースラインとして Diffie-Hellman と MQV を認めている。
- 乱数生成—CESG はベースラインとして、FIPS 186-2 に従って FIPS 140-2 の乱数生成を要求している。
- エンティティ認証—FIPS 196 、ISO/IEC 9798 と Kerberos Network Authntication Service (V5) RFC 1510 が適切としている。

4.1.4. 電子政府における非 ISO/IEC 暗号の利用

高位の保護レベルには主に国産のアルゴリズムが使用されるが、殆どの電子政府システムはそのような高い保護レベルは要求していない。CESG Assisted Products Scheme (CAPS) 21 は政府が要求する暗号製品の商用開発を支援する。それにより、CESG が政府暗号基準に適合しているかを確認し、正式に政府や他の適切な組織での使用が認められる。CAPS が認める製品は、移動中のデータの暗号化（通信のセキュリティ）や蓄積されたデータの暗号化（例えばラップトップ PC の保護）だけでなく、文書の認証や個人認証のような他の仕組みを可能とする暗号にも及ぶ。CAPS スキームに依頼される製品評価は CESG が自前で行い、合格すれば政府使用許可が与えられる。HMG Infosec Standard No. 4 （英国政府情報セキュリティ基準 4 番：IS 4）は、通信におけるセキュリティと暗号化を扱い、通信傍受の観点からのシステム独自の脆弱性を定義している。CESG は国産アル

[1] http://www.govtalk.gov.uk/schemasstandards/egif_document.asp?docnum=839

ゴリズムについての詳細には触れていないが、それらが使われていると思われる暗号製品のリストを Directory of Infosec Assured Products 2005 April に公開している。[1]

4.1.5. 電子政府における ISO/IEC 暗号の利用

CESG は以下の ISO/IEC 暗号を電子政府で使用することを推奨している。

- ISO/IEC 9798（エンティティ認証用）
- ISO/IEC 7816-8 および ISO/IEC 7816-9（スマートカード用）
- ISO/IEC 7816-11 および ISO/IEC 7816-15（将来スマートカード用として検討中）

4.1.6. 電子政府の暗号製品のサプライヤ

Sun Software AG が政府ゲートウェイサービスにおける暗号製品を提供している。
Thales が CAPS で認証されたセキュリティ製品を提供している。
Geo Trust Europe と Equifax UK が政府オンラインサービスへのアクセスのための Secure Mark ディジタル証明書を提供している。

4.1.7. 電子政府のシステムインテグレータ

電子政府のシステムインテグレータとしては、BT Syntegra、Logica、ICL、 EADS や IBM などがある。

4.2. 英国の暗号政策

4.2.1. 暗号技術政策を主管する政府機関

CESG は英国における軍事的･非軍事的目的での公的な暗号利用に関して国レベルの許可を与える権威的組織であり、より一般的には情報セキュリティの技術的権威である。データ保護のための政府の政策を策定し、その実現について助言する。Gloucestershire の Cheltenham を本拠地とし、政府の通信本部司令部（Government Communications Headquarters ：GCHQ)のセキュリティ専門部隊として運営されている。暗号製品に対する顧客の要求に関して、幅広く様々なサービスを提供する。また、機密区分に関わらず全てのタイプの公式情報への承認された保護対策を提供する。CESG の主な顧客は、公式情報を扱ったり加工する人々で、通常は政府内の大小の部門や空軍、さらに政府から委託されて仕事をする機関や民間企業である。CESG は基本的にはこれら以外のセクターからのアドバイス要求に対してもオープンであるが、現在はそれを大規模に提供できる資源がない。CESG は、コスト回収ベースで運用されており、顧客特有のサービスは有料であるが、公的な組織に提供する一般的な当局のサービスは概ね無料である。CESG は一般的にはセキュリティ

[1] http://www.cesg.gov.uk/site/publications/media/directory.pdf

製品を製造せず、民間企業と協業して、政府のニーズを満たす幅広く適切な製品・サービスとそれらをサポートする基盤が確実に提供されるようにしている。

CESG の主要な活動分野には以下が含まれる。

- 暗号と実装技術の研究
- 汎用およびカスタマイズ暗号製品の設計と開発
- それらの製品の評価と認証
- ライセンスされた暗号製品の製造契約の締結
- CESG が設計した暗号製品の設計変更やアフターサービス、技術サポート
- 暗号アルゴリズムと集積回路の開発
- 英国政府市場のための暗号製品やシステムの商用リスクについて民間企業に助言
- 一度限りまたは緊急使用のセキュリティ機器の調達
- 政府プロジェクトでの市販暗号パッケージ製品の適切性、応用、インテグレーションについて中立的なアドバイス

CAPS(CESG Assisted Products Scheme)は政府の要求に対応する暗号製品の商用開発を支援する。政府環境の中で商用レベルの暗号が要求される場合に、その適用をサポートすることを CAPS の目的としている。CAPS に依頼された暗号製品の評価は CESG 内部で実施され、合格すれば政府使用の適合証が出される。

GCHQ 運営の年間予算は公式にはオープンになっていないが、およそ£800M と見られ、約 4,000 人のスタッフを抱える。CESG のスタッフ数やレベルおよび予算は明らかではない。

4.2.2. 政府調達における推奨・標準暗号の選択方針と手順

e-GIF(e-Government Interoperability Framework)[1] は政府および公共機関の中を流通する情報を統制する技術的方針および仕様を定義している。セキュリティは特に Security Framework Documents でカバーされている。CESG もまた数多くの情報セキュリティ規格（Infosec Standards and Memoranda）を作り、ガイダンスやポリシーを提供している。 HMG Infosec Standard No 4 は、通信セキュリティと暗号化を扱い、通信傍受の観点からのシステム特有の脆弱性を定義している。
CESG の暗号選択の手順の詳細は明らかではないが、CESG 内の Applied Security Technologies チーム[2]が関与していると見られる。このチームは 2000 年の始めに、政府サービスにおける新しい技術と英国の重要インフラ保護について調査・研究するために結成され、既存およびこれから出てくるセキュリティ技術の性質、メリット、考慮点についての知識と理解を拡大してきた。このチームの業務には以下のようなテーマが含まれる。

- PKI（Public Key Infrastructures）
- セキュアな業務アプリケーション
- セキュリティ技術の理解

このチームは、PKC(Identifier-Based Public Key Cryptography)の変更に関わっており、暗号の選択、再評価、廃棄についても重要な役割を果たすものと見られる。

---

[1] e-GIF
http://en.wikipedia.org/wiki/E-GIF
[2] http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=0&displayPage=0

CESG の暗号選択はまた、NIST の FIPS の手順をかなり踏襲しており、FIPS に採用された暗号を優先する傾向がある。

4.3. 電子政府での暗号製品の調達

4.3.1. 暗号製品調達の政府方針と手順

2002 年 9 月発行の文書「Security: e-Government Strategy Framework Policy and Guidelines Version 4.0 」は、新規あるいは拡張する電子政府サービスの開発や導入の各フェーズにおいて、ある特定のサービスの実現に対する適切なセキュリティ対策を実施するには何をすればよいのか、という課題の議論や合意のためにベースラインやガイダンスを提供している。この文書によれば、独立した認定者（accreditor：即ち、非サービス提供者）、サービス提供者、そして、その電子政府サービスの提供に責任を持つ政府組織がその提案されたサービスが満たすべきセキュリティ要件の最初の評価を行う。そのサービスのセキュリティ面の設計、開発、テストは、サービスそのものの設計、開発、テスト作業と並行して行われ、リスクに対して適切に保証された対策が取り組まれる。認定者は、全てのセキュリティ面について電子政府サービスの責任者に助言し、どのように様々なセキュリティ目標が達成されるかの評価を含め、全てのセキュリティ関連の文書のレビューを行う。設計段階では、市販ソフトウェアによるセキュリティ対策が満足のゆくものかどうか、その対策はカスタマイズされたソフトウェアで強化されるべきか、などの評価が含まれる。もし汎用的な製品が使われれば、それが確実に目的に適合しており、政府で使用するためにどのような変更や構成が必要か、の評価がなされなければならない。

4.3.2. 電子政府のため標準･推奨暗号アルゴリズム

e–Government Interoperability Framework (eGIF) は、政府や公共機関の中を流通する情報の制御に関する技術政策や仕様を定義している。セキュリティは特に Security Framework Documents でカバーされる。極秘ではないが、個人情報や商業上の秘密情報など取扱いに注意が必要な情報に対しては、2005 年 9 月発行の e-Government Interoperability Framework (eGIF) Technical Standards Catalogue, Version 6.2 で、次の認定アルゴリズムの使用を推奨している。

暗号化	Triple DES, AES (FIPS 197), Blowfish
ディジタル署名	RSA, DSA, DSS (FIPS 186-2)
鍵配送	RSA, DSA
ハッシュ関数	SHA-512, SHA-256 (FIPS 180-2)
	SHA-1, MD5 （下位互換性のため）

CESG は、このアルゴリズムのリストは完全なものではなく、ダイナミックに追加･修正･削除されるものとしている。たとえば、Blowfish や TripleDES が推奨されているが、実際にはこれらは殆ど使われておらず、将来のある時点でリストから削除される可能性が高いという。CSIA(Central Sponsor for

Information Assurance)に問い合わせれば、特定の実装やアルゴリズムについてのより詳細なアドバイスが提供される。

4.3.3. 電子政府での暗号製品利用の現状

CESG によれば、電子政府の構築は 0～3 の4段階の影響度に対して承認される。セキュリティ機能のレベルは、機密文書である HMG Infosec Standard No. 4 で定義されている。
レベル 0 と 1 については、正式な承認は不要である。レベル 2 については、FIPS-140-2 で認証されている暗号が推奨されている。レベル 3 については、暗号が目的に合致しているかどうかという基準で、CESG の承認が要求される。このレベルでも、CESG は NIST が認可する暗号を優先する。推奨されていない、ベンダ独自の暗号アルゴリズムが認められる可能性はあるが、そのベンダは CESG の認証を受ける必要があり、そのためには費用と時間がかかる。一般的には、CESG は所有権の問題のない、公になっている暗号の使用を優先する。
CESG の Information Assurance and Certification Services (IACS)はセキュリティ機能をもつ電子製品やシステムの評価を行うが、その主要な機能が暗号である場合は、CESG Assisted Products Scheme (CAPS)によるコンサルテーションを受けることが IACS 評価の前提となる。CAPS は民間企業が英国政府やその関連組織で使われる暗号製品の開発を行うことを支援する。CAPS は情報セキュリティの国家技術権威である CESG の暗号の知識と民間企業のノウハウや資源を結びつける。CESG の認定を受けた暗号製品は、英国政府や公的機関が調達するのに適したものであると宣伝してもらえる可能性がある。
CAPS スキームは、英国政府の暗号製品に対する需要の増大に対応するために作られた。CESG が以前から何年も提供してきたサービスを正式にして強化したものであり、既に幅広い商用パッケージ製品が供給され政府で使用されている。CAPS の元で開発された製品は政府の暗号要求に対応するものである。電子政府で使用されるものはレベル 2 が典型的だが、FIPS 140-2 に従って認証される。CAPS で開発された製品の例としては以下のものがある。[1]

- ALBERCOR
- ANWELL
- BEDERAL
- BRENT2
- CAPTAIN
- EUGENIC
- HANNIBAL
- IPCRESS
- PRITCHEL
- RAMBUTAN
- SETERA Secure GSM
- SHELLEYAN II
- SYMONS(SHELLEYAN III)
- THAMER

[1] http://www.cesg.gov.uk/site/publications/media/directory.pdf

4.3.4. 政府調達における推奨･標準、非国際標準製品に関する方針

1990 年以来、英国は他の国と一緒になって、数多くの国内と国際の IT セキュリティ機能を検証する仕組みを相互に一つにする働きかけを行ってきた。この協業の積み重ねがコモンクライテリア（Common Criteria ：CC) となって発表され、現在では国際標準 ISO/IEC 15408 となっている。評価（assurance）のみを取り扱う英国内標準の ITSEC と異なり、コモンクライテリアは標準という名の元に評価だけでなく特定の機能要求をカバーする。IT セキュリティの検証は、CESG の監督下で、民間評価機関（Commercial Evaluation Facilities：CLEF）によって実施される。現在英国には CSEG が任命し、英国認定サービス（UK Accreditation Service :UKAS)に認定された、5 つの民間評価機関がある。CLEF は、決められたセキュリティ基準に対して、暗号製品の設計、開発、実装、生産および流通の分析を行う。
CESG Assisted Products Scheme （CAPS）は、政府の暗号製品に対する要求が増えたことへの対応として作られた。そのスキームは、現在政府で幅広く使われている市販の製品に対して、CESG が何年にも渡って提供してきたサービスを正式化･強化するものである。CAPS の元で開発された製品は、政府の全ての暗号要求に対応する。CAPS により、政府の暗号標準に対して製品が検証され、政府や他の適切な組織での使用が正式に認められる。政府にとっては、CAPS によって保証されたソリューションを調達できるメリットがあり、ベンダにとっては、製品を政府に売り込む機会がそれまで以上に得られるというメリットがある。

4.3.5. 政府調達における国内推奨･標準に含まれない国際標準暗号を使用した製品に対する方針

国内で標準･推奨となっていない ISO/IEC 標準は自動的に承認されるのではなく、CESG が確かに電子政府への適用として目的に合致していることを認定する必要がある。ISO/IEC 19790 でさえ、そのまま国内標準･推奨として認められる訳ではない。NIST 標準から選ばれたものは比較的容易に認められるであろうが、その他のアルゴリズムについては、確実に目的に合致させるために CESG の認定が必要である。

4.4. 暗号国際標準に関する方針

4.4.1. 暗号国際標準に関する方針

CESG は、以下の国際標準暗号を電子政府で使用するものとして推奨している。

- ISO/IEC 9798（個別認証用）
- ISO/IEC 7816-8 および ISO/IEC 7816-9（スマートカード用）
- ISO/IEC 7816-11 および ISO/IEC 7816-15（将来スマート用として検討中）

国内で標準･推奨となっていない ISO/IEC 標準は自動的に承認されるのではなく、CESG が確かに電子政府への適用として目的に合致していることを認定する必要がある。NIST 標準から選ばれたも

の（たとえば ISO/IEC19790）は認められるであろうが、その他のアルゴリズムについては、確実に目的に合致していることを CESG が認定する必要である。

4.4.2. 暗号国際標準化活動

ISO/IEC で情報セキュリティ技術を扱う JTC 1/SC 27 専門委員会には常時参加している。

4.4.3. 電子政府での ISO/IEC 標準暗号の利用と計画

CESG は ISO/IEC 9798 を推奨しているが、電子政府における使用についての詳細情報は明らかにしていない。

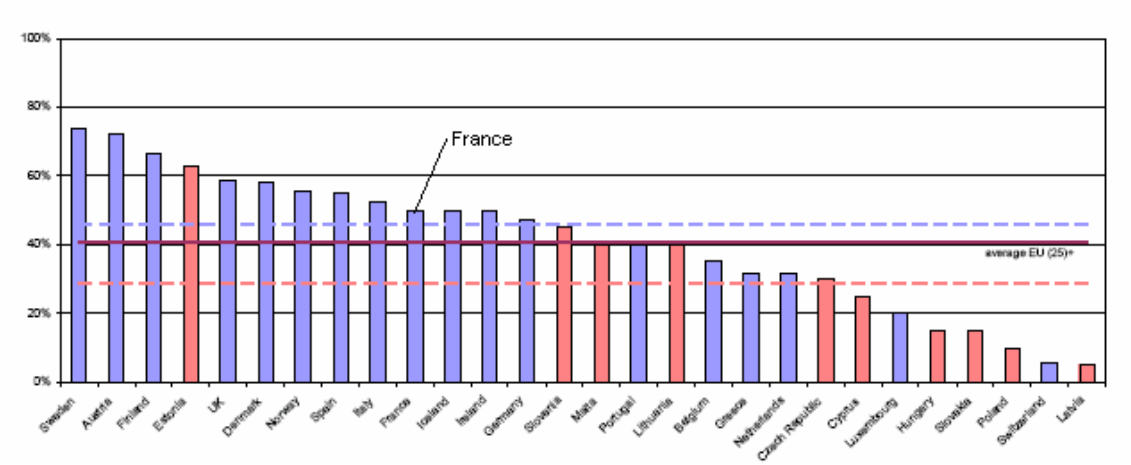
5. フランス

5.1. フランスの概要

5.1.1. 電子政府の展開状況

フランスにおける電子政府最新状況は、いくつかの分野、特に健康分野で進んでおり、他の分野では遅れている。全体的には、最近のヨーロッパ各国の比較では、民事サービスのオンライン利用においてフランスは、中位（下図、左から 10 番目）に位置付けられている。

Online Availability of Public Services



Source: Online Availability of Public Services: How is Europe Progressing, October 2004, Cap Gemini (Exhibit 1)

EU の IDABC（Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens）は、ヨーロッパにおける電子政府の展開、認識向上を進めており、メンバー国の電子政府プログラムの状況を定期的に情報提供している。[1]
2005 年 11 月の最新アップデートでは、フランスにおける電子政府の詳細を、次の表のように紹介している。

2004 年から 2007 年まで、フランス政府の電子政府戦略は、ADAE (the Agency for the Development of Electronic Administration；2006 年 1 月から、ADAE は、新たに創設された DGME: Direction Générale de la Modernisation de l'Etat の傘下に入った。)によって管理される ADELE プログラム (ADministration, ELEctronique)[2]に示されている。
ADELE プログラムは、2004 年 2 月に提起、承認され、戦略計画と行動計画を示しているが、戦略計画では、電子政府展開のロードマップを、目的（分野）と尺度（達成率）とともに明らかにしている。

[1] http://europa.eu.int/idabc/en/chapter/140
[2] http://www.adae.gouv.fr/adele/

分野	2004	2006 目標	2007 目標
民と官の間で、オンラインで行われるコミュニケーションの割合	20%	50%	66%
市民がオンラインで行える官の手続きの割合	15%	50%	100%
政府（官）部門間のオンラインによる業務対応	30%	66%	75%
部門内におけるオンライン対応の割合	60%	75%	>85%

ADELE プログラムは 18 億ユーロの予算を持ち、2007 年までに 50～70 億ユーロのコスト削減効果を持つと試算されている。戦略プラン目的達成の特効薬は、140 もの施策やプロジェクトからなるそのアクションプラン(PSAE)にあり、特定の新電子政府サービスに始まり、トレーニング、セキュリティレベル向上の施策、政府部門間のシステム構築まで広範囲に渡っている。
特定の電子政府サービスについて言えば、最重要なものは‘健康保険カード’SESAM-Vitale（Carte Vitale）である。フランスにおける多くの電子政府プログラムと同様、このシステムは、スマートカードを基に成り立っている。このシステムは 1998 年にフランスで開始され、2004 年にセキュリティ改善、メモリ容量増加の大改定を行った。

他の重要な電子政府サービスは、以下の通りである。

- **Copernic**
  税金に関する情報、アドバイス、オンライン納税/還付を提供する電子政府ポータル。ADELE のなかでも主要なこのプログラムは、最新の tax portal[1] に拡張する予定である。**Copernic** は、企業の付加価値税のオンライン納入を可能にし、現在全体の 54%の支払いに利用されている。
  同時に、個人所得税にも対応しており、2005 年には 280 万件の所得税還付が電子的に行われ、2004 年の 2 倍以上に達している。
- **Accord**
  政府部門向けのオンライン予算管理システム
- **Helios**
  地方自治体向けのオンライン会計、財務システム
- **Mon.Service-Public.fr**
  ADELE のこのプロジェクトは、現在の Service-public.fr ポータルの上に構築される全てのオンライン公的サービスの核になるべく計画されている。このサービスは、個人ユーザもしくは企業ユーザがサイトを自らカストマイズし、あたかも個人ポータルとして利用できるよう計画されている。
  このサービスは、2006 年末に開始予定である。

5.1.2. 暗号政策の担当政府機関

[1] http://www.impots.gouv.fr/

情報システム･セキュリティ推進センターDCSSI (Direction Centrale de la Sécurité des Systemes d'Information、英略名 Central Division for Information Systems Security)[1]が、2001 年 7 月 31 日に設立された。DCSSI は、国防総務事務局の権限下にある。これ以前は、SCSSI がその責を負っていた。

5.1.3. 電子政府システムでの暗号の使用

暗号、セキュリティに関しては、ADELE の戦略計画資料に、認証や電子署名を含む高度なセキュリティを要するいくつかのプロジェクトが参照されている。
それらは、下記のようなものである。

- Carte Vitale（健康保険カードシステム）
- Copernic（オンライン納税/還付）
- Electronic national identity card 電子身分証明書 (CNIE); 2006 年導入予定で、現在検討期間中
- Administrative Services Card (Daily Life Card, Carte Vie Quotidienne),
- 地方毎に配布され、市民が公共の場、施設から安全な公共サービスを受けることを可能にするカードシステム。

使用される暗号例の詳細は、5.3.2 に述べている。

5.1.4. 電子政府における非 ISO/IEC 標準暗号の利用

現状、フランスの推奨暗号リストには、実質国際標準と認識されるものが、殆ど載っている。推奨暗号リストに無い暗号を使用したい場合は、それが国際標準であろうとなかろうと関係なく、定められた評価プロセスを踏むことにより可能となりうる。ここで言うプロセスとは、コモンクライテリアによる評価、及び DCSSI による暗号そのものの評価であるが、このようなケースは実質、特定のアプリケーションに限られる。

5.1.5. 電子政府における ISO/IEC 標準暗号の利用

フランスは、一般的に、情報システムのセキュリティに関し、広く国際標準に従っている。
国際暗号標準に対する方針としても、フランスは国際標準 ISO/IEC を厳密に遵守する傾向がある。推奨暗号リストに無い暗号を使用したい場合は、それが国際標準であろうとなかろうと関係なく、5.1.4 で述べたように定められた評価プロセスを踏むことにより可能となりうる。

5.1.6. 電子政府の暗号製品のサプライヤ

- Carte Vitale（健康保険カードシステム）
  Schlumberger と ST Microelectronics が、PKI 暗号の開発に参加した。

[1] http://www.ssi.gouv.fr/en/dcssi/index.html

ST Microelectronics は、RSA 計算を実行するチップを開発した。

- Copernic（オンライン納税/還付）
  Thales は、多くの電子政府システムに関っており、特に Copernic に関わり深い。このシステムでは、認証、電子署名関連の暗号製品を提供している。
  その他の暗号製品ベンダとしては、Bull、EADS Telecom、があげられる。

5.1.7. 電子政府のシステムインテグレータ

- ATOS Origin
  ATOS は、フランスでは大きな SI ベンダである。電子政府関連では、Copernic のシステム構築に関った。
  Copernic に関った他の会社は、France Telecom、Accenture、Steria 等である。
- France Telecom
  France Telecom は、健康保険カードシステムの一部である Sesame-Vitale のシステム構築に関った。

5.2. フランスの暗号政策

5.2.1. 暗号技術政策を主管する政府機関

DCSSI (Direction Centrale de la Sécurité des Systemes d'Information、英略名 Central Division for Information Systems Security)が、2001 年 7 月 31 日に設立された。これ以前は、SCSSI がその責を負っていた。[1]

- **責務と目的**

DCSSI は、下記6つの責務と目的を持つ。

- 情報システム・セキュリティに関するフランス政府の方針決定に関与する
- 情報システム・セキュリティの統制に関し、政府や民間サービスに採用されるプロセスや暗号製品を含む情報システムの適合性に対し、国としての承認、認許を与える。DCSSI はまた、情報セキュリティ技術の評価センター(CESTI)を管理する。
- 情報システムに対するセキュリティ脅威を評価し、警報を発し、それらに対抗し、未然に防ぐ方法を展開する。(CERTA)[2]
- 情報システム・セキュリティの問題について民間サービスを支援する。
- 国や民間サービスの便に供する情報システム・セキュリティに関する科学技術の専門家を育成する。
- 情報システム・セキュリティのトレーニングセンターの運営を含む、情報システム・セキュリティ関連のトレーニング、情報提供をする。(CFSSI；情報システム・セキュリティ・インフォメーション・センター)[3]

---

[1] http://www.ssi.gouv.fr/en/dcssi/index.html

[2] http://www.certa.ssi.gouv.fr/

[3] http://www.formation.ssi.gouv.fr/

- **組織**

  DCSSI は、国防総務事務局（SGDN）[1]の権限下にある。
  この組織は、国防や国家セキュリティ問題に関する政策を調整し、首相に助言を行う役割を持つ。

- **暗号政策に関する関与**

  DCSSI は、政府部門、国防、民間サービス等に関わる暗号政策について、政府にアドバイスを行う責任主体である。DCSSI が、暗号技術や製品の使用、輸入、輸出に関する政策について、政府に情報提供する。
  DCSSI は又、適切な許認可プロセスを監督する機能を持つ。
  DCSSI は又、認定に関する国家間の相互同意に関し、政策アドバイスの責任を負う。

[1] http://www.premier-ministre.gouv.fr/fr/

1999 年、DCSSI は主な認定機関により提出され、ITSEC 6 以上もしくは CC EAL 7 以上の認証レベルを持つ製品の相互認定同意を可能にする European agreement(SOG-IS)に調印した。
1999 年時点で、この同意の調印国は、英国、フランス、ドイツである。

- **歴史**
  DCSSI は 2001 年、大臣法令により設立された。
  それ以前は、SCSSI (Central Service for Information Systems Security)として知られていた。1986 年のその設立以来、政府部門の情報セキュリティ保護のレベルを監視する SCSSI の初期機能は、研究、調査協調まで拡大してきた。当然のこととして、SCSSI の役割は国防関係のセキュリティとより関連が深くなり、SGDN（国防総務事務局）との協力が始った。1996 年、SCSSI は SGDN に接近し、SGDN 長官の全面管理下におかれることとなった。1998 年、フランス政府は、情報システム・セキュリティの高まる重要性を鑑み、財務・人事を含め、SCSSI と SGDN の全面的な統合に踏み切った。SCSSI は、上記組織図に示すように、他の SGDN 部門と同格レベルの 1 部門となった。DCSSI が 2000 年に設立され、2001 年に法制化された。
- **住所**
  DCSSI は、SGDN の 1 部門としてパリの下記住所にある。
  Secrétariat general de la defense nationale
  DCSSI
  51, boulevard de La Tour-Maubourg
  75700 Paris
- **スタッフ人数**
  DCSSI のスタッフ人数は約 110 名である。
  最近、2005 年 11 月に首相宛に議会から報告されたレポートでは、このスタッフ数が少なすぎることが指摘されている。
- **予算規模**
  2005 年、SGDN 全体の予算は 5,300 万ユーロであった。
  SGDN には 353 名の人員がおり、DCSSI が 110 名であることから、単純な頭数ベースでは DCSSI の年間予算は 1,700 万ユーロくらいと推測できる。
  前述レポートでは、DCSSI の人数のみならず、予算についても不十分であることを示唆している。
- **最近の活動**

Pays	Certificats 2004	Certificats 2005 (prévisionnel)	Nombre de CESTI	Effectif du Centre de Certification
France	36	45	5	6
Allemagne	38	40	13	20
Royaume-Uni	12	8 à fin octobre	5	
Etats-Unis[128]	27	35 à début octobre, **154 en cours**	10	30 en 2002
Canada	9	9 à début août.	3	4
Corée	20	16 à fin octobre	1	?

2004 年、フランスで出された 36 件の認許のうち、25 件がスマートカード関連、8 件が protection profiles、3 件がソフトウェアであった。生体認証関連は 1 件もなかった。

5.2.2. 政府調達における推奨･標準暗号の選択方針と手順

ADAE は、DCSSI、CGTI (General Council for Information Technologies)[1]と共に、電子政府サービス、特に carte vitale（健康保険カードシステム）や電子身分証明書のような高セキュアサービスにおける電子署名と電子認証の使用に関するフレームワークについて、指針を発行した。この指針(PRIS, Politique de Reference Intersectorielle de Securite, or Intergovernmental Reference Policy for Security)は、当初 2003 年に出され、2005 年 7 月に改版された。
ADELE 戦略計画の中で、この指針は経済的スケールメリットを得るため、ドイツの当局部門（BSI を含む）との緊密な協力で準備されたようである。
PRIS については、以下のアドレスから詳細が得られる。[2]
選定の手順、標準に関しては、ADAE とフランス政府当局部門である DCSSI との協力で開発され、2004 年 3 月のドラフト仕様書が 2005 年 7 月の正式発行に先立って、銀行および産業部門に適用された。
2005 年 6 月、フランス政府は、AdmiSource（ソフトウェア共同開発のためのオープンソフトレポジトリーとプラットフォーム）を打ち出した。
暗号に関して、2004 年 11 月に‘Cryptographic Mechanisms’と題して SGDN/DCSSI により出された参考用のガイドラインが、PRIS V2 として出版された。
PRIS V2 には、protection profiles (processes of evaluation, cryptography)に関する推奨の多くは、数多くの組織、特に AFNOR (French Standards Body)[3]、CEN (ESSIE for Electronic Signatures)[4]、ETSI（European Telecommunications Standards Institute）[5]などに基付いていることが示されている。
DCSSI は、‘Cryptographic Mechanisms’について、鍵長の変更や古いアルゴリズムの放棄を含め、新アルゴリズム選定の目的のために、年 1 回内容を改定する。新規標準に代わってある標準が消えてゆく切り換えタイミングにおいても、改定は不定期に必ず行われる。
選定の正確な手順や標準の認定について、これらの多くは CEN や ETSI のようなヨーロッパ標準グループ内で行われる。例えば、電子署名に関して言えば、アルゴリズムのほとんどは、CEN や ETSI と同時運用される EESSI（European Electronic Signature Standardisation Initiative ）[6]によって開発された。これらアルゴリズムの開発プロセスにおいて、又 CWA (CEN Workshop Agreement) 14169-2004 の一部として、the protection profiles は共通標準（CC）に従って評価され、ドイツの BSI により認定された。承認された暗号アルゴリズムや鍵長は、まず ETSI により ETSI SR 002 176 v1 (2003-03)に掲載された。つまり、アルゴリズム選定の多くは、一部に国家固有のガイドラインがあるものの、ヨーロッパレベルのきわめて国際的なプロセスによるものである。

5.3. 電子政府での暗号製品の調達

5.3.1. 暗号製品調達の政府方針と手順

1 http://www.cgti.org/
2 http://www.adae.gouv.fr/article.php3?id_article=547
3 http://www.afnor.fr/portail.asp?Lang=English
4 http://www.cenorm.be/cenorm/index.htm
5 http://www.etsi.org/
6 http://www.ict.etsi.org/EESSI_home.htm

2005 年 12 月フランス政府は、エンドユーザと政府部門間、および異なる政府部門間における情報の電子的交換に関し、指針を出した。この指針は、ADAE と DCSSI による PRIS と相俟って、製品品質、製品適合性の認定、相互運用性、電子署名･暗号の使用等についての手順を設定している。その法令は、政府部門が法令自身および PRIS のルールに従うよう義務付けている。法令の重要要件を以下に示す。

8 章
政府部門に電子署名の使用を許可するが、必ず PRIS のガイドラインに従うこと。
9 章
政府部門が情報システムを適切に用いるには、情報セキュリテイを確保する機能を活用すること。その機能が、PRIS の定める範囲の場合、PRIS に定義された統制ガイドラインを厳守すること。
11 章
情報システムの相互運用性を確保するルールについての一般的参照事項は、システム調達に参加するすべての部門が従わなければならない。
14 章
この章は、以前調達された情報システムに必要とされる適合性について述べている。PRIS 発行の以前に調達されたすべてのシステムは、3 年以内にそのセキュリティルールに準拠すること。PRIS ガイドライン後 6 ヶ月以内に作られたアプリケーションは、12 ヶ月以内にセキュリテイ要件に準拠すること。同様のガイドラインが、システム動作ルールにも適用される。

しかるに、DCSSI 暗号担当者へのインタビューによれば、これら国家標準の暗号アルゴリズムは、いわばガイドラインであり、システムデベロッパーを強く拘束するものではない。但し、推奨暗号リストに無い暗号を使用したい場合は、それが国際標準であろうとなかろうと関係なく、定められた評価プロセスを踏むことにより可能となりうる。ここで言うプロセスとは、コモンクライテリアによる評価、及び DCSSI による暗号そのものの評価である。

PRIS
フランス政府指針である PRIS V2 には、調達方針および手順に関するいくつかの要素が含まれている。

- 政府部門は、PRIS を含めた関連指針に定められたセキュリティおよび相互互換性に関するガイドラインに従うこと。
- 政府部門が用意しようとする新しい電子政府アプリケーションおよびサービスについて、その部門は先ずセキュリティ要求事項に関して、アプリケーションニーズを明らかにしなければならない。これらニーズとはデータのタイプおよび交換情報の機能であり、リスク分析の実施が望まれる。
- セキュリテイニーズの分析から部門は、適切なセキュリテイ機能および必要レベルを、PRIS 指針に決められた機能、レベルに準拠して明らかにしなければならない。
- 当該政府部門は、要求セキュリティ･レベルに合致する全製品、認証サービスを提供できる全プロバイダを、DCSSI を通して、知りうる立場にある。
- 調達に関して、PRIS ガイドラインは政府部門に対し、いかなる特定ベンダからの製品調達、特定 SI からの認証サービス調達を強制していない。

5.3.2. 電子政府のための標準･推奨暗号アルゴリズム

暗号アルゴリズム標準は、ADAE/DCSSI による方針書 PRIS V2 および関連‘Cryptographic Mechanisms’に記されている。PRIS V2 は、経済的スケールメリットを得つつ必要な相互運用性を確保し、またオープンソフトウェアの開発、活用を奨励するために、暗号システム選択の唯一の基盤を提供している。
PRIS V2 は、政府部門および調達部門にとってガイドラインとして役立つと同時に、製品ベンダ、システムインテグレータにも役立つものである。
DCSSI は、産業向けの認定製品リスト(produits_certifies_en.pdf)を広めると同時に、政府部門が電子政府応用に活用できる認定製品リストを発行している。後者（政府部門向け）リストは ADELE 計画(2004-2007)の一部であり、PRIS 方針書にある参考用フレームワークと密接に関係している。
つまり、政府部門は、推奨アルゴリズムを含むセキュリティの基本体系ガイドラインと同時に、その推奨に合致する認定製品リストをも知ることができる。

- **アルゴリズム：ルールと推奨**

“Cryptographic Mechanisms” 即ち PRIS V2 において、DCSSI は暗号の推奨と統制を行っている。推奨としては、より高度なセキュリティ・レベルにおける鍵長等、統制としては、最小要件の規制を行う。

- **共通鍵暗号：ブロック暗号**

鍵長は、以下のように厳密に規定されている。

1. 2010 年まで、共通鍵暗号に使われる最小鍵長は、80 ビット
2. 2010 年以降、共通鍵暗号に使われる最小鍵長は、100 ビット
3. 共通鍵暗号に使われる推奨最小鍵長は、128 ビット

特定のアルゴリズムについて言えば、56 ビットの DES は安全ではない。
128 ビットの AES は、安全と評価できる。同様に 3×56 ビット鍵の TripleDES（TDEA）も、112 ビット（2 鍵の場合）、もしくは 168 ビット（3 鍵の場合）とすることで安全と評価できる。
AES は 128 ビットブロック暗号として働き、一方 Triple DES は、64 ビット暗号として働く。
しかるに DCSSI は、64 ビットブロック暗号は、許されるが充分安全とは考えていない。

a） ブロック暗号の最小ブロックサイズの統制値は、64 ビット
b） ブロック暗号の推奨ブロックサイズは、128 ビット

ブロック暗号の特定アルゴリズムについて、DCSSI は 2 つの主要な条件を提示している。

Ⅰ. 2010 年までに使われるブロック暗号のアルゴリズムは、2^{80} 回以下の攻撃に耐えるものであること。
Ⅱ. 2010 年以降使われるブロック暗号のアルゴリズムは、2^{100} 回以下の攻撃に耐えるものであること。

DCSSI は、ブロック暗号の要求に適合する標準として、上記条件に適合する他の標準を排除しないが、現実には、FIPS 197 による AES のみを推している。
Triple DES は鍵長の最小要求を満たしているが、DCSSI はこのアルゴリズムを、64 ビットのブロック長が短すぎるとして、推奨していない。

- **共通鍵暗号：ストリーム暗号**

DCSSI は、ブロック暗号として述べたⅠ、Ⅱと同じ条件に合致する、ストリーム暗号のアルゴリズムを要求している。しかしながら、DCSSI は、政府組織はストリーム暗号の代わりにブロック暗号を活用すべきとして、ストリーム暗号を推奨していない。

- **公開鍵(非対称鍵)暗号:**

公開鍵暗号(公開/秘密鍵)について、DCSSI はアルゴリズムに関しいくつかの仕様を設定している。

1. 2010 年以降、公開鍵暗号のモジュラス長の最小値は、1,536 ビット
2. 2020 年以降、公開鍵暗号のモジュラス長の最小値は、2,048 ビット

一方、PRIS V2 では、1,024 ビットのモジュラスは、2008 年まで使用可能としている。
しかし、DCSSI は 1,024 ビットの使用を推奨していない。

3. 秘密指数(secret exponent)の値は、モジュラスの長さと同じとする。
4. 公開指数(public exponent)の値は、厳密に $2^{16} = 65,536$ より大きいこと。

DCSSI は、例え 2010 年以前に使用するものであっても、モジュラス長は 2,048 ビット以上とすることを推奨している。

公開鍵暗号の特定アルゴリズムに関しては、DCSSI は、前述ルールによって、RSAES-OAEP (PKCS #1 V2.1)がセキュリティの必要とされる標準レベルであるとしている。

- **電子署名:素因数分解**

素因数分解について、DCSSI は、非対称暗号について前述した 1〜4 が本質的に同じ条件であるとしている。そして、RSA が標準アルゴリズムであるとしている。
さらに DCSSI は、1,024 ビットの長さは、一般的にはかなり安全と考えられるが、あえて 1,536 ビット、できれば 2,048 ビットの長さが推奨されるとしている。

- **電子署名:離散対数**

DCSSI は、楕円関数方式と非楕円関数方式の両方式について述べている。非楕円関数方式に関し、下記のルールが適用される。(p は、素数)

1. 2010 年以降使われる素数モジュラス(prime modulus)の最小の長さは、1,536 ビット
2. 2020 年以降使われる素数モジュラス(prime modulus)の最小の長さは、2,048 ビット
3. 2010 年以前では、the subgroup size は 160 ビットより大きい素数の倍数であること。
4. 2010 年以降では、the subgroup size は 256 ビットより大きい素数の倍数であること。

DCSSI は、例え 2010 年以前に使用するものであっても、素数モジュラス長は 2,048 ビット以上とすることを推奨している。
DCSSI の方針書には、DSA について特に触れていないがアルゴリズムを推奨している政府内部方針書(PRIS V2)では、下記表にあるように DSA と DH (Diffie Hellman)の使用を推奨している。楕円曲線を用いた離散対数として、DCSSI は、FIPS 186-2 の曲線 P-256、P-384、P-521 を推奨している。
下記表では、非対称暗号および電子署名の推奨内容を示している。

	*	**
RSA	1,024bits ou 2,048bits	2,048bits (2)
DSA	1,024bits q=160 ou 2,048bits q=256	2,048bits q=256(2)
ECDSA(typeGF(p))	q=160 ou q=256	q=256(2)
Hachage－SHA(1)	SHA-1 (160bits)	SHA-1 (160bits)

注釈

RSA；1,024 ビット は 2008/12/31 まで使用許可される

DSA or DH,；1024 bit length (q = 160) は 2008/12/31 まで使用許可される

ECDSA (or ECDH)；q ＝ 160 は 2008/12/31 まで使用許可される

＊ ～2008/12/31

＊＊ 2009/1/1～ 出展：PRIS V2

- **ハッシュ関数**

方針書“Cryptographic Mechanisms”において、DCSSI はハッシュ関数の使用に関して下記条件を決めている。

1. 2010 年まで、ハッシュ関数により短縮されたデータ長の最小サイズは 160 ビットである。
2. 2010 年以降、ハッシュ関数により短縮されたデータ長の最小サイズは 256 ビットである。

PRIS V2 にあるように、DCSSI は、FIPS 180-2 に定義された SHA-256 がセキュリティ推奨レベルに合致すると述べている。

- **メッセージ認証**

メッセージ認証は、選定されたアルゴリズムの強力な機能そのものである。

DCSSI は、標準レベルニーズに合致するものとして CBC-MAC を推奨する。特に、AES ブロック暗号と 2 つの別個鍵を使った CBC-MAC を推奨している。

しかしながら、DCSSI は、DES ブロック暗号(2 つの別個鍵を使ったとしても)と CBC-MAC の組み合わせは充分安全でないとしている。

5.3.3. 電子政府での暗号製品利用の状況

5.1.3 にも記述したが、暗号、セキュリテイに関しては、ADELE の戦略計画資料に、認証や電子署名を含む高度なセキュリテイを要するいくつかのプロジェクトが挙げられている。

それらは、下記のようなものである。

- Carte Vitale（健康保険カードシステム）

  2000 年、政府は RSA と ISO/IEC 9796 に基付く 768 ビットの鍵長を使った PKI 導入により、システムのアップグレイドを行った。このソフトウェアは、Schlumberger と ST Microelectronics によって開発された。

  2004 年の末にさらなる改修が行われた。それは、対称暗号に関しては A3S を TripleDES に置き換え、PKI については 1,024 ビット（メッセージ認証）、2,048 ビット（電子署名）を採用した。
- Copernic（オンライン納税/還付）

  Thales 社は、多くの電子政府システムに関っており、特に Copernic に関わり深い。このシステムでは、米国暗号標準である RSA、SHA-1、ECD-DSA、DH に基づいた IETF RFC 3280、IETF RFC 3279 による認証、電子署名を採用している。
- Electronic national identity card 電子身分証明書（CNIE）

  2006 年導入予定で現在検討期間中
- Administrative Services Card (Daily Life Card, Carte Vie Quotidienne)

地方毎に配布され、市民が公共の場、施設から安全な公共サービスを受けることを可能にするカードシステム。

5.3.4. 政府調達における推奨･標準で、かつ国際標準でない暗号を使用した製品に対する方針

フランスは、一般的に、情報システムのセキュリティに関し、広く国際標準に従っている。
国際暗号標準に対する方針としても、フランスは国際標準 ISO/IEC を厳密に遵守する傾向がある。
現状、フランスの推奨暗号リストには、実質国際標準と認識されるものが、殆ど載っている。5.2.2 のアルゴリズム選定の方針/手順で述べたようにアルゴリズム選定の多くは、ヨーロッパレベルのきわめて国際的なプロセスによるものであるからである。

5.3.5. 政府調達における推奨･標準でない国際標準暗号を使用した製品に対する方針

現状、フランスの推奨暗号リストには、実質国際標準と認識されるものが、殆ど載っている。推奨暗号リストに無い暗号を使用したい場合は、それが国際標準であろうとなかろうと関係なく、定められた評価プロセスを踏むことにより可能となりうる。ここで言うプロセスとは、コモンクライテリアによる評価、及び DCSSI による暗号そのものの評価であるが、このようなケースは実質、特定のアプリケーションに限られる。

5.4. 国際標準暗号政策

5.4.1. 暗号国際標準に関する方針

- フランスは、一般的に、情報システムのセキュリテイに関し、広く国際標準に従っている。例えば、参考ドキュメント PSSI(PSSI: Policy for Information System Security)において、DCSSI は、企業や組織が情報システムを保護するための広範囲なガイドラインを提供している。これらガイドラインは、情報セキュリテイの戦略、手順、コード類、動作、技術的、組織上のルール等に渡っている。ガイドラインには、これらが国際標準(ISO/IEC 15408、ISO/IEC 13335 、ISO/IEC 17799)に基づいていることが明記されている。
  ガイドラインは、下記による。[1]

- 電子署名の分野では、フランスは、ヨーロッパ標準、即ち EESSI (European Electronic Signature Standardization Initiative)の標準電子署名を推奨している。

[1] http://www.ssi.gouv.fr/fr/confiance/pssi.html

- 認証について、フランスは、セキュリテイ認証の評価マニュアルを提供する ITSEC の創設メンバーとして、イギリス、ドイツ、オランダと協働した。しかしながら、フランスにおいては、ITSEC の使用は CC 評価標準と逆比例して、明らかに減少している。

- 一般的に、国際暗号標準に対する方針として、フランスは国際標準 ISO/IEC を厳密に遵守する傾向があり、特に米国の暗号標準に基づいていることを、5.3.2 は明らかにしている。

- 電子署名の分野では、DCSSI は、ESSI 内、特に ETSI SR002 176 (2003)の暗号アルゴリズムを推奨している。
  （ここでの暗号標準は、RSA、DSA、ECDSA、SHA 及びドイツ標準の RIPEMD、ECGDSA を含んでいるが、5.3.2 では、ドイツ標準は既に見当たらない。）

5.4.2. 暗号国際標準化活動

フランス国内においても、国際標準化グループへの参加、会議出席等の活動が比較的少ないことが批判されている。ISO/IEC 19790（Security Requirement for Cryptographic Modules)にも、DCSSI は、代表を出さなかった。
フランスにおけるこのような役割は、フランス標準団体の AFNOR（the French standard organization）が担うものと思われる。

5.5. 電子政府のサプライヤ

5.5.1. SAGEM（SAFRAN グループ）

企業プロフィール[1]
2004 年度において、通信と国防セキュリティの 2 部門から成り立っていた。
両方あわせた総売上げ高は 36 億ユーロで、国防部門の人員は 6,880 人であった。2005 年、Snecma と合併し、Safran グループの一員となった。
Sagem の電子政府に関するセキュリティ事業は、次のようなものである；

- Carte Vitale を含む電子政府向けの端末、スマートカードの提供
- 電子政府プロジェクトの仕様設計、システム構築
- 傘下の Keynetics による、電子政府暗号サービス（電子署名、PKI 運用）

電子政府で使用される暗号製品の実例
フランスの健康保険カードシステム（Carte Vitale）は、長い歴史を持ち、その開発には、多くの会社が関ってきた。Sagem もその 1 員として、認証サービス他を担当してきた。
2000 年、政府は RSA と ISO/IEC 9796 に基付く 768 ビットの鍵長を使った PKI 導入により、システムのアップグレイドを行った。このソフトウェアは、Schlumberger と ST Microelectronics によって開発された。

[1] http://www.sagem.com/index.php?id=55&L=0

2004 年の末にさらなる改修が行われた。それは、対称暗号に関しては AES を Triple DES に置き換え、PKI については 1,024 ビット（メッセージ認証）、2,048 ビット（電子署名）を採用した。

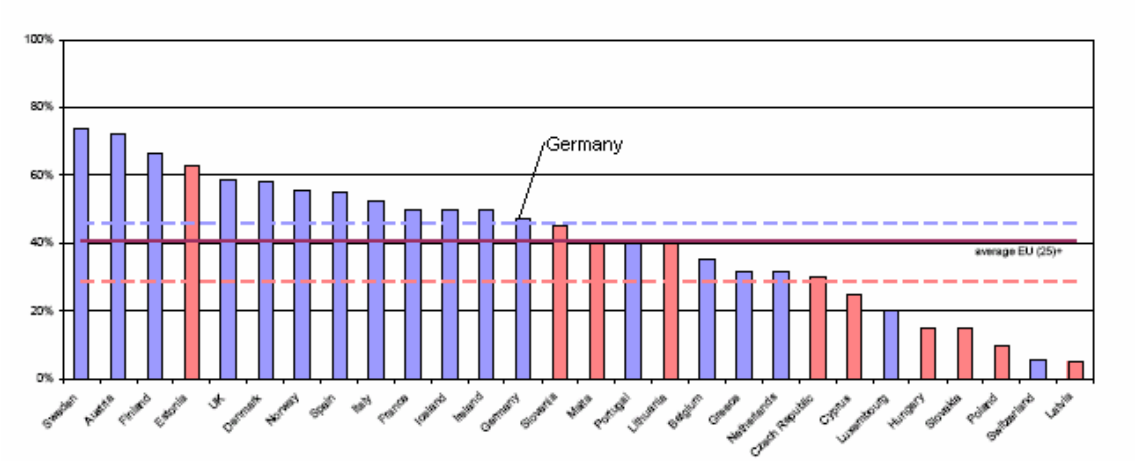
6. ドイツ

6.1. ドイツ の概要

6.1.1. 電子政府普及の状況

ドイツにおける電子政府の最新状況は、英国そして多分フランスにも遅れをとっている。しかし、ドイツ政府の電子政府プロジェクト BundOnline 2005 が、これら認識を踏まえ、推進主体となっている。全体的には、最近のヨーロッパ諸国のベンチマーク評価によれば、ドイツは、民事サービスのオンライン化において中位（下図、左から 13 番目）に位置付けられている。

Online Availability of Public Services



Source: Online Availability of Public Services: How is Europe Progressing, October 2004, Cap Gemini

EU の IDABC（Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens)はヨーロッパにおける電子政府の展開、認識向上を進めており、メンバー国の電子政府プログラムの状況を定期的に情報提供している。[1]
2005 年 11 月の最新アップデートでは、ドイツにおける電子政府の詳細を次のように紹介している。
2000 年 9 月、シュレーダ首相は、電子政府 BundOnline 2005[2]計画を発表し、電子化可能なすべての政府サービスのオンライン化を 2005 年までに達成するとした。2005 年 8 月までに、379 のサービスが電子化され、目標を達成した。これらの中には、次のプロジェクトが含まれる；

- ELSTER: オンライン税申告
- BSV Direct: インターネット・バンキング
- BAfoG-Services Online: 学生ローンサービス
- Virtual Labour Market: 就職サービス

[1] http://europa.eu.int/idabc/en/chapter/140
[2] http://www.bund.de/

BundOnline は、全ての BundOnline アプリケーションに適用可能な、5つの‘基本コンポーネント’を提供している。

- ‘支払い処理’プラットフォーム
- コンテンツ管理システム
- フォーム･サーバー
- データセキュリティ･ プラットフォーム
- 共通ポータル

データセキュリテイコンポーネントの核は“Virtual Post Office”である。
このセキュアメッセージシステムは、IBM によって開発され、認証、電子署名の検証、メッセージの暗号化、復号等の機能を提供する。
BundOnline の全ての機能、コンポーネントは、BSI 他の部門と相談しつつ、KBSt（Coordination and Advisory Agency for IT in the Federal Administration）[1]によって定義された SAGA(Standards and Architectures for eGovernment Applications)に従って標準開発された。
政府レベルの BundOnline に加えて、電子自治体 Deutschland-Online が、ドイツにおける 200 の地方、13,000 の地域自治体 を含む 16 の州のニーズに対応する。現時点では、Deutschland-Online はサービス展開の面では BundOnline に遅れをとっている。Deutschland-Online の多くは、まだ方針、計画段階である。しかしながら、既存の Deutschland-Online 資料には、BundOnline と同じ SAGA に基づくアーキテクチャーを追求するとしている。[2]

6.1.2. 暗号政策の担当政府機関

国の暗号技術問題に関る主管政府機関は、情報技術安全連邦局 BSI（Federal Office for Information Security）である。[3]
BSI は、連邦内務省の IT 監督局（Ministry’s Office of the IT Director）の一部門である。BSI は政府の暗号専門家集団だが、自身が政策を作るというより、方針に影響力を持つ。IT 監督局の他の組織、特に KBSt が SAGA を定めた。
BSI の全体目的は、IT の活用に伴うセキュリティリスクを調査し、予防的セキュリテイ対策をとることである。この役割は、産業界と協調し、IT セキュリティの試験、開発を含めた IT システムのアセスメントの実施を含む。また、情報技術の開発、動向分析を行う。
暗号領域において、BSI は、自身および第 3 者の暗号メカニズムを、IT システムの承認、認証活動の 1 部として評価し、活用に関する更なる推奨を行う。高セキュリティシステムの厳しい要求がゆえに、BSI は、暗号メカニズムの開発、選択、適用を自ら行う。

6.1.3. 電子政府システムでの暗号の使用

ドイツ政府の主要標準は、次のものである。詳細は 5.3.2 章に記す。

- ブロック暗号: AES 、Triple DES
- 非対称暗号: RSA

---

[1] http://www.kbst.bund.de/nn_836802/Content/Home/homepage.html__nnn=true

[2] http://www.deutschland-online.de/

[3] http://www.bsi.de/english/index.htm

- 電子署名: RSA / DSA
- ハッシュ関数: SHA-256、SHA-512、RIPEMD-160

ELSTER（税申告サービス）及び IBM の Virtual Post Office (全ての BundOnline プロジェクトの基盤)が、これら標準を展開するドイツ電子政府プロジェクトの例である。

6.1.4. 電子政府における非 ISO/IEC 暗号の利用

ドイツ政府の方針は、電子政府には国家標準を含めた国際暗号標準を使うことである。非ドイツ標準を使ったいくつかのシステム例があるようだが、今回の調査では、明らかにできなかった。

6.1.5. 電子政府における ISO/IEC 暗号の利用

5.1.3. 、5.1.4 の記述のように、ドイツ政府の方針は、電子政府には国家標準を含めた国際暗号標準を使うことである。5.3.4 及び 5.3.5 参照。

6.1.6. 電子政府の暗号製品のサプライヤ

- G&D の子会社, Secunet Security Networks AG；ELSTER（税申告システム）のセキュリティ基盤開発
- 小規模ベンダ、SECUDE IT Security GmbH ； Electronic Legal Communication プロジェクトに SECUDE Gateway を提供
- ELSTER 及び Electronic Legal Communication プロジェクトは、 BundOnline の一環である。.

6.1.7. 電子政府のシステムインテグレータ

- IBM は、BundOnline コアデータセキュリテイモジュール生成するセキュリテイ製品, Virtual Post Office を開発した。
- T-System は、電子政府セキュリティにかんする、他のシステムインテグレータである。例えば、地方自治体システムの一部である BEA WebLogic Portal を提供した。
- Siemence Buisiness Service は、BundOnline の 1 部である Materna 社 及び Lucom 社とともに、様式管理を含む電子政府セキュリティ・サービスを提供した。

6.2. ドイツの暗号政策

6.2.1. 暗号技術政策を主管する政府機関

国の暗号技術問題に関る主管政府機関は、情報技術安全連邦局 BSI（Federal Office for Information Security）である。しかし、方針展開に責任を持つ組織は、BSI だけではない。
連邦内務省は、全ての電子政府戦略、暗号を含む政策に包括責任を持つ。連邦内務省の IT 監督局（The Ministry's Office of the IT Director）が BundOnline 2005 プロジェクトグループ、KBSt（Coordination and Advisory Agency for IT in the Federal Administration）、生体認証プロジェクト、等とともに BSI を統括する。これらチームの中で、BSI は、セキュリティ及び暗号の専門家であるが、KBSt を含む他の IT 監督チームもまた方針策定に重要な役割を担っている。
暗号に関する総合方針書である SAGA は、KBSt により出版されている。

BSI のプロフィールを記す。

- **目的と役割**

  BSI の全体目的は、IT の活用に伴うセキュリティリスクを調査し、予防的セキュリティ対策をとることである。BSI は、情報技術の活用に際して、リスクと脅威の情報を提供し、適切な解を探す。この役割は、産業界と協調し、IT セキュリティの試験、開発を含めた IT システムのアセスメントの実施を含む。

  例え技術的にセキュアな情報通信システムであっても、不適切な管理または使用によって、リスク及び障害は発生する。これらリスクを避けるもしくは最小化するために、BSI のサービスは多くの対象グループ、たとえば情報製品の製造者、販売者、使用者、に対して助言をする。また、情報技術の開発、動向分析を行う。
- **政府内の位置付け**

  連邦内務省の IT 監督局の一部門
- **暗号技術政策への取り組み**

  BSI の暗号関連部門（Division 2, Department 1）は、自身および第三者の暗号メカニズムを、IT システムの承認、認証活動の一部として評価し、活用に関する更なる推奨を行う。特に、ドイツの署名法に定義された適切なメカニズムのリストは、毎年更新発行される。高セキュリティ・システムの厳しい要求がゆえに、BSI は、暗号メカニズムの開発、選択、適用を自ら行う。

  EU 及び NATO 内の国際協調の結果としての開発は勿論、数学的暗号、暗号技術における基礎開発、新開発等が適切な検討対象として、考慮される。
- **歴史**

  BSI の歴史上の主な出来事を次に記す。
  - **1986** 中央暗号局（Central Cipher Agency ）が、特定案件を扱うシステムのコンピュータセキュリティ対応の役割を委任された。
  - **1987** Interdepartmental Committee for IT Security (ISIT) が、連邦内務省の主導で設立された。
  - **1989** 中央暗号局は、その業務範囲の拡大と共にITセキュリティのためのセンター部局へと発展移行した。
  - **1990** 1989年6月政府発行のIT政策報は、1990年12月のBSI確立法へと発展した。
  - **2001** 2001年8月1日連邦内務省は、BSIをドイツ政府の中心的ITセキュリティサービスセンターへとさらなる展開を促進するため、新しい組織と技術フレームワークの強化を図った

- **2003** 2003 年 3 月ヘルムブレヒト博士が、2002 年 11 月に辞任したヘンツ博士の後任となった。

- **所在地**
  Godesberger Allee 185-189, 53175 Bonn, Germany
- **スタッフ数**
  BSI は 2003 年で、約 300 名の専門家と、上級スタッフを擁するといわれる。
- **財政規模**
  BSI は 2003 年で、約 4,500 万ユーロの年間予算といわれる。

6.2.2. 国内推奨･標準暗号の選択方針と手順

BSI は、暗号を含めた各種 IT セキュリティ手法の使用について、アドバイスや最適解を提供する電子政府マニュアルを発行してきた。マニュアルはモジュール分割形式で発行された非常に大きなドキュメントであり、これらモジュールのいくつかが最近やっと完成し、それらモジュールの数点が英訳された。詳細情報は下記による。[1]
暗号を含む技術標準についての電子政府政策に関連する統合モジュールは、SAGA v2.1（2005 年 9 月）である。現在は、v2.0 (2003 年)のみが最近英訳されている。今回の報告には、v2.0 を使用し、アップデートや改正が可能なところについて v.2.1 を参照した[2]。SAGA は、電子政府システムの開発、殊に BundOnline 2005 imitative に関して技術標準を規定している。SAGA v2.0 の導入部で、作者は SAGA を、ガイドライン設定のみならず、他の部分でガイドラインの実行説明や現実的アドバイスの提供をする電子政府マニュアルであると性格付けている。なぜなら、BundOnline は最重要事項であり、従って SAGA は実質、ドイツにおける電子政府システムの暗号アルゴリズムおよび他の IT 標準の国家方針である。
加えて、地方自治体方針である Deutschland-Online もまた、SAGA に準じる意向である。KBSt は、SAGA にあるアルゴリズムの選定方針と手順を設定し、BSI を含む多くの専門化グループや関連利益団体の相談に応じる。
SAGA は、暗号は勿論、相互運用性等の多くの IT 標準を規定する。事実、SAGA の資料には、標準の選択および既選択アルゴリズムの破棄といった、一般的選択プログラムが述べられている。この選択プログラムの概要、選別スキームは次のようなものである。
SAGA は、標準を Mandatory（強制）、 Recommended（推奨）、Under Observation（観察中）に区別し、各々を次のように定義している。

- **Mandatory（強制）；**
  標準が、実証済みであり、好ましい解を代表するものである時、その標準は強制（Mandatory）となる。このような標準は、優先的に検討され、適用されなければならない。
  mandatory および recommended standards もしくは standards under observation が同時に存在する時、後者つまり standards under observation は、正当化しうる、例外的なケースでのみ採用されるべきである。
  Mandatory に位置付けられた標準が、すべての電子政府応用で使われるべきということでは、必ずしも無い。
  強制標準は、この標準の技術や機能の使用が必要であったり、そのアプリケーションの要求から見て妥当である場合にのみ、固執されるものである。

[1] http://www.bsi.de/english/themes/egov/3_en.htm

[2] http://www.kbst.bund.de/saga

- **Recommended（推奨）；**
  標準が、実証済みであるが mandatory（強制）ではない場合、もしくは、好ましい解を代表するものではない場合、もしくは、強制に位置付けるにはさらなる同意を要する場合、その標準は、推奨に位置付けられる。推奨標準以外に競合する強制標準が無い場合、推奨標準の適用が、例外的ケースではあるが、認められる。
- **Under Observation（観察中）:**
  標準が、意図した開発方向にあっているがまだ成熟レベルに無いか、もしくは市場でまだ充分価値を証明できていない場合、その標準は、観察中に位置付けられる。観察中標準に加えて、競合する強制標準もしくは推奨標準が無い場合、観察中標準が取りあえずの解となりうる。

KBSt のライフサイクル・モデルは、上述したものとは別の３段階クラス分けを使っている。それは、活用中の標準“White list”、既に拒絶された標準“Black list”、そして効力を保持中の標準“Grey list”である。
以前のバージョンが強制もしくは推奨であったり、過去に広く市場で使われていたが、最新の SAGA の版にはもはや載らなくなった標準は、“grey list”に加えられる。
White、Black、Grey lists は、脚注の URL に詳述されている。[1]

SAGA のライフサイクルについての記述によれば、ある標準は、強制標準になる前に拒絶され、“Black list”に加えられうるが、時代遅れになった強制標準は、通常“Black list”に加えられるのではなく、“Grey list”に加えられる。

6.3 電子政府での暗号製品の調達

6.3.1 暗号製品調達の政府方針と手順

SAGA 2.0 には、「ドイツ国内で電子政府サービスを提供するすべてのプロセス、システムにとって、SAGA への適合は一般的必要条件である。」と述べている。
SAGA には、BundOnline（SAGA の主対象）および将来的には多分 Deutschland-Online システムをも包含する電子政府システムを提供しようとするベンダが守るべき強制標準が含まれている。
SAGA は、‘SAGA 適合申請’の雛形を用意しており、公共機関が電子政府システム入札に際し活用することを期待している。適合性は、多くのシステムコンポーネントに対するチェックリストを基本にして、確立される。
SAGA には、強制標準が必ず全てのアプリケーションに含まれるべきなのではなく、標準の選択時に、競合する標準に対して優先的に扱われるべきことを述べている。
要約すれば、SAGA 適合性は、ある特定なアプリケーションに関して、全 SAGA 標準の中から特定のサブセットを使うことで達成される。SAGA 適合性試験の準備は、計画中の将来課題である。
電子政府アプリケーションの調達責任を持つ特定政府部門もまた、SAGA 適合責任を負う。SAGA 適合性を欠くシステムの開発者に対しては、連邦政府は次の制約/罰則を科する。

- 基本コンポーネントの使用制限
- 開発センターによるアドバイス、コンサルテーションの制限もしくは禁止

[1] http://www.kbst.bund.de/Standards-Life-Cycle-,229/start.htm

- 当該システムとのインターフェースのサポート禁止
- 補助金、特に BundOnline 2005 からの資金が利用できない
- サービスポータルへのシステム接続ができない

SAGA には適合しているが BundOnline の一部ではない（例えば、Deutschland-Online システム）電子政府システムに科せられるであろう罰則については、内容を把握できていない。

6.3.2 電子政府のための推奨･標準暗号アルゴリズム

SAGA による主要推奨品は以下のようなものである。今回の、SAGA 主要参照バージョンは、英訳の完了した 2.0 であるが、独語 2.1 バージョン（方針の変動あり）からの情報アップデートを行っている。

- **共通鍵暗号：ブロック暗号**
  ブロック暗号としては、SAGA は、AES（最小鍵長 128 ビット）の使用を定めている。
  TripleDES も、推奨標準として含まれる。SAGA によれば、Triple DES（3×56 ビット）は、安全と考えられるが、パフォーマンスが充分でない。

  SAGA 2.0（2003 年）と最新バージョン 2.1 の間に、SAGA は明確に、ブロック暗号のデファクト標準として AES を格上げした。v2.0 では、Triple DES が“Mandatory”で、AES は“Under observation”であった。v2.1 では、AES が“Mandatory”として現われ、TripleDES は“Recommended”に降格した。

- **共通鍵暗号：ストリーム暗号**
  ストリーム暗号の使用は奨励されず、ブロック暗号を推奨することから推し量れるように、SAGA にはストリーム暗号の記述がない。

- **公開鍵暗号：公開鍵**
  公開鍵暗号（公開/秘密鍵）として、SAGA は、最小 1,024 ビットの RSA を強制標準としている。加えて SAGA は、Diffie-Hellman 鍵暗号を推奨（強制ではない）している。
  XML 暗号の SAGA 分野では、SAGA はより詳細な RSA 要求を用意している。それによれば、RSA (RSAES-PKCS ＃1-v1-5)が適合するとしている。

- **電子署名：素因数分解**
  SAGA は、公開鍵暗号でのべたように、素因数分解として RSA を標準としてあげている。

- **電子署名：離散対数**
  電子署名アルゴリズムとして、SAGA は、DSA および DSA 変形タイプが適合するとしている。SAGA に参照される DSA 変形タイプには、EC-DSA、EC-KDSA、EC-GDSA、aNyberg-Rueppel 署名がある。Diffie-Hellman アルゴリズムは電子署名としては述べられていない。

- **ハッシュ関数：**
  多くの例において、SAGA v2.1 は、ハッシュ関数として、SHA-256（もしくは SHA-512）を強制標準としている。しかし、SHA-1 が、XML 暗号および SSL/TLS に適合するとしている。SAGA v2.0 では、SHA-1 は全ての用例に充分と言われた。一般的に言って SAGA は、

SHA ベースのハッシュ関数を使い、可能なら最新標準バージョンに改定することを意図していることが明らかである。
XML 暗号と電子署名応用において、SAGA は SHA ベースのハッシュ関数に代わって RIPEMD-160 (160 ビット)が使用可能としている。

- メッセージ認証と完全性:
多くの例において、SAGA はメッセージ認証標準を特定していない。しかし、XML 署名については、SAGA は、HMAC-SHA1 (対称鍵) (IETF RFC 2104)を標準としている。

6.3.3 電子政府での暗号製品利用の現状

多くの例において、ドイツ政府はベンダに、出来合いのセキュリティ製品を買うより、むしろ仕様に合わせて開発することを委託した。このようにして開発された卓越した 3 例を挙げると;

- G&D の子会社、Secunet Security Networks AG,は ELSTER 税申告サービスのセキュリティ基盤を、仕様に合わせて開発した。
- ここで使用された暗号標準は、PKCS #7、PKCS #10、PKCS #11、PKCS #12、XMLDSIG などである。
- IBM は、核となる BundOnline データセキュリティモジュール、Virtual Post Office をつくり、それを活用してセキュリティ製品を開発した。
- SECUDE IT Security GmbH は、Electronic Legal Communication プロジェクトに SECUDE セキュアゲートウェイ を提供した。

6.3.4 政府調達における推奨･標準で国際標準でない暗号を使用した製品に対する方針

ドイツは、国際標準でないものは、ドイツ国家標準として認めない。

6.3.5 政府調達における国内推奨･標準でない国際標準暗号を使用した製品に対する方針

5.3.1 参照。
KBSt は、未評価のリスト、不合格の標準、旧版互換 (backwards compatibility) のために保持される主として旧標準からなる“grey”リスト、を保持している。これらのリストは、明らかに SAGA 要件ではない、多くの国際標準を含んでいる。SAGA は、その標準を遵守する要求は明らかで、国際標準だが、国家推奨･標準でない暗号製品の対応方針はこの要求から推測できる。
SAGA (国家標準) では無い、国際標準を使った電子政府システムは、その国際標準が SAGA の仕様と競合せず、法準拠を保持するならば、容認される。
SAGA 方針の論理は次のようなものである。

- 国際標準が x を採用し、SAGA が y を‘強制’と規定し、x と y の仕様が同じ場合、x は使用できない。

- 国際標準がzを採用し、SAGA にはzと同じ仕様の暗号が無い場合、(例;zが新機能)、zは容認される。

しかしながら、現実には SAGA は、共通的で広く使われだした国際標準を包含するよう働くので、このような状況は滅多に起こらない。

6.4. 暗号国際標準に関する政策

6.4.1. 暗号国際標準に関する方針

5.3.4 及び 5.3.5 参照。
ドイツは、国際標準でないものは、ドイツ国家標準として認めない。
SAGA (国家標準) では無い、国際標準を使った電子政府システムは、その国際標準の仕様と競合せず、法準拠を保持するならば、容認される。

6.4.2. 暗号国際標準化活動

ドイツは、殆どの暗号国際標準化活動に積極的に参加、支援している。

6.5 電子政府のサプライヤ

6.5.1 Secunet Security Networks AG

企業プロフィール[1]
G&D の子会社、**Secunet Security Networks AG**;ELSTER (税申告システム) のセキュリティ基盤開発を担当した。

推奨・標準暗号に対する戦略

- **国内戦略**
  Secunet は、ドイツ政府の優良なパートナーとして、ドイツの暗号国家標準選定のプロセスに参画している。そのプロセスは、充分に確立され、満足のいくものであり、従ってその成果は市場要求に合致し、ベストプラクティスを提供するものと評価している。
- **国際戦略**
  Secunet が直接、国際標準化、国外標準化プロセスに関与したことは、無い。
- **政府調達における推奨・標準暗号と国際標準の差異への対処**
  国家標準でない国際標準の採用について、その国際標準が充分な強度、パフォーマンスを持つものであれば、(追加評価等の手順によって) 可能であろう。特に、コモンクライテリア、IT-SEC、BS 7799 の採用については、問題は少ないであろう。

[1] http://www.secunet.de/

電子政府で使用される暗号製品の実例

- **国家推奨･標準暗号を使用したシステム**

  1999 年 1 月 1 日、ﾄﾞｲﾂ税務当局は、所得税申告の電子申請について、抜本的かつサービス向上を狙った改善方向を打ち出し、システム（ELSTER）構築に着手した。

  2001 年 1 月 1 日、システム拡張改善を実施した。

  Secunet 社は、セキュﾘﾃｨ基盤開発を担当した。

  ここで使用された暗号標準は、PKCS #7、PKCS #10、PKCS #11、PKCS #12、XMLDS などである。

- **国際標準暗号を使用したシステム**

  国家標準に無い国際標準を使用したシステム構築例は、無い。

7. オーストラリア

7.1. オーストラリアの概要

7.1.1. 電子政府普及の状況

- **電子政府への取り組み**

1997年12月、時のジョン・ハワード首相は‘Investing for Growth’において、すべての適切な政府サービスは2001年までにオンライン化するとの政策を発表した。
続いてオーストラリア政府は、‘Electronic Transactions Act 1999’を出し、さらに、2000 年 4 月、‘Government Online Strategy’を発表した。[1]
これら戦略の狙いは、政府機関の主要機能のオンライン化実行におけるフレームワークを定めるものであった。特に

① 2001年までに、適切なサービスは全てオンライン化可能とする。但し、既存の電話、FAX、カウンターサービスを補足する手段とする。
② プライバシー、セキュリティ、アクセシビリテイ等重要な分野につき、最小限の基準を提供する。

ものであった。
2002年、‘Better Services、Better Government’が発表され、更なる電子政府拡大の支援枠組みとなった。この戦略の狙いは、政府の情報サービス提供、運用管理に、より理解しやすく統合化されたアプリケーションを適用すること、また次フェーズへの移行を描き出すものであった。

- **電子政府展開の現状**

各国の電子政府展開の相対的位置比較がいくつか試みられており、その中でオーストラリアは先進リーダーとして位置付けられている。
2005年、アクセンチュアが発表した‘電子政府・リーダーシップレポート’では、オーストラリアは3位にランクされている。また、2004 年国連から出版された‘E-Government Readiness Report’では、6位にランクされている。
これは、オーストラリアが電子政府において革新リーダーであると同時に、インターネット基盤整備、普及においても世界のリーダーであることを意味する。
事実、2004年度で61%の家庭がインターネットへのアクセスを行っている。ブロードバンドの利用については、2004年11月に42%であったが、2005年4月には51%に急増した。
2004 年度における、電子政府サービスの活用、満足度について、AGIMO による以下の調査結果がある（AGIMO；Australian Government Information Management Office）。[2]

① オーストラリア人の大人は、10人中7人が過去にインターネットを使ったことがある。
② オーストラリア人の大人の39%が、政府との接触にインターネットを使っている。（2002年の調査では、21%であった。）
③ インターネット経由での政府サービスへのアクセス順位は、
所得税、個人税（16%）、土地（格付け、税）（10%）

[1] http://www.agimo.gov.au/publications/2004/05/egovt_challenges
[2] http://www.agimo.gov.au/

車、ボート、他乗り物の登録/免許 （8%）
④ オンライン政府サービスを利用したユーザの 90%が、その結果に満足している。
⑤地域サービスと社会サービスが、もっともアクセスの多いサービスである。

1 例として e-Tax システムをあげると、このシステムは、1997 年オーストラリア税務局によってつくられ、公開鍵暗号の電子署名フレームワークを使った歳入システムとして、世界初のものであった。2004 年 12 月度時点で 80%以上の税金還付がこのシステムで行われ、さらに増え続けている。

7.1.2. 暗号政策の担当政府機関

DSD；Defence Signals Directorate（国防監督局）[1]

DSD は、オーストラリア国防省（Department of Defence）の一機関として、オーストラリアにおけるコンピュータおよび情報セキュリティに関する警告を発動する国家機関である。DSD は主に 2 つの役割を果たしている。

① 海外の秘密情報（Sigint 部門）の収集及び普及
② オーストラリア政府及び国防省に対し、情報セキュリティ（Infosec）製品及びサービスの提供

上記②項の役割を遂行するなかで、DSD は下記の技術支援サービスを行う。

- 官、民を問わず、暗号サービスを伴う製品の選定、使用に対する技術支援
- AISEP（Australian Information Security Evaluation Program）[2]により評価されたセキュリティ製品の選定、使用に対する技術支援
- PKI 展開におけるシステムの評価、認証
  例えば、e-Commerce における PKI サービス、関連活動においてその確立、運用についてガイダンスを提供する。

これらの支援サービスは、DSD が発行、運用する **ACSI-33（Australian Government Information and Communications Technology Security Manual）**[3]に詳しく詳細が定義づけられている。このマニュアルには、政府機関同志、又は政府と民間サービスプロバイダ間における情報交換、データ交換等において、保証された情報セキュリティ環境を達成するために準拠すべきガイダンスが提供されている。ここには、DSD によって承認された ICT セキュリティ標準が、暗号技術を含め、詳細に定義されている。

7.1.3. 電子政府システムでの暗号の使用

上述したように、**ACSI-33** には、政府機関同士、又は政府と民間サービスプロバイダにおける情報交換、データ交換等において、保証された情報セキュリティ環境を達成するために準拠すべきガイダンスが、暗号技術を含め提供されている。

1 例として e-Tax システムをあげると、このシステムは、1997 年オーストラリア税務局によってつくられ、公開鍵暗号の電子署名フレームワークを使った歳入システムとして、世界初のものであった。2004 年 12 月度時点で 80%以上の税金還付がこのシステムで行われ、さらに増え続けている。

[1] http://www.dsd.gov.au/infosec/
[2] http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep.html
[3] http://www.dsd.gov.au/library/infosec/acsi33.html

7.1.4. 電子政府における非 ISO/IEC 暗号の利用

下記の暗号アルゴリズムは、オーストラリア DSD 標準（ACSI-33）にあるが、ISO/IEC には正式採用されていない。

分類	アルゴリズム名
公開鍵暗号	ECDH
共通鍵暗号 （ブロック暗号）	該当なし

7.1.5. 電子政府における ISO/IEC 暗号の利用

下記の暗号アルゴリズムは、オーストラリア DSD 標準（ACSI-33）にあり、かつ ISO/IEC にも正式採用されている。

分類	アルゴリズム名
公開鍵暗号	・ RSA ・DH ・ DSA ・ECDSA
共通鍵暗号 （ブロック暗号）	・ Triple DES（TDEA） ・ AES

補足；

① DSD が承認したアルゴリズム（ACSI-33 による）を使っていないモジュールは、例え FIPS-140 で評価されていても、オーストラリア政府の情報保護の立場から、使用を許可されない。

② DSD は、DACPs（DSD Approved Cryptographic Protocols）を除いて、AISEP かもしくは CCRA（Common Criteria Recognition Arrangement）の承認を得ていない暗号技術は許可しない。[1]

7.1.6. 電子政府の暗号製品のサプライヤ

SecureNet Limited；ネットワークセキュリティ製品、PKI 関連製品/サービスに大きな実績を持つ暗号製品/サービスベンダー。オーストラリア及びニュージーランドで主に事業展開をしている。電子政府及び電子ビジネスの認証システム/暗号製品、認証局運営に大きな実績を持つ。

[1] http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep_partners.html

7.2. オーストラリアの暗号政策

7.2.1. 暗号技術政策を主管する政府機関

オーストラリア国防省の一機関である DSD（国防監督局）が、コンピュータや、暗号技術を含む情報セキュリティに関して主導的な役割を果たす。東西冷戦終結後、皮肉にも世界はますます不確実性を増し、オーストラリア政府はそれに的確に対応するために、タイムリーな行動、情報の収集を必要とした。また、昨今の情報技術の革新が生み出した新しい生活、新しいビジネス形態（電子商取引、電子政府等）に対応する情報通信インフラに対する技術支援を必要とした。

DSD の Information Security Group は、オーストラリア政府の情報通信システムの保全に重要な役割を担っている。電子的及びそれに類する手段で所有、保管、通信される情報に対して、Information Security Group は、以下の責務を持っている。

- オーストラリア連邦政府各省、内閣や王室等の権威、国防省に対して、政府情報のセキュリティ、統合性、およびそれが国家安全保障に影響を与えるような損失や漏洩について、資料、アドバイス、援助を提供する。
- 国家安全保障には関係しないが、プライバシー、ファイナンス、またはその他の理由で許可なく公開されてはならないような、機密性の高い政府情報に関連して、政府各省および権威からの要求に基つきアドバイスを提供する。
- 国防省長官を通じて、国家安全保障長官委員会（Secretaries Committee on National Security）に常時、通信とコンピュータのセキュリティの状況について情報提供を行う。

Information Security Group は、政府各省および権威に対するサポートに加えて、新しい暗号技術を評価し、暗号製品の開発に向けて産業界と協業する上での重要な役割を担う。AISEP を運営管理し、AISEP の評価結果を承認する認定機関である ACA（Australian Certification Authority）にスタッフを派遣している。
（AISEP は、オーストラリアで増大しつつあった IT セキュリティ評価サービスへの需要に対応するために、1995 年に設立された。）

- **本部所在地**

Information Security Group
Defence Signals Directorate
Locked Bag 5076
KINGSTON ACT 2604

- **規模（職員数、予算等）**

DSD は国防省に属しており、国家安全保障に関する情報であるので公開されない。
民間機関からの情報によると、2002 年度で DSD スタッフ約 60 名、AISEP 担当者 6 名であった。

7.2.2. 政府調達における推奨･標準暗号の選択方針と手順

オーストラリア政府は、政府省庁が使うべき国家安全保障にはかかわらないレベルの標準暗号を定めている。暗号サービスは、システムやアプリケーションに安全なセキュリティ対策を提供する上で

重要である。暗号は、情報の機密性、統合性を守り、認証と否認防止を確保するために使われる。
暗号に関する DSD の具体的任務は下記である。

① 国家安全保障には関わらない情報を保護するための標準暗号を定める。
② 政府省庁に適用する暗号鍵回復の最低限の標準を定める。
③ AISEP の補助で実施される暗号製品の評価のためのガイドを提供する。
④ 暗号鍵管理の計画策定のためのガイドを提供する。

標準暗号は、ACSI-33 に詳細に定義されている。
DSD は、標準暗号アルゴリズムの採用/改廃およびそれら変更に関する情報の提供も含め
任務を負っている。
例えば

① DES（56 ビット）の再評価と廃止の決定、通知、既存システムの改修要否に関する方針の通知[1]
② ハッシュ関数 SHA-1、MD5 への衝突困難性の議論に関する解説、対処要否の判断指示[2]

暗号評価には多大な時間、労力、資源がかかるため、DSD では標準暗号を選定するために独自に多くの暗号評価をやることはできない。
むしろ、既に市場でもっとも広く受け入れられており、安全性に問題がないことが実証されている暗号を選び、それを評価して、政府が使うべき標準暗号として採用している。
これはコスト効率の良いやり方で、多大な努力の末に標準化したものが市場と乖離しているために結局は使われない、というリスクも低減できる。

7.3. 電子政府での暗号製品の調達

7.3.1. 暗号製品調達の政府方針と手順

DSD の運営管理する AISEP の目的は、オーストラリア政府が使用するために商用レベルで評価された暗号製品を提供することである。
AISEP は、政府の監督下でライセンスを受けた民間の評価機関が評価を実施するという形をとる。
オーストラリアの政府ユーザーにとっては、MRA（Mutual Recognition Arrangement）署名以降に提出されたすべての妥当な認証が DSD により自動的に承認される。一方海外で評価され DSD の EPL（Evaluated Products List）に掲載されたいくつかの暗号製品は、暗号システムの基準により、政府関係機関での利用に適合するか、DSD によるレビューを受ける必要がある。オーストラリア政府機関で利用される暗号製品選定の基準は、DSD の EPL にある。

7.3.2. 電子政府のための推奨･標準暗号アルゴリズム

しかるべき情報やシステムを守るために暗号を活用しようとする政府省庁は、DSD の定める標準（ACSI-33 に詳細定義）に従うことが義務付けられる。
ACSI-33 に定められた標準暗号アルゴリズムは、以下の通りである。

[1] http://www.dsd.gov.au/library/infosec/single_des.html
[2] http://www.dsd.gov.au/library/infosec/hash_function.html

- **公開鍵暗号**

分類	アルゴリズム名	使用方法	使用条件
離散対数	Diffie-Hellman (DH)	暗号セッション鍵	最小 1,024 ビット
	Digital Signature Algorithm (DSA)	ディジタル署名	最小 1,024 ビット
楕円曲線暗号	Elliptic Curve Diffie-Hellman (ECDH)	暗号セッション鍵	Field/key size 最小 160 ビット
	Elliptic Curve Digital Signature Algorithm (ECDSA)	ディジタル署名	Field/key size 最小 160 ビット
素因数分解	Rivest-Shamir-Adleman (RSA)	ディジタル署名 鍵配送	最小 1,024 ビット

- **ハッシュ関数**

アルゴリズム名	備考
Message Digest v5 (MD5)	AS 2805.13.3 RFC 1321
Secure Hashing Algorithms (SHA-1、SHA-224、SHA-256、SHA-384、SHA-512)	AS 2805.13.3 FIPS 180-2

補足;
DSD は、上記の中で SHA ファミリーの使用を推奨している。

- **共通鍵暗号**

アルゴリズム名	使用条件	備考
Advanced Encryption Standard (AES)	鍵長 128/192/256 ビット	FIPS 197
Triple DES (3DES)	下記どちらかの使い方 2 つの別個鍵(112 ビット) 3 つの別個鍵(168 ビット)	AS-2805.5.4 ANSI-X9.52

補足;
DES (56 ビット) は、もはや標準からはずされ、許可されない。

7.3.3. 電子政府での暗号製品利用の現状

1 例として e-Tax システムをあげると、このシステムは、1997 年オーストラリア税務局によってつくられ、公開鍵暗号の電子署名フレームワークを使った歳入システムとして、世界初のものであった。2004 年 12 月度時点で 80%以上の税金還付がこのシステムで行われ、さらに増え続けている。

7.3.4. 国際推奨･標準、非国際標準製品に対する方針

7.1.4 に挙げた暗号アルゴリズムは、オーストラリア DSD 標準（ACSI-33）にあるが、ISO/IEC には正式採用されていない。
ここまで述べてきた標準選定の経緯から、これらのアルゴリズムは、オーストラリア政府の推奨アルゴリズムであり、当然オーストラリア国内での使用は許可される。

7.3.5. 非国際推奨･標準、国際標準製品に対する方針

7.1.5 でも述べたように、DSD が承認したアルゴリズム（ACSI-33 による）を使っていないモジュールは、例え FIPS 140 で評価されていても、オーストラリア政府の情報保護の立場から、オーストラリア国内での使用を許可されない。
AISEP に対し製品評価を申請するベンダは、その製品の暗号機能を DSD に評価させるか、FIPS 140 の基で評価させるかを選択する。後者の場合、DSD がオーストラリアの国家暗号政策との適合性を確認すべく評価レポートを精査し合否決定する。事実、FIPS 140 の基で承認されているいくつかのアルゴリズムは、DSD の承認を得られていない。[1]

7.4. 暗号国際標準に関する方針

7.4.1. 暗号国際標準に関する方針

暗号評価には多大な時間、労力、資源がかかるため、DSD では標準暗号を選定するために独自に多くの暗号評価をやることはできない。
むしろ、既に市場で最も広く受け入れられており、安全性に問題がないことが実証されている暗号を選び、それを評価して、政府が使うべき標準暗号として採用している。
これはコスト効率の良いやり方で、多大な努力の末に標準化したものが市場と乖離しているために結局は使われない、というリスクも低減できる。
結果として、オーストラリアの暗号国家標準は、その選定手順からわかるように、
国際標準暗号ときわめて近い内容になる。

7.5. 電子政府のサプライヤ

7.5.1. SecureNet Limited

[1] http://www.dsd.gov.au/library/infosec/fips_140.html

企業プロフィール[1]

ネットワークセキュリティ製品、PKI 関連製品/サービスに大きな実績を持つ暗号製品/サービスベンダー。オーストラリア及びニュージーランドで主に事業展開をしている。電子政府及び電子ビジネスの認証システム、認証局運営に大きな実績を持つ。

国家推奨・標準暗号を使用したシステム

標準暗号を使用したネットワークセキュリティ製品、PKI 関連製品/サービスを、AISEP 認証製品リストに多く連ね、電子政府での活用に供している。

[1] http://www.securenet.com.au/

8. 韓国

8.1. 韓国の概要

8.1.1. 電子政府普及の状況

UN Global E-Government Survey 2003, 2004(UN DESA)によると韓国の電子政府準備指数は、2003 年にドイツに次いで 4 位の 0.744、2004 年にはアメリカに次いで 0.857 の 2 位、またオンライン参加指数は 2003 年アメリカの 0.966 に次いで 0.483 の 3 位、2004 年にはシンガポールの 0.836 に次いで 4 位とされる。また、2003 年度の Information Society Index (DC, 2004)は 904.1 とカナダの 924.9 に次ぐ 4 位であり、インターネット利用率を示す World Telecommunication Indicators 2004 (TU, 2004)は 60.97 とアイスランドに次ぐ 2 位にランクされているなど、環境的には整っているにもかかわらず、電子政府指数は世界第 15 位水準（2003、UN）に留まっている。

行政自治部の対国民サービスの窓口である大韓民国電子政府(G4C)・調達庁の統合電子調達システム(G2B)・国税庁の総合国税システム(Home Tax System)などによって代表される韓国の電子政府(実際には高速国家網・地方行政網や民間のネットワークなどを通じてつながる各機関が運営するシステムの巨大なネットワーク)の現状を見てみると、2004 年下半期の電子決裁及び電子文書の流通率は各 96.9%及び 97.4%、税金の電子処理において 2004 年の電子申告件数 11,694 千件、2005 年電子人事システム利用率約 90%、行政サービス申請(総数 1,020 種)中インターネットによる申請可能サービスの数は、2005 年 499 種・2006 年 800 種(計画)・2007 年 1,000 種(電子政府 11 大課題理用現況調査、2004.12)、政府に対する情報公開申請においてインターネット情報公開システムによる申請率 23%(インターネット情報公開システム利用現況、2004)と、2007 年まで電子政府指数基準、そのレベルを世界第 5 位水準まで引き上げることを目標に持続的に整備・開発が続けられている。ちなみに 2006 年度の電子政府予算は前年比 12.3%増額の 4,469 億ウォンであり、過去・将来計画を通し最大である。

韓国の電子政府事業推進は大きく 3 段階に分けて展開されてきた。初期段階の電子政府は 1994 年に情報通信部が設立され、1995 年に「情報化促進基本法」が制定されることにより、情報化促進委員会・情報化促進基金が設立される。以後、韓国電算院の技術支援及び基金からの資金支援のより各行政機関内のフロント及びバック・オフィス開発レベルの電子政府事業が展開された。第 2 段階としては、金大中大統領の「国民の政府」にて 11 大事業を中心に、多機関関連事業を推進する為、2001 年 1 月、政府革新推進委員会に電子政府特別委員会が設置・運営された。第 3 段階としては、現在の「参与政府」の政府革新地方分権委員会に電子政府専門委員会が設置され、31 大汎政府事業を推進中である。

現政権におき、電子政府事業は、1)仕事のやり方革新（G2G）、2）政府サービスの革新（G2C, G2B）、3)情報資源管理の革新(共通基盤)の 3 分野においての革新を通し、①原則と信頼、②公定と透明、③対話と妥結、④分権と自律の 4 大国政原理を導き、政権の国政目標を達成する為の抜本的、最も重要な事業であり、31 大課題のロードマップを作成し、汎政府レベルで積極的に進められている。

電子政府ロードマップの推進は、さらに 2 段階･5 レベルに分けられており、2003-2005 年を第 1 段階(基盤整備)とし、行政内部業務及び共通基盤構築･選別敵対国民/大企業サービス革新、2006-2007 年を第 2 段階(サービスの高度化)とし、行政内部業務情報化の高度化･対国民/大企業統合サービスを構築することにより、最終的には、部署間/機関間の境界がないサービスを提供し、電子政府化指数（UN）を世界第 5 位以内に引き上げることを目標に進められている。

電子政府特別委員会が推進した 11 大電子政府事業

事　　業	主 管 機 関
情報化を通じた国民志向的対民サービス（G4C)	行政自治部･情報通信部･企画予算庁
4 大社会保険情報システム構築	保険福祉部･労働部
政府統合電子調達システム(G2B)	企画予算庁･情報通信部
インターネットを通じた総合国税サービス体系構築	国税庁･財政経済部
国家財政情報システム	財政経済部･企画予算庁
市･郡･区行政総合情報化	行政自治部･ソウル市
教育行政情報システム構築	教育人的資源部･財政経済部
標準人事管理システム(PPSS)構築	中央人事委員会
電子決裁及び電子文書流通の定着	行政自治部
電子官印システム構築及び電子署名システムの拡散	行政自治部･情報通信部
汎政府的統合電算環境の段階的構築	行政自治部

電子政府 31 大ロードマップ課題及び担当機関

分野	アジェンダ	課題/細部推進課題	主管機関
仕事のやり方革新	電子的業務処理定着	**1.文書処理全過程電子化**	
		1.1.電子文書流通システム拡充及び流通体系高度化	行政自治部
		1.2.記録物管理体系構築	国家記録院
		1.3.文書台帳の電子化	行政自治部
		2.国家及び地方財政総合情報化	
		2.1.地方財政情報化	行政自治部
		2.2.国家財政情報高度化	財政経済部
		3.電子地方政府の具現	
		3.1.市･道行政情報化	行政自治部
		3.2.市･郡･区行政情報システム高度化	行政自治部
		6.統合刑事司法体系構築	大検察庁
		7.人事行政総合情報化	
		7.1.自治体人事行政情報システム構築	行政自治部
		7.2.電子人事管理システム高度化	中央人事委員会
		8.外交通産情報化	外交通産部
		9.国政課題実時間管理(政府業務管理システム)	行政自治部
	行政情報共同利用拡大	**10.行政情報共有拡大**	
		10.1.行政情報共同利用拡大	行政自治部
		10.2.汎国家情報共同利用推進戦略樹立	行政自治部
		10.3.行政機関の知識管理体系拡散	行政自治部
	サービス中心業務再設計	**11.政府機能連携モデル(BRM) 開発**	行政自治部
サービスの拡大	対国民サービス高度化	**12.インターネット行政サービス高度化**	行政自治部
		13.国家安全管理総合サービス	

		14.建物･土地登記連携及び高度化 14.1.建築行政高度化 14.2.不動産情報管理及び連携 14.3.建築物台帳整備	 建設交通部 行自部･建交部 建設交通部
		15.総合国税サービス高度化	国税庁
		16.国家福祉総合サービス	保健福祉部
		17.食･医薬品総合情報サービス 17.1.食･医薬品安全管理サービス 17.2.農･畜･水産物安全管理サービス	 食品医薬品安全庁 農林部･海洋水産部
		18.雇用･就業情報サービス	労働部
		19.行政審判インターネットサービス	法制処
	対企業 サービス 高度化	**20.企業支援単一窓口(G4B)サービス**	産業資源部
		21.国家物流総合サービス	海洋水産部･関税庁
		22.電子貿易サービス	産業資源部
		23.外国人総合支援サービス	産業資源部など
		24.電子政府海外進出支援	情報通信部
	電子的 国民参与	**25.オンライン国民参与拡大** 25.1.オンライン国民参与拡大 25.2.電子政府サービス利用活性化 25.3.行政情報オンライン公開拡大 25.4.電子投票及び電子選挙	 行政自治部 行政自治部 行政自治部 中央選挙管理委員会
情報資源管理革新	**情報資源 統合 標準化**	**26.汎政府統合電算環境構築**	情報通信部
		27.電子政府通信網高度化	情報通信部
		28.汎政府情報技術アーキテクチャ(ITA)適用	情報通信部
	情報保護 体系強化	**29.情報保護体系構築**	国家情報院など
	情報化人力 組織専門化	**30.情報化人力及び運営組織強化･整備**	行政自治部
法制整備	**電子政府 法制整備**	**31.電子政府具現及び安全性関連法制整備**	情報革新地方分権委員会
合計	10大 アジェンダ	**31 個課題、45 個細部課題**	-

出典:

- 2005 電子政府事業年次報告書(行政自治部、韓国電算院)
- 電子政府の未来像(韓国電算院)

8.1.2. 暗号政策の担当政府機関

韓国における暗号を含む情報セキュリティの担当政策機関は国家情報院(National Intelligence Service)であり、情報セキュリティ・システムの認証などは同院の **IT 保安認証事務局**[1]が担当している。

8.1.3. 電子政府における暗号の使用

電子政府における暗号の使用については、2段階の政策が実施されている。暗号製品は単体でエンド・ユーザー(電子政府)に納品される例はなく、情報セキュリティ製品に搭載される形で導入されている。

第一段階として、民間企業の情報セキュリティ製品が電子政府に採用されるためには、国家情報院 IT 保安事務局の「商用情報保護システム適合性検証制度」により検証されなければならない。この検証制度では、侵入遮断システム・侵入探知システム・ネットワーク情報セキュリティ製品群・ネットワーク情報保護製品群・コンピューティング情報保護製品群・情報保護基盤製品群のカテゴリーに分け、製造会社・製品・バージョンにより特定された製品ごとの検証及びセキュリティレベルを発給している。

第二段階として、これら国家情報院のセキュリティ適合性検証を得た製品に対し、その製品に暗号モジュールが搭載される場合、暗号モジュールの採択には別途の政策が施行されている。まず、該当する情報セキュリティ製品の用途が国家・公共機関間の場合、これらの情報セキュリティ製品に搭載される暗号モジュールには、国家情報院が提供する国家機関用暗号モジュール(非公開アルゴリズム)を採用しなければならない。

次に、その用途が諸証明の発行、電子申告、一般情報の検索・閲覧など対国民・市民に対する行政サービス(対国民行政業務用：G2C 及び G2B)である場合、2004 年までは特に決められた暗号アルゴリズムの推奨などは無く、使用機関又は納品業者により自律的に選択されたものが使用されてきた。しかし、民間企業が製作する暗号モジュールの場合、ビジネス上の理由により、複数の国内・国際標準アルゴリズムに対応するものが一般的であり、SEED （ISO/IEC 18033-3、IETF RFC 4269）、ARIA(韓国技術標準公示第 2004-1149 号）、DES（Triple DES）、AES などのアルゴリズムが代表的である。

その後、電子政府の対国民行政業務用システムに適用される暗号モジュールについては、2005 年から新たに実施された、国家情報院の「暗号試験及び認証制度」が適用されることになった。この制度では、民間企業製作の暗号モジュールを製造会社・製品種類・バージョン等によって特定された製品ごとに試験及びセキュリティレベルの認証を行い、合格したもののみが当該電子政府システムでの使用が可能になった。ここで、暗号検証制度による検証とは、国際標準規格などで定められたアルゴリズムや方式など基本的仕様の検証ではなく、実際に「製品」として実装された特定暗号モジュールに対し実使用上の安全性を試験するものである。

このように、韓国、特に電子政府における、暗号を含む情報セキュリティ製品に関する政策は、実装された特定製品ごとに、その安全性を検証することを基本としており、ISO/IEC などの標準方式別の分類は難しい。

[1] http://www.kecs.go.kr/default.jsp

8.1.4. 電子政府の暗号製品のサプライヤ

2005 年から正式施行に入っている暗号検証制度の下で検証申請･検証契約締結の段階まで進んだベンダとしては、この報告書執筆の時点で、Softforum㈱、㈱Initech、㈱Oullim の 3 社がある。この中で㈱Softforum は 2005 年 11 月に検証試験を完了、他の 2 社は予備検証を通過、2005 年 9 月に検証試験契約が結ばれており、現在検証の本試験中である。

8.1.5. 電子政府のシステムインテグレータ

Samsung SDS、LG CN、SK C&C、Ssanyong 情報通信、Daewoo 情報システムなど大手財閥系が中心である。適用暗号に関しては公開情報はない。

8.2. 韓国の暗号政策

8.2.1. 暗号技術政策を主管する政府機関

国家情報院(National Intelligence Service)
国家情報院は、国家情報院法･保安業務規定等の法令に基づく、国家情報保安業務の企画･調整及びセキュリティ政策の樹立･試行など、国家･公共機関に対する情報セキュリティ業務を総括する機関であり、国家･公共機関用暗号装置等の開発･普及、情報保護システムの認証業務、中央行政機関網･自治体網･公共機関網などの公共分野情報通信網に対し直接安全性を確認するなど、暗号を含む韓国の国家レベルでの情報セキュリティの総括機関である。

暗号検証委員会
国家情報院の「暗号検証制度」により設立された官･学･研の 15 人以内で構成される検証委員会であり、対国民行政業務用として検証対象になる暗号アルゴリズムの推奨リストにかかわる政策、基準、承認及び暗号検証制度による試験･検証の結果に対する妥当性･公定性などを審議･議決する。

その他、暗号を含む情報セキュリティの専門研究機関としては

- **国家セキュリティ技術研究所(National Security Research Institute)**

  国家セキュリティ技術研究所は、重要情報通信基盤施設などを保護する為の技術開発及び支援、国家･公共機関の情報通信システム及び情報通信網に対するサイバー侵害に効果的に対応する為の技術及び政策の開発･支援を目的に 2000 年に設立された情報保護専門研究機関であり、国家情報通信セキュリティ基本指針･国家情報通信技術開発指針などを含む公共分野のサイバー関連技術の確保を目的とした研究開発を行う。

  電子政府において、行政機関が対国民サービスを提供する為に設置される情報セキュリティ製品に搭載する暗号モジュールの安全性を検証する暗号検証制度の下での暗号モジュール試験機関（2005 年からの1段階）である。

- **韓国情報保護振興院（Korea Information Security Agency; KISA）**

  情報通信部(Ministry of Information and Communication; MIC) の傘下にあり、調査、情報提供、事業提案などを通じて MIC を支援する一方で、情報セキュリティ関連研究開発を行い、公的認証最上位機関としての役割を持ち、さらに、プライバシー侵害やスパムメールへの対応などのセキュリティ対策を行う。

  1996 年「情報化促進基本法」により韓国情報保護センターとして出発、その後 2001 年 7 月から改正・施行された「情報通信網利用促進及び情報保護などに関する法律」に」より韓国情報保護振興院に昇格された。民間分野情報保護のための政策及び制度の調査研究・技術開発・標準及び基準開発・情報保護システムの研究開発・個人情報保護の為の対策研究などを行う。また、電子署名法に基づく公認認証書の民間最上位認証機関である。

  電子政府において、行政機関が対国民サービスを提供する為に設置される情報セキュリティ製品に搭載する暗号モジュールに対する安全性を検証する「暗号検証制度」の下での暗号モジュール試験機関（2006 年からの 2 段階で追加）である。

- **韓国電子通信研究院(ETRI) 情報保護研究団(Information Security Research Division, ETRI)**

  韓国電子通信研究院(ETRI)内の情報保護研究団は通信・放送・インターネットの大統合(u-Korea)時代の到来と共に、重要ネットワークインフラの障害、有害情報の流通、個人情報流出などの情報化の阻害要因を解消する先導技術を確保し、情報技術の速やかな産業化を支援する。

出典
- 2005 国家情報保護白書(国家情報院)
- 韓国情報保護振興院（KISA)

8.2.2. 政府調達における推奨・標準暗号の選択方針と手順

2005 年から実施されている、韓国電子政府の対国民行政業務用の検証対象暗号アルゴリズムの選定方針は大きく

- 用途に適合である安全性 → 計算複雑度 2^{80} 以上
- 既存に政府機関で使用されているアルゴリズムを収容 → 既存製品との互換性確保

の 2 点であるが、選定基準の詳細は非公開となっている。

これら、検証対象暗号アルゴリズムの選定に関する方針・選定基準・リストの入れ替えなどは、全て暗号検証委員会の承認を得て決定される。

出典
- 暗号検証示範事業説明会（NSRI、2004.07.16）
- KISA

8.3. 電子政府での暗号製品の調達

8.3.1. 暗号製品調達の政府方針と手順

国家情報院の「国家情報セキュリティ基本指針」により、各政府機関は、商用情報保護システム又は情報保護機能が搭載された情報通信システムを使用する場合、検証に合格した情報保護システムを導入しなければならない。

電子政府法第25条(標準化)及び第27条(情報通信網等のセキュリティ対策樹立·施行)、事務管理規定第105条(機器及び利用技術の標準化)により、各行政機関が情報セキュリティ製品を選択する際、「行政情報保護用システム」として選定された製品を優先的に考慮し、「行政情報保護用システム」を導入した場合、製品に対するセキュリティ機能の検討は省略される。(但し、関連事業に対するセキュリティ性検討は別途に推進。)

但し、各行政機関でまだ「行政情報保護用システム」として選定されていない情報保護用システムの使用を要望する場合、次の手順で国家情報院のセキュリティ適合性検証を得れば導入することができる。また、これら情報セキュリティ製品に暗号モジュールが搭載される場合、各行政機関は別途、国家情報院長に「国家機関用暗号モジュール」(非公開)を要請して使用するものとされる。

① 行政機関は情報セキュリティ製品ベンダに必要資料の作成·提出を要請
② 行政機関は国家情報院にセキュリティ適合性検証を要請
③ 国家情報院はセキュリティ適合性を試験検証
④ 国家情報院はセキュリティ適合性試験·検証結果を行政機関に通知
⑤ 国家情報院はセキュリティ適合性試験·検証結果を行政自治部に通知
⑥ 検証合格の場合、行政自治部は「行政情報保護用システム」として選定·公示
⑦ 行政自治部は調達庁に第3者の為の製品単価契約依頼
⑧ 調達庁は生産業者と第3者の為の製品単価契約を締結、その結果を官報に公示
⑨ 各行政機関は「行政情報保護用システム」を調達·購入

手順③のセキュリティ適合性検証は国家情報院の国家情報セキュリティ基本指針第 92 条～102 条により定められており、検証の対象になるのは情報化促進基本法又は情報保護製品国際相互認証協定(CCRA)から認定書が発行された製品に限られている。また、提出資料として、「暗号モジュール試験及び認証指針」に基づき発行された検証書の写しの提出が要求されており、暗号モジュールが搭載された製品に関しては、国家情報院の「暗号認証制度」により試験合格とされた暗号モジュールの搭載が必須とされる。

電子政府において、行政機関が対国民サービスを提供する為に設置される情報セキュリティ製品(同じく検証合格製品)に搭載する暗号モジュールに対しては、製品全体のセキュリティ適合性検証とは別に国家情報院が「暗号試験及び認証指針(2004.12)」に基く「暗号認証制度」(2005.01 施行)により安全性を検証した暗号モジュールを使用するものとされている。

＜暗号検証制度＞

- **関連法令**

行政自治部公示第 2004-45 号(官報 15885 号)、「暗号試験及び検証指針」 (公示 2004.12.31)、電子政府具現の為の行政業務などの電子化促進に関する法律施行令第 34 条第5項に法律的根拠を置く。

- **目的及び対象**

電子政府におけるセキュリティ対策により暗号製品の需要が発生し、民間開発暗号製品の国家機関使用が増加する状況下で、行政情報サービスの為に情報通信網で使用される暗号モジュールの必要性が大きくなっている。そのため、電子政府法施行令第 34 条第 5 号にて規定される、国家情報院長のセキュリティ対策の効率的実施の為、各政府機関で使用する暗号モジュールの試験及び認証などに必要な事項を定め施行する.

- **検証対象暗号モジュール**

行政機関が対国民行政サービスを提供する為に設置した情報セキュリティ製品に搭載される暗号モジュールを対象とする。但し、暗号モジュール試験及び認証に合格したモジュールは、国家機関の間の情報交換の為に使用されてはならず、秘密情報の交換に使用してはいけない。

- **暗号検証制度**

暗号検証制度は、電子政府情報システムにおいて、機密に分類されない重要情報を保護する為の暗号製品(暗号モジュール)に対し、安全性と実装の正確性をセキュリティ要求事項に準じて検証するための制度である。

暗号検証のセキュリティ要求事項は暗号モジュールが提供すべきセキュリティ機能を規定するものではあるが、セキュリティ要求事項を満足するからと言って特定の暗号モジュールが安全である事を保証するものではない。同じく、検証された暗号モジュールを使用しても、情報システム全体の安全は保証されない。

暗号モジュール運用者は応用分野及び環境によって適切なセキュリティレベルの暗号モジュールを選択しなければならない。各機関の情報担当部署又は担当者は暗号モジュールを利用する情報システムが応用分野及び環境にて要求されるセキュリティレベルを提供するかを確認しなければならない。

- **暗号検証制度の体系**

1. 検証機関

検証機関は国家情報院とし、次の業務を随行する。

1. 国家用暗号モジュール認証制度設置及び施行

2. 試験機関の試験業務管理·監督及び試験結果認定
3. 認定書発給
4. 認定申請者と試験機関官の紛争調整
5. 国家用暗号モジュール認証目録管理
6. 国家用暗号モジュール試験基準の承認
7. 国家用暗号モジュール試験基準の開発

2. 検証委員会

検証委員会は、行政自治部を含む関係機関、学界、研究機関、検証·試験機関などの専門家の中で検証機関の長が委嘱した 15 人以内の委員で構成され、委員長は委員の中から検証機関の長が決める。

検証委員会は試験·検証結果の妥当性·公定性に対する審議·議決及び申請人と試験機関の間の紛争調整の為に運営される。

3. 暗号モジュール試験機関

暗号モジュール試験機関は、国家セキュリティ技術研究所（NSRI）と韓国情報保護振興院(KISA, 2006 年以後)とし、次の業務を随行する。

1. 暗号モジュール検証契約締結及び試験の施行
2. 暗号モジュール試験基準及び試験関連技術開発
3. その他、暗号モジュール試験関連業務

セキュリティレベル

セキュリティレベル 1

セキュリティレベル1は最も低い水準のセキュリティを提供し、暗号モジュールの基本セキュリティ要件を規定している。(例：暗号モジュールは最小1個の検証対象アルゴリズム又は検証対象セキュリティ機能を使用しなければならない。)　セキュリティレベル1の暗号モジュールを構成する部品は物理的セキュリティを要求しない。セキュリティレベル1で暗号モジュールのソフトウェア及びファームウェア構成要素が評価されていない運営体系を使用する汎用コンピュータで実行されても良い。セキュリティレベル 1 に該当する暗号モジュールの例としては個人用コンピュータ(PC)暗号ボードを挙げることができる。

セキュリティレベル 2

セキュリティレベル 2 は、セキュリティレベル1の物理的セキュリティメカニズムを向上させるため、改竄の証拠又はロック装置要求事項を追加した。改竄の証拠は改竄証拠コーティング又は封印の使用を含み、ロック装置は暗号モジュールのドア又は着脱式カバーに適用され剥がされない物でなければならない。 不法造作証拠コーティング及び封印は暗号モジュール内の暗号鍵と CSP(Critical Security Parameter)に対する物理的接近が行われたとき必ず破損される所になければならない。 不法造作証拠·封印又はロックは許可されない物理的接近を防止できるようカバー又はドアの上に位置しなければならない。

セキュリティレベル 2 は最小限役割基盤認証を要求する。これを通し、暗号モジュールは運用者が特定の役割を受け持つことができるかと、役割に対応するサービスを随行する権限があるかを認証する。

セキュリティレベル 2 暗号モジュールのソフトウェアとファームウェア構成要素は次のような運営体系を使用するコンピューターシステム上で随行されることを許容する。

暗号検証基準添付 2 に登載される国家機関用保護プロファイル中、保証レベル EAL2 以上のプロテクションプロファイルを満足する製品に使用される OS(但し、評価製品と別途に OS を認定しない。)

セキュリティレベル 3
セキュリティレベル 3 は、セキュリティレベル 2 で提供される改竄証拠物理的セキュリティメカニズムに暗号モジュール内に維持される CSP に対する侵入者の接近を遮断するメカニズムが追加されなければならない。セキュリティレベル 3 は暗号モジュールに対する物理的接近、使用及び変造の試みを高い確率で検出し対応する為のセキュリティメカニズムを要求する。物理的セキュリティメカニズムは丈夫な外装の使用、着脱式カバー又はドアーが開けられたとき平文形態の全ての CSP がゼロ化されられる不法造作探知及び対応回路を含むことができる。

セキュリティレベル 3 ではセキュリティレベル 2 で明示された役割認証メカニズムが提供するセキュリティ性を向上させた、身元基盤認証メカニズムが必要とされる。暗号モジュールは運用者の身元を認証し、識別された運営者が特定の役割を受け持つ権限及び該当するサービスを実行する権限をもつかを確認する。

セキュリティレベル 3 は平文の CSP が他のポートと物理的に分離されたポート又は他のインターフェイスと論理的に分離された信頼できる経路を使用して注入･出力されることを要求する。

セキュリティレベル 3 は暗号モジュールのソフトウェアとファームウェアの構成要素が次のような運営体系を使用する汎用コンピューターシステム上で随行されることを許容する。

暗号検証基準添付 2 に登載される国家機関用プロテクションプロファイル中、保証レベル EAL3 以上のプロテクションプロファイルを満足する製品に使用される OS(但し、評価製品と別途に OS を認定しない。)
信頼される経路(FTP_TRP.1)の機能要求事項と否定形的 TOE セキュリティ政策モデル(ADV_SPM.1)の保証要求事項追加。

セキュリティレベル 4
セキュリティレベル 4 は最も高い水準のセキュリティを提供する。このレベルでは、物理的セキュリティメカニズムが許可されない全ての物理的接近の試みを探知し対応する為、暗号モジュールを包む完全な保護外装を提供しなければならない。暗号モジュールは外装を通過しようとする試みを非常に高い確率で探知し、これに対応して即時に平文形態の全ての CSP をゼロ化しなければならない。セキュリティレベル 4 の暗号モジュールは物理的保護が難しい環境で使用することができる。

セキュリティレベル 4 の暗号モジュールは正常的電圧又は温度の範囲を外れる環境条件又は変化による損傷より暗号モジュールを保護する。攻撃者は暗号モジュールの防御装置を無力化するため正常的動作範囲を外れる故意的運営をすることもある。暗号モジュールはこのような変化を感知し CSP をゼロ化するように設計された特別な環境障害保護機能を含むか、暗号モジュールが正常的動作範囲を超える変化に影響されない事を合理的に保証する為の厳格な環境障害試験を通さなければならない。

セキュリティレベル 4 は暗号モジュールのソフトウェアとファームウェアの構成要素が次のような運営体系を使用する汎用コンピューターシステム上で随行されることを許容する。

暗号検証基準添付 2 に登載される国家機関用プロテクションプロファイル中、保証レベル EAL4 以上のプロテクションプロファイルを満たす製品に使用される OS(但し、評価製品と別途に OS を認定しない。)
信頼される経路(FTP_TRP.1)の機能要求事項と否定形的 TOE セキュリティ政策モデル(ADV_SPM.1)の保証要求事項追加。

暗号検証制度の手順

予備検証

1) 申請者は試験機関に検証申請に対する案内を通して必要な支援を要請することができる。
2) 申請者は検証申請書及び提出物を作成し試験機関に暗号モジュール検証を申請する。
3) 試験機関は暗号モジュール試験及び検証のための試験班を構成し、提出物に対する予備検討を行う。
4) 試験機関は予備検討で提出物に不適合事項が発見された場合申請者に提出物の補完を要請する。
5) 申請者は試験機関の提出物補完要請に従って提出物を補完し試験機関に提出する。
6) 試験機関は補完が完了した提出物に対し再検討を行う。
7) 再検討後、提出された検証申請書及び提出物が試験随行に不適合である場合、試験機関は暗号検証契約を拒否する。
8) 予備検討及び再検討後、暗号モジュール試験及び検証実施が可能な場合、試験機関と申請者は「暗号検証契約」を締結する。

試験検証

1) 試験機関は予備検証段階を完了した提出物に対し試験実施計画書を作成する。
2) 試験機関は必要な場合、試験の円滑な実施と提出物に対する理解の為、試験環境支援と提出物に対する説明会の開催を申請者に要請できる。
3) 試験機関は検証及び試験基準を適用し、試験を実施する。
4) 試験機関は提出物の試験実施により補完事項を発見した際、1回に限り申請者に補完を要請することができる。
5) 試験機関は提出物に対する不適合が発生した場合、提出物に対する検証を中断する。
6) 試験機関は試験完了後、試験結果報告書を作成し検証機関に提出する。
7) 試験機関は試験完了した提出物に対し提出物を処理する。
8) (検証委員会は試験結果報告書を審議する。)
9) (検証機関は検証委員会の審議を得た申請に対し検証書を発給する。)

試験実施現況

製品名	申請者	申請セキュリティレベル	検証契約日
Xecurecrypto V1.2.0.2	Softforum	セキュリティレベル1	試験完了
INISAFE Crypto V1.0	Initech	セキュリティレベル 1	2005.09.02
SWCLM V1.0	OSullim	セキュリティレベル2	2005.09.29

出典

- NSRI (http://www.nsri.re.kr/crypto_cert/)

- 2005 年「行政情報保護用システム」選定計画(行政自治部)
- 国家情報セキュリティ基本指針(第 91条-102 条)(国家情報院)
- 暗号モジュール試験及び検証指針(2004.12)(行政自治部)

8.3.2. 電子政府のための推奨･標準暗号アルゴリズム

2005 年 1 月 1 日の暗号検証制度施行以来適用されている「対国民行政業務用検証対象アルゴリズム」は、次のとおりである。

対国民行政業務用検証対象アルゴリズム

ブロック暗号	SEED, ARIA
暗号利用モード（Mode of Operation）	ECB, CBC, CFB, OFB, CTR
MAC	HMAC
ハッシュ関数	SHA-1/-256/-384/-512, HAS-160
乱数生成	FIPS PUB 186-2 DSS Appendix 3 ANSI X9.62 ECDSA Appendix A.4 TTAS.KO-12.0001/R1 KCDSA Appendix 4
公開鍵アルゴリズム	RSAES-OAEP v2.0, RSAES-OAEP v2.1
ディジタル署名	RSASSA-PKCS-v1.5, RSASSA-PSS, KCDSA, ECDSA

対国民行政業務用検証対象アルゴリズムにリストされていないものは、暗号検証制度による検証の対象とされない。したがって、韓国電子政府のシステムに搭載することはできない。

これら対国民行政業務用検証対象アルゴリズムの使用(製品化)に関しては、暗号検証基準 V1.1 によりガイドされている。(暗号検証基準 V1.1 は、資料に対する不法複製･配布、細部内容の漏出及びこれに準ずる行為をしない内容の誓約書を提出した関連業者にだけ渡されるもので、その内容は一般に公開されていない。)

出典：KISA、KISIA

8.3.3. 電子政府での暗号製品利用の現状

現在、暗号検証制度が実施されてわずか 1 年足らずであり、実際に使用事例として挙げられる製品は無い。検証申請･検証契約締結の段階まで進んだベンダとして、㈱Softforum、㈱Initech、㈱Oullim の 3 社が挙げられるのみである。この中で㈱Softforum は 2005 年 11 月に検証試験を完了、他の 2 社は予備検証を通過、2005 年 9 月に検証試験契約が結ばれており、現在検証の本試験中である。

2004 年までは、各行政機関及び納品業者が自律的にアルゴリズムを選択し使用していたが、これら既存に導入された暗号モジュールに対しても今後バージョン･アップなどの際に、対国民行政業務用検証対象アルゴリズムにリストされたアルゴリズムを使い、暗号検証制度により検証合格とされた製品に取り替えられて行く事などが予測される。(既存暗号製品の使用事例に関する詳細な資料は公開されていない。)

出典：KISA

8.3.4. 政府調達における推奨･標準、非国際標準製品に対する方針

特に、これに対応する明確な政策はない。

8.3.5. 政府調達における推奨･標準でない国際標準暗号を使用した製品に対する方針

特に、これに対応する明確な政策はない。

8.4. 暗号国際標準に関する方針

韓国電子政府において、暗号を含むセキュリティシステムの適用は、国家安保の観点からの情報セキュリティと言う概念に根拠するものと見るのが妥当であり、その政策に国際標準との関わりを見出すのは難しい。

8.4.1. 暗号国際標準に関する方針

電子政府に関する限り、国家機関用暗号モジュール及び対国民行政業務用検証対象アルゴリズムのリストが唯一の標準であり、国際標準暗号アルゴリズムに対応するための政策は特にないようである。

8.4.2. 暗号国際標準化活動

自国暗号アルゴリズムの国際標準化活動としては、韓国情報保護振興院(KISA)が開発した 128 ビット 共通鍵ブロック暗号の SEED (TTAS.KO-12.0004)が ISO/IEC(SC 27/WG 2)にて IS 18033-3(2005)： algorithms Part 3. Block ciphers として、また IETF にて RFC 4269：The SEED Encryption Algorithm として採択されているほか、 KCDSA(TTAS.KO-12.0001/R1)/ECKCDSA(TTAS.KO-12.0015)が ISO/IEC(SC 27/WG 2)にて FDIS 14888-3： Digital signatures with appendix Part 3. Discrete logarithm based mechanisms として採択されている。

その他、ISO/IEC(SC 27/WG 2)に対し、IBS-2 電子署名アルゴリズムを同じく IS 14888-3 に、EC-KCDSA 電子署名アルゴリズムを IS 15946(2002): Cryptographic techniques based on elliptic curves Part 2 に、EC-KRN 電子署名アルゴリズムを IS 15946-4(2004): Cryptographic techniques

based on elliptic curves Part 4: Digital signatures giving message recovery に提案しているなど、産業資源部傘下の技術標準院を窓口として国際標準化活動が行われている。

出典：KISA

8.4.3. 電子政府での ISO/IEC 標準暗号の利用と計画

電子政府において、どのシステムにどういう暗号製品(情報セキュリティ製品)が使用されているかに関する情報や統計は公開されていない。これを調査して公開するには当局の許可が必要なものと判断される。しかし、一般的には、これまでに ISO/IEC 18033 の SEED アルゴリズムが幅広く使われてきている一方、電子署名関連分野で ISO/IEC 14888 の KCDSA/EC-KCDSA も多く使用されており、今後も幅広く使用されていくことが推測される。

9. 結果のまとめ

9.1. 調査の実施結果

本調査の最終的な実施状況を以下にまとめた。

調査対象国	政府調達に関する基準、ガイドライン、資料類	政府機関 調査先	サプライヤ 調査先
米国	NIST SP 800-21 Guideline for Implementing Cryptography in the Federal Government, FIPS PUB 140-2 Security Requirement for Cryptographic Module, Federal Acquisition Regulation	NIST-STG	Entrust, Certicom
カナダ	CSE-CST Alert ITSA 11-(b), IT Security Directives ITSD-01 Management of Information Technology Security (MITS)	CAC-ITS, CMVP-CSE	Entrust
英国	E-Government Interoperability Framework Technical Standard Catalog V.6.2, Security e-Government Strategy Framework Policy and Guideline V.4	CESG	—
フランス	Politique de Reference Intersectorielle de Securite (PRIS)	DCSSI	—
ドイツ	Standards and Architecture for e-Government Applications (SAGA)	BSI	Secunet Security Networks
オーストラリア	Australian Government Information and CommunicationTechnology Security Manual (ACSI-33)	DSD	—
韓国	電子政府白書、2005年国家情報保護白書(国家情報院=NIS), 国家情報保安基本指針(国家情報院=NIS), 2005年行政情報保護用システム選定計画(行政自治部)	KISA	—

9.2. 各国暗号政策のまとめ

調査対象7ヶ国の暗号政策の特徴を以下にまとめた。

調査対象国	暗号政策組織	推奨・標準暗号の例	推奨・標準暗号に関する規格	ISO/IEC対応例(ブロック暗号)	特徴
米国	OMB, NIST-STG, NSA-CSS	AES, RSA	FISMA, FIPS 140-1/-2	AES	FIPSに採用された暗号の国際標準化
カナダ	CSE-ITS, CIOB	CAST5, El-Gamal	MITS	CAST5	FIPS指向
英国	CESG	AES, DSA	e-GIF	AES	CAPS (官民協業)
フランス	DCSSI	RSA-OAEP, SHA-256	PRIS	AES	ADELEプログラム (電子政府戦略)
ドイツ	BSI	AES, ECDSA	SAGA	AES	三段階暗号リストとライフサイクル
オーストラリア	DSD	AES, DH	ACSI-33	AES	デファクト採用による効率性
韓国	NIS,NSRI, KISA,ETRI	SEED, ARIA	NIS	SEED	暗号アルゴリズム試験制度開始

9.3. 国際標準と各国標準暗号のまとめ

ISO/IEC 暗号標準と調査対象7ヶ国および日本のそれぞれの国内推奨・標準暗号との対応を別紙の表（「各国標準暗号対応表」）にまとめた。

9.4. 調査結果から得られた知見

本調査の結果を通じて、今後の日本での暗号政策検討のために参考となる知見として、以下のポイントが得られた。

- **国内推奨暗号の役割**
  今回調査した全ての国で、政府が推奨する暗号アルゴリズムの存在が確認された。商用レベルの暗号が要求されている場合では、韓国を除き、殆どの国で推奨する暗号アルゴリズムが公開されていた（韓国では KISA に依頼して入手）。その強制力については、各国で表現の違いはあるものの、基本的には推奨されたアルゴリズムを実装した製品が政府調達の対象となり、「標準」とは明示していないものの、実質的な標準アルゴリズムとなっている。実際の政府調達では、推奨・標準アルゴリズムの採用はあくまで前提条件であって、実装レベルで検証される必要がある。

- **国内推奨・標準暗号以外の暗号の電子政府への採用可能性**
  国内推奨・標準以外の暗号の電子政府への採用については、可能としつつも、評価（コスト・時間がかかる）を必要としている国が多い（米国、カナダ、英国、フランス、ドイツ、オーストラリア）。日本の場合、CRYPTREC との整合性を取り、方針を決定する必要がある。

- **国際標準暗号の国内推奨・標準暗号への採用可能性**
  ISO/IEC 国際標準暗号も、元々国内の推奨・標準になっていなければ新規暗号と同様に国内の評価が必要、即ち、そのまま国内標準にはならない、としている国が多かった。この場合、EU 加盟諸国（フランス、ドイツ）ではコモンクライテリア相互認証制度での評価が、カナダ、オーストラリアでは米国の FIPS（Fideral Information Processing Standards：連邦情報処理規格）の評価が、重要な判断基準として位置付けられている。

- **電子政府用暗号の階層化**
  電子政府用の暗号として、G2G（Government to Government：政府内および政府間）と G2C（Government to Consumer：政府と国民・市民間）を区別して使い分けることは、一般には行われていないが、一部の国（韓国、米国、英国）では、G2G の中でもより機密性の高い領域で使われるをアルゴリズムを非公開にしたり、一般の G2G や G2C と階層を区別して評価・管理する例がある。

- **国内推奨・標準暗号リストのライフサイクル・モデル**
  国内推奨暗号リストを定期・不定期的に見直すとしている国は多かったが、暗号リストを三段階のクラスに分けてライフサイクル管理を行うドイツのモデルが注目に値する。日本でも、暗号の危殆化やデファクト・スタンダード暗号への対応のためにも、推奨リストの見直しの方法を検討することは必要であろう。

添付資料

- 国際標準暗号各国対応表
- 暗号用語英和対訳表
- インタビュー依頼レターテンプレート(政府用)
- インタビュー依頼レターンプレート(サプライヤ用)
- インタビュー質問票
- 各国主要文献