

CRYPTREC2001

暗号技術検討会

2001年度報告書

総務省 / 経済産業省

2002年3月

目次

1．はじめに	P 1
2．検討会開催の背景、構成員及び開催状況	P 3
3．暗号技術に関する現状	P 7
4．電子政府推奨暗号の策定	P 9
5．暗号技術評価結果について	P 11
6．要件調査WGにおける検討結果	P 18
7．今後の検討課題	P 25
8．暗号プロトコル評価、及び暗号モジュール評価の重要性	P 27
9．次年度以降の評価を含む活動指針	P 31

【資料】

- ・要件WG活動報告
- ・評価委員会報告書

1. はじめに

近年のインターネットの急速な拡大に代表されるように、社会における IT 化の進展はめざましいものがある。我が国政府においても、ミレニアム・プロジェクトとして、2003 年までに世界最高水準の電子政府の基盤構築を目指している。これは、行政の効率化や国民負担の軽減を目標に、申請届出手続や政府調達などの行政手続の電子化を実現するものである。

他方、IT 化による利便性の増大とともに、新種ウィルスや、不正アクセス件数の増加等、IT に対する脅威が増加しており、その姿も多様化している。このような環境の中、いかに IT の安全性・信頼性を確保するかという問題は、我々の社会が直面している喫緊の課題と言えよう。

政府としても、安全性及び信頼性の高い電子政府を実現するために、情報セキュリティの確保が不可欠であり、情報セキュリティ技術の基盤をなす暗号技術が重要であるとの認識を深めている。この認識は、2001 年 3 月に IT 戦略本部において決定された「e-Japan 重点計画」においても示され、さらに、同年 10 月に情報セキュリティ対策推進会議において「総務省及び経済産業省は、両省で実施している研究会の成果等も踏まえ、2002 年度中に「電子政府」における調達のための推奨すべき暗号のリストを作成し、これを踏まえ、各省庁における暗号の利用方針について合意を目指す」ことが決定された。

これに先立ち、2000 年度、経済産業省から暗号技術評価プロジェクトが情報処理振興事業協会（IPA）に委託され、IPA は筆者が委員長を勤める暗号技術評価委員会を設置し、このプロジェクトを CRYPTREC と命名して、遂行した。このプロジェクトは、電子政府で利用可能な暗号技術を、安全性および実装性など技術的な面から評価するものである。さらに、2001 年度には、暗号技術の利用に関し政策的な観点から検討を行うために、総務省大臣官房技術総括審議官及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術検討会（以下、本検討会）を設置した。

本検討会の主要な検討事項としては、電子政府に利用される暗号技術の要件整理および総合的評価、電子署名法に基づいて利用される暗号技術の総合的評価、暗号技術の国際標準化への対応、電子政府推奨暗号に関する利用方針案の策定、今後の暗号技術評価のあり方の検討が挙げられる。

暗号技術の要件整理のためには、本検討会の下に、佐々木良一東京電機大学教授をリーダーに迎え、要件調査ワーキング・グループを設置し、調査を行った。これにより、電子政府のための暗号技術評価において考慮すべき要件が明らかになり、本検討会における電子政府推奨暗号の検討の基礎となった。

本報告書は、2001 年度の本検討会における検討結果をまとめるとともに、今後の暗号技術政策に関して提言を行い、総務省及び経済産業省の担当両局長に対して報告するものである。また併せて、本検討会にオブザーバとしてご参加頂いている各省庁、ならびに電子政府を構築する省庁関係者にも広く読んで頂くことを想定している。さらに、暗号一般のユーザの方々にも、現在の代表的暗号の安全性・実装性に関する評価結果、暗号技術に関わる国内外情勢、電子政府における暗号技術の利用などに関し、最も質の高い有益な情報を提供できる報告書になっていると自負している。

前述の暗号技術評価委員会については、2001 年度から、IPA 及び通信・放送機構（TAO）の共同プロジェクトとして、CRYPTREC というプロジェクトの下、本検討会と連携して主に技術的な評価活動を行ってきた。技術的な事項については、IPA 及び TAO によってまとめられる「CRYPTREC Report 2001」をご参照頂きたい。

電子政府推奨暗号リストの作成に向け、CRYPTREC は来年度大きな山場を迎えることになる。国民が安心して使える電子政府を構築していくためには、本検討会および IPA 及び TAO の暗号技術評価委員会など CRYPTREC 関係の諸団体が一体となって前進することが必須である。今後とも関係者の方々の御協力を頂きながら、本プロジェクトを推進していく所存である。

末筆であるが、本検討会にご協力いただいた構成員の方々及びオブザーバとしてご参加頂いた方々、精力的に調査検討を行って頂いた要件調査ワーキング・グループの構成員の方々をはじめ関係者の皆様に心から謝意を表する次第である。

2002 年 3 月

暗号技術検討会
座長 今井 秀樹

2. 検討会開始の背景、体制、構成員及び開催状況

(1) 検討会開始の背景

高度情報通信ネットワーク社会形成基本法に基づく e-Japan 重点計画（2001 年 3 月 29 日高度情報通信ネットワーク社会推進戦略本部決定）においては、我が国の高度情報通信ネットワークの安全性及び信頼性を世界最先端の IT 国家にふさわしいものにするため、高度情報通信ネットワークにおける脅威に起因するサービス提供機能の停止が最小限となるように、政府は各種の施策を実施することとしている。

特に、電子署名等の電子認証の普及、電子政府の構築等に向けて、高度情報通信ネットワークの安全性及び信頼性を確保するためには、基盤技術である暗号技術について、客観的な評価や標準化が重要になっていく。

このため、総務省及び経済産業省は、暗号技術を公募の上客観的に評価し、実装性に優れた利用可能性の高い暗号技術を各省に推薦し、高度な信頼性及び安全性に支えられた電子政府の構築に貢献することを目指すこととした。

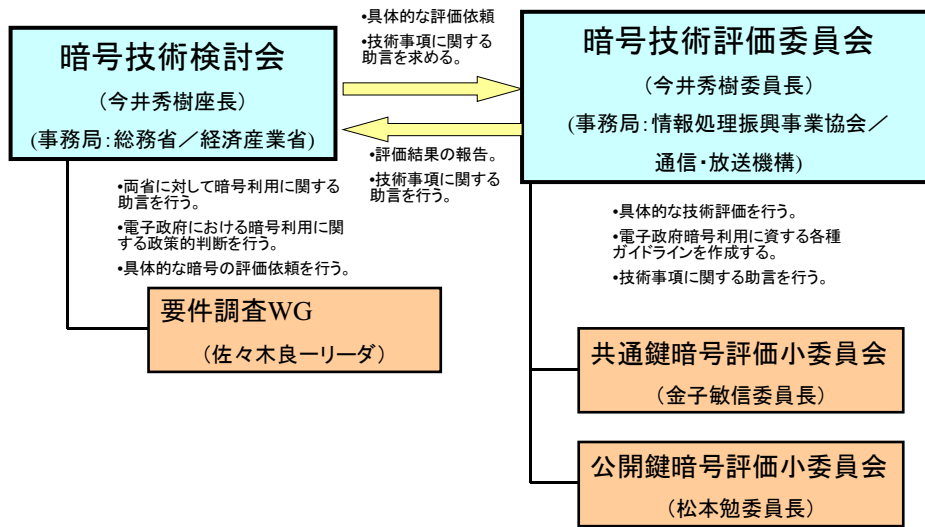
(2) CRYPTREC の体制

2001 年度は、下記の体制で検討・評価を進めた。

- ・暗号技術検討会：総務省及び経済産業省を事務局に、政策的な検討を行う。検討会の下に要件調査WGを設置し、電子政府で求められる暗号技術の要件を調査した。
- ・暗号技術評価委員会：情報処理振興事業協会及び通信・放送機構を事務局に、技術的な評価を行う。

なお、CRYPTREC とは、従来（2000 年度）は、暗号技術評価委員会（Cryptography Research and Evaluation Committee）のことを指していたが、2001 年度より、総務省及び経済省の両担当局長の主催により、暗号技術検討会が開催されたこと、及び CRYPTREC という名称が既に日本における暗号技術の評価プロジェクトとして広く国内外において認知されていることから、今後は、暗号技術検討会及び暗号技術評価委員会の両者を含めた形でプロジェクト名として CRYPTREC を使用することとする。なお、CRYPTREC は、Cryptography Research and Evaluation Committees の略称とする。

CRYPTREC体制



(3) 構成員 (特段の明示がない限り、肩書きは 2 0 0 2 年 3 月 末 現 在 。)

【検討会】

座長	今井 秀樹	東京大学生産技術研究所教授
顧問	辻井 重男	中央大学理工学部情報工学科教授
WG リーダ	佐々木良一	東京電機大学工学部情報通信工学科教授
	生宗 潤	(社)情報サービス産業協会セキュリティ委員会委員
	岩下 直行	日本銀行金融研究所研究第 2 課調査役
	岡崎 宏	通信機械工業会常務理事
	岡本 栄司	東邦大学理学部情報科学科教授
	岡本 龍明	日本電信電話株式会社情報流通プラットフォーム研究所主席研究員 (電気通信事業者協会代表兼務)
	加藤 義文	(社)テレコムサービス協会技術委員会委員長
	金子 敏信	東京理科大学理工学部電気工学科教授
	国分 明男	ニューメディア開発協会常務理事開発本部長
	櫻井 幸一	九州大学大学院システム情報科学研究科助教授
	宝木 和夫	(社)電子情報技術産業協会情報セキュリティ委員会委員
	苗村 憲司	慶應義塾大学環境情報学部教授
	松井 充	三菱電機株式会社情報技術総合研究所情報セキュリティ技術部チームリーダー
	松本 勉	横浜国立大学大学院環境情報研究院教授

(オブザーバ)(肩書きは基本的に参加当時のもの。)

須永 和男	内閣官房情報セキュリティ対策推進室内閣参事官(～第5回)
吉原 順二	内閣官房情報セキュリティ対策推進室内閣参事官(第6回～)
松田 正一	警察庁情報通信局技術対策課長
中島 明彦	防衛庁運用局指揮通信課長(～第2回)
中村 範明	防衛庁運用局指揮通信課長(第3回～)
高森 國臣	総務省行政管理局管理官
太田 健治	法務省民事局総務課民事調査官
粗 信仁	外務省大臣官房情報通信課長(～第5回)
石川 正紀	外務省大臣官房情報通信課長(第6回～)
中田 悟	財務省大臣官房審議官室長(～第3回)
中山 峰孝	財務省大臣官房審議官室長(第4回～)
木戸 達雄	経済産業省産業技術環境局標準課情報電気標準化推進室長
福地 一	独立行政法人通信総合研究所 情報通信部門長
大蒔 和仁	独立行政法人産業技術総合研究所 情報処理研究部門長
鈴木 薫	通信・放送機構研究企画管理部長
小林 正彦	情報処理振興事業協会セキュリティセンター所長(～第2回)
内藤 理	情報処理振興事業協会セキュリティセンター所長(第3回～)
米倉 昭利	(財)日本品質保証機構電子署名・認証調査センター所長
小倉 久宜	(財)金融情報システムセンター監査安全部長

【要件調査ワーキング・グループ(WG)】

リ-ダ	佐々木良一	東京電機大学工学部情報通信工学科教授
	岩下 直行	日本銀行金融研究所研究第2課調査役
	岡本 栄司	東邦大学理学部情報科学科教授
	川村 信一	株式会社東芝 研究開発センター コンピュータ・ネットワーク ラボラトリー 主任研究員
	洲崎 誠一	株式会社日立製作所 システム開発研究所 第7部 H01研究 ユニット 研究員
	館林 誠	松下電器産業株式会社 マルチメディア開発センター メディア 情報グループ チームリーダー
	米倉 昭利	財団法人日本品質保証機構 電子署名・認証調査センター 所長
	渡辺 創	独立行政法人産業技術総合研究所 情報処理部門

(4) 開催状況

- ・ 第一回 2001年5月16日(水):「開催要綱案、実施計画案」等
 - ・ 座長の選出
 - ・ 開催要綱案、実施計画案
 - ・ 評価委員会
 - ・ ISO/IEC JTC1 SC27

- ・ 第二回 6月22日(金):「電子政府での暗号技術の要件整理調査」等
 - ・ 評価委員会の活動方針
 - ・ 電子政府での暗号技術の要件整理調査

- ・ 第三回 7月27日(金):「2001年度暗号技術公募要領」等
 - ・ 要件調査WGの検討状況
 - ・ CRYPTREC Report 2000のJIS-TR化
 - ・ 2001年度暗号技術公募要領

- ・ 第四回 10月3日(水):「電子政府で利用する暗号」等
 - ・ 要件調査WGの検討状況
 - ・ 電子政府で利用する暗号
 - ・ 2001年度暗号技術公募状況
 - ・ 最終報告書案

- ・ 第五回 2002年1月18日(金):「電子政府推奨暗号リストの作成」等
 - ・ 電子政府推奨暗号リストの作成
 - ・ 2001年度報告書 骨子案
 - ・ 要件調査WGの検討状況
 - ・ 評価委員会活動(報告書案)

- ・ 第六回 2月22日(金):「要件調査WGの検討状況」
 - ・ 電子政府推奨暗号リストの作成
 - ・ 2001年度報告書 一次案
 - ・ 要件調査WGの検討状況
 - ・ 次年度以降の活動

- ・ 第七回 3月11日(月):「2001年度報告書 最終案」
 - ・ 2001年度報告書 最終案
 - ・ 要件調査WGの検討結果

3. 暗号技術に関する現状

現在、世界規模でのインターネット普及に伴い、より効率的でサービス内容が充実した電子政府システムの構築が各国で推進されている。特に米国やオーストラリアなどでは、電子政府調達システムをはじめとして、インターネットによる情報公開システム、各省庁への届出申請が一ヶ所でできるワンストップサービスなどの多くの電子政府システムが稼働している。

このような電子政府システムを実現するためには、インターネット関連の技術革新と標準化、暗号技術の開発と標準化、各国政府による PKI などのインフラの整備やセキュリティ各種法制度の確立が重要な役割を果たしている。

(1) 暗号技術の開発動向

暗号技術には長い歴史があるが、電子政府で使用される暗号としては 1970 年代後半に研究が活発化した現代暗号技術である。現代暗号技術の最大の特徴は、暗号アルゴリズムを広く公開している点にある。

現代暗号技術は、1976 年に米国の連邦情報処理標準 (Federal Information Processing Standards; FIPS (以下同様)) として公表された DES(Data Encryption Standard)に代表される共通鍵暗号と、Rivest-Shamir-Adleman により提案された RSA 暗号に代表される公開鍵暗号に大別される。共通鍵暗号は、そのデータ処理の構造により、ブロック単位にデータを処理するブロック暗号とデータを系列と考えるストリーム暗号に分かれる。また、暗号の補助関数として、大きなデータ入力に対して、入力データが簡単に計算できない性質を持つ出力データをつくるハッシュ関数や大きな乱数を生成する擬似乱数生成系がある。

これらは、電子政府システムに欠かせない暗号技術であり、CRYPTREC の暗号技術評価対象とした。

その他、新しい暗号技術として、量子暗号が検討されている。

(2) 暗号技術の標準化動向

暗号技術標準化の大きな動きとしては、米国商務省標準局 (NIST) による AES の FIPS 制定と欧州における暗号評価プロジェクト NESSIE が存在する。

AES プロジェクトは、1997 年 1 月から開始され、3 回の AES Conference を経て、ベルギーの技術者から提案された “Rijndael” が選定され、2001 年 11 月に FIPS 197 として標準暗号に制定された。

また、NESSIE は、EC 指令に基づき 2000 年 1 月より 3 年計画で開始された欧州の暗号評価プロジェクトである。NESSIE の目標は、公募とオープンな評価により、強力な暗号プリミティブのリストを作成することにある。その評価としては 2 つのフェーズで安全性と実装性の両面から評価される。現在はその第 1 フェーズが終了し、第 2 フェーズの評価が行われて

いる段階にある。

その他に ISO/IEC における暗号技術標準化の動きや IEEE P1363 の活動にも今後注目していく必要がある。

(3) 電子政府関連暗号技術標準

米国では暗号技術関連の標準が FIPS などにより定まっており、暗号技術標準として DES、AES などを規定するとともに、暗号利用アプリケーションとして、S/MIME(暗号メール)、Public Key Infrastructure (PKI)などに関するセキュリティ関連文書を発行している。

オーストラリアにおいても、セキュリティ基準に関する重要文書として、Protective Security Manual (PSM) および Australian Communications-Electronic Security Instructions 33 (ACSI 33) がある。この文書においては、セキュリティポリシーをはじめとして、推奨する暗号技術やその利用方法などについても記載されている。

(4) 暗号技術関連製品

日本でも、高度情報通信ネットワーク社会形成基本法 (IT 基本法) や IT 関連製品の評価・認証制度などが整備され、各企業は電子政府システムソリューションを競って提案しており、電子政府システム構築の環境が整いつつある。

電子政府関連システムとしては、電子申請、電子調達、電子入札ほかに電子投票や住民届出サービスなどが検討されている (詳細は 6 章参照)。

暗号活用の製品としては、電子署名の基盤技術である PKI、暗号電子メール S/MIME、インターネットを専用回線にする VPN、Web ブラウザで最もよく用いられている暗号通信 SSL/TLS などが挙げられる。その他 IC カードベースの製品も暗号技術関連製品に含まれる。

4. 電子政府推奨暗号の策定

(1) e-Japan 重点計画における標準化の位置づけ

2001年3月29日にIT戦略本部で決定されたe-Japan重点計画において、下記のように暗号技術の標準化の推進が決定された。

6. 高度情報通信ネットワークの安全性及び信頼性の確保

(3) 具体的施策

情報セキュリティに係る制度・基盤の整備

ウ) 暗号技術の標準化の推進(総務省及び経済産業省)

客観的にその安全性が評価され、実装性で優れた暗号技術を採用するため、2002年度までに、ISO、ITU等における暗号技術の国際標準化の状況を踏まえ、専門家による検討会の開催等を通じて電子政府利用等に資する暗号技術の評価及び標準化を行う。

これを受け、2001年10月に、内閣官房が中心となってとりまとめた、電子政府の情報セキュリティ確保のためのアクションプランにおいてより具体的な方策が決定された。

(2) セキュリティ・アクションプランにおける標準化の位置づけ

2001年10月10日に、情報セキュリティ対策推進会議において決定された「電子政府の情報セキュリティ確保のためのアクションプラン」において決定された内容は下記のとおり。

2. 具体的な方策

(2) 暗号の標準化の推進

・「電子政府」におけるセキュリティ確保のためには、政府調達における一定水準のセキュリティ確保のための情報機器等に関する基準(具体的にはISO/IEC15408)を可能な限り利用することと同様、暗号についても、一定水準以上の安全性及び信頼性を有するものの利用が不可欠であり、これを推進することが必要である。

・このため、総務省及び経済産業省は、両省で実施している研究会の成果等も踏まえ、2002年度中に「電子政府」における調達のための推奨すべき暗号のリストを作成し、これを踏まえ、各省庁における暗号の利用方針について合意を目指す。

(3) 電子政府推奨暗号の意味

電子政府推奨暗号が対象とするシステム、耐用期間、利用方針の合意範囲は以下の事項を想定している。

想定システム：電子申請システムや、電子入札システム等、政府と国民との間で書類の申請等についてやりとりを行う必要があるシステムを想定する。(国防関係の特別なシステムや、政府間限りのやりとりを行うシステムについてはこの対象としない。)なお、地方公共団体については、普及・広報等を通じて本利用方針の活用を奨励していく。

耐用期間：10年間は解読されない暗号を想定する。(ただし、署名の検証においては、

10年過ぎた後でも検証を行う必要性があるのでこの限りではない。) 合意範囲(拘束度合い):「可能な限り利用する。」との表現を用い、推奨のレベルとする。最終的な調達の判断は各省の責任で行う。

特許・知的財産権の扱い: リストのあり方によるが、複数リストの場合には特許・知的財産権の無償化を義務づけることは考えないが、1つに絞った場合にはその無償化を検討する必要がある。

(4) 作業スケジュール

これらの決定を受け、以下のスケジュールで今後の作業を進める予定である。

2001年度末

検討会において、要件調査WGを中心に、電子政府において用いられている、または将来用いられるであろう暗号技術に求められる要件について調査し、結果をまとめた。

また、評価委員会において、技術的な観点から、電子政府推奨暗号として利用することが可能である電子政府暗号候補(技術的な観点から安全性及び実装性について評価委員会において特に問題がないと判断された暗号)を策定した。

2002年10月

要件調査の結果まとめられた要件に基づき、電子政府暗号候補から、電子政府推奨暗号リスト案を作成する。あわせて、調達のためのガイドブック案を作成する。

2002年度末

リスト案に基づき、総務省及び経済産業省において利用方針案を作成し、各省庁において、利用方針の合意を目指す。併せて調達のためのガイドブックを総務省及び経済産業省より各省庁へ提示する。

(5) 最終成果物

検討会としては、最終成果物として、電子政府推奨暗号リスト案、及び 調達のためのガイドブック案を作成する。それを踏まえ、総務省及び経済産業省において、リスト案に基づく利用方針案、及び調達のためのガイドブックを作成し、各省庁合意を目指す。それにより、電子政府における暗号の調達を可能とする。

利用方針案については、どのように利用するかを定める利用方針部分と、添付資料としてのリストから構成される。

調達のためのガイドブック案については、ガイドブックを通じて各省庁における調達担当者がリストからの調達が可能となるための、暗号選定方法、運用方法等について記述することとする。

5 . 暗号技術評価結果について

(1) 暗号技術評価の目的

申請届出手続きや政府調達など行政手続きの電子化を実現する電子政府の機能をより安心して利用できるようにするためには、電子政府で利用可能な暗号技術の評価することが重要であり、2000 年度から暗号技術評価委員会を設置して、暗号技術の公募や委員会による評価対象暗号技術の選定、評価対象暗号技術の評価を進めてきた。

本暗号評価活動は国内暗号技術評価体制に向けた一歩であり、米国政府標準暗号を定める AES プログラムや欧州における暗号評価プロジェクト (NESSIE) の活動情報を参考にしつつ、ISO/IEC の国際標準活動への協力も行っている。

(2) 評価概要

電子政府で利用可能と想定される暗号技術を大きく公開鍵暗号技術、共通鍵暗号技術、ハッシュ関数、擬似乱数生成系の 4 つの分類に分けて、評価対象暗号の募集・選定を行い、各暗号技術の評価を行った。

暗号技術評価は、原則スクリーニング評価を実施した後に、詳細評価を実施する二段階評価のプロセスで評価を行っている。

但し、電子署名法に関する特定分野の暗号やその他評価が必要な暗号の評価について、スクリーニング評価を実施せず詳細評価を行った。

【暗号分類】

- ・ 公開鍵暗号技術 (暗号スキームと暗号プリミティブの組み合わせ)
守秘, 認証, 署名, 鍵共有
- ・ 共通鍵暗号技術
64 ビットブロック暗号, 128 ビットブロック暗号, ストリーム暗号
- ・ ハッシュ関数
- ・ 擬似乱数生成系

【スクリーニング評価 (詳細評価を実施するための評価)】

下記の観点から実施。

- ・ 安全性に明らかな問題がないかの第一次評価
- ・ 第三者実装上問題がないかの第一次評価

【詳細評価】

電子政府で利用可能かどうかとの観点から評価を実施。

- ・ 既知の攻撃法での統一的な評価
- ・ 各候補暗号個別の強度評価 (攻撃)
- ・ パラメータ / 鍵の設定基準に問題がないか
- ・ ソフトウェア実装評価

【これまで(2000.5-2002.3)の暗号技術評価委員会関連の主な活動】

2000年5月	暗号技術評価委員会の設置
2000年6-7月	2000年度暗号技術の公募
2000年8-10月	2000年度暗号技術スクリーニング評価
2000年10月	暗号技術シンポジウム(CRYPTREC活動の目的紹介)
2000年10 -2001年3月	2000年度暗号技術の詳細評価
2001年3月	CRYPTREC Report 2000の発行
2001年4月	暗号技術評価報告会(2000年度CRYPTREC活動報告)
2001年8月-9月	2001年度暗号技術の公募
2001年10月	応募暗号説明会
2001年10 -2002年3月	2001年度継続して応募された暗号技術及びその他評価が必要と判断された 暗号技術の詳細評価
	2001年度新規に応募された暗号技術のスクリーニング評価
2002年1月	暗号技術評価ワークショップ (スクリーニング評価・詳細評価の状況報告)
2002年3月	CRYPTREC Report 2001の発行

(3) 電子政府暗号候補

2000年度、及び2001年度評価結果により、今年度の成果として電子政府暗号候補として下記の暗号を掲げる。

公開鍵暗号技術

(*なお、公開鍵暗号スキームが証明可能安全性を有するとは、そのスキームを攻撃することの非現実性を、暗号理論分野で標準的な安全性評価モデルの枠組に沿って示せることをいう。ただし、それが現時点で示されていないからといって、そのスキームの安全性が否定されるわけではない。)

【署名】

DSA

署名のための公開鍵方式であり、安全性は離散対数問題の困難性に依存している。使用実績はあるが、証明可能安全性は示されていない。擬似乱数生成法は2001年10月に仕様が修正されており、それを使用すべきである。仕様上はパラメータのサイズを選択可能であるが、安全性の観点から電子署名法に係る指針に記載されている1024ビットを使用すべきである。新たな規格が制定される可能性に注意を払う必要がある。

ECDSA (ANSI X9.62)

署名のための公開鍵方式であり、その安全性は楕円曲線上の離散対数問題の困難性に依存している。特殊なモデルでの証明可能安全性は示されているが、そのモデルの妥当性に関し

ては決着がついていない。2001 年時点では安全性に大きな脅威を与えるような問題点は指摘されていない。電子署名法に係る指針にはパラメータの値が 160 ビット以上の ECDSA が記載されている。

ECDSA in SEC1

署名のための公開鍵方式であり、その安全性は楕円曲線上の離散対数問題の困難性に依存している。特殊なモデルでの証明可能安全性は示されているが、そのモデルの妥当性に関しては決着がついていない。2001 年時点では安全性に大きな脅威を与えるような問題点は指摘されていない。

RSA-PKCS#1 v1.5

署名のための公開鍵方式であり、その安全性は相異なる 2 素数の積である整数の素因数分解問題の困難性に依存している。証明可能安全性は示されていないが、広く使われてきた実績、広範な観点からの安全性評価が行われており、2001 年時点では経験的に安全であると考えられる。ただし、多くの署名法のエンコーディング手法について署名の偽造方法が提案されていることにより、本方式で採用されているエンコーディング手法の安全性について検討を継続する必要がある。電子署名法に係る指針に記載されている署名方式の 1 つであり、MD5 版と SHA-1 版があるが、MD5 版の使用は薦められない。

RSA-PSS

署名のための公開鍵方式であり、その安全性は相異なる 2 素数の積である整数の素因数分解問題の困難性に依存している。証明可能安全性が示されている。他の署名方式（全域ハッシュ法等）に比べて緊密な帰着関係を証明できる特徴を有している。RSA-PSS を電子署名法に係る指針に記載することを検討する必要がある。

【守秘】

RSA-OAEP

守秘のための公開鍵方式であり、その安全性は相異なる 2 素数の積である整数の素因数分解問題の困難性に依存している。証明可能安全性が示されている。広く使われてきた実績、広範な観点からの安全性評価が行われており、2001 年時点では経験的にも安全であると考えられる。

【鍵共有】

DH

鍵共有のための公開鍵方式であり、その安全性は離散対数問題の困難性に依存している。能動的な攻撃に対しての証明可能安全性はないが、広く使われてきた実績があり、2001 年時点では経験的に安全であると考えられる。

ECDH in SEC1

鍵共有のための公開鍵方式であり、その安全性は楕円曲線上の離散対数問題の困難性に依存している。SEC2 で具体的に示されている楕円曲線については、特段の問題点は指摘されていない。能動的な攻撃に対しての証明可能安全性はないが、広く使われてきた DH の楕円曲線版であることから、2001 年時点では安全であると考えられる。

共通鍵暗号技術

【64ビットブロック暗号】

CIPHERUNICORN-E

安全性について、今のところ問題は見つかっていない。処理速度は遅いグループである。

Hierocrypt-L1

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

MISTY1

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

Triple DES

安全性について、FIPS等で保証されている間は、問題ないとする。

【128ビットブロック暗号】

Advanced Encryption Standard

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

Camellia

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

CIPHERUNICORN-A

安全性について学術上の観点からの課題が残るものの、実用上の重大な問題点は見つかっていない。処理速度は遅いグループである。（*註：ここでいう学術上の課題とは、種々の攻撃方法のコストが、全数探索法以上となることを理論的に示すことである。）

Hierocrypt-3

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

RC6 Block Cipher

安全性について、今のところ問題は見つかっていない。Pentium III上での暗号化が最速であるが、ソフトウェア処理速度はプラットフォームに大きく依存。

SC2000

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

【ストリーム暗号】

MULTI-S01

安全性について、今のところ問題は見つかっていない。ソフトウェアによる処理速度は速いグループである。

ハッシュ関数

RIPEMD-160

安全性について、いまのところ問題は見つかっていない。

SHA-1

安全性について、いまのところ問題は見つかっていない。

draft SHA-256

draft SHA-384

draft SHA-512

提案されてまだ日が浅いため、安全性に関する評価が定まっていないが、今のところ問題点は見つかっていない。電子政府利用としてはFIPS版の再評価後の使用を薦める。

擬似乱数生成系

PRNG based on SHA-1

電子政府用として現在においては問題ないが長期の使用には注意が必要である。

(* 64ビットブロック暗号(CIPHERUNICORN-E, Hierocrypt-L1, MISTY1, Triple DES)/160ビットハッシュ関数(RIPEMD-160, SHA-1)について、電子政府用システムとして、新システムを構築する場合は、より長いブロック長/ハッシュ値が使用可能な状況にあれば、そちらを選択するのが望ましい。)

(4) 2002 年度詳細評価対象暗号候補

公開鍵暗号技術

(* 公開鍵暗号技術における証明可能安全性については、上記(3) の説明を参照のこと。)

【署名】

ESIGN

署名のための公開鍵方式であり、その安全性は特殊な形の整数の素因数分解問題の困難性に依存している。証明可能安全性は示されていない。電子署名法に係る指針に記載されている ESIGN 署名はその指針に記載されている安全性パラメータの範囲に、無視できない確率で署名の偽造に成功するパラメータが含まれていることが問題である。詳細な評価なしでは電子政府での使用は薦められない。

【守秘】

ECIES in SEC1

守秘のための公開鍵方式であり、その安全性は楕円曲線上の離散対数問題の困難性に依存している。安全性についての議論が最近新たに生じてきたので、詳細な評価なしでは電子政府での使用は薦められない。

HIME(R)

守秘のための公開鍵方式であり、その安全性は特殊な形の素因数分解問題の困難性に依存している。自己評価書における証明可能安全性の主張には疑問があり、詳細な評価なしでは電子政府での使用は薦められない。処理がRSA-OAEPより高速である可能性がある。

【鍵共有】

PSEC-KEM

鍵カプセル化のための公開鍵方式であり、その安全性は楕円曲線上の離散対数問題の困難性に依存している。鍵カプセル化メカニズムとしての証明可能安全性を有するとされる。鍵カプセル化メカニズムの適用領域が明確とはいえ、詳細な評価なしでは電子政府での使用は薦められない。

共通鍵暗号技術

【ストリーム暗号】

MUGI

安全性について、今のところ問題は見つかっていない。1998年に発表されたPANAMAの改良であるとはいえ、発表されてから日が浅く、さらなる安全性及び実装性の評価が必要と考えられる。

RC4

現在評価中であり、2002 年度中に詳細な評価を報告予定である。

(5) 電子署名法に係る指針の改正に関する検討

ESIGN

電子署名法に係る指針に記載された ESIGN 署名は、その指針に記載されたパラメータの一部に署名の偽造が可能なものが含まれている。したがって、電子署名法に係る指針の改訂を検討すべきである。

RSA

電子署名法に係る指針に記載されている RSA-PKCS#1 v1.5 については、証明可能安全性は示されていないが、2001 年時点で特に安全性の問題は存在しない。しかし、証明可能安全性が示されていないことに鑑みて、方式の利用状況、方式の寿命等を考慮しつつ、RSA-PSS を電子署名法に係る指針に新たに追加し、将来的には RSA-PSS に一本化することを含めた議論をしていく必要がある。

RSA-PSSについては、証明可能安全性の証明はランダムオラクルモデルのもとで信頼できる。ただし、設計パラメータの適切な選択は必要であり、引き続き調査・検討が必要である。

MD5

MD5 については、2000 年度の評価結果として「MD5 は 128 ビットのハッシュ値であり、Birthday 攻撃に対して十分な耐性を有さないという意見もある。最近の研究では少なくとも 160 ビット以上必要であると考えられている。」との報告がなされており、電子署名法に係る指針における利用については、その指針から外すことを検討する必要がある。

(6) 国際協力のための評価

ISO/IEC SC27 国内委員会からの評価依頼に基づき、CRYPTREC において下記の暗号を国際協力の観点から評価した。評価結果は次のとおり。

SEED

安全性について、今のところ問題は見つかっていない。処理速度はやや遅いグループに属する。

なお、本章及び次章における、今回の評価結果は、現時点で想定される攻撃等に対する安全性等々を評価したものであり、将来にわたって安全性が保証されるものではなく、自ずと限界があるものであり、本報告書に記載されている評価結果等の情報を利用した結果として生じる損害等に対して責任を持つことはできない。

6. 要件調査WGにおける検討結果

(1) 検討の進め方

(a) 検討対象

以下の全ての条件を満たす電子政府システムを検討対象とした。

国の行政機関のシステム（大学、病院、地方自治体は対象外）

国家の安全保障のため、又は国家の防衛上の目的のためのシステムを除く。

国民との間で行政サービスとしてやりとりを行うもの、及びそのやりとりを安全に行うために必要な関連システム（下位層のシステムを含む）

(b) 調査及び検討方法

2001年6月～2002年3月の間、以下の調査及び検討を行った。

国の行政機関のシステムに関するヒアリング調査

現在、国の行政機関の電子政府等で運用されているシステムのうち、「電子申請」「電子調達」「電子納付」「電子情報提供」「政府認証基盤」に関連するシステムについて、構成イメージ、処理フローイメージ、利用暗号技術等に関するヒアリングを実施した。（調査結果は資料1参照）

メーカ、ベンダ等に対するアンケート調査

暗号技術に関する知識を持ち、政府に対してシステムの提案を行う立場の企業に対して、暗号技術の利用形態、利用目的、要件等についての意見を求めるため、アンケート調査を行った。また、将来の暗号技術のあるべき姿等についても併せて意見聴取を行った。（調査結果は資料1参照）

SSLの現状調査及び安全性評価

でヒアリングを行ったシステムは、SSLをベースに構築し、または、これから構築しようとしているケースが多いことが分かったので、SSLで利用されている暗号アルゴリズムのうち主なもの及びSSLプロトコル本体の安全性について、暗号技術評価委員会に対して評価を依頼した。

海外電子政府システムに関する調査

情報技術の水準の高い主要な国々の政府部門向けセキュリティ標準及び暗号標準、電子政府サービス事例における暗号利用を調査し、特に、実際にアクセスできたSSLで保護されたページについてはパラメータをまとめた。（調査結果は資料1参照）

暗号利用形態の分類及び暗号技術に求められる要件等の検討

上記調査結果を基に、電子政府システムにおける暗号利用形態の分類及び暗号技術に求められる要件等について、検討を行った。

(2) SSLの安全性評価結果

上記(1)(b)で述べた通り、SSLプロトコル自体の安全性と、SSLプロトコルで用いられる暗号のうち、代表的なものとしてRSA、Triple DES、RC2、RC4の安全性に関する評価を暗号技術評価委員会に依頼し、以下のような報告を受けた¹。

(a) SSL/TLS²プロトコルの安全性評価

暗号方式に関わる安全性

RSA 公開鍵暗号方式の暗号化には PKCS#1 と呼ばれる実装仕様が適用されるが、PKCS#1V1.5 に対する適用的選択暗号文攻撃の存在が指摘されており、改良版である PKCS#1V2.0 の利用が推奨される。さらに PKCS#1V2.0 にも別のセキュリティホールが指摘されており、改善策が V2.1 において実現されている。

プロトコルに関する安全性

SSL には相互認証、サーバ認証のみ、匿名の3つの認証モードがあるが、このうち匿名認証モードにおいては2者間の通信の間に不正者が介在する man-in-the-middle 攻撃が存在し、情報の盗聴・改ざんの攻撃を受ける可能性があるため利用することは推奨されない。その他、攻撃者が SSL3.0 に対応しているサーバ、クライアントに対して SSL2.0 やそれ以下の Version で通信を行うように強制する攻撃法である version rollback 攻撃等がありうるが、version rollback 攻撃は、SSL の最新版のみを使用するよう設定運用することで、攻撃を防ぐことができる。

実装に関わる安全性

SSL/TLS の公開鍵証明書を使った認証に関して、証明書検出機構が実装されていないケース、不正な証明書に対して警告を出さないケース、認証動作を迂回する攻撃が可能となるケースなどが報告されている。また、セッション鍵に用いる擬似乱数生成器の内部状態が暴露する攻撃も報告されている。実装に関するセキュリティホールについては、バグを改修した最新版や修正プログラムを用いることで攻撃を回避できる。

運用に関わる安全性

SSL/TLS にはサーバ、クライアント側で運用時に設定するパラメータが幾つか存在し、鍵や証明書を格納するファイル、セッション鍵のライフタイム、乱数生成方法、使用する暗号アルゴリズム、警告メッセージの表示可否等が設定可能である。このためこれらのパラメータの意味を十分理解し適切に設定する必要がある。不用意な設定がセキュリティホールになる可能性がある。

¹ ただし、RC4 は評価開始が遅れたため、本報告書の評価結果報告には含まれていない。

² TLS(Transport Layer Security) V1.0 (<http://www.ietf.org/rfc/rfc2246.txt>, 1999)は、インターネット技術の標準活動を行なっている IETF (Internet Engineering Task Force)が SSL3.0 を引き継いで RFC2246 として規定したもの

SSL/TLSの比較調査

総じてTLSはSSLに比較して、鍵、初期値、MAC生成に関して安全性の根拠を明確にし、署名の構造を若干修正したという点でセキュリティ上の差異があるが、SSLについても実用上問題のないレベルであると考えられる。

(b) SSL/TLSで用いられる暗号の評価

DES

(暗号単独の安全性評価)

鍵長40ビットのDESは鍵総当りにより現実的な時間で解読可能である。鍵長56ビットのDESも現実的に解読可能な領域に達している。鍵長が168ビットの3-key Triple DESであれば当面の間の使用は問題ないといえる。

(SSL/TLSにおける安全性評価)

いずれの鍵長においてもDESはデータ秘匿の目的に用いられる。ブロック暗号モードとしてはCBCモードが用いられる。 2^{32} ブロック以上を同じセッション鍵を用いて暗号化すると平文1ビットの情報がもれる可能性がある。

RC2

(暗号単独の安全性評価)

鍵長40ビットのRC2は鍵総当りにより現実的な時間で解読可能である。鍵長128ビットのRC2も現実的に解読可能な領域に達しつつある。最新の暗号解読理論を適用したとき、鍵総当りよりも効率的な解読が知られている。よって、新規に構築する電子政府システムにおいて鍵長128ビットのRC2を採用することは勧めない。

(SSL/TLSにおける安全性評価)

鍵長はSSL 2.0においては40ビットおよび128ビットが選択可能であり、SSL 3.0においては40ビットのみが選択可能である。40ビットの鍵は、現実的な計算機環境において数時間もあれば全数探索可能である。なお、DESと同じく、 2^{32} ブロック以上を同じセッション鍵を用いて暗号化すると、平文1ビットの情報がもれる可能性がある。

RSA

(暗号単独の安全性評価)

512ビットの鍵長は現実的な素因数分解可能であり安全ではない。2001年時点では、1024ビット以上の鍵長を用いれば安全であると考えられる。

(SSL/TLSにおける安全性評価)

SSL/TLSにおけるRSA暗号を利用した基本的な鍵共有法および署名法の安全性について調べた。その結果、単純な技術の組み合わせの上に最も基本的なスキームを採用しており、暗号プロトコルとしてはセキュリティホールが潜む余地はほとんどないと考えられる。

(c) SSL/TLS 利用にあたっての注意点

SSL/TLS プロトコルに関して

- ・SSL3.0 を利用するにあたっては、セキュリティホールを含む SSL2.0 の利用を不可とするなど既知のセキュリティホールを十分認識した上での設定をすべきである。
- ・市販の SSL ソフトウェアを利用する場合、セキュリティホールに対してパッチのあてられた最新版を利用すべきである。
- ・市販のブラウザである Internet Explorer および Netscape Navigator においては CRL (公開鍵証明書無効化リスト)の管理は行なわれていない。従って CRL を不正に消去した上で不正な証明書を用いて認証を欺くという攻撃がありうる。このようなことがないように証明書を格納するファイルは厳密なアクセス管理のもとに管理するべきである。
- ・情報の盗聴、改ざんの攻撃を受ける可能性があるため、匿名認証モードの利用を推奨しない。
- ・version rollback 攻撃を防ぐため、特に理由がない限り SSL/TLS の最新版のみを使用するよう、設定運用すべきである。
- ・SSL3.0 では利用する暗号方式について変更出来ない。一方、TLS1.0 においては新しい暗号技術を追加することが可能となっている。そのため、既存の暗号技術に問題があった場合にも対応が可能である。
- ・なお、TLS は機能追加を目的として拡張作業が行なわれているが、これらの拡張に伴って新たなセキュリティホールが発生する可能性もあるため、今後とも TLS の動向に注目し、その安全性について継続的な調査・検討が必要である。

SSL/TLS で利用される暗号に関して

- ・RC2 であろうと DES であろうと、鍵長 40 ビットの暗号は鍵の全数探索法により現実的な時間で解読可能であるため、安全性が必要なシステムにおいては用いられるべきではない。
- ・鍵長 56 ビットの DES はもはや現実的に解読可能な領域に達しており、高い安全性が必要なシステムにおいては用いられるべきではない。
- ・鍵長 168 ビットの TDES は当面の間の使用は安全性上特に問題ないが TDES に代わる更に安全な暗号が SSL に採用されれば、それに置きかえるほうが望ましい。
- ・64 ビットブロック暗号である RC2, DES, TDES においては、 2^{32} ブロック以上を同じセッション鍵を用いて暗号化すると平文 1 ビットの情報がもれる可能性があるため、セッション鍵の更新に注意すべきである。
- ・鍵長 128 ビットの RC2 に対して、鍵の全数探索法よりも効率の良い解読方法が存在する。よって、新規に構築する電子政府システムにおいて鍵長 128 ビットの RC2 を採用することは勧めない。

- ・RSA について、512 ビットの鍵長は現実的に素因数分解可能であり安全ではない。2001 年度時点では 1024 ビット以上の鍵長を用いれば安全であると考えられる。

(3) 電子政府システムにおける暗号利用形態

国の行政機関のシステムに関するヒアリング調査等の結果、電子政府システムにおける暗号の利用形態は、利用者および政府側の認証、利用者から政府への、および政府から利用者へのデータ転送における、鍵共有、守秘、完全性認証、否認防止、および政府側のデータ保管における守秘、完全性保証、否認防止と整理するのが適当であると考えられる。

一方、暗号技術利用の要件を整理するための利用形態としては、簡潔で一般的な表現が望ましいことから、次のような点を考慮する。

- ・認証は相手認証であることを明示することが適当である。
- ・利用者と政府の間のデータ転送は、向きに関わらず同じ「通信」として扱うことが適当である。
- ・完全性保証と否認防止を包括的に署名と表現することが適当である。
- ・データ保管に対する強い要求がないので「通信」の利用形態と「保管」の利用形態を同じに扱うことが適当である。
- ・それぞれの項目に簡単な定義を記載することが適当である。

以上より、電子政府システムの暗号利用形態として次の分類表が得られる。

	定 義
相手認証	被認証者の正当性を検証者が確認する機能
鍵共有	電子政府システムにおいて公開の通信路を用いて共通鍵暗号技術を利用する際に送信者と受信者の間で鍵情報を共有する機能
守秘	電子政府システムにおいて公開の通信路または記録媒体を介して正当な利用者以外には知られないように電子情報を共有する機能
署名	電子情報の正当性を確認する機能。署名作成者の確認機能と電子情報自体の改ざんの有無の確認機能の両方を意味する。

この分類表における暗号の利用形態のために、暗号技術が必要に応じて単独又は組み合わされて用いられる。暗号評価委員会においては暗号技術を公開鍵暗号、共通鍵暗号、ハッシュ関数、擬似乱数生成に分け、公開鍵暗号はさらに守秘、認証、署名、鍵共有に分類し、共通鍵暗号を 64 ビット鍵、128 ビット鍵、ストリーム暗号に分けている。各々の暗号利用形態において用いられる代表的な暗号技術は次表の通りまとめられる。

技術 分類 暗号の 利用形態	公開鍵暗号				共通鍵暗号		その他		
	認 証	鍵 共 有	守 秘	署 名	ブロック 暗号		ス ト リ ー ム 暗 号	ハ ッ シ ュ 関 数	擬 似 乱 数 生 成
					64 ビ ット	128 ビ ット			
相手認証								**	
鍵共有									
守秘									
署名					*	*			

* MAC を想定 ** キードハッシュ関数を想定

(4) 暗号技術に求められる要件

(a) 電子政府システムにおける一般的要件

上記の調査及び検討を踏まえ、要件調査WGとして満たすべきであると考え、電子政府で利用する暗号における一般的要件を以下に記述する。

暗号強度が十分高い。

10年間電子政府システムで安心して使えること。ここで10年としたのは以下のような理由による。

- ・システムの置き換え周期が4～5年であり、そのシステムが完全に置き換わるまでに、もう1周期かかることから、最低でも10年は安心して使いたいという要望があること。
- ・供給者としては、コンピュータ性能の向上や解読手法の出現等により、非常に長期間にわたって安全性を保証することが困難であり、非常に長期間にわたる安全性を考慮して暗号を選択しようとする、調達コストの上昇を招く可能性があること。

一般に使われる商用ソフトにあらかじめ入っているか、入る可能性の高いものが選ばれること。

広く国民との間でやりとりを行うシステムにおいては、クライアント側でのインストールを必要としないか、最小限のインストールで済むなど、ユーザに負担を掛けない方が望ましいことから、一般に使われる商用ソフトに予め入っているか、入る可能性の高いものが最低限1つは選ばれること。

その他、処理速度が速く、ICカードへの実装性に優れている事や、何らかの暗号標準又はプロトコル標準になっている事も望ましい。

(b) 暗号の利用形態別要件

既に(3)で述べた通り、暗号の利用形態は、相手認証、鍵共有、守秘、署名、の4つに分類できると考えられる。

そこで使う暗号は、いずれの場合も一般的要件と同様に、次のような要件を満たす事が望ましい。

暗号強度が十分高い。

一般に使われる商用ソフトにあらかじめ入っているか、入る可能性の高いものが選ばれること。

特に、署名の場合は、署名した文書が有効とされる期間、安全でなければならないという特徴があり、暗号の使用期間(想定起点となる時から、安心して暗号化を行える期間)+有効期間(暗号化を行った後、破られない期間)の暗号強度を要求される。

また、ICカードシステムでは実装上、よりパフォーマンスの劣るハードウェアでも有効に機能する暗号アルゴリズムのニーズがある、という個別の要件も得た。

(5) 電子政府における暗号利用に関する提言等

(a) 署名された文書の有効期間の制約

署名の場合、署名した文書の有効期間安全でなければならないという特徴があり、暗号の使用期間+有効期間の暗号強度を要求される。よって、安全な運用のためには、電子政府システムはこの有効期間をある範囲に絞り込み、署名付きの文書を再発行するなどの仕組みも必要となる。例えば、電子免許証システムにおいて4年毎に再発行する決まりにする、などの対応である。

(b) 標準化対応の必要性

推奨暗号に選ばれたとしても、マイクロソフトのSSLや、今後出てくるプレインストールソフトに採用されていない(される見込みがない)と、実際の応用システムに採用されない可能性が高い。特に、クライアント側のユーザが一般住民の場合はそうである。そのためには、まず、ISOやIETFでオーソライズすることも必要となってくる。

(c) プロトコル、製品評価の必要性

現実に指摘される弱点は、暗号アルゴリズムよりも暗号プロトコルや暗号製品の方が多い。また、電子政府システムの安全性は、暗号プロトコルや暗号製品も安全であって初めて保たれる。したがって、暗号アルゴリズムの安全性評価だけでなく、電子政府で用いられる可能性のある暗号モジュールや暗号プロトコル、暗号製品に関する安全性評価のニーズも強いことから、今後対応していくことが望ましい。

7. 今後の検討課題

以下の事項については、リスト作成のために今後更なる検討を要する。

(1) 推奨暗号数

以下の3つの案が想定されるが、それぞれ長所・短所を考慮した上でどの形が望ましいかを整理する必要がある。なお検討に際しては、コスト、相互接続性、安全性、実装性、標準等を勘案する必要がある。

単独暗号

複数暗号(2～3個)

複数暗号(数は限定せず、安全性等の観点から一定の条件をクリアした暗号をリストアップする。)

(2) 相互接続性の問題

暗号レベル、暗号プロトコルレベル、製品レベルでの相互接続性について検討を加える必要がある。

(3) 製品との関係

調達に際して以下の事項を整理する必要がある。

製品レベルでの調達との関係：最終的に調達においては、リスト化された電子政府推奨暗号を用いた製品を調達することになるので、推奨暗号を採用するためにはどのような製品を調達すれば良いのかについて検討する必要がある。

CCの認定との関係：個々のシステム・製品の安全性を図る基準として、ISO/IEC15408(いわゆるコモンクライテリア：CC)がある。推奨暗号を利用した製品を調達する際に、このCCとどのような関係で調達を行えば良いかを整理する必要がある。

(4) 推奨暗号と暗号プロトコルとの関係

SSL等既存の暗号プロトコルにおいて既に利用されている暗号の考え方：SSL等既存のプロトコルで利用されている暗号をどのように評価するかについて整理する必要がある。

推奨暗号と将来の暗号プロトコルとの関係：同時に、推奨暗号をどのように将来策定される暗号プロトコルに盛り込むかについてその関係を整理する必要がある。

(5) 暗号プロトコル評価、及び暗号モジュール評価の必要性：(下記8.参照)

(6) 標準化に関する考え方

ISO/IECにおいて2003～2004年頃に向け、守秘のための共通鍵、及び公開鍵暗号の標準化が行われる見通しであり、将来的にはこれら国際標準暗号と電子政府推奨暗号の関係を整理する必要がある。

仮にISO/IECにおいて標準が策定された場合には、それら国際標準暗号を取り込んだ形で電子政府推奨暗号を策定することで問題が少ないと考えられる。その場合には、国際標準暗号と電子政府推奨暗号との技術的同等性を確保する必要がある。

(7) リスト案、ガイドブック案の内容

それぞれ以下の内容を記述することを想定。

リスト案

分類

- ・ 利用形態（電子署名、通信、データ保存等）
- ・ 製品（ICカード等）
- ・ 暗号方式（公開鍵、共通鍵、ハッシュ等）
- ・ 利用目的（守秘、認証、署名等）
- ・ その他（求められる安全性のレベル等）

最低限の条件（要件）

- ・ 安全性
- ・ 実装性
- ・ その他考慮すべき事項

その他、調達に必要な事項

ガイドブック案

暗号選定

セキュリティと暗号との関係（セキュリティポリシーとの関係）

システムと利用目的

推奨暗号と製品の関係（製品リスト）

実際に調達する暗号方式及び推奨暗号

各推奨暗号の特性

実装

実装時の留意点

運用

運用に係る鍵管理、実装、利用モード

その他関連情報

標準

8. 暗号プロトコル評価、及び暗号モジュール評価の重要性

8.1 暗号プロトコル評価

(1) 暗号プロトコルとは何か

一般に、通信プロトコルとは、2者間以上の参加者の間でメッセージを授受しながら計算を進めていくための分散されたアルゴリズムのことを言う。そこで、ここでは暗号プロトコルを、「暗号アルゴリズムを組み合わせてデータ守秘やメッセージ認証を実現する通信プロトコル」のことと考える。具体的には、SSL、S/MIMEなどが典型であるが、古典的には、Triple DESで鍵交換しDESで秘密通信を行う一連の手順なども含まれる。こうした暗号プロトコルを実現するためのクライアント側の製品としては、Internet Explorerとか、Outlook Expressなどがある。

隔地間で暗号プロトコルを利用して通信を行う状況を想定した場合、データ守秘やメッセージ認証が正しく達成されるかどうかは、暗号プロトコルの安全性と暗号アルゴリズムの安全性の双方に依存する。自動車に喩えて言うならば、暗号アルゴリズムはエンジンのようなものであり、その安全性は必要不可欠であるが、ハンドルや車輪が正しく機能していなければ安全に運転できないように、暗号アルゴリズムだけが強くて、暗号プロトコル全体のセキュリティが高いことは保証されない。

(2) SSLの場合

例えば、SSLの場合、暗号鍵の生成、鍵交換、データの暗号化など、詳細な手順が仕様として定められている。ただ、このうち特に鍵生成や鍵交換の部分は、最近の証明可能安全性を巡る研究などを踏まえると、その安全性がきちんと検証された訳ではない。ここで、プロトコルの安全性については、(1)仕様書に書かれているプロトコルに欠陥はないか、(2)仕様書の内容を実装した技術に欠陥はないか、という2つの観点から確認が必要となる。

よく知られた事例であるが、1995年9月、代表的なWWWブラウザであるNetscape Navigator Ver.1.2の暗号プログラムに問題点があることが指摘された³が、これは後者に該当するものであった。こうした観点からは、暗号プロトコルや暗号製品の実装面まで立ち入った安全性評価が必要となるが、その実現は容易ではない。というのも、(1)については、SSLの仕様書は比較的曖昧な書き方になっていて、仕様書だけで欠陥を指摘するのは難しい。一方、(2)については、実際に使われているマイクロソフト社やネットスケープ社の実装の内容を検証することが困難であるためである。

しかし、例えば、SSLで利用されているRC4(128)の暗号解析の結果、仮に「解読するためには 2^{100} 以上の計算量が必要」などという結論が出たとしても、それが「RC4(128)を利用し

³ この事件は、Netscape Navigator Ver.1.2において、暗号通信のための鍵を生成するプログラム（すなわち鍵管理）に問題があり、暗号が容易に破られてしまうことが分かったというもの。その報道を受けて、当時インターネットを利用したオンライン・バンキングのサービスを提供していた米国の銀行は、相次いでサービスの停止に踏み切った。この事例は、善意の解析者が問題点を指摘したという点で、個々の利用者の被害を未然に防ぐ効果があり、暫くして問題点を修正したプログラムがVer.2.0として配布されたことによって解決されたが、暗号技術の欠陥が社会に大きな影響を及ぼしたという意味で、注目される事件であった。

た SSL の安全性」を保証するものではないという点には注意が必要である。例えば、鍵生成や鍵交換に対するアタックで、 10^{10} 以下の計算量で実現できるものがあるかも知れない。そういった観点も含めて、「暗号プロトコルの評価」が必要と考えられる。

(3) SSL 以外の場合

SSL 以外の例を考えると、そもそもテーラーメイドの技術が多く、ある程度は個別に解析することが可能であり、評価すること自体の難しさは少ない可能性がある。ただ、あまり使われていない暗号プロトコルの場合、誰もチェックしていないので、より危険性が高いかも知れない。こうした観点からは、電子政府で利用する「信頼できる暗号プロトコル、暗号製品」の数をある程度絞り込んだ上で、それらについて悉皆で安全性確認を行うというアプローチが考えられる。

8.2 暗号モジュール評価の重要性

(1) 暗号モジュールとは何か

第三章で検討中の電子政府システムに対して必要な暗号機能を組込む場合、(a) アプリケーション毎に必要な暗号機能を直接作り込む、(b) 市販の暗号ライブラリを利用する、(c) 暗号機能付きの IC カードなどのハードウェアを利用するという、3つの方法が一般的に行われている。

(a) 暗号機能を直接作り込む方法は、暗号技術が一般的でなく暗号ツールの入手が困難であった時代には散見された。しかし、この方法は、アプリケーション毎に暗号機能を組込むため生産性が低く、また、アプリケーション毎に暗号機能を作り込むために、セキュリティホール⁴の原因になり易いという欠点を持っている。そのため最近では、(b) 暗号研究者・技術者が作成した暗号ライブラリや(c) 暗号機能を実現する専用のハードウェア(HSM⁵)を利用する方法が一般的になっている。専門家が作った暗号ライブラリや暗号機能を司る専用ハードウェアのことを「暗号モジュール(CM⁶)」や「暗号サービスプロバイダ(CSP⁷)」と総称する。

この様な暗号モジュールを想定すると、アプリケーション作成担当部門は暗号モジュールが提供するアプリケーションインタフェース(Crypto-API⁸)を介して、暗号機能を利用することが可能となり、暗号機能サブルーチン等を作成する手間が軽減される。

⁴ セキュリティホールの例：簡単なセキュリティホールの実例を紹介する。暗号機能を利用するときに、専用の作業領域を確保する必要があり、この領域に本来秘匿しなければならない鍵情報等が一時的ではあるが存在する。暗号処理終了後、この領域を開放する場合に秘匿対象情報を消し忘れるケースが一つの例である。

⁵ HSM : Hardware Security Module

⁶ CM : Cryptographic Module

⁷ CSP : Cryptographic Service Provider

⁸ Crypto-API : Cryptographic Application Interface

また、この様に暗号機能をまとめて管理することにより、暗号アルゴリズムの多様化や換装といった作業の軽減も可能となっている。

従って、暗号モジュールを「安全」に作る事ができれば、アプリケーション作成担当部門は、Common Criteria の要求するところに従って、アプリケーションを開発すればよいことになる。一方、暗号モジュールに対しては、8.1節で述べたように、電子政府で利用する「信頼できる暗号製品（暗号モジュール）」に対する要求を明確にし、「暗号モジュール」製品がその「要求」を満たしているか否かを評価する必要がある。この分野で先行している米国標準・技術院情報技術研究所(NIST⁹)が策定し公開している暗号モジュール評価プログラム（CMVP¹⁰）の例を次節で紹介する。

(2) NISTにおける暗号モジュール評価

NISTにおける、暗号モジュールの評価は、FIPS 140-1/-2 と呼ばれる連邦情報処理標準に則って実施されている。FIPS 140-1 は1994年1月に制定されており、既に10年近い運用実績を持っている。運用のイメージを図9.1に示す。

FIPS 140-1/-2 は、機密情報を保護するセキュリティシステム内で利用される暗号モジュールが満たすべきセキュリティ要件を規定するものである。連邦情報処理標準（FIPS）

140-2 およびその他の暗号に基づく標準に対する暗号モジュールの認証は、暗号モジュール認証プログラム（CMVP）という制度で運用されている。CMVP は、NIST とカナダ政府通信安全保障局（CSE）との共同事業であり、FIPS 140-1/-2 に適合と認証された製品は、両国の連邦政府によって機密情報（米国）または指定情報（カナダ）の保護向けとして認証される。CMVP の目標は、認証済み製品の使用を促進すること、ならびに暗号モジュールを装備した機器を調達する際に用いることができるセキュリティ測定基準を連邦政府に提供することである。

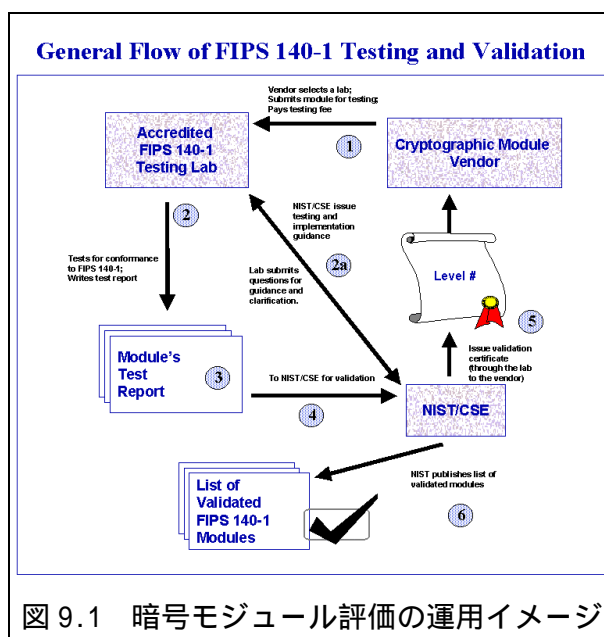


図9.1 暗号モジュール評価の運用イメージ

⁹ National Institute of Standards and Technology (<http://csrc.nist.gov/>)

¹⁰ Cryptographic Module Validation Program

次に米国政府標準暗号と CMVP との関係について述べる。米国政府が現在までに定めている標準暗号は FIPS 46-3(DES, Triple DES), FIPS 186-2(DSS¹¹), FIPS 180-1(SHS¹²), FIPS 185(Skipjack), FIPS 197(AES)の5種類¹³であり、これらの標準暗号が試験手続 (Testing Requirements)¹⁴

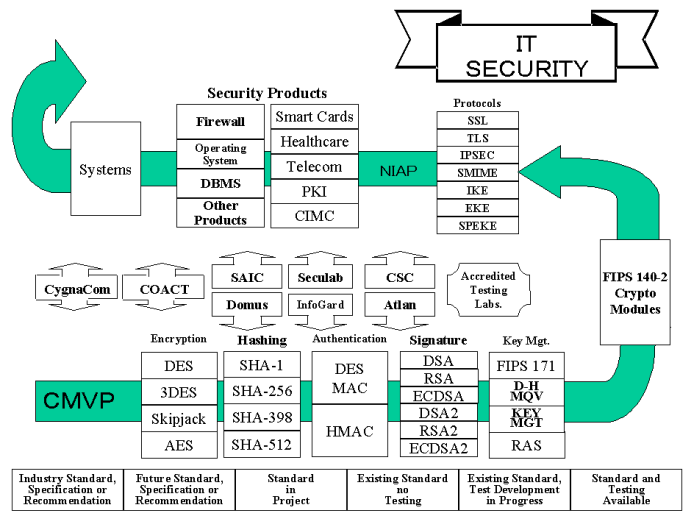


図 9.2 標準暗号と暗号モジュール評価

に沿って、FIPS 140-1/-2 で定める要求に適合しているか否かが評価される。CMVP(暗号モジュール評価)と標準暗号、Common Criteria の関係を図 9.2¹⁵に示す。CMVP としては、2001 年の終わりには、200 以上の暗号モジュール (HW, LSI, SW, FW) の評価を完了すると見込んでいる。

(4) 我が国での暗号モジュール評価の在り方

我が国では、理論研究に重きが置かれ、実装面からの評価という面では、欧米に遅れをとっているのが現状である。

また、欧米では古くから TEMPEST¹⁶等の電磁波放射による情報漏洩などに代表される実装面での評価技術 (言い換えれば、情報収集技術) に関する研究開発や、欧州ではクレジットカードの Smart-Card 化が進んでいるため、民間でも評価技術 (解析技術) に対する要求があったことも見逃せない。

米国 NIST は CMVP のスキームを ISO 化することを目指しており、今回の FIPS 140 の改訂はそのステップの一部であろう。また、英独が興味を示していること、仏が IC カードの評価において、類似のスキームを有しているとの話も聞こえてくることから考えて、欧州の状況を早急に調査する必要があると考える。また、適合試験実施試験機関の一つである CygnaCom に対する調査では、どの評価機関とも暗号モジュール評価単独では採算が合わないといっていることから、CC との共同運用も視野に入れた、我が国としての暗号モジュール評価のあり方を研究する必要があると考える。

¹¹ Digital Signature Standard : DSA, RSA, ECDSA を規定
¹² Secure Hash Standard : SHA-1 を規定
¹³ 今後、SHA-256/-384/-512, DSA2, RSA2, ECDSA2 等が追加される計画がある。
¹⁴ この試験手続は、Derived Test Requirements [DTR] として公開されている。
¹⁵ NIST 資料より転載
¹⁶ Transient Electromagnetic Pulse Standard

9．次年度以降の評価を含む活動指針（検討会及び評価委員会の両者における活動）

（１）電子政府推奨暗号に関する活動案

- ・前記４．で記述したとおり、2002年度中に推奨暗号に関するリスト案を作成し、各省庁において合意を目指す必要がある。そのために、リスト案をCRYPTRECで作成し、併せて調達のためのガイドブック案を作成する必要がある。

（２）2002年度活動案

来年度の活動案は以下のとおり。

4月～9月

- ・ リスト案の作成。（評価の継続及び精査、要件の精査）
- ・ 調達のためのガイドブック案の作成。
- ・ 新規提案暗号に関する公募は行わない。

10月～3月

- ・ 各省庁合意のサポート。
- ・ 調達のためのガイドブックの完成。
- ・ 普及・啓蒙。
- ・ 新規提案暗号に関する公募は行わない。

（３）2003年度以降の活動案

中長期的な活動内容として以下の事項が挙げられる。これらの事項に関して、適宜2002年度から検討・調査を進めることとする。

電子政府推奨暗号のモニタリング。

5年ごとの評価見直し。

暗号の利用方法に関する各種ガイドラインの整備（作成、改訂）。

データベースの管理。

体制の拡充、高度化に向けた研究開発、人材育成、利用の定常化、普及の推進。

暗号プロトコル評価、暗号モジュール評価の実施。

米国NIST、ISO/IEC JTC1 SC27等との国際協力。

必要に応じ国際標準との関係を整理。

（４）評価体制のあり方

2003年度以降の評価体制のあり方について、米国NIST等を参考にしつつ、恒常的な評価事務局の設置も含め、引き続き検討を行う必要がある。

（了）

要件調査ワーキンググループ報告書

2002年3月

暗号技術検討会

要件調査ワーキンググループ

目次

はじめに

1. 本報告書の目的	1
1.1 ワーキンググループ活動の背景	1
1.2 ワーキンググループ活動の目的	1
2. 検討の進め方	1
2.1 概要	1
2.1.1 要件調査WGにおける検討対象	1
2.1.2 検討事項	2
2.1.3 調査及び検討方法	2
2.1.4 会合開催状況	3
3. 調査結果	4
3.1 ヒアリング調査結果	4
3.1.1 実施要領	4
3.1.2 調査結果	4
3.2 アンケート調査結果	6
3.2.1 実施要領	6
3.2.2 主な調査結果	6
3.3 SSLで利用される暗号の安全性評価結果	11
3.3.1 調査の目的	11
3.3.2 調査の対象と範囲	12
3.3.3 調査の方法	12
3.3.4 調査結果	12
3.3.5 SSL/TLSの運用及び利用にあたっての注意点	14
3.4 海外電子政府システム調査結果	16
3.4.1 概要	16
3.4.2 海外電子政府システムの暗号利用形態事例	16
3.4.3 セキュリティ要件	19
3.4.4 プロトコル、製品評価制度事例	21
3.4.5 まとめ	22
4. 電子政府システムにおける暗号技術利用の要件	24
4.1 電子政府のシステム別モデル	24
4.1.1 電子申請システム	25
4.1.2 電子調達システム	27
4.1.3 電子納付システム	29
4.1.4 電子情報提供システム	31
4.1.5 政府認証基盤	34

4.2	電子政府システムにおける暗号利用形態	37
4.3	暗号技術に求められる要件	38
4.3.1	電子政府システムにおける一般的要件	38
4.3.2	暗号の利用形態別要件	39
5	電子政府における暗号利用に関する提言等	41
5.1	推奨暗号の数に関する考察	41
5.2	その他の提案	43

はじめに

近年、インターネット等の高度利用をもたらすブロードバンド化及び常時接続化が急速に進行しつつある。これに伴い、インターネット等を利用したコンテンツ配信、電子商取引等も急速に拡大している。

政府においても、2001年3月にe-Japan重点計画が決定され、インターネット等を利用した行政情報の電子的提供、申請・届出等手続の電子化等を主な項目とする「電子政府」を2003年度までに実現することを目指している。

電子政府においては、客観的にその安全性が評価され、実装性で優れた暗号技術を採用する必要があることから、2001年5月から、総務省と経済産業省の共同で「暗号技術検討会（委員長：今井秀樹東京大学教授）」が開催され、2002年度中に電子政府における調達のための推奨すべき暗号のリストを作成すべく、評価が行われているところである。

本WGは、暗号技術検討会のサブグループとして設置されたものである。本WGでは、主に暗号技術の評価にあたり、電子政府システムのニーズに合致した評価ができるようにすると共に、評価結果のシステムへの迅速な反映等を目的として、電子政府等の政府利用における暗号技術に対する要求条件に関する検討を行ってきた。この過程で、本WGでは、国内及び海外で既に運用中のシステムを調査するに止まらず、メーカ、SI等の意見を聴取することにより、暗号利用の現状、そのあるべき姿等にも踏み込んで検討を行った。

最後に、本WGでの調査に協力いただいた官庁や企業の方々、ならびに、本WGで熱心に御議論頂いた構成員や事務局の方々に、この場を借りて感謝の意を表したい。

暗号技術検討会要件調査ワーキンググループ
リーダー 佐々木 良一

第1章 本報告書の目的

1.1 ワーキンググループ活動の背景

2001年3月にIT戦略本部において決定されたe-Japan重点計画では、高度情報通信ネットワークの安全性及び信頼性の確保のため、「暗号技術の標準化の推進」を具体的施策の一つに掲げている。

これに基づき、総務省と経済産業省は、共同で「暗号技術検討会（座長：今井秀樹東京大学教授）」を開催し、実装性に優れた利用可能性の高い暗号技術を各省に推薦し、高度な信頼性及び安全性に支えられた電子政府の構築に貢献することを目指している。

暗号技術検討会では、推奨すべき暗号リストの作成に向けて検討を行っているが、電子政府等の政府利用における、暗号技術に対する要求条件を明らかにするための調査及び検討を集中的に実施する必要性が生じたため、サブグループとして要件調査ワーキンググループ（要件調査WG）を設置することとした。

1.2 ワーキンググループ活動の目的

要件調査WGでは、暗号技術の評価にあたって、評価精度の向上、評価の効率的な実施、評価結果のシステムへの迅速な反映等を目的とし、電子政府等の政府利用における暗号技術に対する要求条件（要件）を明確にするための検討を行った。

第2章 検討の進め方

2.1 概要

2.1.1 要件調査WGにおける検討対象

要件調査WGで検討対象とする電子政府システムは、以下の全ての条件を満たすものとした。

- (1) 国の行政機関のシステム（大学、病院、地方自治体は対象外）
- (2) 国家の安全保障のため、又は国家の防衛上の目的のためのシステムを除く。
- (3) 国民との間で行政サービスとしてやりとりを行うもの、及びそのやりとりを安全に行うために必要な関連システム（下位層のシステムを含む。）

2.1.2 検討事項

要件調査WGでは、以下の項目について検討を行った。

- (1) 電子政府において暗号技術を利用すると想定されるシステムのモデル化
- (2) 電子政府に関連する海外の先行事例における暗号技術の取り扱い
- (3) 技術的な要求条件の抽出
- (4) 暗号技術を利用するにあたっての留意事項

2.1.3 調査及び検討方法

(1) 国の行政機関のシステムに関するヒアリング調査

現在、国の行政機関の電子政府等で運用されているシステムにおける、暗号利用の現状を把握し、要件抽出の参考とするため、「電子申請」「電子調達」「電子納付」「電子情報提供」「政府認証基盤」の各システムに関連するシステムについて、構成イメージ、処理フローイメージ、利用暗号技術等に関するヒアリングを実施した。

(2) メーカー、ベンダ等に対するアンケート調査

暗号技術に関する知識を持ち、政府に対してシステムの提案を行う立場のメーカー、ベンダ等に対して、要件調査WGが(1)のヒアリングの結果に基づいて想定した暗号技術の利用形態、利用目的、要件等についての意見を求めるため、アンケート調査を行った。また、将来の暗号技術のあるべき姿等についても併せて意見聴取を行った。

(3) SSLの現状調査及び安全性評価

(1)でヒアリングを行ったシステムは、SSLをベースに構築し、またはこれから構築しようとしているケースが多いことが分かった。そのため、SSL等で利用されている暗号アルゴリズムを詳細に調査し、主なものについては、暗号技術評価委員会に対して安全性評価を依頼した。

(4) 海外電子政府システムに関する調査

北米、欧州、アジア・オセアニアにおける情報技術の水準の高い主要な国々について、政府部門向けセキュリティ標準および暗号標準、電子政府サービス事例における暗号利用を調査した。特に、セキュリティ標準および暗号標準が整備・公開されている国について詳しく状況を調べた。電子政府サービスについては、電子納税などセキュリティの重要なサービスを中心に提供方式を調べ、実際にアクセスできたSSLで保護されたページのパラメータをまとめた。

2.1.4 会合開催状況

要件調査WG会合は、2001年6月から2002年3月まで計12回開催した。各回の開催日時と主な議題を下表に示す。

回数	開催日	主な議事
第1回	2001年6月27日	- 電子政府での暗号技術の要件整理調査について - 要件調査WGの今後の作業について
第2回	2001年7月16日	- ヒアリング結果概要報告 - 要件の整理方法に関する検討
第3回	2001年7月19日	- ヒアリング結果概要報告 - WGの今後の活動方針 - 海外電子政府における調査項目 - SSL、S/MIMEなどの暗号利用状況 - システムモデルの検討
第4回	2001年8月1日	- 海外調査の進め方の検討 - ヒアリング調査内容の検討 - SSL、S/MIMEに標準的に実装されている暗号についての報告
第5回	2001年8月27日	- ヒアリング調査内容の検討 - 国内及び海外調査内容の検討
第6回	2001年9月19日	- システム別モデルの検討 - アンケート調査票内容の検討 - 海外調査項目及びスケジュールの検討 - SSLに利用されている暗号に関する調査依頼に関する検討 - 最終報告書イメージの検討
第7回	2001年11月30日	- システムのモデル化及び要件の抽出 - 最終報告書目次案の検討
第8回	2001年12月25日	- 海外電子政府システム調査中間報告 - アンケート調査経過報告 - 最終報告書目次案の検討
第9回	2002年1月15日	- アンケート調査結果報告 - 最終報告書骨子案の検討
第10回	2002年2月8日	- 海外電子政府システム調査経過報告 - 国内アンケート調査結果報告 - 最終報告書一次案の検討
第11回	2002年2月18日	- 推奨暗号数に関する検討 - 最終報告書一次案の検討
第12回	2002年3月1日	- 海外電子政府システム調査結果報告 - SSLに利用されている暗号に関する調査結果について - 最終報告書案の検討

第3章 調査結果

3.1 ヒアリング調査結果

3.1.1 実施要領

以下の要領で、既存の政府関係システムに関するヒアリング調査を行った。

実施時期 2001年7月～2001年11月
 実施方法 面接（事前に質問票をメールで送付）

3.1.2 調査結果

各システムの概要、SSL利用の有無、暗号利用形態を下図の通りまとめた。

システム名 (ヒアリング実施日)	SSL	暗号利用形態	
総務省 電子申請システム (2001.7.6) 詳細仕様未定	利用 する	申請側署名 公開鍵：RSA(1024,2048) 官庁側署名 公開鍵：RSA(1024) 通信暗号化 未定	ハッシュ：SHA-1,MD5 ハッシュ：SHA-1
経済産業省 電子申請システム (2001.7.13) 【システム概要】 経済産業省が所管する申請業務 における受付、審査、決裁、 公文書発行	利用 せず	申請側署名 公開鍵：RSA 申請側送信 公開鍵：RSA 共通鍵：TDES,DES 一次形式審査 公開鍵：RSA 公文書発行 公開鍵：RSA 民間側公文書取得 公開鍵：RSA 共通鍵：TDES,DES	ハッシュ：SHA-1,MD5 ハッシュ：SHA-1,MD5 ハッシュ：SHA-1,MD5 ハッシュ：SHA-1,MD5 ハッシュ：SHA-1,MD5
電子申請推進コンソーシアム 電子申請システム (2001.7.13) 【システム概要】 利用者から行政機関への申請 及び届出	利用 する	申請書式入手 公開鍵：RSA(1024) 利用者側署名 公開鍵：RSA(1024) 通信暗号化 公開鍵：RSA(1024) 共通鍵：未定（CAST,DES,TDES,RC2等を予定）	ハッシュ：SHA-1
経済産業省 電子入札パイロットシステム (2001.8.1) 【システム概要】 経済産業省における入開札業務	利用 する	利用者側署名 公開鍵：RSA(1024) 入札書暗号化 公開鍵：RSA(1024) 共通鍵：RC2(128) 通信暗号化 公開鍵：RSA(CA:2048,EE:1024) 共通鍵：RC2(128)	ハッシュ：SHA-1
ICカードシステム (2001.8.1)	利用 せず	(Common Access Cardの例) 公開鍵：RSA(1024) ハッシュ：SHA-1,MD5 共通鍵：DES,TDES,Skipjack	

システム名 (ヒアリング実施日)	SSL	暗号利用形態
マルチペイメントネットワーク (2001.11.13) 【システム概要】 <ul style="list-style-type: none"> 金融機関～収納機関の照会依頼及び照会応答の中継 金融機関～収納機関の消込依頼及び消込応答の中継 金融機関から収納機関口座への入金データ及び金融機関間の決済データの作成・送信 	利用せず	<ul style="list-style-type: none"> データの暗号化：TDES(3key) 認証：Pre-Shared キー 鍵共有：DH(1024) 通信暗号化：IPsec
政府認証基盤 (2001.11.13) 【システム概要】 <ul style="list-style-type: none"> BCA システム BCA リポジトリ 統合リポジトリ 証明書検証システム 	利用する	ブリッジ CA～各府省 CA 間で相互認証証明書発行：RSA(1024) リポジトリ複製処理 証明書 RSA(1024) 暗号化 RC4(128,64,40)*, RC2(128,40)*, DES, TDES *：ビット長の長いものから優先的に選択 証明書検証処理：RSA(1024)
法務省 債権譲渡登記オンライン申請システム (2001.11.14) 【システム概要】 <ul style="list-style-type: none"> 申請プログラムの配布 電子署名及び暗号化された申請データの受付 	利用せず	<ul style="list-style-type: none"> 申請データ署名：RSA(1024or2048 の選択可) ハッシュ：SHA-1 通信暗号化：TDES (鍵配信：RSA(1024))
建設 CALS (2001.11.14) 【システム概要】 (電子入札システム) <ul style="list-style-type: none"> 調達案件登録、入札参加資格確認申請や入札書の受付 入札公告、入札書、入札結果等の公開等 入札参加資格確認申請や入札書の送信等 入札書公開鍵の生成、管理等 (PPI 入札情報サービスシステム) 調達情報の公開、作成支援、自動収集 	利用する	(電子入札システム) <ul style="list-style-type: none"> 入札参加申請書の暗号化：RSA(政府側 1024,利用者側 1024) (CA 局のルート鍵 1024) 入札参加申請書への署名：SHA-1 入札書及び内訳書の暗号化：RC2(128) (PPI 入札情報サービスシステム) 地方クライアント～中央サーバ間の調達情報自動収集における通信暗号化：RC4(56,64,128), RC2(40,128), TDES, DES サーバ・クライアント間のハンドシェイクにより決定

3.2 アンケート調査結果

3.2.1 実施要領

以下の要領で、メーカー及びベンダ等へのアンケート調査を行った。

実施時期	2001年12月～2002年1月
実施方法	メールで質問票を送付
対象企業	17社
うち回答企業	16社

3.2.2 主な調査結果

(1) 総論

暗号の要件

- ・暗号の要件としては、第一優先として安全性（今後、10年間利用可能）を挙げる回答が最も多かったが、実装性（処理速度、サイズ）、暗号標準（デファクト又は国際標準であること）とする回答もあった。
- ・他には、認定制度をクリアしていること、採用実績、等の回答があった。
- ・また、各要件の優先順位を点数化（1位：5点、2位：4点、3位：3点）すると、点数の高いものは 1：安全性、2：実装性、3：暗号標準、の順であった。

質問 1-(5) 暗号の要求条件（要件）として、安全性、実装性、暗号標準、プロトコル標準、製品、特許、を想定しています。このうち、要件に該当しないものがありますか。また、他に考えられる要件がありますか。更に、要件に該当する物について、優先順位はどうですか。

回答)・要件に該当するかどうか

上記6つは全て該当する：11社

該当しない物がある：3社（製品：2社、暗号標準、プロトコル標準：各1社）

無回答：2社

・他に考えられる要件

- 認定制度(今は無いが、FIPS140-2のようなものを想定)をクリアしていること(2社)
- 採用実績があること(1社)
- 国内製品であること(1社)

・上記要件の優先順位（同順回答、無回答あり）

安全性 1位：11社、2位：1社、3位：0社、4位以下：2社

実装性 1位：3社、2位：6社、3位：1社、4位以下：4社

暗号標準 1位：2社、2位：3社、3位：1社、4位以下：7社

10年後の要件の優先順位

・10年後の要件の優先順位は「現在と変わらない」「変わる」で半々だった
変わらないとする意見は「10年間で暗号解読技術が進歩する一方、新たな
暗号関連技術も登場するので、現在の基準はそのまま当てはまるとされる」
が、主な理由だった。一方、変わるとする意見の主な理由は「ハードウェア
の性能の向上により、実装性の順位が相対的に低下すると思われる」だった。

質問 1-(5)-2) 上記の優先順位は10年後には変わると思うか。

回答) 変わる : 7社
変わらない : 7社
無回答 : 2社

暗号の耐用年数

・暗号の耐用年数は「一部の用途については10年以上必要」とする回答が
多かった。10年以上の耐年が必要な用途としては、署名に使う暗号処理、
CAの秘密鍵という意見が多かった。

質問 1-(6) 暗号の利用耐年について、どのように考えるか。

回答) 全て10年程度の耐年で良い : 3社
一部の用途は10年以上必要 : 10社
全て10年以上必要 : 0社
その他 : 3社

(2) 暗号アルゴリズム各論

要件に値しないカテゴリー

・通信路(利用者~政府間)の守秘における要件については、SSL等の
プロトコル標準に入っている必要はない、との意見があった。

質問 2-(a)-1, 2-(b)-1

要件に値しない(カテゴリーとして考慮しない)とお考えのカテゴリーに
ついて、要件表の欄目の番号と理由をお書き下さい。

回答) (6)(ウ)(キ)

理由 ・システムに作り込みが発生するため、関係ない
・組み込みプラグイン・ソフトなどで対応可能なので、必ずしも
SSLの標準である必要はない。

・政府側のデータ保管については、改ざん防止と否認防止のための暗号化が
必要、との意見があった。

質問 2-(a)-2

要件として考慮するものについて、それぞれの判断基準がふさわしくないとお考えの場合は、その栞目の番号とお考えの要件をお書き下さい。

回答) (5)(シ)(ス)

- 理由
- ・政府側が保管している申請書を改ざんする場合もありうるので、改ざん防止と否認防止は必要。
 - ・完全性の保証/否認防止の双方とも、非公開/公開に関わらず必要。
 - ・高い安全性を求めるべき
 - ・電子署名も必要となる。

- ・また、政府側のデータ保管における要件については、守秘の際の処理は高速である必要がある、との意見があった。

質問 2-(a)-2

要件として考慮するものについて、それぞれの判断基準がふさわしくないとお考えの場合は、その栞目の番号とお考えの要件をお書き下さい。

回答) (4)(シ)(ス)

- 理由
- ・保存についても件数によっては速度についての考慮要
 - ・運用の負担を考えると処理速度は速いほうが良い。

(3) 調達・リスト化

リストの利用形態区分

- ・推奨暗号リストの利用形態区分については、半数以上が「署名、認証通信、保存」を修正すべき、と答えた。

質問 3-(1) 暗号のリスト化にあたり、利用形態の区分を署名・認証、通信、保存、と想定しているが、適当か。

回答) 適当である : 7社

その他 : 9社

(修正例)

- 署名と認証を分離し、署名・否認防止、通信・認証、秘匿とすべき。
- 「通信」ではなく「守秘」とすべき。
- 「保存」を「長期完全性保証」と「長期守秘」に分けるべき

- ・また、各区分を方式別(公開鍵、共通鍵等)、目的別(守秘、認証等)に更に細分化すべき、という意見が多かった。

質問 3-(2) また、3-(1)以外の区分によってリスト化すべき、更に詳細に細分化すべきという考えがあれば、お書き下さい。(例えば公開鍵、共通鍵といった方式別や、守秘、認証といった目的別)

回答) 方式別に細分化すべき : 7社
目的別に細分化すべき : 2社
その他 : 6社
無回答 : 1社

推奨暗号の個数

- ・各区分における暗号の個数は、2～3個を望ましいとする意見がほとんどだった。

質問 3-(3) 上記(1)や(2)のように区分した場合、それぞれの区分における暗号は一つまたは複数のどちらが望ましいかお選び下さい。また、その理由をお書き下さい。

回答) 1つが好ましい : 1社
複数が好ましい : 15社
2～3個 : 14社、
3～5個 : 1社

政府調達における仕様の指定

- ・政府が電子政府システムを調達する際、仕様書に暗号アルゴリズムを指定することについては、問題ない、又は条件付きで問題ない、という意見が大多数であり、逆に製品名まで指定することには大多数が反対だった。

質問 3-(4) 政府が電子政府システムを調達する際の仕様書の書き方について、アルゴリズムが指定される調達方法について、何か問題があるとお考えですか。

回答) 問題ない : 1社
条件が満たされれば問題ない : 12社 ()
問題あり : 2社
無回答 : 1社

条件

- ・指定の範囲が特定の企業、ベンダの製品を指すものではないこと
- ・「指定した暗号と同じ条件(強度等)を持つもの」とすること
- ・権利対策がなされた(ベンダの対策が不要)状態で指定されること

質問 3-(6) アルゴリズムだけでなく、製品名までも指定された方が望ましいかどうか、ご意見をお聞かせ下さい。

回答) 望ましい : 0社
条件が満たされれば望ましい : 1社
望ましくない/必要ない : 14社
その他 : 1社

(4) その他

市販ソフトに組み込まれている暗号を考慮すべきか

- ・推奨暗号を選定する際、SSL等の市販のクライアントソフトに組み込まれている暗号を考慮すべきかどうかについて、「考慮すべき」又は「どちらかと言えば考慮すべき」とする意見は約半数だった。

質問 4-(1) 電子政府システムで利用する暗号を選定する際、SSL等の市販のクライアントソフトに組み込まれている暗号を考慮すべきですか。

回答) 考慮すべき : 3社
どちらかと言えば考慮すべき : 4社
考慮せず、技術的に優れた暗号を選定すべき : 5社
その他 : 4社

ICカードシステムにおいて利用する暗号の技術的要件

- ・ICカードシステムで用いる暗号の要件としては、「実装サイズ、実装可能性」「処理速度」が最も多く、以下、「標準暗号」「耐タンパ性」「鍵サイズ」「暗号強度」といった回答が多かった。

質問 4-(2) ICカードで利用する暗号の技術的要件には、どのようなものがありますか。要件とその判断基準をお書き下さい。
(複数回答可)

回答) 実装サイズ、実装可能性 : 9社
処理速度 : 9社
標準暗号、耐タンパ性 : 各5社
鍵サイズ、暗号強度 : 各4社

暗号に関して考慮すべき技術要素

- ・暗号に関して、アルゴリズム以外に考慮すべき技術要素としては、「通信プロトコル」「鍵管理方式」「運用管理」の順に多かった。

質問 4-(3) システムのセキュリティ確保のため、暗号に関してアルゴリズム以外に考慮すべき技術的要素はありますか。
(複数回答可)

回答) 通信プロトコル : 6社
鍵管理方式 : 4社
運用管理 : 3社
実装 : 2社
アルゴリズム互換性 : 2社
乱数生成 : 2社

3.3 SSLで利用される暗号の安全性評価結果

電子政府システムの構築にあたって、予め利用者のパソコンに組み込まれた市販ソフトを利用して暗号機能を実現するケースが考えられる。

暗号機能を含む代表的なセキュリティ仕様であり、一般にクライアントソフトが市販されているものとしてはSSLとS/MIMEがある。3.1節の既存政府関係システムのヒアリング調査によれば対象とした10システムのうち6システムがSSLを利用している。さらに、3.2節のアンケート調査では、電子政府に用いられる暗号として、SSL等の市販のクライアントソフトに組み込まれる暗号も考慮すべきという意見が半数を占めた。また、海外の電子政府事例調査においても、電子申請システムにおいてユーザ名とパスワードをSSLで保護する事例がある(3.4節参照)。

一方、S/MIMEに関しては利用実績や特段の意見は認められなかった。

これらのことより、要件調査WGはSSLプロトコルが政府関係システムに用いられており、今後も用いられるケースが多いと判断し、SSLプロトコルの詳細調査を行い、SSLプロトコル自体の安全性とSSLプロトコルで用いられる暗号の安全性評価を行うものとした。評価対象の暗号は、公開鍵暗号としてRSA、共通鍵暗号としてDES、TDES、RC2、RC4とした。

3.3.1 調査の目的

SSLはインターネットにおいて最も普及しているセキュリティプロトコルである。SSLはWeb上の暗号化や認証機能などを実現するものであり、インターネットを用いた電子商取引に広く用いられている。また、SSLとほぼ同じ仕様がTLSという名称でインターネット標準として検討されている。

本調査では、SSL/TLSプロトコル及びそこで用いられる暗号の安全性の調査と評価を行っている。本調査の結果が、電子政府のセキュリティシステムの調達者・設計者・ユーザに対してSSL/TLSに用いられる暗号とプロトコルの安全性について正しい理解を与え、SSL/TLSが適切に利用されることを期待する。

SSL/TLSプロトコルの安全性調査としては、SSLの仕様上および一般に普及している実装ソフトウェア上のセキュリティホールを調査する。SSLに含まれる暗号技術の安全性評価は、可能な限り他の電子政府用暗号候補に対するものと同様のレベルで行ない、SSL/TLSで用いられる暗号を他の暗号と比較することを図る。

本調査のまとめとして、電子政府システムにおいてSSLを運用する場合の注意点について述べる。

3.3.2 調査の対象と範囲

SSLとは、OSI参照モデルのうちセッション層に位置するプロトコル(通信手順)で、Webブラウザやファイル転送といったアプリケーションによらない汎用的なセキュリティを実現できる。

SSL3.0 (<http://home.netscape.com/eng/ssl3/draft302.txt>, 1996)は米国 Netscape Communications 社によって規定されたプロトコルである。一方、TLS(Transport Layer Security) Vr1.0 (<http://www.ietf.org/rfc/rfc2246.txt>, 1999)は、インターネット技術の標準活動を行なっている IETF (Internet Engineering Task Force)が SSL3.0 を引き継いで RFC2246 として規定したものである。本調査では、SSL3.0 と TLS1.0 の差異と IETF で行なわれている TLS の拡張作業についても調査した。

暗号技術検討会から暗号技術評価委員会に対して、以下の暗号の安全性を SSL の利用環境のもとで評価するように依頼を行なった。

共通鍵暗号：RC2(40,128ビット)、RC4(40,128ビット)、DES(40,56,168ビット)
公開鍵暗号：RSA 暗号

本節では、これらの暗号の安全性評価結果を述べる。ただし、RC4については権利者との調整に時間がかかり、評価が間に合わなかったため本報告の対象から外した。

3.3.3 調査の方法

暗号評価に関しては内外の暗号研究者(組織)に評価を依頼し、暗号技術評価委員会で結果のとりまとめを行なった。各暗号の評価者数は、DES 1名(組織)、RC2 2名(組織)、RSA 5名(組織)である。また評価期間は2001年10月より14年2月までである。

3.3.4 調査結果

(1) SSL/TLS プロトコルの安全性評価

SSL/TLS プロトコルについて、暗号方式の安全性、プロトコルとしての安全性、実装に関する安全性、運用上の安全性に分類して調査したところ次のような結果が得られた。

(a) 暗号方式に関わる安全性

RSA 公開鍵暗号方式の暗号化には PKCS#1 と呼ばれる実装仕様が適用されるが、PKCS#1V1.5 に対する適用的選択暗号文攻撃の存在が指摘されており、改良版である PKCS#1V2.0 の利用が推奨される。さらに PKCS#1V2.0 にも別のセキュリティホールが指摘されており、改善策が V2.1 において実現されている。

(b) プロトコルに関する安全性

SSL には相互認証、サーバ認証のみ、匿名の 3 つの認証モードがあるが、このうち匿名認証モードにおいては 2 者間の通信の間に不正者が介在する man-in-the-middle 攻撃が存在し、情報の盗聴・改ざんの攻撃を受ける可能性があるため利用することは推奨されない。その他、攻撃者が SSL3.0 に対応しているサーバ、クライアントに対して SSL2.0 やそれ以下の Version で通信を行うように強制する攻撃法である version rollback 攻撃などがありうるが、version rollback 攻撃は、SSL の最新版のみを使用するよう設定運用することで、攻撃を防ぐことができる。

(c) 実装に関わる安全性

SSL/TLS の公開鍵証明書を使った認証に関して、証明書検出機構が実装されていないケース、不正な証明書に対して警告を出さないケース、認証動作を迂回する攻撃が可能となるケースなどが報告されている。また、セッション鍵に用いる擬似乱数生成器の内部状態が暴露する攻撃も報告されている。実装に関するセキュリティホールについては、バグを改修した最新版や修正プログラムを用いることで攻撃を回避できる。

(d) 運用に関わる安全性

SSL/TLS にはサーバ、クライアント側で運用時に設定するパラメータがいくつか存在し、鍵や証明書を格納するファイル、セッション鍵のライフタイム、乱数生成方法、使用する暗号アルゴリズム、警告メッセージの表示可否などが設定可能である。このためこれらのパラメータの意味を十分理解し適切に設定する必要がある。不用意な設定がセキュリティホールになる可能性がある。

(e) SSL/TLS の比較調査

総じて TLS は SSL に比較して、鍵、初期値、MAC 生成に関して安全性の根拠を明確にし、署名の構造を若干修正したという点でセキュリティ上の差異があるが、SSL についても実用上問題のないレベルであると考えられる。

(2) SSL/TLS に用いられる暗号の評価

SSL/TLS で用いられる暗号の安全性評価について次のような調査結果が得られた。

(a) DES

(暗号単独の安全性評価)

鍵長 40 ビットの DES は鍵総当りにより現実的な時間で解読可能である。鍵長 56 ビットの DES も現実的に解読可能な領域に達している。鍵長が 168 ビットの 3-key TDES であれば当面の間の使用は問題ないといえる。

(SSL/TLS における安全性評価)

いずれの鍵長においても DES はデータ秘匿の目的に用いられる。ブロック暗号モードとしては CBC モードが用いられる。 2^{32} ブロック以上を同じセッション鍵を用いて暗号化すると平文 1 ビットの情報がもれる可能性がある。

(b) RC2

(暗号単独の安全性評価)

鍵長 40 ビットの RC2 は鍵総当りにより現実的な時間で解読可能である。鍵長 128 ビットの RC2 も、現実的に解読可能な領域に達しつつある。最新の暗号解読理論を適用したとき、鍵総当りよりも効率的な解読が知られている。よって、新規に構築する電子政府システムにおいて鍵長 128 ビットの RC2 を採用することは勧めない。

(SSL/TLS における安全性評価)

鍵長は SSL2.0 においては 40 ビットおよび 128 ビットが選択可能であり、SSL3.0 においては 40 ビットのみが選択可能である。40 ビットの鍵は現実的な計算機環境において数時間もあれば全数探索可能である。なお、DES と同じく、 2^{32} ブロック以上を同じセッション鍵を用いて暗号化すると平文 1 ビットの情報が漏れる可能性がある。

(c) RSA

(暗号単独の安全性評価)

512 ビットの鍵長は現実的に素因数分解可能であり安全ではない。2001 年時点では、1024 ビット以上の鍵長を用いれば安全であると考えられる。

(SSL/TLS における安全性評価)

SSL および TLS における RSA 暗号を利用した基本的な鍵共有法および署名法の安全性について調べた。その結果、単純な技術の組み合わせの上に最も基本的なスキームを採用しており、暗号プロトコルとしてはセキュリティホールが潜む余地はほとんどないと考えられる。

3.3.5 SSL/TLS の運用及び利用にあたっての注意点

上記の通り、SSL/TLS プロトコル及び用いられる暗号の安全性評価の結果、これらのプロトコルを利用するにあたっては、以下の点に注意する必要がある。

(1) SSL/TLS プロトコルに関して

- ・SSL3.0 を利用するにあたっては、セキュリティホールを含む SSL2.0 の利用を不可とするなど既知のセキュリティホールを十分認識した上での設定をすべきである。
- ・市販の SSL ソフトウェアを利用する場合、セキュリティホールに対してパッチのあてられた最新版を利用すべきである。
- ・市販のブラウザである Internet Explorer および Netscape Navigator においては CRL (公開鍵証明書無効化リスト)の管理は行なわれていない。従って CRL を不正に消去した上で不正な証明書を用いて認証を欺くという攻撃がありうる。このようなことがないように証明書を格納するファイルは厳密なアクセス管理のもとに管理するべきである。
- ・情報の盗聴、改ざんの攻撃を受ける可能性があるため、匿名認証モードの利用を推奨しない。
- ・version rollback 攻撃を防ぐため、特に理由がない限り SSL/TLS の最新版のみを使用するよう、設定運用すべきである。
- ・SSL3.0 では利用する暗号方式について変更出来ない。一方、TLS1.0 においては新しい暗号技術を追加することが可能となっている。そのため、既存の暗号技術に問題があった場合にも対応が可能である。
- ・なお、TLS は機能追加を目的として拡張作業が行なわれているが、これらの拡張に伴って新たなセキュリティホールが発生する可能性もあるため、今後とも TLS の動向に注目し、その安全性について継続的な調査・検討が必要である。

(2) SSL/TLS で利用される暗号に関して

- ・RC2 であろうと DES であろうと、鍵長 40 ビットの暗号は鍵の全数探索法により現実的な時間で解読可能であるため、安全性が必要なシステムにおいては用いられるべきではない。
- ・鍵長 56 ビットの DES はもはや現実的に解読可能な領域に達しており、高い安全性が必要なシステムにおいては用いられるべきではない。
- ・鍵長 168 ビットの TDES は当面の間の使用は安全性上特に問題ないが、TDES に代わる更に安全な暗号が SSL に採用されれば、それに置きかえるほうが望ましい。
- ・64 ビットブロック暗号である RC2, DES, TDES においては、 2^{32} ブロック以上を同じセッション鍵を用いて暗号化すると平文 1 ビットの情報がもれる可能性があるため、セッション鍵の更新に注意すべきである。
- ・鍵長 128 ビットの RC2 に対して、鍵の全数探索法よりも効率の良い解読方法が存在する。よって、新規に構築する電子政府システムにおいて鍵長 128 ビットの RC2 を採用することは勧めない。
- ・RSA について、512 ビットの鍵長は現実的に素因数分解可能であり安全ではない。2001 年度時点では、1024 ビット以上の鍵長を用いれば安全であると考えられる。

3.4 海外電子政府システム調査結果

3.4.1 概要

以下の国々を対象として、電子政府事例およびセキュリティ標準/暗号標準に関する調査を行った。

- ・北米： 米国、カナダ
- ・欧州： 英国、ドイツ、フランス、スイス、アイルランド、フィンランド、スウェーデン
- ・アジア シンガポール、韓国、イスラエル
- ・オセアニア オーストラリア

3.4.2 海外電子政府システムの暗号利用形態事例

電子政府システムを情報提供、意見公募、電子申請、その他、に分類して調査した。

調査した限り、情報提供では情報保護をしている事例はなかった。やや特殊な例として、一部データを登録利用者に限って提供している事例（ドイツの統計局）で、ユーザ名、パスワードをSSL通信で保護している。

意見公募は事例数が少なかったが、コンピュータ犯罪被害届けを受付けるサイト（米国 IFCC）で情報提供者が特定できる情報をSSL通信で保護している等の事例があった。

電子申請では、米国、カナダ、英国、アイルランドなどでインターネットで納税申告、特許出願のできる事例が始まっている。米国の特許出願システムでは Entrust 社の提供するPKI技術を用いたクライアント認証を行っており、またアイルランドの納税申告システムでは Baltimore 社のPKI技術を用いたクライアント認証を行っている。前者ではクライアント側で専用ソフトを用いるようになっているのに対し、後者では普及した Web ブラウザを用いるようになっている。これは、基本的に企業を対象とするサービス（すなわち、GtoB）である特許出願と、一般国民を対象とするサービス（すなわち、GtoC）である納税申告の差を反映していると思われる。米国州政府における事例として、アリゾナ州の運転免許に関する各種申請サービスでは、利用者の氏名、住所、運転免許番号を平文で送信するようになっている。一般に米国州政府の電子政府システムは通信守秘が厳しくない傾向が見受けられた。

その他の事例として、シンガポールの電子調達、米国の総務サービス局（GSA）のオークションサイトなどで、SSL保護された通信を行っている。

下表に、電子政府システムにSSL通信でページにアクセスできた場合のパラメータを示す（Internet Explorer 6.0 の標準インストールによりアクセス）。

不特定多数を対象とした電子政府サービスでは普及している Web ブラウザを前提とせざるを得ないが、その中で、様々なプロトコル、暗号アルゴリズムの設定が見受けられた。

種類	サイト	運営主体	SSL	暗号利用形態
情報提供	政府情報ポータル FirstGov など http://www.firstgov.gov/ など	米国、カナダ、英国、 オーストラリアなど	利用 せず	暗号化：なし
	Electronic Access Service (EAS) (土地登記情報) https://www.landregistry .ie/	アイルランド Land Registry	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(1024) 暗号化：TDES(168) サーバ認証：MD5RSA RSA Data Security, Inc. クライアント認証：ユーザ名、パスワード
	SWISSREG (知的財産権情報提供) https://www.swissreg.ch/ index.jsp?sessionid=1013 041605202114009&lang=eng	スイス知的財産登録 所 Swiss Federal Institute of Intellectual Property	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(512) 共通鍵暗号：RC4(40) サーバ認証：MD5RSA RSA Data Security, Inc
意見 公募	Public Opinion Messaging System (POMS) (世論受付) http://www.legis.state.a k.us/poms/	米国アラスカ州	利用 せず	暗号化：なし 利用者情報：住所、氏名等
電子 申請	Revenue On-line Service (ROS) (納税申告) http://www.ros.ie/	アイルランド Irish Revenue Commission	利用 する	サーバ認証：(不明) クライアント認証 デジタル証明書 CA：Baltimore 社ホスティングサービ スを利用して、Irish Revenue Commission が運営 クライアント：Web ブラウザ
	NETFILE (納税申告) http://www.netfile.gc.ca /	カナダ関税歳入庁 (Canada Customs and Revenue Agency)	利用 する	プロトコル：SSL 共通鍵暗号：RC4(128) クライアント認証 社会保険番号、生年月日、個人アクセ スコード(4桁~10桁の数字) (electronic signature と称する)
	Electronic Filing System (EFS) (特許出願) http://www.uspto.gov/ebc /efs/	米国特許商標庁 (USPTO)	利用 せず	サーバ認証：(不明) クライアント認証 デジタル証明書 Entrust 社 PKI 使用 クライアント：専用ソフト
	Electronic Filing of Patent Transaction (特許出願) https://www.epatents.gov .sg/FormSubmission/	シンガポール特許庁	利用 する	デジタル証明書によるクライアント認証 によりアクセス許可している 模様(詳細不明)
	On-line Services (特許出願) https://pericles.ipaustr alia.gov.au/home_page/ec entre/eccs/index.cfm?fus eaction=logon	オーストラリア特許 庁 (IPAustralia)	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(1024) 共通鍵暗号：RC4(128) サーバ認証：MD5RSA GTE Corporation クライアント認証 ユーザ名・パスワード

種類	サイト	運営主体	SSL	暗号利用形態
電子申請	KIPONET (特許出願) http://www.kipo.go.kr/eh tml/eIndex.html (概要説 明)	韓国特許 (KIPO)	利用 する	共通鍵暗号： クライアント認証 デジタル証明書 (詳細不明)
	Driving Test Application (運転免許試験申込み) https://www.drivingtest. ie/drivingtest/secure/dr ivertestapplication.asp? status=new	アイルランド環境自 治省	利用 する	プロトコル：SSL (詳細不明) サーバ認証：MD5RSA Thawte Consulting cc
	ServiceArizona (運転免許更新、住所変更 など。支払も可能) https://servicearizona.i host.com/renewal/cgi-add r/addrupdate (住所変更)他	米国アリゾナ州	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(512) 共通鍵暗号：RC4(40) サーバ認証：MD5RSA VeriSign/RSA Secure Server CA
	e-OFCOM (電話番号割当申請) https://www.e-ofcom.ch/e ndb/servlets/com.eofcom. servlet.resource.Resource esServlet?lang=E	スイス連邦通信局 Federal Office of Communications (OFCOM)	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(1024) 共通鍵暗号：RC4(128) サーバ認証：sha1RSA Swisskey AG
電子調達	Defense Finance and Accounting Service https://ecweb.dfas.mil/n otes/MainPage.cfm	米国国防総省	利用 する	プロトコル：TLS 1.0 鍵交換：RSA(1024) 暗号：RC4(56) サーバ認証：sha1RSA U.S. Government (DoD)
	GeBIZ Partner http://www.gebiz.gov.sg/	シンガポール	利用 する	プロトコル：TLS 1.0 鍵交換：RSA(1024) 共通鍵暗号：RC4(128) サーバ認証：MD5RSA VeriSign Trust Network
	Ireland e-Procurement (現状、調達情報のみ) http://www.e-tenders.gov .ie/cmod/Tenders.nsf/Hom ePageEnglish	アイルランド政府	利用 する	暗号化：なし クライアント認証： 登録制(住所、氏名など)
電子納付	BillPay https://www.billpayment. co.uk/	Girobank 銀行 (政府機関・地方公 共団体・公益企業向 け納付)	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(1024) 共通鍵暗号：RC4(128) サーバ認証：MD5RSA VeriSign Trust Network クライアント認証 ユーザ番号・パスワード
	e-PAY http://www.iras.gov.sg/ ePay/Promotion.htm	シンガポール歳入庁	利用 する	プロトコル：TLS 1.0 鍵交換：RSA(1024) 共通鍵暗号：RC4(128) サーバ認証：MD5RSA VeriSign Trust Network
総合	NSF FastLane (研究提案、状況確認、等) https://www.fastlane.nsf .gov/fastlane.jsp	米国 NSF	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(1024) 共通鍵暗号：RC4(128) サーバ認証：MD5RSA RSA Data Security, Inc
	MAXI (住所変更・支払等総合サ ービス) https://www3a.maxi.com.a u/devs/Main.maxi	オーストラリア・ビ クトリア州	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(1024) 共通鍵暗号：RC4(128) サーバ認証：MD5RSA VeriSign Trust Network

種類	サイト	運営主体	SSL	暗号利用形態
その他	GSA Auction (政府物品オークション) https://www.gsaauctions.gov/index.htm	米国 GSA	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(1024) 共通鍵暗号：RC4(128) サーバ認証：MD5RSA RSA Data Security
	Statistik-Shop (統計データ販売) https://www-ec.destatis.de/	ドイツ統計庁	利用 する	プロトコル：SSL 3.0 鍵交換：RSA(1024) 共通鍵暗号：RC4(128) サーバ認証：MD5RSA Thawte Consulting cc
	SHS (Secure Messaging System) (電子政府ネットワークインフラ(構築中))	スウェーデン	利用 する	SSL, S/MIME など

(サーバ認証は、署名アルゴリズムとCA運営者を記した。)

3.4.3 セキュリティ要件

(1) 暗号標準

調査対象の国々の中で、政府機関での情報保護に用いられる暗号標準の整備・公開が確認されたのは米国、カナダ、オーストラリアの三カ国である。なお、英国には情報セキュリティ基本文書 (Manual for Protective Security) があり、また政府向け暗号開発が行われているが、公開されていない。

米国では、国立標準技術局 (NIST) の定める連邦情報処理標準 (FIPS) の中で、セキュリティ標準および暗号標準が規定されている。なお、2001年11月に AES が FIPS 197 として公布された。当面、TDES (DES は新たな調達では採用してはならない) と AES は共存し、AES への移行が緩やかに進められる。現在、NIST では、暗号化、電子署名、鍵管理等に関する FIPS 標準やガイドラインの集まりとしての包括的な「暗号ツールキット」を整備中 (<http://csrc.nist.gov/encryption/>) である。具体的には、メッセージダイジェストサイズの大きい SHA-256, SHA-384, SHA-512 を含むハッシュ関数標準 FIPS180-2 を準備中であり、共通鍵ベースを含む鍵管理標準の検討等が進められている。

カナダでは、国防省の下通信安全機構 (CSE) が政府部内向け暗号標準を定めている。オーストラリアでは、国防省の国防信号局 (DSD) が A S C I 3 3 文書の中で暗号標準を定めている。それらを表にまとめる。

(a) 米国

種類	標準	根拠となるFIPS文書			備考
		番号	タイトル	発行年	
暗号モジュール評価基準		FIPS 140-2	SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES	2001	
共通鍵暗号	DES	FIPS 46-3	DATA ENCRYPTION STANDARD (DES)	1999	新規調達での採用不可
	Triple DES	FIPS 46-3	DATA ENCRYPTION STANDARD (DES)	1999	
	AES	FIPS 197	ADVANCED ENCRYPTION STANDARD	2001	
	DES実装・利用	FIPS 74	GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION	1981	
	DES操作モード	FIPS 81	DES MODES OF OPERATION	1980	
電子署名	DSA	FIPS 186-2	DIGITAL SIGNATURE STANDARD (DSS)	2000	
	RSA	FIPS 186-2	DIGITAL SIGNATURE STANDARD (DSS)	2000	ANSI X9.31 を参照
	ECDSA	FIPS 186-2	DIGITAL SIGNATURE STANDARD (DSS)	2000	ANSI X9.62 を参照
データ認証	DAC	FIPS 113	COMPUTER DATA AUTHENTICATION	1985	
鍵移送/管理	(共通鍵ベース)	FIPS 171	KEY MANAGEMENT USING ANSI X9.17	1992	
	SHA-1	FIPS 180-1	SECURE HASH STANDARD (SHS)	1995	
鍵預託	EES(SKIPJACK)	FIPS 185	ESCROWED ENCRYPTION STANDARD	1994	
乱数生成		FIPS 186-2	DIGITAL SIGNATURE STANDARD (DSS)	2000	付録3に記述。DSA向け
自動パスワード生成	APG	FIPS 181	AUTOMATED PASSWORD GENERATOR	1993	

FIPS185 の参照している SKIPJACK は内容が機密だったが、1998年に declassify され、定義が公表された。ただし、FIPS 文書とはなっていない。

(b) カナダ

種類	標準	番号	タイトル
共通鍵暗号	TripleDES	ANSI X9.52	Triple DES Encryption Algorithm Modes of Operation specifies the acceptable methods of implementing DES
	CAST5-80	RFC2144	
	CAST5-128	RFC2144	
	SKIPJACK		SKIPJACK and KEA Algorithm Specifications
鍵交換	RSA (Rivest, Shamir, Adleman) & RW (Rabin, Williams) (modulus \geq 1024 bits)	ANSI X9.44	Key Establishment Using Factoring based Public Key Cryptography for the Financial Industry
	KEA		SKIPJACK and KEA Algorithm Specifications
	離散対数問題を元にした他のアルゴリズム (CSEの認定が必要)		
	D-H (Diffie-Hellman) and MQV (Menezes, Qu, Vanstone) (field size \geq 1024 bits, prime)	ANSI X9.42	Agreement of Symmetric Keys using Discrete Logarithm Cryptography
	Elliptic Curve Cryptography	ANSI X9.63	Public Key Cryptography for the Financial Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography
ハッシュ関数	SHA-1	X9.30-2	Secure Hash Algorithm (SHA-1) (REVISED)
電子署名	RSA (Rivest, Shamir, Adleman) & RW (Rabin, Williams) (modulus \geq 1024 bits)	ANSI X9.31	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rdsa)
	Digital Signature Algorithm (DSA)	ANSI X9.30-1	Public Key Cryptography for the Financial Services Industry: Part 1: The Digital Signature Algorithm
	有限体での累乗計算に基づく他のアルゴリズム (El-Gamal など)		
	ECDSA	ANSI X9.62	Elliptic Curve Digital Signature Algorithm

(c) オーストラリア

種類	標準	備考
電子署名	DSA (モジュラス:最低1024ビット) + SHA-1	
	RSA (モジュラス:最低1024ビット) + MD5	DSAが望ましい
共通鍵暗号	[IN-CONFIDENCE, PROTECTEDなど向け] DES (鍵長:最低56ビット)	CBCモード、CFモードのみ (ECBモードは不可)
	[IN-CONFIDENCE, PROTECTEDなど向け] DESと同等以上の強度を持つとDSDが認定したアルゴリズム (IDEA, RC4, RC5, BLOWFISH など)	現状、認定されたものなし
	[CONFIDENTIAL, SECRET, TOP SECRET向け] GFE (Government Furnished Encryption)	GFEの詳細は機密
鍵交換	RSA (モジュラス:最低1024ビット)	
	Diffie-Hellman(モジュラス:最低1024ビット)	
鍵回復	認定暗号機器は鍵回復手段を持たなければならない。	

(2) 電子政府システムのセキュリティ

電子政府システムは、行政部門の情報システムという点において、従来のセキュリティ規準の対象となるが、調査の限りでは、行政機関外部との通信については明確な規準がない。

ただし、オーストラリアでは政府機関の運営する Web サービスにおけるガイドラインが文書化されており、セキュリティに関する部分では ACSI 33 などの既存の規準を参照している。なお、DSD が Web サーバにおける SSL の使用に関する勧告文書を公表している。これによると、インターネット上で SSL を用いて通信してよいのは、sensitive だが classified でない情報であり、それらの情報の通信の際の SSL パラメータの設定は下表のように要請されている。

オーストラリア DSD 勧告における SSL パラメータ推奨設定

種類	要件
プロトコル	SSL 3.0 (SSL 2.0 は禁止)
鍵交換	RSA 1024 ビット以上
共通鍵暗号	TDES(168) (CBC モード) 又は RC4(128)
ハッシュ関数	SHA MAC 又は MD5 MAC

なお、ごく最近、米国 NIST も公共 Web サーバのセキュリティ確保に関するガイドライン (ドラフト) を公表した。

(<http://csrc.nist.gov/publications/drafts/PP-SecuringWebServers-RFC.pdf>)

英国ではより包括的な電子政府サービスのフレームワーク文書のシリーズが順次発行されつつあり、個人情報的重要度に応じた情報保護方策や認証・登録に関する規定がなされている。現時点では、具体的な暗号アルゴリズムについての規準は記されていない。

3.4.4 プロトコル、製品評価制度事例

(1) 米国とカナダ

CMVP (Cryptographic Module Validation Program) は、NIST とカナダ CSE が共同で運用している FIPS140-1 および FIPS140-2 をベースとした暗号モジュールの評価プログラムである。NIST は、民間の研究機関を評価機関として認定し、それらの機関が製品等の評価を行う制度 NVLAP (NATIONAL VOLUNTARY LABORATORY ACCREDITATION PROGRAM) を有している。暗号モジュールに評価機関による認定制度 CMVP は、NVLAP CRYPTOGRAPHIC MODULES TESTING と呼ばれる。

スキームは以下のようになっている。

- ・ NVLAP により調査機関が選定される
- ・ ベンダは、暗号モジュールを認定費用とともに、調査機関に提出する
- ・ 調査機関は認定費用を NVLAP に提出するとともにテストレポートを作成する
- ・ NVLAP は、調査機関リストを管理する
- ・ NIST と CSE は、暗号モジュールに関して FIPS140-1 (または FIPS140-2) 準拠であることを認定し、ベンダに交付する

(2) 他の国における認定制度

・ イギリス

CESG (Communications-Electronics Security Group) が、イギリス政府開発の暗号アルゴリズムである Thames Bridge と Red Pike について、製品の認定を行っている。

・ フランス

DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) が、他の機関を認定し、その機関が暗号製品の評価および認証を行っている。DCSSI は、ITSEC に準拠した暗号製品評価プロフィールを作成している。

・ ドイツ

BSI (Bundesamt für Sicherheit in der Informationstechnik) によって許可された評価機関が、暗号製品の認定を行っている。対象は、ドイツ政府で利用する暗号製品である。

3.4.5 まとめ

(1) 政府の暗号政策の対象領域

政府の暗号政策の対象領域は、

- (a) 国家安全(軍事、外交)における機密保護・機密解読のための暗号技術使用
- (b) 一般行政機関における機密保護のための暗号技術使用
- (c) 民間・一般社会における暗号技術使用

の三つがある。

今回の海外調査は、二番目の領域を対象としたものである。当領域では、行政部門の情報化に伴って情報保護が問題となり、米国では 1977 年に DES が定められている。従来、行政部門内の情報システムは行政機関内(ないし、行政機関間)に閉じた存在であり、行政機関を拘束する規則により、情報保護が達成されていた。ところが、行政サービスを電子的に提供することが目的の電子政府システムでは、行政機関の管理の届かない部分(特にインターネット)における情報セキュリティが問題となるという点が新しい。この新しい領域は、組織内の規則が及ぶ範囲を越えること、多くの利用者を得るためには、普及している Web ブラウザ

などの技術に依存しなければならないこと、といった困難があり、現時点では試行錯誤的に行っているように思われる。オーストラリア、英国では、電子政府サービスでの情報セキュリティは、電子政府推進機関と暗号専門機関のいずれか、または両方が協調して定めており、それが自然なあり方であろう。

(2) 暗号専門機関とセキュリティ標準

電子政府向けに限らないが、米国、カナダ、英国、オーストラリアなどには、政府標準暗号を制定する権限を有する暗号専門機関がある。

例えば、米国の FIPS 標準は、公布から発効までの移行期間があり、移行期間終了後は、新しい標準に適合した調達をすることが義務づけられている。ただし、既存システムの使用は継続でき、また、標準準拠が不都合な場合の救済策としての適用除外手続きが規定されている。FIPS 標準は 5 年毎など定期的に見直され、不要になったものは廃止され、必要に応じて一つの標準の新しい版や新たな標準が定められる。なお、NIST の鍵管理ワークショップでは、鍵管理ガイドラインを準備中であり、そのドラフト ([http://csrc.nist.gov/encryption/kms/key-management-guideline-\(workshop\).pdf](http://csrc.nist.gov/encryption/kms/key-management-guideline-(workshop).pdf)) では 2015 年までのデータ保護に

使用できる推奨暗号アルゴリズムと鍵長、及び、2016 年以降までデータ保護が必要な場合の推奨暗号アルゴリズムと鍵長を示している。

第4章 電子政府システムにおける暗号技術利用の要件

要件調査WGでは、電子政府システムにおける暗号技術利用の要件について、ヒアリングおよびアンケート調査を行った。今回、分析の対象とした電子政府システムは、電子申請、電子調達、電子納付、電子情報提供、政府認証基盤、の5つである。以下では、各システムにおけるモデルと処理フロー、想定される暗号技術利用の要件について、システム毎に整理を行った。もとより、これらのシステムはまだ設計・構想段階のものが少なくなく、詳細要件が未定となっているシステムもあるほか、関連する幾つかのシステムを統合して整理している部分もある。このため、以下の記述のうち、特に暗号技術利用の具体的な要件の内容については、関連する電子政府システムにおいて想定される一例を示したものとなっている。

4.1 電子政府のシステム別モデル

今回、ヒアリングおよびアンケート調査の結果に基づいて、分析対象とした電子政府システムにおける暗号技術利用状況をモデル化すると、大きく分けて2種類のモデルが存在することが分かる。ひとつは、一般国民・民間企業など、不特定多数と行政機関等が情報を授受するGtoCモデル、もうひとつは、特定業界の企業など、比較的限定された相手と行政機関が情報を授受するGtoBモデルである。電子申請、電子情報提供を始め、多くの電子政府システムはGtoCに該当し、電子調達（受注者 - 政府機関間）および電子納付（金融機関 - 政府機関間）の一部はGtoBと分類できる。このように分類することで、電子政府システムにおける暗号技術利用の特徴について、大きな傾向を掴むことができる。

この各々のモデルにおいて利用される暗号技術についてみると、基本的に、GtoCモデルは、SSLによるデータ秘匿に代表される、予め利用者のパソコンに組み込まれた技術を利用する「thin client 指向」である一方、GtoBモデルは、独自プログラムや閉域ネットワークを利用するなど、「作り込み指向」であることが分かる。しかし、GtoCにおいてもthin clientでは実現できない要件（特に、電子署名）が要求される場合、ある程度の作り込みが必要となるため、利用者に負担を掛けずに追加的な暗号技術を実装するための方法が課題となっている。こうした暗号利用形態の違いを図式化すれば、次のようになる。

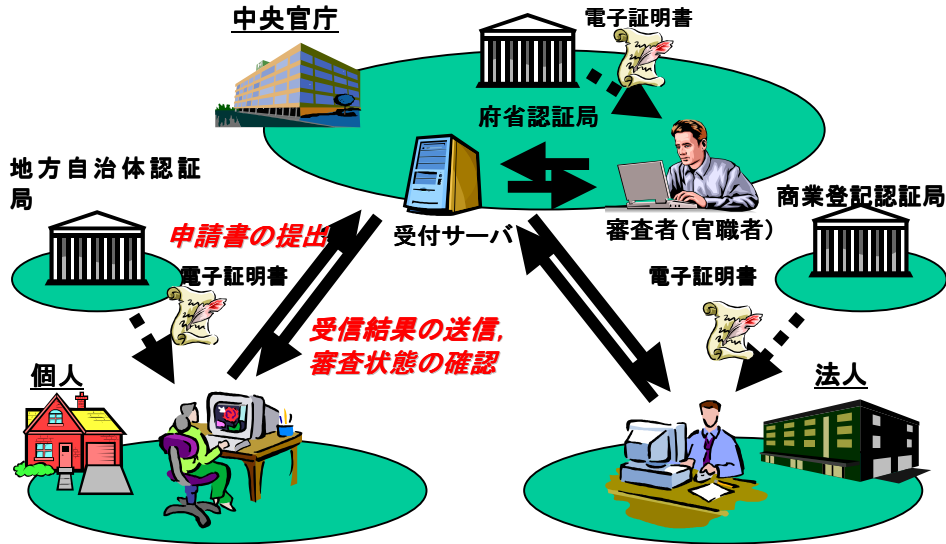
	予め組み込まれた技術	独自にシステムに組み込む技術
GtoC モデル (電子申請、 電子情報提供)	SSLによるデータ秘匿 パスワード認証	電子署名によるデータ保全
GtoB モデル (電子調達、 電子納付)		電子署名によるデータ保全 ICカードによる秘密鍵の格納 IP-VPNの利用・IPsec対応ルーターの利用によるデータ秘匿・データ保全 作り込み通信暗号によるデータ秘匿・相手認証

4.1.1 電子申請システム

(1) 電子申請システムのモデル

電子申請システムとは、個人並びに法人が中央官庁に対して行っている現行の申請・届出手続きを、インターネットのようなオープンなネットワークを介して電子的に行うことができるようにするものである。

電子政府における電子申請システムのモデル図を以下に示す。

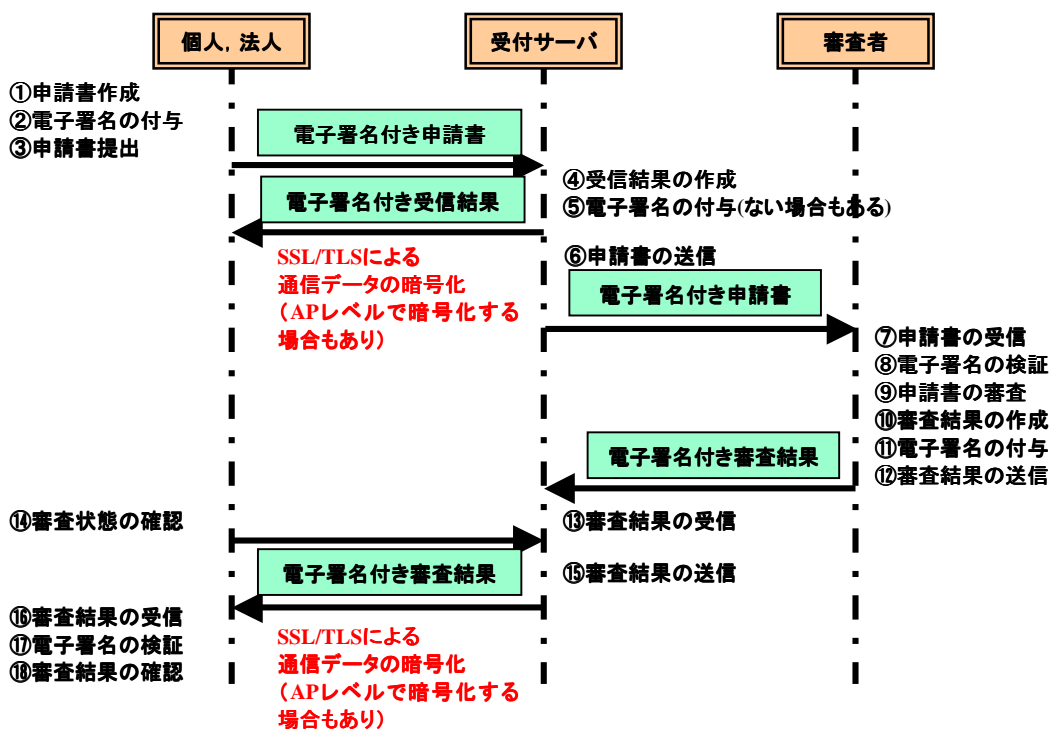


(2) 処理フローモデル

電子申請システムにおける処理は、

1. 個人/法人が申請書を作成し、受付サーバに提出するフェーズ
2. 提出された申請書を審査者が審査(受理/却下)するフェーズ
3. 個人/法人が審査結果を確認するフェーズ

といった3つのフェーズによって構成される。処理フローを以下に示す。



(3) 想定される電子申請システムの暗号要件

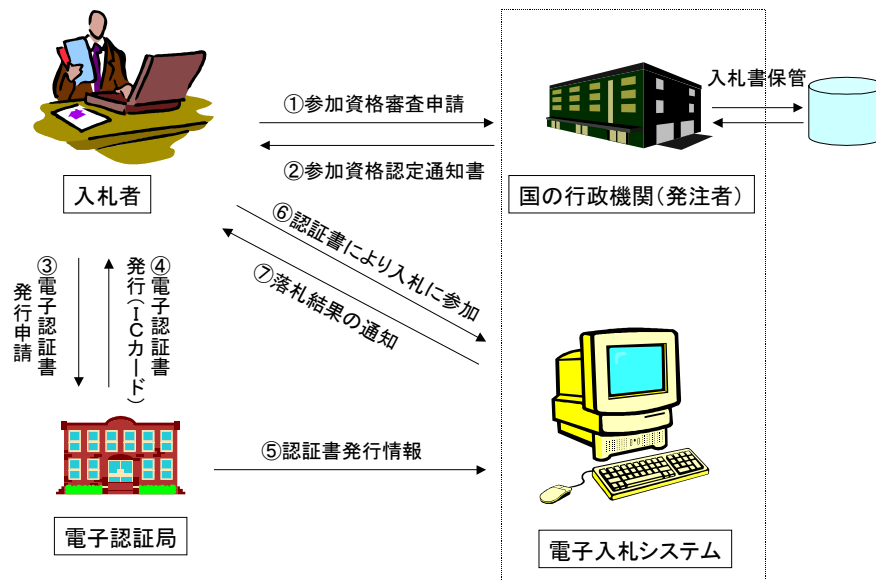
【利用形態毎 / 整理項目毎の分類表】

利用形態		整理項目	システム概要			要件		
			(1)データ内容	(2)データサイズ	(3)回線速度	(4)現在利用している暗号処理速度	(5)現在利用している暗号強度	(6)その他
(ア) <利用者側> 認証			申請書	数MB	-	人間が気にならない程度	RSA(1024)相当 (近年中に2048bit相当へv.up要)	
利用者 政府 (申請書の提出)	(イ) 鍵共有	鍵情報	SSLの場合 RSA使用時は 46バイト	インターネット	人間が気にならない程度	RSA(1024)相当 (近年中に2048bit相当へv.up要)		
	(ウ) 守秘	申請書	数MB		人間が気にならない程度	TDES, AES相当	SSL等の プロトコル 標準に 入っている こと	
	(エ) 完全性保証				(ア)で対応	-	-	
	(オ) 否認防止							
政府 利用者 (受信結果の送信)	(カ) 鍵共有	鍵情報	SSLの場合 RSA使用時は 46バイト	人間が気にならない程度	RSA(1024)相当 (近年中に2048bit相当へv.up要)			
	(キ) 守秘	受信結果 審査状態確認	数kB	人間が気にならない程度	TDES, AES相当	SSL等の プロトコル 標準に 入っている こと		
	(ク) 完全性保証			(コ)で対応	-	-		
	(ケ) 否認防止							
(コ) <政府側> 認証			受信結果 審査状態確認	数kB	-	人間が気にならない程度	RSA(1024)相当 (近年中に2048bit相当へv.up要)	
<政府側> データ保管	(サ) 守秘	申請書	数MB (システム毎に 保管期間は異なる)	-	処理速度が速い 必要は無い	なし (非公開情報なら は必要)	-	
	(シ) 完全性保証							
	(ス) 否認防止							

4.1.2 電子調達システム

(1) 電子調達システムのモデル

電子調達システムとは、中央官庁が行っている調達業務のうち、入札参加申請、入開札、落札者通知を、インターネットを介して電子的に行うことが出来るようにしたシステムである。

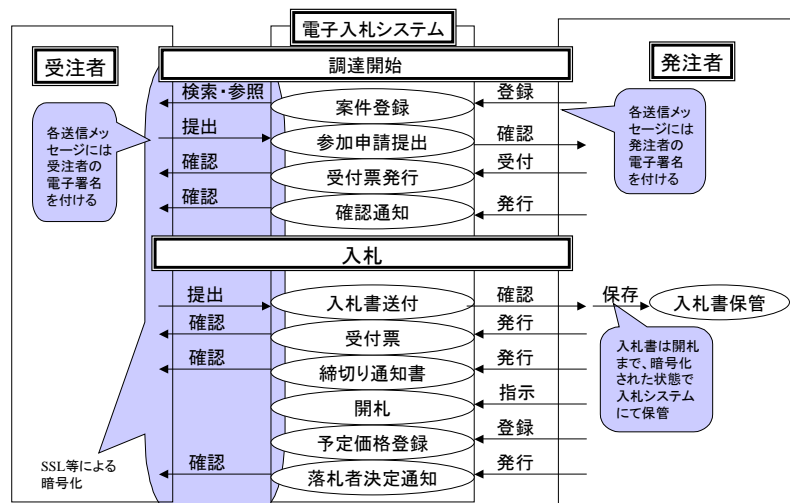


(2) 処理フローモデル

電子調達システムにおける処理は、以下の各フェーズにより構成される。

1. 入札参加資格の申請 / 審査 / 認定通知
2. 入札書の提出 / 保管
3. 開札及び落札結果通知

【システムの処理フロー図】



(3) 想定される電子調達システムの暗号要件

【利用形態毎 / 整理項目毎の分類表】

利用形態		整理項目	システム概要			要件		
			(1)データ内容	(2)データサイズ	(3)回線速度	(4)現在利用している暗号処理速度	(5)現在利用している暗号強度	(6)その他
		(ア) <利用者側> 認証	-	-	-	ユーザが気にならない程度	RSA(1024)相当	-
利用者 政府 (申請書の提出)	(イ) 鍵共有	鍵情報	SSL の場合 RSA 使用時は 46 バイト	ISDN: 128kbps LAN: 10Mbps	ユーザが気にならない程度	RSA(1024)相当	-	
	(ウ) 守秘	・参加申請データ (業者参加申請に関するデータ) ・入札書データ (入札金額など)	数百 B ~ 1 MB	ISDN: 128kbps LAN: 10Mbps	ユーザが気にならない程度	RC2(128)相当	SSL 等のプロトコル標準に入っていること	
	(エ) 完全性保証	・参加申請データ (業者参加申請に関するデータ) ・入札書データ (入札金額など)	数百 B ~ 1 MB	ISDN: 128kbps LAN: 10Mbps	(ア) に対応	RSA(1024) SHA-1 相当	-	
	(オ) 否認防止							
政府 利用者 (受信結果の送信)	(カ) 鍵共有	鍵情報	SSL の場合 RSA 使用時は 46 バイト	ISDN: 128kbps LAN: 10Mbps	ユーザが気にならない程度	RSA(1024)相当	-	
	(キ) 守秘	-	-	ISDN: 128kbps LAN: 10Mbps	ユーザが気にならない程度	RC2(128)相当	SSL 等のプロトコル標準に入っていること	
	(ク) 完全性保証	-	-	ISDN: 128kbps LAN: 10Mbps	(コ) に対応	RSA(1024) SHA-1 相当	-	
	(ケ) 否認防止							
		(コ) <政府側> 認証	-	-	-	ユーザが気にならない程度	RSA(1024)相当	-
<政府側> データ保管	(サ) 守秘	・入札書データ (開札までの保管)	数百 B ~ 1 MB	-	サーバでの ソフト処理で十分	-	-	
	(シ) 完全性保証	・入札書データ (開札までの保管)	数百 B ~ 1 MB	-		-	-	
	(ス) 否認防止							
		CA 公開鍵証明書	ユーザ公開鍵の 証明書	-	-	-	RSA(1024) SHA-1 相当	-

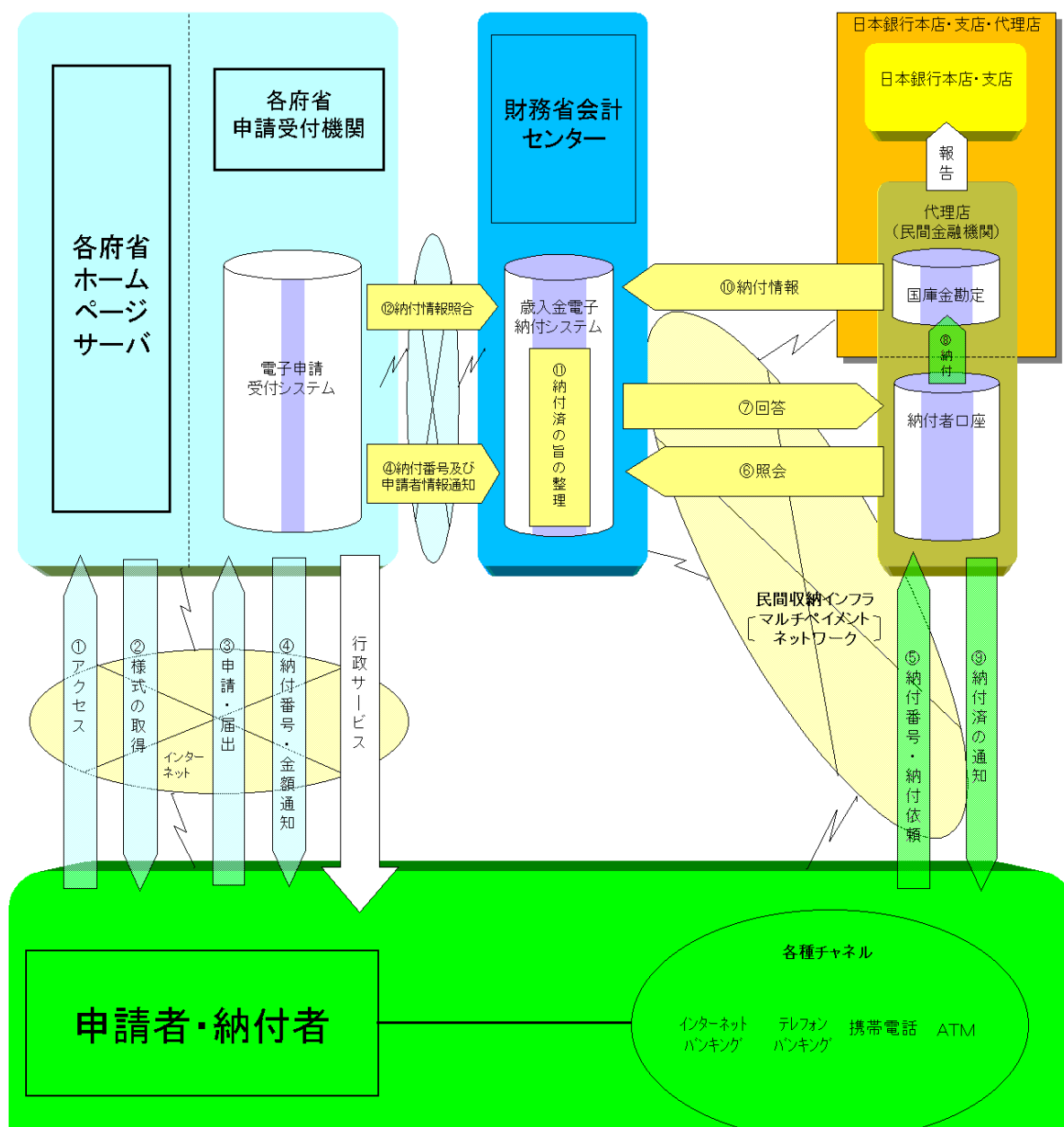
4.1.3 電子納付システム

(1) 電子納付システムのモデル

電子納付システムとは、個人ならびに法人が中央官庁に対して行っている現行の税金や行政手数料等の納付業務を、インターネットのようなオープンなネットワークを介して電子的に行うことができるようにするものである。

電子政府における電子収納システムのモデル図を以下に示す。

国庫会計事務電子化後イメージ図(行政手数料)



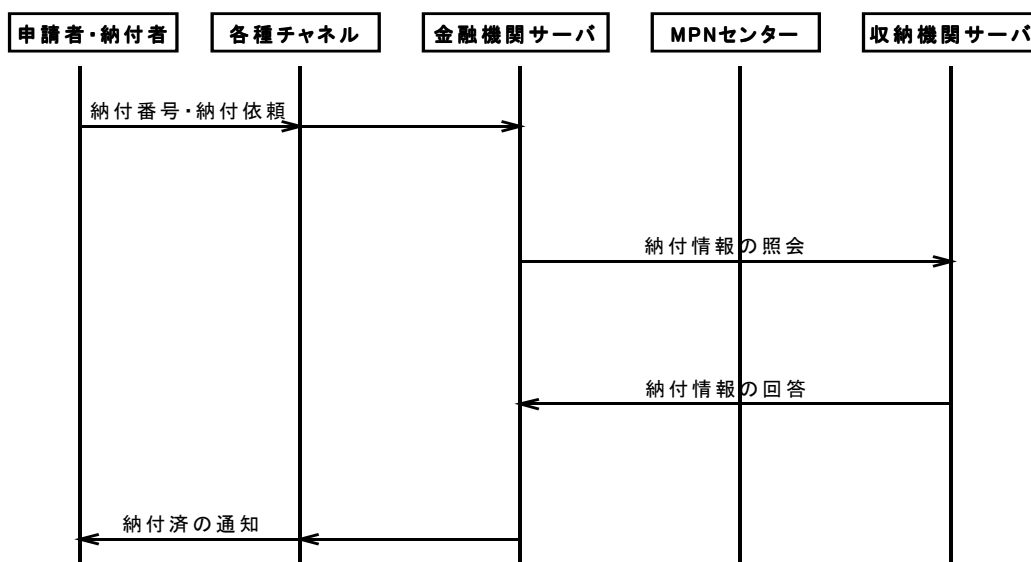
出典 : <http://www.kantei.go.jp/jp/it/network/dai3/3siryous3.html>

(2) 処理フロー・モデル

電子納付システムは、行政サービス等を提供する各府省側のシステムと、申請者・納付者が国庫金を納付するための金融機関側のシステムとを連結することによって機能するものである。その処理フローは、連動するシステムの作りに依存する部分もあるが、基本的には、金融機関側から送られてきた納付情報を、各府省（収納機関）側のシステムに配信する作りとなる。処理フローは、

- 1．申請者・納付者が、金融機関に納付番号・金額を依頼するフェーズ
- 2．金融機関が、収納機関に納付情報を照会し、その回答を受け取るフェーズ
- 3．金融機関が、申請者・納付者に納付済の通知を行うフェーズ

の3つのフェーズによって構成される。このうち、1および3のフェーズは、金融機関が主体となってサービスを提供する一方、2のフェーズについては、金融機関と政府のシステム間の連動処理となる。各フェーズの処理フローを以下に示す。



(3) 想定される電子納付システムの暗号要件

上記3フェーズのうち、2のフェーズにおいて、政府のシステムと民間のシステムとの連動を行うネットワークにおいて要請されている暗号要件は、以下のとおりである。なお、1および3のフェーズについては、金融機関が顧客に提供するサービスで採用している暗号要件であり、その内容も金融機関によって区々であるため、「参考」として表記した。

【利用形態毎 / 整理項目毎の分類表】

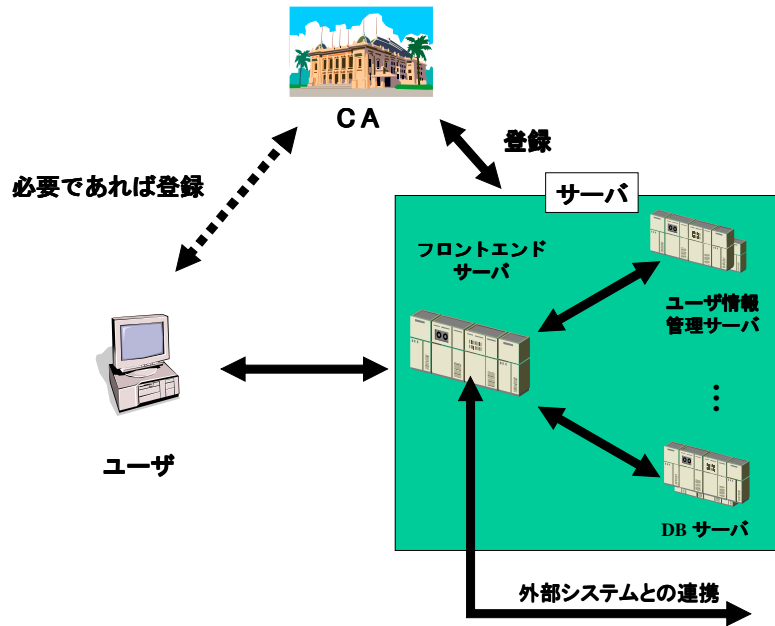
整理項目 利用形態	システム概要			要件		
	(1)データ内容	(2)データサイズ	(3)回線速度	(4)現在利用している暗号処理速度	(5)現在利用している暗号強度	(6)その他
<金融機関 = MPN センター間> 納付情報の照会	数値、文字	1 件 当 り 100 byte 程度	512Kbps 程度	IPsec 対応ルータ を利用	TDES(168bit,3キー) Diffie-Hellman (1024bit)	
<収納機関(政府含む) = MPN センター間> 納付情報の回答	数値、文字	100 byte ~ 数 KB 程度	512Kbps 程度	IPsec 対応ルータ を利用	TDES (168bit,3キー) Diffie-Hellman (1024bit)	
(参考) <利用者=金融機関間> 納付番号・納付依頼の 入力、納付済の通知等	数値、文字 (納付情報等の プライバシー データ、 暗証番号等を 含む)	1 件 当 り 100 byte 程度	利用者 の環 境に よ り区 々。 数 Kbps ~ 数 Mbps	PC 程度	利用者が利用する金 融機関等のサービス 内容により区々。 多くの場合、SSL V3.0 (RC4 128bit, RSA 1024bit) が利用され ている。	

4.1.4 電子情報提供システム

(1) 電子情報提供システムのモデル

電子情報提供システムとは、個人並びに法人が中央官庁により提供されている情報に、インターネットのようなオープンなネットワークを介して電子的にアクセスすることができるようにするものである。他のシステムに比べると、公開情報を扱うことが多いこともあり、暗号に対する要件はそれほど強くないと考えられる。電子図書館などでは著作権料の支払が必要な情報もあるため、流通する情報を保護する必要も考えなければならない。

電子政府における電子情報提供システムのモデル図を以下に示す。

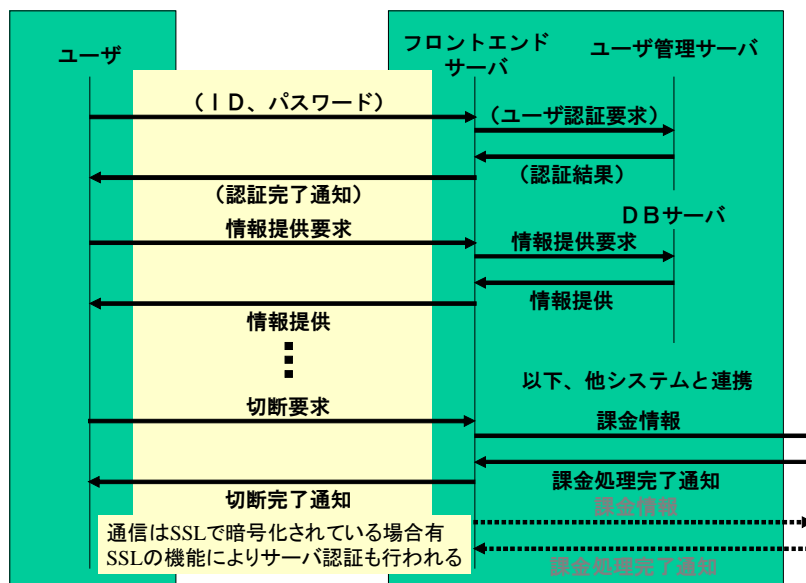


(2) 処理フローモデル

電子情報提供システムにおける処理は、

- 0. 個人/法人が前もって利用者登録をするフェーズ (無い場合もあり)
- 1. 個人/法人が情報を要求し、システムがそれを提供するフェーズ
- 2. 外部システムと連携する等、決済処理を行うフェーズ

といった3つのフェーズによって構成される。処理フローモデル(例)を以下に示す。



(3) 想定される電子情報提供システムの暗号要件

【利用形態毎 / 整理項目毎の分類表】

利用形態	整理項目	システム概要			要件		
		(1)データ内容	(2)データサイズ	(3)回線速度	(4)現在利用している暗号処理速度	(5)現在利用している暗号強度	(6)その他
	(ア) <利用者側> 認証	SSL 等の暗号化通信路上でのパスワード	数 B	インターネット	ユーザが気にならない程度	推測できない程度	-
利用者 政府 (データの要求)	(イ) 鍵共有	鍵情報	SSL の場合 RSA 使用時は 46 バイト		ユーザが気にならない程度	RSA(1024)相当	-
	(ウ) 守秘	要求データの情報	~ 数 KB		ユーザが気にならない程度	RC2(128)程度で十分	SSL 等のプロトコル標準に入っていること
	(エ) 完全性保証	-	-		-	-	-
	(オ) 否認防止	-	-		-	-	-
政府 利用者 (要求データの送信)	(カ) 鍵共有	鍵情報	SSL の場合 RSA 使用時は 46 バイト		ユーザが気にならない程度	RSA(1024)相当	-
	(キ) 守秘	要求データ	~ 数十 MB		ユーザが気にならない程度	RC2(128)程度で十分	SSL 等のプロトコル標準に入っていること
	(ク) 完全性保証	-	-		-	-	-
	(ケ) 否認防止	-	-		-	-	-
	(コ) <政府側> 認証	SSL 等のサーバ認証	数百 KB		ユーザが気にならない程度	RSA(1024)相当	-
<政府側> データ保管	(サ) 守秘	-	-	-	-	-	
	(シ) 完全性保証	提供する電子情報	数 MB ~ 数 TB	-	ユーザが気にならない程度	-	-
	(ス) 否認防止					-	-

4.1.5 政府認証基盤

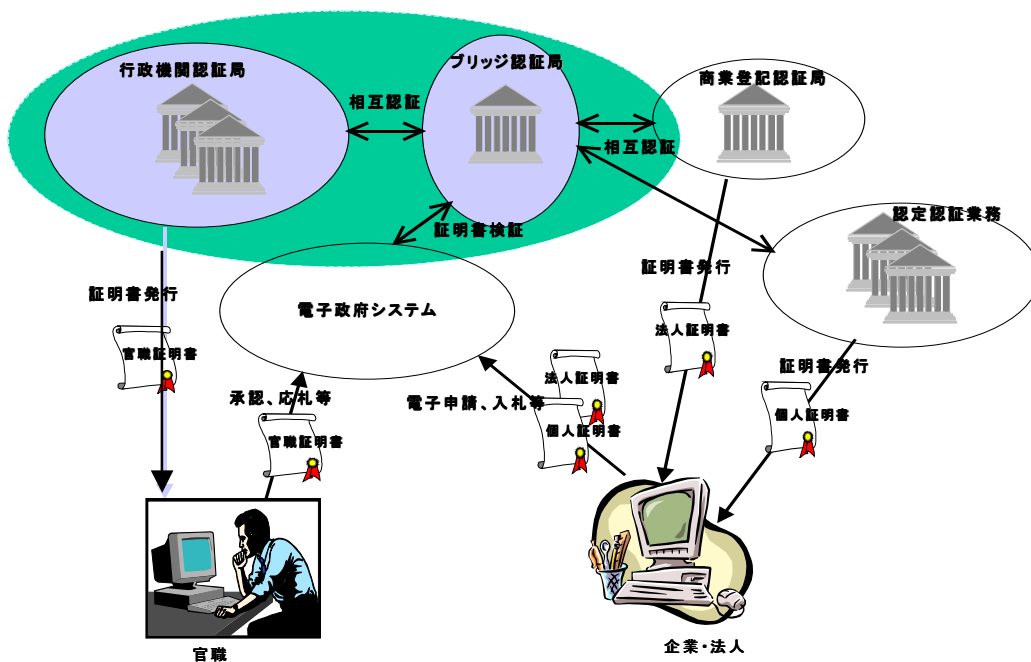
(1) 政府認証基盤のシステム構成

政府認証基盤は、官職、企業、法人、個人等の電子政府システム利用者の本人認証や申請、届出等の情報の真正性を確保する等のために用いられる公開鍵暗号方式をベースにした電子認証システムである。

政府認証基盤における電子証明書利用者の登録、電子証明書発行を行う認証機関としては、官職に電子証明書を発行する各省庁の認証局と各省庁認証局間の相互認証を行うためのブリッジ認証局が規定されている。但し、電子政府システムによる電子申請、届出等の業務の民間利用のために、商業登記簿制度に基づき企業、法人に電子証明書を発行する商業登記認証局、電子署名法に定める認定を得た自然人に電子証明書を発行する民間の認定認証局が、ブリッジ認証局を経由して政府認証基盤に接続することを可能としている。

商業登記認証局および民間の認定認証局を含めると、政府認証基盤における電子証明書の利用者、検証者としては、電子申請、届出等の処分権限者である官職および電子申請、届出等を行う企業、法人、自然人が対象となる。

政府認証基盤のシステム構成イメージを下図に示す。



(2) 政府認証基盤における各認証局の役割

省庁認証局

各種行政手続の処分権限者である官職からの電子証明書発行要求を受けて、その身元の識別、認証を行った上で、政府認証基盤で規定されている様式に沿った電子証明書を作成し、当該官職に送付する。

官職の変更が生じた場合、官職の所有する秘密鍵が漏洩、盗難等による危殆化もしくはその恐れが生じた場合等には、官職からの要求に応じて電子証明書を失効して、電子証明書の有効性を検証するための情報としてリポジトリに登録し、検証者の求めに応ずる。

また、上記官職への電子証明書の発行、失効情報への署名およびブリッジ認証局との相互認証証明書への署名等に用いる秘密鍵と証明書の検証等に用いる公開鍵のペア生成とそれらの厳重なライフサイクル管理を行う

ブリッジ認証局

省庁認証局と同様に、秘密鍵と公開鍵ペアを作成し、それらのライフサイクル管理を行う。

各省庁認証局、商業登記認証局および民間の認定認証局との間の相互認証を行うための相互認証証明書を作成し、各認証局と交換すると共にブリッジ認証局のリポジトリにそれら相互認証証明書を登録する。

他の認証局への相互認証書の発行に用いた秘密鍵が危殆化もしくはその恐れが生じた場合、政府認証基盤の相互運用性仕様との相違があった場合等においては、相互認証証明書を失効し、失効に関する情報をブリッジ認証局のリポジトリに登録する。

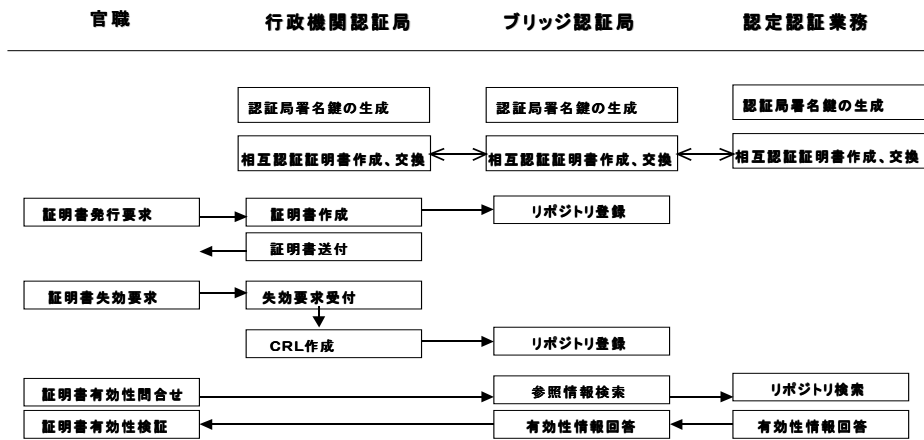
また、ブリッジ認証局には電子証明書を検証するシステムがあり、官職が電子申請、届出を行う申請者の電子証明書の有効性確認を行う事ができる。電子申請、届出を行う申請者による官職証明書の有効性確認は、統合リポジトリにある情報によって行える。

商業登記認証局、民間の認定認証局

商業登記認証局は、商業登記簿制度に基づいて電子証明書の発行を求める企業、法人に対して電子証明書を発行し、民間の認定認証局は電子署名法および政府認証基盤の規定に従って、電子政府システムにおける電子申請、届出等に使用する電子証明書を発行する。

また、それぞれの認証局は各認証局に求められる公開鍵ペアの生成から廃棄までに至るライフサイクル管理を実施すると共に、それぞれの基準に従って発行した電子証明書を失効する。

(3) 処理フローモデル



(4) 政府認証基盤におけるシステム要件

			現在利用されている暗号		署名アルゴリズム
			アルゴリズム	鍵長	
電子署名	認証局の鍵	ブリッジCA	RSA	2048ビット	①SHA1withRSAencryption もしくは ②MD5withRSAencryption ただし、新規発行は①とする
		省庁CA		2048ビット	
		民間CA		1024ビット以上	
	利用者の鍵	官職	RSA	1024ビット以上	
申請者					
TLSの認証	公開鍵	サーバ、クライアント	RSA	1024ビット以上	_____
		共通鍵	注	TDES	
				RC4	

注：掲載したアルゴリズム、ビット長は例であり、実際の適用はサーバ、クライアント間で相互に認識可能なものの中から最強なものを選択する

4.2 電子政府システムにおける暗号利用形態

本節では、4.1節で作成した電子政府システムとその処理フローのモデルに基づき、電子政府システムのメーカーおよびベンダーの意見を参考にしつつ、電子政府システムに共通の暗号利用形態（暗号の利用目的）を決定する。一方、暗号技術は公開鍵暗号、秘密鍵暗号などの一般的な分類がある。本節では導出した各暗号利用形態とそこで用いられる暗号技術との対応を明らかにする。

4.1節で検討した複数の電子政府システムの利用形態は、利用者および政府側の認証、利用者から政府への、および政府から利用者へのデータ転送における、鍵共有、守秘、完全性認証、否認防止、および政府側のデータ保管における守秘、完全性保証、否認防止となっているのでこれらをベースとすることが望ましい。

一方、暗号技術利用の要件を策定するための利用形態としては、簡潔で一般的な表現が望ましいので次のような点を考慮する。

- ・ 認証は相手認証であることを明示する。
- ・ 利用者と政府の間のデータ転送の向きにかかわらず「通信」として同じに扱う。
- ・ 完全性保証と否認防止を包括的に署名と表現する。
- ・ データ保管に対する強い要求がないので「通信」の利用形態と「保管」の利用形態を同じに扱う。
- ・ それぞれの項目に簡単な定義を記載する。

以上の観点を考慮して電子政府システムの暗号利用形態として次の分類表が得られる。

	定義
相手認証	被認証者の正当性を検証者が確認する機能
鍵共有	電子政府システムにおいて公開の通信路を用いて共通鍵暗号技術を利用する際に送信者と受信者の間で鍵情報を共有する機能
守秘	電子政府システムにおいて公開の通信路または記録媒体を介して正当な利用者以外には知られないように電子情報を共有する機能
署名	電子情報の正当性を確認する機能。署名作成者の確認機能と電子情報自体の改ざんの有無の確認機能の両方を意味する。

この分類表における暗号の利用形態のために暗号技術が組み合わせられて用いられる。暗号評価委員会においては暗号技術を公開鍵暗号、共通鍵暗号、ハッシュ関数、擬似乱数生成に分け、公開鍵暗号はさらに守秘、認証、署名、鍵共有に分類し、共通鍵暗号を64ビット鍵、128ビット鍵、ストリーム暗号に分けている。それぞれの暗号利用形態において用いられる代表的な暗号技術は次図のように表される。

技術 分類 暗号の 利用形態	公開鍵暗号				共通鍵暗号		その他		
	認証	鍵共有	守秘	署名	ブロック暗号		ストリーム暗号	ハッシュ関数	擬似乱数生成
					64ビット	128ビット			
相手認証								**	
鍵共有									
守秘									
署名					*	*			

* MAC を想定

** キードハッシュ関数を想定

4.3 暗号技術に求められる要件

4.3.1 電子政府システムにおける一般的要件

3.1 節に記述したように、官庁の担当者などへのヒアリングによって得られた要件に関する主要な知見は、以下のとおりである。

- (1) クライアント側ソフトは、電子入札のように企業で利用する場合を除いて、商用OSなどに組み込まれたSSLなどの既存ソフトを用いている。従って、プロトコル標準に組みこまれ、一般の人が使う有力メーカーのソフト製品の中に入っていることが、大きな要件の一つになっている事が分かる。
- (2) 暗号処理速度やハッシュ関数の処理速度については、高速化の要求は特に出なかった。現状の暗号の性能で問題ない範囲でシステム設計していることもあると考えられる。
- (3) 公開鍵暗号はRSAの1024ビット、2048ビット鍵長、ハッシュ関数はSHA-1が大部分であり、共通鍵暗号についてはRC2、RC4、DEFS、TDESの利用が多かった。比較的保守的な判断が多いが、RSAの512ビットやRC2、RC4の40ビット鍵長と言うのはほとんど無かった。安全性にも一応の配慮をしている事であると考えられる。

一方、企業の技術者などへのアンケートによって得られた要件に関する知見は3.2節に示す通りであり、以下のように要約できる。

- (1) 安全性(暗号強度)が最高のプライオリティであると答えている人が最も多い。
- (2) また、処理速度やサイズなどの実装性や、暗号標準になっているかどうかを重視する人も多い。

このようなことを踏まえ、要件調査WGとして満たすべきであると考え、電子政府利用暗号における一般的要件を以下に記述する。

- (1) 暗号強度が十分高い。

10年間電子政府システムで安心して使えること。ここで10年としたのは以下のような理由による。

- ・システムの置き換え周期が4～5年であり、そのシステムが完全に置き換わるまでに、もう1周期かかることから、最低でも10年は安心して使いたいという要望があること。
- ・供給者としては、コンピュータ性能の向上や解読手法の出現等により、非常に長期間にわたって安全性を保証することが困難であり、非常に長期間にわたる安全性を考慮して暗号を選択しようとする、調達コストの上昇を招く可能性があること。

- (2) 一般に使われる商用ソフトにあらかじめ入っているか、入る可能性の高いものが選ばれること。

広く国民との間でやりとりを行うシステムにおいては、クライアント側でのインストールを必要としないか、最小限のインストールで済むなど、ユーザに負担を掛けない方が望ましいことから、一般に使われる商用ソフトに予め入っているか、入る可能性の高いものが最低限1つは選ばれること。

その他、処理速度が速く、ICカードへの実装性に優れている事や、何らかの暗号標準又はプロトコル標準になっている事も望ましい。

4.3.2 暗号の利用形態別要件

4.2で述べた通り、暗号の利用形態としては次の4つに分類できると考えている。

- (1) 相手認証
- (2) 鍵共有
- (3) 守秘
- (4) 署名

いずれの場合も、一般的要件と同様に、そこで使う暗号は次のような要件を満たす事が望ましい。

- (a) 暗号強度が十分高い。
- (b) 一般に使われる商用ソフトにあらかじめ入っているか、入る可能性の高いものが選ばれること。

特に、署名の場合は、署名した文書が有効とされる期間安全でなければならないと言う特徴があり、暗号の使用期間（想定起点となる時から、安心して暗号化を行える期間）+ 有効期間（暗号化を行った後、破られない期間）の暗号強度を要求される。

また、ICカードシステムでは実装上、よりパフォーマンスの劣るハードウェアでも有効に機能する暗号アルゴリズムのニーズがある、という個別の要件も得た。

第5章 電子政府における暗号利用に関する提言等

5.1 推奨暗号の数に関する考察

推奨暗号の数については、以下のような3つの選択肢があると考えられる。

- (a) 分類別に1つに絞り込む
- (b) 分類別に複数個(2 - 3個)に絞り込む
- (c) 分類別に基準をクリアしたものを全てリストアップする

ちなみに、官庁の担当者へのヒアリング結果では、推奨暗号を1つに絞り込むべきであるという意見はなく、(c)の方式で良いという意見が多かった。また、アンケート結果では(b)という意見が多く、(c)の方式で良いという意見もあった。

これらの結果を踏まえ、要件調査WGとしても3回にわたる会議で検討を実施した。ここでの検討において、次のような評価指標を考えた。

- 指標1：社会的混乱が生じないか
- 指標2：省庁の調達者が判断に困らないか
- 指標3：電子政府システムのユーザ(官庁職員、企業社員、住民)が困らないか
- 指標4：CRYPTRECで公正な選出が困難でないか

(a)の分類別に1つに絞り込む方式は、他システムとの接続性がよいことが期待できる。また、他に問題が無ければ、暗号の選定に調達者は悩む必要がない。一方、その暗号がブレイクした場合のリスクが大きく、社会的混乱をきたす可能性が強いという大きな問題がある。また、米国等の推奨暗号と異なる場合やシステム稼働時点で市販のソフトにその暗号が入っていない場合には、調達者は各種の関連ソフトの開発や配布が必要となり、ユーザはそれらのソフトのインストールが不可欠となる。したがって、運用上、調達者やユーザが困る事になる。さらに、CRYPTRECで1つを選ぶのは非常に難しい。したがって、この方式は適当とは言えない。

残る(b)と(c)の長所・欠点は以下のように整理できる。

(b) 分類別に複数個に絞り込む

<長所>

- (イ) 各省庁の担当者は選択に比較的自由度があり、また、他システムとの接続性が比較的良好なことが期待できる。
- (ロ) たとえ1つの暗号がブレイクされても代替暗号が残る。

< 欠点 >

- (イ) 米国等の推奨暗号と異なる場合やシステム稼働時点で市販のソフトにそれらの暗号が入っていない場合には社会的に混乱し、調達者やユーザが困ることになる。
- (ロ) 定量的な基準が明確でない中で、CRYPTRECで色々な要因を考えつつ推奨暗号を選択せざるを得ず、困難が予想される。

(c) 目的別に基準をクリアしたものを全てリストアップする

< 長所 >

- (イ) 調達者は選択に自由度があり、かつ、一定の安心感が得られる。
- (ロ) CRYPTRECは基準をクリアしているかどうか評価するだけでよいので、判断が比較的容易。
- (ハ) たとえ1つの暗号がブレイクされても代替暗号が残る。

< 欠点 >

- (イ) 調達者は、自由度がありすぎて選択に迷う可能性がある。また、全ての暗号に対応しようとする、サーバ側の暗号ソフトの開発コストが高くなる可能性がある。
- (ロ) ユーザ側は複数のシステムを利用する際、クライアントに多くの暗号ソフトをインストールすることが必要となる可能性があり、コストの上昇が生じる可能性がある。

このように(b)と(c)とは互いに絶対的な差がないが、要件調査WGとしては、以下のような理由により(c)を採用すべきであるという結論になった。

- (イ) CRYPTRECの当初の目的は、電子政府システムにおいて、安全性などの面で問題のある暗号を選択しないようにすることであった。この目的は(c)の方式によって十分達成される。
- (ロ) 目的別に基準をクリアしたものを全てリストアップする場合は、確かに、調達者は、自由度がありすぎて選択に迷う可能性があり、全ての暗号に対応しようとする、暗号ソフトの開発コストが高くなる可能性がある。しかし現実にはマーケットが絞り込みを行い、その時々で選択しうる数にまで絞り込まれている可能性が強い。それらと、CRYPTRECによりリストアップされた推奨暗号の両方に入っている物を採れば良いので判断に迷う事は少ない。また、すべてを実装しなくても、異なる暗号システム間の変換だけを行えば良いので、開発コストの上昇は避けられる。
- (ハ) クライアント側は、商用ソフトで用意されていない物は実質的に採用されず、そこに入っている物から選択すればよいので、コストの上昇は避けられる。

一方、(b)にする際のメリットは(c)のメリットとどちらが大きいとも言えず、しかも、定量的な基準が明確でない中で、CRYPTRECで分類別に推奨暗号を2～3個に絞り込む過程を外部に納得してもらえる形で公正に行うのは非常に難しい。したがって、積極的に(b)を提案するのは適切と考えにくい。

5.2 その他の提案

(1) 署名された文書の有効期間の制約

署名の場合は、署名した文書の有効期間安全でなければならないという特徴があり、暗号の使用期間+有効期間の暗号強度を要求される。したがって、安全な運用のためには、電子政府システムとしてはこの有効期間をある範囲に絞り込み、署名付きの文書を再発行するなどの仕組みも必要となる。例えば、電子免許証システムにおいて4年ごとに再発行する決まりにするなどの対応である。

(2) 標準化対応の必要性

推奨暗号としても、マイクロソフトのSSLや今後出てくるプレインストールソフトに採用されていない(される見込みがない)と、実際の応用システムに採用されない可能性が強い。特に、クライアント側のユーザが一般住民の場合はそうである。そのためには、まず、ISOやIETFでオーソライズすることも必要となってくる。

(3) プロトコル、製品評価の必要性

現実に指摘される弱点は、暗号アルゴリズムよりも暗号プロトコルや暗号製品の方が多い。また、電子政府システムの安全性は、暗号プロトコルや暗号製品も安全であって初めて保たれる。したがって、暗号アルゴリズムの安全性評価だけでなく、電子政府で用いられる可能性のある暗号モジュールや暗号プロトコル、暗号製品に関する安全性評価のニーズも強いことから、今後対応していくことが望ましい。

以上