資料

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

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　　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、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、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)　ハッシュ：SHA-1,MD5 官庁側署名　公開鍵：RSA(1024)　ハッシュ：SHA-1 通信暗号化　未定
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　ハッシュ：SHA-1,MD5 申請側送信　公開鍵：RSA　ハッシュ：SHA-1,MD5 共通鍵：TDES,DES 一次形式審査　公開鍵：RSA　ハッシュ：SHA-1,MD5 公文書発行　公開鍵：RSA　ハッシュ：SHA-1,MD5 民間側公文書取得 公開鍵：RSA　ハッシュ：SHA-1,MD5 共通鍵：TDES,DES
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)　ハッシュ：SHA-1 通信暗号化　公開鍵：RSA(1024) 共通鍵：未定（CAST,DES,TDES,RC2 等を予定）
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)　ハッシュ：SHA-1 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)
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】 ・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	・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】 ・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】 ・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	・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） ・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） ・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

①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、①安全性、②実装性、③暗号標準、④プロトコル標準、⑤製品、⑥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（⑤製品：２社、③暗号標準、④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

②１０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思われる」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

③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

①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、要件表の桝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には、その桝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には、その桝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

①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「①署名、認証②通信、③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①署名・認証、②通信、③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、①署名・否認防止、②通信・認証、③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

②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

③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な）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

①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

②ＩＣ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

③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 ブラウズ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ので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ので、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=1013041605202114009&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.ak.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.ipaustralia.gov.au/home_page/ecentre/eccs/index.cfm?fuseaction=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/ehtml/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/drivertestapplication.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.ihost.com/renewal/cgi-addr/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/endb/servlets/com.eofcom.servlet.resource.ResourcesServlet?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/notes/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/HomePageEnglish	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.au/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、国防省の下の通信安全機構（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ＡＳＣＩ３３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 >= 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 >= 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 >= 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-Hellan(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ＡＣＳＩ３３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、個人情報の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 とも呼ばれる。

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 Cenrale de la Securite des Systems 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 fur 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）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、①電子申請、②電子調達、③電子納付、④電子情報提供、⑤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。

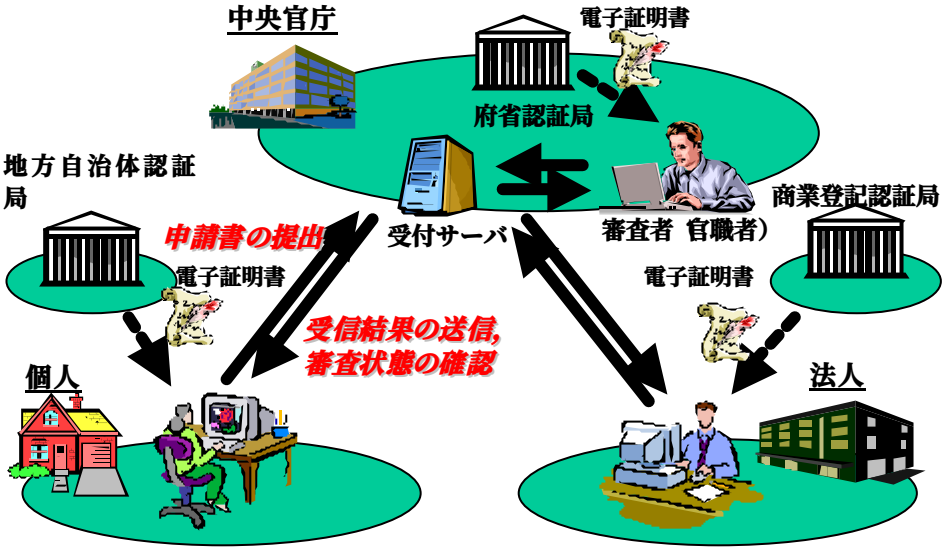
	予め組み込まれた技術	独自にシステムに組み込む技術
GtoCモデル （電子申請、 電子情報提供）	SSLによるデータ秘匿 パスワード認証	電子署名によるデータ保全
GtoBモデル （電子調達、 電子納付）		電子署名によるデータ保全 ICカードによる秘密鍵の格納 IP-VPNの利用・IPsec対応ルーターの利用によるデータ秘匿・データ保全 作り込み通信暗号によるデータ秘匿・相手認証

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

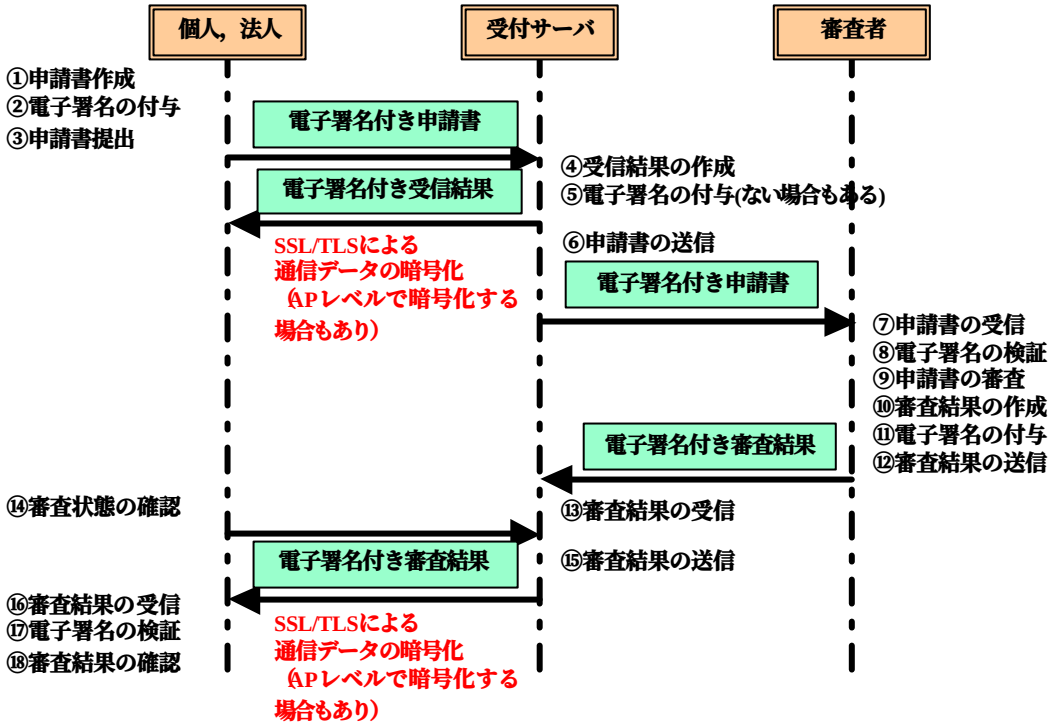
電子申請システムにおける処理は、

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

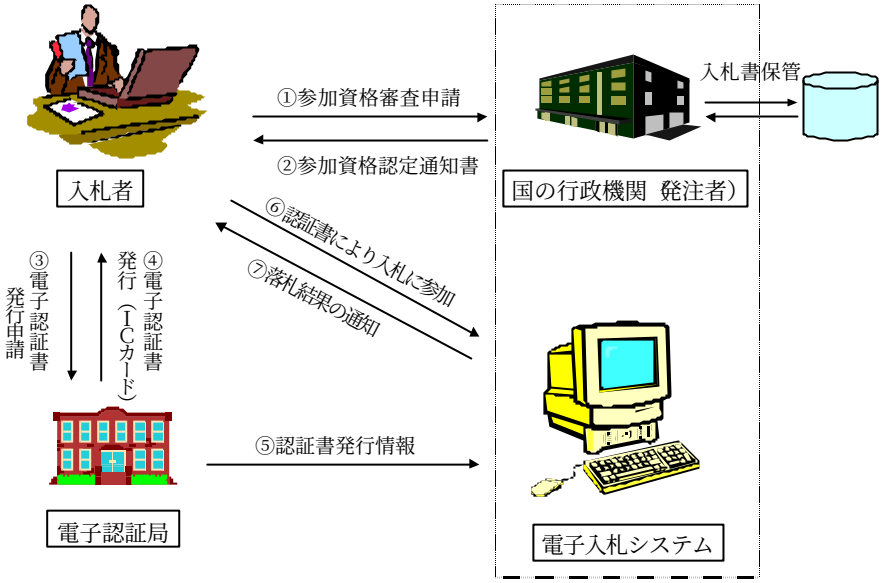
【利用形態毎／整理項目毎の分類表】

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

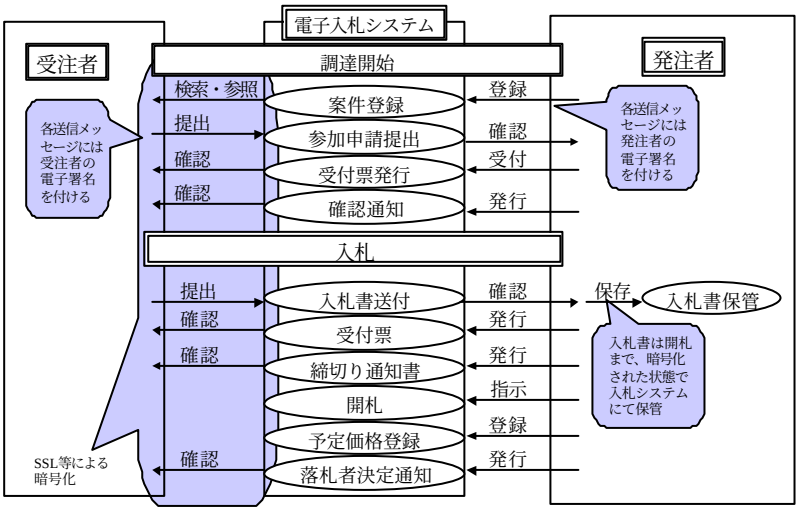
電子調達システムにおける処理は、以下の各フェーズにより構成される。

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】

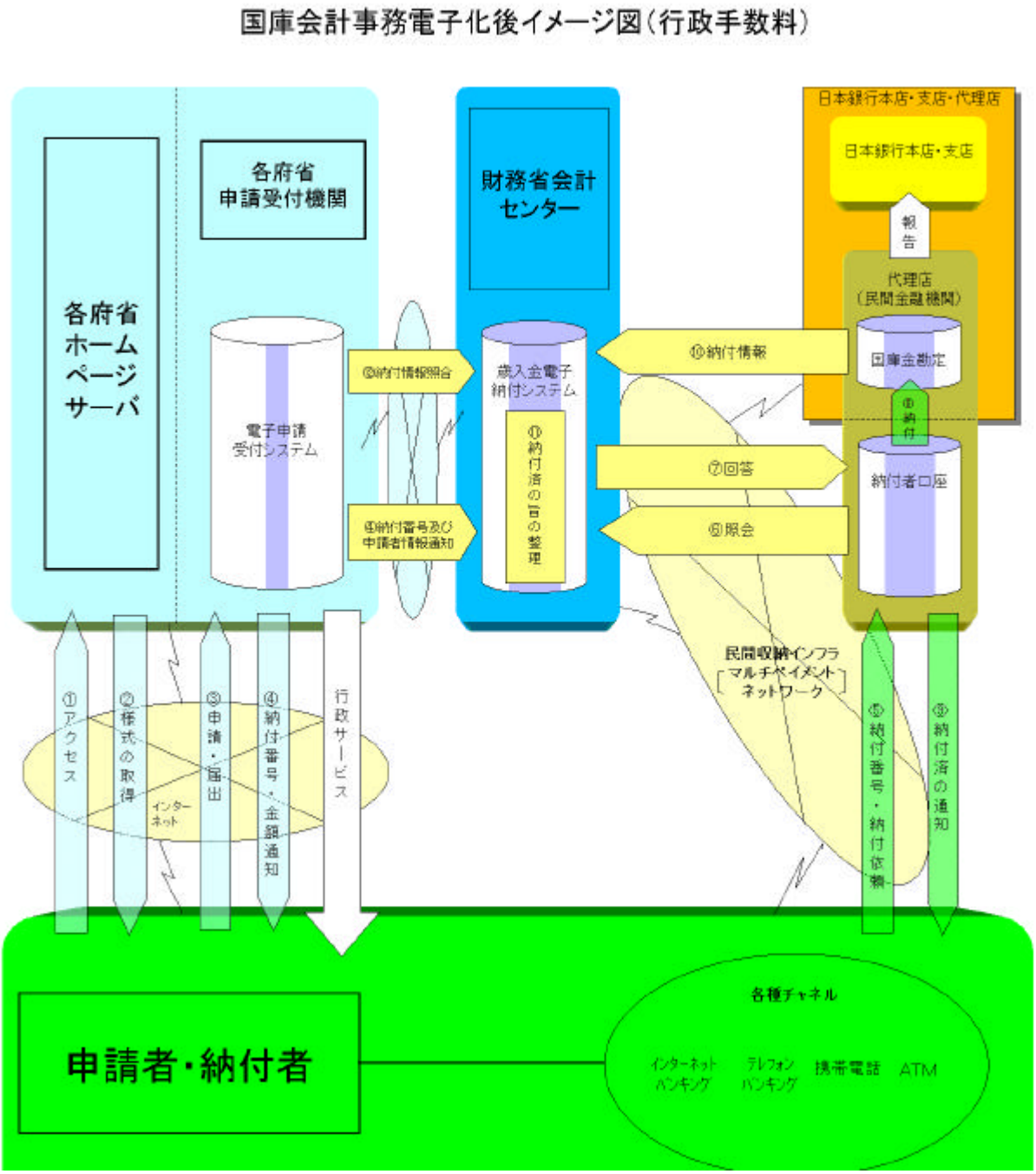
<table>
<tr><th colspan="2" rowspan="2">整理項目
利用形態</th><th colspan="3">システム概要</th><th colspan="3">要　件</th></tr>
<tr><th>(1)データ内容</th><th>(2)データサイズ</th><th>(3)回線速度</th><th>(4)現在利用している暗号処理速度</th><th>(5)現在利用している暗号強度</th><th>(6)その他</th></tr>
<tr><td colspan="2">(ア)＜利用者側＞認証</td><td>－</td><td>－</td><td>－</td>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

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。



出典：http://www.kantei.go.jp/jp/it/network/dai3/3siryou6s3.html

（2）処理フロー・モデル

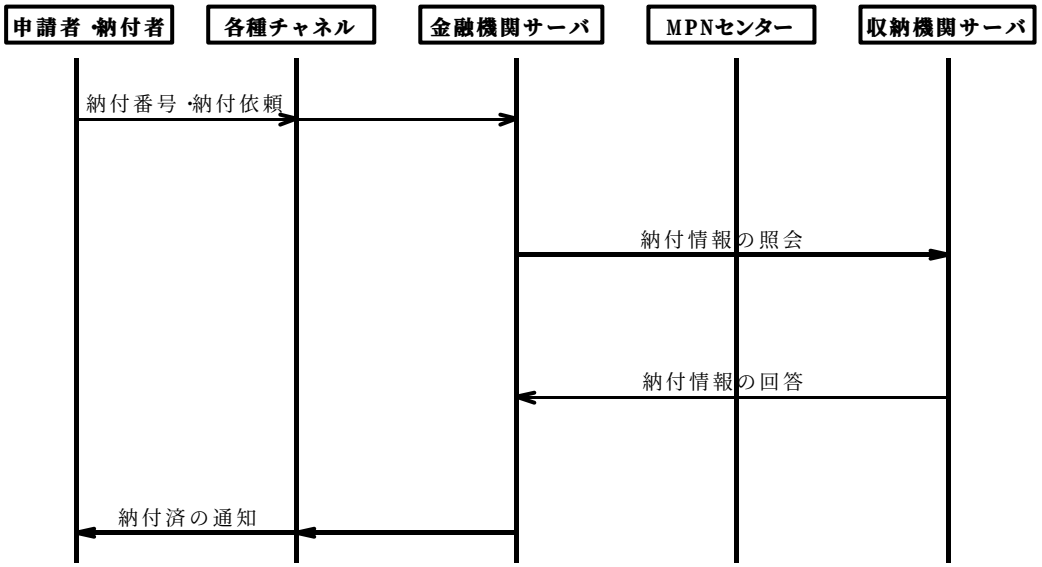
電子納付システムは、行政サービス等を提供する各府省側のシステムと、申請者・納付者が国庫金を納付するための金融機関側のシステムとを連結することによって機能するものである。その処理フローは、連動するシステムの作りに依存する部分もあるが、基本的には、金融機関側から送られてきた納付情報を、各府省（収納機関）側のシステムに配信する作りとなる。処理フローは、

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】

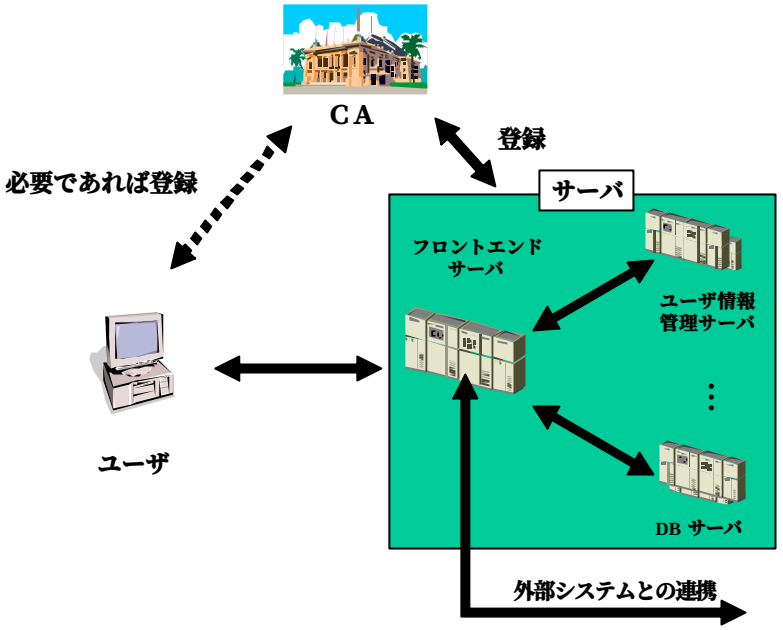
整理項目 ＼ 利用形態	システム概要			要　件		
	(1)データ内容	(2)データサイズ	(3)回線速度	(4)現在利用している暗号処理速度	(5)現在利用している暗号強度	(6)その他
<金融機関 ＝MPN センター間> 納付情報の照会	数値、文字	1 件当り 100 byte 程度	512Kbps 程度	IPsec 対応ルータを利用	TDES(168bit,3 キー) Diffie-Hellman (1024bit)	
<収納機関（政府含む） ＝MPN センター間> 納付情報の回答	数値、文字	100 byte ～数 KB 程度	512Kbps 程度	IPsec 対応ルータを利用	TDES (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

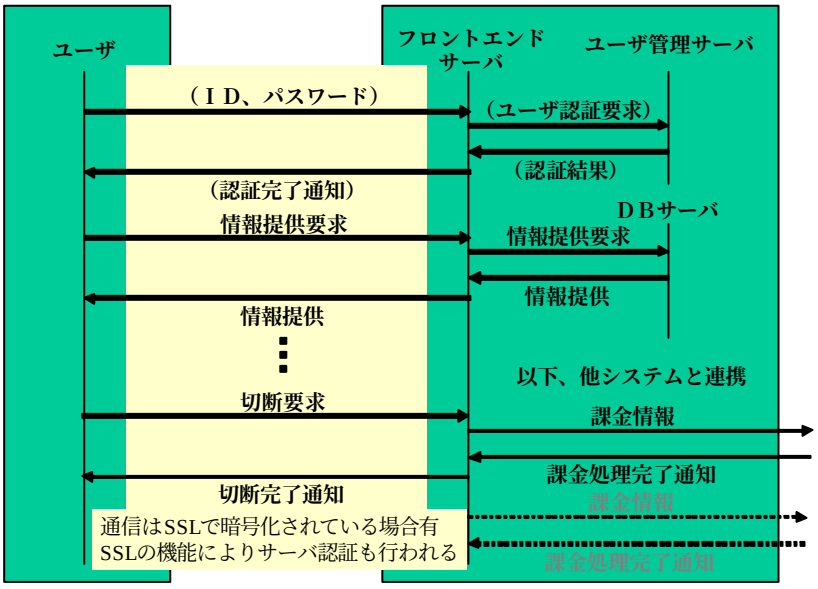
電子情報提供システムにおける処理は、

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

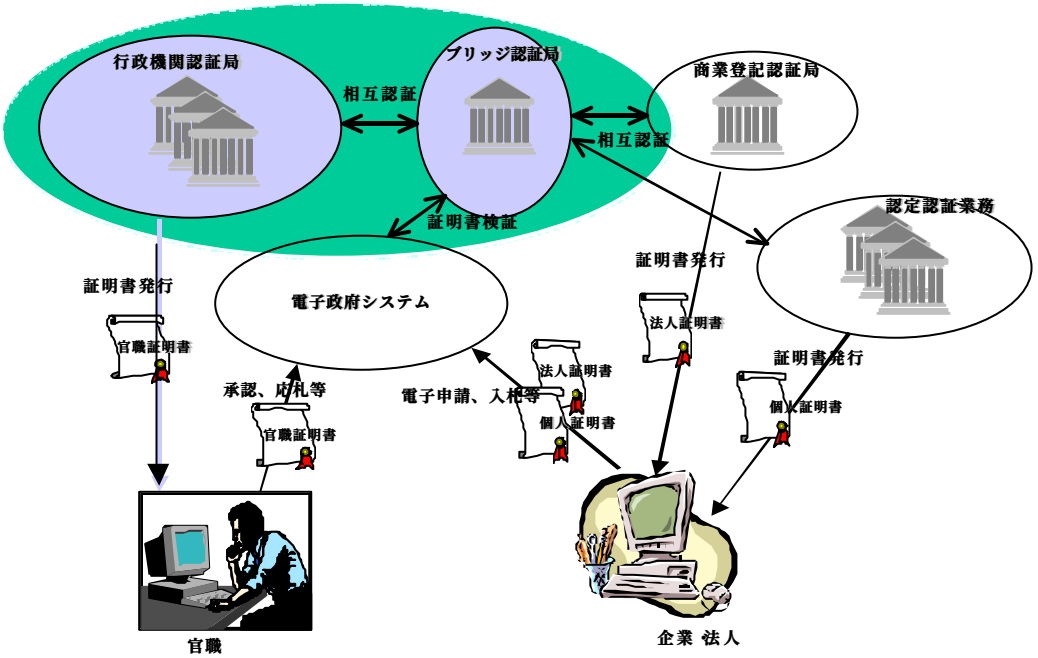
（１）政府認証基盤のシステム構成

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

①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

②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。

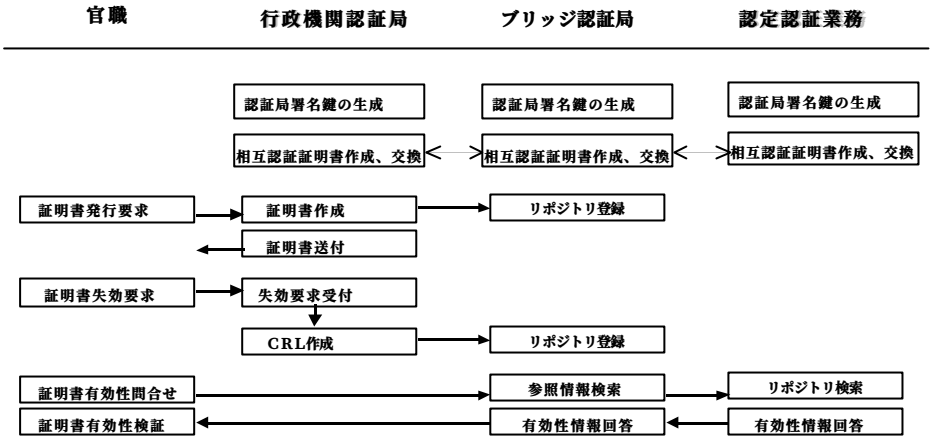
また、ブリッジ認証局には電子証明書を検証するシステムがあり、官職が電子申請、届出を行う申請者の電子証明書の有効性確認を行う事ができる。電子申請、届出を行う申請者による官職証明書の有効性確認は、統合リポジトリにある情報によって行える。

③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	168ビット	
			RC4	128ビット	

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されて用いられる。暗号評価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、ＤＥＳ、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る、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と、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（想定の起点となる時から、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言う意見はなく、（ｃ）の方式で良いと言う意見が多かった。また、アンケート結果では（ｂ）と言う意見が多く、（ｃ）の方式で良いと言う意見もあった。

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いことが期待できる。
（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と、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と、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言う特徴があり、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