暗号技術検討会

２００２年度報告書

暗号技術検討会

２００３年３月

目次

【資料】

- 「暗号調達のためのガイドブック」

【参考資料】

- 「各府省の情報システム調達における暗号の利用方針」

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、e-Japan 重点計画に基づき、2003 年度までに電子情報を紙情報と同等に扱う行政の実現を目指している。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（旧通商産業省）からの委託を受けて、情報処理振興事業協会（IPA）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ことを目的とした暗号技術評価委員会を設置するとともに同委員会の事務局を務めた。2001 年度からは通信・放送機構（TAO）が同委員会の共同事務局として参加した。また、2001 年度には、暗号技術評価委員会に加えて、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、暗号技術の利用に関し政策的な観点から検討を行うことを目的として、暗号技術検討会（以下、本検討会）を設置した。

本検討会は、電子政府で利用される暗号技術、国際標準化に関する暗号技術及び電子署名法等に基づいて利用される暗号技術の評価・調査研究、並びにその他暗号技術の利用等に関連する技術課題を検討対象としており、特に、2002 年度は、2001 年度に引き続き暗号技術の評価を行うとともに、電子政府推奨暗号リスト案の策定、暗号の調達のためのガイドブックの作成、及び 2003 年度以降の CRYPTREC 活動についての検討を行った。

なお、暗号調達ガイドブックに関しては、本検討会の下に設置された暗号調達ガイドブック作成ＷＧが暗号調達ガイドブック案の作成作業を行った。

本報告書は、2002 年度の本検討会における検討結果をまとめたものであり、総務省及

び経済産業省に対して報告するとともに、電子政府を構築する各府省関係者、及び一般の暗号ユーザの方々にも広く読んで頂くことを想定している。

なお、2002 年度の CRYPTREC 活動のうち、詳細な技術的事項については、暗号技術評価委員会並びに同委員会の下に設置された共通鍵暗号評価小委員会及び公開鍵暗号評価小委員会における議論を踏まえて、IPA 及び TAO によってまとめられている「CRYPTREC Report 2002」を御参照頂きたい。

本検討会は、2002 年度、当面の目標であった電子政府推奨暗号リスト案及び暗号調達ガイドブックを作成した。しかしながら、国民が安心して利用できる電子政府を構築し、運用していくためには、2003 年度以降も継続して暗号技術を監視し、評価するとともに、暗号モジュールに関する安全性評価基準を作成する等の活動を実施していく必要がある。

これらの活動を実施していくためには、CRYPTREC 関係者が一致団結することが不可欠であり、今後とも関係者の方々の御協力を頂きながら、暗号技術検討会をはじめとする CRYPTREC 活動を積極的に推進していきたい。

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、精力的に暗号調達ガイドブックを作成して頂いた暗号調達ガイドブック作成 WG 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。

2003 年 3 月

暗号技術検討会
座長　今井　秀樹

２．暗号技術検討会開催の背景、構成員及び開催状況

２．１．暗号技術検討会開催の背景

高度情報通信ネットワークの安全性及び信頼性の確保は、我が国が目指す世界最先端の IT 国家構築の基盤となるものであり、国民一人一人が安心してネットワークを利用するための前提となるものである。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）及び e-Japan 重点計画-2002（2002 年 6 月 18 日　同本部決定）では、特に電子政府、電子商取引、重要インフラについて、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をゼロとすることを目標として、政府は情報セキュリティのための諸施策を実施することとされている。

暗号技術は情報セキュリティの基盤技術であり、その安全性を暗号技術の専門家により技術的、専門的な見地から客観的に評価することが重要である。また、2003 年度までに「電子政府」の実現が予定されており、そのセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリスト化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府の構築に貢献することを目指すこととした。

２．２．CRYPTREC の体制

CRYPTREC とは Cryptography Research and Evaluation Committees の略であり、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：今井秀樹東京大学教授）と、通信・放送機構（TAO）及び情報処理振興事業協会（IPA）が共同で開催する暗号技術評価委員会（委員長：今井秀樹東京大学教授）による暗号技術評価プロジェクトを指す（CRYPTREC の体制図は図１参照）。検討会及び評価委員会は以下のように検討及び評価を進めた。

２．２．１．暗号技術検討会

暗号技術検討会（以下、「検討会」）は、総務省及び経済産業省に対して暗号利用に関する助言を行うとともに、電子政府における暗号利用に関する政策的判断を行った。また、検討会の下には、必要に応じてワーキンググループを設置し、詳細な検討を効率的に実施することとしており、2002 年度は、「暗号調達ガイドブック作成ワーキンググループ（リーダ：佐々木良一東京電機大学教授）」を設置し、電子政府推奨暗号を円滑に調達するための手引書を作成した。

検討会は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の研究会として開催し、内閣官房、警察庁、防衛庁、法務省、外務省、財務省等がオブザーバとして参加した。

２．２．２．暗号技術評価委員会

暗号技術評価委員会（以下、「評価委員会」）は、暗号アルゴリズム等に関する技術的評価を行い、評価結果を検討会に報告した。また、検討会に対して暗号に関する技術的助言を行った。評価委員会の下には、共通鍵暗号評価小委員会（委員長：金子敏信東京理科大学教授）及び公開鍵暗号評価小委員会（委員長：松本勉横浜国立大学教授）を設置した。

TAO 及び IPA の委員会として開催し、総務省、経済産業省、警察庁、防衛庁、外務省等がオブザーバとして参加した。

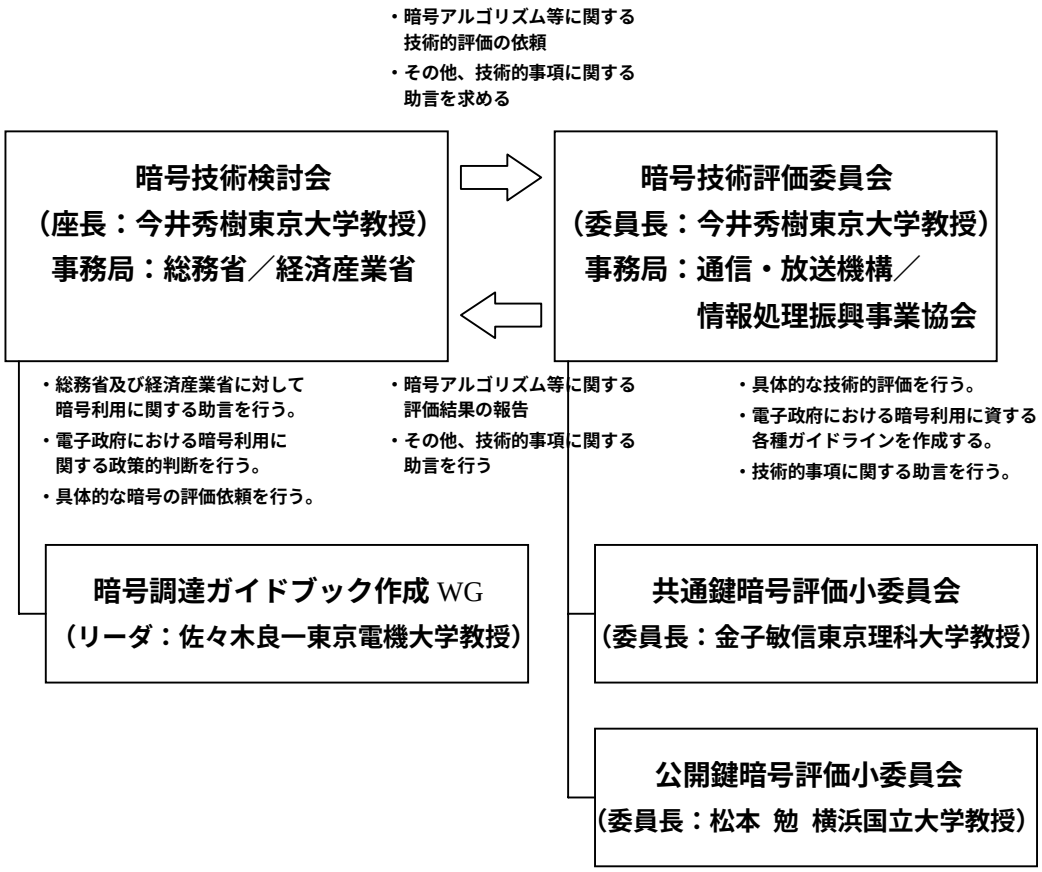


図１　2002 年度の CRYPTREC の体制図

２．３．メンバー

２．３．１．暗号技術検討会メンバー

（構成員）※肩書は 2003 年 3 月末現在。敬称略。

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	中央大学理工学部教授
	岩下　直行	日本銀行金融研究所調査第２課企画役
	岡崎　宏	情報通信ネットワーク産業協会常務理事
	岡本　栄司	筑波大学電子・情報工学系教授
	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（社団法人電気通信事業者協会代表兼務）
	小田　雅一	社団法人情報サービス産業協会セキュリティ委員会委員
	小柳津　育郎	ＮＴＴエレクトロニクス株式会社セキュリティシステム事業部技術部長
	加藤　義文	社団法人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	財団法人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教授
	佐々木　良一	東京電機大学工学部情報メディア学科教授
	宝木　和夫	社団法人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）※肩書は原則として参加当時のもの。敬称略。

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
手塚　新樹	警察庁情報通信局技術対策課長
中村　範明	防衛庁運用局指揮通信課長（第１回）
青木　信義	防衛庁長官官房情報通信課長（第２回～）
高森　國臣	総務省行政管理局管理官
猿渡　知之	総務省自治行政局自治政策課情報政策企画官
中垣　治夫	法務省民事局商事課補佐官
石川　正紀	外務省大臣官房情報通信課長（第１回）
楠田　かおる	外務省大臣官房情報通信課長（第２回～）
中山　峰孝	財務省大臣官房審議官室長（第１回）

	宇野　雅夫	財務省日野参事官室企画官（第２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（第１回）
	蓮池　和夫	独立行政法人通信総合研究所情報通信部門長（第２回～）
	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（第１回）
	喜安　拓	通信・放送機構研究企画管理部長（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
	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
	小倉　久宜	財団法人金融情報システムセンター監査安全部長

２．３．２．暗号調達ガイドブック作成ＷＧメンバー

※肩書は 2003 年 3 月末現在。敬称略。

リーダ	佐々木　良一	東京電機大学工学部情報メディア学科教授
	岩下　直行	日本銀行金融研究所研究第２課企画役
	宇賀村　直紀	社団法人電子情報技術産業協会ＩＴセキュリティセンター部長
	岡本　栄司	筑波大学電子・情報工学系教授
	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
	中村　逸一	株式会社ＮＴＴデータ　ビジネス開発事業本部セキュリティ事業部　営業グループ　部長
	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研究員

２．４．開催状況

2002 年度、検討会は計 6 回開催された。各回会合の開催日及び主な議題は以下のとおり。なお、暗号調達ガイドブック作成ＷＧの会合開催状況は第４章を参照のこと。

【第 1 回】平成 14 年 5 月 16 日（木）
（主な議題）暗号技術検討会 2002 年度活動計画
電子政府推奨暗号の数
暗号技術評価委員会への依頼事項
暗号調達ガイドブック作成ワーキンググループの設置

【第 2 回】平成 14 年 7 月 16 日（火）
（主な議題）暗号調達のためのガイドブック案
電子政府推奨暗号の数
電子政府推奨暗号リスト素案の検討状況
暗号モジュール評価の現状把握

【第 3 回】平成 14 年 9 月 30 日（月）
（主な議題）電子政府推奨暗号リスト案
暗号調達のためのガイドブック案

【第 4 回】平成 14 年 11 月 27 日（水）
（主な議題）電子政府推奨暗号リスト案
同リスト案に対するパブリックコメント
暗号調達のためのガイドブック案
暗号プロトコルの現状把握（１）
今後の CRYPTREC 活動

【第 5 回】平成 15 年 2 月 12 日（水）
（主な議題）電子政府推奨暗号リストの決定
パブリックコメントに対する回答
暗号調達のためのガイドブック案
暗号プロトコルの現状把握（２）
今後の CRYPTREC 活動

【第 6 回】平成 15 年 3 月 24 日（月）
（主な議題）2002 年度報告書
暗号調達のためのガイドブック
今後の CRYPTREC 活動

３．電子政府推奨暗号リスト

３．１．e-Japan 重点計画及びセキュリティ・アクションプランにおける電子政府の実現及び暗号技術評価の位置付け

2001 年 3 月 29 日に、高度情報通信ネットワーク社会推進戦略本部で決定された e-Japan 重点計画では、行政の情報化及び公共分野における情報通信技術の活用の推進における施策の意義として「電子政府」の実現が掲げられており、また、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の具体的施策の一つとして、「暗号技術の標準化の推進」が掲げられている。

（「e-Japan 重点計画」より抜粋）

５．行政の情報化及び公共分野における情報通信技術の活用の推進

（２）施策の意義

（略）

特に、国の行政機関においては、行政の情報化により、事務・事業及び組織の改革を推進するとともに、セキュリティの確保に留意しつつ、「紙」による情報の管理からネットワークを駆使した電子化された情報の管理へ移行し、高度に情報化された行政、すなわち以下のような「電子政府」を実現する。

（主な項目）行政情報の電子的提供
申請・届出等手続の電子化
歳入・歳出の電子化
調達手続の電子化
ペーパーレス化（電子化）

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

①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、実装性に優れた暗号技術を採用するため、2002 年度中に、ISO、ITU 等における暗号技術の国際標準化の動向を踏まえ、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。

e-Japan 重点計画の決定を受け、2003 年度からの電子政府の実現に向けて政府の情報セキュリティ確保に万全を尽くすことを目的として、「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」が内閣官房が中心となって取りまとめられ、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。その中では、具体的な方策の一つとして、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ることが掲げられている。

（「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」より抜粋）

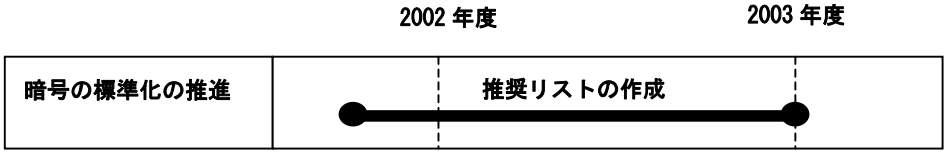
２．具体的な方策

（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。

（参考）日程表



2002 年 6 月 18 日に策定された「e-Japan 重点計画-2002」においても、高度情報通信ネットワーク社会形成のために政府が迅速かつ重点的に実施すべき施策の中に、「電子政府の実現」及び「暗号技術の標準化の推進」が掲げられている。

３．２．暗号技術評価について

３．２．１．暗号技術評価の目的

申請届出や調達など行政手続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[1]を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及び評価を進めてきた。

本暗号技術評価活動は我が国における暗号技術評価体制の確立に向けた一歩であり、米国政府標準暗号を定める AES (Advanced Encryption Standard)プログラムを参考にしつつ、欧州における暗号評価プロジェクト（NESSIE：New European Schemes for Signatures, Integrity, and Encryption)や ISO/IEC における国際標準化活動への協力も行っている。

３．２．２．評価概要

電子政府で利用可能と想定される暗号技術の評価は暗号アルゴリズム[2]の評価を中心として実施した。公開鍵暗号、共通鍵暗号、ハッシュ関数、擬似乱数生成系の４つの分類について、評価対象暗号技術の募集・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、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た。なお、今年度評価を実施した暗号技術は、昨年度でスクリーニング評価を終了しているため、詳細評価のみを行った。

（１）暗号分類

（イ）公開鍵暗号

守秘，署名，認証、鍵共有

（ロ）共通鍵暗号

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）ハッシュ関数

（ニ）擬似乱数生成系

（２）スクリーニング評価※今年度は実施せず

詳細評価を実施するに値するかどうかを判断するためのスクリーニング評価を下記の観点から実施した。

（イ）安全性に明らかな問題がないかどうかを評価する。

（ロ）第三者実装上問題がないかどうかを評価する。

---

[1] ：暗号技術とは、暗号（暗号アルゴリズム、暗号方式)、暗号プロトコル、暗号モジュール、暗号鍵管理等を含む概念とする。

[2] ：暗号アルゴリズムは、単に暗号、または、暗号方式とも呼ばれる。

（３）詳細評価

スクリーニング評価で問題がないと判断された暗号について、電子政府で利用可能かどうかの観点から評価する詳細評価を下記の観点から実施した。

（イ）既知の攻撃法に対する統一的な強度評価

（ロ）各詳細評価対象暗号特有の攻撃法に対する強度評価

（ハ）パラメータ／鍵の設定基準の評価

（ニ）ソフトウェア実装評価

（ホ）ハードウェア実装評価

３．２．３．各暗号技術の評価基準の概要

各暗号技術の評価基準の概要は、以下の通りである。詳細は、暗号技術評価報告書（2002 年度版）(CRYPTREC Report 2002)を参照のこと。

（１）公開鍵暗号

比較的長い期間にわたる使用実績・評価実績があり、インターオペラビリティの観点から仕様の変更を簡単には求められない公開鍵暗号方式[3]については、多くの研究者から十分な評価研究を受けているが、実運用における安全性に関する問題点が指摘されていないこと、すなわち経験的に安全であることを求めた。

使用実績が少ない新しい公開鍵暗号方式については、既存暗号技術とは独立に仕様を定めることができることから、最低限の条件として証明可能安全性が示されていることを必須とした。

これらに加えて、プリミティブが依存する数論的な問題の困難性や、推奨パラメータの選択方法や補助関数のスキームの中での利用方法を含めて総合的に安全性を評価した。

（２）共通鍵暗号

以下の条件のいずれかを満たすことを求めた。

（イ）現時点の最良の解読技術を適用しても、秘密鍵の総当たりである 2^{128} 以上の計算量が必要と判断されるもの。特に、差分攻撃や線形攻撃などの代表的な攻撃法について、安全性が確認されているもの。

（ロ）世界的に広く使用され、かつ多くの研究者から十分な評価研究を受けているが、実運用における安全性上の大きな問題点が指摘されておらず、現時点で安全と判断されるもの。この場合、2^{100} 以上の解読計算量を目安とした。

---

[3] ：公開鍵暗号方式（または公開鍵暗号スキーム）は、プリミティブ（基本関数）とその他の要素技術（ハッシュ関数、擬似乱数生成系等）を組み合わせて構成される公開鍵暗号全体の仕組みを指す専門用語。

（３）ハッシュ関数

以下の条件のいずれかを満たすことを求めた。

（イ）特定の出力に対する入力値を発見する手間への耐性が十分に高く（最良の解読技術を適用しても 2^{160} 以上の計算量）、かつ出力値が一致するような異なる入力値を発見する計算量が最良の解読技術を適用しても 2^{80} 以上であること。

（ロ）世界的に広く使用され、かつ実運用における安全性上の問題点が指摘されていないこと。なお、全ハッシュ値の長さが少なくとも 160 ビット以上であること。

（４）擬似乱数生成系

以下の条件をすべて満たすことを求めた。

（イ）統計的性質が真性乱数に近く、かつ、既知の出力ビット履歴から未来又は過去の未知出力ビットが予測困難であること。

（ロ）擬似乱数生成系を使用するシステムの総当たり攻撃に対し、十分に耐性をもつ程に、実質的入力空間が大きいこと。

（ハ）統計的性質は、例えば NIST が公表している SP800-22 等の代表的な擬似乱数検定テストに合格するものであること。

３．２．４．暗号技術評価結果の概要

今年度の暗号技術評価結果の概要を以下に示す。なお、詳細は、暗号技術評価報告書（2002 年度版）(CRYPTREC Report 2002)を参照のこと。

（１）公開鍵暗号方式の総評[4]

（イ）DSA　（署名）

米国 NIST(National Institute of Standards and Technology)によって提案、標準化された電子署名方式であり、電子署名法に係る指針[5]に記載されている。オブジェクト識別子は、1 2 840 10040 4 3 である。

安全性は有限体上の離散対数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経験的に安全である。

安全性の観点からパラメータ p のサイズは 1024 ビットを選択することを強く推奨する。2001 年 10 月に NIST が FIPS PUB 186-2 (+ change notice 1)に提示した擬似乱数生成系の修正に従うべきである。

---

[4]：公開鍵暗号方式が証明可能安全性を有するとは、その方式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、その方式の安全性が否定されるわけではない。

[5]：電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年総務省 法務省 経済産業省告示第 2 号）のことを指す。以下、同指針を「電子署名法に係る指針」と略記する。

（ロ）ECDSA　**（署名）**

CRYPTREC **では** ECDSA (ANSI X9.62)**と** ECDSA (SEC 1[6])**とを評価した。** ECDSA(ANSI X9.62)**は電子署名法に係る指針に記載されている署名方式であり、オブジェクト識別子は、**1 2 840 10045 4 1 **である。**

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。証明可能安全性は示されていないが経験的に安全であり、2002 **年時点では安全性について重大な問題点は指摘されていない。**

ECDSA(SEC 1)**における楕円曲線パラメータは** SEC 1 **に示されている。これらの楕円曲線については特段の問題点は指摘されていない。安全性の観点から群位数が** 160 **ビット以上の素因子をもつようなパラメータを選択することを強く推奨する。擬似乱数生成器に関して** NIST **が** FIPS PUB 186-2 (+ change notice 1)**に提示した擬似乱数生成器の動向に注意すべきである。**

（ハ）ESIGN　**（署名）**

ESIGN **署名の仕様は複数存在する。**ESIGN**（応募暗号）の評価の参考にするために** TSH-ESIGN **も評価した。**

プリミティブの安全性は $n = p^2q$ **型素因数分解問題の困難性に依存している。**ESIGN **の署名生成速度は** RSA **署名と比べて高速であるが、**RSA **プリミティブと同程度の安全性を** ESIGN **のプリミティブにおいて得るためには** RSA **の法パラメータのサイズよりも少し大きな法パラメータを利用しなければならない。**

（ａ）ESIGN **は証明可能安全性を有しない。実際に、一部のパラメータの利用に際して、無視できない確率で署名の偽造が可能である。**

（ｂ）TSH-ESIGN **には新提案技術に必須とされた証明可能安全性が示されていない。**

（ニ）RSA　**（署名、守秘）**

RSA **プリミティブを利用した署名方式にはいくつかの仕様が存在する。**CRYPTREC **では** RSASSA-PKCS1-v1_5 **と** RSA-PSS **を評価した。**RSASSA-PKCS1-v1_5 **と** RSA-PSS **は両方とも電子署名法に係る指針に記載されている署名方式であり、それぞれのオブジェクト識別子は、**1 2 840 113549 1 1 5 **および** 1 2 840 113549 1 1 10 **である。**

また RSA **プリミティブを利用した守秘方式にはいくつかの仕様が存在する。**CRYPTREC **では** RSAES-PKCS1-v1_5 **と** RSA-OAEP **を評価した。**

これら 4 **つの** RSA **方式は長期間広く使われてきた実績と、広範な観点から評**

---

[6] **：Standards for Efficient Cryptography Group (SECG)から提供されている技術文書の 1 つ。**

価が行われてきたことから経験的に安全である。

（ａ）RSASSA-PKCS1-v1_5 は電子署名法に係る指針に記載されている署名方式の 1 つである。証明可能安全性は示されていない。

（ｂ）RSA-PSS は新提案技術に必須とされた証明可能安全性を有する。

（ｃ）RSAES-PKCS1-v1_5 は SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。経験的安全性は有するが、証明可能安全性は持たず、実際に能動的攻撃が成立する可能性も無視できないので、実運用環境上における攻撃に対する対策を十分に施し細心の注意を払う必要がある。

（ｄ）RSA-OAEP は新提案技術に必須とされた証明可能安全性を有する。

RSA プリミティブの安全性は、n = pq 型素因数分解問題の困難性に依存している。安全性の観点から法パラメータ n = pq のサイズは 1024 ビット以上のものを利用することを強く推奨する。

（ホ）ECIES （守秘）

ECIES は、2000 年度には ECAES として CRYPTREC に応募されていたが、2001 年度では暗号技術名を ECIES に変更して応募されている。ECIES にはいくつかの仕様が存在する。CRYPTREC では SEC 1 に記載された仕様を基に評価した。

SEC 1 に記載された仕様の ECIES におけるスキームには KDF 関数への入力及び MAC の取り扱い方法の不備が原因で、脆弱性が存在し、新提案技術に必須とされた証明可能安全性を有しない。

（ヘ）HIME(R) （守秘）

2000 年度応募された HIME-1 と HIME-2 の改良版として 2001 年度に応募された技術である。

プリミティブの安全性は $n = p^2q$ 型素因数分解問題の困難性に依存している。RSA プリミティブと同程度の安全性を HIME(R)のプリミティブにおいて得るためには RSA の法パラメータのサイズよりも少し大きな法パラメータを利用しなければならない。

HIME(R)にはその仕様書に不備・曖昧さがあり、2002 年 9 月時点で信頼に足る HIME(R)の仕様書が公に手に入る状況になっていないと判断された。このため、HIME(R)の第三者による実装性や相互接続性が担保されないと判断された。HIME(R)の仕様の曖昧さを埋めてその仕様を合理的に定めたとしても、自己評価

書に記載されている証明可能安全性の証明中いくつかの箇所に問題があり、不完全であり、2002 年 9 月時点で新提案技術に必須とされた証明可能安全性を有すると断定できないと評価された。

（ト）ECDH （鍵共有）

ECDH は、2000 年度には ECDHS として CRYPTREC に応募されていたが、2001 年度では暗号技術名を ECDH に変更して応募されている。

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。能動的攻撃に対しては証明可能安全性は示されていないが経験的に安全である。使用にあたっては運用上の注意が必要である。

ECDH(SEC 1)における楕円曲線パラメータは SEC 1 に示されている。これらの楕円曲線については特段の問題点は指摘されていない。安全性の観点から群位数が 160 ビット以上の素因子をもつようなパラメータを選択することを強く推奨する。

（チ）DH （鍵共有）

DH にはいくつかの仕様が存在する。CRYPTREC では ANSI X9.42-2001 を対象とした。

安全性は有限体上の離散対数問題の困難性に依存している。能動的攻撃に対しては証明可能安全性は示されていないが経験的に安全である。使用にあたっては運用上の注意が必要である。

安全性の観点からパラメータ p のサイズは 1024 ビット以上を選択することを強く推奨する。

（リ）PSEC-KEM （鍵共有）

2000 年度に応募された PSEC を ISO/IEC 18033-2 において審議されている KEM 技術に適合するように変更を加えたもので、2001 年度に応募された。

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。KEM技術に関する証明可能安全性を有するので、PSEC-KEM を KEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism)構成に利用することは安全であるといえる。しかし、それ以外の目的の利用について安全性の研究は十分ではないので、今後の研究に注意すべきである。

CRYPTRECとしてはSEC 1で規定される曲線の利用を推奨する。これらの楕円曲線については特段の問題点は指摘されていない。安全性の観点から群位数が160ビット以上の素因子をもつようなパラメータを選択することを強く推奨する。

（２）共通鍵暗号の総評

（イ）CIPHERUNICORN-E**（６４ビットブロック暗号）**[7]

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。

（ロ）Hierocrypt-L1**（６４ビットブロック暗号）**[7]

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。

（ハ）MISTY1**（６４ビットブロック暗号）**[7]

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。

（ニ）Triple DES**（６４ビットブロック暗号）**[7]

安全性について、FIPS**等で保証されている間は、問題ないと考える。**

（ホ）Advanced Encryption Standard**（１２８ビットブロック暗号）**

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。

（ヘ）Camellia**（１２８ビットブロック暗号）**

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。

（ト）CIPHERUNICORN-A**（１２８ビットブロック暗号）**

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。

（チ）Hierocrypt-3**（１２８ビットブロック暗号）**

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。

（リ）RC6 Block Cipher**（１２８ビットブロック暗号）**

---

[7] **：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が使用可能な状況にあれば、128ビットブロック暗号を選択するのが望ましい。**

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する。

なお、CRYPTREC事務局では、2002年10月16日付文書で、RSAセキュリティ株式会社から、「知的財産権上の問題により、今後RC6の普及活動は行わない」との連絡を受領している。

（ヌ）SC2000（１２８ビットブロック暗号）

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。

（ル）MUGI（ストリーム暗号）

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。

（ヲ）MULTI-S01（ストリーム暗号）

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。

（ワ）RC4（ストリーム暗号）

標準仕様（ワード長n=8、状態数256)のRC4については、現在のところ、現実的な解読法は提案されていない。しかし、秘密鍵から生成される初期状態によっては、必ずしも安全ではないという報告がなされている。したがって、RC4の利用に関してその初期状態の決定には注意が必要である。

SSL3.0/TLS1.0での利用に関しては、現在のところその安全性に関して欠陥は報告されていない。ただし、SSL3.0/TLS1.0の仕様上は40ビット秘密鍵（40-bit RC4）と128ビット秘密鍵（128-bit RC4）が利用可能であるが、CRYPTRECとしては、40ビット秘密鍵によって初期状態を生成する40-bit RC4は鍵の推定が可能であることから安全ではないと判断する。

（３）ハッシュ関数[8]

（イ）RIPEMD-160

[8] ：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、より長いハッシュ値のものを採用することができるのであれば、ハッシュ値が256ビット以上となるハッシュ関数を選択することが望ましい。ただし、例えば、公開鍵暗号の仕様上利用すべきハッシュ関数が指定されている場合やインターオペラビリティの必要性が生じる場合はこの限りではない。

安全性について、いまのところ問題は見つかっていない。

（ロ）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。

（ハ）SHA-256

安全性について、いまのところ問題は見つかっていない。

（ニ）SHA-384

安全性について、いまのところ問題は見つかっていない。

（ホ）SHA-512

安全性について、いまのところ問題は見つかっていない。

（４）擬似乱数生成系

（イ）PRNG in ANSI X9.42-2001 Annex C.1/C.2

パラメータが適切に設定された Annex C.1 については、今のところ、実用上の重大な問題点は見つかっていない。適切なパラメータの設定法については CRYPTREC Report 2002 の該当節を参照のこと。なお、Annex C.2 については強い攻撃法を仮定した場合の弱点が指摘されているので推奨できない。

（ロ）PRNG in ANSI X9.62-1998 Annex A.4

パラメータによっては擬似乱数出力分布について、PRNG for DSA in FIPS PUB 186-2 Appendix 3 を利用した DSA に対する攻撃に使われたと同様の大きな偏りが生じるので推奨できない。

（ハ）PRNG in ANSI X9.63-2001 Annex A.4

パラメータによっては擬似乱数出力分布について、PRNG for DSA in FIPS PUB 186-2 Appendix 3 を利用した DSA に対する攻撃に使われたと同様の大きな偏りが生じるので推奨できない。

（ニ）PRNG for DSA in FIPS PUB 186-2 Appendix 3

{0, 1}の分布の偏りを利用した 2^{64} の計算量と 2^{22} の既知署名を必要とする攻撃法が発表されている。

この攻撃法は DSA での擬似乱数の使用時に特定の一つの鍵の使用回数を 200 万回以下に抑えることで防御できるものの、擬似乱数としては乱数出力に大きな偏りが生じているので推奨できない。

（ホ）PRNG for general purpose in FIPS PUB 186-2 (+ change notice 1) Appendix 3.1

いまのところ、パラメータを適切に設定すれば、実用上の重大な問題点は見つかっていない。但し、仕様書中で定義されている使い方の中には安全とは言い切れない方法が含まれているので、利用の際には適切なパラメータの設定法については CRYPTREC Report 2002 の該当節を参照の上、適切な使い方を選択する必要がある。

（ヘ）PRNG in FIPS PUB 186-2 (+ change notice 1) revised Appendix 3.1

いまのところ、パラメータを適切に設定すれば、実用上の重大な問題点は見つかっていない。但し、仕様書中で定義されている使い方の中には安全とは言い切れない方法が含まれているので、利用の際には適切なパラメータの設定法については CRYPTREC Report 2002 の該当節を参照の上、適切な使い方を選択する必要がある。

なお、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。

３．３．電子政府推奨暗号リスト

暗号技術評価委員会から報告された暗号技術評価結果に基づき、第 4 回検討会会合（平成 14 年 11 月 27 日）において、電子政府推奨暗号リスト案を作成した。リスト案の作成にあたっては、2001 年度に暗号技術検討会の下に設置した「要件調査ワーキンググループ」における検討結果に基づき、暗号強度が十分高く、10 年間電子政府システムで安心して使えること、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、等を考慮した。

リスト案については、平成 14 年 11 月 28 日から平成 14 年 12 月 25 日まで、総務省及び経済産業省においてパブリックコメントを行った。その結果寄せられた意見等を第 5 回検討会会合（平成 15 年 2 月 12 日）において検討した結果、平成 15 年 2 月 20 日に、両省から電子政府推奨暗号リストとして公表された。（21 頁及び 22 頁にリストを掲載）

電子政府推奨暗号リストには、公開鍵暗号 9 方式（内訳：署名 4 方式、守秘 2 方式、鍵共有 3 方式）、共通鍵暗号 12 方式（内訳：64 ビットブロック暗号 4 方式、128 ビッ

トブロック暗号 5 方式、ストリーム暗号 3 方式)、ハッシュ関数 5 方式、擬似乱数生成系（例示）3 方式の計 29 方式が掲載された。また、利用の際に注意を要する暗号については、個別に注釈が付記された。

電子政府推奨暗号リストの決定を踏まえ、「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（第 2 章第 1 項参照)」に基づき、平成 15 年 2 月 28 日に、行政情報システム関係課長連絡会議において、各府省が情報システムの構築に当たり暗号を利用する場合には、可能な限り、電子政府推奨暗号リストに掲載された暗号の利用を推進する旨の「各府省の情報システム調達における暗号の利用方針」（参考資料参照）が了承された。

「各府省の情報システム調達における暗号の利用方針」では、今後、総務省及び経済産業省が、電子政府推奨暗号リストに掲載された暗号の安全性及び信頼性について今後の情報通信技術の進展を踏まえ必要に応じて評価する、とされており、両省は CRYPTREC において電子政府推奨暗号の監視を行っていくこととしている。詳細は第 5 章参照。

電子政府推奨暗号リスト

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注 1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注 2)
共通鍵暗号	64 ビットブロック暗号(注 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注 4)
	128 ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注 5)
その他	ハッシュ関数	RIPEMD-160(注 6)
		SHA-1(注 6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注 7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈：

(**注** 1)　SSL3.0/TLS1.0 **で使用実績があることから当面の使用を認める。**

(**注** 2)　KEM（Key Encapsulation Mechanism）-DEM(Data Encapsulation Mechanism)**構成における利用を前提とする。**

(**注** 3)　**新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、**128 **ビットブロック暗号を選択することが望ましい。**

(**注** 4)　3-key Triple DES **は、以下の条件を考慮し、当面の使用を認める。**

1) FIPS46-3 **として規定されていること**

2) **デファクトスタンダードとしての位置を保っていること**

(**注** 5) 128-bit RC4 **は、**SSL3.0/TLS1.0 **以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。**

(**注**6) **新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、**256**ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。**

(**注**7) **擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。**

３．４．電子政府推奨暗号の仕様に関する情報提供

電子政府推奨暗号リストにおいては、CRYPTREC で評価・選定した暗号の暗号名のみを掲載しているところであるが、その暗号名に対応する暗号の仕様を一意に保つ必要ある。また、電子政府推奨暗号の調達を円滑に行うためには、調達担当者が電子政府推奨暗号の仕様を容易に入手できることが必要である。しかし、各電子政府推奨暗号の仕様の管理者は CRYPTREC ではなく、応募暗号の提案元又は NIST 等であるため、以下のような方策により、調達担当者に仕様に関する情報を提供することとした。

（イ）電子政府推奨暗号の仕様を可能な限りTAO及びIPAのホームページに掲載する。

（ロ）電子政府推奨暗号のうちその仕様をTAO及びIPAのホームページに掲載することができないものについては、当該暗号の仕様を参照することのできるホームページのＵＲＬ、あるいは、その仕様を参照する方法をTAO及びIPAのホームページに掲載する。

（ハ）（ロ）の場合であって、当該暗号の仕様を参照することができなくなった場合には、その旨を TAO 及び IPA のホームページに掲載する。

４．暗号調達のためのガイドブックについて

４．１．暗号調達ガイドブック作成 WG 設置の目的

電子政府推奨暗号リストの決定により、電子政府において安全性及び信頼性に優れた暗号アルゴリズムを採用することが可能になった。しかし実際に、各府省の調達担当者が、利用目的に合った暗号アルゴリズムを電子政府推奨暗号リストから適切に選択するためには、調達するシステムにおける暗号の利用目的の抽出から、暗号アルゴリズムの選定までの手順を分かりやすく示す手引書が望まれるところである。

そこで、暗号技術検討会の下に、暗号研究者、セキュリティの専門家及びシステム開発の専門家から構成される「暗号調達ガイドブック作成 WG（以下「ガイドブックWG」という。リーダ：佐々木良一東京電機大学教授）」を平成 14 年 5 月に設置し、暗号技術評価委員会及び公開鍵暗号／共通鍵暗号評価小委員会の協力を得つつ、各府省の調達担当者が適切な電子政府推奨暗号を円滑に調達するための「暗号調達のためのガイドブック（以下、ガイドブック）」を作成した。

４．２．ガイドブック作成の進め方

４．２．１．対象とする読者

ガイドブックの作成にあたっては、各府省における電子政府システムの調達の担当者が読者となることを想定するとともに、暗号やセキュリティに関する知識があまり豊富でない読者でも理解できるような記述レベルを目指すことにした。

４．２．２．盛り込む内容

上記のような読者を対象とすることから、ガイドブックには以下のような内容を盛り込むことにした。

（１）暗号の利用目的の抽出から暗号アルゴリズムの選定までの手順の解説
（２）電子政府推奨暗号及び電子政府推奨暗号リストの解説
（３）調達仕様書作成にあたり、暗号に関連して留意すべき点

４．２．３．ISO/IEC15408 を活用した調達との関連

セキュリティに関する信頼度の高い情報システムの構築については、既に「可能な限り ISO/IEC15408 に基づいて評価又は認証された製品等の利用を推進する」旨の省庁間合意が成されている。ただし、ISO/IEC15408 では、暗号技術の選択に関する要件については触れられていない。

そこで、セキュリティに関する諸要件と暗号に関する要件をそれぞれ指定して調達を進める場合は、本ガイドブックと「ISO/IEC15408 を活用した調達のガイドブック（経済産業省情報セキュリティ政策室発行）」を並行して参照することを意図した。

４．２．４．検討方法

上記の内容について、以下の手順及び方法により検討を行った。また、暗号アルゴリズムの解説をはじめ、技術的な内容の記述に関しては、暗号技術評価委員会及び公開鍵暗号／共通鍵暗号評価小委員会の協力を得た。

（１）調達担当者及び情報システム担当者へのヒアリング

検討に先立ち、システム調達（特に暗号調達）についての現状、及び、ガイドブックに対する要望を把握するため、各府省の調達担当者及び情報システム担当者へのヒアリングを行った。また、ガイドブックの原案を作成した時点で再びヒアリングを行い、記述内容に関するコメントを求めた。

（２）海外の電子政府の事例に関する調査

海外の電子政府システムにおける、暗号調達ガイドラインの事例を調査した。

（３）作業委員会による編集

ガイドブックＷＧの下に作業委員会を設置し、上記ヒアリング及び事例調査等に基づいてガイドブック原案の作成作業を集中的に行った。同委員会は平成 14 年 6 月から 8 月まで計 7 回開催した。

４．２．５．WG 会合の開催状況

【第 1 回】　5 月 22 日（水）
（主な議題）会合開催スケジュール、検討事項、目次案及び作業事項の確認
【第 2 回】　7 月 8 日（月）
（主な議題）ガイドブック骨子案の検討、海外電子政府事例の確認
【第 3 回】　7 月 19 日（金）
（主な議題）ガイドブック一次案の検討
【第 4 回】　9 月 3 日（火）
（主な議題）ガイドブック最終案の検討
【第 5 回】　9 月 24 日（火）
（主な議題）ガイドブック最終案の検討
【第 6 回】　11 月 19 日（火）
（主な議題）ガイドブック案の決定

４．３．ガイドブックの概要

４．３．１．システム全体の検討作業と暗号調達作業との関わり

暗号は、情報システムの構築作業の中でセキュリティ対策の一部として利用されるので、暗号を調達するにあたっては、その前段としてリスク分析を行うことにより、どんな目的で暗号を利用すべきか、整理をしておく必要がある。（図１）

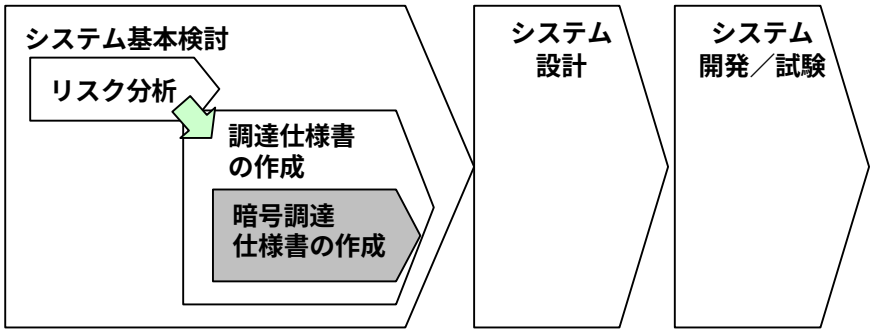


図１　システム構築作業の流れ及び暗号調達の位置付け

このリスク分析に基づき、システムに必要となる暗号アルゴリズムを選定していくことになるが、その手順は図 2 に示すようなものになる。ガイドブックでは、この手順に沿って、暗号調達、及び、この手順を進める上で必要となる技術的概念である暗号利用形態及び暗号技術分類に関する解説、電子政府推奨暗号に選定された各暗号アルゴリズムの概要について記述した。

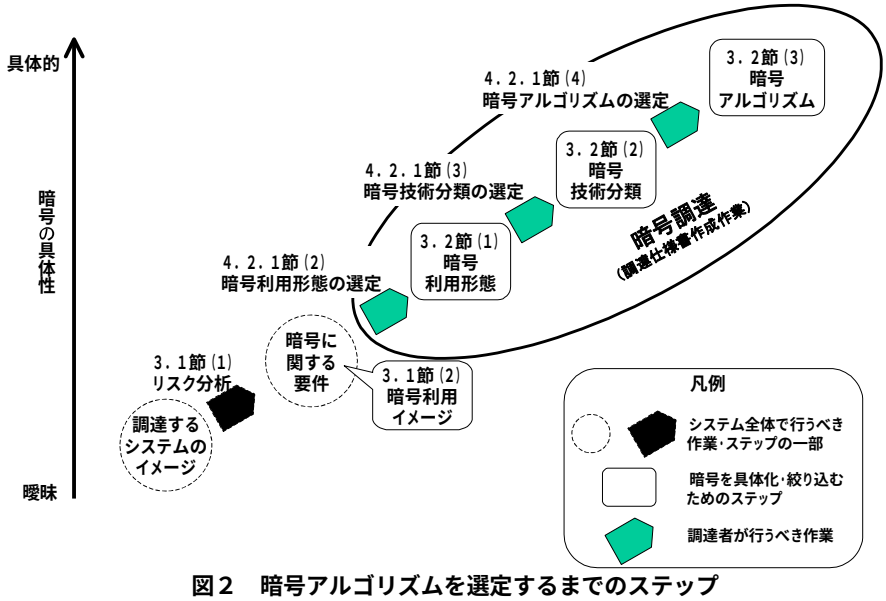


図２　暗号アルゴリズムを選定するまでのステップ
（図中の数字はガイドブック本文の節番号に対応）

４．３．２．電子政府システムにおける暗号利用イメージ

e-Japan 重点計画-2002 に挙げられている電子政府の主な項目のうち、「電子申請」「電子調達」、「電子納付」、「電子情報提供」、の各システム及び「政府認証基盤」における暗号利用イメージ図及び説明を記載した。

４．３．３．暗号利用形態及び暗号技術分類

電子政府システムにおける暗号の利用目的を分類したものである「暗号利用形態」と、暗号アルゴリズムを機能的、技術的に整理したものである「暗号技術分類」についての解説を記載した。

４．３．４．電子政府推奨暗号の概要

電子政府推奨暗号に選定された暗号アルゴリズム 29 方式の概要説明、及び、利用にあたっての注意点等を記載した。

４．３．５．暗号調達の手順に関する説明

暗号アルゴリズムを選定するための作業について、調達担当者及び情報システム担当者へのヒアリング等を基に、2 通りのモデル化を行い、それぞれについて解説した。

（１）暗号調達の流れ

電子政府システムの調達の流れ（図 3 及び図 4）の中で、調達者はシステムに必要な暗号の要件を明確化し、電子政府推奨暗号リストの中から暗号アルゴリズムを絞り込む必要がある。暗号アルゴリズムを絞り込む作業の進め方は、以下に挙げる 2 つのモデルが考えられる。

（イ）調達者指定モデル

調達仕様書の作成時に、調達するシステムについて詳細に説明し、その中で、電子政府推奨暗号リストから暗号アルゴリズムを指定する方法

（ロ）提案審査モデル

調達仕様書では、暗号については概略を説明するに止め、業者に電子政府推奨暗号リストから暗号アルゴリズムを選択させ、提案資料を見て審査する方法

上記 2 モデルのうち、調達者指定モデルは仕様書作成段階で暗号への要件を詳細化することが必要となり、提案審査モデルでは提案書受領後の審査段階で同様の作業が必要となる。よって、暗号調達に関して必要となる、調達者の作業は、システム調達全体を通して同等になると考えられる。

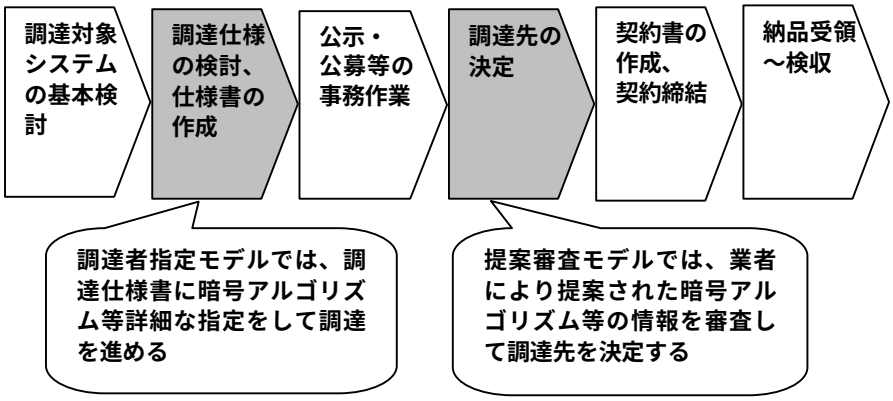


図３　システム調達の流れ及び両モデルの位置付け

調達の流れ	作　業　概　要
調達対象システムの基本検討	システムの背景、目的、対象範囲、構築条件、概算費用等、調達を進める基本的事項の整理、その他、暗号に関連した作業として、リスク分析等が行なわれる
調達仕様の検討、仕様書の作成	システムへの要件となる事項の具体化検討と仕様書の作成（必要に応じて、パブリックコメントを募集する場合がある）
公示・公募等の事務作業	公示・公募、提案の受付などの事務作業
調達先の決定	調達システムに適合する提案をした業者を選定
契約書作成、契約締結	調達システムの特記事項等を盛り込んで、契約書を作成、契約を締結
納品受領～検収	調達したシステムを受領、仕様と相違ないことを確認検収

図４　　システム調達の流れにおける作業の概要

（２）調達者指定モデルによる調達仕様書の作成

調達者指定モデルにおける暗号調達の流れを図５に示す。調達者は、リスク分析の結果等、調達対象システムの基本検討の結果を把握した上で、暗号利用形態の選定、暗号利用分類の選定、暗号アルゴリズムの選定、の順で作業を進め、暗号調達仕様書を完成する。

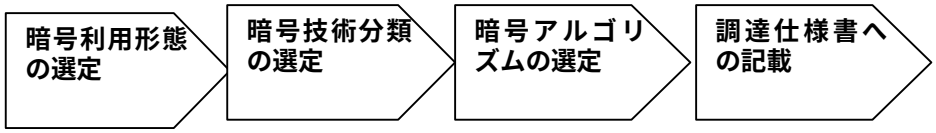


図５　調達者指定モデルにおける暗号アルゴリズム選定までの流れ

（イ）暗号利用形態の選定

ガイドブックでは、システムの基本検討におけるリスク分析等の様々な作業の一貫として暗号利用形態の選定が行われることを想定し、一般的なセキュリティ

上の脅威に対して、暗号利用形態を選定する場合の基本的な考え方を示した。

（ロ）暗号技術分類の選定

暗号利用形態の決定後、調達するシステムの目的や特性を考慮して暗号技術分類を選択する。ガイドブックでは、暗号利用形態別に、共通鍵暗号と公開鍵暗号のそれぞれがよく用いられる事例等について説明した。

（ハ）暗号アルゴリズムの選定

暗号技術分類の決定後、電子政府推奨暗号リストの中から、暗号技術分類別に１つ又は必要な数の暗号アルゴリズムを選択する。ガイドブックには参考資料として、アルゴリズム安全性評価結果（リストに載せた根拠）、主なパラメータ・補助関数に関する要件、国際標準への対応等について一覧表にまとめた「評価・特徴一覧」を掲載した。なお、主な留意点又は着目すべき点は以下のとおり。

（ａ）実装方法によっては、電子政府推奨暗号を使用したとしても様々な実装攻撃に曝される危険性を排除できないので、実装攻撃の脅威に対する十分な配慮、検討を行い、適切な対策を施して実装するよう注意する必要がある。

（ｂ）公開鍵暗号は、暗号利用形態に応じて、プロトコル標準への採用の有無等を考慮して選択する。なお、許容される処理速度の範囲で、使用される鍵長（RSA 暗号の場合、2 つの素数の積となる合成数のビット数）を長くする（RSA 暗号の場合は 1024 ビット以上にする）などの検討が必要である。また、各アルゴリズムの数論的困難性を確保するため、パラメータの選択に十分留意する必要がある。

（ｃ） 共通鍵暗号は、処理速度、メモリ制限環境での実装性、プロトコル標準への採用の有無等を考慮して選択する。ブロック暗号を選択する場合、安全性の面から今後は可能な限りブロック長 128 ビットの暗号を使用する。なお、ブロック暗号を利用した暗号化処理に関連して、暗号利用モード（Modes of Operation）と呼ばれる技法がいくつか規定されており、各モードごとに実現している目的や機能が異なるので、実装環境や利用用途に応じて、適切な暗号利用モードを選択する必要がある。

（ｄ）ハッシュ関数は、可能であれば 256 ビット以上の長さのハッシュ値を出力するものを選択することが望ましい。ただし、既に選択した公開鍵暗号又は共通鍵暗号の仕様書でハッシュ関数が指定されている場合は、その中から選択する。

（ｅ）擬似乱数生成については、リストに掲載されている以外の「暗号学的に安全な擬似乱数アルゴリズム」を利用することができる。また、リストに掲載されている暗号アルゴリズムの仕様自体に特定の擬似乱数生成アルゴリズムの使用が規定されている場合は、その使用を妨げるものではない。

（ニ）調達仕様書への記載

上記のような手順により選択した暗号アルゴリズムを、どのように調達仕様書に記載するかを例示した。（図 6）

暗号による保護を必要とする情報	暗号利用形態	暗号アルゴリズム
・申請データ	守秘	*共通鍵暗号その１*
・申請内容確認で授受されるデータ 到達確認通知 ・状況確認で授受されるデータ	相手認証	*公開鍵暗号その１* または *公開鍵暗号その３*
・審査終了通知 ・許認可等公文書の取得要求データ ・許認可等公文書	署名	*公開鍵暗号その１* または *公開鍵暗号その３*
・鍵情報	鍵共有	*公開鍵暗号その２*
上記暗号アルゴリズムにて 特に指定の無い場合は 右記アルゴリズムを使用すること	ハッシュ関数として	*ハッシュ関数その１*
	擬似乱数生成として	*擬似乱数生成その１*

図 6　　電子申請システムにおける暗号アルゴリズム指定表の記載例[9]

（３）提案審査モデルによる調達仕様書の作成

提案審査モデルの場合、調達者は調達仕様書に下記項目を記載する。

（イ）電子政府推奨暗号の使用に関する指示

調達するシステムには、可能な限り電子政府推奨暗号を使用するよう、提案を行う業者に指示する。

（ロ）暗号アルゴリズム選定理由の明記に関する指示

提案書の審査において、調達者は、暗号アルゴリズムの選定が妥当であることを検証する必要があるため、調達するシステムのイメージから暗号アルゴリズム選定までの過程を、理由を付けて分かりやすく説明した文書を提案書に添付するよう、調達を行う業者に指示する。

9 ：実際の調達においては、サンプル自体を引用するのではなく、個別具体的な状況に応じた適切な調達を行うこと

４．３．６．調達仕様書作成上の留意点

調達者が調達仕様書を作成する際に留意すべき点を記載した。

（１）複数暗号アルゴリズムの実装について

電子政府システムにおけるサーバや、パソコン等に複数の暗号アルゴリズムを同時に実装する場合、セキュリティ面だけ考えると以下のようにいえる。

（イ）複数暗号実装のメリット

電子政府推奨暗号リストに掲載される暗号アルゴリズムにおいては暗号解読問題発生の可能性が低いとはいえ、1 つの暗号アルゴリズムが解読された場合に備えて、複数の暗号を実装し切り替えられるようにすることは、セキュリティを向上する上で有効である。

（ロ）複数暗号実装のデメリット

複数の暗号アルゴリズムを同じシステムに実装し、これを切り替えて利用できるように作り込んだ場合、切り替え部分等にセキュリティホールが混入してしまう恐れがある。そのため脆弱性が上昇し、セキュリティが減少する可能性がある。

（ハ）対応策

したがって、セキュリティ脆弱性の上昇により懸念されるリスクが、暗号アルゴリズムが解読されるリスクに比べて小さいと判断された場合にのみ、複数暗号アルゴリズムを実装すべきである。

なお、インターネットなどを通じて広く一般国民が利用するシステムにおいて、利用者の利用する暗号アルゴリズムが全体として 1 つに特定できない場合などには、政府側のサーバ装置で、複数の暗号アルゴリズムをどちらでも扱えるようにしておかなければならない場合がある。このような場合には、セキュリティホールを作りこまないよう十分な配慮をしつつ複数暗号を実装しておくことが利用者の利便性を向上させる上でも望ましい。

（２）暗号プログラムの配布と外国為替及び外国貿易法による暗号輸出規制

不特定多数の利用者に、暗号機能を含むプログラムを配布することは、ワッセナーアレンジメントに基づき、外国為替及び外国貿易法による規制がある。

ガイドブックでは、電子政府システムにおいて不特定多数の利用者に暗号機能を含むプログラムを配布する場合の、法制度上の留意点について解説した。

４．３．７．調達先の決定、契約及び納品

調達仕様書に基づき提出される提案書の審査、調達者の決定、契約、納品における、

暗号調達の観点からの留意点を記載した。

４．３．８．参考資料

（１）各府省の情報システム調達における暗号の利用方針

電子政府推奨暗号の利用に関する府省間合意文書を掲載した。

（２）電子政府推奨暗号の評価・特徴一覧

電子政府推奨暗号の、アルゴリズム安全性（リストに載せた根拠）、主なパラメータ・補助関数に関する要件、国際標準等への採用状況等に関する情報を、一覧表にして掲載した。

５．今後の CRYPTREC 活動について

CRYPTREC では、発足以来の当面の目標であった、電子政府推奨暗号リストの策定及び暗号調達のためのガイドブックの作成を行った。しかし、国民が安心して電子政府を利用できるようにするためには、電子政府の安全性及び信頼性を確保するための活動を引き続き推進していく必要があり、CRYPTREC としても、それに貢献していくことが重要であるとの認識に立っている。そこで、2003 年度以降、以下のような活動を行っていくこととした。

５．１．今後の CRYPTREC の活動目的及び活動内容

５．１．１．活動目的

CRYPTREC は、暗号技術及び暗号関連技術の評価等を通じて、電子政府等の安全性及び信頼性の確保に貢献することを目的として活動する。

５．１．２．活動内容

CRYPTRECは、2003年度以降、以下の活動を行う。なお、今後、新たに必要と考えられる事案が生じた場合には、その都度、暗号技術検討会において具体的な活動内容を検討していくものとする。

（１）電子政府推奨暗号の監視

電子政府推奨暗号に選定された各暗号の安全性等についての情報収集や評価を行い、必要に応じて修正情報の周知やリストからの削除等の電子政府推奨暗号リストの変更を行う。

（２）電子政府推奨暗号の安全性及び信頼性確保のための調査・検討

（イ）暗号アルゴリズム等を主な対象とする調査・検討

暗号アルゴリズムや素因数分解問題等の数論的問題の困難性を主な対象とする調査及び検討を行う。

（ロ）暗号実装関連技術を主な対象とする調査・検討

実装攻撃等の暗号実装関連技術を主な対象とする調査及び検討を行う。

（３）電子政府推奨暗号リストの改訂に関する調査・検討

将来の電子政府推奨暗号リストの改訂（新たな電子政府推奨暗号リストの策定及び本件電子政府推奨暗号リストの廃棄）のために必要な調査及び検討（電子政府における暗号利用状況調査等）を行う。その際、総務省、経済産業省及び行政情報シ

ステム関係課長連絡会議との連携を図ることとする。

（４）暗号モジュール評価基準の作成

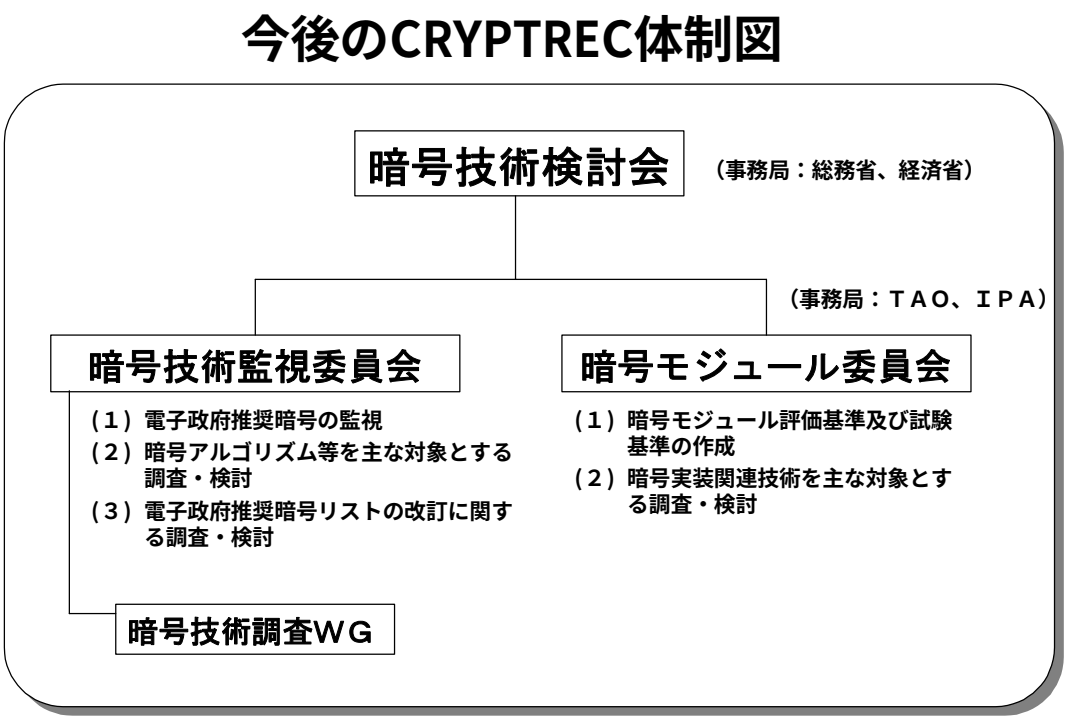
暗号モジュール評価基準及び試験基準を作成する。

５．２．今後の CRYPTREC 体制

2003 年度以降、当面の CRYPTREC の体制として、暗号技術検討会は存続し、暗号技術検討会の下に「暗号技術監視委員会」及び「暗号モジュール委員会」を設置する。また、暗号技術監視委員会の下に「暗号技術調査 WG」を設置する（図 7：今後の CRYPTREC の体制図）。

従来の暗号技術評価委員会は暗号技術監視委員会に発展的に再編することとする。また、公開鍵暗号評価小委員会及び共通鍵暗号評価小委員会は暗号技術調査ＷＧに再編することとする。

各委員会及びＷＧの位置づけ、構成及び機能は以下のとおり。



（図 7）

５．２．１．暗号技術検討会

暗号技術検討会（「検討会」）は、電子政府推奨暗号リストに掲載された暗号技術の

監視、関連する調査研究、及び、暗号技術の危殆化や暗号プロトコル等その他暗号技術の評価・利用等に関する事項について、総合的な観点から検討を行う。また、電子政府等のセキュリティの確保のため、政府のセキュリティ関係機関等との連携、調整を図る。

５．２．２．暗号技術監視委員会

暗号技術監視委員会（以下、「監視委員会」）は検討会の下に設置される。監視委員会は、数名の有識者等により構成され、安全性及び信頼性確保の観点から、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討を適宜行うとともに電子政府推奨暗号リストの改訂に関する調査・検討を行う。なお、監視委員会の日常業務を行う監視要員をTAO／通信総合研究所（CRL）（両機関は2004年4月に統合予定）及びIPAに配置する。

（１）暗号技術調査WG

（イ）暗号技術調査WG（以下、「調査WG」）は、電子政府推奨暗号リストの変更案等の作成、及び電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする具体的な調査・検討に際して監視委員会を支援することを目的として、監視委員会の下に設置される。

（ロ）調査WGは、監視委員会委員、従来の暗号技術評価委員会委員、共通鍵暗号評価小委員会委員及び公開鍵暗号評価小委員会委員等を元に構成される。これらのWGメンバーは、共通鍵暗号評価グループ及び公開鍵暗号評価グループに区分される。監視委員会は、事案の性質に応じて、共通鍵暗号評価グループ及び／または公開鍵暗号評価グループを召集し、調査WGを開催する。調査WGは、監視委員会に対して電子政府推奨暗号リストの変更案等の作成に関する専門的助言を行う。

（ハ）その他、調査WGは、監視委員会の要望により事案に応じて開催され、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする具体的な調査・検討（電子政府における暗号利用状況調査等）を行い、監視委員会に対して専門的な助言を行う。

５．２．３．暗号モジュール委員会

暗号モジュール委員会は検討会の下に設置される。暗号モジュール委員会は、ISO/IEC等の国際標準の動向を注視しつつ、将来的に政府調達基準等として利用され得ることをも視野に入れながら、2005年3月を目処に暗号モジュール評価基準及び試験基準を作成する。また、電子政府推奨暗号の安全性及び信頼性確保のための、主として暗号実装関連技術等を対象とする調査・検討を行う。

５．３．電子政府推奨暗号の監視

５．３．１．電子政府推奨暗号の監視の基本的考え方

今後、CRYPTRECは、電子政府推奨暗号の安全性及び信頼性を確保することを目的とし、継続的に暗号技術に関する情報を収集し、必要に応じて暗号の安全性を評価する電子政府推奨暗号の監視活動を行う。

監視は、以下のような考え方に基づいて実施することとする。

（１）実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。

（２）電子政府推奨暗号の仕様変更は原則として認めない。

（３）電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

５．３．２．電子政府推奨暗号の監視の具体的内容

電子政府推奨暗号の監視は、調査研究、リストからの削除、修正情報の周知等からなる。それぞれの具体的内容は以下（１）～（４）のとおりとする。

（１）暗号技術調査・研究及びデータの蓄積

暗号技術に関する調査研究を実施し、国際標準化の動向等種々のデータを蓄積する。

（２）電子政府推奨暗号の削除

（イ）電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、かつ当該暗号の仕様を変更すること無く攻撃を回避することが不可能であると判断される場合には、当該暗号をリストから削除する。

（ロ）電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、かつ当該暗号の仕様を変更すること無く、パラメータの修正等の簡易な修正を行うことによって攻撃を回避することが可能であると判断される場合であっても、その方法等を記述した修正情報が当該暗号の仕様書の管理者より提案されない場合には、当該暗号をリストから削除する。

（３）電子政府推奨暗号に関する修正情報の周知

（イ）電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、電子政府推奨暗号の仕様変更ではなくパラメータの修正等の簡易な修正を実施することにより当該攻撃を回避することができると判断される場合には、当該修正方法を修正情報として周知する。

（ロ）（イ）の場合において、修正情報は仕様書の管理者から提案させることとし、監視委員会は、提案された修正情報を加味して当該電子政府推奨暗号の安全性評価を実施する。仕様書の管理者より修正情報の提案がなされない場合には、当該暗号をリストから削除する。

（ハ）監視委員会は応募暗号[10]以外の電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いとは判断していないにも関わらず、当該暗号に関する修正情報が仕様書の管理者により発行された場合であって（パラメータ修正等の簡易な修正に限る）、監視委員会が当該修正情報を加味した上で安全性評価を実施し、安全性が確保されていると判断する場合には当該修正情報を周知する。

（４）電子政府推奨暗号の追加

（イ）電子政府推奨暗号リストの改訂（新たな電子政府推奨暗号リストの策定及び本件電子政府推奨暗号リストの廃棄）が行われるまでは、電子政府推奨暗号の追加は例外的な扱いとする。

（ロ）電子政府推奨暗号リストに掲載されていない暗号が国際的に高い評価を得ている場合であって、暗号技術検討会が当該暗号を新たに評価することが必要と判断し、かつ、評価の結果、暗号技術検討会が当該暗号を電子政府推奨暗号リストへ掲載することが適切と判断する場合には、当該暗号を電子政府推奨暗号リストへ追加する。

（ハ）電子政府推奨暗号リストへの追加を検討する場合には、「10年間は安心して利用できる」という観点から評価を行う。

---

[10] ：応募暗号：電子政府推奨暗号のうち、以下のものを指す。
（公開鍵暗号）ECDSA，RSA-PSS，RSA-OAEP，ECDH，PSEC-KEM
（共通鍵暗号）CIPHERUNICORN-E，Hierocrypt-L1，MISTY1，
Camellia，CIPHERUNICORN-A，Hierocrypt-3，SC2000，
MUGI，MULTI-S01

（ニ）電子政府調達者より、電子政府推奨暗号リストに無い新たな用途及び当該用途に適した暗号の追加に関する要望がよせられた場合であって、かつ、暗号技術検討会としても当該用途の追加が適切と判断した上で、それに適した暗号の評価を実施し、その結果、適切な暗号を選定した場合には、当該用途及び当該暗号を電子政府推奨暗号リストへ追加することとする。

５．３．３．電子政府推奨暗号の監視の手順

電子政府推奨暗号の監視の手順は、（１）監視委員会における情報収集、（２）監視委員会における情報分析、（３）監視委員会及び検討会における審議及び決定の３段階からなる。具体的には以下のとおりとする。

（１）監視委員会における情報収集

監視委員会において、電子政府推奨暗号の安全性に関する情報を迅速かつ円滑に入手するためには、監視委員会自らが情報収集を行うだけでなく、過去3年間のCRYPTREC活動によって形成された、暗号研究者とのネットワークを活用することが重要である。そこで、以下のように情報収集を行うこととする。

（イ）国内外の学会等への参加等を通じて暗号技術に関する情報（学術論文、発表原稿等）を収集する。
（ロ）暗号技術調査WGメンバー等との連絡体制を整備し、同メンバーから恒常的に情報提供を受ける。
（ハ）応募暗号については、原則として応募元から情報提供を受ける。
（ニ）その他一般からの情報提供も受ける。

（２）監視委員会における情報分析

監視委員会は、（１）により収集された情報を分析し、電子政府推奨暗号の削除等を検討すべき事態が発生しているか否か判断する。その結果、監視委員会が電子政府推奨暗号の削除等を検討すべき事態が発生していると判断する場合には、事案に応じて、暗号技術調査ＷＧの共通鍵暗号評価グループおよび／または公開鍵暗号評価グループを召集し、暗号技術調査ＷＧを開催する。ただし、監視委員会が、電子政府推奨暗号の削除等を直ちに行うべき事態が発生していると判断する場合は、その緊急性に応じた対応を実施する。

（３）監視委員会及び検討会における審議及び決定

（イ）暗号技術調査WGは、技術的観点から、監視委員会に対して助言を行う。なお、暗号技術調査WGは、応募元等より修正情報の提供を受け、同修正情報

を加味した暗号の安全性評価も行う。

（ロ）監視委員会は、暗号技術調査WGの助言を踏まえて、電子政府推奨暗号の削除等を実施するか否かについて素案を作成し、暗号技術検討会に報告する。

（ハ）暗号技術検討会は、総合的な観点から当該素案を審議し電子政府推奨暗号の削除等に関する案を作成する。同案が電子政府推奨暗号リストに変更を加えるものである場合、総務省及び経済産業省はパブリックコメントに付し、その結果を暗号技術検討会に報告する。暗号技術検討会は、パブリックコメントの結果を踏まえて、電子政府推奨暗号の削除等に関する案を決定する。

（ニ）暗号技術検討会の決定に基づいて電子政府推奨暗号リストの変更を行った場合、総務省及び経済省は、電子政府推奨暗号リストの変更について行政情報システム関係課長連絡会議等に連絡する。

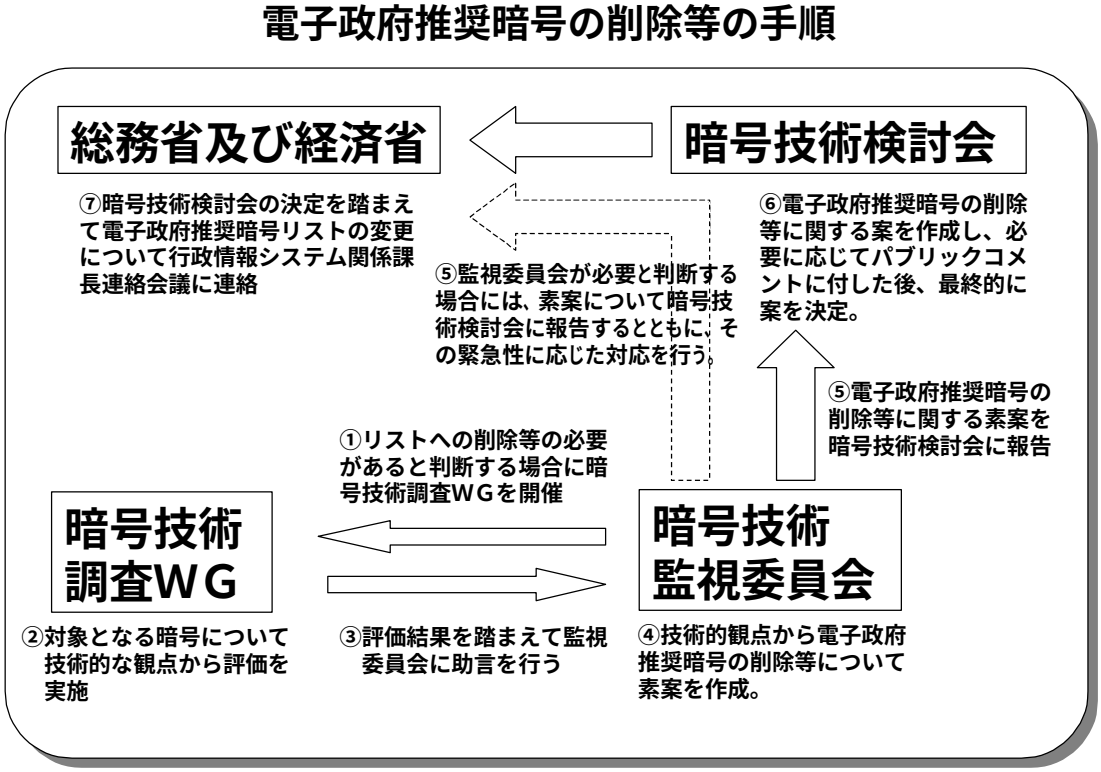


図８：電子政府推奨暗号削除等の手順

５．４．電子政府推奨暗号リストの改訂

５．４．１．基本的認識

電子政府推奨暗号は、現時点において、今後 10 年間は安心して利用できるという観点から選定された暗号である。しかし、暗号に対する解析や攻撃の技術や手法はますます高度化しており、電子政府推奨暗号は常に危殆化の危険にさらされている。一方、新たな暗号の開発も進んでおり、今後、安全性や実装性に優れた新しい暗号の出現が期待されるところである。そこで、危殆化した暗号の削除や新しい暗号の選定等により、電子政府推奨暗号リストを一定期間毎に改訂することが望ましい。改訂を実施する際に、仮に公募を実施する場合は、公募のアナウンス（公募開始時期、公募期間、評価期間、新リスト発表時期等の公表）から新リストの策定まで、5 年程度の期間をかけることが望ましい。

５．４．２．基本的考え方

リストの改訂作業の具体的な実施内容については、電子政府の導入状況及び電子政府推奨暗号の監視状況を考慮しつつ、然るべきタイミングで検討を行うこととする。なお、リスト改訂作業の実施方法としては、現在のところ、以下のような検討事項が想定されるところである。

（想定される検討事項）

（イ）公募の要否

（ロ）リスト項目（技術分類等）の見直し

（ハ）項目別の掲載暗号数

（ニ）評価基準、評価方法

また、改訂作業の具体的な開始時期については、2003年度以降に暗号技術検討会において検討の上決定するが、改訂作業の完了及び新リストの決定は、遅くとも10年後の2013年までとする。なお、仮に公募を実施するとした場合は、5年程度の期間をかけることが望ましいと考えられることから、遅くとも2008年3月頃には公募のアナウンスを行うことが望ましい。

５．５．暗号モジュールに関する検討

電子政府の安全性及び信頼性を確保するためには、暗号技術レベルの安全性だけでなく暗号技術の実装の安全性を確保する必要があり、この観点から暗号モジュールの安全性評価基準を作成することが急務である。他方、暗号モジュールの安全性評価基準に関しては、米国が自国の政府調達基準であるFIPS140-2のISO/IEC化を提案しており、暗号モジュールの安全性評価基準を我が国において作成するにあたっては、ISO/IEC等にお

ける議論を注視していく必要がある。

このような状況を踏まえて、検討会の下に暗号モジュール委員会を設置する。暗号モジュール委員会は、ISO等の国際標準の動向を注視しつつ、将来的に政府調達基準等として利用され得ることをも視野に入れながら、2005年3月を目処に暗号モジュール評価基準及び試験基準を作成する。

なお、暗号モジュール委員会は、暗号技術監視委員会と連絡をとりつつ、電子政府推奨暗号の安全性及び信頼性確保のための暗号実装関連技術を主な対象とする調査・検討を併せて行うこととする。

資料「暗号調達のためのガイドブック」

暗号調達のためのガイドブック

平成１５年３月

暗号技術検討会

暗号調達ガイドブック作成ワーキンググループ

目次

１．　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 重点計画及び e-Japan 重点計画-2002 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である。

このため、総務省及び経済産業省は、平成１３年５月から「暗号技術検討会（座長：今井秀樹東京大学教授）」を開催し、電子政府利用等に資する暗号技術の評価等を実施してきた。なお、従来は「暗号技術評価委員会（委員長：今井秀樹東京大学教授）」をＣＲＹＰＴＲＥＣと称したが、平成１４年度からは「暗号技術検討会」及び、「暗号技術評価委員会」の両者を含めて、ＣＲＹＰＴＲＥＣ（Cryptography Research and Evaluation Committees）プロジェクトとして暗号技術の評価等の活動を継続している。その活動の成果として、安全性が客観的に評価され、実装性に優れた暗号技術が、電子政府における調達のための推奨すべき暗号（電子政府推奨暗号）としてリスト化（電子政府推奨暗号リスト）された。各府省は、「各府省の情報システム調達における暗号の利用方針（平成１５年２月２８日、行政情報システム関係課長連絡会議了承）」（以下、「連絡会議了承」）により、各府省における暗号技術の利用方針について合意したところである。

各府省が電子政府システムを構築する際、電子政府推奨暗号リストを活用し、適切な暗号を調達することが重要であることから、総務省及び経済産業省は、適切な電子政府推奨暗号を調達するための手引書として「暗号調達のためのガイドブック」を作成した。

２．　本ガイドブックの利用にあたって

電子政府システムにおける重要な課題である情報セキュリティを確保するための方策として、暗号技術の利用が考えられる。「連絡会議了承」では、各府省が電子政府システムで利用する暗号を調達する際には、電子政府推奨暗号リストに掲載された暗号アルゴリズムを可能な限り利用する旨、合意されている。

本ガイドブックの目的は、各府省の調達担当者が、適切な暗号アルゴリズムを円滑に調達することができるよう、一つの道筋を示すことである。なお、本ガイドブックに引用されている掲載例はあくまでも一つの参考であり、各府省の調達担当者が実際に調達を実施するにあたっては、掲載例自体を引用するのではなく、掲載例を参照しつつ個別の具体的な状況に応じた適切な調達を実施する必要がある。

２．１　本ガイドブックについて

（１）「暗号調達のためのガイドブック」とは

「暗号調達のためのガイドブック」は、電子政府システムの調達に際し、暗号技術を利用したセキュリティ確保が必要な場合に、調達者が効率的に電子政府推奨暗号の調達を進められるよう、調達における電子政府推奨暗号リストの利用手順や考え方について説明するものである。（図２．１－１参照）

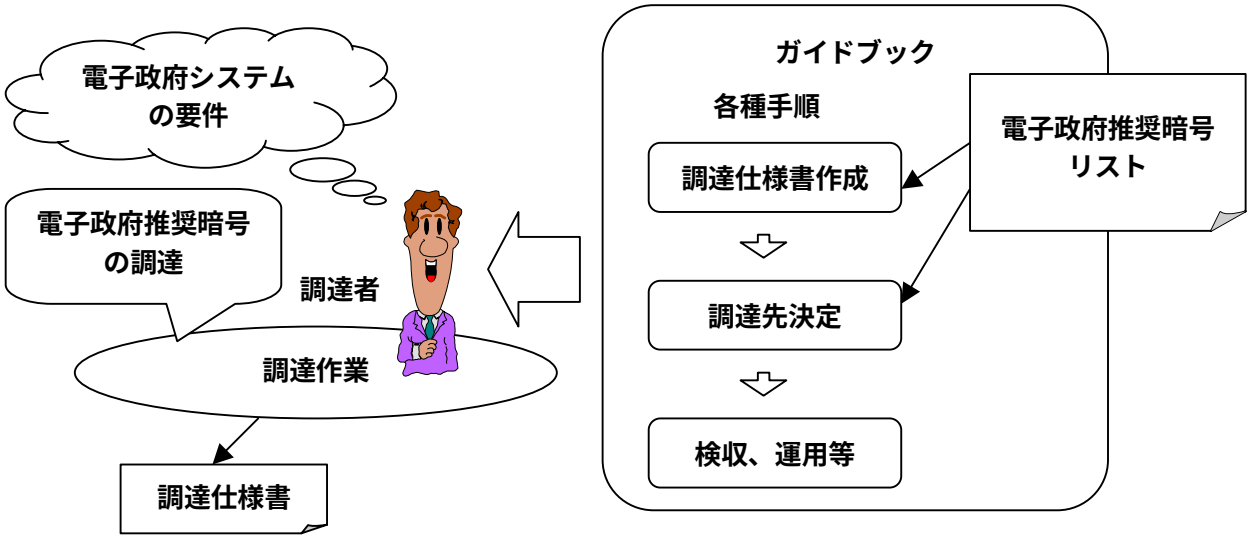


図２．１－１　本ガイドブックの位置付け

（2）本ガイドブック利用のメリット

本ガイドブックは、電子政府システムの構築の際、電子政府推奨暗号リストを活用して効率的に電子政府推奨暗号を調達することを目的として作成された。本ガイドブックを利用することにより、以下のようなメリットが得られる。

- 調達に必要な暗号関連の技術や用語の概要が把握できる。
- ガイダンスに沿って電子政府推奨暗号の調達を進められる。

２．２　本ガイドブックの位置付け

ここでは、本ガイドブックと関係の深い電子政府推奨暗号リスト、及び、情報機器等の情報セキュリティ関連国際規格である ISO/IEC15408 と本ガイドブックの関係について説明する。

（1）電子政府推奨暗号リストについて

本ガイドブックにおいて利用を推奨する電子政府推奨暗号リストは、以下の想定のもとに、電子政府推奨暗号を技術的観点から分類し、リスト化したものである。

- 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、政府内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。）
- 耐用期間：１０年間は安心して利用できる暗号アルゴリズムを想定する。
- リストの見直し：　今後の電子政府推奨暗号の電子政府における利用状況等も踏まえ、平成１５年度以降、CRYPTREC において具体的に検討する。

（２）ISO/IEC15408 を活用した調達と暗号調達の関連について

セキュリティ関連のシステム調達に関するガイドブックとして、本ガイドブックの他に、「ISO/IEC15408 を活用した調達のガイドブック（経済産業省情報セキュリティ政策室発行、http://www.meti.go.jp/policy/netsecurity/downloadfiles/CCguide_ver1_06.pdf)」がある。このガイドブックは、国際標準である ISO/IEC15408 に基づいて評価又は認証された製品等の調達を効率的に行えるように、調達の仕方等について説明をしたものである。

ISO/IEC15408 では、セキュリティ確保の具体的な方法の一つである暗号技術の選択については触れていないため、ISO/IEC15408 の認証を取得している製品やシステムであっても、電子政府推奨暗号リストに掲載されていない暗号アルゴリズムが使われている場合もある。このため、「ISO/IEC15408 を活用した調達のガイドブック」に従って暗号機能を含む製品・システムを調達しても、安全な暗号技術が調達できるとは限らないことから、本ガイドブックにおいて、暗号技術の選定を中心に説明するものである。

したがって、図２．２－１に示すとおり、セキュリティ確保に関する諸要件と暗号要件をそれぞれに指定して調達を進める場合は、それぞれのガイドブックを参照し、セキュリティ確保に関する諸要件の一部として暗号要件を指定する場合には、セキュリティ確保全体については「ISO/IEC15408 を活用した調達のガイドブック」を参照したうえで、暗号要件の選定に関してのみ、本ガイドブックを参照することを意図している。

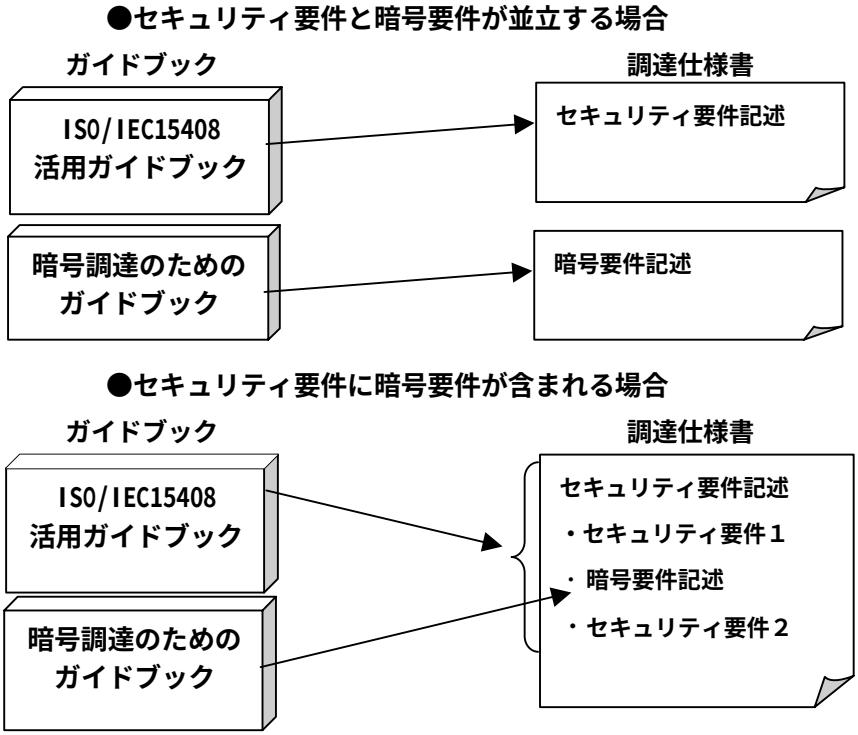


図２．２－１　ISO/IEC15408 を活用した調達と暗号調達の関連

３．　暗号調達、及び関連する暗号技術の概要

電子政府システムの調達における暗号の調達手順については第４章で詳細に説明するが、この章では第４章で説明する調達手順を理解し、実行するために必要な事項、すなわちシステム全体の検討作業と暗号調達の作業の関わり、及び暗号調達に必要な暗号関連の技術的概念について説明する。

暗号はセキュリティ対策の一部として利用されるので、暗号を調達するにあたっては、その前段として、システム全体を見たときに、どのような目的で暗号を利用すべきかの整理をしておく必要がある。この作業がリスク分析である。図３－１にシステム全体で行う作業に占める暗号調達（調達仕様書作成作業）の位置付けを示す。

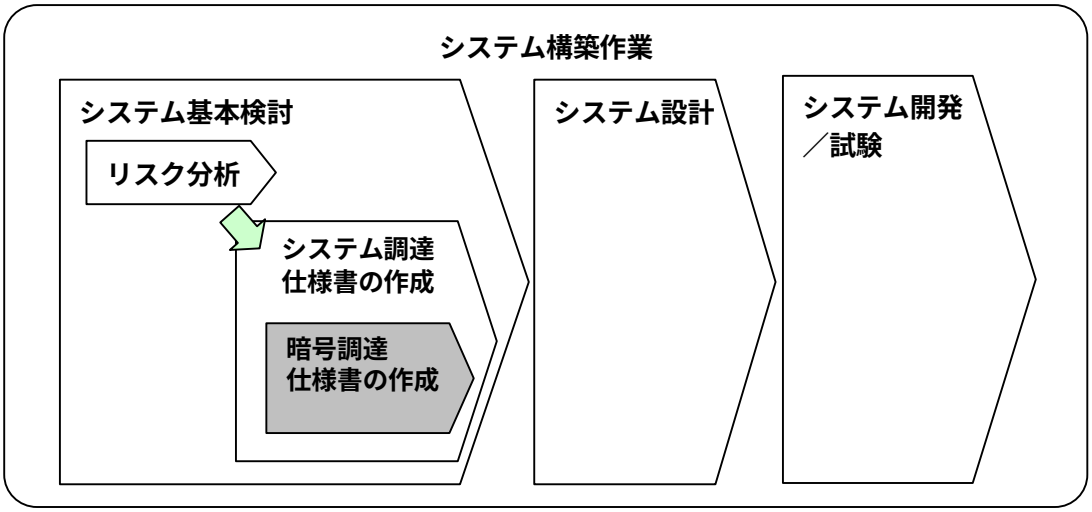


図３－１　システム全体の作業に占める暗号調達（調達仕様書作成作業）の位置付け

以下では、３．１節において、（１）でシステム全体として行う作業のうち暗号調達に深い関連を持つリスク分析について概説し、（２）で実際の電子政府システムにおいて暗号が利用されるイメージの例示を行う。

また、３．２節において、暗号調達の主要な手順である暗号アルゴリズムを選定するまでの道筋（図３－２参照）を意識しながら、この手順を進めるうえで必要となる技術的概念、すなわち、暗号利用形態、暗号技術分類、暗号アルゴリズムの３つについて説明する。

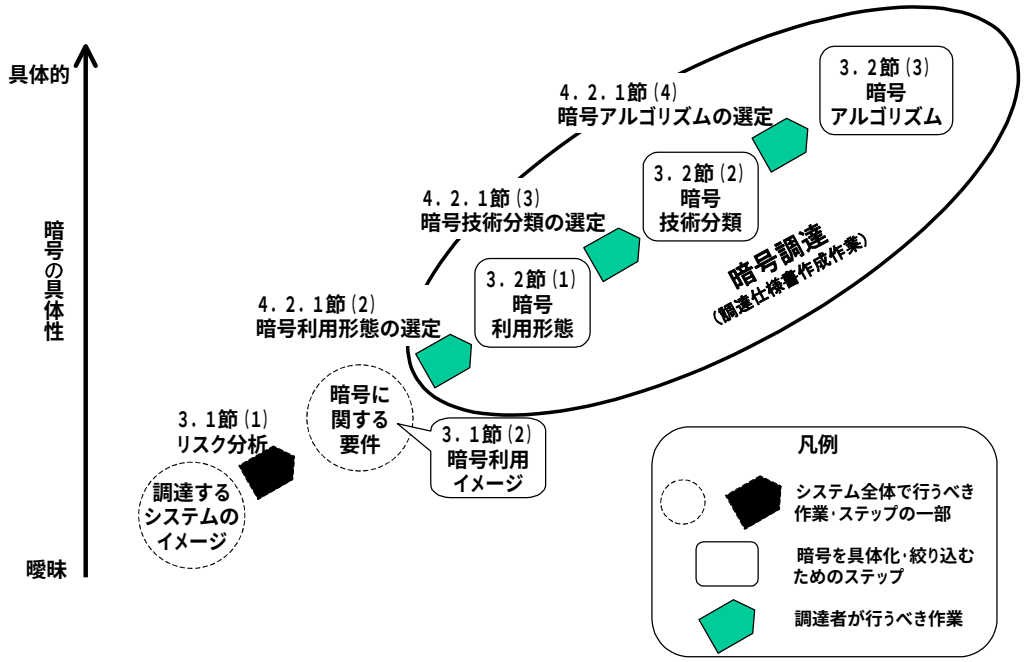


図３－２　暗号を具体化・絞り込みを行うためのステップ

３．１　システム全体の検討作業と暗号調達の作業の関わり

（１） リスク分析と暗号調達の関わり

電子政府システムのような社会的影響の大きなシステムにおいては、セキュリティが重要な要件であるため、システムの基本検討の段階においてセキュリティ関連の要件を整理する必要がある。このためにリスク分析の作業が行われる。リスク分析の手順については、様々な方法が考えられるが、最も標準的なものとしては、ISO/IEC15408 に準拠した手順が考えられる。

リスク分析等の作業の中で、暗号調達を進めるにあたって必要な事項は、該当システムに必要な暗号利用の目的の決定、及びその他の暗号技術への要件（暗号化の処理速度など）の決定である。

暗号利用の目的については、作業を標準化するため、電子政府システムにおける暗号利用の目的を４つに類型化して暗号利用形態を定義している。この整理した暗号利用形態については、３．２節（１）にて解説する。

（2）電子政府システムにおける暗号利用イメージ

本節では、システムにおける暗号利用を理解するために重要な以下の要素、
・調達するシステムが実現する機能
・調達するシステムの構成要素（装置、人物、組織）
・各要素間で授受される情報（電子情報、鍵情報など）
を抽出、整理したうえで、電子政府システムにおける暗号の利用に関するイメージをまとめたものである。

すべての電子政府システムについて個別に説明することはできないので、電子政府システムのうち暗号の利用が想定される主な 5 つのシステムにおける暗号利用イメージを例示、解説している。なお、例示したシステムモデルは、「e-Japan 重点計画－2002（http://www.kantei.go.jp/jp/singi/it2/index.html）」にも挙がっている 4 つのシステムモデルと、それらの共通基盤となるシステムモデルのあわせて 5 つである。

- 電子申請システムモデル
  e-Japan 重点計画-2002 では「申請・届出等手続の電子化」と表現している。
- 電子調達システムモデル
  e-Japan 重点計画-2002 では「調達手続の電子化」と表現している。
- 電子納付システムモデル
  e-Japan 重点計画-2002 では「歳入・歳出の電子化」と表現している。
- 電子情報提供システムモデル
  e-Japan 重点計画-2002 では「行政情報の電子的提供」と表現している。
- 政府認証基盤
  上記４システムモデルの共通基盤。

以下に、この 5 つの暗号利用システムモデルについて説明する。
なお、これら暗号利用システムモデルについては、参考資料「暗号技術検討会 2001 年度報告書」（http://www.soumu.go.jp/s-news/2002/020416_2.html　又は http://www.meti.go.jp/policy/netsecurity/crypt.htm）に記載されているので、詳細についてはそちらを参照されたい。

a)　電子申請システムモデル

電子申請システムとは、利用者（個人ならびに法人）が政府（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。

電子申請システムにおける要素と、要素間で授受される主な情報を図にしたもの（モデル図と呼ぶ）を図３．１－１に示す。

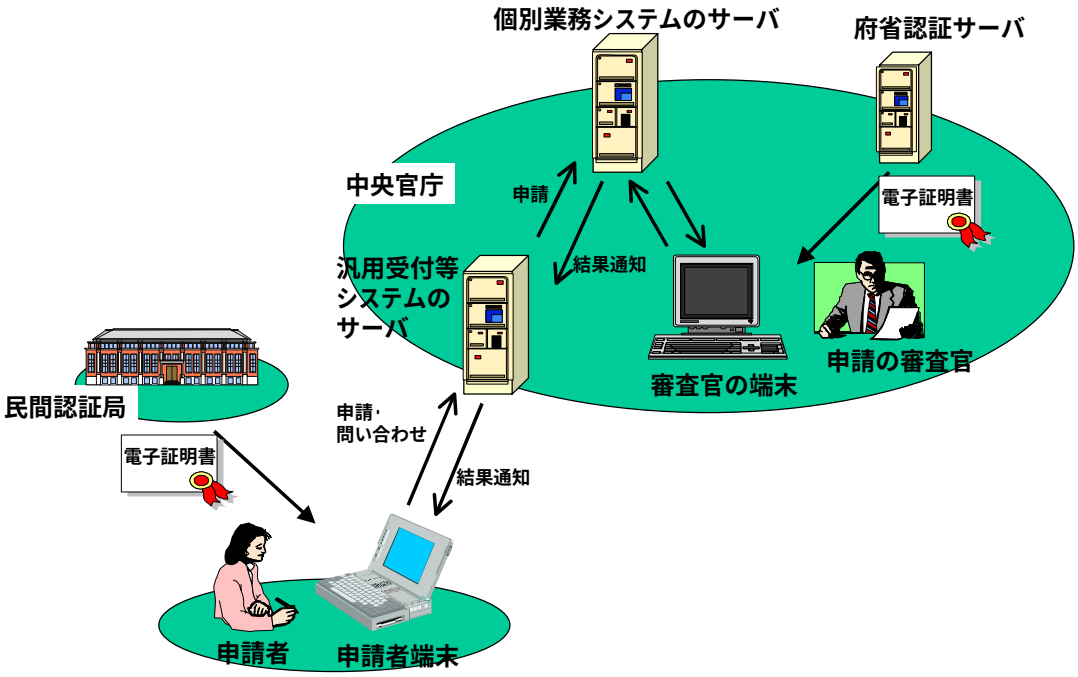


図３．１－１　電子申請システムのモデル図

図３．１－１は、図中左下の申請者が、図中右上の政府（中央官庁）に対して、インターネットを介して電子的に申請を行い、政府の審査官がその内容を審査し、審査結果を返信している状況を表している。

当該システムにおいては、利用者と審査官の間の通信において、相手認証、署名、守秘が、また、それらの通信に必要な暗号化の鍵情報について、鍵共有の暗号利用形態が想定される。

b)　電子調達システムモデル

電子調達システムとは、政府（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したシステムである。

電子調達システムにおけるモデル図を図３．１－２に示す。

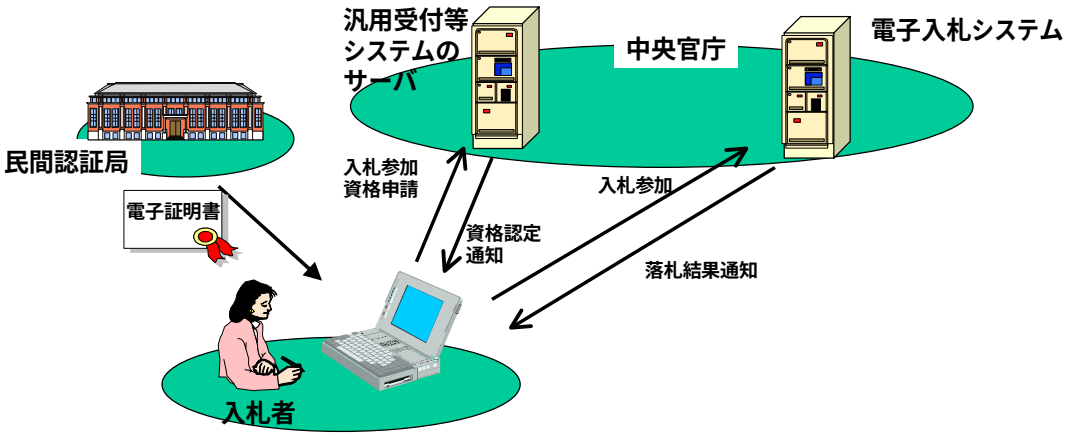


図３．１－２　電子調達システムのモデル図

図３．１－２は、図中左下の入札者が、図中右上の政府（中央官庁）に対して、インターネットを介して電子的に入札参加申請を行った上で、入札を行い、落札結果を受け取っている状況を表している。

当該システムにおいては、入札者と中央官庁の間の通信において、相手認証、署名、守秘が、また、それらの通信に必要な暗号化の鍵情報について、鍵共有の暗号利用形態が想定される。

c)　電子納付システムモデル

電子納付システムとは、個人ならびに法人が政府（中央官庁）に対して行っている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。

電子納付システムにおけるモデル図を図３．１－３に示す。

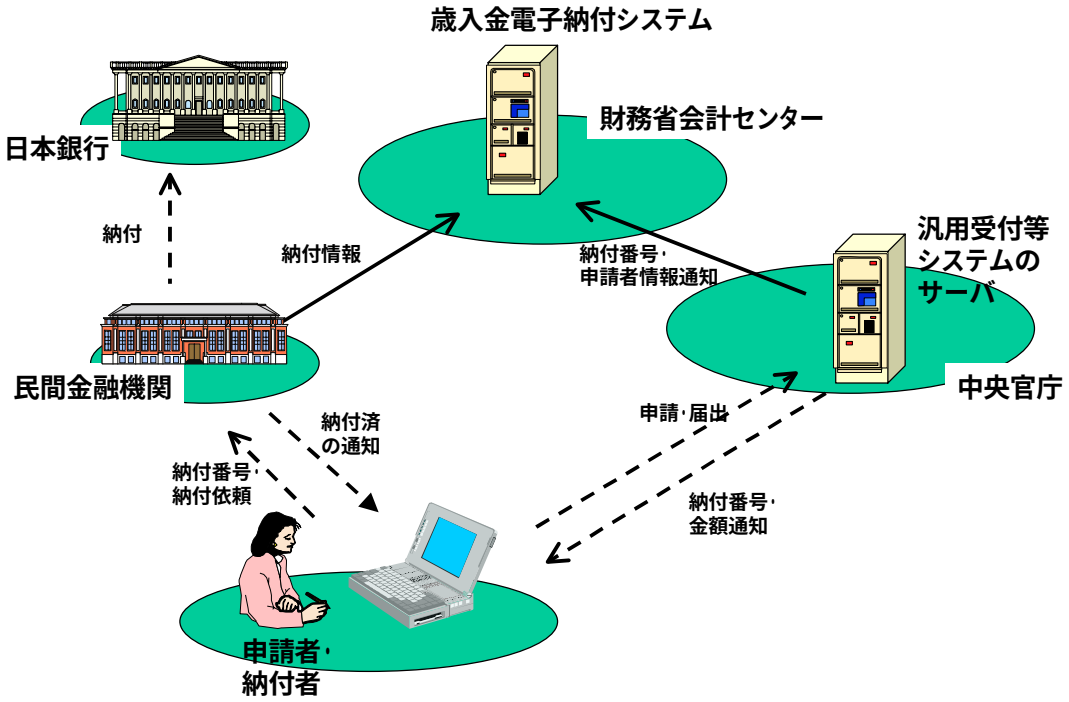


図３．１－３　電子納付システムのモデル図

図３．１－３は、図中左下の申請者・納付者が、図中右の政府（中央官庁）に対して納付の申請手続きを行った上で、図中左の民間金融機関を経由して日本銀行の政府口座に入金し、図中上の財務省会計センターで申請と入金の突き合わせ確認を行っている状況を表している。

図３．１－３のうち、申請者・納付者と中央官庁間は電子申請システムの対象であり、また納付者と民間金融機関間は民間のシステムが実現すべき部分である。

当該システムにおいては、民間金融機関と財務省会計センター間の通信において、相手認証、署名、守秘が、また、それらの通信に必要な暗号化の鍵情報について、鍵共有の暗号利用形態が想定される。

d)　電子情報提供システムモデル

電子情報提供システムとは、個人ならびに法人が政府（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できるようにするものである。

電子情報提供システムにおけるモデル図を図３．１－４に示す。

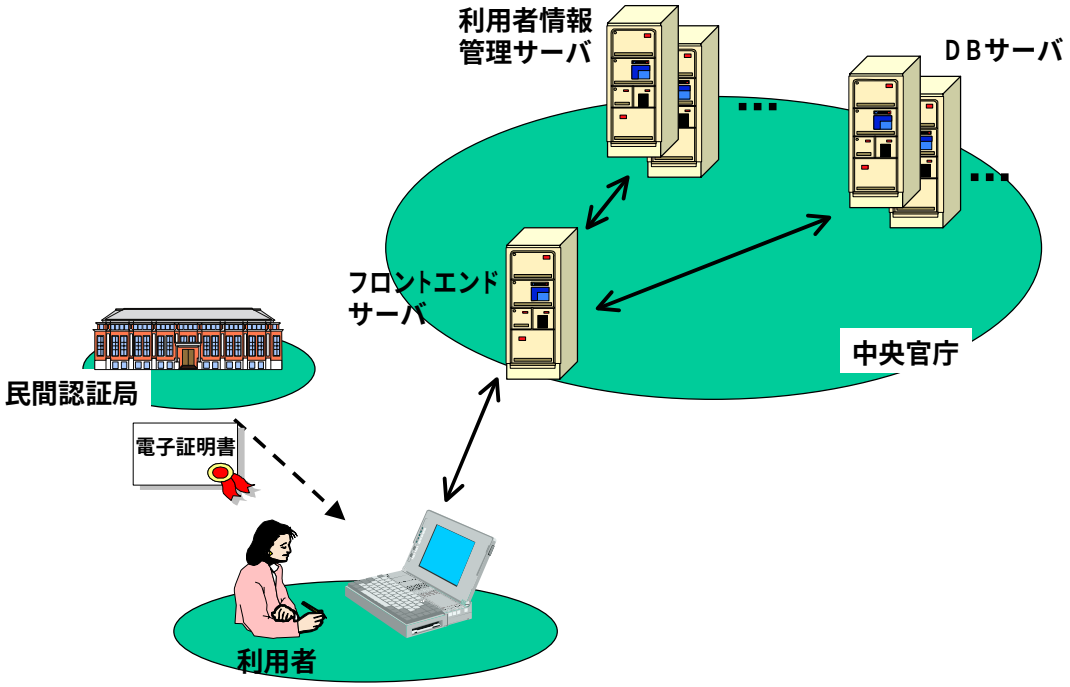


図３．１－４　電子情報提供システムのモデル図

図３．１－４は、図中左下の利用者が、図中右上の政府（中央官庁）サーバにアクセスし、情報の提供を受けている状況を表している。

当該システムにおいては、政府からの情報提供にあたり申請・登録等による利用者の認証を想定しており、利用者と中央官庁との間の通信において、相手認証（利用者は必要に応じて認証局(ＣＡ)に登録する)、署名、守秘の暗号利用形態が、また、それらの通信に必要な暗号化の鍵情報について、鍵共有の暗号利用形態が想定される。

e)　政府認証基盤

政府認証基盤は、官職の認証や申請、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り、現在ＧＰＫＩとして実用化されている。

政府認証基盤におけるモデル図を図３．１－５に示す。

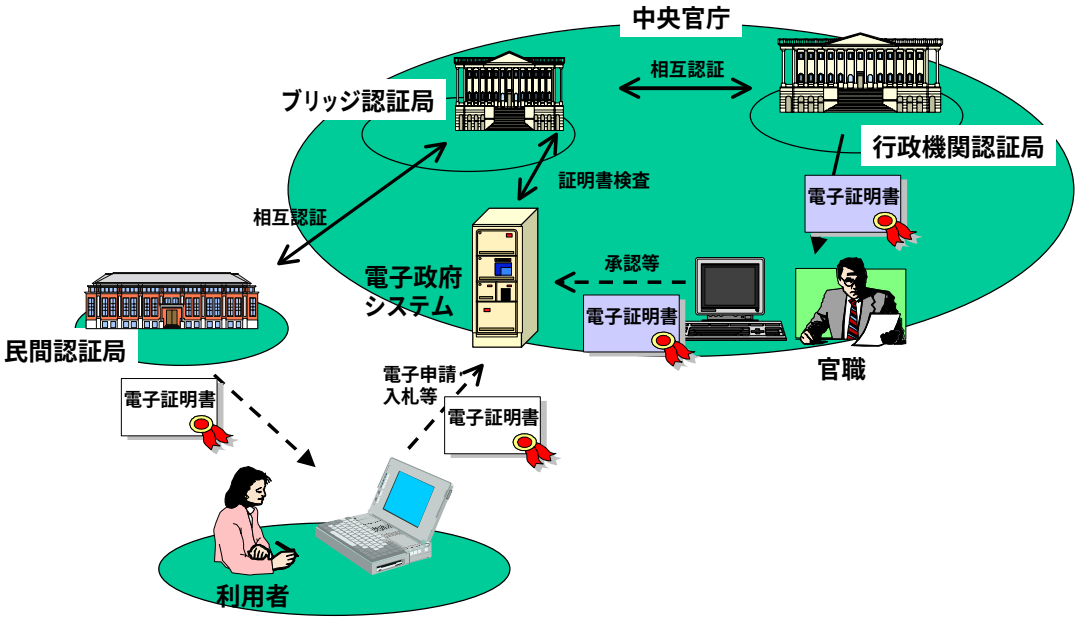


図３．１－５　政府認証基盤のモデル図

図３．１－５は、図中右上の政府（中央官庁）の官職、または図中左下の利用者が電子政府システムを利用するにあたり、図中右上の行政機関認証局、または図中左の民間認証局から電子証明書の発行を受けている状況、ならびにそれら証明書の有効性を検証するための手段を提供するブリッジ認証局（図３．１－５の中央上）を表している。

当該システムは電子政府システムにおける相手認証及び署名の暗号利用形態を支援して、認証のために必要な情報を管理するシステムである。

３．２　暗号調達に必要な暗号関連の技術的概念

（1）暗号利用形態の解説

暗号利用形態とは、電子政府システムにおける暗号利用の目的を整理、分類したものである。

表３．２－１では、電子政府システムにおける暗号利用の目的を整理、分類した 4 つの暗号利用形態について説明している。

表３．２－１　暗号利用形態一覧

暗号利用形態	概　　要
相手認証	やりとりの相手の正当性を保証すること
鍵共有	インターネット等のオープンなネットワークを用いて共通鍵暗号技術を利用する際に、通信の当事者間で鍵情報を共有すること
守秘	インターネット等のオープンなネットワークや、記録媒体を使って電子情報をやりとりするときに、知られて良い利用者以外には内容を知られないようにすること
署名	電子情報が正当であることを確認できるようにすること このことは、電子情報自体が改竄されていないかを確認できることと、署名を作った者を第三者が確認できることの二つの目的を同時に満たすことを意味する

（2）暗号技術分類の解説

暗号技術分類とは、暗号アルゴリズムを、機能的、技術的に類似するグループに整理及び分類したものである。

表３．２－２では、現存する暗号アルゴリズムを機能的、技術的に整理及び分類した 4 つの暗号技術分類について説明している。

なお、これらの暗号技術分類のうち、中核となるものが公開鍵暗号と共通鍵暗号であり、ハッシュ関数と擬似乱数生成は、公開鍵暗号または共通鍵暗号に付随して用いられることが多い。

表３．２－２　暗号技術分類一覧

暗号技術分類	概　　要
公開鍵暗号	公開鍵と秘密鍵という対をなす２種類の鍵を用いる暗号（または暗号技術）を総称して公開鍵暗号（または公開鍵暗号技術）という。公開鍵から秘密鍵を求めることは計算の手間が膨大となり事実上困難であるという特性を持っている。守秘のための方式と署名のための方式とに大別でき、前者を（狭い意味で）公開鍵暗号方式、後者を公開鍵署名方式と呼んで区別することがある。前者の意味での公開鍵暗号方式においては、平文を暗号化する時に用いる鍵（暗号化鍵）が公開鍵であり、暗号文を復号する時に用いる鍵（復号鍵）が秘密鍵である。公開鍵署名方式においては、平文に対して署名文を生成する時に用いる鍵（署名生成鍵）が秘密鍵であり、署名文を検査し平文を取り出す時に用いる鍵（署名検査・復号鍵）が公開鍵である。
共通鍵暗号	平文を暗号化する時に使用する鍵と、暗号文を復号する時に使用する鍵が共通の暗号方式。 高速性に優れているが、共通鍵の配送を安全に行うことが求められる。 共通鍵暗号は、データを一定の長さ（ブロック）に分割し、ブロック単位で処理を行う方式（ブロック暗号）と、データを 1 ビットないし 1 バイト程度の短い単位で処理する方式（ストリーム暗号）に分けることができる。
ハッシュ関数	入力データの長さに関わらず、固定長のハッシュ値を出力する関数。ハッシュ関数には、出力から入力を簡単に計算できない一方向性と、異なる 2 つの入力に対し同じハッシュ値を出力しない無衝突性が求められる。
擬似乱数生成	暗号学的に安全な乱数 *1 にできるだけ近づけた数の系列を人為的に生成する仕組み。

*1)「暗号学的に安全な乱数」とは、過去の履歴から次の値が予測できないような数字列を意味する。

（３）電子政府推奨暗号の概要

ここでは、電子政府推奨暗号の概要を説明する。なお、詳細については、以下の資料等を参照のこと。

・JIS－TR X0050（暗号技術評価報告書　CRYPTREC Report 2000）
（http://www.meti.go.jp/policy/netsecurity/crypt.htm　又は
http://www.ipa.go.jp/security/enc/CRYPTREC/fy12/cryptrec20010418.html）
・暗号技術検討会 2001 年度報告書
（http://www.soumu.go.jp/s-news/2002/pdf/020416_2_a.pdf　又は
http://www.meti.go.jp/policy/netsecurity/downloadfiles/cryptrec2001report.pdf）
・JIS-TR X0087（暗号技術評価報告書(2001 年度版)　CRYPTREC Report 2001）
（http://www.meti.go.jp/policy/netsecurity/crypt.htm　の「CRYPTREC Report 2001」、
http://www.ipa.go.jp/security/enc/CRYPTREC/fy14/cryptrec20020418_report01.html
http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy14/cryptrec20020418_report01.html）
・暗号技術検討会 2002 年度報告書
（http://www.soumu.go.jp/s-news/2003/pdf/030331_4_1.pdf　又は
http://www.meti.go.jp/policy/netsecurity/index.html）
・暗号技術評価報告書　2002 年度版　CRYPTREC Report 2002
（http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030401_report01.html
http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec200304_report02.html）

a)　公開鍵暗号

<u>（署名）</u>

● DSA(Digital Signature Algorithm)

米国規格協会(ANSI: American National Standards Institute)が ANSI X9.30:1-1997 として 1997 年に標準化した離散対数問題の困難性に基づく署名方式。

我が国の「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（以下、電子署名法の指針）」にも記載されている。

また、市販のブラウザソフト等に多く用いられている暗号プロトコル SSL(Secure Socket Layer)3.0/TLS（Transport Layer Security）1.0 に採用されている。

● ECDSA（Elliptic Curve Digital Signature Algorithm）

楕円曲線暗号の標準仕様策定のためのコンソーシアムである SECG（Standards for Efficient Cryptography Group）が策定している SEC 1: Elliptic Curve Cryptography(Version 1.0)（以下、SEC 1）で 2000 年に規格化された楕円曲線上の離散対数問題の困難性に基づく署名方式。CRYPTREC へは富士通株式会社から応募されている。

我が国の電子署名法の指針にも一部のパラメータを除いて適合している。

欧州の暗号評価事業である NESSIE(New European Schemes for Signatures, Integrity, Encryption）プロジェクトにおいて、推奨アルゴリズムに選定されている。

● RSASSA-PKCS1-v1_5(RSA Signature Scheme with Appendix based on PKCS#1 v1.5)

米 RSA 研究所が策定している暗号規格 PKCS（Public Key Cryptography Standards）シリーズの１つである PKCS #1 Version 2.1 で 2002 年に RSASSA-PKCS1-v1_5 として規格化された素因数分解問題の困難性に基づく署名方式で、PKCS #1 Version 1.5 で 1993 年に規格化された署名方式とはハッシュ関数の選択に関して、MD4 が除かれ、SHA-1、SHA-256、SHA-384、SHA-512 が追加されたことを除いて同じである。

我が国の電子署名法の指針にも記載されている。また、PKCS #1 Version 1.5 で規格化された署名方式が SSL3.0/TLS1.0 に採用されている。

● RSA-PSS(RSA Public-Key Cryptosystem with Probabilistic Signature Scheme)

米 RSA 研究所が策定している暗号規格 PKCS シリーズの１つである PKCS #1 Version 2.1 で RSASSA-PSS として 2002 年に規格化された素因数分解問題の困難性に基づく証明可能安全性を有する署名方式。CRYPTREC へは RSA セキュリティ株式会社から応募されている。

我が国の電子署名法の指針にも記載されている。

NESSIE プロジェクトにおいて、推奨アルゴリズムに選定されている。

（守秘）

● RSA-OAEP(RSA Public-Key Cryptosystem with Optimal Asymmetric Encryption Padding)

米 RSA 研究所が策定している暗号規格 PKCS シリーズの１つである PKCS #1 Version 2.1 で 2002 年に RSAES-OAEP として規格化された素因数分解問題の困難性に基づく証明可能安全性を有する守秘方式で、PKCS #1 Version 2.0 で 1998 年に RSAES-OAEP として規定された守秘方式と同じである。CRYPTREC へは RSA セキュリティ株式会社から応募されている。

● RSAES-PKCS1-v1_5(RSA Encryption Scheme based on PKCS#1 v1.5)

米 RSA 研究所が策定している暗号規格 PKCS シリーズの１つである PKCS #1 Version 2.1 で 2002 年に RSAES-PKCS1-v1_5 として規格化された素因数分解問題の困難性に基づく守秘方式で、PKCS #1 Version 1.5 で 1993 年に規定された守秘方式と同じである。

PKCS #1 Version 1.5 で規格化された守秘方式が SSL3.0/TLS1.0 に採用されている。

【CRYPTREC からのコメント】
《注意》SSL3.0/TLS1.0 で使用実績があることから、当面の使用を認める。

（鍵共有）

● DH（Diffie-Hellman）

米国規格協会が ANSI X9.42-2001 として 2001 年に標準化した離散対数問題の困難性に基づく鍵共有方式で、1976 年に W. Diffie と M. E.. Hellman が論文（"New Directions in Cryptography," IEEE Transactions on Information Theory, vol. IT-22, pp. 644-654, Nov. 1976）で発表した鍵共有方式に基づくものである。

W. Diffie と M. E.. Hellman が論文で発表した鍵共有方式が SSL3.0/TLS1.0 に採用されている。

● ECDH(Elliptic Curve Diffie-Hellman Scheme)

SECG が策定している SEC 1 で 2000 年に規格化された楕円曲線上の離散対数問題の困難性に基づく鍵共有方式で、DH における離散対数計算を楕円曲線上の離散対数計算に置き換えたものである。CRYPTREC へは富士通株式会社から応募されている。

● PSEC-KEM

日本電信電話株式会社が 2001 年に提案した、楕円曲線上の離散対数問題の困難性に基づく鍵カプセル化メカニズム。CRYPTREC へは日本電信電話株式会社から応募されている。

NESSIE プロジェクトにおいて推奨アルゴリズムに選定されている。

【CRYPTREC からのコメント】
《注意》KEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

b) 共通鍵暗号

（64 ビットブロック暗号）

【CRYPTREC からのコメント】
《注意》共通鍵ブロック暗号を使用して新たな電子政府用システムを構築する場合、より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

- CIPHERUNICORN-E
  1998 年に日本電気が発表した、鍵長 128 ビットの 64 ビットブロック暗号である。

- Hierocrypt-L1
  2000 年に東芝が発表した、鍵長 128 ビットの 64 ビットブロック暗号である。

- MISTY1
  1996 年に三菱電機が発表した、鍵長 128 ビットの 64 ビットブロック暗号である。NESSIE プロジェクトにおいて、推奨アルゴリズムに選定されている。

- 3-key Triple DES（Data Encryption Standard）
  1979 年に FIPS 認定された DES *1 の組み合わせ暗号である、鍵長 168 ビットの 64 ビットブロック暗号。1998 年に NIST により FIPS46-3 として標準化され、ANSI X9.52 としても規格化されている。SSL3.0/TLS1.0 に採用されている。

  *1）DES： 1977 年に FIPS46 として標準化された、鍵長 56 ビットの 64 ビットブロック暗号

【CRYPTREC からのコメント】
《注意１》3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。
1）FIPS46-3 として規定されていること
2）デファクトスタンダードとしての地位を保っていること
《注意２》Triple DES には鍵長 112 ビットの 2-key Triple DES もあるが、CRYPTREC として 2-key Triple DES の使用は推奨しない。

（128 ビットブロック暗号）

- AES

  2001 年に、Rijndael *2 をもとに、NIST が FIPS 197 として標準化した、鍵長 128 ビット、192 ビット、256 ビットの 128 ビットブロック暗号である。

  NESSIE プロジェクトにおいて、推奨アルゴリズムに選定されている。

  *2）Rijndael： 1998 年にベルギーの J.Daemen と V.Rijmen により AES プロジェクトに提案され、2000 年に AES Winner に選定されたブロック暗号

- Camellia

  2000 年に発表された、NTT と三菱電機の共同開発による、鍵長 128 ビット、192 ビット、256 ビットの 128 ビットブロック暗号。

  NESSIE プロジェクトにおいて、推奨アルゴリズムに選定されている。

- CIPHERUNICORN-A

  2000 年に日本電気が発表した、鍵長 128 ビット、192 ビット、256 ビットの 128 ビットブロック暗号である。

- Hierocrypt-3

  2000 年に東芝が発表した、鍵長 128 ビット、192 ビット、256 ビットの 128 ビットブロック暗号である。

- SC2000

  2000 年に発表された、富士通と東京理科大学の共同研究による、鍵長 128 ビット、192 ビット、256 ビットの 128 ビットブロック暗号である。

（ストリーム暗号）

- MUGI

  2001 年に日立製作所が発表した、鍵長 128 ビットのストリーム暗号である。

- MULTI-S01

  2000 年に日立製作所が発表した、鍵長 256 ビットのストリーム暗号である。

- 128-bit RC4

  1987 年に RSA セキュリティ社（当時 RSA データセキュリティ社）が発表した、鍵長 128 ビットのストリーム暗号である。SSL3.0/TLS1.0 に採用されている。

  【CRYPTREC からのコメント】
  《注意》 128-bit RC4 は、SSL3.0/TLS1.0 に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、可能な限りそちらを使用することが望ましい。
  《警告》 RC4 は、SSL3.0/TLS1.0 では鍵長 40 ビットと鍵長 128 ビットを選択して利用することが可能であるが、RC4 を使うとしても、安全性確保の観点から、CRYPTREC としては、鍵長 128 ビットで利用すべきであり、鍵長 40 ビットでの利用は避けるべきであると警告する。

c) ハッシュ関数

【CRYPTREC からのコメント】
《注意》新たな電子政府用システムを構築する場合、より長いハッシュ値のものがが利用できるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合は、この限りではない。

- RIPEMD-160

  1997 年に、RIPEMD *3 の安全性強化版として、H. Dobbertin、A. Bosselaers、B. Preneel により提案された、出力ハッシュ値 160 ビット長のハッシュ関数である。ISO/IEC 10118-3 に採用されている。

  *3）RIPEMD： ヨーロッパの RIPE（RACE Integrity Primitive Evaluation）プロジェクトで策定されたハッシュ関数

- SHA-1

  1994 年に NIST が FIPS 180 として標準化した、出力ハッシュ値 160 ビット長のハッシュ関数である。我が国の電子署名法の指針に記載されている。ISO/IEC 10118-3、SSL3.0/TLS1.0 に採用されている。

- SHA-256

  2002 年に NIST が FIPS 180-2 として標準化した、出力ハッシュ値 256 ビット長のハッシュ関数である。

  NESSIE プロジェクトにおいて推奨アルゴリズムに選定されている。

- SHA-384

  2002 年に NIST が FIPS 180-2 として標準化した、出力ハッシュ値 384 ビット長のハッシュ関数である。

  NESSIE プロジェクトにおいて推奨アルゴリズムに選定されている。

- SHA-512

  2002 年に NIST が FIPS 180-2 として標準化した、出力ハッシュ値 512 ビット長のハッシュ関数である。

  NESSIE プロジェクトにおいて推奨アルゴリズムに選定されている。

d) 擬似乱数生成

【CRYPTREC からのコメント】
《注意１》擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、以下に挙げる擬似乱数は例示であり、これら以外の「暗号学的に安全な擬似乱数生成アルゴリズム」の採用を妨げるものではない。
《注意２》以下の３つのアルゴリズムについては、パラメータの選び方によっては、仕様書中に定義されている使い方の中に安全とは言い切れないものが存在する。利用にあたっては、CRYPTREC Report 2002 の該当章を確認の上、適切な使い方を選択する必要がある。

- PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1

  2001 年に ANSI が規格化した ANSI X9.42-2001 Public Key Cryptography for the Financial Services Industry : Agreement of Symmetric Keys Using Discrete Logalithm Cryptography で利用する擬似乱数生成方式。ハッシュ関数 SHA-1 をもとにした構成になっている。

- PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1（*）

  2000 年に NIST が標準化した規格 FIPS 186-2 をベースに、変更情報（change notice 1）が 2001 年に付け加えられた FIPS 186-2 (+ change notice 1) Digital Signature Standard (DSS)に掲載されている擬似乱数生成方式。本規格中では、複数の擬似乱数生成方式が規定されているが、そのうち本アルゴリズム及び下記(**)のアルゴリズムを CRYPTREC としては例示する。ハッシュ関数 SHA-1 をもとにした構成になっている。

- PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1（**）

  2000 年に NIST が標準化した規格 FIPS 186-2 をベースに、変更情報（change notice 1）が 2001 年に付け加えられた FIPS 186-2 (+ change notice 1) Digital Signature Standard (DSS)に掲載されている擬似乱数生成方式。本規格中では、複数の擬似乱数生成方式が規定されているが、そのうち本アルゴリズムと上記(*)のアルゴリズムを CRYPTREC としては例示する。ハッシュ関数 SHA-1 をもとにした構成になっている。

４．　調達の手順

４．１　概要

（1）暗号調達の流れ

電子政府システムの調達に係る作業の流れはおおよそ図４．１－１及び表４．１－１のとおりである。本節では、この流れを意識しながら、暗号調達に関わる事項のみを抜粋して説明する。

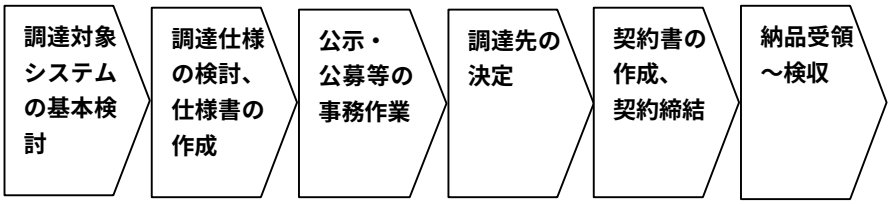


図４．１－１　システム調達の流れ

表４．１－１　各作業の概要

調達の流れ	作　業　概　要
調達対象システムの基本検討	システムの背景、目的、対象範囲、構築条件、概算費用等、調達を進める基本的事項の整理、その他、暗号に関連した作業として、リスク分析等が行なわれる
調達仕様の検討、仕様書の作成	システムへの要件となる事項の具体化検討と仕様書の作成（必要に応じて、パブリックコメントを募集する場合がある）
公示・公募等の事務作業	公示・公募、提案の受付などの事務作業
調達先の決定	調達システムに適合する提案をした業者を選定
契約書作成、契約締結	調達システムの特記事項等を盛り込んで、契約書を作成、契約を締結
納品受領～検収	調達したシステムを受領、仕様と相違ないことを確認検収

（２）暗号調達の進め方について

調達作業の流れの中で、調達者はシステムに必要な暗号の要件を明確化し、業者に示す必要がある。このために、調達者は電子政府推奨暗号リストの提示する情報をもとにして、暗号技術を絞り込む作業を実施する。

絞り込む作業の進め方には、以下に挙げる２種類の方法が考えられる。

- 調達仕様書の作成時に、調達システムについて詳細に説明し、その中で暗号アルゴリズムを指定する。（以下では調達者指定モデルと記載）

- 調達仕様書では暗号について概略を説明し、業者に電子政府推奨暗号リストに準じて暗号アルゴリズムを選定させ、提案資料を見て審査する。（以下では提案審査モデルと記載）

前記した２種類の方法のうち、前者（調達者指定モデル）の場合は仕様書作成段階で暗号への要件を詳細化することが必要であるが、後者（提案審査モデル）においては提案書受領時の審査時に同様の作業が必要となるため、システム調達全体を通じての調達者の作業については同等になるものと考えられる。

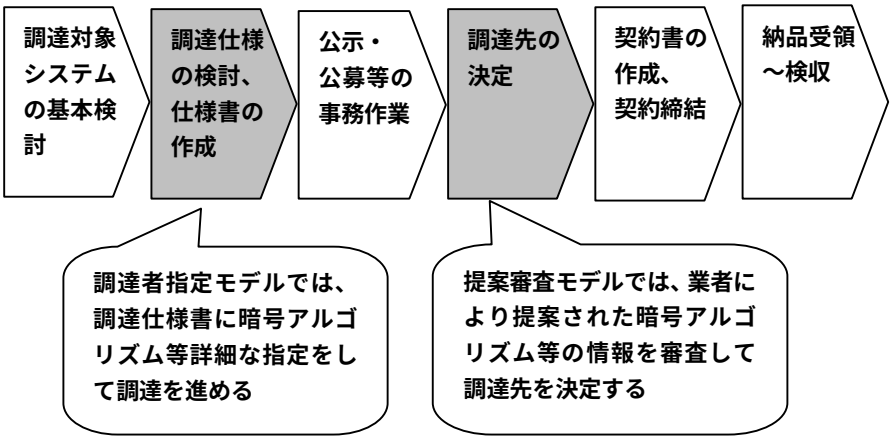


図４．１－２　暗号要件絞り込みのポイント

４．２　調達仕様書の作成

調達仕様書の作成においては、４．１節の（２）で説明した調達者指定モデルと、提案審査モデルにおいて、作業手順が異なるため、以下では各々のモデルに対して個別に手順の説明を行う。

４．２．１　調達者指定モデルの場合

（１）概要

この節では、調達する暗号アルゴリズムを選定するために、調達者が検討すべき内容と、実際の記載内容について説明する。

調達者は、リスク分析結果等の調達するシステムの基本検討の結果を把握した上で、次の順番で、調達する暗号アルゴリズムに関する検討を行い、調達仕様書を作成する。

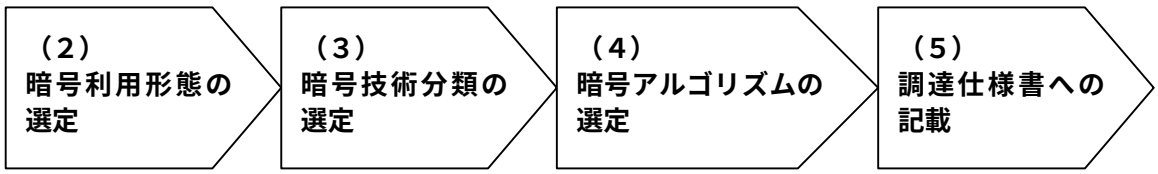


図４．２．１－１　調達者指定モデルにおける調達仕様書作成の流れ

（2）暗号利用形態の選定

本ガイドブックでは、システムの基本検討におけるリスク分析等の様々な作業の一環として暗号利用形態の選定が行われた後に、本ガイドブックにしたがって、暗号技術分類、暗号アルゴリズムを選定することを想定している。

ここでは、確認の意味で、一般的なセキュリティ上の脅威に対して暗号利用形態を選定する場合の基本的な考え方の例を示す。

- 暗号による保護が必要である情報が漏洩する可能性があり、その情報が漏洩しては困るもの（利用者または政府に金銭的又はその他の被害を与えることが想定される場合。以下同様）については、暗号利用形態のうち「守秘」による保護が必要となる。

- 暗号による保護が必要である情報が改竄されるか、または否認（後になって異議を申し立てられる）の可能性があり、その情報が改竄または否認されては困るものについては、暗号利用形態のうち「署名」による保護が必要となる。

- 暗号による保護が必要である情報を交換する相手に他人による成りすましの可能性があり、その情報が成りすました他人と授受を行われては困るものについては、暗号利用形態のうち「相手認証」による保護が必要となる。

- 「守秘」、「署名」、「相手認証」のいずれかの暗号利用形態において共通鍵暗号を利用する場合には、暗号鍵を安全に共有するために、「鍵共有」による鍵情報の保護が必要な場合がある。
  共通鍵暗号の利用が未だ明確でない場合、この段階では「鍵共有」は必要なものとして作業を進めることも可能であるが、暗号技術分類の選定が進んだ段階で、再度必要性を検討することが必要となる。

＜参考　：　作業の進め方の例＞

たとえば、電子申請システムの場合を例にとって説明する。

「申請・届出等手続きのオンライン化に関わる汎用受付等システムの基本的な仕様（平成 13 年 8 月 6 日　行政情報化推進各省庁連絡会議幹事会了承）」（http://www.soumu.go.jp/gyoukan/kanri/010806_1.htm）に基づくシステムモデル図が図４．２．１－２である。

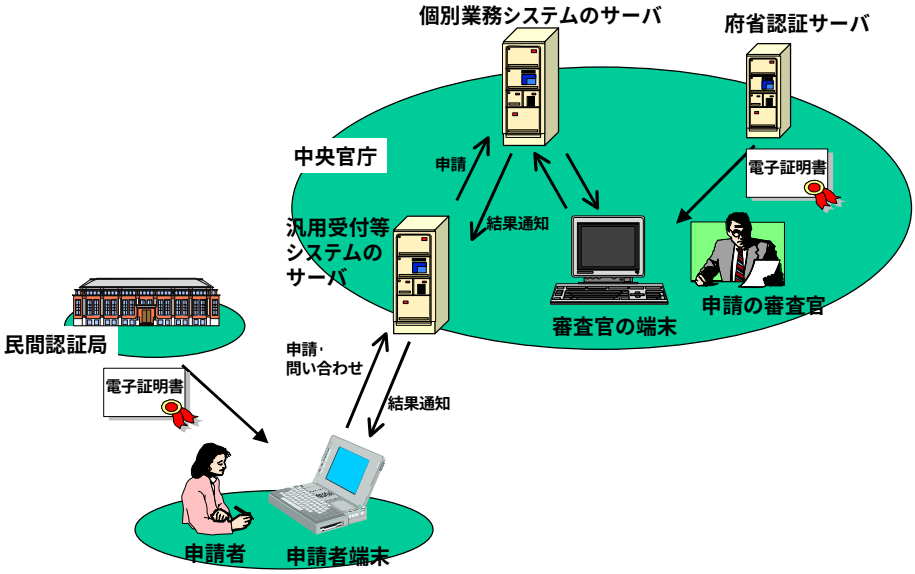


図４．２．１－２　電子申請システムのシステムモデル図

システム全体におけるリスク分析で、このシステムに登場する暗号による保護を必要とする情報を洗い出し、それらの情報に対応する暗号利用の目的、すなわち暗号利用形態を検討する。さらに、暗号アルゴリズム選定の過程において考慮すべき暗号技術への要件をまとめた表のサンプルが表４．２．１－１である。

表４．２．１－１　暗号利用形態選定表のサンプル※

暗号による保護を必要とする情報	暗号利用形態	暗号技術への要件
・申請データ ・申請内容確認で授受されるデータ ・到達確認通知 ・状況確認で授受されるデータ ・審査終了通知 ・許認可等公文書の取得要求データ ・許認可等公文書	・相手認証 ・署名 ・守秘	・通信速度は、利用者の負担とならない程度の速度であること。 ・多くの利用者にとって利用が負担とならないように、暗号アルゴリズムは標準的なものであることが望ましい。
（・鍵情報）	（鍵共有）	（必要になった時のための欄）

※ 実際の調達においては、サンプル自体を引用するのではなく、個別具体的な状況に応じた適切な調達を行うこと。

（３）暗号技術分類の選定

ここでは、暗号利用形態毎に、電子政府システムにおいて多く使用される暗号技術分類を例示する。

調達者は、調達するシステムの目的、特性を考慮して、暗号利用形態に対して適切と思われる暗号技術分類を選定すること。

なお、暗号技術分類の選定にあたっての留意点は以下の通り。

・ハッシュ関数と擬似乱数生成は、他の２つの暗号技術分類、共通鍵暗号と公開鍵暗号に付随して使用されることが多いため、ここでは共通鍵暗号と公開鍵暗号のどちらを選択するかについて説明している。ハッシュ関数と擬似乱数生成については、共通鍵暗号、公開鍵暗号のいずれを選択した場合でも使用されるものとして次項（４）に進んで構わない。

・説明にあたり、暗号利用形態によって、共通鍵暗号と公開鍵暗号の出現する順番が変わっているが、電子政府システム又は世間一般において、より多く使用されている暗号技術分類について先に説明している。

・暗号利用形態「守秘」「署名」「相手認証」において共通鍵暗号を使用した場合は、通信当事者間で暗号鍵を安全に共有するために「鍵共有」に対応する暗号技術分類も選定しておくこと。

a) 暗号利用形態が「守秘」の場合

- **共通鍵暗号を用いる場合**
  多くの場合、守秘では共通鍵暗号が使用される。
  特に、「送受信するデータ量が多い場合」、「高速処理が要求される場合」には、共通鍵暗号が使用される。
- **公開鍵暗号を用いる場合**
  他の暗号利用形態で公開鍵暗号を使用しており、共通的に使用する場合など、場合によっては守秘に公開鍵暗号が使用されることがある。
  公開鍵暗号は共通鍵暗号に比べて処理速度はかなり遅いが、送受信されるデータ量が少ない場合には、処理速度の影響が小さくなるので、公開鍵暗号を使用しても問題にはならないことがある。

b) 暗号利用形態が「鍵共有」の場合

・ 公開鍵暗号を用いる場合

多くの場合、鍵共有では公開鍵暗号が使用される。

特に近年では、安全に鍵情報を共有するために公開鍵暗号が多く使用される。

・ 共通鍵暗号を用いる場合

一部の方式（Kerberos 等）では鍵共有に共通鍵暗号を使用することがある。ただし、鍵共有のために使用する共通鍵暗号の暗号鍵を、事前に何らかの方法で安全に配布できる場合に限られる。

なお、頻繁に鍵情報を交換する必要がある場合には、処理速度を上げるために共通鍵暗号を用いることがある。

c) 暗号利用形態が「署名」の場合

・ 公開鍵暗号を用いる場合

多くの場合、署名では公開鍵暗号が使用される。

公開鍵暗号を用いた署名では、信頼できる公開鍵を入手する必要があり、そのためのインフラとしてＰＫＩを用いることが一般的である。

また、多くの場合、改竄を防ぐために添付されるデータの作成にはハッシュ関数が使用される。

・ 共通鍵暗号を用いる場合

署名には共通鍵暗号を用いることもできるが、署名を使用する目的のうち、「署名を作った者を第三者が確認できること」の実現は困難である。

共通鍵暗号を用いて署名に類似する目的を実現する方式として、ＭＡＣ（Message Authentication Code：メッセージ認証子）を用いる方法がある。

d) 暗号利用形態が「相手認証」の場合

・ 公開鍵暗号を用いる場合

多くの場合、相手認証では公開鍵暗号が使用される。実際、被認証者が特定の情報に署名を施し、検証者がそれを署名検証することで被認証者の同一性が判断できるので、特定の手続きと共に用いれば、リストに記載されたすべての署名方式は相手認証への応用が基本的に可能である。たとえば、JIS X5056-3:2002(ISO/IEC 9798-3:1998)に詳しい手続きの記述がある。

・ 共通鍵暗号を用いる場合

一部の方式（チャレンジ＆レスポンス等）では相手認証に共通鍵暗号を使用することがある。ただし、相手認証のために使用する共通鍵暗号の暗号鍵を、事前に何らかの方法で安全に配布できる場合に限られる。

なお、相手認証を高速に実行する必要がある場合には、処理速度を上げるために共通鍵暗号を用いることがある。

＜参考　：　作業の進め方の例＞

前項（２）と同じく、電子申請システムを例にとって説明する。

表４．２．１－１で選定した暗号利用形態から、暗号技術への要件を考慮して、選定した暗号技術分類をまとめた表のサンプルが表４．２．１－２である。

暗号利用形態「守秘」においては、暗号技術への要件でもある通信速度を考慮して共通鍵暗号を選定している。暗号利用形態「相手認証」、「署名」においては、特に考慮すべき要件が無いので、多く使用される公開鍵暗号を選定している。暗号利用形態「守秘」において共通鍵暗号を選定したため、暗号利用形態「鍵共有」が必要となり、特に考慮すべき要件が無いので、多く使用されている公開鍵暗号を選定している。

表４．２．１－２　暗号技術分類選定表のサンプル※

暗号による保護を必要とする情報	暗号利用形態	暗号技術分類	暗号技術への要件
・申請データ ・申請内容確認で授受されるデータ	守秘	共通鍵暗号	・通信速度は、利用者の負担とならない程度の速度であること。 ・多くの利用者にとって利用が負担とならないように、暗号アルゴリズムは標準的なものであることが望ましい。
・到達確認通知 ・状況確認で授受されるデータ	相手認証	公開鍵暗号	
・審査終了通知 ・許認可等公文書の取得要求データ ・許認可等公文書	署名	公開鍵暗号	
・鍵情報	鍵共有	公開鍵暗号	

※ 実際の調達においては、サンプル自体を引用するのではなく、個別具体的な状況に応じた適切な調達を行うこと。

（4）暗号アルゴリズムの選定

本来、電子政府推奨暗号リストに掲載されている暗号アルゴリズムは、安全な実装が行われている限り、すべて安全な暗号であり、電子政府システムにおいてどの暗号アルゴリズムを使用しても問題はない。ここで挙げている観点は、そのような安全な暗号アルゴリズムの中から 1 つ又は必要な数の暗号アルゴリズムを選定する場合に、どのような点に着目すべきかを説明するものである。

なお、最も適切な暗号アルゴリズムの選定が困難な場合は、調達仕様書では複数の暗号アルゴリズムを列挙し、その中から調達参加業者に選択させても構わない。

<< 注意 >>

実装方法によっては、このリストに掲載されている暗号アルゴリズムを使用したとしても、様々な実装攻撃にさらされる危険性を排除できない。したがって、実装攻撃の脅威に対する十分な配慮、検討を行い、適切な対策を施して実装するよう注意すること。

詳しくは、CRYPTREC Report 2002 の第６章「暗号技術の実装に関わる攻撃」を参照すること。

暗号アルゴリズム比較の観点として、次の４点が挙げられる。

これらの観点は、参考２「評価・特徴一覧」からの抜粋である。参考２において記載がない観点は以下に示す比較のための表から省いている。

① 暗号利用形態

機能的に、利用が適している暗号利用形態を掲載している。

共通鍵暗号、ハッシュ関数は、どの暗号利用形態にも適用可能であるので、この欄は省略している。

② 処理速度

Pentium IIIチップを用いた暗号化処理速度における比較。

共通鍵暗号、ハッシュ関数、擬似乱数生成では 3-key Triple DES を基準とした比較を示している。

表中の表示は、

Ａ：処理速度が、3-key Triple DES よりもかなり速い

Ｂ：処理速度が、3-key Triple DES よりも速い

Ｃ：処理速度が、3-key Triple DES と同程度

Ｄ：処理速度が、3-key Triple DES よりも遅い

を意味している。

なお、一般的には、公開鍵暗号による暗号化処理速度は、共通鍵暗号による処理速度の1/100 以下である。

③ メモリ制限環境での実装性（ＩＣカード等）

低機能型ＩＣカード（8 ビットＣＰＵ、ＲＯＭは数 k～10kbyte 程度、ＲＡＭ 128byte 程度）における使用ＲＯＭサイズ、使用ＲＡＭサイズ、処理速度の総合性能による比較。

表中の表示は、

Ａ：メモリ制限環境での実装性が、3-key Triple DES よりもかなり良い

Ｂ：メモリ制限環境での実装性が、3-key Triple DES よりも良い

Ｃ：メモリ制限環境での実装性が、3-key Triple DES と同程度

Ｄ：メモリ制限環境での実装性が、3-key Triple DES よりも劣る

－：未評価

を意味している。

④ プロトコル標準（SSL 3.0、TLS 1.0）

暗号アルゴリズムのうち、標準的暗号プロトコルに採用されているもの、すなわち国民が使用するパソコンの多くにプレインストールされていると思われるものを、SSL 3.0、TLS 1.0 を例にとって掲載している。ただし、これらの標準的暗号プロトコルに規格上は採用されていても、市販の製品には実装されていないものもあるため、注意が必要である。たとえば、共通鍵暗号の AES は、比較的最近 TLS 1.0 に採用されたため、既存の多くの実装には含まれていない。

a)　公開鍵暗号

表４．２．１－３は、電子政府推奨暗号リストに掲載されている公開鍵暗号アルゴリズムの比較表である。

なお、公開鍵暗号に使用される鍵長(より詳しくいえば、例えば RSA 暗号の場合、2 つの素数の積となる合成数のビット長を指す)と処理速度の関係について、一般的には鍵長が 2 倍になると処理速度は数分の 1 になるため、調達するシステムにおいて公開鍵暗号を利用する場合には、許容出来る処理速度の範囲で鍵を長くする（例えば RSA の場合は 1024 ビット以上にする）などの検討が必要である。

表４．２．１－３　公開鍵暗号における暗号アルゴリズム比較表

	DSA	ECDSA	RSASSA-PKCS1-v1_5	RSA-PSS	RSA-OAEP	RSAES-PKCS1-v1_5 *1)	DH	ECDH	PSEC-KEM
①暗号利用形態	署名	署名	署名	署名	守秘	守秘	鍵共有	鍵共有	鍵共有
④プロトコル標準 SSL3.0	○	－	○	－	－	○	○	－	－
TLS	TLS1.0 (Proposed Standard)	Internet-Draft	TLS1.0 (Proposed Standard)	—	—	TLS1.0 (Proposed Standard)	TLS1.0 (Proposed Standard)	Internet-Draft	—

*1）SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。なお、リストに掲載している別の暗号が利用できるのであれば、可能な限りそちらを使用することが望ましい。

なお、公開鍵暗号については、各アルゴリズムの数論的困難性を担保するため、パラメータの選択に十分留意する必要がある。そのため、選択した暗号の仕様書、及び、「CRYPTREC Report 2002」の、選択した暗号に関する記述部分を参考にして記載する。

又は、選択した暗号の仕様書、あるいは「CRYPTREC Report 2002」を業者に提示し、調達するアルゴリズムがパラメータ要件を満たすよう業者に指示しても構わない。

b）共通鍵暗号

表４．２．１－４～表４．２．１－６は、電子政府推奨暗号リストに掲載されている共通鍵暗号アルゴリズムの比較表である。観点の①「暗号利用形態」については、表４．２．１－４、表４．２．１－５では、ブロック暗号はどの暗号アルゴリズムでも相手認証、署名、守秘、鍵共有の全ての暗号利用形態に適用可能なため省略している。また表４．２．１－６では、ストリーム暗号は主に守秘に用いられるため、記載していない。

共通鍵暗号における暗号アルゴリズムの選定は、下記の点に留意して行うこと。

- ブロック暗号は、現在はブロック長が 64 ビットの暗号が多く使われているが安全性の面から、今後は可能な限りブロック長が 128 ビットの暗号を使用すること。
- ストリーム暗号は、高速の通信路で、主に守秘を目的として使用されることが多い。

表４．２．１－４　共通鍵暗号（128 ビットブロック暗号）アルゴリズム比較表

	128 ビットブロック暗号				
	AES	Camellia	CIPHERUNICORN-A	Hierocrypt-3	SC2000
②処理速度	A	A	C	B+	A
③メモリ制限環境での実装性	B+	B+	D以下	B	C+
④プロトコル標準	RFC3268: AES Ciphersuits for TLS (Proposed Standard)	TLS1.0 (Internet Draft)	－	－	－

表４．２．１－５　共通鍵暗号（64 ビットブロック暗号）アルゴリズム比較表

	64 ビットブロック暗号			
	CIPHERUNICORN-E	Hierocrypt-L1	MISTY1	3-key Triple DES
②処理速度	C-	A	B+	（比較基準：C）
③メモリ制限環境での実装性	D以下	B	B+	（比較基準：C）
④プロトコル標準	－	－	－	SSL3.0/TLS1.0 (Proposed Standard)

表４．２．１－６　共通鍵暗号（ストリーム暗号）アルゴリズム比較表

	ストリーム暗号		
	MULTI-S01	MUGI	128-bit RC4 *1
②処理速度	A+	A+	A+
③メモリ制限環境での実装性	－	－	－
④プロトコル標準	－	－	SSL 3.0/TLS 1.0 (Proposed Standard)

*1）128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載している別の暗号が利用できるのであれば、可能な限りそちらを使用することが望ましい。

なお、ブロック暗号を利用した暗号化処理に関連して、安全性の向上を図ったり、伝送中のビット誤りの影響が拡散して復号できなくなる事態を回避したりすることを目的とした、暗号利用モード（Modes of Operation）と呼ばれる技法が、いくつか規定されている。

暗号利用モードごとに実現している目的や特性が異なるので、ブロック暗号の利用にあたっては、実装環境や利用用途に応じて、適切な暗号利用モードを選択する必要がある。なお、代表的な暗号利用モードが JIS X5052 や JIS X5053 に示されているので、これを参考にされたい。

あるいは、上記規格又は「CRYPTREC Report 2002」を業者に提示し、適切な暗号利用モードを選択するよう、業者に指示しても構わない。

c) ハッシュ関数

観点の①「暗号利用形態」については、どのハッシュ関数であっても、適切な公開鍵暗号との組み合わせなどによって、相手認証、署名、守秘、鍵共有のどの暗号利用形態にも適用可能であるため、掲載していない。また、観点③「メモリ制限環境での実装性」は未評価であるため、やはり掲載していない。

ハッシュ関数は公開鍵暗号または共通鍵暗号に付随して使用されることが多い暗号技術であるため、次の３点を考慮して選定する。

1) 電子政府推奨暗号リストに掲載されているハッシュ関数のうち、適切ないずれかを選定する。
2) その場合、可能であれば 256 ビット以上の長さのハッシュ値を出力するハッシュ関数を選択することが望ましい。
3) ただし、すでに選定している公開鍵暗号または共通鍵暗号の暗号アルゴリズム仕様書で指定されている場合は、その限りではない。

表４．２．１－７　ハッシュ関数における暗号アルゴリズムの比較表

	RIPEMD-160	SHA-1	SHA-256	SHA-384	SHA-512
②処理速度	A+	A+	A	C+	C+
④プロトコル標準	－	SSL 3.0/TLS 1.0 (Proposed Standard)	－	－	－
＜参考＞ ハッシュ値の長さ	160 ビット	160 ビット	256 ビット	384 ビット	512 ビット

d) 擬似乱数生成

擬似乱数生成アルゴリズムは、その利用特性上、インタオペラビリティ（相互接続性）を確保する必要性がないため、「暗号学的に安全な擬似乱数アルゴリズム」であれば、どれを利用しても基本的に問題は生じない。したがって、リストに掲載されている擬似乱数生成アルゴリズムのほか、「暗号学的に安全な擬似乱数アルゴリズム」を利用することができる。

なお、リストに掲載されている暗号アルゴリズムの仕様自体に、特定の擬似乱数生成アルゴリズムを使用するよう規定されている場合は、その使用を妨げるものではない。

<< 注意 >>

擬似乱数生成アルゴリズムを実装する場合には、例えば以下の点を考慮すべきである。

- C言語の rand 関数のような擬似乱数生成関数は暗号学的には安全ではないので、暗号アルゴリズムで利用する擬似乱数生成アルゴリズムとして利用してはならない。
- 擬似乱数生成アルゴリズムで利用する種（seed）として、ユーザ ID やプロセス ID、マシン ID、time 関数の出力値など、推測が比較的容易な情報のみを使用することは避ける。
- 種（seed）のビット長として、128 ビット以上にすることが望ましい。
- NIST が発行する NIST Special Publication 800-22, A Statistical Test Suit for Random and Pseudorandom Number Generators に記載されている検定テスト（http://csrc.nist.gov/encryption/tkring を参照のこと）や、フロリダ州立大学 George Marsaglia 教授が開発した DIEHARD による検定テスト（http://stat.fsu.edu/pub/diehard を参照のこと）などの擬似乱数検定法を実施する。この擬似乱数検定法により不合格になった擬似乱数生成アルゴリズムの利用は避けるべきである。なお、擬似乱数生成アルゴリズムの検定方法の詳細については、CRYPTREC Report 2002 の 5.4「擬似乱数生成系の検定方法」を参照されたい。

上記のような考慮が必要な理由は、出力データのランダム性及び予測不可能性（過去の出力ビット列を利用しても次に出力されるビットが推測できないという性質）、種（Seed）の安全性を満たしていない擬似乱数生成アルゴリズムを利用した場合、たとえリストに掲載されている暗号アルゴリズムを利用していても、予期せぬ安全性上の問題を生じさせる可能性がある。このため、暗号アルゴリズムで利用する擬似乱数生成においては、上記の特性を満たすような「暗号学的に安全な擬似乱数生成アルゴリズム」を利用しなければならない。

＜参考　：　作業の進め方の例＞

前項（３）と同じく、電子申請システムを例にとって説明する。

表４．２．１－２で選定した暗号技術分類から、暗号技術への要件を考慮して、選定した暗号アルゴリズムをまとめたものが表４．２．１－８である。

選定にあたっては、標準的な暗号アルゴリズムという要件を考慮し、暗号利用形態「守秘」においては、プロトコル標準 SSL 3.0 に採用されている暗号アルゴリズムのうちもっとも処理速度の速いものを選定している。暗号利用形態「署名」、「鍵共有」も同じくプロトコル標準 SSL 3.0 に採用されている暗号アルゴリズムを選定している。

ハッシュ関数、擬似乱数生成は、暗号アルゴリズム仕様で指定されているものがあればそれを使用するが、特に指定が無い場合のための候補を選定している。

表４．２．１－８　暗号アルゴリズム選定表のサンプル※

暗号による保護を必要とする情報	暗号利用形態	暗号技術分類	暗号アルゴリズム	暗号技術への要件
・申請データ ・申請内容確認で授受されるデータ ・到達確認通知 ・状況確認で授受されるデータ ・審査終了通知 ・許認可等公文書の取得要求データ ・許認可等公文書	守秘	共通鍵暗号	*共通鍵暗号その１*	・通信速度は、利用者の負担とならない程度の速度であること ・多くの利用者にとって利用が負担とならないように、暗号アルゴリズムは標準的なものであることが望ましい
	相手認証	公開鍵暗号	*公開鍵暗号その１* または *公開鍵暗号その３*	
	署名	公開鍵暗号	*公開鍵暗号その１* または *公開鍵暗号その３*	
・鍵情報	鍵共有	公開鍵暗号	*公開鍵暗号その２*	
上記暗号アルゴリズムにて特に指定の無い場合は右記アルゴリズムを使用すること		ハッシュ関数	*ハッシュ関数その１*	
		擬似乱数生成	*擬似乱数生成その１*	

※ 実際の調達においては、サンプル自体を引用するのではなく、個別具体的な状況に応じた適切な調達を行うこと。

（５）調達仕様書記載項目

以上のような手順により、調達者は下記記載例のような「暗号アルゴリズム指定表」を調達仕様書に記載する。

＜参考　：　アルゴリズム指定表の記載例＞

電子申請システムにおける、アルゴリズム指定表の記載例を表４．２．１－９に示す。

表４．２．１－９　暗号アルゴリズム選定表の記載例※

暗号による保護を必要とする情報	暗号利用形態	暗号アルゴリズム
・申請データ ・申請内容確認で授受されるデータ ・到達確認通知 ・状況確認で授受されるデータ ・審査終了通知 ・許認可等公文書の取得要求データ ・許認可等公文書	守秘	*共通鍵暗号その１*
	相手認証	*公開鍵暗号その１* または *公開鍵暗号その３*
	署名	*公開鍵暗号その１* または *公開鍵暗号その３*
・鍵情報	鍵共有	*公開鍵暗号その２*
上記暗号アルゴリズムにて特に指定の無い場合は右記アルゴリズムを使用すること	ハッシュ関数として	*ハッシュ関数その１*
	擬似乱数生成として	*擬似乱数生成その１*

※ 実際の調達においては、サンプル自体を引用するのではなく、個別具体的な状況に応じた適切な調達を行うこと。

４．２．２　提案審査モデルの場合

（１）概要

提案審査モデルの場合、調達者は調達仕様書には最低限の要件だけを指定し、提案を行う業者に、最新の技術や方式、又は斬新なシステムの提案を行わせ、もって電子政府システムとして先端的な、又は最適なシステムを構築することを目的とする。

（２）調達仕様書記載項目

調達者は、下記項目を調達仕様書に記載すること。

a) 電子政府推奨暗号リスト掲載の暗号アルゴリズムの使用に関する指示

調達するシステムでは、可能な限り電子政府推奨暗号リストに記載されている暗号アルゴリズムを使用するよう、提案を行う業者に指示すること。

調達仕様書に記載する内容としては、たとえば、次のような文章が考えられる。

「本システムで使用する暗号アルゴリズムは、本システムのセキュリティ要件を満たし、かつ可能な限り電子政府推奨暗号リストに掲載されている暗号アルゴリズムから、適切なものを選定すること」

b) 暗号アルゴリズム選定理由の明記に関する指示

提案書の審査にあたっては、暗号アルゴリズムの選定（公開鍵暗号のパラメータ選択、及び、共通鍵ブロック暗号の利用モードの選択を含む）が妥当であることを審査する必要があるため、提案を行う業者に、調達するシステムのイメージから暗号アルゴリズム選定（同上）までの過程を理由を付けてわかり易く説明した文書を提案書に添付させること。

調達仕様書に記載する内容としては、たとえば、次のような文章が考えられる。

「提案書には『暗号選定理由書』を添付すること。『暗号選定理由書』では、本システムの仕様から暗号アルゴリズム選定（公開鍵暗号のパラメータ選択、及び、共通鍵ブロック暗号の利用モードの選択を含む）までの過程を、理由を付けてわかりやすく説明すること。なお、使用する用語は可能な限り電子政府推奨暗号リストで使用されている用語にあわせること」

＜参考　：　暗号選定理由の記載例＞

暗号選定理由書の参考例を表４．２．２－１に示す。暗号選定理由書は調達参加業者が作成、提出するものであるが、最低限、次の 3 項目が記載されていることが望ましい。

a) リスク分析の概要と暗号利用形態の選定理由

リスク分析作業のアウトプットとして、暗号による保護を必要とする情報、暗号利用形態、暗号技術への要件について、の選定理由

b) 暗号技術分類の選定理由

個々の暗号利用形態に対して、なぜその暗号技術分類を選定したのか。

c) 暗号アルゴリズムの選定理由

個々の暗号技術分類に対して、なぜその暗号アルゴリズムを選定したのか。

表４．２．２－１　暗号選定理由のサンプル（「守秘」に関する部分）※

項目	選定したもの	選定理由
暗号による保護を必要とする情報	・申請データ ・審査終了通知　... ＜以下略＞...	このシステムで使用する電子情報のうち、暗号による保護を必要とする情報は、「申請データ」、「審査終了通知」、＜中略＞である。
暗号利用形態	守秘	これらの情報は、政府と利用者間でやり取りされるが、そのやり取りはインターネット上で行われるため、盗聴、改竄等のリスクが存在する。その一方で、これらの情報には、利用者のプライバシーに関する情報や事業の展開上秘匿すべき情報が含まれるため、「守秘」による保護が必要である。
暗号に関する要件	・処理速度は、.. ＜以下略＞ ・利用者の負担とならない.. ＜以下略＞	暗号技術への要件としては、利用者に負担をかけないという観点から、「利用者が負担に感じない程度の処理速度」と「可能な限り標準的に実装されている暗号アルゴリズムの使用」が挙げられる。
暗号技術分類	共通鍵暗号	処理速度が高速であること、より一般的に使用されている（鍵情報を公開鍵暗号にて共有し、情報のやり取りは共通鍵暗号にて行う方式が多く使用されている）こと、この 2 点から共通鍵暗号を選定する。
暗号アルゴリズム	*共通鍵暗号その 1*	電子政府推奨暗号リストに掲載されている共通鍵暗号のうち、処理速度がより高速であるもの、標準プロトコルで採用されているもの、この 2 点から「*共通鍵暗号その 1*」を選定する。なお、*共通鍵暗号その 1* の利用用途は＜略＞であるから、利用モードはは「(モード名称)」とした。

※ 実際の調達においては、サンプル自体を引用するのではなく、個別具体的な状況に応じた適切な調達を行うこと。

４．２．３　調達仕様書作成上の留意点

調達者が調達仕様書を作成する際に、留意すべきである点について、以下に示す。

（１） 複数暗号アルゴリズムの実装について

電子政府システムにおけるサーバや、パソコン等に複数の暗号アルゴリズムを同時に実装する事に関する考え方について記載する。
セキュリティ面だけ考えると以下のようにいえる。

a) 複数暗号実装のメリット

電子政府推奨暗号リストに掲載される暗号アルゴリズムにおいては暗号解読問題発生の可能性が低いとはいえ、１つの暗号アルゴリズムが解読された場合に備えて、複数の暗号を実装し切り替えられるようにすることは、セキュリティを向上する上で有効である。

b) 複数暗号実装のデメリット

複数の暗号アルゴリズムを同じシステムに実装し、これを切り替えて利用できるように作り込んだ場合、切り替え部分等にセキュリティホールが混入してしまう恐れがある。そのため、脆弱性が上昇し、セキュリティが減少する可能性がある。

c) 対応策

したがって、セキュリティ脆弱性の上昇により懸念されるリスクが、暗号アルゴリズムが解読されるリスクに比べて小さいと判断された場合にのみ、複数暗号アルゴリズムを実装すべきである。

なお、インターネットなどを通じて広く一般国民が利用するシステムにおいて、利用者の利用する暗号アルゴリズムが全体として１つに特定できない場合などには、政府側のサーバ装置で、複数の暗号アルゴリズムをどちらでも扱えるようにしておかなければならない場合がある。このような場合には、セキュリティホールを作りこまないよう十分な配慮をしつつ複数暗号を実装しておくことが利用者の利便性を向上させる上でも望ましい。

（２）暗号プログラムの配布と、外国為替及び外国貿易法による暗号輸出規制について

不特定多数の利用者に暗号機能を含むプログラムを配布することには、ワッセナー・アレンジメントに基づき、外国為替及び外国貿易法による規制がある。
ここでは、電子政府システムにおいて、不特定多数の利用者に暗号機能を含むプログラムを配布する場合の法制度上の留意点について説明する。

電子政府システムにおいて、政府、国民間でやり取りされる電子情報の保護のために使用される暗号アルゴリズムとして、先進性などの理由から十分に国民に普及していない暗号アルゴリズムを利用する場合、政府が管理するサーバ装置上のホームページ等にてその暗号アルゴリズムを内包する通信プログラムを公開し、不特定多数の利用者が自由にその通信プログラムをダウンロードし、使用できるようにすることが考えられる。
このような、日本国内に居住していない者を含む不特定多数の利用者に暗号機能を含むプログラムを配布することは、外国為替及び外国貿易法（第 25 条第 1 項第 1 号）により、経済産業大臣の許可を必要とする行為である。
そのため、調達者は調達するシステムの形態の検討にあたって、そもそも不特定多数の利用者に通信プログラムを配布しないですむよう配慮するか、又は暗号アルゴリズムの選定または通信プログラムの配布にあたり、配布する通信プログラムが次の３点を全て満たしていることに留意すること。後者の留意については、具体的には、調達仕様上で調達者が確認するか、調達仕様書で「ワッセナー・アレンジメントに関し、外国為替及び外国貿易法による規制に注意して暗号機能を設計すること」等の指示を行うこと。

・市販製品（購入に関して何ら制限されず販売されるもの）をそのまま組み込むか、プログラムが無償で提供されること。
・暗号機能が利用者によって変更できないこと。
・プログラム使用に際して技術支援が不要であるように設計されていること。

なお、認証 *1 またはデジタル署名 *2 のための暗号機能はこの規制の対象外である。

詳しくは、「外国為替及び外国貿易法」（第 25 条第 1 項第 1 号）、「輸出貿易管理令」（第 1 条第 1 項）、「外国為替令」（第 17 条第 1 項）、「輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物または技術を定める省令」（第 8 条第 1 項第 9 号）、「外国為替及び外国貿易法第 25 条第 1 項第 1 号の規定に基づき許可を要する技術を提供する取り引きについて（役務通達）」を参照のこと。

また、これら法令の解釈、個別の状況判断に関する問い合わせは経済産業省 貿易経済協力局 貿易管理部 安全保障貿易管理課（Web ページは、
http://www.meti.go.jp/policy/boekikanri/anpo_hourei/index.html）まで。

*1：ここで言う「認証」にはユーザ認証とデータ認証の 2 つの概念が含まれており、前者は暗号利用形態の「相手認証」にほぼ該当する。後者は「署名」がほぼ該当するが、「鍵共有」が該当する場合もある。実際のシステムにおける利用の形態がここで言う「認証」に該当するかどうかは、個別に経済産業省 貿易経済協力局 貿易管理部 安全保障貿易審査課に確認のこと。

*2：ここで言う「デジタル署名」は暗号利用形態の「署名」にほぼ該当する。実際のシステムにおける利用の形態がここで言う「デジタル署名」に該当するかどうかは、個別に経済産業省 貿易経済協力局 貿易管理部 安全保障貿易審査課に確認のこと。

４．３　調達先決定

調達先決定においては、４．１節の（２）で説明した調達者指定モデルと、提案審査モデルにおいて、作業手順が異なるため、以下では各々のモデルに対して個別に手順の説明を行う。

４．３．１　調達者指定モデルの場合

（１）提案書の審査

この項では、業者から、システム提案書の提出を受けた場合の審査の観点を説明する。

調達者指定モデルの場合では、調達するシステムにおける暗号に関する必要な要件は、既に調達仕様書で指定しているので、ここでは業者の提案が、調達仕様書で指定した要件を満たしているかどうかを確認する。

最も注目すべき点は、指定した暗号利用形態に対して、指定した暗号アルゴリズムを指定通りに使用しているか、という点である。

（２）業者の選定

システムを納入する業者としては、システム全体に対して適切な提案を行った業者を選定するので、暗号に関する要件の満足度だけで業者選定を左右することはない。

一方、暗号に関する要件の満足度は、業者を選定する理由の重要な点でもあるので、ここでは、暗号に関してどのような点に留意すべきかについて述べる。

業者選定における評価項目として、暗号に関するものには次のようなものがある。

・調達仕様書への準拠

業者からの提案において、調達仕様書に指示した暗号アルゴリズムが、同じく指示したパラメータを満たして使用されている場合には、調達仕様書の指示を守ったものとして、評価を是とするか、又は加点する。

４．３．２　提案審査モデルの場合

（１）提案書の審査

提案審査モデルの場合では、業者の提案が、調達するシステムにおける暗号の使用について適切であることを確認する。

審査にあたっては、本ガイドブック「４．２．１　調達者指定モデルの場合」における暗号利用形態選定から暗号アルゴリズム選定までの過程を参照しながら、提案書に添付されている「暗号選定理由書」に記載されている暗号アルゴリズム選定の過程ならびに選定の理由が、論理的に整合性が取れているか、また納得できる内容であるかを、必要に応じて専門家や第三者の助言を仰ぎながら審査する。また、選定された暗号アルゴリズムが電子政府推奨暗号リストに記載されているかどうかも確認する。

（２）業者の選定

システムを納入する業者としては、システム全体に対して適切な提案を行った業者を選定するので、暗号に関する要件の満足度だけで業者選定を左右することはない。

一方、暗号に関する要件の満足度は、業者を選定する理由の重要な点でもあるので、ここでは、暗号に関してどのような点に留意すべきかについて述べる。

業者選定における評価項目として、暗号に関するものには次のようなものがある。

・電子政府推奨暗号リストへの準拠

　業者からの提案において使用されている暗号アルゴリズムが、電子政府推奨暗号リストに掲載されており、かつそのパラメータが各暗号アルゴリズムの仕様書やCRYPTREC Report 2002で指定された要件を満たしている場合には、評価を是とする。

　一方、業者からの提案において使用されている暗号アルゴリズムが、電子政府推奨暗号リストに掲載されていないか、又は電子政府推奨暗号リストに掲載されていても、そのパラメータが各暗号アルゴリズムの仕様書やCRYPTREC Report 2002で指定された要件を満たしていない場合には、その提案の採用は薦められない。

・実装方法の適切さ

　電子政府推奨暗号リストに掲載されている暗号アルゴリズムを使用したとしても、実装方法によっては、様々な実装攻撃にさらされる危険性を排除できない。

　したがって、業者からの提案において、実装攻撃に対する十分な配慮、検討が行われ、適切な対策が施されている場合には、評価を是とする。一方、実装攻撃に対する適切な対策が行われていない場合、その提案の採用は薦められない。

・暗号利用形態と暗号アルゴリズムの対応の適切さ

業者からの提案において、暗号利用形態から暗号アルゴリズム選定までの過程と理由が、論理的に整合性が取れており、納得できる内容である場合には基準を満たしているものとして、評価を是とするか、又は加点する。

４．４　契約

契約は、調達するシステム全体について業者と取り交わすため、暗号だけについて別途契約を取り交わす必要はない。

ただし、暗号製品・システムにかかるセキュリティ上の支障が発見された場合の保守・保証の方法及び範囲について、必要に応じて追加すること。

４．５　納品

ここでは、調達した暗号が正しく実装されていることを確認する方法について説明する。

通常、電子政府システムでは、暗号はシステムの一部として機能するよう設計・構築されており、暗号製品・システムが正しく納品されていることをシステムと切り離して個別に評価することは困難である。したがって、一般に行えるのは、疎通テスト程度となる。

ただし、技術的に踏み込んで、調達した暗号の実装が正しいことをより厳密に確認する方法として、次のような方法が挙げられる。

（１）テストベクトルの利用

テストベクトルを利用したテストでは、まず、正しく実装された暗号において確認された、暗号鍵と暗号化される前のデータ（「データ１」とする）、並びに暗号化された後のデータ（「データ２」とする）の３点を用意する。評価する暗号の実装において、データ１を与えられた暗号鍵で暗号化し、得られたデータとデータ２が同一であることをもって、評価する暗号の実装が正しいとする方式である。

（２）別の暗号製品・システムとの対向通信

評価する暗号と同等の機能を有する、正しく実装された暗号を用意し、それと評価する暗号とを通信させ、様々なパターンのデータについて、一方で暗号化されたデータをもう一方で復号できること、およびその逆方向の処理ができることをもって、評価する暗号の実装が正しいとする方法である。

（３）第三者機関による評価

第三者機関に各種のテストを行わせ、暗号の実装が正しいことを確認させる方法である。米国ではＮＩＳＴが FIPS 140-2 に基づいて、暗号製品の安全性の認定を行っているが、国内においては公的に承認されている評価機関はまだ存在しないので、暗号の専門家に評価を依頼する等の方策が必要である。

５．　連絡先

●本ガイドブックに関する問い合わせ

・総務省　情報通信政策局　通信規格課
　ｅ－ｍａｉｌ：　cryptrec-inq@soumu.go.jp
　ＵＲＬ：　http://www.soumu.go.jp/joho_tsusin/security/security.html
・経済産業省　商務情報政策局　情報政策ユニット　情報セキュリティ政策室
　ｅ－ｍａｉｌ：　it-security@meti.go.jp
　ＵＲＬ：　http://www.meti.go.jp/policy/netsecurity/

●暗号に関する技術的な問い合わせ

・情報処理振興事業協会（ＩＰＡ）　セキュリティセンター　暗号技術グループ
　ｅ－ｍａｉｌ：　cryptrec@ipa.go.jp
　ＵＲＬ：　http://www.ipa.go.jp/security/
・通信・放送機構（ＴＡＯ）　研究企画管理部　研究企画課
　ｅ－ｍａｉｌ：　cryptrec@shiba.tao.go.jp
　ＵＲＬ：　http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html

６．　参考資料

● 各府省の情報システム調達における暗号の利用方針　：参考１
（別添：電子政府推奨暗号リスト）

● 評価・特徴一覧（公開鍵暗号／共通鍵暗号）　：参考２

・JIS－TR X0050（暗号技術評価報告書　CRYPTREC Report 2000）
下記 Web ページよりダウンロード可能
－ http://www.meti.go.jp/policy/netsecurity/crypt.htm
－ http://www.ipa.go.jp/security/enc/CRYPTREC/fy12/cryptrec20010418.html

・暗号技術検討会 2001 年度報告書
下記 Web ページよりダウンロード可能
－ http://www.soumu.go.jp/s-news/2002/020416_2.html
－ http://www.meti.go.jp/policy/netsecurity/crypt.htm

・JIS－TR X0087（暗号技術評価報告書(2001 年度版) CRYPTREC Report 2001）
下記 Web ページよりダウンロード可能
－ http://www.meti.go.jp/policy/netsecurity/crypt.htm
（この Web ページでは、「CRYPTREC Report 2001」と表記している）
－ http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy14/cryptrec20020418_report01.html
－ http://www.ipa.go.jp/security/enc/CRYPTREC/fy14/cryptrec20020418_report01.html

・暗号技術検討会 2002 年度報告書
下記 Web ページよりダウンロード可能
－ http://www.soumu.go.jp/s-news/2003/pdf/030331_4_1.pdf
－ http://www.meti.go.jp/policy/netsecurity/index.html

暗号技術評価報告書　2002 年度版　CRYPTREC Report 2002
下記 Web ページよりダウンロード可能
－ http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030401_report01.html
－ http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec200304_report02.html

７．　用語集

ANSI（American National Standard Institute：米国規格協会）
米国における国内標準を定める民間組織。

FIPS（Federal Information Processing Standard：連邦情報処理規格）
NIST が策定する米国連邦政府の情報処理の標準仕様

Kerberos
暗号による認証方式の一つ。通信経路上の安全が保障されないインターネットなどのネットワークにおいて、サーバとクライアントの間で身元の確認を行なうのに使う。マサチューセッツ工科大学(MIT)の「Athena」プロジェクトによる、認証サービスや関連するプロトコル、プログラムなどの総称。共通鍵暗号を用いることにより、クライアント/サーバアプリケーションに強固な認証システムを提供できるように設計されている。

MAC（Message Authentication Code：メッセージ認証子）
通信当事者間で共有する秘密情報と、送信する情報を組み合わせたうえで、ハッシュ関数などによって処理を行った結果であるデータのこと。MAC を元の情報と一緒に送信し、受信側で受信した情報と秘密情報を組み合わせて処理を行った結果と、受信した MAC が一致すれば、受信した情報が改竄されていないと考えて良い。

NIST（National Institute of Standards and Technology：国立標準技術研究所）
米国政府機関で利用される情報セキュリティ技術等の標準化を行う、商務省傘下の機関

PKI（Public Key Infrastructure：公開鍵基盤）
公開鍵を配布する仕組み、電子証明書を作成・発行・配布する仕組み、電子証明書の有効性を確認する仕組みなどの公開鍵暗号の運用に関わる基盤技術の総称

SECG（Standards for Efficient Cryptography Group）
楕円暗号の業界標準を策定するための国際的コンソーシアム

ストリーム暗号
共通鍵暗号の一種で、データを１ビットないし１バイト程度の短い単位で処理する方式

チャレンジ＆レスポンス

相手認証を行う側（認証側）がランダムに生成したデータ（このデータを「チャレンジ」と呼ぶ）を、相手認証を行われる側（被認証側）に送信し、被認証側で双方が共有している秘密情報を用いて暗号化したデータを認証側に送信する（この行為が「レスポンス」である）。認証側では、認証側で秘密情報を用いて暗号化したデータと、受信したデータを比較して、両者が一致したら被認証側が正当である、とする方式。

ハッシュ値

ハッシュ関数が出力する固定長のデータのこと

ブロック暗号

共通鍵暗号の一種で、データを一定の長さ（ブロック）に分割し、ブロック単位で処理する方式

ブロック長

共通鍵暗号の一種であるブロック暗号における、暗号処理を行う情報の長さの単位

ワッセナー・アレンジメント（the Wassenaar Arrangement）

通常兵器及び関連汎用品・技術の責任ある輸出管理を実施することにより、地域の安定を損なう虞れのある通常兵器の過度の移転と蓄積を防止することを目的として、1996 年 7 月に成立した新しい国際的申し合わせに基づく国際輸出管理体制
より詳しくは、http://www.meti.go.jp/topic/data/ewasenaj.html　を参照のこと

相手認証

暗号利用形態の 1 つで、やりとりの相手の正当性を保証すること

暗号アルゴリズム

暗号機能を実現するための仕様

暗号技術分類

暗号アルゴリズムを、機能的・技術的に類似するグループに整理、分類するためのものであるで、公開鍵暗号、共通鍵暗号の２つの主要な分類と、この２つの主要な分類に付随する２つの分類、ハッシュ関数、擬似乱数生成からなる

暗号利用形態

電子政府システムにおける暗号利用の目的を整理し、４つの形態にまとめたもの

改竄

第三者によって、情報の内容の一部または全部を別のデータで置き換えられてしまうこと

鍵共有

暗号利用形態の 1 つで、インターネット等のオープンなネットワークを用いて共通鍵暗号技術を利用する際に、通信の当事者間で鍵情報を共有すること

鍵長

暗号鍵の長さ。電子政府推奨暗号リストでは、共通鍵暗号の場合で 128〜256 ビット、公開鍵暗号の場合で 1024 ビット以上（素因数分解の困難性に基づく方式の場合）の暗号アルゴリズムが選定されている

擬似乱数生成

暗号技術分類の 1 つで、暗号学的に安全な乱数（過去の履歴から次のビットが予測できないような数字列）にできるだけ近づけた数の系列を人為的に生成する仕組み

共通鍵暗号

暗号技術分類の 1 つで、平文を暗号化する時に使用する鍵と、暗号文を復号する時に使用する鍵が共通の暗号方式。この鍵のことを共通鍵と呼ぶ。
高速性に優れているが、共通鍵の配送を安全に行うことが求められる。
共通鍵暗号はさらに、データを一定の長さ（ブロック）に分割し、ブロック単位で処理を行う方式（ブロック暗号）と、データを 1 ビットないし 1 バイト程度の短い単位で乱数などによって生成される鍵系列を用いて処理する方式（ストリーム暗号、または逐次暗号）に分けることができる。

公開鍵暗号

公開鍵と秘密鍵という対をなす２種類の鍵を用いる暗号（または暗号技術）を総称して公開鍵暗号（または公開鍵暗号技術）という。公開鍵から秘密鍵を求めることは計算の手間が膨大となり事実上困難であるという特性を持っている。守秘のための方式と署名のための方式とに大別でき、前者を（狭い意味で）公開鍵暗号方式、後者を公開鍵署名方式と呼んで区別することがある。前者の意味での公開鍵暗号方式においては、平文を暗号化する時に用いる鍵（暗号化鍵）が公開鍵であり、暗号文を復号する時に用いる鍵（復号鍵）が秘密鍵である。公開鍵署名方式においては、平文に対して署名文を生成する時に用いる鍵（署名生成鍵）が秘密鍵であり、署名文を検査し平文を取り出す時に用いる鍵（署名検査・復号鍵）が公開鍵である。

守秘

暗号利用形態の 1 つで、インターネット等のオープンなネットワークや、記録媒体を使って電子情報をやりとりするときに、知られて良い利用者以外には内容を知られないようにすること

署名

暗号利用形態の 1 つで、電子情報が正当であることを確認できるようにすること
この中には署名を作った者を確認すること（否認防止）と、電子情報自体が改竄されていないかを確認すること（完全性保証）の二つの目的がある

電子政府

「行政の情報化により、事務・事業及び組織の改革を推進するとともに、セキュリティの確保等に留意しつつ、「紙」による情報の管理からネットワークを駆使した電子化された情報の管理へ移行し、高度に情報化された行政」のこと
詳細は「e-Japan 重点計画-2002（http://www.kantei.go.jp/jp/singi/it2/index.html よりダウンロード可能）」を参照のこと

電子政府システム

電子政府を実現するための情報システム
本ガイドブックでは、主に、政府と国民の間で、書類の申請等の電子情報をやり取りするためのシステムを想定して記述している

成りすまし

第三者が、資格のある利用者のふりをして情報を利用すること

否認

情報を送信または受信したにもかかわらず、その事実を認めないこと

漏洩

情報の内容を第三者に知られてしまうこと

参考１

「各府省の情報システム調達における暗号の利用方針」

参考１

各府省の情報システム調達における暗号の利用方針

平成１５年2月２８日
行政情報システム関係課長連絡会議了承

電子政府における情報セキュリティ確保のために、各府省の情報システムにおいて暗号を利用する場合には、一定水準以上の安全性及び信頼性を有する暗号の利用が不可欠であり、また、その安全性・信頼性は客観的な評価を得たものであることが必要である。

かかる観点から、「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」（平成１３年１０月１０日、情報セキュリティ対策推進会議）に基づき、総務省及び経済産業省において、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（「電子政府推奨暗号リスト」：別添参照）を策定したところである。

これを踏まえ、各府省は、情報システムの構築に当たり暗号を利用する場合には、調達仕様書において上記暗号リストに掲載された暗号を利用することを入札要件とする等の方法により、必要とされる安全性・信頼性などに応じ、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとする。

なお、総務省及び経済産業省は、「電子政府推奨暗号リスト」に掲載された暗号の安全性及び信頼性について、今後の情報通信技術の進展を踏まえ必要に応じ評価を行うとともに、「電子政府推奨暗号リスト」の内容の変更を行う場合には本会議に報告することとする。

別　添

電子政府推奨暗号リスト

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注 1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注 2)
共通鍵暗号	64 ビットブロック暗号(注 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注 4)
	128 ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注 5)
その他	ハッシュ関数	RIPEMD-160(注 6)
		SHA-1(注 6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注 7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈：

(注 1)　SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

(注 2)　KEM（Key Encapsulation Mechanism）-DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

(注 3)　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

(注 4)　3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。

1)　FIPS46-3 として規定されていること

2)　デファクトスタンダードとしての位置を保っていること

(注 5)　128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

(注6)　新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

(注7)　擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

参考２

「評価・特徴一覧（公開鍵暗号）」

「評価・特徴一覧（共通鍵暗号）」

「評価・特徴一覧の利用にあたって」

評価・特徴一覧（公開鍵暗号）

利用形態			署名				守秘		鍵共有		
暗号アルゴリズム名			**DSA**	**ECDSA**	**RSASSA-PKCS1-v1_5**	**RSA-PSS**	**RSA-OAEP**	**RSAES-PKCS1-v1_5**	**DH**	**ECDH**	**PSEC-KEM**
参照すべき仕様書			ANSI X9.30:1-1997 (http://www.x9.org/)	SEC1 (Version 1.0) (http://www.secg.org/)	PKCS#1v2.1 (http://www.rsasecurity.com/rsalabs/pkcs/)	PKCS#1v2.1 (http://www.rsasecurity.com/rsalabs/pkcs/)	PKCS#1v2.1 (http://www.rsasecurity.com/rsalabs/pkcs/)	PKCS#1v2.1 (http://www.rsasecurity.com/rsalabs/pkcs/)	ANSI X9.42-2001 (http://www.x9.org/)	SEC1 (Version 1.0) (http://www.secg.org/)	PSEC-KEM仕様書(2002 年5 月14日) (http://info.isl.ntt.co.jp/psec/CRYPTREC/index-j.html)
リストに載せた根拠	経験的安全性		○	○	○	○	○	○	○	○	-
	証明可能安全性の有無		-	-	-	○	○	-	-	-	○
		仮定するモデル	-	-	-	ランダムオラクルモデル	ランダムオラクルモデル	-	-	-	ランダムオラクルモデル
		帰着される問題	-	-	-	RSA問題の困難性	RSA問題の困難性	-	-	-	楕円曲線上のDH計算問題
		安全性の到達度	-	-	-	適応的選択文書攻撃に対して存在的偽造不可	適応的選択暗号文攻撃に対して強秘匿	-	-	-	鍵カプセル化メカニズムとして適応的選択暗号文攻撃に対して強秘匿
プリミティブの安全性の根拠			有限体上の離散対数問題	楕円曲線上の離散対数問題	素因数分解問題	素因数分解問題	素因数分解問題	素因数分解問題	有限体上の離散対数問題	楕円曲線上の離散対数問題	楕円曲線上の離散対数問題
主なパラメータ・補助関数に関する要件	パラメータの範囲		・「参照すべき仕様書」に記載の各暗号技術の仕様書で指定されたパラメータのうち、CRYPTREC Report 2002で指定された条件を満たすものを使用すること								
	ハッシュ関数		・電子政府推奨暗号リストに記載されたものを使用すること					-	・電子政府推奨暗号リストに記載されたものを使用すること		
	擬似乱数生成器		・電子政府推奨暗号リストの注釈7を参照のこと								
国際標準等への採用状況 (2003年1-3月期)	仕様策定	電子署名法に係る指針	○	○	○	○	-	-	-	-	-
		ANSI[注1]	・X9.30:1-1997	・X9.62-1998	-	-	-	・X9.44(Draft)	・X9.42-2001	・X9.63-2001	-
		IEEE[注2]	・P1363-2000	・P1363-2000	・P1363a(Draft)	・P1363a(Draft)	・P1363-2000	-	・P1363-2000	・P1363-2000	
		ISO/IEC[注3]	・14888-3	・14888-3 ・15946-2	-	-	-	-	・11770-3	・11770-3 ・15946-3	・18033-2(Committee Draft)
		NESSIE[注4]	-	○	-	○	-	-	-	-	○ (Public-key Encryptionとして)
		NIST[注5]	・FIPS PUB 186-2(+Change Notice1)	・FIPS PUB 186-2(+Change Notice1)	-	-	-	-	-	-	-
	利用実績	IETF[注6]	・RFC2246(Proposed Standard) ・RFC3275(Draft Standard) ・RFC3279(Proposed Standard) ・RFC3370(Proposed Standard)	・RFC3278(Informational) ・RFC3279(Proposed Standard) ・ipsec(Internet-Draft) ・tls(Internet-Draft)	・RFC2246(Proposed Standard) ・RFC3275(Draft Standard) ・RFC3279(Proposed Standard) ・RFC3370(Proposed Standard) ・RFC3447(Informational)	・RFC3447(Informational) ・pkix(Internet-Draft) ・smime(Internet-Draft)	・RFC3447(Informational) ・pkix(Internet-Draft) ・smime(Internet-Draft)	・RFC2246(Proposed Standard) ・RFC3370(Proposed Standard) ・RFC3447(Informational)	・RFC2246(Proposed Standard) ・RFC2409(Proposed Standard) ・RFC2631(Proposed Standard) ・RFC3370(Proposed Standard) ・RFC3279(Proposed Standard)	・RFC3278(Informational) ・RFC3279(Proposed Standard) ・ipsec(Internet-Draft) ・tls(Internet-Draft)	-
		SET[注7]	-	-	○	-	-	-	-	-	-
		SSL3.0[注8]	○	-	○	-	-	○	○	-	-
		WAP/WTLS[注9]	-	○	○	-	-	○	○	○	-
		W3C[注10]	・XML-Signature Syntax and Processing(12 February 2002)	-	・XML-Signature Syntax and Processing(12 February 2002)	-	・XML Encryption Syntax and Processing(10 December 2002)	・XML Encryption Syntax and Processing(10 December 2002)	・XML Encryption Syntax and Processing(10 December 2002)	-	-
提案元			・ANSI	・Standards for Efficient Cryptography Group (SECG)	・RSA Laboratories	・RSA Laboratories	・RSA Laboratories	・RSA Laboratories	・ANSI	・Standards for Efficient Cryptography Group (SECG)	・日本電信電話株式会社
電子政府利用にあたっての知的財産権の実施の権利に関する考え方	問い合わせ先		ー	富士通株式会社	RSAセキュリティ株式会社	RSAセキュリティ株式会社	RSAセキュリティ株式会社	RSAセキュリティ株式会社	ー	富士通株式会社	日本電信電話株式会社
	(a) 該当する知的財産権		(参考情報) ・ISO/IEC 14888-3 Annex Gでは、Contact Address欄に[no license required]と記載されている ・U.S. Patent 5,231,668, July 1993	・SECG member patent letters (http://www.secg.org/collateral/certicom_secg_patent.pdf)を参照のこと。 ・富士通株式会社の所有する特許は、特になし。	RSAセキュリティ株式会社は、上記アルゴリズムについての知的財産権を持たない。ただし、上記アルゴリズムを具現化したソフトウェア（RSA BSAFEシリーズ）についての著作権は、同社に帰属する。	RSAセキュリティ株式会社は、上記アルゴリズムについての知的財産権を持たない。ただし、上記アルゴリズムを具現化したソフトウェア（RSA BSAFEシリーズ）についての著作権は、同社に帰属する。	RSAセキュリティ株式会社は、上記アルゴリズムについての知的財産権を持たない。ただし、上記アルゴリズムを具現化したソフトウェア（RSA BSAFEシリーズ）についての著作権は、同社に帰属する。	RSAセキュリティ株式会社は、上記アルゴリズムについての知的財産権を持たない。ただし、上記アルゴリズムを具現化したソフトウェア（RSA BSAFEシリーズ）についての著作権は、同社に帰属する。	(参考情報) ・U.S. Patent 4,200,770, April 1980(1997年に失効している)	・SECG member patent letters (http://www.secg.org/collateral/certicom_secg_patent.pdf)を参照のこと。 ・富士通株式会社の所有する特許は、特になし。	・特開2000-148011「ランダム関数利用公開鍵暗号の暗号装置」 ・特開2001-222218「暗号化装置、方法、複合装置、方法、暗号システム及びプログラムを記憶した記憶媒体」
	(b) 上記(a)の知的財産権の扱い[注11]		ー	(2) ※当該知的財産権の内容、条件の詳細は、特許所有者、及びSECGのウェブサイトを参照のこと。 (http://www.secg.org/patent_policy.htm , http://www.secg.org/collateral/certicom_secg_patent.pdf , http://www.secg.org/index.htm) 富士通は、本アルゴリズムに関する特許を所有していない。特許技術の使用許諾が必要となる場合には、上記URLを参照の上、特許所有者と交渉すること。	ー	ー	ー	ー	ー	(2) ※当該知的財産権の内容、条件の詳細は、特許所有者、及びSECGのウェブサイトを参照のこと。 (http://www.secg.org/patent_policy.htm , http://www.secg.org/collateral/certicom_secg_patent.pdf , http://www.secg.org/index.htm) 富士通は、本アルゴリズムに関する特許を所有していない。特許技術の使用許諾が必要となる場合には、上記URLを参照の上、特許所有者と交渉すること。	(1)
特記事項			・より大きなサイズのパラメータを選択可能とするために仕様の変更が検討されていることに注意を払う必要がある。	・電子署名法の指針にも（一部のパラメータを除いて）適合している。 ・Koblitz曲線と呼ばれる曲線は、そのクラス特有の攻撃法が出現する可能性に注意を払う必要がある。	ー	ー	ー	・SSL3.0/TLS1.0で使用実績があり当面の使用を認める。	・鍵とエンティティとの結び付きを保証する手段を備え、またセッション鍵として使用する場合、交換する公開鍵は一時的なものとするべきである。	・鍵とエンティティとの結び付きを保証する手段を備え、またセッション鍵として使用する場合、交換する公開鍵は一時的なものとするべきである。 ・Koblitz曲線と呼ばれる曲線は、そのクラス特有の攻撃法が出現する可能性に注意を払う必要がある。	・KEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism)構成における利用を前提とする。 ・Koblitz曲線と呼ばれる曲線は、そのクラス特有の攻撃法が出現する可能性に注意を払う必要がある。

注1: 米国規格協会(http://www.ansi.org) 注2: IEEE（電気電子学会）(http://homepage1.nifty.com/ieeetokyo/faq.htmによる) 注3: 国際標準化機構（International Organization for Standardization）/国際電気標準会議（International Electrotechnical Commission）(http://www.jisc.go.jp/international/isoiec.htmlによる) 注4: 欧州における暗号技術評価プロジェクトで、New European Schemes for Signatures, Integrity, and Encryptionの略称(http://www.cryptonessie.org) 注5: 米国の国立標準技術局(http://www.nist.gov) 注6: インターネットに係わる技術の標準化を制定する業界団体(Internet Engineering Task Force)(http://www.ietf.org/) 注7: Secure Electronic Transactionの略称(http://www.setco.org/) 注8: Secure Sockets Layer protocol(http://wp.netscape.com/eng/ssl3/) 注9: Wireless Application Protocol(http://www.wapforum.org/) 注10: World Wide Web Consortium(http://www.w3.org/) 注11: 括弧内の数字の意味については、別添2「評価・特徴一覧の利用にあたって」の「○公開鍵暗号／共通鍵暗号　共通」「知的財産権情報について」を参照のこと。

評価・特徴一覧（共通鍵暗号）

1. 64 ビットブロック暗号

評価項目			CIPHERUNICORN-E	Hierocrypt-L1	MISTY1	3-key Triple DES
アルゴリズム安全性評価コメント*			[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない	[B] FIPS 等で保証されている間は問題ないと考える
実装性	ソフトウェア実装	Pentium III 実装	[C-] 総合的な処理性能は Triple DES 同程度以下 • 暗号化処理速度[C-]：Triple DES の 0.6 倍程度の性能 • 鍵生成込暗号化処理[C-]：Triple DES の 0.8 倍程度の性能	[A] 総合的な処理性能は Triple DES よりもかなり高い • 暗号化処理速度[A]：Triple DES の 4.25 倍前後の性能 • 鍵生成込暗号化処理[A/B+]：暗号化では Triple DES の 5.25 倍程度、復号では同 3.2 倍程度の性能	[B+] 総合的な処理性能は Triple DES よりも高い • 暗号化処理速度[B+]：Triple DES の 4 倍超の性能 • 鍵生成込暗号化処理[A]：Triple DES の 5.5 倍超の性能	[C] 実用的には問題ないことも多いが、一般には処理速度が遅いといわれる（基準性能） • 暗号化処理速度は遅いといわれる[C] • 鍵生成込暗号化処理は遅いといわれる[C]
		他プラットフォーム実装	[C-] 総合的な処理性能は Triple DES 同程度以下 • UltraSPARC IIi での暗号化処理速度[C-]、鍵生成込暗号化処理[D] • Alpha 21264 での暗号化処理速度[C-]、鍵生成込暗号化処理[C/C-]	[B+] 総合的な処理性能は Triple DES よりも高い • UltraSPARC IIi での暗号化処理速度[B]、鍵生成込暗号化処理[B/C] • Alpha 21264 での暗号化処理速度[A]、鍵生成込暗号化処理[A/B+] • 鍵生成込暗号化処理は暗号化よりも復号の方がより重い	[B+] 総合的な処理性能は Triple DES よりも高い • UltraSPARC IIi での評価なし • Alpha 21264 での暗号化処理速度[A]、鍵生成込暗号化処理[A]	[C] 実用的には問題ないことも多いが、一般には処理速度が遅いといわれる • 暗号化処理速度は遅いといわれる[C] • 鍵生成込暗号化処理は遅いといわれる[C]
		鍵即応性**	[C] 鍵交換ペナルティは中程度 • 鍵生成時間は Triple DES と同程度である	[B]鍵交換ペナルティは少ない • 鍵生成時間は、暗号化では Triple DES の 1/5 程度、復号では 2/5 程度である • 復号の場合には、暗号化の場合と比較して、少なくとも鍵生成または復号のどちらかにより重い処理を実行させることが必要となるため、全体として性能が低下する	[B] 鍵交換ペナルティは少ない • 鍵生成時間は Triple DES の 1/7 程度である	[C] 鍵交換ペナルティは中程度 • 鍵生成時間は暗号化処理と同程度の時間が必要である
	メモリ制限環境での実装性能（低機能型 IC カード評価***）		[D 以下] 評価未実施であり、最終的な結論ではないが、少なくとも Triple DES の処理性能と同程度以上にはならないと推定	[B] やや使用 ROM サイズが大きいことを除けば、総合的な処理性能および実装性は Triple DES よりもやや優れている • 使用 ROM サイズはやや大きい[D] • 使用 RAM サイズは少ない[C] • 処理速度は Triple DES よりも高速であるが、復号性能は暗号化性能の約 85%程度[B+]	[B+] 総合的な処理性能および実装性は Triple DES よりも優れている • 使用 ROM サイズは中程度[C-] • 使用 RAM サイズは中程度[C-] • 処理速度は Triple DES よりも高速である[B+]	[C] 総合的な処理性能および実装性はおおむね良好である • 使用 ROM サイズは少ない[C] • 使用 RAM サイズは少ない[C] • 処理速度は中程度といわれる[C]
	ハードウェア実装		第三者実装が可能であることを確認	第三者実装が可能であることを確認	第三者実装が可能であることを確認	第三者実装が可能であることを確認

* アルゴリズム安全性評価コメント：暗号アルゴリズムそのものの安全性強度を評価したものであり、実装攻撃の脅威は対象としていない。実装攻撃に対する概要について、CRYPTREC Report 2002 第 3 章『共通鍵暗号技術の評価』中の個別暗号技術の結果（第 3.3 節）ならびに第 6 章『暗号技術の実装に関わる攻撃』を参照すること。

** 鍵即応性：パケット通信のように、大量の短いデータ（数十 byte 程度）を異なる秘密鍵で暗号化（あるいは復号）するときの処理性能適性をあらわす。処理速度だけでなく、鍵生成（鍵セットアップ）に関する処理負荷も大きな特性要素となる。

*** メモリ制限環境での実装性能：低機能型 IC カード（8 ビット CPU、ROM 数 k～10kbyte 程度、RAM128byte 程度）を想定した評価を基にしている。

評価・特徴一覧（共通鍵暗号）

（続）64 ビットブロック暗号

評価項目			CIPHERUNICORN-E	Hierocrypt-L1	MISTY1	3-key Triple DES
その他	国際標準などへの採用状況	仕様が定められた規格	ISO/IEC 9979 （アルゴリズム公開登録）	なし	IETF RFC 2994 (Informational) ISO/IEC 9979 （アルゴリズム公開登録） ISO/IEC 18033-3 (Committee Draft) NESSIE	ANSI X9.52-1998 ANSI X9.65 (Working Draft) FIPS PUB 46-3 ISO/IEC 18033-3 (Committee Draft)
		仕様が引用された規格	なし	なし	なし	RFC 2246: SSL3.0/TLS1.0 (Proposed Standard)
	電子政府利用にあたっての提案元が保有する知的財産権の実施の権利に関する考え方	(a)該当する知的財産権	特許 出願番号：出願平 9-213274 名称： 暗号装置及び暗号装置を実現するプログラムを記録したコンピューターが読み取り可能な記録媒体 著作物 CIPHERUNICORN-E のプログラム 商標 登録番号 第 4221077 号	特許出願番号（公開番号） 特願 2000-210484 「暗号化装置及び暗号化方法、復号装置及び復号方法並びに演算装置」 特許出願番号（公開番号） 特願 2000-211686 「暗号化装置、復号装置及び拡大鍵生成装置、拡大鍵生成方法並びに記憶媒体」 特許出願番号（公開番号） 特願 2000-212175 「パラメータ決定装置、パラメータ決定方法、暗号化装置、および復号装置」 特許出願番号（公開番号） 特願 2001-68742 「暗号化装置及び暗号化方法、復号装置及び復号方法並びに記憶媒体」	出願番号 PCT/JP96/02154 「データ変換装置及びデータ変換方法」 （参考） 日本特許： 特許第 3035358 号	FIPS PUB 46-3 において、Patents に関する記述は以下のとおり。 「**Patents.** Cryptographic devices implementing this standard may be covered by U.S. and foreign patents, including patents issued to the International Business Machines Corporation. However, IBM has granted nonexclucive, royality-free licenses under the patents to make, use and sell apparatus which complies with this standard. The terms, conditions and scope of the licenses are set out in notices published in the May 13, 1975 and August 31, 1976 issues of the Official Gazette of the United States Patent and Trademark Office (934 O.G. 452 and 949 O.G. 1717).」
		(b) 上記(a)の知的財産権の扱い	（2）	（2）	（1）	下記問い合わせ先 URL 等を参照のこと。
	提案元		日本電気株式会社	株式会社東芝	三菱電機株式会社	NIST
	問い合わせ先		日本電気株式会社	株式会社東芝	三菱電機株式会社	http://csrc.nist.gov/encryption/tkencryption.html
	特記事項					• FIPS46-3 に登録されており、かつデファクトスタンダードの地位にあることを考慮し、当面の使用を認める。 • 2-key Triple DES での使用は推奨しない。

2. 128 ビットブロック暗号

評価項目			AES	Camellia	CIPHERUNICORN-A	Hierocrypt-3	SC2000
アルゴリズム安全性評価コメント*			[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない
実装性	ソフトウェア実装	Pentium III 実装 (128 ビット鍵)	[A] 総合的な処理性能は Triple DES よりもかなり高い • 暗号化処理速度[A+/A]：暗号化では Triple DES の 7 倍超、復号では同 4.75 倍程度の性能 • 鍵生成込暗号化処理[A+/B]：暗号化では Triple DES の 7 倍弱、復号では同 2.3 倍程度の性能 • 鍵長により処理速度が 15-30%程度低下	[A] 総合的な処理性能は Triple DES よりもかなり高い • 暗号化処理速度[A]：Triple DES の 5.25 倍程度の性能 • 鍵生成込暗号化処理[A+]：Triple DES の 8.3 倍超の性能 • 鍵長により処理速度が 25%程度低下	[C] 総合的な処理性能は Triple DES 同程度 • 暗号化処理速度[C]：Triple DES 同程度の性能 • 鍵生成込暗号化処理[C]：Triple DES の 0.8 倍程度の性能 • 鍵長による処理速度低下はほとんどない	[B+] 総合的な処理性能は Triple DES よりも高い • 暗号化処理速度[A/B+]：Triple DES の 4 倍超の性能 • 鍵生成込暗号化処理[A/B+]：暗号化では Triple DES の 5.5 倍弱、復号では同 3 倍弱の性能 • 鍵長により処理速度が 15-25%程度低下	[A] 総合的な処理性能は Triple DES よりもかなり高い • 暗号化処理速度[A]：Triple DES の 4.25 倍前後の性能 • 鍵生成込暗号化処理[A]：Triple DES の 5 倍弱の性能 • 鍵長によって、処理速度が 15%程度低下
		他プラットフォーム実装	[A] 総合的な処理性能は Triple DES よりもかなり高い • UltraSPARC IIi での評価未実施 • Alpha 21264 での暗号化処理速度[A+/-]、鍵生成込暗号化処理は[B+/-] • 鍵生成込暗号化処理は、暗号化よりも復号の方がより重いとされる	[A] 総合的な処理性能は Triple DES よりもかなり高い • UltraSPARC IIi での暗号化処理速度[A]、鍵生成込暗号化処理[A] • Alpha 21264 での暗号化処理速度[A+]、鍵生成込暗号化処理[A+]	[C-] 総合的な処理性能は Triple DES 同程度以下 • UltraSPARC IIi での暗号化処理速度[C-]、鍵生成込暗号化処理[D-] • Alpha 21264 での暗号化処理速度[C/C+]、鍵生成込暗号化処理[C/C-]	[B+] 総合的な処理性能は Triple DES よりも高い • UltraSPARC IIi での暗号化処理速度[B+/B]、鍵生成込暗号化処理[B+/C] • Alpha 21264 での暗号化処理速度[A]、鍵生成込暗号化処理[A/B+] • 鍵生成込暗号化処理は、暗号化よりも復号の方がより重い	[A] 総合的な処理性能は Triple DES よりもかなり高い • UltraSPARC IIi での暗号化処理速度[A]、鍵生成込暗号化処理[B+] • Alpha 21264 での暗号化処理速度[A+]、鍵生成込暗号化処理[A+] • キャッシュサイズが大きい CPU では実装性能が向上
		鍵即応性**	[B/C] 鍵交換ペナルティは小～中程度 • 鍵生成時間は、暗号化では Triple DES の 1/5 程度、復号では Triple DES と同程度である • 復号の場合には、暗号化の場合と比較して、少なくとも鍵生成または復号のどちらかにより重い処理を実行させることが必要となるため、全体として性能が低下する	[B] 鍵交換ペナルティは小さい • 鍵生成時間は Triple DES の 1/7 程度である	[D] 鍵交換ペナルティは大きい • 鍵生成時間は Triple DES の 3 倍程度である	[B/C] 鍵交換ペナルティは小～中程度 • 鍵生成時間は、暗号化では Triple DES の 1/3 程度、復号では Triple DES と同程度である • 復号の場合には、暗号化の場合と比較して、少なくとも鍵生成または復号のどちらかにより重い処理を実行させることが必要となるため、全体として性能が低下する	[B] 鍵交換ペナルティは小さい • 鍵生成時間は Triple DES の 1/3 程度である

* アルゴリズム安全性評価コメント：暗号アルゴリズムそのものの安全性強度を評価したものであり、実装攻撃の脅威は対象としていない。実装攻撃に対する概要について、CRYPTREC Report 2002 第 3 章『共通鍵暗号技術の評価』中の個別暗号技術の結果（第 3.3 節）ならびに第 6 章『暗号技術の実装に関わる攻撃』を参照すること。

** 鍵即応性：パケット通信のように、大量の短いデータ（数十 byte 程度）を異なる秘密鍵で暗号化（あるいは復号）するときの処理性能適性をあらわす。処理速度だけでなく、鍵生成（鍵セットアップ）に関する処理負荷も大きな特性要素となる。

評価･特徴一覧（共通鍵暗号）

（続）128 ビットブロック暗号

評価項目			AES	Camellia	CIPHERUNICORN-A	Hierocrypt-3	SC2000
実装性	メモリ制限環境での実装性能（低機能型 IC カード評価***）		[B+] 総合的な処理性能および実装性は Triple DES よりも優れている • 使用 ROM サイズは少ない[C] • 使用 RAM サイズは中程度[C-] • 処理速度は Triple DES よりも高速である[B+] • 復号処理速度は暗号化処理速度の約 70%程度	[B+] 総合的な処理性能および実装性は Triple DES よりも優れている • 使用 ROM サイズは少ない[C] • 使用 RAM サイズは中程度[C-] • 処理速度は Triple DES よりも高速である[B+]	[D 以下] 評価未実施であり、最終的な結論ではないが、少なくとも Triple DES の処理性能と同程度以上にはならないと推定	[B] やや使用メモリ量が大きいことを除けば、総合的な処理性能および実装性は Triple DES よりやや優れている • 使用 ROM サイズはやや大きい[D] • 使用 RAM サイズはやや大きい[D] • 処理速度は Triple DES よりも高速である[B+/B] • 復号処理速度は暗号化処理速度の約 70%程度	[C+] 総合的な処理性能および実装性は Triple DES と同程度以上 • 使用 ROM サイズは中程度[C-] • 使用 RAM サイズは中程度[C-] • 処理速度は Triple DES 同程度以上[C+]
	ハードウェア実装		第三者実装が可能であることを確認	第三者実装が可能であることを確認	第三者実装が可能であることを確認	第三者実装が可能であることを確認	第三者実装が可能であることを確認
その他	国際標準などへの採用状況	仕様が定められた規格	FIPS PUB 197 ISO/IEC 18033-3 (Committee Draft) NESSIE	IETF RFC: (Internet Draft) ISO/IEC 18033-3 (Committee Draft) NESSIE	なし	なし	なし
		仕様が引用された規格	IETF RFC 3268: AES Ciphersuites for TLS (Proposed Standard) IETF RFC 3394: AES Key Wrap Algorithm (Informational) IETF S/MIME (Internet Draft) IETF IPsec (Internet Draft) TV-Anytime Forum Specification S-7 WAP/WTLS1.0	IETF TLS1.0 (Internet Draft) IETF S/MIME (Internet Draft) TV-Anytime Forum Specification S-7	なし	なし	なし
	電子政府利用にあたっての提案元が保有する知的財産権の実施の権利に関する考え方	(a) 該当する知的財産権	FIPS PUB 197 において、Patents に関する記述は以下のとおり。 「Patents. Implementation of the algorithm specified in this standard may be covered by U.S. and foreign patents.」	特願 2001-565161 「データ変換装置及びデータ変換方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体」 PCT/JP01/01796 「データ変換装置及びデータ変換方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体」 中華民国出願 90105464 「データ変換装置及びデータ変換方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体」	特許 出願番号：出願平 9-213274 名称：暗号装置及び暗号装置を実現するプログラムを記録したコンピューターが読み取り可能な記録媒体 著作物 CIPHERUNICORN-A のプログラム 商標 登録番号 第 4221077 号	特許出願番号（公開番号） 特願 2000-210484 「暗号化装置及び暗号化方法、復号装置及び復号方法並びに演算装置」 特許出願番号（公開番号） 特願 2000-211686 「暗号化装置、復号装置及び拡大鍵生成装置、拡大鍵生成方法並びに記憶媒体」 特許出願番号（公開番号） 特願 2000-212175 「パラメータ決定装置、パラメータ決定方法、暗号化装置、および復号装置」 特許出願番号（公開番号） 特願 2001-68742 「暗号化装置及び暗号化方法、復号装置及び復号方法並びに記憶媒体」	特願 2001-108016（特開 2001-282102） 「暗号設計装置、暗号設計プログラム及び記憶媒体」 特願 2000-212813（特開 2000-91297） 「F 関数内部に SPN 構造を用いた演算装置及び演算方法」 特願 2000-212814（特開 2002-91295） 「Feistel 構造と SPN 構造とを組み合わせた演算装置及び演算」 特願 2000-212482（特開 2002-91296） 「拡大鍵生成装置及び記憶媒体」
		(b) 上記(a)の知的財産権の扱い	下記問い合わせ先 URL 等を参照のこと。	(1)	(2)	(2)	(2)
提案元			NIST	日本電信電話株式会社 三菱電機株式会社	日本電気株式会社	株式会社東芝	富士通株式会社
問い合わせ先			http://csrc.nist.gov/encryption/tkencryption.html	日本電信電話株式会社 三菱電機株式会社	日本電気株式会社	株式会社東芝	富士通株式会社
特記事項							

*** メモリ制限環境での実装性能：低機能型 IC カード（8 ビット CPU、ROM 数～10KB 程度、RAM128byte 程度）を想定した評価を基にしている。

評価・特徴一覧（共通鍵暗号）

3. ストリーム暗号

評価項目			MUGI	MULTI-S01	128-bit RC4
アルゴリズム安全性評価コメント*			[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない	[B] SSL/TLS としての利用に関しては、今のところ問題は見つかっていない
実装性	ソフトウェア実装	Pentium III 実装	[A+] 処理性能は Triple DES よりもかなり高い • 暗号化処理速度[A+]：Triple DES の 10.75 倍前後の性能である	[A+] 処理性能は Triple DES よりもかなり高い • 暗号化処理速度[A+]：Triple DES の 7.5 倍前後の性能である	[A+] 処理性能は Triple DES よりもかなり高い • 暗号化処理速度[A+]：Triple DES の 8.3 倍の性能である
		鍵即応性**	[E] 鍵交換ペナルティは非常に大きい • 鍵生成時間は Triple DES の 20 倍程度である	[D] 鍵交換ペナルティは大きい • 鍵生成時間は Triple DES の 5 倍前後である	―――
	メモリ制限環境での実装性能（低機能型 IC カード***）		―――	―――	―――
	ハードウェア実装		第三者実装が可能であることを確認	第三者実装が可能であることを確認	―――
その他	国際標準などへの採用状況	仕様が定められた規格	なし	ISO/IEC 18033-4 (Committee Draft)	ISO/IEC 9979 （アルゴリズム非公開登録）
		仕様が引用された規格	なし	なし	RFC 2246: SSL3.0/TLS1.0 (Proposed Standard)
	電子政府利用にあたっての提案元が保有する知的財産権の実施の権利に関する考え方	(a) 該当する知的財産権	特願 2001-145783 （公開番号なし） 「疑似乱数生成装置またはそれを用いた暗号復号処理装置」 特願 2001-274433 （公開番号なし） 「疑似乱数生成装置またはそれを用いた暗号復号処理装置」	特願 2000-108334 （特開 2001-007800） 「暗号化装置および方法」 特願 2000-210690 （特開 2001-324925） 「共通鍵暗号方法及び装置」	RSA セキュリティ株式会社によると、RC4 に関する権利は以下のとおり。 "The mark RC4 is a registered trademark of RSA Security Inc. and may not be used by third parties creating implementations of the algorithm. RSA Security does not hold any patents nor does it have any pending applications on the RC4 algorithm. However, RSA Security does not represent or warrant that implementations of the algorithm will not infringe the intellectual property rights of any third party. Proprietary implementations of the RC4 encryption algorithm are available under license from RSA Security Inc. For licensing information, contact: RSA Security Inc. 2955 Campus Drive, Suite 400, San Mateo, CA 94403-2507, USA, or http://www.rsasecurity.com."
		(b) 上記(a)の知的財産権の扱い	（2）	（2）	下記問い合わせ先等に照会のこと。
	提案元		株式会社日立製作所	株式会社日立製作所	RSA セキュリティ株式会社
	問い合わせ先		株式会社日立製作所	株式会社日立製作所	RSA セキュリティ株式会社
	特記事項				128 ビット鍵長を選択のうえ、SSL3.0/TLS1.0 に限定して利用することを想定している。その他の暗号を利用できるのであれば、そちらを選択することが望ましい。

* アルゴリズム安全性評価コメント：暗号アルゴリズムそのものの安全性強度を評価したものであり、実装攻撃の脅威は対象としていない。実装攻撃に対する概要について、CRYPTREC Report 2002 第 3 章『共通鍵暗号技術の評価』中の個別暗号技術の結果（第 3.3 節）ならびに第 6 章『暗号技術の実装に関わる攻撃』を参照すること。

** 鍵即応性：パケット通信のように、大量の短いデータ（数十 byte 程度）を異なる秘密鍵で暗号化（あるいは復号）するときの処理性能適性をあらわす。処理速度だけでなく、鍵生成（鍵セットアップ）に関する処理負荷も大きな特性要素となる。

*** メモリ制限環境での実装性能：低機能型 IC カード（8 ビット CPU、ROM 数 k～10kbyte 程度、RAM128byte 程度）を想定した評価を基にしている。

評価・特徴一覧（共通鍵暗号）

4. ハッシュ関数

評価項目			RIPEMD-160	SHA-1	SHA-256	SHA-384	SHA-512
アルゴリズム安全性評価コメント*			[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない	[A] 今のところ問題は見つかっていない
実装性	ソフトウェア実装（Pentium III 実装）		[A+] 処理速度は Triple DES よりも極めて速い	[A+] 処理速度は Triple DES よりも極めて速い	[A] 処理速度は Triple DES よりもかなり速い	[C+] 処理速度は SHA-512 相当であり、Triple DES 同程度以上	[C+] 処理速度は Triple DES 同程度以上
	メモリ制限環境での実装性能（低機能型 IC カード***）		―――	―――	―――	―――	―――
	ハードウェア実装		―――	―――	―――	―――	―――
その他	国際標準などへの採用状況	仕様が定められた規格	ISO/IEC 10118-3	ANSI X9.30 (Part2) FIPS PUB 180-2 IETF RFC 3174 (Informational) ISO/IEC 10118-3	FIPS PUB 180-2 NESSIE	FIPS PUB 180-2 NESSIE	FIPS PUB 180-2 NESSIE
		仕様が引用された規格	なし	RFC 2246: SSL3.0/TLS1.0 (Proposed Standard)	なし	なし	なし
	電子政府利用にあたっての提案元が保有する知的財産権の実施の権利に関する考え方	(a) 該当する知的財産権	下記 URL において、Patents に関する記述は以下のとおり。 「The authors of RIPEMD-160 and RIPEMD-128 do not hold any patents on the algorithms (nor on the optional extensions), and are also not aware of any patents on these algorithms.」	FIPS PUB 180-2 において、Patents に関する記述は以下のとおり。 「**Patents.** Implementation of the secure hash algorithms in this standard may be covered by U.S. and foreign patents.」	FIPS PUB 180-2 において、Patents に関する記述は以下のとおり。 「**Patents.** Implementation of the secure hash algorithms in this standard may be covered by U.S. and foreign patents.」	FIPS PUB 180-2 において、Patents に関する記述は以下のとおり。 「**Patents.** Implementation of the secure hash algorithms in this standard may be covered by U.S. and foreign patents.」	FIPS PUB 180-2 において、Patents に関する記述は以下のとおり。 「**Patents.** Implementation of the secure hash algorithms in this standard may be covered by U.S. and foreign patents.」
		(b) 上記(a)の知的財産権の扱い	下記問い合わせ先 URL 等を参照のこと。	下記問い合わせ先 URL 等を参照のこと。	下記問い合わせ先 URL 等を参照のこと。	下記問い合わせ先 URL 等を参照のこと。	下記問い合わせ先 URL 等を参照のこと。
	提案元		Hans Dobbertin, Antoon Bosselaers, and Bart Preneel	NIST	NIST	NIST	NIST
	問い合わせ先		http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html	http://cscr.nist.gov/encryption/tkhash.html	http://cscr.nist.gov/encryption/tkhash.html	http://cscr.nist.gov/encryption/tkhash.html	http://cscr.nist.gov/encryption/tkhash.html
	特記事項		より長いハッシュ値のものを採用することができるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。	より長いハッシュ値のものを採用することができるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。			

* アルゴリズム安全性評価コメント：暗号アルゴリズムそのものの安全性強度を評価したものであり、実装攻撃の脅威は対象としていない。実装攻撃に対する概要について、CRYPTREC Report 2002 第 3 章『共通鍵暗号技術の評価』中の個別暗号技術の結果（第 3.3 節）ならびに第 6 章『暗号技術の実装に関わる攻撃』を参照すること。

** 鍵即応性：パケット通信のように、大量の短いデータ（数十 byte 程度）を異なる秘密鍵で暗号化（あるいは復号）するときの処理性能適性をあらわす。処理速度だけでなく、鍵生成（鍵セットアップ）に関する処理負荷も大きな特性要素となる。

*** メモリ制限環境での実装性能：低機能型 IC カード（8 ビット CPU、ROM 数 k～10kbyte 程度、RAM128byte 程度）を想定した評価を基にしている。

5. 擬似乱数生成系（例示）

評価項目			PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1	PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1	PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1
アルゴリズム安全性評価コメント*			[A] 今のところ、パラメータなどを適切に設定すれば、実用上の重大な問題点は見つかっていない	[A] 今のところ、パラメータなどを適切に設定すれば、実用上の重大な問題点は見つかっていない	[A] 今のところ、パラメータなどを適切に設定すれば、実用上の重大な問題点は見つかっていない
実装性	ソフトウェア実装（Pentium II/III 実装）		[A+] ほぼ SHA-1 の処理速度に等しい。SHA-1 の実装性能を参照。	[A+] ほぼ SHA-1 の処理速度に等しい。SHA-1 の実装性能を参照。	[A+] ほぼ SHA-1 の処理速度に等しい。SHA-1 の実装性能を参照。
	メモリ制限環境での実装性能（低機能型 IC カード***）		―――	―――	―――
	ハードウェア実装		―――	―――	―――
その他	国際標準などへの採用状況	仕様が定められた規格	ANSI X9.42-2001 Annex C.1	FIPS PUB 186-2 (+ change notice 1) Appendix 3.1	FIPS PUB 186-2 (+ change notice 1) Revised Appendix 3.1
		仕様が引用された規格	なし	なし	なし
	電子政府利用にあたっての提案元が保有する知的財産権の実施の権利に関する考え方	(a) 該当する知的財産権	下記問い合わせ先等に照会のこと。	FIPS PUB 186-2 において、Patents に関する記述は以下のとおり。「Patents. The algorithms in this standard may be covered by U.S. and foreign patents.」	FIPS PUB 186-2 において、Patents に関する記述は以下のとおり。「Patents. The algorithms in this standard may be covered by U.S. and foreign patents.」
		(b) 上記(a)の知的財産権の扱い	下記問い合わせ先等に照会のこと。	下記問い合わせ先 URL 等を参照のこと。	下記問い合わせ先 URL 等を参照のこと。
	提案元		ANSI	NIST	NIST
	問い合わせ先		日本規格協会	http://cscr.nist.gov/encryption/tkrng.html	http://cscr.nist.gov/encryption/tkrng.html
	特記事項		仕様書中で定義されている使い方の中には安全とは言い切れない方法がある。利用の際には、CRYPTREC Report 2002 の該当節を確認のうえ、適切な使い方を選択する必要がある。	仕様書中で定義されている使い方の中には安全とは言い切れない方法がある。利用の際には、CRYPTREC Report 2002 の該当節を確認のうえ、適切な使い方を選択する必要がある。	仕様書中で定義されている使い方の中には安全とは言い切れない方法がある。利用の際には、CRYPTREC Report 2002 の該当節を確認のうえ、適切な使い方を選択する必要がある。

* アルゴリズム安全性評価コメント：暗号アルゴリズムそのものの安全性強度を評価したものであり、実装攻撃の脅威は対象としていない。実装攻撃に対する概要について、CRYPTREC Report 2002 第 3 章『共通鍵暗号技術の評価』中の個別暗号技術の結果（第 3.3 節）ならびに第 6 章『暗号技術の実装に関わる攻撃』を参照すること。

** 鍵即応性：パケット通信のように、大量の短いデータ（数十 byte 程度）を異なる秘密鍵で暗号化（あるいは復号）するときの処理性能適性をあらわす。処理速度だけでなく、鍵生成（鍵セットアップ）に関する処理負荷も大きな特性要素となる。

*** メモリ制限環境での実装性能：低機能型 IC カード（8 ビット CPU、ROM 数 k～10kbyte 程度、RAM128byte 程度）を想定した評価を基にしている。

評価･特徴一覧の利用にあたって

○公開鍵暗号/共通鍵暗号　共通

知的財産権情報について

各応募暗号の、電子政府システムでの利用における提案元が保有する知的財産権の実施の権利の取扱いについて、提案元に確認を行った。「(b)　上記(a)の知的財産権の取扱い」の「(1)」「(2)」は、それぞれ以下のような取扱いを示す。

※提案元以外の第三者が保有する知的財産権については、その有無も含めて確認されていないので、注意すること。

(1)　当社は、上記「暗号アルゴリズム名」に記載された暗号アルゴリズムの使用にあたって、上記(a)に記載されている当社保有知的財産権に関し、いかなる者に対しても、非差別的かつ無償で通常実施権(又は著作権の利用)を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権所有者であって、(1)の条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

(2)　当社は、上記「暗号アルゴリズム名」に記載された暗号アルゴリズムの使用にあたって、上記(a)に記載されている当社保有知的財産権に関し、いかなる者に対しても、当該知的財産権の権利の内容、条件を明らかにした上で、非差別的かつ妥当な条件(無償の場合を除く。)で通常実施権(又は著作物の利用)を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権所有者であって、(1)又は(2)の条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

○共通鍵暗号

各評価項目における記号表記は以下のように設定されている。なお、評価基準が各評価項目により異なるので、評価項目間の単純な記号比較は意味がないことに注意されたい。

1.　アルゴリズムの安全性評価について

安全な実装が行われているとの前提のもとに、アルゴリズムそのものの安全性強度を評価したものであり、その結果を表1の基準に従って示す。CRYPTRECとしてはB以上を実用上安全であると判断する。すなわち、電子政府推奨暗号リストに掲載されている暗号は全てB以上の評価を受けたものである。

なお、実装方法によっては、安全とされるアルゴリズムを使用したとしても、さまざまな実装攻撃にさらされる危険性を排除できない。したがって、実装攻撃の脅威に対する十分な配慮・検討を行い、適切な対策を施して実装するよう注意されたい。実装攻撃に対する詳細については、CRYPTREC Report 2002 第 3 章『共通鍵暗号技術の評価』中の個別暗号技術の結果（第 3.3 節）、ならびに第 6 章『暗号技術の実装に関わる攻撃』を参照すること。

表 1：アルゴリズム安全性評価における記号表記基準

A	今のところ問題は見つかっていない
B	学術的には解読可能とされるが、今後 10 年間の使用について実用上の問題はないと考える
C	今後 10 年間に現実時間内で解読に成功する可能性がある
D	現実時間内で解読に成功する

2. ソフトウェア実装評価について

- ソフトウェアによる処理性能では表 2 の基準にしたがって表すものとし、基準表価値として Triple DES の性能を評価「C」の中位に設定する。
  なお、各評価段階は 1.5 倍の処理性能差により区分されるものとする。

性能比較のイメージ図

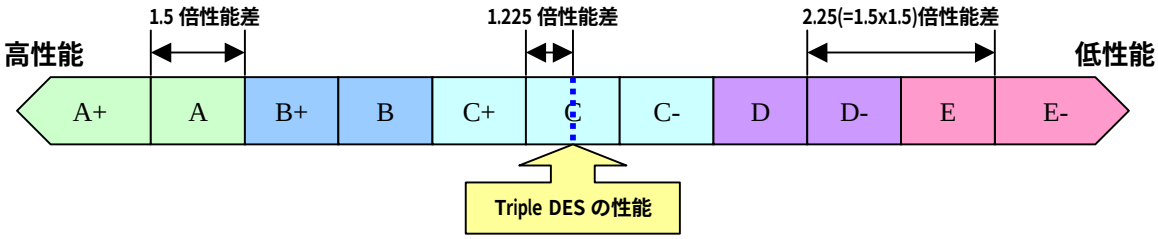


表 2：ソフトウェアによる処理性能における記号表記基準

	Triple DES との相対性能比	評価コメント
A+	6.20 倍以上	Triple DES の処理性能と比較して極めて高い
A	6.20 – 4.13 倍	Triple DES の処理性能と比較してかなり高い
B+	4.13 – 2.76 倍	Triple DES の処理性能と比較して高い
B	2.76 – 1.84 倍	Triple DES の処理性能と比較してやや高い
C+	1.84 – 1.23 倍	Triple DES 同程度以上の性能
C	1.23 – 0.82 倍	Triple DES 同程度の性能
C-	0.82 – 0.54 倍	Triple DES 同程度以下の性能
D	0.54 – 0.36 倍	Triple DES の処理性能と比較してやや低い
D-	0.36 – 0.24 倍	Triple DES の処理性能と比較して低い
E	0.24 – 0.16 倍	Triple DES の処理性能と比較してかなり低い
E-	0.16 倍以下	Triple DES の処理性能と比較して極めて低い

注意事項

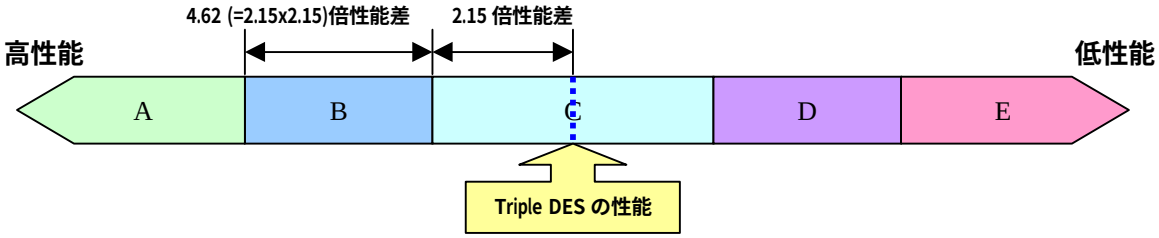
i. 最速値と平均値が測定されている暗号技術については最速値を採用する。
ii. 規定計測プログラムと修正計測プログラムとの両方が測定されている暗号技術については、速い方の値を採用する。
iii. 記号に付随する数値は、Triple DES との相対性能比を表す。
iv. X/Y と表記されている暗号技術は、暗号化性能評価が X、復号性能評価が Y であることを示す。特に区別がない場合は、暗号化性能と復号性能が同程度であることを示す。
v. X～Y と表記されている暗号技術は、プラットフォーム (Pentium II/III, UltraSPARC IIi, Alpha 21264) 等の実装条件によって性能評価が X から Y まで変わりうることを示す。

- ソフトウェアによる鍵即応性では、表 3 に示す基準にしたがって表すものとする。なお、Triple DES の性能を評価「C」の中位に設定する。

表 3：鍵即応性における記号表記基準

	Triple DES 鍵セットアップとの相対クロック比	評価コメント
A	0.10 倍以下	鍵交換ペナルティはほとんどない
B	0.10 – 0.47 倍	鍵交換ペナルティは少ない
C	0.47 – 2.15 倍	鍵交換ペナルティは中程度
D	2.15 – 9.9 倍	鍵交換ペナルティは大きい
E	9.9 倍以上	鍵交換ペナルティが非常に大きい

性能比較のイメージ図



注意事項

i. 本評価の便宜上、暗号化処理速度と鍵込処理速度の差を鍵セットアップ時間とみなす。
ii. 最速値と平均値が測定されている暗号技術については、最速値を採用する。
iii. 規定計測プログラムと修正計測プログラムとの両方が測定されている暗号技術については、速い方の値を採用する。
iv. X/Y と表記されている暗号技術は、暗号化性能評価が X、復号性能評価が Y であることを示す。

- メモリ制限環境における使用メモリ量および逐次副鍵生成の評価項目では、表 4 の基準にしたがって表すものとする。なお、Triple DES の性能を評価「C」の中位に設定するため、評価「A+, A, B+, B」に該当する評価値はないことに注意されたい。

表 4：使用メモリ量および逐次副鍵生成における記号表記基準

	使用メモリ量		逐次副鍵生成 (on-the-fly subkey generation)
	ROM	RAM	
C+	0.5 KB 以下	16 byte 以下	---
C	0.5 – 1.5 KB	16 – 32 byte	処理性能低下および使用 RAM サイズ増加がほとんどなしに実行可能
C-	1.5 – 2.5 KB	32 – 64 byte	処理性能低下および使用 RAM サイズ増加がほとんどなしに実行可能。ただし、復号性能は暗号化性能に比べて劣る。
D	2.5 – 5 KB	64 – 80 byte	若干の処理性能低下または使用 RAM サイズ増加を必要とするが、実行可能
D-	5 – 10 KB	80 – 128 byte	若干の処理性能低下または使用 RAM サイズ増加を必要とするが、実行可能。ただし、復号性能は暗号化性能に比べて劣る。
E	10 – 20 KB	128 – 256 byte	著しい処理性能低下または大幅な使用 RAM サイズ増加がなければ実行困難。
E-	20 KB 以上	256 byte 以上	---

以　上

参考資料「各府省の情報システム調達における暗号の利用方針」

各府省の情報システム調達における暗号の利用方針

平成１５年2月２８日
行政情報システム関係課長連絡会議了承

電子政府における情報セキュリティ確保のために、各府省の情報システムにおいて暗号を利用する場合には、一定水準以上の安全性及び信頼性を有する暗号の利用が不可欠であり、また、その安全性・信頼性は客観的な評価を得たものであることが必要である。

かかる観点から、「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」（平成１３年１０月１０日、情報セキュリティ対策推進会議）に基づき、総務省及び経済産業省において、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（「電子政府推奨暗号リスト」：別添参照）を策定したところである。

これを踏まえ、各府省は、情報システムの構築に当たり暗号を利用する場合には、調達仕様書において上記暗号リストに掲載された暗号を利用することを入札要件とする等の方法により、必要とされる安全性・信頼性などに応じ、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとする。

なお、総務省及び経済産業省は、「電子政府推奨暗号リスト」に掲載された暗号の安全性及び信頼性について、今後の情報通信技術の進展を踏まえ必要に応じ評価を行うとともに、「電子政府推奨暗号リスト」の内容の変更を行う場合には本会議に報告することとする。

別　添

電子政府推奨暗号リスト

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注 1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注 2)
共通鍵暗号	64 ビットブロック暗号(注 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注 4)
	128 ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注 5)
その他	ハッシュ関数	RIPEMD-160(注 6)
		SHA-1(注 6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注 7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈：

(注 1)　SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

(注 2)　KEM（Key Encapsulation Mechanism）-DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

(注 3)　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

(注 4)　3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。

1)　FIPS46-3 として規定されていること

2)　デファクトスタンダードとしての位置を保っていること

(注 5)　128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

(注6)　新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

(注7)　擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。