暗号技術検討会

２００３年度報告書

暗号技術検討会

２００４年３月

目次

【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」

・「暗号調達のためのガイドブック」

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、IT の活用による国民の利便性の向上や行政の効率化を実現するため、申請・届出手続のオンライン化等を推進している。

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が悪質化する等、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、独立行政法人情報処理推進機構（IPA、旧情報処理振興事業協会）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、2002 年度には、それまでの検討及び評価を踏まえ、電子政府推奨暗号リスト案を作成した。これを受けて、総務省及び経済産業省は 2003 年 2 月に「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として公表した。2003 年度は、電子政府推奨暗号の監視、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、暗号モジュール評価基準及び試験基準の作成のための調査・検討、並びに 2004 年度以降の CRYPTREC 活動についての検討を行った。

本報告書は、2003 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、2003 年度の CRYPTREC 活動のうち、詳細な技術的事項については、暗号技術監視委員会及び暗号モジュール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 2003」を御参照頂きたい。

本検討会は、2004 年度も 2003 年度に引き続き、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、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評価基準及び試験基準を作成する等の活動を実施していく必要がある。このためには、CRYPTREC に関係する諸団体が一致団結して前進することが必要であり、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。

2004 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-2003（2003 年 8 月 8 日　IT 戦略本部決定）では、特に、電子政府や電子自治体、重要インフラ等の公共的分野のサービスについては、国民の社会経済活動に大きな影響を及ぼすことのないよう、情報セキュリティ対策の一層の充実を図ることを目標としており、政府は情報セキュリティに関する諸施策を実施している。

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。電子政府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し、2001 年度から本検討会を開催した。両省は、本検討会での検討及び評価の結果を踏まえ 2003 年 2 月 20 日に「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（電子政府推奨暗号リスト）を公表し、2003 年 2 月 28 日には、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あ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」が了承された。

総務省及び経済産業省は、国民が安心して電子政府を利用できるように、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実施していくこととした。

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）及び独立行政法人情報処理推進機構（IPA）が共同で開催する暗号技術監視委員会（委員長：今井秀樹東京大学教授）及び暗号モジュール委員会（委員長：松本勉横浜国立大学教授）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)。暗号技術検討会、暗号技術監視委員会及び暗号モジュール委員会は以下のように検討等を進めた。

２．２．１．暗号技術検討会

暗号技術検討会（以下、「検討会」）は、電子政府推奨暗号の監視、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・検討及び暗号モジュールの評価基準及び試験基準の作成等について、総合的な観点から検討を行った。

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、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・検討を行った。なお、監視委員会の日常業務を行う監視要員を TAO／独立行政法人通信総合研究所（CRL）（両機関は 2004 年 4 月に独立行政法人情報通信研究機構として統合予定）及び IPA に配置した。また、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に、同委員会の下に暗号技術調査 WG として暗号利用モード調査 WG（主査：古原和邦東京大学助手）及び擬似乱数生成系調査 WG（主査：金子敏信東京理科大学教授）を設置し、検討を行った。

監視委員会は 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。

２．２．３．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、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ることをも視野に入れながら、電子政府推奨暗号に準拠した暗号モジュール製品に対する暗号モジュール評価基準及び試験基準の策定に向けた検討を行った。また、上記評価基準及び試験基準の検討に資するため、暗号実装関連技術に関して、サイドチャネル攻撃及びタンパーに関する調査・検討を行った。

暗号モジュール委員会は 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、防衛庁等がオブザーバとして参加した。

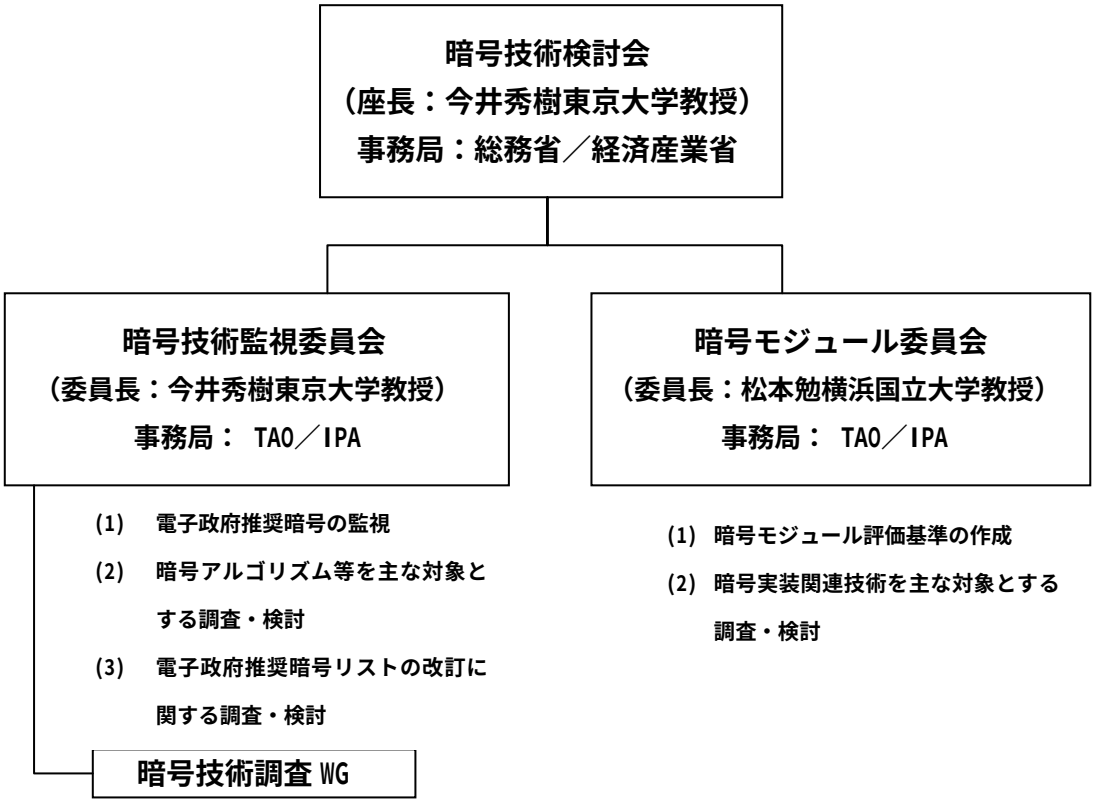


図 1　2003 年度の CRYPTREC の体制図

２．３．暗号技術検討会メンバー

（構成員）※肩書は 2004 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	中央大学理工学部情報工学科教授
	会田　雄一	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
	岩下　直行	日本銀行金融研究所研究第２課企画役
	太田　和夫	電気通信大学電気通信学部情報通信工学科教授
	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）
	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電子情報工学科教授
	国分　明男	財団法人ニューメディア開発協会常務理事・開発グループ長
	櫻井　幸一	九州大学大学院システム情報科学研究院教授
	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 技術部主席研究員
	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
青木　信義	防衛庁長官官房情報通信課長（第 1 回）
河村　延樹	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（第 1 回）
牧　慎太郎	総務省自治行政局自治政策課情報政策企画官（第 2 回～）
中垣　治夫	法務省民事局商事課補佐官
楠田　かおる	外務省大臣官房情報通信課長
宇野　雅夫	財務省日野参事官室企画官（第 1 回）
河野　一郎	財務省大臣官房文書課業務企画室長（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（第 1 回）

坂井　喜毅	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（第 2 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 1 回）
松島　裕一	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（兼）研究エディネータ（情報通信担当）
喜安　拓	通信・放送機構研究企画管理部長（第 1 回）
大久保　明	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（第 1 回）
早貸　淳子	独立行政法人情報処理推進機構セキュリティセンター所長（第 2 回～）
米倉　昭利	財団法人情報処理開発協会電子署名・認証センター長
郡山　信	財団法人金融情報システムセンター監査安全部長

２．４．暗号技術検討会開催状況

2003 年度、検討会は計 3 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。

【第 1 回】2003 年 5 月 26 日（月）

（主な議題）暗号技術検討会の運営方針
暗号技術検討会 2003 年度活動計画

【第 2 回】2003 年 12 月 9 日（火）

（主な議題）暗号技術監視委員会活動報告
暗号モジュール委員会活動報告
今後の CRYPTREC 活動

【第 3 回】2004 年 3 月 23 日（火）

（主な議題）暗号技術監視委員会活動報告
暗号モジュール委員会活動報告
今後の CRYPTREC 活動
暗号技術検討会 2003 年度報告書

３．暗号技術監視委員会活動報告

３．１．監視活動

電子政府推奨暗号リストに掲載された暗号に対する攻撃の予兆や被害に関する情報収集・分析が重要であることから、暗号技術監視委員会が 2003 年度に組織され、活動を行っている。以下に監視委員会の活動内容について説明を行う。

３．１．１．活動の指針

監視委員会は電子政府推奨暗号リスト掲載の暗号に関する研究動向を把握して、暗号技術の安全性について監視を行い、必要に応じて電子政府システムにおける暗号技術の情報収集と電子政府推奨暗号リストの改訂について検討会に対して助言を行う。また、暗号理論全体の技術動向を把握して、最新技術との比較を行い、電子政府システムにおける暗号技術の陳腐化を避けるため、将来の電子政府推奨暗号リストの改正を考慮して、電子政府推奨暗号に関する調査・検討を行う。監視活動は、「情報収集」、「情報分析」、「審議及び決定」の 3 つのフェーズからなる。

検討会における電子政府推奨暗号の監視に関する基本的考え方は以下の通りである。

（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。

以上の指針に基づき、監視委員会では TAO/CRL 及び IPA に監視要員を配置した。監視要員は研究集会、国際会議、研究論文誌、インターネット上の情報等を監視し、電子政府推奨暗号の安全性に関して情報を分析するとともに、それを監視委員会に報告する。監視委員会のもと暗号技術調査ワーキンググループ（以下、「調査 WG」）を構成し、電子政府推奨暗号の安全性に問題を有する疑いがある場合には早急に検討できる体制を作った。また電子政府推奨暗号の応募者からの自発的な情報提供を呼びかけている。監視要員は情報を参考にして情報分析を行い、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。

３．１．２．監視状況

監視活動には、監視委員会のもと、調査 WG の活動、監視要員の調査活動等がある。調査 WG においては擬似乱数生成系の検定法と暗号利用モードについて調査した。1024 ビットの RSA 型合成数の素因数分解問題について、計算機実験と専用ハードウェア構築の実現性の両面からの調査、及び SSL/TLS で実装されている RSA 暗号の問題点に関する

調査を実施した。また代数的攻撃法について注目し監視を行った。

監視要員は研究論文誌、インターネット上の情報や研究集会における情報を収集するとともに、国際学会等に参加し、電子政府推奨暗号に関する安全性を脅かす研究動向があるかどうか監視を行った。その結果 2003 年度においては、監視活動における 3 つのフェーズである「情報収集」、「情報分析」、「審議及び決定」における「審議及び決定」に至る案件はなかった。すなわち、監視要員を主体に情報収集を行ない、その情報を分析した結果、電子政府推奨暗号の安全性に懸念を持たせるような事態はなかった。

一方、検討課題と考えられたものは以下の通りである。

（１）いくつかの擬似乱数生成系の検定法
（２）暗号利用モード
（３）素因数分解問題の現状（TWIRL の実現性と計算機実験）
（４）SSL/TLS で実装される暗号の問題点
（５）代数的攻撃

３．１．３．暗号技術監視委員会開催状況

（１）暗号技術監視委員会

2003 年度、監視委員会は計 3 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。

【第 1 回】2003 年 5 月 19 日（月）
（主な議題）暗号技術監視委員会の運営
暗号技術監視委員会 2003 年度活動方針 等

【第 2 回】2003 年 11 月 19 日（水）
（主な議題）監視の方法及び状況報告
暗号技術調査 WG 活動報告
国際学会等の参加報告
暗号モジュール委員会の検討状況報告 等

【第 3 回】2004 年 2 月 10 日（火）
（主な議題）暗号技術調査 WG 活動報告
監視及び調査状況報告
国際学会等の参加報告
暗号技術監視委員会 2004 年度活動計画 等

（２）暗号技術調査ワーキンググループ

2003 年度、調査 WG は計 3 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。

【第 1 回】2003 年 6 月 23 日（月）
（主な議題）暗号技術調査 WG の運営
監視要員配置と監視活動
暗号技術調査 WG 2003 年度活動方針 等

【第 2 回】2003 年 7 月 14 日（月）

（主な議題）調査内容の中間報告 等

【第 3 回】2004 年 2 月 2 日（月）

（主な議題）調査結果の報告

暗号技術調査 WG 2003 年度報告書の作成

暗号技術調査 WG 2004 年度活動計画 等

３．１．４． 国際学会等における発表の動向

2003 年度は表 1 に示すような国際会議に監視要員を派遣し、最新の暗号解読技術に関する情報収集を実施した。以下では、これらの国際会議で発表された論文を中心に、暗号解読技術の最新動向について述べる。

表 1　国際会議への参加状況

学会名・会議名		開催国・都市	期間
EUROCRYPT 2003	Eurocrypt	Warsaw, Poland	2003/5/5 ～ 2003/5/8
SAC 2003	Selected Areas in Cryptography	Ottawa, Ontario, Canada	2003/8/13 ～ 2003/8/15
CRYPTO 2003	Crypto Conference	Santa Barbara, Ca., USA	2003/8/18 ～ 2003/8/21
CHES 2003	Workshop on Cryptographic Hardware and Embedded Systems	Cologne, Germany	2003/9/8 ～ 2003/9/10
ISO SC27	International Organization for Standardization	Saint Denis, France	2003/10/20 ～ 2003/10/24
ASIACRYPT 2003	Asiacrypt	Taipei, Taiwan	2003/12/1 ～ 2003/12/4
EIDMA-CWI WS	EIDMA-Cryptography Working Group	Utrecht, Netherlands	2003/12/12 ～ 2003/12/12
SCIS 2004	Symposium on Cryptography and Information Security	宮城県仙台市	2004/1/27 ～ 2004/1/30
FSE 2004	Fast Software Encryption	Delhi, India	2004/2/5 ～ 2004/2/7
TCC 2004	Theory of Cryptography Conference	Cambridge, MA, USA	2004/2/19 ～ 2004/2/21
CT-RSA 2004	RSA Conference 2004, Cryptographers' Track	San Francisco, Ca., USA	2004/2/23 ～ 2004/2/27
PKC 2004	International Workshop on Practice and Theory in Public Key Cryptography	Singapore	2004/3/1 ～ 2004/3/4

表 2 は最重要の成果が報告される IACR（International Association for Cryptographic Research: 国際暗号学会）主催の 5 つの国際会議に報告された暗号解読技術に関する論文件数を、暗号技術の分類に従って集計したものである。

公開鍵暗号に関する暗号解読技術については、素因数分解等の暗号学的仮定（安全性の根拠となる仮定）に対する基礎的な研究が 14 件中 10 件と多く報告されている。これは最近の証明可能安全性理論の発展により、主要な公開鍵暗号技術が暗号学的仮定に帰着する証明を備えていることから、暗号解読技術も個別のアルゴリズムに対する解読法の提案は減少し、暗号学的仮定そのものを対象にする傾向が強まっているためと考えられる。暗号学的仮定を対象とする基礎的な研究では、2003 年度は後述の TWIRL に代表される素因数分解のための特殊なハードウェアの構成法に関する報告や、楕円曲線暗号の定義体の違いによる強度解析が多く見られる。表 2 のその他の項目は、Braid 群や Lattice など、電子政府推奨暗号のアルゴリズムが依拠していない暗号学的仮定に対するものである。

共通鍵暗号に関する暗号解読技術の傾向としては、公開鍵暗号とは対照的に、個別アルゴリズムに対する攻撃法が報告されることが多い。特にストリーム暗号に関する解読技術が 19 件中 15 件と多数を占め、その中でも代数的攻撃法の研究が数多く報告されている。共通鍵暗号に特化している FSE 2004 では、代数的攻撃法に関するセッションも設けられる状況となっている。

2003 年度の暗号解読技術に関する最新動向調査の結果としては、今後も注意深い監視が必要な内容があるが、電子政府推奨暗号リストの見直しを必要とする事態には至っていない。

表 2　暗号解読技術の分野別発表件数

	Eurocrypt	CRYPTO	Asiacrypt	FSE	PKC	計
公開鍵暗号	**4**	**4**	**3**	**0**	**3**	**14**
暗号学的仮定						
楕円曲線	1		1			2
素因数分解		2	2		2	6
その他		1			1	2
守秘	1	1				2
署名	2					2
鍵交換						0
共通鍵暗号	**3**	**3**	**1**	**12**	**0**	**19**
ブロック暗号	1		1	2		4
ストリーム暗号	2	3		10		15
その他	**1**	**1**	**1**	**0**	**0**	**3**
ハッシュ関数			1			1
擬似乱数生成系	1	1				2

（１）公開鍵暗号

（イ）暗号学的仮定に関連する報告

・素因数分解ハードウェアの構成法

素因数分解に用いられる数体篩（ふるい）法の一部で特に大きな処理コストが必要となる篩（ふるい）部分と線形代数部分に専用ハードウェアを用いる方

法が盛んに研究されている。Shamir-Tromer らは篩（ふるい）部分について、Geiselman-Steinwandt らは篩（ふるい）部分および線形代数部分のそれぞれについて、特殊なハードウェアの構成法を示し、従来の見積もりよりも低いコストで RSA 合成数の素因数分解が可能であると報告した。

Shamir-Tromer らの提案は、WSI（Wafer-Scale Integration）を前提とした革新的なハードウェア構成（TWIRL）を採用することにより 1024bit の素因数分解を目指しているのに対し、Geiselman-Steinwandt らの提案は、既存の LSI 技術を多用した回路を 4.9cm 角のシリコンチップに実装することで、768bit の素因数分解について TWIRL よりコストパフォーマンスが 1/6 程度に低下するものの実現性が高いと主張している。これらの新しい技術に関連して、３．３．２．において TWIRL に関する評価結果を記述している。

・楕円曲線暗号

Hessは、GHS（Gaudry-Hess-Smart）攻撃を一般化し、標数 2 の拡大体$\mathbf{F}_{2^n}$を定義体とする従来より多くの楕円曲線に適用可能とした。また、Menezes-Teske-Wengらも同じく標数 2 の拡大体$\mathbf{F}_{2^n}$ について、Pollardのρ法やGHS攻撃法などが効率良く適用できるパラメータを考察し、いくつかの場合に攻撃に必要な計算量を 1/1000 以下に削減できると主張している。さらに、Thériaultは種数が小さな超楕円曲線に対するIndex Calculusの改良について考察し、例えば種数 3 の超楕円曲線ではメモリサイズで 5%程度大きな定義体を採用すべきだと主張している。いずれの攻撃法も特に電子政府推奨暗号リストの見直しを必要とする事態には至っていないが、楕円曲線暗号のパラメータを選択する際には、これらの攻撃法に対しても留意する必要があろう。

（ロ）守秘目的の公開鍵暗号アルゴリズムに関連する報告

Braid群に基づく公開鍵暗号系及びHidden Field Equation（HFE）に基づく公開鍵暗号系に関する解読法が報告されているが、電子政府推奨暗号リストに直接影響を与えるものではない。

Braid 群に基づく公開鍵暗号に対するものでは、Lee-Park ら及び Cheon-Jun らが解読法を提案している。特に、Cheon-Jun らの提案は多くの暗号アルゴリズムが困難性を仮定していた Braid Diffie-Hellman 共役問題と呼ばれる問題についての多項式時間アルゴリズムを与えている。Braid 群に関する一連の研究は、新しい暗号学的仮定に基づく暗号アルゴリズムの安全性評価の難しさを示唆している。

また、Hidden Field Equation（HFE）に基づく暗号システムに関しては、Faugere-Jouxらがグレブナー基底の計算アルゴリズムを利用したHFEの解読法を提案している。 HFEにおいて、秘匿する多項式の次数dが固定された場合には，この解読法は変数の数に関する多項式時間でHFEを解読でき、HFE-Challenge（d=96, n=80）が約 2 日で解けることも示している。Courtoisは、代数的攻撃法を適用すればこの解読法をさらに効率化できると主張している。HFEに関するこれらの結果は、ストリーム暗号に対する代数的攻撃法に関する研究とも関係が深い。

（ハ）署名アルゴリズムに関連する報告

電子政府推奨暗号の一つであるDSAのvariantであるRDSA[1]に関し、Fouque-PoupardらがRDSAに関する既知文書攻撃（known-message attack）による解読法を報告している。この解読法は非常に少ない計算量で、署名鍵を導けることを示す強力なものである。

ただし、この解読法は RDSA に固有の特殊な性質を利用しており、DSA の安全性への影響はない。

（2）共通鍵暗号

（イ）ブロック暗号に関連する報告

ブロック暗号の安全性評価手法に関する報告が Biryukov らよりなされた。ブロック暗号の解析では、線形特性や差分特性など、線形変換やアフィン変換により不変な特性を利用することがあるが、Biryukov らの報告では、任意の２つのpermutation（S-box）が線形（アフィン）等価（相互に変換可能）か否かを判定する効率のよいアルゴリズムを構成できることを示している。

（ロ）ストリーム暗号に関連する報告

ストリーム暗号に関連する暗号解読技術として、代数的攻撃法が数多く報告されている。Courtoisはoverdefined（項の数より方程式の数の方が多いこと）な連立代数方程式を解く方法を工夫し、ToyocryptやLILI-128 等のストリーム暗号の解読が理論的に可能であると主張している。また、Armnknecht らはBluetooth採用のストリーム暗号システムE_0について、鍵更新機能等を除いて内部の鍵ストリーム生成器だけを対象にすれば、理論的には実用的な時間で破れるという見積もりを示している。さらにArmknechtは、Courtois のCRYPTO 2003 の結果の一部（Precomputationに関する部分）に含まれる曖昧さを修正し、厳密に定義してさらに 8 倍高速化したと主張している。

ただし、代数的攻撃法に関する報告の多くは理論的な結果であり、シミュレーション等による実験的な結果が示されていないことなどから、代数的攻撃法の有効性については懐疑的な意見も多い。また、現在までに示されている代数的攻撃法は LFSR に基づくストリーム暗号に対してのものであり、電子政府推奨暗号リストに掲載されているストリーム暗号は全て LFSR に基づかない方式のため、これらの安全性に関して直接的な影響はないと考えられる。

（3）その他

電子政府推奨暗号リストに記載されたハッシュ関数及び擬似乱数生成系に直接影響する発表はなかった。

---

[1] RDSAはBiehlらが 2002 年に論文誌Designs, Codes and Cryptographyで発表した署名アルゴリズムである。その名称は、位数が未知の群におけるRoot problem(n乗根を求める問題)に基づいており、かつDSAと式の形が似ていることに由来しているが、離散対数問題に基づくDSAとは別物である。

３．２．暗号技術調査ワーキンググループ

３．２．１．擬似乱数生成系調査ワーキンググループ

３．２．１．１．調査背景

擬似乱数生成系は相互運用性を確立する必要性がないことから、電子政府推奨暗号リストにおいては SHA-1 を使った擬似乱数生成器が例示されているのみである。適切でない擬似乱数生成器の利用は安全性を損なう可能性もあることから、少なくとも高い乱数性を持つ擬似乱数生成器が採用されるために乱数検定ツールが必要と考えられる。CRYPTREC が乱数性の検定を行うにあたっては、これまでは NIST FIPS PUB 140-2 と NIST SP800-22 を準拠にしていた。しかしながら、いくつかの乱数検定法の不具合について 2002 年度版暗号技術評価報告書において指摘されている上、いくつかの学術論文が発表されたことと、暗号モジュールの評価においても乱数検定が必要になるという背景がある。さらに乱数の検定法は一般的な乱数を対象としているが、CRYPTREC が対象としているのは暗号利用用途の擬似乱数であり、このような観点から CRYPTREC が推奨する乱数検定法をまとめた検定ツール（以下、「CRYPTREC 乱数検定ミニマムセット」）を作成することを最終的な目標として、擬似乱数生成系の調査を行う必要性が監視委員会で認められ、今年度からワーキンググループを組織し、調査を行うこととなった。

３．２．１．２．今年度の調査内容

NIST SP800-22 の離散フーリエ変換検定と Lempel-Ziv 圧縮検定の問題点については、2002 年度版暗号技術評価報告書において指摘されている上、いくつかの学会などでも研究報告がなされている。今年度は大きく問題点が指摘されているこの 2 種類の検定法の問題点の追求と修正の可能性について調査、検討することに注力した。

３．２．１．３．調査概要とまとめ

今年度の調査結果について、以下に記す。

（１）離散フーリエ変換検定に関する調査

NIST SP800-22 に示される離散フーリエ変換検定では、NIST が用意した 16 種類全ての例示的擬似乱数生成器が p-value の一様性の検定に合格しないという問題があり、フーリエ変換された値を 2 値系列に変換する際の閾値が理論的に誤っているという指摘がある。離散フーリエ変換検定の問題点を検証し、修正を試みた結果を表 3 に示す。

（２）Lempel-Ziv 圧縮検定に関する調査

NIST SP800-22 に示される Lempel-Ziv 圧縮検定は、増分分解系列数 $W(n)$（n:乱

数系列長）で圧縮可能性を評価し、圧縮が可能な系列の場合、乱数性が悪いと判断する検定法である。NIST の定めた $W(n)$の平均値と分散の閾値の決定に不明瞭な点があり調査を行った。本ワーキンググループにおける議論の結果、Lempel-Ziv 圧縮検定はさらなる理論的解析が望まれる検定法であり、現在のところ CRYPTREC 乱数検定ミニマムセットに加えるには検討を要すると判断した。

（3）線形合同法の解析手法に関する調査

線形合同法の出力を乱数とする擬似乱数生成器は乱数性が良好な反面、暗号学的に安全でないため CRYPTREC では使用を推奨していない。本ワーキンググループでは、乱数検定と同時にその乱数が線形合同法によって安直に生成されていないかをチェックする目的で、線形合同法の解析手法に関する調査を行った。対象となった解析手法は、Freize らのアルゴリズムと Knuth のアルゴリズムである。しかしながら NIST が例示する擬似乱数生成器は、これら解析手法が仮定している条件の範囲外であるため、出力系列からそれが線形合同法による系列であるかどうかの判断を行う解析手法の開発は、現在知られているアルゴリズムの応用では単純には解決しないことが分かった。

以上の議論を経て、CRYPTREC 乱数検定ミニマムセットの導出においては理論的な裏付けがないものは積極的には採用しない方向に決まった。また理論的裏付けがあったとしても、計算機実験が行える程度の実際的な規模において追試を行い、閾値などの設定値が適切か確認が必要であろうとの判断となった。

表 3　離散フーリエ変換検定の調査概要

	NIST	調査結果
周波数スペクトルの分布	・正規分布 ・95%点の閾値=$\sqrt{3n}$	・ 自由度 2 の χ^2分布 ・95%点の閾値 =$\sqrt{(-\ln 0.05)n} = \sqrt{2.9957\cdots\ n}$
閾値で 2 値化した系列の分布	・2 項分布 ・平均＝$nP/2$ ・分散=$nP(1-P)/2$	・ 複数の実験結果から「2 項分布とならない」ことを確認 ・ 平均＝$nP/2$ ・ 分散　$nP(1-P)/4$ と推測

３．２．２．暗号利用モード調査ワーキンググループ

３．２．２．１．調査背景

昨年度までの暗号技術評価委員会における活動では、暗号利用モードの安全性に関する話題や実装性に関する記述は未整理であり、ユーザが操作モードを選択し、適切に用いるための必要な情報が提供できていなかった。暗号利用モードはブロック暗号

を実装する際には欠かせない技術であり、システム設計の際の暗号利用モードの選択は重要である。標準化状況についても、従来の標準を見直し新たな暗号利用モードを付け加える動きもある。このような背景から暗号利用モードに関する調査を行い、調達側が適切な暗号利用モードを選べるようにすることが必要であるとの合意が監視委員会において得られ、今年度からワーキンググループを組織し、調査を行うこととなった。

３．２．２．２．今年度の調査内容

暗号利用モードは相互運用性が最重視される技術であり、既に標準化されたものが重視される傾向がある。その上で、世界中の研究者達から学会や標準化団体などに対し、既存の利用モードに新たな機能を追加する形で新たな暗号利用モードが提案されている状況がある。今年度は、一般に暗号利用モードと呼ばれる技術の検証に注力することとした。

３．２．２．３．調査概要

（１）暗号利用モードの現状と提案されている MAC の方式について

現在利用されている、もしくは提案されている暗号利用モードについて調査し、主に安全性の観点からその特徴をまとめる。また、同様に MAC についても調査し特徴をまとめる。

（２）暗号利用モードの安全性評価について

現在までに知られている暗号利用モードの評価の方法について、理論的な手法か、運用的な面も考慮したものか、という視点から調査しまとめる。

３．２．２．４．調査結果

相互運用性の観点と米国における標準化動向から、ECB、CBC、CFB(*k*-CFB)、OFB、CTR についてのみ表 4 にまとめる。表中、*n* はブロック暗号の処理ビットサイズ、*k* は暗号利用モードの処理ビットサイズを示す。ECB 以外については、実運用上で現実的な脅威と考えられる問題点は指摘されていないが、ECB においても例えば数ブロックの非常に短い通信においては問題なく運用できるなど、安全に使用できる場合もある。

表 4　秘匿に関する暗号利用モードのまとめ

	秘匿に関する注意点	1[bit]エラー伝播範囲	処理速度	並列実装性		復号関数実装の必要性	コメント
				暗号化	復号		
ECB	・暗号文を見るだけで平文ブロックが同じ値であるか否かを判定できる。よって、特別な理由がない限り、通常のデータの暗号化などへは用いるべきでない。	1 ブロック	1	有り	有り	必要	
CBC	・$2^{n/2}$ブロック程度以上の平文を暗号化すると、暗号文一致攻撃により、暗号文を見るだけで平文に関する１ブロック分の情報が得られる可能性がある。	1 ブロック+1 ビット	1	無し	有り	必要	
CFB	・$2^{n/2}$ ブロック程度以上の平文を暗号化すると、暗号文一致攻撃により、暗号文を見るだけで平文に関する１ブロック分（kビット）の情報が得られる可能性がある。 ・k が小さい場合、初期値と平文の組み合わせによっては、鍵ストリームの周期が極端に小さくなる恐れがある。	($\lfloor n/k \rfloor$～$\lceil n/k \rceil$) 平文ブロック+1 ビット (1 平文ブロック=kビット)	k/n	無し	有り	不要	k[bit]の自動同期回復機能がある。
OFB	・$2^{n/2}$ブロック程度で周期を形成。（kが小さい場合、IVによっては、暗号文から容易に鍵の候補を絞り込むことが可能。） ・初期値の運用を誤ると重大な欠陥につながる恐れがあり、注意が必要。	1 ビット	1	無し	無し	不要	

CTR	・初期値の運用を誤ると重大な欠陥につながる恐れがあり、注意が必要。	1 ビット	1	有り	有り	不要	

３．３．その他の調査

３．３．１．素因数分解問題と計算機実験

３．３．１．１．調査背景とその目的

2001 年度から施行された「電子署名及び認証業務に関する法律」では、その第 33 条において、特定認証業務に関する認定の制度の円滑な実施を図るため、電子署名及び認証業務に係る技術の評価に関する調査及び研究を行うことが記されている。また、「電子署名及び認証業務に関する法律施行規則」では、その第 2 条第 1 項において、電子署名の安全性に適合する基準の 1 つとして、「ほぼ同じ大きさの 2 つの素数の積である 1024 ビット以上の整数の素因数分解」が有する困難性を挙げている。

これらを受けて、2001 年度、検討会では、電子署名法等に基づいて利用される暗号技術の評価（電子署名に用いる暗号技術等への助言）を実施することが決められた。検討会からの要請を受け、公開鍵暗号評価小委員会では 2000 年度に実施された評価を踏まえて、さらに詳細な安全性評価を実施すべく調査・研究を開始した。数論的問題の困難性に依拠して暗号プリミティブの安全性を主張する暗号スキームを横断的に評価するため、2002 年度までに調査された内容については、CRYPTREC Report 2002 にまとめられている。

本計算機実験プロジェクトは、素因数分解問題の困難性の調査・研究の一環として挙げられ、実施されたものの中の 1 つであって、素因数分解を実行するソフトウェアを用いて実際に素因数分解を行うことにより、いろいろな論文等の評価で述べられている 1024 ビット素因数分解の難しさが妥当かどうかを実験的に検証することが主な目的である。

３．３．１．２．素因数分解計算機実験プロジェクトにおける調査結果の概要

2002 年 1 月から 2004 年 3 月までの 2 年強の間、素因数分解計算機実験プロジェクトが実施され、その間に、大きな数の素因数分解に必要な計算量について従来よりも信頼性の高い見積りを出すべく、統一された環境で数多くの RSA のモジュラスの素因数分解が行なわれた。

すなわち、世界水準の一般数体ふるい法（GNFS）の実装を用い、90 桁から 150 桁までの 10 桁刻の合成数の分解実験をいくつか行ない、得られた実験データを理論的に予想される評価式に当てはめ、それを外挿（extrapolation）することにより 1024 ビットの素因数分解の実行時間の見積りを行ったところ、現在、市販されている汎用

のハードウェア（パソコン等）を用いて、2 年程度（関係式収集および行列計算ステップにそれぞれ 1 年位）で素因数分解を完了するためには、一企業や一研究グループでは集められないような数の計算機資源を要することが推測されるとの見積りを得た。詳細については、CRYPTREC Report 2003 を参照のこと。

また副産物として、表 5 に挙げる従来因子の知られていなかった合成数の分解に成功した。特に、この表中、c164 in 2,1826L は GNFS で分解された合成数の大きさでは現時点において世界第 2 位である。これに関して、関係式収集時間は約 7 年(Pentium 4 2.53GHz 換算)、収集した relations 数は 458 百万、行列計算時間は約 12 日(16 x Pentium 4 2.6GHz)と報告されている。なお、GNFS で分解された合成数の大きさにおいて現時点で世界第 1 位である RSA-576 に関しては、関係式収集時間は 13.2 年(Pentium III 1GHz 換算)、収集した relation 数は 635 百万、行列計算時間は 12 日(64 x Alpha 660MHz)と速報されている。

これらの結果は、実際に利用された GNFS 実装が世界水準に達していることを示しており、そこから得られる実験データが現時点でベストに近いものであることを示している。

表 5　本計算機実験プロジェクト等で分解した合成数、p(・)は分割数を示す。

c161 in 3,409+	SNFS	3146556580457915284319008046876542171617718876815478513 x p107
c173 in 3,419+	SNFS	65563728961043731460088120174018899370841141507626949 x p120
c163 in p(29675)	ECM	22397255528160225411990840248205316 97 x p126
c163 in p(22733)	ECM	45211894866667804086453435775564396429676244467 x p116
c164 in 7,316+	ECM	88170017041631125909548421501685555401545129 x p122
c165 in 2,2030L	ECM	87678355175652250615083617929401084618044201 x p121
c198 in 3,431-	SNFS	532747533936487674927670927580505985209056283901216 7 x p147
c164 in 2,1826L	GNFS	343346448861824465462730089242420846343270897895597712158640922548 49 x p97
c249 in 2,827+	ECM	697873770677228814866020945027612539302629325789244385 39 x p193

・主なスケジュール

2001 年度末：立教大学で勉強会を 4 回開催。プロジェクトの進め方及び数体ふるい方に関する報告書が提出される。

2002 年度：　不定期に勉強会を数回開催。line sieve プログラム実装における高速化の解説や関連論文の解説等が行なわれる。

2003 年度：　8 月頃までに Block Lanczos 法の実装が終了し、SNFS で Line Sieve を用いて、Cunningham 数をいくつか分解することに成功する。引き続き、Lattice Sieve 及び平方根の実装完了にともない、いくつか

の Cunningham 数、及び 90～150 桁の分解実験を行なった。また、いくつかの未分解 Cunningham 数や分割数の分解に成功した。SCIS や ISEC などへ結果などが論文発表された。

３．３．１．３．まとめ

（１）2004 年 3 月までの 2 年強の間実施された素因数分解計算機実験プロジェクトの結果提出された実験データを理論的に予想される評価式に当てはめ、外挿（extrapolation）することにより 1024 ビットの素因数分解の実行時間の見積りを行った。その結果、当面の間、1024 ビット以上の整数の素因数分解が有する数論的困難性の安全性基準には問題がないことがわかった。しかしながら、1024 ビットの素因数分解における関係式収集時間については、今回の素因数分解計算機実験プロジェクトの予測よりも大きい見積りを提出している論文もあり、これらの点についてはさらなる検討が必要であると考えられる。

（２）近年、専用のハードウェアによる素因数分解を行う提案がいくつか行われている。ハードウェアの進歩は非常に速いことから、今後の発展状況を継続して注意深く監視していくことが必要であると考えられる。

３．３．２．TWIRL 調査

３．３．２．１． 調査背景とその目的

2003 年に、Shamir と Tromer は、数体ふるい法におけるふるい処理部分を効率的に行うための TWIRL と呼ばれる計算機アーキテクチャの提案を行なった。TWIRL によって 1024 ビットの合成数を分解する時間と費用の見積もりは、1 年未満で 10M ドル（約 10 億円）であると、提案者達は彼らの論文の中で見積もっている。主要な公開鍵暗号である RSA 暗号の標準的な鍵の長さは現時点（2004 年 3 月）において 1024 ビットであり、仮に TWIRL が現実に製造・動作可能となると、RSA 暗号が解読可能であることを意味することになる。そこで、TWIRL 構築の実現性とそのための開発･設計費用について詳細な評価が喫緊の課題とされた。

３．３．２．２． 調査結果およびまとめ

TWIRL の実現性の検討を行った結果、以下に述べるような結論を得た。

結論１：提案者の主張通り TWIRL を単一の LSI に実装するには、直径 100㎜ 以上の巨大ウェハーを欠損なく製造するテクノロジーが必要となる。しかしこのような巨大なウェハーは現在のテクノロジーでは歩留まり率等から考えて製造不可能である。

もし TWIRL を複数の LSI に分割して実装したとしても必要 LSI 数が膨大となり、単一のボードには実現不可能である。また、分割した LSI を複数のボードに実装したとしても、提案者が主張する周波数（1 GHz）を前提とした場合、ボード間の I/O 数が多数であることから、現在のテクノロジーでは実現不可能である。

結論２：TWIRL ではパイプライン化された多数の加算器部に対する配送機構が必要になるものの、提案者の主張はアイデアのレベルにとどまっており、詳細な装置仕様を記述するに至っていない。また、本調査における検討では、配送機構を実現するために必要な回路規模は非常に大きく、現在のテクノロジーでは実現不可能であるという結論を得た。

結論３：故障耐性については原著にて付録として扱っている。しかし、独立性の低い高並列な回路構成ゆえに、多くの出力に故障が起こることが想定されるなど、原著の検討で故障耐性が十分であるとは考えない。さらに、現在のテクノロジーでは、今回の評価対象に適切な故障耐性を持たせる場合、全体でもかなりの部分を占めるパートについて、場合により大規模な冗長回路構成とする必要がある。すなわち、30cm ウェハに原著者が主張する機能を搭載するのは困難と考えるのが妥当である。

結論４：電力消費からくる発熱に対する冷却、および動作中のメンテナンスなども動作のコストとして計上されるべきであるが、これらは 30cm ウェハという大きな回路であり、現実的にどう克服してよいか、ノウハウがない。

結論５：その他、クロックツリーの構築、冗長回路の埋め込み、試運転段階の動作検査用論理などサポート技術、製造上のサイズマージン等、現実に実装を試みた場合には回路規模の増加が強く見込まれる。

したがって、現時点（2004 年 1 月）のテクノロジーを用いた場合、提案者が想定する性能を持つ TWIRL の実現は不可能であると考えられる。なお、懸念点の多くは装置が占めるウェハ上の面積に関わる部分であり、テクノロジーが進歩し集積度が上がれば、これらは克服できる可能性があることに注意が必要である。

３．３．３．SSL/TLS 調査

３．３．３．１．調査背景とその目的

2001年度、検討会により電子政府システム等に暗号技術を組み入れる際に利用される可能性が高いと判断された暗号プロトコルであるSSL/TLSに関して、これまでに報

告されてきた脆弱性について、
（１）暗号方式そのものの安全性
（２）プロトコル（メカニズム）としての安全性
（３）実装に関する安全性
（４）運用上の安全性
といった観点から調査を行い、「最新版で修正プログラムを当てている限り安全である」という結論であった。

その後約2年が経過し、その間にOpenSSLについて、Bleichenbacherの攻撃の拡張、VaudenayのCBCパディング攻撃、ASN.1ライブラリにおける脆弱性等、サイドチャネル攻撃等の方式や実装に関わる新たな攻撃や改良された攻撃が指摘されており、こういったSSLの現状を把握しておく必要があると考えた。そのため、SSLの現状を把握する追加調査および修正プログラムに関する運用方法についての調査を行うこととした。

なお、調査対象をSSLVer3.0/TLS Ver1.0以上とし、前回の調査後から2004年1月時点までに新たに発見・指摘された脆弱性の分析と対処法を調査項目とした。

３．３．３．２．調査結果概要

以下に調査結果の概要を示す。

（１）サイドチャネル攻撃

（イ）CBC パディング関連：SSL/TLS で用いられる暗号化のパディング（CBC パディング）における、正当性チェックの結果を利用した攻撃手法。

（ロ）RSA Encryption 関連：これまで報告された Bleichenbacher の PKCS#1 v1.5 に対する適用的選択暗号文攻撃を改良した実用的な攻撃手法や、PKCS#1 v.2.1 に従う EME-OAEP-DECODE 手法による復号プロセスにおける新たな攻撃法。

（ハ）タイミング攻撃：高速化を目的とした RSA 復号処理において、その入力値の大きさにより処理ロジックが異なる事を利用したタイミング攻撃。

以上のサイドチャネル攻撃について、実用的な攻撃が可能と考えられるものについては、対処がなされており、最新の修正プログラムを当てている限り安全である。

（２）実装上、その他の問題点

（イ）ASN.1 関連：通信プロトコルを記述するために用いられる ASN.1（Abstract Syntax Notation 1）における BER（Basic Encoding Rules）エンコードに関わるバッファオーバーフロー等の脆弱性。
OpenSSL における ASN.1 の BER エンコードにおける脆弱性は複数回報告されている。実用的な攻撃が可能と考えられるものについては、対処がなされているが、今後も発生する可能性があるので注意が必要である。

（ロ）その他：ルート証明書の更新手法における証明書管理技術に関する課題や、ブラウザのセキュリティホールによるアドレスバーの詐称の問題等。
種々のセキュリティホールについては、パッチによる対策がなされているが、アドレスバーの脆弱性については、現時点でパッチが公開されていない（2004 年 1 月末現在）。

（３）修正プログラムの管理･運用方法について
（イ）SSL 機能を持つサーバ及びクライアントを使用する上での各種設定方法など運用方法と、それに伴うセキュリティについて考察を行った。
（ロ）一般的なソフトウェアの運用の課題として、米国の NIST（National Institute of Standards and Technology）から発行されている、セキュリティ上の問題を修正するパッチの運用指針を定めた“(SP 800-40) Procedures for Handling Security Patches”に関する調査を行った。

３．３．３．３．まとめ

SSL/TLS はある種、完成されたセキュリティプロトコルと考えられているが、2001 年度の調査後も、バッファオーバーフロー等の実装上の問題点に加えて、タイミング攻撃等の新たなサイドチャネル攻撃が提案されているのが実状である。

これらに対しては実装上で対策が取られており、最新版で修正プログラムを当てている限り安全であるが、利用者は常に最新の状態に保つことが必要となる。

そのため、電子政府等の各種システムで暗号プロトコルである SSL/TLS を安全に利用するためには、今後も継続的に SSL/TLS の安全性について監視を行い、脆弱性に関する正確な情報を入手していくとともに、ソフトウェアに最新の対策を施すための運用にまで目を配ることが望まれる。

４．暗号モジュール委員会活動報告

４．１．暗号モジュール委員会活動の背景と目的

４．１．１．暗号モジュール評価に関する国際動向

米国 NIST[2]は、カナダ CSE[3]と共同で、CMVP（Cryptographic Module Validation Program）という暗号技術を実装レベルで評価・認証する制度を運用している。また、2002 年 10 月にワルシャワで開催されたISO/IEC[4] JTC1 の会合で、米国とカナダが自国の政府調達基準であるFIPS PUB 140-2[5]（以下、FIPS 140-2 と記す）をベースに、暗号モジュールに対するセキュリティ要求事項の国際標準化をNWI[6]として提案した。英、仏、独等の欧州諸国もこの動きに同調しており、ISO/IEC JTC1/SC27 WG3 における審議の結果、第 1 フェーズとして、FIPS 140-2 をなるべくそのまま生かす形で標準化する方向で検討が進められることになった。

欧州各国においても、独自の基準によって暗号モジュールに対する評価・認証が行われているようであるが、その内容は公開されていない。世界的に見ても、現在のところ、暗号モジュールの評価に関して参照可能なものは、FIPS 140-2 及びその試験基準である DTR（Derived Test Requirements for FIPS PUB 140-2）だけであり、本委員会の活動の一つとして、上記 2 つの資料をベースに、我が国において適用可能な基準を検討することとなった。

４．１．２．暗号モジュールに対する攻撃に関する研究動向

暗号モジュールの設計者は、多くの場合、信頼できる計算環境の中に秘密情報が保存され、それらの情報が外部からはアクセスできないことを想定している。しかし、実際には、マイクロチップは秘密情報を用いて演算を行う際、設計者の予想しなかった情報（side-channel information）を外部に漏らしてしまうことがある。このような情報を利用して、秘密情報の解析を行う方法がサイドチャネル攻撃である。

具体的には、実行時の漏洩情報、すなわち、暗号処理装置外部から計測可能な情報（例えば、計算時間や電力消費量など）と、秘密鍵等の秘密情報との間の相関関係を利用して、秘密情報を推定しようとする攻撃手法であり、特に IC カードに対しては、大きな脅威となり得ることが報告されている。

本委員会では、このような攻撃を非破壊攻撃と呼び、LSI チップなどを破壊して中の秘密情報を盗み出すというような攻撃を破壊攻撃と呼ぶことにした。後述のように、本委員会では非破壊攻撃を主な対象として調査検討を進めることとした。

現在、我が国における非破壊攻撃に関する研究は、世界レベルで見ると遅れている。

---

[2] National Institute of Standards and Technology

[3] Communications Security Establishment

[4] International Organization For Standardization / International Electrotechnical Commission

[5] Federal Information Processing Standards Publication 140-2

[6] New Work Item

また現時点では、FIPS 140-2 には攻撃に対する具体的な項目は規定されていないが、FIPS 140-2（又は、ISO/IEC 標準）の数年後の内容改訂時には、非破壊攻撃に関する対策項目が追加される可能性が大きい。

欧米の標準を単に利用するだけでなく、我が国が主体的に技術研究を行って、その成果を国際標準化に反映し、世界に貢献することが求められている。そのためには、非破壊攻撃に関する研究を今から進め、数年後に他国と同等に意見が交わせるよう、我が国のポテンシャルを上げておくことが必要である。

４．１．３．暗号モジュール委員会の活動目的

以上のような状況を踏まえ、2002 年度の暗号技術検討会の報告書において、本委員会の活動目的が次のように設定された。

（１）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。

（２）暗号技術監視委員会と連携をとりつつ、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。

上記を踏まえ、今年度の活動目的として、次の項目を設定した。

（１）FIPS 140-2 及び DTR の内容を調査・検討し、我が国の基準として適用可能な暗号モジュールの評価基準及び試験基準第 0 版を作成する。

（２）暗号実装関連技術について、最新の研究動向を調査し、各種攻撃手法やその対策の検討、評価基準への取り入れ方策等に関して、今後の調査・研究方針を決定する。

４．２．暗号モジュール委員会開催状況

2003 年度、暗号モジュール委員会は計 9 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。

【第 1 回】2003 年 6 月 16 日（月）

（主な議題）暗号モジュール委員会の活動方針

ISO/IEC JTC1/SC27 WG2 ケベック会合報告

【第 2 回】2003 年 7 月 25 日（金）

（主な議題）暗号モジュール委員会の活動方針

暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究

・研究方針検討のための文献調査依頼

暗号モジュール評価基準及び試験基準の検討

・暗号モジュール仕様

・暗号モジュールのポートとインタフェース

【第 3 回】2003 年 8 月 29 日（金）

（主な議題）ISO/IEC JTC1/SC27 1st Working Draftについてのコメント

暗号モジュール評価基準及び試験基準の検討

・役割、サービス、及び認証

・有限状態モデル

【第 4 回】2003 年 9 月 17 日（水）

（主な議題）暗号モジュールに実装された暗号アルゴリズムの検証方法について

【第 5 回】2003 年 10 月 10 日（金）

（主な議題）暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究

・研究方針案

暗号モジュール評価基準及び試験基準の検討

・物理セキュリティ

【第 6 回】2003 年 11 月 20 日（木）

（主な議題）暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究

・研究方針案

暗号モジュール評価基準及び試験基準の検討

・動作環境

・暗号鍵管理

【第 7 回】2003 年 12 月 19 日（金）

（主な議題）評価用標準プラットフォームでの研究に関する検討

・評価用標準プラットフォーム要求仕様案、研究方法について

暗号モジュール評価基準及び試験基準の検討

・電磁妨害/電磁両立性

・自己テスト

【第 8 回】2004 年 1 月 16 日（金）

（主な議題）評価用標準プラットフォームでの研究に関する検討

・評価用標準プラットフォーム要求仕様案、研究方法について

暗号モジュール評価基準及び試験基準の検討

・設計保証

・その他の攻撃の対処

【第 9 回】2004 年 2 月 13 日（金）

（主な議題）暗号モジュール評価基準及び試験基準の検討（第 0 版案）

2003 年度報告書の検討

４．３．暗号モジュール評価基準及び試験基準の策定

４．３．１．FIPS 140-2 の概要

FIPS 140 は、コンピュータシステム及び電気通信システム内の暗号モジュールに対

するセキュリティ要求事項を規定した、NIST が発行する米国政府標準である。

FIPS 140 は、政府及び産業界で構成されたワーキンググループによって開発された。1994 年 1 月に FIPS 140-1 が制定され、2001 年 5 月には FIPS 140-2 として改訂された。FIPS 140-2 は、ベンダ、試験機関、及びユーザ団体から寄せられたコメントに基づいた変更だけでなく、FIPS 140-1 が開発された以降に利用可能となった標準及び技術の変更も取り入れている。FIPS 140-2 は、その後、CHANGE NOTICE が発行されており、本委員会では、2002 年 12 月に発行された版を基準策定のための検討資料とした。

FIPS 140-2 は、暗号モジュールのセキュアな設計及び実装のために、暗号モジュールが満たすべき 11 分野（暗号モジュール仕様、暗号モジュールのポート及びインタフェース、役割・サービス・認証、有限状態モデル、物理セキュリティ、動作環境、暗号鍵管理、電磁妨害/電磁両立性、自己テスト、設計保証、その他の攻撃の対処）のセキュリティ要求事項を規定しており、さらに、保護すべきデータの重要性と使用環境に応じて暗号モジュールを提供できるように、分野ごとに 4 段階のセキュリティレベル（セキュリティレベル 1～4）を規定している。

４．３．２．DTR の概要

DTR は、暗号モジュールが FIPS 140-2 で規定されたセキュリティ要求事項を満たしているかどうかを試験する際に、試験者が実施しなければならない試験手順及びベンダが提供しなければならない情報を規定したものである。

DTR も FIPS 140 と同様、適宜改訂される。本委員会では、2003 年 2 月に発行されたドラフト版を基準策定のための検討資料とした。

DTR は、全 11 章から構成されており、各章は FIPS 140-2 で規定された 11 分野に対応している。各章では、FIPS 140-2 に対応するセキュリティ要求事項をアサーション（すなわち、設定されたセキュリティレベルで、設定された分野のセキュリティ要求事項を暗号モジュールが満足するために適用しなければならない宣言）として記述している。全てのアサーションは FIPS 140-2 から直接引用している。

各アサーションの次には、順に、ベンダが提供しなければならない情報、試験者が実施しなければならない試験手順を記述している。

４．３．３．評価基準及び試験基準第 0 版の作成

暗号モジュールの評価基準及び試験基準の作成に関しては、FIPS 140-2 及び DTR の翻訳作業から着手した。FIPS 140-2 に記載されている全ての要求事項は、DTR ではアサーションとして同じ内容が記載されており、作業重複を避けるため、DTR の翻訳作業を中心に進めた。また、4.1.1 節で述べたように、ISO/IEC JTC1/SC27 WG3 において、現在、FIPS 140-2 をベースにした暗号モジュール評価基準の国際標準化に関する審議が行われており、そうした動向に柔軟に対応できるようにするため、翻訳作業においては、なるべく原文に近い形で訳文を作成することにした。

次に、作成した訳文をもとに、英文解釈の統一を図るとともに、基準内容に関する不

明点及び問題点の抽出・整理を行い、22 項目の問題点を洗い出した[7]。なお、制度面に関するものについては、本委員会だけでは解決できないことから、問題点抽出のみにとどめ、主に技術的内容についての議論を行った。また、委員会内で解決できなかった技術的内容については、NISTへ質問状を送付し、回答を求める等の作業を実施した。

以上の作業より作成した FIPS 140-2 及び DTR の翻訳版は、暗号モジュールの評価基準及び試験基準の第 0 版と位置付け、今後、これら第 0 版をもとに、抽出・整理した問題点の解決や運用上の問題点の洗い出し等について調査検討を進め、我が国の基準として適用可能な暗号モジュールの評価基準及び試験基準の第 1 版を作成する予定である。

また、本委員会では、経済産業省からの依頼を受け、平成 15 年 6 月に ISO/IEC JTC1/SC27 WG3 から提示された暗号モジュール評価基準に関する国際規格の一次案について、その内容を精査し、本委員会としてのコメント提出を行った。

４．３．４．評価基準及び試験基準第 0 版の構成

暗号モジュール評価基準第 0 版は”FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHENGE NOTICE (12-03-2002)”を翻訳したものであり、構成は FIPS 140-2 と同様の構成である。

本文は、第 1 章には概要、第 2 章には用語及び略語集、第 3 章には機能的セキュリティ目標、第 4 章にはセキュリティ要求事項を記述している。さらに、第 4 章は全 11 節から構成され、各節でそれぞれの分野のセキュリティ要求事項を規定している。第 4.1 節には暗号モジュール仕様、第 4.2 節には暗号モジュールのポート及びインタフェース、第 4.3 節には役割・サービス・認証、第 4.4 節には有限状態モデル、第 4.5 節には物理セキュリティ、第 4.6 節には動作環境、第 4.7 節には暗号鍵管理、第 4.8 節には電磁妨害/電磁両立性、第 4.9 節には自己テスト、第 4.10 節には設計保証、第 4.11 節にはその他の攻撃の対処を記述している。

また、附属書として、APPENDIX A には文書要求事項のまとめ、APPENDIX B には推奨ソフトウェア開発手順、APPENDIX C には暗号モジュールのセキュリティポリシ、APPENDIX D には参考文献、APPENDIX E には使用可能なインターネットの URL を記述している。

暗号モジュール試験基準第 0 版は、”Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules (February 12, 2003 Draft)”を翻訳し、さらに英文の解釈や基準内容の理解に必要と思われる箇所には、欄を設け、解説やコメント等を加えたものであり、構成は、DTR と同様である。

本文は、第 1 章には暗号モジュール仕様、第 2 章には暗号モジュールのポート及びインタフェース、第 3 章には役割・サービス・認証、第 4 章には有限状態モデル、第 5 章には物理セキュリティ、第 6 章には動作環境、第 7 章には暗号鍵管理、第 8 章には電磁妨害/電磁両立性、第 9 章には自己テスト、第 10 章には設計保証、第 11 章にはその他

[7] 詳細は「CRYPTREC Report 2003 暗号モジュール委員会報告書」参照。
http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html

の攻撃の対処を記述している。

また、附属書として、APPENDIX A には文書要求事項のまとめ、APPENDIX B には推奨ソフトウェア開発手順、APPENDIX C には暗号モジュールのセキュリティポリシを記述している。

試験基準では、評価基準に対応するセキュリティ要求事項をアサーションと呼び、AS で始まるシーケンス番号で識別している。また、そのアサーションに対応したベンダに課せられる要求事項は VE で始まるシーケンス番号で識別し、そのアサーションに対応した試験者に課せられる要求事項は TE で始まるシーケンス番号で識別している。各章では、アサーションごとに、AS、VE、TE の順に各要求事項を記述している。

暗号モジュール評価基準第 0 版及び暗号モジュール試験基準第 0 版については、下記 URL の「CRYPTREC Report 2003 の公開」で参照できる。

http://www.ipa.go.jp/security/enc/CRYPTREC/index.html

http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html

４．４．非破壊攻撃及び破壊攻撃に対する調査・研究

４．４．１．暗号モジュールへの攻撃法

暗号モジュールに埋め込まれている暗号鍵や復号鍵等の秘密情報を暴露したり推定したりする攻撃には、以下の例に示すように大きく 2 種類に分けられる。

（１）暗号モジュールを動作させた時の実行時間や消費電力量等、外部から観測することにより得られる情報のみを用いて、秘密情報を取り出すような攻撃

（２）暗号モジュールを包んでいるパッケージ等をレーザや薬品などで破壊し、暗号モジュール内部の回路を露出させ、秘密情報を取り出すような攻撃

本委員会では、上記（１）のような攻撃を「非破壊攻撃」、（２）のような攻撃を「破壊攻撃」と定義した。各攻撃には、更にいくつかの攻撃法があり、その分類を図 2 に示す。

非破壊攻撃は、破壊攻撃を受けた場合と異なり、攻撃を受けた跡（タンパー証跡）が残りにくく、また攻撃コストも破壊攻撃に比べ安価に攻撃が行える傾向にある。

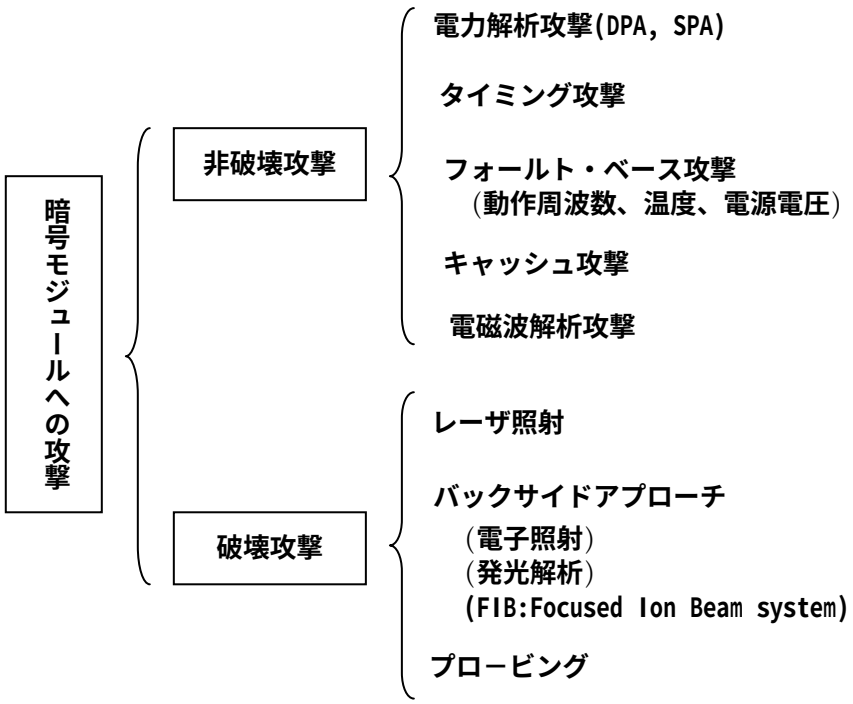


図 2　攻撃手法の分類

４．４．２．具体的な調査・研究テーマについての検討

暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究において、その具体的な調査・研究テーマを検討するにあたり、日本規格協会情報技術標準化研究センター(INSTAC)[8]耐タンパー性に関する標準化調査研究委員会と共同で文献調査を行った。

調査する文献については、最近の約 5 年間で主要な学会等（CRYPTO，CHES 等）で発表されている暗号モジュールの非破壊攻撃及び破壊攻撃に関する主な論文を抽出し、その内容を調査した。文献調査結果のまとめを表 6 に示す。

この調査結果を見ると、攻撃への対策が記述されている非破壊攻撃の電力解析攻撃に関する文献が多い。これは、この攻撃が現在注目されており、各研究機関で多くの対策が検討され、研究が進んでいると考えられる。

非破壊攻撃に関しては、以下のような理由からも、第一に調査・研究を進める必要があると考える。

（１）非破壊攻撃は、安価な攻撃コストで多大な攻撃効果が得られる可能性が高い。

（２）非破壊攻撃は、タンパー証跡が残らないものが多く、対策を運用でカバーできない場合がある。

（３）欧州のCC[9]評価機関、米国のCMVP試験機関やNIST、カナダのCSEへのヒアリングにおいても、サイドチャネル攻撃対策は必須という意見が得られている。

上記結果から、暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究の具体的なテーマを非破壊攻撃の電力解析攻撃に関する調査・研究とした。

---

[8] http://www.jsa.or.jp/domestic/instac/base.htm

[9] Common Criteria

表 6　暗号モジュールへの非破壊攻撃及び破壊攻撃に対する文献調査まとめ

対策の記載有無	攻撃内容		件数	割合
有り	破壊攻撃		5	5%
	非破壊攻撃	電力解析攻撃	36	38%
		電力解析攻撃＋α	8	8%
		タイミング攻撃	6	6%
		フォールト･ベース	4	4%
		キャッシュ攻撃	2	2%
		電磁波解析	2	2%
		その他	6	6%
無し	---		27	28%
合計			96	100%

４．４．３．電力解析攻撃に対する評価用標準プラットフォームの検討

（1）電力解析攻撃に関する研究方針

この電力解析攻撃に関する研究の位置付けは、電力解析攻撃への対策に関する評価基準及び試験基準策定のための予備的な研究である。このため理論だけでなく、攻撃及び対策の効果に対する追試実験等を行い、実データに基づいた研究を行うことを研究方針とした。

本研究方針を進める具体的方法としては、基準策定のための必要なデータを多くの研究機関から効率的に収集できるように、評価用標準プラットフォームを構築し、このプラットフォーム上での評価手法の確立を目指すこととした。

（2）評価用標準プラットフォーム構築に関する検討

電力解析攻撃に関して実データに基づく研究を進める場合、現状以下のような問題点が考えられる。

･ 各社の研究機関でASIC[10]又はASSP[11]による評価研究がなされていることが予想さ

[10] Application Specific Integrated Circuit

れるが、その評価結果は機密情報となることが多いため、評価結果の公表が難しく、研究発展の障壁になっている。
- 電力解析攻撃対策の効果検証については、自他間の比較評価が効果的だが、ASIC等による評価の場合、他社製チップは設計内容等が不明（機密情報）であり、比較評価が難しい。
- 現在、電力解析攻撃に関する論文は、シミュレーション結果の報告が多く、実証データは少ない。

上記問題点を踏まえ、評価用標準プラットフォームを構築する手段としては、以下の理由により、FPGA[12]で構築することとした。
- FPGA は、ASIC や ASSP よりもはるかに安価で容易に製造できるため、共通的な実験環境を広範囲にしかも容易に整えることができる。
- 評価用標準プラットフォームを FPGA で構築することにより、同一の実験環境が各機関で容易に準備できるため、色々な技術や効果の比較が容易にでき、電力解析攻撃の研究に関する技術力向上に貢献できる。
- 評価用標準プラットフォームでの評価結果は、一般的なデータとなり、公表し易く、研究促進に貢献できる。

ただし、FPGA で構築した評価用標準プラットフォームで研究を進めるにあたり、以下のような懸念点も残る。
- FPGA による評価結果と ASIC 等による評価結果が一致しない（相関性がない）ことが考えられる。
- FPGA による評価は、電力解析攻撃対策の中でも、実装のためのアルゴリズム対策の検討には効果的と思われるが、ゲートレベルでのハードウェア対策の検討には効果的でない。

しかし、本研究分野において、我が国が主体的に技術研究を行い、基準策定を進めていくためには、早い時期から必要な基礎データを数多く収集する必要がある。従って、委員会では、いくつかの懸念点はあるものの、早期に着手可能であり、評価対象を柔軟かつ広範囲に設定できる FPGA による電力解析攻撃の評価を行うこととした。

（3）評価用標準プラットフォームの要求仕様

FPGA による評価用標準プラットフォーム作成において、今年度はその要求仕様を検討した。

まず、評価用標準プラットフォーム作成の方針は以下とした。
- ハードウェア暗号機能ブロック（共通鍵暗号アクセラレータ、法剰余演算アクセ

---

[11] Application Specific Standard Product

[12] Field Programmable Gate Array

ラレータ）の電力解析攻撃の耐性評価が行えること。
- タイミング攻撃の評価も行えること。
- 対策効果の確認が容易に行えること。

評価用標準プラットフォームのイメージ図を図 3 に示す。イメージ図に記載されている FPGA 部、インタフェース部、電源部についての要求仕様を以下にまとめる。

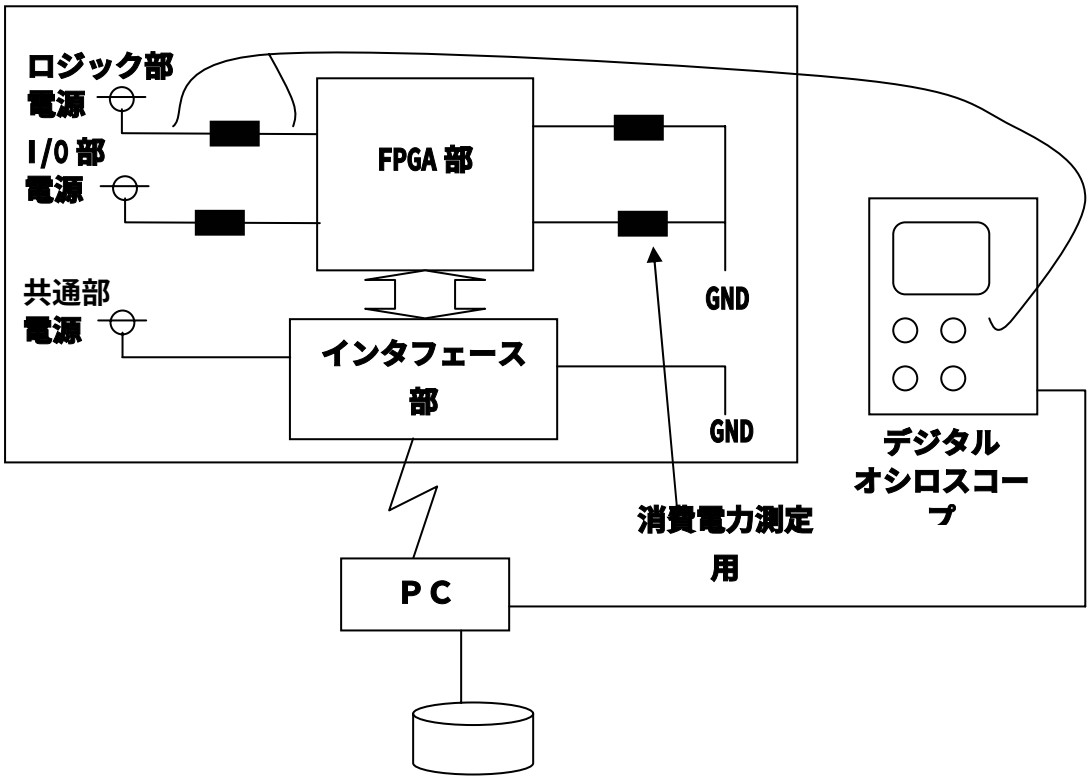


図 3　評価用標準プラットフォームのイメージ図

（イ）FPGA 部

[必須仕様]

- 子基板上に実装し、子基板の差替えで複数の FPGA に対応できること。
- FPGA の I/O 部及びロジック部の電源は別々にすること。
- 暗号機能部を FPGA に実装ができること。
- 暗号機能部で処理するデータは PC から入力できること。
- 動作クロックの変更（水晶発振器の差し替え、外部クロック入力端子経由等）が可能なこと。
- 暗号機能部で処理するデータは PC に出力できること。

[オプション仕様]

- HDL 記述の MPU（SH-2、M32R、Z80 等）が搭載できること。

・動作クロックへの干渉（クロック入力端子経由）が可能なこと。
・汎用 MPU（32bitMPU、16bitMPU、8bitMPU）と FPGA、RAM（32KB 以上）、ROM を備えた子基板にも対応できること。

（ロ）インタフェース部
[必須仕様]
・PC とのインタフェースとして、RS-232C インタフェースを有すること。
・シリアルパラレル変換回路を有すること。
・FPGA 部とのインタフェース仕様を変更できること。
・測定の開始点を指示するトリガ出力（端子）を設けること。
[オプション仕様]
・パラレルシリアル変換回路を有すること。

（ハ）電源部
[必須仕様]
・評価用標準プラットフォームの基板上に実装すること。
・電源、FPGA 部、周辺ロジック（インタフェース部、FPGA コンフィグレーション回路等）はそれぞれ分離すること。
・消費電力測定用抵抗器は基板表層で挿入でき、かつ、電力供給側又は GND 側のいずれかの挿入の選択が可能なこと。
・上記挿入する抵抗器は 10Ωを標準とする（容易に変更可能なこと）。
・デジタルオシロスコープのプローブ接続用端子を基板上に設けること（電圧プローブ又は電流プローブに対応可能なこと）。
[オプション仕様]
・電源へ干渉（供給電圧の変更、瞬断、電源電圧の瞬間的な変更等）が可能なこと。
・電源ノイズは、無負荷状態（FPGA を実装していない状態）で 50mVp-p 以下に抑えること。

※類似の FPGA に関する参考資料
（ａ）S. Berna Örs, E. Oswald, and B. Preneel, ”Power-Analysis Attacks on an FPGA － First Experimental Results”, CHES2003, LNCS 2779, pp.35-50, Springer, 2003(September)
（ｂ）山口、橋本、大熊、”高集積 FPGA 上に実装した共通鍵暗号への電力差分解析”、SCIS2004、2A4-5、2004-01

４．４．４．今後の活動方針
今後の活動としては、評価用標準プラットフォームを作成し、これを用いた評価手法

の確立を目指す。評価手法確立後は、評価用標準プラットフォームの利用推進を検討し、暗号モジュール評価基準及び試験基準策定のための評価データの蓄積を行っていく。また、4.4.3(2)項で示したように、FPGA による評価結果と ASIC 等による評価結果が一致しない（相関性がない）ことが考えられる。この点を明らかにする目的で、ASIC 等による評価の検討も行っていく。

５．今後の CRYPTREC 活動について

CRYPTREC は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、2004 年度以降以下の活動を実施していくこととする。

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、2004年度以降も引き続き以下の活動を行う。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

CRYPTREC は、2004 年度以降も引き続き、「暗号技術検討会」、暗号技術検討会の下に設置される「暗号技術監視委員会」及び「暗号モジュール委員会」並びに暗号技術監視委員会の下に設置される「暗号技術調査 WG」により構成されるものとする（図 4：今後の CRYPTREC の体制図）。

暗号技術検討会、暗号技術監視委員会、暗号モジュール委員会、暗号技術調査 WG の位置づけ、構成及び機能は以下のとおり。

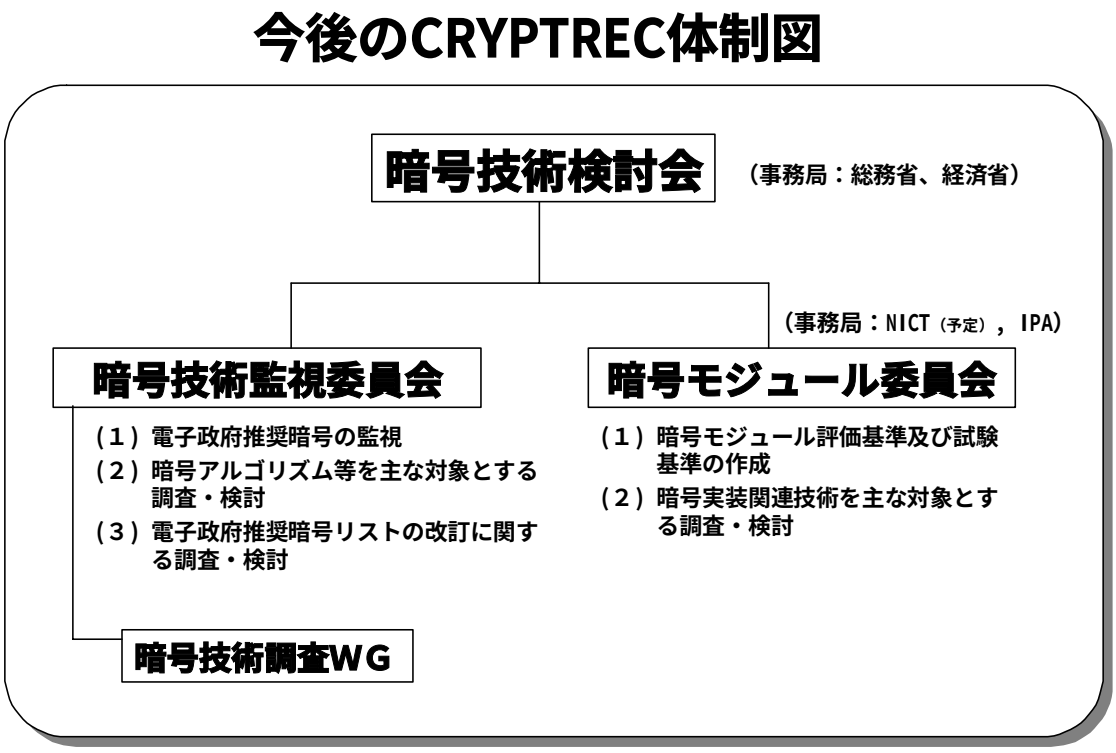


図 4　今後の CRYPTREC 体制図

５．２．１．暗号技術検討会

暗号技術検討会（以下、「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/CRL（両機関は2004年4月に独立行政法人情報通信研究機構として統合予定）及びIPAに配置する。

（１）暗号技術調査ワーキンググループ

（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、監視委員会からの要請により事案の性質に応じて開催されることとし、監視委員会に対して電子政府推奨暗号リストの変更案の作成等に関する専門的助言を行う。

（ハ）その他、調査WGは、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

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、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、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。

（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、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。

---

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

（１）監視委員会における情報収集

監視委員会は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）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、事案の性質に応じて、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）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、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、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、検討会に報告する。

（ハ）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、その結果を検討会に報告する。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）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。

電子政府推奨暗号の削除等の手順

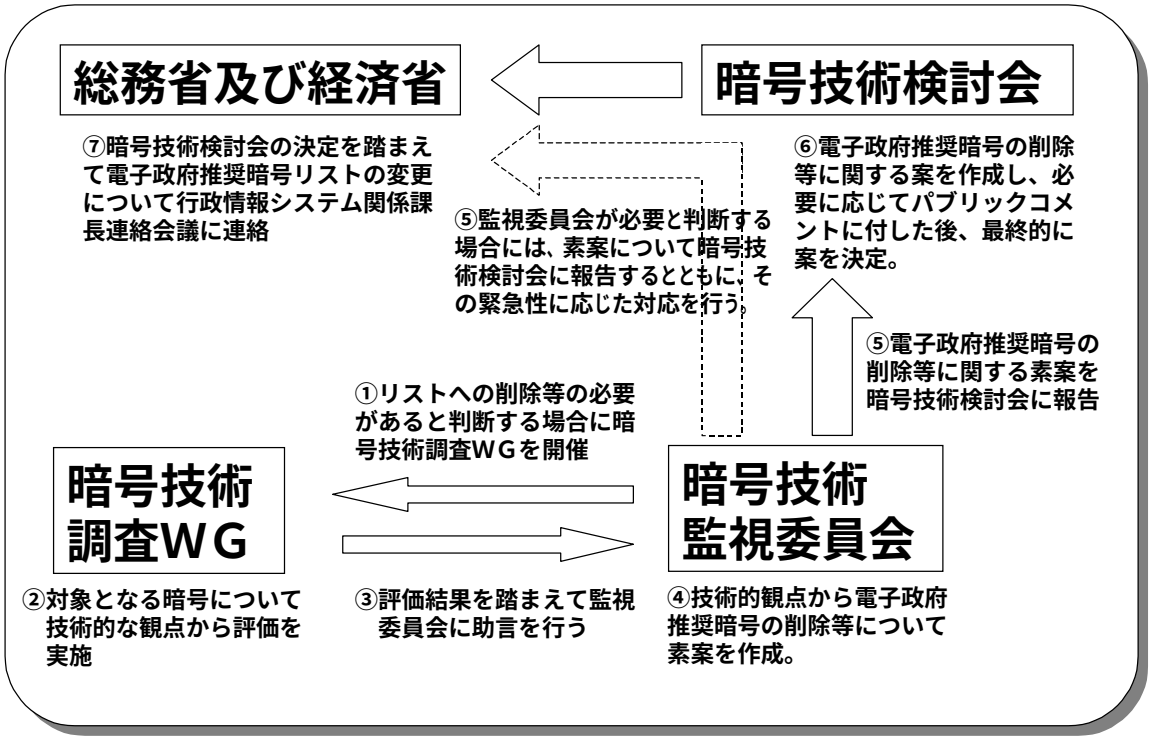


図5　電子政府推奨暗号削除等の手順

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、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、遅くともリスト策定から10年を経た2013年までに行うこととする。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、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、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。

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。

参考資料「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）

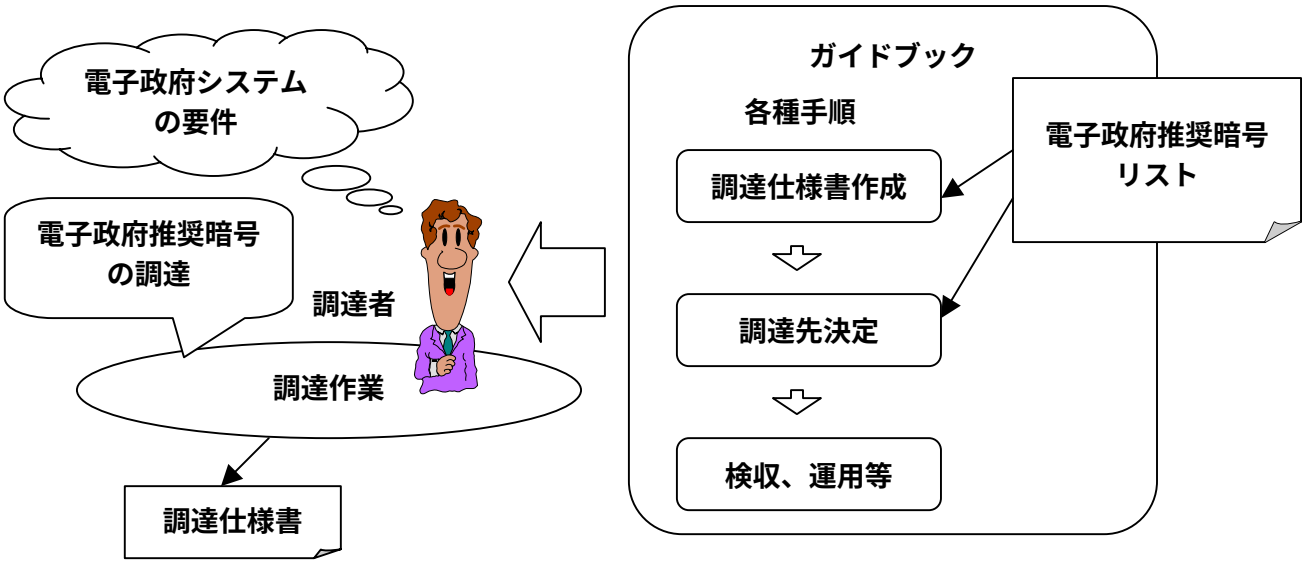


図２．１－１　本ガイドブックの位置付け

（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。

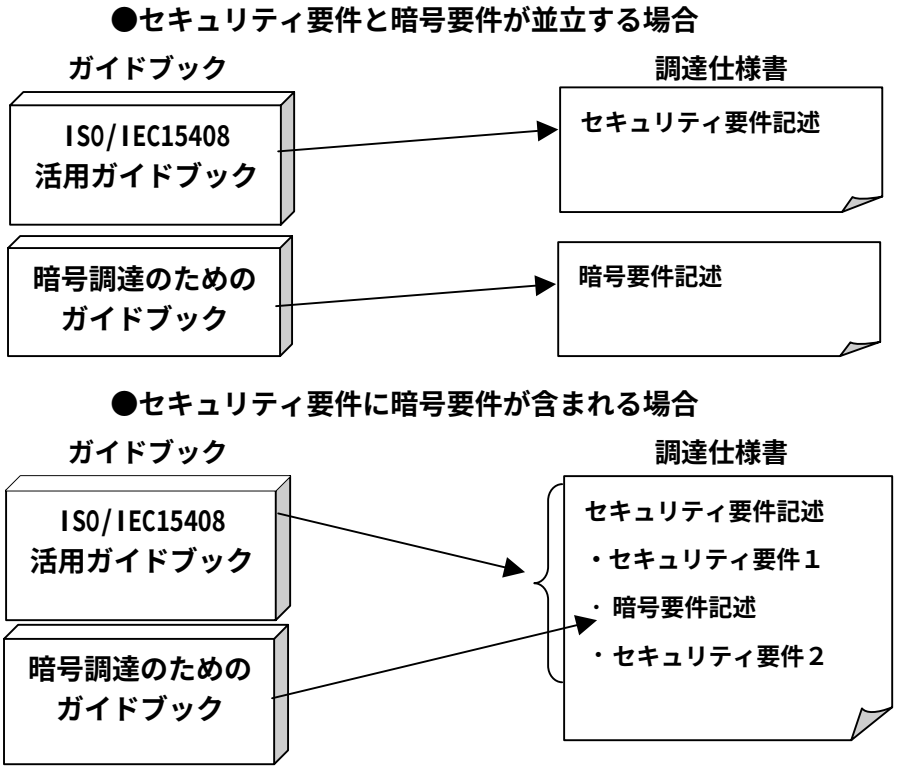


図２．２－１　ISO/IEC15408 を活用した調達と暗号調達の関連

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。

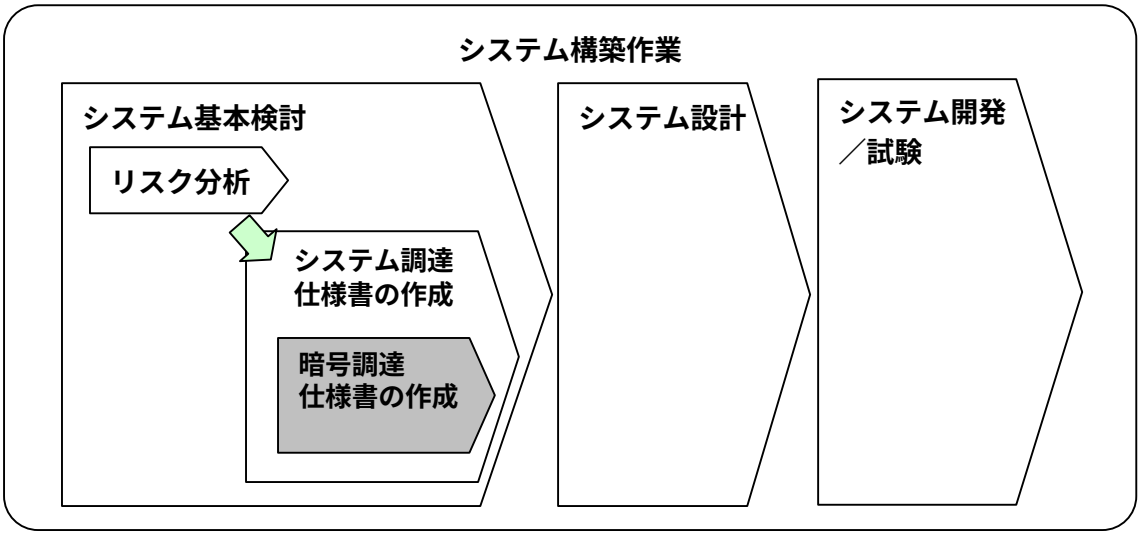


図３－１　システム全体の作業に占める暗号調達（調達仕様書作成作業）の位置付け

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。

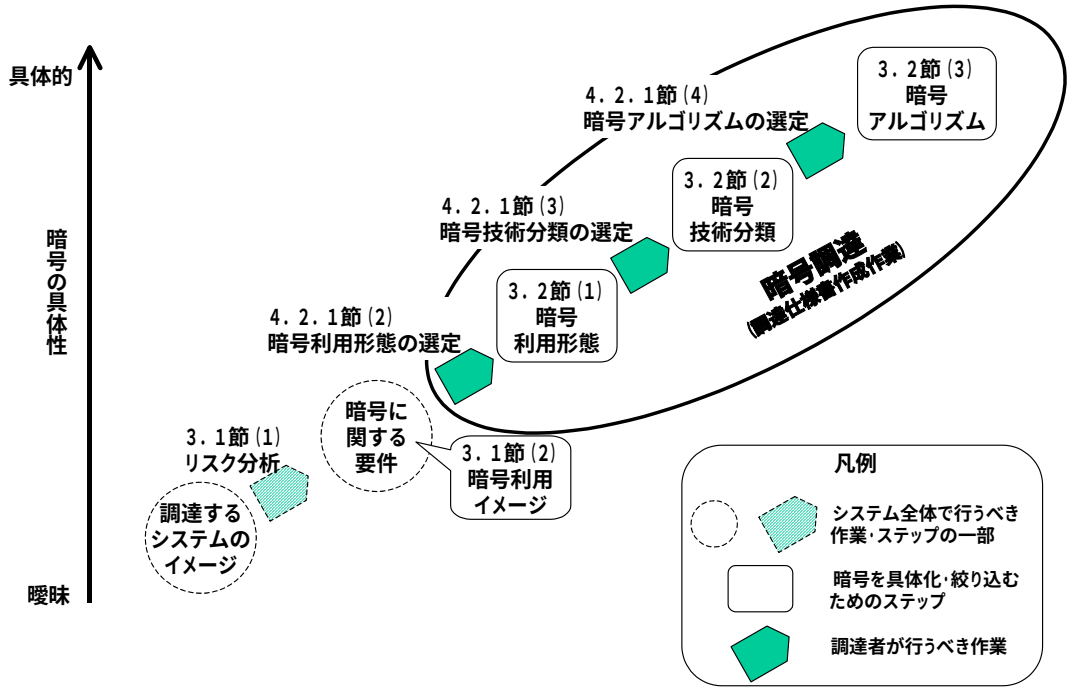


図３－２　暗号を具体化・絞り込みを行うためのステップ

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。

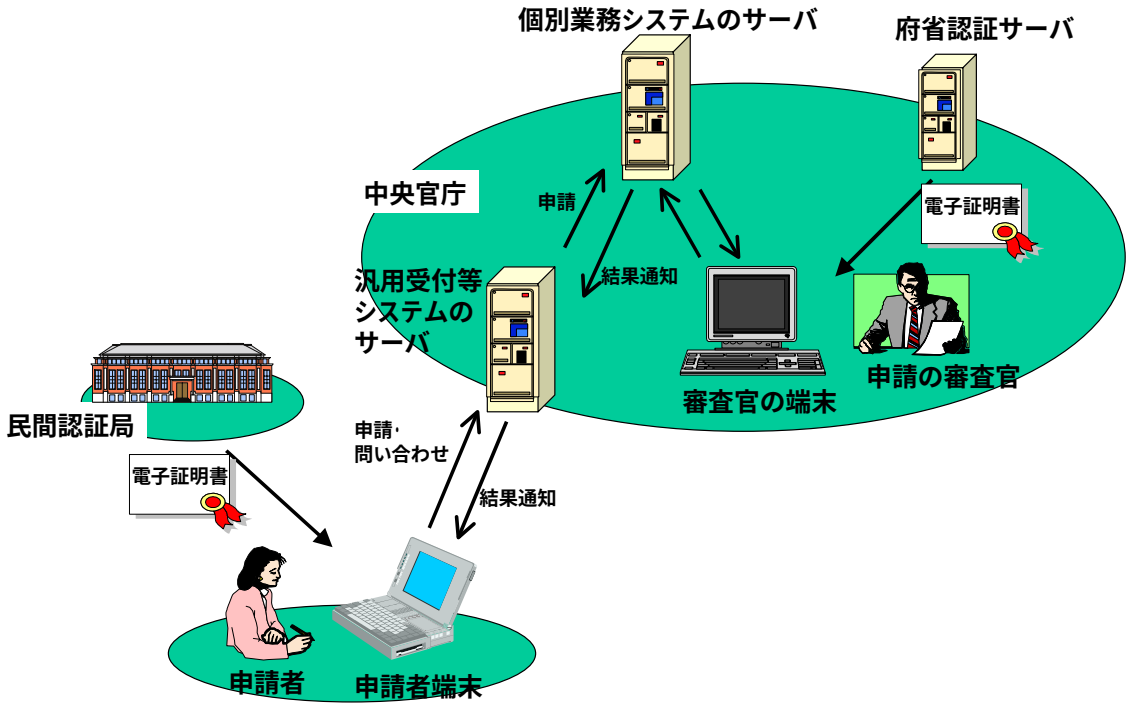


図３．１－１　電子申請システムのモデル図

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。

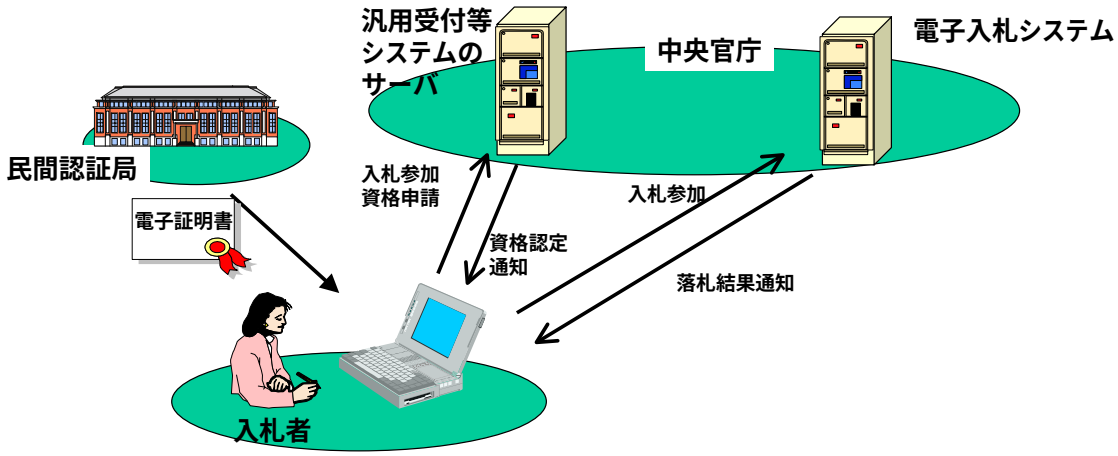


図３．１－２　電子調達システムのモデル図

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。

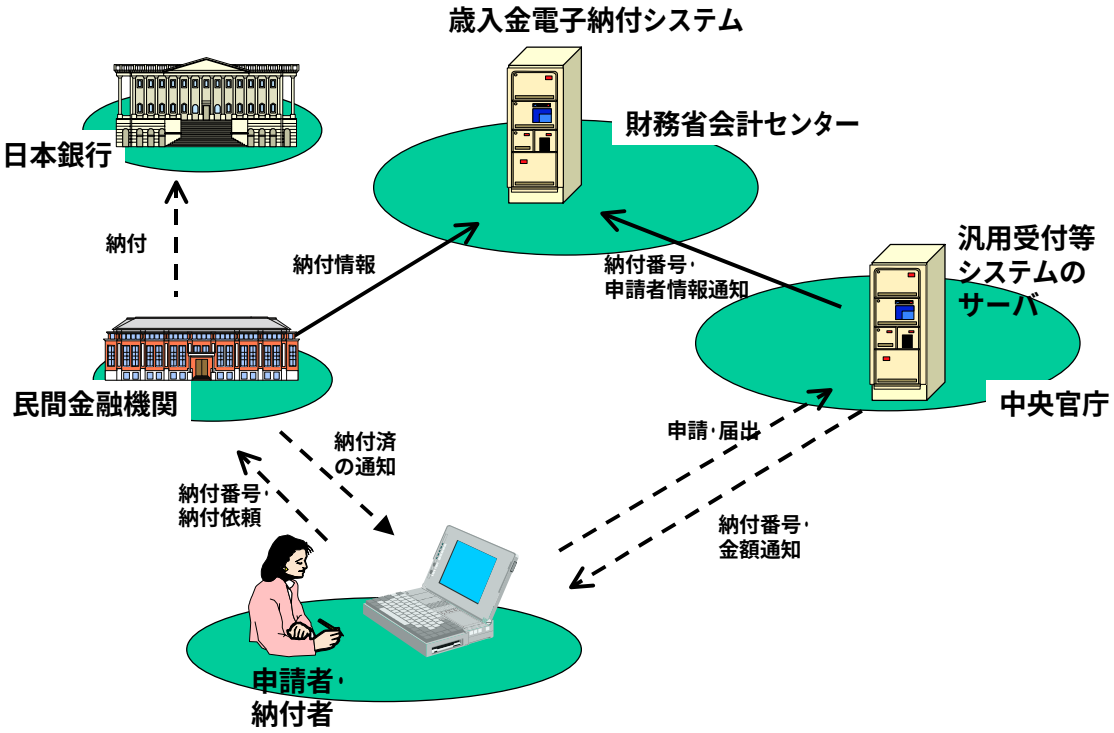


図３．１－３　電子納付システムのモデル図

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。

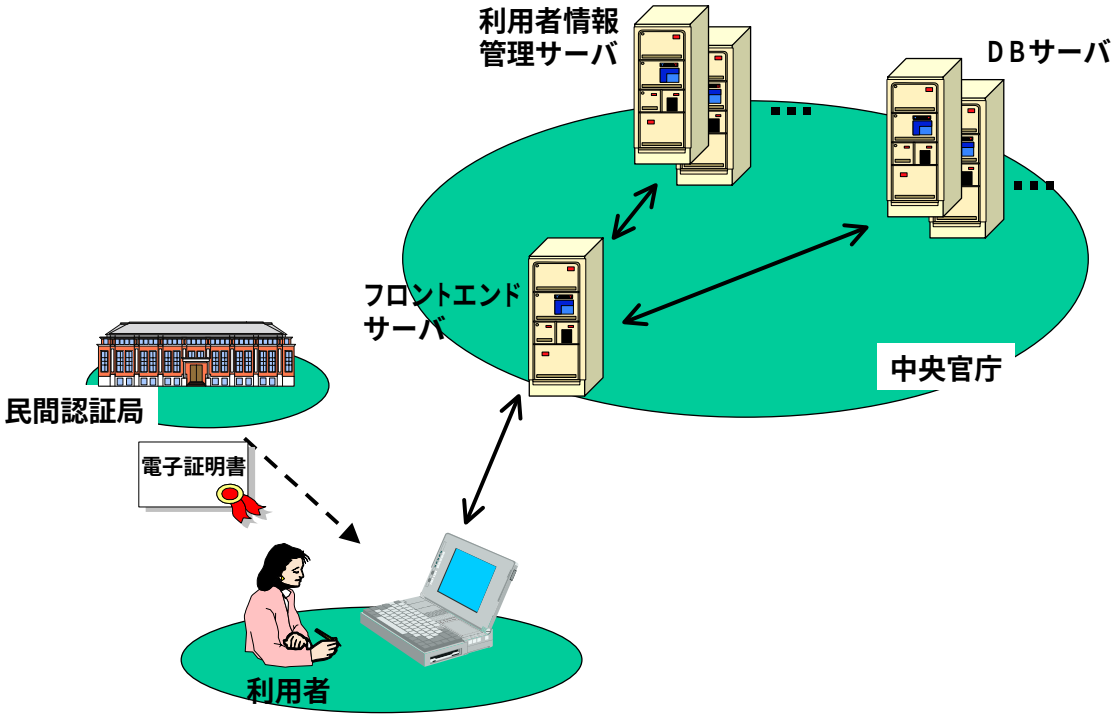


図３．１－４　電子情報提供システムのモデル図

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。

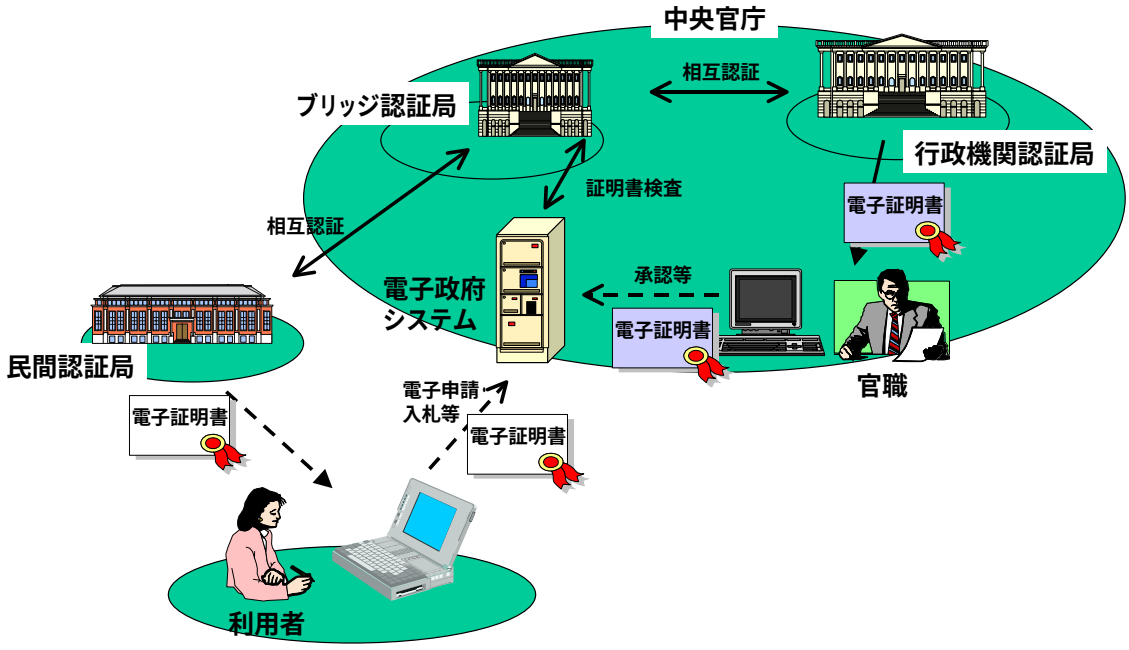


図３．１－５　政府認証基盤のモデル図

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/　　又は
http://www.meti.go.jp/　　）
・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。

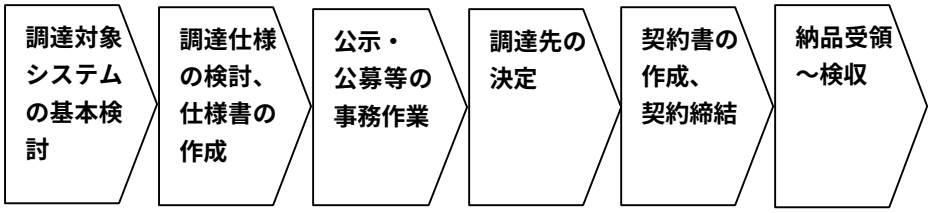


図４．１－１　システム調達の流れ

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。

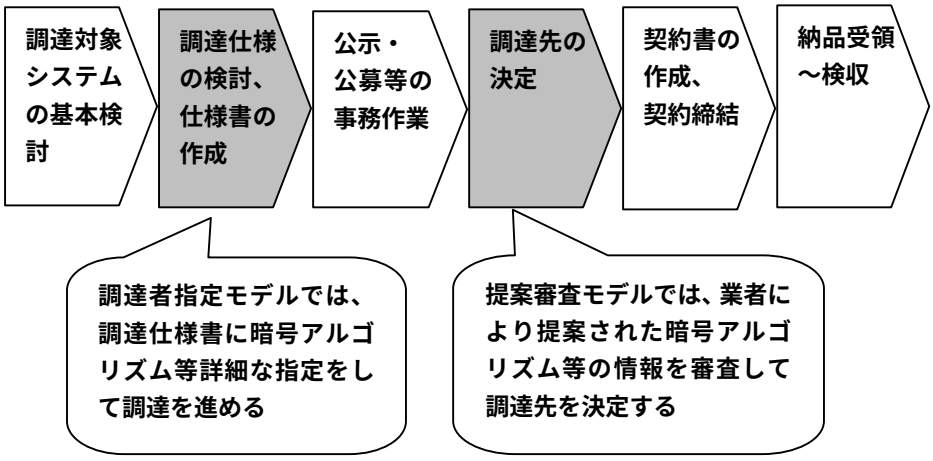


図４．１－２　暗号要件絞り込みのポイント

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。

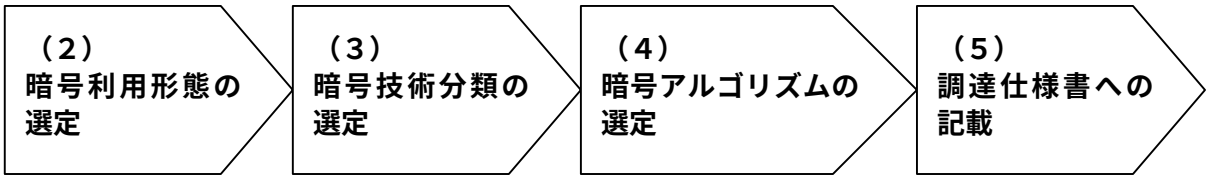


図４．２．１－１　調達者指定モデルにおける調達仕様書作成の流れ

（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。

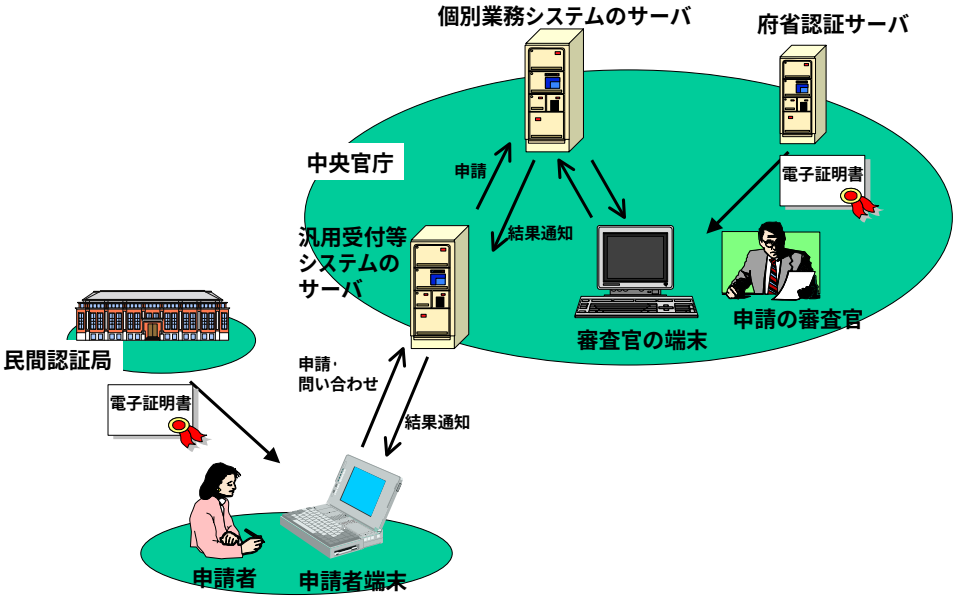


図４．２．１－２　電子申請システムのシステムモデル図

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 ・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	・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	
	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	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*

※ 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/
－ http://www.meti.go.jp/

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）

参考2

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。

（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。

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。

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

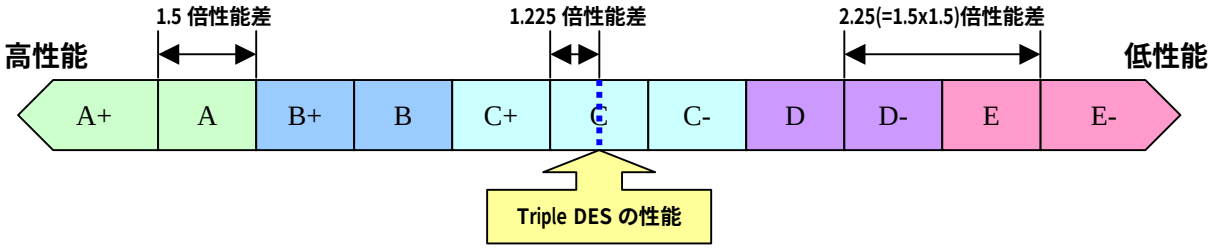


表 2：ソフトウェアによる処理性能における記号表記基準

	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

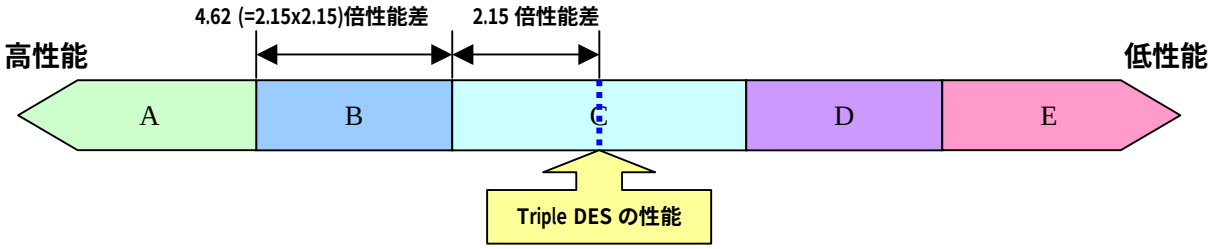
i. 最速値と平均値が測定されている暗号技術については最速値を採用する。
ii. 規定計測プログラムと修正計測プログラムとの両方が測定されている暗号技術については、速い方の値を採用する。
iii. 記号に付随する数値は、Triple DES との相対性能比を表す。
iv. X/Y と表記されている暗号技術は、暗号化性能評価が X、復号性能評価が Y であることを示す。特に区別がない場合は、暗号化性能と復号性能が同程度であることを示す。
v. X～Y と表記されている暗号技術は、プラットフォーム（Pentium II/III, UltraSPARC IIi, Alpha 21264）等の実装条件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