暗号技術検討会

２０１３年度報告書

２０１４年３月

目　　次

１．はじめに ····· － 1－

２．暗号技術検討会開催の背景及び開催状況 ····· － 2－
　２．１．暗号技術検討会開催の背景 ····· － 2－
　２．２．CRYPTREC の体制 ····· － 2－
　２．３．暗号技術検討会の開催状況 ····· － 3－

３．各委員会の活動報告 ····· － 4－
　３．１．暗号技術評価委員会 ····· － 4－
　　３．１．１．活動の概要 ····· － 4－
　　３．１．２．2013 年度の活動内容 ····· － 4－
　　３．１．３．暗号技術評価委員会の開催状況 ····· － 4－
　３．２．暗号技術活用委員会 ····· － 6－
　　３．２．１．活動の概要 ····· － 6－
　　３．２．２．2013 年度の活動内容 ····· － 6－
　　３．２．３．暗号技術活用委員会開催状況 ····· － 6－

４．今後の CRYPTREC の活動について ····· － 8－

１．はじめに

情報通信技術を安心・安全に利用できる環境を構築していくにあたり、暗号技術は必要不可欠なものとなっている。また、昨今暗号技術は、クラウドコンピューティングやビッグデータの活用においても、データの活用とプライバシー保護の両立などのキーテクノロジーとしてますます注目を集めている。このため、暗号解読技術等の進展に注意を払い、適切なものを使用するよう努めることが重要であり、引き続き監視を行っていくことが重要である。

政府においても、情報セキュリティ政策会議（議長：内閣官房長官)において、2013 年 6 月に「サイバーセキュリティ戦略」が決定され、暗号技術については、「安全評価がなされたものの利用」を推進することが示されている。また間もなく改定が予定されている「政府機関の情報セキュリティ対策のための統一基準」では、暗号化及び電子署名のアルゴリズムについて、CRYPTREC 暗号リストに記載されたアルゴリズムを使用することが定められる見込みである。CRYPTREC としても、暗号に関する技術的な評価等を通じて、政府のこれらの動きを適切に支援していく。

CRYPTREC は、「電子政府推奨暗号リスト」（平成 15 年 2 月 20 日公表）を昨年度に改定した「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト)」を策定したことを踏まえ、今年度から暗号技術検討会の下に暗号技術評価委員会と暗号技術活用委員会の 2 委員会を設ける体制に移行した。新設の暗号技術評価委員会では前年度の暗号方式委員会の全課題及び暗号実装委員会の一部課題を、また新設の暗号技術活用委員会では前年度の暗号運用委員会の全課題及び暗号実装委員会の一部課題を引き継ぎ、暗号技術に関する継続的な評価・監視を通じてリスト掲載暗号の安全性を担保すると同時に、掲載暗号の利用の取組を推進する。

今年度の委員会別の活動として、暗号技術評価委員会では、暗号技術の安全性及び実装に係る監視及び評価、軽量暗号などの新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査等を行った。暗号技術活用委員会では、運用ガイドラインの検討や標準化推進に向けた調査等の暗号の普及促進・セキュリティ産業の競争力強化に係る検討、暗号技術の利用状況に係る調査及び必要な対策の検討等を行った。なお、2013 年度の活動のうち、詳細な技術的事項については、暗号技術評価委員会及び暗号技術活用委員会における議論を踏まえて、独立行政法人情報通信研究機構及び独立行政法人情報処理推進機構が取りまとめる「CRYPTREC Report 2013」を参照いただきたい。

末筆であるが、本検討会及び関係委員会に御協力いただいた構成員、オブザーバの方々をはじめ、関係者の皆様に心から謝意を表する次第である。

2014 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及び開催状況

２．１．暗号技術検討会開催の背景

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 年度から暗号技術検討会を開催した。

暗号技術検討会において 2002 年度に策定された電子政府推奨暗号リストは、2012 年度に 10 年ぶりの改定が行われ、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（以下、「CRYPTREC 暗号リスト」という。）として発表されたが、その後においても、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の更なる普及促進を行うため、総務省及び経済産業省は、継続的に暗号技術検討会を開催している。

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：今井秀樹中央大学教授）と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する委員会から構成される暗号技術評価プロジェクトをいう。

2013 年度の CRYPTREC の体制は、前年度の３委員会体制（暗号方式委員会、暗号実装委員会、暗号運用委員会）を再編し、暗号技術検討会の下に、暗号技術評価委員会及び暗号技術活用委員会の２つの委員会を設置し、調査・検討を行った。

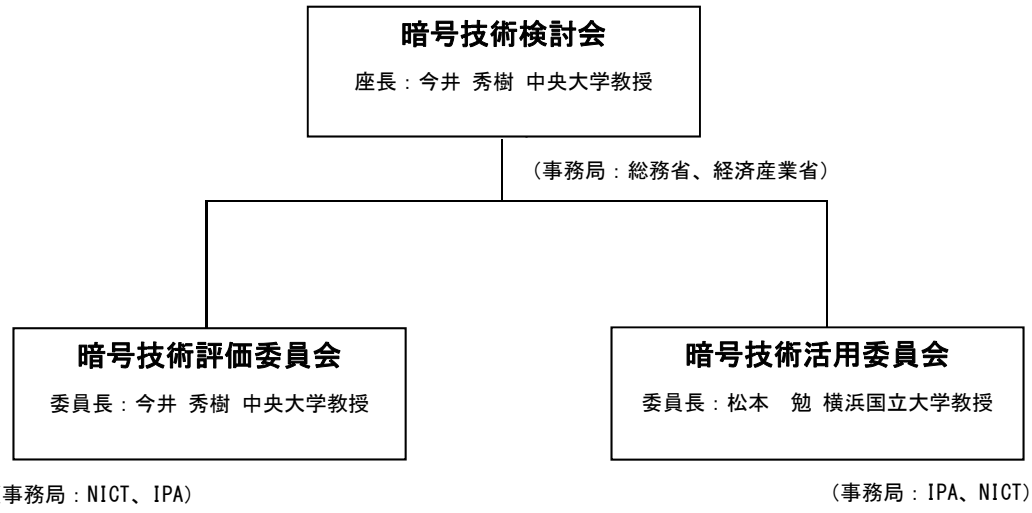

図 2.1　2013 年度 CRYPTREC の体制図

２．３．暗号技術検討会の開催状況

2013 年度の暗号技術検討会は、暗号技術評価委員会及び暗号技術活用委員会の活動計画及び報告等を審議するために２回開催し、その他に暗号技術活用委員会で作成する「SSL/TSL サーバ構築ガイドライン」の策定状況について、メールによる意見照会を実施した。

【第 1 回】2013 年 7 月 5 日（金）14:00～15:30

（主な議題）

- 暗号技術評価委員会及び暗号技術活用委員会の活動計画について
- CRYPTREC 暗号リストの暗号アルゴリズム仕様書について

（概要）

- 暗号技術評価委員会及び暗号技術活用委員会の 2013 年度の活動計画について説明を行い、承認を得た。
- 暗号技術活用委員会で作成する、SSL/TLS に関する運用ガイドラインについて、策定に当たっての検討の結果、運用ガイドラインでは必ずしも電子政府推奨暗号リストに掲載された暗号のみを取り上げるわけではないことも想定されるため、これまでの CRYPTREC の活動と整合するかどうか等の観点から作成されたガイドラインを事前に検討会でチェックし、CRYPTREC のクレジットとして発行すべきものか否かを判断する場を設けることとした。
- CRYPTREC ホームページにおいて掲載している CRYPTREC 暗号リストに掲載された暗号技術の仕様書の参照先を更新することにした。

【第 2 回】2014 年 3 月 27 日（木）14:00～15:35

（主な議題）

- 暗号技術評価委員会、暗号技術活用委員会の活動報告について
- 2013 年度暗号技術検討会報告書（案）について
- 2014 年度の暗号技術検討会、暗号技術評価委員会及び暗号技術活用委員会の活動計画について

（概要）

- 暗号技術評価委員会及び暗号技術活用委員会の 2013 年度の活動概要について報告を行った。
- RC4 の脆弱性を広く周知する重要性が指摘され、暗号技術評価委員会が発行する暗号技術ガイドライン（SSL/TLS における近年の攻撃への対応）の公開等により、周知を強化することとなった。
- 乱数の生成方法について、次年度の暗号技術ガイドラインのテーマとして検討することとなった。
- 暗号技術活用委員会において作成中の、SSL/TLS サーバ構築ガイドラインについて、暗号の利用実態を考慮し、電子政府推奨暗号である DH よりも、運用監視暗号である RSA の優先順位を高くした旨の説明がなされた。
- 今後の電子政府推奨暗号リストの活用方法を検討するに当たり、暗号の強度と共に、引き続き実用面についても考慮していくべきとの意見があった。
- 2013 年度暗号技術検討会報告書について説明を行い、後日、第 2 回暗号技術検討会の議事内容を反映させ、最終確認を行うことで承認を得た。

・ 2014 年度暗号技術検討会活動計画について説明を行い、承認を得た。
・ 暗号技術評価委員会及び暗号技術活用委員会の 2014 年度の活動計画について説明を行い、承認を得た。なお、暗号技術活用委員会の活動計画については、SSL/TLS サーバ構築ガイドライン作成後、次にどのようなガイドラインが必要かを検討することを活動計画に盛り込むこととなった。

【メールによる意見照会】2013 年 12 月 24 日（火）～2014 年 1 月 17 日（金）
・ 暗号技術活用委員会において策定中の「SSL/TLS サーバ構築ガイドライン」について、第１回暗号技術検討会における議論を踏まえ、中間とりまとめの段階でメールによる意見照会を実施した。構成員からは、特段の意見は出されなかった。

３．各委員会の活動報告

３．１．暗号技術評価委員会

３．１．１．活動の概要

暗号技術評価委員会は、2013 年度に新たに発足した委員会であり、2012 年度まで開催していた暗号方式委員会の全課題及び暗号実装委員会の一部課題を主に引き継ぎ、暗号技術の信頼性に関する調査・検討を実施する。

2013 年度は、暗号技術の安全性及び実装に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査等を行った。以下に、その具体的内容を報告する。

３．１．２．2013 年度の活動内容

暗号技術の安全性及び実装に係る監視及び評価

2013 年度は、研究集会、国際会議、研究論文誌の情報等を収集し、リスト掲載暗号の安全性について監視活動を行った。攻撃研究等に関して、早急な対処が必要なものは存在しなかったが、暗号解読技術等の進展が見られ、これらについて引き続き注視していく必要がある。

また、擬似乱数生成アルゴリズム Dual_EC_DRBG の脆弱性の可能性等、リストに掲載されていない暗号に関しても、社会への影響が大きい話題については注意喚起を実施した。

新世代暗号に係る調査

本項目に係る活動に関しては、暗号技術評価委員会の下に暗号解析評価 WG 及び軽量暗号 WG を設置し、議論した。暗号解析評価 WG では、素因数分解や離散対数問題の困難性等、暗号技術の安全性に係る調査を実施した。軽量暗号 WG では、リソースの限られたデバイスにも実装可能な軽量暗号について、要求条件や評価方法等の検討を行った。

暗号技術の安全な利用方法に関する調査

CRYPTREC 暗号技術ガイドラインとして「SSL/TLS における近年の攻撃への対応」及び「SHA-1」を発行した。前者は、近年効率的な攻撃手法が開発された SSL/TLS について、安全に利用するための適切な設定等を推奨するための文書であり、今年度暗号技術活用委員会において作成された「SSL/TLS サーバ構築ガイドライン」においても参照されている。後者は、現在でも広範に使用されている一方で危殆化が進むハッシュ関数 SHA-1 について、許容される使用例を明示した文書である。

また、「電子政府推奨暗号リスト」の改訂を踏まえたリストガイドの改訂方針を検討した。

３．１．３．暗号技術評価委員会の開催状況

2013 年度、暗号技術評価委員会は計 3 回開催した。各回会合の概要は表 3.1 のとおりである。

表 3.1　暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2013 年　7 月 29 日	暗号技術評価委員会活動方針の検討 WG 活動方針の検討 外部評価についての検討 監視状況報告 改訂された暗号アルゴリズム仕様書に関する検討
第 2 回	2013 年　12 月 13 日	WG 中間活動報告 外部評価についての検討 監視状況報告 暗号技術ガイドラインに関する検討 改訂された暗号アルゴリズム仕様書に関する検討
第 3 回	2014 年　3 月 6 日	WG 今年度活動報告 外部評価についての報告 監視状況報告 暗号技術ガイドライン策定の報告 次年度の検討項目に関する検討

３．２．暗号技術活用委員会

３．２．１．活動の概要

暗号技術活用委員会は、2013 年度から新たに設置された委員会であり、2012 年度まで開催していた暗号運用委員会の全課題及び暗号実装委員会の一部課題を引き継ぎ、CRYPTREC 暗号リスト改定の一環である暗号技術の利用状況に係る調査、暗号技術における国際競争力の向上及び運用面での安全性向上に関する検討を実施する。主要な検討課題は以下のとおりである。

・暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）
・暗号技術の利用状況に係る調査及び必要な対策の検討等
・暗号政策の中長期的視点からの取組の検討（暗号人材育成等）

2013 年度は、暗号の普及促進・セキュリティ産業の競争力強化に係る検討、暗号政策の中長期的視点からの取組の検討を行った。以下に、その具体的内容を報告する。

３．２．２．2013 年度の活動内容

暗号の普及促進・セキュリティ産業の競争力強化に係る検討

暗号技術の普及促進・セキュリティ産業の競争力強化についての課題分析を行うに当たって、まずは現状を把握するため、電子政府推奨暗号リストの活用状況や国産暗号に対する考え方等について、関係機関にヒアリングを実施した。

また、暗号の普及促進の具体的な方策について検討するため、暗号技術活用委員会の下に運用ガイドライン WG 及び標準化推進 WG を設置した。

運用ガイドライン WG では、暗号システムを安全に利用できるようにすることを目的とした運用ガイドラインの作成について議論を行い、2013 年度は利用者が多い SSL/TLS について取り上げ、「SSL/TLS サーバ構築ガイドライン」の策定作業を行った。本ガイドラインは、本年 7 月に完成する見込みである。

標準化推進 WG では、各標準化機関に対して、日本から暗号アルゴリズムを提案する際に効率的な提案活動が行えるよう、各標準化機関での活動状況について発表及び意見交換を行い、効率的な提案方法等について情報共有を行った。

暗号政策の中長期的視点からの取組の検討

暗号政策の中長期的視点からの取組である暗号人材育成について、必要な人材像を把握するために、暗号アルゴリズムの選択時の留意点や現状の実務担当者の暗号に関する知識レベル等について、関係機関にヒアリングを行った。

３．２．３．暗号技術活用委員会の開催状況

2013 年度、暗号技術活用委員会は、計 3 回開催された。各回会合の概要は表 3.2 のとおりである。

表 3.2　暗号技術活用委員会の開催

回	年月日	議題
第 1 回	2013 年　9 月 11 日	本年度の活動計画 運用ガイドライン WG 及び標準化推進 WG の活動内容の検討 「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」について分析を行うためのヒアリング内容の検討
第 2 回	2013 年　12 月 13 日	SSL/TLS サーバ構築ガイドラインとりまとめの中間報告 標準化推進 WG の活動についての中間報告 ヒアリングについての中間報告
第 3 回	2014 年　3 月 19 日	ヒアリング調査報告 WG 活動報告 次年度の活動計画

４．今後の CRYPTREC 活動について

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、2014 年度以降も引き続き以下の活動を実施する予定である。

(1) CRYPTREC暗号リストの小改定に関する意思決定（暗号技術検討会が実施予定）
- (a) 推奨候補暗号リストに掲載されている暗号技術の昇格を検討する
- (b) 新規暗号（事務局選出）及び新技術分類の追加（新規暗号公募含む）に関する方針を検討する。
- (c) 内閣官房情報セキュリティセンター等政府関係機関との連絡・調整を実施する。

(2) 暗号技術の安全性評価を中心とした技術的な検討（暗号技術評価委員会が実施予定）
- (a) 新世代暗号に係る調査（軽量暗号、セキュリティパラメータ、ペアリング、耐量子計算機暗号等）を実施する。
- (b) 暗号技術の安全性に係る監視及び評価（SHA-3の評価を含む）を実施する。
- (c) 暗号技術の安全な利用方法に関する調査（技術ガイドラインの整備、学術的な安全性の調査・公表等）を実施する。

(3) セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討（暗号技術活用委員会が実施予定）
- (a) 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）を実施する。
- (b) 暗号技術の利用状況に係る調査及び必要な対策の検討等を実施する。
- (c) 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）を実施する。