暗号技術検討会
２０１４年度　報告書

２０１５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－
　　３．１．２．2014 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－
　　３．２．２．2014 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、セキュリティの基盤技術として暗号技術の必要性は益々大きくなっている。昨年 11 月 6 日に「サイバーセキュリティ基本法」が成立し、今年 1 月 9 日に「サイバーセキュリティ戦略本部」が設置されるなど、政府もサイバーセキュリティ対策をより一層強く推進している。「政府機関の情報セキュリティ対策のための統一基準」にも、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ており、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。

また、同法では「情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題」であることが謳われているが、情報の自由な流通とサイバーセキュリティを両立させるための基盤技術として、暗号技術に対する社会からの要請は一段と大きく、多様化していくものと考えられる。来たるべき IoT 社会においては、情報の流通量が顕著に増加するだけでなく、接続される機器の種類や性能も千差万別となり、それぞれの使用目的に合わせた暗号技術の利用が飛躍的に広がることが期待される。

CRYPTREC は、「CRYPTREC 暗号リストの大改定」及び「暗号技術評価委員会及び暗号技術活用委員会からなる 2 委員会体制への移行」を行ってから 2 年が経過した。CRYPTREC として、従来通りの暗号技術の評価・監視活動を引き続き堅持するとともに、軽量暗号等の新暗号技術への取組や、一般での利用も想定した形での「SSL/TLS 暗号設定ガイドライン」の策定など、上記のような暗号技術に対する社会の要請に応えるべく、新しい領域の活動も推進してきたが、これらの取組を行っていく中で、改めて重要性を認識した点、新たに課題として浮き彫りにされた点などが確認された。日本の暗号政策の要石を担う存在として、新しい時代の要請にあわせ CRYPTREC が今後どう在るべきか、改めて検討することが有意義であると思われる。

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策定、標準化推進に向けた取組、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等を行った。なお、2014 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 2014」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。

2015 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：今井秀樹東京大学名誉教授）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。

2014 年度の CRYPTREC の体制は、前年度に引き続き、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。

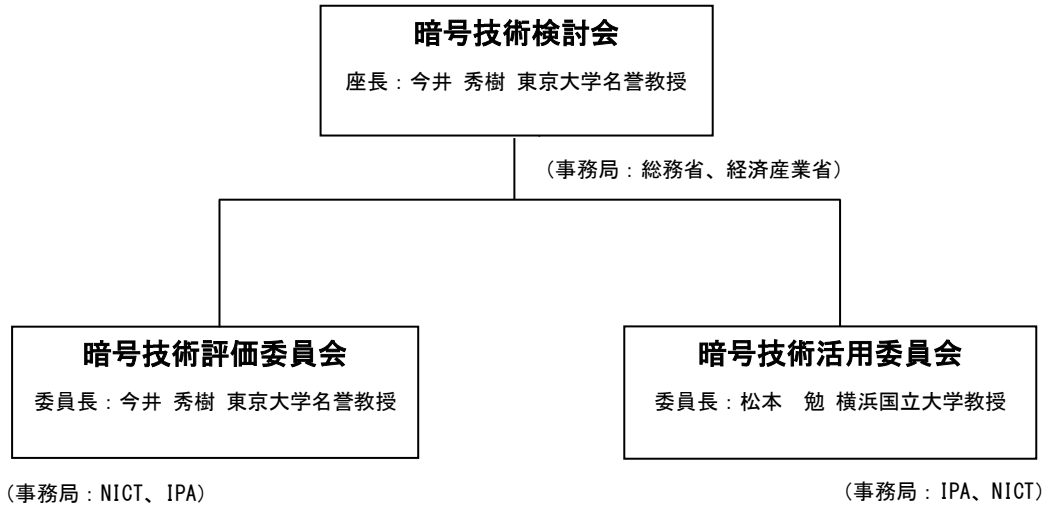

図 2.1　2014 年度 CRYPTREC の体制図

２．３．暗号技術検討会の開催状況

2014 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報告、CRYPTREC 暗号リストの注釈変更等を審議するために２回開催した。

【第 1 回】2014 年 10 月 9 日（木）14:00～15:05
（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中間報告について
（概要）
・ 暗号技術検討会の下部委員会である、暗号技術評価委員会及び暗号技術活用委員会の 2014 年度の活動の中間報告を行った。
・ 軽量暗号について、国内でどういったアプリケーションを利用し、どのように利用を推進していくのかという視点での検討が必要との意見があった。
・ 「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」及び「暗号政策の中長期的視点からの取組の検討」に関して、国産暗号、暗号アルゴリズムといった枠組みにとらわれず広い意味での暗号技術と産業競争力や課題解決との関係性を整理するべきという意見があった。

【第 2 回】2015 年 3 月 27 日（金）10:00～12:00
（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
・ CRYPTREC 暗号リストの注釈の一部変更について
・ 2014 年度暗号技術検討会報告書（案）について
・ 暗号技術検討会における小グループの設置について
・ 2015 年度の暗号技術評価委員会活動計画について
・ 2015 年度の暗号技術活用委員会の活動について
（概要）
・ 暗号技術評価委員会及び暗号技術活用委員会の 2014 年度の活動概要について報告を行った。
・ 運用監視暗号リストに掲載されている 128-bit RC4 について、128-bit RC4 への有力な攻撃手法が示されている実態を踏まえ、電子政府推奨暗号リストに掲載されている安全な暗号技術への速やかな移行を促すため、CRYPTREC 暗号リストの注釈の一部変更を行うことで承認を得た。
・ 2014 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。
・ 2015 年度に暗号技術検討会の下に小グループを設置し、今後の CRYPTREC の活動内容及び対象範囲について集中的に議論を行うことで承認を得た。
・ 2015 年度暗号技術評価委員会活動計画及び 2015 年度の暗号技術活用委員会の活動について説明を行い、承認を得た。

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、CRYPTREC 暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う。主要な検討課題は以下のとおりである。

・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

これらの課題について 2014 年度に行った具体的な検討内容を、以下のとおり報告する。

３．１．２．2014 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

2014 年度は、① 学会等での情報収集に基づく CRYPTREC 暗号等の監視、② 128-bit RC4 の注釈に係る検討、③ 推奨候補暗号リストへの追加のための外部評価等を実施した。

①について、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。

②について、128-bit RC4 に対する有力な攻撃手法が明らかにされたことから、速やかに他のアルゴリズムに移行されることが望ましいという合意に至り、「互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。」という注釈変更案を採択した。

③について、推奨候補暗号リストへの追加を検討する事務局選出の暗号アルゴリズムとして、SHA-2 ファミリーに新たに追加されたハッシュ関数や SHA-3 について安全性に係る外部評価を実施した。

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技術調査 WG（暗号解析評価）及び暗号技術調査 WG（軽量暗号）を設置し、議論した。暗号技術調査 WG（暗号解析評価）では、格子問題や離散対数問題の困難性等、暗号技術の安全性を支える数学的問題の困難性に係る調査を実施した。暗号技術調査 WG（軽量暗号）では、昨年度から実施してきた現状調査、実装評価等に基づき、来年度以降に暗号技術ガイドラインを作成する等の CRYPTREC としての活動方針について暗号技術評価委員会に対して提言を行った。

暗号技術の安全な利用方法に関する調査

昨年度発行した CRYPTREC 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」について、2014 年 10 月に SSL3.0 における CBC モードに対する新たな攻撃として「POODLE 攻撃」が公表されたことを受け、当該攻撃に関する記載を追加した。

３．１．３．暗号技術評価委員会の開催状況

2014 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	2014 年　8 月 4 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 128-bit RC4 の注釈変更に関する検討 監視状況報告 CRYPTREC 暗号リスト掲載暗号技術の仕様書に関する検討
第 2 回	2014 年　12 月 25 日	WG 中間活動報告 外部評価についての中間報告 監視状況報告 暗号技術ガイドラインの更新に関する検討 CRYPTREC 暗号リスト掲載暗号技術の仕様書に関する検討
第 3 回	2015 年　3 月 2 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 128-bit RC4 の注釈変更に関する検討 暗号技術ガイドラインの更新に関する検討 CRYPTREC 暗号リスト掲載暗号技術の仕様書に関する検討 CRYPTREC2014 の目次案に関する検討 次年度の活動計画に関する検討

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、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）

2014 年度は、2013 年度から 2 年間かけて取り組んだ、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について、取りまとめを行った。以下に、その具体的内容を報告する。

３．２．２．2014 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は、2013 年度に実施した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に関するヒアリング内容を踏まえ、課題分析を行い、今後の検討にあたっての留意点を取りまとめた。

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て、利用者が多い SSL/TLS について、「SSL/TLS 暗号設定ガイドライン」の策定を行い、利用者が必要な設定を確認しやすいよう、「SSL/TLS 暗号設定ガイドラインチェックリスト」についても策定した。

標準化推進 WG では、今後暗号技術を提案する者が提案先を選定する際に参考となるような資料として、規格の参照関係を整理した、「暗号技術参照関係の俯瞰図」を作成した。また、様々な標準化機関に対する日本からの暗号アルゴリズム提案を支援するため、標準化団体における基本的な情報、提案活動に関する交渉ノウハウや課題等を取りまとめた。

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は、2013 年度に実施した必要な人材像に関するヒアリング内容を踏まえ、今後実施していくべき人材育成策について検討するにあたっての留意点を取りまとめた。

RC4 の注釈について

CRYPTREC 暗号リストにおける RC4 の注釈について検討を行い、早期に RC4 からの移行を進めることが望ましく、今後は極力利用すべきでないという意図を明確化する観点から、暗号技術活用委員会として、「互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。」という注釈変更案を採択した。

３．２．３．暗号技術活用委員会の開催状況

2014 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	2014 年　10 月 30 日	本年度の活動計画の確認 運用ガイドライン WG 及び標準化推進 WG の活動について 最終報告書とりまとめに向けた論点整理 128-bit RC4 の注釈変更について
第 2 回	2015 年　1 月 26 日	SSL/TLS 暗号設定ガイドラインの中間審議 標準化推進 WG の活動についての中間審議 最終報告書の内容に関する中間審議 128-bit RC4 の注釈変更について
第 3 回	2015 年　3 月 10 日	運用ガイドライン WG 及び標準化推進 WG の活動報告 最終報告書の審議

４．今後の CRYPTREC の活動について

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、暗号技術の安全性及び実装に係る監視及び評価を引き続き実施するとともに、現在の２委員会体制に移行してから２年間が経過したことを踏まえ、暗号技術検討会に２年間の活動の評価と今後の CRYPTREC のあり方について議論を行う小グループを設置し、日本の安全な ICT 基盤確立にむけて CRYPTREC が取り組むべき活動の範囲や方針について提言を行う。