暗号技術検討会
２０１７年度　報告書

２０１８年３月

目　　次

１．はじめに

情報通信技術の急速な発展により、自動車、家電、医療、農業、工場など様々な分野で、あらゆるモノがネットワークに繋がる IoT 社会が到来し、サイバー空間と実空間の高度な融合により、多様なニーズにきめ細やかに対応したモノやサービスを提供できる社会への産業構造の変化が進みつつある。一方で、IoT の普及に伴うサイバー攻撃の起点の増加や、サイバー攻撃自体の巧妙化・複雑化が続く中で、サイバー攻撃の影響が実空間にまで到達するリスクも増していくと考えられる。このような産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応したセキュリティ確保が求められる中、暗号技術は既に様々な製品やサービスに組み込まれ、セキュリティを支える基盤技術として欠かせないものであるが、IoT から得られる大量のデータの流通・連携を支える上でも、その重要性は一層増すと考えられる。

このような社会の変化に伴い、CRYPTREC においても、これまで取り組んできた暗号アルゴリズムのセキュリティ確保を引き続き推進することに加えて、暗号アルゴリズムを利用したプロトコルのセキュリティ確保のための活動拡大や、情報システム全体のセキュリティ確保に向けた暗号技術の利活用のための情報提供等の貢献が求められている。

本年度の CRYPTREC は、昨年度までの「重点課題検討タスクフォース」での議論を踏まえた検討体制の下で、暗号技術検討会では、これまでの成果物である CRYPTREC 文書について、文書番号から内容を判断できるように文書番号体系の整理を実施した。

また、本年度の各委員会の活動として、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、DSA 及び DH の安全性に関する注意喚起レポートの発行、SHA-1 の衝突を受けた「暗号技術ガイドライン(SHA-1)」の改定、新技術に関する調査及び評価等の検討等を行った。また、同委員会の下に設置された暗号技術調査 WG において、欧米での調査・検討や標準化に向けた議論が始まっている耐量子計算計算機暗号の研究動向調査を行った。暗号技術活用委員会では、情報システム全般のセキュリティ確保に寄与することを目的として、作成すべき運用ガイドラインの候補を昨年度取りまとめたが、その中から必要性・重要性の高い鍵管理に関する運用ガイドラインの作成に向けた調査を行った。加えて、2015 年に発行した「SSL/TLS 暗号設定ガイドライン」について、近年の状況変化を踏まえた改定に向けた検討等を行った。これらの 2017 年度の活動の詳細については、国立研究開発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 2017」を参照いただきたい。

今後も暗号技術を用いた情報システム及び情報社会全体のセキュリティ確保のために、成果物の検討や情報発信等を行っていく所存である。

末筆であるが、暗号技術検討会及び関係委員会等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。

2018 年 3 月

暗号技術検討会
座長　松本　勉

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 年度に暗号技術検討会を設置した。

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：松本勉横浜国立大学教授）と、国立研究開発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。

2017 年度の CRYPTREC においては、暗号アルゴリズムの安全性確保やその利活用に係る議論のみならず、暗号技術に対する社会ニーズの変化や、社会情勢の変化を踏まえ、暗号技術評価委員会では、ハッシュ関数 SHA-1 を継続利用する際の指針となるガイドラインの改定や、耐量子計算機暗号（Post-Quantum Cryptography）の技術動向調査を実施し、暗号技術活用委員会では、SSL/TLS 暗号設定ガイドラインの改定に向けた検討や、鍵管理のガイドライン作成に向けた調査を実施した。

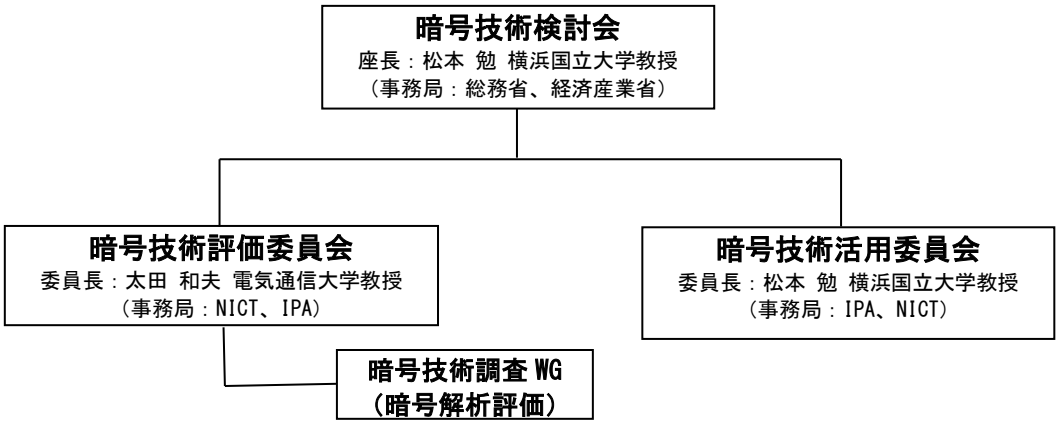

図 1　2017 年度 CRYPTREC 体制図

２．３．暗号技術検討会の開催実績

2017 年度の暗号技術検討会は、暗号技術評価委員会、暗号技術活用検討会の活動計画についてメールによる審議を年度当初に実施した上で、暗号技術評価委員会、暗号技術活用委員会の活動報告、CRYPTREC 暗号リストの改定について審議するために１回開催した。

【第 1 回】2018 年 3 月 29 日（木）15:00～17:00
（主な議題）
- 文章番号体系について
- 2017 年度 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 暗号リストの改定について
- 2017 年度 暗号技術検討会報告書（案）について

（概要）
- 2016 年度の暗号技術検討会での承認を受けて、事務局で決定した CRYPTREC 文書に対する文書番号の付番方法の報告が行われた。
- 2017 年度の暗号技術評価委員会及び暗号技術活用委員会の報告が行われた。
- CRYPTREC 暗号リストの 64 ビットブロック暗号に付記されている注釈について、引き続き安全に利用できることを目的とした注釈の変更案について審議を行い、原案を一部修正の上で注釈を変更することが承認された。
- 3-key Triple DES の取扱いについて審議を行い、原案のとおり、注釈を削除した上で、電子政府推奨暗号リストから運用監視暗号リストへ移すことが承認された。
- MISTY1 のフルラウンド攻撃への対応について審議を行い、原案のとおり、64 ビットブロック暗号に付記する注釈の変更をもって対応する方針が承認された。
- 認証暗号 ChaCha20-Poly1305 の推奨候補暗号リストへの追加について審議を行い、原案のとおり承認された。併せて、技術分類に「認証暗号」を新設することが承認された。
- 2017 年度暗号技術検討会報告書（案）について事務局より説明があり、後日、暗号技術検討会の議事概要を追記し、最終確認を行うことで承認を得た。

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、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
・暗号技術の電子政府推奨暗号リストからの降格
・暗号技術に関する注意喚起レポートの CRYPTREC ホームページへの公表
・新世代暗号に係る調査

これらの課題について 2017 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。

３．１．２．2017 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

2017 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 3-key Triple DES の電子政府推奨暗号リストからの降格、③ 64 ビットブロック暗号の注釈に関する検討を実施した。

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。2016 年度に報告済であるが、位数が 768 ビット長の素数である有限体における離散対数の計算に関する学会発表、及び、ハッシュ関数 SHA-1 のフルラウンド(全 80 ステップのうち 80 ステップすべて)の仕様に対する衝突発見に関する学会発表があった。前者に関しては、後述の注意喚起を行い、後者に関しては、暗号技術ガイドライン(SHA-1)の改定を検討した。それ以外において、攻撃研究等に関して緊急に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、現在、電子政府推奨暗号リストに記載されている 3-key Triple DES に関して、近年の状況に鑑みて、電子政府推奨暗号リストから運用監視暗号リストへ降格されることが適切であると判断した。

③ について、共通鍵暗号の 64 ビットブロック暗号に関して、近年の解析動向を考慮し、適切な注釈案の検討を行った。

暗号技術に関する注意喚起レポートの CRYPTREC ホームページでの公表

有限体上の離散対数問題は、電子政府推奨暗号リストに掲載されている DSA 及び DH や、インターネットで使われている通信プロトコル TLS における鍵共有方式など、多くの暗号技術の安全性の根拠として利用されているが、昨年、位数が 768 ビット長の素数である有限体における離散対数の計算結果が示された。RSA1024 に係る移行指針と同様に、DSA や DH を利用する場合には、鍵長において、2048 ビット以上の素数位数の有限体を用いることを推奨する注意喚起レポートを CRYPTREC ホームページで公表した。

新世代暗号に係る調査

本項目に係る活動に関しては、昨年度に引き続き、ChaCha20-Poly1305 の安全性及び実装性能の評価を行った。ChaCha20-Poly1305 は、認証暗号として十分な安全性及び実装性能を有していると判断した。また、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）を設置し、主に、耐量子計算機暗号（Post-Quantum Cryptography）の技術動向調査を実施した。

３．１．３．暗号技術評価委員会の開催状況

2017 年度、暗号技術評価委員会は計 2 回開催した。各回会合の概要は表 1 のとおりである。

表 1　暗号技術評価委員会の開催状況

回	開催日	議題
第 1 回	2017 年 7 月 21 日	・委員会今年度活動計画の検討 ・WG 活動計画の検討 ・外部評価(ChaCha20-Poly1305)についての検討 ・暗号技術ガイドライン(SHA-1)の改定の検討 ・64 ビットブロック暗号の今後の利用の検討 ・768 ビット素数の有限体上の離散対数問題の状況と DSA, DH の今後の利用についての注意喚起の検討 ・監視状況報告
第 2 回	2018 年 2 月 28 日	・WG 今年度活動報告 ・3-key Triple DES 及び 64 ビットブロック暗号の今後の利用についての検討 ・暗号技術ガイドライン(SHA-1)改定案の検討 ・外部評価(ChaCha20-Poly1305 の安全性及び実装性能)の検討 ・監視状況報告 ・CRYPTREC Report 2017(暗号技術評価委員会報告)の目次案提示

2017 年度、暗号技術調査 WG（暗号解析評価）は計 2 回開催した。各回会合の概要は表 2 のとおりである。

表 2　暗号技術調査 WG（暗号解析評価）の開催状況

回	開催日	議題
第 1 回	2017 年 7 月 27 日	・WG 活動計画の報告 ・今年度の作業内容についての審議
第 2 回	2018 年 2 月 21 日	・予測図の更新 ・耐量子計算機暗号の研究動向調査の進捗状況報告 ・WG 活動報告案の提示

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では、情報システム全般のセキュリティ確保に寄与することを目的として必要な活動を行うものとする。具体的には、実運用とセキュリティ確保の両面の観点から、以下の対象を取り扱う。

- 暗号アルゴリズムの利用及び設定に関する運用マネジメント
- 暗号プロトコルの利用及び設定に関する運用マネジメント
- その他、情報システム全体のセキュリティ確保に有用な暗号に関わる運用マネジメント

３．２．２．2017 年度の活動内容

2016 年度に取りまとめられた運用面でのマネジメントに関するガイドライン（以下、運用ガイドライン）の候補のなかから、必要性、目的、課題、関連組織等の状況を踏まえ、具体的に運用ガイドラインの対象を選定し、ガイドライン作成に向けた活動を行った。

具体的には、「鍵管理に関する運用ガイドライン作成に向けた活動」と「SSL/TLS 暗号設定ガイドラインのアップデートに向けた活動」からなる。

鍵管理に関する運用ガイドライン作成に向けた活動

2016 年度に取りまとめた運用ガイドラインの候補の中で鍵管理に関するものが多数を占めており、また実際に暗号を利用するうえでも鍵の正しい運用は不可欠である点から、鍵管理に関する運用ガイドラインの重要性は他と比較しても高いものと考えられる。

一方で、鍵管理に関するガイドラインは、その重要性からも、国内外を含め、いくつか発行されている。しかしながら、いずれのガイドラインも広く認知され、利用されているとは言い難い点を踏まえれば、従来の鍵管理ガイドラインには「ガイドラインとして利用しにくい」問題点が隠れているように思われる。例えば、

- 鍵管理として扱うべき範囲、考慮すべき範囲が広い
- 記述内容が抽象的になりがちである
- 技術的な観点だけでなく、法制度や運用ルール的な観点との整合性が求められる

といった意見が委員からも指摘された。

そこで、2017 年度の暗号技術活用委員会では、いきなり鍵管理に関するガイドラインを作成するのではなく、鍵管理に関する規格を網羅的に調査し、どのような体系・順番で鍵管理に関するガイドラインを作成していくのがよいのかを取りまとめた。

具体的には、鍵管理に関する運用ガイドライン作成に向けた事前調査として鍵管理に関する規格（21 文献）を網羅的に調査した。この調査結果から、SP 800-57 Part1 と SP 800-130 は非常に強い関連性を持ち、また、鍵管理全体のフレームワークとしてもっとも基本的な文献であると考えられることが確認できた。

今後、鍵管理に関する運用ガイドラインについては、SP 800-57 の内容と SP 800-130 の内容をより精査した上で、実際のガイドライン作成に臨むこととする。

なお、調査報告の詳細については、暗号技術活用委員会報告を参照されたい。

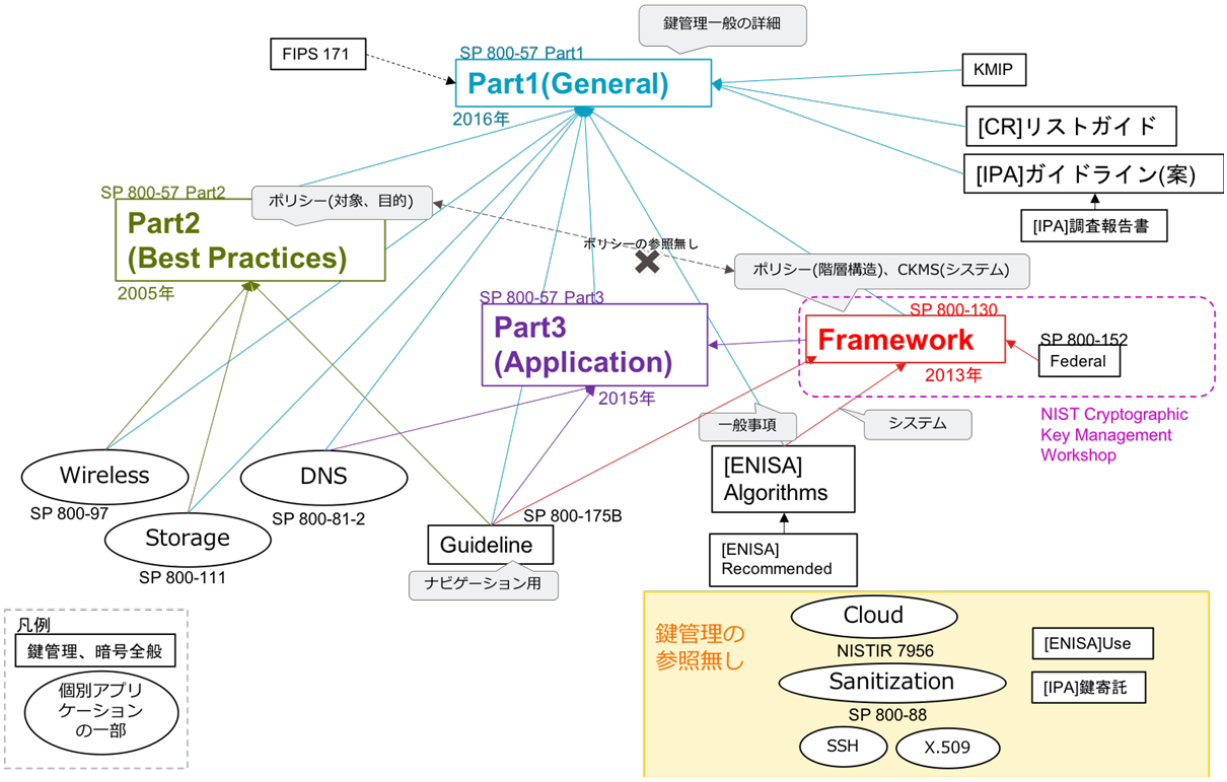

図 2　各文献における鍵管理に関する他文献への参照関係

SSL/TLS 暗号設定ガイドラインのアップデートに向けた活動

「SSL/TLS 暗号設定ガイドライン」については、2015 年発行時から状況が変化していること、10 万件を越えるダウンロード数があるなどニーズが多いことにから、2017 年度に、外部動向の追加ならびにそれに対応するためのマネジメント方針の追記・修正などを行い、SSL/TLS 暗号設定ガイドラインのアップデート案を作成した。

具体的には、2015 年以降の動向調査を実施し、その結果を踏まえて 22 箇所の SSL/TLS 暗号設定ガイドラインの記述を修正・追記・削除すべきかを検討した。合わせて、コラム記事を更新すべきかの議論を行った。

特に、前回 SSL/TLS 暗号設定ガイドラインを公開した 2015 年当時は、レガシーシステムや携帯電話などで SSL3.0 や SHA-1 証明書の利用を必要とするケースが無視できないことから、「セキュリティ例外型」を設け「早期移行を前提として暫定的な利用継続」を認めていたが、この 3 年間で SSL3.0 や SHA-1 証明書の利用からの脱却が大きく進んだことから「推奨セキュリティ型への早期移行を求めるものであり、すでに最低限の安全性水準を満たしているとは言えない状況になっている。」との記述変更を行う、などのアップデート案を策定した。

このアップデート案を反映したガイドラインを 2018 年 5 月に公開する予定である。

３．２．３．暗号技術活用委員会の開催状況

2017 年度 2 回開催された暗号技術活用委員会での審議概要は表 3 のとおりである。さらには、暗号技術活用委員会とは別に、SSL/TLS に関する動向及び鍵管理に関する公募調査の中間報告会を委員向けに実施した。

表 3　暗号技術活用委員会の開催状況

回	開催日	議題
第 1 回	2017 年 9 月 7 日	・SSL/TLS 暗号設定ガイドラインのアップデート作業について ・鍵管理に関する運用ガイドラインの事前検討について
報告会	2017 年 12 月 27 日	・SSL/TLS に関する動向及び鍵管理に関する公募調査の中間報告
第 2 回	2018 年 3 月 15 日	・SSL/TLS 暗号設定ガイドラインのアップデート案について ・鍵管理に関する運用ガイドライン作成に向けた今後の計画について

４．今後のCRYPTRECの活動について

CRYPTREC では、暗号アルゴリズムの安全性確保やその利活用に係る議論のみならず、鍵管理の安全な運用に向けた取組など、暗号技術を取り巻く環境変化に応じた新たなニーズへの対応などに取り組むこととしている。

暗号技術評価委員会においては、今後も引き続き、暗号技術の安全性に係る監視・評価及び実装に係る技術の監視・評価を行うと共に、耐量子計算機暗号の技術動向調査を取りまとめる。また、暗号技術活用委員会においては、本年度の検討を踏まえて鍵管理に関する運用ガイドラインを作成する。両委員会の範囲を超えるものについては、必要に応じて、暗号技術検討会で審議・判断する。

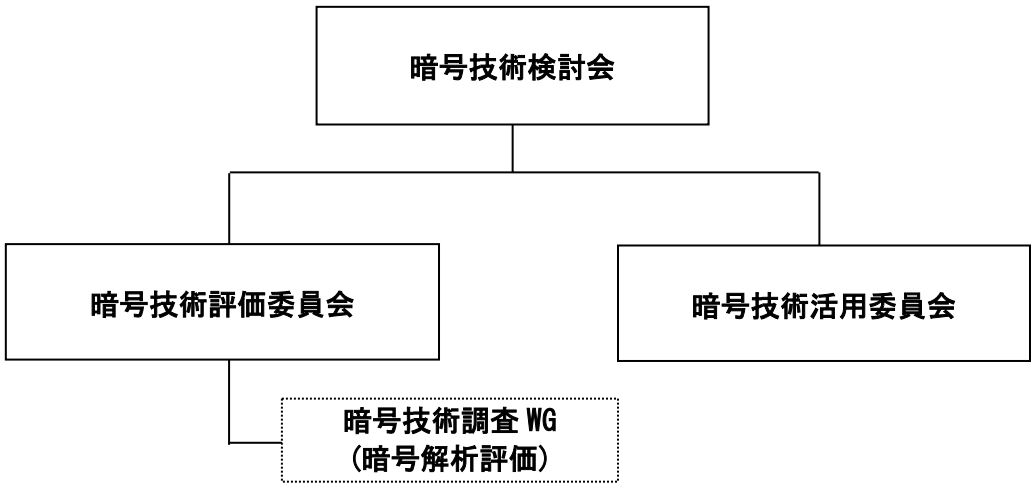

図 3　2018 年度 CRYPTREC の体制図（予定）