暗号技術検討会
２０１６年度　報告書

２０１７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融合が進みつつある。IoT の発展がもたらす利便性・効率の向上を享受できる一方で、巧妙化・複雑化を続けるサイバー攻撃のリスクも増していくと考えられるため、情報システム全体のセキュリティ確保は喫緊の課題である。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、その重要性は IoT 社会の到来により一層増すと考えられる。

このような社会の変化に伴い、CRYPTREC には、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といった貢献が求められている。

本年度、CRYPTREC では「重点課題検討タスクフォース」において、これまで年度ごとに整理されていた 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あり方について議論を行った。また、政府統一基準に向けた新たな CRYPTREC 成果物や、新たな社会ニーズを見据えた新規活動等の、前年度から把握している課題については、暗号技術検討会および各委員会に議論の場を移すこととするなど、今後の CRYPTREC の体制の整理を行った。

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、SHA-1 の安全性低下に関する注意喚起レポートの発行、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軽量暗号 WG において、軽量暗号技術の利用促進を図るため、昨年度より作成を進めていた「暗号技術ガイドライン（軽量暗号)」を公開した。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対象及び取扱い範囲の切り分けの検討、作成した運用ガイドラインのアップデート方法の検討等を行った。加えて、CRYPTREC として暗号プロトコルをどのように扱うかを重点的に検討するため、新たに「暗号プロトコル課題検討 WG」を設置し、まずは暗号プロトコルをテーマとする運用ガイドラインの検討対象を検討した。これらの 2016 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 2016」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。

2017 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：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。

2016 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軽量暗号ガイドラインを策定し、暗号技術活用委員会では新たにガイドラインを策定すべきものについて議論を進め、来年度に向けて整理を行った。また、昨年度に引き続き、重点課題検討タスクフォースにて議論を行い、文書番号体系の検討や、同タスクフォースの廃止に伴い、今後の体制を整理した。

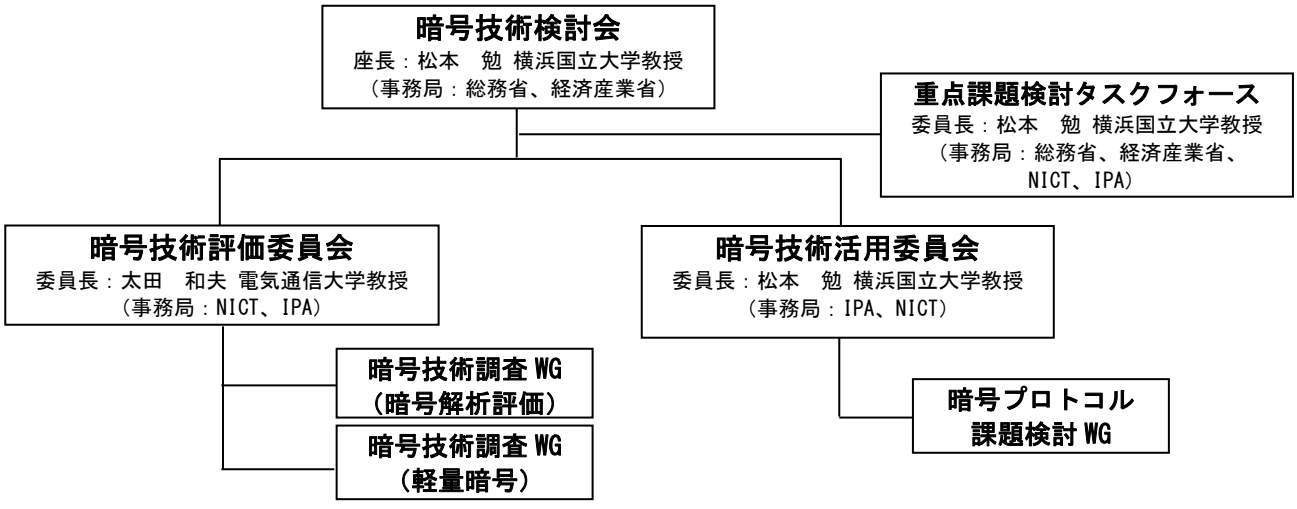


図 2.2.1　2016 年度 CRYPTREC の体制

２．３．暗号技術検討会の開催状況

2016 年度の暗号技術検討会は、以下に挙げる議題について審議、承認を行うために１回開催した。

〇2017 年 3 月 30 日（木）15:00～17:00

（主な議題）

- CRYPTREC の今後の体制（案）について
- 文書番号体系について
- 2016 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
- SHAKE128 の推奨候補暗号リストへの追加について
- ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に入れた評価について
- KCipher-2 の仕様書について
- SHA-1 の安全性低下について
- 2016 年度　暗号技術検討会報告書（案）について

（概要）

- CRYPTREC の今後の体制（案）について検討会事務局より説明が行われ、重点課題検討ＴＦの廃止、及び今後の暗号技術検討会の運用方法について承認を得た。
- 文書番号体系について重点課題検討ＴＦにて審議された内容の説明が行われ、提案のとおり承認された。
- 2016 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。
- SHAKE128 の推奨候補暗号リストの追加について審議が行われ、原案のとおり、SHAKE128 を推奨候補暗号リストに追加することで承認を得た。
- ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に入れた評価について、引き続き評価委員会にて安全性評価を実施していくことで承認を得た。また、今後新たにその他の暗号アルゴリズムの評価を行うかどうかの判断は、暗号技術検討会で行うことが承認された。
- KCipher-2 の仕様書の変更について、原案のとおり、仕様書を修正することで承認を得た。
- SHA-1 に関する速報掲載について、報告が行われた。これに対し、これ以上危殆化が進んだ場合の対応について考える必要があるとのコメントがあった。
- 共通鍵暗号の安全性調査と MISTY1 についての審議が行われた。これに対し、今後も同様の事態は起こる可能性があり、個別に判断をしなければならないとのコメントがあった。出された意見をもとに、引き続き暗号技術評価委員会で検討を進めていくこととした。
- 2016 年度暗号技術検討会報告書（案）について検討会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．重点課題検討タスクフォース

３．１．１．設置の経緯

2015 年 6 月から 8 月までに開催された「CRYPTREC の在り方に関する検討グループ」での議論の結果、政府統一基準に向けた新たな CRYPTREC 成果物の在り方、暗号プロトコルのセキュリティ確保に向けた活動等において、継続的な議論が必要との結論となった。

このため、暗号技術検討会の下に「重点課題検討タスクフォース」を設置し、これら継続的に議論することとなった論点や、その他 CRYPTREC の方向性を機動的に検討し、トップダウン的な意思決定もできる体制を構築することとした。

３．１．２．重点課題検討タスクフォースの開催状況

本年度、重点課題タスクフォースは１回開催した。会合の概要は表 3.1 のとおり。

表 3.1.1　重点課題検討タスクフォースの開催実績

回	年月日	主な議題
第４回	2017 年 2 月 22 日	・CRYPTREC の今後の体制（案）について ・文書番号体系（案）について

３．１．３．2016 年度の議論概要

2016 年度、重点課題検討タスクフォースを１回開催した。タスクフォースでの審議事項は、主に(1) CRYPTREC の今後の体制について、(2)文書番号体系についてを議論した。具体的な議論の概要は次のとおり。

(1) CRYPTREC の今後の体制(案)について

昨年度に行われた第３回重点課題検討タスクフォースにおいて、本年度の主な課題として以下が挙げられた。

① 文書体系のあり方について
② 政府統一基準に向けた新たな CRYPTREC 成果物
③ 新たな社会ニーズを見据えた新規活動
④ 情報システム全体のセキュリティ確保を意識した他団体との連携
⑤ その他

①についての詳細は「（２）文書番号体系（案）について」に記載するが、本年度タスクフォースにおいて議論を行い、結果について暗号技術検討会にて審議を受けることとした。

②、③については、政府統一基準等から参照されやすい文書の作成やプライバシー保護のような社会ニーズを見据えた検討等の新たな取り組みについて、今後どのように議論を進めていくかを NISC との相談を含め、事務局で整理を行い、その内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号活用委員会に議論の場を移して検討を行うこととした。

④については、今後他団体との連携を必要とする対象のタスクが明確になった段階で、タス

クの内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号技術活用委員会に議論の場を移し、具体的な連携方法について検討を行うこととした。

⑤については、CRYPTREC としてどう取り組むか議論が必要なテーマに関する検討であるが、昨年度、例として挙がった ChaCha20 の安全性評価の必要性については、本年度、暗号技術評価委員会にて議論され、安全性評価が実施されている。

以上をもって、重点課題検討タスクフォースのミッションを終了とし、同タスクフォースを廃止することとした。

また、暗号技術検討会については現状の活動状況を踏まえ、年１回開催を基本とし、メールベースの審議や報告などをタイムリーに行う体制を整えることによって、暗号技術検討会のアクティビティが低下しないように活動の効率化を図る。

(2) 文書番号体系（案）について

これまで CRYPTREC においては、年度成果物としてガイドライン、報告書を公開しているが、今後は文書の番号から内容（およびその文書の位置づけ）がわかる文書管理をするため、CRYPTREC 文書について、番号体系を整理することとした。

表 3.1.2　CRYPTREC 文書と想定される対象

CRYPTREC 文書	想定される対象
・総務省、経済産業省によって承認された文書 ・暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会によって承認された文書 ・暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会、及び WG での配付資料	・CRYPTREC 暗号リスト ・CRYPTREC 暗号リストと各暗号アルゴリズム仕様書との対応表 ・CRYPTREC が報告書またはガイドラインとして公開するもの ・CRYPTREC が公表する注意喚起レポート ・外部評価レポート（外部評価者が作成した技術報告書） ・委員会資料（議事録を含む）

それらの体系ルールとして以下のような整理を行った。

＜文書番号＞::=CRYPTREC＜カテゴリ＞－＜連番＞－＜管理情報＞

アップデートあり：(前バージョンはアーカイブ)

・CRYPTREC LS-0001-2016　⇔　2016 年度発行 CRYPTREC 暗号リスト（最新）

・CRYPTREC LS-0001-2012　⇔　2012 年度発行 CRYPTREC 暗号リスト（アーカイブ）

アップデートなし：(アーカイブなし)

・CRYPTREC RP-0001-2015　⇔　2015 年度暗号技術検討会報告書

・CRYPTREC RP-0002-2015　⇔　2015 年度暗号技術評価委員会報告書

【参考】

・　FIPS - XXX - yyy　⇒　米国連邦強制規格

・NIST SP800 - XXX　rev.　⇒　NIST が自ら作ったガイドライン

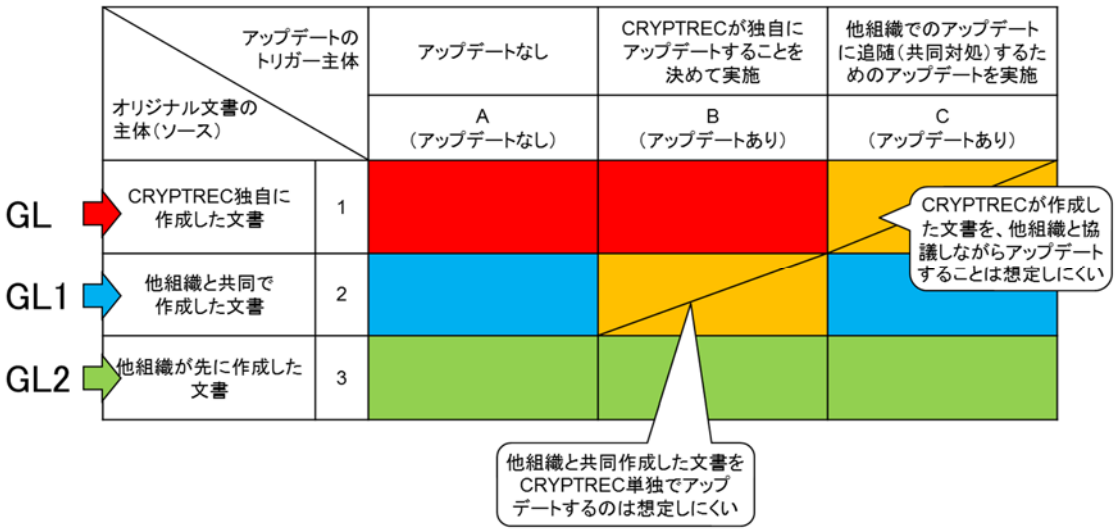
・NIST SP1800 - XXX　⇒　NCCoE プロジェクトで作ったガイドライン

表 3.1.3　カテゴリ表記

CRYPTREC 文書分類	該当する既存の CRYPTREC 文書例	表記名
CRYPTREC 暗号リスト関係	・CRYPTREC 暗号リスト ・CRYPTREC 暗号リストと仕様書の対応関係表	LS
年次報告書	・年次報告書	RP
早期に公開する注意喚起	・注意喚起レポート	ER
ガイドライン	・暗号技術ガイドライン ・暗号運用ガイドライン	GL
技術報告書	・調査 WG 報告書 ・推奨セキュリティパラメータ設定	TR
外部評価報告書	・外部評価者が作成した安全性評価報告書 ・外部評価者が作成した実装性能評価報告書	EX
会議資料	・暗号技術検討会資料 ・各委員会資料	MT

また、「ガイドライン」が主な対象と想定されるが、これらのことを前提として表記名の他、「作成主体」や「アップデートの作業主体」の違いが分かるように識別子を付すことがある。
＜例＞ＧＬ　⇒　ＧＬ，ＧＬ１，ＧＬ２と表記

表 3.1.4　カテゴリ内の識別子表記



また、CTYPTREC 文書の作業主体区分の考え方としては以下のように整理を行った。

表 3.1.5　【オリジナル文書の主体（ソース)】

#	ソース	概要	過去の文書例
1	CRYPTREC が独自に作成した文書	・CRYPTREC が独自に作成した文書 ※WG またはアウトソーシングで実施	全文書
2	他組織と共同で作成する文書	・他組織と共同で作成する文書 ※両組織で発行されることを想定 ※主体は他組織。CRYPTREC はサポート	なし

3	他組織が先に作成した文書	・他組織が作成した文書をベースに、 （できるかぎり少ない変更で） CRYPTREC としての文書を作成 ※最小限の場合、「外部文書の参照関係を示す」だけの文書となることもありうる	なし

表 3.1.6　【アップデートのトリガー主体】

#			過去の文書例
A	アップデートなし	・発行後は原則アップデートしない	年次報告書
B	CRYPTREC が独自にアップデートすることを決めて実施	・CRYPTREC でアップデートを実施 ※WG またはアウトソーシングで実施	CRYPTREC 暗号リスト 解析計算量評価
C	他組織でのアップデートに追随（共同対処）するために CRYPTREC としてもアップデートを実施	他組織と共同、または他組織がアップデートした内容をベースに、CRYPTREC としてのアップデートを実施 ※WG 設置は想定しない	なし

※「アップデート」とは、文書内容の質自体に関わる記述をいずれ改訂することを当初から意図しており、かつそれを実行することを意味する。アップデート後、前バージョンの文書は廃止（アーカイブ）される。「記述内容の正誤修正」、「作成時点で改訂を意図していない文書」は「アップデート」には含まない。

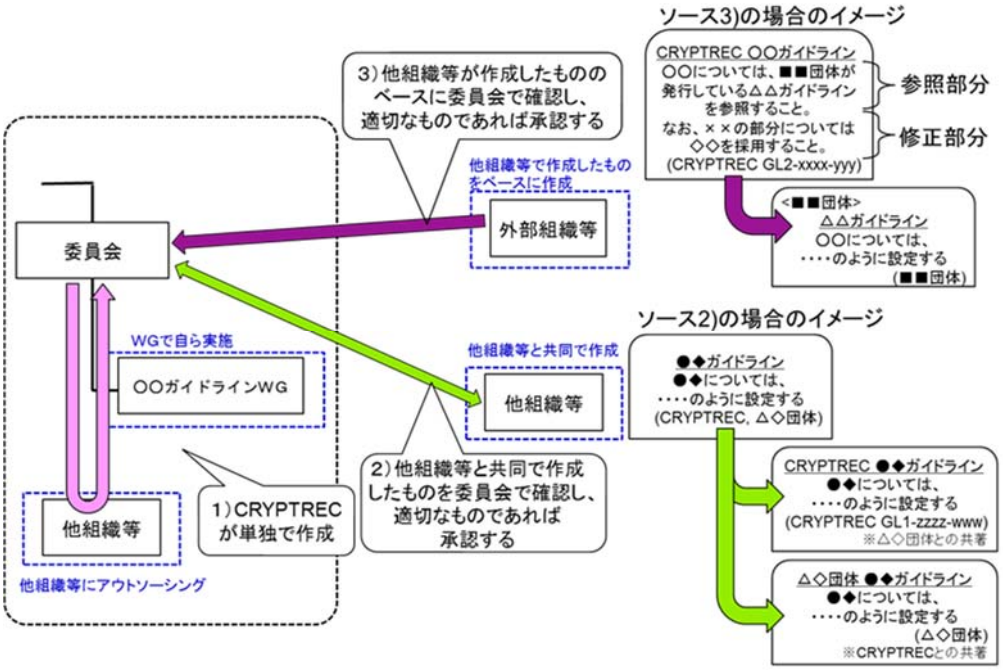


図 3.1.1　「文書の作成主体（＝ソース）の違い」の説明図

３．２．暗号技術評価委員会

３．２．１．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 2016 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。

３．２．２．2016 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

2016 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 ハッシュ関数 SHA-3 に属する SHAKE128 に関して CRYPTREC 暗号リストへの追加のため検討を実施した。

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。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、ハッシュ関数 SHA-3 ファミリーのうち、CRYPTREC 暗号リストに含まれていなかった SHAKE128 について、出力長を 256 ビット以上とするようパラメータを選択すれば、CRYPTREC 暗号リストへ追加するのに十分な安全性と実装性能を有していることが確認できた。

その他、KCipher-2 の仕様書に見つかった誤記について、電子政府推奨暗号リスト選定の際に行われた安全性評価・実装評価に誤記修正による影響はないことを確認した。DH/ECDH の仕様書の参照先について、参照先の仕様書の変更が軽微なものであることを確認した。共通鍵暗号の安全性について調査を行い、MISTY1 の今後の利用について提示すべき推奨方針案について検討を行った。

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

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)の仕様に対して具体的な衝突が初めて発見された。従前通り、移行対策を実施すべきであると考えられる。

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、楕円曲線上の離散対数問題の困難性に関する調査、多重線形写像及び難読化の最新動向等、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、技術レポートとして、CRYPTREC ホームページより公開予定である。暗号技術調査 WG（軽量暗号）では、軽量暗号を選択・利用する際の技術的判断に資すること、今後の利用促進を図ることを目的とした「暗号技術ガイドライン(軽量暗号)」(日本語、英語)を完成させ、CRYPTREC ホーム

ページより公開予定である。また、ChaCha20-Poly1305 の安全性評価を行った。現時点では ChaCha20-Poly1305 は、認証暗号として、具体的な脅威は見つかっていないと考えられる。

３．２．３．暗号技術評価委員会の開催状況

2016 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 3.2.1 のとおりである。

表 3.2.1　暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2016 年 7 月 27 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 今後の課題に関する検討
第 2 回	2017 年 3 月 21 日	WG 今年度活動報告 ハッシュ関数 SHAKE128 の取扱いについての検討 外部評価レポート(ChaCha20-Poly1305 の安全性調査)についての検討 KCipher2 の仕様書の修正に関する検討 SHA-1 に関する注意喚起レポートについて報告 共通鍵暗号の安全性調査に関する検討 CRYPTREC Report 2016 の目次案提示 監視状況報告

３．３．暗号技術活用委員会

３．３．１．活動概要

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

2016 年度は、上記の活動目的を踏まえ、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）を本格的に整備していくことを今後の暗号技術活用委員会（以下、活用委員会）での活動の中心に据えることを視野に、以下の項目について検討を行った。

① 作成すべき運用ガイドラインの対象及び取扱い範囲の切り分けの検討
② 作成した運用ガイドラインのメンテナンス体制の検討
③ 外部組織や業界団体との連携方法の検討
④ 運用ガイドラインの作成
⑤ ベンダや業界団体等の意向をバランスよく取り入れつつ、セキュリティも担保する利用

価値の高い成果物となるようにコントロールする

⑥ その他

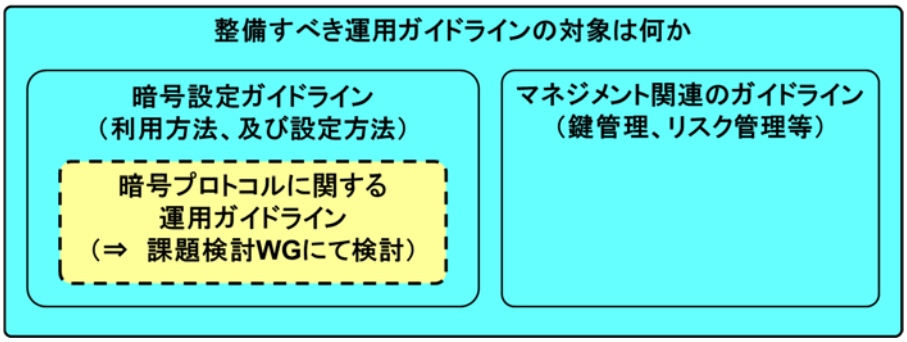
CRYPTREC として暗号プロトコルをどのように扱うかを重点的に検討するため、「暗号プロトコル課題検討 WG（以下、課題検討 WG)」を設置

なお、①については、暗号プロトコルに関わる部分を課題検討 WG で、それ以外の範囲を活用委員会でそれぞれ検討した。また、④と⑤については、実際の運用ガイドラインを作成する際に、テーマに応じて適切な手段を活用委員会で判断して実施していくことになった。

３．３．２．2016 年度の活動内容

運用ガイドラインの対象について

2017 年度以降に活用委員会として運用ガイドラインを作成する価値がある対象を検討するにあたっては、以下の目的と領域に合致する範囲のガイドラインを想定して議論を行った。なお、暗号設定ガイドラインのうち、暗号プロトコルに関する部分については課題検討 WG にて検討を行い、それ以外の部分については活用委員会にて検討を行った。



【暗号プロトコルに関する運用ガイドライン以外の対象】

もともと運用ガイドラインの必要性が高いと考えられている対象を中心に、以下の観点から整理を行い、今後、運用ガイドラインを作成していく際に優先的に取り上げていくことが望ましい対象を取りまとめた。具体的な検討結果は活用委員会報告書を参照されたい。

- 【対象】
  どのような用途で使う運用ガイドラインであるか
- 【目的・内容】
  どのような目的をもった運用ガイドラインを意図したものか
- 【内容】
  運用ガイドラインに記載される内容はどのようなものか
- 【想定読者】
  その運用ガイドラインの想定読者は誰か
- 【必要性】
  なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか

- 【課題】
  ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か
- 【他組織のガイドライン等】
  他組織が同種のガイドラインを作っていないか／作ろうとしていないか
- 【関連組織】
  どのような他組織と連携していくのがよいか

【暗号プロトコルに関する運用ガイドラインの対象】

暗号プロトコルに関する運用ガイドラインの対象を検討するにあたっては、「(STEP1) 検討対象とする暗号プロトコルの列挙」と「(STEP2) 列挙した暗号プロトコルのなかから運用ガイドラインを作る価値がある／必要性が高いと判断したものを抽出」の 2 段階で議論を行った。

運用ガイドラインを作る価値があるか／必要性が高いかを判断するために、以下の観点から整理を行った。その結果、「必要性」「目的・内容」「想定読者」の 3 点について明確に説明できるものを「運用ガイドラインを作る価値がある／必要性が高い」と判断・抽出し、より詳細な検討を加えた。具体的な検討結果は活用委員会報告書を参照されたい。

- 【必要性】
  運用ガイドラインを作る価値／必要性を明確に示すことができるか（なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか）
- 【目的・内容】
  どのような目的・内容をもった運用ガイドラインを意図したものかを明確に示すことができるか
- 【想定読者】
  その運用ガイドラインの想定読者を具体的に示すことができるか
- 【課題】
  ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か
- 【他組織のガイドライン等】
  他組織が同種のガイドラインを作っていないか／作ろうとしていないか
- 【関連組織】
  どのような他組織と連携していくのがよいか

<u>運用ガイドラインのアップデート方法に関連する検討</u>

運用ガイドラインは、ガイドライン作成時の標準化状況や製品状況、利用環境や利用実績等を踏まえて、その時点での現実的かつ効果的な推奨設定や推奨基準を提示するものである。このことは、ある程度の時間が経過し、標準化状況や製品状況、利用環境や利用実績等が変化すれば、運用ガイドラインの中身も陳腐化し、ガイドラインとしてふさわしくないものとなることを意味する。

このため、今後運用ガイドラインの整備を進めるにあたっては、単に運用ガイドラインを作るだけでなく、運用ガイドラインの質を維持するためにどのような方法でアップデートを行っていくかを検討しておく必要がある。そこで、活用委員会では、具体的な運用ガイドライン例として「SSL/TLS 暗号設定ガイドライン」を取り上げ、アップデートの在り方の検討を行った。

外部連携について

運用ガイドラインの作成については、CRYPTREC 単独での作成よりも関連する外部組織や業界団体など（以降、他組織等という）との連携を進めたほうがよいとの指摘があった。これらの指摘を踏まえ、来年度より開始する運用ガイドラインの作成にあっては、従来の WG 形式での作成に捕らわれずに柔軟な作成スタイルを考慮する。

1) CRYPTREC が単独で作成
2) 他組織等と共同で作成
3) 他組織等で実施したものをベースに作成

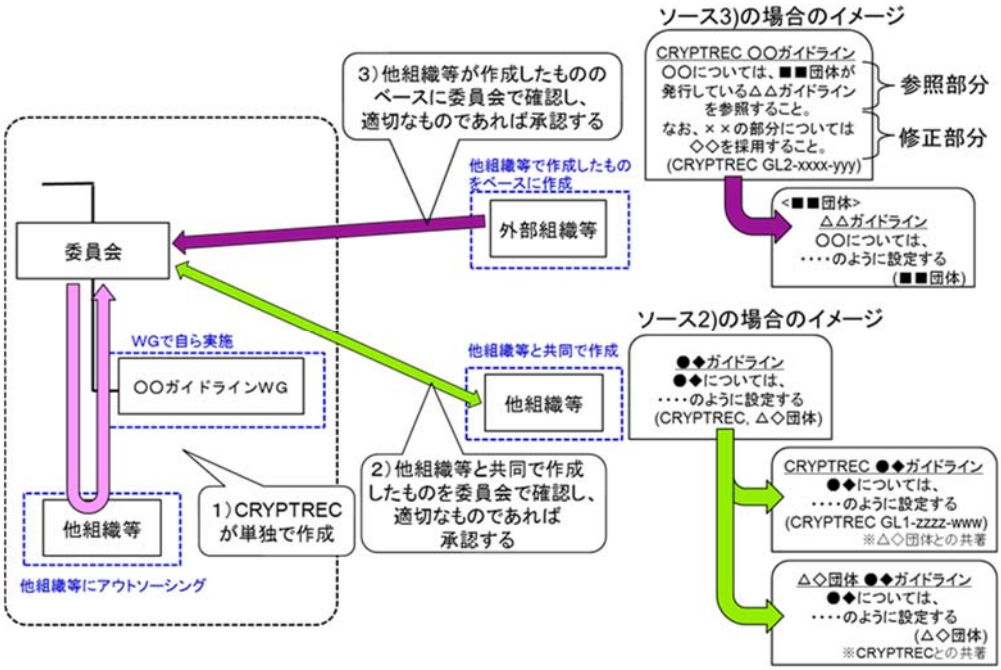


図 3.3.1　作成手段の説明図

実際の運用ガイドラインの作成手段を決定するにあたっては、以下のポイントを重視して判断を行う。

- 他組織等と連携したほうが有用性のある運用ガイドラインが作成できるか
- 連携先の外部組織等が信頼できる組織・団体であるか
- 他組織等と連携することによって作業効率を上げることができるか（例えば作業スケジュール等）
- 予算面やリソース面からの考慮

今後に向けて

2017 年度は新たな運用ガイドラインを実際に作成していく方向で活動計画を検討する。具体的な対象の選定等については、2017 年度第一回暗号技術活用委員会にて決定する方向である。

また、SSL/TLS 暗号設定ガイドラインについては、2016 年度活動で出た意見を踏まえ、2017 年度にアップデートを行う計画とする予定である。

３．３．３．暗号技術活用委員会の開催状況

2 回開催された活用委員会での審議概要は表 3.3.1 のとおりである。

表 3.3.1　暗号技術活用委員会　開催状況

回	開催日	議案
第 1 回	2016 年 11 月 9 日	・暗号プロトコル課題検討 WG 活動状況報告 ・運用ガイドライン（「SSL/TLS 暗号設定ガイドライン」）のメンテナンス方法に関する検討 ・運用ガイドラインの対象範囲に関する検討
第 2 回	2017 年 3 月 15 日	・暗号プロトコル課題検討 WG 活動報告 ・暗号プロトコル以外の運用ガイドラインの対象の検討 ・外部連携の進め方の検討 ・2016 年度暗号技術活用委員会報告書

3 回開催された課題検討 WG での審議概要は表 2 のとおりである。

表 3.3.2　暗号プロトコル課題検討 WG　開催状況

回	開催日	議案
第 1 回	2016 年 10 月 27 日	WG 活動概要の説明、課題についての自由討議
第 2 回	2016 年 12 月 26 日	第 1 回 WG での討議を踏まえた課題の整理と更なる検討
第 3 回	2017 年 2 月 10 日	報告書案の取りまとめ

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、SSL/TLS 等の暗号を用いたプロトコルの安全な利用環境の確保のための取組など、暗号をとりま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、本年度 ChaCha20 の安全性評価を実施しているが、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・評価を行い、暗号技術活用委員会においては、本年度の検討を受けて新たな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。

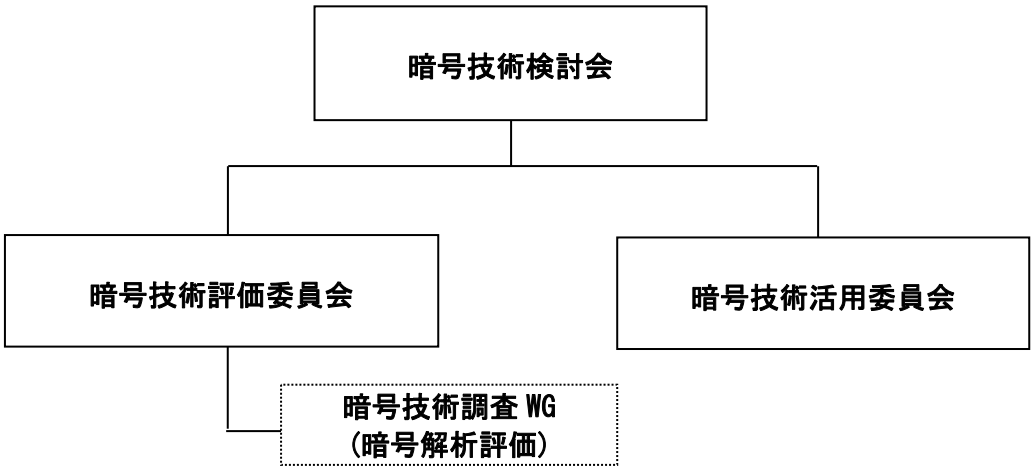


図 4.1.1　2017 年度 CRYPTREC の体制図（予定）