暗号技術検討会
２０１５年度　報告書

２０１６年３月

目　　次

１．はじめに

IoT 社会の到来により、あらゆるモノがネットワークに繋がり、大量のセンサーからデータが集められ、それらを活用して、新たな価値や行動が創造されていくこととなる。こうした新しい情報社会の中で、日々高度化・複雑化するサイバー攻撃に対処して、情報システム全体の信頼性を確保していくことが必要となっている。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。2014 年 11 月に制定された「サイバーセキュリティ基本法」に基づき、2015 年 9 月 4 日に閣議決定された「サイバーセキュリティ戦略」においても、サイバーセキュリティのコア技術の１つとして、安全保障の観点等から国が維持すべき技術に暗号技術が挙げられているなど、国の戦略レベルにおいても暗号技術は重要な位置付けとなっている。

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（安全性）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（安全性）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。

2015 年度、CRYPTREC では、このような社会情勢の変化を踏まえた柔軟な活動を図るべく、暗号技術検討会の下に「CRYPTREC の在り方に関する検討グループ（以下「検討グループ」という。)」を新たに設置し、4 回の集中的な議論により、CRYPTREC で対象とする暗号技術や活動範囲、安全性確保に係る活動の在り方等の見直しを行った。検討グループでこれらを見直した結果、暗号プロトコルの信頼性確保のための取組みや利用者ニーズを踏まえた対策等をこれまでの活動目的に追加し、その実現のために関連団体との連携や新たな社会ニーズを踏まえた対応を検討していくことを決定した。加えて「重点課題検討タスクフォース」を設置し、CRYPTREC の活動の方向性について、トップダウン的な意志決定ができる体制を構築した。

2015 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、新しい暗号技術に係る調査、標準化動向を鑑み電子政府システム等での利用が見込まれると判断される暗号技術の追加の検討等を行った。暗号技術活用委員会では、作成すべき運用ガイドライン対象及び運用ガイドラインのメンテナンスに係る検討等を行った。これらの 2015 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 2015」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情報社会システム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。

2016 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。

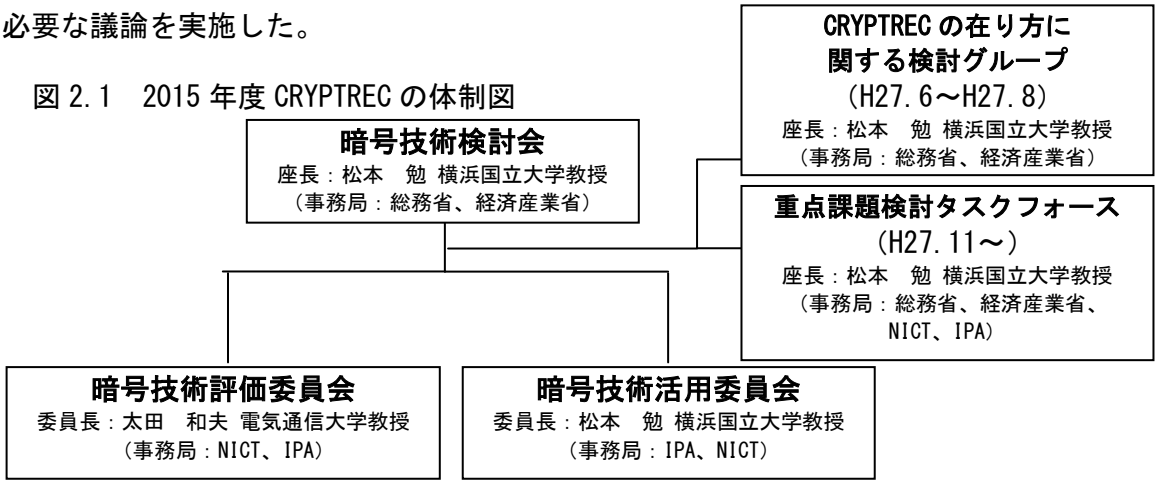
２．２． CRYPTREC の体制

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。

2015 年度の CRYPTREC においては、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、柔軟な活動を図るため、CRYPTREC で対象とする暗号技術の見直しや、活動範囲、また安全性確保等にかかる活動の在り方の見直しを議論するため、暗号技術検討会の下に、「CRYPTREC の在り方に関する検討グループ」（H27.6～H27.8）を設置・議論するとともに、当該検討グループでの議論を継続的に行うため、「CRYPTREC 重点課題検討タスクフォース」（H27.11～）を暗号技術検討会の直下に設置し、議論を行った。

また、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を設置した。暗号技術評価委員会においては継続して必要となる調査・検討を行うとともに、暗号技術活用委員会においては、CRYPTREC 重点課題検討タスクフォースによる審議結果を踏まえ、必要な議論を実施した。

図 2.1　2015 年度 CRYPTREC の体制図



２．３．暗号技術検討会の開催状況

2015 年度の暗号技術検討会は、CRYPTREC のタスク見直しに関する議論、暗号技術評価委員会、暗号技術活用委員会の活動報告、CRYPTREC 推奨候補暗号リストの変更等を審議するために２回開催した。

【第 1 回】2015 年 10 月 5 日（月）10:00～12:00

（主な議題）

- CRYPTREC の在り方に関する検討グループにおける議論結果について
- 重点課題検討タスクフォースの設置について
- 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）

- 「CRYPTREC の在り方に関する検討グループにおける議論結果について」において、暗号プロトコルの信頼性確保の取組や利用者ニーズを踏まえた対策等を目的に追加すること、その実現のための関係団体との連携、新たな社会ニーズを踏まえた対応を検討していくことを決定した。

  これに対して、ユーザーが必要な情報を提供することの必要性はあり、ヒアリング等を行いつつ進めていくべき等のコメントがあった。
- 「重点課題検討タスクフォースの設置について」の審議において、CRYPTREC の在り方に関する検討グループでの議論を継続的に実施するため、「重点課題検討タスクフォース」を設置することを説明した。

  これに対して、既存の暗号プロトコルの普及戦略についても検討に含めてもらいたい等のコメントがあった。
- 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 2015 年度の活動計画案の報告を行った。

【第 2 回】2016 年 3 月 29 日（火）16:30～18:30

（主な議題）

- 2015 年度暗号技術検討会報告書（案）について
- 重点課題検討タスクフォース活動報告について
- 2015 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（推奨候補暗号リスト）への新規追加について
- 2016 年度の暗号技術評価委員会、暗号技術活用委員会の活動計画について

（概要）

- 2015 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追記し、最終確認を行うことで承認を得た。
- 重点課題検討タスクフォースの 2015 年度の活動概要（(1) CRYPTREC 暗号技術活用委員会の今後の活動に向けて、(2) 暗号アルゴリズムの脆弱性に関する情報発信フローについて、(3) 暗号プロトコルのセキュリティ確保に向けた活動について）について報告を行った。
- 暗号技術評価委員会及び暗号技術活用委員会の 2015 年度の活動概要について報告を行った。
- 2015 年度までに暗号技術評価委員会にて安全性評価及び実装性能評価を実施してきたハッ

シュ関数 SHA-512/256、SHA3-256、SHA3-384、SHA3-512、SHAKE256（ハッシュ長は 256 ビット以上に限定）を CRYPTREC 暗号リスト（推奨候補暗号リスト）に追加することの承認を得た。

- 2016 年度の暗号技術評価委員会の活動計画について CRYPTREC 事務局より説明が行われ、原案のとおり承認された。なお、これに対し、SHA-1 の衝突事例が発見された場合の対応や暗号アルゴリズムの脆弱性に関する情報発信の際の NISC との連携についても検討してもらいたい等のコメントがあった。
- 2016 年度暗号技術活用委員会の活動計画について CRYPTREC 事務局より説明が行われ、原案のとおり承認された。なお、これに対し、既存ガイドラインのアップデートも暗号技術活用委員会の活動とすることを検討して欲しい等のコメントがあった。

２．４．CRYPTREC 暗号リストの改定

［背景］

・SHA-2

FIPS 180-4 で規定されているハッシュ関数 SHA-2 のうち、SHA-256,SHA-384,SHA-512 のみが電子政府推奨暗号リストに掲載されていた。

表 2.1　FIPS180-4 で規定されている SHA-2

Algorithm	Message Size (bits)	Block Size (bits)	Word Size (bits)	Message Digest Size(bits)
SHA-224	$<2^{64}$	512	32	224
SHA-256	$<2^{64}$	512	32	256
SHA-384	$<2^{128}$	1024	64	384
SHA-512	$<2^{128}$	1024	64	512
SHA-512/224	$<2^{128}$	1024	64	224
SHA-512/256	$<2^{128}$	1024	64	256

・SHA-3

SHA-1、SHA-2 の安全性への懸念から、米国 NIST が SHA-3 のコンペティションを開催し、Keccak 方式が選ばれ、2015 年８月に FIPS202 として SHA-3 が正式に出版された。

上記の背景により、暗号技術評価委員会にて、SHA-2 のうち電子政府推奨暗号リストから外れていたアルゴリズム及び SHA-3 に関する安全性評価を実施し、審議を行った結果、SHA-2 および SHA-3 に含まれるアルゴリズム（ハッシュ長が 256 ビット以上のアルゴリズムとする）は、適切な安全性・実装性能を有しているという結果が得られた。

上記を踏まえ、本検討会にて、暗号技術評価委員会事務局よりリスト改定について説明が行われ、原案の通り、ハッシュ関数 SHA-512/256、SHA3-256、SHA3-384、SHA3-512、SHAKE256（ハッシュ長は 256 ビット以上とする）を CRYPTREC 暗号リスト（推奨候補暗号リスト）に追加することが承認された。

改定された CRYPTREC 暗号リストについては、以下 CRYPTREC ホームページに掲載。

・CRYPTREC 暗号リスト（平成 28 年 3 月 29 日版）

http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf

３．各委員会の活動報告

３．１．CRYPTREC の在り方に関する検討グループ

３．１．１．設置の経緯

2001 年に CRYPTREC が発足した当初の目的は、安全でない暗号アルゴリズムが乱立する中で、電子政府において利用が推奨される安全な暗号アルゴリズムを確定させることであり、活動成果として 2003 年に「電子政府推奨暗号リスト」を策定した。

その後、CRYPTREC は、その発足の趣旨に鑑み、電子政府推奨暗号リスト掲載の暗号アルゴリズムについて安全性低下などの問題（暗号危殆化）の監視、注意喚起等を実施など、安心な暗号利用について貢献してきた。一方で、国際標準規格の策定などの要因により、国際的に利用できるデファクト暗号アルゴリズムへの集約が進み、安全でない暗号アルゴリズムが混在するという懸念は激減した。このような外部環境の変化を踏まえ、市場性や利用状況等を加味して評価した結果 2012 年度末に「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（以下「リスト改定」という。）した。

また、リスト改定後は、従来からの「CRYPTREC 暗号リストの安全性維持に係る取組」に加え、「新しい暗号技術の調査」、「暗号技術の普及促進に係る取組」、「中長期的視点に立った暗号政策に係る検討」等を行ってきた。

上記活動を通じて、暗号技術を取り巻く環境、サイバーセキュリティ基本法の施行といった社会情勢の変化等に鑑み、CRYPTREC が果たすべき役割は、CRYPTREC 暗号リストの策定及び維持に限られるものではなく、より柔軟に活動することが望ましいといった意見があった。

このため、今後、社会ニーズ等を踏まえた柔軟な活動を図るべく、CRYPTREC で対象とする暗号技術の見直しや、活動範囲、また安全性確保等にかかる活動の在り方（緊急時対応、必要な体制の見直し）等の議論を行うことが望ましいと考えられ、暗号技術検討会に「CYPTREC の在り方に関する検討グループ」（以下「検討グループ」という。）を設置し、議論を行った。

３．１．２．CRYPTREC の在り方に関する検討グループの開催実績

検討グループは、表 3.1 のとおり、計 4 回開催した。各会合の開催日及び主な議題は表 3.1 のとおり。

表 3.1　CRYPTREC の在り方に関する検討グループの開催

回	年月日	議題
第１回	2015 年 6 月 3 日	(1)「CRYPTREC の在り方に関する検討グループ」開催要綱について (2)CRYPTREC に関する現状について
第２回	2015 年 6 月 24 日	(1)前回議事確認と本日の議論の進め方について (2)CRYPTREC に関する問題意識 (3)暗号プロトコル評価技術コンソーシアム(CELLOS)の概要 (4)サービス視点からの暗号技術(の重要性) (5)全体を通しての意見交換
第３回	2015 年 7 月 3 日	(1)前回議事確認と本日の議論の進め方について (2)CRYPTREC で取り組む新しい暗号技術 (3)これからの CRYPTREC について (4)第１回、第２回の発言ポイントまとめ (5)全体を通しての意見交換
第４回	2015 年 8 月 3 日	(1)前々回の議事確認と本日の議論の進め方について (2)CRYPTREC の在り方に関する検討グループまとめ案 (3)全体を通しての意見交換

３．１．３．議論概要

① 全体俯瞰図に関する議論

CRYPTREC が担うべきタスクに関する議論にあたって、以下の論点を踏まえた検討が必要との方針がまず示された。

・目的：従来のミッションから変更すべきか、何を追加すべきか。
・対象とする活動領域：暗号アルゴリズム等従来に加えて何を対象とするか。
・主な適用範囲：電子政府に加えて一般向けの情報システムも対象とするか。
・成果物：CRYPTREC 暗号リストに加え、どのような成果物が考えられるか。

ただし議論の過程において、「情報システムにおける暗号技術のセキュリティ確保の全体俯瞰図を共通認識として持ち、それを踏まえた上で議論をすべき」との意見が多くの構成員より提出された為、以下の観点から全体俯瞰図を整理した。

- 情報システムにおける暗号技術のセキュリティは開発及び運用段階で分けて考える必要がある。
- さらにそれぞれを「仕様と実装」、「規程とその規程の実運用」とに分けて考えた方が良い。
- その上で様々な暗号プリミティブ、プロトコル、製品から情報システム全体といったレイヤ別に確認が必要。

上記を踏まえて図 3.1 を作成した。

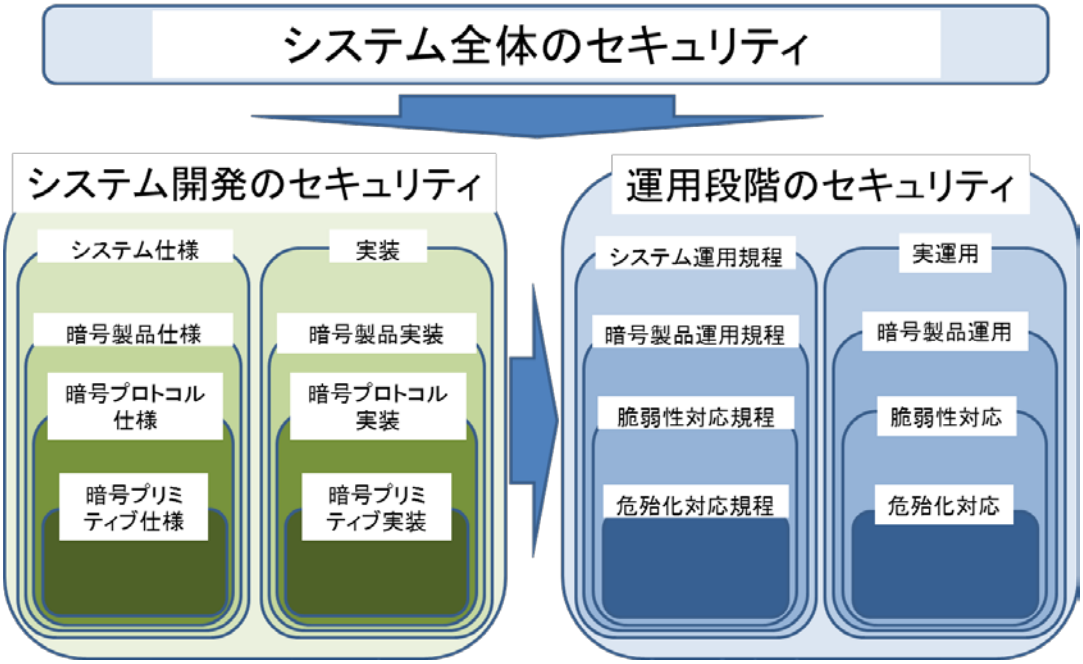
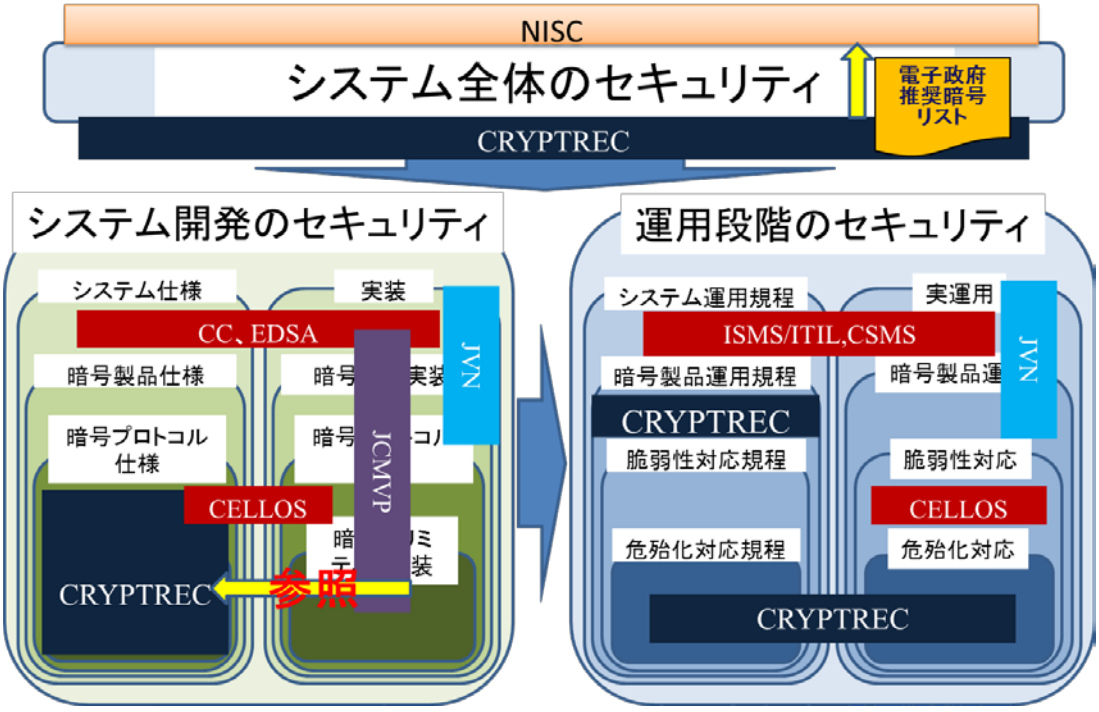


図 3.1　システムにおける暗号技術のセキュリティ確保の全体俯瞰図

さらにこの俯瞰図を踏まえた上で、現状の「政府」情報システムにおける暗号技術のセキュリティ確保する既存の各活動と各役割の整理を図 3.2 のとおり行った。



※CC(Common Criteria):IT 製品のセキュリティ認証制度　CELLOS（Cryptographic protocol Evaluation toward Long-Lived Outstanding Security(CELLOS) Consortium）：暗号プロトコル評価技術コンソーシアム　CSMS(Cyber Security Management System):制御システムに関するセキュリティマネジメントシステム　EDSA(Embedded Device Security Assurance):制御機器（組込み機器）のセキュリティ保証に関する認証制度　ITIL(Information Technology Infrastructure Library):IT サービスマネジメントのベストプラクティスをまとめたフレームワーク　JCMVP(Japan Cryptographic Module Validation Program):暗号モジュール試験及び認証制度　JVN(Japan Vulnerability Notes):ソフトウェアなどの脆弱性対策情報ポータルサイト

図 3.2　「政府」システムにおける暗号技術のセキュリティ確保の各役割（現状）

その結果、以下のような CRYPTREC の現状の位置付けと、関連する活動の状況が整理された。

- CRYPTREC は主に、情報システム開発の暗号プリミティブへの対応を主眼におき、暗号プロトコルの仕様まで対象に含めて対応してきた。
- 運用に関しても、CRYPTREC は危殆化監視活動の他、一部製品レベルに踏み込んだ運用規程（SSL/TLS 暗号設定ガイドライン等）を提供している。
- CRYPTREC が主に対象としている以外の領域にも、基本的にはセキュリティの担保をするための認証制度や情報提供機能等の仕組みがある。

上記の全体俯瞰状況を踏まえた上で、各項目について議論を行った。

② CRYPTREC のミッション（目的）に関する議論結果概要

CRYPTREC ミッションに関わる事項についても多くの議論がなされた。
現行のミッションは「CRYPTREC 暗号の安全性及び信頼性確保のための調査・検討、CRYPTREC 暗号リストの改定に関する調査・検討に加え、暗号技術の普及による情報セキュリティ対策の推進検討」となっているが、それらに対して各種意見が出され、以下の課題が整理された。

- 暗号アルゴリズムより上のレベルであるプロトコルや製品、また実装・実運用に関する活動に関して、CRYPTREC としてどのようなミッションを持つか。
- CRYPTREC で行う 「暗号技術の普及による情報セキュリティ対策の推進検討」を今後どうするか。
- プライバシー保護や IoT 社会など社会ニーズを見据えた暗号技術への取組や提言機能をミッションとして加えるか。

上記の課題に対して、以下のような検討の指針が示された。

- 活動領域の詳細議論にて、情報システム全体のセキュリティ確保に最適な CRYPTREC 活動の在り方について検討。
- 今後、CRYPTREC で行うべき「普及促進」の明確化が必要。
- 新たな社会ニーズの把握と、必要な提言機能のミッション追加を検討する。

これらを踏まえて、新たなミッションに関する案が示された。
「CRYPTREC 暗号（※１）のセキュリティ及び信頼性確保のための調査（※２）・検討、CRYPTREC 暗号リストの改定に関する調査・検討に加え、関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討（※３）や提言」

（※１）暗号プロトコルを含む。
（※２）監視活動を含む。
（※３）一般利用者からのニーズの検討も含む。

ただしミッションについては、その他の各種議論を踏まえた上で最終的には見直すものであり、継続的な議論が必要との結論となっている。

③ CRYPTREC が対象とする活動領域に関する議論結果概要

対象とする活動領域の検討について、既存の他団体の活動（プロトコルのセキュリティ評価（CELLOS)、製品（ソフトウェア）の脆弱性（JVN）等）との関係を考慮した上で各種議論がなされ、以下のような課題が整理された。

- CRYPTREC の網羅性
- 暗号プロトコル評価に関する CELLOS との役割分担
- その他既存の他団体と連携

上記の課題に対して、それぞれ以下のような議論がなされた。

- CRYPTREC の網羅性に関しては、既に CRYPTREC で活動している領域でも、活動の網羅性（政府調達から参照されるべき成果物を揃えることができるか、という観点）から再検討されるべき、という観点で多くの議論がなされた。例えば暗号プロトコル及び運用面（鍵管理等）での活動を再検討することが必要といった意見がみられた。
- 暗号プロトコルでの評価活動を検討するにあたっては、活動目標に応じて、CELLOS との詳細な情報交換を行い、具体的連携方法の議論が必要との認識が示された。
- CRYPTREC の限られたリソースも考慮すると、実装や製品評価といった個別評価の分野や脆弱性対応など迅速性が要求される分野は積極的に他団体との連携を検討することが必要との認識が示された。

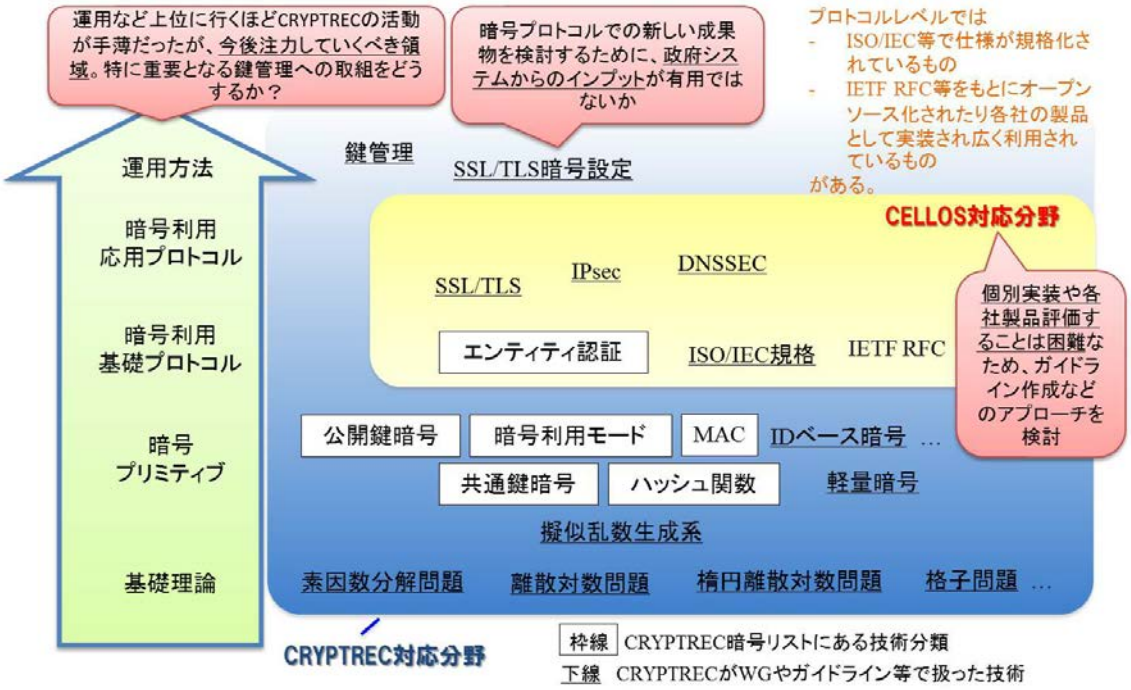


図 3.3　暗号技術マップのイメージ

これらを踏まえて、活動領域に関する以下の案が示された。

・既存の CRYPTREC 活動領域について、以下の観点で見直す。
　-暗号プロトコル仕様のセキュリティ確保対策について、CELLOS との連携を考慮しつつ、引き続き検討する。
　-運用のセキュリティ確保に関連して必要な活動について、引き続き検討する。

・実装や製品評価といった個別評価の分野や脆弱性対応など迅速性が要求される分野について、他団体との具体的連携を引き続き検討する。
　-CELLOS との脆弱性対応での連携における具体的フロー検討
　-その他の団体との連携に関する必要性やその具体的フロー検討

④　CRYPTREC の成果物の主な適用範囲に関する議論結果概要

主な適用範囲については、ビジネスの現状や今後の IoT 社会の到来などの変化も踏まえて、技術的な安全性は前提としながらも、厳密性と運用上の制約とのバランスを考慮しながら、CRYPTREC 活動が主に対象とする領域をどう考えるべきか議論が行われた。

まず電子政府情報システムから一般情報システムへと領域拡大を検討すべきかが議論されたが、その差異をあまり意識する必要はないとの結論となった（電子政府情報システム向けの成果物でも利用しやすいものであれば一般情報システムでも利用可能）。

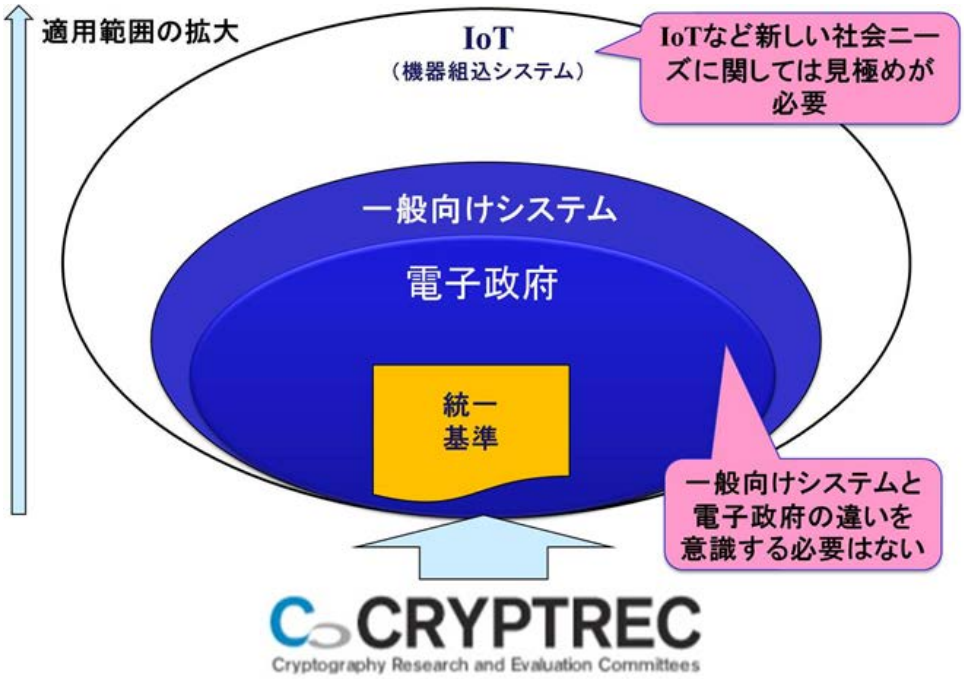


図 3.4　CRYPTREC 成果の適用範囲のイメージ

ただし、IoT やプライバシーなど新しい社会ニーズに関しては見極めが必要との意見が多く出され、以下の課題が整理された。

- IoT 社会を見据えた暗号技術への取組
- 社会ニーズを見据えた調査・検討と提言機能

これらに対して、以下の様な解決に向けた方針が示された。

- IoT 社会で重要になる軽量暗号等について、CRYPTREC として更なるアプローチが可能か、検討が必要。
- 暗号技術が社会において活用されるために必要な制度・ガイドラインについて検討し、各種制度や法律も視野に入れた議論が出来る体制が必要。

これらを踏まえて、成果物の主な適用範囲に関する以下の案が示された。

- 軽量暗号に関する更なる活動強化を引き続き議論
- 新たな社会ニーズを調査・検討する体制を検討

⑤　CRYPTREC の成果物に関する議論結果概要

成果物として、まずは電子政府向けでも現状の暗号リスト以外に柱となるべきものの検討が必要との観点から、以下の課題を挙げた。

- 「情報システム全体における暗号技術のセキュリティ確保」の為に必要なコンテンツ（成果物）の整理

特に CRYPTREC の本来の活動領域である政府調達情報システムにおいて上記課題を解決するために、CRYPTREC がどのような活動を行うべきかが議論された。その結果、既存ガイドライン類を改善し、より政府統一基準等から参照しやすいものとすべき、との意見が提出された。具体的には、成果物ごとの目的の明確化とそれに合わせた内容作成・更新とその情報発信が必要との認識であり、例えば以下のような改善案が示された。

・附番し、より短いサイクルでの再評価・改訂
・改訂時には積極的に分割して小さな単位で参照できるようにする

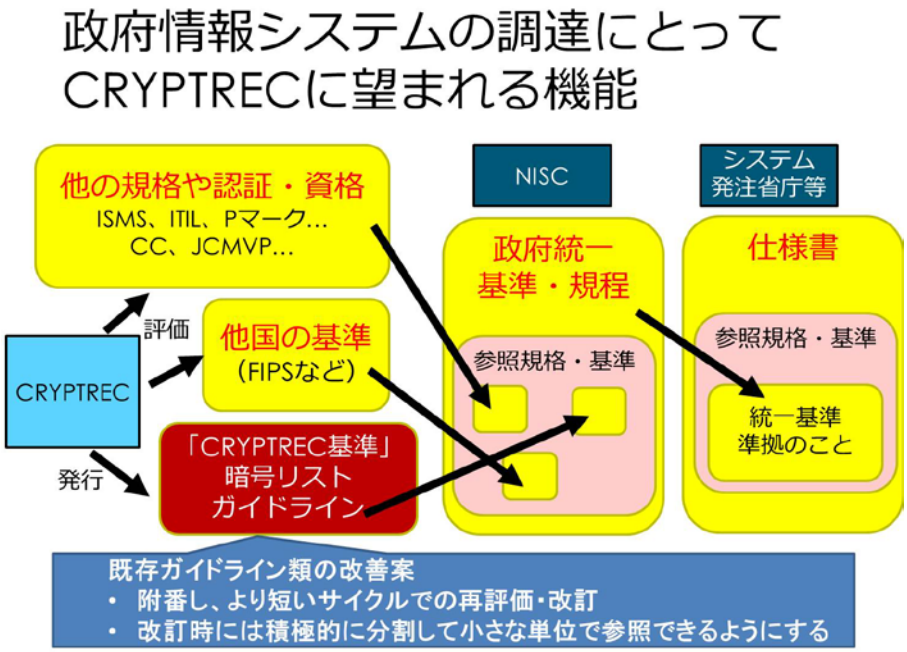


図 3.5　政府調達と CRYPTREC 成果物のあるべき関係性イメージ

これらを踏まえて、成果物に関する検討に対して、以下の案が示された。

- 政府調達に向け統一基準から参照可能な成果物体系の議論を引き続き継続
  -NIST との比較分析を含む
- 適切な情報発信の在り方について引き続き検討
  -他団体との連携方法

３．２．重点課題検討タスクフォース

３．２．１．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志決定もできる体制を構築することとした。

３．２．２．重点課題検討タスクフォースの開催実績

2015 年度、重点課題タスクフォースは計 3 回開催した。各回会合の概要は表 3.2 のとおり。

表 3.2　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 1 回	2015 年 11 月 20 日	「重点課題検討タスクフォース」開催要綱 重点課題検討タスクフォースの設置 ハッシュ関数 SHA-2, SHA-3 の取扱い CRYPTREC 活動方針についての論点
第 2 回	2015 年 12 月 21 日	CRYPTREC 暗号技術活用委員会の今後の活動 暗号アルゴリズムの脆弱性に関する情報発信フロー 暗号プロトコルのセキュリティ確保に向けた活動
第 3 回	2016 年 2 月 3 日	暗号アルゴリズムの脆弱性に関する情報発信フロー 暗号プロトコルのセキュリティ確保に向けた活動 来年度以降の検討課題

３．２．３．2015 年度の議論概要

2015 年度、重点課題検討タスクフォースを計 3 回開催した。タスクフォースでの審議事項は、主に(1) CRYPTREC 暗号技術活用委員会の今後の活動に向けて、(2) 暗号アルゴリズムの脆弱性に関する情報発信フローについて、(3) 暗号プロトコルのセキュリティ確保に向けた活動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 暗号技術活用委員会の今後の活動に向けて

暗号技術活用委員会では、暗号技術における国際競争力の向上及び運用面でのセキュリティ向上等を目的とした活動を行っているが、これらは判断基準や評価軸がいろいろ考えられ、様々な視点・論点から議論する必要があるテーマである。このようなテーマでは、有識者の知見などに基づく、暗号技術活用委員会としての「主体的な評価・判断」が実質的な議

論のベースになる。

一方、今までの CRYPTREC では、CRYPTREC 暗号リスト作成に代表されるように、あらかじめ「コンセンサスが得られた基準をもとにした中立性・公平性」を基本の評価軸として暗号アルゴリズムに関する議論を行ってきた。

このため、暗号技術活用委員会で取り扱うテーマを従来と同じ考え方で議論をすることが難しくなってきており、最初に暗号技術活用委員会での具体的な活動の前提となる運営方針の見直しの必要性について議論した。

議論の結果、客観的なセキュリティ評価という基準は残しつつ、暗号技術活用委員会の主体的な基準での判断ができるように「中立性・客観性の意味合いを広げた」従来とは異なる運営方針を採用し、その方針を基に「セキュリティ向上に役立つ暗号の取り扱いに関わるドキュメント類の作成」まで活動対象範囲を拡大することを決定した。

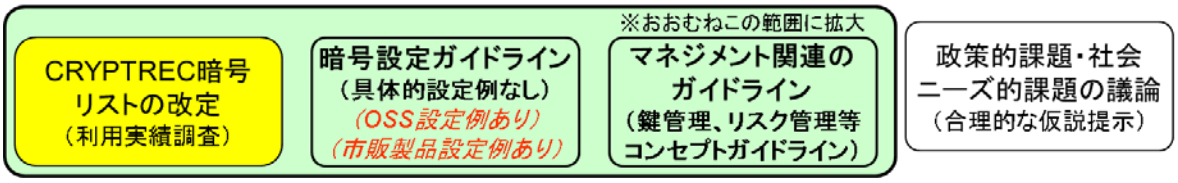


図 3.6　暗号技術活用委員会における活動対象範囲

新しい運営方針を基づき、2015 年度以降の暗号技術活用委員会での活動内容の方向性が以下のように決められた。

- 暗号技術活用委員会が作成すべき暗号の取り扱いに関わる運用ガイドライン対象の検討
- 作成された運用ガイドライン（「SSL/TLS 暗号設定ガイドライン」をモデルケース）のメンテナンス方法の検討
- 他組織との連携体制（例：NCCoE のようなもの）の検討

なお、従来の CRYPTREC とは異なる運営方針で作成されたドキュメント類については、作成にあたった運営方針の違いが分かるように整理したうえで公開すべきであるとの意見が出され、適切な文書体系の在り方について、引き続き、重点課題検討タスクフォースで検討することとなった。

(2) 暗号アルゴリズムの脆弱性に関する情報発信フローについて

暗号アルゴリズムの脆弱性に関する CRYPTREC からの情報発信について議論し、以下に示す内容にて取り扱うこととした。

暗号アルゴリズムの脆弱性情報を検知した後、 CRYPTREC において参照している仕様に対する攻撃成功に関する情報か、もしくは攻撃成功までは到達していないが攻撃に必要となる計算量の著しい低下につながる結果であるか否かについて判断をし、以下のいずれに属する情報であるかを分類する。

A: 暗号アルゴリズムの完全な危殆化による緊急対応

B: 正確で信頼性の高い情報を発信することによる過剰反応防止

C: 長期的なシステムの安全性維持のための対策喚起
D: 対応不要

上記分類のうち、A もしくは B に分類される脆弱性情報については、速報を公開し、また、安全性評価を実施し、その評価結果を公開する。C に分類される脆弱性情報については、必要に応じて C に分類された情報であることの公表や安全性評価を実施する。ここで、速報とは、外部で公開されている情報に基づき記載するもので、CRYPTREC では自ら詳細評価は行っていないが、信頼に足る機関・組織等から得た情報に基づくものとする。安全性評価報告は、CRYPTREC として安全性評価を実施しその評価結果をまとめたものとする。

取り扱う暗号アルゴリズムの範囲は、CRYPTREC 暗号リストに掲載されている暗号技術、および CRYPTREC 暗号リストに掲載されていないが、影響度が高いと暗号技術評価委員会で認められた暗号技術を対象とする。

速報および安全性評価結果は暗号技術評価委員会の審議に基づき公開される。また、これら脆弱性情報は、暗号技術評価委員会から暗号技術検討会に報告される。

具体的な情報発信フローを図 3.7 に示す。

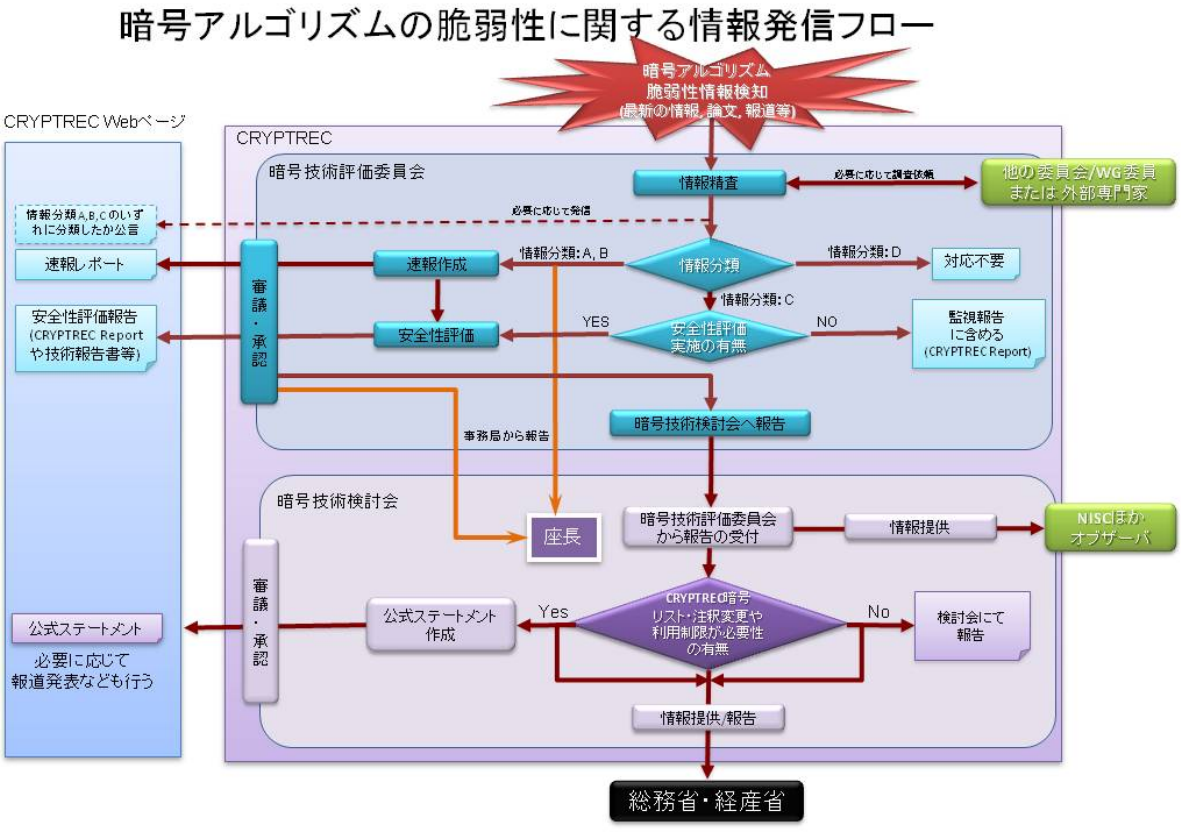


図 3.7　暗号アルゴリズムの脆弱性に関する情報発信フロー

(3) 暗号プロトコルのセキュリティ確保に向けた活動について

CRYPTREC に求められる暗号プロトコル関連の活動として、以下の三点について議論した。

① 暗号プロトコルの脆弱性情報の集約・情報発信

② 暗号プロトコルの安全性評価

③ 暗号プロトコルの利用促進

暗号プロトコルの脆弱性情報の集約・情報発信については、情報収集・発信情報のレベル、情報発信方法（速報性の重視度合い等）、体制等について議論を行った結果、CRYPTREC に求められることは、速報よりも詳細な評価であるとの意見を多く得た。

その観点から、CRYPTREC として暗号プロトコルの詳細評価を実施するにあたっては、実施体制、詳細評価・情報発信していく対象、評価プロセスなどについて、各種課題があることが整理された。

同様に、暗号プロトコルの安全性評価及び利用促進に向けても、特に何を対象とするかの詳細な議論が必要であることが言及され、それらの課題を来年度以降に検討するために、以下のような体制で各委員会での検討を開始されることが提案された。

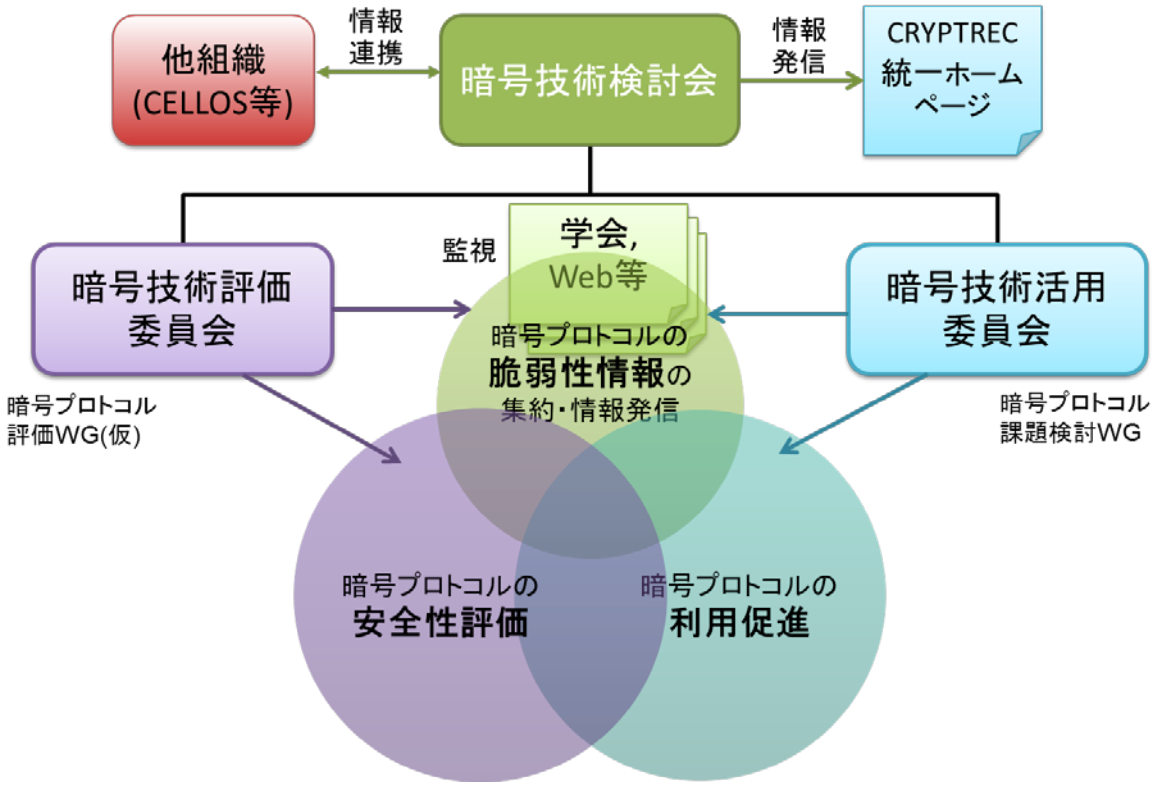


図 3.8　暗号プロトコルに関する CRYPTREC 体制案

各委員会での具体的な活動案については、以下が示された。

＜暗号技術評価委員会での活動案概要＞

・2016 年度

－暗号プロトコルの安全性評価について他組織と連携について意見交換を行いつつ具体的な方針を事務局で検討開始

・2017 年度

－上記方針により安全性評価を開始

－実施方法は WG 立ち上げ、または有識者等への外部評価依頼を想定

－アウトプットイメージ

－Web からの情報発信、ガイドライン作成など

＜暗号技術活用委員会の活動概要＞

・2016 年度

－暗号プロトコル課題検討 WG を立ちあげ、CRYPTREC として扱うべき暗号プロトコルの対象範囲を集中して検討

－運用ガイドラインの作成を前提とした安全性情報や脆弱性情報の取扱方法、他組織との連携方法等の課題整理

－2017 年度以降の暗号プロトコルに関する活動方針案の整理・検討

・2017 年度

－（必要に応じて）暗号プロトコルに関連する運用ガイドライン WG の立ちあげ

等

３．３．暗号技術評価委員会

３．３．１．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 2015 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。

３．３．２．2015 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

2015 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 等のハッシュ関数に関して CRYPTREC 暗号リストへの追加のため検討等を実施した。

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、ハッシュ関数 SHA-2 ファミリーのうち、CRYPTREC 暗号リストに含まれていなかった SHA-512/256、及び、ハッシュ関数 SHA-3 ファミリーのうち、SHA3-256、SHA3-384、SHA3-512、SHAKE256（ハッシュ長は 256 ビット以上とする）を CRYPTREC 暗号リストへ追加する事務局選出のハッシュ関数とした。

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

64 ビットブロック暗号 MISTY1 及びハッシュ関数 SHA-1 に対する解析結果に進展が見られたことから、注意喚起レポートを CRYPTREC のホームページ[1]において公表した。MISTY1 については、フルラウンド(全 8 段のうち 8 段すべて)の仕様に対して鍵の全数探索(すべての鍵の総当たり)よりも少ない解読計算量で導出できることが初めて示された。現時点では解読に必要なデータ量が膨大であることから、現実的な脅威には至っていないものと考えられるが、適用された解析手法の今後の研究動向には引き続き注視が必要である。また、SHA-1 については、フルラウンド(全 80 ステップのうち 80 ステップすべて)の仕様に対して緩い条件ながら衝突が初めて発見された。近い将来に SHA-1 の衝突が発見されるという予測を裏付けるものなので、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た。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)」を作成する等の CRYPTREC 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。

３．３．３．暗号技術評価委員会の開催状況

2015 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 3.3 のとおりである。

表 3.3　暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2015 年 11 月 18 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 MISTY1 及び SHA-1 に関する注意喚起レポートに関する検討 ハッシュ関数 SHA-2、SHA-3 の取り扱いに関する検討

[1] http://www.cryptrec.go.jp/

第 2 回	2016 年 3 月 8 日	WG 今年度活動報告 CRYPTREC2015 の目次案に関する検討 暗号アルゴリズムの脆弱性に関する情報発信についての検討 SHA-1 に関する注意喚起レポートについての検討 ハッシュ関数 SHA-2、SHA-3 の取扱いについての検討 外部評価レポート(Integral 攻撃の最新動向と MISTY1 等への適用)についての検討 共通鍵暗号の安全性予測に関する検討 次年度の活動計画に関する検討 監視状況報告

３．４．暗号技術活用委員会

３．４．１．活動の概要

暗号技術活用委員会は、CRYPTREC の在り方に関する検討グループ及び重点課題検討タスクフォースの検討内容に基づき、今後の具体的な活動内容についての検討を行った。

３．４．２．2015 年度の活動内容

CRYPTREC の在り方に関する検討グループ及び重点課題検討タスクフォースでの検討結果に基づき、暗号技術活用委員会での活動方針の軸足を、「暗号技術を主軸とした検討」から「情報システムとしてのセキュリティ確保に寄与する成果物の提供」に移し、新たな活動方針を以下のように定義し直した。

（活動目的）

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、暗号の取り扱いに関する観点から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

2015 年度は、上記の目的に対応するために、2016 年度以降の活動計画案を中心に検討を行った。

活動計画の柱は、「SSL/TLS 暗号設定ガイドライン」が好評であったことを踏まえ、暗号技術活用委員会が扱う範囲を運用面でのガイドライン（運用ガイドライン）作成に本格的に拡大することである。具体的には、作成すべき運用ガイドラインの対象及び取り扱い範囲の切り分け、メンテナンス体制、外部組織や業界団体との連携方法等を検討することとなる。

また、最近はセキュリティプロトコルの脆弱性が問題となるケースが多くなっていることから、CRYPTREC としてセキュリティプロトコルをどのように取り扱うかについて検討するた

めの「暗号プロトコル課題検討 WG」を新たに設置することとした。

３．４．３．暗号技術活用委員会の開催状況

2015 年度、暗号技術活用委員会は 1 回開催した。概要は表 3.4 のとおりである。

表 3.4　暗号技術活用委員会の開催

回	開催日	議案
第 1 回	2016 年 3 月 2 日	2016 年度暗号技術活用委員会活動計画（案）について ワーキンググループ活動計画（案）について 運用ガイドラインに関する検討事項について

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、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。

2015 年度は、検討グループにより見直しの方向性を審議し、重点課題検討タスクフォースにより具体的な見直し内容を審議し、暗号技術活用委員会の活動方針の見直しなど、CRYPTREC として対応すべきタスクの見直しを実施した。2016 年度においては、重点課題検討タスクフォースにより継続的な審議を行い、CRYPTREC のアウトプットを効率的に作成するために、他団体との協力関係の構築に向けた議論や新たなタスクの具体化のための検討・審議等を引き続き進めるものとする。

また、暗号技術評価委員会及び暗号技術活用委員会において、IoT や情報技術の進展を踏まえつつ、情報セキュリティ技術の信頼の要となる暗号アルゴリズムの安全性の評価や、その利活用方法について継続的に調査・検討を進める。

図 4.1　2016 年度 CRYPTREC の体制図（予定）