2015 年度　第 2 回暗号技術検討会

日時：平成 28 年 3 月 29 日(火)16:30～18:30
場所：経済産業省別館 1 階 104 各省共用会議室

議　事　次　第

１．開　会

２．議　事
(1) 2015 年度　暗号技術検討会報告書（案）について【承認事項】
(2) 2015 年度　重点課題検討タスクフォース活動報告について【承認事項】
(3) 2015 年度　暗号技術評価委員会活動報告について【承認事項】
(4) 2015 年度　暗号技術活用委員会活動報告について【承認事項】
(5) 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【審議事項】
(6) 2016 年度　暗号技術評価委員会活動計画について【承認事項】
(7) 2016 年度　暗号技術活用委員会活動計画について【承認事項】
(8) その他

３．閉　会

（資料番号）	（資　料　名）
資料１	2015 年度 暗号技術検討会報告書（案）
資料２	2015 年度 暗号技術評価委員会活動報告
資料２別添１	64 ビットブロック暗号 MISTY1 の安全性について（続報）
資料２別添２	SHA-1 の安全性について
資料２別添３	2015 年度 暗号技術調査 WG（暗号解析評価）活動報告
資料２別添４	2015 年度 暗号技術調査 WG（軽量暗号）報告
資料２別添５	暗号技術ガイドライン（軽量暗号）作成方針
資料３	2015 年度 暗号技術活用委員会活動報告
資料４	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（案）
資料４別添１	CRYPTREC 暗号リスト変更案
資料５	2016 年度 暗号技術評価委員会活動計画（案）
資料６	2016 年度 暗号技術活用委員会活動計画（案）
参考資料１	2015 年度 第 1 回暗号技術検討会議事概要
参考資料２	2015 年度　暗号技術検討会　構成員・オブザーバ名簿
参考資料３	「CRYPTREC の在り方に関する検討グループ」における議論結果報告
参考資料４－１	CRYPTREC 暗号技術活用委員会の今後の活動に向けて
参考資料４－２－１	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
参考資料４－２－２	暗号アルゴリズムの脆弱性に関する情報発信フロー
参考資料４－３	暗号プロトコルのセキュリティ確保に向けた活動案

資料１

暗号技術検討会
２０１５年度　報告書（案）

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。

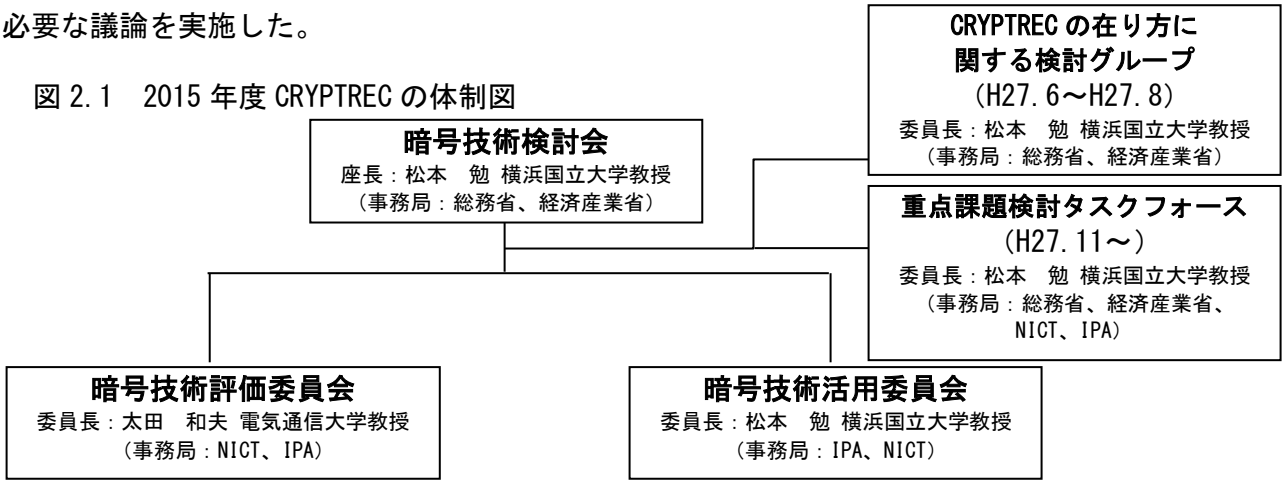
２．２． CRYPTREC の体制

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）
- 本日の議論を踏まえ記載。

２．４．CRYPTREC 暗号リストの改定

本日の議論を踏まえ記載。

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。

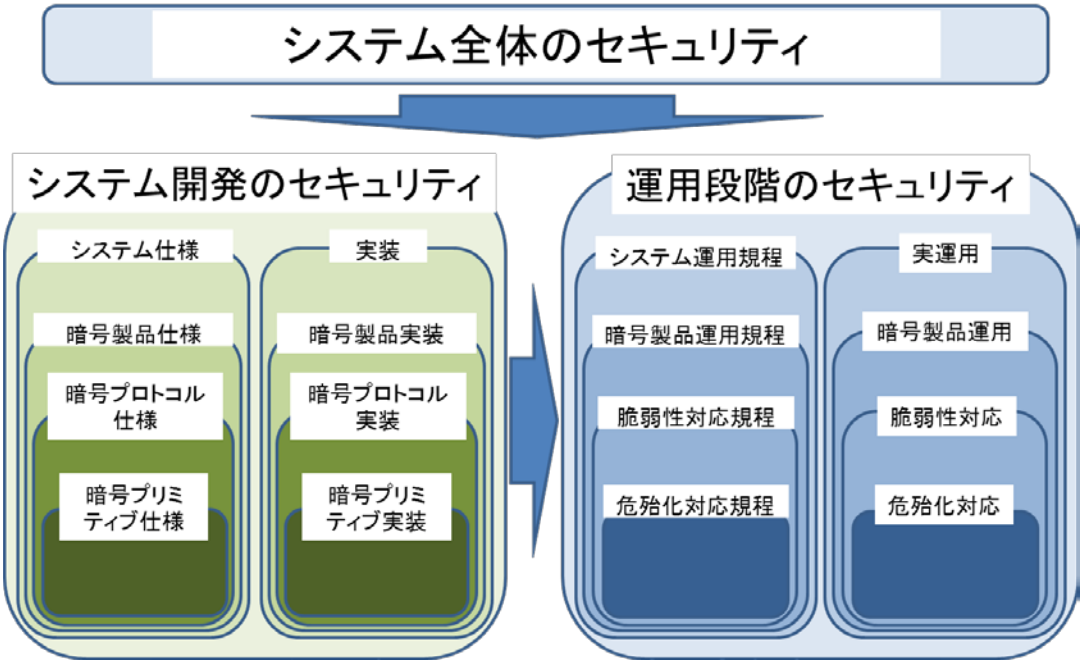
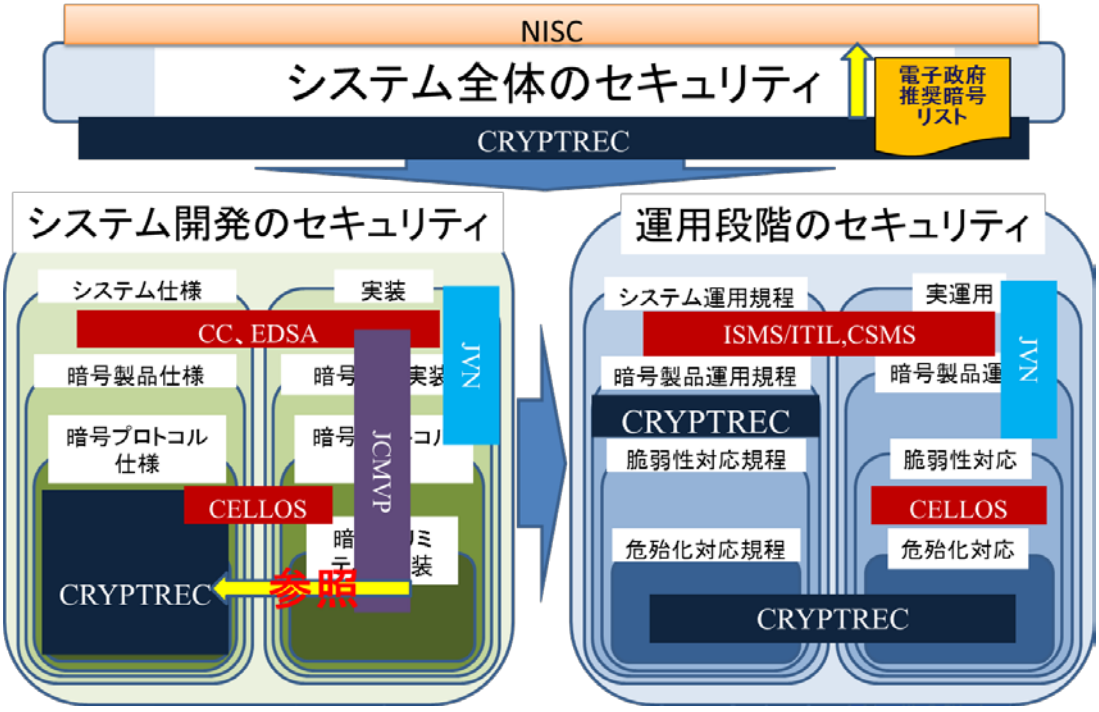


図 3.1　システムにおける暗号技術のセキュリティ確保の全体俯瞰図

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。

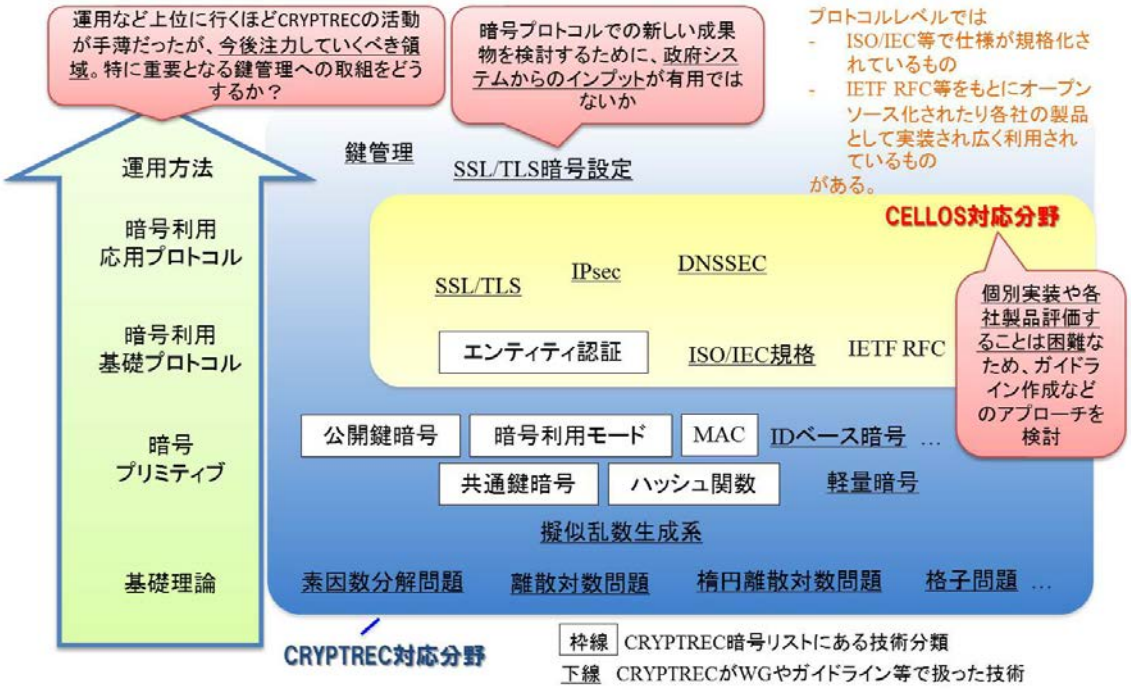


図 3.3　暗号技術マップのイメージ

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）。

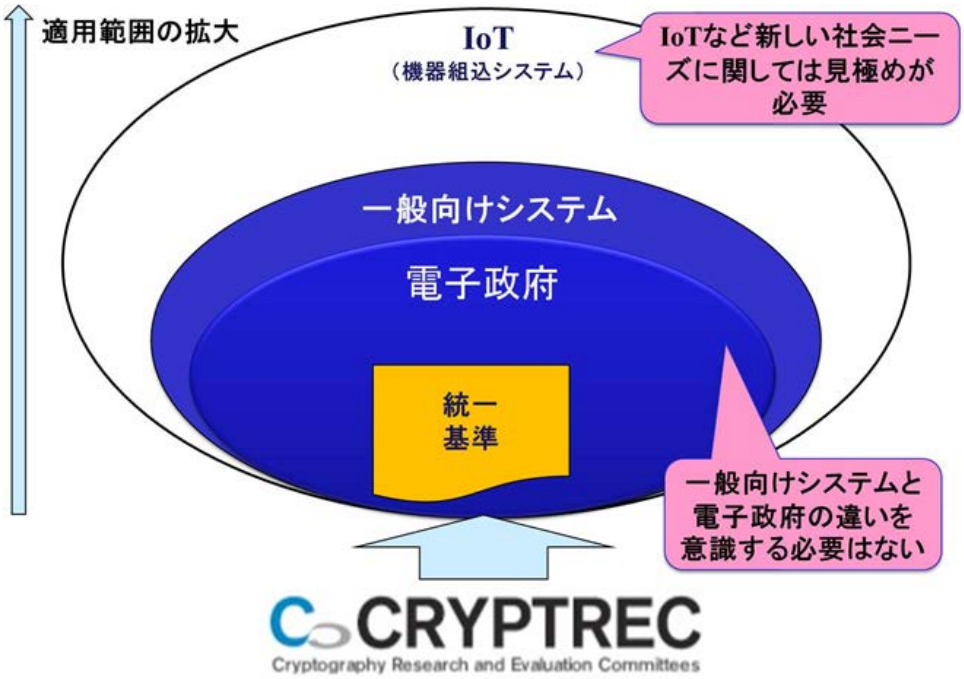


図 3.4　CRYPTREC 成果の適用範囲のイメージ

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

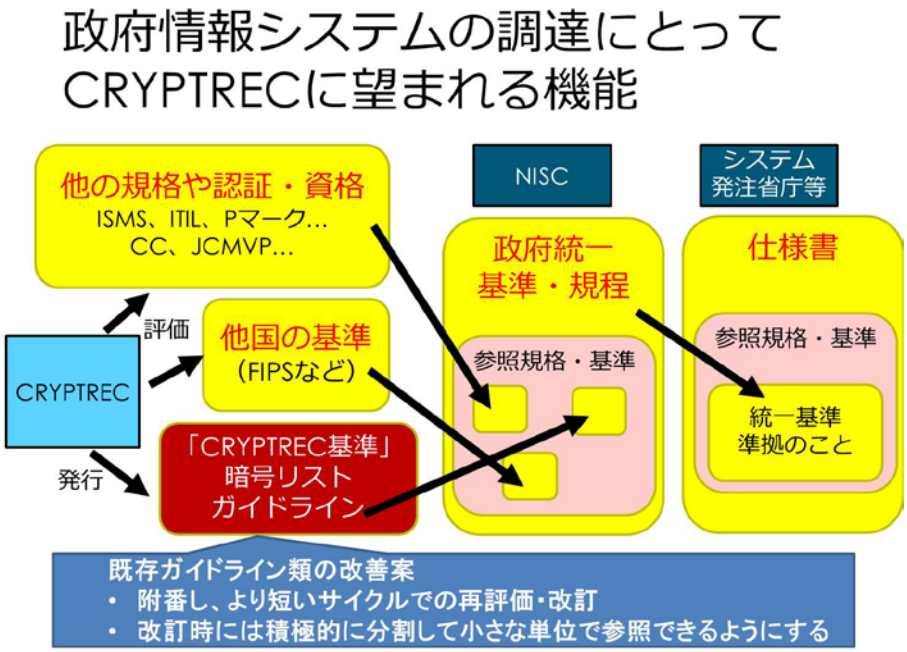


図 3.5　政府調達と CRYPTREC 成果物のあるべき関係性イメージ

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。

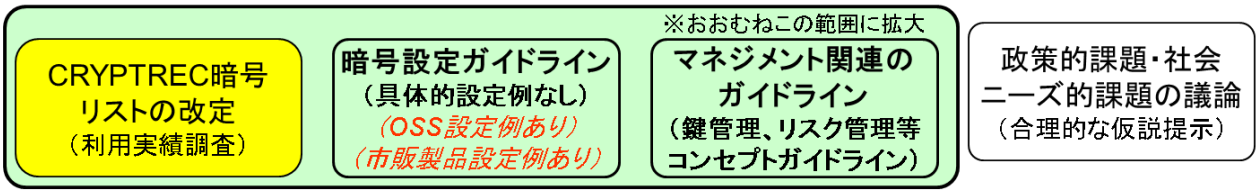


図 3.6　暗号技術活用委員会における活動対象範囲

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。

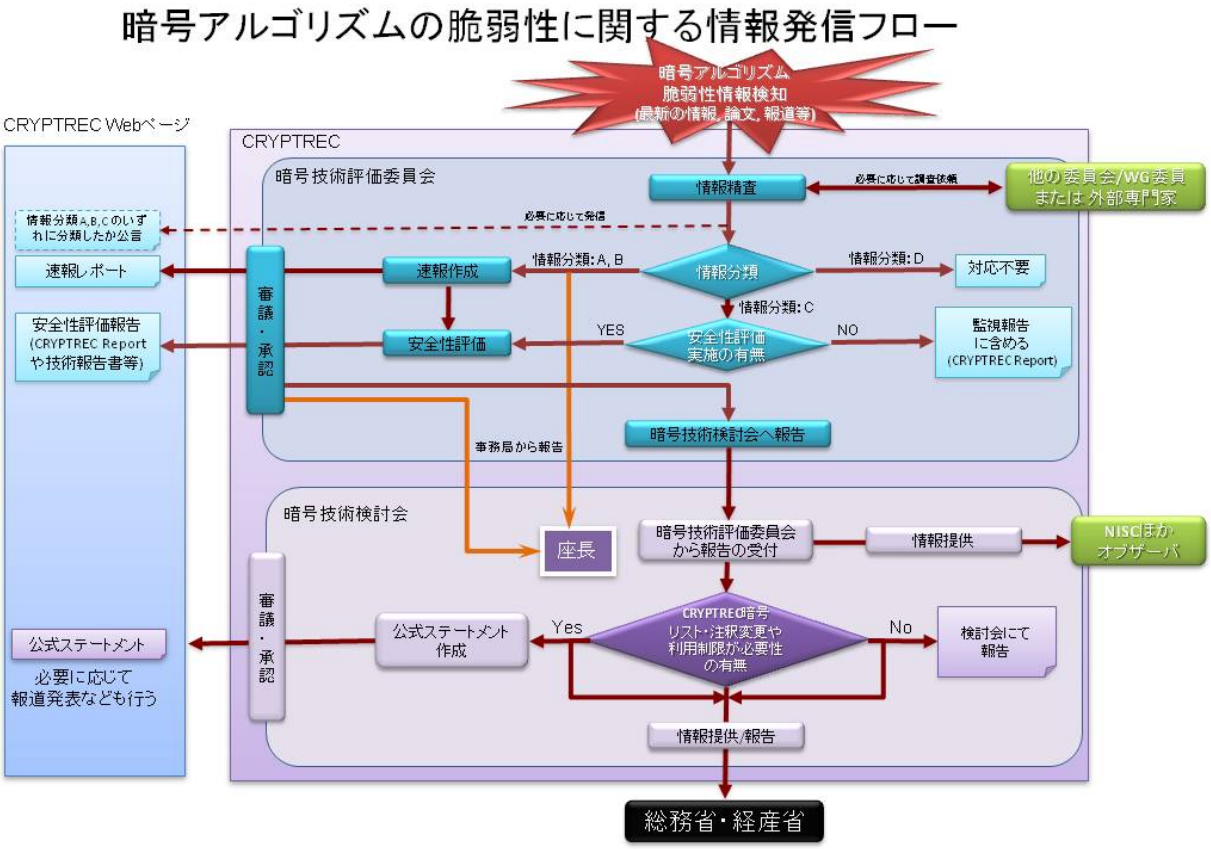


図 3.7　暗号アルゴリズムの脆弱性に関する情報発信フロー

(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。

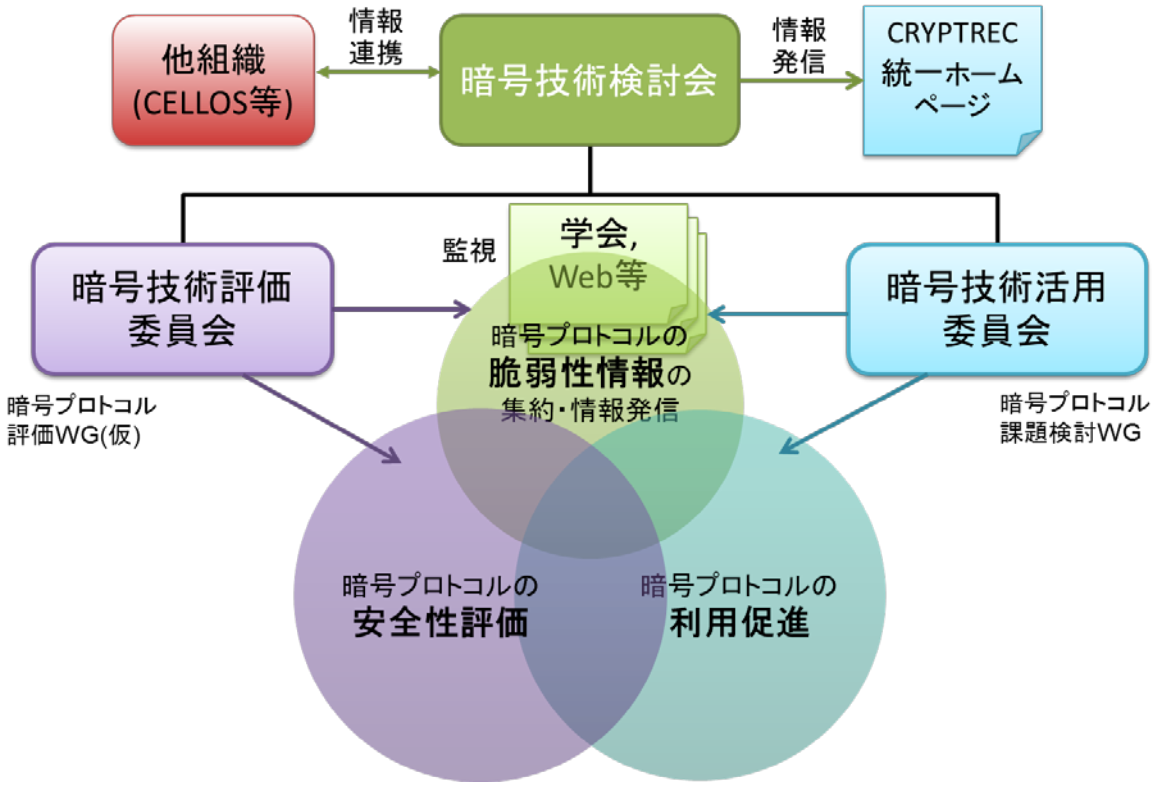


図 3.8　暗号プロトコルに関する CRYPTREC 体制案

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

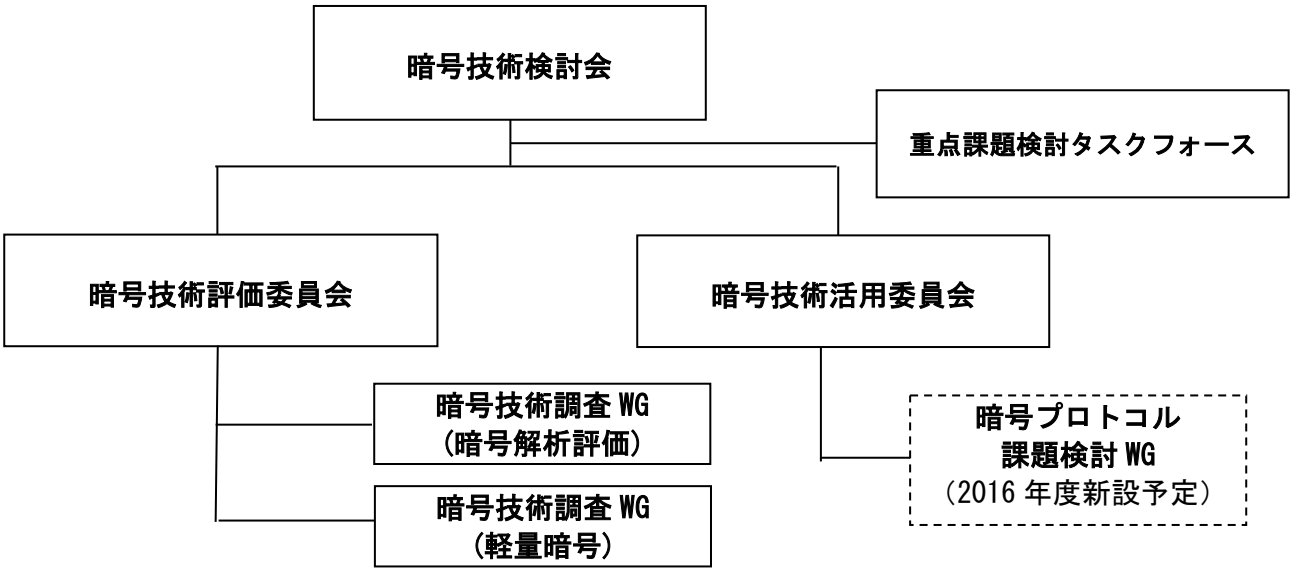
４．今後の CRYPTREC の活動について

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）



資料 2

2015 年度暗号技術評価委員会 活動報告

1. 活動目的

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。

2. 活動概要

(1) 暗号技術の安全性及び実装に係る監視及び評価

下記項目に沿い、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・評価を実施していく。

① CRYPTREC 暗号等の監視

国際会議等で発表される CRYPTREC 暗号リストの安全性及び実装に係る技術（暗号モジュールに対する攻撃とその対策も含む）に関する監視を行う。

- 今年度実施された監視報告の詳細については、CRYPTREC Report 2015 を参照のこと。

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格 及び 運用監視暗号リストからの危殆化が進んだ暗号の削除

CRYPTREC 暗号リストの安全性に係る監視活動を継続的に行い、急速に危殆化が進んだ暗号技術やその予兆のある暗号技術の安全性について評価を行う。また、リストからの降格や削除、注釈の改訂が必要か検討を行う。

- 今年度、降格および削除対象となる暗号技術はなかった。

③ CRYPTREC 注意喚起レポートの発行

CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。

- 今年度は、下記の注意喚起レポートを発行した。
  - 「64 ビットブロック暗号 MISTY1 の安全性について」[1]（2015 年 7 月 16 日）
  - 「64 ビットブロック暗号 MISTY1 の安全性について（続報）」[2]（2015 年 8 月 12 日）
  - 「SHA-1 の安全性について」[3]（2015 年 12 月 18 日）

[1] http://www.cryptrec.go.jp/topics/cryptrec_20150716_misty1_cryptanalysis.html
[2] http://www.cryptrec.go.jp/topics/cryptrec_20150812_misty1_cryptanalysis.html
[3] http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加

標準化動向に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を検討する。

- 暗号技術評価委員会での審議結果、ハッシュ長が 256 ビット以上のアルゴリズムのみとすることとなった。具体的な対象アルゴリズムは以下の通り。
  - SHA-2 ： SHA-512/256
  - SHA-3 ： SHA3-256, SHA3-384, SHA3-512, SHAKE256※

※ハッシュ長は 256 ビット以上とする。

⑤ 新技術に関する調査及び評価

将来的に有用になると考えられる技術について、暗号技術調査ワーキンググループにて調査および評価を行う。また、外部評価等を通して新技術や CRYPTREC 暗号リストに関わる技術の安全性・性能評価を行う。

- 暗号技術調査ワーキンググループ（暗号解析評価）及び暗号技術調査ワーキンググループ（軽量暗号）を設置し、検討・評価を行った。
  - 暗号技術調査ワーキンググループ(暗号解析評価)

    詳細は、別添 3「2015 年度暗号技術調査 WG（暗号解析評価）活動報告」を参照のこと。
  - 暗号技術調査ワーキンググループ(軽量暗号)

    詳細は、別添 4「2015 年度暗号技術調査 WG（軽量暗号）報告」および別添 5「暗号技術ガイドライン（軽量暗号）作成方針」を参照のこと。

(2) 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）

暗号技術を利用する際の技術面での注意点に関する調査、新技術の安全性・性能に関する調査・評価を行う。

- 今年度、暗号技術ガイドラインの更新を行わなかった。

（参考資料） 委員構成

［暗号技術評価委員会］

委員長	太田 和夫	国立大学法人電気通信大学 大学院 情報理工学研究科 総合情報学専攻(セキュリティ情報学コース) 教授
委員	岩田 哲	国立大学法人名古屋大学大学院 工学研究科 准教授
委員	上原 哲太郎	立命館大学 情報理工学部 情報システム学科 教授
委員	金子 敏信	東京理科大学 理工学部 電気電子情報工学科 教授
委員	佐々木 良一	東京電機大学 未来科学部 情報メディア学科 教授
委員	高木 剛	国立大学法人九州大学 マス・フォア・インダストリ研究所 教授
委員	手塚 悟	東京工科大学 コンピュータサイエンス学科 教授
委員	本間 尚文	国立大学法人東北大学 大学院 情報科学研究科 准教授
委員	松本 勉	国立大学法人横浜国立大学 大学院 環境情報研究院 教授
委員	松本 泰	セコム株式会社 IS研究所 コミュニケーションプラットフォームディビジョン ディビジョンマネージャー
委員	盛合 志帆	国立研究開発法人情報通信研究機構 ネットワークセキュリティ研究所 セキュリティ基盤研究室 室長
委員	山村 明弘	国立大学法人秋田大学 大学院 工学資源学研究科 情報工学専攻 教授
委員	渡辺 創	国立研究開発法人産業技術総合研究所 情報技術研究部門 上級主任研究員

［暗号技術調査ワーキンググループ(暗号解析評価)］

主査	高木　剛	国立大学法人九州大学 マス・フォア・インダストリ研究所 教授
委員	青木 和麻呂	日本電信電話株式会社 NTTセキュアプラットフォーム研究所 主任研究員
委員	太田 和夫	国立大学法人電気通信大学 大学院 情報理工学研究科 総合情報学専攻(セキュリティ情報学コース) 教授
委員	草川　恵太	日本電信電話株式会社 NTTセキュアプラットフォーム研究所 研究員
委員	國廣　昇	国立大学法人東京大学大学院 新領域創成科学研究科複雑理工学専攻 准教授
委員	下山　武司	株式会社富士通研究所 知識情報処理研究所 データ・プライバシー保護プロジェクト 主管研究員
委員	安田　雅哉	国立大学法人九州大学 マス・フォア・インダストリ研究所 准教授

［暗号技術調査ワーキンググループ(軽量暗号)］

主査	本間 尚文	国立大学法人東北大学 大学院 情報科学研究科 准教授
委員	青木 和麻呂	日本電信電話株式会社 NTTセキュアプラットフォーム研究所 主任研究員
委員	岩田 哲	国立大学法人名古屋大学 大学院工学研究科 准教授
委員	小川 一人	NHK放送技術研究所 上級研究員
委員	小熊 寿	株式会社トヨタIT開発センター 研究部 シニアリサーチャー
委員	崎山 一男	国立大学法人電気通信大学 大学院 情報理工学研究科 教授
委員	渋谷 香士	ソニー株式会社 生産・物流・調達・品質/環境プラットフォーム エンジニアリング部門 セキュリティ品質技術部
委員	鈴木 大輔	三菱電機株式会社 情報技術総合研究所 主席研究員
委員	成吉 雄一郎	ルネサスエレクトロニクス株式会社 第一ソリューション事業本部 コア技術事業統括部 CPUシステムソリューション部 主任技師
委員	峯松 一彦	日本電気株式会社 クラウドシステム研究所 主任研究員
委員	三宅 秀享	株式会社東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 研究主務
委員	渡辺 大	株式会社日立製作所 システムイノベーションセンタ 主任研究員

以上

資料 2 別添 1

64 ビットブロック暗号 MISTY1 の安全性について（続報）

平成 27 年 8 月 12 日
CRYPTREC 暗号技術評価委員会

CRYPTREC 暗号リストの推奨候補暗号リスト [1]に掲載されている 64 ビットブロック暗号 MISTY1 に対する解析結果を示した論文が発表され [2]、CRYPTREC より本論文に対する見解 [3]を 7 月 16 日に出したところですが、このたび、この解読計算量をさらに削減した新たな解析結果が国際暗号学会 （International Association for Cryptologic Research (IACR)）のアーカイブサイト IACR ePrint Archive にて 7 月 30 日に発表されました [4]。

新たな解析結果では、解読に必要なデータ量は 2^{64} と非常に多く、すべての（平文, 暗号文）の組を集める必要があるものの、$2^{69.5}$回の暗号化演算に相当する現実的な計算量で MISTY1 の 128 ビットの鍵を導出することができると示されています。しかしながら、この攻撃は、解読に必要なデータ量が膨大であることから、現実的な脅威ではないと考えられます。CRYPTREC では、MISTY1 の安全性に関して引き続き調査を行い、CRYPTREC Web サイトにて報告する予定です。

表：Integral Cryptanalysis による MISTY1 の解読計算量

	解読に必要なデータ量 [5]	解読に必要な計算量 [6]
藤堂による解析結果 [2]	$2^{63.58}$	2^{121}
藤堂による解析結果 [2]	$2^{63.994}$	$2^{107.9}$
Bar-On による解析結果 [4]	2^{64}	$2^{69.5}$

[1] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf

[2] Yosuke Todo, “Integral Cryptanalysis on Full MISTY1”, to appear in the proceedings of CRYPTO 2015. https://eprint.iacr.org/2015/682

[3] http://www.cryptrec.go.jp/topics/cryptrec_20150716_misty1_cryptanalysis.html

[4] Achiya Bar-On, “A 2^{70} Attack on the Full MISTY1”. https://eprint.iacr.org/2015/746

[5] 1 単位は（平文, 暗号文）の 1 組で、平文、暗号文ともに 64 ビットである。本攻撃では、攻撃に使える条件を満たす平文を選択し、それに対応する暗号文の組を収集する必要がある（選択平文攻撃）。

[6] 1 単位は 1 回の暗号化に要する計算量である。128 ビット鍵の全数探索（すべての鍵の総当たり）の計算量は 2^{128}である。

ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。

CRYPTREC 事務局
E-mail: info@cryptrec.go.jp

On the Security of 64-bit Block Cipher MISTY1 (Continued Report)

August 12, 2015
CRYPTREC Cryptographic Technology Evaluation Committee

We provided comments[1] on a new cryptanalytic result[2] on MISTY1, which is a 64-bit block cipher on the CRYPTREC Candidate Recommended Ciphers List[3], on July 16th. After that another new cryptanalytic result on MISTY1 with reduced time complexity[4] was published by the International Association for Cryptologic Research (IACR) ePrint Archive on July 30th.

The published paper shows that a 128-bit secret key of full-round MISTY1 can be recovered with a practical time complexity which is equivalent to approximately $2^{69.5}$ encryption operations, although all (2^{64}) pairs of plaintexts and corresponding ciphertexts are required for the attack. Since the required data is huge, this attack is not considered practical. We will continue further evaluation on the security of MISTY1 and report them on the CRYPTREC web site.

Table: Complexities of Integral Cryptanalysis on MISTY1

	Required data[5]	Time complexity[6]
Result by Todo[2]	$2^{63.58}$	2^{121}
Result by Todo[2]	$2^{63.994}$	$2^{107.9}$
Result by Bar-On[4]	2^{64}	$2^{69.5}$

[7] http://www.cryptrec.go.jp/topics/cryptrec_20150716_misty1_cryptanalysis.html
[8] Yosuke Todo, “Integral Cryptanalysis on Full MISTY1”, Advances in Cryptology – CRYPTO 2015, Lecture Notes in Computer Science, Volume 9215, pages 413–432. https://eprint.iacr.org/2015/682
[9] https://www.cryptrec.go.jp/english/method.html
[10] Achiya Bar-On, “A 2^{70} Attack on the Full MISTY1”. https://eprint.iacr.org/2015/746
[11] Unit of the required data is a pair of plaintext block and ciphertext block. Both blocks

are 64-bit length. The attacks require chosen plaintexts and their corresponding ciphertexts.

[12] Unit of the time complexity is the computational cost for one block encryption. The time complexity for the key exhaustive search attack for a 128-bit key is 2^{128}.

If you have any opinions, comments, or inquiries about this topic, please contact us at the following address.

CRYPTREC Secretariat

E-mail: info@cryptrec.go.jp

資料 2 別添 2

SHA-1 の安全性について

平成 27 年 12 月 18 日
CRYPTREC 暗号技術評価委員会

2015 年 10 月 8 日に、CWI(オランダ)、INRIA(フランス)、NTU(シンガポール)の共同研究チームは、ハッシュ関数 SHA-1 のフルラウンド(全 80 ステップ中 80 ステップ)に対して、仕様より緩い条件下ながら初めて衝突発見に成功したと発表しました[1]。本発表のもとになっている論文は国際暗号学会(International Association for Cryptologic Research (IACR))のアーカイブサイト IACR ePrint Archive で公開されています[2]。

今回の発表された内容は、SHA-1 の衝突発見に直接つながるものではありませんが、SHA-1 の衝突発見に至るまでの節目となる出来事、マイルストーンの 1 つであり、近い将来に SHA-1 の衝突が発見されるという予測を強く裏付けるものです。当委員会としては、従前通り、SHA-1 に関する移行対策を実施して頂きたいと考えています。

当委員会(当時は暗号技術監視委員会)では、2005 年に SHA-1 に対する衝突発見アルゴリズムが論文発表された後、安全性評価を行った結果、近い将来この攻撃アルゴリズムが実際に実装可能になり、衝突発見困難性に対して脅威になるものと判断しました[3]。その後、情報セキュリティ政策会議から、2008 年に SHA-1 に関して移行指針[4]が発表されています。現在、CRYPTREC では、SHA-1 を「CRYPTREC 暗号リスト」の「運用監視暗号リスト」[5]に掲載し、互換性維持以外の目的での利用を推奨していません。また、SHA-1 の用途ごとの具体的な利用指針として、「CRYPTREC 暗号技術ガイドライン(SHA-1)」[6]を公開しています。

引き続き、CRYPTREC では、暗号技術などの監視・評価を行い、SHA-1 の取り扱いなどについて変更が生じた場合は、CRYPTREC Web サイトなどを通じてお知らせします。

ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。

CRYPTREC 事務局
E-mail ： info@cryptrec.go.jp

【参考文献】

[1] Press Release “Researchers urge: industry standard SHA-1 should be retracted sooner”, CWI, Inria, NTU, October 8, 2015. https://www.cwi.nl/news/2015/researchers-urge-industry-standard-sha-1-should-be-retracted-sooner

[2] Marc Stevens, Pierre Karpman, and Thomas Peyrin, “Freestart collision for full SHA-1”. IACR ePrint Archive. https://eprint.iacr.org/2015/967

[3] CRYPTREC Report 2005 「暗号技術監視委員会報告」(2006 年 3 月): http://www.cryptrec.go.jp/report/c05_wat_final.pdf

[4] 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」(平成 20 年 4 月 22 日 情報セキュリティ政策会議決定、平成 24 年 10 月 26 日 情報セキュリティ対策推進会議改定) :
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
[5] 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) (2013 年 3 月 1 日 総務省・経済産業省、2015 年 3 月 27 日改定) :
http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2015.pdf
[6] CRYPTREC 暗号技術ガイドライン(SHA-1) (2014 年 3 月):
http://www.cryptrec.go.jp/report/c13_tech_guideline_SHA-1_web.pdf

資料 2 別添 3

2015 年度暗号技術調査 WG（暗号解析評価）活動報告

1. 活動目的

(1)楕円曲線上の離散対数問題(ECDLP)の困難性に関する調査

2012 年度の暗号技術調査 WG(計算機能力評価)における調査結果において言及があったように、ECDLP に対する指数計算法の計算量評価についての研究結果が近年発表されてきている。2015 年～2016 年度は、これらの研究内容を調査し、見解をまとめる。

(2)多重線形写像(multi-linear map)及び難読化(Obfuscation)の最新動向に関する調査

2013 年～2014 年度は、格子問題等の困難性に関する調査を行い、「格子問題等の困難性に関する調査」を作成した。2015 年～2016 年度は、近年研究が進展している多重線形写像及び難読化に関する研究動向を調査する。

(3)予測図の更新

素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関して CRYPTREC が例年公表している予測図の更新を行う。

2. 委員構成

主査：高木 剛(九州大学)
委員：青木 和麻呂(NTT)
委員：太田 和夫(電気通信大学)
委員：草川 恵太 (NTT)
委員：國廣 昇(東京大学)
委員：下山 武司(富士通研究所)
委員：安田 雅哉(九州大学)

3. 活動方針

3.1 楕円曲線上の離散対数問題の困難性に関する調査

CRYPTO2015 で発表された論文[HKY2015]などを精査し、論点や課題を事務局にて整理する。さらなる検討は来年度に行う。

[HKY2015] “Last fall degree, HFE, and Weil descent attacks on ECDLP,” Ming-Deh A. Huang, Michiel Kosters, Sze Ling Yeo
(プレゼン資料 “Sub-exponential algorithms for ECDLP?”[4])

3.2 多重線形写像及び難読化の最新動向に関する調査

(a) 多重線形写像については、既存の文献をリストアップし、それらを用いた応用やアプリケーシ

[4] http://ecc2015.math.u-bordeaux1.fr/documents/kosters.pdf

ョンなどに関する調査を行う。来年度、必要に応じて外部評価を実施し、安全性評価を行う。

(b) 難読化技術については、今年度実施した外部評価者からのレポートに基づき現状を把握し、論点や課題を整理する。今年度の検討結果に基づき、来年度にさらなる評価を実施する。

3.3 予測図の更新

(a) 素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量の評価に大幅な変更がないかどうかの確認を行う。

(b) スーパーコンピュータのベンチマーク結果の 1 位から 500 位を 1993 年から半年毎に集計している Web サイト TOP500.Org[5]における、2015 年 6 月・11 月のベンチマーク結果の追加を行う。

4. 活動概要

4.1 スケジュール

第 1 回　2016 年 1 月 22 日(金) 活動計画案や作業内容についての審議と了承

第 2 回　2016 年 3 月 3 日(木)　調査内容についての審議と了承

4.2 楕円曲線上の離散対数問題の困難性に関する調査

(a) 下記の論文をリストアップし、ECDLP の計算量評価の概要を報告した。

(b) 標数 2 の有限体上の ECDLP の研究動向の解説を論文[GG2016]をベースに、素体上の ECDLP の研究動向の解説を論文[PKM2016]をベースに、次年度に記述することになった。

[S2004] Semaev, “Summation polynomials and the discrete logarithm problem on elliptic curves,” https://eprint.iacr.org/2004/031.pdf.

[D2011] Diem, “On the discrete logarithm problem in elliptic curves、” Compositio Math. 147、2011.

[FPPR2012] Faugère, Perret, Petit and Renault, “Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields,” Eurocrypt 2012.

[PQ2012] Petit and Quisquater, “On polynomial systems arising from a Weil descent,” ASIACRYPT 2012.

[HKY2015] Huang, Kosters and Yeo, “Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP,” CRYPTO 2015.

[GG2016] Galbraith and Gaudry, “Recent progress on the elliptic curve discrete logarithm problem,” Designs, Codes and Cryptography. (2016) 78

[PKM2016] Petit, Kosters and Messeng, “Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields,” PKC 2016.

[5] http://www.top500.org/

4.3 多重線形写像及び難読化の最新動向に関する調査

(a) 多重線形写像については、既存の文献をリストアップし、それらを用いた応用やアプリケーションなどに関する調査を行った。

(b) 難読化技術については、今年度実施した外部評価者からのレポートのレビューを3月末までを目途として行う。外部評価レポートは技術評価レポートとして Web に掲載し、サマリーを CRYPTREC Report 2015 に掲載する。

(c) 次年度は、多重線形写像と難読化の関係を整理しつつ、特に多重線形写像の安全性を重点的に調査・評価を実施する。

4.4 予測図の更新

(a) 素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、2015 年 6 月・11 月のベンチマーク結果を追加して予測図の更新を行った。

(b) 過去の議論・経緯などを把握できるような資料を次年度に作成する。公開するかどうかについては今後検討する。

4.5 Post-Quantum Cryptography の動向について

本 WG では、2013～2014 年度に格子問題等の困難性に関する調査を行った。NIST は、先日、NISTIR 8105 DRAFT Report on Post-Quantum Cryptography[6]を公表し、PQCrypto 2016 において、Post-Quantum Cryptography: NIST's Plan for the Future[7]と題してプレゼンテーションを行っているため、NIST の見解などについて意見交換を行った。

5. 成果概要

5.1 多重線形写像及び難読化の最新動向に関する調査

詳細は、CRYPTREC Report 2015 を参照のこと。

5.2 予測図の更新

「素因数分解問題の困難性」(図１) 及び「楕円曲線上の離散対数問題の困難性」(図２) に関して、2015 年 6 月及び 11 月に TOP500.org のスーパーコンピュータのリストの更新があったため、2014 年度の予測図をそれぞれ更新した。

[6] http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf
[7] https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf

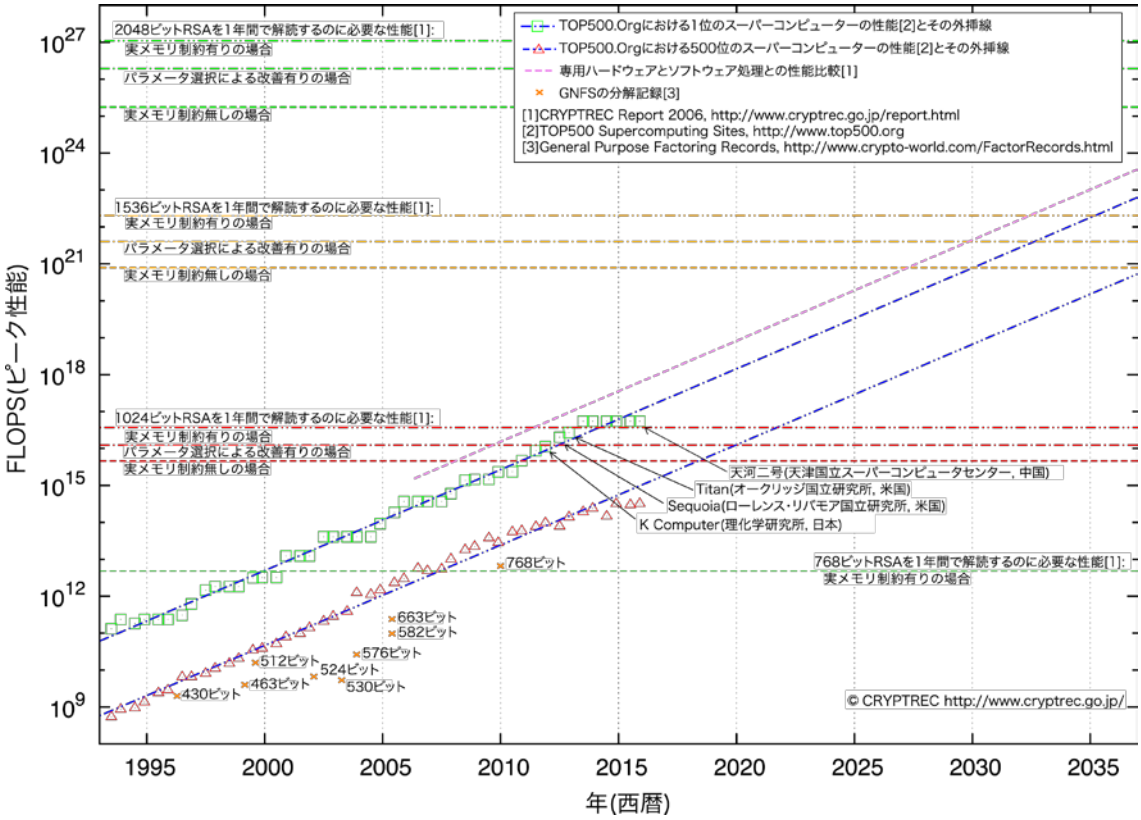


図 1：1 年間でふるい処理を完了するのに要求される処理能力の予測(2016 年 2 月更新)

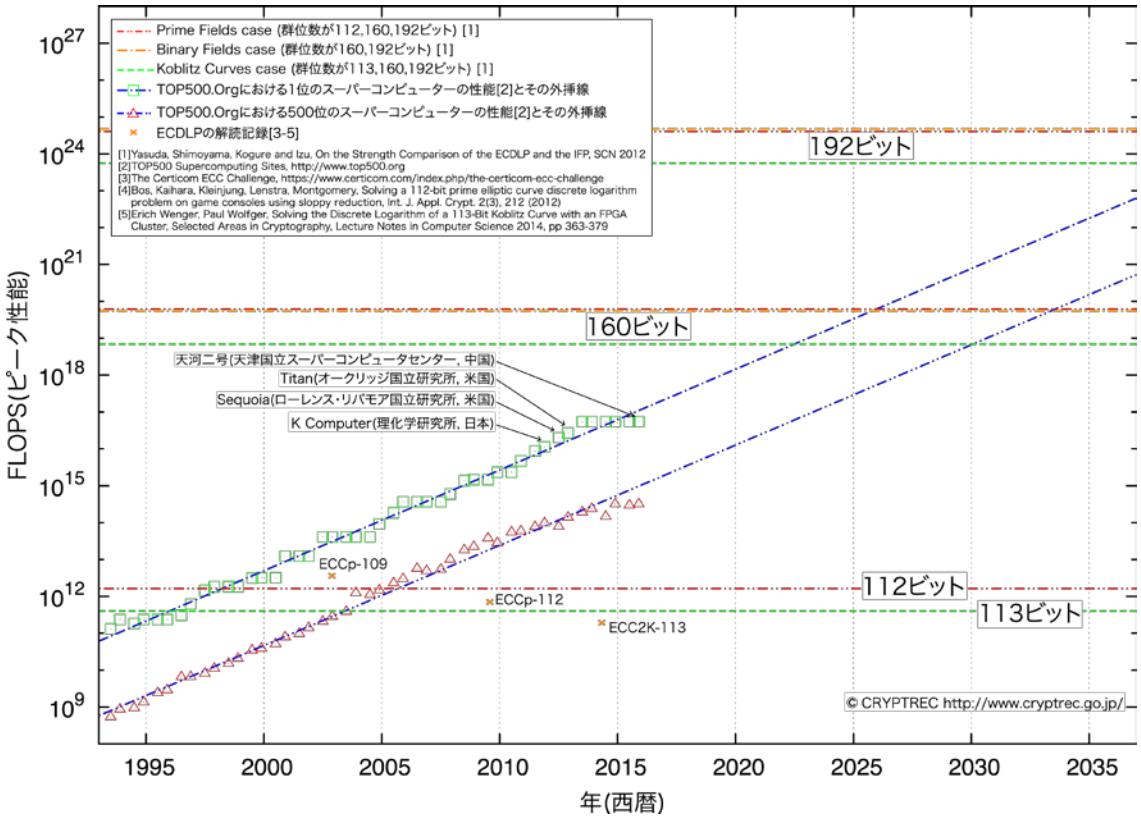


図 2： ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測(2016 年 2 月更新)

資料 2 別添 4

2015 年度暗号技術調査 WG（軽量暗号）報告

1. 活動目的

軽量暗号 WG は、軽量暗号技術が求められるサービスにおいて、電子政府のみならず一般のシステムにおいて、利用者が適切な暗号方式を選択でき、容易に調達できることをめざして活動を行っている。

2015 年度からは、軽量暗号を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的とした「暗号技術ガイドライン（軽量暗号）」を発行するために、2 年かけて詳細評価を行う。

2. 委員構成

主査：本間 尚文（東北大学）
委員：青木 和麻呂（NTT）
委員：岩田 哲（名古屋大学）
委員：小川 一人（NHK）
委員：小熊 寿（トヨタ IT 開発センター）
委員：﨑山 一男（電気通信大学）
委員：渋谷 香士（ソニー）
委員：鈴木 大輔（三菱電機）
委員：成吉 雄一郎（ルネサスエレクトロニクス）
委員：峯松 一彦（NEC）
委員：三宅 秀享（東芝）
委員：渡辺 大（日立）

3. 2015 年度の活動

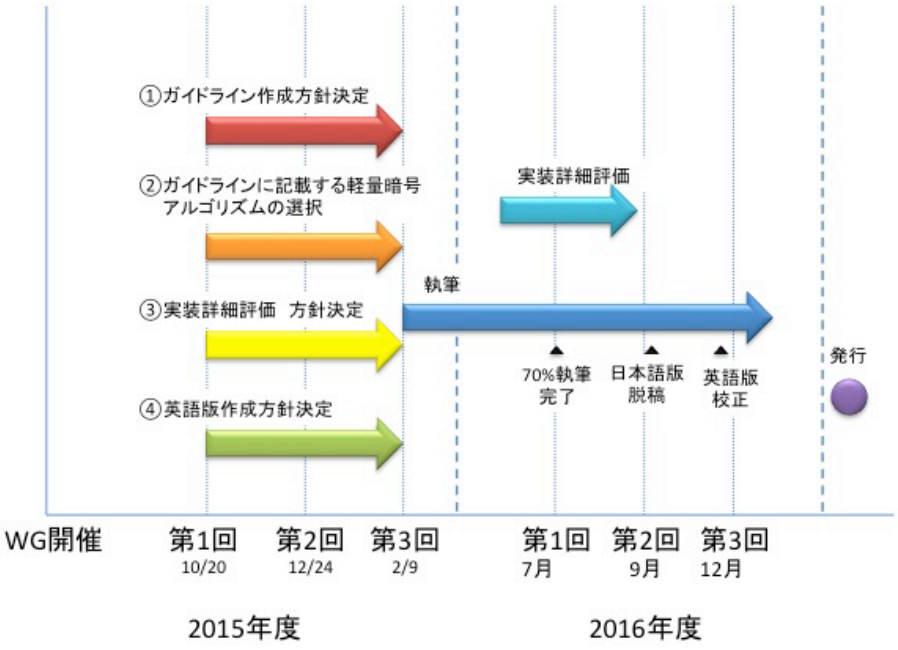
2015 年度は、下記についての検討を行った。

① ガイドラインの作成方針の決定
- 目的の確認、目次案の決定、各章の執筆担当の決定

② ガイドラインに記載する軽量暗号アルゴリズムの選択
- どのような基準で選択するか

③ 実装詳細評価の方針の決定
- 実装プラットフォーム、実装方法、評価（測定）指標、評価対象の軽量暗号アルゴリズム

④ 軽量暗号 WG 活動の対外的アピールのあり方に関する検討
- 英語版作成など



ガイドライン作成スケジュール案

4. 2016 年度の活動計画

① 「暗号技術ガイドライン（軽量暗号）」の執筆を行う

- 日本語版、英語版とも

② 実装詳細評価を行う

資料2別添5

暗号技術ガイドライン（軽量暗号）作成方針

1　作成目的と想定読者

IoT 等の次世代ネットワークサービスにおいて軽量暗号の活用が期待されることから、方式を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的として、暗号技術ガイドラインを作成する。

想定する読者は、情報システムのセキュリティ機能の設計・開発・実装において暗号技術を活用する技術者である。

2　目次案（括弧内は執筆担当者）

I.　はじめに　（本間主査・事務局）

軽量暗号に関するサマリー

II.　軽量暗号の活用例（青木委員、岩田委員、小川委員、小熊委員、崎山委員、成吉委員）

1. 軽量暗号とは

軽量暗号の特徴

2. 軽量暗号はどこに使えるか？

軽量暗号の代表的なユースケース

3. どんな軽量暗号、パラメータを選べばいいか？

軽量暗号の分類と一覧、条件やニーズに対応した軽量暗号の選択

鍵長、ブロック長の説明と選び方

4. 軽量暗号を使う時の留意点

鍵更新のタイミング、鍵更新の方法

鍵更新の頻度を減らせる暗号利用モードの紹介

関連鍵攻撃が指摘されているブロック暗号を利用する時の注意点

5. ユースケースごとの軽量暗号活用例と効果

ユースケース別にお勧めの軽量暗号とその鍵長、ブロック長、暗号利用モードなどを示す

既存暗号を使った場合と比較した優位性を示す(ハードウェア回路規模、消費電力量、レイテンシ、メモリサイズ)

III. 軽量暗号の性能比較　（鈴木委員、三宅委員）

1. ハードウェア実装

- ハードウェア回路規模で比較

- 消費電力量で比較
- レイテンシで比較

2. ソフトウェア実装
   - 必要メモリサイズで比較

IV. 代表的な軽量暗号

1. ブロック暗号　（渋谷委員）
2. ストリーム暗号　（渡辺委員）
3. ハッシュ関数　（三宅委員）
4. メッセージ認証コード　（渡辺委員）
5. 認証暗号　（峯松委員）

3　IV 章に記載するアルゴリズム

ブロック暗号

アルゴリズム名	発表された国際会議，採録/提案されている標準等
LED	CHES 2011
Piccolo	CHES 2011
TWINE	SAC 2012
PRINCE	ASIACRYPT 2012
Midori	ASIACRYPT 2015
PRESENT	CHES 2007, ISO/IEC 29192-2
CLEFIA	FSE 2007, ISO/IEC 29192-2
SIMON	Cryptology ePrint Archive (2013-404)
SPECK	Cryptology ePrint Archive (2013-404)

ストリーム暗号

アルゴリズム名	発表された国際会議，採録/提案されている標準等
Grain v1/-128A	eStream portfolio, ISO/IEC 29167-13
MICKEY 2.0	eStream portfolio
Trivium	eStream portfolio, ISO/IEC 29192-3
Enocoro	ISO/IEC 29192-3
ChaCha20	RFC7539

ハッシュ関数

アルゴリズム名	発表された国際会議，採録/提案されている標準等
PHOTON	CRYPTO2011，ISO/IEC29192
SPONGENT	CHES2011，ISO/IEC29192
QUARK	CHES2010
KECCAK	SHA-3 competition

メッセージ認証コード

アルゴリズム名	発表された国際会議，採録/提案されている標準等
SipHash	INDOCRYPTO2012，DIAC

認証暗号

アルゴリズム名	発表された国際会議，採録/提案されている標準等
ACORN	DIAC'14，15
ASCON	DIAC'14，15，CT-RSA'15(analysis)
AES-JAMBU	DIAC'14，15
AES-OTR	EUROCRYPT 2014，DIAC'15
CLOC and SILC	FSE'14(CLOC)，DIAC'14(SILC)，DIAC'15
Deoxys	ASIACRYPT 2014 (as TWEAKEY)，DIAC'14,15
Joltik	ASIACRYPT 2014 (as TWEAKEY)，DIAC'14,15
Ketje	DIAC'14，(SHA3)
Minalpher	DIAC'14，GCCE'15(Hw)
OCB	ACM CCS 2001，ASIACRYPT 2004，FSE 2011
PRIMATES	FSE'14(APE)，AC'14(RUP,bound)，DIAC'14,15
SCREAM	DIAC'14,15

軽量暗号に関する実装詳細評価の方針について

「暗号技術ガイドライン（軽量暗号)」の作成にあたって、複数の軽量暗号アルゴリズム及び比較対象となる代表的な既存暗号技術を、同一プラットフォーム上で、統一的な実装ポリシーにより実装し、統一的な評価環境で比較を行う「実装詳細評価」が必要と考えられる。以下の実装詳細評価の方針を示す。

1. ハードウェア実装　詳細評価方針
2. ソフトウェア実装　詳細評価方針
3. 実装対象分野およびアルゴリズム

1. ハードウェア実装　詳細評価方針

（ア）　実装プラットフォーム

- ASIC 実装評価
- 標準的な CMOS セルライブラリを利用

  NanGate Open Cell Library (45 nm プロセス)

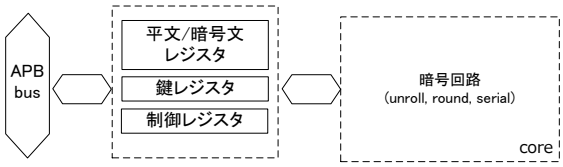
  オープンソースであり第三者による検証が可能、半導体メーカーも採用

（イ）　実装方法 及び 評価指標

- 3 通りのアーキテクチャで実装
  - ①各アルゴリズムの仕様に準じた標準的な実装（round 実装)
  - ②処理速度を優先する実装(unrolled 実装)
  - ③回路規模を優先する実装(serial 実装)
- 各実装アーキテクチャについて、以下の指標の測定を行う
  - ①最大動作周波数
  - ②処理速度
  - ③ゲートカウント
  - ④サイクルカウント
  - ⑤消費電力
  - ⑥ピーク電流

（ウ）　インターフェース

実装対象の各アルゴリズムに対して、平文・暗号文・鍵等の入出力データの与え方や測定方法を統一し、公平に比較可能なインターフェースで実装および測定を行う。



2. ソフトウェア実装　詳細評価方針

(ア)　　実装プラットフォーム

- 組込みプロセッサ上での実装評価
- ルネサスエレクトロニクスのプラットフォーム（組込みマイコン マーケットシェア１位）

(イ)　　実装方法 及び 評価指標

- 処理速度とメモリ(RAM, ROM) サイズを指標とし、処理速度を優先した高速版とメモリサイズを削減した小型版の 2 通りの実装を行う
- それぞれの実装について処理速度とメモリ(RAM, ROM) サイズを測定

(ウ)　　インターフェース

- 実装対象の各アルゴリズムに対して、平文、鍵、暗号文等の入出力データの与え方や測定方法を考慮し、公平に比較可能なインターフェースで実装および測定を行う
- 技術カテゴリ毎に記載

3. 実装対象分野およびアルゴリズム

(ア)　　軽量認証暗号

CAESAR プロジェクト 2nd Round に進んだ「軽量」な方式の中から選択

※先行調査で実装済みの方式：AES-GCM, Minalpher, AES-OTR, CLOC, SILC, Ketje

比較対象の既存技術：AES-GCM

(イ)　　軽量メッセージ認証コード

詳細実装評価までは行わないが、公知情報から速度等の目安が分かるように 3 章に記載する。

(ウ)　　軽量ブロック暗号

CLEFIA, PRESENT, LED, Piccolo, TWINE, PRINCE, SIMON, SPECK, Midori

比較対象の既存技術：AES, Camellia

資料 3

2015 年度　暗号技術活用委員会　活動報告

１．2015 年度の活動内容

1.1　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目的の軸足を、「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、新たな活動目的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。

1.2　委員構成

暗号技術活用委員会の委員は、表 1 の通り。

1.3　今年度の委員会の開催状況

2015 年度暗号技術活用委員会は 1 回開催された。各回会合の概要は表 2 のとおり。

資料 3

表 1　2015 年度暗号技術活用委員会　委員名簿

委員長	松本　勉	横浜国立大学　大学院環境情報研究院 教授
委員	上原　哲太郎	立命館大学　情報理工学部情報システム学科 教授
委員	菊池　浩明	明治大学　総合数理学部　先端メディアサイエンス学科 教授
委員	清藤　武暢	日本銀行　金融研究所　情報技術研究センター
委員	手塚　悟	東京工科大学　コンピュータサイエンス学部 教授
委員	松本　泰	セコム株式会社　IS 研究所　コミュニケーションプラットフォームディビジョン　マネージャー
委員	満塩　尚史	内閣官房　IT 総合戦略室 政府 CIO 補佐官
委員	山口　利恵	東京大学　大学院情報理工学系研究科　ソーシャル ICT 研究センター　特任准教授
委員	山岸　篤弘	日本情報経済社会推進協会（JIPDEC）

表 2　2015 年度暗号技術活用委員会　開催概要

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

以上

資料 4

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

暗号技術検討会事務局

[議題]

本年度の第一回暗号技術検討会において、暗号技術評価委員会より「昨年度までハッシュ関数 SHA-224、 SHA-512/224、 SHA-512/256、 SHA-3 の安全性評価及び実装性能評価について評価を実施してきた。2015 年 8 月 5 日付で SHA-3 を規定した FIPS202 が発行されたことから、これらのハッシュ関数の CRYPTREC 暗号リストへの追加方針について、暗号技術検討会から提示頂きたい。」との提案があった。

これを受けて、ハッシュ関数 SHA-2, SHA-3 の CRYPTREC 暗号リストへの追加について検討を実施したため、追加の可否について、ご審議いただきたい。

[背景]

- SHA-2

  現在、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 が電子政府推奨暗号リストに掲載されている。なお、JCMVP では FIPS 180-4 全体が「承認されたセキュリティ機能」に指定されている。

表 1：FIPS 180-4 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 2007 年より米国 NIST が開始した新ハッシュ関数 SHA-3 のコンペティションの結果、2012 年 10 月に Keccak という方式が選ばれ、2014 年 4 月に SHA-3 を規定した Draft FIPS 202 が公表された。その後、SHA-3 は 2015 年 8 月に FIPS202 として正式に出版された。

[これまでの議論]

上記背景を踏まえ、暗号技術評価委員会にて、SHA-2 のうち現在電子政府推奨暗号リストから外れているアルゴリズム及び SHA-3 に関する安全性評価を昨年度より実施し、今年度の第一回 暗号技術評価委員会にて下記の審議結果を得ている。

- 暗号術評価委員会では、昨年度までに、安全性評価及び実装評価を行ってきた。これらの評価結果を踏まえ、CRYPTREC 暗号リストへの追加の可否を議論するための評価結果を十分にそろえられている。
- 評価結果に対する見解として、昨年度までに行った安全性評価および実装評価の結果を踏まえ、SHA-2 および SHA-3 に含まれるアルゴリズムは、適切な安全性・実装性能を有している。
- CRYPTREC 暗号リストへの追加対象となるアルゴリズム

  (暗号技術評価委員会承認)

  ハッシュ長が 256 ビット以上のアルゴリズムのみとする。

  SHA-2：SHA-512/256

  SHA-3：SHA3-256, SHA3-384, SHA3-512, SHAKE256※

  ※ハッシュ長は 256 ビット以上とする

(理由)

- 現版の電子政府推奨暗号リスト（平成 25 年 3 月 1 日）を選定する際に採用した評価方針として、ハッシュ関数については、ハッシュ長が 256 ビット以上であることが望ましい、としていた。(CRYPTREC Report 2012 暗号方式委員会 表 3.17 参照)
- 旧版の電子政府推奨暗号リスト（平成 15 年 2 月 20 日）では「新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。」と注釈をつけていた。

(配慮すべき点)

FIPS 180-4 で規定されている SHA-2 のアルゴリズム、FIPS 202 で規定されている SHA-3 のアルゴリズムの全てがリストの対象となっているわけではない。

上記の暗号技術評価委員会での結論を踏まえ、追加先リストやその表記方法などの論点については、重点課題検討タスクフォースで議論を行い、事務局案としてまとめた。

【審議事項】

CRYPTREC 暗号リストを資料 4 別添 1 の通り改定して良いか、審議いただきたい。

改定に関わる主な論点は以下の通り。

(論点 1)　リストへの追加対象となるアルゴリズム

(事務局案) ハッシュ長が 256 ビット以上のアルゴリズムのみとする。

SHA-2：SHA-512/256

SHA-3：SHA3-256, SHA3-384, SHA3-512, SHAKE256※

※ハッシュ長は 256 ビット以上とする

(論点 2)　追加先リスト

(事務局案)「推奨候補暗号リスト」に掲載し、然るべきタイミングで実績調査を実施し、調査結果に応じて「電子政府推奨暗号リスト」への掲載を検討する。

(論点 3)　リスト上での表記方法

(事務局案) 各々のアルゴリズムを列挙し、注釈を添える。

注釈案：ハッシュ長は 256 ビット以上とすること。

電子政府推奨暗号リスト

ハッシュ関数	SHA-256
	SHA-384
	SHA-512

推奨候補暗号リスト

ハッシュ関数	SHA-512/256
	SHA3-256
	SHA3-384
	SHA3-512
	SHAKE256(注)

(注) ハッシュ長は 256 ビット以上とすること。

資料４別添１

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）

平成２５年３月１日
総　　務　　省
経　済　産　業　省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	3-key Triple DES(注3)
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報通信担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

（注1） 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注2） より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

（注3） 3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。
1） NIST SP 800-67 として規定されていること。
2） デファクトスタンダードとしての位置を保っていること。

（注4） 初期化ベクトル長は 96 ビットを推奨する。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64 ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128 ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE256(注12)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
エンティティ認証		ISO/IEC 9798-4

（注5） KEM（Key Encapsulating Mechanism）－ DEM（Data Encapsulating Mechanism）構成における利用を前提とする。

（注6） より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

（注7） 平文サイズは 64 ビットの倍数に限る。

（注12） ハッシュ長は 256 ビット以上とすること。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号	該当なし
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		CBC-MAC(注11)
エンティティ認証		該当なし

（注8） 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注9） SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

（注10） 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。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年 3月27日	(注10)	128-bit RC4は、SSL(TLS1.0以上)に限定して利用すること。	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。
平成28年 x月xx日	推奨候補暗号リスト（技術分類：ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256
平成28年 x月xx日	(注12)	[新規追加]	ハッシュ長は256ビット以上とすること。

資料 5

2016 年度暗号技術評価委員会活動計画(案)

1. 活動目的

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。

2. 活動概要

(1) 暗号技術の安全性及び実装に係る監視及び評価

下記の通り、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・評価を実施する。

① CRYPTREC 暗号等の監視

国際会議等で発表される CRYPTREC 暗号リストの安全性及び実装に係る技術（暗号モジュールに対する攻撃とその対策も含む）に関する監視を行い、会議や ML を通して暗号技術評価委員会に報告する。

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格及び 運用監視暗号リストからの危殆化が進んだ暗号の削除

CRYPTREC 暗号リストの安全性に係る監視活動を継続的に行い、急速に危殆化が進んだ暗号技術やその予兆のある暗号技術の安全性について評価を行う。また、リストからの降格や削除、注釈の改訂が必要か検討を行う。

③ CRYPTREC 注意喚起レポートの発行

CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加

標準化動向に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を検討する。

⑤ 新技術等に関する調査及び評価

(将来的に)有用になると考えられる技術やリストに関わる技術について、安全性・性能評価を行う。必要に応じて、暗号技術調査ワーキンググループによる調査・評価、または、外部評価による安全性・性能評価などを行う。

- 引き続き、暗号技術調査ワーキンググループ(暗号解析評価)及び暗号技術調査(軽量暗号）ワーキンググループを設置する。
- 暗号技術調査ワーキンググループ(暗号解析評価)は、楕円曲線上の離散対数問題

（ECDLP）の困難性に関する調査、多重線形写像（multi-linear map）及び難読化（Obfuscation）の最新動向に関する調査、予測図の更新等を行う。

- 暗号技術調査ワーキンググループ（軽量暗号）は、2015 年度に検討した内容に基づき、ガイドラインを作成する。
- 共通鍵暗号の攻撃に関する安全性予測について検討する。

(2) 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）

- 暗号技術を利用する際の技術面での注意点に関する調査、新技術の安全性・性能に関する調査・評価を行う。
- 具体的な内容については、2016 年度第 1 回暗号技術評価委員会にて検討する。

以上

参考資料１

２０１５年度　第１回暗号技術検討会　議事概要

１．日時　平成 27 年 10 月５日（月）　10:00～12:00

２．場所　経済産業省本館 17 階　第１特別会議室

３．出席者（敬称略）

構成員：松本勉（座長）、今井正道、宇根正志、太田和夫、岡本栄司、金子敏信、佐々木良一、近澤武、手塚悟、松井充、松浦幹太、松本泰、向山友也、渡邊創

オブザーバ：太田裕介（坂本三郎　代理）、平和昌、寶木和夫、竹内英二、中村武英（村田利見　代理）、西島学（溝口浩和　代理）、西村敏信、橋本壮司（中山隆介　代理）、橋本敬史、頓宮裕貴、松永一義、松本静香（篠原俊博　代理）、吉岡達宏（木村和仙　代理）

暗号技術評価委員会事務局：盛合志帆（国立研究開発法人情報通信研究機構（NICT））

暗号技術活用委員会事務局：神田雅透（独立行政法人情報処理推進機構（IPA））

暗号技術検討会事務局：

総務省　南俊行、大森一顕、筒井邦弘、丸橋弘人、今野孝紀

経済産業省　前田泰宏、瓜生和久、上坪健治、中野辰実、中村博美

４．配付資料

（資料番号）	（資料名）
資料１－１	「暗号技術検討会」開催要綱（案）
資料１－２	暗号技術検討会の公開について（案）
資料２	「CRYPTREC の在り方に関する検討グループ」における議論結果報告書
資料３	暗号技術検討会における「重点課題検討タスクフォース」の設置について（案）
資料４	2015 年度　暗号技術検討会活動計画
資料５	2015 年度暗号技術評価委員会の活動について（案）
資料５別添	64 ビットブロック暗号 MISTY1 の安全性について
資料６	2015 年度暗号技術活用委員会の活動について（案）
参考資料１	2014 年度　第２回暗号技術検討会議事概要
参考資料２	2015 年度　暗号技術評価委員会活動計画
参考資料３	2015 年度　暗号技術活用委員会活動について（案）
参考資料４	暗号技術検討会　構成員・オブザーバ名簿

５．議事概要

１　開会

暗号技術検討会事務局から開会の宣言があり、総務省の南政策統括官から開会の挨拶が行われた。参考資料４に基づき、暗号技術検討会事務局より構成員及びオブザーバの交代（(東京大学）今井先生、(一般財団法人ニューメディア開発協会）国分様、(独立行政法人情報通信研究機構）松尾様、(日本銀行）中山様→（日本銀行）宇根様、(東京工科大学）手塚先生、(東京大学）松浦先生)、オブザーバの交代（(法務省）野口様→坂本様、(外務省）大村様→松永様、(財務省）武田様→中山様、(厚生労働省）鯨井様→橋本様、(経済産業省）和泉様→橋本様、(独立行政法人情報処理推進機構）伊藤様→頓宮様、（総務省）増田様の辞退）及び構成員の欠席（上原構成員、本間構成員、岡本龍明構成員）について説明が行われ、新たに構成員に加わった方々から挨拶があった。

２　議事

（１）2015 年度暗号技術検討会　開催要綱案等について

資料１－１及び１－２に基づき、「暗号技術検討会開催要綱（案)」及び「暗号技術検討会の公開」について事務局より説明が行われた。質疑はなし。原案のとおり承認された。構成員の互選により、座長として松本勉構成員を選任した。

（２）「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

資料２に基づき、事務局より説明が行われた。

○質疑応答

佐々木構成員：今後の IoT 社会では完全に安全であると言い切ることは出来ない。現実的にはレベル別のセキュリティの在り方の議論が必要であり、リスク評価の観点が必要である。

松本座長：確かに、例えば消費電力がかかるからといってセキュリティを低くして良いのか、ということになる。うまくバランスを取ることが大事。

宇根構成員：システムのセキュリティ要件のまとめ方は非常に難しいため、CRYPTREC 成果物が仕様書へ反映することを意識したものになることは良い。ユーザはどういう情報が必要なのかというところをヒアリングなどにより把握することが大切。また、鍵管理においても、例えば証明書が失効した際の入替え方法など、システムのライフサイクルを予め仕様書の段階から考慮しておかないと、コスト面で問題となる。

（３）「重点課題検討タスクフォース」の設置について

資料３に基づき、暗号技術検討会事務局より説明が行われた。質疑応答は以下の

とおり。原案どおりに承認された。

○質疑応答

佐々木構成員：既存のプロトコルの普及戦略についても検討内容として入れてほしい。例えば最近巷で話題のなりすまし対策における S/MIME 普及の検討や DNSSEC 等である。S/MIME は最初の認証に課題があるなど、一般への普及には困難があるが、マイナンバー制度の始まりをトリガーとして個人認証をしっかりしてほしい。

松本座長：重点課題検討タスクフォース又は、暗号技術活用委員会など、どの検討会で受け取るべきかを含めて検討したい。

宇根構成員：重点課題検討タスクフォースで決定した方向性はその後どうなるのか。

暗号技術検討会事務局：各委員会の活動計画へ反映し、次回検討会で報告する予定。

（４）2015 年度　暗号技術検討会活動計画について

資料４に基づき、暗号技術検討会事務局より説明が行われた。質疑はなし。原案のとおり承認された。

（５）2015 年度暗号技術評価委員会活動計画（案）について

資料５に基づき、暗号技術評価委員会事務局より説明が行われた。質疑応答は以下のとおり。原案のとおり承認された。

○質疑応答

金子構成員：計算量がこれぐらいだから問題が無い、というのは研究者には理解できるが、一般人もそうであるかと言われれば違う。暗号技術調査 WG（暗号解析評価）で作成している「処理能力の予測図」を参照することにより、ある時点で、1024 ビットなら NG だが、2048 ビットなら大丈夫、といった判断ができるように、MISTY1 などの共通鍵暗号系の解析にかかる計算量についても、例えば 2 の 108 乗の場合から 2 の 100 乗となった場合、計算機の処理能力が現状これぐらいだから大丈夫だ、あるいは危ない、というラインが一般人にもわかるような予測図などの表現を考えてほしい。

暗号技術評価委員会事務局：こういった表現を明快にすることは軽量暗号の受け入れにもつながる。評価委員会として検討したい。

（６）2015 年度暗号技術活用委員会活動計画（案）について

資料６に基づき、暗号技術活用委員会事務局より説明が行われた。質疑応答は以下のとおり。原案のとおり承認された。

○質疑応答

宇根構成員：SSL/TLS ガイドラインについて、非常に参考になった。感謝している。引き続きやっていただきたい。アルゴリズムの実績調査について、重点課題検討タスクフォースの検討結果を踏まえて行うとのことであるが、クラウド等において処理されるデータの機密性やプライバシーを確保する技術として高機能暗号が今後活用される場面が増えると思うが、これは活用委員会のスコープに含まれるのか。

暗号技術活用委員会事務局：実績調査はあくまでも CRYPTREC 暗号リストの改定の際に行われるものであり、高機能暗号は実績調査の対象には含まれない。しかし御指摘の点は、重点課題検討タスクフォースで行う予定の新しいニーズ調査での重要なテーマになりうると認識している。

3　閉会

経済産業省の前田審議官から閉会の挨拶が行われた。

暗号技術検討会事務局から 2015 年度第２回暗号技術検討会は３月頃の開催を予定しており、詳細な日程、場所等については、別途連絡する旨の説明が行われた。

以上

参考資料 2

暗号技術検討会　構成員・オブザーバ名簿

2016.3.29 現在

（構成員）

今井　正道	一般社団法人情報通信ネットワーク産業協会　常務理事
上原　哲太郎	立命館大学　情報理工学部情報システム学科　教授
宇根　正志	日本銀行　金融研究所情報技術研究センター　情報技術研究グループ長
太田　和夫	国立大学法人電気通信大学大学院　情報理工学研究科 総合情報学専攻（セキュリティ情報学コース）　教授
岡本　栄司	国立大学法人筑波大学大学院　システム情報工学研究科　教授
岡本　龍明	日本電信電話株式会社　セキュアプラットフォーム研究所 岡本特別研究室　室長（社団法人電気通信事業者協会代表兼務）
金子　敏信	東京理科大学　理工学部電気電子情報工学科　教授
佐々木　良一	東京電機大学　未来科学部情報メディア学科　教授
近澤　　武	独立行政法人情報処理推進機構　セキュリティセンター暗号グループ グループリーダー（ISO/IEC JTC 1/SC27/WG2 Convenor（国際主査））
手塚　　悟	東京工科大学 コンピュータサイエンス学部　教授
本間　尚文	国立大学法人東北大学大学院　情報科学研究科　准教授
松井　　充	三菱電機株式会社　情報技術総合研究所　情報セキュリティ技術部長
松浦　幹太	国立大学法人東京大学 生産技術研究所　教授
松本　　勉	国立大学法人横浜国立大学大学院　環境情報研究院　教授
松本　　泰	セコム株式会社　IS 研究所 コミュニケーションプラットフォームディビジョン　マネージャー
向山　友也	一般社団法人テレコムサービス協会　技術・サービス委員会　委員長
渡邊　　創	国立研究開発法人産業技術総合研究所 情報技術研究部門 上級主任研究員

（五十音順、敬称略）

（オブザーバ）

奥山　　剛	内閣官房内閣サイバーセキュリティセンター 内閣参事官（政府機関総合対策担当）
村田　利見	警察庁情報通信局情報管理課長
稲垣　　浩	総務省行政管理局行政情報システム企画課情報システム企画官
篠原　俊博	総務省自治行政局住民制度課長
坂本　三郎	法務省民事局商事課長
松永　一義	外務省大臣官房情報通信課長
中山　隆介	財務省大臣官房文書課業務企画室長
溝口　浩和	文部科学省大臣官房政策課情報システム企画室長
橋本　敬史	厚生労働省政策統括官付情報セキュリティ対策室長
橋本　道雄	経済産業省産業技術環境局国際電気標準課長
木村　和仙	防衛省整備計画局情報通信課サイバーセキュリティ政策室長
平　　和昌	国立研究開発法人情報通信研究機構ネットワークセキュリティ研究所長
寶木　和夫	国立研究開発法人産業技術総合研究所情報技術研究部門副研究部門長
頓宮　裕貴	独立行政法人情報処理推進機構セキュリティセンター長
竹内　英二	一般財団法人日本情報経済社会推進協会電子署名・認証センター長
西村　敏信	公益財団法人金融情報システムセンター監査安全部長

（敬称略）

参考資料３

2015 年度　第１回暗号技術検討会　資料２

「CRYPTREC の在り方に関する検討グループ」における議論結果報告書

平成 27 年 10 月５日

暗号技術検討会事務局

参考資料３

目次

参考資料３

１.「CRYPTREC の在り方に関する検討グループ」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。

本報告書では、2015 年 6 月より合計４回開催した検討グループの議論の結果と、今後の CRYPTREC の体制について報告することとする。

参考資料３

2.「CRYPTREC の在り方に関する検討グループ」概要

2.1 体制（事務局・構成員）

検討グループは、暗号技術検討会の構成員を中心に、学識経験者、暗号ユーザー、暗号研究者により構成することとし、オブザーバーに NISC の参加を得つつ、総務省、経済産業省が事務局として開催した。構成員は表１の通り。

表１　CRYPTREC の在り方に関する検討グループ　構成員名簿

	委員氏名	所属
座長	松本　勉	国立大学法人横浜国立大学　大学院環境情報研究院 教授
構成員	上原　哲太郎	立命館大学　情報理工学部情報システム学科 教授
構成員	太田　和夫	国立大学法人電気通信大学　大学院 教授
構成員	近澤　武	独立行政法人情報処理推進機構 セキュリティセンター 暗号グループグループリーダー（ISO/IEC JTC 1/SC27/WG2 Convenor（国際主査））
構成員	手塚　悟	東京工科大学 コンピュータサイエンス学部 教授
構成員	松本　泰	セコム株式会社 IS 研究所コミュニケーションプラットフォーム ディビジョンマネージャー
構成員	盛合　志帆	国立研究開発法人情報通信研究機構 ネットワークセキュリティ研究所 セキュリティ基盤研究室 室長
オブザーバー	内閣官房内閣サイバーセキュリティセンター	

事務局

総務省　情報流通行政局　情報セキュリティ対策室

経済産業省　商務情報政策局　情報セキュリティ政策室

参考資料３

2.2 開催実績

検討グループは、表２のとおり、合計４回開催した。各会合の開催日及び主な議題は以下のとおり。

表２　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今回の進め方について (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

参考資料３

3.「CRYPTREC の在り方に関する検討グループ」議論概要

3.1　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。

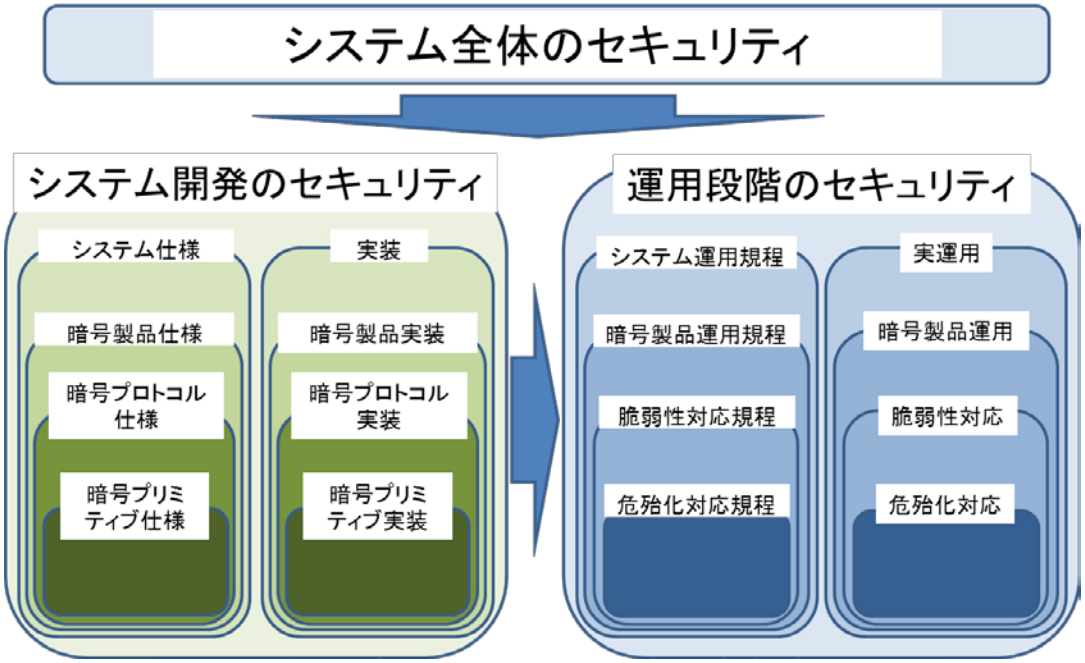
・目的：従来のミッションから変更すべきか、何を追加すべきか
・対象とする活動領域：暗号アルゴリズム等従来に加えて何を対象とするか
・主な適用範囲：電子政府に加えて一般向けの情報システムも対象とするか
・成果物：CRYPTREC 暗号リストに加え、どのような成果物が考えられるか

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。

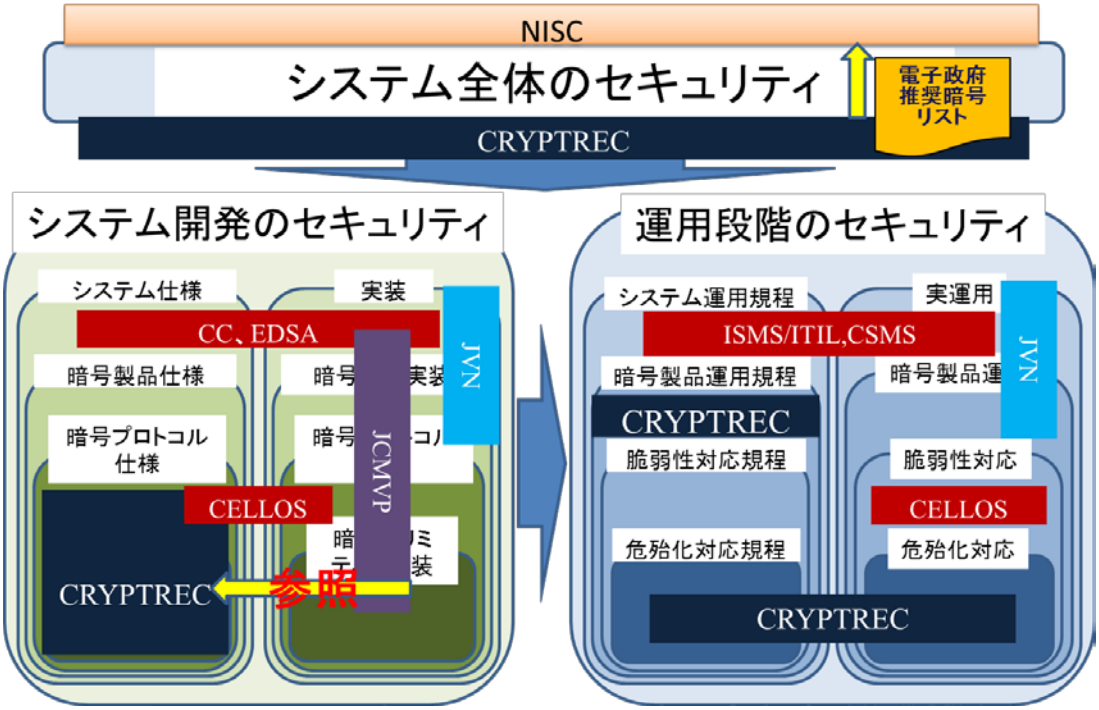
- 情報システムにおける暗号技術のセキュリティは開発及び運用段階で分けて考える必要がある
- さらにそれぞれを「仕様と実装」、「規程とその規程の実運用」とに分けて考えた方が良い
- その上で様々な暗号プリミティブ、プロトコル、製品から情報システム全体といったレイヤ別に確認が必要

上記を踏まえて以下の全体俯瞰図を作成した。

参考資料３



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以下のように行った。



※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

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。

3.2 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。

3.3 CRYPTREC が対象とする活動領域に関する議論結果概要

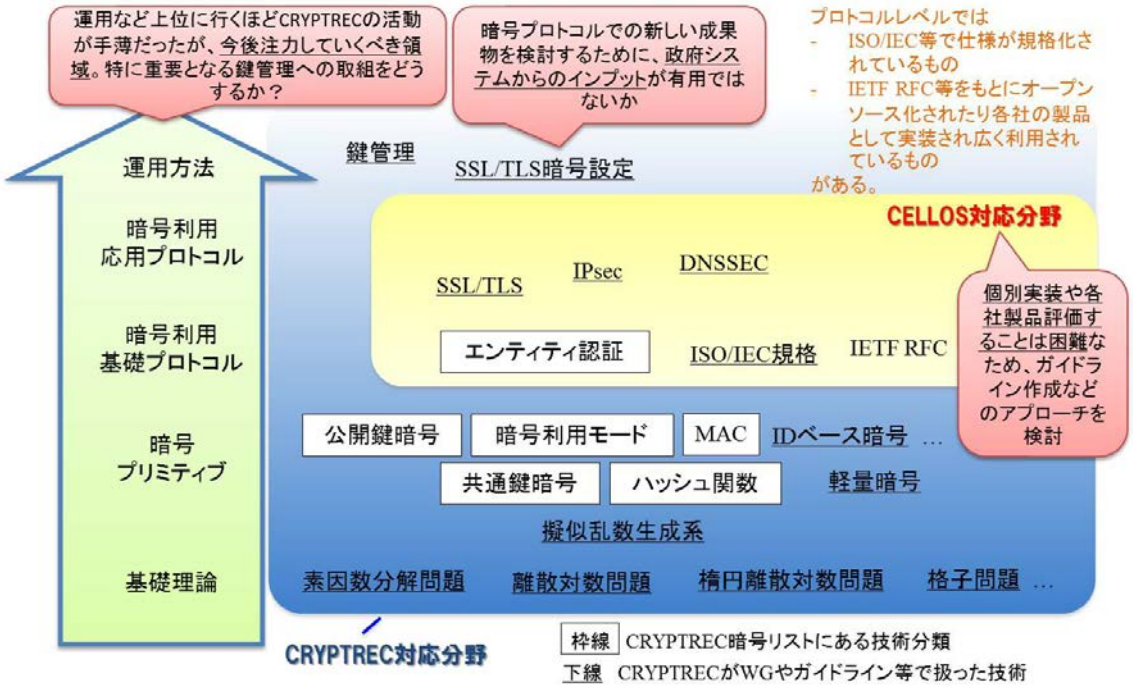
対象とする活動領域の検討について、既存の他団体の活動（プロトコルのセキュリティ評価（CELLOS)、製品（ソフトウェア）の脆弱性（JVN）等）との関係を考慮した上で各種議論がなされ、以下のような課題が整理された。

- 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。

参考資料３



（参考）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

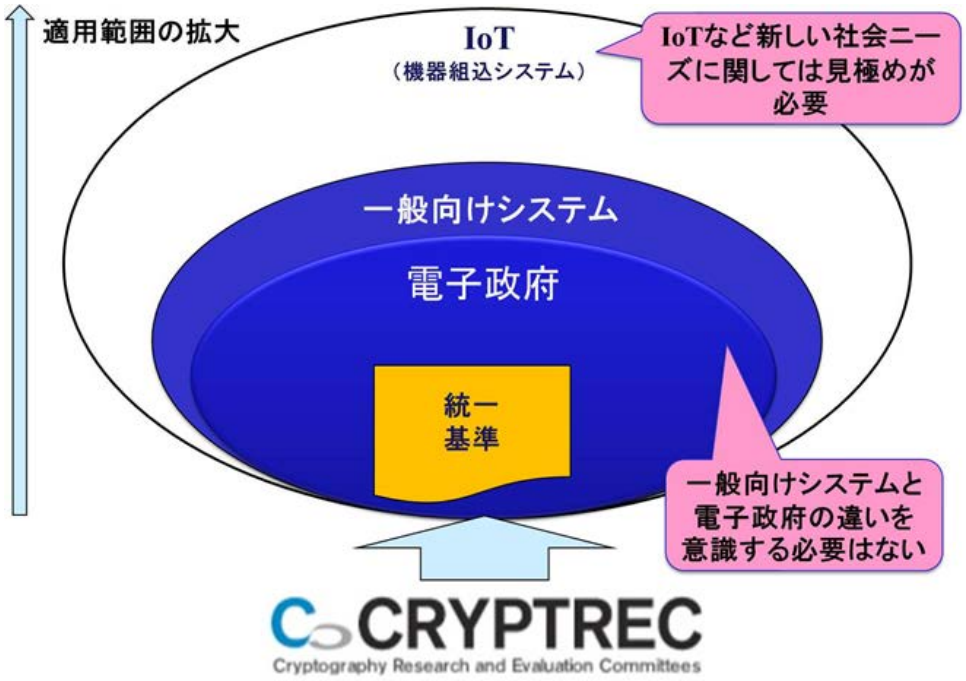
・実装や製品評価といった個別評価の分野や脆弱性対応など迅速性が要求される分野について、他団体との具体的連携を引き続き検討する
-CELLOS との脆弱性対応での連携における具体的フロー検討
-その他の団体との連携に関する必要性やその具体的フロー検討

3.4　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。

参考資料３

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）



（参考）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

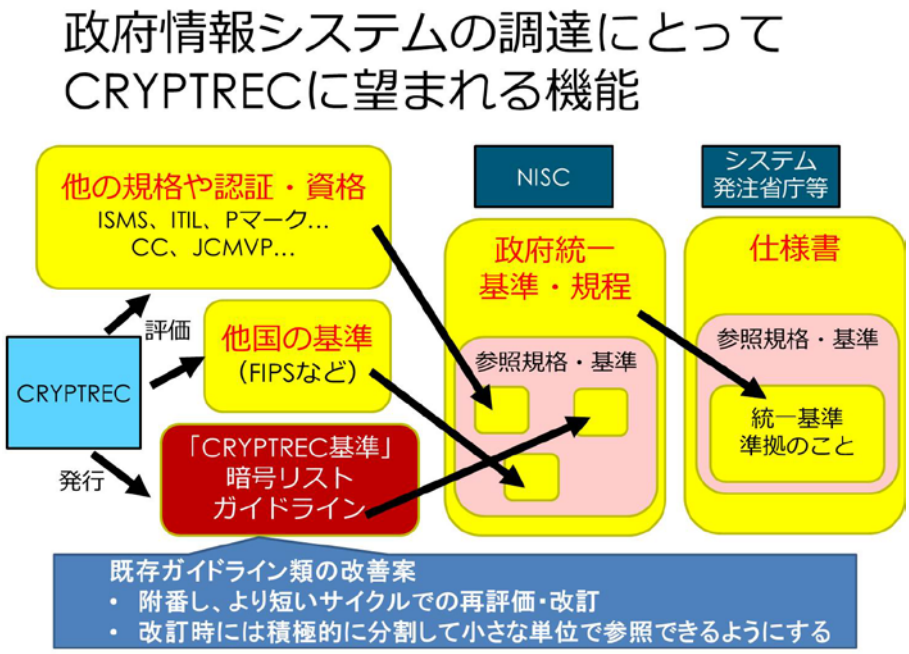
3.5　CRYPTREC の成果物に関する議論結果概要

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



（参考）政府調達と CRYPTREC 成果物のあるべき関係性イメージ

参考資料３

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

以上

参考資料4-1

第2回重点課題検討タスクフォース 資料2

CRYPTREC暗号技術活用委員会の今後の活動に向けて

平成27年12月21日

重点課題検討タスクフォース事務局

第1回TFで議論された活動方向性（論点の再整理）①

暗号技術活用委員会で取り扱う可能性があるテーマの質・対象が
従来とは大きく異なってくることが想定されることから、
暗号技術活用委員会の運営スタイルの考え方自体を再整理

「中立性・客観性」の意味合いを広げた従来とは異なる運営スタイル
での**「セキュリティ向上に役立つドキュメント類」の作成**まで
活動対象範囲を拡大する

CRYPTREC暗号
リストの改定
（利用実績調査）

※おおむねこの範囲に拡大

暗号設定ガイドライン
（具体的設定例なし）
（OSS設定例あり）
（市販製品設定例あり）

マネジメント関連の
ガイドライン
（鍵管理、リスク管理等
コンセプトガイドライン）

政策的課題・社会
ニーズ的課題の議論
（合理的な仮説提示）

- Best Practiceのドキュメント類の作成に当たっては（利害関係者でもある）**ベンダの協力**を仰いでもよいのではないか
- 大枠としての**セキュリティ評価の基本線が揺らいでいるように対外的に見えない**（＝ベンダの言いなりにならない）ようにコントロールすることが重要
- CRYPTRECとしてやるべき範囲と別組織がやるべき**範囲の切り分け**を検討
- 作成にあたった**運営スタイルの違いを考慮**し、**適切な文書体系に整理したうえで公開**すべき

論点

- 文書体系の在り方
  - 成果物の区分の仕方・構成をどう考えるか？
  - 読者の主対象をどこに置くか？
  - CRYPTRECが扱うべき範囲と
    別組織が扱うべき範囲の切り分けをどこに置くか？
  - CRYPTRECクレジットをどういう方針で扱うべきか？
  - どのような文書体系が使いやすいか？

今後の詳細検討を
どこで継続するか
要検討
（TF or 暗号技術活用
委員会？）

- 運用ガイドラインのメンテナンス方法
  - 整備すべき運用ガイドラインの対象
  - 内容更新のメンテナンスの仕組み
  - 他組織との連携方法

暗号技術活用
委員会にて検討
（暗号技術活用委員会
活動方針案）

（2015年度）暗号技術活用委員会活動内容案

- 委員をコアメンバに限定した形（10名程度）で開催
- 審議予定の内容は以下の通り
  - 2016年度暗号技術活用委員会の活動方針案の審議・承認
    - 作成すべき運用ガイドライン対象の検討
    - 委員の追加について
  - 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）のメンテナンスの検討
    - SSL/TLS市販製品での暗号設定状況の調査結果の採用是非
    - ①暗号技術活用委員会で確認・承認、②WGを組織、③CRYPTRECとしては取り扱わない、といった切り分けに関する考え方の整理

最新動向の追記・更新	ガイドライン本体の更新	Appendixの更新・扱い
• 最近のIETF動向反映	• セキュリティ例外型見直し	• 記載内容範囲の切り分け

- 2016年度に持ち越しの論点
  - CRYPTRECとしては直接活動しないが、運用ガイドラインに関連が深いテーマについて扱い
    - 他組織との連携体制（例：NCCoEのようなもの）の検討
  - 文書体系の検討（暗号技術活用委員会で扱うことになれば）

成果物の作成目的からみた区分例

成果物の作成目的からみた区分		具体的な成果物（例） ※下線部は作成したことがある成果物
①	**政府統一基準から参照**される文書	• CRYPTREC暗号リスト
②	攻撃の内容（影響範囲・対処方法等）を**早期に公開し、注意喚起**することを目的とした文書	• 注意喚起レポート
③	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な技術評価**を実施した結果をまとめた文書	• 技術報告書 • 暗号技術調査WG報告
④	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な判断**を行った結果をまとめた文書	• 暗号技術ガイドライン
⑤	委員の技術知見や外部状況等も考慮して、**主体的な判断**を行った結果をまとめた文書	• （仕様書を補完する）推奨セキュリティパラメータ設定 • 暗号運用ガイドライン（主に暗号設定に関する）
⑥	委員の技術知見や外部状況等も考慮して、セキュリティ向上のための**誘導的要素を主体的に組み入れた**文書	• 暗号運用ガイドライン（主にマネジメントに関する）
⑦	委員の技術知見に基づき、**セキュリティに係る情勢等を主体的に分析・考察**した結果をまとめた報告書	• 調査報告書
⑧	実用性を向上させるための**具体的な設定方法を紹介**した文書	• 暗号運用ガイドライン（主にAppendix / Best Practiceに関する）
⑨	**外部機関が作成・公表**する同系列の文書へのリンク	• 報告書、ガイドライン等

暗号運用ガイドラインの構成からみた区分例

汎用性が高い ⟷ 固有要件の反映が可能

抽象度が高い

詳細

General Guidelines
（政府向け、民間向けの明確な区分けをしない）

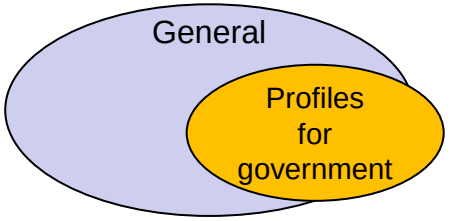
Framework
汎用的・抽象的な検討項目の提示
（※要件というより検討項目・考え方の列挙）

Introduction
ガイドラインの目的や最近動向の説明

General Requirements
必須の検討項目の提示

General Recommendations
汎用的に利用できる推奨要件の提示
（※特定の条件や環境等は考慮しない）

Best Practices
推奨要件に基づく実現例の提示
（※実現例として特定の条件や環境等を設定）



Profiles
特定の条件や環境等（政府向け、民間向け、特定用途向け等に限定）を考慮したうえでの要求項目の提示

Specific-purpose Requirements
要求項目に対応する必須要件の提示

Specific-purpose Recommendations
要求項目に対応する推奨要件の提示

Checklists
推奨要件の実装確認
（※具体的な製品・システムに関する）

NIST文書類作成の関連組織

NIST National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC: GO
CONTACT SITE MAP
Computer Security Division
Computer Security Resource Center

PUBLICATIONS

NIST publishes standards, guidelines, recommendations and research on computer/cyber/information security and privacy using the following NIST technical series. Publication drafts are available for public comment

- Federal Information Processing Standards (FIPS): security standards;
- NIST Special Publications (SPs): security and privacy guidelines, recommendations and reference materials. These include SP 800 subseries (computer security), SP 1800 subseries (NIST Cybersecurity Practice Guides) and selected SP 500-series (information technology) publications directly relevant to computer/cyber/information security and privacy;
- NIST Interagency or Internal Reports (NISTIRs): reports of research findings and background information for FIPS and SPs; and
- Information Technology Laboratory (ITL) Bulletins: monthly overviews of NIST's security and privacy publications, programs and projects.

Sponsored by DHS/NCCIC/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

National Checklist Program Repository

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms.

Search CVE and CCE Vulnerability Database

(Advanced Search)
Keyword search: Search

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
NIST National Institute of Standards and Technology U.S. Department of Commerce

Projects

Overview

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available and open source technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, end-to-end reference designs that are broadly applicable and repeatable.

Use Cases Versus Building Blocks

The center works on use cases, which are sector-specific cybersecurity problems, and building blocks, which address technology gaps affecting multiple sectors.

Final Products

When a project is completed, the NCCoE facilitates rapid, widespread adoption of secure technologies by publishing NIST Cybersecurity Practice Guides (Special Publication series 1800), which include all of the information and instructions needed to deploy a reference design.

Partners

The NCCoE has joined with a variety of U.S. companies through a formal initiative called the National Cybersecurity Excellence Partnership (NCEP). These partners have pledged to provide hardware, software and expertise to our mutual efforts to advance the rapid adoption of secure technologies. In addition to contributing equipment and other products to the NCCoE's test environments, companies may designate guest researchers to work at the center in person or remotely.

We are pleased to work with:

Akamai, ca technologies, cisco, FireEye, hp, HYTRUST, IDW, intel, JUNIPER, Lookout, Lumeta, McAfee, Microsoft, NEXTLABS, paloalto, Ping identity, Pulse Secure, redhat, RSA, splunk>, Symantec, tripwire, VANGUARD, VENAFI

参考：NIST文書類での予想分類例(1)

※ NIST文書類の一部をタイトル名からP.3の区分に当てはめて分類した時の予想分類例

成果物の作成目的からみた区分		予想分類例
①	**政府統一基準から参照**される文書	• **（必須）FIPS** • **（ガイドライン）Special Publication (SP)**
②	攻撃の内容（影響範囲・対処方法等）を**早期に公開し、注意喚起**することを目的とした文書	• なし（あえていえばNews／Announcement）
③	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な技術評価**を実施した結果をまとめた文書	• **NIST Internal/Interagency Report (NISTIR)** NISTIR7427 6th Annual PKI R&D Workshop "Applications-Driven PKI" Proceedings NISTIR7539 Symmetric Key Injection onto Smart Cards NISTIR7896 Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition
④	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な判断**を行った結果をまとめた文書	• **FIPS Appendix／change notice** FIPS186-4 Appendix D: Recommended Elliptic Curves for Federal Government Use • **NIST SP800シリーズ** SP800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications SP800-107 Recommendation for Applications Using Approved Hash Algorithms SP800-108 Recommendation for Key Derivation Using Pseudorandom Functions
⑤	委員の技術知見や外部状況等も考慮して、**主体的な判断**を行った結果をまとめた文書	• **NIST SP800シリーズ** SP800-133 Recommendation for Cryptographic Key Generation SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths SP800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations SP800-77 Guide to IPsec VPNs SP800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i SP800-111 Guide to Storage Encryption Technologies for End User Devices
⑥	委員の技術知見や外部状況等も考慮して、セキュリティ向上のための**誘導的要素を主体的に組み入れた**文書	• **NIST SP800シリーズ** SP800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach SP800-53 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans SP800-114 User's Guide to Securing External Devices for Telework and Remote Access SP800-128 Guide for Security-Focused Configuration Management of Information Systems SP800-130 A Framework for Designing Cryptographic Key Management Systems SP800-152 A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)

参考：NIST文書類での予想分類例(2)

※ NIST文書類の一部をタイトル名からP.3の区分に当てはめて分類した時の予想分類例

成果物の作成目的からみた区分		予想分類例
⑦	委員の技術知見に基づき、**セキュリティに係る情勢等を主体的に分析・考察**した結果をまとめた報告書	• **NIST Internal/Interagency Report (NIST IR)** NISTIR7816 2011 Computer Security Division Annual Report NISTIR7956 Cryptographic Key Management Issues & Challenges in Cloud Services NISTIR7966 Security of Automated Access Management Using Secure Shell (SSH) NISTIR8014 Considerations for Identity Management in Public Safety Mobile Networks • **NIST SP800シリーズ** SP800-145 The NIST Definition of Cloud Computing SP800-176 2014 Computer Security Division Annual Report • **White paper（NIST NCCoE Program）** DATA INTEGRITY - Reducing the impact of an attack
⑧	実用性を向上させるための**具体的な設定方法を紹介**した文書	• **SP800シリーズ（National Checklist Program）** SP800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers • **SP1800シリーズ（NIST NCCoE Program）** SP1800-1 Securing Electronic Health Records on Mobile Devices (DRAFT) SP1800-5 IT Asset Management (DRAFT)
⑨	**外部機関が作成・公表**する同系列の文書へのリンク	• **National Vulnerability Database (NVD)**

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

FIPS

13. Waiver Procedure: The Federal Information Security Management Act (FISMA) does not allow for waivers to a FIPS that is made mandatory by the Secretary of Commerce.

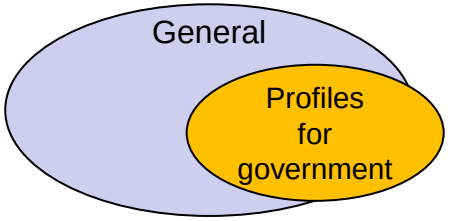
SP

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

参考：ガイドラインの構成例（米国）

For General
（政府・民間の区分けなし）
- SP800-153 Guidelines for Securing Wireless Local Area Networks (WLANs)
- SP800-144 Guidelines on Security and Privacy in Public Cloud Computing
- SP800-119 Guidelines for the Secure Deployment of IPv6
- SP800-88 Guidelines for Media Sanitization
- SP800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

For Non-federal
（民間向け）
- SP800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- SP800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise



For Federal
（政府向け）
- SP800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- SP800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Framework
- SP800-130 A Framework for Designing Cryptographic Key Management Systems

General Recommendations
- SP800-57 Recommendation for Key Management: Part 1: General

Profiles
- SP800-152 A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)

Best Practices
- SP800-57 Recommendation for Key Management: Part 2: Best Practices for Key Management Organization Part 3: Application-Specific Key Management Guidance
- SP1800-1 Securing Electronic Health Records on Mobile Devices
- SP1800-5 IT Asset Management

Checklists
- SP800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
- SP800-69 Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist

参考：ガイドラインの構成例（米国）

■ Practice Guide（SP1800シリーズ）

NIST Special Publication 1800-1b

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Health IT Sector

DRAFT

Gavin O'Brien
Nate Lesser
National Cybersecurity Center of Excellence
Information Technology Laboratory

Brett Pleasant
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

Colin Bowers
Kyle Kamke
Ramparts, LLC
Clarksville, MD

Leah Kauffman, Editor-in-Chief

340 **4.6 Technologies**

341 In January 2013, the NCCoE issued a call in the Federal Register to invite technology providers
342 with commercial products that could meet the desired security characteristics of the mobile
343 device use case to submit letters of interest describing their products' relevant security
344 capabilities. In April of 2013, the center hosted a meeting for interested companies to
345 demonstrate their products and pose questions about the project. Companies with relevant
346 products were invited to sign a Cooperative Research and Development Agreement with NIST,
347 enabling them to participate in a consortium to build a reference design that addresses the
348 challenge articulated in the use case.

349 Table 3 lists all products and the participating companies and open-source providers used to
350 implement the security requirements in Table 2. The CSF aligns with existing methodologies
351 and aids organizations in expressing their management of cybersecurity risk. The complete
352 mapping of representative product to security controls can be found in NIST SP 1800-1d,
353 Standards and Controls Mapping, Section 5.

ACKNOWLEDGEMENTS

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

Name	Organization
Curt Barker	NIST
Doug Bogia	Intel
Robert Bruce	Medtech Enginuity
Lisa Carnahan	NIST
Verbus Counts	Medtech Enginuity
Sally Edwards	MITRE
David Low	RSA
Adam Madlin	Symantec
Mita Majethia	RSA
Peter Romness	Cisco
Steve Schmalz	RSA
Ben Smith	RSA
Matthew Taylor	Intel
Steve Taylor	Intel
Jeff Ward	IBM (Fiberlink)
Vicki Zagaria	Intel

Table 3: Participating Companies and Contributions Mapped to Controls

CSF Function	Company	Application/Product	Use
Identify (ID)	RSA	Archer GRC	centralized enterprise, risk and compliance management tool
Protect (PR)	MedTech Enginuity	OpenEMR	web-based and open source electronic health record and supporting technologies
	open source	Apache Web Server	
	open source	PHP	
	open source	MySQL	
	open source	ModSecurity	Apache module extension, web application firewall (supporting OpenEMR)
	open source	OpenSSL[34]	cryptographically secures transmissions between mobile devices and the OpenEMR web portal service
	Various	mobile devices	Windows, IOS and Android tablets
	Fiberlink	MaaS360	Cloud-based mobile device policy manager
	open source	iptables firewall	stateful inspection firewall
	open source	secure configuration manager / Puppet Enterprise	creation, continuous monitoring, and maintenance of secure server and user hosts
	Cisco	local and remote mobile NAC (Identity Services Engine)	radius-based authentication, authorization and accounting management server
	Cisco	VPN server (ASAv 9.4)	enterprise class virtual private network server based on both TLS and IPSEC
	open source	URbackup	online remote backup system used to provide disaster recovery
	Cisco	wireless access point (RV220W)	Wi-Fi access point

参考：CRYPTRECシンポジウム2013公開資料（抜粋）

5. 将来に向けた展望：文書番号体系の確立とCRYPTREC暗号リストの改定に伴う修正

文書番号体系の確立

- リストガイドを参照しやすくするため、統一的な番号体系を採用し文書番号を付与する

＜文書番号＞::=＜略称＞”-”＜カテゴリ＞”-”＜連番＞
例：CUG-A-003

- 一度付与された連番は，文書の改訂では変更しない
- 改訂における考え方
  - 改訂年度などの情報を入れる（ISO方式）⇒　例：CUG-A-003-2013
  - バージョンを文書に付与する（NIST SP800方式）⇒　例：CUG-A-003 Rev.1

CRYPTREC暗号リスト改定に伴う修正

- CRYPTREC暗号リストの改訂に伴い、これまでに作成したリストガイドを修正する
  - 新しい体系（電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リスト）に対応した内容の追記

参考資料4-2-1

第3回重点課題検討タスクフォース 資料2－1

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

平成28年2月3日

重点課題検討タスクフォース事務局

暗号アルゴリズムの脆弱性に関するCRYPTRECからの情報発信の分類

情報分類	速報の必要性	過去の事例
A. 暗号アルゴリズムの**完全な危殆化**による緊急対応	高	該当なし (イメージ：世界中で使われている暗号アルゴリズムが1台PC で1時間で解読可能など)
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**	中	MISTY1へのintegral attack，SHA-1 free-start collision攻撃など
C. 長期的なシステムの安全性維持のための対策喚起	低	
D. 対応不要	無	

情報発信の手段

情報分類	速報	安全性評価	監視報告 (CRYPTREC Report, 技術報告書等)
A. 暗号アルゴリズムの**完全な危殆化**による緊急対応	実施	実施	実施
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**	実施	実施	実施
C. 長期的なシステムの安全性維持のための対策喚起	無	状況により判断	実施
D. 対応不要	無	非対象	非対象

公開資料の位置づけ

- **速報**
  外部で公開されている情報に基づき記載する
  情報源は信頼に足る機関・組織等とする
  CRYPTRECでは詳細評価していないことを明示する

- **安全性評価報告**
  CRYPTREC として安全性評価を実施する
  CRYPTREC で評価した報告内容であることを明示する
  公開までの期間は、脆弱性の内容に依る

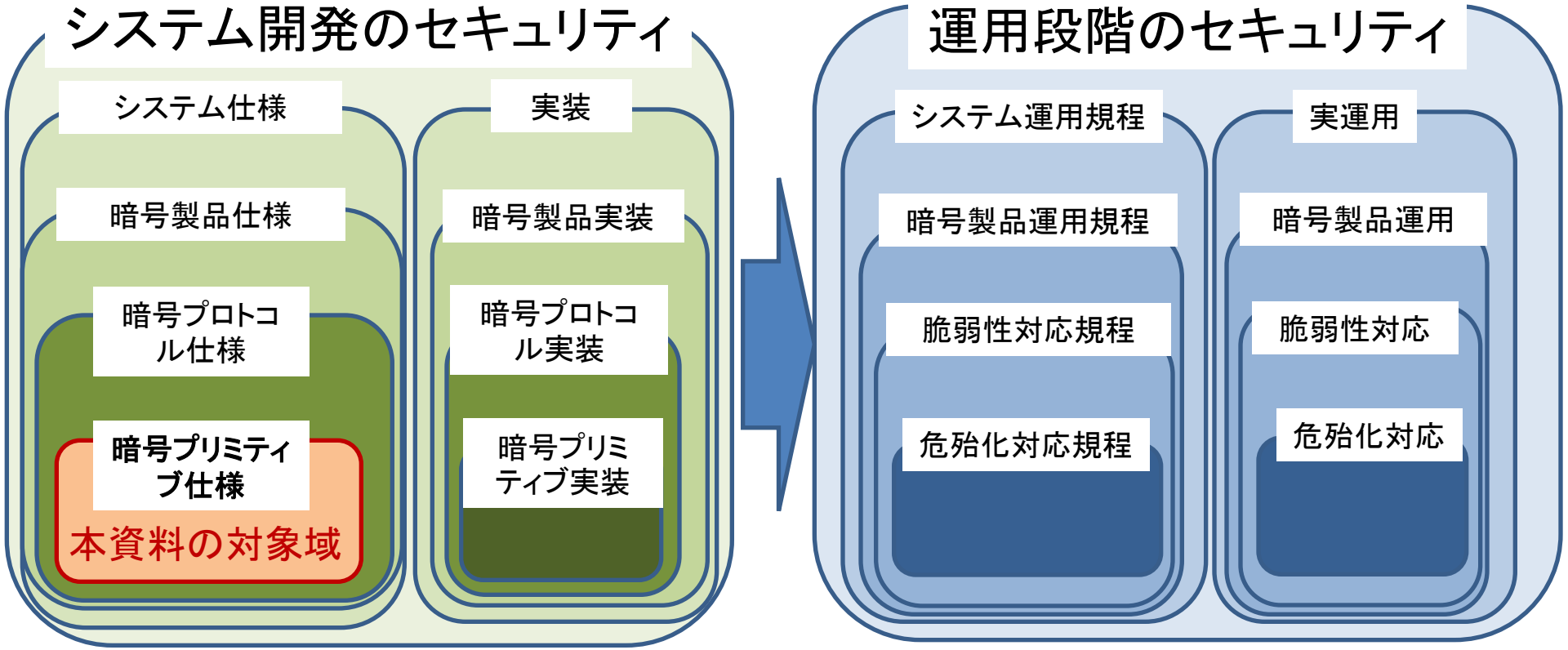
全体フロー図は資料2-2参照

以下参考

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

〇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あり
〇さらにそれぞれ仕様と実装、規程とその規程の実運用とに分けて考えた方が良い
〇その中で様々な暗号プリミティブ、プロトコル、製品からシステム全体といったレイヤ別に確認必要

システム全体のセキュリティ



第4回あり方委員会資料からの抜粋(2015年8月3日)

検討項目

「**暗号アルゴリズム**の脆弱性」の定義	暗号アルゴリズムに対する攻撃計算量の著しい低下 - CRYPTRECにおいて参照している仕様に対する攻撃成功 - 上記までいかないが、上記攻撃の計算量低下につながりうる結果	
確認すべき暗号の範囲	◇CRYPTREC暗号リストに掲載されている暗号技術 ◇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	
緊急時業務の検討事項案	(1) 緊急対応を開始する契機（アラームトリガー）	緊急対応を開始する契機となる事象 （緊急対応を開始する緊急度の目安を含む）
	(2) 緊急対応時に執る行動（アクション）	アラームトリガーを受けての行動
	(3) 緊急対応時に検討するべき事項（役割）	アクションにおける所要の作業内容
	(4) 想定検討期間	役割の遂行に要する期間の目安
	(5) 委員会等からのアウトプット	委員会等から外部へ伝達すべき事項 （外部との連携に要する事項を含む）
情報発信フロー	暗号アルゴリズムの脆弱性に関する情報発信の意思決定フロー	

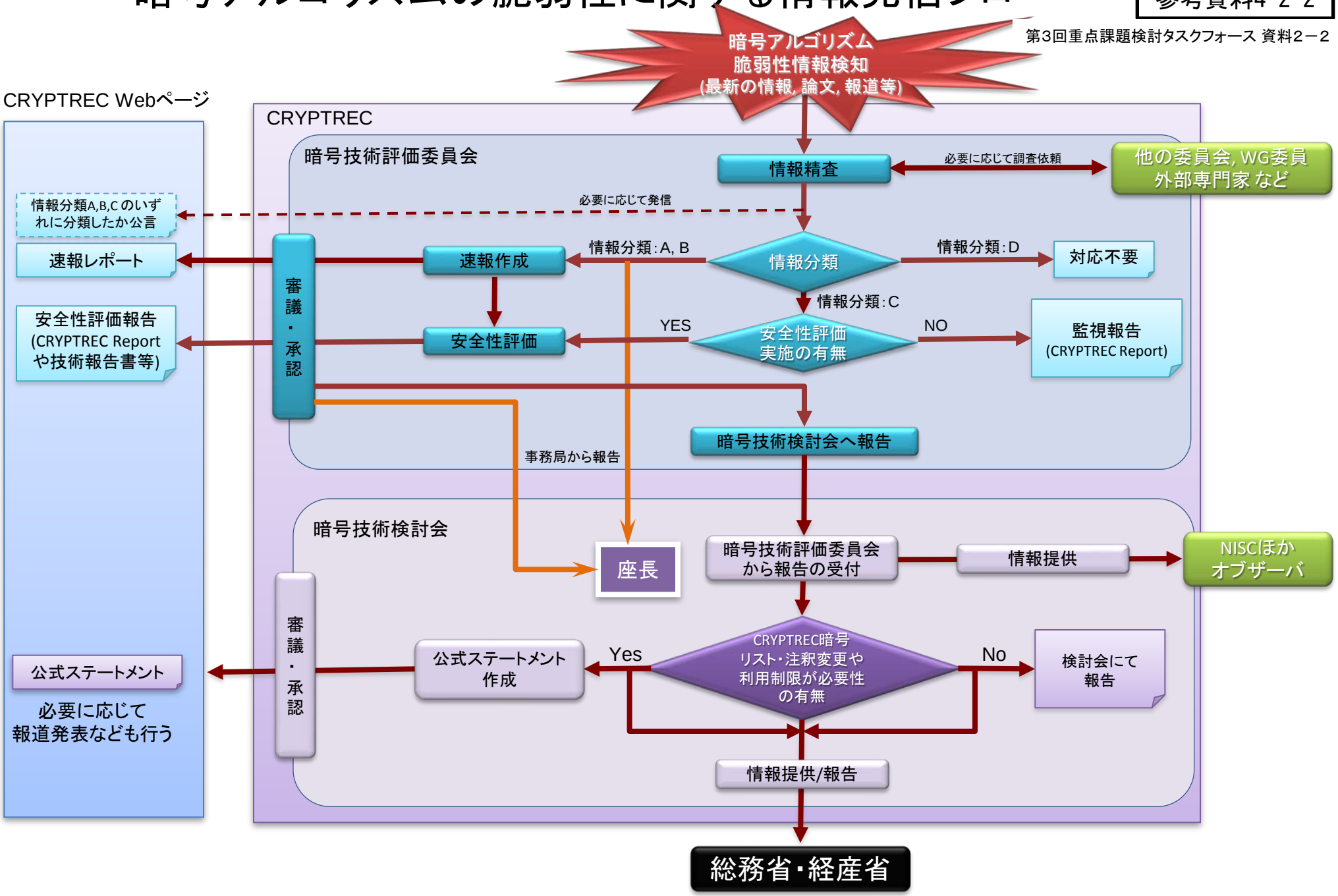
暗号アルゴリズムの安全性低下時における緊急対応

	暗号技術評価委員会	暗号技術検討会
通常業務	◇暗号技術のセキュリティに関する監視・評価等 ◇暗号リストを中心とした暗号技術のセキュリティ評価・監視	◇暗号技術に関する調査・検討 ◇CRYPTREC活動計画の承認 ◇各種成果物の承認
緊急対応を開始する契機（アラームトリガー）	◇緊急性が高いと思われる脆弱性の発生 （最新情報、論文、報道等）	◇暗号技術評価委員会からの報告・通知
緊急対応を開始する緊急度の目安	◇CRYPTREC暗号リストに掲載されている暗号技術に対する攻撃計算量の著しい低下 ◇CRYPTREC暗号リストに掲載されていないが影響度が高いと考えられる暗号技術の安全性低下	◇CRYPTREC暗号リストや注釈に影響を与える可能性があるか ◇その暗号技術の利用制限について各政府機関に周知する必要性があるか
緊急対応時に取る行動	◇暗号技術評価委員会の開催（委員長判断でメール審議も可） ◇委員長判断で他の委員会/WGの委員・外部専門家への調査依頼	◇暗号技術検討会の開催（座長判断でメール審議も可） ◇必要に応じ各委員会の委員や専門家を招聘
緊急対応時に検討するべき事項	◇事項の事実関係の確認 ◇内容の精査（信ぴょう性など） ◇論文等の情報源の詳細精査 ◇技術的確認、検証、追認 ◇技術的安全性の評価、判定（影響度や緊急性など）	◇暗号技術評価委員会が提示する安全性の低下度合いや緊急度に基づき、一般的な実利用状況や代替暗号の有無等の実情を踏まえ、「緊急にCRYPTREC暗号リストや注釈を変更する必要性があるか、利用制限すべき必要性があるか否か」を検討 ◇暗号技術委員会としてのステートメント検討・作成
想定検討期間	状況に応じて適切に設定	状況に応じて適切に設定
委員会としてのアウトプット（外部との連携）	◇重点課題検討TF及び暗号技術検討会座長への報告・通知 ◇暗号技術評価委員会としての技術情報の外部発表（危険度や緊急性に応じて）	◇総務省・経産省への報告 ◇公式ステートメントの発表 ◇NISCほかオブザーバメンバーへの情報提供

暗号アルゴリズムの脆弱性に関する情報発信フロー

参考資料4-2-2

第3回重点課題検討タスクフォース 資料2－2



参考資料4-3

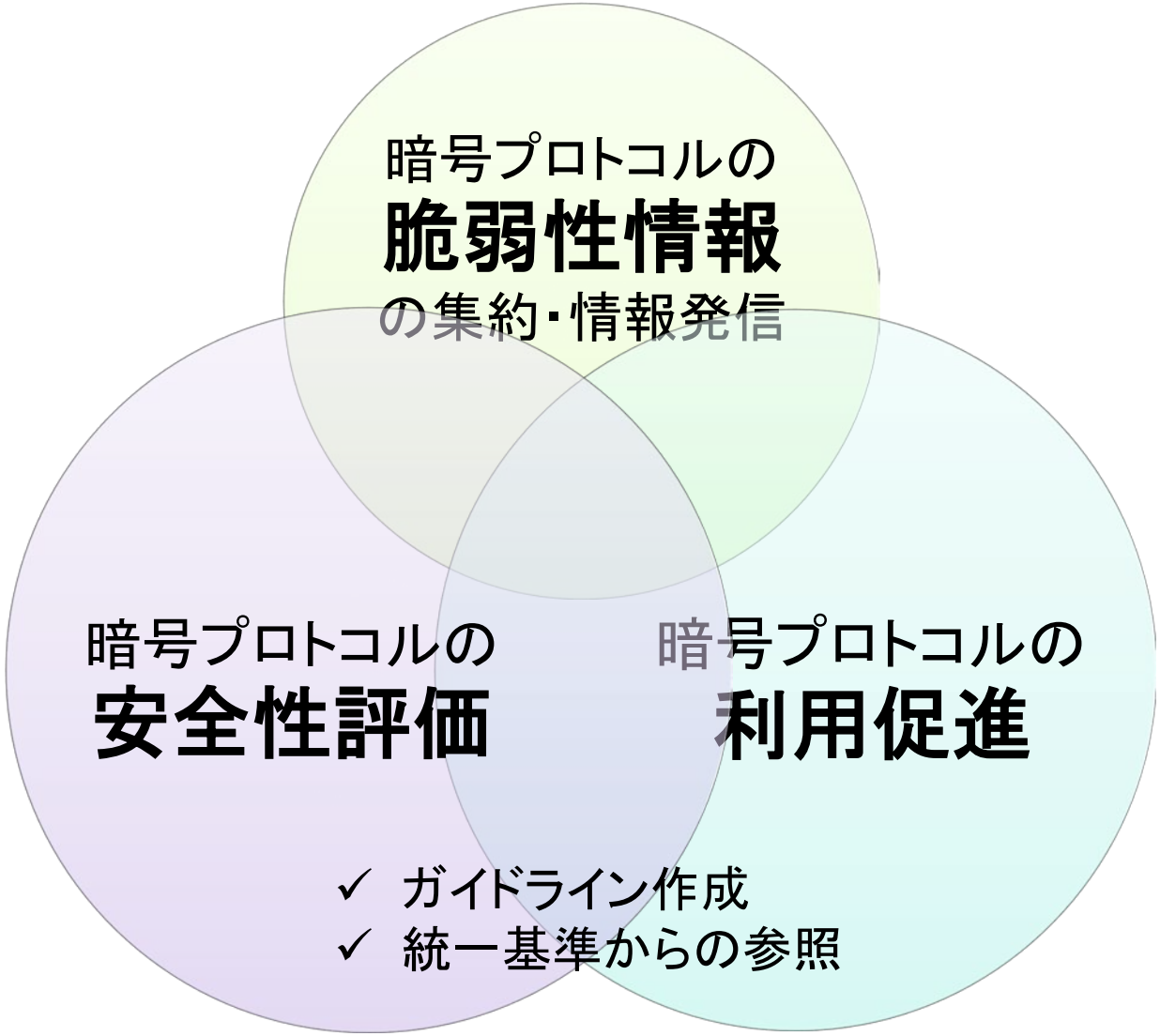
第3回重点課題検討タスクフォース 資料3

暗号プロトコルのセキュリティ確保に向けた活動案

平成28年２月３日

重点課題検討タスクフォース事務局

［再掲］CRYPTRECに求められる暗号プロトコル関連のアウトプット



[再掲]課題整理
①暗号プロトコルの脆弱性情報の集約・情報発信

- 「暗号プロトコルに関する脆弱性情報」としてどのレベルまで情報収集・発信を行うか
  - プロトコル仕様レベル, プロトコル実装レベル, システムレベル…
- どのような情報発信を行うか
  - 外部情報へのリンクのみか、CRYPTREC自身でも評価するか
- どのような体制で実施するか
  - CRYPTREC窓口は？　他機関との連携は？

暗号プロトコルの脆弱性情報の集約・発信の整理

団体	ポリシー	監視	評価	発信
（例）CELLOS	速報性重視	有識者がボランティアベースで社会的影響力のある脆弱性情報に対して日々監視を行う	有識者がボランティアベースで迅速に議論	速報として発信
CRYPTREC活動案（A）	CRYPTRECのチャネルを活かしてタイムリーに発信	他組織より情報を受ける	他組織より情報を受ける	外部情報へのリンクが中心のポータル機能を提供
CRYPTREC活動案（B）	正確性を重視技術的な安全性評価	学会, Web, 他組織等から情報を得る	専任のリソースによる詳細評価	詳細な評価情報を提供

CRYPTRECに求められることは

速報　＜　詳細な評価

暗号プロトコルの「詳細評価」のポイント整理

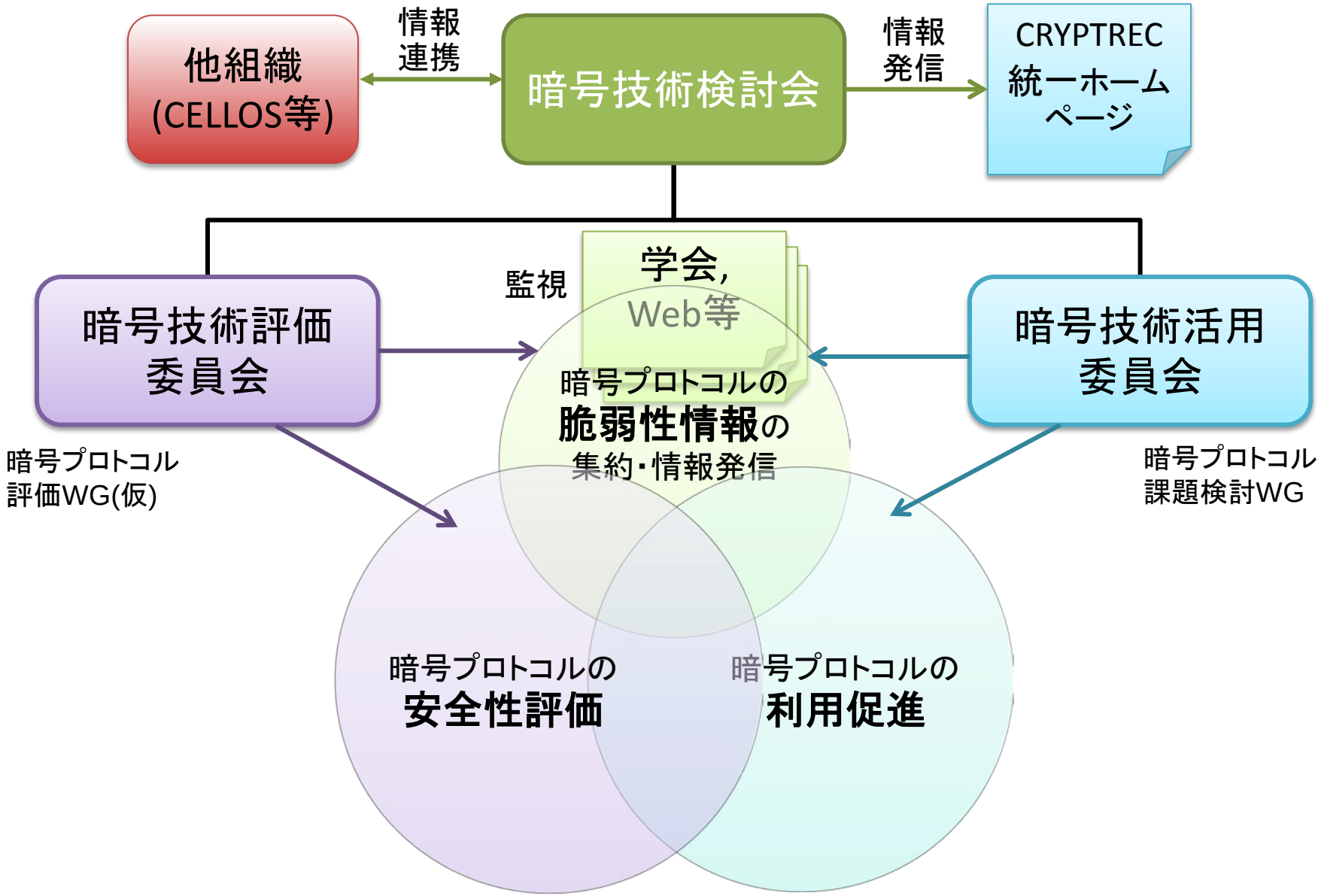
	Who ア)監視/イ）評価/ウ）発信	What 対象		How 情報の入手法
Protocol	暗号技術活用委員会， 暗号技術評価委員会 が連携して実施	電子政府？ ※議論が必要		学会やWebから一次情報を探す／取りに行く、に加え 評価結果を他有識者団体 より受け取る
		仕様	実装	
Primitive	暗号技術評価委員会	CRYPTREC 暗号リスト		学会やWebから一次情報を探す／取りに行く
		仕様	実装	

②暗号プロトコルの安全性評価
③利用促進に向けて何を対象とするか
に関する課題整理

現在の電子政府システムやその他のシステムで活用されている暗号プロトコルの利用状況の調査が必要
（手塚構成員御意見（第2回TF））

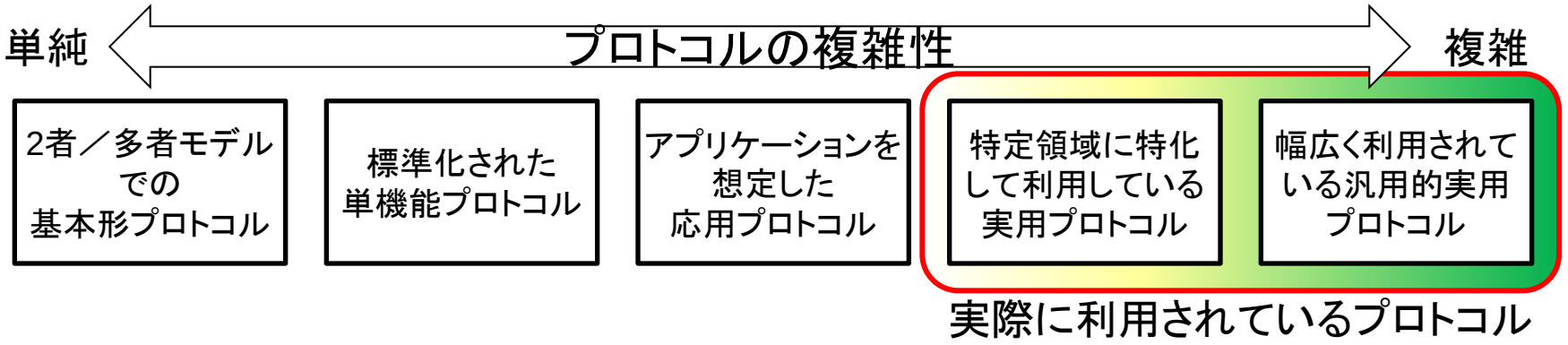
暗号プロトコルの安全性評価について対象及び出口について方向性を決める必要がある

暗号プロトコルに関するCRYPTREC体制案



暗号技術活用委員会の活動概要（案）

- 暗号プロトコル課題検討WG（2016年度 3回開催予定）
  - CRYPTRECとして扱うべき暗号プロトコルの対象範囲の集中検討



  - 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
    - 運用ガイドラインごとにばらつきが大きく出ないような安全性情報や脆弱性情報の取り扱いルールの明確化
    - 運用ガイドラインに含める脆弱性情報の範囲
    - 安全性情報や脆弱性情報を提供してもらう組織、同種ガイドラインを作成している組織、ガイドラインの主要な利用ユーザと想定される組織等との連携方法

  - 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
    - 運用ガイドライン（〇〇プロトコル）WGに衣替えを想定

暗号プロトコルの安全性評価について

- 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