2015 年度　第１回暗号技術検討会

日時：平成 27 年 10 月 5 日(月)10:00～12:00
場所：経済産業省本館 17 階　第 1 特別会議室

議　事　次　第

１．開　会

２．議　事
(1) 暗号技術検討会開催要綱等について【審議事項】
(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【報告事項】
(3)「重点課題検討タスクフォース」の設置について【承認事項】
(4) 2015 年度　暗号技術検討会活動計画について【確認事項】
(5) 2015 年度暗号技術評価委員会の活動について【報告事項、承認事項】
(6) 2015 年度暗号技術活用委員会の活動について【報告事項、承認事項】
(7) その他

３．閉　会

（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の活動について（案）
参考資料４	暗号技術検討会　構成員・オブザーバ名簿

資料１－１

「暗号技術検討会」開催要綱(案)

１　名　称

本検討会は「暗号技術検討会」（以下「検討会」という。）と称する。

２　開催の趣旨・目的

検討会は、総務省政策統括官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する。

３　検討事項

（１）CRYPTREC 暗号リスト掲載暗号技術の監視

（２）CRYPTREC 暗号リスト掲載暗号技術の安全性及び信頼性確保のための調査・検討

（３）CRYPTREC 暗号リストの改定に関する調査・検討

（４）CRYPTREC 暗号リスト掲載暗号技術の普及促進及び暗号技術の利用促進・産業化に向けた取組の検討

（５）その他、システム全体のセキュリティ確保のために必要となる活動の検討等 、暗号技術の評価及び利用に関すること

４　構成等

（１）検討会の構成は、別紙のとおりとする。

（２）検討会には、座長１名を置く。

（３）座長は、構成員の互選により定める。

（４）座長は、検討会構成員の中から顧問及び座長代理を指名できる。

（５）構成員の任期は 委嘱時に定めるもの とし、再任を妨げないものとする。

５　運　営

（１）座長は、検討会の議事を掌握する。

（２）座長が、緊急の理由によりやむを得ず不在となった場合、座長代理が座長に代わり議事を掌握する。

（３）関係する政府機関等で、座長が特に認めたものについては、オブザーバとして検討会に出席することができる。

（４）座長が必要と認めるときは、暗号技術の提案者、関連する利害関係者その他の参考人から意見を聴取することができる。

（５）座長は、検討会が調査する事項について特に専門的な調査を行う必要があると認めるときは、委員会等を置くことができる。

（６）座長は、必要があると認めるときは電子メールによる審議を行うことができる。なお、この審議を行った場合は、次の検討会において当該審議の結果を報告するものとする。
（７）その他検討会の運営に関し必要な事項は、座長が定めるところによる。

６　スケジュール

検討会は、年度内に１回以上 開催する。

７　庶　務

検討会の庶務は、総務省情報流通行政局情報セキュリティ対策室及び経済産業省商務情報政策局情報セキュリティ政策室において処理する。

資料１－２

暗号技術検討会の公開について（案）

１　会議の公開について

（１）民間企業の暗号技術（既製品を含む）の解読方法等について議論を行う可能性があり、当事者又は第三者の権利、利益や公共の利益を害するおそれがあるため、検討会は原則非公開とする。

（２）検討会の出席者は、検討会において知り得た情報で、当事者又は第三者の権利、利益や公共の利益を害するおそれがあるものについては、検討会の出席者及び座長が特に認めた者以外に漏えいしてはならないものとする。

２　検討会の資料の公開について

（１）検討会の資料については、原則公開とする。

（２）ただし、検討会の資料を公開することにより、当事者又は第三者の権利、利益や公共の利益を害するおそれがある場合は、検討会は資料の公開を延期又は非公開とすることができる。

（３）資料は、事務局により閲覧その他の方法により公開するものとする。

３　議事概要の公開について

（１）議事概要については、原則公開とする。

（２）ただし、議事概要を公開することにより、当事者又は第三者の権利、利益や公共の利益を害するおそれがある場合は、議事概要の該当部分を削除した上で公開することができる。

（３）議事概要は、事務局により閲覧その他の方法により公開するものとする。

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

資料２

目次

資料２

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。

資料２

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

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

資料２

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。

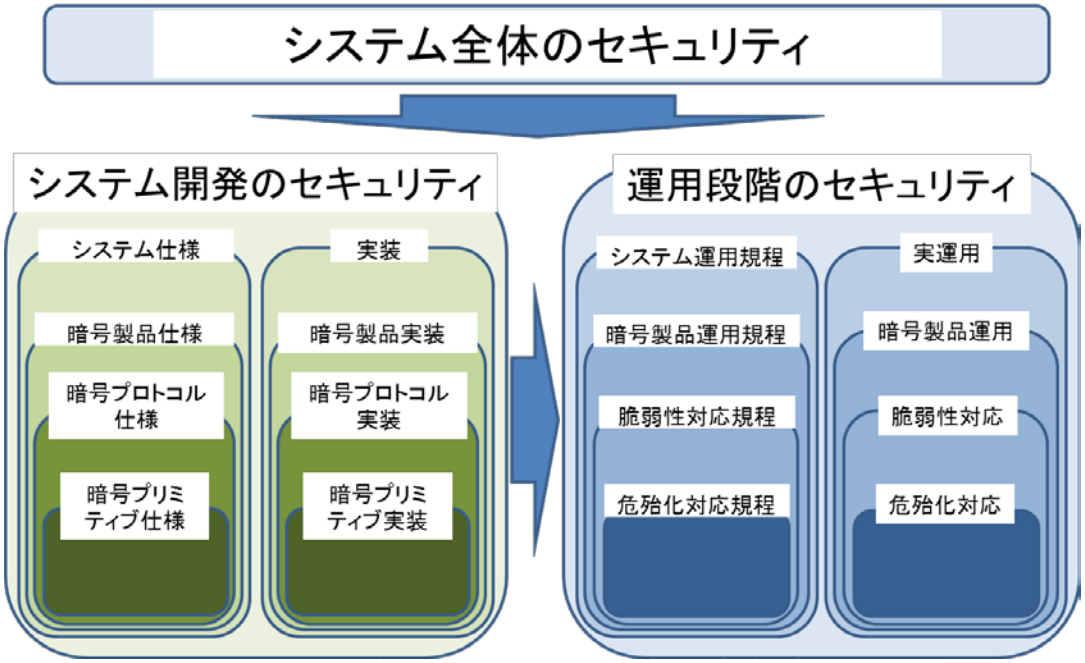
・目的：従来のミッションから変更すべきか、何を追加すべきか
・対象とする活動領域：暗号アルゴリズム等従来に加えて何を対象とするか
・主な適用範囲：電子政府に加えて一般向けの情報システムも対象とするか
・成果物：CRYPTREC 暗号リストに加え、どのような成果物が考えられるか

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。

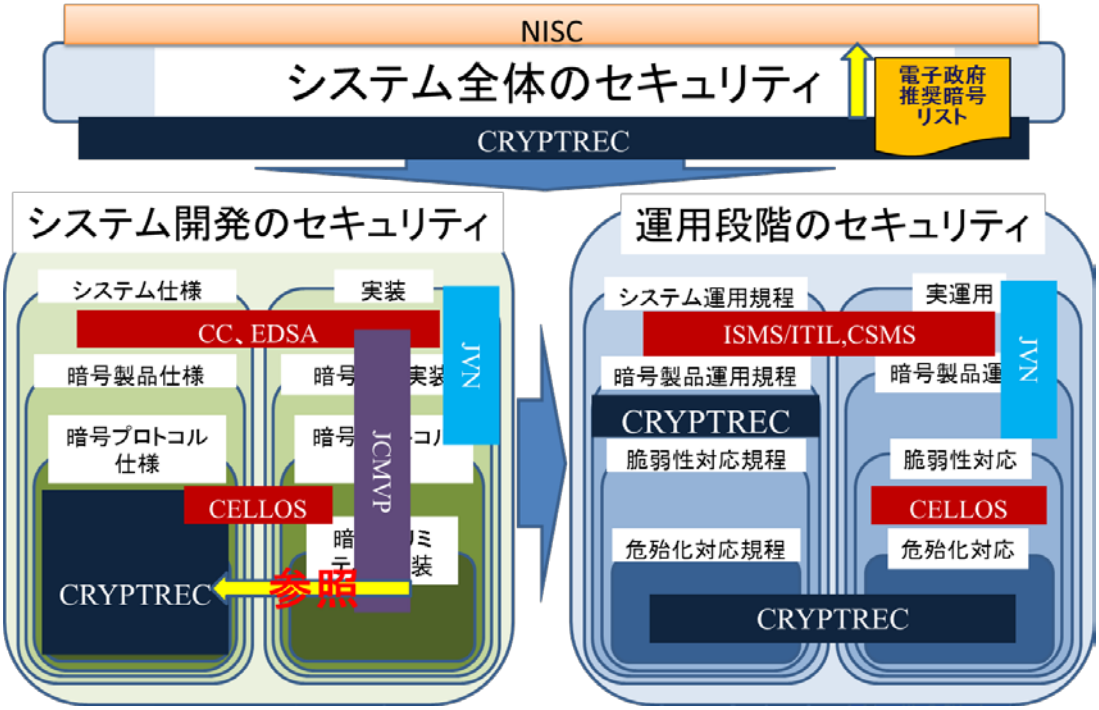
- 情報システムにおける暗号技術のセキュリティは開発及び運用段階で分けて考える必要がある
- さらにそれぞれを「仕様と実装」、「規程とその規程の実運用」とに分けて考えた方が良い
- その上で様々な暗号プリミティブ、プロトコル、製品から情報システム全体といったレイヤ別に確認が必要

上記を踏まえて以下の全体俯瞰図を作成した。

資料２



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

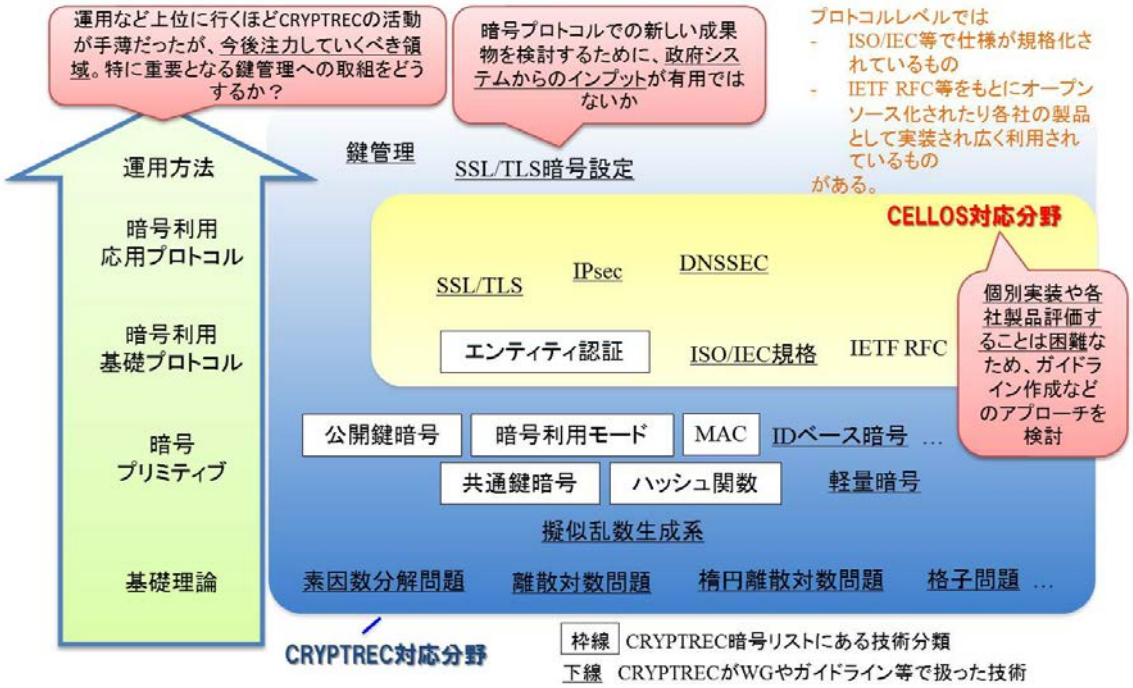
対象とする活動領域の検討について、既存の他団体の活動（プロトコルのセキュリティ評価（CELLOS)、製品（ソフトウェア）の脆弱性（JVN）等）との関係を考慮した上で各種議論がなされ、以下のような課題が整理された。

- 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。

資料２



（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

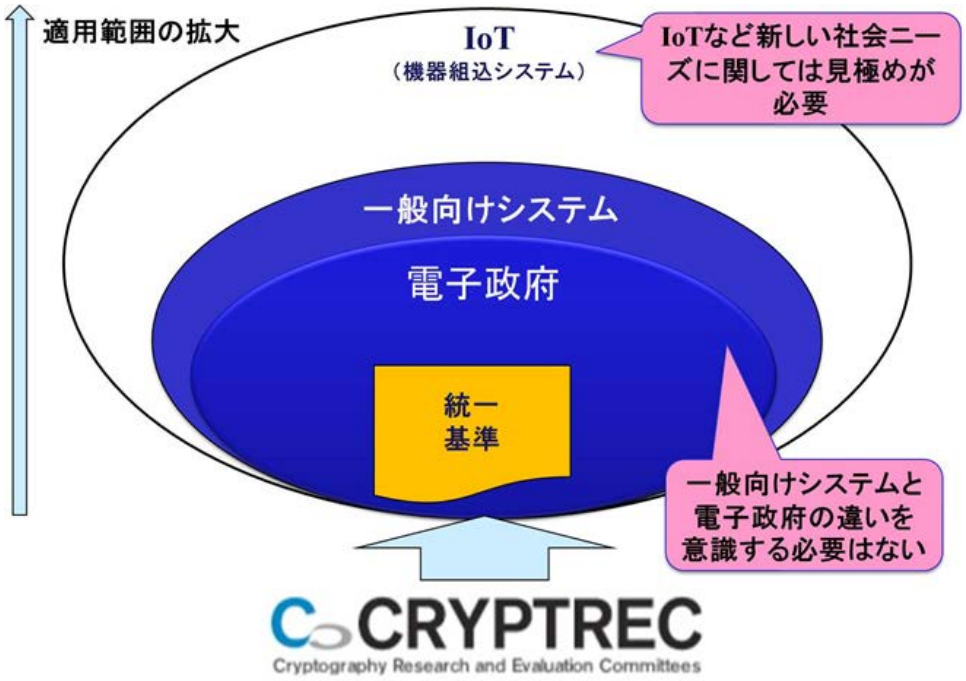
・実装や製品評価といった個別評価の分野や脆弱性対応など迅速性が要求される分野について、他団体との具体的連携を引き続き検討する
-CELLOS との脆弱性対応での連携における具体的フロー検討
-その他の団体との連携に関する必要性やその具体的フロー検討

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。

資料２

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

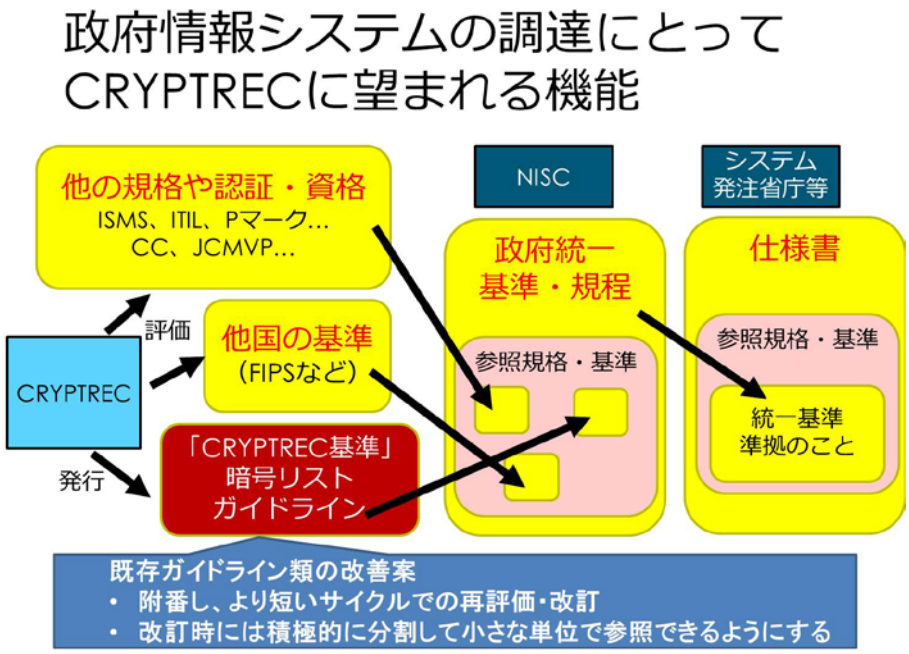
3.5　CRYPTREC の成果物に関する議論結果概要

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

資料２

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

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）

平成 27 年 10 月５日
暗号技術検討会事務局

「CRYPTREC の在り方に関する検討グループ」での議論の結果、以下のような多くの課題について継続的な議論が必要との結論となった。

- 政府統一基準に向けた新たな CRYPTREC 成果物
- 暗号プロトコルレベルのセキュリティ確保に向けた活動
- 新たな社会ニーズを見据えた新規活動
- 情報システム全体のセキュリティ確保を意識した他団体との連携
- 定常的な普及・広報活動に加え、脆弱性対応など緊急時の対応を踏まえた情報発信フローの整備

その為、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、上記課題を引き続き検討することにより、今後の CRYPTREC の活動方向性を報告することとする。

（狙い）

・情報システム全体のセキュリティ確保の為に必要となる活動の網羅性を確保しながら、社会ニーズの変化などを踏まえて、活動全般の方向性を随時議論できる場を確保する。
・CRYPTREC の方向性を機動性を持って検討し、トップダウン的な意志決定もできる体制を構築する。
・各委員会・WG 活動を俯瞰し、方針や活動プロセスを調整する機能を持たせる。各委員会は成果物作成に集中的に取り組むプロセスに改善し、CRYPTREC をより効率的に運営。

（検討会・タスクフォース及び各委員会の役割分担）

・暗号技術検討会は、総合的な知見をもって、取り組むべき方向性をタスクフォースに指示する。
・タスクフォースは、検討会から提示のあった改善すべきタスクの審議、暗号技術評価委員会や暗号技術活用委員会が行うべきタスクの選定や意思決定プロセス管理等を行う調整機能を担う。
・暗号技術評価委員会、暗号技術活用委員会等の各委員会は、タスクフォースから提示されたタスクに集中的に取り組むことによって、CRYPTREC の効率的な運営、活動の強化を目指す。

資料３

（想定する構成員）

・現在の検討グループ構成員を中心に、CRYPTREC の各委員会・WG 活動の意図をより反映できるよう、暗号技術専門家やユーザー側の者の少数名追加を検討する。（合計 9 名以下）

・事務局として総務省・経産省の他、NICT、IPA を想定する。

・ＮＩＳＣは引き続きオブザーバとして参加する。

資料３

CRYPTREC　重点課題検討タスクフォース　構成員・オブザーバ名簿（案）

（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
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 教授
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
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
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
満塩　尚史	内閣官房　政府ＣＩＯ補佐官
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）

内閣官房内閣サイバーセキュリティセンター

（五十音順、敬称略）

＜参考＞
（事務局）

総務省　情報セキュリティ対策室

経済産業省　情報セキュリティ政策室

国立研究開発法人　情報通信研究機構

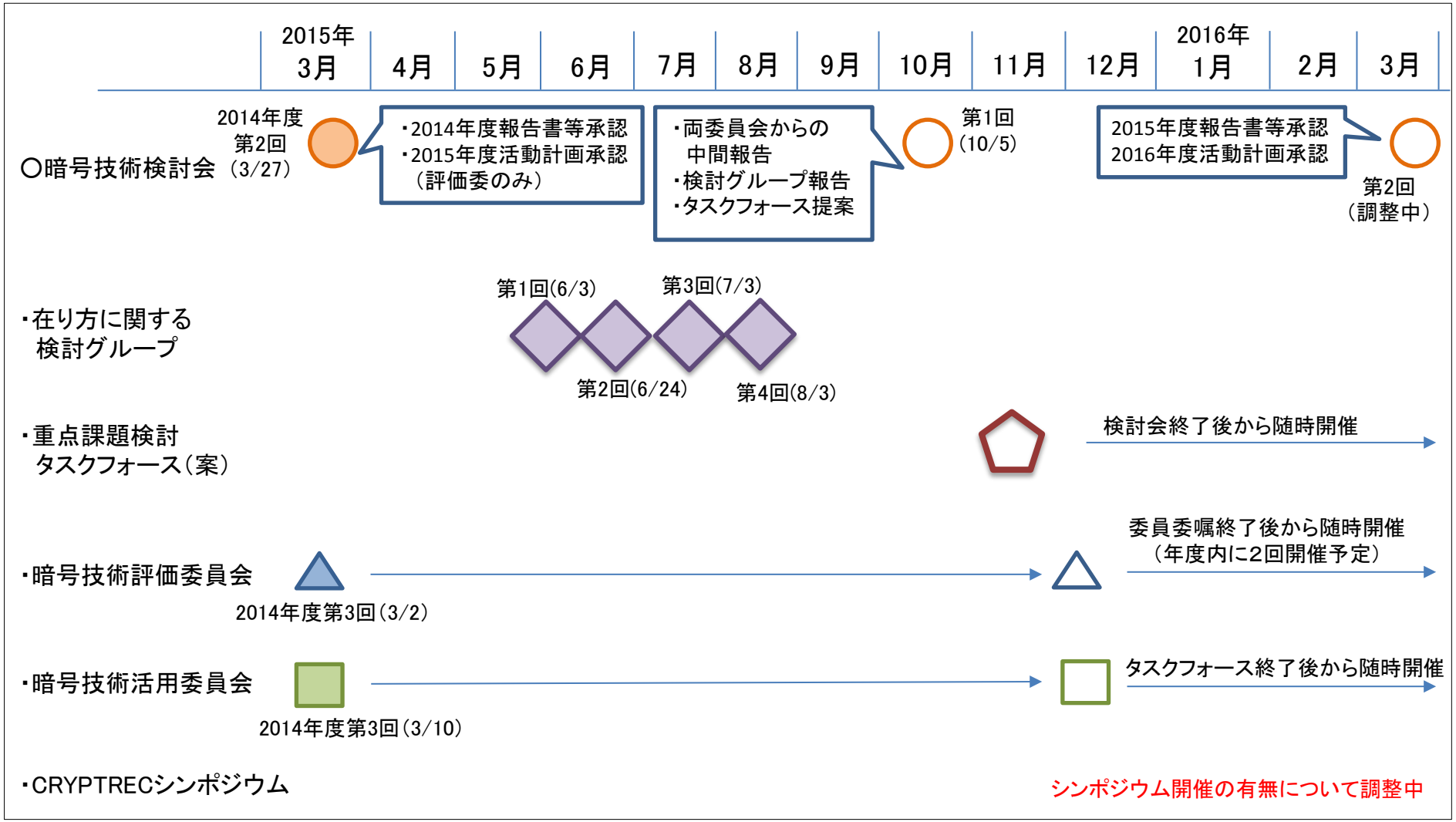
独立行政法人　情報処理推進機構

2015年度　暗号技術検討会活動計画

資料4

暗号技術検討会及び関連委員会（暗号技術評価委員会及び暗号技術活用委員会）の活動を通じて、電子政府推奨暗号等に関する安全性の監視・評価及び普及促進等を実施。

1．CRYPTREC（暗号技術検討会及び関連委員会）の開催実績及び開催予定



2. 2015年度CRYPTREC体制図（案）及び検討事項

暗号技術検討会
（事務局：総務省、経産省）

・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

「政府機関の情報セキュリティ対策のための統一基準」等へのインプット → NISC

在り方に関する検討グループ（終了予定）
座長：松本　勉（横浜国立大学）
（事務局：総務省、経産省）

・CRYTREC活動の見直し

重点課題検討タスクフォース（案）
（事務局：総務省、経産省、NICT、IPA）

（1）CRYPTRECのミッション検討
・政府統一基準への新たな成果物
・暗号プロトコルレベルのセキュリティ確保に向けた活動
・新たな社会ニーズを見据えた新規活動
・他団体との連携
・情報発信フローの整備
（2）上記に基づいたCRYPTREC次年度活動計画方針案検討

暗号技術評価委員会
（事務局：NICT、IPA）

・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
＃評価委員会の一部の活動内容については、重点課題検討タスクフォース（案）の議論後に決定する

暗号技術活用委員会
（事務局：NICT、IPA）

・暗号技術における国際競争力の向上及び運用面でのキュリティ向上等
＃活用委員会の活動については、重点課題検討タスクフォース（案）の議論後に決定する

資料５

2015 年度 暗号技術評価委員会の活動について（案）

1. 活動目的（2014 年度 第 2 回暗号技術検討会提出資料より抜粋）

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。報告は、なるべく直近の暗号技術評価委員会で報告することを目標とする。

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。

- 今年度、既に下記の速報を和文・英文で発行した。

  64 ビットブロック暗号 MISTY1 の安全性について（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)（2015 年 8 月 12 日）

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。

- 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。

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。

(2) 新技術に係る調査

- 暗号技術調査ワーキンググループ(暗号解析評価)

  実施すべき課題を検討し、必要に応じて開催する。具体的な活動内容については、2015 年度第 1 回 暗号技術評価委員会(11 月開催予定)にて検討する。

- 暗号技術調査ワーキンググループ(軽量暗号)

  第 1 回軽量暗号ワーキンググループを 10 月 20 日に開催予定。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て暗号技術ガイドラインを発行する。このため、今年度から 2 年をかけて詳細評価を行う。

  これまで既に、昨年度までのワーキンググループでの活動について、7 月 20-21 日に NIST で開催された Lightweight Cryptography Workshop および 9 月 30 日にお茶の水ソラシティホールで開催された IoT セキュリティフォーラムにて発表を行った。

(3) 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)

- 「CRYPTREC 暗号技術ガイドライン(SSL/TLS における近年の攻撃への対応))」の更新を行う。
- 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、2015 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） 委員構成

[暗号技術評価委員会]

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	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	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

※ 第1回暗号技術評価委員会で、委員の互選により委員長を選出する.

[暗号技術調査ワーキンググループ(暗号解析評価)]

委員委嘱準備中

[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	﨑山　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

資料 5 別添

64 ビットブロック暗号 MISTY1 の安全性について

平成 27 年 7 月 16 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 に対する新たな解析結果を示した論文 [2]が、国際暗号学会 （International Association for Cryptologic Research (IACR)）が主催する国際会議 CRYPTO 2015[3]で採録され、国際会議に先立ち、その詳細が IACR ePrint Archive[4]にて発表されました。

この論文では、Integral Cryptanalysis という従来から知られているブロック暗号に対する攻撃法の解読計算量を新たな手法で改良し、仕様通りの MISTY1 の 128 ビットの鍵が、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ました。この論文では、解読に必要なデータ量 と計算量にトレードオフのある 2 種類の攻撃法が示されており、下記の表にその解読計算量を示します。

これらの攻撃法において、解読に必要なデータ量は $2^{63.58}$, $2^{63.994}$と非常に多く、64 ビットブロック暗号では鍵を固定すると 2^{64}通りの（平文, 暗号文）の組しか存在しないことから、ほとんどすべての（平文, 暗号文）の組を集める必要があること、かつ、解読に必要な計算量も 2^{121}, $2^{107.9}$と非常に多いことから、現実的な脅威につながることはないものと考えられます。本件に関する調査結果については、今後、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 （[2]による）

	解読に必要なデータ量 [5]	解読に必要な計算量 [6]
MISTY1 (full round)	$2^{63.58}$	2^{121}
MISTY1 (full round)	$2^{63.994}$	$2^{107.9}$

[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.
[3] http://www.iacr.org/conferences/crypto2015/
[4] https://eprint.iacr.org/2015/682

[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。

資料 5 別添

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”, Advances in Cryptology – CRYPTO 2015, Lecture Notes in Computer Science, Volume 9215, pages 413–432. 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。

資料 6

2015 年度暗号技術活用委員会の活動について（案）

2014 年度第 2 回暗号技術検討会での「2015 年度暗号技術活用委員会の活動について（案）」に沿って進めている作業状況を報告する。

１．運用ガイドライン

SSL/TLS 暗号設定ガイドラインの公開後、「Public Key Pinning」についての設定方法について誤りとの指摘があり、WG 内で確認したところ、指摘が正しいことを確認した。

対処としては、Public Key Pinning の解説部分は誤りということではないので本文はそのままとし、Appendix の Public Key Pinning の具体的な設定方法の記述を正しいものに差し替えて、WG 承認のもと、Ver 1.1 として再公開した。

本年度下期は、SSL/TLS に関して IETF での議論が急進展し、各種設定状況についてのベンダ対応が進みつつある状況に鑑み、SSL/TLS 暗号設定ガイドラインのアップデートを含めたメンテナンスを準備している。

具体的には、SSL/TLS 暗号設定ガイドラインに準拠するための、市販 SSL/TLS 製品（アクセラレータ・ロードバランサ、WAF 等）での具体的な設定方法の調査を実施する予定である。

そのほかの運用ガイドラインの作成については、重点課題検討タスクフォースでの議論を踏まえて、今後検討していく。

２．暗号アルゴリズム利用実績調査

CRYPTREC の在り方に関する検討グループ等の議論を踏まえつつの対応となるため、本年度の暗号アルゴリズム利用実績調査の実施については、検討を要する。

次年度からの活用委員会活動の早期本格化を見据え、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議論を踏まえた準備作業を引き続き実施する。

３．2014 年度の成果の普及啓発

2014 年度に作成した「SSL/TLS 暗号設定ガイドライン」を公開した。

- CRYPTREC ウェブページ

  http://www.cryptrec.go.jp/topics/cryptrec_20150522_oper_guideline_fy2014.html

- CRYPTREC ウェブページにおける実アクセス数は以下の通り。

	6 月	7 月	8 月
ウェブページ参照数	356	319	158
コンテンツダウンロード数	1,193	896	646

※サーバの設定により 5 月のログファイルが消えてしまっていたため、5 月分が集計不可能

- IPA ウェブページ（安全なウェブサイトのために（暗号設定対策編））

  https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

- IPA ウェブページにおける実アクセス数は以下の通り。

	5 月 12 日～	6 月	7 月	8 月
ウェブページ参照数	20,692 （3 位）	5,080	3,007	2,776
コンテンツダウンロード数	7,564 （1 位）	3,881	2,923	3,743

公開直後の 5 月は 20 日間だったが、ページビューとしては、IPA トップページ、IPA セキュリティセンタートップページに次ぐ参照数

- セキュリティ EXPO 2015 春での 「SSL/TLS 暗号設定ガイドライン」の紹介
  - Appendix に記載されたもの以外の市販 SSL/TLS 製品での具体的な設定方法の要望あり

以上

参考資料１

２０１４年度　第２回暗号技術検討会　議事概要

１．日時　平成２７年３月２７日（金）　１０：００～１１：５０

２．場所　経済産業省別館１階　１０４各省庁共用会議室

３．出席者（敬称略）

構成員：今井秀樹（座長）、今井正道、上原哲太郎、太田和夫、岡本栄司、岡本龍明、金子敏信、国分明男、佐々木良一、近澤武、中山靖司、本間尚文、松井充、松尾真一郎、松本勉、松本泰、向山友也

オブザーバ：奥山剛、中村武英（村田利見 代理）、江森久子（野口宣大 代理）、佐久間明彦（大村周一郎 代理）、岩下守男（鯨井佳則 代理）、岩永敏明（和泉章 代理）、平和昌、寶木和夫、伊藤毅志、竹内英二、西村敏信

暗号技術評価委員会事務局：盛合志帆（独立行政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、赤阪晋介、筒井邦弘、中村一成

経済産業省　大橋秀行、上村昌博、中野辰実、室井佳子

４．配布資料

（資料番号）

資料１	2014 年度 暗号技術評価委員会活動報告
資料１別添１	2014 年度 暗号技術調査 WG（暗号解析評価）活動報告
資料１別添２	離散対数問題の困難性に関する調査
資料１別添３	格子問題等の困難性に関する調査
資料１別添４	2014 年度 暗号技術調査 WG（軽量暗号）活動報告
資料１別添５	暗号技術調査 WG（軽量暗号）報告書（案）
資料２	2014 年度 暗号技術活用委員会活動報告
資料２別添１	暗号普及促進・セキュリティ産業の競争力強化に向けた課題分析と見解
資料２別添２	SSL/TLS 暗号設定ガイドライン
資料２別添３	SSL/TLS 暗号設定ガイドラインチェックリスト
資料２別添４－１	暗号技術参照関係の俯瞰図（全体像）
資料２別添４－２	暗号技術参照関係の俯瞰図
資料２別添５	標準化提案におけるノウハウ・課題・基本的な情報の整理
資料３	CRYPTREC 暗号リストの注釈の一部変更について
資料３別添	CRYPTREC 暗号リストの変更案
資料４	2014 年度 暗号技術検討会報告書（案）

資料５	暗号技術検討会における小グループの設置について（案）
資料６	2015 年度 暗号技術評価委員会活動計画（案）
資料７	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１回暗号技術検討会議事概要
参考資料２	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
参考資料３	2014 年度 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、経済産業省の大橋審議官から開会の挨拶が行われた。

参考資料３に基づき、暗号技術検討会事務局よりオブザーバの交代（(警察庁）佐藤氏→村田氏、(一般社団法人日本情報経済社会推進協会）亀田氏→竹内氏及び構成員の欠席（渡辺構成員）について説明が行われた。

２　議事

（１）2014 年度　暗号技術評価委員会活動報告について

資料１から資料１別添５に基づき、暗号技術評価委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。原案どおり承認された

〇質疑応答

今井座長：軽量暗号に関してこれほど多くの内容を取りまとめた報告書は世界で初めてではないか。今後、IoT のあらゆる面で軽量暗号が重要になってくると思うが、どのような場面で軽量暗号が使用できるかしっかり示すことは意義深い。この報告書は既に公開されているのか。

暗号技術評価委員会事務局:まだ公開されていない。今回の暗号技術検討会の審議の後、4 月以降に誤植等の修正を行った上で、CRYPTREC の HP で公開する。

（２）2014 年度　暗号技術活用委員会活動報告について

資料２から資料２別添５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。原案どおり承認された。

〇質疑応答

松尾構成員：標準化 WG の報告において、公開できない情報があるとのことだが、実際はそのような公開できない情報こそが重要だったりする。今後標準化活動を行う人に、これらの情報を提供する方法は考えているのか。

暗号技術活用委員会事務局：標準化団体の国内委員会等のコンタクト先を掲載することで、対応したい。

佐々木構成員：暗号ライブラリ市場が縮小しているというのは、おっしゃるとおりだと思う。しかし、軽量暗号は半導体への利用が想定されているなど、ライブラリ製品以外への広がりが期待できるのではないか。この動きは産業化に結びつくのか、あるいは、結びつけるにはどうしていったらよいと考えているか。軽量暗号については、どのくらい暗号強度があればリスクを許容可能なのかを示していかないと、利用が進ま

ないのではないかと危惧している。

暗号技術活用委員会事務局：軽量暗号の安全性評価については、暗号技術評価委員会が担当しているが、暗号技術活用委員会として議論のポイントとなったのは、資料２別添１の 16 頁にも記載している点である。日本は各社が全て独自技術で競争しようとするが、米国はある程度のレイヤーで区切りをつけ、共通化すべき部分は共通化している。日本で製品化が進むかどうかは、共通化すべき部分を共通化していくようまとめることができるかどうかにかかっている。

佐々木構成員：民間企業が自らまとまるという方法もあると思うが、CRYPTREC でも検討を行っているため、連携していく道もあるのではないか。

暗号技術活用委員会事務局：暗号技術はロイヤリティフリーが多いため、企業にとって国産暗号を推進するメリットは少ない。しかし、国によっては国産暗号の普及を国が主導して成功している例もある。そこで仮説として、国産暗号の普及が、国にとっても企業にとってもメリットがあり、Win-Win の関係を構築していることが成功の秘訣ではないかと考えている。その仮説に至る具体的な考え方は、資料２別添１の 13～14 頁に記載しているとおり。

暗号技術評価委員会事務局：軽量暗号の安全性に不安を感じている人はいると思う。来年度に作成するガイドラインにおいて、同じ鍵でどれくらいの暗号ならリスクを許容できるのかということを示していきたいと考えている。また、来年度の暗号技術評価委員会では、軽量暗号の普及について、標準化の観点も含めて検討する。

佐々木構成員：国産暗号の普及促進のみを強く言いすぎることも良くないと思うが、せっかく良い暗号アルゴリズムがあるのだから普及させていきたい。現在、一番芽が出そうだと考えているのが軽量暗号である。

（３）CRYPTREC 暗号リストの注釈の一部変更について

資料３及び資料３別添に基づき、暗号技術検討会事務局より説明が行われた。質疑はなし。原案どおり承認された。

（４）2014 年度　暗号技術検討会報告書（案）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。本日の議事内容を反映させた上で、本日の議事概要とともにメールで最終的な確認を行うこととして承認された。

（５）暗号技術検討会における小グループの設置について

資料５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。原案どおり承認された。

〇質疑応答

松尾構成員：資料４の暗号技術検討会の報告書（案）にもあるとおり、重要なのは日本の安全な ICT 基盤の確立であると思う。そこで、安全な ICT 基盤とは何なのか、その中で CRYPTREC が発揮できる強みとは何か、JCMVP 等の制度との連携も含めて検討すべき。

佐々木構成員：産業育成についてもう少し検討していただきたい。国として国産の暗号アルゴリズムを１つは持っていないといけないという事が正しいのかどうかということを含めて小グループで議論していただきたい。

松本（勉）構成員：これまで策定してきた CRYPTREC 暗号リストは、暗号アルゴリズムが中心であるが、もっと暗号プロトコルとその実装まで、CRYPTREC がカバーしていく必要があるのではないか。

今井座長：暗号プロトコルについては、CELLOS とも上手く連携していく必要がある。先日、メディカル ICT で医薬品や医療機器を自国で評価・認証することが重要という話があった。暗号分野においては、まさに CRYPTREC がそういった活動を担っている。人材育成についても、人を増やすことが重要。人が増えれば、評価・認証にかかる時間も短縮される。即応性の観点も重要である。

（６）2015 年度　暗号技術評価委員会活動計画（案）について

資料６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。質疑はなし。原案どおり承認された。

（７）2015 年度　暗号技術活用委員会の活動について

資料７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。原案どおり承認された。

〇質疑応答

松本（泰）構成員：暗号技術評価委員会の 2015 年度の計画にある新技術に関する調査について、どういった暗号技術が今後求められるようになるかという観点からの調査も必要ではないか。例えば、マイナンバーであれば、プライバシー保護技術に関連した暗号技術が有用になると考えられるし、IoT における暗号技術の利用というのも今後進展が期待できる分野と考えられる。そういった暗号研究者にモチベーションを与えるような調査も実施していただきたい。

上原構成員：運用ガイドラインの検討準備についてだが、SSH に関しては、つい最近 CSIRT 協議会がガイドラインを策定している。既に策定されているものに対して、政府が別

の動きをすると現場が混乱する可能性があるので、ガイドラインのテーマは既存のものとなるべく重複しないよう検討していただきたい。

暗号技術活用委員会事務局:既存のテーマと重複しないように、事前準備で確認を行う。

３　閉会

総務省の南政策統括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 1 回暗号技術検討会は夏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。

今年度限りでの CRYPTREC からの退任にあたり、今井座長から挨拶が行われた。

以上

参考資料 2

2015 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）に関する監視を行う。報告は、なるべく直近の暗号技術評価委員会で報告することを目標とする。

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リストに関わる技術の安全性・性能評価を行う。

(2) 新技術に係る調査

- 暗号技術調査ワーキンググループ(暗号解析評価) は、実施すべき課題を検討し、必要に応じて開催する。 具体的な活動については、2015 年度第 1 回 暗号技術評価委員会にて検討する。
- 暗号技術調査ワーキンググループ(軽量暗号)は、詳細評価対象となる技術分類の選定、詳細評価内容の策定を行い、具体的な詳細評価を実施する。詳細評価 の対象技術分類としては、軽量認証暗号の評価を優先的に行う予定である。

(3) 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)

- 「CRYPTREC 暗号技術ガイドライン(SSL/TLS における近年の攻撃への対応))」の更新を行う。
- 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、2015 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３

2015 年度暗号技術活用委員会の活動について（案）

2015 年度以降の暗号技術活用委員会の担当内容及び体制については暗号技術検討会に設置される小グループで検討を行う予定であり、実施項目の詳細及び実施体制は議論結果に準ずるが、並行して行う準備作業として想定される項目は以下の通りである。

１．現時点で想定される項目

(1) 運用ガイドラインの検討準備

- 一般（民間事業者）向けにも利用できる「ガイドライン」の作成に関わる事前準備を行う

  テーマ案：IPsec、SSH 等

(2) 暗号アルゴリズム利用実績調査の準備

- CRYPTREC 暗号リストの小改定に関して必要な調査に係る準備作業を行う

(3) 2014 年度の成果の普及啓発やフィードバック

- SSL/TLS 暗号設定ガイドライン等の広報活動を行い、使い勝手等の利用者からの声を収集する

２．今後の進め方

上記作業を進めるに当たっては、小グループにおける議論の結果を踏まえ、柔軟な対応を行えるよう作業を実施していくこととする。

以上

参考資料 4

暗号技術検討会　構成員・オブザーバ名簿

2015.10.5 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	独立行政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）