2013 年度　第 1 回暗号技術検討会

日時：平成 25 年 7 月 5 日(金) 14:00～15:30
場所：経済産業省本館４Ｆ商情局第１会議室

議　事　次　第

１．開　会

２．議　事
(1)　2013 年度 暗号技術検討会開催要綱等について【承認事項】
(2)　2012 年度 暗号技術検討会報告書（案）について【承認事項】
(3)　暗号技術評価委員会 活動計画（案）について【承認事項】
(4)　暗号技術活用委員会 活動計画（案）について【承認事項】
(5)　CRYPTREC の暗号アルゴリズム仕様書について【承認事項】
(6)　その他

３．閉　会

（資料番号）	（資 料 名）
資料１－１	2013 年度 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	2012 年度 暗号技術検討会報告書（案）
資料３	暗号技術評価委員会 活動計画（案）
資料４	暗号技術活用委員会 活動計画（案）
資料５	CRYPTREC の暗号アルゴリズム仕様書について
参考資料１	2012 年度 第３回 暗号技術検討会議事概要
参考資料２	今後の検討課題に関する方針
参考資料３	2013 年度 暗号技術検討会及び関連委員会の体制
参考資料４	2013 年度　暗号技術検討会　構成員・オブザーバ名簿

資料１－１

２０１３年度「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、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を指名できる。
（５）構成員の任期は平成２６年３月までとし、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、座長からの指名を受けた構成員が座長を代理する。
（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、平成２６年３月まで開催する。

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

暗号技術検討会

２０１２年度報告書（案）

２０１３年７月

目　　次

１．はじめに ····· - 1-

２．暗号技術検討会開催の背景及び開催状況 ····· - 3-
２．１．暗号技術検討会開催の背景 ····· - 3-
２．２．CRYPTREC の体制 ····· - 3-
２．３．暗号技術検討会の開催状況 ····· - 4-

３．各委員会の活動報告 ····· - 6-
３．１．暗号方式委員会 ····· - 6-
３．１．１．活動の概要 ····· - 6-
３．１．２．2012 年度の活動内容 ····· - 6-
３．１．３．暗号方式委員会の開催状況 ····· - 6-
３．２．暗号実装委員会 ····· - 8-
３．２．１．活動の概要 ····· - 8-
３．２．２．2012 年度の活動内容 ····· - 8-
３．２．３．暗号実装委員会開催状況 ····· - 8-
３．３．暗号運用委員会 ····· -10-
３．３．１．活動の概要 ····· -10-
３．３．２．2012 年度の活動内容 ····· -10-
３．３．３．暗号運用委員会の開催状況 ····· -10-
３．４．合同委員会 ····· -12-
３．４．１．開催の目的 ····· -12-
３．４．２．議論の結果 ····· -12-

４．今後の CRYPTREC の活動について ····· -13-

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）
別添２　2012 年度暗号技術検討会構成員・オブザーバ名簿

１．はじめに

情報通信技術を安心・安全に利用できる環境を構築していくにあたり、暗号技術は必要不可欠なものとなっている。このため、解読技術等の進展に注意を払い、適切なものを使用するよう努めねばならない。例えば、昨今、政府の情報システムにも広く使用されている暗号化通信プロトコル SSL/TLS に対する新たな攻撃手法が国際会議等で報告されるなど、新たな脅威が生じており、暗号技術やプロトコルのバージョンの適切な選択及び設定がますます重要となっている。最新の解読方法とその影響について、引き続き監視を行っていくことが重要である。

政府においても、情報セキュリティ政策会議(議長：内閣官房長官)において、「政府機関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（2008 年 4 月)」、「政府機関の情報セキュリティ対策のための統一管理基準（2011 年 4 月 21 日)」及び「サイバーセキュリティ戦略（2013 年 6 月)」が決定され、政府機関に対しては暗号アルゴリズムの着実な移行の実施とともに、暗号化及び電子署名のアルゴリズムについて、「電子政府推奨暗号リストに記載されたものが使用可能な場合には、それを使用すること」と定められ、さらに「暗号技術については安全評価がなされたものの利用を推進すること」などが求められている。CRYPTREC としても、政府機関のこれらの動きに対して適切に支援を行うべく、調査・検討を進める必要がある。

昨年度は、「電子政府推奨暗号リスト」（平成１５年２月２０日公表）を改定した「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)」を策定するなど、CRYPTREC として節目の１年となった。この CRYPTREC 暗号リストは「安全性」及び「実装性」の観点に加え、「製品化、利用実績等」といった様々な視点で検討され、「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」の３つのリストから構成される。今後は、政府機関における情報システムの調達及び利用において、この新しいリストが大いに活用されることが期待される。

委員会別の活動状況を見てみると、暗号方式委員会では、CRYPTREC 暗号リスト策定作業として安全性評価、安全性に関する暗号技術の技術的アピールポイントに関する評価、総合評価及び CRYPTREC 暗号リストの注釈の整理等を行った。暗号実装委員会では、CRYPTREC 暗号リスト策定作業として実装評価、実装性能に関する技術的アピールポイントに関する評価、総合評価等を行った。暗号運用委員会では、CRYPTREC 暗号リスト策定作業として電子政府推奨暗号リストの選定基準の決定及び利用実績調査等を行った。

なお、2012 年度の活動のうち、詳細な技術的事項については、暗号方式委員会、暗号実装委員会及び暗号運用委員会における議論を踏まえて、独立行政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た「CRYPTREC Report 2012」を参照いただきたい。

末筆であるが、本検討会及び関係委員会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。

2013 年 7 月

暗号技術検討会

座長　今井　秀樹

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（以下、「検討会」という。）を開催した。

電子政府推奨暗号リストは、2002 年度に策定、公表したが、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、暗号技術の適切な実装法・運用法を調査・検討するため、総務省及び経済産業省は、継続的に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：今井秀樹中央大学教授）と、独立行政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。

2012 年度の CRYPTREC の体制は、前年度から引き続き、暗号技術検討会の下に、暗号方式委員会、暗号実装委員会及び暗号運用委員会を設置し、調査・検討を行った。

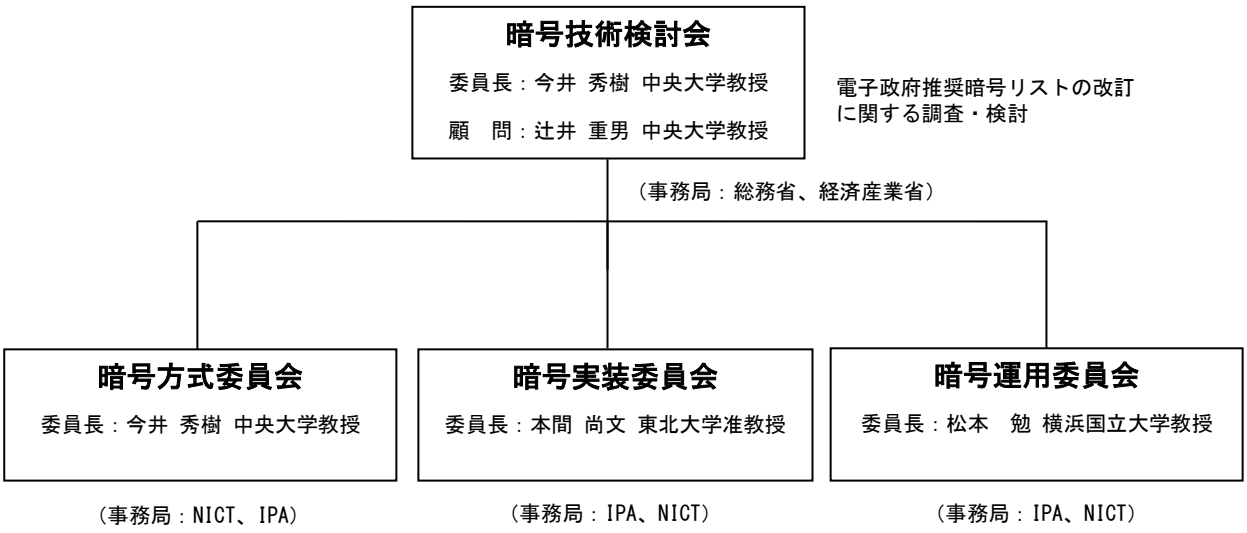


図 2.1　2012 年度 CRYPTREC の体制図

２．３．暗号技術検討会の開催状況

2012 年度の暗号技術検討会は、電子政府推奨暗号の監視、電子政府推奨暗号の安全性及び信頼性確保のための調査・検討、電子政府推奨暗号リスト改定に関する調査・検討等について、総合的な観点から検討を行ったが、その検討の中心は電子政府推奨暗号リスト改定についてであり、以下のとおり年度内に３回開催し、2013 年 3 月には、電子政府推奨暗号リストを改定した「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）」を公表した。

【第 1 回】2012 年 8 月 2 日（木）16:00～18:00

（主な議題）

・ 次期電子政府推奨暗号選定のための評価基準案について

（概要）

・ 電子政府推奨暗号リスト改定に向け、リストに掲載する暗号技術に対する評価項目における選定基準について、暗号方式委員会、暗号実装委員会、暗号運用委員会において検討してきたが、その内容について説明を行い、承認を得た。承認された選定基準について主要なものは以下のとおり。
・ 【評価Ａ】利用実績が十分であり、今後も安定的に利用可能であるかを判断するための評価について、「採用割合 50%」を閾値として採用。また、【評価Ａ】の通過基準については、４項目中、「３項目以上」の選定基準を満たすことを要件とした。
・ 【評価Ｂ】市販製品採用実績については、利用実績調査によって「他社利用が進んでいることを確認」することを条件に「採用割合 10%」を閾値として採用。「市販製品採用実績」以外の選定基準については、「２件以上」かつ「採用割合として 10%以上」となる件数を選定基準とするが、カテゴリ有効数が４件以下の時に限り、「１件」でもよいこととした。また、【評価Ｂ】の通過基準については、８項目中、「３項目以上」の選定基準を満たすことを用件とした。
・ さらなる絞り込みが必要となった場合にのみ評価結果を活用する【総合評価】については「技術的側面」と「非技術的側面」の割合について「１：１」を基本とすることとした。
・ 暗号方式委員会で行った【安全性評価】における判定案について承認するとともに、【評価Ｂ】及び【総合評価】に関する評価項目・配点について、「市場が認める程度の技術的アドバンテージがあるか」（以下、技術的アピールポイント）は、安全性と実装性能の２つの観点から評価することとし、少なくとも一方で「アドバンテージがある」と判断すれば、「技術的アピールポイント」があると判定する。
・ 【実装評価】に関する実装性能の判定方針について、現リスト暗号については、前回の評価時(2000-2002 年度)に十分な実装性能を有していることを既に確認しているので、十分な性能を有すると判定する。新規応募暗号については、現リスト暗号に対する実装上の優位性の有無を判定する。具体的には、ソフトウェア実装については、事務局が用意した性能評価ツール(PC 環境)による計測値を利用し、ハードウェア実装については、事務局が用意した性能評価環境(FPGA 環境)における計測値を利用し、同じカテゴリに属する現リスト暗号よりも優位な値となる計測項目があれば、十分な性能を有すると判定する。

【第 2 回】2012 年 12 月 11 日（火）14:00～16:00
（主な議題）
- 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）（案）について
- 今後の課題について

（概要）
- 11 月 15 日に開催された暗号方式委員会、暗号実装委員会、暗号運用委員会の３委員長による合同委員会の概要（開催の主旨、「CRYPTREC 暗号リスト」の素案の作成）について事務局から紹介。
- ３委員会による評価結果をもとに作成された「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）（案）」を承認。本リスト案をパブリックコメントにかけることを決定。なお、選定作業を行った結果、安全性評価、実装評価、条件適合性評価では十分な絞り込みができない事態をも想定し、更なる絞り込みを行い得る調整措置として設置した「総合評価」については、本リスト案は、安全性が確認され、利用実績が確認できた暗号技術に十分な絞り込みがなされていると判断され、第１回暗号技術検討会において決定した評価基準案に沿った妥当なものであるという結論となり、実施しないことになった。
- 今後の課題について自由討議を行った。

【第 3 回】2013 年 2 月 22 日（金）15:00～17:00
（主な議題）
- 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）について
- 今後の検討課題に関する方針（案）について
- 2013 年度暗号技術検討会及び関連委員会の体制（案）について

（概要）
- 「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）（案）」に対するパブリックコメントの結果について報告するとともに、寄せられた意見に対する考え方について内容の確認を行った。また、パブリックコメントで寄せられた意見を踏まえ、脚注の表記等について一部修正した上でリスト案を確定することが承認された。
- 確定したリストは、3 月 1 日（金）15:00 に総務省及び経済産業省から公表することが了承された。
- 今後の検討課題に関する方針（案）について、議論を行った。プライバシー保護等と個人情報活用の両立にあたって暗号技術を活用すること、ニーズから求められている暗号の応用に、CRYPTREC が視野を広げるべきではないか、暗号技術の普及のために必要な活動に取り組むべき、といった意見が出された。なお、３年又は２年としていた小改定の時期、暗号人材育成において求められる人材像については、事務局において次回検討会までの間に整理することになった。

３．各委員会の活動報告

３．１．暗号方式委員会

３．１．１．活動の概要

暗号方式委員会は、電子政府推奨暗号リストに掲載された暗号に対する攻撃の予兆や影響に関する情報収集・分析を実施、電子政府推奨暗号リストの改定に向けた暗号技術の安全性評価、及び将来電子政府での利用が見込まれる暗号技術の調査を行うために、2008 年度まで開催していた暗号技術監視委員会を引き継ぐ形で、2009 年度から組織された。

暗号方式委員会では、電子政府推奨暗号の監視、電子政府推奨暗号の安全性及び信頼性確保のための調査・検討及び電子政府推奨暗号リスト改定に関する安全性評価を行う。

以下に、2012 年度の暗号方式委員会の活動内容について報告する。

３．１．２．2012 年度の活動内容

2012 年度は、電子政府推奨暗号リスト改定に向けて必要となる暗号技術の安全性に関する評価及び検討を中心に、以下の活動を行った。

(1) 電子政府推奨暗号リスト改定のための安全性評価

最近の暗号解読技術の進歩を踏まえた 128 ビットブロック暗号の安全性評価及び SSL/TLS で利用する際のストリーム暗号 128-bit RC4 の安全性評価を行った。この結果も踏まえ、新規応募暗号技術、従来の電子政府推奨暗号リスト掲載暗号技術、事務局選出暗号技術に対して 2011 年度の暗号技術検討会において承認された「電子政府推奨暗号選定のための選考基準案の考え方」に基づき、「安全性評価」「評価 B」「総合評価」の評価を行った。

(2) 暗号技術調査ワーキンググループの活動

〇リストガイドワーキンググループ

鍵導出関数(KDF)に関する安全性の検討、一般的な暗号プロトコルに関する調査及びリストガイドの利用促進に係る検討を行った。

〇計算機能力評価ワーキンググループ

素因数分解問題や離散対数問題をはじめ、暗号技術で利用される数学的な問題について、困難性の見積りを行った。

(3) 監視活動

電子政府推奨暗号の安全性評価について、研究集会、国際会議、研究論文誌、インターネット上の情報等を収集し、電子政府推奨暗号の安全性に関する情報を分析した。

３．１．３．暗号方式委員会の開催状況

2012 年度、暗号方式委員会は、計 4 回開催された。各回会合の概要は表 3.1 のとおりである。

表 3.1　暗号方式委員会の開催

回	年月日	議題
第 1 回	2012 年　6 月 8 日	暗号方式委員会活動方針の検討 WG 活動方針の検討 安全性に関する次期リストの作成方針の検討 外部評価についての検討 監視状況報告
第 2 回	2012 年　7 月 24 日	今年度の暗号方式委員会審議事項の検討 安全性に関する次期リスト作成についての検討 外部評価についての検討
第 3 回	2012 年　10 月 9 日	審議事項の確認 安全性に関する次期リスト作成についての検討 評価 B の判定決定 総合評価の判定決定
第 4 回	2013 年　3 月 5 日	外部評価の結果報告 WG 活動報告 監視状況報告 次年度の検討項目についての議論

３．２．暗号実装委員会

３．２．１．活動の概要

暗号実装委員会は、電子政府推奨暗号リストに掲載された暗号を正しく安全に実装するための要件を検討するとともに、サイドチャネル攻撃をはじめとする暗号実装関連の技術動向を調査するために、2008 年度まで組織されていた暗号モジュール委員会を引き継ぐ形で、2009 年度から組織された。

2012 年度、暗号実装委員会では、電子政府推奨暗号リスト改定に伴う実装性能評価を実施するとともに、暗号の実装に係る技術及び暗号を実装した暗号モジュールの安全性・信頼性の評価に関する調査・検討を行った。

以下に、2012 年度の暗号実装委員会の活動内容について報告する。

３．２．２．2012 年度の活動内容

2012 年度は、電子政府推奨暗号リスト改定の一環として暗号技術の実装性能評価を実施するとともに、暗号モジュールの安全性と信頼性の評価に関する調査を行った。特に次の項目を実施した。

(1) 電子政府推奨暗号リスト改定のための実装性能評価

新規応募暗号技術及び従来の電子政府推奨暗号リスト掲載暗号技術に対するソフトウェア実装及びハードウェア実装での性能評価を完了した。

(2) サイドチャネル攻撃対策の有効性確認

新規応募暗号技術のうち、128 ビットブロック暗号とストリーム暗号について、応募者が提案するサイドチャネル攻撃対策が有効性を確認した。なお、この評価は暗号利用者向けの参考情報提供を目的とし、リスト改定には利用しなかった。

(3)サイドチャネルセキュリティワーキンググループの活動

〇サイドチャネル攻撃等の実験データに関する調査

サイドチャネル解析用プラットフォームの仕様である SASEBO ボード等を用いた評価・解析実験情報を収集した。

〇国際標準化活動への貢献

暗号モジュールに対するセキュリティ要件及び試験要件の国際標準化活動に協力した。

３．２．３．暗号実装委員会の開催状況

2012 年度、暗号実装委員会は、計 4 回開催された。各回会合の概要は表 3.2 のとおりである。

表 3.2　暗号実装委員会の開催

回	年月日	議題
第 1 回	2012 年　7 月 5 日	暗号実装委員会活動計画の検討 次期リスト作成に向けた実装性能評価方針の検討
第 2 回	2012 年　9 月 4 日	安全性評価/実装評価の実装評価の判定決定 実装性能に関する技術的アピールポイントに関する評価の状況報告
第 3 回	2012 年　10 月 9 日	実装性能に関する技術的アピールポイントに関する評価の判定決定 総合評価の判定決定 実装評性能評価結果の情報公開に関する検討
第 4 回	2013 年　3 月 14 日	実装性能評価データの一部更新 サイドチャネル攻撃対策の有効性確認 今後の検討課題についての議論

３．３．暗号運用委員会

３．３．１．活動の概要

暗号運用委員会は、電子政府システム等で利用される電子政府推奨暗号の適切な運用について、システム設計者・運用者観点から調査・検討を行うために、2009 年度から新たに設置された委員会である。

2012 年度、暗号運用委員会では、電子政府推奨暗号の選考に当たっての公平性・客観性を最大限確保する観点から、上期に電子政府推奨暗号の選定基準案の検討・決定並びに利用実績の調査を実施し、下期に、暗号技術検討会での審議状況を踏まえつつ、次年度以降の CRYPTREC 活動の検討に向けた課題の整理として検討を行った。

以下に、2012 年度の暗号運用委員会の活動内容について報告する。

３．３．２．2012 年度の活動内容

今年度は、第 1 回暗号運用委員会で確認された活動計画に基づき、電子政府推奨暗号の選定基準案の検討並びに利用実績の調査を中心に以下の事項について検討を行った。

(1) 電子政府推奨暗号選定のための選定基準案の検討

2011 年度第 2 回暗号技術検討会において決定された電子政府推奨暗号リストに掲載する暗号技術の選定ルールに基づき、未確定となっている評価基準案の精緻化を行い、暗号技術検討会に諮るための具体的な評価基準値の案を決定した。

(2) 利用実績の調査

新規応募暗号及び旧リスト暗号に対して、電子政府推奨暗号リストに掲載する暗号技術を選定する際の評価項目である現状の利用実績についての調査を実施した。なお、調査主体としては IPA が実施した。

３．３．３．暗号運用委員会の開催状況

2012 年度の暗号運用委員会は、計 4 回開催された。また、メール審議、並びにアドホック会合として利用実績調査報告会が開催された。各回会合の概要は表 3.3 のとおりである。

表 3.3　2012 年度暗号運用委員会の開催

回	開催日時	主な議題
第 1 回	2012 年 6 月 8 日	●暗号運用委員会活動計画について ●選定ルールのフレームワークにおける選定基準の検討について ●利用実績調査について①
第 2 回	2012 年 7 月 25 日	●選定ルールのフレームワークにおける選定基準（暗号運用委員会案）の決定 （※2012 年度第 1 回暗号技術検討会に報告） ●利用実績調査について② （※IPA が実施した利用実績調査に反映）
メール審議	2012 年 8 月 2 日 ～9 月 3 日	●第二次選定（総合評価）の個別配点基準の検討について
アドホック	2012 年 9 月 24 日	●利用実績調査報告会
第 3 回	2012 年 10 月 4 日	●総合評価の個別配点基準（暗号運用委員会案）の決定 ●選定ルールに基づく暗号運用委員会判定の決定
第 4 回	2013 年 3 月 1 日	●次年度以降の CRYPTREC 活動の検討に向けた課題の整理

３．４．合同委員会

３．４．１．開催の目的

合同委員会は 2012 年 11 月 15 日（木）に暗号方式委員会、暗号実装委員会、暗号運用委員会の 3 つの委員会の評価結果を事務局において集約した「CRYPTREC 暗号リスト」素案に関して、3 委員会において検討してきた結果と相違ないものであることを確認するために開催された。

３．４．２．議論の結果

「CRYPTREC 暗号リスト」素案に関して、3 委員会において検討してきた結果と相違ないこと、各委員会での評価結果が第１回暗号技術検討会において決定した評価基準に沿っていることが確認され、妥当なものであることが確認された。

さらに CRYPTREC における今後の検討課題に関して、暗号技術検討会事務局にて課題を特定した上で、第２回暗号技術検討会における審議を踏まえて、第３回暗号技術検討会までに確定していくことを確認した。

４．今後の CRYPTREC 活動について

CRYPTREC は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、2013 年度以降は以下の活動を実施する予定である。

なお、2013 年度からは委員会体制を以下の活動に合わせて、「暗号技術評価委員会」及び「暗号技術活用委員会」の 2 委員会体制に変更する。

(1) CRYPTREC暗号リストの小改定に関する意思決定（暗号技術検討会が実施予定）
- (a) 推奨候補暗号リストに掲載されている暗号技術の昇格方針を検討する。
- (b) 新規暗号（事務局選出）及び新技術分類の追加（新規暗号公募含む）に関する方針を検討する。
- (c) 内閣官房情報セキュリティセンター等政府関係機関との連絡・調整を実施する。

(2) 暗号技術の安全性評価を中心とした技術的な検討（暗号技術評価委員会が実施予定）
- (a) 新世代暗号に係る調査（軽量暗号、セキュリティパラメータ、ペアリング、耐量子計算機暗号等）を実施する。
- (b) 暗号技術の安全性に係る監視及び評価（SHA-3の評価を含む）を実施する。
- (c) 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）を実施する。

(3) セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討（暗号技術活用委員会が実施予定）
- (a) 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）を実施する。
- (b) 暗号技術の利用状況に係る調査及び必要な対策の検討等を実施する。
- (c) 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）を実施する。

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		該当なし
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。

[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） 128-bit RC4 は、SSL （TLS 1.0 以上）に限定して利用すること。

（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。

別添２

2012 年度　暗号技術検討会　構成員・オブザーバ名簿

（構成員）

◎	今井　秀樹	中央大学　理工学部電気電子情報通信工学科　教授
	太田　和夫	電気通信大学　電気通信学部情報通信工学科　教授
	岡本　栄司	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
	国分　明男	一般財団法人ニューメディア開発協会　顧問・首席研究員
	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
	武市　博明	一般社団法人情報通信ネットワーク産業協会　常務理事
	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））
〇	辻井　重男	中央大学　研究開発機構　教授
	中山　靖司	日本銀行　金融研究所情報技術研究センター　企画役
	本間　尚文	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
	松尾　真一郎	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 セキュリティアーキテクチャ研究室　室長（ISO/IEC JTC1 SC27/WG2（国内小委員会主査））
	松本　　勉	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研究所基盤技術ディビジョン 認証基盤グループグループリーダ
	持麾　裕之	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
	渡辺　　創	ISO/IEC JTC1 SC27　国内委員会　委員長

◎：座長、〇：顧問

（オブザーバ）

三角　育生	内閣官房情報セキュリティセンター内閣参事官
羽室　英太郎	警察庁情報通信局情報管理課長
栗原　利男	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
濱島　秀夫	総務省自治行政局地域政策課地域情報政策室長
宮地　　毅	総務省自治行政局住民制度課長
河合　芳光	法務省民事局商事課長
中村　耕一郎	外務省大臣官房情報通信課長
石田　　清	財務省大臣官房文書課業務企画室長
田中　正幸	文部科学省大臣官房政策課情報化推進室長
代田　雅彦	厚生労働省大臣官房統計情報部情報システム課長
鈴木　晴光	経済産業省産業技術環境局基準認証ユニット情報電子標準化推進室長
木村　和仙	防衛省運用企画局情報通信・研究課情報保証室長
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	独立行政法人産業技術総合研究所セキュアシステム研究部門 副研究部門長
笹岡　賢二郎	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
亀田　　繁	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
鈴田　　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

資料３

2013 年度 暗号技術評価委員会活動計画（案）

2013 年度以降の CRYPTREC の活動においては、暗号技術評価委員会で暗号技術における技術的信頼に関する検討を実施する。暗号技術評価委員会では、暗号方式委員会の全部及び暗号実装委員会の一部からの課題を主に引き継ぐ。

① 暗号技術の安全性及び実装に係る監視及び評価（SHA-3 の評価を含む）
② 新世代暗号に係る調査（軽量暗号、セキュリティパラメータ、ペアリング、耐量子計算機暗号等）
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）

1. 暗号技術の安全性及び実装に係る監視及び評価

暗号技術評価委員会では、2013 年度、以下の目的のための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。

- **推奨候補暗号リストへの新規暗号（事務局選出）の追加**

  現時点ではハッシュ関数 SHA-3 の検討を予定している。SHA-3 については、FIPS draft が出版された段階で安全性評価および実装性能評価の調査方針を検討する。その他の暗号技術についても追加すべきものがないか検討を行う。（例：SHA-224 や SHA-512/224, SHA-512/256 など）

- **既存の技術分類の修正を伴わない新技術分類の追加**

  2013 年度より軽量暗号についての検討を開始する。具体的な検討は新設する軽量暗号 WG で行う（後述）。WG での検討状況は暗号技術評価委員会に報告され、これに基づき追加方針等について議論を行う。その他の新世代暗号については、暗号解析評価 WG からの報告に基づき、必要に応じて検討を行う。

- **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**
- **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。（例：RC4 の TLS/SSL

における安全性についての詳細調査、SC2000 の等価鍵など）

- **CRYPTREC 暗号等の監視**

  国際会議等で発表される CRYPTREC 暗号等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）の監視を行う。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。監視活動は、CRYPTREC 事務局が中心となるが、必要に応じて暗号技術評価委員会委員および WG 委員からの協力も得る。

- **CRYPTREC 注意喚起レポートの発行**

  CRYPTREC 暗号等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。なお、作成については関連する委員会委員および WG 委員からの協力を得る。

2013 年度のスケジュール

7 月下旬　**第 1 回 暗号技術評価委員会**

- 活動計画案の審議・承認
- 2013 年度調査方針の審議
- WG 活動計画案の審議・承認

8 月下旬　**第 1 回 軽量暗号 WG**

9 月上旬　**第 1 回 暗号解析評価 WG**

11 月下旬　**第 2 回 暗号技術評価委員会**

- SHA-3 の調査方針について
- 旧リストガイドの改定及び技術ガイドラインについて
- WG 活動報告

12 月中旬　**第 2 回 軽量暗号 WG**

2 月　**第 2 回 暗号解析評価 WG**

第 3 回 軽量暗号 WG

第 3 回 暗号技術評価委員会

- 2013 年度調査報告及び審議
- WG 活動報告及び審議
- 2014 年度検討項目の整理

2. 新世代暗号に係る調査

暗号技術評価委員会の下に暗号技術調査 WG として「暗号解析評価 WG（計算機能力評価 WG より名称変更)」および「軽量暗号 WG（新設)」を設置し、下記の活動を行う。

2.1 暗号解析評価 WG

公開鍵暗号の安全性は、素因数分解の困難性や離散対数問題の困難性などさまざまな数学的問題に依存している。本 WG ではこれまで、素因数分解の困難性に関する調査研究に基づいて RSA1024 ビットの危殆化に関する見積りを行ったり、離散対数問題等の困難性に関する調査を行ってきた。2013 年度も下記の調査等を継続して行う。また、海外連携も視野に入れる。

- 離散対数問題の困難性に関する調査

  近年､研究の進展している有限体上あるいは楕円曲線上の離散対数問題の困難性に関する調査を行う｡離散対数問題の困難性に関する見積りを作成できるかどうかの検討を行い、可能であれば作成する。本調査の成果は、電子政府推奨暗号のうち離散対数問題の困難性に基づく方式の適切なセキュリティパラメータを選択するための技術的根拠として活用が期待できるほか､クラウド等での高度なプライバシ保護技術を可能とするペアリングの実用化に向けた技術的指針となる。

- 格子問題等の困難性に関する調査

  格子問題のほか、NP 困難に係る問題、多変数多項式に係る問題、符号理論に係る問題等、量子計算機が実現しても安全性が保たれると期待されている「耐量子計算機暗号」を支える数学的問題の困難性に関する調査を行う。

2013 年度のスケジュール

9 月上旬　**第 1 回 暗号解析評価 WG**

- 本年度活動内容の審議・承認

(外部評価レポートの執筆、ML での中間報告)

2 月中旬　**第 2 回 暗号解析評価 WG**

- 評価レポートの審議・承認

2.2　軽量暗号 WG (新設)

リソースの限られたデバイスにも実装可能な「軽量暗号」(Lightweight Cryptography) の研究開発および国際標準化が進展してきた。低コスト・低消費電力で動作可能な軽量暗号技術は、今後もスマートカードや RFID タグ、センサー、医療機器をはじめさまざまな用途での利用が期待されており、M2M, IoT といった次世代のネットワークサービスのセキュリティを構築する上で欠かせない技術となると考えられる。

本 WG では、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利用者が最適な暗号方式を選択でき、容易に調達できることをめざし、軽量暗号技術に求められる要求条件や評価方法等を検討する。WG での検討状況を見極め、軽量暗号に関する技術ガイドライン発行、共同開発、公募等、どのアプローチが望ましいかを検討する。公募は国内メーカ等に限定せず、海外からも広く方式を募ることも検討する。これらの活動により、次世代の暗号技術を担う人材を育成するとともに、海外連携をはかることも視野に入れる。

スケジュール案

2013　軽量暗号 WG 立ち上げ
2014　要求条件や評価方法の検討、(公募を行う場合)公募要項作成
2015　軽量暗号技術の公募
2016　評価
2018　評価結果発表
　　ISO/IEC, IETF 等へ展開

2013 年度のスケジュール

8 月下旬　**第 1 回 軽量暗号 WG**

- 軽量暗号技術に関する現状調査について方針・分担の審議（アルゴリズム一覧、実装性能、活用事例、標準化動向）
- アプリケーションに関する議論（既存暗号技術でカバーできないのはどこか、軽量暗号の活用が期待される分野の整理、ヒアリング先の検討）
- CRYPTREC における軽量暗号技術の方針についての議論

12 月中旬　**第 2 回 軽量暗号 WG**

- 軽量暗号技術に関する現状調査中間報告
- 実装評価（外部委託予定）中間報告

- アプリケーションに関する議論（エンドユーザからのヒアリング）
  - 例：車、医療系、スマートメータなど

2 月下旬　**第 3 回 軽量暗号 WG**

- 軽量暗号技術に関する現状調査報告
- 実装評価（外部委託予定）最終報告
- アプリケーションに関する議論
- CRYPTREC における軽量暗号技術の方針決定（ガイドライン作成/公募/共同開発）
- 2014 年度の検討項目の抽出

3. 暗号技術の安全な利用方法に関する調査

暗号技術評価委員会では、暗号技術の安全な利用方法に関して、2013 年度、下記の活動を行う。

- CRYPTREC 暗号技術ガイドラインの発行

  SSL/TLSにおける近年の攻撃に関して、その攻撃手法の概要、システムに対する影響を分析するとともに、暗号スイートにおける安全性の観点での影響について、CRYPTREC 暗号技術ガイドラインを作成する。暗号技術活用委員会で作成されるSSL運用ガイドラインから参照される技術解説という位置づけで作成する。

  記載内容

  - BEAST, TIME, Lucky Thirteen などの SSL/TLS を対象とした攻撃の概要と技術評価
  - SSL/TLS を用いたシステムに与える影響
  - 攻撃の影響を受ける条件
  - 電子政府推奨暗号リスト掲載暗号に基づいた回避方法（古いバージョンの TLS を使わざるを得ない場合、RC4 とブロック暗号のどちらがふさわしいかの技術評価も行う）と、SSL/TLS における暗号技術の応用に関する技術的な安全性評価結果（個別の CipherSuite については記述しない）

- 発行済みリストガイドの改定

  「CRYPTREC 暗号リスト」に対応する旧リストガイドの改定方針を議論し、改定・再発行の必要があるものは、暗号技術活用委員会との連携のもとで新たなガイドラインとして発行する。

- CRYPTREC 運用監視暗号リストに関するガイドラインの発行

  CRYPTREC 運用監視暗号リストに入った暗号技術を利用する際の技術面での注意点について必要な検討を行い、CRYPTREC 暗号技術ガイドラインとして発行する。

  記載内容

  - CRYPTREC 運用監視暗号リスト掲載暗号の想定される応用
  - 当該応用方法における安全性評価と、運用をやめるべき技術的条件

- CRYPTREC 暗号技術ガイドラインの情報提供方法についての検討

  CRYPTREC としての情報提供方法、統一 Web サイトのあり方について議論する。

4. 暗号技術評価委員会委員(調整中)

5. 暗号技術評価委員会英語名称(案)

暗号技術評価委員会： Cryptographic Technology Evaluation Committee

資料４

2013 年度 暗号技術活用委員会活動計画（案）

１．活動目的

2013 年度以降の CRYPTREC の活動においては、2012 年度に「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）」が策定されたことに鑑み、我が国の暗号政策に係る中長期の視野に立って課題に引き続き取り組むため、平成 24 年度までの暗号方式委員会・暗号実装委員会・暗号運用委員会の 3 委員会体制から、暗号技術評価委員会・暗号技術活用委員会の 2 委員会体制に改組された。

暗号技術活用委員会では、2012 年度暗号運用委員会の全部及び暗号実装委員会の一部からの課題を主に引き継ぎ、暗号技術における国際競争力の向上及び運用面での安全性向上に関する検討を実施する。主な検討課題は以下の通り。

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）
② 暗号技術の利用状況に係る調査及び必要な対策の検討等
③ 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）

２．活動概要

2013 年度は、暗号技術の利用状況に係る調査を実施する予定がないことから、①暗号の普及促進・セキュリティ産業の競争力強化に係る検討、及び③暗号政策の中長期的視点からの取組の検討（暗号人材育成等）についてのみ実施する。

2.1. 暗号の普及促進・セキュリティ産業の競争力強化に係る検討

CRYPTREC 暗号リストの策定により、同リストに掲載されている暗号アルゴリズムの普及が促進し、ひいては日本のセキュリティ産業の競争力強化につながることが期待されている。

しかし、現実には「優れた暗号アルゴリズムがセキュリティ産業の競争力強化に直接的に繋がる」という関連性については、2012 年度運用委員会の委員ならびに CRYPTREC シンポジウム 2013 でのパネリストから極めて懐疑的な意見が多数出された。また、2012 年度の暗号技術の利用状況に係る調査結果からは、旧電子政府推奨暗号リスト策定から 10 年経過していたにもかかわらず、同リストに掲載されていた国産の暗号アルゴリズムの普及がほとんど進んでいない実態も明らかとなった。

そのため、本委員会では、「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析について約 2 年間の集中審議期間を設けることにより、暗号アルゴリズムの普及促進やセキュリティ産業の競争力強化に向けた障壁が何かを明らかにするとともに、その解決策を取りまとめる。

2013 年度は、上記課題分析を行うにあたっては幅広く現況を俯瞰する必要があることから、議論を行ううえで有用な基礎データの収集を取りまとめる。すぐに対応可能な課題には本年度中に取り掛かるが、本格的な課題分析や具体的な解決策の検討についてはタイムスケジュールを作成する。

- 各種団体（政府機関を含む）等へのヒアリング
- セキュリティ産業競争力の源泉の俯瞰（市場動向など）
- 政策動向（共通番号制度、医療ガイドラインなど）
- 工程表の作成

2.2. 暗号政策の中長期的視点からの取組の検討

人材育成の観点に関しては、様々なシステムを安全に動かしていく人材にとって、暗号についての必要な知識やスキルがどういうものかを検討することにより、CRYPTREC として取り組むべき課題を明らかにする。

- 各種団体（政府機関を含む）等へのヒアリング
- 工程表の作成

2.3. 標準化推進

様々な標準化機関に対して日本から提案する暗号アルゴリズムが受け入れられるようにするため、標準化活動の取り組みを横断的に支援・意見交換する WG（標準化推進 WG）を設置し、日本からの暗号アルゴリズム提案の効率的な横展開を図る。

標準化推進 WG

- 10～15 程度の標準化団体を対象に、その団体でのキーパーソンを委員に選任
- 2013 年度は、各標準化団体に対して、自らの活動状況や日本からの提案事項における交渉ノウハウや課題などを共有・蓄積し、暗号アルゴリズムの標準化提案に当たっての俯瞰図を取りまとめる
- 2013 年度は 2 回の会合を予定

2.4. 運用ガイドラインの作成

暗号に関する一定水準以上の知識・リテラシーがあることを前提とせずに、暗号システムとして安全に利用できるようにするための運用ガイドラインを、運用ガイドライン WG を設置して作成する。

2013 年度は、利用者が非常に多く、また暗号に関するリテラシーのレベルにも大きな差がある「SSL/TLS」について作成する。

「運用ガイドライン」の位置づけ

- 「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル ～安心・安全のための暗号利用法～」のようなガイドラインを目指す
  - 「易しい暗号技術解説書」ではなく「Best Practice 集」
  - 暗号に関連する“技術的なこと”は原則説明しない
  - 暗号に直接関連しないことでも必要・重要なことは説明する
  - 代表的な製品・OSS について具体的な設定方法を記載する

- 「暗号技術評価の厳密な根拠」よりも「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視して利用方法をまとめる
  - 「暗号による根拠説明」よりも「別の根拠説明」のほうが合理的なら後者を中心とした説明を行う
  - 注釈は一切付けない
  - 「技術的に推奨できるもの」であっても、①製品に搭載されていない（利用できる製品が限定的）、②現状利用者が明らかに少ない、③暗号を知っている技術者・SIer が設定すべきもの、のいずれかに該当するものについては「推奨対象に含めない」
  - 「技術的に推奨できないもの」であっても、“レッドライン”を超えていないものであって、かつ①代替技術が存在していない、②代替技術があっても実際に利用できる製品が限定的、である場合には「使ってはダメ」とは言わない
  - 「厳密な根拠」での成立条件が現実的ではない、もしくは別の実施すべき対策によって成立条件が成立しなくなると判断できる場合には、そのほかの「合理的な根拠」に基づいて利用方法をまとめる

- 「推奨」よりも「ベースライン」を重視する
  - 「ベースライン」は、合理的な根拠に基づいて、暗号技術評価委員会と調整のうえ、使ってはいけない“レッドライン”として明示的に設定する
  - ①「ベースライン」と「推奨」の間に自己リスクで推奨以外のものを使ってもよい範囲を置く、②その際に考えなければいけない事柄（＝引き受けるリスク）の明示、③自己リスク評価ができないなら推奨を使う、の 3 段構成とする
  - ユースケースの違いによって、「ベースライン」や「推奨」についていくつかの差をつける

<u>運用ガイドライン WG</u>

- 10～15 名程度の SSL/TLS に関連（技術がわかる、サービスを提供している、製品を出している、エンドユーザと接点がある）する有識者で構成
- 2013 年度は 2 回の会合を予定するとともに、メールでの“作業”を中心とした運営を行う

３．委員（調整中）

４．2013 年度スケジュール（案）

回	開催日	議案
第 1 回	2013 年 8 月下旬～9 月上旬	● 活動計画案の審議・承認 ● 2013 年度調査方向性の審議 ● ヒアリング内容（ヒアリング先を含む）の審議 ● WG 活動計画案の審議・承認
第 2 回	2013 年 11 月下旬～12 月上旬	● 2013 年度調査の中間報告及び審議
第 3 回	2014 年 2 月下旬	● 2013 年度調査の報告及び審議（課題抽出） ● 課題解決に向けた 2014 年度の検討項目の抽出 ● WG 活動報告 ● SSL/TLS に関する運用ガイドラインの取り纏め
	2015 年 2 月下旬	● 課題解決に向けた分析結果・対策を取り纏め

５．英語名称（案）

暗号技術活用委員会： Cryptographic Technology Promotion Committee

以上

資料５

CRYPTREC の暗号アルゴリズム仕様書について

「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）」が 2013 年 3 月に公表された。CRYPTREC 暗号リストは、2003 年に発表された「電子政府推奨暗号リスト」を改定したものであり、「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」の３つで構成される。

CRYPTREC 暗号リストに掲載されている暗号技術の仕様書の参照先を確認した結果、外部機関の仕様書を参照しているもののうち、廃版になったり、更新されたものがあり、参照先の変更が適当 と考えられるものがある。下記に示す通り修正して問題ないか、第 1 回暗号技術評価委員会で確認を行い、その後、CRYPTREC 統一 Web ページにて「CRYPTREC 暗号リスト」掲載の暗号仕様書一覧を公開する。

1. CRYPTREC 暗号リストの仕様書

「電子政府推奨暗号リスト」掲載の暗号仕様書一覧

技術分類		暗号名称	仕様書	旧仕様書
公開鍵暗号	署名	DSA	NIST FIPS PUB 186-3	NIST FIPS 186-2 (+Change Notice 1)
		ECDSA	SEC 1: Elliptic Curve Cryptography (May 21, 2009 Version 2.0) または ANS X9.62-2005 (*2)	SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) または ANS X9.62-2005
		RSA-PSS	EMC Corporation Public-Key Cryptography Standards (PKCS)#1 v2.2	RSA Security Inc. Public-Key Cryptography Standards (PKCS)#1 v2.1
		RSASSA-PKCS1-v1_5	EMC Corporation Public-Key Cryptography Standards (PKCS)#1 v2.2	RSA Security Inc. Public-Key Cryptography Standards (PKCS)#1 v2.1
	守秘	RSA-OAEP	EMC Corporation Public-Key Cryptography Standards (PKCS)#1 v2.2	RSA Security Inc. Public-Key Cryptography Standards (PKCS)#1 v2.1

	鍵共有	DH	ANS X9.42-2003(*2) または NIST SP 800-56A (March 2007) においてFFC DHプリミティブとして規定されたもの	ANS X9.42-2003 または NIST SP 800-56A においてFFC DHプリミティブとして規定されたもの
		ECDH	SEC 1: Elliptic Curve Cryptography (May 21, 2009 Version 2.0) または NIST SP 800-56A (March 2007) において、C(2, 0, ECC CDH)として規定されたもの。	SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) または NIST SP 800-56A (March 2007) において、C(2, 0, ECC CDH)として規定されたもの。
共通鍵暗号	64ビットブロック暗号	3-key Triple DES	NIST SP 800-67 Revision 1 (January 2012)	NIST SP 800-67
	128ビットブロック暗号	AES	NIST FIPS PUB 197	同左
		Camellia	128ビットブロック暗号 Camellia アルゴリズム仕様書 (第2版：2001年9月26日)	同左
	ストリーム暗号	KCipher-2	ストリーム暗号KCipher-2	同左
ハッシュ関数		SHA-256	NIST FIPS PUB 180-4	NIST FIPS 180-2
		SHA-384	NIST FIPS PUB 180-4	NIST FIPS 180-2
		SHA-512	NIST FIPS PUB 180-4	NIST FIPS 180-2
暗号利用モード	秘匿モード	CBC	NIST SP 800-38A	同左
		CFB	NIST SP 800-38A	同左
		CTR	NIST SP 800-38A	同左
		OFB	NIST SP 800-38A	同左
	認証付き秘匿モード	CCM	NIST SP 800-38C	同左
		GCM	NIST SP 800-38D	同左
メッセージ認証コード		CMAC	NIST SP 800-38B	同左
		HMAC	NIST FIPS PUB 198-1	同左
エンティティ認証		ISO/IEC 9798-2	ISO/IEC 9798-2:2008(*2), ISO/IEC 9798-2:2008/Cor 1:2010, ISO/IEC 9798-2:2008/Cor 2:2012, ISO/IEC 9798-2:2008/Cor 3:2013	同左
		ISO/IEC 9798-3	ISO/IEC 9798-3:1998(*2), ISO/IEC 9798-3:1998/Amd 1:2010(*2), ISO/IEC 9798-3:1998/Cor 1:2009, ISO/IEC 9798-3:1998/Cor 2:2012	同左

「推奨候補暗号リスト」掲載の暗号仕様書一覧

技術分類		暗号名称	仕様書	旧仕様書
公開鍵暗号	署名	該当なし		
	守秘	該当なし		
	鍵共有	PSEC-KEM	PSEC-KEM 仕様書version 2.2 (2008 年4 月14 日)	同左
共通鍵暗号	64ビットブロック暗号	CIPHER UNICORN-E	暗号技術仕様書 CIPHERUNICORN-E	同左
		Hierocrypt-L1	暗号技術仕様書:Hierocrypt-L1 (May 2002)	同左
		MISTY1	暗号技術仕様書 MISTY1 (updated 2002年5月13日)	同左
	128ビットブロック暗号	CIPHER UNICORN-A	暗号技術仕様書 CIPHERUNICORN-A	同左
		CLEFIA	128ビットブロック暗号 CLEFIA 暗号技術仕様書 Version 1.0	同左
		Hierocrypt-3	暗号技術仕様書:Hierocrypt-3 (May 2002)	同左
		SC2000	共通鍵ブロック暗号SC2000 暗号技術仕様書 (2001 年9 月26 日)	同左
	ストリーム暗号	MUGI	疑似乱数生成器MUGI 仕様書 Ver. 1.3 (2002 年5 月8 日)	同左
		Enocoro-128v2	疑似乱数生成器Enocoro 仕様書 Ver. 2.0	同左
		MULTI-S01	仕様書 MULTI-S01 暗号 第1.2 版 (2002年5月12日)	同左
ハッシュ関数		該当なし		
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	暗号技術仕様書 PC-MAC-AES	同左
エンティティ認証		ISO/IEC 9798-4	ISO/IEC 9798-4:1999(*2), ISO/IEC 9798-4:1999/Cor 1:2009, ISO/IEC 9798-4:1999/Cor 2:2012	同左

「運用監視暗号リスト」掲載の暗号仕様書一覧

技術分類		暗号名称	仕様書	旧仕様書
公開鍵暗号	署名	該当なし		
	守秘	RSAES-PKCS1-v1_5	EMC Corporation Public-Key Cryptography Standards (PKCS)#1 v2.2	RSA Security Inc. Public-Key Cryptography Standards (PKCS)#1 v2.1
	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 (Arcfour)	RC4はRSA社のトレードマークである。 128-bit RC4は、SSL3.0/TLS1.0以上に限定して利用することを想定している。 仕様に関する技術情報に関しては、以下の論文を参照のこと。 Fluhrer Scott, Itsik Mantin, and Adi Shamir. Attacks On RC4 and WEP. CryptoBytes, Vol5, No.2, P.26, Summer/Fall 2002	同左
ハッシュ関数		RIPEMD-160	The hash function RIPEMD-160	同左
		SHA-1	NIST FIPS PUB 180-4	NIST FIPS 180-2
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	ISO/IEC 9797-1:2011(*2)	同左
エンティティ認証		該当なし		

(*2)仕様書は、一般財団法人　日本規格協会で購入が可能です。

仕様書のリンク先が、他の団体のWebとなっている場合は、仕様書の管理はその団体が実施することになります。 もしリンクが切れていましたら、CRYPTREC事務局までご一報下さいますと幸いです。

2. 旧仕様書(参照先)からの変更点

2.1 DSA

旧仕様書：NIST FIPS 186-2 (+Change Notice 1)

FIPS のバージョン更新に対応し、リンク先を変更。

186-2 → 186-3

変更点：規格書構成の大幅変更であるが、DSA のアルゴリズム自体の変更はなし。

FIPS186-2 は廃版となり、FIPS186-3 に置き換わっている。

2.2 ECDSA / ECDH

ECDSA旧仕様書：SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0)
または ANS X9.62-2005

ECDH旧仕様書：SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0)
または
NIST SP 800-56A (March 2007) において、C(2, 0, ECC CDH)として規定されたもの。

IPA・JCMVP チームから SEC1 のバージョン更新に対応すべきとの提案があった。

JCMVP では ECDSA 及び ECDH で SEC1 Version 1.0 を参照しているが、使えるハッシュ関数が SHA-1 限定で、CRYPTREC の方針と合致しないのではとのこと。

SEC1 Version 2.0 ではSHA-1, SHA-224, SHA-256, SHA-384, SHA-512 に対応可能。

2.3 RSA-PSS / RSASSA-PKCS1-v1_5 / RSA-OAEP / RSAES-PKCS1-v1_5

旧仕様書：RSA Security Inc. Public-Key Cryptography Standards (PKCS)#1 v2.1

PKCS#1 のバージョン更新に対応し、リンク先を変更。

2.1 → 2.2

変更点 : FIPS180-4 に対応し、SHA-224, SHA-512/224, SHA-512/256 が追加された。

Version 2.1 のスキームはすべてサポートされている。

2.4 DH / ECDH

旧仕様書：ANS X9.42-2003　または

NIST SP 800-56A においてFCC DHプリミティブとして規定されたもの

SP のバージョン更新に対応し、リンク先を変更。

800-56A → 800-56A (March 2007)

変更点：アルゴリズムに関する変更点はなし。

2.5 3-key Triple DES

旧仕様書：NIST SP 800-67

SP のバージョン更新に対応し、リンク先を変更。

800-67A → 800-67A Revision 1 (January 2012)

変更点：アルゴリズムに関する変更点はなし。

2.6 SHA-256 / SHA-384 / SHA-512 / SHA-1

旧仕様書：NIST FIPS 180-2

FIPS のバージョン更新に対応し、リンク先を変更。

180-2 → 180-4

変更点：180-2 → 180-3 では SHA-224 の追加および 規格書構成の大幅変更(安全性に関する記述は NIST SP800-107 に移動、テストベクトル及び OID は NIST の別ホームページに移動)

180-3 → 180-4 では SHA-512/224, SHA-512/256 が追加された。

FIPS180-2, 180-3 は廃版となり、FIPS180-4 に置き換わっている。

参考資料１

２０１２年度　第３回暗号技術検討会　議事概要

１．日時　平成２５年２月２２日（金）　１５：００～１６：１５

２．場所　経済産業省本館２階　２東３共用会議室

３．出席者（敬称略）

構成員：今井 秀樹（座長）、辻井 重男（顧問）、太田　和夫、岡本 栄司、金子 敏信、国分 明男、佐々木　良一、武市 博明、近澤 武、中山 靖司、本間 尚文、時田 俊雄（松井 充 構成員代理）、松尾 真一郎、松本 勉、松本 泰、渡辺　創

オブザーバ：三角 育生、羽室 英太郎、大平　利幸（栗原 利男代理）、中山 紀雄（濱島 秀夫代理）、楢木野 由善（中村 耕一郎代理）、浜田 和之（代田 雅彦代理）、谷口　晋一（木村 和仙代理）、平 和昌、寶木 和夫、笹岡 賢二郎

暗号方式委員会事務局：盛合 志帆（独立行政法人情報通信研究機構（ＮＩＣＴ））

暗号実装委員会事務局：大熊 建司（独立行政法人情報処理推進機構（ＩＰＡ））

暗号運用委員会事務局：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　阪本 泰男、山碕 良志、上原 哲太郎、飯田 恭弘、吉田 丈夫、橋本 直樹

経済産業省　中山　亨、上村 昌博、中谷 順一、守山 速飛

４．配布資料

（資料番号）	（資料名）
資料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）」（案）に対する意見並びにこれに対する総務省及び経済産業省の考え方（案）
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（CRYPTREC 暗号リスト）（案）
資料３	今後の検討課題に関する方針（案）
資料４	2013 年度 暗号技術検討会及び関連委員会の体制（案）
参考資料１	2012 年度 第２回 暗号技術検討会議事概要
参考資料２	次期電子政府推奨暗号リスト策定スキーム
参考資料３	電子政府推奨暗号リスト（現行リスト）
参考資料４	2012 年度　暗号技術検討会　構成員・オブザーバ名簿
参考資料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）」（案）に対する意見募集（平成 24 年 12 月 12 日報道発表）
参考資料６	2012 年度　CRYPTREC シンポジウム開催のご案内

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、総務省の阪本政策統括官から開会の挨拶。

参考資料４について、岡本 龍明構成員、松井 充構成員（時田 俊雄氏が代理出席）、持麾 裕之構成員は欠席。

２　議事

（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）について【承認事項】

資料１及び資料２に基づき、意見募集で寄せられた意見に対する考え方、意見募集の結果を踏まえたCRYPTREC暗号リスト（案）を暗号技術検討会事務局から説明。質疑等なし。原案どおり承認。

（２）今後の検討課題に関する方針（案）ついて【討議事項】

資料３に基づき、今後の検討課題に関する方針案を暗号技術検討会事務局から説明。以下質疑等を踏まえた修正については座長に一任され、暗号技術検討会事務局にて修正案を作成、座長の確認後、各構成員にメールにて送付されることとなった。

○CRYPTRECに求められる活動

辻井顧問：資料中にも触れられているが、プライバシー保護等と個人情報活用の両立にあたって、暗号技術を活用することが求められている。主催しているフォーラムでも暗号の重要性を発信しているが、例えば医療の現場等、なかなか社会に理解されない印象がある。管理（Management）、倫理（Ethics）、法制度（Law system）及び技術（Technology）を合わせて「MELT」とすれば、これら四者の密接な結合と連携による「MELT-UP」が今まさに求められている。暗号化されていればプライバシー情報とすべきではないとの意見がある、とは第２回検討会においても議論があったが、暗号の活用を考えれば技術論だけでなく、法律家との連携が求められている。暗号の活用方法の一つとして電子署名があるが、社会保障・税番号制度における公的個人認証のように電子行政全体の在り方を考えていくことがどこかの場で必要ではないか。

松本（泰）構成員：同様に、CRYPTRECとして視野を広げるべきとの観点から２点申し上げたい。１点目は例えば「２．暗号技術に関する検討」においても「暗号応用」としてプロトコルだけに着目されているが、もっと広く、例えばプライバシー保護等のニーズから求められている暗号の応用にCRYPTRECが視野を広げるべきではないかということ。２

点目は、評価された暗号アルゴリズムが簡単には破れることのない、信頼できる技術に成熟してきた現状を踏まえ、国産暗号アルゴリズムの普及だけにとどまらず、広義の暗号技術の普及のために必要な活動にCRYPTRECが取り組むべきなのではないか、ということ。例えば米国のHIPPAでは暗号化していなかった場合の情報流出に対するペナルティが定められており、これが暗号技術製品開発の強いインセンティブになっている。また、ネット選挙活動の実施のためには、例えばS/MIME技術を活用した電子メールへの電子署名が有用であり、このような応用分野にも目を向ける必要があるのではないか。

佐々木構成員：松本（泰）構成員の御発言と一部重複するが、暗号アルゴリズムそのものは信頼できても、プロトコルまで視野を広げると現実的な攻撃の脅威が知られている。現在の検討会は主に暗号アルゴリズムの専門家で構成されていると思うが、求められる課題によって体制も変えていく必要があるだろう。

辻井顧問：欧州のENISAでも、インシデントが起きた際にどれだけ準備していたかで措置が変わってくるとも聞いている。セキュリティ政策の全ての課題をCRYPTRECで担うべきとは思わないが、社会のニーズに着目してキメの細かい議論が暗号利用の現場、法律家とも求められているように感じる。

今井座長：セキュリティ政策全体を考えたときには、やるべきことは多い。それぞれの役割の中で、CRYPTRECとしては何をするのか、具体論を描いていく必要があるのではないか。

暗号技術検討会事務局：CRYPTREC以外の関係者と対話し、他の組織や会議体と連携することも模索したい。体制を含んで本格的に検討を開始するとなれば、来年度、再来年度にかけて腰を据えて取り組んでいくことも考えたい。また、CRYPTRECシンポジウム2013でも、本日頂いた御意見を踏まえた今後の取組の発信を考えたい。また、暗号アルゴリズムに議論が閉じていることが暗号技術の普及が進まない一因との意見も聞かれる。資料との関係で言えば、１－ウの「普及展開の促進策」については暗号アルゴリズムに着目した普及であるが、３－アの「暗号技術の利用促進」については、暗号アルゴリズムだけでなく、その応用分野に取り組んでいく方針として捉えており、本日頂いた御意見に留意して今後のCRYPTRECの活動を進めていきたい。

〇小改定の実施時期

松本（勉）構成員：資料中、次回小改定の時期について「３年（又は２年）」とあるが、３年か２年かはいつ決めるのか。仮に２年だとすれば、作業スケジュールの関係から早めに決定する必要があるのではないか。

暗号技術検討会事務局：利用実績調査をどの頻度で実施するかも考慮し

なければならない。構成員の方々から２年とする御意見があるかは、伺いたい。また、２００９年度の公募時点で３リストの関係を図示した際に、推奨候補暗号リストから削除するにあたって「３年経っても製品化されないもの」の記載があるため、３年目の利用実績調査を先に示した。

松本（勉）構成員：コスト的な視点から、２年とすることは難しい面がある、と受け取って良いか。

暗号技術検討会事務局：予算の確保だけの面で言えば、２年ごとの利用実績調査を実施することは不可能でない。１０年間の中で、どのように定期的に利用実績を確認していくべきか、という視点に立ち、２０１３年度第１回検討会において各委員会の活動計画を承認するまでに、明確化することとしたい。

松本（勉）構成員：暗号運用委員会では今回のリスト案作成のための利用実績調査で、ノウハウが蓄積された側面もある。次に調査が必要となった場合には、今回より効率的な方法で実施することができるだろう。

〇軽量暗号の検討の進め方

今井座長：軽量暗号の取扱いに係る検討の進め方についてはいかがか。

暗号方式委員会事務局：軽量暗号が利用されている用途、求められているニーズについて検証するため、ＷＧを設置して検討していきたいと考えている。

今井座長：最初の小改定が２年後だとすると、間に合うか。

暗号方式委員会事務局：もう少し長いスパンでの検討を想定していた。

今井座長：軽量暗号については、いわゆる国産暗号としての強みもあり、暗号技術の普及、産業競争力の強化の観点から CRYPTREC としても是非取り組むべき課題だと認識している。標準化の進捗に照らしても、早めの検討が求められているのではないか。

〇人材育成

松本（勉）構成員：「暗号人材育成に向けた取組」については、プライバシー保護と個人情報活用の両立のニーズだけが具体的に言及されているが、より多様な人材が求められているのではないか。例えば、１０年後の CRYPTREC 事務局が務まる人材、暗号をベースに産業界で活躍する人材、暗号研究を担う人材、暗号の標準化を推進する人材もある。

暗号技術検討会事務局：具体的に記載する修正案を考えたい。

今井座長：本日の議論をもとに、資料の修正案を暗号技術検討会事務局にて作成頂きたい。また、今後の修正については座長に一任願いたい。

（異議無し）

暗号技術検討会事務局:資料の修正版については、座長に御確認頂いた後、構成員の皆様にメールで配付することとし、また、来年度の各委員会の活動計画に反映させていくこととしたい。

（３） 2013 年度 暗号技術検討会及び関連委員会の体制（案）について【承認事項】

資料４に基づき、2013 年度の暗号技術検討会及び関連委員会の体制（案）について暗号技術検討会事務局から説明。質疑等なし。原案どおり承認。

（４） その他

暗号方式委員会事務局から、CRYPTREC シンポジウム 2013 の開催について、プログラム及びパネルディスカッションの概要が説明された。

３ 閉会

経済産業省の中山商務情報政策局審議官から閉会の挨拶。

暗号技術検討会事務局から、次回暗号技術検討会の時期、場所等の詳細については、別途連絡する旨が説明された。

以上

今後の検討課題に関する方針

参考資料２

１．今回改定されたCRYPTREC暗号リストに関する検討

ア．次回改定のタイミングについて

（方針） 全面改定は頻繁には行わない（10年程度の運用を想定する）ものの、小改定（推奨候補暗号リストから電子政府推奨暗号リストへの昇格等）は定期的（3年を目途）に見直しをする方向とする。また、運用監視暗号リストへの降格等は随時改定することとする。加えて、各年度で作成する技術ガイドラインの効果的利用方法も検討する。

CRYPTREC暗号リストの改定方法（全面改定、小改定、随時改定）のイメージ

各年度で作成する技術ガイドラインも効果的に利用

①全面改定 ： 以下は、10年を目途に、安全性、実装性能、利用実績（見込み含む）の検討に基づき、全面改定で対応する。
- 既存の技術分類の修正を伴う技術分類見直し、3リスト構成そのものの見直し、新規暗号の全面的公募等

②小改定 ： 以下は、3年を目途に、安全性、実装性能、利用実績（見込み含む）の検討に基づき、小改定で対応する。
- 推奨候補暗号リストへの新規暗号（事務局選出）の追加（現時点ではSHA-3を想定）
- 推奨候補暗号リストから電子政府推奨リストへの昇格
- 推奨候補暗号リストからの製品化されていない暗号の削除

以下は、実施方法及び実施時期等の検討に基づき、小改定で対応する。
- 既存の技術分類の修正を伴わない新技術分類の追加（現時点では軽量暗号（公募を含む）を想定）

③随時改定 ： 以下は、安全性の検討に基づき、随時改定で対応する。
- 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（既存システムへの影響調査要）
- 運用監視暗号リストからの危殆化が進んだ暗号の削除（既存システムへの影響調査要）

１．今回改定されたCRYPTREC暗号リストに関する検討（続き）

イ．運用監視暗号リストの扱い （遷移方法、移行期間等）

（方針） CRYPTRECが暗号の安全性を監視し、必要性、緊急性、重要度等を踏まえ、適切に暗号技術の安全性情報を提供できる体制を検討。

→ 具体策①： 安全性情報の監視及び提供のあり方の検討

→ 具体策②： 中長期的な暗号移行に向けた取扱い指針の整備

ウ．普及展開の促進策

（方針） CRYPTREC暗号リストに基づく暗号技術の利用の推進により企業・個人におけるセキュリティ対策を促進するとともに、セキュリティ関連産業の競争力強化を図るため、以下の取組を実施する。

→ 具体策①： 技術ガイドラインを充実（各暗号利用における注意点）

→ 具体策②： 運用ガイドライン（教育啓発資料を含む。）を作成

→ 具体策③： 政府内調達担当向けの講習会等を活用しCRYPTREC暗号リストの紹介を積極的に行う

→ 具体策④： 広報や講演会など様々なチャネルを使用して宣伝

２．暗号技術に関する検討

ア．暗号応用プロトコルの安全性評価

（方針） 将来的にNISCやCRYPTREC暗号リスト利用者へ安全な暗号プロトコル利用に資する情報提供を行うことを念頭に、国内外で行われる暗号プロトコルの安全性評価に関する調査を行うとともに、その情報提供のあり方を検討する。

イ．新世代暗号の公募、安全性評価 （軽量暗号、ペアリング、耐量子計算機暗号等）

（方針） 既存の技術分類の修正を伴わない新技術分類の追加は、小改定で対応する。特に、軽量暗号については国際標準規格化が進展していることを踏まえ、その取扱方法について2013年度から検討を開始する。一方、既存の技術分類の修正を伴う技術分類見直しは全面改定で対応する。

3. 暗号技術の利用促進・産業化に向けた取組の検討

ア. 目標、ロードマップ

（方針） 国産暗号の活用を視野に、暗号技術を活用した製品・サービスの開発の利用促進策を検討する。

→ 具体策①: 国産暗号導入を阻む課題について調査分析して必要な対策を検討

→ 具体策②: 国産暗号の利用場面を整理して必要な対策を検討

（軽量暗号等の技術分類の追加や利用実績（見込み含む）の無い推奨候補暗号の削除等）

イ. 国際標準化活動とのリンク

（方針） 国産暗号について以下の国際標準化活動に関する取組を実施する。

→ 具体策①: ISOやその他の国際機関における他国の活動を定期的にフォロー

→ 具体策②: IETFにおける国産暗号に関する国際標準化活動をフォロー

4. 暗号人材育成に向けた取組の検討

（方針） プライバシー保護と個人情報活用の両立へのニーズ等の昨今の状況を踏まえながら、以下の暗号人材育成策を検討する。なお、2013年度については、必要な人材像についての検証を行う。

→ 具体策①: 政府全体の情報セキュリティ人材育成施策と協調

→ 具体策②: スキルマップやキャリアパスの提示

その他:

ア. 暗号技術検討会の新たな成果展開方法

（方針） 民間調達に対する新たな成果展開方法について以下の取組を実施する。

→ 具体策①: 民間調達に役立つ技術ガイドラインや運用ガイドライン提示及びその積極的周知

イ. 検討会及び委員会の議論模様の積極的な公開方法

（方針） 以下のような積極的かつ効果的な公開方法を導入する。

→ 具体策①: 検討会議事概要を検討会開催から2週間以内程度でウェブサイトに掲載

→ 具体策②: ウェブサイトに各暗号技術の安全性情報ページ等を追加

→ 具体策③: トピックス等の更新頻度の向上

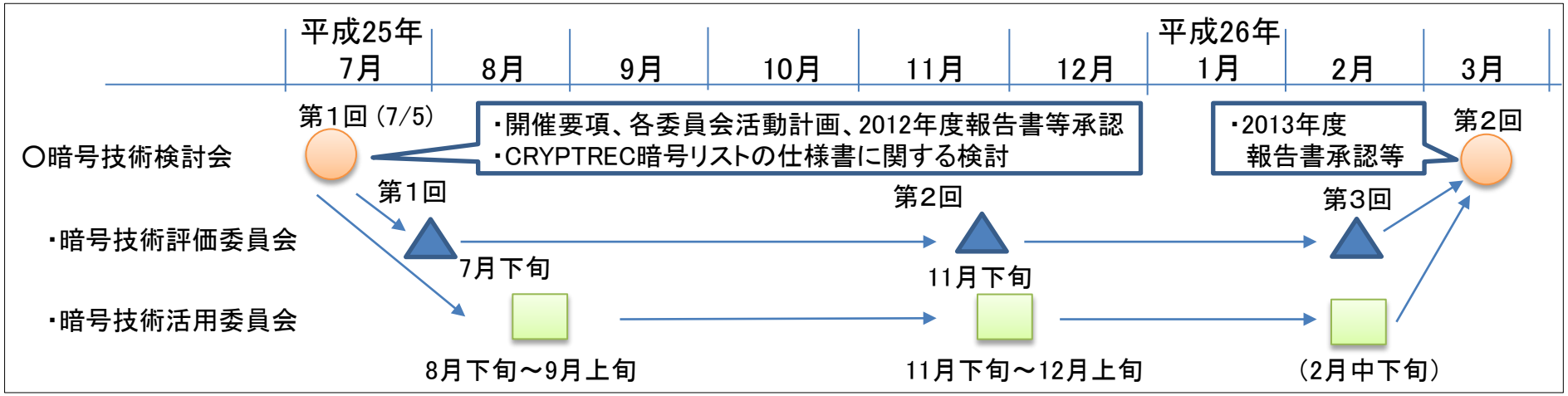
平成25年度CRYPTREC活動計画

参考資料３

平成25年7月5日　暗号技術検討会事務局

○ 本年3月、「電子政府推奨暗号リスト」を10年ぶりに改定して、「CRYPTREC暗号リスト」を策定。
○ 本年度は2委員会体制とし、「CRYPTREC暗号リスト」の普及促進等を実施。

1. CRYPTREC（暗号技術検討会及び関連委員会）の開催予定



2. 平成25年度CRYPTREC体制図及び検討事項

暗号技術検討会
座長：今井 秀樹中央大学教授
（事務局：総務省及び経済産業省）

内閣官房情報セキュリティセンター(NISC)

暗号技術評価委員会
委員長：今井 秀樹中央大学教授
（事務局：NICT及びIPA）

- 暗号解析評価WG
- 軽量暗号WG

検討事項：暗号技術の安全性及び実装に係る監視及び評価、技術ガイドラインの整備等に係る検討を行う。

暗号技術活用委員会
委員長：松本　勉横浜国立大学教授
（事務局：IPA及びNICT）

- 標準化推進WG
- 運用ガイドラインWG

検討事項：暗号の普及促進・セキュリティ産業の競争力強化、暗号人材育成等に係る検討を行う。

参考資料４

2013 年度　暗号技術検討会　構成員・オブザーバ名簿

（構成員）

今井　秀樹	中央大学　理工学部電気電子情報通信工学科　教授
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	電気通信大学　電気通信学部情報通信工学科　教授
岡本　栄司	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
国分　明男	一般財団法人ニューメディア開発協会　顧問・首席研究員
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
武市　博明	一般社団法人情報通信ネットワーク産業協会　常務理事
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））
中山　靖司	日本銀行　金融研究所情報技術研究センター　企画役
本間　尚文	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　三菱電機情報技術総合研究所　技師長 松井暗号プロジェクト統括
松尾　真一郎	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 セキュリティアーキテクチャ研究室　室長（ISO/IEC JTC1 SC27/WG2 （国内小委員会主査））
松本　　勉	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	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
渡辺　　創	ISO/IEC JTC1 SC27　国内委員会　委員長

（オブザーバ）

奥山　　剛	内閣官房情報セキュリティセンター企画官
羽室　英太郎	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
増田　直樹	総務省自治行政局地域政策課地域情報政策室長
篠原　俊博	総務省自治行政局住民制度課長
佐藤　達文	法務省民事局商事課長
中村　耕一郎	外務省大臣官房情報通信課長
郷　　敦	財務省大臣官房文書課業務企画室長
田中　正幸	文部科学省大臣官房政策課情報化推進室長
三富　則江	厚生労働省大臣官房統計情報部情報システム課長
辻本　崇紀	経済産業省産業技術環境局基準認証ユニット情報電子標準化推進室長
木村　和仙	防衛省運用企画局情報通信・研究課サイバー攻撃対処・情報保証企画室長
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	独立行政法人産業技術総合研究所セキュアシステム研究部門 副研究部門長
伊藤　毅志	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
亀田　　繁	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

（五十音順、敬称略）