# 暗号技術検討会

# ２０１２年度報告書

２０１３年７月

目　　次

## 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。

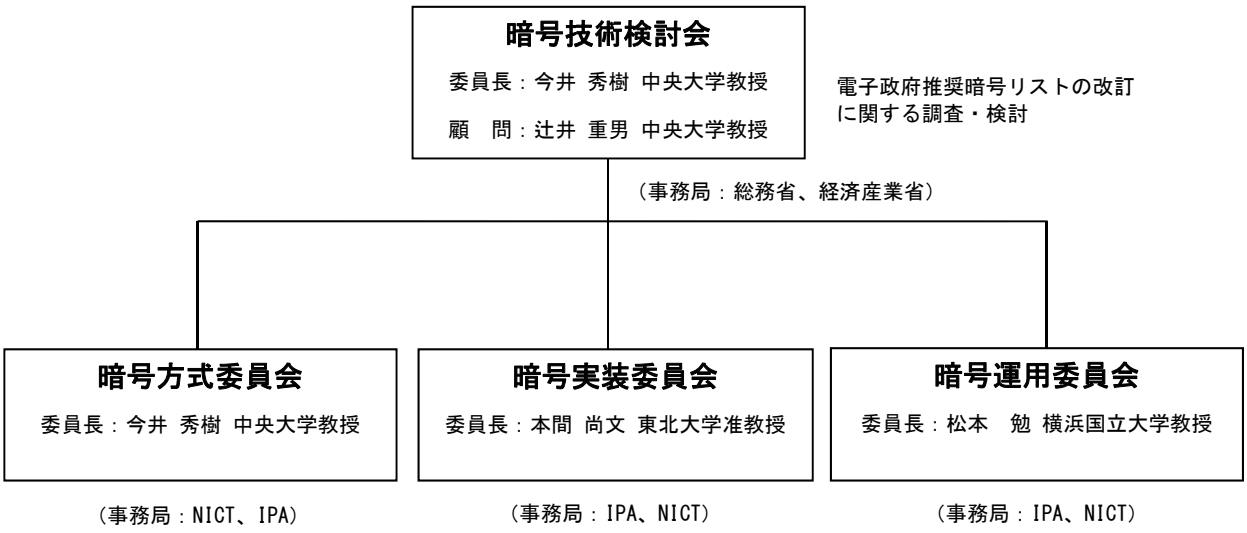


図 2.1　2012 年度 CRYPTREC の体制図

## 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<br>WG 活動方針の検討<br>安全性に関する次期リストの作成方針の検討<br>外部評価についての検討<br>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<br>安全性に関する次期リスト作成についての検討<br>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<br>安全性に関する次期リスト作成についての検討<br>評価 B の判定決定<br>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<br>WG 活動報告<br>監視状況報告<br>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<br>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<br>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<br>総合評価の判定決定<br>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<br>サイドチャネル攻撃対策の有効性確認<br>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<br>●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<br>●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<br>（※2012 年度第 1 回暗号技術検討会に報告）<br>●利用実績調査について②<br>（※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<br>～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<br>●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<br>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<br>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<br>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<br>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 |
| 寳木　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<br>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 |