2014 年度　第 1 回暗号技術検討会

日時：平成 26 年 10 月 9 日(木) 14:00～16:00
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)　2014 年度　暗号技術検討会開催要綱等について【審議事項】
(2)　2014 年度　暗号技術検討会活動計画について【確認事項】
(3)　暗号技術評価委員会の活動に関する中間報告【報告事項】
(4)　暗号技術活用委員会の活動状況【報告事項】
(5)　その他

３．閉　会

（資料番号）	（資　料　名）
資料１－１	2014 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	2014 年度　暗号技術検討会活動計画
資料３	2014 年度　暗号技術評価委員会活動中間報告
資料３別添	監視状況報告
資料４	暗号技術活用委員会の活動状況
参考資料１	2013 年度　第 2 回暗号技術検討会議事概要
参考資料２	2014 年度　暗号技術評価委員会活動計画
参考資料３	2014 年度　暗号技術活用委員会活動計画
参考資料４	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５	2014 年度　暗号技術検討会　構成員・オブザーバ名簿

資料１－１

２０１４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及び座長代理を指名できる。
（５）構成員の任期は平成２７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、平成２７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。

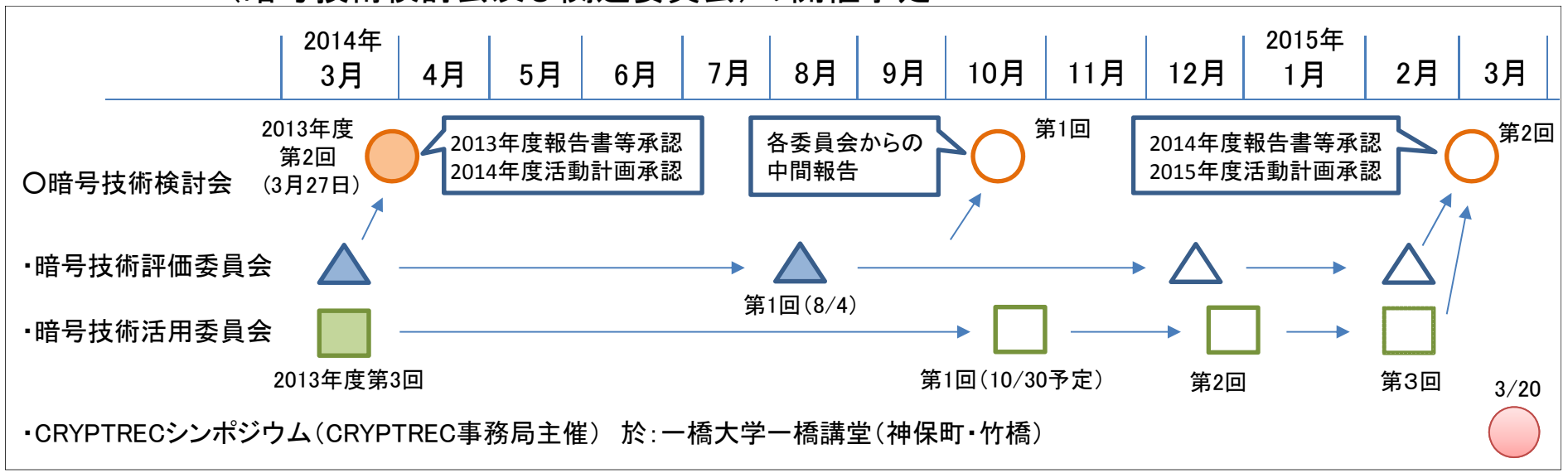
（３）議事概要は、事務局により閲覧その他の方法により公開するものとする。

2014年度　暗号技術検討会活動計画

資料2

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）の開催予定



2．2014年度CRYPTREC体制図及び検討事項

検討事項：
暗号技術に関する調査・検討

暗号技術検討会

座長：今井 秀樹（東京大学）

（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）

「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

暗号技術評価委員会

委員長：今井 秀樹（東京大学）

（事務局：NICT及びIPA（主担当はNICT））

- 暗号解析評価WG
- 軽量暗号WG

検討事項：暗号技術の安全性に関する監視・評価等

暗号技術活用委員会

委員長：松本　勉（横浜国立大学）

（事務局：NICT及びIPA（主担当はIPA））

- 標準化推進WG
- 運用ガイドラインWG

検討事項：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等

資料３

2014 年度 暗号技術評価委員会活動中間報告

1. 活動目的(2013 年度 第 2 回検討会提出資料抜粋)

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. 活動概要中間報告

(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・評価を実施中。

① CRYPTREC 暗号等の監視

- 第 1 回暗号技術評価委員会(8 月 4 日開催)にて監視状況を報告(監視状況報告は別添参照)
- 仕様書の参照先の変更(ECDSA, ECDH)については第 2 回以降の暗号技術評価委員会にて検討予定。

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

- 第 1 回暗号技術評価委員会にて、128-bit key RC4 の注釈の変更について審議を行い、暗号技術評価委員としては下記取扱いとすることが採択された。

  注釈を以下に変更。

  (現行)

  「128-bit RC4 は、SSL(TLS1.0 以上)に限定して利用すること」

  (変更案)

  「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を選択すること。」

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。

- 該当する事象は発生していない。

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。

- 第 1 回暗号技術評価委員会にて、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外部評価を実施することが承認された。報告内容は、第 3 回暗号技術評価委員会(2 月下旬予定)にて報告予定。

⑤ 既存の技術分類の修正を伴わない新技術分類の追加

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）にて調査を実施中。

(2) 新世代暗号に係る調査

- 暗号技術調査ワーキンググループ(暗号解析評価)

  第 1 回暗号解析評価ワーキンググループを 9 月 22 日に開催。

  1. 格子問題等の困難性に関する調査の更新
  2. ID ベース暗号に関する調査報告書(2008-2009 年度)の更新

  を行うことが承認され、各委員の分担についても承認された。

  第 2 回暗号解析評価ワーキンググループは、2 月中旬を予定。

- 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 8 月 29 日に開催。

  軽量暗号 WG では、CRYPTREC における軽量暗号の今後の活動方針を検討し、2014 年度末に暗号技術評価委員会へ提言を行う。この提言内容に盛り込む内容について議論を行い、各委員の分担についても承認された。今後の活動方針については、案として A)「暗号技術ガイドライン（軽量暗号の最新動向)」の発行、B)「暗号技術ガイドライン（軽量暗号の詳細評価)」の発行、C) 軽量暗号に関する技術公募の実施などが出されていたが、審議の結果、A) もしくは B) として技術ガイドラインをまとめる方向で進めていくこととなった。

  第 2 回軽量暗号ワーキンググループは、11 月 12 日に開催予定。

(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)

- 2013 年度作成の「CRYPTREC 暗号技術ガイドライン (SHA-1)」 および「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)」については公開済み。
- 第 1 回暗号技術評価委員会にて、今年度は SSL/TLS の 乱数生成、鍵生成、鍵交換などの脆弱性を踏まえた近年の攻撃の可能性や懸念事項などについて技術的な解説を行うことが承認された。

以上

（参考資料 1）　委員構成

［暗号技術評価委員会］

委員長	今井　秀樹	東京大学 名誉教授
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　マネージャー
委員	盛合　志帆	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	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 セキュアサービス研究グループ　研究グループ長

［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 ソフトウェアシステム研究所 セキュアコンピューティング研究部　主任研究員
委員	安田　雅哉	株式会社富士通研究所 ソフトウェアシステム研究所 セキュアコンピューティング研究部

［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　情報基礎科学専攻　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 計算理工学専攻　准教授
委員	小川　一人	NHK放送技術研究所　ハイブリッド放送システム研究部 上級研究員
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 システム研究開発本部 アプリケーション・プラットフォーム設計部門 セキュリティ技術推進部
委員	鈴木　大輔	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　開発第1グループ 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 ＣＰＵシステム事業推進部 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横浜研究所 エンタープライズシステム研究部　主任研究員

(参考資料 2)　開催スケジュール

[暗号技術評価委員会]

回	開催日	議題
第 1 回	2014年8月4日 開催	• 2014年度暗号技術評価委員会活動計画 • 2014 年度暗号技術調査 WG (暗号解析評価) 活動計画 • 2014 年度暗号技術調査 WG (軽量暗号) 活動計画 • 2014年度外部評価(ハッシュ関数)の実施 • RC4 の注釈変更案の選択 • 暗号技術ガイドライン今年度執筆内容 • 仕様書の参照先の変更 • 監視活動報告
第 2 回	2014年12月上旬 開催予定	• 各WG および活動内容に関する中間報告
第 3 回	2015年2月中旬 開催予定	• 各WG および各実施項目に関する活動報告 • 次年度活動計画審議

[暗号技術調査ワーキンググループ(暗号解析評価)]

回	開催日	議題
第 1 回	2014年9月22日 開催	• 2014 年度暗号技術調査 WG (暗号解析評価) 活動計画に基づく実施内容・実施方法 – 格子問題等の困難性に関する調査 – ID ベース暗号に関する調査報告書の更新
第 2 回	2015年2月中旬 開催予定	• 評価レポートの審議・承認

[暗号技術調査ワーキンググループ(軽量暗号)]

回	開催日	議題
第 1 回	2014年8月4日 開催	• 2014 年度暗号技術調査 WG (軽量暗号) 活動計画に基づく実施内容・実施方法 – 軽量暗号に関する検討 – 軽量暗号技術の現状調査 – 今後の活動方針に関する検討
第 2 回	2014年11月12日 開催予定	• 活動内容に関する中間報告
第 3 回	2015年1月下旬 開催予定	• 暗号技術評価委員会への報告内容の確認

資料３別添

監視状況報告

1. 国際会議への参加状況

2013 年度第 2 回暗号技術評価委員会(2013 年 12 月 13 日)から 2014 年度第 1 回暗号技術評価委員会(2014 年 8 月 4 日)までに、表 1 に示す国際会議に参加するとともに各種調査を行い、暗号解読技術等に関する研究動向を収集した。

表 1 国際会議への参加状況

学会名・会議名		開催国・都市	期間
TCC 2014	Theory of Cryptography Conference	米国・サンディエゴ	2/24～2/26
FSE 2014	International Workshop on Fast Software Encryption	英国・ロンドン	3/3～3/5
PKC 2014	International Conference on Practice and Theory of Public-Key Cryptography	アルゼンチン・ブエノスアイレス	3/26～3/28
Eurocrypt 2014	International Conference on the Theory and Applications of Cryptographic Techniques	デンマーク・コペンハーゲン	5/12～5/15

2. 解読技術等の動向

各国際会議における報告等(3.1～3.3)より、具体的な暗号の攻撃に関する発表を抽出し(3)、電子政府推奨暗号の安全性に直接関わる技術動向(2.1)およびその他の注視すべき技術動向(2.2)について分析を行った。

2.1 電子政府推奨暗号の安全性に直接関わる技術動向

電子政府推奨暗号リスト掲載の暗号技術に関しては、公開鍵暗号、ハッシュ関数、ブロック暗号等に対する攻撃研究が発表された。早急な対処が必要となるものではないが、既存の攻撃を凌ぐ結果である。特に重要なものとして、次の発表がある。

AES に対する単一鍵攻撃の進展

Improved Single-Key Attacks on 9-Round AES-192/256 [FSE 2014]

Leibo Li, Keting Jia and Xiaoyun Wang

AES に対する中間一致攻撃において、鍵依存篩による鍵候補の絞り込みを適用する改善を行い、AES-192 の単一鍵攻撃の解読可能段数を 9 段に伸ばした(仕様は 12 段)。データ計算量は 2^{121} の選択平文、時間計算量が $2^{177.5}$、空間計算量は $2^{186.5}$。

離散対数問題(DLP:Discrete Logarithm Problem)解読の進展

A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small

characteristic [Eurocrypt 2014, BEST PAPER]

Faruk Gologlu, Robert Granger, Gary McGuire and Jens Zumbragel

離散対数問題(DLP: Discrete Logarithm Problem)に対する新しい解読法を提示した(最優秀論文賞)。計算量評価はヒューリスティックな仮定を用いているが、小標数の場合に計算量は準多項式時間となっており、これまで最速であった関数体篩法の準指数時間を凌いでいる。電子政府推奨暗号では、電子署名アルゴリズム DSA 及び鍵共有アルゴリズム DH が関係するが、使用・推奨しているパラメーターは素体(大標数)であり、その範囲では影響しない。ただし、小標数の DLP の困難性に基づいた暗号技術を使用する場合には、新解読アルゴリズムの影響を評価する必要がある。

楕円曲線上の離散対数問題(ECDLP:Elliptic Curve Discrete Logarithm Problem)解読の進展

Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus [Eurocrypt 2014]

Jean-Charles Faugere, Louise Huot, Antoine Joux, Guenael Renault, Vanessa Vitse

楕円曲線上の離散対数問題(ECDLP: Elliptic Curve Discrete Logarithm Problem)に対する解読法の改良を提示した。電子政府推奨暗号では、鍵共有アルゴリズム ECDH が関係する。捩(ねじ)れ点写像の性質を用いる改良であり、例えば IPSEC(SECurity architecture for Internet Protocol)の鍵共有プロトコルに使われている曲線に適用可能であり、解読時間の短縮を図ることができる。まだ現実的な脅威にはなっていないが、影響範囲や効果を評価しておく必要がある。

メッセージ認証コードに対する攻撃

Generic Universal Forgery Attack on Iterative Hash-based MACs [Eurocrypt 2014]

Thomas Peyrin and Lei Wang

ハッシュベースのメッセージ認証コードに対する偽造攻撃の改良が提示された。電子政府推奨暗号では、メッセージ認証コード HMAC が関係する。例えば、任意のメッセージに対する偽造は、RIPEMD-160 を用いた HMAC では、これまで 2 の 160 乗の計算量が必要と考えられていたが、2 の 133.3 乗に改良できるという結果である。現実的脅威とはなっていないが、影響評価を行い、今後の進展に注意する必要がある。

2.2　その他の注視すべき技術動向

使用される機会が多いか今後多くなると予想される暗号プリミティブに関して、上記以外に次の事項が発表された。

ブロック暗号に対する攻撃

Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities [Eurocrypt 2014]

Celine Blondeau and Kaisa Nyberg

ブロック暗号に対する様々な攻撃間の関係(同値性、時間メモリトレードオフによる変換等)をより明らかにする発表を行った。応用例として、26 段 PRESENT に対する既知の多次元線型識別(Multi-dimensional Linear Distinguisher)攻撃が、既知の既知平文(Known Plaintext)攻撃より少ないメモリにより選択平文(Chosen Plaintext)鍵回復攻撃に変換できることを示した。関係性

の提示のため、電子政府推奨暗号に対する当面の影響はないと考えられるが、現実の攻撃条件等を考慮する際には注意しなければならない。

ハッシュ関数に対する攻撃

Practical Complexity Cube Attacks on Round-Reduced Keccak Sponge Function [Eurocrypt 2014, Rump session]

Itai Dinur, Pawel Morawiecki, Josef Pieprzyk, Marian Srebrny, Michal Straus

SHA-3 の縮小版(5/6 段)Keccak のスポンジ関数に対する CUBE 攻撃を発表した。縮退版であるため当面の影響はないが、今後の動向に注意する必要がある。

3. 解読技術等の動向

表 2 に具体的な暗号の攻撃に関する発表のリストをカテゴリー別に示す。★は電子政府推奨暗号の安全性に直接関わる技術動向、☆はその他の注視すべき技術動向である。

表 2 具体的な暗号の攻撃に関する発表

	公開鍵暗号	**頁**
☆	SVP by Enumeration: Bridging the Gap between Theory and Practice [TCC 2014, Rump Session]	5
	Discrete logarithm in GF(2^{809}) with FFS [PKC 2014]	9
☆	Parallel Gauss Sieve Algorithm: Solving the SVP Challenge over a 128-Dimensional Ideal Lattice [PKC 2014]	10
★	A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic [Eurocrypt 2014, BEST PAPER]	10
★	Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus [Eurocrypt 2014]	10
	ブロック暗号	**頁**
	Match Box Meet-in-the-Middle Attack against KATAN [FSE 2014]	5
☆	Improved All-Subkeys Recovery Attacks on FOX, KATAN and SHACAL-2 Block cipher [FSE 2014]	5
★	Improved Single-Key Attacks on 9-Round AES-192/256 [FSE 2014]	6
	Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64 [FSE 2014]	7
	Improved Slender-set Linear Cryptanalysis [FSE 2014]	7
	Cryptanalysis of KLEIN [FSE 2014]	7
☆	Differential Cryptanalysis of round-reduced SIMON and SPECK [FSE 2014]	8
☆	Differential Analysis of Block Ciphers SIMON and SPECK [FSE 2014]	9
	Multiple Differential Cryptanalysis of Round-Reduced PRINCE [FSE 2014]	9
☆	Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities [Eurocrypt 2014]	11
	ストリーム暗号	**頁**

3.1. TCC 2014 の発表

3.1.1. TCC 2014 の発表(ランプセッション)

SVP by Enumeration: Bridging the Gap between Theory and Practice [TCC 2014, Rump Session]

Michael Walter, Daniele Micciancio

量子計算機でも解読できない次世代暗号候補の一つとして格子問題に基づいた暗号が研究されているが、格子の最短ベクトル問題(SVP: Shortest Vector Problem)を数え上げで解くアルゴリズムの改良が発表された。既知のアルゴリズムである Kannan 法と Fincke-Pohst 法とでは、漸近的には Kannan 法が効率的になるが、逆転する格子次元ははっきりとしていない。今回提案の方法では格子次元 30 において逆転することが示されている。次世代暗号研究・調査においてフォローしていく必要がある。

3.2. FSE 2014 の発表

3.2.1. FSE 2014 の発表(1 日目)

Match Box Meet-in-the-Middle Attack against KATAN [FSE 2014]

Thomas Fuhr and Brice Minaud

KATAN は De Canniere らが CHES 2009 で発表した軽量ブロック暗号で、KATAN32, KATAN48, KATAN64 の 3 種類がある。数値はブロック長(単位はビット)を表し、鍵長は 80 ビット、254 段繰り返し構造である。基本的な中間一致攻撃に、biclique 攻撃と match-box 攻撃を適用して攻撃可能段数を伸ばすことにより、K32 の 153 段縮小版、K48 の 129 段縮小版、K64 の 119 段縮小版が理論的に攻撃であることを示した。攻撃では、データ複雑度が 3 種類共通で 2^5 個の選択平文と $2^{78.5}$ の時間複雑度、空間複雑度は各々、2^{76}, 2^{76}, 2^{74} である。

Collision Spectrum, Entropy Loss, T-Sponges, and Cryptanalysis of GLUON-64 [FSE 2014]

Leo Paul Perrin and Dmitry Khovratovich

GLUON は、Africacrypt 2012 で提案された T スポンジ型の軽量ハッシュ関数のファミリであり、GLUON-64 はビットレート r=8、容量 c=128 である。f 関数は置換ではないため、メッセージが長くなるにつれ、エントロピー損失が起こり、衝突の発見が容易となる。本論文では、f 関数の置換からの違いを示す衝突確率スペクトラム(CPS)を導入し、解析した。その結果、最後が 1Mb の 0 で終わるメッセージに対する原像探索に要する計算量が、提案者が示した 2^{128} より小さい $2^{115.3}$ となることを理論的に示した。

Improved All-Subkeys Recovery Attacks on FOX, KATAN and SHACAL-2 Block cipher [FSE 2014]

Takanori Isobe and Kyoji Shibutani

Asiacrypt 2013 で提案された Function Reduction 法を Lai-Massey 型と LFSR 型に適用可能になるよう拡張し、繰り返し型にした ASR(All-Subkeys Recovery)攻撃に適用して必要データ量

を削減す方法を提案し、FOX64/128，KATAN32/48/64，SHACAL-2 に適用した。各暗号に対する攻撃結果を表で示す。

暗号名	鍵長	攻撃段数/仕様	時間複雑度	メモリ複雑度	データ複雑度
FOX64	128	7/64	2^{124}	2^{124}	$2^{30.9}$
FOX128	256	7/64	2^{124}	2^{124}	$2^{30.9}$
KATAN32	32	119/254	$2^{79.1}$	$2^{79.1}$	144
KATAN48	48	105/254	$2^{79.1}$	$2^{79.1}$	144
KATAN64	64	94/254	$2^{79.1}$	$2^{79.1}$	142
SHACAL-2	256	42/64	2^{508}	2^{508}	2^{25}

Improved Single-Key Attacks on 9-Round AES-192/256 [FSE 2014]
Leibo Li, Keting Jia and Xiaoyun Wang

単一鍵モデルにおける AES に対し、鍵依存篩による鍵候補の絞り込みによって、AES-192 の解読可能段数を 9 段に伸ばした。データ計算量は 2^{121} の選択平文、時間計算量が $2^{177.5}$、空間計算量は $2^{186.5}$。

Cryptanalysis of FIDES [FSE 2014]
Itai Dinur and Jeremy Jean

FIDES は鍵なし AES の段関数を利用した認証付き暗号(Authenticated Encryption)である。パラメータ c を持ち、鍵サイズが 80 ビットの FIDES-80 (c=5)と 96 ビットの FIDES-96 (c=6)の 2 種類がある。設計者は 16c ビットの安全性を主張していたが、本論文では、guess-and-determine アルゴリズムによって、17 個の連続する既知平文に対する leaked nibbles と追加値があれば、2^{15c} 回分の計算量で内部状態を復元できることを示した。

3.2.2. FSE 2014 の発表(2 日目)

Impact of ANSI X9.24-1:2009 Key Check Value on ISO/IEC 9797-1:2011 MACs [FSE 2014]
Tetsu Iwata and Lei Wang

Key check value(KCV)は、ANS X9.24-1:2009 の Annex C に記載された、CBC MAC 属の鍵をチェックするための数値である。本論文では、ISO/IEC 9797-1:2001 に掲載されている CBC MAC 属 10 方式のうち 5 方式(MAC2.1, MAC2.2, MAC3, MAC5(CMAC), MAC6.2)の安全性が、KCV によって低下することを示した。KCV を s ビットとすると安全性の低下は s/2 ビット分である。

Plaintext Recovery Attacks Against WPA/TKIP [FSE 2014]
Kenneth G. Paterson, Jacob C. N. Schuldt and Bertram Poettering

WPA/TKIP は無線 LAN の暗号化プロトコルの一つであり、安全性の低下が指摘される RC4 を使用しているが、今なお広く使われている。TKIP(Temporal Key Integrity Protocol)では TKIP sequence Counter (TSC)という 48 ビットのカウンターが利用されており、本論文ではこれに着目し、同じ平文を多数の異なる鍵で通信する設定の攻撃が示された。使用するデータ量を minimum と ideally の 2 種類に分け、実際の攻撃に掛かる計算時間を下表のように評価した。

	鍵ストリーム長 (TSC 組ごと)	TSC 組数	データ量	計算時間 (コア*日数)
minimum	2^{32}	2^{16}	2^{48}	2^{14}
ideal	2^{40}	2^{16}	2^{56}	2^{22}

Dependence in IV-related bytes of RC4 key enhances vulnerabilities in WPA [FSE 2014]
Sourav Sen Gupta, Subhamoy Maitra, Willi Meier, Goutam Paul and Santanu Sarkar

RC4 を使用する WPA に対する既存の攻撃では、鍵ストリーム自体の偏りに注目しているが、本論文では鍵ストリーム間の相関に注目し、観測されている偏りの理論的証明や平文回復攻撃の効率を改善した。

Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64 [FSE 2014]
Itai Dinur, Orr Dunkelman, Nathan Keller and Adi Shamir

ブロック暗号に対する中間一致攻撃において、新規開発の線形鍵篩法と既知平文攻撃に利用可能な splice-and-cut 法を利用する方法提案した。提案法を軽量暗号 LED-64 に適用し、攻撃可能段数は増えないものの攻撃の効率を改良した。攻撃の複雑度は下表の通り。

攻撃タイプ	ステップ数	時間複雑度	データ複雑度	メモリ複雑度
単一鍵	2	2^{48}	2^{16} CP	2^{16}
単一鍵	2	2^{48}	2^{48} KP	2^{48}
関連鍵	3	2^{49}	2^{49} CP	2^{49}

Improved Slender-set Linear Cryptanalysis [FSE 2014]
Guo-Qiang Liu, Chen-Hui Jin and Chuan-Da Qi

ブロック暗号の Maya は PRESENT に類似した構造で、秘密の 4 ビット S-box が利用されている。本論文では、フーリエ変換を利用して S-box を絞り込む方法を利用した攻撃法を提案した。16 段縮小版に対する攻撃では、データ複雑度 2^{36}、時間複雑度 $2^{18.9}$、成功率 87.5%である。

Cryptanalysis of KLEIN [FSE 2014]
Virginie Lallemand and Maria Naya-Plasencia

KLEIN は RFIDSec 2011 で提案された軽量暗号で、KLEIN-64/80/96 の 3 種類がある。従来の攻撃では、高位ニブルと低ニブルの間の拡散が遅いことを利用した。本論文では、ニブル混合(MixNibbles)に注目して鍵候補を絞り込む改良を行った。攻撃は truncated 差分攻撃であるが、差分経路の取り方によってトレードオフがあるので、それらを下表に示す。

暗号名	攻撃段数/仕様	データ複雑度	時間複雑度	メモリ複雑度
KLEIN-64	12/12	$2^{54.5}$	2^{57}	2^{16}
KLEIN-64	12/12	2^{35}	$2^{63.8}$	2^{32}
KLEIN-80	13/16	$2^{60.49}$	$2^{71.1}$	2^{16}
KLEIN-80	13/16	2^{41}	2^{78}	2^{32}
KLEIN-96	14/20	2^{47}	2^{92}	2^{32}
KLEIN-96	14/20	2^{58}	$2^{89.2}$	2^{16}

Branching Heuristics in Differential Collision Search with Applications to SHA-512 [FSE 2014]

Maria Eichlseder, Florian Mendel and Martin Schlaffer

SHA-512 に対する semi-free-start での攻撃可能段数を従来 24 段(仕様では 80 段)から 38 段に拡張した。本論文では、自動化した差分の衝突探索が利用されている。

Collision Attack on 5 Rounds of Grøstl [FSE 2014]
Florian Mendel, Vincent Rijmen and Martin Schlaffer

Grøstl は Knudsen らによって設計された SHA-3 最終 5 候補の一つである。本論で取り上げる Grøstl-256 と Grøstl-512 は各々、10 段と 14 段であり、従来ともに 3 段縮小版までしか攻撃されていなかった。本論文では、差分が複数のメッセージブロックに広がること許容しつつ、計算量削減のため通過する置換は 2 個のうち 1 つに限定した結果、両方とも衝突発見可能段数を 5 段に伸ばした。攻撃は、Grøstl-256 では、時間複雑度が 2^{123}、メモリ複雑度が 2^{64}。Grøstl-512 では、時間複雑度が 2^{176}、メモリ複雑度が 2^{64}。

3.2.3. FSE 2014 の発表(3 日目)

Differential Cryptanalysis of round-reduced SIMON and SPECK [FSE 2014]
Farzaneh Abed, Eik List, Jakob Wenzel and Stefan Lucks

SIMON と SPECK は 2013 年 6 月に NSA が公開した軽量ブロック暗号で、ソフト実装・ハード実装の両方で高い実装性能を示すように設計されている。本論文では、各ブロッ長、鍵長の組み合わせに対し、差分攻撃と長方形(Rectangle)攻撃を適用した結果が発表された。結果を下表に示す。

SIMON に対する差分攻撃

暗号	攻撃段数/仕様	時間複雑度	データ複雑度	メモリ複雑度	成功率
SIMON32/64	18/32	$2^{46.0}$	$2^{31.2}$	$2^{15.0}$	0.63
SIMON48/72	19/36	$2^{52.0}$	$2^{46.0}$	$2^{20.0}$	0.98
SIMON64/96	26/42	$2^{63.9}$	$2^{63.0}$	$2^{31.0}$	0.86
SIMON96/96	35/52	$2^{93.3}$	$2^{93.2}$	$2^{37.8}$	0.63
SIMON128/128	46/68	$2^{125.7}$	$2^{125.6}$	$2^{40.6}$	0.63

SPECK に対する差分攻撃

暗号	攻撃段数/仕様	時間複雑度	データ複雑度	メモリ複雑度	成功率
SPECK32/64	10/22	$2^{29.2}$	2^{29}	2^{16}	0.99
SPECK48/72	12/22	$2^{45.3}$	2^{45}	2^{24}	0.99
SPECK64/96	15/26	$2^{61.1}$	2^{61}	2^{32}	0.99
SPECK96/96	15/28	$2^{89.1}$	2^{89}	2^{48}	0.99
SPECK128/128	16/32	$2^{111.1}$	2^{116}	2^{64}	0.99

SPECK に対する長方形攻撃

暗号	攻撃段数/仕様	時間複雑度	データ複雑度	メモリ複雑度	成功率
SPECK32/64	11/22	$2^{46.7}$	$2^{30.1}$	$2^{37.1}$	～1
SPECK48/72	12/22	$2^{58.8}$	$2^{43.2}$	$2^{45.8}$	～1
SPECK64/96	14/26	$2^{89.4}$	$2^{63.6}$	$2^{65.6}$	～1
SPECK96/144	16/29	$2^{135.9}$	$2^{90.9}$	$2^{94.5}$	～1
SPECK128/192	18/33	$2^{182.7}$	$2^{125.9}$	$2^{121.9}$	～1

Differential Analysis of Block Ciphers SIMON and SPECK [FSE 2014]
Alex Biryukov, Arnab Roy and Vesselin Velichkov

ブロック暗号の差分解読において ARX 型一般に適用可能な差分経路探索法を開発した。この探索法では、探索打ち切りの閾値に新規開発の Highway-Country road approach を利用している。NSA が設計したブロック暗号 SIMON と SPECK に適用したところ、新規の差分経路が発見でき、次に示す各ブロック長、鍵長の組み合わせに対する解読が可能であることを理論的に示した。

暗号	鍵長	攻撃段数/仕様	時間複雑度	データ複雑度
SIMON32	64	19/32	2^{32}	2^{31}
SIMON48	72	20/36	2^{52}	2^{46}
SIMON48	96	20/36	2^{75}	2^{46}
SIMON64	96	26/42	2^{89}	2^{63}
SIMON64	128	26/44	2^{121}	2^{63}
SPECK32	64	11/22	2^{55}	2^{31}
SPECK48	72/96	12/22	2^{43}	2^{43}
SPECK64	96	16/26	2^{63}	2^{63}
SPECK64	128	16/27	2^{63}	2^{63}

Equivalent Key Recovery Attacks against HMAC and NMAC with Whirlpool Reduced to 7 Rounds [FSE 2014]
Jian Guo, Yu Sasaki, Lei Wang, Meiqin Wang and Long Wen

ハッシュ関数に Whirlpool を使用した HMAC に対する鍵回復攻撃において、実際の鍵の代りに HMAC の等価鍵を求めることにより、攻撃可能な縮小版 Whirlpool の段数(仕様では 10 段)を従来の 6 段から 7 段に伸ばした。攻撃は AES ベースのブロック暗号に対して開発された中間攻撃の手法を利用しており、必要な計算コストは、時間複雑度 $2^{482.3}$、メモリ複雑度 2^{481}、データ複雑度 $2^{481.7}$ である。

Multiple Differential Cryptanalysis of Round-Reduced PRINCE [FSE 2014]
Anne Canteaut, Thomas Fuhr, Henri Gilbert, Maria Naya-Plasencia and Jean-Rene Reinhard

PRINCE は Asiacrypt 2012 で Borghoff らが提案したブロック暗号で、ブロック長 64 ビット、鍵長 128 ビット、12 段 SP 構造である。本論文では、複数差分経路の効果を考慮した 6 段 differential を利用して、10 段縮小版に対する攻撃を示した。コストはデータ複雑度 $2^{57.9}$、時間複雑度 $2^{60.7}$、メモリ複雑度 $2^{60.5}$。この結果は 10 段縮小モデルに対する攻撃としては最善のものである。

3.3. PKC 2014 の発表

3.3.1. PKC 2014 の発表(1 日目)

Discrete logarithm in GF(2^{809}) with FFS [PKC 2014]
Razvan Barbulescu, Cyril Bouvier, Jeremie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thome, Marion Videau, Paul Zimmermann

関数体篩法において、GPUを使用した高速化を実現するため、主要部分の高速化と篩計算と線形計算の適切なバランスを取った方法が示された。その結果、有限体 GF(2^{809})上の離散対数問題を 7.6 コア年と 0.1GPU 年で計算できるという理論結果を得た。

3.3.2. PKC 2014 の発表(3 日目)

Parallel Gauss Sieve Algorithm: Solving the SVP Challenge over a 128-Dimensional Ideal Lattice [PKC 2014]

Tsukasa Ishiguro, Shinsaku Kiyomoto, Yutaka Miyake, Tsuyoshi Takagi

最短ベクトル問題(SVP)解決のための並列化したガウス篩アルゴリズムを提案した。提案法の一般的な特徴は、サンプリングした短いベクトルと SIMD 命令の活用である。これに有限体ごとの最適化を行う。
Ideal Lattice Challenge に適用したところ、世界で初めて 128 ビットの解法に成功するなどの成果が得られた。計算には 29,994CPU 時間を要した。

3.4. Eurocrypt 2014 の発表

3.4.1. Eurocrypt 2014 の発表(1 日目)

A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic [Eurocrypt 2014, BEST PAPER]

Razvan Barbulescu, Pierrick Gaudry, Antoine Joux and Emmanuel Thome

離散対数問題(DLP: Discrete Logarithm Problem)に対する新しい解読法を提示した(最優秀論文賞)。計算量評価はヒューリスティックな仮定を用いているが、小標数の場合に計算量は準多項式時間となっており、これまで最速であった関数体篩法の準指数時間を凌いでいる。電子政府推奨暗号では、電子署名アルゴリズム DSA 及び鍵共有アルゴリズム DH が関係するが、使用・推奨しているパラメーターは素体(大標数)であり、その範囲では影響しない。ただし、小標数の DLP の困難性に基づいた暗号技術を使用する場合には、新解読アルゴリズムの影響を評価する必要がある。

Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus [Eurocrypt 2014]

Jean-Charles Faugere, Louise Huot, Antoine Joux, Guenael Renault, Vanessa Vitse

楕円曲線上の離散対数問題(ECDLP: Elliptic Curve Discrete Logarithm Problem)に対する解読法の改良を提示した。電子政府推奨暗号では、鍵共有アルゴリズム ECDH が関係する。捩(ねじ)れ点写像の性質を用いる改良であり、例えば IPSEC(SECurity architecture for Internet Protocol)の鍵共有プロトコルに使われている曲線に適用可能であり、解読時間の短縮を図る

ことができる。まだ現実的な脅威にはなっていないが、影響範囲や効果を評価しておく必要がある。

Generic Universal Forgery Attack on Iterative Hash-based MACs [Eurocrypt 2014]
Thomas Peyrin and Lei Wang

ハッシュベースのメッセージ認証コードに対する偽造攻撃の改良が提示された。電子政府推奨暗号では、メッセージ認証コード HMAC が関係する。例えば、任意のメッセージに対する偽造は、RIPEMD-160 を用いた HMAC では、これまで 2 の 160 乗の計算量が必要と考えられていたが、2 の 133.3 乗に改良できるという結果である。現実的脅威とはなっていないが、影響評価を行い、今後の進展に注意する必要がある。

Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities [Eurocrypt 2014]
Celine Blondeau and Kaisa Nyberg

ブロック暗号に対する様々な攻撃間の関係(同値性、時間メモリトレードオフによる変換等)をより明らかにする発表を行った。応用例として、26 段 PRESENT に対する既知の多次元線型識別(Multi-dimensional Linear Distinguisher)攻撃が、既知の既知平文(Known Plaintext)攻撃より少ないメモリにより選択平文(Chosen Plaintext)鍵回復攻撃に変換できることを示した。関係性の提示のため、電子政府推奨暗号に対する当面の影響はないと考えられるが、現実の攻撃条件等を考慮する際には注意しなければならない。

3.4.2. Eurocrypt 2014 の発表(Rump session)

Practical Complexity Cube Attacks on Round-Reduced Keccak Sponge Function [Eurocrypt 2014, Rump session]
Itai Dinur, Pawel Morawiecki, Josef Pieprzyk, Marian Srebrny, Michal Straus

SHA-3 の縮小版(5/6 段)Keccak のスポンジ関数に対する CUBE 攻撃を発表した。縮退版であるため当面の影響はないが、今後の動向に注意する必要がある。

資料４

暗号技術活用委員会の活動状況

1. 2014 年度の活動計画（2013 年度第 2 回暗号技術検討会了承）

今後、暗号に関する様々な課題解決に向けた政策立案等を行う際に役立てるために、2014 年度は、2013 年度の活動内容を継続して実施し、各検討項目における最終報告書を取りまとめる。

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

本委員会では、2013 年度と 2014 年度の 2 年間をかけて、「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を行い、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活動をしている。

2014 年度は、2013 年度に引き続いて、議論を行ううえで有用な基礎データの収集を上期も継続して実施する。下期には、2013 年度及び 2014 年度上期に収集したデータをもとに、暗号の普及促進・セキュリティ産業の競争力強化に向けた具体的な課題分析や解決策の検討を実施し、報告書に取りまとめる。

② 暗号政策の中長期的視点からの取組の検討

上記の「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」のなかで、様々なシステムを安全に動かしていくための暗号に関連する人材育成についても一緒に検討していくことにより、CRYPTREC として取り組むべき課題を明らかにし、報告書に取りまとめる。

③ 標準化推進

2013 年度の成果を踏まえ、今後、様々な組織が日本からの暗号アルゴリズムの提案を行う場合に、その成果が効果的に得られるようにするための、有望な標準化提案先の選定、当面必要とされる稼働見積もりや交渉方法、提案活動における課題等を、標準化推進 WG にて引き続き検討し、報告書に取りまとめる。

④ 運用ガイドライン作成・公開

2013 年度にドラフト版を完成させた「SSL/TLS サーバ構築ガイドライン」について、引き続き運用ガイドライン WG にて作業を行い、成果物を暗号技術検討会に報告する。

2. 暗号技術活用委員会　中間活動報告

2.1 委員構成

暗号技術活用委員会の委員は以下の通り。

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	遠藤　直樹	東芝ソリューション株式会社　技術統括部 技監
委員	川村　亨	日本電信電話株式会社　研究企画部門 プロデュース担当（セキュリティ） 担当部長／チーフプロデューサ
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	鈴木　雅貴	日本銀行　金融研究所　情報技術研究センター 主査
委員	高木　繁	株式会社三菱東京 UFJ 銀行　システム部システム企画室 次長
委員	角尾　幸保	日本電気株式会社　パブリックビジネスユニット 宇宙・防衛事業推進本部 主席技術主幹
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
退任	**前田　司**	**EMC ジャパン株式会社　RSA 事業本部　技術統括部 部長**
新任	**八束　啓文**	**EMC ジャパン株式会社　RSA 事業本部　技術統括部 システムズ・エンジニアリング部　部長**
委員	松井　充	三菱電機株式会社　情報技術総合研究所 技師長
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　ソーシャル ICT 研究センター 特任准教授
委員	山田　勉	株式会社日立製作所　日立研究所 エネルギーマネジメント研究部　ES3 ユニット ユニットリーダ主任研究員
委員	山本　隆一	東京大学　大学院医学系研究科　医療経営政策学講座 特任准教授

2.2 開催計画

委員会の開催日程・議題については、以下のとおり計画している。

回	開催日	議案
―	メール審議	● WG 活動計画案の審議・承認
第 1 回	2014 年 10 月 30 日	● 活用委員会活動計画の確認 ● 「暗号利用環境に関する動向調査」紹介 ➢ 各国政府の政策動向調査 ➢ セキュリティ認証制度の動向調査 ➢ 暗号製品市場の動向調査 ● ヒアリング調査の報告 ● 最終報告書とりまとめに向けた論点整理 ● 各ワーキンググループからの報告・審議
第 2 回	2014 年 12 月下旬 ～ 2015 年 1 月上旬	● SSL/TLS サーバ構築ガイドラインの審議 ● 最終報告書内容についての中間審議 ● 標準化推進 WG からの報告・審議
第 3 回	2015 年 3 月上旬	● 課題解決に向けた分析結果・対策を取りまとめた最終報告書の審議 ● 各ワーキンググループからの活動報告・審議

3. 標準化推進 WG 中間活動報告

3.1 委員構成

標準化推進 WG の委員は以下の通り。

	委員氏名	所属	担当領域
主査	渡辺　創	独立行政法人産業技術総合研究所	ISO/IEC JTC1/SC27
委員	江原　正規	東京工科大学	ISO/IEC JTC1/SC31
委員	河野　誠一	レノボ・ジャパン株式会社	TCG
委員	木村　泰司	一般社団法人日本ネットワークインフォメーションセンター	IETF
委員	坂根　昌一	シスコシステムズ合同会社	M2M/IoT
委員	佐藤　雅史	セコム株式会社	長期署名（ETSI）
委員	武部　達明	横河電機株式会社	制御機器・制御システム
委員	廣川　勝久	ISO/IEC JTC1/SC17 国内委員会	ISO/IEC JTC1/SC17
委員	真島　恵吾	日本放送協会	放送
委員	真野　浩	コーデンテクノインフォ株式会社	IEEE802.11
委員	茗原　秀幸	三菱電機株式会社	医療

3.2 開催計画

WG の開催日程・議題については、以下のとおり計画している。

回	開催日	議案
第 1 回	2014 年 10 月 15 日	● WG 活動計画報告 ● 各標準化活動状況のアップデート ● 暗号アルゴリズム標準化規格と各種標準化規格との関係俯瞰図のとりまとめ方法 ● 標準化提案における交渉ノウハウ・課題の整理
第 2 回	2014 年 12 月上～中旬	● 暗号アルゴリズム標準化規格と各種標準化規格との関係俯瞰図のとりまとめ ● 標準化提案における交渉ノウハウ・課題のとりまとめ ● 暗号アルゴリズム提案に有望な標準化提案先について ● 暗号アルゴリズム提案に必要な稼働見積り
第 3 回	2015 年 2 月	● 報告書のとりまとめ

4. 運用ガイドライン WG　中間活動報告

4.1 委員構成

運用ガイドライン WG の委員は以下の通り。

主査	菊池 浩明	明治大学
委員	阿部 貴	株式会社シマンテック
委員	漆嶌 賢二	富士ゼロックス株式会社
委員	及川 卓也	グーグル株式会社
委員	加藤 誠	一般社団法人 Mozilla Japan
委員	佐藤 直之	株式会社イノベーションプラス
委員	島岡 政基	セコム株式会社IS研究所
委員	須賀 祐治	株式会社インターネットイニシアティブ
委員	高木 浩光	独立行政法人産業技術総合研究所
委員	村木 由梨香	日本マイクロソフト株式会社
委員	山口 利恵	東京大学

3.2　開催計画

WG の開催日程・議題については、以下のとおり計画している。

回	開催日	議案
―	メール作業（～9 月末）	● ドラフト版及びチェックリスト案を取りまとめ
第 1 回	2014 年 10 月 17 日	● WG 活動計画報告 ● ドラフト版及びチェックリスト案についての審議
―	外部レビュー（11 月）	● 携帯キャリア・SSL-VPN ベンダを想定
第 2 回	2014 年 12 月中旬	● 外部レビューのコメント等の反映・審議
第 3 回	2015 年 2 月中～下旬	● ガイドライン及びチェックリストの最終確定

以上

参考資料１

２０１３年度　第２回暗号技術検討会　議事概要

１．日時　平成２６年３月２７日（木）　１４：００～１５：３５

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）、上原哲太郎、太田和夫、岡本栄司、岡本龍明、国分明男、佐々木良一、武市博明、中山靖司、本間尚文、高島克幸（松井充構成員代理）、松尾真一郎、松本勉、松本泰、向山友也、渡辺創

オブザーバ：奥山剛、根本農史（佐藤正明 代理）、堤紀代子（稲垣浩 代理）、江森久子（野口宣大 代理）、楢木野由善（大村周一郎 代理）、郷敦、岩下守男（三富則江 代理）、岩永敏明（辻本崇紀 代理）、木村和仙、平和昌、寶木和夫、伊藤毅志、山岸篤弘（亀田繁 代理）、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　吉田靖、赤阪晋介、飯田恭弘、河合直樹、中村一成

経済産業省　大橋秀行、上村昌博、中谷順一、室井佳子

４．配布資料

（資料番号）

資料１	2013 年度　暗号技術評価委員会活動報告
資料２	2013 年度　暗号技術活用委員会活動報告
資料３	2013 年度　暗号技術検討会報告書（案）
資料４	2014 年度　暗号技術検討会活動計画（案）
資料５	2014 年度　暗号技術評価委員会活動計画（案）
資料６	2014 年度　暗号技術活用委員会活動計画（案）
参考資料１	2013 年度　第１回暗号技術検討会議事概要
参考資料２	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）
参考資料３	CRYPTREC 暗号技術ガイドライン（SHA-1）
参考資料４	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５	2013 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

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５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）羽室氏→佐藤氏、(法務省）佐藤氏→野口氏、(外務省）中村氏→大村氏）及び構成員の欠席等（松井充構成員の代理として高島克幸氏が出席、金子敏信構成員、近澤武構成員は欠席）について説明が行われた。

２　議事

（１）2013 年度 暗号技術評価委員会活動報告

資料１に基づき、2013 年度暗号技術評価委員会の活動報告について、暗号技術評価委員会事務局から説明が行われた。質疑応答は以下のとおり。

〇質疑応答

佐々木構成員：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）はいつ公開されるのか。本ガイドラインを通じて RC4 の脆弱性について周知することは重要である。ブロック暗号の CBC モードに脆弱性があるために RC4 の使用を推奨している場合があるようで、相談を受けたことがある。その時は RC4 の使用はやめた方がよいのではないかと助言したが、このように暗号の専門家でも RC4 を使用しようとすることがあるため、必ずしも正しい理解が広まっていないのではないと危惧している。

暗号技術評価委員会事務局：今回作成したガイドラインは、TLS1.0、1.1、1.2 でそれぞれどのパッチが当たっているのか、どのバージョンなら RC4 の使用が許容されるのか、TLS1.2 なら GCM のような認証暗号が利用できるオプションがきちんとついている、といったことをバージョン別に記載しており、有用なもの。可能な限り早い時期の公開を予定している。

今井座長:乱数については､CRYPTREC暗号リストの技術項目には含まれていないものの、使い方を間違えると大変なことになる。どのような事例があるか簡単に説明してほしい。

暗号技術評価委員会事務局：乱数については、楕円曲線に関連してクローズアップされていたが、それ以外にも、乱数の生成方法について生成が上手くいかなかった時にどのようなことが起こるかという話題で出てきている。暗号技術ガイドラインの来年度の重要なテーマとして検討していきたい。

今井座長：軽量暗号はいろいろと検討していただいているが、デバイスの進歩を十分考慮に入れなければならない。

本間構成員：ご指摘のとおり。小型デバイスに通信機能を持たせる場合、最先端のプロセスを使うことはできず、いわゆる枯れたプロセスを使うことになる。そこに軽量暗号を使う場合、実装面積が非常に小さくて済むため、大きなアドバンテージがあると認識している。

（２）2013 年度 暗号技術活用委員会

資料２に基づき、2013 年度暗号技術活用委員会の活動報告について、暗号技術活用委員会事務局から説明が行われた。質疑応答は以下のとおり。

〇質疑応答

今井座長：作成中の運用ガイドラインについて、暗号技術評価委員会の結論と相違があるとのことだが、具体的にどういうことか。

暗号技術活用委員会事務局：暗号技術評価委員会というよりは、CRYPTREC 暗号リストとの相違である。現在の CRYPTREC 暗号リストはアルゴリズム名で記載されており、鍵長での判断がない。しかし本ガイドラインでは鍵長を考慮して判断した。具体的には、RSA は 2048 ビットがスタンダードであり、また鍵長を電子証明書でコントロールできる一方で、DH は鍵長をサーバ側がコントロールできず、知らないうちに 1024 ビットの鍵を使用して通信を行う可能性を排除できないため、電子政府推奨暗号である DH よりも運用監視暗号である RSA の優先順位を高くしている。そこが CRYPTREC 暗号リストとの相違である。

松本（勉）構成員：暗号は解読に強くなければならないが、強いだけでもだめで、実際に使えなければ意味がない。今回、暗号技術活用委員会の運用ガイドライン WG で精力的に検討いただき、いろいろと考えなければならない事が明らかになってきた。電子政府推奨暗号リストの活用方法を考えるに当たって、従来より実用面を考慮してきたが、最近はさらに細かい所まで詳細に議論できる環境が整ってきた。これを踏まえて、今後 CRYPTREC の活動をどのように進めていくかということを検討していかなければならない。

今井座長：Forward Secrecy については、十分に意識されていないため、こういったものがあり非常に重要であることが分かるように広報していただきたい。

暗号技術活用委員会事務局：本ガイドライン中に、Forward Secrecy が備わっている方がよいということは記載する。

松本（勉）委員：言葉の問題だが、「特高」セキュリティという名称はいかがなものか。

暗号技術活用委員会事務局：名称は仮称であるため、何か良い名称があればご教示いただきたい。

寶木オブザーバ：NIST が楕円曲線や RSA の鍵長の安全性について調べており、使用の是非についてアナウンスを行っている。そちらとのバランスはどうか。

暗号技術活用委員会事務局：基本的に合わせようと思っている。NIST の場合は政府機関向けとして 1024 ビットを使用不可としてしまうということが簡単だと思う。しかし、本ガイドラインでは、特高セキュリティ型について鍵長を 2048 ビットのみ使用可能と記載してもよいと思うが、ベースラインセキュリティ型について 2048 ビットとしてしまうと、携帯電話からアクセスできない可能性があり、相互接続性を維持する観点から確認が必要と考えている。よって、冒頭説明したバッドプラクティスを書くか

どうかの議論と併せて検討中である。具体的には、ベースラインセキュリティ型としては 2048 ビットとするが、バッドプラクティスとしての 1024 ビットへの言及は行わない等が考えられる。

寳木オブザーバ：概ね NIST の考え方と合致していると認識した。ただ、ビジネスの分野で支障が生じないか懸念している。

暗号技術活用委員会事務局：SSL-VPN のベンダや携帯電話のキャリアに、ドラフトの段階で一度このガイドラインを確認していただく予定である。

今井座長：モバイル決済の観点からはどうか。

中山構成員：モバイル決済は「使える」ということが一番重要。実装を考慮した上でどの暗号を採用するのかということだと思う。

（３）2013 年度 暗号技術検討会報告書（案）

資料３に基づき、2013 年度暗号技術検討会報告書（案）について、暗号技術検討会事務局から説明が行われた。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。

（４）2014 年度 暗号技術検討会活動計画（案）

資料４に基づき、2014 年度暗号技術検討会活動計画について、暗号技術検討会事務局から説明が行われた。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

佐々木構成員：基本的にはこの計画で良いと思うが、サイドチャネル攻撃に関する検討は委員会で行っているのか。

暗号技術評価委員会事務局：サイドチャネル攻撃に関する検討は現在暗号技術評価委委員会の活動に含まれており、監視活動として学会発表の内容等を検討している。本活動は CRYPTREC レポートにも掲載予定である。

佐々木構成員：最近、サイドチャネル攻撃に関して問題になっていることはないのか。

本間構成員：攻撃は進化しているが、緊急に対策が必要なものはない。

今井座長：来年度の暗号技術検討会の開催回数は 2 回を予定しているとのことだが、１回目の開催が 10 月と遅くなるのは何か理由があるのか。

暗号技術検討会事務局：2013 年度については、2012 年度の最後の暗号技術検討会で 2013 年度の活動計画を審議いただくことができなかったため、年度の早い時期に 1 回目の会合を開催する必要があった。2014 年度については、今回の暗号技術検討会で活動計画の承認をいただきたいと考えており、この場合 2014 年度の早い時期に会合を開催する必要はなくなるため、年度中間の 10 月頃の開催を予定している。ただし、緊急で開催する必要が生じた場合は、柔軟に対応したいと考えている。

（５）2014 年度 暗号技術評価委員会活動計画（案）

資料５に基づき、2014 年度暗号技術評価委員会活動計画（案）について、暗号技術評価委員会事務局から説明が行われた。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：乱数の取扱に関しては、活動計画の「（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）」に含まれているのか。

暗号技術評価委員会事務局：そのとおり。

今井座長：SHA-3 については安全性評価を行うということか。

暗号技術評価委員会事務局：安全性評価を実施し、その上でまずは推奨候補暗号リストへの追加を検討したいと考えている。

（６）2014 年度 暗号技術活用委員会活動計画（案）

資料６に基づき、2014 年度暗号技術活用委員会活動計画（案）について、暗号技術活用委員会事務局から説明が行われた。質疑応答は以下のとおり。一部修正を行うこととして承認された。

〇質疑応答

上原構成員：SSL/TLS サーバ構築ガイドラインは、非常に有用で影響が大きいと考えている。というのも、現在、共通番号法に関係して政府のシステムの大規模な改修が行われている。そのような時期にこのガイドラインができるということは非常によいことだと思っている。ただ、例えば認証プロトコルのように、運用方法についてガイドラインが必要なものがあるのではないかと考えている。来年度の後半には、次にどのようなガイドラインが必要か検討してほしい。

松尾構成員：暗号プロトコルの評価については既に NICT で実施しているが、運用や製品の部分に関して CRYPTREC のガイドラインで補完していただくという方法も考えられる。適宜情報共有しながら、連携して進めていきたい。

今井座長：暗号プロトコルの評価については、現在、暗号プロトコル評価技術コンソーシアム（CELLOS）という組織が立ち上がっているため、そちらとの連携も今後検討していただければと思う。暗号技術活用委員会の活動計画については、SSL/TLS サーバ構築ガイドライン完成後に、次にどのようなガイドラインが必要かを検討することを盛り込むよう修正していただきたい。修正内容については、座長一任とさせていただく。

３　閉会

総務省の吉田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、2014 年度第 1 回目の暗号技術検討会は 10 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

2014 年度 暗号技術評価委員会活動計画

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。

- 引き続き、仕様書の参照先の変更(ECDSA, ECDH)について検討を行う。

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。

- 現時点ではハッシュ関数 SHA-3 の検討している。NIST の FIPS Draft が公表されてから安全性評価について検討する。

⑤ 既存の技術分類の修正を伴わない新技術分類の追加

暗号技術調査ワーキンググループにて調査を行い、暗号技術評価委員会は、その調査結果に基づき追加方針等について検討を行う。

(2) 新世代暗号に係る調査

- 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し、下記の内容について検討を行う
- 暗号技術調査ワーキンググループ(暗号解析評価)

  引き続き、

  (i) Shortest Vector Problem (SVP)

  (ii) Learning with Errors (LWE)

  (iii) Learning Parity with Noise (LPN)

  (iv) Approximate Common Divisor (ACD)

  などの数学的問題を利用した公開鍵暗号技術とパラメータ選択に関する検討を行う。
- 暗号技術調査ワーキンググループ(軽量暗号)

  (a) 軽量暗号に関する検討
  - 軽量暗号が既存暗号に対してアドバンテージをもつエリア
  - 軽量暗号で達成すべき安全性

  (b) 軽量暗号技術に関する現状調査 (サーベイ)
  - 認証暗号：CAESAR プロジェクト提案アルゴリズム等から軽量性に優れた方式を調査
  - ハッシュ関数: SHA-3 の調査

  (c) 今後の活動方針に関する検討
  - 暗号技術ガイドライン (軽量暗号の最新動向) の発行、暗号技術ガイドライン (軽量暗号の詳細評価) の発行、軽量暗号に関する技術公募の実施のいずれがよいか検討を行い、暗号技術評価委員会に提言を行う。

(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)

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う。

- 具体的な内容については、2014 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

2014 年度 暗号技術活用委員会活動計画

今後、暗号に関する様々な課題解決に向けた政策立案等を行う際に役立てるために、2014 年度は、2013 年度の活動内容を継続して実施し、各検討項目における最終報告書を取りまとめる。

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

本委員会では、2013 年度と 2014 年度の 2 年間をかけて、「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を行い、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活動をしている。

2014 年度は、2013 年度に引き続いて、議論を行ううえで有用な基礎データの収集を上期も継続して実施する。下期には、2013 年度及び 2014 年度上期に収集したデータをもとに、暗号の普及促進・セキュリティ産業の競争力強化に向けた具体的な課題分析や解決策の検討を実施し、報告書に取りまとめる。

2. 暗号政策の中長期的視点からの取組の検討

上記の「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」のなかで、様々なシステムを安全に動かしていくための暗号に関連する人材育成についても一緒に検討していくことにより、CRYPTREC として取り組むべき課題を明らかにし、報告書に取りまとめる。

3. 標準化推進

2013 年度の成果を踏まえ、今後、様々な組織が日本からの暗号アルゴリズムの提案を行う場合に、その成果が効果的に得られるようにするための、有望な標準化提案先の選定、当面必要とされる可動見積もりや交渉方法、提案活動における課題等を、標準化推進 WG にて引き続き検討し、報告書に取りまとめる。

4. 運用ガイドライン作成・公開

2013 年度にドラフト版を完成させた「SSL/TLS サーバ構築ガイドライン」について、引き続き運用ガイドライン WG にて作業を行い、成果物を暗号技術検討会に報告する。

【参考】2014 年度スケジュール（案）

年 3 回の委員会開催を予定する。

以上

参考資料4

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。

参考資料５

2014 年度　暗号技術検討会　構成員・オブザーバ名簿

2014.10.9 現在

（構成員）

今井　秀樹	東京大学　名誉教授
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
太田　和夫	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	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
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　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 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内閣企画官
佐藤　正明	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
野口　宣大	法務省民事局商事課長
大村　周一郎	外務省大臣官房情報通信課長
武田　一彦	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
鯨井　佳則	厚生労働省政策統括官付情報政策担当参事官
和泉　　章	経済産業省産業技術環境局基準認証ユニット国際電気標準課長
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）