2016 年度　暗号技術検討会

日時：平成 29 年 3 月 30 日(木)15:00～17:00
場所：経済産業省別館 1 階 114 各省共用会議室

議　事　次　第

１．開　会

２．議　事
(1) CRYPTREC の今後の体制（案）について【審議】
(2) 文書番号体系について【審議】
(3) 2016 年度　暗号技術評価委員会活動報告について【承認】
(4) 2016 年度　暗号技術活用委員会活動報告について【承認】
(5) SHAKE128 の推奨候補暗号リストへの追加について【審議】
(6) ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に入れた評価について【審議】
(7) KCipher-2 の仕様書について【審議】
(8) SHA-1 に関する速報掲載について【報告】
(9) 共通鍵暗号の安全性調査と MISTY1 について【審議】
(10) 2016 年度　暗号技術検討会報告書（案）について【承認】
(11) その他

３．閉　会

（資料番号）	（資　料　名）
資料１	CRYPTREC の今後の体制（案）について
資料２	文書番号体系について
資料３	2016 年度　暗号技術評価委員会活動報告
資料３別添１	2016 年度　暗号技術調査 WG（暗号解析評価）活動報告
資料３別添２	2016 年度　暗号技術調査 WG（軽量暗号）活動報告
資料４	2016 年度　暗号技術活用委員会活動報告
資料５	SHAKE128 の推奨候補暗号リストへの追加について
資料６	ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に入れた評価について
資料６参考資料１	ChaCha20-Poly1305 の安全性評価について
資料７	KCipher-2 の仕様書について
資料７参考資料１	KCipher-2 の仕様書の変更について
資料７参考資料２	KCipher-2 の暗号技術仕様書（日本語版・英語版）の誤記について
資料８	SHA-1 に関する速報掲載について（報告）
資料９	共通鍵暗号の安全性調査と MISTY1 について
資料１０	2016 年度　暗号技術検討会報告書（案）
参考資料１	2016 年度　暗号技術検討会　構成員・オブザーバ名簿

資料 1

CRYPTREC の今後の体制（案）について

［背景］

CRYPTREC には、これまで取り組んできた暗号アルゴリズムのセキュリティ（安全性）確保を引き続き推進することに加えて、暗号アルゴリズムを利用したプロトコルのセキュリティ（安全性）確保のための活動拡大や、情報システム全体のセキュリティ確保に向けた暗号技術の利活用のための情報提供といった貢献が求められている。

2015 年度の CRYPTREC においては、暗号技術に対する社会ニーズの変化や、社会情勢の変化を踏まえ、柔軟な活動を図るため、CRYPTREC で対象とする暗号技術の見直しや、活動範囲、また安全性確保等に係る活動の在り方の見直しを議論するため、暗号技術検討会の下に「CRYPTREC の在り方に関する検討グループ」（H27.6～H27.8）を設置、議論するとともに、当該検討グループでの議論を継続的に行うため、「CRYPTREC 重点課題検討タスクフォース」（H27.11～）を暗号技術検討会の直下に設置し、議論を行った。

2015 年度、重点課題検討タスクフォースにおいて主に(1) CRYPTREC 暗号技術活用委員会の今後の活動に向けて、(2) 暗号アルゴリズムの脆弱性に関する情報発信フローについて、(3) 暗号プロトコルのセキュリティ確保に向けた活動について議論した。

2015 年度 第 3 回重点課題検討タスクフォースにおいて、2016 年度の主な課題として以下が挙げられた。

① 文書体系の在り方について
② 政府統一基準に向けた新たな CRYPTREC 成果物
③ 新たな社会ニーズを見据えた新規活動
④ 情報システム全体のセキュリティ確保を意識した他団体との連携
⑤ その他

［今後］

①については CRYPTREC 成果物の区分の仕方・構成、読者、CRYPTREC が扱うべき範囲等をタスクフォース（H28.2.22 開催）での議論を踏まえ、暗号技術検討会に審議を頂く。

②、③については、政府統一基準等から参照されやすい文書の作成やプライバシー保護のような社会ニーズを見据えた検討等の新たな取り組みについて、今後どのように議論を進めていくかを NISC との相談を含め、事務局 4 者で整理する。その後、整理した内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号技術活用委員会に議論の場を移して検討を行う。

④については、今後他団体との連携を必要とする対象のタスクが明確になった段階で、タスクの内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号技術活用委員会に議論の場を移し、具体的な連携方法について検討を行う。⑤については CRYPTREC としてどう取り組むか議論が必要なテーマに関する検討であるが、昨年度、例として挙がった ChaCha20 の安全性評価の必要性については、今年度、暗号技術評価委員会にて議論され、安全性評価が実施されている。

以上をもって、重点課題検討タスクフォースのミッションを終了とする。（今後、暗号技術検討会やその下の両委員会にまたがる検討事項が出てきた場合には、適宜 4 者事務局打合せで調整のうえ、必要に応じて暗号技術検討会やその下の両委員会に付議する。）

なお、暗号技術検討会は、現状の活動状況を踏まえて、フェーストゥフェースでの開催は年 1 回を基本とするが、メールベースの審議や報告などをタイムリーに行う体制を整えるなどの施策を通じて、検討会としてのアクティビティが低下しないように、活動の効率化を図る。
※リスト改定等の大きな動きがある時は適宜開催するものとし、年次活動計画のなかで開催回数を明示

［審議事項］

1. 重点課題検討タスクフォースの廃止

   重点課題検討タスクフォースのミッション終了に伴い、同タスクフォースを廃止することとしたい。

2. 今後の暗号技術検討会の審議や報告の進め方

   今後の暗号技術検討会の審議や報告の進め方について、事務局から以下を提案する。

   暗号技術検討会活動の効率化の観点から、従来、年度初回の暗号技術検討会で行われてきた年度計画等の審議をメールベースで行うこととし、年度末に開催される暗号技術検討会においては、従来どおりご参集いただくこととしたい。

以上

資料2

文書番号体系について

文書番号体系の確立について(1/2)

以下の文書類を「CRYPTREC文書」といい、文書番号から内容(およびその文書の位置づけ)がわかるように文書管理を行うこととする。

- 総務省・経済産業省によって承認された文書
- 暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会によって承認された文書
- 暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会、及びWGでの配布資料
- CRYPTRECが依頼した外部評価レポート

【想定される対象】

- CRYPTREC暗号リスト
- CRYPTREC暗号リストと各暗号アルゴリズム仕様書との対応表
- CRYPTRECが報告書またはガイドラインとして公開するもの
- CRYPTRECが公表する注意喚起レポート
- 外部評価レポート(外部評価者が作成した技術報告書)
- 委員会資料(議事録を含む)

文書番号体系の確立について(2/2)

体系ルール:

＜文書番号＞ ::= CRYPTREC ＜カテゴリ＞-＜連番(4桁)＞-＜管理情報＞

文書ごとに固定

表記例

アップデートあり:(前バージョンはアーカイブ)

- CRYPTREC LS-0001-2016 ⇔ 2016年度発行CRYPTREC暗号リスト(最新)
  - CRYPTREC LS-0001-2012 ⇔ 2012年度発行CRYPTREC暗号リスト(アーカイブ)
  - CRYPTREC LS-0001-2002 ⇔ 2002年度発行電子政府推奨暗号リスト(アーカイブ)
- CRYPTREC GL-0101-1.1 ⇔ SSL/TLS暗号設定ガイドライン ver 1.1(最新)
  - CRYPTREC GL-0101-1.0 ⇔ SSL/TLS暗号設定ガイドライン ver 1.0(アーカイブ)

アップデートなし:(アーカイブなし)

- CRYPTREC RP-0001-2015 ⇔ 2015年度暗号技術検討会報告書
- CRYPTREC RP-0002-2015 ⇔ 2015年度暗号技術評価委員会報告書
- CRYPTREC EX-0001-xxxx ⇔「Integral攻撃の最新動向とMISTY1等への適用」

【参考】

- FIPS xxx - yyy ⇒ 米国連邦強制規格
- NIST SP800 - xxx rev. ⇒ NISTが自ら作ったガイドライン
- NIST SP1800 - xxx ⇒ NCCoEプロジェクトで作ったガイドライン
- NISTIR xxx ⇒ NIST内部用のレポート

カテゴリ表記

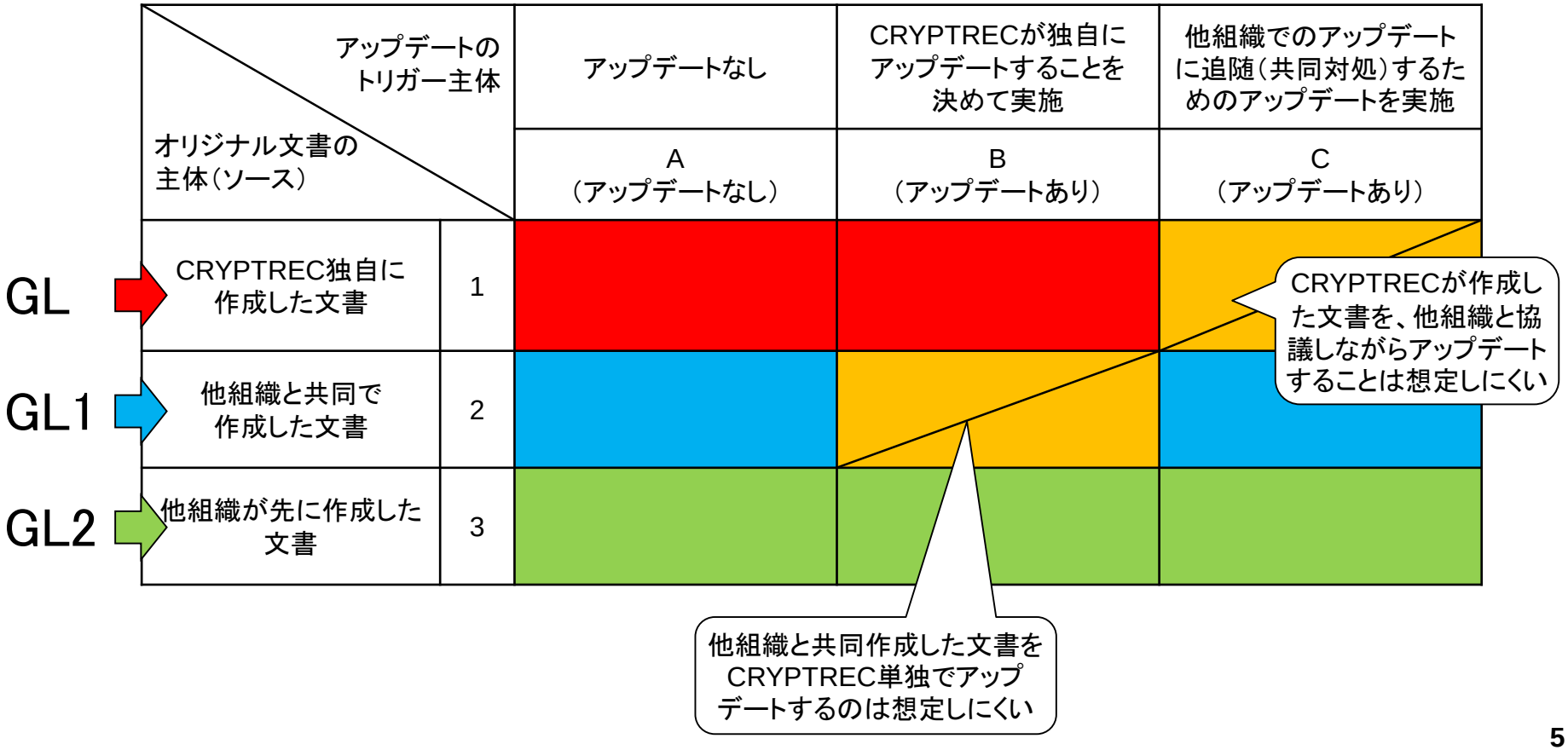
CRYPTREC文書分類	該当する既存のCRYPTREC文書例	表記名
CRYPTREC暗号リスト関係	• CRYPTREC暗号リスト • CRYPTREC暗号リストと仕様書の対応関係表	LS
年次報告書	• 年次報告書	RP
早期に公開する注意喚起	• 注意喚起レポート	ER
ガイドライン	• 暗号技術ガイドライン • 暗号運用ガイドライン	GL
技術報告書	• 調査WG報告書 • 推奨セキュリティパラメータ設定	TR
外部評価報告書	• 外部評価者が作成した安全性評価報告書 • 外部評価者が作成した実装性能評価報告書	EX
会議資料	• 暗号技術検討会資料 • 各委員会資料	MT

カテゴリ内の識別子表記

CRYPTREC文書の「オリジナル文書の主体（ソース）」や「アップデートのトリガー主体」の違いが分かるように、カテゴリ内に識別子を付記することがある

- 「ガイドライン」が主な対象になると想定

  ＜例＞　GL　⇒　GL, GL1, GL2 と表記



CRYPTREC文書の作業主体区分の考え方

【オリジナル文書の主体（ソース）】

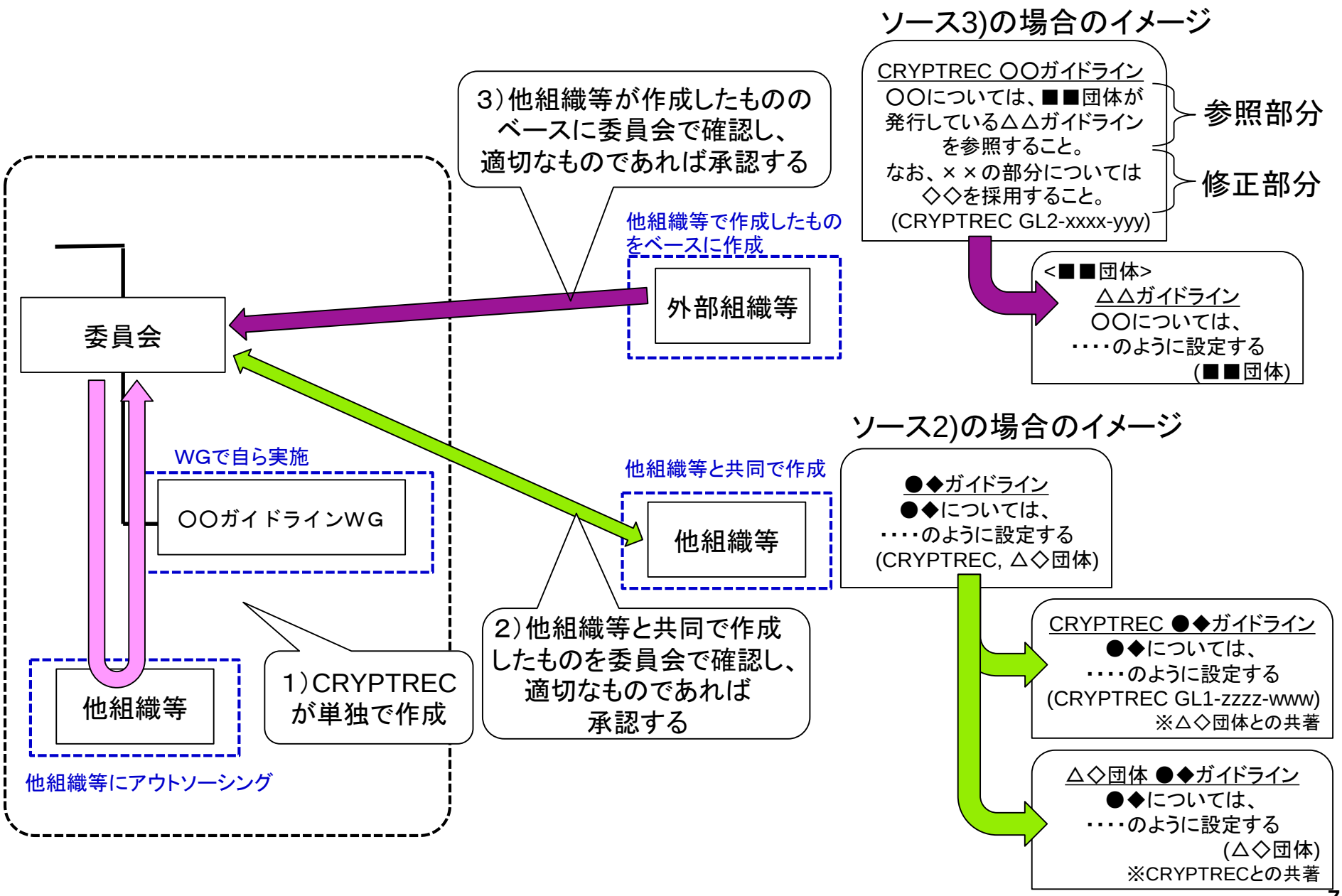
#	ソース	概要	過去の文書例
1	CRYPTREC独自に作成した文書	• CRYPTRECが独自に作成した文書 ※WGまたはアウトソーシングで実施	全文書
2	他組織と共同で作成した文書	• 他組織と共同で作成する文書 ※両組織で発行されることを想定 ※主体は他組織。CRYPTRECはサポート	なし
3	他組織が先に作成した文書	•他組織が作成した文書をベースに、（できるかぎり少ない変更で）CRYPTRECとしての文書を作成 ※最小限の場合、「外部文書の参照関係を示す」だけの文書となることもありうる	なし

【アップデートのトリガー主体】

※「アップデート」とは、文書内容の質自体に関わる記述をいずれ改訂することを**当初から意図**しており、かつそれを**実行**することを意味する。アップデート後、前バージョンの文書は廃止（アーカイブ）される。「記述内容の正誤修正」、「作成時点で改訂を意図していない文書」は「アップデート」には含まない。

#			過去の文書例
A	アップデートなし	• 発行後は原則アップデートしない	年次報告書
B	CRYPTRECが独自にアップデートすることを決めて実施	• CRYPTRECでアップデートを実施 ※WGまたはアウトソーシングで実施	CRYPTREC暗号リスト 解析計算量評価
C	他組織でのアップデートに追随（共同対処）するためにCRYPTRECとしてもアップデートを実施	他組織と共同、または他組織がアップデートした内容をベースに、CRYPTRECとしてのアップデートを実施 ※WG設置は想定しない	なし

参考:「文書の作成主体(＝ソース)の違い」の説明図



資料３

2016 年度暗号技術評価委員会 活動報告

1. 活動目的

CRYPTREC 暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う。

2. 活動概要

(1) 暗号技術の安全性及び実装に係る監視及び評価

下記項目に沿い、暗号技術の安全性に係る監視・評価 及び 実装に係る技術の監視・評価を実施する。

① CRYPTREC 暗号等の監視

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

- 今年度実施された監視報告の詳細については、CRYPTREC Report 2016 を参照のこと。
- KCipher-2 について、仕様書に関わる誤記について、推奨候補暗号リストへの追加の有無の審議の際に行われた安全性評価・実装評価は、誤記修正による影響はないことを確認した。(資料７参照)
- DH/ECDH の仕様書の参照先について、参照先の仕様書の変更が軽微なものであることが確認できた。よって、CRYPTREC の ホームページ上の仕様書参照先を修正する。
- 共通鍵暗号の安全性評価について検討を行い、提示すべき推奨方針案について検討を行った。(資料９参照)

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

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

- 今年度、降格および削除対象となる暗号技術はなかった。

② CRYPTREC 注意喚起レポートの発行

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

- 今年度は、下記の注意喚起レポートを発行した。
  - 「SHA-1 の安全性について」[1]（2017 年 3 月 1 日）(資料 8 参照)

③ 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。

- ハッシュ関数 SHA-3 ファミリーの 1 つである SHAKE128 が追加対象アルゴリズムに入っていなかったが、暗号技術評価委員会での審議結果、SHAKE128 についても、パラメータを選択すれば、CRYPTREC 暗号リストへ追加するのに十分な安全性と実装性能を有していることが確認できたことから、推奨候補暗号リストへの新規暗号として推薦する。(資料 5 参照)

④ 新技術に関する調査及び評価

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

- 暗号技術調査ワーキンググループ（暗号解析評価）及び暗号技術調査ワーキンググループ（軽量暗号）を設置し、検討・評価を行った。
- 暗号技術調査ワーキンググループ(暗号解析評価)
  詳細は、別添 1 「2016 年度暗号技術調査 WG（暗号解析評価）活動報告」を参照のこと。
- 暗号技術調査ワーキンググループ(軽量暗号)
  詳細は、別添 2 「2016 年度暗号技術調査 WG（軽量暗号）活動報告」を参照のこと。
- ChaCha20-Poly1305 の安全性評価
  外部評価を実施し、その安全性評価を実施した。
  現時点では ChaCha20-Poly1305 は、認証暗号として、具体的な脅威は見つかっていないと考えられる。(資料 6 参照)

[1] http://cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html

(2) 暗号技術の安全な利用方法に関する調査（技術ガイドラインの整備、学術的な安全性の調査・公表等）

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

- 引き続き、調査・検討を行っている。

3. 開催スケジュール

第 1 回暗号技術評価委員会　2016 年 7 月 27 日(水)

第 2 回暗号技術評価委員会　2017 年 3 月 21 日(火)

（参考資料） 委員構成

暗号技術評価委員会委員名簿

委員長	太田　和夫	国立大学法人電気通信大学 大学院情報理工学研究科 情報学専攻(セキュリティ情報学プログラム)　教授
委員	岩田　哲	国立大学法人名古屋大学 大学院工学研究科　准教授
委員	上原　哲太郎	立命館大学 情報理工学部情報システム学科　教授
委員	金子　敏信	東京理科大学 理工学部電気電子情報工学科　教授
委員	佐々木　良一	東京電機大学 未来科学部情報メディア学科　教授
委員	高木　剛	国立大学法人九州大学 マス・フォア・インダストリ研究所 教授
委員	手塚　悟	慶應義塾大学 大学院政策・メディア研究科　特任教授
委員	本間　尚文	国立大学法人東北大学　電気通信研究所　教授
委員	松本　勉	国立大学法人横浜国立大学 大学院環境情報研究院　教授
委員	松本　泰	セコム株式会社 IS研究所 コミュニケーションプラットフォーム ディビジョン ディビジョンマネージャー
委員	盛合　志帆	国立研究開発法人情報通信研究機構 サイバー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	渡邊　創	国立研究開発法人産業技術総合研究所 情報技術研究部門 上級主任研究員

[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 情報学専攻(セキュリティ情報学プログラム)　教授
委員	草川　恵太	日本電信電話株式会社 NTTセキュアプラットフォーム研究所　研究員
委員	國廣　昇	国立大学法人東京大学 大学院新領域創成科学研究科複雑理工学専攻　准教授
委員	下山　武司	株式会社富士通研究所 知識情報処理研究所 データ・プライバシー保護プロジェクト　主管研究員
委員	安田　雅哉	国立大学法人九州大学　マス・フォア・インダストリ研究所 准教授

[暗号技術調査ワーキンググループ(軽量暗号)]

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

資料３別添１

2016 年度 暗号技術調査 WG(暗号解析評価)活動報告

1. 活動目的・方針(昨年度からの継続)

(1)楕円曲線上の離散対数問題(ECDLP)の困難性に関する調査

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

- 2015 年度は、ECDLP に対する指数計算法について過去に発表された論文などを精査し、論点や課題を事務局にて整理した。
- 2016 年度は、昨年度事務局が整理した論点や課題に基づき、近年発表されている指数計算法を用いた攻撃手法を解説する資料を作成した。

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

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

- 2015 年度は、多重線形写像に関する過去の論文を調査し、提案されている代表的な応用例についてまとめた。また、難読化に関して安全性について外部評価を行い、その研究動向についてまとめた。
- 2016 年度は、多重線形写像に関して安全性について外部評価を行い、近年研究が進展している多重線形写像に関する研究動向をまとめた。

(3)予測図の更新

例年公表している予測図の更新に大きく影響を与えるような研究結果等がないかどうかの確認を行う。また、TOP500.ORG[1]が公表する計算機能力に関するデータに基づき、例年公表している予測図の更新を行う。

- 2015 年度は、「素因数分解問題の困難性」及び「楕円曲線上の離散対数問題の困難性」に関するグラフの更新を行った。
- 2016 年度は、予測図の更新に加えて、過去の議論・経緯などを把握できる資料について検討した。

[1] https://www.top500.org

2. 委員構成

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

3. スケジュール

第1回　2016年7月27日(水)　　活動計画案や作業内容についての審議と承認
第2回　2017年2月21日(火)　　調査内容についての審議と承認

4. 成果概要

4.1. 楕円曲線上の離散対数問題(ECDLP)の困難性に関する調査

楕円曲線上の離散対数問題(ECDLP)に関する指数計算法(Index Calculus)について調査を行い、研究内容をまとめることが第一回WGにて承認され、下記の通り実施した。第二回WGにて承認された当該調査における見解を下記に記す。なお、調査レポートの概要は付録A.1.に記す。また、調査レポートはCRYPTREC のホームページ上にて公開を予定している。

[評価レポートにおける見解]

楕円曲線上の離散対数問題(ECDLP)の困難性は楕円曲線暗号やペアリング暗号の安全性の基盤となっている（図1)。今のところECDLPを最も効率よく解くアルゴリズムは ρ 法であり、その計算量は群の位数に関して指数時間である。

その一方で、近年、計算量が準指数時間となる、ECDLP に関する指数計算法が提案された[PQ12]。しかし、この計算量評価では検証が不十分な仮定(First Fall Degree Assumption(FFDA)など)が導入されており、その仮定の正当性は理論的にも数値実験的にも十分に立証されていない。さらに ρ 法を利用した場合に解くことが期待できる十分大きなECDLPが当該指数計算法によって解かれたという成果も報告されていない。

従って、現時点では当該指数計算法より、ρ法の方が計算効率が優れていると判断するのが妥当である。

[WG の判断]

当該指数計算法の計算量が準指数時間であることは理論的にも数値実験的にも現時点では十分に立証されていない。従って、ECDLP を安全性の根拠とする暗号の安全性評価について、現時点では、標数に拠らず、今のところ最も効率が良い ρ 法ベースの安全性評価基準を採用していれば十分であると判断する。ただし、引き続き、当該指数計算法の研究動向を把握しておく必要がある。

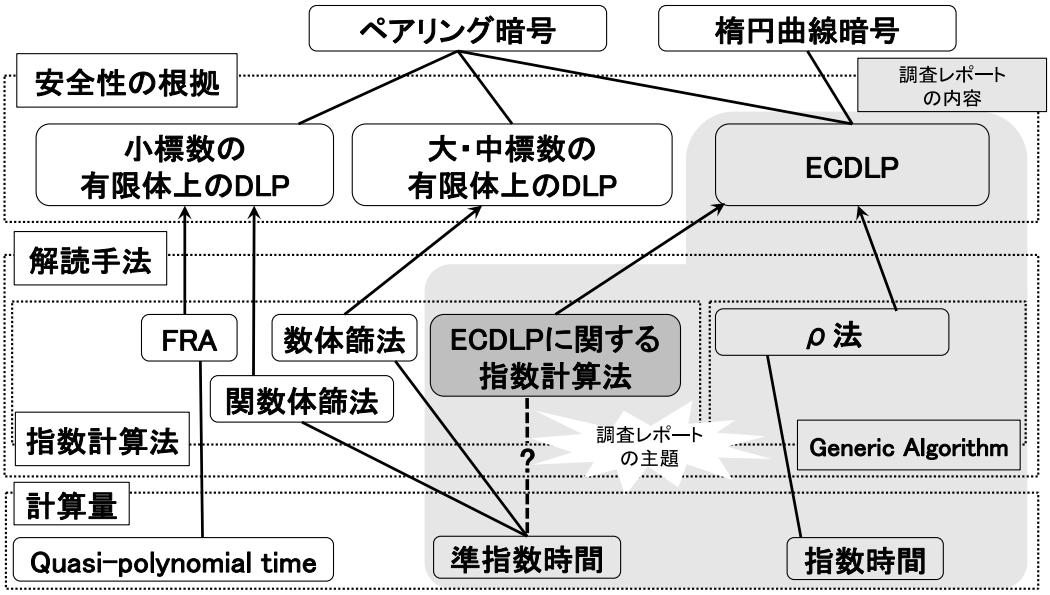


図 1:離散対数問題と種々の解読手法との関係

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

多重線形写像(Multi-linear map)の最新動向に関する調査を行い、研究動向をまとめることが第一回 WG にて承認され、下記の通り実施した。第二回 WG にて承認された多重線形写像の最新動向に関する見解を下記に記す。なお、評価レポートの概要は付録 A.2.に記す。また、評価レポートは CRYPTREC のホームページ上にて公開を予定している。

[評価レポートにおける見解]

現在提案されている多重線形写像は、多重線形写像に基づく多重 Diffie-Hellman 鍵交換方式に対して攻撃論文が存在する。知識型暗号方式（witness encryption） や 識別型難読化方式（indistinguishability obfuscation）の存在証明に用いられていた多くの安全性仮定が成立しないことも示されている。一方、識別型難読化方式 が存在すれば多重線形写像が構成可能であることも示されている。つまり、識別型難読化方式に対する構成不可能性は

示されていないため、その構成可能性は残されている。

[WG の判断]

多重線形写像は、従来技術では実現し難い機能などを提供することができる、有力なプリミティブであり、非常に注目されその進展が目覚ましい技術である。現時点では安全な多重線形写像の構成は実在しないが、その存在の可能性は否定されていないことから、引き続き研究動向は把握しておき、今後具体的な構成方法が提案された折に、改めて評価・検討を行うこととする。

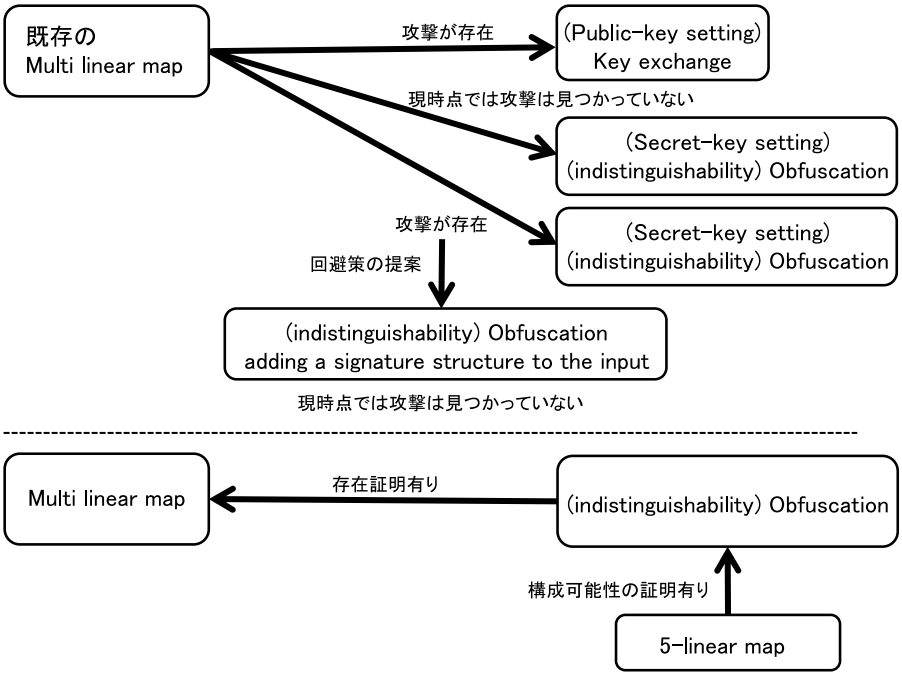


図 2：多重線形写像の構成に関する現状

4.3. 予測図の更新

「素因数分解問題の困難性」及び「楕円曲線上の離散対数問題の困難性」に関して、2016 年 6 月及び 11 月に TOP500.org のスーパーコンピューターのリストの更新があったため、2015 年度に作成した素因数分解問題及び楕円曲線上の離散対数問題の困難性に関する予測図をそれぞれ更新した（付録 A3. 図 3 及び図 4）。

図 3 を作成するにあたって使用したふるい処理に関するデータは 2006 年度のものであり、古くなってきたため、更新が必要である。また、過去の議論・経緯などを把握できる資料の作成については、過去の活動内容を Web 上で検索し易いように改善することで今後対応する。

5 その他

5.1. 有限体上の離散対数問題の安全性に関する最新動向について

(1) 768 ビット DLP の求解記録について

2016 年 6 月 16 日に，メーリングリスト NMBRTHRY[2]に 768 ビットのサイズの素体における離散対数の計算に成功したとの報告が掲載された 。現在、この結果は Cryptology ePrint Archive 2017/067に掲載され [3]、EUROCRYPT 2017 に採録される予定となっている 。以前の記録は，596 ビット(2014 年 6 月 11 日)であった 。篩ステップに 4000 Intel Xeon 2.2GHz・年，線形代数ステップに 900 Intel Xeon 2.2GHz・年を要している(なお，RSA768 について，篩ステップに 1500 Intel Xeon 2.2GHz・年，線形代数ステップに 75 Intel Xeon 2.2GHz・年を要していた。)。

CRYPTREC 暗号リストに掲載されている DSA 及び Diffie-Hellman の安全性については,素体(GF(p),p:素数)から構成されており，p のサイズが 2048 ビット以上であれば直ちに影響はない。

2015 年に Logjam 攻撃を発表した論文 [4]では，特定の素数 p に対して事前計算(数体篩法における多項式選択・篩・線形代数の各ステップに相当)を十分に実行しておけば,同じ p に対してターゲットとなる元の離散対数を効率的に計算可能であるリスクがあることを指摘していた。H. Kario 氏のブログ Securitypitfalls の 2016 年 7 月のデータ [5]によれば，約 60 万の主要なサイトのうち，鍵交換において DH が利用できるのは約 54.3%あり，そのうちの約 35.5%は 1024 ビット以下の鍵長である。鍵長を 2048 ビット以上に設定するなどの注意喚起が必要であると考えられる。

(2) Extended Tower Number Field Sieve の影響について

有限体上離散対数問題(DLP)を計算する「数体篩法」の改良 Extended Tower Number Field Sieve(exTNFS)の提案[1]が CRYPTO 2016 に採録された。exTNFS では，有限体の中でも特に合成数次数の拡大体の DLP を考えている。CRYPTREC 暗号リストには合成数次数拡大体の DLP を安全性の根拠とする暗号技術は掲載されていないため影響は無い。しかし，現在，研究・開発が進められているペアリング暗号の中には合成数次数拡大体の DLP が安全性の根拠となるものがある（例: Barreto-Naehrig 曲線上ペアリングでは 12 次拡大体）ため，それらの安全性に影響があると考えられる。

---

[2] https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1606&L=NMBRTHRY&P=3649
[3] https://eprint.iacr.org/2017/067
[4] https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf
[5] https://securitypitfalls.wordpress.com/2016/09/06/july-2016-scan-results/

拡大体F_Qの DLP に対する数体篩法の漸近的な計算量は

$$L_Q(1/3, c) = \exp((c + o(1))\,(\log Q)^{\frac{1}{3}}\,(\log\log Q)^{\frac{2}{3}}) \qquad (式\ 1)$$

により与えられる。定数cが小さいほど計算量が小さくなる。また，標数の大きさにより漸近的な計算量が異なる（medium prime/boundary/large prime に分けられている)。表 1（[1]から転載）は従来の数体篩法(NFS, TNFS)と exTNFS の計算量の比較である。表中の値は$c = (c'/9)^{1/3}$となるc'である。

表 1：式 1 における c' の値([1]から転載)

$p = L_Q(l_p)$	$1/3 < l_p < 2/3$	best $l_p = 2/3$	$2/3 < l_p < 1$
TNFS [5,6]	none	none	64
NFS-JLSV [7]	128	64	64
NFS-(Conj and GJL) [8]	96	48	64
NFS-SS [9]	96	48	64
exTNFS [1]	48	48	64

特に標数が特殊な構造を持っている場合は，その構造を利用してさらに計算量を小さくすることができる。特にこのような場合には特殊数体篩法(SNFS)と呼ばれる。Barreto-Naehrig 曲線のペアリングでは標数が特殊な構造であるため，特殊数体篩法のケースにあたる。SNFS の場合の計算量を表 2（[1]から転載)に示す。

表 2：式 1 における c' の値([1]から転載)

$p = L_Q(l_p)$	$1/3 < l_p < 2/3$	$2/3 < l_p < 1$
STNFS-JP [10]	64	32
STNFS [5]	none	32
SexTNFS [1]	32	32

Barreto-Naehrig 曲線のペアリングは，例えば IETF Internet Draft[2]によれば，標数が 254 ビット素数，拡大次数 12 のときおおよそ 128 ビットセキュリティ（より正確には 126 ビット[3])であると考えられていた(これらの安全性解析では，数体篩法の計算量は$c = (64/9)^{1/3}$で考慮されていたためである。)。SexTNFS により計算量が$c = (32/9)^{1/3}$に削減されたため，128 ビットセキュリティを満たさないと考えるべきだろう。たとえば，論文[4]では，控えめな見積もりとして 110 ビットセキュリティ程度であると推定している。

表 3：拡大次数 12 の時の計算量評価([4]から転載)

n	algorithm	(η, κ, λ)	with constants	without constants
12	exTNFS	(4, 3, -)	2^{138}	2^{116}
	SexTNFS	(6, 2, 4)	2^{155}	2^{108}

ただし，これはあくまで漸近的な計算量に基づいた理論的解析であり，計算実験による計算量解析はまだ行われていない。実際に安全性にどれだけ影響を与えるか，ビットセキュリティの実際の値はどうなるかを問うためには更なる検証が必要である。

参考文献

[1] T. Kim and R. Barbulescu, “Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case”, CRYPTO 2016, LNCS 9814, pp.543-571, 2016. (IACR Cryptology ePrint Archive: Report 2015/1027.)

[2] A. Kato, M. Scott, T. Kobayashi, and Y. Kawahara, “Barreto-Naehrig Curves”, https://tools.ietf.org/html/draft-kasamatsu-bncurves-02. (Expires: September 19, 2016)

[3] J. Bos, C. Costello, and A. Miele “Elliptic and Hyperelliptic Curves: a Practical Security Analysis”, PKC 2014, LNCS 8383, pp.203-220, 2014. (IACR Cryptology ePrint Archive: Report 2013/644.)

[4] A. Menezes, P. Sarkar, and S. Singh, “Challenges with Assessing the Impact of NFS Advances on the Security of Pairing-based Cryptography”, IACR Cryptology ePrint Archive: Report 2016/1102.

[5]. Barbulescu, R., Gaudry, P., Kleinjung, T.: The towed number field sieve. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 31-55. Springer, Heidelberg (2015).

[6]. Schirokauer, O.: Using number fields to compute logarithms in finite fields. Math. Comput. 69(231), 1267-1283 (2000)

[7]. Joux, A., Lercier, R., Smart, N.P., Vercauteren, F.: The number field sieve in the medium prime case. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp.326-344. Springer, Heidelberg (2006)

[8]. Barbulescu, R., Gaudry, P., Guillevic, A., Morain, F.: Improving NFS for the discrete logarithm problem in non-prime finite fields. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 129-155. Springer, Heidelberg (2015)

[9]. Sarkar, P., Singh, S.: New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 429-458. Springer, Heidelberg (2016).

[10]. Joux, A., Pierrot, C.: The special number field sieve in $\mathbb{F}_{p^n}$. In: Cao, Z., Zhang, F. (eds.) Pairing 2013. LNCS, vol. 8365, pp. 45-61. Springer, Heidelberg (2014)

5.2. Post-Quantum Cryptography の動向について

NIST は、Post-Quantum Cryptography に関するアルゴリズムの公募を 2016 年 12 月 20 日から正式に開始した。公募に関する詳細は Web 上[6]で公開されている。公募の〆切は、2017 年 11 月 30 日である。また、下記の通り、PQCrypto 開催後に、応募者のプレゼンテーションがある予定である。

- PQCrypto 2018： Florida, 9--11 April 2018.
- NIST workshop： 12--13 April 2018.

5.3. 今後の課題について

- Post-Quantum Cryptography に関する技術動向を今後どのように把握していくべきかの検討が必要である。
- 一般数体篩法に関するふるい処理に関するデータは更新が必要である。
- DLP 768 ビットの求解記録に関する注意喚起が必要である。
- SHA-1 の移行問題に観られるように社会基盤に組み込まれた暗号アルゴリズムの移行には、非常に時間がかかる。また、暗号アルゴリズムの評価を行い、暗号アルゴリズムを何時まで利用できるかを検討する際、暗号鍵のライフサイクルを考慮する必要がある。ルート認証局は、すでに RSA2048bit からの移行が始まっているが、これは、20 年以上の有効期限が必要なためである。従来、CRYPTREC では 10 年間は大丈夫としているが、10 年では足りない。社会基盤に組み込まれる暗号技術の観点からは、もっと長期のロードマップに基づいた評価が必要になる。

以上

[6] http://www.nist.gov/pqcrypto

付録 A.1. 楕円曲線上の離散対数問題(ECDLP)の困難性に関する調査

［レポートの概要］

楕円曲線上の離散対数問題(ECDLP)の困難性は楕円曲線暗号やペアリング暗号の安全性の基盤となっている（図 1)。今のところ ECDLP を最も効率よく解くアルゴリズムは ρ 法であり、その計算量は群の位数に関して指数時間である。そして ρ 法の計算量およびそれを用いた計算機実験の結果から安全な鍵長が見積もられている。なお、計算機実験では現時点では約 110 ビット長以上の ECDLP が解かれている。

近年、ECDLP に関する指数計算法の研究が進められている。当該指数計算法では、多変数連立代数方程式を生成する過程及びその多変数連立代数方程式を解く過程を通じて、ECDLP を線形方程式を解く問題に帰着させる。前者の過程では、Summation polynomial 及び Weil descent 等の手法が、後者の過程では、グレブナー基底等の手法が用いられる。

標数が 2 の場合に、ECDLP に関する指数計算法の計算量が準指数時間であることを主張する論文[PQ12]が発表されているが、計算量評価において、検証が不十分な仮定(First Fall Degree Assumption(FFDA)など)が導入されていることが問題となっており、仮定の妥当性やρ法の計算効率との比較が課題となっている。

現時点では、理論的にも数値実験的にも FFDA 等の仮定の正当性が十分に立証されておらず、ρ 法を利用した場合に解くことが期待できる十分大きな ECDLP が指数計算法によって解かれたという成果も報告されていない。これらは、多変数連立代数方程式を解くのに要求されるリソースが非常に高いことも障害となっている。従って、現時点では、標数に拠らず、今のところ最も効率が良い ρ 法ベースの安全性評価基準を採用していれば十分であると判断する。ただし、引き続き、当該指数計算法の研究動向を把握しておく必要がある。

なお、当該調査では、ECDLP に関する指数計算法の文献に現れる実験データを整理することも目的の一つであった。しかし、整理できるほど十分な量の実験データは存在しなかった。即ち、文献で扱われる実験例は連立代数方程式に関するものが多く、指数計算法によって ECDLP を解いた実験例は少なく、解かれた ECDLP のビット長も十分大きくないものであった。

［レポートの構成］

・1 節：はじめに
・2 節：楕円曲線上の離散対数問題 (ECDLP)
  - DLP 及び ECDLP の定義
・3 節：Generic algorithm による DLP の計算
  - ρ法の説明及びρ法による ECDLP の世界記録

曲線の種類	サイズ(bit)	年	著者
素体	112	2009	Bos et al.
標数 2 の拡大体	118	2016	Bernstein et al.
Koblitz	113	2014	Wenger and Wolfger

・4 節：ECDLP に関する指数計算法

- 指数計算法の説明（ECDLP を線型方程式に変換）
- ECDLP に関する指数計算法の説明
  - 線型方程式を生成するために、Summation polynomial と Weil descent を利用して連立代数方程式生成する。
  - F_4-style のアルゴリズムと FGLM を利用して連立代数方程式を解き、その解から線型方程式を生成する。
  - 線型方程式を解くことで ECDLP の解がえられる。

  $E(F_q^n)$ 上の ECDLP に関する指数計算法の計算量の評価

$$O(2^{m^2} + q^{n'} m!\, C_{dcmp} + q^{n'} \omega)$$

  m: summation polynomial のパラメータ、

  n’ m≒n、$2 < \omega \leqq 3$、

  C_{dcmp}: 連立代数方程式を解くために必要な計算量（この段階では未知数として扱う）

・5 節：有限体における連立代数方程式の解法

- 多項式集合 F で与えられる連立代数方程式を解く手順：
  - F_4-style のアルゴリズムを用いて、F の全次数逆辞書式順序のグレブナー基底 G_{DRL}を計算する。
  - FGLM を用いて G_{DRL} を辞書式順序のグレブナー基底 G_{LEX} へ変換する。
  - G_{LEX} に含まれる一変数方程式の解を求め、それを G_{LEX} の他の多項式に代入する。この計算を繰り返すことで F の解を得る.
- F_4-style のアルゴリズムの概要
  - d 次のグレブナー基底の計算に必要な S 多項式及び簡約に利用する多項式の係数を行成分とする行列 M(d) を生成する。($\mathbf{M(d)}$ は d 次の Macaulay 行列の部分行列)
  - M(d) に対して行簡約を行い、d 次のグレブナー基底を生成する。
  - 上記の計算をグレブナー基底の計算が終わるまで繰り返す。(最大の d を D_{reg} であらわす。)
- F_4-style のアルゴリズムの計算量とその評価の課題
  - $O((m+D_{reg})^{D_{reg}\omega})$。

    但し、m は変数の個数、$2<\omega\leqq3$ とする。また、この評価は最悪計算量にあたる。

- D_{reg} の評価は難しいため、仮定（first fall degree assumption (FFDA) など）を導入する場合がある。

- F_4-style とその使用メモリ量
  - F_4-style では Macaulay 行列の部分行列に対して行簡約を行う。従って、行列が素行列であっても簡約が進むにつれて一般的に非零成分が増加し、最終的に多くのメモリを必要とする傾向がある。特に、変数の個数と D_{reg} の増加に伴い膨大なメモリを必要とする。

・6 節：ECDLP に関する指数計算法及び研究動向

- First fall degree D_{first}：(簡単に言うと) グレブナー基底の計算で生じる多項式簡約で、簡約前の多項式 f より次数の小さい多項式が発生するときの、最小の f の次数。
- FFDA: D_{first} は D_{reg} にほぼ等しい。
- Petit と Quisquater は、$E(F_{2^n})$の場合で summation polynomial S_mと Weil descent を利用して生成した連立代数方程式に対して $D_{first} \fallingdotseq O(m^2)$と見積もっている[FP12]。この場合、全体の計算量はある定数 C に対して以下で与えられる：

$$O\left(2^{Cn^{\frac{2}{3}}\log n}\right).$$

- FFDA の妥当性
  - 連立代数方程式によっては、FFDA が成り立つ例も成り立たない例も存在する (6.1.2 節)。
  - ECDLP で summation polynomial と Weil descent を利用した場合、理論的には FFDA が成り立つことも成り立たないことも立証されていない。実験的には $E(F_{2^n})$ で $n \leqq 40$ くらいまでで検証されている。

・7 節：まとめ

- $E(F_{2^n})$上の ECDLP に関する指数計算法で、その計算量が準指数時間になることを主張している文献がいくつか存在する。しかし FFDA など、それらの文献で利用している仮定の正当性は必ずしも保証されていない。
- ECDLP に関する指数計算法とρ法の比較で重要なのは、[GG16] でも述べられているように、現時点で実際にどれくらいの大きさの ECDLP が解かれているかである。
- ρ法で 110 bit 以上の大きさの ECDLP が解かれているのに対して、指数計算法では限られた小さな ECDLP しか解かれていない。
- 以上の理由から、ECDLP に関する指数計算法よりρ法の方が計算効率が優れていると判断する。

- 但し、ECDLP に関する指数計算法に関する研究の動向を今後も見ていく必要がある。

参考文献

[FPPR12] J.-C. Faugère, L. Perret, C. Petit, and G. Renault. Improving the complexity of index calculus algorithms in elliptic curves over binary fields. In EUROCRYPT 2012, Proceedings, pp. 27-44, 2012.

[GG16] S. D. Galbraith and P. Gaudry. Recent progress on the elliptic curve discrete logarithm problem. Des. Codes Cryptography, Vol. 78, No. 1, pp. 51-72, 2016.

[PQ12] C. Petit and J.J. Quisquater. On polynomial systems arising from a Weil descent. In ASIACRYPT 2012, Proceedings, pp. 451-466, 2012.

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

［レポートの概要］

・構成

本レポートは、エクゼクティブサマリ、 1 章 序章、2 章 定義及び構成、3 章 既知の攻撃の紹介、4 章まとめ及び今後の展望となっている。本レポートは、現時点での主要結果を俯瞰したものであり、新しい定義・構成方法・主たるアプリケーション・提案方式に対する攻撃方法・安全性に対する議論等について言及している。なお、このレポートは、2017 年 1 月時点の情報に基づいている。

・要旨

- 多重線形写像には、主たる提案が 3 つある。最初の提案は、Garg, Gentry, Halevi らによるもので、次数付き擬暗号化方式（graded encoding scheme）を用いた構成（GGH13）[GGH13a] である。これに続いて、 Coron, Lepoint, Tibouchi らにより、整数上で動作する構成（CLT13）[CLT13a] が提案された。さらに、Gentry, Gorbunov, Halevi らにより、グラフ誘導擬暗号化方式（graph-induced encoding scheme）を用いた構成（GGH15）[GGH15] が提案された。（Section 2.4.1, Section 2.4.2, Section 2.4.3, Section 2.5）
- 多重線形写像の構成については、解法困難と仮定される問題への帰着などの安全性証明は示されていない。（Section 1.3）
- 多重線形写像の重要なアプリケーションである Diffie-Hellman 多重鍵交換プロトコルについては、それぞれの多重線形写像に基づく方式について、多項式時間で実行可能な攻撃方法が存在する。さらに、知識型暗号方式（witness encryption）や識別型難読化方式（indistinguishability obfuscation）等の存在証明に用いられている安全性仮定

の多くが成立しないことが明らかとなっている。(Section 3)

- これらの状況は、必ずしも具体的な構成に対する攻撃につながるものばかりではない。実際、GGH13・CLT13・GGH15 のそれぞれの多重線形写像に基づいた、具体的攻撃は知られていない識別型難読化方式の構成は存在する。(Section 4.1)
- 理論的に、PRF などが存在する仮定の下では、識別型難読化方式 と関数型暗号 (functional encryption) とが、本質的に等価であることが知られている。このことは、十分大きな n に対する n 重線形写像の存在可能性を意味する。このことから、識別型難読化方式 や関数型暗号を構成する手法を応用した安全な多重線形写像の構成可能性が期待できる。しかし、現時点では具体的な構成は見つかってはいない。(Section 1.4)
- 5 重線形写像 が存在すれば、それを基に識別型難読化方式 が構成可能であることも近年示されている。しかし、双線形写像から 5 重線形写像への拡張方法は現在知られていない。(Section2.3.2, Section 4.2)
- 効率性については、今後の課題の一つとなっている。(Section 4.1)

参考文献

[GGH13a] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, EUROCRYPT 2013, volume 7881 of LNCS, pages 1-17, Athens, Greece, May 26-30, 2013. Springer, Heidelberg, Germany.

[CLT13a] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In Ran Canetti and Juan A. Garay, editors, CRYPTO 2013, Part I, volume 8042 of LNCS, pages 476-493, Santa Barbara, CA, USA, August 18-22, 2013. Springer, Heidelberg, Germany.

[GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, TCC 2015, Part II, volume 9015 of LNCS, pages 498-527, Warsaw, Poland, March 23-25, 2015. Springer, Heidelberg, Germany.

付録 A.3. 予測図の更新(素因数分解問題及び楕円曲線上の離散対数問題の困難性)

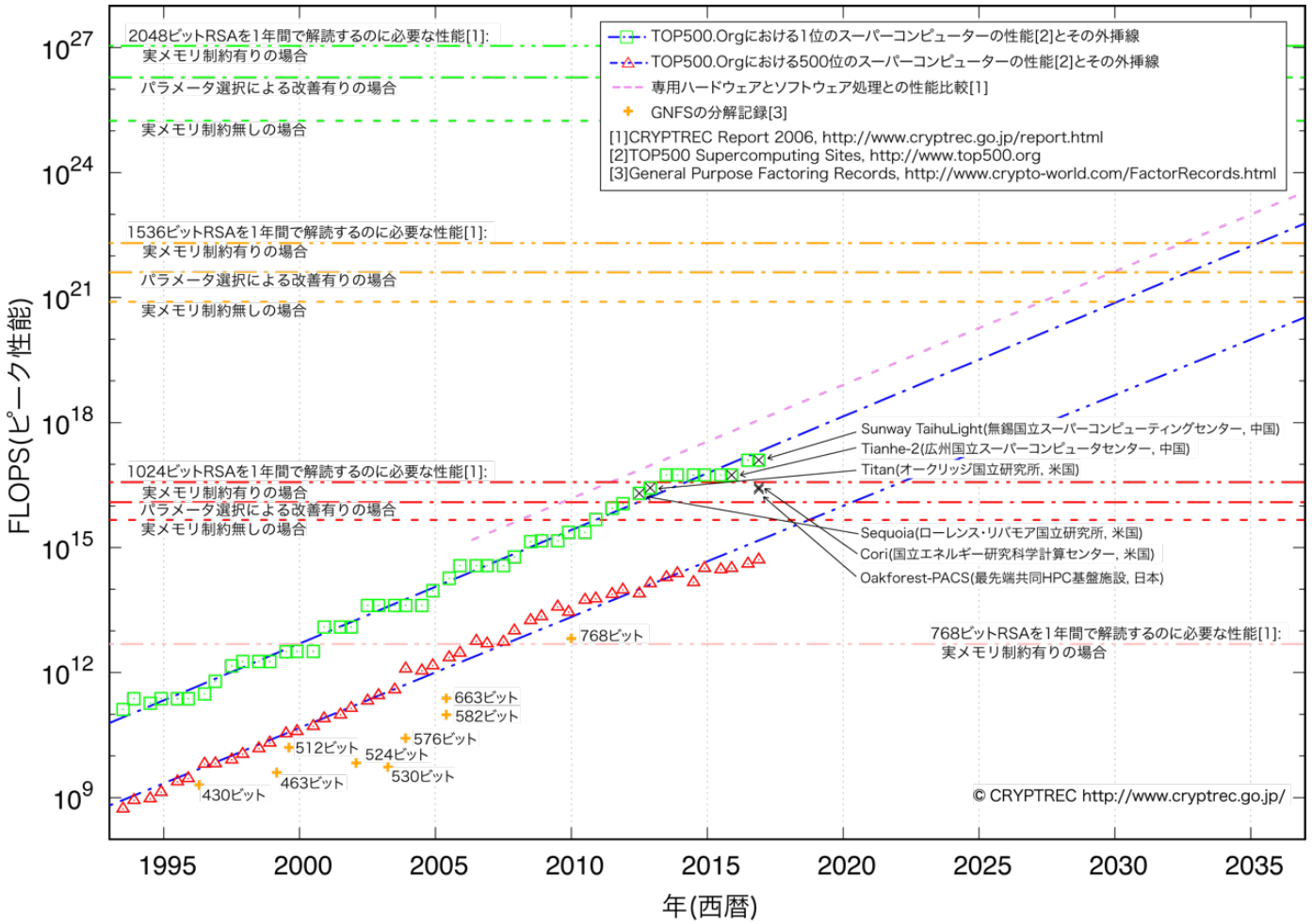


図 3：1 年間でふるい処理を完了するのに要求される処理能力の予測(2017 年 2 月更新)[7]

[7] スーパーコンピューターの性能の伸びに関する外挿線は僅かではあるが鈍化してきている。

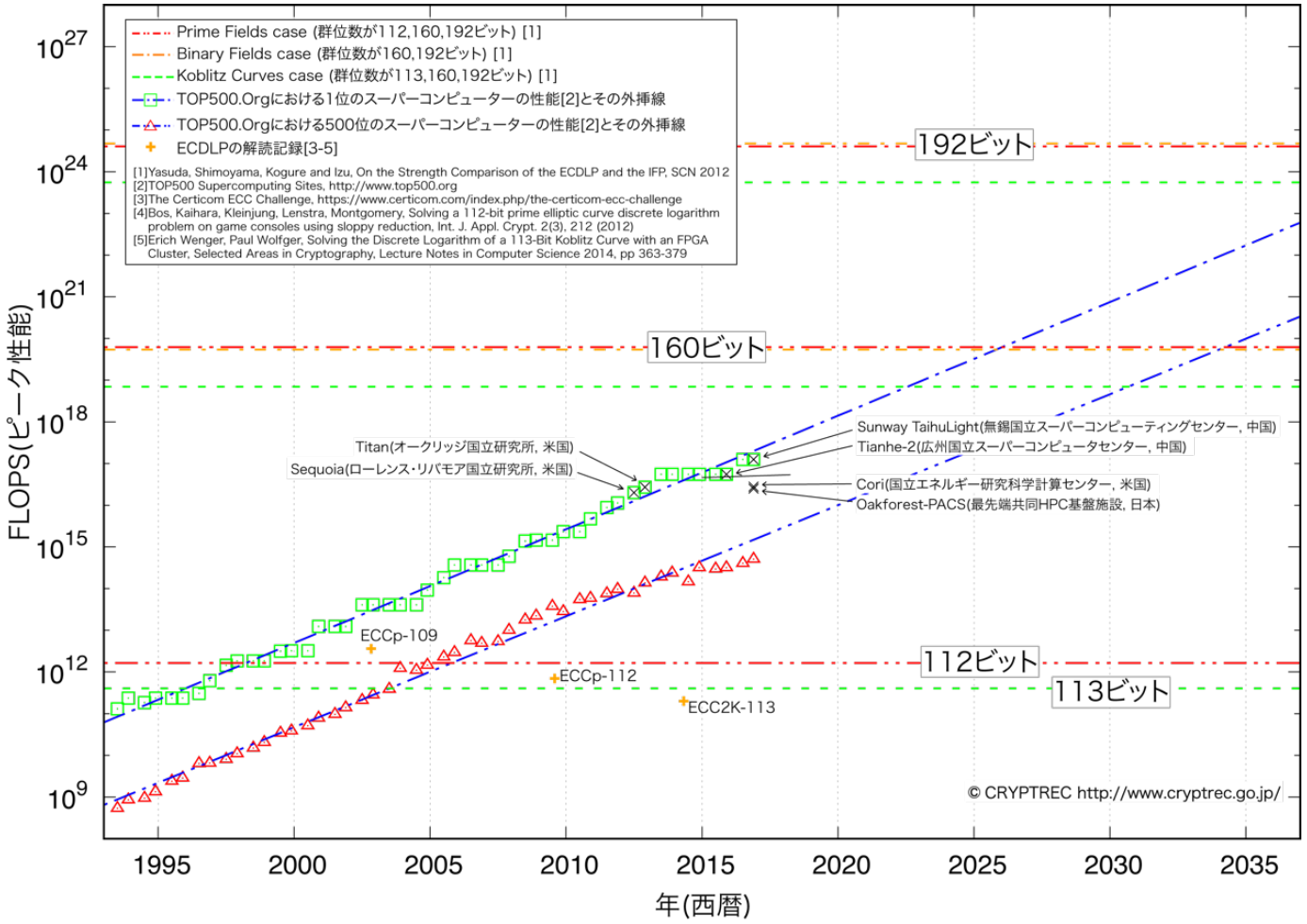


図 4： ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測(2017 年 2 月更新)[8]

以上

[8] スーパーコンピューターの性能の伸びに関する外挿線は僅かではあるが鈍化してきている。

資料３　別添２

2016 年度 暗号技術調査 WG(軽量暗号)活動報告

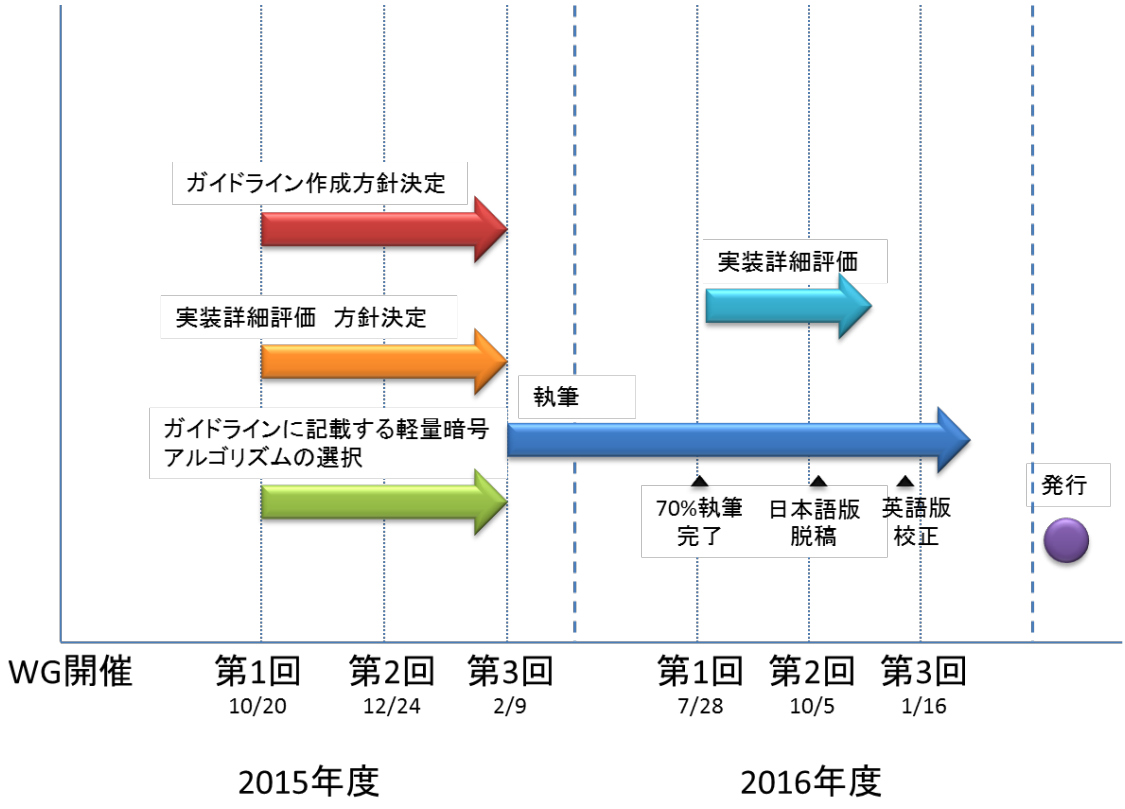
1.　活動目的・方針(昨年度からの継続)

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

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

2015 年度に、ガイドラインの作成方針を決定し、ガイドラインに記載する軽量暗号アルゴリズムを選択し、実装詳細評価方針を決定し、軽量暗号 WG 活動の対外的アピールのあり方に関する検討をした。

2016 年度は、2015 年度の検討結果に基づき、実際に「暗号技術ガイドライン（軽量暗号)」の日本語版・英語版の執筆を行った。ガイドライン執筆に併せて、実装詳細評価を行った。スケジュールは下記のとおり。



暗号技術ガイドライン（軽量暗号）作成スケジュール

2. 委員構成

主査：本間 尚文(国立大学法人東北大学)

委員：青木 和麻呂(日本電信電話株式会社)

委員：岩田 哲(国立大学法人名古屋大学)

委員：小川 一人（日本放送協会）

委員：小熊 寿(株式会社トヨタ IT 開発センター)

委員：崎山 一男(国立大学法人電気通信大学)

委員：渋谷 香士(ソニーグローバルマニュファクチャリング＆オペレーションズ株式会社)

委員：鈴木 大輔(三菱電機株式会社)

委員：成吉 雄一郎（ルネサスエレクトロニクス株式会社)

委員：峯松 一彦(日本電気株式会社)

委員：三宅 秀享(株式会社東芝)

委員：渡辺 大(株式会社日立製作所)

3. スケジュール

第 1 回　2016 年 7 月 28 日(木)	活動計画案、作業内容、実装詳細評価についての審議と承認
第 2 回　2016 年 10 月 5 日(水)	軽量暗号ガイドライン執筆内容についての審議と承認
第 3 回　2017 年 1 月 16 日(月)	実装詳細評価結果の報告及び軽量暗号ガイドライン執筆内容（日本語版・英語版）の審議と承認、出版までのスケジュール確認
今後のスケジュール	2016 年度暗号技術検討会承認後、WEB 公開予定 CRYPTREC Report2016 と同時に出版予定

4. 成果概要

暗号技術ガイドライン（軽量暗号）日本語版・英語版を回覧するので、ご覧ください。

以上

資料４

2016 年度　暗号技術活用委員会活動報告

1.　2016 年度の活動内容と成果概要

1.1　活動内容

2015 年度に、「CRYPTREC の在り方に関する検討グループ」及び「重点課題検討タスクフォース」での検討結果に基づき、暗号技術活用委員会での活動方針の軸足を、「暗号技術を主軸とした検討」から「情報システムとしてのセキュリティ確保に寄与する成果物の提供」に移し、新たな活動方針を以下のように定義し直した。

【活動目的】

暗号技術活用委員会では、情報システム全般のセキュリティ確保に寄与することを目的として必要な活動を行うものとする。具体的には、実運用とセキュリティ確保の両面の観点から、以下の対象を取り扱う。

- 暗号アルゴリズムの利用及び設定に関する運用マネジメント
- 暗号プロトコルの利用及び設定に関する運用マネジメント
- その他、情報システム全体のセキュリティ確保に有用な暗号に関わる運用マネジメント

2016 年度は、上記の活動目的を踏まえ、運用面でのマネジメントに関するガイドライン（以下、運用ガイドライン）を本格的に整備していくことを今後の暗号技術活用委員会（以下、活用委員会）での活動の中心に据えることを視野に、以下の項目について検討を行った。

① 作成すべき運用ガイドラインの対象及び取扱い範囲の切り分けの検討
② 作成した運用ガイドラインのメンテナンス体制の検討
③ 外部組織や業界団体との連携方法の検討
④ 運用ガイドラインの作成
⑤ ベンダや業界団体等の意向をバランスよく取り入れつつ、セキュリティも担保する利用価値の高い成果物となるようにコントロールする
⑥ その他
CRYPTREC として暗号プロトコルをどのように扱うかを重点的に検討するため、「暗号プロトコル課題検討 WG（以下、課題検討 WG)」を設置

なお、①については、暗号プロトコルに関わる部分を課題検討 WG で、それ以外の範囲を暗号技術活用委員会でそれぞれ検討した。また、④と⑤については、実際の運用ガイドラインを作成する際に、テーマに応じて適切な手段を活用委員会で判断して実施していくことになった。

1.2　暗号技術活用委員会の委員構成及び開催状況

活用委員会の委員構成は表 1-1 である。また、2016 年度 2 回開催された活用委員会での審議概要は表 1-2 のとおりである。

表 1-1 暗号技術活用委員会　委員構成

委員長	松本　勉	国立大学法人横浜国立大学　大学院環境情報研究院　教授
委員	上原　哲太郎	立命館大学　情報理工学部情報システム学科　教授
委員	菊池　浩明	明治大学　総合数理学部　先端メディアサイエンス学科　教授
委員	須賀　祐治	株式会社インターネットイニシアティブ　セキュリティ本部セキュリティ情報統括室　シニアエンジニア
委員	杉尾　信行	株式会社 ＮＴＴドコモ　サービスイノベーション部
委員	清藤　武暢	日本銀行金融研究所　情報技術研究センター
委員	手塚　悟	慶應義塾大学　大学院政策・メディア研究科　特任教授
委員	寺村　亮一	NRI セキュアテクノロジーズ株式会社　主任
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	三澤　学	三菱電機株式会社　情報技術総合研究所　情報ネットワーク基盤技術部 車載セキュリティグループ　主席研究員
委員	満塩　尚史	内閣官房　IT 総合戦略室　政府 CIO 補佐官
委員	村木　由梨香	日本マイクロソフト株式会社　セキュリティレスポンスチーム　セキュリティプログラムマネージャー
委員	山岸　篤弘	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　主席研究員
委員	山口　利恵	国立大学法人東京大学　大学院情報理工学系研究科　ソーシャル ICT 研究センター　特任准教授
委員	渡邊　創	国立研究開発法人産業技術総合研究所　情報・人間工学領域研究戦略部 研究企画室　企画主幹

表 1-2　暗号技術活用委員会　開催状況

回	開催日	議案
第 1 回	2016 年 11 月 9 日	・暗号プロトコル課題検討 WG 活動状況報告 ・運用ガイドライン（「SSL/TLS 暗号設定ガイドライン」）のメンテナンス方法に関する検討 ・運用ガイドラインの対象範囲に関する検討
第 2 回	2017 年 3 月 15 日	・暗号プロトコル課題検討 WG 活動報告 ・暗号プロトコル以外の運用ガイドラインの対象の検討 ・外部連携の進め方の検討 ・2016 年度暗号技術活用委員会報告書

1.3　暗号プロトコル課題検討 WG の委員構成及び開催状況

課題検討 WG の委員構成は表 2-1、3 回開催された課題検討 WG での審議概要は表 2-2 のとおりである。

表 2-1 暗号プロトコル課題検討 WG　委員構成

主査	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	大泰司　章	一般財団法人日本情報経済社会推進協会　インターネットトラストセンター　企画室　室長
委員	坂根　昌一	シスコシステムズ合同会社　イノベーションセンター　エンジニア
委員	佐古　和恵	日本電気株式会社　セキュリティ研究所　技術主幹
委員	佐藤　直之	SCSK 株式会社　IT マネジメント事業部門 netX データセンター事業本部　セキュリティサービス部　シニアコンサルタント
委員	下山　武司	株式会社富士通研究所　サイバー&データセキュリティプロジェクト　主管研究員
委員	須賀　祐治	株式会社インターネットイニシアティブ　セキュリティ本部セキュリティ情報統括室　シニアエンジニア
委員	清藤　武暢	日本銀行金融研究所　情報技術研究センター
委員	村木　由梨香	日本マイクロソフト株式会社　セキュリティレスポンスチーム　セキュリティプログラムマネージャー
委員	吉田　博隆	国立研究開発法人産業技術総合研究所　情報技術研究部門サイバーフィジカルウェア研究グループ　主任研究員
委員	寺村　亮一	NRI セキュアテクノロジーズ株式会社 主任
委員	渡辺　大	株式会社日立製作所　研究開発グループ　システムイノベーションセンタ　セキュリティ研究部　主任研究員

表 2-2　暗号プロトコル課題検討 WG　開催状況

回	開催日	議案
第 1 回	2016 年 10 月 27 日	WG 活動概要の説明、課題についての自由討議
第 2 回	2016 年 12 月 26 日	第 1 回 WG での討議を踏まえた課題の整理と更なる検討
第 3 回	2017 年 2 月 10 日	報告書案の取りまとめ

1.4　成果概要

1.4.1　運用ガイドラインの対象について

2017 年度以降に活用委員会として運用ガイドラインを作成する価値がある対象を検討するにあたっては、以下の目的と領域に合致する範囲のガイドラインを想定して議論を行った。なお、暗号設定ガイドラインのうち、暗号プロトコルに関する部分については課題検討 WG にて検討を行い、それ以外の部分については活用委員会にて検討を行った。

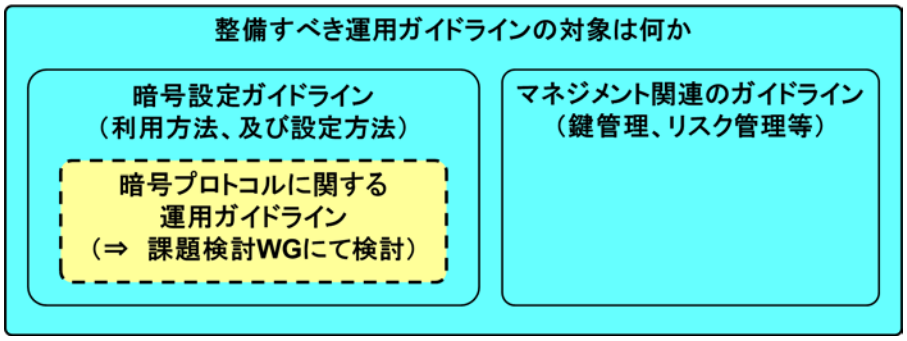
- どのような目的をもつ運用ガイドラインにするか

1. 現在利用されている仕組みの中で安全ではない使われ方を排除し、安全性の底上げを図る（NIST SP800 シリーズのような推奨設定の基準（ガイドライン）をイメージしたもの）
2. 利用者が理解しやすく、かつ採用しやすいベストプラクティスを示す（NIST SP1800 シリーズのような利用しやすいガイドをイメージしたもの）
3. 普及が進んでいない安全な仕組みの普及・活用を促進させる（安全な仕組みへの移行を促すようなガイドをイメージしたもの）
4. 政府、業界団体等が守るべき（半）強制的基準として示す（そうなるような環境整備を含む）

- どのような領域の運用ガイドラインにするか

A. 暗号設定ガイドライン
   - 開発実装に関連するガイドライン
   - 暗号利用・運用・設定に関連するガイドラインで暗号プロトコル以外のもの
   - 暗号利用・運用・設定に関連するガイドラインで暗号プロトコルに関するもの
   - 特定の製品・サービスを安全にするために関連するガイドライン

B. マネジメント関連のガイドライン
   - 暗号システムの運用マネジメントに関連するガイドライン



【暗号プロトコルに関する運用ガイドライン以外の対象】

もともと運用ガイドラインの必要性が高いと考えられている対象を中心に、以下の観点から整理を行った。

表 3-1 に検討結果をまとめる。今後、運用ガイドラインを作成していく際には、表 3-1 に挙げたもののなかから優先的に取り上げていくことが望ましい。なお、「課題」には CRYPTREC が作成する運用ガイドラインの価値を高めるために考慮しなければならないポイントをまとめており、また「関連組織」には連携先として有効と期待される国内組織（国際組織の日本支部を含む）を記した。活動計画の立案に当たっては、これらのポイントを踏まえた計画であることが望まれる。

- 【対象】
  どのような用途で使う運用ガイドラインであるか
- 【目的・内容】
  どのような目的をもった運用ガイドラインを意図したものか（1.4 で挙げた目的の 1.～4. のどれに当たるか）
- 【内容】
  運用ガイドラインに記載される内容はどのようなものか
- 【想定読者】
  その運用ガイドラインの想定読者は誰か
- 【必要性】
  なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか
- 【課題】
  ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か
- 【他組織のガイドライン等】
  他組織が同種のガイドラインを作っていないか／作ろうとしていないか
- 【関連組織】
  どのような他組織と連携していくのがよいか

なお、表 3-1 の「領域」列、及び「目的」列の表記についての注意は次のとおりである。

●「領域」列について
・開発実装に関連する文書類
・暗号利用・運用・設定に関連する文書類で暗号プロトコル以外に関するもの
・暗号システムの運用マネジメントに関連する文書類
・特定の製品・サービスを安全にするために関連する文書類

●「目的」列の表記の意味
①・・・現在利用されている仕組みの中で安全ではない使われ方を排除し、安全性の底上げを図る（安全性評価を含む）
②・・・利用者が理解しやすく、かつ採用しやすいベストプラクティスを示す
③・・・普及が進んでいない安全な仕組みの普及・活用を促進させる
④・・・政府、業界団体等が守るべき（半）強制的基準として示す（そうなるような環境整備を含む）

表 3-1　取りまとめ結果一覧

領域	No.	対象	目的	内容	想定読者	必要性（※委員から意見）	ガイドライン作成にあたっての課題	他組織が発行したガイドライン等	関連組織
A. 開発実装	1	鍵管理（生成・保管・削除）の実装	①②	・乱数性テストのチェック項目 ・安全な鍵生成方法 ・鍵の保管 ・鍵の削除	・システム開発者（特に、プログラマー）・運用者 ・今後システムを構築する中小企業 ・製品開発者	・他の対象に比べて、「鍵管理」を優先的に検討してほしい。 ・鍵の元となる技術であるため、重要（特に公開鍵暗号の鍵生成）。不適切な実装では、知らないうちに素因数を他の鍵と共有している事例もある。 ・日本の情報セキュリティ対策の底上げになる。暗号を応用（利用）したシステム全般の参考にもなる。 ・システム開発者や運用者が想定読者になりうるかは定かでないが、製品開発者向けには必要。 ・SP800-90 では、乱数に必要なエントロピー等について言及しているが、実際には最低限どのようにすればよいのかがわからない。特に、リアルタイム性を要する鍵についてどこまでやればよいかがわかるものがほしい。	・書くべきことの範囲が広い ・抽象的な文書になることが予想されるので、範囲や対象読者を限定しないと作成が困難 ・鍵管理に関する規格を網羅的に調査する必要がある ※「鍵管理」の全体像を整理したのちに優先順位をつけて作成	SP800-90A, B, C	
	2	サーバ証明書の検証方法	①	アプリにおけるサーバ証明書が適切に検証されるための実装方法	システム開発者(特に、アプリケーション開発者)	・アプリでのサーバ証明書検証不備の脆弱性が多い ・IoT 向けに、大量、高速、省リソースという様な観点で、サーバ証明書の検証方法だけでなく、PKI の構築全般について策定されれば、組込機器向けにも参考になる			
	3	電子署名・検証実装方法	①②③	システムに電子署名や検証アプリを実装する方法（ネイティブアプリを作る場合やマルチプラットフォームを想定したブラウザベースの場合等）	システム開発者	・システムへの電子署名や検証アプリの実装者向け文書が少ない。今までは Java でブラウザプラグインとドライバーとつないでいたが、Java がブラウザプラグインをサポートしない方針が表明されており、様々な実装が出てくることが予想されるため、実装に関する情報が必要。 ・民間企業が、JPKI の署名検証を行うことができるようになったので、民間企業のアプリにおいても、電子署名をおこなうアプリを実装することが現実化してきた。 ・実装方法を示さないと多くのアプリが開発されず、電子署名が普及しない。普及のために、実装方法をレクチャーするものという位置づけである。 ・従来は専門家が電子署名の実装を行っていたが、今後は専門ではない SIer も実装に携わる可能性があるため、電子署名を適切に実装させるために必要である。	・実装方法が、技術依存する可能性があり、時期によって変化する。 ・実装方法が複数ある		JNSA 電子署名 WG
	4	Captcha の検証方法	①②	・各社勝手に導入している Captcha の最低限の安全性検査 ・過度に利便性を下げていないか.	システム開発者（特に、アプリケーション開発者）	・各社様々な方式で導入している。銀行などのウェブサイトへのログインにも多用されている。 ・チャレンジレスポンスだと考えれば、必ずしも暗号に無関係ではないため、ガイドラインがあるとよい。			

A. 開発実装	5	将来の暗号危殆化対策を見据えたシステム設計・開発方法 ※C. 暗号システムの運用マネジメントにも記載	②	将来の暗号危殆化対策を見据えたシステム設計・開発方法 　ーインシデント対応方針 　ー暗号アルゴリズムの切替(代替) 　ー当該暗号の使用停止　等	システム設計者・開発者（運用者）	・今後開発されるシステムにおいて、暗号危殆化対応の観点から、設計段階で考慮すべきことを明確化・明文化する必要がある。 ・2030 年頃に使用を停止する 112bit 安全性の暗号に対する危殆化対策は、時期尚早であるため、他のテーマに比べて、優先度は低い。 ・ただし、これから IoT や組み込みなどが普及してくるため、2030 年ぎりぎりまでやらなくてもよいというわけではない。 ・暗号をカセッタブルに実装することが必要であり、それをガイドする必要がある。	・一般的な留意点は整理可能である一方、利用しているシステム毎に暗号の使い方が異なるため、具体手にガイドするのは難しい		
B. 暗号利用・運用・設定（暗号プロトコル以外）	6	鍵管理（生成・保管・削除）の設定/運用	①②③	・鍵管理（生成・保管・削除）上の要求事項 ・代表的な製品での具体的な設定方法例（BitLocker, Azure Key Vault 等）	システム開発者（例えば、プログラマー）・運用者 また、今後システムを構築する中小企業向け。	・暗号を利用するうえで、鍵を秘密に保つことが重要であるにも関わらず、IT 担当者の中には鍵がどういうものかを知らない人すらいる状況であるため、普及啓発が必要。 ・他の対象と比べて「鍵管理」を優先的に検討してほしい。 ・日本の情報セキュリティ対策の底上げになる。暗号を応用（利用）したシステム全般の参考にもなる。 ・鍵管理について個別の製品ごとの設定例が必要である。 ・データ処分(Data Disposed)にも関連する鍵の削除についても必要。 ・例えば、SQL, Exchange といったアプリケーションや、Active Directory での証明書を利用した認証, Federation での認証などを含めると証明書および鍵の管理が必要となる対象が大規模に存在する。 ・ファイル暗号、ディスク暗号に関しても同様に大規模な対象がある。EFS 暗号化、BitLoeker （あるいはデバイス暗号化）の利用率は年々高まっている。	・書くべきことの範囲が非常に広いため、対象範囲を絞る必要がある。 ・抽象的な文書になることが予想されるので、範囲や対象読者を限定しないと作成が困難 ・鍵の生成・削除の文書と併せて用意ができるとよい ※「鍵管理」の全体像を整理したのちに優先順位をつけて作成	・安全な暗号鍵のライフサイクルマネージメントに関する調査　鍵管理ガイドライン（案） ・SP 800-57 Part 2 ・SP 800-57 Part 3 Rev. 1	IPA
	7	SSL・SSH の鍵管理	①②	・OpenSSL の鍵管理 ・CSR を作るときのパスワードの設定	システム管理者、運用者	・他の組織で作成していないようであれば、作成できるのが望ましい。	他組織ですでに存在するようであれば、作成する必要がない。		IPA
	8	ドキュメントへの署名	①③	・PDF の暗号化/署名における暗号の設定	PDF 利用者	・PDF への署名ということでガイドラインがあるべき。PDF の署名で利用する証明書には SHA-1 が利用されている例もあり、適切に利用させる必要があるので、ガイドを作成するべき。 ・署名なしの PDF を出している人も多いため、署名をさせるべき。 ・ユーザが不正な署名に気が付かないので、ユーザへの啓蒙が必要。 ・検討範囲を明確かする必要があるため、時期尚早。代替手段（ファイル暗号化ソフトや Cloud 環境）も存在しており、すぐに対応しなければならないわけではないため、優先度は低い。	・PDF にいくつものバージョンがあり，互換性など懸念 ・ドキュメント管理というと PDF だけでなく、PDF だけでも製品数が多い ・日本では主に JNSA が署名について、検討しているため、JNSA との相談（連携）が必要		JNSA

B. 暗号利用・運用・設定（暗号プロトコル以外）	9	保管データ (Data at Rest)	④	・保管データにおける暗号化方法 ・保管データ暗号化における鍵管理	システム開発者、運用者	・「高度な暗号化」の定義が明確に定まっていないため、明確にした文書（ガイドライン）があるとよい。 ・保管データを暗号化する方法についての文書（や基準）がないため、個人情報保護ガイドラインから参照できるような文書が必要。暗号について議論できる組織体が CRYPTREC しかないので、作成すべき。 ・法律的に定められる必要があり、民間では実施が困難であるため、CRYPTREC で作成するのが望ましい。	他の組織でも検討しているため、歩調を合った基準とするためにもリエゾンを組みながらやらなければならない。	NIST SP800-111	個人情報保護委員会
	10	データの処分 (Data Disposed)	④	・暗号鍵破棄による暗号化された情報の処分についての考え方や方法	システム開発者、運用者	・暗号化を利用して、機密情報を破棄する方法についての文書（や基準）が日本にはないため、個人情報保護ガイドラインから参照できるような文書が必要。CRYPTREC は国内で暗号について議論できる組織体の代表であるため、検討すべき。 ・Cryptographic erase がベストプラクティスであり、法律上認められないとデータの破棄が大変になるので、非常に困るため、検討すべき（例えば、バックアップテープの破棄）。	他の組織でも検討しているため、歩調を合った基準とするためにもリエゾンを組みながらやらなければならない。	NIST SP800-88 Rev.1	個人情報保護委員会
	11	使用中のデータの暗号化 (Data in Use)	②	・暗号化されたまま情報を利用することについての考え方や方法	システム開発者、運用者	・NIST にもガイドラインはないため、検索可能暗号等高機能暗号のガイドラインが必要。	他の組織でも検討しているため、歩調を合った基準とするためにもリエゾンを組みながらやらなければならない。		
C. 暗号システムの運用マネジメント ※考え方・思想を含む	12	鍵管理（生成・保管・削除）の考え方	①③	・鍵管理の考え方 ・鍵生成・管理・削除のライフサイクル ・人がどのように運用するかという手続きも含む	システム開発者（例えば、プログラマー）・運用者 また、今後システムを構築する中小企業向け。	・暗号を利用するうえで、鍵を秘密に保つことが重要であるにも関わらず、IT 担当者の中には鍵がどういうものかを知らない人すらいる状況である。（普及啓発も必要。） ・まずは考え方をまとめたものを作るべきなので、鍵管理関係の中で、優先的に取り組むべき ・鍵管理の考え方が整理されていれば、暗号を応用（利用）したシステム全般の参考にもなるため、日本の情報セキュリティ対策の底上げになる。 ・すでに、2010 年度版　リストガイド（鍵管理）があるため、参考にする、もしくはアップデートするといった方法も視野に入れ、検討すべき。	・技術的な観点だけでなく、法制度を考慮して作成すべき。 ・書くべきことの範囲が広い ・抽象的な文書になることが予想されるので、範囲や対象読者を限定しないと作成が困難 ※「鍵管理」の全体像を整理したのちに優先順位をつけて作成	・SP 800-57 Part 1 Rev. 4 ・NIST Special Publication 800-130　A Framework for Designing Cryptographic Key Management Systems（事）	
	13	暗号システムデザイン	①②（③）	・システム内で利用する暗号機能のマッピング（全体像） ・ネットワークのゾーニングと暗号機能の関係 ・ユースケース別の暗号の使いどころを示す（SSL/TLS 暗号設定ガイドラインの上位レイヤのドキュメントとして位	システム開発者（特に SIer）・運用者・プログラマー等	例えば、得られる費用対効果が大きくないにも関わらず、SSL 通信と IP-VPN を利用した 2 重の暗号化を実施する、機密性を確保できる範囲を意識せず、SSL アクセラレーターを配置するなど、ユーザ及び SIer は暗号対策をどこまでどのように実施すればよいかわからないため、暗号機能を含めたネットワーク設計パターンを示す文書が必要。システムとして、適切なコストでセキュリティを確保するための指針が必要。	・システム構成のサンプル種類がとても多いため、網羅的に書くのは難しい。 ・効果的でない使い方をバッドプラクティスとして検討するのは難しい。		

				置づけ） ・効果的な使い方と効果的でない使い方の例示					
C. 暗号システムの運用マネジメント ※考え方・思想を含む	14	将来の暗号危殆化対策を見据えたシステム設計・開発方法 ※A. 実装開発にも記載	②	将来の暗号危殆化対策を見据えたシステム設計・開発方法 　－インシデント対応方針 　－暗号アルゴリズムの切替(代替) 　－当該暗号の使用停止　等	システム設計者・開発者（運用者）	・今後開発されるシステムにおいて、暗号危殆化対応の観点から、設計段階で考慮すべきことを明確化・明文化する必要がある。 ・2030 年頃に使用を停止する 112bit 安全性の暗号に対する危殆化対策は、時期尚早であるため、他のテーマに比べて、優先度は低い。 ・ただし、これから IoT や組み込みなどが普及してくるため、2030 年ぎりぎりまでやらなくてもよいというわけではない。 ・暗号をカセッタブルに実装することが必要であるため、ガイドする必要がある。	・一般的な留意点は整理可能である一方、利用しているシステム毎に暗号の使い方が異なるため、具体手にガイドするのは難しい。		
	15	RSA から楕円曲線暗号への移行	①③	RSA から楕円曲線暗号への移行の推進	システム設計者・開発者（運用者）	・暗号技術は移行が必要となるので、移行を促進するガイドラインを作成する必要がある（さしあたっては、特に RSA から楕円曲線暗号） ・PKI が最も影響を受ける。 ・暗号の移行には時間がかかるため、RSA から楕円曲線暗号への移行について、早々に整理する必要がある。			
D. 特定の製品・サービス	16	クラウドにおけるセキュリティメカニズムの比較調査	①②	クラウドが採用している暗号化の対象・方式・設定をサービスごとに列挙（秘密計算、秘密分散も含む） ・クラウドサービスにおける TLS で利用している暗号化方式 ・ストレージの暗号化方式 ※定期的に調査を実施するのが好ましい	企画者、システム開発者（特に SIer）	・ユーザがクラウド利用時も暗号に注意して利用するために必要。 ・統一基準でも、クラウドの利用に関しては、クラウドのセキュリティを確認することになっているが、現状では個別に暗号方式や設定等を確認することが困難	・サービス提供者が情報を開示してくれるかは不明。 ・そもそもガイドラインではなく、調査報告書になる可能性がある	JIS Q 27017	・CSA (Cloud Security Alliance)

【暗号プロトコルに関する運用ガイドラインの対象】

暗号プロトコルに関する運用ガイドラインの対象を検討するにあたっては、「(STEP1) 検討対象とする暗号プロトコルの列挙」と「(STEP2) 列挙した暗号プロトコルのなかから運用ガイドラインを作る価値がある／必要性が高いと判断したものを抽出」の 2 段階で議論を行った。

(STEP1) 検討対象とする暗号プロトコルの列挙

課題検討 WG では、暗号プロトコルの列挙にあたって、以下の観点から整理を行った。その結果、表 4-1 にまとめる暗号プロトコルが検討対象として列挙された。

- 【種類】どのような性質のガイドラインが必要と考えられるか

ガイドラインの種類	ガイドラインの概要例	状況
安全性評価に関するガイドライン	• 安全性のお墨付きをつけたプロトコル（＝CRYPTREC 暗号リストのプロトコル版） • 評価されていないプロトコルに対する安全性方法 • 安全なプロトコルを設計するためのガイドライン	• 特定目的のために多くのプロトコルが提案されている • 暗号の専門家が関与しないでプロトコルが作られており、安全性評価が不十分 • 標準化を待っていられないため、先行して実装が進んでいる
実装・開発に関するガイドライン	• 製品の安全な実装・開発をするためのガイドライン • 安全な実装であることを検証するための基準	• この種のガイドラインがない • 各社独自の実装になっている
設定に関するガイドライン	• 製品に実装されている設定方法を適切に設定して安全に利用するためのガイドライン	• プロトコルレベルよりも製品レベルのほうが需要がある • 仕様が固まっている低レイヤのプロトコルであれば、運用ガイドラインが作りやすい

- 【対象】どのようなところで使われる暗号プロトコルを対象範囲とするのがよいか

  Web／証明書失効管理／DNS／NW 管理／鍵管理／ユーザ管理／ユーザ認証／デバイス認証／バイオメトリクス暗号／ID 連携／無線通信／近距離通信／IC カード／メール／リアルタイム通信／ファイル共有／ファイル転送／リモート接続／VPN／自動車／制御システム／仮想通貨／放送暗号

表 4-1　検討対象となりうる暗号プロトコルの列挙一覧

種類	対象	プロトコル名称
安全性評価（暗号技術評価委員会への参考意見とする）	ID 連携	・OpenID Connect
	無線通信	・LoRaWAN
	近距離通信	・Zigbee
		・Bluetooth
	仮想通貨	・Bitcoin プロトコル ・Ethereum ・Hyperledger Fabric ・ブロックチェーン応用（証券決済/契約）
実装／開発	近距離通信	・NFC ・Felica ・ISO/IEC14443 TypeA，TypeB
	IC カード	・Felica
	自動車	【車内】CAN，CAN FD，LIN，FlexRay 【車外】DSRC，ETC2.0 【ハードウェア】EVITA 【センサ】空気圧センサ，ミリ波レーダー
	制御システム	・PLC ・SCADA
設定／運用	Web	・QUIC
		・HTTP/2★

種類	対象	プロトコル名称
設定／運用	バイオメトリクス暗号	・テンプレート保護 ・FIDO
	ID 連携	・OpenID Connect ・SAML
		・OpenID Connect（HTTPS 上で利用） ・代理認証
		・SAML（HTTPS 上で利用） ・代理認証
	無線通信	・WEP ・WPA ・WPA2
	近距離通信	Zigbee
		Bluetooth
	メール	・DKIM ・SPF★ ・DMARC★
		S/MIME を利用したメール送信（メールへの署名）
		・パスワードつき Zip を添付したメール送信 ・S/MIME を利用したメール送信（メールの暗号化） ・オンラインストレージサービス
		OpenPGP を利用したメール送信

設定／運用	証明書 失効管理	・CRL ・OCSP
	DNS	・DNS ・DNSSEC （DANE,DPRIV を含む）
	NW 管理	・SNMP ・NETCONF ・UPnP
	鍵管理	・KMIP
	ユーザ管理	・RADIUS（EAP-TLS 等の利用を含む）・PAP★・CHAPv2・IEEE802.1X
		・LDAP★ （kerberos）
		・PAP★ ・CHAPv2
		・TESLA
	ユーザ認証	・二要素認証
	デバイス認証	・クライアント証明書 ・TPM を利用した認証 ・ISO/IEC9798
	デバイス認証	・Apple MDM ・MS ライセンス認証 ・PUF を利用した認証

設定／運用		・POP 3 ・SMTP ・IMAP （－/over SSL/ with SASL）
		・メッセージングサービス（SMS、Skype、Slack、Line、･･･）
	リアルタイム通信 (VoIP 等)	・SIP★ ・RTP★ ・SRTP
	ファイル共有	・SMB ・CIFS ・WebDAV
	ファイル転送	・SFTP・FTPS・FTP★
	リモート接続	・SSH ・RDP ・telnet★
	VPN	・IPsec-VPN ・TLS-VPN
		・IPsec-VPN
		・TLS-VPN
	仮想通貨	・Bitcoin プロトコル ・Ethereum ・Hyperledger Fabric ・ブロックチェーン応用（証券決済/契約）
	放送暗号	・DRM ・ARIB ・W-CDMA

（STEP2）運用ガイドラインを作る価値がある／必要性が高いと判断したものを抽出

表 4-1 に挙げた暗号プロトコルのうち、運用ガイドラインを作る価値があるか／必要性が高いかを判断するために、以下の観点から整理を行った。その結果、「必要性」「目的・内容」「想定読者」の 3 点について明確に説明できるものを「運用ガイドラインを作る価値がある／必要性が高い」と判断・抽出し、より詳細な検討を加えた。

- 【必要性】
  運用ガイドラインを作る価値／必要性を明確に示すことができるか（なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか）
- 【目的・内容】
  どのような目的・内容をもった運用ガイドラインを意図したものかを明確に示すことができるか（1.4 で挙げた目的の 1. ～4. のどれに当たるかが明確であるか）
- 【想定読者】
  その運用ガイドラインの想定読者を具体的に示すことができるか
- 【課題】
  ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か
- 【他組織のガイドライン等】
  他組織が同種のガイドラインを作っていないか／作ろうとしていないか
- 【関連組織】
  どのような他組織と連携していくのがよいか

表 4-2 に検討結果をまとめる。今後、暗号プロトコルに関する運用ガイドラインを作成していく際には、表 4-2 に挙げたもののなかから優先的に取り上げていくことが望ましい。なお、「課題」には CRYPTREC が作成する運用ガイドラインの価値を高めるために考慮しなければならないポイントをまとめており、また「関連組織」には連携先として有効と期待される国内組織（国際組織の日本支部を含む）を記した。活動計画の立案に当たっては、これらのポイントを踏まえた計画であることが望まれる。

なお、表 4-2 の「目的」列、及び「プロトコル名称」列の表記についての注意は次のとおりである。

「目的」の表記

①・・・現在利用されている仕組みの中で安全ではない使われ方を排除し、安全性の底上げを図る（安全性評価を含む）
②・・・利用者が理解しやすく、かつ採用しやすいベストプラクティスを示す
③・・・普及が進んでいない安全な仕組みの普及・活用を促進させる
④・・・政府、業界団体等が守るべき（半）強制的基準として示す（そうなるような環境整備を含む）

「プロトコル名称」の表記

・「★」がついているプロトコルは暗号に直接関係がないものを指す
・具体的なプロトコル名称がわからないものについては規格やサービスの名称を示す

表 4-2　取りまとめ結果一覧

種類	No.	対象	プロトコル名称	目的	内容	想定読者	必要性	課題	他組織が発行したガイドライン等	関連組織
安全性評価（暗号技術評価委員会への参考意見）	1	ID 連携	OpenID Connect	①	OpenID Connect の安全性評価	（議論せず）	l OpenID Connect は安全性が評価されていないため、CRYPTREC で安全性評価できるとよい。	・OpenID　Connect は暗号プロトコルというよりは枠のようなもので、組み合わせで安全性は当然変わる。	（議論せず）	一般社団法人 OpenID ファウンデーション・ジャパン
	2	無線通信	LoRaWAN	①	LoRa で利用されているプロトコルの安全性評価	（議論せず）	（議論せず）	・業界団体に加入していなければ、仕様を見ることができない。	（議論せず）	（議論せず）
	3	仮想通貨	・Bitcoin プロトコル ・Ethereum ・Hyperledger Fabric ・ブロックチェーン応用（証券決済/契約）	①	ブロックチェーンの安全性評価	（議論せず）	（議論せず）	・標準化が行われている最中であるため、時期尚早。	（議論せず）	（議論せず）
実装／開発	1	自動車	【車内】 CAN，CAN FD，LIN，FlexRay 【車外】 DSRC，ETC2.0 【ハードウェア】 EVITA 【センサ】 空気圧センサ，ミリ波レーダー	②	自動車の中で利用されている暗号の実装ガイドライン（検証方法含む）	自動車ベンダ、部品サプライヤ	・今後の自動運転車などを見据えた際、セキュリティに問題が発生した場合、社会的に大きな問題となることが想定されるため。	・標準化が行われている最中である。 ・規模が大きく CRYPTREC のリソースで対応できる範囲は限られる。 ・プロトコルで挙がっているものを、より細分化し優先順位を付ける必要がある。 ・自動車ベンダの協力が必要である。 ・国内では自動車工業会（JAMA）と連携するか、二人三脚で進めないと作っても受け入れられない懸念あり。 ・自動車業界は、まず欧米の評価を参考とするため、CRYPTEC がガイドラインを作成する場合には自動車業界に受け入れてもらえるような工夫が必要である。 ・DSRC,ETC2.0 のセキュリティを管理するのは ITS-TEA であり、ガイドラインを作成する場	・SAE j3061：Cybersecurity Guidebook for Cyber-Physical Vehicle Systems ・Cybersecurity Best Practices for Modern Vehicles - NHTSA ・Automotive Cybersecurity Best Practices - Auto ISAC	・JSAE ・JasPar

								合、こことコンタクトする必要あるかもしれない。 ・SHE（Secure Hardware Extension）のように仕様が一般公開されないものに対して CRYPTREC がガイドラインを作るべきかは議論する必要がある。		
実装／開発	2	制御システム	・PLC ・SCADA ・BACKnet、OPC 等	① ②	制御システムの中で利用されている暗号プロトコルの実装ガイドラン	システム開発者、運用者	・制御系システムで利用されているソフトウエアに脆弱性が発見された場合は、生命・身体や重要インフラおよび環境へ直接影響を与える可能性があり、重要な問題となりうる。	・PLC、SCADA と挙げているがプロトコル名称ではない。プロトコルは沢山あり、安全性を挙げるために色々なガイドラインを作る必要はあるが沢山あり過ぎて、まずどれから手を付けていいかわからない。他組織との連携も考える必要がある。	・JPCERT/CC のガイドライン、参考資料	・JPCERT/CC https://www.jpcert.or.jp/ics/ ・CSSC
設定／運用	1	ユーザ管理	・RADIUS（EAP-TLS 等の利用を含む） ・PAP★ ・CHAPv2 ・IEEE802.1X	① ②	・Radius＋EAP の推奨 ・Radius＋（PAP or CHAP ｖ２）の非推奨 ・PAP、CHAP ｖ２の非推奨 ・Radius の設定	システム開発者、運用者（ユーザ管理者）、SIer、VPN を使う企業よりのベンダ	・無線 LAN 環境は利用者が多く、また、オリンピックに向けて、アクセスポイント（AP）の設置が増えていくため。 ・公衆無線 LAN 利用者が年々増加しており、3,532 万人を突破している(（株） ＩＣＴ総研調べ)。 ・VPN のユーザ認証に使われている。	・想定読者を誰にするかによって、対象とする技術が変わる。（企業向けにするのであれば RADIUS 認証を利用する） ・ユーザが「野良 AP」にアクセスしないように促すことも検討が必要。	・無線 LAN ビジネスガイドライン ・SP 800-48 Rev. 1 Guide to Securing Legacy IEEE 802.11 Wireless Networks ・SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	総務省
	2		LDAP★（kerberos）	① ②	LDAP＋Kerberos の設定	システム開発者、運用者（ユーザー管理者）、SIer	・Active Directory をはじめとしてディレクトリサービスは企業の ID 管理として利用されているが、特に標的型攻撃で侵入される糸口となるケースが昨今急増している。 ・Windows の Active Directory は広く使われている技術である。 ・組織内データのうち最も狙われやすい情報であり，内部犯行やマルウエア発動による中からの攻撃にも対処する必要がある。	・CRYPTREC で扱う内容であるのかというと疑問、そしてプロトコルの設定として変更できるものはなく、全体的に AD の安全性の設定やシステム設計思想が含まれる内容となると考えられる。 ・主に Kerberos の設定ガイドになりそうである。 ・LDAP に関わる認証方式として Kerberos 以外の実装や運用に関して調査する必要がある。 ・Windows サーバの設定も含まれる。	・Active Directory のセキュリティを保護するためのベスト プラクティス（MS） ・攻撃に対する保護のドメイン コントローラ（MS） ・PtH（Pass-the-Hash) White Papers and Data Sheet（MS） ・『LDAP 認証と Azure Multi-Factor Authentication Server』 ・『RFC2251 Lightweight Directory Access Protocol (v3)』	各種 LDAP 製品ベンダ（MS, Oracle, IBM など）

	3	ユーザ認証	・二要素認証	① ②	・パスワード管理のガイドライン（パスワード管理の一環として二要素認証を位置付ける形）	・サービサー、SIer、ID プロバイダ	・クラウドやバンキングなどで二要素認証の利用が増加しているが適切に管理できていないケースがある。・金銭や証券だけでなく，ポイント・アイテムの管理に利用されているため安全なログイン環境が必要である。	・かつて RFC 化（RFC2289）されているが MD4 ベースであり脆弱である。それ以降の OTP は RFC4226 HMAC-BasedOTP, RFC6238 Time-BasedOTP が標準化されているが利用状況は不明であり，Proprietary なシステムもあると考えられる（＝調査不能）。・OTP 自体はプロトコルではない。OTP の生成方法は本 WG の対象ではない。	・（パスワードに関するガイドラインで触れられているかもしれないが、現時点では OTP に関するガイドラインは見つけられず）・医療システムの安全管理に関するガイドライン（厚生労働省）・オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン	銀行、オンラインゲームサービス企業、SIer
	4	デバイス認証	・クライアント証明書 ・TPM を利用した認証 ・ISO/IEC9798	① ②	・クライアント証明書や TPM を使った実際のデバイス認証のガイドライン ・相互認証等の規格（ISO/IEC9798）が定めているパラメータの選定方法や利用方法の具体化、設計時の指針	・システム開発者、運用者	・IoT 機器なども含め、ネットワーク接続機器が大きく増える見込みの中、デバイスレベルでの認証は安全性確保のため極めて有効である。 ・広く利用されつつあるデバイス認証のセキュリティを強化するため。 ・利用が増えているが、適切な管理などに明るくない管理者が多い。 ・社内もしくは組込み機器等でネットワークに接続する機器が増え、IT 系と同様の対策を講じる際に、設計者、開発者の指針になる文書があるとネットワークを構築する際に参考になる。	・Proprietary なシステムが多く標準化文書はない可能性が高い. また仕様の入手が困難かもしれない。 ・幅広い技術があるので、対象を絞る必要があるか。 ・「暗号プロトコル」に整理できない技術も含まれる。	・TCG アライアンス発行の文書等 ・ISO/IEC9798	TCG アライアンス
設定／運用	5	無線通信	・WEP ・WPA ・WPA2	① ②	・WEP の非推奨 ・WPA, WPA2 の設定	・企業等での無線 LAN の管理者（企業で簡易に無線 LAN を設定する人） ・一般家庭等での無線 LAN の利用者（一般家庭等で無線 LAN 利用する人） ・IoT で Wi-Fi の利用者	・３DS が WEP しか対応されていないことなど利便性を考慮して脆弱な古いプロトコルが未だに利用されているとかんがえられる．それを排除する必要がある。 ・無線 LAN の設置が増えているため。	・想定読者を誰にするかによって、対象とする技術が変わる。（企業向けにするのであれば RADIUS 認証を利用する） ・ユーザが「野良 AP」にアクセスしないように促すことも検討が必要。 ・発言力のある人が言うレベルになっているのではないか。	・無線 LAN<危険回避> 対策のしおり ・SP 800-48 Rev. 1 Guide to Securing Legacy IEEE 802.11 Wireless Networks ・SP 800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i ・無線 LAN ビジネスガイドライン（総務省） ・一般家庭における無線 LAN のセキュリティに関する注意	総務省
	6	メール	・DKIM ・SPF★ ・DMARC★	② ③	DMARC（SPF と DKIM を含	メールサーバを構築するシ	・メール送信ドメインのなりすまし対策として必要。	・ガイドラインを書くにあたっての課題は特段ない。 ・迷惑メール対策推進協議会、お	・dkim.jp リコメンド文書 ・電子メールのセキュリティ ・標的型攻撃に対抗するための	・JIPDEC ・迷惑メール対策推進

				む）の設定/普及	ステム開発者、運用者	・SPF、DKIM、DMARC を全て合わせて使うことを普及すべき。	よび迷惑メール対策委員会と同期を取って、普及することが望ましい。	通信規格の標準化動向に関する調査結果 ・ 府省庁対策基準策定のためのガイドライン（平成 28 年度版）(NISC) ・フィッシング対策ガイドライン(フィッシング対策協議会) ・迷惑メール対策ハンドブック 2016（迷惑メール対策推進協議会） ・「有害情報対策ポータルサイトー迷惑メール対策編ー」（迷惑メール対策委員会）	協議会(事務局：デ協) ・迷惑メール対策委員会（事務局：IAJapan）
設定／運用	7	メール	S/MIME を利用したメール送信（メールへの署名）	② ③	S/MIME の設定／普及	メールサーバを構築するシステム開発者、運用者、メール送受信者	・メールのなりすまし対策として必要。 ・現在未対応の Web メールやスマホのメーラに対応を促したい。（Office365 や Gmail は一部対応済） ・なりすまし対策として S/MIME が（特に署名で）使われ始めているが、メーラごとに癖があり設定の方法がわかりにくい。 ・フィッシング対策として銀行や大手プロバイダが S/MIME を導入する傾向にある。	・ガイドラインを書くにあたっての課題は特段ない。） ・Google の新システムでは秘密鍵をクラウド上で管理するようであり、これまでこの手のガイドラインでは想定していなかった使われ方がなされることも視野に入れる必要があるかもしれない。	・SP 800-45 Version 2 Guidelines on Electronic Mail Security ・SP 800-177 Trustworthy Email ・標的型攻撃に対抗するための通信規格の標準化動向に関する調査結果 ・ 府省庁対策基準策定のためのガイドライン（平成 28 年度版）(NISC) ・フィッシング対策ガイドライン（フィッシング対策協議会） ・電子メールのセキュリティ（IPA）	・総務省 ・JIPDEC ・フィッシング対策協議会 ・IPA
	8		・パスワードつき Zip を添付したメール送信 ・S/MIME を利用したメール送信（メールの暗号化） ・オンラインストレージサービス	① ② ③	・パスワード付き zip 添付メールの排除 ・S/MIME の設定／普及 ・オンラインストレージサービスの使い方の解説	メールサーバを構築するシステム開発者、運用者、メール送受信者	・メールの秘匿性を高めるため。 ・パスワード付き zip ファイルのメール送信をやめることで、受信サイドの業務効率の向上と受信サイドのセキュリティ強化。 ・現在未対応の Web メールやスマホのメーラに対応を促したい。（Office365 や Gmail は一部対応済）	・ガイドラインを書くにあたっての課題は特段ない。 ・オンラインストレージサービスは様々あり、少々書きにくい面はある。 ・Google の新システムでは秘密鍵をクラウド上で管理するようであり、これまでこの手のガイドラインでは想定していなかった使われ方がなされることも視野に入れる必要があるかもしれない。 ・政府系向けのガイドラインでは、組織間の暗号化のように、組織のどこかで責任をもって、一旦、暗号化を外して中を見る等を考慮したガイドラインが必要となるかもしれない。	・SP 800-45 Version 2 Guidelines on Electronic Mail Security ・SP 800-177 Trustworthy Email ・ 府省庁対策基準策定のためのガイドライン（平成 28 年度版）(NISC) ・電子メールのセキュリティ（IPA）	・JIPDEC

	9	リモート接続	・SSH・RDP・telnet★	① ②	・telnet の非推奨・SSH の設定・RDP の設定	・企業等でサーバにリモート接続するシステム運用者・リモートデスクトップ接続を行うシステムを構築しているシステム管理者、運用者	・SIer のほとんどが SSH を利用しているため、SSH は必要。 ・IoT でも SSH は広く利用されるため。・IPsec や SSH のガイドラインはリファレンスとして出せれば役に立つ。 ・Web ホスティングサービスでは SSH サービスを開放しているケースもあり，想定読者はエンジニアだけではなく一般ユーザにも拡大される可能性がある。 ・パラメータが多い為、SSH サーバの設定によっては非常に危険な状態になる。特に特権ユーザのパスワードログインを可能にしている場合は注意が必要。 ・RDP は、クラウド上でも利用されていて、設定が悪いと世界中誰からも乗っ取られて利用される恐れがあるため。	・他組織との連携（例．他組織で作成済みのガイドラインを取り込む）が必要。	・SSH サーバセキュリティ設定ガイド Ver 1.0・SP 800-46 Rev. 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security	日本シーサート協議会

1.4.2　運用ガイドラインのアップデート方法に関連する検討

運用ガイドラインは、ガイドライン作成時の標準化状況や製品状況、利用環境や利用実績等を踏まえて、作成時における現実的かつ効果的な推奨設定や推奨基準を提示するものである。このことは、ある程度の時間が経過し、標準化状況や製品状況、利用環境や利用実績等が変化すれば、運用ガイドラインの中身も陳腐化し、ガイドラインとしてふさわしくないものとなることを意味する。

このため、今後運用ガイドラインの整備を進めるにあたっては、単に運用ガイドラインを作るだけでなく、運用ガイドラインの質を維持するためにどのような方法でアップデートを行っていくかを検討しておく必要がある。そこで、活用委員会では、具体的な運用ガイドラインの例として「SSL/TLS 暗号設定ガイドライン」を取り上げ、アップデートの在り方の検討を行った。

一般的なアップデートの方向性について

- 見直しの期限を設定（定期的なアップデートの実施是非）について：
  ガイドラインの内容自体のアップデート（内容をどのように改訂するか）とガイドラインのステータス管理（アップデートを実施するか否かの判断）を切り分けて考える。具体的には、ステータス管理については定期的に行うが、内容の改訂を行う期限自体はあらかじめ決めておかない。
  なお、ステータス管理ではアップデートを実施するか否かだけを決めることとし、実際の内容の改訂はアップデートすることが決まった後に実施する。

- アップデート方法について：
  毎回本体のアップデートを行うのではなく、注釈を加える程度であれば比較的負荷は掛からないため、必要に応じて注釈を後ろに付け加えていくやり方もある。例えば 2～5 年経過して、注釈が溜まってきたら大きなバージョンアップをして、内容を大幅に改訂する。
  また、緊急に対応すべき情報（補足情報）は、少なくとも運用ガイドラインと併せてインターネット上で入手できるようにすべき。本体と補足情報を合わせて同時に参照することにより対策を打つことができる。

「SSL/TLS 暗号設定ガイドライン」に関してのアップデートの方向性について

- どこまでの内容をアップデートすべきか（次回アップデートの範囲）：
  IETF では、RC4 の使用禁止、SSL3.0 の非推奨、TripleDES の非推奨等の RFC を発行しており、2015 年の「SSL/TLS 暗号設定ガイドライン」発行時とは劇的に状況が変わっている。実際、認定認証事業者が発行する証明書では SHA256 への移行が完了し、パブリック証明書もほぼ SHA256 with RSA2048 ビットになっている。また、2015 年には問題になっていたフィーチャーフォンについてもキャリアが SHA1

証明書での接続はできないと注意喚起しているはずであるため、必ずしもセキュリティ例外型が必要とは言えなくなってきている。
したがって、早期に最新動向の反映、及びセキュリティ例外型の見直しまで含めて、内容の改訂を実施すべきである。
一方、各社の製品の設定は徐々に各社で作るようになっていくべきであるため、市販製品の暗号設定状況の調査結果及び Appendix に乗っている OSS 製品等の暗号設定状況については、ガイドラインから分離すべきである。また、各社の製品の設定例を各社で整備するようにアピールをすべきである。

- セキュリティ例外型の利用を終了させる時期（EOL）の導入是非について：
  EOL を導入することで、EOL までは利用を容認すると誤解される恐れがあるため、セキュリティ例外型について EOL を導入すべきではない。また将来的には、現在の推奨セキュリティ型からセキュリティ例外型に移す必要がある設定が出てくる可能性を踏まえれば、セキュリティ例外型の枠を無くさないほうが望ましい。

1.4.3　外部連携について

運用ガイドラインの作成については、CRYPTREC 単独で作成するよりも関連する外部組織や業界団体等（以降、他組織等という）との連携を進めたほうがよいとの指摘があった。例えば、以下のような指摘である。

- 暗号プロトコル課題検討 WG の検討結果では、必要性が高いと認められた暗号プロトコルはいずれも、外部組織や業界団体との連携するほうが、効果が高い運用ガイドラインが作れると考えられる
- 重点課題検討 TF での議論の中では、従来は民間が必要としていた情報と電子政府を作るうえで必要となる情報の方向性がほぼ一致していたが、現在はそうでないという指摘があった
- ベンダや業界団体等の意向をバランスよく取り入れつつ、セキュリティも担保することが効果的なガイドラインとして評価される

これらの指摘を踏まえ、来年度より開始する運用ガイドラインの作成にあたっては、従来の WG 形式での作成に捕らわれずに柔軟な作成スタイルを考慮する。具体的には、運用ガイドラインの作成手段を次の 4 種類とし（図 1 参照)、作成するガイドラインのテーマによって、暗号技術活用委員会にて適切な作成手段を決定する。

1) CRYPTREC が単独で作成（2 種類）
CRYPTREC が他組織等と連携なしに単独で作成する。ただし、具体的な作成手段としては、従来の WG 形式のほか、スキルのある他組織等にアウトソーシングしてベース

となる素案を作成してもらい活用委員会で内容を確認・承認する形式も含める。

2) 他組織等と共同で作成

他組織等と共同で作成したものを活用委員会で確認・承認する形式である。

3) 他組織等で実施したものをベースに作成

他組織等がすでに作成したものをベースに委員会で確認し、適切なものであれば承認する形式。その際、他組織がすでに作成したものを参照したうえで、必要最小限の追記等を行う可能性がある。

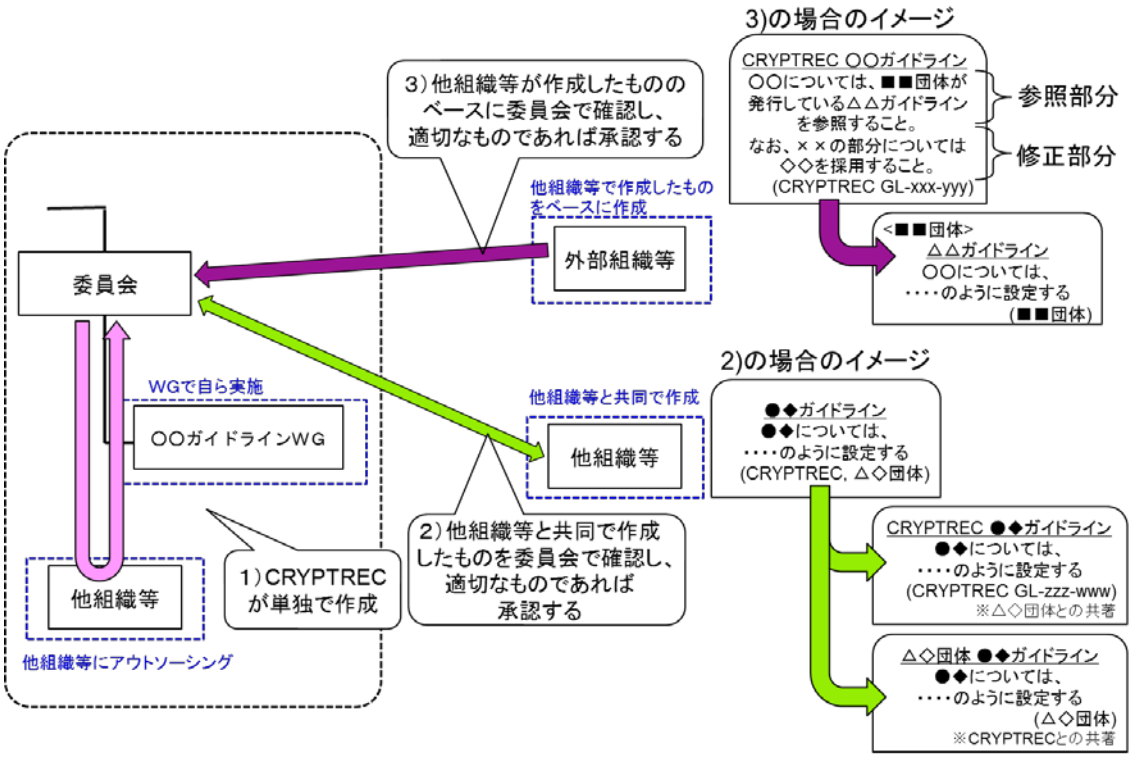


図１　作成手段の説明図

実際の運用ガイドラインの作成手段を決定するにあたっては、以下のポイントを重視して判断を行う。

- 他組織等と連携するほうが有用性のある運用ガイドラインが作成できるか
- 連携先の外部組織等が信頼できる組織・団体であるか
- 他組織等と連携することによって作業効率を上げることができるか（例えば作業スケジュール等）
- 予算面やリソース面からの考慮

2. 今後に向けて

2017 年度は新たな運用ガイドラインを実際に作成していく方向で活動計画を検討する。具体的な対象の選定等については、2017 年度第一回暗号技術活用委員会にて決定する方向である。

また、SSL/TLS 暗号設定ガイドラインについては、2016 年度活動で出た意見を踏まえ、2017 年度にアップデートを行う計画とする予定である。

資料５

SHAKE128 の推奨候補暗号リストへの追加について（審議）

[審議事項]

2015 年度の審議により、ハッシュ関数 SHA-2, SHA-3 が CRYPTREC 暗号リストへ追加されたが、ハッシュ関数 SHA-3 ファミリーの 1 つである SHAKE128 は現在含まれていない。SHAKE128 について、2016 年度第 2 回暗号技術評価委員会での審議の結果、出力長を 256 ビット以上とすれば CRYPTREC 暗号リストへ追加するのに十分な安全性および実装性能を有していることが承認された。これにより、SHAKE128 を推奨候補暗号リストに追加してよいか審議いただきたい。

なお、推奨候補暗号リストへの追加条件は、その暗号技術が十分な安全性および実装性能を有していることとしている。また、SHAKE128 のリスト追加時には、現在の SHAKE256 に対する脚注と同じ「ハッシュ長は 256 ビット以上とすること」という脚注をつける。

[参考：暗号技術評価委員会で承認された SHAKE128 の安全性評価と実装評価]

◆ 安全性評価

SHAKE128 を含む SHA-3 について、下記有識者に外部評価を依頼し、評価レポートを得ている。

- Donghoon Chang 氏（Indraprastha Institute of Information Technology, India）
  2014 年度 技術報告書 「Security Evaluation Report on SHA-224, SHA-512/224, SHA-512/256, and the six SHA-3 Functions」
  http://www.cryptrec.go.jp/estimation/techrep_id2403_2.pdf
- Itai Dinur 氏（École Normale Supérieure, France）
  2014 年度 技術報告書 「Security Evaluation of SHA-3」
  http://www.cryptrec.go.jp/estimation/techrep_id2402.pdf

評価結果：表 1 で示す安全性に対して安全性に十分なマージンがあり、現実的な脅威の観点から大きな問題点は見つかっていない。

表 1：SHA-3 のセキュリティ強度

Algorithm	出力長 (bit)	セキュリティ強度 (bit)		
		Collision	Preimage	2nd preimage
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128	d	min(d/2,128)	≧min(d,128)	min(d,128)
SHAKE256	d	min(d/2,256)	≧min(d,256)	min(d,256)

事務局注：現在の電子政府推奨暗号リスト（平成 25 年 3 月 1 日）を選定する際に採用した評価方針として、「ハッシュ関数については、ハッシュ長が 256 ビット以上であることが望ましい」としていた（CRYPTREC Report 2012 暗号方式委員会報告 表 3.17 参照）。SHAKE128 は SHAKE256 と同様、FIPS PUB 202 で規定された eXtendable-Output Function(XOF)という任意の出力長をとりうる関数である。SHAKE128 は、出力長 d を 256 ビット以上とすれば、Collision resistance 128 ビット、Preimage resistance 128 ビット、2nd preimage resistance 128 ビットの安全性を有し、CRYPTREC 暗号リスト追加に十分な安全性を有していると考えられる。CRYPTREC 暗号リスト追加の際は、SHAKE256 と同様に「ハッシュ長は 256 ビット以上とすること」という脚注をつける。

◆ 実装評価

SHAKE128 を含む SHA-3 について、下記有識者に外部評価を依頼し、評価レポートを得ている。

- これまでに行われてきた実装性能評価に関する研究結果のサーベイ
  依頼先：﨑山 一男 教授 （電気通信大学）
  2013 年度 技術報告書 「ハッシュ関数 SHA-224, SHA-512/224, SHA-512/256 及び SHA-3 (Keccak) に関する実装評価」
  http://www.cryptrec.go.jp/estimation/techrep_id2301.pdf
- FPGA 上での性能評価
  依頼先：佐藤 証 教授 （電気通信大学）
  2013 年度 第三回暗号技術評価委員会 資料 2-3 「ハッシュ関数のハードウェア実装およびその性能測定」

評価結果：ソフトウェア実装、ハードウェア実装ともに十分な実装性能を有する。

資料６

ChaCha20-Poly1305 の
CRYPTREC 暗号リストへの追加を視野に入れた評価について

[審議依頼]

ChaCha20-Poly1305 は、ユーザ数の多いブラウザに採用されるなど、実導入が進んでいるアルゴリズムである。第 1 回暗号技術評価委員会(2016 年 7 月 27 日)および、2015 年度第 3 回重点課題検討タスクフォース(2016 年 2 月 3 日)で、その安全性評価に対する要望が複数あったことから、暗号技術評価委員会にて安全性評価を行っている。

(審議事項)

ChaCha20-Poly1305 について、CRYPTREC 暗号リストへの追加を視野に入れ、引き続き安全性評価・実装性能評価を行ってよいかについて、ご審議いただきたい。

[承認依頼]

2009 年にリスト改定に伴う公募を行った際は、応募暗号アルゴリズムが評価対象となるための必要条件として、査読付き国際会議に採録されていることを課していた(電子政府推奨暗号リスト改訂のための暗号技術公募要項(2009 年度))[1]。一方、「国際標準化等の実績がある」ことを理由に事務局選出のアルゴリズムとして評価対象とした例もあった[2]。

(承認事項)

「国際標準化等の実績がある」ことを根拠として事務局で選出する暗号アルゴリズムに対して CRYPTREC 暗号リストへの追加を視野に入れた評価を開始する場合には、暗号技術検討会で判断を行い、これを受けて暗号技術評価委員会で安全性評価・実装性能評価を行うことする。

---

[1] http://www.cryptrec.go.jp/topics/cryptrec_20090527_application_guide.html
http://www.cryptrec.go.jp/topics/cryptrec_20091001_application_guide_2009-2.pdf

[2] CRYPTREC Report 2011 暗号方式委員会報告(2.3.5 事務局選出暗号技術)

ChaCha20-Poly1305 の安全性評価について(報告)

ChaCha20-Poly1305 は、ユーザ数の多いブラウザに採用されるなど、実導入が進んでいる認証暗号方式である。第 1 回暗号技術評価委員会(2016 年 7 月 27 日)および、2015 年度第 3 回重点課題検討タスクフォース(2016 年 2 月 3 日)で、その安全性評価に対する要望が複数あったことから、下記のとおり外部評価を実施したので報告する。なお、外部評価レポートは、CRYPTREC ホームページにて公開を予定している。

・外部評価依頼先

清本晋作 氏 (KDDI 総合研究所、日本)

・外部評価レポートタイトル

“Security Analysis of ChaCha20-Poly-1305 AEAD”

[評価者の見解]

認証暗号 ChaCha20-Poly1305 に対する安全性評価を行った。ChaCha20-Poly1305 は、暗号化のためにストリーム暗号 ChaCha 20 が使われ、認証のために メッセージ認証コード(MAC) Poly1305 が使われている。認証暗号としての安全性に関しては、ChaCha20 が擬似乱数生成器と見なすことができ、かつ、 Poly1305 が安全なユニバーサルハッシュ関数であれば、ChaCha20-Poly1305 は、認証暗号としての安全性を満たすことが証明されている[Pro14]。

Poly1305 については、 ε-almost-Δ-universal であることが証明でき、安全なユニバーサルハッシュ関数であることが示されている[Ber05b]。

本レポートでは、特に ChaCha20 の安全性に注力し、ストリーム暗号に対して提案されている各種攻撃に対する評価を実施した。タイムメモリデータトレードオフ攻撃に対しては、現実的な設定の下では攻撃に要する計算量が膨大になるといえる。サイドチャネル攻撃に対しては、既存の対策手法により防ぐことが可能である。その他の既知の攻撃に対しては、鍵の総当たりよりも効率的なものは見つかっていない。以上から、 ChaCha20 については、擬似乱数生成器と見なすことができると考えられる。

以上の結果から、認証暗号 ChaCha20-Poly1305 に対する攻撃は発見されていないと結論付ける。

(参考文献)

[Pro14] Gordon Procter. A Security Analysis of the Composition of ChaCha20 and Poly1305, Cryptology ePrint Archive: Report 2014/613, 2014.

(https://eprint.iacr.org/2014/613).

[Ber05b] Daniel Julius Bernstein. The Poly1305-AES message authentication code, FSE 2005, LNCS, volume 3557, pages 32–49, 2005.

[暗号技術評価委員会の判断(案)]

評価者からのレポートを踏まえ、現時点では ChaCha20-Poly1305 は、認証暗号として、具体的な脅威は見つかっていないと考えられる。

[今後の予定]

暗号技術検討会にて、ChaCha20-Poly1305 について CRYPTREC 暗号リストへの追加を視野に入れ、引き続き評価を行っていくかどうか審議頂く。承認頂けた場合、安全性に加え、実装性能についても調査・評価を行っていく。

3 月 30 日に予定されている暗号技術検討会にて下記について、審議・承認頂く。

○ ChaCha20-Poly1305 について、 CRYPTREC 暗号リストへの追加を視野に入れ、引き続き安全性評価・実装性能評価を行ってよいか。

○ CRYPTREC 暗号リストへの追加に関して、事務局で選出する暗号アルゴリズムについて、「国際標準化等の実績がある」かどうかの判断は、検討会で審議を行う。

資料7

KCipher-2 の仕様書について

1. これまでの経緯

2016 月 12 月に IPA(JCMVP)から、KCipher-2 の仕様書(以下、旧仕様書という)において、シフトレジスタの定義式と図の間に不整合があるという報告が CRYPTREC 事務局宛てにあった。

2017 年 1 月に CRYPTREC 事務局から応募者の KDDI に問い合わせたところ、その指摘通り、シフトレジスタの定義式に誤植があり、定義式を図と整合するものに修正した仕様書(以下、新仕様書という)に差し替えをしたいとの回答があった（資料 7 別添 2)。

2. 暗号技術評価委員会における対応

旧仕様書におけるシフトレジスタの定義式を修正することは、編集上は軽微と判断できるが、誤植を修正したことで、旧仕様書に対して行った安全性評価の結果に影響が及ばないか懸念される。

定義式に基づいた評価をおこなったか、図に基づいた評価をおこなったかの確認が必要であった。

3. 審議事項

暗号技術評価委員会では、資料 7 別添 1 の通り、旧仕様書に基づく安全性評価を依頼した評価者らにどちらに基づいて評価をおこなったのかの確認し、回答がともに図に基づいた評価であったので、旧仕様書から新仕様書への差し替えを認める判断を行った。

暗号技術評価委員会での判断の通り、差し替えを認めてもよいかご審議を頂きたい。

以上

資料７　参考資料１

第２回暗号技術評価委員会　資料６－１

KCipher-2 の仕様書の変更について(審議)

1. これまでの経緯

2016 月 12 月に IPA(JCMVP)から、KCipher-2 の仕様書において、シフトレジスタの定義式と図の間に不整合があるという報告が CRYPTREC 事務局宛てにあった（資料 6-2)。2017 年 1 月に CRYPTREC 事務局から応募者の KDDI に問い合わせたところ、2017 年 2 月に IPA の指摘通り仕様書の誤記があるとの回答があった（資料 6-3)。

資料 6-3 は、シフトレジスタの定義式の添え字に誤植があり（表 1)、シフトレジスタの値を 1 つ隣へシフトしていないので、修正したいというものであった。2009 年度応募書類における参照ソースコードでは、シフトレジスタの値は図の通りにシフトされていた。2009 年度応募書類におけるテストベクトルは、ISO/IEC 18033-4:2011 及び IETF RFC 7008 のそれと一致していることを CRYPTREC 事務局でも確認した。(定義式は国際標準と整合性がなく，図は整合性を有する.)

表１：仕様書（日本語版）の修正箇所(資料 6-3 から抜粋)

7 頁 4 行目	$A_{t+i+1} = \begin{cases} A_{t+i+1} & (i = 0,1,2,3) \\ A_{t+3} \oplus \alpha_0 A_t & (i = 4) \end{cases}$
7 頁 6 行目	$B_{t+i+1} = \begin{cases} B_{t+i+1} & (i = 0,1,\ldots,9) \\ (\alpha_1^{cl1_t} + \alpha_2^{1-cl1_t} - 1)B_t \oplus B_{t+1} \oplus B_{t+6} \oplus \alpha_3^{cl2_t} B_{t+8} & (i = 10) \end{cases}$
8 頁 28 行目	$A_{j+i} = \begin{cases} A_{j+i-1} & (i = 0,1,2,3) \\ \alpha_0 A_{j-1} \oplus A_{j+2} \oplus z_{j-1}^L & (i = 4) \end{cases}$
8 頁 30 行目	$B_{j+i} = \begin{cases} B_{j+i-1} & (i = 0,1,\ldots,9) \\ (\alpha_1^{cl1_{j-1}} + \alpha_2^{1-cl1_{j-1}} - 1)B_{j-1} \oplus B_j \oplus B_{j+5} \oplus \alpha_3^{cl2_{j-1}} B_{j+7} \oplus z_{j-1}^H & (i = 10) \end{cases}$

シフトレジスタにおいて、レジスタの値を１つ隣へシフトするように定義式の添え字を正しく修正することは、編集上は軽微と判断できるが、誤植を修正したことで、旧仕様書に対して行った安全性評価の結果に影響が及ばないか懸念される。

2. 旧仕様書に基づく評価の経緯と今回の対応方針

旧仕様書の編集上の変更は軽微であるが、変更が安全性評価結果に影響を与えていないことの確認が必要である。

対応方針：旧仕様書に基づく安全性評価を依頼した下記の 2 名の外部評価者らに、定義式に基づいた評価をおこなったか，図に基づいた評価をおこなったかを確認した.

①　白石善明、KCipher-2 の安全性に関する評価、ID 2009、

http://www.cryptrec.go.jp/estimation/techrep_id2009.pdf

② Bart Preneel ら、Security Evaluation of the K2 Stream Cipher (2011 年 3 月 29 日更新)、ID 2010、
http://www.cryptrec.go.jp/estimation/techrep_id2010_2.pdf

現在のところ、Preneel 氏からは口頭で図に基づいて評価したとの回答を頂いた（すなわち，安全性に問題はない)。また、白石先生からも、影響は無いとの回答をメールで頂いた。

3. 審議事項

上記の対応の結果、旧仕様書に基づく安全性評価を過去に実施した外部評価者らからの回答がともに「安全性に影響なし」であったので、旧仕様書の修正を認めることとしたい。

（参考情報）

⑤ 電子政府推奨暗号の仕様書に瑕疵(誤字、脱字)あるいは実装上の解釈が不明瞭な箇所があり、当該暗号に関する修正情報が仕様書の管理者により提案された場合であって、監視委員会が当該暗号に関する修正情報を当該暗号の仕様変更に当たらないと判断する場合には当該修正情報を周知する。　(暗号技術検討会 2007 年度報告書 p.38 より抜粋)

以上

資料7参考資料2

KCipher-2 の暗号技術仕様書（日本語版・ 英語版）の誤記について

株式会社 KDDI 総合研究所

2017 年 2 月 16 日

1　提出物の正誤

表 1 に，提出書類全体の正誤を示す．暗号技術仕様書（日本語版・ 英語版）のみに誤記が含まれている．

2　暗号技術仕様書（日本語版・ 英語版）の誤記

KCipher-2 の鍵系列出力処理及び初期化処理において，線型フィードバックシフトレジスタ（LFSR : Linear Feedback Shift Register） FSR-A 及び FSR-B のシフト処理を定義するための式のみが誤りを含んでいる．

暗号技術仕様書（日本語版・ 英語版）において, 上記の式以外には，誤りがないことを確認ずみである．暗号技術仕様書（日本語版・ 英語版）の原始多項式又は構成図を参照することにより，FSR-A 及び FSR-B のシフト処理及び KCipher-2 を正しく理解できる．また，参照コード, 参照ハードウェア設計記述, およびテス

表 1　提出書類の正誤表（「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度）」より一部抜粋）

項番	提出書類	正誤
6.1	暗号技術応募書（日本語版・ 英語版）	正
6.2	暗号技術仕様書（日本語版・ 英語版）	誤
6.3	自己評価書（日本語版・ 英語版）	正
6.4	テストベクトル	正
6.5	参照ソースコード	正
	参照ソースコード仕様書（日本語版・ 英語版）	正
	参照ハードウェア設計記述	正
	参照ハードウェア設計記述仕様書（日本語版・ 英語版）	正
	テストベクトル生成ソースコード	正
	テストベクトル生成ソースコード仕様書（日本語版・英語版）	正
6.6	誓約書	正
6.7	公開の状況等に関する情報	正
6.8	応募暗号説明会発表資料（日本語版・ 英語版）	正
6.9	自己チェックリスト	正

トベクトルを利用することで，KCipher-2 を正しく実装できる．

さらに，KCipher-2 の学術論文, ISO/IEC 18033-4 Ed.2, IETF RFC 7008 など，外部の文書を参照しても正しい仕様を参照することが可能である．

3　修正箇所

暗号技術仕様書（日本語版・ 英語版）の修正箇所を示す．

3.1　暗号技術仕様書（日本語版）「ストリーム暗号 KCipher-2」

- 7 ページ，4 行目

修正前

$$A_{t+i+1} = \begin{cases} A_{t+i} & (i = 0, 1, 2, 3) \\ A_{t+3} \oplus \alpha_0 A_t & (i = 4) \end{cases}$$

修正後

$$A_{t+i+1} = \begin{cases} A_{t+i+1} & (i = 0, 1, 2, 3) \\ A_{t+3} \oplus \alpha_0 A_t & (i = 4) \end{cases}$$

- 7 ページ，6 行目

修正前

$$B_{t+i+1} = \begin{cases} B_{t+i} & (i = 0, 1, \ldots, 9) \\ (\alpha_1^{cl1_t} + \alpha_2^{1-cl1_t} - 1)B_t \oplus B_{t+1} \oplus B_{t+6} \oplus \alpha_3^{cl2_t} B_{t+8} & (i = 10) \end{cases}$$

修正後

$$B_{t+i+1} = \begin{cases} B_{t+i+1} & (i = 0, 1, \ldots, 9) \\ (\alpha_1^{cl1_t} + \alpha_2^{1-cl1_t} - 1)B_t \oplus B_{t+1} \oplus B_{t+6} \oplus \alpha_3^{cl2_t} B_{t+8} & (i = 10) \end{cases}$$

- 8 ページ，28 行目

修正前

$$A_{j+i} = \begin{cases} A_{j+i-1} & (i = 0, 1, 2, 3) \\ \alpha_0 A_{j-1} \oplus A_{j+2} \oplus z_{j-1}^L & (i = 4) \end{cases}$$

修正後

$$A_{j+i} = \begin{cases} A_{j+i-1} & (i = 0, 1, 2, 3) \\ \alpha_0 A_{j-1} \oplus A_{j+2} \oplus z_{j-1}^L & (i = 4) \end{cases}$$

- 8 ページ，30 行目

修正前

$$B_{j+i} = \begin{cases} B_{j+i-1} & (i = 0, 1, \ldots, 9) \\ (\alpha_1^{cl1_{j-1}} + \alpha_2^{1-cl1_{j-1}} - 1)B_{j-1} \oplus B_j \oplus B_{j+5} \oplus \alpha_3^{cl2_{j-1}} B_{j+7} \oplus z_{j-1}^H & (i = 10) \end{cases}$$

修正後

$$B_{j+i} = \begin{cases} B_{j+i-1} & (i = 0, 1, \ldots, 9) \\ (\alpha_1^{cl1_{j-1}} + \alpha_2^{1-cl1_{j-1}} - 1)B_{j-1} \oplus B_j \oplus B_{j+5} \oplus \alpha_3^{cl2_{j-1}} B_{j+7} \oplus z_{j-1}^H & (i = 10) \end{cases}$$

3.2　暗号技術仕様書（英語版）「Stream Cipher KCipher-2」

- 7 ページ，4 行目

修正前

$$A_{t+i+1} = \begin{cases} A_{t+i} & (i = 0, 1, 2, 3) \\ A_{t+3} \oplus \alpha_0 A_t & (i = 4) \end{cases}$$

修正後

$$A_{t+i+1} = \begin{cases} A_{t+i+1} & (i = 0, 1, 2, 3) \\ A_{t+3} \oplus \alpha_0 A_t & (i = 4) \end{cases}$$

- 7 ページ，6 行目

修正前

$$B_{t+i+1} = \begin{cases} B_{t+i} & (i = 0, 1, \ldots, 9) \\ (\alpha_1^{cl1_t} + \alpha_2^{1-cl1_t} - 1)B_t \oplus B_{t+1} \oplus B_{t+6} \oplus \alpha_3^{cl2_t} B_{t+8} & (i = 10) \end{cases}$$

修正後

$$B_{t+i+1} = \begin{cases} B_{t+i+1} & (i = 0, 1, \ldots, 9) \\ (\alpha_1^{cl1_t} + \alpha_2^{1-cl1_t} - 1)B_t \oplus B_{t+1} \oplus B_{t+6} \oplus \alpha_3^{cl2_t} B_{t+8} & (i = 10) \end{cases}$$

- 8 ページ，22 行目

修正前

$$A_{j+i} = \begin{cases} A_{j+i-1} & (i = 0, 1, 2, 3) \\ \alpha_0 A_{j-1} \oplus A_{j+2} \oplus z_{j-1}^L & (i = 4) \end{cases}$$

修正後

$$A_{j+i} = \begin{cases} A_{j+i-1} & (i = 0, 1, 2, 3) \\ \alpha_0 A_{j-1} \oplus A_{j+2} \oplus z_{j-1}^L & (i = 4) \end{cases}$$

- 8 ページ，24 行目

修正前

$$B_{j+i} = \begin{cases} B_{j+i-1} & (i = 0, 1, \ldots, 9) \\ (\alpha_1^{cl1_{j-1}} + \alpha_2^{1-cl1_{j-1}} - 1)B_{j-1} \oplus B_j \oplus B_{j+5} \oplus \alpha_3^{cl2_{j-1}} B_{j+7} \oplus z_{j-1}^H & (i = 10) \end{cases}$$

修正後

$$B_{j+i} = \begin{cases} B_{j+i-1} & (i = 0, 1, \ldots, 9) \\ (\alpha_1^{cl1_{j-1}} + \alpha_2^{1-cl1_{j-1}} - 1)B_{j-1} \oplus B_j \oplus B_{j+5} \oplus \alpha_3^{cl2_{j-1}} B_{j+7} \oplus z_{j-1}^H & (i = 10) \end{cases}$$

4　仕様の修正よる KCipher-2 の挙動の差異

修正前の仕様で定義される KCipher-2 は，鍵系列出力処理及び初期化処理の双方において，FSR-A 及び FSR-B の値が変化しない．これは, 一般的なフィードバックシフトレジスタでは, 起こりえない挙動である. このため，一般的なフィードバックシフトレジスタの挙動から，仕様が誤植を含んでいることを容易に推測できる．また，暗号技術仕様書（日本語版・ 英語版）における原始多項式・構成図，参照ソースコード，参照

ハードウェア設計記述及びテストベクトル等の記載と矛盾が生じることからも, 誤植であると判断可能である. さらに, KCipher-2 の仕様を記述した他の外部文書との比較からも, 誤植であることが容易に判別できる.

一方で，修正後の仕様で定義される KCipher-2 は，鍵系列出力処理及び初期化処理において，FSR-A 及び FSR-B の値は時刻ごとに 1 つずつシフトする．すなわち，一般的なフィードバックシフトレジスタの挙動と一致する．また，暗号技術仕様書（日本語版・ 英語版）における原始多項式・構成図，参照ソースコード，参照ハードウェア設計記述及びテストベクトル等の記載と整合する．

5　自己安全性評価の正当性

自己評価書（日本語版・ 英語版）及び Institute for Infocomm Research (I2R) による第三者評価レポートは，修正後の仕様により定義される正しい KCipher-2 の挙動に基づき安全性評価を実施している．このため，今回の仕様の修正は，自己安全性評価の結果に影響を与えない．

5.1　自己評価書（日本語版・ 英語版）

正しい KCipher-2 の挙動に基づいて安全性評価を行っている. 表 1（日本語版 5 ページ）及び Table 1（英語版 5 ページ）において，FSR-A 及び FSR-B の値が，時刻に応じて変化する様子を示しており，修正後の仕様により定義される KCipher-2 の挙動と一致している．

5.2　第三者評価レポート

1.2 節（2 ページ）において，FSR-A 及び FSR-B の挙動を，原始多項式を用いて正しく記述しており，修正後の仕様により定義される KCipher-2 の挙動と一致している．また，誤記に基づき FSR-A 及び FSR-B の値が変化しないことに起因する安全性評価等の記述はない．

6　第三者安全性評価の正当性

2 つの第三者安全性評価は，修正後の仕様により定義される正しい KCipher-2 の挙動に基づいていると考えられる．このため，今回の仕様の修正は，第三者安全性評価の結果に影響を与えない．

6.1　KCipher-2 の安全性に関する評価（名古屋工業大学）

報告書中の以下の記述は，修正後の仕様により定義される KCipher-2 の挙動と一致している．

- 2.1 節（3–5 ページ）において，FSR-A 及び FSR-B の挙動を、原始多項式を用いて正しく記述している．
- 2.2 節（6 ページ）に，「24 サイクル動かして，内部状態を更新する.」との記述がある．
- 3.1.1 節（7 ページ）に，FSR-B の出力の変化を遷移行列 M_i を用いて記述している．
- 3.1.3 節（9 ページ）に，FSR-A の出力の周期が $2^{160} - 1$ であることが記載されている．

また，誤記に基づき FSR-A 及び FSR-B の値が変化しないことを指摘し, それに起因する安全性評価は実施していない．

6.2 Security Evaluation of the K2 Stream Cipher (Katholieke Universiteit Leuven)

報告書中の以下の記述は，修正後の仕様により定義される KCipher-2 の挙動と一致している．

- Table 7, 8, 9, 10, 11 及び 12（22–24 ページ）において、 FSR-A 及び FSR-B の値が時刻ごとに 1 つずつシフトする様子を示している．
- Figure 1（4 ページ）では，FSR-A 及び FSR-B の値がシフトすることを矢印により示している．Figure 4（16 ページ）においても，構造を簡略化した KCipher-2 の FSR-A 及び FSR-B の値がシフトすることを矢印により示している．
- 7 節（28–29 ページ）において，動的フィードバック制御を変化させた場合における FSR-B の出力の周期の検証を行っており，14 以下の周期が存在しないことを示している．

また，誤記に基づき FSR-A 及び FSR-B の値が変化しないことを指摘し, それに起因する安全性評価は実施していない．

資料８

SHA-1 に関する速報掲載について（報告）

下記の通り、2017 年 3 月 1 日付けで、CRYPTREC 統一 Web ページにて SHA-1 の安全性低下に関する速報[1]を公開したので、報告する。なお、2015 年 12 月 18 日にも SHA-1 の安全性について注意喚起[2]を行った。

SHA-1の安全性低下について

平成29年3月1日
CRYPTREC暗号技術評価委員会

2017年2月23日に、CWI AmsterdamとGoogle Researchの共同研究チームが、ハッシュ関数SHA-1の衝突発見に初めて成功したと発表しました[1]。ハッシュ関数とは、入力データに対して固定長のハッシュ値を出力するアルゴリズムで、電子署名等多くの用途で利用されています。ハッシュ関数の衝突を発見するということは、同じハッシュ値を出力する複数の異なる入力データを見つけるということで、安全なハッシュ関数に対しては現実的な計算量では衝突が見つけられないようになっています。今回の発表では、全数探索の計算量(2^{80})よりも10万倍速い$2^{63.1}$回のSHA-1の計算量で衝突を発見したと報告されています。これはCPU 6500年分とGPU 100年分を合わせた計算量に相当するとのことです。ハッシュ関数の衝突が見つけられるようになると、電子署名の偽造が可能となるなどの脅威が考えられます。

これまでCRYPTRECでは、SHA-1の安全性低下について継続的に監視、評価、報告を行ってきました[2] [3]。現在、CRYPTRECでは、SHA-1を「CRYPTREC暗号リスト」の「運用監視暗号リスト」[4]に掲載し、互換性維持以外の目的での利用を推奨していません。また、情報セキュリティ政策会議からも2008年に移行指針[5]が発表されています。このようにSHA-1の安全性低下が進んでいることから、SHA-256等*のより安全なハッシュ関数への移行を推奨いたします。

CRYPTREC では、今後も引続き状況の監視・調査を行い、CRYPTREC Webサイトなどを通じてお知らせしてまいります。ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。

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

【参考文献】
[1] https://shattered.io/
https://shattered.io/static/shattered.pdf
[2] CRYPTREC Report 2005 「暗号技術監視委員会報告」
http://www.cryptrec.go.jp/report/c05_wat_final.pdf
[3] SHA-1の安全性について (平成27年12月)
http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html
[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) (2013年3月1日 総務省・経済産業省、平成28年3月29日改定)：
http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf
[5] 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」(平成20年4月22日 情報セキュリティ政策会議決定、平成24年10月26日 情報セキュリティ対策推進会議改定) :
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf

【脚注】（平成29年3月6日追加）
*「電子政府推奨暗号リスト」または「推奨候補暗号リスト」に掲載されている、安全性が確認されたハッシュ関数

[1] http://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html
[2] http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html

資料９

共通鍵暗号の安全性調査と MISTY1 について

1. 背景と目的

2015 年度に共通鍵暗号 MISTY1 のフルラウンドへの攻撃が発表されたことを受け、現在、CRYPTREC では共通鍵暗号の将来の安全性の判断基準について指針を有していないこと、また、共通鍵暗号の専門家が学術論文等で記載している解読計算量の表現は非専門家にとっては分かりづらいという指摘があったことなどから、今年度、暗号技術評価委員会にて、外部の共通鍵暗号の専門家グループに下記の調査を依頼した。

2. 調査内容(共通鍵暗号の安全性調査)

① 現在使われている代表的な共通鍵暗号少なくとも３方式に対する攻撃法の発展（暗号解読に必要な計算量・データ量・メモリ量等の低下）の調査

② 解読手法の進展や計算機能力の向上を勘案した共通鍵暗号の今後の危殆化に関する考察

3. 調査依頼先

森井昌克*, 五十部孝典*, 藤堂洋介*, 船引悠生*†, 小家 武*†

*神戸大学, †(株)クリプト

4. 調査結果

① AES, Camellia, MISTY1 に対する各攻撃法の発展

図1～図3 にAES, Camellia, MISTY1のこれまでの安全性評価結果を攻撃技術進化マップとして示す。横軸は攻撃の発表年、縦軸はフルラウンドに対する攻撃成功段数を示し、攻撃成功段数/フル段数の割合で表している。100% はフル段数の攻撃を意味する。また、攻撃進化を鍵長ごとに示しており、赤, 青, 緑がそれぞれ128, 192, 256 ビット鍵を示す。また、攻撃ごとに色分けをしており、ピンク色がIntegral 攻撃、青色が不能差分攻撃、黄色が中間一致攻撃、白色が無相関線形攻撃、灰色が切詰差分攻撃である。

図 1　AES の攻撃技術進化マップ

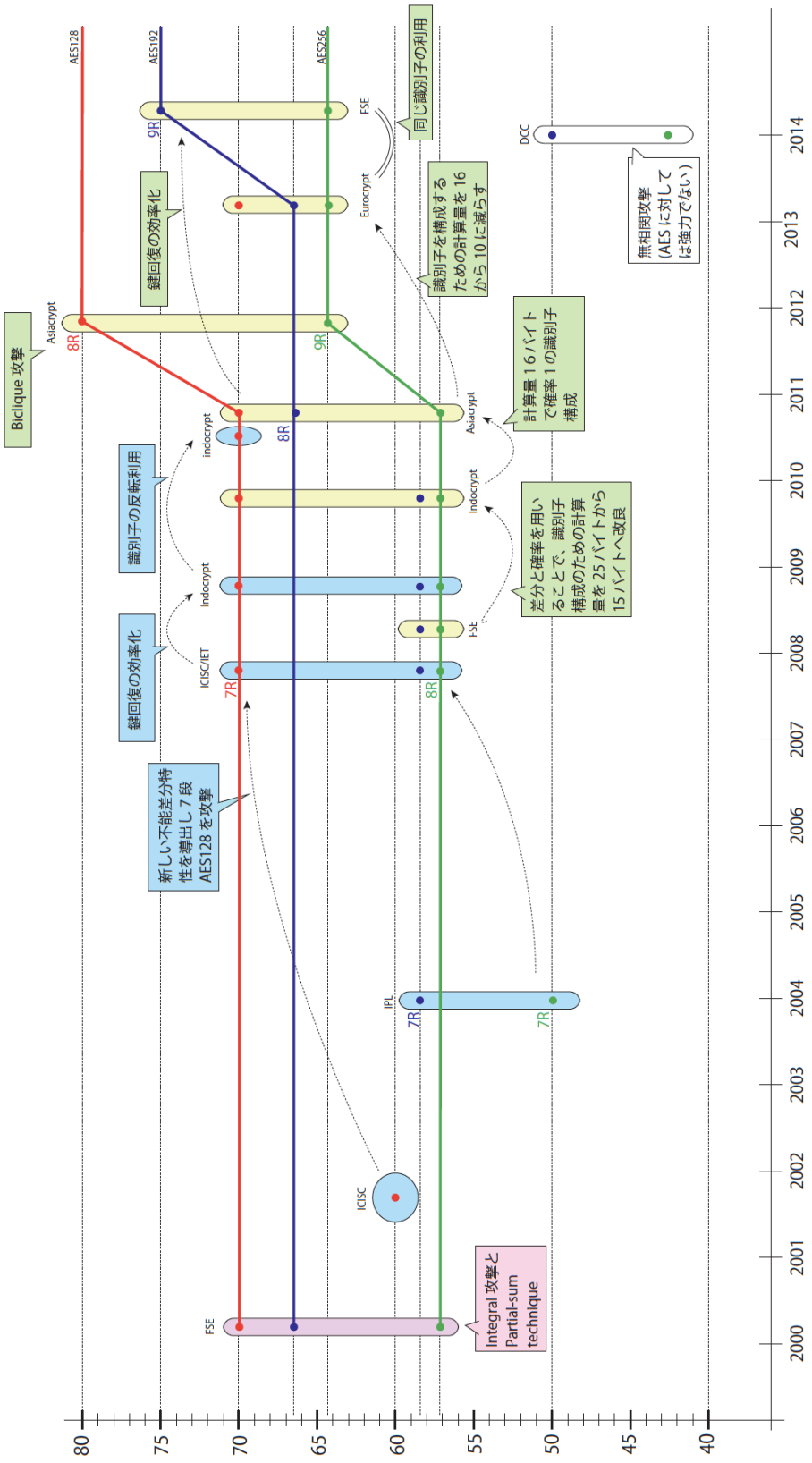


図 2　Camellia の攻撃技術進化マップ

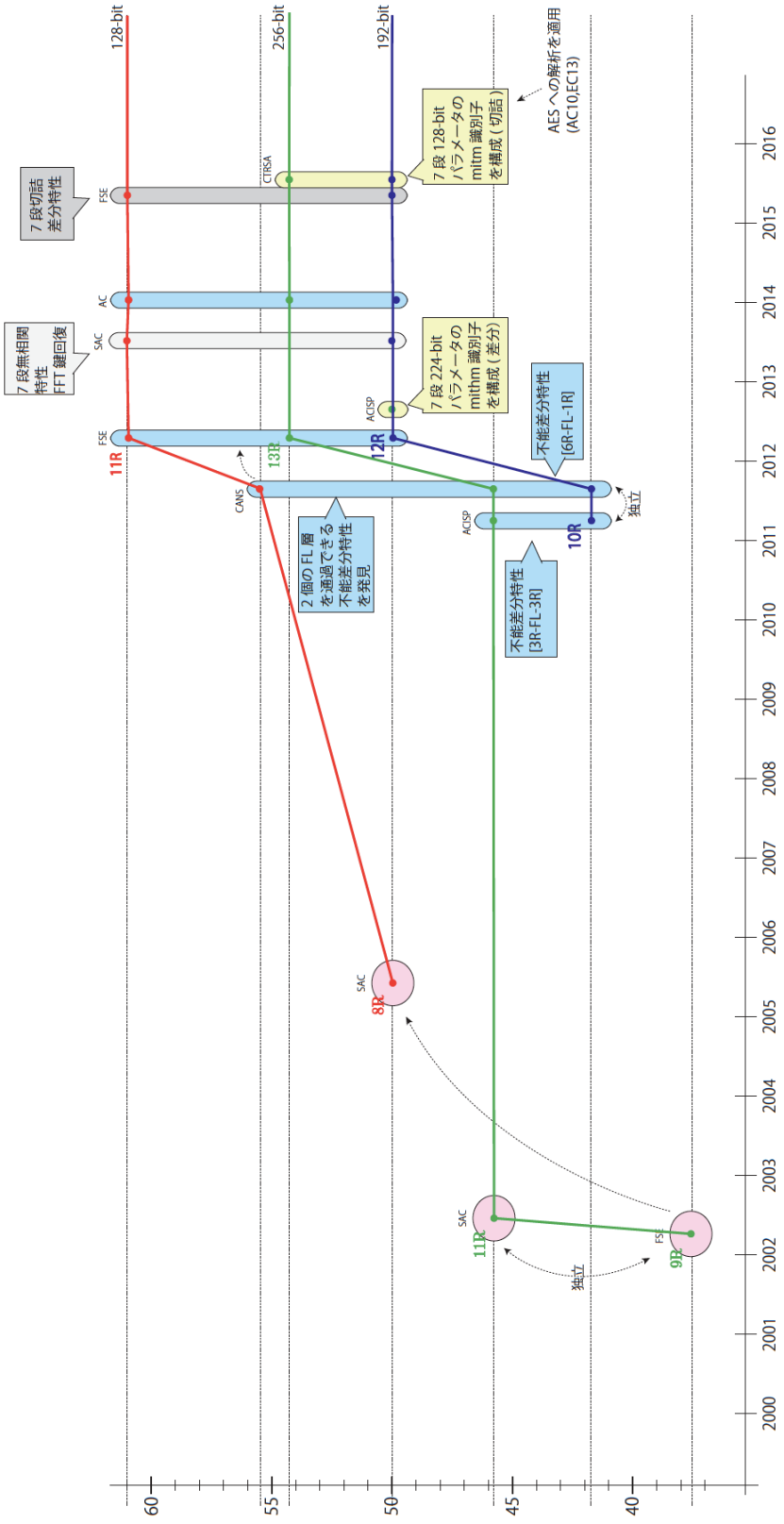
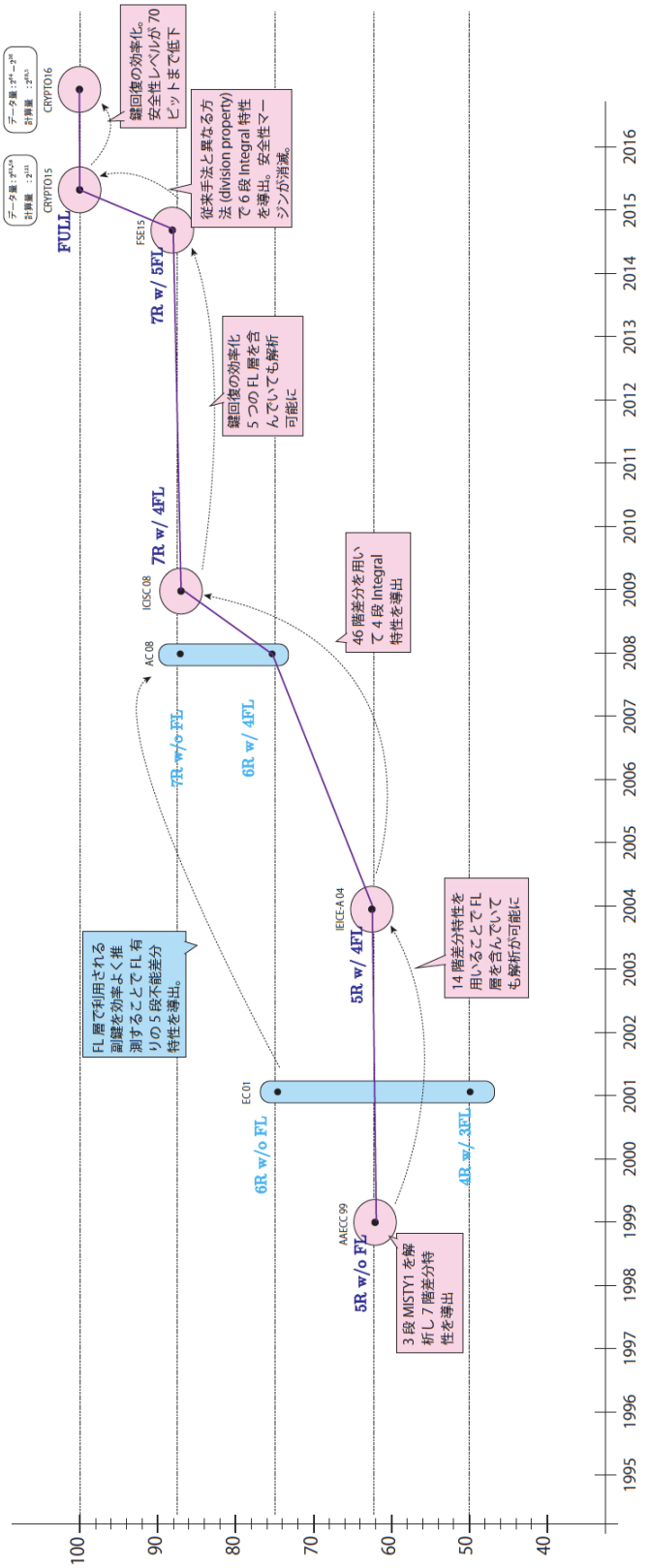


図 3　MISTY1 の攻撃技術進化マップ



② 解読手法の進展や計算機能力の向上を勘案した共通鍵暗号の今後の危殆化に関する考察

■公開鍵暗号と共通鍵暗号の安全性評価手法の違いについて（報告書より抜粋）

「公開鍵暗号に対する解析は主に漸近的な解析手法であり，特定パラメータに特化した解析手法は盛んに行われていない．これは (1)多くの公開鍵暗号はパラメータを大きくすることで安全性を維持できることが多く特定パラメータ特化型な解析手法を研究する動機が削がれること，(2)攻撃性能が実装依存に依るため計算量の単位が定かではなく，特定パラメータ特化型な解析手法を用いたとしても厳密な計算量見積もりが困難なこと，(3)漸近的な評価は暗号理論の外側にある計算機科学や数学の分野でも広く議論されるため，学術的確度の高い評価と言えること，などが要因として考えられる．すなわち攻撃が実行可能な小さなパラメータに対して解読可能かを評価し，これを基に大きなパラメータがどの程度の安全性を有するかを予測する．」

「共通鍵暗号に対する解析は主に特定のパラメータに特化した解析手法であり，漸近的な解析手法は行われていない．これは共通鍵暗号の鍵長はそもそも固定のため漸近的な解析手法が議論できないことに起因する．共通鍵暗号は漸近的な評価が出来ない代わりに，実利用のパラメータに対して厳密に安全性を評価する手法が発展している．例えば共通鍵暗号の一回暗号化に要する計算時間を計算量の単位とするという consensus が確立している．」

■共通鍵暗号の危殆化予測に関して（報告書より抜粋）

「学術的な世界においては，設計者が設定した claimed セキュリティが破られた場合には，暗号の安全性は破られたとみなされる．例えば，128 ビット鍵の場合，全数探索(2^{128}) と比べて鍵の導出に必要な計算量が半分になった場合(2^{127}) でも，理論上は破られたとみなされる．共通鍵暗号における claimed セキュリティは鍵の全数探索を基準としているため，理論上破られたことと，現実的に問題があるレベルにはかい離はあり，理論上の解読が必ずしも現実社会での解読と一致しない．また，鍵の回復に対する計算量を安全性の基準にしているため，全数探索と比較して計算量は少ないが，非常に多くのデータ量が求められる場合も数多く存在する．この場合，実際の攻撃を行うには効率的に攻撃に必要なデータを集める必要があり，ここが実際の攻撃の際にボトルネックとなる場合も考えられる．

しかしながら，理論的な攻撃（claimed セキュリティが破られた場合）と実際的な影響との差を定量的に図ることは不可能である．最悪のケースとしては，理論的に破られたあとにすぐに現実的な攻撃に繋がる可能性もある．例えば，MD5 は2004 年

にcollision 攻撃が発表され，そのすぐ2007 年にStevens らによるX.509証明書の偽造攻撃[69] やSasaki らとLeurent らより電子メールのクライアント認証プロトコルであるAPOP への攻撃[49, 67] が提案されている．＜SHA-1、RC4の例中略＞ そのため，共通鍵暗号の世界ではClaimedセキュリティを基準としており，これが破られた場合，設計者の意図しない脆弱性がはらんでいることから弱い暗号とみなされる．こうなった場合は，学術的な関心は少なくなり，一流の研究者からの解析が行われないため，それ以降の安全性の低下については不明となる．実際，2012 年に中東，イランをターゲットにしたマルウェアFlame には，学術レベルでは未知のMD5 のchosen-prefix collision attack が証明書の偽造に用いられていた[33]．以上の点から，claimed セキュリティが破られた暗号に対しては，新規採用をやめることが望まれる．またアルゴリズム移行には約10 年必要とされていることからも，実際の攻撃に結びつく前にClaimed セキュリティが破られた暗号については移行を検討するべきである．」

■結論（報告書より抜粋）

「上述した通り，暗号学会ではclaimed セキュリティが破られた暗号方式を移行検討の対象とすることで共通鍵暗号の安全性維持に努めている．実際，学術的には攻撃アルゴリズムの進化を予測することは非科学的なため事実上不可能であり，対外的に発表されないアンダーグラウンドな改良の存在も無視できない．仮に継続利用を判断する場合，未発表で改良されている可能性も考慮した上で現在の最良解析手法におけるデータ量・メモリ量・計算量にとらわれることなく慎重な検討が期待される．学術的にはclaimed セキュリティが破られたか否かという厳格な判定基準を設けている以上，継続利用の判断は各利用シーンごとに高度な政治的・経営的判断により行われるべきである．」

5. MISTY1 の攻撃に必要な暗号文データを攻撃者が取得するのに必要な時間（事務局検討）

現在知られているMISTY1のフルラウンド攻撃には2^{64}ブロック分の平文・暗号文ペアが必要である。2^{64}ブロックの暗号文データを攻撃者が通信路から入手すると想定した場合に、データ取得に必要な時間をCRYPTREC事務局で調査した（次ページの図４参照)。IoTデバイス等で暗号化したデータを低速な通信路で伝送する場合から、高速サーバで暗号化したデータを超高速回線で伝送する場合までさまざまなケースがある。低速回線の例として、交通系等で利用されているICカード規格FeliCa（通信速度：

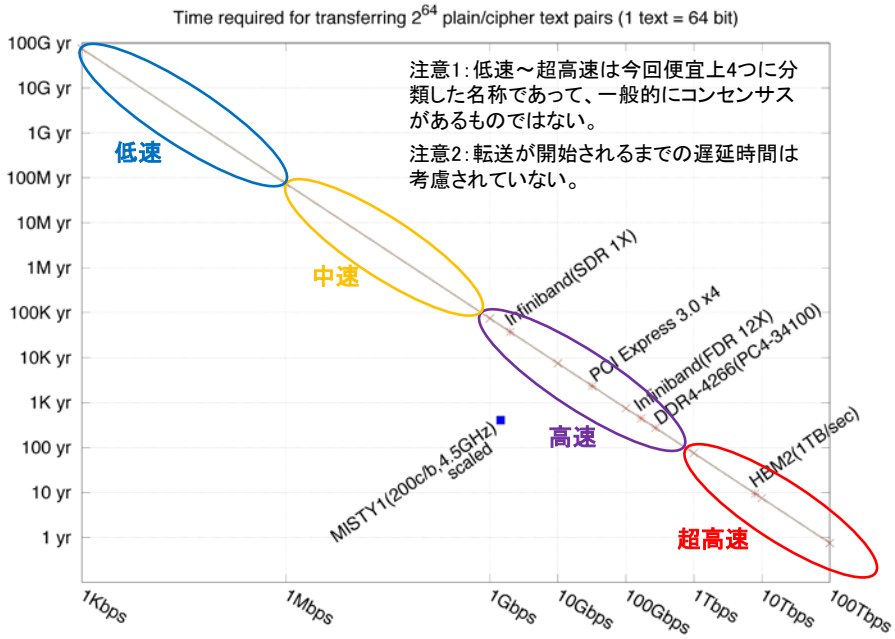


図4：2^{64}ブロックの暗号文データの伝送に要する時間のおおよその目安

212kbps）の場合、暗号文データの収集に約3.5億年、超高速回線の例では、メモリ規格HBM(High Bandwidth Memory)2（メモリ帯域：8Tbps）の場合、暗号文データの収集に約9.4年かかる試算になる。

6. 暗号技術評価委員会での審議

昨年度に出したMISTY1の安全性に関する速報では、「この攻撃は、解読に必要なデータ量が膨大であることから、現実的な脅威ではないと考えられます。CRYPTREC では、MISTY1の安全性に関して引き続き調査を行い、CRYPTREC Webサイトにて報告する予定です。」としている。今年度の調査・検討をふまえて、MISTY1に関して今後どのようなアクションをとるのがよいか、下記の4つの案を例示して審議を行った。

（例）

1. MISTY1の解読に必要なデータ量が膨大であることから、現在の見解を維持する。
2. MISTY1の新規採用は控えるよう、例えばCRYPTREC暗号リストに脚注を加える。（但し現在、64ビットブロック暗号全体に「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。」の脚注あり）
3. 利用形態によりMISTY1からの移行を推奨する。（利用時の注意点を示す）
4. MISTY1からの移行を推奨する。（MISTY1を「推奨候補暗号リスト」から「運用監視暗号リスト」に移す）

審議の結果、1 と 4 はない， 2, 3 を具体的にどうするかについて議論がなされ、

- 今回の外部専門家からの意見等をふまえ、CRYPTRECとして、現在の見解を維持するのではなく、何らかのアクションを検討した方がよいのではないか。例えば、64ビットブロック暗号全体に推奨される安全な利用方法であり、現在報告されているMISTY1に対する攻撃を回避できる方法として、2^{32}ブロックごとに鍵を変更するなどの利用方法を示す。
- MISTY1の利用状況（どこでどう使われているか）の調査を検討してはどうか。すでに利用されている暗号技術に対してCRYPTRECが何かアクションを起こす場合、ユーザにとってどのようなインパクトがあるかを把握しておくことが重要である。

などの意見が出た。

7. 暗号技術検討会での審議依頼事項

暗号技術評価委員会での審議結果及び今年度の調査・検討をふまえて、MISTY1 に関して今後どのようなアクションをとるのがよいかご意見をいただきたい。

資料１０

暗号技術検討会
２０１６年度　報告書（案）

２０１７年３月

目　　次

１．はじめに

情報通信技術の急速な発展により、自動車、家電、医療、農業、工場など様々な分野で、あらゆるモノがネットワークに繋がる IoT 社会が到来し、サイバー空間と実空間の融合が進みつつある。IoT の発展がもたらす利便性・効率の向上を享受できる一方で、巧妙化・複雑化を続けるサイバー攻撃のリスクも増していくと考えられるため、情報システム全体のセキュリティ確保は喫緊の課題である。暗号技術は既に様々な製品やサービスに組み込まれ、セキュリティを支える基盤技術として欠かせないものであるが、その重要性は IoT 社会の到来により一層増すと考えられる。

このような社会の変化に伴い、CRYPTREC には、これまで取り組んできた暗号アルゴリズムのセキュリティ確保を引き続き推進することに加えて、暗号アルゴリズムを利用したプロトコルのセキュリティ確保のための活動拡大や、情報システム全体のセキュリティ確保に向けた暗号技術の利活用のための情報提供といった貢献が求められている。

本年度、CRYPTREC では「重点課題検討タスクフォース」において、これまで年度ごとに整理されていた CRYPTREC 文書について、文書番号から内容を判断できるように文書番号体系のあり方について議論を行った。また、政府統一基準に向けた新たな CRYPTREC 成果物や、新たな社会ニーズを見据えた新規活動等の、前年度から把握している課題については、暗号技術検討会および各委員会に議論の場を移すこととするなど、今後の CRYPTREC の体制の整理を行った。

本年度の各委員会の活動として、暗号技術評価委員会では、暗号技術の安全性及び実装に係る監視及び評価、SHA-1 の安全性低下に関する注意喚起レポートの発行、新技術に関する調査及び評価等の検討等を行った。また、同委員会の下に設置された軽量暗号 WG において、軽量暗号技術の利用促進を図るため、昨年度より作成を進めていた「暗号技術ガイドライン（軽量暗号)」を公開した。暗号技術活用委員会では、情報システム全般のセキュリティ確保に寄与することを目的として、作成すべき運用ガイドラインの対象及び取扱い範囲の切り分けの検討、作成した運用ガイドラインのアップデート方法の検討等を行った。加えて、CRYPTREC として暗号プロトコルをどのように扱うかを重点的に検討するため、新たに「暗号プロトコル課題検討 WG」を設置し、まずは暗号プロトコルをテーマとする運用ガイドラインの検討対象を検討した。これらの 2016 年度の活動の詳細については、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構が取りまとめる「CRYPTREC Report 2016」を参照いただきたい。

今後も暗号技術を用いた情報システム及び情報社会全体のセキュリティ確保のために、成果物の検討や情報発信等を行っていく所存である。

末筆であるが、暗号技術検討会及び関係委員会等に御協力いただいた構成員、オブザーバの方々をはじめ、関係者の皆様に心から謝意を表する次第である。

2017 年 3 月

暗号技術検討会
座長　松本　勉

２．暗号技術検討会開催の背景及び開催状況

２．１．暗号技術検討会開催の背景

暗号技術は情報セキュリティの基盤技術であり、その安全性を暗号技術の専門家により技術的、専門的な見地から客観的に評価することが重要である。電子政府のセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリスト化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府の構築に貢献することを目指し、2001 年度から暗号技術検討会を開催した。

暗号技術検討会において 2002 年度に策定された電子政府推奨暗号リストは、2012 年度に 10 年ぶりの改定が行われ、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（以下、「CRYPTREC 暗号リスト」という。）として発表されたが、その後においても、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の更なる普及促進を行うため、総務省及び経済産業省は、継続的に暗号技術検討会を開催している。

２．２． CRYPTREC の体制

CRYPTREC とは、Cryptography Research and Evaluation Committees の略であり、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：松本勉横浜国立大学教授）と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する委員会から構成される暗号技術評価プロジェクトをいう。

2016 年度の CRYPTREC においては、暗号アルゴリズムの安全性確保やその利活用に係る議論のみならず、暗号技術に対する社会ニーズの変化や、社会情勢の変化を踏まえ、暗号技術評価委員会では軽量暗号ガイドラインを策定し、暗号技術活用委員会では新たにガイドラインを策定すべきものについて議論を進め、来年度に向けて整理を行った。また、昨年度に引き続き、重点課題検討タスクフォースにて議論を行い、文書番号体系の検討や、同タスクフォースの廃止に伴い、今後の体制を整理した。

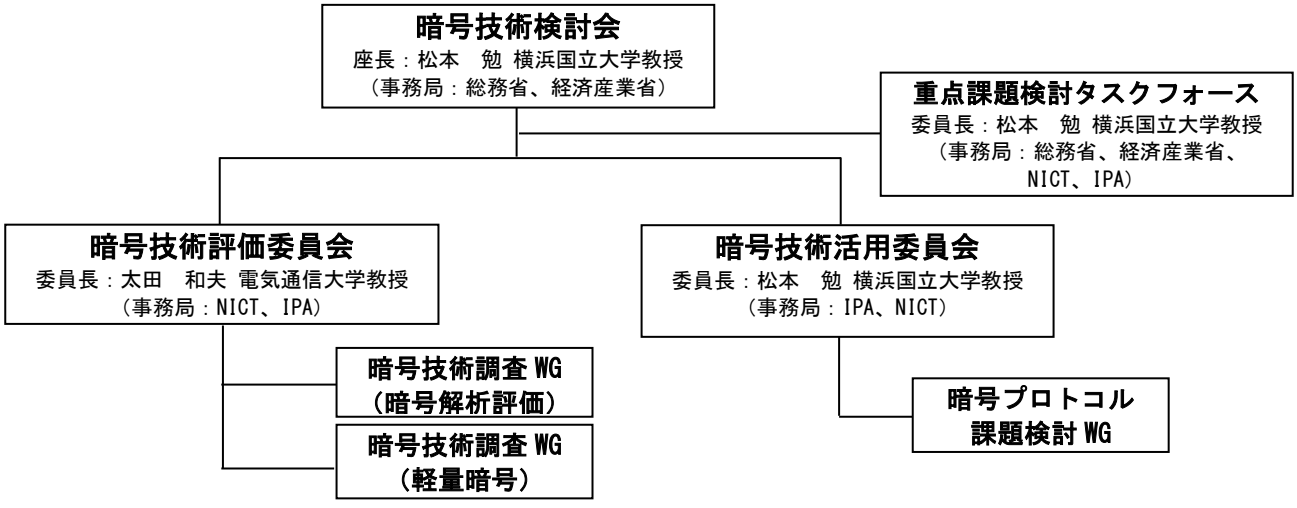


図 2.2.1　2016 年度 CRYPTREC の体制

２．３．暗号技術検討会の開催状況

2016 年度の暗号技術検討会は、以下に挙げる議題について審議、承認を行うために１回開催した。

〇2017 年 3 月 30 日（木）15:00～17:00

（主な議題）

- CRYPTREC の今後の体制（案）について
- 文書番号体系について
- 2016 年度暗号技術評価委員会、暗号技術活用委員会の活動報告について
- SHAKE128 の推奨候補暗号リストへの追加について
- ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に入れた評価について
- KCipher-2 の仕様書について
- SHA-1 の安全性低下について
- 2016 年度　暗号技術検討会報告書（案）について

（概要）

- 検討会での議論を基に作成

３．各委員会の活動報告

３．１．重点課題検討タスクフォース

３．１．１．設置の経緯

2015 年 6 月から 8 月までに開催された「CRYPTREC の在り方に関する検討グループ」での議論の結果、政府統一基準に向けた新たな CRYPTREC 成果物の在り方、暗号プロトコルのセキュリティ確保に向けた活動等において、継続的な議論が必要との結論となった。

このため、暗号技術検討会の下に「重点課題検討タスクフォース」を設置し、これら継続的に議論することとなった論点や、その他 CRYPTREC の方向性を機動的に検討し、トップダウン的な意思決定もできる体制を構築することとした。

３．１．２．重点課題検討タスクフォースの開催実績

本年度、重点課題タスクフォースは１回開催した。会合の概要は表 3.1 のとおり。

表 3.1.1　重点課題検討タスクフォースの開催実績

回	年月日	主な議題
第４回	2017 年 2 月 22 日	・CRYPTREC の今後の体制（案）について ・文書番号体系（案）について

３．１．３．2016 年度の議論概要

2016 年度、重点課題検討タスクフォースを１回開催した。タスクフォースでの審議事項は、主に(1) CRYPTREC の今後の体制について、(2)文書番号体系についてを議論した。具体的な議論の概要は次のとおり。

(1) CRYPTREC の今後の体制(案)について

昨年度に行われた第３回重点課題検討タスクフォースにおいて、本年度の主な課題として以下が挙げられた。

① 文書体系のあり方について
② 政府統一基準に向けた新たな CRYPTREC 成果物
③ 新たな社会ニーズを見据えた新規活動
④ 情報システム全体のセキュリティ確保を意識した他団体との連携
⑤ その他

①についての詳細は「（２）文書番号体系（案）について」に記載するが、本年度タスクフォースにおいて議論を行い、結果について暗号技術検討会にて審議を受けることとした。

②、③については、政府統一基準等から参照されやすい文書の作成やプライバシー保護のような社会ニーズを見据えた検討等の新たな取り組みについて、今後どのように議論を進めていくかを NISC との相談を含め、事務局で整理を行い、その内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号活用委員会に議論の場を移して検討を行うこととした。

④については、今後他団体との連携を必要とする対象のタスクが明確になった段階で、タスクの内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号技術活用委員会に議論の場を移し、具体的な連携方法について検討を行うこととした。

⑤については、CRYPTREC としてどう取り組むか議論が必要なテーマに関する検討であるが、昨年度、例として挙がった ChaCha20 の安全性評価の必要性については、本年度、暗号技術評価委員会にて議論され、安全性評価が実施されている。

以上をもって、重点課題検討タスクフォースのミッションを終了とし、同タスクフォースを廃止することとした。

また、暗号技術検討会については現状の活動状況を踏まえ、年１回開催を基本とし、メールベースの審議や報告などをタイムリーに行う体制を整えることによって、暗号技術検討会のアクティビティが低下しないように活動の効率化を図る。

(2) 文書番号体系（案）について

これまで CRYPTREC においては、年度成果物としてガイドライン、報告書を公開しているが、今後は文書の番号から内容（およびその文書の位置づけ）がわかる文書管理をするため、CRYPTREC 文書について、番号体系を整理することとした。

表 3.1.2　CRYPTREC 文書と想定される対象

CRYPTREC 文書	想定される対象
・総務省、経済産業省によって承認された文書	・CRYPTREC 暗号リスト

・暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会によって承認された文書 ・暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会、及び WG での配付資料	・CRYPTREC 暗号リストと各暗号アルゴリズム仕様書との対応表 ・CRYPTREC が報告書またはガイドラインとして公開するもの ・CRYPTREC が公表する注意喚起レポート ・外部評価レポート（外部評価者が作成した技術報告書） ・委員会資料（議事録を含む）

それらの体系ルールとして以下のような整理を行った。

＜文書番号＞::=CRYPTREC＜カテゴリ＞－＜連番＞－＜管理情報＞

アップデートあり：（前バージョンはアーカイブ）

・CRYPTREC LS-0001-2016 ⇔ 2016 年度発行 CRYPTREC 暗号リスト（最新）

・CRYPTREC LS-0001-2012 ⇔ 2012 年度発行 CRYPTREC 暗号リスト（アーカイブ）

アップデートなし：（アーカイブなし）

・CRYPTREC RP-0001-2015 ⇔ 2015 年度暗号技術検討会報告書

・CRYPTREC RP-0002-2015 ⇔ 2015 年度暗号技術評価委員会報告書

【参考】

・ FIPS - XXX - yyy ⇒ 米国連邦強制規格

・NIST SP800 - XXX rev. ⇒ NIST が自ら作ったガイドライン

・NIST SP1800 - XXX ⇒ NCCoE プロジェクトで作ったガイドライン

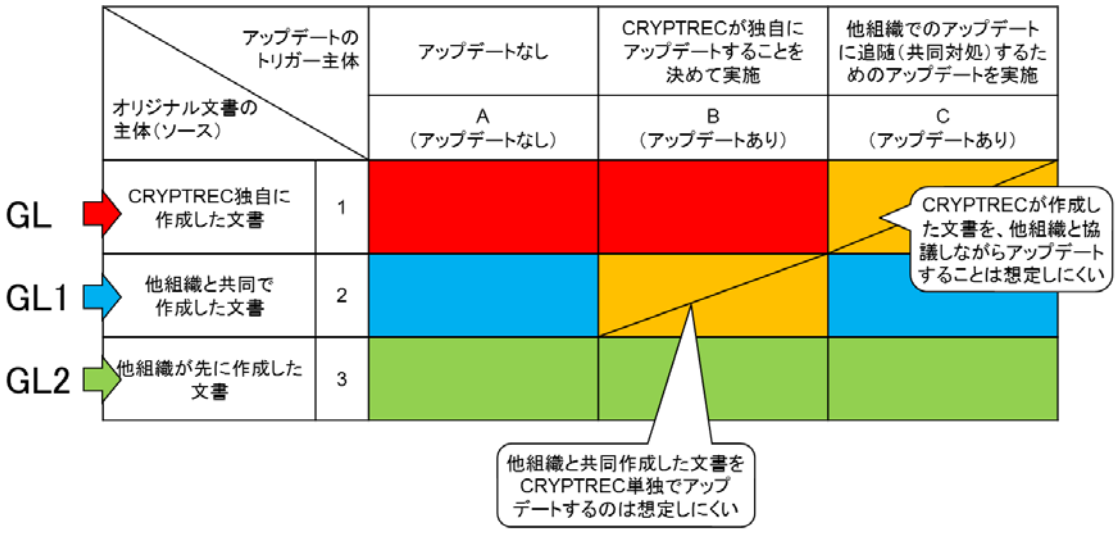
表 3.1.3 カテゴリ表記

CRYPTREC 文書分類	該当する既存の CRYPTREC 文書例	表記名
CRYPTREC 暗号リスト関係	・CRYPTREC 暗号リスト ・CRYPTREC 暗号リストと仕様書の対応関係表	LS
年次報告書	・年次報告書	RP
早期に公開する注意喚起	・注意喚起レポート	ER
ガイドライン	・暗号技術ガイドライン ・暗号運用ガイドライン	GL
技術報告書	・調査 WG 報告書 ・推奨セキュリティパラメータ設定	TR
外部評価報告書	・外部評価者が作成した安全性評価報告書 ・外部評価者が作成した実装性能評価報告書	EX
会議資料	・暗号技術検討会資料 ・各委員会資料	MT

また、「ガイドライン」が主な対象と想定されるが、これらのことを前提として表記名の他、「作成主体」や「アップデートの作業主体」の違いが分かるように識別子を付すことがある。

＜例＞ＧＬ ⇒ ＧＬ，ＧＬ１，ＧＬ２と表記

表 3.1.4　カテゴリ内の識別子表記



また、CTYPTREC 文書の作業主体区分の考え方としては以下のように整理を行った。

表 3.1.5　【オリジナル文書の主体（ソース）】

#	ソース	概要	過去の文書例
1	CRYPTREC が独自に作成した文書	・CRYPTREC が独自に作成した文書 ※WG またはアウトソーシングで実施	全文書
2	他組織と共同で作成する文書	・他組織と共同で作成する文書 ※両組織で発行されることを想定 ※主体は他組織。CRYPTREC はサポート	なし
3	他組織が先に作成した文書	・他組織が作成した文書をベースに、 （できるかぎり少ない変更で） CRYPTREC としての文書を作成 ※最小限の場合、「外部文書の参照関係を示す」だけの文書となることもありうる	なし

表 3.1.6　【アップデートのトリガー主体】

#			過去の文書例
A	アップデートなし	・発行後は原則アップデートしない	年次報告書
B	CRYPTREC が独自にアップデートすることを決めて実施	・CRYPTREC でアップデートを実施 ※WG またはアウトソーシングで実施	CRYPTREC 暗号リスト 解析計算量評価
C	他組織でのアップデートに追随（共同対処）するために CRYPTREC としてもアップデートを実施	他組織と共同、または他組織がアップデートした内容をベースに、CRYPTREC としてのアップデートを実施 ※WG 設置は想定しない	なし

※「アップデート」とは、文書内容の質自体に関わる記述をいずれ改訂することを当初から意図しており、かつそれを実行することを意味する。アップデート後、前バージョンの文書は廃止（アーカイブ）される。「記述内容の正誤修正」、「作成時点で改訂を意図していない文書」は「アップデート」には含まない。

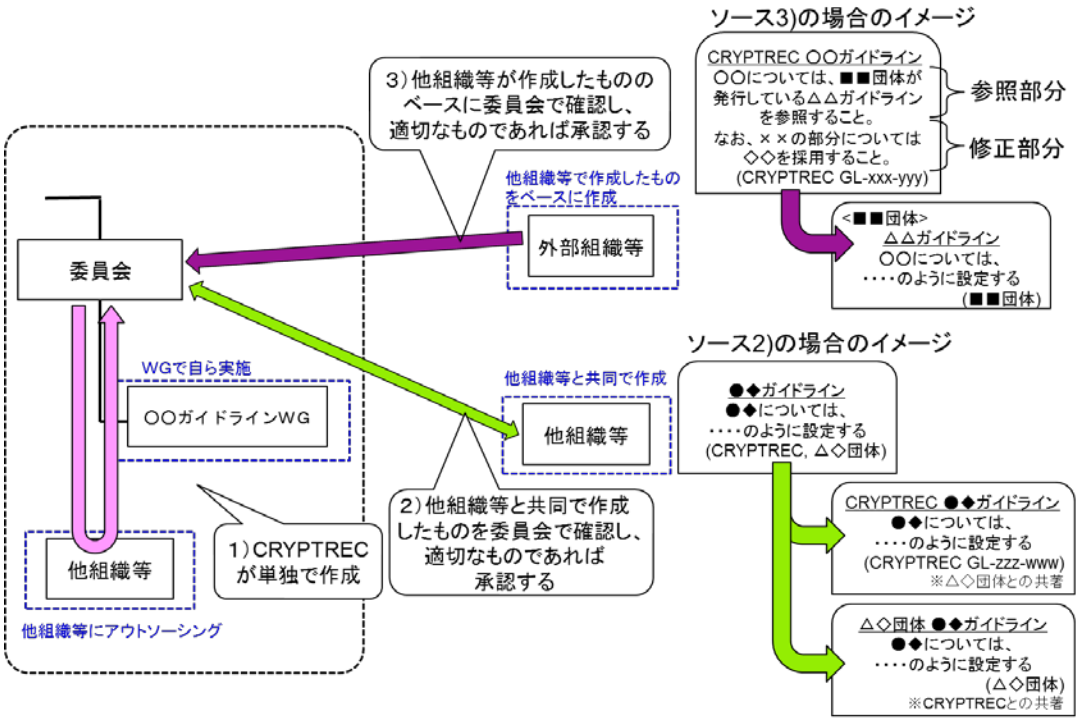


図 3.1.1　「文書の作成主体（＝ソース）の違い」の説明図

３．２．暗号技術評価委員会

３．２．１．活動の概要

暗号技術評価委員会は、CRYPTREC 暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う。主要な検討課題は以下のとおりである。

・暗号技術の安全性及び実装に係る監視及び評価
・暗号技術に関する注意喚起レポートの CRYPTREC ホームページへの公表
・新世代暗号に係る調査

これらの課題について 2016 年度に行った具体的な検討内容を、以下のとおり報告する。

３．２．２．2016 年度の活動内容

暗号技術の安全性及び実装に係る監視及び評価

2016 年度は、① 学会等での情報収集に基づく CRYPTREC 暗号等の監視、② ハッシュ関数 SHA-3 に属する SHAKE128 に関して CRYPTREC 暗号リストへの追加のため検討を実施した。

①について、研究集会、国際会議、研究論文誌の情報等を収集し、リスト掲載暗号の安全性について監視活動を行った。暗号解読技術等の進展が見られ、これらについて引き続き注視していく必要がある。

②について、ハッシュ関数 SHA-3 ファミリーのうち、CRYPTREC 暗号リストに含まれていなかった SHAKE128 について、出力長を 256 ビット以上とするようパラメータを選択すれば、CRYPTREC 暗号リストへ追加するのに十分な安全性と実装性能を有していることが確認できた。

その他、KCipher-2 の仕様書に見つかった誤記について、電子政府推奨暗号リスト選定の際に行われた安全性評価・実装評価に誤記修正による影響はないことを確認した。DH/ECDH の仕様書の参照先について、参照先の仕様書の変更が軽微なものであることを確認した。共通鍵暗号の安全性について調査を行い、MISTY1 の今後の利用について提示すべき推奨方針案について検討を行った。

暗号技術に関する注意喚起レポートの CRYPTREC ホームページでの公表

ハッシュ関数 SHA-1 のフルラウンド(全 80 ステップのうち 80 ステップすべて)の仕様に対して具体的な衝突が初めて発見された。従前通り、移行対策を実施すべきであると考えられる。

新世代暗号に係る調査

本項目に係る活動に関しては、暗号技術評価委員会の下に暗号技術調査 WG（暗号解析評価）及び暗号技術調査 WG（軽量暗号）を設置し、議論した。暗号技術調査 WG（暗号解析評価）では、楕円曲線上の離散対数問題の困難性に関する調査、多重線形写像及び難読化の最新動向等、暗号技術の安全性を支える数学的問題の困難性に係る調査を実施し、技術レポートとして、CRYPTREC ホームページより公開予定である。暗号技術調査 WG（軽量暗号）では、軽量暗号を選択・利用する際の技術的判断に資すること、今後の利用促進を図ることを目的とした「暗号技術ガイドライン(軽量暗号)」(日本語、英語)を完成させ、CRYPTREC ホームページより公開予定である。また、ChaCha20-Poly1305 の安全性評価を行った。現時点では ChaCha20-Poly1305 は、認証暗号として、具体的な脅威は見つかっていないと考えられる。

３．２．３．暗号技術評価委員会の開催状況

2016 年度、暗号技術評価委員会は計 2 回開催した。各回会合の概要は表 3.2.1 のとおりである。

表 3.2.1　暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2016 年 7 月 27 日	暗号技術評価委員会活動方針の検討 WG 活動方針の検討 外部評価についての検討 今後の課題に関する検討
第 2 回	2017 年 3 月 21 日	WG 今年度活動報告 ハッシュ関数 SHAKE128 の取扱いについての検討 外部評価レポート(ChaCha20-Poly1305 の安全性調査)についての検討 KCipher2 の仕様書の修正に関する検討 SHA-1 に関する注意喚起レポートについて報告 共通鍵暗号の安全性調査に関する検討 CRYPTREC Report 2016 の目次案提示 監視状況報告

３．３．暗号技術活用委員会

３．３．１．活動概要

暗号技術活用委員会では、情報システム全般のセキュリティ確保に寄与することを目的として必要な活動を行うものとする。具体的には、実運用とセキュリティ確保の両面の観点から、以下の対象を取り扱う。

- 暗号アルゴリズムの利用及び設定に関する運用マネジメント
- 暗号プロトコルの利用及び設定に関する運用マネジメント
- その他、情報システム全体のセキュリティ確保に有用な暗号に関わる運用マネジメント

2016 年度は、上記の活動目的を踏まえ、運用面でのマネジメントに関するガイドライン（以下、運用ガイドライン）を本格的に整備していくことを今後の暗号技術活用委員会（以下、活用委員会）での活動の中心に据えることを視野に、以下の項目について検討を行った。

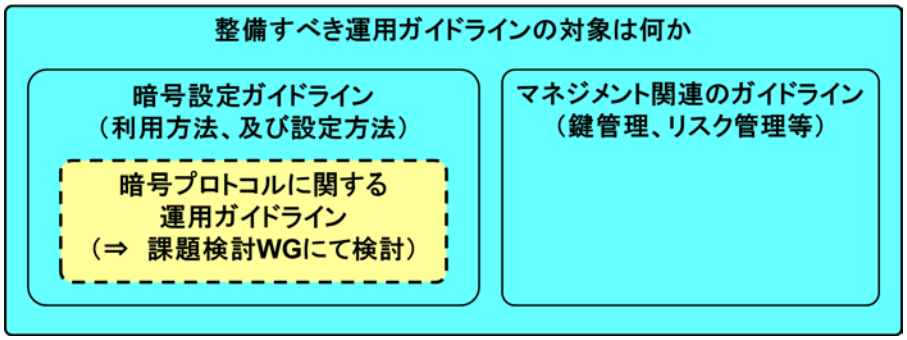
① 作成すべき運用ガイドラインの対象及び取扱い範囲の切り分けの検討
② 作成した運用ガイドラインのメンテナンス体制の検討
③ 外部組織や業界団体との連携方法の検討
④ 運用ガイドラインの作成
⑤ ベンダや業界団体等の意向をバランスよく取り入れつつ、セキュリティも担保する利用価値の高い成果物となるようにコントロールする
⑥ その他
CRYPTREC として暗号プロトコルをどのように扱うかを重点的に検討するため、「暗号プロトコル課題検討 WG（以下、課題検討 WG)」を設置

なお、①については、暗号プロトコルに関わる部分を課題検討 WG で、それ以外の範囲を活用委員会でそれぞれ検討した。また、④と⑤については、実際の運用ガイドラインを作成する際に、テーマに応じて適切な手段を活用委員会で判断して実施していくことになった。

３．３．２．2016 年度の活動内容

運用ガイドラインの対象について

2017 年度以降に活用委員会として運用ガイドラインを作成する価値がある対象を検討するにあたっては、以下の目的と領域に合致する範囲のガイドラインを想定して議論を行った。なお、暗号設定ガイドラインのうち、暗号プロトコルに関する部分については課題検討 WG にて検討を行い、それ以外の部分については活用委員会にて検討を行った。



【暗号プロトコルに関する運用ガイドライン以外の対象】

もともと運用ガイドラインの必要性が高いと考えられている対象を中心に、以下の観点から整理を行い、今後、運用ガイドラインを作成していく際に優先的に取り上げていくことが望ましい対象を取りまとめた。具体的な検討結果は活用委員会報告書を参照されたい。

- 【対象】
  どのような用途で使う運用ガイドラインであるか
- 【目的・内容】
  どのような目的をもった運用ガイドラインを意図したものか
- 【内容】
  運用ガイドラインに記載される内容はどのようなものか
- 【想定読者】
  その運用ガイドラインの想定読者は誰か
- 【必要性】
  なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか
- 【課題】
  ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か
- 【他組織のガイドライン等】
  他組織が同種のガイドラインを作っていないか／作ろうとしていないか
- 【関連組織】
  どのような他組織と連携していくのがよいか

【暗号プロトコルに関する運用ガイドラインの対象】

暗号プロトコルに関する運用ガイドラインの対象を検討するにあたっては、「(STEP1) 検討対象とする暗号プロトコルの列挙」と「(STEP2) 列挙した暗号プロトコルのなかから運用ガイドラインを作る価値がある／必要性が高いと判断したものを抽出」の 2 段階で議論を行った。

運用ガイドラインを作る価値があるか／必要性が高いかを判断するために、以下の観点から整理を行った。その結果、「必要性」「目的・内容」「想定読者」の 3 点について明確に説明できるものを「運用ガイドラインを作る価値がある／必要性が高い」と判断・抽出

し、より詳細な検討を加えた。具体的な検討結果は活用委員会報告書を参照されたい。

- 【必要性】
  運用ガイドラインを作る価値／必要性を明確に示すことができるか（なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか）
- 【目的・内容】
  どのような目的・内容をもった運用ガイドラインを意図したものかを明確に示すことができるか
- 【想定読者】
  その運用ガイドラインの想定読者を具体的に示すことができるか
- 【課題】
  ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か
- 【他組織のガイドライン等】
  他組織が同種のガイドラインを作っていないか／作ろうとしていないか
- 【関連組織】
  どのような他組織と連携していくのがよいか

運用ガイドラインのアップデート方法に関連する検討

運用ガイドラインは、ガイドライン作成時の標準化状況や製品状況、利用環境や利用実績等を踏まえて、その時点での現実的かつ効果的な推奨設定や推奨基準を提示するものである。このことは、ある程度の時間が経過し、標準化状況や製品状況、利用環境や利用実績等が変化すれば、運用ガイドラインの中身も陳腐化し、ガイドラインとしてふさわしくないものとなることを意味する。

このため、今後運用ガイドラインの整備を進めるにあたっては、単に運用ガイドラインを作るだけでなく、運用ガイドラインの質を維持するためにどのような方法でアップデートを行っていくかを検討しておく必要がある。そこで、活用委員会では、具体的な運用ガイドライン例として「SSL/TLS 暗号設定ガイドライン」を取り上げ、アップデートの在り方の検討を行った。

外部連携について

運用ガイドラインの作成については、CRYPTREC 単独での作成よりも関連する外部組織や業界団体など（以降、他組織等という）との連携を進めたほうがよいとの指摘があった。これらの指摘を踏まえ、来年度より開始する運用ガイドラインの作成にあっては、従来の WG 形式での作成に捕らわれずに柔軟な作成スタイルを考慮する。

1) CRYPTREC が単独で作成
2) 他組織等と共同で作成
3) 他組織等で実施したものをベースに作成

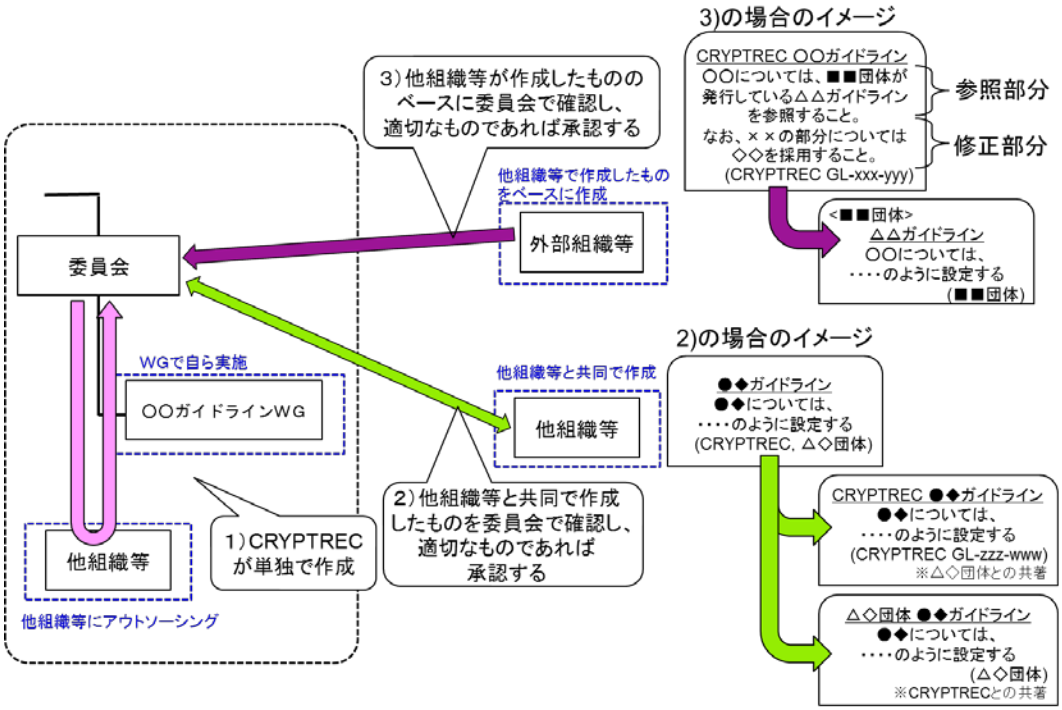


図 3.3.1　作成手段の説明図

実際の運用ガイドラインの作成手段を決定するにあたっては、以下のポイントを重視して判断を行う。

- 他組織等と連携したほうが有用性のある運用ガイドラインが作成できるか
- 連携先の外部組織等が信頼できる組織・団体であるか
- 他組織等と連携することによって作業効率を上げることができるか（例えば作業スケジュール等）
- 予算面やリソース面からの考慮

今後に向けて

2017 年度は新たな運用ガイドラインを実際に作成していく方向で活動計画を検討する。具体的な対象の選定等については、2017 年度第一回暗号技術活用委員会にて決定する方向である。

また、SSL/TLS 暗号設定ガイドラインについては、2016 年度活動で出た意見を踏まえ、2017 年度にアップデートを行う計画とする予定である。

３．３．３．暗号技術活用委員会の開催状況

2 回開催された活用委員会での審議概要は表 3.3.1 のとおりである。

表 3.3.1　暗号技術活用委員会　開催状況

回	開催日	議案
第 1 回	2016 年 11 月 9 日	・暗号プロトコル課題検討 WG 活動状況報告 ・運用ガイドライン（「SSL/TLS 暗号設定ガイドライン」）のメンテナンス方法に関する検討

		・運用ガイドラインの対象範囲に関する検討
第 2 回	2017 年 3 月 15 日	・暗号プロトコル課題検討 WG 活動報告 ・暗号プロトコル以外の運用ガイドラインの対象の検討 ・外部連携の進め方の検討 ・2016 年度暗号技術活用委員会報告書

3 回開催された課題検討 WG での審議概要は表 2 のとおりである。

表 3.3.2　暗号プロトコル課題検討 WG　開催状況

回	開催日	議案
第 1 回	2016 年 10 月 27 日	WG 活動概要の説明、課題についての自由討議
第 2 回	2016 年 12 月 26 日	第 1 回 WG での討議を踏まえた課題の整理と更なる検討
第 3 回	2017 年 2 月 10 日	報告書案の取りまとめ

４．今後の CRYPTREC の活動について

CRYPTREC では、暗号アルゴリズムの安全性確保やその利活用に係る議論のみならず、SSL/TLS 等の暗号を用いたプロトコルの安全な利用環境の確保のための取組など、暗号をとりまく環境変化に応じた新たなニーズへの対応などに取り組むこととしている。

暗号技術評価委員会においては、本年度 ChaCha20 の安全性評価を実施しているが、今後も引き続き、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・評価を行い、暗号技術活用委員会においては、本年度の検討を受けて新たな運用ガイドラインを作成する。両委員会の範囲を超えるものについては、必要に応じて、暗号技術検討会で審議・判断する。

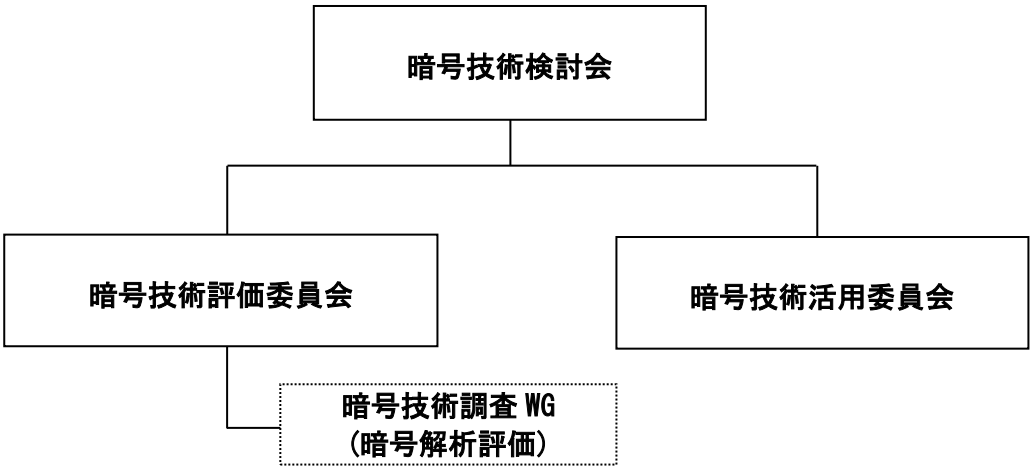


図 4.1.1　2017 年度 CRYPTREC の体制図（予定）