CRYPTREC Report 2015

平成 28 年 3 月

独立行政法人情報処理推進機構

国立研究開発法人情報通信研究機構

「暗号技術活用委員会報告」

目次

はじめに

本報告書は、総務省及び経済産業省が主催している暗号技術検討会の下に設置され、独立行政法人情報処理推進機構及び国立研究開発法人情報通信研究機構によって共同で運営されている暗号技術活用委員会の 2015 年度活動報告である。

暗号技術活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。

2015 年度は、運用ガイドライン WG が 2014 年度に作成した「SSL/TLS 暗号設定ガイドライン」を正式に公開した。これは、具体的な製品の設定方法やチェックリストを用意するなど、サーバ構築者やサーバ管理者にとって使いやすいガイドラインとなることを目指して作成したものであるが、公開後の１年間のダウンロードが約 50,000 件という実績を得ており、本ガイドラインの有用性は広く評価されたといえよう。

一方、昨今の暗号技術を取り巻く環境の変化、サイバーセキュリティ基本法の施行といった社会情勢の変化等を踏まえ、CRYPTREC が担うべき今後の活動内容や暗号技術活用委員会の次のミッション等について、暗号技術検討会の下に設置された 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において約１年にわたり検討が行われてきた。

これらの検討の結果、暗号技術活用委員会の活動目的の軸足を、「暗号技術を主軸とした検討」から「情報システムのセキュリティ確保に寄与する暗号技術等に係る成果物の提供」に移すことになった。具体的には、「SSL/TLS 暗号設定ガイドライン」が好評であったことを踏まえ、暗号技術活用委員会が扱う範囲を、利用者に使いやすい運用面でのガイドライン（運用ガイドライン）の作成にも、2016 年度以降、本格的に拡大していくことを考えている。

このような営みにより、情報システムのセキュリティ確保の底上げをはかり、暗号の普及促進・セキュリティ産業の競争力強化に結び付け、新しい情報社会に適したセキュリティの自立的な充実に貢献できることを期待している。

末筆ではあるが、本活動に様々な形でご協力下さった委員の皆様、関係者の皆様に対して深く謝意を表する次第である。

暗号技術活用委員会 委員長　松本 勉

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。例えば、電子署名や GPKI[1] システム等、暗号関連の電子政府関連システムに関係する業務に従事している方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書は、2015 年度の暗号技術活用委員会の活動内容と成果概要を記述した。

2014 年度以前の CRYPTREC Report は、CRYPTREC 事務局（総務省、経済産業省、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）が共同で運営する下記の Web サイトから参照できる。

http://www.cryptrec.go.jp/report.html

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

【問合せ先】 info@cryptrec.go.jp

[1] GPKI：Government Public Key Infrastructure（政府認証基盤）

委員会構成

暗号技術活用委員会（以下「活用委員会」）は、図 1 に示すように、総務省と経済産業省が共同で運営する暗号技術検討会の下に設置され、独立行政法人情報処理推進機構（IPA）と国立研究開発法人情報通信研究機構（NICT）が共同で運営している。

活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、暗号利用に関するセキュリティ対策の推進、暗号技術の利用促進に向けた環境整備を主に担当する委員会である。

2015 年度は、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いて活用委員会の活動を開始した。このため、活用委員会の開催が 2016 年 3 月の 1 回となり、例年設置するワーキンググループは設置されなかった。

なお、活用委員会と連携して活動する「暗号技術評価委員会（以下「評価委員会」）」も暗号技術検討会の下に設置され、IPA と NICT が共同で運営している。評価委員会は、従来どおりのスケジュールで運営された。

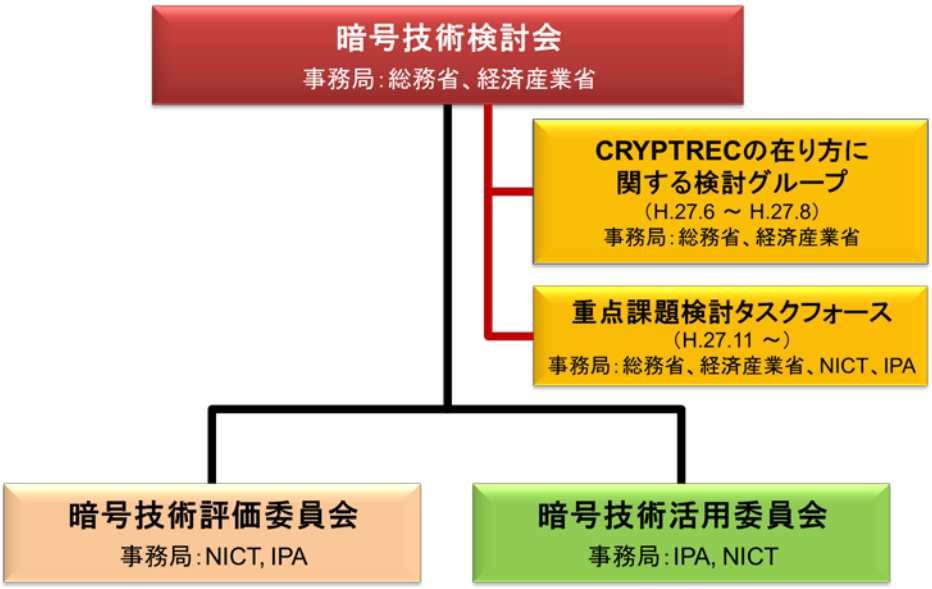

図 1　2015 年度の CRYPTREC の体制

委員名簿

暗号技術活用委員会

委員長	松本 勉	国立大学法人横浜国立大学 大学院 教授
委員	上原 哲太郎	立命館大学 教授
委員	菊池 浩明	明治大学 教授
委員	清藤 武暢	日本銀行 金融研究所
委員	手塚 悟	東京工科大学 教授
委員	松本 泰	セコム株式会社 IS 研究所 ディビジョンマネージャー
委員	満塩 尚史	内閣官房 政府 CIO 補佐官
委員	山口 利恵	国立大学法人東京大学 大学院 特任准教授
委員	山岸 篤弘	一般財団法人日本情報経済社会推進協会 主席研究員

オブザーバー

大川 伸也	内閣官房内閣サイバーセキュリティセンター[2015 年 12 月まで]
久保山 拓	内閣官房内閣サイバーセキュリティセンター
高木 浩光	内閣官房内閣サイバーセキュリティセンター
眞弓 隆浩	内閣官房内閣サイバーセキュリティセンター[2015 年 12 月から]
森安 隆	内閣官房内閣サイバーセキュリティセンター
新家 研介	総務省 行政管理局
松田 花鈴	総務省 行政管理局
筒井 邦弘	総務省 情報流通行政局
近藤 直光	総務省 情報流通行政局[2015 年 7 月まで]
丸橋 弘人	総務省 情報流通行政局[2015 年 8 月から]
中村 一成	総務省 情報流通行政局[2015 年 7 月まで]
今野 孝紀	総務省 情報流通行政局
岩永 敏明	経済産業省 産業技術環境局[2015 年 6 月まで]
加藤 誠司	経済産業省 産業技術環境局[2015 年 7 月から]
上坪 健治	経済産業省 商務情報政策局
中野 辰実	経済産業省 商務情報政策局
室井 佳子	経済産業省 商務情報政策局[2015 年 4 月まで]
中村 博美	経済産業省 商務情報政策局[2015 年 5 月から]
松本 裕悟	防衛省 整備計画局
吉岡 達宏	防衛省 整備計画局
岡野 孝子	警察大学校

相原 大輔　　警察大学校

事務局

独立行政法人情報処理推進機構（伊藤毅志[2015年7月まで]、頓宮裕貴[2015年8月から]、
近澤武、小暮淳、大熊建司、神田雅透、稲垣詔喬、初田瑠里[2016年1月まで]、
兼城麻子[2016年2月から]）
国立研究開発法人情報通信研究機構　（平和昌、盛合志帆、野島良、大久保美也子、
黒川貴司、金森祥子）

2015 年度の活動内容と成果概要

1. 活動内容

暗号技術活用委員会では、昨年度、今後の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、「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行い、報告書を取りまとめたことで一つの区切りを迎えた。

また、暗号技術を取り巻く環境、サイバーセキュリティ基本法の施行といった社会情勢の変化等をも踏まえ、CRYPTREC が担うべき今後の活動内容や暗号技術活用委員会での次のミッション等について、暗号技術検討会の下に設置された 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約１年にわたり検討が行われてきた。

検討グループ及び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目的の軸足を、「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、新たな活動目的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、暗号の取り扱いに関する観点から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

2015 年度は、上記の目的に対応するために、2016 年度以降の活動計画案を中心に検討を行った。

活動計画の柱は、「SSL/TLS 暗号設定ガイドライン」が好評であったことを踏まえ、暗号技術活用委員会が扱う範囲を運用面でのガイドライン（運用ガイドライン）作成に本格的に拡大することである。具体的には、作成すべき運用ガイドラインの対象及び取り扱い範囲の切り分け、メンテナンス体制、外部組織や業界団体との連携方法等を検討することとなる。

また、2015 年度は WG を設置しなかったが、最近はセキュリティプロトコルの脆弱性が問題となるケースが多くなっている。このため、CRYPTREC としてセキュリティプロトコルをどのように取り扱うかについて検討するための「暗号プロトコル課題検討 WG」を新たに設置することとした。

この他、2014 年度に運用ガイドライン WG が作成した SSL/TLS 暗号設定ガイドラインについて、暗号技術活用委員会及び暗号技術検討会での承認を経て、2015 年 5 月に CRYPTREC 及び IPA のホームページで公開した。

2. 今年度の委員会の開催状況

2015 年度暗号技術活用委員会は 1 回開催された。各回会合の概要は表 1 のとおり。

表 1　2015 年度暗号技術活用委員会　開催概要

回	開催日	議案
第 1 回	2016 年 3 月 2 日	● 2016 年度暗号技術活用委員会活動計画（案）について ● ワーキンググループ活動計画（案）について ● 運用ガイドラインに関する検討事項について

3. SSL/TLS 暗号設定ガイドラインの公開

2014 年度に運用ガイドライン WG が作成した SSL/TLS 暗号設定ガイドラインについて、暗号技術活用委員会及び暗号技術検討会での承認を経て、2015 年 5 月に以下のホームページで公開した。

【CRYPTREC 暗号運用ガイドライン】
SSL/TLS 暗号設定ガイドライン
http://www.cryptrec.go.jp/report/c14_oper_guideline_SSLTLS_web_1_1.pdf

【IPA 脆弱性対策　普及啓発資料】
SSL/TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～
https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

本ガイドラインは、2015 年 3 月時点における、SSL/TLS 通信での安全性と可用性（相互接続性）のバランスを踏まえた暗号設定方法をガイドラインとして取りまとめた。対象読者は、主に SSL/TLS サーバを実際に構築するにあたって具体的な設定を行うサーバ構築者、実際のサーバ管理やサービス提供に責任を持つことになるサーバ管理者、並びに SSL/TLS サーバの構築を発注するシステム担当者である。

表 2　安全性と相互接続性との比較

設定基準	概要	安全性	相互接続性の確保
高セキュリティ型	扱う情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に致命的または壊滅的な悪影響を及ぼすと予想される情報を極めて高い安全性を確保する SSL/TLS で通信するような場合に採用する設定基準。 **※とりわけ高い安全性を必要とする明確な理由があるケースを対象としており、非常に高度で限定的な使い方をする場合の設定基準である。** **一般的な利用形態で使うことは想定していない。**	本ガイドラインの公開時点において、標準的な水準を大きく上回る高い安全性水準を達成。	最近提供され始めたバージョンの OS やブラウザが搭載されている PC、スマートフォンでなければ接続できない可能性が高い。 また、PC、スマートフォン以外では、最新の機器であっても一部の機器について接続できない可能性がある。
推奨セキュリティ型	扱う情報が漏えいした際、組織の運営や資産、個人の資産やプライバシー等に何らかの悪影響を及ぼすと予想される情報を、安全性確保と利便性実現をバランスさせて SSL/TLS での通信を行うための標準的な設定基準。 **※ほぼすべての一般的な利用形態で使うことを想定している。**	本ガイドラインの公開時点における標準的な安全性水準を実現。	本ガイドラインで対象とするブラウザが搭載されている PC、スマートフォン等では問題なく相互接続性を確保できる。 バージョンが古い OS やブラウザ、一部の古い機器（フィーチャーフォンやゲーム機等）については接続できない可能性がある。
セキュリティ例外型	脆弱なプロトコルバージョンや暗号が使われるリスクを受容したうえで、安全性よりも相互接続性に対する要求をやむなく優先させて SSL/TLS での通信を行う場合に許容しうる最低限度の設定基準。	推奨セキュリティ型への移行完了までの短期的な利用を前提に、本ガイドラインの公開時点において許容可	最新ではないフィーチャーフォンやゲーム機などを含めた、ほとんどのすべての機器について相互接続性を確保できる。

	※推奨セキュリティ型への早期移行を前提として、暫定的に利用継続するケースを想定している。	能な最低の安全性水準を満たす。	

表 3　要求設定の概要

<table>
<tr><td colspan="2">要件</td><td>高セキュリティ型</td><td>推奨セキュリティ型</td><td>セキュリティ例外型</td></tr>
<tr><td colspan="2">暗号スイートの（暗号化の）セキュリティレベル</td><td>①256 ビット
②128 ビット</td><td>①128 ビット
②256 ビット</td><td>①128 ビット
②256 ビット
③RC4, Triple DES</td></tr>
<tr><td rowspan="5">暗号アルゴリズム</td><td rowspan="2">鍵交換</td><td>鍵長 2048 ビット以上の DHE または鍵長 256 ビット以上の ECDHE</td><td colspan="2">鍵長 1024 ビット以上の DHE
または鍵長 256 ビット以上の ECDHE</td></tr>
<tr><td></td><td colspan="2">鍵長 2048 ビット以上の RSA
鍵長 256 ビット以上の ECDH</td></tr>
<tr><td rowspan="2">暗号化</td><td colspan="3">鍵長 128 ビット及び 256 ビットの AES または Camellia</td></tr>
<tr><td></td><td colspan="2">RC4
Triple DES</td></tr>
<tr><td>モード</td><td>GCM</td><td colspan="2">GCM, CBC</td></tr>
<tr><td>ハッシュ関数</td><td>SHA-384, SHA-256</td><td colspan="2">SHA-384, SHA-256, SHA-1</td></tr>
<tr><td colspan="2">プロトコルバージョン</td><td>TLS1.2 のみ</td><td>TLS1.2～TLS1.0</td><td>TLS1.2～1.0,SSL3.0</td></tr>
<tr><td colspan="2">証明書鍵長</td><td colspan="3">鍵長 2048 ビット以上の RSA または鍵長 256 ビット以上の ECDSA</td></tr>
<tr><td colspan="2">証明書でのハッシュ関数</td><td colspan="2">SHA-256</td><td>SHA-256, SHA-1</td></tr>
</table>

本ガイドラインは 9 章で構成されており、章立ては以下のとおりである。

2 章では本ガイドラインを理解するうえで助けとなる技術的な基礎知識をまとめている。

3 章では、SSL/TLS サーバに要求される設定基準の概要について説明しており、4 章から 6 章で実現すべき要求設定の考え方を示している。

4 章から 6 章では、3 章で定めた設定基準に基づき、具体的な SSL/TLS サーバの要求設定について示している。

第 7 章では、SSL/TLS をより安全に使うために考えておくべきことをまとめている。

第 8 章は、クライアントの一つであるブラウザの設定に関する事項を説明しており、ブラ

ウザの利用者に対して啓発するべき事項を取り上げている。

第 9 章は、そのほかのトピックとして、SSL/TLS を用いたリモートアクセス技術（“SSL-VPN”とも言われる）について記載している。

巻末には、4 章から 6 章までの設定状況を確認するためのチェックリストや、個別製品での具体的な設定方法例も記載している。

3 章から 6 章が本ガイドラインの最大の特長ともいえ、「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視して現実的な利用方法を目指している。具体的には、実現すべき安全性と必要となる相互接続性とのトレードオフを考慮する観点から、安全性と可用性を踏まえたうえで設定すべき「要求事項」として 3 つの設定基準（表 2）を提示し、各々の設定基準ごとに、利用可能な「プロトコルバージョン」「サーバ証明書」「暗号スイート」を具体的かつ詳細に規定している（表 3）。

なお、7 章から 9 章は「情報提供」の位置づけとして記載している。

4. 2016 年度活動計画について

4.1 暗号技術活用委員会の活動計画について

「CRYPTREC 暗号技術活用委員会の今後の活動に向けて（第 2 回重点課題検討タスクフォースでの議題）」のうち、重点課題検討タスクフォースにて決定された活動方針を基に、2016 年度活動計画を定めた。

【活動計画概要】

① セキュリティ向上に役立つドキュメント類として、作成すべき暗号の取り扱いに関わる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

情報システム全体のセキュリティ確保に寄与するために、暗号技術活用委員会が扱う範囲として、どのような種類の暗号の取り扱いに関わる運用ガイドラインをどのような優先順位で作成すべきかを検討する。併せて、外部組織等と役割分担する境界についても検討する。

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

作成済みの運用ガイドラインをどのような方針でメンテナンス・アップデートしていくかについて検討する。特に、メンテナンス・アップデートのタイミングのほか、「i) 暗号技術活用委員会のみの審議対象とする範囲、ii) ワーキンググループ (WG) を組織して本格的な再検討を実施する範囲、iii) 暗号技術活用委員会としてはメンテナンス・アップデートの対象として取り扱わない範囲」といった、暗号技術活用委員会としてのメンテナンスの切り分けに関する考え方を整理する。

③ 外部組織や業界団体との連携方法の検討

運用ガイドラインの効率的な作成・整備・活用を図るため、外部組織や業界団体等に幅広く協力を求め、連携方法を検討する。必要に応じて、外部組織や業界団体等が主体的に作成するガイドラインへの暗号技術活用委員会としての連携の在り方も視野に入れる。

④ 運用ガイドラインの作成

実際の運用ガイドラインの作成にあたって、対象とするテーマ及び具体的な作業方法については暗号技術活用委員会が指定する。作業方法としては、以下のものが想定される。

- 暗号技術活用委員会で運用ガイドライン案を自ら作成する。
- 必要に応じて、対象とするテーマに精通した有識者並びに実運用に関わるベンダ関係者らを委員とするワーキンググループ（WG）を設置し、WG にて運用ガイドライン案を作成する。
- 暗号技術活用委員会での承認を受けた外部組織等に運用ガイドライン案の作成を委託する。

⑤ 成果物について、ベンダや業界団体等の協力を得る場合には、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。ワーキンググループ（WG）を設置する場合には、対応するテーマに応じて、ベンダや業界団体等からの人選について特に留意する。

運用ガイドライン等の作成にあたって、ベンダや業界団体等からの協力を得る場合には、主要ベンダや有力な業界団体等の協力を求めるとともに、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できるように暗号技術活用委員会として確認する。必要に応じて、内容の修正・再議を行う。

⑥ その他

必要に応じて、暗号技術活用委員会として検討テーマを新たに設けることがある。2016 年度は、 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」を設置する。

4.2 暗号プロトコル課題検討 WG の活動計画について

2016 年度暗号技術活用委員会活動計画にあるように、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 が設置される。

本 WG では、以下の観点から議論を行い、2017 年度以降の CRYPTREC における暗号プロトコルに関する活動につなげていく予定である。

【活動計画概要】

① CRYPTREC として扱うべき暗号プロトコルの対象範囲の集中検討

多種多様な暗号プロトコルがある中、CRYPTREC が暗号プロトコルを取り上げる目的を整理し、その目的に沿った取り扱うべき対象範囲を明確にする。

一つの目的としては、「SSL/TLS 暗号設定ガイドライン」のような、世の中で広く使われている暗号プロトコルに関する運用ガイドラインの整備を想定する。

② 運用ガイドラインの作成を前提とした安全性評価結果や脆弱性情報の取扱方法、他組織との連携方法等の課題整理

今後、様々な暗号プロトコルに関する運用ガイドラインを暗号技術活用委員会で整備していく際の課題を整理する。特に、以下のような項目を想定する。

- 作成した運用ガイドラインごとに内容のばらつきが大きく出ないようにするための安全性評価結果や脆弱性情報の取り扱いルールの明確化
- 運用ガイドラインに含める脆弱性情報と含めない脆弱性情報の範囲・境界についての検討
- 安全性情報や脆弱性情報を提供してもらう組織、同種ガイドラインを作成している組織、ガイドラインの主要な利用ユーザと想定される組織等との連携方法

③ 2017 年度以降の暗号プロトコルに関する活動方針案の整理・検討

2017 年度以降の暗号技術活用委員会における暗号プロトコルに関する活動方針案を取りまとめる。

5. 今後の活動について

上記 4 章に記載した暗号技術活用委員会の 2016 年度活動計画に基づき、特に運用ガイドラインや暗号プロトコルに関する活動方針案、及び外部組織や業界団体との連携方法の取りまとめを行う。

発行日　2016 年 6 月17 日 第1 版

発行者

・〒113-6591

東京都文京区本駒込二丁目28 番8 号

独立行政法人 情報処理推進機構

(技術本部 セキュリティセンター 暗号グループ)

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2-28-8 HONKOMAGOME,BUNKYO-KU

TOKYO,113-6591 JAPAN

・〒184-8795

東京都小金井市貫井北町四丁目2 番1 号

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)

NATIONAL INSTITUTE OF

INFORMATION AND COMMUNICATIONS TECHNOLOGY

4-2-1 NUKUI-KITAMACHI,KOGANEI

TOKYO,184-8795 JAPAN