CRYPTREC Report 2019

令和２年６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 2019 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 年度に、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」に移すことに定義し直し、2016 年度から新たな目的に基づいて活動している。

暗号技術活用委員会では、実運用とセキュリティ確保の両面の観点から、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）の作成に注力している。

2019 年度は、2018 年度より検討を進めていた「暗号鍵管理システム設計指針（基本編）」のドラフト案を CRYPTREC シンポジウム 2019 で公開し、パブリックコメントを実施して外部からの意見を募集するなど新しい試みも取り入れつつ、暗号鍵管理の在り方・フレームワークを提示する初めての本格的な暗号鍵管理ガイドラインとなる「暗号鍵管理システム設計指針（基本編）」を完成させた。また、既発行の「SSL/TLS 暗号設定ガイドライン」は SSL/TLS を利用する際の有用な運用ガイドラインとして広く利用されているが、利用環境と技術環境の変化に伴い、記載内容の見直しに向けた詳細な検討を行う TLS 暗号設定ガイドライン WG を 2019 年度に設置した。1 年間にわたる WG での検討を踏まえ、従来の有用性を維持しつつ、技術的に 2020 年 3 月時点でのセキュリティ水準に沿う記載内容に全面的に見直した「TLS 暗号設定ガイドライン」を完成させた。

今回作成した両ガイドラインが広く活用されるとともに、今後も運用ガイドラインの拡充を図っていくことにより、情報システムのセキュリティ確保の底上げ、暗号の普及促進・セキュリティ産業の競争力強化に繋がり、より安心・安全な情報化社会の実現に結び付くことを期待している。

末筆ではあるが、新型コロナウイルスの感染拡大防止の観点から 2019 年度末に開催予定であった暗号技術活用委員会と TLS 暗号設定ガイドライン WG を 2020 年度に移動せざるをえなかった。このような状況にも関わらず、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。

2020 年 7 月

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、2019 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。

2018 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。

https://www.cryptrec.go.jp/

CRYPTREC 報告書

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」という。）は、図 0-1 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（以下「IPA」という。）と国立研究開発法人情報通信研究機構（以下「NICT」という。）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。

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」も暗号技術検討会の下に設置され、NICT と IPA が共同で運営している。

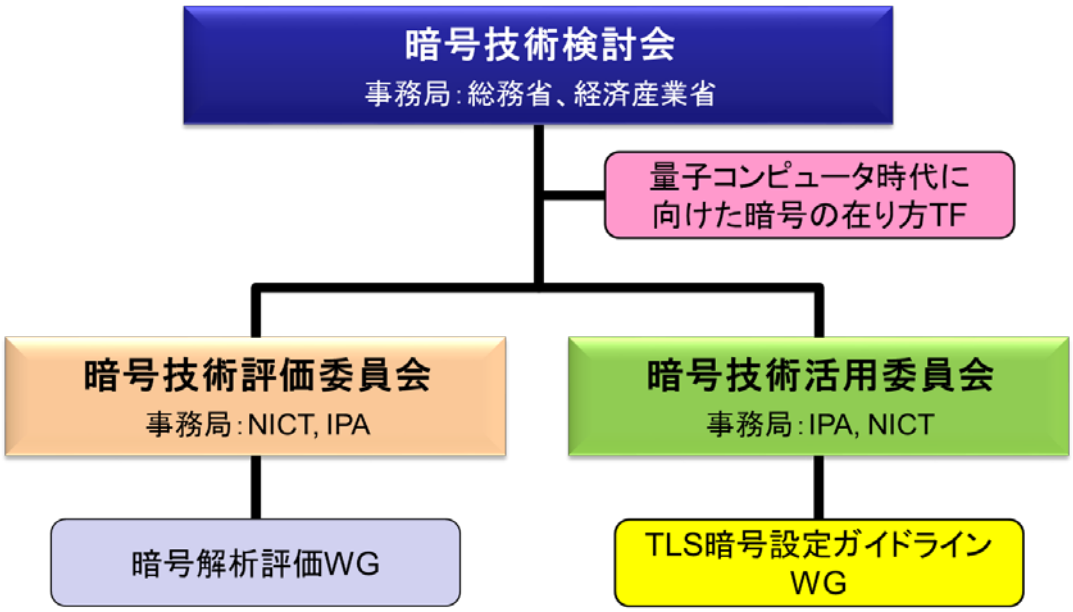

図 0-1　2019 年度の CRYPTREC の体制

委員名簿

暗号技術活用委員会

委員長	松本 勉	横浜国立大学 教授
委員	上原 哲太郎	立命館大学 教授
委員	垣内 由梨香	マイクロソフト株式会社 セキュリティプログラムマネージャー
委員	菊池 浩明	明治大学 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 シニアエンジニア
委員	杉尾 信行	株式会社 NTT ドコモ
委員	清藤 武暢	日本銀行 主査[2019 年 8 月まで]
委員	宇根 正志	日本銀行 情報技術研究グループ長[2019 年 9 月から]
委員	手塚 悟	慶応義塾大学 教授
委員	寺村 亮一	株式会社 NDIAS マネージャー
委員	松本 泰	セコム株式会社 マネージャー
委員	三澤 学	三菱電機株式会社 主席研究員
委員	満塩 尚史	内閣官房 政府 CIO 補佐官
委員	山岸 篤弘	日本情報経済社会推進協会 客員研究員
委員	山口 利恵	東京大学 特任准教授
委員	渡邊 創	産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 副研究センター長

（所属：2020 年 3 月末時点）

オブザーバー

徳永 竜一	内閣官房内閣サイバーセキュリティセンター
木村 誠一郎	内閣官房内閣サイバーセキュリティセンター
川崎 明彦	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
岡田 崇志	個人情報保護委員会 事務局[2019 年 6 月まで]
衛門 愛子	個人情報保護委員会 事務局[2019 年 7 月から]
小高 久義	総務省 行政管理局
豊重 巨之	総務省 サイバーセキュリティ統括官室[2019 年 7 月まで]
遠藤 琢	総務省 サイバーセキュリティ統括官室[2019 年 7 月まで]
黒田 淳	総務省 サイバーセキュリティ統括官室

梅城 崇師	総務省 サイバーセキュリティ統括官室[2019 年 7 月から]
山下 恵一	総務省 サイバーセキュリティ統括官室[2019 年 7 月から]
三島 崇	経済産業省 産業技術環境局
稲垣 良一	経済産業省 商務情報政策局[2019 年 7 月まで]
上田 翔太	経済産業省 商務情報政策局[2019 年 7 月から]
飯山 貴啓	経済産業省 商務情報政策局
荒木 美敬	外務省 大臣官房 情報通信課[2020 年 2 月まで]
魚住 拓摩	外務省 大臣官房 情報通信課[2019 年 12 月まで]
松原 祐衣子	外務省 大臣官房 情報通信課[2019 年 8 月から]
伊藤 江美子	外務省 大臣官房 情報通信課[2020 年 2 月から]
今泉 隆文	防衛省 整備計画局情報通信課[2019 年 5 月まで]
中村 佳憲	防衛省 整備計画局情報通信課[2019 年 12 月まで]
小林 圭寿	防衛省 整備計画局情報通信課[2019 年 8 月から]
椛木 隆慎	防衛省 整備計画局情報通信課[2019 年 12 月から]
山口 義隆	警察大学校
多賀 文吾	警察大学校

事務局

独立行政法人情報処理推進機構（瓜生和久、神田雅透、小暮淳、橋本徹、菅野淳[2019年6月まで]、天内日紗子[2019年7月から]）
国立研究開発法人情報通信研究機構（矢野博之[2019年7月まで]、久保田実[2019年8月から]、盛合志帆[2019年7月まで]、野島良[2019年8月から]、大久保美也子、篠原直行、黒川貴司、金森祥子、吉田真紀、青野良範、笠井祥、大川晋司）

TLS 暗号設定ガイドライン WG

主査	須賀 祐治	株式会社インターネットイニシアティブ シニアエンジニア
委員	漆嶌 賢二	GMO グローバルサイン株式会社 部長
委員	垣内 由梨香	マイクロソフト株式会社 セキュリティプログラムマネージャー
委員	菅野 哲	株式会社レピダム 代表取締役
委員	菊池 浩明	明治大学 教授
委員	北村 英志	グーグル合同会社 デベロッパーアドボケイト
委員	島岡 政基	セコム株式会社 主任研究員

委員	杉尾 信行	株式会社 NTT ドコモ
委員	杉原 弘祐	セコムトラストシステムズ株式会社
委員	松本 照悟	アマゾンウェブサービスジャパン株式会社 シニアセキュリティコンサルタント

（所属：2020 年 6 月末時点）

オブザーバー

徳永 竜一	内閣官房内閣サイバーセキュリティセンター
木村 誠一郎	内閣官房内閣サイバーセキュリティセンター
川崎 明彦	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
衛門 愛子	個人情報保護委員会事務局
梅城 崇師	総務省 サイバーセキュリティ統括官室
林 巧	経済産業省 産業技術環境局
上田 翔太	経済産業省 商務情報政策局
飯山 貴啓	経済産業省 商務情報政策局
荒木 美敬	外務省 大臣官房 情報通信課[2020 年 2 月まで]
松原 祐衣子	外務省 大臣官房 情報通信課
中村 佳憲	防衛省 整備計画局情報通信課[2019 年 12 月まで]
小林 圭寿	防衛省 整備計画局情報通信課
椛木 隆慎	防衛省 整備計画局情報通信課[2019 年 12 月から]
山口 義隆	警警察大学校

事務局

独立行政法人情報処理推進機構（瓜生和久、神田雅透、小暮淳、橋本徹、菅野淳[2019年6月まで]、天内日紗子[2019年7月から]）

国立研究開発法人情報通信研究機構（矢野博之[2019年7月まで]、久保田実[2019年8月から]、盛合志帆[2019年7月まで]、野島良[2019年8月から]、大久保美也子、篠原直行、黒川貴司、金森祥子、吉田真紀、青野良範、笠井祥、大川晋司）

第1章　2019 年度活動内容

1.1. 活動内容

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っている。

2019 年度は、安全な暗号利用に係る運用ガイドラインを整備する観点から、「暗号鍵管理システム設計指針（基本編）」及び「TLS 暗号設定ガイドライン」の作成を行った。

（1）暗号鍵管理システム設計指針（基本編）の作成

2018 年度に作成した「暗号鍵管理システム設計指針（基本編）」のドラフト素案についてさらなる検討を進め、CRYPTREC シンポジウム 2019 の開催に合わせてドラフト版として公開した。

さらに、ドラフト版に対するパブリックコメントを実施して外部からの意見も踏まえつつ、暗号鍵管理の在り方・フレームワークを提示する初めての本格的な暗号鍵管理ガイドラインとなる「暗号鍵管理システム設計指針（基本編）」を完成させた。

（2）TLS 暗号設定ガイドラインの作成

2015 年に Ver1.0/Ver1.1、2018 年に Ver2.0 をリリースした「SSL/TLS 暗号設定ガイドライン（以下「現行ガイドライン」という。）」は累計で 20 万件以上のダウンロードがあるなど、TLS を利用する際の有用な運用ガイドラインとなっている。

このたび、SSL3.0 利用禁止及び TLS1.3 リリースなど、現行ガイドラインの利用環境とは大きく異なりつつある現状であることを踏まえて内容を大幅に見直すこととし、詳細な検討を行うため、TLS 暗号設定ガイドライン WG（以下「TLS ガイドライン WG」という。）を設置した。

TLS ガイドライン WG では、ガイドラインの位置づけ及び想定読者に関しては現行ガイドラインを踏襲し従来の有用性を維持する一方、技術的には 2020 年 3 月時点での TLS の現状を踏まえて全面的に記載内容の見直しを行った。なお、今回の改訂で SSL3.0 を全面的に禁止することになったため、ガイドラインの名称から「SSL」を削除し、「TLS 暗号設定ガイドライン」と呼ぶこととする。

位置づけ

- TLS に関する「Best Practice 集」
- 「暗号技術評価の厳密な根拠」よりも「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視して利用方法をまとめる
- 暗号に関連する“技術的なこと”は原則説明しない

- 暗号に直接関連しないことでも必要・重要なことは説明する

想定読者

- サーバ構築者、サーバ管理者、並びにシステム担当者
- 一部の内容については、ブラウザを使う一般利用者への注意喚起も対象

1.2. 開催状況

2019 年度の活用委員会は実質 2 回開催された。各回会合の概要は表 1-1 のとおり。

なお、新型コロナウイルスの影響により、2019 年度第二回活用委員会は当初予定の 3 月から 6 月に開催が延期されたため、形式上、2020 年度第一回活用委員会として開催された。

表 1-1　2019 年度暗号技術活用委員会　開催概要

回	開催日	議案
2019 年度 第一回	2019 年 6 月 12 日	■ 活用委員会活動計画について ■ TLS 暗号設定ガイドライン WG 活動計画について ■ 暗号鍵管理システム設計指針（基本編）ドラフト版について
2020 年度 第一回	2020 年 6 月 1 日	■ TLS 暗号設定ガイドライン案について ■ 暗号鍵管理システム設計指針（基本編）案について ■ EdDSA に関する安全性評価の必要性について ■ 運用監視暗号リストからの削除について

1.3. TLS 暗号設定ガイドライン WG 開催状況

2019 年度の TLS ガイドライン WG は実質 4 回開催された。各会合での概要は表 1-2 のとおり。

なお、新型コロナウイルスの影響により、2019 年度第四回 WG は当初予定の 2 月から 5 月に開催が延期されたため、形式上、2020 年度第一回 WG として開催された。

表 1-2　2019 年度 TLS 暗号設定ガイドライン WG　開催概要

議論テーマ	2019 年度			2020 年度
	第一回 (19/9/2)	第二回 (19/11/19)	第三回 (20/1/7)	第一回 (20/5/26)
①ガイドライン名の名称変更	★			
②3 段構成の概要の見直し	◎	★		
③推奨プロトコルバージョンの見直し	◎	★		
④サーバ証明書推奨設定の見直し	◎	★		
⑤推奨暗号スイートの見直し	○	◎	★	
⑥具体的な設定方法の見直し	★			
⑦情報提供として記載している内容の見直し			◎	★
⑧ブラウザでの標記に関する留意点の見直し			◎	★
⑨（専用）サーバ―ブラウザ以外も含めた利用形態			○	★
⑩常時 HTTPS 化に伴う留意点			○	★
⑪コラムの題材			○	★

凡例：　★：結論を確認　　◎：重点的に議論し、方向性を決定　　○：自由議論

1.4. CRYPTREC シンポジウム 2019 開催報告

開催日時：2019 年 7 月 12 日（金）13：00～17：00

開催場所：品川シーズンテラスカンファレンス（東京都港区港南 1-2-70）

主　　催：国立研究開発法人情報通信研究機構、独立行政法人情報処理推進機構

共　　催：総務省、経済産業省

参加人数：223 名

表 1-3　プログラム

時間	内容	
13：00	開会挨拶	情報処理推進機構　富田達夫　理事長
13：10	総務省挨拶・経済産業省挨拶	総務省　泉宏哉　大臣官房審議官 経済産業省　三角育生　サイバーセキュリティ・情報化審議官
13：20	暗号技術検討会活動報告	松本勉　座長（横浜国立大学　教授）
13：30	暗号技術活用委員会活動報告	松本勉　委員長（横浜国立大学　教授）
13：50	招待講演① TLS の動向に関連する紹介	須賀祐治　様（（株）インターネットイニシアティブ　シニアエンジニア）
14：50	コーヒーブレイク	
15：20	暗号技術評価委員会活動報告	太田和夫　委員長（電気通信大学　教授） 高木剛　主査（東京大学　教授）
15：50	招待講演② 量子アニーリングの現状と展望	西森秀稔　様（東京工業大学　教授）
16：50	閉会挨拶	情報通信研究機構　徳田英幸　理事長

第2章　成果概要

2.1. 暗号鍵管理システム設計指針（基本編）の作成

あらゆる分野・あらゆる領域の全ての暗号鍵管理システム（以下「CKMS（Cryptographic Key Management System)」という。）を対象に、暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項（Framework Requirements）を網羅的に提供し、設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を取りまとめた「暗号鍵管理システム設計指針（基本編)」を完成させた。

今回作成した暗号鍵管理システム設計指針（基本編）及びチェックリストは、以下のホームページよりダウンロードすることができる。

https://www.cryptrec.go.jp/op_guidelines.html

- 暗号鍵管理システム設計指針（基本編）:

https://www.ipa.go.jp/security/vuln/ckms.html

- 暗号鍵管理システム設計指針（基本編）:
- チェックリスト:

<u>位置づけ</u>

- 本設計指針は、セキュアな暗号アルゴリズムを利用する上で極めて重要な役割を果たす暗号鍵の管理に関する在り方を解説し、CKMS を設計・構築・運用する際に参考すべきドキュメントとして作成された。
  - 「暗号鍵管理の在り方」（暗号鍵管理の位置づけと検討すべき枠組み）では、暗号鍵管理の必要性を認識してもらうための解説を記載した。これは、あらゆる暗号鍵管理を検討する際の基礎となる考え方を示したものである。
  - 「暗号鍵管理についての技術的内容」では、包括的な CKMS 設計指針である NIST SP800-130「A Framework for Designing Cryptographic Key Management Systems」の解説書・利用手引書として活用できるように構成した。本設計指針では、SP800-130 での Framework Requirements を『暗号鍵管理における目的に応じた』対象範囲に分類・再構成することによってそれぞれの検討項目の目的や必要性を明確化した。
- 本設計指針は、あらゆるユースケースにおける暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき事項一覧を提供し、CKMS 設計時に考慮すべきトピックス及び設計書等に明示的に記載する要求事項を示している。

- ただし、本設計指針の中ではセキュリティ要求事項は定義せず、具体的な特定のセキュリティ機能の採用を義務づけることもしない。それぞれの要求事項に対してどのように対応（例えば、ポリシー、暗号アルゴリズム、デバイス等の選択）するかは CKMS 設計者に委ねられ、それらの対応方針が設計仕様書や運用マニュアル等に記載される。
- CKMS 設計者が選択した対応方針が適正かどうかの判断は運用管理者や調達責任者が行う。適切ではないと判断した場合には、CKMS 設計のやり直しを指示すべきである。確認にあたってはチェックリストも活用されたい。

適用範囲

- 本設計指針は、あらゆる分野・あらゆる領域の全ての CKMS を対象とする。CKMS は、暗号処理及びその処理で利用する暗号鍵を管理するシステム全体を包含する。ただし、暗号処理及び暗号鍵を管理・運用するのに必要な機能以外の部分は本設計指針の対象外である。
- 本設計指針の適用範囲に CKMS のシステム規模は問わない。もっとも小さい単純なものは一つのデバイス（の一部分）からなる場合もあるし、暗号鍵管理センタで複数のデバイスを集中管理するような大規模システムの場合もある。
- どの範囲を CKMS の対象とするのかは、「暗号鍵管理システムの設計原理と運用ポリシー」の中で CKMS 設計者によって具体的に定義される。

構成

本設計指針は、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、イントロダクションとして暗号鍵管理の在り方や考え方について解説する。あらゆる暗号鍵管理における基礎をなすものである。

3 章では、本設計指針の活用方法について解説する。

4 章以降が CKMS の包括的な設計指針である SP800-130 の解説書・利用手引書として活用できるように、SP800-130 の内容を再構成したものである。暗号鍵管理における目的ごとに章分けをしている。

本設計指針の特長

本設計指針の最大の特長は、暗号鍵管理の考え方の枠組みを整理し、暗号鍵管理のための設計仕様書や運用マニュアルがどのように作られるべきかを明確にした点にある。大きくは 4 つの視点からなる。

第一の視点：暗号鍵管理の考え方の枠組み

国内外の暗号鍵管理に関するガイドラインの調査結果を基に、暗号鍵管理の考え方の枠組みを図 2-1 のように整理し、暗号鍵管理のための設計仕様書や運用マニュアルがどのように

作られるべきかを明確にした。暗号鍵管理の構成要素は、「Framework Requirements」「Profile Requirements」「System Requirements」「Guidance」の 4 つからなり、暗号鍵管理に関する文書類はそれらの構成要素のいずれかに分類できる。

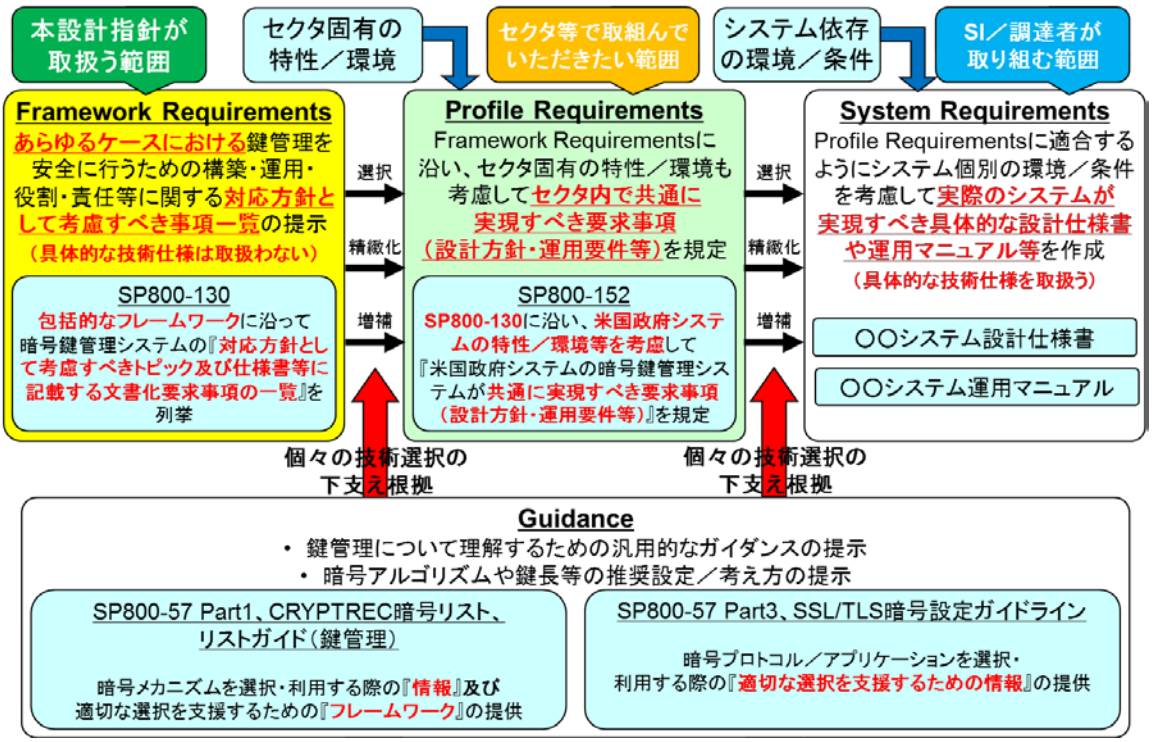

図 2-1　暗号鍵管理の考え方の枠組み

① 「Framework Requirements」:

暗号鍵を必要とするあらゆるユースケースにおける CKMS を対象に、暗号鍵管理を安全に行うための構築・運用・役割・責任等に関する対応方針として考慮すべき一連の事項を包括的なフレームワークとして取りまとめたものである。SP800-130 が代表例であるとともに、本設計指針もここに位置する。

Profile Requirements や System Requirements を具体的に検討・設計する際の考え方や検討項目を列挙した設計手引書的な位置づけのものであり、セクタ（業界や企業、部署等）固有の特性や利用環境等を考慮して当該セクタ内で共通に実現すべき要求事項（設計・運用要件等）にブレークダウンしたプロファイルを作成する際の指針となるように作られている。このため、どのような要求仕様／設計方法を採用するかは、CKMS 設計者、又は SP800-130 や本設計指針に基づいた Profile Requirements のような他のドキュメントに委ねられる。

② 「Profile Requirements」:
セクタ固有の特性や環境を踏まえたセクタ内で共通に実現すべき要求事項(設計方針・運用要件等）を規定したものである。セクタ内での相互運用システムにおいて満たさなければならないセキュリティと相互運用性に関わる要求事項一式を規定するようなものであり、Framework Requirements に記載されている項目一覧に沿って、Guidance の技術的根拠を加味しながらセクタでの必要性を満たすように選択､増補、あるいは精緻化される。

③ 「System Requirements」:
システム個別の利用環境や条件等を考慮して作成された、実際の CKMS が実現すべき具体的な設計仕様書や運用マニュアル等のことである。システムが依存する利用環境や条件等と Guidance の技術的根拠の両方を加味して、参照する Profile Requirements に適合するように選択、増補、あるいは精緻化され、具体的な技術仕様として取りまとめられる。

④ 「Guidance」:
暗号鍵管理についての技術的な理解を助け、推奨設定などを提供する文献のことである。Framework Requirements から Profile Requirements を、また Profile Requirements から System Requirements を策定する場合の選択や精緻化おける技術的根拠となるものである。

第二の視点：暗号鍵管理における検討項目

SP800-130 に記載されているトピックスや Framework Requirements を大きく以下の 6 つの『暗号鍵管理における目的（取り扱い項目）に応じた対象範囲』に分類・グループ化することによって、検討すべき項目の目的や必要性を明確化し、分かりやすく整理し直した。それら 6 つの目的の関係性を図 2-2 に示す。これにより、対象とする CKMS の利用環境に応じて本当に必要な検討項目をあらかじめ抽出することができ、効率よく CKMS 設計・構築に反映できると期待している。

第三の視点：暗号鍵管理における時間管理

暗号鍵管理においては「時間」の概念が非常に重要である。本設計指針では、時間管理の概念を図 2-3 のように整理した。これにより、時間管理の中で、いつまでに何を準備しなければならないのかを判断し、仕様書や運用マニュアルに組み入れることができるようになると考えている。

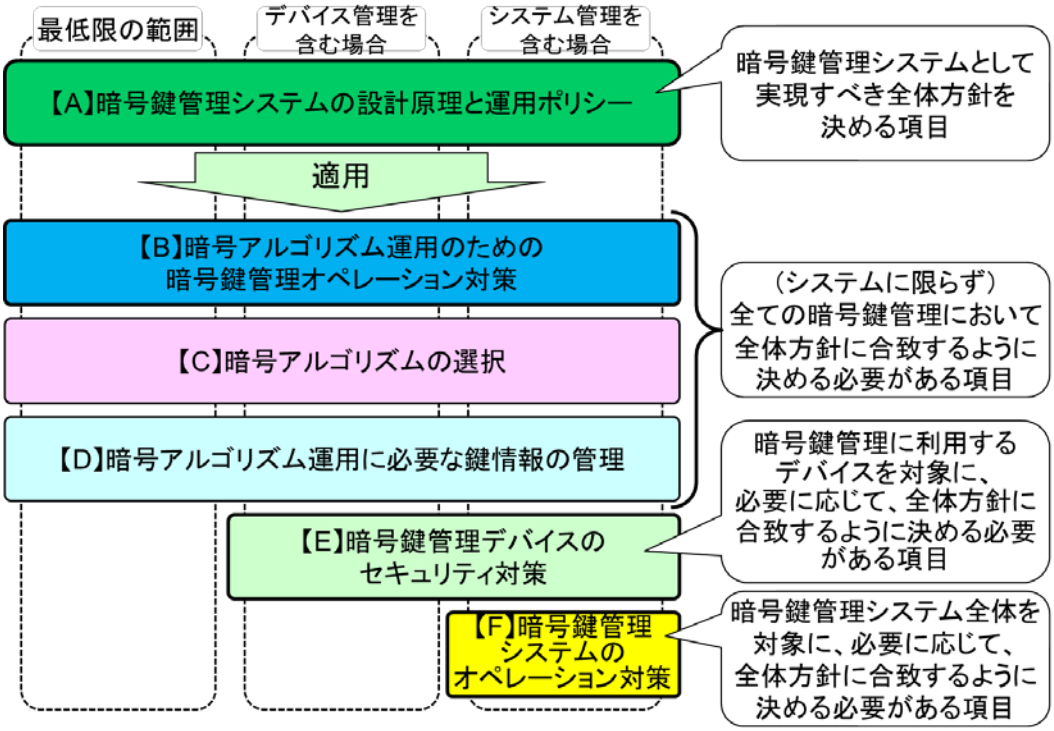

図 2-2　暗号鍵管理における目的別分類関係

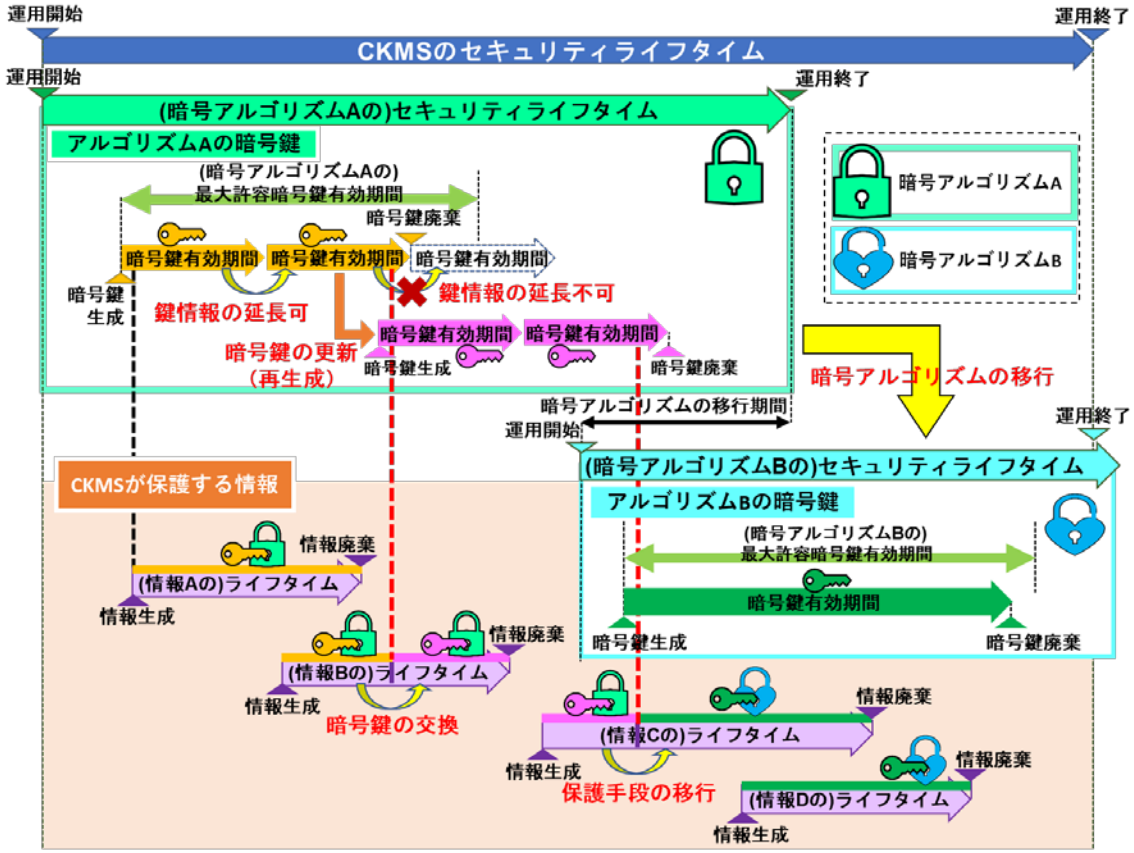

図 2-3　暗号鍵管理における時間管理の概念図

- CKMS のセキュリティライフタイム：
  CKMS の運用開始から運用終了までの期間のことをいう。

- （暗号アルゴリズムの）セキュリティライフタイム：
  暗号アルゴリズムが利用できる運用開始から運用終了までの期間のことをいう。この期間が CKMS のセキュリティライフタイムよりも短ければ、将来的によりセキュリティ強度が高い暗号アルゴリズムへの移行が必要となる（「暗号アルゴリズムの移行」）。

- （情報の）ライフタイム：
  情報が生成されてから廃棄されるまでの期間のことをいう。通常、この期間全体にわたって情報が保護されるようにする必要がある。
  もしこの期間中に、情報を保護するために利用している暗号鍵が廃棄・失効することがあれば、暗号鍵を交換したうえで、再度保護しなおす必要がある（「暗号鍵の交換」）。
  また、利用している暗号アルゴリズムのセキュリティライフタイムが終了する場合には、暗号鍵だけでなく暗号アルゴリズムも交換したうえで、再度保護しなおす必要がある（「保護手段の移行」）。

- 最大許容暗号鍵有効期間：
  同一の鍵情報（暗号鍵やメタデータ）が利用可能な期間の最大許容値のことをいう。この期間を超えて同一の鍵情報（暗号鍵やメタデータ）が利用され続けてはならない（「暗号鍵の延長不可」）。

- 暗号鍵有効期間：
  鍵情報（暗号鍵やメタデータ）が生成されてから廃棄される（予定を含む）までの期間のことをいう。暗号鍵の更新処理を行って新たに設定される廃棄時期が最大許容暗号鍵有効期間内であれば、その廃棄時期まで同一の鍵情報（暗号鍵やメタデータ）を継続して使うこともできる（「暗号鍵の延長可」）。

<u>第四の視点：本設計指針の具体的な活用方法</u>

CKMS の Profile Requirements や System Requirements を作成する設計者を対象に、具体的なプロファイルや仕様書等を作成する際に本設計指針を活用することを想定している。加えて、作成されたプロファイルや仕様書等が漏れなく適切な検討を踏まえて作成されたものであるかどうかをシステム管理責任者や調達責任者が確認・比較できるようにすること期待している。

- CKMS 設計者にとっての具体的な活用方法：

a) Framework Requirements の目的及びそれに続く概要に照らし合わせて、個々のトピックスが今回設計する CKMS が取り扱う対象範囲であるかどうかの判断を行う。対象範囲と判断すれば b）に進み、対象範囲外と判断すれば c）に進む。

b) 対象範囲の Framework Requirements ごとに、どのような要求仕様／設計方法を採用するか、あるいはどのような対応をとるかを決定し、その内容を要求事項として Profile Requirements や System Requirements に記載する。なお、一つの Framework Requirements に対して要求事項は一つとは限らず、複数となる場合もある。

c) 対象外と判断すればそのように判断した理由を明記したうえで当該 Framework Requirements は「対象外」と除外する。

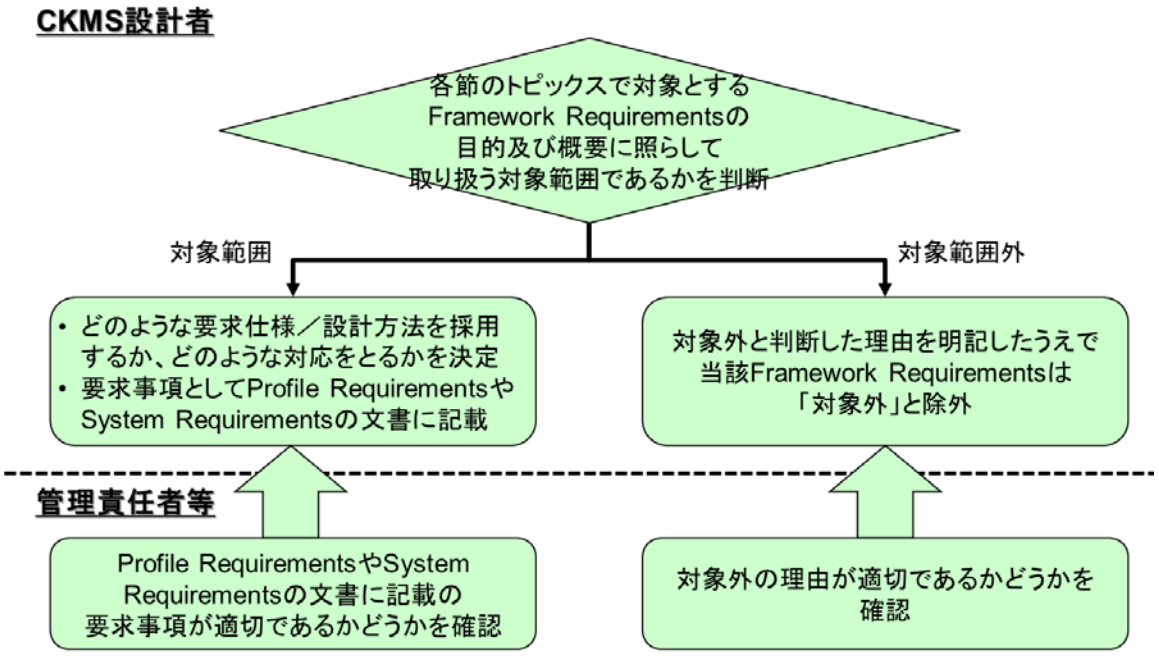

図 2-4　本設計指針の活用方法

- システム管理責任者や調達責任者等にとっての具体的な活用方法：

d) Framework Requirements ごとに、Profile Requirements や System Requirements に記載された要求事項の内容が適切であるかどうかを確認する。また、対象外と判断された項目については、対象外と判断した理由が適切であるかどうかを確認する。

2.2. TLS 暗号設定ガイドラインの作成

SSL/TLS 暗号設定ガイドライン（version 1.x/2.x）発行以降、TLS1.3 発行[RFC8446]及び SSL3.0 禁止[RFC7525]、ChaCha20-Poly1305 追加[RFC7905]及び RC4 禁止[RFC7465]など、同ガイドラインに記載の内容に大きく影響する規格化が相次いで行われており、それに伴い SSL/TLS の利用環境も大きく変化した。実際、SSL Pulse の集計データによれば、図 2-5 のようにプロトコルバージョンや暗号アルゴリズム等のサポート状況に大きな変動が発生していることがわかる。

そこで、2020 年 3 月時点における TLS 通信での安全性と相互接続性のバランスを踏まえた TLS サーバの設定方法におけるガイドラインの内容を大幅に見直すことを目的として、TLS 暗号設定ガイドライン WG 活動計画に基づき、TLS ガイドライン WG では以下の論点について 4 回にわたって議論を行った。

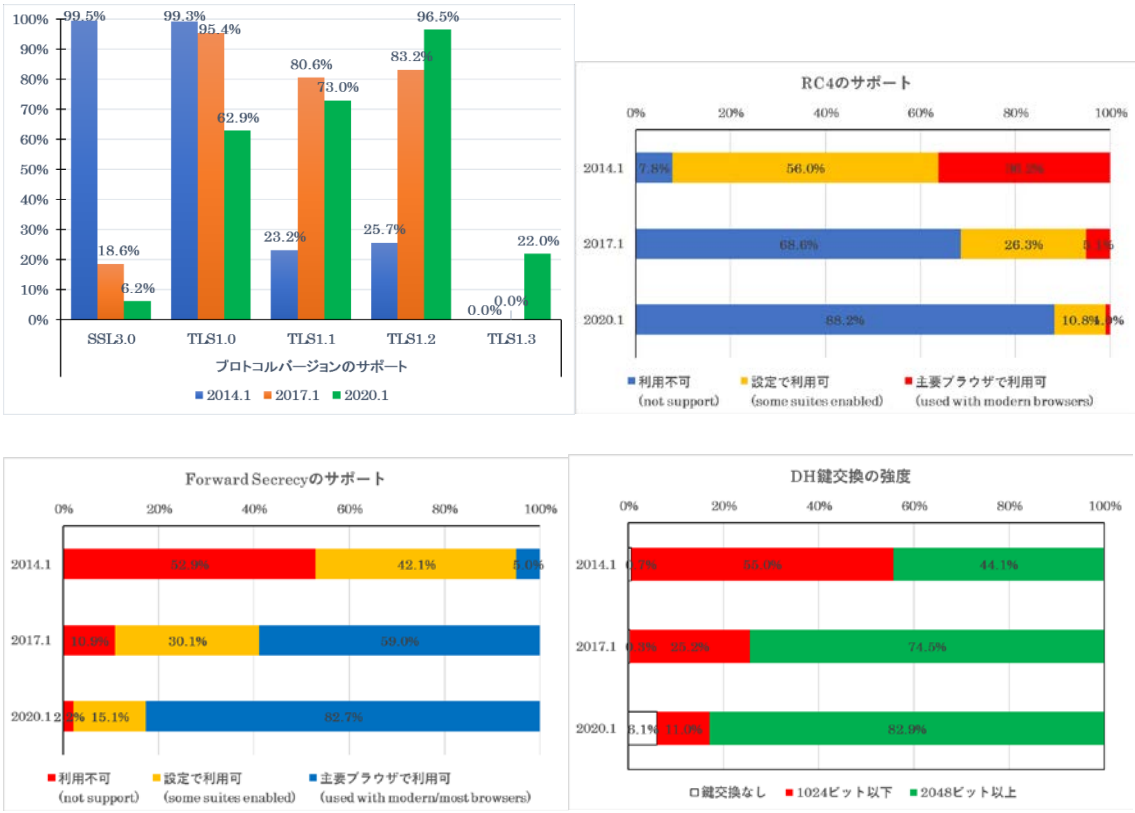

図 2-5　SSL Pulse による集計データを加工

① ガイドライン名の名称変更
② 3 段構成の概要の見直し
③ 推奨プロトコルバージョンの見直し
④ サーバ証明書推奨設定の見直し
⑤ 推奨暗号スイートの見直し
⑥ 具体的な設定方法の見直し
⑦ 情報提供として記載している内容の見直し
⑧ ブラウザでの標記に関する留意点の見直し
⑨ （専用）サーバ―ブラウザ以外も含めた利用形態
⑩ 常時 HTTPS 化に伴う留意点
⑪ コラム

IETF での規格化状況及び SSL Pulse に見られるようなサポート状況の変化等の各種動向を踏まえた TLS ガイドライン WG での検討の結果、大きく以下の 3 点を改訂した。

A) TLS1.3 の採用及び SSL3.0 の禁止に伴う各設定基準における要求設定の変更

プロトコルバージョンの要求設定において TLS1.3 の採用及び SSL3.0 の禁止が行われた。これに伴い、各設定基準における要求設定についても大幅な変更が行われており、SSL/TLS 暗号設定ガイドライン（version 1.x/2.x）における設定基準から一段階高い安全性を求めるようになった項目も多い（図 2-6、表 2-1 参照）。例えば、推奨セキュリティ型で利用が認められていた TLS1.0 や TLS1.1 は、本ガイドラインではセキュリティ例外型のみで利用可能となった。また、鍵交換では Perfect Forward Secrecy の特性をもつ ECDHE や DHE をさらに強く推奨するようにした。

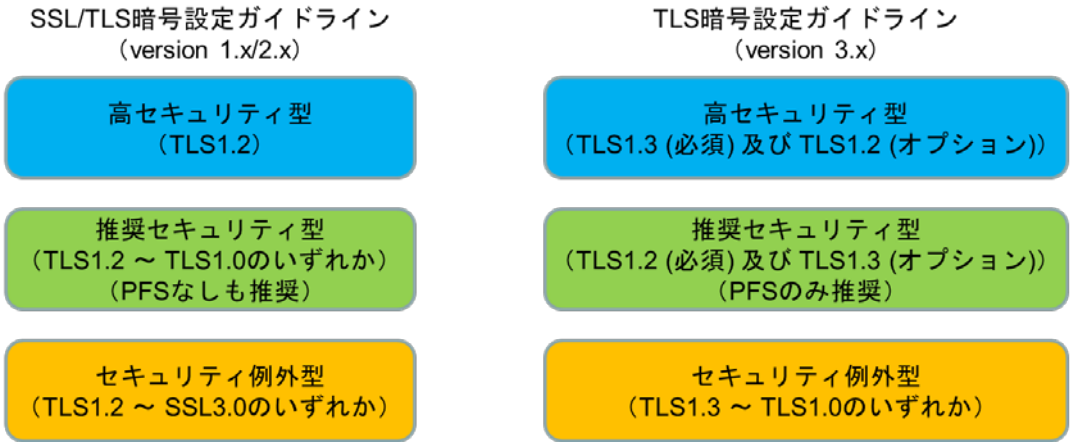

図 2-6 設定基準における要求設定の変更

表 2-1　要求設定の概要

要件		高セキュリティ型	推奨セキュリティ型	セキュリティ例外型
【遵守】想定対象		高い安全性の確保を必要とするケース	一般的な利用形態	推奨セキュリティ型への移行完了までの暫定運用
【遵守】暗号アルゴリズム		高セキュリティ型での利用禁止暗号を利用不可	推奨セキュリティ型での利用禁止暗号を利用不可	セキュリティ例外型での利用禁止暗号を利用不可
【遵守】バージョン		TLS1.3 (必須) 及び TLS1.2 (オプション)	TLS1.2 (必須) 及び TLS1.3 (オプション)	TLS1.3 ～ TLS1.0 のいずれか
【推奨】推奨暗号アルゴリズム設定	鍵交換	①256 ビット以上の ECDHE ②2048 ビット以上の DHE	①256 ビット以上の ECDHE ②2048 ビット以上の DHE	①1024 ビット以上の DHE 又は 256 ビット以上の ECDHE ②2048 ビット以上の RSA, 1024 ビット以上の DH, 256 ビット以上の ECDH のいずれか
	暗号化	128 ビット及び 256 ビットの AES 又は Camellia、もしくは ChaCha20-Poly1305		128 ビット及び 256 ビットの AES 又は Camellia、もしくは ChaCha20-Poly1305
	暗号利用モード	GCM, CCM, CCM_8 のいずれか	①GCM, CCM, CCM_8 のいずれか ②CBC	①GCM, CCM, CCM_8 のいずれか ②CBC
	ハッシュ関数	SHA-384 又は SHA-256	①SHA-384 又は SHA-256 ②SHA-1	SHA-384, SHA-256, SHA-1 のいずれか
【遵守】サーバ証明書	公開キー	鍵長 2048 ビット以上の RSA 又は 256 ビット以上の ECC		鍵長 2048 ビット以上の RSA
	署名アルゴリズム	鍵長 2048 ビット以上の RSA 又は 256 ビット以上の ECDSA		鍵長 2048 ビット以上の RSA
	ハッシュ関数	SHA-256 以上	SHA-256	SHA-256

凡例：　【遵守】遵守項目　　【推奨】推奨項目

B) **要求設定における「遵守項目」と「推奨項目」の区分けの新設**

SSL/TLS 暗号設定ガイドライン（version 1.x/2.x）では全ての設定項目について一律に「要求設定」と位置付けていた。

今回は、設定項目のおける安全性への寄与度を考慮し、TLS 暗号設定ガイドライン（version 3.x）では、選択した設定基準としての最低限の安全性を確保するために必ず満たさなければならない「遵守項目」と当該設定基準としてよりよい安全性を実現するために満たすことが望ましい「推奨項目」とに分け、より現実的かつ実効性が高い要求設定とした。

具体的な要求設定の区分けは表 2-2 の通りである。

表 2-2　要求設定における遵守項目と推奨項目

要求設定	遵守項目	プロトコルバージョン	利用禁止プロトコルバージョンを利用不可にする設定
		サーバ証明書	利用する暗号アルゴリズムと鍵長の設定
			発行・更新時の鍵情報の生成方法の明確化
			警告表示の回避方法の明確化
		暗号スイート	利用禁止暗号アルゴリズムを利用不可にする設定
			公開鍵暗号の鍵長の設定
	推奨項目	プロトコルバージョン	利用プロトコルバージョンの優先順位付け
		暗号スイート	利用推奨暗号アルゴリズムのみでの設定
			推奨暗号スイートの優先順位付け

C) **章構成の変更**

SSL/TLS 暗号設定ガイドライン（version 1.x/2.x）では、

- プロトコルバージョンの設定（4 章）
- サーバ証明書の設定（5 章）
- 暗号スイートの設定（6 章）

の章構成とし、各章に「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」の設定項目を記載していた。

今回、章構成を見直し、TLS 暗号設定ガイドライン（version 3.x）では、

- 推奨セキュリティ型の要求設定（4 章）
- 高セキュリティ型の要求設定（5 章）
- セキュリティ例外型の要求設定（6 章）

の章構成とし、各章に「プロトコルバージョン」「サーバ証明書」「暗号スイート」の設定項目を記載した（図 2-7 参照）。これにより、選択した設定基準での該当章だけを参照すればよ

い構成とした。

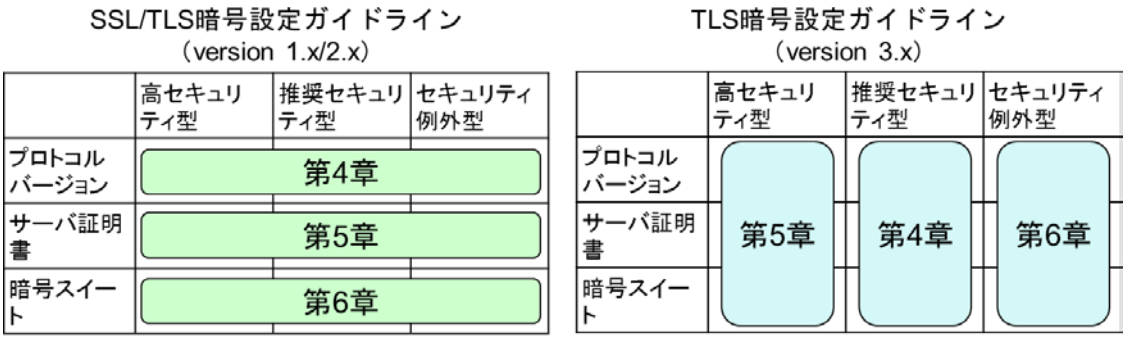

図 2-7　章構成の変更

今回作成した TLS 暗号設定ガイドラインは、以下のホームページよりダウンロードすることができる。

https://www.cryptrec.go.jp/op_guidelines.html

- TLS 暗号設定ガイドライン：

https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

- TLS 暗号設定ガイドライン：
- チェックリスト：
- TLS 暗号設定　サーバ設定編
- TLS 暗号設定　暗号スイートの設定例

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。特に高度な内容は含んでおらず、TLS 及び暗号についての技術的な基礎知識を有している読者は本章を飛ばしてもらって構わない。

3 章では、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す。

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 TLS サーバの要求設定について示す。安全性と相互接続性を踏まえたうえで、選択した設定基準としての最低限の安全性を確保するために必ず満たさなければならない項目である「遵守項目」と、当該設定基準としてよりよい安全性を実現するために満たすことが望ましい項目である「推奨項目」を決めている。

7 章では、チェックリストの対象には含めていないが、TLS を安全に使うために考慮すべきことをまとめている。本章の内容は、「情報提供」の位置づけとして記載している。

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。本章の内容は、7 章と同様、「情報提供」の位置づけのものである。

9 章は、そのほかのトピックとして、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。本章の内容も「情報提供」の位置づけのものである。

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、安全性と相互接続性を踏まえたうえで設定すべき要求設定として 3 つの設定基準（「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」）を提示している。

実際にどの設定基準を採用するかは、安全性の確保と相互接続の必要性の両面を鑑みて、サーバ管理やサービス提供に責任を持つ管理者が最終的に決定すべきことではあるが、本ガイドラインでは、安全性もしくは相互接続性についての特段の要求がなければ「推奨セキュリティ型」の採用を強く勧める。本ガイドラインの発行時点では、「推奨セキュリティ型」がもっとも安全性と相互接続性のバランスが取れている要求設定であると考えている。

Appendix 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等を記載している。チェックリストの目的は、「選択した設定基準に対応した要求設定の設定忘れの防止」と「サーバ構築の作業受託先が適切に要求設定を遵守したことの確認」を行うための手段となるものである。

2.3. EdDSA に関する安全性評価の必要性についての検討

EdDSA は、TLS1.3 で採用された署名アルゴリズムである（RFC 8446）。さらに、TLS1.2 以前では、ECDSA と同じ暗号スイートを使って EdDSA も利用可能となった（RFC8422）。

TLS1.3 では楕円曲線暗号がベース仕様になると記載されており、また NIST は、2018 年以降、再三にわたり、米国政府デジタル署名の次回改定版となる FIPS186-5 において EdDSA を追加する方針を明らかにしている。実際、2019 年 11 月に公表された FIPS186-5 ドラフト版に EdDSA が追加されている。

このように TLS で EdDSA を利用できる環境が整備されつつあるため、現状では楕円曲線暗号では ECDSA が使われることが多いものの、近いうちに EdDSA も TLS で利用される

ようになる可能性が十分にあると TLS ガイドライン WG では判断した。今後の利用状況によっては、早晩、TLS 暗号設定ガイドラインを改訂し EdDSA を推奨暗号スイートに含めるか否かを判断する必要に迫られると思われる。

一方、TLS 暗号設定ガイドラインで推奨暗号スイートに含める暗号アルゴリズムは CRYPTREC 暗号リスト（原則として「電子政府推奨暗号リスト」又は「推奨候補暗号リスト」）に掲載されるものとしているため、EdDSA を推奨暗号スイートに含めるためには、EdDSA が CRYPTREC 暗号リストに掲載されるか、少なくとも CRYPTREC 暗号リストに掲載されている暗号アルゴリズムと同程度の安全性を有していることを確認する必要がある。

このため、暗号技術活用委員会では EdDSA に関する安全性評価の必要性について検討を行った。その結果、今後 EdDSA の利用が進み、TLS 暗号設定ガイドラインに EdDSA を推奨暗号スイートに含めるか否かの判断が迫られた際に速やかに対応できるように準備をしておく観点から、EdDSA に対して CRYPTREC 暗号リストへの掲載是非に資するレベルでの安全性評価を実施することが必要であるとの結論を取りまとめた。併せて、EdDSA では利用する楕円曲線パラメータが Ed25519 と Ed448 であるため、楕円曲線パラメータについて、Ed25519 が P-256 と、Ed448 が P-384 と同程度の安全性を有する楕円曲線パラメータであるかどうか評価することの必要性も指摘した。

この結論は暗号技術検討会に報告された。

2.4. RC4 の運用監視暗号リストからの削除についての検討

RC4 は運用監視暗号リストに掲載されており、かつ（注 10）として「互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。」と記載されている。また、平成 15 年～平成 25 年に使われていた前の電子政府推奨暗号リストにおいても、「128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。」との注釈が付記されている。

今回、TLS 暗号設定ガイドラインにおいて RC4 が TLS での利用禁止暗号アルゴリズムに指定された以上、注釈が想定している例外的な利用形態そのものが存在しなくなると判断される。そのため、暗号技術活用委員会としては、RC4 を運用監視暗号リストに掲載しておく必要性がなくなったと判断し、同リストからの削除についての検討を行った。併せて、運用監視暗号リストからの削除ルール（案）の検討も行った。

この結論は暗号技術検討会に報告された。

【運用監視暗号リストからの削除ルール（案)】

運用監視暗号リストに掲載されている暗号アルゴリズムについて、以下の条件のいずれかを満たすと暗号技術検討会が決定した場合、同リストからの削除猶予期間を定めて周知を行ったうえで、その期間の満了後に同リストから自動的に削除する。

＜削除条件＞

1. 運用監視暗号リストに掲載している注釈で示した互換性維持のための利用形態が必要なくなり、削除が妥当と判断した場合
2. 互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと判断した場合
3. その他、運用監視暗号リストに掲載している必要性の根拠を満たさなくなったと判断した場合

【RC4 の運用監視暗号リストからの削除（案)】

- RC4 は削除条件 1.を満たすと判断する。RC4 を運用監視暗号リストから令和 3 年 3 月 31 日に削除する。
- CRYPTREC ホームページ等を活用し、削除する旨の周知を強化する。

第3章　今後に向けて

「暗号鍵管理システム設計指針（基本編）」及び「TLS 暗号設定ガイドライン」の作成完了に伴い、今後も運用ガイドラインの拡充を図っていく観点から、新たなに作成するガイドラインのテーマを選定した後、具体的な検討作業を行う予定である。

CRYPTREC Report 2019
(暗号技術活用委員会報告 CRYPTREC RP-3000-2019)

発行日　2020年7月31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