資料１

2017 年度 暗号技術検討会

平成３０年３月２９日
１５：００～１７：００
経　済　産　業　省
本館２階西３共用会議室

議事次第

１．開会

２．議事

（１） 文章番号体系について【報告】
（２） 2017 年度 暗号技術評価委員会 活動報告について【承認】
（３） 2017 年度 暗号技術活用委員会 活動報告について【承認】
（４） CRYPTREC 暗号リストの改定について【審議】
（５） 2017 年度 暗号技術検討会 報告書（案）について【承認】
（６） その他

３．閉会

配布資料 一覧

資料１	議事次第・配布資料一覧
資料２	2017 年度 暗号技術検討会 構成員等名簿
資料３	CRYPTREC 文書に対する文書番号の付番方法について
資料４	2017 年度 暗号技術評価委員会 活動報告
資料４別添１	768 ビット素数位数の有限体上の離散対数問題の状況と DSA, DH の今後のパラメータ選択について
資料４別添２	2017 年度 暗号技術調査 WG（暗号解析評価）活動報告
資料４別添３	「暗号技術ガイドライン(SHA-1)」改定案
資料５	2017 年度 暗号技術活用委員会 活動報告
資料５別添１	「SSL/TLS 暗号設定ガイドライン」改定案
資料５別添２	「SSL/TLS 暗号設定ガイドライン」改定案（詳細）
資料６	CRYPTREC 暗号リストの改定について
資料６別添１	3-key Triple DES 及び 64 ビットブロック暗号の今後の利用について
資料６別添２	ChaCha20-Poly1305 の CRYPTREC 暗号リスト追加について
資料６別添３	CRYPTREC 暗号リスト改定案
資料６別添４	CRYPTREC 暗号リスト
資料７	暗号技術検討会 2017 年度 報告書（案）

以上

資料２

暗号技術検討会　構成員・オブザーバ名簿

2018.3.29 現在

（構成員）

	今井　正道	一般社団法人情報通信ネットワーク産業協会　常務理事
	上原　哲太郎	立命館大学　情報理工学部　教授
	宇根　正志	日本銀行　金融研究所　情報技術研究センター　情報技術研究グループ長
	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　教授
	岡本　龍明	日本電信電話株式会社　セキュアプラットフォーム研究所 岡本特別研究室　室長
	高木　　剛	国立大学法人東京大学　大学院情報理工学研究科　教授
	近澤　　武	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　主任研究員
	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
	本間　尚文	国立大学法人東北大学　電気通信研究所　教授
	松井　　充	三菱電機株式会社　開発本部　役員技監
	松浦　幹太	国立大学法人東京大学 生産技術研究所　教授
座長	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
	松本　　泰	セコム株式会社　IS 研究所 コミュニケーションプラットフォームディビジョン　マネージャー
	向山　友也	一般社団法人テレコムサービス協会　技術・サービス委員会　委員長
	渡邊　　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　研究企画室長

（五十音順、敬称略）

（オブザーバ）

山本　雅亮	内閣官房内閣サイバーセキュリティセンター 内閣参事官（政府機関総合対策担当）
小川　久仁子	個人情報保護委員会事務局　参事官
種田　英明	警察庁　情報通信局　情報管理課　情報セキュリティ対策官
小高　久義	総務省　行政管理局　行政情報システム企画課　情報システム管理室長
阿部　知明	総務省　自治行政局　住民制度課長
村松　秀樹	法務省　民事局　商事課長
小川　秀俊	外務省　大臣官房　情報通信課長
佐野　美波	財務省　大臣官房　文書課　業務企画室長
溝口　浩和	文部科学省　大臣官房　政策課　情報システム企画室長
中山　　理	厚生労働省 大臣官房参事官(サイバーセキュリティ・情報システム管理担当)
森田　健太郎	経済産業省　産業技術環境局　国際電気標準課長
二宮　　勉	防衛省　整備計画局　情報通信課　サイバーセキュリティ政策室長
宮崎　哲弥	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長
寶木　和夫	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　副研究部門長
江口　純一	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長
大澤　昭彦	一般財団法人日本情報経済社会推進協会　電子署名・認証センター長
和田　昌昭	公益財団法人金融情報システムセンター　監査安全部長

（敬称略）

資料３

CRYPTREC 文書に対する文書番号の付番方法について

これまで年度成果物として公開されてきたガイドラインや報告書について、文書番号から内容（及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が 2016 年度の暗号技術検討会にて承認された。

この承認を受けて、CRYPTREC 事務局で決定した文書番号の付番方法を報告する。

1. 基本的な考え方

1.1. CRYPTREC 文書の定義

表 1.1 に示す文書類を CRYPTREC 文書として、文書番号の付番対象とする。

ただし、暗号技術検討会または各委員会の成果物によっては、必要性に応じて、文書番号の新たな付番対象とすることがある。

表 1.1 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 ・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 ・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）

1.2. 付番方法の基本ルール

文書番号のフォーマットは以下の通りとする。

文書番号 ::= CRYPTREC␣<カテゴリ>-<連番（4 桁）>-<管理情報>
(「␣」は空白を表す)

※ 文書番号に用いるアルファベットは、すべて大文字とする。

※ 文書番号が付番されたファイル名に用いるアルファベットは、すべて小文字とする。なお、空白は“-” (ハイフンマイナス)に変換する。

例） 文書番号： CRYPTREC␣LS-0001-2012R3
ファイル名： cryptrec-ls-0001-2012r3.pdf

- カテゴリ

  2018 年 3 月時点では、表 1.2 に示す 7 種のいずれかである。

表 1.2 カテゴリ一覧

CRYPTREC 文書カテゴリ	表記名	文書例
CRYPTREC 暗号リスト関係	LS	CRYPTREC 暗号リスト CRYPTREC 暗号リストと仕様書の対応関係表
年次報告書	RP	年次報告書
早期に公開する注意喚起	ER	注意喚起レポート
ガイドライン	GL	暗号技術ガイドライン 暗号運用ガイドライン
技術報告書	TR	調査 WG 報告書 推奨セキュリティパラメータ設定
外部評価報告書	EX	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
会議資料	MT	暗号技術検討会資料 各委員会資料

- 連番
  後述するカテゴリごとの指定にしたがって付番する。

- 管理情報
  後述するカテゴリごとの指定にしたがって付番する。付番方法に指定がない場合は、当該文書を作成する検討会／委員会が付番する。WG が作成するものは当該 WG を設置する検討会／委員会が付番する。

- 付加識別子
  文書の性質に応じて、管理情報に表 3 に示す共通の付加識別子を利用する。

表 1.3 管理情報への付加識別子

文書の性質		付加識別子
改定版の場合		“R” + リビジョン番号
正誤表単体の文書の場合		“E” + 正誤表番号
日本語版と英語版がある文書の場合	日本語版	JP
	英語版	EN

＜参考＞

- カテゴリが RP、GL、TR、MT の文書番号における連番で用いる際の「委員会／WG 番号」の一覧は、2018 年 3 月時点では表 1.4 のとおりである。当該カテゴリで連番の指定においては、「委員会／WG 番号」の必要な部分のみ抜粋している。

表 1.4　カテゴリが RP、GL、TR、MT の文書番号における連番フォーマット

1 桁目	2 桁目	3 桁目	4 桁目
委員会／WG 番号			

委員会／WG 名（2018 年 3 月時点）		番号
暗号技術検討会		10
	要件調査 WG	11
	CRYPTREC の在り方に関する検討グループ	12
	重点課題検討タスクフォース	13
暗号技術評価委員会（2000-2002） 暗号技術監視委員会（2003-2008） 暗号方式委員会（2009-2012） 暗号技術評価委員会（2013-）		20
暗号運用委員会（2009-2012） 暗号技術活用委員会（2013-）		30
暗号モジュール委員会（2003-2007） 暗号実装委員会（2008-2012）		40

2. LS（CRYPTREC 暗号リスト関係）の付番方法

- 連番

  2018 年 3 月時点では、以下の連番とする。

表 2.1 CRYPTREC 文書と連番の対応

文書名	連番
CRYPTREC 暗号リスト	0001
CRYPTREC 暗号リストと当該暗号アルゴリズム仕様書との対応関係表	0002

- 管理情報

  以下の通りに管理情報を付番する。
  - 暗号リストが「最初に発行された年度（西暦 4 桁）」を管理番号として付番し、全面改定までの「期間中は番号変更をしない」ものとする
  - 全面改定までの期間内での修正・小改定は修正版として取扱う
  - 暗号アルゴリズム仕様書のバージョンが変わったときには、対応関係表は当該年度（西暦 4 桁）を新たな管理番号として付番する

表 2.2 CRYPTREC 文書と管理情報の対応

文書名	管理情報
2002 年度発行電子政府推奨暗号リスト	2002
2004 年度注釈改定	2002R1
2012 年度発行 CRYPTREC 暗号リスト	2012
2014 年度注釈改定	2012R1
2015 年度発行 CRYPTREC 暗号リスト	2012R2
2016 年度発行 CRYPTREC 暗号リスト	2012R3

表 2.3 CRYPTREC 文書の付番例（CRYPTREC 暗号リスト関係）

文書名	文書番号
2016 年度発行 CRYPTREC 暗号リスト[1]	CRYPTREC LS-0001-2012R3
2012 年度発行 CRYPTREC 暗号リスト	CRYPTREC LS-0001-2012
2004 年度注釈改定（日本語版）	CRYPTREC LS-0001-2002R1-JP
2004 年度注釈改定（英語版）	CRYPTREC LS-0001-2002R1-EN
2002 年度発行電子政府推奨暗号リスト	CRYPTREC LS-0001-2002

3. RP（年次報告書）の付番方法

- 連番

  表 3.1 に示す連番フォーマットを利用する。
  - 1 桁目は委員会を表す番号、2 桁目は WG を表す番号（親委員会は 0）とする。
  - 同一目的の委員会は、名称が変更になっても同じ連番を利用する。
  - 3~4 桁目は委員会が規定するが、デフォルトは”00”とする。

表 3.1 連番フォーマット（年次報告書）

1 桁目	2 桁目	3 桁目	4 桁目
委員会／WG 番号		委員会が規定する。 ただし、デフォルトは「00」を利用	

委員会／WG 名（2018 年 3 月時点）	番号
暗号技術検討会	10
要件調査 WG	11
暗号技術評価委員会（2000-2002） 暗号技術監視委員会（2003-2008） 暗号方式委員会（2009-2012） 暗号技術評価委員会（2013-）	20
暗号運用委員会（2009-2012） 暗号技術活用委員会（2013-）	30
暗号モジュール委員会（2003-2007） 暗号実装委員会（2008-2012）	40

[1] 2018 年 3 月時点で、“CRYPTREC LS-2016-0001”の文書番号で公開されているが、今後の対応については第 9 章を参照されたい。

- 管理情報
  開催年度（西暦 4 桁）で付番する。

表 3.2 CRYPTREC 文書の付番例（年次報告書）

文書名	文書番号
暗号技術検討会 2016 年度報告書	CRYPTREC RP-1000-2016
CRYPTREC Report 2016 暗号技術評価委員会報告 [2]	CRYPTREC RP-2000-2016
CRYPTREC Report 2016 暗号技術活用委員会報告 [3]	CRYPTREC RP-3000-2016
CRYPTREC Report 2002 暗号技術評価報告書(2002 年度)	CRYPTREC RP-2000-2002-JP
CRYPTREC Report 2002 暗号技術評価報告書(2002 年度)正誤表	CRYPTREC RP-2000-2002E1-JP
CRYPTREC Report 2002; Report of the Cryptographic technique evaluation (FY 2002)	CRYPTREC RP-2000-2002-EN

4. ER（注意喚起）の付番方法

- 連番
  年度ごとに 0001 から通し番号で付番する。

- 管理情報
  公開年度（西暦 4 桁）で付番する。

表 4.1 CRYPTREC 文書の付番例（注意喚起）

文書名	文書番号
768 ビット素数位数の有限体上の離散対数問題の状況と DSA,DH の今後のパラメータ選択について	CRYPTREC ER-0001-2017
SHA-1 の安全性低下について	CRYPTREC ER-0001-2016
SHA-1 の安全性について	CRYPTREC ER-0003-2015
64 ビットブロック暗号 MISTY1 の安全性について（続報）	CRYPTREC ER-0002-2015
64 ビットブロック暗号 MISTY1 の安全性について	CRYPTREC ER-0001-2015
擬似乱数生成アルゴリズム Dual_EC_DRBG について	CRYPTREC ER-0001-2013
128 ビットブロック暗号 AES の安全性について	CRYPTREC ER-0001-2011

[2] 2018 年 3 月時点で、“CRYPTREC RP-0002-2016”の文書番号で公開されているが、今後の対応については第 9 章を参照されたい。
[3] 2018 年 3 月時点で、“CRYPTREC RP-0003-2016”の文書番号で公開されているが、今後の対応については第 9 章を参照されたい。

5. GL（ガイドライン）の付番方法

- 連番

  表 5.1 に示す連番フォーマットを利用する。

  - 1 桁目は委員会を表す番号、2 桁目は WG を表す番号（親委員会は 0）とする。
  - 同一目的の委員会は、名称が変更になっても同じ連番を利用する。
  - 3~4 桁目は委員会が規定する。

表 5.1 連番フォーマット（ガイドライン）

1 桁目	2 桁目	3 桁目	4 桁目
委員会／WG 番号		委員会が規定する。	

委員会／WG 名（2018 年 3 月時点）	番号
暗号技術評価委員会（2000-2002） 暗号技術監視委員会（2003-2008） 暗号方式委員会（2009-2012） 暗号技術評価委員会（2013-）	20
暗号運用委員会（2009-2012） 暗号技術活用委員会（2013-）	30

- 管理情報

  付番方法は指定しない。

表 5.2 CRYPTREC 文書の付番例（ガイドライン）

文書名	文書番号
CRYPTREC 暗号技術ガイドライン（軽量暗号）[4]	CRYPTREC GL-2003-2016JP
CRYPTREC 暗号技術ガイドライン（軽量暗号）（英語版）[5]	CRYPTREC GL-2003-2016EN
SSL/TLS 暗号設定ガイドライン（1.1 版）	CRYPTREC GL-3001-1.1
CRYPTREC 暗号技術ガイドライン（SSL/TLS における近年の攻撃への対応）	CRYPTREC GL-2002-2013
CRYPTREC 暗号技術ガイドライン（SHA-1）	CRYPTREC GL-2001-2013

6. TR（技術報告書）の付番方法

- 連番

  表 6.1 に示す連番フォーマットを利用する。

  - 1 桁目は委員会を表す番号、2 桁目は WG を表す番号（親委員会は 0）とする。
  - 同一目的の委員会は、名称が変更になっても同じ連番を利用する。
  - 3~4 桁目は委員会が規定する。

[4] 2018 年 3 月時点で、“CRYPTREC GL-0001-2016-J”の文書番号で公開されているが、今後の対応については第 9 章を参照されたい。

[5] 2018 年 3 月時点で、“CRYPTREC GL-0001-2016-E”の文書番号で公開されているが、今後の対応については第 9 章を参照されたい。

表 6.1 連番フォーマット（技術報告書）

1 桁目	2 桁目	3 桁目	4 桁目
委員会／WG 番号		委員会が規定する。	

委員会／WG 名（2018 年 3 月時点）	番号
暗号技術評価委員会（2000-2002） 暗号技術監視委員会（2003-2008） 暗号方式委員会（2009-2012） 暗号技術評価委員会（2013-）	20
暗号モジュール委員会（2003-2007） 暗号実装委員会（2008-2012）	40

- 管理情報
  付番方法は指定しない。

表 6.2 CRYPTREC 文書の付番例（技術報告書）

文書名	文書番号
2011 年度版リストガイド(DNSSEC)	CRYPTREC TR-2002-2011
2011 年度版リストガイド(IPsec)	CRYPTREC TR-2001-2011
CRYPTREC Report 2003 ブロック暗号を使った秘匿、メッセージ認証、及び認証暗号を目的とした利用モードの技術調査報告	CRYPTREC TR-2001-2003
CRYPTREC Report 2003 暗号モジュール評価基準 第 0 版	CRYPTREC TR-4000-2003
CRYPTREC Report 2003 暗号モジュール試験基準 第 0 版	CRYPTREC TR-4001-2003

7. EX（外部評価報告書）の付番方法

- 連番
  暗号技術評価委員会管理とし、4 桁数字を使うこと以外の付番方法は指定しない。

- 管理情報
  付番方法は指定しない。

表 7.1 CRYPTREC 文書の付番例（外部評価報告書）

文書名	文書番号
Security Analysis of ChaCha20-Poly1305 AEAD	CRYPTREC EX-0003-2016
楕円曲線上の離散対数問題に関する指数計算法	CRYPTREC EX-0002-2016
Cryptographic Multilinear Maps - A Status Report -	CRYPTREC EX-0001-2016
Integral 攻撃の最新動向と MISTY1 等への適用	CRYPTREC EX-0002-2015
Cryptographic Program Obfuscation	CRYPTREC EX-0001-2015

8. MT（会議資料）の付番方法

- 連番

  表 8.1 に示す連番フォーマットを利用する。

  - 1 桁目は委員会を表す番号、2 桁目は WG を表す番号（親委員会は 0）とする。
  - 同一目的の委員会は、名称が変更になっても同じ連番を利用する。
  - 3 桁目は委員会/WG の開催回、4 桁目は資料の種類とする。

表 8.1 連番フォーマット（会議資料）

1 桁目	2 桁目	3 桁目	4 桁目
委員会／WG 番号		開催回	資料の種類 0: 議事概要 1: 会議資料

委員会／WG 名（2018 年 3 月時点）		番号
暗号技術検討会		10
	要件調査 WG	11
	CRYPTREC の在り方に関する検討グループ	12
	重点課題検討タスクフォース	13
暗号技術評価委員会（2000-2002） 暗号技術監視委員会（2003-2008） 暗号方式委員会（2009-2012） 暗号技術評価委員会（2013-）		20
暗号運用委員会（2009-2012） 暗号技術活用委員会（2013-）		30
暗号モジュール委員会（2003-2007） 暗号実装委員会（2008-2012）		40

- 管理情報

  開催年度（西暦 4 桁）で付番する。

表 8.2 CRYPTREC 文書の付番例（会議資料）

文書名	文書番号
2016 年度 暗号技術検討会 議事概要	CRYPTREC MT-1010-2016
2016 年度 暗号技術検討会 資料	CRYPTREC MT-1011-2016
2015 年度 CRYPTREC の在り方に関する検討グループ 第 1 回 議事概要	CRYPTREC MT-1210-2015
2015 年度 CRYPTREC の在り方に関する検討グループ 第 1 回 資料	CRYPTREC MT-1211-2015
2015 年度 重点課題検討タスクフォース 第 1 回 議事概要	CRYPTREC MT-1310-2015
2015 年度 重点課題検討タスクフォース 第 1 回 資料	CRYPTREC MT-1311-2015

9. 今後の予定

上記の付番方法に基づいて、これまでの成果物である CRYPTREC 文書に対して、文章番号を付与するとともに、CRYPTREC ホームページのリニューアルに合わせて反映する予定である。

なお、2016 年度の成果物である CRYPTREC 文書は、既に文書番号が付番された上で公開されているが、表 9.1 に示す文書番号に改める。

表 9.1 文書番号を変更する CRYPTREC 文書

文書名	現在の文書番号	変更後の文書番号
2016 年度発行 CRYPTREC 暗号リスト	CRYPTREC LS-2016-0001	CRYPTREC LS-0001-2012R3
CRYPTREC Report 2016 暗号技術評価委員会報告	CRYPTREC RP-0002-2016	CRYPTREC RP-2000-2016
CRYPTREC Report 2016 暗号技術活用委員会報告	CRYPTREC RP-0003-2016	CRYPTREC RP-3000-2016
CRYPTREC 暗号技術 ガイドライン（軽量暗号）	CRYPTREC GL-0001-2016-J	CRYPTREC GL-2003-2016JP
CRYPTREC 暗号技術 ガイドライン（軽量暗号） （英語版）	CRYPTREC GL-0001-2016-E	CRYPTREC GL-2003-2016EN

資料４

2017 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

2.1. 暗号技術の安全性及び実装に係る監視及び評価

下記の通り、暗号技術の安全性に係る監視・評価 及び 実装に係る技術の監視・評価を実施した。

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 2017 で報告。

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格及び 運用監視暗号リストからの危殆化が進んだ暗号の削除

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

- 64 ビットブロック暗号を鍵を変えずに使い続ける場合の脅威を踏まえ、64 ビットブロック暗号に付与されている注釈の変更案を検討、暗号技術検討会に提案。
- 3-key Triple DES に付与されている注釈の変更と、3-key Triple DES を「電子政府推奨暗号リスト」から「運用監視暗号リスト」へ変更することを暗号技術検討会に提案。
  （資料６別添１参照）

③ CRYPTREC 注意喚起レポートの発行

CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会

議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。

- 電子政府推奨暗号リストに掲載されている DSA 及び DH の安全性にかかわる有限体上の離散対数問題について、位数が 768 ビット長の素数である有限体における離散対数の計算結果が示されたため、注意喚起レポートを発行し、CRYPTREC ホームページに公開した。
  (資料４別添１参照)

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加

標準化動向に鑑み電子政府システム等での利用が見込まれると判断される暗号技術の追加を検討する。

- ChaCha20-Poly1305 の安全性評価及び実装性能調査について外部評価を実施し、ChaCha20-Poly1305 が、認証暗号として十分な安全性および実装性能を有していると判断、暗号技術検討会に「推奨候補暗号リスト」への追加を提案。
  （資料６別添２参照）

⑤ 新技術等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)
  Post-Quantum Cryptography(耐量子計算機暗号)の技術動向調査を実施。
  （資料４別添２参照）

2.2. 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）性及び実装に係る監視及び評価

- SHA-1 の衝突発見を受け、「暗号技術ガイドライン(SHA-1)」を改定。
  （資料４別添３参照）

3. 開催状況

表１ 暗号技術評価委員会の開催状況

回	開催日	議題
第 1 回	2017 年 7 月 21 日	・暗号技術評価委員会の今年度活動計画の検討 ・暗号技術調査 WG（暗号解析評価）の活動計画の検討 ・外部評価(ChaCha20-Poly1305)についての検討 ・暗号技術ガイドライン(SHA-1)の改定の検討 ・64 ビットブロック暗号の今後の利用に関する検討 ・768 ビット素数の有限体上の離散対数問題の状況と DSA, DH の今後の利用についての注意喚起の検討 ・監視状況報告
第 2 回	2018 年 2 月 28 日	・暗号技術調査 WG（暗号解析評価）の今年度活動報告 ・3-key Triple DES 及び 64 ビットブロック暗号の今後の利用についての検討 ・暗号技術ガイドライン(SHA-1)改定案の検討 ・外部評価(ChaCha20-Poly1305 の安全性及び実装性能)の検討 ・監視状況報告 ・CRYPTREC Report 2017(暗号技術評価委員会報告)の目次案提示

4. 今後の予定

- 「暗号技術ガイドライン(SHA-1)」については、準備が整い次第 CRYPTREC ホームページに公開予定。
- 素因数分解問題の困難性に関する計算量評価については、作成から 10 年経過したことから、2018 年度に再評価を実施し、グラフの更新を図る予定。
- 暗号技術調査 WG（暗号解析評価）にて、耐量子計算機暗号（PQC）に関する技術動向調査を実施し、2018 年度に報告書を完成させる予定。

以上

委員構成

［暗号技術評価委員会］

委員長	太田　和夫	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	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	高木　剛	東京大学 大学院情報理工学系研究科　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	東北大学　電気通信研究所　教授
委員	松本　勉	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	秋田大学 大学院理工学研究科数理・電気電子情報学専攻 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・人間工学領域研究戦略部研究企画室 研究企画室長

［暗号技術調査ワーキンググループ(暗号解析評価)］

主査	高木　剛	東京大学 大学院情報理工学系研究科　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	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　研究主任
委員	國廣　昇	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&IoT セキュリティプロジェクト　主管研究員
委員	高島　克幸	三菱電機 情報技術総合研究所 松井暗号プロジェクトG　主席技師長
委員	安田　貴徳	岡山理科大学工学部 生命医療工学科　准教授
委員	安田　雅哉	九州大学 マス・フォア・インダストリ研究所　准教授

資料４別添１

768 ビット素数位数の有限体上の離散対数問題の状況と DSA, DH の今後のパラメータ選択について

平成 29 年 8 月 30 日
暗号技術評価委員会

有限体上の離散対数問題は、現在、CRYPTREC 暗号リストの電子政府推奨暗号リストに掲載されている DSA 及び DH や、インターネットで使われているセキュア通信プロトコル TLS における鍵共有方式など、多くの暗号技術の安全性の根拠として利用されています。

暗号技術評価委員会は、RSA1024 に係る移行指針と同様に、DSA や DH を利用する場合には、鍵長において、2048 ビット以上の素数位数の有限体を用いることを推奨します。

有限体上の離散対数問題[1]は、現在、CRYPTREC 暗号リストの電子政府推奨暗号リスト[2]に掲載されている DSA 及び DH や、インターネットで使われているセキュア通信プロトコル TLS[3]における鍵共有方式など、多くの暗号技術の安全性の根拠として利用されています。

CRYPTREC では、以前より、(素数位数の)有限体上の離散対数問題における安全なパラメータサイズは、RSA 合成数の素因数分解問題における安全なパラメータサイズと同等であると判断しています[4]。

今般、位数が 768 ビット長の素数である有限体(以下、768 ビットの素体という)における離散対数の計算結果を示した論文[5]が、国際暗号学会 (International Association for Cryptologic Research (IACR)) が主催する国際会議 EUROCRYPT 2017[6]で発表されました。この論文では、768 ビットの素体上の離散対数の計算に要する計算コストが、2.2 GHz Xeon E5-2660 プロセッサ換算で、約 5300 コア・年に相当するものと見積もられています。

768 ビットの RSA 合成数の素因数分解に要する計算コストは、CRYPTO2010 で発表された論文[7]では、約 1700 コア・年と見積もられているので、これらの計算コストの違いはたかだか数倍程度となります。これは上記の判断の妥当性の根拠の一つとみなせます。

このため、暗号技術評価委員会では、RSA1024 に係る移行指針[2, 8]と同様に、今後とも DSA や DH を利用する場合には、鍵長において、2048 ビット以上の素数位数の有限体を用いることを推奨します。

暗号技術評価委員会では、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 at cryptrec.go.jp

【本レポートは、暗号アルゴリズムの脆弱性に関する情報発信フロー(暗号技術検討会 2015 年度報告書[9]の 3.2.3.(2))における「C:長期的なシステムの安全性維持のための対策喚起」として発表しています。】

[1] 有限体の元である g と y が $y = g^x$ を満たすとき x を求める問題を有限体上の離散対数問題といいます。現在までのところ、大きな位数(元の総数)である有限体上の離散対数を計算することは、一般的に難しいこととされています。

[2] 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)
http://www.cryptrec.go.jp/images/cryptrec-ls-0001-2016.pdf

[3] T. Dierks et al., "The Transport Layer Security (TLS) Protocol Version 1.2", RFC5246,
https://tools.ietf.org/html/rfc5246

[4] CRYPTREC Report 2006,
http://www.cryptrec.go.jp/report/c06_wat_final.pdf

[5] T. Kleinjung et al., "Computation of a 768-bit prime field discrete logarithm",
https://eprint.iacr.org/2017/067

[6] https://eurocrypt2017.di.ens.fr/

[7] T. Kleinjung et al., "Factorization of a 768-bit RSA modulus",
https://eprint.iacr.org/2010/006

[8] 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」(平成 20 年 4 月 22 日 情報セキュリティ政策会議決定, 平成 24 年 10 月 26 日改定 情報セキュリティ対策推進会議決定)
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf

[9] 暗号技術検討会 2015 年度報告書
http://www.cryptrec.go.jp/report/c15_kentou_final.pdf

資料４別添２

2017 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

1.1. 耐量子計算機暗号の研究動向調査

近年、量子計算機が実用化されても安全性を保てると期待される暗号（耐量子計算機暗号：PQC）の調査・検討が各国で進められている。特に米国では NIST が PQC の公募を開始しており、欧州では ETSI が PQC の調査活動を行い、ISO/IEC でも標準化に向けた議論が始まっている。このように国内でも PQC の研究動向を把握する必要性がさらに高まっている。

2017 年度暗号技術評価委員会活動計画における「新技術等に関する調査及び評価」の活動として、PQC の技術動向を調査することが暗号技術検討会において承認された。暗号技術評価委員会では、暗号技術調査ワーキンググループ(暗号解析評価)を設置し、本調査を実施した。

- 耐量子計算機暗号（PQC）に関する近年の研究動向を調査し、報告書を作成する。（完成予定は 2018 年度末。）
- PQC の代表的な候補である、4 つの分類（格子暗号、符号ベース暗号、多変数公開鍵暗号、同種写像暗号）を調査対象とする。
- 上記の各分類において、該当する方式及び文献について三つの機能（暗号化、鍵交換、署名）の観点による整理等を実施する。

1.2. 予想図の更新

素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関して CRYPTREC が例年公表している予測図の更新を行った。

- 素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量の評価に大幅な変更がないかどうかの確認を行った。
- スーパーコンピュータのベンチマーク結果の 1 位から 500 位を 1993 年から半年毎に集計している Web サイト TOP500[1]における、2017 年 6 月・11 月のベンチマーク結果の追加を行った。

2. 委員構成

主査：高木 剛(東京大学)
委員：青木 和麻呂(NTT)
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：高島 克幸(三菱電機)
委員：安田 貴徳(岡山理科大学)

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

委員：安田 雅哉(九州大学)

3. 活動概要

3.1. スケジュール

- 第 1 回　2017 年 7 月 27 日(水)
  活動計画案や作業内容についての審議と了承
- 第 2 回　2018 年 2 月 21 日(水)
  活動計画案や作業内容についての審議と了承

3.2. 耐量子計算機暗号の研究動向調査

3.2.1 第 1 回 WG での実施内容及び決定事項

- 調査対象とする 4 つの分類項目について担当者を決定した：

	とりまとめ委員	執筆者
導入	高木主査・事務局	高木主査・事務局
① 格子暗号	下山委員	下山委員、安田(雅)委員、青野（事務局)
② 多変数公開鍵暗号	安田(貴)委員	安田(貴)委員
③ 符号ベース暗号	草川委員	草川委員
④ 同種写像暗号	高島委員	高島委員

- 4 つの分類において、調査対象を具体的に何にするかは、担当のとりまとめ委員を中心に決定する。
- 格子暗号及び符号ベース暗号については、2014 年度の報告書との差分を整理する。

方式及び文献についての報告書は、今後決定される執筆方針に基づいて執筆される。

3.2.2 主要なイベント等

- NIST における PQC の公募では、締め切り(2017 年 11 月 30 日)までに、82 件の方式が提案され、そのうち 69 件が書類選考を通過している。

表 1:米国 NIST 主催 PQC 標準化の書類選考後の提案数(仮分類)※

分類	署名	暗号化／鍵交換
格子暗号	5	21
多変数公開鍵暗号†	9	3
符号ベース暗号	3	17
同種写像暗号	0	1
上記以外のもの	5	7

※NIST から正式な発表はなく、WG で検討された仮分類である

†署名・暗号化両方に提案されている 2 件を含む

3.2.3 第 2 回 WG での実施内容及び決定事項

- スケジュールの修正について

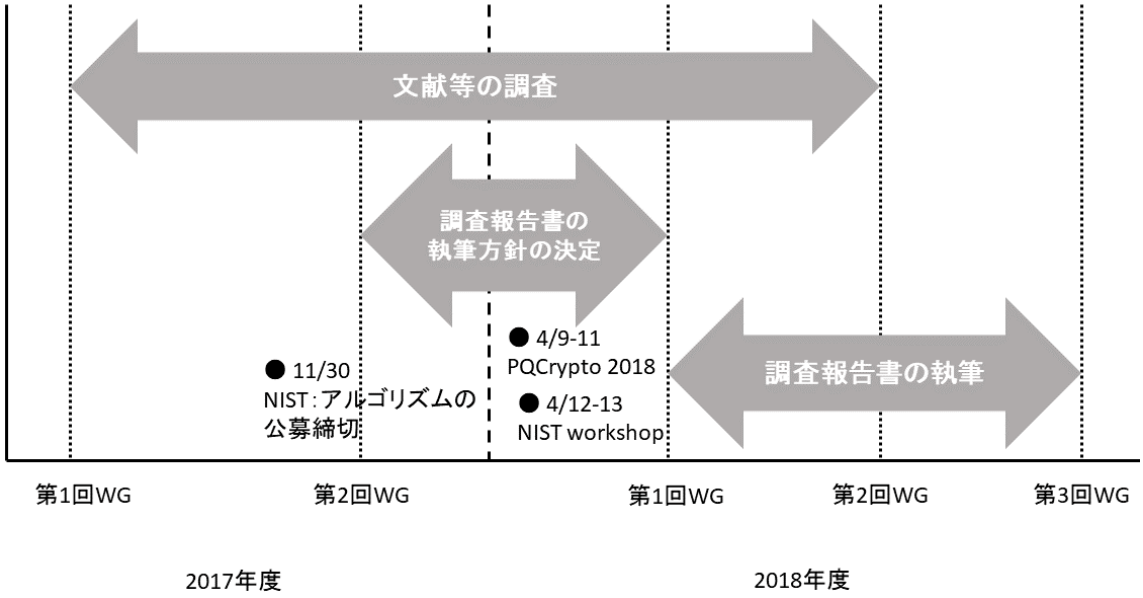
  来年度は三回の WG 実施を計画している。

  2017 年度第 2 回 WG（2018 年 2 月）：執筆方針の選択肢及びそれらへの意見を収集。

  2018 年度第 1 回 WG（2018 年 7 月）：執筆方針を決定する。

  2018 年度第 2 回 WG（2018 年 10 月）：報告書の中間報告。

  2018 年度第 3 回 WG（2019 年 2 月）：報告書完成。



- 執筆方針について

  本 WG では執筆方針を決定する上で重要な項目等を集めることを目的とし、執筆方針の決定自体は、主査・とりまとめ委員・事務局によるメール等での協議を経て、来年度の第 1 回 WG で正式に決定するものとしたい。また、執筆方針を決定する上で重要な項目等の候補を以下に列挙する：

  - 暗号化、署名、鍵交換のいずれに該当するか？
  - アルゴリズム
  - 暗号パラメータの値
  - セキュリティレベルおよびその根拠
  - 攻撃手法とその計算量
  - 実行する演算（鍵生成/暗号化/復号/符号化/検証 等）に必要な計算時間、及び全ての入力・出力（鍵、暗号文、署名など）のサイズ

3.3. 予想図の更新

- 素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、2017 年 6 月・11 月のベンチマーク結果を追加して予測図の更新を行った。

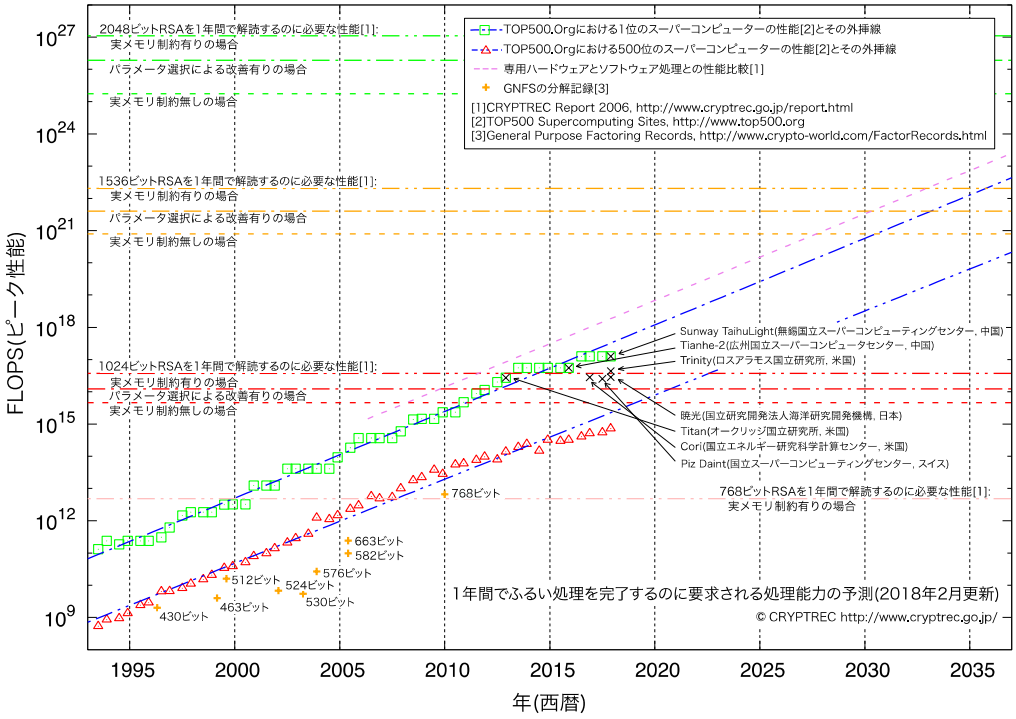


図 1：素因数分解の困難性に関する計算量評価

(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、2018 年 2 月更新)

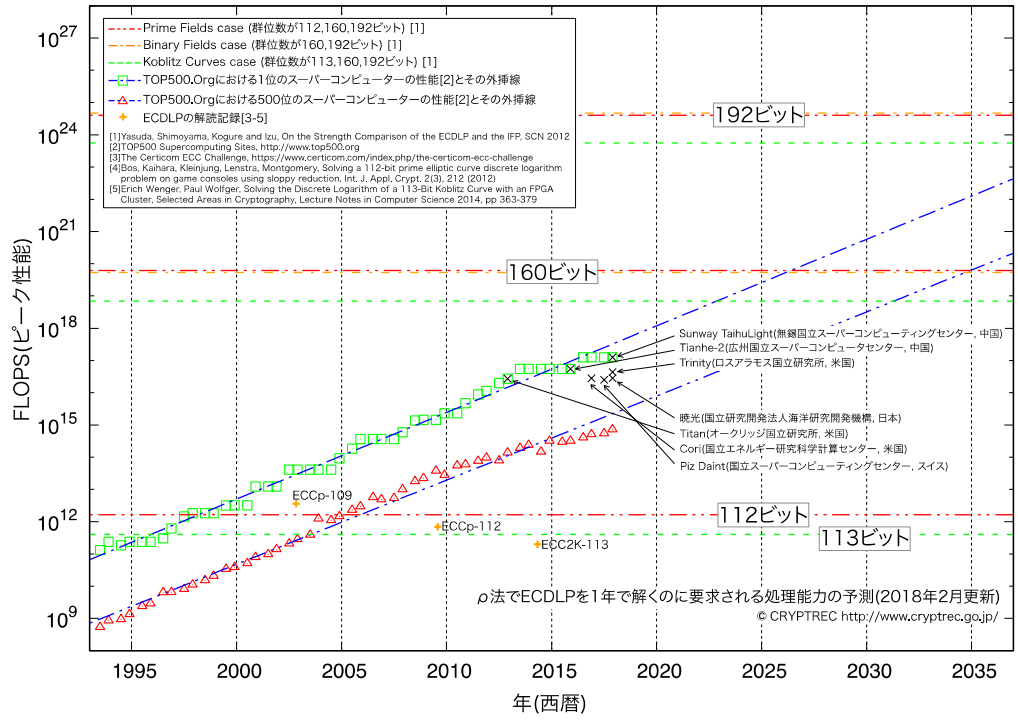


図 2：楕円曲線上の離散対数計算の困難性に関する計算量評価

(ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測、2018 年 2 月更新)

以上

資料4別添3

CRYPTREC 暗号技術ガイドライン (SHA-1)

（改定案）

（2018 年 3 月 16 日）
2018 年 3 月

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

目次

1. 本書の位置付け

1.1. 本書の目的

本書は、電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、「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)[C13a]の「運用監視暗号リスト」[1]に記載されているハッシュ関数 SHA-1 を継続して利用する際に参考となる指針を示すものである。そのために、運用監視暗号リストに記載されている SHA-1 を補助関数として用いる暗号技術が、互換性維持の目的であれば継続利用が容認されるかどうかを示す。

2 章において、SHA-1 を用いる補助関数のタイプ別に各々の暗号技術の継続利用の指針について示し、3 章において SHA-1 を用いる補助関数の種類と継続利用に関する詳細について示す。4 章において SHA-1 の危殆化に関する背景及びそれらに関連する参考情報について示す。

1.2. 本書の適用範囲

本書で取り扱う暗号技術は、1.2.1 節及び 1.2.2 節の範囲とする。

1.2.1. CRYPTREC 暗号リスト

本書で取り扱う暗号技術は、「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)[C13a]の「電子政府推奨暗号」[2]に記載されている暗号技術のうち、SHA-1 を利用する場合のあるものを対象とする(表 1)。

1.2.2. CRYPTREC 暗号の仕様書

本書で取り扱う暗号技術は、「CRYPTREC 暗号の仕様書」[C17b](2018 年 1 月現在)で指定されている仕様書を対象とする(表 1)。

---

[1] 実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

[2] CRYPTREC により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるが今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

表 1: 本書で対象となる暗号技術の範囲と仕様書

技術分類		暗号名称	仕様書
公開鍵暗号	署名	DSA	NIST FIPS PUB 186-4
		ECDSA	SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) または ANS X9.62-2005
		RSASSA-PKCS1-v1_5	Public-Key Cryptography Standards (PKCS)#1 v2.2
		RSA-PSS	Public-Key Cryptography Standards (PKCS)#1 v2.2
	守秘	RSA-OAEP	Public-Key Cryptography Standards (PKCS)#1 v2.2
	鍵共有	DH	ANS X9.42-2003 または NIST SP 800-56A Revision2 (May 2013)において FFC DH プリミティブとして規定されたもの
		ECDH	SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) または NIST SP 800-56A Revision2 (May 2013)において C(2e,0s,ECC CDH) として規定されたもの
メッセージ認証コード		HMAC	NIST FIPS PUB 198-1
エンティティ認証		ISO/IEC 9798-3	ISO/IEC 9798-3:1998, ISO/IEC 9798-3:1998/Amd 1:2010, ISO/IEC 9798-3:1998/Cor 1:2009, ISO/IEC 9798-3:1998/Cor 2:2012

1.3. 注意事項

本書の内容は、2018 年 1 月時点の情報に基づき記載されている。今後、CRYPTREC 暗号リストの改定や攻撃方法の進展状況等によって、本書に掲載される内容が現実にそぐわないケースが発生する可能性がある。

CRYPTREC では、SHA-1 の安全性に関する見解などを公表してきたが、内閣サイバーセキュリティセンター (National center of Incident readiness and Strategy for Cybersecurity、以下 NISC という。) や米国の国立標準技術研究所 (National Institute of Standards and Technology、以下 NIST という。) が示してきたような SHA-1 に関する利用期限については公表していない。

1.4. 謝辞

本書を作成するにあたり、セコム株式会社 IS 研究所の松本 泰 様、佐藤 雅史 様、島岡 政基 様、及び、NPO 日本ネットワークセキュリティ協会(JNSA) 電子署名 WG のメンバーの方々から有益なご意見・コメントいただいた。ここに謝意を表する。

2. CRYPTREC 暗号リストにおいて SHA-1 を補助関数として用いる電子政府推奨暗号の継続利用の指針

ハッシュ関数 SHA-1 は NIST が 1995 年に策定した、ハッシュ長が 160 ビットの暗号学的ハッシュ関数である [NT15b]。一般に、暗号学的ハッシュ関数には、衝突発見困難性[3]、第二原像計算困難性[4]及び原像計算困難性[5]の 3 つの安全性要件を満たすことが求められる。ところが、2017 年に SHA-1 は衝突発見困難性を満たしていないことが発表された[S17a, S17b]。

SHA-1 は、暗号技術の補助関数としてさまざまな部分で利用されており、CRYPTREC 暗号リストの多くの暗号技術において採用されている。その中には、衝突発見が安全性に直接的に影響を与えるものと与えないものが存在している。現状、実運用環境においては SHA-1 の継続利用を避けることが互換性維持の観点から現実的な選択肢ではない場面も想定されるため、CRYPTREC 暗号リストの電子政府推奨暗号リストにおいて補助関数として SHA-1 を用いる場合(ただし、擬似乱数生成系を除く[6])に、互換性維持の目的であれば継続利用が容認されるかどうかを示す(表 2)。

表 2: CRYPTREC 暗号リストにおいて SHA-1 を補助関数として用いる電子政府推奨暗号の継続利用の指針

技術分類	SHA-1 を補助関数として用いる暗号名称	継続利用の指針
署名	DSA, ECDSA, RSASSA-PKCS1-v1_5, RSA-PSS	署名生成については、 電子政府推奨暗号リストに記載された ハッシュ関数への移行を推奨 署名検証については、 互換性維持目的での継続利用は容認
守秘	RSA-OAEP	互換性維持目的での継続利用は容認
鍵共有	DH, ECDH	
メッセージ認証コード	HMAC	
エンティティ認証	ISO/IEC 9798-3	

[3] ハッシュ関数 Hash が衝突発見困難性を有するとは、$X_1 \neq X_2$ かつ Hash (X_1) = Hash (X_2) となる X_1, X_2 を見つけることが困難であることをいう。

[4] ハッシュ関数 Hash が第二原像計算困難性を有するとは、X_1 に対して、$X_1 \neq X_2$ かつ Hash (X_1) = Hash (X_2) となる X_2 を見つけることが困難であることをいう。

[5] ハッシュ関数 Hash が原像計算困難性を有するとは、Y に対して、Hash (X) = Y となる X を見つけることが困難であることをいう。

[6] 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。

3. SHA-1 を用いる補助関数と継続利用の詳細

3.1. SHA-1 を用いる補助関数のタイプ

表 2 の指針の理由を示すため、本書で対象となる暗号技術の範囲における SHA-1 を用いる補助関数を分類する(表 3)。各補助関数のタイプについては、後述する。

表 3: 本書で対象となる暗号技術と補助関数のタイプ

技術分類	SHA-1 を補助関数 として用いる暗号名称	補助関数のタイプ
署名	DSA, ECDSA, RSASSA-PKCS1-v1_5	・メッセージのハッシュ値
	RSA-PSS	・メッセージのハッシュ値 ・ハッシュ値の連結(MGF)
守秘	RSA-OAEP	・ハッシュ値の連結(MGF)
鍵共有	DH, ECDH	・ハッシュ値の連結(KDF)
メッセージ認証コード	HMAC	・ハッシュ関数のカスケーディング
エンティティ認証	ISO/IEC 9798-3	・上記の署名と同じ

3.1.1. メッセージのハッシュ値

本書で対象となる署名では、ハッシュ関数 Hash に関して、署名生成および署名検証対象のメッセージ M を入力として、その出力値(ハッシュ値) H = Hash(M) の計算を行う。

3.1.2. ハッシュ値の連結

3.1.2.1. マスク生成関数(Mask Generation Function, MGF)

本書で対象となる署名または守秘の中では、ハッシュ関数 Hash に関して、Seed を入力として、h を空文字から始めて、Counter を 1 つずつ増やしながら、

h = h || Hash(Seed || Counter)　(||は文字列の連結)

のように、ハッシュ値を連結していくことで、指定された長さの出力値 h の計算を行う。

3.1.2.2. 鍵導出関数(Key Derivation Function, KDF)

(a) 本書で対象となる鍵共有の中では、ハッシュ関数 Hash に関して、共有鍵 Z を入力として、h を空文字から始めて、Counter を 1 つずつ増やしながら、

$$h := \mathrm{Hash}(Z \,||\, \mathrm{OtherInfo}) \,||\, h, \text{ または}$$

$$h := \mathrm{Hash}(\mathrm{Counter} \,||\, Z \,||\, \mathrm{OtherInfo}) \,||\, h$$

のように[7]、出力値を次々に連結していくことで、指定された長さの出力値 h の計算を行うことがある。なお、OtherInfo とは、鍵共有が使われる状況に応じて決定される固有のデータを指す。

(b) 本書で対象となる鍵共有の中では、メッセージ認証コード HMAC [NT08]に関して、共有鍵 Z を入力として、h を空文字から始めて、Counter を 1 つずつ増やしながら、

$$h := \mathrm{HMAC}(\mathrm{Counter} \,||\, Z \,||\, \mathrm{OtherInfo}) \,||\, h$$

のように、出力値を次々に連結していくことで、指定された長さの出力値 h の計算を行う。なお、OtherInfo とは、鍵共有が使われる状況に応じて決定される固有のデータを指す。

3.1.3. ハッシュ関数のカスケーディング

本書で対象となるメッセージ認証コード HMAC [NT08]では、ハッシュ関数 Hash に関して、鍵 K 及びメッセージ M を入力として、

$$\mathrm{HMAC}(K, M) := \mathrm{Hash}(K_2 \,||\, \mathrm{Hash}(K_1 \,||\, M))$$

ただし、$K_1 := K \oplus \mathrm{ipad}$, $K_2 := K \oplus \mathrm{opad}$ である

(ipad と opad はある固定値で、⊕は排他的論理和).

のように、ハッシュ関数 Hash をカスケーディング(関数の合成)してハッシュ値の計算を行う。

[7] 各仕様によって、共有鍵 Z や Counter などの位置が前後する場合がある。

3.2. SHA-1 の継続利用について

3.2.1. 署名

署名には、署名が付与された文書やデータに改ざんが施されていないことを確認する改ざん防止の機能と、文書やデータに付与された署名が署名を付与した本人であることを確認するなりすましを防止する機能がある。ここでは、主に、署名生成から時間が経過した後に署名検証が求められる用途を想定し、指針を示す。このような用途の例としては電子契約等で用いる否認防止[8]目的の署名、コード署名、タイムスタンプ局が発行するタイムスタンプトークンの署名などが考えられる。

(1) 署名生成

署名対象となるハッシュ値が同じである相異なる 2 つの文書やデータの作成が現実的となれば、一方の文書(データ)に署名したあと、他方に差し替えられる(署名者が意図しなかった方の文書やデータに署名したかのように見せかけられる)リスクが高まるため、署名の作成において SHA-1 の継続利用は不適当である。署名を新規作成する場合には、より安全性の高いハッシュ関数(たとえば、ハッシュ関数 SHA-256 など)の利用に切り替えることが推奨される。

(2) 署名検証

電子政府システムやアプリケーションに依存するが、e-文書法など、法律的な要請を考慮して、当面の間、署名検証を必要とする場合もある。過去に SHA-1 を用いて生成された署名であっても、後述する長期署名やその他の手段によって、作成された当時の署名の有効性が維持されていると判断される場合には、署名の検証において SHA-1 の継続利用は互換性維持目的であれば容認される。署名検証の停止、すなわち、SHA-1 を用いて生成された署名の取り扱いを止めることについては、電子政府システムやアプリケーションの運用に依存するため、システムごとに今後、検討が必要である。

署名やタイムスタンプの有効期間を超えた後でも、それらの有効性を確認可能な長期署名フォーマット(CMS、XML 及び PDF に対応)が標準化されているので［I12a, I12b, I17, J08a, J08b］、長期保存が必要な場合は、これらを利用して署名検証を維持・継続できる。

3.2.2. 守秘

[8] 第三者が勝手に契約したり、成立した契約を変えたりする行為を防ぐこと。

RSA-OAEP [R12]は、3.1.2.1.節で述べたように、マスク生成関数の補助関数としてハッシュ関数を使用している。RSA-OAEP の安全性に関しては、用いられているハッシュ関数に衝突耐性が保証されていなかったとしても安全性が保たれるという理論的な研究がなされている[KA10]。安全性について特段の問題点は指摘されていないため、守秘において SHA-1 の継続利用は互換性維持目的であれば容認される。

3.2.3. 鍵共有

過去の評価結果[C00,C01,C02]では、基本的な鍵共有の使用に際しては、受動的攻撃(鍵共有のために通信されるデータに攻撃者が影響を与えることがない場合)に対しては問題点は指摘されていないが、能動的攻撃(鍵共有のために通信されるデータに攻撃者が影響を与える可能性がある場合)に対して、最低限、以下の 3 点に注意を払う必要がある、とされている。

- 公開鍵とエンティティとの結び付きを保証する手段を確保する。
- (更新を前提とする)セッション鍵共有方式として使用する場合には、交換する公開鍵は一時的なものとする。
- 共有される鍵が乱数と見分けがつかなくするためには鍵導出関数を使用する。

共有される鍵を乱数と見分けがつかなくするために使用される鍵導出関数(Key Derivation Function, KDF)は、3.1.2.2.節で述べたように、補助関数のタイプ別では、ハッシュ値の連結ベースのものと、ハッシュ関数のカスケーディングベースのものの 2 つの構成方法がある。安全性について特段の問題点は指摘されていないため、鍵共有において SHA-1 の継続利用は互換性維持目的であれば容認される。

3.2.4. メッセージ認証コード

HMAC [NT08]は、3.1.3.節で述べたように、ハッシュ関数のカスケーディングベースで構成されている。HMAC の安全性に関しては、用いられているハッシュ関数に衝突耐性が保証されていなかったとしても安全性が保たれるという理論的な研究がなされている [B15, G14]。安全性について特段の問題点は指摘されていないため、メッセージ認証コードにおいて SHA-1 の継続利用は互換性維持目的であれば容認される。

3.2.5. エンティティ認証

エンティティ認証とは、認証される者が実際にその者であることを確認する機能である。ここでは、エンティティ認証を実現する仕組みとして署名を用いるものを想定している。3.2.1 節の署名とは異なり、チャレンジ-レスポンスのように、署名対象のデータ[9]と署名のデータを短時間で使い捨てるように利用される。衝突を計算する十分な時間が現時点では確保できないと考えられるため、短時間に認証が完了するのであれば、エンティティ認証に用いられる署名において SHA-1 の継続利用は互換性維持目的であれば容認される。

[9] ISO/IEC 9798-3 では、シークエンス番号、タイムスタンプ、ID 番号や乱数等からなるデータの組み合わせが規定されている。

4. SHA-1 の危殆化に関する背景と参考情報

4.1. CRYPTREC 及び NISC における対応

SHA-1 は、2002 年度に策定した「電子政府における調達のために参照すべき暗号のリスト（電子政府推奨暗号リスト）」(2003 年 2 月 20 日)に、注釈(注 6)[10]を付けて掲載された。暗号技術監視委員会(当時)は、2005 年に SHA-1 に対する衝突探索アルゴリズムに関する論文[W05]が発表された際に、その詳細を検討し[C06]、「SHA-1 の安全性に関する見解」の案[C05]を作成した。その後、この見解案は 2006 年 6 月 28 日に正式に承認され、暗号技術検討会事務局へ提出された[C07]。

その後、電子政府システムにおいて移行についての検討が進められ[ME10,ME11,MI09]、内閣官房情報セキュリティセンター(当時)は、2008 年 4 月に「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」[NC08b]を公表した。なお、この指針は 2012 年 10 月に改定版[NC12b]が公表されている。いままでに、政府認証基盤(GPKI)や地方公共団体組織認証基盤(LGPKI)などにおいて、システムの移行が進んでいる[L14,MI14]。

2012 年度に改定された CRYPTREC 暗号リストにおいては、運用監視暗号リストに、注釈(注 8)[11]を付けて記載された。

2015 年 10 月 8 日に、オランダの国立情報工学・数学研究所(CWI)、フランスの国立情報学自動制御研究所(INRIA)及びシンガポールの南洋理工大学(NTU)の共同研究チームは、SHA-1 のフルラウンド(全 80 ステップ中 80 ステップ)に対して、仕様より緩い条件下ながら衝突発見に成功したと発表した[S15]。暗号技術評価委員会では、CRYPTREC の Web ページにおいてこの件に関する注意喚起を行い[C15a]、暗号技術検討会に報告した[C15b]。

2017 年 2 月 23 日に、CWI 及び Google の共同研究チームは、SHA-1 のフルラウンドに対する衝突発見に成功したと発表した[S17a]。発表された論文[S17b]によれば、衝突発見に要する計算量は、6500 CPU コア・年 + 100 GPU・年であり、768 ビット(10 進 232 桁)の合成数の素因数分解に要した計算量[KL10]や 768 ビットの離散対数の計算[KL17]よりも数倍ほど大きな量であった。暗号技術評価委員会では、CRYPTREC の Web ページにおいてこの件に関する注意喚起を行った[C17a]。

---

[10] 『新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。』

[11] 『「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」(平成 20 年 4 月 情報セキュリティ政策会議決定、平成 24 年 10 月情報セキュリティ対策推進会議改定)を踏まえて利用すること。 http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf (平成 25 年 3 月 1 日現在)』

現在までに、SHA-1 の第二原像計算困難性及び原像計算困難性については実運用環境に影響を及ぼすほどの問題は見つかっていない。

CRYPTREC では、表 3 のように、SHA-1 の安全性に関する意見などを公表してきたが、NIST が示してきたような SHA-1 に関する利用期限については公表していない。

表 3: SHA-1 の衝突に係る主な年表

時期	出来事
1995 年 4 月	FIPS PUB 180-1 策定 (NIST)
2003 年 2 月	電子政府推奨暗号リスト策定 (CRYPTREC)
2004 年 8 月	SHA-1 への攻撃に対する短い声明 (NIST) [NT04]
2005 年 8 月	衝突探索アルゴリズムの論文発表 (Wang ら)
2006 年 4 月	SHA-1 への攻撃に対する声明 (NIST) [NT06]
2006 年 6 月	SHA-1 の安全性に関する見解 (CRYPTREC)
2008 年 4 月	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 に係る移行指針の策定 (NISC)
2011 年 1 月	SP 800-131A 策定(2015 年 10 月に Revision 1 に改定) (NIST)
2013 年 3 月	CRYPTREC 暗号リスト策定 (CRYPTREC)
2015 年 10 月	SHA-1 のフリースタート衝突の発見 (Stevens ら)
2017 年 2 月	SHA-1 の衝突発見(Stevens ら)

4.2. NISTにおける対応

(1) ハッシュ関数

NIST SP 800-57 Part 1 Revision 1では、SHA-1については、表4の通り記載されている。

表4: NISTにおけるハッシュ関数の安全性強度と利用範囲の状況（[NT16]から抜粋）

Security Strength	**Digital Signatures and hash-only applications**	**HMAC, Key Derivation Functions, Random Number Generation**
≤80	SHA-1	
112	SHA-224, SHA-512/224, SHA3-224	
128	SHA-256, SHA-512/256, SHA3-256	SHA-1
192	SHA-384, SHA3-384	SHA-224, SHA-512/224
≥256	SHA-512, SHA3-512	SHA-256, SHA-512/256, SHA-384, SHA-512, SHA3-512

また、NIST SP 800-131A Revision 1では、SHA-1については、表5の通り記載されている。

表5: NISTにおけるSHA-1の承認状況（[NT15c]から抜粋）

Hash Function	**Use**	
SHA-1	Digital signature generation	Disallowed, except where specifically allowed by NIST protocol-specific guidance.
	Digital signature verification	Legacy-use
	Non-digital signature applications	Acceptable

SHA-1 for digital signature generation:
SHA-1 may only be used for digital signature generation where specifically allowed by NIST protocol-specific guidance. For all other applications, SHA-1 **shall not** be used for digital signature generation.

SHA-1 for digital signature verification:
For digital signature verification, SHA-1 is allowed for **legacy-use**.

SHA-1 for non-digital signature applications:
For all other hash function applications, the use of SHA-1 is **acceptable**. The other applications include HMAC, Key Derivation Functions (KDFs), Random Bit Generation, and hash-only applications (e.g., hashing passwords and using SHA-1 to compute a checksum, such as the approved integrity technique specified in Section 4.6.1 of [FIPS 140]).

(2) 擬似乱数生成系

NIST SP 800-131A Revision 1では、FIPS 186-2 や ANS X9.62-1998で指定されている擬似乱数生成系については、表6 の通り記載されている。NISTの基準ではSHA-1 のHASH_DRBG 及びHMAC_DRBG での利用が許容されているが、それ以外での利用は現在では承認されていない。

表 6: NIST における乱数生成器の承認状況 ([NT15c]から抜粋)

Description	Use
HASH_DRBG, HMAC_DRBG and CTR_DRBG	Acceptable
DUAL_EC_DRBG	Disallowed
RNGs in FIPS 186-2, ANS X9.31 and ANS X9.62-1998	Deprecated through 2015 Disallowed after 2015
Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known. **Deprecated** means that the use of the algorithm and key length is allowed, but the user must accept some risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection to data (e.g., encrypting or generating a digital signature).	

なお、現在、NIST SP 800-90C [NT16b]はドラフト版になっている。NICT SP 800-90B [NY16a]は最終版が 2018 年 1 月に公開されている。

(3) 鍵導出関数

NIST SP 800-131A Revision 1では、鍵導出関数について、表7 の通り記載されている。

表 7: NIST における鍵導出関数の承認状況 ([NT15c]から抜粋)

Algorithm	Use	
HMAC-based KDF	Acceptable	
CMAC-based KDF	Two-key TDEA-based KDF	Deprecated through 2015 Disallowed after 2015
	AES and Three-key TDEA	Acceptable
HMAC-based KDF (HMAC is the Keyed-Hash Message Authentication Code [FIPS 198-1]): The use of HMAC-based KDFs is **acceptable** using an **approved** hash function, including SHA-1. See Section 10 for discussions of the key lengths used with HMAC CMAC-based KDF: The use of two-key TDEA as the block cipher algorithm in a CMAC-based KDF is **deprecated** through December 31, 2015. Two-key TDEA **shall not** be used to derive keying material after December 31, 2015. The use of AES and three-key TDEA as the block cipher algorithm in a CMAC-based KDF is **acceptable**.		

5. 参考文献

[B15] M. Bellare, New Proofs for NMAC and HMAC: Security Without Collision-Resistance, Journal of Cryptology 28(4): 844-878 (2015). https://eprint.iacr.org/2006/043

[C00] CRYPTREC Report 2000, 2001 年 3 月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C01] CRYPTREC Report 2001, 2002 年 3 月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C02] CRYPTREC Report 2002, 2003 年 3 月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C03a] 総務省・経済産業省, 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(電子政府暗号リスト), 2003 年 2 月 20 日 http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_fy2005.pdf

[C05] CRYPTREC Report 2005 (第 2 版), 2006 年 5 月 17 日 http://www.cryptrec.go.jp/report/c05_wat_final.pdf

[C06] ハッシュ関数(SHA-1)の安全性評価および攻撃手法整理, CRYPTREC 技術報告書 501 番, 2006 年 3 月, http://www.cryptrec.go.jp/estimation/rep_ID0501.pdf

[C07] 暗号技術検討会報告書(2006 年度), 2007 年 3 月 http://www.cryptrec.go.jp/report/c06_kentou_final.pdf

[C08a] CRYPTREC Report 2007, 2008 年 3 月 http://www.cryptrec.go.jp/report/c07_wat_final.pdf

[C08b] 2007 年度電子政府推奨暗号の利用方法に関するガイドブック, 2008 年 3 月 http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

[C10] 2009 年度版リストガイド, 2010 年 3 月 http://www.cryptrec.go.jp/report/c09_guide_final.pdf

[C13a] 総務省・経済産業省, 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 http://cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf

[C13b] CRYPTREC Report 2012, 2013 年 3 月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C15a] SHA-1 の安全性について, 平成 27 年 12 月 18 日 http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html

[C15b] 暗号技術検討会報告書(2015 年度), 2016 年 3 月 http://www.cryptrec.go.jp/report/c15_kentou_final.pdf

[C17a] SHA-1 の安全性低下について, 平成 29 年 3 月 1 日 http://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html

[C17b] CRYPTREC 暗号の仕様書, 2017 年 6 月 http://www.cryptrec.go.jp/method.html

[G14] P. Gaži, K. Pietrzak, and M. Rybár: The Exact PRF-Security of NMAC and HMAC, CRYPTO 2014, Lecture Notes in Computer Science vol. 8616, pp.113-130, 2014. https://eprint.iacr.org/2014/578.pdf

[I98] ISO/IEC 9798-3:1998, Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques

[I12a] ISO 14533-1:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)
[I12b] ISO 14533-2:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)
[I17] ISO 14533-3:2017, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)
[IK03] Tetsu Iwata and Kaoru Kurosawa: OMAC: One-Key CBC MAC. Fast Software Encryption 2013: 129-153.
https://eprint.iacr.org/2002/180.pdf
[J08a] JIS X 5092:2008, CMS 利用電子署名(CAdES)の長期署名プロファイル
Long term signature profiles for CMS advanced electronic signatures (CAdES)
[J08b] JIS X 5093:2008, XML 署名利用電子署名(XAdES)の長期署名プロファイル
Long term signature profiles for XML advanced electronic signatures (XAdES)
[J14] 独立行政法人情報処理推進機構, 承認されたセキュリティ機能に関する仕様(平成 26 年 4 月 1 日),
https://www.ipa.go.jp/security/jcmvp/documents/asf01.pdf
[K10] Hugo Krawczyk: Cryptographic Extraction and Key Derivation: The HKDF Scheme. CRYPTO 2010, Lecture Notes in Computer Science vol. 6223, pp. 631-648, 2010.
https://eprint.iacr.org/2010/264.pdf
[KA10] Akinori Kawachi, Akira Numayama, Keisuke Tanaka, Keita Xagawa: Security of Encryption Schemes in Weakened Random Oracle Models. Public Key Cryptography 2010: 403-419.
https://www.iacr.org/archive/pkc2010/60560406/60560406.pdf
[KL10] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thome´, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann: Factorization of a 768-bit RSA modulus. CRYPTO 2010, Lecture Notes in Computer Science vol. 6223, pp. 333-350. 2010.
https://eprint.iacr.org/2010/006.pdf
[KL17] T. Kleinjung, C. Diem, A. K. Lenstra1, C. Priplata, and C. Stahlke, Computation of a 768-bit prime field discrete logarithm
https://eprint.iacr.org/2017/067.pdf
[L09] G. Leurent, P. Q. Nguyen: How Risky Is the Random-Oracle Model?, CRYPTO 2009, Lecture Notes in Computer Science vol. 5677, pp. 445-464. 2009.
https://iacr.org/archive/crypto2009/56770440/56770440.pdf
[L14] 地方公共団体情報システム機構, LGPKI の移行方針について, 2014 年 12 月 19 日更新, http://www.lgpki.jp/unei/LGPKI_ikouhoushin_20141219.pdf
[ME10] 「電子署名法における暗号アルゴリズム移行研究会」報告書(2010 年 3 月)
http://www.meti.go.jp/policy/netsecurity/docs/esig/h21_esign-crypto-report.pdf
[ME11] 「電子署名法における暗号アルゴリズム移行研究会」報告書(2011 年 3 月)
http://www.meti.go.jp/policy/netsecurity/docs/esig/h22esig-alg-report.pdf
[MI09] 「公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書」, 平成 21 年 1 月,

http://www.soumu.go.jp/main_sosiki/kenkyu/kouteki_kojin/pdf/090126_houkoku.pdf
[MI14] 総務省 行政管理局 政府認証基盤，暗号アルゴリズムの移行について，https://www.gpki.go.jp/documents/angouikou.html
[NC08a] 内閣官房情報セキュリティセンター（NISC），情報セキュリティ政策会議 第17回会合 資料3-1，政府機関における安全な暗号利用の促進，移行指針(案)に基づく暗号方式の移行完了までのスケジュール，2008年2月4日 http://www.nisc.go.jp/conference/seisaku/dai16/pdf/16siryou0301.pdf
[NC08b] 内閣官房情報セキュリティセンター（NISC），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，2008年4月22日，情報セキュリティ政策会議決定 http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf
[NC12a] 内閣官房情報セキュリティセンター（NISC），情報セキュリティ政策会議 第31回会合 資料3-1，政府機関の暗号アルゴリズムに係る移行指針の改定概要，（参考）政府機関における暗号移行スケジュール，平成24年11月1日 http://www.nisc.go.jp/conference/seisaku/dai31/pdf/31shiryou0301.pdf
[NC12b] 内閣官房情報セキュリティセンター（NISC），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，2012年10月26日改定，情報セキュリティ対策推進会議決定 http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
[NT04] NIST Brief Comments on Recent Cryptanalytic Attacks，2004年8月，https://csrc.nist.gov/News/2004/NIST-Brief-Comments-on-Recent-Cryptanalytic-Attack
[NT06] NIST Comments on Cryptanalytic Attacks on SHA-1，2006年4月，https://csrc.nist.gov/News/2006/NIST-Comments-on-Cryptanalytic-Attacks-on-SHA-1
[NT08] NIST FIPS PUB 198-1，2008年7月 http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
[NT09] NIST Special Publication 800-108，2009年10月 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf
[NT11] NIST Special Publication 800-135 Revision 1，2011年12月 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf
[NT13] NIST Special Publication 800-56A Revision 2，2013年5月 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf
[NT15a] NIST，Special Publication 800-90A Revision 1，2015年6月 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
[NT15b] NIST FIPS PUB 180-4，2015年8月 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
[NT15c] NIST Special Publication 800-131A Revision 1，2015年11月 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
[NT16] NIST，NIST Special Publication 800-57 Part 1 Revision 4，2016年1月 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r

4.pdf
[NT16a] NIST, NIST Special Publication 800-90B, 2018年1月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
[NT16b] NIST, (Second DRAFT) NIST Special Publication 800-90C
http://csrc.nist.gov/publications/drafts/800-90/sp800_90c_second_draft.pdf
[N08] Akira Numayama, Toshiyuki Isshiki, Keisuke Tanaka: Security of Digital Signature Schemes in Weakened Random Oracle Models. Public Key Cryptography 2008: 268-287.
https://www.iacr.org/archive/pkc2008/49390269/49390269.pdf

[R12] RSA Laboratories, PKCS #1 v2.2: RSA Cryptography Standard, 2012年10月
https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf
[S15] Press Release “Researchers urge: industry standard SHA-1 should be retracted sooner”, CWI, INRIA, NTU, October 8, 2015.
https://www.cwi.nl/news/2015/researchers-urge-industry-standard-sha-1-should-be-retracted-sooner
[S17a] Announcing the first SHA1 collision
https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html, February 23, 2017.
[S17b] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, The first collision for full SHA-1,
CRYPTO 2017, Lecture Notes in Computer Science vol. 10401, pp. 570-596, 2017.
https://shattered.io/static/shattered.pdf, February 23, 2017.
[W05] X. Wang, Y. Lisa Yin, and H. Yu, Finding Collisions in the Full SHA-1, CRYPTO 2005, Lecture Notes in Computer Science vol. 3621, pp. 17-36, 2005.
https://www.iacr.org/archive/crypto2005/36210017/36210017.pdf

以上

CRYPTREC 暗号技術ガイドライン(SHA-1), CRYPTREC GL-XXXX-2017

発行日　2018年 3月XX日　第2版

発行者

・〒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

・〒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

資料５

2017 年度暗号技術活用委員会 活動報告

1. 2017 年度の活動内容と成果概要

1.1. 活動内容

2016 年度に取りまとめられた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）の候補のなかから、必要性、目的、課題、関連組織等の状況を踏まえ、具体的に運用ガイドラインの対象を選定し、ガイドライン作成に向けた活動を行った。

具体的には、「鍵管理に関する運用ガイドライン作成に向けた活動」と「SSL/TLS 暗号設定ガイドラインのアップデートに向けた活動」からなる。

■ 鍵管理に関する運用ガイドライン作成に向けた活動

2016 年度に取りまとめた運用ガイドラインの候補の中で鍵管理に関するものが多数を占めており、また実際に暗号を利用するうえでも鍵の正しい運用は不可欠である点から、鍵管理に関する運用ガイドラインの重要性は他と比較しても高いものと考えられる。

一方で、鍵管理に関するガイドラインは、その重要性からも、国内外を含め、いくつか発行されている。しかしながら、いずれのガイドラインも広く認知され、利用されているとは言い難い点を踏まえれば、従来の鍵管理ガイドラインには「ガイドラインとして利用しにくい」問題点が隠れているように思われる。例えば、

- ✧ 鍵管理として扱うべき範囲、考慮すべき範囲が広い
- ✧ 記述内容が抽象的になりがちである
- ✧ 技術的な観点だけでなく、法制度や運用ルール的な観点との整合性が求められる

といった意見が委員からも指摘された。

そこで、2017 年度の暗号技術活用委員会では、いきなり鍵管理に関するガイドラインを作成するのではなく、鍵管理に関する規格を網羅的に調査し、どのような体系・順番で鍵管理に関するガイドラインを作成していくのがよいのかを取りまとめる。

■ SSL/TLS 暗号設定ガイドラインのアップデートに向けた活動

「SSL/TLS 暗号設定ガイドライン」については、2015 年発行時から状況が変化していること、10 万件を越えるダウンロード数があるなどニーズが多いことにから、2017 年度に、外部動向の追加ならびにそれに対応するためのマネジメント方針の追記・修正などを行い、SSL/TLS 暗号設定ガイドラインのアップデート案を作成する。

1.2. 暗号技術活用委員会の委員構成及び開催状況

暗号技術活用委員会の委員構成は表 1 のとおりである。また、2017 年度 2 回開催された暗号技術活用委員会での審議概要は表 2 のとおりである。さらには、暗号技術活用委員会とは別に、SSL/TLS に関する動向及び鍵管理に関する公募調査の中間報告会を委員向けに実施し

た。

表 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	垣内　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　研究企画室長

表 2　暗号技術活用委員会 開催状況

回	開催日	議案
第 1 回	2017 年 9 月 7 日	・SSL/TLS 暗号設定ガイドラインのアップデート作業について ・鍵管理に関する運用ガイドラインの事前検討について
報告会	2017 年 12 月 27 日	・SSL/TLS に関する動向及び鍵管理に関する公募調査の中間報告
第 2 回	2018 年 3 月 15 日	・SSL/TLS 暗号設定ガイドラインのアップデート案について ・鍵管理に関する運用ガイドライン作成に向けた今後の計画について

1.3. 成果概要

1.3.1 鍵管理に関する運用ガイドラインに向けた成果

鍵管理に関する運用ガイドライン作成に向けた事前調査として、鍵管理に関する規格を網羅的に調査した。調査結果から、SP 800-57 Part1 と SP 800-130 は非常に強い関連性を

持ち、また鍵管理全体のフレームワークとして最も基本的な文献であると考えられることが確認できた。

- 調査対象：
  第 1 回暗号技術活用委員会で指摘いただいた資料を中心とした 21 文献

SP 800-57 Part1	Recommendation for Key Management, Part 1: General
SP 800-57 Part2	Recommendation for Key Management, Part 2: Best Practices for Key Management Organization
SP 800-57 Part3 Rev. 1	Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance
SP 800-130	A Framework for Designing Cryptographic Key Management Systems
SP 800-152	A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)
SP 800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
ENISA 2013	Recommended cryptographic measures - Securing personal data
ENISA 2014	Algorithms, key size and parameters report 2014
ENISA 2011	The Use of Cryptographic Techniques in Europe
OASIS	Key Management Interoperability Protocol Specification Version 1.3
CR 2010 GK	2010 年度版　リストガイド（鍵管理） CRYPTREC
IPA 2008 R	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 調査報告書
IPA 2008 G	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）
IPA	「暗号鍵の適切な運用・管理に係る課題調査」報告書
SP 800-81-2	Secure Domain Name System (DNS) Deployment Guide
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
SP 800-111	Guide to Storage Encryption Technologies for End User Devices
SP 800-88 Rev. 1	Guidelines for Media Sanitization
NISTIR 7956	Cryptographic Key Management Issues & Challenges in Cloud Services
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
CSI SSH	SSH サーバセキュリティ設定ガイド

- 調査方法：
  - 調査対象の文献の全体像を把握するため、鍵管理が主テーマ各文献に対して扱っている項目を洗い出し、行に文献の目次の一覧、列に文献を並べたマッピングを作成。
  - 複数の文献で同じ項目や似たような項目を扱っている場合は、述べられている内容

が同じなのか違う内容なのかを確認。

- 参照している文献を確認し、図に整理。
- ポイントとなる文献は重点的に内容を確認し、オリジナルな主張を述べている箇所がある文献についてもその内容を確認。

- 調査概要：
  - 多くの文献が鍵管理の一般的事項は SP 800-57 Part 1 (General)を参照。この文献が鍵管理の基礎の位置付けにある。
  - SP 800-57 以外では、SP 800-130 (Framework)が SP 800-175B (Guideline)と ENISA (Algorithms)で参照されていて、鍵管理(CKM)の文献は SP 800-57 で、鍵管理システム(CKMS)の文献は SP 800-130 であるとしている。
  - NIST「Cryptographic Key Management Workshop」は SP 800-130 (Framework)とこれの連邦政府向けの文献 SP 800-152 (Federal)を作成するための会議であった。
  - SP 800-57 Part2 (Best Practices)と SP 800-130 (Framework)は“ポリシー”を扱っているため内容を比較したところ、SP 800-57 Part2 (Best Practices)では、安全性の検討事項として保護対象の情報、脅威、保護メカニズム、保護要件などが列挙され、組織の役割と責任も説明されている。一方、SP 800-130 (Framework)は SP 800-57 Part2 の参照はなく、ポリシーを鍵管理システムより上位概念の情報管理ポリシーから階層的に分析していて、ポリシーについてより詳細に述べられている。

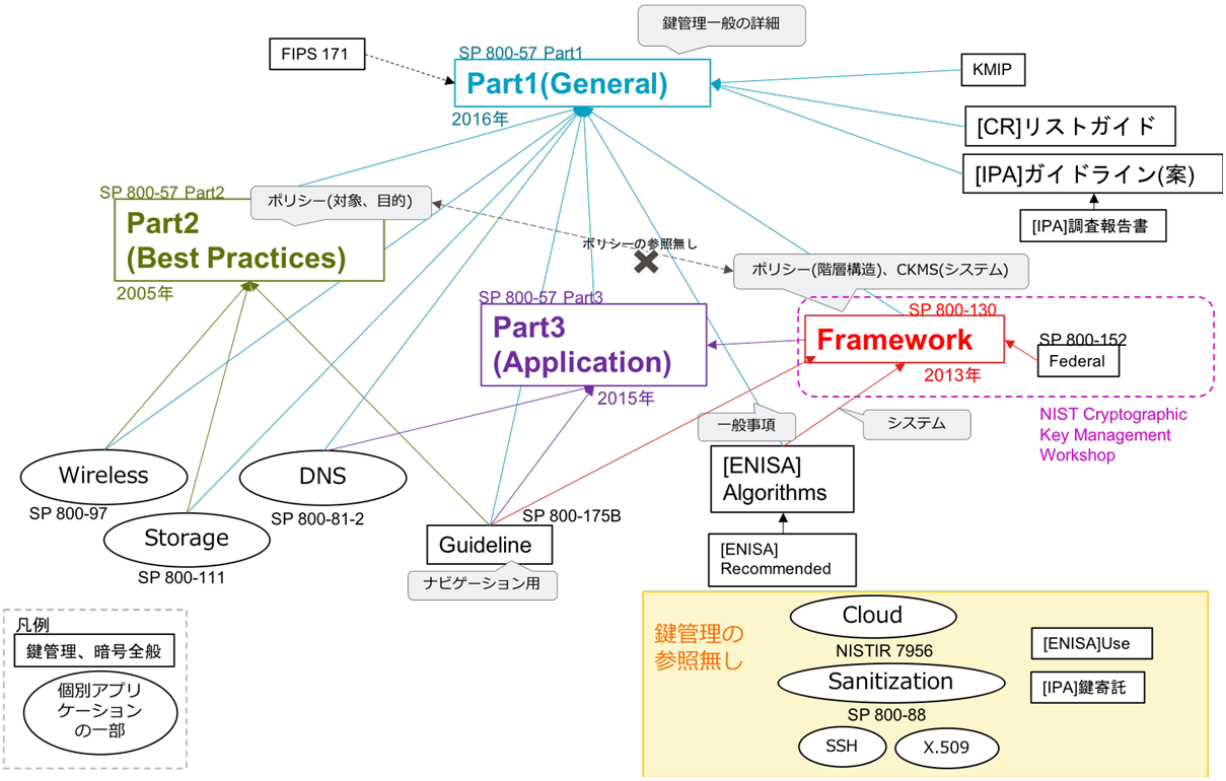


図 1.3.1　各文献における鍵管理に関する他文献への参照関係

- SP 800-57 Part 1 (General)
  - 鍵管理の一般的なガイダンスを提供していて、想定読者はシステム管理者、暗号モジュール開発者、プロトコル開発者と幅が広い。
  - 鍵管理のメインは「一般的な鍵管理ガイダンス」の章と「鍵管理のフェーズと機能」の章。「一般的な鍵管理ガイダンス」では、鍵の種別を説明し、鍵の種別や非対称鍵/対称鍵ごとに暗号期間（鍵の有効期間）を詳しく説明している。
    「鍵管理のフェーズと機能」では、運用前／運用／運用後／破棄の４つのフェーズでの鍵管理の機能が説明されている。
    - 運用前フェーズ：利用者登録機能、システム初期化機能、鍵材料インストール機能、鍵確立機能、鍵登録機能
    - 運用フェーズ：鍵の保管機能、鍵の変更機能、鍵導出方法
    - 運用後フェーズ：アーカイブと鍵回復機能、エンティティ登録抹消機能、鍵登録抹消機能、鍵破棄機能、鍵失効機能
    - 破棄フェーズ
  - 2005 年に初版が発行。2006 年、2007 年、2012 年、2016 年に改訂（最新版は Revision 4）。初版は、1992 年に発行された FIPS 171「Key Management Using ANSI X9.17（金融機関の間の鍵転送プロトコル）」をベースに作られている。

- SP 800-57 Part 2 (Best Practices)
  - 組織が鍵管理のポリシーを作成する際に検討する内容とポリシーを実現するための文書に書くべき内容をガイド。

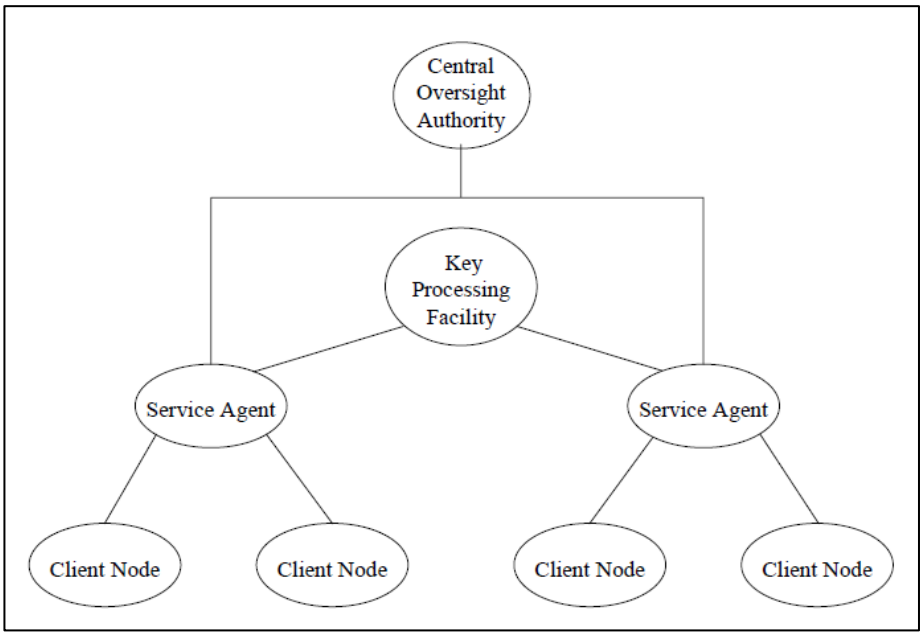


図 1.3.2　鍵管理の基盤（KMI）の概念

  - 中央監視権限、鍵保持機関、サービス代行者、クライアントノードから成る鍵管理の基盤(KMI)の概念が示されている。その基盤では、中央監視権限は組織の鍵管理システムの安全性監視のためポリシーや実施文書を統括し、鍵保持機関は公開鍵証明書の発行や鍵材料の分配を行う。サービス代行者は組織に該当し、組織内の各クライアントノードと鍵保持機関の通信はサービス代行者を通じて行なわれる。
  - 鍵管理ポリシー作成時には以下を検討しポリシーに含める。
    - 保護対象のデータ
    - 脅威
    - 暗号を用いた保護技術
    - 暗号のプロセスと鍵材料に対する保護要件
  - 鍵管理の基盤(KMI)での組織の責任と役割も説明されている。
  - 本文献は 2005 年に SP 800-57 Part 1 と同時に発行されて以来、改定されていない。

- SP 800-130 (Framework)
  - 鍵管理システム(CKMS)の設計者向けのドキュメントであり、設計書に指定すべきことを記したフレームワークを提案している。フレームワーク本体の前に以下のような鍵管理の考え方が述べられている。

1. 鍵管理は鍵だけでなく鍵の属性値であるメタデータも管理する必要がある。メタデータは鍵名称、所有者識別子、ライフサイクルのステータス、フォーマット、暗号アルゴリズム、鍵長といった属性値を指す。
2. CKMS 設計者は組織や部門に合わせてフレームワークを変更したオリジナルの CKMS 設計書“プロファイル”を作成する。
3. プロファイルを満たすには複数のセキュリティメカニズムを組み合わせる。既成品も利用する。標準化された製品の利用も有益である。
4. 鍵管理システムの設計は鍵管理システムの方針（ポリシー）に沿って作成する。鍵管理システムのポリシーは、最上位概念である情報管理ポリシーから、情報セキュリティポリシー、鍵管理システムポリシーへとブレイクダウンしながら分析して策定する。情報管理ポリシーでは保護対象の情報や関係する人の役割と責任を分析し、情報セキュリティポリシーでは脅威やリスクを分析し、鍵管理システムポリシーでは用いる暗号アルゴリズムを検討する。

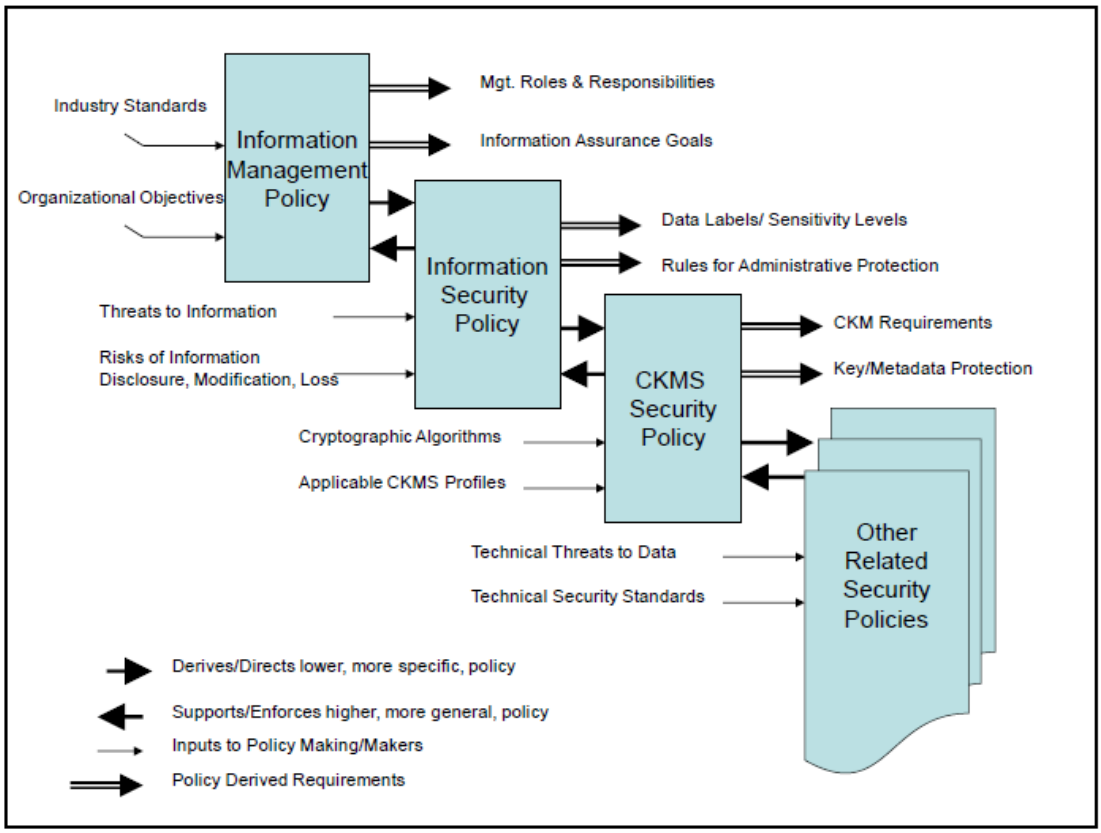


図 1.3.3　セキュリティポリシーの関連図

5. 同じポリシーを適用する範囲をセキュリティドメインと呼び、異なるセキュリティドメインに属するエンティティが鍵やメタデータを受け渡す場合について詳細に述べられている点が特徴的。

6. 安全性の管理の章では、鍵管理に使用するハードウェアや暗号モジュールのソフトウェアを物理的に保護する方法にも言及がある。

1.3.2 SSL/TLS 暗号設定ガイドラインのアップデートに向けた成果

以下の項目について動向調査を実施し、アップデート案の審議を行った。

- 調査対象：

TLS 1.3 動向
2015 年 1 月以降に成立した TLS に関連する RFC
サーバ証明書の取り扱い動向
主要ブラウザの動向調査
国内外の他機関が発行する SSL/TLS に関するガイドライン（2015 年 1 月以降の最新版を対象）との比較
暗号アルゴリズム（RC4, Triple DES, CBC, SHA-1）の利用可否や利用期限などについて、2015 年 1 月以降に国内外の他機関が発行・更新したガイドライン等の整理
現行ガイドラインに記載されている設定・実装状況についての最新化
SSL/TLS に関する脆弱性情報・危殆化情報に係る調査（2015 年 5 月以降）

動向調査の結果を踏まえ、暗号技術活用委員会としては、以下の 22 箇所について、SSL/TLS 暗号設定ガイドラインの記述を修正・追記・削除すべきかを検討した。合わせて、コラム記事を更新すべきかの議論を行った。

特に、前回 SSL/TLS 暗号設定ガイドラインを公開した 2015 年当時は、レガシーシステムや携帯電話などで SSL3.0 や SHA-1 証明書の利用を必要とするケースが無視できないことから、「セキュリティ例外型」を設け「早期移行を前提として暫定的な利用継続」を認めていたが、この 3 年間で SSL3.0 や SHA-1 証明書の利用から脱却が大きく進んだことから「推奨セキュリティ型への早期移行を求めるものであり、すでに最低限の安全性水準を満たしているとは言えない状況になっている。」との記述変更を行う、などのアップデート案を策定した。詳細を別添 1 及び別添 2 に記載する。

2. 今後に向けて

SSL/TLS 暗号設定ガイドラインについては、本日の暗号技術検討会でのアップデート案の承認を前提として、2018 年 5 月にアップデート版の公開を行う予定である。

また、鍵管理に関する運用ガイドラインについては、SP 800-57 の内容と SP 800-130 の内容をより精査した上で、実際のガイドライン作成に臨むこととする。

資料5別添1

「SSL/TLS暗号設定ガイドライン」
アップデート案

アップデート案一覧（詳細記述案は別添2参照）

- 現ガイドラインの記述内容から技術的に大きな変更を行う項目
  - 3.1　実現すべき設定基準の考え方
  - 3.2　要求設定の概要　表5
  - EC曲線系のパテントリスクの記述

- 最新動向を反映した記述内容の新規追加・修正・削除を行う項目

（追加）
  - 2.1.1 SSL/TLSの歴史
  - 2.1.3 TLS1.3の特徴
  - 2.1.4 TLSプロトコルの最新動向

（修正）
  - 8.3.1　鍵長1024ビット、SHA-1を利用するサーバ証明書の警告表示

（削除）
  - 8.3.2　SSL3.0の取り扱い

アップデート案一覧（詳細記述案は別添2参照）

- 最新データへの更新（及びそれに伴う記述更新）を行う項目
  - 6.3.3 DHE/ECDHEでの鍵長の設定状況についての注意
  - 7.1.1 サーバ証明書での脆弱な鍵ペアの使用の回避
  - 7.1.3 サーバ証明書の有効期間に関する注意点
  - 7.2.1 HTTP Strict Transport Security（HSTS）の設定有効化
  - 7.2.4 OCSP Staplingの設定有効化
  - 7.2.5 Public Key Pinningの設定有効化
  - 8.1　本ガイドラインが対象とするブラウザ（2箇所）
  - 8.2　設定に関する確認項目（2箇所）

- エディトリアル的な記述内容の修正を行う項目
  - 1.1　本書の内容及び位置付け
  - 2.2.1　CRYPTREC暗号リスト
  - 2.2.2 異なる暗号アルゴリズムにおける安全性の見方
  - 5.4.3 サーバ証明書で利用すべき鍵長
  - 6.2 暗号スイートで利用可能な候補となる暗号アルゴリズム

アップデート案詳細

■ 3.1 実現すべき設定基準の考え方

- P16 表4 安全性と相互接続性についての比較
- 目的：特に、セキュリティ例外型の記述見直し

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して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 ＜利用例＞ 政府内利用（G2G型）のなかでも、限定された接続先に対して、とりわけ高い安全性が要求される通信を行う場合	本ガイドラインの公開時点（2015年5月）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

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して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~~ ＜利用例＞ 政府内利用（G2G型）のなかでも、~~限定された接続先に対して、~~とりわけ高い安全性が要求される通信を行う場合	本ガイドラインの公開時点（2018年5月）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	本ガイドラインで対象とするブラウザ（8.1.2節）が搭載されているPC、スマートフォンなどでは問題なく相互接続性を確保できる。 本ガイドラインが対象としない、バージョンが古いOSやブラウザの場合や発売開始からある程度の年月が経過している一部の古い機器（フィーチャーフォンやゲーム機など）については接続できない可能性がある。

アップデート案詳細

設定基準	概要	安全性	相互接続性の確保
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 ＜利用例＞ • 政府内利用（G2G型）や社内システムへのリモートアクセスなど、特定された通信相手との安全な通信が要求される場合 • 電子申請など、企業・国民と役所等との電子行政サービスを提供する場合 • 金融サービスや電子商取引サービス、多様な個人情報の入力を必須とするサービス等を提供する場合 • 既存システムとの相互接続を考慮することなく、新規に社内システムを構築する場合	本ガイドラインの公開時点（2015年5月）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（8.1.2節）が搭載されているPC、スマートフォンなどでは問題なく相互接続性を確保できる 本ガイドラインが対象としない、バージョンが古いOSやブラウザの場合や発売開始からある程度の年月が経過している一部の古い機器（フィーチャーフォンやゲーム機など）については接続できない可能性がある

設定基準	概要	安全性	相互接続性の確保
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 ＜利用例＞ • 政府内利用（G2G型）や社内システムへのリモートアクセスなど、特定された通信相手との安全な通信が要求される場合 • 電子申請など、企業・国民と役所等との電子行政サービスを提供する場合 • 金融サービスや電子商取引サービス、多様な個人情報の入力を必須とするサービス等を提供する場合 • 既存システムとの相互接続を考慮することなく、新規に社内システムを構築する場合	本ガイドラインの公開時点（2018年5月）における標準的な安全性水準を実現	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。 ※すでにサポートが切れているなどかなり古い機器などで接続できない場合があるが、この種の機器は本来接続させるべきではない。

アップデート案詳細

設定基準	概要	安全性	相互接続性の確保
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 ＜利用例＞ • 利用するサーバやクライアントの実装上の制約、もしくは既存システムとの相互接続上の制約により、推奨セキュリティ型（以上）の設定が事実上できない場合	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（2015年5月）において許容可能な最低限の安全性水準を満たす	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

設定基準	概要	安全性	相互接続性の確保
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であって、推奨セキュリティ型への移行完了までの短期の暫定運用としての設定基準 ~~※推奨セキュリティ型への早期移行を求めるものであり、すでに最低限の安全性水準を満たしているとは言えない状況になっている~~ ＜利用例＞ • 利用するサーバやクライアントの実装上の制約、もしくは既存システムとの相互接続上の制約により、推奨セキュリティ型（以上）の設定が事実上できない場合	~~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（2018年5月）において、最低限度の安全性水準を満たしているとは言えない状況になっている。速やかな推奨セキュリティ型への移行を強く求める。	~~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。

アップデート案詳細

- P.15　本文（暗号技術活用委員会確認中）
  - 目的：「表4　安全性と相互接続性についての比較」の記載内容変更に伴い、セキュリティ例外型の記述見直し

＜改訂前＞

「セキュリティ例外型」は、システム等の制約上、脆弱なプロトコルバージョンであるSSL3.0の利用を全面禁止することのほうが現時点ではデメリットが大きく、安全性上のリスクを受容してでもSSL3.0を継続利用せざるを得ないと判断される場合にのみ採用すべきである。

したがって、セキュリティ例外型を採用する際は、推奨セキュリティ型への早期移行を前提として、移行計画や利用終了期限を定めたりするなど、今後への具体的な対処方針の策定をすべきである。また、金融サービスや電子商取引サービスなど、不特定多数に公開されるサービス等において使用されるSSL/TLSサーバであって、やむなくセキュリティ例外型を採用している場合では、利用者に対して「SSL3.0の利用を許可しており、脆弱な暗号方式が使われる場合がある」等の注意喚起を行うことが望ましい。

＜改訂後＞

「セキュリティ例外型」は、システム等の制約上、脆弱なプロトコルバージョンであるSSL3.0の利用を全面禁止することが現実的ではなく、安全性上のリスクを受容してでもSSL3.0を継続利用せざるを得ないと判断される場合にのみ採用すべきである。

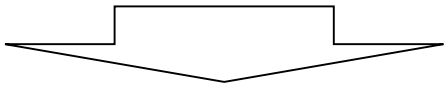
したがって、セキュリティ例外型を採用する際は、推奨セキュリティ型への移行完了までの短期の暫定運用として、移行計画や利用終了期限を定めたりするなど、今後への具体的な対処方針の策定をすべきである。~~また、金融サービスや電子商取引サービスなど、不特定多数に公開されるサービス等において使用されるSSL/TLSサーバであって、やむなくセキュリティ例外型を採用している場合では、利用者に対して「SSL3.0の利用を許可しており、脆弱な暗号方式が使われる場合がある」等の注意喚起を行うことが望ましい。~~

アップデート案詳細

■ 3.2 要求設定の概要

- P.18 表5 要求設定の概要
- 目的:ガイドラインアップデートに伴う記述見直し

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
想定対象		G2G	一般	レガシー携帯電話含む
暗号スイートの（暗号化の）セキュリティレベル		①256 bit ②128 bit	①128 bit ②256 bit	① 128 bit ② 256 bit ③ RC4, Triple DES
暗号アルゴリズム	・・・	・・・	・・・	
	ハッシュ関数	SHA-384, SHA-256	SHA-384, SHA-256, SHA-1	
プロトコルバージョン		TLS1.2のみ	TLS1.2 ～ TLS1.0	TLS1.2～1.0, SSL3.0



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
想定対象		G2G等	一般	推奨セキュリティ型以上の設定が現実的ではない等の特殊事情があるケースに限定
暗号スイートの（暗号化の）セキュリティレベル		①256 bit ②128 bit	①128 bit ②256 bit	① 128 bit ② 256 bit ③ RC4, Triple DES
暗号アルゴリズム	・・・	・・・	・・・	
	ハッシュ関数	SHA-384, SHA-256	SHA-384, SHA-256, SHA-1*	SHA-384, SHA-256, SHA-1
プロトコルバージョン		TLS1.2のみ	TLS1.2 ～ TLS1.0	TLS1.2～1.0, SSL3.0

*** 署名生成及び証明書での利用を除く**

アップデート案詳細

■ EC曲線系のパテントリスクの記述

- 目的：EC曲線系のパテントリスクの記述を見直しの必要性是非

- 該当個所のパテントリスクに関する記述は削除する

  （P.23）この他、非技術的要因として、ECDSAを採用する際にはパテントリスクの存在 が広く指摘されているので、十分な検討のうえで採用の可否を決めることが望ましい。

  （P.39）また、非技術的要因として、ECDHやECDSAを採用する際にはパテントリスクの存在が広く指摘されているので、十分な検討のうえで採用の可否を決めることが望ましい。

  （P.40）パテントリスクについても検討したうえでECDHやECDSAを採用することを決めた場合には、表11の暗号スイートグループを追加してよい。

  （P.42）パテントリスクについても検討したうえでECDHやECDSAを採用することを決めた場合には、表13の暗号スイートグループを追加してよい。

- Appendix Aのチェックリストからも「パテントリスクを考慮したうえで楕円曲線暗号を利用すると決めたか」の部分を削除

□ ④-ii) 楕円曲線暗号を利用する場合は左の□と以下の項目をチェック		
~~④-ii-1) パテントリスクを考慮したうえで楕円曲線暗号を利用すると決めたか~~	~~6.1節~~	~~□~~
④-ii-1) 表1記載の暗号スイート（網掛けを含む）の全部または一部を設定したか	6.1節／6.5.1節	□
④-ii-2) 表1記載のグループαの暗号スイート（網掛けを含む）から少なくとも一つは設定したか	6.1節／6.5.1節	□
④-ii-3) 表1記載の暗号スイートのグループ順番（グループαの暗号スイートの次にグループβの暗号スイートが並ぶ）を守っているか	6.1節／6.5.1節	□
④-ii-4) 表1記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.1節	□
④-ii-5) ECDHEによる鍵交換の鍵長を256ビット以上に設定したか	6.1節／6.5.1節	□

アップデート案詳細

- 最新動向を反映した記述内容の新規追加・削除を行う項目の詳細

（主にTLS1.3の記述追加）

- 2.1.1 SSL/TLSの歴史
  - 目的：データの更新、及びTLS1.3についての記述追加
- 2.1.3　TLS1.3の特徴
  - 目的：TLS1.3についての記述追加
- 2.1.4 TLSプロトコルの最新動向
  - 目的：過去3年間のTLS1.3以外のTLSに関する動向の記述追加

（ブラウザ側の対応を踏まえた記述修正）

- 8.3.1　鍵長1024ビット、SHA-1を利用するサーバ証明書の警告表示
  - 目的：警告から無効化が進んだことによる記述修正

（歴史的経緯としてコラム化を検討）

- 8.3.2　SSL3.0の取り扱い
  - 目的：SSL3.0の無効化が進んだことによる記述削除

アップデート案詳細

- 最新データへの更新（及びそれに伴う記述更新）を行う項目
  - 6.3.3 DHE/ECDHEでの鍵長の設定状況についての注意
    - P38　図4　DHE/ECDHEの鍵長の設定状況（Alexaの調査結果を加工）
    - 目的：データの更新
  - 7.1.1 サーバ証明書での脆弱な鍵ペアの使用の回避
    - P45　既知の解読可能な鍵ペアでないことを確認するサービス
    - 目的：サービスの停止に伴う更新
  - 7.1.3 サーバ証明書の有効期限
    - P.46 – P.47　サーバ証明書の更新作業時の考慮点
    - 目的：既存の鍵ペアでのサーバ証明書の再発行期限が厳格化されたため
  - 7.2.1 HTTP Strict Transport Security（HSTS）の設定有効化
    - P.49　HSTSの記述
    - 目的：HSTSの実装状況の変化に伴う記述更新
  - 7.2.4 OCSP Staplingの設定有効化
    - P52　OCSP Staplingの記述
    - 目的：OCSP Staplingの実装状況の変化に伴う記述更新

アップデート案詳細

- 最新データへの更新（及びそれに伴う記述更新）を行う項目（続）
  - 7.2.5 Public Key Pinningの設定有効化
    - P53 Public Key Pinningの記述
    - 目的：Public Key Pinningの実装状況の変化に伴う記述更新
  - 8.1　本ガイドラインが対象とするブラウザ
    - P55　8.1.1　対象とするプラットフォーム
    - 目的：サポート状況の変化に伴う記述更新
    - P55　8.1.2　対象とするブラウザのバージョン
    - 目的：サポート状況の変化に伴う記述更新
  - 8.2　設定に関する確認項目
    - P56　8.2.2　設定項目　設定項目を標準機能で提供していないブラウザ
    - 目的：サポート状況の変化に伴う記述更新
    - P.56　8.2.2　設定項目　設定項目を標準機能で提供しているブラウザ
    - 目的：サポート状況の変化に伴う記述更新

アップデート案詳細

- エディトリアル的な記述内容の修正を行う項目の詳細
  - 1.1　本書の内容及び位置付け
    - 目的:ガイドラインアップデートに伴う記述修正
  - 2.2.1　CRYPTREC暗号リスト
    - 目的:統一基準改定に伴う記述更新
  - 2.2.2 異なる暗号アルゴリズムにおける安全性の見方
    - 目的:NIST SP改定に伴う記述更新
  - 5.4.3 サーバ証明書で利用すべき鍵長
    - 目的: CRYPTREC Report最新版への更新
  - 6.2 暗号スイートで利用可能な候補となる暗号アルゴリズム
    - 目的:NIST SP改定に伴う記述更新

アップデート案詳細

- コラムの更新
  - 現在載っているコラム　→　おおむね役割を終えたと判断
    - SSL3.0への大打撃となったPOODLE攻撃
    - 実際にあった！漏えいしたかもしれない鍵ペアを再利用した証明書の再発行
    - 輸出規制時代の名残ーFREAK攻撃
    - DigiNotar認証局事件
  - 最近の話題からの候補例
    - ○Measuring HTTPS Adoption on the Web関連
    - ○SSL3.0、RC4、Triple DESなどの歴史
    - Symantecのサーバ証明書がChromeとFirefoxで無効化
    - PCI DSSのTLS1.2化
    - 上記の候補に加え、期日を決めてテーマを募集することとする
- Appendix B（サーバ設定編）及びAppendix C（暗号スイートの設定例）のガイドラインからの分離
  - 製品依存であり更新サイクルが早いこと、更新に当たっては実機での確認を要することなどの理由から別管理情報に位置づける
  - 本ガイドラインからは、リンク情報として誘導する

資料５別添２

「SSL/TLS 暗号設定ガイドライン」アップデート案

【凡例】

- （左側ページ）「改訂前」・・・現在のガイドラインでの記載内容
  - 黄色ハッチングの部分が修正個所

- （右側ページ）「改訂後」・・・記載内容の修正案
  - 水色ハッチングの部分が修正案。なお、改訂前に記載がないものについてはハッチングをしていない

（暗号技術活用委員会確認中）

*)　1.1　本書の内容及び位置付け

P.6　本文

目的：ガイドラインアップデートに伴う記述修正

- 改訂前

　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 SSL/TLS サーバの設定方法を示すものである。

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や、個別製品での具体的な設定方法例も記載している。

- 改訂後

本ガイドラインは、2018 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 SSL/TLS サーバの設定方法を示すものである。前バージョン以前の本ガイドラインを利用している場合には、今バージョンでの設定要件に基づいた見直しを行い、必要に応じて設定変更を実施することが望ましい。

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。

A) 2.1.1 SSL/TLS の歴史

P.9　表 2　SSL/TLS のバージョン概要

目的：データの更新、及び TLS1.3 についての記述追加

➢　改訂前

バージョン	概要
SSL2.0 （1994）	● いくつかの脆弱性が発見されており、なかでも「ダウングレード攻撃（最弱のアルゴリズムを強制的に使わせることができる）」と「バージョンロールバック攻撃（SSL2.0 を強制的に使わせることができる）」は致命的な脆弱性といえる ● SSL2.0 は利用すべきではなく、実際に 2005 年頃以降に出荷されているサーバやブラウザでは SSL2.0 は初期状態で利用不可となっている
SSL3.0 （RFC6101） （1995）	● SSL2.0 での脆弱性に対処したバージョン ● 2014 年 10 月に POODLE[1]攻撃が発表されたことにより特定の環境下での CBC モードの利用は危険であることが認識されている。POODLE 攻撃は、SSL3.0 におけるパディングチェックの仕方の脆弱性に起因しているため、この攻撃に対する回避策は現在のところ存在していない ● POODLE 攻撃の発表を受け、必要に応じてサーバやブラウザの設定を変更し、SSL3.0 を無効化にするよう注意喚起されている [2]
TLS1.0 （RFC2246） （1999）	● 2015 年 3 月時点では、もっとも広く実装されているバージョンであり、実装率はほぼ 100% ● ブロック暗号を CBC モードで利用した時の脆弱性を利用した攻撃（BEAST 攻撃など）が広く知られているが、容易な攻撃回避策が存在し、すでにセキュリティパッチも提供されている。また、SSL3.0 で問題となった POODLE 攻撃は、プロトコルの仕様上、TLS1.0 には適用できない ● 暗号スイートとして、より安全なブロック暗号の AES と Camellia、並びに公開鍵暗号・署名に楕円曲線暗号が利用できるようになった ● 秘密鍵の生成などに擬似乱数関数を採用 ● MAC の計算方法を HMAC に変更
TLS1.1 （RFC4346） （2006）	● ブロック暗号を CBC モードで利用した時の脆弱性を利用した攻撃（BEAST 攻撃等）への対策を予め仕様に組み入れるなど、TLS1.0 の安全性強化を図っている ● 実装に関しては、規格化された年が TLS1.2 とあまり変わらなかったため、TLS1.1 と TLS1.2 は同時に実装されるケースも多く、2015 年 3 月時点でのサーバやブラウザ全体における実装率は約 50%
TLS1.2 （RFC5246） （2008）	● 暗号スイートとして、より安全なハッシュ関数 SHA-256 と SHA-384、CBC モードより安全な認証付暗号利用モード（GCM、CCM）が利用できるようになった。特に、認証付暗号利用モードでは、利用するブロック暗号が同じであっても、CBC モードの脆弱性を利用した攻撃（BEAST 攻撃等）がそもそも適用できない ● 必須の暗号スイートを TLS_RSA_WITH_AES_128_CBC_SHA に変更 ● IDEA と DES を使う暗号スイートを削除 ● 擬似乱数関数の構成を MD5/SHA-1 ベースから SHA-256 ベースに変更 ● 本格的に実装が始まったのは最近であり、2015 年 3 月時点でのサーバやブラウザ全体における実装率は約 55%

[1] POODLE: Padding Oracle On Downgraded Legacy Encryption

[2] SSL3.0 の脆弱性対策について、http://www.ipa.go.jp/security/announce/20141017-ssl.html

➢ 改訂後

バージョン	概要
SSL2.0 （1994）	● いくつかの脆弱性が発見されており、なかでも「ダウングレード攻撃（最弱のアルゴリズムを強制的に使わせることができる）」と「バージョンロールバック攻撃（SSL2.0 を強制的に使わせることができる）」は致命的な脆弱性といえる ● SSL2.0 は利用すべきではなく、~~実際に~~2005 年頃以降に出荷されているサーバやブラウザでは SSL2.0 は初期状態で利用不可となっている
SSL3.0 （RFC6101） （1995）	● SSL2.0 での脆弱性に対処したバージョン ● 2014 年 10 月に POODLE[3]攻撃が発表されたことにより特定の環境下での CBC モードの利用は危険であることが認識されている。POODLE 攻撃は、SSL3.0 におけるパディングチェックの仕方の脆弱性に起因しているため、この攻撃に対する回避策は現在のところ存在していない ● POODLE 攻撃の発表を受け、2018 年 3 月時点での主流の最新版ブラウザで SSL3.0 は初期状態で利用不可となっている
TLS1.0 （RFC2246） （1999）	● 2018 年 3 月時点での SSL Pulse の調査結果 [4]によれば、約 12 万の主要なサイトについて TLS1.0 が利用できるのは約 88% ● ブロック暗号を CBC モードで利用した時の脆弱性を利用した攻撃（BEAST 攻撃など）が広く知られているが、容易な攻撃回避策が存在し、すでにセキュリティパッチも提供されている。また、SSL3.0 で問題となった POODLE 攻撃は、プロトコルの仕様上、TLS1.0 には適用できない ● 暗号スイートとして、より安全なブロック暗号の AES と Camellia、並びに公開鍵暗号・署名に楕円曲線暗号が利用できるようになった ● 秘密鍵の生成などに擬似乱数関数を採用 ● MAC の計算方法を HMAC に変更
TLS1.1 （RFC4346） （2006）	● ブロック暗号を CBC モードで利用した時の脆弱性を利用した攻撃（BEAST 攻撃等）への対策を予め仕様に組み入れるなど、TLS1.0 の安全性強化を図っている ● 実装に関しては、規格化された年が TLS1.2 とあまり変わらなかったため、TLS1.1 と TLS1.2 は同時に実装されるケースも多く、2018 年 3 月時点での SSL Pulse の調査結果 [4]によれば約 12 万の主要なサイトについて TLS1.1 が利用できるのは約 85%
TLS1.2 （RFC5246） （2008）	● 暗号スイートとして、より安全なハッシュ関数 SHA-256 と SHA-384、CBC モードより安全な認証付き秘匿モード（GCM、CCM）が利用できるようになった。特に、認証付き秘匿モードでは、利用するブロック暗号が同じであっても、CBC モードの脆弱性を利用した攻撃（BEAST 攻撃等）がそもそも適用できない ● 必須の暗号スイートを TLS_RSA_WITH_AES_128_CBC_SHA に変更 ● IDEA と DES を使う暗号スイートを削除 ● 擬似乱数関数の構成を MD5/SHA-1 ベースから SHA-256 ベースに変更 ● ~~本格的に実装が始まったのは最近であり、~~2018 年 3 月時点での SSL Pulse の調査結果 [4]によれば約 12 万の主要なサイトについて TLS1.2 が利用できるのは約 91%
TLS1.3 *（draft23）*	● 共通鍵暗号は認証暗号：AEAD（Authenticated Encryption with Associated Data）のみ採用した結果、AES GCM/CCM と ChaCha20-Poly1305 のみになった ● 鍵交換は、DHE/ECDHE のみで楕円曲線を指定した ● 署名は、RSA-PSS、RSASSA-PKCS1-v1_5、ecdsa_secp256r1 が必須になった ● ハッシュは SHA-256 以上になった ● ハンドシェイク性能の向上のため、1-RTT、0-RTT（Round Trip Time）になるようにシーケンスが簡素化された ● ハンドシェイクのデータを暗号化して保護した ● TLS1.2 互換に配慮し、ClientHello、ServerHello、ChangeCipherSpec が規定された ● *まだ draft であるが、*サーバやブラウザで実装が始まっている

※ ガイドラインアップデート版公開までに、TLS1.3 の RFC が発行されれば draft を削除。RFC が発行されなければ、「RFC Editor Queue」と表記します。

[3] POODLE: Padding Oracle On Downgraded Legacy Encryption
[4] https://www.ssllabs.com/ssl-pulse/

B) 2.1.3　TLS1.3 の特徴

新設のセクション

目的：TLS1.3 についての記述追加

- 改訂前

  記述なし

C) 2.1.4 TLS プロトコルの最新動向

新設のセクション

目的：過去 3 年間の TLS1.3 以外の TLS に関する動向の記述追加

- 改訂前

  記述なし

➢ 改訂後

TLS1.3 は、TLS1.2 策定以降に見つかった新たな脆弱性や攻撃手法への対策を施すと共に、QUIC 等のプロトコルに対応するための性能向上を狙いとして、プロトコルとアルゴリズムの抜本的な再設計が行われた。TLS1.2 との互換性などの課題があり、2018 年 1 月現在標準化作業は続いている。2018 年 1 月現在の最新仕様は draft23 である。

TLS1.2 との差異の観点から見た主な特徴を以下に示す。

(1) 脆弱なアルゴリズムとして、Triple DES、DSA、RC4、MD5、SHA-1、SHA-224、静的な RSA が削除された。また、認証暗号（AEAD）でない AES の CBC モードが削除された。
(2) NIST 規定でないアルゴリズムとして、共通鍵暗号の ChaCha20 と署名の EdDSA が追加された。
(3) 鍵交換は、DHE、ECDHE が必須になった。楕円曲線として secp256r1 が必須になった。
(4) 脆弱なハンドシェイク機能として、リネゴシエーション、圧縮、セッション回復が削除された。
(5) ServerHello 以降のハンドシェイクパラメータを暗号化して保護する。
(6) HMAC ベースの導出関数を使った鍵導出に変更された。
(7) 性能向上のため、1-RTT でハンドシェイクが完了するようにメッセージおよび拡張が見直された。
(8) QUIC 等への適用を考慮し、0-RTT でアプリデータを送信する機能が追加された。
(9) ClientHello、ServerHello、ChangeCipherSpec の TLS1.2 互換性を保つことにより、中間ノードによる接続性を向上した。

※(5)～(8)についてはシーケンス図も加工して挿入予定

➢ 改訂後

2015 年 4 月以降に発行された SSL/TLS に関する RFC 32 件のうち、「プロトコルバージョン」「サーバ証明書」「暗号スイート（暗号アルゴリズム)」の 3 つの観点から、利用可否や利用期間などの記述が含まれるものは、以下のとおりである。例えば、既存の TLS1.2 までのプロトコルに対して、SSL3.0 の無効化や RC4 の無効化など、プロトコルの脆弱性の排除に関するものが規格化されている。

RFC	タイトル	概要
7465	Prohibiting RC4 Cipher Suites	RC4 を含む暗号スイートの禁止
7507	TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks	SSL/TLS プロトコルのダウングレード攻撃を防ぐための TLS Fallback Signaling Cipher Suite Value (SCSV)暗号スイートの追加
7525	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)	SSL2.0、SSL3.0 リネゴシエーションの禁止 TLS1.0、TLS1.1 リネゴシエーションの非推奨
7568	Deprecating Secure Sockets Layer Version 3.0	SSL3.0 の禁止
7905	ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)	ChaCha20-Poly1305 を含む暗号スイートの追加

D) 2.2.1　CRYPTREC 暗号リスト

P.11　政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）

目的：統一基準改定に伴う記述更新

- 改訂前

「政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）」（平成 26 年 5 月 19 日、情報セキュリティ政策会議） では以下のように記載されており、 政府機関における情報システムの調達及び利用において、CRYPTREC 暗号リストのうち「電子政府推奨暗号リスト」が原則的に利用される。

政府機関の情報セキュリティ対策のための統一基準（抄）

6.1.5 暗号・電子署名－遵守事項(1)(b)

情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム及び運用方法について、以下の事項を含めて定めること。

（ア） 行政事務従事者が暗号化及び電子署名に対して使用するアルゴリズムについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

（イ） 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズムを採用すること。

（以下、略）

E) 2.2.2 異なる暗号アルゴリズムにおける安全性の見方

P.12　 NIST SP800-57 Part 1

目的：NIST SP 改定に伴う記述更新

- 改訂前

例えば、NIST SP800-57 Part 1 revision 3[5]では、表 3 のように規定している。

[5] NIST SP800-57, Recommendation for Key Management – Part 1: General (Revision 3)

➢ 改訂後

「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」（平成 28 年 8 月 31 日、サイバーセキュリティ戦略本部）では以下のように記載されており、政府機関における情報システムの調達及び利用において、CRYPTREC 暗号リストのうち「電子政府推奨暗号リスト」が原則的に利用される。

政府機関の情報セキュリティ対策のための統一基準（抄）

6.1.5 暗号・電子署名－遵守事項(1)(b)

情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム並びにそれを利用した安全なプロトコル及びその運用方法について、以下の事項を含めて定めること。

(ア) 行政事務従事者が暗号化及び電子署名に対して使用するアルゴリズム及びそれを利用した安全なプロトコルについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。

(イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。

（以下、略）

➢ 改訂後

例えば、NIST SP800-57 Part 1 revision 4[6]では、表 3 のように規定している。

[6] NIST SP800-57, Recommendation for Key Management – Part 1: General (Revision 4)

F) 3.1　実現すべき設定基準の考え方

P.16　表 4　安全性と相互接続性についての比較

目的：特に、セキュリティ例外型の記述見直し

- 改訂前

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して 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** ＜利用例＞ 政府内利用（G2G 型）のなかでも、限定された接続先に対して、とりわけ高い安全性が要求される通信を行う場合	本ガイドラインの公開時点（2015 年 5 月）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** ＜利用例＞ • 政府内利用（G2G 型）や社内システムへのリモートアクセスなど、特定された通信相手との安全な通信が要求される場合 • 電子申請など、企業・国民と役所等との電子行政サービスを提供する場合 • 金融サービスや電子商取引サービス、多様な個人情報の入力を必須とするサービス等を提供する場合 • 既存システムとの相互接続を考慮することなく、新規に社内システムを構築する場合	本ガイドラインの公開時点（2015 年 5 月）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（8.1.2 節）が搭載されている PC、スマートフォンなどでは問題なく相互接続性を確保できる 本ガイドラインが対象としない、バージョンが古い OS やブラウザの場合や発売開始からある程度の年月が経過している一部の古い機器（フィーチャーフォンやゲーム機など）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** ＜利用例＞ • 利用するサーバやクライアントの実装上の制約、もしくは既存システムとの相互接続上の制約により、推奨セキュリティ型（以上）の設定が事実上できない場合	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（2015 年 5 月）において許容可能な最低限の安全性水準を満たす	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

➢ 改訂後

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して 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~~** ＜利用例＞ 政府内利用（G2G 型）のなかでも、~~限定された接続先に対して、~~とりわけ高い安全性が要求される通信を行う場合	本ガイドラインの公開時点（2018 年 5 月）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	本ガイドラインで対象とするブラウザ（8.1.2 節）が搭載されている PC、スマートフォンなどでは問題なく相互接続性を確保できる。 本ガイドラインが対象としない、バージョンが古い OS やブラウザの場合や発売開始からある程度の年月が経過している一部の古い機器（フィーチャーフォンやゲーム機など）については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** ＜利用例＞ • 政府内利用（G2G 型）や社内システムへのリモートアクセスなど、特定された通信相手との安全な通信が要求される場合 • 電子申請など、企業・国民と役所等との電子行政サービスを提供する場合 • 金融サービスや電子商取引サービス、多様な個人情報の入力を必須とするサービス等を提供する場合 • 既存システムとの相互接続を考慮することなく、新規に社内システムを構築する場合	本ガイドラインの公開時点（2018 年 5 月）における標準的な安全性水準を実現	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。 ※すでにサポートが切れているなどかなり古い機器などで接続できない場合があるが、この種の機器は本来接続させるべきではない。
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であって、推奨セキュリティ型への移行完了までの短期の暫定運用としての設定基準 **~~※推奨セキュリティ型への早期移行を求めるものであり、すでに最低限の安全性水準を満たしているとは言えない状況になっている~~** ＜利用例＞ • 利用するサーバやクライアントの実装上の制約、もしくは既存システムとの相互接続上の制約により、推奨セキュリティ型（以上）の設定が事実上できない場合	~~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（2018 年 5 月）において、最低限度の安全性水準を満たしているとは言えない状況になっている。速やかな推奨セキュリティ型への移行を強く求める。	~~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。

（暗号技術活用委員会確認中）

P.15　本文

目的：「表 4　安全性と相互接続性についての比較」の記載内容変更に伴い、セキュリティ例外型の記述見直し

- 改訂前

「セキュリティ例外型」は、システム等の制約上、脆弱なプロトコルバージョンである SSL3.0 の利用を全面禁止することのほうが現時点ではデメリットが大きく、安全性上のリスクを受容してでも SSL3.0 を継続利用せざるを得ないと判断される場合にのみ採用すべきである。なお、セキュリティ例外型であっても、SSL3.0 の無期限の継続利用を認めているわけではなく、近いうちに SSL3.0 を利用不可に設定するように変更される可能性がある。

また、SSL3.0 を利用する関係から、利用可能な暗号スイートの設定においても、脆弱な暗号アルゴリズムである RC4 の利用を認めている。ただし、本来的には RC4 は SSL3.0 に限定して利用すべきであるが、TLS1.0 以上のプロトコルバージョンで RC4 の利用を不可にする設定を行うことが難しいため、TLS1.0 以上であっても RC4 が使われる可能性が排除できないことにも注意されたい。

したがって、セキュリティ例外型を採用する際は、推奨セキュリティ型への早期移行を前提として、移行計画や利用終了期限を定めたりするなど、今後への具体的な対処方針の策定をすべきである。また、金融サービスや電子商取引サービスなど、不特定多数に公開されるサービス等において使用される SSL/TLS サーバであって、やむなくセキュリティ例外型を採用している場合では、利用者に対して「SSL3.0 の利用を許可しており、脆弱な暗号方式が使われる場合がある」等の注意喚起を行うことが望ましい。

---

*) 3.2　　要求設定の概要

P.18　表 5　要求設定の概要

目的：ガイドラインアップデートに伴う記述見直し

- 改訂前

<table>
<tr><th colspan="2">要件</th><th>高セキュリティ型</th><th>推奨セキュリティ型</th><th>セキュリティ例外型</th></tr>
<tr><td colspan="2">想定対象</td><td>G2G</td><td>一般</td><td>レガシー携帯電話含む</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 bit
②128 bit</td><td>①128 bit
②256 bit</td><td>① 128 bit
② 256 bit
③ RC4, Triple DES</td></tr>
<tr><td rowspan="5">暗号アルゴリズム</td><td>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
鍵長 2048 ビット以上の RSA
鍵長 256 ビット以上の ECDH</td></tr>
<tr><td>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
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>

➢ 改訂後

「セキュリティ例外型」は、システム等の制約上、脆弱なプロトコルバージョンである SSL3.0 の利用を全面禁止することが現実的ではなく、安全性上のリスクを受容してでも SSL3.0 を継続利用せざるを得ないと判断される場合にのみ採用すべきである。なお、セキュリティ例外型であっても、SSL3.0 の無期限の継続利用を認めているわけではなく、近いうちに SSL3.0 を利用不可に設定するように変更される可能性がある。

また、SSL3.0 を利用する関係から、利用可能な暗号スイートの設定においても、脆弱な暗号アルゴリズムである RC4 の利用を認めている。ただし、本来的には RC4 は SSL3.0 に限定して利用すべきであるが、TLS1.0 以上のプロトコルバージョンで RC4 の利用を不可にする設定を行うことが難しいため、TLS1.0 以上であっても RC4 が使われる可能性が排除できないことにも注意されたい。

したがって、セキュリティ例外型を採用する際は、推奨セキュリティ型への移行完了までの短期の暫定運用として、移行計画や利用終了期限を定めたりするなど、今後への具体的な対処方針の策定をすべきである。~~また、金融サービスや電子商取引サービスなど、不特定多数に公開されるサービス等において使用される SSL/TLS サーバであって、やむなくセキュリティ例外型を採用している場合では、利用者に対して「SSL3.0 の利用を許可しており、脆弱な暗号方式が使われる場合がある」等の注意喚起を行うことが望ましい。~~

➢ 改訂後

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
想定対象		G2G 等	一般	推奨セキュリティ型以上の設定が現実的ではない等の特殊事情があるケースに限定
暗号スイートの（暗号化の）セキュリティレベル		①256 bit ②128 bit	①128 bit ②256 bit	① 128 bit ② 256 bit ③ RC4, Triple DES
暗号アルゴリズム	鍵交換	鍵長 2048 ビット以上の DHE または 鍵長 256 ビット以上の ECDHE	鍵長 1024 ビット以上の DHE または鍵長 256 ビット以上の ECDHE	
			鍵長 2048 ビット以上の RSA 鍵長 256 ビット以上の ECDH	
	暗号化	鍵長 128 ビット及び 256 ビットの AES または Camellia		
				RC4 Triple DES
	モード	GCM	GCM, CBC	
	ハッシュ関数	SHA-384, SHA-256	SHA-384, SHA-256, SHA-1*	SHA-384, SHA-256, SHA-1
プロトコルバージョン		TLS1.2 のみ	TLS1.2 ～ TLS1.0	TLS1.2～1.0, SSL3.0
証明書鍵長		鍵長 2048 ビット以上の RSA または 鍵長 256 ビット以上の ECDSA		
証明書でのハッシュ関数		SHA-256		SHA-256, SHA-1

* 署名生成及び証明書での利用を除く

G) 5.4.3 サーバ証明書で利用すべき鍵長

P.30　CRYPTREC Report 2013

目的：最新版への更新

- 改訂前

  詳細については、CRYPTREC Report 2013[7] 図 3.1、図 3.2 を参照されたい。

H)　6.2 暗号スイートで利用可能な候補となる暗号アルゴリズム

P.35 脚注　NIST SP800-52 revision 1 (draft)

目的：NIST SP 改定に伴う記述更新

- 改訂前

  [7]NIST SP800-52 revision 1 (draft), Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

[7] http://www.cryptrec.go.jp/report/c13_eval_web_final.pdf

➢ 改訂後

詳細については、CRYPTREC Report 2016[8] 図 3.3、図 3.4 を参照されたい。

➢ 改訂後

[7]NIST SP800-52 revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

[8] http://www.cryptrec.go.jp/report/cryptrec-rp-0002-2016.pdf

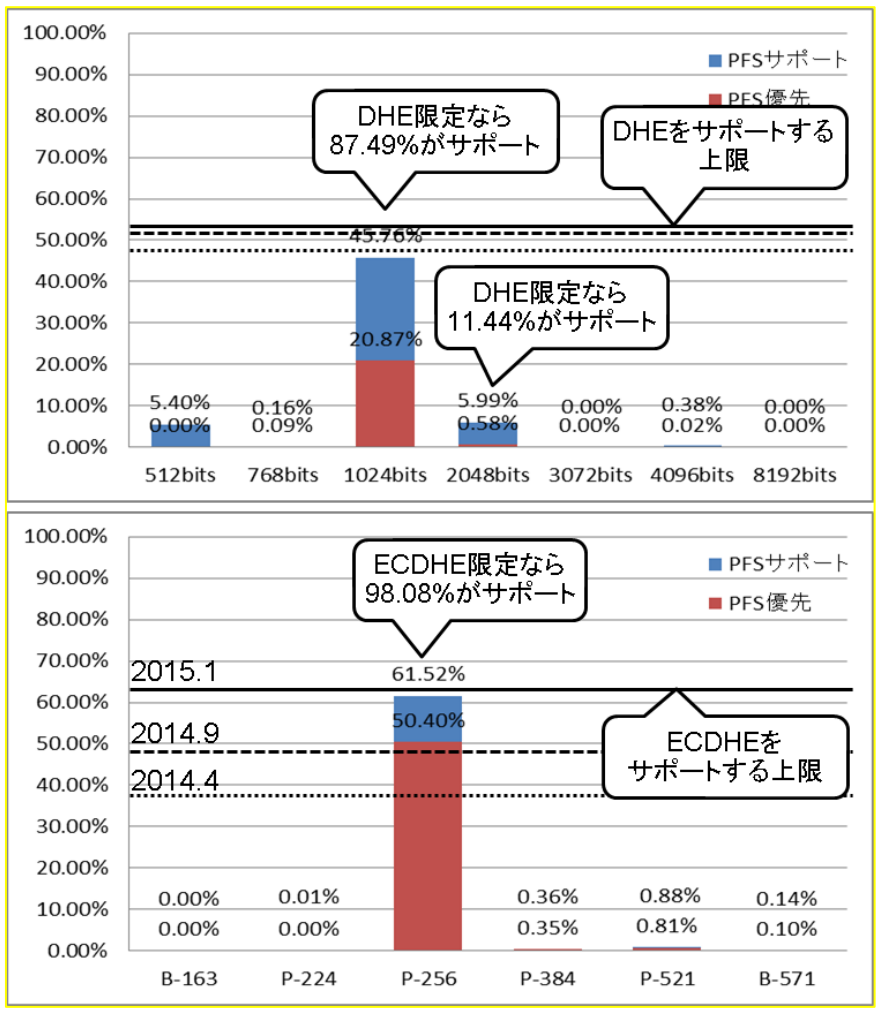
I)　6.3.3 DHE/ECDHE での鍵長の設定状況についての注意

P.38　図 4　DHE/ECDHE の鍵長の設定状況（Alexa の調査結果を加工）

目的：データの更新

- 改訂前

  図 4 の 2015 年 1 月の Alexa の調査結果 [9]によれば、約 47 万の主要なサイトについて、DHE が利用できるのは約 52.3%であり、そのうちの約 87.5%（全体では約 45.8%）が鍵長 1024 ビットを採用している。一方、ECDHE が利用できるのは約 62.7%であり、そのうちの約 98%（全体では約 61.5%）が鍵長 256 ビットを採用している。



（P.39）

これらについては、DHE の鍵長を指定することができず、クライアント側からの指定により 512 ビット、1024 ビット等の弱い鍵パラメータが使われる可能性がある。例えば、サーバ側の設定が鍵長 2048 ビット対応可能だったとしても、本ガイドライン公開時点（2015 年 5 月）では、ブラウザ（クライアント）側が鍵長 2048 ビットに対応していない可能性が十分に考えられる。その場合には、サーバ側は鍵長 1024 ビットを自動的に選択することに注意を要する。

J) 7.1.1 サーバ証明書での脆弱な鍵ペアの使用の回避

P.45 脚注　既知の解読可能な鍵ペアでないことを確認するサービス

目的：サービスの停止に伴う更新

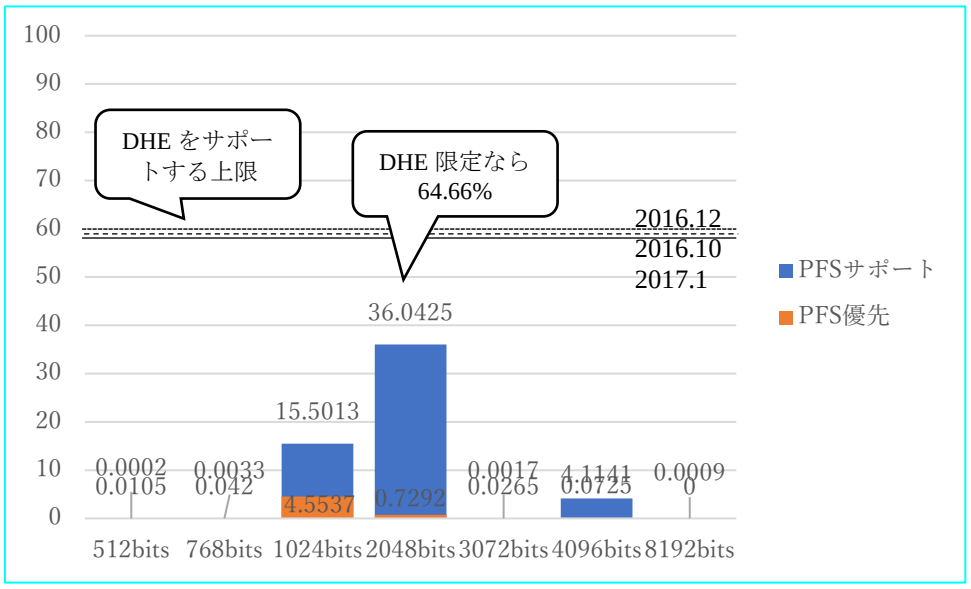
- 改訂前

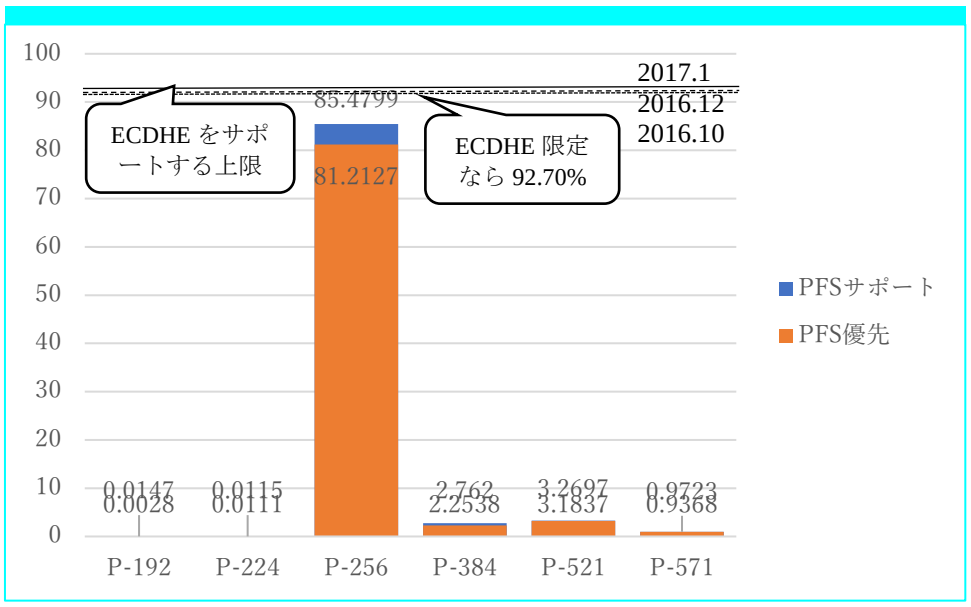
  [12] 例えば https://factorable.net/keycheck.html がある。ただし、安全性を 100%証明するものではないことに注意されたい

[9] https://securitypitfalls.wordpress.com/2015/02/01/january-2015-scan-results/

➢ 改訂後

図 4 の 2017 年 1 月の Alexa の調査結果 [10]によれば、約 47 万の主要なサイトについて、DHE が利用できるのは約 55.7%であり、そのうちの約 64.7%（全体では約 36.0%）が鍵長 2048 ビットを採用している。一方、ECDHE が利用できるのは約 92.2%であり、そのうちの約 92.7%（全体では約 85.4%）が鍵長 256 ビットを採用している。





(P.39)

これらについては、DHE の鍵長を指定することができず、クライアント側からの指定により ~~512 ビット、~~1024 ビット等の弱い鍵パラメータが使われる可能性がある。例えば、サーバ側の設定が鍵長 2048 ビット対応可能だったとしても、~~本ガイドライン公開時点（2015 年 5 月）では、~~ブラウザ（クライアント）側が鍵長 2048 ビットに対応していない~~可能性が十分に考えられる。その~~場合には、サーバ側は鍵長 1024 ビットを自動的に選択することに注意を要する。

➢ 改訂後

[12] 例えば https://keytester.cryptosense.com/がある。ただし、安全性を 100%証明するものではないことに注意されたい

[10] https://securitypitfalls.wordpress.com/2017/04/17/january-2017-scan-results/

K) 7.1.3 サーバ証明書の有効期限

P.46 – P.47　サーバ証明書の更新作業時の考慮点

目的：既存の鍵ペアでのサーバ証明書の再発行期限が厳格化されたため

- 改訂前

市販されているサーバ証明書の有効期間は、半年や 1 年程度のものから、2 年、3 年程度のもの等様々である。一般に、有効期間が長いほど、サーバ証明書の更新頻度が少なく更新作業の工数を削減できる。しかし、その反面、単純なミスによる更新忘れ、組織改編・担当者異動時の引き継ぎ不備による更新漏れ、鍵危殆化（秘密鍵の漏えい）リスクの増大、サーバ証明書に記載されたサーバの運営組織情報が（組織名変更などにより）正確でなくなるリスクの増大、アルゴリズム Agility（セキュリティ強度の変化に対して、安全な側に移行するための対策に要する時間、迅速さの程度）の低下などが危惧されるようになる。特に、2 年や 3 年など比較的長い間有効なサーバ証明書を利用する場合には、管理者がサーバ証明書の有効期限切れに気づかず、更新漏れによるサービス障害の発生が大きなリスクとなりえる。

これらを総合的に勘案し、特段の制約が存在しない限り、サーバ管理者は、1 年程度の有効期間を持つサーバ証明書を選択し、サーバ証明書の更新作業を、年次の定型業務と位置付けることが望ましい。

L) 7.2.1 HTTP Strict Transport Security（HSTS）の設定有効化

P.49　HSTS の記述

目的：HSTS の実装状況の変化に伴う記述更新

- 改訂前

以上のように、HTTPS で安全にサービスを提供したい場合などでは、ユーザに意識させることなくミスを防止でき、ユーザの利便性を向上させることができるので、HSTS の機能を持っているならば有効にすることを推奨する。参考までに、いくつかの設定例を Appendix B.4 で紹介する。

ただし、HSTS が実際に機能するためには、サーバだけでなく、ブラウザも対応している必要があることに注意されたい。また、一度も接続したことがないサーバ（例外的に Firefox 17 以降ではあらかじめ登録されているサーバもある）や、HSTS の期限切れになったサーバの場合にも、HTTPS への変換は行われない。

2014 年 9 月時点での主要な製品の HSTS へのサポート状況は以下の通りである。

- サーバ
  - Apache 2.2.22 以降：設定により可能
  - Lighttpd 1.4.28 以降：設定により可能
  - nginx 1.1.19 以降：設定により可能
  - IIS：設定により可能
- クライアント（ブラウザ）
  - Chrome：4.0.211.0 以降でサポート
  - Firefox：Firefox 17 以降でサポート
  - Opera：Opera 12 以降でサポート
  - Safari：Mac OS X Mavericks 以降でサポート
  - Internet Explorer：Windows 10 IE 以降でサポート予定

➢ 改訂後

市販されているサーバ証明書の有効期間は、半年程度のもの、1 年程度のもの、2 年程度のもの等様々である※脚注。一般に、有効期間が長いほど、サーバ証明書の更新頻度が少なく更新作業の工数を削減できる。しかし、その反面、単純なミスによる更新忘れ、組織改編・担当者異動時の引き継ぎ不備による更新漏れ、鍵危殆化（秘密鍵の漏えい）リスクの増大、サーバ証明書に記載されたサーバの運営組織情報が（組織名変更などにより）正確でなくなるリスクの増大、アルゴリズム Agility（セキュリティ強度の変化に対して、安全な側に移行するための対策に要する時間、迅速さの程度）の低下などが危惧されるようになる。特に、2 年~~や 3 年~~など比較的長い間有効なサーバ証明書を利用する場合には、管理者がサーバ証明書の有効期限切れに気づかず、更新漏れによるサービス障害の発生が大きなリスクとなりえる。

これらを総合的に勘案し、特段の制約が存在しない限り、サーバ管理者は、1 年程度の有効期間を持つサーバ証明書を選択し、サーバ証明書の更新作業を、年次の定型業務と位置付けることが望ましい。

※脚注

CA/ブラウザフォーラムによる「Baseline Requirement」でサーバ証明書の有効期限についての要件が規定されている。2011 年 11 月以降に発行するサーバ証明書の有効期限は 60 ヶ月以内とされていたが、その後、2015 年 4 月以降の発行では 39 ヶ月以内、2018 年 3 月以降の発行では 825 日（約 27 ヶ月）以内と、徐々に有効期限が短くなってきている。

➢ 改訂後

以上のように、HTTPS で安全にサービスを提供したい場合などでは、ユーザに意識させることなくミスを防止でき、ユーザの利便性を向上させることができるので、HSTS の機能を持っているならば有効にすることを推奨する。

なお、HSTS は、主要なサーバ、クライアント（ブラウザ）ともに、2018 年 3 月時点の最新バージョンではすべてサポートされている。

M) 7.2.4 OCSP Stapling の設定有効化

P52　OCSP Stapling の記述

目的：OCSP Stapling の実装状況の変化に伴う記述更新

- 改訂前

  なお、OCSP Stapling は 2014 年 9 月時点で以下の環境においてサポートされている。参考までに、いくつかの設定例を Appendix B.5 で紹介する。

  - サーバ
    - Apache HTTP Server 2.3.3 以降
    - nginx 1.3.7 以降
    - Microsoft IIS on Windows Server 2008 以降

    など
  - クライアント（ブラウザ）
    - Mozilla Firefox 26 以降
    - Microsoft Internet Explorer （Windows Vista 以降）
    - Google Chrome

N) 7.2.5 Public Key Pinning の設定有効化

P.53 Public Key Pinning の記述

目的：Public Key Pinning の実装状況の変化に伴う記述更新

- 改訂前

  2014 年 9 月時点で、Public Key Pinning をサポートしている環境は以下の通りである。

  - サーバ
    - HTTP ヘッダを追加可能な任意のサーバ
  - クライアント
    - Google Chrome 13 以降
    - Mozilla Firefox 32 以降（デスクトップ版）、34 以降（Android 版）
    - Internet Explorer： マイクロソフト脆弱性緩和ツール（EMET[11]） を導入することで設定可能（EMET バージョン 4.0 以降よりサポート）

  期待されるハッシュ値の提供方法には 2 通りある。

  1)　ブラウザのソースコードに主要なサイトの SPKI フィールドの情報のハッシュ値リストを保持し、これと比較して SSL サーバ証明書が正当であるかを調べるもの。2014 年 9 月時点では Google Chrome や Mozilla Firefox がサポートしている。

  2)　サイトから送られる HTTP ヘッダに含まれる、SSL サーバ証明書の SPKI フィールドの情報のハッシュ値を元に正当性を比較するもの。IETF において、Public Key Pinning Extension for HTTP として発行された。参考までに、いくつかの設定例を Appendix B.6 で紹介する。

O) 8.1　本ガイドラインが対象とするプラットフォーム

P.55　8.1.1　対象とするプラットフォーム

目的：サポート状況の変化に伴う記述更新

- 改訂前
  - デスクトップ向け OS
    - ✓ Windows Vista Service Pack 2 （2017 年 4 月 11 日サポート終了）
    - ✓ Windows 7 Service Pack 1 （2020 年 4 月 11 日サポート終了）
    - ✓ Windows 8 （2016 年 1 月 12 日サポート終了）
    - ✓ Windows 8.1 （2023 年 1 月 10 日サポート終了）
    - ✓ Mac OS X 10.9
  - スマートフォン向け OS
    - ✓ 当該端末で利用できる最新の Android（もっとも古いもので Android4.x）
    - ✓ iOS 8

[11] http://technet.microsoft.com/ja-jp/security/jj653751

➢ 改訂後

なお、OCSP Stapling は、主要なサーバ、クライアント（ブラウザ）ともに、2018 年 3 月時点の最新バージョンではすべてサポートされている。

➢ 改訂後

ただし、現状では、多くのブラウザがサポートを取りやめているか取りやめる計画をしており、主要ブラウザでは Mozilla Firefox がサポートしているだけである。

➢ 改訂後

- デスクトップ向け OS
  - ✓ Windows 7 Service Pack 1 （2020 年 4 月 11 日サポート終了）
  - ✓ Windows 8.1 （2023 年 1 月 10 日サポート終了）
  - ✓ Windows 10 Home/Pro/Pro for Workstation バージョン 1709（提供日 2017 年 10 月 17 日、2019 年 4 月 9 日サポート終了）
  - ✓ Windows 10 Home/Pro/Pro for Workstation バージョン 1703（提供日 2017 年 4 月 5 日、2018 年 10 月 9 日サポート終了）
  - ✓ Windows 10 Enterprise/Education バージョン 1709（提供日 2017 年 10 月 17 日、2019 年 10 月 9 日サポート終了）
  - ✓ Windows 10 Enterprise/Education バージョン 1703（提供日 2017 年 4 月 5 日、2019 年 4 月 9 日サポート終了）
  - ✓ Windows 10 Enterprise/Education バージョン 1607（提供日 2016 年 8 月 2 日、2018 年 10 月 10 日サポート終了）
  - ✓ Windows 10 Enterprise 2015 LTSB（提供日 2015 年 7 月 29 日、2025 年 10 月 14 日サポート終了）
  - ✓ Windows 10 Enterprise 2016 LTSB（提供日 2016 年 8 月 2 日、2026 年 10 月 13 日サポート終了）
  - ✓ OS X El Capitan (10.11)（2017 年 12 月 6 日アップデート）
  - ✓ macOS Sierra (10.12)（2017 年 12 月 6 日アップデート）
  - ✓ macOS High Sierra (10.13)（2017 年 12 月 6 日アップデート）
- スマートフォン向け OS
  - ✓ 当該端末で利用できる最新の Android（2018 年 3 月時点で最新バージョンは Android 8.x）
  - ✓ 当該端末で利用できる最新の iOS（2018 年 3 月時点で最新バージョンは iOS 11.x）

P) 8.1　本ガイドラインが対象とするブラウザ

P.55　8.1.2　対象とするブラウザのバージョン

目的：サポート状況の変化に伴う記述更新

- 改訂前
  - Microsoft Internet Explorer

    2016 年 1 月 12 日以降は、サポートされるオペレーティングシステムで利用できる最新バージョンの Internet Explorer のみがテクニカルサポートとセキュリティ更新プログラムを提供されるようになる（表 1）。詳細は、以下を参照のこと。

    Microsoft Internet Explorer サポート ライフサイクル ポリシーに関する FAQ

    http://support2.microsoft.com/gp/microsoft-internet-explorer

  - Microsoft Internet Explorer 以外のブラウザ
    - ✓ Apple Safari 最新版
    - ✓ Google Chrome 最新版
    - ✓ Mozilla Firefox 最新版
    - ✓ Mobile Safari（iOS）：iOS 8 に搭載する Mobile Safari

表 1　Internet Explorer のサポート期間

ブラウザバージョン	OSバージョン	サポート期間（ライフサイクルポリシー@2014年11月10日時点）
		2015 / 2016 / 2017 / 2018 / 2019 / 2020 / 2021 / 2022 / 2023
Internet Explorer 7	Windows Vista SP2	2016/1/12
Internet Explorer 8	Windows Vista SP2	2016/1/12
	Windows 7 SP1	2016/1/12
Internet Explorer 9	Windows Vista SP2	2017/4/11
	Windows 7 SP1	2016/1/12
Internet Explorer 10	Windows 7 SP1	2016/1/12
	Windows 8	2016/1/12
Internet Explorer 11	Windows 7 SP1	2020/1/14
	Windows 8.1	2023/1/10

Q) 8.2　設定に関する確認項目

P56　8.2.2　設定項目　設定項目を標準機能で提供していないブラウザ

目的：サポート状況の変化に伴う記述更新

- 改訂前

  以下のブラウザは、設定変更オプションが提供されておらず、そもそも設定変更ができない。

  - PC 版 Web ブラウザ
    - Apple Safari
    - Google Chrome
  - スマートフォンに含まれる Web ブラウザ
    - Android 標準ブラウザ
    - Mobile Safari (iOS)

➢ 改訂後

- Microsoft Internet Explorer 11
- Microsoft Edge
- Apple Safari 最新版
- Google Chrome 最新版
- Mozilla Firefox 最新版
- Mobile Safari（iOS）

➢ 改訂後

以下のブラウザは、設定変更オプションが提供されておらず、そもそも設定変更ができない。

- PC 版 Web ブラウザ
  - Apple Safari
  - Google Chrome
- スマートフォンに含まれる Web ブラウザ
  - Google Chrome
  - Mobile Safari (iOS)

R) 8.2　設定に関する確認項目

P.56　8.2.2　設定項目　設定項目を標準機能で提供しているブラウザ

目的：サポート状況の変化に伴う記述更新

- 改訂前
  - Microsoft Internet Explorer

他のブラウザとは異なり、Internet Explorer では、

“ツール”→“インターネットオプション”→“詳細設定”

を選択すると多数の設定項目が表示され、ユーザが細かく設定できるようになってはいる。

しかし、安全性を考慮してデフォルト設定が行われていることから、特段の理由がない場合には“プロトコルバージョンの設定を除いて”設定を変更することは推奨しない。

なお、Internet Explorer のセキュリティ機能及びデフォルト設定については、以下に一覧としてまとめられている。

バージョン別 IE のセキュリティ機能

http://msdn.microsoft.com/ja-jp/ie/cc844005.aspx

【プロトコルバージョンの設定】

“ツール”→“インターネットオプション”→“詳細設定”を選択した後、設定項目を“セキュリティ”までスクロールさせると、「SSL2.0 を使用する」「SSL3.0 を使用する」「TLS1.0 を使用する」「TLS1.1 を使用」「TLS1.2 を使用」といったチェックボックスが表示される。ここでのチェックボックスにチェックが入っているプロトコルバージョンが、ブラウザが使うことができるプロトコルバージョンとなる。

本ガイドライン公開時点（2015 年 5 月）のデフォルト設定では、IE6 では「SSL2.0 を使用する」にチェックが入っている一方、IE8 以降では TLS1.1 や TLS1.2 をサポートしているものの「TLS1.1 を使用」「TLS1.2 を使用」にはチェックが入っていない。

このように、Internet Explorer は使うバージョンによって利用できるプロトコルバージョンが異なるので、プロトコルバージョンについてのみ、適切な設定になっているかを確認し、必要に応じて設定変更することを推奨する。

	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
IE6（参考）	×	×	▲	○	○
IE7	×	×	○	○	▲
IE8	▲	▲	○	○	▲
IE9	▲	▲	○	○	▲
IE10	▲	▲	○	○	▲
IE11	▲	▲	○	○	▲

○：デフォルト設定 ON　▲：デフォルト設定 OFF　×：サポートしていない

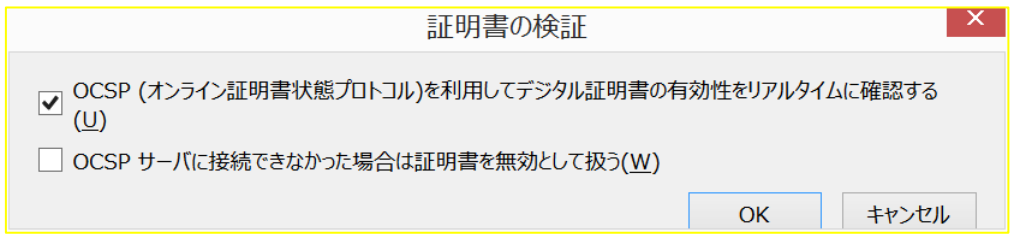
- Firefox

Firefox では、サーバ証明書の検証、失効機能においてどのように処理するかの動作についてのみ設定方法を提供している。この設定については、

“メニュー”→“オプション”→“詳細”→“証明書”→“検証(V)…”

を選択することで設定方法へのダイアログが表示される。

デフォルトの設定は以下のようになっており、特段の理由がない場合に変更することは推奨しない。



➢ 改訂後

- Microsoft Internet Explorer／Microsoft Edge

  他のブラウザとは異なり、Internet Explorer と Microsoft Edge では、

  “ツール”→“インターネットオプション”→“詳細設定”

  を選択すると多数の設定項目が表示され、ユーザが細かく設定できるようになってはいる。

  しかし、安全性を考慮してデフォルト設定が行われていることから、特段の理由がない場合には~~“プロトコルバージョンの設定を除いて”~~設定を変更することは推奨しない。

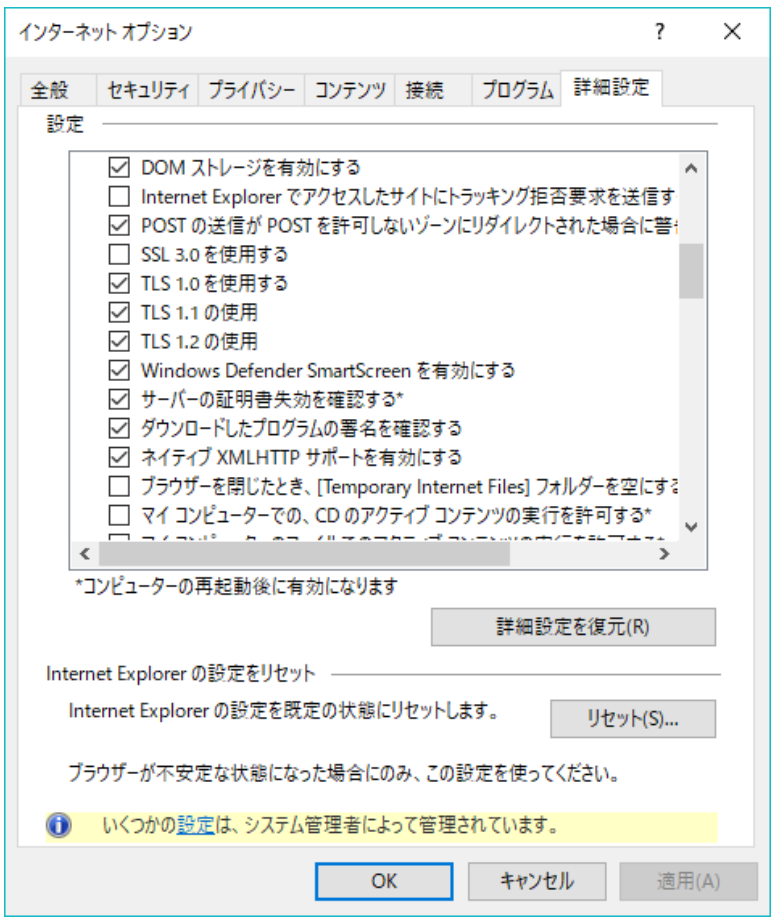
  ~~なお、Internet Explorer のセキュリティ機能及びデフォルト設定については、以下に一覧としてまとめられている。~~

  ~~バージョン別 IE のセキュリティ機能~~

  ~~http://msdn.microsoft.com/ja-jp/ie/cc844005.aspx~~

  【プロトコルバージョンの設定】

  “ツール”→“インターネットオプション”→“詳細設定”を選択した後、設定項目を“セキュリティ”までスクロールさせると、~~「SSL2.0 を使用する」~~「SSL3.0 を使用する」「TLS1.0 を使用する」「TLS1.1 を使用」「TLS1.2 を使用」などといったチェックボックスが表示される。ここでのチェックボックスにチェックが入っているプロトコルバージョンが、ブラウザが使うことができるプロトコルバージョンとなる。以下は、Windows10 Internet Explorer 11 の設定画面である。



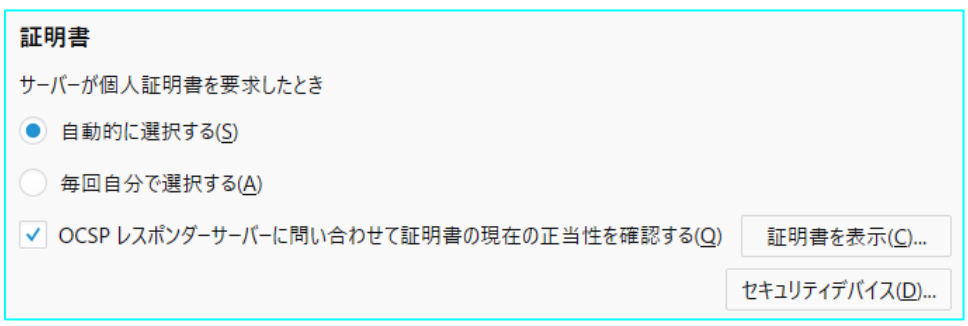
- Firefox

  Firefox では、サーバ証明書の検証、失効機能においてどのように処理するかの動作についてのみ設定方法を提供している。この設定については、

  “メニュー”→“オプション”→“プライバシーとセキュリティ”→“証明書”

  で選択することで設定のチェックボックスが表示される。

  デフォルトの設定は以下のようになっており、特段の理由がない場合に変更することは推奨しない。



S) 8.3.1　鍵長 1024 ビット、SHA-1 を利用するサーバ証明書の警告表示

P.58　8.3.1　鍵長 1024 ビット、SHA-1 を利用するサーバ証明書の警告表示

目的：警告から無効化が進んだことによる記述修正

- 改訂前

8.3.1　鍵長 1024 ビット、SHA-1 を利用するサーバ証明書の警告表示

CA/Browser Forum にて、サーバ証明書の有効期限が 2014 年 1 月 1 日以降の場合、RSA の鍵長を最小 2048 ビットにすると決められている。このため、ブラウザベンダ各社では、RSA の鍵長が 2048 ビット未満のものは順次無効にする対処がされている。また、SHA-1 についても、順次無効化する対処が予定されている。

詳しくは以下のとおりである。

- Microsoft Internet Explorer

2017 年 1 月 1 日より SHA-1 で署名されたサーバ証明書を受け付けない [12]。詳細は別途追記予定

- Google Chrome

Chrome 39 より順次、SHA-1 で署名されたサーバ証明書については、アドレスバーの鍵アイコンが別表記になる [13,14]。以下のようにサーバ証明書の有効期限によって表記は変化する。

バージョン	サーバ証明書の有効期限	アドレスバーの鍵アイコンの表記
39	2017 年 1 月 1 日以降	黄色い三角アイコン
40	2016 年 6 月 1 日～12 月 31 日	黄色い三角アイコン
	2017 年 1 月 1 日以降	HTTP と同様の表示
42	2016 年 1 月 1 日～12 月 31 日	黄色い三角アイコン
	2017 年 1 月 1 日以降	赤い×アイコン

- Firefox

2014 年以降、SSL/TLS で利用される RSA の鍵長が 2048 ビットに満たないルート証明書は順次無効になり、2015 年の中頃までにはすべてで無効になる [15]。

また SHA-1 で署名されたサーバ証明書についても、2015 年以降にリリースされる最新版の Firefox では、以下のように変更をする予定である [16]。

バージョン	サーバ証明書の有効期限	アドレスバーの鍵アイコンの表記
2015 年以降のバージョン	2017 年 1 月 1 日以降	警告表示をする UI を追加
2016 年以降のバージョン	2017 年 1 月 1 日以降	“接続の安全性を確認できません”と表示
2017 年以降のバージョン	すべて	“接続の安全性を確認できません”と表示

[12] http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx
[13] http://blog.chromium.org/2014/09/gradually-sunsetting-sha-1.html
[14] https://groups.google.com/a/chromium.org/forum/#!topic/security-dev/QNVVo4_dyQE
[15] https://wiki.mozilla.org/CA:MD5and1024
[16] https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signaturealgorithms/

➢ 改訂後

8.3.1 ~~鍵長 1024 ビット、~~SHA-1 を利用するサーバ証明書の警告表示

CA/Browser Forum では、2016 年 1 月 1 日以降、商用認証局は SHA-1 で署名されたサーバ証明書を発行しないことが決められている。このため、ブラウザベンダ各社では、SHA-1 で署名されたサーバ証明書を無効化する対処をしている。

詳しくは以下のとおりである。

- Microsoft Internet Explorer／Microsoft Edge

  2017 年 5 月 9 日に公開した更新版で、Internet Explorer 11、Edge では、SHA-1 で署名されたサーバ証明書の無効化をしている [17]。

- Google Chrome

  Chrome56 から SHA-1 で署名されたサーバ証明書の無効化をしている [18]。

- Firefox

  Firefox36 から SHA-1 で署名されたサーバ証明書の無効化をしている [19]。

[17] https://technet.microsoft.com/ja-jp/library/security/4010323
[18] https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html
[19] https://www.fxsitecompat.com/en-CA/docs/2016/sha-1-certificates-issued-by-public-ca-will-no-longer-be-accepted/

T) 8.3.2　SSL3.0 の取り扱い

P.60　8.3.2　SSL3.0 の取り扱い

目的：SSL3.0 の無効化が進んだことによる記述削除

- 改訂前

8.3.2　SSL3.0 の取り扱い

POODLE 攻撃の公表を受け、各ブラウザベンダは順次 SSL3.0 を利用不可とする対処を取り始めている。

- Internet Explorer

  セキュリティ情報 MS15-032「Internet Explorer 用の累積的なセキュリティ更新プログラム （3038314）」により、Internet Explorer 11 では SSL3.0 がデフォルトで無効になっている。

  それ以外のバージョンの Internet Explorer では、設定を変更することにより、SSL3.0 を無効化することができる。詳しくは、下記 URL のマイクロソフトセキュリティアドバイザリを参照のこと。

  マイクロソフト セキュリティ アドバイザリ 3009008

  https://technet.microsoft.com/ja-jp/library/security/3009008.aspx

- Google Chrome

  Chrome 40 からデフォルトで SSL3.0 が無効化されている。

- Firefox

  Firefox 34 および Firefox ESR 31.3.0 からデフォルトで SSL3.0 が無効化されている。

V) EC 曲線系のパテントリスクの記述

目的：EC 曲線系のパテントリスクの記述を見直すべきか

- CRYPTREC としては「パテント」に関していかなる判断も下さないため

- 改訂前（該当記述）：

（P.23）この他、非技術的要因として、ECDSA を採用する際にはパテントリスクの存在 が広く指摘されているので、十分な検討のうえで採用の可否を決めることが望ましい。

（P.39）また、非技術的要因として、ECDH や ECDSA を採用する際にはパテントリスクの存在が広く指摘されているので、十分な検討のうえで採用の可否を決めることが望ましい。

（P.40）パテントリスクについても検討したうえで ECDH や ECDSA を採用することを決めた場合には、表 11 の暗号スイートグループを追加してよい。

（P.42）パテントリスクについても検討したうえで ECDH や ECDSA を採用することを決めた場合には、表 13 の暗号スイートグループを追加してよい。

➢ 改訂後

（全削除）し、コラムに移す

➢ 改訂後

該当する文章を削除

合わせて、Appendix A のチェックリストからも「パテントリスクを考慮したうえで楕円曲線暗号を利用すると決めたか」の部分を削除

例＞

☐ ④-ii) 楕円曲線暗号を利用する場合は左の☐と以下の項目をチェック

~~④-ii-1) パテントリスクを考慮したうえで楕円曲線暗号を利用すると決めたか~~	~~6.1 節~~	~~☐~~
④-ii-1) 表 1 記載の暗号スイート（網掛けを含む）の全部または一部を設定したか	6.1 節／6.5.1 節	☐
④-ii-2) 表 1 記載のグループαの暗号スイート（網掛けを含む）から少なくとも一つは設定したか	6.1 節／6.5.1 節	☐
④-ii-3) 表 1 記載の暗号スイートのグループ順番（グループαの暗号スイートの次にグループβの暗号スイートが並ぶ）を守っているか	6.1 節／6.5.1 節	☐
④-ii-4) 表 1 記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1 節／6.5.1 節	☐
④-ii-5) ECDHE による鍵交換の鍵長を 256 ビット以上に設定したか	6.1 節／6.5.1 節	☐

資料６

CRYPTREC 暗号リストの改定について

CRYPTREC 暗号リストの改定に関する以下の各項目について御審議いただきたい。なお、事務局の提案する CRYPTREC 暗号リスト改定案を別添３に、現行の CRYPTREC 暗号リストを別添４にそれぞれ示す。

1. 64 ビットブロック暗号の注釈の変更

近年、64 ビットブロック暗号を鍵を変えずに使い続ける場合の脅威が指摘されている。そのため、64 ビットブロック暗号を安全に利用できるよう注釈を変更し、同じ鍵で暗号化を行う場合やメッセージ認証コードを生成する場合の最大ブロック数を示す。(別添１参照)

2. 3-key Triple DES の注釈の削除及び「電子政府推奨暗号」から「運用監視暗号リスト」への降格

3-key Triple DES は、注釈にて「NIST SP 800-67 で規定され、デファクトスタンダードであること」を条件として電子政府推奨暗号として当面の利用が認められているが、今後 TLS での 3-key Triple DES の利用が推奨されなくなる動向など、この注釈が現実とそぐわなくなってきている。そのため、本注釈を削除するとともに、「電子政府推奨暗号リスト」から「運用監視暗号リスト」へ変更する。(別添１参照)

3. MISTY1 のフルラウンド攻撃への対応

64 ビットブロック暗号 MISTY1 のフルラウンド攻撃への対応について、上記１で 64 ビットブロック暗号に対する注釈の追加により、現在知られている同攻撃を回避する指針となるため、MISTY1 個別に注釈を追加することとはしない。(別添１参照)

4. 認証暗号 ChaCha20-Poly1305 の「推奨候補暗号リスト」への追加

認証暗号 ChaCha20-Poly1305 は、TLS1.3 で実装必須の ciphersuite となるなど、今後の利用拡大が予想されることから、外部評価を実施し、安全性評価及び実装性能調査を行ってきた。この評価結果に基づき、暗号技術評価委員会で ChaCha20-Poly1305 が認証暗号として十分な安全性および実装性能を有していると判断されたことから、「推奨候補暗号リスト」へ追加する。(別添２参照)

5. 技術分類「認証暗号」の新設及び注釈の追加

認証暗号 ChaCha20-Poly1305 の追加にあたり、CRYPTREC 暗号リストの技術分類として「認証暗号」カテゴリを新設する。なお、「ブロック暗号」と「暗号利用モード」の「認証付き秘匿モード」を組み合わせても「認証暗号」を実現できることから、「認証暗号」及び「認証付き秘匿モード」にその旨を記した注釈を付与する。(別添 2 参照)

資料６別添１

3-key Triple DES および 64 ビットブロック暗号の今後の利用について

1. 背景

ACM CCS 2016 にて、64 ビットブロック暗号を、鍵を変えずに 2^{32} ブロック以上暗号化した場合の脅威（いわゆる Sweet32）について発表[1][2]があったことを受け、IETF 等の標準化機関や主要なブラウザで、64 ビットブロック暗号の優先順位を下げたり、同じ鍵で暗号化できるデータ量を制限するなどの対策が取られている。

また、NIST が 2017 年 11 月に TDEA に関する文書 SP 800-67 を Revision 2 に更新し[3]、TDEA で同一の鍵を用いて暗号化できる最大ブロック数を 2^{32} ブロックから 2^{20} ブロックに下げたほか、今後、TLS や IPsec で TDEA の利用を許容しない(disallow)方針を打ち出した。

これらの動向を受け、CRYPTREC 暗号リストにおける 64 ビットブロック暗号及び 3-key Triple DES の方針について暗号技術評価委員会で議論した結果を報告するとともに、以下の各論点についてそれぞれ御審議いただきたい。

2. 64 ビットブロック暗号について【審議事項】

現在、CRYPTREC 暗号リストの 64 ビットブロック暗号に付与されている注釈について、暗号技術評価委員会で検討を行った結果、以下の変更案が提案された。

【現在の注釈】

「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。」

【変更後の注釈】

「CRYPTREC 暗号リストとして使う場合は、64 ビットブロック暗号で同一の鍵を用いて暗号化する場合、最大 2^{20} ブロックまで、同一の鍵を用いて CMAC でメッセージ認証コードを生成する場合、最大 2^{21} ブロックまでとする。」

変更後の注釈における、64 ビットブロック暗号で同一の鍵を用いて暗号化する場合の最大ブロック数「2^{20}」は、Sweet32[2]において HTTPS で secure cookie を導出する攻撃において最初の collision を見つけるのに必要なブロック数から導出されており、NIST SP 800-67 Revision 2[3]で規定されている数字である。

また、64 ビットブロック暗号で同一の鍵を用いて CMAC でメッセージ認証コー

ドを生成する場合の最大ブロック数「2^{21}」は、同一の MAC が生成される（collision が起きる）確率が 100 万分の 1 以下となるよう導出された数字であり、NIST SP 800-38B[4]で推奨されている。暗号技術検討会事務局としても国際的な標準との整合性を取るためにこれらの値を採用するのがよいと考えられるため、上記変更案について御審議いただきたい。

3. 3-key Triple DES について【審議事項】

現在、電子政府推奨暗号リストにおいて、3-key Triple DES には下記のように注釈（注３）が付与されている。

> （注３） 3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。
> １） NIST SP 800-67 として規定されていること。
> ２） デファクトスタンダードとしての位置を保っていること。

NIST が 2017 年 11 月に公開した Draft NIST SP 800-52 Revision 2[5]において ”The Triple Data Encryption Algorithm (TDEA), also known as 3DES is no longer approved for use with TLS”とし、また、Triple DES の sunset date に関するスケジュールを検討しており、当該注釈（注３）は現実とそぐわなくなっている。

このような状況を踏まえ、CRYPTREC 暗号リストにおける 3-key Triple DES の扱いについて、暗号技術評価委員会から以下のような意見があった。

- 3-key Triple DES の利用状況を踏まえて運用監視暗号リストへの移行に伴う問題点を確認し、問題がなければ、運用監視暗号リストに移す。
- 運用監視暗号リストに移す際に、現在 3-key Triple DES についている注釈（注３）は削除する。なお、運用監視暗号リストにおいても、64 ビットブロック暗号の安全な使い方に関する注釈はつける。
- 推奨候補暗号リストに掲載されている 3 つの 64 ビットブロック暗号については、引き続き検討を行い、結論を得るまでは現状維持とする。

暗号技術検討会事務局としては、上記の意見を踏まえて CRYPTREC 暗号リストを改定すべきと考えるが、これらについて御審議いただきたい。

4. MISTY1 について【審議事項】

2015 年に 64 ビットブロック暗号 MISTY1 のフルラウンド攻撃が発表されて以来、対応を検討してきた。現在知られているフルラウンド攻撃には 2^{64} ブロック分の平文・暗号文ペアが必要となっている。今回、64 ビットブロック暗号に対して付与しようとしている新たな注釈は、MISTY1 についてもこの攻撃を回避する安全な使い方の指針となるため、暗号技術評価委員会では、MISTY1 個別の注釈を追加することは不要という意見で一致した。

暗号技術検討会事務局としても上記意見に沿って追加の注釈は不要と考えるが、この方針について御審議いただきたい。

【参考文献】

[1] Karthikeyan Bhargavan, Gaëtan Leurent, “On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN”, ACM CCS 2016.

[2] Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN, https://sweet32.info/

[3] NIST Special Publication (SP) 800-67, Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Nov 21, 2017.

[4] NIST Special Publication (SP) 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, May, 2005.

[5] (DRAFT) NIST Special Publication 800-52 Revision 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Nov, 2017.

資料６別添２

ChaCha20-Poly1305 の CRYPTREC 暗号リスト追加について

1. 背景

ChaCha20-Poly1305 については、昨年度の暗号技術検討会（2017 年 3 月 30 日）にて、CRYPTREC 暗号リストへの追加を視野に入れ、安全性評価・実装性能評価を実施することが承認されている。

第 1 回暗号技術評価委員会（2017 年 7 月 21 日）の承認を受け、暗号技術評価委員会にて、安全性評価および実装性能について外部評価を実施した。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。

[本年度実施した外部評価]

1. ChaCha20-Poly1305 および Poly1305 の安全性調査および評価
   内容：ChaCha20-Poly1305 の認証暗号としての安全性および Poly1305 のメッセージ認証コード(MAC) としての安全性に関する調査及び評価
   依頼先：岩田 哲 様 (名古屋大学)

2. ChaCha20-Poly1305 の実装性能調査
   内容：ChaCha20-Poly1305 の実装性能に関する文献調査及び公開されているベンチマーク実装評価の調査
   依頼先：菅野 哲 様 (レピダム株式会社)

2. 安全性及び実装性能に関する判断について

外部評価の結果を踏まえ、暗号技術評価委員会では、認証暗号 ChaCha20-Poly1305 について、CRYPTREC 暗号リストへの追加条件となる安全性及び実装性能について審議を行い、十分な安全性及び実装性能を有していると判断した。

2.1. 安全性評価

ChaCha20-Poly1305 の構成を図 1 に示す。暗号化のためにストリーム暗号 ChaCha20 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。

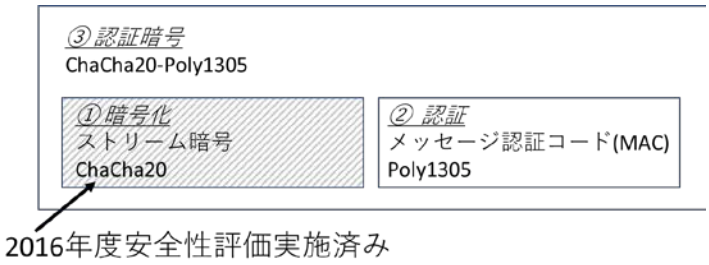


図 1 ChaCha20-Poly1305

安全性については、以下の条件を満たす場合、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]。

① 暗号化機能の安全性：ChaCha20 を擬似乱数生成器とみなすことができる。

② 認証機能の安全性：Poly1305 が安全なユニバーサルハッシュ関数である。

① 暗号化機能の安全性

2016 年度の評価結果より、既知の様々な攻撃について鍵の総当たりよりも効率的な攻撃が見つからなかったことから、擬似乱数生成器とみなすことができるとの見解を得ている。(詳細は、CRYPTREC 技術報告書 No.2601「Security Analysis of ChaCha20-Poly1305 AEAD」参照)

② 認証機能の安全性

評価レポートでは、以下の安全性評価について報告されている。

・証明可能安全性：Poly1305 は、ユニバーサルハッシュ関数とみなすことができる

また、そのほかの安全性解析についても以下の通り報告されている。

攻撃の種類	解析結果
関連鍵攻撃	現実的な脅威とはならない
再偽造可能性	理想的な MAC と同等の安全性を有する
弱鍵	存在したとしても全体の直接的な安全性への影響はない
複数ユーザ安全性	ユーザ数の安全性に対する影響は小さい
ナンス再利用	ハッシュ鍵の導出を容易にする ゆえに、仕様書に沿い、ナンスの再利用は行ってはならない

以上の評価結果から、②の条件を満足し、Poly1305 は十分な安全性を満たすと考えられる。

③ 認証暗号としての安全性

評価レポートでは、以下の安全性評価について報告されている。

・証明可能安全性：①および②の安全性要件を満たし、ChaCha20-Poly1305 は、認証暗号と

しての安全性を有する

また、そのほか 2017 年度の外部評価レポートでは、以下の安全性解析についても報告されている。

攻撃の種類	解析結果
関連鍵攻撃	ChaCha20 が①を満たす条件の下で安全性証明が可能である
弱鍵	存在しても現実的な脅威とはならない
複数ユーザ安全性	ユーザ数の安全性に対する影響は小さい
復号ミスユース	暗号化に関する安全性は満たさないが、認証に関する安全性は満たす
ナンス再利用	再利用されたナンスを伴う出力については偽造可能となる ゆえに、仕様書に沿い、ナンスの再利用は行ってはならない
再偽造可能性	ナンスを再利用しない限り理想的な認証暗号と同等の安全性をもつが、ナンスを再利用した場合、偽造可能となる ゆえに、仕様書に沿い、ナンスの再利用は行ってはならない

以上の評価結果に基づき、暗号技術評価委員会では、安全性について、CRYPTREC 暗号リストに掲載するために十分な安全性を満たしていると判断した。

2.2. 実装性能評価

本年度、実装性能に関する調査・評価を実施した。

認証暗号として、AES-GCM は広く知られている一方、AES 計算のための拡張命令(ハードウェアによる AES アクセラレーション)が利用できない組み込みデバイスなどの CPU などで、計算コストが小さく、処理速度の速い認証暗号として ChaCha20-Poly1305 が注目されている。ChaCha20-Poly1305 は、AES-GCM と比べ、ソフトウェア実装に向いていると言われており、TLS 1.3 では実装することが必須のアルゴリズムとなっている。

評価レポートの結果から、ChaCha20-Poly1305 は、特に、組み込み機器や低電力アプリケーション向けの CPU で優位性があることが確認できた。一例として、世界中で広く利用されている OpenSSL を用いた実測による Linux 上での性能比較結果（暗号化処理速度） を図 2 に示す。AES-GCM と比較評価し、AES 計算のための拡張命令(ハードウェアによる AES アクセラレーション)を用いない環境で、ChaCha20-Poly1305 (鍵長 256 ビット)は約 2.86～4.46 倍の処理速度をもち、優位性があることがわかる。このように AES 計算のための拡張命令(ハードウェアによる AES アクセラレーション)を利用できない環境で、ChaCha20-Poly1305 は AES-GCM と比較し、実装性能が優れている。

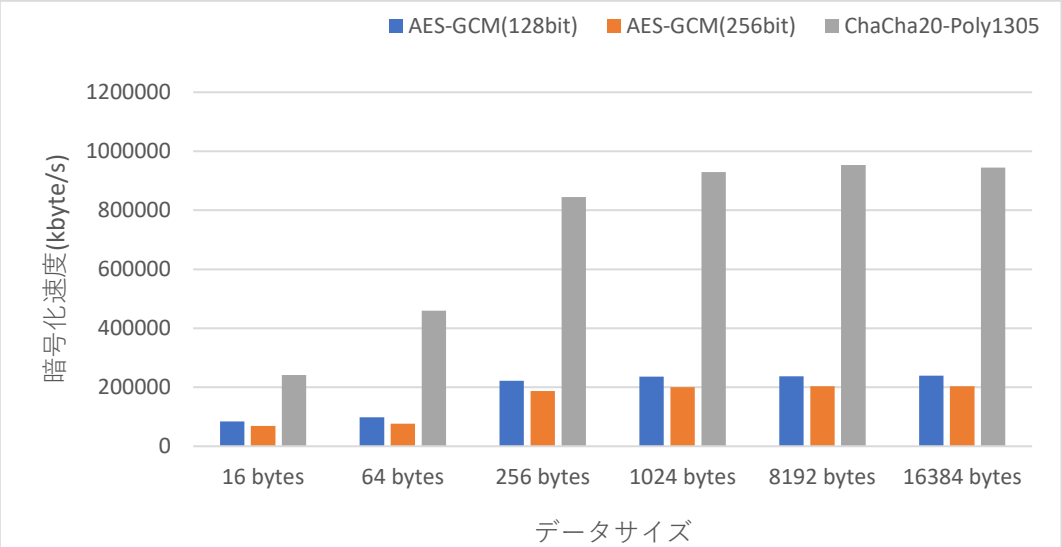


図2 Linuxにおける認証付き暗号の性能比較

(データは評価レポート表 5.15 より抜粋)

なお、ChaCha20-Poly1305 についてハードウェア実装評価は実施していないが、TLS 1.3 で実装必須のアルゴリズムとなっている点、また、組込みデバイスなどでの利用が期待されている点など、主たる利用がソフトウェアでの実装となることも考慮し、十分な実装性能を有すると考えられる。

以上の調査および評価結果に基づき、暗号技術評価委員会では、実装性能について、CRYPTREC 暗号リストに掲載するために十分な実装性能を有していると判断した。

3. CRYPTREC 暗号リストへの追加について【審議事項】

暗号技術検討会事務局としては、第 2 章に示した暗号技術評価委員会からの報告に基づいて、認証暗号 ChaCha20-Poly1305 を CRYPTREC 暗号リストの「推奨候補暗号リスト」に新たに掲載することを提案するが、この方針についてご審議いただきたい。

また、現在の CRYPTREC 暗号リストの技術分類には、「認証暗号」は存在しない。ChaCha20-Poly1305 を追加する場合の技術分類「認証暗号」の追加方法及び注釈について、暗号技術評価委員会での議論等を踏まえた事務局案を下記に示す。これらについても併せて御審議いただきたい。

	事務局案
追加する技術分類	大分類
追加する技術分類の名称	認証暗号
追加する技術分類の位置	「メッセージ認証コード」と「エンティティ認証」の間
注釈を追記する箇所	「認証暗号」および「認証付き秘匿モード」
追記する注釈	「CRYPTREC 暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせても、「認証暗号」として使うことができる。」

【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).

資料６別添３

電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）案

平成２５年３月１日
総　務　省
経済産業省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64 ビットブロック暗号(注2)	~~3-key Triple DES(注3)~~ 該当なし
	128 ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード(注＊)	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号(注＊)		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報セキュリティ担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

（注1）　「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25年 3 月 1 日現在）

（注2）　~~より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。~~CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、最大2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、最大2^{21}ブロックまでとする。

~~（注3）　3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。~~
~~1）NIST SP 800-67 として規定されていること。~~
~~2）デファクトスタンダードとしての位置を保っていること。~~

（注4）　初期化ベクトル長は 96 ビットを推奨する。

（注＊）　CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64 ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128 ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード(注＊)	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号(注＊)		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

（注5） KEM（Key Encapsulating Mechanism）－ DEM（Data Encapsulating Mechanism）構成における利用を前提とする。

（注6） ~~より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。~~ CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、最大2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、最大2^{21}ブロックまでとする。

（注7） 平文サイズは 64 ビットの倍数に限る。

（注12） ハッシュ長は 256 ビット以上とすること。

（注＊） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせても、「認証暗号」として使うことができる。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号(注＊＊)	~~該当なし~~ 3-key Triple DES
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード(注＊)	該当なし
メッセージ認証コード		CBC-MAC(注11)
認証暗号(注＊)		該当なし
エンティティ認証		該当なし

（注8） 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注9） SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

（注＊＊）CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、最大2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、最大2^{21}ブロックまでとする。

（注10） 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。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

（注＊） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年 3月27日	(注 10)	128-bit RC4 は、SSL (TLS1.0 以上)に限定して利用すること。	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。
平成28年 3月29日	推奨候補暗号リスト（技術分類：ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)
	(注 12)	[新規追加]	ハッシュ長は 256 ビット以上とすること。
平成29年 3月30日	推奨候補暗号リスト（技術分類：ハッシュ関数）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128(注12) SHAKE256(注12)
平成30年 3月29日	電子政府推奨暗号リスト（技術分類：共通鍵暗号）	64ビットブロック暗号に3-key Triple DESを記載	3-key Triple DESの「運用監視暗号リスト」への降格に伴い、(注3)を削除
	電子政府推奨暗号リスト（技術分類：認証暗号）	[新規追加]	技術分類として「認証暗号」を新設

	電子政府推奨暗号リスト（注＊）	［新規追加］	認証付き秘匿モード及び認証暗号に、ブロック暗号を認証付き秘匿モードと組み合わせて認証暗号として使用できる旨の(注＊)を追加
	推奨候補暗号リスト（注６）	128ビットブロック暗号の選択が望ましい	64ビットブロック暗号で暗号化可能な最大ブロック数を規定
	推奨候補暗号リスト（技術分類：認証暗号）	［新規追加］	認証暗号という技術分類を新設し、ChaCha20-Poly1305を追加
	推奨候補暗号リスト（注＊）	［新規追加］	暗号利用モードの認証付き秘匿モード及び認証暗号に、ブロック暗号を認証付き秘匿モードと組み合わせて認証暗号として使用できる旨の(注＊)を追加
	運用監視暗号リスト（技術分類：共通鍵暗号）	64ビットブロック暗号は「該当なし」	64ビットブロック暗号に3-key Triple DESを追加 また、64ビットブロック暗号で暗号化可能な最大ブロック数を示す（注＊＊）を追加

	運用監視暗号リスト（技術分類：認証暗号）	［新規追加］	技術分類として「認証暗号」を新設
	運用監視暗号リスト（注＊）	［新規追加］	暗号利用モードの認証付き秘匿モード及び認証暗号に、ブロック暗号を認証付き秘匿モードと組み合わせて認証暗号として使用できる旨の（注＊）を追加

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

平成25年3月1日
総務省
経済産業省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	3-key Triple DES(注3)
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報通信担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

（注1） 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注2） より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

（注3） 3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。
1） NIST SP 800-67 として規定されていること。
2） デファクトスタンダードとしての位置を保っていること。

（注4） 初期化ベクトル長は 96 ビットを推奨する。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64 ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128 ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
エンティティ認証		ISO/IEC 9798-4

（注5） KEM（Key Encapsulating Mechanism）－ DEM（Data Encapsulating Mechanism）構成における利用を前提とする。

（注6） より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

（注7） 平文サイズは 64 ビットの倍数に限る。

（注12） ハッシュ長は 256 ビット以上とすること。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号	該当なし
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		CBC-MAC(注11)
エンティティ認証		該当なし

（注8） 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注9） SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

（注10） 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。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年 3月27日	(注10)	128-bit RC4は、SSL(TLS1.0以上)に限定して利用すること。	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。
平成28年 3月29日	推奨候補暗号リスト（技術分類：ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)
	(注12)	[新規追加]	ハッシュ長は256ビット以上とすること。
平成29年 3月30日	推奨候補暗号リスト（技術分類：ハッシュ関数）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128(注12) SHAKE256(注12)

資料７

暗号技術検討会
２０１７年度　報告書（案）

２０１８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高度な融合により、多様なニーズにきめ細やかに対応したモノやサービスを提供できる社会への産業構造の変化が進みつつある。一方で、IoT の普及に伴うサイバー攻撃の起点の増加や、サイバー攻撃自体の巧妙化・複雑化が続く中で、サイバー攻撃の影響が実空間にまで到達するリスクも増していくと考えられる。このような産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応したセキュリティ確保が求められる中、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、IoT から得られる大量のデータの流通・連携を支える上でも、その重要性は一層増すと考えられる。

このような社会の変化に伴い、CRYPTREC においても、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等の貢献が求められている。

本年度の CRYPTREC は、昨年度までの「重点課題検討タスクフォース」での議論を踏まえた検討体制の下で、暗号技術検討会では、これまでの成果物である 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整理を実施した。

また、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、DSA 及び DH の安全性に関する注意喚起レポートの発行、SHA-1 の衝突を受けた「暗号技術ガイドライン(SHA-1)」の改定、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暗号技術調査 WG において、欧米での調査・検討や標準化に向けた議論が始まっている耐量子計算計算機暗号の研究動向調査を行った。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候補を昨年度取りまとめたが、その中から必要性・重要性の高い鍵管理に関する運用ガイドラインの作成に向けた調査を行った。加えて、2015 年に発行した「SSL/TLS 暗号設定ガイドライン」について、近年の状況変化を踏まえた改定に向けた検討等を行った。これらの 2017 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 2017」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。

2018 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。

2017 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、ハッシュ関数 SHA-1 を継続利用する際の指針となるガイドラインの改定や、耐量子計算機暗号（Post-Quantum Cryptography）の技術動向調査を実施し、暗号技術活用委員会では、SSL/TLS 暗号設定ガイドラインの改定や、鍵管理のガイドライン作成に向けた検討を行った

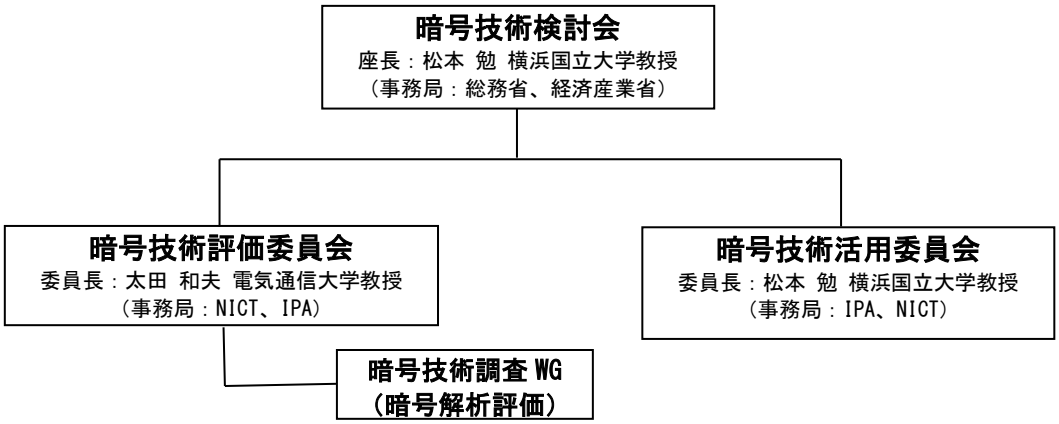


図 2.2.1　2017 年度 CRYPTREC 体制図

２．３．暗号技術検討会の開催実績

2017 年度の暗号技術検討会は、暗号技術評価委員会、暗号技術活用検討会の活動計画についてメールによる審議を実施した上で、暗号技術評価委員会、暗号技術活用委員会の活動報告、CRYPTREC 暗号リストの改定を審議するために１回開催した。

【第 1 回】2018 年 3 月 29 日（木）15:00～17:00
（主な議題）
- 文章番号体系について
- 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
- CRYPTREC 暗号リストの改定について
- 2017 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．暗号技術評価委員会

３．１．１．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
・暗号技術の電子政府推奨暗号リストからの降格
・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 2017 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。

３．１．２．2017 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

2017 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 3-key Triple DES の電子政府推奨暗号リストからの降格、③ 64 ビットブロック暗号の注釈に関する検討を実施した。

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。2016 年度に報告済であるが、位数が 768 ビット長の素数である有限体における離散対数の計算に関する学会発表、及び、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)の仕様に対する衝突発見に関する学会発表があった。前者に関しては、後述の注意喚起を行い、後者に関しては、暗号技術ガイドライン(SHA-1)の改定を検討した。それ以外において、攻撃研究等に関して緊急に対処が必要なものは存在しなかったが、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、現在、電子政府推奨暗号リストに記載されている 3-key Triple DES に関して、近年の状況に鑑みて、電子政府推奨暗号リストから運用監視暗号リストへ降格されることが適切であると判断した。

③ について、共通鍵暗号の 64 ビットブロック暗号に関して、近年の解析動向を考慮し、適切な注釈案の策定を行った。

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

有限体上の離散対数問題は、電子政府推奨暗号リストに掲載されている DSA 及び DH や、インターネットで使われている通信プロトコル TLS における鍵共有方式など、多くの暗号技術の安全性の根拠として利用されているが、昨年、位数が 768 ビット長の素数である有限体における離散対数の計算結果が示された。RSA1024 に係る移行指針と同様に、DSA や DH を利用する場合には、鍵長において、2048 ビット以上の素数位数の有限体を用いることを推奨する。

新世代暗号に係る調査

本項目に係る活動に関しては、昨年度に引き続き、ChaCha20-Poly1305 の安全性及び実装性能の評価を行った。ChaCha20-Poly1305 は、認証暗号として十分な安全性及び実装性能を有していると判断した。また、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）を設置し、主に、耐量子計算機暗号（Post-Quantum Cryptography）の技術動向調査を実施した。

３．１．３．暗号技術評価委員会の開催状況

2017 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 3.1.1 のとおりである。

表 3.1.1　暗号技術評価委員会の開催状況

回	開催日	議題
第 1 回	2017 年 7 月 21 日	・委員会今年度活動計画の検討 ・WG 活動計画の検討 ・外部評価(ChaCha20-Poly1305)についての検討 ・暗号技術ガイドライン(SHA-1)の改定の検討 ・64 ビットブロック暗号の今後の利用の検討 ・768 ビット素数の有限体上の離散対数問題の状況と DSA, DH の今後の利用についての注意喚起の検討 ・監視状況報告
第 2 回	2018 年 2 月 28 日	・WG 今年度活動報告 ・3-key Triple DES 及び 64 ビットブロック暗号の今後の利用についての検討 ・暗号技術ガイドライン(SHA-1)改定案の検討 ・外部評価(ChaCha20-Poly1305 の安全性及び実装性能)の検討 ・監視状況報告 ・CRYPTREC Report 2017(暗号技術評価委員会報告)の目

		次案提示

2017 年度、暗号技術調査 WG（暗号解析評価）は計 2 回開催した。

３．２．暗号技術活用委員会

３．２．１．活動の概要

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

３．２．２．2017 年度の活動内容

2016 年度に取りまとめられた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）の候補のなかから、必要性、目的、課題、関連組織等の状況を踏まえ、具体的に運用ガイドラインの対象を選定し、ガイドライン作成に向けた活動を行った。

具体的には、「鍵管理に関する運用ガイドライン作成に向けた活動」と「SSL/TLS 暗号設定ガイドラインのアップデートに向けた活動」からなる。

鍵管理に関する運用ガイドライン作成に向けた活動

2016 年度に取りまとめた運用ガイドラインの候補の中で鍵管理に関するものが多数を占めており、また実際に暗号を利用するうえでも鍵の正しい運用は不可欠である点から、鍵管理に関する運用ガイドラインの重要性は他と比較しても高いものと考えられる。

一方で、鍵管理に関するガイドラインは、その重要性からも、国内外を含め、いくつか発行されている。しかしながら、いずれのガイドラインも広く認知され、利用されているとは言い難い点を踏まえれば、従来の鍵管理ガイドラインには「ガイドラインとして利用しにくい」問題点が隠れているように思われる。例えば、

- 鍵管理として扱うべき範囲、考慮すべき範囲が広い
- 記述内容が抽象的になりがちである
- 技術的な観点だけでなく、法制度や運用ルール的な観点との整合性が求められる

といった意見が委員からも指摘された。

そこで、2017 年度の活用委員会では、いきなり鍵管理に関するガイドラインを作成するのではなく、鍵管理に関する規格を網羅的に調査し、どのような体系・順番で鍵管理に関するガイドラインを作成していくのがよいのかを取りまとめた。

具体的には、鍵管理に関する運用ガイドライン作成に向けた事前調査として鍵管理に関する規格 21 文献を網羅的に調査した。この調査結果から、SP800-57 Part1 と SP800-130 は非常に強い関連性を持ち、また鍵管理全体のフレームワークとしてもっとも基本的な文献であ

ると考えられることが確認できた。

今後、鍵管理に関する運用ガイドラインについては、SP800-57 の内容と SP800-130 の内容をより精査した上で、実際のガイドライン作成に臨むこととする。

なお、調査報告の詳細については、暗号技術活用委員会報告を参照されたい。

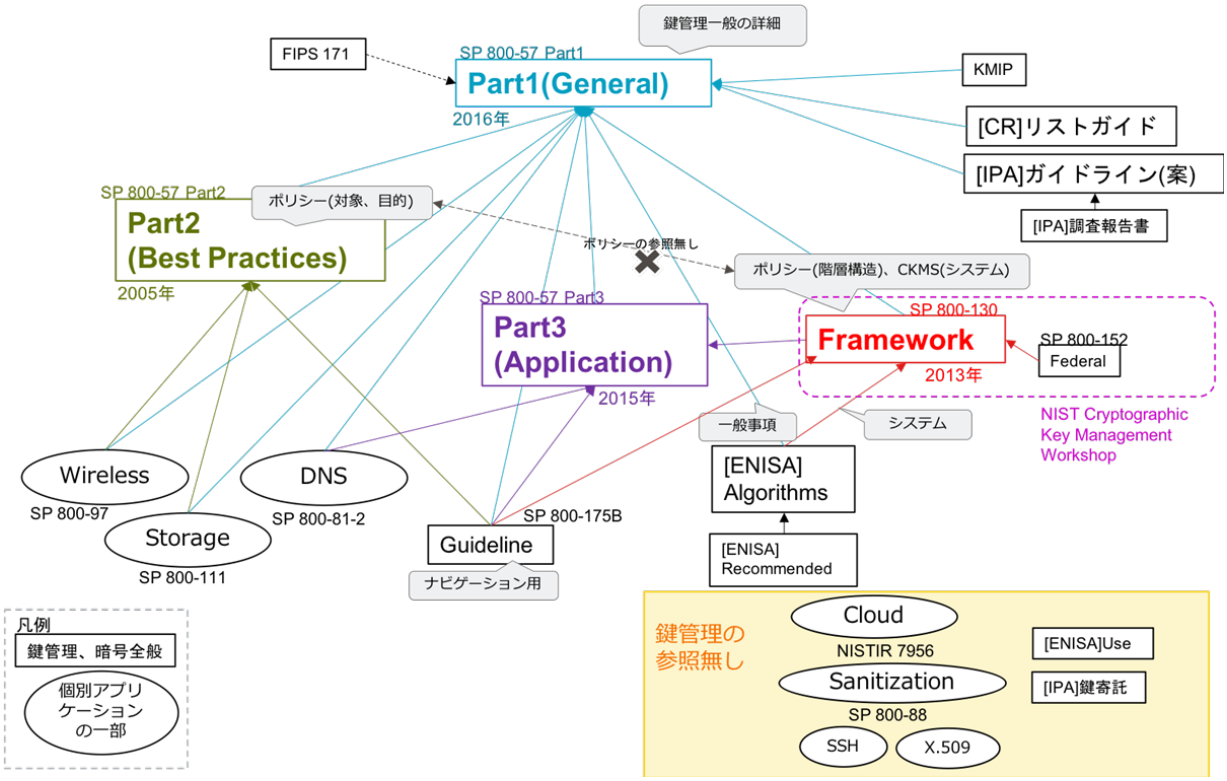


図 3.2.1　各文献における鍵管理に関する他文献への参照関係

SSL/TLS 暗号設定ガイドラインのアップデートに向けた活動

「SSL/TLS 暗号設定ガイドライン」については、2015 年発行時から状況が変化していること、10 万件を越えるダウンロード数があるなどニーズが多いことにから、2017 年度に、外部動向の追加ならびにそれに対応するためのマネジメント方針の追記・修正などを行い、SSL/TLS 暗号設定ガイドラインのアップデート案を作成した。

具体的には、2015 年以降の動向調査を実施し、その結果を踏まえて 22 箇所の SSL/TLS 暗号設定ガイドラインの記述を修正・追記・削除すべきかを検討した。合わせて、コラム記事を更新すべきかの議論を行った。

特に、前回 SSL/TLS 暗号設定ガイドラインを公開した 2015 年当時は、レガシーシステムや携帯電話などで SSL3.0 や SHA-1 証明書の利用を必要とするケースが無視できないことから、「セキュリティ例外型」を設け「早期移行を前提として暫定的な利用継続」を認めていたが、この 3 年間で SSL3.0 や SHA-1 証明書の利用からの脱却が大きく進んだことから「推奨セキュリティ型への早期移行を求めるものであり、すでに最低限の安全性水準を満たしているとは言えない状況になっている。」との記述変更を行う、などのアップデート案を策定した。

このアップデート案を反映したガイドラインを 2018 年 5 月に公開する予定である。

３．２．３．暗号技術活用委員会の開催状況

2017 年度 2 回開催された活用委員会での審議概要は表 3.2.1 のとおりである。さらには、活用委員会とは別に、SSL/TLS に関する動向及び鍵管理に関する公募調査の中間報告会を委員向けに実施した。

表 3.2.1　暗号技術活用委員会の開催状況

回	開催日	議題
第 1 回	2017 年 9 月 7 日	・SSL/TLS 暗号設定ガイドラインのアップデート作業について ・鍵管理に関する運用ガイドラインの事前検討について
報告会	2017 年 12 月 27 日	・SSL/TLS に関する動向及び鍵管理に関する公募調査の中間報告
第 2 回	2018 年 3 月 15 日	・SSL/TLS 暗号設定ガイドラインのアップデート案について ・鍵管理に関する運用ガイドライン作成に向けた今後の計画について

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、鍵管理の安全な運用に向けた取組など、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、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鍵管理に関する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。

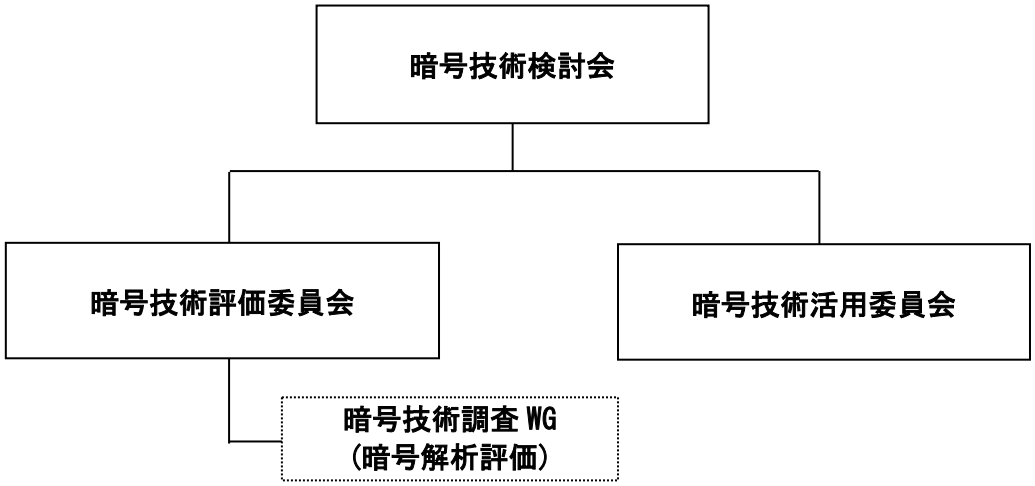


図 4.1　2018 年度 CRYPTREC の体制図（予定）