暗号技術活用委員会活動報告

2017年12月18日

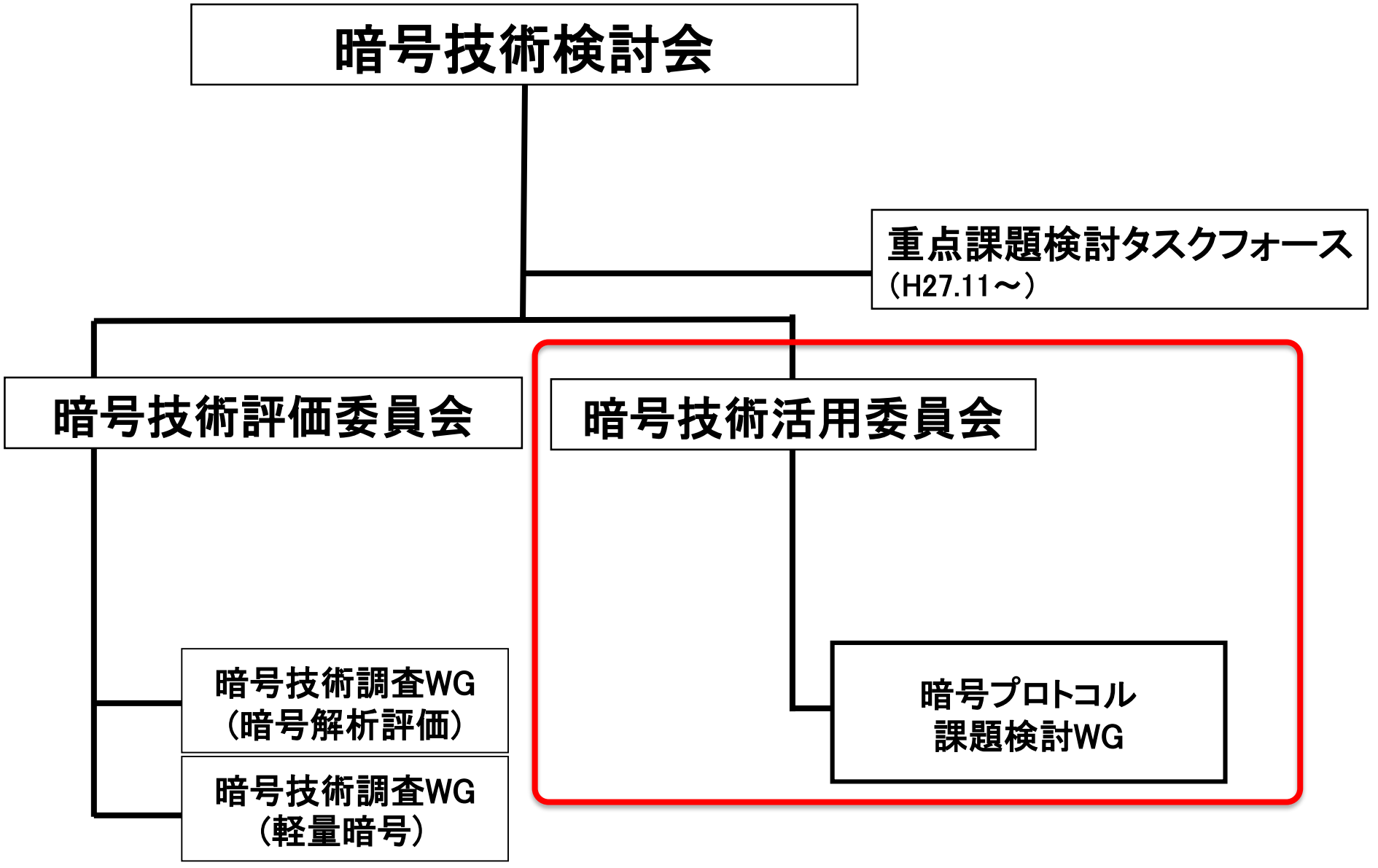
暗号技術活用委員会委員長
松本 勉
(横浜国立大学)

目次

1. 暗号技術活用委員会の概要
2. 2016年度暗号技術活用委員会活動概要
3. 2017年度暗号技術活用委員会活動概要（途中経過）

1. 暗号技術活用委員会の概要

2016年度CRYPTREC体制



2016年度暗号技術活用委員会委員

CRYPTREC
Cryptography Research and Evaluation Committees

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　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部　車載セキュリティグループ 主席研究員
委員	満塩 尚史	内閣官房　IT総合戦略室　政府CIO補佐官
委員	村木 由梨香	日本マイクロソフト株式会社　セキュリティレスポンスチーム　セキュリティプログラムマネージャー
委員	山岸 篤弘	一般財団法人日本情報経済社会推進協会　電子署名・認証センター　主席研究員
委員	山口 利恵	国立大学法人東京大学　大学院情報理工学系研究科　ソーシャルICT研究センター　特任准教授
委員	渡邊 創	国立研究会開発法人産業技術総合研究所　情報・人間工学領域　研究戦略部　研究企画室　企画主幹

（注）2016年4月時点

暗号技術活用委員会活動目的＆計画

CRYPTREC
Cryptography Research and Evaluation Committees

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

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

2016年度活動計画

(1) 作成すべき運用ガイドラインの対象の検討

(2) 作成した運用ガイドラインのアップデート方法に関連する検討

(3) 外部組織や業界団体との連携方法（外部連携）の検討

(4) その他

- CRYPTRECとして暗号プロトコルをどのように扱うかを重点的に検討するため、**「暗号プロトコル課題検討WG」を設置**

暗号技術活用委員会と暗号プロトコル課題検討WGの関係

■作成すべき運用ガイドラインの対象及び取扱い範囲の切り分け

整備すべき運用ガイドラインの対象は何か

暗号設定ガイドライン
（利用方法、及び設定方法）

- 開発実装に関連する文書類
- 暗号利用・運用・設定に関連する文書類で暗号プロトコル以外に関するもの
- 特定の製品・サービスを安全にするために関連する文書類

暗号プロトコルに関する運用ガイドライン

- 暗号利用・運用・設定に関連する文書類で暗号プロトコルに関するもの

この部分の検討を暗号プロトコル課題検討WGが担当

マネジメント関連のガイドライン
（鍵管理、リスク管理等）

- 暗号システムの運用マネジメントに関連する文書類

2016年度暗号技術活用委員会審議状況

CRYPTREC
Cryptography Research and Evaluation Committees

■暗号技術活用委員会

回	開催日時	主な議題
第1回	2016. 11. 09	● 暗号プロトコル課題検討WG活動状況報告 ● 運用ガイドライン(「SSL/TLS暗号設定ガイドライン」)のアップデート方法に関する検討 ● 運用ガイドラインの対象範囲に関する検討
第2回	2017. 3.15	● 暗号プロトコル課題検討WG活動報告 ● 暗号プロトコル以外の運用ガイドラインの対象の検討 ● 外部連携の進め方の検討 ● 2016年度暗号技術活用委員会報告書

■暗号プロトコル課題検討WG

詳細は菊池主査から報告

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

2016年度暗号技術活用委員会活動概要

運用ガイドラインの対象

運用ガイドラインのアップデート方法

運用ガイドラインの対象の検討

暗号技術活用委員会が運用ガイドラインを作成する価値がある対象は何かを明らかにする

⇒ 2017年度以降、具体的な運用ガイドラインの作成に着手

■ 検討のポイント

【領域・対象】どのような用途で使う運用ガイドラインであるか

【目的】どのような目的をもった運用ガイドラインを意図したものか

【内容】運用ガイドラインに記載される内容はどのようなものか

【想定読者】その運用ガイドラインの想定読者は誰か

【必要性】なぜ運用ガイドラインが必要なのか、あるいは運用ガイドラインがないとどのように困るのか

【課題】 ガイドラインを作るうえで問題となりそうな課題／注意しなければならない課題は何か（運用ガイドラインの価値を高めるための考慮ポイント）

【他組織のガイドライン等】他組織が同種のガイドラインを作っていないか／作ろうとしていないか

【関連組織】 どのような他組織と連携していくのがよいか

具体的な検討項目の例

- 【領域・対象】どのような用途で使うか
  - 開発実装に関連するガイドライン
  - 暗号利用・運用・設定に関連するガイドラインで暗号プロトコル以外に関するもの
  - 暗号システムの運用マネジメントに関連するガイドライン
  - 特定の製品・サービスを安全にするために関連するガイドライン

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

取りまとめ結果の例

CRYPTREC
Cryptography Research and Evaluation Committees

領域	対象	目的	内容	想定読者	必要性	ガイドライン作成にあたっての課題	他組織ガイドライン	関連組織
A. 開発実装	鍵管理（生成・保管・削除）の実装	①②	・乱数性テストのチェック項目 ・安全な鍵生成方法 ・鍵の保管 ・鍵の削除	・システム開発者（特に、プログラマー）・運用者 ・今後システムを構築する中小企業 ・製品開発者	・他の対象に比べて、「鍵管理」を優先的に検討してほしい ・鍵の元となる技術であるため、重要（特に公開鍵暗号の鍵生成） 不適切な実装では、知らないうちに素因数を他の鍵と共有している事例もある ・日本の情報セキュリティ対策の底上げになる。暗号を応用（利用）したシステム全般の参考にもなる ・システム開発者や運用者が想定読者になりうるかは定かでないが、製品開発者向けには必要 ・SP800-90では、乱数に必要なエントロピー等について言及しているが、実際には最低限どのようにすればよいのかがわからない 特に、リアルタイム性を要する鍵についてどこまでやればよいかがわかるものがほしい	・書くべきことの範囲が広い ・抽象的な文書になることが予想されるので、範囲や対象読者を限定しないと作成が困難 ・鍵管理に関する規格を網羅的に調査する必要がある ※「鍵管理」の全体像を整理したのちに優先順位をつけて作成	SP800-90A, B, C	
	サーバ証明書の検証方法	①	アプリにおけるサーバ証明書が適切に検証されるための実装方法	システム開発者(特に、アプリケーション開発者)	・アプリでのサーバ証明書検証不備の脆弱性が多い ・IoT向けに、大量、高速、省リソースという様な観点で、サーバ証明書の検証方法だけでなく、PKIの構築全般について策定されれば、組込機器向けにも参考になる			

取りまとめ結果

CRYPTREC
Cryptography Research and Evaluation Committees

取りまとめ結果全容（全16対象）は「CRYPTREC Report 2016 暗号技術活用委員会報告」にて公開

領域	No	対象	目的
A. 開発実装	1	鍵管理（生成・保管・削除）の実装	①②
	2	サーバ証明書の検証方法	①
	3	電子署名・検証実装方法	①②③
	4	Captchaの検証方法	①②
	5	将来の暗号危殆化対策を見据えたシステム設計・開発方法 ※C. 暗号システムの運用マネジメントにも記載	②
B. 暗号利用・運用・設定（暗号プロトコル以外）	6	鍵管理（生成・保管・削除）の設定/運用	①②③
	7	SSL・SSHの鍵管理	①②
	8	ドキュメントへの署名	①③
	9	保管データ(Data at Rest)	④
	10	データの処分(Data Disposed)	④
	11	使用中のデータの暗号化(Data in Use)	②

領域	No	対象	目的
C. 暗号システムの運用マネジメント ※考え方・思想を含む	12	鍵管理（生成・保管・削除）の考え方	①③
	13	暗号システムデザイン	①② （③）
C. 暗号システムの運用マネジメント ※考え方・思想を含む	14	将来の暗号危殆化対策を見据えたシステム設計・開発方法 ※A. 実装開発にも記載	②
	15	RSAから楕円曲線暗号への移行	①③
D. 特定の製品・サービス	16	クラウドにおけるセキュリティメカニズムの比較調査	①②

運用ガイドラインの対象

運用ガイドラインのアップデート方法

（参考）「SSL/TLS暗号設定ガイドライン」

CRYPTREC
Cryptography Research and Evaluation Committees

■ SSL/TLSを安全に使うためのBest Practice集

- 2015年3月時点でのSSL/TLSの安全性と可用性（相互接続性）のバランスを踏まえた推奨暗号設定方法をガイダンス
- 3段階の推奨設定基準を用意
- OpenSSLやWindows等の「設定方法例」をAppendixに記載
- 設定確認するための「チェックリスト」も用意

■ 主な想定読者

- 具体的な構築・設定を行うサーバ構築者
- サービス提供に責任を持つサーバ管理者
- サーバ構築を発注するシステム担当者

2015年5月公開後、120，000件以上のダウンロード

運用ガイドラインのアップデート方法の必要性

CRYPTREC
Cryptography Research and Evaluation Committees

運用ガイドラインは、ガイドライン作成時の標準化状況や製品状況、利用環境や利用実績等を踏まえて、作成時における現実的かつ効果的な推奨設定や推奨基準を提示

ある程度の時間が経過し、標準化状況や製品状況、利用環境や利用実績等が変化すれば、運用ガイドラインの中身も陳腐化し、ガイドラインとしてふさわしくなくなる場合も

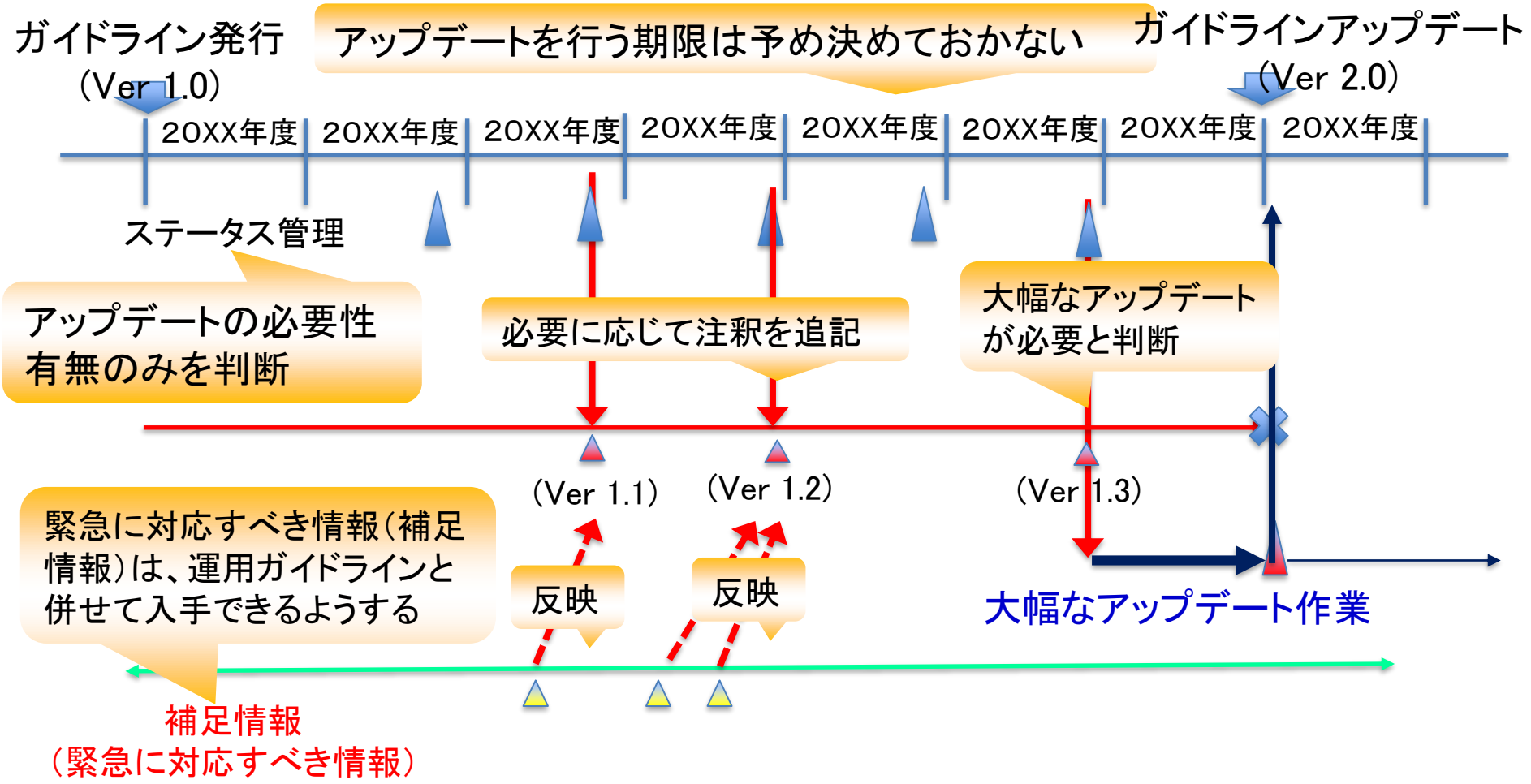
運用ガイドラインの質を維持するためにどのような方法でアップデートを行っていくかが課題

→ 「SSL/TLS暗号設定ガイドライン」を例にアップデートの在り方を検討

運用ガイドラインのアップデート方法の検討(1/2)

CRYPTREC Cryptography Research and Evaluation Committees

■一般的なアップデートの方向性についての検討
- 見直し期限の設定(定期的なアップデートの実施是非)
- アップデートの具体的な方法



運用ガイドラインのアップデート方法の検討(2/2)

CRYPTREC Cryptography Research and Evaluation Committees

■「SSL/TLS暗号設定ガイドライン」のアップデートの方向性について

- 最新動向の反映、及びセキュリティ例外型の見直しまで含める
  - IETFでは、RC4使用禁止、SSL3.0非推奨、TripleDES非推奨、等のRFCを発行
  - 認定認証事業者が発行する証明書ではSHA-1からSHA256への移行完了、パブリック証明書でも、ほぼSHA256 with RSA2048ビットに移行
  - フィーチャーフォンでもキャリアがSHA-1証明書での接続はできないと注意喚起しており、必ずしもセキュリティ例外型が必要とは言えない状況

  ⇒ 何らかの形でセキュリティ例外型の記述は見直す方向

- 市販製品及びOSS製品等の暗号設定状況はガイドラインから分離する
  - 各社の製品の設定例は徐々に各社で作るようになっていくべき

- セキュリティ例外型の利用を終了させる時期(EOL)は導入せず
  - EOL導入で、EOLまでは利用を容認すると誤解される恐れあり

2017年度暗号技術活用委員会活動概要

（途中経過）

2017年度CRYPTREC体制

2017年度暗号技術活用委員会委員

CRYPTREC
Cryptography Research and Evaluation Committees

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　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	国立研究会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　室長

（注）2017年4月時点

2017年度暗号技術活用委員会活動計画

CRYPTREC
Cryptography Research and Evaluation Committees

■ 活動計画

（1）鍵管理に関する運用ガイドライン作成に向けた活動

（2）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

2018年春に
アップデート予定

■ 委員会開催計画

回	開催日	主な議案
第1回	2017.9.7	● 活用委員会活動計画の確認 ● 鍵管理に関する公募調査に向けた意見募集 ● SSL/TLS暗号設定ガイドラインのアップデート対象の審議
Ad hoc	―	● 途中経過確認のための中間報告
第2回	2018.3上旬	● 鍵管理に関する報告書の審議 ● SSL/TLS暗号設定ガイドラインのアップデートの審議