暗号技術活用委員会活動報告

2016年6月27日

暗号技術活用委員会委員長

松本 勉

（横浜国立大学）

CRYPTREC
Cryptography Research and Evaluation Committees

2015年度CRYPTREC体制

暗号技術検討会

2015年度新設

CRYPTRECの在り方に関する検討グループ
（H27.6～H27.8）

重点課題検討タスクフォース
（H27.11～）

暗号技術評価委員会

（1）暗号技術の安全性及び実装に係る監視及び評価

（2）新世代暗号に係る調査

（3）暗号技術の安全な利用方法に関する調査

暗号技術活用委員会

（1）暗号の普及促進・セキュリティ産業の競争力強化に係る検討
（2）暗号技術の利用状況に係る調査及び必要な対策の検討等
（3）暗号政策の中長期的視点からの取組

CRYPTREC
Cryptography Research and Evaluation Committees

2015年度暗号技術活用委員会委員

委員長	松本 勉	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	清藤 武暢	日本銀行金融研究所
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	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	満塩 尚史	内閣官房　IT総合戦略室　政府CIO補佐官
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

CRYPTREC
Cryptography Research and Evaluation Committees

2015年度暗号技術活用委員会活動内容

■「SSL/TLS暗号設定ガイドライン」の公開

- 2014年度に運用ガイドラインWGで作成した成果物

■委員会開催概要

第1回／第2回重点課題検討タスクフォースの議論結果を踏まえて

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

CRYPTREC
Cryptography Research and Evaluation Committees

「SSL/TLS暗号設定ガイドライン」の公開

「SSL/TLS暗号設定ガイドライン」の公開

- **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

公開後、50，000件以上のダウンロード

CRYPTREC
Cryptography Research and Evaluation Committees

SSL/TLS暗号設定ガイドライン（考え方）

設定基準	概要	安全性
高セキュリティ型	**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**	標準的な水準を**大きく上回る高い安全性水準**を達成
推奨セキュリティ型	ほぼすべての**一般的な利用形態で使う**ことを想定	**標準的な安全性水準**を実現
セキュリティ例外型	**安全性よりも相互接続性に対する要求をやむなく優先**させるような場合	**短期的な利用を前提に許容可能な最低の安全性水準**を満たす

それぞれの設定基準に応じた要求設定を規定

- プロトコルバージョン
- サーバ証明書
- 暗号スイート

プロトコルバージョンの要求設定

	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
高セキュリティ型	◎	×	×	×	×
推奨セキュリティ型	◎	○	○	×	×
	ー	◎	○	×	×
	ー	ー	◎	×	×
セキュリティ例外型	◎	○	○	○	×
	ー	◎	○	○	×
	ー	ー	◎	○	×
対象外	ー	ー	ー	○	×

○：設定有効（◎：優先するのが望ましい）　×：設定無効化　ー：実装なし

CRYPTREC
Cryptography Research and Evaluation Committees

委員会の開催概要

CRYPTREC暗号技術活用委員会の今後の活動に向けて

（2015年度第2回重点課題検討タスクフォース資料）

第1回TFで議論された活動方向性（論点の再整理）①

暗号技術活用委員会で取り扱う可能性があるテーマの質・対象が
従来とは大きく異なってくることが想定されることから、
暗号技術活用委員会の運営スタイルの考え方自体を再整理

「中立性・客観性」の意味合いを広げた従来とは異なる運営スタイル
での**「セキュリティ向上に役立つドキュメント類」の作成**まで
活動対象範囲を拡大する

CRYPTREC暗号リストの改定（利用実績調査）	暗号設定ガイドライン（具体的設定例なし）*（OSS設定例あり）*（市販製品設定例あり）	マネジメント関連のガイドライン（鍵管理、リスク管理等コンセプトガイドライン）	政策的課題・社会ニーズ的課題の議論（合理的な仮説提示）

- Best Practiceのドキュメント類の作成に当たっては（利害関係者でもある）**ベンダの協力**を仰いでもよいのではないか
- 大枠としての**セキュリティ評価の基本線が揺らいでいるように体外的に見えない**（=ベンダの言いなりにならない）ようにコントロールすることが重要
- CRYPTRECとしてやるべき範囲と別組織がやるべき**範囲の切り分け**を検討
- 作成にあたった**運営スタイルの違いを考慮**し、**適切な文書体系に整理したうえで公開**すべき

CRYPTREC
Cryptography Research and Evaluation Committees

活動目的の見直し

【2013～2014年度の活動目的】

暗号技術活用委員会では、2012年度暗号運用委員会の全部及び暗号実装委員会の一部からの課題を主に引き継ぎ、**暗号技術における国際競争力の向上及び運用面での安全性向上に関する検討**を実施する。主な検討課題は以下の通り。

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）
② 暗号技術の利用状況に係る調査及び必要な対策の検討等
③ 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）

【新しい活動目的】

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年度暗号技術活用委員会活動計画概要①

(1) 作成すべき運用ガイドラインの対象及び取扱い範囲の切り分けの検討

- どのような種類の運用ガイドラインをどのような優先順位で作成するか
- 外部組織等と役割分担する境界についての検討

(2) 作成した運用ガイドラインのメンテナンス体制の検討

- 作成済みの運用ガイドラインをどのような方針でメンテナンスやアップデートをしていくか

(3) 外部組織や業界団体との連携方法の検討

- 外部組織や業界団体等に幅広く協力を求め、連携方法を検討

(4) 運用ガイドラインの作成

- 対象とするテーマ及び具体的な作業方法については暗号技術活用委員会が指定

CRYPTREC
Cryptography Research and Evaluation Committees

2016年度暗号技術活用委員会活動計画概要②

(5) ベンダや業界団体等の意向をバランスよく取り入れつつ、セキュリティも担保する利用価値の高い成果物となるようにコントロールする

- WGを設置する場合には、対応するテーマに応じて、ベンダや業界団体等からの人選について特に留意
- ベンダや業界団体等の意向をバランスよく取り入れつつセキュリティも担保できるように暗号技術活用委員会として確認

(6) その他

- 2016年度は、CRYPTRECとして暗号プロトコルをどのように扱うかを重点的に検討するため、**「暗号プロトコル課題検討WG」を設置**
- 必要に応じて、検討テーマを新たに設けることがある

CRYPTREC
Cryptography Research and Evaluation Committees

暗号プロトコル課題検討WGの活動計画概要

(1) CRYPTRECとして扱うべき暗号プロトコルの対象範囲の集中検討

- CRYPTRECが暗号プロトコルを取り上げる目的を整理
- 目的に沿った取り扱うべき対象範囲の明確化

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

- 安全性評価結果や脆弱性情報の取り扱いルールの明確化
- 安全性情報や脆弱性情報を提供してもらう組織、同種ガイドラインを作成している組織、主要な利用ユーザと想定される組織等との連携方法

(3) 暗号プロトコルに関する活動方針案の整理・検討

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

暗号技術活用委員会・活動報告（まとめ）

昨今の暗号技術を取り巻く環境の変化、サイバーセキュリティ基本法の施行といった社会情勢を踏まえ、CRYPTRECの活動を大きく見直した。今後、暗号技術活用委員会では暗号技術を主軸とした検討から情報システムのセキュリティ確保に寄与する暗号技術等に係る成果物の提供へと活動目的の軸足を移すことになった。

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

CRYPTREC
Cryptography Research and Evaluation Committees