CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会活動報告

暗号技術検討会 座長
（横浜国立大学 教授）
松本 勉

目次

参考

暗号技術検討会　構成員

CRYPTREC暗号リスト

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECとは

Cryptography Research and Evaluation Committees

CRYPTRECの概要

○ 総務省・経済産業省・NICT・IPAが共同で開催する暗号技術評価プロジェクト

○ 当プロジェクトは、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討すること等を通じて、セキュアなIT社会の実現を目指すもの

○ 暗号技術検討会並びに暗号技術検討会の下に設置される暗号技術評価委員会及び暗号技術活用委員会により運営

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC活動体制（2016年度-2017年度）

暗号技術検討会

（1）CRYPTREC暗号のセキュリティ及び信頼性確保のための調査・検討
（2）CRYPTREC暗号リストの改定に関する調査・検討
（3）関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討・提言

重点課題検討タスクフォース
（～2017年2月）

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

暗号技術調査WG（軽量暗号）
（～2017年1月）

暗号技術調査WG（暗号解析評価）

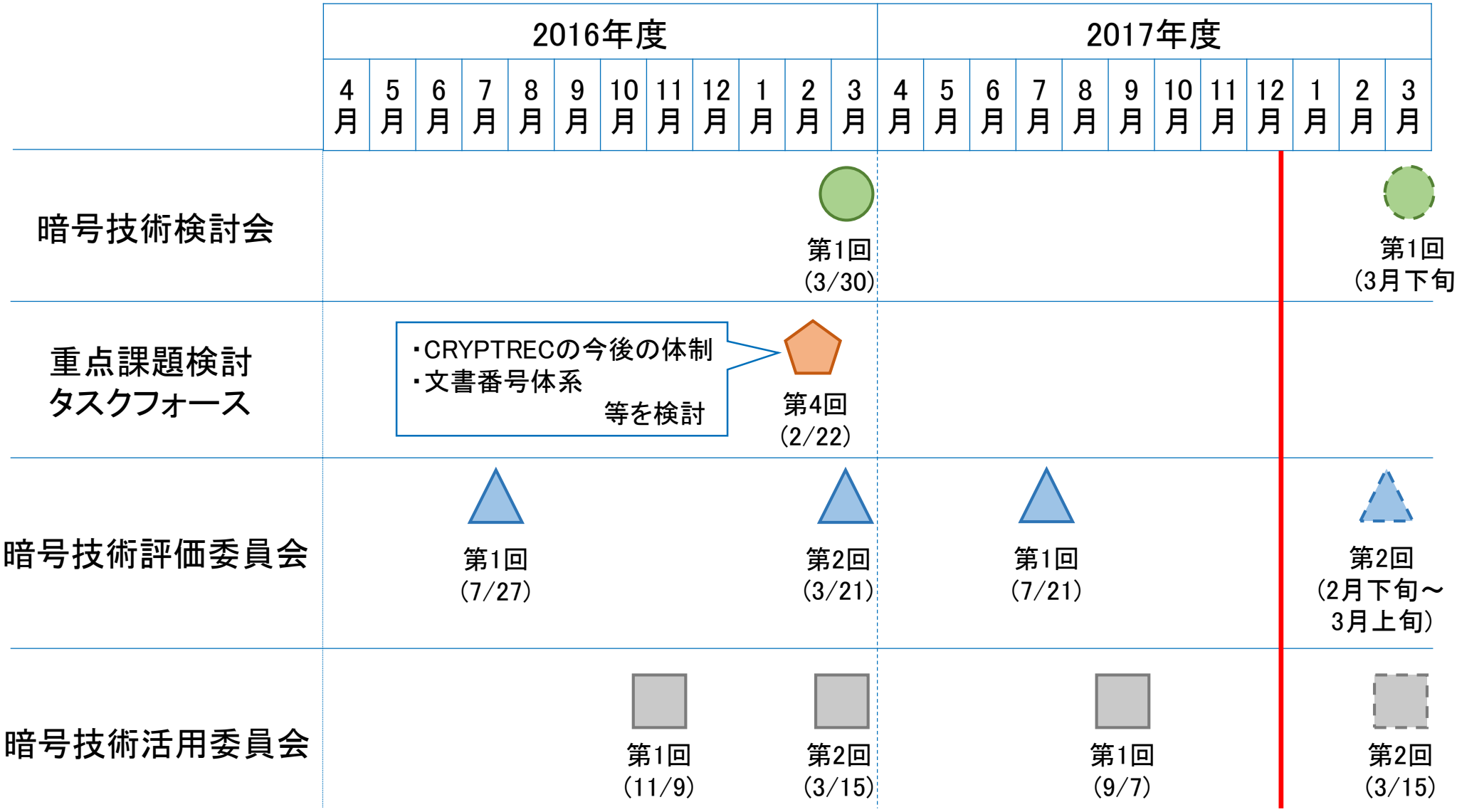
暗号技術活用委員会

（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
（3）暗号政策の中長期的視点からの取組の検討

暗号プロトコル課題検討WG
（～2017年2月）

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会等の開催概要



CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC活動の見直し

CRYPTRECの在り方に関する検討グループ

- 暗号技術に対する社会ニーズの変化をふまえ、CRYPTRECの活動領域、適用範囲、成果物について議論
- 2015年6月～8月、集中的に4回開催

重点課題検討タスクフォース

- 政府統一基準に向けたCRYPTREC成果物の在り方、暗号アルゴリズムの脆弱性に関する情報発信フロー等、重点課題について議論
- 2015年11月～2017年2月に4回開催

- 電子政府情報システムだけではなく、IoT社会で重要になる軽量暗号等についても取り組む
  ⇒「暗号技術ガイドライン（軽量暗号）」を策定・発行
- 暗号アルゴリズムや実装だけではなく、暗号の運用方法についても取り組む
  ⇒「鍵管理」について調査・検討

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECの今後の方針

〇政府統一基準に向けた新たなCRYPTREC成果物
〇新たな社会ニーズを見据えた新規活動

- 政府統一基準等から参照されやすい文書の作成やプライバシー保護のような社会ニーズを見据えた検討等の新たな取り組みについて、今後どのように議論を進めていくかをNISC（内閣サイバーセキュリティセンター）との相談を含め、事務局で整理を行い、その内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号活用委員会に議論の場を移して検討

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECの今後の方針

○情報システム全体のセキュリティ確保を
　意識した他団体との連携

- 他団体との連携を必要とする対象のタスクが明確になった段階で、タスクの内容に応じて、暗号技術検討会、暗号技術評価委員会もしくは暗号技術活用委員会に議論の場を移し、具体的な連携方法について検討

CRYPTREC
Cryptography Research and Evaluation Committees

文書番号体系

〇文書番号体系についてタスクフォースで議論し、検討会で承認

番号書式

CRYPTREC-<カテゴリ>-<連番>-<管理情報>

カテゴリ　：文書の種別毎の英字2字の表記（次ページ）
連番　　：年度内におけるカテゴリ毎の4桁の通し番号
管理情報　：アップデートされるものは発行年度もしくはバージョン番号、されないものは発行年度

例

- アップデートされるもの（前バージョンはアーカイブ）
  - 〇2016年度発行CRYPTREC暗号リスト（最新）　CRYPTREC-LS-0001-2016
  - 〇SSL/TLS暗号設定ガイドライン ver 1.1（最新）　CRYPTREC-GL-0101-1.1
- アップデートされないもの
  - 〇2016年度暗号技術検討会報告書　CRYPTREC-RP-0001-2016
  - 〇2016年度暗号技術評価委員会報告書　CRYPTREC-RP-0002-2016

CRYPTREC
Cryptography Research and Evaluation Committees

文書カテゴリ

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

※作成・アップデート主体を区別する必要がある場合、カテゴリ表記名に数字を付番

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会　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　数理情報学専攻　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	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、所属は2017年11月末時点のもの）

オブザーバ：内閣サイバーセキュリティセンター、警察庁、個人情報保護委員会、総務省、法務省、外務省、財務省、
文部科学省、厚生労働省、経済産業省、防衛省、NICT、AIST、IPA、JIPDEC、FISC

CRYPTREC
Cryptography Research and Evaluation Committees

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。

CRYPTREC
Cryptography Research and Evaluation Committees

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

[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。

（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。

CRYPTREC
Cryptography Research and Evaluation Committees

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

[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。

（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。

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