第１回重点課題検討タスクフォース

日時：平成 27 年 11 月 20 日(金) 18:00～20:00
場所：経済産業省 別館 3 階 301 共用会議室

議　事　次　第

１．開　会（資料確認等）

２．議　事
(1) 「重点課題検討タスクフォース」開催要綱について
(2) 重点課題検討タスクフォースの設置について
(3) ハッシュ関数 SHA-2,SHA-3 の取扱いについて
(4) CRYPTREC 活動方針についての論点
(5) その他

３．閉　会

（資料番号）	（資　料　名）
資料１	「重点課題検討タスクフォース」開催要綱（案）
資料２	重点課題検討タスクフォースの設置について
資料３	ハッシュ関数 SHA-2,SHA-3 の取扱いについて
資料４	CRYPTREC 活動方針についての論点 ～活用委員会の活動ポリシーの見直し～
参考資料１	「CRYPTREC の在り方に関する検討グループ」における議論結果報告について（2015 年度第１回暗号技術検討会 資料２）
参考資料２	重点課題検討タスクフォース　構成員・オブザーバ名簿

資料１

「重点課題検討タスクフォース」開催要綱(案)

１　名　称

本検討会は「重点課題検討タスクフォース」（以下「タスクフォース」という。）と称する。

２　開催の趣旨・目的

暗号技術を取り巻く環境やサイバーセキュリティ基本法（平成 26 年法律第 104 号）の施行といった社会情勢の変化に鑑み、今後の情報システム全体のセキュリティ基盤の為に必要となる CRYPTREC の活動の方向性の議論を行い、今後 CRYPTREC が取り扱うべき暗号に係る技術分野の選定や情報発信の在り方等を決定し、トップダウン的な意志決定も出来る体制の構築を目的として開催する。

３　検討事項

（１）CRYPTREC のミッション検討

・政府統一基準への新たな成果物
・暗号プロトコルレベルのセキュリティ確保に向けた活動
・新たな社会ニーズを見据えた新規活動
・他団体との連携
・情報発信フローの整備

（２）上記に基づいた CRYPTREC 次年度活動計画方針案検討

４　構成等

（１）タスクフォースの構成は、別紙のとおりとする。
（２）タスクフォースには、座長１名を置く。
（３）座長は、構成員の互選により定める。
（４）座長は、タスクフォース構成員の中から顧問及び座長代理を指名できる。
（５）構成員の任期は委嘱時に定めるものとし、再任を妨げないものとする。

５　運　営

（１）座長は、タスクフォースの議事を掌握する。
（２）座長が、緊急の理由によりやむを得ず不在となった場合、座長代理が座長に代わり議事を掌握する。
（３）関係する政府機関等で、座長が特に認めたものについては、オブザーバとしてタスクフォースに出席することができる。
（４）座長が必要と認めるときは、暗号技術の提案者、関連する利害関係者その他の参考人から意見を聴取することができる。

（５）座長は、タスクフォースが調査する事項について特に専門的な調査を行う必要があると認めるときは、委員会等を置くことができる。
（６）座長は、必要があると認めるときは電子メールによる審議を行うことができる。なお、この審議を行った場合は、次のタスクフォースにおいて当該審議の結果を報告するものとする。
（７）その他タスクフォースの運営に関し必要な事項は、座長が定めるところによる。

６　議事の公開

タスクフォースは非公開とするが、タスクフォースで使用した資料及びタスクフォースの議事概要については、次の場合を除き、公開する。
（１）公開することにより当事者又は第三者の権利、利益や公共の利益を害するおそれがあると座長が認める場合
（２）その他、非公開とすることが必要と座長が認める場合

７　スケジュール

タスクフォースは、年度内に１回以上開催する。

８　庶　務

タスクフォースの庶務は、総務省情報流通行政局情報セキュリティ対策室、経済産業省商務情報政策局情報セキュリティ政策室、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において処理する。

資料2

重点課題検討タスクフォースの設置について

平成２７年１１月２０日
重点課題検討タスクフォース事務局

1．CRYPTRECにおいて議論が必要な議題について

2015年度第１回暗号技術検討会（以下「検討会」という）での審議の結果、検討会の下に「重点課題検討タスクフォース（以下「タスクフォース」という。）」を設置し、「CRYPTRECの在り方に関する検討グループ（参考資料１を参照）」に引き続き、以下の課題を検討することとなった（構成員及びオブザーバは参考資料2を参照）。

（検討会資料3「暗号技術検討会における「重点課題検討タスクフォース」の設置について（案）」より抜粋）

- 政府統一基準に向けた新たなCRYPTREC成果物
- 暗号プロトコルレベルのセキュリティ確保に向けた活動
- 新たな社会ニーズを見据えた新規活動
- 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
- 定常的な普及・広報活動に加え、脆弱性対応など緊急時の対応を踏まえた情報発信フローの整備

2. タスクフォース設置の狙い

（検討会資料3「暗号技術検討会における「重点課題検討タスクフォース」の設置について（案）」より抜粋）

- 情報システム全体のセキュリティ確保の為に必要となる活動の網羅性を確保しながら、社会ニーズの変化などを踏まえて、活動全般の方向性を随時議論できる場を確保する。

- CRYPTRECの方向性を機動性を持って検討し、トップダウン的な意志決定もできる体制を構築する。

- 各委員会・WG活動を俯瞰し、方針や活動プロセスを調整する機能を持たせる。各委員会は成果物作成に集中的に取り組むプロセスに改善し、CRYPTRECをより効率的に運営。

3. 検討会・タスクフォース及び各委員会の役割分担

（検討会資料3「暗号技術検討会における「重点課題検討タスクフォース」の設置について（案）」より抜粋）

- 暗号技術検討会は、総合的な知見をもって、取り組むべき方向性をタスクフォースに指示する。

- タスクフォースは、検討会から提示のあった改善すべきタスクの審議、暗号技術評価委員会や暗号技術活用委員会が行うべきタスクの選定や意思決定プロセス管理等を行う調整機能を担う。

- 暗号技術評価委員会、暗号技術活用委員会等の各委員会は、タスクフォースから提示されたタスクに集中的に取り組むことによって、CRYPTRECの効率的な運営、活動の強化を目指す。

4. 本年度CRYPTREC体制図及び検討事項

（検討会資料4「2015年度 暗号技術検討会活動計画」を元に作成）

暗号技術検討会
（事務局：総務省、経産省）

・暗号技術に関する調査・検討
・CRYPTREC活動計画の承認
・各種成果物の承認

「政府機関の情報セキュリティ対策のための統一基準」等へのインプット → NISC

在り方に関する検討グループ（終了予定）
座長：松本　勉（横浜国立大学）
（事務局：総務省、経産省）

・CRYTREC活動の見直し

重点課題検討タスクフォース
（事務局：総務省、経産省、NICT、IPA）

（1）CRYPTRECのミッション検討
・政府統一基準に向けた新たなCRYPTREC成果物
・暗号プロトコルレベルのセキュリティ確保に向けた活動
・新たな社会ニーズを見据えた新規活動
・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
・定常的な普及・広報活動に加え、脆弱性対応など緊急時の対応を踏まえた情報発信フローの整備

（2）上記に基づいた活用委員会本年度活動計画、CRYPTREC次年度活動計画方針案検討

暗号技術評価委員会
（事務局：NICT、IPA）

・暗号技術のセキュリティに関する監視・評価等
・暗号リストを中心とした暗号技術のセキュリティ評価・監視
＃評価委員会の一部の活動内容についてはタスクフォースの議論後に決定する

暗号技術活用委員会
（事務局：NICT、IPA）

・暗号技術における国際競争力の向上及び運用面でのキュリティ向上等
＃活用委員会の活動については、タスクォースの議論後に決定する

5. 本年度及び来年度の主な議題（案）

⓪ CRYPTREC活動方針についての論点～活用委員会の活動ポリシーの見直し～
→具体的な活動にあたっての前提となる方針を議論する。特に活用委員会の活動の評価軸議論が必要。これまでCRYPTRECの活動はリスト作成に代表されるようにあらかじめコンセンサスが得られた基準をもとにした“中立性・公平性”を基本の評価軸としてきたが、活用委員会の活動ポリシーの見直しが必要か議論する。

その他（ SHA-2,SHA-3の取扱い　等）
→SHA-2,SHA3の取扱い方針、タスクフォース設置の目的確認等。

第1回検討

既存活動に関わる為、優先的に議論必要（必要に応じて第2回でも議論）

① 定常的な普及・広報活動に加え、脆弱性対応など緊急時の対応を踏まえた情報発信フローの整備　（暗号アルゴリズムのみ）
→脆弱性に関する情報発信の意思決定フローを整備する。このため、脆弱性の定義、トリガーとすべき事象、情報発信時期、確認方法、情報発信手段、確認すべき暗号の範囲等を議論。

② 暗号プロトコルレベルのセキュリティ確保に向けた活動
→どのようなタスク（脆弱性対応、リスト作成、ガイドライン作成等）を想定しているか議論した上で、実施する体制を決め、他関連組織(CELLOSなど) との連携方法を検討。

③ 来年度以降の議論方針　等

第2回検討

必要に応じて第3回開催も想定

④ 政府統一基準に向けた新たなCRYPTREC成果物
→過去の成果物の検証及び、NISCの改定方針も踏まえた詳細な計画化が必要

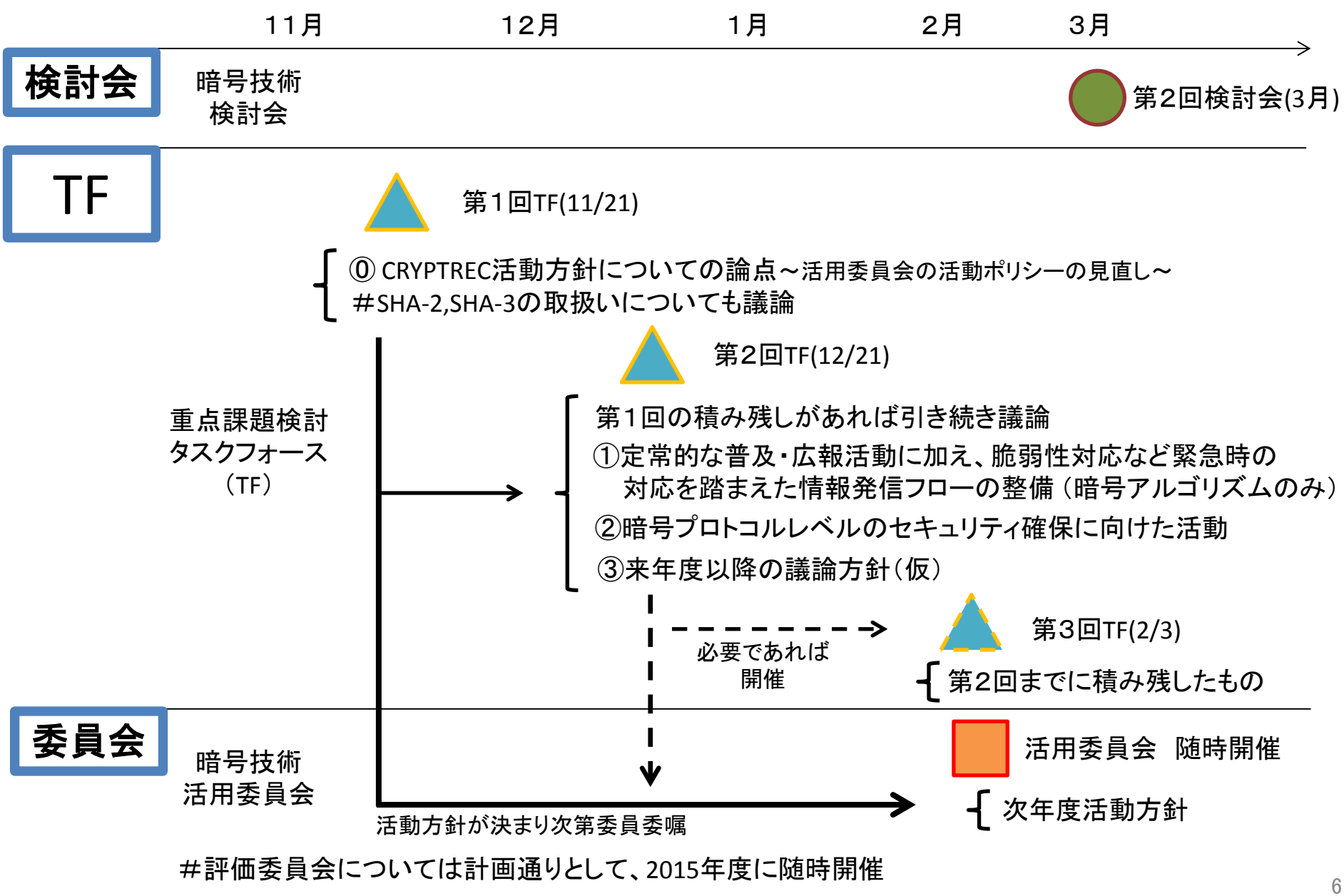
⑤ 新たな社会ニーズを見据えた新規活動
→方向性をある程度事務局で整理した上で議論すべき。

⑥ 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
→JCMVP等との連携。今後対象のタスクがある程度具体化してからの議論。

来年度検討

時間の制約上今年度は検討方針のみ議論想定

6. 本年度のスケジュール（案）



＃評価委員会については計画通りとして、2015年度に随時開催

資料３

ハッシュ関数 SHA-2、SHA-3 の取扱いについて

[議題]

ハッシュ関数 SHA-2, SHA-3 について、下記議論いただきたい。

1. リストへの追加対象となるアルゴリズム
2. 追加先リスト
3. 表記方法

[背景]

- SHA-2

  現在、FIPS 180-4 で規定されているハッシュ関数 SHA-2 のうち、SHA-256, SHA-384, SHA-512 が電子政府推奨暗号リストに掲載されている。(参考資料 2 参照) なお、JCMVP では FIPS 180-4 全体が「承認されたセキュリティ機能」に指定されている。

表 1：FIPS 180-4 で規定されている SHA-2

Algorithm	Message Size (bits)	Block Size (bits)	Word Size (bits)	Message Digest Size (bits)
SHA-224	$< 2^{64}$	512	32	224
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{128}$	1024	64	384
SHA-512	$< 2^{128}$	1024	64	512
SHA-512/224	$< 2^{128}$	1024	64	224
SHA-512/256	$< 2^{128}$	1024	64	256

- SHA-3

  SHA-1, SHA-2 の安全性への懸念から 2007 年より米国 NIST が開始した新ハッシュ関数 SHA-3 のコンペティションの結果、2012 年 10 月に Keccak という方式が選ばれ、2014 年 4 月に SHA-3 を規定した Draft FIPS 202 が公表された。その後、SHA-3 は 2015 年 8 月に FIPS202 として正式に出版された。

第一回 暗号技術評価委員会にて下記の審議結果を得ている。

- 暗号術評価委員会では、昨年度までに、安全性評価及び実装評価を行ってきた。これらの評価結果を踏まえ、CRYPTREC 暗号リストへの追加の可否を議論するための評価結果を十分にそろえられている。
  (評価結果の詳細については、参考 1・2 参照)
- 評価結果に対する見解として、昨年度までに行った安全性評価および実装評価の結果を踏まえ、SHA-2 および SHA-3 に含まれるアルゴリズムは、適切な安全性・実装性能を有している。
  (評価結果の詳細については、参考 1・2 参照)
- CRYPTREC 暗号リストへの追加対象となるアルゴリズム
  (暗号技術評価委員会承認案)
  ハッシュ長が 256 ビット以上のアルゴリズムのみとする。
  SHA-2：SHA-512/256
  SHA-3：SHA3-256, SHA3-384, SHA3-512, SHAKE256 (d≧256)

(理由)

- 現版の電子政府推奨暗号リスト（平成 25 年 3 月 1 日）を選定する際に採用した評価方針として、ハッシュ関数については、ハッシュ長が 256 ビット以上であることが望ましい、としていた。(CRYPTREC Report 2012 暗号方式委員会 表 3.17 参照)
- 旧版の電子政府推奨暗号リスト（平成 15 年 2 月 20 日）では「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。」と注釈をつけていた。

(配慮すべき点)

FIPS 180-4 で規定されている SHA-2 のアルゴリズム、FIPS 202 で規定されている SHA-3 のアルゴリズムの一部分のみがリストの対象となる。

[議題 1] リストへの追加対象となるアルゴリズム

(事務局案)ハッシュ長が 256 ビット以上のアルゴリズムのみとする

SHA-2：SHA-512/256

SHA-3：SHA3-256, SHA3-384, SHA3-512, SHAKE256 (d≧256)

[議題 2] 追加先リスト

(案 1) 即座に(実績調査は実施せず)「電子政府推奨暗号リスト」に掲載

(案 2) 即座に「推奨候補暗号リスト」に掲載し、然るべきタイミングで実績調査を実施し、調査結果に応じて「電子政府推奨暗号リスト」への昇格

(案 3) すぐにはリストに掲載せず、然るべきタイミングで実績調査を実施し、調査結果に応じて「推奨候補暗号リスト」もしくは「電子政府推奨暗号リスト」に掲載

[議論 3] 表記方法

(案 1) 各々のアルゴリズムを列挙し、注釈を添える

(案 2) SHA-2, SHA-3 と表記し、注釈を添える

案 1 のイメージ

ハッシュ関数	SHA-256
	SHA-384
	SHA-512
	SHA-512/256
	SHA3-256
	SHA3-384
	SHA3-512
	SHAKE256(注)

(注)「ハッシュ長は 256 ビット以上とすること。」など、 審議結果に基づき適切な注釈を入れる。

案 2 のイメージ

ハッシュ関数	SHA-2(注)
	SHA-3(注)

(注)「ハッシュ長は 256 ビット以上とすること。」など、審議結果に基づき適切な注釈を入れる。

<現在の電子政府推奨暗号リスト（ハッシュ関数のみ抜粋)>

ハッシュ関数	SHA-256
	SHA-384
	SHA-512

<暗号技術評価委員会での議論>

- 新たな方式は「推奨候補暗号リスト」(安全性と実装性能において問題なし)に追加する表記方法がよいのではないか
- SHA-2, SHA-3 のようにはまとめない方がよいのではないか

電子政府推奨暗号リスト

ハッシュ関数	SHA-256
	SHA-384
	SHA-512

推奨候補暗号リスト

ハッシュ関数	SHA-512/256
	SHA3-256
	SHA3-384
	SHA3-512
	SHAKE256(注)

(注)「ハッシュ長は 256 ビット以上とすること。」など、審議結果に基づき適切な注釈を入れる。

[参考 1] 安全性評価

昨年度までに下記有識者に外部評価を依頼し、評価レポートを得ている。

(SHA-2)

依頼先：

Donghoon Chang 氏（Indraprastha Institute of Information Technology, India）

http://www.cryptrec.go.jp/estimation/techrep_id2403_2.pdf

Florian Mendel 氏（Graz University of Technology, Austria）

http://www.cryptrec.go.jp/estimation/techrep_id2401.pdf

結論：表 2 で示す安全性に対して十分なマージンがあり、現実的な脅威の観点から大きな問題点は見つかっていない。

表 2：SHA-2 のセキュリティ強度

Algorithm	出力長 (bit)	セキュリティ強度（bit）		
		collision	Preimage	2nd preimage
SHA-512/256	256	128	256	256
SHA-512/224	224	112	224	224
SHA-224	224	112	224	min(224, 256−M)*

* メッセージ長が 2^Mブロックの時の 2nd preimage attack に対する耐性。

Merkle-Damgard 構成であることから Joux の multicollision 攻撃が適用でき、2^{32}ブロック以上の長いメッセージの場合、全数探索より少ない計算量で 2nd preimage が見つかる。

(SHA-3)

依頼先：

Donghoon Chang 氏（Indraprastha Institute of Information Technology, India）

http://www.cryptrec.go.jp/estimation/techrep_id2403_2.pdf

Itai Dinur 氏（École Normale Supérieure, France）

http://www.cryptrec.go.jp/estimation/techrep_id2402.pdf

結論：表 3 で示す安全性に対して安全性には十分なマージンがあり、現実的な脅威の観点から大きな問題点は見つかっていない。

表 3：SHA-3 のセキュリティ強度

Algorithm	出力長 (bit)	セキュリティ強度（bit）		
		collision	Preimage	2nd preimage
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128	*d*	min(*d*/2,128)	≧min(*d*,128)	min(*d*,128)
SHAKE256	*d*	min(*d*/2,256)	≧min(*d*,256)	min(*d*,256)

[参考 2] 実装評価

昨年度までに下記有識者に外部評価を依頼し、評価レポートを得ている。

(SHA-2 および SHA-3)

- これまでに行われてきた実装性能評価に関する研究結果のサーベイ
  依頼先：﨑山 一男教授　（電気通信大学）
  http://www.cryptrec.go.jp/estimation/techrep_id2301.pdf
- FPGA 上での性能評価
  依頼先：佐藤 証教授　（電気通信大学）
  (2013 年度 第三回暗号技術評価委員会 資料 2-3 「ハッシュ関数のハードウェア実装およびその性能測定」)

結論：ソフトウェア実装、ハードウェア実装ともに実用上、十分な実装性能を有する。

資料４

CRYPTREC活動方針についての論点

～活用委員会の活動ポリシーの見直し～

平成27年11月20日

重点課題検討タスクフォース事務局

CRYPTRECは「客観的な評価」を実施する

2. 経緯と役割　（CRYPTRECホームページ）

我が国が目指す世界最先端のIT 国家を構築するには、基盤となる電子政府のセキュリティを確保する必要があり、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。この目的のため、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た暗号技術をリスト化する暗号技術評価プロジェクトが2000年度から3年間の予定で組織化され、CRYPTREC(Cryptography Research and Evaluation Committees)と名づけられた。

客観性を確保するためにCRYPTREC（特に評価委員会）が留意してきた立場

（評価対象）

- **「仕様が公開」**されている**「公募」**または**「委員会で決定」**したもの

（評価方法）

- **「判断基準としてのコンセンサスがおおむね得られている（特定の）評価軸」**に沿った**「技術的評価」**を実施、評価結果を当該基準で判断

（審議方法）

- 上記評価結果をベースにした審議により**「（技術的な）中立性・客観性」**を重要視
- **「説明責任」**が取れる結論

CRYPTREC活用委員会のあり方について①

今までのCRYPTREC運営スタイル

- 評価軸に**判断基準としてのある一定のコンセンサス**がある（＝もともとコンセンサスがある分野がCRYPTRECの対象）
- データさえそろえば**一定の結論に集約**可能（＝判断基準に照らせば同じデータから何通りもの解釈ができるようなケースはない）
- **主体的な判断を極力排除**し、データに裏付けされた技術的観点から判断を行う**中立性・客観性を重視**（＝CRYPTREC発足時の「委員＝応募者＝評価者」が行う結果についての対外的説明責任の表明手段）

運用委員会／活用委員会での運営において見えてきた課題

- 非技術的観点を考慮する場合、**判断基準や優先すべき評価軸が変わってくる**ことがある（＝実用性を高めるためには製品の実装状況や設定状況を無視できないが、どこまで優先すべきかのコンセンサスがあらかじめあるわけではない）
- 初めからデータの**網羅性を満たすことは不可能**であるうえ、判断基準や評価軸の取り方によってデータの**解釈にも幅**がある（＝同じデータでも解釈によっては180度結論が違うことがありうる）
- 「判断基準や評価軸がいろいろ考えられる」テーマになるほど、どのような判断基準や評価軸で考えることが適切かを決めるところから**主体的な判断が入ってくる**（＝あらかじめ判断基準や評価軸が決まっているわけではない）

CRYPTREC活用委員会のあり方について②

- 「判断基準や評価軸がいろいろ考えられる」テーマを取り扱う場合には、各種データが意味する内容を紐解きながら**仮説検証プロセスを回して一定の結論**を導き出すことが必要ではないか
- 主体的判断である以上、**様々な視点・論点から議論**されるべき。**重要と考えられるがデータとしては裏付けが取れない視点、有識者の知見に基づく主観的な視点からの仮説等も議論の俎上**に載せて議論をする運営スタイルを取ることにより、むしろ厚みのある結論に至るのではないか

仮定

「判断基準や評価軸がいろいろ考えられる」テーマを扱うのであれば、**仮説検証プロセスを前提とした主体的判断と結果責任**を伴う形で活用委員会の運営を行うべきではないか。その際、CRYPTRECの運営スタイルにおける**「中立性・客観性」の意味合いを広げて従来とは質的に異なる運営スタイルを許容する必要**があると思われる。

- ✓ 総合的観点からの主体的判断をベースに仮説を組み立てて結論を導く以上、多数の人から合理的説明になっている、そういう判断は妥当だよね、といってもらえる程度の論理構成になっているかどうかが重要ではないか（**主体的な判断による合理的な説明・解釈がついている結論＝中立性・客観性をもった結論**）
- ✓ データの網羅性を初めから満たすことは不可能であるうえ、データの解釈にも幅があることを前提に、仮説検証プロセスを通じて**数少ないデータからでもデータの妥当性や判断が正しいかどうかをチェック**していくしかないのではないか

【論点①】活用委員会での活動ポリシーの再整理

運用／活用委員会での審議内容は、従来のCRYPTRECの
運営スタイルの枠内で行うことが難しくなってきていることが露呈

↓

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、
活用委員会の運営スタイルの考え方自体を再整理する必要がある

【論点】

- 活用委員会の運営スタイルとして、評価委員会と同じ運営スタイルを適用するか異なる運営スタイルを新たに定義するか
- （評価委員会と同じ運営スタイルを適用する場合）どこの活動テーマが本来許容できる範囲か
- （評価委員会と異なる運営スタイルを設定する場合）どこまでの活動テーマを扱うことが期待されているか

例）← 主体的判断の要素小さい　　主体的判断の要素大きい →

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）

運用スタイルの再整理にあたっての考慮ポイント

- 「判断基準や評価軸がいろいろ考えられる」テーマの議論では、有識者の知見や暗号製品等の利用者の動向に基づく、委員会としての**「主体的な評価・判断」が実質的なベース**になる
  - 仮説を先に設定しないと何を論点として議論すべきかわからない点に留意が必要だが、仮説を作る時点ですでに主体的な判断が入っている
  - 利用状況、ユーザビリティ等の非技術的要素については、調査に網羅性を持たせることは事実上不可能
  - 判断基準や評価軸がいろいろ考えられる以上、非技術的要素での評価結果をどう判断するかは主体的な解釈に委ねられる
  - どのような結論であれ、合理的と考えられる仮説、思想などに基づく選択肢を「主体的に判断」した結果を提示していることとなる
- 実用性を上げる情報を提供するほど、**「従来の意味での中立性・公平性は低下」**
  - 技術的には同等以上のものが並んでいても、利用状況等の非技術的要因で優先度・推奨度に事実上の優劣がつく（場合によっては逆転もある）
  - 多く利用されている暗号製品を取り上げた場合であっても、設定に当たっての対象製品を具体的に例示することで、特定製品の利用推奨につながるおそれがある

【論点②】想定する活用委員会活動内容とプロセス整理

- SSL/TLS暗号設定ガイドラインのアップデート（どこまでやるか）
  - アップデート内容案（1）：最新動向の追記・更新
    - 最近のIETF動向反映
      - RFC7465 – Prohibiting RC4 Cipher Suites
      - RFC7469 – Public Key Pinning Extension for HTTP
      - RFC7568 – Deprecating Secure Sockets Layer Version 3.0
    - SHA-2非対応携帯電話でのアクセス終了アナウンスの反映
  - アップデート内容案（2）：ガイドライン本体の更新
    - セキュリティ例外型の記載内容の見直し是非
  - アップデート内容案（3）：Appendixの更新
    - 実用性向上の観点から市販製品での具体的な設定方法をAppendixに追加

【論点】

- 特に**アップデート内容案（3）まで踏み込むべきか**否か

メリット	懸念点
● 実用性は確実に向上 ● SSL/TLS市販製品の利用・調達の際のセキュリティ向上が期待できる ● チェックリスト化がしやすい	● 特定のSSL/TLS市販製品を推奨しているかのように誤解される／使われる恐れ ● ガイドライン本文の要求条件に近い設定が可能だが差異がある場合に、どこまでOKとするかについての判断が必要

【論点②】想定する活用委員会活動内容とプロセス整理

- どの種類のガイドラインから整備することが期待されるか
  - SSL/TLS暗号設定ガイドラインと同系列の設定ガイドライン
    - **従来と同じ運営スタイル**で実施可能（SSL/TLS暗号設定ガイドラインが基準）
  - マネジメント関連のガイドライン
    - フレームワークとしての誘導になるので、「何を目指してどう実現するか」という委員の知見集約による**主体的な判断に基づいたコンセプト提示に沿う運営プロセス**が必要
- 何らかの政策的課題・社会ニーズ的課題を取り扱うか
  - どんな課題が期待されているか
    - **仮説検証プロセスの運営スタイル**でないとそもそも扱うことが困難

【論点③】成果物の扱い方法と展開方法の整理

■ 成果物の種類と展開方法

成果物の種類	CRYPTREC成果物（従来）		展開方法
特定の基準に基づき、**中立性を重視した客観的な技術評価**を実施した結果をまとめたドキュメント	• 技術報告書 • 暗号技術調査WG報告 • リストガイド	評価委員会	• CRYPTRECホームページ
特定の基準に基づき、**中立性を重視した客観的な判断**を行った結果をまとめたドキュメント	• 暗号技術ガイドライン	評価委員会	• CRYPTRECホームページ
	• CRYPTREC暗号リスト	評価委員会	• CRYPTRECホームページ • NISC統一基準での参照
委員の技術知見や外部状況等も考慮して、**主体的な判断**を行った結果をまとめたドキュメント	• 暗号運用ガイドライン（本文）	活用委員会	• CRYPTRECホームページ • IPAホームページ • IPA印刷による展示会冊子配布
委員の技術知見や外部状況等も考慮して、セキュリティ向上のための**誘導的要素を主体的に組み入れた**ドキュメント	（今までなし）	活用委員会	（今までなし）
委員の技術知見に基づき、**セキュリティに係る情勢等を主体的に分析・考察**した結果をまとめたドキュメント	（今までなし）	活用委員会	（今までなし）
実用性を向上させるための**具体的な設定方法を紹介**したドキュメント	• 暗号運用ガイドライン（Appendix）	活用委員会	• CRYPTRECホームページ • IPAホームページ • IPA印刷による展示会冊子配布
外部機関が作成・公表する同系列のドキュメントへの**お墨付きを与えた**ドキュメント	（今までなし）		（今までなし）

【論点】

- ■ CRYPTRECブランド（ロゴ）をどういう方針で扱うべきか
- ■ 展開方法とどうリンクさせるべきか
  - • 冊子のニーズは想像以上に大きい（特に管理職クラス以上）

参考：活用委員会（運用委員会含む）での評価内容拡大

- 電子政府推奨暗号リストの位置づけ明確化の決定（2010年度）
  - 電子政府推奨暗号リストと推奨候補暗号リストの位置づけの違いをどこに置くかを決めるために、暗号アルゴリズム選択方法についての「アンケート調査」を実施（→ユーザーの視点を加味）
- 電子政府推奨暗号リストの選考（2012年度）
  - 電子政府推奨暗号リスト選考のための「利用実績調査」を実施（→ユーザーの利用状況を加味）
- SSL/TLS暗号設定ガイドラインの作成（2014年度）
  - 実用性を高めることを考慮し、製品実装状況・設定状況などの「非技術的要素」も加味（→利用環境に応じた設定を加味）
- 暗号普及促進・競争力強化に向けた課題分析と見解（2014年度）
  - コンセンサスがそもそもなく、「何が正解であるかすら分からない」テーマであり、論点整理では「仮説」も採用（→事務局主観の方向性を作成）
  - 課題分析のために「ヒアリング調査」と「文献調査」を実施（→ヒアリングで事務局仮説の裏付け）
- SSL/TLS暗号設定ガイドラインのアップデート（予定）
  - 「市販製品」での具体的設定方法の記載も検討（→ユーザの利便性向上）

参考①：2010年度調査での課題

- 暗号アルゴリズム選択方法についてのアンケート調査（2010.12）

（調査目的）

実際の電子政府情報システムの構築及び暗号搭載製品の開発・製造の現場においては、必ずしも技術的観点だけで暗号アルゴリズムの選択が行われているわけではない。そこで、「（旧）電子政府推奨暗号リスト」の課題点を抽出し、「CRYPTREC暗号リスト」をどのような考え方のもとで作成することがよいのかについての情報を得る

（調査手法）

- 各企業の暗号アルゴリズム選択方法の実態を調査
- 応募企業の他、17分野シェアトップ級企業2，3社（合計40社程度）を主な対象に調査
- 各企業にIPAが直接訪問して調査目的及び回答内容の取扱い方法を説明し、了解を得たうえでアンケート調査回答を依頼
- 社名公開了承を受けた企業のみ、調査協力会社として社名公開。個別の回答内容は、委員会審議を含め、完全非公開を保証
- 回答原本データはIPAで管理、回答内容と回答会社のリンクを切ったうえで統計処理後のデータのみを公開（事務局内は回答内容のみ共有）

（調査結果の取り扱い）

電子政府推奨暗号リスト作成に際して利用実績に基づく絞り込みを行うと決定する傍証になった

（調査における課題等）

- 調査趣旨に了解を得た**少数の企業**からしかアンケート回答結果が得られなかった
- 選択肢形式のアンケート調査であるため、**選択肢に回答が誘導**される恐れがある
- 公開できるデータに限界があり、**データ以上の説明責任は果たせない**
- コンセンサスが得られている評価基準に照らし合わせたわけではなく、**どの解釈が“最も合理的そうか”の観点での委員会結論が「絞り込みを行うべき」**となった

参考②:2012年度調査での課題

- 暗号利用実績についてのアンケート調査(2012.07)

(調査目的)

電子政府推奨暗号を選定するための評価基準に沿った基礎データとして、個々の暗号アルゴリズムの利用実績を調査する

(調査手法)

- 応募者、市販会社(20分野に製品群をカテゴリわけ)、政府機関、標準化団体、OSSごとに暗号アルゴリズムごとの利用実績を調査。アンケート項目については委員会承認を実施
- IPA単独委託調査事業で実施(ただし、調査手法や調査対象の範囲、調査結果の集計方法等について、2012年度第1回及び第2回での委員会において審議し、IPA調査を監督)
- 回答原本データはIPAで管理、回答内容と回答会社のリンクを切ったうえで統計処理後のデータのみを公開
- 市販会社へのアンケート配布数1849社、回答数127社(443製品)。回収率6.87%
- 製品シェアは考慮しない

(調査結果の取り扱い)

先に承認された選定基準に照らして電子政府推奨暗号を選定する主要な根拠となった

(調査における課題等)

- **網羅性の保証は不可能**。理想的なアンケート配布ができても網羅性を持った回収は期待できず
- アンケート回答会社の結果しか反映されない
- 公開できるデータに限界があり、**データ以上の説明責任は果たせない**
- 製品シェアやシステム重要性についての評価基準のコンセンサスがないので、製品やシステムの重要性の**「重みづけをしないほうが客観性を確保できる」と委員会で結論**
- 非公開システムでの実績は確認できないので、**「選考除外とするほうが客観性を確保できる」と委員会で結論**

参考③：2014年度調査での課題

- 競争力強化分析のヒアリング調査（2014.06）

（調査目的）

「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析を行うにあたって幅広く現況を俯瞰することための情報を得る

（調査手法）

- セキュリティビジネスの現状に関するヒアリング調査
- IPA単独委託調査事業で実施
- 調査会社が選定した9社でヒアリング
- 調査会社がヒアリング先の完全非公開を保証してヒアリングを実施
- ヒアリング先とのリンクが取れない形で回答要旨のみを議事録にまとめて納品

（調査結果の取り扱い）

仮説議論、論点整理をする際の参考データとなった

（調査における課題等）

- **少数の企業**からのヒアリング結果でしかないが、ヒアリング調査ではそもそも数はこなせない
- 公開できるデータに限界があり、**データ以上の説明責任は果たせない**
- 各社ごとの個別ヒアリング調査であるため、すべての担当者が同じ認識レベルで対応してくれているとは限らない
- 選択肢形式のアンケートとは異なり、ヒアリング結果をまとめる際に**様々な担当者の主体的な判断・解釈が無意識に入っているおそれ**がある
- コンセンサスが得られている評価基準に照らし合わせたわけではなく、**“合理的に説明できそうな解釈”の観点での論点整理が委員会結論**となった

参考④：2015年度下期調査（予定）の課題

- SSL/TLS市販製品での暗号設定状況の調査（2016.01予定）

（調査目的）

SSL/TLS暗号設定ガイドラインでのAppendixのアップデートを視野に、市販製品レベルでの具体的な暗号設定に基づくSSL/TLSプロトコルの適正な利用促進を図る

（調査手法）

- SSL/TLS市販製品での暗号設定状況を調査
- IPA単独委託調査事業での実施（確定）
- 調査費の観点から機器調達の独自実施は不可能。ホームページやビジネス年鑑等を参考にコンタクト先企業を選定し、無償貸出を依頼
- 各企業にIPAが直接訪問して調査目的を説明し、企業名をIPA調査報告書に明示・公開することを約束したうえで製品無償貸出の協力を得る（10社強）
- 協力いただく企業のほうで無償貸出する製品の機種選定を実施
- 調査結果は公開前に協力いただいた企業に報告・協議をすることを約束

（調査結果の取り扱い）

IPA調査報告書としては2016年夏に公開（予定）。SSL/TLS暗号設定ガイドラインのAppendixのアップデートに組み込むかは別途議論

（調査における課題等）

- コンタクト先を選ぶ時点ですでに**網羅性が乏しい**
- ビジネス的にメリットがあると判断した企業しか協力が得られない。機種選定の**主導権は協力いただく企業（＝協力企業）**のほうにある
- 協力企業が**自社ビジネス活動に有利になるように調査結果を活用**することが容易に想定される
- SSL/TLS暗号設定ガイドライン本文の要求条件に近い設定が可能だが差異がある場合に、**どこまでOKとするかについての判断が必要**になると想定される

参考資料１

「CRYPTREC の在り方に関する検討グループ」における議論結果報告書

平成 27 年 10 月５日

暗号技術検討会事務局

参考資料１

目次

参考資料１

１.「CRYPTREC の在り方に関する検討グループ」設置の経緯

2001 年に CRYPTREC が発足した当初の目的は、安全でない暗号アルゴリズムが乱立する中で、電子政府において利用が推奨される安全な暗号アルゴリズムを確定させることであり、活動成果として 2003 年に「電子政府推奨暗号リスト」を策定した。

その後、CRYPTREC は、その発足の趣旨に鑑み、電子政府推奨暗号リスト掲載の暗号アルゴリズムについて安全性低下などの問題（暗号危殆化）の監視、注意喚起等を実施など、安心な暗号利用について貢献してきた。一方で、国際標準規格の策定などの要因により、国際的に利用できるデファクト暗号アルゴリズムへの集約が進み、安全でない暗号アルゴリズムが混在するという懸念は激減した。このような外部環境の変化を踏まえ、市場性や利用状況等を加味して評価した結果 2012 年度末に「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)」を策定（以下「リスト改定」という。）した。

また、リスト改定後は、従来からの「CRYPTREC 暗号リストの安全性維持に係る取組」に加え、「新しい暗号技術の調査」、「暗号技術の普及促進に係る取組」、「中長期的視点に立った暗号政策に係る検討」等を行ってきた。

上記活動を通じて、暗号技術を取り巻く環境、サイバーセキュリティ基本法の施行といった社会情勢の変化等に鑑み、CRYPTREC が果たすべき役割は、CRYPTREC 暗号リストの策定及び維持に限られるものではなく、より柔軟に活動することが望ましいといった意見があった。

このため、今後、社会ニーズ等を踏まえた柔軟な活動を図るべく、CRYPTREC で対象とする暗号技術の見直しや、活動範囲、また安全性確保等にかかる活動の在り方（緊急時対応、必要な体制の見直し）等の議論を行うことが望ましいと考えられ、暗号技術検討会に「CYPTREC の在り方に関する検討グループ」（以下「検討グループ」という。）を設置し、議論を行った。

本報告書では、2015 年 6 月より合計４回開催した検討グループの議論の結果と、今後の CRYPTREC の体制について報告することとする。

参考資料１

2.「CRYPTREC の在り方に関する検討グループ」概要

2.1 体制（事務局・構成員）

検討グループは、暗号技術検討会の構成員を中心に、学識経験者、暗号ユーザー、暗号研究者により構成することとし、オブザーバーに NISC の参加を得つつ、総務省、経済産業省が事務局として開催した。構成員は表１の通り。

表１　CRYPTREC の在り方に関する検討グループ　構成員名簿

	委員氏名	所属
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
構成員	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
構成員	太田　和夫	国立大学法人電気通信大学　大学院 教授
構成員	近澤　武	独立行政法人情報処理推進機構 セキュリティセンター 暗号グループグループリーダー（ISO/IEC JTC 1/SC27/WG2 Convenor（国際主査））
構成員	手塚　悟	東京工科大学 コンピュータサイエンス学部 教授
構成員	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
構成員	盛合　志帆	国立研究開発法人情報通信研究機構 ネットワークセキュリティ研究所 セキュリティ基盤研究室 室長
オブザーバー	内閣官房内閣サイバーセキュリティセンター	

事務局

総務省　情報流通行政局　情報セキュリティ対策室

経済産業省　商務情報政策局　情報セキュリティ政策室

2.2 開催実績

検討グループは、表２のとおり、合計４回開催した。各会合の開催日及び主な議題は以下のとおり。

表２　CRYPTREC の在り方に関する検討グループの開催

回	年月日	議題
第１回	2015 年 6 月 3 日	(1)「CRYPTREC の在り方に関する検討グループ」開催要綱について (2)CRYPTREC に関する現状について
第２回	2015 年 6 月 24 日	(1)前回議事確認と本日の議論の進め方について (2)CRYPTREC に関する問題意識 (3)暗号プロトコル評価技術コンソーシアム(CELLOS)の概要 (4)サービス視点からの暗号技術(の重要性) (5)全体を通しての意見交換
第３回	2015 年 7 月 3 日	(1)前回議事確認と本日の議論の進め方について (2)CRYPTREC で取り組む新しい暗号技術 (3) これからの CRYPTREC について (4)第１回、第２回の発言ポイントまとめ (5)全体を通しての意見交換
第４回	2015 年 8 月 3 日	(1)前々回の議事確認と今回の進め方について (2)CRYPTREC の在り方に関する検討グループまとめ案 (3)全体を通しての意見交換

参考資料１

3.「CRYPTREC の在り方に関する検討グループ」議論概要

3.1　全体俯瞰図に関する議論

CRYPTREC が担うべきタスクに関する議論にあたって、以下の論点を踏まえた検討が必要との方針がまず示された。

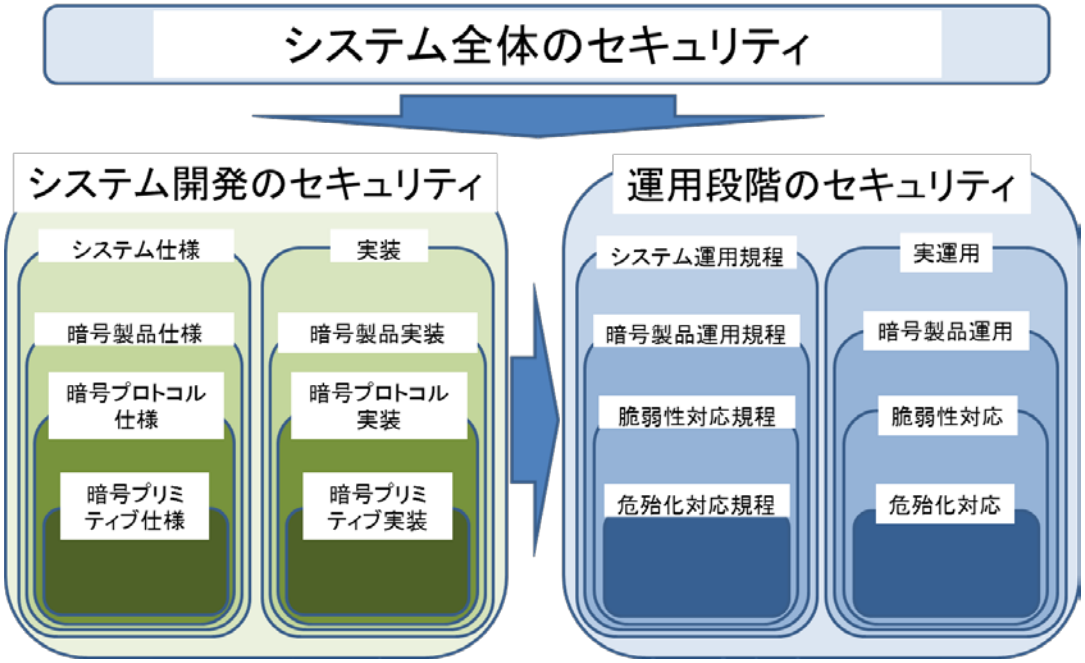
・目的：従来のミッションから変更すべきか、何を追加すべきか
・対象とする活動領域：暗号アルゴリズム等従来に加えて何を対象とするか
・主な適用範囲：電子政府に加えて一般向けの情報システムも対象とするか
・成果物：CRYPTREC 暗号リストに加え、どのような成果物が考えられるか

ただし議論の過程において、「情報システムにおける暗号技術のセキュリティ確保の全体俯瞰図を共通認識として持ち、それを踏まえた上で議論をすべき」との意見が多くの構成員より提出された為、以下の観点から全体俯瞰図を整理した。

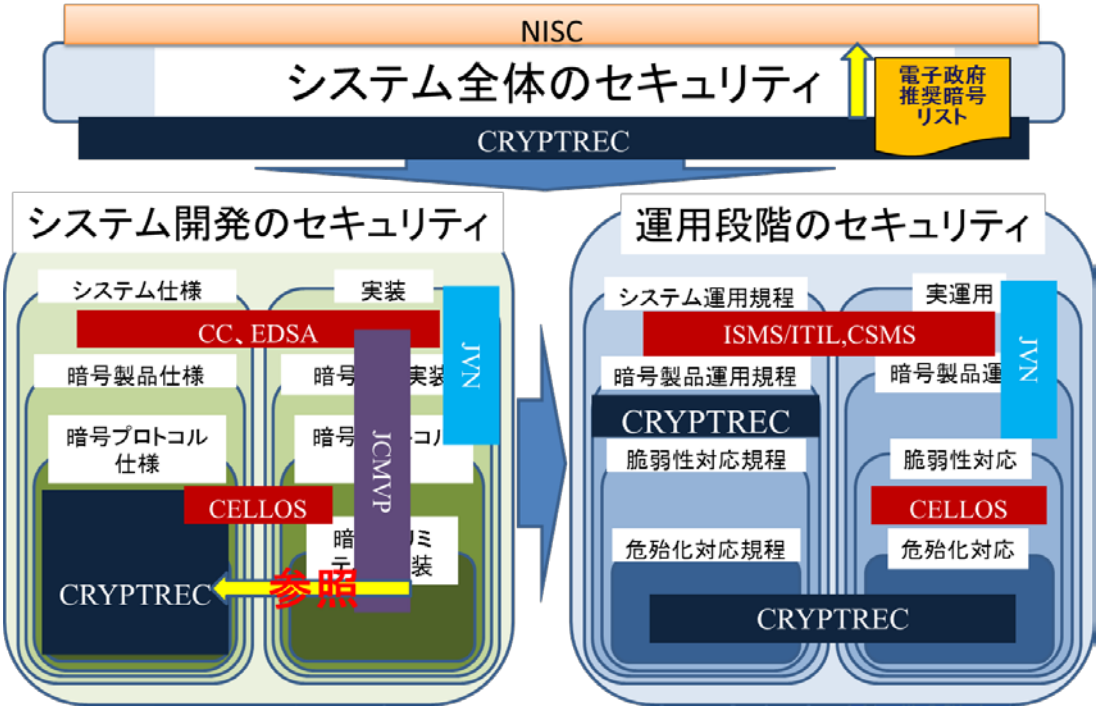
- 情報システムにおける暗号技術のセキュリティは開発及び運用段階で分けて考える必要がある
- さらにそれぞれを「仕様と実装」、「規程とその規程の実運用」とに分けて考えた方が良い
- その上で様々な暗号プリミティブ、プロトコル、製品から情報システム全体といったレイヤ別に確認が必要

上記を踏まえて以下の全体俯瞰図を作成した。

参考資料１



さらにこの俯瞰図を踏まえた上で、現状の「政府」情報システムにおける暗号技術のセキュリティ確保する既存の各活動と各役割の整理を以下のように行った。



※CC(Common Criteria):IT 製品のセキュリティ認証制度　CELLOS(Cryptographic protocol Evaluation toward Long-Lived Outstanding Security(CELLOS) Consortium) : 暗号プロトコル評価技術コンソーシアム　CSMS(Cyber Security Management System):制御システムに関するセキュリティマネジメントシステム　EDSA(Embedded Device Security Assurance):制御機器（組込み機器）のセキュリティ保証に関する認証制度　ITIL(Information Technology Infrastructure Library):IT サービスマネジメントのベストプラクティスをまとめたフレームワーク　JCMVP(Japan Cryptographic Module Validation Program):暗号モジュール試験及び認証制度
JVN(Japan Vulnerability Notes):ソフトウェアなどの脆弱性対策情報ポータルサイト

その結果、以下のようなCRYPTRECの現状の位置付けと、関連する活動の状況が整理された。

- CRYPTREC は主に、情報システム開発の暗号プリミティブへの対応を主眼におき、暗号プロトコルの仕様まで対象に含めて対応してきた。
- 運用に関しても、CRYPTREC は危殆化監視活動の他、一部製品レベルに踏み込んだ運用規程（SSL/TLS暗号設定ガイドライン等）を提供している。
- CRYPTREC が主に対象としている以外の領域にも、基本的にはセキュリティの担保をするための認証制度や情報提供機能等の仕組みがある。

上記の全体俯瞰状況を踏まえた上で、各項目について議論を行った。

3.2 CRYPTRECのミッション（目的）に関する議論結果概要

CRYPTRECミッションに関わる事項についても多くの議論がなされた。

現行のミッションは「CRYPTREC暗号の安全性及び信頼性確保のための調査・検討、CRYPTREC暗号リストの改定に関する調査・検討に加え、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」となっているが、それらに対して各種意見が出され、以下の課題が整理された。

- 暗号アルゴリズムより上のレベルであるプロトコルや製品、また実装・実運用に関する活動に関して、CRYPTRECとしてどのようなミッションを持つか
- CRYPTRECで行う「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」を今後どうするか
- プライバシー保護やIoT社会など社会ニーズを見据えた暗号技術への取組や提言機能をミッションとして加えるか

上記の課題に対して、以下のような検討の指針が示された。

- 活動領域の詳細議論にて、情報システム全体のセキュリティ確保に最適なCRYPTREC活動の在り方について検討
- 今後、CRYPTRECで行うべき「普及促進」の明確化が必要
- 新たな社会ニーズの把握と、必要な提言機能のミッション追加を検討する

これらを踏まえて、新たなミッションに関する案が示された。

「CRYPTREC 暗号(※１)のセキュリティ及び信頼性確保のための調査(※２)・検討、CRYPTREC 暗号リストの改定に関する調査・検討に加え、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（※３）や提言」

（※１）暗号プロトコルを含む。

（※２）監視活動を含む。

（※３）一般利用者からのニーズの検討も含む。

ただしミッションについては、その他の各種議論を踏まえた上で最終的には見直すものであり、継続的な議論が必要との結論となっている。

3.3 CRYPTREC が対象とする活動領域に関する議論結果概要

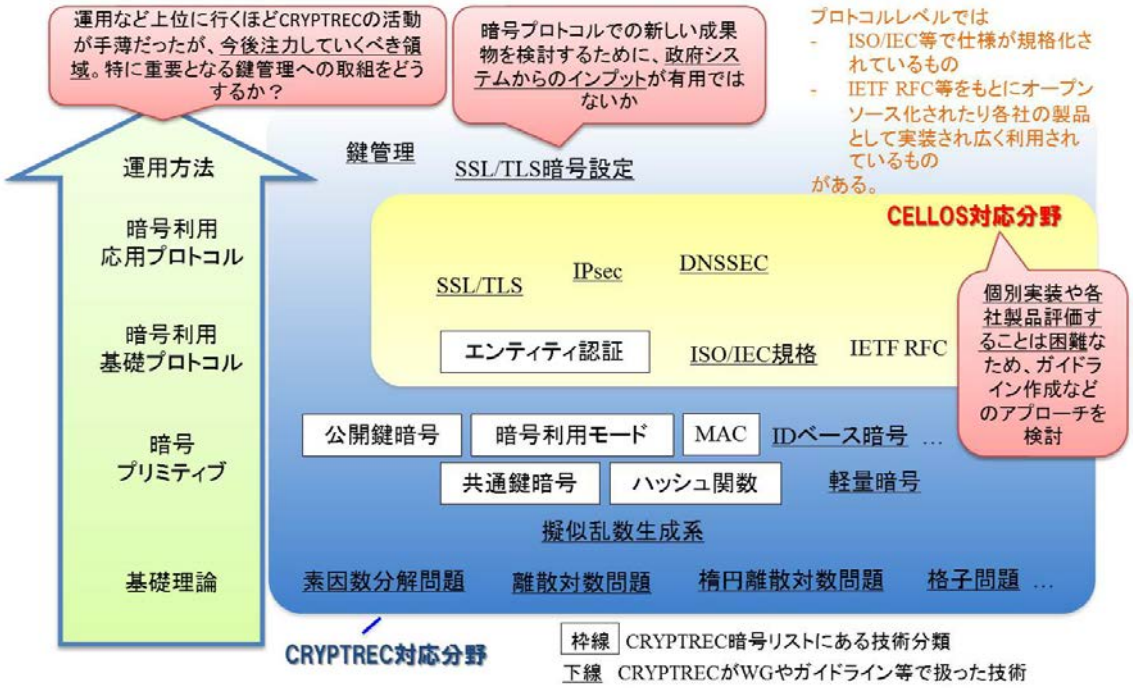
対象とする活動領域の検討について、既存の他団体の活動（プロトコルのセキュリティ評価（CELLOS)、製品（ソフトウェア）の脆弱性（JVN）等）との関係を考慮した上で各種議論がなされ、以下のような課題が整理された。

- CRYPTREC の網羅性
- 暗号プロトコル評価に関する CELLOS との役割分担
- その他既存の他団体と連携

上記の課題に対して、それぞれ以下のような議論がなされた。

- CRYPTREC の網羅性に関しては、既に CRYPTREC で活動している領域でも、活動の網羅性（政府調達から参照されるべき成果物を揃えることができるか、という観点）から再検討されるべき、という観点で多くの議論がなされた。例えば暗号プロトコル及び運用面（鍵管理等）での活動を再検討することが必要といった意見がみられた。
- 暗号プロトコルでの評価活動を検討するにあたっては、活動目標に応じて、CELLOS との詳細な情報交換を行い、具体的連携方法の議論が必要との認識が示された。
- CRYPTREC の限られたリソースも考慮すると、実装や製品評価といった個別評価の分野や脆弱性対応など迅速性が要求される分野は積極的に他団体との連携を検討することが必要との認識が示された。

参考資料１



（参考）暗号技術マップのイメージ

これらを踏まえて、活動領域に関する以下の案が示された。

・既存の CRYPTREC 活動領域について、以下の観点で見直す
-暗号プロトコル仕様のセキュリティ確保対策について、CELLOS との連携を考慮しつつ、引き続き検討する
-運用のセキュリティ確保に関連して必要な活動について、引き続き検討する

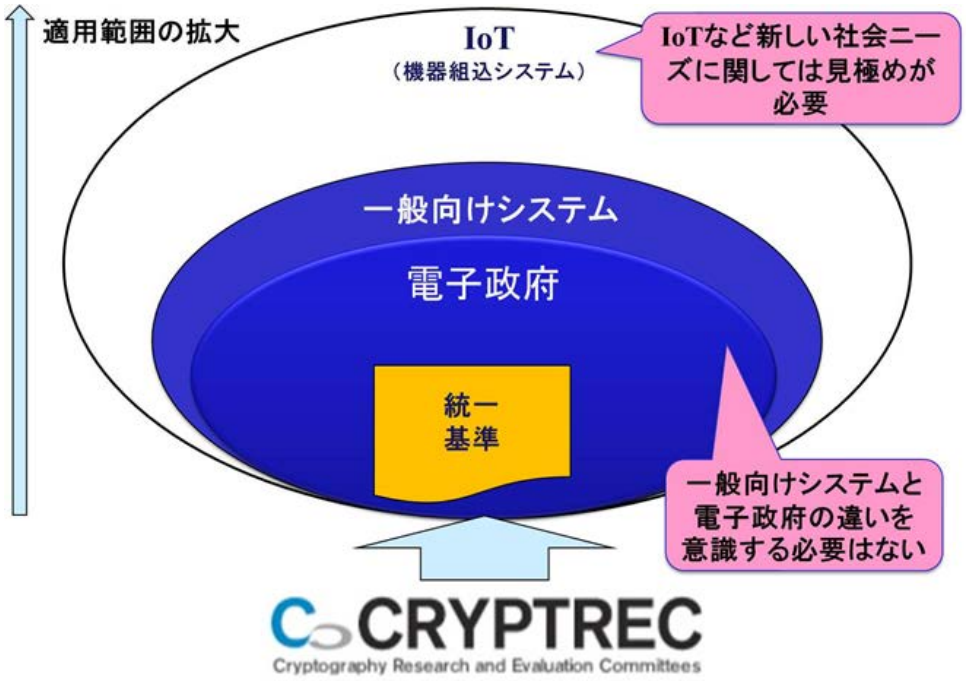
・実装や製品評価といった個別評価の分野や脆弱性対応など迅速性が要求される分野について、他団体との具体的連携を引き続き検討する
-CELLOS との脆弱性対応での連携における具体的フロー検討
-その他の団体との連携に関する必要性やその具体的フロー検討

3.4　CRYPTREC の成果物の主な適用範囲に関する議論結果概要

主な適用範囲については、ビジネスの現状や今後の IoT 社会の到来などの変化も踏まえて、技術的な安全性は前提としながらも、厳密性と運用上の制約とのバランスを考慮しながら、CRYPTREC 活動が主に対象とする領域をどう考えるべきか議論が行われた。

参考資料１

まず電子政府情報システムから一般情報システムへと領域拡大を検討すべきかが議論されたが、その差異をあまり意識する必要はないとの結論となった。（電子政府情報システム向けの成果物でも利用しやすいものであれば一般情報システムでも利用可能）



（参考）CRYPTREC 成果の適用範囲のイメージ

ただし、IoT やプライバシーなど新しい社会ニーズに関しては見極めが必要との意見が多く出され、以下の課題が整理された。

- IoT 社会を見据えた暗号技術への取組
- 社会ニーズを見据えた調査・検討と提言機能

これらに対して、以下の様な解決に向けた方針が示された。

- IoT 社会で重要になる軽量暗号等について、CRYPTREC として更なるアプローチが可能か、検討が必要
- 暗号技術が社会において活用されるために必要な制度・ガイドラインについて検討し、各種制度や法律も視野に入れた議論が出来る体制が必要

これらを踏まえて、成果物の主な適用範囲に関する以下の案が示された。

- 軽量暗号に関する更なる活動強化を引き続き議論
- 新たな社会ニーズを調査・検討する体制を検討

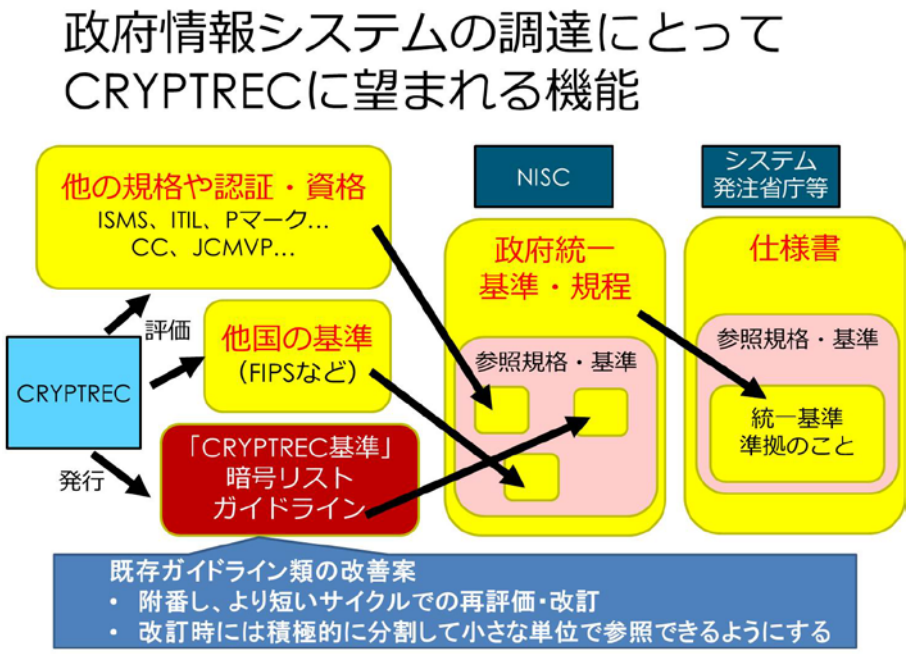
3.5　CRYPTREC の成果物に関する議論結果概要

成果物として、まずは電子政府向けでも現状の暗号リスト以外に柱となるべきものの検討が必要との観点から、以下の課題を挙げた。

- 「情報システム全体における暗号技術のセキュリティ確保」の為に必要なコンテンツ（成果物）の整理

特に CRYPTREC の本来の活動領域である政府調達情報システムにおいて上記課題を解決するために、CRYPTREC がどのような活動を行うべきかが議論された。その結果、既存ガイドライン類を改善し、より政府統一基準等から参照しやすいものとすべき、との意見が提出された。具体的には、成果物ごとの目的の明確化とそれに合わせた内容作成・更新とその情報発信が必要との認識であり、例えば以下のような改善案が示された。

・附番し、より短いサイクルでの再評価・改訂
・改訂時には積極的に分割して小さな単位で参照できるようにする



（参考）政府調達と CRYPTREC 成果物のあるべき関係性イメージ

参考資料１

これらを踏まえて、成果物に関する検討に対して、以下の案が示された。

- 政府調達に向け統一基準から参照可能な成果物体系の議論を引き続き継続
  -NIST との比較分析を含む
- 適切な情報発信の在り方について引き続き検討
  -他団体との連携方法

以上

参考資料２

CRYPTREC　重点課題検討タスクフォース　構成員・オブザーバ名簿

（構成員）

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
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
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
近澤　　武	独立行政法人情報処理推進機構 セキュリティセンター暗号グループ グループリーダー（ISO/IEC JTC 1/SC27/WG2 Convenor（国際主査））
手塚　　悟	東京工科大学 コンピュータサイエンス学部 教授
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
満塩　尚史	内閣官房　政府ＣＩＯ補佐官
盛合　志帆	国立研究開発法人情報通信研究機構 ネットワークセキュリティ研究所 セキュリティ基盤研究室 室長

（オブザーバ）

内閣官房内閣サイバーセキュリティセンター

（五十音順、敬称略）

＜参考＞
（事務局）

総務省　情報セキュリティ対策室

経済産業省　情報セキュリティ政策室

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