CRYPTREC検討会活動報告

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会　座長
（横浜国立大学 教授）
松本　勉

目次

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。

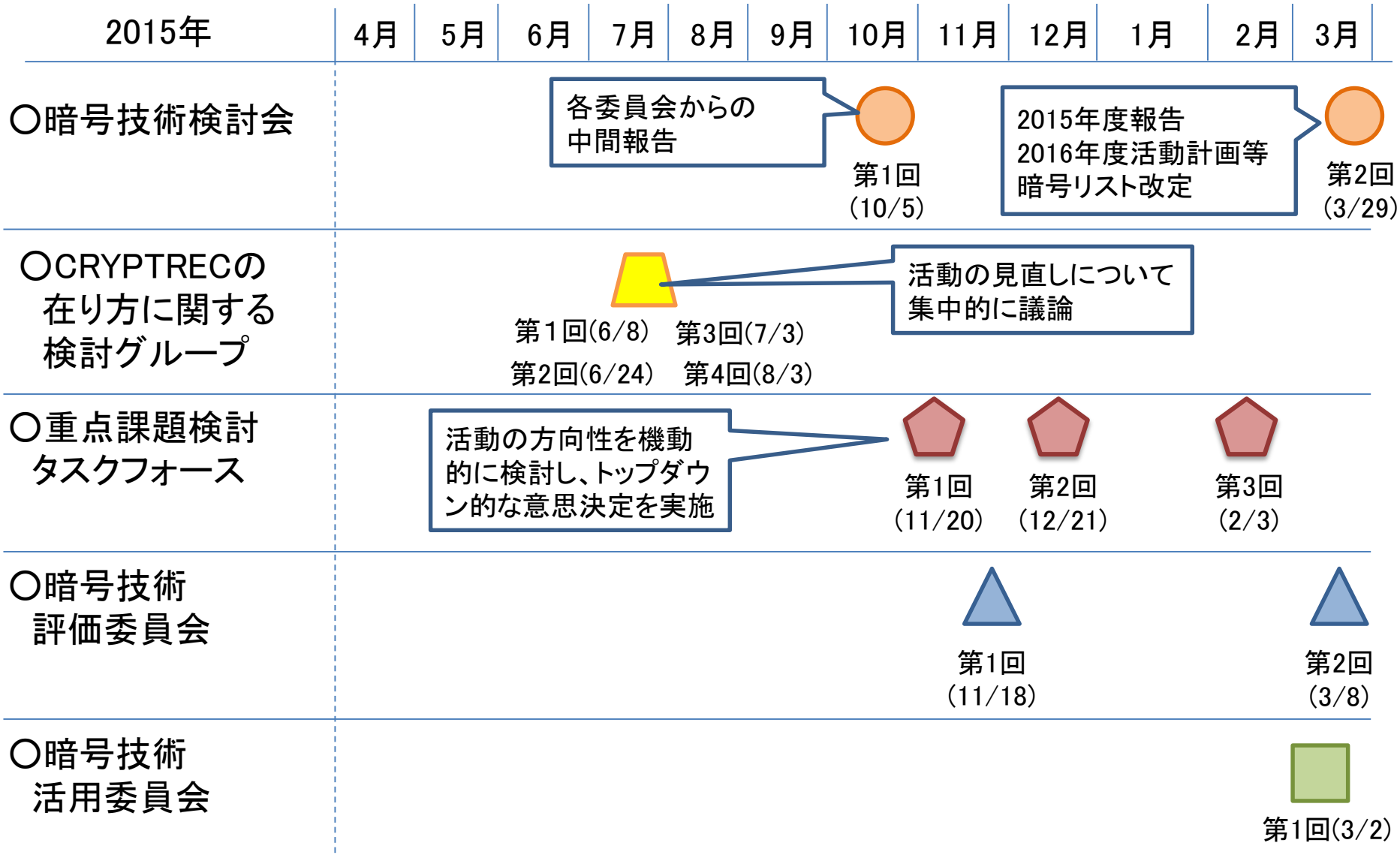
– 暗号技術検討会並びに暗号技術検討会の下に設置される暗号技術評価委員会及び暗号技術活用委員会により運営。

（活動の見直し）

– 2015年度、暗号技術に対する社会ニーズや社会情勢の変化を踏まえ、暗号技術検討会の直下に検討の場を設置。

CRYPTREC
Cryptography Research and Evaluation Committees

2015年度暗号技術検討会等の開催概要



CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術に対する社会ニーズの変化

暗号技術の位置付けの変化

- 暗号技術が社会基盤の重要なひとつの要素となった為に、暗号の安全性を確保することの社会的意義が拡大。
- 暗号アルゴリズムは、ビジネスや普及促進といった観点において、競争力の要素となりにくくなり、製品やサービスレベルまで含めての対応が必要。
- 安全性確保という観点からは、暗号アルゴリズムを利用したプロトコルやアプリケーションの安全性評価や脆弱性対応等の重要性が増加。

IoT社会の到来

- あらゆるモノがネットワークに繋がり、大量のセンサーからデータが集められ、新たな価値や行動が創造。
- 暗号技術が組み込まれた製品が、急速に社会へ普及。

情報システム全体を視野に入れた暗号技術を用いたセキュリティ確保が重要との観点からCRYPTRECの活動を見直し

CRYPTREC
Cryptography Research and Evaluation Committees

2015年度の体制図（当初）

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）

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

CRYPTRECの在り方に関する検討グループ

＜CRYPTRECの見直しに係る論点＞

CRYPTRECが担うべきタスクについて、以下の論点を踏まえた検討を実施

- 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のもの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システムも対象とするか
- 成果物
  CRYPTREC暗号リストに加え、新たな成果物が考えられるか

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECの在り方に関する検討グループ

＜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＞

- 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
- それぞれ仕様と実装、規程とその規程の実運用とに分けて考えた方が良い
- 様々な暗号プリミティブ、プロトコル、製品からシステム全体といったレイヤ別に確認が必要

情報システム全体のセキュリティ

システム開発のセキュリティ

- システム仕様
  - 暗号製品仕様
  - 暗号プロトコル仕様
  - 暗号プリミティブ仕様
- 実装
  - 暗号製品実装
  - 暗号プロトコル実装
  - 暗号プリミティブ実装

運用段階のセキュリティ

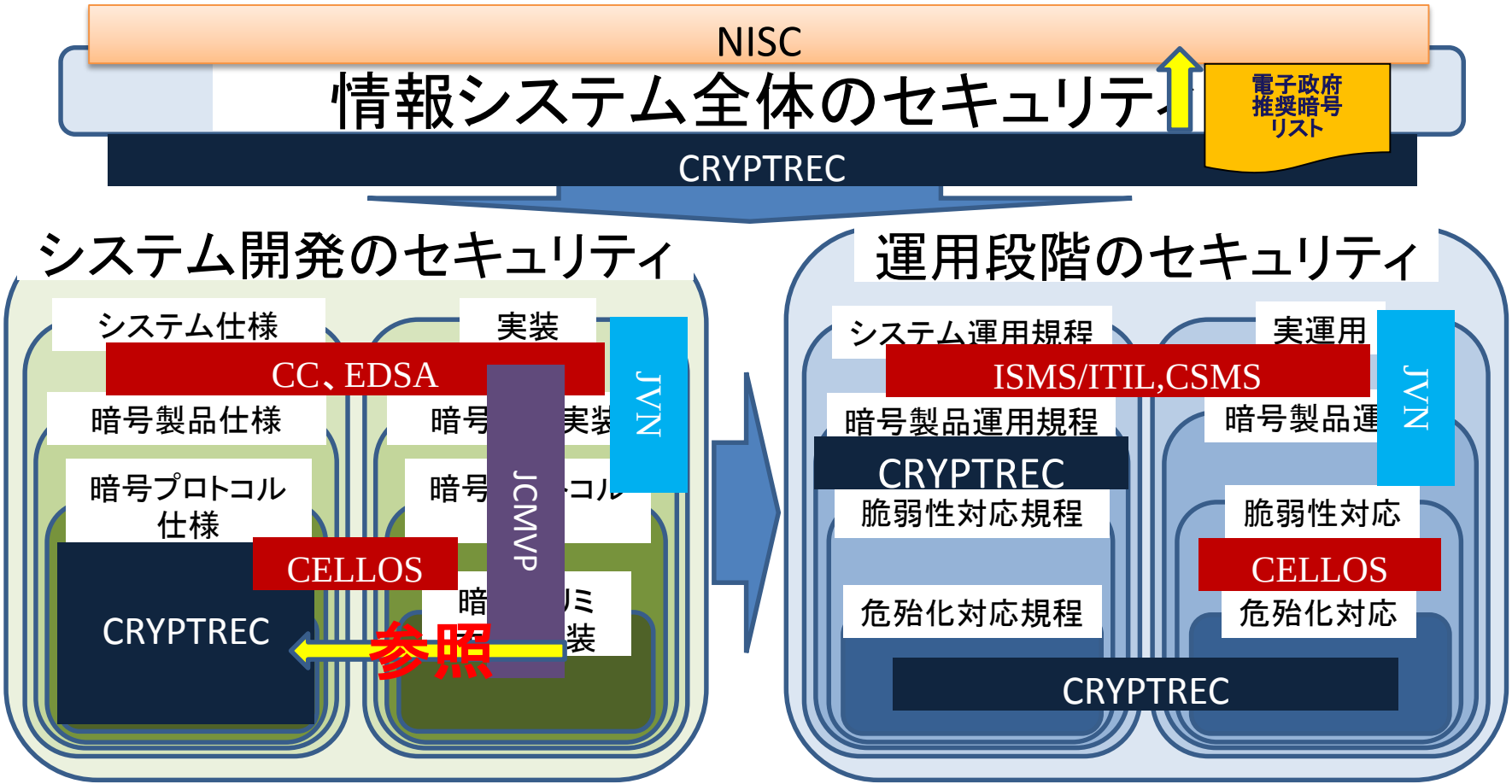
- システム運用規程
  - 暗号製品運用規程
  - 脆弱性対応規程
  - 危殆化対応規程
- 実運用
  - 暗号製品運用
  - 脆弱性対応
  - 危殆化対応

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTRECの在り方に関する検討グループ

＜「政府」システムにおける暗号技術のセキュリティ確保の各役割（現状）＞

- 従前のCRYPTRECは主に、システム開発の暗号プロトコル以下の仕様を念頭に対応
- 運用に関しては、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を提供
- それ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何らかの仕組みあり



CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECの在り方に関する検討グループ

＜目的（ミッション）に関する論点＞

下記の現在のミッションを修正すべきかを検討
「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」

検討の結果、以下の方針が示された。

- 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の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、提言機能のミッション追加を検討

◎新たなミッション案（検討継続中）

「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

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECの在り方に関する検討グループ

＜活動領域に関する論点＞

提示された論点

- CRYPTRECは暗号アルゴリズムのセキュリティ確保について重点を置いて活動してきたが、政府調達において参照されるべき成果物を作成できるか、という観点からCRYPTRECの網羅性に関して、既に活動している暗号プロトコル等も含めた領域についても再検討を行う必要がある。
- その場合、既存の他団体の活動（プロトコルのセキュリティ（CELLOS）、製品（ソフトウェア）の脆弱性（JVN）等）との関係を考慮する必要がある。

既存のCRYPTREC活動領域について

- 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等との連携も視野に入れて、引き続き検討
- 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

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

- 脆弱性対応においてCELLOSと連携するとした場合の具体的フロー検討
- 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

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTRECの在り方に関する検討グループ

＜暗号技術マップのイメージ＞

運用など上位に行くほどCRYPTRECの活動が手薄だったが、今後注力していくべき領域。特に重要となる鍵管理への取組をどうするか？

暗号プロトコルでの新しい成果物を検討するために、政府システムからのインプットが有用ではないか

プロトコルレベルでは
- ISO/IEC等で仕様が規格化されているもの
- IETF RFC等をもとにオープンソース化されたり各社の製品として実装され広く利用されているものがある。

運用方法

暗号利用
応用プロトコル

暗号利用
基礎プロトコル

暗号
プリミティブ

基礎理論

鍵管理　SSL/TLS暗号設定

SSL/TLS　IPsec　DNSSEC

エンティティ認証　ISO/IEC規格　IETF RFC

公開鍵暗号　暗号利用モード　MAC　IDベース暗号 …

共通鍵暗号　ハッシュ関数　軽量暗号

擬似乱数生成系

素因数分解問題　離散対数問題　楕円曲線離散対数問題　格子問題 …

CRYPTREC対応分野

枠線　CRYPTREC暗号リストにある技術分類

下線　CRYPTRECがWGやガイドライン等で扱った技術

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECの在り方に関する検討グループ

＜適用範囲に関する論点＞

提示された論点

電子政府情報システムと一般情報システムについて、電子政府向けの成果物であれば一般向けシステムでも利用可能であることから、それらについて違いを意識する必要はなく、それよりも、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検討する必要がある。

検討の結果、以下の方針が示された。

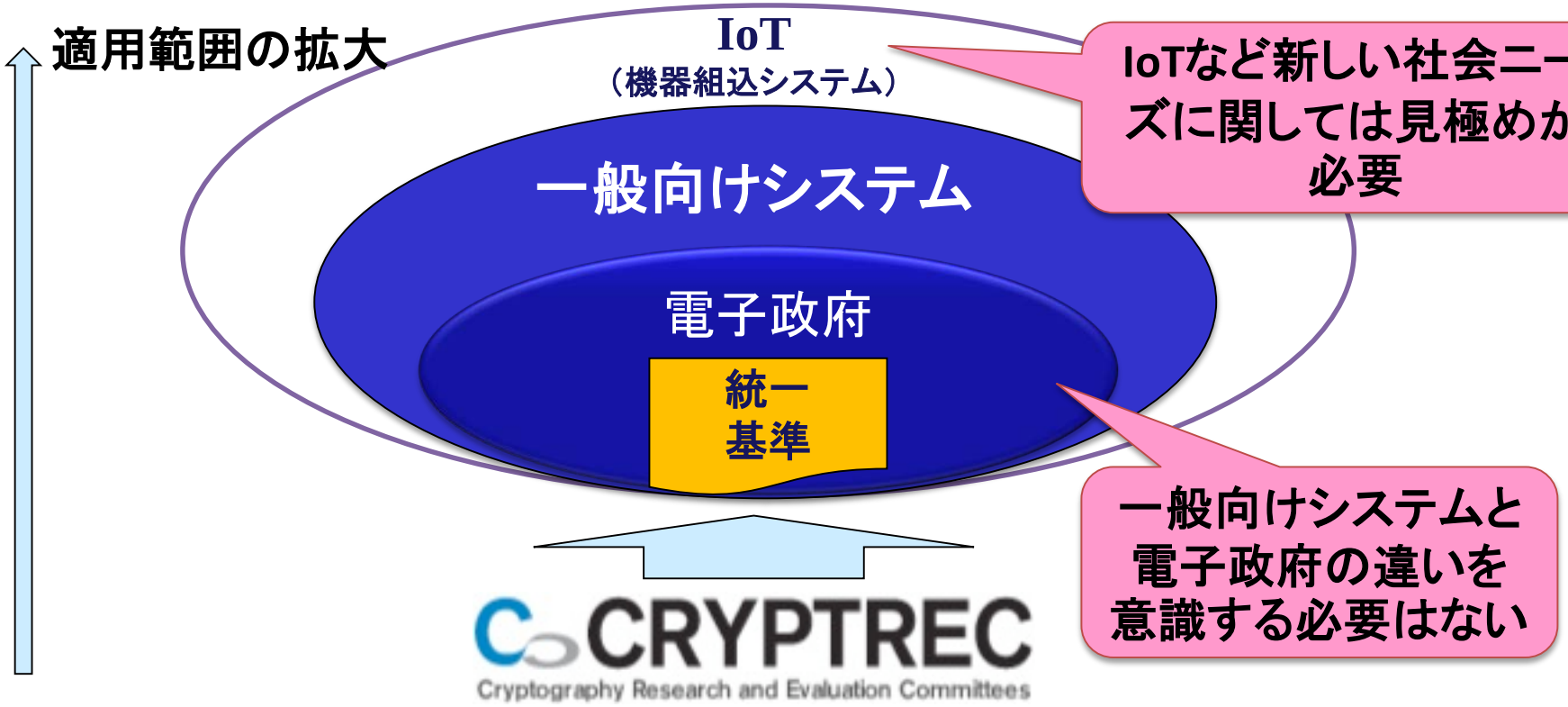
- IoT社会で重要になる軽量暗号等について、CRYPTRECとして更なるアプローチが可能か、検討が必要
- 暗号技術が社会において活用されるために必要な制度・ガイドラインについて検討し、各種制度や法律も視野に入れた議論ができる体制が必要

- 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

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECの在り方に関する検討グループ

＜CRYPTRECの成果の適用範囲のイメージ＞



- 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

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECの在り方に関する検討グループ

＜成果物に関する論点＞

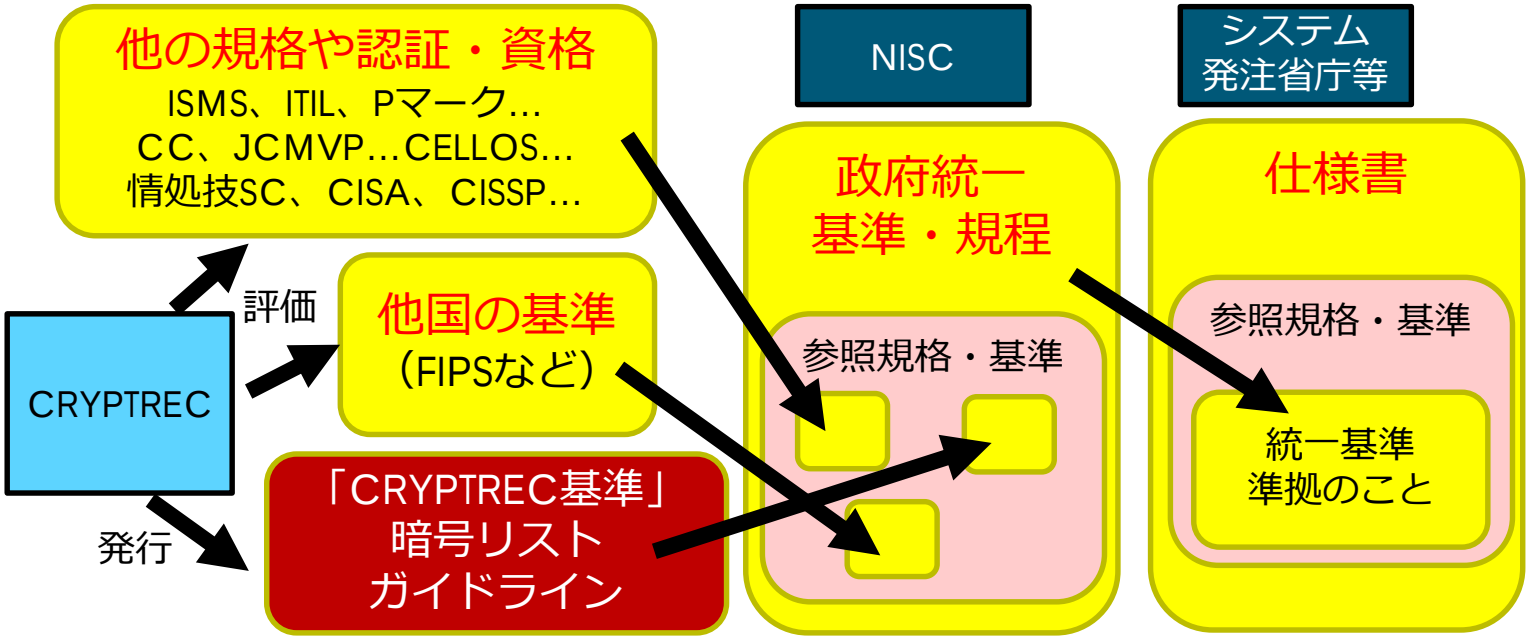
提示された論点
成果物として、まずは電子政府向けでも現状の暗号リスト以外に柱となるべきものがないか検討が必要。

- 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検討
- 適切な情報発信の在り方について引き続き検討

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTRECの在り方に関する検討グループ

＜政府情報システムの調達にとってCRYPTRECに望まれる機能＞



既存ガイドライン類の改善案
- **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**

- 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検討
- 適切な情報発信の在り方について引き続き検討

CRYPTREC
Cryptography Research and Evaluation Committees

2015年度の体制図（検討グループ開催後）

2015年度新設

暗号技術検討会

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

重点課題検討タスクフォース

設置の経緯

「CRYPTRECの在り方に関する検討グループ」での議論の結果、政府統一基準に向けたCRYPTREC成果物の在り方、暗号プロトコルのセキュリティ確保に向けた活動等において、継続的な議論が必要であるとの結論

→暗号技術検討会の下に「重点課題検討タスクフォース」を設置し、これらを継続的に議論することとなった論点や、その他CRYPTRECの方向性を機動的に検討し、トップダウン的な意志決定もできる体制を構築

2015年度の議論概要

2015年度においては3回実施、主な審議事項は以下の4点

- CRYPTREC暗号技術活用委員会の今後の活動
- 暗号アルゴリズムの脆弱性に関する情報発信フロー
- 暗号プロトコルのセキュリティ確保に向けた活動
- CRYPTREC暗号リストの改定の検討　→　暗号技術検討会への報告

CRYPTREC
Cryptography Research and Evaluation Committees

重点課題検討タスクフォース

CRYPTREC暗号技術活用委員会の今後の活動

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

※おおむねこの範囲に拡大

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）

- 暗号技術活用委員会が作成すべき暗号の取扱いに関わる運用ガイドライン対象の検討
- 作成された運用ガイドライン（「SSL/TLS暗号設定ガイドライン」をモデルケース）のメンテナンス方法の検討
- 他組織との連携体制（例：NCCoEのようなもの）の検討

CRYPTREC
Cryptography Research and Evaluation Committees

重点課題検討タスクフォース

＜暗号アルゴリズムの脆弱性に関する情報発信フロー＞

情報分類	速報の必要性	速報公開対象か	過去の事例
A. 暗号アルゴリズムの**完全な危殆化**による緊急対応	高	対象	該当なし (イメージ：世界中で使われている暗号アルゴリズムが PC 1台で1時間で解読可能など)
B. 正確で信頼性の高い情報を発信することによる**過剰反応防止**	中	対象	MISTY1へのintegral attack, SHA-1 free-start collision攻撃など
C. 長期的なシステムの安全性維持のための対策喚起	低	非対象	
D. 対応不要	無	非対象	

速報の対象

CRYPTREC
Cryptography Research and Evaluation Committees

重点課題検討タスクフォース

＜暗号アルゴリズムの脆弱性に関して発信する情報の位置づけ＞

- **速報レポート**
  外部で公開されている情報に基づき記載する
  情報源は信頼に足る機関・組織等とする
  CRYPTRECでは詳細評価していないことを明示する

- **安全性評価報告**
  CRYPTREC として安全性評価を実施する
  CRYPTREC で評価したことを明示する
  公開までの期間 ： 脆弱性の内容に依る

CRYPTREC
Cryptography Research and Evaluation Committees

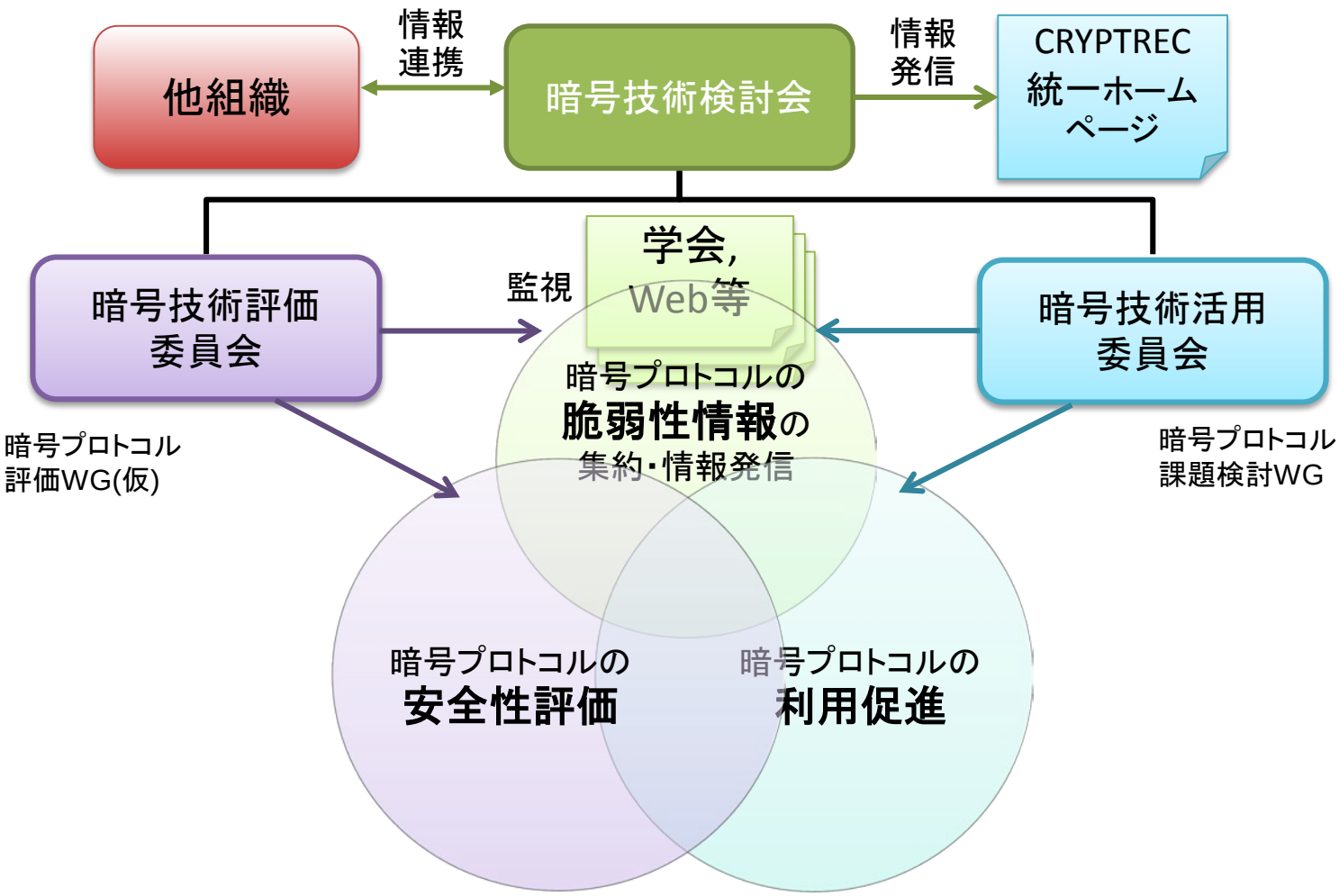
重点課題検討タスクフォース

＜暗号プロトコルのセキュリティ確保に向けた活動＞

CRYPTREC
Cryptography Research and Evaluation Committees

重点課題検討タスクフォース

＜暗号プロトコルに関するCRYPTREC体制案＞



CRYPTREC暗号技術検討会活動内容

第1回暗号技術検討会（１０月５日開催）

- 各委員会からの報告
- 重点課題検討タスクフォースの設置承認

第2回暗号技術検討会（３月２９日開催）

- 各委員会からの報告
- 重点課題検討タスクフォースからの報告
- CRYPTREC暗号リスト改定の審議

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト

電子政府推奨暗号リスト

- ✓ 安全性評価済み技術
- ✓ 市場での利用実績が確認された技術

製品化・利用実績がある ↑

危胎化 ↓

推奨候補暗号リスト

- ✓ 安全性評価済み技術

運用監視暗号リスト

- ✓ 互換性維持のためだけに一時的な利用を許可する技術

CRYPTREC
Cryptography Research and Evaluation Committees

改正の概要

[SHA-2] FIPS 180-4で規定されているハッシュ関数SHA-2のうち、一部のみが電子政府推奨暗号リストに掲載されていた。

FIPS 180-4で規定されているSHA-2　※網掛け部は以前よりリストに掲載

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、SHA-3のコンペティションを開催。結果、Keccak方式が選ばれ、FIPS 202として正式に出版された。

リストに掲載されていなかったSHA-2,SHA-3について評価委員会にて評価、審議

適切な安全性・実装性能を有していると判断（※）

※ハッシュ長が256ビット以上のアルゴリズムのみ

CRYPTREC Cryptography Research and Evaluation Committees

推奨候補暗号リスト（H28.3.29付変更）

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
		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。

CRYPTREC
Cryptography Research and Evaluation Committees

今後の活動予定

- 暗号プロトコルの安全な利用環境の確保など、暗号を取り巻く環境変化に応じた新たなニーズへの対応を検討

  - 重点課題検討タスクフォースによる継続的な議論の実施
    ①文書体系の在り方について
    ②政府統一基準に向けた新たなCRYPTREC成果物
    ③新たな社会ニーズを見据えた新規活動
    ④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

  - 暗号技術評価委員会及び暗号技術活用委員会と連携し暗号プロトコルのセキュリティ確保に係る活動を実施

CRYPTREC
Cryptography Research and Evaluation Committees

2016年度の体制図（予定）

暗号技術検討会

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）や政策提言

（※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。

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

暗号技術調査WG
（暗号解析評価）

暗号技術調査WG
（軽量暗号）

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

暗号プロトコル
課題検討WG
（2016年度新設予定）

（参考）
2015年度　暗号技術検討会　構成員

CRYPTREC
Cryptography Research and Evaluation Committees

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
	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　情報理工学部情報システム学科　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 総合情報学専攻（セキュリティ情報学コース）　教授
	岡本　栄司	国立大学法人筑波大学　大学院システム情報工学研究科　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（社団法人電気通信事業者協会代表兼務）
	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
	佐々木　良一	東京電機大学　未来科学部情報メディア学科　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
	本間　尚文	国立大学法人東北大学　大学院情報科学研究科　准教授
	松井　充	三菱電機株式会社　情報技術総合研究所　情報セキュリティ技術部長
	松浦　幹太	国立大学法人東京大学　生産技術研究所　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　情報技術研究部門　上級主任研究員

（五十音順、敬称略、所属は2015年度末時点もの）

オブザーバ：　内閣サイバーセキュリティセンター、警察庁、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

（参考）
CRYPTRECの在り方に関する検討グループ　構成員

CRYPTREC
Cryptography Research and Evaluation Committees

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

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
総合情報学専攻（セキュリティ情報学コース）　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　　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

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長

（五十音順、敬称略、所属は2015年度末時点もの）

オブザーバ：　内閣サイバーセキュリティセンター

（参考）
重点課題検討タスクフォース　構成員

CRYPTREC
Cryptography Research and Evaluation Committees

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

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
総合情報学専攻（セキュリティ情報学コース）　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　　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長

（五十音順、敬称略、所属は2015年度末時点もの）

オブザーバ：　内閣サイバーセキュリティセンター

（参考）
電子政府推奨暗号リスト

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

（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。

[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。

（参考）
推奨候補暗号リスト

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
		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。

（参考）
運用監視暗号リスト

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

（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）

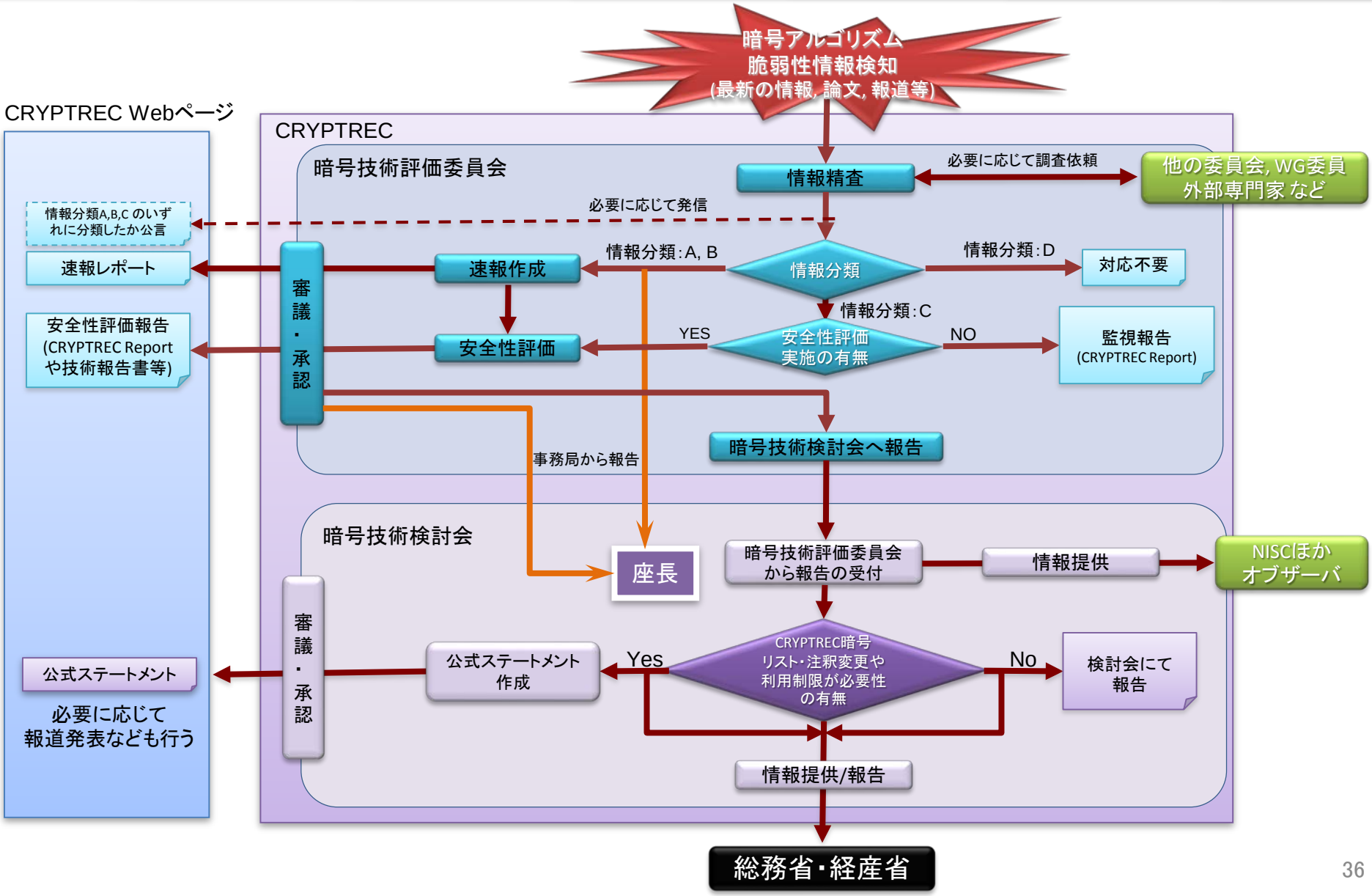
（注9）SSL 3.0 / TLS 1.0, 1.1, 1.2で利用実績があることから当面の利用を認める。

（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。

（参考）
暗号アルゴリズムの脆弱性に関する情報発信フロー図



CRYPTRECの詳細はこちら

■CRYPTRECホームページ

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

■CRYPTREC暗号リスト（平成28年3月29日版）

http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf

CRYPTREC
Cryptography Research and Evaluation Committees