CRYPTREC活動紹介

暗号技術検討会事務局
（総務省情報セキュリティ対策室課長補佐）
筒井　邦弘

CRYPTRECとは？

- Cryptography Research and Evaluation Committees
  - 総務省・経済産業省・NICT・IPAが共同で開催する暗号評価プロジェクト。
  - 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検討体制(FY2013から）

CRYPTREC体制図

暗号技術検討会
（事務局：総務省、経済産業省）

暗号技術評価委員会
（事務局：NICT, IPA）

（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

- 暗号解析評価WG
- 軽量暗号WG

暗号技術活用委員会
（事務局：NICT, IPA）

（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の検討

- 運用ガイドラインWG
- 標準化推進WG

暗号技術検討会の目的・検討事項

- 暗号技術検討会の目的
  - 総務省政策統括官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。（構成員は次スライドの通り）

- 暗号技術検討会の検討事項
  （1）CRYPTREC暗号リスト掲載暗号技術の監視
  （2）CRYPTREC暗号リスト掲載暗号技術の安全性及び信頼性確保のための調査・検討
  （3）CRYPTREC暗号リストの改定に関する調査・検討
  （4）CRYPTREC暗号リスト掲載暗号技術の普及促進及び暗号技術の利用促進・産業化に向けた取組の検討
  （5）その他、暗号技術の評価及び利用に関すること

CRYPTREC
Cryptography Research and Evaluation Committees

2014年度　暗号技術検討会　構成員

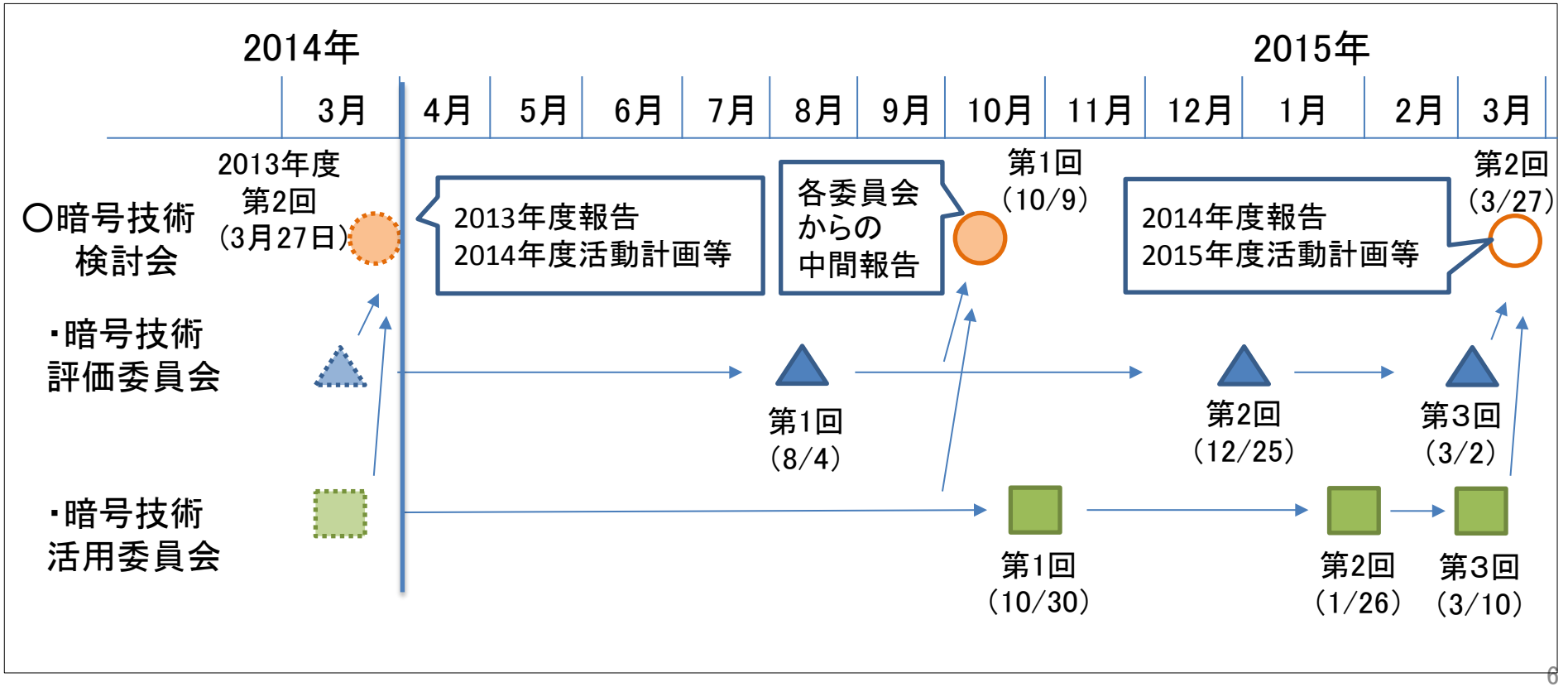
座長	今井　秀樹	東京大学　名誉教授
	今井　正道	一般社団法人情報通信ネットワーク産業協会　常務理事
	上原　哲太郎	立命館大学　情報理工学部情報システム学科　教授
	太田　和夫	電気通信大学大学院　情報理工学研究科 総合情報学専攻（セキュリティ情報学コース）　教授
	岡本　栄司	筑波大学大学院　システム情報工学研究科　教授
	岡本　龍明	日本電信電話株式会社　セキュアプラットフォーム研究所　岡本特別研究室　室長 （社団法人電気通信事業者協会代表兼務）
	金子　敏信	東京理科大学　理工学部電気電子情報工学科　教授
	国分　明男	一般財団法人ニューメディア開発協会　顧問・首席研究員
	佐々木　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））
	中山　靖司	日本銀行　金融研究所情報技術研究センター　企画役
	本間　尚文	東北大学大学院　情報科学研究科　情報基礎科学専攻　准教授
	松井　　充	三菱電機株式会社　情報技術総合研究所　技師長
	松尾　真一郎	独立行政法人情報通信研究機構　社会還元促進部門　統括 （ISO/IEC JTC1 SC27/WG2（国内小委員会主査））
	松本　　勉	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	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
	渡辺　　創	ISO/IEC JTC1 SC27　国内委員会　委員長

オブザーバ：　内閣官房情報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

2014年度　暗号技術検討会活動概要

暗号技術検討会の関連委員会（暗号技術評価委員会及び暗号技術活用委員会）の活動報告（各WG活動含む）を中心に、今年度は2回の暗号技術検討会を開催

CRYPTREC（暗号技術検討会及び関連委員会）の開催概要



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（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

- ✓ 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

危殆化

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

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（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。

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（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		該当なし
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。

[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。

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（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）128-bit RC4は、SSL（TLS 1.0以上）に限定して利用すること。

（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。

“暗号”を取り巻く近年の動向

- ✓ 攻撃手法の進歩
- ✓ マイナンバー制度の開始
- ✓ サイバーセキュリティ基本法の成立

攻撃手法の進歩

日々、サイバー攻撃は進歩

- RC4に対する攻撃 ・・・・ RC4の注釈変更を審議
- Dual_EC_DRBG への懸念 ・・・・ 注意喚起を実施（2013年11月6日）
- BEAST攻撃 etc.,

計算機の演算能力も着実に向上

CRYPTREC暗号リストの維持・管理が重要

マイナンバー制度の開始

2015年10月より開始予定

政府・地方自治体等のシステム構築が進められている

- 中央官庁の他、全国約1800の地方自治体のシステムも更改
- 初期費用だけでも2700億円規模
- 関連需要は全国で3兆円に上るという試算※1

※1　大和証券試算

電子政府における、より一層のセキュリティ対策が求められる

サイバーセキュリティ基本法の成立

2014年11月6日、サイバーセキュリティ基本法が成立

目的

- 急増するサイバー攻撃への対応
- 通信、電力等の重要インフラの保護
- 2020年の東京オリンピックに向けたサイバーセキュリティ強化

内容

- 基本理念、国・事業者等の責務に関する規定（第1章）
- サイバーセキュリティ戦略の策定（第2章）
- サイバーセキュリティに関する基本施策（第3章）
- サイバーセキュリティ戦略本部の設置（第4章）　等

政府におけるサイバーセキュリティ対策のより一層の推進

“暗号”を取り巻く動向を受けて

- ✓ 攻撃手法の進歩
- ✓ マイナンバー制度の開始
- ✓ サイバーセキュリティ基本法の成立

CRYPTRECの活動の重要性は、
今後ますます大きくなっていく

ご清聴有り難うございました。

CRYPTREC
Cryptography Research and Evaluation Committees