CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会活動報告

2023年7月26日

暗号技術検討会 座長
横浜国立大学　教授　松本　勉

目次

1. CRYPTRECの概要

- CRYPTRECとは
- CRYPTREC活動体制（2022年度）
- 暗号技術検討会構成員
- 暗号技術検討会等の開催状況

2. 暗号技術検討会の活動概要

- CRYPTREC暗号リストの概要
- CRYPTREC暗号リスト移行ルール
- 公募提案暗号の自主取下げルールの策定及びリスト改定
- CRYPTREC暗号リストの大規模改定
- CRYPTREC暗号リスト改定版の策定 (2023年3月30日初版)
- ガイドライン類の策定（暗号技術評価委員会）
- ガイドライン類の策定（暗号技術活用委員会）

1.CRYPTRECの概要

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTRECとは

CRYPTography **R**esearch and **E**valuation **C**ommittees

CRYPTRECの概要

■ デジタル庁・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（2022年度）

暗号技術検討会 （事務局：デジタル庁、総務省、経済産業省）

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

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

- 暗号技術調査WG（耐量子計算機暗号）（2021年6月～）
- 暗号技術調査WG（高機能暗号）（2021年6月～）

暗号技術活用委員会 （事務局：IPA、NICT）

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

- 暗号鍵管理ガイダンスWG（2021年6月～）

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会構成員

座長	松本 勉	横浜国立大学 教授
構成員	阿部 正幸	日本電信電話株式会社　フェロー
	石井 義則	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 教授
	田村 裕子	日本銀行 金融研究所 企画役
	太田 和夫	電気通信大学 名誉教授
	高木 剛	東京大学 教授
	近澤 武	三菱電機株式会社 担当部長
	手塚 悟	慶應義塾大学 教授
	本間 尚文	東北大学 教授
	松井 充	三菱電機株式会社 主席技監
	松浦 幹太	東京大学 教授
	松本 泰	セコム株式会社 顧問
	向山 友也	一般社団法人テレコムサービス協会 技術・サービス委員長
	渡邊 創	国立研究開発法人産業技術総合研究所 副研究センター長
	吉田 博隆	国立研究開発法人産業技術総合研究所 研究チーム長

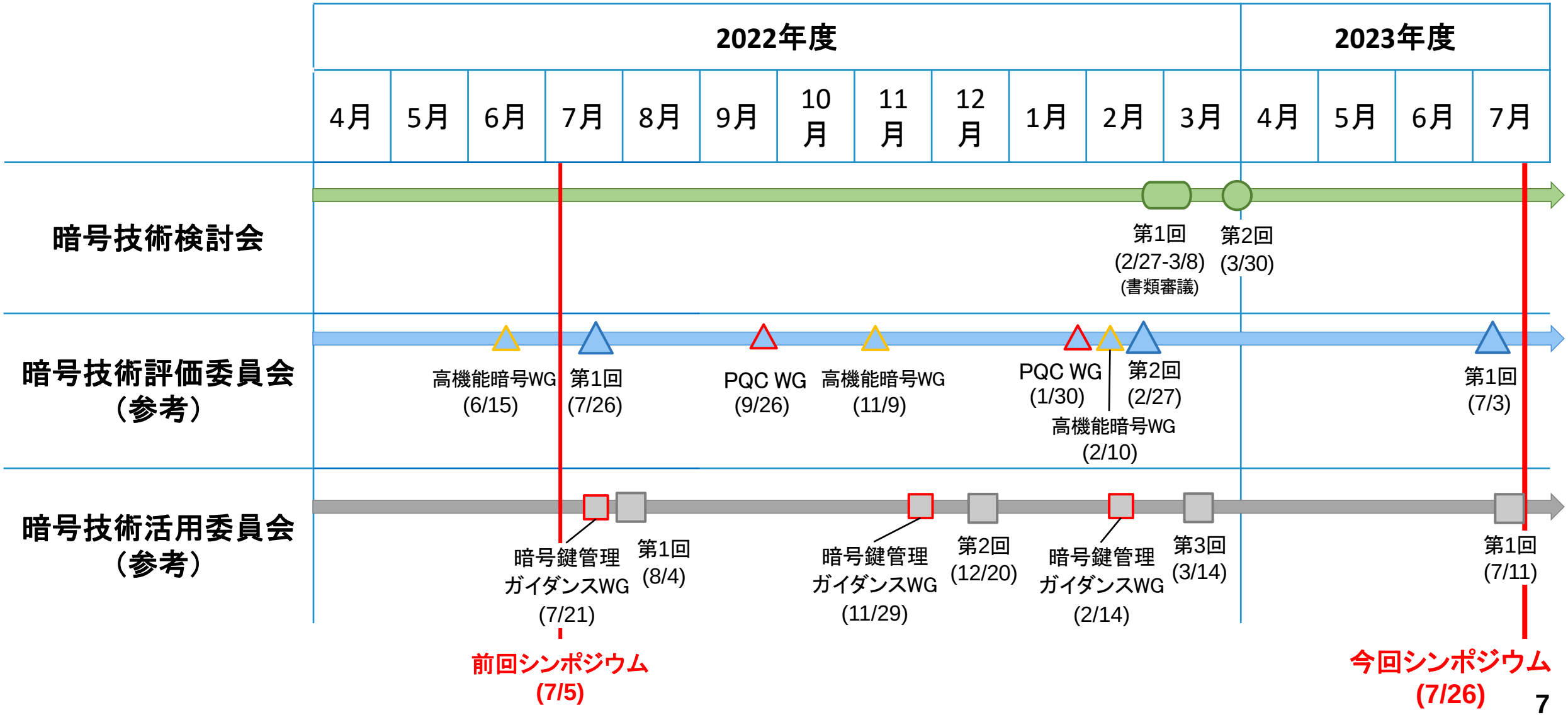
（五十音順、敬称略、所属は2023年6月末時点のもの）

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

事務局：デジタル庁、総務省、経済産業省

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会等の開催状況



2.暗号技術検討会の活動概要

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの概要

- CRYPTRECの活動を通して**安全性・実装性能等が確認された暗号技術**について、デジタル庁、総務省及び経済産業省において**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。
- CRYPTREC暗号リストは以下の**3リスト**により構成される。（注：現在の3リスト構成は2013年より）

①電子政府推奨暗号リスト

安全性及び実装性能が確認された暗号技術で、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、利用を推奨するもののリスト

②推奨候補暗号リスト

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のリスト

③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と確認されたが、互換性維持のために継続利用を容認する暗号技術のリスト。

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト移行ルール

次の条件のいずれかを満たすと暗号技術検討会が決定した場合
1. 5年ごとの利用実績調査により、複数の利用実績を確認した場合
2. その他、普及していることが明らか又は急速な普及が大いに見込まれる場合

①電子政府推奨暗号リスト

安全性維持が困難（危殆化した）と暗号技術検討会が決定した場合

※電子政府推奨暗号リストに掲載された暗号技術は、利用者がいる前提であり、原則として、危殆化以外の理由では遷移させず、また、移行のための時間を確保する必要があるため、いきなりリストから削除することはしない。

標準化等により将来的な利用が見込まれ、安全性や実装性能が十分にあると暗号技術検討会が決定した場合（公募や事務局提案等）

②推奨候補暗号リスト

- CRYPTREC暗号リストへの掲載から20年を超えた後に実施する最初の利用実績調査までに、十分な利用実績を確認できなかったもの

新たに策定

- **公募提案暗号について、提案会社より自主取下げ要望があり、暗号技術検討会における審議の結果「今後の普及が見込まれない公募提案暗号」であると判断されたもの**

※利用実績調査の具体的な実施内容・評価基準は、暗号技術活用委員会において検討し、暗号技術検討会の承認を経た上で実施する。

安全性維持が困難（危殆化した）と判断した場合

③運用監視暗号リスト

（2019年度暗号技術検討会　決定事項）

次の条件のいずれかを満たすと暗号技術検討会が決定した場合、削除猶予期間を定めて周知を行った上で、その期間の満了後に自動的に削除する。
1. 運用監視暗号リストに掲載している注釈で示した互換性維持のための利用形態が必要なくなり、削除が妥当と判断した場合
2. 互換性維持の継続利用として使うにしても安全性維持が極めて困難で、互換性維持の継続利用が容認できないと判断した場合
3. その他、運用監視暗号リストに掲載している必要性の根拠を満たさなくなったと判断した場合

リストから削除

CRYPTREC
Cryptography Research and Evaluation Committees

公募提案暗号の自主取下げルールの策定及びリスト改定

■ 公募提案暗号の自主取下げ要望が提案会社よりあったが、これの取り扱いの規定が存在しなかったため、暗号技術検討会において新たにルールを策定。

① 取下げ申請の承認は「推奨候補暗号リスト」に掲載されている自社の公募提案暗号のうち「今後の普及が見込めない公募提案暗号」であると判断されるものに限る。

② 「電子政府推奨暗号リスト」及び「運用監視暗号リスト」に掲載されている公募提案暗号については既に「普及している公募提案暗号」として扱い、取下げ申請は却下する。

③ ただし、前2項の基準にかかわらず、知的財産権の無償譲渡や利用状況（今後の見込みを含む）などにより、当該暗号技術のCRYPTREC暗号リストへの掲載に伴う対応をCRYPTREC事務局が自主的に管理すべきであると判断される場合は、取下げ申請を受けて、公募提案暗号から事務局提案暗号に位置づけを変更する。

■ 提案会社より自主取下げの要望があった「ECDSA、ECDH及びSC2000」について、新たに策定したルールに基づき対応を実施。

- 「ECDSA」「ECDH」については、③によりCRYPTREC暗号リストへの掲載を継続。
- 「SC2000」については、①によりCRYPTREC暗号リストからの削除を実施。

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの大規模改定

■ **2023年3月**に、**10年ぶり**となる**CRYPTREC暗号リストの大規模改定を実施**

●「推奨候補暗号リスト」に掲載されている暗号技術の内、「製品化・利用実績がある」と認められた暗号技術10件が電子政府推奨暗号リスト掲載に昇格した。

暗号技術	技術分類
EdDSA	公開鍵暗号-署名
SHA-512/256	ハッシュ関数
SHA3-256	ハッシュ関数
SHA3-384	ハッシュ関数
SHA3-512	ハッシュ関数
SHAKE128	ハッシュ関数
SHAKE256	ハッシュ関数
XTS	暗号利用モード-秘匿モード
ChaCha20-Poly1305	認証暗号
ISO/IEC 9798-4	エンティティ認証

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト改定版の策定 (2023年3月30日初版)

電子政府推奨暗号リスト

第7版（更新日：2022年3月30日）

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH
共通鍵暗号	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
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

推奨候補暗号リスト

第7版（更新日：2022年3月30日）

技術分類		名称
公開鍵暗号	署名	EdDSA
	守秘	該当なし
	鍵共有	PSEC-KEM
共通鍵暗号	64ビットブロック暗号	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
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128
		SHAKE256
暗号利用モード	秘匿モード	XTS
	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
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

自主取下げを承認

運用監視暗号リスト

第7版（更新日：2022年3月30日）

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号	3-key Triple DES
	128ビットブロック暗号	該当なし
	ストリーム暗号	該当なし
ハッシュ関数		RIPEMD-160
		SHA-1
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
認証暗号		該当なし
エンティティ認証		該当なし

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト改定版の策定 (2023年3月30日初版)

電子政府推奨暗号リスト

(令和5年3月30日 デジタル庁、総務省、経済産業省共同発表)

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		EdDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH
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	AES
		Camellia
	ストリーム 暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128
		SHAKE256

技術分類		名称
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
		XTS
	認証付き秘匿モード	CCM
		GCM
メッセージ認証コード		CMAC
		HMAC
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

推奨候補暗号リスト

(令和5年3月30日 デジタル庁、総務省、経済産業省共同発表)

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
共通鍵暗号	64ビットブロック暗号	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01
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
認証暗号		該当なし
エンティティ認証		該当なし

運用監視暗号リスト

(令和5年3月30日 デジタル庁、総務省、経済産業省共同発表)

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号	3-key Triple DES
	128ビットブロック暗号	該当なし
	ストリーム暗号	該当なし
ハッシュ関数		RIPEMD-160
		SHA-1
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
認証暗号		該当なし
エンティティ認証		該当なし

CRYPTREC
Cryptography Research and Evaluation Committees

ガイドライン類の策定（暗号技術評価委員会）

■ 耐量子計算機暗号ガイドライン

- 量子コンピュータの実用化によって公開鍵暗号方式の安全性が低下することを踏まえ、耐量子計算機暗号（以下PQC）に関する調査結果をまとめたもの。
- PQCについて、用途別の利用形態や、量子コンピュータの脅威・データ保護期間を踏まえた課題とその対策について紹介。また、世界的に使用が見込まれる代表的なPQCの方式について紹介。
- 対象：一般的な読者・暗号初学者～暗号技術に携わる研究者・技術者

■ 高機能暗号ガイドライン

- 高機能で高効率であり、様々な用途での利用が期待されている高機能暗号の利用を促進するために、高機能暗号の方式及びユースケース等を調査した結果をまとめたもの。
- 高機能暗号について、ユースケースや従来の暗号方式と比較した際のメリット、運用時の注意点等を具体的に示す。
- 対象：暗号技術を活用する技術者

CRYPTREC
Cryptography Research and Evaluation Committees

ガイドライン類の策定（暗号技術活用委員会）

■ 暗号鍵管理ガイダンス

- 暗号鍵管理が必要なシステムの設計者向けに、暗号鍵管理の設計で明記する事項や考慮する点などを解説することを目的としたガイダンス。
- 2020年に発行した「暗号鍵管理システム設計指針（基本編）」を詳しく解説。また、暗号鍵管理で必要になる項目について、シンプルなモデルを例示して説明。
- 対象：暗号鍵管理機能を持つシステム設計者

https://www.cryptrec.go.jp/