CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会活動報告

2022年7月5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（2019年度～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

- 量子コンピュータ時代に向けた暗号の在り方の検討
- （参考）量子コンピュータ時代に向けた暗号の在り方検討タスクフォース
- タスクフォースの検討結果（量子コンピュータ等関係、CRYPTREC暗号リスト関係）
- CRYPTREC暗号リストの更新に関する決定
- CRYPTREC暗号リスト移行ルール
- CRYPTREC暗号リストの更新（2019年度～2021年度）
- （参考）CRYPTREC暗号リストの更新（2013年度～2021年度）

参考　CRYPTREC暗号リスト

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（2019年度～2022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

量子コンピュータ時代に向けた暗号の在り方検討タスクフォース
（2019年6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（暗号解析評価）
（～2021年2月）

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

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

TLS暗号設定ガイドラインWG
（2019年6月～2020年6月）

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

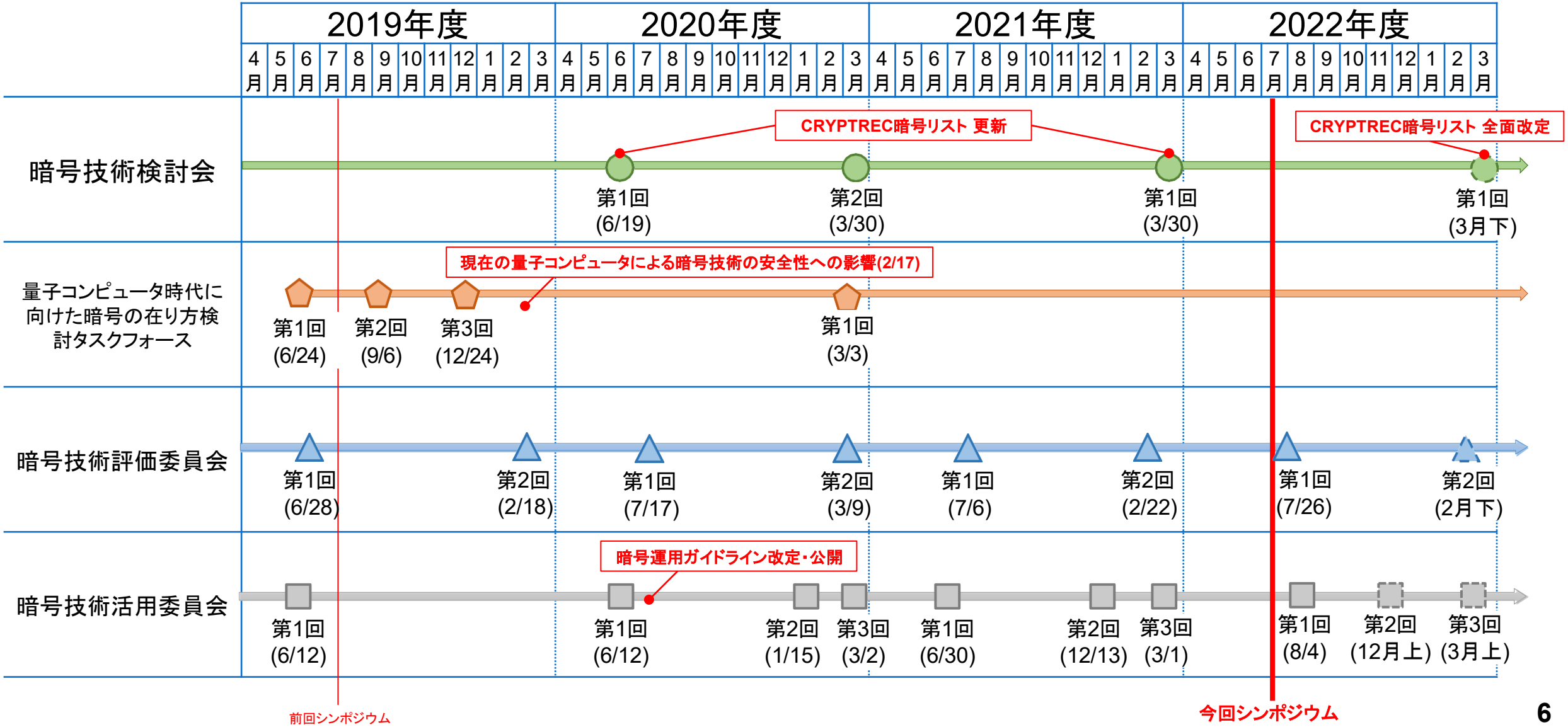
座長	松本 勉	横浜国立大学 教授
構成員	阿部 正幸	日本電信電話株式会社　フェロー
	石井 義則	一般社団法人情報通信ネットワーク産業協会 常務理事
	上原 哲太郎	立命館大学 教授
	田村 裕子	日本銀行 金融研究所 企画役
	太田 和夫	電気通信大学 名誉教授
	高木 剛	東京大学 教授
	近澤 武	三菱電機株式会社 担当部長
	手塚 悟	慶應義塾大学 教授
	本間 尚文	東北大学 教授
	松井 充	三菱電機株式会社 役員技監
	松浦 幹太	東京大学 教授
	松本 泰	セコム株式会社 マネージャー
	向山 友也	一般社団法人テレコムサービス協会 技術・サービス委員長
	吉田 博隆	国立研究開発法人産業技術総合研究所 研究チーム長
	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

（五十音順、敬称略、所属は2022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

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会等の開催状況



CRYPTREC Cryptography Research and Evaluation Committees

量子コンピュータ時代に向けた暗号の在り方の検討

- 量子コンピュータが実現したとしても、解読が困難とされる耐量子計算機暗号の研究開発・標準化が各国で進展。
  大規模な量子コンピュータの出現に向けて、我が国においても耐量子計算機暗号について議論を行う必要性が高まっている。
- 上述の背景を踏まえ、CRYPTRECの暗号技術検討会の下に「**量子コンピュータ時代に向けた暗号の在り方検討タスクフォース**」を設置し、量子コンピュータ時代の推奨暗号の在り方について検討（2019年6月～）。

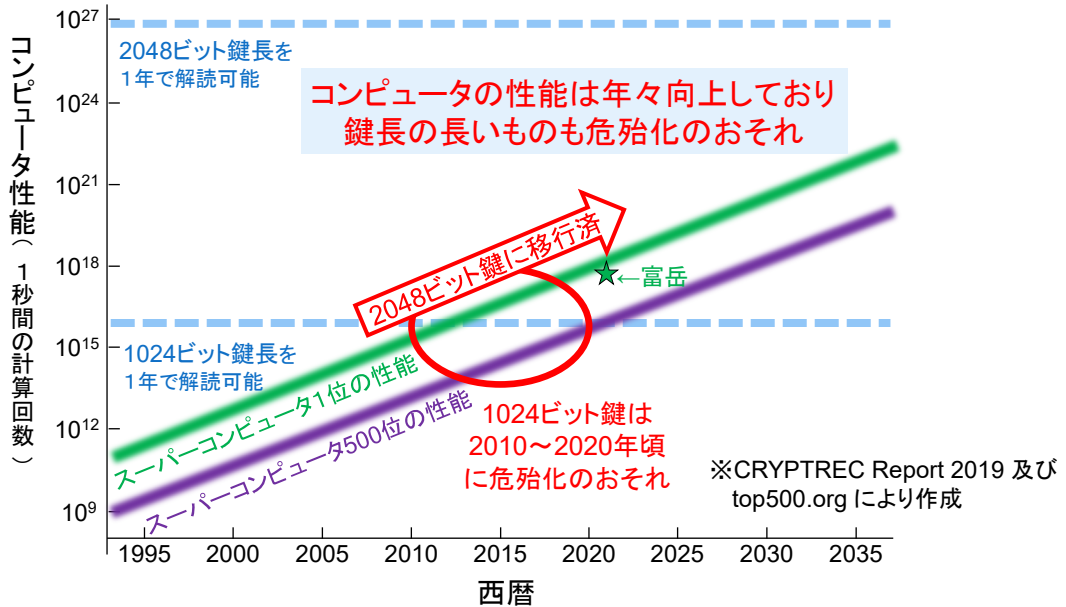
  ＜検討事項＞
  1. 大規模な量子コンピュータの動向を踏まえた次期CRYPTREC暗号リストに求められる要件等の検討
  2. その他新たな暗号技術の動向等（軽量暗号や秘密計算に利用される準同型暗号等）を踏まえた検討等

検討の背景

- ✓ 遠くない将来に現在の公開鍵暗号（RSA暗号や楕円曲線暗号）が容易に解読されるおそれ
- ✓ 大規模システムの改修・更改には10年以上を要する

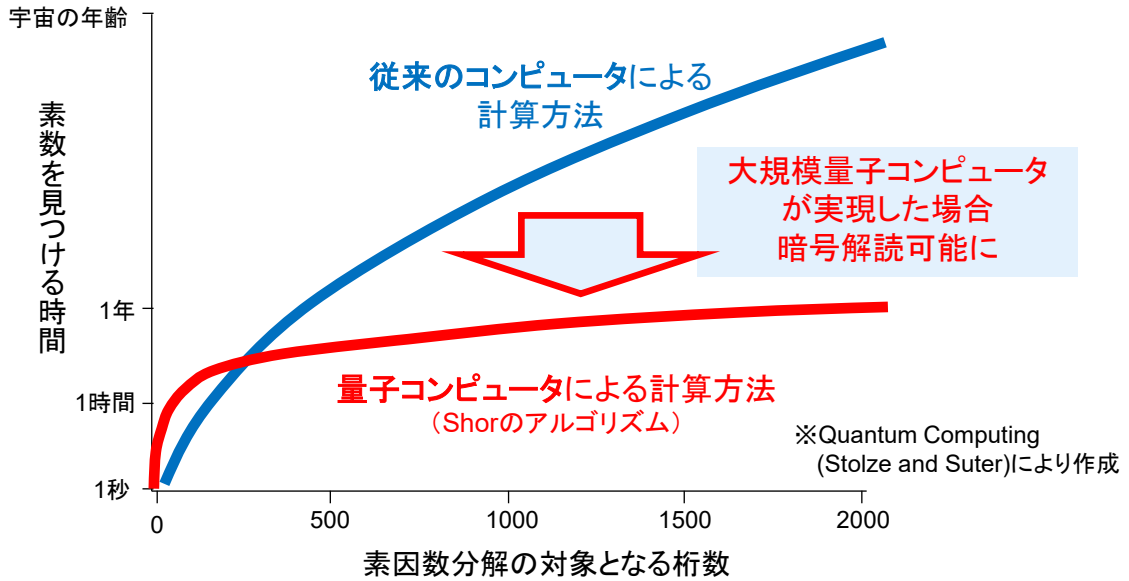
※RSA暗号：大きな桁数の素因数分解は困難なことを安全性の根拠とした公開鍵暗号

従来のコンピュータの性能向上による影響　例：RSA暗号の安全性評価



※CRYPTREC Report 2019 及び top500.org により作成

実用的な量子コンピュータによる影響　例：RSA暗号の安全性評価



※Quantum Computing (Stolze and Suter)により作成

CRYPTREC Cryptography Research and Evaluation Committees

（参考）量子コンピュータ時代に向けた暗号の在り方タスクフォース

（構成員） （令和3年3月末時点）

	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
	國廣 昇	筑波大学システム情報系教授
	高木 剛	東京大学大学院情報理工学系研究科教授
	松井 充	三菱電機株式会社開発本部役員技監
（座長）	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
	満塩 尚史	内閣官房情報通信技術(IT)総合戦略室政府CIO補佐官

（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事務局、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、警察大学校、国立研究開発法人産業技術総合研究所

（事務局）

総務省、経済産業省、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

（開催概要）

2019年度 第１回　令和元年６月24日 ①量子コンピュータの動向について、②耐量子計算機暗号の動向について

第２回　令和元年９月６日 ①CRYPTREC暗号リストにおける耐量子計算機暗号の扱いについて、②軽量暗号の動向について、③CRYPTREC暗号リストにおける軽量暗号等の扱いについて

第３回　令和元年12月24日 CRYPTREC暗号リストに関する論点等について

2020年度 第１回　令和３年３月３日 ①量子コンピュータに関する動向等について、②量子コンピュータに対する暗号技術の動向等について③CRYPTREC暗号リストでの推奨候補暗号リストの取扱いについて

CRYPTREC Cryptography Research and Evaluation Committees

タスクフォースの検討結果（量子コンピュータ等関係）

量子コンピュータ等の技術動向

- ✓ 量子コンピュータの**現状の規模（量子ビット数）は50程度**だが、**暗号解読には数千程度以上**が必要。
- ✓ 量子コンピュータの性能は、量子ビット数に加えて、**ノイズ（計算誤り）**や**演算可能回数**も重要な指標。
- ✓ 現状は**ノイズ（誤り）等の問題があり**、規模だけ拡大しても**暗号解読に活用できる水準**ではない。

→ **現状の暗号技術が近い将来に危殆化する可能性は低い**旨、2020年２月に公表・周知した。
https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html

耐量子計算機暗号（PQC）の技術動向

- ✓ 米国NIST（国立標準技術研究所）が標準化作業中で、2022～2024年に標準化ドラフトが策定予定。

CRYPTREC暗号リスト（電子政府推奨暗号リスト）における位置付けについて

- ✓ **CRYPTREC暗号リスト**は、利用環境によらない安全性の評価に加え、**利用実績等も考慮**して作成。
- ✓ **PQC**は、**多数の方式が提案**され安全性を検討している段階で、利用実績等に言及できる段階ではない。
- ✓ 今後、利用が拡大すると想定される、IoT機器等に用いられる「**軽量暗号**」や、暗号状態で情報処理が可能な「**高機能暗号**」は、**利用環境やアプリケーションが限定**され、従来暗号とは取り扱いが異なる。

→ **PQC、軽量暗号、高機能暗号**は、CRYPTREC暗号リストに組み込まず、**別途ガイドライン**を作成する。
（暗号技術評価委員会にて、CRYPTREC暗号リストの改定作業（2022年度末目途）と並行して実施予定）

タスクフォースの今後の取組

- ✓ **量子コンピュータやPQCの状況をフォロー**するため、2020年度以降も**タスクフォースを継続して開催**。

CRYPTREC Cryptography Research and Evaluation Committees

タスクフォースの検討結果（CRYPTREC暗号リスト関係）

CRYPTREC暗号リストの構成

✓ CRYPTREC暗号リストについて、次の**3リスト構成は維持**し、リスト間の**遷移ルールを明確化**。

①電子政府推奨暗号リスト（安全性・実装性能が確認され、利用実績や普及見込みがあると判断されたもの）
②推奨候補暗号リスト（安全性・実装性能が確認され、今後①のリストに掲載される可能性のあるもの）
③運用監視暗号リスト（危殆化等により推奨すべき状態ではなく、互換性維持のために継続利用を容認するもの）

✓ 各暗号技術は十分成熟しているため、技術分類※は変更せず、新たな暗号技術の公募も実施しない。
※7分類：公開鍵暗号／共通鍵暗号／ハッシュ関数／暗号利用モード／メッセージ認証コード／認証暗号／エンティティ認証

暗号技術のパラメータ

✓ CRYPTREC暗号リストでは推奨する暗号技術（暗号アルゴリズム）を示してきたが、パラメータは提示していない。
✓ 推奨パラメータの明示は、安全なシステム構築や計画的な暗号技術の移行を促進するために有用。
→ **推奨パラメータを規定する別の文書を新たに作成**。（CRYPTREC暗号リストから当該文書を参照する構成とする。）
（暗号技術活用委員会にて作成に向けた検討を実施し、**「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」**を策定。）

CRYPTREC暗号リストの今後の改定

✓ 2003年に作成、2013年に改定を行い、**今般、2023年目途に改定作業中**であり、10年単位で改定。
✓ 常に危殆化等の監視を行い、必要に応じた暗号技術の加除等も行っており、10年単位とする必要もない。
→ 次の改定以後は、改定後5年以内を目途に暗号技術検討会において改定是非を判断することとする。

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの更新に関する決定

■ 暗号技術評価委員会、暗号技術活用委員会の活動報告を受けて、CRYPTREC暗号リストを以下のとおり更新することを決定。

＜2020年度＞

推奨候補暗号リストにXTSを追加**（技術分類：暗号利用モード　秘匿モード）**

✓ 暗号技術評価委員会にて実施した安全性評価（2018年度）、実装性能評価（2019年度）の結果に基づき、注釈として（条件1）、（条件2）を付与した上での追加の提案を受け、追加。
（条件1）利用用途はNIST SP800-38E の規格に沿ったストレージデバイスの暗号化に限る。
（条件2）XTS 内のブロック暗号には、CRYPTREC暗号リスト掲載128 ビットブロック暗号を使う。

運用監視暗号リストからの削除ルールの策定

運用監視暗号リストから128-bit RC4を削除（技術分類：共通鍵暗号　ストリーム暗号）

✓ 暗号技術活用委員会にて新たに作成した「TLS 暗号設定ガイドライン Ver3.0」で、RC4がTLSでの利用禁止暗号アルゴリズムに指定され、注釈が想定している例外的な利用形態そのものが存在しなくなるため、削除が妥当と判断し、令和3年3月31日に削除。

＜2021年度＞

推奨候補暗号リストにEdDSAを追加（技術分類：公開鍵暗号　署名）

✓ 暗号技術評価委員会にて実施した安全性評価（2020年度）、実装性能評価（2021年度）の結果に基づく追加の提案を受け、追加。

各暗号リストの本文に「暗号強度要件に関する設定基準」を参照する旨を追記

✓ 暗号技術活用委員会にて作成した「暗号強度要件に関する設定基準」を踏まえ、電子政府推奨暗号リスト・推奨候補暗号リスト・運用監視暗号リストのそれぞれにおいて参照することを追記。

運用監視暗号リストの本文に脚注を追加

✓ 「互換性維持」の脚注に、「既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること」との旨を追加。

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト移行ルール

①電子政府推奨暗号リスト

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

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

③運用監視暗号リスト

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

安全性維持が困難(危殆化した)と判断した場合

（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

※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。

リストから削除

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの更新（2019年度～2021年度）

電子政府推奨暗号リスト

(平成25年3月1日 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
		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

(平成25年3月1日 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	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

運用監視暗号リスト

(平成25年3月1日 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	~~128-bit RC4~~
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

2021年3月削除（オレンジ）

2022年4月追加（緑色）

2020年7月追加（青色）

CRYPTREC Cryptography Research and Evaluation Committees

（参考）CRYPTREC暗号リストの更新（2013年度～2021年度）

電子政府推奨暗号リスト
(平成25年3月1日 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
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5
	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	~~3-key Triple DES~~
	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
(平成25年3月1日 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	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

運用監視暗号リスト
(平成25年3月1日 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	~~128-bit RC4~~
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

2018年3月降格（桃色）

2021年3月削除（オレンジ）

2016年3月追加（黄色）

2022年4月追加（黄緑色）

2017年3月追加（緑色）

2018年3月追加（水色）

2020年7月追加（青色）

CRYPTREC Cryptography Research and Evaluation Committees

（参考）電子政府推奨暗号リスト

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	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(注13)	CCM
		GCM(注4)
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

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。

なお、利用する鍵長について、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[5]の規定に合致しない鍵長を用いた場合には、電子政府推奨暗号リストの暗号技術を利用しているとは見なされないことに留意すること。

[1] デジタル庁統括官、総務省サイバーセキュリティ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、デジタル庁、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。

[5] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

（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4）初期化ベクトル長は96ビットを推奨する。

（注13）CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

（出典）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)より抜粋
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf

（参考）推奨候補暗号リスト

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(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	XTS(注17)
	認証付き秘匿モード(注14)	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

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。

なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[6]の規定に合致する鍵長を用いることが求められることに留意すること。

[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。

[6] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

（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）CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いて CMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（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。

（注１４）CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

（注１７）ブロック暗号には、CRYPTREC暗号リスト掲載128ビットブロック暗号を使う。利用用途はストレージデバイスの暗号化に限り、実装方法はNIST SP800-38Eに従うこと。

（出典）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)より抜粋
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf

CRYPTREC Cryptography Research and Evaluation Committees

（参考）運用監視暗号リスト

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(注15)	3-key Triple DES
	128ビットブロック暗号	該当なし
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(注16)	該当なし
メッセージ認証コード		CBC-MAC(注11)
認証暗号		該当なし
エンティティ認証		該当なし

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CRYPTRECにより確認された暗号技術[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[7]以外の目的での利用は推奨しない。

なお、本リストに記載されている暗号技術を利用する際は、「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[8]の規定に合致する鍵長を用いることが求められることに留意すること。

[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。

[7] 既に稼働中のシステムやアプリケーション等との間での相互運用を継続すること

[8] CRYPTREC, 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準, https://www.cryptrec.go.jp/list.html

（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）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。

（注15）CRYPTREC暗号リストにおいて、64ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いて CMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注16）CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

（出典）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)より抜粋
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf

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