CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会活動報告

2019年7月12日

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

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC活動体制（2017年度～2019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)

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～）

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会構成員

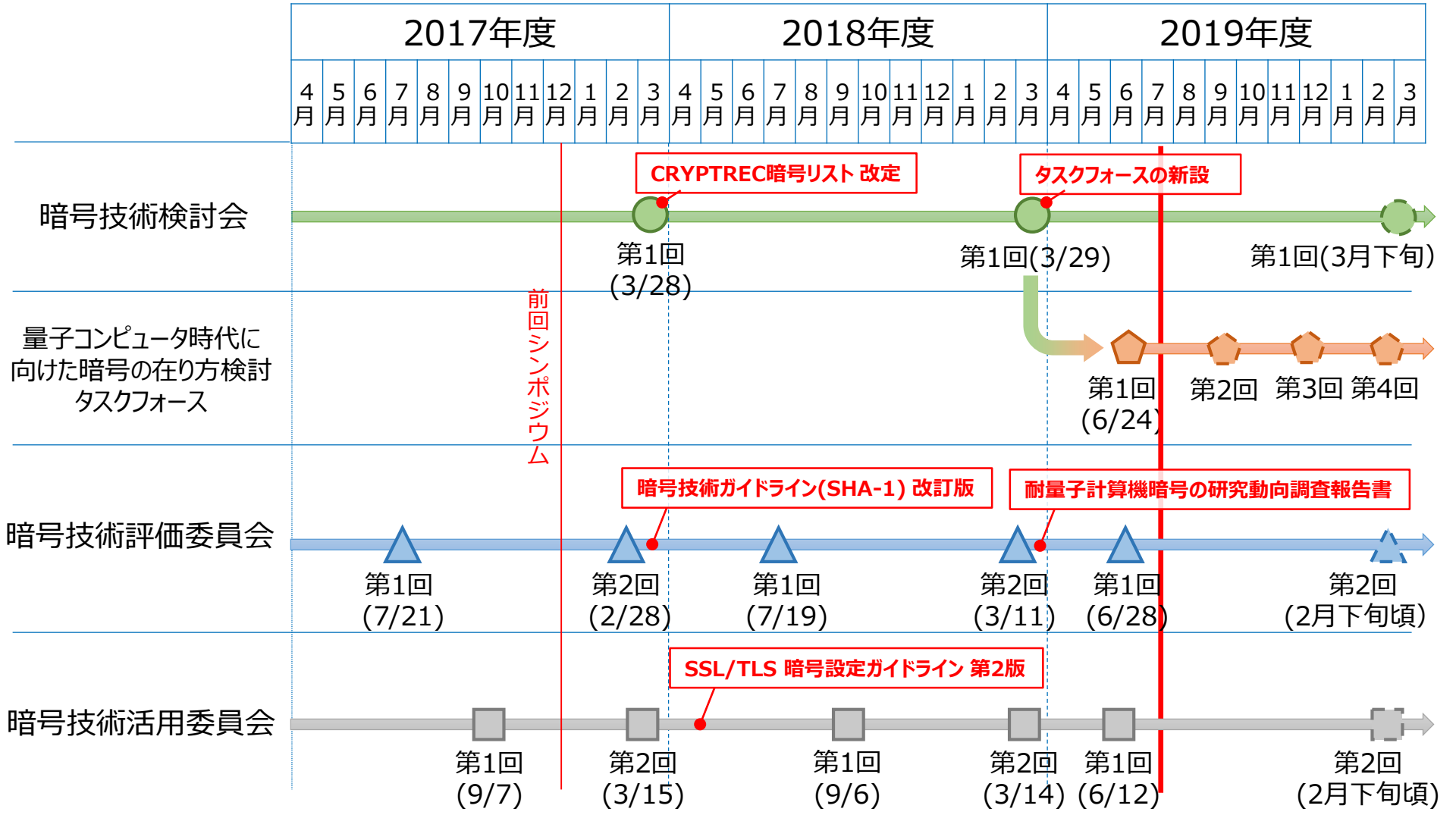
	今井	正道	一般社団法人情報通信ネットワーク産業協会　常務理事
	上原	哲太郎	立命館大学　情報理工学部　教授
	宇根	正志	日本銀行　金融研究所情報技術研究センター　情報技術研究グループ長
	太田	和夫	電気通信大学大学院　情報理工学研究科　教授
	高木	剛	東京大学大学院　情報理工学系研究科　教授
	近澤	武	独立行政法人情報処理推進機構　セキュリティセンター　主任研究員
	手塚	悟	慶應義塾大学大学院　政策・メディア研究科　特任教授
	本間	尚文	東北大学　電気通信研究所　教授
	松井	充	三菱電機株式会社　開発本部　役員技監
	松浦	幹太	東京大学　生産技術研究所　教授
座長	松本	勉	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
	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	産業技術総合研究所　サイバーフィジカルセキュリティ研究センター　副研究センター長

（五十音順、敬称略、所属は2019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



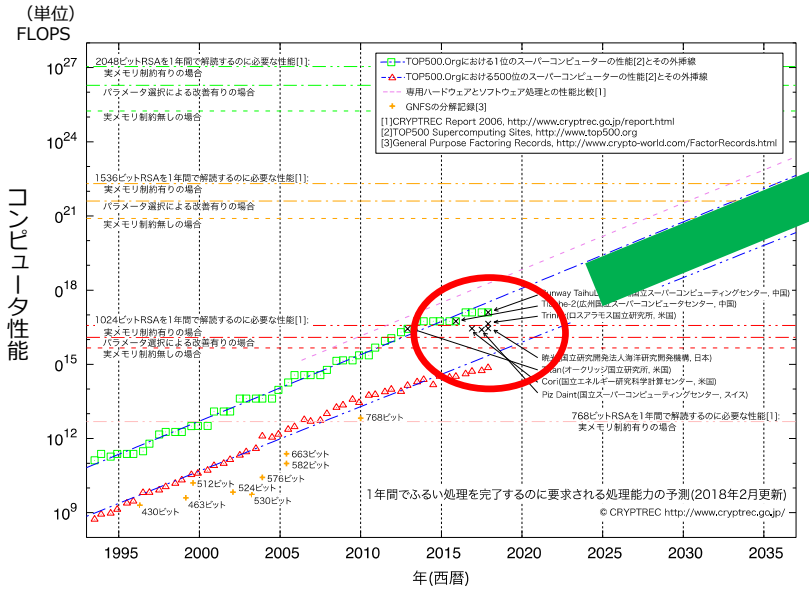
CRYPTREC
Cryptography Research and Evaluation Committees

量子コンピュータ時代に向けた暗号の在り方

量子コンピュータ時代の暗号技術の課題（例）

・RSA暗号や楕円曲線暗号等を破るような強力な
量子コンピュータが出現した場合への備えが必要

・大規模システムの改修・更改には十年以上を要する



RSA暗号（※）の安全性評価

**本格的量子コンピュータがもし実現し、
2048ビットや3072ビットのRSA暗号も
危殆化するとしたらどうするのか？**

（※）桁数が大きい合成数の素因数分解が困難であることを安全性の根拠とした公開鍵暗号。過去、1024ビットの鍵長のものが使われていたが、その危殆化（解読されるおそれがあること）により、現在は**2048ビット以上の鍵長のものが推奨されている**。

（注）グラフの縦軸は、コンピュータが１秒間に処理可能な演算の回数（FLOPS：Floating-Point Operations Per Second）。

CRYPTREC
Cryptography Research and Evaluation Committees

タスクフォースの新設

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

- 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。
- 我が国においても、大規模な量子コンピュータの出現に向けて、耐量子計算機暗号の取扱いについて議論を行う必要性が高まっていることから、次期CRYPTREC暗号リストに求められる要件等を整理する。
- 2019年6月末に第1回会合を開催。

検討事項

- 次期CRYPTREC暗号リストに求める要件や課題について集中的に検討を行う。

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

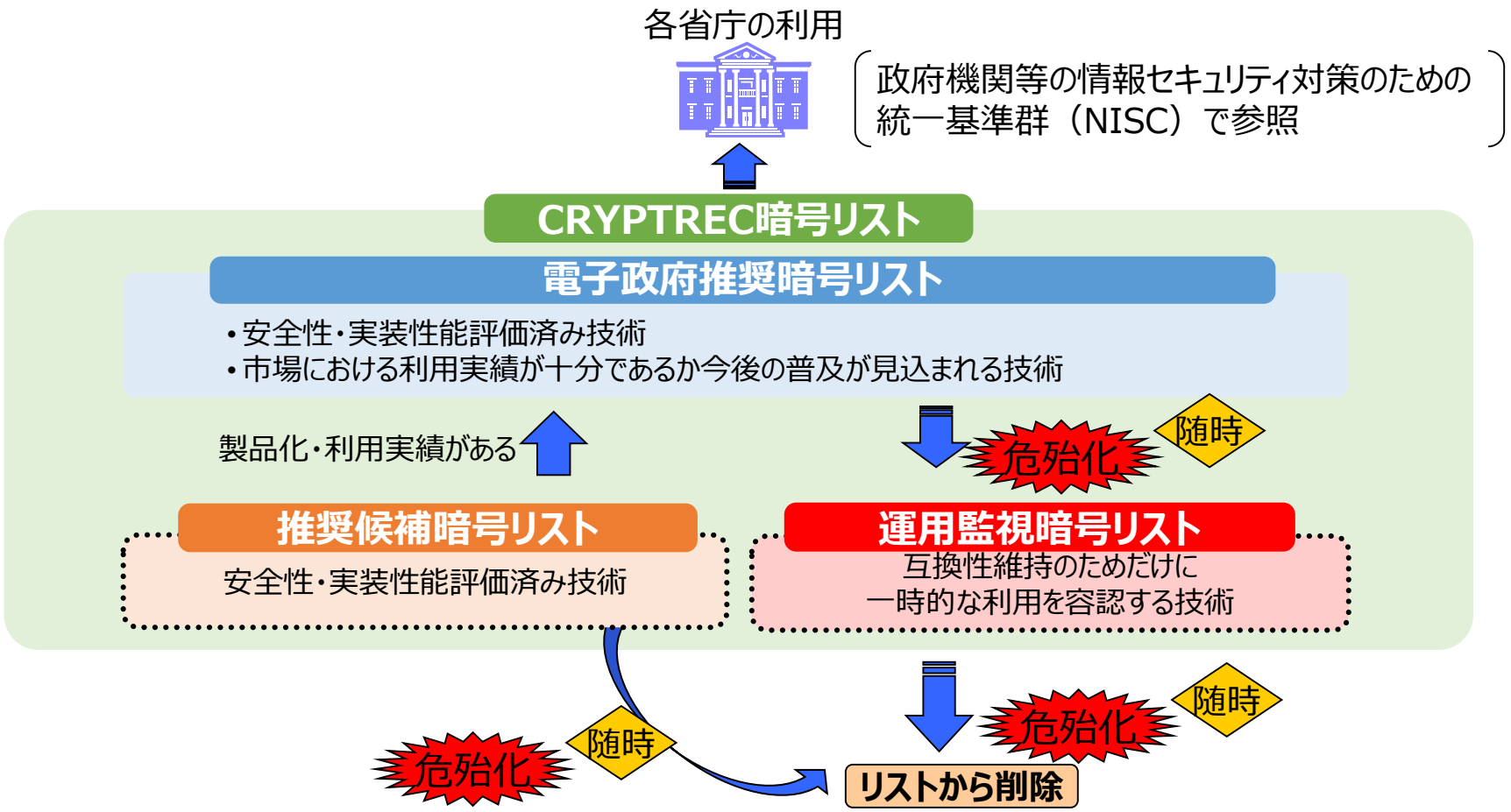
等

⇒ **今後の次期CRYPTREC暗号リストの策定に活用**

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの改定の流れ

■ 平成25年3月1日に、「電子政府推奨暗号リスト」（平成15年2月20日公表）を改定した「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
Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの改定（2018年3月）

■ 暗号技術評価委員会の報告を受けて、CRYPTREC暗号リストを以下のとおり改定。

64ビットブロック暗号に付記されている注釈の変更

- 64ビットブロック暗号の鍵を変えずに使い続ける場合の脅威への対応。

3-key Triple DES の取扱いの変更

- 3-Key Triple DES は、注釈で「デファクトスタンダードであること」を条件として、
  電子　政府推奨暗号として当面の利用を認めていたが、
  NISTにおいても、今後TLSでの利用が推奨されなくなるなど状況が変化。
- 「電子政府推奨暗号リスト」から「運用監視暗号リスト」に移動。

ChaCha20-Poly1305 の追加

- 安全性及び実装性能の評価結果を踏まえて、認証暗号 ChaCha20-Poly1305 を CRYPTREC暗号リストの「推奨候補暗号リスト」に新たに追加。
- CRYPTREC暗号リストの技術分類に「認証暗号」を新設。

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）	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
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

[1] 総務省政策統括官（情報セキュリティ担当）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。

（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）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。

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
		SHAKE128（注１２）
		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（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

[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。

（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、220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、221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。

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（注１５）	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（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（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

[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。

（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。

（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。

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