

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)

令和5年3月30日
デジタル庁・総務省・経済産業省
(最終更新：令和8年3月30日)

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（セキュリティ）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」³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。

<表1 現行暗号リスト>

技術分類		暗号技術
公開鍵暗号	署名	DSA ^(注1)
		ECDSA
		EdDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH ECDH ^(注2)
共通鍵暗号	64ビットブロック暗号 ^(注3)	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 ^(注4)
		SHAKE256 ^(注4)
(次ページに続く)		

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。

3 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>
なお、当該設定基準の見直しの検討を行う予定であり、当面の間、表2（耐量子計算機暗号（PQC）リスト）の公開鍵暗号は、当該設定基準を適用しない。

技術分類		暗号技術
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
		XTS (注5)
	認証付き秘匿モード (注6)	CCM
		GCM (注7)
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

(注1) FIPS PUB 186-5では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。

(注2) 使用するMACはHMAC又はCMACに限る。

(注3) 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) ハッシュ長は256ビット以上とすること。

(注5) 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。

(注6) 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7) 初期化ベクトル長は96ビットを推奨する。

<表 2 耐量子計算機暗号 (PQC) リスト>

現行暗号の解読に利用可能な水準の量子計算機 (CRQC: Cryptographically Relevant Quantum Computer) への耐性を有することが確認された暗号技術のリスト⁴。

技術分類		暗号技術	
		名称	パラメーターセット ^(注8)
公開鍵暗号	署名	—	—
	鍵共有	ML-KEM	ML-KEM-768 (Category 3) ML-KEM-1024 (Category 5)
共通鍵暗号		AES	AES-192 (Category 3) AES-256 (Category 5)
ハッシュ関数		SHA2	SHA-384 (Category 4) SHA-512
		SHA3	SHA3-384 (Category 4) SHA3-512

(注 8) セキュリティのカテゴリを合わせて記載する。各カテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、カテゴリ名の右に記載の鍵探索又は衝突探索と同程度以上の計算資源が攻撃に必要であることを意味する。

- ・ Category 1 128ビット鍵を持つブロック暗号に対する鍵探索
- ・ Category 2 256ビットのハッシュ関数に対する衝突探索
- ・ Category 3 192ビット鍵を持つブロック暗号に対する鍵探索
- ・ Category 4 384ビットのハッシュ関数に対する衝突探索
- ・ Category 5 256ビット鍵を持つブロック暗号に対する鍵探索

<https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf> (令和8年3月25日現在)

⁴ 暗号技術の耐量子計算機暗号 (PQC) リストへの追加について検討中である。
<https://www.cryptrec.go.jp/report/cryptrec-mt-1501-2026.pdf>

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⁵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。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM (注9)
共通鍵暗号	64ビットブロック暗号 (注10)	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 (注11)
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 (注12)	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

(注9) KEM (Key Encapsulating Mechanism) - DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

(注10) 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11) 平文サイズは64ビットの倍数に限る。

(注12) 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。

5 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>

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⁷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⁸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」⁹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。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5 ^(注13)
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号 ^(注14)	3-key Triple DES ^(注15)
	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		RIPEND-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 ^(注16)	該当なし
メッセージ認証コード		CBC-MAC ^(注17)
認証暗号		該当なし
エンティティ認証		該当なし

(注13) 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14) 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15) SP 800-67 Revision 2では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。

(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。

(注17) 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。

7 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。

8 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

9 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>

更新履歴情報

更新日付	更新箇所	更新前の記述	更新後の記述
令和6年 5月16日	注	[新規追加]	(注18) FIPS PUB 186-5では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。
	注	[新規追加]	(注19) SP 800-67 Revision 2では廃止されているが、本リスト掲載時から安全性・利用実績の状況に大きな変化がないため、掲載を継続する。
令和8年 3月30日	電子政府推奨暗号リスト(本文)	暗号技術検討会及び関連委員会(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。	暗号技術検討会及び関連委員会(以下「CRYPTREC」という。)により安全性(セキュリティ)及び実装性能が確認された暗号技術について、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。
	電子政府推奨暗号リスト(表)	[表の件名付与]	<表1 現行暗号リスト>
	電子政府推奨暗号リスト(表)	[表の新設]	<表2 耐量子計算機暗号(PQC)リスト> 現行暗号の解読に利用可能な水準の量子計算機(CRQC: Cryptographically Relevant Quantum Computer)への耐性を有することが確認された暗号技術のリスト。
	電子政府推奨暗号リスト(耐量子計算機暗号(PQC)リスト)	[技術分類の追加]	技術分類: 公開鍵暗号-署名 名称/パラメーターセット: - 技術分類: 公開鍵暗号-鍵共有 名称: ML-KEM パラメーターセット: ML-KEM-768 (Category 3) ML-KEM-1024 (Category 5)
	電子政府推奨暗号リスト(耐量子計算機暗号(PQC)リスト)	[技術分類の追加]	技術分類: 共通鍵暗号 名称: AES パラメーターセット: AES-192 (Category 3) AES-256 (Category 5)
	電子政府推奨暗号リスト(耐量子計算機暗号(PQC)リスト)	[技術分類の追加]	技術分類: ハッシュ関数 名称: SHA2 パラメーターセット: SHA-384 (Category 4) SHA-512 名称: SHA3 パラメーターセット: SHA3-384 (Category 4) SHA3-512
	脚注	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	3 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 なお、当該設定基準の見直しの検討を行う予定であり、当面の間、表2(耐量子計算機暗号(PQC)リスト)の公開鍵暗号は、当該設定基準を適用しない。
	脚注	[新規追加]	4 暗号技術の耐量子計算機暗号(PQC)リストへの追加について検討中である。 https://www.cryptrec.go.jp/report/cryptrec-mt-1501-2026.pdf
	脚注	脚注3、4、7、8	脚注5、7、8、9
	注	(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。 https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf (平成25年3月1日現在)	[削除]

注	(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。 https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf (平成25年3月1日現在)	[削除]
注	[新規追加]	(注2) 使用するMACはHMACまたはCMACに限る。
注	[新規追加]	(注8) セキュリティのカテゴリを合わせて記載する。各カテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、カテゴリ名の右に記載の鍵探索又は衝突探索と同程度以上の計算資源が攻撃に必要であることを意味する。 ・Category 1 128ビット鍵を持つブロック暗号に対する鍵探索 ・Category 2 256ビットのハッシュ関数に対する衝突探索 ・Category 3 192ビット鍵を持つブロック暗号に対する鍵探索 ・Category 4 384ビットのハッシュ関数に対する衝突探索 ・Category 5 256ビット鍵を持つブロック暗号に対する鍵探索 https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf (令和8年3月25日現在)
注	注18、2、12、17、13、4、5～7、14、9、15、19、11	注1、3、4、5、6、7、9～11、12、13、14、15、17