

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) **【改定イメージ】**

令和~~5~~**8**年~~3~~**3**月~~30~~**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4-1-1)
		ECDSA
		EdDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
共通鍵暗号		ECDH ^(注4-1-2)
	~~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
	ストリーム暗号	Camellia
ハッシュ関数		KCipher-2
		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128 ^(注4-1-3)
		SHAKE256 ^(注4-1-3)
(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 (注1-4)	秘匿モード	CBC	
		CFB	
		CTR	
		OFB	
		XTS (注5-1-5)	
	認証付き秘匿モード (注6-1-6)	CCM	
GCM (注7-1-7)			
メッセージ認証コード (注1-4)		CMAC	
		HMAC	
認証暗号		ChaCha20-Poly1305	
エンティティ認証 (注1-4)		ISO/IEC 9798-2	
		ISO/IEC 9798-3	
		ISO/IEC 9798-4	

(注1-1-1) 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2-1-2) 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4-1-3) ハッシュ長は256ビット以上とすること。

(注1-4) CRYPTREC暗号リストに掲載する他の技術分類の暗号技術と組み合わせて利用すること。

(注5-1-5) 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 SP 800-38Eに従うこと。

(注6-1-6) 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7-1-7) 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コンピュータ（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。Category 3以上の利用を推奨する。

技術分類		暗号技術		セキュリティ カテゴリ (注2-1)
公開鍵 暗号	署名	ML-DSA	ML-DSA-44 (注2-2)	Category 1 (注2-3)
			ML-DSA-65	Category 2 (注2-3)
			ML-DSA-87	Category 3
		SLH-DSA	SLH-DSA-SHA2-192[s/f]	Category 5
			SLH-DSA-SHAKE-192[s/f]	Category 3
			SLH-DSA-SHA2-256[s/f]	Category 3
			SLH-DSA-SHAKE-256[s/f]	Category 5
		鍵共有	ML-KEM	ML-KEM-768
	ML-KEM-1024			Category 3
共通鍵 暗号	ブロック 暗号	AES	AES-192	Category 3
			AES-256	Category 5
		Camellia	Camellia-192	Category 3
			Camellia-256	Category 5
	ストリーム 暗号	＝	＝	＝
		ハッシュ関数	SHA2	SHA-384
SHA-512	Category 4 (注2-4)			
SHA3	SHA3-384		Category 4	
	SHA3-512		Category 4 (注2-4)	
SHAKE	SHAKE256 (注2-5)		Category 4	
暗 号 利 用 モ ード (注2-6)	秘匿モード		CBC	組み合わせて利 用する暗号技術 のセキュリティ カテゴリに準ず る。
		CFB		
		CTR		
		OFB		
		XTS (注2-7)		
	認 証 付 き 秘匿モード (注2-8)	CCM		
		GCM (注2-9)		
	メッセージ認証コード (注2-6)		CMAC	
			HMAC	
認証暗号		ChaCha20-Poly1305	Category 5	

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>

(注8-2-1) セキュリティのカテゴリを合わせて記載する。各セキュリティカテゴリはNISTの“Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”に従い、次のように、セキュリティ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2-2) 可能な限りML-DSA-65又はML-DSA-87の利用を推奨し、特に長期的な保護が必要なデータを取り扱う用途ではこれを強く推奨する。

(注2-3) ML-DSA-44について、鍵生成に用いる乱数生成器のセキュリティ強度が192ビット以上の場合にはCategory 2、128ビット以上192ビット未満の場合にはCategory 1となる。

(注2-4) 512ビットのハッシュ関数に対する衝突探索には、384ビットのハッシュ関数に対する衝突探索よりも大きな計算資源が必要となるため、ハッシュ関数の衝突探索を基準とする最上位のCategory 4として記載する。

(注2-5) ハッシュ長は384ビット以上とする。

(注2-6) 表2に掲載する他の技術分類の暗号技術と組み合わせて利用すること。

(注2-7) 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 SP 800-38Eに従うこと。

(注2-8) 表2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2-9) 初期化ベクトル長は96ビットを推奨する。

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9-3-1)
共通鍵暗号	64ビットブロック暗号(注103-2)	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113-3)
ハッシュ関数		該当なし
暗号利用モード (注3-4)	秘匿モード	該当なし
	認証付き秘匿モード(注123-5)	該当なし
メッセージ認証コード(注3-4)		PC-MAC-AES
認証暗号		該当なし
エンティティ認証(注3-4)		該当なし

(注9-3-1) KEM (Key Encapsulating Mechanism) - DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

(注103-2) 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113-3) 平文サイズは64ビットの倍数に限る。

(注3-4) CRYPTREC暗号リストに掲載する他の技術分類の暗号技術と組み合わせて利用すること。

(注123-5) 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承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134-1)
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号 ^(注144-2)	3-key Triple DES ^(注154-3)
	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 ^(注4-4)	秘匿モード	該当なし
	認証付き秘匿モード ^(注164-5)	該当なし
メッセージ認証コード ^(注4-4)		CBC-MAC ^(注174-6)
認証暗号		該当なし
エンティティ認証 ^(注4-4)		該当なし

(注134-1) 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144-2) 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、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154-3) NIST 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4-4) CRYPTREC暗号リストに掲載する他の技術分類の暗号技術と組み合わせて利用すること。

(注164-5) 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174-6) 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>