

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6年5月16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。

技術分類		暗号技術
公開鍵暗号	署名	DSA ^(注18)
		ECDSA
		EdDSA
		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
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128 ^(注12)
		SHAKE256 ^(注12)
(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。

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>

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17)
	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		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

(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)

(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12) ハッシュ長は256ビット以上とすること。

(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。

(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。

(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。

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。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
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01 ^(注7)
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14)	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。

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>

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。

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 ^(注19)
	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 ^(注8)
暗号利用モード ⁶	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

(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)

(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、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。

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>

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18)	[新規追加]	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19)	[新規追加]	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。