CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト改定報告

2023年7月26日

CRYPTREC事務局

（デジタル庁・総務省・経済産業省・NICT・IPA）

目次

1. CRYPTREC暗号リスト概要

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの概要 再掲

■ CRYPTRECの活動を通して**安全性・実装性能等が確認された暗号技術**について、デジタル庁、総務省及び経済産業省において**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暗号リストは以下の**3リスト**により構成される。（注：現在の3リスト構成は2013年より）

①電子政府推奨暗号リスト

安全性及び実装性能が確認された暗号技術で、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、利用を推奨するもののリスト

②推奨候補暗号リスト

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のリスト

③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確認されたが、互換性維持のために継続利用を容認する暗号技術のリスト。

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リストの概要

各省庁での利用

「政府機関等のサイバーセキュリティ対策のための統一基準」
（サイバーセキュリティ戦略本部決定）の遵守事項に記載

CRYPTREC暗号リスト

「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」に合致する
アルゴリズムと鍵長の組み合わせを利用することが求められる。

①電子政府推奨暗号リスト

- 安全性・実装性能評価済み技術
- 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技術

製品化・利用実績がある

危殆化（随時）

②推奨候補暗号リスト

安全性・実装性能評価済み技術

③運用監視暗号リスト

互換性維持のためだけに一時的な利用を容認する技術

危殆化（随時）

長期の利用実績なし（定期的）

危殆化（随時）

容認不可（随時）

リストから削除

安全性・実装性評価等

公募

国際標準
(ISO・ITU-T等)（随時）

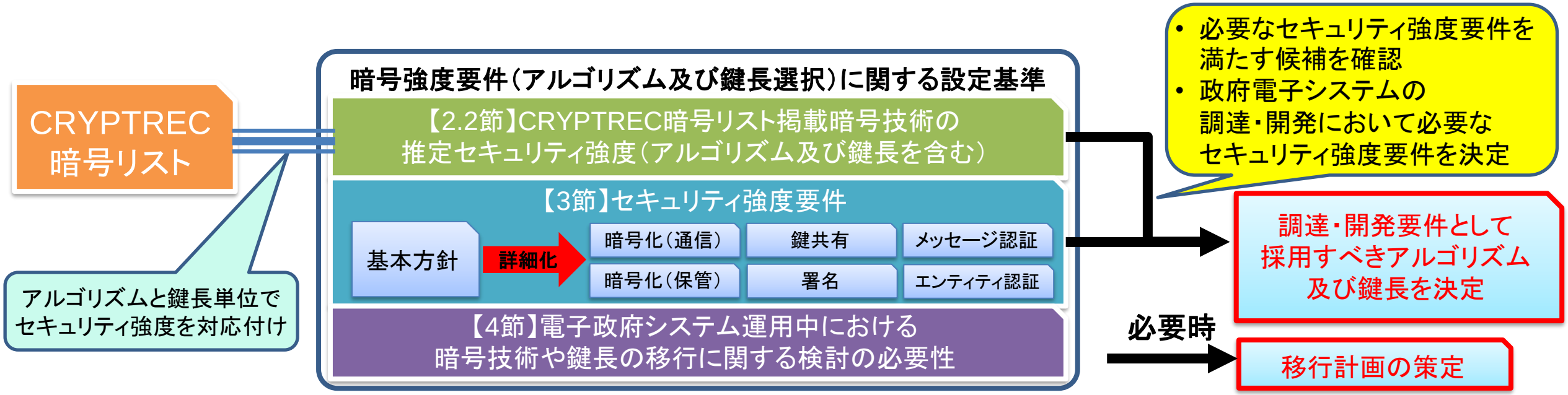
利用実績（随時）

CRYPTREC
Cryptography Research and Evaluation Committees

（参考）暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準の概要

■ CRYPTREC暗号リストに掲載されている暗号技術を利用する際に、適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定した基準（2021年度策定）

● 本基準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。



CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト移行ルール 改変再掲

①電子政府推奨暗号リスト

利用実績による選定基準

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

- 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
- 公募提案暗号について、提案会社より自主取下げ要望があり、暗号技術検討会における審議の結果「今後の普及が見込まれない公募提案暗号」であると判断されたもの

安全性維持が困難（危殆化した）と判断した場合

③運用監視暗号リスト

（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

リストから削除

※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。

CRYPTREC
Cryptography Research and Evaluation Committees

利用実績による選定基準

■「電子政府推奨暗号リスト」への昇格対象とする暗号技術の利用実績による選定基準

- 2012年度のリスト改定時（現在の3リスト構成化）に導入、2021年度に見直しを実施。
- 大きく分けて、
  「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」
  「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」の2基準が存在。

■「利用実績による選定基準」見直し（2021年度暗号技術活用委員会）

- 以下の観点等から、利用実績による選定基準はあくまで昇格の目安とし、明確な選定基準・閾値を設けず、実際の昇格判断は個々の状況を鑑みて個別に行うものとした。
  - 暗号アルゴリズムの普及の仕方について、以前の、利用の前提・環境整備としての「標準化」を踏まえて徐々に利用が広がっていくものから、「有力ベンダが大規模採用」した影響を受け、急速にその周辺に利用範囲が広がり、後から標準化につながっていく流れに変化しつつあることに留意
  - 5年ごとの利用実績調査では、急激な利用実績の変動に対応できないことに繋がる（昇格が適切と認められる状況であったとしても、基準・閾値を満たさないという理由で昇格が認められないのは本末転倒）
  - 有力ベンダの採用状況等から近い将来手中となる可能性が高いと判断できる暗号アルゴリズムであれば、早いうちから採用できる環境を整えるべき（有力ベンダの今後の採用状況等の未来予測も加味して利用実績を判断すべき）

CRYPTREC
Cryptography Research and Evaluation Committees

利用実績による選定基準

考慮項目		選定目安
採用実績	以下のいずれかを満たす場合、昇格の検討対象に含める。なお、採用実績は、 • 5年ごとに実施予定の大規模アンケート調査による「**利用実績調査**」 • 必要に応じて、事務局が（大規模アンケート調査によらずに）情報収集する「**利用実態確認**」 により確認するものとする。	
	① **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術を昇格検討対象とする。
	② **利用実績調査**又は**利用実態確認**の結果、**電子政府システムや重要インフラ等、日本の基幹システム**においてすでに利用されていることが確認された場合	必要に応じて、利用実績調査に代わって、各府省庁等への照会を実施し、照会結果（クローズドな利用を含め）を基に昇格検討対象を選定する。
	利用実績調査又は**利用実態確認**の結果、③～⑤のいずれかが確認された場合： ③ **利用者が多い主要な汎用製品群の複数**に搭載されるなど、明らかに採用が進展していると判断された場合 ④ **利用者が多い主要なオープンソースソフトウェアの複数**に搭載されるなど、明らかに採用が進展していると判断された場合 ⑤ **利用者が多い主要なサービスやプロトコルの複数**で利用されるなど、明らかに採用が進展していると判断された場合	「複数」「利用者が多い（主要な）」というキーワードの両方を十分に満たし、明らかな採用促進が確認された場合には、必要に応じて、昇格検討対象とする。 ※「複数」の意味は、必要条件として「2個以上が必要」ということであって、「2個以上あればよい」という十分条件としての意味ではないことに留意
標準化実績	以下を満たす場合、昇格の検討対象に含める。	
	⑥ **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合	電子政府推奨暗号リスト掲載の（同一カテゴリの）暗号技術の採用実績と同等以上の採用実績がある推奨候補暗号リスト掲載の暗号技術は昇格検討対象とする。

2. CRYPTREC暗号リスト改定

CRYPTREC
Cryptography Research and Evaluation Committees

これまでのCRYPTREC暗号リスト改定

電子政府推奨暗号リスト（2003年2月策定）

✓電子政府システム構築にあたり参考とできる、各システムの情報セキュリティを確保するために必要な、適正な評価が行われた暗号技術のリストを策定

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）（2013年3月策定）

✓「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3リスト体制へ

✓本リストは小改訂等を除き10年程度の運用を想定して策定したものであり、本リストを策定した2012年度暗号技術検討会において、10年後を目途に全面改定を実施する等決定

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）（2023年3月策定）

✓推奨候補暗号リストに掲載されている暗号の内「製品化・利用実績がある」と認められた暗号10件が電子政府推奨暗号リストへ昇格

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト改定のプロセス

暗号技術評価委員会

暗号技術の安全性及び実装に係る監視及び評価等

NICT
「暗号アルゴリズムの安全性評価」の実施

暗号技術活用委員会

選定基準の見直し
利用実績に基づく選定基準案の検討

暗号技術の利用実績に係る評価

IPA
利用実績調査の実施

暗号技術検討会

次回リスト改定の大枠の決定

利用実績に基づく選定基準の決定

昇格候補として推薦する暗号アルゴリズムの決定

CRYPTREC暗号リスト改定案の提示

改定に係る取組み等の広報（随時）

CRYPTREC シンポジウム

CRYPTREC Report・報告書

デジタル庁・総務省・経済産業省

CRYPTREC暗号リスト改定案の決定

意見募集の実施

CRYPTREC暗号リストの改定

CRYPTREC
Cryptography Research and Evaluation Committees

2022年度リスト改定の流れ

(年度)

2012

暗号技術検討会

- 前回のCRYPTREC暗号リスト全面改定を実施。
- 次回の全面改定を10年後を目途に実施する等、今後のリスト改定の大枠を決定。

2020

暗号技術検討会

- 2022年度目途のリスト改定にあたり、3リスト構成を維持する方針を決定。
- 各暗号技術について十分成熟している為、新たな暗号技術の公募を実施せず、技術分類※1の構成を維持する方針を決定。

※1 次の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

2021

暗号技術検討会

- 暗号技術活用委員会において検討された、「推奨候補暗号リスト」から「電子政府推奨暗号リスト」へ昇格させる暗号アルゴリズムを選定する際の**暗号アルゴリズムの利用実績による選定基準**を決定。

CRYPTREC
Cryptography Research and Evaluation Committees

2022年度リスト改定の流れ

(年度)

2022

IPA

- CRYPTREC暗号リストの改定に向けた情報として活用するため、各種市販製品、標準規格、オープンソースソフトウェア等を対象に、**「暗号アルゴリズムの利用実績に関する調査」を実施**。

暗号技術活用委員会

- 「暗号アルゴリズムの利用実績に関する調査」の結果を踏まえ、「電子政府推奨暗号リスト」への昇格候補として**暗号技術検討会に推薦する暗号アルゴリズムを決定**。

暗号技術評価委員会

- 「暗号アルゴリズムの安全性評価」の結果を踏まえ「電子政府推奨暗号リスト」への昇格候補として**暗号技術検討会に推薦する暗号アルゴリズムを決定**。

暗号技術検討会

- 暗号技術活用委員会において決定された暗号技術検討会に推薦する暗号アルゴリズムを踏まえ、意見募集において公示する**CRYPTREC暗号リストの改定案を提示**。

デジタル庁、総務省、経済産業省

- CRYPTREC暗号リストの改定案に対する意見募集を実施。
- **CRYPTREC暗号リストの改定を実施。**

CRYPTREC
Cryptography Research and Evaluation Committees

利用実績による選定基準 改変再掲

考慮項目	
採用実績	以下のいずれかを満たす場合、昇格の検討対象に含める。なお、採用実績は、 • 5年ごとに実施予定の大規模アンケート調査による「**利用実績調査**」 • 必要に応じて、事務局が（大規模アンケート調査によらずに）情報収集する「**利用実態確認**」 により確認するものとする。
	① **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合
	② **利用実績調査**又は**利用実態確認**の結果、**電子政府システムや重要インフラ等、日本の基幹システム**においてすでに利用されていることが確認された場合
	利用実績調査又は**利用実態確認**の結果、③～⑤のいずれかが確認された場合： ③ **利用者が多い主要な汎用製品群の複数**に搭載されるなど、明らかに採用が進展していると判断された場合
	④ **利用者が多い主要なオープンソースソフトウェアの複数**に搭載されるなど、明らかに採用が進展していると判断された場合
	⑤ **利用者が多い主要なサービスやプロトコルの複数**で利用されるなど、明らかに採用が進展していると判断された場合
標準化実績	以下を満たす場合、昇格の検討対象に含める。
	⑥ **利用実績調査**の結果、電子政府推奨暗号リストに掲載されている（同一カテゴリの）暗号技術の採用実績と遜色がないことが確認された場合

① 既掲載暗号との利用実績比較
- ChaCha20-Poly1305
- XTS
- ISO/IEC 9798-4

②基幹システムにおける利用
- ChaCha20-Poly1305
- XTS
- ISO/IEC 9798-4

④ 主要 OSS での利用
- ChaCha20-Poly1305
- XTS
- EdDSA
- SHA-512/256、SHA3-256、SHA3-384、SHA3-512、SHAKE128、SHAKE256

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト改定 改変再掲

■2023年3月にCRYPTREC暗号リストの大規模改定を実施

- 「利用実績による選定基準」を踏まえ、「推奨候補暗号リスト」に掲載されている暗号の内、「製品化・利用実績がある」と認められた暗号10件が電子政府推奨暗号リストへ昇格した。

暗号技術	技術分類
EdDSA	公開鍵暗号-署名
SHA-512/256	ハッシュ関数
SHA3-256	ハッシュ関数
SHA3-384	ハッシュ関数
SHA3-512	ハッシュ関数
SHAKE128	ハッシュ関数
SHAKE256	ハッシュ関数
XTS	暗号利用モード-秘匿モード
ChaCha20-Poly1305	認証暗号
ISO/IEC 9798-4	エンティティ認証

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト (2023年3月30日初版)

電子政府推奨暗号リスト

第7版（更新日：2022年3月30日）

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

第7版（更新日：2022年3月30日）

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

自主取下げを承認

運用監視暗号リスト

第7版（更新日：2022年3月30日）

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	該当なし
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

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC暗号リスト (2023年3月30日初版)

電子政府推奨暗号リスト

(令和5年3月30日 デジタル庁、総務省、経済産業省共同発表)

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		EdDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号	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
		SHAKE256

技術分類		名称
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
		XTS
	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		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3
		ISO/IEC 9798-4

推奨候補暗号リスト

(令和5年3月30日 デジタル庁、総務省、経済産業省共同発表)

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
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
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01
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	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

運用監視暗号リスト

(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	該当なし
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

CRYPTREC
Cryptography Research and Evaluation Committees

今後のCRYPTREC暗号リスト改定

■ CRYPTREC暗号リストの小改定

以下を踏まえて、引き続き小規模改定を実施。

- 暗号技術評価委員会における、暗号技術の安全性及び実装に係る監視及び評価
- 暗号技術活用委員会における、暗号技術の利用状況に係る調査

■ 今後のCRYPTREC暗号リスト大規模改定

- 過去、2003年に作成、2013年、2023年に改定と10年単位で改定を実施しているが、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年単位とする必要が低い。
- 次期改定については、本改定後5年以内を目途に暗号技術検討会において改定の是非を判断することとする。