CRYPTREC暗号リストについて

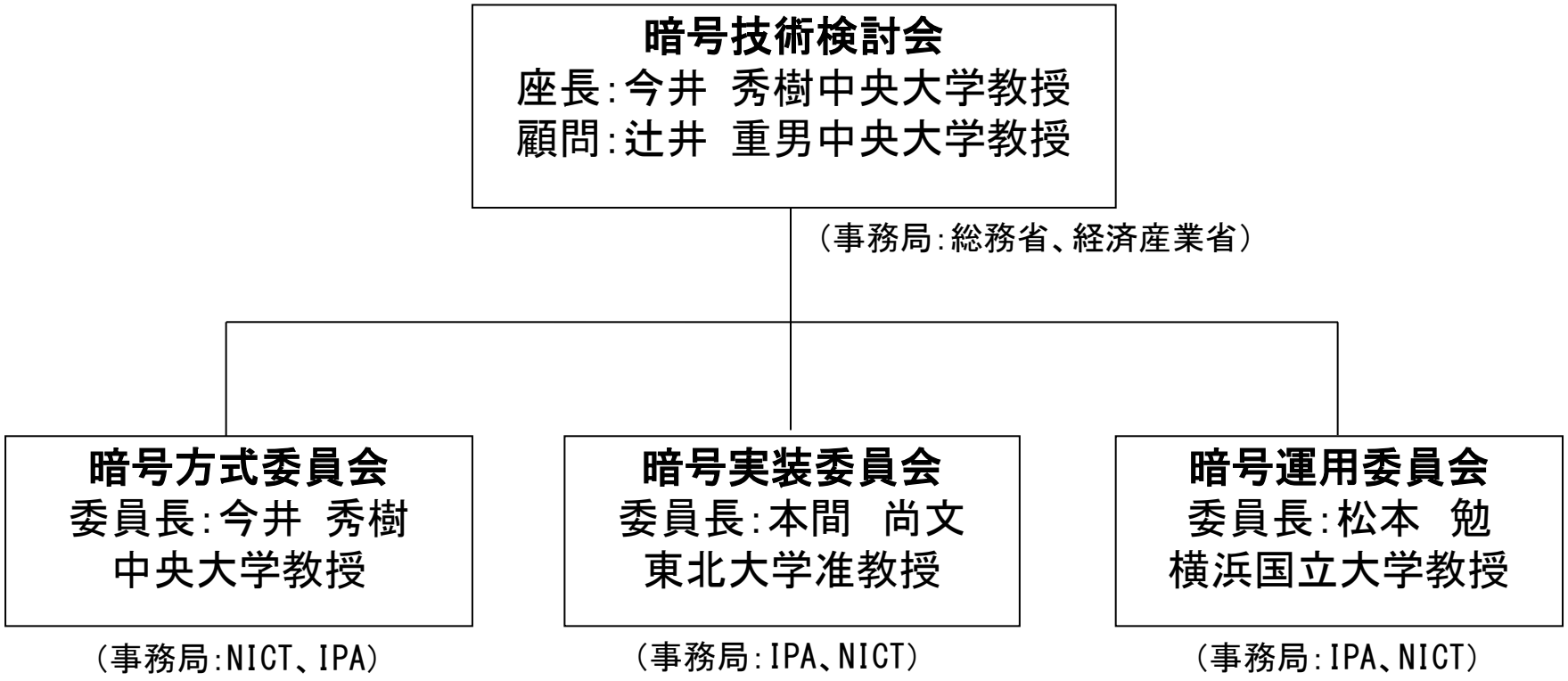
CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会事務局
（総務省情報セキュリティ対策室標準化推進官）
上原　哲太郎

CRYPTRECとは？

- Cryptography Research and Evaluation Committees
  - 総務省及び経済産業省が共同で開催する暗号評価プロジェクト。
  - 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方式委員会、暗号実装委員会及び暗号運用委員会により運営。
    （※ただし、平成25年度から委員会構成を変更する予定。）

平成24年度CRYPTREC検討体制



暗号技術検討会の目的・検討事項

- 暗号技術検討会の目的
  - 総務省政策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、総務省及び経済産業省における施策の検討に資する。（構成員は次スライドの通り。）

- 暗号技術検討会の検討事項
  - 電子政府推奨暗号の監視
  - 電子政府推奨暗号の安全性及び信頼性確保のための調査・検討
  - **電子政府推奨暗号リストの改定**に関する調査・検討
  - 暗号モジュールに関する国際標準化への協力
  - その他、暗号技術の評価及び利用に関すること

CRYPTREC
Cryptography Research and Evaluation Committees

2012年度　暗号技術検討会　構成員

座長	今井　秀樹	中央大学　理工学部電気電子情報通信工学科　教授
	太田　和夫	電気通信大学　電気通信学部情報通信工学科　教授
	岡本　栄司	筑波大学大学院　システム情報工学研究科　教授
	岡本　龍明	日本電信電話株式会社　セキュアプラットフォーム研究所　岡本特別研究室　室長 （社団法人電気通信事業者協会代表兼務）
	金子　敏信	東京理科大学　理工学部電気電子情報工学科　教授
	国分　明男	一般財団法人ニューメディア開発協会　顧問・首席研究員
	佐々木　良一	東京電機大学　未来科学部情報メディア学科　教授
	武市　博明	一般社団法人情報通信ネットワーク産業協会　常務理事
	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暗号グループ グループリーダー（ISO/IEC　JTC 1/SC27/WG2 Convenor（国際主査））
顧問	辻井　重男	中央大学　研究開発機構　教授
	中山　靖司	日本銀行　金融研究所情報技術研究センター　企画役
	本間　尚文	東北大学大学院　情報科学研究科　准教授
	松井　充	三菱電機株式会社　情報技術総合研究所　情報セキュリティ技術部長
	松尾　真一郎	独立行政法人情報通信研究機構　ネットワークセキュリティ研究所　セキュリティアーキテクチャ研究室　室長（ISO/IEC JTC1 SC27/WG2（国内小委員会主査））
	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研究所基盤技術ディビジョン 認証基盤グループグループリーダ
	持麾　裕之	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
	渡辺　創	ISO/IEC JTC1 SC27　国内委員会　委員長

オブザーバ：　内閣官房情報セキュリティセンター、警察庁、総務省、法務省、外務省、財務省、文部科学省、経済産業省、防衛省、NICT、AIST、IPA、JIPDEC、FISC

【参考】(旧)電子政府推奨暗号リスト

CRYPTREC
Cryptography Research and Evaluation Committees

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注2)
共通鍵暗号	64ビットブロック暗号(注3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注4)
	128ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注5)
その他	ハッシュ関数	RIPEMD-160(注6)
		SHA-1(注6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈:

(注1) SSL3.0/TLS1.0で使用実績があることから当面の使用を認める。

(注2) KEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

(注3) 新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128ビットブロック暗号を選択することが望ましい。

(注4) 3-key Triple DESは、以下の条件を考慮し、当面の使用を認める。
1) FIPS46-3として規定されていること
2) デファクトスタンダードとしての位置を保っていること

(注5) 128-bit RC4は、SSL3.0/TLS1.0以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

(注6) 新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

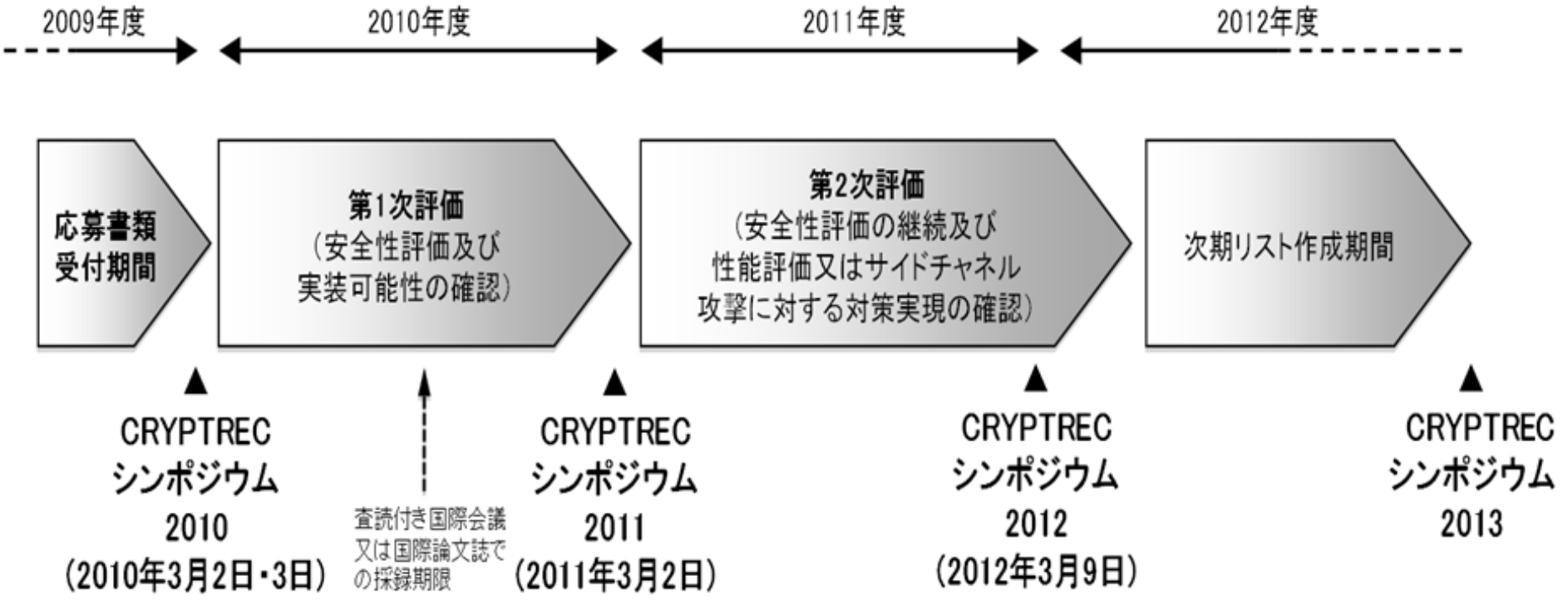
(注7) 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

(別添)電子政府推奨暗号リストに関する修正情報

修正日付	修正箇所	修正前	修正後	修正理由
平成17年10月12日	注釈の注4)の1)	FIPS46-3として規定されていること	SP800-67として規定されていること	仕様変更を伴わない、仕様書の指定先の変更

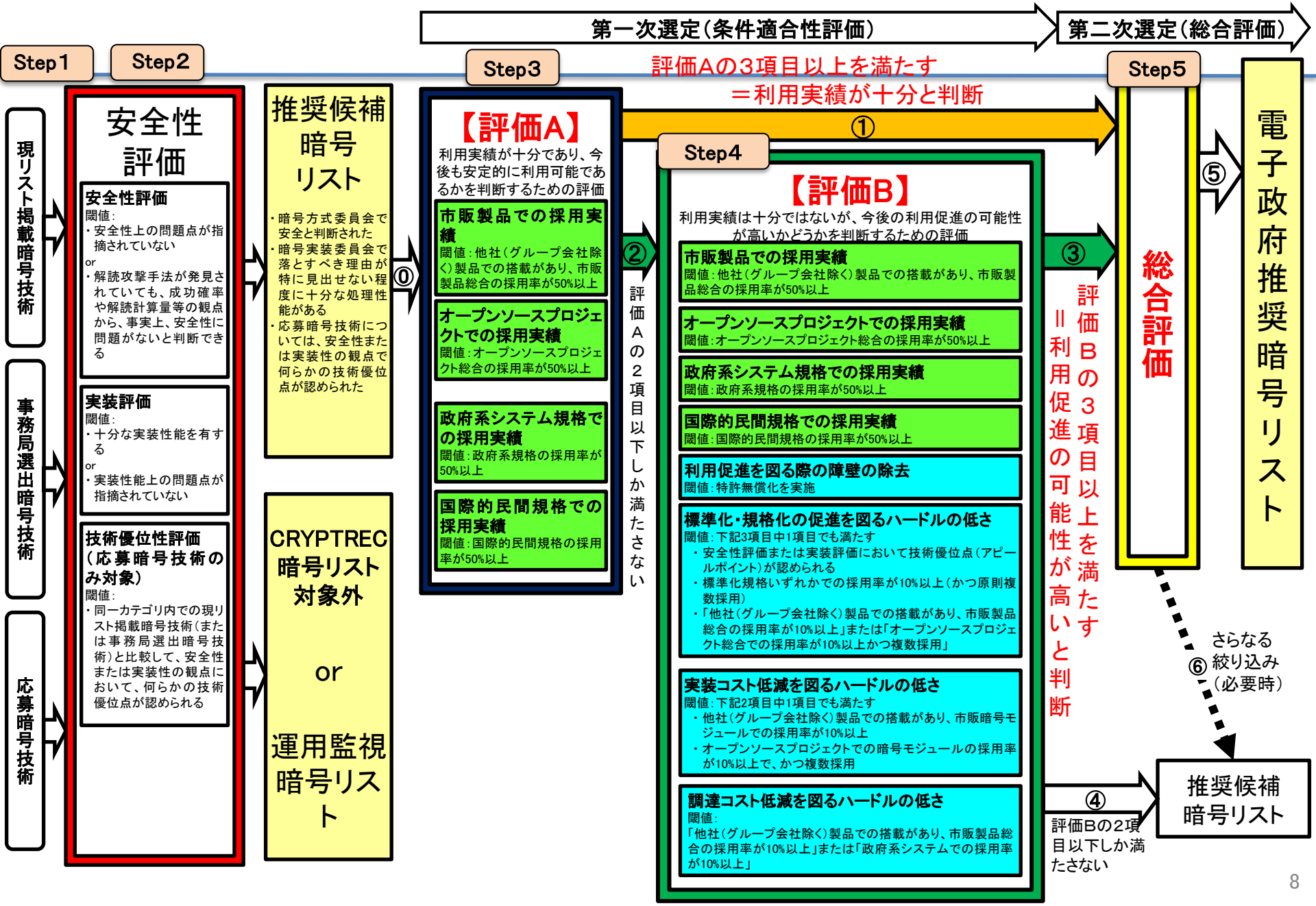
電子政府における調達のために参照すべき暗号のリスト

CRYPTREC暗号リスト（改定までの経緯）



【参考】CRYPTREC暗号リスト選定基準

CRYPTREC
Cryptography Research and Evaluation Committees



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（電子政府推奨暗号リスト）

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）	3-key Triple DES（注3）
	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（注4）
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

（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）より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。

（注3）3-key Triple DESは、以下の条件を考慮し、当面の利用を認める。
1） NIST SP 800-67として規定されていること。
2） デファクトスタンダードとしての位置を保っていること。

（注4）初期化ベクトル長は96ビットを推奨する。

[1] 総務省政策統括官（情報通信担当）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。

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（推奨候補暗号リスト）

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		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
エンティティ認証		ISO/IEC 9798-4

（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）より長いブロック長の暗号が利用できるのであれば、128ビットブロック暗号を選択することが望ましい。

（注7）平文サイズは64ビットの倍数に限る。

[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。

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（運用監視暗号リスト）

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	該当なし
	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	該当なし
メッセージ認証コード		CBC-MAC（注11）
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。
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）　128-bit RC4は、SSL（TLS 1.0以上）に限定して利用すること。

（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。

[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。

【参考】CRYPTREC暗号リスト選定遷移図

CRYPTREC
Cryptography Research and Evaluation Committees

技術分類		電子政府推奨暗号リスト(平成15年2月20日版)
公開鍵暗号	署名	DSA ECDSA RSA-PSS RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP RSAES-PKCS1-v1_5
	鍵共有	DH ECDH PSEC-KEM
共通鍵暗号	64ビットブロック暗号	CIPHERUNICORN-E Hierocrypt-L1 MISTY1 3-key Triple DES
	128ビットブロック暗号	AES Camellia CIPHERUNICORN-A Hierocrypt-3 SC2000
	ストリーム暗号	MUGI MULTI-S01 128-bit RC4
ハッシュ関数		RIPEMD-160 SHA-1 SHA-256 SHA-384 SHA-512
暗号利用モード		
MAC		
エンティティ認証		

技術分類		新規評価対象暗号	
		新規応募暗号	事務局選出暗号
公開鍵暗号	署名		
	守秘		
	鍵共有		
共通鍵暗号	64ビットブロック暗号		
	128ビットブロック暗号	CLEFIA	該当なし
	ストリーム暗号	Enocoro-128v2 KCipher-2	該当なし
ハッシュ関数			
暗号利用モード		該当なし	CBC CFB CTR OFB CCM GCM
MAC		PC-MAC-AES	CBC-MAC CMAC HMAC
エンティティ認証		該当なし	ISO/IEC9798-2 ISO/IEC9798-3 ISO/IEC9798-4

安全性評価／実装評価

【評価A】

利用実績が十分であり、今後も安定的に利用可能であるかを判断するための評価

【評価B】

利用実績は十分ではないが、今後の利用促進の可能性が高いかどうかを判断するための評価

①

②

③

④

技術分類		運用監視暗号リスト	CRYPTREC暗号リスト外
公開鍵暗号	署名	該当なし	該当なし
	守秘	RSAES-PKCS1-v1_5	該当なし
	鍵共有	該当なし	該当なし
共通鍵暗号	64ビットブロック暗号	該当なし	該当なし
	128ビットブロック暗号	該当なし	HyRAL※
	ストリーム暗号	128-bit RC4	該当なし
ハッシュ関数		RIPEMD-160 SHA-1	該当なし
暗号利用モード		該当なし	該当なし
MAC		CBC-MAC	該当なし
エンティティ認証		該当なし	該当なし

※ 新規応募暗号HyRAL（128ビットブロック暗号）については、2010年度の第一次評価の結果、第一次評価までで終了とし、CRYPTREC暗号リストに掲載しないこととなった。

技術分類		電子政府推奨暗号リスト	
		評価A通過（①）	評価B通過（②③）
公開鍵暗号	署名	DSA RSASSA-PKCS1-v1_5	ECDSA RSA-PSS
	守秘	該当なし	RSA-OAEP
	鍵共有	DH	ECDH
共通鍵暗号	64ビットブロック暗号	3-key Triple DES	該当なし
	128ビットブロック暗号	AES	Camellia
	ストリーム暗号	該当なし	KCipher-2
ハッシュ関数		該当なし	SHA-256 SHA-384 SHA-512
暗号利用モード		CBC	CFB CTR OFB CCM GCM
MAC		HMAC	CMAC
エンティティ認証		該当なし	ISO/IEC9798-2 ISO/IEC9798-3

総合評価

⑤

電子政府推奨暗号リスト

技術分類		推奨候補暗号リスト
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 SC2000
	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		該当なし
MAC		PC-MAC-AES
エンティティ認証		ISO/IEC9798-4

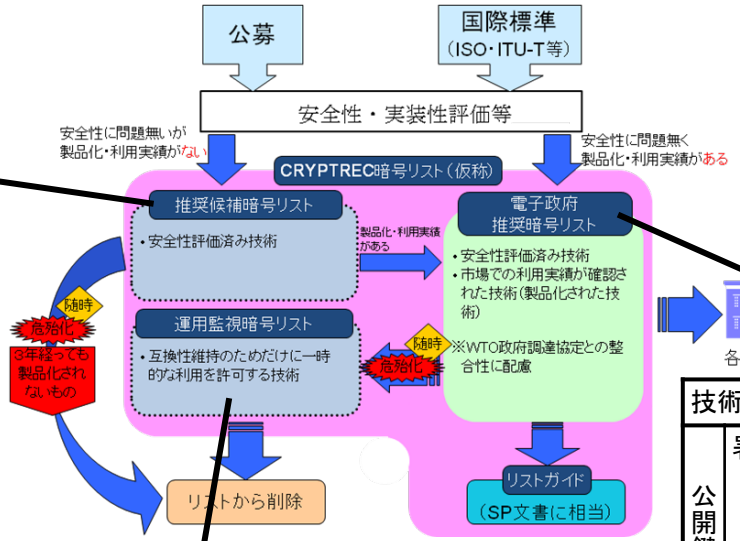
⑥

さらなる絞り込み（必要時）

【参考】CRYPTREC暗号リストの3つのリストの関係

CRYPTREC
Cryptography Research and Evaluation Committees

技術分類		推奨候補暗号リスト
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 SC2000
	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		該当なし
MAC		PC-MAC-AES
エンティティ認証		ISO/IEC9798-4



技術分類		運用監視暗号リスト
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	該当なし
	128ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4
ハッシュ関数		RIPEMD-160 SHA-1
暗号利用モード		該当なし
MAC		CBC-MAC
エンティティ認証		該当なし

技術分類		電子政府推奨暗号リスト
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	64ビットブロック暗号	3-key Triple DES
	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		CBC CFB CTR OFB CCM GCM
MAC		CMAC HMAC
エンティティ認証		ISO/IEC9798-2 ISO/IEC9798-3

ご静聴有り難うございました。

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術検討会事務局
（総務省情報セキュリティ対策室標準化推進官）
上原　哲太郎