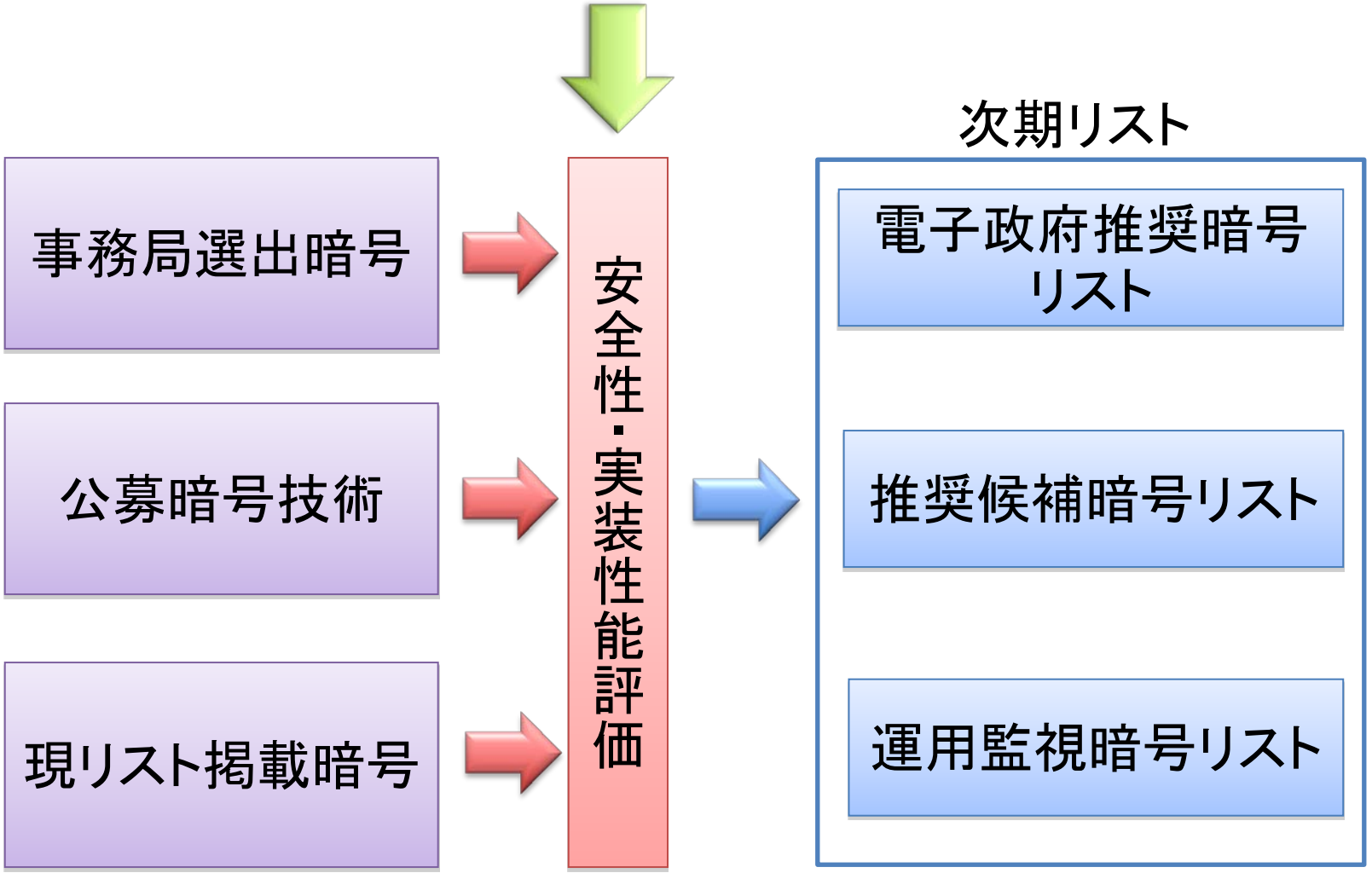
暗号方式委員会活動報告

CRYPTREC
Cryptography Research and Evaluation Committees

リスト入りまでの基本的な流れ



CRYPTREC
Cryptography Research and Evaluation Committees

現リストのカテゴリ

技術分類	
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
	ストリーム暗号
その他	ハッシュ関数
	擬似乱数生成系

CRYPTREC
Cryptography Research and Evaluation Committees

現リスト:公開鍵暗号

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
	鍵共有	DH
		ECDH
		PSEC-KEM

現リスト:共通鍵暗号

技術分類		名称
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

CRYPTREC
Cryptography Research and Evaluation Committees

現リスト:その他(1)

技術分類		名称
その他	ハッシュ関数	RIPEMD-160
		SHA-1
		SHA-256
		SHA-384
		SHA-512

現リスト:その他(2)

技術分類		名称
その他	擬似乱数生成系	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

公募対象の暗号技術の種別と第二次評価中の応募暗号技術

2009年度公募対象の暗号技術の種別

暗号技術の種別
ブロック暗号
暗号利用モード
メッセージ認証コード
ストリーム暗号
エンティティ認証

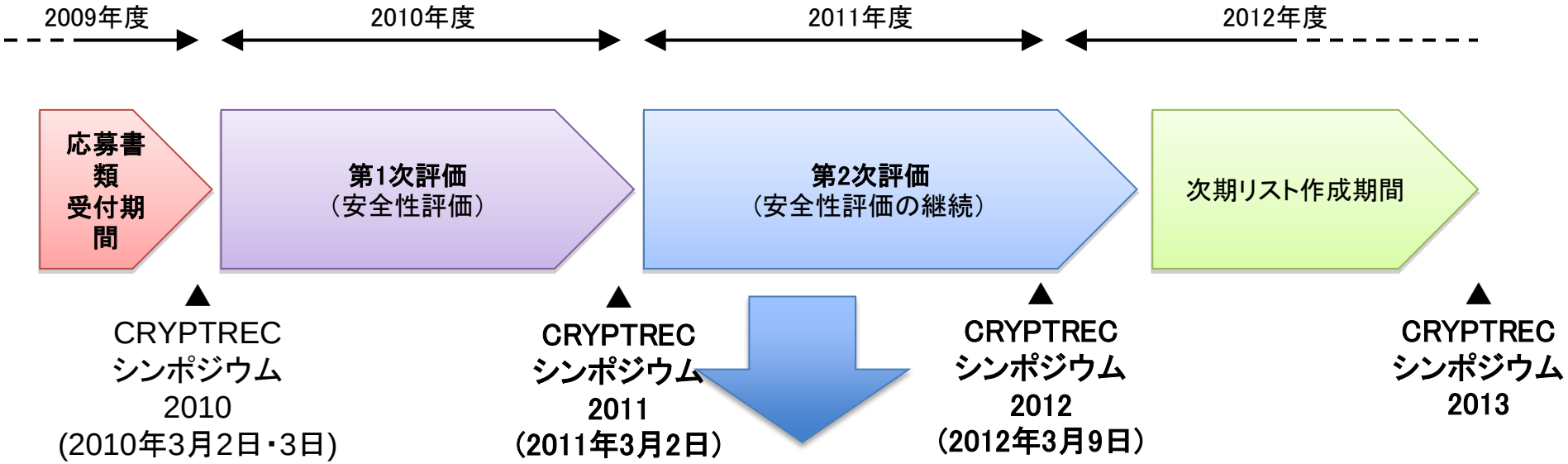
暗号種別	暗号技術名
128ビットブロック暗号	CLEFIA
ストリーム暗号	Enocoro-128v2
	KCipher-2
メッセージ認証コード	PC-MAC-AES

CRYPTREC
Cryptography Research and Evaluation Committees

事務局選出暗号技術

暗号種別	暗号技術名
メッセージ認証コード	CBC-MAC
	CMAC
	HMAC
暗号利用モード	CBCモード
	CFBモード
	OFBモード
	CTRモード
	GCMモード
	CCMモード
エンティティ認証	共通鍵暗号利用による認証プロトコル
	電子署名利用による認証プロトコル
	メッセージ認証コード（MAC）による認証プロトコル

現リスト掲載暗号・応募暗号の評価スケジュール



暗号方式委員会実施事項

- 電子政府推奨暗号リスト安全性監視活動
- 現リスト掲載暗号・応募暗号の安全性評価

CRYPTREC
Cryptography Research and Evaluation Committees

現リスト掲載暗号・応募暗号の安全性評価

ブロック暗号

- 現リスト掲載のブロック暗号の関連鍵攻撃に対する安全性
- 192/256ビット鍵の場合の安全性

ストリーム暗号

- MULTI-S01はストリーム暗号として現リストに掲載されているが、提案者はMAC機能も謳っている。
- 次期リストにはメッセージ認証コードというカテゴリがあるため、MAC機能の評価が必要。

その他の暗号種別

- 来年度審議

CRYPTREC
Cryptography Research and Evaluation Committees

現リスト掲載暗号・応募暗号の安全性評価

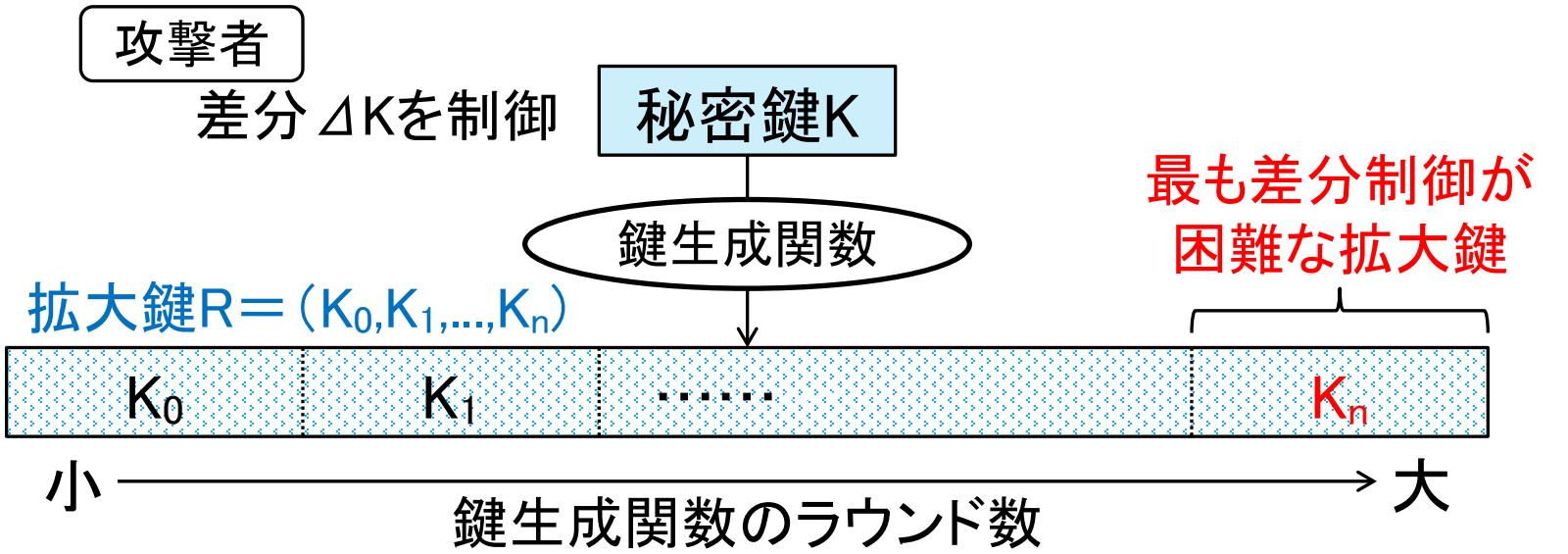
電子政府推奨暗号リストの128ビットブロック暗号について関連鍵攻撃に対する安全性を評価
- 鍵生成関数の丸め差分特性確率による概算評価
- AESと他の128ビットブロック暗号との比較

鍵長192/256ビットの場合の安全性を評価
- データ撹拌全ラウンドの丸め差分・線形特性確率で評価
- 各鍵長における計算量的安全性の概算評価

CRYPTREC
Cryptography Research and Evaluation Committees

128ビットブロック暗号の関連鍵攻撃に対する安全性評価

関連鍵攻撃 = 攻撃者が秘密鍵を操作できる攻撃



(ΔK→ΔR)の最大差分確率 ≦ (ΔK→ΔKn)の最大差分確率

↳ この確率(の上界)で評価

安全性を鍵生成関数の差分特性確率で評価

ただし、排他的論理和、定数加乗算に関しては全て攻撃者に都合の良い差分伝播が確率1で生じるとし、攻撃者有利に評価

CRYPTREC
Cryptography Research and Evaluation Committees

128ビットブロック暗号の関連鍵攻撃 評価結果

アルゴリズム＼鍵長	差分特性確率の上界		
	128ビット	192ビット	256ビット
AES	2^{-24}	2^{-6}	2^{-6}
Camellia	2^{-30}	2^{-18}	2^{-18}
CIPHERUNICORN-A	2^{-259}	2^{-175}	2^{-133}
Hierocrypt-3	2^{-36}	2^{-36}	2^{-36}
SC2000	2^{-48}	2^{-24}	2^{-24}

AESと比較して、Camellia、CIPHERUNICORN-A、Hierocrypt-3、SC2000は関連鍵攻撃に対してより耐性があると見積もられる

CRYPTREC
Cryptography Research and Evaluation Committees

192/256ビットの場合の安全性評価

192/256ビット鍵の場合の計算量的安全性を乱数識別攻撃の立場で概算評価

- 差分特性確率、線形特性確率の上界

排他的論理和やビットシフトなどの線形演算に関しては確率1で、算術加乗算やs-boxなどの非線形演算に関しては最大差分確率で、それぞれ攻撃者に都合の良い差分伝播が生じるとし、攻撃者有利の評価を行っている。

192/256ビットの場合の安全性評価
差分特性確率の上界(1)

アルゴリズム＼鍵長	差分特性確率の上界		
	128ビット	192ビット	256ビット
AES	2^{-336}	2^{-456}	2^{-486}
Camellia	2^{-216}	2^{-288}	192ビット鍵と同じ
CIPHERUNICORN-A	2^{-190}	128ビット鍵と同じ	128ビット鍵と同じ
Hierocrypt-3	2^{-450}	2^{-480}	2^{-600}
SC2000	(2^{-187})	(2^{-215})	192ビット鍵と同じ

()内の値は、自己評価書の繰り返しパスを全ラウンドに、そのまま適用した値

CRYPTREC
Cryptography Research and Evaluation Committees

192/256ビットの場合の安全性評価
差分特性確率の上界(2)

アルゴリズム＼鍵長	攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数		
	128ビット	192ビット	256ビット
AES	4/10	7/12	8/14
Camellia	12/18	17/24	22/24
CIPHERUNICORN-A	12/16	-	-
Hierocrypt-3	2/6	4/7	4/8
SC2000	(13/19)	(21/22)	-

()内の値は、自己評価書の繰り返しパスを全ラウンドに、そのまま適用した値

CRYPTREC
Cryptography Research and Evaluation Committees

192/256ビットの場合の安全性評価
差分特性確率の関する結論

AES、Camellia、Hierocrypt-3

- 特に問題は見つかっていない。

CIPHERUNICORN-A

- 差分特性確率は鍵長によらず一定
- 256ビット鍵の場合、鍵長から期待される計算量的安全性を確認できなかった。

SC2000

- 自己評価書の結果を全ラウンドに適用

⇒ 128ビット鍵では2^{-187}、192/256ビット鍵では2^{-215}の差分パスが存在

- 256ビット鍵では、関連鍵攻撃まで許容した場合、乱数識別攻撃の可能性あり

CRYPTREC
Cryptography Research and Evaluation Committees

192/256ビットの場合の安全性評価
線形特性確率の上界(1)

アルゴリズム＼鍵長	線形特性確率の上界		
	128ビット	192ビット	256ビット
AES	2^{-330}	2^{-450}	2^{-480}
Camellia	2^{-204}	2^{-276}	192ビット鍵と同じ
CIPHERUNICORN-A	2^{-171}	128ビット鍵と同じ	128ビット鍵と同じ
Hierocrypt-3	2^{-450}	2^{-480}	2^{-600}
SC2000	$(2^{-162.98})$	$(2^{-201.81})$	192ビット鍵と同じ

()内の値は、自己評価書の繰り返しパスを全ラウンドに、そのまま適用した値

CRYPTREC
Cryptography Research and Evaluation Committees

192/256ビットの場合の安全性評価
線形特性確率の上界(2)

アルゴリズム＼鍵長	攻撃計算量が鍵全数探索を上回るラウンド数／暗号化ラウンド数		
	128ビット	192ビット	256ビット
AES	4/10	7/12	8/14
Camellia	12/18	17/24	23/24
CIPHERUNICORN-A	12/16	-	-
Hierocrypt-3	2/6	4/7	4/8
SC2000	(16/19)	(22/22)	-

()内の値は、自己評価書の繰り返しパスを全ラウンドに、そのまま適用した値

CRYPTREC
Cryptography Research and Evaluation Committees

192/256ビットの場合の安全性評価
線形特性確率の関する結論（1）

AES、Camellia、Hierocrypt-3

- 特に問題は見つかっていない。

SC2000

- 自己評価書の繰り返しパスを全ラウンドにそのまま適用
- 256ビット鍵では、関連鍵攻撃まで許容した場合、乱数識別攻撃の可能性あり

192/256ビットの場合の安全性評価
線形特性確率の関する結論（2）

CIPHERUNICORN-A

- 線形特性確率は鍵長によらず一定
- ラウンド関数の構造が複雑

⇒ 簡易な構造に変形したmF関数を用いて評価

- 192/256ビット鍵の場合、鍵長から期待される計算量的安全性を確認できず

次年度の活動

- リスト改訂に向けて
  - 各暗号技術の安全性評価を継続
  - 各暗号技術に求める安全性要件の基準作り
    例えば、ブロック暗号の場合 …
    - 関連鍵攻撃への耐性、192/256ビット鍵の場合の安全性をどの程度考慮に入れるかなど