暗号運用委員会活動報告

委員長　松本 勉

横浜国立大学

CRYPTREC
Cryptography Research and Evaluation Committees

目次

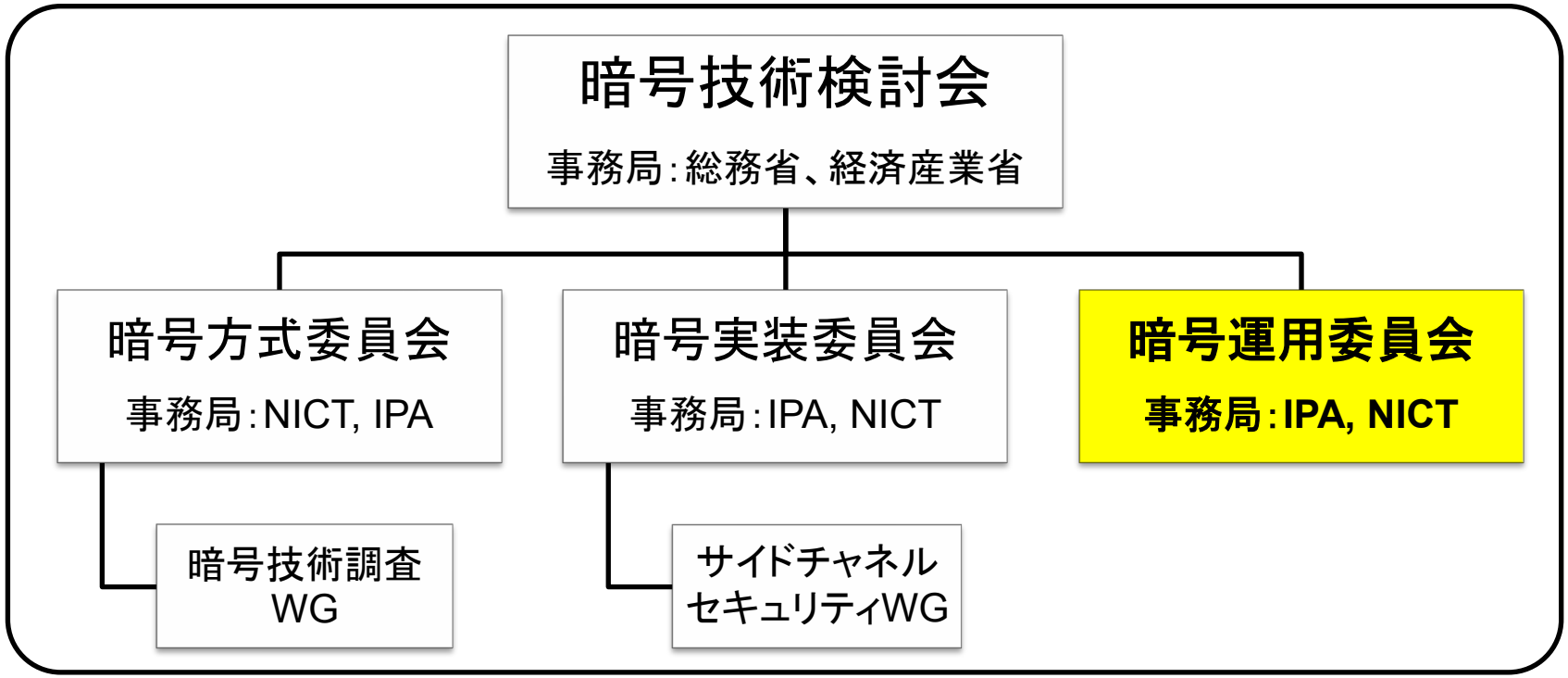
CRYPTREC
Cryptography Research and Evaluation Committees

0. 暗号運用委員会の概要

暗号運用委員会の紹介

2009年度に新設された委員会

電子政府システム等で利用される電子政府推奨暗号の適切な運用について、システム設計者・運用者の観点から調査・検討を行う



CRYPTREC
Cryptography Research and Evaluation Committees

2012年度暗号運用委員会委員

委員長	松本　勉	**横浜国立大学** 大学院環境情報研究院
委員	菊池　浩明	**東海大学** 情報通信学部　通信ネットワーク工学科
委員	木村　道弘	**日本情報経済社会推進協会(JIPDEC)** 電子情報利活用推進部
委員	近藤　潤一	**情報処理推進機構** 技術本部　セキュリティセンター
委員	佐藤　直之	**日本ベリサイン株式会社** 社長室
委員	鈴木　雅貴	**日本銀行** 金融研究所　情報技術研究センター
委員	瀧田　佐登子	**Mozilla Japan** 代表理事
委員	手塚　悟	**東京工科大学** コンピュータサイエンス学部
委員	西原　敏夫	**シスコシステムズ合同会社** ボーダレスネットワークシステムズエンジニアリング
委員	半田　富己男	**大日本印刷株式会社** 情報ソリューション事業部　ICカードソフト開発本部
委員	前田　司	**EMCジャパン株式会社** RSA事業本部
委員	松尾　真一郎	**情報通信研究機構** ネットワークセキュリティ研究所
委員	山口　利恵	**産業技術総合研究所** セキュアシステム研究部門　セキュアサービス研究グループ

CRYPTREC
Cryptography Research and Evaluation Committees

2012年度の活動内容

(1) 電子政府推奨暗号の選定基準の検討

2011年度第2回暗号技術検討会において決定された電子政府推奨暗号リストに掲載する暗号技術の選定ルールに基づき、未確定となっている評価基準案の精緻化を行い、具体的な選定基準値（案）を決定する。

(2) 利用実績の調査

新規応募暗号及び現リスト暗号に対して、電子政府推奨暗号リストに掲載する暗号技術を選定する際の評価項目である現状の利用実績についての調査を実施する。なお、調査主体としてはIPAが実施する。

(3) 運用監視暗号リストへの遷移要件に関する基準検討

電子政府推奨暗号リストに掲載されている暗号アルゴリズムの安全性が暗号学会等で低下したことが判明した場合の対応について検討する。

(4) 電子政府推奨暗号の利用促進体制の検討

電子政府推奨暗号リストに掲載される暗号アルゴリズムについて、費用対効果の観点を考慮しつつ、当該暗号アルゴリズムの利用が促進されるような取り組み方法について検討する。

(5) その他

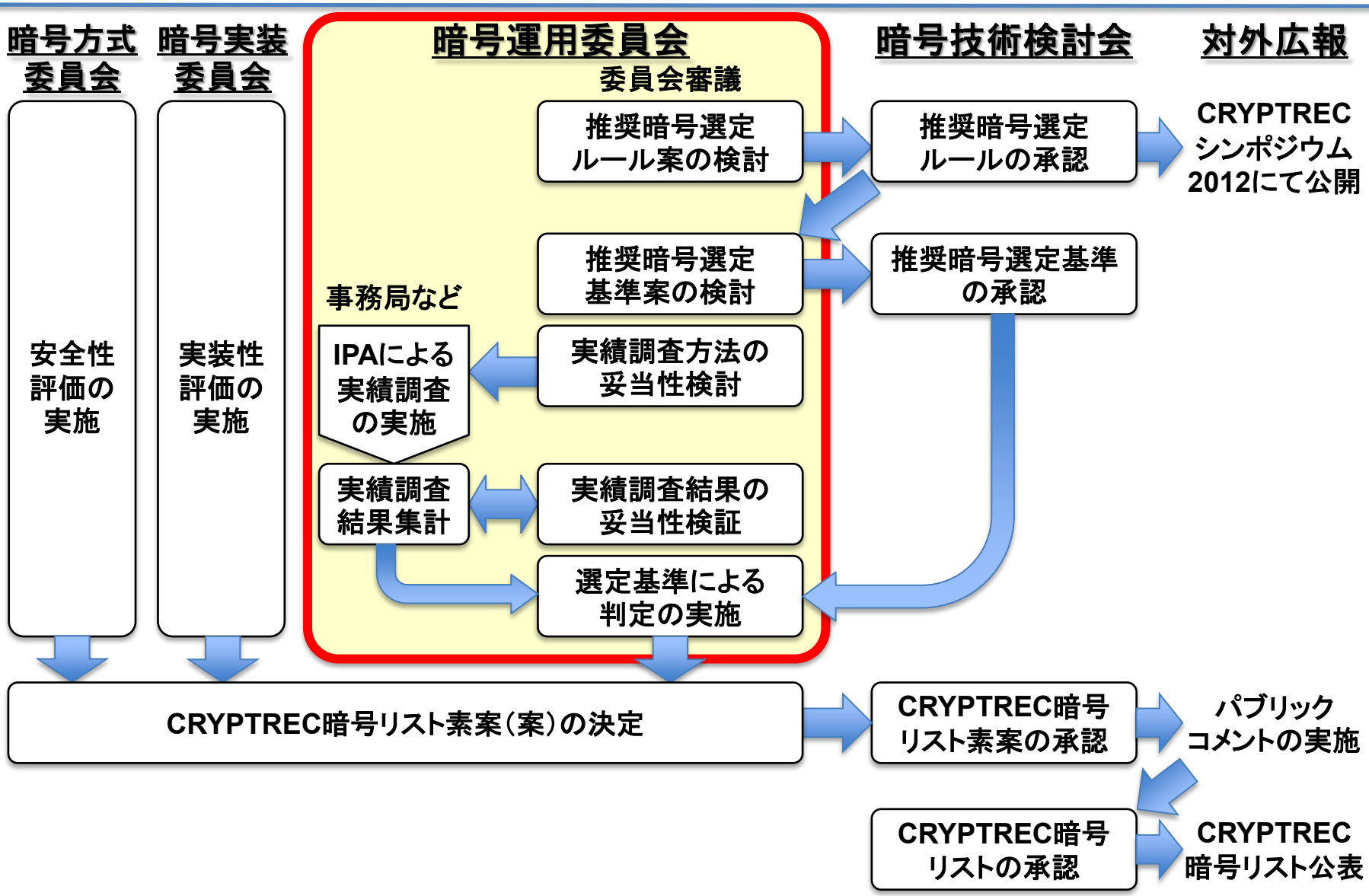
セキュリティ人材育成の観点を含め、CRYPTREC暗号リスト策定に伴う暗号学界への影響と対策等に関する検討を開始する。また、現在移行が進められているRSA1024, SHA-1等の安全性評価について、新たな展開が発生した場合に、暗号運用委員会としてのコンティンジェンシープランに対する寄与の可能性について継続して検討する。

CRYPTREC
Cryptography Research and Evaluation Committees

2012年度の委員会審議状況

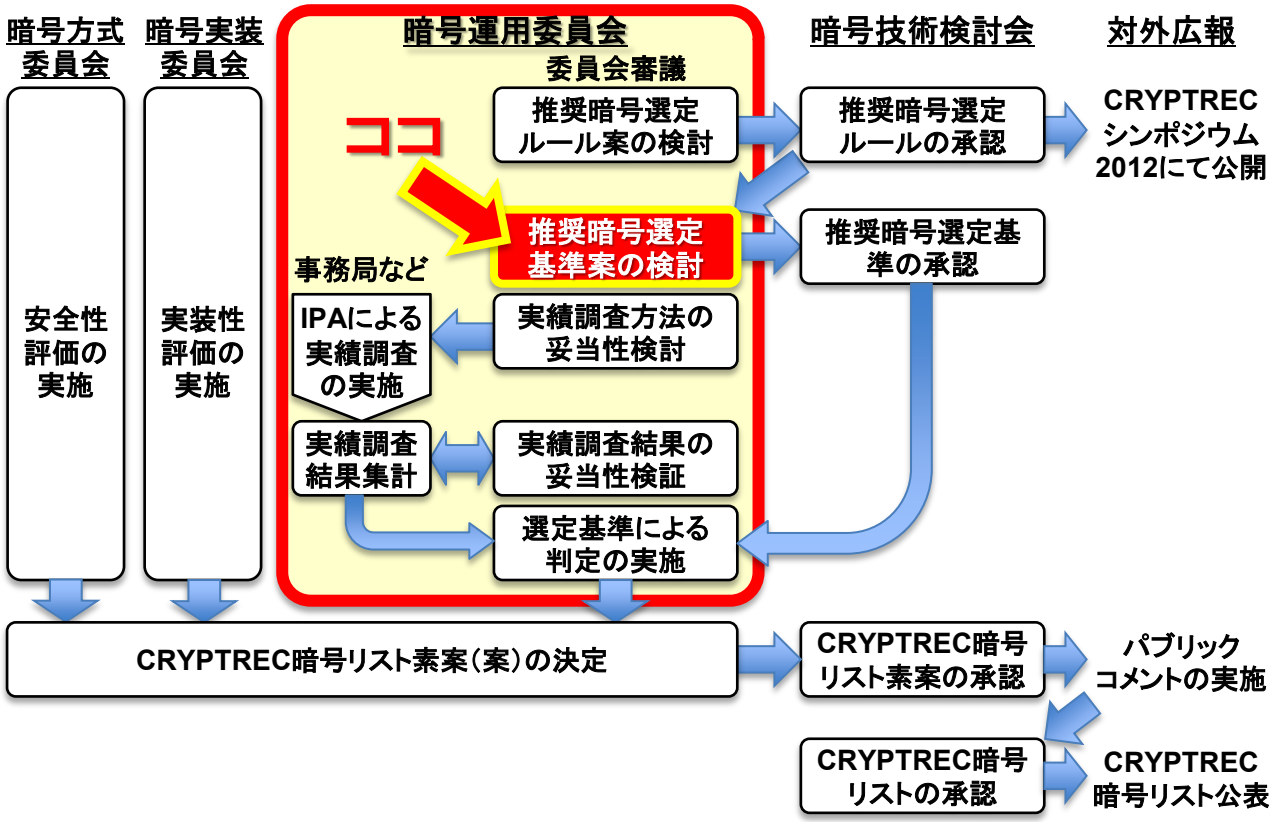
回	開催日時	主な議題
第1回	2012. 6. 8	● 暗号運用委員会活動計画について ● 選定ルールのフレームワークにおける選定基準の検討について ● 利用実績調査について①
第2回	2012. 7. 25	● 選定ルールのフレームワークにおける選定基準（暗号運用委員会案）の決定 **（※2012年度第1回暗号技術検討会に報告）** ● 利用実績調査について② **（※IPAが実施した利用実績調査に反映）**
メール審議	2012. 8. 2 ～ 9. 3	● 第二次選定（総合評価）の個別配点基準の検討について
アドホック	2012. 9. 24	● 利用実績調査報告会
第3回	2012. 10. 4	● 総合評価の個別配点基準（暗号運用委員会案）の決定 ● 選定ルールに基づく暗号運用委員会判定の決定
第1回 合同委員会	2012. 11. 15	● CRYPTREC暗号リスト（案）素案の決定 （※2012年度第2回暗号技術検討会に報告）
第4回	2013. 3. 1	● 次年度以降のCRYPTREC活動の検討に向けた課題整理

CRYPTREC暗号リスト策定の流れ



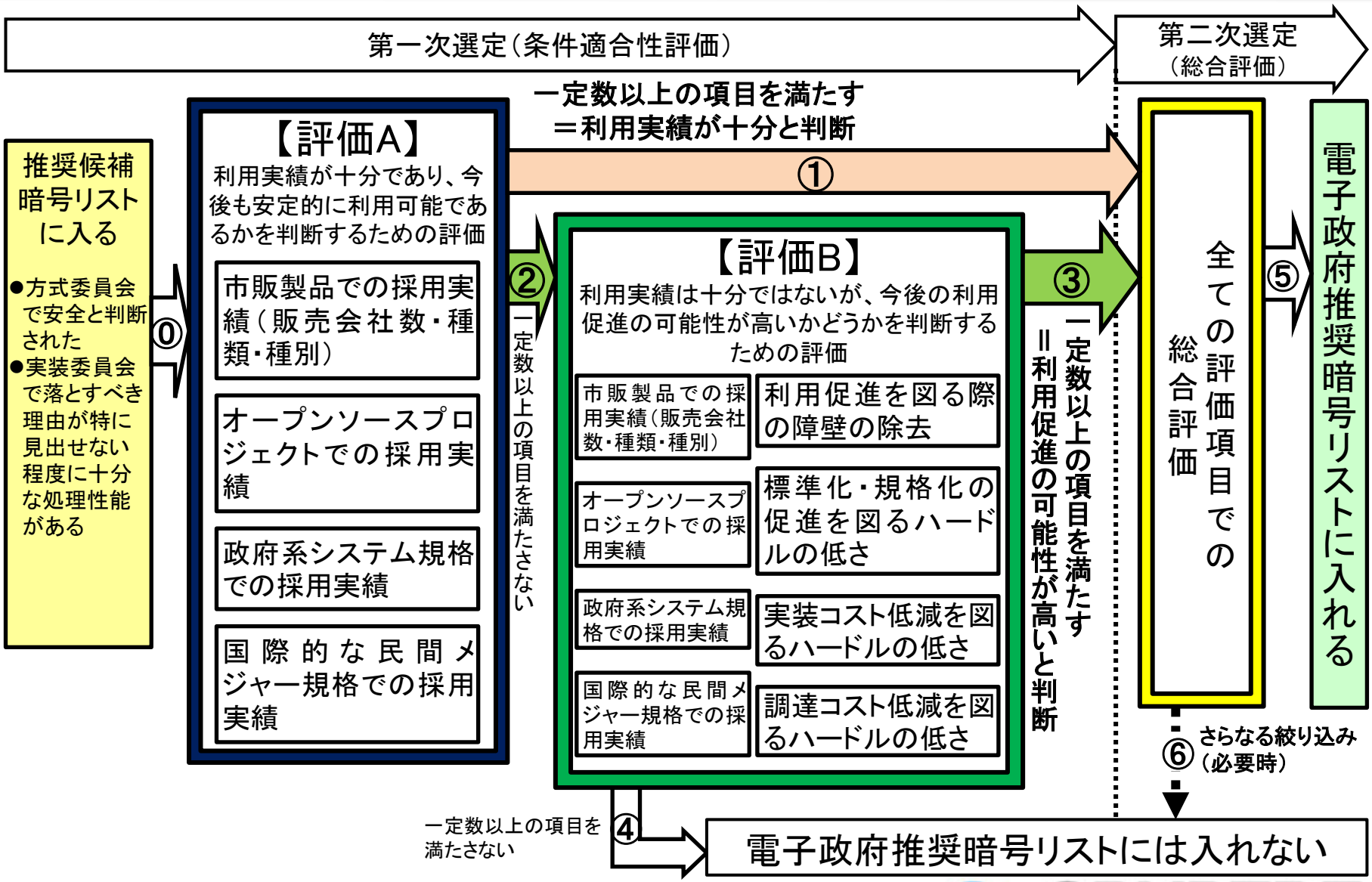
CRYPTREC
Cryptography Research and Evaluation Committees

1. 電子政府推奨暗号の選定基準の審議結果概要



CRYPTREC
Cryptography Research and Evaluation Committees

選定ルールのフレームワーク（2011年度承認）



CRYPTREC
Cryptography Research and Evaluation Committees

推奨暗号リスト選定基準の基本的考え方

推奨暗号の個数を絞り込むための明示的な“選定基準”

- 推奨暗号不選定の理由の明確化

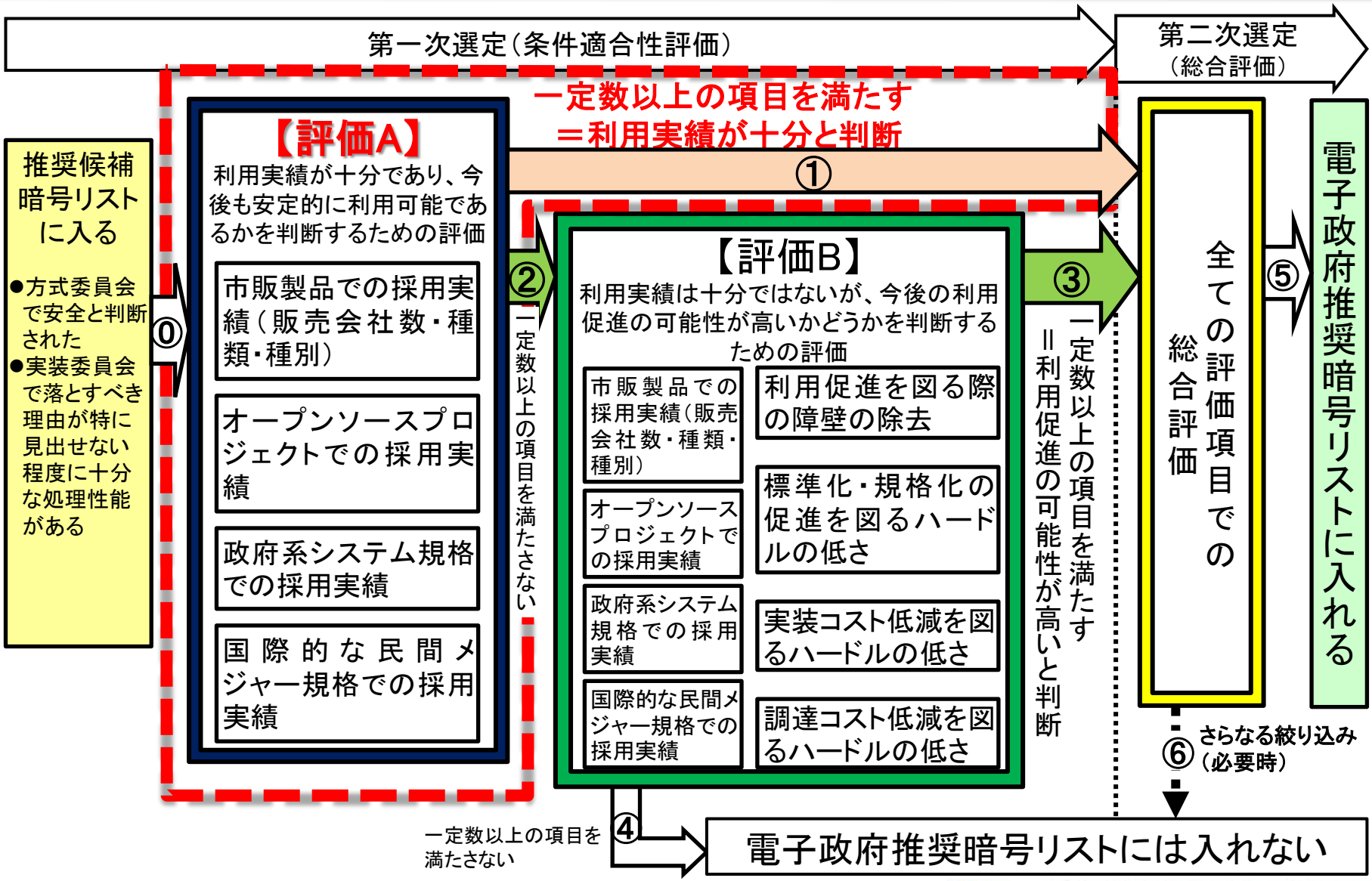
- 利用実績の調査結果には精度上の問題がある程度含まれることは予め織り込んでおく

  ➡ 精度上の問題がある程度含まれていても、推奨暗号の選定・不選定が極力変わらないような選定基準にする

- 推奨暗号の個数を絞り込むための評価として「第二次選定（総合評価）」を利用することは極力避ける

  ➡ 多くの暗号技術が「第一次選定（条件適合性評価）」を通過するような緩い選定基準は極力避ける

評価Aによる選定＝利用実績が十分と判断

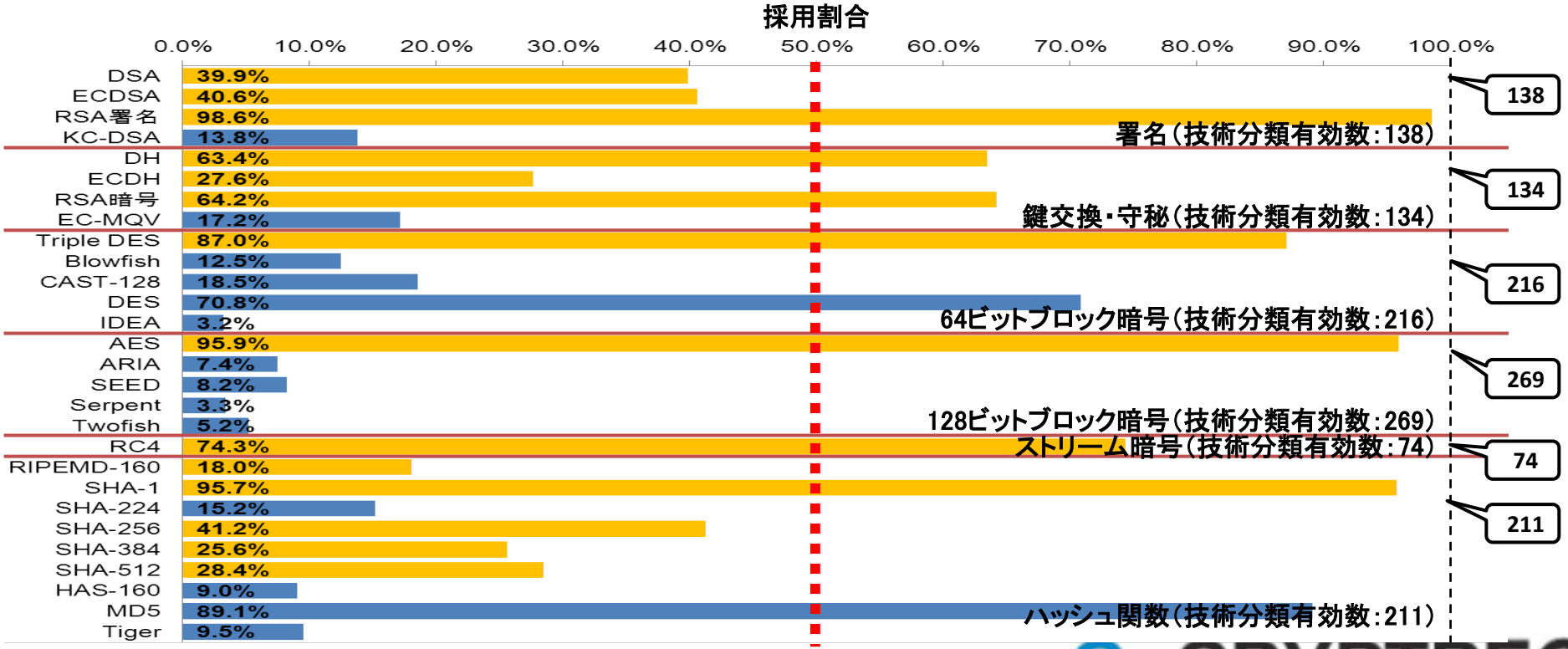


CRYPTREC
Cryptography Research and Evaluation Committees

評価Aにおける各評価項目における選定基準

全項目について「採用割合50%」を閾値として採用

- 「調査対象数のマジョリティ（50%以上）の採用実績があることが望ましい」との見解で一致
- 2009年度調査結果からみて「採用割合50%以上」でも矛盾なし



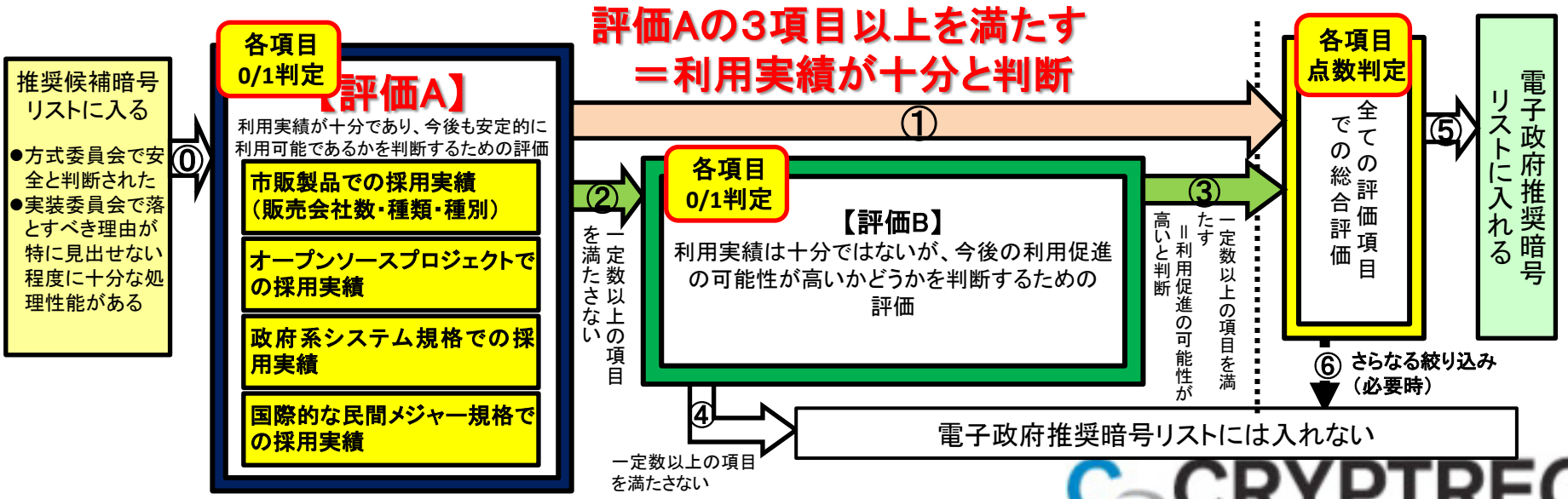
CRYPTREC
Cryptography Research and Evaluation Committees

評価A「利用実績が十分」と判断する閾値

【評価A】 4項目中、「3項目以上」の選定基準を満たす

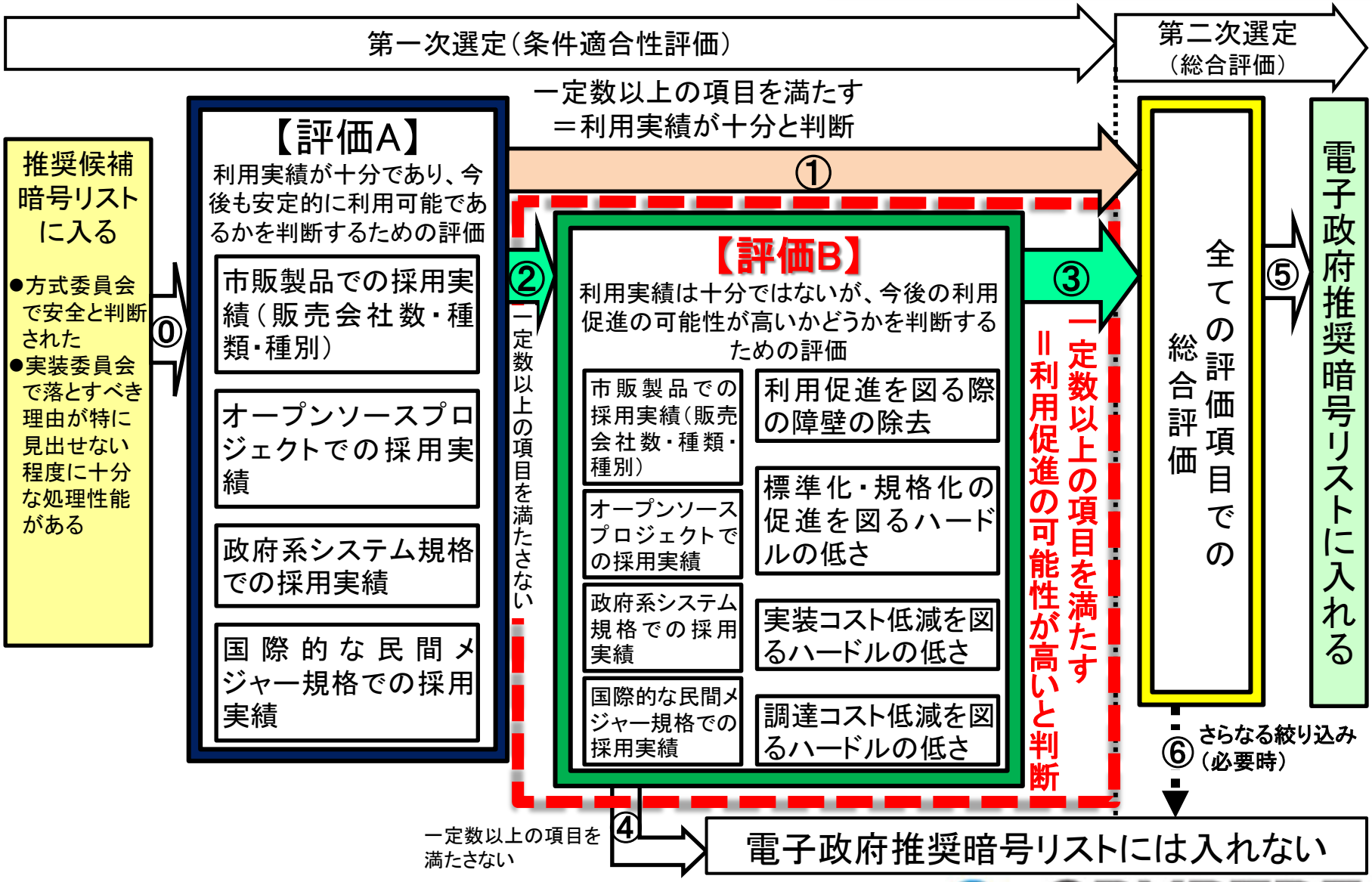
■ できるだけ多くの選定基準を満たすべき、だが・・・

- 「オープンソースを公開しない」場合でも、企業努力で十分に普及させたのならば認めてもよい
- 「政府系システム規格での採用実績」が足らない場合でも、製品・OSSが多数あれば実際には政府調達が可能



CRYPTREC Cryptography Research and Evaluation Committees

評価Bによる選定＝利用促進の可能性高いと判断



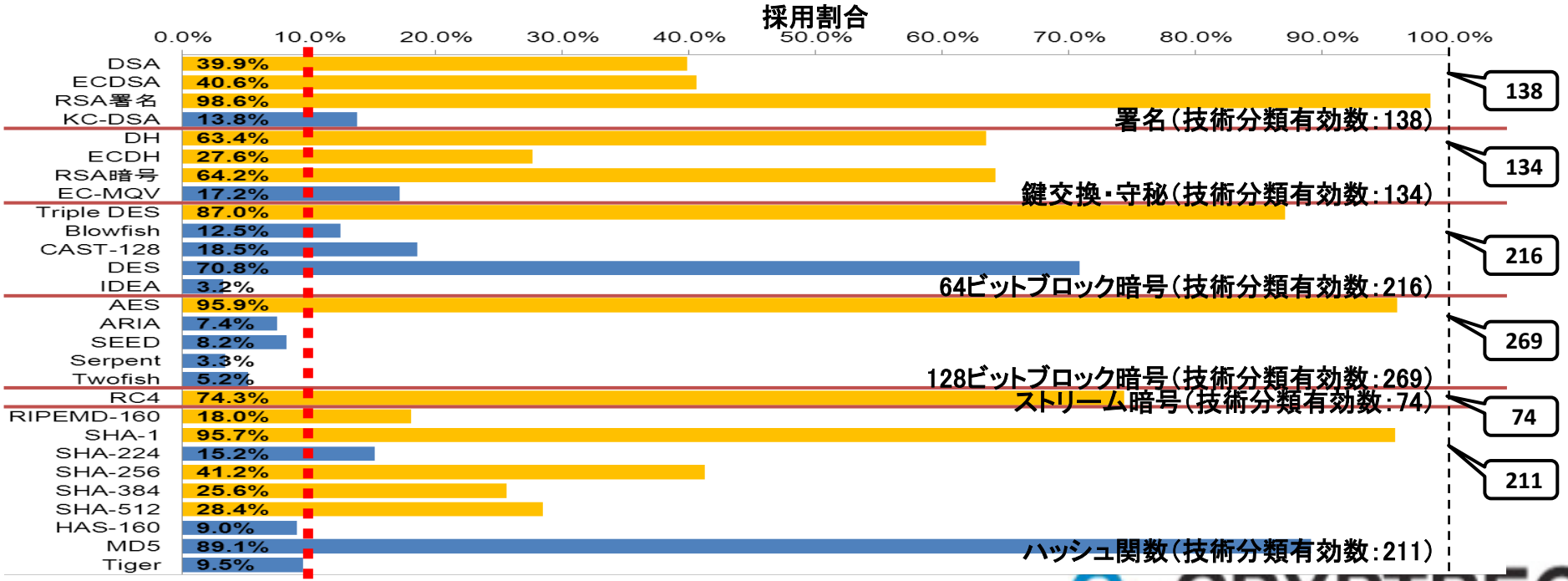
CRYPTREC
Cryptography Research and Evaluation Committees

評価Bにおける各評価項目における選定基準 (1)

「他社利用が進んでいることを確認」することを条件に「採用割合10%」を閾値として採用

■ 今後の標準化推進・利用拡大が期待できる高い閾値

- 「採用割合5%は低すぎる」との見解で一致
- 「他社利用が進んでいることは重要」との見解で一致



CRYPTREC
Cryptography Research and Evaluation Committees

評価Bにおける各評価項目における選定基準 (2)

「市販製品採用実績」以外の選定基準には
「2件以上」かつ「採用割合として10%以上」となる件数を
閾値に採用
（ただし、カテゴリ有効数が4件以下の時に限り、「1件」でもよい）

- **利用実績におけるカテゴリ有効数が少ない点を考慮**
  - 「調査対象に偶然1件選ばれただけで選定基準を満たすと判断されることになるのは危険」との見解で一致。採用割合に関わらず、最低「2件」は必要

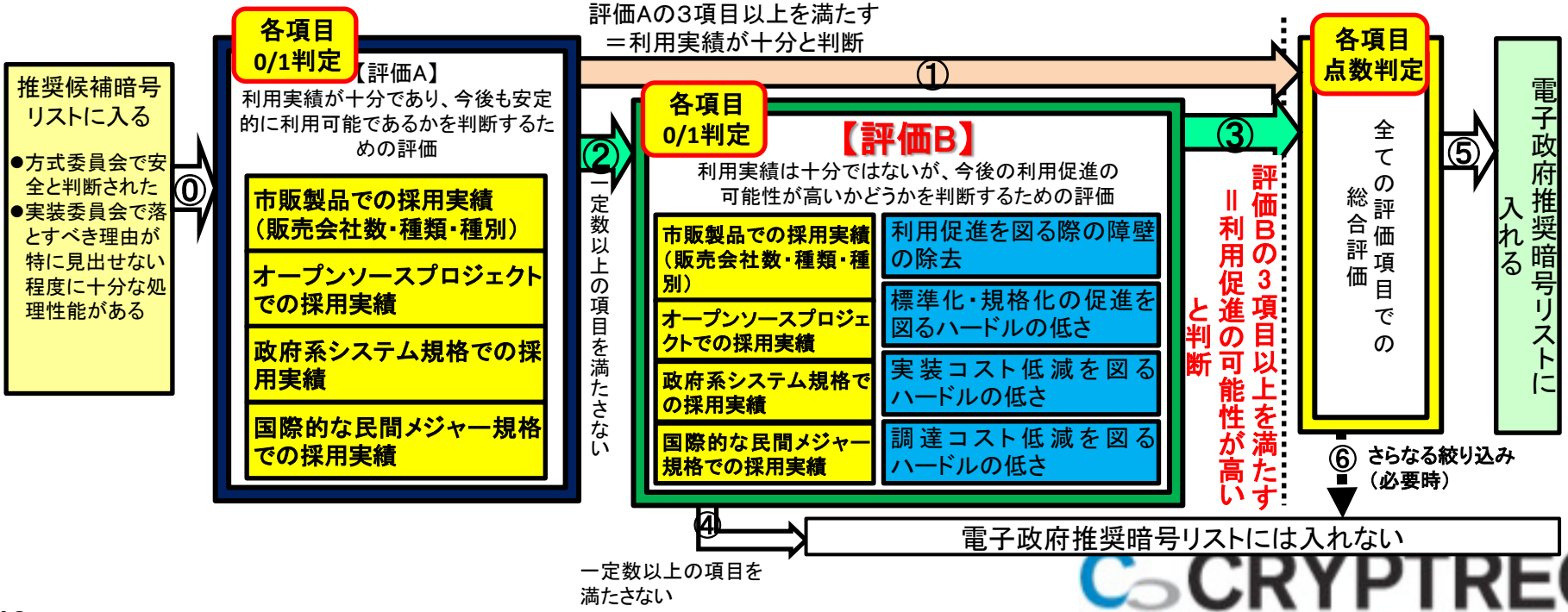
- **評価Aの基準を上回る選定基準にはしない**
  - カテゴリ有効数が4件以下の場合に「2件以上」を条件にすると、評価Aの基準（採用割合50%）を上回る

CRYPTREC
Cryptography Research and Evaluation Committees

評価B「利用促進可能性高い」と判断する閾値

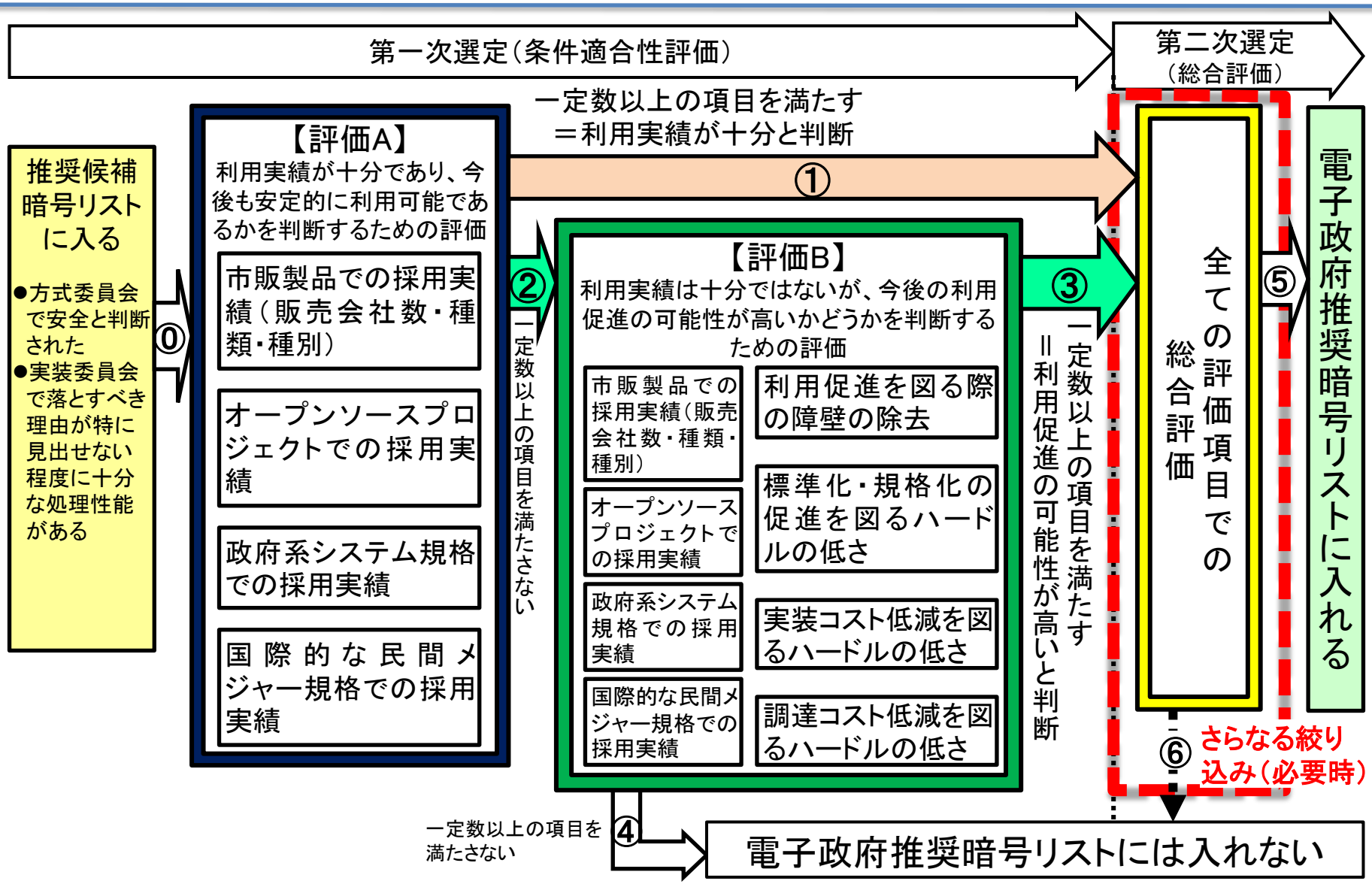
【評価B】 8項目中、「3項目以上」の選定基準を満たす

- 「5項目以上」では、新しい暗号は評価Aを一つも満たせず、評価Bも通過できない可能性が大きい
- 「特許無償化を実施しない」場合でも、企業努力で普及させたのならば認めてもよい



CRYPTREC Cryptography Research and Evaluation Committees

総合評価＝さらなる絞り込みが必要な場合の措置



CRYPTREC
Cryptography Research and Evaluation Committees

総合評価の考え方

■ 目的

総合評価でさらなる絞り込みを実施することになった場合にのみ、絞り込み候補を見極めるために活用

※絞り込みを実施しない場合には個別の採点は行わない

■ 加点基準の考え方

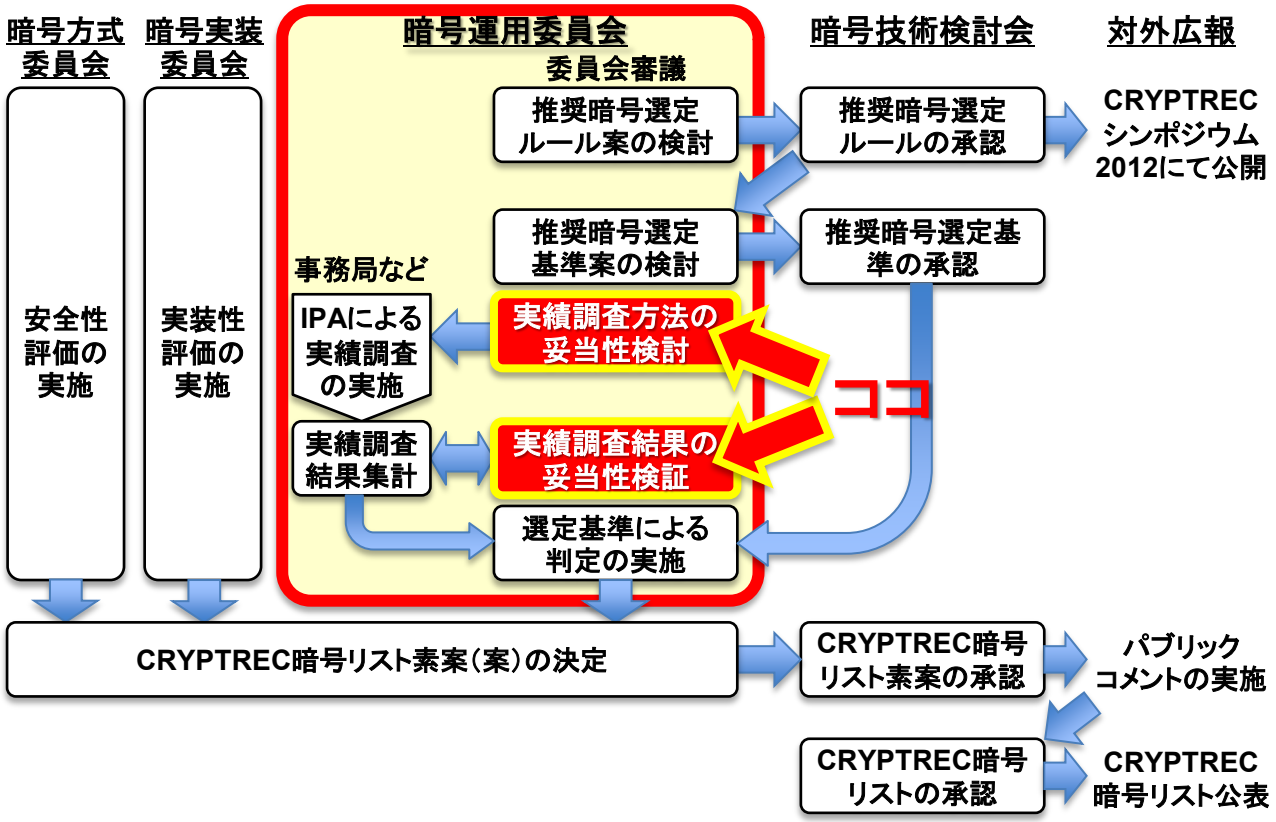
- 得点配分の精緻化よりも、効率よく絞り込み候補が見極められるようなシンプルかつ明快な基準にする
  - 「広く利用され、影響範囲が広いと考えられるグループ」・「中間グループ」・「影響範囲が比較的限定的と考えられるグループ」のような分け方ができればよい
- 「技術的側面」と「非技術的側面」の重要度は同等
- 現状の利用実績だけが理由で著しく有利・不利が生じないような配点バランスを考慮

総合評価の選定基準

評価項目				評価Aを通過		評価Bを通過	
合計				480		540	
技術的側面			安全性についての仕様上のアドバンテージ	240 (50.0%)	100	240 (44.4%)	100
			論文数の多寡によるアドバンテージ		20		20
			実装性能評価		60		60
			実装性能における技術的アピールポイント		60		60
非技術的側面	現状での利用実績		政府系システムでの採用実績	240 (50.0%)	30	240 (44.4%)	30
			市販製品での採用実績		30		30
			オープンソースプロジェクトでの採用実績		30		30
		利用促進手段採用による普及効果	特許ライセンスによる利用促進効果		30		30
			オープンソース公開による利用促進効果				
			政府系システム規格での採用実績		30		30
			国際標準規格での採用実績		30		30
			国際的な民間メジャー規格での採用実績		30		30
			民間の特定団体規格での採用実績		30		30
	利用促進が図られると期待される根拠		利用促進を図る際の障壁の除去			60 (11.1%)	20
			標準化・規格化の促進を図るハードルの低さ				20
			実装コスト低減を図るハードルの低さ				10
			調達コスト低減を図るハードルの低さ				10

CRYPTREC
Cryptography Research and Evaluation Committees

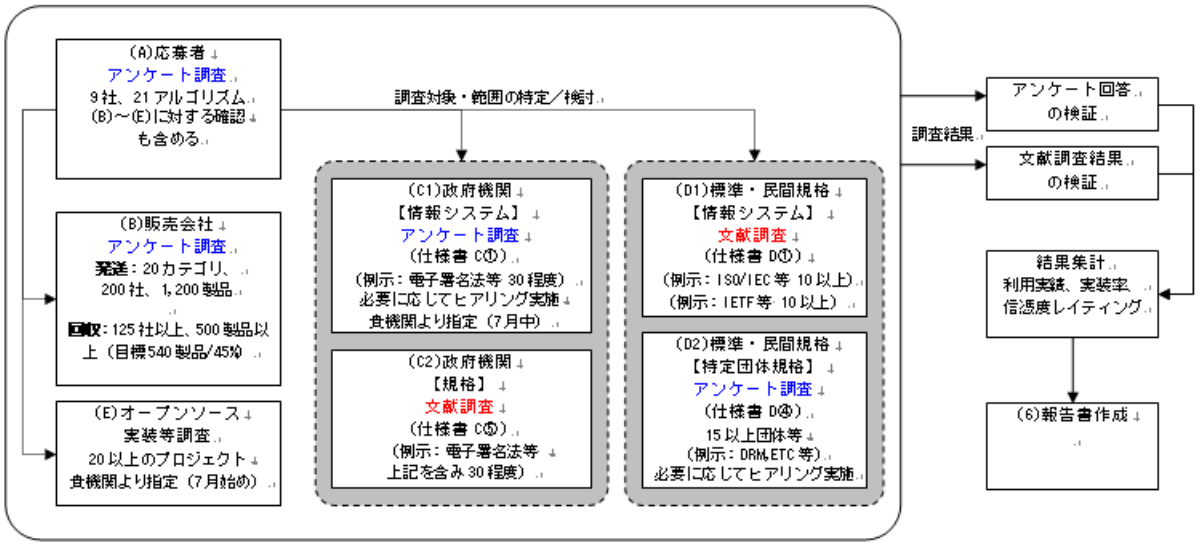
2. 利用実績調査に関する審議結果概要



CRYPTREC
Cryptography Research and Evaluation Committees

調査方法の俯瞰 (1)

- **IPAが実施した「暗号アルゴリズムの利用実績に関する調査」**
  - 調査A：応募者に対するアンケート調査
  - 調査B：市販製品メーカー・販売会社等に対するアンケート調査
  - 調査C：政府系システム・規格に対する調査
  - 調査D：国際標準規格・国際的民間規格・特定団体規格に対するアンケート調査・公開情報調査
  - 調査E：オープンソースプロジェクトに関する調査



暗号運用委員会の助言のもと調査を実施

CRYPTREC
Cryptography Research and Evaluation Committees

調査方法の俯瞰 (2)

■ 調査A

- 全応募者（9社）よりアンケート回答を回収
- 応募暗号以外の利用実績も特定できた情報のみ調査B～Eの有効回答にカウント。それ以外は参考情報扱い

■ 調査B

- 市販製品に関するアンケート調査
  アンケート配布社数：1849、有効回答：会社数127、製品数443
- 公開情報を基にみずほ情報総研が調査
  調査対象：会社数35、製品数90

⇒ そのうち、利用実績評価の基礎データとなった市販製品の総数は469

調査方法の俯瞰 (3)

■ 調査C

- 回答内容については当該府省庁の情報システム課が検証
- システム利用実績: 8府省庁77システム
- 政府系規格:合計12規格(公開情報調査(7規格)含む)

■ 調査D

- 国際標準規格:12
- 国際的民間規格:108(15種類)
- 特定団体規格:アンケート調査(有効回答数:16(3団体))、
  公開情報調査(調査数:8(6団体))

■ 調査E

- オープンソースプロジェクトの最新安定版(調査数:24)

暗号運用委員会の主な助言事項（調査段階）(1)

■ 調査B

- 調査対象に極端な偏りや調査対象漏れが生じないように、暗号製品を区分するカテゴリ20個を設定

1	オペレーティングシステム
2	暗号化ツールキット／ライブラリ
3	アプリケーションソフトウェア
4	ネットワーク装置（無線含む）
5	サーバ
6	ストレージ
7	端末
8	外部記憶装置
9	認証機器
10	システム

11	カード
12	ICチップ
13	ハードウェアセキュリティモジュール
14	複合機・プリンタ
15	情報家電・生活用品
16	センサー
17	消耗品認証
18	サービス
19	特注品・SIシステム
20	その他

- 回答内容の確認方法についての質問項目を設ける

Lev. 1	公開情報等（URL等）に記載されており、当該情報から回答内容を検証可能
Lev. 2	回答内容を検証できる情報を提供してもよい
Lev. 3	NDAを締結すれば、回答内容を検証できる情報を提供してもよい
Lev. 4	回答内容を検証できる情報はあるが、提供はできない
Lev. 5	回答内容を検証できる情報があるかどうか判明していない／確認できない

CRYPTREC
Cryptography Research and Evaluation Committees

暗号運用委員会の主な助言事項（調査段階）(2)

■ 調査D

- 重要な標準化規格の調査漏れが生じないようにするため、調査対象を指定
  - 国際標準化規格

ISO/IEC9796 (Digital signature schemes giving message recovery)
ISO/IEC9797 (Message Authentication Codes (MACs))
ISO/IEC10116 (Modes of operation for an n-bit block cipher)
ISO/IEC10118 (Hash-functions)
ISO/IEC14888 (Digital signatures with appendix)
ISO/IEC18033 (Encryption algorithms)
ISO/IEC19772 (Authenticated encryption)
ISO/IEC29192 (Lightweight cryptography)
ISO/IEC7816 (Identification cards — Integrated circuit cards —)

  - 国際的な民間メジャー規格

名称	調査対象数
IETF TLS	20
IETF IPsec	34
IETF S/MIME, CMS	16
IETF PGP	3
IEEE802.11i	1

名称	調査対象数
RSA PKCS#11	1
EMV	2
3GPP	2
3GPP2	3
OMA	1

CRYPTREC
Cryptography Research and Evaluation Committees

暗号運用委員会の主な助言事項（調査段階）(3)

■ 調査E

- 重要なオープンソースプロジェクトの調査漏れが生じないようにするため、調査対象を指定

カテゴリ		プロジェクト名	バージョン
OS（カーネル）	汎用OS	Linux	3.4.7
		Debian	6.0.5
		FreeBSD	9.0
	組込OS	Android	4.0
アプリケーション開発ツール	言語	Java	SE 7
		Bouncy Castle	(jdk15-17)1.47
		PHP	5.4.5
	開発環境	Subversion	1.7.6
		Eclipse	4.2
	アプリケーションサーバ	Samba	3.6.6
		Tomcat	7.0.29
インターネット	Webサーバ	Apache	2.4.2
	メールサーバ	Qmail	1.06
	電子メール系	Thunderbird	14.0
	ブラウザ	Firefox	14.0.1
		Webkit	r125966

カテゴリ		プロジェクト名	バージョン
暗号化ライブラリ		NSS	3.13.5
		OpenSSL	1.0.1c
		GnuPG	2.0 (2.0.19)
		MCrypt	2.6.8
データベース		MySQL	5.5.25a
		PostgreSQL	9.1.4
アプリケーション	アプリケーション	OpenOffice	3.4.0
	圧縮ツール	7-zip	9.2

CRYPTREC
Cryptography Research and Evaluation Committees

暗号運用委員会の主な助言事項(集計段階) (4)

■ 調査B

- 何らかの手段で回答内容の検証が可能な担保がある信頼度(Lev1～Lev3)の情報のみを活用(総数:469)

Lev 1	公開情報等により回答内容が確認できた	351
Lev 2	回答内容を検証できる情報を提供してもよい	66
Lev 3	NDAを締結すれば、回答内容を検証できる情報を提供してもよい	52
Lev 4	回答内容を検証できる情報はあるが、提供はできない	20
Lev 5	回答内容を検証できる情報があるかどうか判明しなかった	44

■ 調査C

- SSL/TLSまたはIPsecを利用している場合、実装必須暗号アルゴリズムをすべて含める

SSL/TLSを利用しているシステム	RFC2246及びRFC5246で実装必須と指定 (RSAES-PKCS1-v1_5, DH, RSASSA-PKCS1-v1_5, DSA, Triple DES, AES, CBC, SHA-1)
IPsecを利用しているシステム	RFC4835 (ESP, AH)及びRFC4307 (IKE)で実装必須と指定 (DH, Triple DES, AES, CBC, HMAC, SHA-1)

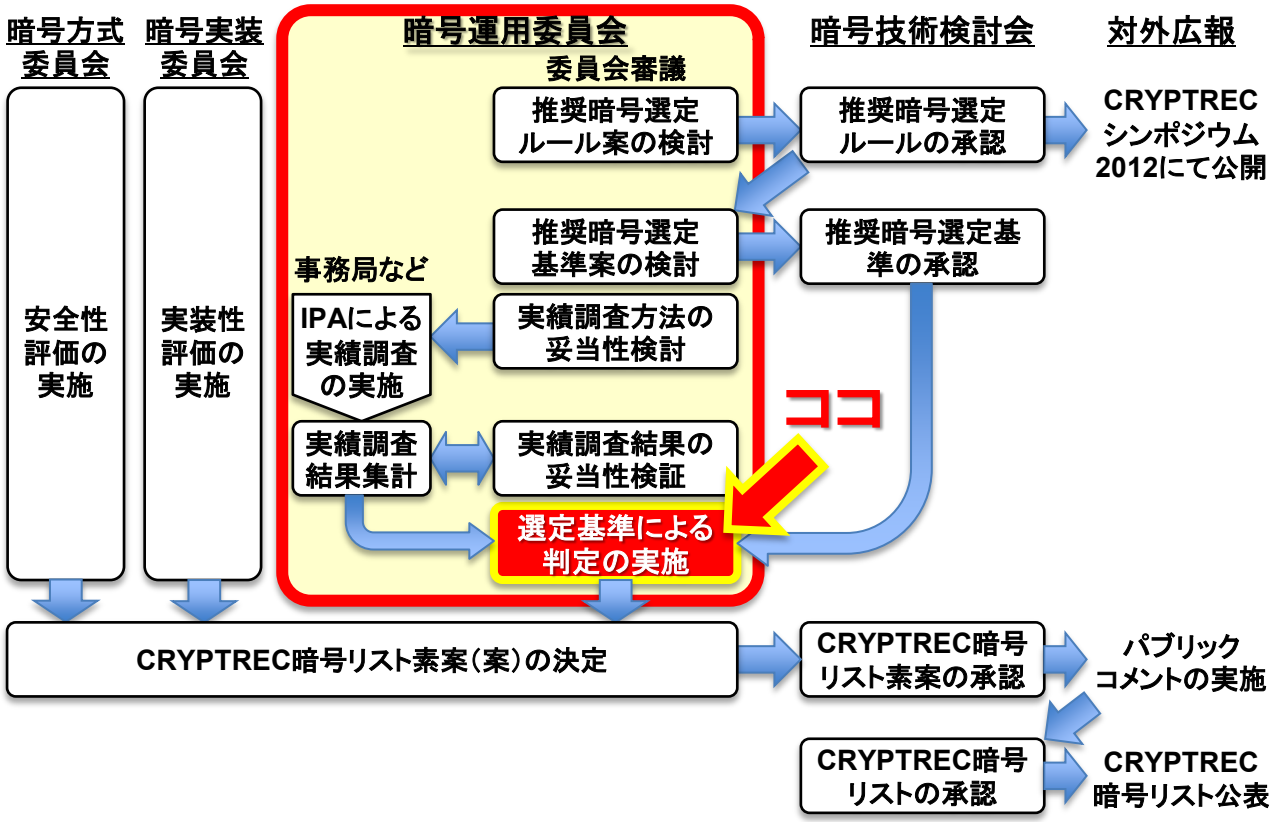
CRYPTREC
Cryptography Research and Evaluation Committees

暗号運用委員会の主な助言事項（集計段階）(5)

■ 調査E

- 特に依存関係が強いオープンソースプロジェクトはまとめて集計
  - Linux と Debian
  - Qmail と OpenSSL
  - Firefox と Thunderbird と NSS
- 応募者からの情報があっても、実装確認できなかったものは当該ソースコードについて対象外
- ダブルカウントを避けるため、他オープンソースプロジェクト管理のソースコードについては対象外

3. 暗号運用委員会担当分の評価Aと評価Bの結果



CRYPTREC
Cryptography Research and Evaluation Committees

評価Aの各評価項目における選定基準

【2012年度第1回暗号技術検討会にて承認】

「（評価A）利用実績が十分にある」と判断するための閾値
下記4項目中、**「3項目以上」**の選定基準を満たす

市販製品での採用実績	**「提案会社・グループ会社以外での採用実績」があり**、**「採用割合として50%以上」**の採用実績があること
オープンソースプロジェクトでの採用実績	**「採用割合として50%以上」**のオープンソースプロジェクトでの採用実績がある ※正式版（リリース版）に採用済みのものだけを取り上げる
政府系システム規格での採用実績	**「採用割合として50%以上」**の政府系システム規格での採用実績がある ※規格化への採用が合意された段階のものまで含める（最終承認待ち）
国際的な民間規格での採用実績	**「採用割合として50%以上」**の国際的な民間規格での採用実績がある ※規格化への採用が合意された段階のものまで含める（最終承認待ち）

IPAが実施した「暗号アルゴリズムの利用実績に関する調査」の調査結果に基づき、判定を行う

CRYPTREC
Cryptography Research and Evaluation Committees

評価Aでの結果まとめ (1)

		判定結果		市販製品採用実績		オープンソースプロジェクト採用実績		政府系システム規格採用実績		国際的な民間規格採用実績	
署名	**DSA**	○	**3/4**	×	(44.7%)	○	(82.4%)	○	(66.7%)	○	(54.8%)
	ECDSA	×	**0/4**	×	(28.2%)	×	(41.2%)	×	(22.2%)	×	(35.5%)
	RSA-PSS	×	**0/4**	×	(20.9%)	×	(23.5%)	×	(11.1%)	×	(16.1%)
	RSASSA-PKCS1-v1_5	○	**4/4**	○	(80.6%)	○	(88.2%)	○	(100.0%)	○	(74.2%)
守秘・鍵共有	**DH**	○	**4/4**	○	(61.5%)	○	(62.5%)	○	(71.4%)	○	(51.3%)
	ECDH	×	**0/4**	×	(23.9%)	×	(43.8%)	×	(14.3%)	×	(25.6%)
	PSEC-KEM	×	**0/4**	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	RSA-OAEP	×	**0/4**	×	(19.7%)	×	(25.0%)	×	(0.0%)	×	(28.2%)
64ビットブロック暗号	CIPHERUNICORN-E	×	**0/4**	×	(2.2%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	Hierocrypt-L1	×	**0/4**	×	(2.6%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	MISTY1	×	**0/4**	×	(1.5%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	(3-key) Triple DES	○	**4/4**	○	(70.2%)	○	(100.0%)	○	(85.7%)	○	(80.8%)
128ビットブロック暗号	**AES**	○	**4/4**	○	(95.4%)	○	(100.0%)	○	(100.0%)	○	(94.2%)
	Camellia	×	**0/4**	×	(13.7%)	×	(46.7%)	×	(25.0%)	×	(17.3%)
	CIPHERUNICORN-A	×	**0/4**	×	(1.1%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	CLEFIA	×	**0/4**	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	Hierocrypt-3	×	**0/4**	×	(0.5%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	SC2000	×	**0/4**	×	(2.2%)	×	(0.0%)	×	(0.0%)	×	(0.0%)

凡例：（判定結果） ○ 評価Aを満たす（総合評価に進む） × 評価Aを満たしていない（評価Bに進む）
（根拠データ） ○ 採用実績が選定基準を満たす × 採用実績が選定基準を満たしていない

CRYPTREC
Cryptography Research and Evaluation Committees

評価Aでの結果まとめ (2)

		判定結果		市販製品採用実績		オープンソースプロジェクト採用実績		政府系システム規格採用実績		国際的な民間規格採用実績	
ストリーム暗号	Enocoro-128v2	×	0/4	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	KCipher-2	×	0/4	×	(10.2%)	×	(0.0%)	×	(33.3%)	×	(0.0%)
	MUGI	×	0/4	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
	MULTI-S01	×	0/4	×	(3.8%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
ハッシュ関数	SHA-256	×	2/4	○	(61.7%)	○	(77.8%)	×	(36.4%)	×	(43.4%)
	SHA-384	×	1/4	×	(34.7%)	○	(66.7%)	×	(18.2%)	×	(37.7%)
	SHA-512	×	1/4	×	(37.6%)	○	(66.7%)	×	(18.2%)	×	(22.6%)
暗号利用モード（秘匿）	**CBC**	○	4/4	○	(82.7%)	○	(100.0%)	○	(100.0%)	○	(84.0%)
	CFB	×	1/4	×	(20.5%)	○	(52.9%)	×	(0.0%)	×	(16.0%)
	CTR	×	0/4	×	(23.7%)	×	(35.3%)	×	(0.0%)	×	(34.0%)
	OFB	×	0/4	×	(17.3%)	×	(47.1%)	×	(16.7%)	×	(16.0%)
暗号利用モード（認証付秘匿）	CCM	×	0/4	×	(9.6%)	×	(23.5%)	×	(0.0%)	×	(22.0%)
	GCM	×	0/4	×	(11.5%)	×	(29.4%)	×	(0.0%)	×	(32.0%)
メッセージ認証コード	CMAC	×	1/4	×	(7.5%)	×	(33.3%)	○	(50.0%)	×	(12.8%)
	HMAC	○	4/4	○	(82.1%)	○	(100.0%)	○	(50.0%)	○	(87.2%)
	PC-MAC-AES	×	0/4	×	(0.0%)	×	(0.0%)	×	(0.0%)	×	(0.0%)
エンティティ認証	ISO/IEC9798-2	×	0/4	×	(24.6%)	ー	該当なし	×	(0.0%)	ー	該当なし
	ISO/IEC9798-3	×	1/4	×	(10.1%)	ー	該当なし	○	(100.0%)	ー	該当なし
	ISO/IEC9798-4	×	0/4	×	(1.4%)	ー	該当なし	×	(0.0%)	ー	該当なし

評価Bの各評価項目における選定基準 (1)

【2012年度第1回暗号技術検討会にて承認】

「(評価B)利用促進の可能性が高い」と判断するための閾値(Y)
下記8項目中、**「3項目以上」**の選定基準を満たす

評価A基準	市販製品での採用実績			「提案会社・グループ会社以外での採用実績」があり、「採用割合として50%以上」の採用実績があること
	オープンソースプロジェクトでの採用実績			「採用割合として50%以上」のオープンソースプロジェクトでの採用実績がある ※正式版(リリース版)に採用済みのものだけを取り上げる
	政府系システム規格での採用実績			「採用割合として50%以上」の政府系システム規格での採用実績がある ※規格化への採用が合意された段階のものまで含める(最終承認待ち)
	国際的な民間規格での採用実績			「採用割合として50%以上」の国際的な民間規格での採用実績がある ※規格化への採用が合意された段階のものまで含める(最終承認待ち)
追加基準	利用促進を図る際の障壁の除去			**特許無償ライセンスの付与(契約有無は問わない)** ● 特許なし、もしくは契約不要の特許無償ライセンス許諾 ● 非差別的無償許諾契約に基づく無償ライセンス
	標準化・規格化の促進を図るハードルの低さ	OR条件	技術的アピールポイント	方式委員会、又は、実装委員会により**技術的アピールポイントがあると認められる**
			標準化等のアピールポイント	「政府系システム規格」「国際標準規格」「国際的な民間規格」「特定団体規格」のいずれかの規格において、**「2件以上」かつ「採用割合として10%以上」となる件数**での採用が同意されていること ※ただし、カテゴリ有効数が4件以下の時に限り、「1件」でもよいこととする
			採用実績のアピールポイント	以下のいずれかの条件を満たしている ● オープンソースプロジェクトで**「2件以上」かつ「採用割合として10%以上」となる件数**での採用があること ● 市販製品で、**「提案会社・グループ会社以外での採用実績」があり**、「**採用割合として10%以上」となる件数**の採用実績があること

CRYPTREC
Cryptography Research and Evaluation Committees

評価Bの各評価項目における選定基準 (2)

追加基準	実装コスト低減を図るハードルの低さ	OR条件	採用実績のアピールポイント	OSや暗号モジュール（ライブラリやチップなど：市販製品調査カテゴリ#1, #2, #11, #12, #13）として使える市販製品において、**「提案会社・グループ会社以外での採用実績」があり、「2件以上」かつ「採用割合として10%以上」となる件数**の採用実績があること
			オープンソースのアピールポイント	暗号モジュール（OSカーネル及び暗号化ライブラリ）として使えるオープンソースプロジェクトにおいて、**「2件以上」かつ「採用割合として10%以上」となる件数**の採用実績があること ※ただし、カテゴリ有効数が4件以下の時に限り、「1件」でもよいこととする
	調達コスト低減を図るハードルの低さ		採用実績のアピールポイント	以下のいずれかの条件を満たしている ● 市販製品で、**「提案会社・グループ会社以外での採用実績」があり、「採用割合として10%以上」となる件数**の採用実績があること ● 政府系システムで実際に**「2件以上」かつ「採用割合として10%以上」となる件数**での採用実績があること

- 技術的アピールポイントに関わる評価項目は、暗号方式委員会及び暗号実装委員会が独自に判定を行う
- 知的財産権に関わる評価項目は、2012年9月30日時点における応募会社各社の特許ライセンス宣誓を基に判定を行う
  ※応募会社各社に特許ライセンス宣誓の確認
- 利用実績に関わる評価項目は、IPAが実施した「暗号アルゴリズムの利用実績に関する調査」の調査結果に基づき、判定を行う

CRYPTREC
Cryptography Research and Evaluation Committees

評価Bでの結果まとめ (1)

		判定結果↓ / 判定根拠データ→		市販製品採用実績	オープンソースプロジェクト採用実績	政府系システム規格採用実績	国際的な民間規格採用実績	利用促進を図る際の障壁除去	標準化・規格化の促進を図るハードルの低さ	実装コスト低減を図るハードルの低さ	調達コスト低減を図るハードルの低さ
署名	**ECDSA**	○	**3/8**	×	×	×	×	×	○	○	○
	RSA-PSS	○	**4/8**	×	×	×	×	○	○	○	○
守秘・鍵共有	**ECDH**	○	**3/8**	×	×	×	×	×	○	○	○
	PSEC-KEM	×	**2/8**	×	×	×	×	○	○	×	×
	RSA-OAEP	○	**4/8**	×	×	×	×	○	○	○	○
64ビットブロック暗号	CIPHERUNICORN-E	×	**1/8**	×	×	×	×	×	○	×	×
	Hierocrypt-L1	×	**1/8**	×	×	×	×	×	○	×	×
	MISTY1	×	**2/8**	×	×	×	×	○	○	×	×
128ビットブロック暗号	**Camellia**	○	**4/8**	×	×	×	×	○	○	○	○
	CIPHERUNICORN-A	×	**1/8**	×	×	×	×	×	○	×	×
	CLEFIA	×	**1/8**	×	×	×	×	×	○	×	×
	Hierocrypt-3	×	**1/8**	×	×	×	×	×	○	×	×
	SC2000	×	**1/8**	×	×	×	×	×	○	×	×

凡例：（判定結果） ○ 評価Bを満たす（総合評価に進む） × 評価Bを満たしていない
（根拠データ） ○ 結果が選定基準を満たす × 結果が選定基準を満たしていない

CRYPTREC
Cryptography Research and Evaluation Committees

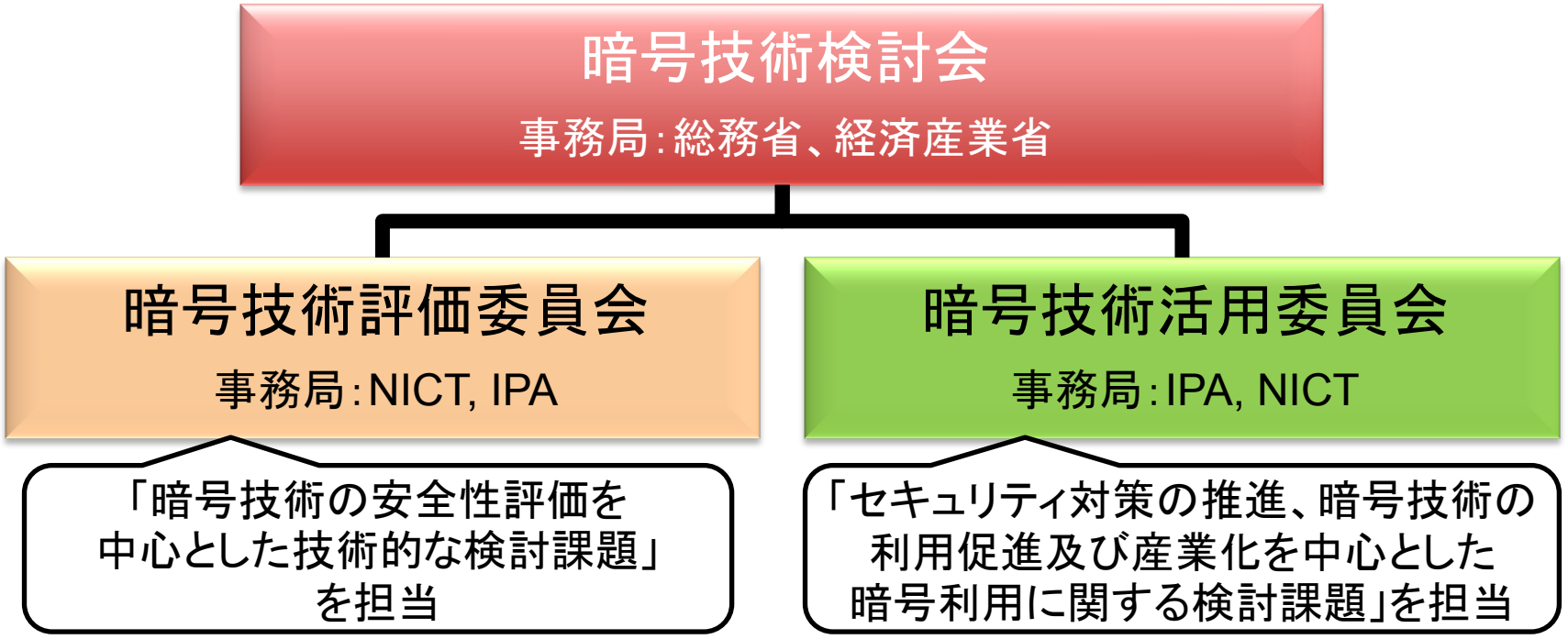
評価Bでの結果まとめ (2)

		判定結果		市販製品採用実績	オープンソースプロジェクト採用実績	政府系システム規格採用実績	国際的な民間規格採用実績	利用促進を図る際の障壁除去	標準化・規格化の促進を図るハードルの低さ	実装コスト低減を図るハードルの低さ	調達コスト低減を図るハードルの低さ
		判定根拠データ→									
ストリーム暗号	Enocoro-128v2	×	1/8	×	×	×	×	×	○	×	×
	KCipher-2	○	3/8	×	×	×	×	○	○	×	○
	MUGI	×	2/8	×	×	×	×	○	○	×	×
	MULTI-S01	×	1/8	×	×	×	×	×	○	×	×
ハッシュ関数	**SHA-256**	○	6/8	○	○	×	×	○	○	○	○
	SHA-384	○	5/8	×	○	×	×	○	○	○	○
	SHA-512	○	5/8	×	○	×	×	○	○	○	○
暗号利用モード（秘匿）	**CFB**	○	5/8	×	○	×	×	○	○	○	○
	CTR	○	4/8	×	×	×	×	○	○	○	○
	OFB	○	4/8	×	×	×	×	○	○	○	○
暗号利用モード（認証付秘匿）	**CCM**	○	3/8	×	×	×	×	○	○	○	×
	GCM	○	4/8	×	×	×	×	○	○	○	○
メッセージ認証コード	**CMAC**	○	4/8	×	×	○	×	○	○	○	×
	PC-MAC-AES	×	1/8	×	×	×	×	×	○	×	×
エンティティ認証	**ISO/IEC9798-2**	○	3/8	×	–	×	–	×	○	○	○
	ISO/IEC9798-3	○	3/8	×	–	○	–	×	○	×	○
	ISO/IEC9798-4	×	1/8	×	–	×	–	×	○	×	×

CRYPTREC
Cryptography Research and Evaluation Committees

4. 今後のCRYPTREC活動に向けての課題整理

CRYPTREC新体制



■暗号技術活用委員会での検討項目

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）

② 暗号技術の利用状況に係る調査及び必要な対策の検討等

③ 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術活用委員会への引き継ぎ課題①

■暗号政策に関する中長期的視点からの取り組み

- 「電子政府システムを安全に維持していくために、ビジネスとは関係なく日本として行うべきこと」と「セキュリティ産業の競争力強化策として行うべきこと」を分けて検討すべき
- 暗号政策上の課題の構造がどのようになっているのかを最初に時間をかけて検討すべき

■暗号利用促進によるセキュリティ産業の競争力強化

- 暗号がないと色々なことができないのは事実だが、暗号だけで成り立っているビジネスもほとんどない。現状を一度俯瞰してからどうするかを組み立てるべき
- 海外を含め、暗号技術でうまくビジネスにつながっているモデルケースを調べてみるべき

暗号技術活用委員会への引き継ぎ課題②

■暗号人材育成

- システムを安全に動かしていく人材にとって、暗号についての必要な知識やスキルがどういうものかを検討すべき
- 社会インフラ系や制御系システムではITを使わざるを得ないが、暗号には馴染みが薄い。そういったインフラ系を支えている人たちに暗号利用の考え方を伝えていくのは今後の日本の産業界にとって非常に重要である

■国際標準化WGの設置

- 主に日本から提案する暗号技術の横断的な国際標準化活動の取組を支援・意見交換する場として設置を計画中
  - 各標準化団体における交渉ノウハウや課題を蓄積
  - 暗号提案の効率的な横展開を図る体制を構築
- 暗号標準規格を作る側だけでなく、暗号標準規格を参照する側（組込む側・使う側）もメンバになっていただくべき

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術活用委員会への引き継ぎ課題③

■暗号技術の普及促進・理解促進へ取り組み

- 適切な暗号利用に対する助言や、脆弱性に対する公的な調査ができる体制についても検討すべき
- 暗号アルゴリズムだけに限らず、Web脆弱性やSNSでの攻撃など、暗号がらみで社会にインパクトがある事例も調査対象に含めるべき。例えば、USENIXなどでの動向

■運用ガイドラインの整備

- 「鍵管理」についてガイドラインを整備すべき。本来、暗号は鍵管理の安全性に頼っているはずなのに、「そもそも鍵管理が何か」すらよく理解されていないのが現状ではないか
- ガイドラインは想定読者の立場を考慮して記述すべき。現状のリストガイドの記述レベルでは、暗号をよく理解している読者しか読みこなせない