CRYPTRECシンポジウム2012
暗号運用委員会報告

暗号運用委員会事務局

CRYPTREC
Cryptography Research and Evaluation Committees

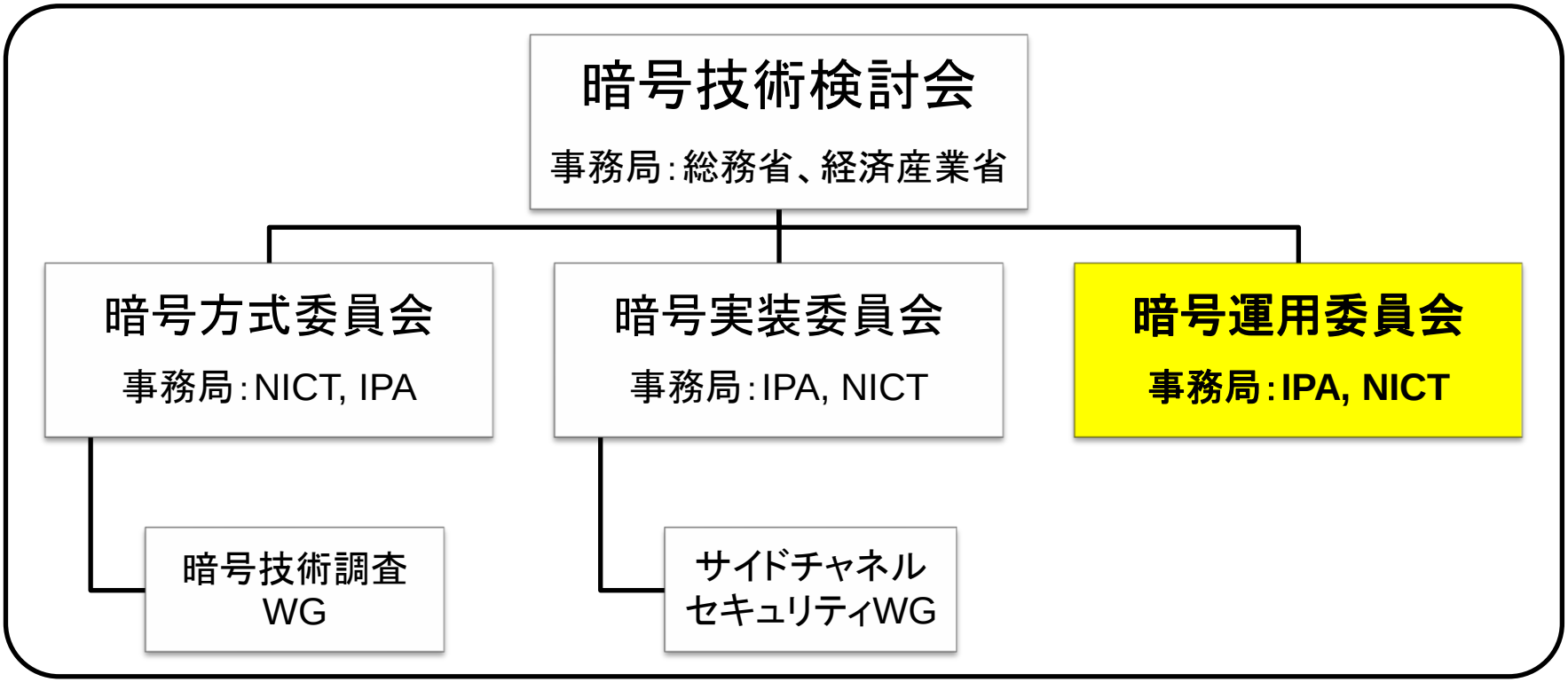
目次

- 暗号運用委員会の紹介
- 2011年度暗号運用委員会の成果概要と今後の予定
- 2011年度暗号運用委員会での議論の方針
- 2011年度活動成果の詳細

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

2011～2012年度暗号運用委員会委員

【主な議題】

(1) 電子政府推奨暗号選定のための選考基準の検討

- 次期推奨暗号リストに掲載する暗号技術選定のための評価項目の検討
- 次期推奨暗号リストに掲載する暗号技術の選定ルールの考え方についての検討
- 選考基準案についての検討

(2) 電子政府推奨暗号の利用促進体制の検討

- 次期奨暗号リストに掲載される暗号技術の利用促進に向けた取り組み方法についての検討

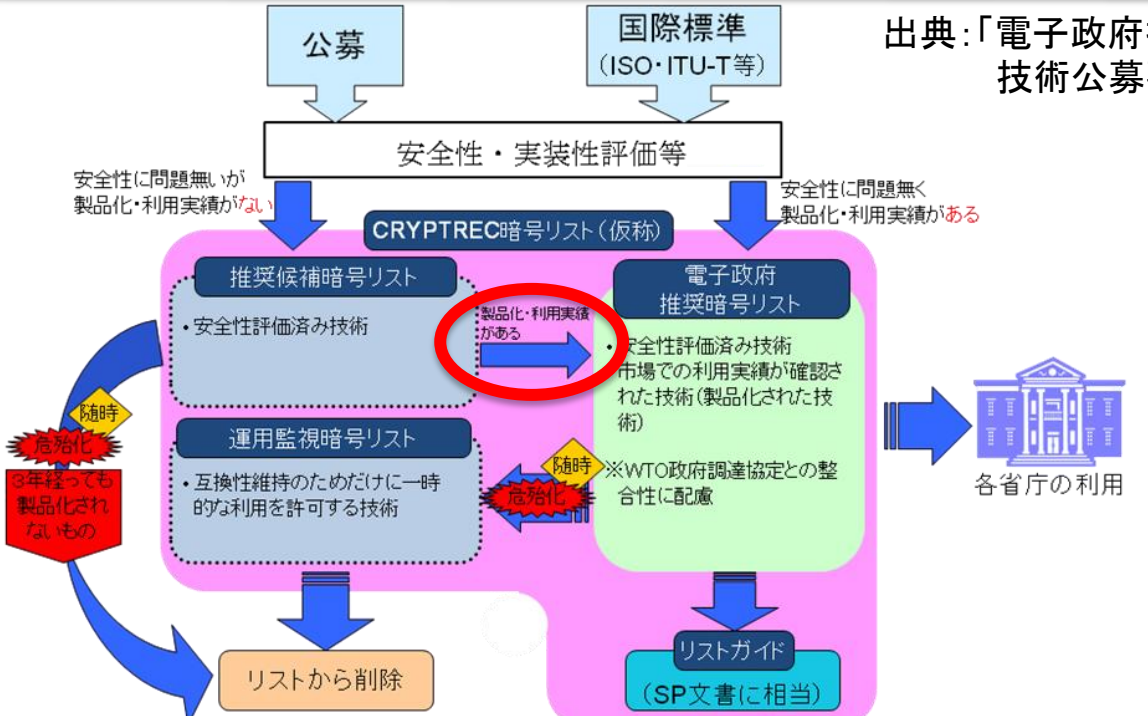
委員長	松本　勉	**横浜国立大学大学院** 環境情報研究院
委員	菊池　浩明	**東海大学** 情報通信学部　通信ネットワーク工学科
委員	木村　道弘	**日本情報経済社会推進協会(JIPDEC)** 電子情報利活用推進部
委員	近藤　潤一	**情報処理推進機構** 技術本部　セキュリティセンター
委員	佐藤　直之	**日本ベリサイン株式会社** 社長室
委員	鈴木　雅貴	**日本銀行** 金融研究所　情報技術研究センター
委員	瀧田　佐登子	**Mozilla Japan** 代表理事
委員	手塚　悟	**東京工科大学** コンピュータサイエンス学部
委員	西原　敏夫	**シスコシステムズ合同会社** 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** IPS事業部　セキュリティソリューション本部
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** 情報セキュリティ研究センター

CRYPTREC
Cryptography Research and Evaluation Committees

2011年度暗号運用委員会の成果概要と今後の予定

次期のCRYPTREC暗号リスト(仮称)の構成

出典:「電子政府推奨暗号リスト改訂のための暗号技術公募要項(2009 年度)」 P.5



(1) 電子政府推奨暗号リスト

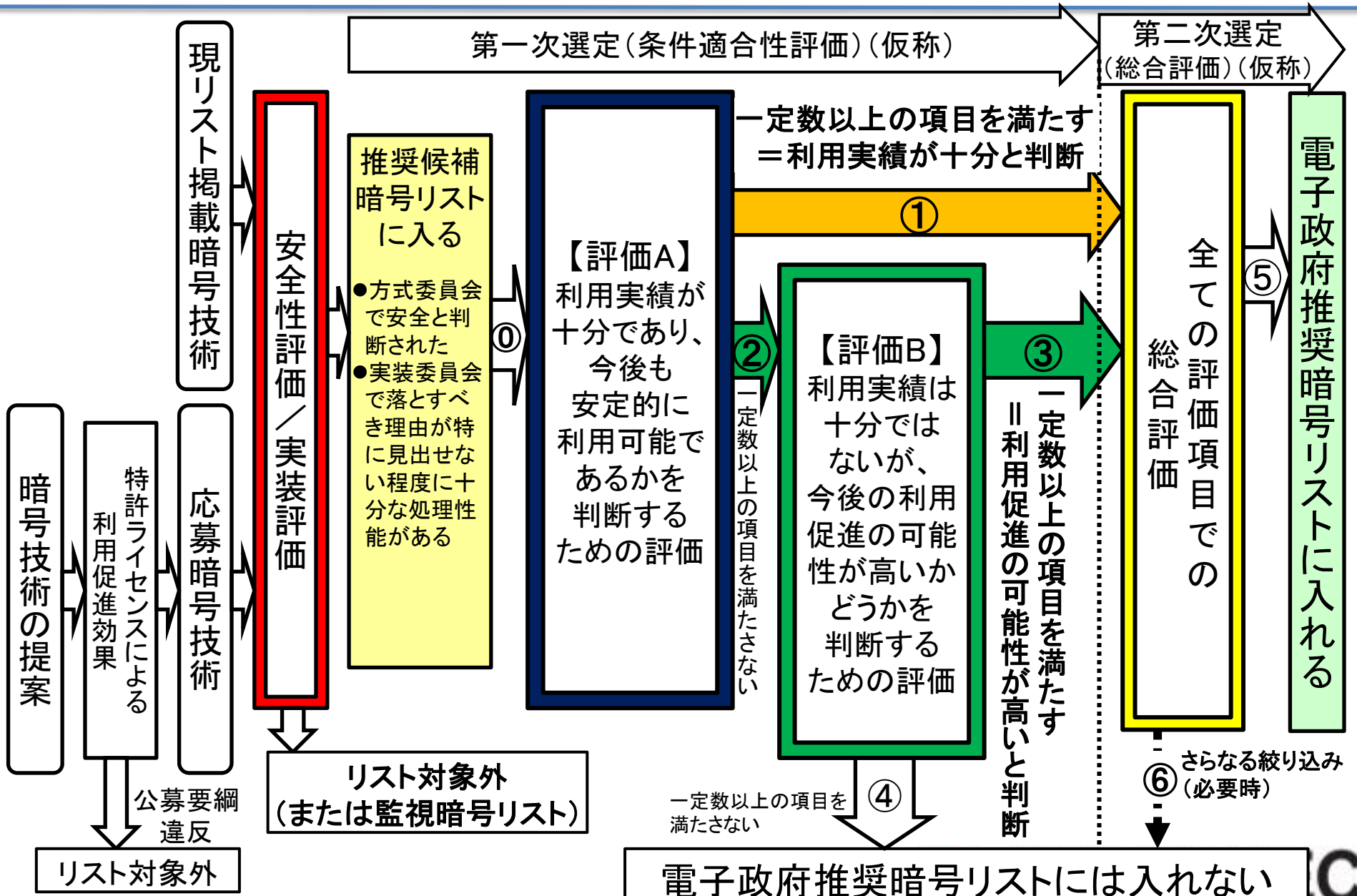
CRYPTRECにより安全性が確認され、かつ**市場において利用実績が十分**である暗号技術リスト。電子政府構築(政府調達)の際には当該技術の利用を推奨します(現リストと同等の位置づけ)。ここに登録される技術は国際標準化機関等により、標準化されていることが望まれます。

(2) 推奨候補暗号リスト

CRYPTREC により安全性が確認されているが、**市場において利用実績が十分でない普及段階**にある暗号技術が登録されているリスト。今後、利用が期待される新規技術等はここに分類されます。電子政府構築(政府調達)の際には当該技術も利用することができます。

本リストに登録された技術は、一定期間ごとに普及の度合いの調査を行い、利用実績が十分であると認められれば電子政府推奨暗号リストに登録されます。また、利用実績が十分であると認められなかった場合にはここから削除されます。危殆化が生じた暗号技術については、随時ここから削除されます。

選定ルールのフレームワーク



推奨暗号リスト選考基準の基本的考え方

- 次期推奨暗号リストに掲載される暗号技術の**個数を絞り込むために、明示的な基準を“選考基準”**として設定する
  - 次期推奨暗号リストへの不選定の理由が明確に説明できる
  - 調査方法や調査対象の選定の仕方によって、評価結果における精度上の問題がある程度含まれることは織り込んでおく
  - 評価結果における精度上の問題がある程度含まれていても、次期推奨暗号リストへの選定・不選定が極力変わらないような選考基準とする
  - 総合評価は、「ルート①で第一次選定を通過した暗号技術」と「ルート②③で第一次選定を通過した暗号技術」との間で、現状の利用実績の評価差をある程度緩和することが本来の趣旨であり、絞り込み評価として利用することは極力避ける
  - 本来の選定意図とは異なる暗号技術が第一次選定を通過するような緩い選考基準は極力避ける

評価A「十分な利用実績」と判断するための選考基準

市販製品での採用実績（販売会社数・種類・種別）	一定数以上の採用実績があることに加え、提案会社・グループ会社以外での採用実績もある
オープンソースプロジェクトでの採用実績	一定数以上の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	一定数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）
国際的な民間メジャー規格での採用実績	一定数以上の国際的な民間メジャー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）

評価B「利用促進の期待根拠」を判断するための選考基準

<table>
<tr><td colspan="4">評価A（「市販製品での採用実績　（販売会社数・種類・種別）」「オープンソースプロジェクトでの採用実績」「政府系システム規格での採用実績」「国際的な民間メジャー規格での採用実績」）に加えて</td></tr>
<tr><td colspan="3">利用促進を図る際の障壁の除去</td><td>非差別的に特許無償許諾を実施
（許諾契約締結が条件であってもよい）</td></tr>
<tr><td rowspan="3">標準化・規格化の促進を図るハードルの低さ</td><td rowspan="3">ＯＲ条件</td><td>技術的アピールポイント</td><td>市場が認める程度の技術的アドバンテージがある</td></tr>
<tr><td>標準化等のアピールポイント</td><td>他の一定数以上の標準化・規格化に採用されていれる</td></tr>
<tr><td>採用実績のアピールポイント</td><td>一定数以上の利用実績や製品・オープンソースプロジェクトでの採用実績がある</td></tr>
<tr><td rowspan="2">実装コスト低減を図るハードルの低さ</td><td rowspan="2">ＯＲ条件</td><td>採用実績のアピールポイント</td><td>一定数以上のOSや暗号モジュールでの採用実績がある</td></tr>
<tr><td>オープンソースのアピールポイント</td><td>一定数以上の暗号モジュールとして使えるオープンソースプロジェクトでの採用実績がある</td></tr>
<tr><td>調達コスト低減を図るハードルの低さ</td><td colspan="2">採用実績のアピールポイント</td><td>一定数以上の利用実績や製品・オープンソースプロジェクトでの採用実績がある</td></tr>
</table>

総合評価の基本的考え方

■各評価項目で決められた加点基準をもとに総合評価

		ルート①で通過	ルート②③で通過
技術的側面	安全性についての仕様上のアドバンテージ	○	○
	論文数の多寡によるアドバンテージ	○	○
	ソフトウェア実装性能評価	○	○
	ハードウェア実装性能評価	○	○
現状での利用実績	政府系システムでの採用実績	○	○
	市販製品での採用実績	○	○
	オープンソースプロジェクトでの採用実績	○	○
	特許ライセンスによる利用促進効果	○	○
	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	○	○
	国際標準規格での採用実績	○	○
	国際的な民間メジャー規格での採用実績	○	○
	民間の特定団体規格での採用実績	○	○
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**	ー	○
	標準化・規格化の促進を図るハードルの低さ	ー	○
	実装コスト低減を図るハードルの低さ	ー	○
	調達コスト低減を図るハードルの低さ	ー	○

今後のスケジュール

- 2012年度上期：選考基準及び加点基準の精緻化完了

- 利用実績調査： 2012年5月下旬～9月下旬を予定
  - 2012年度第1回運用委員会にて調査対象を決定
  - **2012年6月30日時点**までで、発売または公開中で入手可能、もしくは新製品としての発売がアナウンスされているもの

- 「特許ライセンスによる利用促進効果」及び「利用促進を図る際の障壁の除去」の評価：
  - **2012年9月30日時点**の特許ライセンス宣誓により実施
  - 2012年9月30日までは特許ライセンス宣誓の変更を認める

2011年度暗号運用委員会での議論の方針
（2010年度暗号運用委員会の成果を踏まえて）

推奨暗号リストの考え方の明確化の必要性

- 「電子政府推奨暗号リスト」と「推奨候補暗号リスト」の差異をどのように考えるかが不明確
  - 「市場において利用実績が十分」が意味する目的が明確ではない

    ⇒ 製品化・利用実績の「ある・ない」の基準についてコンセンサスがない
  - 実際に暗号製品を作っているベンダの意見が反映される仕組みがなかったのではないか

    ⇒ ビジネス展開を実際に担う産業界とのコンセンサス作りが不十分だったのではないか

市場における製品化・利用実績等に関する評価の考え方を決める上で、「電子政府推奨暗号リスト」と「推奨候補暗号リスト」とに与える役割を明確にする必要がある

CRYPTREC
Cryptography Research and Evaluation Committees

電子政府推奨暗号の実装率（2009年度調査）

■「暗号モジュールの市場動向等に関する調査研究」

http://www.meti.go.jp/meti_lib/report/2010fy01/E001139.pdf

暗号分類	暗号アルゴリズム	2003年度実装率%（製品数）	2009年度実装率%（製品数）	増減
128ビットブロック暗号	AES	**24.9% (62)**	**72.5% (222)**	**+47.6%**
	Camellia	**0% (0)**	**14.4% (44)**	**+14.4%**
	CIPHERUNICORN-A	**0% (0)**	**0.3% (1)**	**+0.3%**
	Hierocrypt-3	**0% (0)**	**0% (0)**	**+0%**
	SC2000	**0.4% (1)**	**0.3% (1)**	**△0.1%**
64ビットブロック暗号	CIPHERUNICORN-E	**0% (0)**	**0.3% (1)**	**+0.3%**
	Hierocrypt-L1	**0% (0)**	**0% (0)**	**+0%**
	MISTY1	**4.0% (10)**	**2.0% (6)**	**△2.0%**
	TDES	**45.0% (112)**	**47.4% (145)**	**+2.4%**
ストリーム暗号	MUGI	**0% (0)**	**1.0% (3)**	**+1.0%**
	MULTI-S01	**0% (0)**	**0% (0)**	**+0%**
	RC4 (128bit)	**14.1% (35)**	**5.9% (18)**	**△8.2%**

暗号分類	暗号アルゴリズム	2003年度実装率%（製品数）	2009年度実装率%（製品数）	増減
公開鍵署名	DSA	**13.7% (34)**	**14.1% (43)**	**+0.4%**
	ECDSA	**4.8% (12)**	**9.5% (29)**	**+4.7%**
	RSASSA-PKCS1-v1_5	**29.3% (73)**	**34.6% (106)**	**N/A**
	RSA-PSS	**7.6% (19)**		
	RSAES-PKCS1-v1_5	**16.1% (40)**		
	RSA-OAEP	**9.2% (23)**		
ハッシュ関数	RIPEMD-160	**2.0% (5)**	**9.2% (28)**	**+7.2%**
	SHA-1	**49.4% (123)**	**28.8% (88)**	**△20.6%**
	SHA-256	**4.4% (11)**	**14.4% (44)**	**+10.0%**
	SHA-384	**3.2% (8)**	**7.2% (22)**	**+4.0%**
	SHA-512	**3.2% (8)**	**9.2% (28)**	**+6.0%**
鍵共有	DH	**27.7% (69)**	**22.2% (68)**	**△5.5%**
	ECDH	**2.0% (5)**	**7.5% (23)**	**+5.5%**
	PSEC-KEM	**0% (0)**	**0.3% (1)**	**+0.3%**

推奨暗号リストの考え方の明確化に向けて(1)

■ 電子政府推奨暗号リストに「何を求める」のか

⇒ それぞれの設定意図を参考に4つのシナリオを設定

シナリオ			推奨リスト例	シナリオの設定意図
No. 1	実際に利用されている暗号だけを電子政府推奨暗号に選定	実際に利用されている暗号だけを電子政府推奨暗号リストに限定することでリストの有効性を高めるために **「現状の調達容易性（利用実績）」を主たる判断材料** としたうえで、有力な標準化規格で必須実装に指定されているなどの「純技術的なその他要件」を考慮	米国政府標準暗号のみ	調達容易性の観点から、特定の暗号アルゴリズムが政府システムにおいて広く利用されている実態を考慮
No. 2	国際標準化・製品化促進の手段として電子政府推奨暗号リストを活用	「安全性」、「現状の調達容易性（利用実績）」、「将来的な調達容易性（利用実績）」の見通しを踏まえつつ、電子政府推奨暗号リストの掲載個数を限定したうえで、提案暗号の普及展開をどのように進めるべきかといった **「非技術的なその他要件」を最大限加味**	米国政府標準暗号＋国産暗号（1 or 少数）	米国政府標準暗号以外の暗号は国際標準化や規格化、製品化からも排除される流れが強まっている点を考慮。 提案暗号に対する国としてのバックアップの明確化

推奨暗号リストの考え方の明確化に向けて(2)

シナリオ			推奨リスト例	シナリオの設定意図
No. 3	一定期間経過後の利用実績不振による電子政府推奨暗号からの降格	当初は電子政府推奨暗号リスト入りさせるが、一定期間経過後の普及状況を厳格に判定する**「将来的な調達容易性（利用実績）」を重要視**	短期的にはシナリオNo. 4。中長期的にはシナリオNo. 1, 2, 4のいずれにもなりうる	提案暗号の普及展開を強力に実施するモチベーションを応募企業に持たせる一方、一定期間経過後の普及展開が思わしくない提案暗号には電子政府推奨暗号リストから降格してもらうルールを新たに導入
No. 4	政府調達の選択肢としての提示	電子政府推奨暗号リストと推奨候補リストとの区分は**「安全性」を主たる判断基準**として行うことにより、現状とほぼ同様の構成	現状とほぼ同様	「調達容易性」を判断することは難しいうえ電子政府推奨暗号リストの掲載個数を削減することによる効果も定かではない点、ならびに暗号研究体制に与えるマイナス影響を考慮

CRYPTREC
Cryptography Research and Evaluation Committees

推奨暗号リストの考え方に対する評価(1)

■ 各シナリオ実施時のメリット・デメリット・留意点洗い出し

⇒ 評価軸ごとに洗い出した後、評価点を採点

≪評価軸≫

A)「安全性」に関する検討項目

推奨暗号の安全性評価の充実度や危殆化に伴う影響・対策有無、等

B)「調達容易性」に関する検討項目

実利用されている暗号との相関度やベンダロックインの懸念有無、等

C)「標準化・規格化等への影響」に関する検討項目

国際標準化（ISO/IEC等）や規格化（IETF等）策定に与える影響、等

D)「提案暗号（国産暗号）の利用促進」に関する検討項目

提案暗号（国産暗号）をサポートするモチベーションや政策支援効果、等

E)「セキュリティ研究体制への影響」に関する評価項目

新暗号開発へのモチベーションや国内セキュリティ研究体制への影響、等

F)「CRYPTREC活動成果」に関する評価項目

CRYPTRECリストの位置づけやCRYPTREC活動成果の対外的効果、等

≪評価点≫

4：メリットのほうがかなり多い

3：どちらかといえばメリットのほうが多い

2：どちらかといえばデメリットのほうが多い

1：デメリットのほうがかなり多い

※評価点は、審議過程で抽出されたメリット・デメリットの個数ではなく、メリット・デメリットの効果の大きさで判断

※評価点は、解決すべき問題点への対策が実施されたとしての前提で判断（対策が実施されない場合は評価点が変わることがある）

推奨暗号リストの考え方に対する評価(2)

- 国内外の主要暗号製品ベンダ・システムインテグレータを主な対象とした実態調査アンケート
  - 暗号搭載製品の開発製造、情報システムの構築等における暗号利用（選択プロセス）に関する実態を把握
  - 現在の「電子政府推奨暗号リスト」の活用実態を把握
  - 国産暗号に対する認識を広く把握

ベンダ（全39社、67プロダクト）

凸版印刷株式会社
オーセンテック株式会社
キヤノン株式会社
KDDI株式会社
大日本印刷株式会社
三菱電機インフォメーションシステムズ株式会社
日本電気株式会社
株式会社PFU
ルネサスエレクトロニクス株式会社
EMCジャパン株式会社
一般社団法人 Mozilla Japan
インフィニオンテクノロジーズジャパン株式会社
株式会社リコー
株式会社東芝
富士ゼロックス株式会社
富士通株式会社
ソニー株式会社
アマノビジネスソリューションズ株式会社
株式会社ACCESS
ヤマハ株式会社
マイクロソフト株式会社
セコムトラストシステムズ株式会社
日本ベリサイン株式会社
株式会社バッファロー
タレスジャパン株式会社
シスコシステムズ合同会社
インテル株式会社

SIer（全8社、11システム）

三菱電機株式会社
東芝ソリューション株式会社
新日鉄ソリューションズ株式会社
三菱電機インフォメーションシステムズ株式会社
株式会社日立製作所

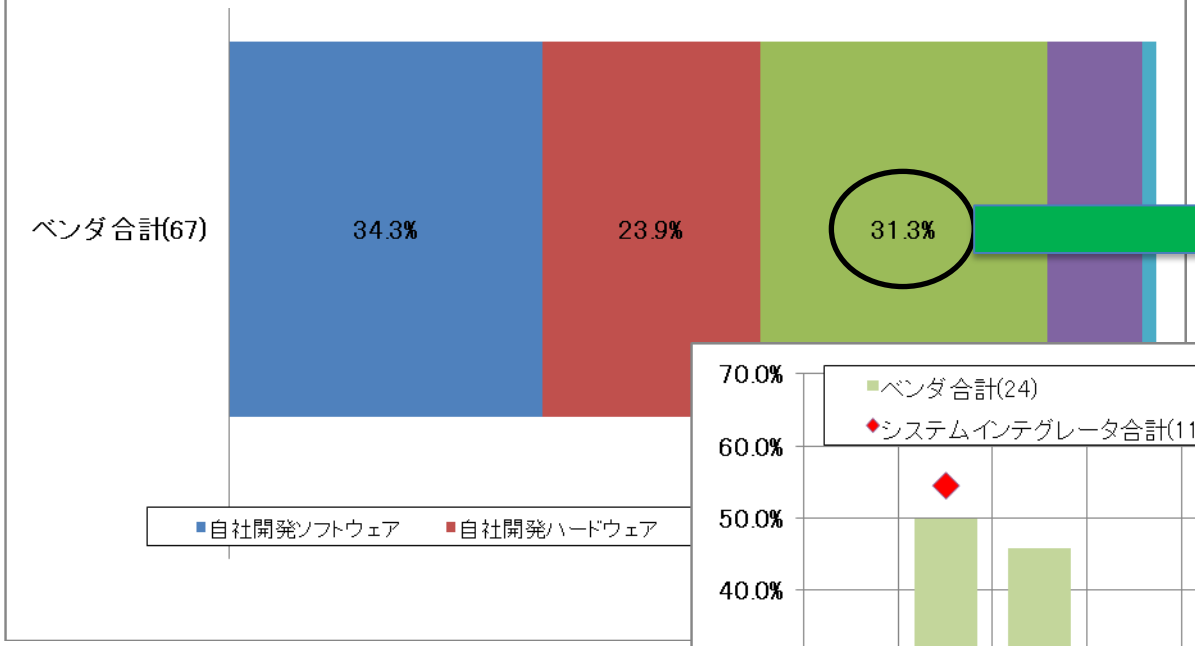
政府機関
（全4府省、6システム）

応募者（研究開発部門）
（全9社）

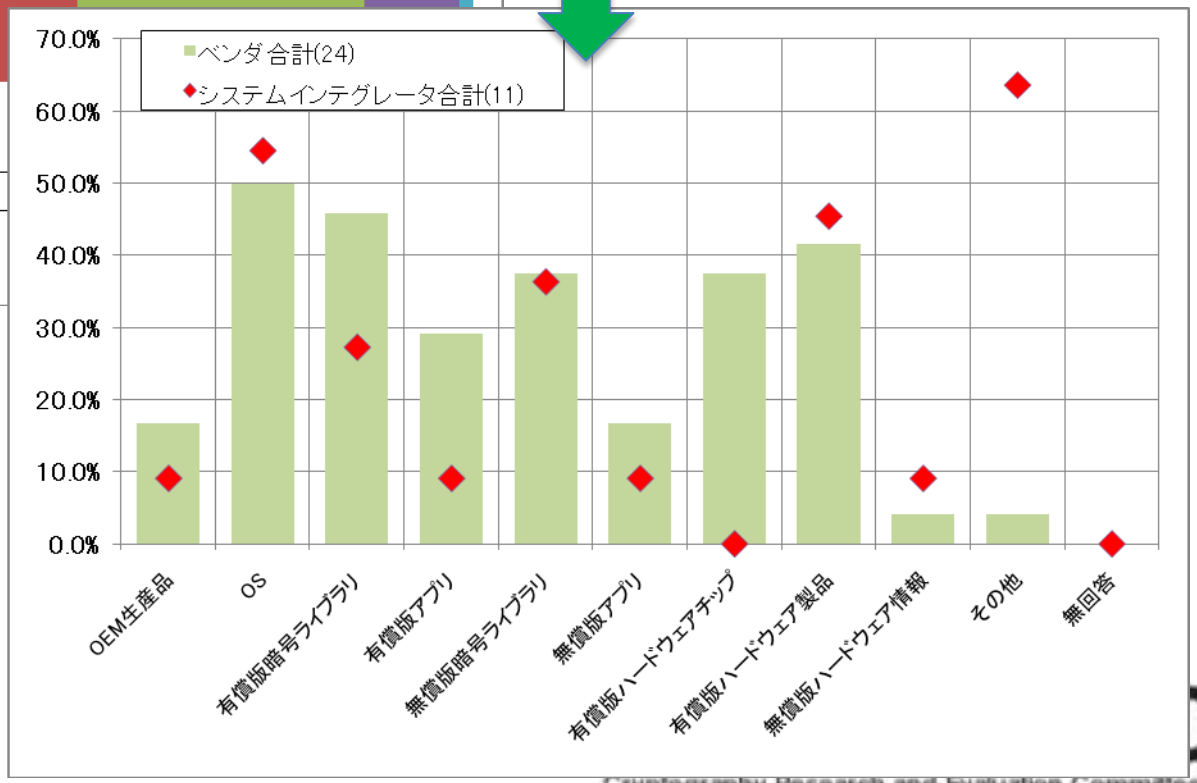
CRYPTREC
Cryptography Research and Evaluation Committees

アンケート結果の例(1)

暗号搭載製品で利用する暗号アルゴリズムをどのような方法で実現しているか？



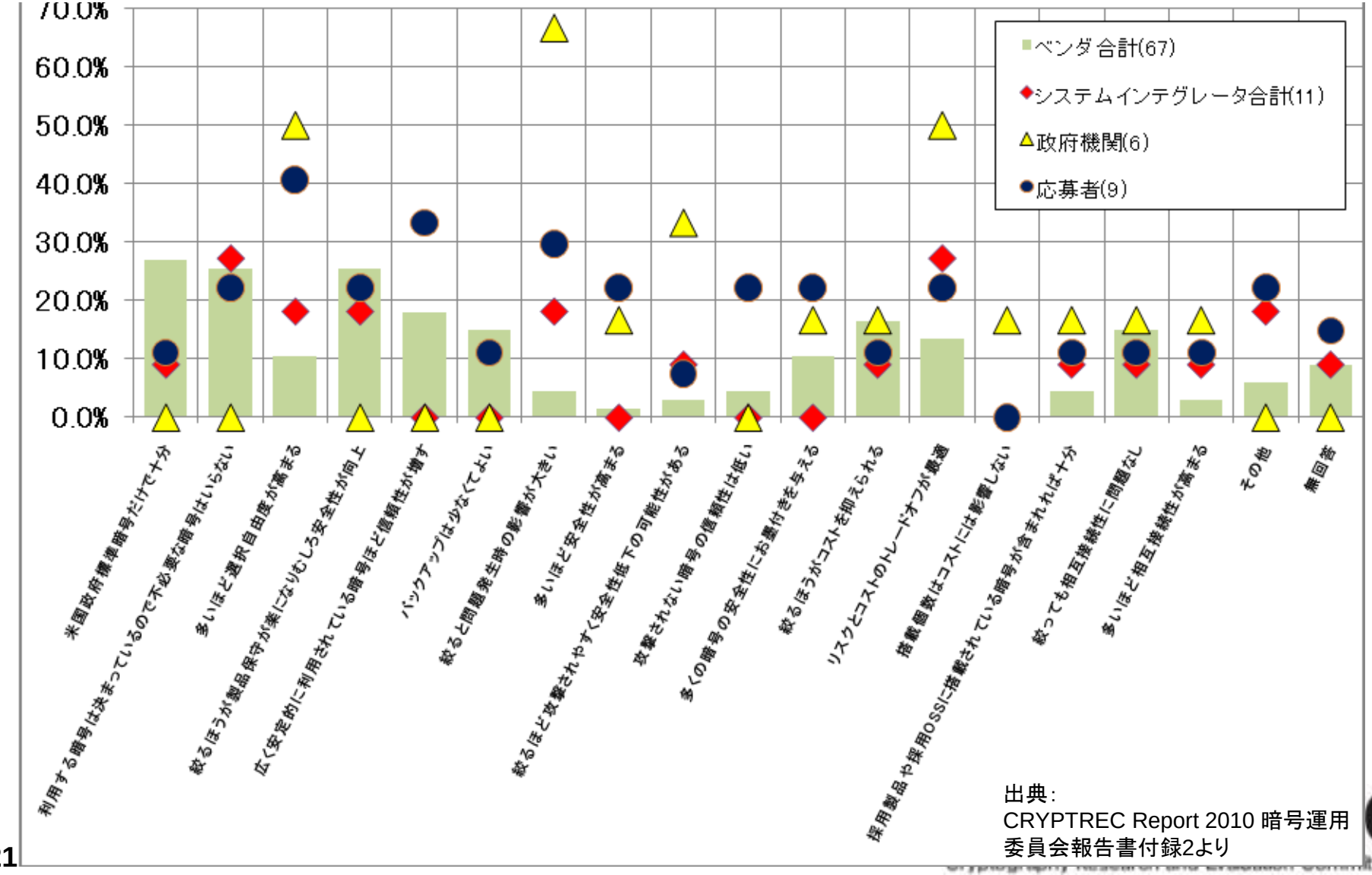
他社製品を利用している場合、どのような他社製品に搭載されている暗号アルゴリズムを利用しているか？



出典:
CRYPTREC Report 2010 暗号運用委員会報告書
付録2より

アンケート結果の例(2)

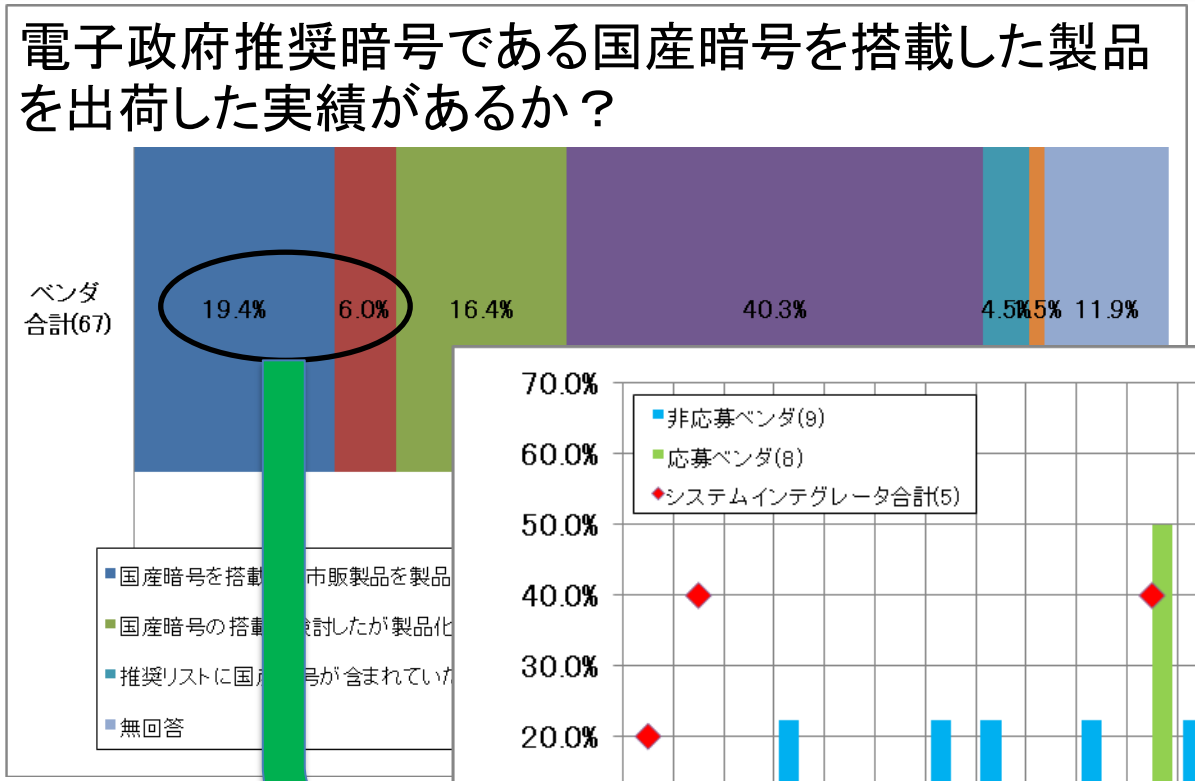
（推奨暗号リストに掲載されるアルゴリズムの個数はどの程度がよいかの質問に続いて）
なぜそのように考えるのか？

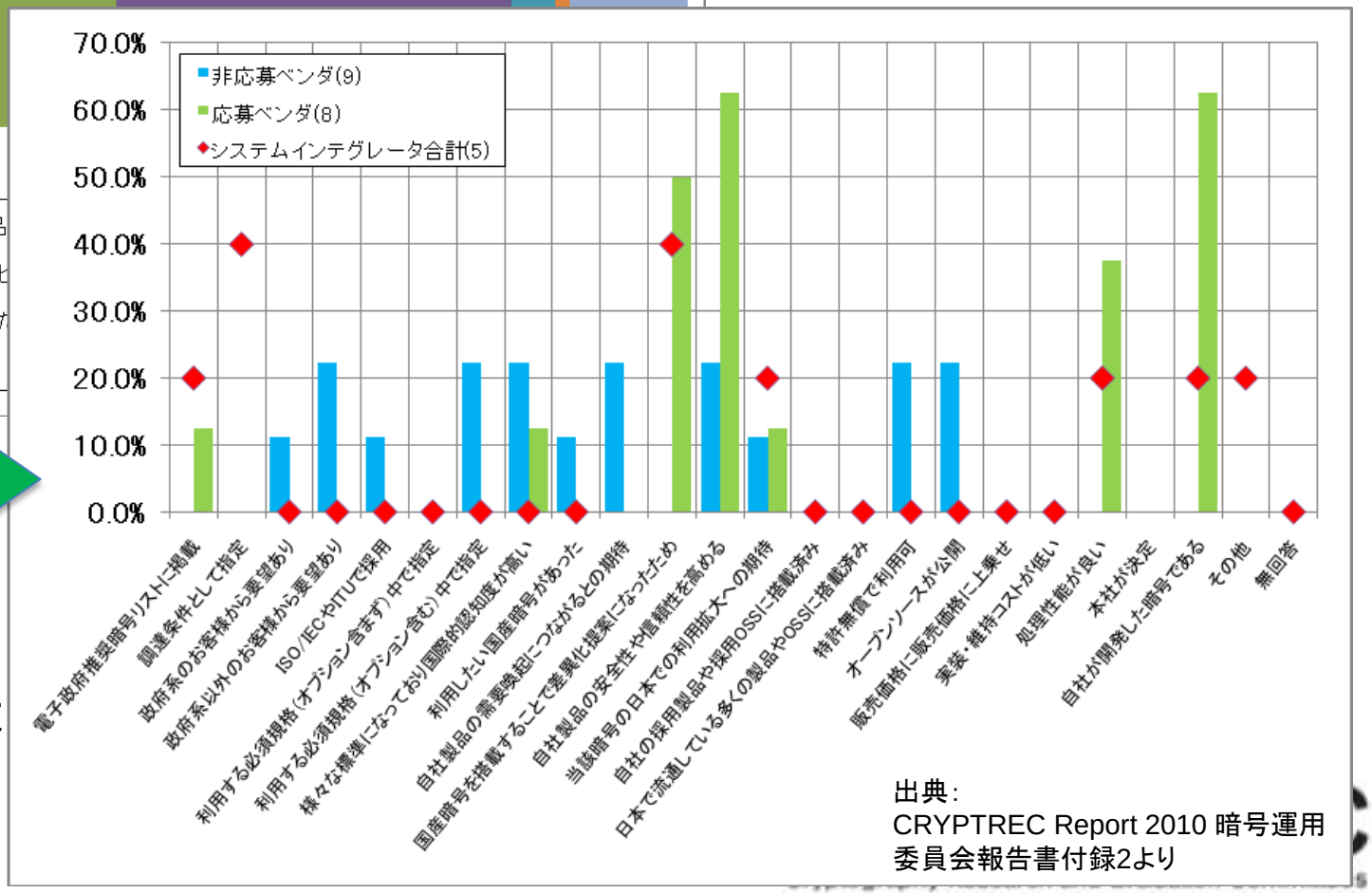


出典:
CRYPTREC Report 2010 暗号運用委員会報告書付録2より

アンケート結果の例(3)

電子政府推奨暗号である国産暗号を搭載した製品を出荷した実績があるか？



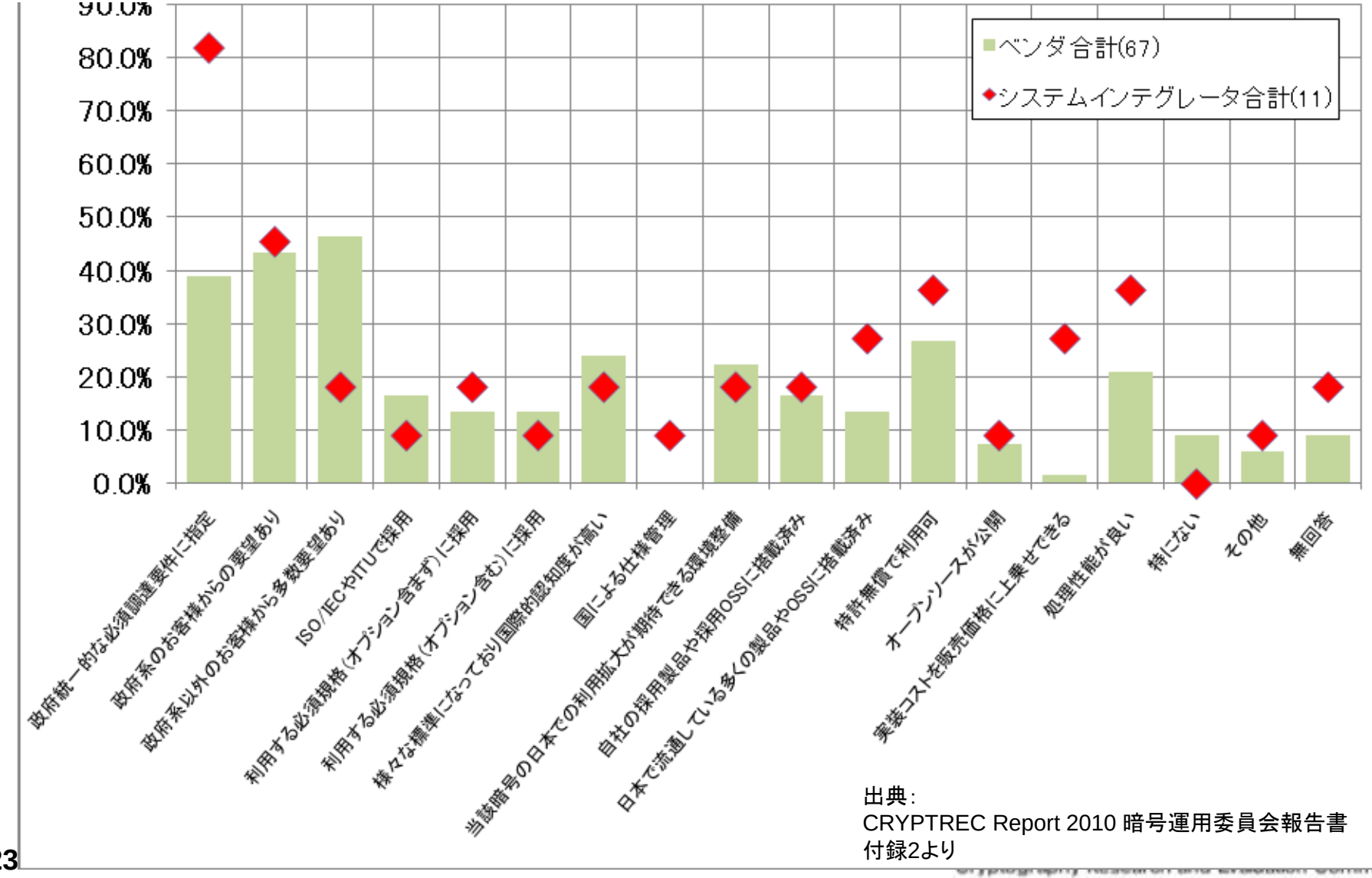


出典:
CRYPTREC Report 2010 暗号運用委員会報告書付録2より

電子政府推奨暗号である国産暗号を暗号搭載製品・システムに採用したのはなぜか？

アンケート結果の例(4)

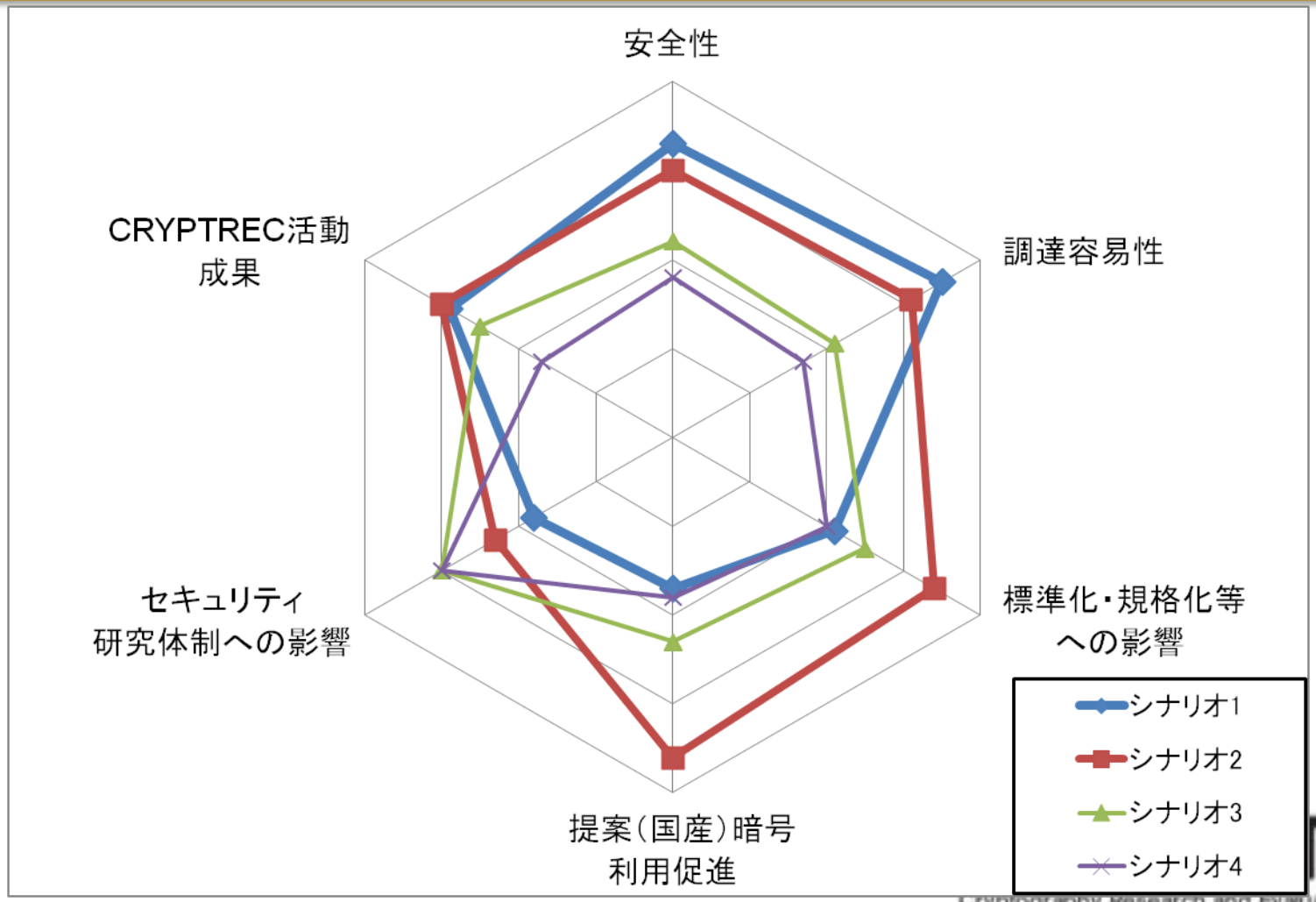
今後、電子政府推奨暗号である国産暗号を暗号搭載製品・システムに採用するために必要と考える条件は何か？



出典：
CRYPTREC Report 2010 暗号運用委員会報告書
付録2より

評価点比較のまとめ（2010年度運用委員会成果）

「CRYPTREC Report 2010 暗号運用委員会報告書」をご覧ください　(http://www.cryptrec.go.jp/report.html)



TREC
Cryptography Research and Evaluation Committees

暗号技術検討会の審議の結果

- 2010年度暗号運用委員会の検討において、4つの電子政府推奨暗号リストの設定意図を設定し、効果を評価
  - 実施時のメリット・デメリット・留意点を参考に評価点を採点

- 暗号技術検討会での審議の結果、電子政府推奨暗号リスト改訂にあたっては以下の方針で推進するよう答申

No.2	**国際標準化・製品化促進の手段**として電子政府推奨暗号リストを活用	**米国政府標準暗号＋国産暗号（1 or 少数）**	米国政府標準暗号以外の暗号は国際標準化や規格化、製品化からも排除される流れが強まっている点を考慮。 **提案暗号に対する国としてのバックアップの明確化**

推奨暗号選定ルールの検討方針について

■暗号技術検討会での答申趣旨を以下のように解釈

【観点(i)】

すでに現状の調達容易性（利用実績）が十分に高く、かつ将来的な安全性にも十分な余裕度があって今後も安定して利用できる見込みがある暗号技術を選定する

【観点(ii)】

現状の調達容易性（利用実績）は十分に高いとは言えないものの以下の条件すべてを満たす暗号技術を選定する

- 上記観点(i)で選定される暗号技術のなかで最も高い安全性を有するものと同等かそれ以上の安全性を有すると評価される
- 今後の普及展開支援によって、国際標準化・製品化促進が図られると期待できる根拠がある
- 今後の普及展開支援によって、将来的な調達容易性（利用実績）が十分に高くなると期待できる根拠がある

これらの観点を実現するための選定ルール・選考基準を検討

2011年度活動成果の詳細

評価項目に何を取り上げるか

- 技術的側面
  - 技術的に優れているかどうか
    - 安全性
    - 処理性能
- 現状での利用実績
  - 主に観点(i)の意味での利用実績を満たしているかどうか
    - 市販製品やオープンソースプロジェクトでの利用状況
    - 政府系システムでの利用状況
    - 各種標準化・規格化での採用状況
- 利用促進が図られると期待される根拠
  - 主に観点(ii)の意味での利用促進の期待される根拠を満たしているかどうか
    - 各種標準化・規格化が促進されるか
    - 調達コストや実装コストの低減につながるか

評価項目一覧(1)

評価項目		評価意図
技術的側面	安全性についての仕様上の特長に関するアドバンテージ	安全性評価の安全性アドバンテージを認めるかを判断する
	論文数の多寡によるアドバンテージ	安全性評価の信頼性アドバンテージを認めるかを判断する
	ソフトウェア実装性能評価	ソフトウェアでの実装性能の優位性を判断する
	ハードウェア実装性能評価	ハードウェアでの実装性能の優位性を判断する
現状での利用実績	政府系システムでの採用実績	政府系システムでの利用状況により必要性を判断する
	市販製品での採用実績（販売会社数・種類・種別）	市販製品での利用状況により必要性を判断する
	オープンソースプロジェクトでの採用実績	利用容易性・利用促進性、及び仲間作りの進捗度合いを判断する
	特許ライセンスによる利用促進効果	特許ライセンスによるベンダロックインの懸念度合い及び利用容易性・利用促進性を判断する
	オープンソース公開による利用促進効果	利用容易性や利用促進性を判断する
	政府系システム規格での採用実績	政府系システムでの必要性を判断する
	国際標準規格での採用実績	国際的な認知度・成熟度の進捗度合いを判断する
	国際的な民間メジャー規格での採用実績	利用可能性及び国際的な認知度・成熟度・仲間作りの進捗度合いを判断する
	民間の特定団体規格での採用実績	民間での必要性を判断する

評価項目一覧(2)

評価項目		評価意図
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	既存アルゴリズムと比較して、利用促進を図る際の障壁を除去できるかを判断する
	標準化・規格化の促進を図るハードルの低さ	標準化・規格化済みアルゴリズムに対する、標準化・規格化を促進するうえでのアピールポイントの有効度を評価する
	実装コスト低減を図るハードルの低さ	新たな暗号を追加で実装する際の実装コストを低減するうえでのアピールポイントの有効度を判断する
	調達コスト低減を図るハードルの低さ	新たな暗号が追加された製品やシステムを調達する際の調達コストを低減するうえでのアピールポイントの有効度を判断する

「十分な利用実績」を判断するための選考基準

【評価A】 十分な利用実績があるかを判断する（ルート①で第一次選定を通過する）ための選考基準

現状での利用実績	政府系システムでの採用実績	「政府系システム規格」での採用実績により評価を行えばよい
	市販製品での採用実績（販売会社数・種類・種別）	評価Aの選考基準に採用
	オープンソースプロジェクトでの採用実績	評価Aの選考基準に採用
	特許ライセンスによる利用促進効果	公募要綱との関係から、特許ライセンス条件について厳しい条件を課すことは適当ではない
	オープンソース公開による利用促進効果	製品またはプロジェクトとしてのサポートがなく、利用促進効果が明確ではない
	政府系システム規格での採用実績	評価Aの選考基準に採用
	国際標準規格での採用実績	国際標準規格に採用されただけでは実質的な利用促進効果が大きくない（現時点では影響力がある支配的な規格とはいえない）
	国際的な民間メジャー規格での採用実績	評価Aの選考基準に採用
	民間の特定団体規格での採用実績	得られる情報の精度に幅があり、適切な評価が困難である

「十分な利用実績」を判断するための選考基準のポイント

市販製品での採用実績（販売会社数・種類・種別）	一定数以上の採用実績があることに加え、**提案会社・グループ会社以外での採用実績**もある ➡ コスト低減の観点から複数企業から調達できるようにすべき
オープンソースプロジェクトでの採用実績	一定数以上の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 ➡ 実際の製品やシステムに組み込まれて使われるのは「正式版（リリース版）」である
政府系システム規格での採用実績	一定数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） ➡ 最終承認待ち以前では規格化されないで終わる可能性あり
国際的な民間メジャー規格での採用実績	一定数以上の国際的な民間メジャー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） ➡ 最終承認待ち以前では規格化されないで終わる可能性あり

「利用促進の期待根拠」を判断するための選考基準

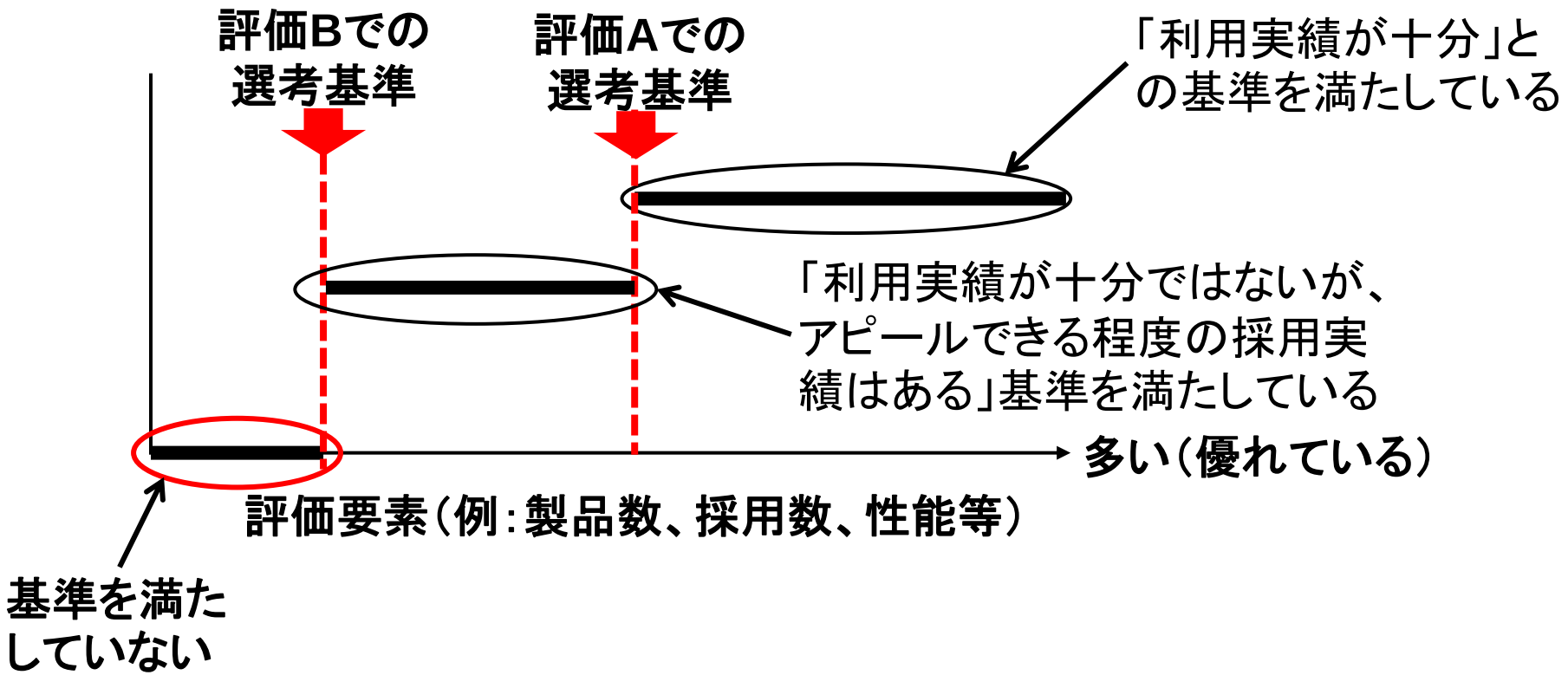
【評価B】 利用促進の期待根拠があるかを判断する（ルート②③で第一次選定を通過する）ための選考基準

評価A（「市販製品での採用実績 （販売会社数・種類・種別）」「オープンソースプロジェクトでの採用実績」「政府系システム規格での採用実績」「国際的な民間メジャー規格での採用実績」）に加えて			
利用促進を図る際の障壁の除去			非差別的条件での特許無償許諾を実施（許諾契約締結が条件であってもよい）
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	市場が認める程度の技術的アドバンテージがある
		標準化等のアピールポイント	他の一定数以上の標準化・規格化に採用されていれる
		採用実績のアピールポイント	一定数以上の利用実績や製品・オープンソースプロジェクトでの採用実績がある
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	一定数以上のOSや暗号モジュールでの採用実績がある
		オープンソースのアピールポイント	一定数以上の暗号モジュールとして使えるオープンソースプロジェクトでの採用実績がある
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		一定数以上の利用実績や製品・オープンソースプロジェクトでの採用実績がある

「利用促進の期待根拠」を判断するための選考基準のポイント

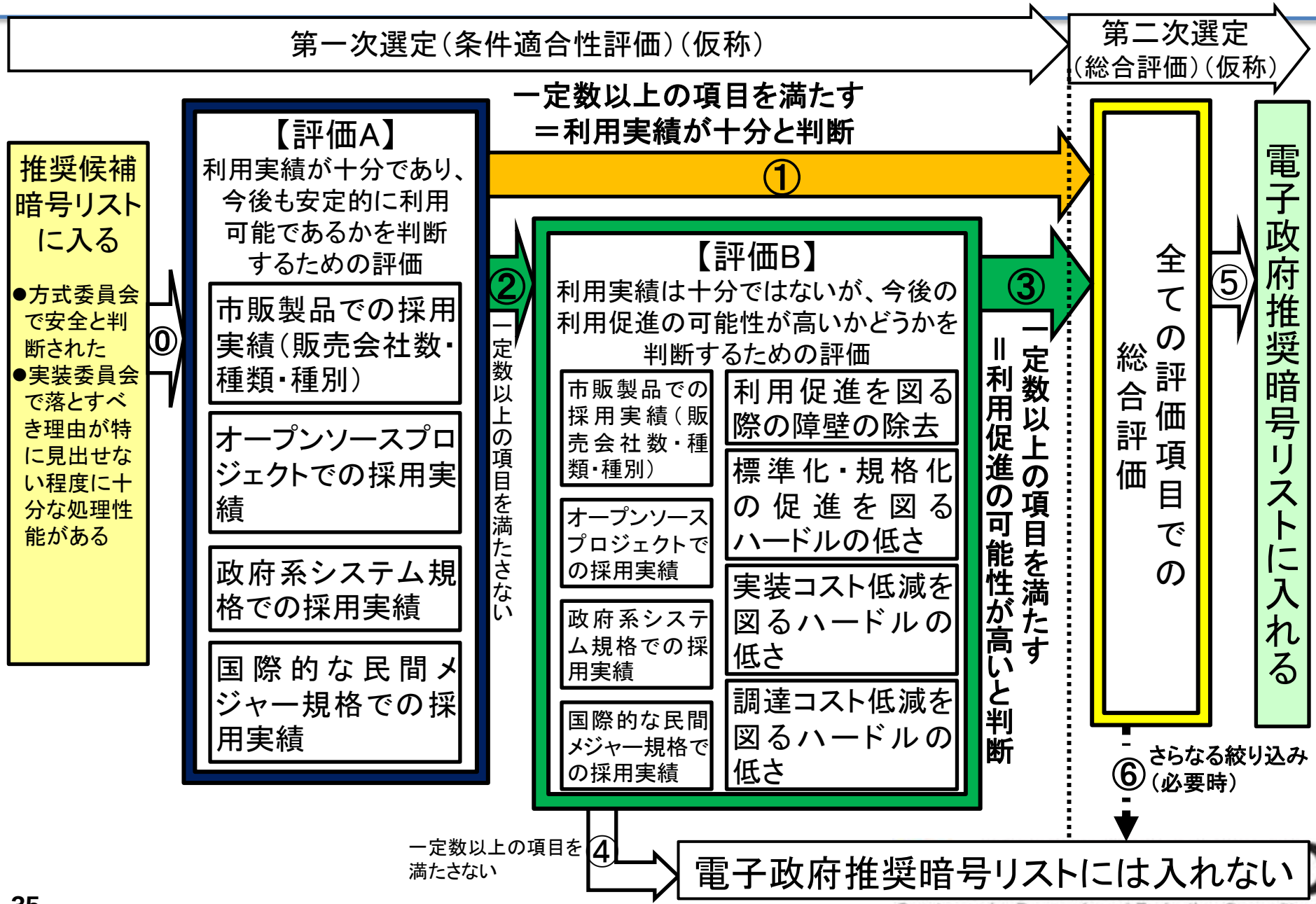
■ 評価A「十分な利用実績」の選考基準とどこが違うのか

例：「市販製品での採用実績」での「一定数以上の採用実績」と
「採用実績のアピールポイント」での「一定数以上の採用実績」



CRYPTREC
Cryptography Research and Evaluation Committees

選定ルールのフレームワーク（詳細）



Cryptography Research and Evaluation Committees

第一次選定（条件適合性評価）のイメージ例(1)

○：選考基準を満たす △：選考基準を満たす可能性がある ×：選考基準を満たさない －：評価対象外

状況例	評価Aの選考基準を満たした評価項目が一定数(x/4)以上あればルート①により第一次選定を通過							
	評価Bの選考基準を満たした評価項目が一定数(y/8)以上あればルート②③により第一次選定を通過							
	市販製品での採用実績	オープンソースプロジェクトでの採用実績	政府系システム規格での採用実績	国際的な民間メジャー規格での採用実績	利用促進を図る際の障壁の除去	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
評価Aの選考基準を超える市販製品での採用実績がある	○	－	－	－	－	○	△ OSや暗号モジュールがあれば	○
評価Aの選考基準を超えるオープンソースプロジェクトでの採用実績がない	－	×	－	－	－	△	△	△
評価Aの選考基準を超える国際的な民間メジャー規格での採用実績がある	－	－	－	○	－	○	－	－
評価Aの選考基準を超える政府系システム規格での採用実績がある	－	－	○	－	－	○	－	－

評価Aの評価項目を3つ満たしている

CRYPTREC Cryptography Research and Evaluation Committees

第一次選定（条件適合性評価）のイメージ例(2)

○：選考基準を満たす △：選考基準を満たす可能性がある ×：選考基準を満たさない －：評価対象外

状況例	評価Aの選考基準を満たした評価項目が一定数(x/4)以上あればルート①により第一次選定を通過							
	評価Bの選考基準を満たした評価項目が一定数(y/8)以上あればルート②③により第一次選定を通過							
	市販製品での採用実績	オープンソースプロジェクトでの採用実績	政府系システム規格での採用実績	国際的な民間メジャー規格での採用実績	利用促進を図る際の障壁の除去	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
評価Aの選考基準を超える市販製品での採用実績がない	×	－	－	－	－	△	△	△
評価Aの選考基準を超えるオープンソースプロジェクト（暗号ライブラリ含む）での採用実績がある	－	○	－	－	－	○	○	○
評価Aの選考基準を超える国際的な民間メジャー規格での採用実績がない	－	－	－	×	－	△	－	－
評価Aの選考基準を超える政府系システム規格での採用実績がない	－	－	×	－	－	△	－	－

評価Aの評価項目を1つ満たしている　評価Bの評価項目を4つ満たしている

Cryptography Research and Evaluation Committees

第一次選定（条件適合性評価）のイメージ例(3)

○：選考基準を満たす △：選考基準を満たす可能性がある ×：選考基準を満たさない －：評価対象外

状況例	評価Aの選考基準を満たした評価項目が一定数(x/4)以上あればルート①により第一次選定を通過							
	評価Bの選考基準を満たした評価項目が一定数(y/8)以上あればルート②③により第一次選定を通過							
	市販製品での採用実績	オープンソースプロジェクトでの採用実績	政府系システム規格での採用実績	国際的な民間メジャー規格での採用実績	利用促進を図る際の障壁の除去	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
評価Aと評価Bの選考基準を間にある市販製品（暗号ライブラリを含む）での採用実績がある	×	－	－	－	－	○	○	○
評価Aの選考基準を超えるオープンソースプロジェクトでの採用実績がない	－	×	－	－	－	△	△	△
評価Aの選考基準を超える国際的な民間メジャー規格での採用実績がない	－	－	－	×	－	△	－	－
評価Aの選考基準を超える政府系システム規格での採用実績がない	－	－	×	－	－	△	－	－

評価Aの評価項目を一つも満たしていない　評価Bの評価項目を3つ満たしている

Cryptography Research and Evaluation Committees

第一次選定（条件適合性評価）のイメージ例(4)

○：選考基準を満たす △：選考基準を満たす可能性がある ×：選考基準を満たさない －：評価対象外

状況例	評価Aの選考基準を満たした評価項目が一定数(x/4)以上あればルート①により第一次選定を通過							
	評価Bの選考基準を満たした評価項目が一定数(y/8)以上あればルート②③により第一次選定を通過							
	市販製品での採用実績	オープンソースプロジェクトでの採用実績	政府系システム規格での採用実績	国際的な民間メジャー規格での採用実績	利用促進を図る際の障壁の除去	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
評価Bの選考基準を超える市販製品での採用実績がない	×	－	－	－	－	×	×	×
評価Bの選考基準を超えるオープンソースプロジェクトでの採用実績がない	－	×	－	－	－	×	×	×
評価Aと評価Bの選考基準の間にある国際的な民間メジャー規格での採用実績がある	－	－	－	×	－	○	－	－
評価Aの選考基準を超える政府系システム規格での採用実績がある	－	－	○	－	－	○	－	－

評価Aの評価項目を1つ満たしている　評価Bの評価項目を2つ満たしている

第一次選定（条件適合性評価）のイメージ例(5)

○：選考基準を満たす △：選考基準を満たす可能性がある ×：選考基準を満たさない ー：評価対象外

状況例	評価Aの選考基準を満たした評価項目が一定数(x/4)以上あればルート①により第一次選定を通過							
	評価Bの選考基準を満たした評価項目が一定数(y/8)以上あればルート②③により第一次選定を通過							
	市販製品での採用実績	オープンソースプロジェクトでの採用実績	政府系システム規格での採用実績	国際的な民間メジャー規格での採用実績	利用促進を図る際の障壁の除去	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
非差別条件での特許無償許諾（許諾契約必要）	ー	ー	ー	ー	○	ー	ー	ー
市場が認める程度の技術的アドバンテージがある	ー	ー	ー	ー	ー	○	ー	ー
評価Bの選考基準を超える国際標準化規格での採用実績がある	ー	ー	ー	ー	ー	○	ー	ー
評価Bの選考基準の超える民間の特定団体規格での採用実績がある	ー	ー	ー	ー	ー	○	△ 実装されている可能性が高いため	△ 実装されている可能性が高いため

CRYPTREC Cryptography Research and Evaluation Committees

第二次選定（総合評価）の基本的考え方(1)

■総合評価の加点基準の基本的考え方

評価項目		加点基準	重みづけ
技術的側面	安全性についての仕様上の特長に関するアドバンテージ	暗号方式委員会に見解を求める	
	論文数の多寡によるアドバンテージ	暗号方式委員会に見解を求める	
	ソフトウェア実装評価	暗号実装委員会に見解を求める	
	ハードウェア実装評価	暗号実装委員会に見解を求める	
現状での利用実績	市販製品での採用実績（販売会社数・種類・種別）	採用実績による2～3段階の点数をつける	製品の重要度やシェアによる重みづけを考慮する
	特許ライセンスによる利用促進効果	ライセンス条件による2段階の点数をつける •許諾契約なしの特許無償または特許なし •許諾契約ありの特許無償	
	オープンソースプロジェクトでの採用実績	採用実績による2～3段階の点数をつける	プロジェクトの重要度や信頼度による重みづけを考慮する

CRYPTREC
Cryptography Research and Evaluation Committees

第二次選定（総合評価）の基本的考え方(2)

評価項目		加点基準	重みづけ
現状での利用実績	政府系システムでの採用実績	採用実績による2～3段階の点数をつける	システムの違いによる重みづけを考慮する
	オープンソース公開による利用促進効果	1段階 •一定の性能を持ったオープンソースをオープンソースプロジェクトに提案しているものだけを対象	
	政府系システム規格での採用実績	採用実績による2～3段階の点数をつける	規格の違いによる重みづけを考慮する
	国際的な民間メジャー規格での採用実績	採用実績による2～3段階の点数をつける	規格の違いによる重みづけを考慮する
	国際標準規格での採用実績	1段階 •対象となる規格が少ないと考えられるため	
	民間の特定団体規格での採用実績	採用実績による2～3段階の点数をつける	規格の違いによる重みづけを考慮する

第二次選定（総合評価）の基本的考え方(3)

評価項目		加点基準	重みづけ
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	ライセンス条件による2段階の点数をつける •許諾契約なしの特許無償または特許なし •許諾契約ありの特許無償	
	標準化・規格化の促進を図るハードルの低さ	アピールポイントによる2～5段階の点数をつける	
	実装コスト低減を図るハードルの低さ	アピールポイントによる2～5段階の点数をつける	
	調達コスト低減を図るハードルの低さ	アピールポイントによる2～5段階の点数をつける	

利用実績調査について(1)

- 利用実績調査における基本的考え方

  2009年度に経済産業省が実施した利用実績調査とほぼ同様の手法を採用

  （手法）

  以下の情報源から利用している暗号技術を調査し、現状での利用実績とみなす

  - 応募暗号及び現リスト掲載暗号の応募者からの情報提供
  - 暗号技術を搭載している市販製品の販売会社へのアンケート
    - 例１：2009年度の利用実績調査の際にアンケート票を送付した企業
    - 例２：市場調査報告書等において売上高調査に協力している企業
  - 政府機関へのアンケート
  - インターネット上で公開されている情報
    - 例１：オープンソースプロジェクト
    - 例２：国際的な民間メジャー規格

利用実績調査について(2)

（想定調査対象数）

- 市販製品：2009年度の利用実績調査時をやや上回る調査数
- 政府機関：10～20程度
- （政府機関を除く）規格等：
  - 国際標準規格（ISO/IEC, ITU, ICAO）
  - 国際的な民間メジャー規格（IETF, IEEE, EMVCo, OMA（携帯電話））
  - 民間の特定団体規格（CAS, DRM, ETC, DNLA, …）：当該規格を管理するコンソーシアム（10～20程度）
- オープンソースプロジェクト（OpenSSL, Mozilla, Linux, FreeBSD, OpenJava, Android, …）：信頼度の高いプロジェクトから20程度

（注意）

- 非公開製品・非公開システム・非公開規格での採用実績などについて、**用意できるどのような手段を用いても確認できないものは実績として考慮しない**

最後に・・・来年度に向けての重要な課題

推奨暗号の個数を絞ることによるデメリットがあるのでは？

米国政府標準暗号＋国産暗号（1 or 少数）	①民間で技術者を抱えられなくなる ⇒ 顕在化が早いかもしれない ②国産暗号の絞り込みが大変 ③絞り込んだとして本当に使われるのか ⇒ 絞り込むことによるメリットを生かせないとやる意味がない	① 暗号研究者の公的機関における雇用が必要（安全な暗号を公的に評価・監視する体制） ② 国産暗号が使われるように振興する目的であることを明確化 ②-1 パテントフリー等の実施 ②-2 推奨リストから外れた組織へのフォロー ②-3 ISO等、標準化機関とのリエゾン関係構築 ③ プロトコル等へ展開（注力先の変更）

■国産暗号の利用促進への取り組みについても検討

- 将来的な目標として、現在の米国政府標準暗号と同じように、標準化や製品化での主導権を日本が取れるようにしていくためのロードマップを描くべきである
- 実際問題として、暗号のバンドル先であるIT製品が米国主導で作られている以上、市場原理で国産暗号が普及していくのを期待することは難しい
- 日本の技術力は高いが、標準化・規格化への提案の仕方に統一性が見られないので、技術力とは関係ない部分で存在感を示せていない