CRYPTREC Report 2010

平成 23 年 3 月

独立行政法人 情報処理推進機構

独立行政法人 情報通信研究機構

「暗号運用委員会報告」

目次

はじめに ……1
本報告書の利用にあたって ……2
委員会構成 ……3
委員名簿 ……4
第 1 章　2010 年度の活動内容と成果概要 ……6
1.1　活動概要 ……6
1.1.1　活動内容 ……6
1.1.2　今年度の委員会の開催状況 ……8
1.2　成果概要 ……9
1.2.1　2010 年度以降の活動計画 ……9
1.2.2　電子政府推奨暗号リストの考え方の明確化に向けた検討 ……10
1.2.3　暗号アルゴリズムの利用実態に関する外部アンケート調査 ……11
1.2.4　監視リストに登録された暗号技術の取り扱いについての検討 ……13
1.2.5　急激な安全性低下に伴う運用委員会としての対応方針 ……14
第 2 章　推奨リストの考え方の明確化に向けた検討 ……15
2.1　暗号に関する外部環境についての整理 ……15
2.1.1　輸出管理状況 ……15
2.1.2　標準化状況等 ……15
2.1.3　暗号製品化状況 ……16
2.2　電子政府推奨暗号の考え方の明確化に向けた評価軸について ……16
2.3　「電子政府推奨暗号リストの考え方」に対するシナリオ ……19
2.4　「電子政府推奨暗号リストの考え方」に対する比較評価 ……22
2.4.1　メリット・デメリットのとりまとめ ……22
2.4.2　シナリオ間比較評価と問題点の洗い出し ……23
2.4.3　シナリオごとの個別評価結果 ……26
第 3 章　暗号アルゴリズムの利用実態に関する外部アンケート調査 ……37
3.1　外部アンケート調査の概要 ……37
3.1.1　調査目的 ……37
3.1.2　調査手法 ……37
3.2　外部アンケート調査結果の概要 ……39
付録 ……43
付録 1　「電子政府推奨暗号リストの考え方」に対するメリット・デメリットのとりまとめ ……44
付録 2　外部アンケート結果概要（抜粋） ……57

はじめに

本報告書は、総務省及び経済産業省が主催している暗号技術検討会の下に設置され、独立行政法人情報処理推進機構及び独立行政法人情報通信研究機構によって共同で運営されている暗号運用委員会の 2010 年度活動報告である。

暗号技術に対する解析・攻撃技術の高度化や新たな暗号技術の開発の進展に伴い、暗号技術の危殆化及び移行対策等を含めた、適切な暗号技術の選択を支援するため、CRYPTREC では、現在の電子政府推奨暗号リストを改訂し、2013 年度から新たな推奨暗号の体系に移行する計画である。新しい電子政府推奨暗号リスト（以下、「次期リスト」という）は、「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」、及び、「リストガイド」から構成され、それらの全体を「CRYPTREC 暗号リスト（仮称）」として公開する予定である。

2010 年度の暗号運用委員会では、昨年度の委員会審議を踏まえ、次期リストを策定するために必要となる暗号技術の製品化・利用実績等の評価に関する検討の準備として、電子政府推奨暗号リストに与える役割を明確化する検討を行った。具体的には、「電子政府推奨暗号リストの考え方」として 4 つの異なるシナリオを設定し、「当該シナリオを採用した」と想定した場合の実施に伴って想定されるメリット（効果）・デメリット（課題）、並びに課題解決への方向性を各シナリオについて取りまとめることを主たる目標に審議を行った。

合わせて、現在の「電子政府推奨暗号リスト」の課題点を抽出し、次期リストをどのような考え方のもとで作成することがよいのかについての情報を得ることを目的として、国内外の主要ベンダを中心に外部アンケートを実施した。本アンケート調査結果は、上記の「電子政府推奨暗号リストの考え方」に対するシナリオでの特徴的なメリット・デメリットの抽出等を検討するうえでの基礎情報として取り扱った。

今年度の運用委員会で取りまとめた結果は、電子政府推奨暗号リストを含む次期リスト全体の方向性を今後政府部内で議論する際の客観的資料として用いることを想定しており、暗号技術検討会での審議を経て、総務省及び経済産業省に報告されることとなっている。

次年度以降は、政府部内等での議論を踏まえ決定された電子政府推奨暗号リストの考え方に基づき、その考え方を具体的に反映するための製品化、利用実績、国際標準化等の評価手法について調査・検討を行う予定である。

末筆ではあるが、本活動に様々な形でご協力下さった委員の皆様、関係者の皆様に対して深く謝意を表する次第である。

暗号運用委員会 委員長 佐々木 良一

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。例えば、電子署名や GPKI[1] システム等、暗号関連の電子政府関連システムに関係する業務に従事している方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書は、第 1 章には 2010 年度の暗号運用委員会の活動内容と成果概要、第 2 章には電子政府推奨暗号リストの考え方の明確化に向けた検討結果、第 3 章には暗号アルゴリズムの利用実態に関する外部アンケート調査結果を記述した。

2009 年度以前の CRYPTREC Report は、CRYPTREC 事務局（総務省、経済産業省、独立行政法人情報通信研究機構、及び独立行政法人情報処理推進機構）が共同で運営する下記の Web サイトから参照できる。

http://www.cryptrec.go.jp/report.html

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

【問合せ先】 info@cryptrec.go.jp

[1] GPKI：Government Public Key Infrastructure（政府認証基盤）

委員会構成

暗号運用委員会（以下「運用委員会」）は、図 1 に示すように、総務省と経済産業省が共同で共催する暗号技術検討会の下に設置され、独立行政法人情報処理推進機構（IPA）と独立行政法人情報通信研究機構（NICT）が共同運営している。

運用委員会は、新しい電子政府推奨暗号リスト（以下「次期リスト」）を策定・運用していくにあたって必要となる暗号技術の運用を主な対象とする調査・検討を行う。具体的には、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。特に、次期リスト策定における暗号技術に対する製品化・利用実績等の評価について評価手法の検討を行い、さらに、電子政府推奨暗号と国際標準技術との整合性も検討する。また、電子政府システムの危殆化対策について検討を行う。

運用委員会と連携して活動する「暗号方式委員会」及び「暗号実装委員会」も、運用委員会と同様、暗号技術検討会の下に設置され、IPA と NICT が共同で運営している。

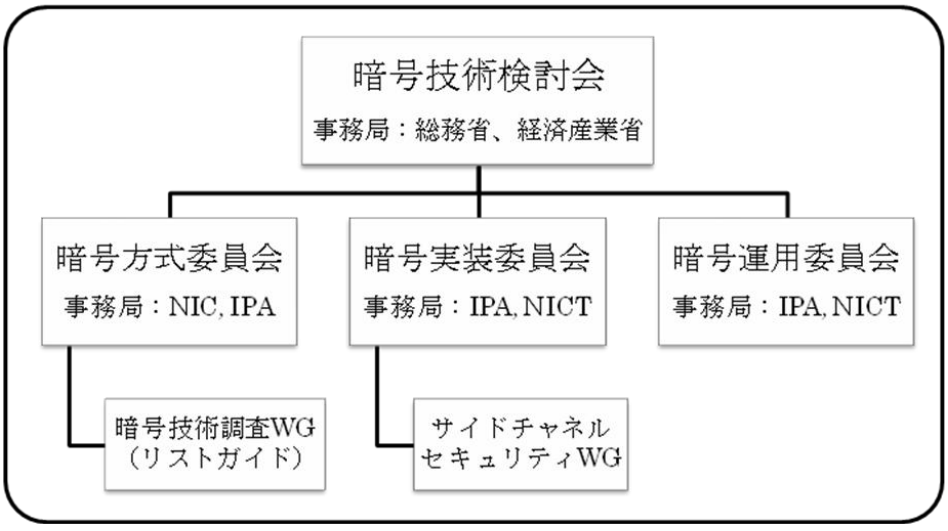


図 1　2010 年度の CRYPTREC の体制

委員名簿

暗号運用委員会 （2011 年 3 月現在）

委員長	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
委員	大岩　寛	独立行政法人産業技術総合研究所 情報セキュリティ研究センター ソフトウェアセキュリティ研究チーム　研究員
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　教授
委員	小松　文子	独立行政法人情報処理推進機構　セキュリティセンター 情報セキュリティ分析ラボラトリー　ラボラトリー長
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	手塚　悟	東京工科大学　コンピュータサイエンス学部　教授
委員	松尾　真一郎	独立行政法人情報通信研究機構 情報通信セキュリティ研究センター セキュリティ基盤グループ　主任研究員
委員	北村　伸弘	日本電気株式会社　第一システムソフトウェア事業部 マネージャー
委員	佐野　文彦	東芝ソリューション株式会社　IT 技術研究所 研究開発部　情報セキュリティラボラトリー　研究主務
委員	下江　達二	富士通株式会社 ソフトウェアＢＧミドルウェア事業本部 システム・マネジメント・ミドルウェア事業部 第三開発部　部長
委員	羽根　慎吾	株式会社日立製作所　システム開発研究所 第七部 702 研究ユニット　主任研究員
委員	前田　司	EMC ジャパン株式会社　RSA 事業本部 テクニカルサポート技術部　部長
委員	宮崎　一哉	三菱電機株式会社　情報技術総合研究所 情報システム構築技術部　チームリーダ

オブザーバ

中嶋　良彰	内閣官房　情報セキュリティセンター　内閣参事官補佐
山口　利恵	内閣官房　情報セキュリティセンター　主査

根本　農史	内閣官房　情報セキュリティセンター　主査
松宮　志麻	総務省　行政管理局　行政情報システム企画課　課長補佐
山中　豊	経済産業省　産業技術環境局　情報電子標準化推進室　課長補佐
日高　隆	経済産業省　大臣官房　情報システム厚生課 セキュリティ担当課長補佐
石川　正興	防衛省　技術研究部　電子装備研究所　ネットワーク技術研究部 情報セキュリティ研究室長

事務局

独立行政法人　情報処理推進機構

矢島　秀浩
山岸　篤弘
近澤　武
神田　雅透
大熊　建司
小暮　淳
鈴木　幸子

独立行政法人　情報通信研究機構

高橋　幸雄
近藤　玲子
田中　秀磨
黒川　貴司
大久保　美也子
側高　幸治
金森　祥子
笠井　祥

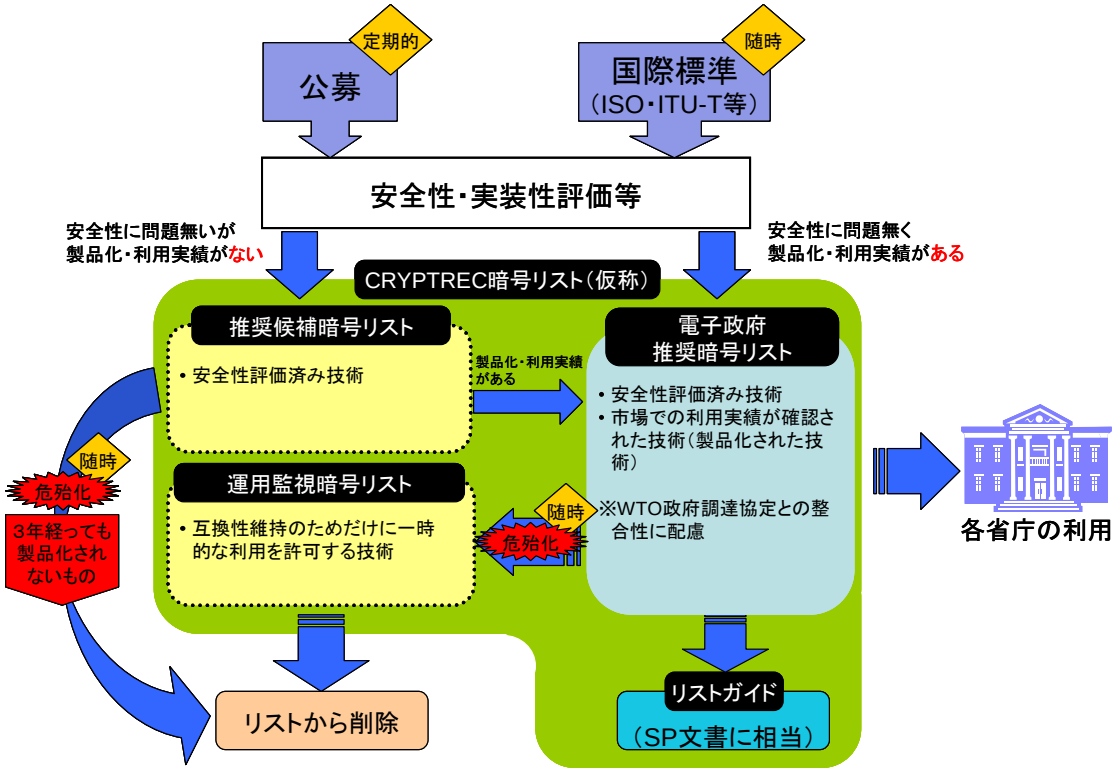
第１章　2010 年度の活動内容と成果概要

1.1　活動概要

1.1.1　活動内容

暗号技術に対する解析・攻撃技術の高度化や新たな暗号技術の開発の進展に伴い、暗号技術の危殆化及び移行対策等を含めた、適切な暗号技術の選択を支援するため、CRYPTREC では、2012 年度末の電子政府推奨暗号リストの改訂（以下、「次期リスト」という）に向けた検討を行っているところである。

次期リストは、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から構成され、CRYPTREC 暗号リスト（仮称）として公開する予定である。次期リスト掲載の対象となる暗号技術は、政府等による調達等を容易にすることを目的として、「安全性」及び「実装性」の観点に加え、「製品化、利用実績等」の観点も踏まえて、いずれかのリストに分類・登録される。登録は、WTO 政府調達協定との整合性に配慮しつつ、安全性や市場動向により決定するとともに、一定の間隔で見直すこととしている。



（参考）次期リストの役割[2]

- 電子政府推奨暗号リスト（以下、「推奨リスト」ともいう）

  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する（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る。

- 推奨候補暗号リスト（以下、「候補リスト」ともいう）

  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る。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る。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る。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る。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る。

- 運用監視暗号リスト（以下、「監視リスト」ともいう）

  電子政府推奨暗号リストに登録されていたが、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もののうち、互換性維持のために継続利用を容認するもののリスト。暗号解読のリスクと、電子政府システムにおける移行コスト等を勘案して、定期的に掲載継続の可否を判断する。CRYPTREC として互換性維持以外の目的では利用を推奨しない。

暗号運用委員会では、次期リスト策定における「暗号技術に対する製品化・利用実績等の評価」についての評価手法の検討を行うに当たり、昨年度の委員会審議を踏まえ、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性を認識した。そのため、今年度は主に電子政府推奨暗号リストの考え方の明確化について検討を行うこととした。具体的には、「電子政府推奨暗号リストの考え方」として 4 つの異なるシナリオを設定し、「当該シナリオを採用したと想定」した場合の実施に伴って想定される「メリット（効果）・デメリット（課題）」、並びに課題解決への方向性を各シナリオについて取りまとめることを主たる目標に審議を行った。

合わせて、現在の「電子政府推奨暗号リスト」の課題点を抽出し、次期リストをどのような考え方のもとで作成することがよいのかについての情報を得ることを目的として、国内外の主要ベンダを中心に外部アンケートを実施した。本アンケート調査結果は、上記の「電子政府推奨暗号リストの考え方」に対するシナリオでの特徴的なメリット・デメリットの抽出等を検討するうえでの基礎情報として取り扱うものとした。

[2] 今後の審議結果によっては、各リストの役割や定義が適切な表現等に見直されることがあり得ることに留意されたい。

今年度の運用委員会で取りまとめた結果は、電子政府推奨暗号リストを含むCRYPTREC 暗号リスト（仮称）全体の方向性を今後政府部内で議論する際の客観的資料として用いることを想定しており、暗号技術検討会での審議を経て、総務省及び経済産業省に報告されることとなっている。

このほか、第 1 回暗号技術検討会における審議結果に基づき、急激な安全性低下に伴う暗号運用委員会としての対応方針について審議を行った。

1.1.2 今年度の委員会の開催状況

2009 年度第 2 回暗号技術検討会において、2010 年度の暗号運用委員会での活動項目が以下の通り承認された。

(1) 暗号技術の製品化、利用実績等の評価手法の検討

電子政府暗号推奨リストに登録された暗号技術の利用者、市場における利用実績、国際標準化等に関する 2009 年度の議論を踏まえ、暗号技術の製品化・利用実績の評価手法に関する調査・検討を行い、評価項目の具体化、判断基準の検討等を行う。

また、WTO 政府調達協定との整合性に配慮する観点から、国際標準化された暗号技術、国際的な標準化団体における標準の取り扱い等について調査・検討を行う。

(2) 運用監視暗号リストに登録された暗号技術に関する検討

暗号技術の製品化、利用実績等の評価等を踏まえ、危殆化対策について調査・検討を行う。情報システムの移行における課題を整理しつつ、運用監視暗号リストに登録される暗号技術の取り扱い等について調査・検討を行う。

本年度の暗号運用委員会では、上記事項の具体的検討を行うにあたり、

① 2010 年度以降の活動計画の承認
② 電子政府推奨暗号リストの考え方の明確化に向けた検討
③ 暗号アルゴリズムの利用実態に関する外部アンケート調査
④ 監視リストに登録された暗号技術の取り扱いについての検討
⑤ 急激な安全性低下に伴う運用委員会としての対応方針

について審議を行うこととし、2010 年度の暗号運用委員会は計 5 回開催された。各回会合の概要は表 1 のとおりである。また、第 2 回委員会から第 4 回委員会までの期間を利用し、外部アンケート調査を実施した。

表 1.　暗号運用委員会の開催

回	開催日時	主な議題
第 1 回	2010 年 9 月 14 日	● 暗号運用委員会活動方針について ● 電子政府推奨暗号リストの考え方の明確化に向けた論点整理について ● 運用監視暗号リスト等に掲載される暗号技術の取り扱い方法について
第 2 回	2010 年 11 月 4 日	● 外部アンケート調査について ● 電子政府推奨暗号リストの考え方の明確化に向けたシナリオ再整理について ● シナリオ議論の論点整理について
	2010 年 12 月 ～2011 年 2 月	外部アンケート調査
第 3 回	2011 年 1 月 20 日	● シナリオ議論における論点項目のとりまとめについて ● 急激な安全性の低下時における運用委員会の役割について
第 4 回	2011 年 2 月 24 日	● アンケート調査結果について ● シナリオ議論における比較評価表のとりまとめについて ● 急激な安全性の低下時における運用委員会の役割について（第 2 回）
第 5 回	2011 年 3 月 2 日	● 暗号運用委員会の活動報告（2010 年度 CRYTREC 合同委員会）

1.2　成果概要

1.2.1　2010 年度以降の活動計画

2009 年度第 2 回暗号技術検討会で承認された活動計画に基づき、第 1 回運用委員会にて暗号運用委員会の今後 3 年間の活動内容及びスケジュールが次のように再整理された。

- **2010 年度活動内容：電子政府推奨暗号の考え方の明確化**

  以下の項目について議論を行い、その結果を取り纏めて電子政府推奨暗号リストの考え方（案）として暗号技術検討会に報告し、審議を求める。

✧ 電子政府推奨暗号リストに何を求めるのか
✧ その際のメリット（効果）・デメリット（課題）は何か
✧ デメリット（課題）に対してどのように対応すべきか

- **2011 年度活動内容：製品化、利用実績等の評価手法の検討**

  電子政府推奨暗号リストの考え方を具体的に反映するための製品化、利用実績、国際標準化等の評価手法について、2009 年度の議論を踏まえて検討を行う。

- **2012 年度活動内容：製品化、利用実績等の評価**

  2011 年度の検討結果を踏まえて、実際の製品化、利用実績、国際標準化等の調査・評価を行い、次期電子政府推奨暗号リスト改訂に反映させる。

1.2.2 電子政府推奨暗号リストの考え方の明確化に向けた検討

推奨リストと候補リストとの関係では、「市場における利用実績が十分か」及び「国際標準化機関等での標準化が進んでいるか」が両リストを区分けする評価基準となっている。昨年度の暗号運用委員会では、製品化・利用実績及び国際標準化状況を評価するうえでの課題洗い出しや調査方法について審議を行った。その結果、電子政府推奨暗号リストの考え方によって設定すべき評価基準が大きく異なる可能性が出てきた。

以上の指摘を踏まえ、今年度の暗号運用委員会としては、評価基準を決める前提となる「電子政府推奨暗号リストの考え方」を明確化するための審議を行うこととした。

具体的には、「電子政府推奨暗号リストの考え方」として 4 つの異なるシナリオを設定し、「当該シナリオを採用したと想定」した場合の実施に伴って想定される「メリット（効果）・デメリット（課題）」の抽出、並びに課題解決への方向性を各シナリオについて取りまとめた。評価軸として設定した検討項目は以下のとおりである。

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

また、以上の検討結果をもとに、各評価軸のメリット度合いを「評価点」としてシナリオごとに採点し、4 段階を基準としたレーダーチャートとして取りまとめた。なお、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した。

詳細については第 2 章を参照されたい。なお、本検討結果は、電子政府推奨暗号リストを含む CRYPTREC 暗号リスト（仮称）全体の方向性を今後政府部内及び暗号技術検討会で議論する際の客観的資料として用いることを想定しており、暗号運用委員会として方向性の結論を出したものではないことに注意されたい。

1.2.3 暗号アルゴリズムの利用実態に関する外部アンケート調査

現在の電子政府推奨暗号リストは技術的観点のみから作成されたものである。しかし、実際の電子政府情報システムの構築及び暗号搭載製品の開発・製造の現場においては、必ずしも技術的観点だけで暗号アルゴリズムの選択が行われているわけではない。

そこで、現在の「電子政府推奨暗号リスト」の課題点を抽出し、「CRYPTREC 暗号リスト（仮称）」をどのような考え方のもとで作成することがよいのかについての情報を得ることを目的として、国内外の主要ベンダを対象にアンケート調査を実施した。

具体的には、以下の項目についての情報を主に把握することを目的とする。

- 暗号搭載製品の開発や製造、情報システムの構築等における暗号利用（とりわけ暗号アルゴリズムの選択プロセス）に関する実態を把握すること
- 現在の「電子政府推奨暗号リスト」の活用実態を把握すること
- 「CRYPTREC 暗号リスト（仮称）」や CRYPTREC に期待すること
- 暗号搭載製品の開発や製造、情報システムの構築等における提案暗号（国産暗号）に対する認識を広く把握すること

本調査では、運用委員会が選定した以下の 17 カテゴリの各々シェアトップ級ベンダとシステムインテグレータ、並びに政府機関を調査対象先として選定した。その中には、CRYPTREC が実施している前回公募(2001 年)または今回公募（2009 年）に応募した暗号技術（以下、「提案暗号」という）を開発している企業（以下、「応募会社」という）の事業部門及びその関連会社3の事業部門（以下、両事業部門を合わせて「応募ベンダ」という）も含む。

[3] 応募会社の出資率が 50%超の企業のことを指す。

また、応募会社の暗号開発部門（以下、「応募者」という）に対しては、開発部門としての現状認識を別途質問した。

＜対象カテゴリ＞

- 官公庁向けシステムインテグレータ
- オペレーションシステム
- ブラウザ
- アプリケーションソフトウェア（ブラウザを除く）
- 暗号ライブラリ（暗号アルゴリズムを集めたソフトウェア）
- ルータ
- セキュリティアプライアンス製品
- サーバ／ストレージ
- HSM／PKI システム／認証局システム
- IC カード
- 半導体チップ
- デジタル複合機
- 輸入販売代理による輸入製品
- 固定網／NGN 通信事業者
- 携帯電話通信事業者
- サービスプロバイダ
- タイムスタンプビジネス

最終的に、ベンダ全 39 社（67 プロダクト）、システムインテグレータ全 8 社（11 システム）、政府機関全 4 府省（6 システム）、全応募者から回答を得ることができた。ベンダ及びシステムインテグレータで協力いただいた企業は以下のとおりである（順不同、公表不可を除く）。

詳細については第 3 章を参照されたい。

● ベンダ

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
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

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
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
他、全 39 社・67 プロダクト

● システムインテグレータ

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
他、全 8 社・11 システム

1.2.4 監視リストに登録された暗号技術の取り扱いについての検討

当初予定していた運用監視暗号リスト等に掲載される暗号技術の取り扱い方法については、第 1 回委員会で論点整理を始めたものの、電子政府推奨暗号リストを含む CRYPTREC 暗号リスト（仮称）全体の方向性の議論と密接に関連することから、次年度以降、CRYPTREC 暗号リスト（仮称）全体の方向性が固まってから検討を再開することとした。

今後の論点としては、

- 代替手段がある場合とそうでない場合とで、電子政府推奨暗号リストから運用監視暗号リストへの遷移基準を変えるべきか否か
- 安全性上は多少の難点があるが、代替手段が実質的にない、もしくは代替手段を無理に取ろうとすればコスト高になることが明らかな場合でも、運用監視暗号リストに移行するほうが合理的か否か
- 各リストにおける注釈の付け方をどのようにすべきか
- 運用監視暗号リストの実運用フロー（遷移手順等）をどのようにするか

などが挙げられた。

1.2.5　急激な安全性低下に伴う運用委員会としての対応方針

今年度は、第１回暗号技術検討会における審議結果に基づき、急激な安全性低下に伴う暗号運用委員会としての対応方針について審議を行った。

急激な安全性低下とは、従来の安全性評価の将来予測から大きく外れ、かつ状況によっては実害が発生しうるような想定外の事態が発生した、もしくは発生する恐れが非常に懸念される状態のことを指すものとする。したがって、暗号の世代交代のような、安全性評価の将来予測に基づいて（不定期に開催される）通常の暗号運用委員会で当該暗号アルゴリズムの取り扱い方法を審議する状態とは区別する。

以上の前提の上で、急激な安全性低下の発生時に「電子政府推奨暗号リストからの除外や利用制限」を緊急に実施すべきか否か等を判断するために発動される緊急対応に対し、暗号運用委員会としての対応方針案を検討した。本検討結果は、暗号技術検討会事務局に報告され、方式委員会及び実装委員会としての対応方針と合わせ、CRYPTREC全体としての対応方針を検討する材料として使われる。

第 2 章　推奨リストの考え方の明確化に向けた検討

2.1　暗号に関する外部環境についての整理

「調達容易性」及び「標準化・規格化等への影響」について検討を進めていく際の前提として、暗号に関する外部環境についての現状を以下に整理する。

2.1.1　輸出管理状況

2000 年以前は米国政府が暗号技術の 輸出管理を厳格に実施しており、金融サービス向け等の一部例外を除いて、高強度の米国政府標準暗号の米国からの輸出は困難であった。しかし、2000 年に米国政府が暗号技術に対する輸出管理規定を大幅に緩和したことにより、現在では以下のような状況が生まれている。

- 特定地域（イラン、イラク、リビア、北朝鮮、アフガニスタン等）向けを除いて、国際的に暗号技術の輸出規制が大幅に緩和
- 日本市場向けは無制限・無条件に高強度の米国政府標準暗号が利用可能
- 実務面からは輸出管理としてチェックシート（パラメータシート）を作る必要がある。このなかでは該当する暗号名を明示する必要があり、AES など有名な暗号はともかく、独自暗号の場合にはきちんとした証書を作らなければならないという心理的な障壁をシステムインテグレータは持っている。その結果、アジアなどへの輸出を考えると独自暗号の採用を躊躇する要因となる
- 米国での輸出管理手続きが変わり、30 日間のソースコードレビューを受けることが必要になった。「自由に輸出可能」にはなっているが、手続きとして様々な実務的ハードルが残る

2.1.2　標準化状況等

暗号アルゴリズムは「武器」扱いのため標準化になじまないと判断されていた時期もあったが、現在では多くの標準化・規格化において暗号アルゴリズムが規定されるようになった。以下では現在の評価状況等について整理する。

- ISO/IEC では、従来方針を変更し、国際標準規格（ISO/IEC 18033）を策定。同時に暗号登録制度を廃止
- IETF 等、ISO/IEC 以外の多くの標準化団体でも米国政府標準暗号を必須採用
- 米国政府標準暗号（楕円暗号系を除く）は世界中特許無償で使える
- 欧米を主体に“Unclassified but sensitive”クラス（及びランクの低い

“Classified”クラス）の情報保護手段として米国政府標準暗号が指定されているケースがある

- 標準化の目的について、“お墨付きを与える”との意味合いが強い「カタログ的標準（使うかどうかわからないがとりあえず載せておく）」を定めるのか、“当該暗号による相互接続性を担保する”との意味合いが強い「必須的標準（多くのユーザが使うと考えられるものだけに限定する）」を定めようとするのか、との間で議論が起きている
- “必須的標準”を定めようとする標準化の場合、米国政府標準暗号に対するバックアップがそもそも必要かという点から議論されることも多い（後でアルゴリズムを追加する仕組みはあってもいいが、バックアップを現時点で決める必要はない、必要最小限にとどめるべきという論理）
- BRICs（特にロシアと中国）や韓国などは、WTO/TBT 協定への対応と実際の製品化を促す観点から、国策として当該国の政府標準暗号の国際標準化を ISO/IEC や IETF などの様々な標準化の場で同時並行的に強力に推進している

2.1.3 暗号製品化状況

過去には米国政府標準暗号以外の暗号アルゴリズムを搭載した暗号製品も多数存在したが、2009 年度に経済産業省が実施した「暗号モジュールの市場動向等に関する調査研究」の調査結果の報告によれば、以下の状況が読み取れる。

- 調査対象となったほとんどの暗号製品で米国政府標準暗号を搭載するのが主流となった。例えば、128 ビットブロック暗号搭載製品の 96%に AES が、64 ビットブロック暗号搭載製品の 87%に Triple DES が、署名搭載製品の 99%に RSA 署名が、ハッシュ関数搭載製品の 96%に SHA-1 がそれぞれ搭載されている。
- オープンソースコミュニティでも米国政府標準暗号を搭載するのが主流となった
- 電子政府推奨暗号リストに掲載されていない独自暗号（だけ）を搭載していることをメインに掲げているような製品はほとんど見かけなくなった

2.2 電子政府推奨暗号の考え方の明確化に向けた評価軸について

「電子政府推奨暗号リストの考え方」として 4 つの異なるシナリオを設定し、「当該シナリオを採用したと想定」した場合の実施に伴って想定される「メリット（効果）・デメリット（課題）」の抽出、並びに課題解決への方向性を各シナリオについて取りまとめるにあたり、そのための評価軸として、従来は「安全性」と「利用実績」が取り上げられてきた。

一方、第 1 回暗号運用委員会において、「暗号政策的観点」、「国際競争力」、「提案暗号

（国産暗号）の取り扱い」、「人材育成」、「リストに対するユーザの使いやすさ」等といった「安全性」と「利用実績」以外の評価軸も考える必要があるのではないかとの指摘があった。

以上の指摘を受け、「標準化活動を通じた国際競争力向上」、「提案暗号（国産暗号）の取り扱い」、「人材育成」の 3 項目を「暗号政策的観点」での主要な構成要素をなすものとして取り上げることとした。最終的に、6 つの評価軸についてメリット・デメリットを検討する際の論点項目を以下のように設定した。

A) 「安全性」に関する検討項目

(A-1) 電子政府推奨暗号アルゴリズムの安全性評価の充実度や監視活動の効率化に与える影響度の違い

(A-2) 電子政府推奨暗号アルゴリズムの安全性評価・監視活動の実施能力に与える影響度の違い

(A-3) 電子政府推奨暗号アルゴリズムの危殆化に伴う影響度の違い

(A-4) 電子政府推奨暗号アルゴリズムの危殆化対策（バックアップ）を日本政府の独自判断に基づいて実施することの実現可能性の違い

(A-5) その他、安全性に関する項目

B) 「調達容易性」に関する検討項目

(B-1) 電子政府推奨暗号リストと政府調達・製品製造段階での利用暗号アルゴリズム選択に関する相関度の違い

(B-2) 電子政府推奨暗号アルゴリズムの危殆化対策済み（バックアップ搭載）製品の調達コストに与える影響度の違い

(B-3) 電子政府推奨暗号アルゴリズムが政府調達におけるベンダロックイン（応募ベンダからしか事実上調達できない）の原因となる可能性の違い

(B-4) 電子政府推奨暗号アルゴリズムを選定する際の現在の利用実績の重要度の違い

(B-5) その他、電子政府推奨暗号アルゴリズムの搭載製品・システム調達等における調達容易性に関する項目

C) 「標準化・規格化等への影響」に関する論点項目

(C-1) ISO/IEC や ITU の国際標準化策定に与える影響度の違い

(C-2) ISO/IEC や ITU 以外の様々な規格化（例えば IETF や IEEE など）等の活動に与える影響度の違い

(C-3) 応募会社による標準化・規格化等への活動に対するモチベーションの違い

(C-4) その他、電子政府推奨暗号アルゴリズムの標準化・規格化等の活動全体に与える影響に関する項目

D) 「提案暗号（国産暗号）の利用促進」に関する論点項目

(D-1) （応募会社以外の企業・団体等が）電子政府推奨暗号リストに選定された提案暗号（国産暗号）をサポートすることに対するモチベーションの違い

(D-2) 電子政府推奨暗号リストに選定された提案暗号（国産暗号）の知的所有権（特許ライセンス）を全世界特許無償化（worldwide royalty-free）することによる当該暗号アルゴリズムの利用促進効果の違い

(D-3) 応募会社による提案暗号（国産暗号）の利用促進活動に対するモチベーションの違い

(D-4) 電子政府推奨暗号リストに選定された提案暗号（国産暗号）の利用促進活動を政策的に支援した場合のコストパフォーマンスの違い

(D-5) その他、電子政府推奨暗号リストに選定された提案暗号（国産暗号）の利用促進効果に関する項目

E) 「セキュリティ研究体制への影響」に関する評価項目

(E-1) 企業が新しい暗号アルゴリズムを開発することの位置づけ／モチベーションの違い

(E-2) 日本全体としての暗号研究体制に与える影響度の違い

(E-3) セキュリティ分野の競争力強化に向けた日本全体としてのセキュリティ研究体制の見直し機運につながる影響度の違い

(E-4) その他、セキュリティ研究体制の維持向上への影響に関する項目

F) 「CRYPTREC 活動成果」に関する評価項目

(F-1) 電子政府推奨暗号リストと推奨候補暗号リストとに分割することによる効果の違い

(F-2) 推奨候補暗号リストの位置づけの違い

(F-3) CRYPTREC 活動による成果利用全般に対するコストパフォーマンスの違い

(F-4) その他、CRYPTREC 活動成果に関する項目

2.3 「電子政府推奨暗号リストの考え方」に対するシナリオ

「電子政府推奨暗号の考え方」の 4 つのシナリオは、それぞれ異なる設定意図を参考として、以下のとおりに設定した。

【シナリオ 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)】
CRYPTREC は今まで技術的側面で評価を実施してきたので、電子政府推奨暗号リストの掲載個数を限定するために、**「現状の調達容易性（利用実績)」を主たる判断材料**とし、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**して電子政府推奨暗号リストと推奨候補リストとの区分を行う。

【本シナリオの設定意図】

暗号方式委員会にて「安全である」と判断されない限りは、「電子政府推奨暗号リスト」はもとより「推奨候補暗号リスト」にさえ掲載されることはない。したがって、両リストの差異は「市場における利用実績が十分か否か」の観点しかない。

一方、2000 年の暗号輸出規制緩和以降は、事実上米国政府標準暗号だけが様々な国際標準化・規格化や製品化の対象として扱われ、そのほかの暗号は様々な国際標準化・規格化もしくは製品化から排除される流れが強まるなど、暗号をめぐる国際環境はこの 10 年で大きく変貌している。このことは、2009 年度に経済産業省が実施した暗号製品採用実績調査結果とも合致している。

以上の点を考慮すれば、「市場における利用実績（調達容易性）が十分か否か」の判断は、**2009 年度（もしくは 2011 年度に再実施する）暗号製品採用実績調査結果をベースに考えれば事実上十分**であるといえる。

【本シナリオの前提条件】

- 政府調達されるシステム・製品は、調達可能製品[4]をそのまま利用、もしくは調達可能製品をベースに開発されているケースが多い
- 電子政府推奨暗号リストに掲載されている特定の暗号アルゴリズム名（とりわけ米国政府標準暗号以外）を指定してシステム・製品を調達するケースは非常に少ない
- 「市場における調達容易性が十分」と判断されるには、調査時点で多数の企業等が販売している多種多様な調達可能製品に当該暗号アルゴリズムが搭載されていることが必要

[4] 「政府の情報システムでも利用される一般市販製品」のことを意味する。

【シナリオ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)】
「現状での調達容易性（利用実績)」だけで判断した場合には米国政府標準暗号のみが電子政府推奨暗号リストに掲載される可能性が高いうえ、米国政府標準暗号以外の暗号は国際標準化・製品化からも排除される流れが強まっている。
本シナリオでは、上記の点を考慮し、**「安全性」、「現状の調達容易性（利用実績)」ならびに「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（国産暗号）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**して、電子政府推奨暗号リストと推奨候補リストとの区分を行う。

【本シナリオの設定意図】

2000 年の暗号輸出規制緩和以降は、事実上米国政府標準暗号だけが様々な国際標準化・規格化や製品化の対象として扱われ、そのほかの暗号は国際標準化・規格化もしくは製品化から排除される流れが強まるなど、暗号をめぐる国際環境はこの 10 年で大きく変貌している。

結果として、多数の提案暗号が現在の電子政府推奨暗号リストに掲載されているにもかかわらず、応募会社以外からのサポートがほとんど受けられないがゆえに、提案暗号の国際標準化・規格化、及び製品化が進んでいないのが実状である。加えて、米国政府標準暗号は「その他評価が必要な暗号」としてすでに取り扱われており、仮に提案暗号が１個も電子政府推奨暗号リストに掲載されなくても政府調達手段として困ることはない。

このような現状を鑑みると、電子政府推奨暗号リストにおける提案暗号をどのように取り扱うべきかについて検討しなおす必要がある。そのひとつの考え方として、日本（政府）が利用する（少数個の）対象暗号を明確にすることにより、**当該暗号の様々な国際標準化・規格化、並びに製品化が国内外で促進され、製品調達が容易になることを期待する手段として電子政府推奨暗号リストを活用**することが考えられる。

【本シナリオの前提条件】

- 政府調達されるシステム・製品は、調達可能製品をそのまま利用、もしくは調達可能製品をベースに開発されているケースが多い
- 日本（政府）が利用する対象暗号を明確にすることは、当該暗号の様々な標準化・製品化を日本（政府）が有形無形の形で事実上支援することになる可能性がある。このため、当該暗号が特定企業に有利に作用するベンダロックインの原因となるような事態、もしくは当該暗号の普及展開活動上の支障が発生する事態は避けるべきであり、事前にそのための対策をとっておく必要がある（とりわけ知的財産権の取り扱い）
- 電子政府推奨暗号リストに選定される提案暗号は、米国政府標準暗号に次ぐ位置づけにある（もしくは次ぐ位置づけを明確に目指している）と国際的に認められる程

度の普及度を実現する必要がある

【シナリオ 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）】
「現状での調達容易性（利用実績）」だけで判断した場合には米国政府標準暗号のみが電子政府推奨暗号リストに掲載される可能性が高いため、2012 年度末に CRYPTREC 暗号リスト（仮称）が改訂されるのに合わせて、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会社に持たせる必要がある。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導入することにより、将来的に電子政府推奨暗号リストの掲載個数を削減する余地を残す。
本シナリオでは、上記の点を考慮し、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**して、電子政府推奨暗号リストと推奨候補リストとの区分を行う。

【本シナリオの設定意図】
当初から「電子政府推奨暗号リスト」と「推奨候補暗号リスト」に区分されてしまうと、「推奨候補暗号リスト」に入れられた（電子政府推奨暗号リストに掲載されなかった）提案暗号は一段格下の暗号と市場から受け取られる可能性があり、普及展開活動を行う上でマイナスの影響を及ぼす恐れがある。
一方で、ひとたび電子政府推奨暗号リストに掲載された後は利用実績や普及展開が思わしくなくても継続して掲載され続けることになれば、提案暗号の普及展開を強力に実施しない可能性がある。
以上の点を考慮すれば、一定期間経過後の普及状況を厳格に判定するルールを定め、**利用実績や普及展開が思わしくない提案暗号を電子政府推奨暗号リストから降格**させることにより、将来的に電子政府推奨暗号リストの掲載個数を削減する余地を残しつつ、削減に伴う国内におけるセキュリティ研究開発体制への影響軽減に一定の配慮を行うやり方が考えられる。

【本シナリオの前提条件】
- 政府調達されるシステム・製品は、調達可能製品をそのまま利用、もしくは調達可能製品をベースに開発されているケースが多い
- 「市場における調達容易性が十分」と判断されるには、調査時点で多数の企業等が販売している多種多様な調達可能製品に当該暗号アルゴリズムが搭載されていることが必要
- 「電子政府推奨暗号リスト」から「推奨候補暗号リスト（もしくは監視暗号リスト）」への降格ルールの導入が必須（現状では、降格ルールの導入は想定されていない）

【シナリオ 4（政府調達の選択肢としての提示。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。
本シナリオでは、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とする。

【本シナリオの設定意図】

提案暗号は電子政府推奨暗号になっても市場でほとんど利用してもらえない現実があり、提案暗号の普及展開への取り組みに対して現在の電子政府推奨暗号リストが役に立っていないことは明らかである。

一方で、電子政府推奨暗号リストに入らなければ政府調達に向けた選択肢として認めてもらえず、応募会社さえも提案暗号の普及展開への取り組みをしなくなり、結果として国内におけるセキュリティ研究体制に対して大きなマイナスの影響を与える恐れがある。加えて、電子政府推奨暗号リストの掲載個数を削減したからといって、電子政府推奨暗号リストに掲載された提案暗号が市場で使われるようになる保証はない。

以上の点を考慮すれば、現状とほぼ同様の構成とすることによって、**政府調達に向けた選択肢の提示だけに役割をとどめ**、提案暗号の国際標準化・製品化促進の手段としては考えない。

【本シナリオの前提条件】

- 安全性上の問題が発見されるか自主的な取り下げ等がなければ、電子政府推奨暗号リストからの削除はしない
- 電子政府推奨暗号リストに掲載されている少なくとも一つの提案暗号と同程度の普及展開が図られれば候補暗号リストから推奨暗号リストに昇格させる
- 電子政府推奨暗号リストに掲載される各暗号の「市場における調達容易性」が大きく異なっていてもよい

2.4 「電子政府推奨暗号リストの考え方」に対する比較評価

2.4.1 メリット・デメリットのとりまとめ

2.3 節で設定したシナリオ 4 つ個々について、2.2 節で定めた 6 つの評価軸における論点項目ごとに、当該シナリオを実施したと想定したときのメリット（効果）やデメリット（課題）等を検討した。検討にあたっては、2.1 節の現状認識及び 3 章の外部アンケート調査結果も判断材料として利用した。

各論点項目において、基本的にプラス面の効果が考えられる場合には「メリット」、マイナス面の影響が考えられる場合には「デメリット」として取り扱うものとした。なお、同一の論点項目について「メリット」と「デメリット」の両方が考えられる場合には「両

論併記」とする。また、メリット・デメリットのどちらとも言えないが、注意する必要がある点については「留意点」として挙げることとした。

（例）

A)「安全性」に関する検討項目

(A-1) 電子政府推奨暗号アルゴリズムの安全性評価の充実度や監視活動の効率化に与える影響度の違い

- ✧ 安全性評価の充実度向上や監視活動の効率化が期待できるなど、プラス面が考えられる場合はメリットとして扱う
- ✧ 安全性評価の充実度低減やばらつきが生じる、監視活動の効率化が阻害されるなど、マイナス面が考えられる場合はデメリットとして扱う
- ✧ メリットやデメリットではないコメント等が必要な場合には留意点として取り扱う

以上の検討により洗い出した各シナリオ・各評価軸におけるメリット、デメリット、留意点を取りまとめた結果を参考１に示す。

2.4.2　シナリオ間比較評価と問題点の洗い出し

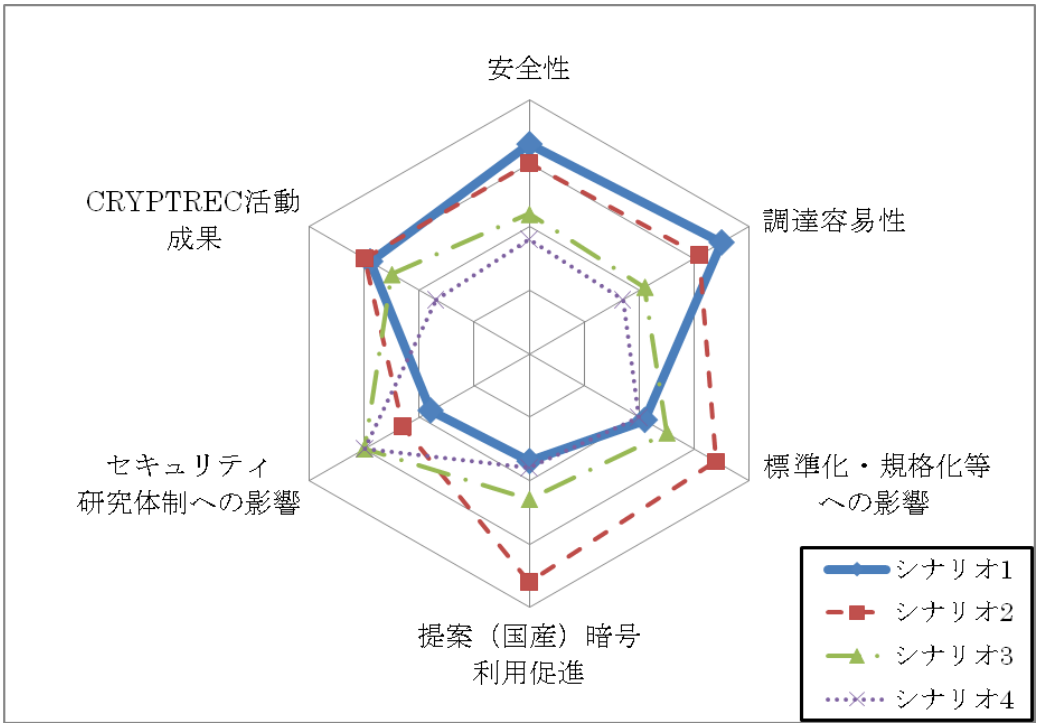
2.4.1 節で取りまとめたメリット・デメリットをもとに、以下の 4 段階を基準として、シナリオごとに各評価軸のメリット度合いを「評価点」として表現した。

なお、評価点は、2.4.1 節で取りまとめたメリット・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した。例えば、メリットの個数が少なくてもメリット効果が大きいと判断される場合、評価点は「3」ではなく「4」となる。一方、デメリットの個数が多くても全体としてそれほど大きなデメリット効果はないと判断される場合、評価点は「1」ではなく「2」となる。

＜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

各シナリオのメリット（効果）が大きいかどうかをイメージしやすくなるように、評価点によるレーダーチャートを以下に示す。一番外側が「4」で内側へ行くごとに「3」「2」「1」となる。



2.3 節で設定したシナリオにおいて、全体的にみると、シナリオ 2、シナリオ 1、シナリオ 3、シナリオ 4 の順にメリットが大きいと判断された。

他方、「セキュリティ研究体制への影響」の評価軸における評価点とそれ以外の評価軸における評価点との出方が反対になっていることが象徴的である。これは、日本における暗号研究体制と現実の暗号利用の実態との間で大きな乖離が生じている可能性があることを意味する。その結果、どのシナリオを取るにせよ、以下のような大きな問題が生じることが予想される。

なお、**上記の評価点は、それぞれのシナリオにおける以下の問題点が解消される、もしくは解消するための施策とセットで実施することが前提**となっていることに注意されたい。すなわち、以下の問題点が解消される施策がセットで行われない場合には、必ずしも上記の評価点が得られるとは限らない。

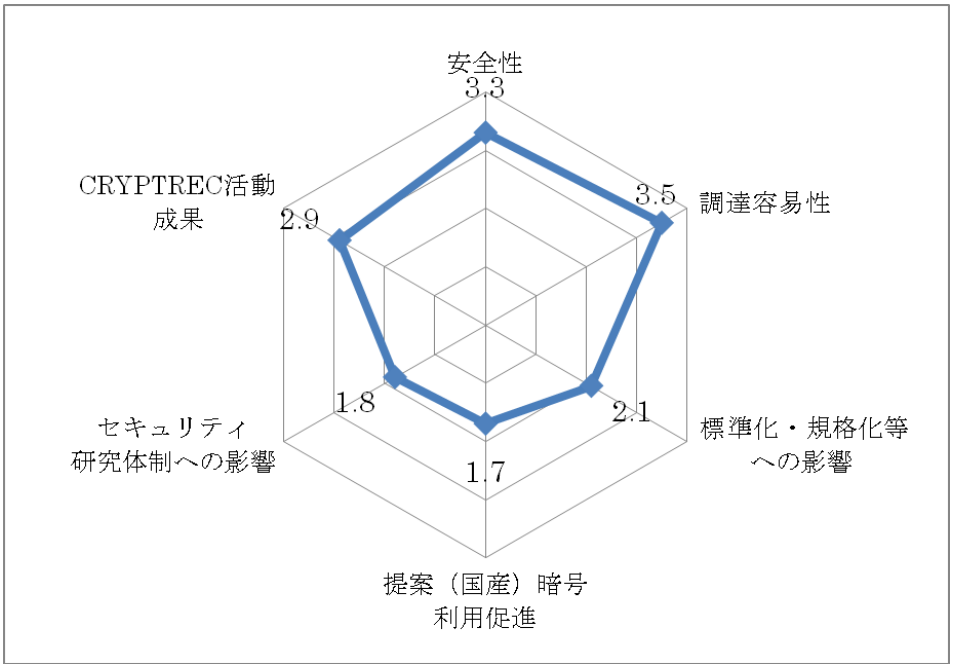
ｼﾅﾘｵ	問題点	問題点の解消法（案）
ｼﾅﾘｵ 1	① 民間企業が新たな暗号アルゴリズムを開発する必要性が低下し、民間企業で暗号研究者を抱えられなくなる ⇒ CRYPTREC における暗号評価・監視に民間企業の暗号研究者が大きな役割を果たしているため、民間企業の暗号研究者の減少は暗号評価・監視が出来なくなることを意味する	暗号研究者の公的機関における雇用が必要（公的機関での暗号評価・監視の可能性）
ｼﾅﾘｵ 2	① 民間企業が新たな暗号アルゴリズムを開発する必要性が低下し、民間企業で暗号研究者を抱えられなくなる ⇒ 応募企業間で優劣がつく可能性があり、シナリオ1よりも顕在化する時期が早い可能性あり ② 提案暗号の絞り込みが大変 ⇒ 従来のCRYPTRECのやり方から見ると大きな軌道修正になる ③ 絞り込んだとして本当に使われるのか疑問 ⇒ 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（公的機関での暗号評価・監視の可能性） ② 広く使われるように提案暗号を振興することが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 推奨暗号リストから外れた組織への対応 ②-3 ISO 等からとのリエゾン関係構築 ③ プロトコル等へ活動範囲を展開（注力先の変更）
ｼﾅﾘｵ 3	① 結局、現状と変わらない可能性が高い ⇒ いずれシナリオ1かシナリオ4になるのではないか？ ⇒ （応募企業以外も広く利用するような）提案暗号の振興が目的にないのであれば CRYPTREC を継続する産業政策的意義は少ない ② 現状のまま継続しても、提案暗号の利用機会が少ない現状から見て、いずれ民間企業で暗号研究者を抱えられなくなるのではないか ⇒ 気がついたときには暗号評価、監視をするための体制がない事態も想定される	（解消法（案）未検討）

ｼﾅﾘｵ 4	① 現状と変わらないと思われる ⇒ （応募企業以外も広く利用するような）提案暗号の振興が目的にないのであれば CRYPTREC を継続する産業政策的意義が説明できない ② 現状のまま継続しても、提案暗号の利用機会が少ない現状から見て、いずれ民間企業で暗号研究者を抱えられなくなるのではないか ⇒ 気がついたときには暗号評価、監視をするための体制がない事態も想定される	（解消法（案）未検討）

2.4.3 シナリオごとの個別評価結果

以下では、各シナリオについての個別の評価結果を述べる。主な特徴点は、2.4.1 節で取りまとめられたメリット・デメリットのうち、評価点を決める上で大きな要因となったメリット・デメリットを評価軸ごとに 2 ～6 個選定したものである。

【シナリオ 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）】



＜安全性＞

■ 全世界の安全性評価研究成果結果を享受することができるため、安全性評価結果に対する蓄積・信頼性が厚い。また、監視活動が効率化できることで、監視

コストが最も軽減できる

- 電子政府推奨暗号アルゴリズムは実際に広く使われる暗号なので、実装上のミスが少なく保守も容易になるため、むしろ安全性は高い
- 特定の電子政府推奨暗号アルゴリズムが広く利用されている可能性が高く、当該推奨暗号アルゴリズムが危殆化した場合の影響は広範囲に渡り、緊急対応すべき影響範囲は極めて大きい
- 電子政府推奨暗号アルゴリズムに対する危殆化に関する影響、対策に関する情報が国内外から得られ、的確で迅速な対応が可能となる

＜調達容易性＞

- 電子政府推奨暗号リストと製品調達上の利用可能暗号アルゴリズムとの親和性は極めて高い
- 提案暗号をバックアップに利用することは難しいが、米国の対応方針に沿って形成された市場からバックアップ製品を調達することができると考えられる
- あらゆるベンダの製品について電子政府推奨暗号アルゴリズムの多くに対応したモジュールが開発されるので、暗号アルゴリズムとしてのベンダごとの差異が少なくなり、ベンダロックインの要因になる恐れはない
- 日本独自の判断で、現時点で主流の暗号アルゴリズムから将来的に別のものに誘導しようとしても、実施は極めて困難

＜標準化・規格化等への影響＞

- 電子政府推奨暗号アルゴリズムは国際標準化・規格化済みと考えられ、ほとんど影響を与えることはない
- 提案暗号を国際標準化・規格化に提案する際、電子政府推奨暗号リストに含まれず推奨候補暗号リストに掲載されることになるので、普及度の低いものとして不利な解釈を受ける可能性がある
- 提案会社の国際標準化・規格化活動への支援材料にはならない可能性が高いため、応募会社のモチベーションを上げることは難しい

＜提案暗号（国産暗号）の利用促進＞

- 全世界特許無償化しても、提案暗号が電子政府推奨暗号リストに入らなければサポートするメリットが見出せず、採用拡大は期待できないため、（米国政府標準暗号によって）寡占されたままになる
- 提案暗号が電子政府推奨暗号アルゴリズムに選ばれる可能性は高くなく、支援対象が政策的に支援したい対象とマッチするとは限らない

＜セキュリティ研究体制への影響＞

- 新しい暗号アルゴリズムを開発しても市場で受け入れられる可能性は低い。電

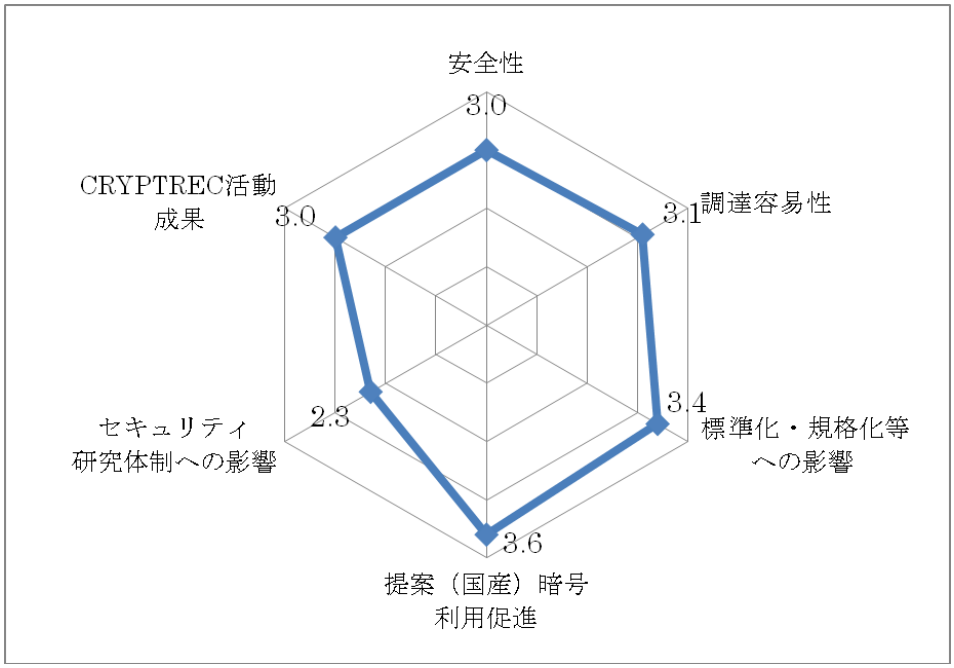
子政府推奨暗号リスト入りするのは困難であり、推奨候補暗号リストでは普及が見込めないのでモチベーションが低下する

- 現在主流の暗号アルゴリズムの寿命が十分あると見込まれる間は独自暗号開発不要論が強まる可能性があり、特に企業における暗号研究体制の縮小が余儀なくされる恐れがある
- 欧米のように、現在の暗号アルゴリズム主体の研究体制からセキュリティ応用研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを促す効果が期待できる

＜CRYPTREC 活動成果＞

- 電子政府推奨暗号リストと推奨候補暗号リストで差異化が図られるので、リストの役割が明確化され、参照しやすくなる
- 電子政府推奨暗号リストに活動を注力でき、コストパフォーマンスが良い
- 提案暗号が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できる可能性はほとんどない
- 結果的に米国政府の動きを追随する形になり、日本独自の施策がほとんど含まれていないため、事実上、CRYPTREC の活動の必要性低下が懸念される

【シナリオ 2(様々な標準化・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＞

- 電子政府推奨暗号アルゴリズムの個数を限定するため、当該推奨暗号アルゴリズムに対する注目度が国内外で高まることが期待でき、安全性評価や監視活動

を効率的に実施することができる。監視コストも軽減される

- 電子政府推奨暗号アルゴリズムは実際に広く使われる暗号なので、実装上のミスが少なく保守も容易になるため、むしろ安全性は高い
- 特定の電子政府推奨暗号アルゴリズムが広く利用されている可能性が高く、当該推奨暗号アルゴリズムが危殆化した場合の影響は広範囲に渡り、緊急対応すべき影響範囲は極めて大きい
- 電子政府推奨暗号アルゴリズムの個数を限定するため事前に相互接続等の必要な準備を整えておくことが可能であるので、危殆化時のバックアップとして迅速に供することができ、危殆化の影響を低減できると期待される

＜調達容易性＞

- 限定された電子政府推奨暗号アルゴリズムとしての提案暗号の位置づけが明確になり、利用の期待が高まる、あるいは調達基準として明確になれば、当該提案暗号の製品化が促進され、調達コストに与える影響が最低限に抑えられる
- 電子政府推奨暗号アルゴリズムの個数を限定するので当該推奨暗号アルゴリズムを搭載した製品が存在していると期待することができ、バックアップとして調達することが容易であると考えられる
- 電子政府推奨暗号アルゴリズムとしての提案暗号の位置づけが明確になれば、多くの企業の製品に当該提案暗号が搭載されることが期待できるので、ベンダロックインの要因になる恐れは少ない
- ある程度の製品数が整うまでの期間、危殆化対策済み（バックアップ搭載）製品を調達しようとすると、調達先が限定、もしくはコスト高につながる恐れがある
- 提案暗号の普及展開を重視すると利用実績だけでは判断できず、他の指標が必要。調達における基準の平等性の担保が確保できない可能性がある

＜標準化・規格化等への影響＞

- 電子政府推奨暗号リストが提案暗号の国際標準化・規格化促進手段として活用されれば国内外での注目が集まり、国際標準化（ISO/IEC や ITU）・規格（例えば IETF や IEEE）策定が促進される可能性がある
- 公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる
- 電子政府推奨暗号アルゴリズムに選ばれた応募会社にとっては国際標準化や様々な規格化への支援材料になることが期待できるため、国際標準化や規格化活動へのモチベーションが上がる
- 電子政府推奨暗号アルゴリズムに選ばれなかった応募会社にとっては国際標準化や様々な規格化活動へのモチベーション向上につながらない

＜提案暗号（国産暗号）の利用促進＞

- 提案暗号が電子政府推奨暗号リストに含まれ製品化促進手段として活用されることで、促進策の内容がそのまま提案暗号をサポートすることに対するモチベーションにつながり、当該提案暗号の利用促進が期待できる
- 電子政府推奨暗号アルゴリズムの個数が限定されるため、政策的な支援の意図が明確になる上一つあたりの利用促進のためにかけられるコストが大きくなるので、当該提案暗号に対して効果的な支援が可能
- 電子政府推奨暗号リストに選ばれた提案暗号について特許無償化と国際標準化・規格化の促進により、他社（応募会社や他のシステム開発会社等）からの製品化・サポートも受けやすくなるため、当該提案暗号の利用が促進される可能性がある
- ベンダロックインを回避するためには全世界特許無償化をしていない提案暗号を利用促進活動の対象とすることはできない

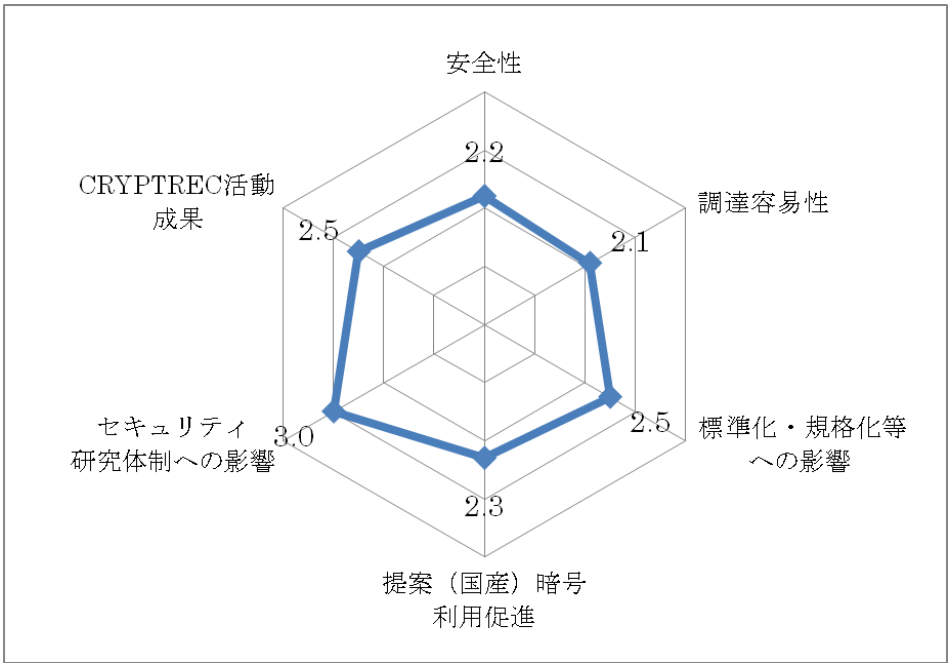
＜セキュリティ研究体制への影響＞

- 電子政府推奨暗号アルゴリズムの個数を限定するため、新しい暗号アルゴリズムを開発しても電子政府推奨暗号リスト入りするのは困難であり、推奨候補暗号リストでは普及が見込めないのでモチベーションが低下する
- 電子政府推奨暗号アルゴリズムの個数を限定するため、独自暗号開発不要論が強まる可能性があり、企業としての暗号研究体制の縮小の可能性がある
- 国産暗号として有望な暗号アルゴリズムが開発された場合には、応募会社の枠を超え官学民からのバックアップが期待される
- 欧米のように、現在の暗号アルゴリズム主体の研究体制からセキュリティ応用研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを促す効果が期待できる

＜CRYPTREC 活動成果＞

- 電子政府推奨暗号リスト選定には提案暗号の普及展開の要素が必要であり、その判断・運用を行う組織として、CRYPTREC 活動の必要性を主張できる
- 電子政府推奨暗号リストに活動を注力でき、コストパフォーマンスが良い
- 電子政府推奨暗号リストと推奨候補暗号リストで差異化が図られるので、推奨する提案暗号を明確にするという意味から極めて明確
- 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「その他」の要素が明確にならない限り、リストの位置づけは不明確
- 電子政府推奨リストに選ばれた提案暗号のプロモーションのためのコストが発生する

【シナリオ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）】



＜安全性＞

- 代替暗号アルゴリズムの選択肢がある程度選択肢として用意されており、危殆化対策としてある程度の実現可能性はある
- 学会等での注目度の低い暗号アルゴリズムでは安全性評価の蓄積が少なく、普及度判定時に安全性の再評価が必要となる可能性がある。また暗号アルゴリズムごとに評価を行う暗号研究者が固定化されやすく、全体の安全性評価の充実度につながらない
- 電子政府推奨暗号アルゴリズムの数は多いが、実際に利用される暗号は限定されるため、結果として実装・保守における安全性はシナリオ 1, 2 と同程度になると考えられる
- 電子政府推奨暗号アルゴリズムの数で考えればシナリオ 1, 2 よりもいずれかの電子政府推奨暗号アルゴリズムが危殆化する可能性は高い。広く利用されていない電子政府推奨暗号アルゴリズムが危殆化した場合、経済的な影響は限定的となる可能性があるが、「CRYPTREC がお墨付きを与えていた暗号（電子政府推奨暗号）が危殆化した」という点で CRYPTREC の信用が低下する可能性がある

＜調達容易性＞

- 意図してバックアップのアルゴリズムを用意する場合、選択肢が豊富
- サポートすべき電子政府推奨暗号アルゴリズムが明らかではなく、製品化を行う際の指針とはならないため、応募会社以外の暗号アルゴリズムの利用はすでにシェアを握った一部に限られる。そのほかの暗号アルゴリズムの製品化は進

まず、調達先は依然限定され調達コストは高くなる

- 特定製品にしか搭載されていない電子政府推奨暗号アルゴリズムが採用されると将来にわたってベンダロックインが発生する恐れがある
- 採用した電子政府推奨暗号アルゴリズムが利用実績不足を理由に推奨候補暗号リストへ降格する恐れがある

＜標準化・規格化等への影響＞

- 電子政府推奨暗号アルゴリズムに選ばれた応募会社にとっては国際標準化への支援材料になると期待できるため、これらの国際標準化活動へのモチベーションはある
- 公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる
- 複数の提案暗号が電子政府推奨リストに残る場合には、日本としてどの暗号アルゴリズムを必要としているのがはっきりしない、また普及状況により電子政府推奨暗号リストから外される可能性もあるため、日本からの国際標準化・規格化への提案が軽視もしくは無視される可能性が高い
- 提案会社は自らが興味を持つ国際標準化・規格化しか推進しない可能性がある
- 国際標準化や規格化（入り・選定中）を理由に、電子政府での利用実態がないにもかかわらず推奨リストに残り続けることがないか

＜提案暗号（国産暗号）の利用促進＞

- 純粋な自由競争であり、利用実績に応じて降格の可能性があるため、応募会社の利用促進活動に対するモチベーションを向上させる可能性がある
- 他社実績をつませないため、少なくとも自社の提案暗号が推奨候補暗号リストに降格しない限り、他社暗号アルゴリズムを利用しないモチベーションとなる。応募会社による囲い込み意識が働く
- 全世界特許無償は様々な国際標準化・規格化への採用活動をしていない応募会社のビジネスモデルと壊す恐れが高い
- 全世界特許無償化しても、様々な国際標準化・規格化に採用されていない提案暗号は（応募会社以外にとって）事実上サポートする対象になりえない
- 推奨候補暗号リストへの降格の恐れがある提案暗号の場合、応募会社以外の企業・団体がサポートする対象にはなりにくい
- 電子政府推奨暗号アルゴリズムの個数が多くなるほど、一つあたりの利用促進のためにかけられるコストが小さくなるため、効果的な支援は困難

＜セキュリティ研究体制への影響＞

- 電子政府推奨暗号リストが新しい暗号アルゴリズムを開発した場合の一つの到

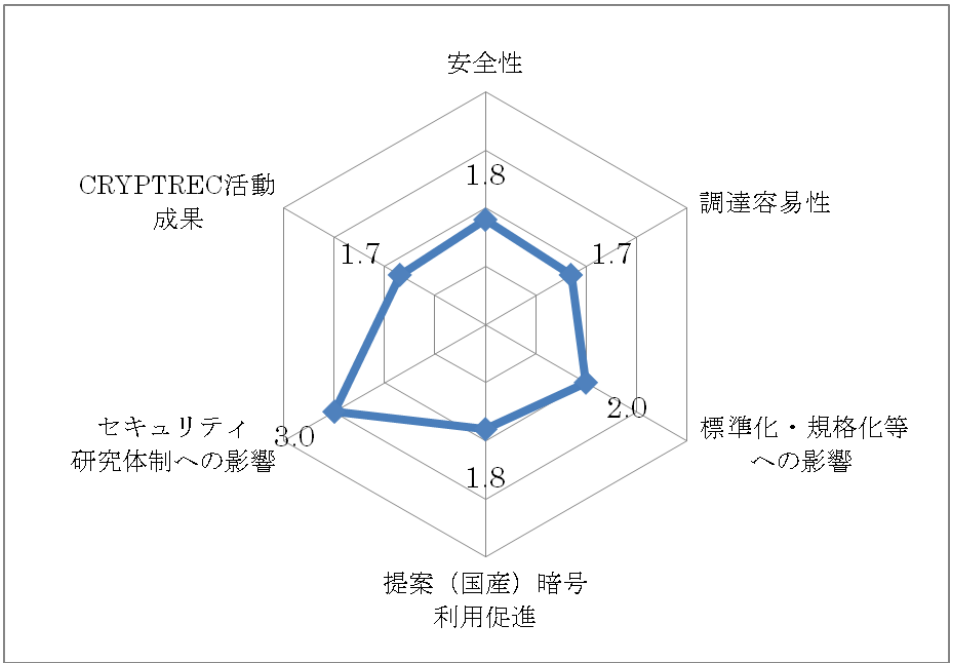
達点としてのモチベーションにつながり、新しい暗号アルゴリズムの開発が継続できる可能性が高まる

- 安全性評価対象が多いため、新しい安全性評価技術や検証の豊富な研究素材となり、暗号研究の強化につながる
- 普及度（だけ）が技術評価の指標としてクローズアップされる可能性があり、推奨候補暗号リストへ降格した提案暗号の応募会社では研究体制維持を難しくする可能性がある
- 応募会社内だけで自社開発暗号アルゴリズムを利用することが事実上の前提であるならば、経営判断の影響を受けやすい構造にある

＜CRYPTREC 活動成果＞

- 推奨候補暗号リストへの降格においてはその判断・運用を行う組織が必要であり、推奨候補暗号リストへの降格を行った後の電子政府推奨暗号リストを活かせるのであれば CRYPTREC 活動の必要性を主張できる
- 利用実績による降格は明確な基準が困難であり、電子政府推奨暗号リストと推奨候補暗号リストとの差異、位置づけは不明確
- 単に市場での普及に任せていても、現在の米国暗号有利の状況が変わるわけではなく、分割の意味ある効果は期待できない
- 危殆化以外の理由（利用実績等）による降格は暗号開発ベンダ、および市場に受け入れられない可能性がある
- 推奨候補暗号リストへの「降格の基準」に応じて、シナリオ 3 は、シナリオ 1, 2, 4 のいずれにもなりうる。シナリオ 3 を選択する場合には、推奨候補暗号リストへの降格後に電子政府推奨暗号リストがどうなるかをイメージできる程度に基準について議論しておくことが望ましい

【シナリオ 4（政府調達の選択肢としての提示。現状とほぼ同様）】



＜安全性＞

- 電子政府推奨暗号リストに代替暗号アルゴリズムが選択肢として用意されている
- 暗号アルゴリズムごとの安全性評価の度合に差が生じ、統一的な運用基準が適用できない。また暗号アルゴリズムごとに評価を行う暗号研究者が固定化されやすく、全体の安全性評価の充実度につながらない
- 電子政府推奨暗号アルゴリズムの個数が多いため、特定の暗号アルゴリズムに特化した安全性評価や監視活動を定常的に実施することは困難であり、全体的な評価効率も悪く監視コストがかさむ
- 電子政府推奨暗号アルゴリズムの数は多いが、実際に利用される暗号は限定されるため、結果として実装・保守における安全性はシナリオ 1, 2 と同程度になると考えられる
- 電子政府推奨暗号アルゴリズムの数で考えればシナリオ 1, 2 よりもいずれかの電子政府推奨暗号アルゴリズムが危殆化する可能性は高い。広く利用されていない電子政府推奨暗号アルゴリズムが危殆化した場合、経済的な影響は限定的となる可能性があるが、「CRYPTREC がお墨付きを与えていた暗号（電子政府推奨暗号）が危殆化した」という点で CRYPTREC の信用が低下する可能性がある

＜調達容易性＞

- 意図してバックアップのアルゴリズムを用意する場合、選択肢が豊富
- 製品調達が極めて容易なものからそうでないものまで同格に扱われ、実際の暗

号アルゴリズム選択との相関性は薄い

■応募会社以外の暗号アルゴリズムの利用はすでにシェアを握った一部に限られ、利用度が低い電子政府推奨暗号アルゴリズムが様々な企業で製品化される可能性は低く、調達先は限定され調達コストは高くなる

■ 特定製品にしか搭載されていない電子政府推奨暗号アルゴリズムが採用されると将来にわたってベンダロックインが発生する恐れがある

＜標準化・規格化等への影響＞

■ 電子政府推奨暗号アルゴリズムに選ばれた応募会社にとっては国際標準化への支援材料になると期待できるため、これらの国際標準化活動へのモチベーションはある

■ 公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる

■ 多数の暗号アルゴリズムの標準化提案は本来の標準化の意義に沿わない。日本としてどの暗号アルゴリズムを必要としているのかはっきりしないため、日本からの国際標準化・規格化への提案は拒絶または無視、軽視される可能性が高い

■ 応募会社は自らが興味を持つ標準化・規格化しか推進しない可能性がある

＜提案暗号（国産暗号）の利用促進＞

■ 純粋な自由競争であり、応募会社が自社のビジネス範囲内に囲い込んで利用することに対してはモチベーションがあると考えられる

■ 自社の提案暗号が電子政府推奨暗号アルゴリズムとなっている状況で、他社の提案暗号をサポートするという状況は想定し難い

■ 全世界特許無償化しても、様々な国際標準化・規格化に採用されていない提案暗号は（応募会社以外にとって）事実上サポートする対象になりえない

■ 全世界特許無償は様々な国際標準化・規格化への採用活動をしていない応募会社のビジネスモデルと壊す恐れが高い

■ 電子政府推奨暗号アルゴリズムの個数が多いため、一つあたりの利用促進のためにかけられるコストが小さく、平等公平に効果的な支援は困難

＜セキュリティ研究体制への影響＞

■ 電子政府推奨暗号リストが新しい暗号アルゴリズムを開発した場合の一つの到達点としてのモチベーションにつながり、新しい暗号アルゴリズムの開発が継続できる可能性が高まる

■ 安全性評価対象が多いため、新しい安全性評価技術や検証の豊富な研究素材となり、暗号研究の強化につながる

- 応募会社内だけで自社開発暗号アルゴリズムを利用することが事実上前提であるため、経営判断の影響を受けやすい構造にある
- 欧米とは違い、暗号アルゴリズム主体の研究体制からセキュリティ応用研究主体の研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを妨げる恐れがある

＜CRYPTREC 活動成果＞

- 電子政府推奨暗号リストと推奨候補暗号リストとの差異、位置づけの違いは極めて不明確
- 推奨候補暗号リストに含まれる暗号アルゴリズムはほとんどないと考えられ、別リストである利点がない
- 電子政府推奨暗号アルゴリズムとなっていても調達が難しい暗号が存在する可能性があり、その場合、電子政府推奨暗号リストの価値が低下し、CRYPTREC の成果も分かりにくくなる

第 3 章　暗号アルゴリズムの利用実態に関する外部アンケート調査

3.1　外部アンケート調査の概要

3.1.1　調査目的

現在の電子政府推奨暗号リストは技術的観点のみから作成されたものである。しかし、実際の電子政府情報システムの構築及び暗号搭載製品の製造の現場においては、必ずしも技術的観点だけで暗号アルゴリズムの選択が行われているわけではない。

そこで、現在の電子政府推奨暗号リストの課題点を抽出し、CRYPTREC 暗号リスト（仮称）をどのような考え方のもとで作成することがよいのかについての情報を得ることを目的として、国内外の主要ベンダを主な対象に実施した。

具体的には、以下の項目についての情報を主に把握することを目的とする。

- 暗号搭載製品の開発や製造、情報システムの構築等における暗号利用（とりわけ暗号アルゴリズムの選択プロセス）に関する実態を把握すること
- 現在の「電子政府推奨暗号リスト」の活用実態を把握すること
- 「CRYPTREC 暗号リスト（仮称）」や CRYPTREC に期待すること
- 暗号搭載製品の開発や製造、情報システムの構築等における提案暗号（国産暗号）に対する認識を広く把握すること

本アンケート調査で特に重視する点は、今まで CRYPTREC とは直接的な接点があまりないが実際の暗号搭載製品の市場供給力が非常に大きい国内外の主要ベンダ、ならびに CRYPTREC が実施している前回公募(2001 年)または今回公募（2009 年）に応募した暗号技術（以下、「提案暗号」という）を開発している企業（以下、「応募会社」という）の事業部門及びその関連会社の事業部門（以下、両事業部門を合わせて「応募ベンダ」という）が暗号アルゴリズムの利用実態をどのように認識しているのかを把握することである。

なお、本調査結果は、2.4 節の比較評価を行う際の特徴的なメリット・デメリットの抽出や評価点を検討するうえでの基礎情報として取り扱った。

3.1.2　調査手法

本アンケート調査では、暗号アルゴリズムの利用実態を正しく把握することに留意し、

以下の担当部門を主な対象としてアンケート調査を実施した。なお、アンケートの回答方法は選択方式とし、設問により単一回答もしくは複数回答とした。

- 政府機関：
  総務省・経済産業省等が依頼した各府省庁の調達担当部門
  （政府機関向けのアンケート調査の主な項目）
  - ■ 現在の電子政府推奨暗号リストを政府調達の際にどのように活用しているか
  - ■ 暗号に対する調達コストの考え方
  - ■ 提案暗号（国産暗号）に対する政府調達時の考え方
  - ■ 次期 CRYPTREC 暗号リスト（仮称）が 3 部構成になることによる効果
  - ■ 調達した暗号の電子政府推奨暗号の位置づけが変わった時の対応

- システムインテグレータ：
  電子政府システムへの納入実績が多数あるシステムインテグレータの法人営業本部（公共担当）またはそれに類する部門、もしくはシステムインテグレーション開発を担当する開発部・技術本部
  （システムインテグレータ向けのアンケート調査の主な項目）
  - ■ 現在の電子政府推奨暗号リストを政府調達の際にどのように活用しているか
  - ■ 暗号アルゴリズムの実現コストに対する考え方
  - ■ 提案暗号（国産暗号）に対する考え方
  - ■ 次期 CRYPTREC 暗号リスト（仮称）が 3 部構成になることによる効果
  - ■ 調達した暗号の電子政府推奨暗号の位置づけが変わった時の対応

- 暗号搭載製品製造ベンダ（サービス提供ベンダを含む）：
  運用委員会で選定したカテゴリの各々シェアトップ級ベンダの法人営業本部（公共担当）またはそれに類する部門、もしくは当該ベンダの主力製品（主力サービス）の開発計画・技術支援を担当する開発部・技術本部
  （ベンダ向けのアンケート調査の主な項目）
  - ■ 暗号アルゴリズムの実装方法
  - ■ 暗号アルゴリズムの実現コストに対する考え方
  - ■ 現在の電子政府推奨暗号リストと調達可能製品開発計画との関連性
  - ■ 提案暗号（国産暗号）に対する考え方
  - ■ 次期 CRYPTREC 暗号リスト（仮称）が 3 部構成になることによる効果
  - ■ 搭載している暗号に安全性に問題が生じた時の対応

  ＜対象カテゴリ＞
  - ➢ オペレーションシステム

- ブラウザ
- アプリケーションソフトウェア（ブラウザを除く）
- 暗号ライブラリ（暗号アルゴリズムを集めたソフトウェア）
- ルータ
- セキュリティアプライアンス製品
- サーバ／ストレージ
- HSM／PKI システム／認証局システム
- IC カード
- 半導体チップ
- デジタル複合機
- 輸入販売代理による輸入製品
- 固定網／NGN 通信事業者
- 携帯電話通信事業者
- サービスプロバイダ
- タイムスタンプビジネス

- 応募者：
  応募会社の暗号研究開発部門
  （応募者向けのアンケート調査の主な項目）
  - ■ 提案暗号の必要性に対する考え方
  - ■ 提案暗号の国際標準化・規格化に対する考え方
  - ■ 提案暗号の知的財産権に対する考え方
  - ■ 提案暗号の普及状況・利用実績に対する考え方
  - ■ 現在の電子政府推奨暗号リストの活用状況
  - ■ 次期 CRYPTREC 暗号リスト（仮称）が 3 部構成になることによる効果
  - ■ 外部環境変化による研究開発体制への影響

3.2 外部アンケート調査結果の概要

最終的に、ベンダ全 39 社（67 プロダクト）、システムインテグレータ全 8 社（11 システム）、政府機関全 4 府省（6 システム）、全応募者から回答を得ることができた。ベンダ及びシステムインテグレータで本アンケート調査に協力いただいた企業は以下のとおりである（順不同、公表不可を除く）。

● ベンダ

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

他、全 39 社・67 プロダクト

● システムインテグレータ

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

他、全 8 社・11 システム

本調査結果の概要は以下のとおりであり、その根拠データを付録 2 にまとめる。

なお、本アンケート調査全体にわたる詳細な取りまとめ結果については、総務省及び経済産業省に別途報告されており、今後政府部内で暗号政策を議論する際の客観的資料として用いられる。

● 「ベンダ」からみる全体的な傾向
  - （米国政府標準暗号以外の）暗号をサポートするかどうかは「お客様がいるか」「市場としての広がりがあるか」「様々な標準になっていて国際的知名度があるか」「特許無償で利用可能であるか」が大きなポイント

- 暗号アルゴリズム実装では「30%超のベンダ」が他社製品や OSS を利用
- 50%以上のベンダはサポートする暗号アルゴリズムの数が「必要最少限」もしくは「少ないほどよい」と考えている
- 80%以上のベンダが（CRYPTREC 以外の）標準規格等を製品開発の中で利用。相互接続性の観点から ISO/IEC だけでなく、ITU, IETF, IEEE なども多く参照
- 現在の国産暗号の製品化率は約 20～30%。今後国産暗号をサポートするかどうかは条件次第が約 40～50%で一番多い
- （日本以外の）各国政府等からの要求に対応して当該国の政府標準暗号を別途追加したケースが 10～20%はある
- 50%以上は 3 部構成の次期リストに対して好意的。特に「監視リスト」の受けが良い

- 「応募ベンダ」と「非応募ベンダ」との認識の違い
  - 「応募ベンダ」と「非応募ベンダ」とでは、一部の設問や回答に違いがみられるものの、全体的な傾向としては両者に大きな差があるわけではない
  - 「応募ベンダ」と「非応募ベンダ」とで回答に違いがあったものの一つに国産暗号の採用理由がある。
    - 非応募ベンダの採用理由では、「お客様要望」「様々な標準に採用され国際的知名度が高い」「特許無償で利用可」などが多い
    - 応募ベンダの採用理由では、「他社との差異化提案」「自社開発暗号である」「処理性能が良い」などが多い

- 「ベンダ（システムインテグレータ）」と「政府機関」との認識の違い
  - 推奨暗号の数を絞るか絞るべきではないかに対する考えが大きく異なる。
    - ベンダの多数意見は「使う暗号は決まっている」「絞るほどむしろ安全性が高まる」「コストが抑えられる」「相互接続に問題ない」など“数を絞る”
    - 政府機関の多数意見は「選択自由度が高まる」「絞ると影響が大きい」「絞るほど攻撃されやすい」など“数を絞らない

- 「応募者」の主な現状認識
  - 80%以上が「自社事業部や子会社での利用を約束」したうえでの開発目的に掲げる一方、現在の自社事業部や子会社での利用進捗率は 40～50%程度。ちなみに応募ベンダからの回答では国産暗号製品化実績率は約 30%
  - 70%以上が「社会基盤としての利用」「米国政府標準暗号だけに頼るべきでない」と開発目的に掲げる一方、社会基盤のために必要な標準化を実際に進めているは半数にとどまる。しかもその対象は提案中を含めても ISO/IEC だけが約 40%、そのほかの IETF などメジャーな標準化・規格化は 10%にも届かない

- 標準化を進める目的が「お墨付きを得るため」であり、「相互接続確保のため」は半数にとどまる

付録

付録１　「電子政府推奨暗号リストの考え方」に対するメリット・デメリットのとりまとめ

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
A)「安全性」				
	【メリット】　推奨暗号アルゴリズムが学会等でも注目度の高いものに限定されるため、暗号アルゴリズム間で安全性評価基準が平準化され、安全性評価のばらつきが少なくなる	【メリット】　推奨暗号アルゴリズムの個数を限定するため、暗号アルゴリズム間で安全性評価基準が平準化されやすくなり、安全性評価のばらつきが少なくなることが期待できる	【デメリット】　学会等では注目度の低い暗号アルゴリズムも推奨暗号リストに含まれる可能性があり、安全性評価に大きなばらつきが生じる可能性がある	【デメリット】　学会等では注目度の低い暗号アルゴリズムも推奨暗号リストに含まれるため、安全性評価に大きなばらつきが生じる
	【メリット】　全世界の安全性評価研究成果結果を享受することができるため、安全性評価結果に対する蓄積・信頼性が厚い。また、監視活動が効率化できることで、監視コストが最も軽減できる	【メリット】　推奨暗号アルゴリズムの個数を限定するため、当該暗号アルゴリズムに対する注目度が国内外で高まることが期待でき、安全性評価や監視活動を効率的に実施することができる。監視コストも軽減される	【デメリット】　推奨暗号アルゴリズムの個数が多いため、特定の暗号アルゴリズムに特化した安全性評価や監視活動を定常的に実施することは困難であり、全体的な評価効率も悪く監視コストがかさむ	【デメリット】　推奨暗号アルゴリズムの個数が多いため、特定の暗号アルゴリズムに特化した安全性評価や監視活動を定常的に実施することは困難であり、全体的な評価効率も悪く監視コストがかさむ
			【メリット】　候補リストへの降格が予想される暗号アルゴリズムの重みを軽くするなどして監視活動リソースの選択的投入が可能	
	【メリット】　推奨暗号アルゴリズムは実際に広く使われる暗号なので、実装上のミスが少なく保守も容易になるため、むしろ安全性は高い	【メリット】　推奨暗号アルゴリズムは実際に広く使われる暗号なので、実装上のミスが少なく保守も容易になるため、むしろ安全性は高い	【デメリット】　学会等での注目度の低い暗号アルゴリズムでは安全性評価の蓄積が少なく、普及度判定時に安全性の再評価が必要となる可能性がある。また暗号アルゴリズムごとに評価を行う暗号研究者が固定化されやすく、全体の安全性評価の充実度につながらない	【デメリット】　暗号アルゴリズムごとの安全性評価の度合に差が生じ、統一的な運用基準が適用できない。また暗号アルゴリズムごとに評価を行う暗号研究者が固定化されやすく、全体の安全性評価の充実度につながらない
	【メリット】　推奨暗号アルゴリズムの安全性評価結果は外部からも入手できるので、分析能力さえあれば一定の監視活動は実施可能			
		【メリット】　提案暗号利用推進は、国内における安全性評価・監視活動強化の良いモチベーションとなり、安全性評価能力の向上につながる可能性がある		
			【メリット】　新規アルゴリズムの提案が促進されるならば、企業・大学における暗号研究人員の強化につながる	【メリット】　企業における暗号研究体制は現状維持と考えられ、世界最高水準の安全性評価能力が維持される
	【デメリット】　外部から十分な安全性評価が得られるため、国内での監視活動に対する評価が低下する可能性がある。監視活動継続リソースが「仕分け」されることで、安全性評価能力の低下や監視活動ができる人材の層が薄くなる恐れがある	【デメリット】　企業の新しい暗号研究への新規投資が抑制され、暗号研究体制の縮小が余儀なくされる可能性があり、安全性評価能力の低下や監視活動ができる人材の層が薄くなる恐れがある	【デメリット】　企業の新しい暗号研究への新規投資が抑制され、または推奨リスト残留（普及度）が研究の主要の評価指針となることにより、暗号研究体制の縮小が余儀なくされる可能性がある。安全性評価能力の低下や監視活動ができる人材の層が薄くなる恐れがある	【デメリット】　企業の新しい暗号研究への新規投資が抑制され、暗号研究体制の縮小が余儀なくされる可能性があり、安全性評価能力の低下や監視活動ができる人材の層が薄くなる恐れがある

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
	【デメリット】 特定の推奨暗号アルゴリズムが広く利用されている可能性が高く、その推奨暗号が危殆化した場合の影響は広範囲に渡り、緊急対応すべき影響範囲は極めて大きい	【デメリット】 特定の推奨暗号アルゴリズムが広く利用されている可能性が高く、その推奨暗号が危殆化した場合の影響は広範囲に渡り、緊急対応すべき影響範囲は極めて大きい	【デメリット】 推奨暗号アルゴリズムの数で考えればシナリオ 1, 2 よりもいずれかの推奨暗号アルゴリズムが危殆化する可能性は高い。 広く利用されていない推奨暗号アルゴリズムが危殆化した場合、経済的な影響は限定的となる可能性があるが、「CRYPTREC がお墨付きを与えていた暗号（推奨暗号）が危殆化した」という点で CRYPTREC の信用が低下する可能性がある	【デメリット】 推奨暗号アルゴリズムの数で考えればシナリオ 1, 2 よりもいずれかの推奨暗号アルゴリズムが危殆化する可能性は高い。 広く利用されていない推奨暗号アルゴリズムが危殆化した場合、経済的な影響は限定的となる可能性があるが、「CRYPTREC がお墨付きを与えていた暗号（推奨暗号）が危殆化した」という点で CRYPTREC の信用が低下する可能性がある
	【メリット】 国内外から危殆化に関する影響、対策に関する情報が得られ、的確で迅速な対応が可能となる	【メリット】 推奨暗号アルゴリズムの個数を限定するため事前に相互接続等の必要な準備を整えておくことが可能であるので、危殆化時のバックアップとして迅速に供することができ、危殆化の影響を低減できると期待される	【メリット】 代替暗号アルゴリズムの選択肢がある程度選択肢として用意されており、危殆化対策としてある程度の実現可能性はある	【メリット】 推奨リストに代替暗号アルゴリズムが選択肢として用意されている
			【デメリット】 普及度の低い暗号は相互接続性の観点から危殆化対策とはなりえないが、その存在により有力な推奨暗号アルゴリズムの製品化を阻害して危殆化時の迅速な対応を妨げる可能性がある	【デメリット】 普及度の低い暗号は相互接続性の観点から危殆化対策とはなりえないが、その存在により有力な推奨暗号アルゴリズムの製品化を阻害して危殆化時の迅速な対応を妨げる可能性がある
		【メリット】 代替暗号アルゴリズムが組み込まれる可能性が高まると期待され、その場合日本政府の独自判断で危殆化対策を実施することが可能	【メリット】 代替暗号アルゴリズムが組み込まれていれば、日本政府の独自判断で危殆化対策を実施することが可能	【メリット】 代替暗号アルゴリズムが組み込まれていれば、日本政府の独自判断で危殆化対策を実施することが可能
	【デメリット】 代替暗号アルゴリズムが用意されていない状況になる可能性が高く、日本政府の独自判断で危殆化対策を実施することは事実上困難	【デメリット】 推奨暗号アルゴリズムの個数を限定するため、バックアップとして利用可能な地域は限定され、日本政府の独自判断で危殆化対策を実施することは困難	【留意点】 推奨暗号アルゴリズムの数は多いが、実際に利用される暗号は限定されるため、結果として実装・保守における安全性はシナリオ 1, 2 と同程度になると考えられる	【留意点】 推奨暗号アルゴリズムの数は多いが、実際に利用される暗号は限定されるため、結果として実装・保守における安全性はシナリオ 1, 2 と同程度になると考えられる
	【留意点】 候補リストについては、その後の安全性評価はあまり行われないか、評価活動自体が期待されない。コストを抑え監視活動の実施能力を向上させるためには、CRYPTREC 暗号リスト全体の暗号アルゴリズムの数も考慮する必要がある	【留意点】 候補リストについては、その後の安全性評価はあまり行われないか、評価活動自体が期待されない。コストを抑え監視活動の実施能力を向上させるためには、CRYPTREC 暗号リスト全体の暗号アルゴリズムの数も考慮する必要がある	【留意点】 候補リストについては、その後の安全性評価はあまり行われないか、評価活動自体が期待されない。コストを抑え監視活動の実施能力を向上させるためには、CRYPTREC 暗号リスト全体の暗号アルゴリズムの数も考慮する必要がある	【留意点】 候補リストについては、その後の安全性評価はあまり行われないか、評価活動自体が期待されない。コストを抑え監視活動の実施能力を向上させるためには、CRYPTREC 暗号リスト全体の暗号アルゴリズムの数も考慮する必要がある
			【留意点】 上記のデメリットは、いくつかのアルゴリズムが候補リストに降格されることで緩和される可能性がある	

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
B)「調達容易性」				
	【メリット】　推奨リストと製品調達上の利用可能暗号アルゴリズムとの親和性は極めて高い	【メリット】　サポートすべき推奨暗号アルゴリズムが限定されることで様々な企業で製品化が促進され、推奨リストと製品調達上の利用可能暗号アルゴリズムとの相関度が高まる可能性は十分ある	【デメリット】　利用実績を考慮する前に推奨暗号アルゴリズムが選定されており、推奨リストと製品調達上の利用可能暗号アルゴリズムとの親和性はやや低い	【デメリット】　製品調達が極めて容易なものからそうでないものまで同格に扱われ、実際の暗号アルゴリズム選択との相関性は薄い
	【メリット】　推奨暗号アルゴリズムがごく少数に限られるならば、実質的にすべてを実装する場合が多い	【メリット】　限定された推奨暗号アルゴリズムとしての提案暗号の位置づけが明確になり、利用の期待が高まる、あるいは調達基準として明確になれば、当該提案暗号の製品化が促進され、調達コストに与える影響が最低限に抑えられる	【留意点】　いくつかのアルゴリズムが候補リストに降格されることで相関が高まると期待される。例えば、普及が十分進んでいるアルゴリズムが推奨暗号アルゴリズムに選定されるのでベンダロックインの危険性は低減、利用実績を調達時に考慮したい場合には分かりやすい指標化など	
	【メリット】　提案暗号をバックアップに利用することは難しいが、米国の対応方針に沿って形成された市場からバックアップ製品を調達することができると考えられる	【メリット】　推奨暗号アルゴリズムの個数を限定するので当該推奨暗号アルゴリズムを搭載した製品が存在していると期待することができ、バックアップとして調達することが容易であると考えられる		
	【デメリット】　日本政府の独自判断としての推奨暗号アルゴリズムをバックアップ搭載させることは事実上不可能（もしくは極めてコスト高）	【デメリット】　ある程度の製品数が整うまでの期間、危殆化対策済み（バックアップ搭載）製品を調達しようとすると、調達先が限定、もしくはコスト高につながる恐れがある	【デメリット】　サポートすべき推奨暗号アルゴリズムが明らかではなく、製品化を行う際の指針とはならないため、提案会社以外の暗号アルゴリズムの利用はすでにシェアを握った一部に限られる。そのほかの暗号アルゴリズムの製品化は進まず、調達先は依然限定され調達コストは高くなる	【デメリット】　提案会社以外の暗号アルゴリズムの利用はすでにシェアを握った一部に限られ、利用度が低い推奨暗号アルゴリズムが様々な企業で製品化される可能性は低く、調達先は限定され調達コストは高くなる
	【デメリット】　意図してバックアップのアルゴリズムを用意する場合、選択肢が限られる	【デメリット】　意図してバックアップのアルゴリズムを用意する場合、選択肢が限られる	【メリット】　意図してバックアップのアルゴリズムを用意する場合、選択肢が豊富	【メリット】　意図してバックアップのアルゴリズムを用意する場合、選択肢が豊富
	【メリット】　あらゆるベンダの製品について推奨暗号アルゴリズムの多くに対応したモジュールが開発されるので、暗号アルゴリズムとしてのベンダごとの差異が少なくなり、ベンダロックインの要因になる恐れはない	【メリット】　推奨暗号アルゴリズムとしての提案暗号の位置づけが明確になれば、多くの企業の製品に当該推奨暗号アルゴリズムが搭載されることが期待できるので、ベンダロックインの要因になる恐れは少ない		
			【デメリット】　採用した推奨暗号アルゴリズムが利用実績不足を理由に候補リストへ降格する恐れがある	
		【デメリット】　政府が事実上特定ベンダを支援する形となるため、ベンダロックインの要因になる恐れが高い	【デメリット】　特定製品にしか搭載されていない推奨暗号アルゴリズムが採用されると将来にわたってベンダロックインが発生する恐れがある	【デメリット】　特定製品にしか搭載されていない推奨暗号アルゴリズムが採用されると将来にわたってベンダロックインが発生する恐れがある

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
	【デメリット】 利用実績は正のフィードバックで強化される傾向にあるので、寡占化が進み、他のアルゴリズムは調達可能であっても運用されることは少ない			
	【デメリット】 日本独自の判断で、現時点で主流の暗号アルゴリズムから将来的に別のものに誘導しようとしても、実施は極めて困難	【デメリット】 提案暗号の普及展開を重視すると、利用実績だけでは判断できず、他の指標が必要。調達における基準の平等性の担保が確保できない可能性がある	【デメリット】 利用実績を調達時に考慮したい場合、実績のタイムラグがあるため、後発提案アルゴリズムの普及の阻害要因となる	
	【留意点】 市場における暗号アルゴリズムの利用実績を基に日本独自の方針を打ち出すことは難しいのではないか（「他国を追随することでコストを抑える」という独自の方針を採るならば可能であるが）。日本独自の方針を推進するには、方針に沿った市場が形成されるように関係者にインセンティブを与えながら方針の実現に向けて推進する必要があるのではないか	【留意点】 市場における暗号アルゴリズムの利用実績を基に日本独自の方針を打ち出すことは難しいのではないか（「他国を追随することでコストを抑える」という独自の方針を採るならば可能であるが）。日本独自の方針を推進するには、方針に沿った市場が形成されるように関係者にインセンティブを与えながら方針の実現に向けて推進する必要があるのではないか	【留意点】 市場における暗号アルゴリズムの利用実績を基に日本独自の方針を打ち出すことは難しいのではないか（「他国を追随することでコストを抑える」という独自の方針を採るならば可能であるが）。日本独自の方針を推進するには、方針に沿った市場が形成されるように関係者にインセンティブを与えながら方針の実現に向けて推進する必要があるのではないか	【留意点】 市場における暗号アルゴリズムの利用実績を基に日本独自の方針を打ち出すことは難しいのではないか（「他国を追随することでコストを抑える」という独自の方針を採るならば可能であるが）。日本独自の方針を推進するには、方針に沿った市場が形成されるように関係者にインセンティブを与えながら方針の実現に向けて推進する必要があるのではないか
	【留意点】 SHA-2 より SHA-1 の方が利用実績があるなど、利用実績だけを考慮するだけでは不十分なケースがある。利用実績だけを考慮すれば自然と安全性が高まる方向にあるのか否かを見極めつつ、利用実績以外を考慮する必要がある場合には追加的な判断材料（例えば、アルゴリズムの昇格や降格を行う）を提供する必要がある	【留意点】 SHA-2 より SHA-1 の方が利用実績があるなど、利用実績だけを考慮するだけでは不十分なケースがある。利用実績だけを考慮すれば自然と安全性が高まる方向にあるのか否かを見極めつつ、利用実績以外を考慮する必要がある場合には追加的な判断材料（例えば、アルゴリズムの昇格や降格を行う）を提供する必要がある	【留意点】 SHA-2 より SHA-1 の方が利用実績があるなど、利用実績だけを考慮するだけでは不十分なケースがある。利用実績だけを考慮すれば自然と安全性が高まる方向にあるのか否かを見極めつつ、利用実績以外を考慮する必要がある場合には追加的な判断材料（例えば、アルゴリズムの昇格や降格を行う）を提供する必要がある	【留意点】 SHA-2 より SHA-1 の方が利用実績があるなど、利用実績だけを考慮するだけでは不十分なケースがある。利用実績だけを考慮すれば自然と安全性が高まる方向にあるのか否かを見極めつつ、利用実績以外を考慮する必要がある場合には追加的な判断材料（例えば、アルゴリズムの昇格や降格を行う）を提供する必要がある
	【留意点】 暗号アルゴリズムの違いだけでベンダロックインが生じているわけではない。ベンダロックインを回避するためには、データフォーマットの標準仕様を決めたうえで調達を行うなどの対応が別途必要ではないか	【留意点】 暗号アルゴリズムの違いだけでベンダロックインが生じているわけではない。ベンダロックインを回避するためには、データフォーマットの標準仕様を決めたうえで調達を行うなどの対応が別途必要ではないか	【留意点】 暗号アルゴリズムの違いだけでベンダロックインが生じているわけではない。ベンダロックインを回避するためには、データフォーマットの標準仕様を決めたうえで調達を行うなどの対応が別途必要ではないか	【留意点】 暗号アルゴリズムの違いだけでベンダロックインが生じているわけではない。ベンダロックインを回避するためには、データフォーマットの標準仕様を決めたうえで調達を行うなどの対応が別途必要ではないか

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
C) 「標準化・規格化等」				
	【留意点】　推奨暗号アルゴリズムは国際標準化・規格化済みと考えられ、ほとんど影響を与えることはない	【メリット】　推奨リストが提案暗号の国際標準化・規格化促進手段として活用されれば国内外での注目が集まり、国際標準化・規格策定が促進される可能性がある （海外製の推奨暗号は、そもそも国際標準化されているなど、一定の地位にあると考えられる）	【デメリット】　複数の提案暗号が推奨リストに残る場合には、日本としてどの暗号アルゴリズムを必要としているのがはっきりしない、また普及状況により推奨暗号リストから外される可能性もあるため、日本からの国際標準化・規格化への提案が軽視もしくは無視される可能性が高い	【デメリット】　多数の暗号アルゴリズムの標準化提案は本来の標準化の意義に沿わない。日本としてどの暗号アルゴリズムを必要としているのかはっきりしないため、日本からの国際標準化・規格化への提案は拒絶または無視、軽視される可能性が高い
			【メリット】　利用実績に応じた候補リストへの降格により推奨暗号アルゴリズムが絞り込まれたとすれば、国際標準化・規格化に良い影響を与える可能性がある	
	【メリット】　公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる	【メリット】　公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる	【メリット】　公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる	【メリット】　公的なお墨付きとして安全性評価の裏付けや電子政府への採用実績を紹介できる
	【メリット】　提案暗号が推奨リストに含まれる場合には、NB からの提案として意見をまとめやすいと思われる	【メリット】　NB からの提案として意見をまとめやすいと思われる		
		【デメリット】　日本の国策暗号として注目されることで、国際標準化・規格化に対し海外からネガティブな反応を受ける可能性がある		
	【デメリット】　提案暗号を国際標準化・規格化に提案する際、推奨リストに含まれず候補リストとなるので、普及度の低いものとして不利な解釈を受ける可能性がある	【デメリット】　提案暗号を国際標準化・規格化に提案する際、候補リストよりも推奨リスト入りが期待される。候補リストでは普及度の低いものとして不利な解釈を受ける可能性がある		
	【デメリット】　提案会社の標準化・規格化活動への支援材料にはならない可能性が高いため、提案会社のモチベーションを上げることは難しい	【メリット】　推奨暗号アルゴリズムに選ばれた提案会社にとっては国際標準化や様々な規格化への支援材料になることが期待できるため、国際標準化や規格化活動へのモチベーションが上がる	【メリット】　推奨暗号アルゴリズムに選ばれた提案会社にとっては国際標準化への支援材料になると期待できるため、これらの国際標準化活動へのモチベーションはある	【メリット】　推奨暗号アルゴリズムに選ばれた提案会社にとっては国際標準化への支援材料になると期待できるため、これらの国際標準化活動へのモチベーションはある
			【デメリット】　複数の提案暗号が推奨暗号に残る場合には、日本としてどの暗号アルゴリズムを必要としているのがはっきりせず、様々な規格化活動への支援材料にはならないため、それら規格化策定への当該提案会社のモチベーション向上につながらない	【デメリット】　複数の提案暗号が推奨暗号に残る場合には、日本としてどの暗号アルゴリズムを必要としているのがはっきりせず、様々な規格化活動への支援材料にはならないため、それら規格化策定への当該提案会社のモチベーション向上につながらない

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
			【メリット】　暗号アルゴリズムの降格により、推奨暗号が絞り込まれたとすれば、国際標準化に良い影響を与える可能性があり、提案会社のモチベーションが上がる可能性がある	
		【デメリット】　推奨暗号アルゴリズムに選ばれなかった提案会社にとっては国際標準化や様々な規格化活動へのモチベーション向上につながらない	【留意点】　提案会社は自らが興味を持つ国際標準化・規格化しか推進しない可能性がある	【留意点】　提案会社は自らが興味を持つ標準化・規格化しか推進しない可能性がある
			【留意点】　国際標準化や規格化（入り・選定中）を理由に、電子政府での利用実態がないにもかかわらず推奨リストに残り続けることがないか	
			【留意点】　推奨暗号から候補暗号への降格の基準に応じて、評価点が大きく変化する	

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
D)「提案暗号利用促進」				
	【デメリット】　全世界特許無償化しても、提案暗号が推奨リストに入らなければサポートするメリットが見出せず、採用拡大は期待できないため、（米国政府標準暗号によって）寡占されたままになる	【メリット】　提案暗号が推奨リストに含まれ製品化促進手段として活用されることで、促進策の内容がそのまま提案暗号をサポートすることに対するモチベーションにつながり、当該提案暗号の利用促進が期待できる	【デメリット】　全世界特許無償化しても、様々な国際標準化・規格化に採用されていない提案暗号は（提案会社以外にとって）事実上サポートする対象になりえない	【デメリット】　全世界特許無償化しても、様々な国際標準化・規格化に採用されていない提案暗号は（提案会社以外にとって）事実上サポートする対象になりえない
			【デメリット】　様々な国際標準化・規格化に採用された提案暗号（国産暗号）も日本市場での利用見通しがはっきりせず、サポート困難である可能性が高い	【デメリット】　様々な国際標準化・規格化に採用された提案暗号だったとしても、日本市場での利用見通しがはっきりせず、サポート困難
	【メリット】　推奨暗号アルゴリズムの個数が限定されるため、フルラインナップ戦略が可能であり、提案会社以外もサポートする	【メリット】　推奨暗号アルゴリズムの個数が限定されるため、フルラインナップ戦略が可能であり、提案会社以外もサポートすると期待される	【デメリット】　候補リストへの降格の恐れがある提案暗号の場合、提案会社以外の企業・団体がサポートする対象にはなりにくい	【デメリット】　例え社内で提案暗号のサポートのメリットが理解されたとしても、多数の提案暗号をサポート（製品化、継続的サポート）することは困難
	【留意点】　提案暗号が推奨暗号アルゴリズムに選ばれる可能性は高くなく、支援対象が政策的に支援したい対象とマッチするとは限らない	【メリット】　推奨暗号アルゴリズムの個数が限定されるため、政策的な支援の意図が明確になる上一つあたりの利用促進のためにかけられるコストが大きくなるので、当該提案暗号に対して効果的な支援が可能	【デメリット】　推奨暗号アルゴリズムの個数が多くなるほど、一つあたりの利用促進のためにかけられるコストが小さくなるため、効果的な支援は困難	【デメリット】　推奨暗号アルゴリズムの個数が多いため、一つあたりの利用促進のためにかけられるコストが小さく、平等公平に効果的な支援は困難
			【メリット】　候補暗号への降格により、推奨暗号が絞り込まれた場合には、政府がサポートする対象が明確になる	
			【デメリット】　候補リストへの降格が予想される暗号アルゴリズムを支援対象にすることは無駄であり、推奨リストと候補リストで支援内容を分ける方法はシナリオ 3 の方針では理解を得にくいのではないか	
		【デメリット】　提案暗号の利用が継続されなければサポート品質（改良、危殆化対策など）が低下する		
	【メリット】　基本特許が無償化されることで利用が促進される	【メリット】　推奨リストに選ばれた提案暗号について特許無償化と国際標準化・規格化の促進により、他社（提案会社や他のシステム開発会社等）からの製品化・サポートも受けやすくなるため、当該提案暗号の利用が促進される可能性がある	【メリット】　推奨リストに選ばれた提案暗号について特許無償化と国際標準化･規格化が促進していれば、他社（提案会社や他のシステム開発会社等）からの製品化・サポートも受けやすくなるため、当該提案暗号の利用が促進される可能性がある	【メリット】　推奨リストに選ばれた提案暗号について特許無償化と国際標準化･規格化が促進していれば、他社（提案会社や他のシステム開発会社等）からの製品化・サポートも受けやすくなるため、当該提案暗号の利用が促進される可能性がある
		【メリット】　全世界特許無償化によって契約上のリスク（訴訟費用負担など）が軽減されるため、製品化・サポートに対する社内での理解を得やすい	【メリット】　全世界特許無償化によって契約上のリスク（訴訟費用負担など）が軽減されるため、製品化・サポートに対する社内での理解を得やすい	

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
	【留意点】 ベンダロックインを回避するためには全世界特許無償化をしていない提案暗号を利用促進活動の対象とすることはできない	【留意点】 ベンダロックインを回避するためには全世界特許無償化をしていない提案暗号を利用促進活動の対象とすることはできない	【留意点】 ベンダロックインを回避するためには全世界特許無償化をしていない提案暗号を利用促進活動の対象とすることはできない	【留意点】 ベンダロックインを回避するためには全世界特許無償化をしていない提案暗号を利用促進活動の対象とすることはできない
	【留意点】 提案会社および第三者による回避困難な実装特許までを含めて無償化しなければ、促進効果は見込めない	【留意点】 提案会社および第三者による回避困難な実装特許までを含めて無償化しなければ、促進効果は見込めない	【留意点】 提案会社および第三者による回避困難な実装特許までを含めて無償化しなければ、促進効果は見込めない	【留意点】 提案会社および第三者による回避困難な実装特許までを含めて無償化しなければ、促進効果は見込めない
			【デメリット】 全世界特許無償化をしていない提案暗号が国際標準化や様々な規格化に採用される可能性はほとんどない	【デメリット】 全世界特許無償化をしていない提案暗号が国際標準化や様々な規格化に採用される可能性はほとんどない
			【デメリット】 全世界特許無償は様々な国際標準化・規格化への採用活動をしていない提案会社のビジネスモデルと壊す恐れが高い	【デメリット】 全世界特許無償は様々な国際標準化・規格化への採用活動をしていない提案会社のビジネスモデルと壊す恐れが高い
	【メリット】 シェアを奪えなければ、推奨リスト入りできないので、提案会社による利用促進が見込める	【メリット】 推奨リストが製品化促進手段として活用されるため、推奨リストに選ばれた提案暗号の提案会社による利用促進に対するモチベーション向上につながる	【メリット】 純粋な自由競争であり、利用実績に応じて降格の可能性があるため、提案会社の利用促進活動に対するモチベーションを向上させる可能性がある	【メリット】 純粋な自由競争であり、提案会社が自社のビジネス範囲内に囲い込んで利用することに対してはモチベーションがあると考えられる
			【デメリット】 他社実績をつませないため、少なくとも自社の提案暗号が候補リストに降格しない限り、他社暗号アルゴリズムを利用しないモチベーションとなる。提案会社の囲い込み意識が働く	【デメリット】 自社の提案暗号が推奨暗号アルゴリズムとなっている状況で、他社の提案暗号をサポートするという状況は想定し難い
		【留意点】 推奨リストに選ばれた提案暗号を（推奨リストに選ばれなかった）他の提案会社がサポートする可能性があるか否かをヒアリングで確認する必要がある	【留意点】 推奨リストに選ばれた提案暗号を（推奨リストに選ばれなかった）他の提案会社がサポートする可能性があるか否かをヒアリングで確認する必要がある	
	【デメリット】 推奨リスト入りが難しく、政府調達の可能性が狭まるため、提案会社のモチベーションを上げることは難しい		【デメリット】 普及度を基準にすると、推奨暗号に提案暗号が含まれる可能性は低く、モチベーションが高まる可能性は低い	【デメリット】 現在の推奨暗号リストにおける状況と変わらないため、提案会社のモチベーション向上につながらない可能性がある
			【留意点】 推奨暗号から候補暗号への降格の基準に応じて、評価点が大きく変化する	
	【留意点】 法拠による公告（例：米国反トラスト法）であれば、無償化は保証できるかもしれないが、日本で無償化を保証する（第三者による特許侵害警告）手段が思い当らない。同様に提案会社による保証も困難	【留意点】 法拠による公告（例：米国反トラスト法）であれば、無償化は保証できるかもしれないが、日本で無償化を保証する（第三者による特許侵害警告）手段が思い当らない。同様に提案会社による保証も困難	【留意点】 法拠による公告（例：米国反トラスト法）であれば、無償化は保証できるかもしれないが、日本で無償化を保証する（第三者による特許侵害警告）手段が思い当らない。同様に提案会社による保証も困難	【留意点】 法拠による公告（例：米国反トラスト法）であれば、無償化は保証できるかもしれないが、日本で無償化を保証する（第三者による特許侵害警告）手段が思い当らない。同様に提案会社による保証も困難

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
	【留意点】　オブジェクト ID（OID）を持たないアルゴリズムもあるので、基本用途について統一的に OID を発行すれば、利用促進になる	【留意点】　オブジェクト ID（OID）を持たないアルゴリズムもあるので、基本用途について統一的に OID を発行すれば、利用促進になる	【留意点】　オブジェクト ID（OID）を持たないアルゴリズムもあるので、基本用途について統一的に OID を発行すれば、利用促進になる	【留意点】　オブジェクト ID（OID）を持たないアルゴリズムもあるので、基本用途について統一的に OID を発行すれば、利用促進になる
	【留意点】　輸出管理での取り扱いに、推奨リストや候補リストごとの統一基準を提供できれば、利用促進になる	【留意点】　輸出管理での取り扱いに、推奨リストや候補リストごとの統一基準を提供できれば、利用促進になる	【留意点】　輸出管理での取り扱いに、推奨リストや候補リストごとの統一基準を提供できれば、利用促進になる	【留意点】　輸出管理での取り扱いに、推奨リストや候補リストごとの統一基準を提供できれば、利用促進になる

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
E) 「セキュリティ研究体制」				
	【デメリット】 新しい暗号アルゴリズムを開発しても市場で受け入れられる可能性は低い。推奨リスト入りするのは困難であり、候補リストでは普及が見込めないのでモチベーションが低下する	【デメリット】 推奨暗号アルゴリズムの個数を限定するため、新しい暗号アルゴリズムを開発しても推奨リスト入りするのは困難であり、候補リストでは普及が見込めないのでモチベーションが低下する	【メリット】 推奨リストが新しい暗号アルゴリズムを開発した場合の一つの到達点としてのモチベーションにつながり、新しい暗号アルゴリズムの開発が継続できる可能性が高まる	【メリット】 推奨リストが新しい暗号アルゴリズムを開発した場合の一つの到達点としてのモチベーションにつながり、新しい暗号アルゴリズムの開発が継続できる可能性が高まる
			【デメリット】 提案会社内だけで自社開発暗号アルゴリズムを利用することが事実上の前提であるならば、経営判断の影響を受けやすい構造にある	【デメリット】 提案会社内だけで自社開発暗号アルゴリズムを利用することが事実上前提であるため、経営判断の影響を受けやすい構造にある
		【メリット】 国産暗号として有望な暗号アルゴリズムが開発された場合には、提案会社の枠を超え官学民からのバックアップが期待される	【メリット】 安全性評価対象が多いため、新しい安全性評価技術や検証の豊富な研究素材となり、暗号研究の強化につながる	【メリット】 安全性評価対象が多いため、新しい安全性評価技術や検証の豊富な研究素材となり、暗号研究の強化につながる
	【デメリット】 新しいアルゴリズムが推奨リスト入りするのは困難であり、リストが固定化しやすい。モチベーションにつながらないので企業での研究体制の低迷につながる	【デメリット】 新しいアルゴリズムが推奨リスト入りするのは困難であり、リストが固定化しやすい。モチベーションにつながらないので企業での研究体制の低迷につながる	【デメリット】 多くの場合、最終的に推奨リストとして残る可能性は低いためモチベーションを維持することは難しい	
	【デメリット】 現在主流の暗号アルゴリズムの寿命が十分あると見込まれる間は独自暗号開発不要論が強まる可能性があり、特に企業における暗号研究体制の縮小が余儀なくされる恐れがある	【デメリット】 推奨暗号アルゴリズムの個数を限定するため、独自暗号開発不要論が強まる可能性があり、企業としての暗号研究体制の縮小の可能性がある	【デメリット】 普及度（だけ）が技術評価の指標としてクローズアップされる可能性があり、候補リストへ降格した提案暗号の提案会社では研究体制維持を難しくする可能性がある	
		【デメリット】 推奨リストとしての普及活動に要員リソースを投入する必要がある		
	【メリット】 欧米のように、現在の暗号アルゴリズム主体の研究体制からセキュリティ応用研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを促す効果が期待できる	【メリット】 欧米のように、現在の暗号アルゴリズム主体の研究体制からセキュリティ応用研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを促す効果が期待できる	【デメリット】 欧米とは違い、暗号アルゴリズム主体の研究体制からセキュリティ応用研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを妨げる恐れがある	【デメリット】 欧米とは違い、暗号アルゴリズム主体の研究体制からセキュリティ応用研究主体の研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを妨げる恐れがある
			【メリット】 候補リストへ降格した提案暗号の提案会社では、欧米のように、現在の暗号アルゴリズム主体の研究体制からセキュリティ応用研究や特定用途向けセキュリティ研究主体の研究体制へのリソースシフトを促す効果が期待できる	

	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
F) 「CRYPTREC 活動成果」				
	【メリット】 推奨リストと候補リストで差異化が図られるので、リストの役割が明確化され、参照しやすくなる	【メリット】 推奨リストと候補リストで差異化が図られるので、推奨する提案暗号を明確にするという意味から極めて明確	【デメリット】 利用実績による降格は、明確な基準が困難であり、推奨リストと候補リストとの差異、位置づけは不明確	【デメリット】 推奨暗号リストと候補暗号リストとの差異、位置づけの違いは極めて不明確
			【デメリット】 単に市場での普及に任せていても、現在の米国暗号有利の状況が変わるわけではなく、分割の意味ある効果は期待できない	
			【デメリット】 危殆化以外の理由（利用実績等）による降格は暗号開発ベンダ、および市場に受け入れられない可能性がある	
			【メリット】 推奨リストと候補リストで差異化が図られるので、リストの役割が明確化され、参照しやすくなる	
		【デメリット】 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「その他」の要素が明確にならない限り、リストの位置づけは不明確		
	【メリット】 候補リストは安全性についてのお墨付きを与えるポジション	【メリット】 候補リストは安全性についてのお墨付きを与えるポジションであり、国産暗号育成手段として明確	【メリット】 候補リストは安全性についてのお墨付きを与えるポジションで位置づけは明確だが、効果は限定的	【デメリット】 候補暗号リストに含まれる暗号アルゴリズムはほとんどないと考えられ、別リストである利点がない
	【デメリット】 提案暗号が候補リストから推奨リストへ昇格できる可能性はほとんどない	【留意点】 推奨されていない候補リストの位置づけになるので、実質的にアルゴリズム利用終息勧告と受け取られないか		
	【デメリット】 結果的に米国政府の動きを追随する形になり、日本独自の施策がほとんど含まれていないため、事実上、CRYPTREC の活動の必要性低下が懸念される	【メリット】 推奨リスト選定には提案暗号の普及展開の要素が必要であり、その判断・運用を行う組織として、CRYPTREC 活動の必要性を主張できる	【メリット】 候補リストへの降格においてはその判断・運用を行う組織が必要であり、候補リストへの降格を行った後の推奨リストを活かせるのであれば CRYPTREC 活動の必要性を主張できる	【デメリット】 推奨暗号アルゴリズムとなっていても調達が難しい暗号が存在する可能性があり、その場合、推奨リストの価値が低下し、CRYPTREC の成果も分かりにくくなる
			【メリット】 国産暗号技術を育て、さらにそれを取捨選択する機関として評価できる	
			【デメリット】 推奨リストに提案暗号が残らない可能性があり、その場合、CRYPTREC 活動の必要性を主張しにくくなる可能性がある	

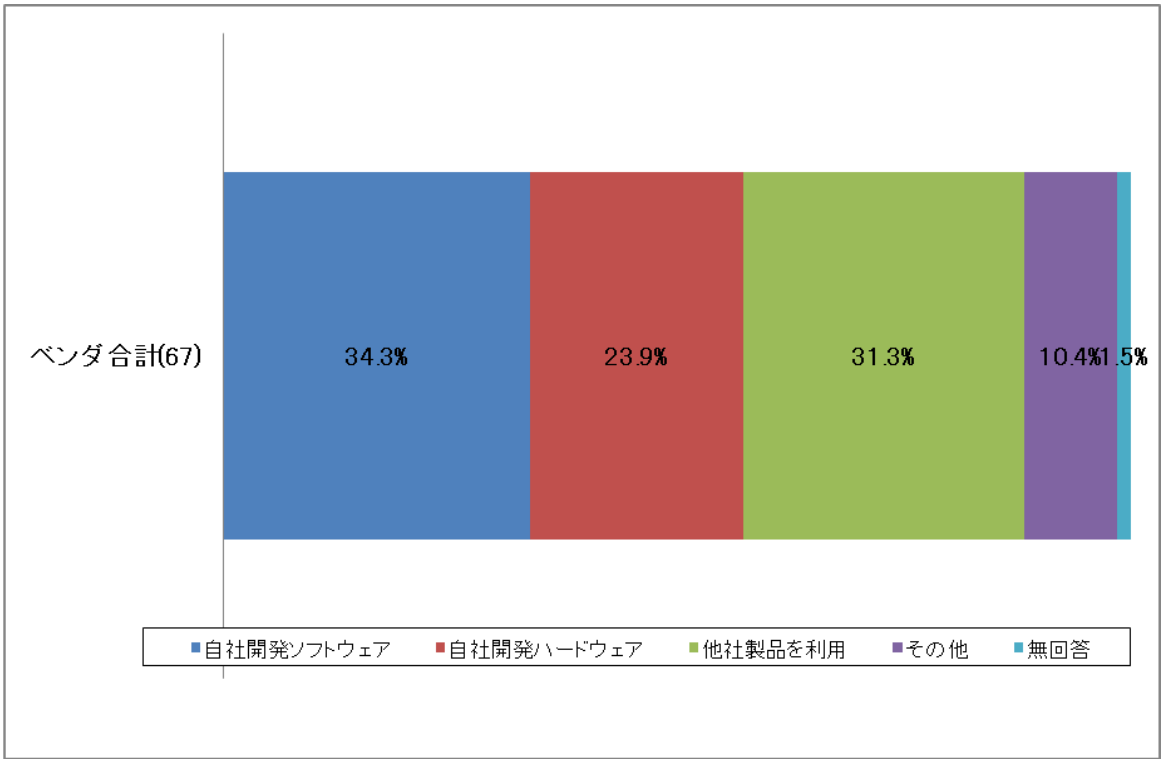
	シナリオ 1 現状の利用実績最重視	シナリオ 2 製品化促進手段として活用	シナリオ 3 次期リスト改訂後の普及で判断	シナリオ 4 現状リストとほぼ同等
	【メリット】　推奨リストに活動を注力でき、コストパフォーマンスが良い	【メリット】　推奨リストに活動を注力でき、コストパフォーマンスが良い		【デメリット】　リストは増加方向なのでコストは増大する一方であり、コストパフォーマンスは低下する
		【デメリット】　推奨リストに選ばれた提案暗号のプロモーションのためのコストが発生する		
	【デメリット】　安全性評価に関しては海外から多くの成果を享受できるため、CRYPTREC 活動の評価が得られにくい			【デメリット】　推奨リストが調達の実情と相関性が薄いため、実体として暗号研究者のためだけの活動とみなされる恐れがある
			【留意点】　候補リストへの「降格の基準」に応じて、シナリオ 3 は、シナリオ 1, 2, 4 のいずれにもなりうる。シナリオ 3 を選択する場合には、候補リストへの降格後に推奨リストがどうなるかをイメージできる程度に基準について議論しておくことが望ましい	
	【留意点】　十分に普及していないが今後普及させたい暗号アルゴリズムや推奨暗号アルゴリズムが危殆化した場合のバックアップの扱い（どのようにリスト間の遷移を図るか）などを検討する必要があると考えられる			
	【留意点】　たとえば日本が優勢の産業分野での利用の観点など、日本独自の判断基準を維持するための活動として必要である	【留意点】　たとえば日本が優勢の産業分野での利用の観点など、日本独自の判断基準を維持するための活動として必要である		
		【留意点】　推奨リストの取り扱いは、非関税障壁とならないよう、公平性の担保に留意する必要がある		

付録 2　外部アンケート結果概要（抜粋）

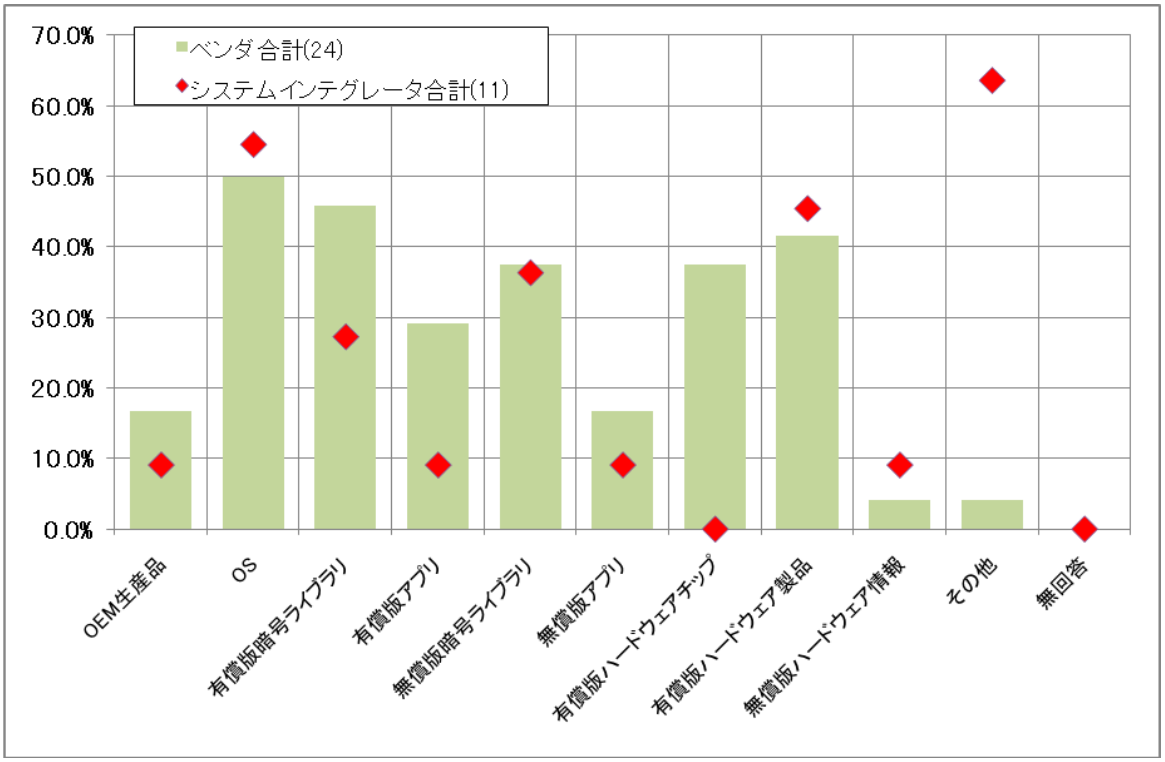
以下のグラフ中の有効回答数は、特に断りがない限り、以下の数値である。
なお、実際の有効数は凡例または見出し中に「○○(xx)」のように記述する。

- ベンダ合計：67
  非応募ベンダ：43　応募ベンダ（応募企業の事業部門及び応募企業のグループ会社）：24
- システムインテグレータ合計：11
- 政府機関：6
- 応募者（応募企業の研究開発部門）：9

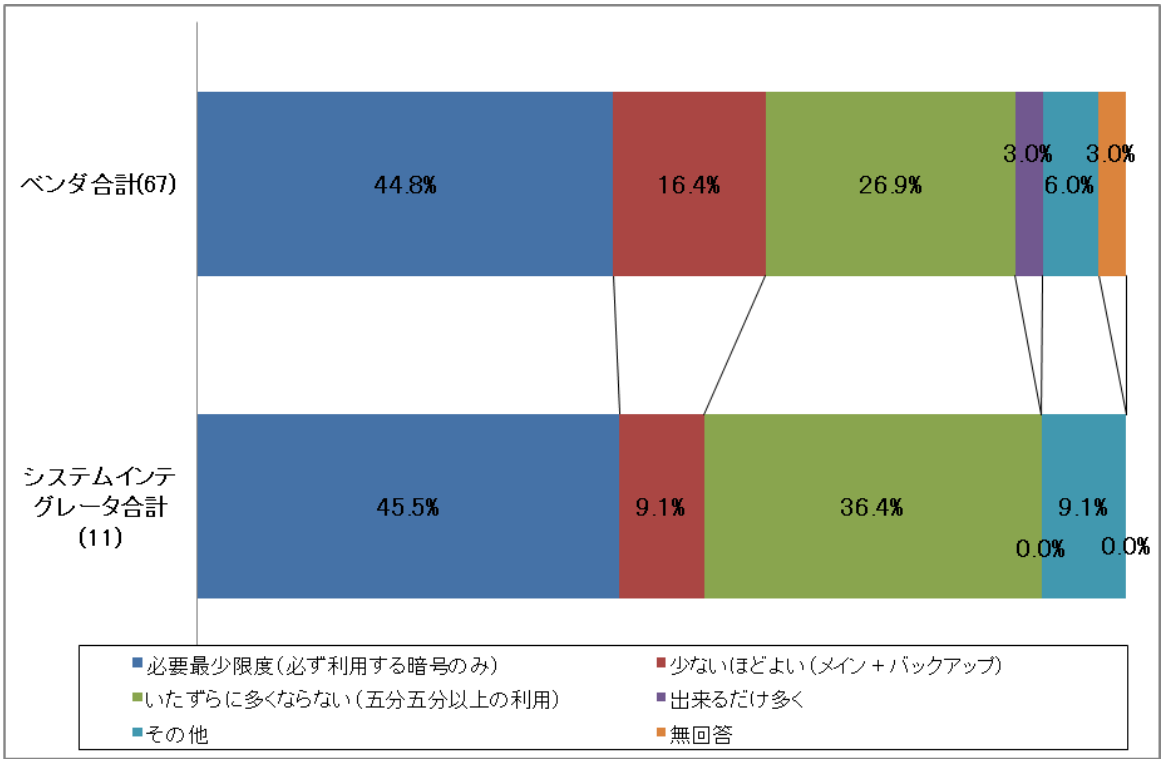
● 暗号搭載製品で利用する暗号アルゴリズムをどのような方法で実現しているか？



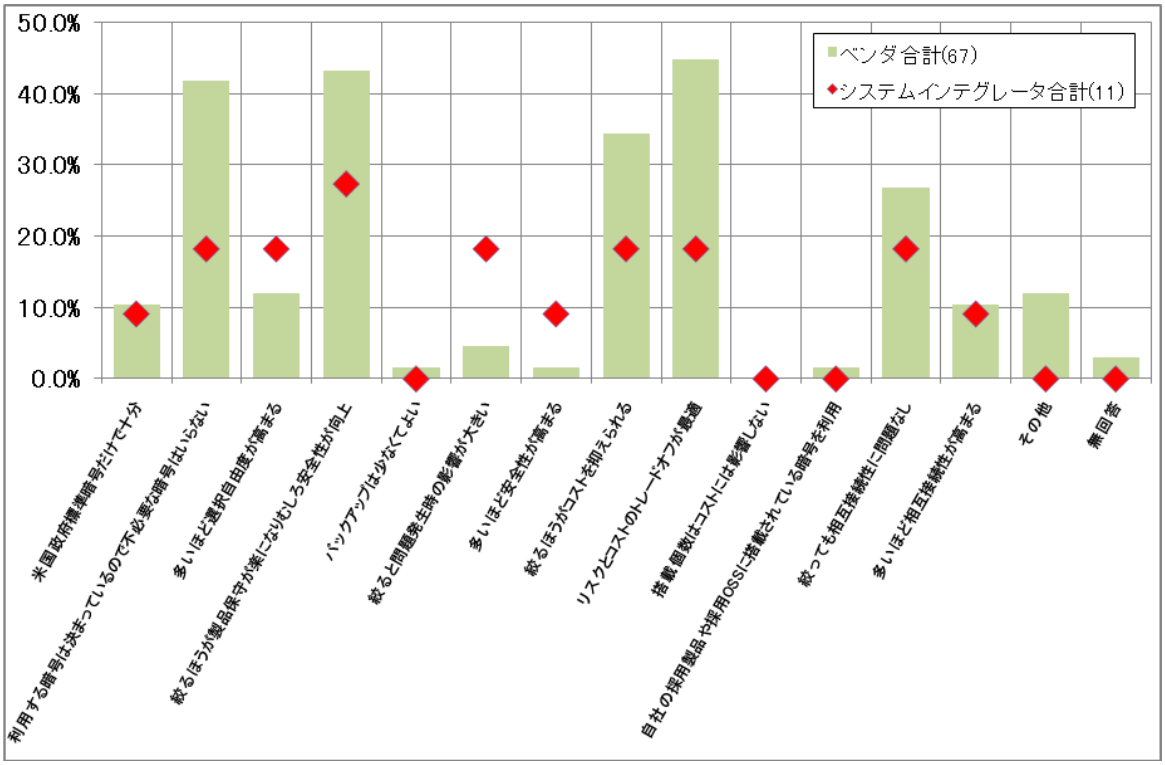
● 他社製品を利用している場合、どのような他社製品に搭載されている暗号アルゴリズムを利用しているか？



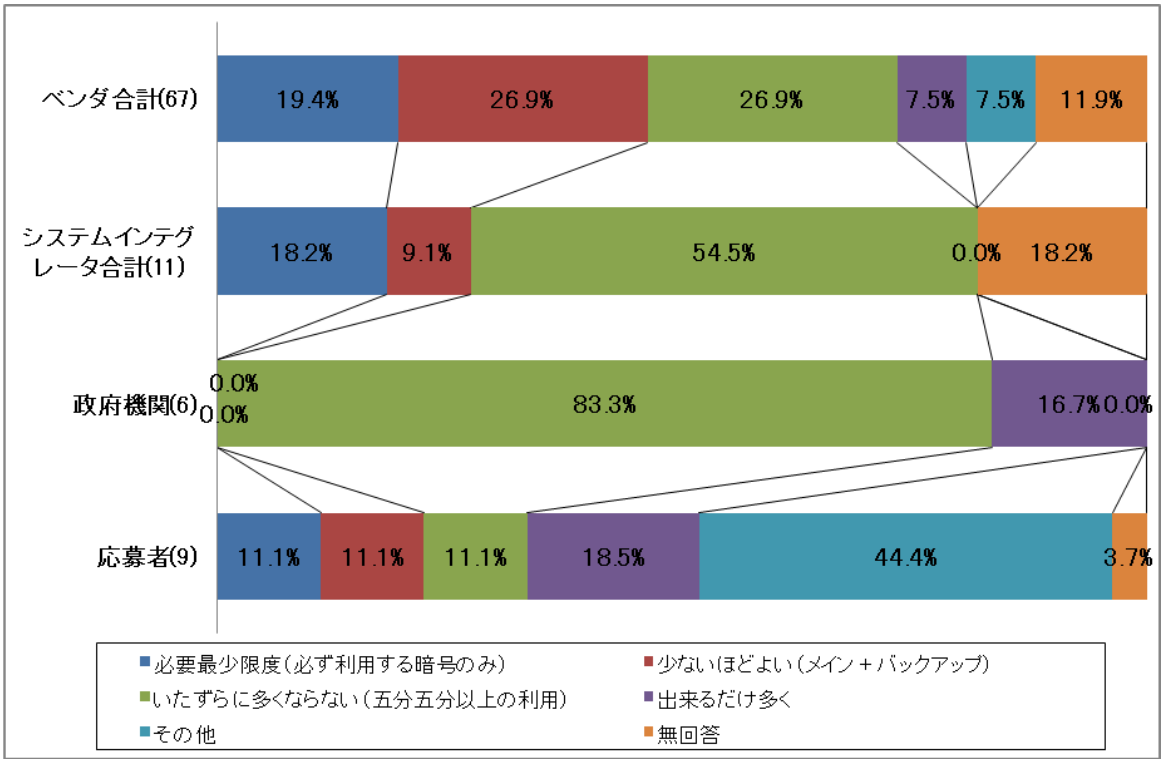
● 暗号搭載製品・システムに搭載する暗号アルゴリズムの個数はどの程度がよいか？



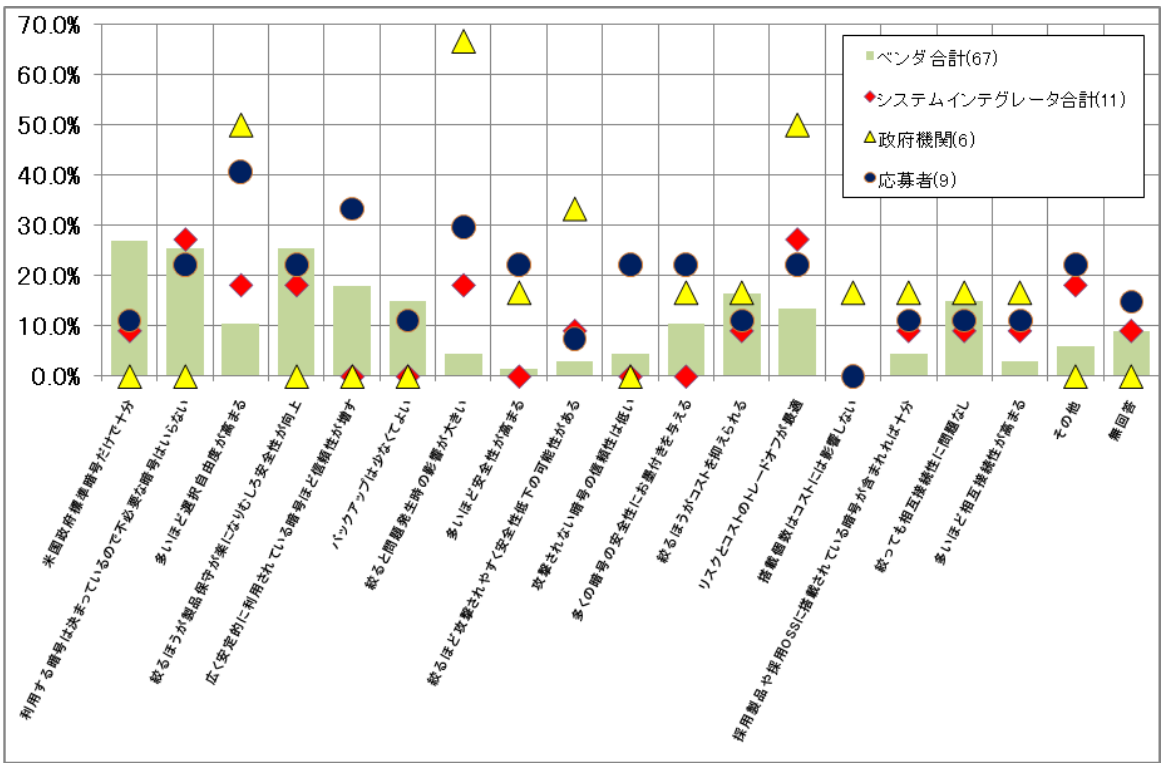
● なぜ上記のように考えるのか？



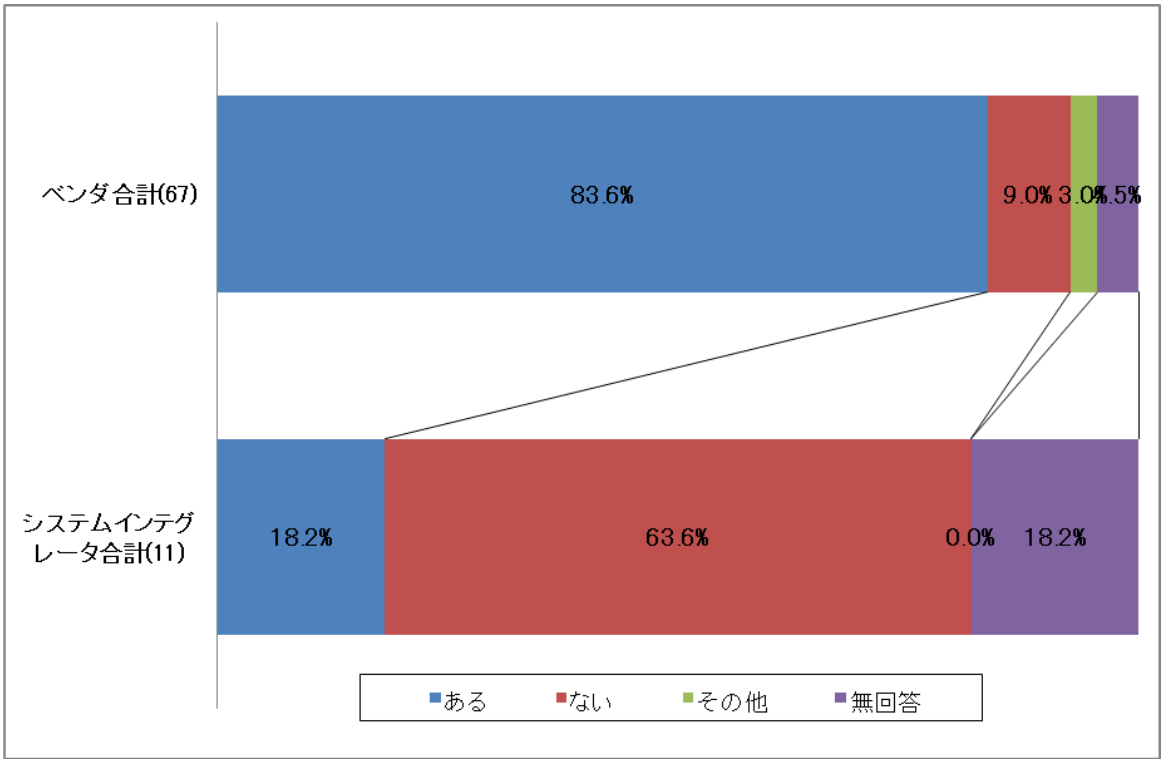
● 次期電子政府推奨暗号リストに掲載されるアルゴリズムの個数はどの程度がよいか？



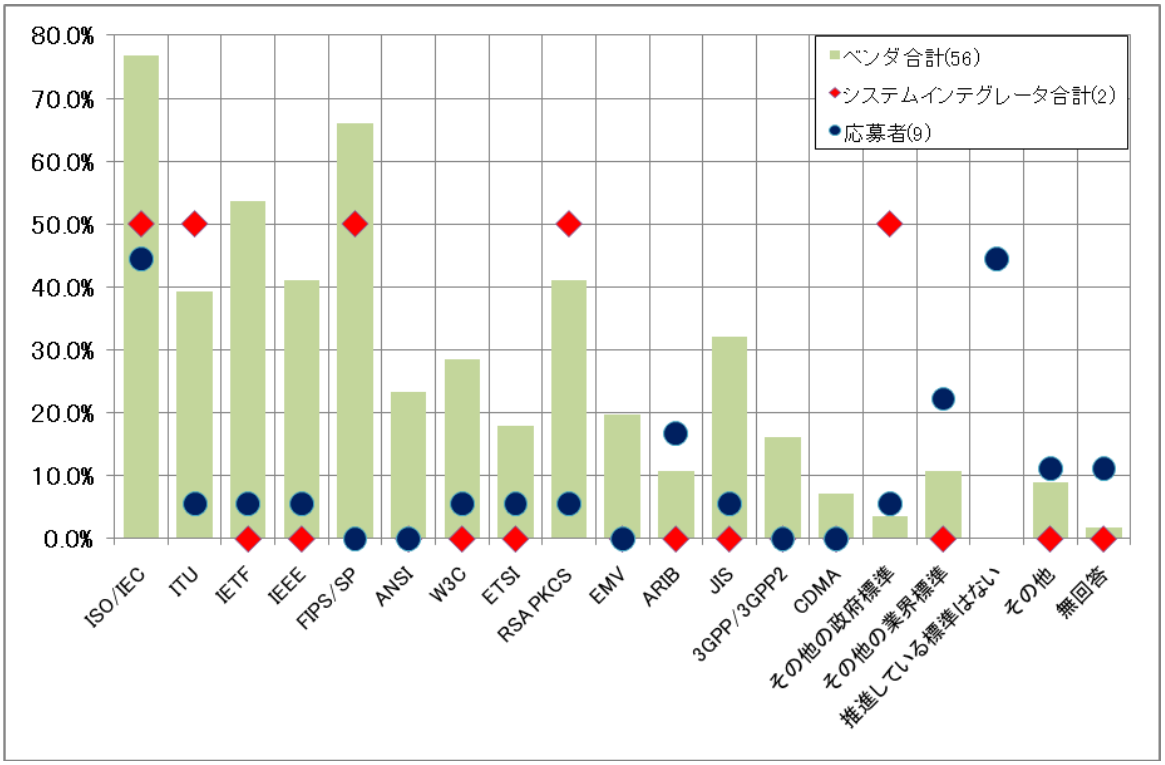
● なぜ上記のように考えるのか？



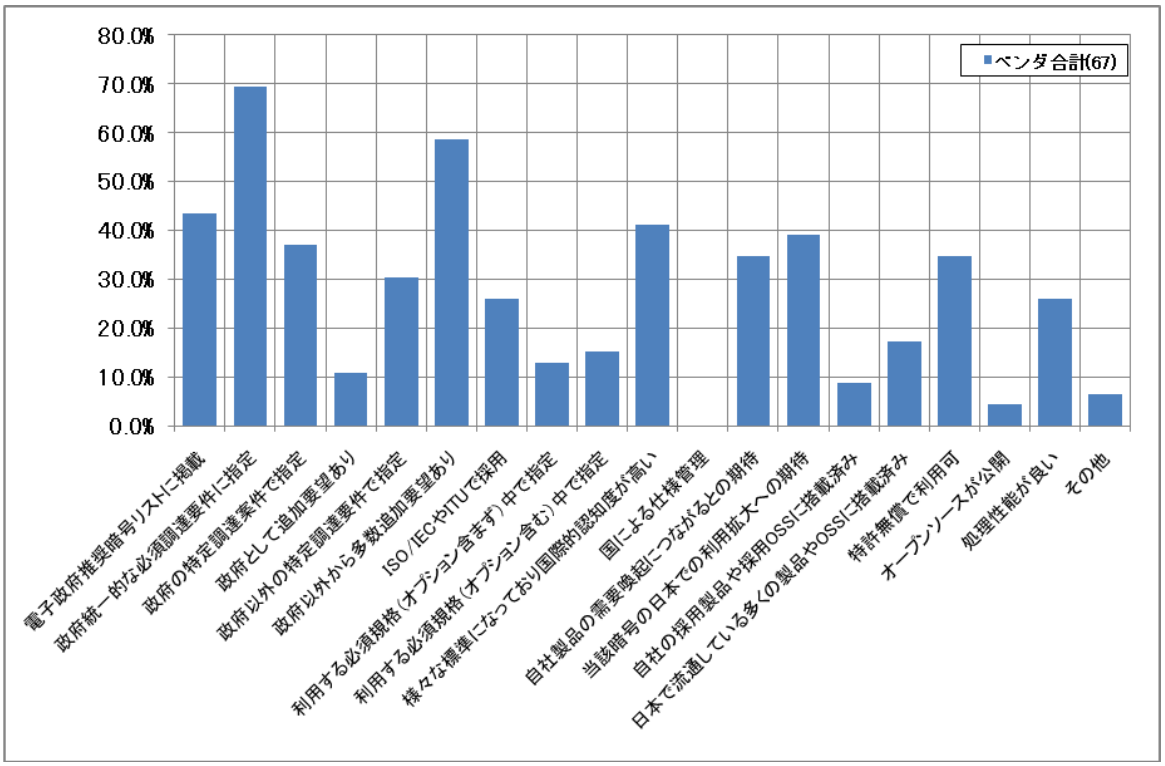
● 暗号搭載製品・システムの開発で利用する標準規格等があるか？



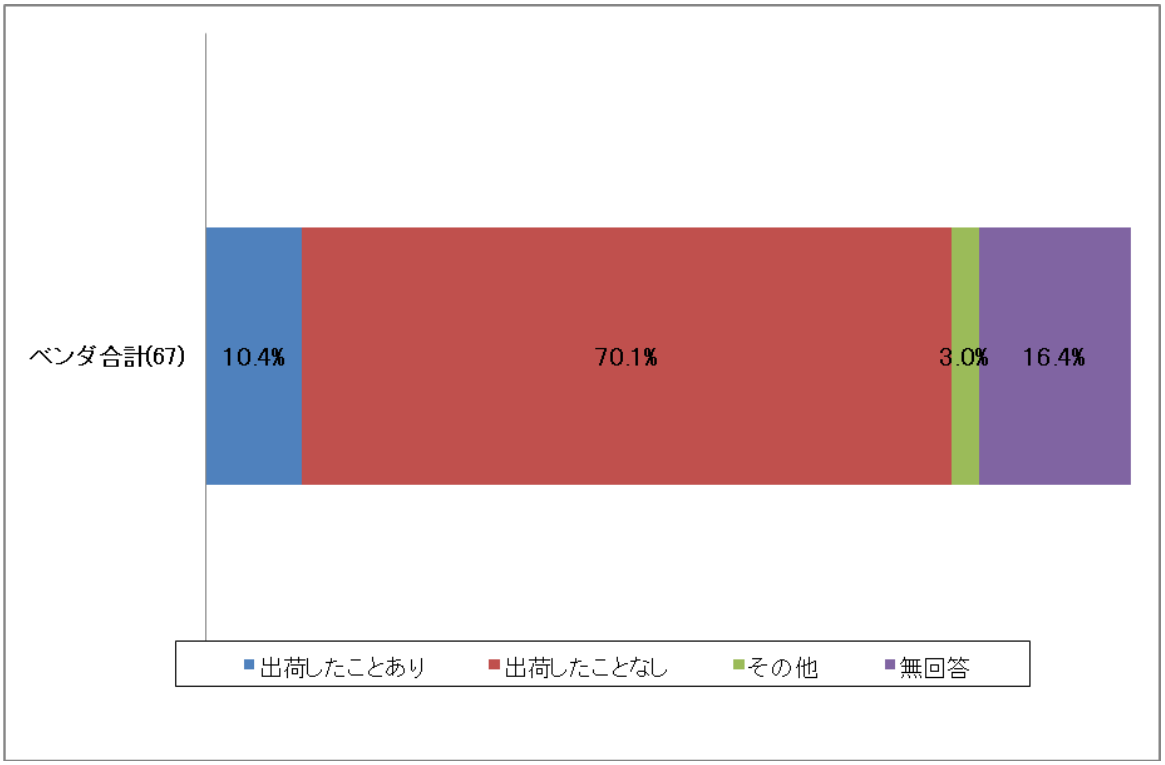
● 暗号搭載製品・システムの開発で利用する標準規格等は何か？／推進している標準化規格等は何か？



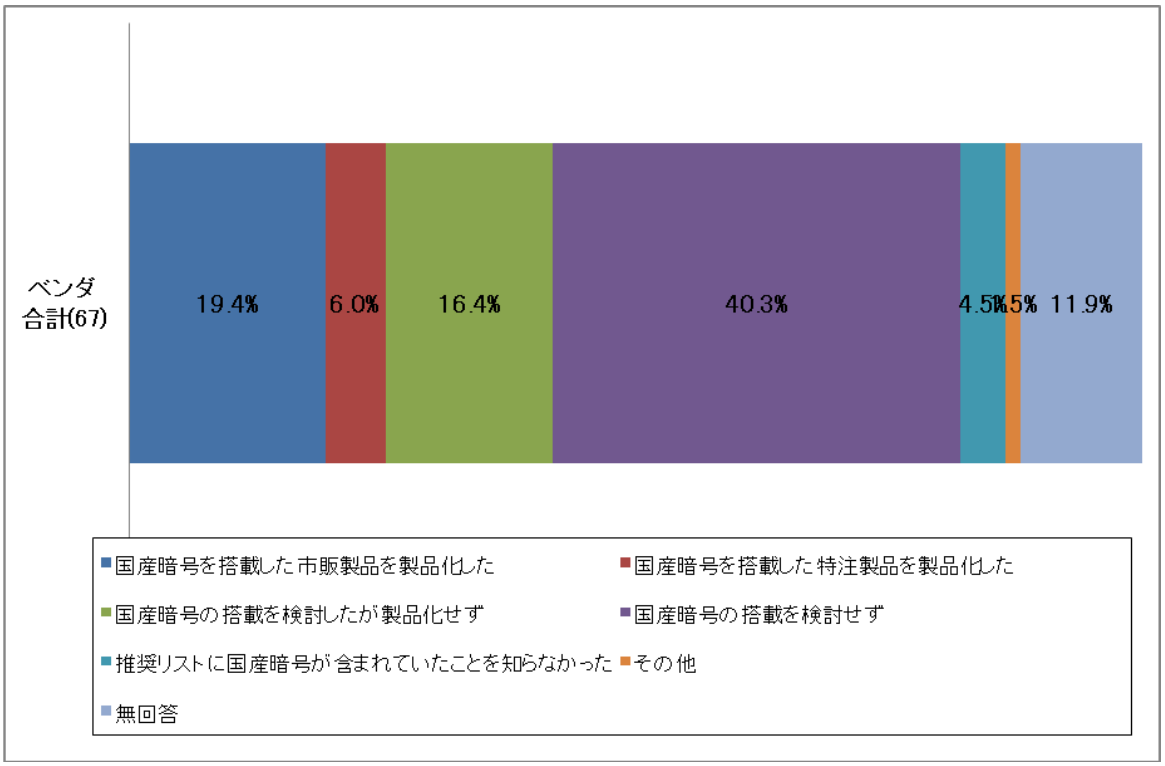
● 米国政府標準暗号以外を追加する条件は何か？



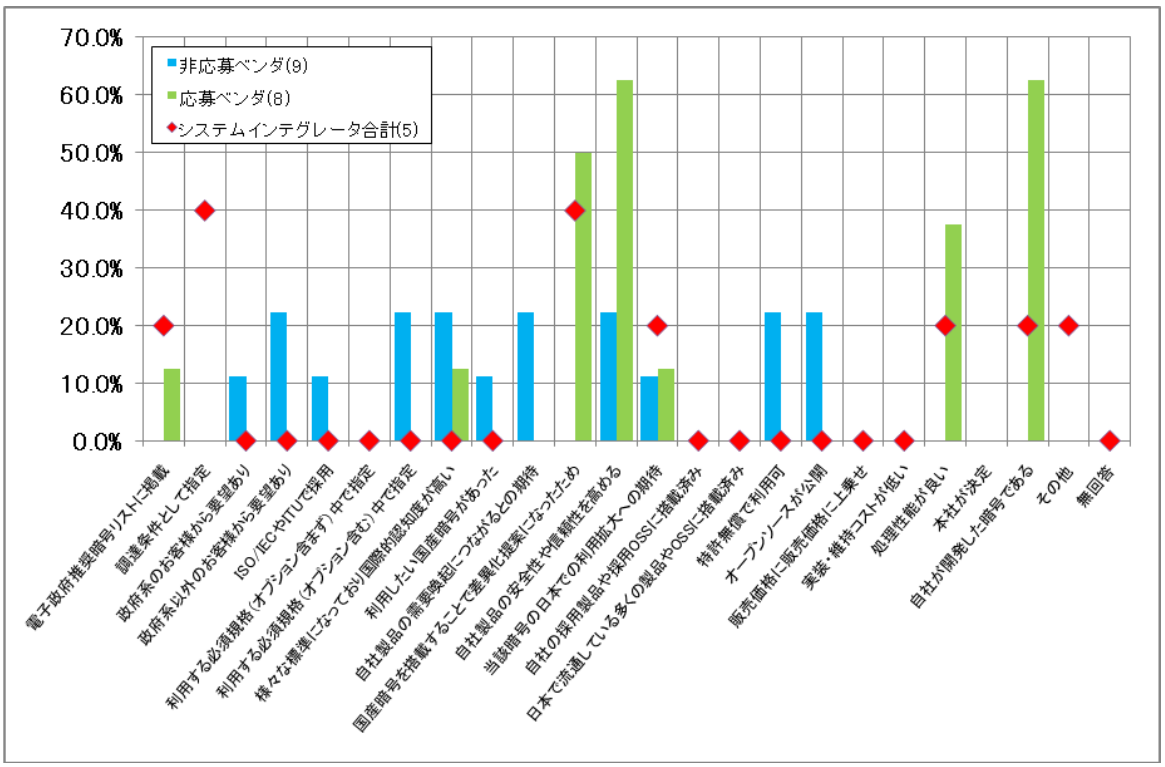
● 各国政府からの要求に対応して暗号搭載製品に別途暗号アルゴリズムを追加して出荷した実績があるか？



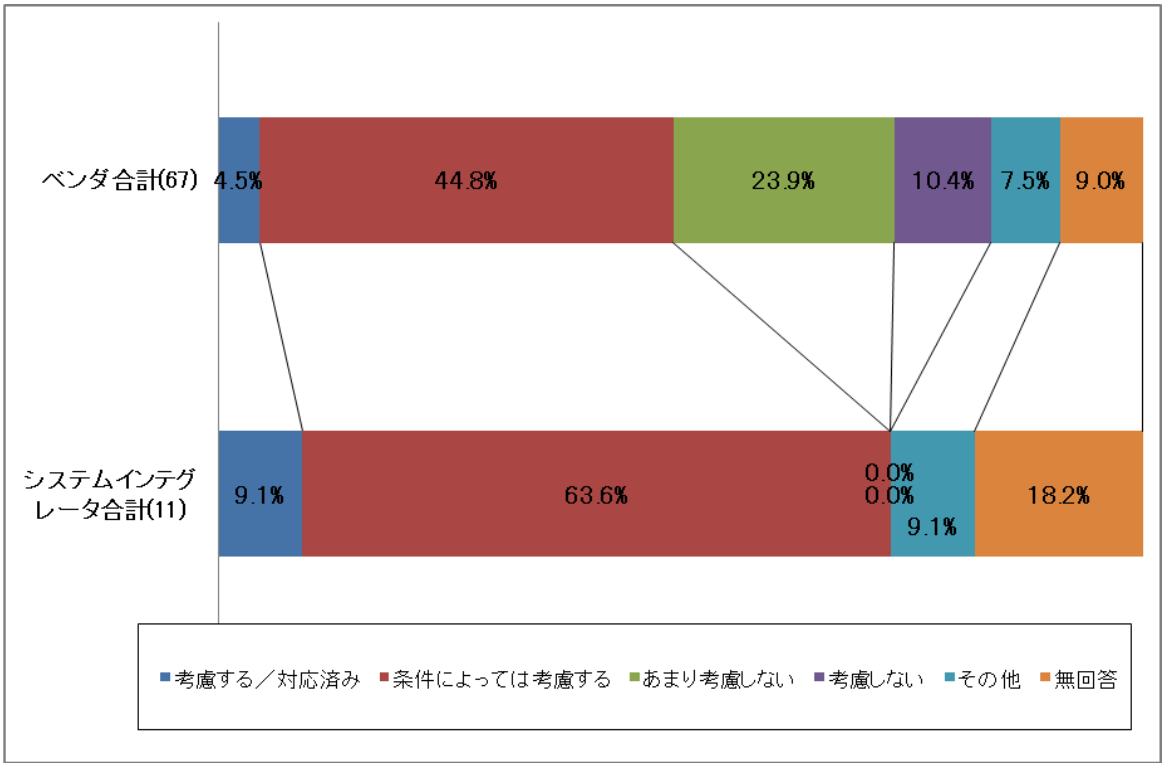
● 電子政府推奨暗号である国産暗号を搭載した製品を出荷した実績があるか？



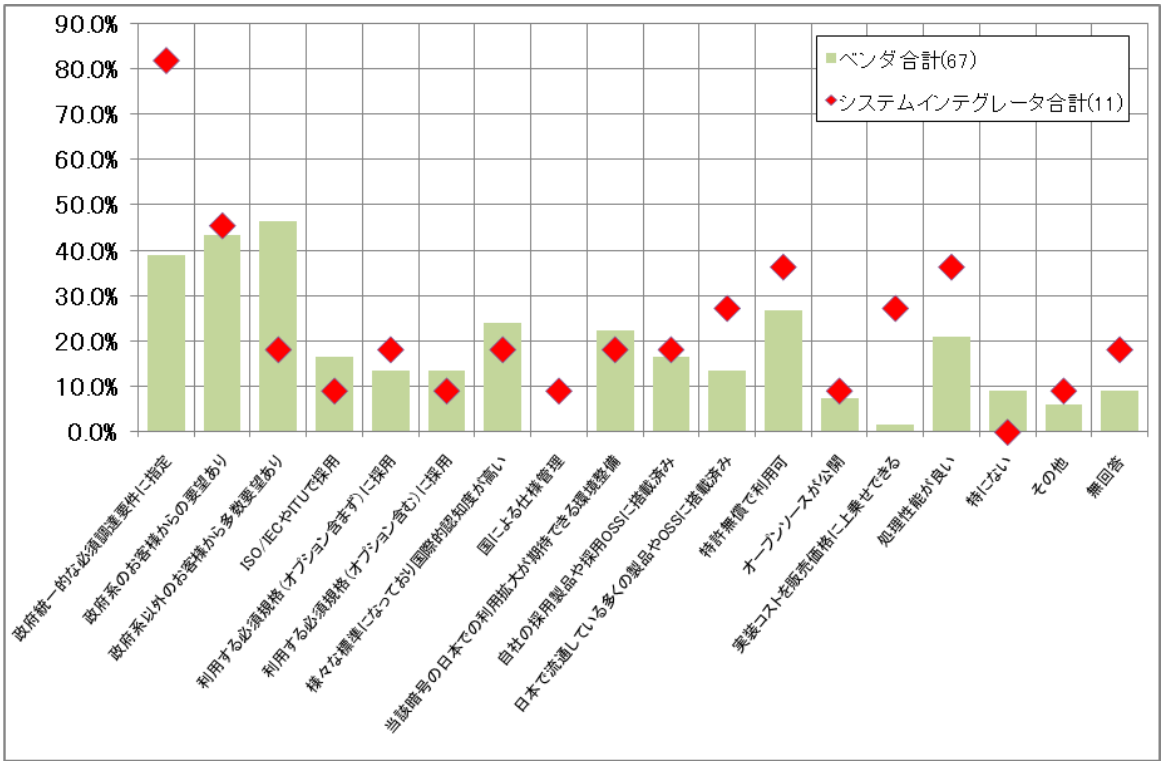
● 電子政府推奨暗号である国産暗号を暗号搭載製品・システムに採用したのはなぜか？



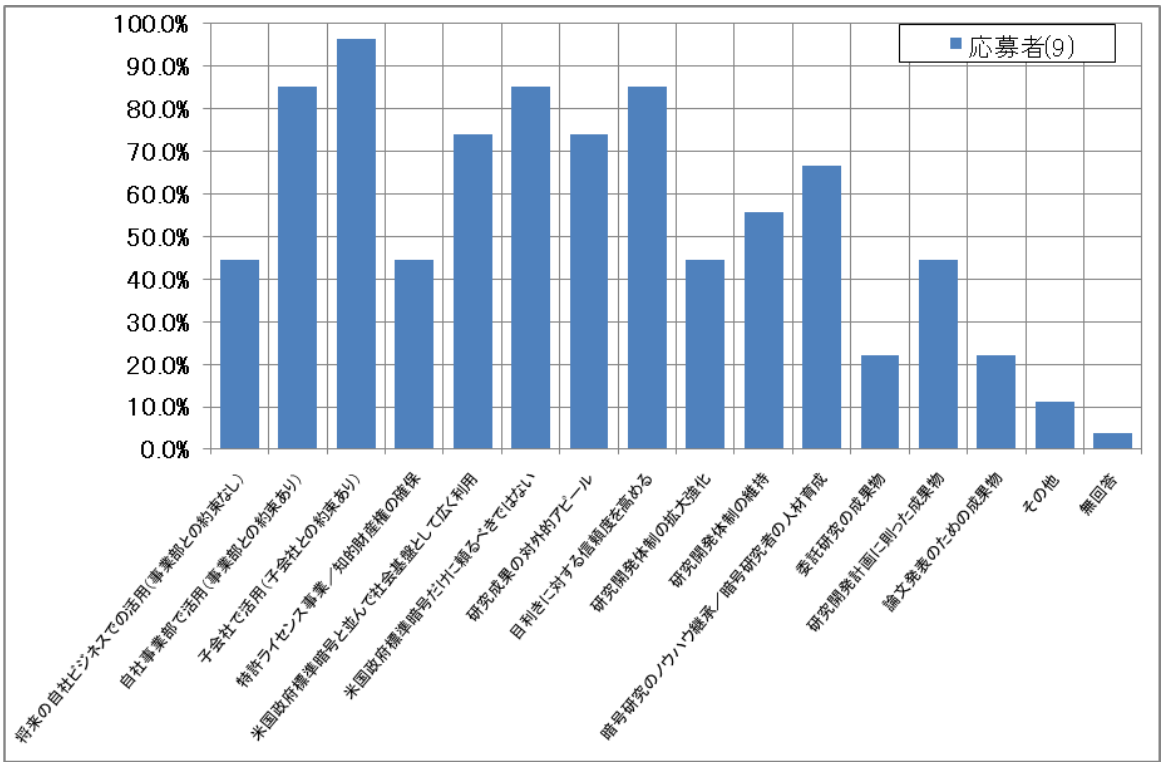
● 今後、電子政府推奨暗号である国産暗号を暗号搭載製品・システムに採用するか？



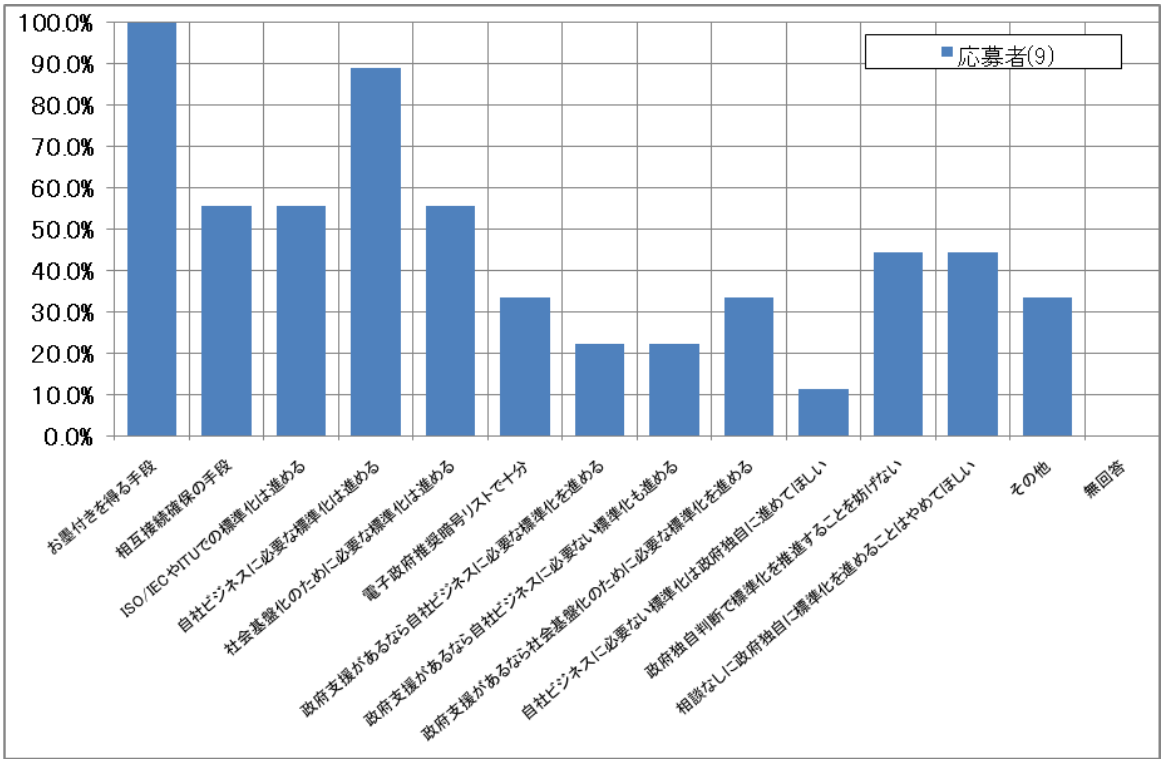
● 今後、電子政府推奨暗号である国産暗号を暗号搭載製品・システムに採用するために必要と考える条件は何か？



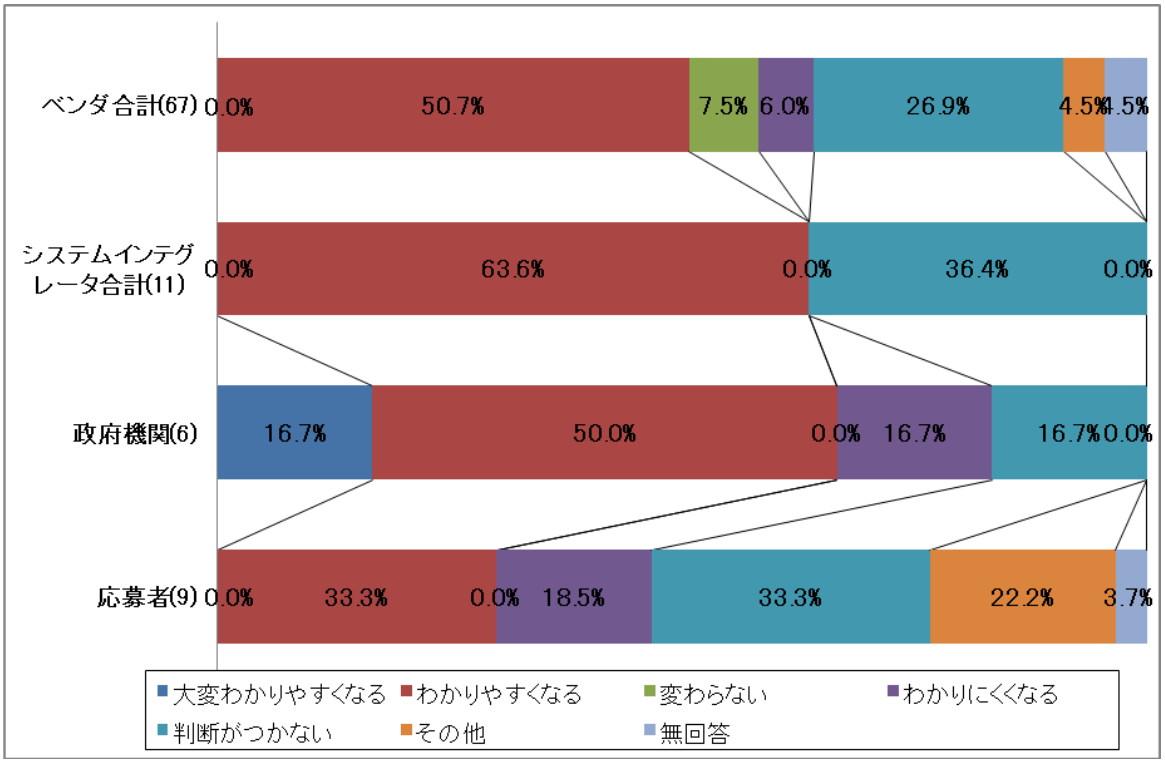
● 提案暗号の開発目的は何か？



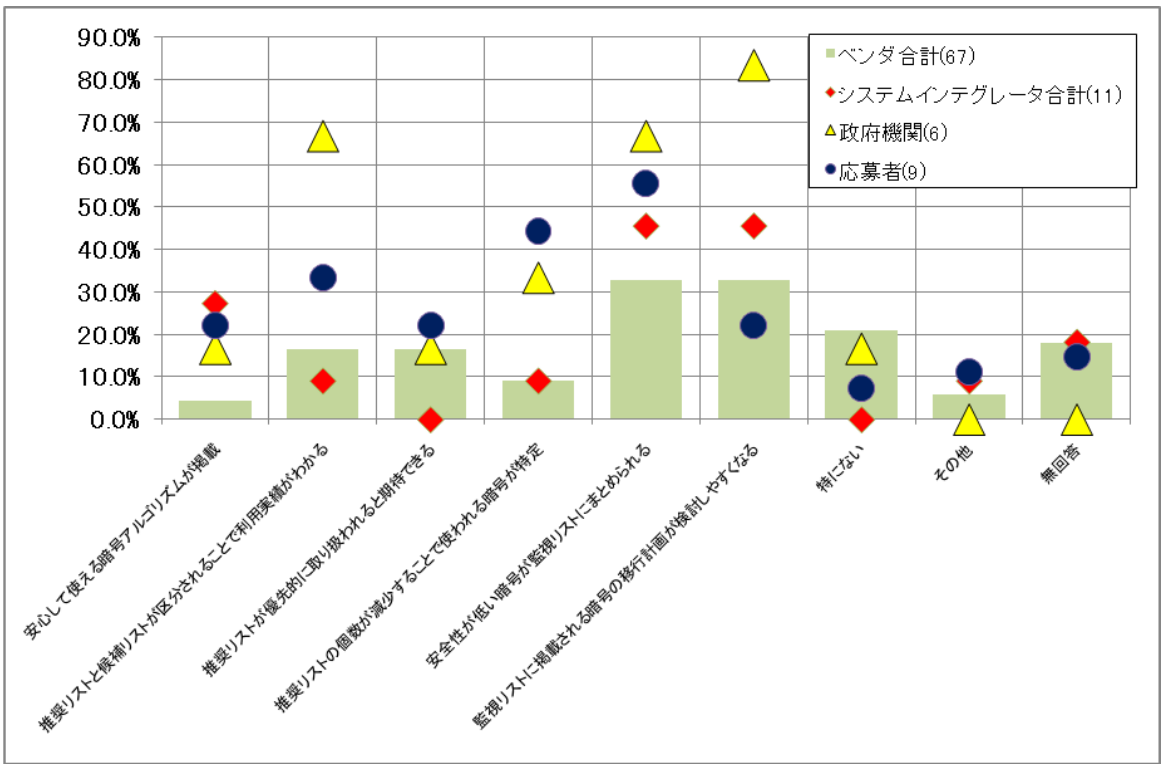
● 提案暗号の標準化を進める目的は何か？



● 次期リストの位置づけは分かりやすくなるか？



● 次期リストがよくなりそうと感じる点はどこか？



発行日　2011 年 6 月 20 日　第 1 版
発行者
・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
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）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME, BUNKYO-KU
TOKYO, 113-6591 JAPAN

・〒184-8795
東京都小金井市貫井北四丁目 2 番 1 号
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
セキュリティ基盤研究室、セキュリティアーキテクチャ研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI, KOGANEI
TOKYO, 184-8795 JAPAN