CRYPTREC Report 2011

平成 24 年 3 月

独立行政法人情報通信研究機構
独立行政法人情報処理推進機構

「暗号運用委員会報告」

目次

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 2011 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。

今年度の暗号運用委員会では、暗号技術検討会にて意見集約された「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」するとの方針の趣旨を踏まえ、次期電子政府推奨暗号リストに選定するために用いる選考基準案の検討、及び、選定された推奨暗号技術の利用が促進されるような取り組み方法についての検討を主に実施した。

具体的には、次期電子政府推奨暗号（特に国産暗号）の普及展開に対する国としてのバックアップが効果的に進むようにするために、「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）」といった様々な評価項目の視点から評価・選定するフレームワークを取りまとめた。本成果は、暗号技術検討会の審議を経て、総務省及び経済産業省に報告されている。

来年度は、年度末の次期リスト策定に向け、次期推奨暗号リストに掲載する暗号技術の選定ルールについてさらに精緻化し、具体的な選考基準値案を上期に確定するとともに、製品化や利用実績、標準化等についての利用実績調査を実施する予定である。

また、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の調査・検討、さらには、国産暗号の利用促進が図られるような取組や、次期 CRYPTREC 暗号リスト（仮称）策定に伴う暗号学界への影響と対策等についても検討する予定である。

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　松本 勉

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 GPKI1 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 2011 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選定のための選考基準案の検討結果を記述した。

2010 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。

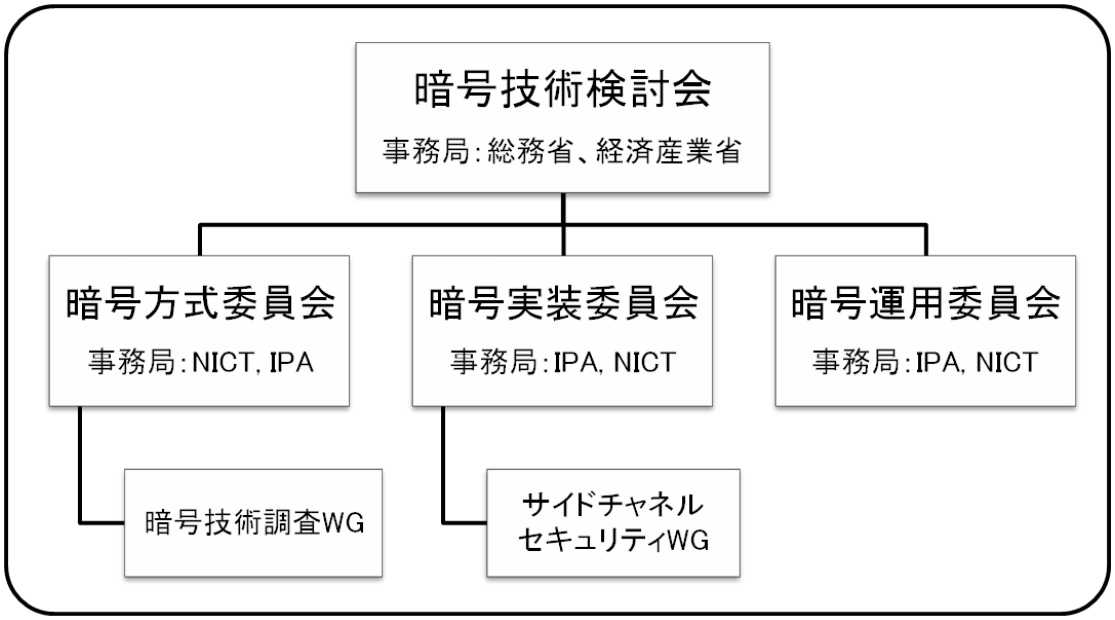


図 1　2011 年度の CRYPTREC の体制

委員名簿

暗号運用委員会 （2012 年 3 月現在）

委員長	松本　勉	横浜国立大学大学院　環境情報研究院　教授
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	木村　道弘	一般財団法人日本情報経済社会推進協会（JIPDEC） 電子情報利活用推進部　主席研究員
委員	近藤　潤一	独立行政法人情報処理推進機構 技術本部セキュリティセンター 情報セキュリティ認証室 JCMVP チーム　次長
委員	佐藤　直之	日本ベリサイン株式会社　社長室　主席研究員
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	一般社団法人 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　教授
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 コンサルティングシステムズエンジニア
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　開発部　主席研究員
委員	前田　司	EMC ジャパン株式会社　RSA 事業本部　本部長
委員	松尾　真一郎	独立行政法人情報通信研究機構 ネットワークセキュリティ研究所 セキュリティアーキテクチャ研究室　室長
委員	山口　利恵	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 セキュリティ基盤技術研究チーム　研究員

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　（2011 年 6 月まで）
福永　利徳	内閣官房情報セキュリティセンター　（2011 年 7 月より）
今福　健太郎	内閣官房情報セキュリティセンター　（2011 年 6 月より）
根本　農史	内閣官房情報セキュリティセンター　（2011 年 6 月まで）
中山　慎一	内閣官房情報セキュリティセンター　（2011 年 7 月より）
松宮　志麻	総務省　行政管理局

水野　伸太郎　　総務省　情報流通行政局　(2011 年 7 月まで)
飯田　恭弘　　総務省　情報流通行政局　(2011 年 7 月より)
佐々木　信行　　総務省　情報流通行政局　(2011 年 9 月まで)
鮫島　清豪　　総務省　情報流通行政局　(2011 年 9 月より)
谷岡　大祐　　総務省　情報流通行政局　(2011 年 7 月まで)
樋口　有二　　総務省　情報流通行政局　(2011 年 7 月より)
荒木　美敬　　外務省　大臣官房
新谷　祐司　　外務省　大臣官房
日高　隆　　経済産業省　大臣官房
町田　昇　　経済産業省　大臣官房
渡邊　孝治　　経済産業省　大臣官房
山中　豊　　経済産業省　産業技術環境局
山田　安秀　　経済産業省　商務情報政策局　(2011 年 7 月まで)
江口　純一　　経済産業省　商務情報政策局　(2011 年 7 月より)
福田　賢一　　経済産業省　商務情報政策局　(2011 年 7 月より)
森川　淳　　経済産業省　商務情報政策局
池西　淳　　経済産業省　商務情報政策局　(2011 年 4 月まで)
守山　速飛　　経済産業省　商務情報政策局　(2011 年 5 月より)
佐藤　史生　　防衛省　技術研究本部
岡野　孝子　　警察大学校　警察情報通信研究センター　(2012 年 2 月より)

事務局

独立行政法人情報処理推進機構　技術本部　セキュリティセンター
矢島　秀浩　(2011 年 7 月まで)
笹岡　賢二郎　(2011 年 7 月より)
山岸　篤弘
近澤　武
神田　雅透
大熊　建司
小暮　淳
恵本　健亮
鈴木　幸子

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
高橋　幸雄
近藤　玲子　(2011 年 7 月まで)

沼田　文彦　(2011 年 9 月より)
田中　秀磨　(2011 年 12 月まで)
大久保　美也子
蓑輪　正
野島　良
黒川　貴司
金森　祥子
多賀　文吾
側高　幸治

第 1 章　2011 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

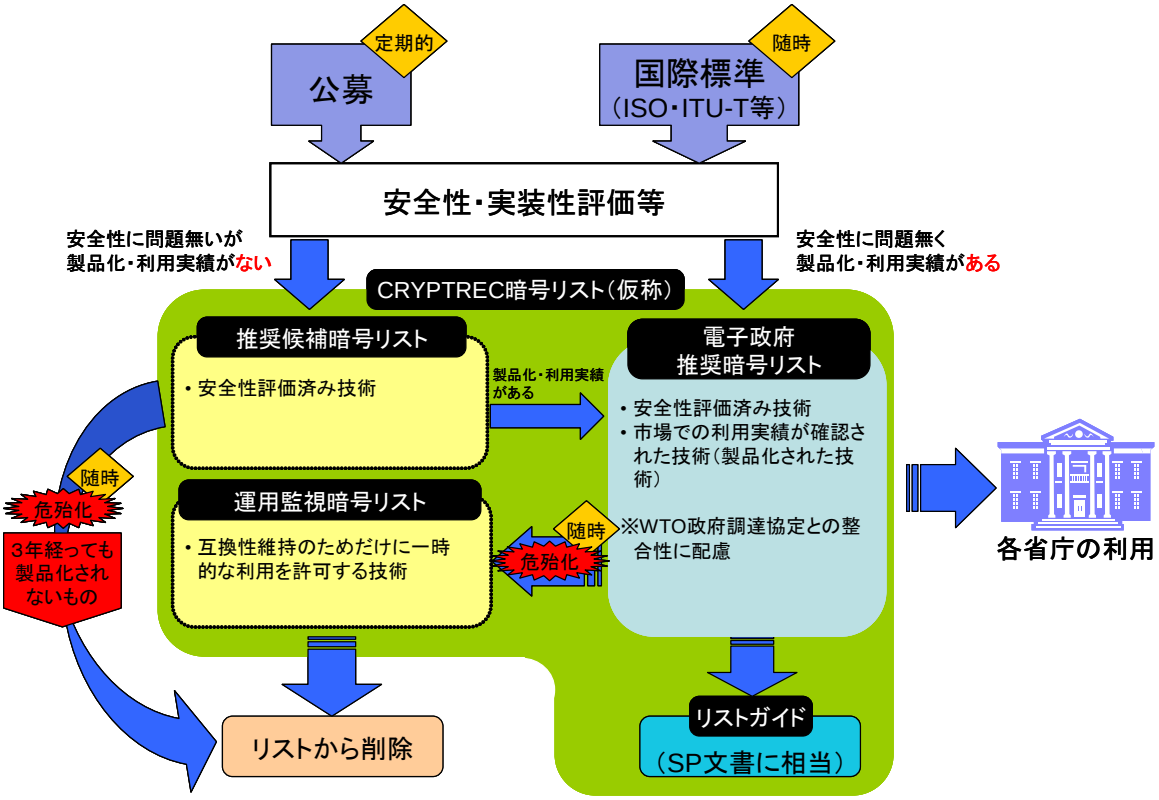
暗号技術に対する解析・攻撃技術の高度化や新たな暗号技術の開発の進展に伴い、暗号技術の危殆化及び移行対策等を含めた、適切な暗号技術の選択を支援するため、CRYPTREC では、2012 年度末の電子政府推奨暗号リストの改訂（以下、「次期リスト」という）に向けた検討を行っているところである。

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（図 2)。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。

2010 年度の暗号運用委員会では、次期リストの位置づけを明確化するために、「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等についてとりまとめを行った。この活動報告をもとに、2011 年度第 1 回暗号技術検討会にて審議を行った結果、次期リストに求める役割としては、以下の目標を実現する方向で今後の検討を進めるよう、意見集約が行われた（表 1)。

表 1　暗号技術検討会での意見集約結果

次期リストに求める役割の概要		選定意図	次期リスト例
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	米国政府標準暗号＋国産暗号(1 or 少数)



【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】

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】

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。

図 2　新しい電子政府推奨暗号リストの構成

2011 年度の暗号運用委員会では、暗号技術検討会での上記方針を踏まえ、次期リストの実運用における方向性を具体化するための必要な検討を行った。具体的には、2012 年度に電子政府推奨暗号を選定するために用いる選考基準案の検討、及び、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の検討を主に実施した。

以下に、2011 年度の暗号運用委員会の活動内容について報告する。

1.1.2 今年度の活動指針

2011 年度第 1 回暗号技術検討会において承認された 2011 年度暗号運用委員会活動計画に基づき、本年度の暗号運用委員会の審議を行った。

特に、(1)の電子政府推奨暗号選定のための選考基準については、実際の電子政府推奨暗号の選定作業が本格化する前に明らかにしておく必要があるため、本年度の最重要項目として検討を行い、選考基準案の考え方を取りまとめた。

(1) 電子政府推奨暗号選定のための選考基準案の検討

次期 CRYPTREC 暗号リスト（仮称）の方向性を踏まえ、2012 年度に電子政府推奨暗号を選定するために用いる選考基準案を検討する。

(2) 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。

(3) 運用監視暗号リストへの遷移要件に関する基準の検討

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、必要に応じて検討する。

(4) その他

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、必要に応じて、継続して検討する。

また、2012 年度に向けて、推奨候補暗号リストの活用方法、次期 CRYPTREC 暗号リスト（仮称）策定に伴う暗号学界への影響と対策、等に関する予備検討を開始する。

1.1.3 今年度の委員会の開催状況

2011 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 2 のとおり。

表 2　2011 年度暗号運用委員会概要

回	開催日時	主な議題
第 1 回	2011 年 9 月 21 日	●暗号運用委員会活動計画について ●次期電子政府推奨暗号の選考基準案の検討について①
第 2 回	2011 年 11 月 18 日	●次期電子政府推奨暗号の利用促進取り組みへの検討について ●次期電子政府推奨暗号の選考基準案の検討について②
第 3 回	2012 年 1 月 27 日	●次期電子政府推奨暗号の選考基準案の検討について③
第 4 回	2012 年 2 月 24 日	●次期電子政府推奨暗号の選考基準案の検討について④
第 5 回	2012 年 3 月 9 日	●暗号運用委員会の活動報告（2011 年度 CRYTREC 合同委員会）

1.2　成果概要

1.2.1　次期電子政府推奨暗号リストに掲載する暗号技術選定の基本的考え方

暗号技術検討会にて意見集約された「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」するとの方針の趣旨について、2011 年度暗号運用委員会では、「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）」の見通しを考慮した、以下の 2 つの観点で次期推奨暗号リストに掲載する暗号技術を選定することと解釈した。

その解釈を前提として、電子政府推奨暗号選定のための選考基準案の検討を進めた。

【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 3 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

1.2.2　次期電子政府推奨暗号選定のための選考基準案の考え方

1.2.1 節の観点(i)及び観点(ii)の考え方に沿い、次期推奨暗号リストに含める暗号技術を以下の考え方により選定する（図 3）。詳細については第 2 章を参照されたい。

なお、本選考基準案の考え方については、2011 年度第 2 回暗号技術検討会で承認された。

- 観点(i)により選定される可能性がある暗号技術は、評価 A において「現在の利用実績が十分である」と判断されたものである（選定ルート①を通るもの）
- 観点(ii)により選定される可能性がある暗号技術は、評価 B により「現在の利用実績は十分とは言えないが、今後の利用促進の可能性が高い」と判断されたものである（選定ルート②③を通るもの）

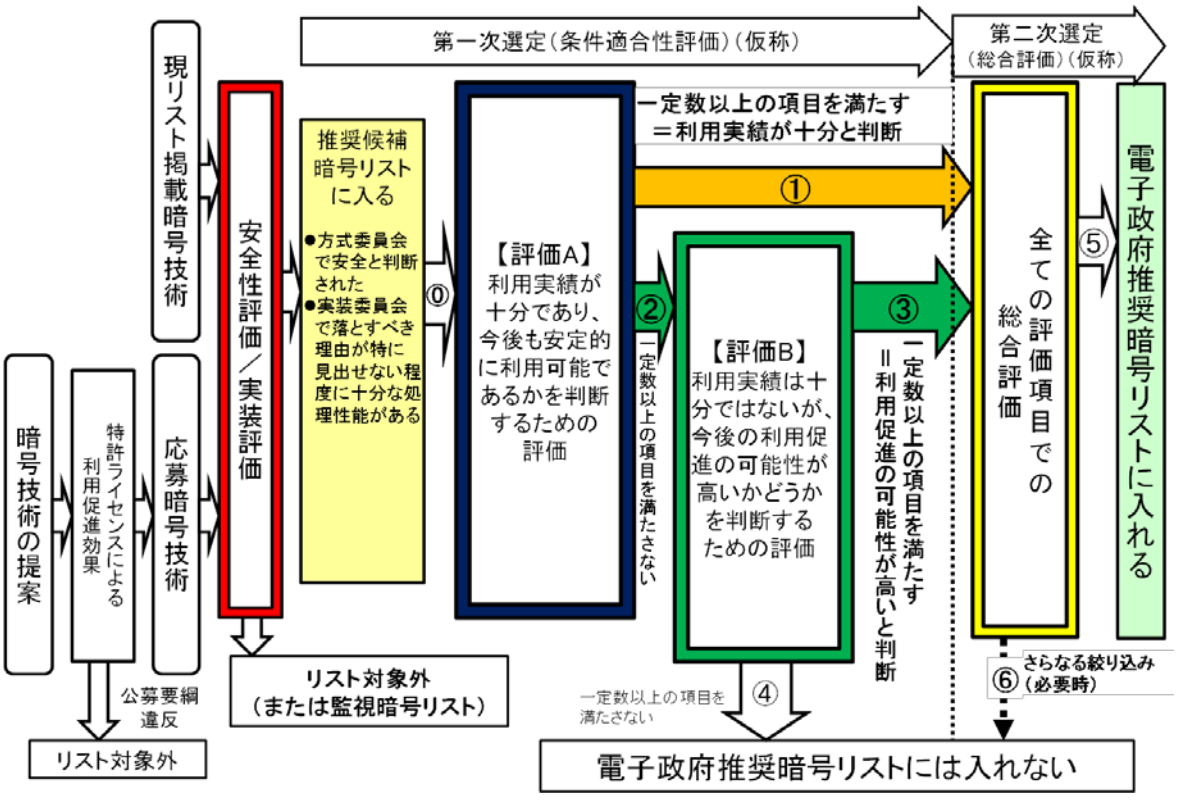


図 3　選定ルールのフレームワーク

評価 A で用いる「利用実績が十分であり、今後も安定的に利用可能であるかを判断するための評価」を行うために、表 3 に示す 4 つの評価項目を用いる。各々の評価項目について設定された選考基準を満たしているかを判断し、4 つの評価項目のうち一定数以上の項目が基準を満たしていれば「現在の利用実績が十分である」と判断する。

表 3　評価 A での評価項目及び選考基準の基本的な考え方

評価項目	選考基準の基本的な考え方
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）

現時点では、各評価項目での選考基準の“具体的な基準値”は審議中であるので、選考基準を決めるにあたっての“基本的な考え方”を示しておく。なお、選考基準の基本的な考え方としては、第一次選定（条件適合性評価）（仮称）段階（評価 A 及び評価 B）において出来る限り次期リストに掲載される暗号技術の個数を絞り込むこととし、そのための明示的な基準を“選考基準”として設定する。その意図は以下のとおりである。

- 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ようにする
- 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、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート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

同様に、評価 B で用いる「利用実績は十分ではないが、今後の利用促進の可能性が高いかどうかを判断するための評価」を行うために、評価 A で用いた評価項目 4 つに加え、表 4 に示す 4 つの評価項目を追加する。つまり、評価 B においては、8 つの評価項目のうち一定数以上の項目が基準を満たしていれば「今後の利用促進の可能性が高い」と判断する。

表 4　評価 B での評価項目及び選考基準の基本的な考え方

<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">評価項目</td><td>選考基準の基本的な考え方</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>

第二次選定（総合評価）においては、表 5 に示す各評価項目に決められた加点基準をもとに総合評価を行うことする。その際、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート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ために、「利用促進が図られると期待される根拠」に該当する 4 つの評価項目については「選定ルート②③で第一次選定を通過した暗号技術」に対してのみ加点対象とする。

表 5　総合評価の基本的な考え方

評価項目		選定ルート①で通過	選定ルート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	－	○
	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	－	○

凡例：　○：加点対象　　－：加点対象としない

1.2.3　利用実績調査の基本的考え方

2012 年度には、評価 A 及び評価 B での利用実績評価の基礎データとなる利用実績調査を実施する予定としている。利用実績調査の基本的考え方は、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踏襲するものとする。具体的には以下の通り。

（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

（想定調査対象数）

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

- 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

1.2.4 特許ライセンスの取り扱い

特許ライセンス条件の取り扱いについて、応募時点での公募要綱に書かれた条件とは少なからず異なる状況が発生している。そのため、本報告書及び CRYPTREC シンポジウム 2012 等で特許ライセンスの取り扱いについて説明した後、必要があれば応募者が特許ライセンスの宣誓を変更できるようにすべきである。

そこで、暗号運用委員会としては、2012 年 9 月 30 日時点の特許ライセンス宣誓により評価を実施することとし、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ことが妥当と判断した。

1.2.5　電子政府推奨暗号の利用促進体制の検討

次期電子政府推奨暗号リストに掲載する国産暗号を絞り込んだとしても本当に使われるようになるのかという課題がある。

そのため、本年度の暗号運用委員会では、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する目的を達成するために、次期電子政府推奨暗号、とりわけ国産暗号の利用促進が図られるような取り組みを検討するにあたって考慮すべき観点と論点の洗い出しを行った。次年度、論点の検討を進めていくこととした。

(1) 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。

論点：主導権をとるといった場合、いつ頃（達成時期）までにどのような状態を達成すべきゴールとして目指すべきかについて明らかにする必要がある。

(2) 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。

論点：調達コストに大きく跳ね返らないレベルで、十分な制約をかけて国産暗号を使わせる土壌を少しずつ作っていく方策について検討する必要がある。

論点：米国政府標準暗号といえども米国内の主要ベンダの支持が得られず全く普及しなかったものもあることを考慮すれば、日本で決定したことに対して主要ベンダの支持が得られるようにするための方策について検討する必要がある。

(3) 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。

論点：標準化を手掛けると専門的に人を長期間張り付ける必要があり、企業負担が大きいなか、今後の標準化・規格化への活動主体として誰が何を担うべきかについて検討する必要がある。

1.3　CRYPTREC シンポジウム 2011 の開催状況

1.3.1　プログラムの概要

日　時　：　2012 年 3 月 9 日（金）10：00～15：45
場　所　：　秋葉原 UDX
主　催　：　独立行政法人情報通信研究機構、独立行政法人情報処理推進機構
共　催　：　総務省、経済産業省
参加人数：　205 名

表 6　プログラム

3 月 9 日(金)		
時間	内容	
10:00	開会挨拶	
10:10	暗号方式委員会報告	応募暗号技術や現リストに掲載されている暗号技術に対する安全性評価の進行状況についての説明
10:40	暗号実装委員会報告	応募暗号技術や現リストに掲載されている暗号技術に対する実装性評価の進行状況についての説明
11:40	昼休み	
12:40	暗号運用委員会報告	次期電子政府推奨暗号選定にあたっての考え方、並びに選定基準の検討状況についての説明
13:55	休憩	
14:10	ネットワークセキュリティについて 篠田陽一教授（北陸先端技術大学院大学）	
14:55	情報セキュリティ人材育成について 今井秀樹教授（中央大学）	
15:40	閉会挨拶	

1.3.2　暗号運用委員会報告に対する質疑応答

2011 年度暗号運用委員会での活動成果報告に対する質疑応答は以下のとおりである。

Q：推奨暗号に選定した国産暗号を世界に売り出したいという方針に対して、実際の選定の考え方としては先に市場で普及してきたものを推奨暗号として認めるというように見える。方向性や思いと実際のやり方に違いがあるのではないか？

A：米国とは異なり、現状の日本の体制では先に暗号を決めて使わせるというのは困難。また、現在のように数も多いと、全部を同じようにというわけにもいかない。そのため、先に決めて売り出すのは難しく、支援することによって今後の展開が期待できるような、ある程度広まっているものを推さざるを得ない現状を反映している。

Q：ある程度実績が必要ならば推奨暗号に選定されるメリットがよくわからない。どこまでやれば政府が推すかを言ってほしい。

A：政府の支援方法などは今後ロードマップで検討すべき事項であると認識している。

Q：日本の CC（コモンクライテリア）認証では、推奨暗号リストに入っている暗号を利用することが事実上必須的条件になっている。推奨暗号を国が推すスタンスとして今回検討している選定基準は、調達サイドのスタンスから考えた基準か、それとも暗号開発促進も含む産業政策としてのスタンスから考えた基準か？

A：現在、電子政府推奨暗号リストの取り扱いについては、内閣官房情報セキュリティセンター（NISC）が発行している政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準で記載されており、今後もこの方針から大きく変わることはない。しかし、次期リストでは 3 分割されるため、調達基準として実際にどのような記述修正を行うかについては、NISC、総務省、経済産業省との協議により決まっていく。

なお、リスト改訂にあたっては広い意味では産業政策も含むスタンスだが、暗号アルゴリズム開発を促進するのか、それとも暗号の応用分野にシフトさせていくのかという視点の議論はある。

Q：現在の推奨暗号リストに載っている既存暗号と今回公募された新規暗号とで同じ基準で評価されるのか？利用実績は時間が経てば増えていくことを考えれば、別の基準のほうが妥当ではないのか。

A：使う評価基準は同じ。ルート①（利用実績が十分）とルート②③（今後の利用促進が期待できる）との二つの選定ルートを設けることにより、利用実績が不利な新規暗号であっても、ルート②③を考慮することで推奨暗号に値すると判断されるものは選定されるようになっている。

Q：評価の透明性をあげるための施策は？

A：評価に利用したデータは年度末報告書（CRYPTREC Report）で公開する。

Q：アピールポイントについて、「誰がアピール」して「誰が採点」するのか？

A：特に「誰がどのようにアピールするか」という視点を決めて言っているわけではない。例えば「どこで使われているの？」という質問に対して、「どこそこで使われている」といえばある程度の利用実績が理解できる、という意味である。

Q：選定基準の線引きを誰がどう決めるのか？

A：運用委員会で選定基準案を作る。その後は、他委員会の評価結果を含めてリスト作成の過程で反映され、暗号技術検討会の承認を経たうえで、総務省と経済産業省が決めたリスト案に対するパブリックコメントという手順を踏む。

一般の人がコメントできるのはリスト案に対するパブリックコメントの時である。

Q：候補暗号は一定期間内に採用されないと削除されることになっている。その際、非公開での利用実績がカウントされずに候補暗号リストから削除される可能性があるのならば、候補暗号リストからの採用に二の足を踏む。候補暗号については、利用実績の判断だけでいきなり削除するような運用はやめてほしい。

A：今回の利用実績調査の結果で候補暗号からのリスト削除を行うことはない。監視リストを含めて、文言については今後議論し、多少変えるかもしれない。

Q：評価 A において、国際標準化を利用実績としてカウントしないのはなぜか？政府系システムに入るためには WTO/TBT 協定等の関係で国際標準化は重要なはずである。

A：国際標準化は WTO/TBT 協定等の関係で重要であることは確かであるが、本当に使われているのであれば、国際標準化後に政府系システム規格やインターネットでの規格等でも採用されているはずである。そこで、政府系システム規格や民間メジャー規格での利用実績からでも拾えることを考慮し、国際標準化を評価 A に含める必要はないと判断した。

なお、評価 B では国際標準化の利用実績もカウントされる。

Q：各社は様々な目的（CRYPTREC は目的の一つにすぎない）で多様な暗号を開発しているのに、日本として一つの暗号を選定し特許無償化やオープンソースを求めるのは、ビジネスモデルの変更を強要し、民業を圧迫するのではないか。

A：電子政府推奨暗号を決めるそもそもの目的が、ある企業のビジネスのためのお墨付きを与えるためなのか、政府が安全に安く調達しやすい製品を選択できるようにするためなのか、という議論を経て、後者に舵を切った。

特許無償化やオープンソースを求めるのは、製品開発の競争を促進し、調達コストを下げるための環境整備の一環。ただし、それらが電子政府推奨暗号に選定されるための必須条件というわけではない。

Q：選考基準が公表されたのは今日と考えてよいか？

A：はい。

Q：推奨暗号選定までのタイムスケジュールを教えてほしい。

A：来年度上期にデータを揃え、年末・年明けまでにリスト案を完成させ、パブリックコメントを実施する予定。今後、8～9 ヶ月かけて実施する。

第2章　次期電子政府推奨暗号リストに掲載する暗号技術選定のための選考基準案

2.1　次期電子政府推奨暗号技術選定のための評価項目

2.1.1　次期電子政府推奨暗号リストに掲載する暗号技術選定の基本的考え方

2010 年度の暗号運用委員会での活動報告をもとに、2011 年度第 1 回暗号技術検討会にて審議を行った結果、次期リストに求める役割としては、以下の目標を実現する方向で今後の検討を進めるよう、意見集約が行われた（表 1)。

表 1　暗号技術検討会での意見集約結果（再掲）

次期リストに求める役割の概要		選定意図	次期リスト例
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	米国政府標準暗号＋国産暗号(1 or 少数)

暗号技術検討会にて意見集約された「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」するとの上記方針の趣旨について、2011 年度暗号運用委員会では、「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)」の見通しを考慮した、以下の 2 つの観点で次期推奨暗号リストに掲載する暗号技術を選定することと解釈した。

その解釈を前提として、電子政府推奨暗号選定のための選考基準案の検討を進めた。

【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 3 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

2.1.2 次期電子政府推奨暗号技術選定に向けた評価項目の詳細

2.1.1 節で記した観点(i)及び観点(ii)の考え方に則った暗号技術を次期推奨暗号リストに選定するために、どのような意図をもった評価項目を含めるべきかについての検討を行った。その際、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」における「暗号アルゴリズムの市場性」の調査結果、ならびに 2010 年度に暗号運用委員会が実施した「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」の調査結果等も参考にした。

検討の結果、以下の評価観点を踏まえ、最終的に 17 個の評価項目を選定した。具体的な評価項目並びに評価意図は表 7 にまとめたとおりである。

- **「技術的側面」での評価観点**

  技術的に優れているかどうかを評価する
  - 安全性
  - 処理性能
- **「現状の調達容易性（利用実績）」での評価観点**

  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を評価する
  - 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」での評価観点**

  主に観点(ii)の意味での利用促進が図られると今後期待される根拠を満たしているかどうかを評価する
  - 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

表 7　評価項目及び評価意図のまとめ

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
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

2.2　次期電子政府推奨暗号技術選定のフレームワーク

2.2.1　次期電子政府推奨暗号技術選定ルールの基本的考え方

2.1.2 節で選定した全 17 個の評価項目における評価結果をもとに、次期推奨暗号リストに掲載する暗号技術を選定することになる。そこで、2.1.1 節で示した観点(i)及び観点(ii)の考え方に沿い、次期推奨暗号リストに掲載する暗号技術を以下の考え方により選定するフレームワークを検討した（図 3）。

- 観点(i)により選定される可能性がある暗号技術は、評価 A において「現在の利用実績が十分である」と判断されたものである（選定ルート①を通るもの）
- 観点(ii)により選定される可能性がある暗号技術は、評価 B により「現在の利用実績は十分とは言えないが、今後の利用促進の可能性が高い」と判断されたものである（選定ルート②③を通るもの）

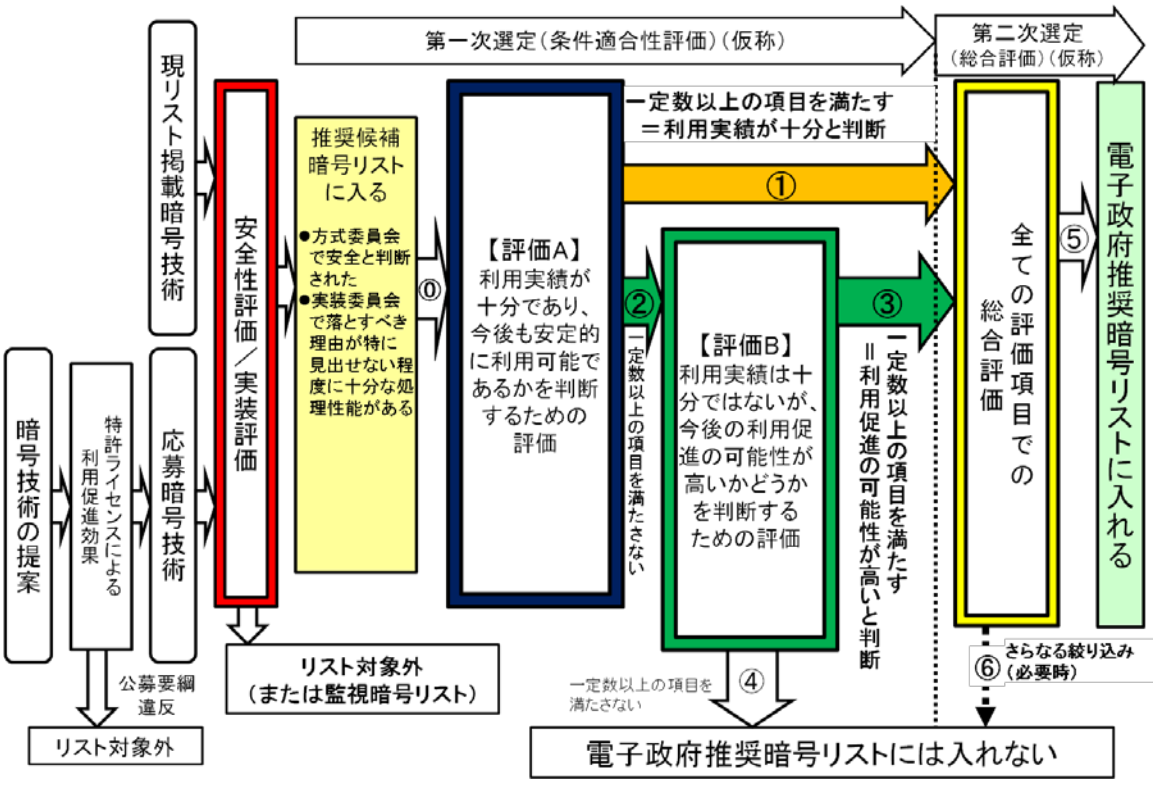


図 3　選定ルールのフレームワーク（再掲）

その際、次期推奨暗号リストが頻繁に更新されるような選定ルールであると政府調達の場面で混乱が生じる懸念があるため、ある程度の期間は固定して安定的に利用できることを想定する必要がある。また、2012 年度の改訂では次期推奨暗号リストに掲載されなかった暗号技術や今後新規に開発される暗号技術が、次々回以降の改訂において電子政府推奨

暗号リストを目指す場合にどのような普及活動を行っておくべきかの指針を与えることにも留意した。

このフレームワークでは、評価 A にて、「利用実績が十分であり、今後も安定的に利用可能であるかを判断するための評価」を行うための評価項目について各々設定された選考基準を満たしているかを判断し、一定数以上の評価項目が基準を満たしていれば「現在の利用実績が十分である」と判断する。

評価 B でも、「利用実績は十分ではないが、今後の利用促進の可能性が高いかどうかを判断するための評価」を行うための評価項目について同様の考え方を行い、評価 B における評価項目のうち一定数以上の項目が基準を満たしていれば「今後の利用促進の可能性が高い」と判断する。

なお、各評価項目に設定する選考基準を決めるにあたっての基本的な考え方としては、第一次選定（条件適合性評価）（仮称）段階（評価 A 及び評価 B）において出来る限り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こととし、そのための明示的な基準を“選考基準”として設定する。その意図は以下のとおりである。

- 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ようにする
- 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、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート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

第二次選定（総合評価）においては、各評価項目に決められた加点基準をもとに総合評価を行うことする。その際、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート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ために、「利用促進が図られると期待される根拠」に該当する 4 つの評価項目については「選定ルート②③で第一次選定を通過した暗号技術」に対してのみ加点対象とする。

2.2.2 第一次選定（条件適合性評価）（仮称）の評価 A における選考基準案の基本的考え方

評価 A で用いる「利用実績が十分であり、今後も安定的に利用可能であるかを判断するための評価」を行うための評価項目の対象としては、表 7 における「現状での利用実績」における 9 項目が該当する。これらについて、評価 A での選考基準に採用するか否か、採用するとすればどのような選考基準案とすべきかについて検討を行った。

検討の結果、9 項目中 4 項目について評価 A での選考基準として採用することとし、合わせて選考基準の基本的な考え方を取りまとめた（表 8）。つまり、評価 A においては、表 8 の 4 つの評価項目について設定された選考基準を満たしているかを判断し、一定数以上の評価項目が基準を満たしていれば「現在の利用実績が十分である」と判断する。

なお、基本的な考え方における意図は以下のとおりである。

- 十分な利用実績があると判断する以上は「一定数以上の採用実績」は必要である
- コスト低減の観点からは、提案会社・グループ会社以外の企業を含めた、複数企業から調達できるようにすべきである
- オープンソースプロジェクトで採用された暗号技術が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
- 規格化については、最終承認待ちまで来ればいずれ規格化されるが、それ以前の状態では規格化されないまま終わる可能性がある

表 8　評価 A での評価項目及び選考基準の基本的な考え方

評価項目	選考基準の基本的な考え方
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）

また、評価 A での選考基準に採用しなかった 5 項目については、採用しなかった理由を表 9 に記す。

表 9　評価 A での選考基準に採用しなかった理由

評価項目	採用しなかった理由
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
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
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）
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

2.2.3　第一次選定（条件適合性評価）（仮称）の評価 B における選考基準案の基本的考え方

評価 B で用いる「利用実績は十分ではないが、今後の利用促進の可能性が高いかどうかを判断するための評価」を行うために、評価 A で用いた評価項目 4 つに加え、表 7 に示す「利用促進が図られると期待される根拠」の 4 つの評価項目を追加する（表 10）。つまり、評価 B においては、表 10 の 8 つの評価項目のうち一定数以上の項目が基準を満たしていれば「今後の利用促進の可能性が高い」と判断する。

評価 B における選考基準の基本的考え方は表 10 に示すとおりであり、基本的な考え方における意図は以下のとおりである。

- 利用促進として様々な後押しを図るのであれば特許ライセンス条件による制約は極力除去すべきである
- 技術的アピールポイントを認める項目が一つもないと採用実績があるものしか選考基準を満たすことができず、新規に開発した暗号技術ほど不利な状況に置かれるので、何らかの対策が必要である
- 利用実績が全くなく、普及に向けた活動や条件が整っていないものは今後も利用促進の可能性が高くないと考えられるため、そのことを判断するための基準として「一定数の採用実績」は必要。ただし、評価 A での「一定数」の基準よりも低めの基準とすることで、評価 A と評価 B での採用実績等の差を考慮する

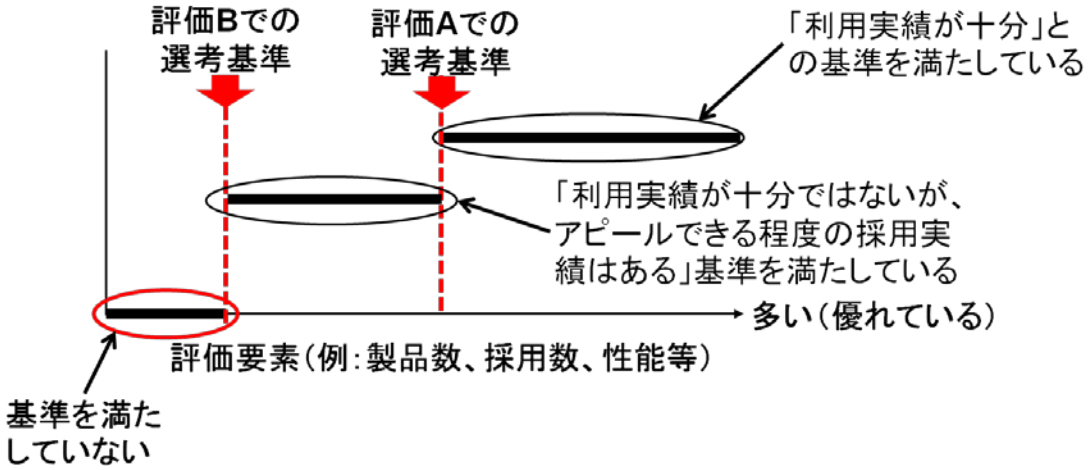


表 10　評価 B での評価項目及び選考基準の基本的な考え方

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			
評価項目			選考基準の基本的な考え方
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

2.2.4　第二次選定（総合評価）（仮称）における基本的な考え方

第二次選定（総合評価）においては、表 7 に示す各評価項目に決められた加点基準をもとに総合評価を行うことする。その際、「選定ルート①で第一次選定を通過した暗号技術」と「選定ルート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ために、「利用促進が図られると期待される根拠」に該当する 4 つの評価項目については「選定ルート②③で第一次選定を通過した暗号技術」に対してのみ加点対象とする。

総合評価の加点基準の基本的な考え方は、評価項目ごとに評価要素（例：製品数、採用数、性能等）の優劣によって 1 段階から数段階の配点を割り当て、最終的にはそれらの配点の合計点により総合評価を行うことを想定している。その際、製品やシステム、規格等の重要性等による重みづけを考慮する。表 11 に総合評価の基本的な考え方をまとめる。

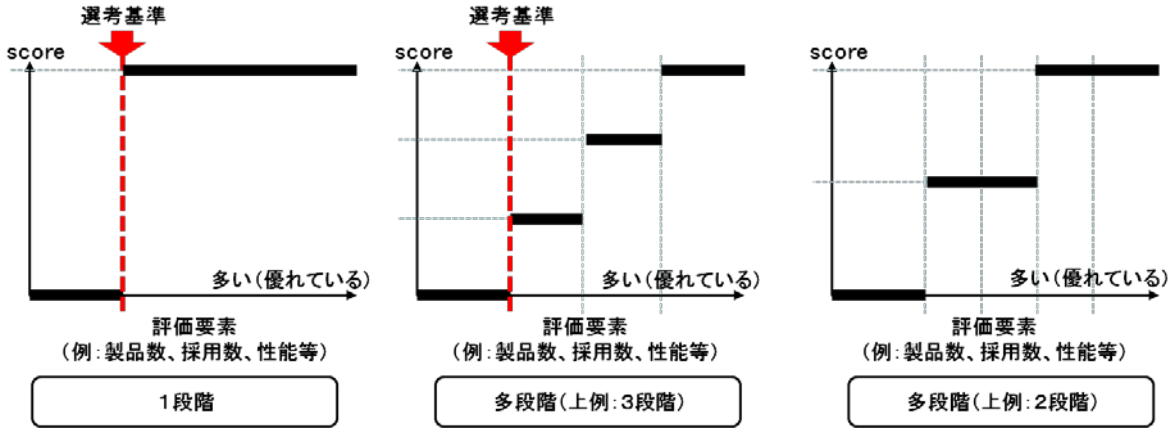


表 11　総合評価の基本的な考え方（その 1）

凡例：　○：加点対象　　－：加点対象としない

評価項目		加点基準	重みづけ	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	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		○	○
	ソフトウェア実装性能評価	暗号実装委員会に見解を求める		○	○
	ハードウェア実装性能評価	暗号実装委員会に見解を求める		○	○

表 11　総合評価の基本的な考え方（その 2）

評価項目		加点基準	重みづけ	ルート①で通過	ルート②③で通過
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	○	○
	市販製品での採用実績	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	○	○
	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	○	○
	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	○	○
	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		○	○
	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	○	○
	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	○	○

表 11　総合評価の基本的な考え方（その 3）

評価項目		加点基準	重みづけ	ルート①で通過	ルート②③で通過
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		－	○

2.2.5　利用実績調査等の基本的考え方

2012 年度には、評価 A 及び評価 B での利用実績評価の基礎データとなる利用実績調査を実施する予定としている。そのために、利用実績調査に関する調査対象や手法、特許ライセンスの取り扱い等についても検討を行った。

取りまとめた基本的考え方については、1.2.3 節及び 1.2.4 節を参照されたい。

2.3　今後の予定

2011 年度の暗号運用委員会で検討した次期推奨暗号リストに掲載する暗号技術の選定ルールについてさらに精緻化し、具体的な選考基準値案を 2012 年度上期に確定するとともに、利用実績調査を実施し、2012 年度末の次期推奨暗号リストの策定につなげていく。

また、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の調査・検討を 2012 年度下期に行う。さらに、引き続き、国産暗号の利用促進が図られるような取組や、次期 CRYPTREC 暗号リスト（仮称）策定に伴う暗号学界への影響と対策等について検討する。

発行日　2011年 5月 23日　リリース候補第1版
発行者

・〒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

・〒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