CRYPTREC Report 2012

平成 25 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

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 2012 年度活動報告である。

本年度は、CRYPTREC としても大きな節目を迎えた年度である。

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に、2002 年に策定した電子政府推奨暗号リストの改定作業が 2009 年度から実施されてきた。本年度、その改定作業が無事に完了し、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」に移行することとなった。この CRYPTREC 暗号リストは、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」及び「運用監視暗号リスト」から構成される。また、付属ドキュメントして「リストガイド」が作られている。

今年度の暗号運用委員会では、上期前半（4～7 月）に電子政府推奨暗号の選定に向けた選定ルールの精緻化の審議を行い、電子政府推奨暗号リストに掲載する暗号アルゴリズムを選定する具体的な選考基準値案を確定した。この期間は、実質的な選定作業を開始する前に選定ルールを確定させることに注力することにより、電子政府推奨暗号の選考に当たっての公平性・客観性を最大限確保するような委員会運営が行われたことを付記する。

上期後半（7～10 月）に、暗号運用委員会の助言のもと、独立行政法人情報処理推進機構（IPA）により市販製品や標準化等での採用実績についての調査が実施された。さらに、本調査結果の妥当性の確認、ならびに先に確定した選定ルールに照らし合わせた結果判定を実施した。本判定は、暗号方式委員会及び暗号実装委員会との合同委員会の審議を経て、暗号技術検討会に報告された。

また、下期には、2013 年度の CRYPTREC 体制の改組に伴って新設が計画されている暗号技術活用委員会に引き継ぐべき課題について論点整理を行った。ここで整理した検討課題はいずれも重要な課題であるので、次年度以降の暗号技術活用委員会で広く議論されることを強く期待する。

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 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 2012 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 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。

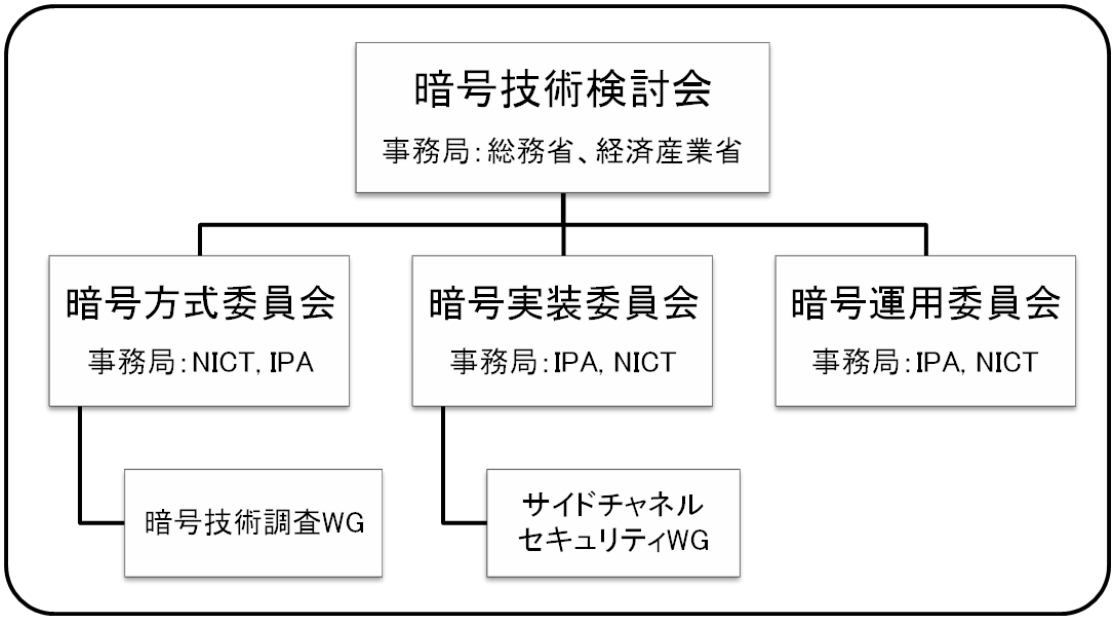


図　2012 年度の CRYPTREC の体制

委員名簿

暗号運用委員会 （2013 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　主査
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 情報ソリューション事業部　IC カードソフト開発本部 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 セキュアシステム研究部門 セキュアサービス研究グループ　研究員

オブザーバ

福永　利徳	内閣官房情報セキュリティセンター
今福　健太郎	内閣官房情報セキュリティセンター
中山　慎一	内閣官房情報セキュリティセンター
村田　莉衣奈	総務省　行政管理局
山碕　良志	総務省　情報流通行政局

上原　哲太郎　　総務省　情報流通行政局（2012 年 8 月から）
飯田　恭弘　　総務省　情報流通行政局
鮫島　清豪　　総務省　情報流通行政局（2012 年 8 月まで）
樋口　有二　　総務省　情報流通行政局（2012 年 7 月まで）
吉田　丈夫　　総務省　情報流通行政局（2012 年 8 月から）
橋本　直樹　　総務省　情報流通行政局（2012 年 10 月から）
新谷　祐司　　外務省　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（2012 年 6 月まで）
植田　勝彦　　経済産業省　大臣官房（2012 年 7 月から）
山中　豊　　経済産業省　産業技術環境局（2012 年 6 月まで）
岩永　敏明　　経済産業省　産業技術環境局（2012 年 7 月から）
上村　昌博　　経済産業省　商務情報政策局
森川　淳　　経済産業省　商務情報政策局（2012 年 11 月まで）
中谷　順一　　経済産業省　商務情報政策局（2012 年 10 月から）
守山　速飛　　経済産業省　商務情報政策局
谷口　晋一　　防衛省　技術研究本部
一藁　伸二　　警察大学校　警察情報通信研究センター

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
笹岡　賢二郎
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　ネットワークセキュリティ研究所
高橋　幸雄（2012 年 9 月まで）
平　　和昌（2012 年 10 月から）
沼田　文彦
盛合　志帆
大久保　美也子（2012 年 9 月まで）
蓑輪　正　（2013 年 1 月まで）
江村　恵太（2012 年 8 月から）

野島　良
黒川　貴司
金森　祥子
多賀　文吾
側高　幸治
八代　祐子

第 1 章　2012 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に、2002 年に策定した電子政府推奨暗号リストの改定作業が 2009 年度から実施されてきた。本年度、その改定作業が無事に完了し、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」に移行することとなった。この CRYPTREC 暗号リストは、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」及び「運用監視暗号リスト」から構成される（図 参照）。また、付属ドキュメントして「リストガイド」が作られている。

今年度の暗号運用委員会の活動内容は、CRYPTREC 暗号リストの策定に向けた最終的な審議を進めていく関係から、大きく 3 フェーズに分かれている。

- 上期前半（4～7 月）：

  2011 年度に決定した電子政府推奨暗号の選定に向けた選定ルールの精緻化の審議を行い、電子政府推奨暗号リストに掲載する暗号アルゴリズムを選定する具体的な選考基準値案を確定した。

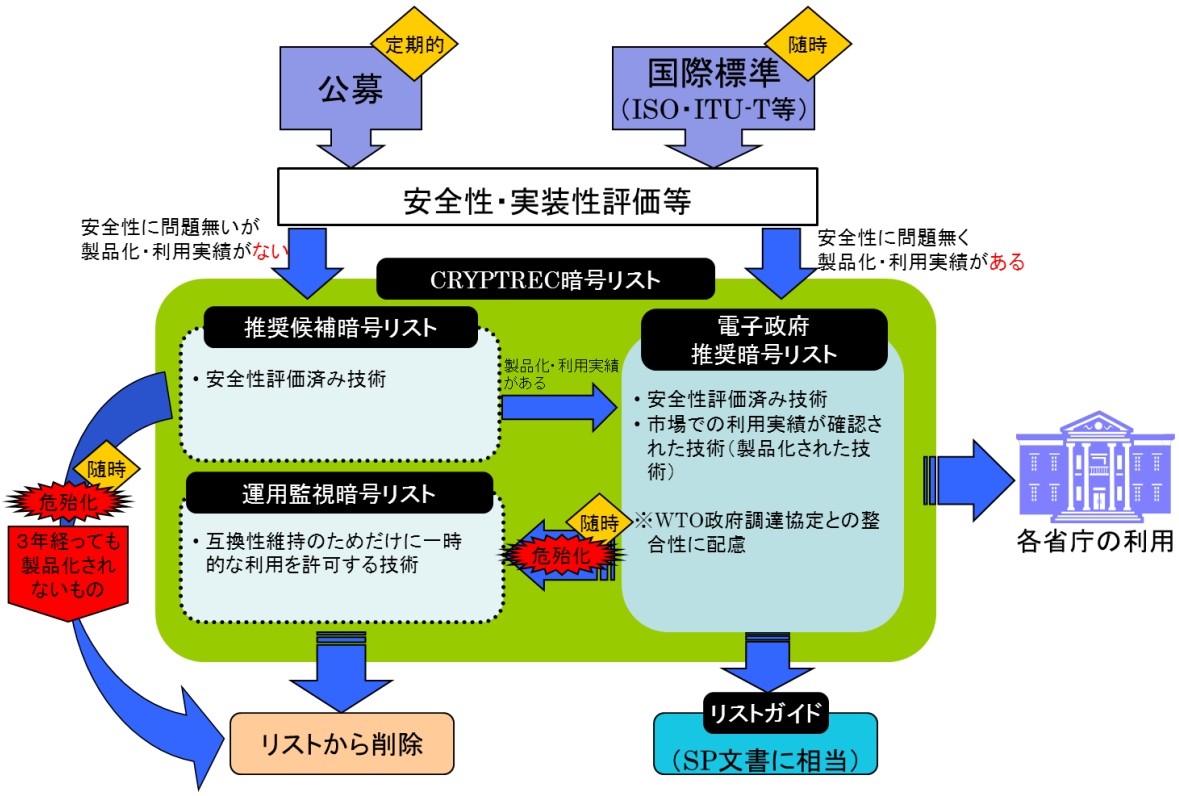
- 上期後半（7～10 月）：

  暗号運用委員会の助言のもと、独立行政法人情報処理推進機構（IPA）が実施した市販製品や標準化等での採用実績についての調査結果の妥当性の確認、ならびに先に確定した選定ルールに照らし合わせた結果判定を実施した。本判定は、暗号方式委員会及び暗号実装委員会との合同委員会の審議を経て、暗号技術検討会に報告された。

- 下期：

  2013 年度の CRYPTREC 体制の改組に伴って新設が計画されている暗号技術活用委員会に引き継ぐべき課題について論点整理を行った。

以下に、2012 年度の暗号運用委員会の活動内容について報告する。



【電子政府推奨暗号リスト】

暗号技術検討会及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断されたもののリスト。

【推奨候補暗号リスト】

CRYPTREC により安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト。

【運用監視暗号リスト】

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暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

図　CRYPTREC 暗号リストの構成

1.1.2　今年度の活動指針

2011 年度第 2 回暗号技術検討会において承認された 2012 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。

表　暗号技術検討会において承認された 2012 年度暗号運用委員会活動計画

(1) 電子政府推奨暗号の選定基準の検討

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

(2) 利用実績の調査

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

(3) 運用監視暗号リストへの遷移要件に関する基準の検討

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検討する。

(4) 電子政府推奨暗号の利用促進体制の検討

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

(5) その他

セキュリティ人材育成の観点を含め、CRYPTREC 暗号リスト策定に伴う暗号学界への影響と対策等に関する検討を開始する。

また、現在移行が進められている RSA1024, SHA-1 等の安全性評価について、新たな展開が発生した場合に、暗号運用委員会としてのコンティンジェンシープランに対する寄与の可能性について継続して検討する。

特に、電子政府推奨暗号の選考に当たっての公平性・客観性を最大限確保する観点から、(1)の電子政府推奨暗号選定のための選定基準については、実質的な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。このため、上期前半での最重要項目として集中的な検討・とりまとめを行うとともに、2012 年度第 1 回暗号技術検討会において選定基準案を報告し、審議をお願いした。

また、(3)～(5)については、今年度の暗号技術検討会での検討課題とも重複する部分があったため、暗号技術検討会での審議状況を踏まえつつ、次年度以降の CRYPTREC 活動の検討に向けた課題の整理として検討を行った。

1.1.3 今年度の委員会の開催状況

2012 年度の暗号運用委員会は、単独の委員会として 4 回、暗号方式委員会及び暗号実装委員会との合同委員会として 2 回の、計 6 回開催された。また、メール審議、並びにアドホック会合として利用実績調査報告会が開催された。各回会合の概要は表 のとおり。

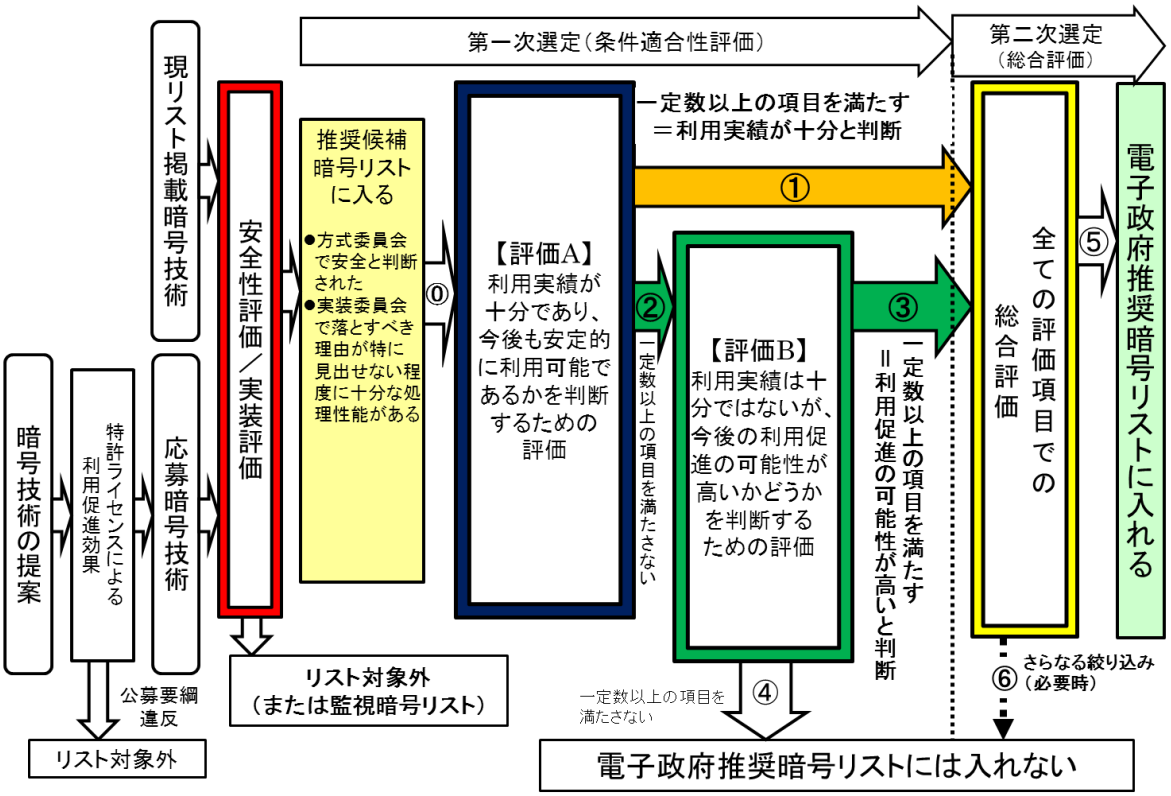
表　2012 年度暗号運用委員会概要

回	開催日時	主な議題
第 1 回	2012 年 6 月 8 日	●暗号運用委員会活動計画について ●選定ルールのフレームワークにおける選定基準の検討について ●利用実績調査について①
第 2 回	2012 年 7 月 25 日	●選定ルールのフレームワークにおける選定基準（暗号運用委員会案）の決定 （※2012 年度第 1 回暗号技術検討会に報告） ●利用実績調査について② （※IPA が実施した利用実績調査に反映）
メール審議	2012 年 8 月 2 日 ～9 月 3 日	●第二次選定（総合評価）の個別配点基準の検討について
アドホック	2012 年 9 月 24 日	●利用実績調査報告会
第 3 回	2012 年 10 月 4 日	●総合評価の個別配点基準（暗号運用委員会案）の決定 ●選定ルールに基づく暗号運用委員会判定の決定
第 1 回 合同委員会	2012 年 11 月 15 日	●CRYPTREC 暗号リスト（案）素案の決定 （※2012 年度第 2 回暗号技術検討会に報告）
第 4 回	2013 年 3 月 1 日	●次年度以降の CRYPTREC 活動の検討に向けた課題の整理
第 2 回 合同委員会	2012 年 3 月 26 日	●暗号運用委員会の 2012 年度活動報告

1.2 成果概要

1.2.1 第一次選定（条件適合性評価）における選定基準（暗号運用委員会案）

2011 年度第 2 回暗号技術検討会で承認された選定ルールのフレームワーク（図 参照）及び選定基準の基本的な考え方に基づき、評価 A 及び評価 B の選定基準案を精緻化した。詳細については第 2.1 章及び第 2.2 章を参照されたい。



- 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（選定ルート①を通るもの）
- 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（選定ルート②③を通るもの）

図　選定ルールのフレームワーク

＜選定基準の基本的な考え方＞

第一次選定（条件適合性評価）段階（評価 A 及び評価 B）において出来る限り電子政府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。

- 電子政府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、電子政府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定基準とする
- 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定基準は極力避ける

＜評価 A の選定基準＞

「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、評価 A では、表 に示す 4 つの評価項目各々について設定された選定基準を満たしているかを判断し、「それら 4 つの評価項目のうち一定数以上の項目が選定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」ところまでが 2011 年度第 2 回暗号技術検討会において承認された。

2012 年度第 1 回及び第 2 回暗号運用委員会では、具体的な選定基準値について審議を行い、以下のような選定基準（暗号運用委員会案）を決定した（表 最右列参照）。本基準案は 2012 年度第 1 回暗号技術検討会に報告され、同検討会にて審議・承認された。

表　評価 A の選定基準

※下線部分が今年度の暗号運用委員会審議で精緻化した部分

	2011 年度第 2 回暗号技術検討会で承認された選定基準の基本的な考え方	2012 年度第 2 回暗号運用委員会で決定した具体的な選定基準（暗号運用委員会案）
評価 A の選定値 ＼ 評価項目	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	4 つの評価項目のうち 3 つ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
市販製品での採用実績	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	提案会社・グループ会社以外での採用実績があり、「採用割合として 50%以上」の採用実績があること
オープンソースプロジェクトでの採用実績	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	「採用割合として 50%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）	「採用割合として 50%以上」の政府系システム規格での採用実績がある ※規格化への採用が合意された段階のものまで含める（最終承認待ち）
国際的な民間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）	「採用割合として 50%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 の選定基準＞

「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 B では、表 に示す評価 A で用いた評価項目 4 つに加え、新たに 4 つの評価項目を追加する。表 に示す合計 8 つの評価項目各々について設定された選定基準を満たしているかを判断し、「それら 8 つの評価項目のうち一定数以上の項目が選定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」ところまでが 2011 年度第 2 回暗号技術検討会において承認された。

2012 年度第 1 回及び第 2 回暗号運用委員会では、具体的な選定基準値について審議を行い、以下のような選定基準（暗号運用委員会案）を決定した（表 最右列参照）。本基準案についても、2012 年度第 1 回暗号技術検討会に報告され、同検討会にて審議・承認された。

表　評価 B の選定基準

※下線部分が今年度の暗号運用委員会審議で精緻化した部分

	2011 年度第 2 回暗号技術検討会で承認された選定基準の基本的な考え方	2012 年度第 2 回暗号運用委員会で決定した具体的な選定基準（暗号運用委員会案）
評価 B の選定値 ＼ 評価項目	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	8 つの評価項目のうち 3 つ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
市販製品での採用実績	表 と同様	
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	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）	以下のいずれかの特許無償ライセンスの付与 ● 特許なし、もしくは契約不要の特許無償ライセンス許諾 ● 非差別的無償許諾契約に基づく無償ライセンス

表　評価 B の選定基準（続）

			2011 年度第 2 回暗号技術検討会で承認された選定基準の基本的な考え方	2012 年度第 2 回暗号運用委員会で決定した具体的な選定基準（暗号運用委員会案）
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	暗号方式委員会、または暗号実装委員会において、技術的アピールポイントがあると判断される
		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	「政府系システム規格」「国際標準規格」「国際的な民間規格」「特定団体規格」のいずれかの規格において、「採用割合として 10%以上」かつ「2 件以上」となる件数での採用が同意されている
		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	以下のいずれかの条件を満たしている ●オープンソースプロジェクトで「採用割合として 10%以上」かつ「2 件以上」となる件数での採用がある ●市販製品で、「提案会社・グループ会社以外での採用実績」があり、「採用割合として 10%以上」となる件数の採用実績がある
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	OS や暗号モジュール（ライブラリやチップなど：市販製品調査カテゴリ#1, #2, #11, #12, #13）として使える市販製品において、「提案会社・グループ会社以外での採用実績」があり、「採用割合として 10%以上」かつ「2 件以上」となる件数の採用実績がある
		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	暗号モジュール（OS カーネル及び暗号化ライブラリ）として使えるオープンソースプロジェクトにおいて、「採用割合として 10%以上」かつ「2 件以上」となる件数の採用実績がある
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	以下のいずれかの条件を満たしている ●市販製品で、「提案会社・グループ会社以外での採用実績」があり、「採用割合として 10%以上」となる件数の採用実績がある ●政府系システムで実際に「採用割合として 10%以上」かつ「2 件以上」となる件数での採用実績がある

※「OR 条件」はいずれかのアピールポイントを満たせば基準を満たしたと判断する

※「2 件以上」の条件は、技術分類の有効数が 4 件以下の時に限り、「1 件」でもよいこととする

1.2.2 第二次選定（総合評価）における配点基準（暗号運用委員会案）

第二次選定（総合評価）は、第一次選定（条件適合性評価）を通過した暗号技術が多数になり、更なる絞り込みを実施することが必要になった時に、その絞り込みを行い得る調整措置として設置されたものである。

ここでは、総合評価による更なる絞り込みが実施されることになった場合に限り、第一次選定（条件適合性評価）を通過した暗号技術に対して、「技術的側面」と利用実績等の「非技術的側面」の両面から見た総合評価を実施する。その際、評価 A により選定された（図 のルート①を通る）暗号技術だけで事実上最終的な選定が行われることがないように、評価 B により選定された（図 のルート②③を通る）暗号技術を対象に、「利用促進が図られると期待される根拠」による合理的な加点を行う方法も準備する。

なお、本配点による総合評価は、さらなる絞り込みを行う必要性が生じた場合にのみ実施されることに注意されたい。また、詳細については第 2.3 章を参照されたい。

＜全体配点＞

総合評価の対象となる暗号技術は、いずれも、安全性や実装性能など「技術的側面」において問題がなく、また利用実績等の「非技術的側面」においても市場に受け入れられている、もしくは今後受け入れられる可能性が高いと期待される。したがって、どこか一側面だけに注目して絞り込み対象を選定するのは望ましくない。

そこで、以下の視点でのバランスを考慮しつつ、全体配点（暗号運用委員会案）を表 のように分配した。本配点案は 2012 年度第 1 回暗号技術検討会に報告され、同検討会にて審議・承認された。

- 「技術的側面」と「非技術的側面」の重要度を同等と考え、両者の配点合計ができるだけ同じになることを基本に置く
- 「非技術的側面」の評価の優劣が「現状での利用実績」だけで事実上決まってしまうことがないようにするため、評価 B により選定された暗号技術に対しては、「利用促進が図られると期待される根拠」による合理的な加点を行う。一方、その加点によって、評価 A により選定された暗号技術が著しく不利にならないように配慮する

＜個別配点＞

絞り込みを行う候補を見極めるために活用することを目的として、得点配分の精緻化よりも、効率よく絞り込み候補が見極められるようなシンプルかつ明快な個別配点（暗号運用委員会案）を策定した（表 参照：暗号運用委員会担当の評価項目部分のみ）。例えば、「広く利用され、影響範囲が広いと考えられる高得点グループ（200 点台）」・「中間グループ（100 点台）」・「影響範囲が比較的限定的と考えられる低得点グループ（100 点未満）」のような分け方ができればよく、点数の絶対値だけをもって優劣や絞り込み対象を決定するような使い方は想定していない。

表　総合評価の全体配点（暗号運用委員会案）

<table>
<tr><td colspan="2" rowspan="2">合計</td><td colspan="2">評価 A での選定</td><td colspan="2">評価 B での選定</td></tr>
<tr><td colspan="2">480</td><td colspan="2">540</td></tr>
<tr><td rowspan="3">技術的側面</td><td>安全性についての仕様上のアドバンテージ</td><td rowspan="3">240
(50.0%)</td><td rowspan="2">120</td><td rowspan="3">240
(44.4%)</td><td rowspan="2">120</td></tr>
<tr><td>論文数の多寡によるアドバンテージ</td></tr>
<tr><td>実装性能評価によるアドバンテージ</td><td>120</td><td>120</td></tr>
<tr><td rowspan="8">現状での利用実績</td><td>政府系システムでの採用実績</td><td rowspan="8" colspan="2">240
(50.0%)</td><td rowspan="13" colspan="2">300
(55.6%)</td></tr>
<tr><td>市販製品での採用実績</td></tr>
<tr><td>オープンソースプロジェクトでの採用実績</td></tr>
<tr><td>利用促進手段採用による普及効果</td></tr>
<tr><td>政府系システム規格での採用実績</td></tr>
<tr><td>国際標準規格での採用実績</td></tr>
<tr><td>国際的な民間メジャー規格での採用実績</td></tr>
<tr><td>民間の特定団体規格での採用実績</td></tr>
<tr><td rowspan="4">利用促進が図られると期待される根拠</td><td>利用促進を図る際の障壁の除去</td><td rowspan="4" colspan="2"></td></tr>
<tr><td>標準化・規格化の促進を図るハードルの低さ</td></tr>
<tr><td>実装コスト低減を図るハードルの低さ</td></tr>
<tr><td>調達コスト低減を図るハードルの低さ</td></tr>
</table>

表　総合評価の個別配点（暗号運用委員会案）

<table>
<tr><td colspan="2">評価項目</td><td>満点</td><td colspan="3">個別配点</td></tr>
<tr><td rowspan="4">現状での利用実績</td><td>政府系システムでの採用実績</td><td>30</td><td>【10 点】採用割合として 10%以上</td><td>【20 点】採用割合として 30%以上</td><td>【30 点】採用割合として 50%以上</td></tr>
<tr><td>市販製品での採用実績</td><td>30</td><td>【10 点】他社利用があり、採用割合として 10%以上</td><td>【20 点】他社利用があり、採用割合として 30%以上</td><td>【30 点】他社利用があり、採用割合として 50%以上</td></tr>
<tr><td>オープンソースプロジェクトでの採用実績</td><td>30</td><td>【10 点】採用割合として 10%以上</td><td>【20 点】採用割合として 30%以上</td><td>【30 点】採用割合として 50%以上</td></tr>
<tr><td>利用促進手段採用による普及効果</td><td></td><td colspan="2">【15 点】「特許無償化（契約の有無を問わず）」もしくは「オープンソース公開」のいずれかを実施している</td><td>【30 点】「特許無償化（契約の有無を問わず）」及び「オープンソース公開」の両方を実施している</td></tr>
</table>

表　総合評価の個別配点（暗号運用委員会案）（続）

<table>
<tr><th colspan="2">評価項目</th><th>満点</th><th colspan="5">個別配点</th></tr>
<tr><td rowspan="4">現状での利用実績</td><td>政府系システム規格での採用実績</td><td>30</td><td colspan="2">【10 点】採用割合として 10%以上（原則 2 件以上*）</td><td colspan="2">【20 点】採用割合として 30%以上（原則 2 件以上*）</td><td>【30 点】採用割合として 50%以上（原則 2 件以上*）</td></tr>
<tr><td>国際標準規格での採用実績</td><td>30</td><td colspan="5">【30 点】採用割合として 10%以上（かつ原則 2 件以上*）</td></tr>
<tr><td>国際的な民間メジャー規格での採用実績</td><td>30</td><td colspan="2">【10 点】採用割合として 10%以上（原則 2 件以上*）</td><td colspan="2">【20 点】採用割合として 30%以上（原則 2 件以上*）</td><td>【30 点】採用割合として 50%以上（原則 2 件以上*）</td></tr>
<tr><td>民間の特定団体規格での採用実績</td><td>30</td><td colspan="2">【10 点】採用割合として 10%以上（原則 2 件以上*）</td><td colspan="2">【20 点】採用割合として 30%以上（原則 2 件以上*）</td><td>【30 点】採用割合として 50%以上（原則 2 件以上*）</td></tr>
<tr><td rowspan="4">利用促進が図られると期待される根拠</td><td>利用促進を図る際の障壁の除去</td><td>20</td><td colspan="3">【10 点】許諾契約ありの特許無償化を実施している</td><td colspan="3">【20 点】許諾契約なしの特許無償化を実施、または特許なし</td></tr>
<tr><td>標準化・規格化の促進を図るハードルの低さ</td><td>20</td><td>【4 点】下記基準で「ポイントが 1」</td><td>【8 点】下記基準で「ポイントが 2」</td><td>【12 点】下記基準で「ポイントが 3」</td><td>【16 点】下記基準で「ポイントが 4」</td><td>【20 点】下記基準で「ポイントが 5 以上」</td></tr>
<tr><td>実装コスト低減を図るハードルの低さ</td><td>10</td><td colspan="2">【4 点】暗号モジュールとして利用可能な市販製品またはオープンソースプロジェクトでの採用実績のいずれかにおいて、「採用割合が 10%以上（原則 2 件以上）」</td><td colspan="2">【7 点】暗号モジュールとして利用可能な市販製品及びオープンソースプロジェクトでの採用実績の両方で「採用割合が 10%以上（原則 2 件以上*）」る、もしくはいずれか一方において「採用割合が 30%以上（原則 2 件以上*）」となる場合</td><td>【10 点】暗号モジュールとして利用可能な市販製品及びオープンソースプロジェクトでの採用実績の両方で「採用割合が 30%以上（原則 2 件以上*）」となる、もしくはいずれか一方において「採用割合が 50%以上（原則 2 件以上*）」となる場合</td></tr>
<tr><td>調達コスト低減を図るハードルの低さ</td><td>10</td><td colspan="2">【4 点】市販製品または政府系システムでの採用実績のいずれかにおいて「採用割合が 10%以上」</td><td colspan="2">【7 点】市販製品及び政府系システムでの採用実績の両方で「採用割合が 10%以上」となる、もしくはいずれか一方において「採用割合が 30%以上」となる場合</td><td>【10 点】市販製品及び政府系システムでの採用実績の両方で「採用割合が 30%以上」となる、もしくはいずれか一方において「採用割合が 50%以上」となる場合</td></tr>
</table>

表　総合評価の個別配点（暗号運用委員会案）（続）

「標準化・規格化の促進を図るハードルの低さ」のポイント（合算：最大 6 ポイント）	
技術的アピールポイント	● 安全性について、技術的アピールポイントがあると暗号方式委員会が判断すれば**「1 ポイント獲得」** ● 実装性について、技術的アピールポイントがあると暗号実装委員会が判断すれば**「1 ポイント獲得」**
標準化等のアピールポイント	● 「政府系システム規格」「国際標準規格」「国際的な民間規格」「特定団体規格」のなかの 1 つまたは 2 つのいずれかの規格において、「採用割合として 10%以上」かつ「原則 2 件以上*」となる件数での採用が同意されている場合には**「1 ポイント獲得」** ● 「政府系システム規格」「国際標準規格」「国際的な民間規格」「特定団体規格」のなかの 3 つ以上の規格において、「採用割合として 10%以上」かつ「原則 2 件以上*」となる件数での採用が同意されている場合には**「2 ポイント獲得」**
採用実績のアピールポイント	● 市販製品またはオープンソースプロジェクトでの採用実績のいずれかにおいて「採用割合が 10%以上」かつ「他社利用あり」となる場合、**「1 ポイント獲得」** ● 市販製品及びオープンソースプロジェクトでの採用実績の両方において「採用割合が 10%以上」かつ「他社利用あり」となる場合、**「2 ポイント獲得」**

※「原則 2 件以上」の条件は、技術分類の有効数が 4 件以下の時に限り、「1 件」でもよいこととする

1.2.3　利用実績調査の概要と調査結果の活用

暗号技術の利用実態として、単に製品やシステムに“搭載されている”だけでなく、“実際に利用している”暗号技術を調べるのが理想的ではある。しかしながら、どの暗号技術を実際に利用しているかは設定や利用環境に依存し、販売会社等から得られる製品情報から判断することは現実には不可能である。このため、次善の方法として、製品やシステムでの搭載状況をもって採用実績とした。

また、広く利用されている製品や重要な製品と、あまり利用されていない製品との間での扱いについても、製品シェアやシステムの重要度等による重み付けをするのが理想的ではある。ただ一方で、現状においては、多くの市販製品についてどの程度利用されているかを判断する客観的かつ検証可能な、信頼できる根拠データを入手することは極めて困難であるのも事実である。そのような状況において製品間での重み付けをすることは、例えば「製造会社名・販売会社名」や「製品の知名度」あるいは「自称の販売シェア」などといった、客観性や検証可能性に乏しい情報をもとにした恣意的な算出方法によって製品間の重み付けをすることにもなりかねず、むしろ客観性を損なう結果につながる恐れがある。このため、公平かつ検証可能なデータのみをそのまま用い、重み付けをしないほうが客観性を確保できると判断した。

以上の観点を踏まえ、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[2]とほぼ同様の手法を踏襲するものとし、IPA が実施主体となって、2012 年 7 月～9 月にかけて実施された。詳細については、IPA ホームページに報告書が公開[3]されているので、そちらを参照されたい。

暗号運用委員会としては、2012 年度第 1 回及び第 2 回での委員会審議の結果を踏まえ、IPA に対して、以下の観点に留意して調査を実施するよう、助言を行った。この他、調査対象について適宜報告を受け、調査内容の確認を行った。

詳細については第 3 章を参照されたい。

- 市販製品の調査対象に極端な偏りが生じないようにするために、暗号製品を区分するカテゴリ 20 個を暗号運用委員会が設定し、当該カテゴリ間でアンケート配布先に極端な偏りが生じないように実施させた
- アンケート回答の妥当性・信憑性が検証できるようにするために、回答内容をどのように検証できるのかを尋ねる質問項目をアンケート票に入れた
- 調査対象とすべき、国際標準規格や国際的な民間メジャー規格、オープンソースプロジェクトを暗号運用委員会が指定し、調査を実施させた

本調査結果については、アドホックに開催された利用実績調査報告会ならびに第 3 回暗号運用委員会において、調査手法や結果の妥当性についての質疑を行い、内容の信憑性を確認した。最終的に、評価 A 及び評価 B で使用する利用実績評価の基礎データは、以下の観点により確定した。

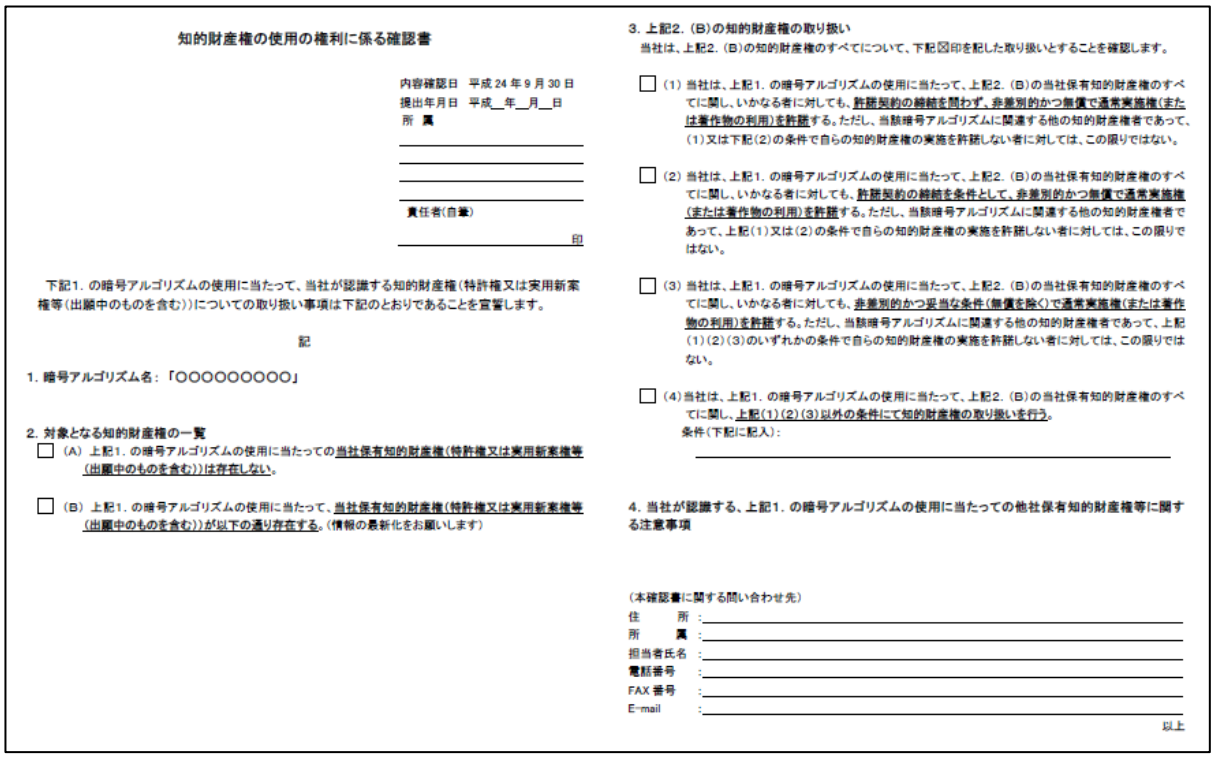
- 全応募者（9 社）より、2002 年度策定の電子政府推奨暗号リストに掲載されている暗号技術、または今回の公募に提案している暗号技術についての最新の利用実績についてアンケートを回収し、調査対象に加えた。なお、当該暗号技術以外の利用実績も特定できたアンケートは有効回答にカウントしたが、当該暗号技術以外の利用実績が特定できなかったアンケートは、参考情報にとどめ、有効回答とは認めなかった
- 市販製品に関するアンケート調査（アンケート配布社数：1849； 有効回答：会社数 127, 製品数 443）、及び公開情報を基にみずほ情報総研が調査（調査対象：会社数 35, 製品数 90）した結果のうち、何らかの手段で回答内容の検証が可能な担保がある信頼度（Lev1～Lev3）の情報のみを活用することとした。この結果、利用実績評価の基礎データとなった市販製品の総数は 469 であった
- 電子政府関連については主に各府省庁より提供された情報を用いた。政府系システムについては 8 府省庁 77 システム、政府系規格については 12 規格が対象となった

[2] http://www.meti.go.jp/meti_lib/report/2010fy01/E001139.pdf
[3] http://www.ipa.go.jp/security/fy24/reports/cryptrec/crypto-algorithm/index.html

- 標準化・規格化については、暗号運用委員会が指定した規格を含む、国際標準規格 12、国際的な民間メジャー規格 108（15 種類）、特定団体規格 24（アンケート調査：16（3 団体）、文献調査数：8（6 団体））が調査対象となった
- オープンソースプロジェクトについては、暗号運用委員会が指定した 24 プロジェクトの最新安定版が調査対象となった。なお、データ集計にあたっては、特に依存関係が強いオープンソースプロジェクトについてはまとめて集計するものとし、その対象として、Linux と Debian、Qmail と OpenSSL、Firefox・Thunderbird・NSS の 3 組を指定した。例えば、Linux と Debian について、両者に搭載されていても 1 としてカウントをする
- 公平性・客観性の観点から、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かった

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、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。



知的財産権の使用の権利に係る確認書

内容確認日　平成 24 年 9 月 30 日
提出年月日　平成＿年＿月＿日
所　属

責任者(自筆)　　印

下記1. の暗号アルゴリズムの使用に当たって、当社が認識する知的財産権（特許権又は実用新案権等（出願中のものを含む））についての取り扱い事項は下記のとおりであることを宣誓します。

記

1. 暗号アルゴリズム名：「OOOOOOOOO」

2. 対象となる知的財産権の一覧

☐ (A) 上記1. の暗号アルゴリズムの使用に当たっての当社保有知的財産権（特許権又は実用新案権等（出願中のものを含む））は存在しない。

☐ (B) 上記1. の暗号アルゴリズムの使用に当たって、当社保有知的財産権（特許権又は実用新案権等（出願中のものを含む））が以下の通り存在する。（情報の最新化をお願いします）

3. 上記2. (B)の知的財産権の取り扱い

当社は、上記2. (B)の知的財産権のすべてについて、下記☒印を記した取り扱いとすることを確認します。

☐ (1) 当社は、上記1. の暗号アルゴリズムの使用に当たって、上記2. (B)の当社保有知的財産権のすべてに関し、いかなる者に対しても、許諾契約の締結を問わず、非差別的かつ無償で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、(1)又は下記(2)の条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

☐ (2) 当社は、上記1. の暗号アルゴリズムの使用に当たって、上記2. (B)の当社保有知的財産権のすべてに関し、いかなる者に対しても、許諾契約の締結を条件として、非差別的かつ無償で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記(1)又は(2)の条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

☐ (3) 当社は、上記1. の暗号アルゴリズムの使用に当たって、上記2. (B)の当社保有知的財産権のすべてに関し、いかなる者に対しても、非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記(1)(2)(3)のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

☐ (4) 当社は、上記1. の暗号アルゴリズムの使用に当たって、上記2. (B)の当社保有知的財産権のすべてに関し、上記(1)(2)(3)以外の条件にて知的財産権の取り扱いを行う。
条件（下記に記入）：

4. 当社が認識する、上記1. の暗号アルゴリズムの使用に当たっての他社保有知的財産権等に関する注意事項

（本確認書に関する問い合わせ先）
住　　所：
所　　属：
担当者氏名：
電話番号：
FAX 番号：
E-mail：

以上

図　　特許ライセンス確認書の統一フォーマット

このため、2012 年 9 月 30 日時点における特許ライセンスの取り扱い状況について、図の統一フォーマットにより応募者に確認を行った。2012 年 9 月 30 日時点における、CRYPTREC 暗号リストに掲載された暗号技術の応募者による取り扱い状況は付録のとおり。

1.2.5 選定ルールに基づく暗号運用委員会判定

1.2.1 節で決定された選定ルールに基づき、1.2.3 節及び 1.2.4 節での結果を当てはめて判定した結果は以下のとおりである。

表　評価 A の暗号運用委員会判定結果

凡例：（判定結果）　○：評価 A の通過条件を満たす　×：評価 A の通過条件を満たさない
（根拠データ）　○：選定基準を満たす　×：選定基準を満たさない

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

表　評価 A の暗号運用委員会判定結果（続）

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

表　評価 B の暗号運用委員会判定結果

凡例：（判定結果）　○：評価 B の通過条件を満たす　×：評価 B の通過条件を満たさない

（根拠データ）　○：選定基準を満たす　×：選定基準を満たさない

		判定結果		判定根拠データ							
				市販製品採用実績	オープンソースプロジェクト採用実績	政府系システム規格採用実績	国際的な民間規格採用実績	利用促進を図る際の障壁除去	標準化・規格化の促進を図るハードルの低さ	実装コスト低減を図るハードルの低さ	調達コスト低減を図るハードルの低さ
署名	ECDSA	○	3/8	×	×	×	×	×	○	○	○
	RSA-PSS	○	4/8	×	×	×	×	○	○	○	○
守秘・鍵共有	ECDH	○	3/8	×	×	×	×	×	○	○	○
	PSEC-KEM	×	2/8	×	×	×	×	○	○	×	×
	RSA-OAEP	○	4/8	×	×	×	×	○	○	○	○
64 ビットブロック暗号	CIPHERUNICORN-E	×	1/8	×	×	×	×	×	○	×	×
	Hierocrypt-L1	×	1/8	×	×	×	×	×	○	×	×
	MISTY1	×	2/8	×	×	×	×	○	○	×	×
128 ビットブロック暗号	Camellia	○	4/8	×	×	×	×	○	○	○	○
	CIPHERUNICORN-A	×	1/8	×	×	×	×	×	○	×	×
	CLEFIA	×	1/8	×	×	×	×	×	○	×	×
	Hierocrypt-3	×	1/8	×	×	×	×	×	○	×	×
	SC2000	×	1/8	×	×	×	×	×	○	×	×
ストリーム暗号	Enocoro-128v2	×	1/8	×	×	×	×	×	○	×	×
	KCipher-2	○	3/8	×	×	×	×	○	○	×	○
	MUGI	×	2/8	×	×	×	×	○	○	×	×
	MULTI-S01	×	1/8	×	×	×	×	×	○	×	×
ハッシュ関数	SHA-256	○	6/8	○	○	×	×	○	○	○	○
	SHA-384	○	5/8	×	○	×	×	○	○	○	○
	SHA-512	○	5/8	×	○	×	×	○	○	○	○
暗号利用モード（秘匿）	CFB	○	5/8	×	○	×	×	○	○	○	○
	CTR	○	4/8	×	×	×	×	○	○	○	○
	OFB	○	4/8	×	×	×	×	○	○	○	○
（認証付秘匿）	CCM	○	3/8	×	×	×	×	○	○	○	×
	GCM	○	4/8	×	×	×	×	○	○	○	○

表　評価 B の暗号運用委員会判定結果（続）

		判定結果		判定根拠データ							
				市販製品採用実績	オープンソースプロジェクト採用実績	政府系システム規格採用実績	国際的な民間規格採用実績	利用促進を図る際の障壁除去	標準化・規格化の促進を図るハードルの低さ	実装コスト低減を図るハードルの低さ	調達コスト低減を図るハードルの低さ
ﾒｯｾｰｼﾞ認証ｺｰﾄﾞ	CMAC	○	4/8	×	×	○	×	○	○	○	×
	PC-MAC-AES	×	1/8	×	×	×	×	×	○	×	×
エンティティ認証	ISO/IEC9798-2	○	3/8	×	－	×	－	×	○	○	○
	ISO/IEC9798-3	○	3/8	×	－	○	－	×	○	×	○
	ISO/IEC9798-4	×	1/8	×	－	×	－	×	○	×	×

1.2.6　次年度以降の CRYPTREC 活動の検討に向けた課題の整理

2013 年度の CRYPTREC 体制の改組に伴って、暗号技術の安全性評価を中心とした技術的な検討課題を主に担当する「暗号技術評価委員会」と、セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討課題を主に担当する「暗号技術活用委員会」が設置される予定である。

暗号技術活用委員会での検討項目としては、以下の 3 点が計画されている。

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）
② 暗号技術の利用状況に係る調査及び必要な対策の検討等
③ 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）

そこで、暗号運用委員会としては、上記検討項目に関連し、暗号技術活用委員会に引き継ぐべき課題についての論点整理を行った。詳細については、第 4 章を参照されたい。

1.3　CRYPTREC シンポジウム 2013 の開催状況

日　時　：2013 年 3 月 26 日（火）10：00～15：45
場　所　：コクヨホール
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：238 名

表　プログラム

3 月 26 日(火)		
時間	内　容	
10：00	開会挨拶	
10：05	総務省挨拶・経済産業省挨拶	
10：15	CRYPREC 暗号リストについて	暗号技術検討会事務局
10：45	暗号方式委員会報告	中央大学　今井教授
11：05	暗号実装委員会報告	東北大学　本間准教授
11：25	暗号運用委員会報告	横浜国立大学　松本教授
11：45	昼休み	
13：10	（パネルディスカッション） CRYPTREC 暗号リストの活用と日本の暗号・情報セキュリティ技術の競争力向上に向けて	NISC、総務省、総務省行政管理局、経済産業省、パネリスト
14：40	休憩	
15：00	リストガイド WG 報告	東京工科大学　手塚教授
15：30	計算機能力評価 WG 報告	九州大学　高木教授
16：00	閉会挨拶	

第２章　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定基準

2.1　評価 A の選定基準

2011 年度第２回暗号技術検討会において承認された選定フレームワークにおける評価 A は「利用実績が十分かどうか」を判定するものであり、そのなかで利用される評価項目は以下の 4 項目である（図 参照）

- 「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」

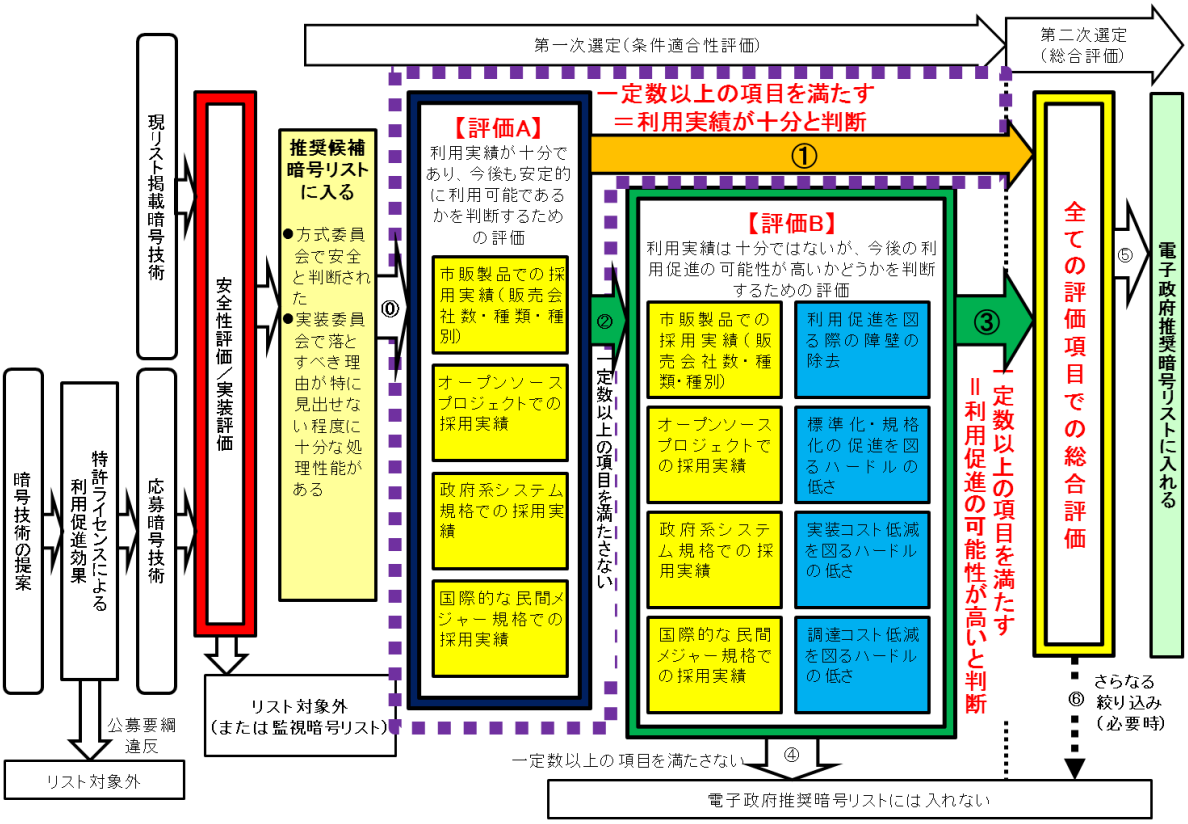


図　　選定フレームワークにおける評価 A の位置づけ

それらの評価項目について、2012 年度暗号運用委員会では、第 1 回及び第 2 回の委員会審議において、評価 A における選定基準を議論し、確定した。その際の論点は以下の 3 点である。

- どのような尺度（集計方法）を持って評価を行うか
- 評価項目ごとの「利用実績が十分」と判断する基準をどこに置くか
- 4 つの評価項目中、いくつの項目が「利用実績が十分」と満たせば評価 A を満たした（①のルートで総合評価に移る）ことにするか

【どのような尺度（集計方法）を持って評価を行うか】

今回実施する利用実績調査（3 章参照）の手法は、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ことから、暗号運用委員会として入手可能な調査データの精度自体はそれほど変わらないものと想定した。

したがって、「2009 年度の利用実績調査でも当時の利用実態をそれなりに反映している」ということを前提として、どのような尺度（集計方法）として表現すれば「利用実績が十分である」と判断しやすいかの視点で議論を行った。その際、公平性・客観性の観点から、CRYPTREC 事務局が選定した暗号技術及び CRYPTREC 暗号リスト対象外の暗号技術を対象とした。調査データの集計方法として検討したのは表 に挙げる 3 案である。

表　集計方法の比較

集計方法案	**案 1：「絶対数」評価** 個々の暗号技術の採用実績数である「絶対数」で集計	**案 2：「絶対割合」評価** 個々の暗号技術の採用実績数の、全回答総数に対する「絶対割合」で集計	**案 3:「相対割合」評価** 個々の暗号技術の採用実績数の、その技術分類に該当する回答総数に対する「相対割合」で集計
選定基準設定の考え方	技術分類ごとに異なる選定基準の設定が必要	技術分類ごとに異なる選定基準の設定が必要	技術分類を問わず、共通の選定基準の設定が可能
アンケート回収総数の多寡による影響	アンケート回収総数が多くなるほど、個々の暗号技術の採用実績数が必然的に多くなることが想定され、安定的な基準値で判断できない	アンケート回収総数が多くなるほど、個々の暗号技術の採用実績数の割合としては安定すると想定され、安定的な基準値で判断可能と期待できる	アンケート回収総数が多くなるほど、個々の暗号技術の採用実績数の割合としては安定すると想定され、安定的な基準値で判断可能と期待できる
今後の目標	選定基準値を満たしているか独自に判断できる	再調査をしない限り、選定基準値を満たしているか判断ができない	再調査をしない限り、選定基準値を満たしているか判断ができない

具体例として、例えばアンケート回収総数が 20 個であるとする。このうち、何らかの署名を利用しているもの（技術分類「署名」）が 8 個あり、うち 6 個が A 署名を利用して

いるとする。同様に、何らかの 128 ビットブロック暗号を利用しているもの（技術分類「128 ビットブロック暗号」）が 17 個あり、うち 13 個が B 暗号を利用しているとする。この場合、A 署名と B 暗号はそれぞれ以下のような評価値として扱われる。

- 案 1「絶対数」評価の場合：A 署名は「6」、B 暗号は「13」
- 案 2「絶対割合」評価の場合：A 署名は「30%（=6/20）」、B 暗号は「65%（=13/20）」
- 案 3「相対割合」評価の場合：A 署名は「75%（=6/8）」、B 暗号は「76.5%（=13/17）」

審議の結果、①技術分類の違いによる回答総数の差異があらかじめ反映され、技術分類に関わらずに共通の選定基準が設定可能であること、②市販製品に対する利用実績調査のアンケート回収数が 500 件以上との目標であることから絶対数よりも割合のほうが安定的な基準値を設けられる、点を重視し、案 3 の集計方法を採用することとした。

以降では、この割合のことを「採用割合」と呼ぶこととする。

【評価項目ごとの「利用実績が十分」と判断する基準をどこに置くか】

2009 年度の利用実績調査結果をベースに、CRYPTREC 事務局が選定した暗号技術及び CRYPTREC 暗号リスト対象外の暗号技術を対象として採用割合を表したものが図 となる。これに、当該暗号技術の 2009 年度の利用実態を勘案しながら検討を行った結果、以下の理由により、「採用割合 50%以上」を選定基準の閾値とすることで暗号運用委員会の合意が図られた。

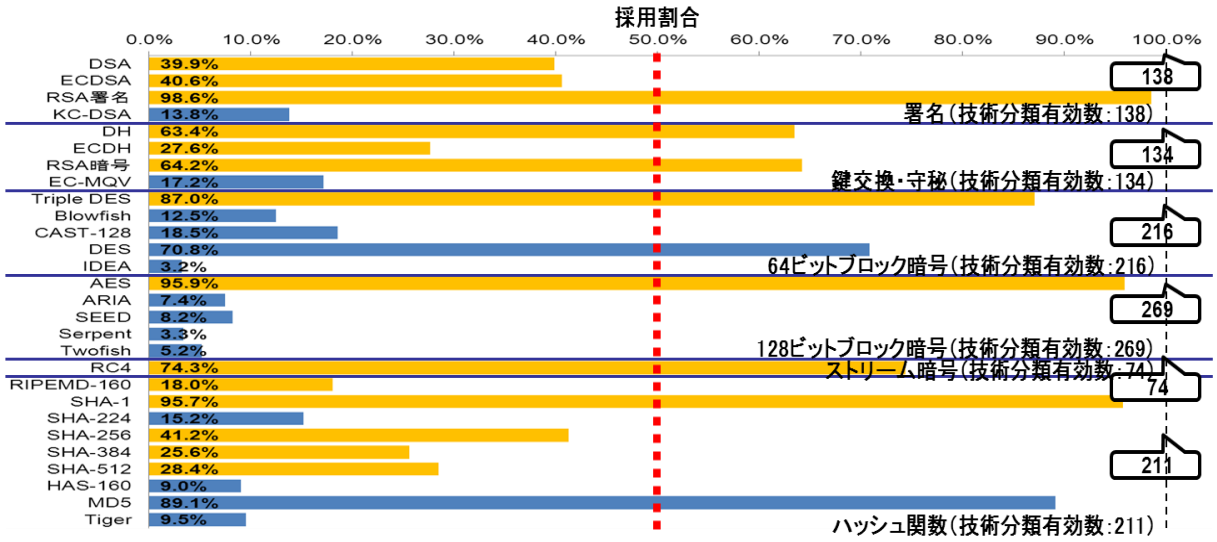


図　2009 年度の利用実績調査結果をベースにした採用割合

- 「利用実績が十分」と判断するには、調査対象数のマジョリティ（50%以上）の採用実績があることが望ましい

- 2009 年度調査結果と照らしても、「採用割合 50%以上」とすることで問題が生じるとはいえない（2009 年当時であれば、DSA, ECDSA, SHA-256 などが「利用実績が十分とは言えない」との判断でも違和感がない）

【いくつの項目が「利用実績が十分」と満たせば評価 A を満たしたことにするか】

選定基準の基本的な考え方として、第一次選定（条件適合性評価）段階（評価 A 及び評価 B）において出来る限り電子政府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ていることから、評価 A の選定基準は高めに設定することが望まれる。

この観点から、暗号運用委員会としては、「4 つの評価項目の選定基準をすべて満たす」か「4 つの評価項目の選定基準のうち 3 つ以上を満たす」のいずれかとすることで最初の合意がなされた。次いで、この 2 つのどちらにすべきかの検討を行ったが、以下のような、いずれか 1 つの評価項目が満たされていなくても利用実績が十分であると判断しても構わないと考えられるケースがあることから、「4 つの評価項目の選定基準のうち 3 つ以上を満たす」を条件とすることに決した。

- 例えば、「オープンソースを公開しない」といった場合でも、企業努力で他に十分に普及させたのならば、利用実績が十分と認めてもよいと考えられる
- 例えば、「政府系システム規格での採用実績が閾値を満たしていない」といった場合でも、製品やオープンソースなどが多数あるならば実際には政府調達できるケースも多いと考えられる

2.2 評価 B の選定基準

2.1 節で述べたように、暗号運用委員会が設定した評価 A での選定基準は、国際的にも「デファクトスタンダード」と認められるようなレベルの普及度を持っているような暗号技術のみが選定されることを想定しており、「利用実績が十分」と判断するためのハードルとしては極めて高い。逆に言えば、ほとんどの暗号技術は評価 A では選定基準を満たさず、評価 B に回されてくることとなる。

そこで、2011 年度第 1 回暗号技術検討会にて意見集約された電子政府推奨暗号リストの役割（表 参照）に基づき、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できるように、将来的にデファクトスタンダードの一つになることを目指せるような暗号技術を電子政府推奨暗号に選定することを評価 B での目的とする。つまり、技術面の優位性だけではなく、官民あるいは国内外による幅広い支援・バックアップを得ることが期待できるかなど、様々な観点で将来的なデファクトスタンダードを目指すうえでの潜在力を見極め、「今後の利用促進の可能性が高いかどうか」を判定する。

表　暗号技術検討会での意見集約結果

電子政府推奨暗号リストに求める役割の概要		選定意図	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）

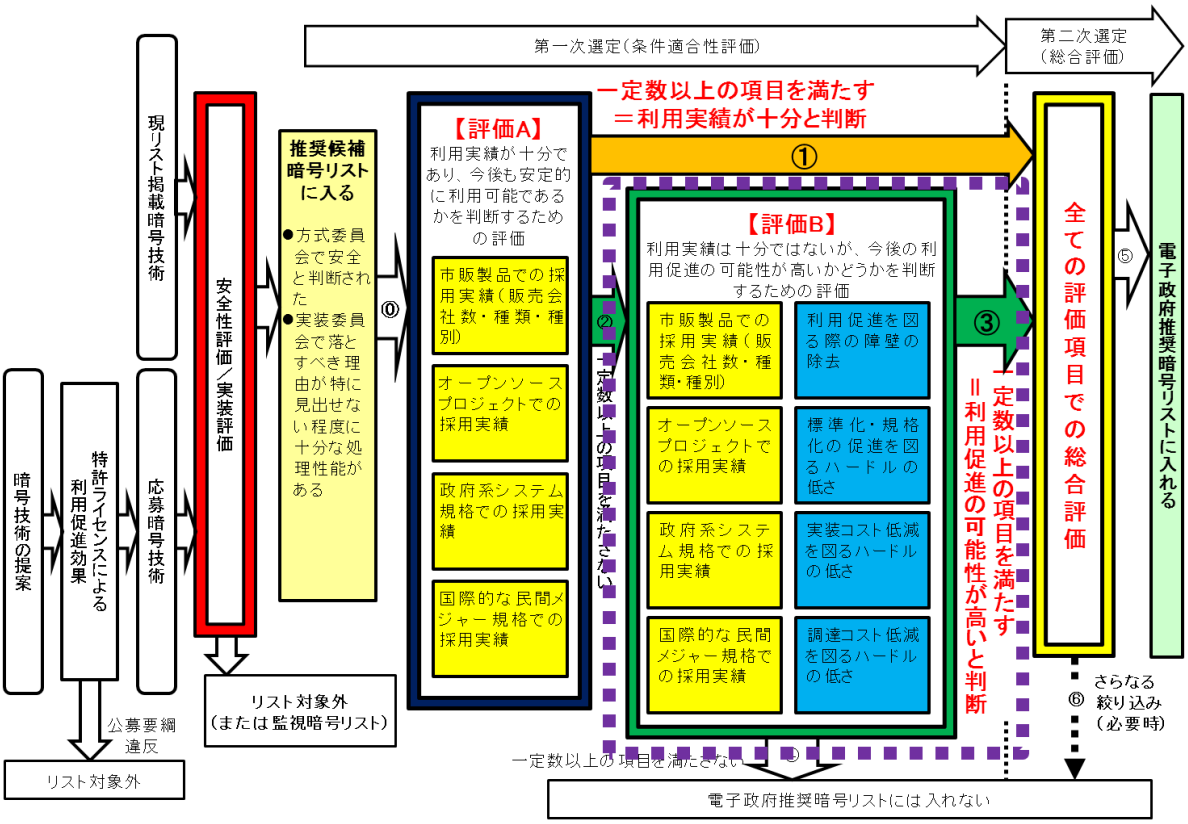


図　選定フレームワークにおける評価 B の位置づけ

具体的には、評価 B で利用される評価項目には、以下のように、評価 A と同じ評価項目 4 項目と評価 B で新たに追加される 4 項目の合計 8 個の評価項目がある（図　参照）。

（評価 A と同じ評価項目）

- 「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」

（評価 B で新たに追加された評価項目）

- 「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」

そのうち、新たに追加される 4 つの評価項目について、2012 年度第 1 回及び第 2 回暗号運用委員会での審議を通じ、今後の普及展開支援によって、「国際標準化・製品化促進」や「将来的な調達容易性（利用実績）が十分に高くなる」と期待できる根拠となるような閾値を設定した。

【特許ライセンスの取り扱い】

CRYPTREC Report 2011 でも記載されている通り、利用促進として幅広い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。その観点から、「特許なし、もしくは契約不要の特許無償ライセンス許諾」または「非差別的無償許諾契約に基づく無償ライセンス許諾」している暗号技術を優位に取り扱うこととした。

【利用実績の取り扱い】

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」は必要である。また、暗号技術の提案会社ならびにグループ会社・関連会社以外の「他社が利用」しているかどうかは、提案会社以外からの支援が得られやすい状況にあるかどうかのバロメータにもなりうる。

そこで、2009 年度の利用実績調査結果をベースに、「他社利用が広く進んでいなければ基準を満たすことが難しく、かつ分かりやすい閾値を設定」するとの方針で検討を行った結果、「採用割合 10%以上」を選定基準の閾値とすることで暗号運用委員会の合意が図られた。その理由としては、「採用割合 10%」以外の選択肢として、例えば「採用割合 5%以上」では他社利用がなくても基準を満たせる可能性がある一方、現状では（米国以外の）政府標準暗号であっても「採用割合 15%以上」の基準を満たすことは簡単ではない、と考えられたためである。

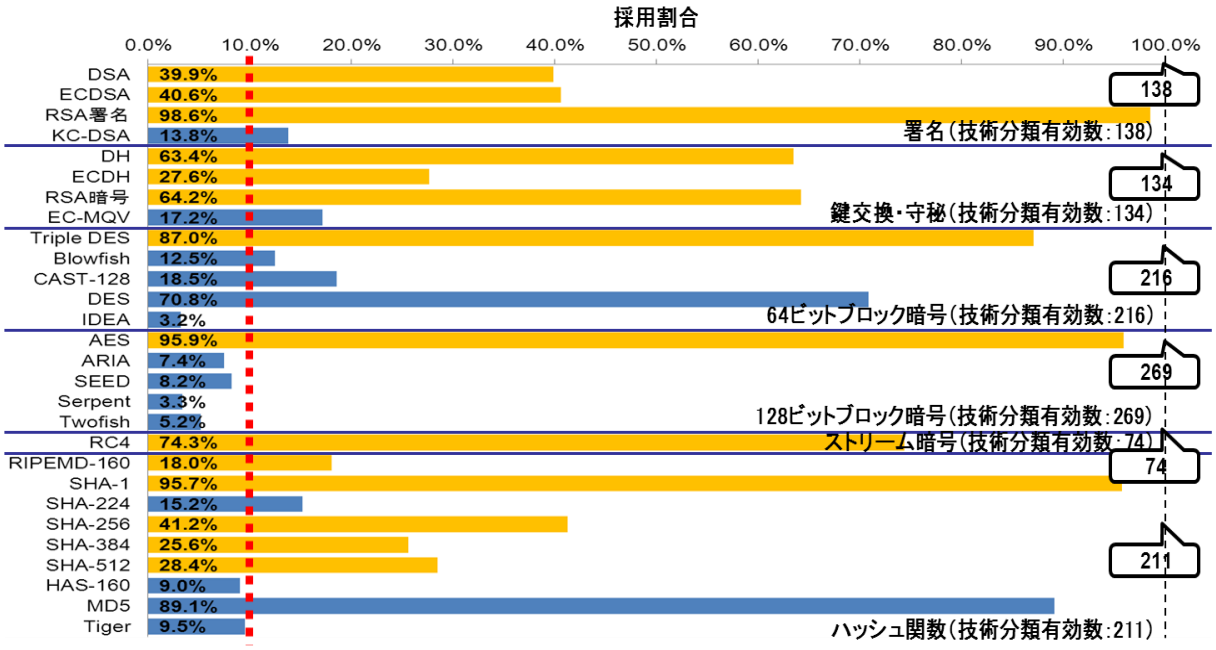


図　2009 年度の利用実績調査結果をベースにした採用割合

なお、標準化・規格化等では、調査対象数自体が少ないため、「1 件」の採用実績でも「採用割合が 10%以上」になることが想定される。これに対し、暗号運用委員会の席上、「採用実績が 1 件しかなくても、調査対象に偶然選ばれただけで選定基準を満たすと判断されることになるのは危険」との見解が出され、最終的に「採用割合だけでなく、「2 件以上」も必要条件に含める」こととした。

ただし、技術分類有効数が 4 件以下の場合に「2 件以上」を条件とすると、評価 A の基準（採用割合 50%）を上回ることになり、評価 B の基準としてふさわしくない。そこで、技術分類有効数が 4 件以下の場合に限り「1 件」でもよいこととした。

【利用実績のアピールポイントの対象】

「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」のいずれのアピールポイントも、採用実績をベースに評価する部分がある。一方で、それぞれのアピールポイントの目的は異なるため、それぞれの意図に応じた利用実績として評価する必要がある。

そこで、利用実績として取り扱う対象範囲を、以下のように限定することとした。

- 標準化・規格化の促進を図るハードルの低さ

  〔評価意図〕　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

  〔対象範囲〕　利用実績を持って標準化・規格化の促進を図るためには、多くの製品やオープンソースプロジェクトで使われている暗号技術であることがアピール

ポイントの一つとなると期待される。このことから、市販製品全体、及びオープンソースプロジェクト全体での利用実績を対象範囲とする。なお、政府系システムでの利用実績は、現状では標準化・規格化の促進に対してアピール力があるとは言い切れないため、対象外とする

- 実装コスト低減を図るハードルの低さ

〔評価意図〕 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

〔対象範囲〕 新たな暗号を追加する際、当該暗号が実装された製品パーツがすでに存在していれば、その製品パーツを組み込むだけでよく、自ら当該暗号を実装する必然性がなくなる。このことは、当該暗号を搭載する暗号製品の開発期間や設計コスト、検査コストなどを含めた実装コスト全体の低減につながることは明らかである。そこで、製品パーツとして組込みやすい、①OS（市販製品調査カテゴリ#1)、②暗号化ツールキット／ライブラリ（同#2)、③カード（同#11)、④IC チップ（同#12)、⑤ハードウェアセキュリティモジュール（同#13）の各市販製品、ならびに、⑥OS、⑦暗号化ツールキット／ライブラリの各オープンソースプロジェクトでの利用実績を対象範囲とする

- 調達コスト低減を図るハードルの低さ

〔評価意図〕 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

〔対象範囲〕 同じ暗号が搭載された多くの市販製品が存在するほうが調達時における価格競争原理が働き、調達コストの低減につながる。また、実際に政府系システムで採用されていることは、調達コストが問題ないレベルにあったことの実績として評価可能である。したがって、市販製品全体、及び政府系システムでの利用実績を対象範囲とする。なお、オープンソースプロジェクトの利用実績は、オープンソースプロジェクト自体を調達することはないため、対象外とする

【いくつの評価項目と満たせば評価 B を満たしたことにするか】

選定基準の基本的な考え方として、第一次選定（条件適合性評価）段階（評価 A 及び評価 B）において出来る限り電子政府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にしていること、また評価 A の選定基準が高めに設定されたことから、評価 B の選定基準も高めに設定することが望まれる。

この観点から、暗号運用委員会としては、以下の 4 つの選択肢を候補に議論を行った。

- 「8 つの評価項目の選定基準のうち、6 項目を満たす」
- 「8 つの評価項目の選定基準のうち、5 項目以上を満たす」
- 「8 つの評価項目の選定基準のうち、4 項目以上を満たす」
- 「8 つの評価項目の選定基準のうち、3 項目以上を満たす」

これらについて、「評価 A の 4 つの選定基準のうち、少なくとも 1 項目以上を満たすことを必須条件として課すべきか否か」、「特許無償化を強い条件として課すべきか否か」の視点で検討を行い、以下の理由により、「8 つの評価項目の選定基準のうち、3 項目以上を満たす」を条件とすることに決した。

- 評価 A の選定基準は「採用割合 50%」と高いため、新しい暗号技術などは評価 A の評価項目を一つも満たさない可能性が高い。一方、「5 項目以上」または「6 項目」を基準にすると、評価 A の評価項目を一つも満たさない暗号技術は直ちに評価 B を通過できなくなるので、問題がある
- 評価 A の評価項目を一つも満たさない暗号技術であって「特許無償化を実施しない」といった場合でも、企業努力で残りの「3 項目」（「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」）を満たしたのならば、評価 B を満たしていると認めてもよい
- 「3 項目以上」では、特許無償化を選択した場合に評価 B の基準を満たすことと、特許無償化をせずに評価 B の基準を満たすこととの差が大きすぎるのではないか、との指摘があった。しかし、今まで評価 B の 8 つの評価項目間には重み付けをせずに判断すると対外的に説明してきたため、現時点で評価項目間に重み付けをすることは適当ではない

2.3 総合評価の選定基準

総合評価による更なる絞り込みが実施されることになった場合に限り、第一次選定（条件適合性評価）を通過した暗号技術に対して、「技術的側面」と利用実績等の「非技術的側面」の両面から見た総合評価を実施する。その際、総合評価の対象となる暗号技術は、いずれも、安全性や実装性能など「技術的側面」において問題がなく、また利用実績等の「非技術的側面」においても市場に受け入れられている、もしくは今後受け入れられる可能性が高いと期待される。したがって、どこか一側面だけに注目して絞り込み対象を選定するのは望ましくない。

上記の視点を踏まえ、2012 年度暗号運用委員会では、第 2 回の委員会審議において全体配点案と個別配点案の考え方を議論・確定し、第 3 回の委員会審議において具体的な個別配点案を確定した。なお、全体配点案については、2012 年度第 1 回暗号技術検討会に報告

され、同検討会にて審議・承認された。

2.3.1 全体配点案

2011 年度第 2 回暗号技術検討会において承認された選定フレームワークでは、総合評価で取り扱う評価項目として表 の基本的な考え方が承認されている。なお、「利用促進が図られると期待される根拠」にある 4 項目については、評価 B により選定された（図　選定フレームワークにおける評価 B の位置づけ図 のルート②③を通る）暗号技術についてのみ取り扱い、評価 A により選定された（図 のルート①を通る）暗号技術については除外される。

以上の総合評価の基本的な考え方を踏まえ、実際の全体配分案の策定に当たっては、以下の視点でのバランスを考慮しながら検討を行った。

- 「技術的側面」と「非技術的側面（現状での利用実績及び利用促進が図られると期待される根拠)」の重要度を同等と考え、両者の配点合計ができるだけ同じになることを基本に置く
- 「非技術的側面」の評価の優劣が「現状での利用実績」だけで事実上決まってしまうことがないようにするため、評価 B により選定された暗号技術に対しては、「利用促進が図られると期待される根拠」による合理的な加点を行う。一方、その加点によって、評価 A により選定された暗号技術が著しく不利にならないように配慮する

表　2011 年度に承認された総合評価の基本的な考え方

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	
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

表　2011 年度に承認された総合評価の基本的な考え方（続）

評価項目		加点基準	重みづけ
現状での利用実績	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
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	

ここで、評価 B により選定された暗号技術を対象とした「利用促進が図られると期待される根拠」による合理的な加点を行う方法では、「評価 A により選定された暗号技術」と「評価 B により選定された暗号技術」との間での現状の利用実績の評価差をある程度緩和させることを主眼に置く。これは、「非技術的側面」の評価の優劣が「現状での利用実績」

だけで事実上決まってしまうことがないようにするための措置である。

その観点で「現状での利用実績」にある評価項目をみると、現状の利用実績の違いで点数差が特に生じやすいと考えられる項目は以下の 6 項目である。このことは、これらの評価項目の点数差を緩和できれば、合理的な加点を行う目的が達成できると考えられる。

- 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
- 民間の特定団体規格での採用実績

上記 6 項目について、評価 A により選定された暗号技術と評価 B により選定された暗号技術がそれぞれどの程度の点数を取る可能性があるかを検討し、最終的に評価 A の基準には及ばないがそれに次ぐ程度の利用実績がある暗号技術であれば得点差がほぼ解消されるレベルの点数を「利用促進が図られると期待される根拠」に割り当てることとした。そうすることにより、わずかに評価 A の基準に及ばず、評価 B により選定された暗号技術のほうが、評価 A により選定された暗号技術よりも明らかに有利になることを防ぐ。

具体的には、2.3.2 節で述べるように、利用実績の評価 1 段の違いが配点の 1/3 に相当することから、上記 6 項目に割り当てられる「合計点の 1/3」を配点することとした。

以上の点を踏まえ、最終的に、技術的側面に「240 点」、現状での利用実績に「240 点（うち、上記 6 項目の合計は 180 点）」、利用促進が図られると期待される根拠に「60 点」を配点することとした。これにより、評価 A により選定された暗号技術は 480 点満点、評価 B により選定された暗号技術は 540 点満点となる（表 参照）。

2.3.2 個別配点案

総合評価では、絞り込みを行う候補を見極めるために活用することを目的としていることから、得点配分の精緻化よりも、効率よく絞り込み候補が見極められるようなシンプルかつ明快な個別配点案を検討した。例えば、「広く利用され、影響範囲が広いと考えられる高得点グループ（200 点台）」・「中間グループ（100 点台）」・「影響範囲が比較的限定的と考えられる低得点グループ（100 点未満）」のような分け方ができればよく、点数の絶対値だけをもって優劣や絞り込み対象を決定するような使い方は想定していない。

以上の点を踏まえ、表 にある 2011 年度に決めた総合評価の各評価項目における配点については、以下の方針で行うことが合意された。

- 総合評価の対象となる暗号技術はいずれも、安全性・実装性・利用実績・標準化等の

すべての面において一定水準以上にあると期待される。したがって、総合評価における、現状での利用実績はどの評価項目も重要度は同じであるとし、均等に配点する

- 評価 B により選定された暗号技術にとっては、現状での利用実績よりも今後の利用促進が期待できるかのほうがより重要である。この観点から、現状での利用実績が反映されやすい「実装コスト低減を図るハードルの低さ」と「調達コスト低減を図るハードルの低さ」の評価項目よりも、「利用促進を図る際の障壁の除去」と「標準化・規格化の促進を図るハードルの低さ」の評価項目のほうが、重要性が高いと判断する。そこで、「利用促進が図られると期待される根拠」における配点は以下の方針で行う。
  - 「実装コスト低減を図るハードルの低さ」と「調達コスト低減を図るハードルの低さ」は現状の採用実績から期待される利用促進のハードルの低さを表すものとし、「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」、「採用実績から期待される利用促進のハードルの低さ」のいずれもが同程度の重要度があるとみなし、均等に配点する
  - 「実装コスト低減を図るハードルの低さ」と「調達コスト低減を図るハードルの低さ」の重要度は同程度とみなし、「採用実績から期待される利用促進のハードルの低さ」の配点の均等割りとする

【現状での利用実績①】

評価項目ごとの加点基準については、表 にある 2011 年度に決めた総合評価の加点基準の基本的な考え方を踏襲し、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ることとした。

以下の 6 項目については、評価 B により選定された暗号技術間での利用実績の違いを反映するため、評価 A の閾値 50%、評価 B の閾値 10%を基準として、両閾値の間にもう一つの閾値を設定することとした。つまり、当該暗号技術の利用実績が、評価 A に近い利用実績であるのかそうでないのかを区別する。

- 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
- 民間の特定団体規格での採用実績

中間に設定する閾値をどこに設定するか、またその時の配点をどのようにするか、についていくつかの案を検討した結果、総合評価の目的や加点基準の考え方に沿い、もっともシンプルかつ明快な配点方法として、図 の基準を採用することとした。

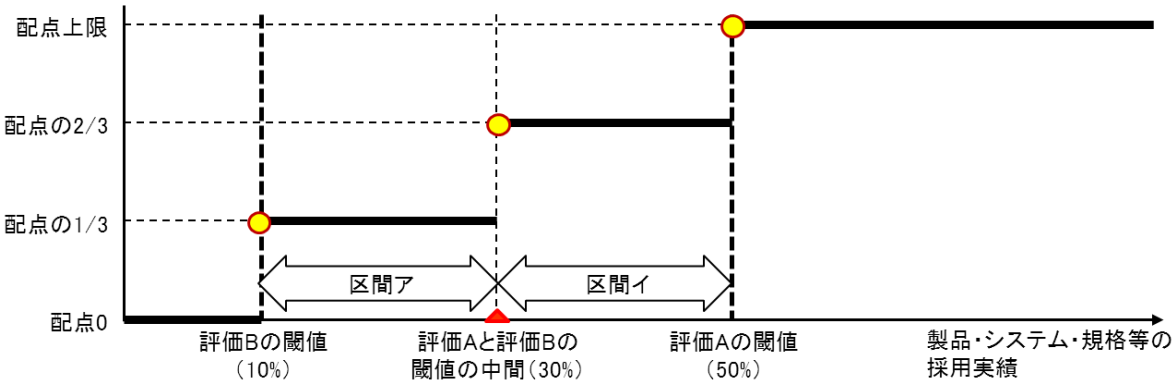


図　現状での利用実績①における個別配点

【現状での利用実績②】

表 では、「特許ライセンスによる利用促進効果」と「オープンソース公開による利用促進効果」を別個の評価項目として考えていたが、両者はあくまで利用促進手段であり、利用実績を直接反映する指標ではないとの見解が出された。また、無償許諾契約有無の影響は、現状でのその他の利用実績に反映されていると考えられた。

以上の点を考慮し、「特許ライセンスによる利用促進効果」と「オープンソース公開による利用促進効果」の評価項目に替えて、「利用促進手段採用による普及効果」の評価項目を加えた。そのなかで、利用促進手段としては 「特許ライセンス無償化」と「オープンソース公開」を考慮し、両方を採用している場合には満点、どちらか一方を採用した場合には配点の半分を得るものとした。

この変更に伴い、現状での利用実績での評価項目は、表 で示した 9 項目から表 で示した 8 項目となった。

なお、「利用促進を図る際の障壁の除去」の観点においては、許諾契約有無は大きな差として存在することは明らかであることから、両者を区別することが妥当であるし、許諾契約有無の違いにより配点に差をつけることとした。

【「標準化・規格化の促進を図るハードルの低さ」の評価】

「標準化・規格化の促進を図るハードルの低さ」では、まったく異なる性質のアピールポイントを使って評価されることから単一の評価基準での配点を行うことができない。また、アピールポイントの強弱によって、細かく差をつけることが望ましい。

そこで、評価対象である「技術的アピールポイント」「標準化等のアピールポイント」「採用実績のアピールポイント」のそれぞれについて、アピールポイントの強弱が判定できるように 2 ポイントずつ割り当て（表 参照）、その合計点により配点を行うポイント制を採用（図 参照）することとした。なお、アピールポイントの判定は評価 B での閾値をベースに検討した。

表　アピールポイントの判定

評価 B での閾値			獲得ポイント数
OR 条件	技術的アピールポイント	方式委員会、及び、実装委員会に基準策定を任せる	● 安全性について技術的アピールポイントがあると方式委員会が判断すれば「1 ポイント」 ● 実装性について技術的アピールポイントがあると実装委員会が判断すれば「1 ポイント」
	標準化等のアピールポイント	以下のいずれかの規格において、「2 件以上」かつ「採用割合として 10%以上」となる件数での採用が同意されている（ただし、技術分類の有効数が 4 件以下の時に限り、「1 件」でもよいこととする） ● 政府系システム規格 ● 国際標準規格 ● 国際的な民間規格 ● 特定団体規格	● 左項目において、1 つまたは 2 つのいずれかの規格において条件を満たしている場合には「1 ポイント」 ● 左項目において、3 つ以上のいずれかの規格において条件を満たしている場合には「2 ポイント」
	採用実績のアピールポイント	以下のいずれかの条件を満たしている ● オープンソースプロジェクトで「2 件以上」かつ「採用割合として 10%以上」となる件数での採用があること ● 市販製品で、「提案会社・グループ会社以外での採用実績」があり、「採用割合として 10%以上」となる件数の採用実績があること	● 左項目において、いずれか 1 つの条件を満たしている場合には「1 ポイント」 ● 左項目において、両方の条件を満たしている場合には「2 ポイント」

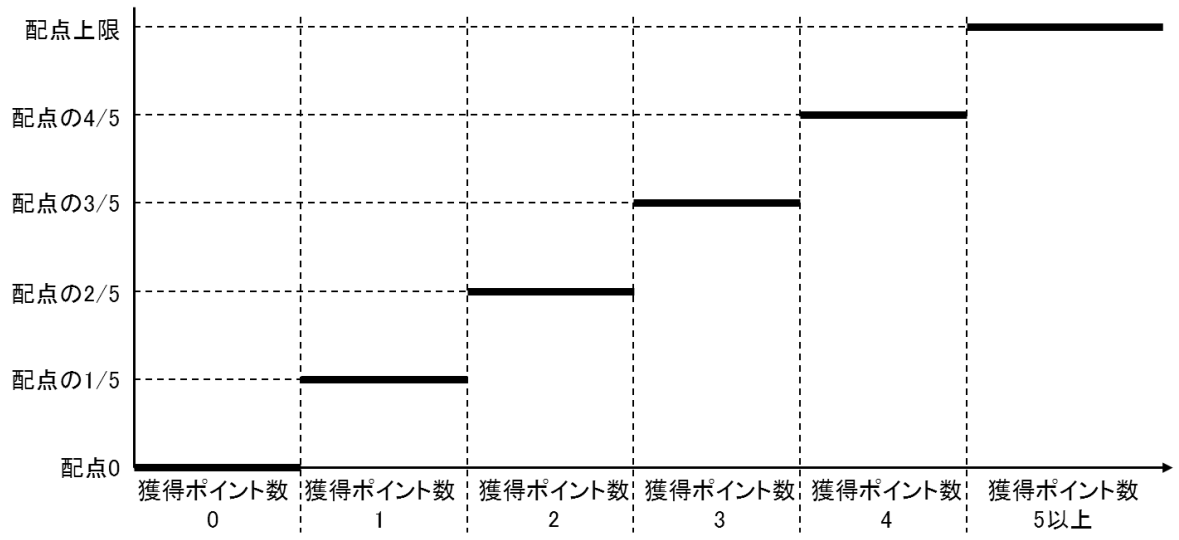


図　「標準化・規格化の促進を図るハードルの低さ」における配点

【「実装コスト低減／調達コスト低減を図るハードルの低さ」の評価】

「実装コスト低減を図るハードルの低さ」と「調達コスト低減を図るハードルの低さ」でも、異なる対象の利用実績のアピールポイントを使って評価されることから単一の評価基準での配点を行うことが難しい。そこで、図 の考え方を踏襲して、二つの利用実績によるアピールポイントの強弱を表 のように割り当て、図 のポイント制による配点を行うこととした。

表　アピールポイントの判定

獲得ポイント数	閾値
1 ポイント	採用割合 10%以上の利用実績が 1 項目
2 ポイント	採用割合 30%以上の利用実績が 1 項目、または 10%以上の利用実績が 2 項目
3 ポイント	採用割合 50%以上の利用実績が 1 項目、または 30%以上の利用実績が 2 項目

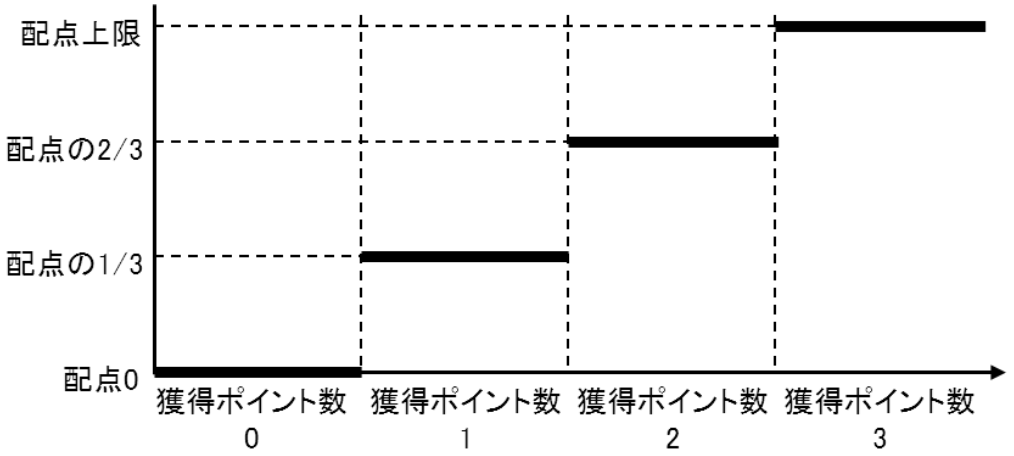


図　「実装コスト低減／調達コスト低減を図るハードルの低さ」における配点

【重要度による重み付けの是非】

表 にあるように、利用実績の評価に当たっては、システム・製品・規格等の重要度の違いによる重み付けを考慮すべきではないかとの認識を持ち、重み付けの方法を考慮することとなっていた。

しかしながら、実際に利用実績調査で調べた情報からでは、以下の理由により、適切な重み付けを行うに足る信頼できる客観的な根拠を得ることができなかった。そのような状況において、CRYPTREC として重み付けをつけることは、製品間に客観性に乏しい普及率や重要度という恣意的な基準を入れることが必要となり、むしろ客観性を損なう結果につながる恐れがある。このため、客観性を確保する観点から、重要度による重み付けをしないほうが公平であると判断した。

- 市販製品：
  様々な製品が調査対象となっているため、理想的には重み付けを行うべきと考える。しかし、現状においては、多くの市販製品についてどの程度利用されているかを判断する客観的かつ検証可能な、信頼できる根拠データを入手することは極めて困難である。事実、今回実施したアンケートの調査項目に「売上高」や「ライセンス数」を問う設問も用意されていたが、必ずしも回答が得られたわけではなく、また回答された内容が正しいかどうかを確認することもできなかった。そのような状況で、無理して重み付けを行うとすれば、「会社名」や「知名度」のみで判断せざるを得ず、結果としてミスリーディングを起こす懸念がある
- 政府系システム：
  政府系システムでの機密性保持の観点から、各府省庁の情報システム担当課の責任において調査対象システムを選定し、必要なデータのみを特例として回答いただいたものであり、回答内容についての重み付けを判断できる材料がない
- 各種規格：
  今回の調査対象は、暗号運用委員会にて選定・審議・承認された規格のみを対象に行われているため、重み付けを行う必要があるほどの重要度の違いがあるとは考えにくい
- オープンソースプロジェクト：
  今回の調査対象は、暗号運用委員会にて審議・選定されたオープンソースプロジェクトのみを対象に行われているため、重み付けを行う必要があるほどの重要度の違いがあるとは考えにくい

第 3 章　利用実績調査について

暗号技術の利用実態として、単に製品やシステムに“搭載されている”だけでなく、“実際に利用している”暗号技術を調べるのが理想的ではある。しかしながら、どの暗号技術を実際に利用しているかは設定や利用環境に依存し、販売会社等から得られる製品情報から判断することは現実には不可能である。このため、次善の方法として、製品やシステムでの搭載状況をもって採用実績とした。

また、広く利用されている製品や重要な製品と、あまり利用されていない製品との間での扱いについても、製品シェアやシステムの重要度等による重み付けをするのが理想的ではある。ただ一方で、現状においては、多くの市販製品についてどの程度利用されているかを判断する客観的かつ検証可能な、信頼できる根拠データを入手することは極めて困難であるのも事実である。そのような状況において製品間での重み付けをすることは、例えば「製造会社名・販売会社名」や「製品の知名度」あるいは「自称の販売シェア」などといった、客観性や検証可能性に乏しい情報をもとにした恣意的な算出方法によって製品間の重み付けをすることにもなりかねず、むしろ客観性を損なう結果につながる恐れがある。このため、公平かつ検証可能なデータのみをそのまま用い、重み付けをしないほうが客観性を確保できると判断した。

以上の観点を踏まえ、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[4]とほぼ同様の手法を踏襲するものとし、IPA が実施主体となって、2012 年 7 月～9 月にかけて実施された。詳細については、IPA ホームページに報告書が公開[5]されているので、そちらを参照されたい。

暗号運用委員会としては、IPA の調査が公平かつ客観的に実施されるようにするため、調査手法や調査対象の範囲、調査結果の集計方法等について、2012 年度第 1 回及び第 2 回での委員会において審議を行った。審議項目は以下のとおりであり、それらの審議結果は、IPA の調査に反映された。また、調査結果についても、第 3 回委員会での報告のほか、別途調査報告会を開催し、調査内容の確認を行った。

【応募暗号及び現推奨暗号リスト掲載暗号の応募者に対する調査】

以下に挙げる企業の暗号技術については、当該暗号技術の利用実態・採用状況を当該企業から入手することとした。

- EMC ジャパン（RSASSA-PKCS1-v1_5, RSA-PSS, RSA-OAEP, RSAES-PKCS1-v1_5, RC4）

[4] http://www.meti.go.jp/meti_lib/report/2010fy01/E001139.pdf
[5] http://www.ipa.go.jp/security/fy24/reports/cryptrec/crypto-algorithm/index.html

- NTT（PSEC-KEM, Camellia）
- KDDI（KCipher-2）
- ソニー（CLEFIA）
- 東芝（Hierocrypt-L1, Hierocrypt-3）
- 日本電気（CIPHERUNICORN-E, CIPHERUNICORN-A, PC-MAC-AES）
- 日立製作所（MUGI, MULTI-S01, Enocoro-128v2）
- 富士通（ECDSA, ECDH, SC2000）
- 三菱電機（MISTY1）

公平性を確保するため、当該企業からの回答内容については、「市販製品の販売会社へのアンケート調査」「政府機関に対する利用実績調査」「国際標準規格・民間規格等での採用実績調査」「オープンソースプロジェクトでの利用実績調査」のいずれかで入手できる調査結果と同程度の情報が含まれている場合に限り、有効回答としてカウントさせることとした。つまり、ある製品において、当該暗号技術が採用されていることが確認できたとしても、それ以外に採用されている暗号技術が特定できなかった場合には、その情報は参考情報として扱い、有効回答とは認めなかった。

なお、当該企業が詳細を把握していない他社製品や規格等については、連絡先や製品名、規格名等が明示されているものについて追跡調査を別途行い、詳細が判明したものについては有効回答に含めた。

【市販製品の販売会社へのアンケート調査】

市販製品の利用実績調査においては、公平性や客観性を保つ観点から、以下の点に留意して調査を実施するよう、助言を行った。

- 市販製品の調査対象に極端な偏りや調査対象漏れが生じないようにするために、暗号製品を区分するカテゴリ 20 個を暗号運用委員会が設定した。設定したカテゴリと代表的な製品例は表 の通り
- アンケート回答内容の精度を同じにするため、アンケート調査票は選択方式を基本とした。特に、製品に搭載されている暗号技術については、調査対象とした暗号技術名すべてを一覧表で提示し、そのなかから選択させる方式をとった
- アンケート回答内容の妥当性・信憑性について検証できるようにするため、回答内容をどのように確認できるのかを尋ねる質問項目をアンケート票に入れた。具体的には、表 に挙げるいずれの方法で確認できるのかを選択させる方法をとった
- 公平性・客観性の観点から、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こととし、アンケートを取る段階で注意喚起を行わせた

表　市販製品の調査カテゴリ

	大分類	小分類（代表的な製品例）
1	オペレーティングシステム	汎用 OS／携帯端末用 OS／VM
2	暗号化ツールキット／ライブラリ	暗号化ツールキット／ライブラリ
3	アプリケーションソフトウェア	暗号化メール関連ソフトウェア ファイル暗号化ソフトウェア（除外：OS、暗号化ツールキット） ブラウザ オンラインバンキングソフトウェア／オンライントレードソフトウェア／金融系ソフトウェア その他ソフトウェア全般
4	ネットワーク装置（無線含む）	ルータ・スイッチ イーサネット暗号化装置 VPN 装置 その他ネットワーク関連機器／ソフトウェア ネットワークシステム
5	サーバ	サーバ関連機器／ソフトウェア 電子認証局サーバ関連機器／ソフトウェア ユーザ認証サーバ関連機器／ソフトウェア タイムスタンプサーバ関連機器／ソフトウェア （電子メール用）署名生成サーバ関連機器／ソフトウェア 業務支援ソフトウェア
6	ストレージ	ストレージ関連機器／ソフトウェア データベースソフトウェア
7	端末	PC 本体（CPU／MPU）／周辺機器（ソフトウェアを除く） PDA／スマートフォン／携帯電話 ハンディターミナル／POS／ATM／関連ソフトウェア
8	外部記憶装置	USB メモリ／SD メモリカード／ハードディスク／関連ソフトウェア
9	認証機器	認証デバイス関連機器
10	システム	シンクライアントシステム 情報漏洩対策システム テレビ会議システム 電話・無線・音声システム シネマコンテンツ配信システム オンライン教育システム 見守りシステム DRM／著作権保護システム

表　市販製品の調査カテゴリ（続）

	大分類	小分類（代表的な製品例）
11	カード	IC カード／SIM カード／関連ソフトウェア カードリーダライタ／関連ソフトウェア
12	IC チップ	汎用 IC 特定用途 IC（除外：IC カード、SIM カード、CPU、HSM、TPM、センサーチップ、消耗品認証用チップ等） IC 組込用ソフトウェア
13	ハードウェアセキュリティモジュール	HSM TPM
14	複合機・プリンタ	複合機／プリンタ関連機器／関連ソフトウェア
15	情報家電・生活用品	ネットワーク制御型家電／関連ソフトウェア デジタルカメラ／Web カメラ／関連ソフトウェア カーナビ／車載機器／関連ソフトウェア ゲーム機
16	センサー	スマートメータ 監視カメラ RFID／タグ センサー（センサーチップ） NFC セキュリティ製品（除外：カード）／関連ソフトウェア
17	消耗品認証	インクカートリッジ認証 消耗品認証 機器認証
18	サービス	データ預かりサービス クラウドサービス 大容量データ転送サービス
19	特注品・SI システム	顧客仕様に基づいて製造され、納入された特注品、SI システム（一般へ販売はしていない）
20	その他	上記のいずれにも該当しないもの

表　アンケート回答内容の確認方法

	回答内容の確認方法
Lev. 1	搭載されている暗号技術について公開情報等（URL 等）に記載されており、当該情報から回答内容を検証できる
Lev. 2	公開情報はないが、要求があれば回答内容を検証できる情報を提供してもよい
Lev. 3	公開情報はないが、NDA を締結すれば、回答内容を検証できる情報を提供してもよい
Lev. 4	回答内容を検証できる情報はあるが、提供はできない
Lev. 5	回答内容を検証できる情報があるかどうか判明していない／確認できない

また、アンケートの集計において、以下の視点で集計したものを評価 A 及び評価 B で使用する利用実績評価の基礎データとすることにした。

- 調査カテゴリをまたがる製品の利用時における重複カウントの扱い

  OS や暗号ライブラリ、IC チップなどは、単体として利用される場合のほか、上位の製品に組込まれて使われているケースも多く考えられる。この場合、例えば、暗号ライブラリ S に搭載されている暗号技術 A は、当該暗号ライブラリを組み込んでいる製品 X においても自動的に搭載されることとなる（図 参照）。

  このようなケースについて、暗号技術 A の採用実績を「暗号ライブラリ S のみ」とするか、「暗号ライブラリ S と製品 X の両方」とみなすかについて検討を行った。

  検討の結果、ある製品（暗号ライブラリ S）が他製品（製品 X）に組込まれて使われることは、当該製品 S がより重要・基盤的な製品であることが反映された結果であると解釈できる。このことは、当該製品に搭載されている暗号技術 X にとっても、重要性の高い製品に組込まれていることと同義であり、一種の重み付けが行われているともいえるため、暗号技術 X の利用実績としては「暗号ライブラリ S と製品 X の両方」とみなすほうが妥当であると判断した

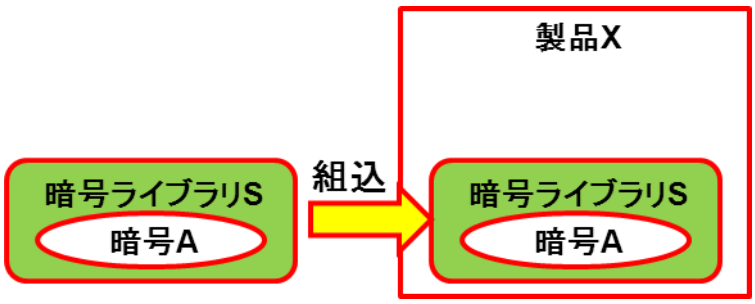


図　調査カテゴリをまたがる製品の利用

- データの集計対象について

  アンケート調査（アンケート配布社数：1849；有効回答：会社数 127，製品数 443）、及び公開情報を基にみずほ情報総研が調査（調査対象：会社数 35，製品数 90）し、データが入手できた対象の内訳は表 のとおりである。

  このうち、公平性・客観性の観点から、何らかの手段で回答内容の検証が可能な担保がある Lev. 1～Lev. 3 の情報のみを活用することとした。この結果、利用実績評価の基礎データとなった市販製品の総数は 469 となった。

表　市販製品利用実績調査対象の内訳

製品カテゴリ	該当数	64 ビットブロック暗号	128 ビットブロック暗号	ストリーム暗号	モード	メッセージ認証コード	署名	守秘・鍵交換	ハッシュ関数	エンティティ認証
1: オペレーティングシステム	**11**	7	9	5	7	8	9	8	11	0
2: 暗号化ツールキット／ライブラリ	**65**	36	58	27	34	21	34	32	34	14
3: アプリケーションソフトウェア	**94**	35	63	26	18	13	15	18	46	12
4: ネットワーク装置	**94**	69	82	33	29	50	52	67	78	14
5: サーバ	**16**	7	9	3	2	1	7	9	9	3
6: ストレージ	**25**	17	22	7	7	2	13	18	20	9
7: 端末	**12**	3	11	2	0	3	4	3	4	0
8: 外部記憶装置	**33**	7	25	0	3	5	11	8	13	3
9: 認証機器	**6**	0	6	0	0	0	0	0	1	0
10: システム	**13**	4	8	5	1	0	0	1	3	4
11: カード	**15**	11	10	0	10	8	9	8	10	0
12: IC チップ	**13**	7	7	1	1	0	3	2	5	1
13: ハードウェアセキュリティモジュール	**21**	21	19	11	14	11	19	18	20	0
14: 複合機・プリンタ	**44**	42	38	32	31	5	16	18	34	11
15: 情報家電・生活用品	**6**	3	5	2	3	3	3	1	4	1
16: センサー	**2**	1	2	1	1	0	1	1	1	0
17: 消耗品認証	**0**	0	0	0	0	0	0	0	0	0
18: サービス	**37**	16	21	10	3	4	19	15	24	7
19: 特注品	**13**	12	4	2	0	0	1	1	3	1
20: その他	**13**	4	4	4	4	4	7	4	8	0
市販製品総合	**533**	**302**	**403**	**171**	**168**	**138**	**223**	**232**	**328**	**80**
市販暗号モジュール（#1,#2,#11,#12,#13）	**125**	**82**	**103**	**44**	**66**	**48**	**74**	**68**	**80**	**15**

表　回答内容の信頼度

	回答内容の確認方法	該当数
Lev. 1	搭載されている暗号技術について公開情報等（URL 等）に記載されており、当該情報から回答内容を検証できる	351
Lev. 2	公開情報はないが、要求があれば回答内容を検証できる情報を提供してもよい	66
Lev. 3	公開情報はないが、NDA を締結すれば、回答内容を検証できる情報を提供してもよい	52
Lev. 4	回答内容を検証できる情報はあるが、提供はできない	20
Lev. 5	回答内容を検証できる情報があるかどうか判明していない／確認できない	44

【政府系システム・規格に対する調査】

政府系システム・規格については、総務省及び経済産業省を調整のうえ、各府省庁の情報システム担当課の協力を得て調査を実施した。なお、政府系システムでの機密性保持の観点から、担当課の責任において調査対象システム・規格を選定し、必要なデータのみを特例として回答を得た。回答があった総数は、政府系システムについては 8 府省庁 77 システム、政府系規格については 5 規格である。

なお、SSL/TLS または IPsec を利用している政府系システムについては、当該プロトコルとして実装必須となっている表 の暗号技術が当然搭載されているとの判断に立ち、回答内容に当該暗号技術の利用実績として漏れがないかを確認し、適切にカウントした。

表　実装必須と判断した暗号技術

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

また、公開情報からみずほ情報総研が独自に調査した表 の政府系システム規格について追加することを承認した。

表　公開情報から追加した政府系システム規格

電子署名法	電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針
公的個人認証	認証業務及びこれに附帯する業務の実施に関する技術的基準
商業登記認証局	「電子証明書の方式等に関する件（告示）」
医療情報システムの安全管理に関するガイドライン	医療情報システムの安全管理に関するガイドライン 第 4.1 版
政府認証基盤（GPKI）	政府認証基盤（GPKI）政府認証基盤相互運用性仕様書　平成 13 年 4 月 25 日　平成 24 年 3 月 23 日改定
住民基本台帳法（昭和 42 年法律第 81 号）	住民基本台帳カード Version 2 組込みソフトウェア プロテクションプロファイル
標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式	標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式第八条第一号及び第二号の規定に基づくスクランブルの方式　総務省告示第三百二号

【国際標準規格・国際的な民間メジャー規格・特定団体規格に対する調査】

国際標準規格及び国際的な民間メジャー規格については重要な規格の調査漏れが起きないようにするため、2012 年度第 1 回及び第 2 回暗号運用委員会にて、表 及び表 に示す規格を調査対象に含めるよう助言した。その他、みずほ情報総研が独自に調査した表 に示す規格について、調査対象に追加することを承認した。

以上の結果、国際標準規格 12 種類、国際的な民間メジャー規格 15 種類（全 108 規格）が調査対象となった。

特定団体規格については、社会的にも重要なインフラとして多数の利用者を持つ大規模システムを規定するものもあり、調査対象としての重要度は高い。しかしながら、これらの規格は、サービス提供事業者やインフラ構築会社、会員企業等にのみ仕様が公開されていることも少なくない。

このため、当初から確実に協力が得られる見込みが立たない状況での調査を実施する必要があることから、明らかに利用者が多く、社会的にも重要なインフラやサービスを提供している団体を対象に調査依頼を行い、最終的に回答が得られた 3 団体のみ（表 参照）を 2012 年度第 3 回暗号運用委員会にて調査対象として承認した。このほか、特定団体規格ながら仕様が公開されている 6 団体（表 参照）についても追加することを承認した。

以上の結果、特定団体規格 24（アンケート調査：16（3 団体）、文献調査数：8（6 団体））が調査対象となった。

なお、この調査過程では、調査拒否の団体が大多数であった中で、積極的に協力していただいた団体がある。この団体からは多数の仕様に対する回答が寄せられたため、全体の回答数に対する割合が当該団体の回答に大きく依存する形となった。暗号運用委員会では、この割合の是非について慎重に審議を行ったが、①今回の調査結果全体の傾向と齟齬がないこと、②当該割合の違いが電子政府推奨暗号の選定に影響を与えることがないこと、を確認し、最終的に当該団体からの全ての回答を認めることとした。

表　暗号運用委員会が調査対象として指定した国際標準規格

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

表　暗号運用委員会が調査対象として指定した国際的な民間メジャー規格

名称	調査対象数
IETF TLS	20
IETF IPsec	34
IETF S/MIME, CMS	16
IETF PGP	3
IEEE802.11i	1
RSA PKCS#11	1
EMV	2
3GPP	2
3GPP2	3
OMA	1

表　みずほ情報総研が独自に調査対象に追加した規格

	名称	調査対象数
国際標準規格	ITU-T Y.SecMechanisms (NGN Security Mechanisms)	
	ITU-T H.233/H.234 (audiovisual services)	
	ICAO Doc 9303 (Machine readable travel documents)	
国際的な民間メジャー規格	IETF DNSSec	10
	IETF Kerberos	9
	IEEE1619	1
	Trusted Computing Group	3
	その他	2

表　特定団体規格についてのアンケート回答が得られた特定団体名

ARIB
Marline Joint Development Association
一般財団法人日本データ通信協会

表　みずほ情報総研が独自に調査対象に追加した特定団体規格

団体名	規格名
ZigBee SIG-Japan	ZigBee 和訳仕様書
Bluetooth SIG, Inc	Bluetooth 仕様書
Wi-Fi Alliance	WiFi 仕様書
IPTV フォーラム	デジタルテレビ ネットワーク(デジタルテレビ情報化研究会／IPTV Forum Japan) IPTVFJ STD-0001～0009
DCCJ	Digital Cinema Initiatives, LLC　DCI 規格（V1.0)
AACS	AACS 仕様書

【オープンソースプロジェクトに関する調査】

オープンソースプロジェクトは多数存在するため、調査対象に極端な偏りが生じたり、重要なオープンソースプロジェクトの調査漏れが起きないようにする必要がある。

このため、2012 年度第 1 回及び第 2 回暗号運用委員会の審議において、表 に示す 24 個のオープンソースプロジェクトを調査対象とすべきと助言した。これらは、調査対象としたカテゴリにおける代表的なオープンソースプロジェクトである。

表　暗号運用委員会が調査対象として指定したオープンソースプロジェクト

カテゴリ		プロジェクト名	バージョン
OS（カーネル）	汎用 OS	Linux	3.4.7
		Debian	6.0.5
		FreeBSD	9.0
	組込 OS	Android	4.0
アプリケーション開発ツール	言語	Java	SE 7
		Bouncy Castle	(jdk15-17)1.47
		PHP	5.4.5
	開発環境	Subversion	1.7.6
		Eclipse	4.2
	アプリケーションサーバ	Samba	3.6.6
		Tomcat	7.0.29
インターネット	Web サーバ	Apache	2.4.2 (released 2012-04-17)
	メールサーバ	Qmail	1.06
	電子メール系	Thunderbird	14.0
	ブラウザ	Firefox	14.0.1
		Webkit	r125966
暗号化ライブラリ		NSS	3.13.5
		OpenSSL	1.0.1c
		GnuPG	2.0 (2.0.19)
		MCrypt	2.6.8
データベース		MySQL	5.5.25a
		PostgreSQL	9.1.4
アプリケーション	アプリケーション	OpenOffice	3.4.0
	圧縮ツール	7-zip	9.2

オープンソースプロジェクトの中には強い依存関係にあるものが少なからずある。例えば、オープンソースプロジェクト A に採用されると、別のオープンソースプロジェクト B でも採用されたり、B の中に A がそのまま組込まれたりするような関係である。そのような依存関係を表 に挙げたすべてのプロジェクトに対して考慮することは現実的ではないものの、「相関が明らかに強そうである」という組み合わせについては極力一つとして集計するほうが望ましいと判断した。

暗号運用委員会としては、そのような特に依存関係が強いオープンソースプロジェクトの組み合わせとして以下の 3 組を指定した。例えば、Linux と Debian について、両者に搭載されている場合でも「1」として集計するということである。

- 「Linux 及び Debian」
- 「Qmail 及び OpenSSL」
- 「Firefox、Thunderbird、及び NSS」

これにより、調査数としては 24 個であったが、データ集計数としてはオープンソースプロジェクト全体で 20 個、暗号モジュールとして 7 個（OS と暗号ライブラリの合計）となった。

なお、オープンソースプロジェクトでは、様々な他のオープンソースプロジェクトの成果物を同梱する場合も少なくなく、バージョンも頻繁に更新される。そのため、公平性を確保する観点から、調査に当たっては以下のルールを採用するよう助言した。

- 調査対象となるオープンソースプロジェクトを入手し、当該プロジェクトが管理するソースコードにおいて、みずほ情報総研が確認できなかった暗号技術は利用実績の対象外とする
- 調査対象となるオープンソースプロジェクトにおいて、同梱されている他オープンソースプロジェクトが管理するソースコード中に含まれる暗号技術についても利用実績の対象外とする。例えば、Android の external 直下のフォルダに含まれる Camellia について、Camellia は Android に搭載されているとは認めないこととした
- その後のバージョンのオープンソースプロジェクトに含まれた暗号技術であったとしても、調査対象となるバージョンのプロジェクトに含まれていなければ、当該暗号技術の利用実績対象外とする
- エンティティ認証のソースコードには、ISO/IEC 9798 等の明示がないため、調査対象外とする

第 4 章　今後に向けて

次年度の CRYPTREC 体制の改組に伴って、現行の暗号方式委員会・暗号実装委員会・暗号運用委員会の「3 委員会」体制から、暗号技術の安全性評価を中心とした技術的な検討課題を主に担当する「暗号技術評価委員会」と、セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討課題を主に担当する「暗号技術活用委員会」の「2 委員会」体制に移行する予定である（図 参照）。

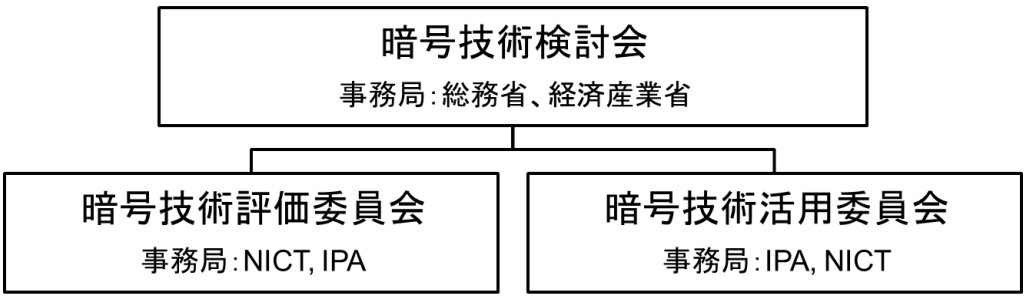


図　次年度の CRYPTREC 体制

現在の暗号運用委員会の担当業務の大半は暗号技術活用委員会に引き継がれる見通しであり、暗号技術活用委員会での検討項目としては、以下の 3 点が計画されている。

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）
② 暗号技術の利用状況に係る調査及び必要な対策の検討等
③ 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）

そこで、暗号運用委員会としては、上記検討項目に関連し、暗号技術活用委員会に引き継ぐべき課題についての論点整理を行った。主な論点整理の結果は以下のとおりである。

- 暗号政策に関する中長期的視点からの取り組み、及び暗号利用促進によるセキュリティ産業の競争力強化の視点

  （検討方針案） 国産暗号の活用を視野に、暗号技術を活用した製品・サービスの開発の利用促進策を検討する

  - 暗号がないと色々なことができないのは事実だが、暗号だけで成り立っているビジネスもほとんどない。暗号技術と産業競争力強化の相関性は薄いとの指摘に対し、現状を一度俯瞰してから暗号政策をどうするかを組み立てるべき

- 暗号政策上の課題の構造がどのようになっているのかを最初に時間をかけて検討すべき
- 「電子政府システムを安全に維持していくために、ビジネスとは関係なく日本としてやらなければならないこと」と「ビジネスに関連して、セキュリティ関連産業の競争力強化策としてやるべきこと」は分けて議論すべき

- 暗号人材育成に向けた取組検討の視点

（検討方針案）プライバシー保護と個人情報活用の両立へのニーズ等の昨今の状況を踏まえながら暗号人材育成策を検討する

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

- 国際標準化 WG 設置の視点

（検討方針案）主に日本から提案する暗号技術の横断的な国際標準化活動に関する取組を実施する

- 色々ある国際標準化の相互の関連性について、暗号アルゴリズムがどこでどう参照されているかを整理すべき
- 暗号標準規格を作る側だけでなく、暗号標準規格を参照する側（組込む側・使う側）もメンバになっていただくべき

- 暗号技術の普及促進・理解促進へ取り組みの視点
  - 適切な暗号利用に対する助言や、脆弱性に対する公的な調査ができる体制についても検討すべき
  - CRYPTREC の対象を暗号アルゴリズムだけに限らず、Web 脆弱性や SNS での攻撃など、暗号がらみで社会にインパクトがある事例も調査対象に含めるべき
  - 運用ガイドラインを整備すべき。その際、想定読者の立場を考慮して記述すべき

付録

知的財産権の使用の権利に係る確認書

2012 年 9 月 30 日時点における各暗号技術の特許ライセンス宣言の要旨は以下のとおりである。

実際の使用に当たっては、CRYPTREC ホームページに掲載される最新の特許ライセンス宣言にて原本を確認すること。なお、特許ライセンス宣言の解釈について質問がある場合には、各暗号技術の提案会社の問い合わせ窓口に直接問い合わせること。CRYPTREC に問い合わせをしても一切取次ぎや回答を行わない。

電子政府推奨暗号リストに掲載されている暗号技術（ABC 順）

Camellia （提案会社：日本電信電話株式会社・三菱電機株式会社）

（１）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、**許諾契約の締結を問わず、非差別的かつ無償で通常実施権（または著作物の利用）を許諾**する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、（１）又は下記（２）の条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

ECDH （提案会社：富士通株式会社）

（A）上記１．の暗号アルゴリズムの使用に当たっての**当社保有知的財産権（特許権又は実用新案権等（出願中のものを含む））は存在しない**。

当社が認識する、上記１．の暗号アルゴリズムの使用に当たっての他社保有知的財産権等に関する注意事項

特許所有者、及び SECG のウェブサイトを参照のこと。特許技術の使用許諾が必要となる場合には、下記 URL を参照のうえ、特許所有者との交渉をお願いします。

http://www.secg.org/index.php?action=secg,about_patents

http://www.secg.org/download/aid-398/certicom_patent_letter_SECG.pdf

ECDSA （提案会社：富士通株式会社）

（A）上記１．の暗号アルゴリズムの使用に当たっての**当社保有知的財産権（特許権又は実用新案権等（出願中のものを含む））は存在しない**。

当社が認識する、上記１．の暗号アルゴリズムの使用に当たっての他社保有知的財産権等に関する注意事項

特許所有者、及び SECG のウェブサイトを参照のこと。特許技術の使用許諾が必要となる場合には、下記 URL を参照のうえ、特許所有者との交渉をお願いします。

http://www.secg.org/index.php?action=secg,about_patents
http://www.secg.org/download/aid-398/certicom_patent_letter_SECG.pdf

KCipher-2 （提案会社：KDDI 株式会社）

（1）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、許諾契約の締結を問わず、非差別的かつ無償で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、（1）又は下記（2）の条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

RSAES-PKCS1-v1_5 （提案会社：EMC ジャパン株式会社）

（A）上記１．の暗号アルゴリズムの使用に当たっての当社保有知的財産権（特許権又は実用新案権等（出願中のものを含む））は存在しない。

RSA-OAEP （提案会社：EMC ジャパン株式会社）

（A）上記１．の暗号アルゴリズムの使用に当たっての当社保有知的財産権（特許権又は実用新案権等（出願中のものを含む））は存在しない。

RSA-PSS （提案会社：EMC ジャパン株式会社）

（A）上記１．の暗号アルゴリズムの使用に当たっての当社保有知的財産権（特許権又は実用新案権等（出願中のものを含む））は存在しない。

RSASSA-PKCS1-v1_5 （提案会社：EMC ジャパン株式会社）

（A）上記１．の暗号アルゴリズムの使用に当たっての当社保有知的財産権（特許権又は実用新案権等（出願中のものを含む））は存在しない。

推奨候補暗号リストに掲載されている暗号技術（ABC 順）

CIPHERUNICORN-A （提案会社：日本電気株式会社）

（3）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）（2）（3）のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

CIPHERUNICORN-E （提案会社：日本電気株式会社）

（3）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保

有知的財産権のすべてに関し、いかなる者に対しても、非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）（2）（3）のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

CLEFIA （提案会社：ソニー株式会社）

（3）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）（2）（3）のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

Enocoro-128v2 （提案会社：株式会社日立製作所）

（3）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）（2）（3）のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

Hierocrypt-3 （提案会社：株式会社東芝）

（3）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）（2）（3）のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

Hierocrypt-L1 （提案会社：株式会社東芝）

（3）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）（2）（3）のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

MISTY1 （提案会社：三菱電機株式会社）

（2）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、許諾契約の締結を条件として、非差別的かつ無償で通常実施権（または著作物の利用）を許諾する。ただし、

当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）又は（2）の条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

MUGI （提案会社：株式会社日立製作所）

（1）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、**許諾契約の締結を問わず、非差別的かつ無償で通常実施権（または著作物の利用）を許諾**する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、（1）又は下記（2）の条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

MULTI-S01 （提案会社：株式会社日立製作所）

（3）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、**非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾**する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）（2）（3）のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

PC-MAC-AES （提案会社：日本電気株式会社）

（3）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、**非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾**する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）（2）（3）のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

PSEC-KEM （提案会社：日本電信電話株式会社）

（1）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、**許諾契約の締結を問わず、非差別的かつ無償で通常実施権（または著作物の利用）を許諾**する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、（1）又は下記（2）の条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

SC2000 （提案会社：富士通株式会社）

（3）当社は、上記１．の暗号アルゴリズムの使用に当たって、上記２．（B）の当社保有知的財産権のすべてに関し、いかなる者に対しても、**非差別的かつ妥当な条件（無償を除く）で通常実施権（または著作物の利用）を許諾**する。ただし、当該暗号アルゴリズムに関連する他の知的財産権者であって、上記（1）（2）（3）のいずれかの条件で自らの知的財産権の実施を許諾しない者に対しては、この限りではない。

発行日　2013 年 4 月 30 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
（技術本部　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