CRYPTREC Report 2009

平成 22 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、独立行政法人情報通信研究機構及び独立行政法人情報処理推進機構によって共同で運営されている暗号運用委員会の 2009 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。

暗号運用委員会は、このように次期リストを策定・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・検討を行うために、今年度から新たに設置された委員会である。本委員会では、暗号アルゴリズムに関する検討を行う暗号方式委員会、及び、暗号モジュールに関する検討を行う暗号実装委員会と連携して、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関する検討を行うこととなっている。

2009 年度は、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」に掲載された暗号技術の利用者に関する分析を行うとともに、「電子政府推奨暗号リスト」と「推奨候補暗号リスト」を区分するため、市場における利用実績及び国際標準に関する評価の考え方について議論を行った。次年度では、これらの議論を踏まえ、暗号技術の製品化・利用実績等についての評価項目や評価基準、及び、「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。たとえば、電子政府において電子署名や GPKI 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つい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、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 サイトで参照することができる。

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

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

委員会構成

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

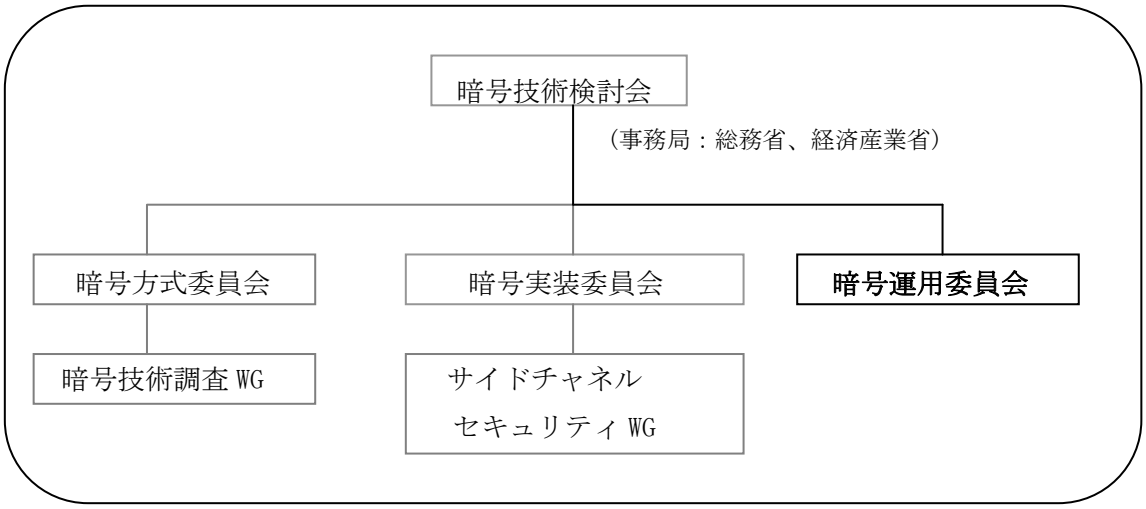


図 1　CRYPTREC 体制図

委員名簿

暗号運用委員会

委員長	佐々木 良一	東京電機大学 教授
委員	宇根 正志	日本銀行 企画役
委員	大岩 寛	独立行政法人産業技術総合研究所 研究員
委員	菊池 浩明	東海大学 教授
委員	小松 文子	独立行政法人情報処理推進機構 ラボラトリー長
委員	手塚 悟	東京工科大学 教授
委員	松尾 真一郎	独立行政法人情報通信研究機構 主任研究員
委員	北村 伸弘	日本電気株式会社 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 研究主務
委員	下江 達二	富士通株式会社 部長
委員	羽根 慎吾	株式会社日立製作所 主任研究員
委員	前田 司	RSA セキュリティ株式会社 本部長
委員	宮崎 一哉	三菱電機株式会社 チームリーダ

オブザーバー

中嶋　良彰	内閣官房 情報セキュリティセンター
山口　利恵	内閣官房 情報セキュリティセンター
根本　農史	内閣官房 情報セキュリティセンター
松本　和人	総務省 行政管理局
佐々木　信行	総務省 情報流通行政局
島田　淳一	総務省 情報通信国際戦略局
古賀　康之	総務省 情報通信国際戦略局
梶原　亮	総務省 情報通信国際戦略局
齊藤　修啓	総務省 情報通信国際戦略局
山中　豊	経済産業省 産業技術環境局
日高　隆	経済産業省 大臣官房情報システム厚生課
下里　圭司	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

事務局

独立行政法人 情報通信研究機構 （篠田陽一、田中秀磨、松尾真一郎、側高幸治、黒川貴司、金森祥子、笠井祥）

独立行政法人 情報処理推進機構（矢島秀浩、山岸篤弘、大熊建司、神田雅透、小暮淳、近澤武、星野文学、鈴木幸子）

第1章　　2009 年度の活動内容と成果概要

1.1. 活動の概要

1.1.1. 活動目的

現在の電子政府推奨暗号リストの策定から 5 年余りが経過し、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が進展している状況にあることから、CRYPTREC では、電子政府推奨暗号リストの改訂に向けた検討を行っているところであり、新しい電子政府推奨暗号リストに掲載される暗号については、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」の観点も取り入れることとしている。また、リスト掲載暗号の危殆化リスクが高まった際には、すぐにリストから削除するのではなく、「運用監視暗号リスト」に掲載し、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予定である。

これまで、暗号技術検討会では、「電子政府推奨暗号の安全性及び信頼性確保のための調査・検討」として「暗号アルゴリズム等を主な対象とする調査・検討」及び「暗号実装関連技術を主な対象とする調査・検討」を行ってきており、これらの検討事項に関する技術的な検討を「暗号技術監視委員会」及び「暗号モジュール委員会」において行っていたところである。

本年度、新たに設置された本委員会では、今後、新しい電子政府推奨暗号リスト（以下「次期リスト」という。）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。

1.1.2. 暗号運用委員会の開催状況

2009 年度の暗号運用委員会は、計 2 回開催された。各回会合の概要は表 1 のとおりである。

表 1　2009 年度暗号運用委員会の開催状況

回	開催日時	主な議題
第 1 回	2009 年 10 月 23 日	暗号運用委員会活動計画についての検討 電子政府推奨暗号リストに関する検討
第 2 回	2010 年 2 月 22 日	国際標準化及び市場での利用実績に関する検討 2009 年度暗号運用委員会の活動報告(案)についての検討

1.2. 活動方針

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」について評価方針や評価基準について検討を行う。また、電子政府推奨暗号リストと国際標準技術等との整合性についても検討する。

また、次期リスト策定における「運用監視暗号リスト」に掲載された暗号技術の取り扱い方針について検討する。システム運用者の観点から、今後危殆化により移行が必要とされた場合、より円滑な作業を可能にするための調査・検討を行う。

1.3. 活動内容と成果概要

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、暗号技術検討会において、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こととなった。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（以下、「3 リスト」という。）、リストガイドから構成され、CRYPTREC 暗号リスト(仮称)として公開することとなった。安全性が確認された暗号技術は、3 リストのいずれかに登録されることになり、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

（１）電子政府推奨暗号リスト

CRYPTREC により安全性が確認され、かつ市場において利用実績が十分である暗号技術リスト。電子政府構築（政府調達）の際には当該技術の利用を推奨する（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。

（２）推奨候補暗号リスト

CRYPTREC により安全性が確認されているが、市場において利用実績が十分でない普及段階にある暗号技術が登録されているリスト。今後、利用が期待される新規技術等はここに分類される。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。

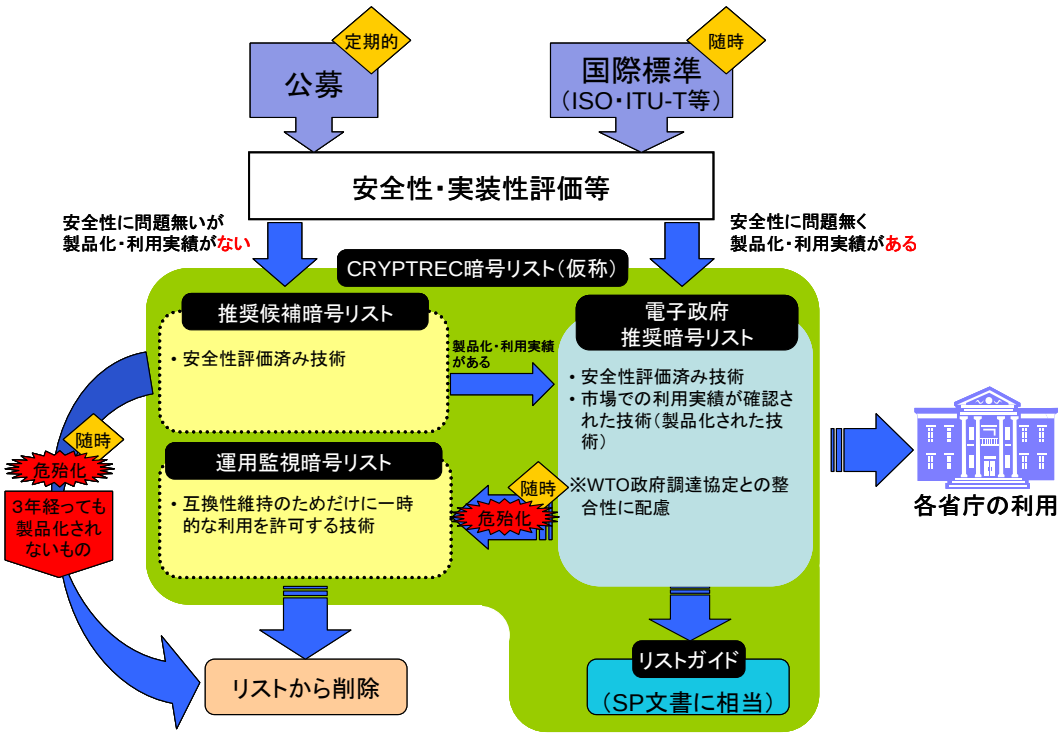
（３）運用監視暗号リスト

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。

（4）リストガイド

電子政府で利用されている、あるいは利用する可能性のある暗号技術について、その技術概要と、推奨する利用方法を記述します。また、次期リストに記載された技術の中で、安全性を維持するため正しいパラメータの設定が要求される技術における具体的なパラメータ設定方法の記述を行う。さらに、将来必要になると予想されるセキュリティ技術については、その開発状況や利用可能性について記載する。リストガイドは、システム運用者及び設計者の利用や、システム利用者への啓発を目的とする。



今年度は、暗号運用委員会では、3 リストの参照者の分析を行うとともに、電子政府推奨暗号リストと推奨候補暗号リストを区分するため、市場における利用実績及び国際標準に関する評価の考え方、危殆化した暗号技術として運用監視暗号リストに登録された暗号技術の扱い等について議論した。具体的な活動内容は以下の通り。

1.3.1. 電子政府推奨暗号リストの参照者の分析

暗号技術の製品化、利用実績等の評価に当たって、電子政府推奨暗号リストに掲載された暗号技術の利用者について整理を行った。

まず、電子政府を構築するために情報システムを調達する政府が第一義的な利用者となる。各府省が情報システムの構築に当たり暗号を利用する場合には、可能な限り「電子政府推奨暗号リスト」に掲載された暗号の利用を推進することとしている他、「政府機関の情報セキュリティ対策の統一基準（第４版）」（2009 年 2 月情報セキュリティ政策会議）においては、暗号化及び電子署名のアルゴリズムについてリストに掲載されたものが使用可能な場合には、それを

使用することとしている。

特定の暗号技術についての電子政府における利用実績は、次期リストの運用に当たっては重要な指標となる。

次に、暗号技術の製品化状況の評価に当たっては、暗号技術、暗号ライブラリ、暗号モジュール等の開発を行う暗号ベンダが暗号技術をどのように市場に供給しているかということも重要な指標となり得る。

その他、暗号ベンダの提供する暗号ライブラリや暗号モジュール等を利用して、特定の目的の情報システムを構築し、政府等に納入するシステムインテグレータや政府が調達することとなるような暗号を組み込んだコンシューマ向けの製品や電子政府と関わる認証業務等を行う製品・サービス提供者が電子政府推奨暗号リストの参照者と考えられる。

製品化、利用実績等の評価に当たっては、以上の 4 者を対象とした調査等が必要と考えられ、今後具体的な調査手法について検討を行う必要がある。

1.3.2. 市場における利用実績に関する考え方

IT 製品には、様々な暗号技術が用いられていることから、すべての暗号アルゴリズムの利用実績を網羅的に調査することは困難である。このため、利用実績に関する判断基準として、例えば、一つの製品でも搭載実績があれば利用実績があればよいと考える方法、搭載されている製品の重要性を加味して重要と判断されたアプリケーションへの搭載実績を利用実績とする方法など、以下の例が考えられる。

① 搭載されている製品が一つでもあることを利用実績とする判断方法の例

- 暗号アルゴリズム開発会社自身が販売する部品・製品への搭載事例があること
- 暗号アルゴリズム開発会社以外の会社等が販売する部品・製品への搭載事例があること
- JCMVP 等の関連制度の認証を受けている製品への搭載事例があること

② 搭載されている製品の重要性を加味して利用実績を検討する方法の例

- 主要なオープンソースソフトウェア(Linux など)への搭載事例があること
- 主要なアプリケーションでの搭載事例があること

暗号技術の利用実績については、どのような考え方が適切か、暗号アルゴリズムが搭載された製品の市場シェア・販売数量・販売額等について考慮すべきか、具体的にどのような調査方法が有効と考えられるか等の観点から、議論を行い、以下のような意見があげられ、さらに検討を続けることとなった。

- 利用実績が多い暗号の方が安全性評価の対象になり易いので、利用実績が少なく安全性評価の機会が少ない暗号よりも、利用実績が多く安全性評価の機会が多い暗号の方が安全性の面で良いと考えられる。
- 導入後のサポートへの期待という意味でも、製品化・普及の評価は意味があると考えられる。

- 業界で採用している暗号とこれから利用を推進していく暗号において同じ基準で評価するのは適切ではないのではないか。
- デファクト暗号についてのコンセンサスは概ね取れているものと考えられるが、明確な基準を設けるのは難しい。
- 暗号モジュールのセキュリティ機能に関する動作確認をしておくことは調達において重要であることから、JCMVP 認証製品への搭載の有無も暗号アルゴリズムの利用実績を評価するうえでの基準とすべきと考えられる。

1.3.3. 国際標準についての考え方

政府等が情報システムを調達するに当たっては、WTO 政府調達協定と整合的に調達する必要がある。WTO 政府調達協定では、技術仕様について適当な場合には国際標準が存在するときは当該国際標準等に基づいて定めることとされていることから、次期リストに登録される暗号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。

国際標準の観点からの評価を実施するため、暗号技術がどのような条件を満たせば、国際標準と考えることが適当か検討を行った。

例えば、国際機関である国際標準化機構(ISO)、国際電気標準化会議(IEC)、国際電気通信連合(ITU)において、暗号技術がアルゴリズムとして標準化されている場合、アプリケーションやシステムの規格において暗号アルゴリズムが指定されている場合がある他、事実上の標準として採用されている暗号技術の標準を定めている業界団体や特定の国、組織等があり、国際機関と類似した標準化が行われており、具体的には以下のような例がある。

① 国際標準化機関が定めた標準

＜例＞

○国際標準化機構（ISO）、国際電気標準会議（IEC）[1]

ISO/IEC でアルゴリズムとして標準化されている例[2]

ISO/IEC 9796：(デジタル署名)
ISO/IEC 9797: (MAC)
ISO/IEC10118：(ハッシュ関数)
ISO/IEC11770：(鍵管理)
ISO/IEC14888：(デジタル署名)
ISO/IEC18031：(擬似乱数生成)
ISO/IEC18033：(公開鍵暗号・ブロック暗号・ストリーム暗号)　等

ISOやISO/IECでアプリケーションやシステムの規格において暗号アルゴリズムが指定されている可能性がある例（”encryption”のキーワードで検索される例）[3]

ISO 9564：(金融サービスでの PIN 暗号化)
ISO15764：(高度交通システムのデータリンク)
ISO21000：(MPEG-21 著作権保護)
ISO26429：(デジタルシネマ)

[1] ISO/IEC JTC 1：Joint Technical Committee 1
[2] ISO/IEC JTC1/SC27 が管理
[3] ISO/IEC JTC1/SC27 以外が管理

ISO26430：(デジタルシネマ)
ISO/IEC29116:（メディアストリーミング）　等

○国際電気通信連合（ITU)
ITU でアルゴリズムとして標準化されている例
規格名を見る限り現時点では発見できなかった。

ITU でアプリケーションやシステムの規格において暗号アルゴリズムが指定されている可能性がある例（”encryption”のキーワードで検索される例)
ITU SECU：(サイバーセキュリティガイド)
ITU H.235：(音声暗号)
ITU Y.SecMechanisms:（NGN セキュリティ機構)
ITU-R M.1457：(国際間携帯通信インタフェース)　等

② 業界団体（IETF,IEEE,W3C など）が定めた標準
＜例＞
○IETF(Internet Engineering Task Force)[4]
RFC[5]でアルゴリズムとして標準化されている例（いずれもInformationalとして扱われる)
RFC2994, RFC3174, RSA3447, RFC3713　等

RFC でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例（メインプロトコルの場合 Standard として扱われることが多い)
RFC4132, 5746：SSL/TLS 関連
RFC2451, 3602, 4306, 4312：IPsec 関連
RFC3565, 3657, 3853, 4056, 5083, 5652, 5750, 5751, 5754: S/MIME, CMS 関連
RFC3156: OpenPGP 関連
RFC3962, 4120: Kerberos 関連
RFC4344, 4419, 4432: SSH 関連　等

○IEEE (The Institute of Electrical and Electronics Engineers)
IEEE でアルゴリズムとして標準化されている例
IEEE P1363：(公開鍵暗号)　等

IEEE でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例
IEEE802.1AE：LAN 等での伝送関連
IEEE802.3AH：GE-PON 技術関連
IEEE802.11i：無線 LAN 技術関連　等

○W3C(World Wide Web Consortium)[6]
WWW でアルゴリズムとして標準化されている例
規格名を見る限り現時点では発見できなかった。

WWW でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例

[4] インターネット技術の標準化を推進する任意団体
[5] RFC:Request For Comments
[6] WWW で利用される技術の標準化をすすめる団体

XML Encryption, XML Signature：XML 関連　　等

③ 特定の国が定めた標準（FIPS,ANSI,ETSI など）

＜例＞

○FIPS (Federal Information Processing Standards)[7]

FIPS/SP でアルゴリズムとして標準化されている例

FIPS180-3, FIPS186-3, FIPS197, SP800-67　　等

FIPS/SP でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例

FIPS191：Guideline for The Analysis of Local Area Network Security,
FIPS201, SP800-78-1：Personal Identity Verification
SP800-52: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
SP800-77: Guide to IPsec VPN　　等

○米国規格協会（ANSI ： American National Standards Institute）[8]

ANSI でアルゴリズムとして標準化されている例

ANSI X9.30, ANSI X9.42, ANSI X9.63, ANSI X9.65, ANSI X9.82　　等

ANSI でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例

ANSI X9.24：(リテール金融サービス)
ANSI X9.96：(XML 暗号化)
ANSI X9.97：(金融向けセキュアデバイス)　　等

○欧州電気通信標準化機構（ETSI: European Telecommunications Standards Institute）[9]

ETSI でアルゴリズムとして標準化されている可能性がある例

TS 102 176　　等

ETSI でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例

TS 187 003：(NGN セキュリティ)
TS 102 731：(高度交通システム)
TS 102 573：(電子署名基盤)　　等

④ 特定の組織（RSA,EMV など）が定めた標準

＜例＞

○PKCS(Public-Key Cryptography Standards)[10]

PKCS でアルゴリズムとして標準化されている例

PKCS#1, PKCS#3, PKCS#13　　等

PKCS でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている可能性がある例

PKCS#7：(電子メール)

---

[7] 米国標準技術研究所(NIST)が策定している規格

[8] 米国における工業的な分野の標準化組織

[9] ヨーロッパにおける電気通信産業に関する標準化組織

[10] RSA セキュリティが定めた公開鍵暗号標準

PKCS#11：(トークンインターフェース)　　等

○EMV (Europay-Mastercard-Visa) [11]
EMV でアプリケーションやプロトコルの規格において暗号アルゴリズムが指定されている例
EMV4.2：(クレジットカード用 IC 仕様)　　等

暗号技術の国際標準に関しては、暗号アルゴリズムの標準のみを対象とすべきか、アプリケーションやシステムの規格で採用されている標準を考慮する必要があるか、どのような標準（アルゴリズム又はアプリーション）が、実際の製品開発の参考にされているか、いずれの標準化機関により標準化されている標準を国際標準ととらえるか、標準化団体により標準の位置づけの違い、事実上の標準となっている場合の考え方等の観点から、議論を行い、以下のような意見があげられ、さらに検討を続けることとなった。

- 標準化団体によっては技術毎にステータスがあり、取り扱いが異なる場合があるのではないか。
- 標準化されていなくても社会インフラレベルまで普及した場合は、評価すべきではないか。
- 標準化団体の動向が運用に与える影響を調査すべきではないか。
- 電子政府推奨暗号を選定する際の国際標準化の整理であれば、国際標準の暗号からどのような暗号を選ぶかというのではなく、それぞれの暗号がどのような条件を満たしていれば国際標準化されていると言えるのかという視点で検討するのが良いのではないか。
- 応募暗号と事務局提案暗号との間で対象となる標準化団体やステータスなどについての考え方が異なっても良いのではないか。

1.3.4. 運用監視暗号リスト登録暗号の危殆化対策の検討

運用監視暗号リストに登録されることなった暗号の危殆化対策の検討については、当該リストへの登録、当該リストからの削除の評価基準等の具体化が必要なことから、暗号技術の製品化、利用実績等の評価も踏まえつつ、暗号技術の３リストへの登録見直しの期間や方法の具体化を図った上で、次期リストの運用監視暗号リストに登録する暗号の危殆化対策の検討を次年度に実施していくこととした。

1.3.5. 先導的技術調査ワーキンググループ

危殆化対策など、優先すべき課題があるとの指摘を踏まえ、あらためて調査・検討の優先度が高いセキュリティ技術を整理した上で、ワーキンググループの設置の検討を行うこととした。

[11] 3 大クレジットカード会社がクレジットカード共通仕様として標準化したもの

発行日　2010年 5月 28日　第1版第1刷
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
（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）
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