

**暗号技術検討会**  
**2002年度報告書**

**暗号技術検討会**  
**2003年3月**

## 目次

|   |    |
|---|----|
| 1 . はじめに  | 1  |
| 2 . 暗号技術検討会開催の背景、構成員及び開催状況  | 3  |
| 2 . 1 . 暗号技術検討会開催の背景  | 3  |
| 2 . 2 . CRYPTREC の体制  | 3  |
| 2 . 2 . 1 . 暗号技術検討会   | 3  |
| 2 . 2 . 2 . 暗号技術評価委員会   | 4  |
| 2 . 3 . メンバー  | 5  |
| 2 . 3 . 1 . 暗号技術検討会メンバー   | 5  |
| 2 . 3 . 2 . 暗号調達ガイドブック作成WGメンバー                                    | 6  |
| 2 . 4 . 開催状況  | 7  |
| 3 . 電子政府推奨暗号リスト   | 8  |
| 3 . 1 . e-Japan 重点計画及びセキュリティ・アクションプランにおける電子政府の実現<br>及び暗号技術評価の位置付け | 8  |
| 3 . 2 . 暗号技術評価について  | 10 |
| 3 . 2 . 1 . 暗号技術評価の目的   | 10 |
| 3 . 2 . 2 . 評価概要  | 10 |
| 3 . 2 . 3 . 各暗号技術の評価基準の概要   | 11 |
| 3 . 2 . 4 . 暗号技術評価結果の概要   | 12 |
| 3 . 3 . 電子政府推奨暗号リスト   | 19 |
| 3 . 4 . 電子政府推奨暗号の仕様に関する情報提供                                       | 23 |
| 4 . 暗号調達のためのガイドブックについて  | 24 |
| 4 . 1 . 暗号調達ガイドブック作成 WG 設置の目的                                     | 24 |
| 4 . 2 . ガイドブック作成の進め方  | 24 |
| 4 . 2 . 1 . 対象とする読者   | 24 |
| 4 . 2 . 2 . 盛り込む内容  | 24 |
| 4 . 2 . 3 . ISO/IEC15408 を活用した調達との関連                              | 24 |
| 4 . 2 . 4 . 検討方法  | 25 |
| 4 . 2 . 5 . WG 会合の開催状況  | 25 |
| 4 . 3 . ガイドブックの概要   | 26 |
| 4 . 3 . 1 . システム全体の検討作業と暗号調達作業との関わり                               | 26 |
| 4 . 3 . 2 . 電子政府システムにおける暗号利用イメージ                                  | 27 |
| 4 . 3 . 3 . 暗号利用形態及び暗号技術分類  | 27 |

|                               |    |
|-------------------------------|----|
| 4.3.4. 電子政府推奨暗号の概要            | 27 |
| 4.3.5. 暗号調達の手順に関する説明          | 27 |
| 4.3.6. 調達仕様書作成上の留意点           | 31 |
| 4.3.7. 調達先の決定、契約及び納品          | 31 |
| 4.3.8. 参考資料                   | 32 |
| <br>                          |    |
| 5. 今後の CRYPTREC 活動について        | 33 |
| 5.1. 今後の CRYPTREC の活動目的及び活動内容 | 33 |
| 5.1.1. 活動目的                   | 33 |
| 5.1.2. 活動内容                   | 33 |
| 5.2. 今後の CRYPTREC 体制          | 34 |
| 5.2.1. 暗号技術検討会                | 34 |
| 5.2.2. 暗号技術監視委員会              | 35 |
| 5.2.3. 暗号モジュール委員会             | 35 |
| 5.3. 電子政府推奨暗号の監視              | 36 |
| 5.3.1. 電子政府推奨暗号の監視の基本的考え方     | 36 |
| 5.3.2. 電子政府推奨暗号の監視の具体的内容      | 36 |
| 5.3.3. 電子政府推奨暗号の監視の手順         | 38 |
| 5.4. 電子政府推奨暗号リストの改訂           | 40 |
| 5.4.1. 基本的認識                  | 40 |
| 5.4.2. 基本的考え方                 | 40 |
| 5.5. 暗号モジュールに関する検討            | 40 |

**【資料】**

- ・「暗号調達のためのガイドブック」

**【参考資料】**

- ・「各府省の情報システム調達における暗号の利用方針」

## 1. はじめに

近年のインターネットの急速な拡大に代表されるように、社会における IT 化の進展はめざましいものがある。我が国政府においても、e-Japan 重点計画に基づき、2003 年度までに電子情報を紙情報と同等に扱う行政の実現を目指している。これは、行政の効率化や国民負担の軽減を目標に、申請届出手続や調達などの行政手続の電子化を実現するものである。

他方、IT 化による利便性の増大とともに、新種ウィルスや、不正アクセス件数の増加等、IT に対する脅威が増加しており、その姿も多様化している。このような環境の中、いかに IT の安全性・信頼性を確保するかという問題は、我々の社会が直面している喫緊の課題と言えよう。

政府としても、安全性及び信頼性の高い電子政府を実現するために、情報セキュリティの確保が不可欠であり、情報セキュリティ技術の基盤をなす暗号技術が重要であるとの認識を深めている。この認識は、2001 年 3 月に IT 戦略本部において決定された「e-Japan 重点計画」においても示され、さらに、同年 10 月に情報セキュリティ対策推進会議において「総務省及び経済産業省は、両省で実施している研究会の成果等も踏まえ、2002 年度中に「電子政府」における調達のための推奨すべき暗号のリストを作成し、これを踏まえ、各省庁における暗号の利用方針について合意を目指す」ことが決定された。

これに先立ち、2000 年度、経済産業省（旧通商産業省）からの委託を受けて、情報処理振興事業協会（IPA）は電子政府で利用可能な暗号技術を安全性および実装性など技術的な面から評価することを目的とした暗号技術評価委員会を設置するとともに同委員会の事務局を務めた。2001 年度からは通信・放送機構（TAO）が同委員会の共同事務局として参加した。また、2001 年度には、暗号技術評価委員会に加えて、総務省大臣官房技術総括審議官及び経済産業省商務情報政策局長が、暗号技術の利用に関し政策的な観点から検討を行うことを目的として、暗号技術検討会（以下、本検討会）を設置した。

本検討会は、電子政府で利用される暗号技術、国際標準化に関する暗号技術及び電子署名法等に基づいて利用される暗号技術の評価・調査研究、並びにその他暗号技術の利用等に関連する技術課題を検討対象としており、特に、2002 年度は、2001 年度に引き続き暗号技術の評価を行うとともに、電子政府推奨暗号リスト案の策定、暗号の調達のためのガイドブックの作成、及び 2003 年度以降の CRYPTREC 活動についての検討を行った。

なお、暗号調達ガイドブックに関しては、本検討会の下に設置された暗号調達ガイドブック作成WGが暗号調達ガイドブック案の作成作業を行った。

本報告書は、2002 年度の本検討会における検討結果をまとめたものであり、総務省及

び経済産業省に対して報告するとともに、電子政府を構築する各府省関係者、及び一般の暗号ユーザの方々にも広く読んで頂くことを想定している。

なお、2002年度のCRYPTREC活動のうち、詳細な技術的事項については、暗号技術評価委員会並びに同委員会の下に設置された共通鍵暗号評価小委員会及び公開鍵暗号評価小委員会における議論を踏まえて、IPA及びTAOによってまとめられている「CRYPTREC Report 2002」を御参照頂きたい。

本検討会は、2002年度、当面の目標であった電子政府推奨暗号リスト案及び暗号調達ガイドブックを作成した。しかしながら、国民が安心して利用できる電子政府を構築し、運用していくためには、2003年度以降も継続して暗号技術を監視し、評価するとともに、暗号モジュールに関する安全性評価基準を作成する等の活動を実施していく必要がある。

これらの活動を実施していくためには、CRYPTREC関係者が一致団結することが不可欠であり、今後とも関係者の方々の御協力を頂きながら、暗号技術検討会をはじめとするCRYPTREC活動を積極的に推進していきたい。

末筆であるが、本検討会にご協力いただいた構成員の方々及びオブザーバとしてご参加頂いた方々、精力的に暗号調達ガイドブックを作成して頂いた暗号調達ガイドブック作成WGの構成員の方々をはじめ関係者の皆様に心から謝意を表する次第である。

2003年3月

暗号技術検討会  
座長 今井 秀樹

## 2. 暗号技術検討会開催の背景、構成員及び開催状況

### 2.1. 暗号技術検討会開催の背景

高度情報通信ネットワークの安全性及び信頼性の確保は、我が国が目指す世界最先端の IT 国家構築の基盤となるものであり、国民一人一人が安心してネットワークを利用するための前提となるものである。高度情報通信ネットワーク社会形成基本法に基づく e-Japan 重点計画（2001 年 3 月 29 日高度情報通信ネットワーク社会推進戦略本部決定）及び e-Japan 重点計画-2002（2002 年 6 月 18 日 同本部決定）では、特に電子政府、電子商取引、重要インフラについて、ネットワークにおける脅威に起因するサービス提供機能の停止をゼロとすることを目標として、政府は情報セキュリティのための諸施策を実施することとされている。

暗号技術は情報セキュリティの基盤技術であり、その安全性を暗号技術の専門家により技術的、専門的な見地から客観的に評価することが重要である。また、2003 年度までに「電子政府」の実現が予定されており、そのセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリスト化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府の構築に貢献することを目指すこととした。

### 2.2. CRYPTREC の体制

CRYPTREC とは Cryptography Research and Evaluation Committees の略であり、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：今井秀樹東京大学教授）と、通信・放送機構（TAO）及び情報処理振興事業協会（IPA）が共同で開催する暗号技術評価委員会（委員長：今井秀樹東京大学教授）による暗号技術評価プロジェクトを指す（CRYPTREC の体制図は図 1 参照）。検討会及び評価委員会は以下のように検討及び評価を進めた。

#### 2.2.1. 暗号技術検討会

暗号技術検討会（以下、「検討会」）は、総務省及び経済産業省に対して暗号利用に関する助言を行うとともに、電子政府における暗号利用に関する政策的判断を行った。また、検討会の下には、必要に応じてワーキンググループを設置し、詳細な検討を効率的に実施することとしており、2002 年度は、「暗号調達ガイドブック作成ワーキンググループ（リーダー：佐々木良一東京電機大学教授）」を設置し、電子政府推奨暗号を円滑に調達するための手引書を作成した。

検討会は総務省大臣官房技術総括審議官及び経済産業省商務情報政策局長の研究会として開催し、内閣官房、警察庁、防衛庁、法務省、外務省、財務省等がオブザーバとして参加した。

## 2.2.2. 暗号技術評価委員会

暗号技術評価委員会（以下、「評価委員会」）は、暗号アルゴリズム等に関する技術的評価を行い、評価結果を検討会に報告した。また、検討会に対して暗号に関する技術的助言を行った。評価委員会の下には、共通鍵暗号評価小委員会（委員長：金子敏信東京理科大学教授）及び公開鍵暗号評価小委員会（委員長：松本勉横浜国立大学教授）を設置した。

TAO 及び IPA の委員会として開催し、総務省、経済産業省、警察庁、防衛庁、外務省等がオブザーバとして参加した。

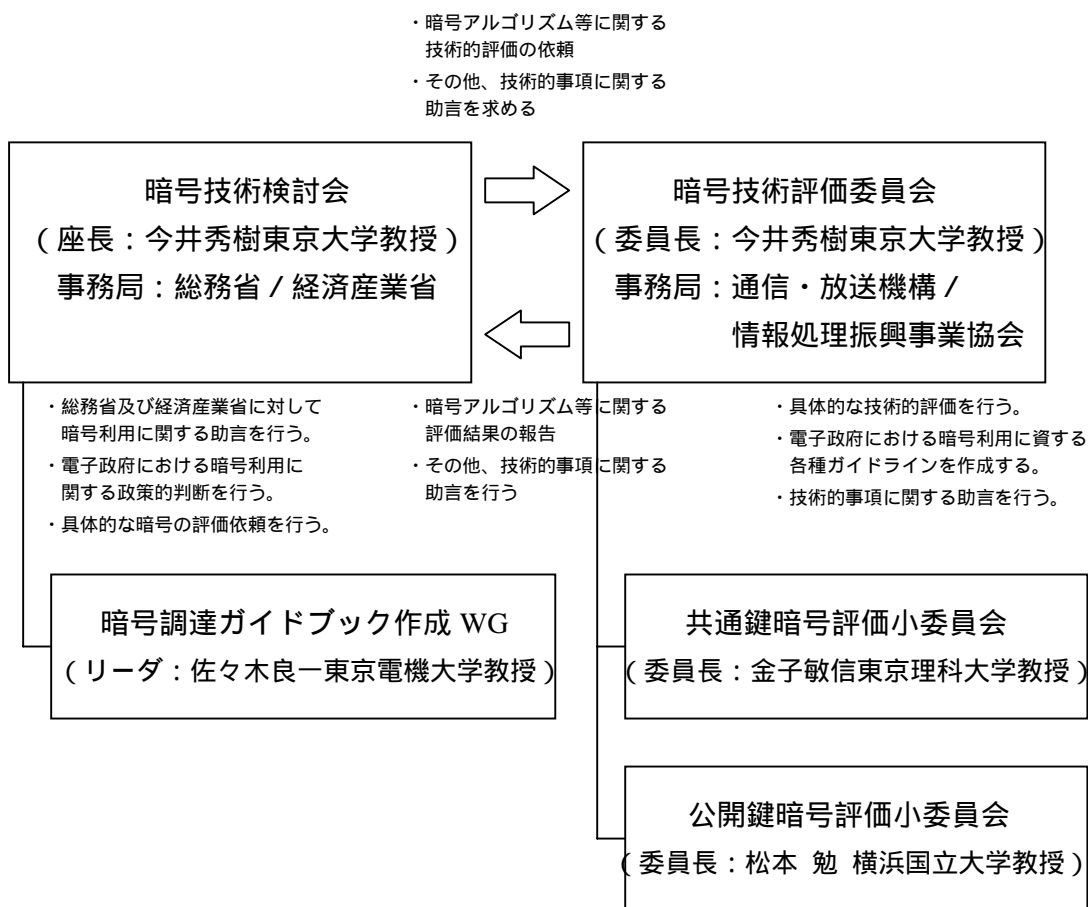


図1 2002年度のCRYPTRECの体制図

## 2.3. メンバー

### 2.3.1. 暗号技術検討会メンバー

(構成員) 肩書は2003年3月末現在。敬称略。

|    |        |   |
|----|--------|---|
| 座長 | 今井 秀樹  | 東京大学生産技術研究所教授   |
| 顧問 | 辻井 重男  | 中央大学理工学部教授  |
|    | 岩下 直行  | 日本銀行金融研究所調査第2課企画役                                     |
|    | 岡崎 宏   | 情報通信ネットワーク産業協会常務理事                                    |
|    | 岡本 栄司  | 筑波大学電子・情報工学系教授  |
|    | 岡本 龍明  | 日本電信電話株式会社情報流通プラットフォーム研究所<br>主席研究員(社団法人電気通信事業者協会代表兼務) |
|    | 小田 雅一  | 社団法人情報サービス産業協会セキュリティ委員会委員                             |
|    | 小柳津 育郎 | NTTエレクトロニクス株式会社セキュリティシステム<br>事業部技術部長                  |
|    | 加藤 義文  | 社団法人テレコムサービス協会技術委員会委員長                                |
|    | 金子 敏信  | 東京理科大学理工学部電気工学科教授                                     |
|    | 国分 明男  | 財団法人ニューメディア開発協会常務理事開発本部長                              |
|    | 櫻井 幸一  | 九州大学大学院システム情報科学研究科教授                                  |
|    | 佐々木 良一 | 東京電機大学工学部情報メディア学科教授                                   |
|    | 宝木 和夫  | 社団法人電子情報技術産業協会情報セキュリティ委員会<br>委員                       |
|    | 苗村 憲司  | 慶應義塾大学環境情報学部教授  |
|    | 松井 充   | 三菱電機株式会社情報技術総合研究所情報セキュリティ<br>技術部チームリーダー               |
|    | 松本 勉   | 横浜国立大学大学院環境情報研究院教授                                    |

(オブザーバ) 肩書は原則として参加当時のもの。敬称略。

|        |                        |
|--------|------------------------|
| 吉原 順二  | 内閣官房情報セキュリティ対策推進室内閣参事官 |
| 手塚 新樹  | 警察庁情報通信局技術対策課長         |
| 中村 範明  | 防衛庁運用局指揮通信課長(第1回)      |
| 青木 信義  | 防衛庁長官官房情報通信課長(第2回~)    |
| 高森 國臣  | 総務省行政管理局管理官            |
| 猿渡 知之  | 総務省自治行政局自治政策課情報政策企画官   |
| 中垣 治夫  | 法務省民事局商事課補佐官           |
| 石川 正紀  | 外務省大臣官房情報通信課長(第1回)     |
| 楠田 かおる | 外務省大臣官房情報通信課長(第2回~)    |
| 中山 峰孝  | 財務省大臣官房審議官室長(第1回)      |

|       |                                 |
|-------|---------------------------------|
| 宇野 雅夫 | 財務省日野参事官室企画官（第2回～）              |
| 木戸 達雄 | 経済産業省産業技術環境局標準課情報電気標準化推進室長      |
| 福地 一  | 独立行政法人通信総合研究所情報通信部門長（第1回）       |
| 蓮池 和夫 | 独立行政法人通信総合研究所情報通信部門長（第2回～）      |
| 大蒔 和仁 | 独立行政法人産業技術総合研究所 情報処理研究部門長       |
| 鈴木 薫  | 通信・放送機構研究企画管理部長（第1回）            |
| 喜安 拓  | 通信・放送機構研究企画管理部長（第2回～）           |
| 内藤 理  | 情報処理振興事業協会セキュリティセンター所長          |
| 米倉 昭利 | 財団法人日本品質保証機構電子署名・認証調査センター<br>所長 |
| 小倉 久宜 | 財団法人金融情報システムセンター監査安全部長          |

## 2.3.2. 暗号調達ガイドブック作成WGメンバー

肩書は2003年3月末現在。敬称略。

|      |        |  |
|------|--------|--|
| リーダー | 佐々木 良一 | 東京電機大学工学部情報メディア学科教授                          |
|      | 岩下 直行  | 日本銀行金融研究所研究第2課企画役                            |
|      | 宇賀村 直紀 | 社団法人電子情報技術産業協会ITセキュリティ<br>センター部長             |
|      | 岡本 栄司  | 筑波大学電子・情報工学系教授                               |
|      | 川村 信一  | 株式会社東芝 研究開発センター<br>コンピュータ・ネットワークラボラトリー主任研究員  |
|      | 洲崎 誠一  | 株式会社日立製作所システム開発研究所第7部<br>H01研究ユニット研究員        |
|      | 館林 誠   | 松下電器産業株式会社マルチメディア開発センター<br>メディア情報グループチームリーダー |
|      | 中村 逸一  | 株式会社NTTデータ ビジネス開発事業本部セキュリ<br>ティ事業部 営業グループ 部長 |
|      | 米倉 昭利  | 財団法人日本品質保証機構電子署名・認証調査センター<br>所長              |
|      | 渡辺 創   | 独立行政法人産業技術総合研究所情報処理部門研究員                     |

## 2.4. 開催状況

2002 年度、検討会は計 6 回開催された。各回会合の開催日及び主な議題は以下のとおり。なお、暗号調達ガイドブック作成WGの会合開催状況は第 4 章を参照のこと。

【第 1 回】平成 14 年 5 月 16 日（木）

（主な議題）暗号技術検討会 2002 年度活動計画  
電子政府推奨暗号の数  
暗号技術評価委員会への依頼事項  
暗号調達ガイドブック作成ワーキンググループの設置

【第 2 回】平成 14 年 7 月 16 日（火）

（主な議題）暗号調達のためのガイドブック案  
電子政府推奨暗号の数  
電子政府推奨暗号リスト素案の検討状況  
暗号モジュール評価の現状把握

【第 3 回】平成 14 年 9 月 30 日（月）

（主な議題）電子政府推奨暗号リスト案  
暗号調達のためのガイドブック案

【第 4 回】平成 14 年 11 月 27 日（水）

（主な議題）電子政府推奨暗号リスト案  
同リスト案に対するパブリックコメント  
暗号調達のためのガイドブック案  
暗号プロトコルの現状把握（1）  
今後の CRYPTREC 活動

【第 5 回】平成 15 年 2 月 12 日（水）

（主な議題）電子政府推奨暗号リストの決定  
パブリックコメントに対する回答  
暗号調達のためのガイドブック案  
暗号プロトコルの現状把握（2）  
今後の CRYPTREC 活動

【第 6 回】平成 15 年 3 月 24 日（月）

（主な議題）2002 年度報告書  
暗号調達のためのガイドブック  
今後の CRYPTREC 活動

### 3. 電子政府推奨暗号リスト

#### 3. 1. e-Japan 重点計画及びセキュリティ・アクションプランにおける電子政府の実現及び暗号技術評価の位置付け

2001年3月29日に、高度情報通信ネットワーク社会推進戦略本部で決定された e-Japan 重点計画では、行政の情報化及び公共分野における情報通信技術の活用の推進における施策の意義として「電子政府」の実現が掲げられており、また、高度情報通信ネットワークの安全性及び信頼性の確保のための具体的施策の一つとして、「暗号技術の標準化の推進」が掲げられている。

(「e-Japan 重点計画」より抜粋)

#### 5. 行政の情報化及び公共分野における情報通信技術の活用の推進

##### (2) 施策の意義

(略)

特に、国の行政機関においては、行政の情報化により、事務・事業及び組織の改革を推進するとともに、セキュリティの確保に留意しつつ、「紙」による情報の管理からネットワークを駆使した電子化された情報の管理へ移行し、高度に情報化された行政、すなわち以下のような「電子政府」を実現する。

(主な項目) 行政情報の電子的提供

申請・届出等手続の電子化

歳入・歳出の電子化

調達手続の電子化

ペーパーレス化(電子化)

#### 6. 高度情報通信ネットワークの安全性及び信頼性の確保

##### (3) 具体的施策

情報セキュリティに係る制度・基盤の整備

ウ) 暗号技術の標準化の推進(総務省及び経済産業省)

客観的にその安全性が評価され、実装性に優れた暗号技術を採用するため、2002年度中に、ISO、ITU等における暗号技術の国際標準化の動向を踏まえ、専門家による検討会の開催等を通じて電子政府利用等に資する暗号技術の評価及び標準化を行う。

e-Japan 重点計画の決定を受け、2003 年度からの電子政府の実現に向けて政府の情報セキュリティ確保に万全を尽くすことを目的として、「電子政府の情報セキュリティ確保のためのアクションプラン」が内閣官房が中心となって取りまとめられ、2001 年 10 月 10 日に情報セキュリティ対策推進会議において決定された。その中では、具体的な方策の一つとして、2002 年度中に「電子政府」における調達のための推奨すべき暗号のリストを作成することが掲げられている。

**(「電子政府の情報セキュリティ確保のためのアクションプラン」より抜粋)**

**2. 具体的な方策**

**(2) 暗号の標準化の推進**

- ・ 「電子政府」におけるセキュリティ確保のためには、政府調達における一定水準のセキュリティ確保のための情報機器等に関する基準（具体的には ISO/IEC15408）を可能な限り利用することと同様、暗号についても、一定水準以上の安全性及び信頼性を有するものの利用が不可欠であり、これを推進することが必要である。
- ・ このため、総務省及び経済産業省は、両省で実施している研究会の成果等も踏まえ、2002 年度中に「電子政府」における調達のための推奨すべき暗号のリストを作成し、これを踏まえ、各省庁における暗号の利用方針について合意を目指す。

**(参考) 日程表**



2002 年 6 月 18 日に策定された「e-Japan 重点計画-2002」においても、高度情報通信ネットワーク社会形成のために政府が迅速かつ重点的に実施すべき施策の中に、「電子政府の実現」及び「暗号技術の標準化の推進」が掲げられている。

## 3.2. 暗号技術評価について

### 3.2.1. 暗号技術評価の目的

申請届出や調達など行政手続の電子化を実現する電子政府の機能をより安心して利用できるようにするためには、電子政府で利用可能な暗号技術<sup>1</sup>を評価することが重要であり、2000年度から暗号技術評価委員会を設置して、暗号技術の公募や委員会による評価対象暗号技術の選定及び評価を進めてきた。

本暗号技術評価活動は我が国における暗号技術評価体制の確立に向けた一歩であり、米国政府標準暗号を定める AES (Advanced Encryption Standard) プログラムを参考にしつつ、欧州における暗号評価プロジェクト (NESSIE : New European Schemes for Signatures, Integrity, and Encryption) や ISO/IEC における国際標準化活動への協力も行っている。

### 3.2.2. 評価概要

電子政府で利用可能と想定される暗号技術の評価は暗号アルゴリズム<sup>2</sup>の評価を中心として実施した。公開鍵暗号、共通鍵暗号、ハッシュ関数、擬似乱数生成系の4つの分類について、評価対象暗号技術の募集・選定を行い、各暗号技術の評価を行った。

暗号技術評価は、原則スクリーニング評価を実施した後、詳細評価を実施する二段階評価のプロセスで評価を行った。なお、今年度評価を実施した暗号技術は、昨年度でスクリーニング評価を終了しているため、詳細評価のみを行った。

#### (1) 暗号分類

##### (イ) 公開鍵暗号

守秘, 署名, 認証, 鍵共有

##### (ロ) 共通鍵暗号

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

##### (ハ) ハッシュ関数

##### (ニ) 擬似乱数生成系

#### (2) スクリーニング評価 今年度は実施せず

詳細評価を実施するに値するかどうかを判断するためのスクリーニング評価を下記の観点から実施した。

(イ) 安全性に明らかな問題がないかどうかを評価する。

(ロ) 第三者実装上問題がないかどうかを評価する。

---

<sup>1</sup> : 暗号技術とは、暗号 (暗号アルゴリズム、暗号方式)、暗号プロトコル、暗号モジュール、暗号鍵管理等を含む概念とする。

<sup>2</sup> : 暗号アルゴリズムは、単に暗号、または、暗号方式とも呼ばれる。

### (3) 詳細評価

スクリーニング評価で問題がないと判断された暗号について、電子政府で利用可能かどうかの観点から評価する詳細評価を下記の観点から実施した。

- (イ) 既知の攻撃法に対する統一的な強度評価
- (ロ) 各詳細評価対象暗号特有の攻撃法に対する強度評価
- (ハ) パラメータ / 鍵の設定基準の評価
- (ニ) ソフトウェア実装評価
- (ホ) ハードウェア実装評価

### 3.2.3. 各暗号技術の評価基準の概要

各暗号技術の評価基準の概要は、以下の通りである。詳細は、暗号技術評価報告書(2002年度版)(CRYPTREC Report 2002)を参照のこと。

#### (1) 公開鍵暗号

比較的長い期間にわたる使用実績・評価実績があり、インターオペラビリティの観点から仕様の変更を簡単には求められない公開鍵暗号方式<sup>3</sup>については、多くの研究者から十分な評価研究を受けているが、実運用における安全性に関する問題点が指摘されていないこと、すなわち経験的に安全であることを求めた。

使用実績が少ない新しい公開鍵暗号方式については、既存暗号技術とは独立に仕様を定めることができることから、最低限の条件として証明可能安全性が示されていることを必須とした。

これらに加えて、プリミティブが依存する数論的な問題の困難性や、推奨パラメータの選択方法や補助関数のスキームの中での利用方法を含めて総合的に安全性を評価した。

#### (2) 共通鍵暗号

以下の条件のいずれかを満たすことを求めた。

- (イ) 現時点の最良の解読技術を適用しても、秘密鍵の総当たりである  $2^{128}$  以上の計算量が必要と判断されるもの。特に、差分攻撃や線形攻撃などの代表的な攻撃法について、安全性が確認されているもの。
- (ロ) 世界的に広く使用され、かつ多くの研究者から十分な評価研究を受けているが、実運用における安全性上の大きな問題点が指摘されておらず、現時点で安全と判断されるもの。この場合、 $2^{100}$  以上の解読計算量を目安とした。

---

<sup>3</sup> : 公開鍵暗号方式(または公開鍵暗号スキーム)は、プリミティブ(基本関数)とその他の要素技術(ハッシュ関数、擬似乱数生成系等)を組み合わせる公開鍵暗号全体の仕組みを指す専門用語。

### (3) ハッシュ関数

以下の条件のいずれかを満たすことを求めた。

- (イ) 特定の出力に対する入力値を発見する手間への耐性が十分に高く（最良の解読技術を適用しても  $2^{160}$  以上の計算量）かつ出力値が一致するような異なる入力値を発見する計算量が最良の解読技術を適用しても  $2^{80}$  以上であること。
- (ロ) 世界的に広く使用され、かつ実運用における安全性上の問題点が指摘されていないこと。なお、全ハッシュ値の長さが少なくとも 160 ビット以上であること。

### (4) 擬似乱数生成系

以下の条件をすべて満たすことを求めた。

- (イ) 統計的性質が真性乱数に近く、かつ、既知の出力ビット履歴から未来又は過去の未知出力ビットが予測困難であること。
- (ロ) 擬似乱数生成系を使用するシステムの総当たり攻撃に対し、十分に耐性をもつ程に、実質的入力空間が大きいこと。
- (ハ) 統計的性質は、例えば NIST が公表している SP800-22 等の代表的な擬似乱数検定テストに合格するものであること。

## 3.2.4. 暗号技術評価結果の概要

今年度の暗号技術評価結果の概要を以下に示す。なお、詳細は、暗号技術評価報告書（2002 年度版）(CRYPTREC Report 2002)を参照のこと。

### (1) 公開鍵暗号方式の総評<sup>4</sup>

#### (イ) DSA（署名）

米国 NIST(National Institute of Standards and Technology)によって提案、標準化された電子署名方式であり、電子署名法に係る指針<sup>5</sup>に記載されている。オブジェクト識別子は、1 2 840 10040 4 3 である。

安全性は有限体上の離散対数問題の困難性に依存している。証明可能安全性は示されていないが経験的に安全である。

安全性の観点からパラメータ  $p$  のサイズは 1024 ビットを選択することを強く推奨する。2001 年 10 月に NIST が FIPS PUB 186-2 (+ change notice 1)に提示した擬似乱数生成系の修正に従うべきである。

<sup>4</sup> : 公開鍵暗号方式が証明可能安全性を有するとは、その方式を攻撃することの非現実性を、暗号理論分野で標準的な安全性評価モデルの枠組に沿って示せることをいう。ただし、それが現時点で示されていないからといって、その方式の安全性が否定されるわけではない。

<sup>5</sup> : 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（平成 13 年総務省 法務省 経済産業省告示第 2 号）のことを指す。以下、同指針を「電子署名法に係る指針」と略記する。

(ロ) ECDSA (署名)

CRYPTREC では ECDSA (ANSI X9.62) と ECDSA (SEC 1<sup>6</sup>) とを評価した。

ECDSA (ANSI X9.62) は電子署名法に係る指針に記載されている署名方式であり、オブジェクト識別子は、1 2 840 10045 4 1 である。

安全性は楕円曲線上の離散対数問題の困難性に依存している。証明可能安全性は示されていないが経験的に安全であり、2002 年時点では安全性について重大な問題点は指摘されていない。

ECDSA (SEC 1) における楕円曲線パラメータは SEC 1 に示されている。これらの楕円曲線については特段の問題点は指摘されていない。安全性の観点から群位数が 160 ビット以上の素因子をもつようなパラメータを選択することを強く推奨する。擬似乱数生成器に関して NIST が FIPS PUB 186-2 (+ change notice 1) に提示した擬似乱数生成器の動向に注意すべきである。

(ハ) ESIGN (署名)

ESIGN 署名の仕様は複数存在する。ESIGN (応募暗号) の評価の参考にするために TSH-ESIGN も評価した。

プリミティブの安全性は  $n = p^2q$  型素因数分解問題の困難性に依存している。ESIGN の署名生成速度は RSA 署名と比べて高速であるが、RSA プリミティブと同程度の安全性を ESIGN のプリミティブにおいて得るためには RSA の法パラメータのサイズよりも少し大きな法パラメータを利用しなければならない。

(a) ESIGN は証明可能安全性を有しない。実際に、一部のパラメータの利用に際して、無視できない確率で署名の偽造が可能である。

(b) TSH-ESIGN には新提案技術に必須とされた証明可能安全性が示されていない。

(ニ) RSA (署名、守秘)

RSA プリミティブを利用した署名方式にはいくつかの仕様が存在する。CRYPTREC では RSASSA-PKCS1-v1\_5 と RSA-PSS を評価した。RSASSA-PKCS1-v1\_5 と RSA-PSS は両方とも電子署名法に係る指針に記載されている署名方式であり、それぞれのオブジェクト識別子は、1 2 840 113549 1 1 5 および 1 2 840 113549 1 1 10 である。

また RSA プリミティブを利用した守秘方式にはいくつかの仕様が存在する。CRYPTREC では RSAES-PKCS1-v1\_5 と RSA-OAEP を評価した。

これら 4 つの RSA 方式は長期間広く使われてきた実績と、広範な観点から評

---

<sup>6</sup> : Standards for Efficient Cryptography Group (SECG) から提供されている技術文書の 1 つ。

価が行われてきたことから経験的に安全である。

( a ) RSASSA-PKCS1-v1\_5 は電子署名法に係る指針に記載されている署名方式の 1 つである。証明可能安全性は示されていない。

( b ) RSA-PSS は新提案技術に必須とされた証明可能安全性を有する。

( c ) RSAES-PKCS1-v1\_5 は SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。経験的安全性は有するが、証明可能安全性は持たず、実際に能動的攻撃が成立する可能性も無視できないので、実運用環境上における攻撃に対する対策を十分に施し細心の注意を払う必要がある。

( d ) RSA-OAEP は新提案技術に必須とされた証明可能安全性を有する。

RSA プリミティブの安全性は、 $n = pq$  型素因数分解問題の困難性に依存している。安全性の観点から法パラメータ  $n = pq$  のサイズは 1024 ビット以上のものを利用することを強く推奨する。

(ホ) ECIES (守秘)

ECIES は、2000 年度には ECAES として CRYPTREC に応募されていたが、2001 年度では暗号技術名を ECIES に変更して応募されている。ECIES にはいくつかの仕様が存在する。CRYPTREC では SEC 1 に記載された仕様を基に評価した。

SEC 1 に記載された仕様の ECIES におけるスキームには KDF 関数への入力及び MAC の取り扱い方法の不備が原因で、脆弱性が存在し、新提案技術に必須とされた証明可能安全性を有しない。

(ヘ) HIME(R) (守秘)

2000 年度応募された HIME-1 と HIME-2 の改良版として 2001 年度に応募された技術である。

プリミティブの安全性は  $n = p^2q$  型素因数分解問題の困難性に依存している。RSA プリミティブと同程度の安全性を HIME(R)のプリミティブにおいて得るためには RSA の法パラメータのサイズよりも少し大きな法パラメータを利用しなければならない。

HIME(R)にはその仕様書に不備・曖昧さがあり、2002 年 9 月時点で信頼に足る HIME(R)の仕様書が公に手に入る状況になっていないと判断された。このため、HIME(R)の第三者による実装性や相互接続性が担保されないと判断された。HIME(R)の仕様の曖昧さを埋めてその仕様を合理的に定めたとしても、自己評価

書に記載されている証明可能安全性の証明中いくつかの箇所に問題があり、不完全であり、2002年9月時点で新提案技術に必須とされた証明可能安全性を有すると断定できないと評価された。

(ト) ECDH (鍵共有)

ECDHは、2000年度にはECDHSとしてCRYPTRECに応募されていたが、2001年度では暗号技術名をECDHに変更して応募されている。

安全性は楕円曲線上の離散対数問題の困難性に依存している。能動的攻撃に対しては証明可能安全性は示されていないが経験的に安全である。使用にあたっては運用上の注意が必要である。

ECDH(SEC 1)における楕円曲線パラメータはSEC 1に示されている。これらの楕円曲線については特段の問題点は指摘されていない。安全性の観点から群位数が160ビット以上の素因子をもつようなパラメータを選択することを強く推奨する。

(チ) DH (鍵共有)

DHにはいくつかの仕様が存在する。CRYPTRECではANSI X9.42-2001を対象とした。

安全性は有限体上の離散対数問題の困難性に依存している。能動的攻撃に対しては証明可能安全性は示されていないが経験的に安全である。使用にあたっては運用上の注意が必要である。

安全性の観点からパラメータ  $p$  のサイズは1024ビット以上を選択することを強く推奨する。

(リ) PSEC-KEM (鍵共有)

2000年度に応募されたPSECをISO/IEC 18033-2において審議されているKEM技術に適合するように変更を加えたもので、2001年度に応募された。

安全性は楕円曲線上の離散対数問題の困難性に依存している。KEM技術に関する証明可能安全性を有するので、PSEC-KEMをKEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism)構成に利用することは安全であるといえる。しかし、それ以外の目的の利用について安全性の研究は十分ではないので、今後の研究に注意すべきである。

CRYPTRECとしてはSEC 1で規定される曲線の利用を推奨する。これらの楕円曲線については特段の問題点は指摘されていない。安全性の観点から群位数が160ビット以上の素因子をもつようなパラメータを選択することを強く推奨する。

(2) 共通鍵暗号の総評

(イ) CIPHERUNICORN-E (64ビットブロック暗号)<sup>7</sup>

安全性について、今のところ問題は見つかっていない。処理速度は遅いグループである。

(ロ) Hierocrypt-L1 (64ビットブロック暗号)<sup>7</sup>

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

(ハ) MISTY1 (64ビットブロック暗号)<sup>7</sup>

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

(ニ) Triple DES (64ビットブロック暗号)<sup>7</sup>

安全性について、FIPS等で保証されている間は、問題ないとする。

(ホ) Advanced Encryption Standard (128ビットブロック暗号)

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

(ヘ) Camellia (128ビットブロック暗号)

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

(ト) CIPHERUNICORN-A (128ビットブロック暗号)

安全性について、今のところ問題は見つかっていない。処理速度は遅いグループである。

(チ) Hierocrypt-3 (128ビットブロック暗号)

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

(リ) RC6 Block Cipher (128ビットブロック暗号)

---

<sup>7</sup> : 電子政府用システムとして、新システムを構築する場合は、より長いブロック長が使用可能な状況にあれば、128ビットブロック暗号を選択するのが望ましい。

安全性について、今のところ問題は見つかっていない。Pentium III上での暗号化が最速であるが、ソフトウェア処理速度はプラットフォームに大きく依存する。

なお、CRYPTREC事務局では、2002年10月16日付文書で、RSAセキュリティ株式会社から、「知的財産権上の問題により、今後RC6の普及活動は行わない」との連絡を受領している。

(ヌ) SC2000 (128ビットブロック暗号)

安全性について、今のところ問題は見つかっていない。処理速度は速いグループである。

(ル) MUGI (ストリーム暗号)

安全性について、今のところ問題は見つかっていない。ソフトウェアによる処理速度は速いグループである。

(ロ) MULTI-S01 (ストリーム暗号)

安全性について、今のところ問題は見つかっていない。ソフトウェアによる処理速度は速いグループである。

(ワ) RC4 (ストリーム暗号)

標準仕様 (ワード長 $n=8$ 、状態数256)のRC4については、現在のところ、現実的な解読法は提案されていない。しかし、秘密鍵から生成される初期状態によっては、必ずしも安全ではないという報告がなされている。したがって、RC4の利用に関してその初期状態の決定には注意が必要である。

SSL3.0/TLS1.0での利用に関しては、現在のところその安全性に関して欠陥は報告されていない。ただし、SSL3.0/TLS1.0の仕様上は40ビット秘密鍵 (40-bit RC4) と128ビット秘密鍵 (128-bit RC4) が利用可能であるが、CRYPTRECとしては、40ビット秘密鍵によって初期状態を生成する40-bit RC4は鍵の推定が可能であることから安全ではないと判断する。

(3) ハッシュ関数<sup>8</sup>

(イ) RIPEMD-160

---

<sup>8</sup> : 電子政府用システムとして、新システムを構築する場合は、より長いハッシュ値のものを採用することができるのであれば、ハッシュ値が256ビット以上となるハッシュ関数を選択することが望ましい。ただし、例えば、公開鍵暗号の仕様上利用すべきハッシュ関数が指定されている場合やインターオペラビリティの必要性が生じる場合はこの限りではない。

安全性について、いまのところ問題は見つかっていない。

(口) SHA-1

安全性について、いまのところ問題は見つかっていない。

(ハ) SHA-256

安全性について、いまのところ問題は見つかっていない。

(ニ) SHA-384

安全性について、いまのところ問題は見つかっていない。

(ホ) SHA-512

安全性について、いまのところ問題は見つかっていない。

(4) 擬似乱数生成系

(イ) PRNG in ANSI X9.42-2001 Annex C.1/C.2

パラメータが適切に設定された Annex C.1 については、今のところ、実用上の重大な問題点は見つかっていない。適切なパラメータの設定法については CRYPTREC Report 2002 の該当節を参照のこと。なお、Annex C.2 については強い攻撃法を仮定した場合の弱点が指摘されているので推奨できない。

(口) PRNG in ANSI X9.62-1998 Annex A.4

パラメータによっては擬似乱数出力分布について、PRNG for DSA in FIPS PUB 186-2 Appendix 3 を利用した DSA に対する攻撃に使われたと同様の大きな偏りが生じるので推奨できない。

(ハ) PRNG in ANSI X9.63-2001 Annex A.4

パラメータによっては擬似乱数出力分布について、PRNG for DSA in FIPS PUB 186-2 Appendix 3 を利用した DSA に対する攻撃に使われたと同様の大きな偏りが生じるので推奨できない。

(ニ) PRNG for DSA in FIPS PUB 186-2 Appendix 3

{0, 1}の分布の偏りを利用した  $2^{64}$  の計算量と  $2^{22}$  の既知署名を必要とする攻撃法が発表されている。

この攻撃法は DSA での擬似乱数の使用時に特定の一つの鍵の使用回数を 200 万回以下に抑えることで防御できるものの、擬似乱数としては乱数出力に大きな偏りが生じているので推奨できない。

(ホ) PRNG for general purpose in FIPS PUB 186-2 (+ change notice 1) Appendix 3.1

いまのところ、パラメータを適切に設定すれば、実用上の重大な問題点は見つかっていない。但し、仕様書中で定義されている使い方の中には安全とは言い切れない方法が含まれているので、利用の際には適切なパラメータの設定法については CRYPTREC Report 2002 の該当節を参照の上、適切な使い方を選択する必要がある。

(ヘ) PRNG in FIPS PUB 186-2 (+ change notice 1) revised Appendix 3.1

いまのところ、パラメータを適切に設定すれば、実用上の重大な問題点は見つかっていない。但し、仕様書中で定義されている使い方の中には安全とは言い切れない方法が含まれているので、利用の際には適切なパラメータの設定法については CRYPTREC Report 2002 の該当節を参照の上、適切な使い方を選択する必要がある。

なお、今回の評価結果は、現時点で想定される攻撃等に対する安全性等評価したものであり、将来にわたって安全性が保証されるものではなく、自ずと限界があるものであり、本報告書に記載されている評価結果等の情報を利用した結果として生じる損害等に対して責任を持つことはできない。

### 3.3. 電子政府推奨暗号リスト

暗号技術評価委員会から報告された暗号技術評価結果に基づき、第4回検討会会合(平成14年11月27日)において、電子政府推奨暗号リスト案を作成した。リスト案の作成にあたっては、2001年度に暗号技術検討会の下に設置した「要件調査ワーキンググループ」における検討結果に基づき、暗号強度が十分高く、10年間電子政府システムで安心して使えること、一般に使われる商用ソフトにあらかじめ入っているか、入る可能性の高いものが選ばれること、等を考慮した。

リスト案については、平成14年11月28日から平成14年12月25日まで、総務省及び経済産業省においてパブリックコメントを行った。その結果寄せられた意見等を第5回検討会会合(平成15年2月12日)において検討した結果、平成15年2月20日に、両省から電子政府推奨暗号リストとして公表された。(21頁及び22頁にリストを掲載)

電子政府推奨暗号リストには、公開鍵暗号9方式(内訳:署名4方式、守秘2方式、鍵共有3方式)、共通鍵暗号12方式(内訳:64ビットブロック暗号4方式、128ビット

トブロック暗号 5 方式、ストリーム暗号 3 方式)、ハッシュ関数 5 方式、擬似乱数生成系(例示)3 方式の計 29 方式が掲載された。また、利用の際に注意を要する暗号については、個別に注釈が付記された。

電子政府推奨暗号リストの決定を踏まえ、「電子政府の情報セキュリティ確保のためのアクションプラン(第 2 章第 1 項参照)」に基づき、平成 15 年 2 月 28 日に、行政情報システム関係課長連絡会議において、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旨の「各府省の情報システム調達における暗号の利用方針」(参考資料参照)が了承された。

「各府省の情報システム調達における暗号の利用方針」では、今後、総務省及び経済産業省が、電子政府推奨暗号リストに掲載された暗号の安全性及び信頼性について今後の情報通信技術の進展を踏まえ必要に応じて評価する、とされており、両省は CRYPTREC において電子政府推奨暗号の監視を行っていくこととしている。詳細は第 5 章参照。

電子政府推奨暗号リスト

平成15年2月20日

総務省  
経済産業省

| 技術分類  |                              | 名称   |
|-------|------------------------------|--|
| 公開鍵暗号 | 署名                           | DSA  |
|       |                              | ECDSA  |
|       |                              | RSASSA-PKCS1-v1_5  |
|       |                              | RSA-PSS  |
|       | 守秘                           | RSA-OAEP   |
|       |                              | RSAES-PKCS1-v1_5 <sup>(注1)</sup>   |
|       |                              |  |
| 鍵共有   | DH                           |  |
|       | ECDH                         |  |
|       | PSEC-KEM <sup>(注2)</sup>     |  |
| 共通鍵暗号 | 64 ビットブロック暗号 <sup>(注3)</sup> | CIPHERUNICORN-E  |
|       |                              | Hierocrypt-L1  |
|       |                              | MISTY1   |
|       |                              | 3-key Triple DES <sup>(注4)</sup>   |
|       | 128 ビットブロック暗号                | AES  |
|       |                              | Camellia   |
|       |                              | CIPHERUNICORN-A  |
|       |                              | Hierocrypt-3   |
|       |                              | SC2000   |
|       | ストリーム暗号                      | MUGI   |
|       |                              | MULTI-S01  |
|       |                              | 128-bit RC4 <sup>(注5)</sup>  |
|       |                              |  |
| その他   | ハッシュ関数                       | RIPEMD-160 <sup>(注6)</sup>   |
|       |                              | SHA-1 <sup>(注6)</sup>  |
|       |                              | SHA-256  |
|       |                              | SHA-384  |
|       |                              | SHA-512  |
|       | 擬似乱数生成系 <sup>(注7)</sup>      | PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1   |
|       |                              | PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1         |
|       |                              | PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1 |
|       |                              |  |
|       |                              |  |

注釈：

(注1) SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

(注2) KEM ( Key Encapsulation Mechanism ) -DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

(注3) 新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

(注4) 3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。

- 1) FIPS46-3 として規定されていること

2) デファクトスタンダードとしての位置を保っていること

- (注5) 128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。
- (注6) 新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。
- (注7) 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

### 3.4. 電子政府推奨暗号の仕様に関する情報提供

電子政府推奨暗号リストにおいては、CRYPTREC で評価・選定した暗号の暗号名のみを掲載しているところであるが、その暗号名に対応する暗号の仕様を一意に保つ必要がある。また、電子政府推奨暗号の調達を円滑に行うためには、調達担当者が電子政府推奨暗号の仕様を容易に入手できることが必要である。しかし、各電子政府推奨暗号の仕様の管理者は CRYPTREC ではなく、応募暗号の提案元又は NIST 等であるため、以下のような方策により、調達担当者に仕様に関する情報を提供することとした。

- (イ) 電子政府推奨暗号の仕様を可能な限りTAO及びIPAのホームページに掲載する。
- (ロ) 電子政府推奨暗号のうちその仕様をTAO及びIPAのホームページに掲載することができないものについては、当該暗号の仕様を参照することのできるホームページのURL、あるいは、その仕様を参照する方法をTAO及びIPAのホームページに掲載する。
- (ハ)(ロ)の場合であって、当該暗号の仕様を参照することができなくなった場合には、その旨を TAO 及び IPA のホームページに掲載する。

## 4．暗号調達のためのガイドブックについて

### 4．1．暗号調達ガイドブック作成 WG 設置の目的

電子政府推奨暗号リストの決定により、電子政府において安全性及び信頼性に優れた暗号アルゴリズムを採用することが可能になった。しかし実際に、各府省の調達担当者が、利用目的に合った暗号アルゴリズムを電子政府推奨暗号リストから適切に選択するためには、調達するシステムにおける暗号の利用目的の抽出から、暗号アルゴリズムの選定までの手順を分かりやすく示す手引書が望まれるところである。

そこで、暗号技術検討会の下に、暗号研究者、セキュリティの専門家及びシステム開発の専門家から構成される「暗号調達ガイドブック作成 WG (以下「ガイドブックWG」という。リーダ：佐々木良一東京電機大学教授)」を平成 14 年 5 月に設置し、暗号技術評価委員会及び公開鍵暗号 / 共通鍵暗号評価小委員会の協力を得つつ、各府省の調達担当者が適切な電子政府推奨暗号を円滑に調達するための「暗号調達のためのガイドブック (以下、ガイドブック)」を作成した。

### 4．2．ガイドブック作成の進め方

#### 4．2．1．対象とする読者

ガイドブックの作成にあたっては、各府省における電子政府システムの調達の担当者が読者となることを想定するとともに、暗号やセキュリティに関する知識があまり豊富でない読者でも理解できるような記述レベルを目指すことにした。

#### 4．2．2．盛り込む内容

上記のような読者を対象とすることから、ガイドブックには以下のような内容を盛り込むことにした。

- (1) 暗号の利用目的の抽出から暗号アルゴリズムの選定までの手順の解説
- (2) 電子政府推奨暗号及び電子政府推奨暗号リストの解説
- (3) 調達仕様書作成にあたり、暗号に関連して留意すべき点

#### 4．2．3．ISO/IEC15408 を活用した調達との関連

セキュリティに関する信頼度の高い情報システムの構築については、既に「可能な限り ISO/IEC15408 に基づいて評価又は認証された製品等の利用を推進する」旨の省庁間合意が成されている。ただし、ISO/IEC15408 では、暗号技術の選択に関する要件については触れられていない。

そこで、セキュリティに関する諸要件と暗号に関する要件をそれぞれ指定して調達を進める場合は、本ガイドブックと「ISO/IEC15408 を活用した調達のガイドブック (経済産業省情報セキュリティ政策室発行)」を並行して参照することを意図した。

#### 4.2.4. 検討方法

上記の内容について、以下の手順及び方法により検討を行った。また、暗号アルゴリズムの解説をはじめ、技術的な内容の記述に関しては、暗号技術評価委員会及び公開鍵暗号 / 共通鍵暗号評価小委員会の協力を得た。

##### (1) 調達担当者及び情報システム担当者へのヒアリング

検討に先立ち、システム調達（特に暗号調達）についての現状、及び、ガイドブックに対する要望を把握するため、各府省の調達担当者及び情報システム担当者へのヒアリングを行った。また、ガイドブックの原案を作成した時点で再びヒアリングを行い、記述内容に関するコメントを求めた。

##### (2) 海外の電子政府の事例に関する調査

海外の電子政府システムにおける、暗号調達ガイドラインの事例を調査した。

##### (3) 作業委員会による編集

ガイドブックWGの下に作業委員会を設置し、上記ヒアリング及び事例調査等に基づいてガイドブック原案の作成作業を集中的に行った。同委員会は平成 14 年 6 月から 8 月まで計 7 回開催した。

#### 4.2.5. WG 会合の開催状況

##### 【第 1 回】 5 月 22 日（水）

（主な議題）会合開催スケジュール、検討事項、目次案及び作業事項の確認

##### 【第 2 回】 7 月 8 日（月）

（主な議題）ガイドブック骨子案の検討、海外電子政府事例の確認

##### 【第 3 回】 7 月 19 日（金）

（主な議題）ガイドブック一次案の検討

##### 【第 4 回】 9 月 3 日（火）

（主な議題）ガイドブック最終案の検討

##### 【第 5 回】 9 月 24 日（火）

（主な議題）ガイドブック最終案の検討

##### 【第 6 回】 11 月 19 日（火）

（主な議題）ガイドブック案の決定

#### 4.3. ガイドブックの概要

##### 4.3.1. システム全体の検討作業と暗号調達作業との関わり

暗号は、情報システムの構築作業の中でセキュリティ対策の一部として利用されるので、暗号を調達するにあたっては、その前段としてリスク分析を行うことにより、どんな目的で暗号を利用すべきか、整理しておく必要がある。(図1)

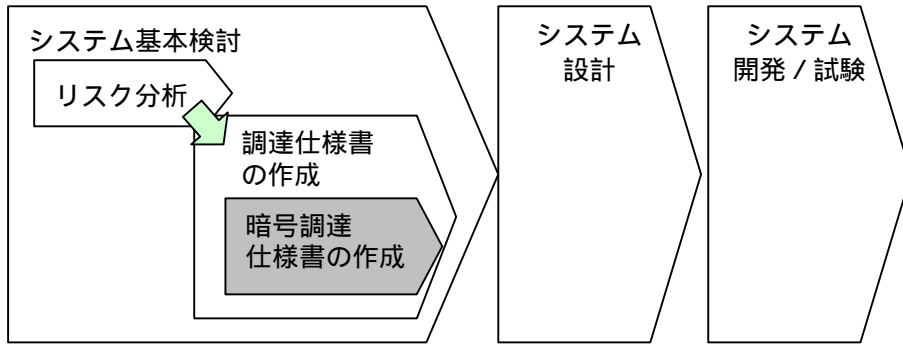


図1 システム構築作業の流れ及び暗号調達の位置付け

このリスク分析に基づき、システムに必要となる暗号アルゴリズムを選定していくことになるが、その手順は図2に示すようなものになる。ガイドブックでは、この手順に沿って、暗号調達、及び、この手順を進める上で必要となる技術的概念である暗号利用形態及び暗号技術分類に関する解説、電子政府推奨暗号に選定された各暗号アルゴリズムの概要について記述した。

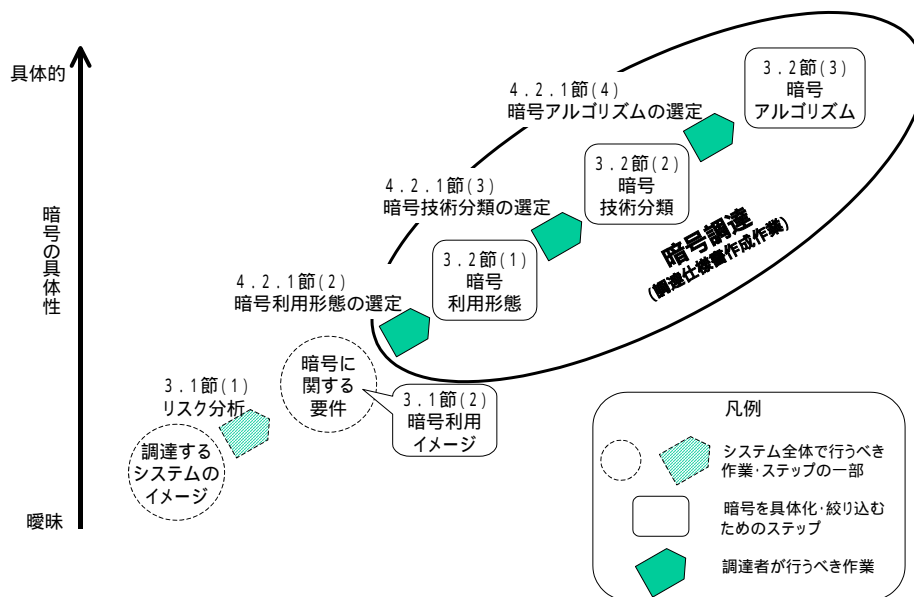


図2 暗号アルゴリズムを選定するまでのステップ  
(図中の数字はガイドブック本文の節番号に対応)

#### 4.3.2. 電子政府システムにおける暗号利用イメージ

e-Japan 重点計画-2002 に挙げられている電子政府の主な項目のうち、「電子申請」「電子調達」「電子納付」「電子情報提供」の各システム及び「政府認証基盤」における暗号利用イメージ図及び説明を記載した。

#### 4.3.3. 暗号利用形態及び暗号技術分類

電子政府システムにおける暗号の利用目的を分類したものである「暗号利用形態」と、暗号アルゴリズムを機能的、技術的に整理したものである「暗号技術分類」についての解説を記載した。

#### 4.3.4. 電子政府推奨暗号の概要

電子政府推奨暗号に選定された暗号アルゴリズム 29 方式の概要説明、及び、利用にあたっての注意点等を記載した。

#### 4.3.5. 暗号調達の手順に関する説明

暗号アルゴリズムを選定するための作業について、調達担当者及び情報システム担当者へのヒアリング等を基に、2 通りのモデル化を行い、それぞれについて解説した。

##### (1) 暗号調達の流れ

電子政府システムの調達の流れ(図3及び図4)の中で、調達者はシステムに必要な暗号の要件を明確化し、電子政府推奨暗号リストの中から暗号アルゴリズムを絞り込む必要がある。暗号アルゴリズムを絞り込む作業の進め方は、以下に挙げる2つのモデルが考えられる。

##### (イ) 調達者指定モデル

調達仕様書の作成時に、調達するシステムについて詳細に説明し、その中で、電子政府推奨暗号リストから暗号アルゴリズムを指定する方法

##### (ロ) 提案審査モデル

調達仕様書では、暗号については概略を説明するに止め、業者に電子政府推奨暗号リストから暗号アルゴリズムを選択させ、提案資料を見て審査する方法

上記2モデルのうち、調達者指定モデルは仕様書作成段階で暗号への要件を詳細化することが必要となり、提案審査モデルでは提案書受領後の審査段階で同様の作業が必要となる。よって、暗号調達に関して必要となる、調達者の作業は、システム調達全体を通して同等になると考えられる。

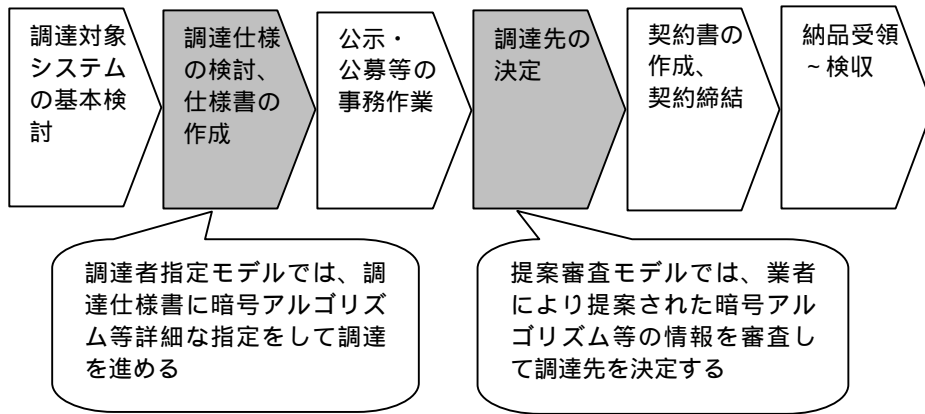


図3 システム調達の流れ及び両モデルの位置付け

| 調達の流れ          | 作業概要  |
|----------------|---|
| 調達対象システムの基本検討  | システムの背景、目的、対象範囲、構築条件、概算費用等、調達を進める基本的事項の整理、その他、暗号に関連した作業として、リスク分析等が行なわれる |
| 調達仕様の検討、仕様書の作成 | システムへの要件となる事項の具体化検討と仕様書の作成（必要に応じて、パブリックコメントを募集する場合がある）                  |
| 公示・公募等の事務作業    | 公示・公募、提案の受付などの事務作業  |
| 調達先の決定         | 調達システムに適合する提案をした業者を選定   |
| 契約書作成、契約締結     | 調達システムの特記事項等を盛り込んで、契約書を作成、契約を締結   |
| 納品受領～検収        | 調達したシステムを受領、仕様と相違ないことを確認検収  |

図4 システム調達の流れにおける作業の概要

(2) 調達者指定モデルによる調達仕様書の作成

調達者指定モデルにおける暗号調達の流れを図5に示す。調達者は、リスク分析の結果等、調達対象システムの基本検討の結果を把握した上で、暗号利用形態の選定、暗号利用分類の選定、暗号アルゴリズムの選定、の順で作業を進め、暗号調達仕様書を完成する。

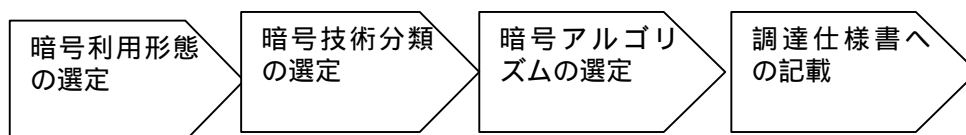


図5 調達者指定モデルにおける暗号アルゴリズム選定までの流れ

(イ) 暗号利用形態の選定

ガイドブックでは、システムの基本検討におけるリスク分析等の様々な作業の一貫として暗号利用形態の選定が行われることを想定し、一般的なセキュリティ

上の脅威に対して、暗号利用形態を選定する場合の基本的な考え方を示した。

(ロ) 暗号技術分類の選定

暗号利用形態の決定後、調達するシステムの目的や特性を考慮して暗号技術分類を選択する。ガイドブックでは、暗号利用形態別に、共通鍵暗号と公開鍵暗号のそれぞれがよく用いられる事例等について説明した。

(ハ) 暗号アルゴリズムの選定

暗号技術分類の決定後、電子政府推奨暗号リストの中から、暗号技術分類別に1つ又は必要な数の暗号アルゴリズムを選択する。ガイドブックには参考資料として、アルゴリズム安全性評価結果(リストに載せた根拠)、主なパラメータ・補助関数に関する要件、国際標準への対応等について一覧表にまとめた「評価・特徴一覧」を掲載した。なお、主な留意点又は着目すべき点は以下のとおり。

(a) 実装方法によっては、電子政府推奨暗号を使用したとしても様々な実装攻撃に曝される危険性を排除できないので、実装攻撃の脅威に対する十分な配慮、検討を行い、適切な対策を施して実装するよう注意する必要がある。

(b) 公開鍵暗号は、暗号利用形態に応じて、プロトコル標準への採用の有無等を考慮して選択する。なお、許容される処理速度の範囲で、使用される鍵長(RSA 暗号の場合、2つの素数の積となる合成数のビット数)を長くする(RSA 暗号の場合は1024ビット以上にする)などの検討が必要である。また、各アルゴリズムの数論的困難性を確保するため、パラメータの選択に十分留意する必要がある。

(c) 共通鍵暗号は、処理速度、メモリ制限環境での実装性、プロトコル標準への採用の有無等を考慮して選択する。ブロック暗号を選択する場合、安全性の面から今後は可能な限りブロック長128ビットの暗号を使用する。なお、ブロック暗号を利用した暗号化処理に関連して、暗号利用モード(Modes of Operation)と呼ばれる技法がいくつか規定されており、各モードごとに実現している目的や機能が異なるので、実装環境や利用用途に応じて、適切な暗号利用モードを選択する必要がある。

(d) ハッシュ関数は、可能であれば256ビット以上の長さのハッシュ値を出力するものを選択することが望ましい。ただし、既に選択した公開鍵暗号又は共通鍵暗号の仕様書でハッシュ関数が指定されている場合は、その中から選択する。

(e) 擬似乱数生成については、リストに掲載されている以外の「暗号的に安全な擬似乱数アルゴリズム」を利用することができる。また、リストに掲載されている暗号アルゴリズムの仕様自体に特定の擬似乱数生成アルゴリズムの使用が規定されている場合は、その使用を妨げるものではない。

## (二) 調達仕様書への記載

上記のような手順により選択した暗号アルゴリズムを、どのように調達仕様書に記載するかを例示した。(図6)

| 暗号による保護を必要とする情報  | 暗号利用形態    | 暗号アルゴリズム                    |
|--|-----------|-----------------------------|
| <ul style="list-style-type: none"> <li>・ 申請データ</li> <li>・ 申請内容確認で授受されるデータ<br/>到達確認通知</li> <li>・ 状況確認で授受されるデータ</li> <li>・ 審査終了通知</li> <li>・ 許認可等公文書の取得要求データ</li> <li>・ 許認可等公文書</li> </ul> | 守秘        | 共通鍵暗号その1                    |
|  | 相手認証      | 公開鍵暗号その1<br>または<br>公開鍵暗号その3 |
|  | 署名        | 公開鍵暗号その1<br>または<br>公開鍵暗号その3 |
| ・ 鍵情報  | 鍵共有       | 公開鍵暗号その2                    |
| 上記暗号アルゴリズムにて<br>特に指定の無い場合は<br>右記アルゴリズムを使用すること  | ハッシュ関数として | ハッシュ関数その1                   |
|  | 擬似乱数生成として | 擬似乱数生成その1                   |

図6 電子申請システムにおける暗号アルゴリズム指定表の記載例<sup>9</sup>

## (3) 提案審査モデルによる調達仕様書の作成

提案審査モデルの場合、調達者は調達仕様書に下記項目を記載する。

### (イ) 電子政府推奨暗号の使用に関する指示

調達するシステムには、可能な限り電子政府推奨暗号を使用するよう、提案を行う業者に指示する。

### (ロ) 暗号アルゴリズム選定理由の明記に関する指示

提案書の審査において、調達者は、暗号アルゴリズムの選定が妥当であることを検証する必要があるため、調達するシステムのイメージから暗号アルゴリズム選定までの過程を、理由を付けて分かりやすく説明した文書を提案書に添付するよう、調達を行う業者に指示する。

<sup>9</sup> : 実際の調達においては、サンプル自体を引用するのではなく、個別具体的な状況に応じた適切な調達を行うこと

#### 4.3.6. 調達仕様書作成上の留意点

調達者が調達仕様書を作成する際に留意すべき点を記載した。

##### (1) 複数暗号アルゴリズムの実装について

電子政府システムにおけるサーバや、パソコン等に複数の暗号アルゴリズムを同時に実装する場合、セキュリティ面だけ考えると以下のようにいえる。

##### (イ) 複数暗号実装のメリット

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おいては暗号解読問題発生の可能性が低いとはいえ、1つの暗号アルゴリズムが解読された場合に備えて、複数の暗号を実装し切り替えられるようにすることは、セキュリティを向上する上で有効である。

##### (ロ) 複数暗号実装のデメリット

複数の暗号アルゴリズムを同じシステムに実装し、これを切り替えて利用できるように作り込んだ場合、切り替え部分等にセキュリティホールが混入してしまう恐れがある。そのため脆弱性が上昇し、セキュリティが減少する可能性がある。

##### (ハ) 対応策

したがって、セキュリティ脆弱性の上昇により懸念されるリスクが、暗号アルゴリズムが解読されるリスクに比べて小さいと判断された場合にのみ、複数暗号アルゴリズムを実装すべきである。

なお、インターネットなどを通じて広く一般国民が利用するシステムにおいて、利用者の利用する暗号アルゴリズムが全体として1つに特定できない場合などには、政府側のサーバ装置で、複数の暗号アルゴリズムをどちらでも扱えるようにしておかなければならない場合がある。このような場合には、セキュリティホールを作りこまないよう十分な配慮をしつつ複数暗号を実装しておくことが利用者の利便性を向上させる上でも望ましい。

##### (2) 暗号プログラムの配布と外国為替及び外国貿易法による暗号輸出規制

不特定多数の利用者に、暗号機能を含むプログラムを配布することは、ワッセナーアレンジメントに基づき、外国為替及び外国貿易法による規制がある。

ガイドブックでは、電子政府システムにおいて不特定多数の利用者に暗号機能を含むプログラムを配布する場合の、法制度上の留意点について解説した。

#### 4.3.7. 調達先の決定、契約及び納品

調達仕様書に基づき提出される提案書の審査、調達者の決定、契約、納品における、

暗号調達の観点からの留意点を記載した。

#### 4.3.8. 参考資料

##### (1) 各府省の情報システム調達における暗号の利用方針

電子政府推奨暗号の利用に関する府省間合意文書を掲載した。

##### (2) 電子政府推奨暗号の評価・特徴一覧

電子政府推奨暗号の、アルゴリズム安全性（リストに載せた根拠）、主なパラメータ・補助関数に関する要件、国際標準等への採用状況等に関する情報を、一覧表にして掲載した。

## 5．今後の CRYPTREC 活動について

CRYPTREC では、発足以来の当面の目標であった、電子政府推奨暗号リストの策定及び暗号調達のためのガイドブックの作成を行った。しかし、国民が安心して電子政府を利用できるようにするためには、電子政府の安全性及び信頼性を確保するための活動を引き続き推進していく必要があり、CRYPTREC としても、それに貢献していくことが重要であるとの認識に立っている。そこで、2003 年度以降、以下のような活動を行っていくこととした。

### 5．1．今後の CRYPTREC の活動目的及び活動内容

#### 5．1．1．活動目的

CRYPTREC は、暗号技術及び暗号関連技術の評価等を通じて、電子政府等の安全性及び信頼性の確保に貢献することを目的として活動する。

#### 5．1．2．活動内容

CRYPTRECは、2003年度以降、以下の活動を行う。なお、今後、新たに必要と考えられる事案が生じた場合には、その都度、暗号技術検討会において具体的な活動内容を検討していくものとする。

##### (1) 電子政府推奨暗号の監視

電子政府推奨暗号に選定された各暗号の安全性等についての情報収集や評価を行い、必要に応じて修正情報の周知やリストからの削除等の電子政府推奨暗号リストの変更を行う。

##### (2) 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

###### (イ) 暗号アルゴリズム等を主な対象とする調査・検討

暗号アルゴリズムや素因数分解問題等の数論的問題の困難性を主な対象とする調査及び検討を行う。

###### (ロ) 暗号実装関連技術を主な対象とする調査・検討

実装攻撃等の暗号実装関連技術を主な対象とする調査及び検討を行う。

##### (3) 電子政府推奨暗号リストの改訂に関する調査・検討

将来の電子政府推奨暗号リストの改訂（新たな電子政府推奨暗号リストの策定及び本件電子政府推奨暗号リストの廃棄）のために必要な調査及び検討（電子政府における暗号利用状況調査等）を行う。その際、総務省、経済産業省及び行政情報シ

ステム関係課長連絡会議との連携を図ることとする。

(4) 暗号モジュール評価基準の作成

暗号モジュール評価基準及び試験基準を作成する。

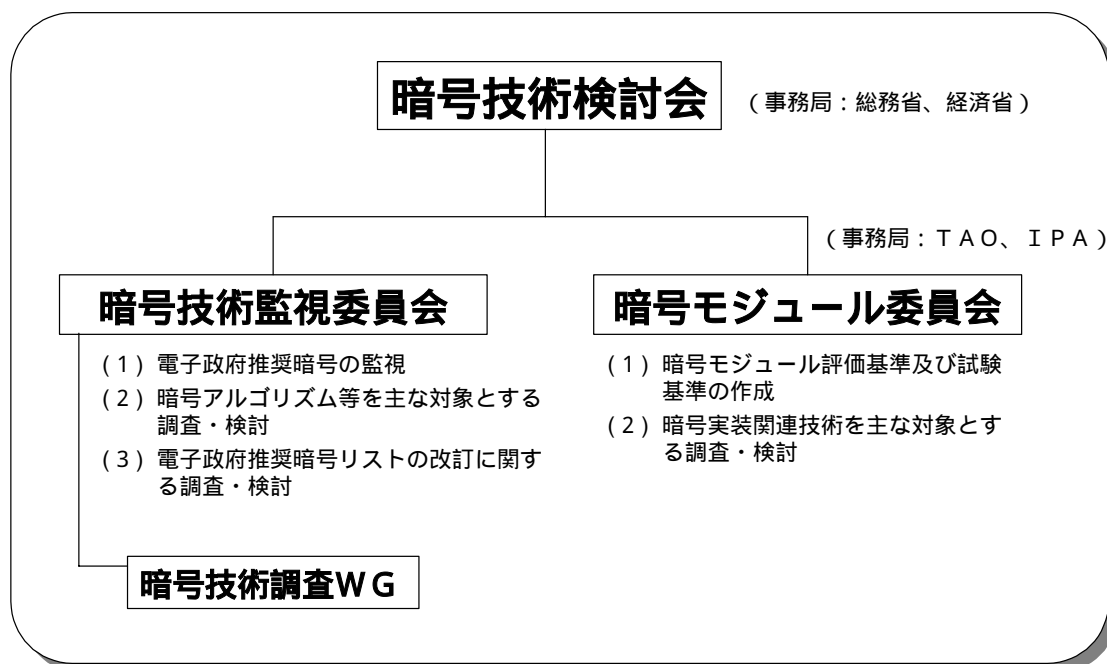
5.2. 今後のCRYPTREC体制

2003年度以降、当面のCRYPTRECの体制として、暗号技術検討会は存続し、暗号技術検討会の下に「暗号技術監視委員会」及び「暗号モジュール委員会」を設置する。また、暗号技術監視委員会の下に「暗号技術調査WG」を設置する(図7:今後のCRYPTRECの体制図)。

従来の暗号技術評価委員会は暗号技術監視委員会に発展的に再編することとする。また、公開鍵暗号評価小委員会及び共通鍵暗号評価小委員会は暗号技術調査WGに再編することとする。

各委員会及びWGの位置づけ、構成及び機能は以下のとおり。

### 今後のCRYPTREC体制図



(図7)

5.2.1. 暗号技術検討会

暗号技術検討会(「検討会」)は、電子政府推奨暗号リストに掲載された暗号技術の

監視、関連する調査研究、及び、暗号技術の危殆化や暗号プロトコル等その他暗号技術の評価・利用等に関する事項について、総合的な観点から検討を行う。また、電子政府等のセキュリティの確保のため、政府のセキュリティ関係機関等との連携、調整を図る。

#### 5.2.2. 暗号技術監視委員会

暗号技術監視委員会（以下、「監視委員会」）は検討会の下に設置される。監視委員会は、数名の有識者等により構成され、安全性及び信頼性確保の観点から、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討を適宜行うとともに電子政府推奨暗号リストの改訂に関する調査・検討を行う。なお、監視委員会の日常業務を行う監視要員をTAO / 通信総合研究所（CRL）（両機関は2004年4月に統合予定）及びIPAに配置する。

##### （1）暗号技術調査WG

（イ）暗号技術調査WG（以下、「調査WG」）は、電子政府推奨暗号リストの変更案等の作成、及び電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする具体的な調査・検討に際して監視委員会を支援することを目的として、監視委員会の下に設置される。

（ロ）調査WGは、監視委員会委員、従来の暗号技術評価委員会委員、共通鍵暗号評価小委員会委員及び公開鍵暗号評価小委員会委員等を元に構成される。これらのWGメンバーは、共通鍵暗号評価グループ及び公開鍵暗号評価グループに区分される。監視委員会は、事案の性質に応じて、共通鍵暗号評価グループ及び/または公開鍵暗号評価グループを召集し、調査WGを開催する。調査WGは、監視委員会に対して電子政府推奨暗号リストの変更案等の作成に関する専門的助言を行う。

（ハ）その他、調査WGは、監視委員会の要望により事案に応じて開催され、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする具体的な調査・検討（電子政府における暗号利用状況調査等）を行い、監視委員会に対して専門的な助言を行う。

#### 5.2.3. 暗号モジュール委員会

暗号モジュール委員会は検討会の下に設置される。暗号モジュール委員会は、ISO/IEC等の国際標準の動向を注視しつつ、将来的に政府調達基準等として利用され得ることをも視野に入れながら、2005年3月を目処に暗号モジュール評価基準及び試験基準を作成する。また、電子政府推奨暗号の安全性及び信頼性確保のための、主として暗号実装関連技術等を対象とする調査・検討を行う。

### 5.3. 電子政府推奨暗号の監視

#### 5.3.1. 電子政府推奨暗号の監視の基本的考え方

今後、CRYPTRECは、電子政府推奨暗号の安全性及び信頼性を確保することを目的とし、継続的に暗号技術に関する情報を収集し、必要に応じて暗号の安全性を評価する電子政府推奨暗号の監視活動を行う。

監視は、以下のような考え方に基づいて実施することとする。

- (1) 実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。
- (2) 電子政府推奨暗号の仕様変更は原則として認めない。
- (3) 電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

#### 5.3.2. 電子政府推奨暗号の監視の具体的内容

電子政府推奨暗号の監視は、調査研究、リストからの削除、修正情報の周知等からなる。それぞれの具体的内容は以下(1)～(4)のとおりとする。

- (1) 暗号技術調査・研究及びデータの蓄積  
暗号技術に関する調査研究を実施し、国際標準化の動向等種々のデータを蓄積する。
- (2) 電子政府推奨暗号の削除
  - (イ) 電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、かつ当該暗号の仕様を変更すること無く攻撃を回避することが不可能であると判断される場合には、当該暗号をリストから削除する。
  - (ロ) 電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、かつ当該暗号の仕様を変更すること無く、パラメータの修正等の簡易な修正を行うことによって攻撃を回避することが可能であると判断される場合であっても、その方法等を記述した修正情報が当該暗号の仕様書の管理者より提案されない場合には、当該暗号をリストから削除する。

(3) 電子政府推奨暗号に関する修正情報の周知

(イ) 電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いと判断される場合であって、電子政府推奨暗号の仕様変更ではなくパラメータの修正等の簡易な修正を実施することにより当該攻撃を回避することができると判断される場合には、当該修正方法を修正情報として周知する。

(ロ)(イ)の場合において、修正情報は仕様書の管理者から提案させることとし、監視委員会は、提案された修正情報を加味して当該電子政府推奨暗号の安全性評価を実施する。仕様書の管理者より修正情報の提案がなされない場合には、当該暗号をリストから削除する。

(ハ) 監視委員会は応募暗号<sup>10</sup>以外の電子政府推奨暗号が実運用環境上において攻撃により破られる可能性が高いとは判断していないにも関わらず、当該暗号に関する修正情報が仕様書の管理者により発行された場合であって(パラメータ修正等の簡易な修正に限る)監視委員会が当該修正情報を加味した上で安全性評価を実施し、安全性が確保されていると判断する場合には当該修正情報を周知する。

(4) 電子政府推奨暗号の追加

(イ) 電子政府推奨暗号リストの改訂(新たな電子政府推奨暗号リストの策定及び本件電子政府推奨暗号リストの廃棄)が行われるまでは、電子政府推奨暗号の追加は例外的な扱いとする。

(ロ) 電子政府推奨暗号リストに掲載されていない暗号が国際的に高い評価を得ている場合であって、暗号技術検討会が当該暗号を新たに評価することが必要と判断し、かつ、評価の結果、暗号技術検討会が当該暗号を電子政府推奨暗号リストへ掲載することが適切と判断する場合には、当該暗号を電子政府推奨暗号リストへ追加する。

(ハ) 電子政府推奨暗号リストへの追加を検討する場合には、「10年間は安心して利用できる」という観点から評価を行う。

---

<sup>10</sup> : 応募暗号 : 電子政府推奨暗号のうち、以下のものを指す。

(公開鍵暗号) ECDSA, RSA-PSS, RSA-OAEP, ECDH, PSEC-KEM

(共通鍵暗号) CIPHERUNICORN-E, Hierocrypt-L1, MISTY1,

Camellia, CIPHERUNICORN-A, Hierocrypt-3, SC2000,

MUGI, MULTI-S01

- (二) 電子政府調達者より、電子政府推奨暗号リストに無い新たな用途及び当該用途に適した暗号の追加に関する要望がよせられた場合であって、かつ、暗号技術検討会としても当該用途の追加が適切と判断した上で、それに適した暗号の評価を実施し、その結果、適切な暗号を選定した場合には、当該用途及び当該暗号を電子政府推奨暗号リストへ追加することとする。

### 5.3.3. 電子政府推奨暗号の監視の手順

電子政府推奨暗号の監視の手順は、(1) 監視委員会における情報収集、(2) 監視委員会における情報分析、(3) 監視委員会及び検討会における審議及び決定の3段階からなる。具体的には以下のとおりとする。

#### (1) 監視委員会における情報収集

監視委員会において、電子政府推奨暗号の安全性に関する情報を迅速かつ円滑に入手するためには、監視委員会自らが情報収集を行うだけでなく、過去3年間のCRYPTREC活動によって形成された、暗号研究者とのネットワークを活用することが重要である。そこで、以下のように情報収集を行うこととする。

- (イ) 国内外の学会等への参加等を通じて暗号技術に関する情報(学術論文、発表原稿等)を収集する。
- (ロ) 暗号技術調査WGメンバー等との連絡体制を整備し、同メンバーから恒常的に情報提供を受ける。
- (ハ) 応募暗号については、原則として応募元から情報提供を受ける。
- (ニ) その他一般からの情報提供も受ける。

#### (2) 監視委員会における情報分析

監視委員会は、(1)により収集された情報を分析し、電子政府推奨暗号の削除等を検討すべき事態が発生しているか否か判断する。その結果、監視委員会が電子政府推奨暗号の削除等を検討すべき事態が発生していると判断する場合には、事案に応じて、暗号技術調査WGの共通鍵暗号評価グループおよび/または公開鍵暗号評価グループを召集し、暗号技術調査WGを開催する。ただし、監視委員会が、電子政府推奨暗号の削除等を直ちに行うべき事態が発生していると判断する場合は、その緊急性に応じた対応を実施する。

#### (3) 監視委員会及び検討会における審議及び決定

- (イ) 暗号技術調査WGは、技術的観点から、監視委員会に対して助言を行う。なお、暗号技術調査WGは、応募元等より修正情報の提供を受け、同修正情報

を加味した暗号の安全性評価も行う。

(ロ) 監視委員会は、暗号技術調査WGの助言を踏まえて、電子政府推奨暗号の削除等を実施するか否かについて素案を作成し、暗号技術検討会に報告する。

(ハ) 暗号技術検討会は、総合的な観点から当該素案を審議し電子政府推奨暗号の削除等に関する案を作成する。同案が電子政府推奨暗号リストに変更を加えるものである場合、総務省及び経済産業省はパブリックコメントに付し、その結果を暗号技術検討会に報告する。暗号技術検討会は、パブリックコメントの結果を踏まえて、電子政府推奨暗号の削除等に関する案を決定する。

(ニ) 暗号技術検討会の決定に基づいて電子政府推奨暗号リストの変更を行った場合、総務省及び経済省は、電子政府推奨暗号リストの変更について行政情報システム関係課長連絡会議等に連絡する。

### 電子政府推奨暗号の削除等の手順

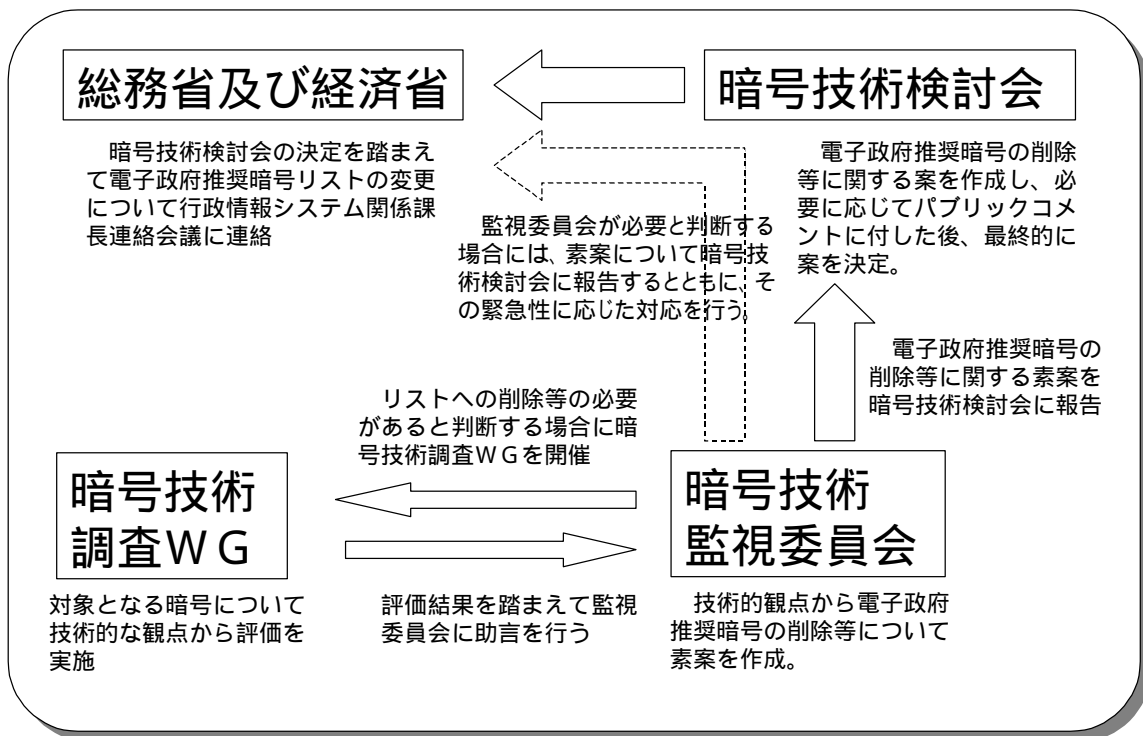


図 8 : 電子政府推奨暗号削除等の手順

## 5.4. 電子政府推奨暗号リストの改訂

### 5.4.1. 基本的認識

電子政府推奨暗号は、現時点において、今後 10 年間は安心して利用できるという観点から選定された暗号である。しかし、暗号に対する解析や攻撃の技術や手法はますます高度化しており、電子政府推奨暗号は常に危殆化の危険にさらされている。一方、新たな暗号の開発も進んでおり、今後、安全性や実装性に優れた新しい暗号の出現が期待される場所である。そこで、危殆化した暗号の削除や新しい暗号の選定等により、電子政府推奨暗号リストを一定期間毎に改訂することが望ましい。改訂を実施する際に、仮に公募を実施する場合は、公募のアナウンス（公募開始時期、公募期間、評価期間、新リスト発表時期等の公表）から新リストの策定まで、5 年程度の期間をかけることが望ましい。

### 5.4.2. 基本的考え方

リストの改訂作業の具体的な実施内容については、電子政府の導入状況及び電子政府推奨暗号の監視状況を考慮しつつ、然るべきタイミングで検討を行うこととする。なお、リスト改訂作業の実施方法としては、現在のところ、以下のような検討事項が想定される場所である。

（想定される検討事項）

- （イ）公募の要否
- （ロ）リスト項目（技術分類等）の見直し
- （ハ）項目別の掲載暗号数
- （ニ）評価基準、評価方法

また、改訂作業の具体的な開始時期については、2003年度以降に暗号技術検討会において検討の上決定するが、改訂作業の完了及び新リストの決定は、遅くとも10年後の2013年までとする。なお、仮に公募を実施するとした場合は、5年程度の期間をかけることが望ましいと考えられることから、遅くとも2008年3月頃には公募のアナウンスを行うことが望ましい。

## 5.5. 暗号モジュールに関する検討

電子政府の安全性及び信頼性を確保するためには、暗号技術レベルの安全性だけでなく暗号技術の実装の安全性を確保する必要があり、この観点から暗号モジュールの安全性評価基準を作成することが急務である。他方、暗号モジュールの安全性評価基準に関しては、米国が自国の政府調達基準であるFIPS140-2のISO/IEC化を提案しており、暗号モジュールの安全性評価基準を我が国において作成するにあたっては、ISO/IEC等にお

ける議論を注視していく必要がある。

このような状況を踏まえて、検討会の下に暗号モジュール委員会を設置する。暗号モジュール委員会は、ISO等の国際標準の動向を注視しつつ、将来的に政府調達基準等として利用され得ることをも視野に入れながら、2005年3月を目処に暗号モジュール評価基準及び試験基準を作成する。

なお、暗号モジュール委員会は、暗号技術監視委員会と連絡をとりつつ、電子政府推奨暗号の安全性及び信頼性確保のための暗号実装関連技術を主な対象とする調査・検討を併せて行うこととする。

**資料「暗号調達のためのガイドブック」**

**参考資料「各府省の情報システム調達における  
暗号の利用方針」**

## 各府省の情報システム調達における暗号の利用方針

平成15年2月28日  
行政情報システム関係課長連絡会議了承

電子政府における情報セキュリティ確保のために、各府省の情報システムにおいて暗号を利用する場合には、一定水準以上の安全性及び信頼性を有する暗号の利用が不可欠であり、また、その安全性・信頼性は客観的な評価を得たものであることが必要である。

かかる観点から、「電子政府の情報セキュリティ確保のためのアクションプラン」（平成13年10月10日、情報セキュリティ対策推進会議）に基づき、総務省及び経済産業省において、電子政府における調達のための推奨すべき暗号のリスト（「電子政府推奨暗号リスト」：別添参照）を策定したところである。

これを踏まえ、各府省は、情報システムの構築に当たり暗号を利用する場合には、調達仕様書において上記暗号リストに掲載された暗号を利用することを入札要件とする等の方法により、必要とされる安全性・信頼性などに応じ、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ものとする。

なお、総務省及び経済産業省は、「電子政府推奨暗号リスト」に掲載された暗号の安全性及び信頼性について、今後の情報通信技術の進展を踏まえ必要に応じ評価を行うとともに、「電子政府推奨暗号リスト」の内容の変更を行う場合には本会議に報告することとする。

## 電子政府推奨暗号リスト

平成15年2月20日

総 務 省

経 済 産 業 省

| 技術分類  |                              | 名称   |
|-------|------------------------------|--|
| 公開鍵暗号 | 署名                           | DSA  |
|       |                              | ECDSA  |
|       |                              | RSASSA-PKCS1-v1_5  |
|       |                              | RSA-PSS  |
|       | 守秘                           | RSA-OAEP   |
|       |                              | RSAES-PKCS1-v1_5 <sup>(注1)</sup>   |
|       | 鍵共有                          | DH   |
|       |                              | ECDH   |
|       |                              | PSEC-KEM <sup>(注2)</sup>   |
| 共通鍵暗号 | 64 ビットブロック暗号 <sup>(注3)</sup> | CIPHERUNICORN-E  |
|       |                              | Hierocrypt-L1  |
|       |                              | MISTY1   |
|       |                              | 3-key Triple DES <sup>(注4)</sup>   |
|       | 128 ビットブロック暗号                | AES  |
|       |                              | Camellia   |
|       |                              | CIPHERUNICORN-A  |
|       |                              | Hierocrypt-3   |
|       |                              | SC2000   |
|       | ストリーム暗号                      | MUGI   |
|       |                              | MULTI-S01  |
|       |                              | 128-bit RC4 <sup>(注5)</sup>  |
|       |                              |  |
| その他   | ハッシュ関数                       | RIPEMD-160 <sup>(注6)</sup>   |
|       |                              | SHA-1 <sup>(注6)</sup>  |
|       |                              | SHA-256  |
|       |                              | SHA-384  |
|       |                              | SHA-512  |
|       | 擬似乱数生成系 <sup>(注7)</sup>      | PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1   |
|       |                              | PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1         |
|       |                              | PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1 |
|       |                              |  |
|       |                              |  |

注釈:

(注1) SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

(注2) KEM (Key Encapsulation Mechanism) -DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

- (注3) 新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。
- (注4) 3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。
- 1) FIPS46-3として規定されていること
  - 2) デファクトスタンダードとしての位置を保っていること
- (注5) 128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。
- (注6) 新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。
- (注7) 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用してても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。