# 3-3-4　CRYPTREC 活動
## －3 ガイドラインの発行と電子政府推奨暗号リスト改定－
## *3-3-4　CRYPTREC Activities: Publication of Three Guidelines and a Revision of the e-Government Recommended Ciphers List*

青野 良範　伊藤 竜馬　大久保 美也子　小川 一人　金森 祥子　黒川 貴司　吉田 真紀　篠原 直行
AONO Yoshinori, ITO Ryoma, OHKUBO Miyako, OGAWA Kazuto, KANAMORI Sachiko, KUROKAWA Takashi, YOSHIDA Maki, and SHINOHARA Naoyuki

本稿では 2016 年度から 2023 年度までの間にセキュリティ基盤研究室が主に担当した CRYPTREC（Cryptography Research and Evaluation Committees）の活動について紹介する。

This paper outlines the activities of the Cryptography Research and Evaluation Committees (CRYPTREC) that the Security Fundamentals Laboratory has primarily managed from FY2016 to FY2023, including the publication of three guidelines and the revision of the e-Government recommended ciphers list.

## 1　まえがき

CRYPTREC とは Cryptography Research and Evaluation Committees の略であり、暗号技術の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。NICT では CRYPTREC の中の暗号技術評価委員会の事務局を主に担当しているため（CRYPTREC の体制については後述）、本稿では暗号技術評価委員会の活動を中心に紹介する。2016 年度から 2023 年度における主な活動として、2016 年度に軽量暗号、2018 年度にハッシュ関数 SHA-1、2022 年度に耐量子計算機暗号と高機能暗号に関するガイドラインをそれぞれ作成するとともに、2023 年度には 2016 年度に作成した軽量暗号に関するガイドラインを改定した。また、2022 年度には CRYPTREC 暗号リストを改定した。これらの活動を含む暗号技術評価委員会の活動の詳細については、CRYPTREC Report [1]、暗号技術検討会報告書 [2] を参照していただきたい。

本稿では、**2** において CRYPTREC の体制について述べる。次に、**3** において 2022 年度に作成した耐量子計算機暗号に関するガイドラインと高機能暗号に関するガイドライン、そして 2023 年度に改定した軽量暗号に関するガイドラインについて述べる。**4** において CRYPTREC 暗号リストの改定について述べ、最後に、**5** において今後の展望について述べる。

## 2　CRYPTREC の体制

### 2.1　体制

CRYPTREC は 2013 年度以降、暗号技術検討会の下に、暗号技術評価委員会及び暗号技術活用委員会を置いた体制になっている。2023 年度については、暗号技術評価委員会の下に、暗号技術調査ワーキンググループ（耐量子計算機暗号）、暗号技術活用委員会の下に、暗号鍵管理ガイダンスワーキンググループを設置し（図 1）、技術の詳細に関し議論した。

### 2.2　委員会の開催状況

暗号技術評価委員会、暗号技術調査ワーキンググループの開催回数は、状況により多少変化はするが、例年ではどちらも年 2 回が開催されてきた。2023 年度は、2023 年 7 月 3 日に第 1 回暗号技術評価委員会、2024 年 2 月 27 日に第 2 回暗号技術評価委員会が開催された。

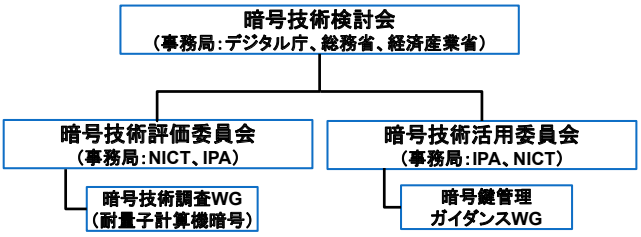

図 1　CRYPTREC 体制図（2023 年度）

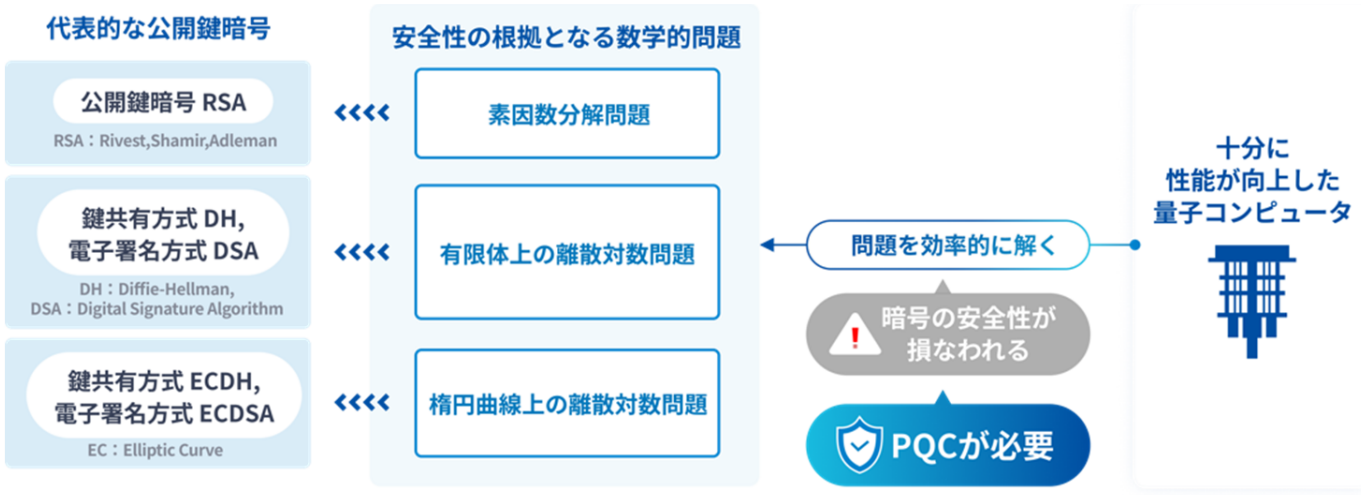


図 2　代表的な公開鍵暗号における安全性の根拠と量子コンピュータ・PQC の関係

また、2023 年 9 月 13 日に第 1 回暗号技術調査ワーキンググループ（耐量子計算機暗号）、2024 年 1 月 19 日に第 2 回暗号技術調査ワーキンググループ（耐量子計算機暗号）が開催された。

## 3　暗号技術評価委員会の活動内容

暗号技術評価委員会では、暗号技術の安全性評価を中心とした技術的な内容の検討、すなわち、

A）新世代暗号に係る調査（耐量子計算機暗号、高機能暗号、軽量暗号等）
B）暗号技術の安全性に係る監視及び評価
C）暗号技術の安全な利用方法に関する調査（技術ガイドラインの整備、学術的な安全性の調査・公表等）

を実施した。

そこで、2021 年度から 2022 年度にかけて、暗号技術調査ワーキンググループ（耐量子計算機暗号）と暗号技術調査ワーキンググループ（高機能暗号）の 2 つのワーキンググループを設置するとともに、2022 年度末までに『暗号技術ガイドライン（耐量子計算機暗号）』と『暗号技術ガイドライン（高機能暗号）』を作成し、2022 年 4 月に CRYPTREC の Web サイト [3][4] で公開した。また、2021 年度から 2023 年度にかけて、暗号技術評価委員会を中心に 2016 年度に作成した『CRYPTREC 暗号技術ガイドライン（軽量暗号）』[5] を改定し、2024 年 4 月に CRYPTREC の Web サイト [6] で公開した。また、2023 年 3 月には『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）』[7] を公開した。本リストは 2013 年 3 月に策定した「電子政府における調達のために参照すべき暗号リスト（CRYPTREC 暗号リスト）」（初版 [8]：2013 年 3 月 1 日、最終改定 [9]：2023 年 3 月 8 日）を改定したものである。

### 3.1　暗号技術ガイドライン（耐量子計算機暗号）

現在広く使われている RSA 暗号・楕円曲線暗号の安全性の根拠となる素因数分解問題・楕円曲線上の離散対数問題が大規模な量子コンピュータにより高速に解かれることが 30 年ほど前に証明された。以降、量子コンピュータの開発が世界的に進められ、特にこの 10 年間で大幅な性能進化が生じた。2024 年現在での量子コンピュータの性能は、現用の暗号を解くまでには達していないものの、今後数十年以内には現実の暗号の脅威となるという予測が存在する。

一方で、大規模な量子コンピュータが開発された後にも現実的なリソースでは解読が困難と期待される暗号技術の開発と標準化活動も進んでいる。古典（量子コンピュータではない現在のコンピュータ）・量子双方のコンピュータによる攻撃に耐性のある暗号を総称して耐量子計算機暗号（Post-Quantum Cryptography: PQC）と呼ぶ（図 2）。

CRYPTREC では 2017 年度に暗号技術調査ワーキンググループ（暗号解析評価）を設置、2 年間で PQC の動向調査を行い 2018 年度に『耐量子計算機暗号の研究動向調査報告書』[10] を公開した。その後、量子コンピュータが量子超越を実現したと主張する発表と世の中での暗号に対する影響への関心の高まりを受け、2020 年 2 月に注意喚起情報の形で『現在の量子コンピュータによる暗号技術の安全性への影響』[11] を公開した。

PQC の発展に対応する形で 2021 年度に暗号技術調査ワーキンググループ（耐量子計算機暗号）――以降 PQC WG と記述する――を設置、2 年間の研究動向調

査を行い 2022 年度に『CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）』（以下ガイドライン）[3] 及び『耐量子計算機暗号の研究動向調査報告書』（以下調査報告書）[12] を公開、2023 年度以降も最新の研究動向調査を継続している。

一般的な PQC の定義として学術的に合意の取れたものは存在しないが、狭義には公開鍵暗号の守秘・署名・鍵共有の中で、その安全性の根拠となる計算問題の求解が量子コンピュータを用いても困難であると期待される一連の暗号技術を指す。守秘とは、第三者に秘匿する文書等を暗号化するための技術である。署名は、文書等を作成する人、文書等を送る人及び通信している機器の認証を行う、若しくは、それらに電子的な署名を付与するための技術である。鍵共有は、文章等の送受信をする人の間での暗号鍵の共有のための技術である。PQC WG においては守秘・鍵共有・署名をそれらの安全性の根拠となる計算問題の種類ごとに 5 つのグループ（格子に基づく暗号技術、符号に基づく暗号技術、多変数多項式に基づく暗号技術、同種写像に基づく暗号技術、ハッシュ関数に基づく署名技術）に分類し、動向調査を行った。ガイドラインは暗号初学者を対象としており、調査報告書は暗号についての知見を持つ技術者や専門家を対象とした。

ガイドラインの章立ては、第 1 章　はじめに、第 2 章　PQC の活用方法、第 3 章　格子に基づく暗号技術、第 4 章　符号に基づく暗号技術、第 5 章　多変数多項式に基づく暗号技術、第 6 章　同種写像に基づく暗号技術、第 7 章　ハッシュ関数に基づく署名技術としている。そして、PQC の暗号技術を紹介するだけでなく、量子コンピュータの開発、量子コンピュータによる暗号の解読実験、PQC 標準化の最新動向を第 1 章に、暗号初学者向けに PQC の活用方法についての解説を第 2 章で行ったことがガイドラインの特色である。第 3 章から第 7 章までは安全性の根拠となる計算問題の種類ごとにまとめ、各章で計算問題の代表的な求解方法、ベースとなる教科書的な暗号方式を記述した後に標準化の候補となる主要な暗号方式について主に 2022 年 9 月までの調査を基に解説した。特に近年の研究動向を反映し、多変数多項式署名方式 Rainbow、同種写像鍵共有方式 SIDH、ハッシュ関数に基づく署名方式 SPHINCS+ に関する攻撃とその影響範囲についてある程度速報的な形で取り上げた。なお、調査報告書では第 2 章の活用方法は割愛した。

## 3.2　暗号技術ガイドライン（高機能暗号）

ネットワークの高速化・広帯域化、コンピュータの高性能化、特に、クラウドサービスの充実、人工知能（AI：Artificial Intelligence）技術の進歩、さらには 2020 年に訪れたコロナ禍においては、すべての対応をオンライン化しなければならない状況が生じ、リモートワークや、リモート会議等のオンラインサービス、それらに伴う技術が著しく進歩してきた。

以前より、これらの社会の変化に伴った現状のサービスの改善や、将来のサービス変化を見越して、既存の暗号技術よりも効率的で高機能な方式の研究開発が進められている。従来技術より、低コスト、高機能の特徴をもつ「高機能暗号」は様々な用途での利用が期待されている。CRYPTREC では、高機能暗号技術が求められる製品やサービスにおいて、利用者が適切な暗号方式を選択でき、容易に調達できることを目指し、『CRYPTREC 暗号技術ガイドライン（高機能暗号）』[4] を作成し、公開した。

従来の守秘、認証、署名の機能だけではなく、様々な機能を持つ「高機能暗号」の研究開発が進み、学会等で提案されている。また、ISO/IEC 等において標準化が進められている高機能暗号技術もある。

様々な機能を有する高機能暗号技術は、今後の発展が予想される 5G 及び Beyond5G の社会における種々のサービスで利用できる可能性があり、Society5.0 における基盤となる CPS（Cyber Physical System）といった次世代のネットワークサービスを構築する上でも有効なセキュリティ技術の一つとなることが期待されている。

高機能暗号技術には、様々な機能を有する方式が存在する。それらを一つの指標で比較することは困難である。このため、国際的に「高機能暗号」に対して一般的に合意されている定義はない。そこで、新たに、「従来の暗号技術に対して、機能が追加・向上される等の優位性を主張する暗号技術及び従来の暗号技術では困難であった事象を解決できる等の新規機能を有することを主張する暗号技術」と高機能暗号を定義し、CRYPTREC 暗号リスト [5] に挙げられているような暗号技術に対して、何らかの機能・性能で優位性（高機能性）を持つ暗号技術を主な対象として、ガイドラインを作成した。

高機能暗号は、その使用目的にあった選択が必要となる。そこで、本ガイドラインでは、高機能暗号の目的に応じて、“守秘”、“認証・署名”、“その他” の 3 つに分類した。

守秘は、第三者に秘匿する文書等を暗号化するための技術である。認証･署名は、文書等を作成する人、文書等を送る人及び通信している機器の認証を行う、若しくはそれらに署名を付与するための技術である。その他については、守秘、認証・署名には属さない新たな技術である。

以下に、本ガイドラインに記載した暗号方式の一覧を示す。

| 分類 | 高機能暗号名 | 特徴 |
|---|---|---|
| 守秘 | ID ベース暗号 | ID を公開鍵にすることが可能 |
| | 属性ベース暗号 | 受信者の属性に応じたアクセス制御が可能 |
| | 放送型暗号 | 1 対多である放送用のコンテンツの効率的なアクセス制御が可能 |
| | 準同型暗号 | 暗号化した状態での演算が可能 |
| | プロキシ再暗号化 | サーバにおいて暗号化鍵を変更することが可能 |
| 認証・署名 | 属性ベース署名 | 個人ではなく、属性に応じた署名が可能 |
| | 集約 MAC、マルチ MAC、集約署名、マルチ署名 | 複数の MAC／署名をまとめることが可能 |
| | グループ署名、リング署名 | グループを構成するメンバの誰かが匿名で署名をすることが可能 |
| | しきい値署名 | しきい値となるある人数以上の署名者がそろうことで、署名が完成する方式 |
| その他 | 秘密分散 | 一つの秘密データを複数に分割し秘匿する方法 |
| | マルチパーティ計算 | 複数のサーバによる秘密計算 |
| | ゼロ知識証明 | 秘密情報を秘匿しつつ、秘密情報を持っていることの証明が可能 |
| | Oblivious Random Access Machine | RAM をシャッフルすることで、RAM へのアクセスからの情報漏洩を防止可能。DB へのアクセスパターンの秘匿が可能 |
| | Private Information Retrieval | 個人が検索するデータを秘匿しつつ、利用者に必要な情報を取得するプロトコル |
| | 検索可能暗号 | DB から必要となるデータを暗号化した状態で検索が可能 |

ガイドラインでは、ここに示した暗号方式の解説、具体アルゴリズム、標準化動向、活用事例を調査し、記載した。ガイドラインの構成は、第 1 章に本ガイドラインの総説を記載し、第 2 章においては高機能暗号一覧に記した高機能暗号の活用事例と標準化動向、第 3 章では一覧に記した高機能暗号の技術的詳細・代表的な方式を記載し、第 4 章でまとめとしている。

## 3.3　暗号技術ガイドライン（軽量暗号）

限られた実装環境でも安全で高性能な暗号技術を搭載したいというニーズは古くからあり、このニーズに応えて小型で高速な暗号技術の開発が進められてきた。昨今では、IoT（Internet of Things）や CPS のような情報通信技術の発展が著しく、センサーやアクチュエータ等の計算リソースの限られたデバイスがネットワークに接続されるようになり、これに伴って、セキュリティやプライバシー上の脅威が高まってきたことから、暗号技術に対してより多様な実装要件が求められるようになった。

計算リソースの限られたデバイスにも実装可能な軽量暗号の研究開発が進展している。欧州では 2004 年から European Commission の第 6–7 次 Framework Programme の研究プロジェクトである ECRYPT I と ECRYPT II のテーマとして取り上げられた。また、軽量暗号の標準化も進展している。ISO/IEC では、軽量暗号アルゴリズムを技術分野ごとに定めた ISO/IEC 29192 や RFID 向けの暗号技術を定めた ISO/IEC 29167 を策定している。米国 NIST（National Institute of Standards and Technology）では、2015 年から軽量暗号の標準化プロジェクトを開始し、2023 年 2 月に最終選考方式として Ascon を選出した。

このような背景の下、CRYPTREC では、軽量暗号技術が求められる製品やサービスにおいて、利用者が最適な暗号方式を選択でき、容易に調達できることを目指し、2013 年度から 2016 年度にかけて、暗号技術評価委員会の下に軽量暗号ワーキンググループ（WG）を設置した。2016 年度に作成した『CRYPTREC 暗号技術ガイドライン（軽量暗号）』（以下、2016 年度版ガイドラインという）[5] は、軽量暗号の方式を選択・利用する際の技術的判断に資すること、今後の利用促進を図ることを目的として、軽量暗号 WG が作成したものである。

一般的に合意されている軽量暗号の定義はない。これまで提案されてきた軽量暗号技術には、ハードウェア実装の回路規模・消費電力量・レイテンシの観点で軽量性を追求したもの、組み込みソフトウェア実装で必要なメモリサイズの軽量性を追求したもの、などの様々な性能指標で最適化された方式が存在する。また、性能と安全性のトレードオフも相まって、実際の性能は多岐に渡る。そこで、本ガイドラインでは「実装性

能と安全性のトレードオフを勘案した上で、従来の暗号技術に対して特定の性能指標で優位性（軽量性）を持つように設計された暗号技術」をスコープとし、用途が想定される代表的な性能指標に対して優位性を主張する暗号技術を主な対象とした。また、公開鍵暗号系において、軽量暗号として広くコンセンサスが取れている方式がほとんどないことから、本ガイドラインでは共通鍵暗号系を対象としている。

その後、軽量暗号に関する研究開発の最新動向や米国 NIST 等の標準化動向を踏まえ、2021 年度から 2023 年度にかけて軽量暗号の安全性、実装性能、標準化動向に関する技術動向調査・評価を国内有識者に依頼し、これらの調査結果・評価結果を外部評価報告書として CRYPTREC の Web サイトで公開した。これらの外部評価報告書に基づき、暗号技術評価委員会が中心となって 2016 年度版ガイドラインを改定し、『CRYPTREC 暗号技術ガイドライン（軽量暗号）2023 年度版』（以下、2023 年度版ガイドラインという）[6] として公開した。

2023 年度版ガイドラインの構成は、次のとおりである。第 1 章では、本ガイドラインの総説を記載している。第 2 章では、軽量暗号の概要、軽量暗号の標準化動向、軽量暗号の活用例、そして軽量暗号の使用時における手引き（特に、軽量暗号の特徴、代表的な方式、パラメータの選定方法、ユースケース、使用時の留意点など）を示している。第 3 章では、代表的な軽量暗号（12 種類のブロック暗号と 10 種類の認証暗号）の実装性能を示している。加えて、米国 NIST の標準化プロジェクトにおいて最終選考方式に選出された Ascon の実装性能、特にサイドチャネル攻撃等への対策を施さない場合と対策を施した場合におけるソフトウェア実装性能とハードウェア実装性能、そしてサイドチャネル攻撃耐性の評価結果について示している。第 4 章では、代表的な軽量暗号技術の基本情報をブロック暗号、ストリーム暗号、ハッシュ関数、メッセージ認証コード、認証暗号の技術分野別に示している。

## 4　CRYPTREC 暗号リストの改定

2019 年度から暗号技術検討会の下に「量子コンピュータ時代に向けた暗号の在り方検討タスクフォース」（以下「検討 TF」という。）が設置され、大規模な量子コンピュータの動向を踏まえた次期 CRYPTREC 暗号リストに求められる要件等を検討することになった（図 3）。

検討 TF における検討の結果、次期 CRYPTREC 暗号リストの構成に関しては、「電子政府推奨暗号リス

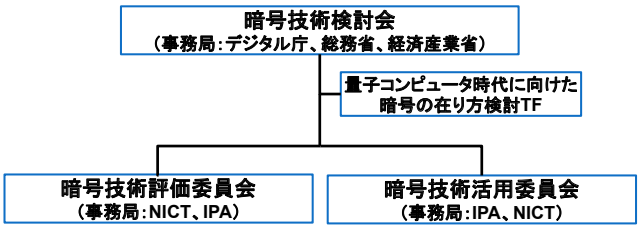


図 3　CRYPTREC 体制図（2019 年度～ 2021 年度まで）

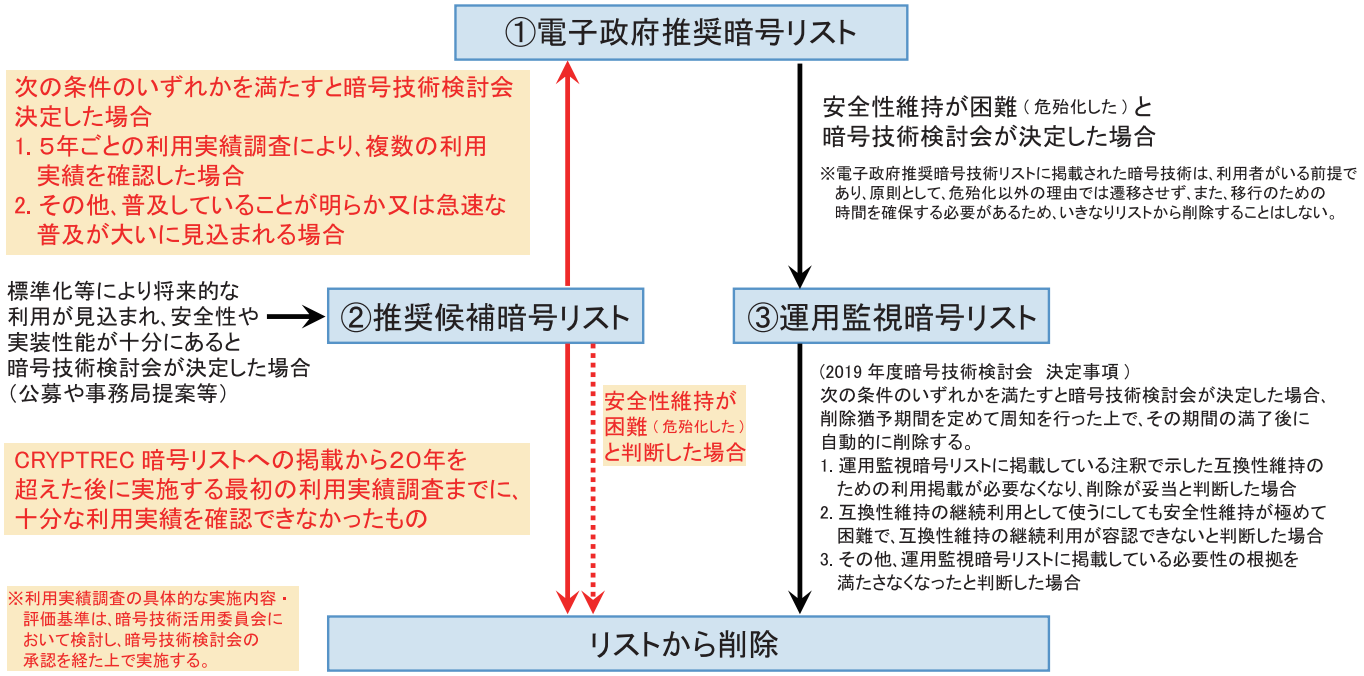


図 4　CRYPTREC 暗号リストの 3 リスト構成とその移行ルール

ト」、「推奨候補暗号リスト」及び「運用監視暗号リスト」の3リスト構成からは変更しないこと、各暗号技術は十分成熟しているため、各々の技術分類は変更しないこと、新たな暗号技術の公募も実施しないこととした。また、推奨候補暗号リストに対して新たに移行ルールを設け、CRYPTREC 暗号リストへの掲載から 20 年を超えた後に実施する最初の利用実績調査までに十分な利用実績を確認できなかったものは CRYPTREC 暗号リストから削除することとなった。耐量子計算機暗号、軽量暗号、高機能暗号については、次期 CRYPTREC 暗号リストには含めず、それぞれ暗号技術ガイドラインとしてまとめることとなった。(図 4)。

また、これまでの CRYPTREC 暗号リストでは推奨する暗号技術を示してきたが、そこで使う暗号技術の推奨パラメータを明示的に提示してこなかった。推奨パラメータの明示は安全なシステム構築や計画的な暗号技術の移行を促進するために有用であるため、推奨パラメータを規定する別の文書を新たに作成し、CRYPTREC 暗号リストから当該文書 [13] を参照する構成とすることとなった。

2022 年度の CRYPTREC 暗号リスト改定前の、2016 年度から 2021 年度までに、CRYPTREC 暗号リストの小改定が行われ、いくつかの暗号技術が推奨候補暗号リストに追加されてきた。暗号技術評価委員会では、2016 年度にハッシュ関数 SHAKE128 を、2017 年度に認証暗号 ChaCha20-Poly1305 を、2019 年度に暗号利用モード (秘匿モード) XTS を、2021 年度に公開鍵暗号 (署名) EdDSA を、安全性評価及び実装性能評価を実施して十分な安全性及び実装性能を有していると判断したことから、これらの暗号技術を CRYPTREC 暗号リストの推奨候補暗号リストに追加する提案を暗号技術検討会に対して対応する各年度で行った。また、2017 年度に、電子政府推奨暗号リスト掲載の 64 ビットブロック暗号 3-key Triple DES に付与されている注釈の変更及び 3-key Triple DES を「電子政府推奨暗号リスト」から「運用監視暗号リスト」へ変更することを暗号技術検討会に提案した。

2022 年度に公開鍵暗号 (署名) ECDSA、公開鍵暗号 (鍵共有) ECDH 及び共通鍵暗号 (128 ビットブロック暗号) SC2000 の応募暗号について取下げの申請があったため、ECDSA 及び ECDH については応募暗号技術から CRYPTREC 事務局が選出した暗号技術に変更して現状通り電子政府推奨暗号リストに記載し、SC2000 については取下げの申請を認め推奨候補暗号リストから削除した。それに加えて、2022 年度に暗号技術活用委員会において、独立行政法人情報処理推進機構にて実施された暗号アルゴリズム利用実績調査の結果及び 2021 年度に承認された利用実績に基づく選定基準に基づき、2021 年度までに推奨候補暗号リストに掲載された暗号アルゴリズムのうち、認証暗号 ChaCha20-Poly1305、暗号利用モード (秘匿モード) XTS、エンティティ認証 ISO/IEC 9798-4、ハッシュ関数 SHA-512/256、SHA3-256、SHA3-384、SHA3-512、SHAKE128、SHAKE256、公開鍵暗号 (署名) EdDSA が電子政府推奨暗号リストへの追加候補として暗号技術検討会に提案された。2023 年 3 月に、『「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)」(案) に対する意見の募集』(デジタル庁、総務省、経済産業省)、いわゆるパブリックコメントが行われ、その後、暗号技術検討会にて CRYPTREC 暗号リストの改定案が審議され了承された。

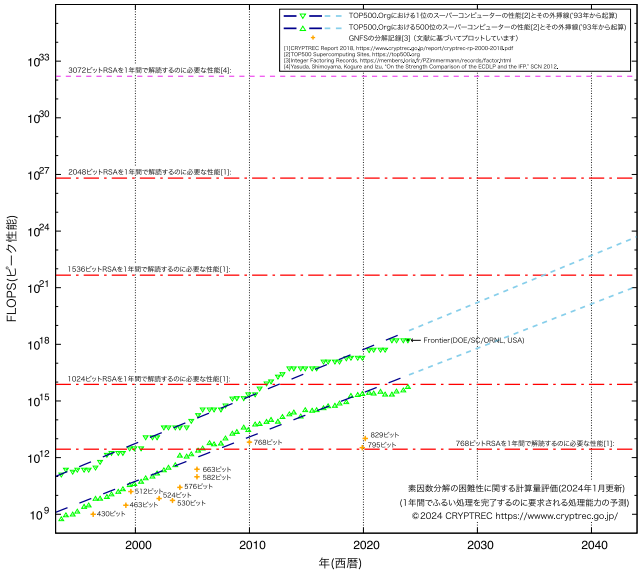


図 5　素因数分解の困難性に関する計算量評価 ([1] からの引用 )

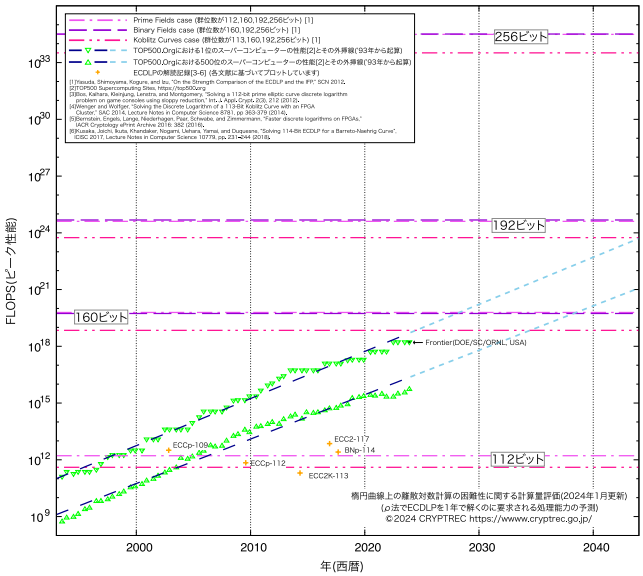


図 6　楕円曲線上の離散対数計算の困難性に関する計算量評価 ([1] からの引用)

## 5 むすび

本稿では、2016 年度から 2023 年度までの間にセキュリティ基盤研究室が事務局を担当した CRYPTREC 活動について紹介した。特に、2022 年度、2023 年度に作成、改定された 3 つのガイドラインと、電子政府推奨暗号リストの改定について紹介した。この活動以外にも、電子政府推奨暗号リストに関連する暗号の解析研究などを監視している。さらに、暗号の安全性に直結する「素因数分解の困難性に関する計算量評価」や「楕円曲線上の離散対数計算の困難性に関する計算量評価」を示す予測図（図 5、6）を毎年作成している。今後も暗号・セキュリティ技術に対して様々な解析・攻撃手法が出現すると予想されるが、それらに対して正しい対処法を提案することで、安心・安全な社会となるように活動する。

## 謝辞

この場を借りて、今まで CRYPTREC 活動に参加し、暗号アルゴリズムの安全性評価や実装性能評価の検討にご協力いただいた全ての方々に感謝する。

### 【参考文献】


1 CRYPTREC 暗号技術評価委員会, “CRYPTREC Report 暗号技術評価委員会報告,” https://www.cryptrec.go.jp/eval_cmte.html
2 CRYPTREC 暗号技術検討会, “暗号技術検討会報告書,” https://www.cryptrec.go.jp/adv_board.html
3 CRYPTREC 暗号技術調査ワーキンググループ (耐量子計算機暗号), “CRYPTREC 暗号技術ガイドライン (耐量子計算機暗号),” https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf
4 CRYPTREC 暗号技術調査ワーキンググループ (高機能暗号), “CRYPTREC 暗号技術ガイドライン (高機能暗号),” https://www.cryptrec.go.jp/report/cryptrec-gl-2005-2022.pdf
5 CRYPTREC 暗号技術ワーキンググループ, “CRYPTREC 暗号技術ガイドライン (軽量暗号),” https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf
6 CRYPTREC 暗号技術評価委員会, “CRYPTREC 暗号技術ガイドライン (軽量暗号) 2023 年度版,” https://www.cryptrec.go.jp/report/cryptrec-gl-2006-2023.pdf
7 デジタル庁, 総務省, 経済産業省, “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) ― CRYPTREC LS-0001-2022,” https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf
8 総務省, 経済産業省, “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) ― CRYPTREC LS-0001-2012,” https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012.pdf
9 デジタル庁, 総務省, 経済産業省, “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) ― CRYPTREC LS-0001-2012 R8,” https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r8.pdf
10 CRYPTREC 暗号技術調査ワーキンググループ (暗号解析評価), “耐量子計算機暗号の研究動向調査報告書,” https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2018.pdf
11 CRYPTREC 暗号技術評価委員会, “現在の量子コンピュータによる暗号技術の安全性への影響,” https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html
12 CRYPTREC 暗号技術調査ワーキンググループ (耐量子計算機暗号), “耐量子計算機暗号の研究動向調査報告書,” https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2022.pdf
13 デジタル庁, 総務省, 経済産業省, “暗号強度要件 (アルゴリズム及び鍵長選択) に関する設定基準,” https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf



**青野 良範**（あおの よしのり）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士 (理学)
公開鍵暗号の安全性評価
【受賞歴】
2023 年　IEEE Signal Processing Society Best Paper Award
2021 年　科学技術分野の文部科学大臣表彰 若手科学者賞
2017 年　情報処理学会コンピュータセキュリティ研究会 (CSEC) 優秀研究賞



**伊藤 竜馬**（いとう りょうま）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士 (工学)
共通鍵暗号の解析・設計、実際のシステムに対する安全性評価
【受賞歴】
2023 年　Journal of Information Processing, Specially Selected Paper certificate, IPSJ
2023 年　情報処理学会 2022 年度山下記念研究賞
2022 年　電子情報通信学会 SCIS 2021 イノベーション論文賞



**大久保 美也子**（おおくぼ みやこ）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士 (工学)
暗号理論、暗号プロトコル
【受賞歴】
2018 年　電子情報通信学会 SCIS 2018 イノベーション論文賞
2015 年　市村清新技術財団市村学術賞　功績賞
2000 年　電子情報通信学会 SCIS 2000 論文賞



**小川 一人**（おがわ かずと）
サイバーセキュリティ研究所
セキュリティ基盤研究室
上席研究員
博士 (情報理工学)
高機能暗号

**金森 祥子**（かなもり さちこ）

サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究技術員
プライバシー、ユーザブルセキュリティ
【受賞歴】
2024 年　2024 年度山下記念研究賞
2023 年　CSS2023 優秀論文賞（兼・UWS 優秀論文賞）

**黒川 貴司**（くろかわ たかし）

サイバーセキュリティ研究所
セキュリティ基盤研究室
研究技術員
博士（工学）
暗号技術の安全性評価

**吉田 真紀**（よしだ まき）

サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
暗号理論、情報理論、NewSpace セキュリティ
【受賞歴】
2022 年　情報処理学会 IPSJ-ONE2022
2011 年　電子情報通信学会第 67 回（平成 22 年度）論文賞
2009 年　情報理論とその応用学会 2008 年 SITA 奨励賞

**篠原 直行**（しのはら なおゆき）

サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
博士（数理学）
暗号に関する数理学
【受賞歴】
2019 年　The 14th International Workshop on Security（IWSEC 2019）Best Paper Award
2013 年　第 12 回（2013 年）ドコモ・モバイル・サイエンス賞先端技術部門優秀賞
2008 年　日本数式処理学会第 17 回大会 2008 年度奨励賞