CRYPTREC シンポジウム 2024

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会 活動報告
(2023年度～2024年度)

2024年 9月2日

暗号技術評価委員会　委員長
高木 剛(東京大学、教授)

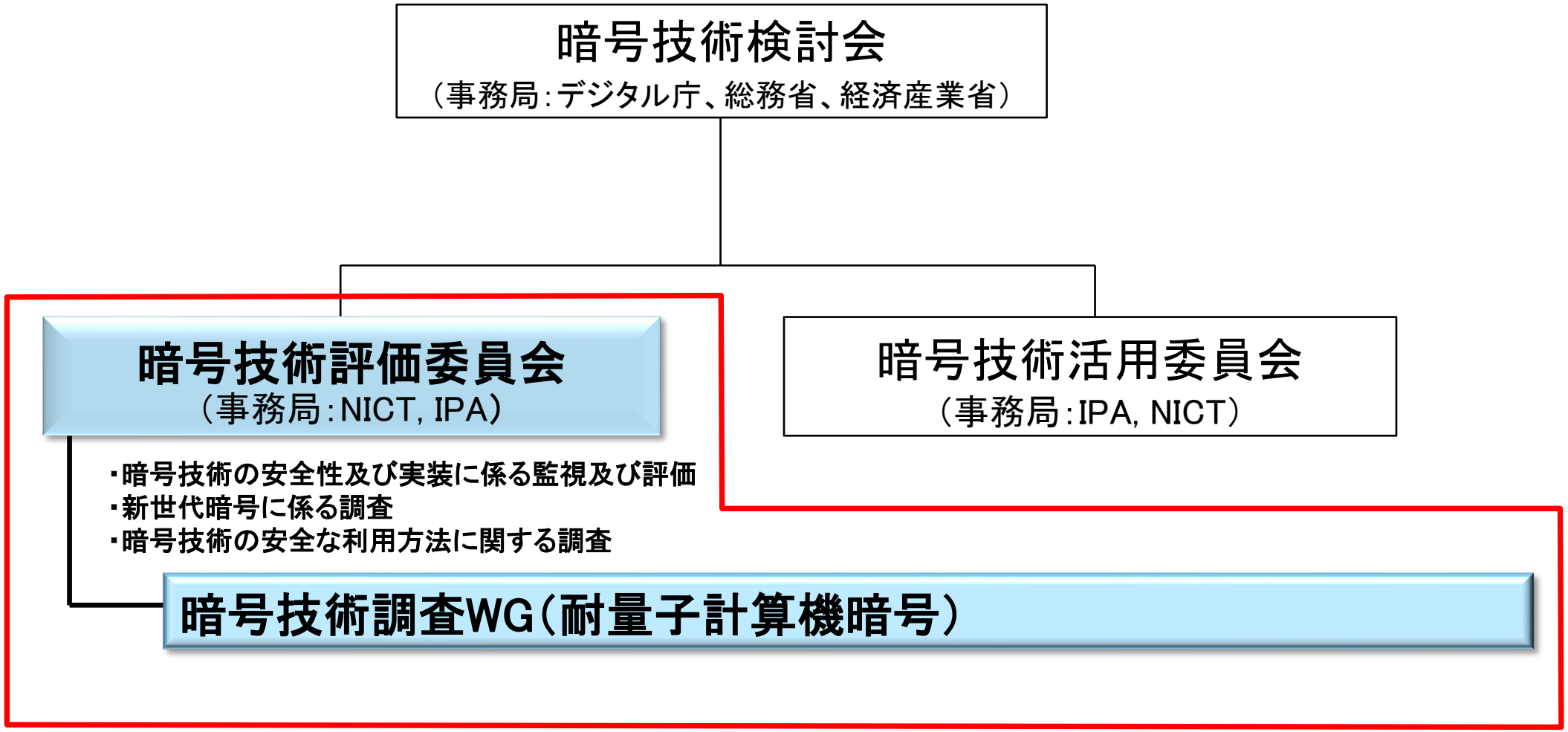
暗号技術調査WG(耐量子計算機暗号)　主査
國廣 昇(筑波大学、教授)

目次

1. 暗号技術評価委員会報告
2. 暗号技術ガイドライン（軽量暗号）2023年度版
3. 暗号技術調査ワーキンググループ（耐量子計算機暗号）報告
4. まとめ

1. 暗号技術評価委員会報告

2023-2024年度　CRYPTREC体制（暗号技術評価委員会）



2023-2024年度 暗号技術評価委員会 委員

委員長　高木　剛	
委員　青木　和麻呂	委員　花岡　悟一郎
委員　岩田　哲	委員　藤崎　英一郎
委員　上原　哲太郎	委員　本間　尚文
委員　大東　俊博	委員　松本　勉
委員　國廣　昇	委員　松本　泰
委員　四方　順司	委員　山村　明弘
委員　手塚　悟	

暗号技術評価委員会の活動目的

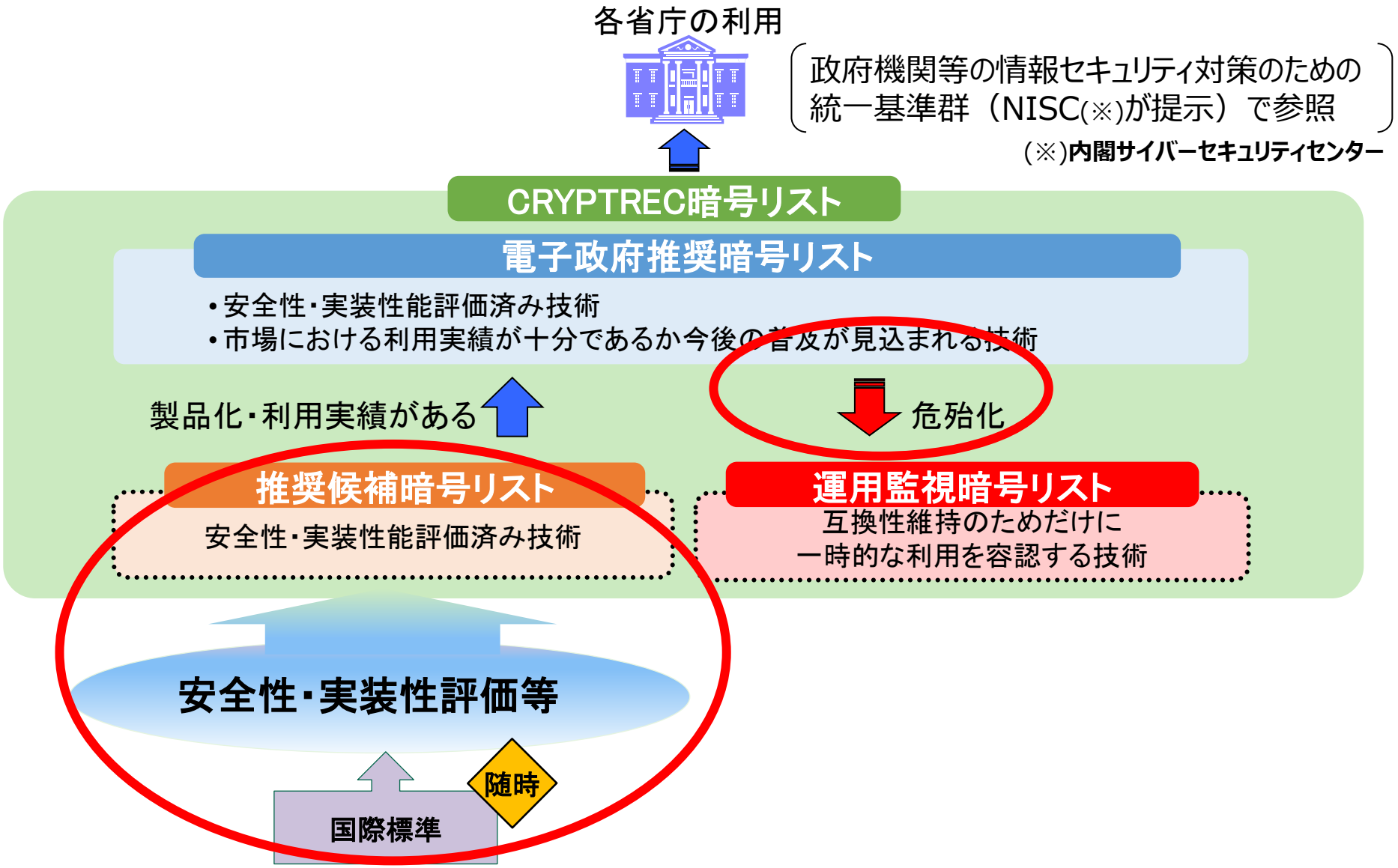
■ 活動目的

CRYPTREC暗号リストに掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保のために安全性及び実装に係る監視及び評価を行う

■ 活動概要

- 暗号技術の安全性及び実装に係る監視及び評価
  - ① CRYPTREC 暗号等の監視
  - ② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視リストへの降格、運用監視暗号リストからの危殆化が進んだ暗号の削除に係る検討
  - ③ 推奨候補暗号リストへの新規暗号(事務局選出)の追加に係る検討
  - ④ CRYPTREC 注意喚起レポートの発行
  - ⑤ 新技術などに関する調査及び評価
- 暗号技術の安全な利用方法に関する調査

CRYPTREC暗号リストの構成



CRYPTREC暗号等の監視

■CRYPTREC暗号リストに記載されている暗号技術に関する研究動向

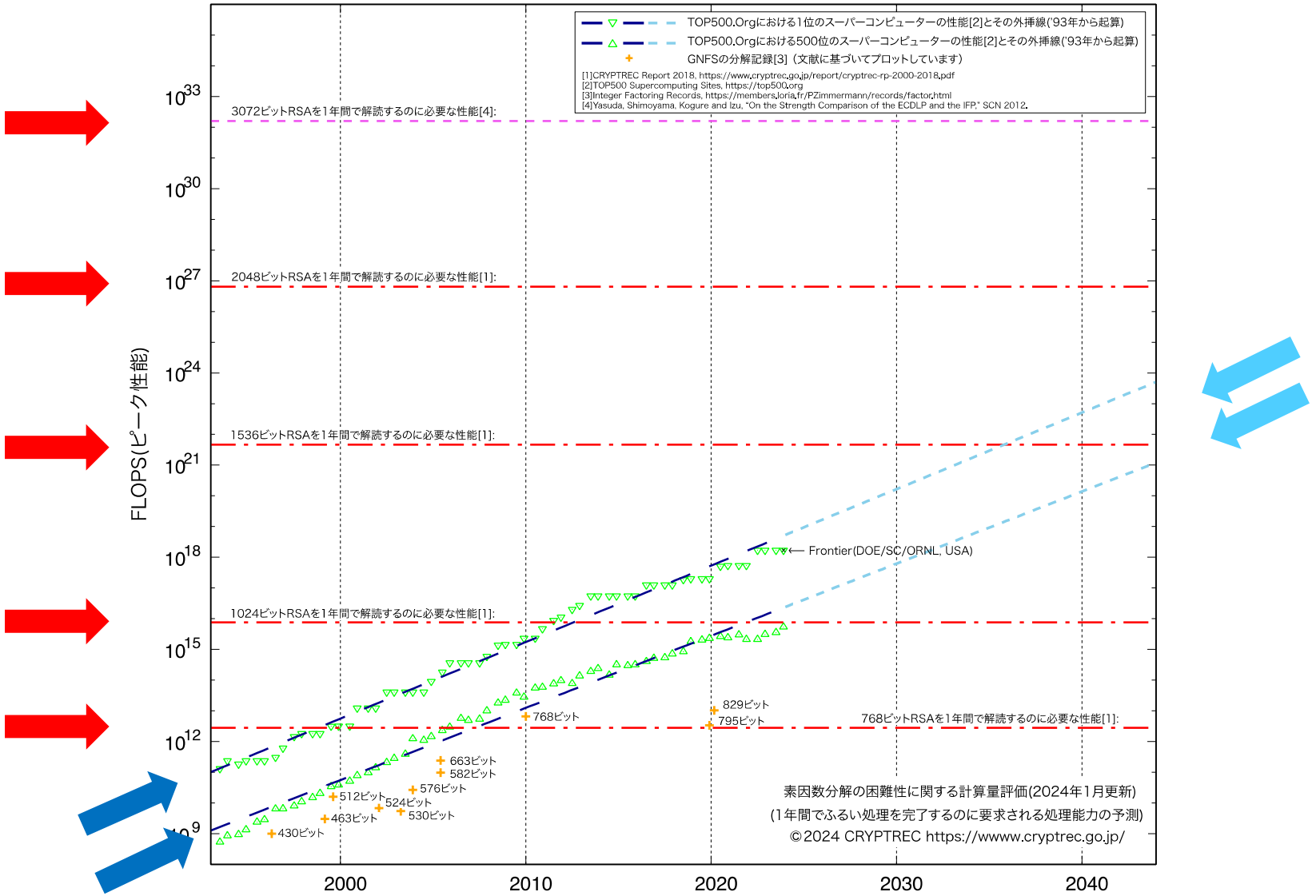
- 毎年発行している**CRYPTRECレポート（暗号技術評価委員会報告）**にて報告

■素因数分解の困難性、離散対数問題の困難性に基づく暗号の危殆化の時期を予測する図の今後の取り扱い

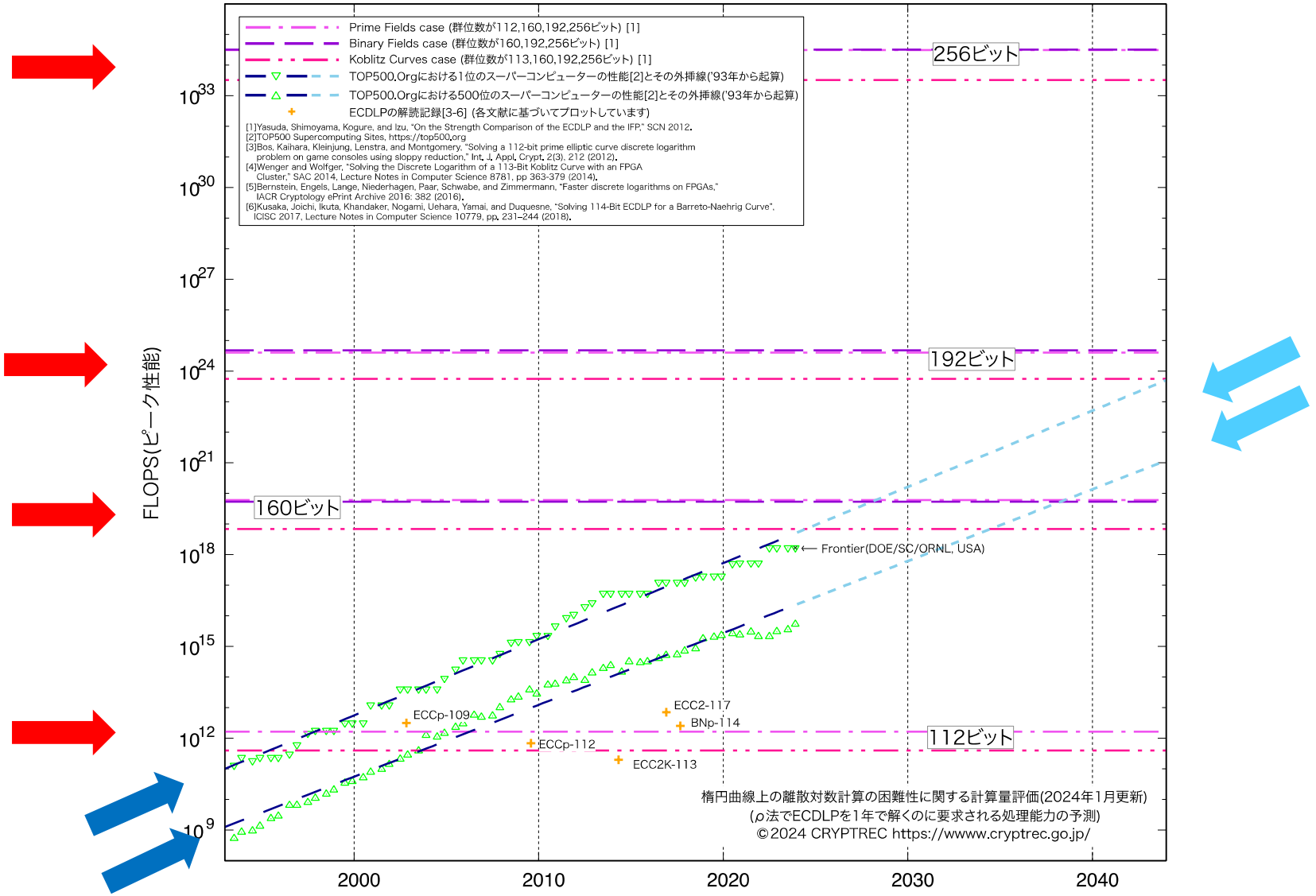
- 解読の脅威の尺度に用いているスーパーコンピュータの性能向上が鈍化傾向にあるものの、いわゆるムーアの法則を仮定して外挿線を年度末からプラス20年後まで直線で引き、評価に大きな変動がないと考えられる限りにおいては、安全サイドに倒した評価として当面の間更新していく
- 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、関係各所などを含めて検討する

  ⇒2021年度暗号技術活用委員会にて、暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準を策定（https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf）

①CRYPTREC暗号等の監視
－素因数分解の困難性に関する計算量評価（2023年度版）



①CRYPTREC暗号等の監視
－ 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（2023年度版）



2023-2024年度活動内容
新技術などに関する調査及び評価

CRYPTREC
Cryptography Research and Evaluation Committees

■耐量子計算機暗号に関する研究動向調査報告書・耐量子計算機暗号ガイドラインを策定

⇒　詳細は、暗号技術調査ワーキンググループ（耐量子計算機暗号）へ

■軽量暗号技術に関するガイドラインを策定

●「CRYPTREC 暗号技術ガイドライン（軽量暗号）」2016年度版を基に更新

➢NIST LWC ファイナリストなどの安全性に関わる動向調査を実施

2. 暗号技術ガイドライン（軽量暗号）2023年度版

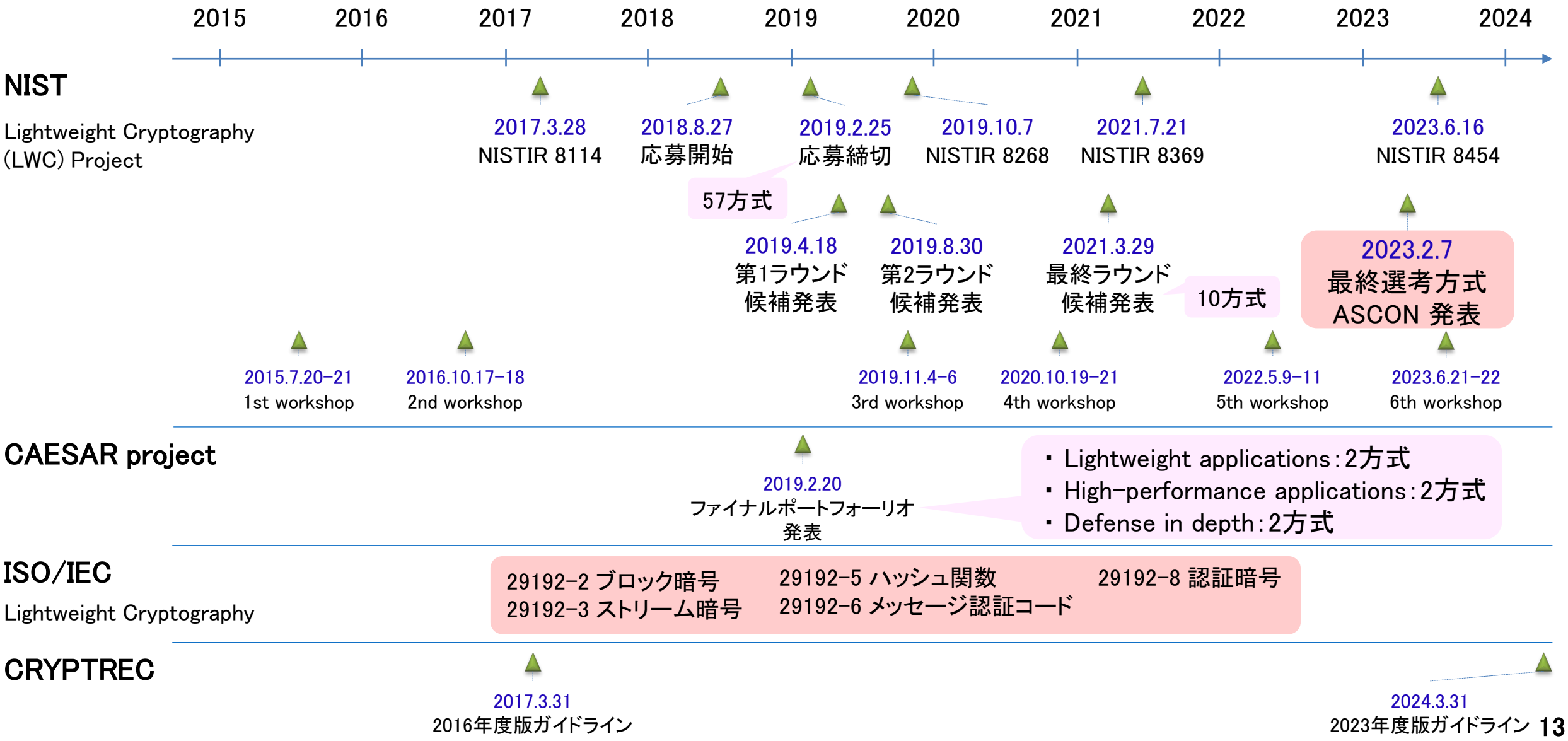
軽量暗号に関わる取り組み

■ CRYPTREC暗号技術ガイドライン(軽量暗号)†の発行

- 2013年度 ～ 2016年度　軽量暗号WGにて検討、2017年3月公開‡
- ガイドラインの目的
  - IoT等の次世代ネットワークサービスにおいて軽量暗号の活用が期待されることから、方式を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的として、暗号技術ガイドラインを作成
- 想定する読者
  - システム設計時に暗号技術の選択・利用の判断に関わるセキュリティや暗号の技術者
- 代表的な軽量暗号
  - 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

† 以降、「2016年度版ガイドライン」と呼ぶ
‡ https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf（文書番号：CRYPTREC GL-2003-2016JP）

軽量暗号に関わる技術動向



2016年度版ガイドラインの改定

■ CRYPTREC暗号技術ガイドライン（軽量暗号）2023年度版†の発行‡

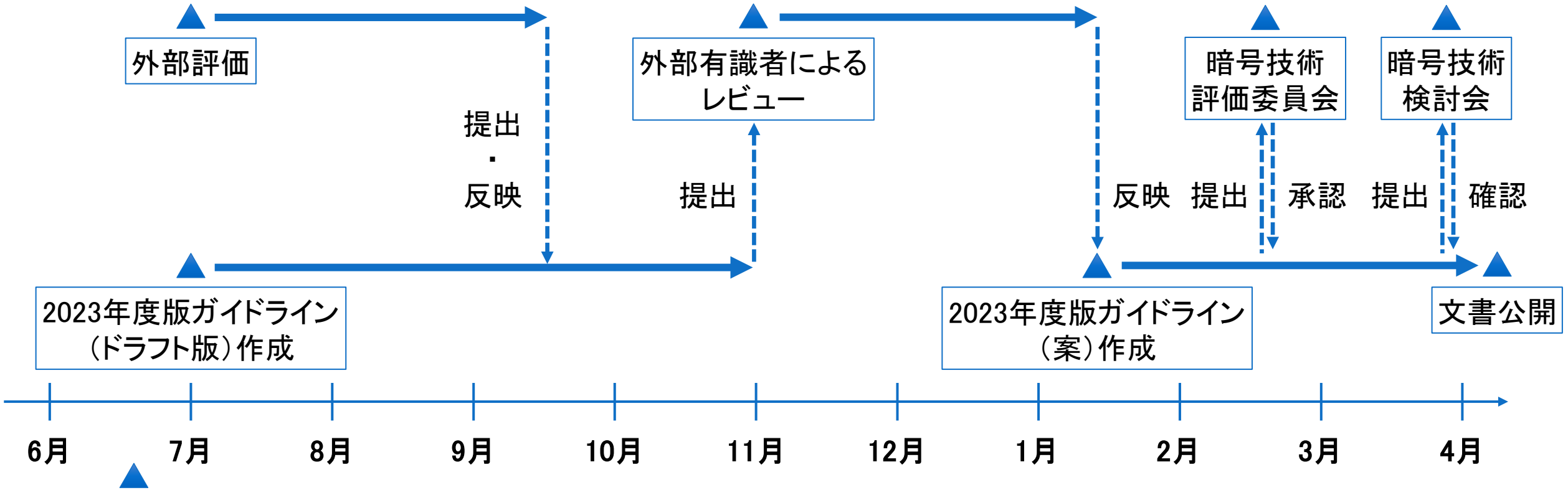
- 2021年度から2023年度にかけて実施した外部評価に基づき、2016年度版ガイドラインを更新および新規情報を追加した文書
  - 2021年度：2016年度版ガイドライン掲載の暗号方式に関する安全性評価の動向調査
  - 2022年度：NIST LWCファイナリスト等の安全性・実装性能・標準化動向に関する調査・評価
  - 2023年度：NIST LWC最終選考方式ASCONの実装性能・標準化動向に関する調査・評価

- 主な更新・追加内容（詳細は後述）
  - 更新：2016年度版ガイドライン掲載の暗号方式に関する安全性解析状況等
  - 追加：2017年度以降の軽量暗号に関する標準化動向
  - 追加：ASCONの実装性能
  - 追加：ASCONに対するサイドチャネル攻撃対策手法と物理攻撃手法に関する情報
  - 追加：NIST LWCファイナリスト等の代表的な軽量暗号に関する情報

† 以降、「2023年度版ガイドライン」と呼ぶ
‡ https://www.cryptrec.go.jp/report/cryptrec-gl-2006-2023.pdf（文書番号：CRYPTREC GL-2006-2023）

2023年度実施内容(1/3)

■2023年度スケジュール



- NISTIR 8454発行：6/16
- NIST LWC workshop 2023：6/21-22

2023年度実施内容(2/3)

■ 軽量暗号ASCONの実装性能に関する調査・評価を外部評価により実施

- 依頼先：崎山 一男 様（電気通信大学）
- 主な依頼内容
  - 物理攻撃†対策を施したASCONの実装性能
  - ASCONに対する物理攻撃耐性

■ 軽量暗号ASCONなどに関わる標準化動向調査を外部評価により実施

- 依頼先：菅野 哲 様（GMOサイバーセキュリティ byイエラエ株式会社）
- 主な依頼内容
  - NIST LWC projectにてASCONが選出されるに至った選定基準と選定プロセス
  - 他標準化団体における軽量暗号（特に、ASCON）の標準化動向

† サイドチャネル攻撃等を含めた物理的な攻撃という意味で「物理攻撃」という用語を使用する。

2023年度実施内容(3/3)

■ 外部有識者によるレビュー

- 依頼先：本間 尚文 様（東北大学）、峯松 一彦 様（日本電気株式会社）
- 主な依頼内容
  - 2023年度版ガイドライン（ドラフト版）における改定内容の妥当性等を評価
    - 本間様：主に第1章～第3章（はじめに、軽量暗号とその活用法、軽量暗号の性能比較）
    - 峯松様：主に第4章（代表的な軽量暗号）

■ 2023年度版ガイドラインの執筆・編集

- 担当：CRYPTREC事務局

2023年度版ガイドラインの目次

CRYPTREC Cryptography Research and Evaluation Committees

赤字：追加箇所、青字：更新箇所

第2章　軽量暗号とその活用方法

2.2　軽量暗号の標準化動向

2.2.1　CAESARコンペティション

2.2.2　NIST LWCプロジェクト

2.2.3　他標準化団体におけるASCONの検討状況

■ 2022年度・2023年度外部評価に基づく追加

- CAESARコンペティションの最終選考結果とその評価基準
- NIST LWCプロジェクトの評価基準と選定プロセス、ASCONに関する評価
- 5団体（IETF、W3C、ISO/IEC、ITU-T、Global Platform）におけるASCONの標準化動向

第3章　軽量暗号の実装性能

3.3　ASCONの実装性能

3.3.1　ハードウェア実装性能

3.3.2　ソフトウェア実装性能

3.3.3　物理攻撃耐性

■ 2022年度・2023年度外部評価に基づく追加

- ハードウェア実装：面積コスト、スループット、消費電力の観点で調査・評価
- ソフトウェア実装：レイテンシ、ROMサイズ、コードサイズの観点で調査・評価
- 物理攻撃耐性：
  - サイドチャネル攻撃対策が施された実装への評価：TI、DOM
  - 物理攻撃耐性：相関電力解析、故障利用攻撃、テンプレート攻撃、など
  - 付録A（ASCONの物理攻撃耐性）で各種評価手法を解説

第4章　代表的な軽量暗号

4.1　ブロック暗号
4.2　ストリーム暗号
4.3　ハッシュ関数
4.4　メッセージ認証コード
4.5　認証暗号

■ 2021年度・2022年度外部評価に基づく更新・追加

- 更新：2016年度版ガイドライン掲載の暗号方式に関する安全性解析状況等
- 追加：ISOで規格化された（または規格化予定の）暗号方式に関する情報
- 追加：CAESARコンペティションの最終選考方式AEGISとCOLMに関する情報（付録B）
- 追加：NIST LWCファイナリスト（ASCONを除く）に関する情報を追加（付録C）

3. 暗号技術調査WG（耐量子計算機暗号）報告

2023-2024年度耐量子計算機暗号WG委員

主査　國廣　昇	
委員　青木　和麻呂	委員　成定　真太郎
委員　伊藤　忠彦	委員　廣瀬　勝一
委員　下山　武司	委員　安田　貴徳
委員　高木　剛	委員　安田　雅哉
委員　高島　克幸	

耐量子計算機暗号WGの活動目的

■ 背景

- 量子コンピュータでも攻撃が困難であると期待される暗号（耐量子計算機暗号:PQC）の技術開発、標準化活動などが世界的に活発に進められている
- 長期間かかると想定されるPQCへの移行スケジュールを策定し準備を行うため、国内外の技術動向を調査・把握する必要がある
- 2022年度には耐量子計算機暗号の調査報告書・ガイドラインを公表し、利用指針を示した （https://www.cryptrec.go.jp/tech_reports.html）

■ WGの活動目的

- 2024年9月末までの耐量子計算機暗号に関する情報を可能な限り網羅的に調査
- 2024年度までに新たな耐量子計算機暗号の調査報告書・ガイドラインを作成

耐量子計算機暗号WGの活動概要

■ 技術動向調査の範囲

- ●耐量子計算機暗号に関する開発・標準化の動向を可能な限り網羅的に調査
  - ➢国際会議CRYPTO、Eurocrypt、Asiacrypt、PQCrypto
  - ➢2024年9月末までに発表された文献を調査

- ●その他大きな話題があれば取り上げる
  - ➢NIST PQC FIPS化/Round 4/Additional Digital Signatureの進展状況
    - ✓2024年8月 FIPS203～205公表(ML-KEM、ML-DSA、SLH-DSA)
  - ➢Regevの量子素因数分解アルゴリズム
    - ✓2023年8月 arXiv:2308.06572 Shorのアルゴリズムよりも少ないゲート数での素因数分解を主張。後続研究として改良や離散対数問題への応用が検討される
  - ➢ChenによるLWE問題の量子アルゴリズム
    - ✓2024年4月 ePrint 2024/555 新たなアイディアによる量子攻撃の提案。その後コアの部分に間違いが発見された

2024年度版調査報告書・ガイドラインの方針

■ 色付きは2022年度と比較して大きな差分のある箇所

■ １章（はじめに）
- 2022年度版から内容を拡充し、ガイドラインはその抜粋とする
- 量子コンピュータ開発と暗号解読の現状
- 研究、標準化の動向の概要
- 調査対象としたPQCの種類、執筆者リスト

■ ２章（PQCの活用方法）
- 調査報告書・ガイドラインの両方に掲載
  - ➢ 調査報告書の内容を拡充し、ガイドラインはその抜粋とする
- 公開鍵暗号の用途（署名、守秘、鍵共有）ごとの利用形態
- PQCの導入により期待される効果と課題、移行、Cryptographic agilityに関する話題を拡充

2024年度版調査報告書・ガイドラインの方針

■ 色付きは2022年度と比較して大きな差分のある箇所

■ 3章～7章（暗号方式の解説）

- 格子に基づく暗号、符号に基づく暗号、多変数多項式に基づく暗号、同種写像に基づく暗号、ハッシュ関数に基づく署名を各章で取り上げる
- 2022年度版から新たな章は作らない
  - MPC-in-the-headを新たな章とはしない
  - 主要な暗号方式として取り上げるべきものがある場合には、根拠となる計算問題に従い各章の執筆担当者が記載する

2024年度版調査報告書・ガイドラインの方針

■ 色付きは2022年度と比較して大きな差分のある箇所

■ 3章～7章の各章ごとに含まれる内容

- 安全性の根拠となる計算問題と代表的な解法、最新の攻撃状況
- 主要な暗号方式およびそれらの基礎（構成のひな形）となる代表的な方式の紹介
  - アルゴリズムの擬似コード/パラメータ（暗号文長、署名長、鍵長等）
- ガイドラインには抜粋として、主要な暗号方式のみを記載

■ 主要な暗号方式選定の基準

- 世界的に使用が見込まれる耐量子計算機暗号を記載する
  - NIST PQC 標準化への提案方式等
- 特にFIPS標準化方式に関して、調査報告書にはFIPSバージョンと開発者らの最新仕様書との差分を解説、ガイドラインには抜粋としてFIPSバージョンのみを掲載する

■2024/8/13　3件のNIST FIPS203～205が公開

Cryptography	Underlying Security Problems	Algorithm	FIPS
Public-key Encryption and Key-establishment Algorithms	Lattice-based	CRYSTALS-KYBER	FIPS203 (ML-KEM)
Digital Signature Algorithms	Lattice-based	CRYSTALS-DILITHIUM FALCON	FIPS204 (ML-DSA) FIPS206 (FN-DSA)予定
	Hash-based	SPHINCS+	FIPS205 (SLH-DSA)

https://csrc.nist.gov/pubs/fips/203/final
https://csrc.nist.gov/pubs/fips/204/final
https://csrc.nist.gov/pubs/fips/205/final

4. おわりに

おわりに

委員会活動・ガイドラインの公開

■ CRYPTREC Report：暗号技術評価委員会の活動報告

https://www.cryptrec.go.jp/eval_cmte.html

検索：　CRYPTREC　評価委員会

■ 暗号技術ガイドライン（軽量暗号）、暗号技術ガイドライン（耐量子計算機暗号）

https://www.cryptrec.go.jp/tech_guidelines.html

検索：　CRYPTREC　ガイドライン

おわりに

今後も暗号技術評価委員会では、

- 暗号技術の安全性及び実装に係る監視及び評価
- 新世代暗号に係る調査
- 暗号技術の安全な利用方法に関する調査

など、健全なサイバー空間の実現・維持につなげるべく、暗号技術の安全性という観点から必要とされる活動を展開していきたい。

https://www.cryptrec.go.jp/