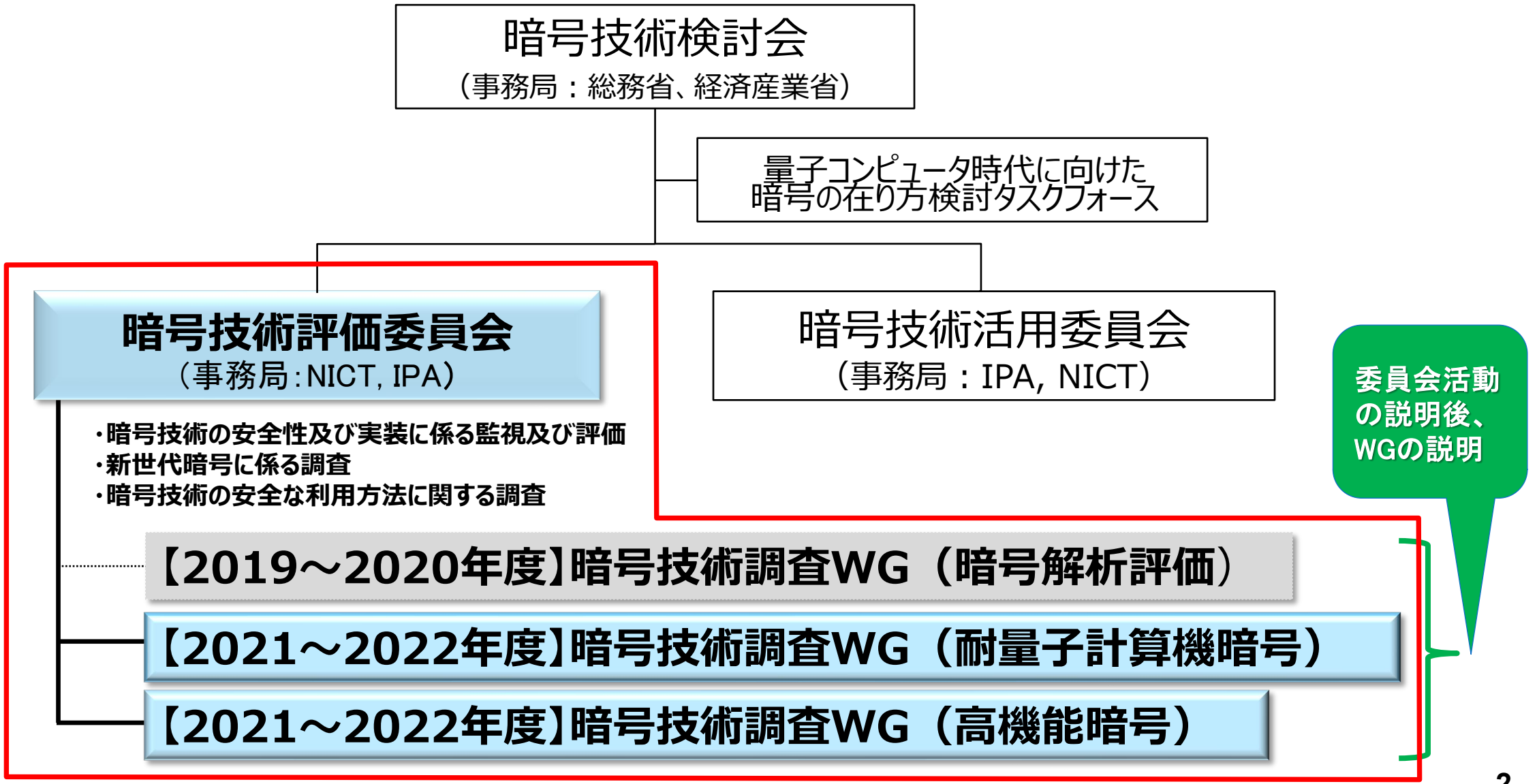
CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会　活動報告
（2019年度～2022年度）

2022年　7月　5日

暗号技術評価委員会　委員長
（東京大学　教授）
高木 剛

2019～2022年度 CRYPTREC体制



暗号技術評価委員会の活動目的

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

- 暗号技術の安全性及び実装に係る監視及び評価
  - **CRYPTREC 暗号等の監視**
  - 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
  - **CRYPTREC 注意喚起レポートの発行**
  - **仕様書の参照先の変更**
  - **推奨候補暗号リストへの新規暗号(事務局選出)の追加**
  - **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

（技術ガイドラインの整備・学術的な安全性の調査・公表など）

  - 暗号技術を利用する際の技術面での注意点に関する調査、新技術の安全性・性能に関する調査・評価

2019～2022年度 暗号技術評価委員会 委員

2019～2020年度 暗号技術評価委員会 委員		
委員長	高木　剛	東京大学　教授
委員	岩田　哲	名古屋大学　准教授
委員	上原　哲太郎	立命館大学　教授
委員	大東　俊博	東海大学　准教授
委員	國廣　昇	筑波大学　教授
委員	四方　順司	横浜国立大学　教授
委員	手塚　悟	慶應義塾大学　教授
委員	藤﨑　英一郎	北陸先端科学技術大学院大学 教授
委員	本間　尚文	東北大学　教授
委員	松本　勉	横浜国立大学　教授
委員	松本　泰	セコム株式会社　マネージャー
委員	盛合　志帆	国立研究開発法人情報通信研究機構 上席研究員
委員	山村　明弘	秋田大学　教授
委員	渡邊　創	国立研究開発法人産業技術総合研究所 副研究センター長

(注)2021年3月末時点

2021～2022年度 暗号技術評価委員会 委員		
委員長	高木　剛	東京大学　教授
委員	青木　和麻呂	文教大学　准教授
委員	岩田　哲	名古屋大学　准教授
委員	上原　哲太郎	立命館大学　教授
委員	大東　俊博	東海大学　准教授
委員	國廣　昇	筑波大学　教授
委員	四方　順司	横浜国立大学　教授
委員	手塚　悟	慶應義塾大学　教授
委員	花岡　悟一郎	国立研究開発法人産業技術総合研究所　首席研究員
委員	藤﨑　英一郎	北陸先端科学技術大学院大学 教授
委員	本間　尚文	東北大学　教授
委員	松本　勉	横浜国立大学　教授
委員	松本　泰	セコム株式会社　マネージャー
委員	山村　明弘	秋田大学　教授

(注)2022年6月末時点

CRYPTREC暗号等の監視　https://www.cryptrec.go.jp/eval_cmte.html

■「素因数分解の困難性に関する計算量評価」の更新

- 2006年度と2018年度に安全性評価を実施（一般数体篩法の計算量評価）

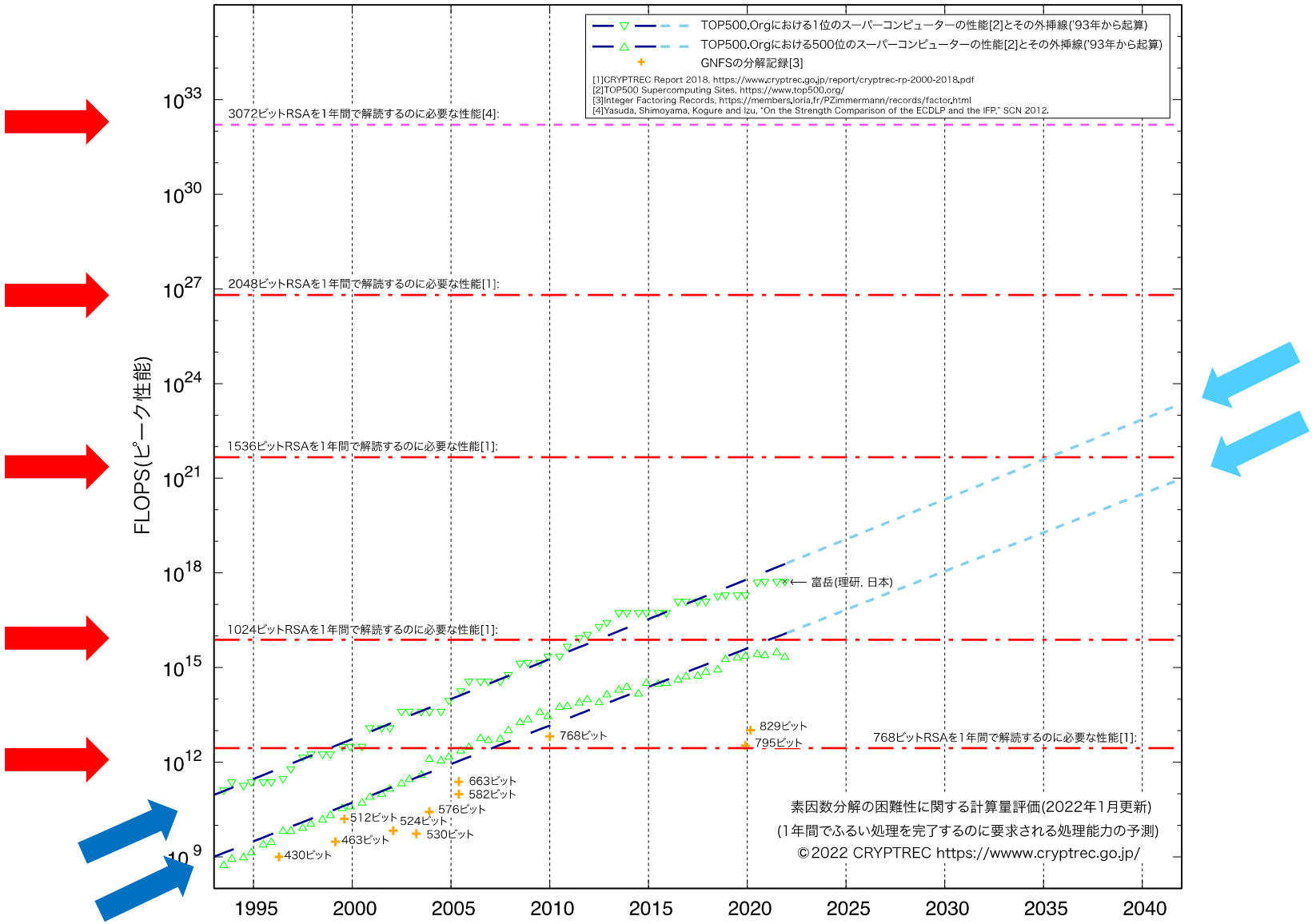
参考：CRYPTRECシンポジウム2019（暗号技術評価委員会活動報告）
https://www.cryptrec.go.jp/symposium/2019_cryptrec-eval.pdf

■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（2019年度～）

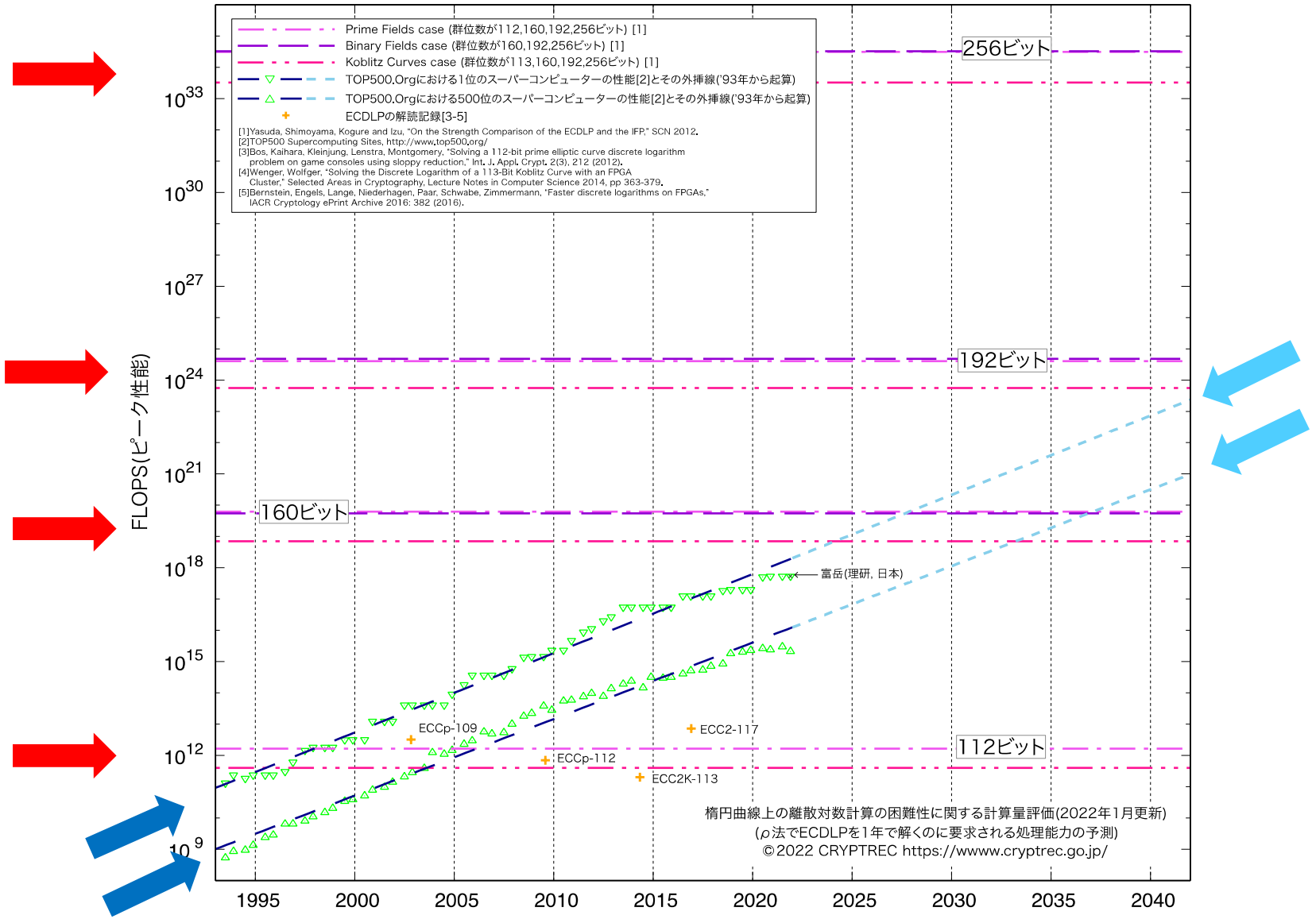
- 解読の脅威の尺度に用いていたスーパーコンピュータの性能向上が鈍化傾向にあるものの、いわゆるムーアの法則を仮定して外挿線を年度末から20年後まで直線で引き、安全サイドに倒した評価として当面の間更新していく
- 公開鍵暗号のパラメータ選択に関する対応方針については、安全性以外にも相互接続性など、運用上の観点もあるため、今後は、関係各所などを含めて検討する

（☞ 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.html

CRYPTREC暗号等の監視 – 素因数分解の困難性に関する計算量評価（2021年度版）

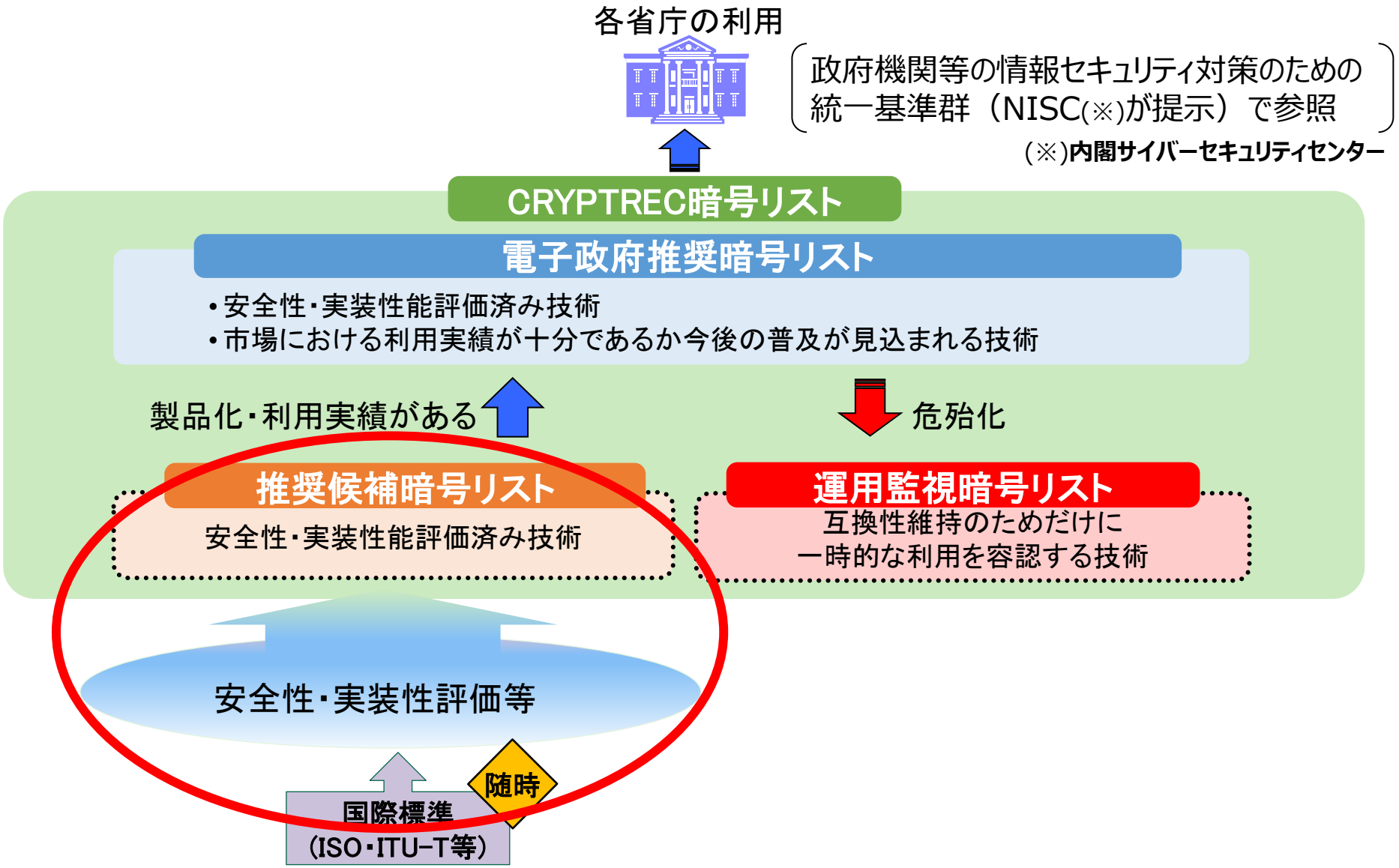


CRYPTREC暗号等の監視 – 楕円曲線上の離散対数計算の困難性に関する計算量評価（2021年度版）



CRYPTREC 暗号リストの構成

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



推奨候補暗号リストへの新規暗号(事務局選出)の追加 – XTS

■暗号利用モード(秘匿モード) XTS

- ストレージデバイス上のデータの暗号化の規格として標準化され、製品に搭載されるなどの実績がある
- 2018年度までの安全性評価において、暗号利用モード (秘匿モード) としてCRYPTREC暗号リストへ追加するための安全性要件を満たしていると判断した
- 2019年度に実施した実装性能評価の結果も併せて、XTSモードはCRYPTREC暗号リストに掲載するために十分な安全性及び実装性能を有すると判断した
- 2019年度の審議により、安全性要件は、下記の２つに変更された

(1) 利用用途はNIST SP 800-38Eの規格に沿ったストレージデバイスの暗号化に限る

(2) XTS内のブロック暗号には、CRYPTREC暗号リスト掲載の128ブロック暗号を使う

推奨候補暗号リストへの新規暗号(事務局選出)の追加 – EdDSA

■ディジタル署名 EdDSA

- RFC 8032で規定され、TLS 1.3(RFC 8446)で採用され、米国NISTにおいてもFIPS 186-5(現在はDraft版)において追加予定である。2019年度暗号活用委員会においても安全性評価の必要性が示された
- 2020年度はCRYPTREC暗号リストへ追加するための安全性評価を実施した。国内・国外1名ずつ有識者による外部評価を実施
- 2021年度はCRYPTREC暗号リストへ追加するための実装性能評価を実施した。国内1名の有識者による外部評価を実施

評価内容	評価を依頼した有識者（肩書きは評価実施時のもの）
EdDSAで使われる楕円曲線の安全性評価	(1) 安田雅哉 准教授（立教大学） (2) Steven Galbraith 教授(University of Auckland)
方式の構成そのものの安全性評価	(1) 藤崎英一郎 教授 (北陸先端科学技術大学院大学) (2) Steven Galbraith 教授 (University of Auckland)
EdDSAの実装性能に関する評価・調査	菅野 哲 様（株式会社インフォーズ、現在は、GMO サイバーセキュリティ byイエラエ株式会社）

推奨候補暗号リストへの新規暗号(事務局選出)の追加 – EdDSA

■ディジタル署名 EdDSA

- 曲線に関する安全性評価
  - 安全性は現在使用されている楕円曲線暗号の場合と同じく、結果として主に基礎体の大きさで決定される。従って、Curve25519の場合はほぼ128ビットセキュリティ、Curve448の場合はほぼ224ビットセキュリティの安全性を持つと判断した
- 方式の構成に関する安全性評価
  - 複数の観点から安全性に関わる考察が示されており、いずれも安全性に問題を与える点はなかった。現実的な脅威に結びつくような脆弱性は指摘されておらず、ECDSAと比較してもその安全性に劣る点はないと考えられると判断した
- 実装性能評価
  - 公開されている第三者の測定結果および本調査による測定結果の範囲では、Ed25519及びEd448はECDSAと同等以上であると評価
- 2020年度に実施した安全性評価および2021年度に実施した実装性能評価の結果に基づき、EdDSAはCRYPTREC暗号リストに掲載するために十分な安全性及び実装性能を有すると判断した。

CRYPTREC 注意喚起レポートの発行

■ CRYPTREC ER-0001-2019

- ゲート型の量子コンピュータが量子超越を実現したと主張する論文が2019年10 月にNature誌で発表された
- 暗号技術評価委員会では、正確で信頼性の高い情報を発信することによる過剰反応防止の目的で注意喚起レポートを公表した
- 量子コンピュータを用いて2048ビットRSA合成数の素因数分解を行う場合には（ショアのアルゴリズムを想定）、量子誤り訂正無しという環境下で、4098量子ビットが必要であり、10^{12}～10^{13}回のゲート演算が必要であると見積もられています。また、量子誤り訂正有りという環境下で、2000万量子ビットが必要であるという見積もりもある
- 暗号解読には規模の拡大だけでなく量子誤り訂正などの実現が必要であるため、CRYPTREC暗号リスト記載の暗号技術が近い将来に危殆化する可能性は低いものと判断
- 詳細は
  https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html

仕様書の参照先の変更

■ CRYPTREC の Web サイトでは、CRYPTREC 暗号リストに掲載している暗号技術の仕様書の参照先を掲載しています

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

■仕様書のバージョンアップがある場合に、仕様の変更がないかどうか、安全性に影響がないかどうか、の確認をした上で、適宜、参照先を訂正

- 例：米国NIST FIPSやSP 800の更新への対応
- 例：RSA暗号（RSA-PSS、RSASSA-PKCS1-v1_5、RSA-OAEP、RSAES-PKCS1-v1_5）のリンク先を、IEFTのRFC 8017に変更

新技術などに関する調査及び評価

■次期CRYPTREC暗号リストとは別文書として、**耐量子計算機暗号**、**軽量暗号**及び**高機能暗号**に関するガイドラインを作成することが暗号技術検討会にて決定された。

■耐量子計算機暗号及び高機能暗号については、
- ●暗号技術調査ワーキンググループ(耐量子計算機暗号)を実施
- ●暗号技術調査ワーキンググループ(高機能暗号)を実施

委員会活動の説明後、WGの説明

■軽量暗号について
- ●２０１６年度発行の「CRYPTREC 暗号技術ガイドライン (軽量暗号)」を更新する方針

軽量暗号技術に関わる取り組み

■「CRYPTREC 暗号技術ガイドライン(軽量暗号)」の発行

- 2013年～2016年　軽量暗号WG にて検討、2017年3月公開

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

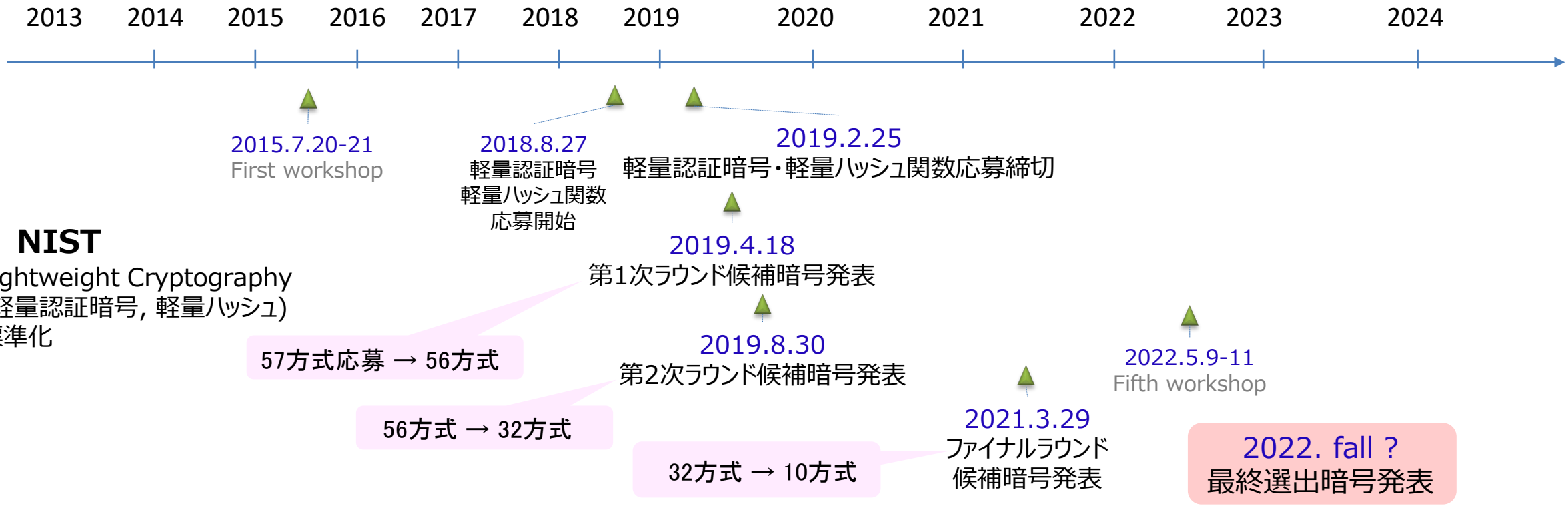
- 日本語版および英語版

- 作成の目的
  - 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

軽量暗号に関わる技術動向



軽量暗号ガイドライン更新

■「CRYPTREC 暗号技術ガイドライン (軽量暗号)」2023年度版(※)

(※) 以降、2023年度版軽量暗号ガイドライン呼ぶ

- 「CRYPTREC 暗号技術ガイドライン (軽量暗号)」2016年度版(※)
  を基に更新を行う

  (※) 以降、2016年度版軽量暗号ガイドライン呼ぶ

  - 主たる追加は、2016年度版軽量暗号ガイドライン4章「代表的な軽量暗号」に相当する軽量暗号方式の紹介とする。
  - 既に4章に掲載されている方式については、2021年実施の安全性評価の動向調査を基に更新する。
  - 1章～3章は、2016年度版軽量暗号ガイドラインをそのまま用いる。ただし、4章に新規追加・更新する方式に関わる情報は、適切な章に節を追加し、掲載する。
  - 付録を追加し、関連情報を掲載する。
- 追加情報の対象
  - NIST Lightweight コンペティション最終選考で採択された方式
  - 軽量な方式として ISO に近年採録されたもしくは採録される予定の方式

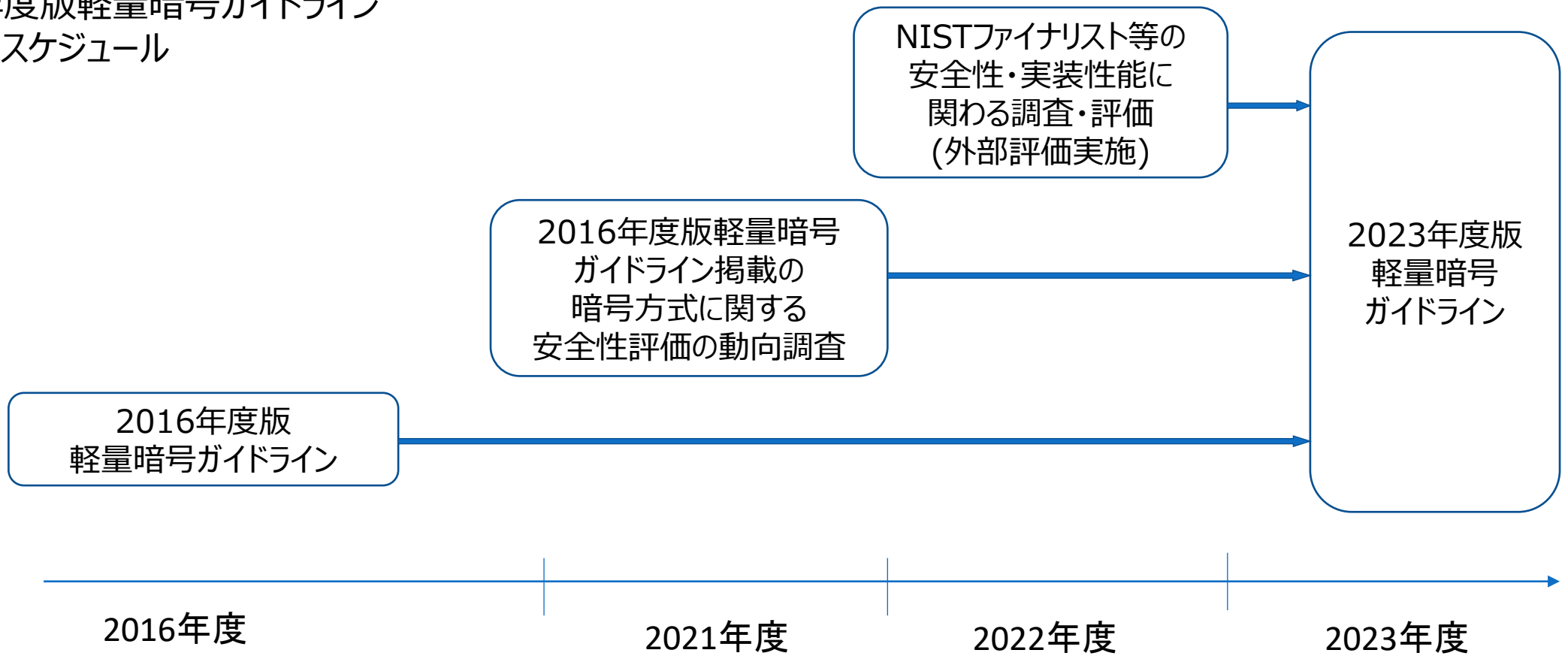
2021年度実施内容

■軽量暗号方式に関する安全性評価の動向調査を実施

- ●調査対象
  - ➢ 2016年度版軽量暗号ガイドラインに掲載されている方式
  - ➢ 軽量暗号に関わるISO/IEC 29192シリーズに近年採録されたもしくは採録される予定の方式について、2016年度版軽量暗号ガイドラインにおける掲載の有無およびそれらの安全性に関わる攻撃の有無
  - ➢ CAESARプロジェクトの最終選出ポートフォーリオ6方式(3ケース各2方式)について、2016年度版軽量暗号ガイドラインにおける掲載の有無、およびそれらの安全性に関わる攻撃の有無
- ●実施方法
  - ➢ 調査報告書の執筆：事務局
  - ➢ 調査報告書レビュー：峯松　一彦　様（日本電気株式会社）
- ●実施結果
  - ➢ ガイドラインに掲載されている方式については、即座にガイドラインから外すべき甚大な脆弱性を持つ方式は無かった
  - ➢ 2023年度版軽量暗号ガイドラインに反映

2023年度版軽量暗号ガイドラインに向けた予定

2023年度版軽量暗号ガイドライン
に向けたスケジュール



NIST
Lightweight Cryptography
Project 動向

▲ ファイナルラウンド候補暗号発表

▲ 最終選出暗号発表(予定)

暗号技術調査ワーキンググループ
（暗号解析評価：2019年度～2020年度）
（耐量子計算機暗号：2021年度～2022年度）
活動報告

2022年　7月　5日

ワーキンググループ　主査
（筑波大学　教授）
國廣 昇

暗号解析評価WG委員（2019年度～2020年度）

主査	**國廣　昇**	筑波大学　教授
委員	青木　和麻呂	文教大学　准教授
委員	草川　恵太	日本電信電話株式会社 主任研究員
委員	桑門　秀典	関西大学　教授
委員	下山　武司	国立情報学研究所 特任研究員
委員	高木　剛	東京大学　教授

委員	高島　克幸	三菱電機株式会社 主管技師長
委員	峯松　一彦	日本電気株式会社 主席研究員
委員	安田　貴徳	岡山理科大学　准教授
委員	安田　雅哉	立教大学　准教授

(注)2021年3月末時点

量子コンピュータによる共通鍵暗号への影響の調査

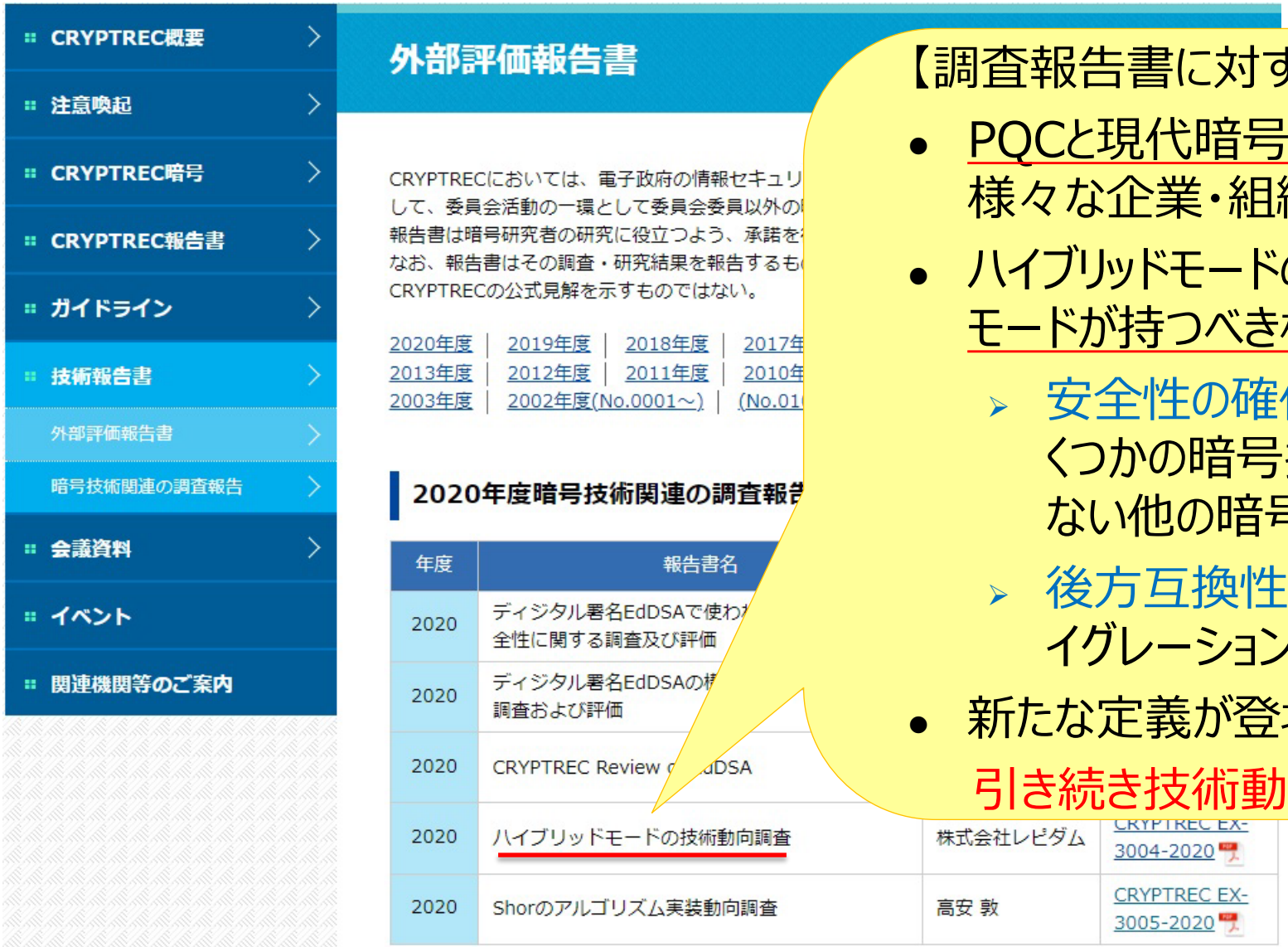
量子コンピュータによる公開鍵暗号への影響の調査

【調査報告書に対する暗号解析評価WGの見解】

- Shor のアルゴリズムと量子コンピュータ実機によって解かれた素因数分解問題や離散対数問題は以下のとおりである。
  - 素因数分解: 15, 21
  - 有限体上の離散対数問題:

    $2^x \equiv 1 (\mathrm{mod}\ 3)$
- 現状の量子コンピュータによるRSA2048などへの現実的な脅威が生じる可能性は極めて低く、**現状ではCRYPTRECでの具体的な対応は不要である。**

耐量子計算機暗号を導入する際の技術の調査



【調査報告書に対する暗号解析評価WGの見解】

- PQCと現代暗号を併用するいわゆるハイブリッドモードが様々な企業・組織で世界的に議論されている。
- ハイブリッドモードの合意の取れた定義はなく、ハイブリッドモードが持つべき様々な要件が議論されている。
  - 安全性の確保：システムなどの中で利用されているいくつかの暗号技術の安全性に問題があっても、問題のない他の暗号技術によって全体としての安全性を保つ。
  - 後方互換性の確保：暗号技術の移行やシステムマイグレーションを円滑に行う一助となる。
- 新たな定義が登場する可能性もあるため

  引き続き技術動向を把握する必要がある。

耐量子計算機暗号WG委員（2021年度～2022年度）

主査	**國廣　昇**	筑波大学　教授
委員	青木　和麻呂	文教大学　准教授
委員	伊藤　忠彦	セコム株式会社　主務研究員
委員	草川　恵太	日本電信電話株式会社 主任研究員
委員	下山　武司	国立情報学研究所 特任准教授
委員	高木　剛	東京大学　教授

委員	高島　克幸	早稲田大学　教授
委員	廣瀬　勝一	福井大学　教授
委員	安田　貴徳	岡山理科大学　准教授
委員	安田　雅哉	立教大学　教授

(注)2022年6月末時点

耐量子計算機暗号WGの活動目的と活動概要

■ 背景

- 量子コンピュータが実用化されても安全性を保てると期待される暗号（耐量子計算機暗号：PQC）の研究開発及び標準化などが各国で進められている。
- 国内においても耐量子計算機暗号について議論を行う必要性が高まっている。
- CRYPTRECで耐量子計算機暗号ガイドラインを作成し、利用指針を示す。

■ WGの活動目的

- 2022年度までに、耐量子計算機暗号のガイドラインを作成する

■ WGの活動概要

- 暗号技術調査WG（暗号解析評価）において2019年に公開した「耐量子計算機暗号の研究動向調査報告書」を基に、更なる技術動向調査を実施する。
- 上述の調査をもとに、耐量子計算機暗号ガイドラインを作成する。

ガイドラインに掲載する暗号の選定及び分類

■ 選定の基準

- 公開鍵暗号を中心にまとめる。
- 世界的に使用が見込まれる耐量子計算機暗号（NIST PQC 標準化への提案方式等）を記載する。

■ 分類

- 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暗号技術

耐量子計算機暗号ガイドラインの目次案

1. 導入
2. 耐量子計算機暗号の活用方法
3. 格子に基づく暗号技術
4. 符号に基づく暗号技術
5. 多変数多項式に基づく暗号技術
6. 同種写像に基づく暗号技術
7. ハッシュ関数に基づく暗号技術

■ 1章
- PQCの調査の背景
  （量子コンピュータによる現代暗号への脅威など）

■ 2章
- 実社会でのPQCの活用事例を説明。
  （特に守秘・鍵交換・署名の活用事例）

■ 3章～7章
- 安全性の根拠となる問題の説明
- 各暗号技術の説明
  （アルゴリズムの擬似コード、暗号文・署名、
  鍵長のサイズなど）

暗号技術調査ワーキンググループ（高機能暗号）活動報告

2022年　7月　5日

ワーキンググループ　主査
（横浜国立大学　教授）
四方 順司

高機能暗号WG委員

主査	**四方　順司**	横浜国立大学　教授
委員	岩本　貢	電気通信大学　教授
委員	大原　一真	国立研究開発法人産業技術総合研究所 主任研究員
委員	勝又　秀一	国立研究開発法人産業技術総合研究所 主任研究員
委員	金岡　晃	東邦大学　准教授
委員	川原　祐人	日本電信電話株式会社　主任研究員
委員	国井　裕樹	セコム株式会社　グループリーダー
委員	須賀　祐治	株式会社インターネットイニシアティブ シニアエンジニア

委員	鈴木　幸太郎	豊橋技術科学大学　教授
委員	花岡　悟一郎	国立研究開発法人産業技術総合研究所 首席研究員
委員	外園　康智	株式会社野村総合研究所　上級研究員
委員	濱田　浩気	日本電信電話株式会社　主任研究員
委員	山田　翔太	国立研究開発法人産業技術総合研究所 主任研究員
委員	米山　一樹	茨城大学　教授
委員	渡邉　洋平	電気通信大学　助教

(注)2022年6月末時点

高機能暗号WGの活動目的と活動概要

■ 背景

- アプリケーションの多様化に伴い、公開鍵暗号の活用が広まる。
- 機能が向上した高機能暗号が、アプリケーションに適し、効率的に作用する。
- どのような高機能暗号があるか知られていない。
- 高機能暗号の利用方法についてガイドが存在しない。

■ WGの活動目的

- 2022年度までに、高機能暗号のガイドラインを作成し、高機能暗号の利用指針を示す。

■ WGの活動概要

- 高機能暗号の定義を明確化する。
- 高機能暗号の技術に関する現状調査を行う。
- 高機能暗号のアプリケーションに関する現状調査を行う。
- 定義、現状調査をもとに、高機能暗号ガイドラインを作成する。

ガイドラインの読者

- セキュリティ技術の標準化を目指す団体
- セキュリティ機能の設計・開発・実装を行う技術者
- セキュリティ機能を搭載した情報システムの導入を推進する企業

章立て（後述）と想定する読者

- 第１章、第２章：　どのような暗号があり、どのような利用方法があるかを知りたい読者
- 第３章　　：　暗号技術の詳細を知りたい読者

高機能暗号ガイドラインで扱う高機能暗号の定義

「高機能暗号」とは何か

■ 一般的に合意されている定義が存在しない。

⇩

定義を作る必要有り。

⇩

ガイドラインで扱う高機能暗号の定義

「従来の暗号技術に対して、機能が追加・向上されるなど優位性を主張する暗号、および、従来の暗号技術では困難であった事象を解決できるなどの新規機能を有することを主張する暗号技術」

高機能暗号の分類

高機能暗号の現状調査により、以下に示す3分類、19項目に関し、技術・アプリケーション・標準化についてガイドラインに掲載することとした。

分類	項目
守秘	IDベース暗号、属性ベース暗号、放送型暗号、しきい値暗号、準同型暗号、プロキシ再暗号化
署名・認証	IDベース署名、属性ベース署名、集約署名・MAC・マルチ署名、グループ署名、リング署名、しきい値署名
その他	秘密分散、マルチパーティ計算ー秘密分散ベース、マルチパーティ計算ーGarbled Circuitベース、ゼロ知識証明、検索可能暗号、Private Information Retrieval、Oblivious RAM

高機能暗号ガイドラインの目次案

1．はじめに

2．高機能暗号技術とその活用法

2.1．高機能暗号とは

2.2．高機能暗号の種類と分類

2.3．高機能暗号はどこに使えるか、その有用性

2.4．高機能暗号の活用例と効果

2.4.1．守秘関連の活用事例

2.4.2．認証・署名関連の活用事例

2.4.3．その他の高機能暗号の活用事例

アプリケーション・標準化関係

詳細技術関係

3．主な高機能暗号技術のアルゴリズム

3.1．守秘関連のアルゴリズム

3.2．署名・認証関連のアルゴリズム

3.3．その他のアルゴリズム

4．おわりに

暗号技術評価委員会　今後の予定

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。

■ 暗号技術の安全性及び実装に係る監視及び評価を継続する。

■ 暗号技術の安全な利用方法に関する調査を継続する。

- 2022年度　耐量子計算機暗号ガイドライン、高機能暗号ガイドラインを作成する。
- 2023年度版軽量暗号ガイドラインに向け、ガイドラインの更新に取り組む。