CRYPTREC シンポジウム 2023

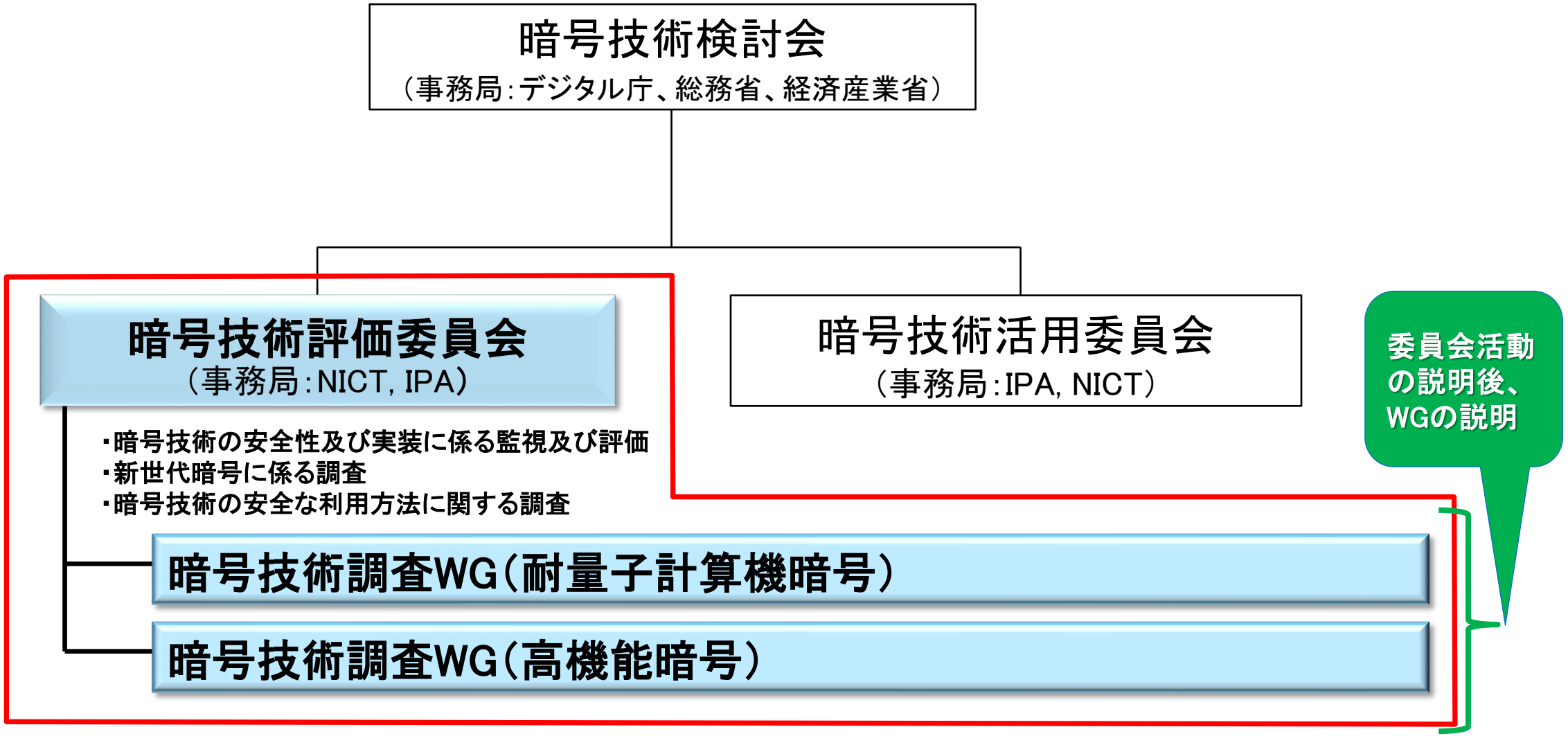
CRYPTREC
Cryptography Research and Evaluation Committees

# 暗号技術評価委員会 活動報告
## (2022年度～2023年度)

2023年 7月26日

暗号技術評価委員会　委員長
高木 剛(東京大学、教授)

# 2022年度　CRYPTREC体制（暗号技術評価委員会）



# 2022年度及び2023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暗号リストの
改定（2022年度）

各省庁の利用

政府機関等の情報セキュリティ対策のための
統一基準群（NISC(※)が提示）で参照

(※)内閣サイバーセキュリティセンター

**CRYPTREC暗号リスト**

**電子政府推奨暗号リスト**

- 安全性・実装性能評価済み技術
- 市場における利用実績が十分であるか今後の普及が見込まれる技術

製品化・利用実績がある

危殆化

**推奨候補暗号リスト**

安全性・実装性能評価済み技術

**運用監視暗号リスト**

互換性維持のためだけに
一時的な利用を容認する技術

安全性・実装性評価等

国際標準

随時

- ✓ 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に係る検討
- ✓ 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

# 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

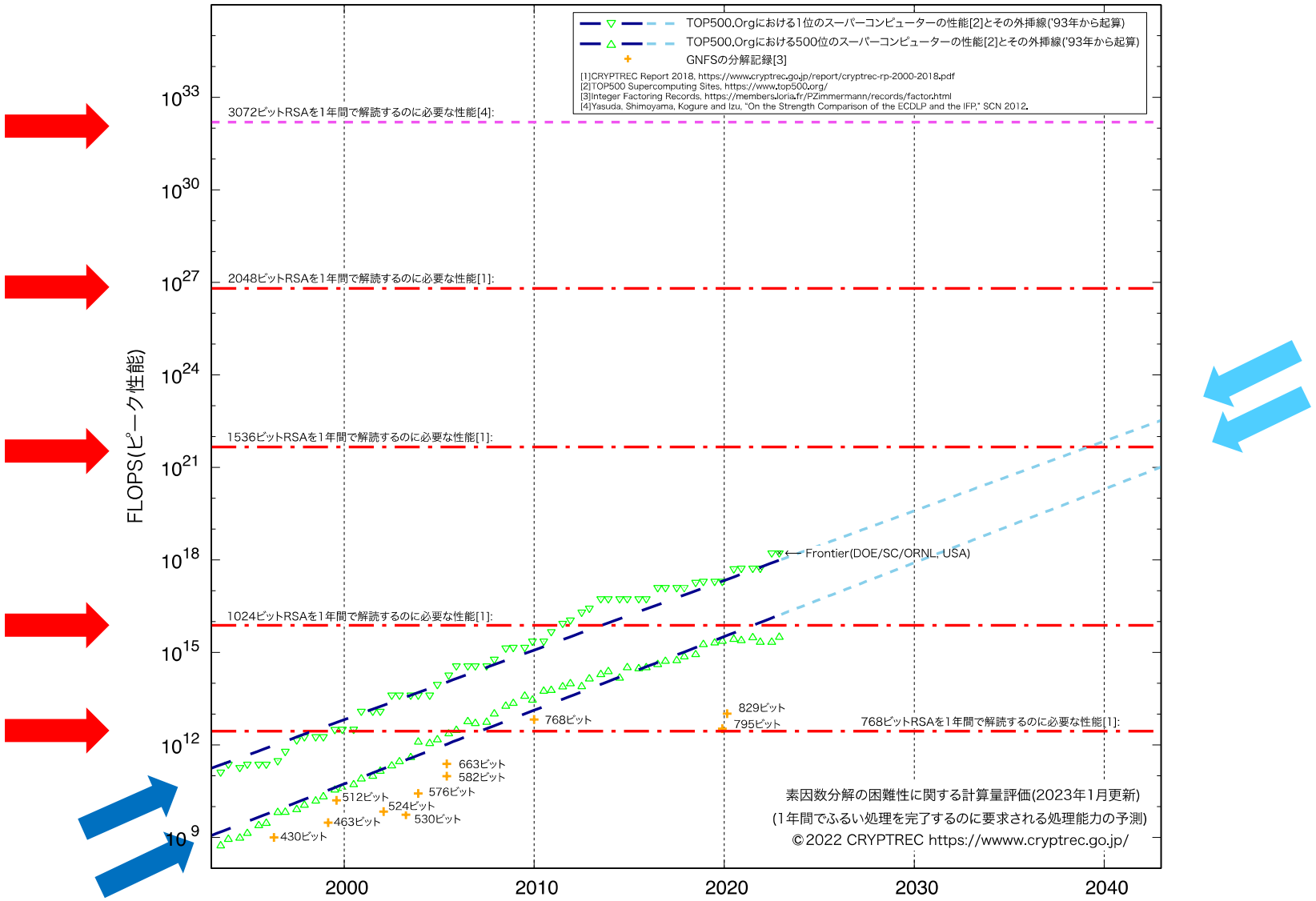
■素因数分解の困難性、離散対数問題の困難性に基づく暗号の危殆化の時期を予測する図の今後の取り扱い

- 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、今後は、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）**

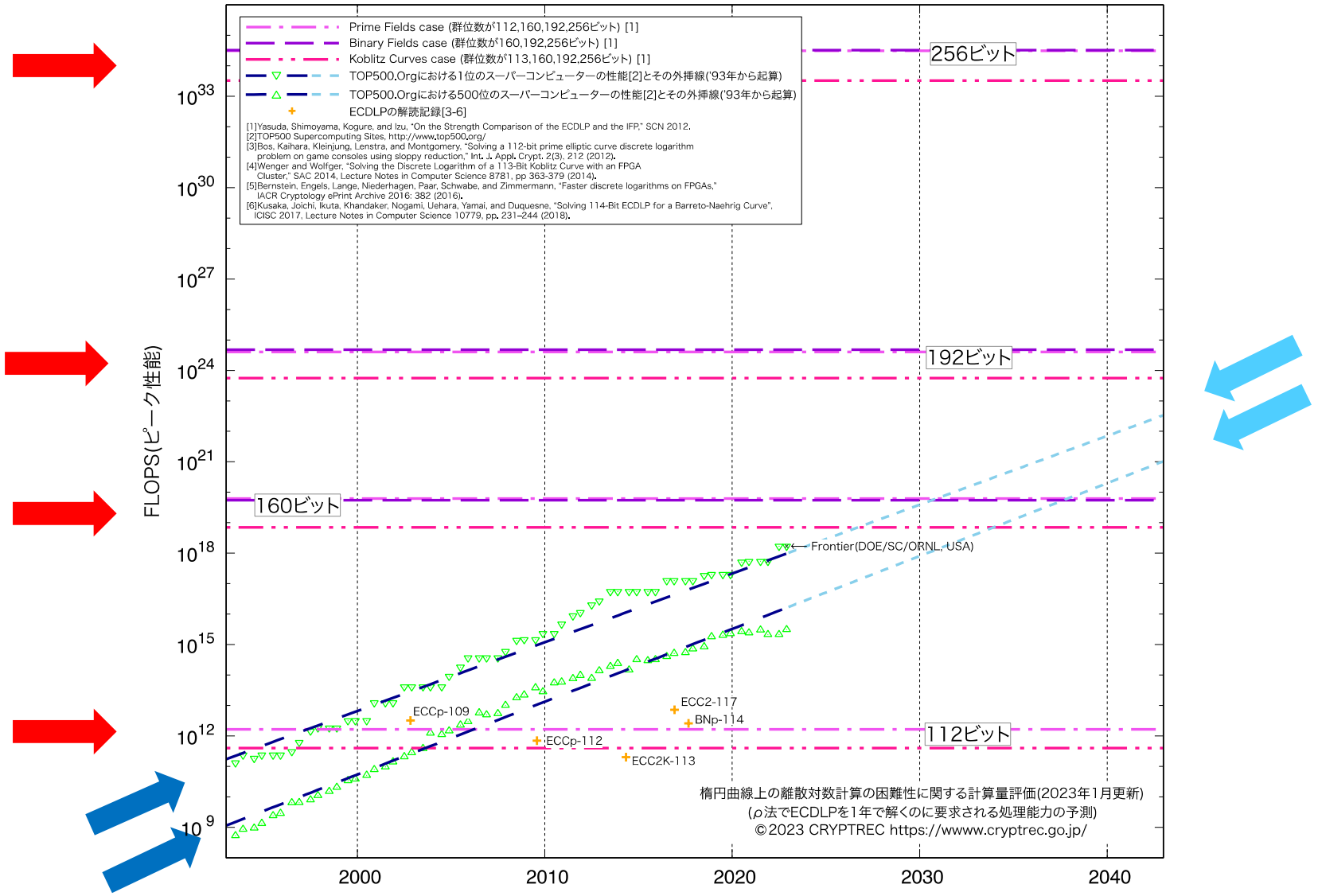
# ①CRYPTREC暗号等の監視
# －素因数分解の困難性に関する計算量評価（2022年度版）

CRYPTREC
Cryptography Research and Evaluation Committees



# 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（2022年度版）

CRYPTREC
Cryptography Research and Evaluation Committees



# 2022年度活動内容　新技術などに関する調査及び評価

■耐量子計算機暗号及び高機能暗号に関するガイドラインを策定

- ●耐量子計算機暗号に関する研究動向調査報告書及び耐量子計算機暗号ガイドラインの作成

  ⇒　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

- ● 高機能暗号ガイドラインの作成

  ⇒　詳細は、暗号技術調査ワーキンググループ（高機能暗号）の活動報告へ

■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）」2016年度版を基に更新を行う
  - ➢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

# 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

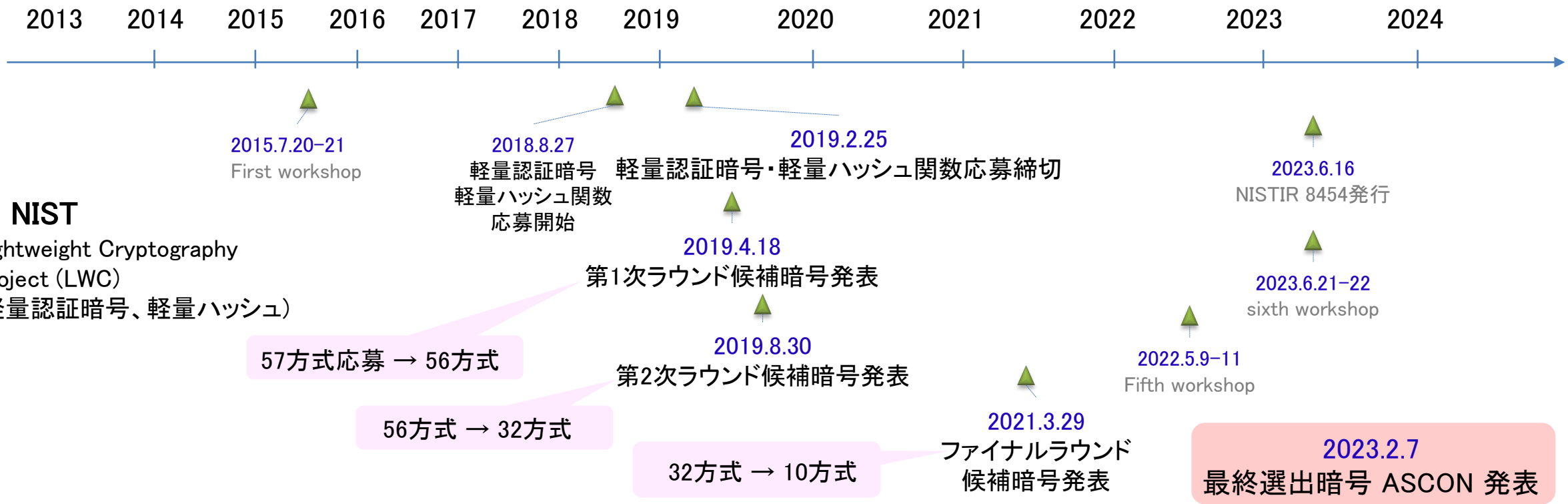
- 日本語版および英語版

- 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 Cryptography Project の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

# 2022年度実施内容(1/2)

■ 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

- 調査対象
  - NIST LWCファイナリスト 10方式：
    ASCON, Elephant, GIFT-COFB, Grain-128AEAD, ISAP,
    PHOTON-Beetle, Romulus, SPARKLE, TinyJAMBU, Xoodyak
  - ISO/IEC標準規格29192 シリーズで規格化された軽量メッセージ認証コード：
    Tsudik’s keymode
- 実施方法
  - 有識者による外部評価を実施
  - 依頼先：
    岩田 哲　 様（名古屋大学）
    内藤 祐介 様（三菱電機株式会社）
    藤堂 洋介 様（日本電信電話株式会社）
    井上 明子 様（日本電気株式会社）

# 2022年度実施内容(2/2)

■ NIST LWC ファイナリストなどの実装性能に関わる動向調査を実施

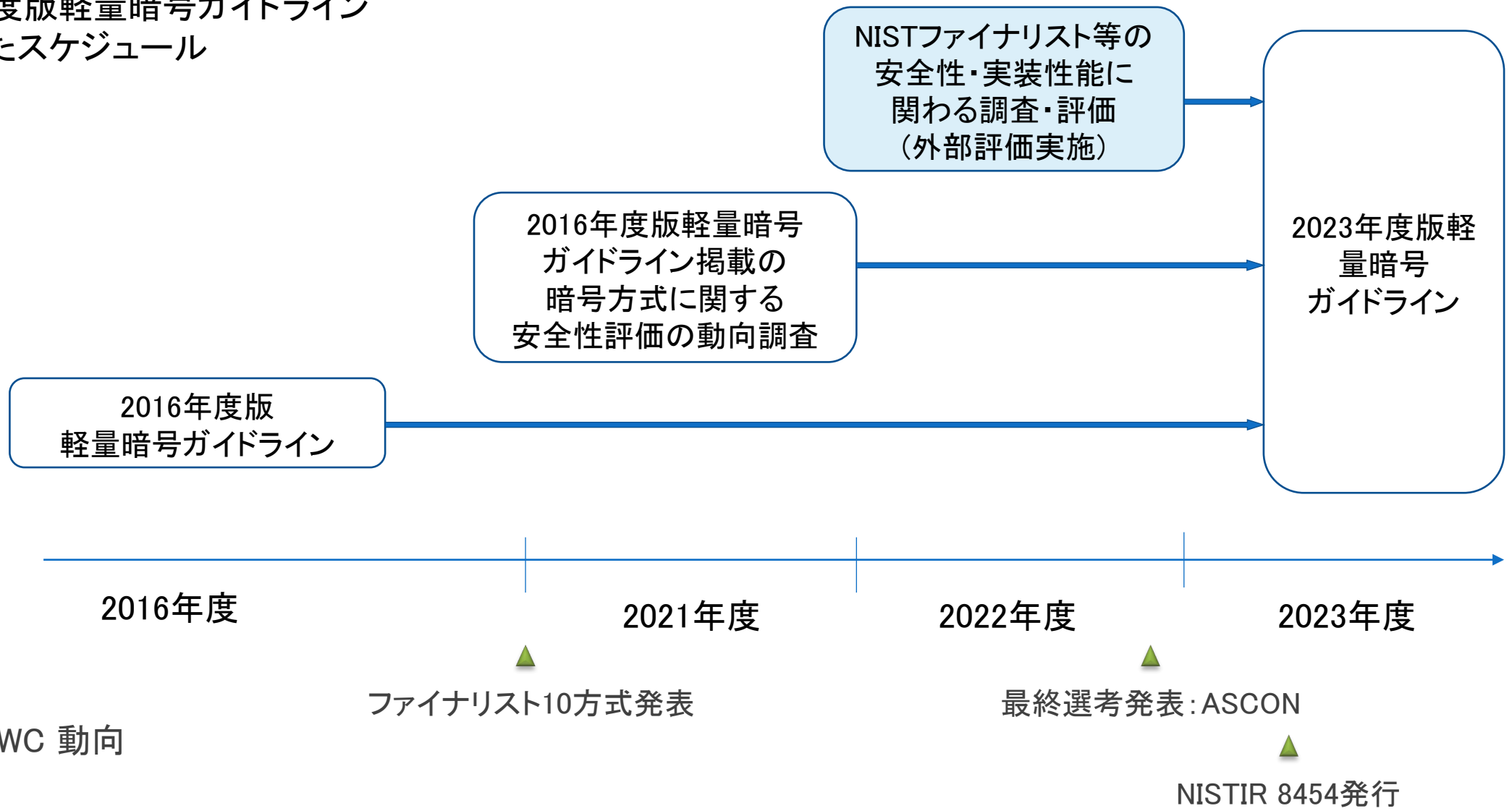
- 調査対象
  - NIST LWCファイナリスト 10方式
- 実施方法
  - 有識者による外部評価を実施
  - 依頼先：崎山 一男 様（電気通信大学）

■NIST LWC ファイナリストなどを中心とした標準化などの動向調査を実施

- 調査対象
  - NIST LWCファイナリスト選出に関わる選定指標や評価指標など
  - 軽量暗号に関わる ISO/IEC などの標準化動向など
- 実施方法
  - 有識者による外部評価を実施
  - 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）

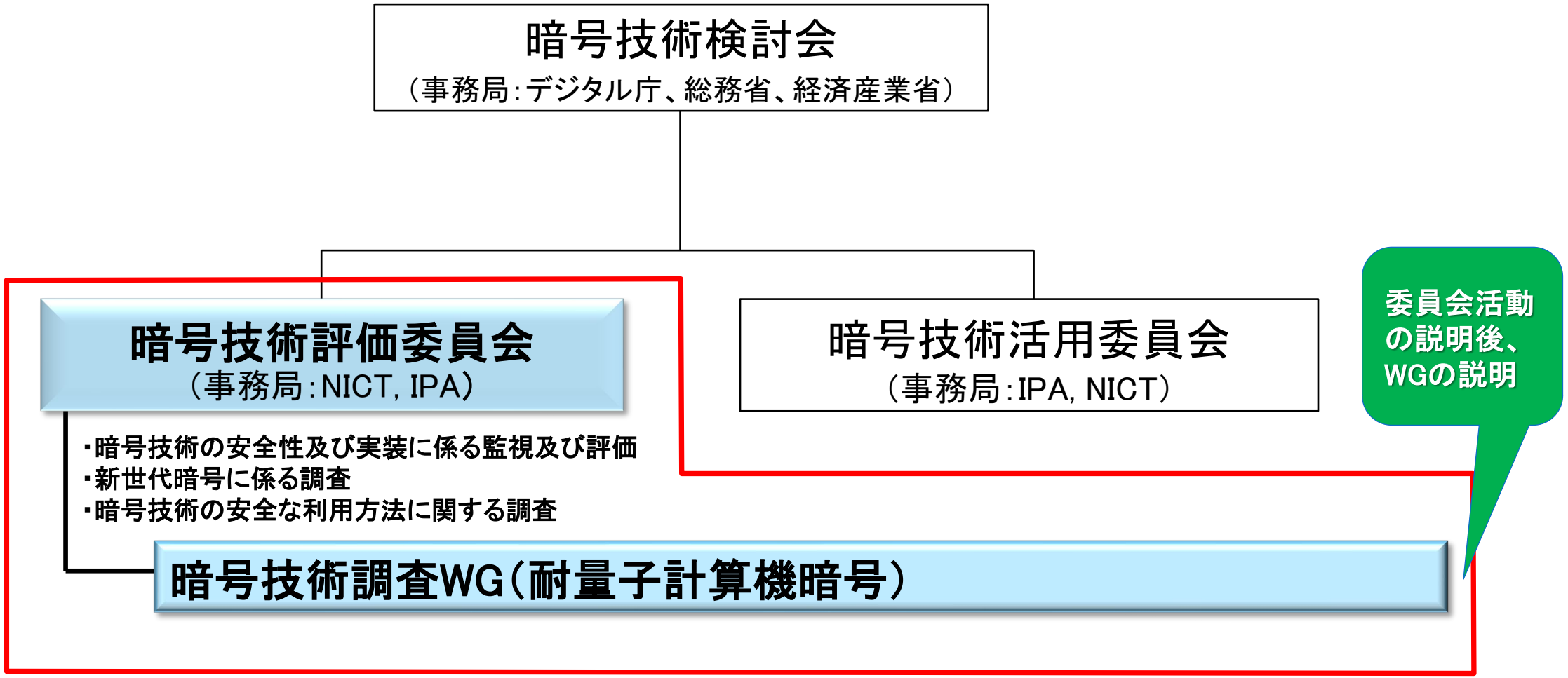
# 2023年度版軽量暗号ガイドラインに向けた予定

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　LWC 動向

# 2023年度　CRYPTREC体制（暗号技術評価委員会）



# 2023年度活動内容　新技術などに関する調査及び評価

## ■軽量暗号ガイドラインの更新

- ●NISTファイナリスト ASCONの安全性・実装性能に関わる調査・評価
- ●「CRYPTREC暗号技術ガイドライン（軽量暗号）」2023年度版を公開予定

## ■耐量子計算機暗号に関する研究動向調査及びガイドラインの更新

- ●米国NISTでは、PQC標準化第4ラウンドが現在も進行中であり、また、さらに、短い署名長をもち、署名検証処理が速いデジタル署名の追加公募が行われ、受付が締め切られたところ（2023年6月〆切）
- ●引き続き、暗号技術調査ワーキンググループ（耐量子計算機暗号）の設置し、最新動向を把握

⇒　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

CRYPTREC シンポジウム 2023

CRYPTREC
Cryptography Research and Evaluation Committees

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

2023年　7月　26日

ワーキンググループ　主査
（筑波大学　教授）
國廣 昇

# 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　高島　克幸 |
| 委員　伊藤　忠彦 | 委員　廣瀬　勝一 |
| 委員　草川　恵太 | 委員　安田　貴徳 |
| 委員　下山　武司 | 委員　安田　雅哉 |
| 委員　高木　剛 | |

# 耐量子計算機暗号WGの活動目的

## ■ 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9月末までの耐量子計算機暗号に関する情報を網羅的に調査
- 2022年度までに、耐量子計算機暗号の調査報告書・ガイドラインを作成する

# 耐量子計算機暗号WGの活動概要

## ■ 技術動向調査

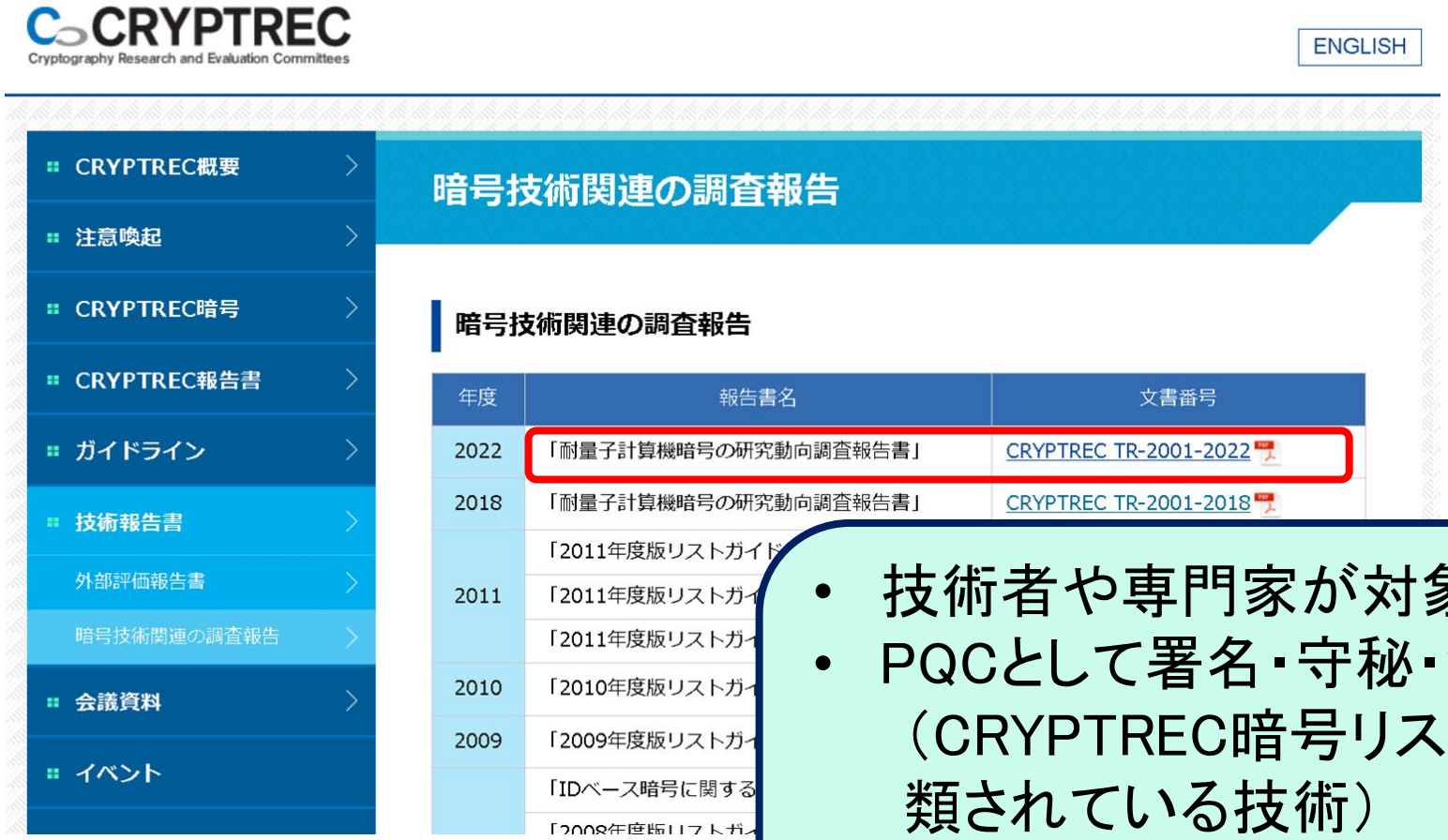
- 「耐量子計算機暗号の研究動向調査報告書2018年度版」を基にした
- 2022年9月末までの耐量子計算機暗号に関する情報を網羅的に調査
  - 国際会議CRYPTO、Eurocrypt、Asiacrypt、PQCrypto

- それ以降でも大きな話題があれば取り上げた
  - ハッシュ関数に基づく署名SPHINCS+の安全性レベルの見直し（PQCrypto2022）
  - SIDH鍵共有へのCastryck-Decru攻撃(Eurocrypt2022)およびその対策(ePrint 2023/013等)

## ■ 調査報告書およびガイドラインの公開

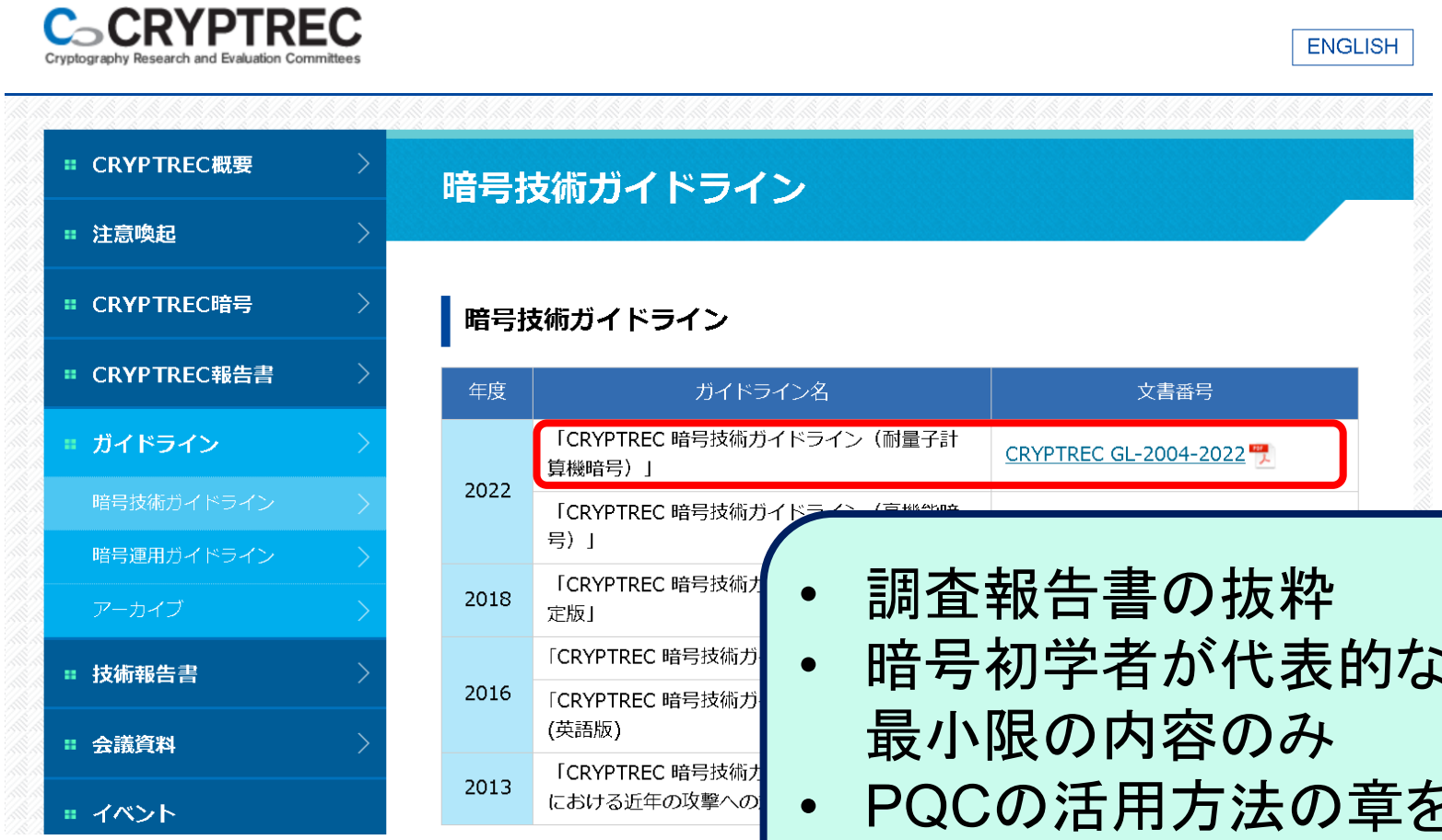
- 耐量子計算機暗号の研究動向調査報告書2022年度版
- CRYPTREC暗号技術ガイドライン（耐量子計算機暗号）2022年度版

# 耐量子計算機暗号の研究動向調査報告書




- 技術者や専門家が対象
- PQCとして署名・守秘・鍵共有を扱う（CRYPTREC暗号リストの中で「公開鍵暗号」として分類されている技術）
- 格子、符号、多変数、同種写像、ハッシュベースのPQCを調査
- 2018年版から大幅に内容を追記・修正

# 耐量子計算機暗号の暗号技術ガイドライン




- 調査報告書の抜粋
- 暗号初学者が代表的なPQC方式を把握するために最小限の内容のみ
- PQCの活用方法の章を追加

# 1章：はじめに

## ■暗号技術調査ワーキンググループ(耐量子計算機暗号)の活動概要

### ■ 耐量子計算機暗号（PQC）の必要性について

- 近年の量子コンピュータの開発状況と暗号解読実験の状況

  2022年9月末の時点で、現実的な大きさのパラメータを持つ暗号が解かれたという報告は存在しない

### ■ 研究の動向

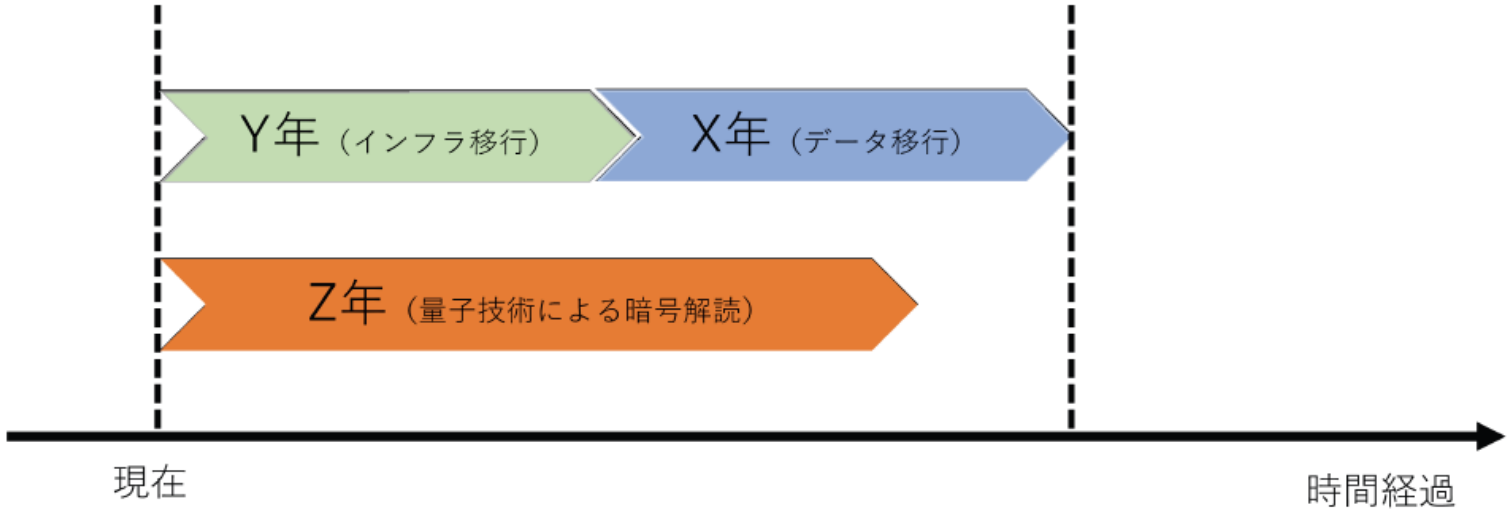
- PQCに関する国際会議
- NIST PQC標準化の概要

### ■ 調査対象としたPQCの種類

- 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署名技術

# 2章：PQCの活用方法 （ガイドラインのみ）

- PQCの背景、実社会での活用方法
- 暗号の利用形態
  - 公開鍵暗号を署名、守秘、鍵共有に分類
- 各利用形態における量子コンピュータの影響と課題
- 各利用形態ごとの固有の対策方法



# 3章～7章： 暗号技術の説明

- 調査報告書では2章～6章
- 主要な暗号方式およびそれらのベースとなる代表的な暗号方式の説明
  - アルゴリズムの擬似コード
  - 暗号文長、署名長、鍵長
  - 安全性の根拠となる計算問題
- 代表的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
    - 歴史的に関係の深いそれらの基礎となっている方式（構成のひな形）等
  - ガイドラインには主要な暗号を掲載した

# 主要な暗号方式として取り上げたものの一覧表

| ベースとなる問題の種類 | 暗号化・鍵交換 | 署名 |
|---|---|---|
| 格子 | NewHope, FrodoKEM, NTRU, SABER, CRYSTALS-Kyber, | CRYSTALS-Dilitium, FALCON |
| 符号 | Classic McEliece, BIKE, HQC | |
| 多変数 | | UOV |
| 同種写像 | | SQISign |
| ハッシュ | | LMS, XMSS, SPHINCS+ |

（赤字：暗号化・鍵交換、青字：署名、下線：ガイドライン掲載）

# 今後の予定

- 暗号技術調査ワーキンググループ（耐量子計算機暗号）を2023～2024年度にかけて設置、引き続き耐量子計算機暗号の技術調査を行う
  - NIST PQCの候補に残った暗号方式に対しても脆弱性が発見され、攻撃・暗号方式双方の改良が続いている

- 調査の方針は2022年度版と同様
  - 2024年9月末までの耐量子計算機暗号に関する情報を網羅的に調査
  - それ以降でも大きな話題があれば掲載
  - 2022年度版ガイドラインで取り上げた分類以外の暗号技術でも、必要があれば取り上げて追加

# NIST PQC: Selected Algorithms 2022

| Cryptography | Underlying Security Problems | Algorithm |
|---|---|---|
| Public-key Encryption and Key-establishment Algorithms | Lattice-based | CRYSTALS-KYBER |
| Digital Signature Algorithms | Lattice-based | CRYSTALS-DILITHIUM<br>FALCON |
| | Hash-based | SPHINCS+ |

https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

# NIST PQC: Round 4 Submissions

| Cryptography | Underlying Security Problems | Algorithm |
|---|---|---|
| Public-key Encryption and Key-establishment Algorithms | Lattice-based | BIKE |
| | Code-based | Classic McEliece<br>HQC |
| | Isogeny | SIKE<br>(The SIKE teams acknowledges that SIKE and SIDH are insecure and should not be used.) |

https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

# NIST PQC: Additional Digital Signature Schemes (Round 1)

| Round 1 Additional Signatures | # submits | Algorithm (Updated July 17, 2023) |
|---|---|---|
| Code-based Signatures | 5 | Enhanced pqsigRM, FuLeeca, LESS, MEDS, Wave |
| Isogeny Signatures | 1 | SQIsign |
| Lattice-based Signatures | 7 | EagleSign, EHTv3 and EHTv4, HAETAE, HAWK, HuFu, Raccoon, SQUIRRELS |
| MPC-in-the-Head Signatures | 7 | CROSS, MIRA, MiRitH, MQOM, PERK, RYDE, SDitH |
| Multivariate Signatures | 11 | 3WISE, Biscuit, DME-Sign, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX |
| Symmetric-based Signatures | 4 | AIMer, Ascon-Sign, FAEST, SPHINCS-alpha |
| Other Signatures | 5 | ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Preon, Xifrat1-Sign.I |

https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures

# 2023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 | |

# 暗号技術調査ワーキンググループ（高機能暗号）活動報告

2023年　7月　26日

2022年度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 | | | |
|---|---|---|---|
| 委員 | 岩本　貢 | 委員 | 鈴木　幸太郎 |
| 委員 | 大原　一真 | 委員 | 花岡　悟一郎 |
| 委員 | 勝又　秀一 | 委員 | 外園　康智 |
| 委員 | 金岡　晃 | 委員 | 濱田　浩気 |
| 委員 | 川原　祐人 | 委員 | 山田　翔太 |
| 委員 | 国井　裕樹 | 委員 | 米山　一樹 |
| 委員 | 須賀　祐治 | 委員 | 渡邉　洋平 |

# 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
- 高機能暗号の技術／アプリケーションに関する現状調査
- 2023年4月に「CRYPTREC暗号技術ガイドライン（高機能暗号）」を公開

# 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の目次

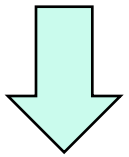


詳細技術を記載

アプリケーション・標準化関係を記載

# 第1章　はじめに

- サイバー空間、フィジカル空間が融合したSociety5.0の進展
- サービスの高度化
  - クラウドサービスの充実
  - 人工知能技術の進歩
  - コロナ禍に伴うオンライン業務、オンラインサービスの拡張



- 現状のサービスの改善、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

# 第2章　高機能暗号とその活用法

## 2.1　高機能暗号とは

一般的に合意されている定義が存在しないため、ガイドラインで扱う高機能暗号を定義した

**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」

# 第2章　高機能暗号とその活用法

## ■ ２．２　高機能暗号はどこに使えるか、その有用性

■ 高機能暗号毎に異なる特徴を有し、それぞれの優位性を持つ （以下例示）

- ランダムな暗号化鍵ではなく、良く知るメールアドレスや人名を暗号化鍵にできる
- 復号鍵の漏洩対策として、複数人の複合情報が集まらなければ元のデータを復号できない
- 暗号化したまま論理演算や算術演算が可能
- 複数の署名を集めて、一度に検証が可能
- 個人情報を秘匿し、その個人があるグループのメンバーに所属していることを証明可能
- 所有する秘密情報を公開することなく、その秘密情報を所持していることを証明可能
- データベースの管理者に対してであっても、データベースに保存したデータを秘匿可能

# 第2章　高機能暗号とその活用法

## 2.3　高機能暗号の種類と分類

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

| 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 |

# 第2章　高機能暗号とその活用法

## ２．４　高機能暗号の活用事例と標準化動向

- ２．４．１　守秘関連の活用事例と標準化動向
- ２．４．２　認証・署名関連の活用事例と標準化動向
- ２．４．３　その他の高機能暗号の活用事例と標準化動向
- ２．４．４　活用事例からみた高機能暗号の利用方法

■ 2.4.1~2.4.3節については、アルゴリズムからの視点で活用事例を紹介

■ 2.4.4節については、実用サービスからの視点でどのような高機能暗号をどのように使ったかを紹介

# 第3章　主な高機能暗号アルゴリズム

## ３．１　守秘関連のアルゴリズム

- 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

# 第3章　主な高機能暗号アルゴリズム

## 3．1　守秘関連のアルゴリズム例：準同型暗号

- 守秘関連の暗号の中で、注目度の高い暗号として準同型暗号が挙げられる
- 準同型暗号は暗号化した状態で、演算が可能であり、クラウドを演算に用いる際のサーバへのデータの秘匿等に利用が見込まれている

通常の計算
- クライアント　：　A，Bをサーバに
- サーバ（演算）　：　A＋B
- クライアント　：　A＋Bをサーバから受け取る

AもBも平文であり、サーバはすべての値を知る

準同型暗号による計算
- クライアント（暗号化）　：　Enc（A），Enc（B）をサーバに
- サーバ（演算）　：　C＝Enc（A＋B）
- クライアント（復号）　：　Cをサーバから受け取り
- 　　：　A＋B＝Dec（C）　により復号

AもBも暗号文でサーバに渡され、サーバは値を知ることが不可能

# 第3章　主な高機能暗号アルゴリズム

## ３．２　署名・認証関連のアルゴリズム

- 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

# 第3章　主な高機能暗号アルゴリズム

## ３．２　署名・認証関連のアルゴリズム例：しきい値署名

- しきい値署名は複数の署名者が署名を行うが、それぞれの署名は署名の一部であり、しきい値以上の数の署名を集めることにより、真の署名となり、検証が可能となる
- 暗号通貨などによる取引内容を複数の利用者が認めるケース等への利用が見込まれる

通常の署名――――署名者数と同じ数の検証鍵が必要

| | | |
|---|---|---|
| A、B、Cさんがそれぞれ署名 | ： | Sign_A, Sign_B, Sign_C |
| A、B、Cさんの署名をそれぞれ検証 | ： | Ver( Sign_A), Ver(Sign_B), Ver(Sign_C) |

しきい値署名（しきい値が2人の場合）――――検証鍵は一つ

| | | |
|---|---|---|
| A、B、Cさんがそれぞれ署名 | ： | Sign_A, Sign_B, Sign_C |
| しきい値の数の署名を収集、合成 | ： | Sign_AB （Sign_A, Sign_Bの合成） |
| 署名の検証 | ： | Ver（Sign_AB) |

# 第3章　主な高機能暗号アルゴリズム

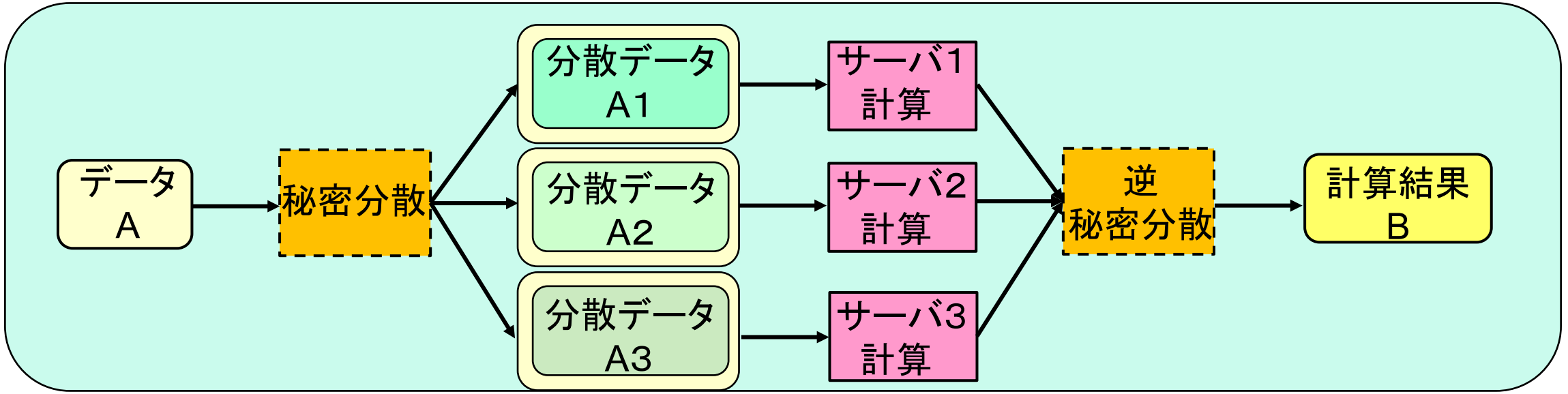
## ３．３　その他のアルゴリズム

- 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（PIR）
- Oblivious RAM

# 第3章　主な高機能暗号アルゴリズム

## 3．3　その他のアルゴリズム例：MPC―秘密分散ベース

- MPCは複数のサーバにより計算を行うが、第1ステップとして秘密分散を行い、分散されたデータに対してサーバで計算を行い、その結果を集めることで、真の結果を得る
- クラウドサーバを演算に用いる際のサーバへのデータの秘匿等に利用が見込まれている



# 第4章　おわりに

## 高機能暗号

### ■ 課題

- 研究開発は現在も進行している。アルゴリズムの進展だけでなく、安全性評価も進歩するため、今後の外部動向の注視が必要
- 高機能暗号の導入には専門的な知識が要求される。この知識を有する人材の確保が必要

### ■ 最後に

本ガイドラインが、用途に適した高機能暗号を選択するため、および、研究者、システム開発者、利用者にとっての指針となれば幸いである。