CRYPTREC
Cryptography Research and Evaluation Committees

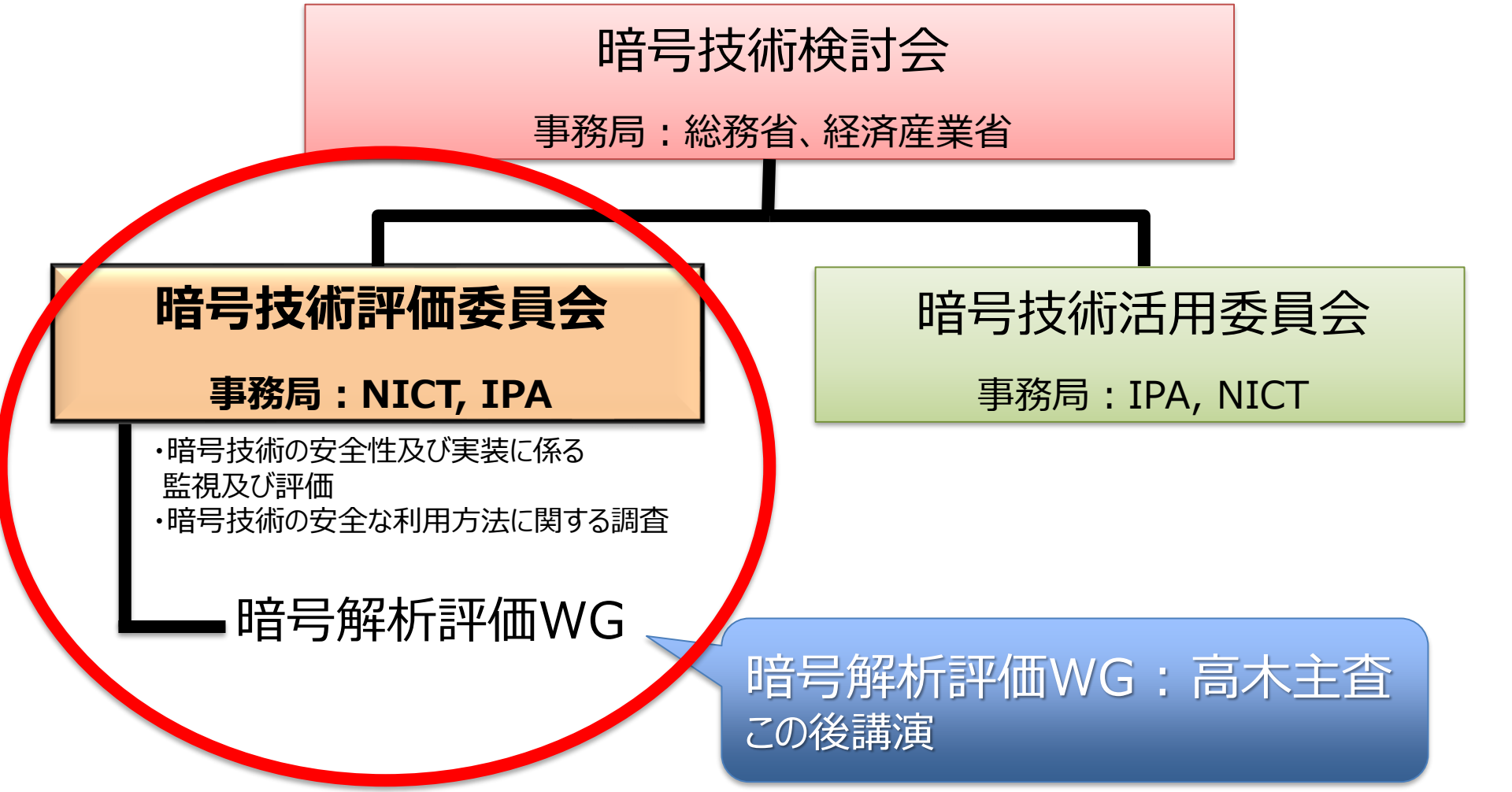
暗号技術評価委員会
活動報告

2019年7月12日

暗号技術評価委員会 委員長
（電気通信大学 教授）
太田 和夫

CRYPTREC
Cryptography Research and Evaluation Committees

2018年度 CRYPTREC 体制



CRYPTREC
Cryptography Research and Evaluation Committees

2018年度 暗号技術評価委員会 委員

委員長	太田　和夫	電気通信大学　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	金子　敏信	東京理科大学　教授
委員	高木　剛	東京大学　教授
委員	手塚　悟	慶應義塾大学　特任教授
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　ディビジョンマネージャー
委員	盛合　志帆	国立研究開発法人情報通信研究機構　研究室長
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

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。

CRYPTREC
Cryptography Research and Evaluation Committees

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
  - –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および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
  - –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

2018年度の活動概要

- 暗号技術の安全性及び実装に係る監視及び評価
  - **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および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
  - **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**

公開鍵暗号の歴史

RSA暗号　(素因数分解問題)

広く普及

楕円曲線暗号 (離散対数問題)

ペアリング暗号 (クラウド時代向けの暗号)

標準化、製品化

耐量子計算機暗号 (格子理論, 多変数多項式,符号理論)

完全準同型暗号, 多重線形性暗号, 難読化

研究段階

全てのフェーズの暗号技術を監視対象としている

CRYPTREC
Cryptography Research and Evaluation Committees

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」の更新

- 2006年：暗号技術調査WG(公開鍵暗号WG)
  [外部評価] 依頼先：T.Kleinjung氏
- **今年度：暗号技術調査WG(暗号解析評価WG)**
  再評価実施
  [外部評価] 依頼先　：T.Kleinjung 氏および A.K.Lenstra氏
  実施内容：計算量見積もりの主要部分の評価

素因数分解の困難性に関する計算量を再評価

CRYPTREC
Cryptography Research and Evaluation Committees

素因数分解の困難性に関する計算量の再評価結果

[1] Evaluation of Complexity of Mathematical Algorithms, T. Kleinjung, 2006
[2] Evaluation of complexity of the sieving step of the general number field sieve, T. Kleinjung and A. K. Lenstra, 2018

法パラメータのサイズ(ビット)	768	1024	1536	2048
2006年度 (※) 評価結果[1]		2.8×10^{6}	0.92×10^{12}	4.4×10^{16}
2018年度 評価結果[2]	561.99	1.52×10^{6}	0.92×10^{12}	12.8×10^{16}

(※) ふるい処理に関するパラメータ選択をより改善した場合

表: 篩処理時間の推測結果

単位
2006年度評価 : AMD Athlon 64 X2 4200+ 2.2 GHz ×年
2018年度評価 : Intel Xeon E5-2680 v3 2.5 GHz コア×年

今年度の評価結果 :

- より正確な推測結果を得ることができた
- 2006年度の評価結果と比較し、大幅なずれがないことが確認できた

➡ 評価レポートは、CRYPTREC ホームページに公開

危殆化の時期を予測する図の更新

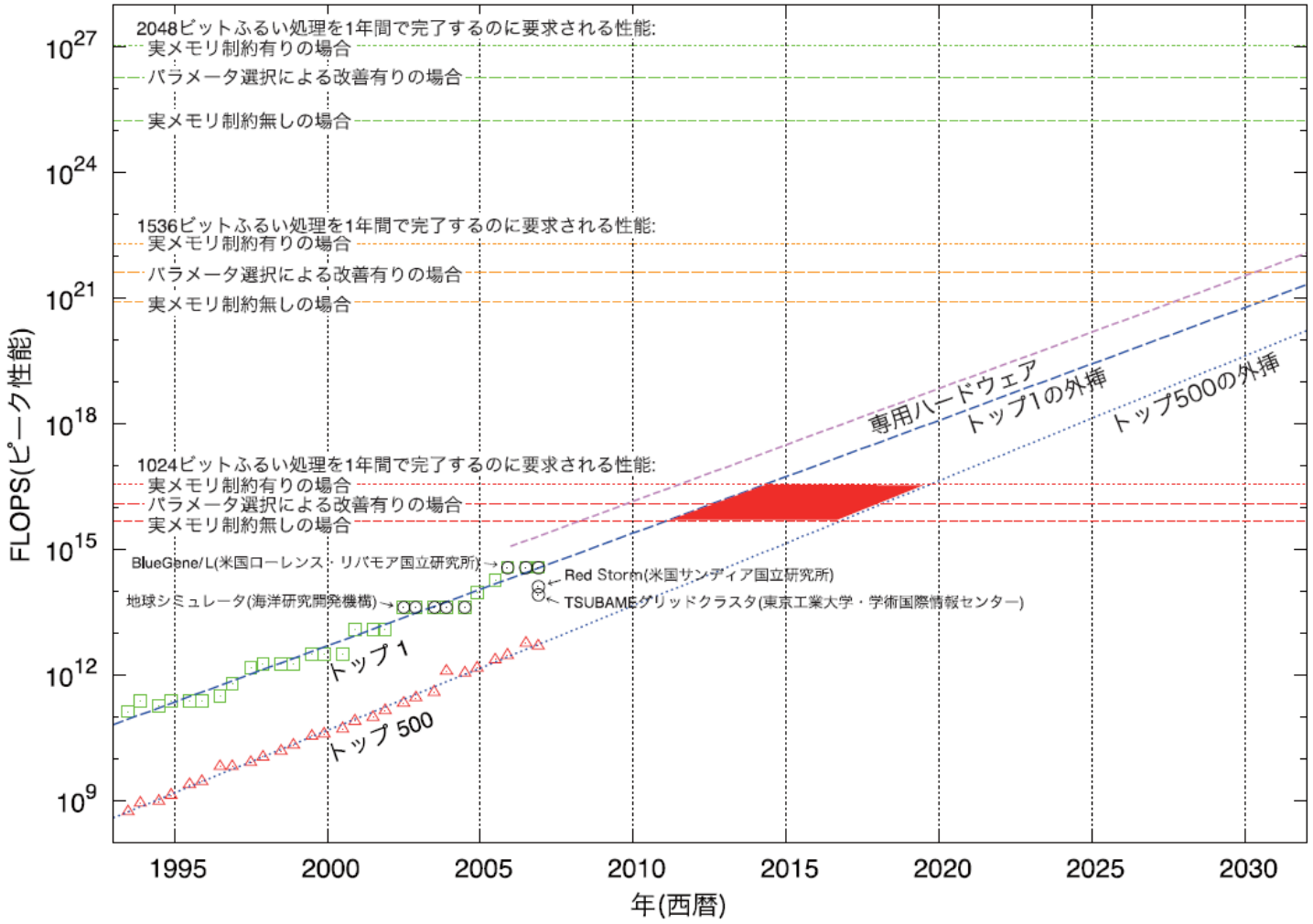
「素因数分解の困難性に関する計算量評価」

解読の脅威の尺度：スーパーコンピュータの性能の伸び

危殆化の時期を予測する図

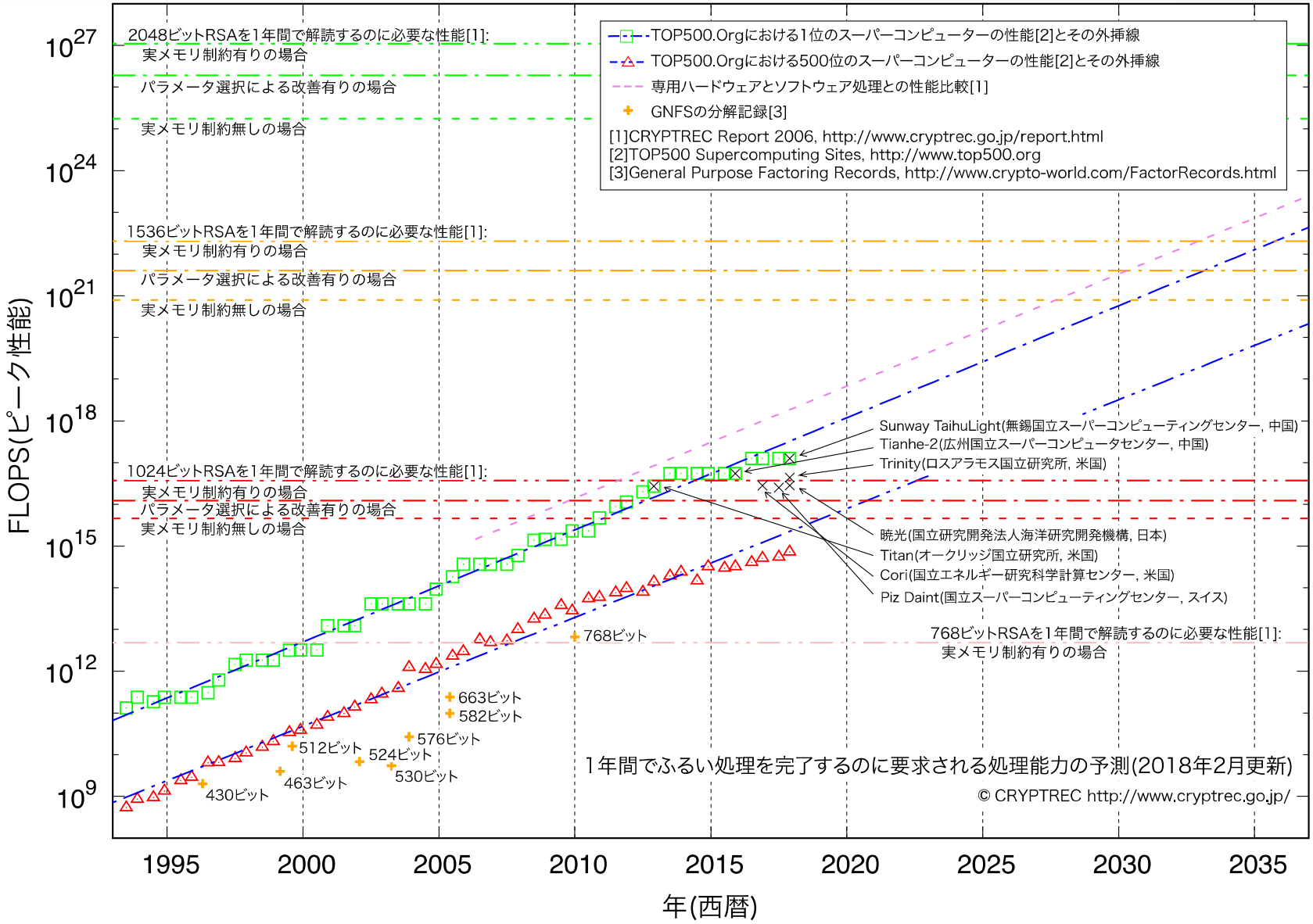
素因数分解の困難性に関する計算量評価(2006年版)

図 2.2　1 年間でふるい処理を完了するのに要求される処理性能の予測[14]



CRYPTREC
Cryptography Research and Evaluation Committees

素因数分解の困難性に関する計算量評価(2017年版)



危殆化の時期を予測する図の更新

「素因数分解の困難性に関する計算量評価」

解読の脅威の尺度：スーパーコンピュータの性能の伸び

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更新を検討

- 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
- 解読の要因となる脅威が多様化している
(多種デバイスや多種アーキテクチャが解読に利用できる可能性が出てきている)

どのように表現していくか暗号解析評価WGにて次年度継続検討

2018年度の活動概要

- 暗号技術の安全性及び実装に係る監視及び評価
  - **–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および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
  - **–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**

CRYPTREC 暗号リストの構成

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 随時

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

定期的 公募

随時 国際標準
(ISO・ITU-T等)

CRYPTREC 暗号リストの構成

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 随時

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

危殆化 随時

危殆化 随時

リストから削除

CRYPTREC 暗号リストの位置づけ

電子政府推奨暗号リスト

－CRYPTREC により安全性及び実装性能が確認された暗号技術について、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と判断され、当該技術の利用を推奨するもののリスト

推奨候補暗号リスト

－CRYPTREC により**安全性及び実装性能**が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト

運用監視暗号リスト

－実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない

CRYPTREC 暗号リストの構成

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 随時

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

安全性・実装性能評価等

定期的 公募

随時 国際標準 (ISO・ITU-T等)

CRYPTREC 暗号リストへの追加条件を満たしているか判断

標準化が進んでいる技術：
暗号利用モード(秘匿モード) XTS

暗号利用モード(秘匿モード) XTS

- 暗号利用モード (秘匿モード)の一つ
- ストレージデバイス上のデータの暗号化の規格として
  IEEE Standard 1619-2007, 1619-2018 で標準化されている
- NISTでも、2010年にNIST SP 800-38E として規定されている
- 大きな市場を持つ製品に搭載されるなどの実績がある。

  (例) Microsoft Windows 搭載の BitLocker
  macOS 搭載の FileVault 等のディスク暗号化機能
  など

推奨候補暗号リストへの新規暗号 (事務局選出) の追加候補とした

推奨候補暗号リストへの新規暗号(事務局選出)の追加

- 安全性評価

  従来、CRYPTREC 暗号リストへの追加に際しては、
  国内・国外 1 名ずつ有識者による外部評価を実施

  [評価対象] 暗号利用モード(秘匿モード)　XTS

  – 2010年：Phillip Rogaway 氏による安全性評価レポート
  – **今年度　：峯松 一彦氏に外部評価を依頼**

暗号利用モード (秘匿モード) XTS の安全性評価

下記3点の条件下で、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。

(条件1) 利用用途は IEEE および NIST SP 800-38E の規格に沿ったストレージやディスクの暗号化に限る。

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

(条件3)※ ~~同一の鍵を用いて暗号化する場合、2^{20} ブロックまでとする。~~

⇒ 同一の鍵を用いて暗号化する場合、データユニット毎の最大サイズは2^{20}ブロックとする

CRYPTRECシンポジウムにて警察大学校の岡野様にご指摘を頂き、上記の通り、修正させて頂きました。

推奨候補暗号リストへの追加に向けた XTS の評価

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 随時

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

完了

安全性 実装性能評価等

2019年度実装性能評価実施予定

定期的 公募

随時 国際標準 (ISO・ITU-T等)

CRYPTREC
Cryptography Research and Evaluation Committees

2018年度の活動概要

- 暗号技術の安全性及び実装に係る監視及び評価
  - **–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および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
  - **–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**

新技術などに関する調査及び評価

- 耐量子計算機暗号への対応や
  次期 CRYPTREC 暗号リストに向けた方針について議論を実施

- 暗号技術調査ワーキンググループ(暗号解析評価)を実施

耐量子計算機暗号への対応や次期 CRYPTREC 暗号リストに向けた方針にかかわる課題

CRYPTREC
Cryptography Research and Evaluation Committees

- 耐量子計算機暗号への対応
- 軽量認証暗号・軽量ハッシュ関数への対応
- 次期 CRYPTREC 暗号リストの策定方針

耐量子計算機暗号 (背景)

- 現在使われている RSA-2048 を破る
  大規模量子コンピュータが2030年頃に実現する
  可能性がある [NIST IR 8240]

現在使われている現代暗号の安全性が著しく低下する

大規模量子コンピュータが実現されたとしても安全な
耐量子計算機暗号 **PQC** (**P**ost-**Q**uantum **C**ryptography) の
研究が世界各国で進められている

CRYPTRECでの検討状況は暗号解析評価 WG にて紹介

耐量子計算機暗号への対応や次期 CRYPTREC 暗号リストに向けた方針にかかわる課題

CRYPTREC
Cryptography Research and Evaluation Committees

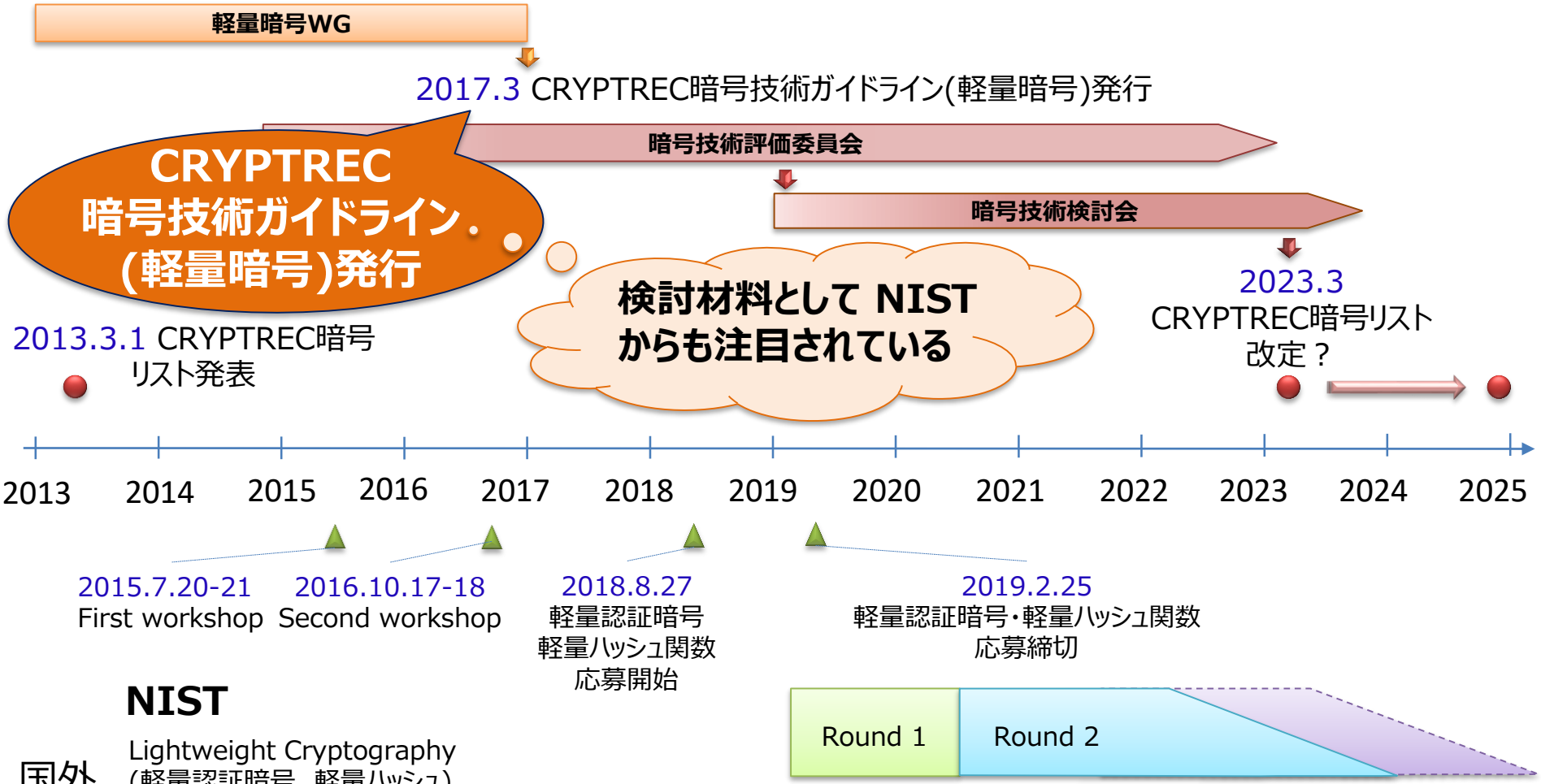
- 耐量子計算機暗号への対応
- 軽量認証暗号・軽量ハッシュ関数への対応
- 次期 CRYPTREC 暗号リストの策定方針

CRYPTRECにおける軽量暗号への取組み

国内

CRYPTREC

軽量暗号に関連する活動



国外

NIST

Lightweight Cryptography
(軽量認証暗号, 軽量ハッシュ)
標準化

Cryptrec (Cryptography Research and Evaluation Committees)

NIST による国際会議での招待講演資料から抜粋：軽量暗号ガイドラインが紹介されている

- Project to evaluate and monitor the security of cryptographic techniques used in Japanese e-Government systems.
- Publishes three lists
  - e-Government recommended cipher list: approved in terms of security and implementation aspects as well as current and future market development.
  - Candidate recommended cipher list: approved in terms of security and implementation aspects.
  - Monitored ciphers list: not recommended for use, because of high risk of compromise, allowed to use only for interoperability with legacy systems.
- In March'17, published a guideline on lightweight cryptography.

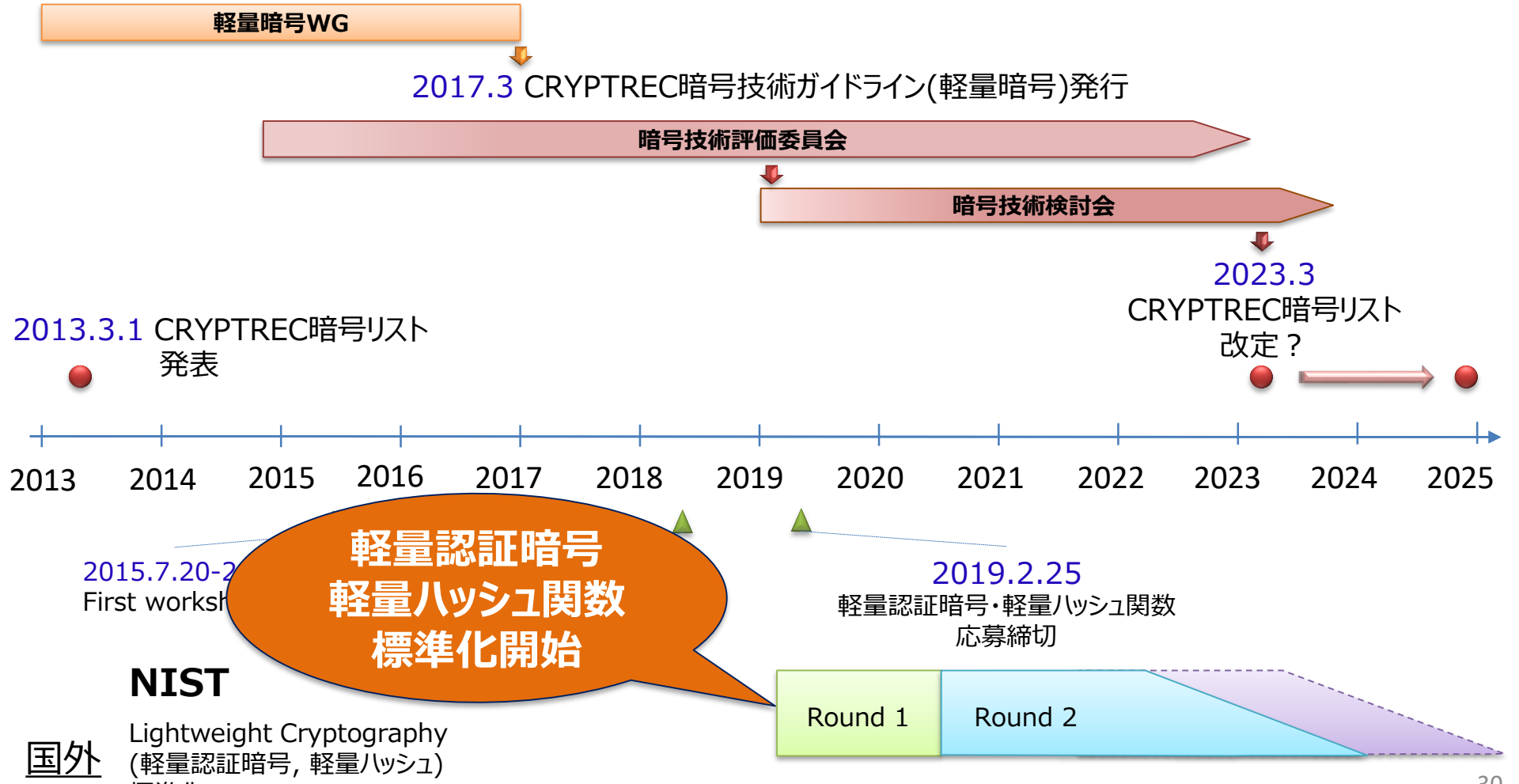
出典
ApplicationsandStandardizationofLightweightCryptography
MeltemS ̈onmezTuran(NIST)
SACSummerSchool(S3),2018,Calgary,Canada

米国国立標準技術研究所(NIST)の軽量暗号に関する取組み

国内

CRYPTREC

軽量暗号に関連する活動



国外

NIST

Lightweight Cryptography
(軽量認証暗号, 軽量ハッシュ)
標準化

CRYPTREC 暗号リスト改定と NIST 標準化スケジュール

国内

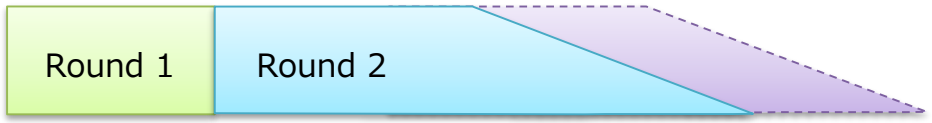
CRYPTREC

軽量暗号に関連する活動

国外

NIST

Lightweight Cryptography
(軽量認証暗号, 軽量ハッシュ)
標準化



軽量暗号の CRYPTREC 暗号リストでの位置づけ

- 軽量暗号の現状
  - セキュリティマージンを小さくせざるをえない
  - CRYPTREC暗号リストの枠組みにそぐわない
- 64ビットブロック暗号
  - 現在の電子政府推奨暗号リストには入れない
  - IoT機器などでの需要が大きい

➡ **安全性に対する基本的な考え方の見直しが必要**

➡ **次期 CRYPTREC 暗号リスト改定に向けて検討**

耐量子計算機暗号への対応や次期 CRYPTREC 暗号リストに向けた方針にかかわる課題

CRYPTREC
Cryptography Research and Evaluation Committees

- 耐量子計算機暗号への対応
- 軽量認証暗号・軽量ハッシュ関数への対応
- 次期 CRYPTREC 暗号リストの策定方針

過去の経験を振り返る

CRYPTREC Cryptography Research and Evaluation Committees

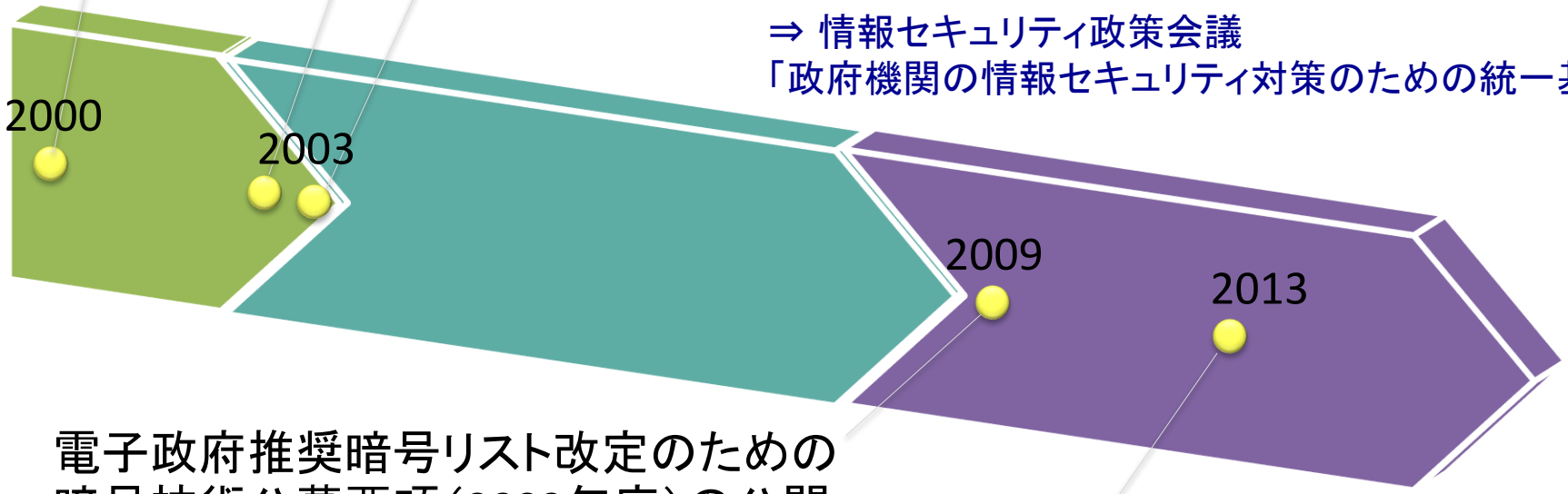
CRYPTREC 暗号リスト策定および改定の流れ (2003 年および 2013 年)

CRYPTREC発足, 暗号技術の公募

「電子政府推奨暗号リスト」の公表

「各府省の情報システム調達における暗号の利用方針」
各府省が情報システムの構築にあ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

⇒ 情報セキュリティ政策会議
「政府機関の情報セキュリティ対策のための統一基準」



電子政府推奨暗号リスト改定のための
暗号技術公募要項（2009年度）の公開

「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）」の公表

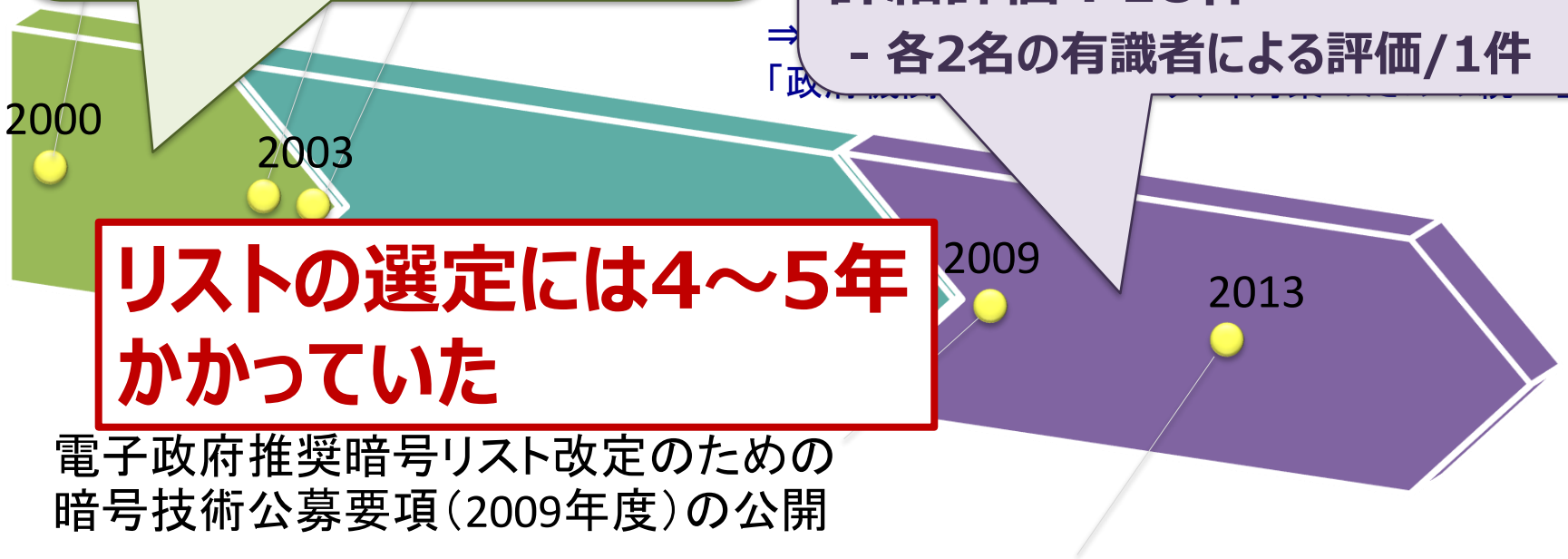
歴史から学ぶ

CRYPTREC Cryptography Research and Evaluation Committees

CRYPTREC 暗号リスト策定および改定の流れ (2003 年および 2013 年)

応募アルゴリズム：48件
スクリーニング評価：48件
詳細評価：35件
- 各2名の有識者による評価/1件

応募アルゴリズム：6件
事務局選出アルゴリズム：12件
詳細評価：18件
- 各2名の有識者による評価/1件



リストの選定には4～5年かかっていた

電子政府推奨暗号リスト改定のための暗号技術公募要項（2009年度）の公開

「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）」の公表

耐量子計算機暗号への対応や次期 CRYPTREC 暗号リストに向けた方針にかかわる課題

CRYPTREC
Cryptography Research and Evaluation Committees

- 耐量子計算機暗号への対応
- 軽量認証暗号・軽量ハッシュ関数への対応
- 次期 CRYPTREC 暗号リストの策定方針

➡ **2019年度タスクフォースにて継続検討**

新技術などに関する調査及び評価

- 耐量子計算機暗号への対応や
  次期 CRYPTREC暗号リストに向けた方針について議論を実施

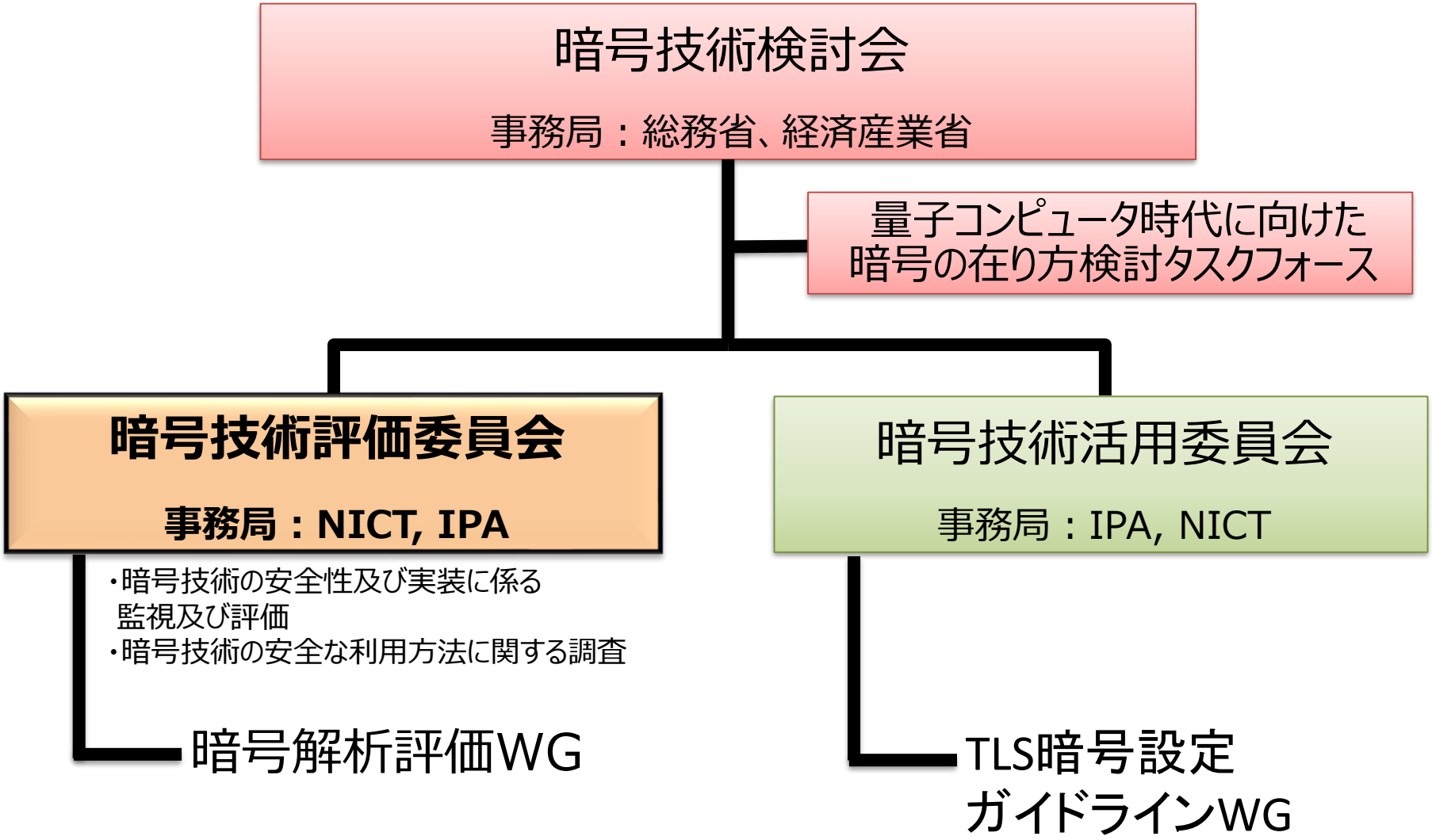
- 暗号技術調査ワーキンググループ(暗号解析評価)を実施

暗号解析評価WG：高木主査
この後講演

2019年度 暗号技術評価委員会

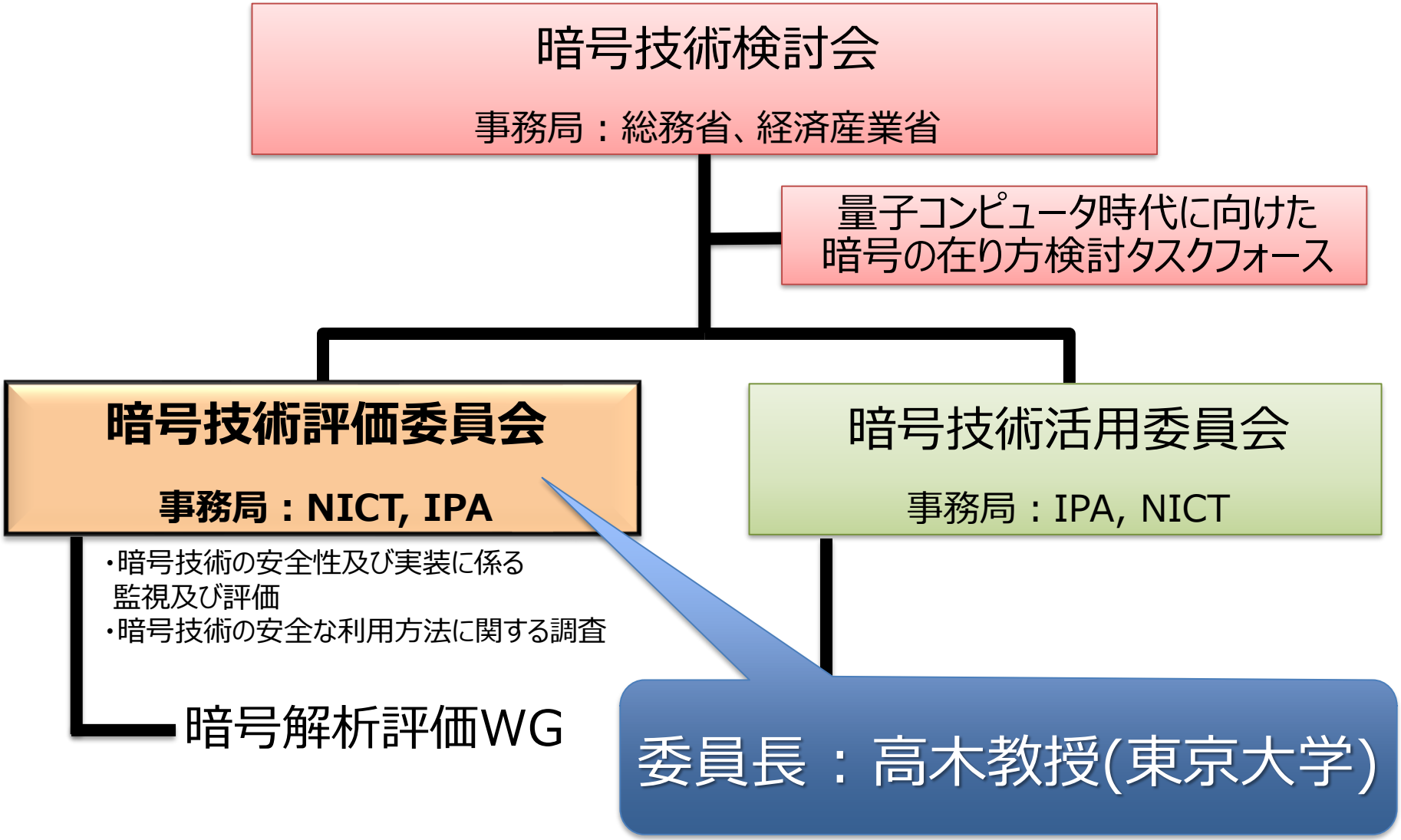
CRYPTREC
Cryptography Research and Evaluation Committees

2019年度 CRYPTREC 体制



CRYPTREC
Cryptography Research and Evaluation Committees

2019年度 CRYPTREC 体制



CRYPTREC
Cryptography Research and Evaluation Committees

2019年度 暗号技術評価委員会 委員

2019年7月12日現在

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　特任教授
委員	藤崎　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　ディビジョンマネージャー
委員	盛合　志帆	国立研究開発法人情報通信研究機構 研究室長
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

Fin

CRYPTREC Cryptography Research and Evaluation Committees

NIST の軽量暗号に関する今後のスケジュール

対象技術：軽量認証暗号，軽量ハッシュ関数
評価対象：安全性，ソフトウェア・ハードウェアパフォーマンス
選定期間：3～4 年を予定

2019年4月18日　First Round ：57 件応募があり，56 件通過
(日本人が著者に含まれる提案 16 件)

約 1年の評価期間を設ける

2019年9月　Second Round 公開予定

2019年11月4-6日　第 3 回 Lightweight Cryptographic Workshop 開催

CRYPTREC
Cryptography Research and Evaluation Committees

暗号解析評価WG 活動報告

2019年7月12日

暗号解析評価WG 主査
（東京大学 教授）
高木 剛

2018年度 CRYPTREC 体制

暗号技術検討会

事務局：総務省、経済産業省

暗号技術評価委員会

事務局：NICT, IPA

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

暗号解析評価WG

暗号技術活用委員会

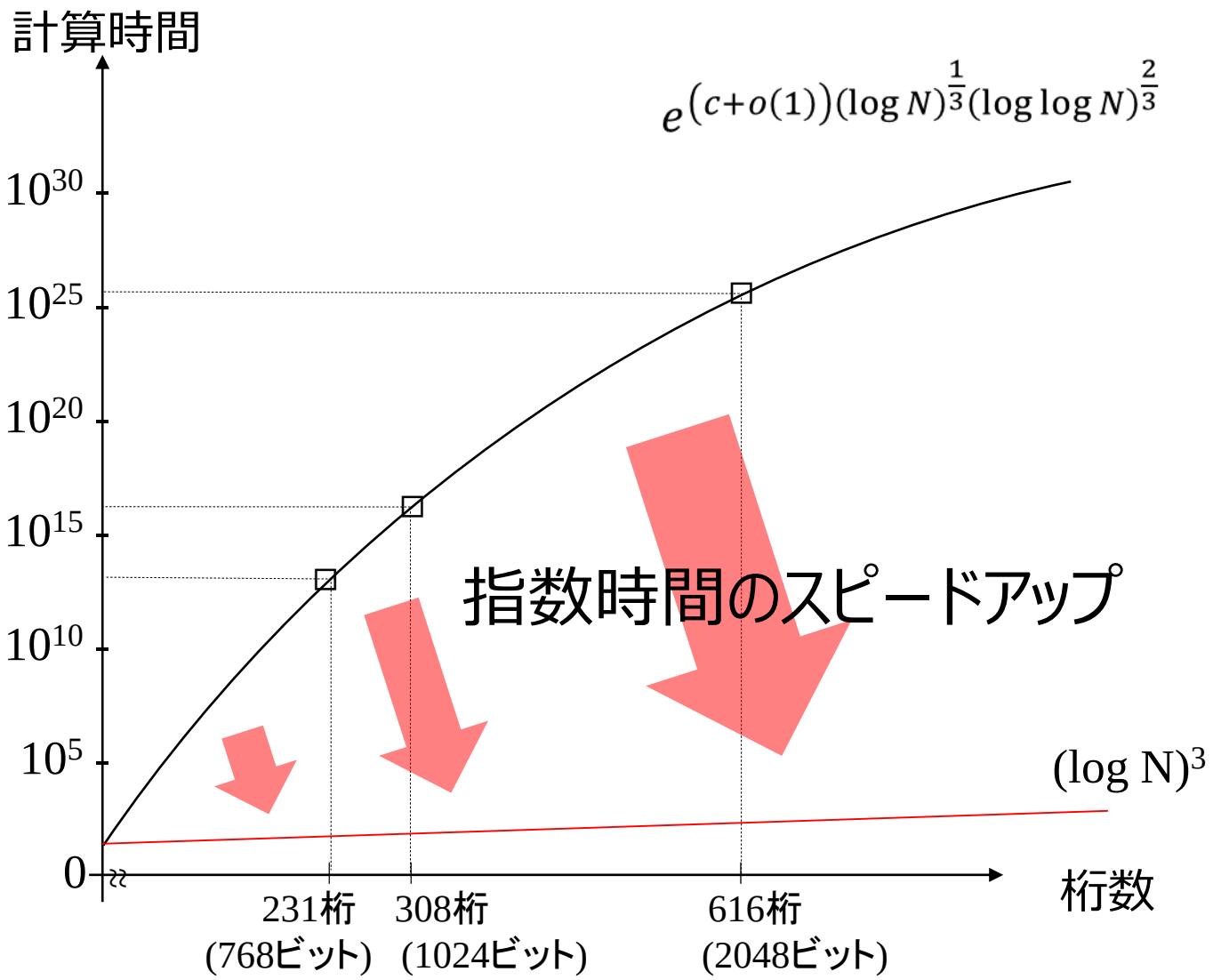
事務局：IPA, NICT

「耐量子計算機暗号の研究動向調査」を実施
（2017～2018年度）

暗号技術に及ぼす量子計算機の影響

- Shor のアルゴリズムと大規模量子コンピュータを利用することで、整数の素因数分解と離散対数問題を多項式時間で解くことができる
  ⇒ RSA 暗号と楕円曲線暗号の安全性が大きく低下

暗号技術に及ぼす量子計算機の影響



暗号技術に及ぼす量子計算機の影響

- Shor のアルゴリズムと大規模量子コンピュータを利用することで、整数の素因数分解と離散対数問題を多項式時間で解くことができる

  ⇒ RSA 暗号と楕円曲線暗号の安全性が大きく低下

- 2000-bit RSA を破る大規模量子コンピュータが2030年頃に実現する可能性がある [NISTIR 8105]

- 大規模量子コンピュータが実現されたとしても安全な耐量子計算機暗号 **PQC** (**P**ost-**Q**uantum **C**ryptography) の研究が世界各国で進められている

耐量子計算機暗号 (PQC) の標準化をめぐる国内外の動き

PQC の標準化をめぐる国内外の動き

国内

CRYPTREC

PQC に関連する活動

暗号解析評価WG

2015.3
「格子問題等の困難性に関する調査」発行

2019.3 PQC 技術報告書発行

暗号技術評価委員会

CRYPTRECにおける
PQC対応 検討開始

暗号技術検討会

2013.3.1
CRYPTREC 暗号リスト発表

2023.3
CRYPTREC 暗号リスト
改定？

2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025

NIST

PQC標準化

2016.4.28
NISTIR 8105
リリース

2016.12.20
募集要項
発表

2017.11.30
応募締切

2019.1.30
Round 2 候補発表

最速スケジュール

PQC のDraft Standards 公開
(2022～2024 年)

2020～2021 年に開始または
Round 3 なしで選定完了

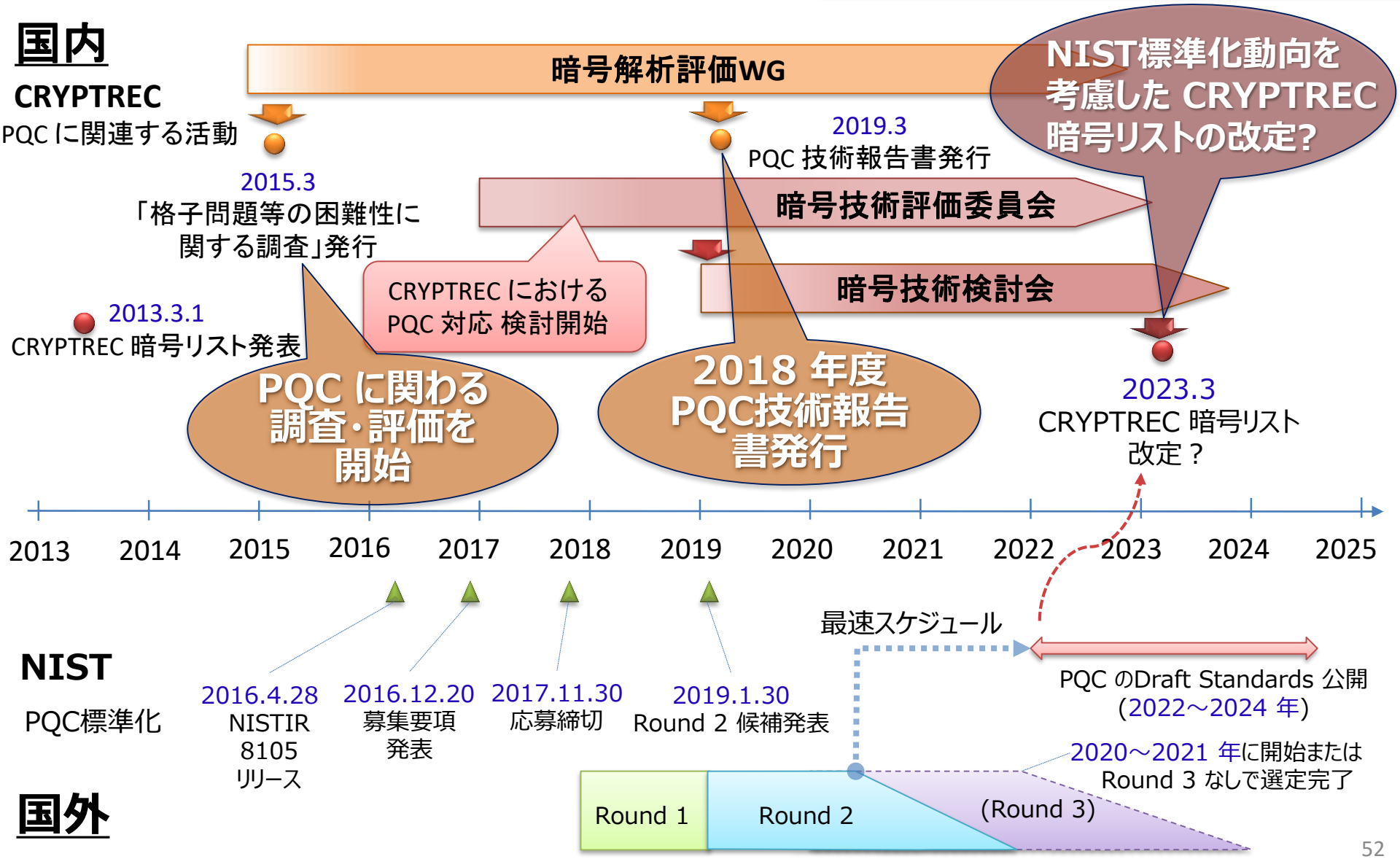
Round 1 Round 2 (Round 3)

国外

NIST第2ラウンドの26方式

格子に基づく暗号	
	鍵交換・暗号化 (9方式): CRYSTALS-KYBER, Frodo-KEM, LAC, NewHope, NTRU, NTRU Prime, Round5, SABER, Three Bears ディジタル署名 (3方式): CRYSTALS-DILITHIUM, FALCON, qTESLA
符号に基づく暗号	
	鍵交換・暗号化 (7方式): BIKE, Classic McEliece, HQC, ROLLO, LEDAenc, NTS-KEM, RQC
多変数多項式に基づく暗号	
	ディジタル署名 (4方式): GeMSS, LUOV, MQDSS, Rainbow
ハッシュ関数に基づく署名	
	ディジタル署名 (1方式): SPHINCS+
同種写像に基づく暗号	
	鍵交換・暗号化 (1方式)：SIKE
その他	
	ディジタル署名 (1方式)： Picnic

PQC の標準化をめぐる国内外の動き



耐量子計算機暗号の研究動向調査（2017～2018 年度）

2018年度 暗号解析評価WG 委員

主査	高木　剛	東京大学　教授
委員	青木 和麻呂	日本電信電話株式会社　グループリーダ
委員	草川　恵太	日本電信電話株式会社　研究主任
委員	國廣　昇	東京大学　准教授
委員	下山　武司	株式会社富士通研究所　主管研究員
委員	高島　克幸	三菱電機株式会社　主管技師長
委員	安田　貴徳	岡山理科大学　准教授
委員	安田　雅哉	九州大学　准教授

公開鍵暗号と数学と量子計算機

**量子計算機と
Shor のアルゴリズムで
効率よく解くことができる**

- 現在使用されている公開鍵暗号
  - RSA 暗号: 整数の素因数分解
  - 楕円曲線暗号: 楕円曲線上の離散対数問題

- PQC として期待される公開鍵暗号
  - 格子に基づく暗号: 格子問題（LWE 問題等）
  - 符号に基づく暗号: LPN 問題
  - 多変数多項式に基づく暗号: MP 問題, IP 問題
  - 同種写像に基づく暗号: 同種写像問題

耐量子計算機暗号の研究動向調査報告書

PQC の代表的な四方式について三つの機能を中心に調査し，
結果を報告書にまとめた。

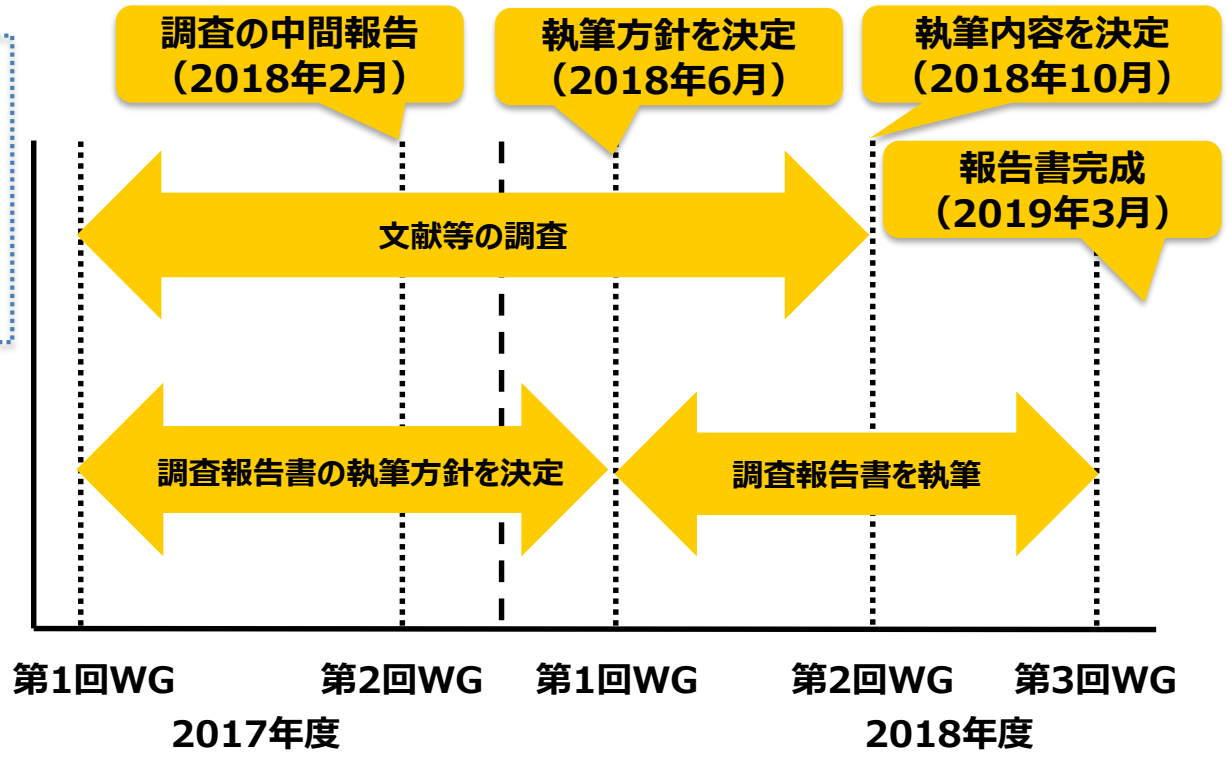
(2019.4.5 公開済み) https://www.cryptrec.go.jp/topics/cryptrec_20190405_tr_2001_2018.html

四つの暗号方式

- 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

三つの機能

- 暗号
- 署名
- 鍵交換



2019 年度 暗号解析評価 WG の紹介

2019年度 CRYPTREC 体制

暗号技術検討会

事務局：総務省、経済産業省

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

暗号技術評価委員会

事務局：NICT, IPA

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

暗号技術活用委員会

事務局：IPA, NICT

暗号解析評価WG

主査：國廣教授(筑波大学)

CRYPTREC
Cryptography Research and Evaluation Committees

2019年度 暗号解析評価ワーキンググループ

2019年7月12日現在

主査	國廣　昇	筑波大学　教授
委員	青木 和麻呂	日本電信電話株式会社　グループリーダ
委員	草川　恵太	日本電信電話株式会社　研究主任
委員	桑門　秀典	関西大学　教授
委員	下山　武司	株式会社富士通研究所　主管研究員
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　主幹研究員
委員	安田　貴徳	岡山理科大学　准教授
委員	安田　雅哉	九州大学　准教授

Fin