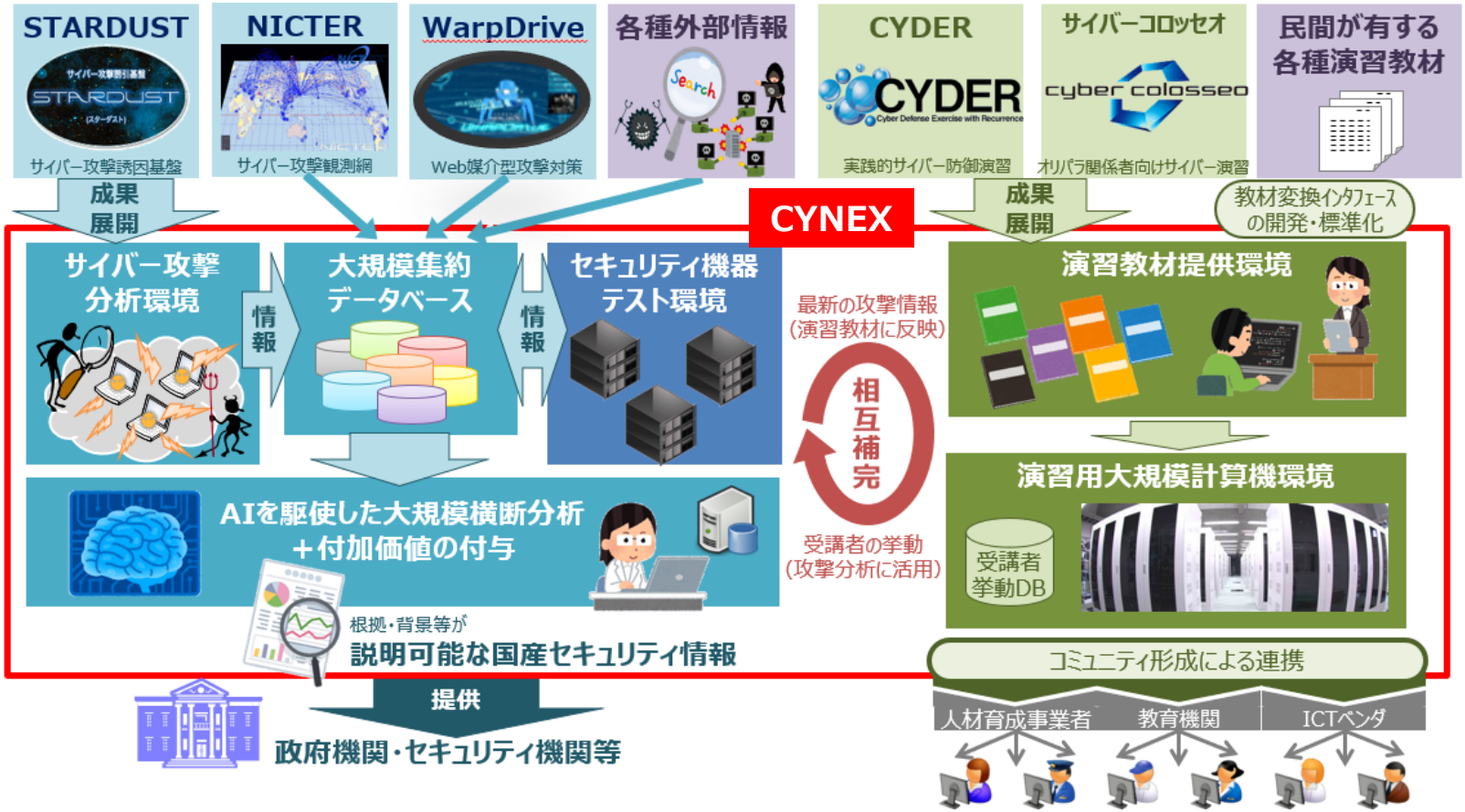
資料２

総務省における研究開発関連の取組

令和４年９月
総務省
サイバーセキュリティ統括官室

サイバーセキュリティ統合知的・人材育成基盤の構築

● サイバーセキュリティ情報を国内において収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤（CYNEX）を国立研究開発法人情報通信研究機構（NICT）に構築し、産学の結節点として開放することで、我が国全体のサイバーセキュリティ対応能力を強化。



次のとおり活用可能な基盤をNICTに構築。

➢ **国産セキュリティ情報の収集・蓄積・分析・提供**
幅広くサイバーセキュリティ情報を収集・蓄積し、AIを駆使して横断的に分析することで、高信頼で即時的なセキュリティ情報を生成し、政府・セキュリティ機関等に提供。

➢ **セキュリティ機器テスト環境**
国産のセキュリティ機器・サービスの開発を推進するため、最新のサイバー攻撃情報を活用し、その対応状況をセキュリティ事業者がテストできる環境を提供。

➢ **高度解析人材の育成**
収集したセキュリティ情報を活用し高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成。

➢ **人材育成のための基盤提供**
NICTが有する人材育成に関する環境・知見を民間・教育機関等に開放し、自立的な人材育成を推進。

（事業主体）　国立研究開発法人情報通信研究機構（NICT）
（事業スキーム）　補助事業
（補助対象）　機器購入費、環境構築費、運営費
（補助率）　定額補助
（計画年度）　令和３年度～令和７年度

暗号技術に係る取組み（CRYPTRECの概要）

- **CRYPTREC**（Cryptography Research and Evaluation Committees）は、**電子政府推奨暗号**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。
- 安全性・実装性能等が確認された暗号技術について、CRYPTREC暗号リスト（電子政府推奨暗号リスト）として平成15年2月に策定。平成25年3月に改定し、現在、再改定の検討中（令和4年度末目途）。

CRYPTRECの体制

デジタル庁統括官、総務省サイバーセキュリティ統括官及び
経済産業省商務情報政策局長の研究会として開催

暗号技術検討会
座長：松本 勉　横浜国立大学教授
（事務局：デジタル庁、総務省、経済産業省）

- CRYPTREC暗号の安全性及び信頼性確保のための調査・検討
- CRYPTREC暗号リストの改定に関する調査・検討
- 暗号技術の普及による情報セキュリティ対策の推進の検討

2019年度から設置
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
委員長：高木 剛　東京大学大学院教授
（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
- 新技術等に係る調査及び評価
- 暗号技術の安全な利用方法に関する調査

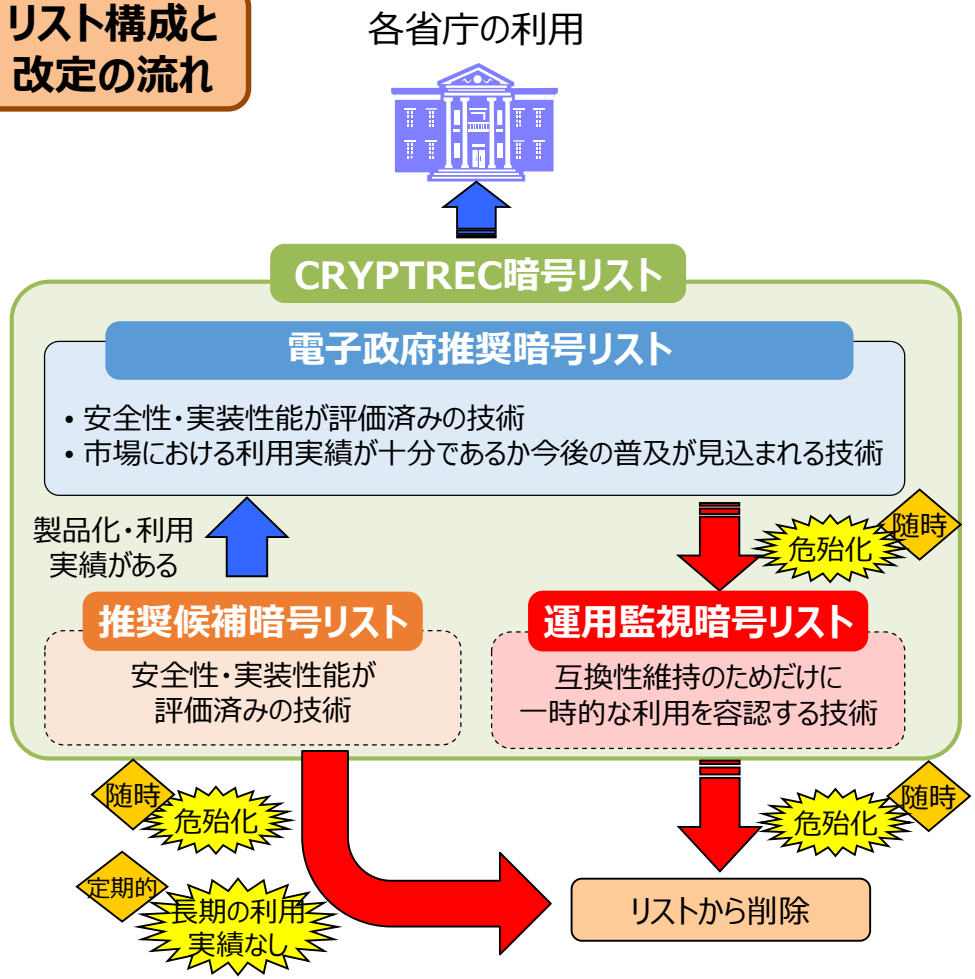
2021年度から設置
暗号技術調査WG(耐量子計算機暗号)
暗号技術調査WG(高機能暗号)

暗号技術活用委員会
委員長：松本 勉　横浜国立大学教授
（事務局：IPA、NICT）

- 暗号の普及促進・セキュリティ産業の競争力強化に係る検討
- 暗号技術の利用状況に係る調査及び必要な対策の検討等
- 暗号政策の中長期的視点からの取組の検討

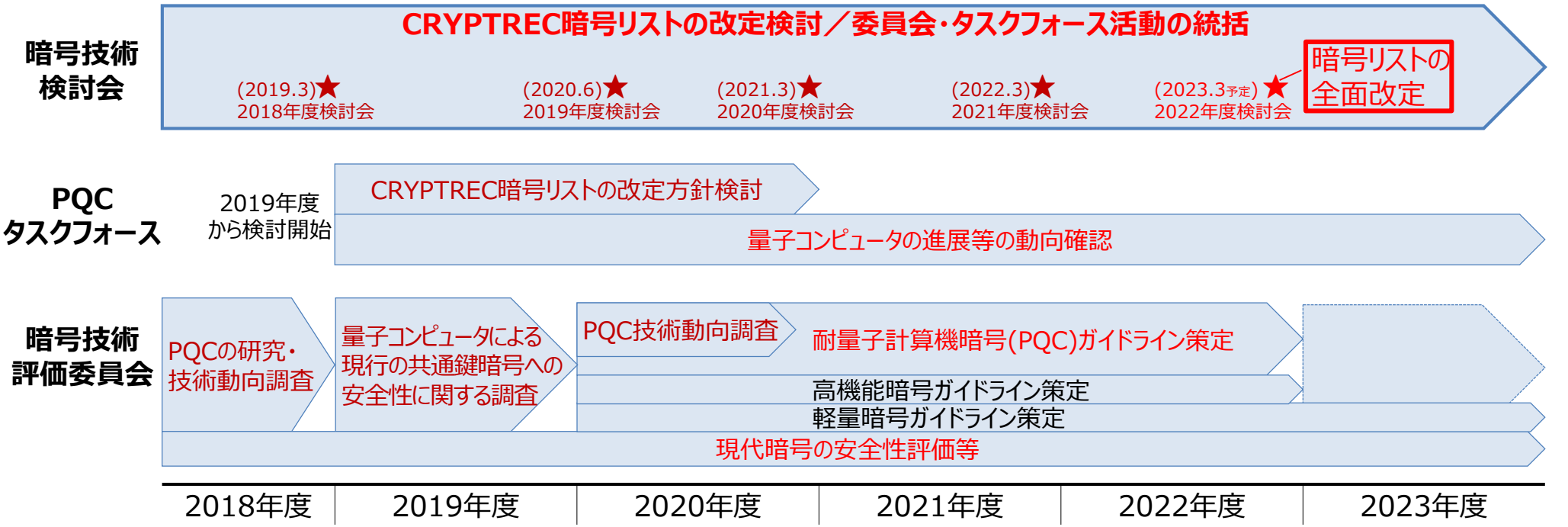
2021年度から設置
暗号鍵管理ガイダンスWG

リスト構成と改定の流れ



暗号技術に係る取組み（CRYPTRECの今後のスケジュール）

- 2023年を目途とした**CRYPTREC暗号リストの改定**検討を行っているほか、**耐量子計算機暗号(PQC)・高機能暗号・軽量暗号に関するガイドライン**の策定等の検討を行っている。



暗号技術に係る取組み（安全な無線通信サービスのための新世代暗号技術に関する研究開発）

5G等の高度化において、大規模量子コンピュータ等に解読されないよう、①LTEと同等の安全性を確保しつつ、超高速・大容量に対応した共通鍵暗号方式、②5G等の特性を損なわないよう、5G等のユースケースに応じた耐量子計算機暗号（PQC）への機能付加技術等を確立することで、無線通信リソースの効率的な利用環境を提供することにより、無線リソースのひっ迫を抑止し電波の有効利用を図る。

【背景・課題】

・大規模量子コンピュータ等が実用化されると、共通鍵暗号方式においては、LTEと同等の安全性を確保するためには鍵長を増加する必要があるが、スマートフォン等の限られた情報処理能力の中で5G等が求める高速・大容量に対応した暗号方式の設計が課題である。

・また、公開鍵暗号方式においては、高速な解読が可能となるため、PQCへの移行が必要である。今後、複数の暗号方式が採用される予定であるが、5G等のユースケースに応じて最適化し、スマートフォン等の計算資源や通信量を抑えるようにPQCへの機能付加等が必要である。

【実施内容】

大規模量子コンピュータ等に解読されないよう、①LTEと同等の安全性を確保するために鍵長を倍にしつつ、超高速・大容量に対応できる共通鍵暗号方式、②5G等のユースケースに応じ、通信データ量を抑え、PQCへの機能付加技術等を確立し、無線通信の効率的な利用環境を提供することにより、電波の有効利用を図る。

目標

超高速・大容量に対応する共通鍵暗号方式及びPQCへの機能付加技術等を令和6年までに開発するとともに、ISOや3GPP等の標準化団体に提案し、標準化策定に寄与することを目指す。

対象周波数帯

5G等のバンド：3.6GHz～4.6GHz、27.0GHz～29.5GHz、100GHz超の高い周波数帯

実施期間

令和3年度～令和6年度 （4か年）