2021年12年6日（月）

資料２

量子セキュリティ分野の動向と展望

国立研究開発法人 **情報通信研究機構**

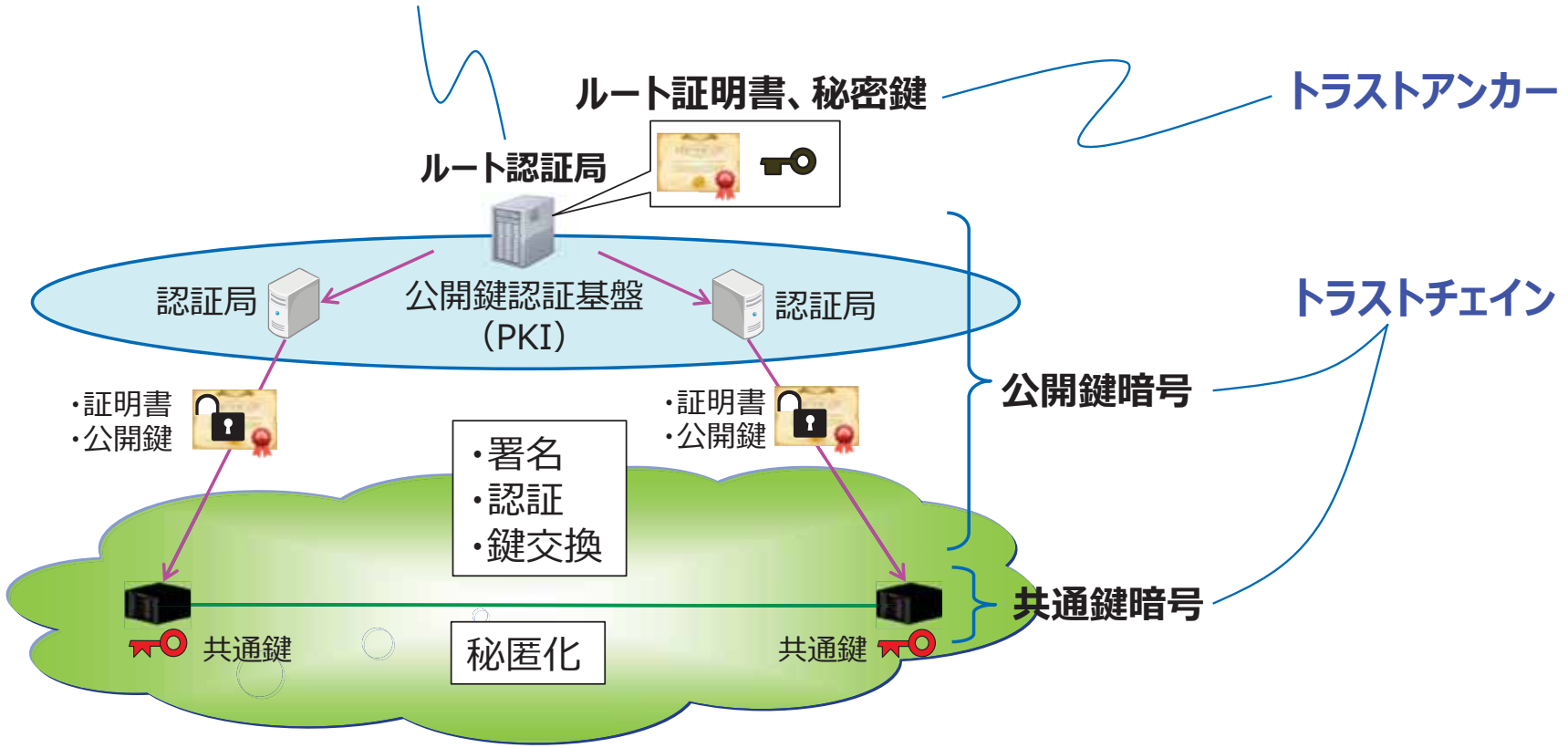
量子ICT協創センター

研究センター長 佐々木　雅英

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

現在の暗号基盤

国家機関や信頼のある企業が厳重に管理・運用



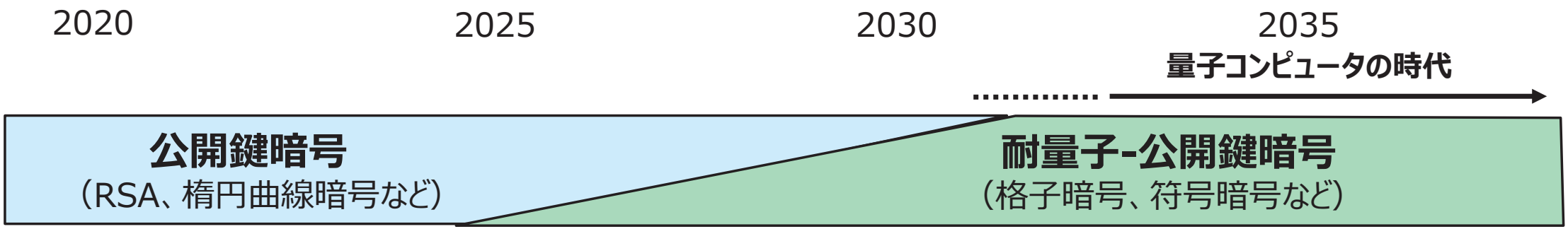
量子コンピュータが実現すると
現在使われている公開鍵暗号（RSA暗号、楕円曲線暗号）が解読される

	暗号技術	現在のコンピュータでの強度 [bits]	量子コンピュータでの強度 [bits]	解読に使われる量子アルゴリズム
公開鍵暗号	RSA-2048	112	0	ショアのアルゴリズム Shor's algorithm
	RSA-3072	128		
	DSA-2048	112		
	DSA-3072	128		
	ECC-256	128		
	ECC-521	256		
共通鍵暗号	AES-128	128	64	グローバーのアルゴリズム Grover's algorithm
	AES-256	256	128	

量子コンピュータでも解読困難と期待される

耐量子-公開鍵暗号への移行準備が各国でスタート

その移行は、かつてない規模で、2025年頃から本格化



暗号インフラ移行において認識すべき点

- 理論上、破られることが示された時点で暗号インフラの移行準備は始まる
- 暗号解読できる量子コンピュータがいつ実現するかは問題ではない
- これまで、暗号が実際に破られる前に、方式の移行が行われてきた

  （と考えられている。解読されていたとしても公表されるのはだいたい50年後）
- 重要なのは暗号インフラの移行プランが国際標準化機関から示されたこと
- 問題は、暗号インフラの移行をビジネスチャンスと捉えられるかどうか
- 日本は大きく出遅れた

  ・それは、日本が長年、平和国家であったことの証であり、誇るべき点
  ・しかし、サイバー空間では、どの国も戦争状態に突入 ⇒『状況は変わった』
  ・暗号インフラのトラストアンカーが万が一瓦解すると、
  影響は即座に広範囲に伝搬し、デジタルシステムは即死する

我が国のこれまでの問題点

・暗号技術のビジネス化、普及には標準化・認定制度が必須
・暗号の標準化や認定制度では、これまで欧米が先行。
　競争力のある製品も欧米企業から産み出されている状況。
・**日本は標準化、ビジネス化で常に欧米の後塵を拝してきた**

今後の方向性

・量子暗号では、日本が技術性能、アプリケーション、標準化で世界をリード
・量子暗号と現代暗号を統合しながら、量子セキュリティ分野の開拓を先導

量子セキュリティ x 量子コンピュータ ⇒ 量子セキュアクラウド

Beyond 5Gなど次世代通信インフラ上に統合

量子セキュアクラウド

量子時代のクラウドサービスと暗号基盤を提供

次世代コンピューティング基盤

- 量子・古典ハイブリッドソルバー

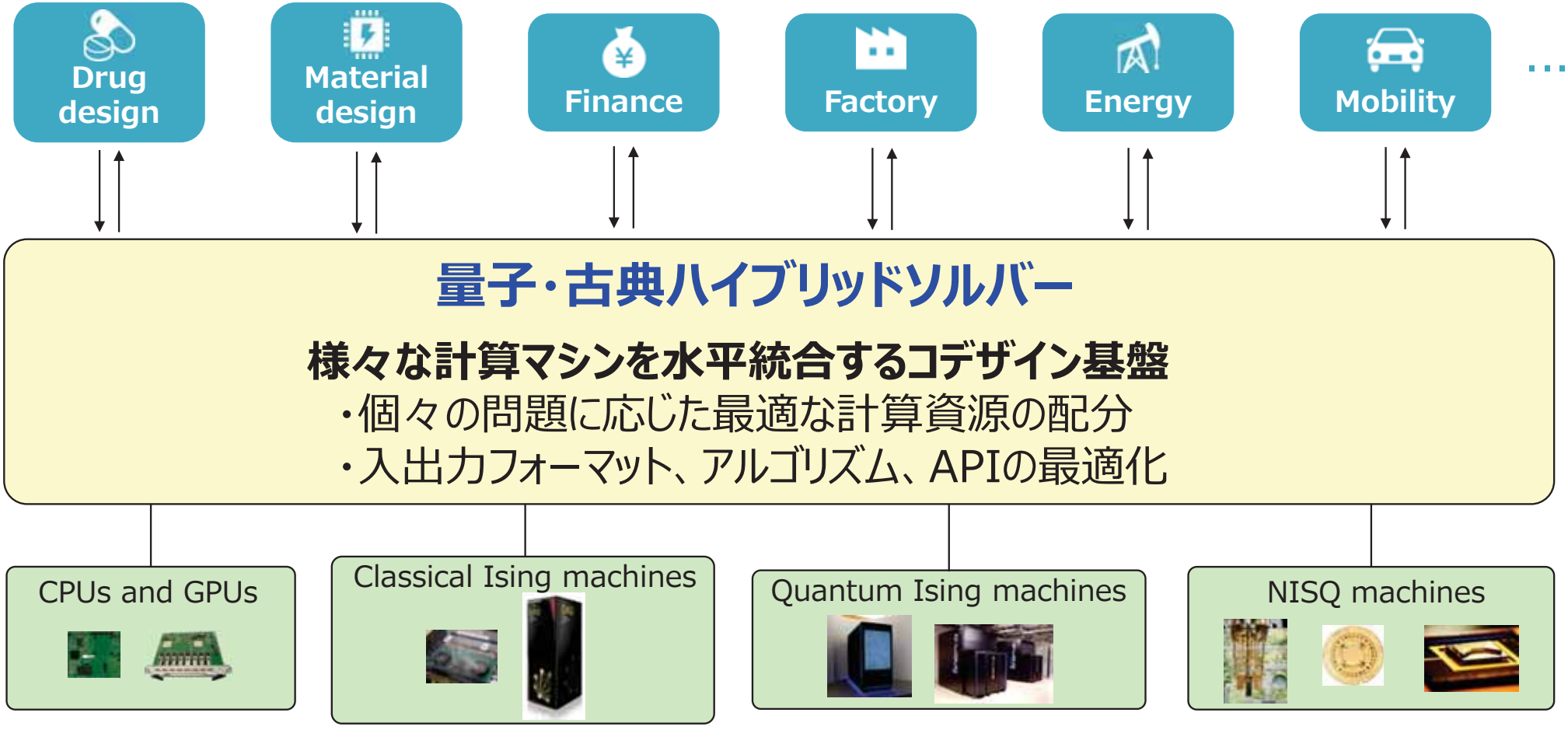
X

超長期セキュリティを保証する次世代暗号基盤

- 耐量子計算機-暗号
- 量子暗号
- 秘密分散

次世代コンピューティング基盤

・各領域ごとにAPIを垂直統合し最適化、普及を加速、人材育成プログラムとも連携
・ユーザ側に若手人材を派遣、コンテスト等を通じ問題の定式化・プログラミング ⇒ ユースケースを拡大

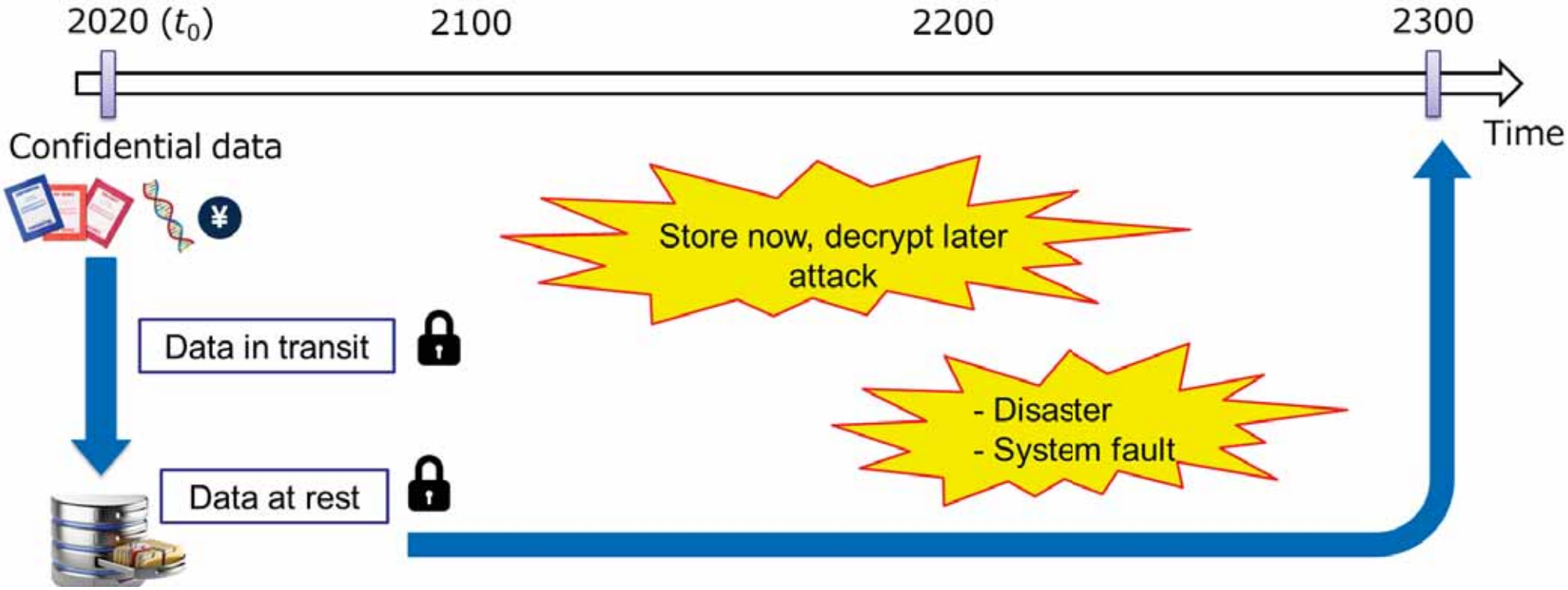


超長期セキュリティの必要性

ビジネス価値の高いデータや利用者に個別最適化された情報などが
大量に生み出され、クラウド上に**ほぼ永遠に保管され続ける**時代が到来

超長期セキュリティとは

- No information leak of the data in transit and at rest.
- The data existed at time t_0 and has not been changed since.
- The data should not be lost.

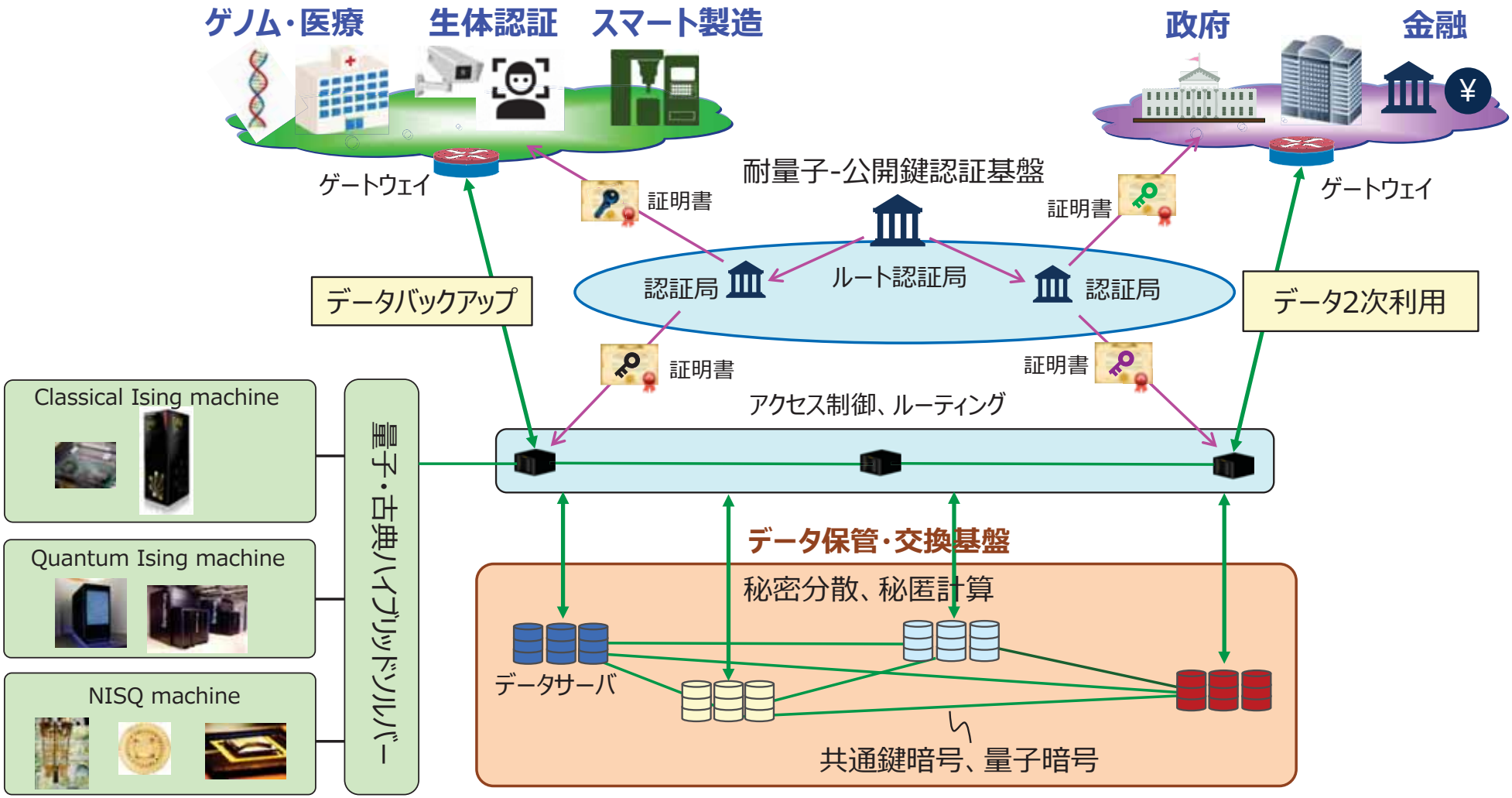


次世代暗号インフラに必要となる4つの技術

機密性	・**共通鍵暗号**（計算量的安全性）⇒重要情報 ・**量子暗号**（情報理論的安全性）⇒高機密情報
完全性	・**耐量子-公開鍵暗号**による署名、鍵交換
可用性	・**秘密分散**によるバックアップ保管

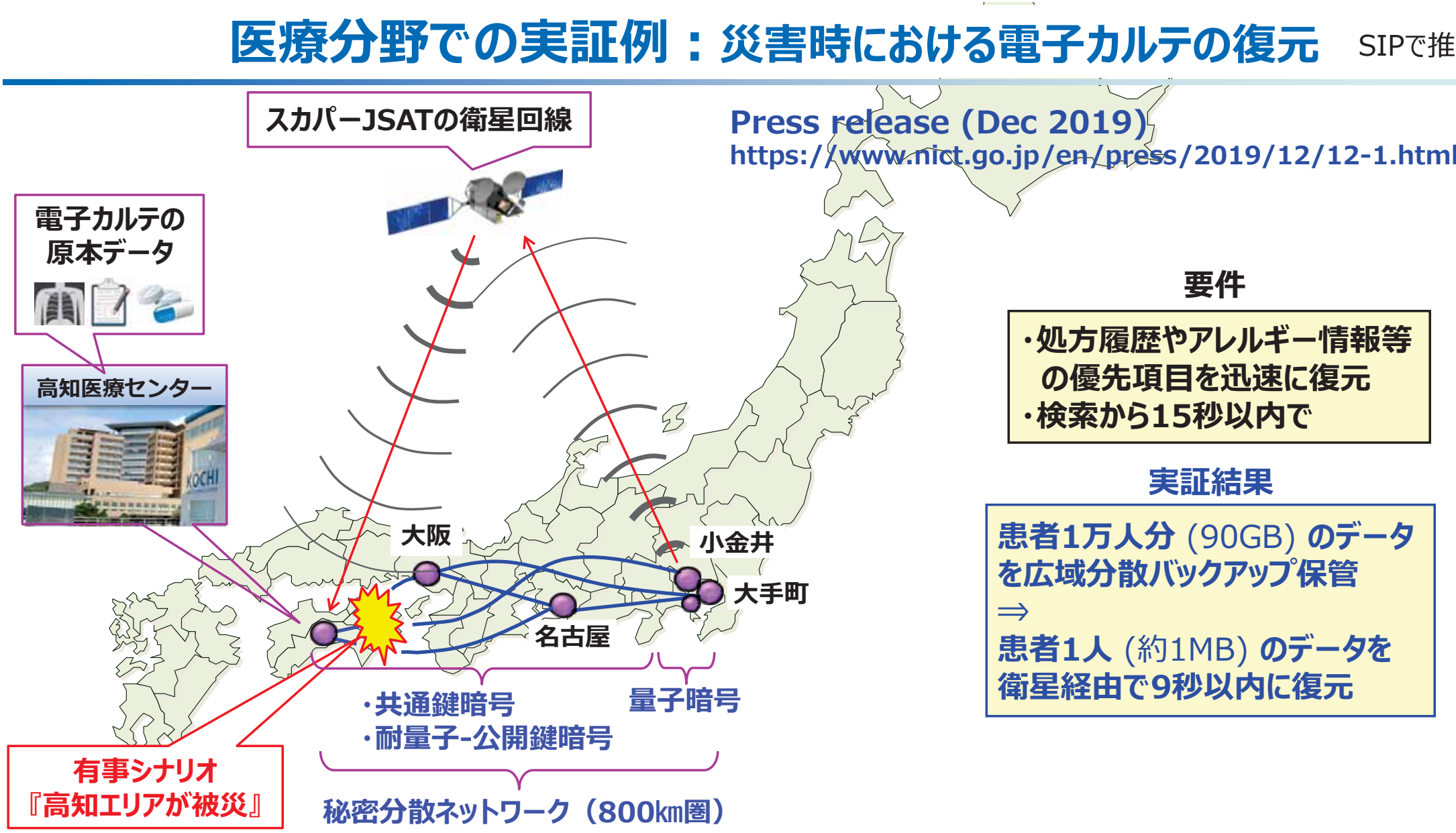
量子セキュアクラウド

SIP、総務省予算等で社会実装を推進中



医療分野での実証例：災害時における電子カルテの復元

SIPで推進



Press release (Dec 2019)
https://www.nict.go.jp/en/press/2019/12/12-1.html

要件

- 処方履歴やアレルギー情報等の優先項目を迅速に復元
- 検索から15秒以内で

実証結果

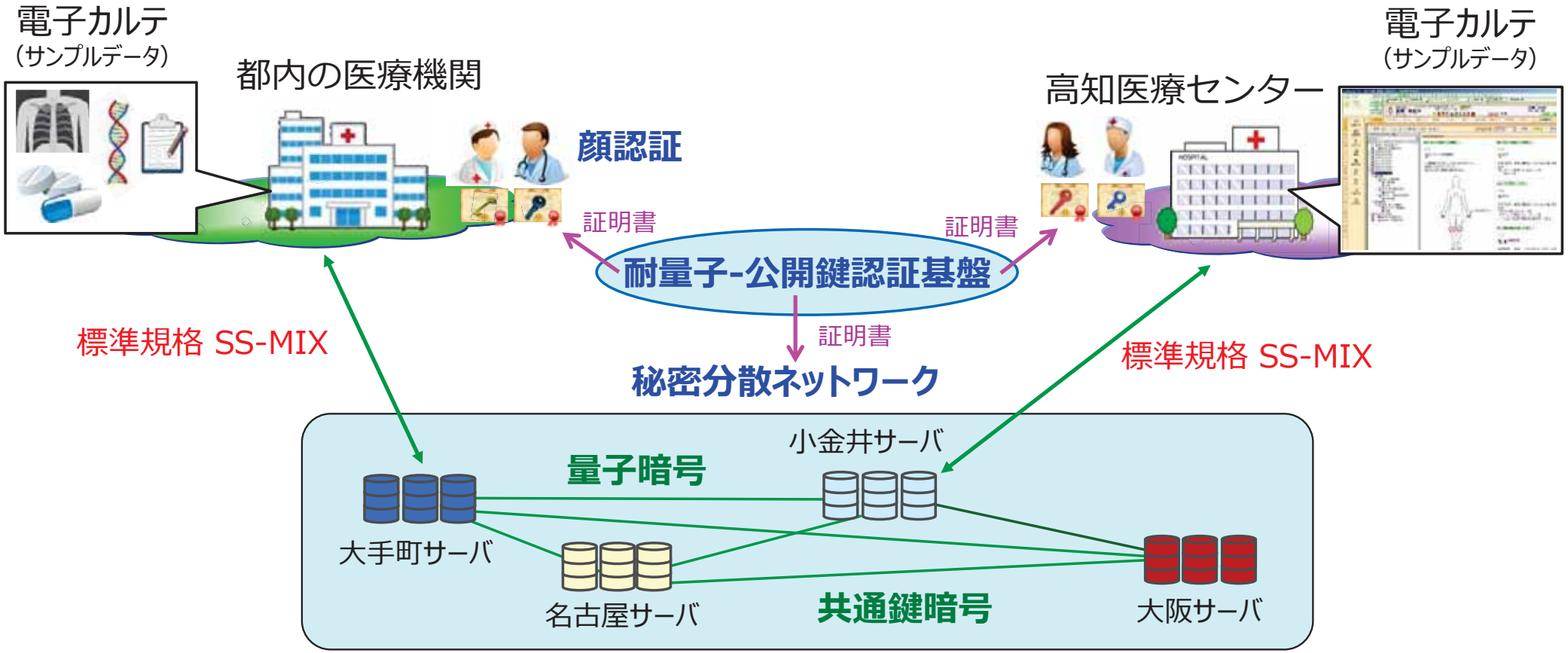
患者1万人分 (90GB) のデータを広域分散バックアップ保管
⇒
患者1人 (約1MB) のデータを衛星経由で9秒以内に復元

多要素認証によるアクセス管理、電子カルテデータの相互参照（2020年）

SIPで推進

・3要素認証：顔認証、耐量子-公開鍵認証、ID・パスワード
・遠隔の医療機関の間で電子カルテデータの相互参照

2020年10月22日 報道発表（NEC、NICT、ZenmuTech）

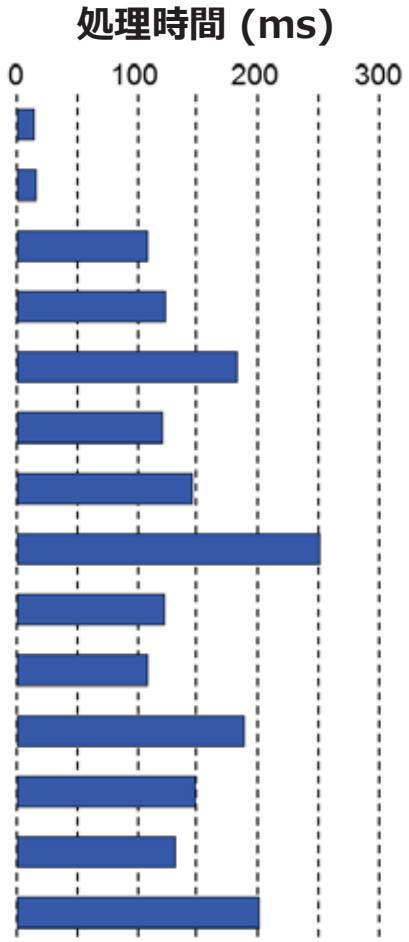


耐量子-公開鍵認証基盤

SIPで推進

有望な方式を7つ選定し、インターネット規格(TLS)の準拠した12種類の暗号パッケージを実装し、動作検証とベンチマーキングに成功。処理時間 100ms ～ 250ms (既存方式の約10倍)

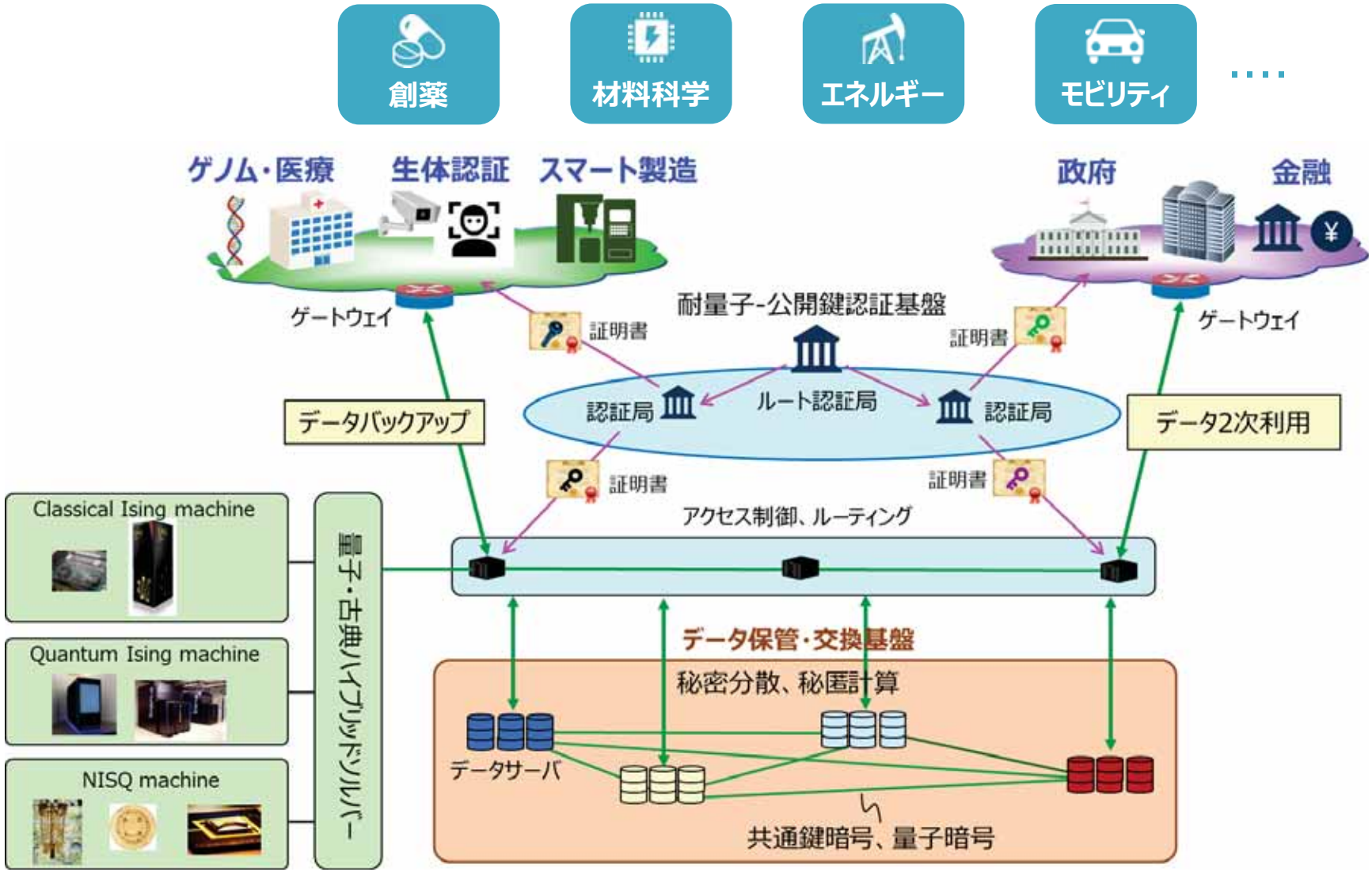
	Root certificate	Key exchange	Signature	Time (ms)
TLS	RSA	ECDHE	SHA384	14.4
		RSA	SHA384	15.8
Post Quantum TLS	LMS (Hash)	NewHope (Lattice)	Dilithum (Lattice)	107.2
			q-TESLA (Lattice)	122.2
			Rainbow (Multivariate)	183.9
		SIDH (Isogeny)	Dilithum (Lattice)	120.2
			q-TESLA (Lattice)	146.4
			Rainbow (Multivariate)	251.7
	XMSS (Hash)	NewHope (Lattice)	Dilithum (Lattice)	121.7
			q-TESLA (Lattice)	107.7
			Rainbow (Multivariate)	189.6
		SIDH (Isogeny)	Dilithum (Lattice)	149.2
			q-TESLA (Lattice)	130.0
			Rainbow (Multivariate)	201.9



フィールド環境での統合実証として世界初

NICT、カナダ・ISARA、ダルムシュタット工科大

量子セキュアクラウドという共通基盤の上に、今後もユースケースを拡大



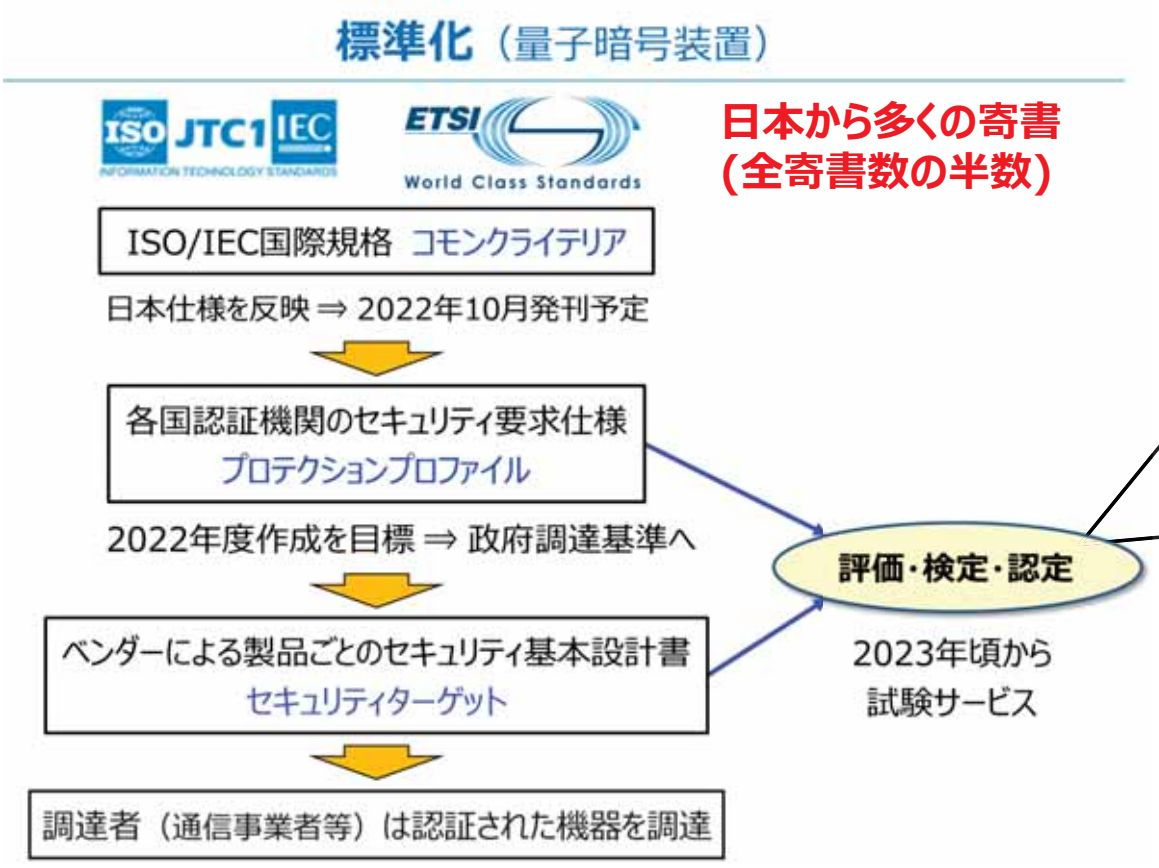
喫緊の課題

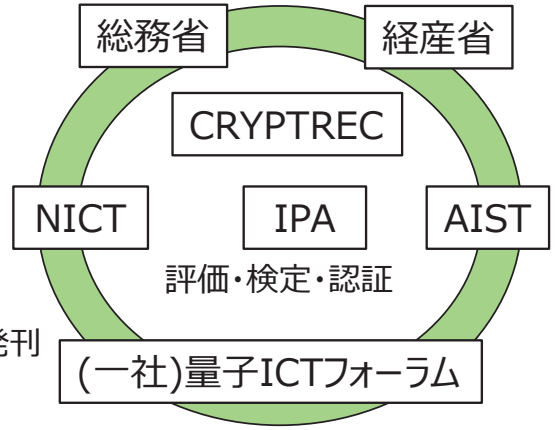
1. 標準化と制度整備

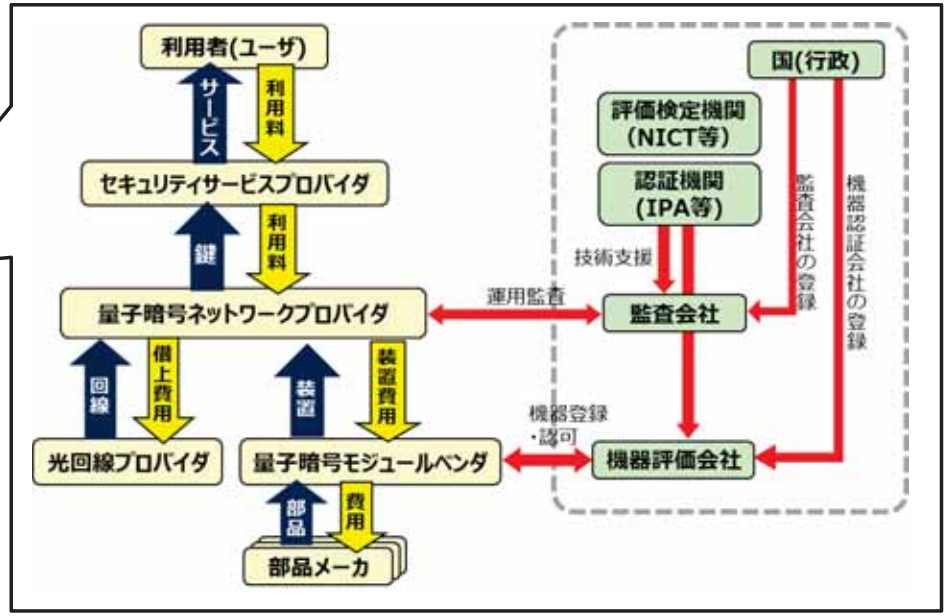
セキュリティ対策は、強制力がなければ、後回しになりがち

⇒**企業は投資しづらく、ユーザは導入しづらい**

⇒**利用インセンティブを高めるガイドラインや法整備が必要**







２．通信事業者、クラウド事業者の連携、オープンテストデッドの拡張

政府の補正予算事業の活用、『量子技術による新産業創出協議会』との迅速な連携

・2022年、政府系、金融系ユーザに量子セキュアクラウドの簡易検証環境を提供
・2023年頃、ユーザ拠点に量子暗号回線を伸長、
ベンダー、通信事業者による量子暗号サービスを提供

量子暗号通信に関するロードマップ

2023年頃

ユーザ拠点に量子暗号回線を伸長。ベンダー、通信事業者が量子暗号サービスを提供

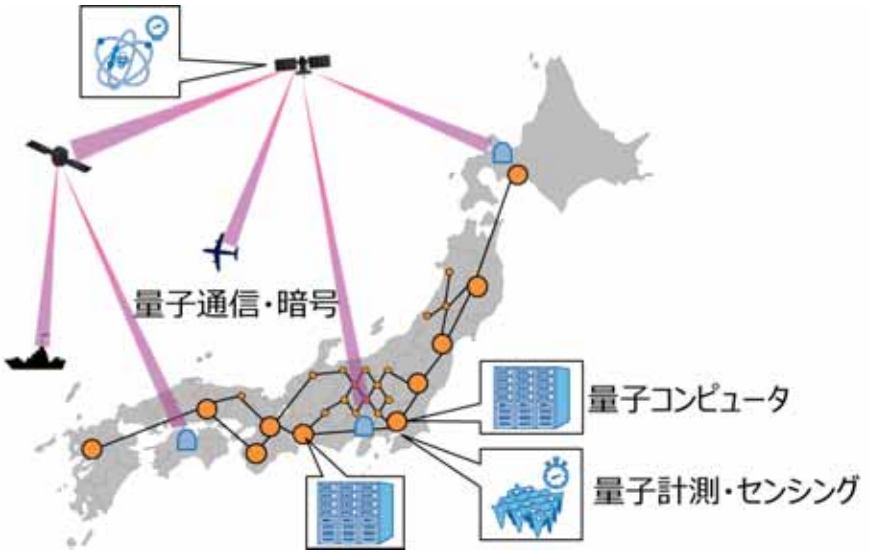
2025年頃

都市間の量子暗号通信網

・装置の量産化、低価格化
・ビジネスエコシステムの検証

2030年頃

衛星・地上網の統合
本格普及、ビジネスエコシステムの確立



３．国産サプライチェーンの確立

特に、単一光子検出器（半導体APD）の国産化、サプライチェーンの安定化

現在、中国のRMY Electronics社が国際的な供給拠点（かつての供給源・米PLI社の技術と同等の性能）

日本の問題点

・国産素子の性能向上に向けて、未だ設計・製造の勘所をつかめていない
・素子の試作・評価・分析のターンアラウンドの絶対数が少ない（人と時間を割けていない）
・企業側に投資に見合う市場規模が見定められていない

対策

・量子暗号、LiDAR、微弱光計測・イメージング、分析など
広い用途に向けた『基礎寄り』の国プロの提案、活用
・研究者、技術者が効率的に情報交換、議論できる場を強化（拠点運営）

・2025年頃、国産APD生産体制の整備
・2030年頃、計測・センシング、スマートモビリティ、衛星通信・センシングなど適用分野の拡大

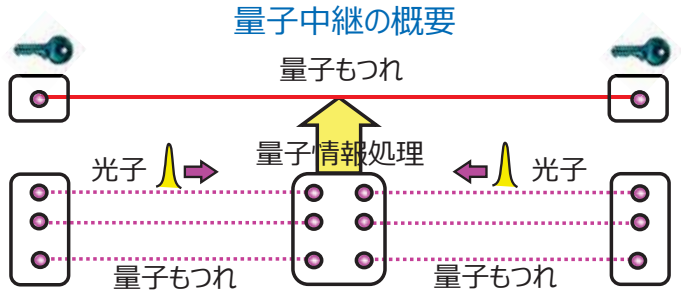
４．量子中継など基盤技術の研究開発、人材育成の強化

実証計画案（フィジビリティについて今後、要検討）
- ・2022年頃、実験室ボビンファイバで実証
- ・2023年頃、構内敷設ファイバ上で実証
- ・2024年頃、量子暗号との相互接続試験
- ・2025年頃、オープンテストベッド上に導入

⇔

人材育成プログラムとの連携
- ・NICT Quantum Camp
- ・Q-LEAP
- ・大学のカリキュラム

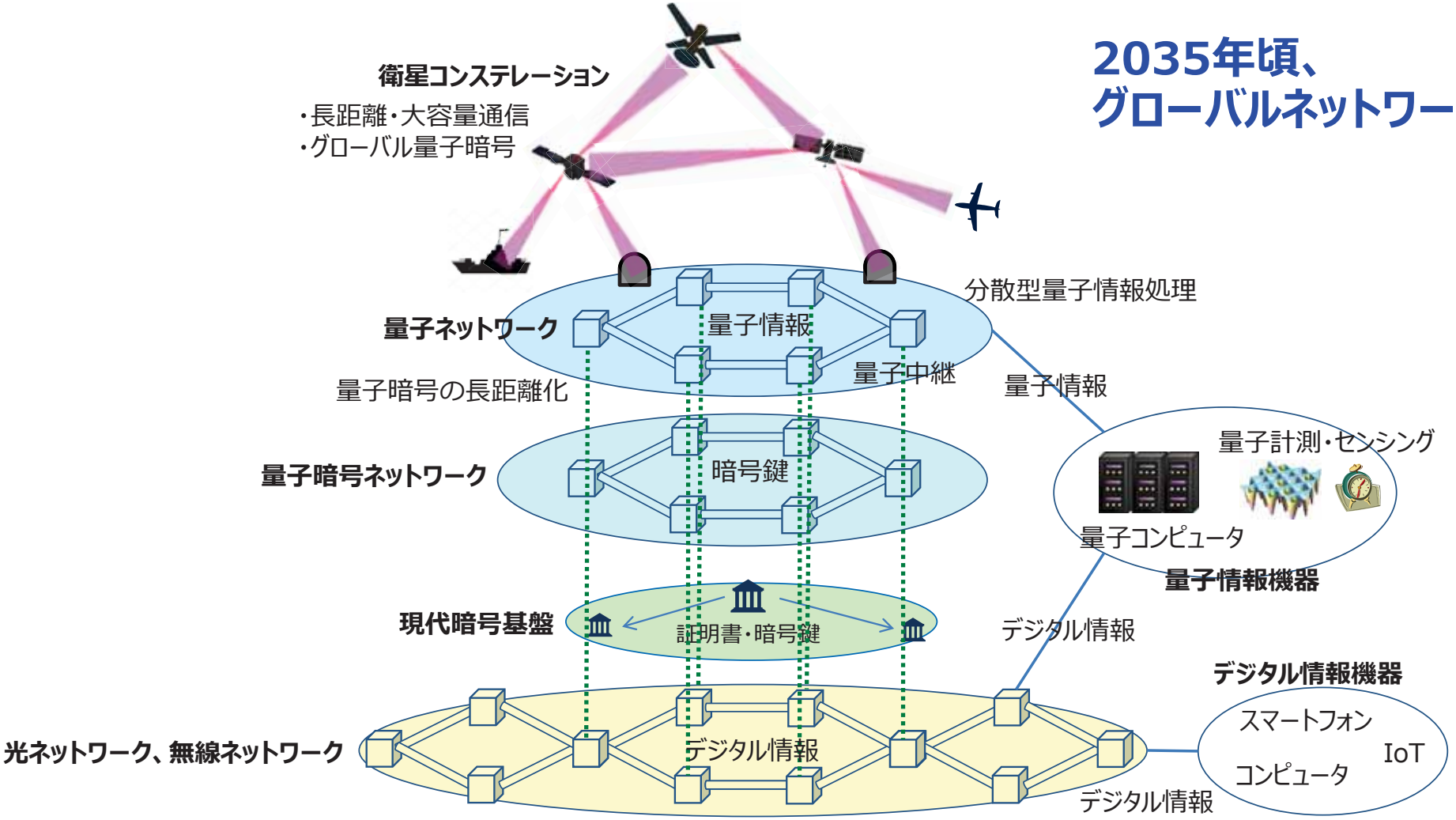
など



今後の展望

量子技術プラットフォーム構想

量子コンピュータ、量子通信・暗号、量子計測・センシングを情報通信インフラに導入し統合



ご清聴ありがとうございました