量子セキュアクラウドの社会実装の現状

【スマートIoT 推進フォーラム技術戦略検討部会第１３ 回テストベッド分科会】

2022年9月27日（火曜）

本研究(の一部)は、以下のプロジェクトの支援を受けています。
・内閣府総合科学技術・イノベーション会議の戦略的イノベーション
創造プログラム（SIP)「光・量子を活用したSociety 5.0 実現化技術」
（管理法人：量研(又はQST)）
・総務省「ICT重点技術の研究開発プロジェクト(JPMI00316)」

情報通信研究機構
未来ICT研究所
小金井フロンティア研究センター
量子ICT研究室
藤原　幹生

目次

守るべき情報資産

秘匿期間	分野	情報	セキュリティレベル	理由
30	防衛	作戦計画等	**非常に高い**	防衛情報を扱っている為
		防衛装備品に関する技術情報	**非常に高い**	防衛情報かつ法律でも定められている為
30	行政	政策	**普通**	国の混乱を招く恐れがあるが一時的となる可能性が高い為
		外交情報	**非常に高い**	国の信用問題であり各国との関係に悪影響を及ぼす為
＞100	医療	ゲノム情報	**非常に高い**	遺伝情報は一度漏洩すれば永続的に生命を脅かすリスク、社会的差別のリスクに繋がる為
		電子カルテ	**高い**	アレルギーなど人の生死に係る為
30	インフラ	SCADA	**高い**	ライフラインを不正操作された場合各地域に影響を及ぼす為
		新エネルギー開発	**高い**	国際的に重要な開発は資産である為
5	金融	金融政策	**高い～普通**	非公開期間が短期間である為
		株式	**非常に高い**	企業情報が主な秘密情報である為

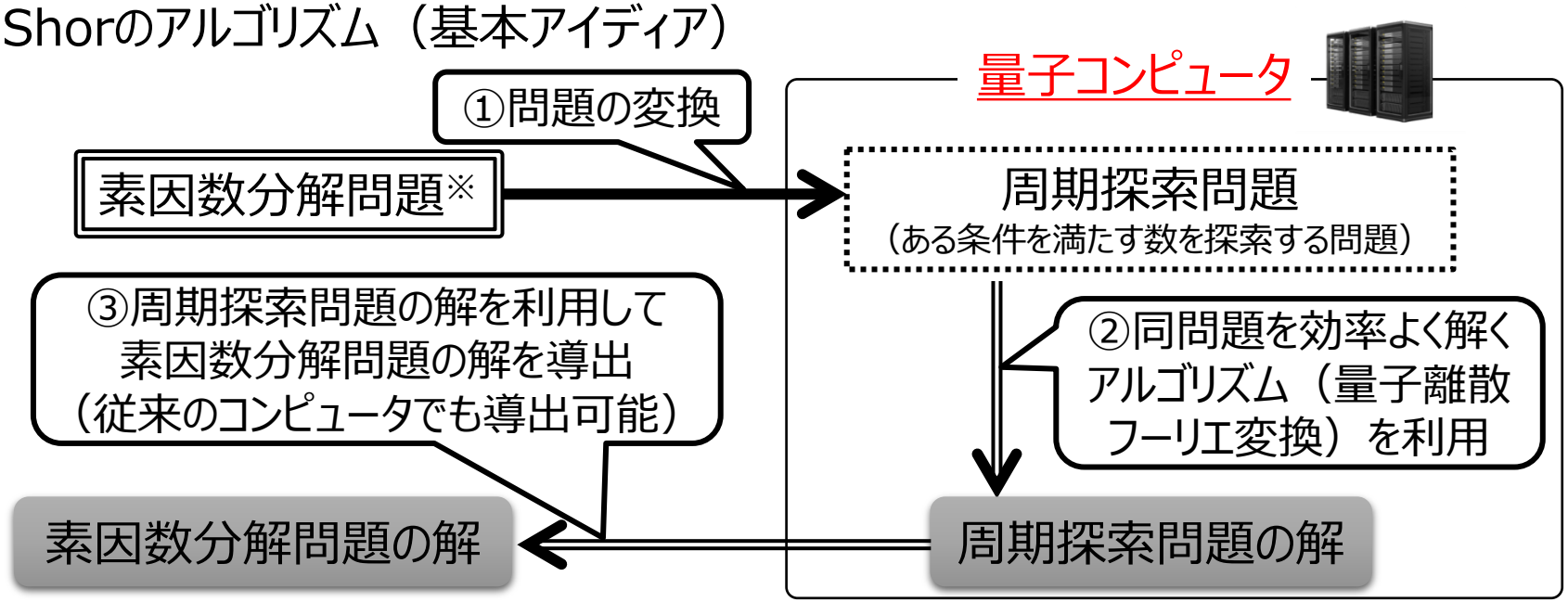
量子コンピュータによる公開鍵暗号解読

■ 量子コンピュータ（ユニタリー型）の実現が現在主流の公開鍵暗号に与える影響は大

現在主流の公開鍵暗号	安全性の根拠となる数学的問題
RSA暗号	素因数分解問題
楕円曲線暗号	楕円曲線離散対数問題

量子コンピュータ上で動作するShorのアルゴリズムで容易に解読可能（潜在的な脅威）

□ Shorのアルゴリズム（基本アイディア）



※楕円曲線問題離散対数問題も同様に解くことが可能

量子コンピュータによる現代暗号への影響

- **大規模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の安全性が急低下**

	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	

離れた二者間で鍵を共有する事に使用されている公開鍵暗号で
現在広く使われている方式は量子コンピュータ耐性を持っていない
→上記に代わる鍵交換手段が近々に必要

耐量子計算機暗号　Post Quantum Cryptography (PQC)

- 大規模量子コンピュータが実現しても
  安全性が保たれると期待される暗号技術
  - 安全性の根拠となる数学的問題を効率的に解く
    量子アルゴリズムが見つかっていない、という意味
- 現在の公開鍵暗号と置き換え可能

方式	安全性の根拠（数学上の難問）
格子に基づく暗号技術	格子問題
符号に基づく暗号技術	誤り訂正符号
多変数多項式に基づく暗号技術	多変数多項式求解問題
同種写像に基づく暗号技術	同種写像問題
ハッシュ関数に基づく署名	ハッシュ関数の衝突

6

米国での暗号技術の標準化の動き

米国NISTでのPQC標準化

- 米政府標準を置換える標準策定
  電子署名(FIPS186), 鍵確立(NIST SP800-56)
- 2016年募集開始
- **2022年７月標準化プロトコルの選定とround 4での評価を必要とするプロトコルの発表**

・加速する可能性大
・耐量子暗号の必要性は共通認識
・2022年round 4に進んだSIKEに重大な結果が見つかったとの報告（安全性は研究者の数と研究期間に依存し勝ち）

世界中から
82方式　応募
<書類選考>
2017年11月

→ 69方式
<Round 1評価>
2017年12月

→ 26方式
<Round 2評価>
2019年1月

→ 7+8方式
<Round 3評価>
2020年7月

→ 4方式標準化
+4方式
<Round 4評価>
2022年7月

Dilithium
Falcon
SPHINCS+
Kyber

BIKE
Classic McEliece
HQC
SIKE

数学的ではなく，物理的に安全性が確認できる量子鍵配送も一定の需要が望める

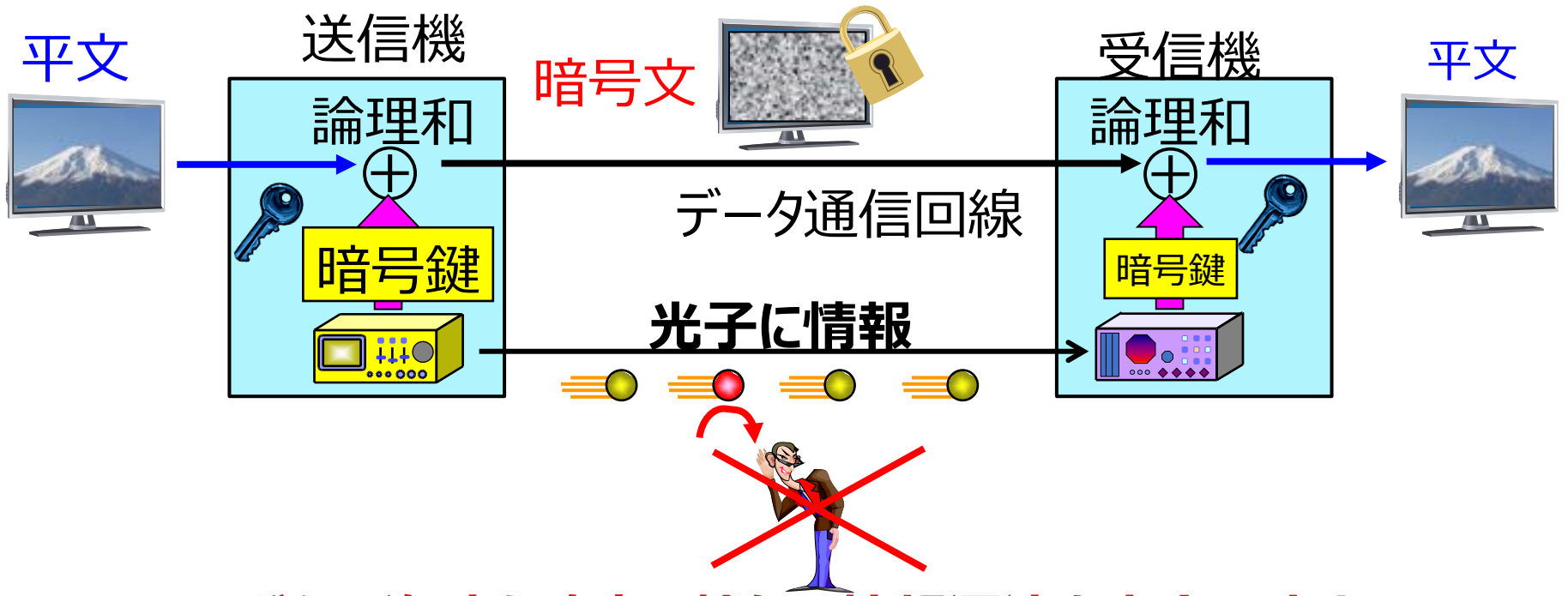
January 30, 2019	Second Round Candidates announced (26 algorithms)
March 15, 2019	Deadline for updated submission packages for the Second Round
May 8-10, 2019	NIST Presentation at PQCrypto 2019: Round 2 of the NIST PQC "Competition" - What was NIST Thinking?
August 22-24, 2019	Second PQC Standardization Conference
July 22, 2020	Third Round Candidates announced (7 Finalists and 8 Alternates)
October 1, 2020	Deadline for updated submission packages for the Third Round
2022/2024	Draft Standards Available

安全な通信を実現　量子鍵配送・量子暗号とは

「どんな計算機でも解読できない」ことを証明できる現在唯一の暗号方式

・量子鍵配送（QKD）により平文と同じサイズの暗号鍵を共有
・送りたい情報と暗号鍵を1ビットずつ排他的論理和を計算し暗号化
（1度使った鍵は2度と使い回さない → Vernam's ワンタイムパッド暗号：OTP）

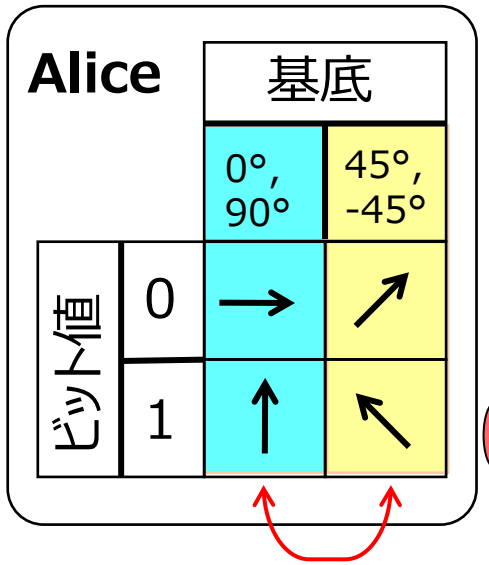
（情報理論的安全）



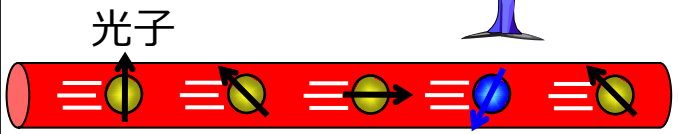
どんな盗聴も確実に検知　情報漏洩を完全に防止

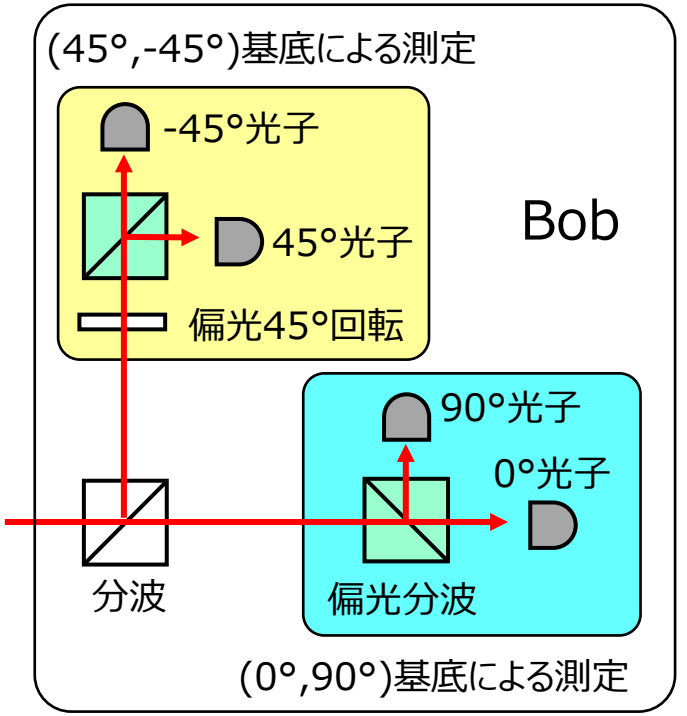
量子鍵配送の代表的なプロトコルBB84

光子の４つの偏光状態



盗聴行為は光子の状態に変化をもたらす（不確定性原理）
⇒盗聴が露見





互いに非直交な2つの『基底』

W. K. Wooters

非直交状態の系列を誤り無くコピーすることは不可能

No-cloning定理〝自然の摂理“

量子鍵配送装置の鍵生成レート

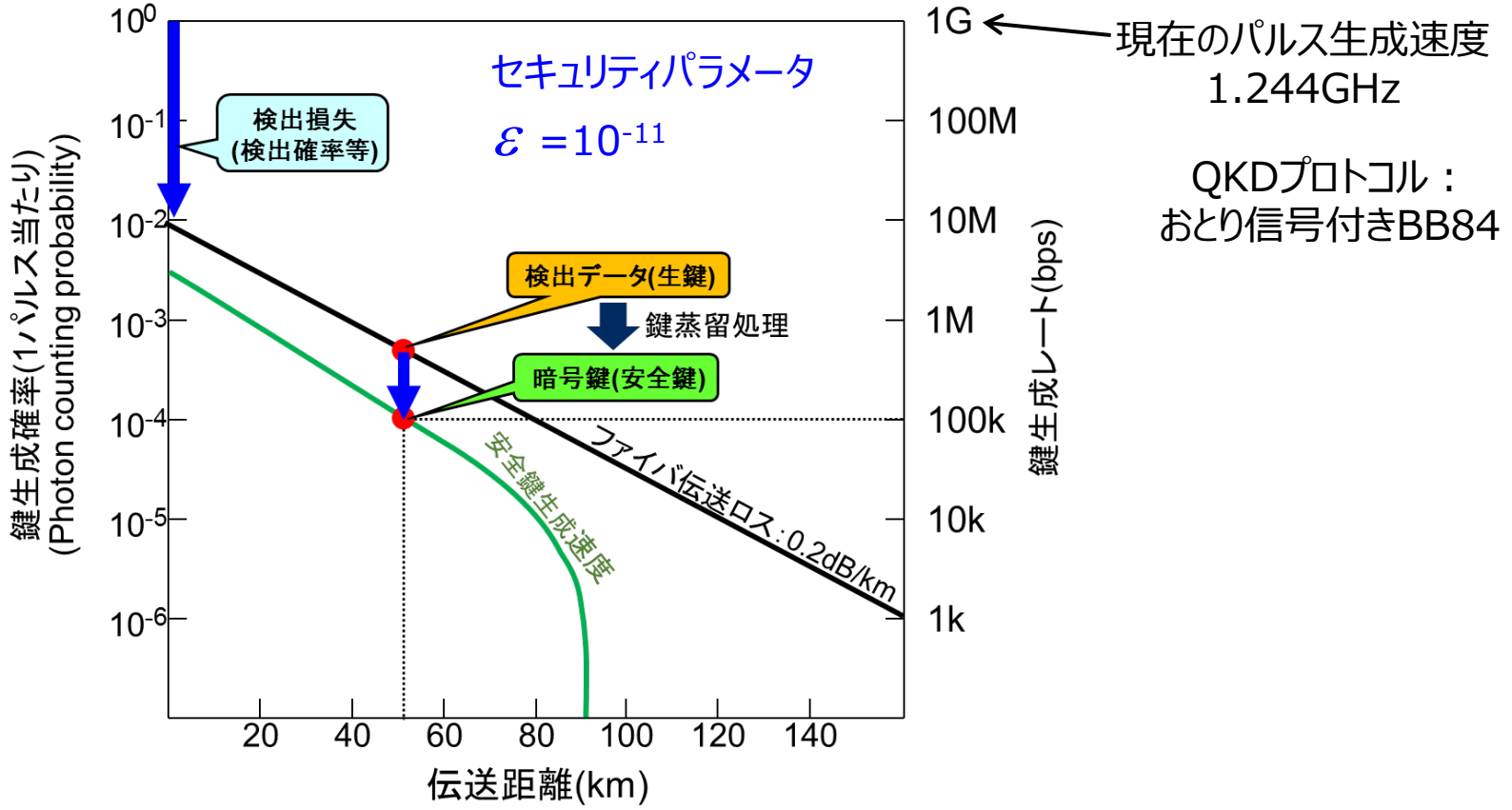
・安全性を向上（セキュリティパラメータεを小さく）させると鍵生成速度は下がる

・鍵生成速度＝(パルス生成速度) x (通信路透過率)

x [1 − (誤り訂正レート) − (秘匿性増強レート)]

観測されたビット誤り率から直接計算

安全性理論に基づいてビット誤り率から推定

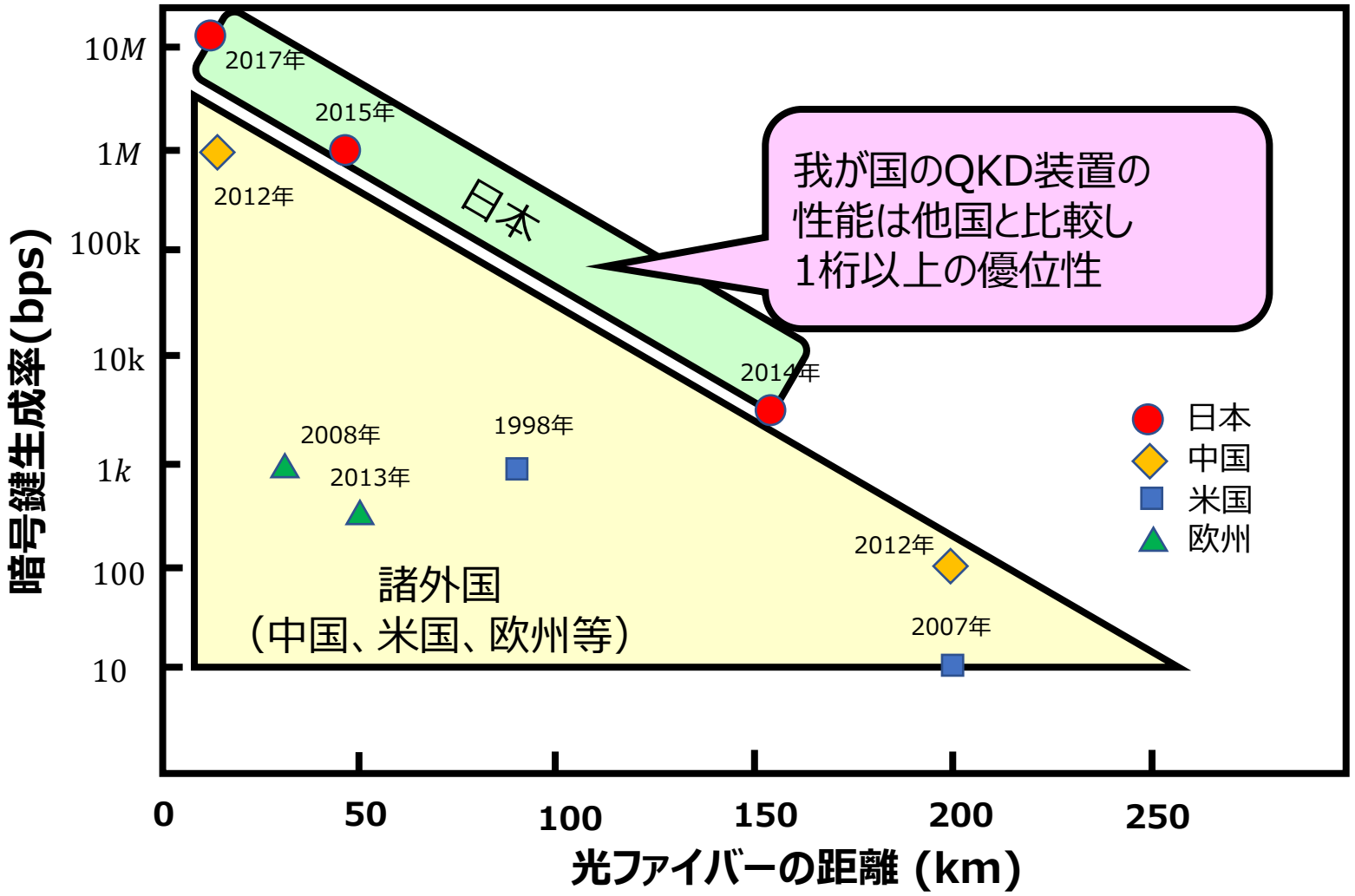


現在のパルス生成速度
1.244GHz

QKDプロトコル：
おとり信号付きBB84

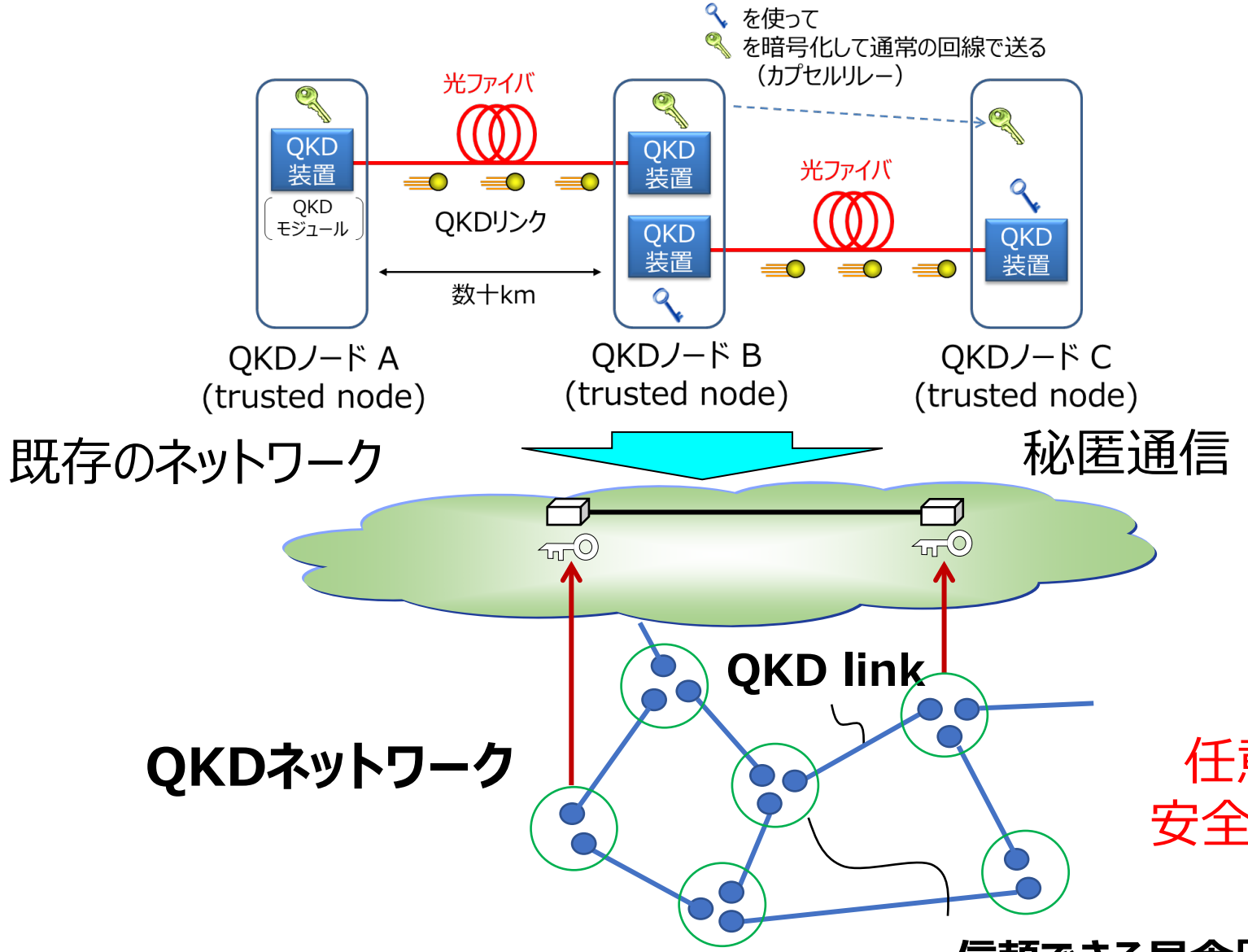
我が国の量子鍵配送装置の優位性

暗号鍵生成量/装置コスト　我が国の装置は優位



論文，標準化活動，有力企業のWEB情報より

『信頼できる局舎』を介した鍵のカプセルリレー



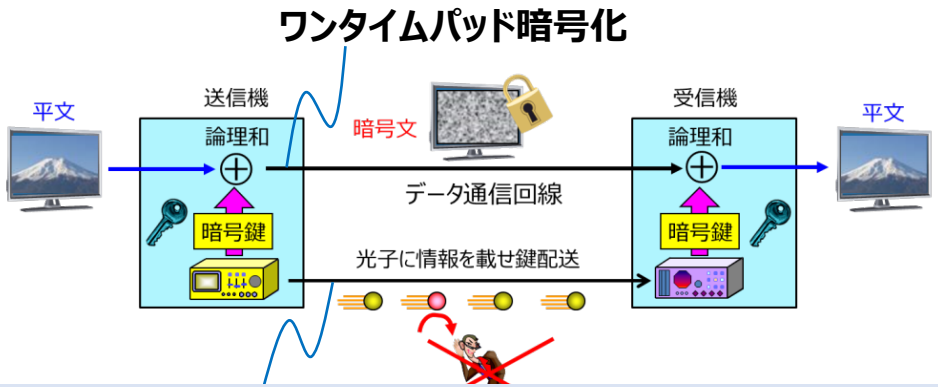
任意の局舎間で
安全な通信が可能

信頼できる局舎「Trusted node」

量子セキュアクラウド　安全な分散データバックアップ・データの二次利用

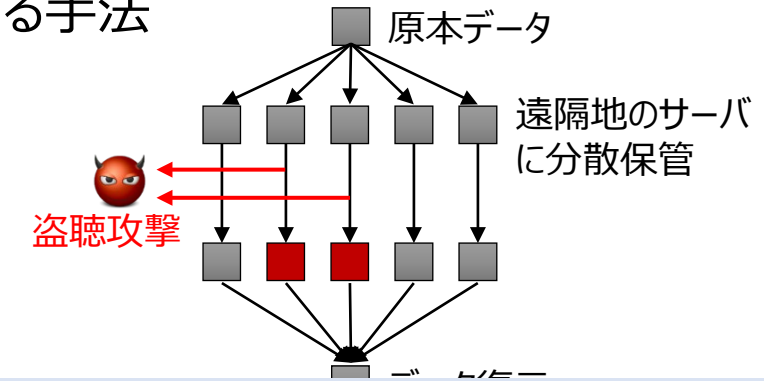
量子暗号

『**どんな計算機でも解読できない**こと』を証明できる現在唯一の暗号通信方式



秘密分散

原本データを無意味化された複数のデータ（シェア）に**分散し保管**する手法

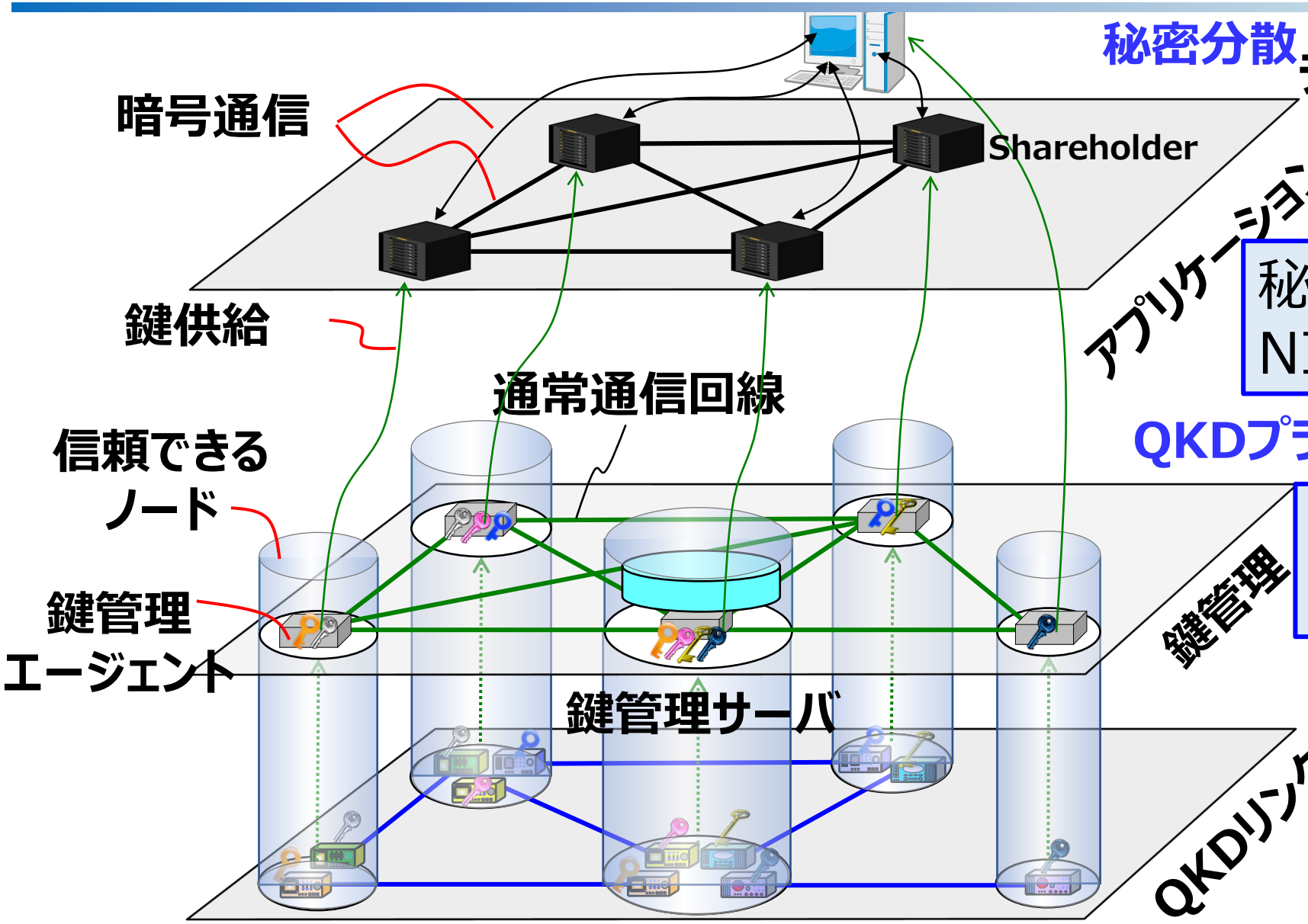


超長期に秘匿すべきデータの保護・利用をデモ
（電子カルテ，ゲノム関連データ，生体認証データ等）

『量子セキュアクラウド』

- ✓ 将来にわたり機密漏洩と不正改竄を防ぐ安全なデータ保管を実現
- ✓ 一部のサーバが棄損した場合でも必要時に原本データを復元可能
- ✓ 安全なデータの二次利用を実現

量子暗号ネットワークの階層モデルとSIPでの活動



秘密分散・秘匿計算：
NICT，ZenmuTech

安全性評価：
東大，北大

装置開発：
NEC，東芝，学習院大

量子暗号・量子セキュアクラウドの社会実装計画

(1) 電子カルテ（模擬）の秘密分散保管
(2) ゲノムデータ（模擬）の秘密分散保管
(3) レーザ加工拠点の重要回線の秘匿化
(4) 生体認証の参照データの秘密分散保管

高知医療センター

(1) 高知～東京 800km圏、
電子カルテ模擬データを
共通鍵暗号で秘匿化

仙台 10km圏

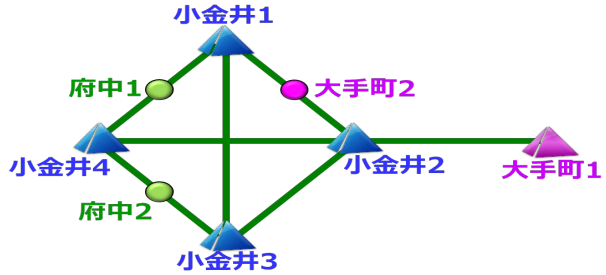
(2) ゲノム解析データの
暗号通信、秘密分散

大阪拠点

名古屋拠点

共通鍵暗号による秘匿化

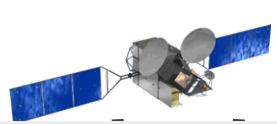
(3) レーザ加工拠点間回線の秘匿化



東京 100km圏

(1) 電子カルテ模擬データh秘匿化・分散保管
(4) 生体認証の実データを量子暗号
で秘匿化　参照データの分散バックアップ
(5) 金融応用

（1）電子カルテデータへの適用



上り1MB/s
下り3M/s

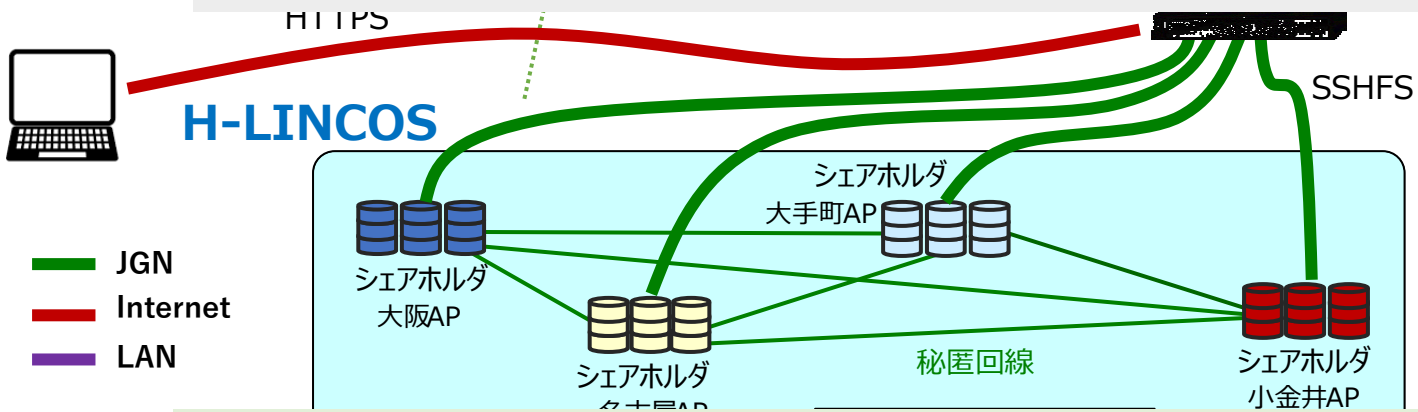
高知医療
地上

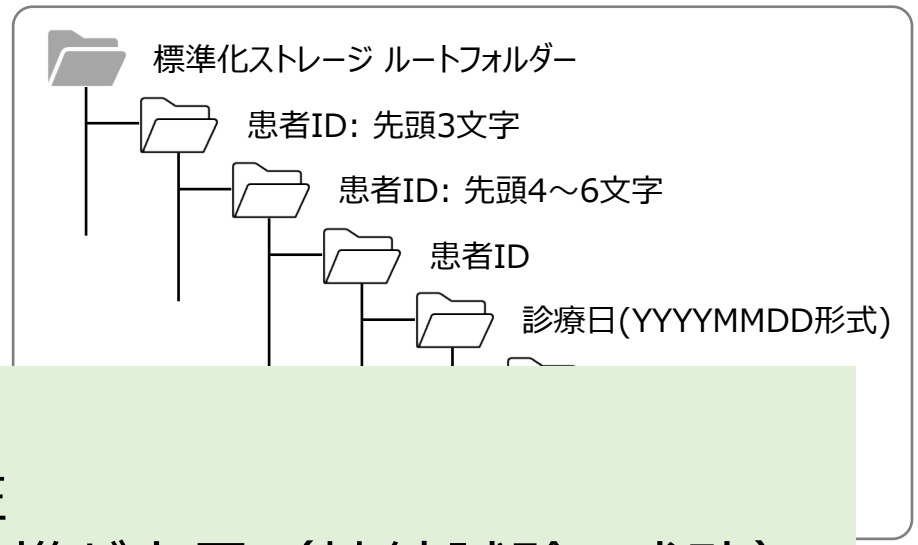
HTTPS

Webブラウザー

格納データ諸元：
- **患者数： 1万人**
- **ファイル数： 12,490,000ファイル**
- **データサイズ： 90GB**

患者基本上表示にかかる時間：
- **地上網 ： 2～4秒**
- **衛星経由： 4～8秒**





衛星管制局経由での接続のメリット

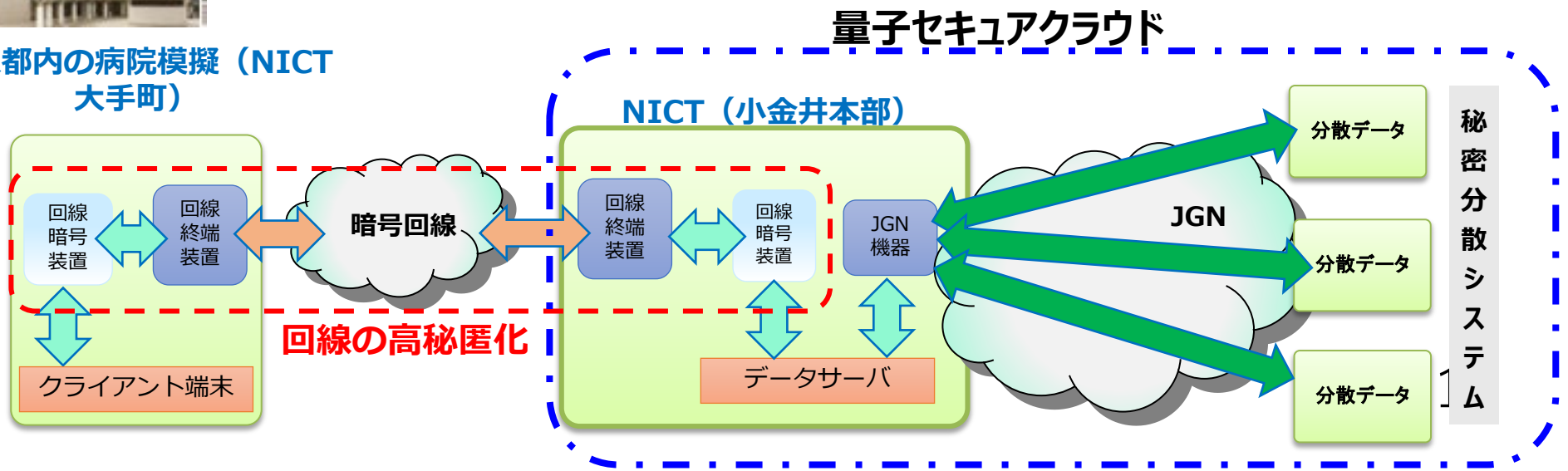
1. DMATや他の地域医療連携への展開の可能性
2. 広域災害救急医療情報システム(EMIS)との連携が容易（接続試験に成功）

（1）電子カルテデータへの適用

- Tokyo QKD Network上で東京都内の公的病院とPOCを開始
  ⇒系列6病院の**日毎の更新データを15分以内**に書き込む技術を確立。実用性を確認。
  （1日当りの来院患者5000人分のデータ 320MB程度）　電子カルテSS-MIX模擬データ
- 高知医療センターとの模擬データの相互参照を実証（地域医療連携の有効性を確認）

東京都内の病院模擬（NICT大手町）

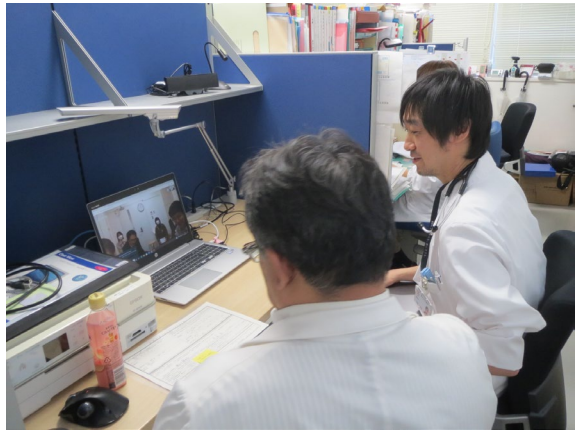
2020年10月22日プレスリリース



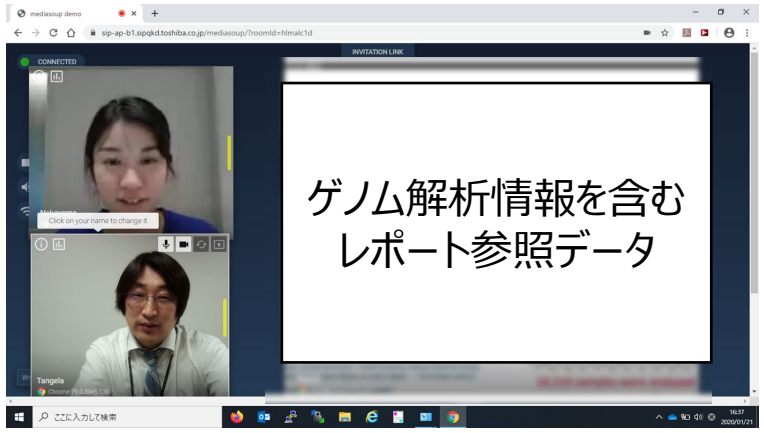
（2）ゲノム医療への適用

オンラインの完全秘匿なTV会議・レポート参照データ伝送

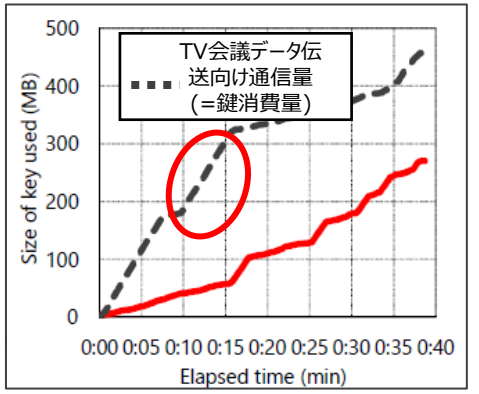
- 医師含む延べ10名が参加し延べ65分間のTV会議を実施
  医師による主観評価において，良好に利用できることを確認
- 平均鍵消費速度は約1.6Mbps。東芝製量子暗号装置の鍵配信速度(最大10Mbps)によって問題なくサポート可能であることを確認



大学病院拠点の実証の様子



TV会議画面例



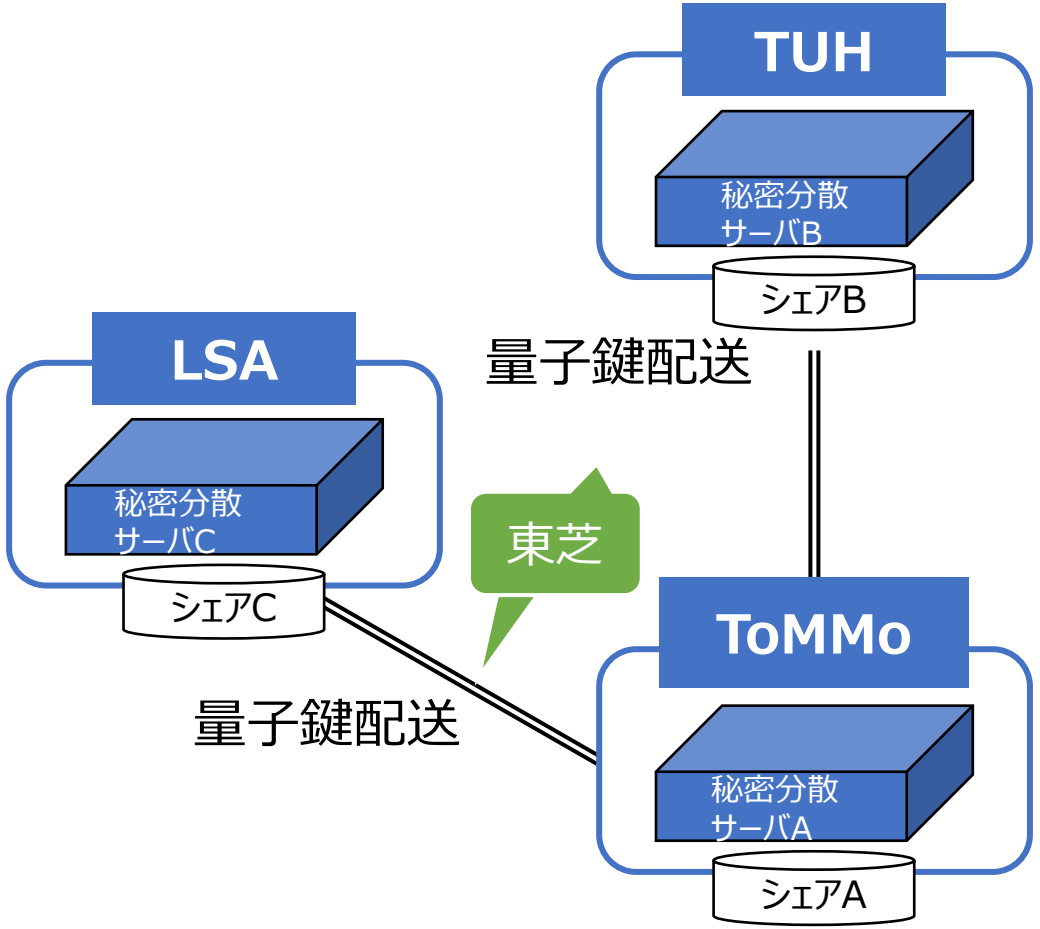
TV会議データ伝送時の暗号鍵消費量

OTP暗号化伝送向けに十分な速度で暗号鍵を共有

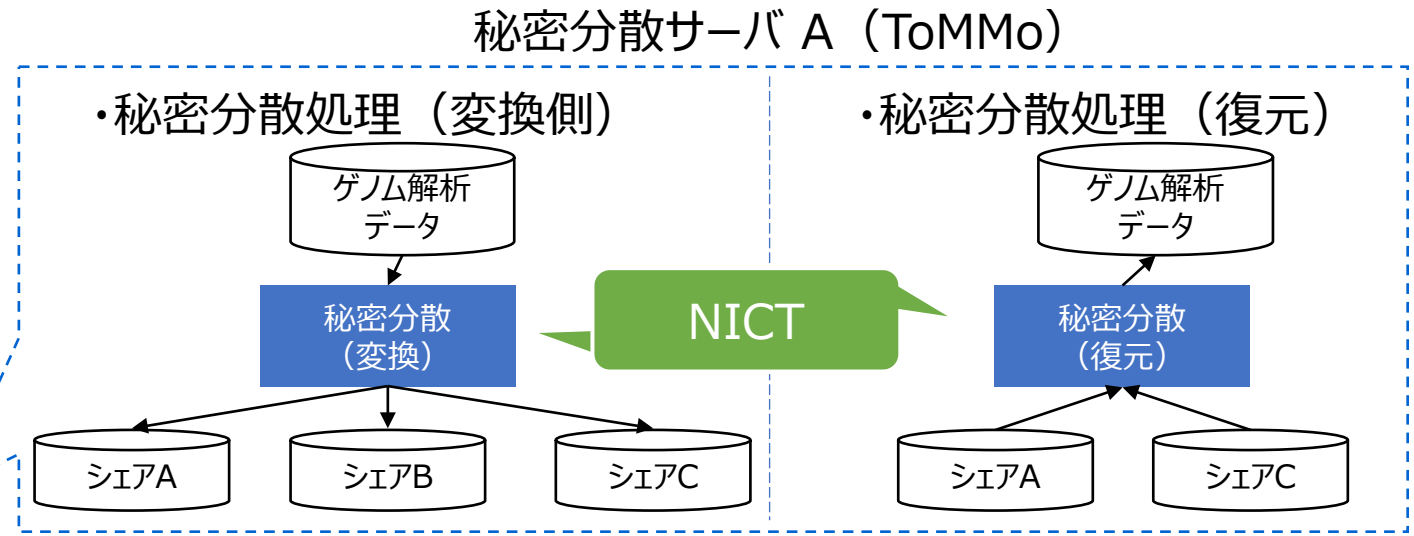
2020年8月7日　プレスリリース

（2）ゲノム医療への適用

ゲノムデータの情報理論的安全な伝送と保管



８０GBのデータを秘密分散で数時間で３か所に分散



OTP: ワンタイムパッド
LSA：東芝ライフサイエンス解析センター
ToMMo：東北大学東北メディカル・メガバンク機構
TUH：東北大学病院
NICT：情報通信研究機構

（４）生体認証への適用

顔認証システムの特徴

生体情報である顔画像を認証等に利用する技術　**ユーザにやさしい認証技術**

漏えい事件と機微情報の重要度の高まり

Amazon Web Servicesへの攻撃

- 米大手金融某社の一部社会保障番号や銀行口座番号を含む顧客情報が、AWSへの攻撃から不正取得された

2800万人の生体認証情報が流出

- 韓国大手セキュリティサービス事業者が提供するサービスで、指紋や顔写真を含む生体認証情報2780万件以上が流出した

ゲノム情報から顔の容貌を再現可能な時代

- バイオテクノロジー分野の某社が身元不明のゲノム情報から顔の容貌を再現可能なアルゴリズムを発表

【上段】容疑者はAWS元従業員と現地報道、米金融大手で1億件超の個人情報漏洩（日経XTECH）<https://tech.nikkeibp.co.jp/atcl/nxt/news/18/05628/>
【中段】Report: Data Breach in Biometric Security Platform Affecting Millions of Users（vpnMentor）<https://www.vpnmentor.com/blog/report-biostar2-leak/>
【下段】Researchers produce images of people's faces from their genomes（The Economist）
<https://www.economist.com/science-and-technology/2017/09/09/researchers-produce-images-of-peoples-faces-from-their-genomes>

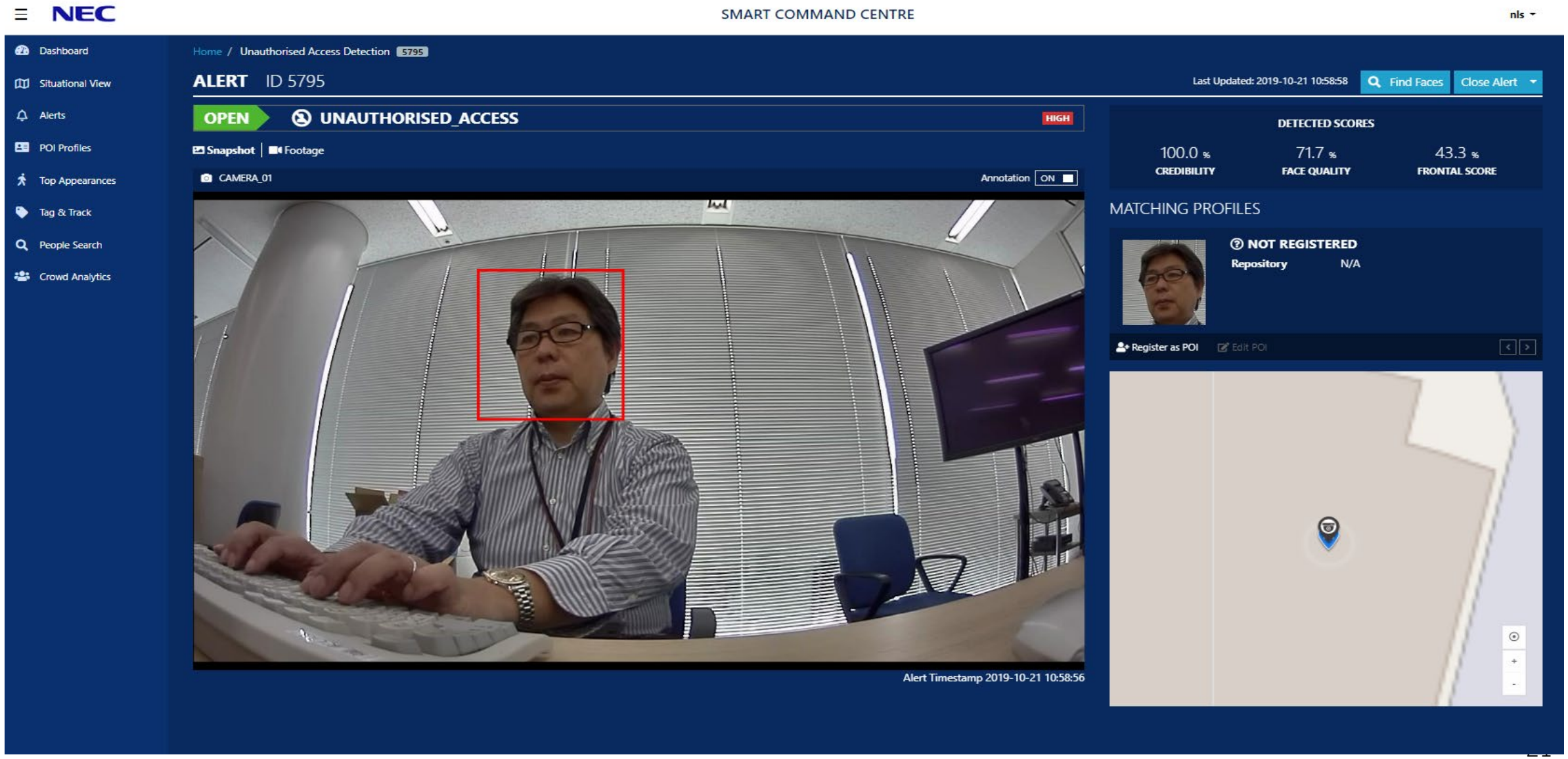
また、ゲノム情報から顔の容貌を再現できる時代になりつつあるため

新しい通知

・個人情報の漏洩は**多額の損害賠償の懸念**

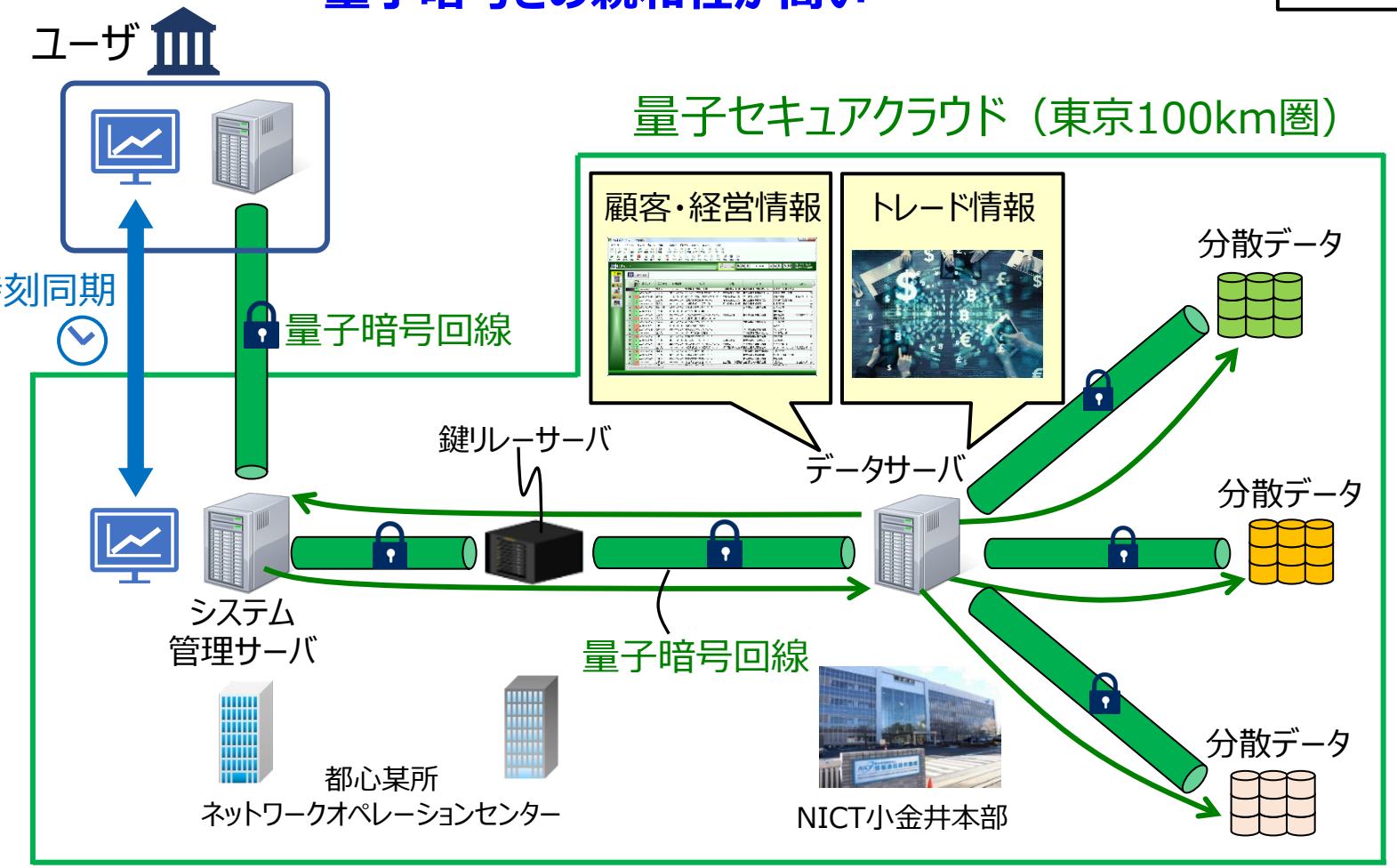
（４）生体認証への適用

・ナショナルチームが**実際に使用しているデータの保護**に活用
→法律上の保護対象である**生体認証への量子暗号・量子セキュアクラウド技術活用**



(5) 金融分野への応用

金融分野では専用線を用いるケースが多く，量子暗号との親和性が高い



2022年1月14日　プレスリリース

✓ **野村證券 野村HD様と共同実証開始**

- **実証環境構築（都心部）**
- **金融情報の高秘匿伝送実験**
  低遅延性・大容量耐性

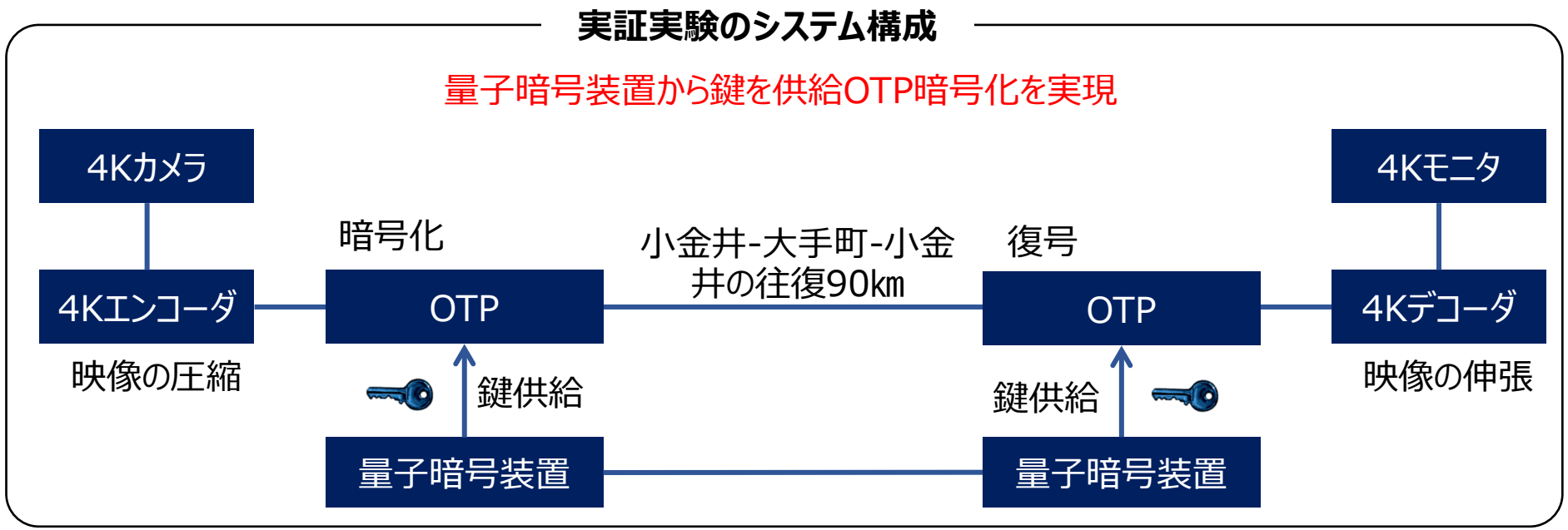
→80倍のボリュームのデータに対し，40msの付加的遅延で成功

- 技術的な評価に成功
→個人情報保護への適用など
ガイドラインの整備も含め実施予定

遅延性の実験　QKD＋OTP の4K画像高速伝送

✓ 量子鍵配送＋OPT暗号，4K映像の高秘匿圧縮伝送を実証

- 90㎞の敷設環境で**OTPでも１Gbpsの高秘匿伝送が可能**
  （小金井-大手町-小金井の往復回線）



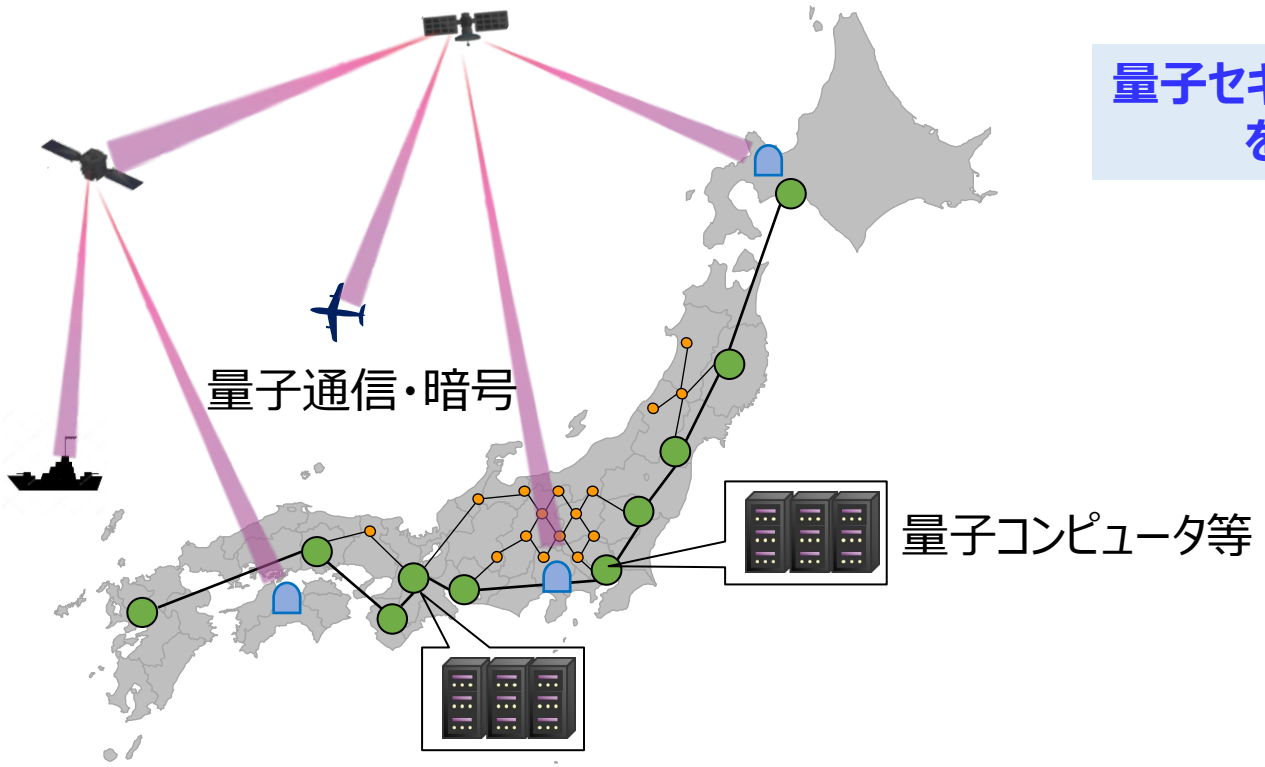
4K高精細動画高秘匿伝送技術　遠隔医療にも活用可能か？

ロードマップ

・NICTに『量子セキュリティ拠点』を整備中
・東京QKDを拡張するともに産学官共同利用を一層拡大

⇒ **民間投資とユーザの拡大**

第1段階（2023年頃）：関東圏での量子セキュアクラウド形成
第2段階（2025年頃）：各都市での量子セキュアクラウドコロニー形成
第3段階（2030年頃）：衛星・地上網の統合（日本全土）
第4段階（2035年頃）：グローバルネットワーク化



量子セキュアクラウド技術を海外展開

まとめ

1. 将来の盗聴リスクを考えると量子暗号，量子セキュアクラウドは必要

2. 我が国の量子暗号装置，アプリケーションは世界最高水準

3. ビジネス化には量子暗号を利用するための制度の充実が必須

4. 安全性検定，ガイドライン，量子暗号導入によるインセンティブ向上を担保する法整備など暗号業界全体の協力関係が不可欠