

OB/OG親ぼく会「研究講演会」 「量子の夢に導かれて」

社会実装の現状

2022年10月14日（金曜）

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**

CRL時代 基礎先端部門 量子情報技術グループ オープニングスタッフ



NICTに残っているのは2名だけ…
当方が量子に参加する前はデバイス屋でした

赤外天文衛星ASTRO-F（あかり）に搭載

青く示された箇所が温かい星間物質（波長 $90\mu\text{m}$ ）、赤いほど冷たい星間物質（ $140\mu\text{m}$ ）の存在を示す。星間物質が温かい領域ほど、より多くの新しい星が生まれつつある

→ **世界でもっとも深く高精度な遠赤外全天画像**
天文観測で実力を証明し、NICTの性能評価の正しさが証明

- ・イントロ 何故量子暗号が必要か
- ・量子暗号の現状
 - ・ファイバー地上局での性能
 - ・各国での状況
 - ・我が国での活動内容紹介
- ・ロードマップ

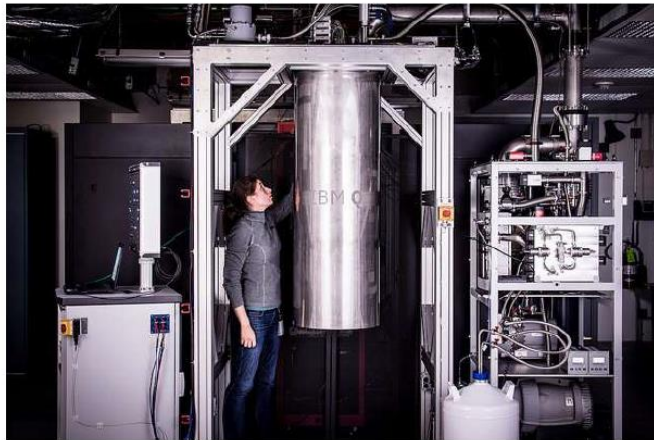
守るべき情報資産

| 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 |

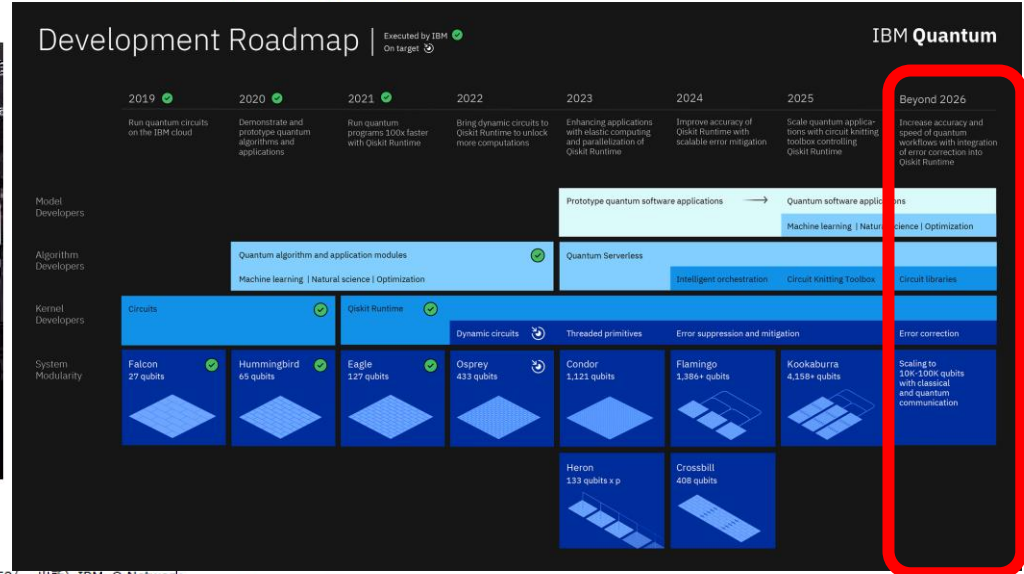
進む量子コンピュータ開発

IBM

IBM Q ハードウェア概観



出所) IBMリサーチ
https://www.flickr.com/photos/ibm_research_zurich/34662903516/in/album-72157663611181258/
 NRI Copyright (C) Nomura Research Institute, Ltd. All rights reserved.



出所) IBM Q Network
<https://quantumexperience.ng.bluemix.net/qx/editor>

11

「IBM Q」公開中 **誰でも無償でIBM社にある量子コンピュータを実際に利用**
数年以内に1000qbitsに達する計画

Google

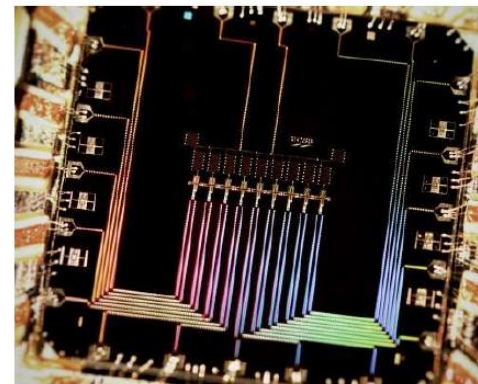
Google Quantum A.I. Lab



(注) マルチネス博士は現在オーストラリアでシリコンでの量子計算機開発に従事

出所) UCSBニュース
<http://www.news.ucsb.edu/2014/014064/and-fritz-london-memorial-prize-goes-to%E2%80%A6>

9Qubit版の量子チップ



出所) UCSBマルチネス研究室
<https://web.physics.ucsb.edu/~martinigroup/index.shtml>

100キュービット以上のSycamoreなど量子プロセッサで量子プログラム利用可能

2030年頃には使える量子コンピュータができる可能性

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

- 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 |

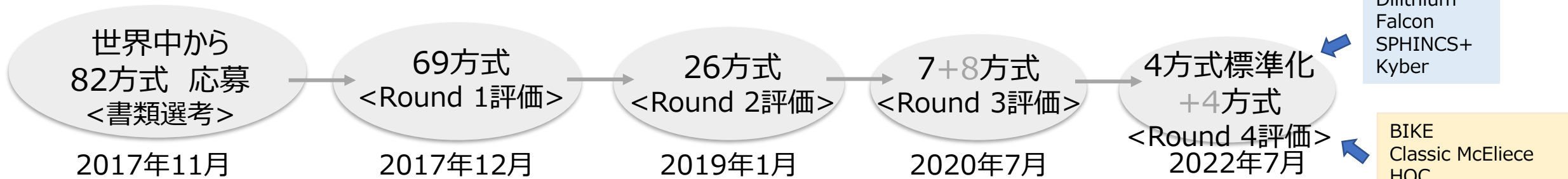
米国での暗号技術の標準化の動き

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に重大な欠陥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)



| | |
|--------------------|---|
| 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 |

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

諸外国政府の量子コンピュータ開発動向

○政府の取組



✓ **2018年9月**、国家科学技術会議が「**量子情報科学の国家戦略**

概要」を策定

✓ **毎年2億ドル(約218億円)**オーダーの投資を現在実施。2018年12月、**2019年より5年間で13億ドル(約1,400億円)**規模の投資に関する法律が成立



✓ **2017年6月**、欧州委員会の有識者会議が「**量子技術フラッグ**

シップ最終報告書」をとりまとめ

✓ **2018年から10年間で、10億ユーロ(約1250億円)規模**のプロジェクト「Quantum Technology Flagship」を開始



✓ 量子技術に関する大型プロジェクトを**2014年より総額2.7**

億ポンド(約456億円)で実施 (**5年計画**)



✓ **2018年9月**、「**量子技術の基本計画**」を閣議決定

✓ **2021年までに**、量子技術の研究開発のために**6.5億ユーロ(約845億円)**を投資



✓ 「**科学技術イノベーション第13次五カ年計画(2016年)**」において量子通信と**量子コンピュータを重大科学技術プロジェクト**とて位置づけている。

✓ 「**量子情報科学国家実験室**」を安徽省合肥市に**約70億元(約1,200億円)**かけて建設中(2020年完成予定)

情報漏洩・消失 今そこにある危機

(1) “Store now, decrypt later” attack

アメリカ国家安全保障局のデータセンター
140 テラバイト x 世界全人口分のデータを保存

今はまだ解読できなくてもデータを盗聴
保存しておき、将来高度な計算機で
過去に遡って全データを解読



- ・10年前に暗号化したデータはすでに解読されている可能性が高い
- ・すでに諜報機関が解読できる暗号方式を知らないまま使っている可能性も否定できない

耐量子-公開鍵暗号でも将来解読される可能性を否定できない

(2) 予期せぬ災害や障害

東日本大震災ではデータサーバが被災し、電子カルテや戸籍謄本が消失

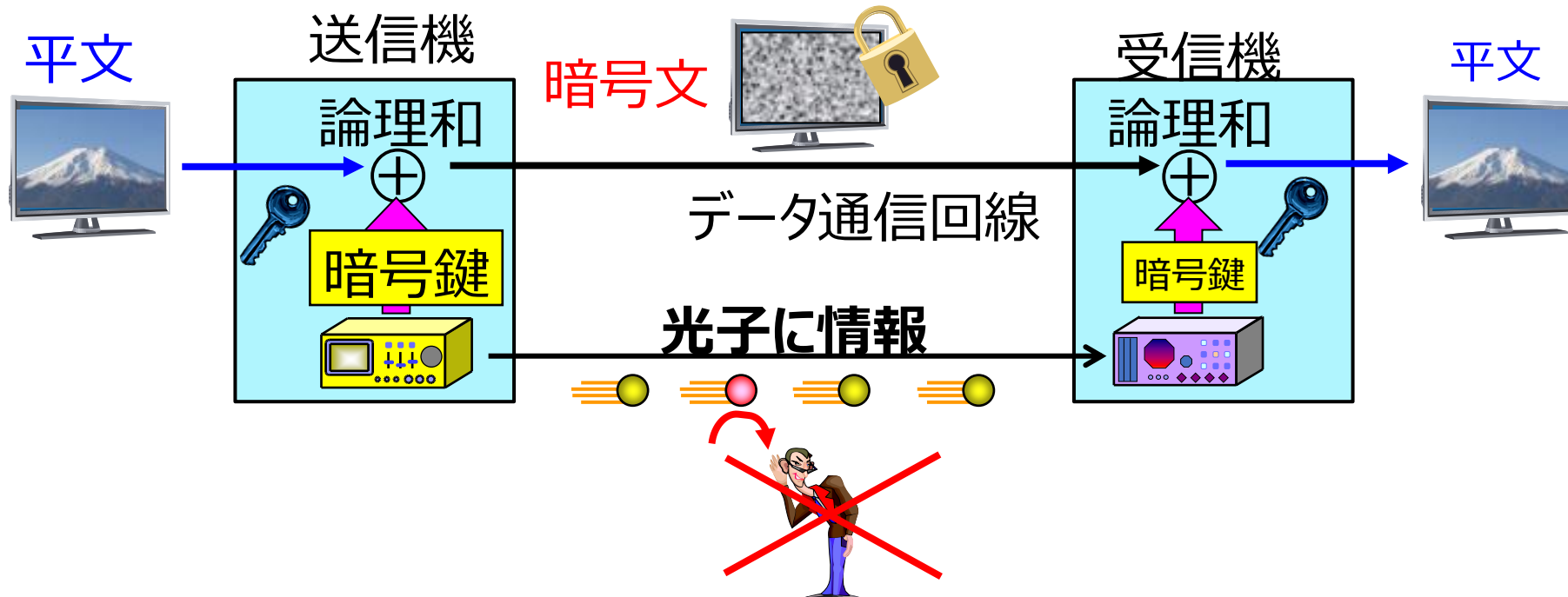
どんな計算機でも解読できない暗号通信・データバックアップ技術が必要

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
(一度使った鍵は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

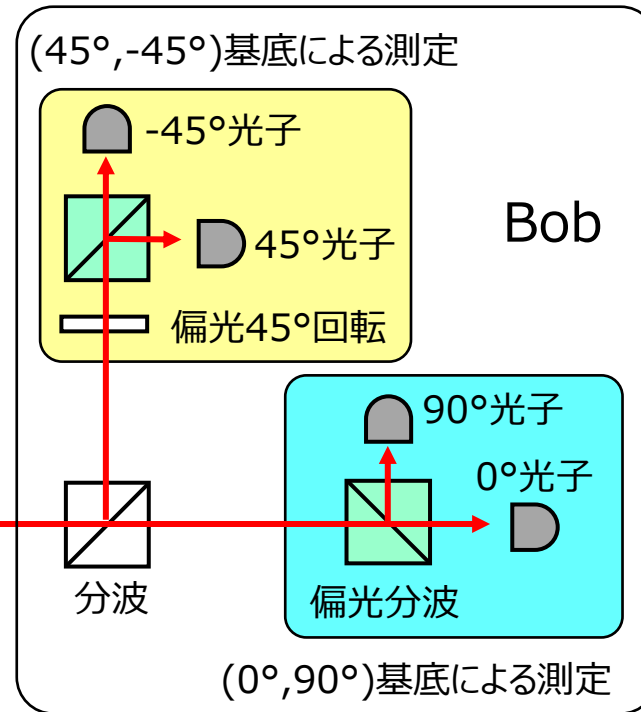
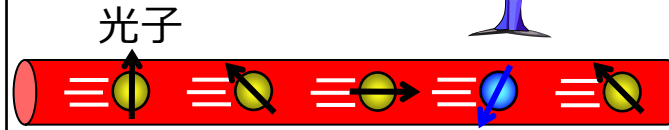
量子鍵配送の代表的なプロトコルBB84

光子の4つの偏光状態

| | | | |
|--------------|---|---------|-----------|
| Alice | | 基底 | |
| | | 0°, 90° | 45°, -45° |
| ビット値 | 0 | → | ↗ |
| | 1 | ↑ | ↖ |

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

Eve



互いに非直交な2つの『基底』

W. K. Wothers





















































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”



BB84プロトコル

| | | | | | | | | | | | | | | | |
|---------------------------|--------|--|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 送信者 Alice | 送信乱数 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| | 送信基底 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| | 送信状態 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 受信者 Bob | 受信基底 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| | 受信状態 |  | — | — |  |  |  | — |  |  |  | — |  | — |  |
| | 受信ビット | 1 | — | — | 1 | 0 | 0 | — | 1 | 0 | 0 | — | 1 | — | 0 |
| 送信者, 受信者の基底が一致するスロットのみを選択 | | | | | | | | | | | | | | | |
| 双方 チェック | テストビット | ○ | | | | ○ | | | | | ○ | | | | |
| | ふるい鍵 | | | | 1 | 0 | | | 1 | 0 | | | 1 | | 0 |

テストビットを選んで誤り率を評価

さらに鍵蒸留処理を施し, 安全な乱数列を生成

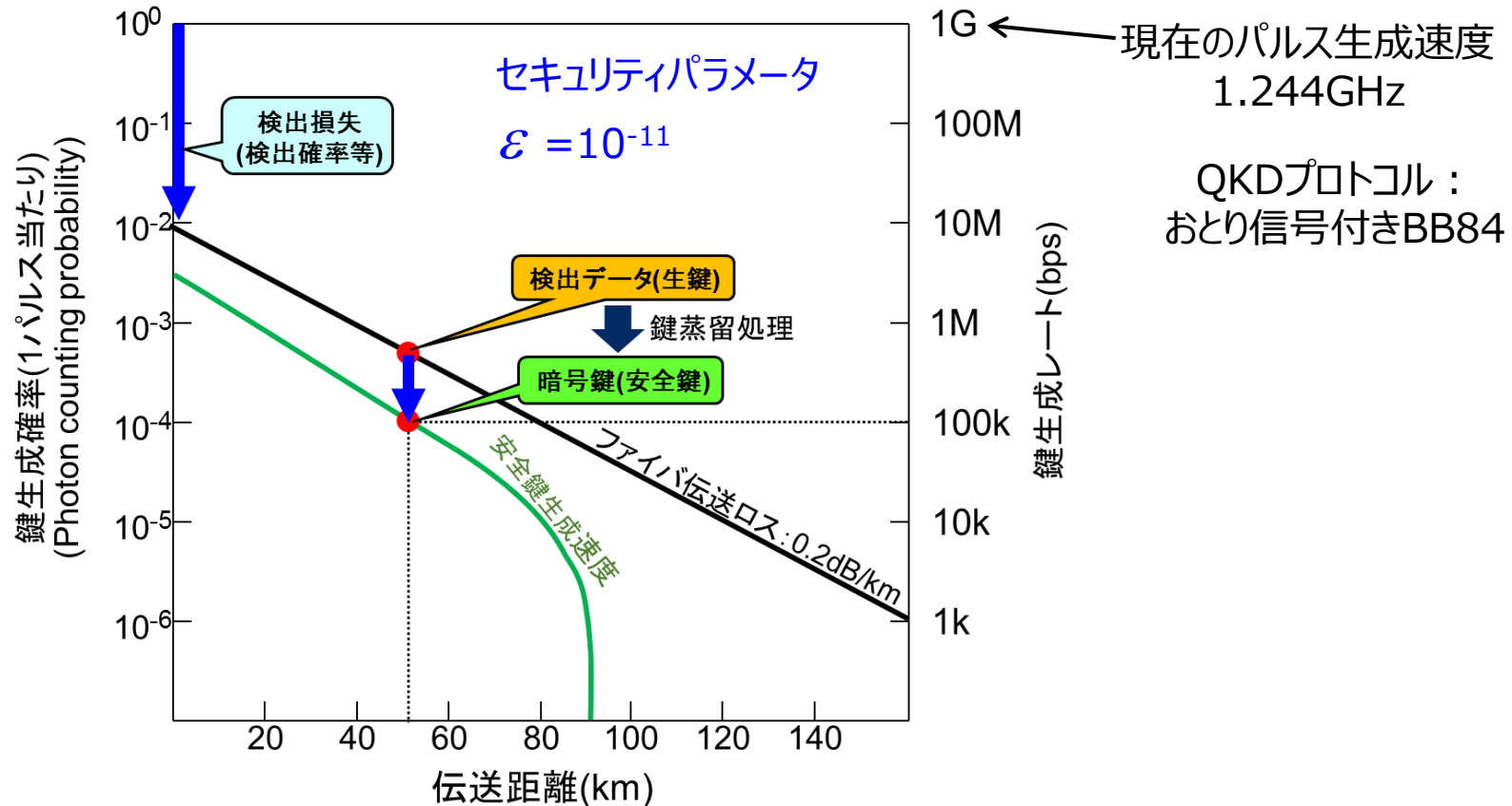
量子鍵配送装置の鍵生成レート

- ・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) × (通信路透過率)

$$\times [1 - (\text{誤り訂正レート}) - (\text{秘匿性増強レート})]$$

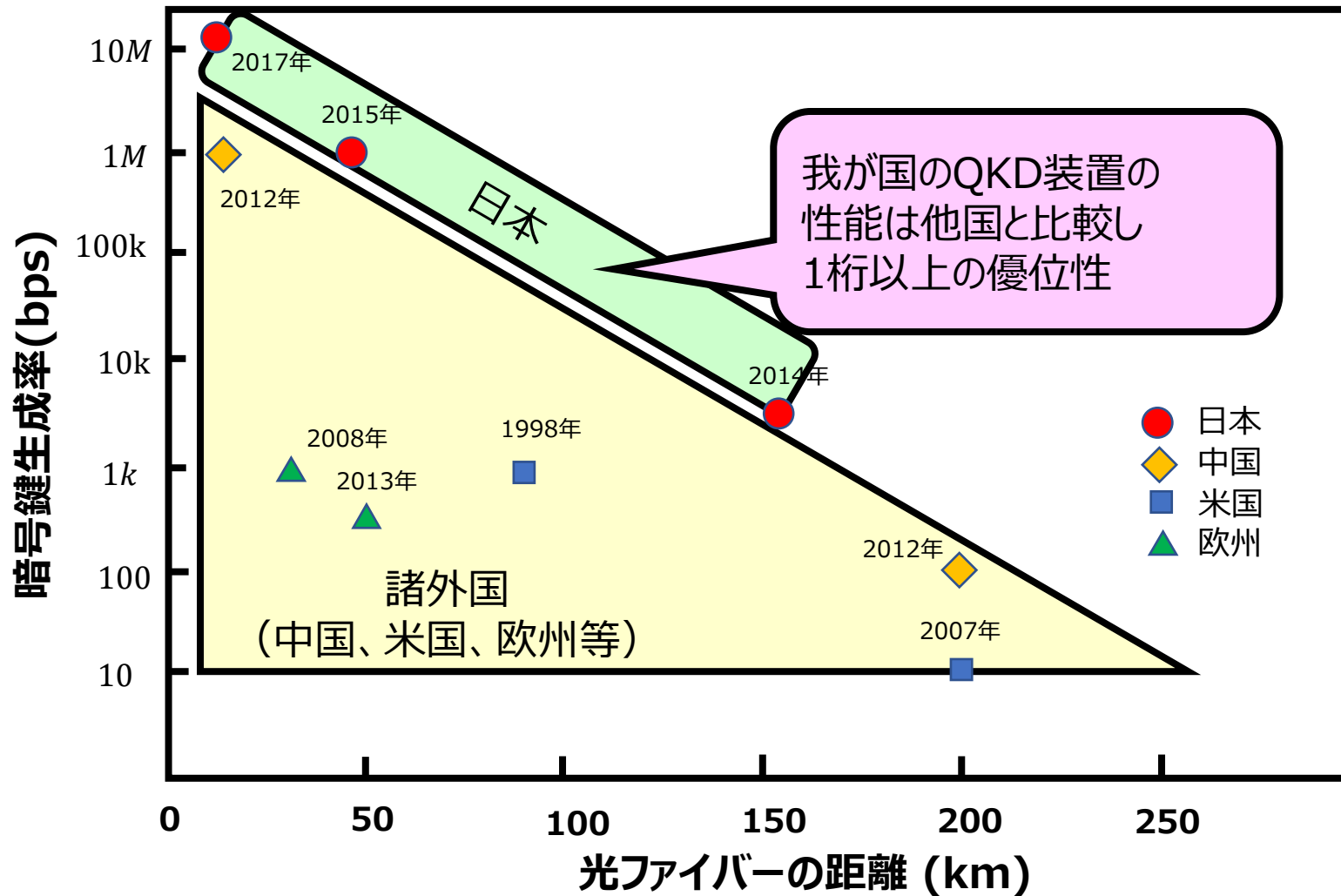
観測されたビット誤り率から直接計算

安全性理論に基づいてビット誤り率から推定



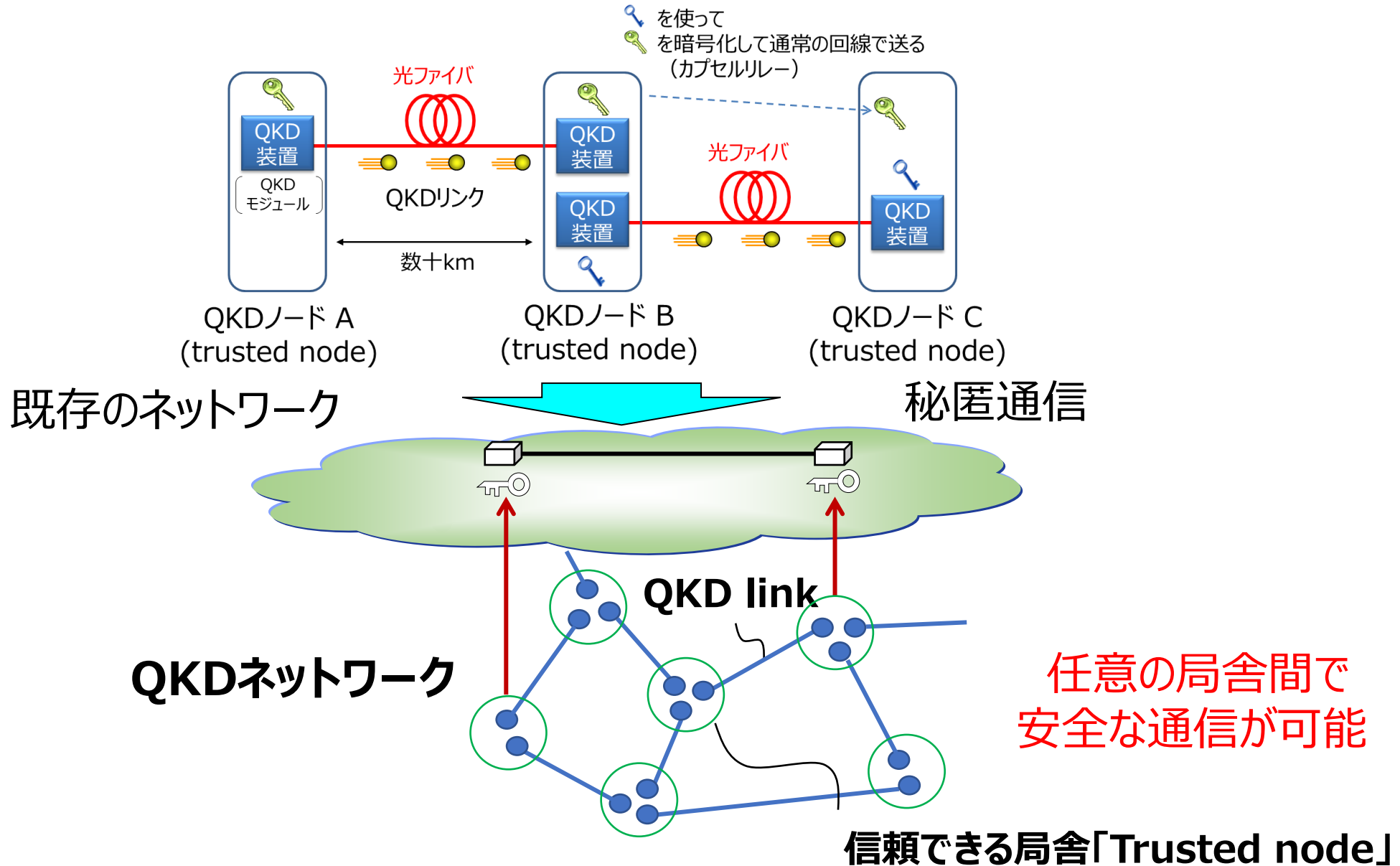
我が国の量子鍵配送装置の優位性

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



QKD network testbed in USA



University of Chicago and Argonne National Laboratory developed a quantum Internet prototype, and this group succeeded in entangled photon pair sharing through a field installed fiber of 52 miles (about 84 km) in February 2020.



124-mile quantum network was established in 2022, and QKD experiments are being conducted in collaboration with Toshiba Corporation.

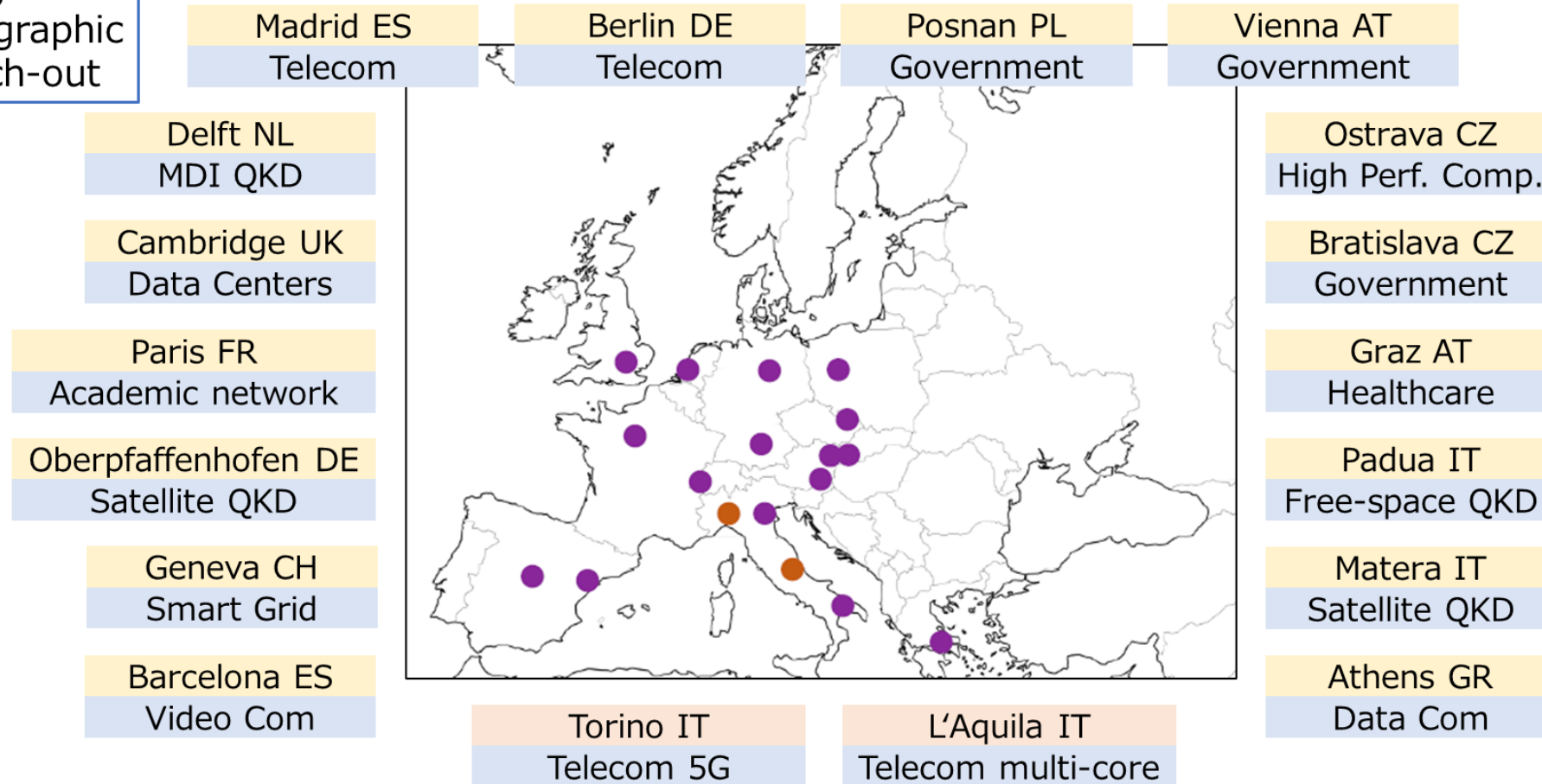
Testbed toward a secure quantum internet (<https://news.uchicago.edu/story/chicago-quantum-network-argonne-pritzker-molecular-engineering-toshiba>)

Quantum Internet will be built primarily by 17 national laboratories under the Department of Energy

QKD network testbed in EU

18 OpenQKD testbed sites

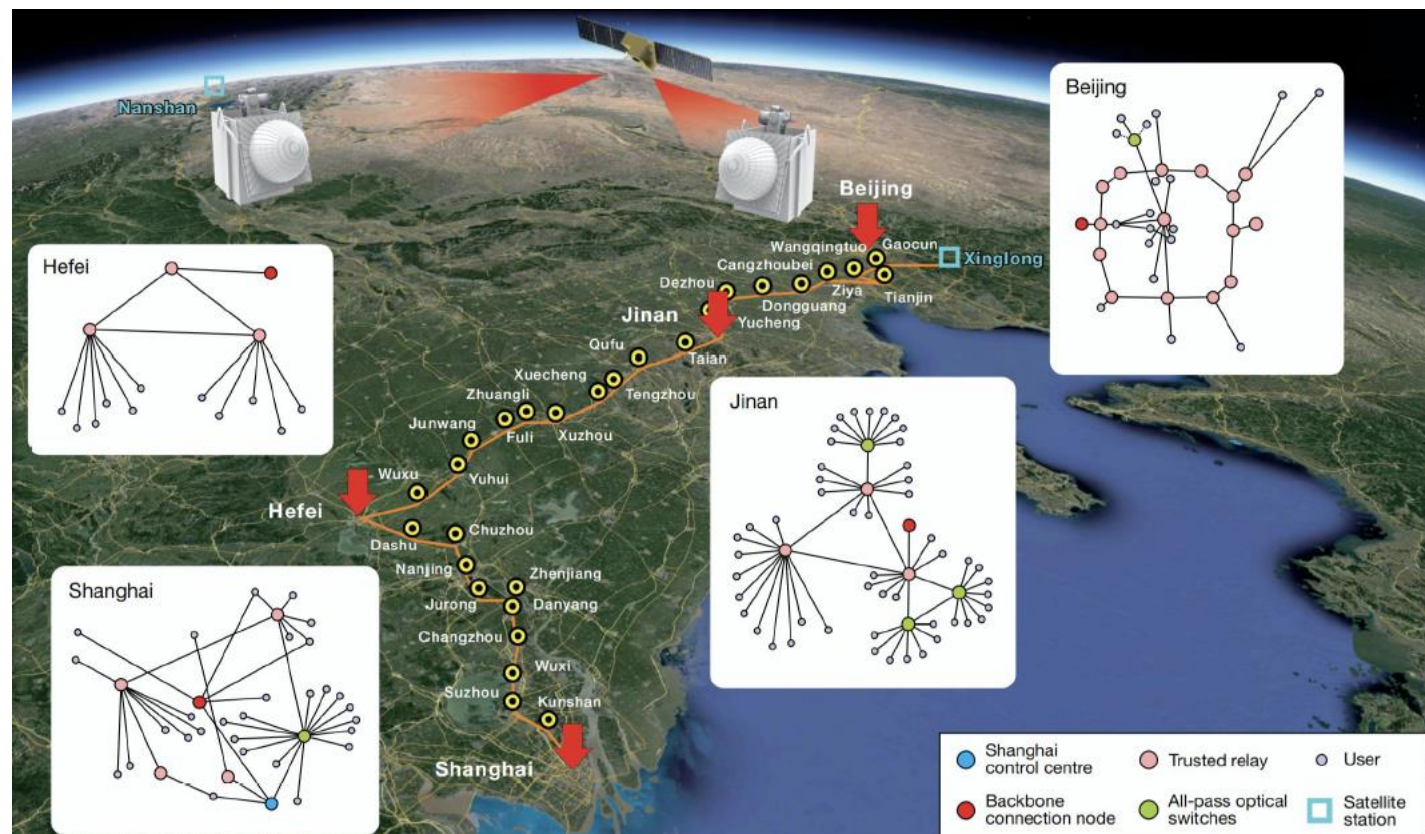
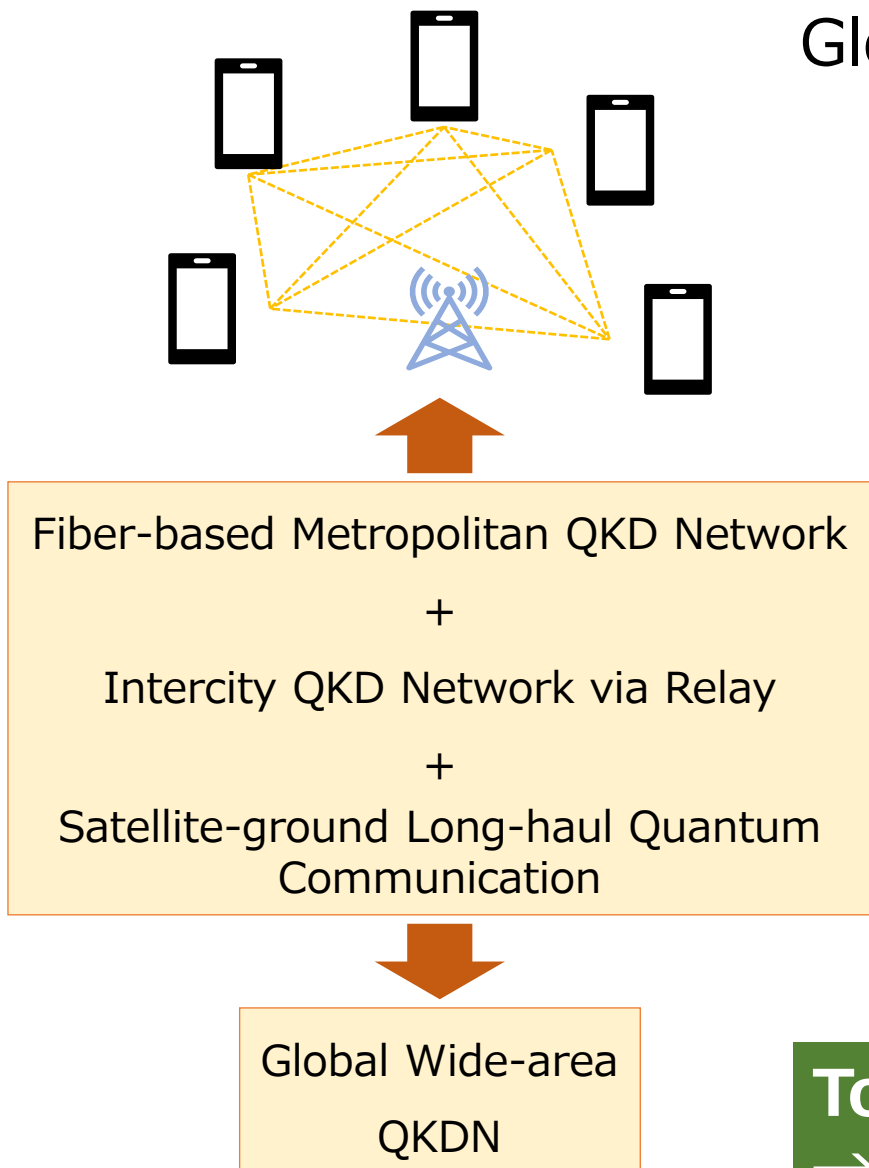
Large geographic reach-out



OPEN QKD
 Use-cases in the Open European
 Quantum Key Distribution Testbed
 Andreas POPPE slide (ITU Webinars, May 26, 2021)

Satellite – fiber base QKD network integration

Global Wide-area QKDN Infrastructure

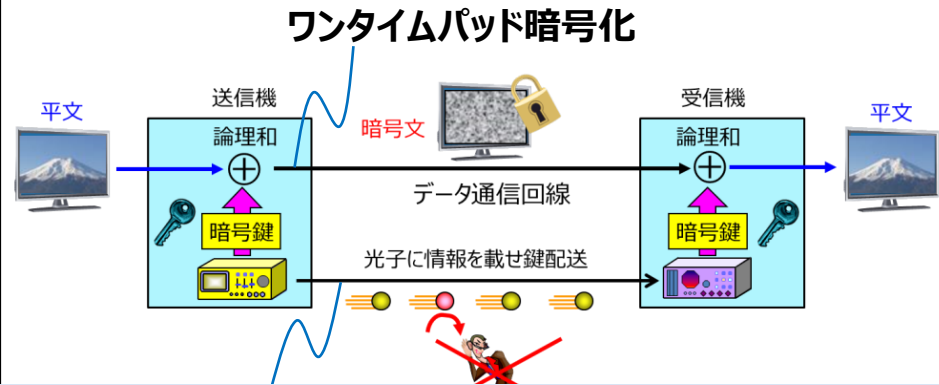


An integrated space-to-ground quantum communication network over 4,600 kilometers. Nature(2021)

Total length 4600km
→ secure communication infrastructure

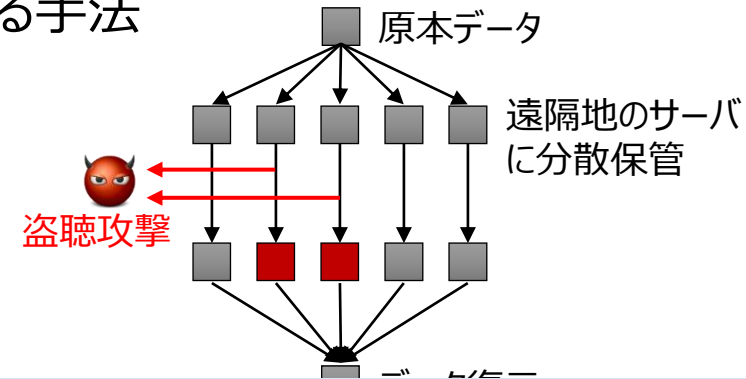
量子暗号

『**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

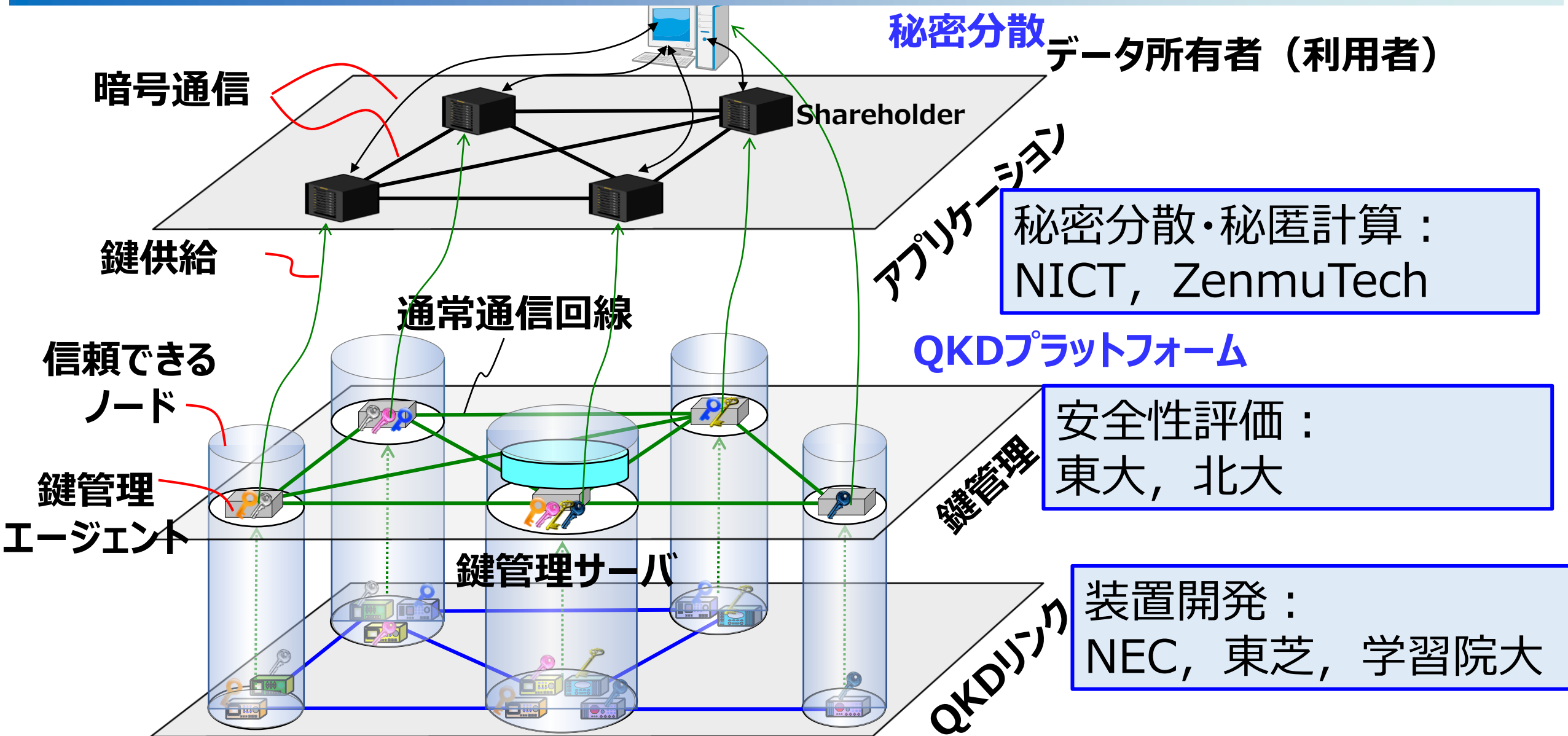


**超長期に秘匿すべきデータの保護・利用をデモ
(電子カルテ, ゲノム関連データ, 生体認証データ等)**

『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



量子暗号・量子セキュアクラウドの社会実装計画

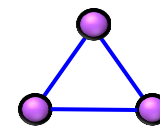
- (1) 電子カルテ（模擬）の秘密分散保管
- (2) ゲノムデータ（模擬）の秘密分散保管
- (3) レーザ加工拠点の重要回線の秘匿化
- (4) 生体認証の参照データの秘密分散保管

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



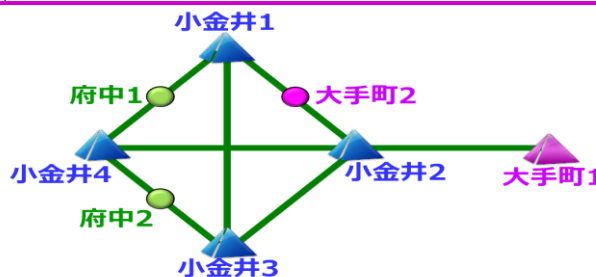
(2) ゲノム解析データの
暗号通信、秘密分散

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

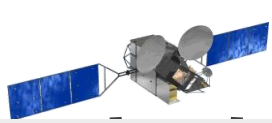


東京 100km圏

- (1) 電子カルテ模擬データの秘匿化・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

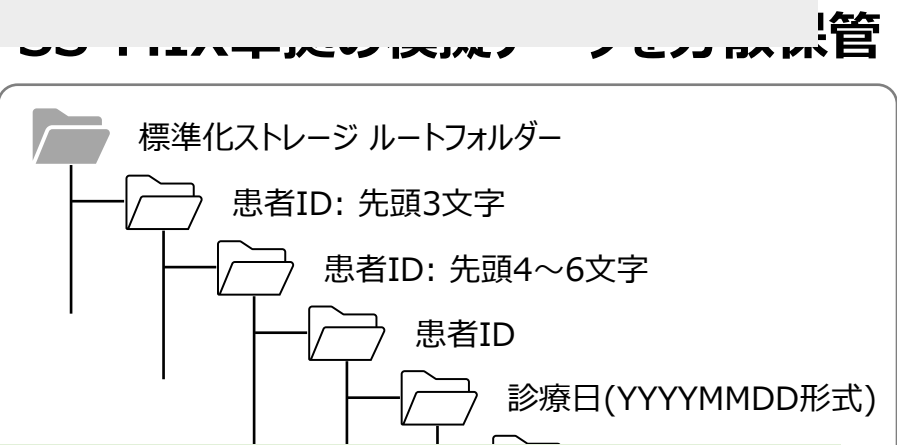
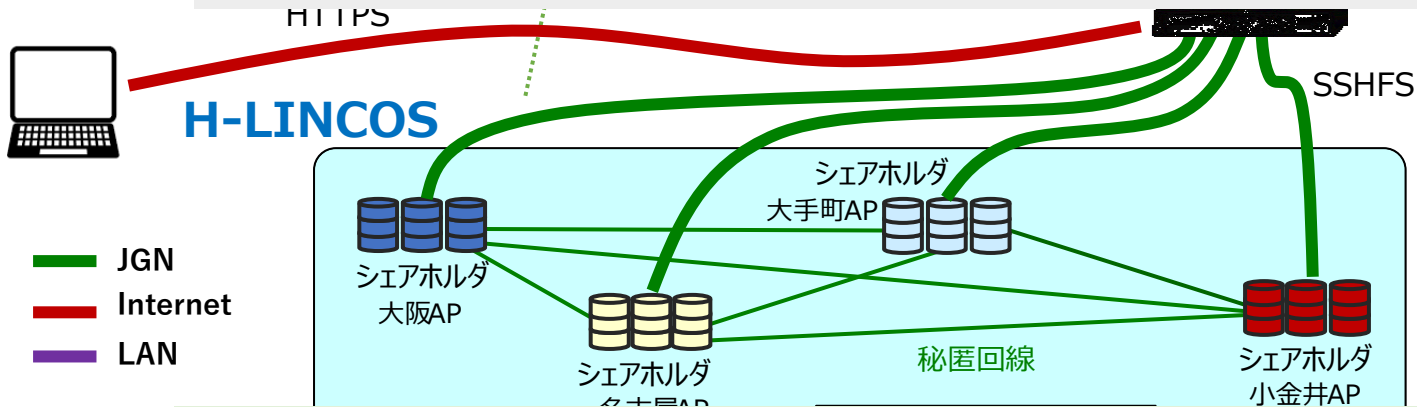


格納データ諸元：

- ・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



衛星管理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)

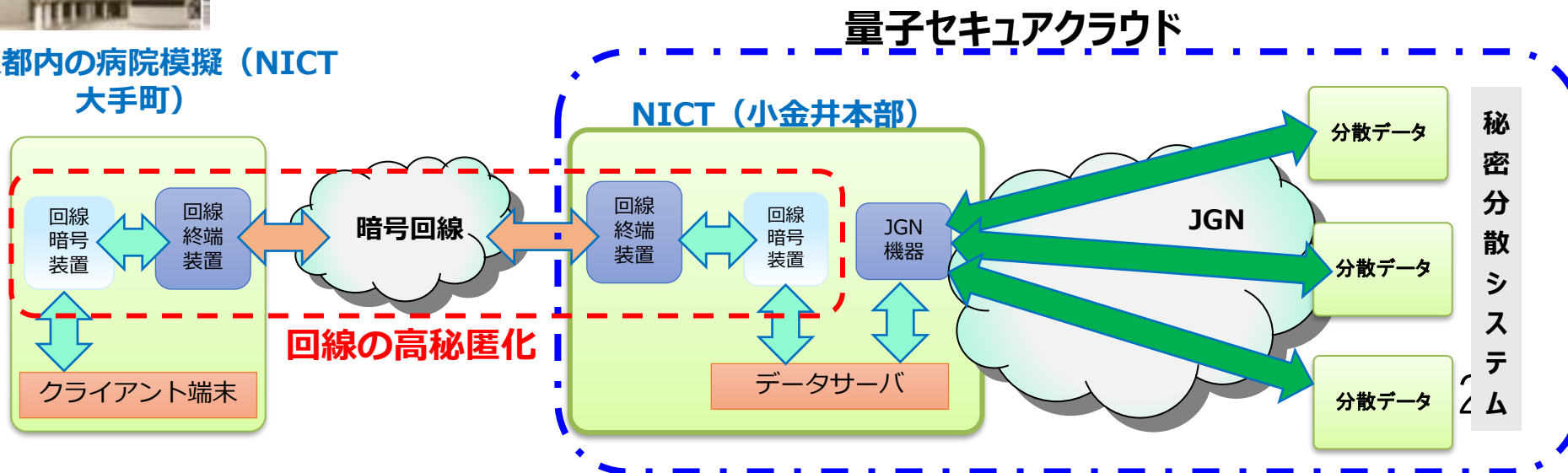
(1) 電子カルテデータへの適用

- 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認。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)

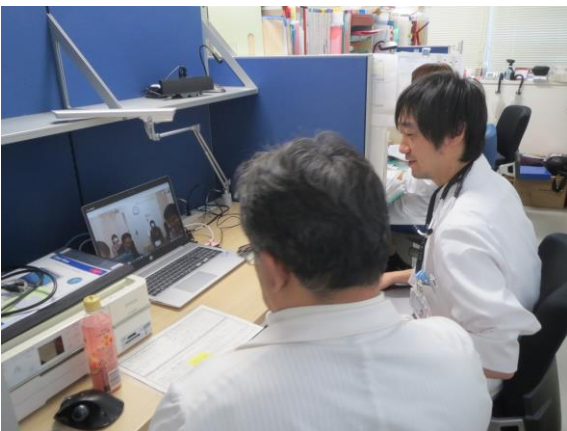
2020年10月22日プレスリリース



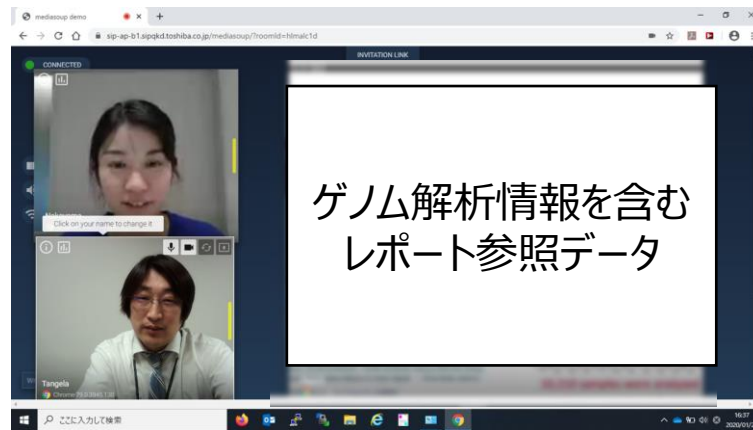
(2) ゲノム医療への適用

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

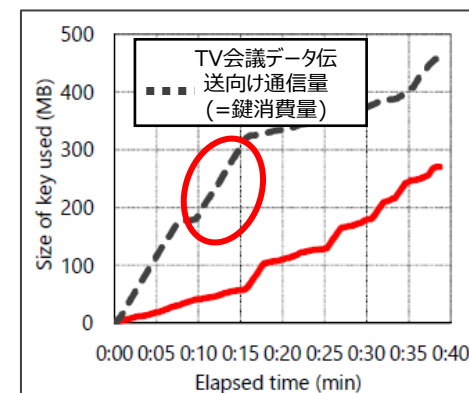
- 医師含む延べ10名が参加し延べ65分間のTV会議を実施
医師による主観評価において、良好に利用できることを確認
- 平均鍵消費速度は約1.6Mbps。東芝製量子暗号装置の鍵配信速度(最大10Mbps)によって問題なくサポート可能であることを確認



大学病院拠点の実証の様子



TV会議画面例



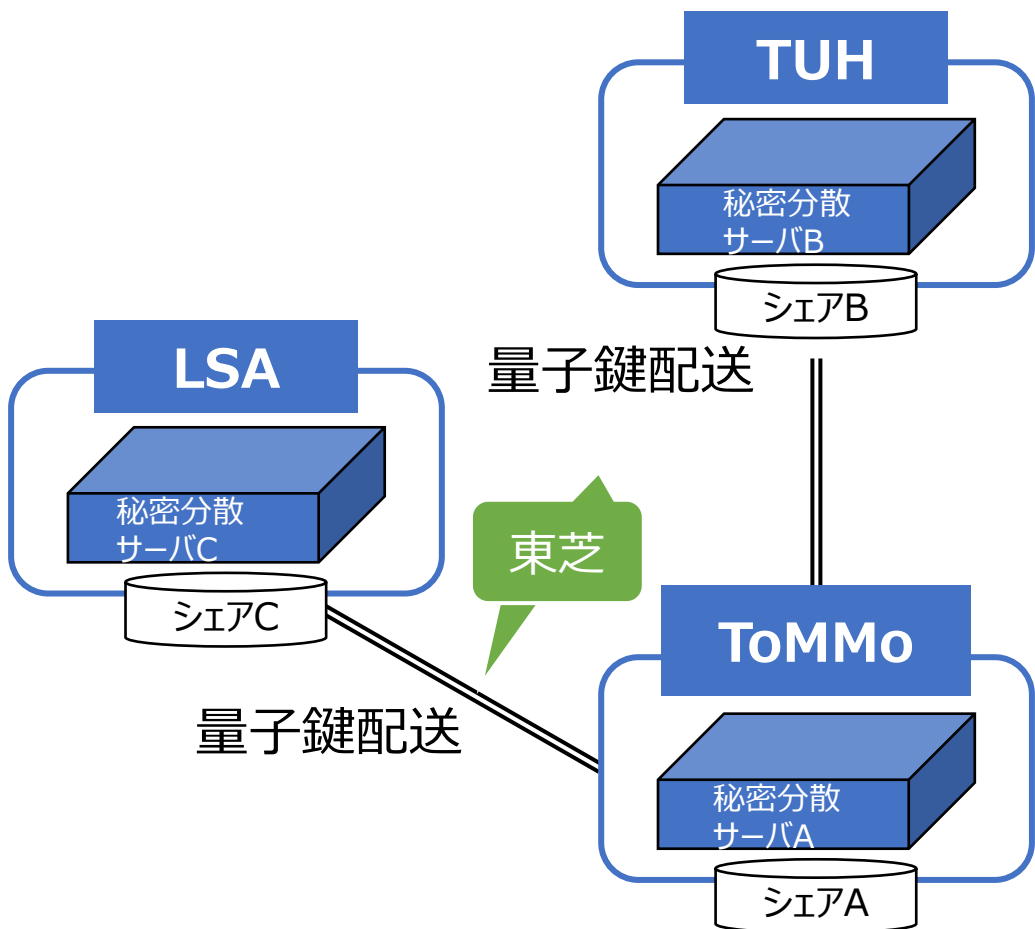
TV会議データ伝送時の暗号鍵消費量

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

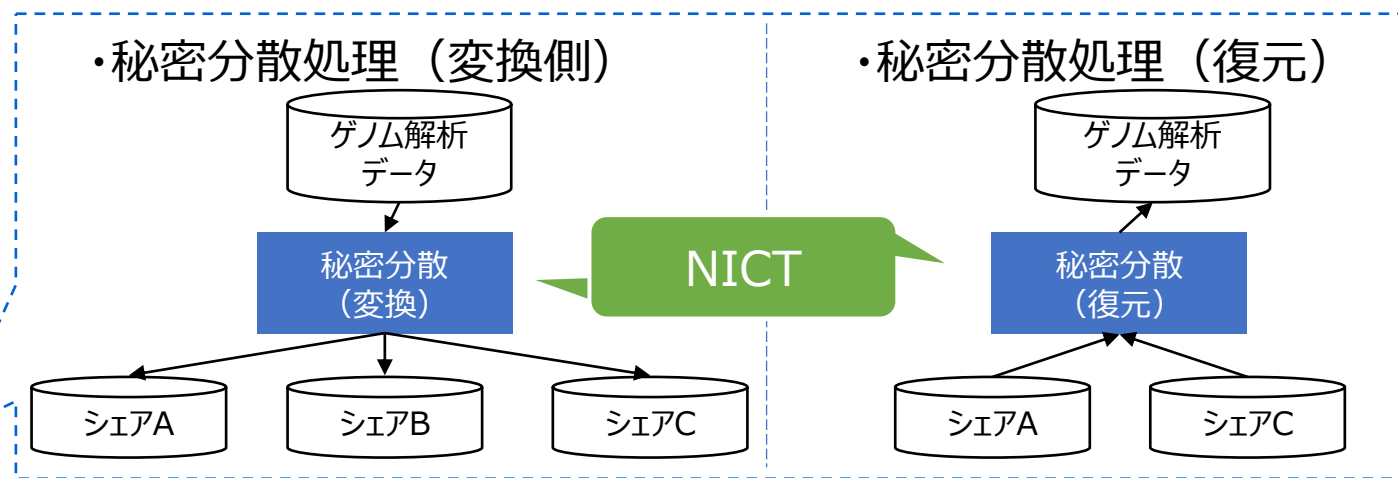
(2) ゲノム医療への適用

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

秘密分散サーバ A (ToMMo)



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

(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**


NEC SMART COMMAND CENTRE nls

Home / Unauthorised Access Detection 5795

ALERT ID 5795 Last Updated: 2019-10-21 10:58:58 Find Faces Close Alert

OPEN **UNAUTHORISED_ACCESS** HIGH

Snapshot Footage CAMERA_01 Annotation ON




Alert Timestamp 2019-10-21 10:58:56

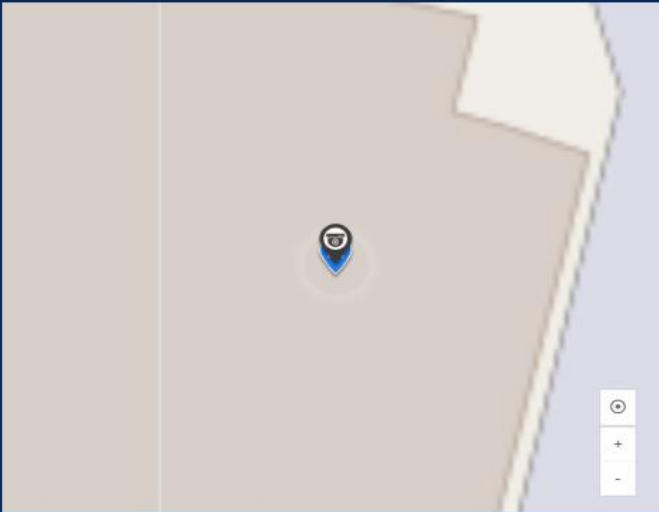
DETECTED SCORES

| | | |
|------------------------|------------------------|-------------------------|
| 100.0 % CREDIBILITY | 71.7 % FACE QUALITY | 43.3 % FRONTAL SCORE |
|------------------------|------------------------|-------------------------|

MATCHING PROFILES

 **NOT REGISTERED**
Repository N/A

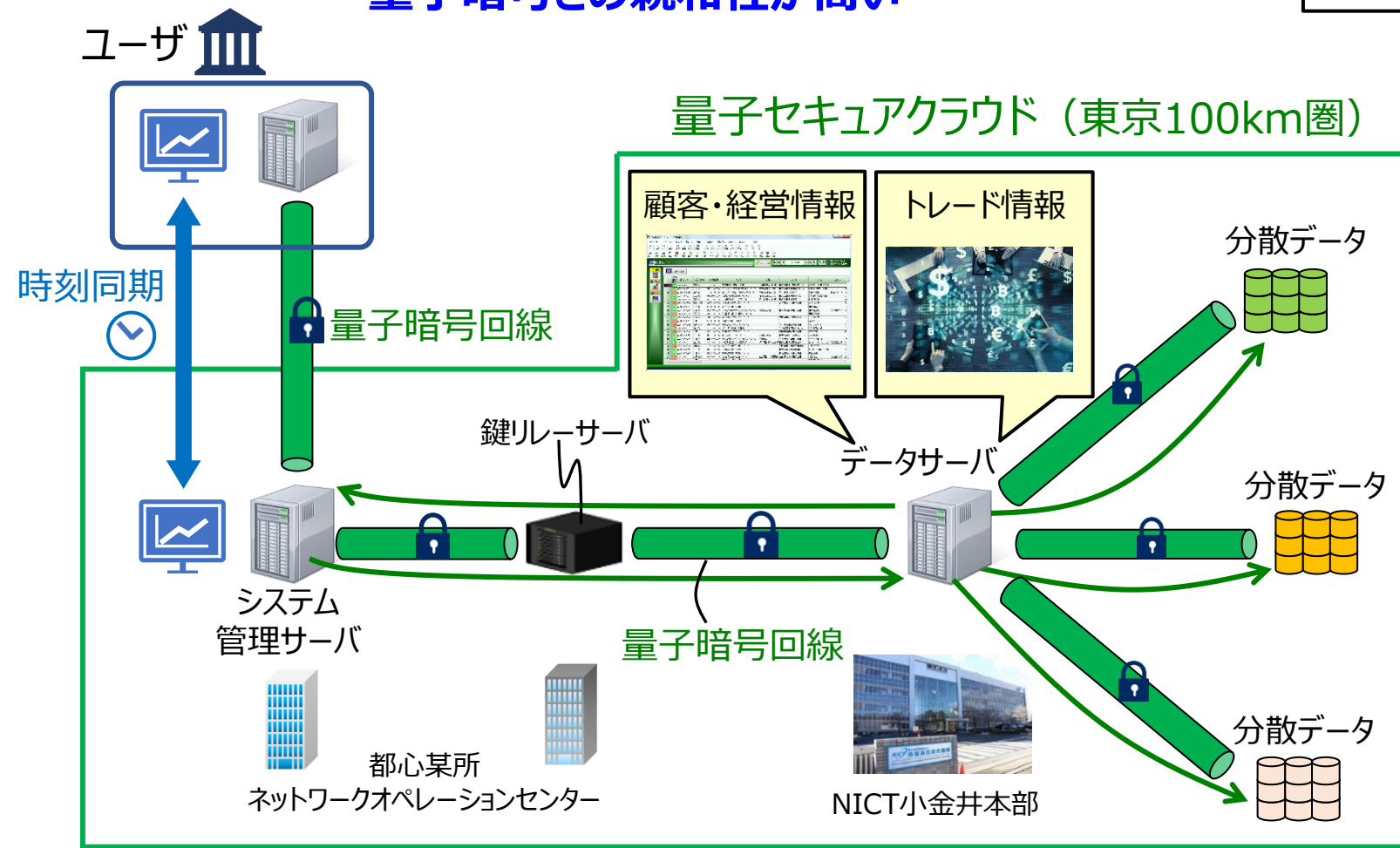
Register as POI Edit POI



(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

✓ **野村証券 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

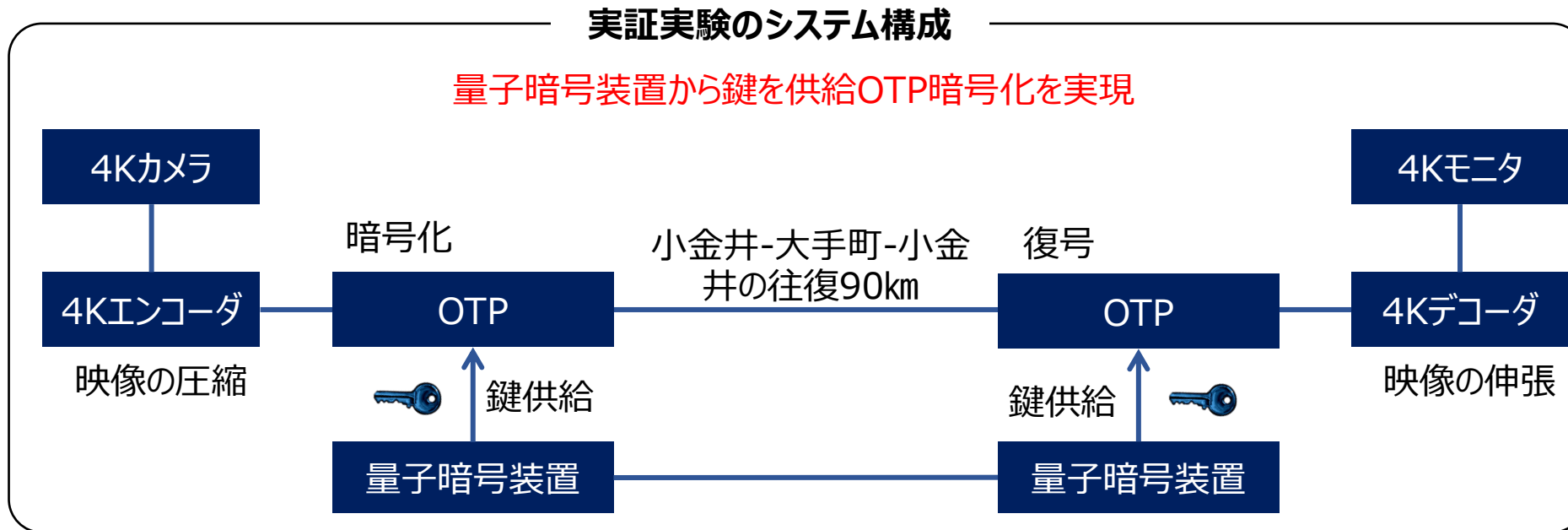
- 技術的な評価に成功
→個人情報保護への適用など
ガイドラインの整備も含め実施予定

2022年1月14日 プレスリリース

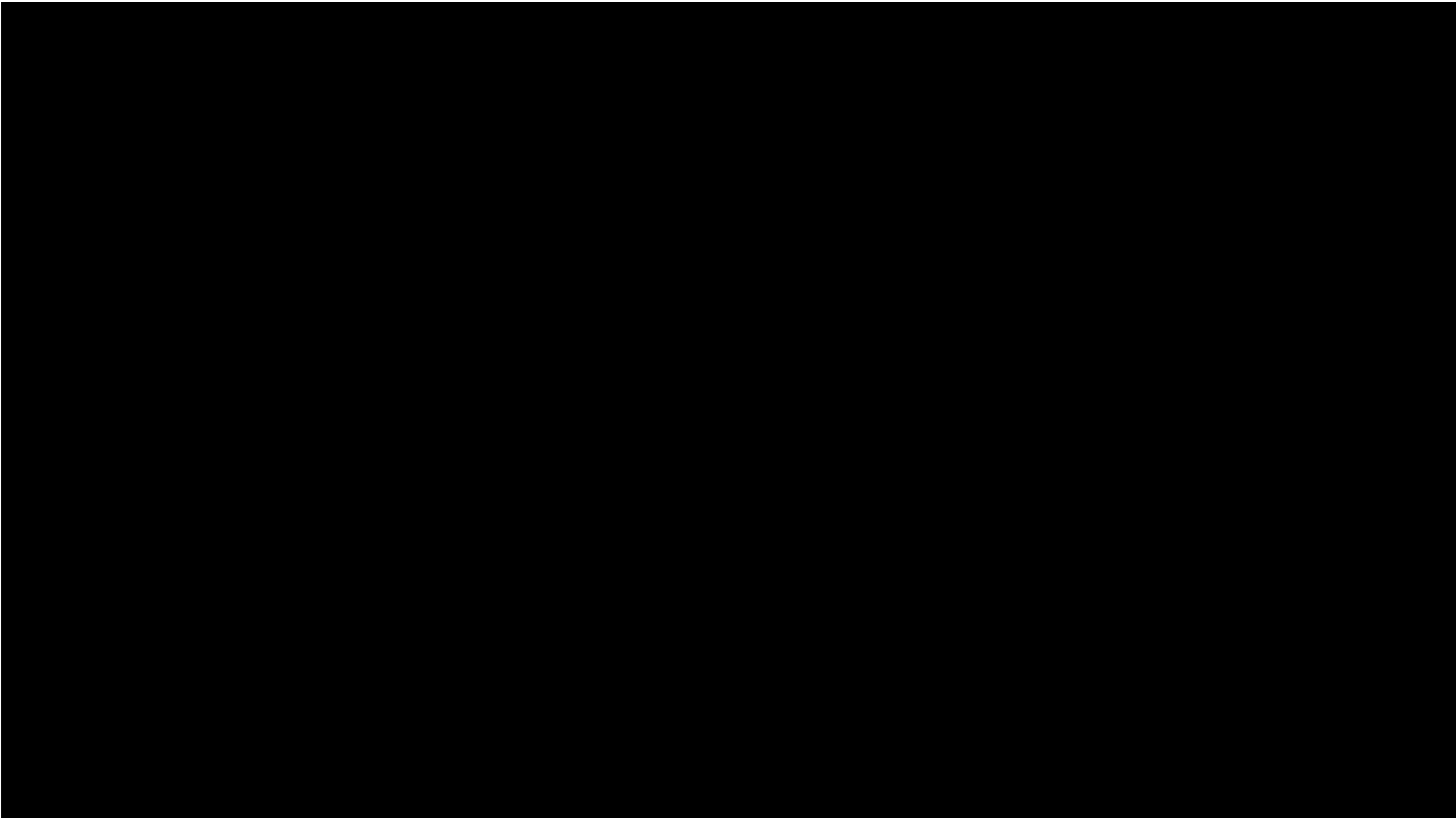
遅延性の実験 QKD + OTP の4K画像高速伝送

✓ 量子鍵配送 + OPT暗号, 4K映像の高秘匿圧縮伝送を実証

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



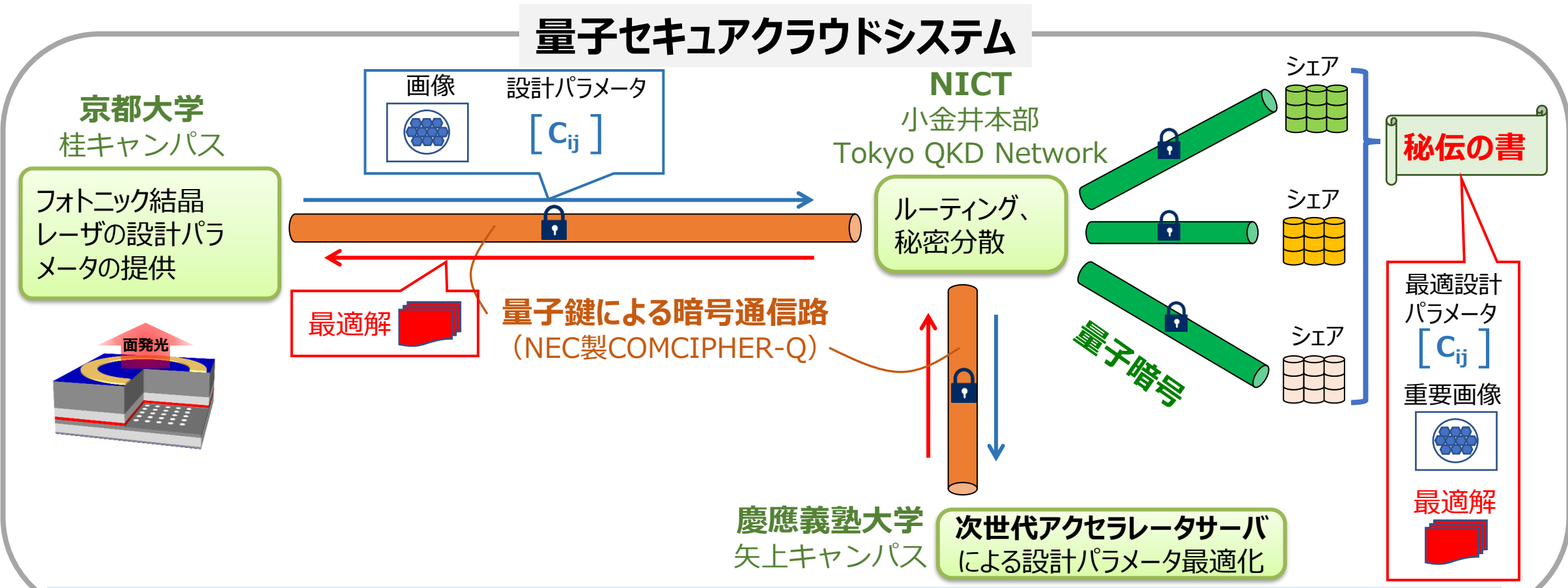
4K高精細動画高秘匿伝送技術 遠隔医療にも活用可能か？





(5) スマート製造への展開

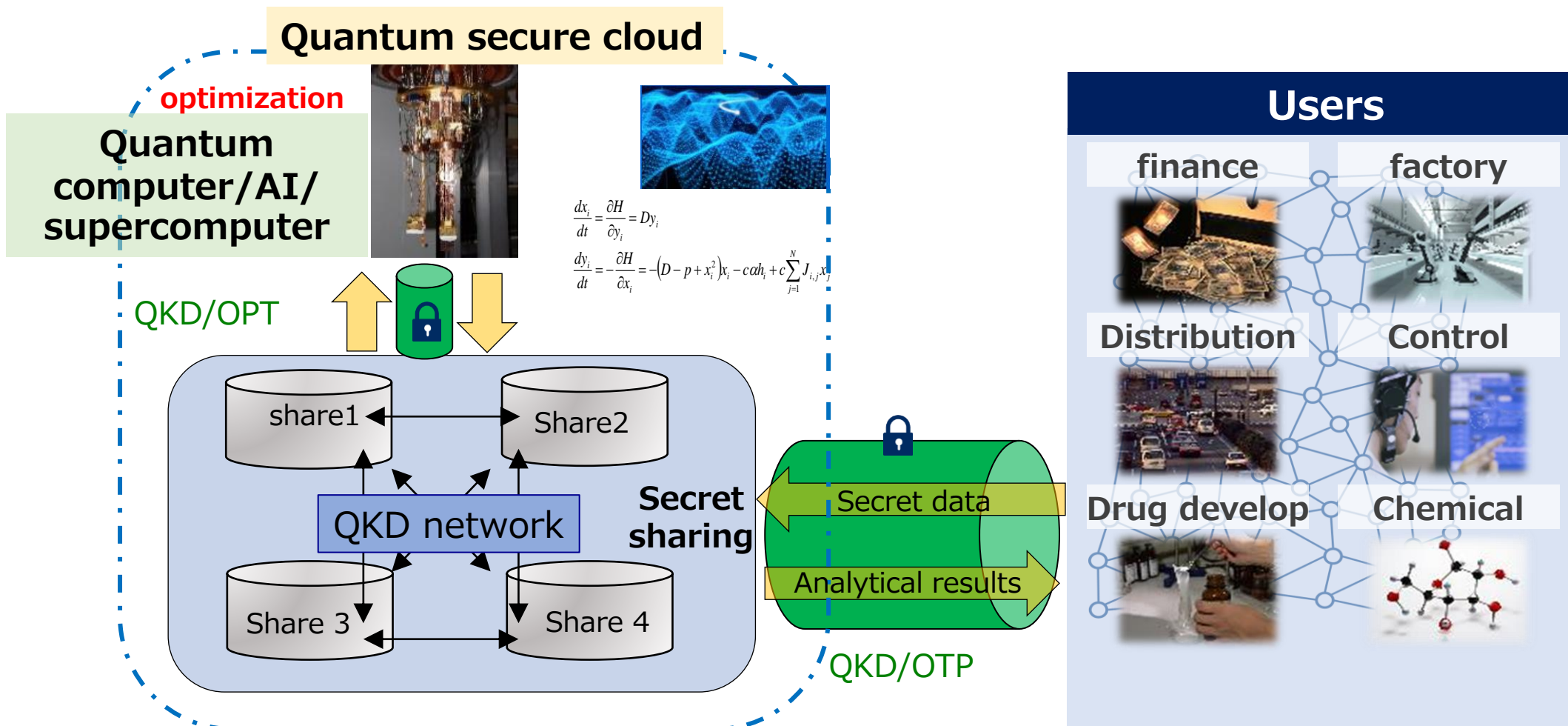
(次世代アクセラレータと連携した量子セキュアクラウドによりフォトニック結晶レーザーの設計情報の処理・伝送・保管を実現)



次世代アクセラレータと連携した量子セキュアクラウドにより
スマート製造分野における適用可能性を確認 明日プレスリリース予定

Quantum secure cloud image

Future image of a quantum secure cloud with secure computation function. Several specialized computers (including quantum computers) are embedded in the quantum secure cloud.



- 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**

遠赤外検出器や量子暗号の研究開発を経て実感したこと

全ての研究開発は3つの段階を経る

第一段階 笑いものにされる

第二段階 大反対される

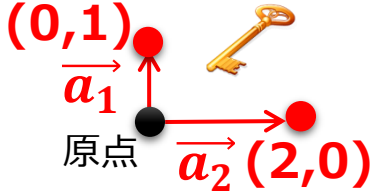
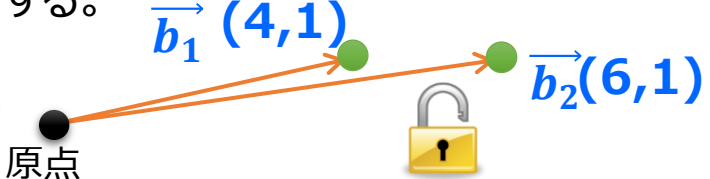
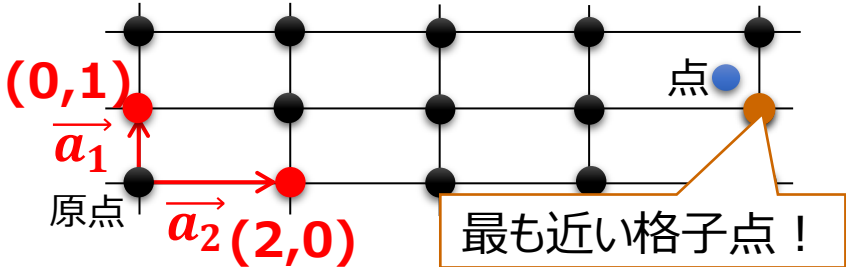
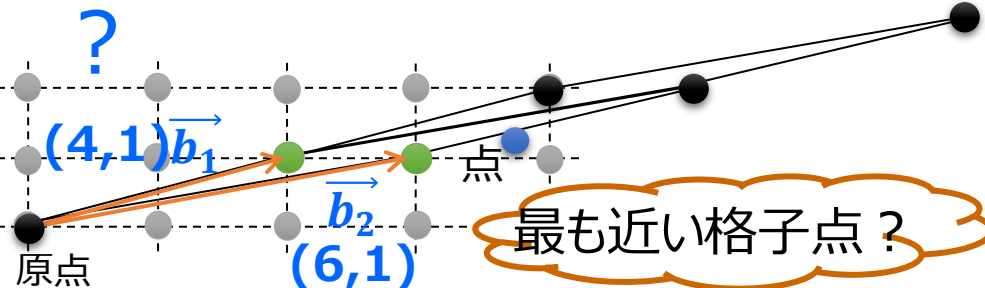
第三段階 判り切ったこととして受け入れられる



色々めげずに頑張るしかないですねえ…

格子暗号：鍵の設定（イメージ）

鍵の設定：

| 秘密鍵 | 公開鍵 |
|--|--|
| <p>① 秘密鍵として直交している基底ベクトル (\vec{a}_1, \vec{a}_2) を選ぶ。</p>  | <p>② (\vec{a}_1, \vec{a}_2) を利用して、同じ格子を表現できる直交していない基底ベクトル (\vec{b}_1, \vec{b}_2) を計算する。</p>  <p>容易 → 困難</p> <p>どの直交ベクトルを使っているのか特定できない</p> |
| <p>特徴</p> <ul style="list-style-type: none"> □ 格子上の任意の格子点を表現しやすい（格子の全体像を把握するのが容易）。 <p>ある点に近い格子点を見つけやすい</p>  <p>最も近い格子点！</p> | <p>特徴</p> <ul style="list-style-type: none"> □ 格子上の任意の格子点を表現しにくい（格子の全体像を把握するのが困難）。 <p>ある点に近い格子点を見つけにくい</p>  <p>最も近い格子点？</p> |

格子暗号ではこれらの特徴を利用

格子暗号：暗号化処理（イメージ）

■ 暗号化処理：

1. 暗号化したい平文を2つの整数 (m_1, m_2) で表現。
2. 公開鍵 (\vec{b}_1, \vec{b}_2) を利用して、格子点 P を以下のように計算。

$$\text{格子点 } P = m_1 \times \vec{b}_1 + m_2 \times \vec{b}_2$$

3. 小さな実数ベクトル \vec{r} をランダムに選び、暗号文 $C = P + \vec{r}$ を計算。

