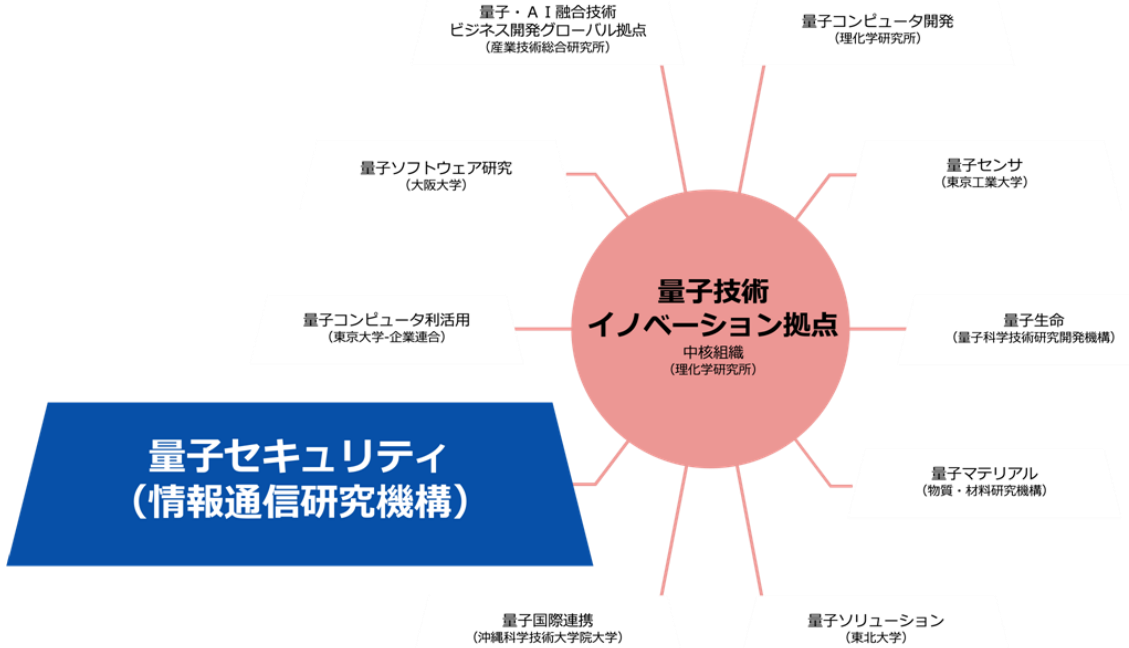
量子暗号技術
拡張された東京QKDネットワーク

情報通信研究機構
量子ICT協創センター　藤原幹生

NICT National Institute of Information and Communications Technology

量子セキュリティ拠点　（NICT）

内閣府の「統合イノベーション戦略推進会議」で
策定された「量子技術イノベーション戦略」の中で
NICTは「量子セキュリティ拠点」に指定されました.
2022年3月に竣工した本建屋は
量子セキュリティ拠点の中核を担っています.



以下の11企業と拠点連携参画規約を締結

- KDDI株式会社
- さくらインターネット株式会社
- スカパーJSAT株式会社
- 株式会社大和証券グループ本社
- 株式会社東芝
- 凸版印刷株式会社
- 日本電気株式会社
- 野村ホールディングス株式会社
- 株式会社マクニカ
- 株式会社みずほフィナンシャルグループ
- 株式会社ワイ・デー・ケー

暗号とは　通信に必要な技術

- データを秘匿化するために必要なもの
  - 暗号アルゴリズム＋鍵

暗号は身近なところで既に利用

ネット社会に必須の技術
しかし**現在使われている暗号が将来も安全とは言えない**
暗号を解読するコンピュータ技術も進歩しているため（量子コンピュータなど）

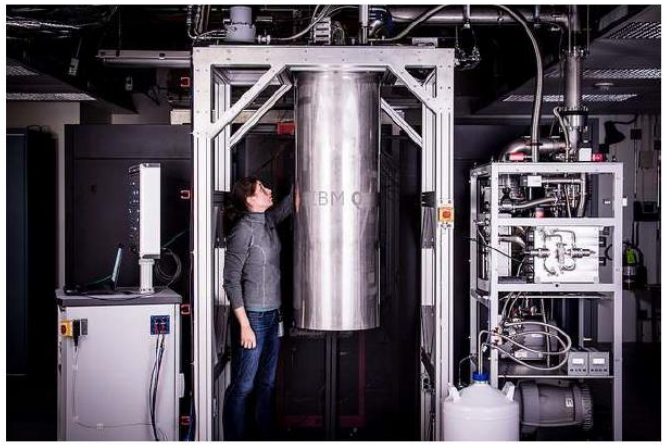
守るべき情報資産

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

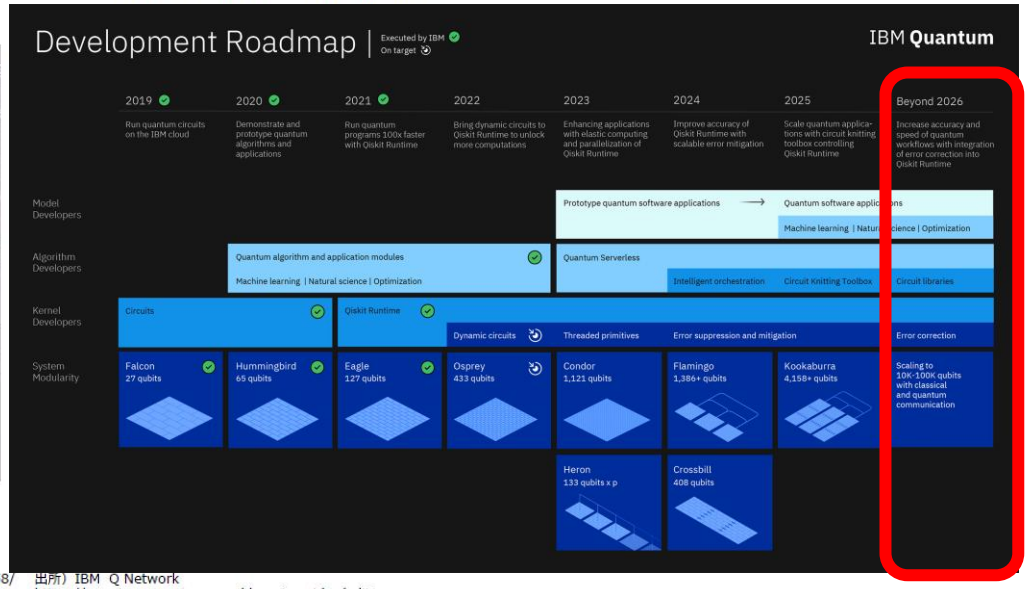
何故量子暗号が必要か？　進む量子コンピュータ開発

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/



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

11

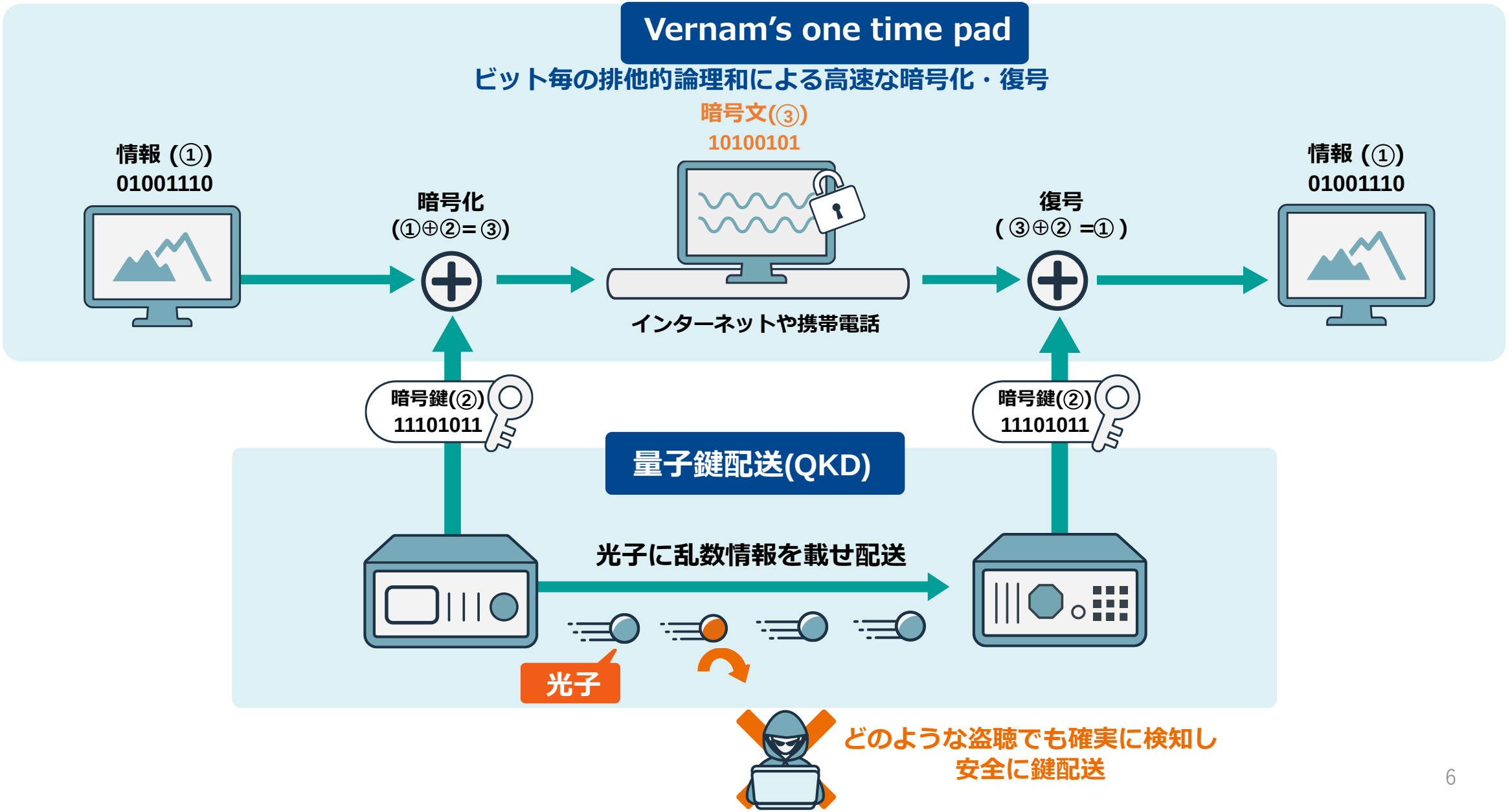
「IBM Q」公開中　**誰でも無償でIBM社にある量子コンピュータを実際に利用**
数年以内に1000qbitsに達する計画

2030年頃には使える量子コンピュータができる可能性

- **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暗号（公開鍵暗号）の安全性が急低下**
  →通信の秘匿性が担保できなくなる

本年６月９日参議院本会議可決「良質かつ適切なゲノム医療を国民が安心して受けられるようにするための施策の総合的な推進に関する法律」に応えられる暗号技術が必須

量子鍵配送・量子暗号


Vernam's one time pad
ビット毎の排他的論理和による高速な暗号化・復号
暗号文(③)
10100101
情報 (①)
01001110
暗号化
(①⊕②= ③)
インターネットや携帯電話
復号
(③⊕② =①)
情報 (①)
01001110
暗号鍵(②)
11101011
暗号鍵(②)
11101011
量子鍵配送(QKD)
光子に乱数情報を載せ配送
光子
どのような盗聴でも確実に検知し
安全に鍵配送

量子鍵配送装置の鍵生成レート

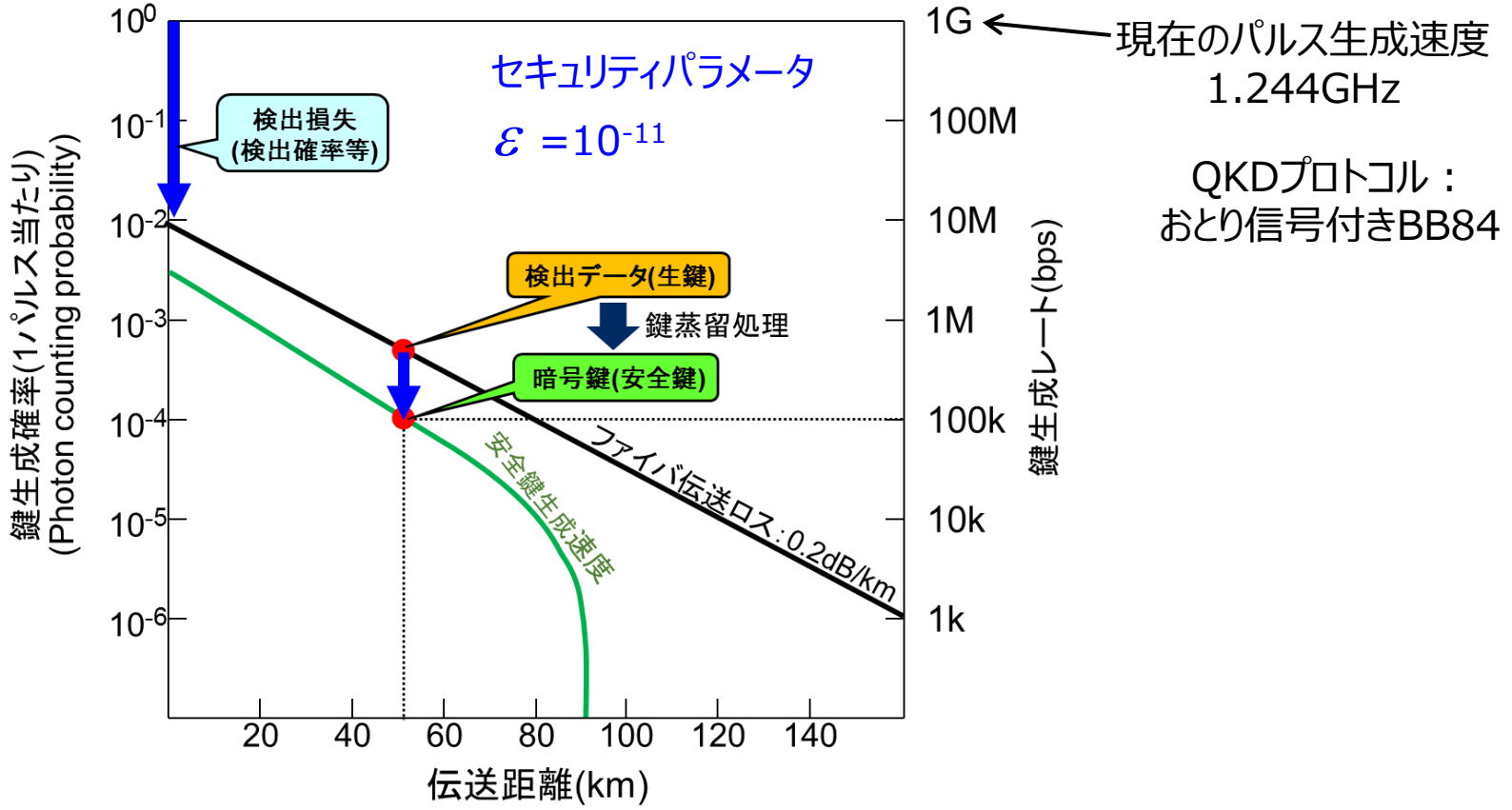
・安全性を向上（セキュリティパラメータεを小さく）させると鍵生成速度は下がる

・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)]

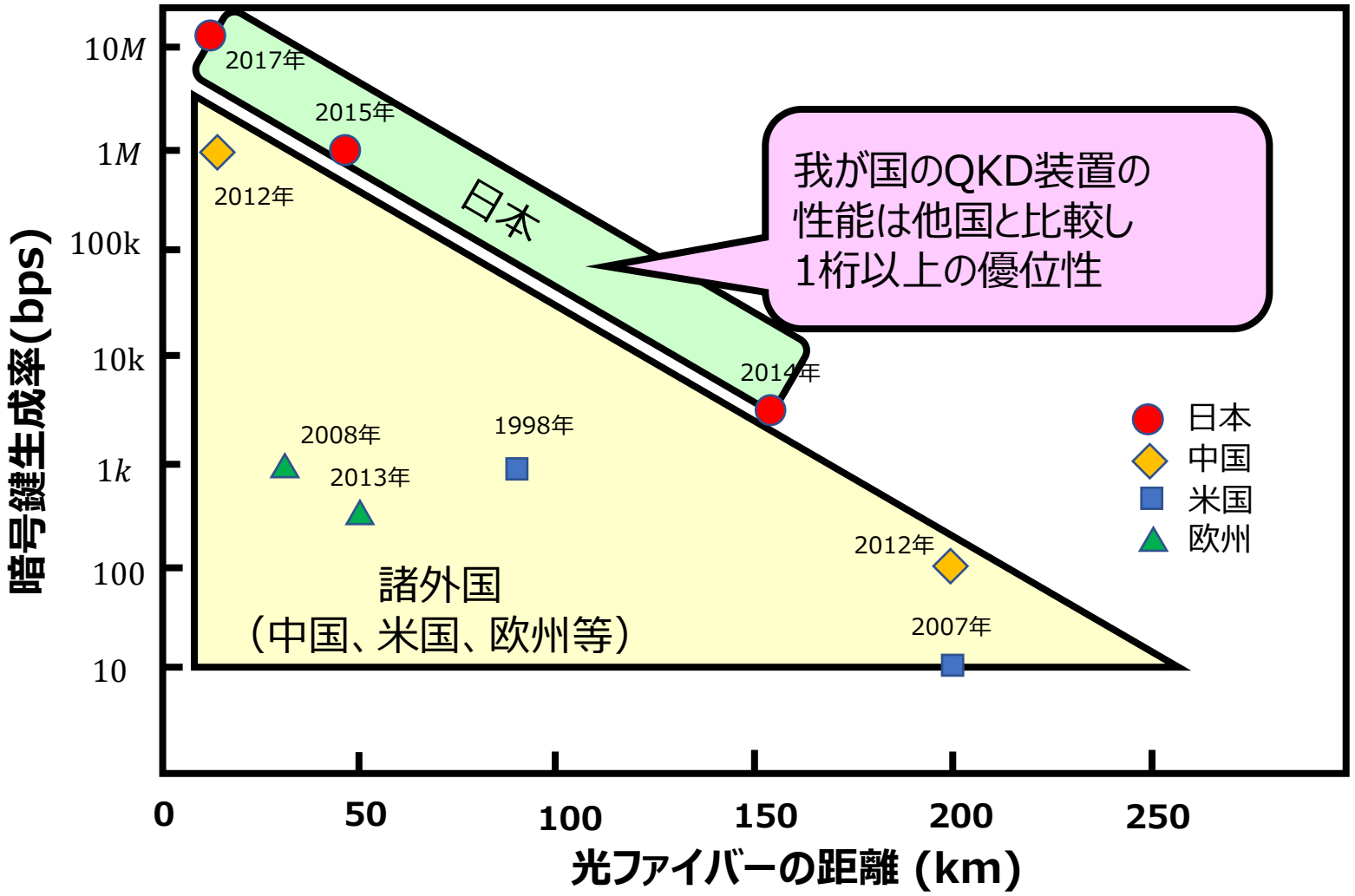
観測されたビット誤り率から直接計算

安全性理論に基づいてビット誤り率から推定



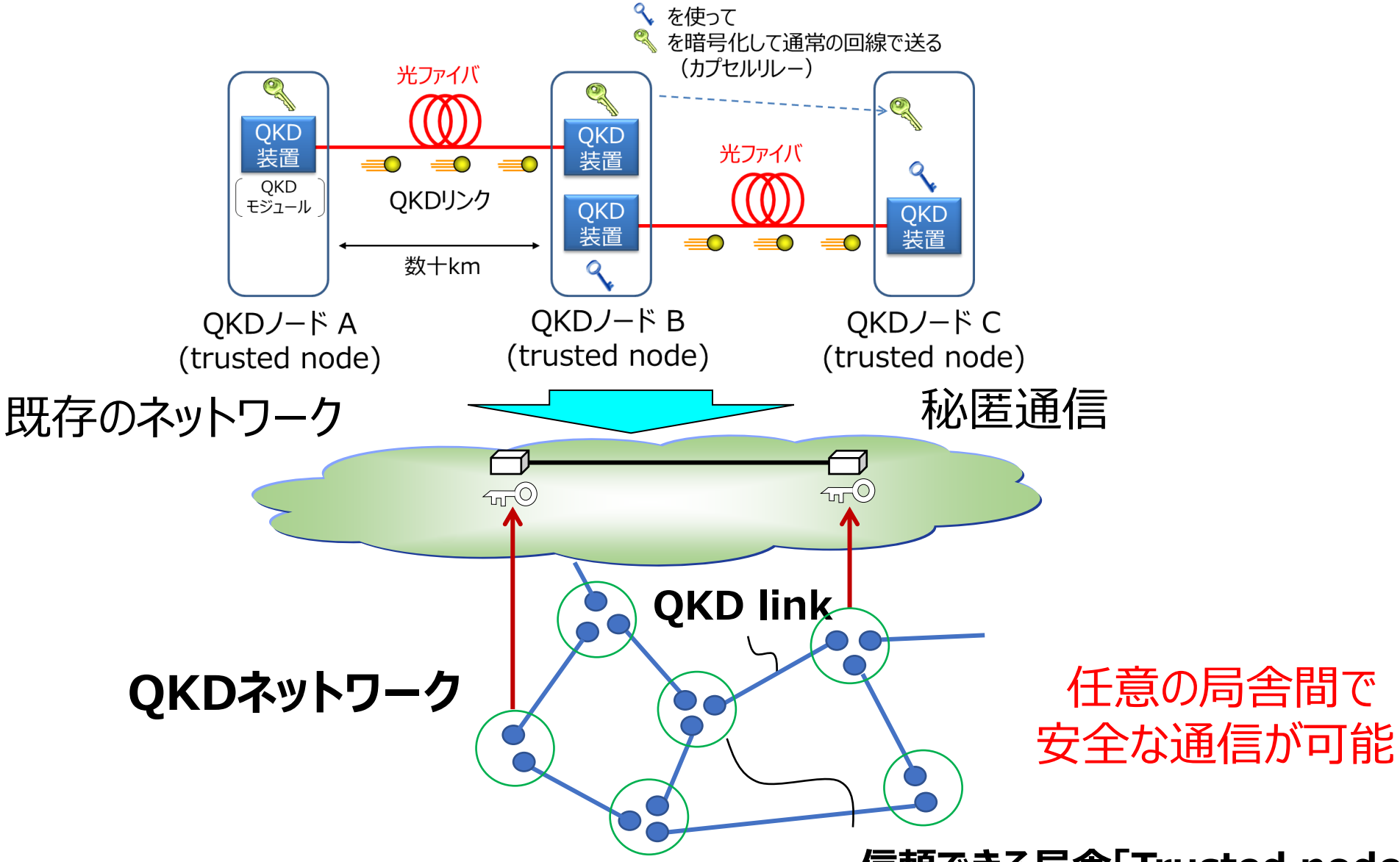
我が国の量子鍵配送装置の優位性

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

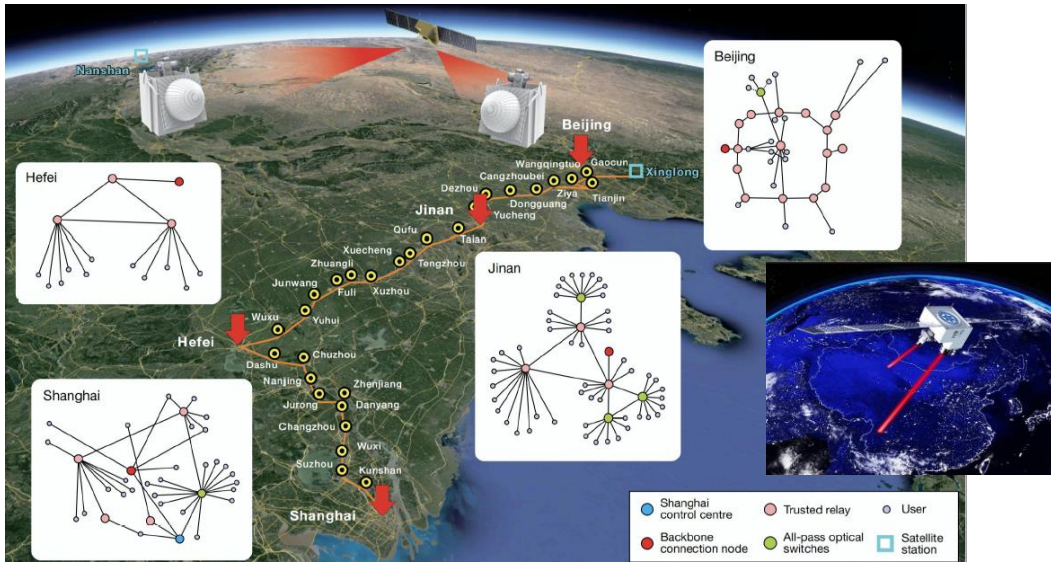


世界で進むネットワーク整備

米国

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

中国



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

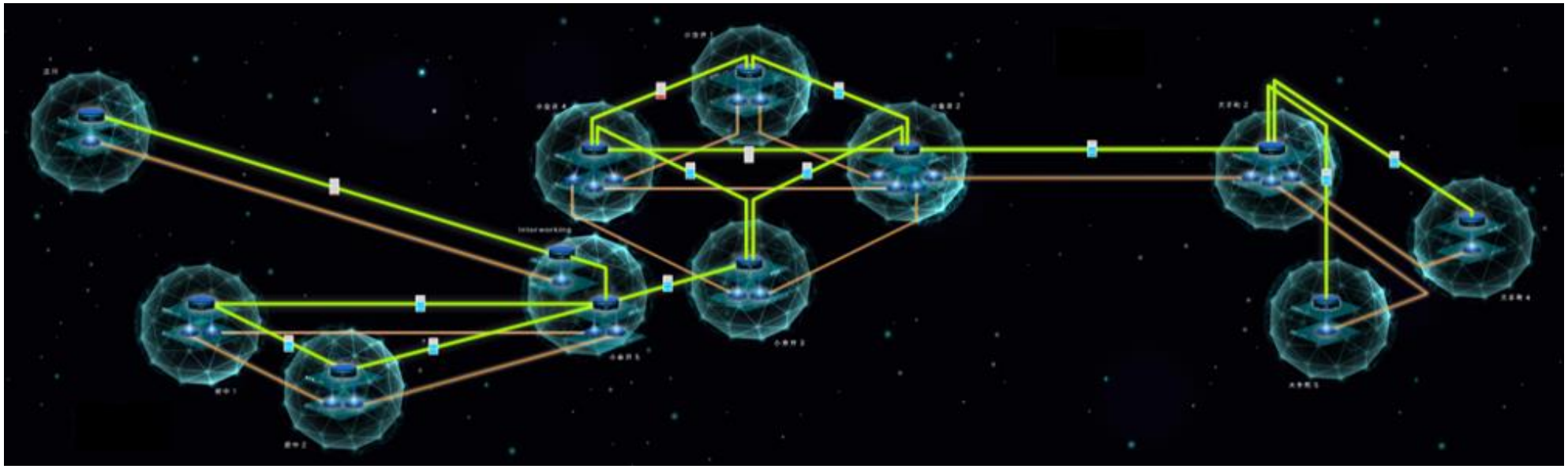
欧州

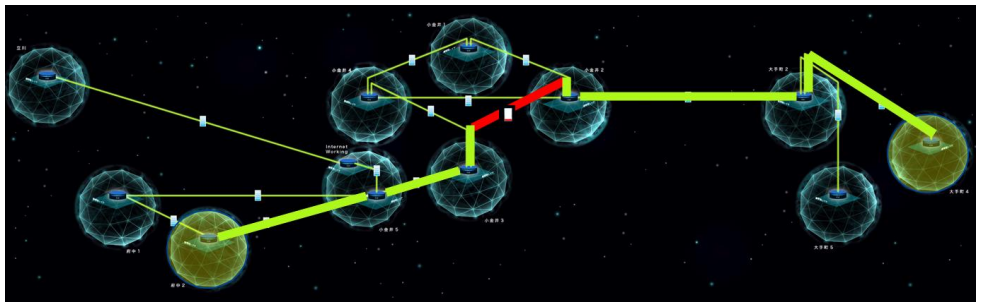
https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/Temporary/Yasser%20Omar%20-%20A%20compass%20for%20the%20Quantum%20Era%20-%20EuroQCI%20-%202021.pdf

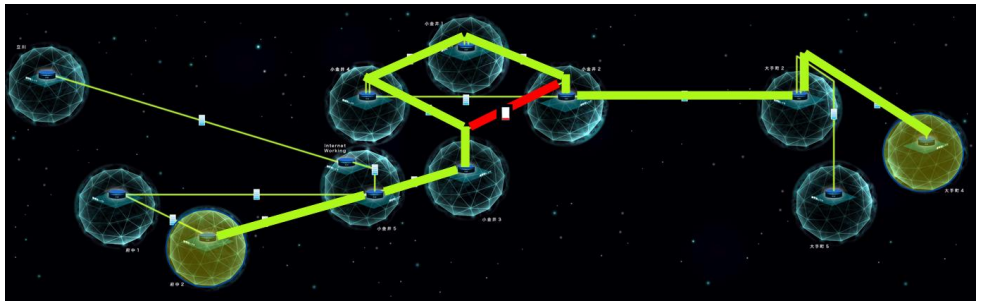
我が国独自のテストベッド　Tokyo QKD Network

2010年より運用
世界で最も運用実績の長いネットワーク
日本製は世界最高性能
2020年に東芝事業化

QKD network monitoring
Rerouting of key relay

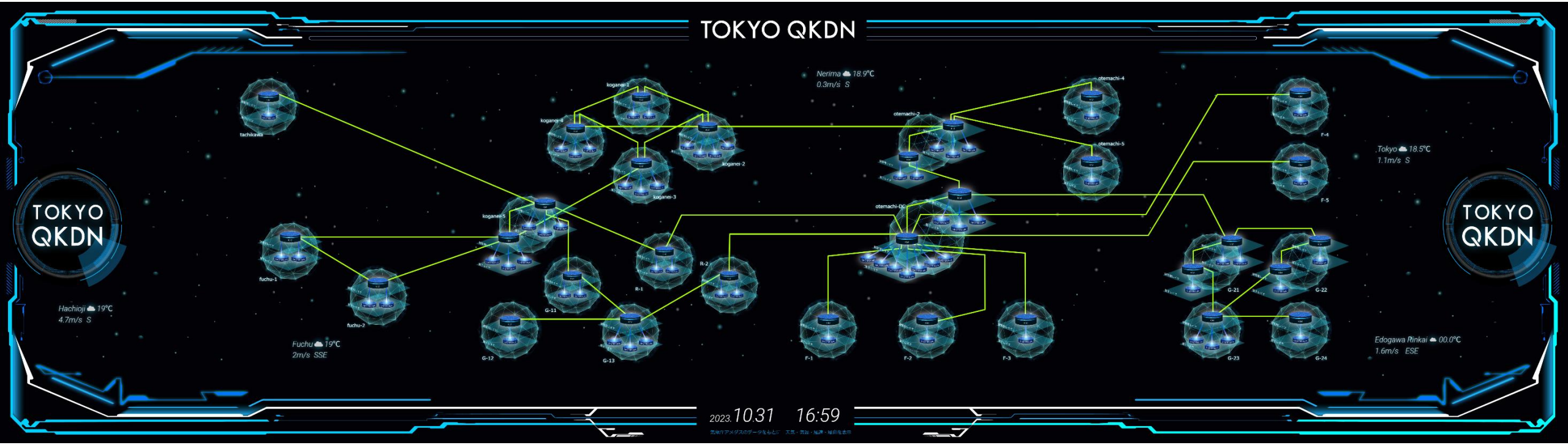






我が国独自のテストベッド　Tokyo QKD Network

拡張された東京QKDネットワーク
20を超えるノード数のネットワーク



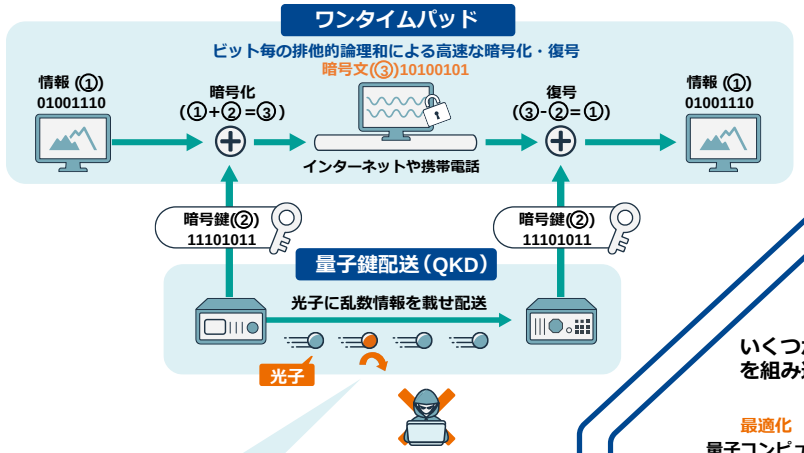
複数の大手金融機関様と直接リンクを形成

量子セキュアクラウド

日本独自の量子暗号ネットワークの高機能化
秘匿伝送，データ保管，二次利用を情報理論的安全に実施

量子鍵配送（QKD）技術

QKDにより『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



- 光の粒（光子）1つ1つに0, 1のデータを載せて暗号鍵（乱数列）を送る
- 途中で光子が盗み見られると痕跡が残るため、必ず盗聴を検知できる
- ワンタイムパッド方式とQKDを組み合わせ情報理論的に安全な通信を実現

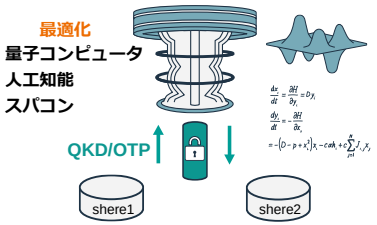
統合

超長期に秘匿すべきデータの伝送・保管・二次利用を情報理論的安全に実現

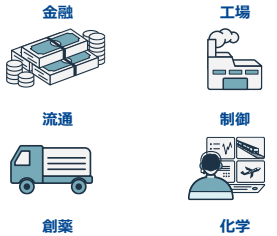
量子セキュアクラウド

秘密計算機能を備えた量子セキュアクラウドの将来像

いくつかの専用コンピューター（量子コンピュータ他）を組み込んだ量子セキュアクラウド

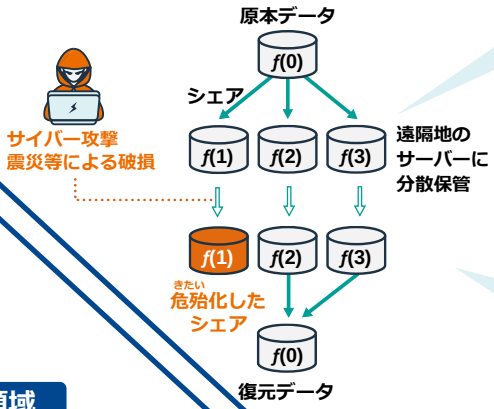


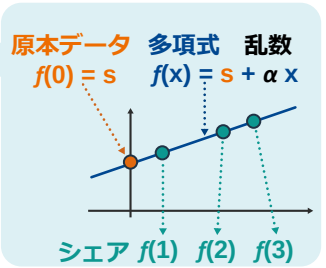
適用領域

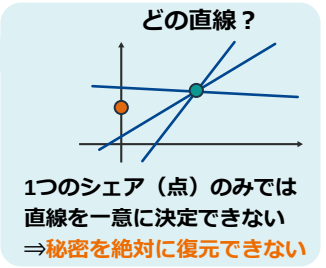


秘密分散技術

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







Shamir, Adi (1979),
"How to share a secret",
Communications of the ACM, 22 (11)

テストベッドで利用できる内容

QKDネットワークを利用した量子暗号アプリケーション

・秘匿通信アプリケーション

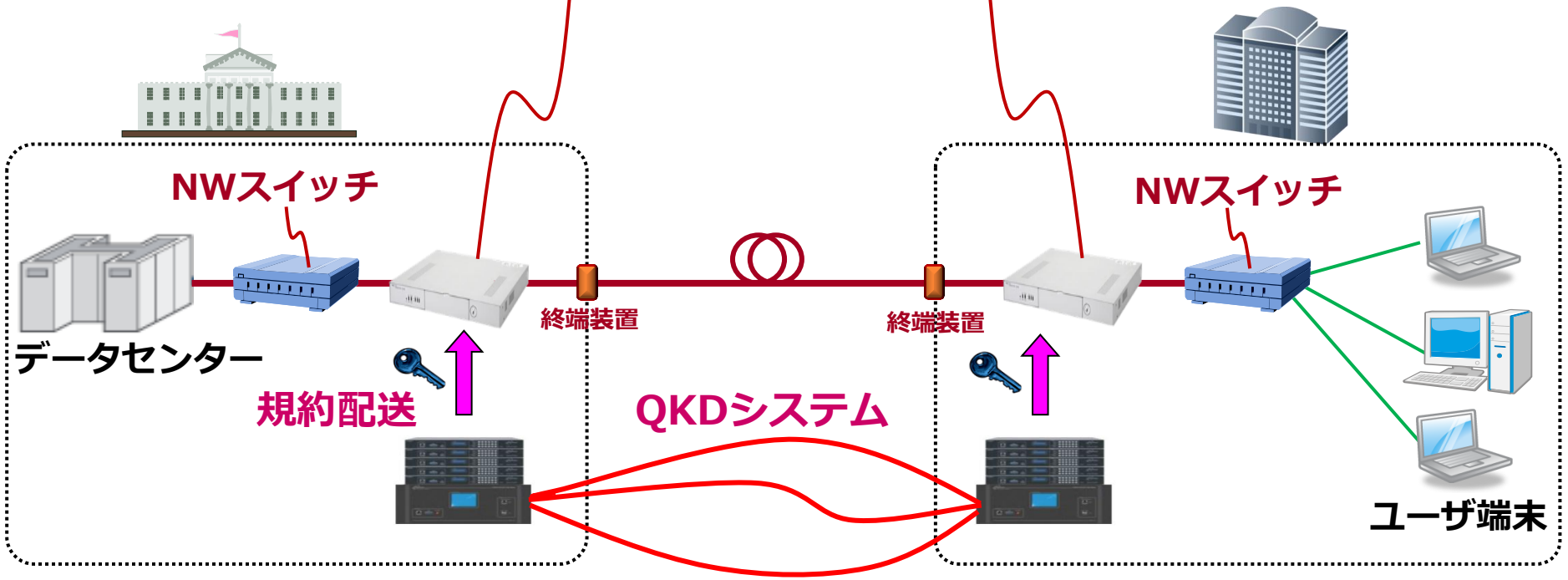
ファイル転送，メール，TV会議等を想定（金融機関同士で通信も可能）

ユーザニーズや通信トラフィックの状況に応じて適宜、アプリケーションを切換え

①高速OTP暗号による完全秘匿通信

②共通鍵暗号（AES等）の安全性強化(種鍵の更新)

Advanced Encryption Standard
（代表的な共通鍵暗号方式）

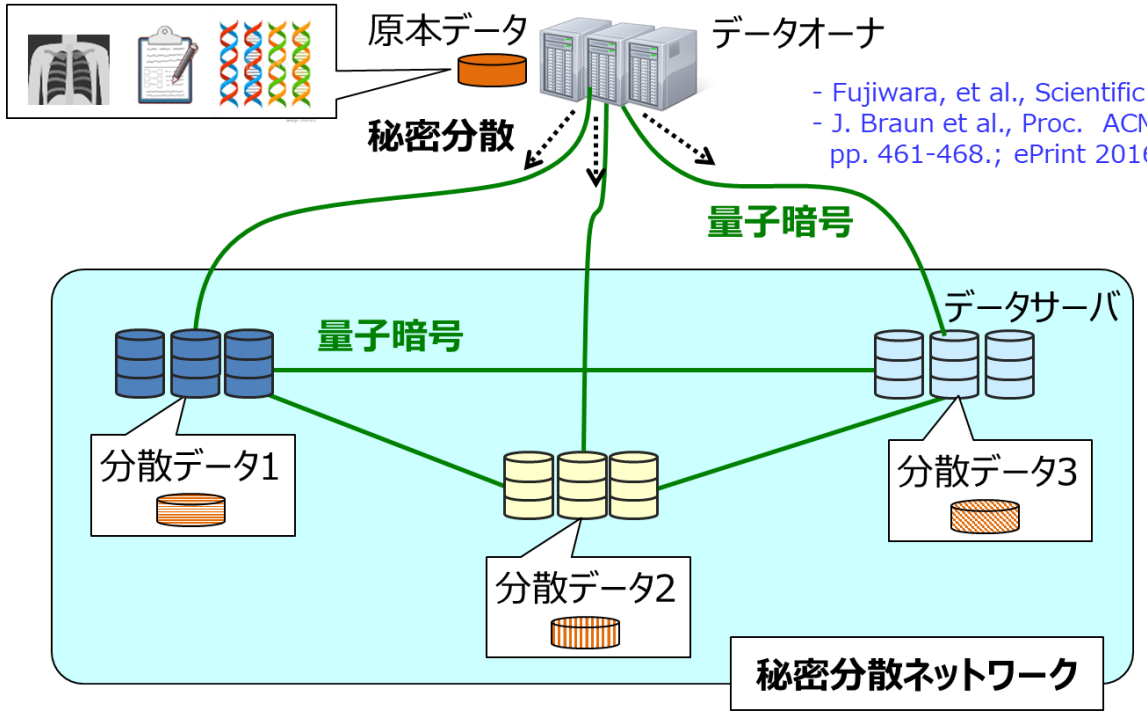


テストベッドで利用できる内容

QKDネットワークを利用したアプリケーション（続き）

・秘密分散　秘匿通信を前提とし，データの安全な分散保管（秘匿性＋可用性）

→　３つのシェア（乱数データにしか見えない状態）に分散，データ復元時には２つのシェアを集めて計算（排他的論理和）し復元.



- Fujiwara, et al., Scientific Reports, 6:28988 (2016).
- J. Braun et al., Proc. ACM Asia CCS2017, pp. 461-468.; ePrint 2016/742

・疑似量子アニーラーを用いた最適化

→東芝製半導体アニーラー（量子アニーラーを古典技術で模擬）を導入予定．MAXCUT問題など，今流行の最適化問題を安全なネットワーク（外国勢力のクラウドサービスではない）環境で実施可能.

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
(5) 金融データ秘匿伝送

・高知医療センター
・高知工科大学

(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

共通鍵暗号

大阪
京都
名古屋

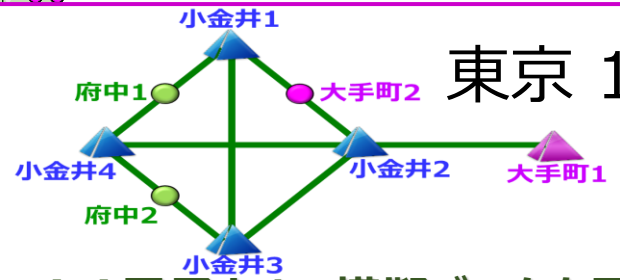
800km

(3) レーザ加工拠点間回線の秘匿化
東大柏キャンパス、京大ーNICTー慶応大学

仙台 10km圏

(2) ゲノム解析データの暗号通信、秘密分散

東京 100km圏

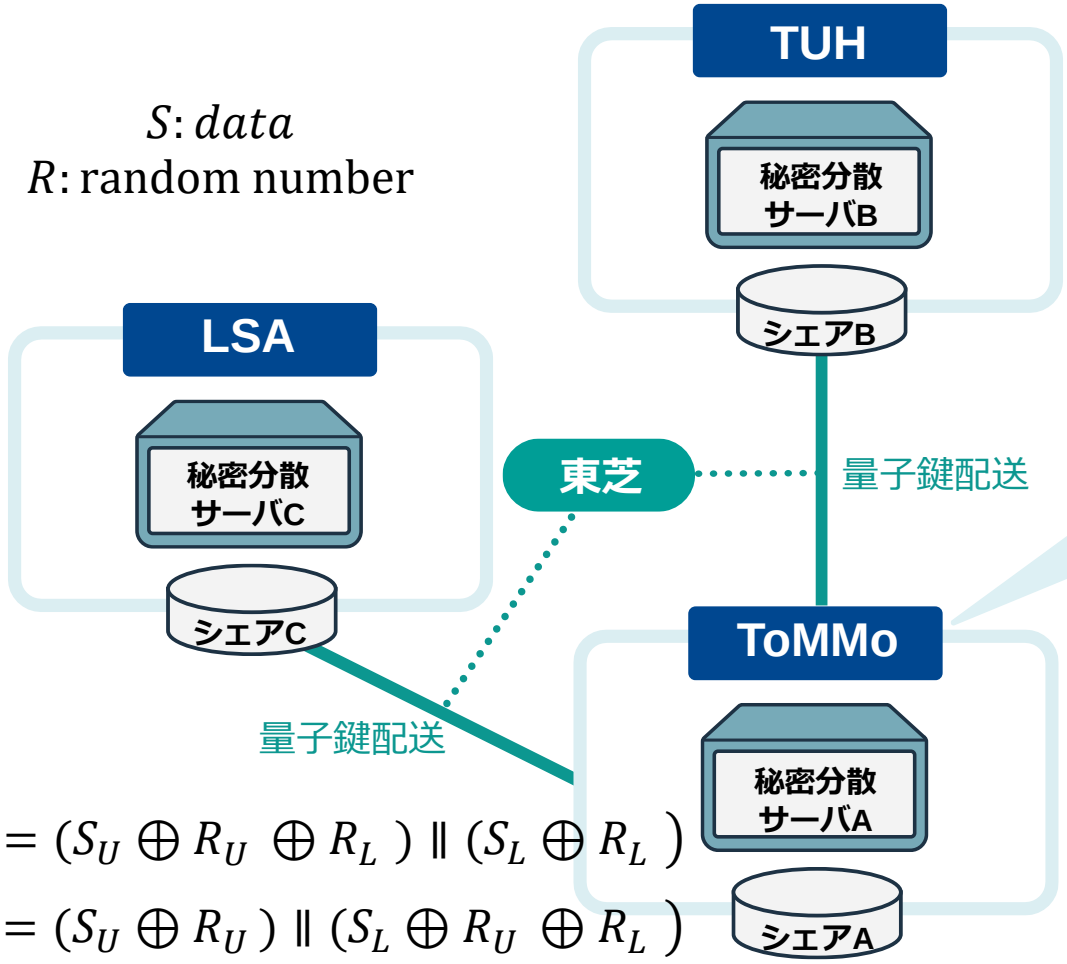


(1)電子カルテ模擬データを量子暗号で秘匿化
(4) 生体認証の実データを量子暗号で秘匿化分散バックアップ
(5) 金融データの秘匿伝送

ゲノム医療への適用　大容量秘密分散

ゲノムデータの情報理論的安全な伝送と保管

S: $data$
R: random number

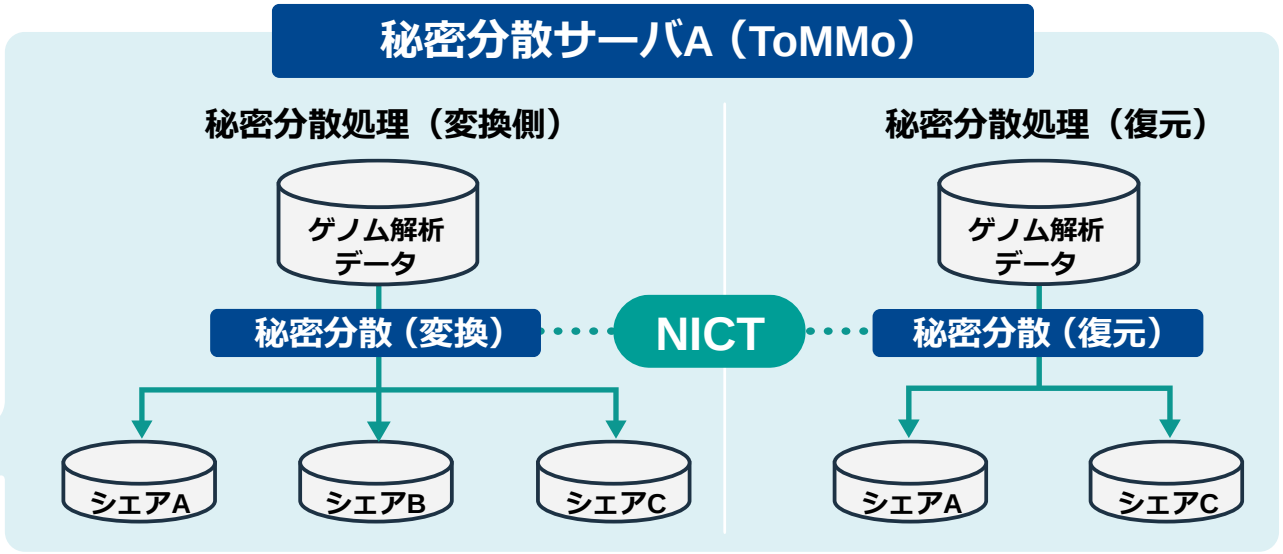


$$A = (S_U \oplus R_U \oplus R_L) \| (S_L \oplus R_L)$$

$$B = (S_U \oplus R_U) \| (S_L \oplus R_U \oplus R_L)$$

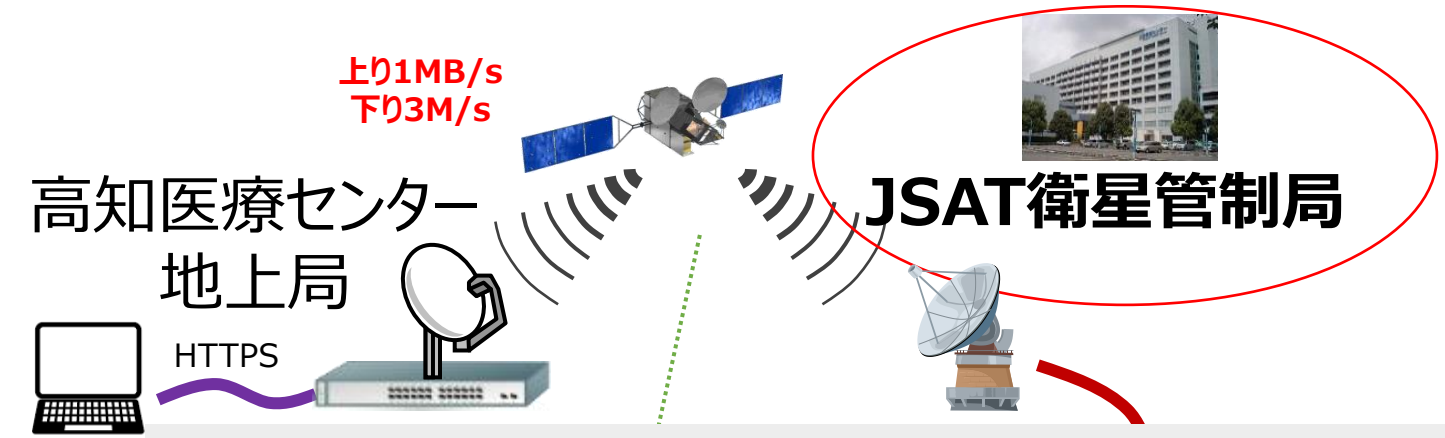
$$C = R_U \| R_L$$

80GBのデータを秘密分散で3か所に分散
OTPの高速化で数時間で完了



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

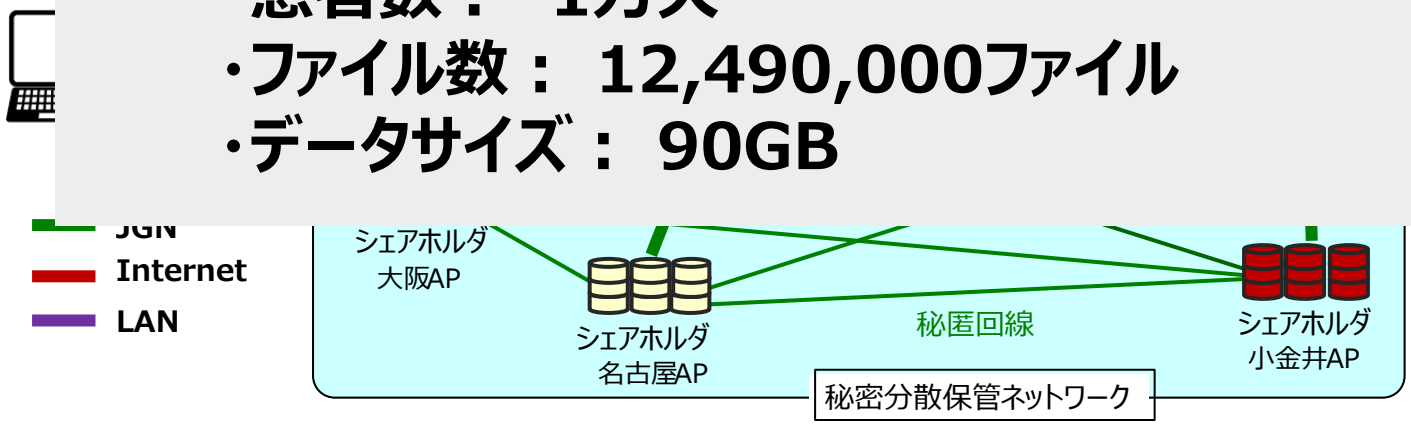
電子カルテデータへの適用



災害時を想定し、
患者データを衛星経由で復元

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



ログアウト　医師　太郎

患者検索へ戻る

よさこい高知中央病院

患者基本情報

患者ID	0021417906
患者名	高知 太郎
カナ名	コウチ タロウ
性別	男性
生年月日	1958/03/06

詳細

所見等

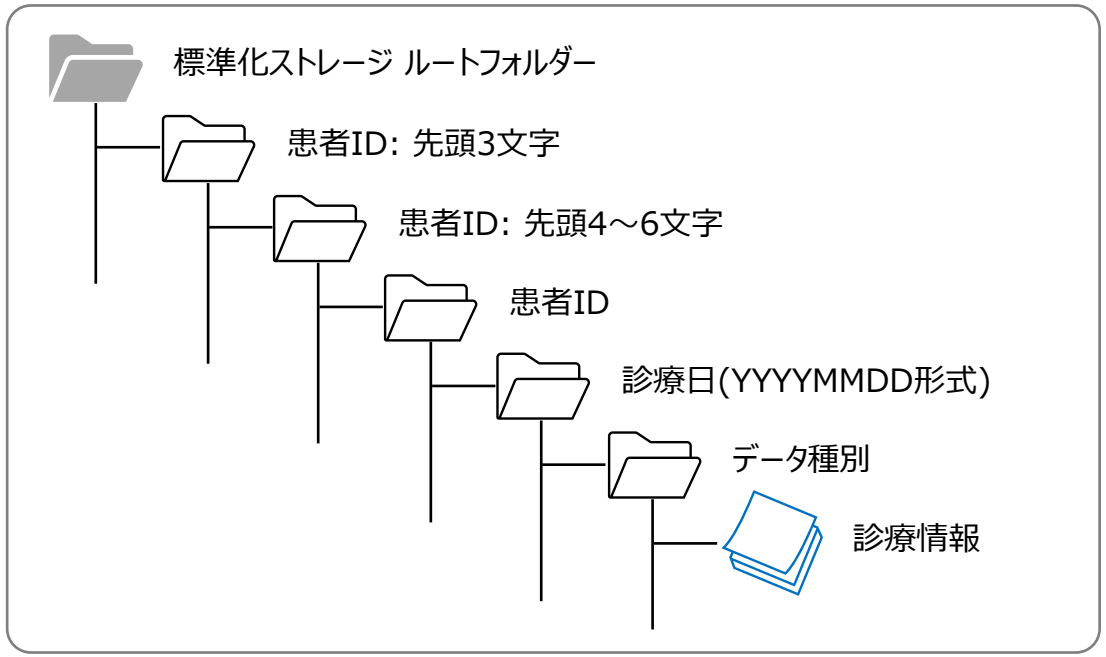
- 病名
- アレルギー
- 処方オーダ
- 処方実施
- 注射オーダ
- 注射実施
- 検体検査オーダ
- 検体検査結果
- 放射線検査オーダ
- 放射線検査実施
- 内視鏡検査オーダ

処方オーダ

- 2017/11/01
  - （救命救急科：検証 医師）
    - Rp1
      - アクトス錠 15mg「糖尿病用薬」 2 錠
        3 日分　服用開始日(2017/11/01)
    - Rp2
      - トプラシン点眼液 0．3% 5mL 3 本
        目薬　両眼　1日1回　朝　1回1滴　　服用開始日(2017/11/01)
    - Rp3
      - MS温シップ（20gX5枚／袋）50 枚
        はり薬　1日1回　1回1～2枚　　服用開始日(2017/11/01)
- 2017/11/01
  - （救命救急科：検証 医師）
    - Rp1
      - トプラシン点眼液 0．3% 5mL 2 本
        目薬　両眼　1日1回　朝　1回1滴　　服用開始日(2017/11/01)
    - Rp2
      - MS温シップ（20gX5枚／袋）20 枚
        はり薬　1日1回　1回1～2枚　　服用開始日(2017/11/01)
    - Rp3
      - ダイアップ坐剤 4mg 2 個
        坐薬　疼痛時 肛門へ挿入 2 回分　服用開始日(2017/11/01)
- 2017/07/25
  - （婦人科：検証 医師）

電子カルテデータの活用

SS-MIX準拠のフォーマット

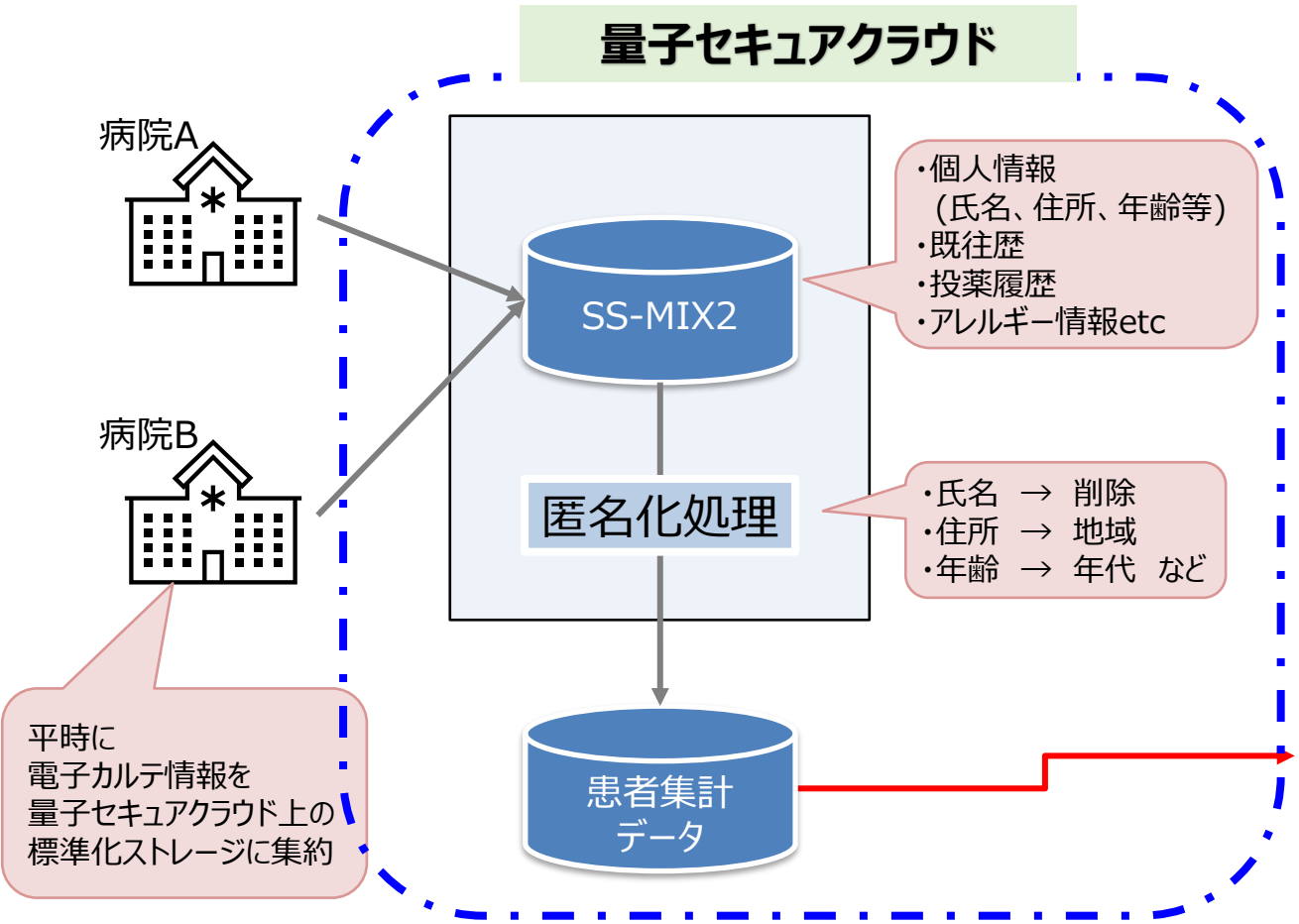


各社の相互参照機能が充実してきている半面，深いディレクトリー構造や**非構造化データ（アレルギー情報など）**が含まれるなど，秘密分散やAIなどとの親和性が必ずしも良いとは言えない．

部分復元が容易な秘密分散方式
（データベース化）

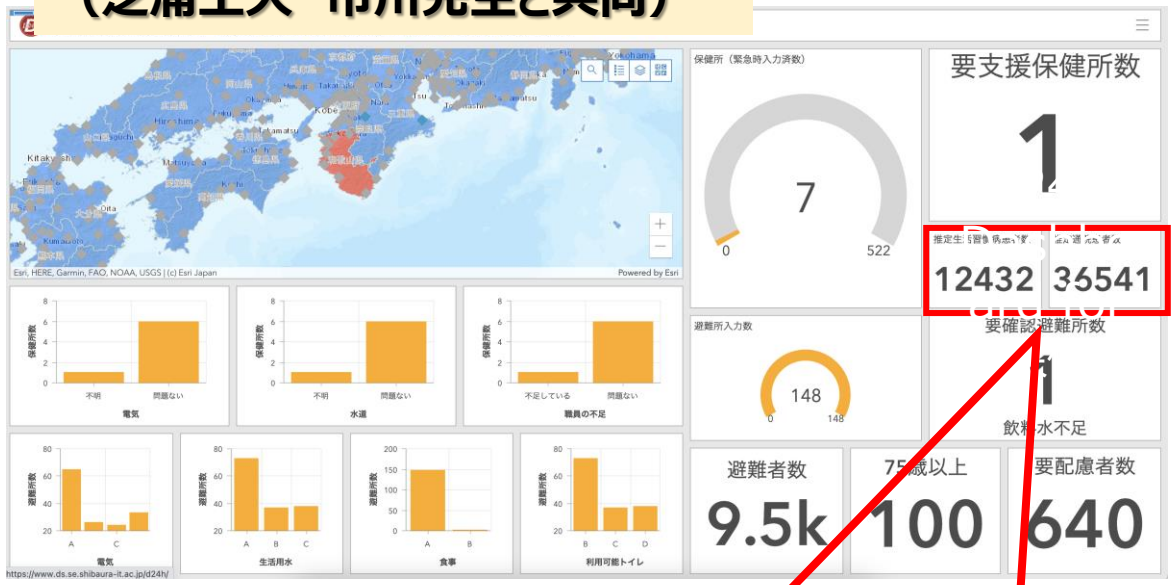
ファイルシステム＋排他的論理和ベース
秘密分散＋構造化

電子カルテデータの国家レジリエンスへの応用



ZenmuTechによる開発

D24H Dashboard for 保健
（芝浦工大　市川先生と共同）



CSV形式等で出力

市区町村番号,カルテ患者数,高血圧,糖尿病,…
30102,1233,231,332,…
30201,342,109,211,…

- **個人情報を保護できる！**
- **どの地域にどのような健康危機管理案件が起きているかがわかる**
- **保健所で避難所支援を指揮する際の網羅的な情報が得られる**

秘密分散の特徴　部分復元

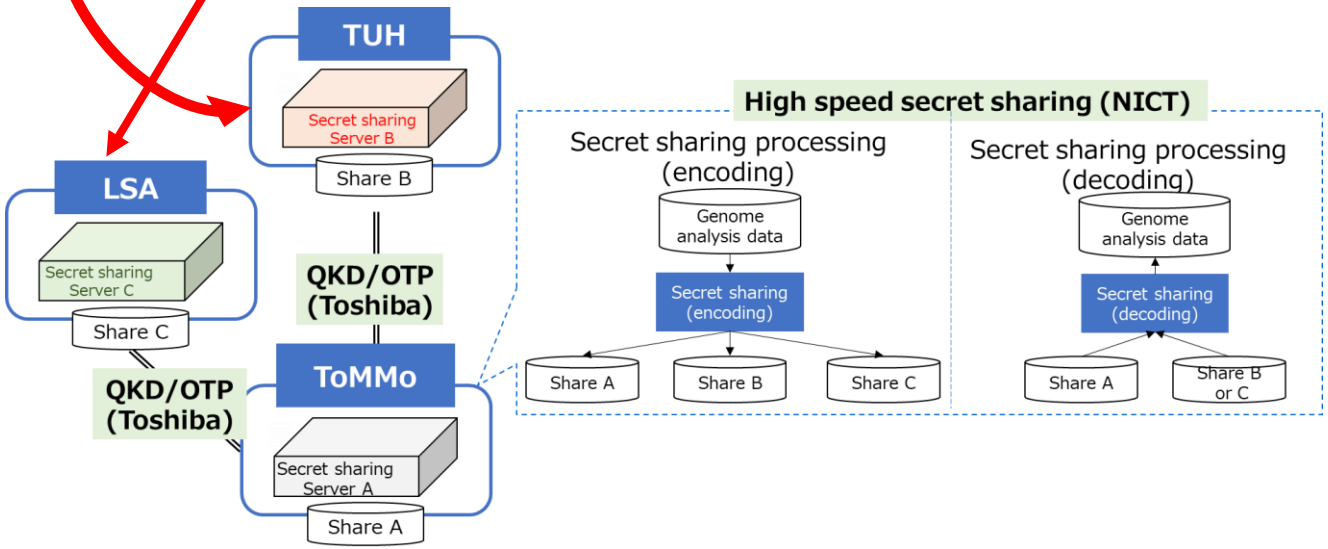
秘密分散＋データベース ⇒ **顧客情報の安全なデータ保管，二次利用時の個人情報保護**

Secret data $= S_U \| S_L$　　Random number$= R_U \| R_L$

$$\text{share A} = (S_U \oplus R_U \oplus R_L) \| (S_L \oplus R_L)$$

$$\text{share B} = (S_U \oplus R_U) \| (S_L \oplus R_U \oplus R_L)$$

$$\text{share C} = R_U \| R_L \ (random\ number)$$



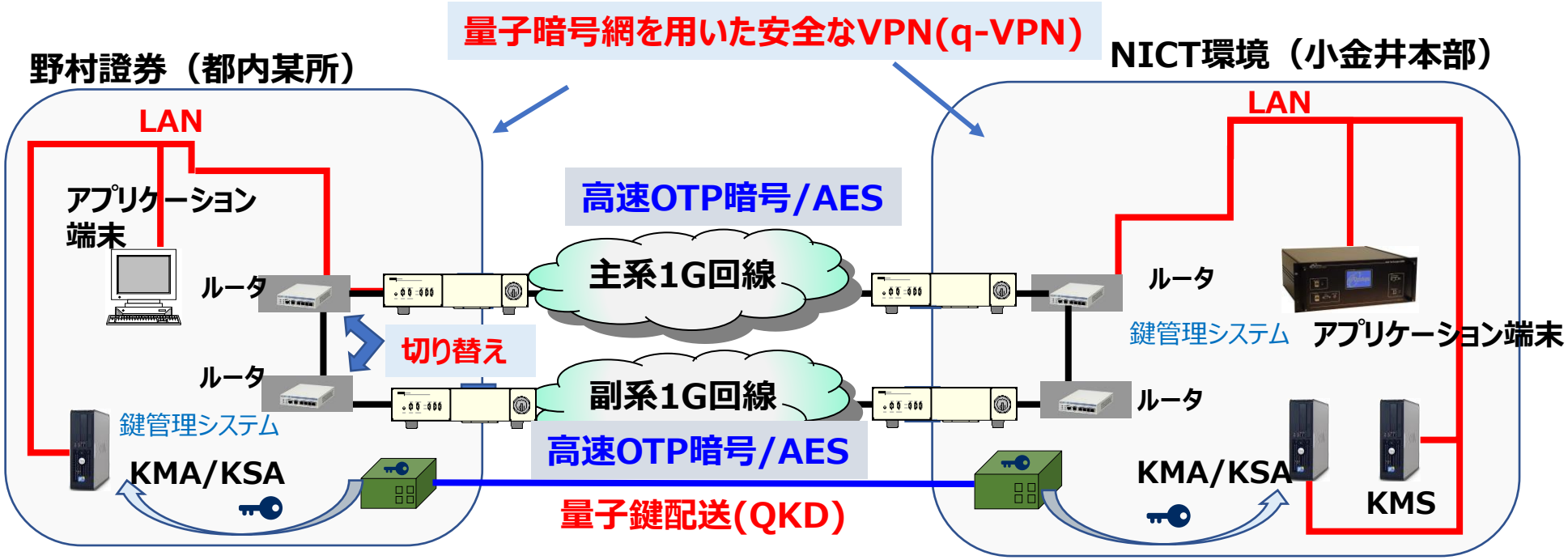
排他的論理和ベースで実装しているため
部分的に復号することが極めて容易
→余計な情報を復元する必要がないため
個人情報を秘匿しデータベース化が容易

金融情報でもディレクトリ構造が明確な構造化データであれば容易にデータベースを構築できる！

既にゲノム解析分野で応用

金融データの秘匿伝送実験

野村證券・野村HD参画　金融分野POC試験環境



野村證券，野村HD：金融アプリ提供
東芝：量子鍵配送装置を稼働
NEC：高速回線暗号装置を稼働
NICT：高速OTP暗号装置を開発

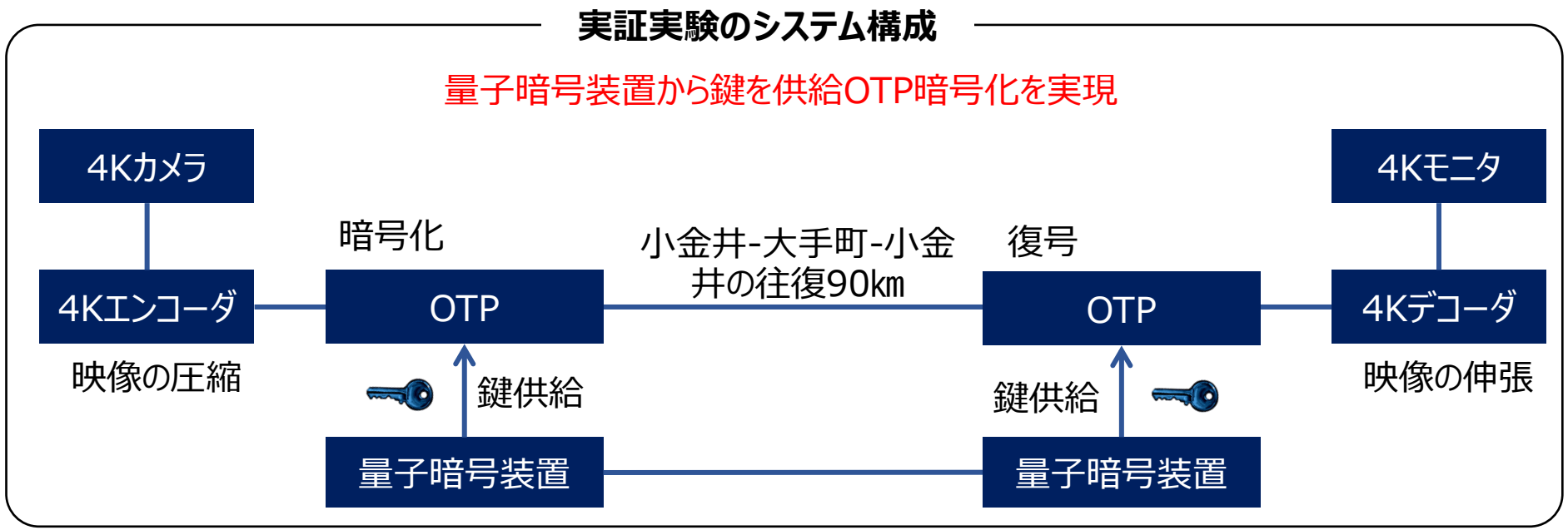
2022年1月14日プレスリリース

テスト内容：
- QKD装置の鍵生成レート：100k~300kbps程度
- １日あたりの蓄積鍵：3.2GB
- １日あたりの伝送データ：4.2GB
- OTPで伝送し，鍵が不足してきた場合AESに移行
- 主系・副系の切り替え実験にも成功(200ms)
- 大量データ，長期安定として，4.2GBのデータ伝送を１週間程度実施

遅延性の実験　QKD＋OTP の4K画像高速伝送

✓ 量子鍵配送＋OTP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２Gbpsの高秘匿伝送が可能**
  （小金井-大手町-小金井の往復回線）



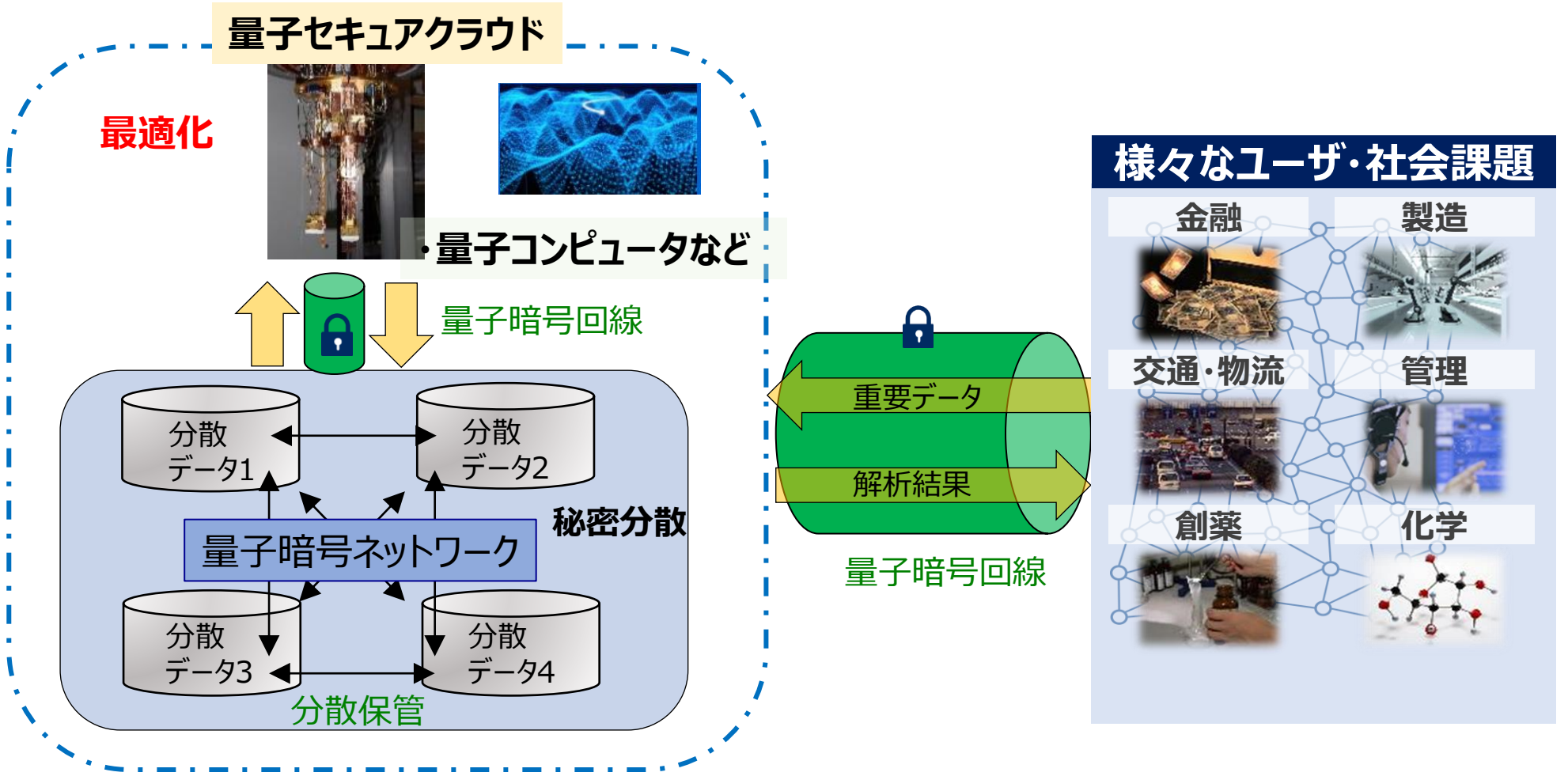
4K高精細動画高秘匿伝送技術　遠隔医療にも活用可能か？

安全なデータ利活用に向けて　量子セキュアクラウド

創造される付加価値の高い経験知（情報）を安全に伝送・保存・利用

→量子暗号・量子セキュアクラウド技術

量子セキュアクラウドの将来像



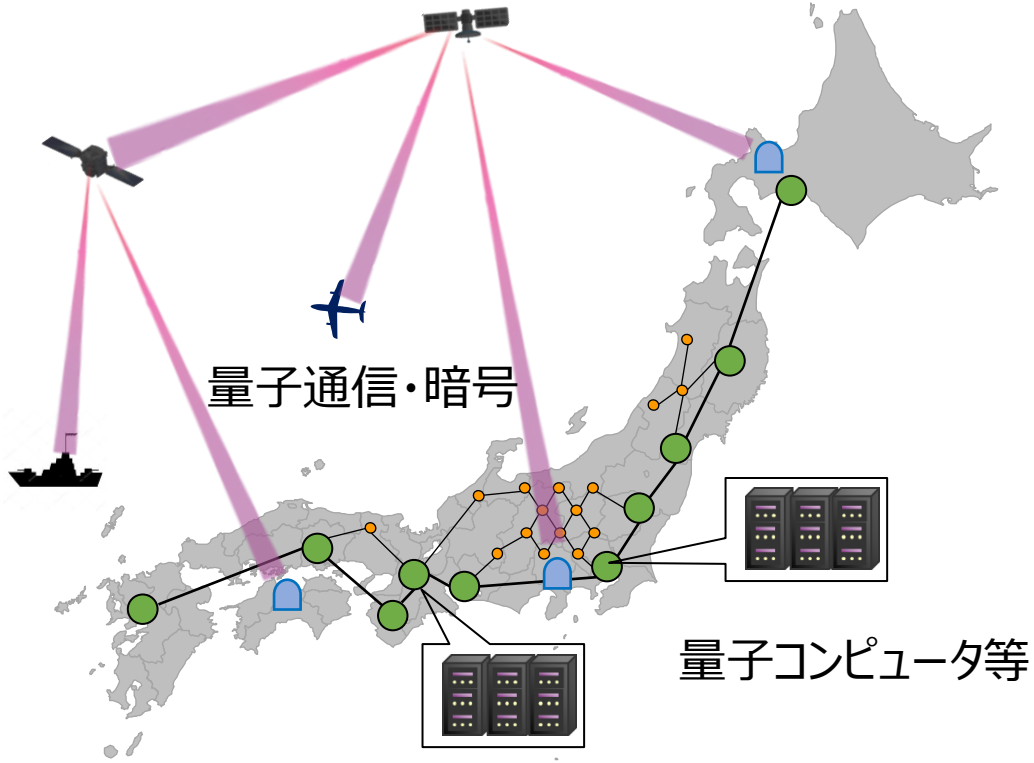
量子・古典イジングマシーン・高性能GPU,FPGAなど,
高性能計算エンジンを安全に利用できる環境を整備し,
安心してデータを利用できるプラットフォームに進化

ロードマップ

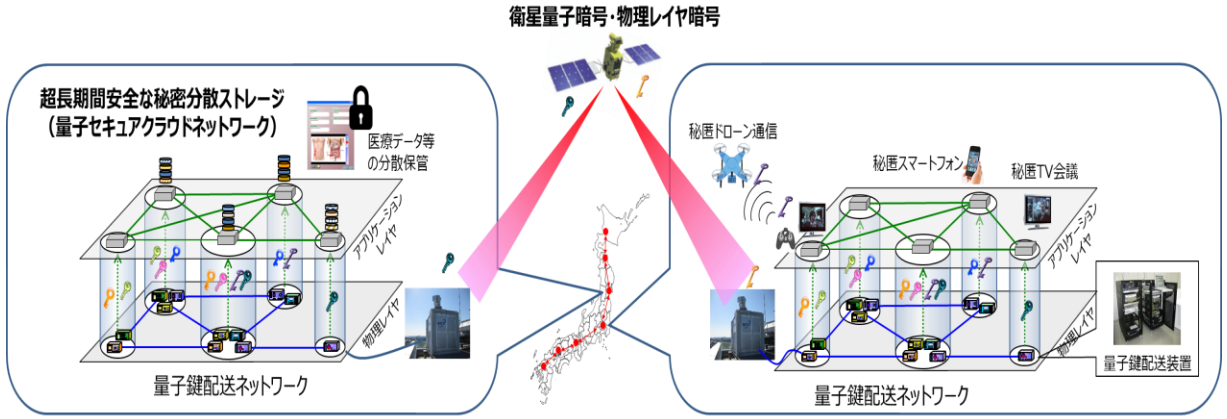
・NICTに『量子セキュリティ拠点』を整備
・東京QKDを拡張するともに産学官共同利用を一層拡大

⇒ **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



地上ー衛星を統合したグローバルな量子セキュアネットワーク