JGNを用いた量子暗号ネットワーク

「光・量子を活用したSociety 5.0実現化技術」における量子暗号技術の役割

情報通信研究機構　藤原幹生

参画機関：NEC　東芝　学習院大学　東京大学　北海道大学

（株）ZenmuTech

発表内容

１．「光・量子を活用したSociety 5.0実現化技術」
　　における量子暗号技術の役割及び開発モチベーション

２．量子暗号技術の紹介

３．量子セキュアクラウド技術の紹介

４．JGNを用いた様々なデモの紹介

2018年度より第二期SIPにて量子暗号を研究開発

レーザー加工の研究テーマと研究代表者

① CPS型レーザー加工機システムの研究開発

研究代表者：東京大学　小林　洋平

研究題目：「CPS型レーザー加工機システムによるスマート製造推進拠点」

② 空間光制御技術に係る研究開発

研究代表者：浜松ホトニクス　豊田　晴義

研究題目：「高精度・高スループットレーザー加工のための空間光制御技術開発」

共同研究機関：宇都宮大学

③ フォトニック結晶レーザーに係る研究開発

研究代表者：京都大学　野田　進

研究題目：「フォトニック結晶レーザーの高輝度化およびスマート化の研究開発」

共同研究機関：三菱電機㈱、ローム㈱

光・量子通信の研究テーマと研究代表者

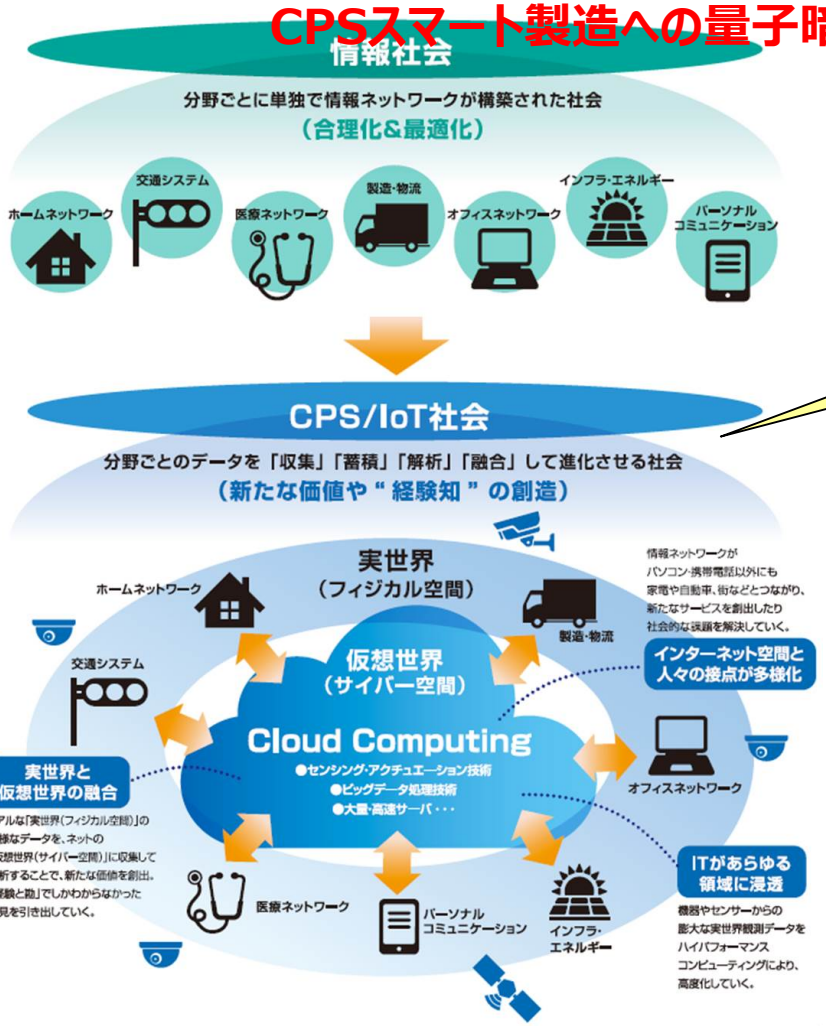
研究代表者：情報通信研究機構　藤原幹生

研究題目：「量子暗号技術と量子セキュアクラウドに関する研究開発」

共同研究機関：日本電気㈱、㈱東芝、学習院大学、東京大学、
北海道大学、㈱ZenmuTech

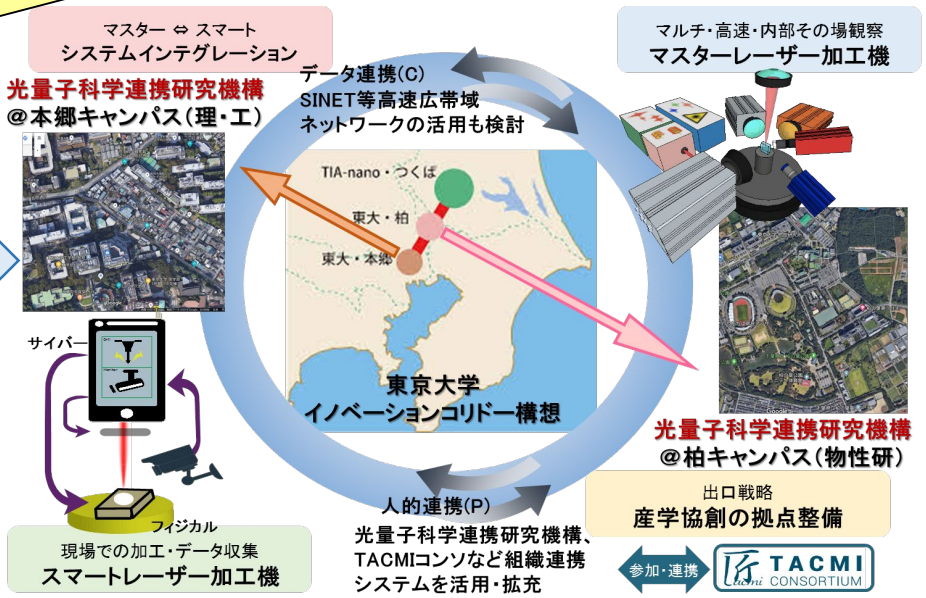
「光・量子を活用したSociety 5.0実現化技術」における量子暗号技術の役割

CPSスマート製造への量子暗号・量子セキュアクラウド技術の貢献



https://www.jeita.or.jp/cps/about/
より引用

人・物の情報を有機的に融合し経験知の創造

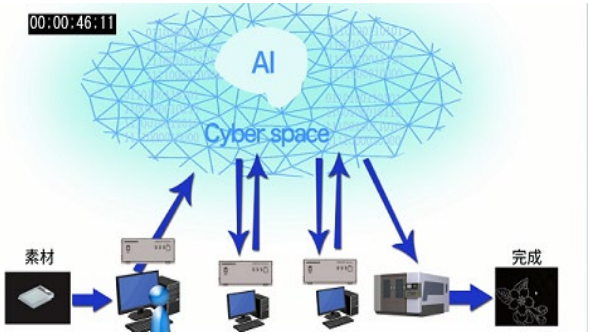


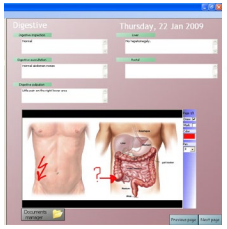
スマート製造推進拠点（構築中）

付加価値の高い経験知（情報）や個人情報を安全に伝送・保存・利用

→量子暗号・量子セキュアクラウド（秘密分散）技術

量子暗号技術導入のモチベーション





・医療・ゲノム情報等の重要個人情報
・スマート製造情報等の重要企業情報

・複数の世代，複数の家系にわたり生命を脅かすリスク
・社会・経済活動に深刻な影響を及ぼすリスク

世紀単位の安全性確保が必要
盗聴などの脅威からの解放が必須

暗号技術への脅威：量子コンピュータ開発の活発化

下院科学・宇宙・技術委員会
ラマー・スミス委員長
（テキサス州 共和党員）
2018.06.12

「量子は次世代科学のブレークスルーを再定義しようとしている。我々は米国が量子プログラムの進歩において他国に遅れをとらないようにしなければならない」

トランプ大統領は2018年末，量子コンピューティングの研究開発に投資する**「National Quantum Initiative Act」法案に署名**

https://www.congress.gov/bill/115th-congress/house-bill/6227

米国：量子コンピュータ開発に12億ドルの投資がされる可能性
→想像よりも早くに現在の公開鍵暗号が破られる危険性
→現在のネットを行き交う情報全てを解読される恐れ！

諸外国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)

どの様なデータを守るか？

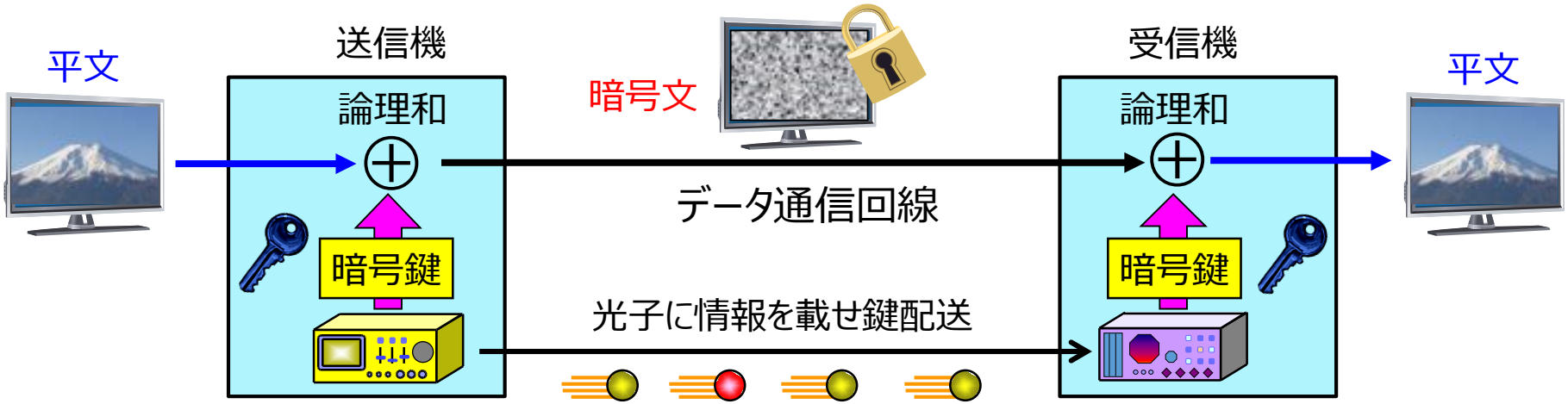
秘匿期間	分野	情報	セキュリティレベル	理由
30	防衛	指令系通信等	**非常に高い**	防衛情報を扱っている為
		防衛装備品に関する技術情報	**非常に高い**	防衛情報かつ法律でも定められている為
30	行政	政策	**普通**	国の混乱を招く恐れがあるが一時的となる可能性が高い為
		外交情報	**非常に高い**	国の信用問題であり各国との関係に悪影響を及ぼす為
＞100	医療	**遺伝子情報**	**非常に高い**	遺伝情報から差別や，雇用における採否に影響する可能性がある為
		電子カルテ	**高い**	アレルギーなど人の生死に係る為
30	**インフラ Cyber Physical System (CPS)**	**暗号鍵情報（生体認証参照データ含む）**	**非常に高い**	情報インフラの安全性の基点である為
		企業機密（スマート製造等）	**非常に高い**	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

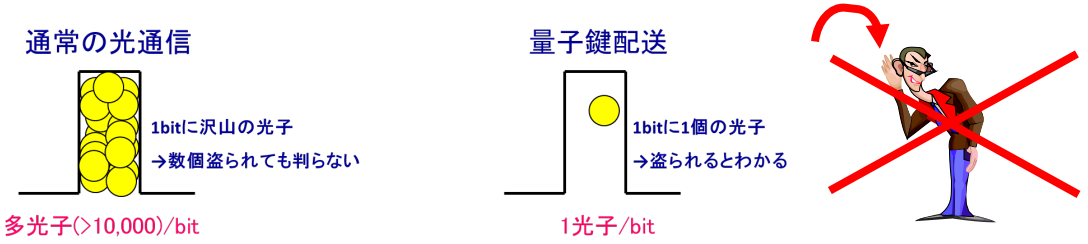
一般的ユーザー向け社会実装を想定し競争力強化を実施

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　（情報理論的安全）

・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）



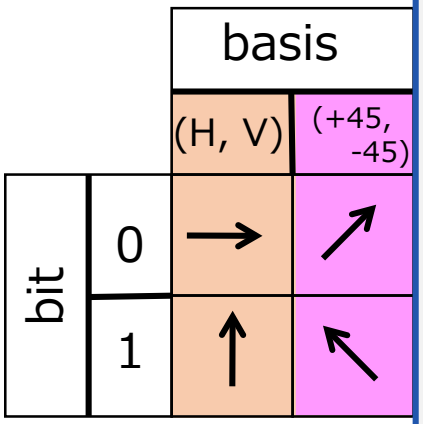


どんな盗聴も確実に検知　情報漏洩を完全に防止

QKDの仕組み

単一光子の偏光状態に情報を載せる
例：BB84プロトコル

Alice



Bob

detector

(+45,-45)

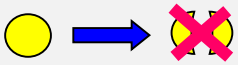
2.5°

PBS

V) basis

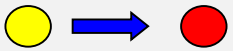
光子の量子力学的性質

1. 光子は粒子の最小単位（量子）
（これ以上分割が不可能）



⇒光子を盗むと受信側に届かない

2. 光子の観測・増幅等の作用は
光子状態を必ず変化させる（不確定性原理，no-cloning 定理）
→非直行な状態を誤り無しで識別できない



⇒非直行状態の光子列を伝送し，一部の鍵情報を開示して誤り率を測定することにより盗み見る行為による状態変化を受信側で検知できる

Alice と
した基底

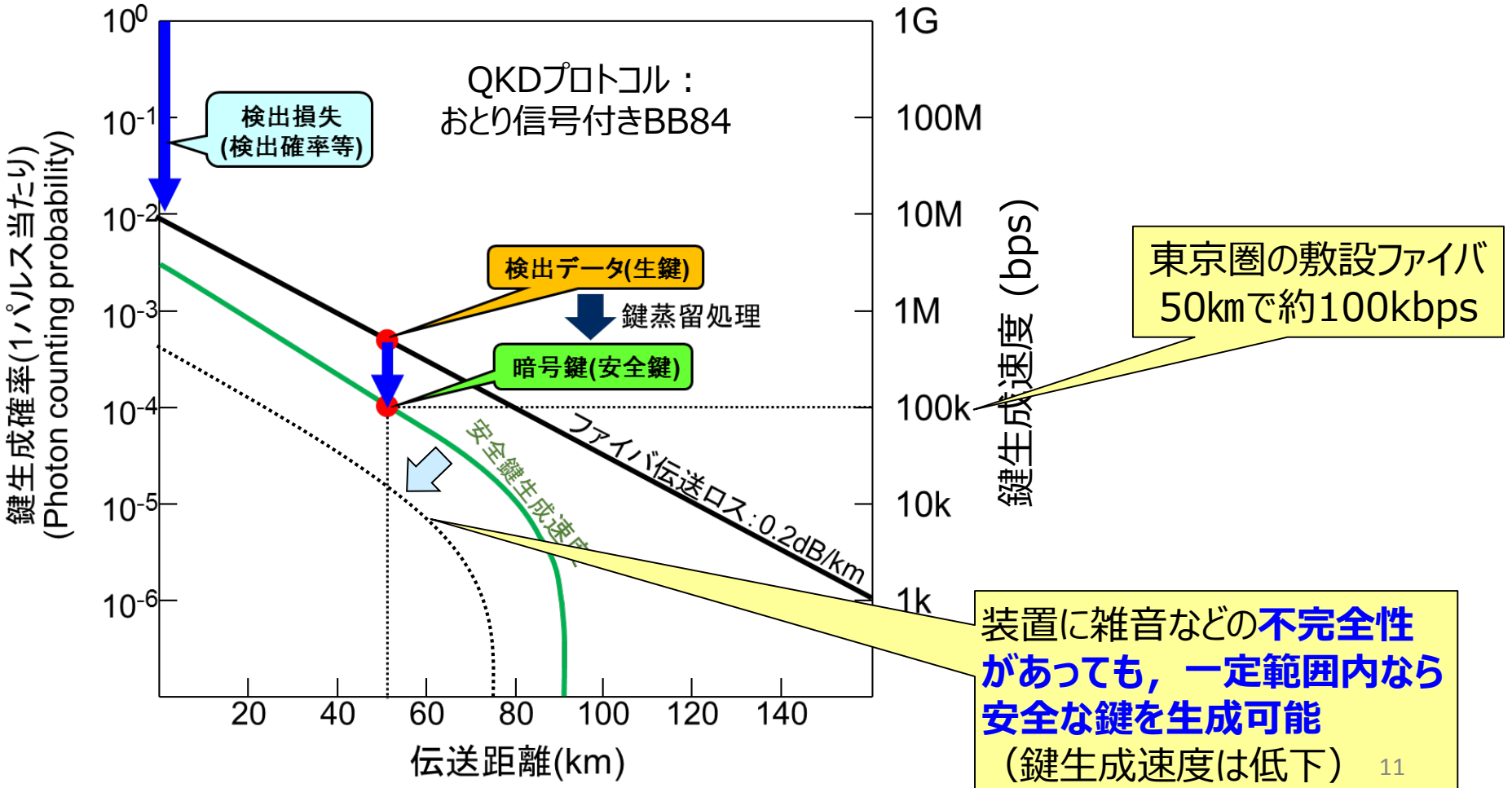
基底が一致したビットについて一部公開し誤り率を推定
エラー訂正・秘匿性増強を行い，共通鍵（暗号鍵）として使用

量子鍵配送の性能

東京圏の敷設ファイバ50㎞で約100kbps

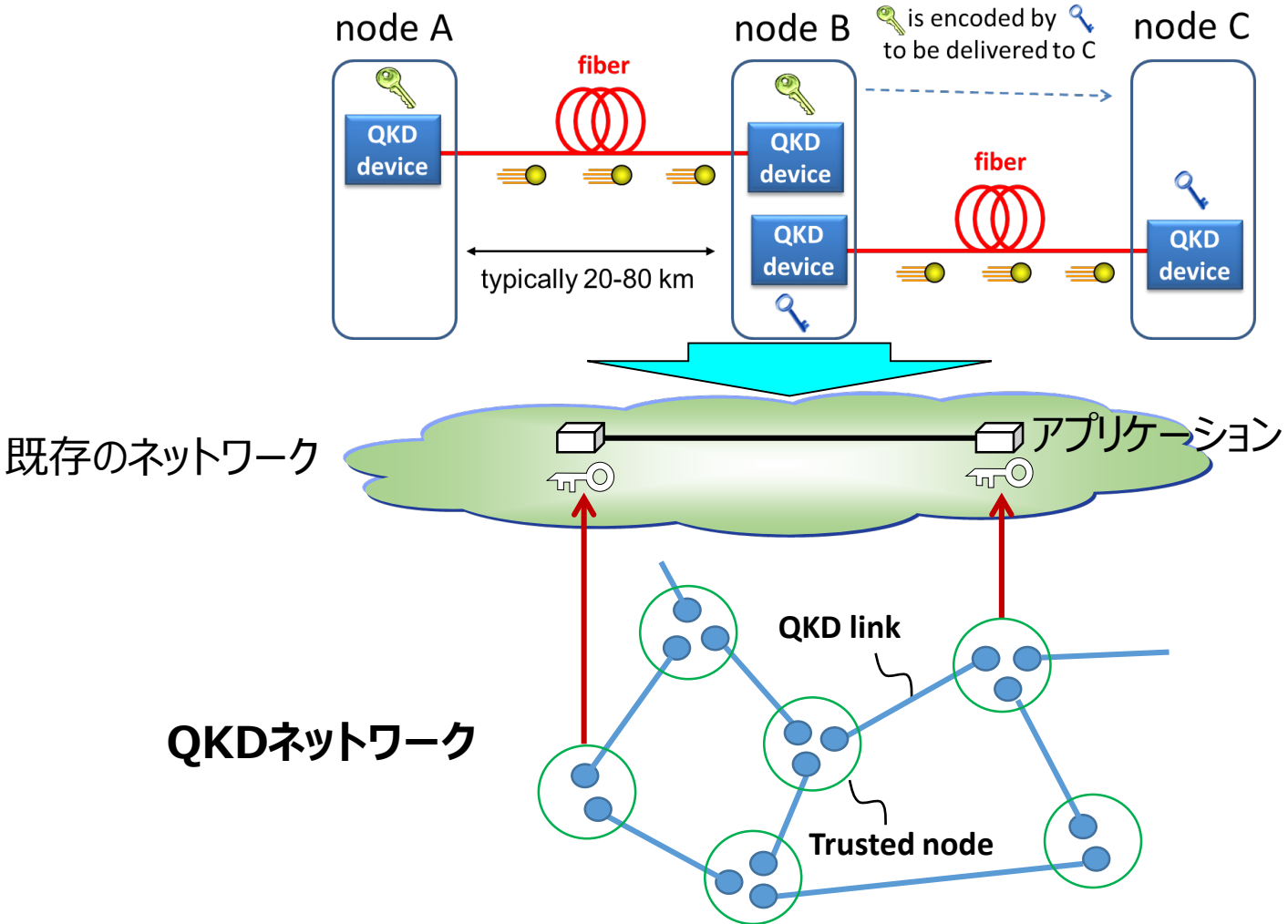
⇒ 常時鍵を生成し，サーバ上に蓄積

⇒ ここぞと言う重要通信の際に鍵を利用



量子暗号ネットワーク化　サービスエリア拡大

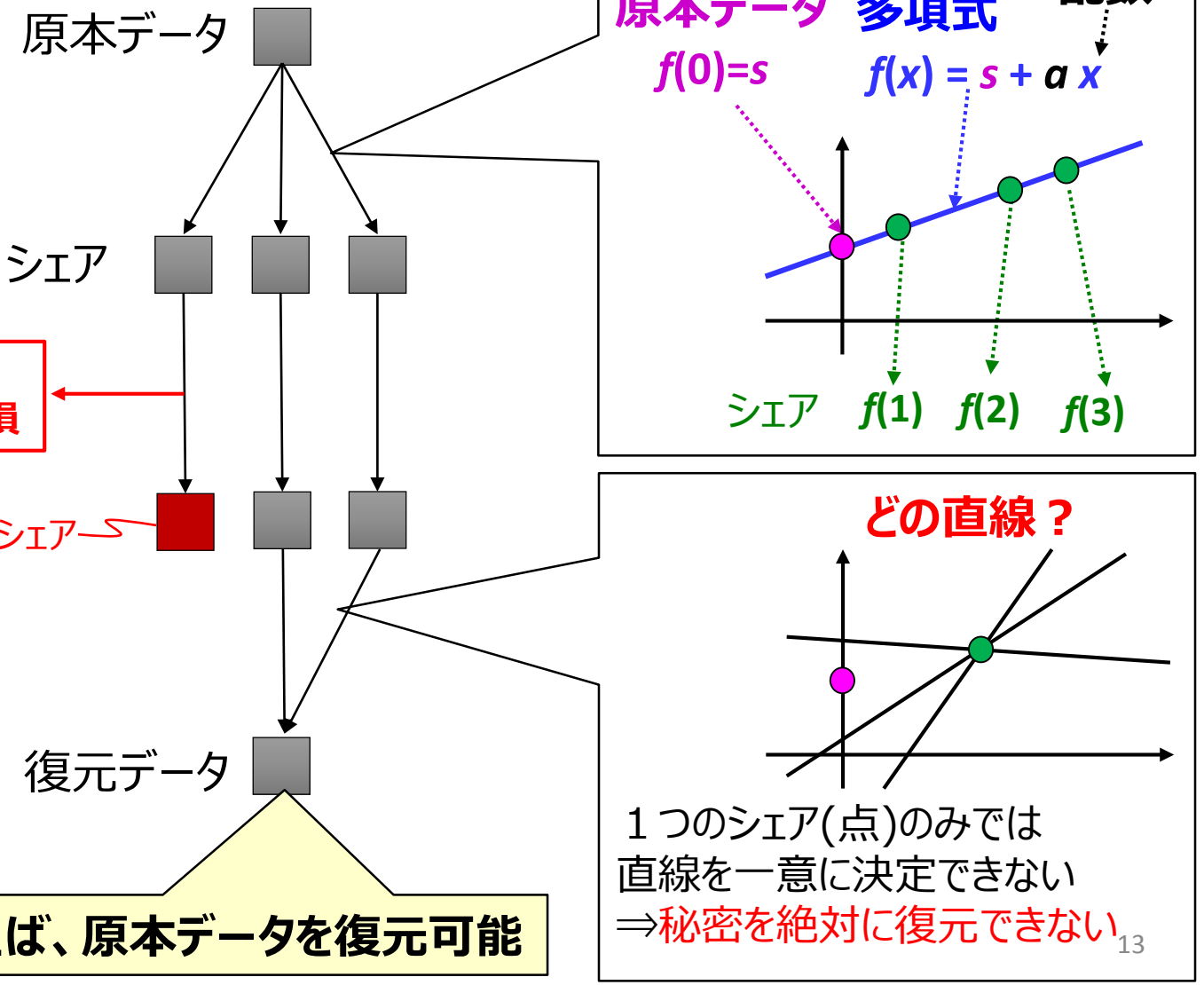
ネットワーク化は『**信頼できる局舎**』を介した鍵のカプセルリレーで実現
→サービスエリアの拡大　任意の局舎間で安全な通信が可能



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）に分割　1979 Shamir

例
n=3個に分散、
k=2のシェアから復元



２つのシェアが揃えば、原本データを復元可能

超長期安全性を実現するQKD秘密分散ストレージ

要件

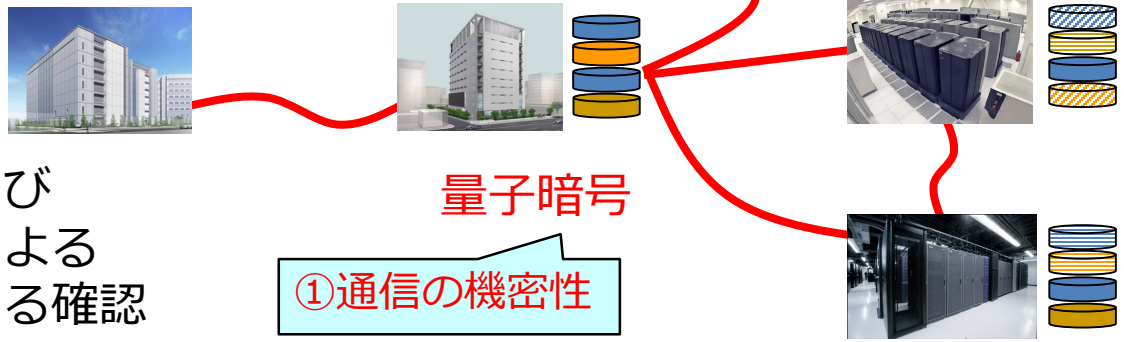
1. 機密性：正規ユーザ以外に平文が漏れない　⇒ 暗号化
2. 完全性：平文が改竄されていない　⇒ 署名、認証
3. 可用性：必要な時に平文を得られる　⇒バックアップ
4. 機能性：機密性を保ったまま情報処理できる ⇒ 準同型性

現代暗号のみでは
実現不可能
サーバ間通信の
機密性を超長期間
保証できない

① 保存の機密性
③ 可用性
④ 機能性

秘密分散法

② 完全性



デジタル署名および
メッセージ認証による
データ保有者による確認

量子暗号

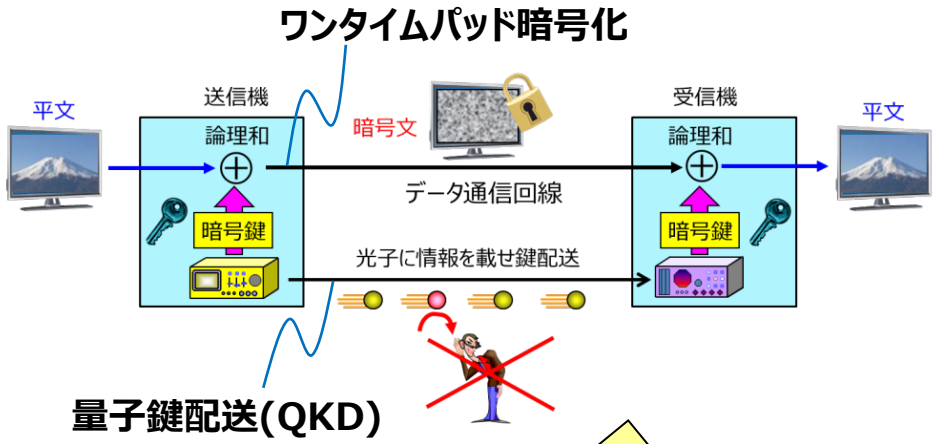
①通信の機密性

現代暗号，ネットワーク技術，量子暗号の融合によって初めて実現可能

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

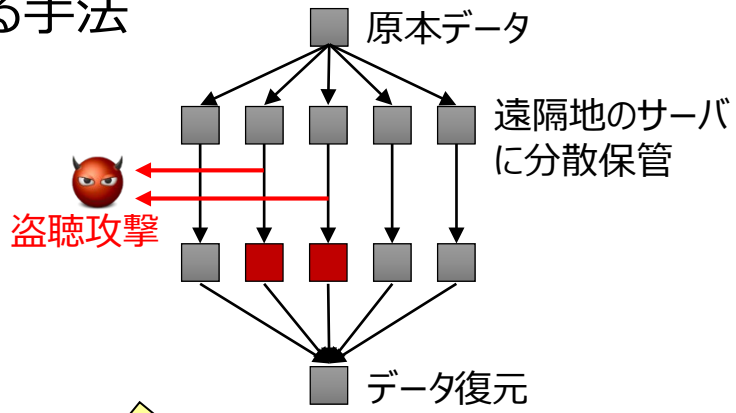
量子暗号

『**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



統合

革新的研究開発推進プログラム ImPACT

『超長期セキュア秘密分散保管技術』

世界初

- ✓ 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
- ✓ **パスワード1つでも情報理論的安全な本人認証を実現**（秘匿計算を応用）

Fujiwara, et al., Scientific Reports, 6:28988 (2016).

量子セキュアクラウドへ発展

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（量子暗号の要素技術、量子暗号、量子セキュアクラウド）
(2) ゲノムデータ（模擬）の秘密分散保管（量子暗号技術、量子セキュアクラウド）
(3) レーザ加工拠点の重要回線の秘匿化（量子暗号技術、量子セキュアクラウド）
(4) 生体認証の参照データの秘密分散保管（量子暗号技術、量子セキュアクラウド）

高知医療センター

電子カルテの標準データ交換規格に基づく模擬データを提供

(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

大阪拠点

名古屋拠点

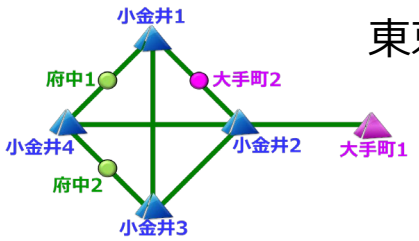
共通鍵暗号による秘匿化

(3) レーザ加工拠点の重要回線の秘匿化

仙台 10km圏

(2) ゲノム解析データの暗号通信、秘密分散

東京 100km圏

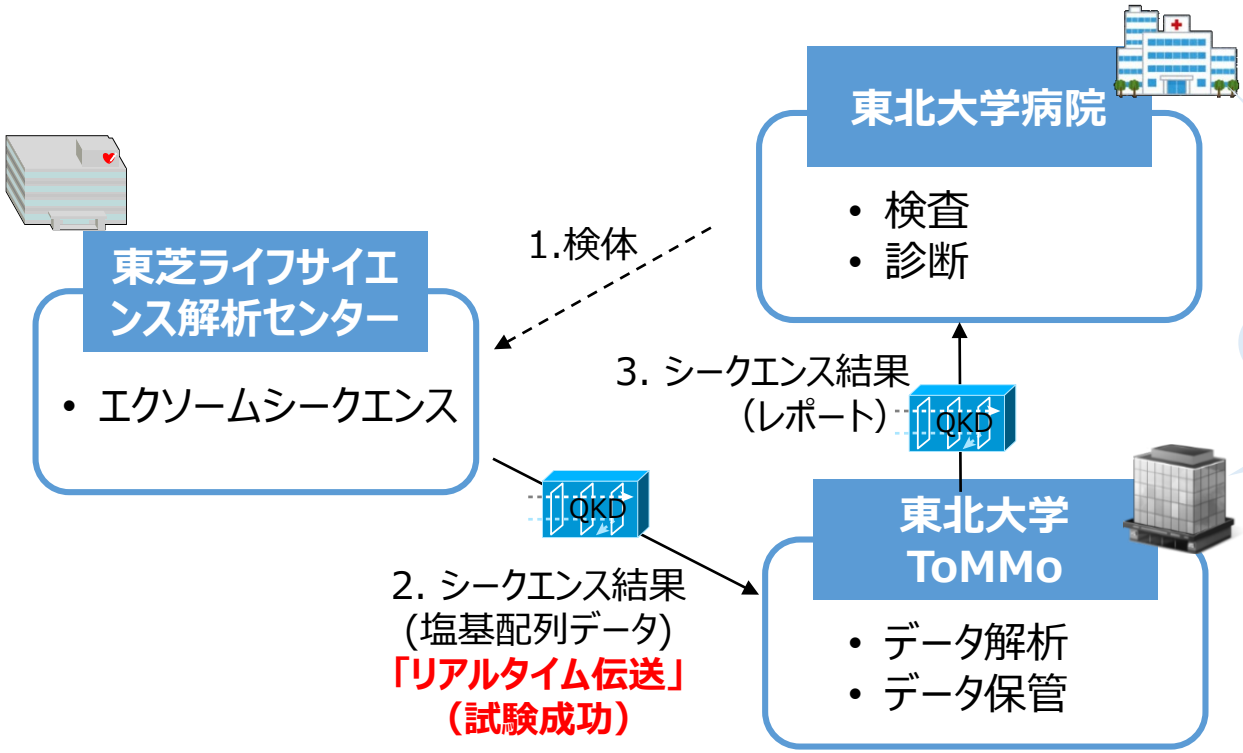


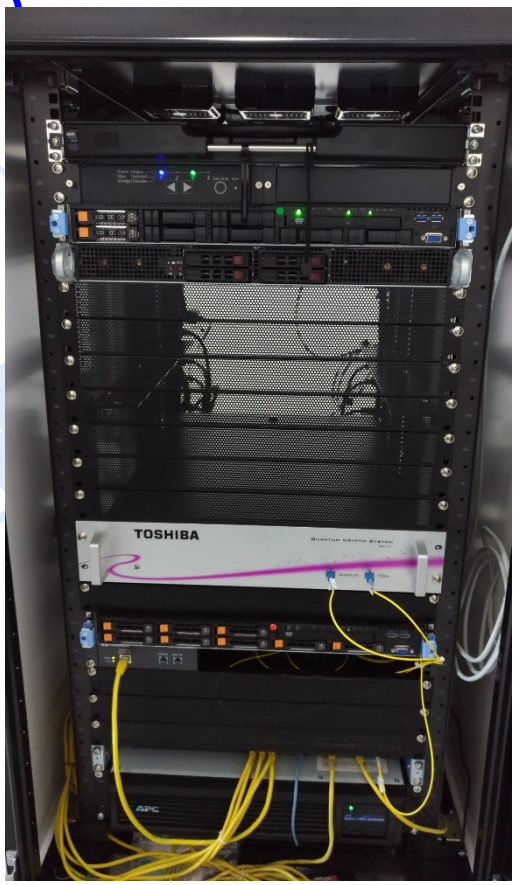
(1) 電子カルテ模擬データを量子暗号で秘匿化
(4) 生体認証の実データを量子暗号で秘匿化　参照データの分散バックアップ

（2）ゲノムデータ（模擬データ）への量子セキュアクラウド技術

- 「がんクリニカルシーケンス」のデータを完全秘匿化
- 社会実装の拠点開設を完了　光ファイバ敷設等に向け準備中

「がんゲノムシークエンス情報の受け渡しからエキスパートパネルの開催に至るまで」のデータフローの社会実装を実施・評価（今年度中）





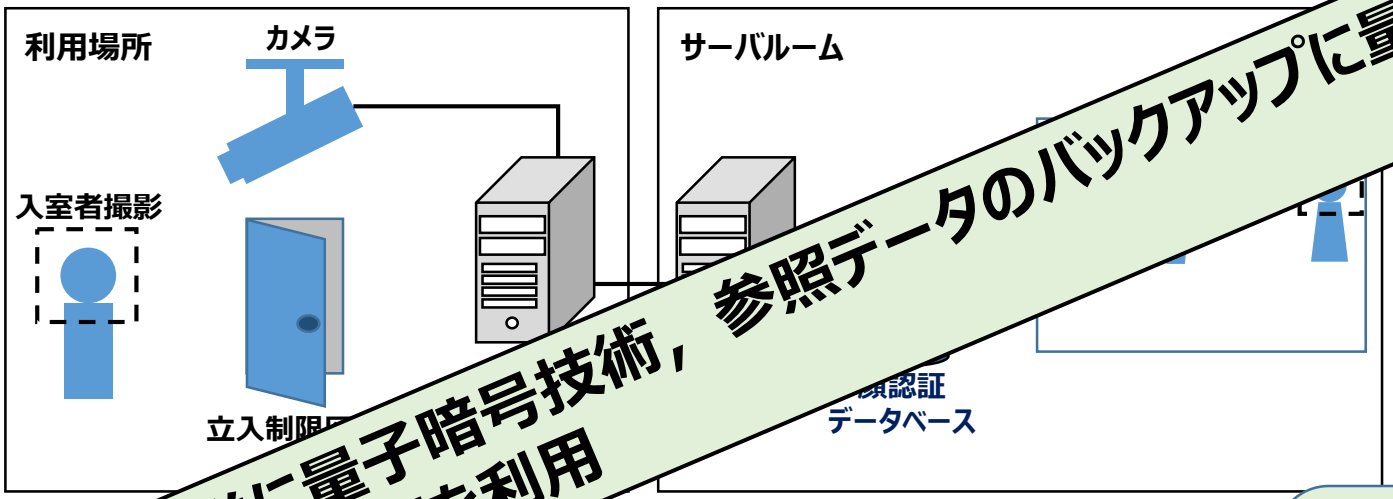
※1　ToMMo: 東北大学　東北メディカル・メガバンク機構
※2 東芝LSA: 東芝ライフサイエンス解析センター
※3 エキスパートパネル: 専門家による解析結果の意義づけと診療方針の検討を行う会議システム
※4 秘密分散は東芝LSA, ToMMo, 東北大学病院の3拠点で今年度整備実施予定　(NICT担当)

（４）生体認証への量子セキュアクラウド技術　CPSスマート製造への展開

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**

本人認証	なりすまし防止	ＶＩＰ対応	犯罪捜査等
・入退場管理 ・機密情報取り扱い	・銀行等での窓口業務 ・店舗等での業務取扱	・重要顧客の識別	・**犯罪者等の特定/追跡** ・**テロ対策等**



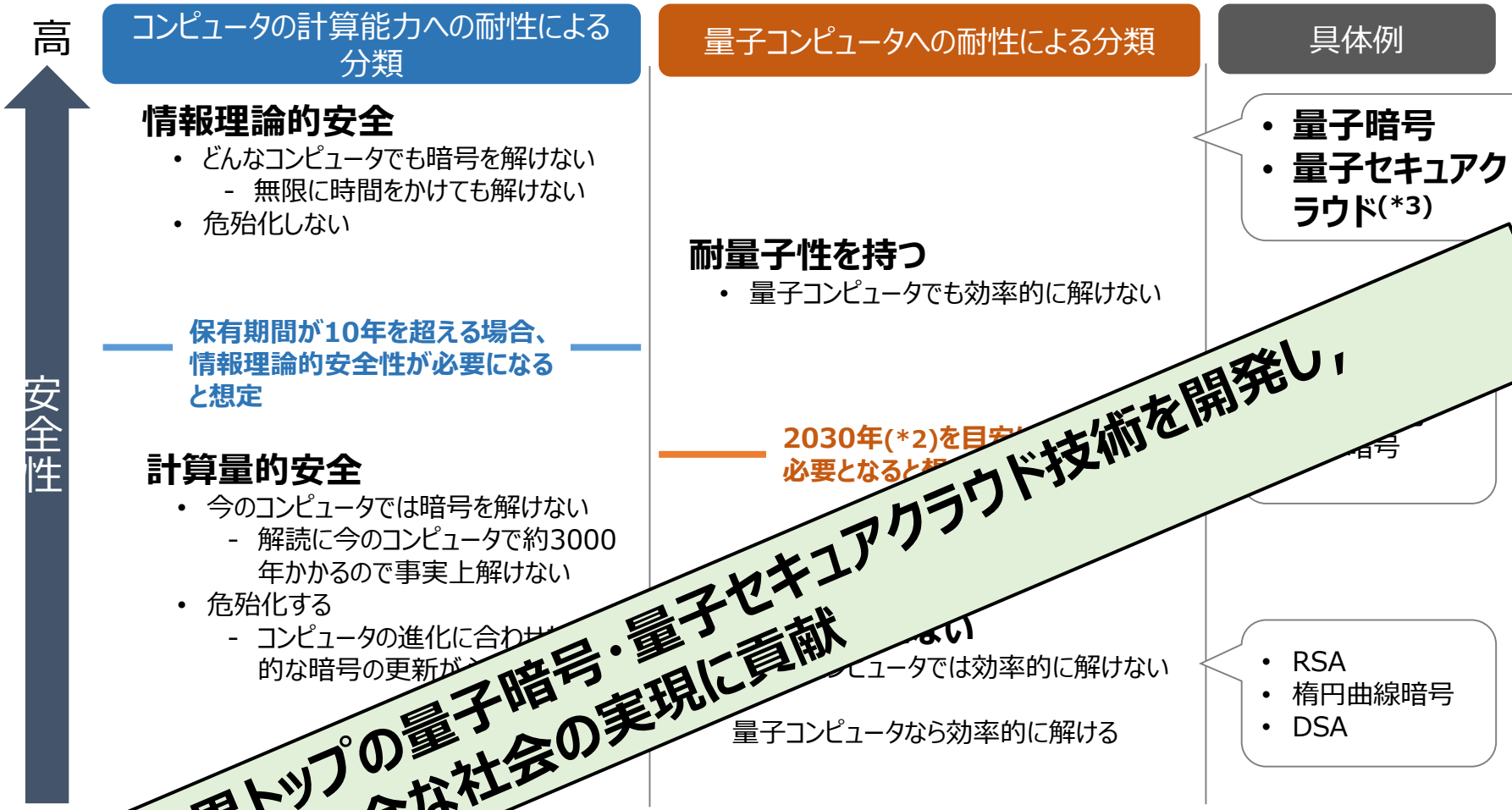
・データ伝送に量子暗号技術，参照データのバックアップに量子セキュアクラウド技術を利用

生体情報の漏洩リスク対策に量子暗号・量子セキュアクラウドを応用

適用の課題

・生体情報も**個人情報保護法の対象**
・生体情報は**登録時にも変更できない（高精度生体認証装置全般）**
・情報漏洩で偽造されると**なりすまし等の被害**が発生し甚大被害
・個人情報の漏洩は**多額の損害賠償の懸念**

まとめ



(*1) 便宜
以では十分に安全とされている
(*2) NIST
Part1 Rev4, 5.6.2（https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf）にて
「112b
ecurity は2030年まで許容するが、それ以降の適用は禁止」と明言している
(*3) 乱数生成方法等にも依存し，プロトコルの検討が必要