資料2

量子暗号技術に関する動向と展望

情報通信研究機構 未来ICT研究所
主管研究員　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

背景

様々な重要情報がデジタル化されて、データサーバ上に永遠に保存され続ける時代

・個人の生体認証データ、医療・ゲノム情報
・企業競争力の源泉となる製造ノウハウ、技術情報

一度漏洩すれば

・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

→ 世紀単位の超長期間にわたる安全性保証

今そこにある脅威

(1) “Store now, decrypt later” attack

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

米国家安全保障局データセンタ

(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

重要データの流通、保管には

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

現代暗号のみでは実現不可能

解決に向けた戦略

どんな計算機でも解読できない暗号通信を実現

量子暗号

秘密分散

原本データを無意味化された複数のデータに分散し保管

統合

どんな計算機でも解読や改竄ができない**超長期セキュアデータ保管システム**を実現

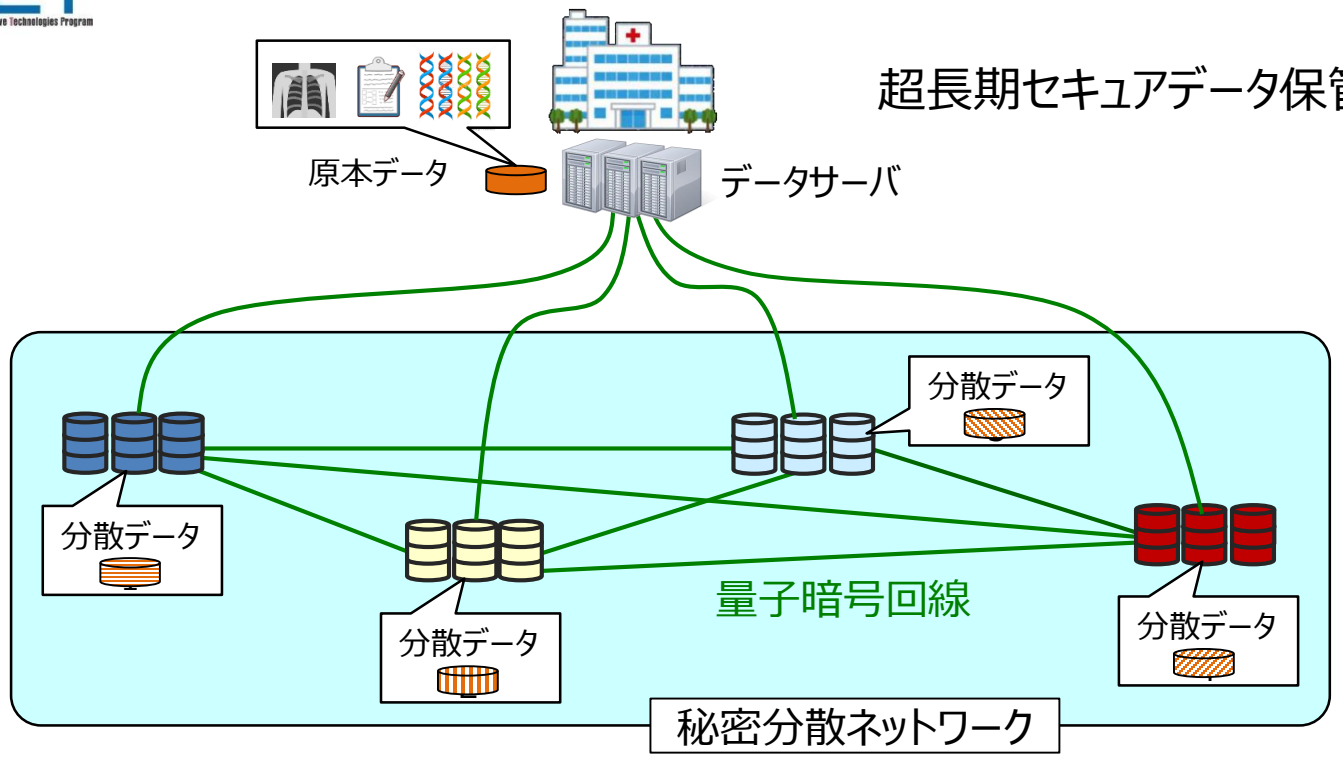
- ✓ 暗号方式を更新することなく、世紀単位の超長期間にわたりデータを安全に保管
- ✓ 震災等で一部のサーバが棄損しても、残ったサーバから原本データを復元

革新的研究開発推進プログラム ImPACT Impulsing Paradigm Change through Disruptive Technologies Program

NICT

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

超長期セキュアデータ保管システム

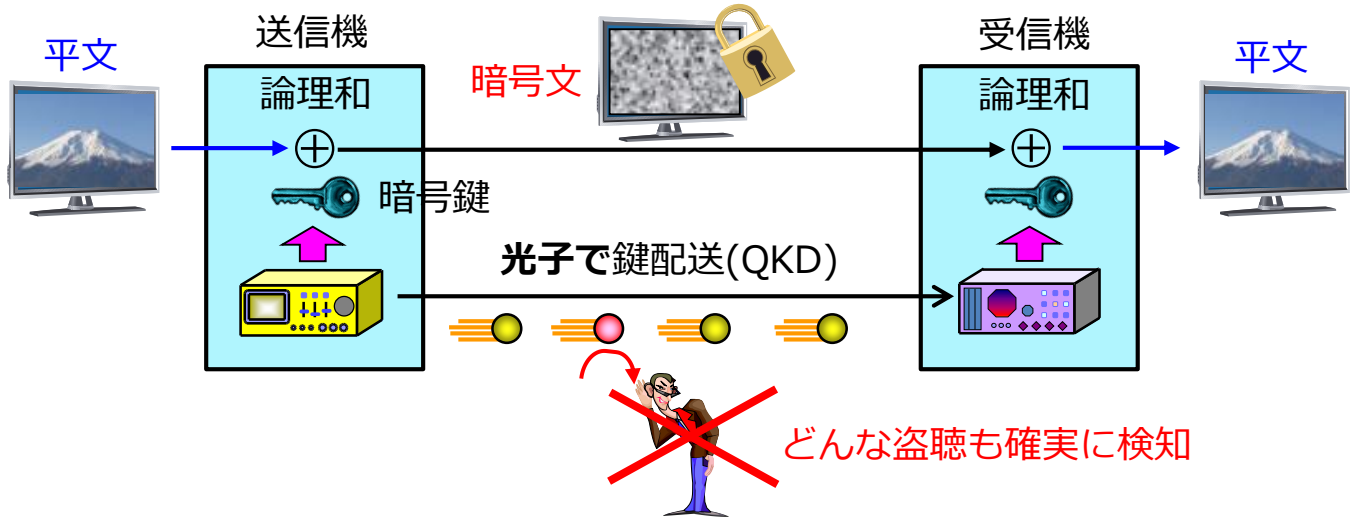


量子暗号

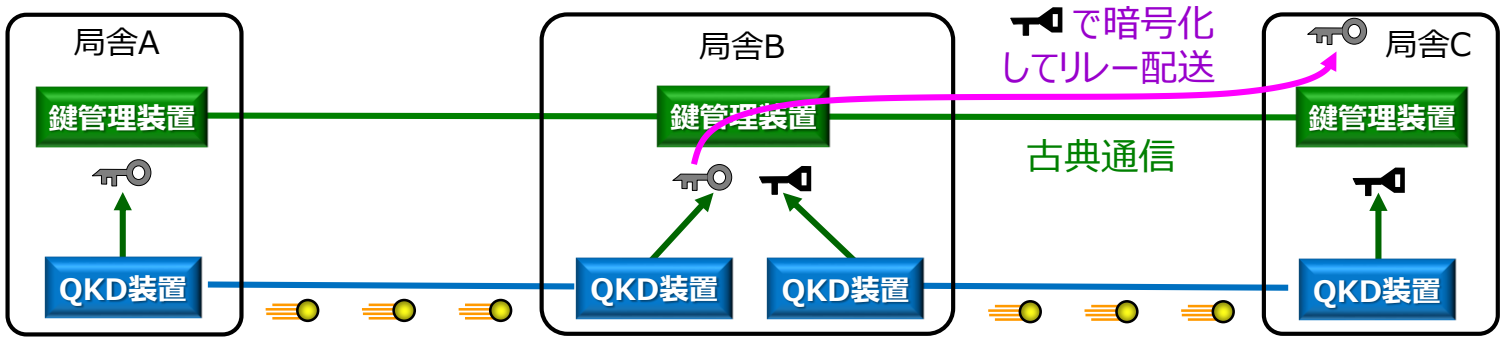
どんな計算機でも解読できない暗号通信を実現

①光子一個一個に乱数情報を載せて伝送、2地点間で同一の鍵を共有
量子鍵配送（Quantum Key Distribution: QKD）

②平文と同じサイズの鍵で暗号化、一回一回使い捨て：**ワンタイムパッド（OTP）**



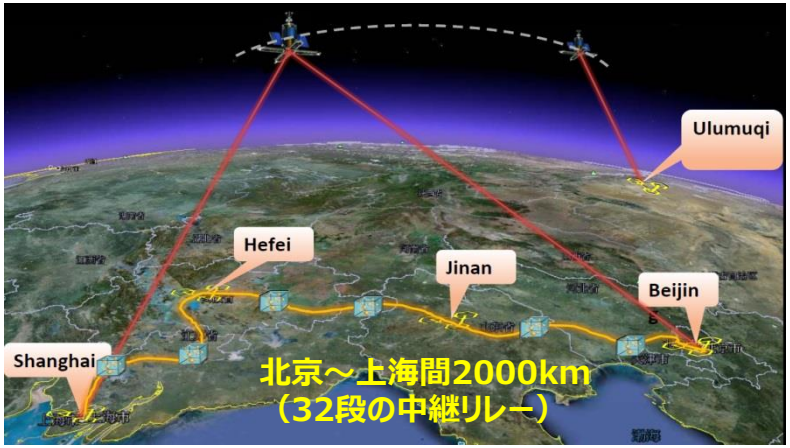
ネットワーク化は『**信頼できる局舎**』を介した鍵のバケツリレーで実現



海外動向

中国の躍進

・2017年7月、衛星量子暗号を世界で初めて実証
・2018年3月、世界最大の量子暗号ネットワークを構築
⇒新華社通信、中国工商銀行、国家電網公司などが利用。
重要インフラ網を他国のサイバー攻撃から防御する狙い
Q. Zhang et al., Opt. Express 26, 24260 (2018).



図は中国科学技術大学, Q. Zhang氏のご好意による

2018年、大手通信キャリアが投資を開始

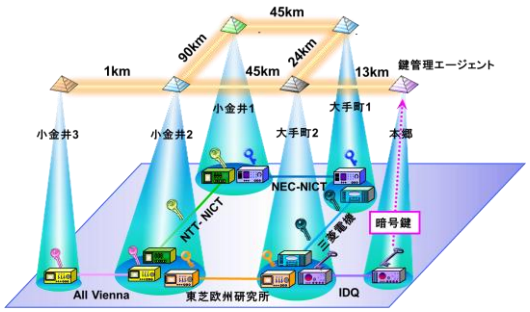
・2月、SK Telecom（韓国）がジュネーブ大発のベンチャーID Quantique社に$65M（71億円）出資。５Gのセキュリティインフラ市場を狙う。
https://www.idquantique.com/id-quantique-sk-telecom-join-forces/
・3月、ブリティッシュテレコムが英国初の量子暗号網をCambridge ~ Ipswich間に構築。
https://www.advaoptical.com/en/newsroom/press-releases/20180613-adva-fsp-3000-powers-uks-first-quantum-network
・6月、テレフォニカ，ファーウェイ，マドリード工科大学が商用網で量子暗号の実証試験を開始。
https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S01_WORLD_TOUR/UNIofYORK_SPILLER.pdf
・6月、米Quantum Xchange社がWall Street金融市場向けに量子暗号サービスを発表。
https://quantumxc.com/
・7月、ドイツテレコムの実証通信網にSK Telecom、IDQが量子暗号システムを提供。
https://www.zdnet.com/article/sk-telecom-applies-quantum-key-to-deutsche-telekom-network/

我が国の取り組みの経緯と現状

2010年 2018年 2023年

NICT委託研究 → **ImPACT** → **SIP第2期**

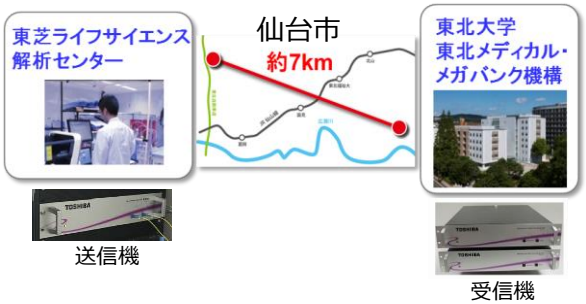
2010年、東京量子暗号ネットワークテストベッドを構築



✓ 動画の量子暗号化を世界で始めて実現

NEC：サイバーセキュリティ関連施設で試験運用

東芝：ゲノム解析データの暗号通信



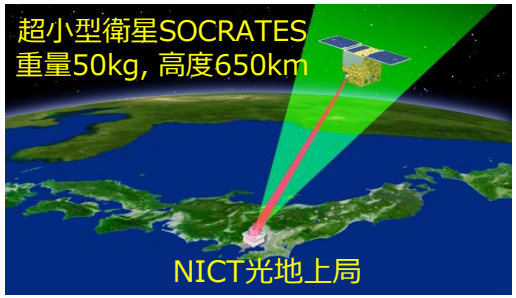
✓ **世界最高速の装置**を開発
300kbps @45km （東芝）

海外製の**10倍高速、2倍長距離**

✓ 鍵管理アーキテクチャ確立

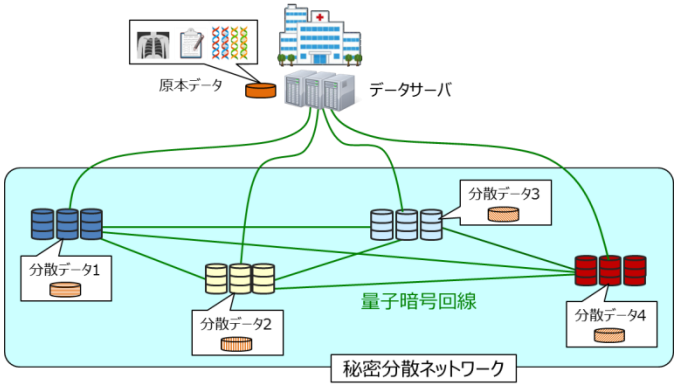
✓ 新たなアプリの開発
「超長期セキュアデータ保管」
(**量子暗号x秘密分散**)

✓ NICTが超小型衛星で量子通信を実証（2017年）



光・量子を活用したSociety5.0実現化技術

量子セキュアクラウド技術を開発し、将来にわたり安全なデータ保管と利活用を実現



➢ 専用用途での量子暗号サービス

政府重要拠点間等での利用を検討
⇒ 民間用途への展開

➢ 標準化、運用ガイドライン案を策定

➢ 量子セキュアクラウドシステムの社会実装

総務省・委託研究

衛星通信における量子暗号技術

量子暗号に関する標準化活動

- Network framework (SG13)
- Network security (SG17)

2018年9月からネットワークのフレイムワーク、鍵管理、アーキテクチャの3項目について勧告草案化（日本、中国、韓国、スイスなど）。
⇒2019年5月NICTで中間会合

2019年1月ネットワークセキュリティについて勧告草案化（日本、中国、韓国、スイス、アメリカなど）。
⇒ 2019年6月上海で中間会合

World Class Standards

2008年からIndustry Specification Group -QKDにおいて、部品・モジュール・インターフェース仕様策定、実装安全性（サイドチャネル攻撃対策など）の標準化。

装置の安全性評価手法

2017年10月からカナダ、中国、英国、日本など

日本からNICT、東芝、NEC等が参加。
・実装安全性に関する白書(2018年7月)
・東芝が鍵供給インタフェースを標準化(2019年2月)

量子ICTフォーラム/量子鍵配送技術推進委員会

2017年10月設立

電子カルテの分散バックアップ実証実験

- **第1世代：共通鍵暗号**
  ⇒量子コンピュータでも解読困難
- **第2世代：量子暗号**
  ⇒将来のどんな計算機でも解読不可能

電子カルテの標準データ
交換規格 SS-MIX準
拠の模擬データ

JGN-大阪AP

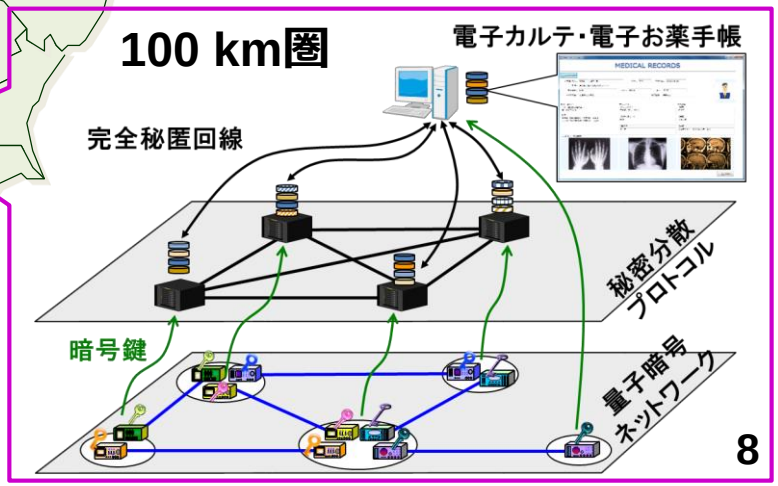
JGN-名古屋AP

JGN-大手町AP

800 km

第1世代
広域圏用の共通鍵暗号

第2世代：量子暗号
(Tokyo QKD Network)



耐量子-公開鍵認証基盤によるアクセス管理の実装

量子コンピュータでも解読が困難とされる公開鍵暗号

厚生労働省推奨のHealthcare PKI

・医療従事者の国家資格
・患者の被保険者番号

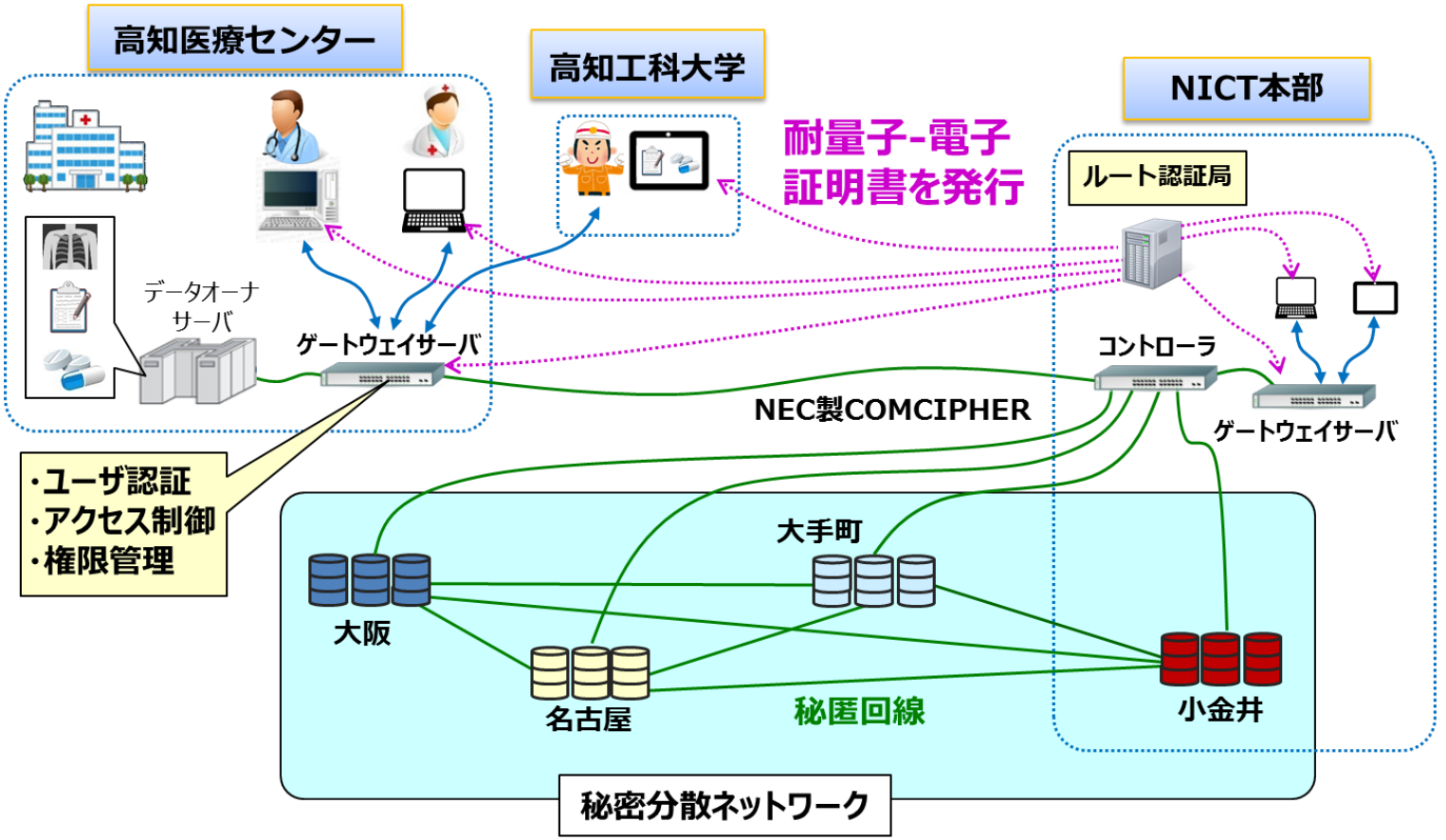
} に基づくユーザ認証　⇒ 耐量子化

革新的研究開発推進プログラム ImPACT Impulsing Paradigm Change through Disruptive Technologies Program

NICT

TECHNISCHE UNIVERSITÄT DARMSTADT

ISARA



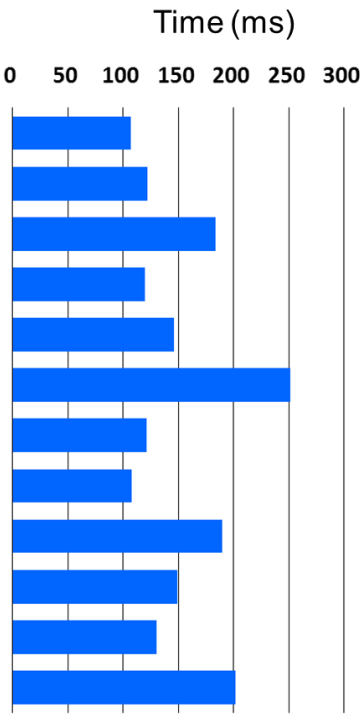
ルート認証局	鍵交換	署名	暗号化	メッセージ認証
LMS（ハッシュ）	NewHope（格子）	Dilithium (格子)	AES 256 (GCM)	SHA 384
		q-TESLA（格子）		
		Rainbow（多変数）		
	SIDH（超特異楕円）	Dilithium (格子)		
		q-TESLA（格子）		
		Rainbow（多変数）		
XMSS（ハッシュ）	NewHope（格子）	Dilithium (格子)		
		q-TESLA（格子）		
		Rainbow（多変数）		
	SIDH（超特異楕円）	Dilithium (格子)		
		q-TESLA（格子）		
		Rainbow（多変数）		

12種類の暗号スウィートを実装、評価

高知医療センター・ゲートウェイサーバとNICT・クライアント端末間で、耐量子-TLSによる認証、鍵交換の動作試験を実施

Transport Layer Security (インターネットの標準的なセキュリティプロトコル)

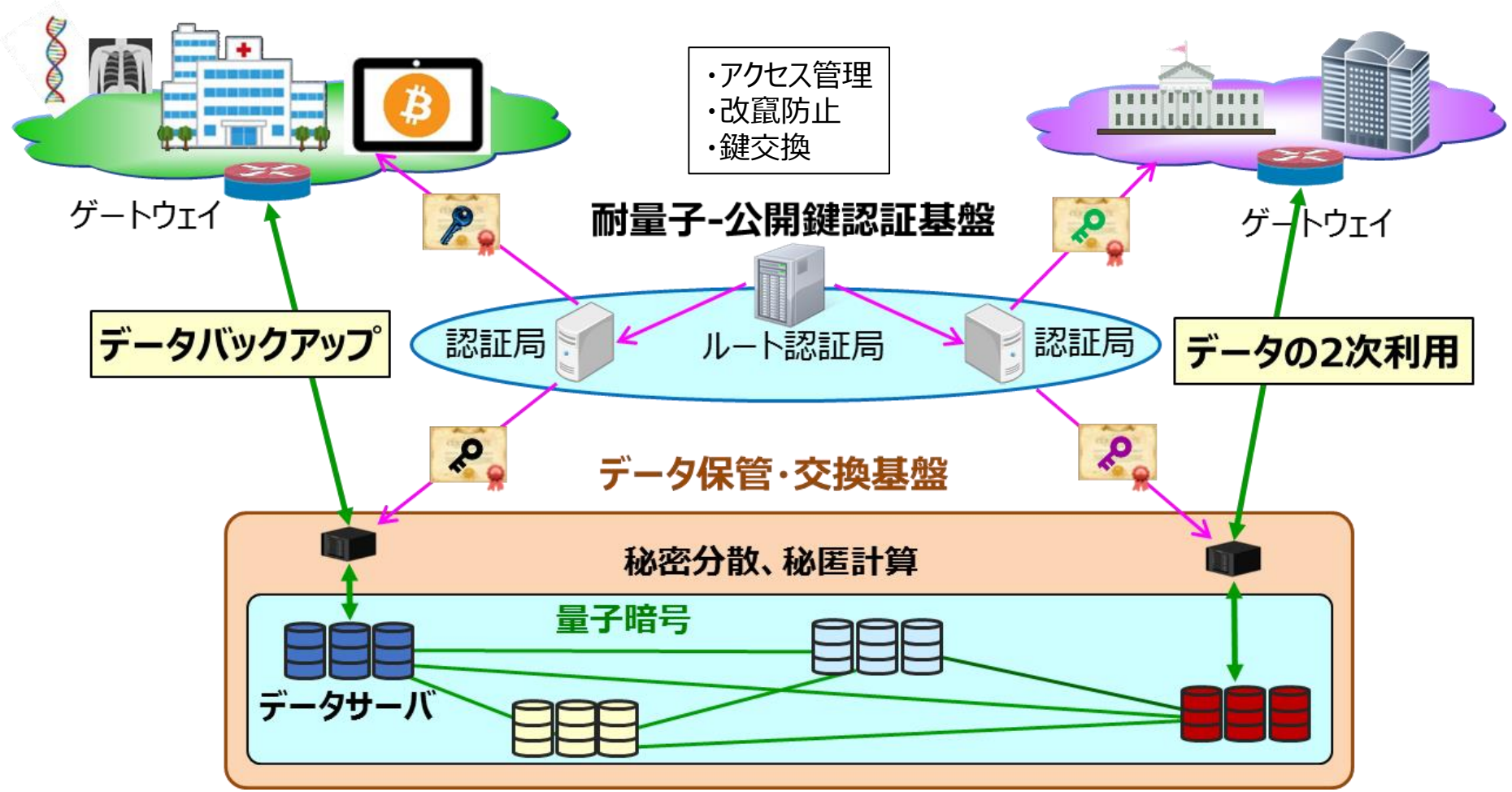
Root certificate	Key exchange	Signature	Time (ms)
LMS	NewHope	Dilithum	107.2
		q-TESLA	122.2
		Rainbow	183.9
	SIDH	Dilithum	120.2
		q-TESLA	146.4
		Rainbow	251.7
XMSS	NewHope	Dilithum	121.7
		q-TESLA	107.7
		Rainbow	189.6
	SIDH	Dilithum	149.2
		q-TESLA	130.0
		Rainbow	201.9



高知医療センター 認証サーバ⇔NICT ノートPC 処理時間

全ての暗号スウィートが正常動作、既存TLSと同等の処理速度

将来の実装イメージ


・アクセス管理
・改竄防止
・鍵交換
ゲートウェイ
耐量子-公開鍵認証基盤
ゲートウェイ
データバックアップ
認証局
ルート認証局
認証局
データの2次利用
データ保管・交換基盤
秘密分散、秘匿計算
量子暗号
データサーバ