平成28年8月4日
有識者会議

公開用
資料３

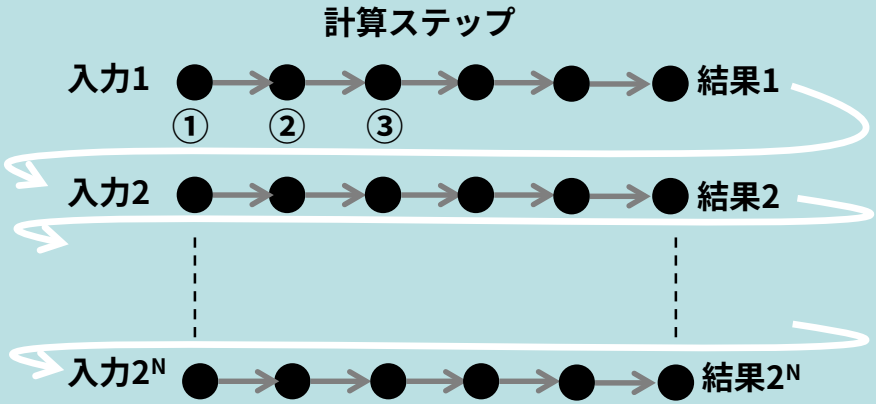
革新的研究開発推進プログラム（ImPACT）

「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」進捗状況報告について

プログラム・マネージャー
山本　喜久

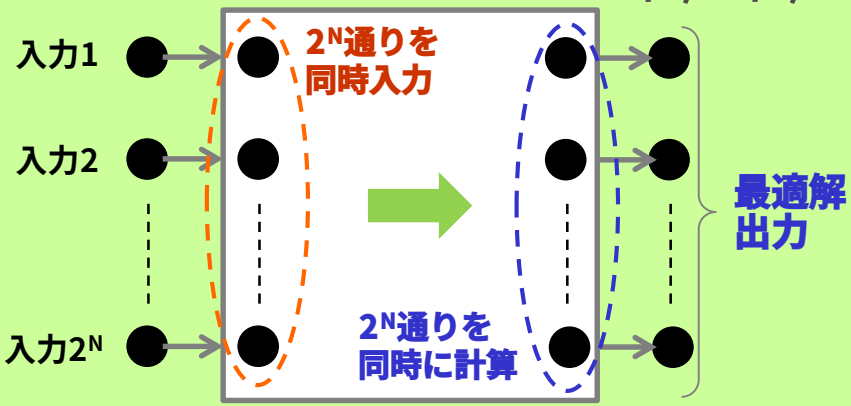
目標設定の背景
ー現代コンピュータの限界と量子コンピュータの登場ー

現代コンピュータ



N個の自由度（ビット）に対して2^N通りある全ての入力値に対する総当り計算が必要である。

量子コンピュータ（量子ビット $|0\rangle + |1\rangle$）



N個の量子ビットは2^N通りの全ての入力値を同時に表し、並列計算を可能にする。

スーパーコンピュータ

スーパーコンピュータを使っても追いつかない計算量爆発

問題サイズ N	解の候補 2^N
10	1000
20	100万
30	10億
40	1兆
50	1000兆
⋮	⋮

研究開発プログラム構想

解決すべき課題

現代社会の様々な分野（創薬、通信ネットワーク、スパース推定など）では、大規模な**組合せ最適化問題**を**高速**で解くことが大きなブレークスルーへつながる。

社会に**クラウドサービス**が普及し、サーバやネットワークに存在する**個人情報や機密情報のセキュリティ**をどうやって担保するのか、が喫緊の課題になっている。

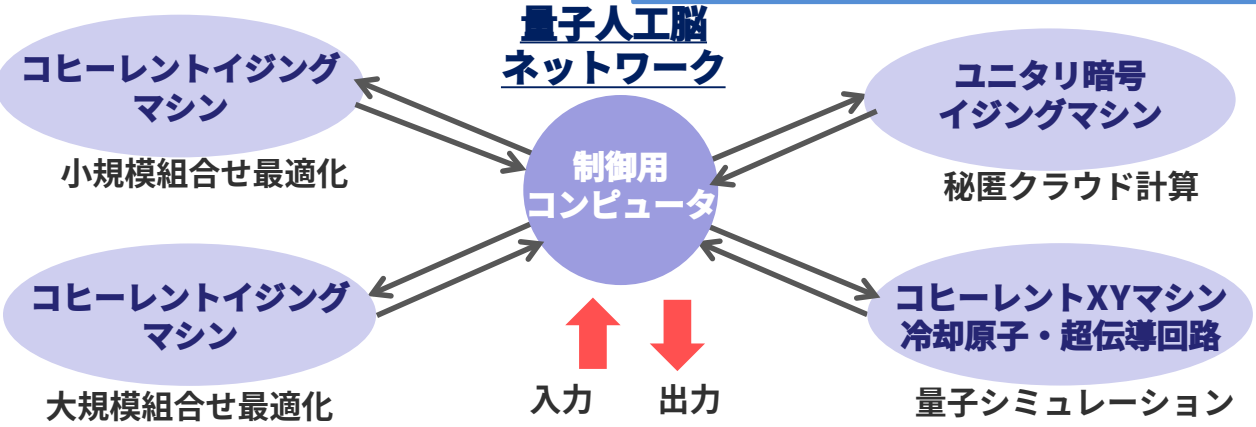
物質探索や分子合成の現場では、**数値シミュレーション**の重要性が増してきているが、現代コンピュータの計算能力はそうした需要に追いついていない。

ImPACTプロジェクトのねらい

従来のコンピュータアーキテクチャーを捨て、**ニューラルネットワーク全体に広がった波動関数**を利用して計算を行なう量子人工脳を開発する。

クラウドユーザだけが持っている秘密鍵で暗号化されたデータ（暗号文）上で直接計算を実行できる**秘匿計算ネットワーク**を開発する。

対象である物質や分子を記述するモデルをニューラルネットワークに広がった波動関数に埋め込み、**模擬実験**により科学的探索を可能にする**量子シミュレータ**を開発する。



実施体制の再編成

量子セキュアネットワーク

ネットワーク設計・アプリケーション実装
NICT (佐々木)

量子鍵配送装置開発
NEC（津村）
東芝（井上）
三菱電機（松井）
学習院（平野）

安全性評価技術
北大（富田）
NTT（玉木）

新原理・新方式開拓
東大（小芦）
東工大（松本）

量子人工脳

アルゴリズム開発
東大（合原）
NII（宇都宮）
東理大（長谷川）
京大（大関）
はこだて未来大（香取）
東工大（青西）

ハードウェア開発
小規模システム
スタンフォード大 (Fejer)
大規模システム
NTT (武居)
量子測定フィードバック
阪大（井上）
XYマシン
NII (宇都宮)
アルネアラボラトリ (太田)

平成28年度第一四半期で終了

基礎理論
NII（宇都宮，河原林）
東大（合原）
スタンフォード大（Mabuchi）

量子シミュレーション

半導体・超伝導量子シミュレータ開発
理研（樽茶，中村，蔡）

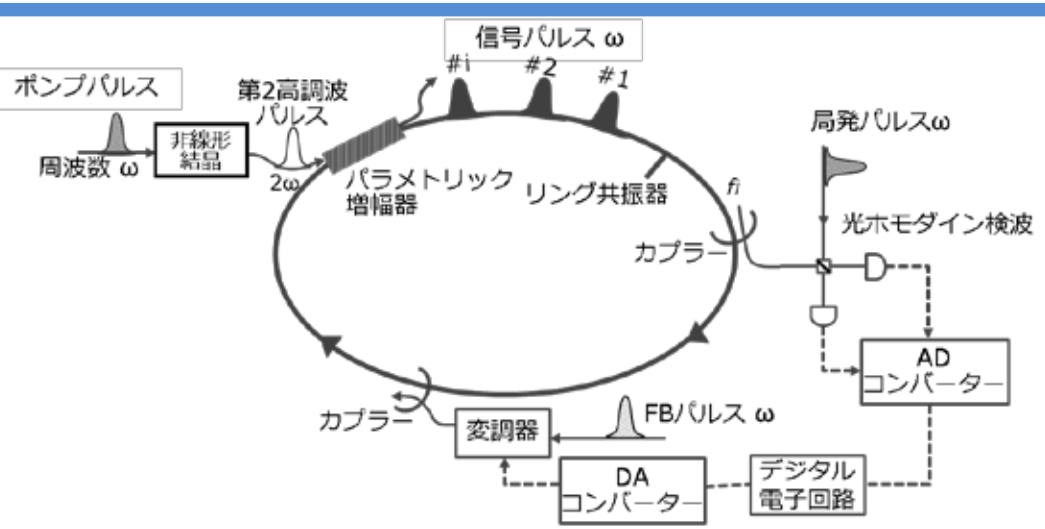
冷却原子量子シミュレータ開発
京大（高橋）
理研（福原）

ポラリトン量子シミュレータ開発
ウルツブルグ大 (Höfling)

非平衡開放系量子シミュレーション理論
阪大（小川）
理研（永長，Nori）
東大（川島・青木）

量子アニーリング理論
東工大（西森）

量子人工脳ハードウェア開発



- スタンフォードマシン
  （100ニューロン, 連続値全結合）
- NTTマシン
  （2000ニューロン, 離散値全結合）

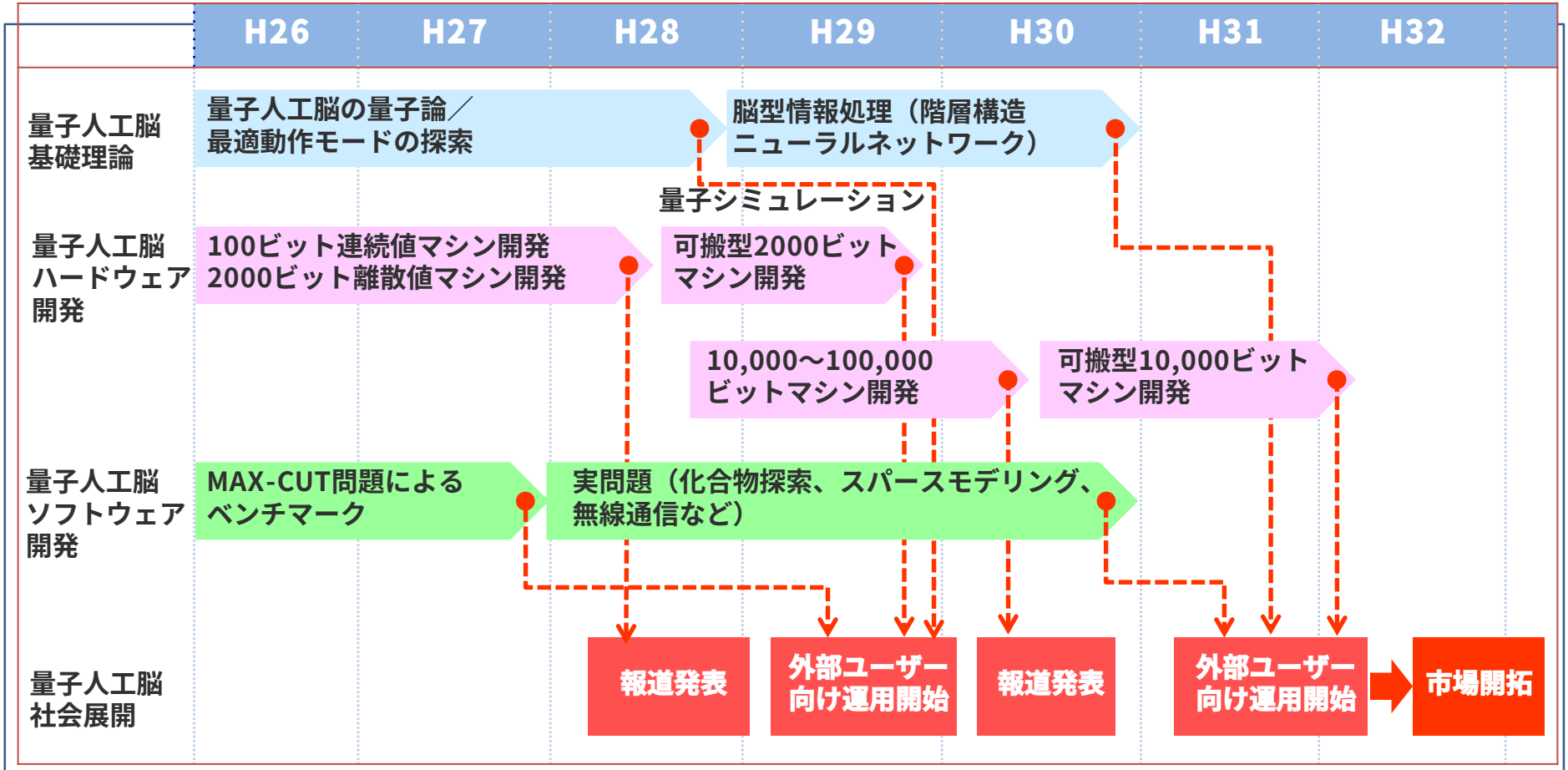
競合技術との比較

	NTTマシン	D-WAVEマシン	Hitachiマシン	IBM True North
原理	量子(ニューラルネットワーク)	量子(アニーリング)	古典(アニーリング)	古典(ニューロチップ)
ビット数N	2048 (~ 10^5)	1156	20,000	256 (~ 10^6)
結合数	全結合（~ $4x10^6$） 全結合（~ 10^{10}）	スパース（~ 3,300）	スパース（~ $5x10^4$）	全結合（~ $6x10^4$） 疎結合（~ $2x10^8$）
問題サイズ	N = 2048 (N = 10^5)	$\sqrt{N}$ = 33	$\sqrt{N}$ = 140	N = 256 ($\sqrt{N}$ = 10^3)

今後のマシン開発計画

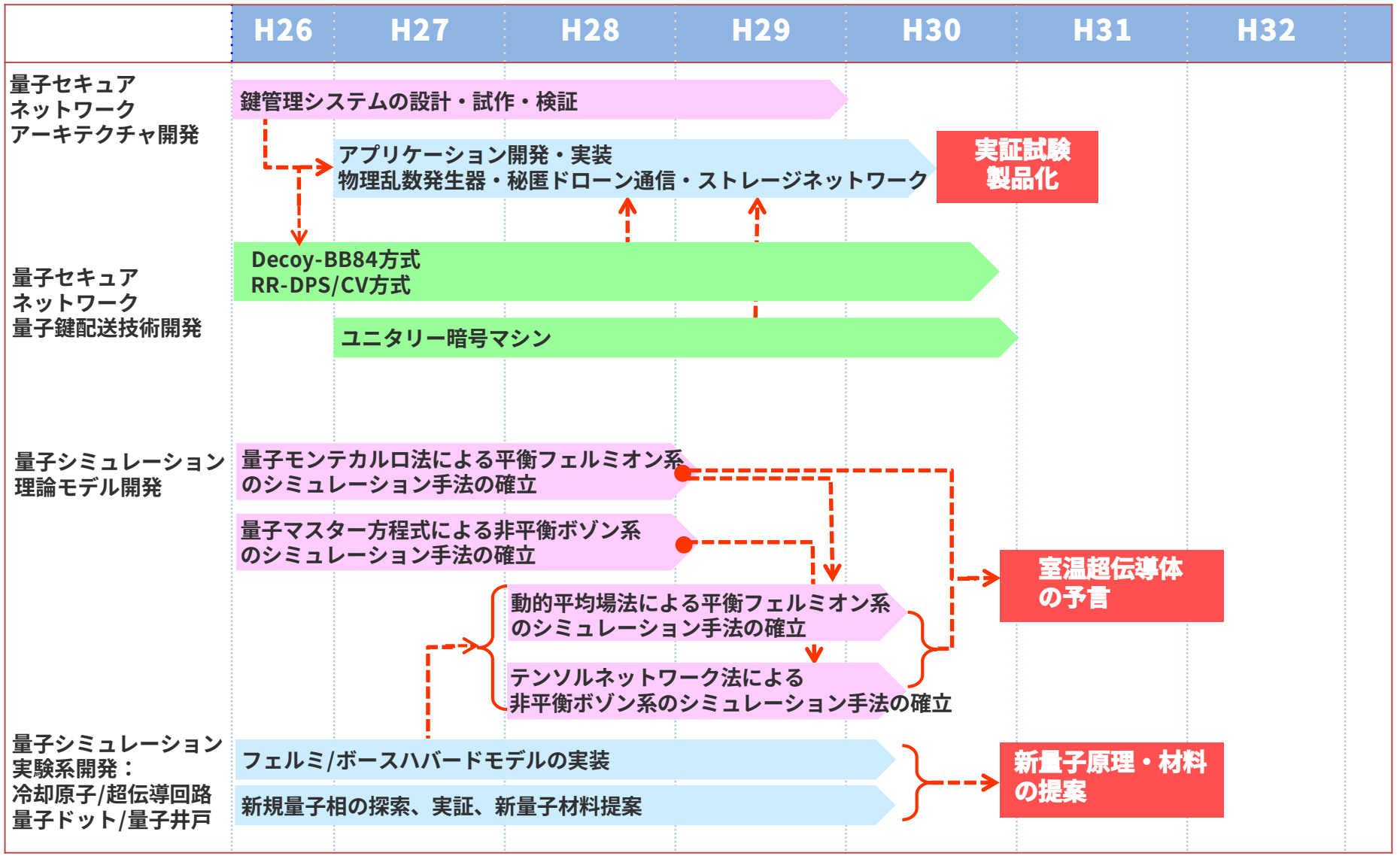
- 可搬型マシン（H29.3）　2,048ビット（離散値全結合）　512ビット（連続値全結合）
- 大型マシン　（H29.12）　100,000ビット（離散値）　10,000ビット（連続値）

開発ロードマップ



- H28年度末までに、2000ビット量子人工脳の開発を完了し、報道発表を行なう。
- H29年度半ばまでに、2000ビット量子人工脳（可搬型）を用いた外部ユーザー向け運用を開始する。
- H30年度半ばまでに、様々な実問題アルゴリズムを実装した10,000～100,000ビット量子人工脳の開発を完了し、報道発表を行なう。
- H31年度末までに、10,000～100,000ビット量子人工脳（可搬型）を用いた外部ユーザー向け運用を開始する。
- その後、市場開拓、セキュリティ対策、小型化・低価格化に取り組む。

開発ロードマップ２


H26
H27
H28
H29
H30
H31
H32
量子セキュア
ネットワーク
アーキテクチャ開発
鍵管理システムの設計・試作・検証
アプリケーション開発・実装
物理乱数発生器・秘匿ドローン通信・ストレージネットワーク
実証試験
製品化
量子セキュア
ネットワーク
量子鍵配送技術開発
Decoy-BB84方式
RR-DPS/CV方式
ユニタリー暗号マシン
量子シミュレーション
理論モデル開発
量子モンテカルロ法による平衡フェルミオン系
のシミュレーション手法の確立
量子マスター方程式による非平衡ボゾン系
のシミュレーション手法の確立
動的平均場法による平衡フェルミオン系
のシミュレーション手法の確立
テンソルネットワーク法による
非平衡ボゾン系のシミュレーション手法の確立
室温超伝導体
の予言
量子シミュレーション
実験系開発：
冷却原子/超伝導回路
量子ドット/量子井戸
フェルミ/ボースハバードモデルの実装
新規量子相の探索、実証、新量子材料提案
新量子原理・材料
の提案

量子セキュアネットワークプロジェクト

(1) 解決すべき課題

現代暗号は、将来盗聴される、あるいは既に盗聴されている危険性を内包しており、常に改訂や変更を繰り返す必要がある複雑なシステムとなっている。
また、クラウドサービスの普及が進み、クラウド上に保存したデータや計算結果のセキュリティをどう担保するか、が重要な社会的課題となっている。

(2) 課題のブレークダウン

- ゲノム情報など世紀単位の超長期間にわたって秘匿すべき重要情報が急増
- 計算量に基づく現代暗号のみでは、クラウド上での超長期間の安全性保証は実現不可能
- 抜本的対策は未開発
  ⇒ 暗号分野のホットトピック

- ドローンやスマートフォン、自動運転車など移動体のネットワーク技術が急進展
- これらの通信を守る暗号技術は未だ満足に実装されていない
- 安心安全なサービスを実現してゆく上で大きな障害

(3) 解決に向けた戦略・シナリオ

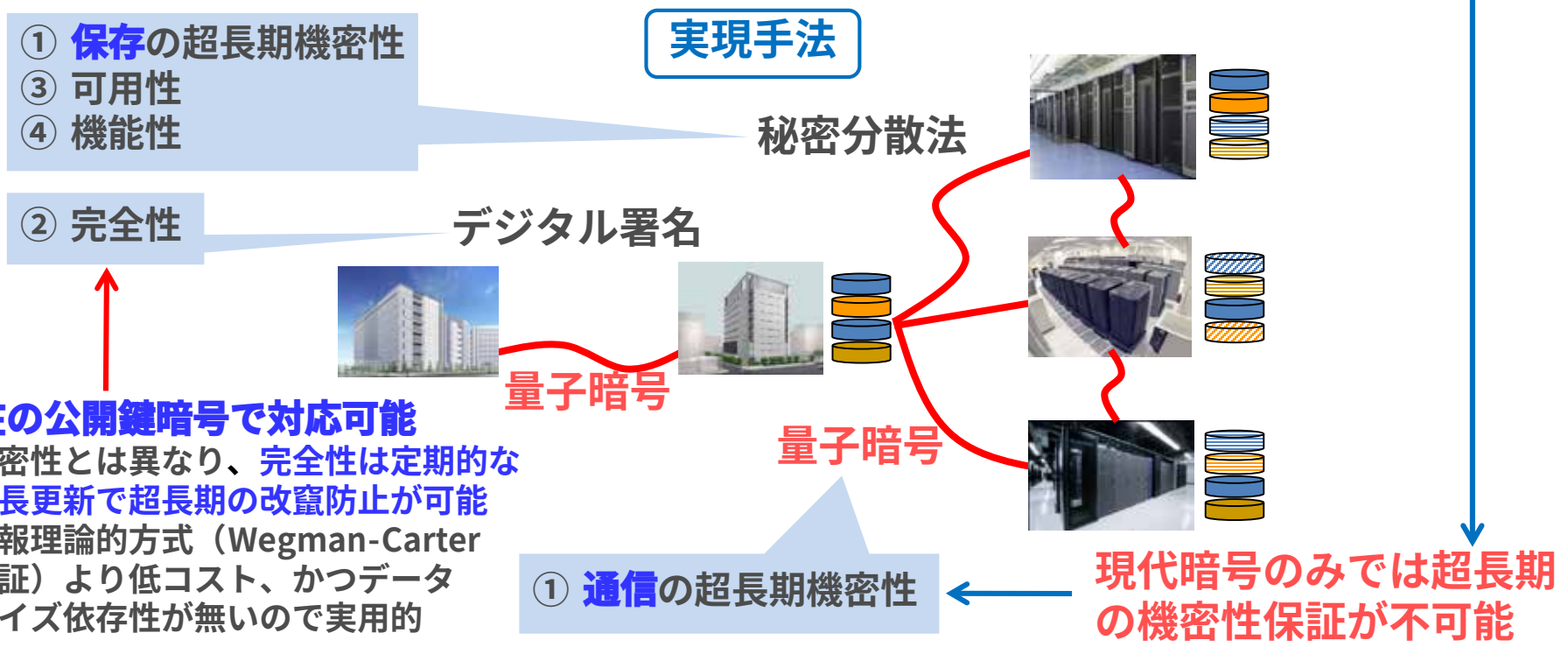
盗聴・解読技術が進展しても安全性が危殆化しない量子セキュアネットワークを構築
⇒
秘密分散法と組み合わせることにより、**超長期安全性を保証しながら計算機能も有するデジタルアーカイブ技術**を開発

様々な移動体に量子セキュアネットワークから鍵を供給することで、**ワイヤレスネットワークのセキュリティを向上**
⇒
将来にわたり安心安全なサービスを実現してゆくための基盤を構築

(4) 戦略・シナリオ実現へのアプローチ

超長期間安全性を保証するデジタルアーカイブシステムに要求される要件

① 機密性：通信時と保存時に正規ユーザ以外に平文が漏れないこと ⇒ 暗号化
② 完全性：平文が改竄されていないこと ⇒ 署名、認証
③ 可用性：必要な時に平文を得られること ⇒ データバックアップの分散化
④ 機能性：暗号文のまま情報処理ができること ⇒ 完全準同型暗号化

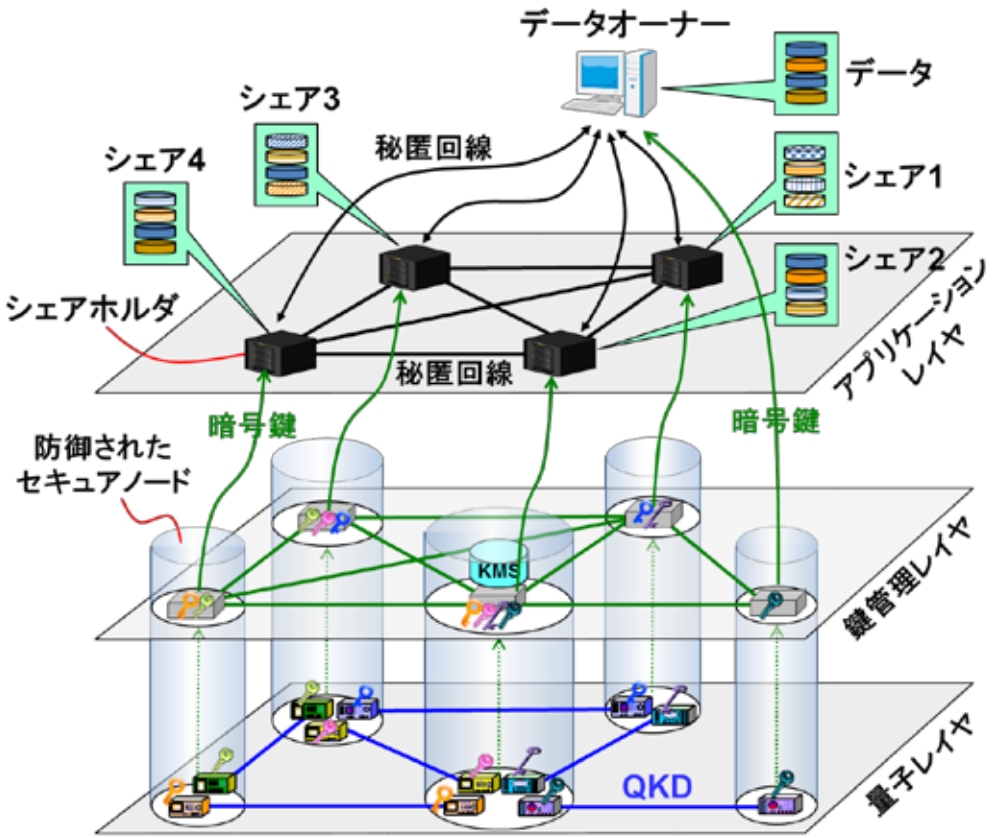


超長期デジタルアーカイブシステムは、現代暗号、ネットワーク技術、量子暗号の融合によって初めて実現される ⇒ 我が国が世界に先駆けて実現し、産業競争力を強化

研究開発の現状と今後の課題（1/2）

超長期安全性を持つデジタルアーカイブ技術の原理実証に成功

- 計算量には拠らない安全な保存と伝送 ⇒ 超長期（世紀単位）の機密性
- 量子鍵によるメッセージ認証 ⇒ 超長期の改竄防止
- 分散シェアの一部が失われてもデータを復元可能 ⇒ 高い可用性
- 分散シェアで加算・乗算が可能 ⇒ 秘匿化したまま情報処理が可能



フィールドテストベッド (Tokyo QKD Network) 上での実証に成功

シャミアの閾値秘密分散プロトコル

量子鍵を使いデータ回線の秘匿化とメッセージ認証を実現

量子鍵配送 (QKD) ネットワーク

今後、
- 鍵運用を効率化
- 秘密分散処理を高速化

研究開発の現状と今後の課題 (2/2)

- 様々なセキュリティアプリケーション（下図）を開発し国家戦略特区等で実証試験を実施
  ⇒ 今後、乱数源、認証技術などの要素技術をドローンやスマートフォンに搭載し製品化
- 実用機の信頼性試験を開始（サイバーセキュリティ関連情報やゲノムデータの暗号化試験など）
  ⇒ 今後、各デバイスコンポーネントの信頼性向上、装置の安全性保証技術の開発を強化
- 雑音耐性を向上させる新原理を開拓、小型化・波長多重化を可能にする方式を開発
  ⇒ 今後、次世代技術としてさらにブラッシュアップ

秋田県仙北市(地方創生・近未来特区)における実証実験(2016年4月)

実用機：
おとり信号型BB84方式
次世代技術：
- 雑音耐性に優れたラウンドロビン差動位相シフトQKD方式
- 直交位相変調QKD方式

今後、
- デバイスコンポーネントの信頼性向上
- 装置の安全性保証技術の開発