量子コンピューターの先端動向と未来

サイバーセキュリティシンポジウム2023

科学技術振興機構 研究開発戦略センター フェロー　嶋田 義皓

サイバーセキュリティ研究所
Cybersecurity Research Institute

はじめに…

しまだ　よしあき
嶋田 義皓
科学技術振興機構（JST）
研究開発戦略センター（CRDS）　フェロー

略歴

東京大学大学院工学系研究科物理工学専攻博士課程修了。博士（工学、公共政策分析）。
専門分野は、物性物理、科学コミュニケーション、ICT、科学政策。

日本科学未来館で科学コミュニケーターとして展示解説や実演・展示制作に、JST戦略研究推進部でICT分野の研究推進業務に従事後、2017年より現職。著書に『量子コンピューティング 基本アルゴリズムから量子機械学習まで』（オーム社）。

第２次量子革命

次なる”半導体級”イノベーションへの期待

量子ICT社会

量子センサー

量子暗号・量子通信

相補性

量子コンピューター

猫状態

量子テレポーテーション

量子シミュレーション

ホログラフィー原理

複製不可能定理

量子マテリアル

量子もつれ

ベル不等式

量子相制御

EPR相関

マクロ量子現象

トポロジカル物質

量子干渉

トンネル効果

半導体技術

エネルギー準位

ICT

光通信

不確定性原理

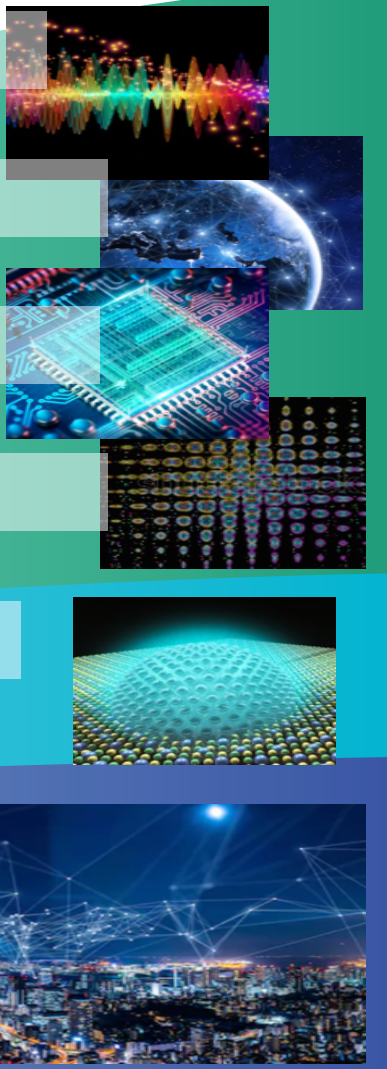
バンド構造

2nd 量子革命

量子力学による
情報の制御

1st 量子革命

量子力学による
物質・エネルギーの
制御

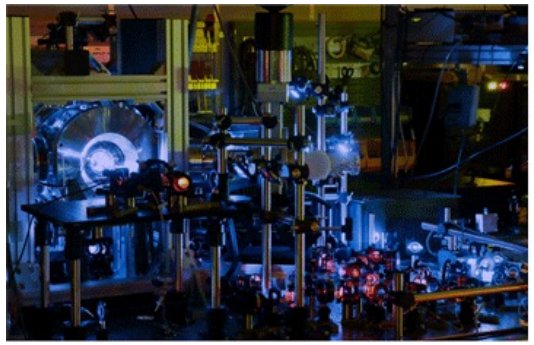


量子ICT

量子力学の性質を情報処理に役立てる

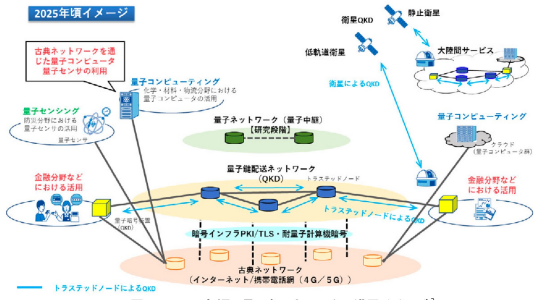
量子センシング

量子干渉・量子もつれを使ってセンサーを高精度化・高感度化



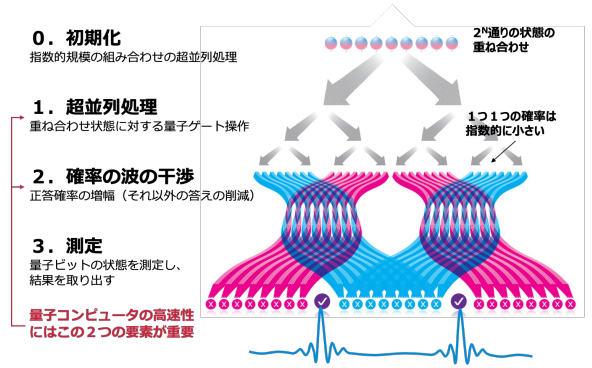
量子暗号・通信

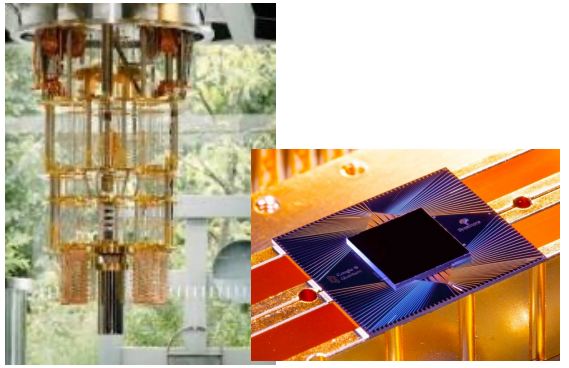
不確定性原理・量子もつれを使って通信・ネットワークの安全性を向上



量子コンピューター

量子干渉・量子もつれを使ってコンピューターを高速化・省エネ化





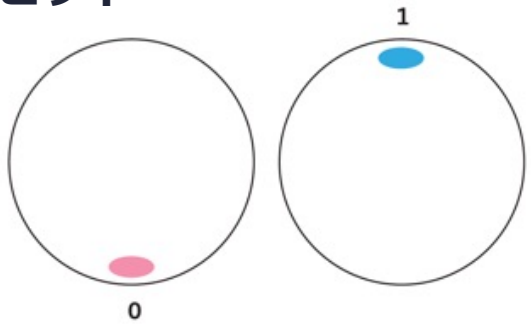
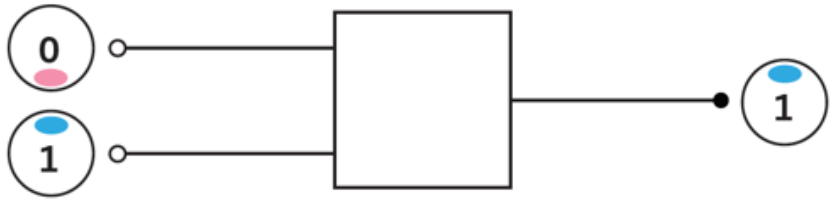
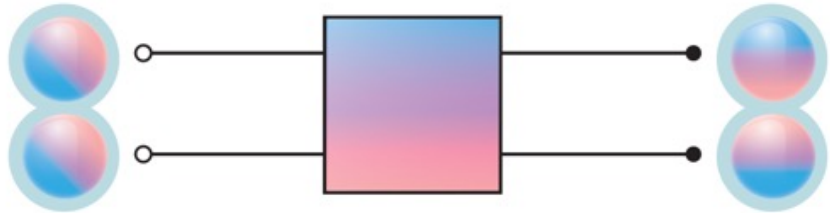
量子未来社会ビジョン

従来ICTとの融合（ハイブリッド）

量子は量子のみで成立するのではない。制御・運用・材料・設計など様々な最先端技術が必須。

内閣府「量子未来社会ビジョン」（2022/4/22）

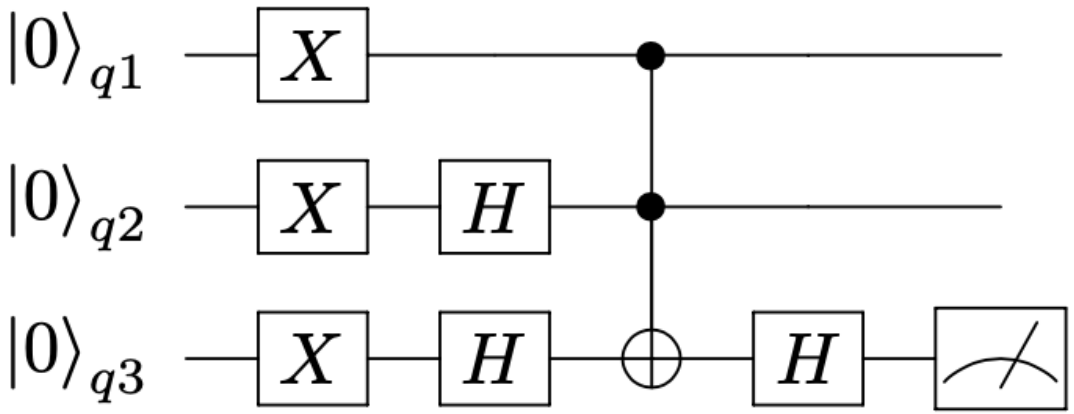
ビットと量子ビット

	コンピュータ	量子コンピュータ
ビット	ビット 	量子ビット 
ゲート	論理ゲート 	量子論理ゲート 
	• 0 または 1 • コピーが可能	• 0 と 1の重ね合わせ状態 • コピーは不可能 • 量子もつれ利用可能
	$x \in \{0,1\}$	$\lvert\psi\rangle = a\lvert 0\rangle + b\lvert 1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \quad \lvert a\rvert^2 + \lvert b\rvert^2 = 1$

A. Trabesinger, *Nature* 543, S2–S3 (2017)

量子計算＝指数関数的に大きな行列の高効率の操作

量子回路 ＝ 量子論理ゲートの列 ＝ 2^N次元の大きな行列



3 量子ビット
＝**2^3** 次元ベクトル

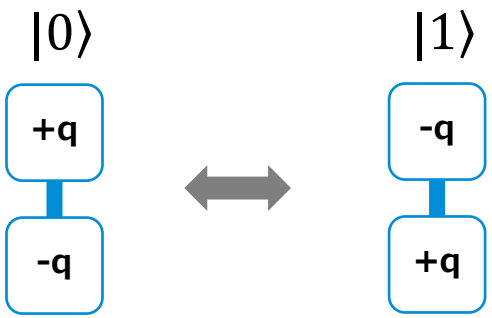
$$\begin{bmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{bmatrix} \xrightarrow{X} \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{bmatrix} \xrightarrow{H} \begin{bmatrix}0\\0\\0\\0\\0.5\\-0.5\\-0.5\\0.5\end{bmatrix} \xrightarrow{\text{Toffoli}} \begin{bmatrix}0\\0\\0\\0\\0.5\\-0.5\\0.5\\-0.5\end{bmatrix} \xrightarrow{H} \begin{bmatrix}0\\0\\0\\0\\0\\\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\end{bmatrix}$$

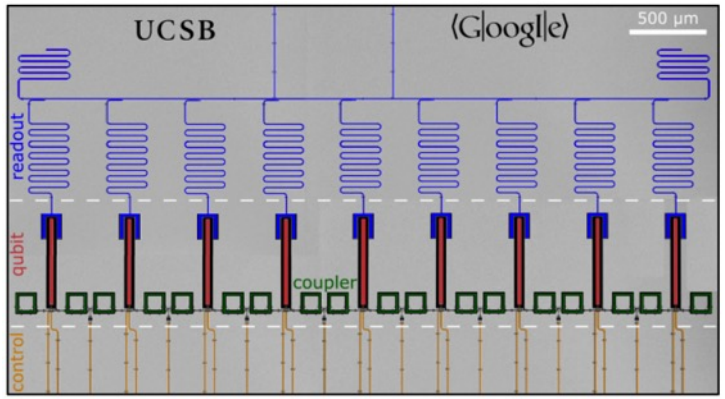
量子ビットの実現系

候補の物理系は多数あるが、いずれも「決め手」に欠く

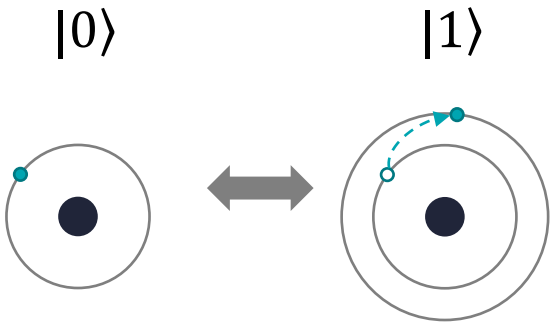
超伝導回路、イオントラップ、シリコン量子ドット、光、冷却原子、ダイヤモンドNVC…

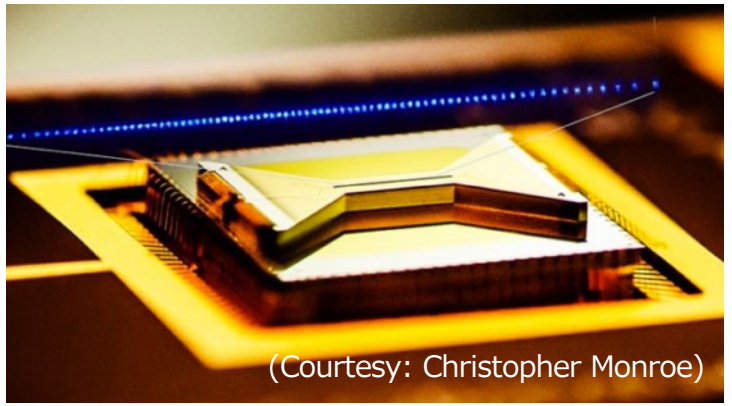
超伝導回路



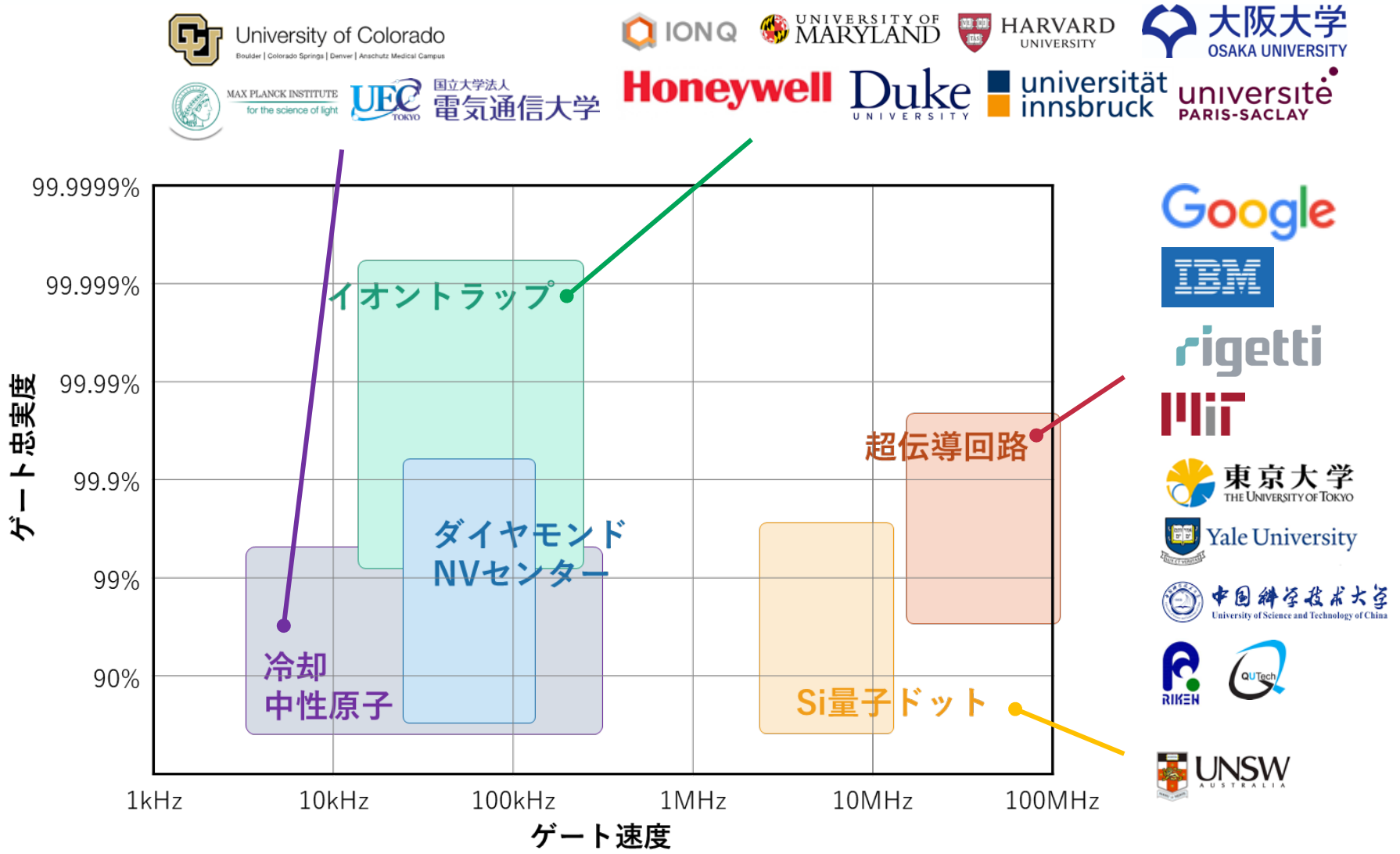


イオントラップ





量子コンピュータの実現系いろいろ

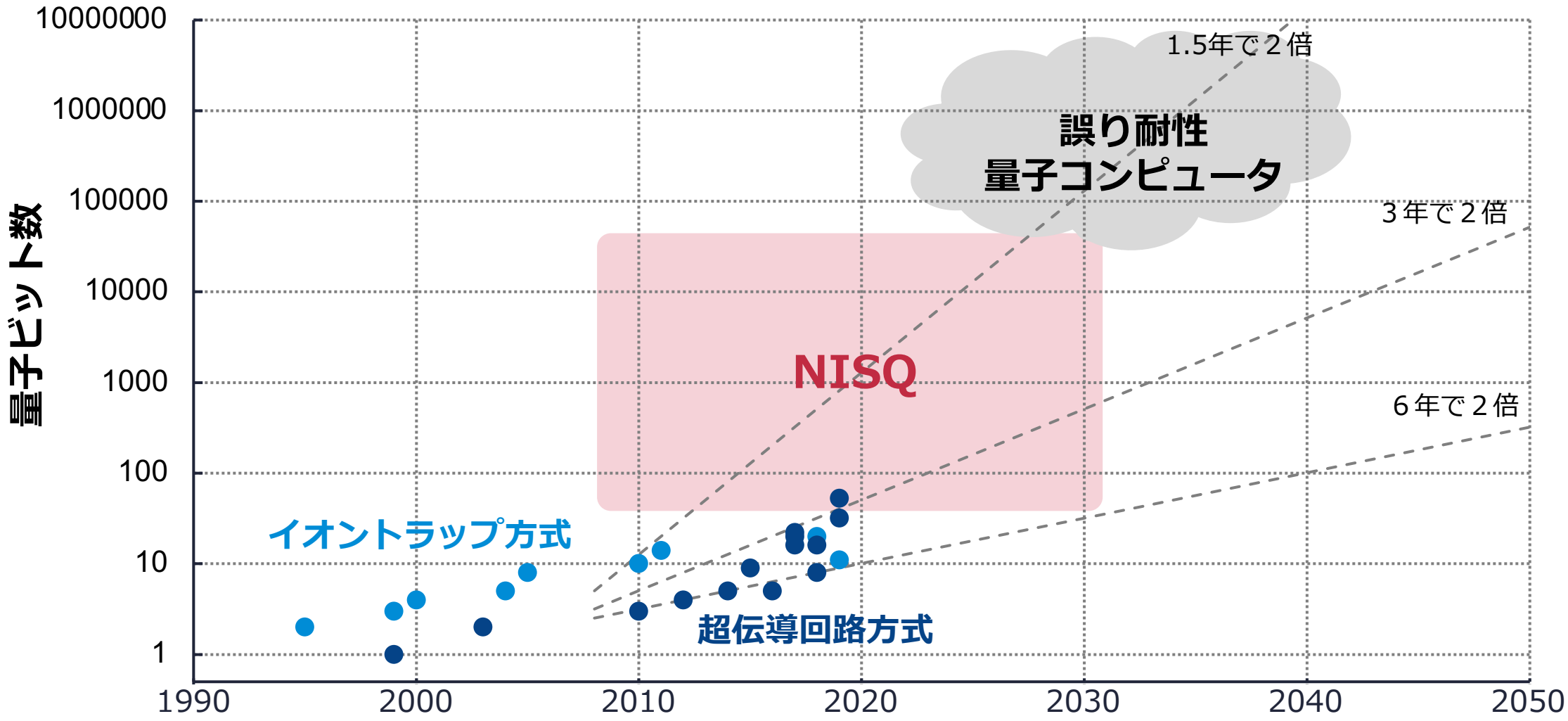


CRDS戦略プロポーザル「みんなの量子コンピューター～情報・数理・電子工学と拓く新しい量子アプリ～」 (2018)

量子コンピュータHWベンダ

方式	北米	欧州	アジア・太平洋
超伝導	IBM🇺🇸, Google🇺🇸, Rigetti Computing🇺🇸, qci🇺🇸, Bleximo🇺🇸, D-wave🇨🇦, Nord Quantique🇨🇦	QuTech🇳🇱, QuantWare🇳🇱	Alibaba🇨🇳, 本源量子（Origin Quantum）🇨🇳, 富士通（w/理研）🇯🇵
イオントラップ	IonQ🇺🇸, Quantinuum（旧Honeywell）🇺🇸	Oxford Ionics🇬🇧, Universal Quantum🇬🇧, AQT🇦🇹	启科量子（Qudoor）🇨🇳
冷却原子	Infeqtion（旧ColdQuanta）🇺🇸, Atom Computing🇺🇸, QuEra Computing🇺🇸	Pasqal🇫🇷, Planqc🇩🇪	
半導体	EeroQ🇺🇸, Photonic Inc🇨🇦	Intel（w/QuTech）🇳🇱, Quantum Motion🇬🇧	Silicon Quantum Computing🇦🇺,日立製作所🇯🇵
光	PsiQuantum🇺🇸, Xanadu🇨🇦,	ORCA🇬🇧, QuiX Quantum🇳🇱	TuringQ🇨🇳
ダイヤモンド			Quantum Brilliance🇦🇺
NMR			量旋科技（SpinQ）🇨🇳
マヨラナ	Microsoft🇺🇸, Nokia/BellLabs🇺🇸		

量子版ムーアの法則



NISQ量子コンピューター

フルの量子コンピュータはまだ手にはらない。しかし…

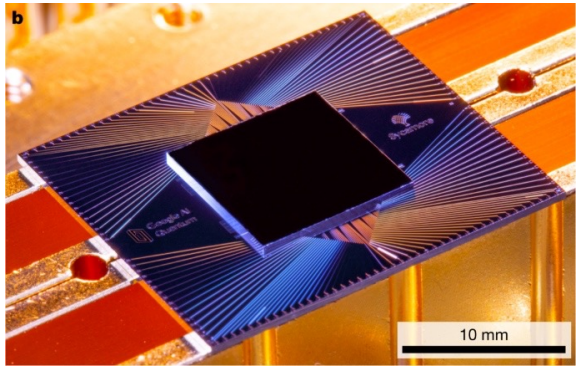
Noisy
ノイズあり
誤り訂正なし。高エラー率。

Intermediate-**S**cale
中規模スケールの
50～100量子ビット程度

Quantum
量子デバイス
量子効果を使うデバイス

シミュレーションが難しい

50量子ビット程度でもスパコン必要

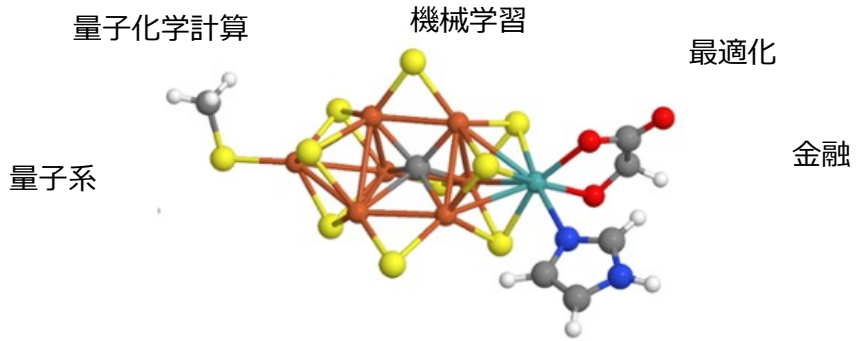


F. Arute *et al.* Quantum supremacy using a programmable superconducting processor, *Nature* 574, 505–510 (2019).

表裏一体

何かには使えそう

限られたHW資源を活かす
知恵・ソフトウェアが重要



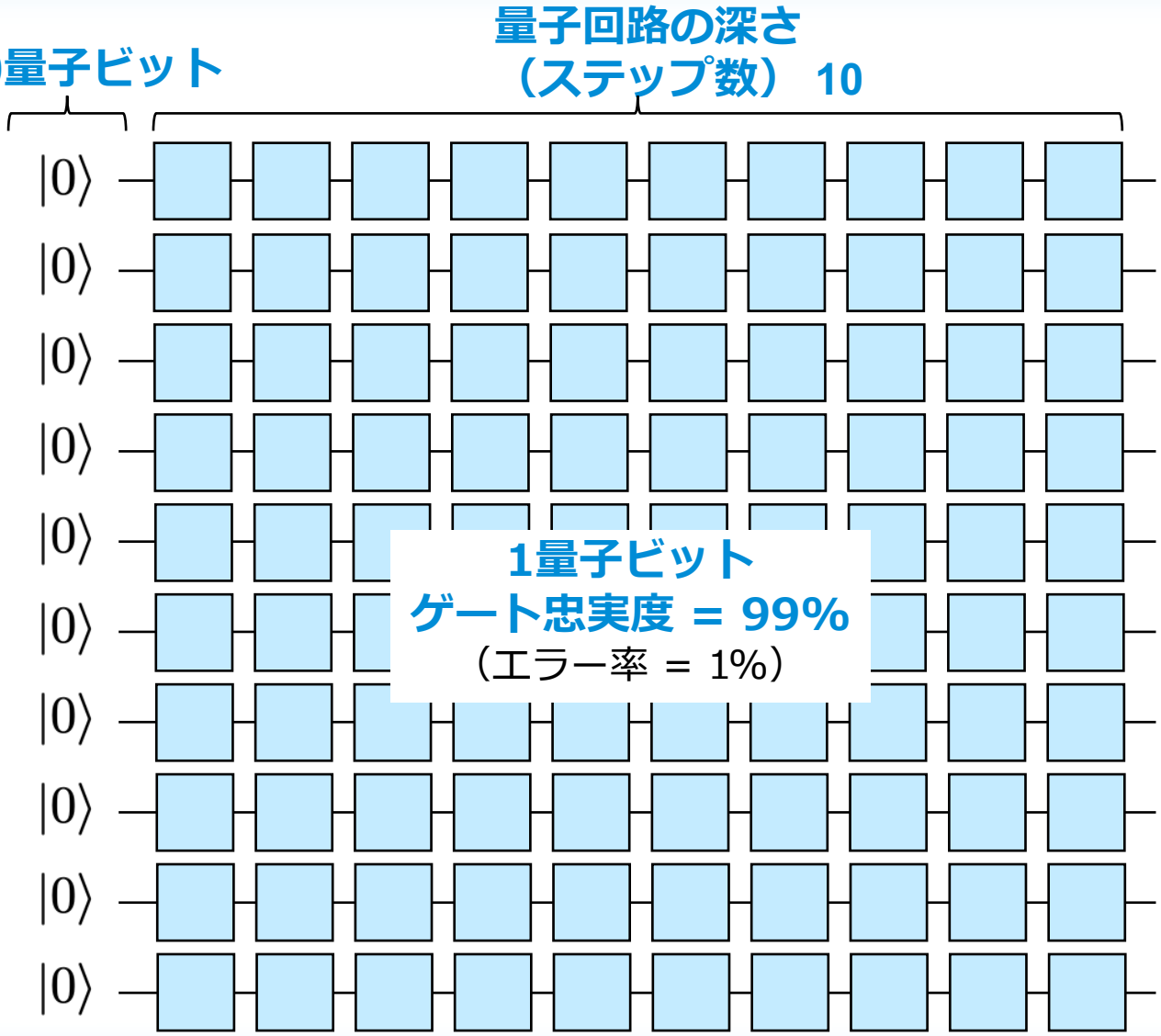
M. Reiher *et al*. Elucidating reaction mechanisms on quantum computers, *PNAS* 114 (29), 7555-7560 (2017).

各社ロードマップ

物理量子ビット
論理量子ビット

企業	方式	‘21	‘22	‘23	‘24	‘25	‘26	‘27	‘28	‘29	‘30	‘31	‘32
IBM	超伝導	127	433	1121	1386	4158							
Google	超伝導	53								1M			
Rigetti	超伝導	80			1K		4K						
本源量子	超伝導	24		144		1024			10K				1M
								100					1K
富士通	超伝導			>100	>100		>1K						
IonQ	イオントラップ	11	32						32K				
				29	35	64	256	384	1024				
ColdQuanta	冷却原子		100		1K								
Pasqal	冷却原子		100										
QuEra	冷却原子		64	64	1024		10K			1M			
Silicon Quantum	Si量子ドット		10							100			

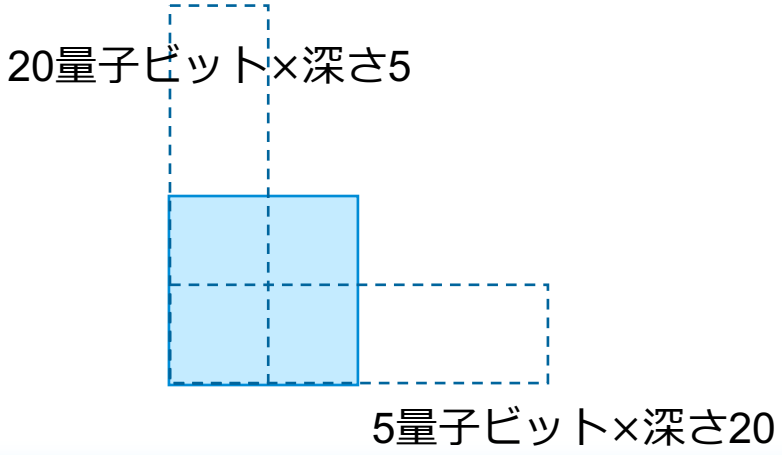
スケーラビリティ問題（NISQをそのまま大きくしてもダメ）



結果の忠実度

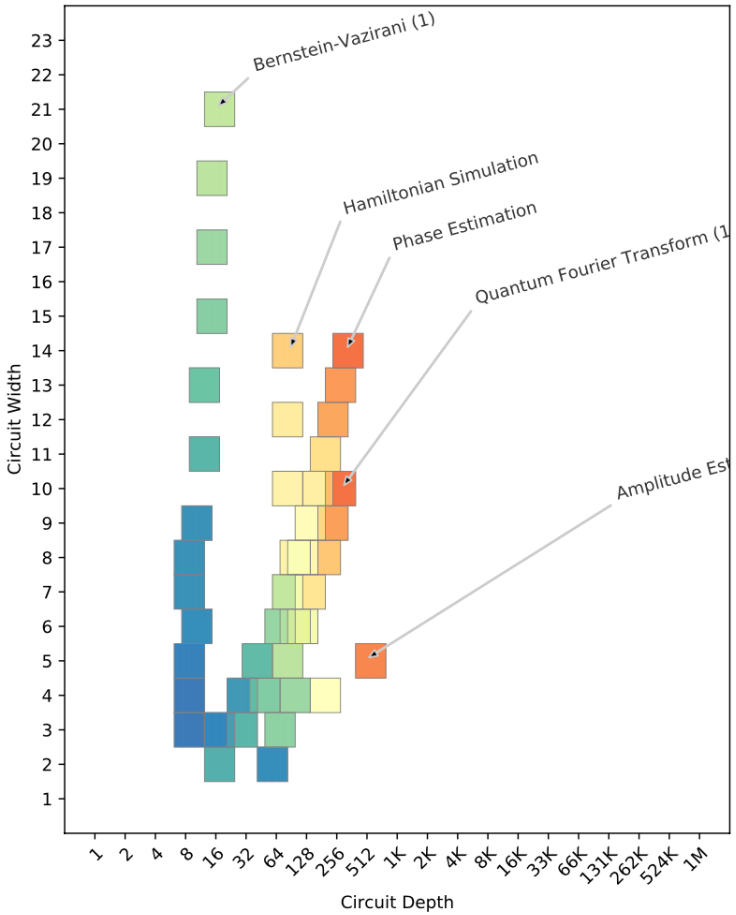
$(0.99)^{100}$ = **36.6%**

結果の忠実度を固定して考えると
量子ビット数と回路深さはトレードオフ

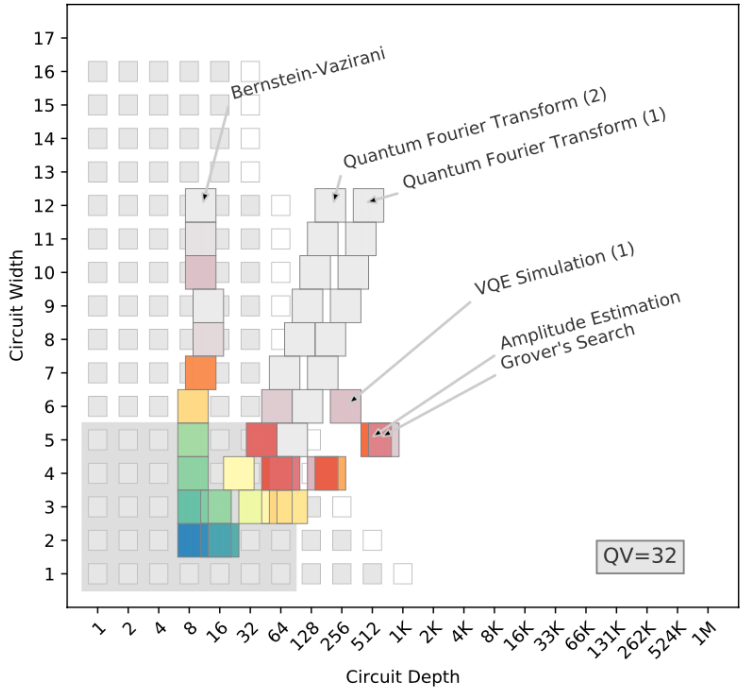


NISQマシンのベンチマーク

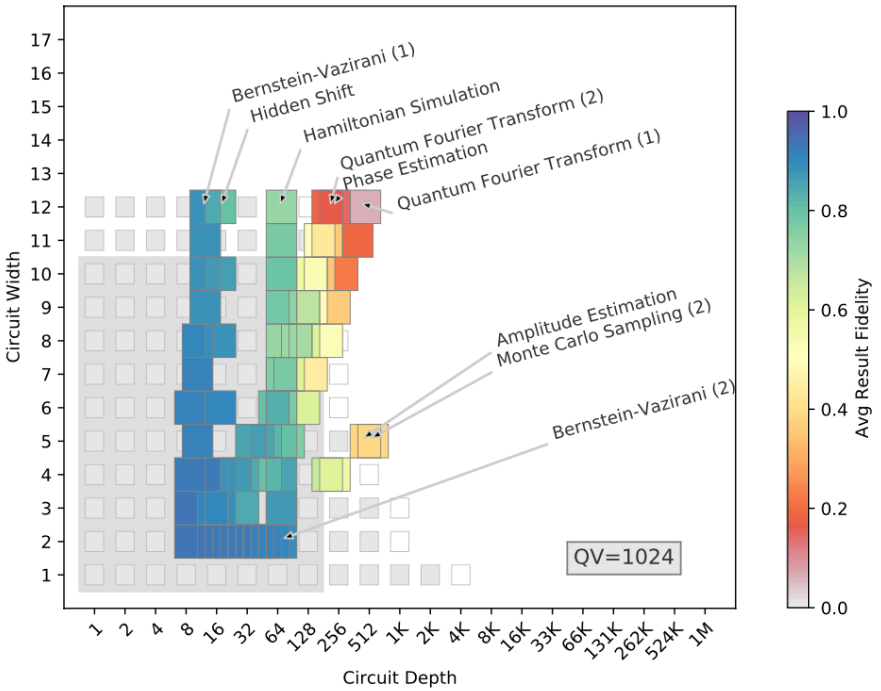
IonQ Aria



IBM Guadalupe

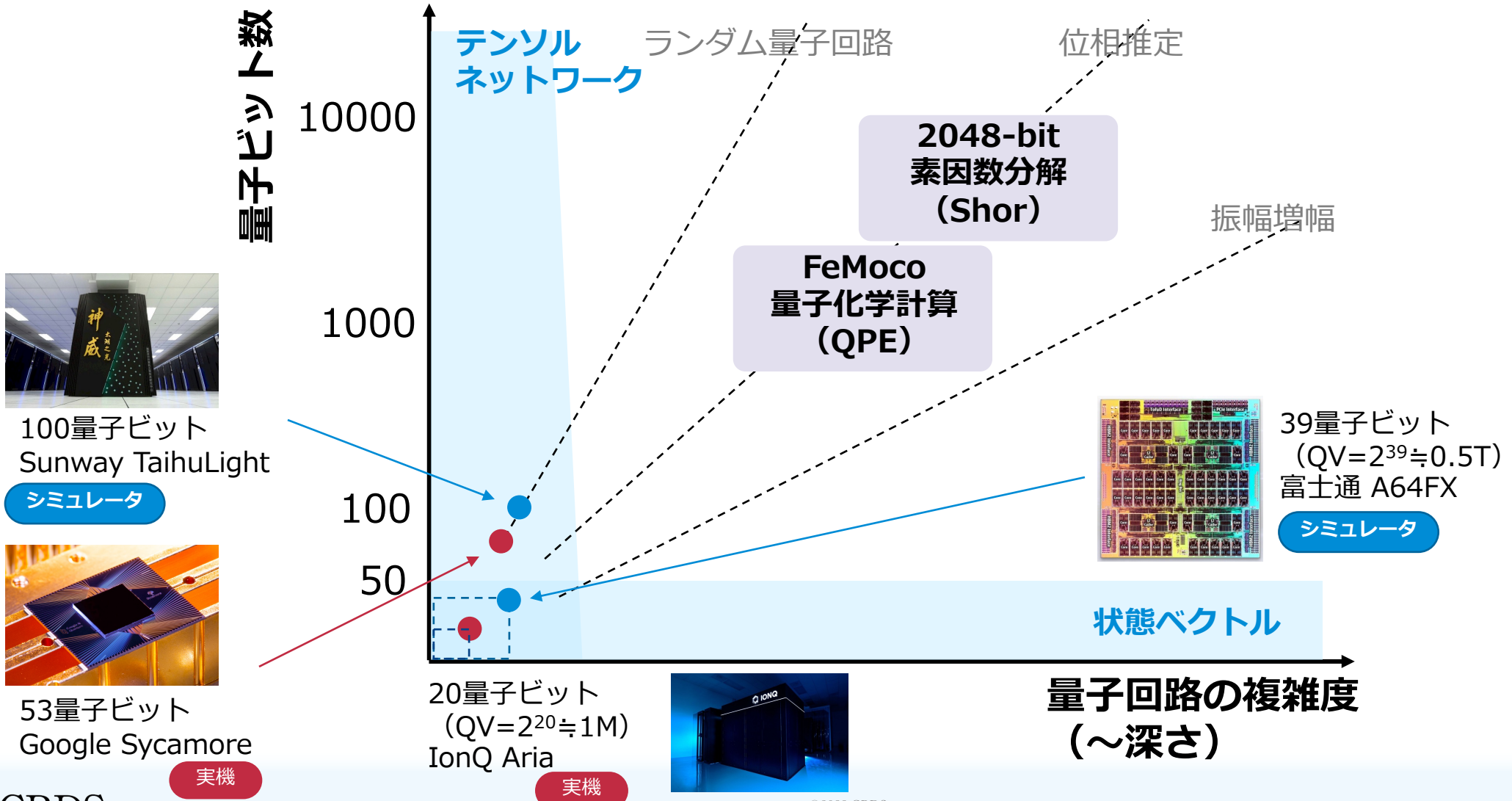


Quantinuum H1



T. Lubinski et. al., Application-Oriented Performance Benchmarks for Quantum Computing, arXiv:2110.03137

量子コンピュータの性能とシミュレーション技術の向上



量子誤り訂正符号

量子ビットに冗長性をもたせ、エラーを検出・訂正する

古典のハミング符号と同じような考え方だが、量子コンピュータ特有の事情の考慮が必要

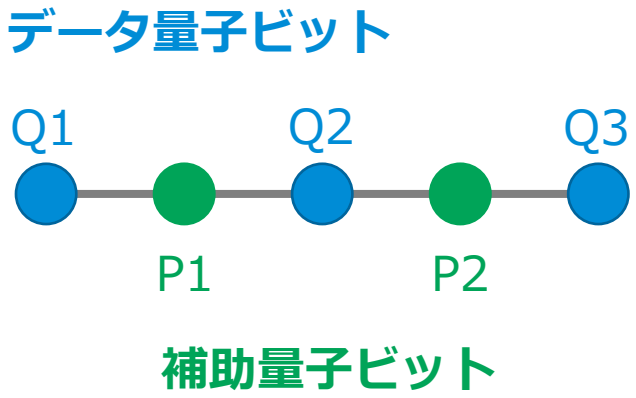
特有の事情

1. ビット反転エラーに加えて位相反転エラーが存在
2. 任意の量子状態のコピペは不可（No-Cloning定理）
3. 計算実行中のレジスタを護る必要がある（符号化されたまま演算）
4. **エラーの有無を確認する測定操作により量子ビットの重ね合わせ状態が壊れる**
5. エラー検出・訂正に必要なゲート操作も高い確率で誤る

パリティチェック

エラーそのものを測定せず、パリティ測定結果からエラー位置を推定

補助ビットP1, P2にQ1-Q2, Q2-Q3の
パリティ値をCNOTゲートで書き込む



Q1～3の状態が|0⟩か|1⟩かの情報を**使わずに**
P1, P2の測定結果からエラーの位置が推定できる

Q1	Q2	Q3	P1	P2	
|0⟩	|0⟩	|0⟩	|0⟩	|0⟩	→ エラーなし
|1⟩	|1⟩	|1⟩	|0⟩	|0⟩	
|1⟩	|0⟩	|0⟩	|1⟩	|0⟩	→ Q1にエラー
|0⟩	|1⟩	|1⟩	|1⟩	|0⟩	
|0⟩	|1⟩	|0⟩	|1⟩	|1⟩	→ Q2にエラー
|1⟩	|0⟩	|1⟩	|1⟩	|1⟩	
|0⟩	|0⟩	|1⟩	|0⟩	|1⟩	→ Q3にエラー
|1⟩	|1⟩	|0⟩	|0⟩	|1⟩	

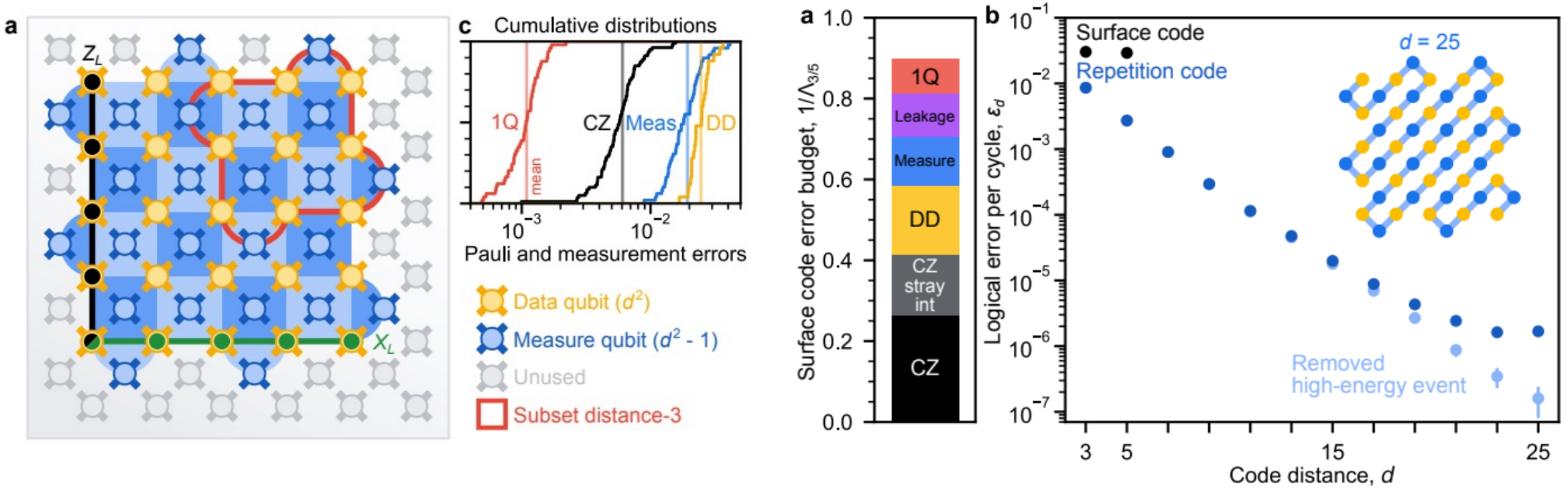
エラー位置の推定問題＝最小重み完全マッチング問題（MWPM）
（古典多項式アルゴリズムが存在）

量子誤り訂正の実験検証

[[n, k, d]]
n:物理ビット数、k:論理ビット数、d:符号長
（(d - 1) / 2の誤りを訂正できる）

表面符号

[[9, 1, 3]]-[[25, 1, 5]] @17～49量子ビット （反復符号 [3, 1, 3]-[25, 1, 25]）



Google Quantum AI. Suppressing quantum errors by scaling a surface code logical qubit, arXiv:2207.06431

量子誤り訂正符号によるオーバーヘッド

2048bitの数の素因数分解

12000

論理量子ビット
実行効率を鑑みてやや冗長

x10000

誤り訂正（表面符号、d＝56）
量子ビットのエラー率0.2%

x8

魔法状態蒸留
（非クリフォード群ゲートのため）

x1.25

量子ビットの配線

x5

デバイスの歩留まり

6,000,000,000

物理量子ビット

R. Van Meter, C. Horsman, “A blueprint for building a quantum computer”, Comm. of the ACM 56, 84 (2013).

（最新の結果）

14000

誤り訂正（表面符号、d＝27）
量子ビットのエラー率0.1%

魔法状態蒸留（3500量子ビット）
（上記量子ビット数に含まれている）

回路レベル～アルゴリズムレベルの工夫
- Approximate encoded permutations → 和の改善
- Windowed arithmetic → 積、指数化の改善
- AutoCCZ magic state → 時空間レイアウト改善
- Short discrete logarithm → 量子ビット数削減

20,000,000

C. Gidney, M. Ekerå, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”, Quantum 5, 433 (2021).

量子コンピュータの優位性

素因数分解や量子化学計算は量子コンピュータにとっても難しい問題

物理量子ビット数

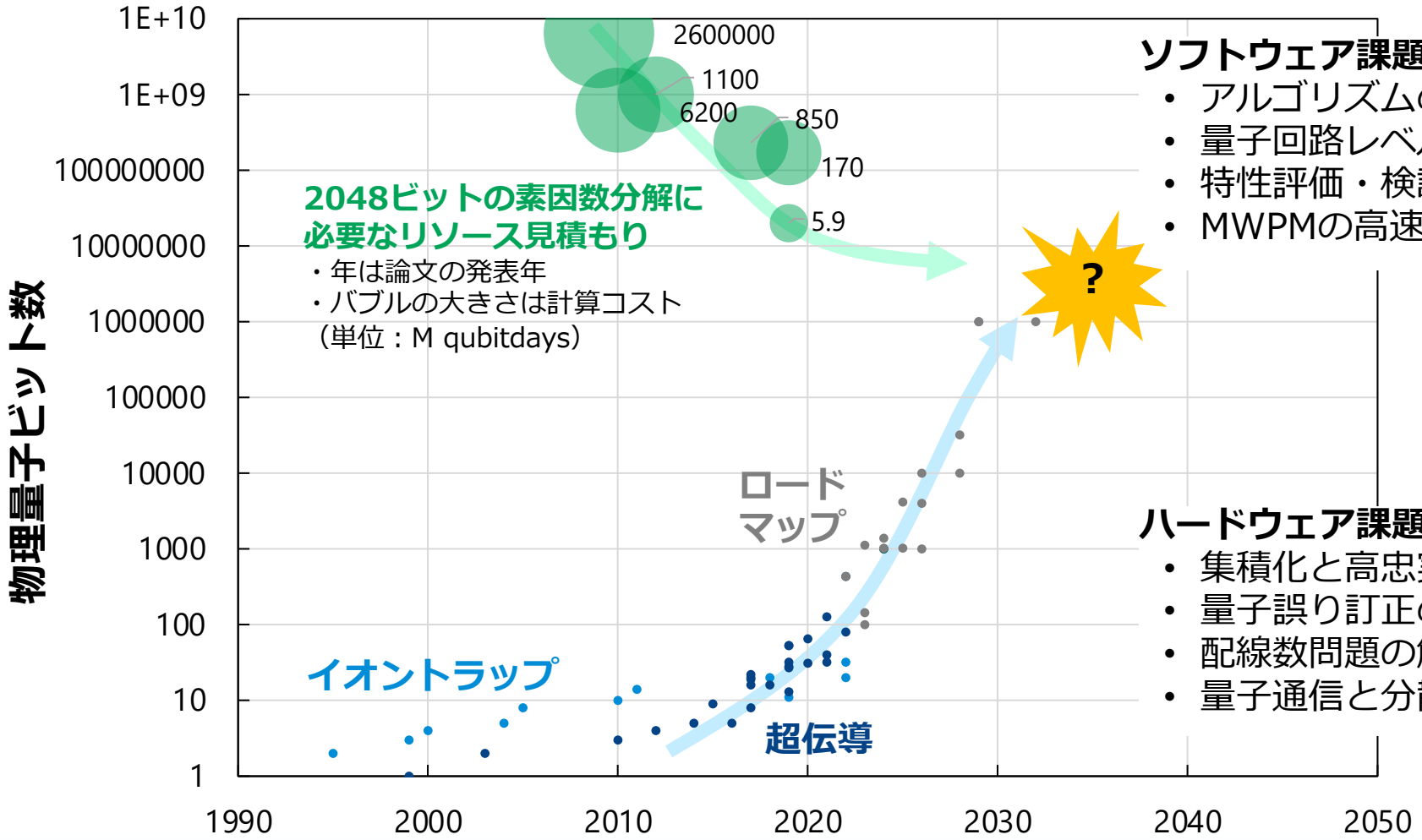
10^2 10^3 10^4 10^5 10^6 10^7 10^8

	サンプリング [1]	物性物理 [2]	量子化学 [3]	素因数分解 [4]
具体的タスク	60ビット ランダム量子回路 (忠実度10%)	2次元J_1-J_2 Hハイゼン ベルグモデル (10x10格子)	FeMoco の基底状態 (精度1kcal/mol)	2048ビット整数の 素因数分解 (忠実度27%)
量子ビット数	2.5 x 10^4	5 x 10^5	4 x 10^6	2 x 10^7
実行時間	0.25 sec	14 Hours	4days	8 hours

[1] C. Gidney, Estimating the Fault Tolerant Cost of Classically Intractable Quantum Computations, Talks at Simon Institute (Feb. 27, 2020)
[2] N. Yoshioka et. al., Hunting for quantum-classical crossover in condensed matter problems, arXiv:2210.14109 (2022).
[3] M. Reiher et al., Elucidating reaction mechanisms on quantum computers, PNAS 114 (29), 7555-7560 (2017).
[4] C. Gidney and M. Ekera, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, Quantum 5, 433 (2021).

まとめ・今後の展望

量子コンピュータ実現／開発競争は工学（エンジニアリング）フェーズに突入



ソフトウェア課題

- アルゴリズムの改善
- 量子回路レベルの改善（誤り訂正含む）
- 特性評価・検証・シミュレーション（QCVV）
- MWPMの高速解法（サイクル1μsの達成）

ハードウェア課題

- 集積化と高忠実度の同時達成
- 量子誤り訂正の実装
- 配線数問題の解決（量子版レント則？）
- 量子通信と分散処理（量子版アムダール則？）