目　次

サマリー　1

1　コンピューティングの進歩　15

1.1　現代のコンピューティングの起源　16
1.2　量子コンピューティング　17
1.3　コンピューティングにおける進歩の歴史：ムーアの法則　19
1.4　トランジスタを安価なコンピュータに変える　23
1.5　スケーリングの減速　24
1.6　コンピューティングへの新しいアプローチとしての量子　26
1.7　参考文献　27

2　新たなパラダイムとしての量子コンピューティング　28

2.1　直観に反する量子の世界　29
2.2　量子技術の現状　31
2.3　ビットと量子ビット　35
2.3.1　古典コンピューティングの基礎：アナログ信号から
ビットおよびデジタルゲートへ　35
2.3.2　量子ビット　39

2.3.3　多量子ビット系　41
2.4　量子ビットを使った計算　43
2.4.1　量子シミュレーション，量子アニーリング，断熱量子計算　46
2.4.2　ゲートベースの量子コンピューティング　47
2.5　量子コンピュータの設計についての制約　51
2.6　実用的な量子コンピュータの可能性　57
2.7　参考文献　61

3　量子アルゴリズムとアプリケーション　64

3.1　理想的なゲートベース量子コンピュータ用の量子アルゴリズム　67
3.1.1　量子フーリエ変換と量子フーリエサンプリング　68
3.1.2　量子素因数分解と隠れた構造の探索　71
3.1.3　Grover のアルゴリズムと量子ランダムウォーク　72
3.1.4　ハミルトニアンのシミュレーション　74
3.1.5　線形代数の量子アルゴリズム　77
3.1.6　マシンの性能についての要求水準　79
3.2　量子誤り訂正と誤り低減　79
3.2.1　誤り低減の方策　80
3.2.2　量子誤り訂正符号　81
3.2.3　量子誤り訂正のオーバーヘッド　84
3.3　近似的な量子アルゴリズム　89
3.3.1　変分量子アルゴリズム　89
3.3.2　アナログ量子アルゴリズム　91
3.4　量子コンピュータの応用　92
3.4.1　量子コンピュータの近未来のアプリケーション　93
3.4.2　量子超越性　94
3.4.3　理想的な量子コンピュータのアプリケーション　97
3.5　コンピューティングのエコシステムにおける量子コンピュータの位置づけ　98

3.6 参考文献 99

4 暗号に対する量子コンピュータの影響 108

4.1 現行の暗号化アルゴリズム 109
4.1.1 鍵交換と公開鍵暗号 110
4.1.2 共通鍵暗号 112
4.1.3 証明書とデジタル署名 114
4.1.4 暗号学的ハッシュ関数とパスワードハッシュ 115
4.2 サイズの見積もり 117
4.3 耐量子計算機暗号 118
4.3.1 共通鍵暗号とハッシュ関数 119
4.3.2 鍵交換と署名 119
4.4 実際の展開における難しさ 122
4.5 参考文献 126

5 量子コンピュータの基本的なハードウェア要素 129

5.1 量子コンピュータのハードウェアの構造 130
5.1.1 量子データ層 131
5.1.2 制御・測定層 132
5.1.3 制御プロセッサ層とホストプロセッサ 133
5.1.4 量子ビット技術 135
5.2 捕捉イオン量子ビット 135
5.2.1 捕捉イオン量子コンピュータの現状 136
5.2.2 スケーラブルな捕捉イオン量子コンピュータを作る難しさと可能性 137
5.3 超伝導量子ビット 140
5.3.1 超伝導量子コンピュータの現状 140
5.3.2 スケーラブルな量子コンピュータを作るための課題と可能性 141

5.4　その他の技術　145
5.5　将来の見通し　147
5.6　参考文献　149

6　スケーラブルな量子コンピュータの基本ソフトウェア要素　154

6.1　問題点と解決の方向性　155
6.2　量子プログラミング言語　157
6.2.1　プログラマが直接扱う（高水準）プログラミング言語　158
6.2.2　制御プロセッサ（低水準）言語　161
6.2.3　ソフトウェアライブラリのサポート　163
6.2.4　アルゴリズムのリソース解析　164
6.3　シミュレーション　166
6.4　仕様，検証，デバッグ　167
6.5　高水準のプログラムからハードウェアへのコンパイル　170
6.5.1　ゲート合成　173
6.5.2　量子誤り訂正　173
6.6　まとめ　174
6.7　参考文献　175

7　量子コンピューティングの実現可能性と時間スケール　179

7.1　進歩の現状　179
7.1.1　好循環を作る　181
7.1.2　近未来の量子コンピュータ用のアプリケーションの重要さ　183
7.2　量子コンピューティングの進歩を評価する枠組み　184
7.2.1　物理量子ビットと論理量子ビットのスケーリングを追跡する方法　185
7.2.2　量子ビット技術の現状　189
7.3　マイルストーンと時間評価　192
7.3.1　小規模な（数十ビットの）コンピュータ（マイルストーンG1）　194

7.3.2　ゲートベースの量子超越性（マイルストーン G2a）　194
7.3.3　アニーラベースの量子超越性（マイルストーン A2）　196
7.3.4　量子誤り訂正の大規模な実行（マイルストーン G2b）　197
7.3.5　商業的価値のある量子コンピュータ（マイルストーン A3 および G3）　198
7.3.6　モジュラー構造の大規模量子コンピュータ（マイルストーン G4）　199
7.3.7　マイルストーンの要約　201
7.4　量子コンピューティングの研究開発　203
7.4.1　世界的な研究動向　203
7.4.2　量子コンピューティング研究開発の重要性　205
7.4.3　開かれたエコシステム　211
7.5　成功に向けて　212
7.5.1　量子コンピュータのサイバーセキュリティ上の意義　213
7.5.2　量子コンピューティングの将来性　213
7.6　参考文献　215

付録

A　本委員会の任務　221
B　捕捉イオン量子コンピュータ　222
C　超伝導量子コンピュータ　232
D　その他の技術　241
E　研究開発投資の世界的動向　257
F　委員とスタッフおよび各機関の紹介　262
G　委員会で意見を聞いた方々　272
H　用語解説　273

索　引　279