# 量子コンピュータ時代の新暗号

初版投稿：2016/09/02 ， 最新版投稿：2018/06/20
執筆者：小柴 等（研究員）

## 量子コンピュータの出現：そのインパクト

### ノイマン型コンピュータから量子コンピュータへ

1940 年代後半から 50 年代前半にコンピュータが発明されて半世紀以上，コンピュータの高速化・小型化が進展し，今日では様々なモノにセンサやコンピュータが埋め込まれ，IoT（Internet of Things：もののインターネット）といった言葉も流行っています．

しかしながら，コンピュータの基本的な原理・性質そのものは発明当初から大きく変わるものではなく，どれも「ノイマン型コンピュータ」と呼ばれるような種類のモノでした．

この「コンピュータの基本的な原理・性質そのもの」が大きく異なる新種のコンピュータが「量子コンピュータ」です．

### 量子コンピュータの実現可能性

量子コンピュータは「量子力学」の知見を用い，これまでのコンピュータとは違った発想で非常に高速な計算を可能にします．

これにより，現在のコンピュータでは計算しきれない膨大な量のデータを処理できるようになることが期待されており，日本でも早くから NEC など複数のメーカーで研究が行われてきていました．

これまで量子コンピュータは理論や基本原理の実証が主でしたが，2010 年代に入って D-wave 社が，能力的には限定的ながら量子コンピュータの開発に成功したと主張し，実際に市販を始めて Google 社が購入したことなどから，実用化への期待・可能性が高まっています．

### 量子コンピュータのインパクト

このように量子コンピュータは大きな可能性をもつ夢の技術なのですが，その性能の高さ故に問題点も懸念されています．

その一つが「暗号」に関する問題です．特定の種類の量子コンピュータに限定されるものの，あまりに高速な計算ができるため，これまでインターネット上の通信などデジタルデータの保護に使われてきた多くのデジタル暗号を力任せに解析できてしまうのです．

量子コンピュータの取得は，オンライン決済，国家や企業の機密情報のやりとりなど，様々な情報のマスターキーを手に入れるのと同じ，と言えるかもしれません．

## 量子コンピュータ時代に対応した新暗号

そこで現在，量子コンピュータ時代に対応した暗号の開発が進んでいます．

暗号化の方式にも幾つかの種類があり，「格子暗号」もそのひとつです．

最近では KDD 研究所と九州大学が 60 次元の格子暗号をノイマン型のコンピュータで解析することに成功するなど，新たな暗号方式の安全性や基準の確立・標準化に向けた競争が激化していると同時に，我が国の存在感を示しています．

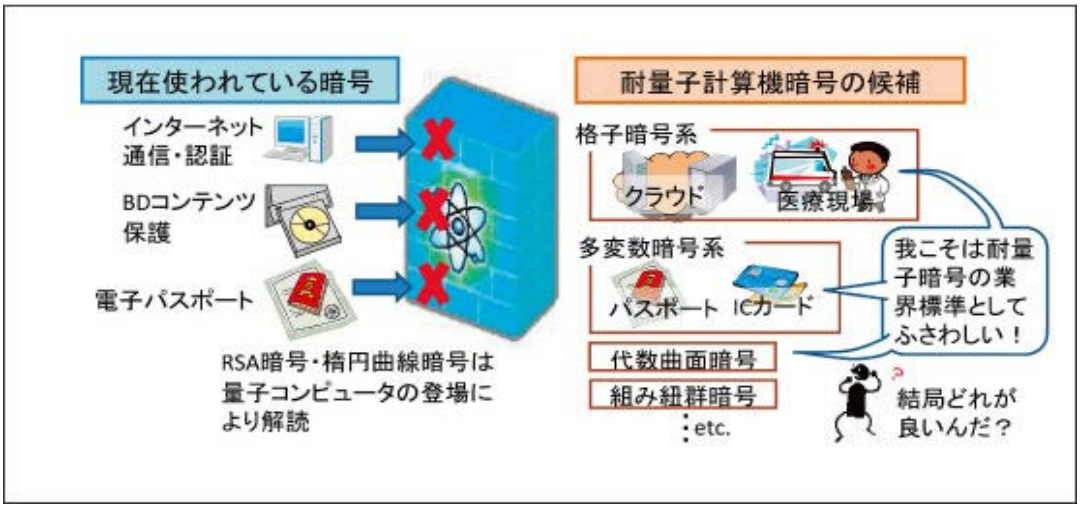


図 1　耐量子計算機暗号の業界標準に向けて（ NICT NEWS より転載）

## 今後に向けて

量子コンピュータがもたらす膨大な計算能力は社会の有り様を大きく変える可能性を有しています．

そのような時代に対応した新たなセキュリティのあり方や，過渡期（新暗号技術の確立，普及より先に暗号解読可能な量子コンピュータが完成した場合など）における情報保護制度のあり方などについての検討が必要な時期に来ていると言えるかもしれません．

### 出典

格子暗号の実用化に向けて 青野 良範 - NICT NEWS http://www.nict.go.jp/publication/NICT-News/1303/0...
世界で誰にも解読されていない暗号問題を初めて解読！
http://www.kddilabs.jp/newsrelease/2016/071901.htm...

## 参考

「格子暗号」の最新動向 - 日本銀行金融研究所
http://www.imes.boj.or.jp/research/papers/japanese...

## 関連するデルファイ課題

*様々なアルゴリズムに適用可能な汎用性のある量子コンピューティング（2010 年：第 9 回）*
*10k 量子ビット間でコヒーレンスが実現され従来解決困難だった問題を高速に処理できるゲートモデル型量子コンピュータ（2015 年：第 10 回）*
*世界的規模でセキュアな情報化社会を実現する実用的な量子暗号（2010 年：第 9 回）*
*100km を超える都市間における特定用途向け量子暗号通信技術（2015 年：第 10 回）*
*量子暗号通信のためにオンデマンドで単一光子を発生できる新デバイス（2015 年：第 10 回）*