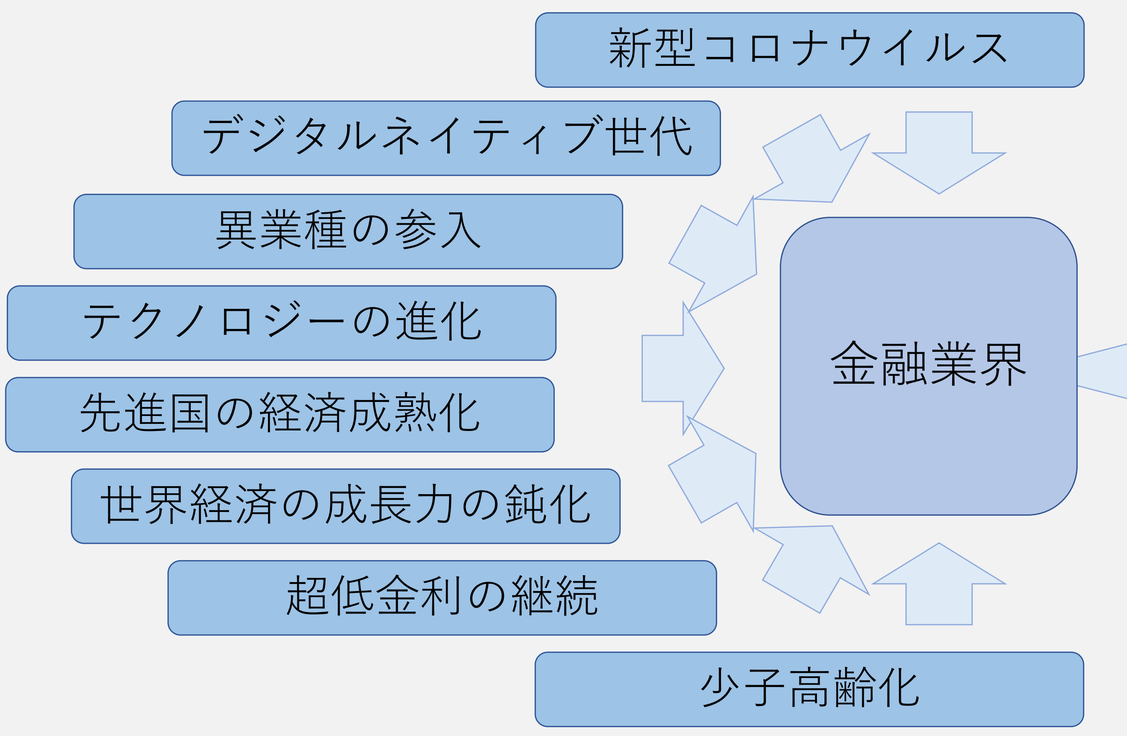
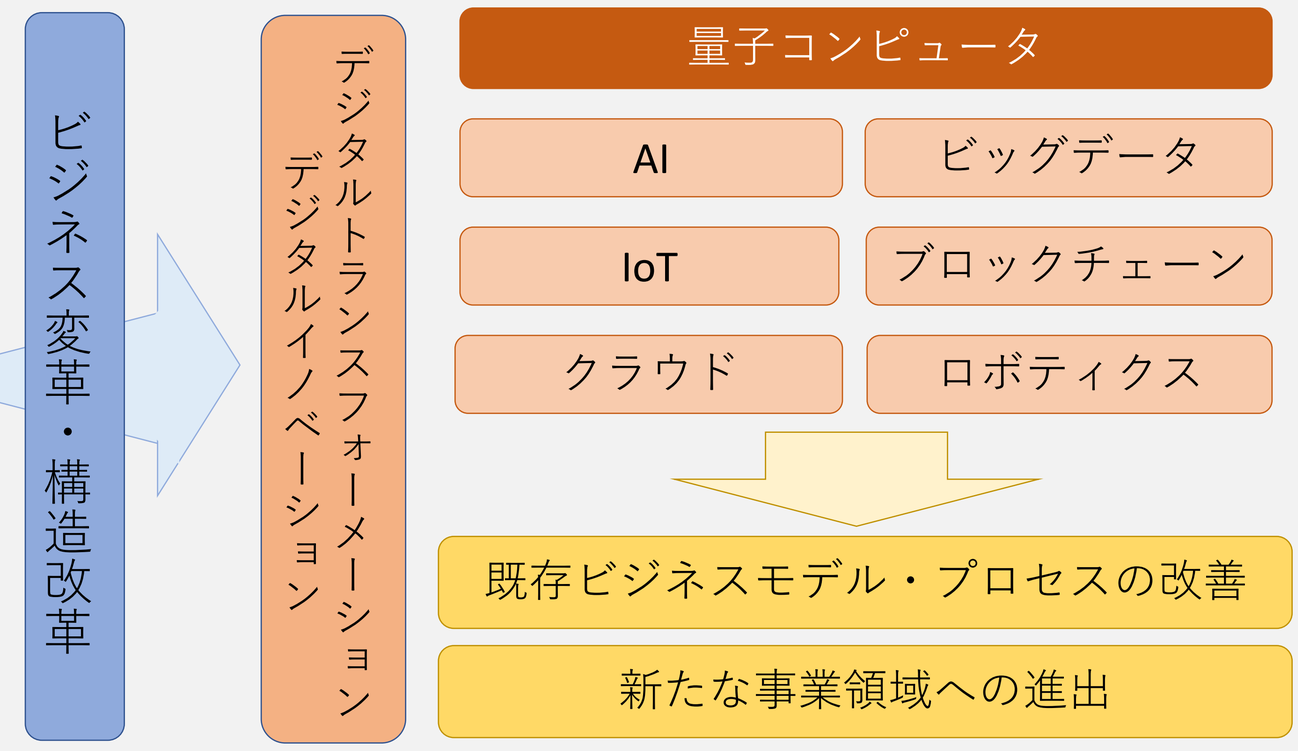
IBM Q Hub 金融チームの活動紹介

背景

- **金融業界の現状**
  - 現在の環境変化を踏まえ、テクノロジー・デジタルを起点とした改革を推進

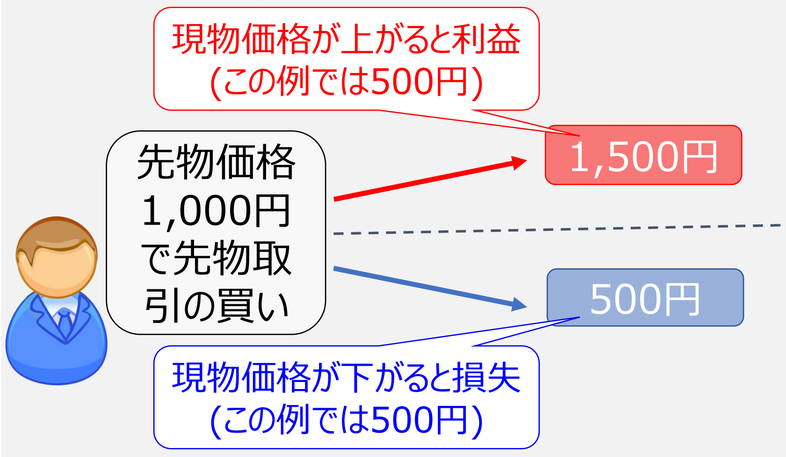


- **デジタル化への対応**
  - その一つとして、量子コンピュータの活用を目指す



活用事例1：金融派生商品(デリバティブ)の価格決定の高速化

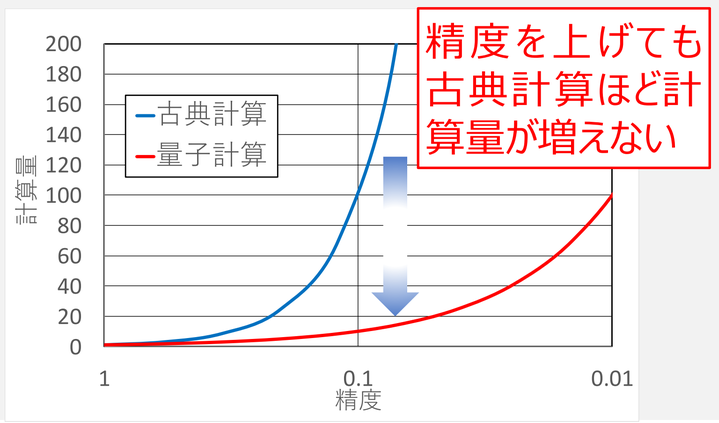
- 金融派生商品（デリバティブ）
  - 金融派生商品とは、株式、債券、金利、通貨、金、原油等の原資産の価格を基準に、価格が決まる金融商品の総称。
  - 価格変動等のリスクを回避・低減する、あるいは、リスクを取り高い収益を追求する為に、利用する。



<金融派生商品の例(先物取引)>

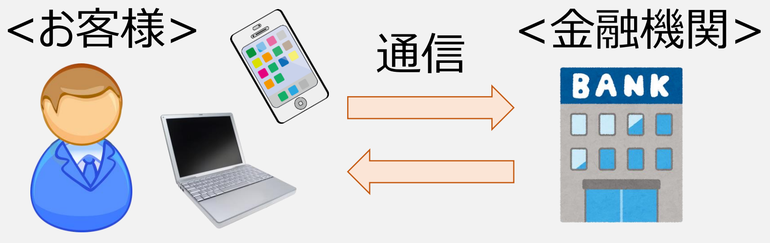
- モンテカルロシミュレーション
  - デリバティブの計算には、日々の資産の価格変動等、確率的な要素が含まれるため、乱数を用いたシミュレーション（モンテカルロシミュレーション）が用いられる。
  - 現在の高性能コンピュータを使っても、この計算に毎日数時間以上を費やすなど、金融機関で長時間コンピュータを使う計算の一つ。

- 量子コンピュータでの検証
  - 量子コンピュータでは、モンテカルロシミュレーションを高速化することが出来る。
  - 精度を100倍にしたければ…
    従来の場合：10,000倍の計算量
    量子の場合：100倍の計算量
  - Q Hubでは、既存の方法に比べてゲート数やビット数が少ない方法の開発を行っている
    [Quantum Information Processing, 19, 75, 2020]



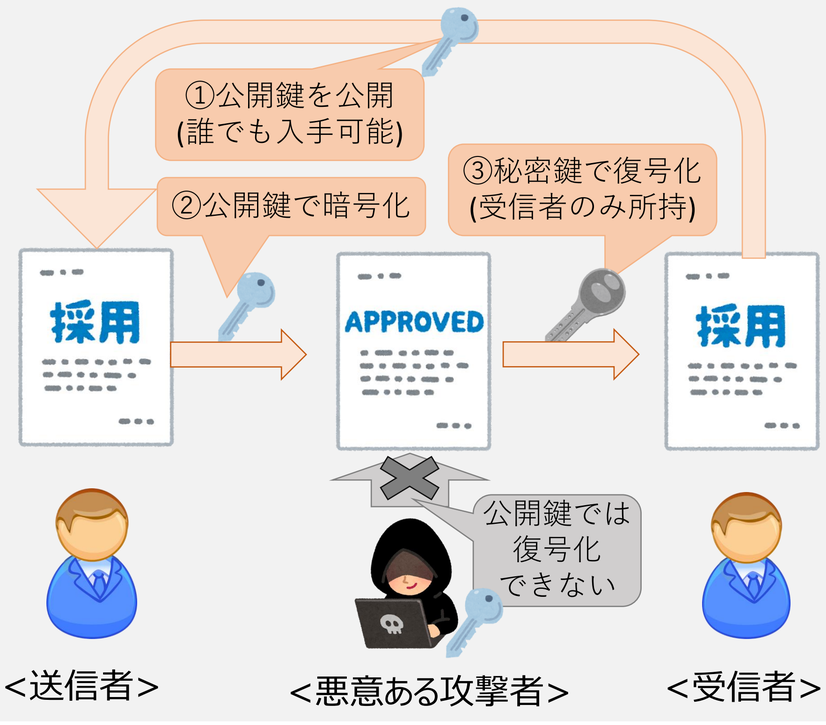
活用事例2：暗号解読によるセキュリティリスクへの対応

- **現状の金融機関**
  - 現在、金融機関では、パソコンやモバイル端末等を介して日々数十億件、数千兆円の取引が行われている。



  - 取引の根幹を担う通信は、暗号化によって守られており、暗号の安全性の維持が必須。
  - 金融機関では、インターネットバンキングを始めとし、一金融機関あたり、数百～数千のシステムがあり、システムの改修・更改には、数年の時間がかかるため(長い場合は10年超)、予め計画的な準備が必要。

- **公開鍵暗号方式**
  - 現在の一般的な通信方法の一つに、公開鍵暗号方式というものがある。



- **量子コンピュータでの検証**
  - 暗号には、大きな合成数の素因数分解が困難という数学的な特徴を用いている。
  - 量子コンピュータでは、従来のコンピュータより、素因数分解が高速に解ける可能性があると言われている。(Shorのアルゴリズム)
  - Q Hubでは、量子コンピュータの実機（65量子ビット）等を用いて、現在の暗号の安全性と、将来的な見通しを検証している。