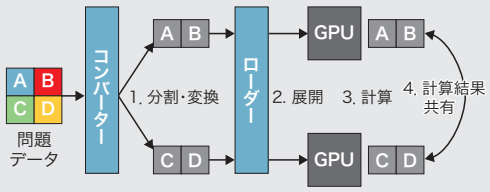
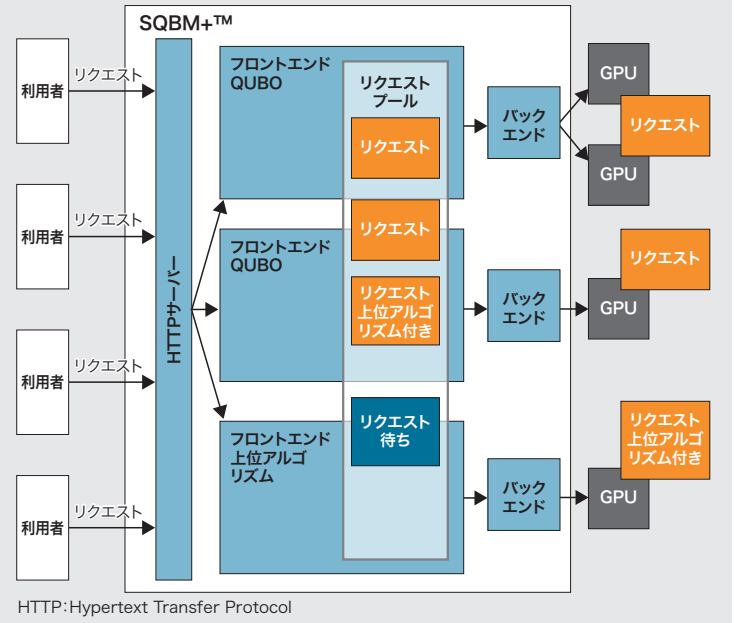
10億変数の大規模最適化問題の求解を可能にした量子インスパイアード最適化ソリューションSQBM+™



1. 問題データをコンバーターで分割し，GPU上に展開できる形式に変換する。その際，4.の計算結果共有のためのデータ転送が少なくなるように分割する。
2. 分割した問題データをローダーでGPU上に展開する。
3. GPUで問題データを用いて計算処理を行う。
4. GPUは互いの計算結果を共有して残りの計算処理を行う。3.と4.を繰り返す。

問題分割による大規模問題処理手法
Decomposition approach to large-scale optimization problems



フロントエンドとバックエンドの分離によるGPUリソースの柔軟な割り当て
Frontend–backend decoupling for flexible graphics processing unit (GPU) resource allocation

社会や産業の現場には組み合わせが膨大な最適化問題があり，効率化や価値創造に直結する。量子インスパイアード最適化ソリューションSQBM+™は，東芝の量子技術研究を基に実用的な解を高速に導くソフトウェアである。よりスケーラブルで実用的なものを目指すために，次の三つの課題があった。

⑴ 10億変数規模の大規模化　例えば，小口債権をリスク回避目的で組み分けするとき，債券と組の組み合わせごとに変数が必要になり，100万債権×1,000組では10億変数となる。この規模は現実的な処理が困難で，量子インスパイアード技術の価値が問われる領域である。

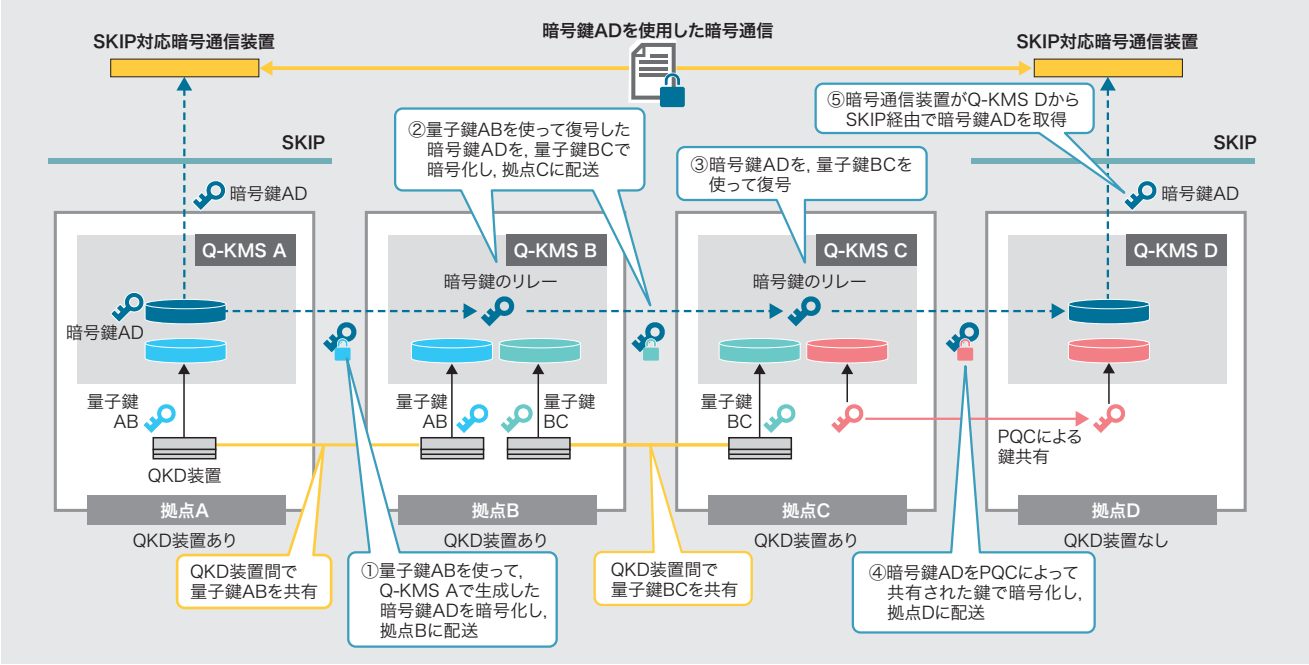
⑵ GPU（Graphics Processing Unit）の柔軟な活用　従来は高速性優先でリクエストごとにGPUを占有したが，複数利用者に対するスループット向上と両立できる効率的な運用が課題である。

⑶ 容易なインターフェース追加　SQBM+™の基本インターフェースはQUBO（二次制約なし二値最適化）という問題定義である。しかし，実問題では上位アルゴリズムとの連携が不可欠で，インターフェース追加を容易にする拡張性が課題である。

これらの課題を次のように解決した。一つは，問題分割とGPUコード最適化である。10億変数規模では，GPUメモリー容量の確保とGPU間データ転送コストの削減が課題になる。転送コストが減るようなブロックに問題データを分割してGPUに割り当てることで解決した。そして，メモリーアクセスや同期タイミングの最適化などで，大規模問題のGPU計算を高速化させた。もう一つは，フロントエンド分離とGPU動的割り当てである。フロントエンドで受けた複数リクエストに，バックエンドが管理するGPUを動的に割り当てることで，⑵に対応した。また，フロントエンド分離を生かしてマイクロカーネルアーキテクチャーを採用したことで，上位アルゴリズムの追加を容易にして拡張性を高め，⑶に対応した。これらの解決策で，10億変数・100億非ゼロ要素の大規模問題が解けることを確認し，特定問題を解く上位アルゴリズムを入れ替え可能な形で追加し，拡張性も確認できた。

東芝デジタルソリューションズ（株）

多様なネットワーク環境への対応を強化した量子鍵管理システム Q-KMS



Q-KMSの概要
Quantum Key Management System (Q-KMS) overview

量子鍵配送（QKD：Quantum Key Distribution）は，量子力学の原理を利用し，盗聴の有無を確実に検知できる仕組みにより暗号鍵を安全に共有できる技術である。QKDの実用化には，生成した暗号鍵を管理・配布する鍵管理システム（KMS：Key Management System）が不可欠である。

KMSは，光ファイバーなどを通じてQKD装置間で共有した量子鍵を用いて，複数拠点間で暗号鍵をリレーすることで，QKD装置同士が直接接続されていない拠点間でも安全に暗号鍵を配送できる。更に，鍵の有効期限や使用状況を管理し，大量の鍵を事前に蓄積することで，安定した鍵提供を実現する。

当社は，多様なネットワーク環境に対応できるように，既存製品の量子鍵管理システム（Q-KMS：Quantum KMS）の機能を拡張した。

まず，暗号通信装置などがQ-KMSから暗号鍵を取得するために使用するインターフェースとして，従来のETSI GS QKD 014（欧州電気通信標準化機構が定めた標準規格）への対応に加え，多数のCisco社製ネットワーク機器でサポートされるSKIP（Secure Key Integration Protocol）に対応した。SKIPへの対応で，既存のCisco社製機器を活用した暗号通信システムが構築可能になった。

そして，新たに耐量子計算機暗号（PQC：Post-Quantum Cryptography）による鍵配送機能を追加した。PQCは，将来登場する強力な量子コンピューターでも解読が困難な数学的問題に基づいた暗号技術である。この機能で，地理的な制約などからQKD装置を設置できない拠点でも，暗号鍵の共有が可能になった。QKDとPQCを組み合わせることで，コストとセキュリティーのバランスを取りながらネットワーク全体の耐量子性を高めることができる。

今後も，市場のニーズに合わせて機能改善を進めていく。

東芝デジタルソリューションズ（株）