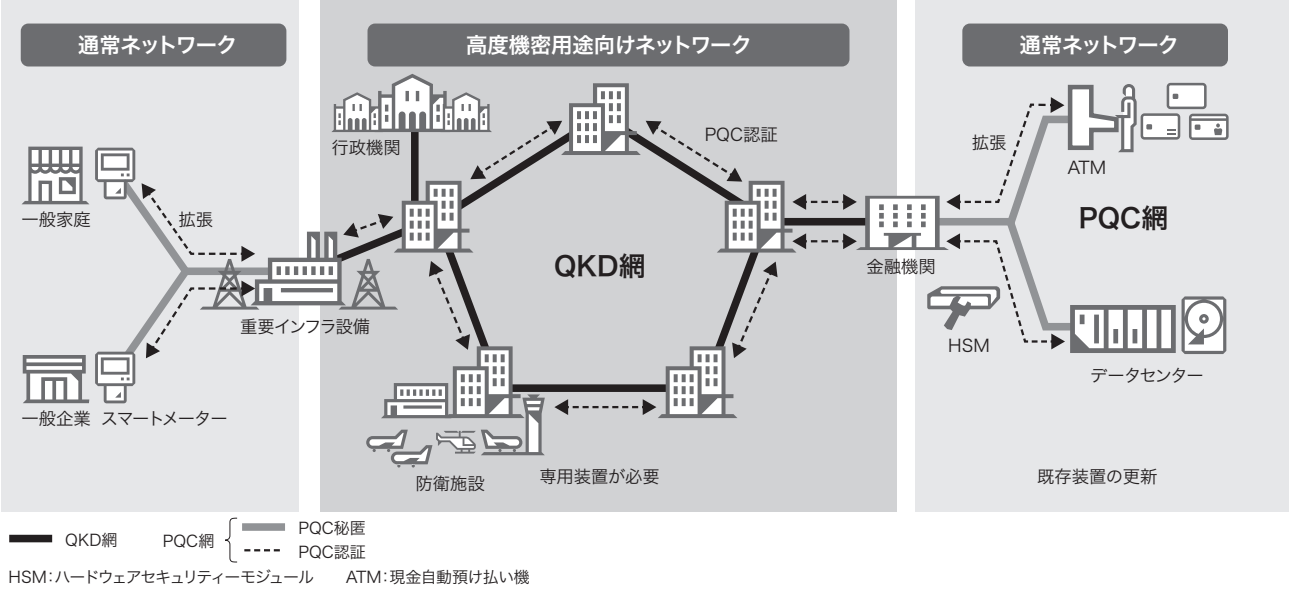
量子セキュアネットワークを実現する量子鍵配送・耐量子計算機暗号技術

Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) Technologies for Realizing Quantum-Secure Networks



量子セキュアネットワークの構成例
Example of quantum-secure network configuration

量子計算機の進展により，これまで計算困難と考えられてきた素因数分解問題や離散対数問題が効率的に解けるようになり，これらの問題を安全性の根拠としている現行の公開鍵暗号やデジタル署名が近い将来破られることが懸念されている。このセキュリティー上の脅威に耐え得る情報通信基盤を構築し移行することが喫緊の課題となっている。

そのための要素技術には，物理的な性質を使って安全性を担保する量子鍵配送（QKD）と，量子計算機でも解読困難な耐量子計算機暗号（PQC）の二つがある。

QKDは，光子の量子状態を利用した鍵共有方式であり，盗聴を物理的に検知可能なことから高い安全性を持つ。一方，専用装置の導入や中継拠点の運用が必要なため，高度機密用途への適用が想定されている。東芝は，普及に向けて微弱光子検出と高速信号処理の融合による高速化と，独自のTwin Field QKDプロトコルや位相安定化技術により通信距離の長距離化を実証している。PQCは，量子計算機に対しても計算困難とされている問題に基づく公開鍵暗号であり，専用装置の必要がない一方で，鍵サイズが大きく，計算資源が乏しいデバイスでの適用が懸念されている。当社は，メモリーの少ないデバイスでも実装可能とする省メモリー化技術や，非線形不定方程式の求解問題に基づく軽量なPQCの開発を進め，適用範囲を広げる取り組みを行っている。

量子計算機の脅威に対しては，欧米を中心に2035年までのPQC移行の勧告が出され，移行が進められている。当社は，PQC移行を推進しつつも，今後の継続的な計算機の発展によるPQCの危殆（きたい）化リスクへの対策として，量子計算機でも解読困難なQKDとPQCを効果的に組み合わせた，量子セキュアネットワークの構築を進めている。すなわち，高度機密用途向けネットワークでは，QKDで鍵を共有し，認証はPQCで補完する。これ以外の通常ネットワークでは，現行の公開鍵暗号をPQCに変更する。これらによりPQC移行を進めつつ，高度機密情報の秘匿性を長期に担保する。

今後は，通信インフラとの連携を含むQKD網の広域展開と，各種デバイスへのPQC実装を推進し，量子計算機時代においても安全な情報基盤を実現する。

松本　麻里　MATSUMOTO Mari
総合研究所 AIデジタルR&Dセンター コンピュータ&ネットワークシステム研究部

谷澤　佳道　TANIZAWA Yoshimichi
総合研究所 AIデジタルR&Dセンター コンピュータ&ネットワークシステム研究部

秋山　浩一郎　AKIYAMA Koichiro
総合研究所 AIデジタルR&Dセンター セキュリティ基盤研究部