R&Dフェーズ｜研究　**実用化時期**｜FY27-

Mehr Licht!
More Photonics for Intelligence

#C19

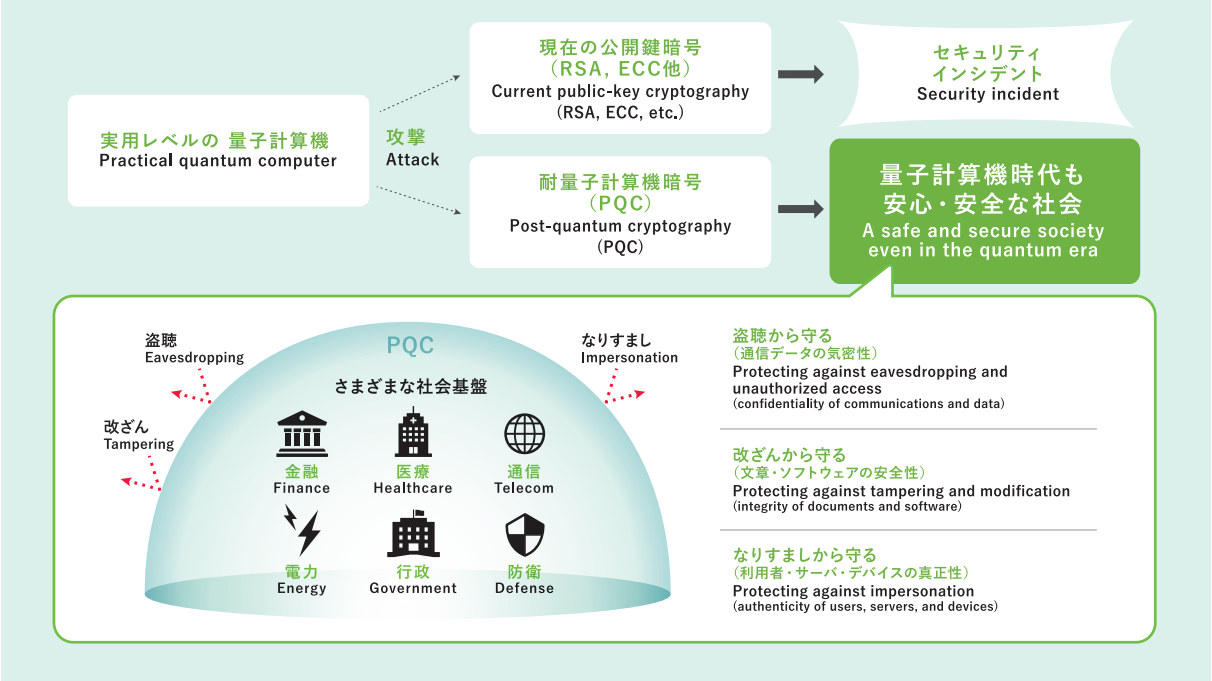
#安心・安全#リスクマネジメント

量子計算機時代の社会を支える国産暗号技術

世界最高水準の暗号研究を基に、量子計算機時代も安心・安全で信頼できる社会基盤を支えます

技術課題・ゴール

量子計算機の出現により、現在広く利用されている公開鍵暗号の安全性に対する脅威が高まっています。私たちは、この課題に対応するため、耐量子計算機暗号技術（PQC: Post-Quantum Cryptography）の研究・標準化を進めてきました。今後、PQCの社会実装が進むことにより、量子計算機時代でも安心・安全なデジタル社会が継続的に実現されます。



技術ポイント

要素技術

・処理効率で優位性のあるPQC暗号化方式：NTRU
・署名サイズの小ささで優位性のあるPQC署名方式：QR-UOV、SQIsign

市中技術差異点

・国産技術を核にした、最高レベルの安全性（IND-CCA2, EUF-CMA）を持つPQC暗号化・署名方式を保有
・国内で唯一、研究・国際標準化・社会実装を一貫して推進。PQC暗号化・署名方式の高速実装を保有

適用ビジネス/ユースケース

情報技術

通信暗号化、デジタル署名、PKI基盤などで広く利用されている公開鍵暗号を耐量子化することにより、量子計算機時代でも安心・安全なデジタル社会を実現します。

出展組織

NTT株式会社 社会情報研究所