SoftBank R&D SOFTBANK CORP. RESEARCH INSTITUTE OF ADVANCED TECHNOLOGY

量子コンピューター時代のセキュリティ対策

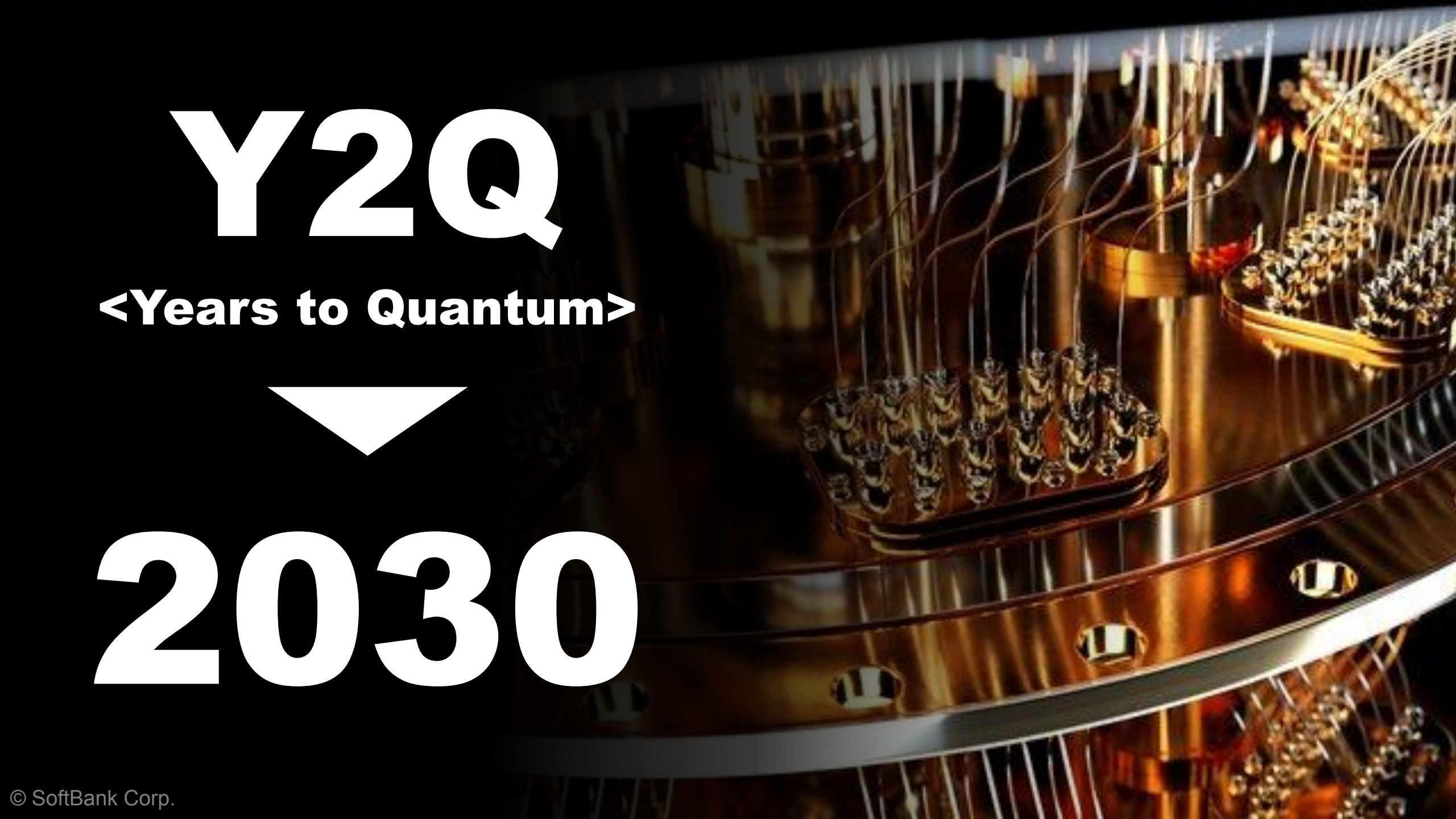
先端無線部　課長

稲井　誠

Y2Q

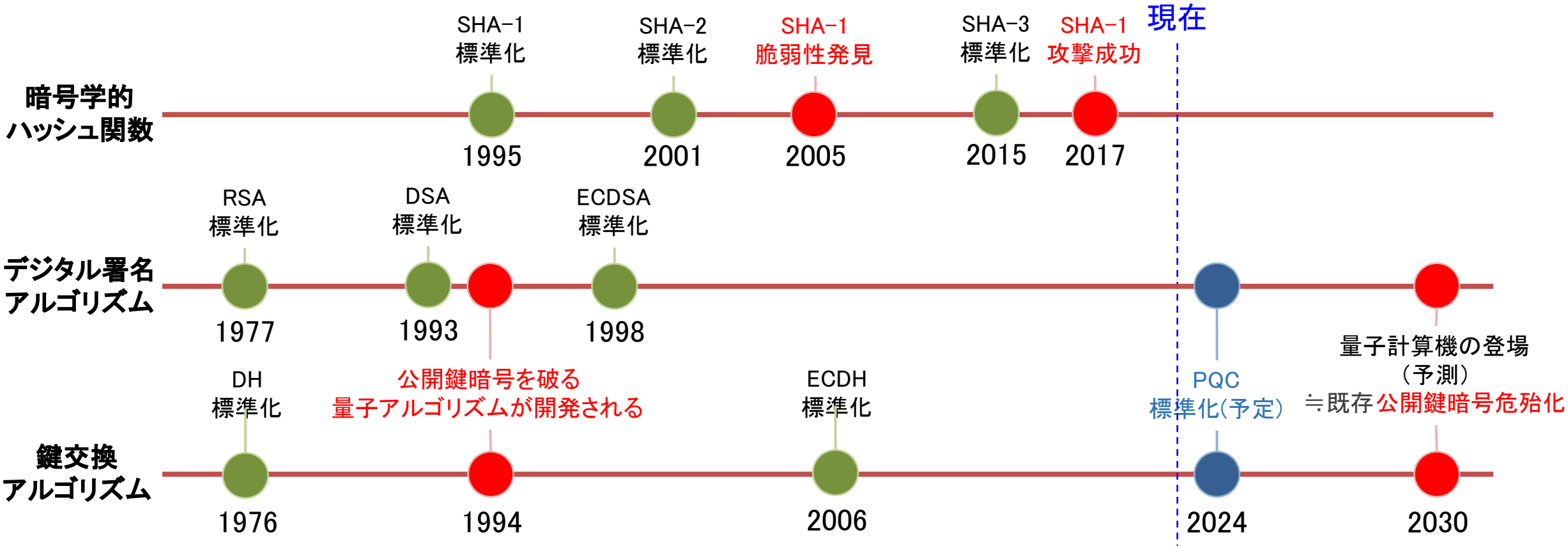
<Years to Quantum>

2030

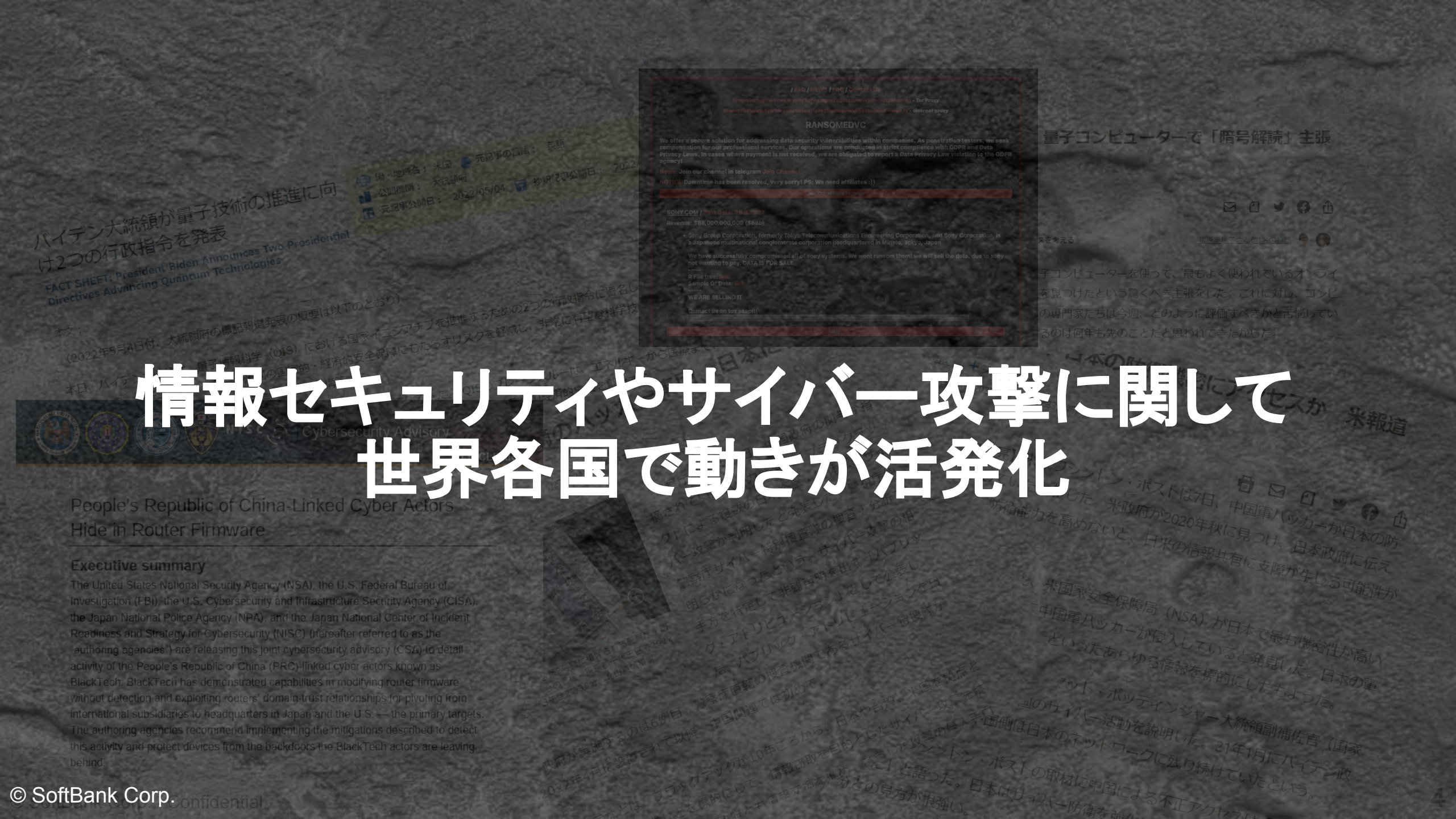


SoftBank R&D

暗号技術の過去と未来



量子コンピューターの登場により、
セキュリティ技術は新時代へ



情報セキュリティやサイバー攻撃に関して世界各国で動きが活発化

ハーベスティング攻撃

今の内に機密データを搾取、保管

量子コンピューター登場後に解読

各業界への影響

金融

政府機関

医療

等…

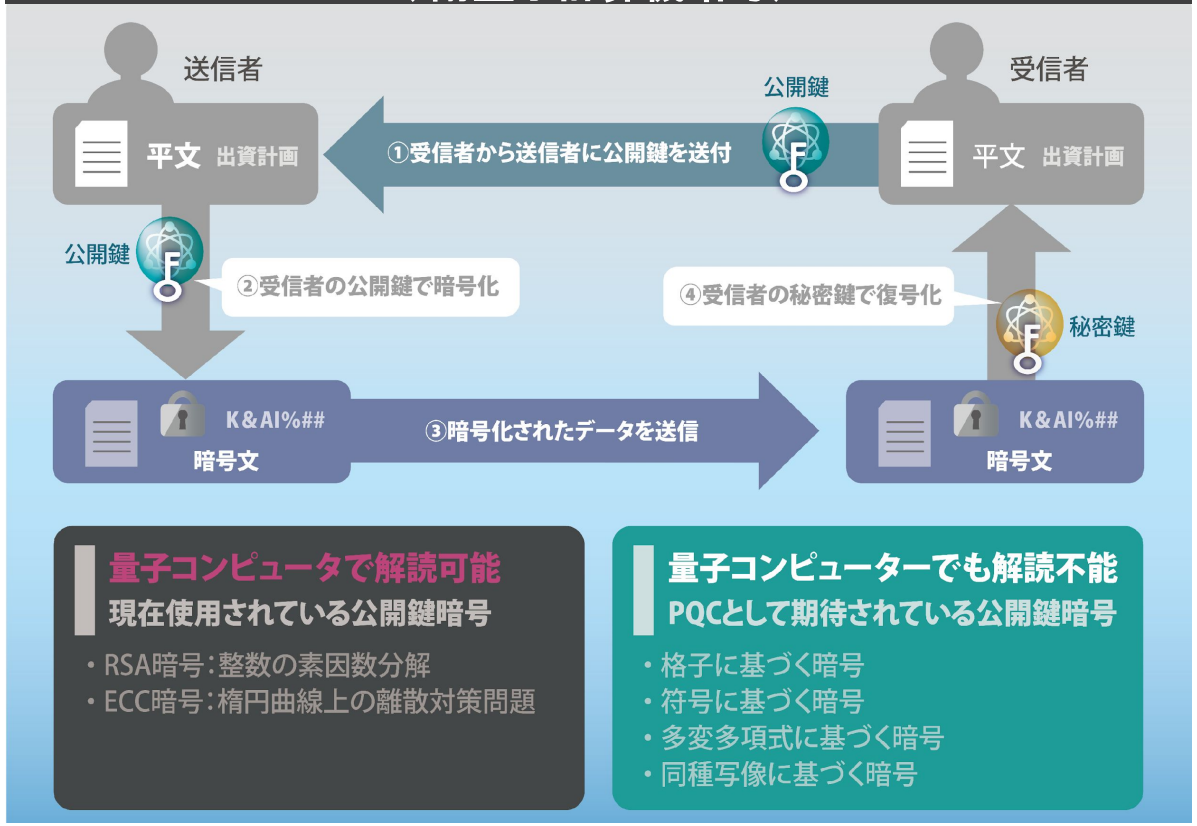
デジタル社会での情報の安全は最重要

次世代のセキュリティ技

QKD
（量子鍵配送／量子暗号通信）

量子通信による暗号鍵配送技術
様々な国や研究機関で実験が進められている。

PQC
（耐量子計算機暗号）



既存暗号技術の進化系
2024年にNISTによる標準化が実施される予定

ソフトバンクの取り組み

QKD

ソフトバンクと東芝デジタルソリューションズ、IPsec QKD-VPNの実証実験に成功

～Beyond 5G／6G時代の量子セキュアネットワークの実現に向けて共創を開始～

2023年9月20日
ソフトバンク株式会社
東芝デジタルソリューションズ株式会社

ソフトバンク株式会社（以下「ソフトバンク」）と東芝デジタルソリューションズ株式会社（以下「東芝デジタルソリューションズ」）は、Beyond 5G／6G時代の量子セキュアネットワークの実現に向けて共創を開始し、量子暗号技術であるQKD（Quantum Key Distribution、量子鍵配送）を用いた拠点間VPN（Virtual Private Network）通信の実証実験に成功しましたので、お知らせします。

実験に用いたQKDシステム装置

背景

Beyond 5G／6Gの時代、通信ネットワークは社会インフラの一部に進化し、今よりも強固なセキュリティーが求められることになります。現在の通信ネットワークで使われている暗号技術はおよそ10年ごとに世代交代が行われ、2030年末には現在使われている暗号技術の一部（RSA2048など）がセキュリティー寿命を迎えると言われています。そのため、世界各国で通信の安全を守るための研究が進んでおり、ソフトバンクでも、これまでに量子コンピューターでも解読が困難な新しい暗号技術であるPQC（Post Quantum Cryptography、耐量子計算機暗号）の実用化に向けて取り組みを行ってきました。
（https://www.softbank.jp/corp/news/press/sbkk/2023/20230228_01/）

https://www.softbank.jp/corp/news/press/sbkk/2023/20230920_01/

PQC

耐量子計算機暗号アルゴリズムの実用性を確認

～ソフトバンクとSandboxAQとのパートナーシップを通して実証～

2023年2月28日
ソフトバンク株式会社
SandboxAQ

ソフトバンク株式会社（本社：東京都港区、代表取締役 社長執行役員 兼 CEO：宮川 潤一、以下「ソフトバンク」）は、米国SandboxAQ（所在地：米国カリフォルニア州パロアルト、CEO：Jack Hidary）とのパートナーシップを通して、PQC（Post Quantum Cryptography、耐量子計算機暗号）を早期に利用可能にする、古典暗号（楕円曲線暗号）とPQCとのハイブリッド方式の実証を完了し、既存のネットワークにも問題なく適用できることを確認しましたので、お知らせします。

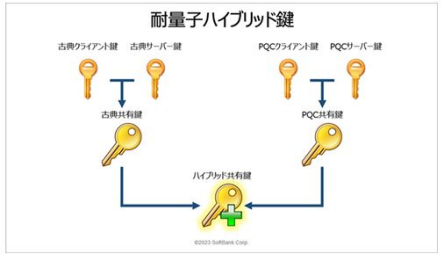
量子コンピューターが登場し、公開鍵暗号アルゴリズムの脅威となることで、セキュリティー意識が高い組織は、PQCの導入を余儀なくされます。また、米国国立標準技術研究所（NIST）によってPQCは標準化される予定で、今後多くの行政などでも使用が義務付けられると想定されます。古典暗号ベースの暗号体系が、今後数年で量子コンピューターによって破綻に追い込まれる可能性はなく、当面は、安心して通信サービスを利用することができますが、インターネット上のデータから不正にパケットを盗み出して保管しておき、量子コンピューターの実用後に解読するSNDL（Store Now, Decrypt Later）という攻撃の脅威にさらされる可能性があり、PQCの早期導入が必要と考えられています。また、さらなる高度情報化社会の発展により、ネットワークにPQCを適用することが重要となります。

PQCは、量子コンピューターで解読することが困難で強固なアルゴリズムですが、実績がある古典暗号とのハイブリッド方式を採用することで、お客さまが安心かつ容易に導入していただけるようになります。このハイブリッド方式によって、これまで古典暗号によって担保されてきた安全性を失うことなく、量子コンピューターの攻撃に対しても安全性を確保することが可能になります。一方で、暗号化処理の複雑化によって、暗号・復号に要する時間、装置に対する処理負荷、通信に対するオーバーヘッド率を悪化させてしまう懸念がありました。

今回、汎用のスマートフォンとサーバーを利用してモデル化した実トラフィックを、古典暗号とPQCとのハイブリッド方式に適用し、暗号・復号の処理遅延、プロセッサーやメモリーの負荷や負荷率、接続率、通信に必要なデータ量などを評価した結果、ハイブリッド方式の性能が実用的であることが確認できました。

また、標準化候補のPQCアルゴリズム間で比較した結果、構造付き格子暗号と古典暗号との組み合わせが最少のオーバーヘッド率であり、最も優れた性能を発揮することが、ソフトバンクのネットワークを利用した実証で確認ができました。

ハイブリッド方式のイメージ



https://www.softbank.jp/corp/news/press/sbkk/2023/20230228_01/

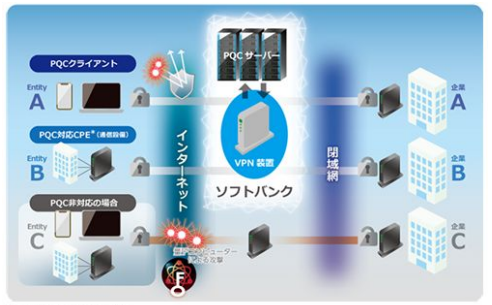
ソフトバンクがSandbox AQと共同で量子コンピューターで解読不可能な次世代暗号方式の早期実装へ

2022年3月23日
ソフトバンク株式会社
Sandbox AQ

ソフトバンク株式会社（本社：東京都港区、代表取締役 社長執行役員 兼 CEO：宮川 潤一、以下「ソフトバンク」）と米国Sandbox AQ（所在地：カリフォルニア州パロアルト、CEO：Jack Hidary、以下「Sandbox」）は、耐量子計算機暗号（Post Quantum Cryptography、以下「PQC」）を使用したVPNなどの実用化に向けて、日本での共同実証実験に関するパートナーシップ契約を締結しました。この契約により、ソフトバンクは、アメリカ国立標準技術研究所（NIST）が推進する「耐量子計算機暗号標準化プロジェクト」のラウンド3の最終候補および代替候補に選定されたPQCアルゴリズムを使用した検証を行い、将来的な標準化を見据えたPQCをいち早く実用化することも可能になります。

昨今の生活においてインターネットは必要不可欠であり、クレジットカード情報や個人情報などの機密情報をスマートフォンのアプリなどでやりとりをする機会が増えています。現在は、それらの通信内容を秘匿にするために、公開鍵暗号（RSA暗号や楕円曲線暗号）などを用いて高い安全性を保っています。しかし、世界中で開発が進められている量子コンピューターによって、現在広く普及しているこれらの暗号が、今後、瞬時に解読され通信の中身が簡単に盗まれる可能性が危惧されています。この問題を解決するために、量子コンピューターでも解読が困難な新しい暗号であるPQCの実用化および導入が必要不可欠です。PQCは、秘匿だけでなく認証（デジタル署名）にも適用することができ、ソフトウエアで実装できるため、インターネットとの親和性が高く、スマートフォンやタブレットなど、既存の通信デバイス上での利用が想定されています。

米国では、2030年ごろまでに暗号鍵長2,048ビットのRSA暗号を解読可能な量子コンピューターの登場を想定し、NISTにおいて「耐量子計算機暗号標準化プロジェクト」を推進しており、PQCとして採用する暗号アルゴリズムを2024年に決定するとしています。今回、Sandbox AQが提供するPQCは、NISTの「耐量子計算機暗号標準化プロジェクト」のラウンド3の最終候補および代替候補として選定されたさまざまなアルゴリズムを使用することができ、将来の標準化を見据えた検証を行うことが可能となります。ソフトバンクは、2022年夏までに、5G、4G、Wi-Fiなどのさまざまなネットワーク上でPQCアルゴリズムを動作させ、ネットワーク、マシン、ユーザーそれぞれの観点から性能を評価・検証していきます。また、今後お客さまが量子コンピューターからの攻撃にも耐性を持つセキュリティーを活用できるよう、商用ネットワークに早期にPQCを適用することも検討していきます。

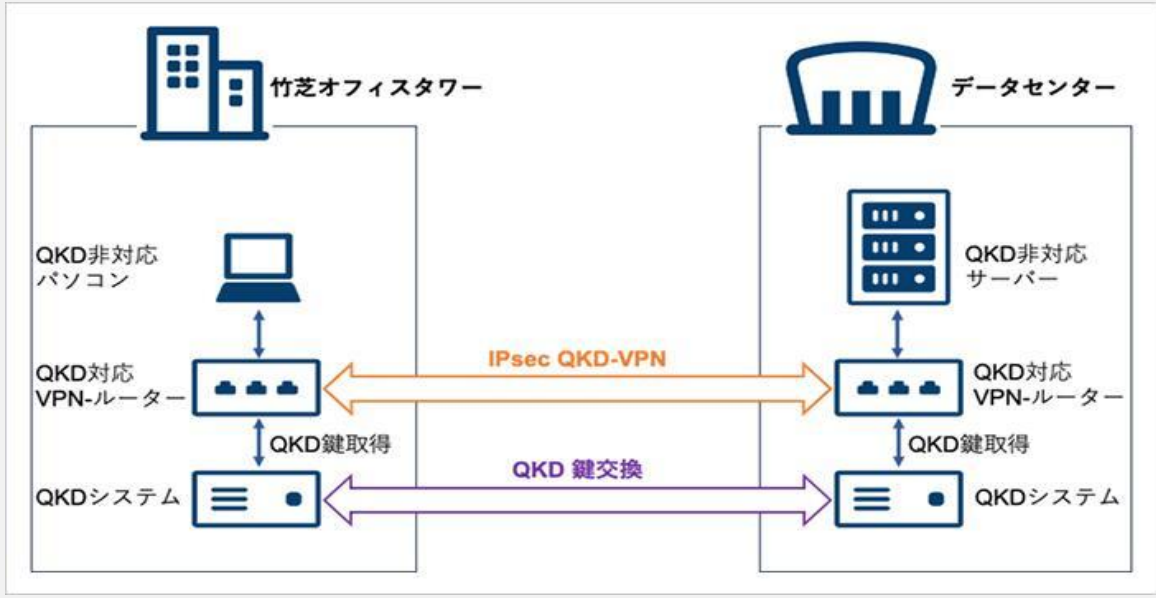


耐量子計算機暗号システム構成イメージ

https://www.softbank.jp/corp/news/press/sbkk/2022/20220323_01/

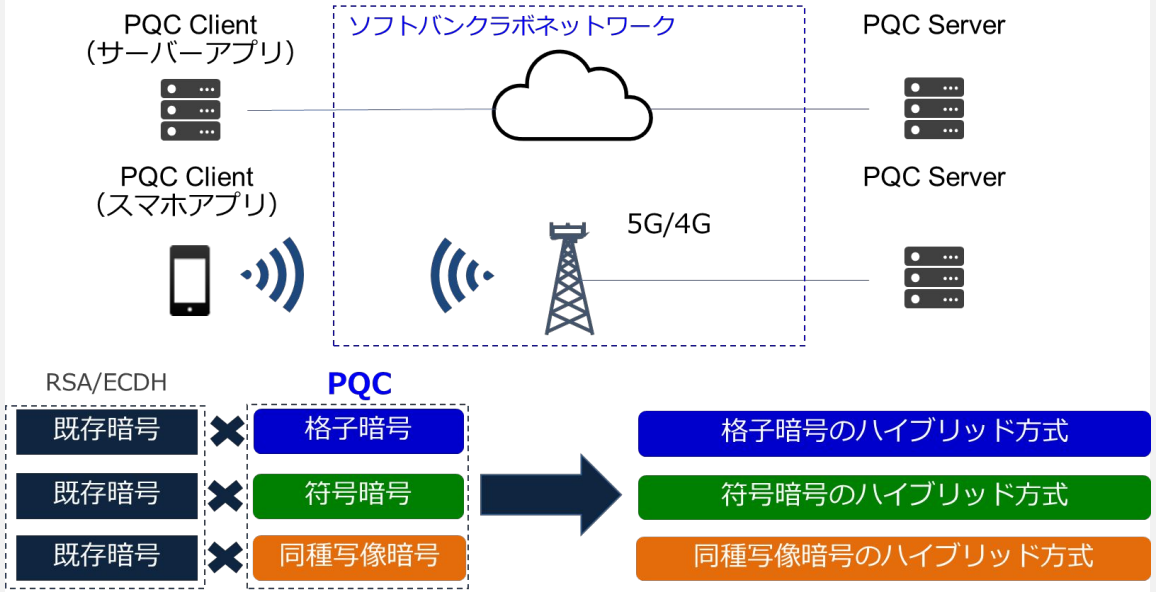
ソフトバンクの取り組み

QKD
（量子鍵配送／量子暗号通信）



上記の基本構成に加えて、次世代技術を組み込んだ拡張性の高い新たなQKDの研究も進行中

PQC
（ 耐量子計算機暗号）

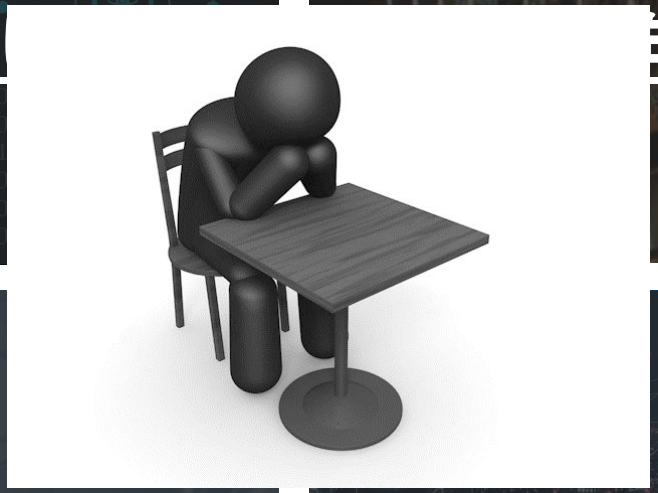


RSAを代表する成熟された既存暗号と若いPQCを組み合わせる事によって、初期の課題を解決

世の中の印象と対策課題

今のままで対策出来て

年って、まだまだ先…



対策方法が不明

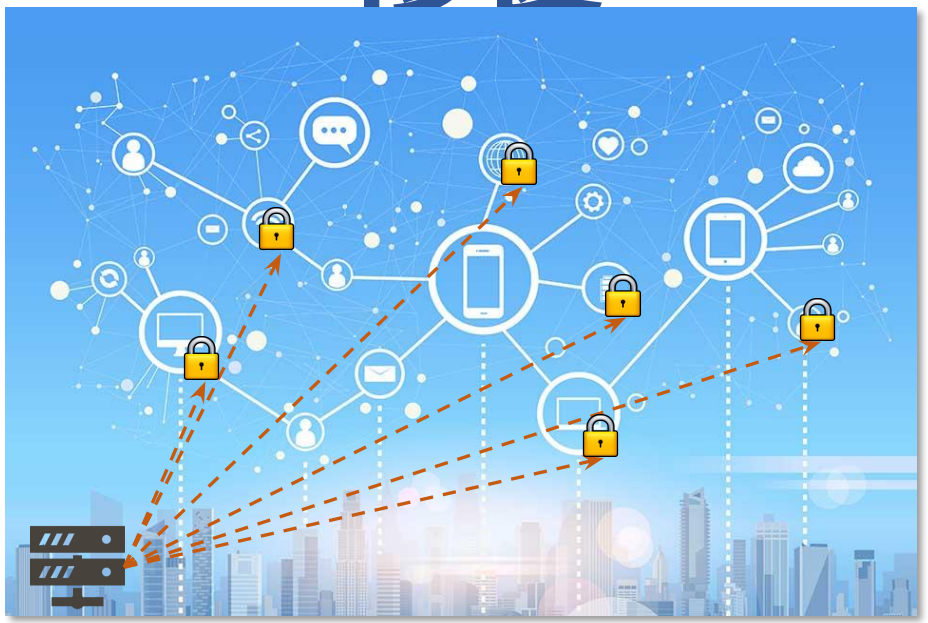
リプレイスは大変

未来に向けた活動

発見

ネットワーク内の脆弱性を自動で発見

修復



脆弱性を自動で次世代暗号技術へ修復

容易に安心を手に入れる未来を実現するべく活動中

まとめ

- ✔ 2030年に量子時代に突入しデジタル社会の脅威への対策が必須
- ✔ 既にデジタル社会の安全は脅かされている
- ✔ 量子時代の対策はQKD、PQCの新暗号技術にて対策可能
- ✔ 容易に安全を手に入れるべくソフトバンクは進行中

SoftBank R&D

情報革命で人々を幸せに