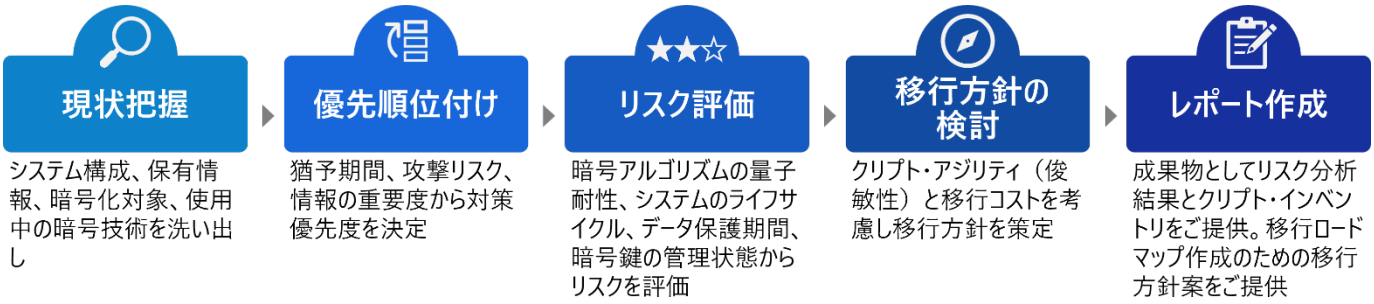
News Release

HITACHI

2025 年 10 月 7 日
株式会社日立ソリューションズ

量子コンピュータ時代に向けてデータ資産を守る「耐量子計算機暗号への移行に向けた支援サービス」を提供開始

金融機関を中心に、既存の暗号技術の分析からリスク評価、移行の優先付け、移行方針の提案まで、トータルに支援



「耐量子計算機暗号への移行に向けた支援サービス」で提供する5つのステップ

株式会社日立ソリューションズ（本社：東京都品川区、取締役社長：森田 英嗣／以下、日立ソリューションズ）は、量子コンピュータで暗号化を破られる将来的なリスクに備え、企業が IT システムで使用している暗号技術の洗い出しからリスク評価、移行方針の提案までを行う「耐量子計算機暗号への移行に向けた支援サービス」を、10 月 8 日より提供開始します。長期秘匿性が必要なデータに対し、解読困難な数学的構造を基盤にした耐量子計算機暗号[*1]（以下、PQC）への移行を支援します。量子コンピュータの実用化が近づく中、現在の暗号通信を盗聴、保存する HNDL 攻撃[*2]の脅威が高まり、金融庁は金融機関に対し、PQC への早期移行を要請しています。本サービスは、セキュリティ専門のエンジニアが設計書の解析と管理者へのヒアリングを元に、暗号技術の使用箇所や方式、用途などをリスト化するクリプト・インベントリ[*3]を作成します。クラウドのシステムは Fortanix® Inc.の「Key Insight」も用い、暗号化の状態やアルゴリズムを洗い出します。暗号技術の変更を見据え、クリプト・アジリティ（俊敏性）を考慮した移行方針も提案します。

日立ソリューションズは、30 年以上「秘文」の開発で蓄積した暗号化技術の知見を新たな技術分野へと発展させ、企業や社会のサステナビリティ・トランスフォーメーション(SX)実現に貢献していきます。

*1 耐量子計算機暗号（PQC）：Post-Quantum Cryptography。格子ベース暗号、符号ベース暗号、多変数多項式暗号のように、量子計算でも解読困難な数学的構造を基盤にした暗号方式

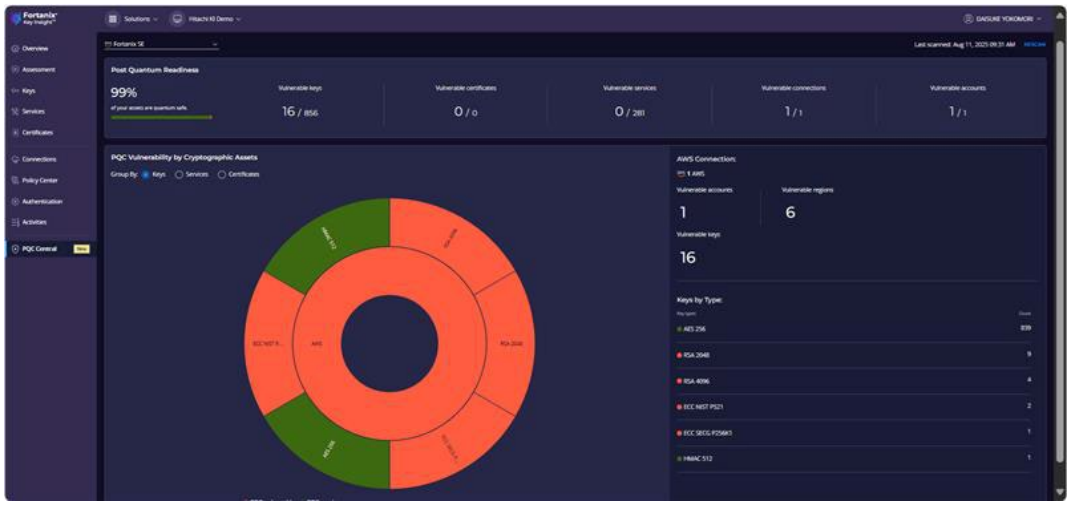
*2 HNDL 攻撃：Harvest Now, Decrypt Later。現在の暗号データを盗聴・保存しておき、将来量子コンピュータで解読する攻撃手法

*3 クリプト・インベントリ：暗号技術の使用箇所・方式・用途を棚卸し、暗号アルゴリズムの種類、鍵の属性、暗号化対象、利用システムやサービス名、データの保存期間や暗号の用途、耐量子計算機暗号対応状況などを体系的にリスト化したもの

「耐量子計算機暗号への移行に向けた支援サービス」の特長

1. 暗号技術に精通する日立ソリューションズのエンジニアがクリプト・インベントリを作成。リスクを評価し、量子耐性が低い暗号技術の使用箇所について、猶予期間、攻撃リスク、情報の重要度などから、移行の優先付けを実施

2. AWS や Microsoft Azure 上のシステムは Fortanix® Inc.の「Key Insight」を活用し、暗号化の状態、暗号鍵の管理状態、証明書の管理状態、量子脆弱性などのセキュリティリスクを迅速に分析（11 月より提供開始）
3. 使用中の暗号アルゴリズムの洗い出しに加え、暗号鍵の管理状態や暗号機能の実装方法を評価。また、評価結果を踏まえて、暗号化技術の変更が必要になった場合に備えて、すばやく対応できるよう、柔軟性を考慮した移行策を提案



「Key Insight」による分析イメージ

今後の展開

量子コンピュータという画期的な技術の台頭に伴い、セキュリティ対策の見直しは、持続可能な社会や企業経営にむけて取り組むべき課題です。日立ソリューションズは従来のセキュリティノウハウを発展、洗練化させるとともに、日立製作所と連携し、金融機関をはじめ、医療や行政などに、耐量子計算機暗号への移行を支援するサービスを拡大していきます。

背景

量子コンピュータの実用化により、RSA[*4] や ECDSA[*5] などの既存の公開鍵暗号技術で暗号化したデータが解読されるリスクが高まっています。金融庁は、2025 年 5 月、大手銀行や地方銀行などの金融機関に向けて、PQC を実装したシステムへと早期移行を要請しています。数年にわたるシステム移行では、暗号技術の使用箇所や方式を洗い出したクリプト・インベントリを整備し、適切なリスク評価、優先付け、移行計画の策定が重要です。

日立ソリューションズは、情報漏洩防止ソリューション「秘文」の開発や、秘匿化、暗号鍵分野での実績を有するとともに、ホワイトハッカーやセキュリティコンサルティングをはじめ、セキュリティを専門とする人財を育成してきました。これらのノウハウや人財を量子計算という新たな分野に発展させ、本サービスを提供していきます。

*4 RSA（Rivest Shamir Adleman）

*5 ECDSA（Elliptic Curve Digital Signature Algorithm）

「耐量子計算機暗号への移行に向けた支援サービス」について

https://www.hitachi-solutions.co.jp/pqc/

日立ソリューションズについて

日立ソリューションズは、お客さまとの協創をベースに、最先端のデジタル技術を用いたさまざまなソリューションを提供することで、デジタルトランスフォーメーションを実現します。欧米、東南アジア、インドの各拠点が連携し、社会や企業が抱える課題に対して、グローバルに対応します。

そして、人々が安全にかつ安心して快適に暮らすことができ、持続的に成長可能な社会の実現に貢献していきます。

詳しくは、日立ソリューションズのウェブサイト(https://www.hitachi-solutions.co.jp/)をご覧ください。

ソリューションに関するお問い合わせ先

株式会社日立ソリューションズ

https://www.hitachi-solutions.co.jp/inquiry/

報道機関お問い合わせ先

担当：大鳥、安藤
株式会社日立ソリューションズ
経営企画本部 広報部
koho@hitachi-solutions.com

――

――