信頼される安心を、社会へ。
SECOM

量子コンピュータによる暗号解読の脅威と対応の概観

～耐量子計算機暗号（PQC）の果たす役割～

セコム株式会社 IS研究所　伊藤忠彦

本発表は発表者個人の見解に基づくものであり、発表者が所属する組織等の公式見解ではありません

自己紹介

信頼される安心を、社会へ。 SECOM

伊藤　忠彦

セコム株式会社　IS研究所　暗号・トラストグループ

- 主な研究分野：
  - **暗号鍵管理**全般
  - **ルート認証局**のポリシー管理・運用
  - 暗号システムの**移行**・制度設計

- 主な活動領域：標準化やルール整備
  - **IETF** (鍵管理関連規格提案：RFC 8813, RFC 9295, RFC 9336など)
  - **CA/BForum** (Web用証明書に関するルール整備)
  - **IPA**　非常勤 研究員（ガイドライン作り等）

- 耐量子計算機暗号に関連する活動：
  - 量子コンピュータの暗号への影響調査（2017～）
  - 日本銀行　金融研究所より、ディスカッションペーパー公開（2019）
  - CA/BForumにて、PQCに関する検討（～2021）
  - CRYPTREC(暗号技術評価委員会) 耐量子暗号WG 委員（2022～）
  - IETFやCABForum等の標準化団体で、課題や論点の打ち込み
  - その他、論文等

整理した論点を公開したもの

https://www.secom.co.jp/isl/news/2023/1115-IEICE-ito/1026-1030_IEICE_journal_November_06.pdf

目次

- 背景
  - 量子コンピュータによる暗号解読
  - 影響範囲：公開鍵暗号
  - 最大の課題：猶予期間の不透明性
- 脅威と対策
  - 脅威
  - 対策
- 要検討事項：より優先して対応した方が良いユースケースもある
  - 優先度が低めな事例（1件）
  - 優先度が高い事例（2件）

背景

背景：量子コンピュータによる暗号解読の脅威

- Shorのアルゴリズム(1994年)
  - 理想的な量子コンピュータが存在すれば、素因数分解を高速で解ける
    ※現在の多くの暗号の安全性は、素因数分解の困難性に依存している

- 商用量子コンピュータが発表される（D-Wave、2011年）
  - 素因数分解が解けるタイプではなかったが、「量子コンピュータによる暗号解読」が現実の脅威となりうるのでは？と話題に

- その後も、量子コンピュータ技術は継続して発展

- **「耐量子性」**（量子コンピュータが登場しても安全な性質）のニーズが高まる
  - 既存暗号の中には、耐量子性を持たないものもある。

量子コンピュータによる攻撃の影響範囲

NISTの見解

公開鍵暗号

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

公開鍵暗号の代表的な利用局面

- 通信相手との暗号鍵（共通鍵）の共有
  - 通信コンテンツは共通鍵暗号で暗号化されていても、
    共通鍵暗号で用いる暗号鍵の共有に、公開鍵暗号を利用
  - 公開鍵暗号の利用により、鍵管理のコストを削減し、
    スケーラビリティを大幅にあげることができる。

- 通信相手の認証
  - 相手を確認できる
  - （例えば、インターネットにおいて、以下をスケーラブルに実施）
    - 利用者は目当てのサービスであることを確認できる。
    - サービス提供者は、匿名の相手（や初めて利用する相手）にサービスを提供できる

公開鍵暗号は、インターネットにおいても、様々な用途で、広く使われている

脅威と対策

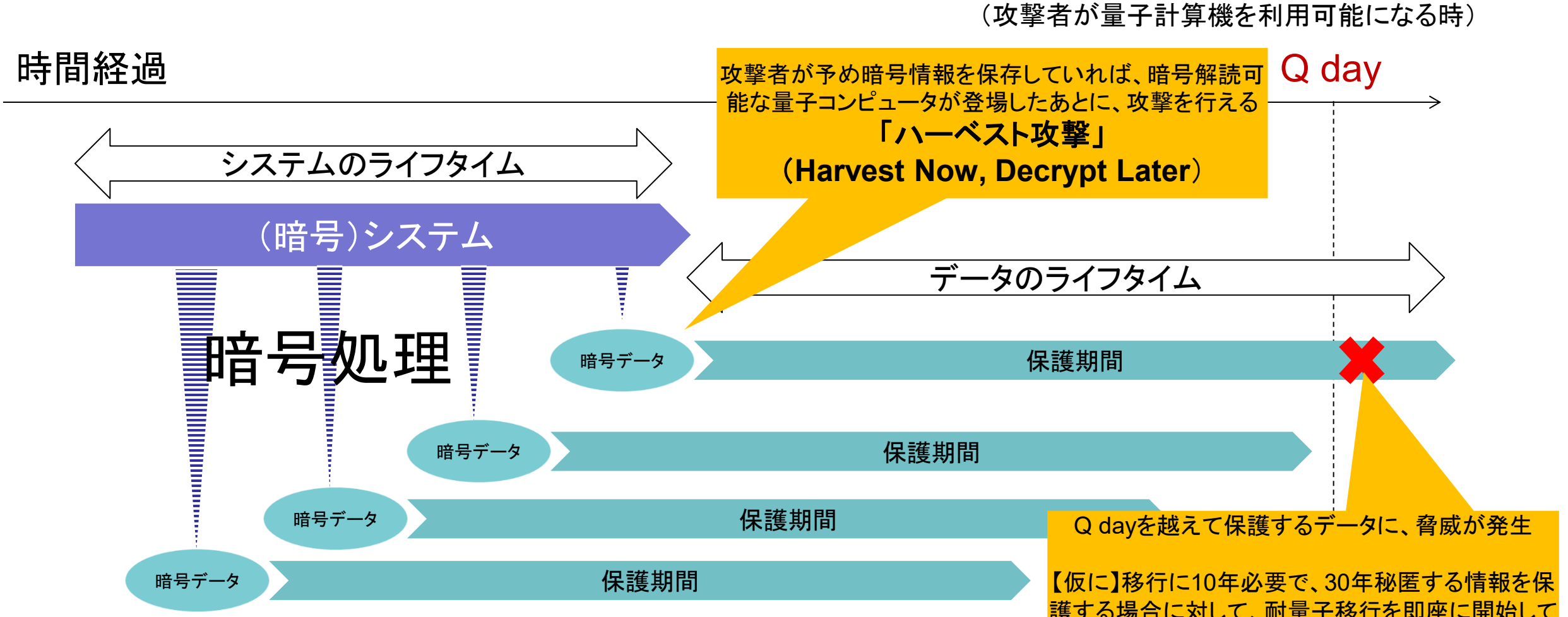
脅威を特定する上での課題

- 「量子コンピュータによる暗号解読」が、いつ実現しそうかの予測が困難
  - 暗号解読を行うためには、様々な技術的ブレークスルーが必要
  - 実現時期については、多様な見解
    - 2030年に「解読できる」と言っている人もいる（いた）
    - 「CRYPTREC暗号リスト記載の暗号技術が**近い将来に危殆化する可能性は低い**」（CRYPTREC, 2020）
    - 米国政府は、**2035年までに**、できる限りの**量子耐性**を持たせるように要求（NSM10, 2022）
    - 「**2050年頃まで**に、大規模化を達成し、**誤り耐性型汎用量子コンピュータ**を実現する」ことがターゲット（内閣府　ムーンショット目標6）
    - 100年程度では実現しないのでは？という意見も
- 公開鍵暗号は非常に広く使われているが、ユースケースによって脅威が大きく異なる（後述）
  - スマホ、PCの中には、様々な用途に利用される、大量の鍵が存在する
  - 用途（やプロトコル）毎に別の鍵を利用することが推奨されているため、鍵は減らない
- 公開鍵暗号以外の方式を採用する場合は、脅威モデルの再評価が必要となりうる（後述）
  - 従来、公開鍵暗号を効率的に使うことで、アタックサーフェスを限定してきたが…
    その前提が崩れるかもしれない

いつ実現するか分からない脅威に、何故備えるか？
何故そんな急いでいるのか？

手遅れになるかもしれないから
（既に手遅れのものもあるかもしれないから）

脅威の概観：長期間ライフサイクルにおける脅威



脅威の程度に大きな影響を与える要素

- 公開鍵暗号の利用形態
  - **秘匿用途** / 認証用途 / 署名用途

攻撃者が予め暗号情報を保存していれば、暗号解読可能な量子コンピュータが登場したあとに、攻撃を行える
（**Harvest Now, Decrypt Later**）

- システムのライフサイクルの長短
  - 毎月アップデートする（できる）システム
  - 仕様変更に長期間かかるシステム

システム移行に時間がかかるのであれば、早めに準備しないといけない

- データの保護期間の長短
  - 使い捨て / 1週間 / 10年間 / 永年保管

データを永年保管するのであれば、保管期間中に量子コンピュータによる暗号解読は実現するとも考えられる

脅威と対策

対策ツール(スケーラビリティ順)

- **削除・匿名化**
  - 情報を保管しない or 漏洩しても問題ないように加工
- **耐量子計算機暗号（PQC）の利用：詳細は菅野さん**
  - **守る側が既存コンピュータのみを利用し、攻める側は量子コンピュータも使う想定**
  - **PQCの利用は、最も一般的な解決策**
  - **脅威モデルは既存のものを流用できる：(暗号回りの仕組みだけ変更し、運用等の変更は最低限にするアプローチを取れる)**
  - **スケーラビリティで優位 （スケールさせる場合のコスト倍率は、既存暗号と同程度）**
- **長期署名（又はカウンター署名）**
  - 署名用途と相性が良い（インターネットで広く使われているのは、秘匿用途と認証用途なので…）
  - 既存の署名に、再度署名を行えるようにする
  - 量子コンピュータが出てきそうになったら、PQC署名を付与する（より長い猶予期間が確保できる）
  - データ構造等の変更が必要
- **公開鍵暗号を用いない、鍵配布（や鍵合意）手段を導入**
  - 公開鍵暗号の利用を廃止するアプローチ
  - 暗号鍵を配布する手段を別途確保する必要がある（人による運搬、ICカードを全員に配る、QKD（量子鍵配送）など）
  - スケーラビリティが低い
  - 匿名通信や、プライバシ保護に関して、再設計が必要になるかも？（IDのトラッキングが容易になるかもしれない）
- **物理アクセス制御**
  - 他の対策が取れないが、それでも保護したい場合の最終手段
  - コストが非常に高い（インターネットでは使いにくい）

- （番外）全部over HTTPSにして、HTTPSのTLSをPQC対応
  - アタックサーフェスが大きく変わる。別途、内部不正対策等が必要。最後の手段その２？

対策の実施時期は？

公開鍵暗号は広く使われていて、全ての対策を一斉に実施すると破綻しそう

- 円滑なシステム更新を行うための前準備
  - プライオリティが高い情報システムの把握
    - 利用している暗号の把握
    - 脅威やリスクの評価
  - 迅速に対応ができるような体制の整備
    - クリプトグラフィック・アジリティ
    - 実装や運用面での、受け入れ態勢の整備

優先度の異なるケース（例）

優先度が低めなケース（例）

- ごく短期間しか使わないシステム（１年しか使わないシステムなど）
- 猶予期間が長いもの（すなわち、システムの移行期間が短く、データ保護期間も短いもの）
- 攻撃が成功しても、影響が少ないもの

- 例えば…
  - ソフトウェア実装されており、
  - 迅速なファームウェアアップデートが可能であり、
  - ピュアな認証用途であり、せいぜい1週間くらいしか使わない

優先度の高いケース1：TLSの鍵共有

- TLS通信のコンテンツに様々な情報が含まれる
  - 保管期間が長いものもあれば、短いものもある
- 「耐量子性が必要なコンテンツ」のみ、異なる制御を行うことは容易ではない
- 全てのペイロードに対し、耐量子性を持たせるアプローチの方が良さそう（鍵共有部分※）

※認証に使う情報の有効期間は大概短く、プライオリティは低め

優先度の高いケース2：コード署名

- ファームウェアのコード署名のライフサイクルは、非常に長いことも多い
- ファームウェアのコード署名は、入れ替えが困難なことも多い
  - 情報システムで利用されるハードウェアの中には、容易に入れ替えできないものが存在する
  - それらのハードウェアに対応するソフトウェアの中にも、容易に入れ替えられないものが存在する

- ファームウェアに対するコード署名は、優先して検討することが望ましい

本日のお話、ふりかえり

- 量子コンピュータによる暗号解読に備える手段は複数ある
- インターネットにおける対策は、
  耐量子計算機暗号（PQC）が主要な役割を果たす見通し
- 早めの準備が必要なケースもある

最後に

インターネット業界は何か考えたほうが良い？

インターネットのスケーラビリティは、公開鍵暗号によるものが大きい

スケーラビリティ維持のためにも、
PQC移行の必要性と実現性は意識した方が良さそう

その他の資料

特集 12.

耐量子計算機暗号への移行へ向けた課題と社会実装への論点整理

Issues for the Transition to Post-quantum Cryptography

伊藤忠彦

abstract

現代社会においては，多様な情報が様々な暗号技術により保護されている．それらの暗号技術の中には，将来の量子コンピュータによって解読が可能とされる暗号，すなわち量子耐性を持たない暗号も存在する．そのような暗号技術は，暗号解読可能な量子コンピュータの登場前に，量子耐性を持つ暗号技術へ移行することが望まれる．一方で，一般に暗号アルゴリズムの移行には，時間や費用面で高いコストが要求される．特に量子耐性を持つ暗号への移行は，かつてない規模となることが想定され，入念な準備を整えた上で計画的に行うことが望まれる．本稿では，それらの暗号技術への移行を効果的に行う上での課題，及び移行を助ける仕組みについて考察する．

キーワード：耐量子計算機暗号，暗号アルゴリズム移行，データガバナンス

1. は じ め に

現代社会において，公開鍵暗号は様々な情報を保護するために利用されており，今後もより多様な用途に利用されることが期待されている[1]．一方で，将来，一定以上の能力を持つ量子コンピュータが登場した場合には，既存の公開鍵暗号が解読される（破られる）という脅威が指摘されている[2]-[6]．

量子コンピュータによる暗号解読の脅威への対応は幾つか考えられるが，最も汎用的かつ根本的な対応は，既存の公開鍵暗号アルゴリズムを耐量子計算機暗号アルゴリズム[7]に置き換える，すなわち耐量子計算機暗号へ移行することである．しかしながら，少なくとも耐量子計算機暗号への移行は，実装をシンプルに切り替えただけでは完了しない．運用やデータ管理に係る様々な処理も併せて移行する必要がある．加えて，社会には多様な暗号技術が広く普及している．それら全ての公開鍵暗号を耐量子計算機暗号へ移行するには，極めて長い期間と労力を要することが想定され，現実的なコストで実現できる確証もない．

本稿では，上記のような実情を踏まえ，現在，標準化業界を中心に関心が寄せられている課題について，現状把握，インフラ移行，データ管理及びプライオリティ設定の四つの視点で整理する．また，量子コンピュータによる暗号解読に効果的に備えるための考慮点等についても考察する．

2. 現状把握における課題

本章では，現状把握における諸課題を考察する．

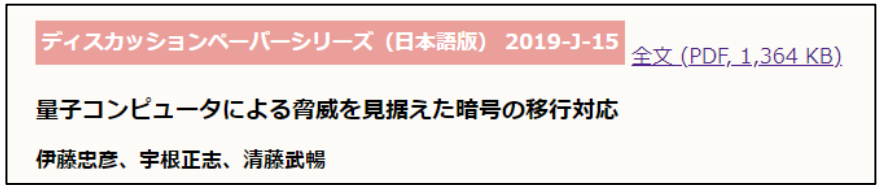
課題 1-1 量子コンピュータによる暗号解読の実現時期を予想することが困難

現在広く利用されている公開鍵暗号が，量子コンピュータによる攻撃に起因して，近い将来に危殆化する可能性は低い[2]と考えられている．

一方で，Michele Mosca[8]が指摘するように，暗号処

伊藤忠彦　セコム株式会社 IS 研究所
E-mail tadahi-ito@secom.co.jp
Tadahiko ITO, Nonmember (Intelligent Systems Laboratory, SECOM CO., LTD, Tokyo, 181-8528 Japan).
電子情報通信学会誌 Vol.106 No.11 pp.1026-1030 2023 年 11 月

https://www.secom.co.jp/isl/news/2023/1115-IEICE-ito/1026-1030_IEICE_journal_November_06.pdf

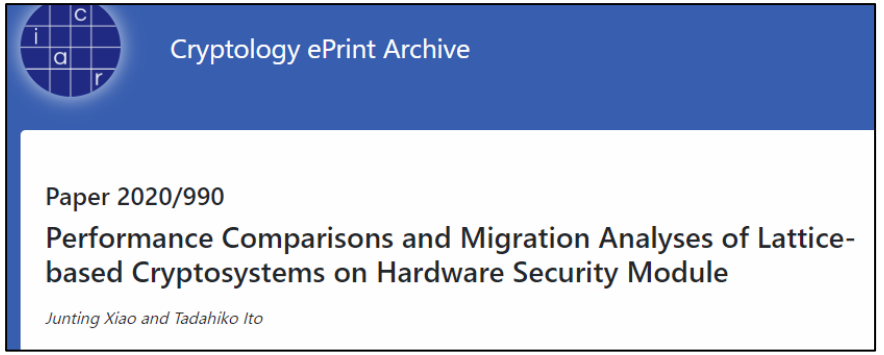


ディスカッションペーパーシリーズ（日本語版） 2019-J-15　全文 (PDF, 1,364 KB)

量子コンピュータによる脅威を見据えた暗号の移行対応

伊藤忠彦、宇根正志、清藤武暢

https://www.imes.boj.or.jp/research/papers/japanese/1



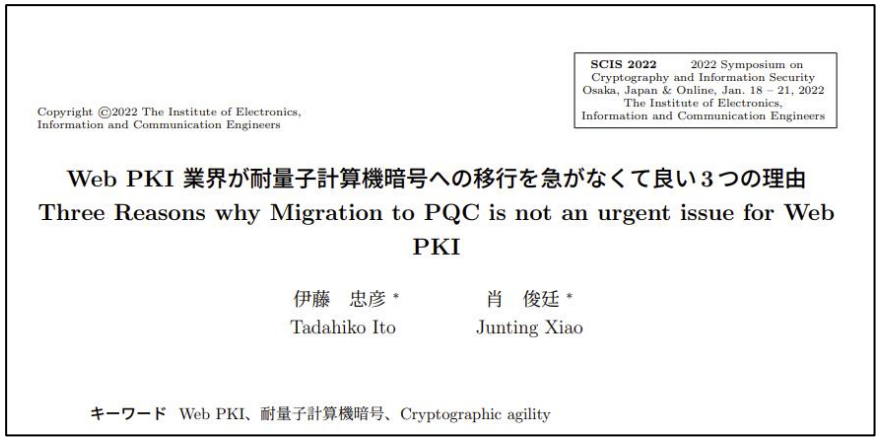
Cryptology ePrint Archive

Paper 2020/990

Performance Comparisons and Migration Analyses of Lattice-based Cryptosystems on Hardware Security Module

Junting Xiao and Tadahiko Ito

https://eprint.iacr.org/2020/990
（NIST SP 1800-38Cで引用された）



SCIS 2022　2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

Web PKI 業界が耐量子計算機暗号への移行を急がなくて良い３つの理由

Three Reasons why Migration to PQC is not an urgent issue for Web PKI

伊藤　忠彦 *　　肖　俊廷 *
Tadahiko Ito　　Junting Xiao

キーワード　Web PKI、耐量子計算機暗号、Cryptographic agility

https://www.iwsec.org/scis/2022/_abst/2A2-2.pdf