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

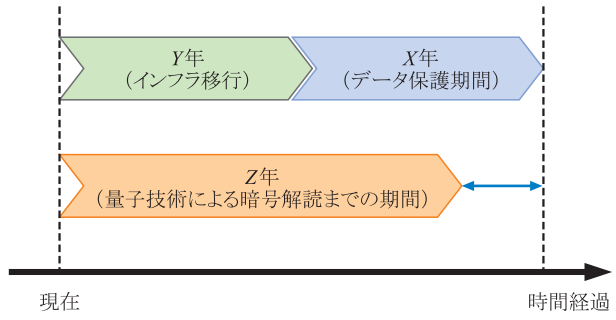

図1　インフラ移行期間とデータ保護期間を足した期間と量子コンピュータ登場までの期間の関係　Mosca の発表資料[8]を参考に作成．

理の実装の置き換えに要する期間（本稿では「インフラ移行期間」という）と，各データに対する暗号による保護が期待される期間（本稿では「データ保護期間」という）を足したものが，暗号解読可能な量子コンピュータ登場までの期間よりも長い場合は，何らかの対応が必要となる（図1）．

ここで，暗号解読可能な量子コンピュータの登場時期を高い精度で予想できるのであれば，攻撃可能時期とその時点における攻撃成功時のインパクトを踏まえて，ある程度のリスク評価が可能となる．しかしながら，革新的な技術発展が起こり得ることも考慮すると，現状においては量子技術の開発の見通しに不透明な点も多く，攻撃可能時期を推測することは困難である．そのため，リスク評価も，それに基づいた移行計画を立案することも困難となっている．

この課題への対応方針には，①耐量子計算機暗号への移行を可能な限り早期に開始する，②インフラ移行期間とデータ保護期間を短縮するような施策を行う，③量子技術の開発動向を見守る，等のアプローチを並行して行うことが効果的だと考えられる．

なお，NSA[注1]は上記①の選択を推奨しているようにうかがわれるが[3]，この選択では量子技術の進展が遅い場合や，標準化された耐量子計算機暗号にぜい弱性が発見された場合に移行に費やされる総コストが大きくなることが予想される．そのため，重要性の低い情報についても①のみを選択する場合には，総コストが非常に大きくなり得る点に留意されたい．

課題 1-2　情報システムの管理者は自らが管理する情報システムが利用する暗号アルゴリズムを把握していない

暗号技術が高度に発展した結果，情報システムの利用者のみならず管理者も，暗号技術の詳細を（場合によっては存在すらも）意識せずに暗号技術を利用することが可能となった．人々が数々の暗号技術を意図せずに利用可能であることは，暗号技術発達のすばらしい側面ではあるものの，移行を検討する上での障壁となり得る．例えば，情報システムの管理者が，移行が必要な暗号モジュールを把握することができず，移行計画の立案ができないという事態が考えられる．

この課題への対応としては，自らが管理する情報システムが利用する暗号アルゴリズムをスキャンするようなディスカバリーツール[9]や，SBOM（Software Bill of Materials）関連技術等のソフトウェアサプライチェーン管理技術を用いることが効果的であると考えられる．

課題 1-3　保護期間を長く設定し過ぎたデータが存在する．保護期間が設定されていないデータが存在する

課題 1-1 に示したように，暗号解読に関する時期の側面からの配慮が必要か否かは，インフラ移行期間とデータ保護期間に依存する．

例えば，その場限りの認証用のデータであれば，データ保護期間は非常に短くなることが想定され，移行の必要性についてはインフラ移行期間の影響が支配的となる．そのため，対策時の変数が三つから二つに減り，対策実施時の難易度が低くなることが期待される．

一方で，例えば，永久保管と指定されたデータは，量子コンピュータにより暗号解読が可能となる時期より後までデータを保護することになるものと考えられる．そのため，量子計算機の影響を検討することが必要だと考えられる．一般に，守る必要のないデータに対して非常に長い保管期間を設定する行為が組織内で常態化すれば，その組織における移行コストが更に増加する．そして，対策実施の難易度が上昇することが予想される．

上記課題は，保護期間が設定されていないデータを「永久保管」と判断する事情がある場合も発生する．

本課題に対応するためには，データのライフサイクル管理を適切に行い，データの保護期間を保護のためのコストも踏まえて適切に設定した上で，適切なタイミングでデータの消去や公開を行うことが考えられる．何をもって適切とするかは課題 3-2 となる．

3.　インフラ移行における課題

本章では，インフラ移行における諸課題を考察する．

課題 2-1　暗号アジリティの低い製品への対応

一般に，インフラ移行の対象となる情報システムが標準プロトコルを採用していること，暗号モジュールに標準プロトコルを利用していること，その API が適切に定義されていること，相互運用性が確保されているこ

（注1）　National Security Agency（アメリカ国家安全保障局）の略称．

と，及び暗号回路を含むファームウェアアップデートをオンラインで実施できることを満たしているのであれば，インフラ移行期間は比較的短くなる．一方で，それらの特徴を持たない場合は，インフラ移行期間が長くなる傾向にある．

また，関連するステークホルダ数が多いことに起因して，各ステークホルダのポリシに相互依存関係がある場合等では，その依存関係の解決に多くのステップを要し，インフラ移行期間が更に長くなることもある．

上記の課題に対応するためには，情報システムを，暗号プロトコルの変更を迅速にできる性質の高いもの，すなわち暗号アジリティの高いものにシフトさせていく施策が効果的であると考えられる．

課題 2-2　データサイズや計算量の増加

耐量子計算機暗号アルゴリズムは，暗号鍵のデータ量，ディジタル署名のデータ量，必要とする計算量のうち，少なくとも一つ以上で既存の公開鍵暗号アルゴリズムに比べて多くのリソースを消費する．

これに起因し，例えば，現状の TLS 通信[10]の Server Hello においては，ペイロードのデータ量の制限から，サーバ認証に用いる耐量子計算機暗号の証明書を単一のペイロードに格納できないという課題が指摘されている[11]．また，計算量の増加やハードウェアアクセラレーション回路の不備等に伴い，単一の Web サーバが同時に処理可能なコネクション数が減少し得る．

これらの課題に対応するためには，前者はプロトコル仕様の変更，後者はより性能の高いハードウェアへの置換え等を行うことが考えられる．プロトコル仕様の変更は，変更後のプロトコルが普及するまでに時間を要することが推測される．また，ハードウェアの置換えにおいては，仮に何らかの認定（例えば，CMVP[注2]）を受けたハードウェアの利用がポリシ上要求されており，かつ，要件を満たすハードウェアが計画時点で存在しない場合等においては，置換えに時間を要することが想定される．

課題 2-3　ディジタル署名処理から，ハッシュ処理を分離できなくなる

既存の公開鍵暗号アルゴリズムを用いたディジタル署名（すわなち，RSA[注3]や ECDSA[注4]）では，署名対象となるデータのハッシュ値を計算し，ハッシュ値を計算した「後に」ハッシュ値に対して非対称演算を行う．しかしながら，現状，NIST[注5]の候補に残っている耐量子計算機暗号では，これら二つの処理を分離してディジタル署名を実施することは容易ではない[12]．

既存の情報システムにおいては，ハッシュ演算と非対称演算は分離可能である性質を利用し，二つの計算を異なる環境で実施することも多い．特に高いセキュリティが求められる環境において，データ管理及びハッシュ計算をセキュリティ強度の比較的低い環境で行い，他方で鍵管理及び非対称演算をセキュリティ強度の比較的高い環境で行うことは，一般的な実装形態である．二つの環境を結ぶネットワークは低速のこともあるが，ハッシュ値を転送する限りにおいては，特に問題はない．

このような情報システムを対象として NIST の候補に残っている耐量子計算機暗号を実装する場合においては，今まで 2 か所で計算していたディジタル署名処理を 1 か所で計算することになり，アーキテクチャの大幅な変更を伴うことが予想される．また，例えば，今まで分離していたデータ管理と鍵管理の権限について，その分離の程度が低下し得るため，その場合はガバナンスやポリシにも影響することも考えられる．

課題 2-4　暗号プロトコルが DH 型鍵共有特有の性質に依存していることがある

昨今，TLS 等の通信プロトコルの鍵共有では，RSA 暗号等による暗号化ではなく，DH[注6]を用いた鍵交換を用いることが望ましいとされている．現行の“TLS 暗号設定ガイドライン”[13]においても，「鍵交換では Perfect Forward Secrecy の特性を持つ ECDHE[注7]や DHE[注8]を更に強く推奨」しており，それら DH 型の鍵共有は広く利用されている．

しかしながら，DH 鍵共有部分を，NIST の候補に残っている耐量子計算機暗号（暗号化用途）で実装する場合には，暗号モジュールに収まらない変更が必要になる可能性がある．

例えば，DH を用いたプロトコルの通信遅延が増加することが考えられ，DH を利用した Authenticated Key Exchange の実装が 0.5RTT（Round-Trip Time）で実現可能であることに対して，KEM[注9]を利用した Authenticated Key Exchange には 1 RTT を要するものしか提案されていないとの指摘[11]が存在する．

なお，変更のアプローチによっては，ポリシの変更や追加の機能を必要とする可能性もある．

（注 2）　Cryptographic Module Validation Program（暗号モジュール試験及び認証制度）の略称．
（注 3）　Rivest, Shamir, Adleman の頭文字から命名された公開鍵暗号．
（注 4）　Elliptic Curve Digital Signature Algorithm（だ円曲線ディジタル署名アルゴリズム）の略称．
（注 5）　National Institute of Standards and Technology（米国国立標準技術研究所）の略称．
（注 6）　Diffie, Hellman の頭文字から命名された公開鍵暗号．
（注 7）　Elliptic Curve Diffie-Hellman Ephemeral（Ephemeral（鍵を使い捨てる）だ円曲線 DH）の略称．
（注 8）　Diffie-Hellman Ephemeral（Ephemeral（鍵を使い捨てる）DH）の略称．
（注 9）　Key Encapsulation Mechanisms（鍵カプセル化メカニズム）の略称．

課題 2-5　暗号鍵の状態管理（使用回数制限等）

幾つかの耐量子計算機暗号アルゴリズムには，暗号鍵の使用回数に制約があり，アプリケーションによってはその回数を超過することが起こり得る．暗号鍵の使用回数に制限のない既存情報システムの暗号モジュールを，使用回数に上限のある耐量子計算機暗号アルゴリズムに置き換える場合，幾つかの問題が発生し得る．

例えば，オンプレミスの HSM[注10]を利用している場合においては，利用者は鍵の使用回数を把握するオペレーションを追加する必要があることが考えられる．

また，LMS[注11]のように状態を記憶する必要があるアルゴリズムを HSM で運用する場合においては，実環境サービスで運用中の HSM と，バックアップシステムに存在する HSM で状態を何らかの手段で同期する必要があるところ，運用中の HSM とバックアップシステムの HSM との通信回数が大きく上昇する可能性がある．バックアップシステムの中には非常に厳密に隔離された環境に保管され，相当程度の危機にのみ使用されることが想定されたものもあり，仮にそのようなシステムに（場合によっては頻繁な）同期処理を導入するのであれば様々な注意が必要となる．

課題 2-6　知財のクリアランス

NIST は耐量子計算機暗号アルゴリズムの標準化に際し，その暗号アルゴリズムの利用に関連する知財の調査及びそれらの知財が耐量子計算機暗号アルゴリズムの利用を妨げないことの確認を行っている．そのため，少なくとも米国内においては，耐量子計算機暗号アルゴリズムの実装者が，予期せぬ知財侵害を行うおそれは低いものと考えられる．

一方で，米国以外の知財については，NIST の調査能力にも限界があると思われる．例えば，複数国に対してサービスを提供するような事業者では，耐量子計算機暗号アルゴリズムの利用に際し，追加の調査を実施することが考えられる．

課題 2-7　ポリシ移行

暗号移行において，旧システムから新システムへの過渡期においては，新旧双方のシステムを並列して運用することは一般的な試みである．しかしながら，新システムと旧システムの出力が異なる場合に，どのように対応するかという点に課題が存在する．

例えば，一つのコンテンツに既存アルゴリズムと耐量子計算機暗号アルゴリズムの 2 種類のディジタル署名が付与されているケースを考える．その場合において，それぞれのディジタル署名の検証結果が異なる場合，つまり片方は正当なディジタル署名として受け入れられ，もう一方は拒否される場合にどのように処理するのかは，状況によって異なると考えられる．具体的には，二つとも正当なディジタル署名である場合以外は受け入れないという判断もあり得る一方で，片方だけでも正当なディジタル署名であれば受け入れるという判断もあり得る．古いアルゴリズムは危殆化の影響を強く受けるため，新しい耐量子計算機暗号アルゴリズムのディジタル署名を優先するという判断もあり得る一方で，耐量子計算機暗号は歴史が新しく十分評価されていないため，既存アルゴリズムのディジタル署名を優先するという判断もあり得る．これらのうちどの判断を採用するかは，関連技術の開発動向等に依存することになり，既存の情報システム設計では可能であった設計時にあらかじめ選択することが困難となることが予想される．上記のような事情から，耐量子計算機暗号のディジタル署名を利用する情報システムでは，署名検証を行う上でのポリシ（上記の例でいえば，どの判断を優先するか）を，社会動向に合わせて動的に切り替え，移行していくことも視野に設計を行うことが有効だと考えられる．

なお，想定される検証者に含まれるステークホルダが増加するほど，署名検証ポリシを動的に切り替えることが難しくなり，ポリシ移行の困難性も上昇する．

4. データ管理に関する課題

本章では，データ管理に関する諸課題を考察する．

課題 3-1　暗号で保護されたデータの価値を評価する必要がある

本稿の冒頭で述べたように，社会に広く普及する公開鍵暗号を，全て耐量子計算機暗号へ移行するには，極めて長い期間及び労力を要することが想定される．そのような状況においては，プライオリティを設定した上で順次対策を行うことが必要となる．プライオリティを設定する上で特に有用であろう情報には，保護対象のデータの価値と，データの保管期間が挙げられる．データの価値は，社会の変化や時間経過に伴って上下し得るが，適切なデータの類型化が行われていれば，価値を適時かつ効果的に評価可能となることが期待できる．一方で，保護対象となるデータの類型化が行われていない場合には，データ漏えい時の影響試算等が困難であり，プライオリティ設定も困難となる．

なお，データ類型化はガバナンスを強化する上で非常に重要な要素であり，ゼロトラストネットワークを適切に運用する上での重要性も指摘されている[14]．そのため，データの類型化に予算を割くことは，耐量子という

（注 10）　Hardware Security Module の略称．暗号鍵の管理及び暗号処理を提供する物理機器．
（注 11）　Leighton-Micali Signature の略称．ハッシュ関数に基づくディジタル署名方式．

文脈以外の効果も期待される．

課題 3-2　データのライフサイクル管理の不備

各データに対し，適切なライフサイクル管理を行い，適切なタイミングでデータ消去，データ公開，または匿名処理を行った上での保管等を行い，暗号による保護を打ち切ることは，非常に重要である．適切なライフサイクル管理が行われたデータであれば，現実的なコストでの暗号移行の実現も期待できる．

一方で，課題 1-3 でも述べたように，守る必要のないデータに対して非常に長い保管期間を設定する行為が組織内で常態化すれば，その組織における移行コストが大きく増加する．そのため，データのライフサイクル管理が適切に行われていない場合は，耐量子計算機暗号へ移行する上での大きな課題となり得る．

5. プライオリティ設定の課題

本章では，プライオリティ設定について考察する．

課題 4　プライオリティ設定

本稿で繰り返し述べたように，社会に広く普及する公開鍵暗号を全て耐量子計算機暗号へ移行するには，極めて長い期間及び労力を要することが予測される．そのような状況において効果的に対応を行うには，プライオリティ設定は必須と言える．一方で，プライオリティ設定を適切に行うためには，様々な専門的な知識が必要となる．

例えば，データの保護期間が極めて短い認証用途のデータのみを使用するシステムにおいては，暗号アジリティを高める施策（課題 2-1 に対応）を行いつつ，量子コンピュータの開発動向を確認するのみで足りる場合があり得る．一方で，価値のある情報を長期間保護する必要が認められる場合には，データの類型化を優先した上で，保護期間の長いデータから対応するという判断が適切となる場合があり得る．

また，本稿で示した解決策の中には，耐量子計算機暗号の標準化や実装を待たないと実施できないものもあれば，今からすぐに実施できるデータの類型化等の施策もある．そのため，プライオリティ設定においては，開始可能な時期も考慮に入れることが望ましい．

6. お　わ　り　に

耐量子計算機暗号への移行は，長い期間及び労力を要する息の長い活動になることが予想される．現状において量子関連技術の発展の見通しは明確ではなく，対策も不確実要素の上で行わざるを得ない．そのような状況で費用と効果のバランスを検討するのは多くの困難が伴う．しかしながら，暗号移行を効率的に行う準備を怠ってはならないはずである．具体的には，学術界においては，量子計算機の開発動向の把握や，安全かつより効率的にデータの保護が可能となる技術の研究が考えられる．産業界においては，自らが管理する情報システムの現状態を日常的に把握して移行のプライオリティを設定し，その上で暗号アルゴリズムの移行準備やデータのガバナンス強化を行うことが推奨される．本稿がそのような活動を行う一助になることを期待する．

文　　献

（1） 伊藤忠彦，国井裕樹，“暗号鍵管理によるデータ保護効率の観点から見たトラストや暗号技術の発展とこれから，”2023 年暗号と情報セキュリティシンポジウム，no. 2B4-3, Jan. 2023.
（2） CRYPTREC, 注意喚起情報，“現在の量子コンピュータによる暗号技術の安全性への影響，”CRYPTREC ER-0001-2019, 2020.
（3） National Security Agency, “Announcing the commercial national security algorithm suite 2.0,” U/OO/194427-22, 2022.
（4） M. Pecen, “Chairman’s report for 2018 : ETSI cyber working group for quantum safe cryptography,” presentation at ETSI/IQC Quantum Safe Workshop, European Telecommunications Standards Institute, 2018.
（5） 伊藤忠彦，“量子コンピュータの公開鍵基盤に与える影響と対策，”2018 年暗号と情報セキュリティシンポジウム，no. 3A3-6, Jan. 2018.
（6） 伊藤忠彦，宇根正志，清藤武暢，“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，”日本銀行金融研究所ディスカッションペーパーシリーズ，2019-J-15, Aug. 2019.
（7） NIST, “Report on post-quantum cryptography,” NISTIR 8105, 2016.
（8） M. Mosca, “Cybersecurity in a quantum world : will we be ready? workshop on cybersecurity in a post-quantum world,” April 2015. https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf
（9） NIST NCCoE, “Migration to post-quantum cryptography : preparation for considering the implementation and adoption of quantum safe cryptography,” NIST SP1800-38A, 2023.
（10） E. Rescorla, “The transport layer security（TLS）protocol version 1.3,” IETF RFC 8446, 2018.
（11） M. Ounsworth, “PQC at the internet engineering task force（IETF）,” Post-Quantum Cryptography Conference, Ottawa, Canada, March 2023.
（12） J. Xiao and T. Ito, “Performance comparisons and migration analyses of lattice-based cryptosystems on hardware security module,” Cryptology ePrint Archive, Paper 2020/990, Jan. 2021（revised）.
（13） CRYPTREC, “TLS 暗号設定ガイドライン，”CRYPTREC GL-3001-3.0.1, 2020.
（14） NIST NCCoE, “Implementing data classification practices,” NIST SP 1800-39A, 2023.

（2023 年 6 月 1 日受付　2023 年 6 月 16 日最終受付）

伊藤（いとう）　忠彦（ただひこ）

平 17 筑波大大学院理工学研究科修士課程了，平 24 同大学院システム情報工学研究科単位満了退学．同年セコム株式会社入社．以来，ルート認証局及び暗号鍵管理の研究・ポリシ管理・標準化に従事．現在，同社 IS 研究所主務研究員．CRYPTREC 暗号技術調査 WG（耐量子計算機暗号）委員．IETF RFC 8813, IETF RFC 9295, IETF RFC 9336 等執筆．