ExpertInsights@IBV

両刃の剣を振りかざす

直ちに量子世界のサイバー・セキュリティーに備えよ

IBM Institute for Business Value

提言

大規模量子コンピューターは、計算能力の大幅な拡大により、サイバー・セキュリティー強化の新たな可能性を開くだろう。量子時代のサイバー・セキュリティーでは、損害が発生する前にサイバー攻撃を検出・回避することが可能となる。一方、量子コンピューティングは、両刃の剣のように大きな被害ももたらしかねない。例えば、難解な数学的問題を迅速に解決できるようになれば、一部の暗号化方式がいともたやすく破られるといった新たなリスクも生じる。ポスト量子暗号の標準化はまだ検討の最終段階にあり、企業やその他の団体は、すぐにでも準備を開始すべきである。

量子コンピューティングの時代へ

量子力学とは、物質世界の根本的な仕組みを追究する物理学の一分野である。ミクロな量子の世界では、粒子は同時に 2 つ以上の状態を取ることができ、たとえ空間的に遠く離れていても、相関関係を持つことができる。量子コンピューティングは、このような量子現象を活用した、全く新しい情報処理を可能にする。[1] 量子コンピューティングの世界市場規模は、2024 年までに 100 億米ドルを超えると予測されている。[2]

今日の古典的コンピューターによる暗号化では、主に「共通鍵」と「公開鍵」という 2 つの暗号方式のアルゴリズムが使用されている。共通鍵暗号方式では、データの暗号化と復号化に同じ鍵を使用する。米国政府によって採用されている AES（Advanced Encryption Standard）アルゴリズムは、共通鍵暗号アルゴリズムの一例であり、128 ビット、192 ビット、および 256 ビットの 3 つの鍵長に対応している。3 共通鍵暗号アルゴリズムは、大規模なデータベースやファイル・システム、オブジェクト・ストレージなど、バルク暗号化のタスクによく利用されている。

一方、公開鍵暗号方式では、一般的に公開鍵と呼ばれる 1 つの鍵でデータを暗号化し、秘密鍵と呼ばれる別の鍵で復号化を行う。公開鍵と秘密鍵は異なる鍵ではあるが、数学的な関連性を持っている。幅広く使用されている Rivest-Shamir-Adleman（RSA）アルゴリズムは、公開鍵暗号アルゴリズムの一例である。公開鍵暗号方式は、共通鍵暗号方式よりも処理に時間がかかる一方、暗号化における重要な課題の 1 つである鍵配送問題を解決できる。

量子コンピューティングによる計算方法

量子コンピューターは、古典的コンピューターで使用されている 2 進数のビット（0 と 1）の代わりに、極めて複雑なスイッチである量子ビットを使用する。量子ビットにより処理能力が大幅に強化された量子コンピューターには、今までのコンピューターでは「手に負えない」問題を解決する可能性があると期待されている。[4] 2 量子ビットでは、4 つの値を同時に表すことができ、3 量子ビットでは 2^3、つまり 8 つの値を、50 量子ビットでは 1,000 兆以上の値を、また 100 量子ビットでは 1,000 兆の 2 乗以上の値を同時に表すことができる。[5]

サイバー・セキュリティーにおいて「量子」がもたらすリスク

暗号化の将来

DES と呼ばれる初の相互運用可能なデータ暗号化標準規格と、幅広く使用されている HMAC 規格が、今日におけるほとんどのデータ認証スキームの基礎となっている。**量子時代に向けて**、現在および将来の脅威からシステムを守る新しい暗号化アルゴリズムが、IBM を含む複数の企業によって開発されつつある。一例を挙げるならば、新世代の格子暗号技術により、量子コンピューターと古典的コンピューター双方からの攻撃に対応可能なセキュリティーの実現が研究されている。もう1つの例としては、「完全準同型暗号」がある。この暗号技術では、暗号化データの演算を機密性を保持した状態で、制約なしに実行することが可能となる。

量子コンピューティングの到来は、暗号化方式に大きな変化をもたらすだろう。現在、最も幅広く使用されている公開鍵暗号アルゴリズムは、大きな数の素因数分解といった難解な数学的問題がベースとなっているが、このような問題は今日最も強力なスーパーコンピューターをもってしても、解決には数千年かかると見込まれている。しかし、Peter Shor（ピーター・ショア）が MIT で 20 年以上前に実施した研究によると、大規模量子コンピューターを使用すれば、同じ問題を理論上は数日や数時間で解決できることが証明されている。[6] つまり、将来の量子コンピューターは、整数の素因数分解や離散対数をセキュリティーのベースとする公開鍵暗号化ソリューションを無効化してしまう恐れがあるということだ。

一方で、共通鍵アルゴリズムはショアのアルゴリズムによる影響を受けないが、量子コンピューティングの処理能力に対抗するには、鍵長を長くする必要がある。例えば、量子コンピューティングで探索を行うための代表的アルゴリズム、グローバーのアルゴリズムを実行する大規模量子コンピューターで、量子の概念を使用してデータベースを高速検索すれば、AES などの共通鍵暗号化アルゴリズムに対する総当たり攻撃の能力が加速度的に増長してしまう可能性がある。[7] その総当たり攻撃に対抗して、同じレベルの保護能力を実現するには、鍵長を 2 倍にしなければならない。つまり、AES の場合、今日の 128 ビットのセキュリティー強度を維持するためには、256 ビットの鍵を使用する必要があるということである。[8]

大規模量子コンピューターはまだ商用化されていないものの、量子サイバー・セキュリティー・ソリューションを今すぐ準備しておくことで、有利な立場に立つことができる。例えば、何らかの悪意ある集団に、現段階で主要なセキュア通信を捕捉されてしまったとする。そして、大規模量子コンピューターが入手可能になった段階で、その圧倒的な計算能力を利用して暗号が破られれば、通信内容が筒抜けになってしまうからだ。

量子サイバー・セキュリティーの驚くべき力

量子サイバー・セキュリティーは、潜在的なリスクを減らし、重要なデータや個人情報を守ることができる、今までにない堅牢性と魅力を兼ね備えている。特に量子機械学習と量子乱数生成の分野における有用性が高い。

機械学習においては、すでに以下のような多くのサイバー・セキュリティー用途に活用されている。

- **挙動異常検出**：新しいデバイスや場所からのアクセス、通常時以外の時間帯からのアクセスなど、異常アクティビティーの検出
- **分類**：データ、ユーザー、脅威となる主体（脅威アクター）、マルウェアなどのエンティティーの分類
- **予測**：ネットワークやデータベースの脅威といったイベントの予測

量子コンピューティングにより、機械学習が高速化されれば、サイバー・セキュリティーの有効性を強化できる。例えば、量子によって強化された機械学習を活用することで、膨大なデータの分類を高速化できる。

量子乱数生成：乱数生成は暗号化に不可欠である。旧来の乱数生成における2つの主なカテゴリーとして、疑似乱数生成器（PRNG）と真性乱数生成器（TRNG）がある。

量子乱数生成器（QRNG）は、特殊な TRNG と見なすことができ、データは量子イベントを通じて作り出される。ただし、従来の TRNG が、古典物理学に基づいてある種の決定論をはらんでいるのに対し、QRNG は、量子物理学の「本質的に無作為」という特性に基づいて真の乱数を実現している。真の乱数では、生成する数は予測不能になるため、最高レベルのセキュリティーを実現することができる。

乱数の生成

PRNG と TRNG の違いを説明する 1 つの方法として、ルーレット盤を回すところを想像するとよいかもしれない。PRNG では、まずルーレット盤を何度も回し、その結果から乱数列を作成して、乱数を生成する。つまり、PRNG で乱数が必要になった場合は、乱数列の次の数字が提供されるので、乱数は前もって確定していると言える。他方、TRNG では、乱数が必要になるたびにルーレット盤が回されるので、確定した乱数列は存在しない。[9]

最初に実行すべきこと

移行をスムーズに行うためのレシピ

サイバー・セキュリティーの世界では、量子コンピューターによって現在の暗号は、最終的には破られてしまうという憶測が飛び交っている。先見の明のある企業であれば、それが現実になる前に、古典的コンピューターと量子コンピューター双方の攻撃から身を守るためのサイバー・セキュリティー・ソリューションを導入し、量子時代へのスムーズな移行に備えるべきであろう。

ポスト量子暗号の時代に備えて、企業のリーダーは、今から以下の 4 つのステップを検討すべきである。

1. 必要な量子サイバー・セキュリティーのスキル特定、および人材の再トレーニングや採用を、直接または自社のエコシステムを通じて行う。これら専門家が、自社のサイバー・セキュリティー推進者となって、標準化団体との協業やさまざまな量子サイバー・セキュリティー・アプローチの可能性の模索、自社の量子セキュリティー移行計画の策定などを実施する。
2. 自社内のどの領域でポスト量子セキュリティーの方法論を導入するべきかを特定する。具体的には、量子時代の潜在的なセキュリティー・リスクを以下の観点から評価する。
   - **共通鍵暗号化アルゴリズム**：量子時代においても、引き続き共通鍵暗号アルゴリズムが適切であると考えられる分野では、少なくとも鍵長を現在の 2 倍にすることで、適切なセキュリティー・レベルの強度を保ち、将来の脅威に対応できるようにする。[10]
   - **公開鍵暗号化アルゴリズム**：公開鍵暗号アルゴリズムが現在使用されている分野を特定し、ポスト量子の代替策に切り替えることを計画する。
   - **ハッシング・アルゴリズム**：現在使用されているハッシュ値の出力サイズを評価し、より大きな出力サイズを用いることを計画する。
3. ポスト量子のサイバー・セキュリティー標準の進化や、新しいポスト量子セキュリティー・ソリューション（特に、格子ベースのアプローチ、コード・ベース暗号、多変数暗号、ハッシュ・ベース暗号など）について、常に最新情報を入手する。
4. 暗号化ソリューション・プロバイダーの協力を得て、量子時代に対応した安全な代替策が利用可能となり次第、速やかに展開する。

注釈および出典

1 “What is quantum computing?” IBM. https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/

2 “Quantum Computing Technologies & Global Market, 2017-2024 Volume 1.” Homeland Security Research Corp. 2017.

3 “Cryptographic algorithm and key length.” IBM. https://www.ibm.com/support/knowledgecenter/en/SSWPVP_3.0.0/com.ibm.sklm.doc/overview/cpt/cpt_ic_oview_tech_cryptographic_algorithm.html

4 How do quantum computers work? https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/

5 Pednault, Edwin. “Quantum Computing: Breaking Through the 49 Qubit Simulation Barrier.” IBM. October 17, 2017. https://www.ibm.com/blogs/research/2017/10/quantum-computing-barrier/

6 Nordstrom, Amy. “Quantum Computer Comes Closer to Cracking RSA Encryption.” IEEE Spectrum. March 3, 2016. https://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment

7 “Quantum Computing Now Has a Powerful Search Tool.” MIT Technology Review. April 5, 2017. https://www.technologyreview.com/s/604068/quantum-computing-now-has-a-powerful-search-tool/

8 Chang, Linus. “How secure is today’s encryption against quantum computers?” betanews. October 13, 2017. https://betanews.com/2017/10/13/current-encryption-vs-quantum-computers/

9 Haahr, Mads, Dr. “Introduction to Randomness and Random Numbers.” Random.org. https://www.random.org/randomness/

10 “IBM Multi-Cloud Data Encryption.” IBM. https://www.ibm.com/us-en/marketplace/cloud-data-encryption

ExpertInsights@IBV レポートについて

ExpertInsights@IBV レポートは、ニュース価値の高いビジネスや関連テクノロジーのトピックについて専門家の意見を伝えるレポートです。該当分野の専門家へのインタビューに基づいて作成し、その洞察を刺激的、実践的、包括的な視点にまとめています。詳細については、IBM Institute for Business Value（iibv@us.ibm.com）までお問い合わせください。

専門家

Walid Rjaibi

IBM ディスティングイッシュト・エンジニア兼データ・セキュリティー担当最高技術責任者
IBM Security
https://www.linkedin.com/in/walid-rjaibi-cissp-8325077/
wrjaibi@ca.ibm.com

Sridhar Muppidi

IBM フェロー、バイス・プレジデント兼最高技術責任者
IBM Security
https://www.linkedin.com/in/smuppidi/
muppidi@us.ibm.com

Mary O’Brien

開発担当バイス・プレジデント
IBM Security
https://www.linkedin.com/in/mary-o-brien-4946a590/
obrienma@ie.ibm.com

日本語翻訳監修

橋本光弘

日本アイ・ビー・エム株式会社 戦略コンサルティング & デザイン統括 マネージング・コンサルタント
IBM Q Ambassador
日本学術振興会特別研究員（DC1）、国内大手電機メーカー研究員（中央研究所、米国研究所他）としてストレージ・デバイスの研究開発に従事。その後、米系戦略コンサルティング・ファームおよび IBM にて、電機・機械・エネルギー・金融業界のコンサルティング・プロジェクトに参画。専門領域は全社戦略（中期経営計画、ポートフォリオ戦略、シナリオ・プランニング）、新規事業戦略、M&A（ビジネス・デューデリジェンス、PMI）、オペレーション改革、組織再編。近年は特に IoT・AI・ブロックチェーン等のテクノロジーを活用した新規事業戦略策定やオペレーション改革をテーマにしたプロジェクトを多数手掛けている。博士（工学）。
連絡先：hashimit@jp.ibm.com

西林泰如

日本アイ・ビー・エム株式会社 戦略コンサルティング & デザイン統括 シニア・マネージング・コンサルタント
IBM Q Ambassador
総合電機メーカー、米系戦略コンサルティング・ファームを経て、IBM に参画。専門はビジネス・テクノロジー両輪に関する、経営企画・経営戦略、事業開発・事業戦略、提携・投資 /M&A、海外進出（米国シリコンバレー、シンガポール等での海外駐在経験）、情報通信・インターネット技術（日米 120 件超の特許の筆頭発明者）。IBM では、Global Digital Strategy Group に所属。IBM がリードする破壊的テクノロジーによる革新をテーマに、経営戦略・事業戦略、デジタル戦略、オペレーション戦略、組織チェンジ・マネージメント、テクノロジー・データ戦略の戦略業務に従事している。工学修士（MEng）、および経営管理修士（MBA）。
連絡先：yasuyuki.nishibayashi@ibm.com

New Orchard Road
Armonk, NY 10504
Produced in the United States of America
July 2018

本書は英語版「Wielding a double-edged sword - Preparing cybersecurity now for a quantum world」の日本語訳として提供されるものです。

39017839JPJA-00