

未来の保証:

耐量子セキュリティへの取り組み

Vanguard レポート

2022年4月

委託元:



451 Research

S&P Global
Market Intelligence

©Copyright 2022 S&P Global Market Intelligence. All Rights Reserved.

著者について



ジョン・アボット氏

4SIGHT社、プリンシパル・リサーチ・アナリスト

ジョン・アボット氏は、S&P Global Market Intelligenceの一部である451 Researchでシステム、ストレージ、ソフトウェア・インフラストラクチャーを担当しています。30年以上ものキャリアを積んできた彼は、Unix、スーパーコンピューティング、システム・アーキテクチャー、ソフトウェア開発、ストレージなどの分野での専門技術を取り上げる先駆けとなっています。

そして、1999年10月にThe 451 Groupの共同創設者の一人として、同社のサンフランシスコ事務所でアナリスト業務に携わりました。ストレージ仮想化やブレード・サーバーに関するレポートを含む、多数の451 Research特別レポートの筆頭著者を務め、ストレージ仮想化とブレード・サーバーのいずれのテーマに関しても初めての包括的な調査内容を公開しています。最近、ジョン氏はコンバージド・インフラストラクチャー、新しいシステム・アーキテクチャー、AI、ディープ・ラーニング・アクセラレータなどのトピックに焦点を当てています。新興テクノロジーの将来を見据えた、長期的な調査対象のための451 Researchフレームワークである4SIGHTの確立に尽力しました。

また、テクニカルライターとしての経験と、メインフレーム、初期のPC、および Unixワークステーションを使用した直接的な関与に基づいて、1984年にテクノロジー部門の調査を開始しました。フリーランスのジャーナリストとして、Computing, Computer Weekly, The Financial Times, The Timesなどの出版物に寄稿してきました。1987年には、ComputerWireの週刊 UnixニュースレターUnigram.Xの編集者に任命されました。その後、最初はロンドン、続いてサンフランシスコで、同社の日次発行のComputergram Internationalサービスの編集者になりました。サンフランシスコに451 Researchオフィスを設定し、10年以上駐在しました。

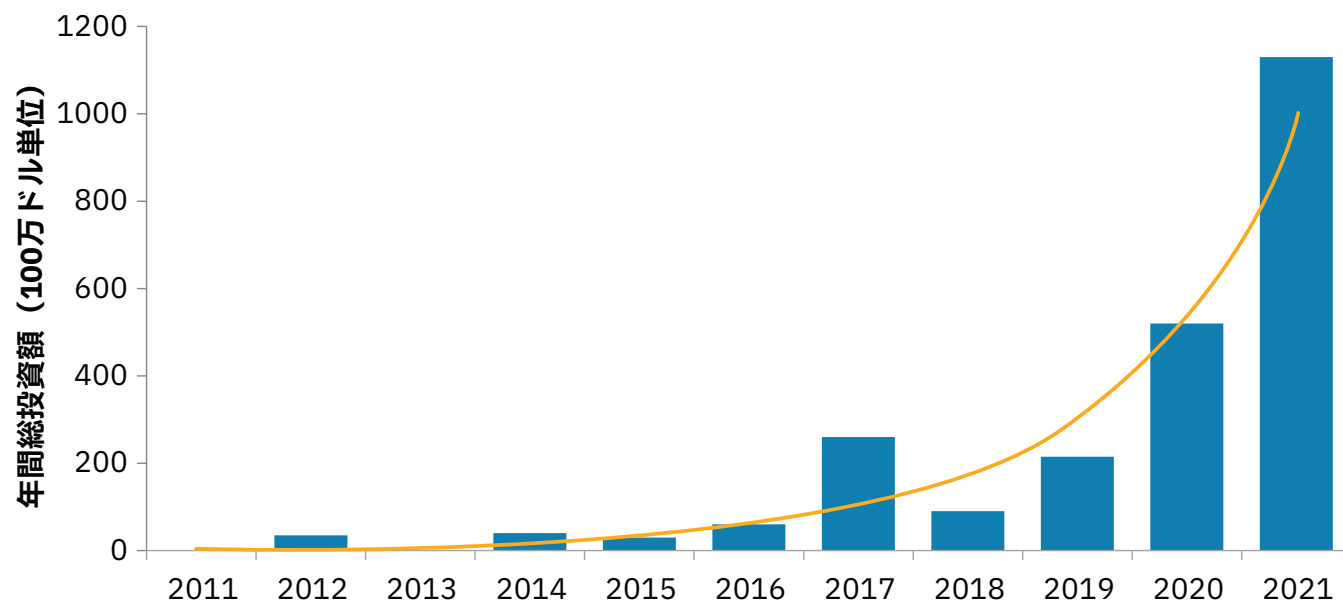
ジョン氏はキール大学で音楽を専攻し、ロンドン大学で現代英文学の修士号を取得しています。

序論

現在の量子コンピューティングは、ハイリスク・ハイリターン型の投資と言えるでしょう。私たちが生きている間に、汎用の実用的な量子コンピューターが実現するという保証はありません。一方、研究所やテクノロジーセクターの民間企業は、日々、困難を乗り越えて、最先端の科学技術の開発を続けています。成功すれば途方もなく大きな成果が期待され、従来のスーパーコンピューターの能力では対処できない問題も解決してしまう可能性があります。売り手とユーザーの両方が、破壊的な可能性を秘めたテクノロジーのチャンスに賭けているのは、これが理由でしょう。S&P Capital IQ Proのデータ(図1)は、量子分野を手がけるスタートアップ企業が、過去10年間で24億ドルの投資を獲得したことを示しています。2021年には、量子関連企業へ11億ドルの資金が投入されるなど、大きな関心が寄せられました。そしてこのデータには、IBM, Amazon, Google, Honeywellなどの世界有数のIT企業による大規模な投資は含まれていません。

このような機会とともに、大きな懸念も生じます。おそらく最も差し迫っている懸念は、現在のセキュリティ慣行に対する脅威です。悪意のあるユーザーが量子コンピューティングを悪用すれば、デジタル署名を偽造して、世界のITシステムに深く組み込まれている公開キーインフラストラクチャーを含む、現在のレベルの暗号手法と暗号化を解読することができます。さらに、現在保護されている暗号化されたデータも、実用的な量子コンピューティングが登場してから解読する目的で、保存される可能性があります。これは、すぐに対処しなければならない問題です。時間がたてばたつほど、より多くのデータが作成され、リスクが大きくなります。

図1: 量子コンピューティングのスタートアップ企業への投資



出典: S&P Capital IQ Pro

451の見解

ショアのアルゴリズムを効果的に実行できる量子コンピューターが幅広く利用され、不正ユーザーがそれにアクセスできるようになる時期を正確に予測することはできません。これまでのところ、量子コンピューティングが従来のコンピューターの性能を意味ある形で超える時期について、明確なタイムラインを提示しているITベンダーはありません。ただし、過去5年間のテクノロジーの急速な進歩と、現在、多額の資金が投入されているという事実から、おそらく2020年代の終わりまでにはその時期が来ることが示唆されています。その場合、公開キーアルゴリズムによって現在保護されているすべての情報が流出するおそれがあります。政府の防衛機関や諜報機関、および規制対象の業界の顧客をもつクラウド・サービス・プロバイダーやシステム・ベンダーにとって、すでに無視できないほどリスクが高まっています。1999年から2000年に変わるときに、幅広く使用されているコンピューター・プログラミングの日付ショートカットが大混乱をもたらすと言われた2000年問題など、これまでに誤った警告もあり、将来のことは未知数であるともいえます。しかし、1つだけ明らかなことがあります。サイバー攻撃による危険性は、現在の大きな問題であり、脅威と脆弱性の性質は絶えず進化しているということです。セキュリティ・ポリシーには継続的な見直しと更新が必要であり、暗号の俊敏性や暗号インベントリーの実装に加えて、今では耐量子暗号テクノロジーが非常に重要となっています。

量子耐性および耐量子シナリオ

問題は次のとおりです。幅広く使用されている現世代のセキュリティ・アルゴリズムは、従来のコンピューターでは解けない難解な数学の問題に基づいています。しかし、これらの問題は、十分なパワーを搭載した量子コンピューターには簡単に解くことができます。これは、アメリカの数学者ピーター・ショア氏が、ショアのアルゴリズムとして現在知られている多項式時間アルゴリズムを発見した1994年以来、広く受け入れられている前提です。最初の量子コンピューターは、その3年後に構築されました。耐量子アルゴリズムの開発は、過去10年間で順調に進んでいます。一方、政府や業界全体で現在広く使用されている公開キー暗号システムから新しい一連のアルゴリズムに移行するには、数十年かかる可能性があります。

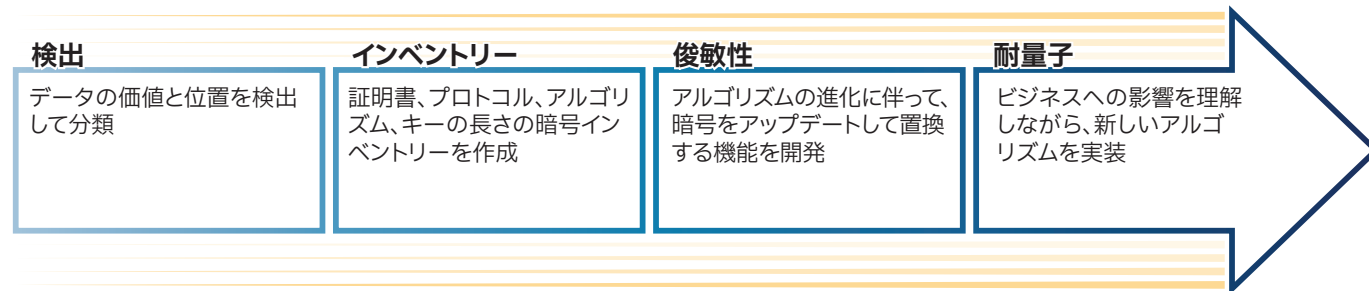
そのため、米国国立標準技術研究所 (NIST) や米国国土安全保障省などの組織は、企業のポスト量子暗号への移行を助けるために、アルゴリズム自体の標準化プロセスや、推奨事項の作成に取り組んでいます。その取り組みにより、1月にホワイトハウス覚書が作成され、政府の防衛および諜報機関に対して、移行の開始が義務付けられました。

現在利用可能な最も強力なコンピューターでも、2,048ビットの複合整数を素因数を見つけるに解読するには、数百万年かかると予測されています。量子コンピューターでは、理論上はそのタスクを数時間で完了できる可能性があります。ショアのアルゴリズムによって解読される現在の公開キーシステムには、開発から45年経過しても、ほとんどすべてのインターネットベースのトランザクションで使用されている尊敬すべきRSAアルゴリズム、ならびにデータセキュリティ標準、Paillier 暗号システム、楕円曲線デジタル署名アルゴリズム、楕円曲線Diffie-HellmanおよびElGamal 暗号化が含まれます。NIST、ISO/IEC、ETSI、およびIETFによって制定された多数の標準が影響を受けます。これは、国際的な問題であることを示しています。

中国のSM2デジタル署名アルゴリズムとSM9国家暗号化標準も解読されています。

2016年に提案を求めて開始されたNIST標準プロセスでは、量子耐性のある新しい一連の候補が特定されました。格子、多変量、ハッシュまたはコードベースの暗号化など、さまざまなアプローチにグループ化されています。これらには、格子ベースのCRYSTALS-Kyberキーカプセル化メカニズム (KEM)、McEliece (コードベースの KEM)、ならびにFalcon (格子ベース) およびRainbow (多変量) のポスト量子署名スキームが含まれます。これらを含む一連の最終候補は、現在競争が完了している第3段階の後、標準化に向けて計画が進んでいます。代替アルゴリズムと署名スキームの追加要求を含む第4段階は、今年から始まり、2024 年末までに完了する予定です。

図 2: 耐量子性への成熟のマイルストーン



出典: 451調査

耐量子暗号化への道のり

今後 10 年間で、情報セキュリティ・アーキテクチャーに耐量子暗号を組み込むための準備として、組織はどのような行動を取るべきでしょうか? すでに進行中である最初のステップは、標準化プロセスに参加することです。不正な認証の防止、暗号化の整合性の保護、デジタル署名の侵害の回避に取り組む組織は、最終的なアルゴリズム、プロセッサ、ツールの承認済みリストが、彼らの要件を満たすものになるように、積極的に参加することが重要です。標準化団体での前進がみられるとはいえ、これはまだ進行中です。より多くのアルゴリズムが必要になります。さらに、後続の成熟マイルストーンでは、耐量子性を実現していくことになります。

- **データの発見と分類:** 重要なデータのインベントリーを例にとりましょう。どれが最も価値がありますか? データはどこにありますか? どのようなコンプライアンス要件がありますか? 多くの組織は自らのデータについて、またはその価値を十分に認識していないため、それらを理解することが非常に重要です。これを理解していなければ、最も深刻な脆弱性を特定することはできません。所有権が定義されたデータインベントリーを作成して管理する必要があります。
- **暗号インベントリー:** 暗号インベントリーには、脆弱な公開キー暗号化が使用されている場所とその方法の詳細が記載されており、証明書、暗号化プロトコル、アルゴリズム、キーの長さなどの詳細が含まれています。インベントリーは、証明書と暗号化キーのライフサイクル全体に対応するように管理しなければなりません。
- **暗号の俊敏性:** 組織は、計画と移行プロセスの中で、暗号の俊敏性を考慮する必要があります。これにより、テクノロジーが進化して、状況が変化した際に、課題を軽減して調整を行うことができます。明確に定義されたリードタイム内に、さらに簡単に、現在の世代の暗号化技術を更新して置き換えてテストできるように、プロセスを設計して組み込む必要があります。
- **耐量子:** 組織は、耐量子暗号がビジネスに与える潜在的なパフォーマンスへの影響を認識して、新しいアルゴリズムを実装しなければなりません。

組織は、それぞれ異なります。例えばコストやライフサイクル管理の課題に起因して、すべての組織がすべてを変える立場にある (またはその見解を持っている) わけではありません。しかし、セキュリティ・プロトコルを更新または置換する機能を設計することは、短期的にも長期的にも重要です。これは、システム・インフラストラクチャーと密接に関連しているため、暗号の俊敏性を実現するには、システム設計者、アプリケーション開発者、セキュリティ専門家の協力が必要になります。現在、このプロセスを支援するために利用できるツールが不足しています。

組織は、さまざまな考慮事項を用いて耐量子暗号化を優先させることになります。保護対象資産の価値、保護対象 (キーストアとパスワード) の脆弱性、どの接続システムが影響を受ける可能性があるか (連邦政府機関を含む外部エンティティとの情報共有)、データ保護が必要とされる期間などです。長い移行期間中は、従来のアルゴリズムと耐量子アルゴリズムを組み合わせた、ハイブリッド・スキームが必要になります。

実装、動機、推進要因

機器とインフラストラクチャーが極めて重要なエンタープライズ・ワークロードをホストしているシステム・ベンダーや大規模なクラウド・サービス・プロバイダーには、耐量子暗号化標準が開発されるまで待つ余裕はありません。両者はこの問題に数年間取り組んでおり、2024年に最終的な標準リストを作成するにあたって、最有力候補のアルゴリズムとプロトコルの選定に貢献しています。多くのクラウドベースのキー管理サービスでは、すでに第2段階および第3段階のアルゴリズムをサポートしています。顧客はこれらのサービスを使用して、帯域幅の使用率と遅延におけるオーバーヘッド増加によるアプリケーションへの潜在的なパフォーマンスの影響を測定し、トランスポート・レベル・セキュリティのプロキシ・レイヤーで発生する潜在的な接続障害を軽減し始めています。一方、標準とテクノロジーが進化するのと並行して、耐量子への移行は数年かかるため、そのプロセスはコア・インフラストラクチャー保護から始めることになるのは当然と言えるでしょう。

大手の銀行、保険会社、電気通信、小売、運輸業界向けのシステムでは、メインフレームが高可用性で安全なコア・インフラストラクチャーとして広く使用されています。この傾向は、半世紀以上にわたって維持されてきました。最新のメインフレームには、耐量子ハードウェア・セキュリティ・モジュールが搭載され、更新されたオペレーティング・システム・コンポーネント、キー管理 API、および一連の新しい量子耐性アルゴリズムのサポートと連携して動作します。システム・ブート・ファームウェアの整合性を保護するために、ハードウェアによるルート・オブ・トラストを搭載した耐量子セキュア・ブート・テクノロジーが使用されます。また、ビジネス・パートナーと暗号化キーを安全に交換できるよう、アプリケーション・プログラミング・インターフェースを介して、耐量子メカニズムが提供されます。

クラウド・サービス・プロバイダーとベンダーは、顧客が耐量子暗号化に移行するのを支援する上で、重要な役割を果たさなければなりません。ユーザー組織に特別な専門知識がなくても使用できるような、明確に確立されたガイドラインができておらず、規制当局の発表だけでは十分ではありません。すでに極めて重要なインフラストラクチャーに集中して取り組んでいるベンダーは、有効化のために、さらなるシステムレベルの変更をすることなく、コア・ビジネス・システムの保護を提供することで、プロセスを容易にすることができます。また、暗号化アプリケーション分析で非常に必要とされている、発見ツールを提供することもできます。従来のアルゴリズムを使用して暗号化されたデータは、今後、高度な量子コンピューターによって復号化される可能性があります。そのため、データを管理する組織は、データがそのライフサイクル全体で、現在から将来にわたって保護する必要があるのです。そのデータを20年間保護する必要がある場合、2040年代の未来を想像しなければなりません。量子コンピューティングが実用化されるまで、まだ何年もかかると疑わない懐疑論者でさえ、現在の進化の状況を見ると、その可能性は非常に大きいことを認めなければならないでしょう。

まとめ

量子コンピューティングのビジネスでの活用事例は、強い可能性を秘めています。量子コンピューターが完成すれば、化学、機械学習、金融、輸送、ヘルスケアなど各業界が大きく進歩します。量子コンピューターは、現在使用されている決定論的な従来のコンピューターでは実行不可能な方程式の処理を、指数関数的に加速させます。

とはいえ、量子コンピューティングでは、データ保護とプライバシーへのサイバー攻撃による脅威が増大し、悪影響が出る可能性もあります。データのビジネス価値が高まるにつれて、データ保護要件の規模とコストも増え続けます。また、データの価値は永続するため、近い将来に、量子コンピューティングが実用化される可能性が高まることを考慮に入れなければなりません。早いうちに行動することで、安全で管理された耐量子コア・インフラストラクチャへと移行し、現在のアプリケーション層の脆弱性を発見できるツールを実装し、組織全体で使用されるキー交換システムを保護し、機密性データを継続的かつ長期にわたり保護することができます。



ミッション・クリティカルなアプリケーションを実行して、サイバー攻撃から機密データを保護する上で、IBM Zプラットフォームのエンタープライズ・クラスのセキュリティと回復力は、世界中の企業から信頼を得ています。ポスト量子暗号の世界で脅威に対処するには、最先端のアプローチが必要です。IBM z16は、業界初の耐量子システムであり、量子コンピューターによってもたらされる将来の脅威から、インフラストラクチャー、アプリケーション、データを保護するために設計されています¹。ビジネス向けの強力で安全なプラットフォームであるIBM z16で利用可能な、耐量子テクノロジー、暗号検出ツール、リスク評価サービスについて説明します。

<https://www.ibm.com/products/z16>

¹ IBM z16 with Crypto Express 8Sカードは、NISTが実施するPQC標準化プロセスで最終候補として選択された耐量子暗号アルゴリズムへのアクセスを提供する、耐量子暗号APIを提供します。 <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions> 耐量子暗号とは、大規模な量子コンピューターが構築された後も情報資産を安全に保つために、従来のコンピューターと量子コンピューターのどちらからの攻撃からも耐えうる暗号アルゴリズムを識別する取り組みです。出典: <https://www.etsi.org/technologies/quantum-safe-cryptography> これらのアルゴリズムは、多数のファームウェアおよびブート・プロセスの整合性を確保するために使用されます。

お問い合わせ

米国

+1 877 863 1306

market.intelligence@spglobal.com

ヨーロッパ、中東、アフリカ

+44 20 7176 1234

market.intelligence@spglobal.com

アジア太平洋地域

+852 2533 3565

market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

Copyright © 2022 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

本資料は、一般に公開されている情報および信頼できるとされる情報源からの情報に基づいて、情報提供のみを目的として作成されています。コンテンツ（インデックスデータ、評価、信用関連の分析およびデータ、調査、モデル、ソフトウェア、またはその他のアプリケーションまたはそれらの出力を含む）またはその一部（コンテンツ）は、いかなる形式でも変更、リバースエンジニアリング、複製、または配布することはできません。S&P Global Market Intelligenceまたはその関連会社（総称して「S&P Global」）の書面による事前の許可なしに、データベースまたは検索システムに保存してはなりません。コンテンツは、違法または無許可の目的で使用しないものとします。S&P Globalおよびサードパーティ・プロバイダー（総称して「S&P Globalの当事者」）は、コンテンツの正確性、完全性、適時性、または可用性を保証するものではありません。S&P Globalの当事者は、コンテンツの使用により生じた結果について、その原因にかかわらず、いかなる誤りまたは欠落についても責任を負いません。コンテンツは「現状有姿」で提供されます。S&P Globalの当事者は、コンテンツの機能が中断されないことや、コンテンツがソフトウェアまたはハードウェア構成で動作することについて、特定の目的または用途に対する商品性もしくは適合性、バグの欠如、ソフトウェアのエラーまたは欠陥、コンテンツの内容の保証を含むがこれらに限定されない、すべての明示的または黙示的な保証を拒否します。S&P Globalの当事者は、コンテンツの使用に関連する直接的、間接的、偶発的、懲罰的、代償的、処罰的、特別または結果的な損害、費用、経費、法定費用、または損失（過失による収入の損失もしくは利益の損失、機会費用または損失を含むがこれらに限定されない）について、そのような損害の可能性について知らされていたとしても、いかなる当事者に対しても責任を負わないものとします。

S&P Global Market Intelligenceの意見、引用、信用関連およびその他の分析は、表明された日付の時点での意見の表明であり、証券の購入、保有、売却、または投資決定を行うための事実または推奨事項の表明ではなく、証券の適合性について示すものではありません。S&P Global Market Intelligenceは、インデックス・データを提供可能です。インデックスへ直接的に投資することはできません。インデックスで表される資産クラスの情報は、そのインデックスに基づく投資可能な商品を通じて利用できます。S&P Global Market Intelligenceは、いかなる形態または形式においても、発行後にコンテンツを更新する義務を負わないものとします。当コンテンツは、投資やその他のビジネス上の意思決定を行う際、依存すべきものではなく、ユーザー、その管理者、従業員、アドバイザー、および/またはクライアントのスキル、判断、経験の代用となるものではありません。S&P Global Market Intelligenceは、企業、テクノロジー、製品、サービス、またはソリューションを推奨するものではありません。

S&P Globalは、それぞれの業務の独立性と客観性を維持するために、部門の特定の業務を互いに分離しています。そのため、S&P Globalの特定の部門には、S&P Globalの他部門が利用できない情報が含まれている場合があります。S&P Globalは、各分析プロセスに関連して入手した特定の非公開情報の機密性を維持するためのポリシーと手順を確立しています。

S&P Globalは、通常、証券の発行者または引受人から、あるいは債務者から、その格付けおよび特定の分析に対する報酬を受け取る場合があります。S&P Globalは、その意見および分析を発信する権利を留保します。S&P Globalの公開格付けと分析は、自社サイト www.standardandpoors.com（無料）および www.ratingsdirect.com（サブスクリプション）で利用可能であり、S&P Globalの出版物やサードパーティの再配布業者など、他の手段で配布されます。評価手数料について詳しくは、www.standardandpoors.com/usratingsfees をご覧ください。