digicert®

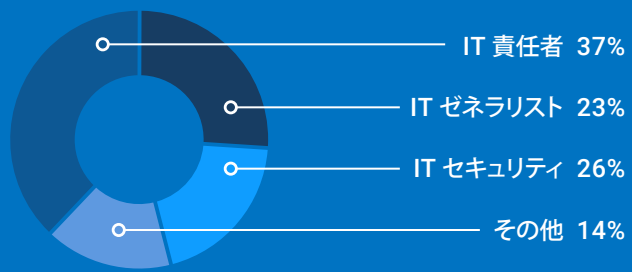
量子コンピューターがもたらす可能性と危険性：

デジサートによる耐量子コンピューター暗号に関する調査、2019 年度版

手法について

デジサートが ReRez Research 社（テキサス州ダラス）に依頼して、従業員数 1,000 人以上の日本企業 400 社の IT プロフェッショナルに対してアンケート調査を実施。

回答者の内訳は、IT 責任者、IT セキュリティマネージャ、IT ゼネラリストなど。



アンケートは 4 つの業種に限定

量子コンピューターがもたらす可能性と危険性

2019 年 1 月、IBM は世界初となる汎用近似量子コンピューティング統合システムである IBM Q System One を発表しました。量子コンピューターの完全な商用利用が実現するのは、まだかなり先ですが、今日のデジタルコンピューターでは処理がきわめて難しい問題の多くを解決できるものとして、量子コンピューティングの可能性には大きな期待が寄せられています。量子コンピューティングで飛躍すると目されている主な分野が、機械学習、メディカルサイエンス、粒子物理学などです。

しかし、量子コンピューティングの将来が、すべて明るいわけではありません。量子コンピューターは将来的に、おそらく今後 10 年以内に、現時点で最新の暗号アルゴリズムを破れるようになり、深刻なセキュリティ問題が引き起こされる — NIST や多くのリーダーたちがそう予測しているからです。

そうなる前に、企業は新しい暗号アルゴリズムを開発しなければなりません。量子コンピューティングの脅威にも耐えうるアルゴリズムです。このようなアルゴリズムを、耐量子コンピューター暗号（Post Quantum Crypt、PQC）と言います。とはいえ、PQC さえあれば対策は十分ということにはなりません。

たとえば、IoT を例にとってみましょう。PQC とは、量子コンピューターによる攻撃にも耐えられるアルゴリズムを指す業界用語です。しかし、ライフサイクルの長い IoT 機器やアプリケーションを作っている企業の製品は、量子コンピューターが最初に脅威になってからも使われ続けるため、かつては安全だった製品が足かせになりかねません。センサーや車載コンピューターを搭載し、インターネットに接続する自動車などがそうなるかもしれません。耐量子コンピューターの戦略を導入しないまま、そうした機器や製品を製造すれば、将来セキュリティ侵害を受ける恐れがあります。

万全の保護をめざすなら、企業は今すぐ、量子コンピューティングの脅威への対策を考え始める必要があります。では、どうやって備え、何をすればいいのでしょうか。そもそも、企業は PQC についてどのくらい理解しているのでしょうか。

こうした PQC をめぐる疑問を探るためにデジサートは、Web サイト、企業アプリケーション、IoT 向けに TLS/SSL などの電子証明書を発行している世界有数のプロバイダーとして、2019 年度版の PQC 調査を依頼しました。その結果は、業界の行動を喚起するにふさわしい内容となっています。

PQC の認知度は高いが、初期段階の混乱も

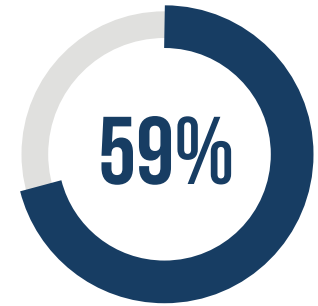
企業の IT 部門では、PQC という言葉がおおむね十分に認知されています。問いに対して、PQC を「ある程度」または「完全に」わかっているという回答が半数を超えましたが、これで話が終わるわけではありません。PQC の意味を本当に理解しているかどうかを確かめる問いを続けたところ、正しい定義を知っているのは 3 分の 2 にすぎませんでした。

さらに言うと、現在ハイブリッド（PQC + RSA/ECC）の証明書を導入しているという回答が 50% に達しましたが、これはいささか疑問です。というのも、PQC 証明書を利用できるのは、早期の試験環境に限られているからです。

もっとも、PQC が新しい概念であり、その意味や対応についてはまだ周知の過程にあることを考えれば、これも無理からぬことでしょう。2012 年のアンケート調査では、「悪天候になるとクラウドコンピューティングに影響がある」と答えた人が半数を超えたそうで、そのときと非常によく似た状況です[1]。混乱があったのは明らかで、その回答者もクラウドコンピューティングを認知するようになり、混乱が長引くことはありませんでした。今や、クラウドコンピューティングは全世界で 2,140 億ドルに及ぶ市場になっています。

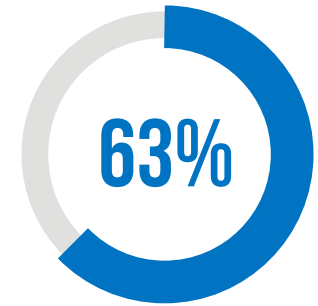
ひとつ言えるのは、量子コンピューティングが多くの人に意識されており、現在および未来の考え方に影響しているということです。今回の調査では、量子コンピューティングが暗号に及ぼす脅威に、セキュリティの専門家がどう対処しようとしているかについても質問しました。

「私たちは、まだ議論の初期段階にいるにすぎません。影響を受けるのは私たちだけではないからです。どうすれば先手を打ってセキュリティを強化できるか、サードパーティのパートナー企業やベンダーと話し合っています。そして、耐量子コンピューター暗号も私たちが検討している重大なトピックのひとつです」— ある金融サービス企業の IT セキュリティマネージャ



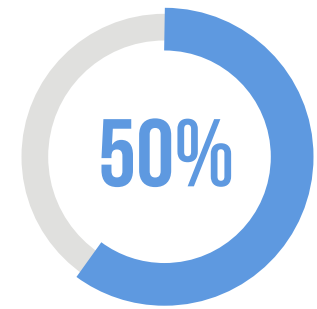
「ある程度、または完全にわかっている」という回答

しかし……



PQC とは何か、正しい説明を選んだ比率

そして、

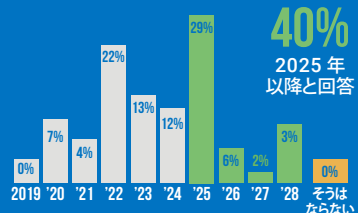


ハイブリッド（PQC + RSA/ECC）証明書をすでに導入しているという回答

1. 51% の人が、悪天候になると「クラウドコンピューティング」に影響があると答えた — Business Insider、2012 年 8 月 30 日

いつ

量子コンピューティングが発達し、現在の暗号アルゴリズムを破れるようになるのはいつでしょうか？



40%
2025 年以降と回答

ほぼ全員が、今の会社に勤務しているうちに脅威が現実のものになると感じている

10 人中 5 人

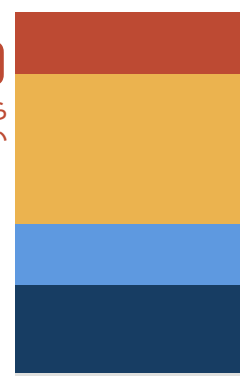
IT 部門が耐量子コンピューターセキュリティについて学ぶことが、ある程度～きわめて重要だと回答

量子コンピューティングの脅威は現実のものであり、目前に迫っている

一部の混乱はともかく、IT 部門は量子コンピューティングが暗号にもたらす脅威を明確に認識しています。量子コンピューティングは現在でも「ある程度」から「きわめて」大きな脅威であるという回答がほぼ 3 分の 2（63%）に及び、将来的に「ある程度」から「きわめて」大きな脅威になるという回答は 74% に達しました。

現在

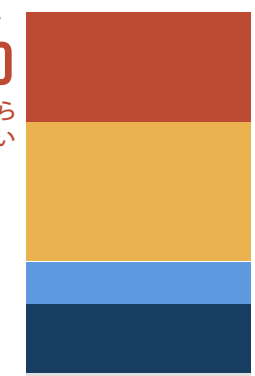
63%
「ある程度」から「きわめて」大きい



- 11%「きわめて大きい」
- 52%「ある程度大きい」
- 19%「どちらとも言えない」
- 18%「ある程度」から「きわめて」大きい
- 0%「わからない」

将来

74%
「ある程度」から「きわめて」大きい



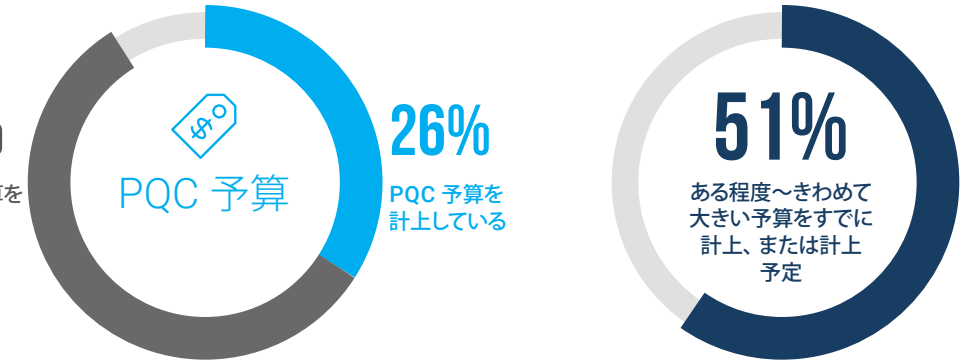
- 21%「きわめて大きい」
- 53%「ある程度大きい」
- 8%「どちらとも言えない」
- 18%「ある程度」から「きわめて」大きい
- 0%「わからない」

では、PQC に関してそもそも「将来」というのは、いつのことを指すと IT は考えているのでしょうか。それほど遠い未来ではないようです。量子コンピューターによるセキュリティ脅威に対抗するために PQC が必要になる時期は、予測の中央値をとると 2024 年でした。それどころか、PQC の到来が 2025 年以降になるという回答は 40% にとどまっています。

脅威がこれほど近くに迫っていると感じているのであれば、対策を練る時間はあまりなく、IT 部門が耐量子コンピューターセキュリティについて学ぶことが重要だという回答が半数近く（48%）に達したのは当然でしょう。PQC について学ぶほか、IT 部門は何に備えればいいのでしょうか。

PQC に備える

企業は実際に PQC への備えを始めており、PQC 予算を計上しているという回答が 4 分の 1 あったほか、予算計上に向けて取り組んでいるという回答も 62% を占めました。では、その予算規模はどうでしょうか。回答者の半数（51%）が、PQC 予算は「ある程度」から「きわめて」大きいと回答しています。予算の用途は、コンサルタント、製品、人材に分かれます。



具体的な活動について見てみると、現在 IT 部門で採用されているトップの戦術は「暗号の変更への対応速度について、そのレベルを理解する」でした。「PQC とその影響について理解を深める」がそれに続きます。この回答からわかるのは、PQC 証明書への切り替えが必要になったとき、企業はその切り替えを迅速かつ効率的に進める必要があると理解されているということです。

上位 5 つに続くのは、「TLS 環境の可視性と管理性を強化する」、「モニタリングする」、「自社の現在のリスクレベルを把握する」となっています。

上位 5 つの移行戦略

1. **暗号の変更への対応速度を強化**
   暗号の変更への対応速度について、そのレベルを理解する
2. PQC とその影響に関する **知識の増強**
3. TLS 環境の **可視化と管理の強化**
4. **モニタリング**
5. **リスクの理解**
   自社の現在のリスクレベルを把握し、リスクを受け入れる

量子コンピューティングといかに闘うか

IT 部門は、量子コンピューティングで直面する暗号のリスクを明確に理解しています。第 1 に懸念しているのは、将来的な量子コンピューティングの脅威や攻撃に対抗するコストが急激に高騰するだろうということです。第 2 に、ひとたび量子コンピューターの攻撃を受ければ顧客の信頼を失うという憂慮があります。そして第 3 に、自社製品に組み込まれたアプリケーションが影響を受けるという点も危ぶまれます。IoT 機器についても、不安は同じです。機器が現時点で最高の暗号を使って設計されているということは、つまり現在の攻撃に対しては安全だが、量子コンピューターによる将来の攻撃に対しては脆弱だということになります。大きな問題になるのは、自動車や ATM のように寿命の長い製品です。

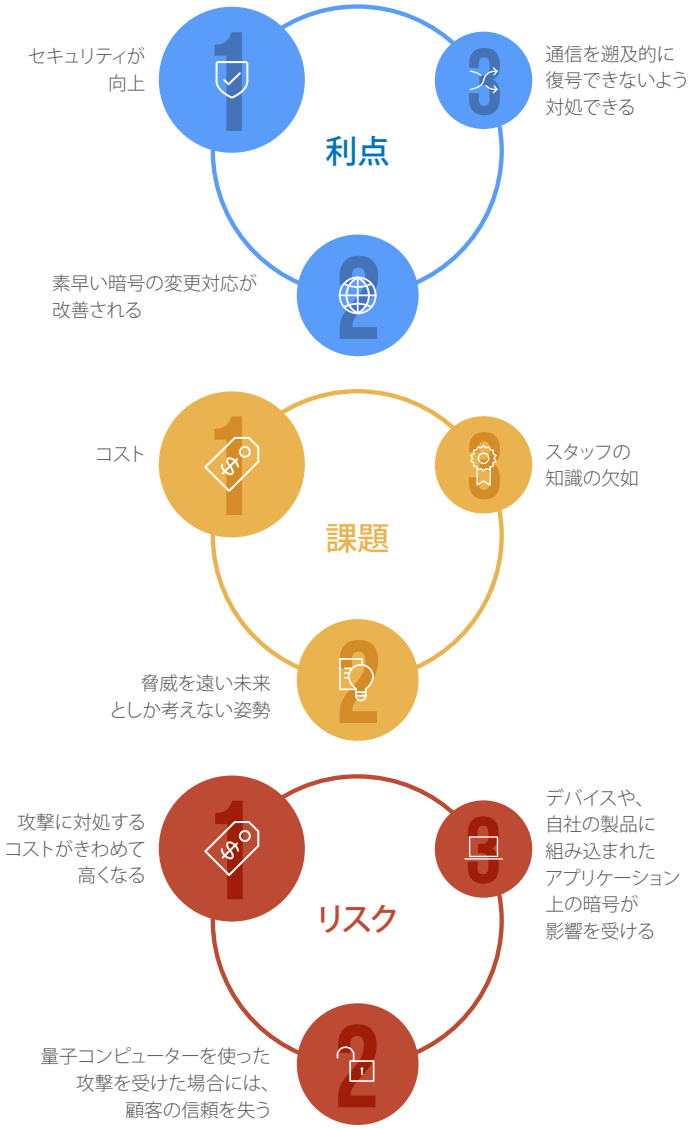
当然、IT は量子コンピューターとの闘いに、すでに備えています。なぜなら、その闘いに勝利すれば、企業のセキュリティが向上し、暗号の変更への対応速度も改善されるというメリットを期待できるからです。

そして、3 つ目のメリットとして、通信を遡及的に復号できないよう対処できます。こうした戦術をとるには、暗号の世界が将来大きく変わることになり、企業はネットワークを停止することなく、古いアルゴリズムから新しいアルゴリズムに短時間で切り替えられなければなりません。

こうしたメリットを考えれば、量子コンピューターと闘う価値は十分にありますが、その闘いに伴うリスクも IT は忘れていません。アンケートの回答によれば、最大の課題はコストです。それに輪をかけて、脅威を遠い未来のこととしか考えていないのも問題です。最後に、スタッフの間で知識が欠如しているという不安も拭い去れません。

総合的に考えると、IT は直面している課題を現実的に捉えていると言えます。実際、暗号をアップグレードして量子コンピューティングの攻撃に備えるのは、ある程度～きわめて難しいという回答が 62% に達しました。

「これは、いつの日か必ず起こることです。そのとき、我々は備えていなければなりません」— ある医療サービス企業の IT マネージャ



デジサートの提言

量子コンピューティングは、企業の未来を形づくる 3 大テクノロジーのひとつです。

しかし、量子がもたらす可能性には、暗号に対するリスクという影が付きまといます。デジサートは、Web 用暗号で世界をリードする企業として、きたるべき量子コンピューターの時代に組織を守る戦略の立案を始めようとする企業のみなさまに、以下のように提言します。

リスク

存在するリスクを知り、耐量子コンピューター暗号に対抗できるモデルを確立する。

技能

組織における暗号の変更への対応速度の重要性を理解し、それを中心的な業務として確立する。

ベストプラクティス

大手ベンダーと協力して電子証明書のベストプラクティスを構築し、常に最先端を走り続けられるように、製品やソリューションなど PQC に関する業界の進展を追跡し続ける。変化が唐突に訪れることはまずありませんが、座して待つのではなく、暗号の変更への対応には今すぐ対処しましょう。

©2019 DigiCert, Inc. All rights reserved.DigiCert 及び DigiCert のロゴは DigiCert, Inc. の商標または登録商標です。シマンテック（Symantec）とノートン（Norton）およびそのロゴは、Symantec Corporation のライセンスにもとづき使用されている商標です。その他の名称もそれぞれの所有者による商標である可能性があります。

デジサート・ジャパン合同会社　本社
〒104-0061
東京都中央区銀座6丁目10番地1号
GINZA SIX 8階

TEL: 03-4560-3900
https://www.digicert.co.jp/

デジサートは、企業向け SSL 証明書、プライベート PKI やマネージド PKI、そして急速に広がる IoT マーケットにデバイス証明書を提供する、世界有数の電子証明書プロバイダーです。約 15 年前に設立されて以来、弊社では、より良い方法を見つけるという理想を掲げて進んでまいりました。それは、インターネットで認証を提供する、より良い方法です。そして、お客様のニーズに合わせたソリューションを提供するための、より良い方法です。この度、弊社の革新的ソリューションにシマンテックの経験とノウハウが加わりました。弊社はより良い方法をもたらす革新によって業界をリードし、デジタルアイデンティティと電子決済により大きな安心を作り上げてゆきます。