耐量子コンピューター暗号 (PQC) 成熟度モデル

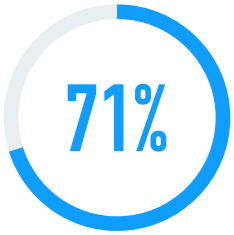
digicert®

目次

差し迫る量子コンピューティングの脅威

量子コンピューティングの進化によって高まる恐ろしい脅威については、ほとんどの企業が認識しています。量子コンピューターの威力の前では、既存の暗号化アルゴリズムの安全性など、泥棒を前にしてドアに鍵をかけずにいるようなものです。デジサートが最近実施した調査[1] では、IT の専門家の多く (71%) が、量子コンピューティングが暗号にもたらす脅威について認識していることが分かりました。とはいえ、同調査で、PQC の脅威をどこまで正確に理解しているかについては、組織によって大きなばらつきがあり、備えについても同様に大きなばらつきがあることが判明しました。

この「耐量子コンピューター暗号の成熟度モデル」は、PQC の脅威を理解するための指針であると同時に、現時点で自社の備えがどの程度できているかを把握するツールでもあり、このコンピューティング革命に伴う課題を乗り越える方法についてヒントを提供するものです。このモデルに従うことで、組織のセキュリティを耐量子時代のセキュリティに近づけることができます。



IT の専門家の大多数が量子コンピューティングが暗号にもたらす脅威を認識している

量子 vs 暗号化

耐量子時代のセキュリティ対策への道のりにおいて、現時点で自社の対策がどの程度まででできているのかを把握するためには、まず量子コンピューティングとは何か、そして現在の暗号化ツールとどのように関係しているのかを知ることが重要です。

量子コンピューティングは、コンピューティングの次なる飛躍的革新です。情報理論を量子力学と融合させることで、量子コンピューターは大量のデータを同時に処理できるので、無限の解を持つ複雑な問題を解くことができます。つまり、量子コンピューターは、線形的な演算プロセスを回避して、非線形の解に素早く到達することができるのです。

現在使用されている公開鍵暗号化アルゴリズムでは、一方向には簡単に実行できるが、逆関数の計算はほぼ不可能に近い「トラップドア」変数を使った数学関数が使用されています。たとえば、2 つの素数の掛け算など、一方向の演算プロセスは、どのコンピューターでも簡単に実行できます。しかし、演算結果の桁数が十分に大きくなると (2,048 ビット以上)、それを 2 つの素数に素因数分解できるコンピューターは存在しません。

ところが、量子コンピューティングの登場により、それが根底から覆されるのです。かつては、それほど大きな桁数の因数分解には数十億量子ビットの量子コンピューターで計算する必要があると考えられていましたが、最近の調査によれば、さらに少ない量子ビット数でも素早く解にたどり着けることが分かりました (8 時間、2000 万量子ビット[2])。

このニュースにより、暗号化業界に激震が走りました。組織は来たるべきセキュリティ脅威に注視せざるを得なったのです。

成熟度レベル

デジサートでは、研究結果と経験をもとに、組織の量子成熟度レベルを測る重要な要素は次の 2 つであることを見極めました。

- 組織が量子コンピューティングの脅威をどの程度知り、理解しているか
- 脅威への備えはどの程度まで進んでいるか

あなたの理解度と計画のレベルをグラフ化することで、今、PQC 対策の導入を成功させる道のりのどこにいるかが分かります。

1 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
2 How to Factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits | Craig Godfrey (Google: 米カリフォルニア州サンタバーバラ) Martin Ekerá (スウェーデン王立工科大学 : スウェーデン、ストックホルム)

成熟度レベルの概要

PQC 初級者

量子コンピューティングが組織にもたらす脅威についてほとんど知らない、あるいはまったく知りません。したがって、その組織では量子コンピューティングの攻撃に対してほとんど、あるいは何も準備をしていません。

PQC 実習生

来たるべき量子コンピューティングの脅威に対して備えに乗り出す必要性について理解しています。自分たちのネットワーク全体の暗号化が、耐量子コンピューターセキュリティ対策の基盤であることに気づいています。さらに、組織における HSM (Hardware Security Module) の利用状況や、HSM が暗号化対策において果たす役割についても理解しています。

PQC 実践家

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の対策にすでに着手しています。組織のリスクレベルを把握し、暗号化を保護するツールを既に導入しています。証明書は管理プラットフォームで一元管理されており、可視性は最適化され、組織のすべての資産がコントロールされています。さらに、現在そして将来の量子コンピューターによる脅威から組織のネットワークを守るための包括的な戦略の第一歩を既に踏み出しています。このレベルの知識と準備が揃った段階で、耐量子コンピューター暗号証明書の実現可能性をテストする組織が現れます。

PQC マスター

組織のポリシー、暗号化に使用されている規格をすべて文書化する作業が完了しており、暗号化の俊敏性とその正しい活用法について理解しています。すべての電子証明書のインベントリを最新に保つ自動化機能を備えたプラットフォームを導入し、暗号化インフラストラクチャ全体が完全に可視化され、コントロールされています。PQC マスターは、本番環境への導入によってクリティカルなシステムやアプリケーションに混乱や障害が発生しないよう、自ら積極的に自社ネットワーク内で耐量子コンピューター暗号をテストし展開するための新しい方法を探し求めます。知識と準備が整ったことで、セキュリティのニーズを事前に予測し、セキュリティへの脅威が現実化する前に問題を解決する備えができていることになります。

不均衡による危険を回避

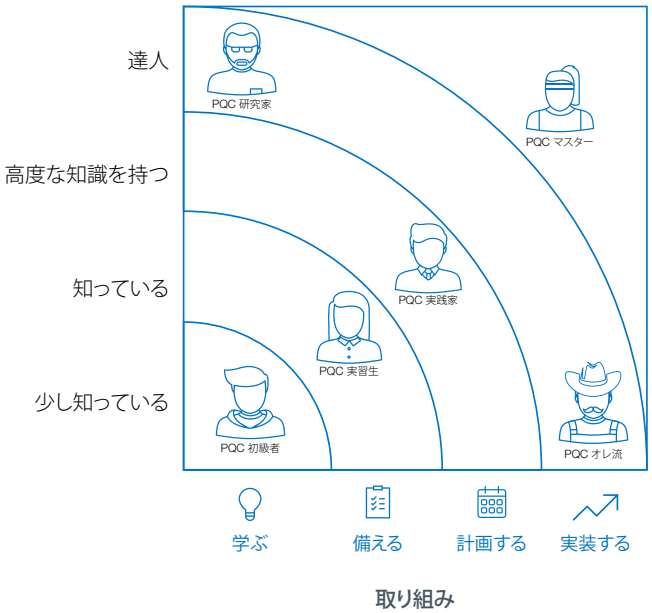
実践なき知識、知識なき実践はいずれも、外部のハッカーと同じくらい組織の暗号化への脅威となる可能性があります。すべての IT プロフェッショナルは、次のいずれのタイプにもならないよう注意してください。

PQC 研究家

来たるべき量子コンピューティングの脅威について深い知識があるのに、現実的に意味のある備えに今だ取り組んでいません。

PQC オレ流

PQC 初級者同然の知識しかない状態で、効果が実証されていないお粗末なセキュリティ対策を導入して備えを始めてしまっています。



PQC 初級者 

量子コンピューティングが組織にもたらす脅威についてほとんど知らない、あるいはまったく知りません。したがって、その組織では量子コンピューティングの攻撃に対してほとんど、あるいは何も準備をしていません。組織内で実習生に準備の開始が任されることもあります。しかし、PQC セキュリティ対策の導入に向けた計画があるわけではありません。

PQC 初級者のリスク

来たるべき脅威

PQC 初級者であることは、組織に大きなリスクをもたらします。デジサートが実施した最近の調査において、IT 専門家の大多数が量子コンピューティングは「ある程度」～「きわめて」大きな脅威であると考えていることが分かりました。脅威が現実化する時期について、予測の中央値をとると 2022 年でした。PQC 初級者が知識を身につけ、量子コンピューター攻撃から組織を守るために必要な計画を立てるために残された時間はわずかしかありません。

知は力なり

PQC 初級者から PQC 実習生になるだけでも、組織のセキュリティリスクは大きく軽減します。量子コンピューティングの脅威について十分に理解することで、組織のセキュリティインフラについて新しい考え方で見ることができるようになります。自動化機能を備えたデジタル証明書管理プラットフォームを採用し、暗号化環境全体を一貫して可視化し、コントロールできるようにするために必要な知識が身につきます。

PQC 初級者が学ぶべきこと

PQC 初級者はまず、暗号化について基礎的な知識を身につける必要があります。組織のネットワーク全体で確実な暗号化を行うことは、耐量子コンピューターセキュリティ対策の基盤です。まずは、ここから始めましょう。

証明書と証明書管理

AOSSL とは何か、なぜ重要なのか

AOSSL は、Always on SSL (常時 SSL) の略で、組織の Web サイト全体に暗号化を適用するための業界標準のベストプラクティスです。AOSSL を正しく導入すると、社内および社外のすべての Web ページが暗号化され、サイバー攻撃にさらされにくくなります。AOSSL は、社内のすべての Web ページに導入するだけでなく、サードパーティとの統合にも導入することでセキュリティ態勢を全体的に強化できます。AOSSL を有効な暗号化管理プラットフォームで導入すれば、AOSSL セキュリティ環境全体を可視化し、管理できます。これにより組織の脅威に対する保護を完全に監視できるようになります。

AOSSL と量子セキュリティの関係

HTTPS のベストプラクティスでは、(内部および外部の) すべての Web ページ、相互接続されたマシン同士に暗号化が正しくインストールされていることが要求されています。信頼できる AOSSL を導入することで、将来的な量子コンピューターによる脅威に対して暗号化をアップデートする準備が整います。

管理プラットフォームが重要である理由

PQC 初級者の多くは、導入したセキュリティ対策が組織の電子的存在のすべてをカバーしているわけではないことを認識していません。量子コンピューターによる脅威に備える最初のステップの 1 つは、組織の暗号化 (電子証明書) 対策を理解することです。有効な暗号化管理プラットフォームでは組織のネットワーク全体を完全に可視化できます。リスクを評価し、セキュリティギャップを修正するためにはプラットフォームの導入が欠かせません。

暗号化管理プラットフォームには、以下の機能を備えている必要があります。

レポート機能 : 包括的なレポートにより、現在暗号化されている内容を確認し、暗号化が正しく設定され (通信が保護されており、コードと文書が署名されている) 更新されていることを確実にできます。

完全な可視化 : 組織のネットワーク全体と接続デバイスをすべて可視化できることは、暗号化の穴を見つける唯一の方法です。見えないものを修正することはできません。

証明書の自動化 : どの証明書が自動化されており、どの証明書が自動化されていないかを知ることは、インフラストラクチャを最適化するために不可欠です。本機能を一貫して使用することは、時間の節約になるだけでなく、証明書の期限切れによるセキュリティギャップの防止にも役立ちます。

ハードウェアセキュリティモジュール (HSM)

独自鍵生成の実装方法を知る

組織が独自鍵の生成にハードウェアセキュリティモジュール (HSM) を使用しているかどうか、HSM をどのように使用しているのかを把握しておくことは重要です。HSM プロバイダに問い合わせて、組織の HSM が耐量子コンピューター暗号化へのアップグレードに対応しているかどうかを確認するとよいでしょう。また、アップグレードのタイムラインを確認する必要もあります。HSM の更新や手順が組織の量子セキュリティ導入に関するタイムラインや計画に合致していることを確認します。デジサートでは、最高の耐量子 HSM を導入するために、業界のリーディングカンパニーである、Gemalto と Utimaco をお勧めしています。

PQC 初級者の取り組み

知識が拡充してきたら、PQC 初級者から PQC 実習生になるために、何らかの取り組みに関わることが重要です。以下のチェックリストは、量子コンピューティングの脅威から組織を守るための取り組みに役立ちます。

- ネットワーク全体の暗号化がセキュリティベストプラクティスの基盤であることを理解するようにします。ネットワーク全体のイメージを掴みます。そうすることで、セキュリティ対策に耐量子コンピューターの保護を加えたときに暗号化が必要になる範囲が分かります。
- 組織の暗号化 (電子証明書) 対策を文書化し、お使いの証明書管理プラットフォームの機能を確認します。リスクとセキュリティギャップを評価します。脆弱な箇所はどこですか？プラットフォームに以下の機能があることを確認します。

  レポート : 証明書、配置場所、ライフサイクル、タイプ

  証明書の検索 : CA に関わらず、使用中のすべての電子証明書をネットワーク全体の全デバイスおよびドメインでスキャン

  自動化 : ネットワーク全体で証明書の自動化を導入し、暗号化の停止やギャップを防ぐ

  可視化 : 暗号化の穴 (証明書の欠如) を表示できること

- 組織で HSM が使用されているか、さらにその HSM が組織の暗号化対策に適合するかを確認します。HSM のプロバイダを特定し、組織のタイムラインに合わせて量子セキュリティソリューションを提供できるかどうかを確認できます。

PQC 実習生

PQC 実習生は、差し迫った量子コンピューティングの脅威に対して備えに乗り出す必要性を理解しています。

組織ネットワーク全体の暗号化が、耐量子コンピューターセキュリティ対策の基盤であることを認識しています。AOSSL とは何かを理解しており、有効な管理プラットフォームの重要性を知っています。さらに、組織における HSM の利用状況や、HSM が組織内の暗号化プロセスにおいて果たす役割についても理解しています。

時代遅れでリスクの高いスプレッドシートによる管理に代わり、最新の証明書管理プラットフォームを導入し、証明書の発行、更新、失効を完全に可視化し、コントロールできています。発生した脅威に迅速に対応できます。

PQC 実習生のリスク

今日は安全でも明日は脅威に

PQC 実習生は、現在の組織に対する脅威に対してしっかりした基盤を構築できていますが、将来発生する脅威の評価には着手していません。これ以上ないほどセキュアなネットワークでも、量子コンピューティングの脅威には脆弱である可能性があります。PQC 実習生が PQC 実践家になるには、暗号化の俊敏性 (既存の暗号をより安全な PQC アルゴリズムに移行する準備がどれほど整っているか) について理解することが必要です。

PQC 実習生が学ぶべきこと

暗号化の俊敏性とは

PQC 実習生が PQC 実践家になるには、暗号化の俊敏性 (暗号の変更への対応速度) について、それが何であり、何が違うかの両方を学ぶ必要があります。

暗号化の俊敏性は、可視性と動的な移行を重要視しています。それは、組織内で暗号化が使用されているありとあらゆる箇所 (プロトコル、ライブラリ、アルゴリズム、証明書など) を認識することです。また、暗号化技術がどのように実装されているかを理解し、問題が発生したときには素早く問題を特定して修正できることでもあります。真の暗号化の俊敏性とは、その暗号化方式が時代遅れになったタイミングで、自動的かつシームレスに新しい方式に置き換えるために必要な機能を備えていることであり、クリティカルな機能 (ハッシュ、署名、暗号化など) に別のアルゴリズムを使用できる能力のことではありません。また、特定の機能についてアルゴリズムを選択できる能力でもありません (SHA-1 か SHA-256 かなど)。

敵は身内の中に紛れている

暗号化の俊敏性について理解した上で、PQC 実習生は、一見友好的なソースから脅威がもたらされる可能性について学ぶ必要があります。耐量子コンピューターの対策をいくら講じたとしても、量子攻撃に対して保護されていない企業などと組織のデータや情報が共有されていれば、データを守ることはできません。

PQC 実習生が PQC 実践家になるためには、ベンダー、パートナー、サードパーティから組織にどのように脆弱性が持ち込まれるかを評価する必要があります。サードパーティのプロバイダとコミュニケーションを取り合い、各社が量子コンピューターの脅威に対してどのような試験やセキュリティ対策を計画しているかを話し合います。

PQC 実習生の取り組み

PQC 実習生のあなたは、量子コンピューターによる差し迫った脅威について十分に理解しています。今こそ、その知識をさらに深め、計画を立案するときです。以下のチェックリストは、量子コンピューティングの脅威から組織を守るための取り組みに役立ちます。

- 「暗号化の俊敏性を高める方法」を読み、その提言に基づいて計画を立て始めます。

  暗号化の俊敏性は、最新のハイブリッド SSL/TLS (RSA/ECC) から始まります。次世代の暗号化の俊敏性はハイブリッド SSL/TLS (RSA/ECC/PQC) です。業界の最新情報を常にチェックすることが大切です。新しい情報が出てきたら、信頼できるソースを組織の計画に含めます。

- サードパーティベンダーのリストを作成します。各社のセキュリティ状況 (完全に暗号化されたネットワークを導入している企業とそうでない企業) を文書にまとめます。

  組織のセキュリティは、最も脆弱なサードパーティーベンダーと同じくらい脆弱です。

- 次世代の暗号は誰によって開発されているのかを知りましょう。

  a. ISARA: https://www.isara.com/crypto-agility-quantum-safe (英語リンク)

  b. Microsoft: https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/ (英語リンク)

PQC 実践家

PQC 実践家は、組織のリスクレベルを把握し、暗号化を保護するツールを既に導入しています。証明書は管理プラットフォームで一元管理されており、可視性は最適化され、組織のすべての資産がコントロールされています。さらに、現在そして将来の量子コンピューターによる脅威から組織のネットワークを守るための包括的な戦略の第一歩を既に踏み出しています。

PQC 実践家のリスク

テストは証拠

PQC 保護自体と同じくらい重要なのは、テスト戦略を策定し、開始することです。システムが何に対して防御できるのかを知るまでは、組織はリスクにさらされたままです。

PQC 実践家のあなたは、テストをする心の準備は万端でしょう。量子コンピューティングに関するかなりの知識と、実行する計画があれば、起こりうる脅威に対してセキュリティ対策をテストするというのは自然な流れです。しかし、どこから始めればよいのでしょうか。現在、PQC 規格は存在しませんが、どのような選択肢があるのでしょうか。

PQC 実践家が学ぶべきこと

テスト環境でのハイブリッド作業

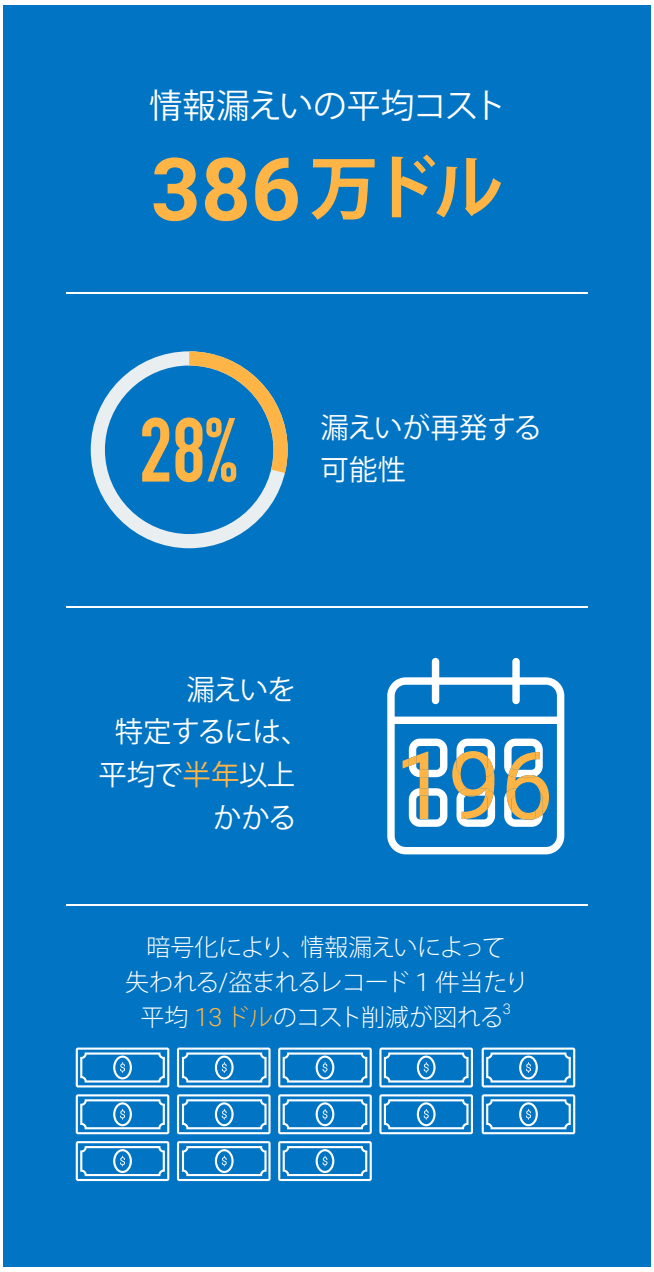
PQC 実践家のあなたは、暗号化の俊敏性に関する能力を元に、組織のシステムの範囲や設定について把握しているはずです。次のステップは、ハイブリッド RSA/PQC を使用して自社のセキュリティ対策にテストテクノロジーを組み込む方法を理解することです。ISARA とデジサートの両社から、ハイブリッド TLS 証明書をテストするために必要なものをすべて含んだ PQC ツールキットが提供されています。

ハイブリッド TLS 証明書では、耐量子コンピューター暗号アルゴリズムを旧知の暗号化アルゴリズムと組み合わせて使用します。そのため、後方互換性を確保しながら、耐量子コンピューターハイブリッド TLS 証明書の実現可能性をテストすることができます。サンドボックス環境で構築しテストを行うことで、組織のセキュリティが危機にさらされる前に、ハイブリッド証明書の経験を積むことができます。テスト環境では、ハイブリッド証明書が現在のアプリケーションとどのように連携するかを確認できるため、本番の PQC セキュリティシステムを実装する前に解決策を探すことができます。

データの機密性

現在の組織に対する最も困難な脅威の 1 つは、量子コンピューターによる攻撃に対して脆弱な情報の盗難です。今は暗号化されていて解読できなくても、将来的に量子テクノロジによるハッキング法で解読できることを見込んで、犯罪者たちはデータを盗み、溜め込んでいます。

PQC の知識を身につけ、導入を計画する上で重要なのは、どの組織が最も機密性が高いか、あるいは最も価値が高いかを決定することです。この情報は、現在の暗号化基準だけでなく将来



情報漏えいによるコストの詳細については、Ponemon Institute の最新の調査結果を参照してください。https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/ (英語リンク)

3 Robert Hackett, Data Breaches Now Cost $4 Million on Average: https://fortune.com/2016/06/15/data-breach-cost-study-ibm/ (英語リンク)

的にも安全であるように PQC セキュリティ対策によって守られなければなりません。将来の脅威に対峙するのは容易なことではありません。最高情報セキュリティ責任者 (CISO) をはじめとする組織のキーパーソンと話し合う必要があります。

真っ先に保護すべき組織資産は何かを考える際には、重要な占有情報の集合 (顧客の個人記録や知的財産など) について考えてください。顧客の個人記録の流出は、組織にとって金銭的にも風評面からも大きなリスクを負うことになります。知的財産は、この 20 年間、従来のハッカーにとって格好の標的でした。他国の知的財産の獲得が、各国の経済およびセキュリティ戦略の一環として利用されるのと同様です。

PQC 実践家の取り組み

PQC 実践家のあなたは、実装予定のセキュリティシステムのテストを開始する準備ができています。それでは、テストを始めます。以下のチェックリストは、量子コンピューティングの脅威から組織を守るための取り組みに役立ちます。

- 組織内のキーパーソンと会い、最初に保護すべき資産および情報は何かを特定します。顧客の個人的記録と知的財産のほか、CIO、CTO をはじめとする組織チーム内の識者が提言するものを優先します。第 1 ラウンドの PQC 展開において、これらの資産を保護する目標を設定します。
- PQC ツールキットを選定し、テストの選択肢やプロセスを学びます。ハイブリッド RSA/PQC 電子証明書を構築しテストする計画を立てます。
- ハイブリッド証明書のテストを実行します。脆弱性と非互換性を特定し、記録します。本番環境に展開する前に、セキュリティギャップを修正する計画を立てます。

PQC マスター 

PQC マスターは、組織内の暗号化に使用される全規格の文書化を既に完了しています。暗号化の俊敏性を理解し、対策の一環として既に導入しています。組織全体の暗号化は完全に可視化されており、すべてのセキュリティ対策が有効なプラットフォームでコントロールされています。

これで、組織のネットワーク全体に耐量子コンピューター暗号をテストし導入するための知識と準備が整いました。テストと綿密なモニタリングを通して、クリティカルなシステムやアプリケーションを停止しなくても、本番ネットワークに PQC を導入できます。真のマスターの学びに終わりはありません。彼らは変化に適応して学ぶことの必要性、求める知識を得られる場所に戻るタイミングを知っています。

PQC マスターのリスク

取り巻く環境の変化

PQC マスターが抱える唯一のリスクは、未知の事柄です。量子コンピューティングはまだ開発段階にありますが、ほどなく実用化されます。テストおよびモニタリングを継続的に行うことで、新しいテクノロジーが進化し続ける状況でも、組織を保護することができるでしょう。

PQC マスターが学ぶべきこと

PQC マスターは、機動性と高い意識を持ち続け、技術の進化にとともに変わり行く量子コンピューティング事情に対応していくだけです。次ページの参考資料が役立つでしょう。

まとめ

以上に述べたことより、耐量子アルゴリズムへの移行を計画するのをぎりぎりまで先延ばしにしていると、組織のデータを不必要にリスクにさらすことになります。成熟度モデルで述べたステップを辿ることで、将来的な移行のために適切な備えをし、最新の技術や手法を活用する準備が整います。デジサートでは、耐量子セキュリティに向けたさまざまなステップにおいて、お客様を全力でサポートします。

NIST
ステートフルハッシュベース署名の最新情報
https://csrc.nist.gov/Projects/Stateful-Hash-Based-Signatures (英語リンク)

IETF
署名方式の最新情報
https://datatracker.ietf.org/doc/rfc8391/ (英語リンク) Quantum Internet Proposed Research Group (QIRG) のセッション

CA/B
https://cabforum.org/2018/03/08/final-minutes-for-ca-browser-forum-f2f-meeting-herndon-va-7-8-march-2018/ (英語リンク)

ANSI
https://webstore.ansi.org/Standards/ASCX9/ASCX9TR502019 (英語リンク)

リスクカリキュレーター
https://quantum.bpi.com/ (英語リンク)

ISARA
https://www.isara.com/ (英語リンク)

マイクロソフト リサーチ
耐量子コンピューター暗号プロジェクト
https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/ (英語リンク)

耐量子コンピューター暗号化についての詳細は、現在連載中のブログ記事 (英語リンク) をご覧ください。また、組織への耐量子セキュリティ対策の導入方法について具体的なご質問がある方は、Tim Hollebeek (tim.hollebeek@digicert.com) までお問い合わせください。

digicert®