CJ Moses による 2023 年以降のセキュリティに関する予測

AWS, Chief Information Security Officer
CJ Moses

2022 年 11 月

目次

クラウドサービスは地球上のほとんどあらゆる場所で使用できます。そして今、宇宙に向かっています。AWS は現在、世界中にある 27 リージョンでお客様にサービスを提供しており、Project Kuiper では、世界中でサービスが提供されていない、または提供が足りていないコミュニティに、高速で価格が手頃なブロードバンドを提供する、衛星コンステレーションを軌道上に送り込もうとしています。クラウドが広く使用されるということは、データがクラウドに急速な勢いで保存されているということです。2020 年に生成されたデータは、毎秒 1.7 MB でした。**2025 年には、463 エクサバイトのデータが生成される**とする予測もあります。同時に、クラウドとデータの連携が急成長したことで、組織に課せられた、クラウドジャーニーを促進するためのスキルを持つ人材の雇用と投資という要求は、重くなっています。企業がイノベーションを迅速に推し進めるにつれて、このデータを保護することが、継続的な成長とクラウドの改革に不可欠であることは明らかです。

テクノロジーと人間の間で稼働するあらゆる領域について、私たちは両方を適切にミックスしクラウドセキュリティの未来を定義する、魅力的なフェーズに入っています。未来に目を向ければ、お客様が差別化につながらない面倒な作業をなくすには、オートメーションが鍵であることは明らかです。そうすれば、クラウドで安全性を保ち、起こりうるセキュリティイベントの際にはより迅速に対応するために、適切な判断を行い続けることができます。

AWS にとって、セキュリティは最優先事項です。AWS は日々、お客様に信頼してもらえるよう努めています。私の仕事の大部分は、将来起こりうるセキュリティのニーズに備える方法を検証することです。この日本語ガイドは、AWS の視点に関してインサイトを提供するものであり、また 2023 年以降のセキュリティの方向性を予測するものです。

予測 1

セキュリティは組織のあらゆる活動に不可欠になる

増え続ける脅威とリスクにより、クラウドへの移行が引き続き促進されるでしょう。クラウドでは、組織のあらゆる活動にセキュリティが組み込まれています。組織は継続的なセキュリティとコンプライアンスに移行し、デジタルトランスフォーメーションの初期段階で、適切なセキュリティを決定するのがより簡単な環境を作成するようになるでしょう。これは、自動化されたセキュリティサービスやツールの普及により可能になります。

毎日のように AWS のお客様から、セルフマネージド型でオンプレミスのセキュリティ技術から、ビジネス変革アーキテクチャをサポートしスケールする責任共有サービスモデルに移行する機会を捉えた方法が、共有されています。これは、ビジネスの拡大に合わせるために、また組織がより簡単に自社を保護できるように、セキュリティはできる限り自動化する必要があると、お客様が理解しているためです。クラウドは、オンプレミスでは不可能だった方法でデータを保護する素晴らしいイノベーションを提供するため、組織はセキュリティを強化しながら、同時にビジネスの成長に集中できます。その結果、組織はセキュリティ文化を受け入れつつあります。つまり、セキュリティを運営方法に組み込むことで、安全に先に進むことができるのです。

このセキュリティへの注目は、効果的なセキュリティプログラムを維持するという中核的な要素から始まります。アイデンティティと許可の管理、ネットワークとインフラストラクチャの保護、脅威の特定と対処、データ保護、コンプライアンスの提示などが含まれます。クラウドでは、各領域に関連したありふれたタスクを自動化できます。数例を上げれば、ログ記録、モニタリング、監査、パッチ適用、既存のツールセットなどです。**AWS Identity and Access Management (IAM)**、**AWS CloudTrail**、**AWS Key Management Service (AWS KMS)**、**AWS WAF**、**Amazon GuardDuty**、**AWS Security Hub** などのツールは、データがどこに保存されているか、いつ誰がアクセスできるか、その暗号化状態、どこに移動されているか、それに対して疑わしい活動があるか、一般的なエクスプロイトの影響を受けやすいかどうかについて、インサイトを得られる重要なツールです。今後数年、クラウド導入が続くことが不可避な状況と相まって、このような分野でさらなる自動化に対する需要が急激に高まるのは間違いないでしょう。

組織は、継続的なセキュリティとコンプライアンスを実施するようになります。AWS のお客様、パートナー、AWS のセキュリティサービスの提供と保守を行う社内のビルダーの経験から、クラウドセキュリティサービスにおける急速なイノベーションにより、あらゆるものにセキュリティを組み込み、継続的なセキュリティの改善を行うのが、さらに簡単になっていることがわかっています。これには、クラウドセキュリティサービスやツールで見られる使いやすさが大いに貢献しており、お客様は開発速度やセキュリティバーを向上させて、最終的には安全に出荷できるようになります。1 つだけ例を挙げると、お客様は、**Amazon Inspector** と **AWS Systems Manager** を使用して、インフラストラクチャやアプリケーションへのパッチ適用を自動化できます。これにより、手動でパッチを適用する負荷を軽減し、複数のオペレーティングシステムにパッチを適用するプロセスを簡易化して、お客様の生産性を向上させることができます。

予測 2

ダイバーシティで継続的なセキュリティ人材のギャップを解決できる

クラウドの規模が大きくなるにつれて、セキュリティのプロフェッショナルの需要も大きくなっています。ダイバーシティは、この問題の解決策の大きな部分を占めています。さまざまな教育的および職業的背景を持つ人々、ニューロダイバースな人々、異なる文化的な出自の人々の雇用に力を入れている組織は、セキュリティにおいて、そうではない組織を上回るでしょう。

2021 年当時、サイバーセキュリティのプロフェッショナルは、世界中で 419 万人でした。しかし、さらに 272 万人が必要でした。セキュリティ要員のギャップを埋めることが、場所を問わずセキュリティを向上させるための重要なステップです。セキュリティのプロは現場に加わり続けていますが、セキュリティのプロに対する需要は供給を上回っています。組織がセキュリティ要員のギャップを埋める方法としては、**Amazon のアフィニティグループ**に似たダイバーシティ、公平性およびインクルージョン (DE&I) の取り組みへの投資、雇用基準の再評価と演習、多様な背景を持つ候補者への投資などがあります。セキュリティのプロの約半数が、IT の門外漢からキャリアを始めており、これは勇気づけられる事実です。意欲と才能で雇用し、技術スキルをトレーニングすれば、企業はさらに安全になり成功することでしょう。マイノリティや多様な背景を持つ人々が業界に参入するのに苦労することがある理由のひとつが、高等教育と多数のセキュリティ認定にかかる莫大な費用です。組織は、特定の技術的な練度や認定にこだわるのではなく、才能や、別の形のスキルを持つ人々の雇用を試してみるべきです。

セキュリティのプロの多様性は、セキュリティにおける視点の多様性を意味し、ひいてはより強力な防御を意味します。例えば、英国の信号諜報機関である GCHQ のような組織では、ニューロダイバースな個人を積極的に雇用し、データのパターンを発見するユニークな能力を活用することで、**この方法の手本を見せています**。AWS にとっては、セキュリティにおけるダイバーシティとは単なる公平性以上のものであり、可能な限り幅広い問題解決能力を利用することによる防御機能の最適化に関するものです。

雇用の多様化は AWS における文化の主要部分であり、セキュリティに関する背景を持たない人々の雇用を意味することにもなります。セキュリティの分野で人が成功を収めるためのスキルは多数あり、このような人材を雇用してセキュリティトレーニングを提供することが重要であると AWS は確信しています。また、既存のスタッフの能力開発と維持に力を入れることも重要です。AWS は、社員や組織がセキュリティ体制を向上させるには教育が肝であると、長年信じてきました。そのため、**Amazon Security Awareness トレーニング**を全員に無料で提供しています。クラウドセキュリティオペレーションの自動化も、人材のギャップを埋めるのに役立つかもしれません。しかしこの問題は、技術だけでは解決できません。第一に人にフォーカスした作業であるべきです。メンターシッププログラムを通して、また次世代のワークフォースをつないで STEM 教育を促進することで、未来のスタッフの開発を強化する必要があります。

AI/機械学習で促進されたオートメーションがセキュリティを強化する

機械学習と人工知能は、クラウドセキュリティに重要なオートメーションのレイヤーを追加します。AI/ 機械学習は開発者のワークストリームを強化するため、開発者は、より信頼性の高いコードを作成して、継続的なセキュリティ向上を促進できます。

セキュリティはこれまで、物事が許可されるかされないかという、二項分類的なルールベースのシステムでした。そして AWS は、さまざまな条件に基づいて「許可」を定義する複雑なシステムを構築してきました。クラウドによりこのモデルが変更され、今では、既存の脅威に対して、強力な防御と効果的なヘッジ戦略を、動的に構築できるようになりました。クラウドセキュリティ改革の次の段階の一部として、脅威の検知と修正に人間レベルのインテリジェンスを適用するのが一般的になるでしょう。今後数年で、機械学習がセキュリティエンジニアの能力拡張に大きな役割を果たすと予測しています。これにより、エンジニアはより安全なアーキテクチャやアプリケーションをクラウドに作成できます。

AI/ 機械学習の予測機能により、お客様は、進化し続ける脅威の状況に立ち向かう、よりプロアクティブなセキュリティスタンスを開発できます。これは、在宅勤務やハイブリッド勤務モデルが台頭してきたここ数年で、ますます重要になってきています。さまざまなネットワークにわたって人々の業務が劇的に変化し、脅威領域が大幅に広がってきたためです。脅威アクターは、リモート勤務によって起こったこの現象を利用し、以前は見られなかったマルウェアを使用して、ランサムウェア、フィッシング、ソーシャルエンジニアリングなどの一般的なセキュリティインシデントを起こすようになりました。

ハイブリッドでますます複雑になるこの環境において、Amazon GuardDuty、**Amazon Detective**、**Amazon CodeGuru**、**Amazon Macie** などの AWS のサービスは、セキュリティや機械学習の統合における基礎を築き続け、インテリジェントなレコメンデーションで、お客様を大規模に支援します。これらや、急速に進化するその他の機械学習クラウド機能は、大量のデータを評価し、異常を感知して、セキュリティの脆弱性、コードの品質、潜在的な脅威に関するインテリジェントなレコメンデーションを提供できるため、有益です。例えば、Amazon GuardDuty でリリースされた**DNS レピュテーションモデリング**では、AWS 全体から DNS リクエストを集めてモデルに入力するため、AWS は、見知らぬドメインをその挙動特性に基づいて悪性または良性に分類できるようになりました。実際、AWS はこれらのモデルが頻繁に忠実性の高い脅威検出を提供することを確認しました。悪意のあるドメインを、商用の脅威フィードで特定され利用可能になるより 7 ～ 14 日早く特定しています。

AI/ 機械学習が引き続きセキュリティに影響を与えると思われるもうひとつのユースケースは、コンプライアンスです。AWS のサービスに組み込まれた自動推論などの AI 技術により、お客様は、世界的なデータセットの中でコンプライアンスリスクを引き起こす異常の検出を自動化して、複雑なシステムにおけるコンプライアンス体制をより深く理解できます。これまでは、コンプライアンスステータスやアクセス許可の変更を評価するのに人間が関わる必要があったため、セキュリティとコンプライアンスに関するタスクの多くがこれに足を引っ張られ、この領域の管理は受け身なプロセスになっていました。**AWS Audit Manager** や **AWS Identity and Access Management Access Analyzer** などのクラウドサービスを利用すると、人間の介入を必要とせずに自動化できるため、お客様は、IT インフラストラクチャに変更をデプロイする前に、コンプライアンス体制とアクセス許可レベルに関してより詳細に理解できます。Audit Manager は、お客様がある時点で手動で評価するのではなく、目的のコンプライアンスフレームワーク (Payment Card Industry Data Security Standard、Center for Internet Security、米国国立標準技術研究所 (NIST) など) 用のエビデンス収集を自動化できます。このエビデンス収集は継続的でもあるため、お客様は目的のフレームワークに対するコンプライアンス準拠に関するレポートを、いつでも出力できます。IAM Access Analyzer を利用すると、お客様はリソースやデータに対して過度にアクセスを許可していないか、ポリシーをモニターできます。ポリシーが作成されると (作成も IAM Access Analyzer が手伝います)、IAM Access Analyzer が人間の介入を必要とせずに認可をモニターします。セキュリティにおいて今後数年、継続的改善というこの概念がますます増え、クラウドプロバイダー、パートナー、クラウドユーザーのエコシステム全体が、世界中のクラウドセキュリティのシステム的な高度化を促進するオートメーション機能をさらに進化させることになるでしょう。

ここで説明したような AI/機械学習駆動のセキュリティイノベーションは、お客様にとって、セキュリティプラクティショナーが現実世界の日々の課題を解決するのに役立っています。例えば、SOC アナリストのワークロードを削減し、セキュリティアーキテクトが、アプリケーションで閉じられているファイアウォールやパッチ適用されたサーバーを検証しなければならないのではなく、脅威モデリングに、より多くの時間をかけることができるようになります。クラウドセキュリティの AI/ 機械学習は、まだ端緒を開いたばかりです。クラウドが急速に成長するにつれ、セキュリティも同様に、迅速に成長する必要があるでしょう。それにより、オートメーションとインテリジェンス駆動のセキュリティのニーズも促進されます。

予測 **4**

データ保護への
より大きな投資が進む

データ保護は、AWS のお客様や世界中の人々にとって、常に重要課題です。生成されるデータ量が急激に増加し続けているため、なおさらです。これほどに成長が著しいと、データ保護に関する立法の増加、データ保護および関連プログラムに対する投資の増加、自動化への移行が予測できます。

EU 一般データ保護規則 (GDPR)、カリフォルニア州消費者プライバシー法 (CCPA)、その他現地に合わせた法律は、データ保護規制の始まりにすぎません。**2019 年に行われた Cisco の調査**では、回答者の半数近く (47%) が、 GDPR に準拠している企業は信頼性が増すと回答しています。データ保護の分野が成熟していき、データ保護法を求める世間の声が大きくなり続けるにつれて、より多くの政府がその声に応え法律を施行し、要件を満たす企業も増えるでしょう。Gartner は、2024 年末には世界の 75% で、個人データが規制の対象となると予測しています。

また、今後数年で、組織はデータ保護に対する投資を増やすでしょう。Gartner は、大組織のプライバシーに関する平均年間予算は **2024 年までに 250 万 USD を超える**と予測しています。この投資の一部は、データに関するリスクの評価方法、現行の管理およびリソース管理タスクの実行方法、機能性を高く保ちながらデータのリスクを軽減するツールの開発方法を含むデータ保護プログラムにかけられます。

AWS では、お客様の信頼を得ることがビジネスの基礎です。AWS は進化し続けるプライバシー規制と立法状況を見守り、変更を特定して、お客様がコンプライアンスのニーズを満たすために必要なツールを判断します。これが AWS の現行のコミットメントです。お客様が、AWS IAM、CloudTrail、Macie その他 AWS のサービスやツールを使用して、データの保管場所、保護方法、アクセス権所有者を判断し、所有するデータをコントロールできるようにします。また、サービスや機能にプライバシーセーフガードを実装し、お客様が、高度なアクセス、暗号化、ログ記録の機能を実装できるようにします。お客様は、世界中の 1 つ以上の **AWS リージョン**のどこにでも、データを保存するように選択できます。AWS のサービスを使用すると、お客様はデータが選択した AWS リージョンにあることを確認できます。

AWS におけるデータ保護の詳細については、**AWS のサービスのプライバシー機能**、**AWS のデータ保護**、**データプライバシーセンター**を参照してください。

予測 **5**

より高度な他要素認証の形が普及していく

認証がさらにバイオメトリクスおよびマルチモーダルな形式に移行していくことで、MFA の未来は強固なセキュリティとユーザビリティを組み合わせたものになり、ユーザーはセキュリティ体制を強化しながら摩擦のないエクスペリエンスを利用できるようになるでしょう。

MFA は、お客様が使用できる最もシンプルでもっとも重要な保護であり、パスワードがオンラインで漏えいしたり、社員がソーシャルエンジニアリングの標的になったりした場合に、悪意のある行為者がアカウントにアクセスするのをより困難にするものです。お客様は MFA を使用して、通常データ漏えいによる盗難に対して脆弱でデータ漏洩による盗難に遭いやすいパスワードの他に、追加要素 (本人の持ち物、本人の知識、バイオメトリクスなど本人の特長) を要求することで、アカウントやアプリケーションのセキュリティを強化します。

MFA は、ビジネスと個人両方の使用において、ますます広く使用されるようになっており、次の未開拓分野は、その利便性とセキュリティの向上性から、認証におけるマルチモーダルバイオメトリクスフォームの使用のさらなる普及にあると、AWS は確信しています。多要素とは、認証を目的として 2 つ以上の要素を使用することであり、ローミング (Yubikeys や Virtual Authenticators) やプラットフォーム (Windows Hello や Apple FaceID などのデバイスの) を含むこともあります。マルチモーダルとは、システムへのアクセスに複数のバイオメトリクスを使用することです。バイオメトリクス認証は、個人に固有の生体的な特長を使用して、本人であることを検証する研究分野であり、通常は物理的または行動における特長を含みます。バイオメトリクスの利用が増えるにつれて、MFA は、お客様にとってより摩擦がない自然なエクスペリエンスになっていきます。マルチモーダルバイオメトリクスシステムでは、物理的なバイオメトリクス要素 (指紋、声、虹彩、顔認識) を、行動的な要素 (キーストローク、手の動き、握力など) と組み合わせた、コンビネーションになっていくことでしょう。

MFA の使用は、過去数年間で政府や有名なセキュリティ組織がセキュリティに対して置いた優先度の向上の恩恵を受けるでしょう。MFA は、FIDO Alliance、NIST、米国政府などの機関により、オンライン保護の基本として推進されており、最近発行された**ステートメント**では、すべての企業が MFA を導入するように促しています。政府、特にサイバーセキュリティ & 社会基盤安全保障庁 (CISA) では、MFA に対する認識と導入を促進するさらなる手段として、#MoreThanAPassword **キャンペーン**を開始しています。

AWS では、お客様に、MFA の予想される高度化を今後数年見守り続け、既存の機能を改善するか、組織のルーチンに新しい MFA 機能を構築する方法を確認することをお勧めします。AWS は今後も、AWS の **MFA の概要ページ** で、MFA の高度化に関してお知らせしていきます。

予測 6

量子コンピューティングはセキュリティにとってメリットになる

量子コンピューティングは、まだ誰もが真っ先に思い浮かべるようなものではありませんが、徐々に高度になっており、耐量子セキュリティもそれにつれて暗号化の形で高度化しています。AWS は既に、ポスト量子化の世界に備えて作業を行っています。長期的には、量子コンピューティングにより安全性が向上すると AWS では予想していますが、今のところ、組織はデータの保護に最新の暗号化手法を必ず使用するようにする必要があります。

量子コンピューティングが手頃な価格になり利用しやすくなる時が来る証拠がいくつかあります。ただし、それが 5 年後か 50 年後かは定かではありません。ただ、その時が来れば、HTTPS や TLS のような転送中のデータのセキュリティプロトコルに使用している種類のものを含む、ある種類の暗号化が弱体化すると予想されます。業界では現在、耐量子暗号化またはポスト量子暗号と呼ばれるものを手掛けています。これは、さまざまなアルゴリズムとさまざまなキーサイズが、量子コンピューターに対しても、今日使用しているのと同じレベルのセキュリティを提供するものです。暗号化アルゴリズムとプロトコルが、将来起こるかもしれないこのリスクを解決するために進化すれば、デバイスが相互に接続する方法に変動が見られることでしょう。携帯電話、パソコン、サーバーがこの新しいテクノロジーを導入し、通信におけるプライバシーを保護するのです。

長期的には、量子コンピューティングはクラウドセキュリティにとって実質的にメリットになります。組織にとって量子コンピューティングや量子アルゴリズムがもっと身近になれば、従来のアルゴリズムについて別の考え方をするようになるでしょう。量子学の影響を受けた新しいプロセスに照らして従来のアルゴリズムを再考すると、既存の機能について創造的なソリューションを生み出す刺激となり、量子学に由来するコンピューティングに関する新しい考え方に基づいた、新しい、または進化した従来のアルゴリズムを開発できます。例えば、**量子学の研究者**はすでに、従来のコンピューターを量子コンピューターの能力に潜在的に合わせ、ユーザーが好む製品をレコメンドする方法を見つけています。

業界が量子コンピューティングのリスクについて考慮すれば、暗号化の標準は進化し続けます。NIST は既にこの取り組みを始めており、2024 年までに新しい耐量子標準を定めることを目指しています。この標準は、数年に渡って行われる複数回の評価に及ぶ、**ポスト量子暗号化の標準化作業**を通して開発されています。AWS を含む大組織が、この取り組みに寄与しています。AWS は 2 つのオプション (BIKE と SIKE) を申請し、どちらも一次選考を通過しています。この選考では、元の 82 の申請が絞り込まれ 26 の提案が残っています。NIST はおそらく、複数の申請で標準化すると思われます。さまざまなアプローチにより、パフォーマンスのさまざまな側面 (コンピューティングは高速化するが、ネットワークメッセージが大きくなるなど) をトレードオフできるためです。

AWS は、他社と協力して将来の標準を実装し、またポスト量子暗号化の開発と実装を続けていきます。AWS KMS は既に、TLS 1.2 向けにハイブリッドポスト量子キー交換アルゴリズムをいくつかサポートしています。バイデン政権は、2022 年の覚書に、国防総省など米国機関のサイバーセキュリティ向上に関してポスト量子暗号化を含めており、ポスト量子暗号化を実装する政府は増えていくだろうと AWS では考えています。

これまで見てきたとおり、組織がデジタル化するにつれて、クラウドのさらなる拡大は避けられません。セキュリティは組織のあらゆる活動に不可欠になり、セキュリティ文化が生まれると AWS は確信しています。この文化では、すべての社員がセキュリティの所有者となって組織のセキュリティにポジティブな影響を与えることができるようになり、セキュリティの実践は、テクノロジーのイノベーションと多様性のある人々が促進する、集合的で継続的な追求となります。これらの要素は、組織と個人両方のセキュリティに対する認識全体の変化に影響を与え、セキュリティは、IT における一連の義務を掲げる「ノー」と言う部署とみなされるのではなく、ビジネスとイノベーションを促進するものとみなされるでしょう。AWS と AWS のお客様は、変化するクラウドセキュリティ環境の最前線に立ち続け、基礎的なイノベーション、ユースケース、ベストプラクティスを提供して、セキュリティをビジネスとテクノロジー両方における未来のイノベーションの中核に位置付けます。