

CISO CJ Moses の提言： 金融サービス業界における セキュリティの推進

AWS、Chief Information Security Officer、
CJ Moses

2023 年 5 月

目次

はじめに	3
トレンド	
セキュリティは組織のあらゆる活動の要になる	4
AI/機械学習が主導する自動化がセキュリティを強化する	5
終わりのないセキュリティ人材のギャップは ダイバーシティによって解決できる	7
セキュリティのカルチャーを構築する	8
時代をリードする AWS.....	9

はじめに

トレンド：
セキュリティは組織のあらゆる活動の要になる

トレンド：
AI/機械学習が主導するオートメーションがセキュリティを強化する

トレンド：終わりのないセキュリティ人材のギャップはダイバーシティによって解決できる

セキュリティのカルチャーを構築する

時代をリードするAWS

はじめに

金融サービス業界には、テクノロジーを使用したビジネスイノベーションの促進に確かな実績があります。お客様との新しい関わり方や新製品の開発、データ分析のスケーリングやエンタープライズレジリエンスの構築など、ビジネスの強化は、強力なセキュリティプログラムなしには起こりえません。

金融サービス組織は、データを使用してビジネス上の意思決定を実行することに関して他をリードしています。クラウドの普及に伴い、データが急激なペースで蓄積されています。**2020年には、個人が生み出すデータは毎秒 1.7 MB でした。2025 年には、世界全体で 463 エクサバイトのデータを生み出すことになるという予測もあります。¹**

そうしたデータの価値を実現するため、組織はスキルを持った人材の雇用と人材投資を行って、クラウドへの道のりを加速させる必要に一層迫られています。

私たちはテクノロジーとヒトをつなぐあらゆる要素を調整しながら、両者をうまく組み合わせることでビジネスイノベーションを促進するという、興味深い段階へと入りました。セキュリティは、ビジネスの成長を促進するものであると同時に、このイノベーションの方程式においても重要です。

この複雑な新しい時代において、セキュリティチームが、クラウドの安全性の維持に適切な判断を下し続け、避けることのできないセキュリティイベントに迅速に対応するにはどうすればいいでしょうか。

企業、特に金融サービス企業は、セキュリティカルチャーを組織全体で築くことに注力すべきです。こういったカルチャーがあると、セキュリティに関する判断を、最も効果を発揮できる場所に移すことができます。

セキュリティカルチャーで成果を出すには、判断を行うチームが最適なアクションを取れるように、適切なオートメーションとツールを提供することが重要です。

クラウドは自動化に適した強固な基盤です。その利点を活用するには、ワークフローに自動化を組み込む必要があります。AI と機械学習の強化が助けとなるでしょう。最近では、AI を問題に適用してセキュリティに関する判断を強化するシナリオが飛躍的に増加しており、今後も増えることが予想されます。

セキュリティとは単なる技術上の課題ではないことを、常に念頭に置くことが重要です。強力なセキュリティポスチャ（セキュリティ態勢）には、人が不可欠です。ここで述べたセキュリティツールは、人間がより優れた判断を下し、唯一無二の価値を生み出す作業に注力できるように設計されたものです。

チーム内のスタッフに多様性があるほど、判断はより効果的になるでしょう。多様な視点やさまざまな経験を備えたチームが、より強力なセキュリティ対策を構築するのを、私たちは目の当たりにしてきました。

業界を問わず企業には、セキュリティカルチャー、AI と機械学習が主導するオートメーション、多様性を備えたチームという3つの領域が不可欠です。強力なセキュリティプログラムが、レジリエンスの向上とイノベーションの促進を可能にします。そして、金融サービス業界では、セキュリティは単なる要件ではなく、企業が目標を達成するために役立つ鍵なのです。

¹ 「How much data is generated each day?」、Jeff Desjardins、World Economic Forum、2019年4月17日。

はじめに

トレンド：
セキュリティは組織のあらゆる活動の要になる

トレンド：
AI/機械学習が主導するオートメーションがセキュリティを強化する

トレンド：終わりのないセキュリティ人材のギャップはダイバーシティによって解決できる

セキュリティのカルチャーを構築する

時代をリードするAWS

トレンド

セキュリティは組織のあらゆる活動の要になる

クラウドに移行するということは、責任共有型のサービスモデルにシフトすることを意味します。このオペレーションモデルは、現在のビジネスをサポートするだけでなく、企業がアーキテクチャを変革しモダン化したときにも円滑にスケールできます。

つまり、組織は増大するビジネスの需要に継続的に応え、より容易にセキュリティを確保するために、セキュリティプロセスと技術を開発する必要があるのです。その第1歩は自動化です。

クラウドには、オンプレミスではできない方法で、セキュリティを自動化する基盤が用意されています。セキュリティカルチャーが浸透していれば、イノベーションが加速する中でも、自動化によって安全に先に進むことができます。

いかなるセキュリティの実践においても、アイデンティティとアクセス許可の管理、ネットワークとインフラストラクチャの保護、脅威の検知と対処、データの保護、コンプライアンスの提示はどれも重要な領域です。同時に、自動化により大きなメリットを得られる領域でもあります。

AWS Identity and Access Management (IAM)、AWS Key Management Service (AWS KMS)、AWS CloudTrail、AWS WAF、Amazon GuardDuty、AWS Security Hub 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、暗号化の状態がどうなっているか、データの移動先はどこか、疑わしい活動があるか、一般的なセキュリティ上の弱点はないかについて、インサイトを得られるツールです。

クラウドセキュリティサービスの急速なイノベーションにより、あらゆる業務にセキュリティを組み込み、継続的に改善することが今までに増して容易になったということ、AWS のお客様、パートナー、また社内ビルダーの経験から実感しています。

良い例として、継続的なコンプライアンスがあります。コンプライアンスの扱いを、年に 1~2 回行う必要がある単なる報告業務ではなく、通常業務にするというシンプルなアイデアです。自動化主導のセキュリティ対策を利用すると、作業を自動化しながら、監査に必要なエビデンスも生成されるため、この類いのパターンを確立できます。

1 つだけ例を挙げましょう。Amazon Inspector と AWS Systems Manager を使用すると、お客様はインフラストラクチャとアプリケーション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しその作業を文書化するという負荷が軽減されます。

セキュリティチームが自動化に重点をおくことで、いずれは組織がより効果的にビジネス目標を達成する助けになると、私たちは考えています。

はじめに

トレンド：
セキュリティは組
織のあらゆる活動
の要になる

トレンド：
AI/機械学習が主
導するオートメー
ションがセキュリ
ティを強化する

トレンド：終わりの
ないセキュリティ
人材のギャップは
ダイバーシティに
よって解決できる

セキュリティの
カルチャーを
構築する

時代をリードする
AWS

トレンド

AI/機械学習が主導する自動化が セキュリティを強化する

セキュリティはこれまで、物事を許可するかしないかという、二項分類的なルールのシステムでした。そして、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。

このモデルを、クラウドが変えます。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。セキュリティが次のフェーズへと進化するにつれて、AI と機械学習が果たす役割は大きくなると私たちは予想しています。

AI と機械学習は、セキュリティエンジニアの能力を強化し、クラウドでより安全なアーキテクチャやアプリケーションを作成できるようにします。AI と機械学習の予測機能により、進化し続ける脅威ランandscapeに立ち向かう、プロアクティブなセキュリティ体制を確立できます。

在宅勤務やハイブリッド型勤務モデルのリスクは、このような要因が作用している良い例です。勤務体系の転換に伴い、さまざまなネットワークにわたって人々の働き方に非常に大きな変化が起こっており、「通常の」オペレーションや活動を判断するのが、ますます複雑になっています。その結果、脅威アクターはこの現象を利用し、新しい特殊なタイプの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よく知られるセキュリティインシデントを起こすようになりました。

このような複雑な環境において、[Amazon GuardDuty](#)、[Amazon Detective](#)、[Amazon CodeGuru](#)、[Amazon Macie](#) などの AWS のサービスは、セキュリティと AI/機械学習を大規模に統合するための基盤となっています。

これらのサービスやその他の急速に進化を続ける AI と機械学習機能を利用して、大量のデータの評価、異常の特定、セキュリティの脆弱性やコード品質、潜在的な脅威などに関するインテリジェントなレコメンデーションを実現しています。

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、DNS リクエストを AWS 全体から集めてモデルに入力し、見知らぬドメインをその行動特性に基づいて悪性または良性に分類します。

実際、AWS では、このようなモデルによる高精度の脅威検知が頻繁に行われていることを確認しています。悪意のあるドメインを、商用の脅威フィードで特定、利用される 7~14 日前に検出できています。

また、AI/機械学習は、コンプライアンス活動にも作用することがわかっています。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、お客様は複雑なシステムにおけるコンプライアンスポスチャをより深く理解できるようになり、世界規模の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います。

はじめに

トレンド：
セキュリティは組織のあらゆる活動の要になる

トレンド：
AI/機械学習が主導するオートメーションがセキュリティを強化する

トレンド：終わりのないセキュリティ人材のギャップはダイバーシティによって解決できる

セキュリティのカルチャーを構築する

時代をリードするAWS

これまで、セキュリティとコンプライアンスに関する多くのタスクは、人間の介入が必要であることが足かせとなっていました。人間がコンプライアンスステータスやアクセス許可の変更を手動で評価する必要があったため、この領域の管理は事後対応的なプロセスになっていたのです。

AWS Audit Manager や IAM Access Analyzer などのクラウドサービスを利用すると、このプロセスを自動化し、人間の介入を減らすことができます。このアプローチでは、お客様はIT インフラストラクチャに変更を加える前に、自社のコンプライアンスポスチャやアクセス許可レベルをより詳細に把握できます。

AWS Audit Manager は、コンプライアンスフレームワーク (PCI-DSS、CIS、NIST など) のエビデンス収集を自動化し、お客様による、ある時点での手動の監査評価を必要としません。このエビデンス収集は継続的に行われるため、特定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、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、ポリシーをモニタリングできます。ポリシーを生成すると (IAM Access Analyzer が生成を支援します)、人間の介入を必要とすることなく認可がモニタリングされます。

このようなツールを利用して、「継続的な改善」の概念を実装できます。クラウドプロバイダー、パートナー、ビルダーが一体となり、自動化機能をさらに進化させることができる、心強い存在です。

AI/機械学習を活用したセキュリティイノベーションは既に、お客様の現実世界の課題解決に日々役立っています。セキュリティオペレーションセンター (SOC) アナリストやセキュリティアーキテクトは、このようなツールを利用して、ファイアウォール変更の検証やサーバーのパッチ適用にかかる時間を減らし、より多くの時間を脅威モデリングやセキュリティプラクティスの改善に使うことができます。



はじめに

トレンド：
セキュリティは組織のあらゆる活動の要になる

トレンド：
AI/機械学習が主導するオートメーションがセキュリティを強化する

トレンド：終わりのないセキュリティ人材のギャップはダイバーシティによって解決できる

セキュリティのカルチャーを構築する

時代をリードするAWS

トレンド

終わりのないセキュリティ人材のギャップはダイバーシティによって解決できる

自動化と AI/機械学習は、より効率的に業務を行うための助けとなります。その一方で、サイバーセキュリティの専門知識を持ったプロフェッショナルが世界中でさらに必要とされていることも、AWS は以前から認識しています。2021 年には、既にプロフェッショナルとして従事している 419 万人に加えて、272 万人の人材が必要だと言われていました。²

現場で働くセキュリティのプロフェッショナルは増えていますが、その供給を上回る需要があります。組織がセキュリティ人材の不足を埋める方法としては、Amazon のアフィニティグループのような、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実践、多様な背景を持つ候補者への投資などがあります。

セキュリティの専門家の約半数は、IT 以外の分野からキャリアに飛び込んでおり、これは勇気づけられる事実です。意欲と才能で雇用し、その後技術スキルをトレーニングすれば、企業はさらに安全性を高め、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理由の 1 つが、高等教育と多くのセキュリティ認定にかかる莫大な費用です。組織は、特定の技術分野での学位や認定にこだわるのではなく、才能や、別の形のスキルにおいて実績のある人々の雇用を目指すべきです。

セキュリティプロフェッショナルのグループに多様性があれば、セキュリティをさまざまな視点で捉え、防御を強化できます。例えば、英国の通信諜報機関である GCHQ のような組織では、ニューロダイバースな人材を意図的に雇用し、人とは違う特別な能力を活用してデータのパターンを発見しており、多様性のある雇用の手本を示しています。AWS にとって、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す。可能な限り幅広い問題解決能力を持つことで、防御機能を最適化することなのです。

² (ISC)². A Resilient Cybersecurity Profession Charts the Path Forward. (ISC)² Cybersecurity Workforce Study, 2021 年。



はじめに

トレンド：
セキュリティは組
織のあらゆる活動
の要になる

トレンド：
AI/機械学習が主
導するオートメー
ションがセキュリ
ティを強化する

トレンド：終わりの
ないセキュリティ
人材のギャップは
ダイバーシティに
よって解決できる

セキュリティの
カルチャーを
構築する

時代をリードする
AWS

セキュリティのカルチャーを構築する

組織がデジタルトランスフォーメーションを通して自らを改革するようになったことで、セキュリティはあらゆる活動の中心になっています。セキュリティカルチャーの構築は、成功に不可欠です。特に金融サービス業界においてはよりいっそう重要なものです。

セキュリティカルチャーのもとでは、すべての社員がセキュリティに当事者意識を持ち、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、セキュリティの実践は、連帯して継続的に追求するものになります。この追求を加速するのが、自動化や AI/機械学習のようなテクノロジーのイノベーションと、人材の多様性です。

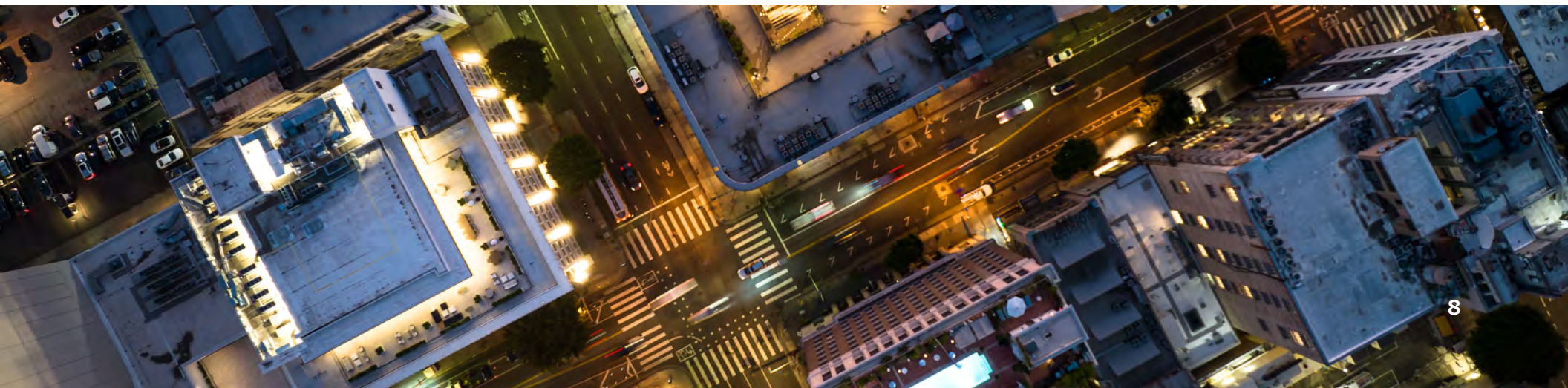
これらの要素が、組織と個人両方のセキュリティに対する全体的な認識の変化に影響を与え、セキュリティを要件としてではなく、ビジネスとイノベーションを促進するものと考えられるようになるでしょう。

金融サービスにおけるセキュリティ強化の鍵となる 3 つの成長領域は、オートメーション、AI/機械学習、多様性を備えたチームです。

これらは、組織がセキュリティプログラムの中で考慮すべき戦略的イニシアチブです。その最初のステップは、[AWS Cloud Adoption Framework](#) と [AWS Well-Architected フレームワーク](#) を使用して立案します。

これらのツールは、実際の経験をもとに作られたガイダンスを提供し、組織が次のステップを計画するのを支援します。ただし、実践的なガイダンスを提供するという AWS カルチャーの精神に則って申し上げれば、今すぐ実行できる間違いのないステップは、組織に多要素認証 (MFA) を導入する、または拡張することです。

デジタルアイデンティティの新時代において、MFA は、企業が使用できる最もシンプルかつ重要な保護であり、パスワードが漏えいしたり、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ても、悪意のある行為者がアカウントにアクセスできないよう阻みます。



はじめに

トレンド：
セキュリティは組織のあらゆる活動の要になる

トレンド：
AI/機械学習が主導するオートメーションがセキュリティを強化する

トレンド：終わりのないセキュリティ人材のギャップはダイバーシティによって解決できる

セキュリティのカルチャーを構築する

時代をリードする
AWS

時代をリードする AWS

AWS は金融サービスとテクノロジーの交差点に位置するパイオニアであり、常に変化する規制に対応しながら、AWS のお客様に広範なサービスとパートナーソリューションを通じて、業務の最適化とイノベーションの加速を提供します。急成長中のフィンテック企業から、グローバルなシステム上重要な金融機関まで、数千社の金融サービス企業が AWS で自社の未来を再形成しています。

金融サービス分野の日本の営業担当者に問い合わせる >