aws FOR FINANCIAL SERVICES

クラウドのセキュリティとコンプライアンスを徹底して金融機関を要塞化する

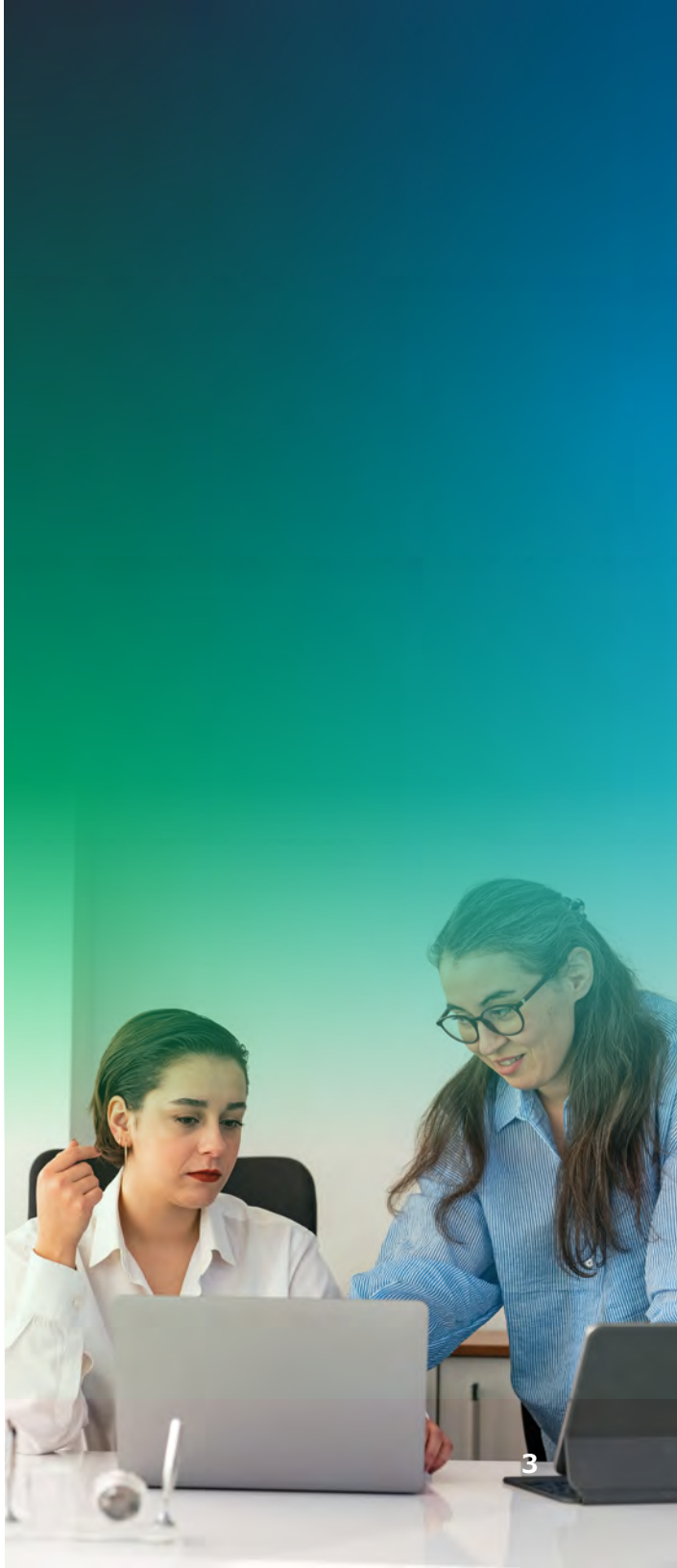
目次

はじめに

金融サービス機関によるクラウドへの移行と、クラウドでの構築が進む中で、回復力、セキュリティ、データプライバシー、規制への準拠は、これまでと同様に重要です。

クラウドテクノロジーは、あらゆる種類のエンタープライズにおいて進化し続けています。金融サービス機関は、取引ライフサイクルプラットフォーム、銀行および保険の基幹システム、支払い処理ソフトウェアなどのビジネスクリティカルなアプリケーションの構築のために、ますます大規模なクラウド移行にフォーカスしています。

クラウドに移行すると継続的にセキュリティとコンプライアンスに遵守でき、金融サービス機関がデジタルトランスフォーメーションの早い段階、またその全体を通じて、セキュリティに関する適切な決定を簡単に行うことができる環境が整います。コンプライアンスを確保した、スムーズでセキュアな移行を実現するため、金融サービス機関は、利用する予定のクラウドサービスプロバイダー (CSP) のセキュリティおよびコンプライアンス能力を慎重に評価して、ベストプラクティス、テクノロジー、ツールの導入準備を整える必要があります。



変化する環境への対応

金融サービス機関は、データ、アプリケーション、インフラストラクチャに関して、規制とセキュリティ要件が常に変化する複雑な環境に直面しています。AWS は、こうした環境に確実に対応できるように金融サービス機関を支援できます。

サイバー攻撃の主なターゲット

この業界は、最もサイバー攻撃の標的になりやすいセクターの 1 つとして常に上位にランクされています。フィッシング、ランサムウェア、サービス拒否 (DoS) 攻撃、内部脅威など、あらゆる脅威ベクトルが存在します。さらに、脅威の数と巧妙さは増すばかりです。

55%

の金融機関が 2021 年にランサムウェア攻撃を受けており、これは 2020 年の 34% から増加[1]

[1] 出典：Sophos

63%

の金融機関で、2021 年に「破壊的な攻撃」が増加[2]

[2] 出典：VMware

一貫性のない複雑な規制要件

データプライバシーとサイバーセキュリティを取り巻く規制環境は複雑で、一貫性に欠ける状況がますます進んでいます。

金融サービス機関は、厳格なデータプライバシー要件に対応しなければなりません。その中で最も有名で広範囲に及ぶものが、EU の一般データ保護規則 (GDPR) です。米国では、カリフォルニア州、コロラド州、コネティカット州、ユタ州、バージニア州が、それぞれ独自のデータプライバシー要件を導入しており、複数の州にまたがって事業を営む組織にとって複雑さが生まれています。

さらに、世界各地の政府や規制当局が、金融サービス機関の業務リスクとして、情報および通信テクノロジー (ICT) の役割を注視しています。特筆すべきは、EU のデジタルオペレーショナルレジリエンス法 (DORA) が業務リスクの構成要素を拡大して、ICT を含めていることです。

注目のオペレーショナルレジリエンス

- **オーストラリア**は、証券と先物市場の運営者や参加者の技術的レジリエンス (回復力) およびオペレーショナルレジリエンスを促進することを目的とした、市場整合性に関する規則を発効しました。
- **香港**は、オペレーショナルレジリエンスの枠組みとタイムラインを策定することを金融サービス機関に要求する、監督ポリシーマニュアルを導入しました。
- **シンガポール**は、運用リスク管理と、アウトソーシングおよびサードパーティーの管理に関するガイダンスを公表しました。また、このガイダンスに照らして業務のベンチマークを行うことを銀行に要求しています。

さらに、2020 年には、米国連邦準備制度が「Sound Practices to Strengthen Operational Resilience」(オペレーショナルレジリエンス強化のためのサウンドプラクティス) を公表しました。これは、既存の規制、ガイダンス、意見表明書、業界標準から導かれた、オペレーショナルレジリエンスを高めるための手順の概要を示すものです。このプラクティスは、効果的なガバナンスおよびリスク管理テクニックに基づいており、サードパーティーのリスクが考慮され、回復力のある情報システムが含まれます。

特にクラウドに関しては、米国財務省が 2023 年 2 月に「The Financial Services Sector' s Adoption of Cloud Services」(金融サービスセクターのクラウドサービス導入) を公開しました。この報告書は、金融サービス機関がクラウドサービスを使用したときに、どのような利点が利用者にもたらされるのかを示しています。これには、「コストの削減、新しい情報テクノロジー (IT) 資産を迅速にデプロイする能力、新製品や新サービスの開発期間の短縮、セキュリティと回復力の能力強化」が含まれます。また、金融セクターによるクラウドサービス使用時の回復力を支援するための、財務省の戦略的ビジョンも概説しています。これには、クラウドサービスの使用で金融セクターのオペレーショナルレジリエンスを促進するための長期的な目標が含まれます。この戦略的ビジョンは、将来にわたる財務省の民間セクターおよび国内外の同等組織への関与について指針となるものです。

クラウドにおけるセキュリティ：セキュリティのカルチャーを構築する

クラウドは、金融サービス機関でセキュリティのカルチャーを構築し、コンプライアンスを合理化するための強力な推進力となります。

増え続ける脅威とリスク、さらにはオペレーショナルレジリエンスの必要性の高まりにより、クラウドへの移行は引き続き進むと考えられます。クラウドでは、組織のあらゆる活動にセキュリティを組み込むことができます。AWS は、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、組織のあらゆる側面にセキュリティを組み込み、継続的な改善を行うことが容易になっていると認識しています。

クラウドの力はオペレーショナルレジリエンスにも及びます。これにより CSP は、ビジネス継続性を確保するために必要となる地理的な多様性やインフラストラクチャの冗長性を効果的に実現できます。こうした冗長性を金融サービス機関が独自に構築して管理した場合には、多大な投資や大量のリソースが必要となり、イノベーションや成長を生み出すプロジェクトに集中できなくなるおそれがあります。

AWS 責任共有モデル

セキュリティとコンプライアンスは、AWS とお客様の間で共有される責任です。この共有モデルは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理的なセキュリティに至るまで、さまざまなコンポーネントを AWS が運用、管理、およびコントロールするため、お客様の運用負担を軽減できます。お客様は、ゲストオペレーティングシステム (更新やセキュリティパッチを含む)、その他の関連アプリケーションソフトウェア、AWS より提供されるセキュリティグループファイアウォールの設定に関する責任と管理を担います。

お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用可能な法律および規制に応じて異なります。したがって、お客様は選択するサービスを注意深く検討する必要があります。また、この責任共有モデルの性質によって柔軟性が得られ、お客様がデプロイを統制できます。次のページの図に示すように、この責任分担は一般に、「クラウドのセキュリティ」と「クラウドにおけるセキュリティ」と呼ばれます。

AWS の責任：クラウドのセキュリティ

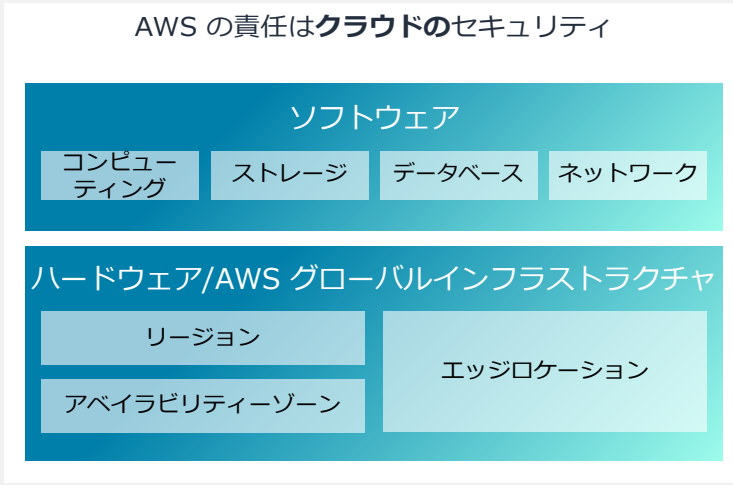
AWS は、AWS クラウドで提供されるすべてのサービスを実行するインフラストラクチャの保護について責任を負います。このインフラストラクチャは、AWS クラウドサービスを実行するハードウェア、ソフトウェア、ネットワーク、および施設で構成されています。

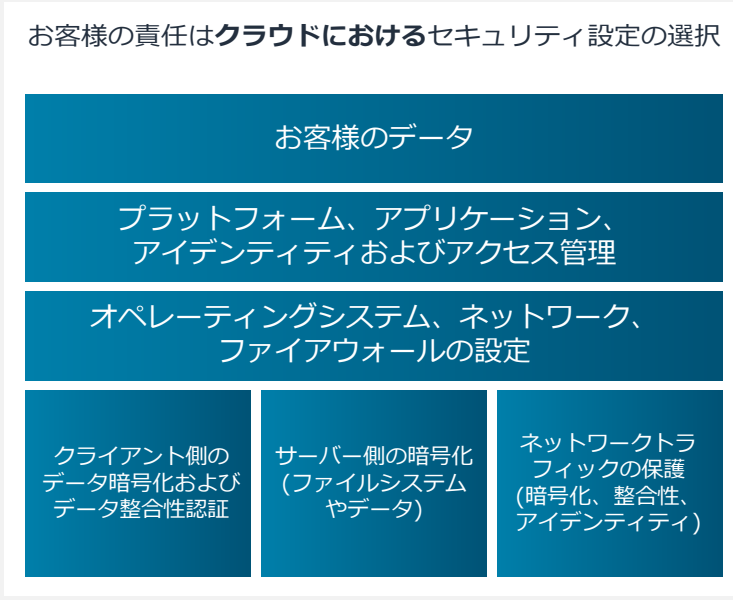
お客様の責任：クラウドにおけるセキュリティ

お客様の責任は、お客様が選択した AWS クラウドサービスによって決まります。これにより、お客様がセキュリティの責任の一部として実行する必要がある設定作業の量が決まります。お客様は、データの管理 (暗号化オプションを含む)、アセットの分類、アイデンティティとアクセスの管理ツールを使用した適切なアクセス許可の適用について責任を負います。

この責任共有モデルは IT 統制もカバーします。IT 環境を運用する責任を AWS とお客様の間で分担するのと同様に、IT 統制の管理、運用、検証も分担となります。AWS 環境にデプロイした物理インフラストラクチャに関連する統制を、それまでお客様が管理していた場合は、AWS が管理することでお客様を支援します。

お客様によって AWS でのデプロイ方法は異なるため、お客様は特定の IT 統制管理を AWS に移行できるというメリットを活用して、新しい分散統制環境を構築できます。その後、必要に応じて AWS の統制およびコンプライアンスドキュメントを使用して、統制の評価および検証手順を実行できます。





AWS のベストプラクティスの導入

すべてのクラウドが同じように、セキュリティとコンプライアンスの確保や促進を行うわけではありません。AWS を使用すれば、金融サービス機関は、今日においてトップレベルの柔軟性とセキュリティを誇るクラウドコンピューティング環境で、ビジネスを運営するために必要な統制と自信を手に入れることができます。金融サービス機関は、AWS リージョンとアベイラビリティーゾーンの回復力や、情報、アイデンティティ、アプリケーション、デバイスを保護するように設計されたインフラストラクチャからメリットを得ることができます。AWS により、金融サービス機関は包括的なサービスと機能を利用して、データのローカリゼーション、保護、機密性など、中核となるセキュリティおよびコンプライアンスの要件を満たす能力を向上させることができます。

金融サービス機関は AWS を利用して、検出や修復といった手動のセキュリティタスクを自動化し、ビジネスの拡大とイノベーションに集中することができます。さらに、AWS は、精査の上でトップシークレットのワークロードに対して十分なセキュリティがあると認められたサービスおよび関連サプライチェーンを持つ唯一の商用クラウドであり、金融サービス機関はそのメリットを享受できます。

セキュリティ、コンプライアンス、プライバシーの最高水準を確保

AWS は、今日においてトップレベルのセキュリティを誇るクラウド環境となるように設計されており、クラウドセキュリティツール群で強化され、300 を超えるセキュリティ、コンプライアンス、ガバナンスのサービスや機能が揃っています。つまり、AWS のお客様にも、きわめて包括的なセキュリティおよびコンプライアンスの統制が適用されます。

AWS は、国際標準化機構 (ISO)、Payment Card Industry Data Security Standard (PCIDSS)、System and Organization Controls (SOC)、FedRAMP、GDPR など、143 のセキュリティ基準やコンプライアンス認証に対応しており、世界中の大多数の規制機関が定めるコンプライアンス要件への準拠を支援しています。さらに、お客様のデータを保存する AWS の 117 のサービスすべてで、データ暗号化機能を提供しています。

AWS は、進化するオペレーショナルレジリエンス要件に対応するため、31 の地理的リージョンに 99 のアベイラビリティーゾーンを有し、クラウドプロバイダーの中で最大規模のフットプリントを誇ります。また、5 つのリージョンに 15 のアベイラビリティーゾーンを追加する計画も発表しています。さらに、AWS グローバルインフラストラクチャは、クラウドプロバイダーの中でもきわめて優れたネットワーク可用性を提供します。

Capital One

2020 年、**Capital One** は 8 つのデータセンターをすべて AWS に移行し、クラウド上ですべて業務を行う米国初の銀行となりました。ある 1 つのワークロードを AWS に移行する前に、同行内のさまざまなグループを関与させ、AWS と連携してリスクフレームワークを構築しました。これはオンプレミス環境のセキュリティおよびコンプライアンスと同様の高水準を満たすものです。Capital One はこの移行を成功させるため、人とテクノロジーの両方を活用しました。同行は、アプリケーションのクラウドへの移行に際して、リスクマネージャーとクラウドエンジニアで構成されるクラウドガバナンス機能グループを設立し、機能やコントロールを厳選しました。また、Cloud Custodian と呼ばれるコンプライアンス適用エンジンを開発し、オープンソース化しました。これにより、ポリシー違反の検出と修正を自動化して、顧客のためにイノベーションを進めるチームの能力を制限することなく、チームのコンプライアンス違反を防いでいます。

強力なデータコントロールを維持

アクセスしにくいデータでは意味がありません。金融サービス機関は、AWS を利用して安全性の高いグローバルインフラストラクチャにシステムを構築でき、暗号化、移動、保持の管理を含め、自社のデータを自社で所有してアクセスを管理できます。AWS に組み込まれたきめ細かいアクセスコントロールにより、適切なリソースが適切なレベルで適切なデータにアクセスするという確信が得られます。さらに、AWS インフラストラクチャは、データを物理的に配置している場所をお客様が常に完全に制御し、データレジデンシーに関する要件を満たせる設計になっています。

National Australia Bank (NAB) は AWS でクラウドファースト戦略を導入し、新しいサービスで世界中の 900 万を超える顧客のカスタマーエクスペリエンスと財務成果を向上しています。すべての AWS ワークロードを保護し、クラウド上の顧客データを保護するため、NAB は Amazon GuardDuty を使用しています。Amazon GuardDuty は、悪意のある行為や不正行為について継続的にアカウントの活動をモニタリングする、フルマネージドのインテリジェントな脅威検出サービスです。

自動化によるリスクの軽減

金融サービス機関は、ビジネス要件、常に拡大と進化を続ける脅威ベクトル、変化する規制要件に対応するため、セキュリティプロセスの自動化を推進したいと考えています。自動化により設定のヒューマンエラーを減らしてセキュリティを高めながら、イノベーションと成長のためのプロジェクトにリソースを移すことができます。

AWS は、オンプレミス実装では不可能な規模で、エンタープライズがセキュリティおよびコンプライアンス機能を自動化できるようにします。セキュリティライフサイクル全体にわたるエンドツーエンドの自動化機能が、影響を最適化するために重要であり、これを理解することが大切です。

AWS は、数多くの手動のセキュリティタスクを堅牢に自動化します。例えば、AWS Identity and Access Management Access Analyzer は人間の介入を必要としない自動化を支援し、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をより詳細に把握できます。Amazon GuardDuty、AWS CloudTrail などの AWS のサービスは、ログ記録、モニタリング、悪意のあるアクティビティへの対処などのタスクを、組織独自のセキュリティおよびコンプライアンスニーズに従って自動化します。AWS Audit Manager は、お客様がポイントインタイムの手動評価に頼ることなく、コンプライアンスフレームワークのエビデンス収集を自動化します。

また、金融サービス機関は AWS Systems Manager を使用して、ハイブリッド環境でのインフラストラクチャとアプリケーションのセキュリティチェックを自動化できます。これにより、オンプレミス環境のシームレスでセキュアな拡張として AWS を簡単に統合できます。

50 を超える国に拠点を持つ多国籍保険会社である **AXA** は、数百のワークロードを規制に準拠したセキュアな方法で実行できるようにしながら、クラウド移行を拡大したいと考えていました。AXA は、管理とセキュリティに関する AWS の 11 のサービスを使用して、同社の移行を加速するためのグローバルランディングゾーンを作成しました。同社は、CI/CD パイプラインを構築してランディングゾーンの配信を自動化し、使用量とリスクの全体的な状況を継続的に把握するためのクラウドデータレイクを構築しました。AXA のローカルチームは、コンプライアンスを一元的にモニタリングおよび統制しながら、ランディングゾーンテンプレートのテスト、検証、変更の提案を自律的に行えるようになりました。

まとめ：
AWS のパワー – 世界で高い信頼を得ているクラウド

自信を持ってイノベーションを加速 – アイデアを迅速にアクションへ

金融サービス機関は、AWS のソリューションとサービスを使用して、迅速に、そして自信を持って、アイデアを実装に移すことができます。AWS の幅広いセキュリティ機能と自動化へのフォーカスにより、金融サービス機関は、最初から「適切な構築」を進めるために必要なリソースを得ることができます。また、最高水準のセキュリティを維持しながら、イノベーションにかける労力を最適化できます。

オペレーショナルレジリエンスの構築

オペレーショナルレジリエンスを実証するための新しい要件に直面している金融サービス機関にとって、AWS は有益なパートナーとなります。AWS は、障害やインシデントから保護することを意図して構築されており、AWS のサービスの設計もこの要素を考慮しています。そのため、障害やインシデントが発生した場合、お客様への影響とサービスの継続性への影響は可能な限り抑えられます。AWS リージョンおよびアベイラビリティーゾーンモデルは、高可用性が求められるエンタープライズアプリケーションの実行に推奨されるアプローチとして、Gartner より認められています。

- AWS のインフラストラクチャは、5 つの大陸に地理的に分散されています。31 の地理的リージョンがあり、それらは 99 の AWS アベイラビリティーゾーンで構成されています。各アベイラビリティーゾーンには複数のデータセンターがあります。
- AWS アベイラビリティーゾーンは物理的に分離され、相互に独立しています。また、局所的な障害に耐えるよう、高度な冗長性を備えたネットワークで構築されています。
- AWS リージョンは相互に分離され、各リージョンには専用のインフラストラクチャスタックとサービスがあるため、1 つのリージョンで障害が発生しても、他のリージョンには影響しません。今日のグローバルな金融機関のオンプレミス環境と比較すると、AWS インフラストラクチャの地域的な多様性により、地理的集中リスクが大幅に軽減します。
- AWS は、インフラストラクチャとサービスにわたって区分化を導入しています。また、さまざまなレベルの独立した冗長コンポーネントを提供する複数のコンストラクトがあります。
- AWS は、サービスの複数のインスタンス化を含む、相互に分離されたセルベースアーキテクチャを使用しています。この設計により、1 つのセルの障害によって他のセルに障害が起こるという可能性が最小限に抑えられます。

サイバーイベントリカバリの拡大

金融サービス機関は、サイバーイベントリカバリプラットフォームを AWS 上に構築しています。これは、オンプレミスでサイバーデータボールトを作成するには数か月かかるのに対して、AWS なら数分で簡単に済むためです。小さく始め、使用した分のみに対して支払い、データの増大に伴って拡大できます。複数のセキュリティサービスを使用して、モダンなサイバーイベントリカバリプラットフォームを構築することもできます。

セキュリティとコンプライアンスの合理化と簡素化

自動化は、セキュリティとコンプライアンスを合理化、簡素化するための鍵となります。AWS は、業界でもきわめて幅広いソリューションを提供し、大規模な自動化を可能にします。

AWS はお客様の管理の実装を包括的にサポート


ID とアクセス管理


検知


インフラストラクチャ保護


データ保護


インシデント対応


コンプライアンス & ガバナンス

さらに、今後数年で、AI/機械学習がセキュリティエンジニアの能力強化に非常に大きな役割を果たすようになるでしょう。これにより、エンジニアはよりセキュアなアーキテクチャやアプリケーションをクラウドで開発し、継続的な改善を推進できます。AI/機械学習の予測機能により、金融機関は、進化し続ける脅威の状況に対し、より能動的なセキュリティ体制を作ることができます。

bowtie

イノベーションの実現例

香港初のオンライン保険会社である Bowtie は、セキュリティと可用性に優れた環境での運用を必要としていました。Bowtie は、Amazon GuardDuty を使用して独自のセキュリティアラートシステムを構築しました。このシステムでは、Amazon Virtual Private Cloud (Amazon VPC)、Amazon Route 53、AWS CloudTrail など、複数の AWS のサービスのログをモニタリングしています。システムで異常が検知されると自動的に Bowtie のクラウドチームに通知が送られるため、すばやい対応が可能になり、プラットフォームの安全性とセキュリティを確保しながら、顧客に引き続き新しいサービスを提供できます。

AWS が提供するもの

AWS のアーキテクチャは、現在提供されているクラウド環境の中でもきわめて高いセキュリティ、スケーラビリティ、回復力を持つように設計されています。非常に強力なクラウドセキュリティツール群で要塞化を後押しします。クラウドの柔軟性を自信を持って取り入れて活用するために必要なテクノロジー、リソース、業界専門知識を見つけましょう。

クラウドアプリケーションのセキュリティを今すぐ強化する ›

aws FOR FINANCIAL SERVICES