AWS における GDPR コンプライアンスに関する情報提供

AWS ホワイトペーパー

AWS における GDPR コンプライアンスに関する情報提供: AWS ホワイトペーパー

Table of Contents

AWS における GDPR コンプライアンスに関する情報提供

公開日: 2020 年 12 月 (改訂履歴 (p. 26))

要約

このドキュメントでは、お客様のアクティビティに適用される可能性がある一般データ保護規則 (GDPR) の要件に適合させるために、アマゾン ウェブ サービス (AWS) で用意されているサービスとリソースに関する情報を提供します。これには、IT セキュリティスタンダードの遵守や、AWS クラウドコンピューティングコンプライアンスコントロールカタログ (C5) 認証、クラウドインフラストラクチャサービス (CISPE) の行動規範の遵守、データアクセスコントロール、モニタリングとロギングツール、暗号化、キー管理が含まれます。

一般データ保護規則の概要

一般データ保護規則 (GDPR) は、2018 年 5 月 25 日に施行可能になった欧州プライバシー法 (欧州議会および 2016 年 4 月 27 日の理事会の規則 2016/679) です。GDPR は、EU データ保護指令 (指令 95/46/EC) に取って代わるもので、各 EU 加盟国に拘束力を持つ唯一のデータ保護法を適用することにより、欧州連合 (EU) 全体でデータ保護法に親和性を持たせることを目的とします。

GDPR は、EU 域内に事業所を有する組織による個人データの処理すべてに対して、または EU 居住者の個人データを処理して EU 域内の個人へ商品やサービスを提供する、あるいは EU 域内における EU 居住者の行動のモニタリングを行う組織に対して適用されます。個人データは、特定のあるいは識別可能な自然人に関する情報を指します。

GDPR により EU 域内で活動する組織が導入すべき変更

GDPR の重要な側面の 1 つは、個人データの安全な処理、使用、やり取りの方法について、EU 加盟国間で一貫性を持たせることです。各組織は、技術的、組織的な措置および個人データの処理に適用されるコンプライアンスポリシーの実施と、定期的な見直しにより、処理するデータのセキュリティおよび GDPR への準拠を継続的に証明する必要があります。EU の監督当局は、GDPR 違反に対して最大 2,000 万ユーロ、または全世界の年間売上高の 4% 相当額のいずれか高い方の罰金を科すことができます。

GDPR に対する AWS の準備

AWS のコンプライアンスやデータ保護、セキュリティのエキスパートは、世界中のお客様からの質問に答え、GDPR の下でクラウドにおけるワークロードの実行準備を支援します。また、エキスパートチームは GDPR の要件に対する AWS の対応状況も確認します。

> Note
>
> AWS のサービスはすべて GDPR に準拠して使用できます。

AWS データ処理補遺条項 (DPA)

AWS では、お客様が GDPR 契約の義務に準拠できるように、GDPR に準拠したデータ処理補遺条項 (GDPR DPA) が用意されています。AWS GDPR DPA は AWS のサービス条件に組み込まれており、GDPR 準拠のために GDPR DPA を必要とする世界中のすべてのお客様に自動的に適用されます。

2020 年 7 月 16 日、欧州連合 (EU) 司法裁判所 (CJEU) は、「モデル条項」として知られる EU-US プライバシーシールドおよび標準契約条項 (SCC) に関する判決を下しました。 この判決で CJEU は、欧州連合 (EU) から米国 (US) への個人データの転送に関して、EU-US プライバシーシールドはもはや有効ではないと判断しました。しかし、同じ判決で CJEU は、EU 外へのデータ転送メカニズムとして企業が引き続き SCC を 使用するのは有効としました。

この判決に従い、AWS のお客様およびパートナーは、一般データ保護規則 (GDPR) を含む EU のデータ保護法に準拠して、ヨーロッパから米国およびその他の国に引き続き AWS を使用してコンテンツを転送することができます。AWS のお客様は、GDPR に準拠して欧州連合外にデータを転送することを選択した

場合、AWS データ処理補遺条項 (DPA) に含まれる SCC に依拠することができます。規制および法的な状況の進展にあわせて、AWS はお客様およびパートナーがどこで事業を運営していても、AWS のメリットを享受し続けることができるように努めます。詳細については、EU-US プライバシーシールドに関するよくある質問を参照してください。

GDPR における AWS の役割

AWS は、GDPR の下でデータ処理者とデータ管理者と両方の役割を担います。

第 32 条は、管理者と処理者が「適切な技術的、組織的措置の実施」において「実施措置の最新性と実装コスト、処理の種類、範囲、背景と目的、そして自然人の権利と自由に影響を及ぼす可能性があり重大なリスク」について考慮することを義務付けています。GDPR では、どのようなセキュリティ措置が必要となるかについて、以下を含む具体的な提案を行っています。

- 個人データの仮名化と暗号化。
- システムとサービスの処理における現存の機密性と完全性、可用性、復元力を確実にする機能。
- 物理的あるいは技術的事由が発生したときに、適時に個人データの可用性とアクセスを復元する機能。
- 処理のセキュリティを確保するために、技術的および組織的な措置の有効性を定期的にテスト、判定、評価するプロセス。

データ処理者としての AWS

お客様と AWS パートナーネットワーク (APN) パートナーが AWS のサービスを使用してコンテンツ内で個人データを処理する際、AWS はデータ処理者としての役割を担います。お客様と APN パートナーは、個人データを処理するために、セキュリティ設定の管理など AWS のサービスで利用可能な管理手段を行使できます。そのような場合、お客様または APN パートナーが、データ管理者またはデータ処理者としての役割を担うことがあり、その際は AWS がデータ処理者または副処理者としての役割を担います。AWS GDPR 準拠のデータ処理補遺条項 (DPA) には、データ処理者としての AWS のコミットメントが組み込まれています。

データ管理者としての AWS

AWS が個人データを収集し、その個人データを処理する目的と手段を決定した場合、AWS はデータ管理者としての役割を担います。例えば、AWS がアカウント登録、管理、サービスへのアクセスのためのアカウント情報を処理する場合や、カスタマーサポート活動を通じて支援するために AWS アカウントの連絡先情報を処理する場合、AWS はデータ管理者としての役割を果たします。

責任分担セキュリティモデル

セキュリティとコンプライアンスは、AWS とお客様の共有責任です。お客様がコンピュータシステムやデータをクラウドに移行すると、セキュリティに関する責任はお客様とクラウドサービスプロバイダの間で分担することになります。お客様が AWS クラウドに移行した場合、AWS には AWS クラウドで提供されるすべてのサービスを実行するグローバルインフラストラクチャを保護する責任があります。Amazon S3 や Amazon DynamoDB などの抽象化されたサービスの場合、AWS はオペレーティングシステムとプラットフォームのセキュリティにも責任を負います。データ管理者またはデータ処理者の役割を担うお客様と APN パートナーは、クラウドに入れるものや、クラウドへ接続するものすべてに責任を負います。この責任の相違は通常、「クラウド自体の」セキュリティと「クラウド内における」セキュリティと呼ばれます。この共有モデルにより、お客様の運用上の負担が軽減され、AWS クラウド内にインフラストラクチャをデプロイするために必要な柔軟性と制御を備えることができます。詳細については、「AWS 責任共有モデル」を参照してください。

AWS 責任共有モデルが GDPR によって変わることはなく、クラウドコンピューティングサービスの使用に重点を置くお客様と APN パートナーにとって引き続き重要になります。責任共有モデルは、GDPR に基づいた AWS のさまざまな責任 (データの処理者または補助処理者として)、ならびにお客様と APN パートナーの責任 (データ管理者またはデータ処理者として) を説明するために役立つアプローチです。

強力なコンプライアンスフレームワークとセキュリティスタンダード

GDPR に準じて、適切な技術的および組織的措置には「(...) 処理するシステムおよびサービスの現存の機密性と完全性、可用性、復元力を確実にする機能」、そして信頼できる復元、テストおよび全体的なリスクマネジメントプロセスを含める必要性が生じることがあります。

AWS コンプライアンスプログラム

AWS は、グローバルな業務全般にわたり、セキュリティとコンプライアンスに関して高い水準を継続的に維持しています。セキュリティは常に私たちの最優先事項であり、まさに「ジョブゼロ (ビジネスの大前提)」です。 AWS は定期的に独立したサードパーティーによる認証監査を受け、制御活動が意図通りに機能していることを保証しています。具体的には、AWS は、地域や業界によって異なるさまざまなグローバルおよびリージョンのセキュリティフレームワークに対して監査を受けています。現在、AWS は 50 を超える監査プログラムに参加しています。

これらの監査の結果は評価機関によって文書化され、AWS Artifact からすべての AWS のお客様が利用できるようになっています。AWS Artifact は、AWS コンプライアンスレポートにオンデマンドでアクセスできる、無料のセルフサービスポータルです。新しいレポートがリリースされると、AWS Artifact で入手できるようになります。お客様は AWS のセキュリティとコンプライアンスを継続的に監視することが可能で、新しいレポートにも即座にアクセスできます。

お客様は、クラウドセキュリティに関する ISO 27017、クラウドプライバシーに関する ISO 27018、SOC 1、SOC 2、SOC 3、PCI DSS レベル 1 などの厳格な国際規格への準拠を実証する、国際的に認められた認証および認定を活用できます。また AWS は、ドイツ政府発行の認証である BSI のコモンクラウドコンピューティングコントロールカタログ (C5) など、ローカルなセキュリティ基準を満たせるようにお客様を支援します。

AWS 認定プログラム、レポート、サードパーティー認証の詳細については、「AWS コンプライアンスプログラム」を参照してください。サービス固有の情報については、「対象範囲内の AWS のサービス」を参照してください。

クラウドコンピューティングコンプライアンスコントロールカタログ

クラウドコンピューティングコンプライアンスコントロールカタログ (C5) は、ドイツ連邦情報セキュリティ局 (BSI) によってドイツで導入された、ドイツ政府が支援する認証スキームです。これは、ドイツ政府の「クラウドプロバイダーに対するセキュリティ勧告」に照らして、一般的なサイバー攻撃に対する運用上のセキュリティを組織が実証できるようにするために作成されました。

データ保護の技術的および組織的対策および情報セキュリティ対策は、機密性、完全性、可用性を確保するためのデータセキュリティを対象としています。C5 では、データ保護にも関連するセキュリティ要件を定義しています。AWS のお客様やコンプライアンスアドバイザーは C5 認証をリソースとして使用することにより、ワークロードをクラウドに移行する際に AWS で提供される IT セキュリティ保証サービスの範囲を把握できます。C5 では、クラウド特有のコントロールの追加とともに、IT 基本保護法 (IT-Grundschutz) と同等の規制上定義された IT セキュリティレベルが追加されます。

C5 では、データのロケーション、サービスのプロビジョニング、管轄の場所、既存の認定、情報公開義務、および全サービスの説明に関連した情報を提供する詳細なコントロールも追加されます。この情報を利用することで、お客様は法規制 (データプライバシーなど)、お客様独自のポリシー、脅威環境が、クラウドコンピューティングサービスの使用にどう関わってくるかを評価できます。

データアクセス制御

GDPR 第 25 条は、管理者が「適切な技術的および組織的措置を実施することで、原則として、必ず特定の処理目的ごとに必要な個人データのみが処理されるようにしなければならない」と定めています。ここで紹介する AWS のアクセスコントロールメカニズムは、認証されたシステム管理者や、ユーザー、アプリケーションのみがAWS リソースとカスタマーデータへアクセス可能にすることで、お客様がこの要件に準拠するよう支援します。

AWS Identity and Access Management

AWS アカウントを作成すると、AWS アカウントの「ルート」ユーザーアカウントが自動的に作成されます。このユーザーアカウントには、お客様の AWS アカウントのすべての AWS のサービスおよびリソースに対する完全なアクセス権が付与されます。このアカウントは日常的なタスクに使用するのではなく、追加のロールとユーザーアカウントを最初に作成する場合や、このアカウントを必要とする管理作業にのみ使用してください。AWS では、タスクごとに異なるユーザーアカウントとロールを定義し、各タスクを完了するために必要な最小限のアクセス権限を指定するという、最小特権の原則を最初から適用することを推奨しています。このアプローチは、GDPR で導入された重要な概念である「設計によるデータ保護」に合致させるためのメカニズムです。AWS Identity and Access Management (IAM) は、AWS リソースへのアクセスを安全にコントロールするために使用できるウェブサービスです。

特定のアクセス権限を持つ IAM ID をユーザーとロールで定義します。認証されたユーザーは、特定のタスクを実行できる IAM ロールを担うことができます。ロールを担う際に一時的な認証情報が作成されます。例えば、IAM ロールを使用して、Amazon S3 バケットや Amazon Relational Database Service (Amazon RDS)、Amazon DynamoDB データベースなど、他の AWS リソースへのアクセスに必要な一時的な認証情報を、Amazon Elastic Compute Cloud (Amazon EC2) で実行されるアプリケーションに対して安全に提供できます。同様に、実行ロールは、Amazon CloudWatch Logs などの他の AWS のサービスやリソースにアクセスしてログをストリーミングしたり、Amazon Simple Queue Service (Amazon SQS) キューからのメッセージを読み込むために必要な権限と併せて AWS Lambda 機能を提供したりします。ロールを作成したら、そのロールにポリシーを追加して認証を定義します。

お客様がリソースポリシーを監視し、意図しないパブリックアクセスまたはクロスアカウントアクセスがあるリソースを特定するためには、IAM Access Analyzer を有効にすると、AWS アカウントの外部からアクセスできるリソースを特定する包括的な検出結果を生成できます。IAM Access Analyzer は、ポリシーで許可されたアクセスパスで使用可能なものを決定するために、数学的な口ジックや推論を使ってリソースポリシーを評価します。IAM Access Analyzer は、新しいポリシーや更新されたポリシーを継続的にモニタリングし、IAM ロールのポリシーだけでなく、Amazon S3 バケットやAWS Key Management Service (AWS KMS) キー、Amazon SQS キュー、Lambda 関数といったサービスリソースのポリシーを使って付与されたアクセス権限を分析します。

Access Analyzer for S3 は、インターネット上の任意のユーザーや他の AWS アカウント (組織外の AWS アカウントを含む) にアクセスを許可するように設定されているバケットに関するアラートを出します。Access Analyzer for Amazon S3 でリスクのあるバケットを確認した場合、バケットへのすべてのパブリックアクセスをワンクリックでブロックできます。AWS では、特定のユースケースをサポートするためにパブリックアクセスが必要な場合を除き、バケットへのすべてのアクセスをブロックすることを推奨しています。すべてのパブリックアクセスをブロックする前に、アプリケーションがパブリックアクセスなしで正常に動作することを確認してください。詳細については、「Amazon S3 を使用したパブリックアクセスのブロック」を参照してください。

IAM では、未使用のアクセス権限を特定して、関連付けられているプリンシパルから削除できるように、最終アクセス情報も提供されます。最終アクセス情報を使用して、ポリシーを絞り込み、必要なサービスとアクションに対してのみアクセスを許可することが可能です。これにより、最小特権のベストプラク

ティスを忠実に守り、適用できるようになります。 IAM または AWS Organizations 環境全体にわたって存在するエンティティまたはポリシーの最終アクセス情報を表示できます。

AWS STS による一時アクセストークン

AWS Security Token Service (AWS STS) を使用して、AWS リソースへのアクセス権限付きの一時的なセキュリティ認証情報を作成し、信頼されたユーザーに提供することができます。一時的なセキュリティ認証情報の機能は、IAM ユーザーに提供される長期的なアクセスキー認証情報とほぼ同じですが、次の相違点があります。

- 一時的なセキュリティ認証情報は、短期的な使用のためのものです。有効期間は 15 分から最長 12 時間まで設定できます。一時的な認証情報の有効期限が切れると、AWS はその認証情報を認識せず、その認証情報を使用して行われた API リクエストからのいかなる種類のアクセスも許可しません。
- 一時的なセキュリティ認証情報は、ユーザーアカウントと一緒に保存されません。代わりに、動的に生成され、リクエストされた時にユーザーに提供されます。一時的なセキュリティ認証情報の有効期限が切れた場合は (または期限が切れる前に)、新しい認証情報をリクエストする権限があるユーザーであればリクエストできます。

これらの違いにより、一時的な認証情報を使用する場合に次のような利点があります。

- 長期の AWS セキュリティ認証情報をアプリケーションに配布したり埋め込んだりする必要がありません。
- 一時的な認証情報はロールおよび ID フェデレーションの基本となります。一時的な AWS ID を定義することで、AWS リソースへのアクセスをユーザーに提供できます。
- 一時的なセキュリティ認証情報には、制約付きのカスタマイズ可能な有効期間があります。このため、認証情報が不要になったときに、ローテーションしたり、明示的に無効にしたりする必要はありません。一時的なセキュリティ認証情報の有効期限が切れると、再利用はできません。認証情報が有効な最長期間を指定できます。

多要素認証

セキュリティ強化のために、AWS アカウントおよび IAM ユーザーに 2 要素認証を追加できます。多要素認証 (MFA) を有効にすると、AWS マネジメントコンソールにサインインしたときに、ユーザー名とパスワード (第 1 要素)、および AWS MFA デバイスからの認証応答 (第 2 要素) の入力を求められます。MFA は AWS アカウントに対して有効にすることも、そのアカウント内に作成した IAM ユーザーに対して個別に有効にすることも可能です。MFA を使用して AWS サービス API へのアクセスをコントロールすることもできます。

例えば、Amazon EC2 のすべての AWS API オペレーションへのフルアクセスを許可する一方、ユーザーが MFA で認証されていない場合は`StopInstances` や `TerminateInstances` などの特定の API オペレーションへのアクセスを明示的に拒否するように、ポリシーを定義できます。

```
{
 “Version”: “2012-10-17”,
 “Statement”: [
     {
        “Sid”: “AllowAllActionsForEC2”,
        “Effect”: “Allow”,
        “Action”: “ec2:*”,
        “Resource”: “*”
     },
    {
```

```
                "Sid": "DenyStopAndTerminateWhenMFAIsNotPResent",
                "Effect": "Deny",
                "Action": [
                    "ec2:StopInstances",
                    "ec2:TerminateInstances"
                ],
                "Resource": "*",
                "Conditions": {
                    "BoolIfExists": {"aws:MultiFactorAuthPresent":false}
                }
            }
        }
}
```

Amazon S3 バケットにさらにセキュリティレイヤーを追加するには、MFA Delete を設定することができます。MFA Delete は、バケットのバージョニング状態を変更してオブジェクトバージョンを完全に削除するために、追加の認証を必要とします。また、セキュリティ認証情報の侵害発生時のセキュリティを強化します。

MFA Delete を使用するために、認証コードの生成にはハードウェアまたは仮想 MFA デバイスを使用できます。サポートされているハードウェアまたは仮想 MFA デバイスのリストについては、多要素認証のページを参照してください。

AWS リソースへのアクセス

AWS リソースへのきめ細かなアクセスを実装するために、さまざまなリソースに対していろいろな人に異なるレベルのアクセス権限を付与できます。例えば、Amazon EC2、Amazon S3、DynamoDB、Amazon Redshift などの AWS のサービスへの完全なアクセスを一部のユーザーのみに許可できます。

他のユーザーには、一部の Amazon S3 バケットのみへの読み取り専用アクセスや、一部の Amazon EC2 インスタンスのみを管理する権限、あるいは請求情報のみへのアクセスを許可することができます。

次のポリシーは、特定の Amazon S3 バケットに対するすべてのアクションを許可し、Amazon S3 以外のすべての AWS のサービスへのアクセスを明示的に拒否するために使用できる 1 つの方法の例です。

```
    {
       "Version": "2012-10-17",
       "Statement": [
           {
              "Effect": "Allow",
              "Action": "s3:*",
              "Resource": [
                   "arn:aws:s3:::bucket-name",
                   "arn:aws:s3:::bucket-name/*"
               ],
            },
            {
              "Effect": "Deny",
              "NotAction": "s3:*",
              "NotResource": [
                   "arn:aws:s3:::bucket-name",
                   "arn:aws:s3:::bucket-name/*"
               ]
            }
        ]
}
```

ポリシーは、ユーザーアカウントまたはロールに付与できます。IAM ポリシーの他の例については、「IAM ID ベースのポリシーの例」を参照してください。

リージョナルサービスアクセスの境界の定義

お客様のコンテンツの所有権はお客様が保持します。また、お客様のコンテンツを処理、保存、ホストする AWS のサービスはお客様が選択します。いかなる目的であっても、AWS はお客様の同意を得ることなく、お客様のコンテンツにアクセスしたり、それを使用したりすることはありません。責任共有モデルに基づいて、コンテンツが保存される AWS リージョンをお客様が選択し、特定の地理的要件に従って、選択した場所に AWS のサービスをデプロイできます。例えば、コンテンツがヨーロッパのみに配置されるようにする場合、ヨーロッパの AWS リージョンの 1 つだけに AWS のサービスをデプロイするよう選択できます。

IAM ポリシーは、特定のリージョンのサービスへのアクセスを制限するシンプルなメカニズムを提供します。IAM プリンシパルに付与した IAM ポリシーにグローバル条件 (`aws:RequestedRegion`) を追加して、すべての AWS のサービスに強制することができます。例えば、次のポリシーでは、リクエストされたリージョンがヨーロッパではない場合、ステートメントに記載されていないすべてのアクションへのアクセスを明示的に拒否する `Deny` 効果を持つ `NotAction` エレメントを使用します。CloudFront、IAM、Amazon Route 53、AWS Support サービスでのアクションは、一般的な AWS グローバルサービスであるため、拒否されるべきではありません。

```
     {
        “Version”: “2012-10-17”,
        “Statement”: [
            {
               “Sid”: “DenyAllOutsideRequestedRegions”,
               “Effect”: “Deny”,
               “NotAction”: [
                     “cloudfront:*”,
                     “iam:*”,
                     “route53:*”,
                     “support:*”
                ],
                “Resource”: “*”,
                “Condition”: {
                   “StringNotLike”: {
                       “aws:RequestedRegion”: [
                             “eu-*”
                       ]
                    }
                }
            }
         ]
}
```

このサンプル IAM ポリシーは、AWS Organizations のサービスコントロールポリシー (SCP) として実装することもできます。SCP は、組織内の特定の AWS アカウントまたは組織単位 (OU) に適用されるアクセス権限の境界を定義します。これにより、複雑なマルチアカウント環境で、リージョンのサービスへのユーザーアクセスを制御できます。

新しく立ち上げられたリージョンには、地域制限機能があります。2019 年 3 月 20 日以降に導入されたリージョンは、デフォルトで無効になっています。これらのリージョンを使用するには、有効にする必要があります。ある AWS リージョンがデフォルトで無効になっている場合は、AWS マネジメントコンソールを使用してリージョンを有効または無効にできます。AWS リージョンを有効化または無効化することで、AWS アカウントのユーザーがそのリージョンのリソースにアクセスできるかどうかの制御が可能になります。詳細については、「AWS リージョンの管理」を参照してください。

ウェブアプリケーションとモバイルアプリケーションへのアクセスの制御

AWS では、お客様のアプリケーション内でのデータアクセス制御を管理するサービスを提供しています。ウェブアプリケーションやモバイルアプリケーションにユーザーログインとアクセス制御機能を追加する必要がある場合は、Amazon Cognito を使用できます。Amazon Cognito ユーザープールでは、何億人ものユーザー規模に対応する安全なユーザーディレクトリを作成できます。ユーザーの ID を保護するために、ユーザープールに多要素認証 (MFA) を追加できます。別の認証要素が必要な可能性があるときを予測するために、リスクベースのモデルを使うアダプティブ認証を使用することもできます。

Amazon Cognito ID プール (フェデレーテッド ID) を使用すると、誰がリソースにアクセスしたか、どこからアクセスが発生したか (モバイルアプリケーションまたはウェブアプリケーション) を確認できます。この情報を使用して、アクセス元の種類 (モバイルアプリケーションまたはウェブアプリケーション) と ID プロバイダーの種類に基づいて、リソースへのアクセスを許可または拒否する IAM ロールとポリシーを作成できます。

モニタリングとロギング

GDPR 第 30 条には、「(...) 各管理者および、必要に応じて管理者の代表者は、その責任下において処理活動の記録を維持する」と記載されてます。この条文には、すべての個人データの処理をモニタリングする際に、どの情報を記録すべきかについての詳細も記載されています。また、管理者と処理者は、侵害の通知をタイムリーに送信する必要があるため、インシデントを迅速に検出することが重要です。お客様がこれらの義務を履行できるように、AWS では以下のモニタリングおよびロギングサービスを提供しています。

AWS Config によるアセットの管理と設定

AWS Config では、AWS アカウントにあるさまざまなタイプの AWS リソースの設定を詳しく確認できます。表示にはリソース間の関係と設定の履歴が含まれるため、時間の経過とともに設定と関係がどのように変わったかを確認できます。

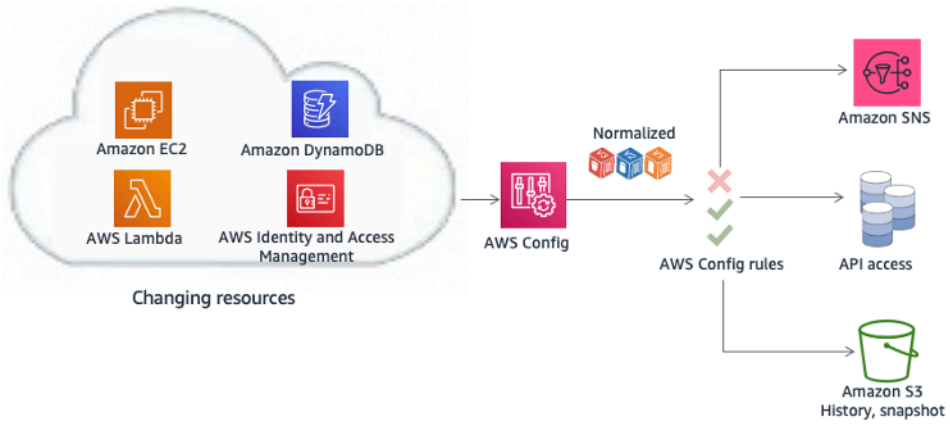

図 1 — AWS Config で設定の変更を時系列でモニタリングする

AWS リソースは、EC2 インスタンスや、Amazon Elastic Block Store (Amazon EBS) ボリューム、セキュリティグループ、Amazon Virtual Private Cloud (Amazon VPC) などの AWS で使用できるエンティティです。AWS Config でサポートされる AWS リソースすべてのリストについては、「サポートされている AWS リソースタイプ」を参照してください。

AWS Config では、次のことを実行できます。

- AWS リソース設定を評価して、設定が正しいことを確認する。
- AWS アカウントに関連付けられているサポート対象リソースの現在の設定のスナップショットを取得する。
- アカウント内にある 1 つ以上のリソースの設定を取得する。
- 1 つ以上のリソースの設定履歴を取得する。
- リソースが作成、変更、または削除されたら通知を受け取る。
- リソース間の関係を見る。特定のセキュリティグループを使用するすべてのリソースを検索するなど。

コンプライアンス監査とセキュリティ分析

AWS CloudTrail を使って、AWS アカウントアクティビティを継続的にモニタリングできます。AWS マネジメントコンソール、AWS SDK、コマンドラインツール、高レベルな AWS のサービスによる API コールを含む、アカウントの AWS API コールの履歴がキャプチャされます。CloudTrail をサポートするサービスの AWS API を呼び出したユーザーやアカウント、呼び出し元の IP アドレス、呼び出しの時間を特定できます。API を使用したアプリケーションへの CloudTrail の統合や、組織の証跡作成の自動化、証跡のステータスのチェック、管理者が CloudTrail ロギングを有効または無効にする方法の制御を行うことができます。

CloudTrail ログは、複数のリージョンと複数の AWS アカウントから 1 つの Amazon S3 バケットに集約できます。AWS では、ロギング用に指定された AWS アカウント (ログアーカイブ) で、アクセスが制限された Amazon S3 バケットにログ、特に AWS CloudTrail ログを書き込むことを推奨しています。バケットに対するアクセス許可は、ログの削除を防止する必要があります。また、Amazon S3 で管理された暗号化キー (SSE-S3)、または AWS KMS で管理されたキー (SSE-KMS) でサーバー側での暗号化を使って、保管中のログを暗号化する必要があります。CloudTrail ログファイルの整合性の検証は、CloudTrail がログファイルを配信した後に変更や削除、変更がなかったかどうかを判断するために使うことができます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュには SHA-256 、デジタル署名には RSA を使用した SHA-256 が使われています。これにより、検出されることなく、CloudTrail ログファイルをコンピュータで変更や削除、偽造することは困難になります。CloudTrail のファイル配信先にあるファイルの検証には、AWS Command Line Interface (AWS CLI) を使用できます。

Amazon S3 バケットに集められた CloudTrail ログは、監査目的で、またはトラブルシューティングのために分析できます。ログが一元化されたら、セキュリティ情報およびイベント管理 (SIEM) ソリューションと統合することや、ログを分析して Amazon QuickSight ダッシュボードで視覚化するために、Amazon Athena や CloudTrail Insights などの AWS のサービスを使用することができます。CloudTrail ログを一元化したら、同じ Log Archive アカウントを使用して、CloudWatch Logs や AWS ロードバランサーなどの他のソースからのログを一元化することもできます。

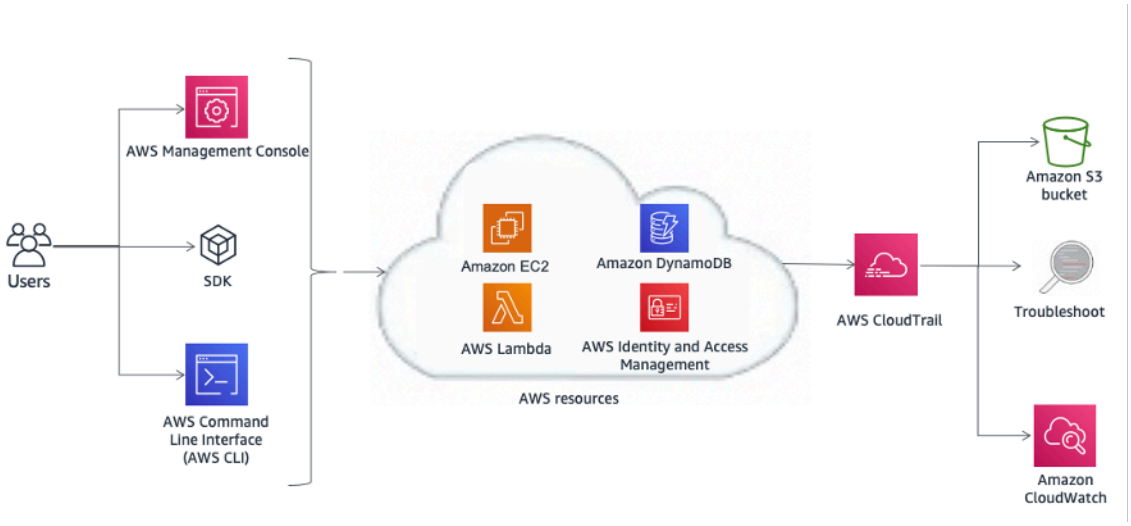

図 2 — AWS CloudTrail を使用したコンプライアンス監査とセキュリティ分析のアーキテクチャの例

AWS CloudTrail ログは、事前設定された Amazon CloudWatch Events を開始することもできます。イベントの発生をユーザーやシステムに通知したり、修復アクションのためにこれらのイベントを使うこともできます。例えば、Amazon EC2 インスタンスのアクティビティをモニタリングする場合、CloudWatch イベントルールを作成できます。Amazon EC2 インスタンスで特定のアクティビティが発生し、イベントがログにキャプチャされると、ルールによって AWS Lambda 関数が実行され、イベントに関する通知メールが管理者に送信されます。(図 3 を参照)。 メールには、イベントの発生日時、アクションを実行したユーザー、Amazon EC2 の詳細などの情報が含まれます。次の図は、イベント通知のアーキテクチャを示しています。

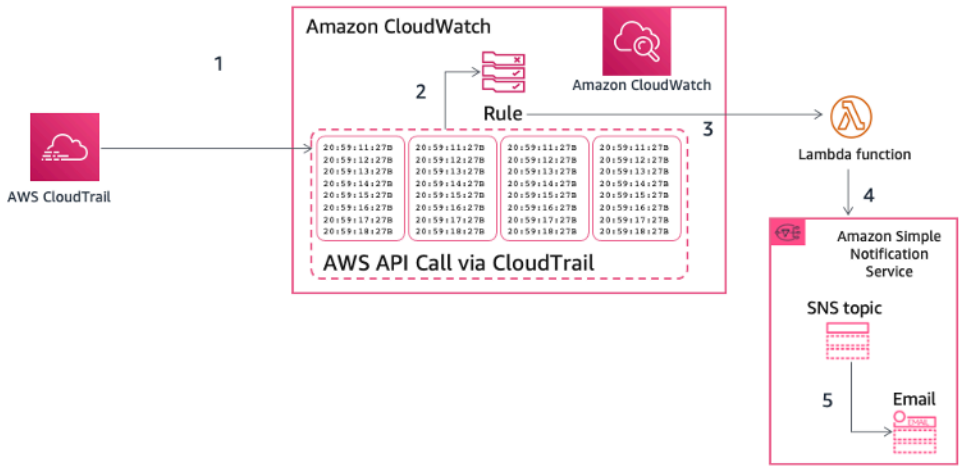

図 3 — AWS CloudTrail イベント通知の例

ログの収集と処理

Amazon EC2 インスタンスや、AWS CloudTrail、Route 53、その他のソースからのログファイルのモニタリング、保存、アクセスするために CloudWatch Logs を使用することができます。詳しくは「CloudWatch Logs にログを発行する AWS のサービス」を参照してください。

ログ情報には、次のような情報が含まれます。

- Amazon S3 オブジェクトへのアクセスの詳細なログ
- VPC-フローログによるネットワーク内のフローに関する詳細情報
- ルールベースの設定検証と AWS Config ルールによるアクション
- CloudFront でウェブアプリケーションファイアウォール (WAF) 機能を使用するアプリケーションへの HTTP アクセスのフィルタリングとモニタリング

Amazon EC2 インスタンスまたはオンプレミスサーバーに CloudWatch エージェントをインストールして、カスタムアプリケーションメトリクスとログを CloudWatch Logs に発行することもできます。

運用上の問題により効率的かつ効果的に対応できるようにクエリを実行する CloudWatch Logs インサイトを使って、ログをインタラクティブに分析することができます。

CloudWatch Logsは、サブスクリプションフィルターを設定することでほぼリアルタイムで処理され、カスタム処理や分析、他のシステムへの読み込みのために、Amazon OpenSearch Service (OpenSearch Service) クラスターや、Amazon Kinesis ストリーミング、Amazon Kinesis Data Firehose ストリーミング、Lambda など他のサービスに配信することが可能です。

CloudWatch メトリクスフィルターは、ログデータで検索するパターンの定義や、数値の CloudWatch メトリクスへの変換、ビジネス要件に基づくアラームの設定に使用できます。例えば、日常的なタスクに root ユーザーを使用しないという AWS の推奨に従い、CloudTrail ログ (CloudWatch Logs に配信される) に特定の CloudWatch メトリクスフィルターをセットアップしてカスタムメトリクスを作成し、AWS アカウントへのアクセスにルートの認証情報が使用されたら利害関係者に通知するためのアラームを設定できます。

Amazon S3 サーバーアクセスログや、Elastic Load Balancing アクセスログ、VPC フローログ、AWS Global Accelerator フローログなどのログは、Amazon S3 バケットに直接配信できます。例えば、Amazon

Simple Storage Service のサーバーアクセスログを有効にすると、Amazon S3 バケットに対して行われたリクエストに関する詳細情報を取得できます。アクセスログのレコードには、リクエストのタイプ、リクエストに指定されたリソース、リクエストが処理された日時など、リクエストの詳細が含まれます。ログメッセージの内容に関する詳細については、Amazon Simple Storage Service 開発者ガイドで「Amazon Simple Storage Server アクセスログの形式」を参照してください。サーバーアクセスログから、バケット所有者の制御下にないクライアントからのリクエストの特性について理解できるため、多くのアプリケーションにとって有用です。デフォルトでは、Amazon S3 はサービスアクセスログを収集しませんが、ロギングを有効にすると Amazon S3 は通常数時間以内にアクセスログをバケットに配信します。より早い配信が必要な場合や、複数の送信先にログを配信する必要がある場合は、CloudTrail ログの使用を検討するか、CloudTrail ログと Amazon S3 の両方を組み合わせて使用することを検討してください。送信先バケットでデフォルトのオブジェクト暗号化を設定すると、保存中のログを暗号化できます。オブジェクトは、Amazon S3 で管理されたキー (SSE-S3) または AWS Key Management Service (AWS KMS) に保存されたカスタマーマスターキー (CMK) のいずれかで、サーバー側の暗号化を使用して暗号化されます。

Amazon S3 バケットに保存されたログは、Amazon Athena を使用してクエリおよび分析できます。Amazon Athena は、標準 SQL を使って S3 内のデータを分析できるインタラクティブなクエリサービスです。Athena では Athena にデータを集めたり、読み込んだりする必要がなく、ANSI SQL を使ってアドホッククエリを実行できます。Athena は非構造化データセットや半構造化データセット、構造化データセットを処理することができ、Amazon QuickSight と統合して視覚化を容易にします。

ログは、脅威の自動検出に役立つ情報源でもあります。Amazon GuardDuty は、VPC フローログや、CloudTrail 管理イベントログ、CloudTrail Amazon S3 データイベントログ、DNS ログなど、複数のソースからのイベントを分析して処理する継続的なセキュリティモニタリングサービスです。悪意のある IP アドレスやドメインのリストなどの脅威インテリジェンスフィードおよび機械学習を使用して、AWS 環境内の予期しない、未許可で悪意のある可能性が高いアクティビティを特定します。あるリージョンで GuardDuty を有効にすると、CloudTrail イベントログの分析が直ちに開始されます。CloudTrail 管理イベントと Amazon S3 データイベントは、独立かつ重複して次々と発生するイベントを介して CloudTrail から直接取り込まれます。

Amazon Macie による大規模なデータの検出と保護

GDPR 第 32 条には、次のように記載されています。「(...) 管理者と処理者は、とりわけ適切なものを含め、リスクに適したレベルのセキュリティを確保するための適切な技術的および組織的措置を実施しなければならない。(...)

(b) システムとサービスの処理における継続的な機密性、完全性、可用性と復元力を確実にする機能。

(...)

(d) 処理過程のセキュリティを確保するための技術的、組織的な措置の効率性を定期的にテスト、査定および評価するプロセス」。

セキュリティデータ処理をデータの性質に合わせて調整するには、継続的なデータ分類プロセスが不可欠です。組織が機密データを管理している場合は、そのデータがどこにあるかを監視して適切に保護し、規制コンプライアンスの要件を満たすために必要とされる通りにデータセキュリティとプライバシーを強化していることを示す証拠を提出します。AWS では、お客様が大規模な機密データを識別して保護できるように、Amazon Macie を提供しています。Amazon Macie は、フルマネージドのデータセキュリティおよびデータプライバシーサービスで、個人を特定できる情報 (PII) の検出にパターンマッチングと機械学習モデルを使用し、S3 バケットに保存されている機密データを検出して保護します。Amazon Macie はこれらのバケットをスキャンし、複数のカテゴリの機密データを検出するように設計されたマネージドデータ識別子を使って、バケットのデータ分類を提供します。Macie は、氏名、メールアドレス、生年月日、国民識別番号、納税者識別番号、参照番号などの PII を検出できます。お客様は、組織の特定のシナリオ (顧客アカウント番号や内部データ分類など) を反映したカスタムデータ識別子を定義できます。

Amazon Macie はバケット内のオブジェクトを継続的に評価し、定義されたデータカテゴリに一致する、暗号化されていないまたはパブリックにアクセス可能なデータが検出された場合に、検出結果のサマリー (図 4) を自動的に提供します。このデータには、AWS Organizations で定義した以外の AWS アカウントと

共有された、暗号化されていない、パブリックにアクセス可能なオブジェクトまたはバケットに関するアラートが含まれる場合があります。Amazon Macie は、AWS Security Hub など他の AWS のサービスと統合され、アクションの対象になり得るセキュリティ検出結果を生成し、その結果に対して自動的かつ事後対応的なアクションを提供します (図 5)。

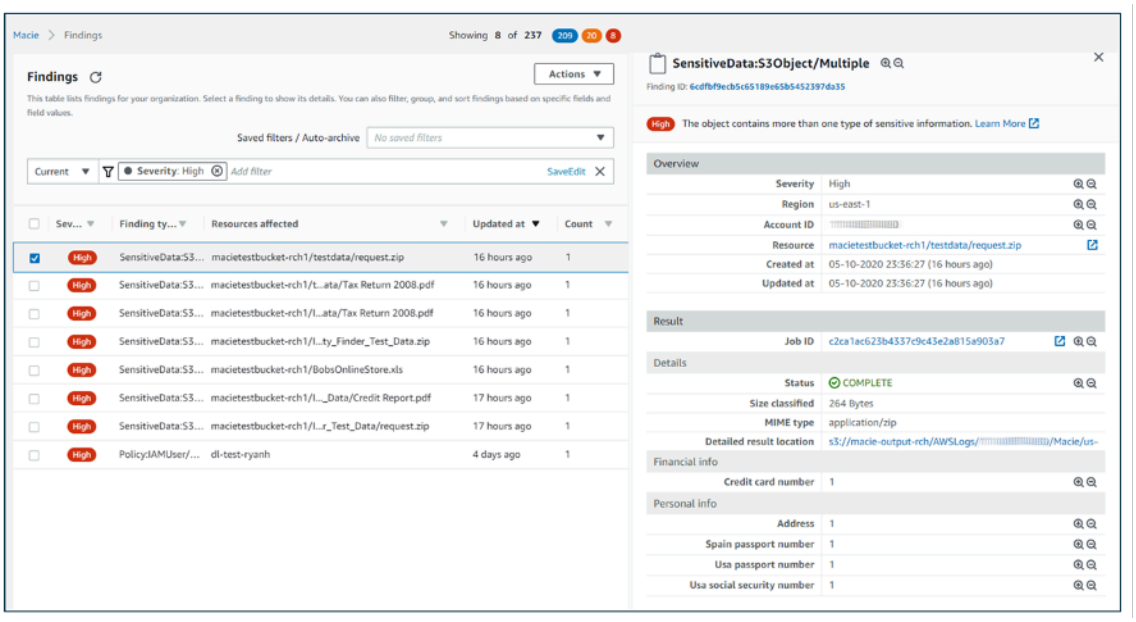

図 4 — データインスペクションと検出結果の例

セキュリティの一元管理:

多くの組織が、環境の可視性と一元管理に関する課題を抱えています。運用フットプリントが拡大するにつれて、セキュリティ設計を慎重に検討しなければ、この課題はさらに複雑になる可能性があります。知識不足にガバナンスやセキュリティプロセスの分散した不均等な管理が相まって、環境が脆弱になるおそれがあります。

AWS は、IT 管理とガバナンスに関する最も困難な要件の一部に対処するのに役立つツールと、設計によるデータ保護をサポートするツールを提供しています。

AWS Control Tower は、新しいセキュアなマルチアカウントの AWS 環境を設定して管理する方法を提供します。ベストプラクティスのブループリントに基づいたマルチアカウント環境であるランディングゾーンの設定を自動化し、事前にパッケージ化されたリストから選択できるガードレールを使用してガバナンスを可能にします。ガードレールは、セキュリティやコンプライアンス、運用に関するガバナンスルールを実装しています。AWS Control Tower は、AWS IAM Identity Center (IAM Identity Center) デフォルトディレクトリを使用した ID 管理を提供し、IAM Identity Center および IAM を使用したクロスアカウント監査を有効にします。また、CloudTrail からのログと Amazon S3 に保存されている AWS Config ログも一元化されます。

AWS Security Hubは、一元化をサポートし、組織の可視性を高めることができるもう 1 つのサービスです。Security Hub は、AWS のアカウントや、Amazon GuardDuty および Amazon Inspector といったサービス全体からのセキュリティおよびコンプライアンスに関する検出結果を一元化して、優先順位を設定します。また、サードパーティーパートナーのセキュリティソフトウェアと統合でき、セキュリティの傾向を分析し、最も重要なセキュリティの問題を特定するのに役立ちます。

Amazon GuardDuty は、インテリジェントな脅威検出サービスで、Amazon S3 に保存されている AWS アカウントや、ワークロード、データをより正確かつ簡単に監視、保護するのに役立ちます。GuardDuty は、AWS CloudTrail 管理イベント、CloudTrail Amazon S3 データイベント、Amazon Virtual Private

Cloud フローログ、DNS ログなど、複数のソースから AWS アカウント全体で数十億ものイベントを分析します。例えば、異常な API コール、既知の悪質な IP アドレスへの不審なアウトバウンド通信、または DNS クエリを転送メカニズムとして使用するデータ窃盗の可能性を検出します。GuardDuty は、機械学習を利用した脅威インテリジェンスとサードパーティーのセキュリティパートナーを活用することで、より正確な検出結果を提供できます。

Amazon Inspector は、Amazon EC2 インスタンスにデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector では、露出、脆弱性、ベストプラクティスからの逸脱に関して、アプリケーションを自動的に評価します。評価が実行された後、セキュリティの検出結果を重大性の順で並べた詳細なリストが Amazon Inspector によって作成されます。

Amazon CloudWatch Events を使用すると、他の AWS アカウントにイベントを送信する、または他のアカウントや組織からのイベントの受取先になるように AWS アカウントを設定できます。この仕組みは、セキュリティインシデントイベントが発生するといつでも必要に応じてタイムリーな修正アクション (Lambda 関数の呼び出し、Amazon EC2 インスタンスでのコマンドの実行など) を実行して、クロスアカウントのインシデント対応シナリオを実装するのに非常に役立ちます。

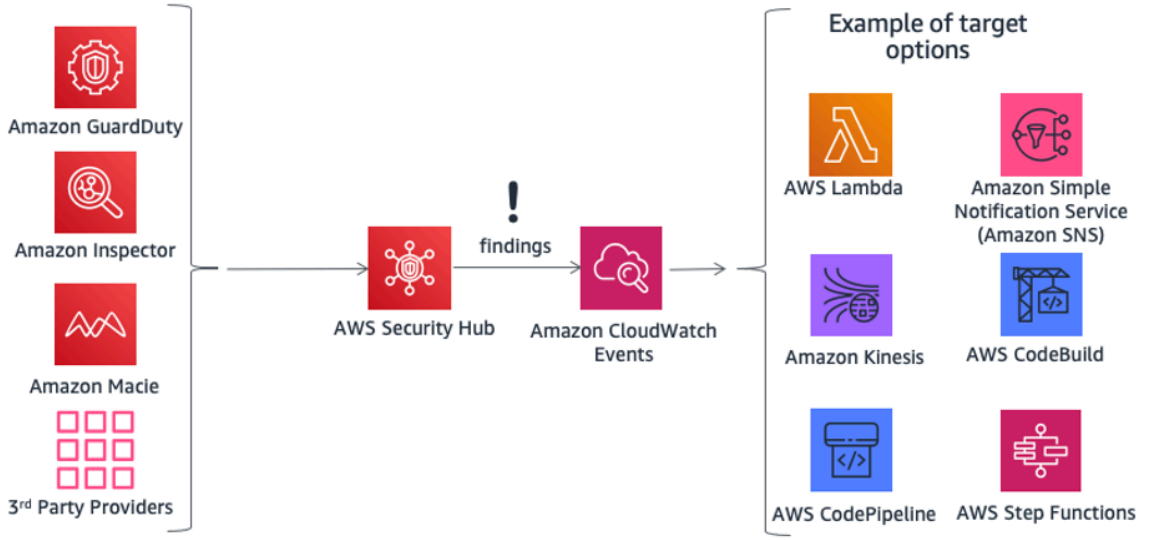

図 5 —AWS Security Hub および Amazon CloudWatch Events を使用したアクションの実行

AWS Organizations は、複雑な環境を一元的に管理、統制するのに役立ちます。これにより、マルチアカウント環境でアクセスやコンプライアンス、セキュリティを制御できます。AWS Organizations は、組織内の特定のアカウントまたは組織単位 (OU) で使用できる AWS のサービスのアクションを定義するサービスコントロールポリシー (SCP) をサポートしています。

AWS Systems Manager は、AWS でご利用のインフラストラクチャを可視化し、制御するためのサービスです。統一されたコンソールから複数の AWS のサービスの運用データを表示し、サービス全体で運用タスクを自動化できます。最近の API アクティビティ、リソース設定の変更、運用アラート、ソフトウェアインベントリ、パッチコンプライアンスステータスに関する情報が得られます。他の AWS のサービスとの統合により、運用上のニーズに応じてリソースに対するアクションを実行して、環境をコンプライアンス状態で維持することができます。

例えば、Amazon Inspector を AWS Systems Manager と統合することで、セキュリティ評価が簡素化および自動化されます。これは、Amazon EC2 インスタンスの起動時に Amazon Elastic Compute Cloud Systems Manager を使用して Amazon Inspector エージェントを自動的にインストールできるためです。Amazon EC2 システムマネージャーと Lambda 関数を使用して、Amazon Inspector の検出結果に対して自動修正を実行することもできます。

AWS におけるデータの保護

GDPR 第 32 条には、組織が「(...) 個人データの仮名化と暗号化 (...) を含む適切な技術的および組織的措置を実施することで、リスクに対応できるセキュリティレベルを確保する (...) 」ことが義務付けられています。また、組織は個人データの不正な開示あるいは個人データへのアクセスに対する安全策を講じる必要があります。

暗号化により、正しいキーがないとデータが読み取れないため、個人データの保存に伴うリスクが軽減されます。徹底した暗号化戦略は、一部のセキュリティ侵害など、さまざまなセキュリティイベントの影響を軽減するのに役立ちます。

保管中のデータの暗号化

保管中のデータの暗号化は、法規制の遵守とデータ保護に不可欠です。ディスクに保存された機密データが、有効なキーを持たないユーザーやアプリケーションから読み取られないようにすることができます。AWS では、保管中の暗号化と暗号化キー管理について、複数のオプションを用意しています。例えば、AWS KMS で作成および管理された CMK で AWS Encryption SDK を使用して、任意のデータを暗号化できます。

暗号化されたデータは保管中も安全に保存され、CMK へのアクセスが承認された当事者のみが復号化できます。その結果、エンベロープ暗号化された機密データ、承認と認証された暗号化のためのポリシーメカニズム、監査ロギングが AWS CloudTrail から得られます。AWS Foundation サービスの中には、保管中の暗号化機能が組み込まれており、不揮発性ストレージに書き込まれる前にデータを暗号化するオプションが提供されています。例えば、AES-256 暗号化を使用して、Amazon EBS ボリュームを暗号化し、サーバー側の暗号化 (SSE) 用の Amazon S3 バケットを設定することができます。Amazon S3 はクライアント側の暗号化もサポートしているため、Amazon S3 に送信する前にデータを暗号化できます。AWS SDK はクライアント側の暗号化をサポートし、オブジェクトの暗号化と復号化の操作を容易にします。Amazon RDS は透過的なデータ暗号化 (TDE) もサポートしています。

組み込みの Linux ライブラリを使用して、Linux Amazon EC2 インスタンスストア上のデータを暗号化することが可能です。このメソッドでは透過的にファイルを暗号化することで、機密データを保護します。その結果、データを処理するアプリケーションではディスクレベルの暗号化が認識されません。

インスタンスストア上のファイルを暗号化するには、次の 2 つの方法があります。

- ディスクレベルの暗号化 — この方法では、ディスク全体、またはディスク内のブロックが 1 つ以上の暗号化キーを使用して暗号化されます。ディスクの暗号化はファイルシステムレベルの下で行われ、オペレーティングシステムに依存せずに、名前やサイズといったディレクトリやファイルの情報を隠します。例えば、暗号化ファイルシステムは、Windows NT オペレーティングシステムの NTFS に対する Microsoft の拡張機能で、ディスクの暗号化を提供します。
- ファイルシステムレベルの暗号化 — この方式では、ファイルとディレクトリは暗号化されますが、ディスク全体またはパーティション全体は暗号化されません。ファイルシステムレベルの暗号化はファイルシステムの上位で行われ、オペレーティングシステム間で移動することも可能です。

不揮発性メモリ Express (NVMe) SSD インスタンスストアボリュームの場合、デフォルトのオプションはディスクレベルの暗号化です。NVMe インスタンスストレージ内のデータは、インスタンスのハードウェアモジュールに実装されている XTS-AES-256 ブロック暗号を使用して暗号化されます。暗号化キーは、ハードウェアモジュールで作成され、NVMe インスタンスストレージデバイスごとに固有です。すべての

暗号化キーは、インスタンスが停止または終了して復元できないときに破棄されます。独自の暗号化キーは使用できません。

転送中のデータの暗号化

AWS では、AWS 内外のリソースを含め、あるシステムから別のシステムへ転送中のデータの暗号化を強く推奨しています。

AWS アカウントを作成すると、AWS クラウドの論理的に分離されたセクション、つまり Amazon Virtual Private Cloud (Amazon VPC) がプロビジョニングされます。そこで、定義した仮想ネットワークで AWS リソースを起動できます。独自の IP アドレス範囲の選択、サブネットの作成、ルートテーブルやネットワークゲートウェイの設定など、仮想ネットワーク環境を完全に制御できます。また、会社のデータセンターと自分の Amazon VPC 間にハードウェアバーチャルプライベートネットワーク (VPN) 接続を作成できるため、AWS クラウドを貴社のデータセンターの延長として活用できます。

Amazon VPC と貴社のデータセンター間の通信を保護するために、いくつかの VPN 接続オプションが用意されており、ニーズに最適なものを選択できます。クライアントベースの VPN サービスを使用して AWS リソースへの安全なアクセスを実現するには、AWS Client VPN を使用することができます。AWS Marketplace で入手可能なサードパーティー製のソフトウェア VPN アプライアンスを使用することもできます。Amazon VPC の Amazon EC2 インスタンスにインストールできます。もしくは、VPC とリモートネットワーク間の通信を保護するために、IPsec VPN 接続を作成することもできます。リモートのネットワークから Amazon VPC への専用プライベート接続を作成するには、AWS Direct Connect を使用できます。この接続を AWS Site-to-Site VPN と組み合わせると、IPsec で暗号化されたプライベート接続を作成できます。

AWS では、TLS プロトコルを使用して通信する HTTPS エンドポイントを提供していることから、AWS API を使用する際に転送中の暗号化が提供されます。ワークロードのシステム間で暗号化されたトランスポートを確立するために使用するプライベート証明書とパブリック証明書の生成や管理、デプロイには、AWS Certificate Manager(ACM) サービスを使用できます。Elastic Load Balancing は ACM と統合されており、HTTPS プロトコルのサポートに使用されます。コンテンツが Amazon CloudFront を通じて配信される場合、暗号化されたエンドポイントがサポートされます。

暗号化ツール

AWS では、AWS で保存および処理されるデータを保護するために、スケーラビリティの高いさまざまなデータ暗号化サービスやツール、メカニズムを提供しています。AWS サービスの機能とプライバシーについては、「AWS のサービスのプライバシー機能」を参照してください。

AWS の暗号化サービスでは、保管中や転送中のデータの整合性を維持するために設計された、幅広い暗号化テクノロジーおよびストレージテクノロジーが使用されています。AWS では、暗号化オペレーションのための 4 つの主要ツールを提供しています。

- AWS Key Management Service(AWS KMS) は、マスターキーとデータキーの両方を生成し、管理する AWS マネージドサービスです。AWS KMS は多くの AWS のサービスと統合されており、お客様のアカウントの AWS KMS キーを使用してサーバー側でのデータ暗号化を提供します。AWS KMS ハードウェアセキュリティモジュール (HSM) は FIPS 140-2 レベル 2 で検証されています。
- AWS CloudHSM は、FIPS 140-2 レベル 3 で検証された HSM を提供します。マスターキーやデータキーなど、さまざまな自己管理型暗号化キーを安全に保存します。
- AWS 暗号化サービスおよびツール
  - AWS Encryption SDK は、あらゆるタイプのデータで暗号化および復号化操作を実施するためのクライアント側暗号化ライブラリを提供します。
  - Amazon DynamoDB 暗号化クライアントは、Amazon DynamoDB などのデータベースサービスに送信する前にデータテーブルを暗号化するための、クライアント側の暗号化ライブラリを提供します。

AWS Key Management Service

AWS Key Management Serviceは、データの暗号化に使用する暗号化キーを簡単に作成および制御できるマネージドサービスで、ハードウェアセキュリティモジュール (HSM) を使用してキーのセキュリティを保護します。AWS KMS は他のいくつかの AWS のサービスと統合されており、これらのサービスで保存するデータを保護するのに役立ちます。AWS KMS は AWS CloudTrail とも統合されており、規制やコンプライアンスのニーズに合わせて、キーの使用状況をすべて記録したログを提供します。

AWS Management Console から、または AWS SDK や AWS CLI を使用して、使用ポリシーを定義し、使用を監査するだけでなく、キーの作成やインポート、ローテーションを簡単に行うことができます。

AWS KMS の CMK は、お客様自身でインポートしたか、KMS により作成されたかに関わらず、必要なときに使用できるように、高い耐久性を持つストレージに暗号化された形式で保存されます。KMS で作成された CMK は、KMS によって 1 年ごとに自動的にローテーションするように設定できます。マスターキーで暗号化済みのデータを再度暗号化する必要はありません。KMS によって過去の暗号化データを自動的に復号化できるため、CMK の旧バージョンを追跡する必要はありません。

AWS KMS のどの CMK でも、キーポリシーまたは IAM ポリシー内の許可やキーポリシー条件など、さまざまなアクセス制御を介して、キーにアクセスできるユーザーやそのキーを使用できるサービスを制御できます。また、独自のキー管理インフラストラクチャからキーをインポートして、KMS で使用できます。

例えば、次のポリシーでは、特定のユーザー (ExampleUser) に代わって特定のリージョン (us-west-2) の Amazon EC2 または Amazon RDS からリクエストが送信された場合にのみ、指定されたアクションに対してカスタマー管理の CMK の使用を許可する kms:ViaService 条件を使っています。

```
        {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Effect”: “Allow”,
                “Principal”: {
                    “AWS”: “arn:aws:iam::111122223333:user/ExampleUser”
                 }
                “Action”: [
                     “kms:Encrypt*”,
                     “kms:Decrypt”,
                     “kms:ReEncrypt*”,
                     “kms:GenerateDataKey*”,
                     “kms:CreateGrant”,
                     “kms:ListGrants”,
                     “kms:DescribeKey”
                 ],
                 “Resource”: “*”,
                 “Condition”: {
                    “ForAnyValue:StringEquals”: {
                        “kms:ViaService”: [
                              “ec2.us-west-2.amazonaws.com”,
                              “rds.us-west-2.amazonaws.com”
                        ]
                     }
              }
}
```

AWS のサービスの統合

AWS KMS は多数の AWS のサービスと統合されています。統合サービスの一覧については、KMS のウェブサイトを参照してください。これらの統合により、サービスに保存するデータを暗号化するために AWS KMS CMK を簡単に使用できます。カスタマー管理の CMK を使用するだけでなく、多くの統合サービス

により自動的に作成および管理された AWS 管理の CMK を使用できます。ただし、それを作成した特定のサービス内でのみ使用可能です。

監査機能

AWS CloudTrail は、CloudTrail の設定で指定した Amazon S3 バケットに配信されるログファイルに、AWS KMS に保存したキーの使用を都度記録します。記録される情報はユーザーの詳細、時間、日付、実行された操作、使用されたキーなどです。

セキュリティ

AWS KMS は、お客様のマスターキーに誰もアクセスできないように設計されています。このサービスは、プレーンテキストのマスターキーを絶対にディスクに保存しない、メモリにマスターキーを残さない、キーを使用するホストにアクセスできるシステムを制限するなど、広範囲にわたる堅牢化のテクニックでマスターキーを保護することを目的として設計されたシステム上に構築されています。サービス内でソフトウェアをアップデートしようとするすべてのアクセスは、複数の関係者によって管理され、AWS 内の独立したグループによって監査およびレビューされます。

AWS KMS の詳細については、AWS Key Management Service のホワイトペーパーを参照してください。

AWS CloudHSM

AWS CloudHSM はクラウドベースのハードウェアセキュリティモジュール (HSM) で、FIPS 140-2 レベル 3 検証済みハードウェアで暗号化キーを生成して使用できるようにすることで、データセキュリティに関する企業、契約、法規制のコンプライアンス要件を満たすことができます。

AWS CloudHSM を使用して、暗号化キーや HSM によって実行される暗号化操作を管理します。

AWS および AWS Marketplace のパートナーにより、AWS プラットフォーム内の機密データを保護するためのさまざまなソリューションが用意されています。しかし、暗号化キーの管理に関する厳格な契約上の要件や法律的な要件の対象となるアプリケーションやデータについては、さらなる保護が必要になることがあります。以前は、機密データ (またはそれを保護する暗号化キー) はオンプレミスのデータセンターに保存するという選択肢しかないこともありました。これにより、アプリケーションをクラウドに移行できなかったり、アプリケーションのパフォーマンスが大幅に低下したりする可能性がありました。AWS CloudHSM を使うと、安全なキー管理に関する米国政府標準規格に適合するように設計され、検証された HSM 内で暗号キーを保護できます。データ暗号化に使用される暗号キーの生成、保存、管理を、所有者だけがキーにアクセスできるような方法で安全に行うことができます。AWS CloudHSM を使用すると、アプリケーションのパフォーマンスを犠牲にせずに、厳密なキー管理要件を満たすことができます。

AWS CloudHSM サービスは Amazon VPC と連携して動作します。AWS CloudHSM のインスタンスは、指定した IP アドレスで Amazon VPC 内にプロビジョニングされ、Amazon EC2 インスタンスへのシンプルでプライベートなネットワーク接続が可能になります。HSM インスタンスを Amazon EC2 インスタンスの近くに配置すると、ネットワークレイテンシーが減り、アプリケーションのパフォーマンスが向上します。AWS は、他の AWS ユーザーから隔離された形で、HSM インスタンスへの排他的な専用 (シングルテナント) アクセスを提供します。複数のリージョンとアベイラビリティーゾーンで利用可能な AWS CloudHSM は、お客様のアプリケーションに安全で耐久性のあるキーストレージを追加できるようにします。

AWS のサービスおよびサードパーティー製アプリケーションとの統合

CloudHSM は、Amazon Redshift や Amazon RDS for Oracle、「ルートオブトラスト」として機能するサードパーティー製アプリケーション (SafeNet Virtual KeySecure など) 、Apache (SSL 終端)、Microsoft SQL Server (透過的データ暗号化) などと一緒に使用できます。また、独自のアプリケーションを作成し、PKCS #11 や Java JCA/JCE、Microsoft CAPI、CNG などの標準暗号化ライブラリを引き続き使用する場合にも、AWS CloudHSM を使用できます。

監査アクティビティ

セキュリティとコンプライアンスの目的で、リソースの変更の追跡やアクティビティの監査が必要な場合は、AWS CloudTrail を使用してアカウントから実行された AWS CloudHSM 経由の管理 API コールを確認できます。さらに、syslog を使用して HSM アプライアンス上での操作を監査したり、syslog ログメッセージを独自のログコレクターに送信したりすることも可能です。

AWS 暗号化サービスおよびツール

AWS には、ベストプラクティスの暗号化を実装するために使用できる、幅広い暗号化セキュリティ規格に準拠した仕組みが用意されています。AWS 暗号化 SDK はクライアント側の暗号化ライブラリで、Java や Python、C、JavaScript、Linux や macOS、Windows をサポートするコマンドラインインターフェイスで使用できます。キーの派生と署名機能を備えた 256 ビット AES-GCM などの安全で認証された対称キーアルゴリズムスイートを含め、高度なデータ保護機能を提供します。Amazon DynamoDB を使用するアプリケーション向けに特別に設計されているため、DynamoDB 暗号化クライアントを使用すると、データベースに送信される前にテーブルデータを保護できます。DynamoDB 暗号化クライアントは、データの取得時にデータの検証と復号化も行います。クライアントは Java 版 と Python 版 があります。

Linux dm-crypt インフラストラクチャ

dm-crypt は、Linux カーネルレベルの暗号化メカニズムです。dm-crypt を使用すると、暗号化されたファイルシステムをマウントできます。ファイルシステムのマウントとは、ファイルシステムをディレクトリ (マウントポイント) にアタッチして、オペレーティングシステムで利用可能にするプロセスを指します。マウント後は、追加の操作なしで、ファイルシステム内のすべてのファイルをアプリケーションから利用できるようになります。ただし、これらのファイルはディスクに保存されるときに暗号化されます。

デバイスのマッパーとは、ブロックデバイスの仮想レイヤーを作成する一般的な方法を提供する Linux 2.6 および 3.x カーネルのインフラストラクチャのことです。デバイスマッパー暗号ターゲットは、カーネル暗号化 API を使用したブロックデバイスの透過的暗号化を提供します。この記事のソリューションでは、dm-crypt を Logical Volume Manager (LVM) によって論理ボリュームにマップされたディスクバックアップのファイルシステムと一緒に使用します。LVM は、Linux カーネル用の論理ボリューム管理を提供します。

設計とデフォルトによるデータ保護

ユーザーまたはアプリケーションが AWS Management Console や AWS API、AWS CLI を使用しようとすると、AWS にリクエストが送信されます。AWS のサービスは、リクエストを受け取ると、特定のポリシー評価ロジックに従って、リクエストを許可するか拒否するかを決定するための一連のステップを実行します。ルート認証情報リクエストを除き、AWS でのすべてのリクエストはデフォルトで拒否されます (デフォルトの拒否ポリシーが適用されます)。つまり、ポリシーで明示的に許可されていないものはすべて拒否されます。ポリシーの定義とベストプラクティスとして、AWS では最小特権の原則の適用を推奨しています。つまり、すべてのコンポーネント (ユーザー、モジュール、サービスなど) は、タスクを完了するために必要なリソースにのみアクセスできる必要があります。

このアプローチは、「管理者が適切な技術的および組織的措置を実施することで、原則として、必ず特定の処理目的ごとに必要な個人データのみが処理されるようにしなければならない」とする GDPR 第 25 条に合致しています。

AWS では、Infrastructure as Code を実装するツールも提供しています。これは、アーキテクチャ設計の最初からセキュリティを含めるための強力な仕組みです。AWS CloudFormation には、セキュリティポリシーやプロセスなど、すべてのインフラストラクチャリソースを記述し、プロビジョニングするための共通言語が用意されています。これらのツールと実践によって、セキュリティはコードの一部となり、組織の要件に応じて、バージョニングシステムを使用してバージョン管理、監視、変更ができます。これにより、セキュリティプロセスとポリシーをアーキテクチャの定義に含めることができ、組織内のセキュリティ対策によって継続的に監視できるため、設計によるデータ保護が可能になります。

AWS で実現できること

表 1 — AWS で GDPR コンプライアンスへの対応を実現する方法

エリア	説明	AWS のサービスとツール
強力なコンプライアンスのフレームワーク	適切な技術的および組織的対策には、「処理するシステムおよびサービスの現存の機密性と完全性、可用性、回復力を確実にする機能」を含める必要性が生じることがあります。	SOC 1/SSAE 16/ISAE 3402 (旧 SAS 70)/SOC 2/SOC 3 PCI DSS レベル 1 ISO 9001/ISO 27001/ISO 27017/ISO 27018 NIST FIPS 140-2 一般的なクラウドコンピューティングコントロールカタログ (C5)
データのアクセスコントロール	管理者は、「(...) 適切な技術的および組織的措置を実施することで、原則として、必ず特定の処理目的ごとに必要な個人データのみが処理されるようにしなければならない」。	AWS Identity and Access Management (IAM) Amazon Cognito AWS Shield および AWS WAF AWS Resource Access Manager Amazon CloudFront AWS Organizations AWS CloudTrail
モニタリングとロギング	「各管理者および、必要に応じて管理者の代表者は、その責任下において処理活動の記録を維持する」。 「(...) 管理者と処理者は、リスクに適したレベルのセキュリティを確保するために、適切な技術的および組織的措置を実施しなければならない (...)」	AWS Config Amazon CloudWatch AWS Control Tower Amazon GuardDuty Amazon Inspector Amazon Macie AWS Systems Manager AWS Security Hub AWS のツールと SDK
AWS におけるデータの保護	組織は、「個人データの仮名化と暗号化を含む適切な技術的および組	AWS Certificate Manager AWS CloudHSM

エリア	説明	AWS のサービスとツール
	織的措置を実施することで、リスクに対応するセキュリティレベルを確保する」。	AWS Key Management Service

寄稿者

本書の作成における寄稿者

- アマゾン ウェブ サービス、テクニカルインダストリースペシャリスト、Tim Anderson
- アマゾン ウェブ サービス、パブリックセクターソリューションアーキテクト、Carmela Gambardella
- アマゾン ウェブ サービス、セキュリティ保証マネージャー、Giuseppe Russo
- アマゾン ウェブ サービス、シニアプログラムマネージャー、Marta Taggart
- アマゾン ウェブ サービス、パブリックセクターソリューションアーキテクト、Luca Iannario

改訂履歴

日付	説明
2017 年 11 月	初版公開
2020 年 12 月	新しい AWS のサービスと機能の追加を含めるための更新。

注意

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明していますが、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤーまたはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または暗示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で締結されるいかなる契約の一部でもなく、その内容を修正するものでもありません。