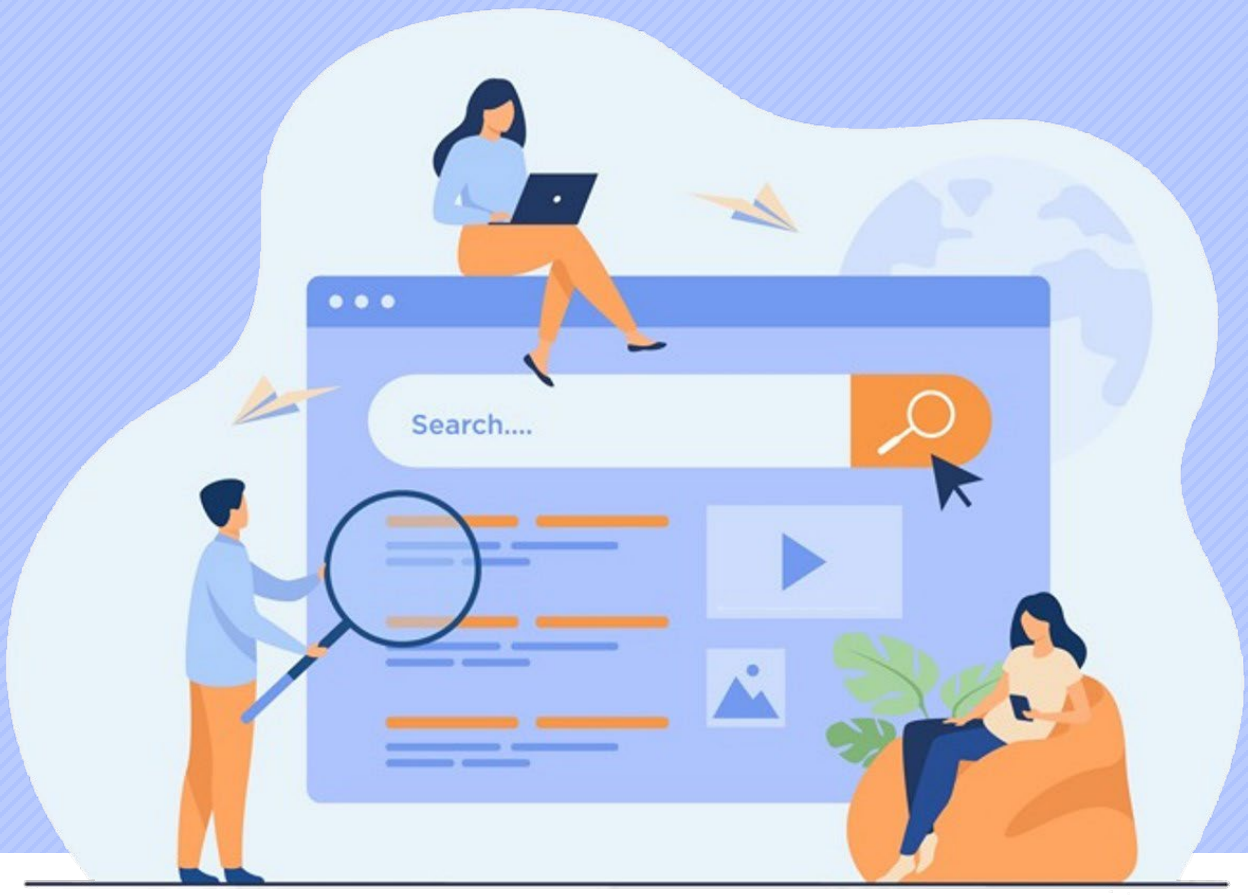
JIG-SAW

AWSを使う人が知っておくべき
セキュリティ対策



JIG-SAW株式会社

電話 03-6262-5160

サービス問合せ https://ops.jig-saw.com/form/contact

Webサイト https://ops.jig-saw.com

システム運用代行
に関するお問合せはこちら

　※本資料は2021年5月に作成されたものです。掲載されている各種情報は作成時点のものです。

はじめに

AWSの利用は簡単に始められますが、その後のセキュリティ対策は意外と見落とされがちです。セキュリティ対策がしっかりできていないと、AWSアカウントへ不正ログインされ高額な利用料の請求に繋がったり、サービス停止に追い込まれたりといった最悪の事態に陥る可能性があります。本コンテンツでは、上記課題をクリアするため、AWSを使う人が知っておくべきセキュリティの考え方からその対策方法についてご説明します。

セキュリティ対策を怠るとどうなる？

AWSサービスを使用するためにはまずAWSアカウントの作成を行いますが、それ自体は簡単に作成でき、すぐにでもサービスの利用を開始することができます。しかし、すぐにサービスを使いたい気持ちを抑えて、まずはセキュリティ対策をしっかりと行うのが望ましいです。AWSアカウントのセキュリティ対策を怠るとどんな被害が起きてしまうのか、事前に知る必要があります。ここからは、被害の例を以下に示します。

不正ログイン、大量のサーバ起動による高額な利用料の請求

AWSアカウントへの不正ログインにより気づかないうちに大量のサーバが起動されてしまい、高額な請求をされてしまうというケースがあります。これはログイン情報を流出してしまった場合に起こることですが、ログイン情報を流出してしまうパターンとしては下記のようなパターンがあります。

1. アカウントのフィッシング
2. キーを埋め込んだソースコードの公開
3. 退職者IDの削除漏れ

フィッシングとは実在する組織になりすましてメールを送り、偽のウェブサイトに誘導し個人情報を取得・悪用する行為のことをいいます。また、CLIからAWS内のリソースを操作するためにはアクセスキー/シークレットキーが必要ですが、それらをソースコードに直接埋め込んでしまいGitなどで公開してしまうというケースもあります。一瞬にして、世界中に機密情報を知られてしまいますので、開発者は特に注意が必要です。最後のパターンとしては、退職者のIAMユーザを削除せずに残してしまい、悪意を持った退職者がいつでもログインできる状況にしてしまっているというパターンです。

サイバー攻撃によるサービス停止

サイバー攻撃とは、サーバやパソコンなどのシステムに対し、さまざまな手段を用い、データを抜き取る、改ざんする、システムを破壊することをいいます。サイバー攻撃の件数は、年々増加しており、特に世界的スポーツイベントの開催国での攻撃件数は増えることがわかっています。サイバー攻撃を受けてサービス停止になるパターンとしては下記のようなパターンがあります。

1. 個人情報の流出によるサービス継続不可
2. 物理的なシステム障害によるサービス提供不可

図1 不正アクセス、なりすましをされている様子

個人情報の流出事件は昨今増加しており大企業が狙われてニュースになることもよく目にするようになりました。企業ダメージが傷つき信用を失うことでサービス継続が危ぶまれることも少なくありません。また、サイバー攻撃によりサーバが負荷に耐えられなくなったり破壊されてしまったりして物理的にサービス提供が不可になることもあります。

セキュリティ被害から守るための対策

セキュリティ被害から守るための対策を3つの観点から考えていきたいと思います。
3つの観点とは「①被害を未然に防ぐ」「②被害に気づく」「③被害状況を調査する」です。
それぞれ順に解説していきます。

1. 被害を未然に防ぐ

まずは被害が起きないようにすることが重要です。そのために事前に対策できることは沢山ありますので、対策の例を下記に記載します。

・不要なIAMの精査
・IAM権限の制限
・MFAの導入
・アクセス情報のハードコード禁止
・WAF製品やIPS/IDS製品の導入
・アーキテクチャの見直し

セキュリティ製品の導入ももちろんですが、IAM情報の管理をしっかりするだけでも、不正アクセスによる被害を防ぐことができます。退職者のIAMユーザ情報が残っていると、不正利用されるため、定期的に確認し削除するのが望ましいです。

そのほか、AWSアカウントへのログインにMFA（多要素認証）を導入する、アクセスキーシークレットキーをソースコードに直接書いて公開しないなどといったことから意識していくことが重要です。

2. 被害に気づく

被害を防ぐための対策をした上で被害が起きてしまった場合はやむを得ないため、次に考えることとしてはいかに早く気付くことができるかです。被害に気付くためにすることはアラート通知の仕組みを用意しておくことです。

・攻撃検知ツール/サービスからのアラート通知
・コスト管理ツールからのアラート通知

まずは攻撃検知の通知をすることができるAmazon GuardDutyなどのAWSサービスや外部のIPS/IDSツールやWAF製品からアラートを通知できるように設定しておくとよいです。また、コストと使用料の可視化をできるAWS Cost Explorerや設定した予算を超えた際にアラート通知をできるAWS Budgetsなどのコスト管理ツールも使用することで異常事態に気づくことができるようになります。

3. 被害状況を調べる

被害に気付いたあとは迅速に状況を調べる必要があります。調査する際に役に立つのがログです。

図2 セキュリティ被害から守るための対策

AWSでは様々なログを取得することができますが、なかでも各AWSサービスのアクセスログや監査ログについては取得することをおすすめします。また、AWSアカウント内での設定変更履歴を記録できるAWS ConfigやAWSアカウント内で行われた操作のイベントログを記録できるAWS CloudTrailについても、有効活用するとよいです。

AWSセキュリティ対策に役立つサービス

AWSにはセキュリティ対策に役立つサービスが充実しています。各セキュリティサービスの概要をご紹介したいと思います。（表1）

AWS Trusted Advisor

AWS Trusted Advisor では、コストの削減、可用性とパフォーマンスの向上、セキュリティの改善に役立つ一連のベストプラクティスチェックと推奨事項を提供しています。AWS Trusted Advisorのダッシュボードでは5つのカテゴリごとのチェック状況が確認できるため、即時の対応が推奨されるチェック項目あるいは、調査が推奨されるチェック項目が存在する場合は、改善対応を行うことをおすすめします。

AWS Security Hub

AWS Security Hub では、セキュリティアラートとセキュリティ状況を、すべての AWS アカウントで包括的に確認できます。複数の AWS サービス やAPN ソリューションでのセキュリティアラートと検出結果を、一元的に集約できるため定期的なレポート取得をおすすめします。

＜対象のAWSサービス＞

Amazon GuardDuty、Amazon Inspector、Amazon Macie、AWS IAM Access Analyzer、AWS Systems Manager、AWS Firewall Manager 等

Amazon Inspector

Amazon Inspector は自動化されたセキュリティ評価サービスで、Amazon EC2 インスタンスへの意図しないネットワークアクセスや、EC2 インスタンス上の脆弱性をチェックできます。専用のエージェントを導入することでEC2内の脆弱性診断を行い、レポートを作成することができるため定期的に実施することをおすすめします。

Amazon GuardDuty

Amazon GuardDuty は、AWSのアカウント、ワークロード、および　Amazon S3 に保存されたデータを保護するために、悪意のあるアクティビティや不正な動作を継続的にモニタリングする脅威検出サービスです。リアルタイムで検知してくれるのでアラートをとばせるように設定しておくことをおすすめします。

表1 AWSにおけるセキュリティサービスの概要

AWSサービス	概要
AWS Trusted Advisor	AWS インフラストラクチャ最適化チェック
AWS Security Hub	AWSのセキュリティチェック
Amazon Inspector	EC2の脆弱性チェック
Amazon GuardDuty	AWSアカウントへの攻撃のリアルタイム検知
AWS IAM Access Analyzer	AWSリソースへの意図しないアクセスの特定

図3 AWS Trusted Advisorにおけるチェック項目

AWS IAM Access Analyzer

AWS IAM Access Analyzer は、AWSリソースに紐付いているポリシーを検査し、他AWSアカウントや外部のインターネット等からのアクセスを可能とするような設定がされているか否かを検出および可視化することができます。これにより意図せぬ公開設定がされていないかを確認できますので、検知する設定を入れておくことをおすすめします。

おわりに

本コンテンツでは、AWSを使う人が知っておくべきセキュリティ対策についてご紹介しました。セキュリティと一口に言っても、様々な対策が必要になります。今回ご紹介したAWSサービスだけでなく、外部ソリューションもうまく組み合わせて、「被害を未然に防ぐ、気づく、調べる」といった仕組みづくりを意識するとよいでしょう。
AWSをこれから使う人は、AWSアカウントを作成後、まずセキュリティ対策の検討からはじめ、既にAWSを使用している人は、今すぐに自社のセキュリティ対策が十分かどうかを見直してみてください。

あなたのシステムにひとつ上のサポートを

JIG-SAWは、これまでにないシステム管理・支援サービスを提供します。
クラウドをはじめとしたあらゆるシステムの「サポート」を科学し、企業の成長を後押しします。

あらゆるシステム管理とサポートを強化

「JIG-SAW OPS」

クラウドや自社で保有されているシステム環境を、管理者様に代わって24時間体制で管理し、企業のシステム管理体制を強化します。
JIG-SAWが開発した「puzzle」を使用した異常検知/自動通知の仕組みと、エンジニアによる技術サポートを組み合わせたサービスをご提供します。お客様が本来の業務に注力し、事業を最大化できるよう、システム管理の側面から全面的にサービスを支援します。

ひとつ上のマルチクラウド包括支援サービス

「JIG-SAW プライム」

Amazon Web Services、Google Cloud、Microsoft Azureを、高いコストパフォーマンスでご利用いただける、マルチクラウドの包括支援サービスです。企業やプロジェクト単位で複数のクラウド、複数のアカウントをお持ちの場合でも、円建ての請求書発行から問合せ窓口まで、一元的に支援します。お困りごとがあれば、クラウドエンジニアによるプロフェッショナルで高品質なサポートをご利用いただけます。

JIG-SAW

お問い合わせ
TEL 03-6262-5160

JIG-SAW株式会社　〒104-0028 東京都中央区八重洲2丁目2-1　東京ミッドタウン八重洲 八重洲セントラルタワー33階
WEB：https://ops.jig-saw.com