

T 3 - 4

デモで理解する！ 基本の Web システムアーキテクチャ - セキュリティ編 -

木村 友則

アマゾン ウェブ サービス ジャパン合同会社
ソリューションアーキテクト



自己紹介



木村 友則 (きむら とものり)

ソリューションアーキテクト

- ・ 業種・業態を問わず、様々なお客様の構成検討を支援
- ・ 前職では、AWS のユーザーの立場として、インフラエンジニアに従事

本サービスで取り上げる AWS のサービス・機能

本セッションで取り上げる AWS のサービス・機能は以下の通りです。
詳細は、AWS クラウドサービス活用資料集 よりご確認頂けます。

- AWS Identity and Access Management (IAM)
- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- AWS Budgets
- AWS Trusted Advisor
- AWS Systems Manager
- Amazon Inspector
- AWS WAF

AWS クラウドサービス活用資料集

アマゾン ウェブ サービスの公式イベントのアーカイブおよびオンデマンドコンテンツの動画や資料がご利用いただけます。

[AWS Webinar お申込 »](#)

[AWS 初心者向け »](#)

[サービス別資料 »](#)

[ハンズオン資料 »](#)

<https://aws.amazon.com/jp/events/aws-event-resource/>



本セッションの対象になる方

- AWS をこれから触り始めようとしている方
- AWS アカウントそのものを守るセキュリティ対策を知りたい方
- 基本的な Web システムのセキュリティ対策を知りたい方

何から対策をしていけば
良いのかよく分からない



ワークフローを守るには
どんな方法があるの？



どんなリスクを想定すれば良い？
予防や対策は何が出来る？



本セッションの内容

- AWS アカウントと基本的な Web システムに対して、セキュリティ対策を実施するデモを行います
 - AWS アカウントに対する対策
 - AWS アカウントをセキュアにする
 - AWS で起きた事実を記録する
 - セキュリティ脅威を自動的に検知する
 - コスト面での「安心」を確保する
 - 繙続的な改善へ取り組む
 - 基本的な Web システムに対する対策
 - 仮想マシンの安全な運用を実現する
 - Web システムを攻撃から守る

※ 全体像を理解していただくことが目的のため、各サービスや機能の詳細説明は行っておりません



本セッションの内容

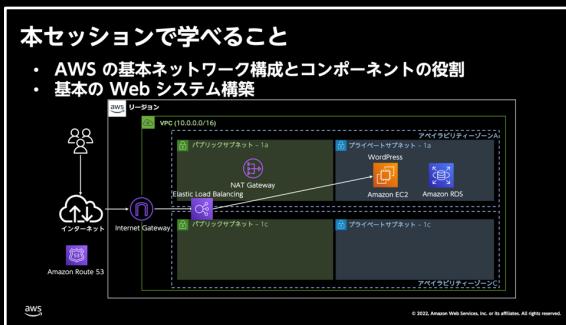
- AWS アカウントと基本的な Web システムに対して、セキュリティ対策を実施するデモを行います
 - AWS アカウントに対する対策
 - AWS アカウントをセキュアにする
 - AWS で起きた事実を記録する
 - セキュリティ脅威を自動的に検知する
 - コスト面での「安心」を確保する
 - 繙続的な改善へ取り組む
 - 基本的な Web システムに対する対策
 - 仮想マシンの安全な運用を実現する
 - Web システムを攻撃から守る

※ 全体像を理解していただくことが目的のため、各サービスや機能の詳細説明は行っておりません

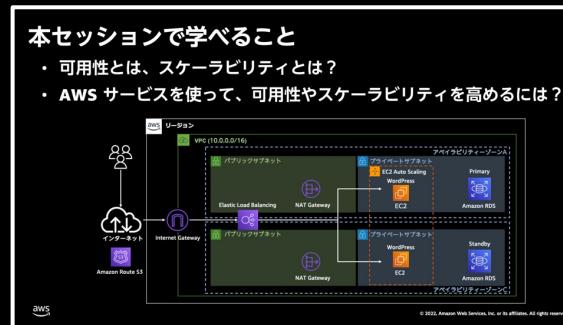


関連セッションについて

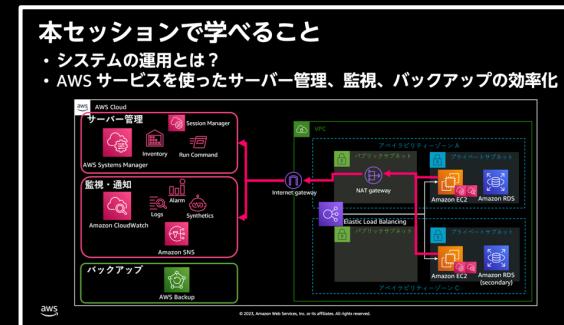
本セッションは、基礎編、スケーラビリティ向上編、運用編、セキュリティ編の4セッションで構成しています。セキュリティ編で例示するアーキテクチャの構築デモは、基礎編をご覧ください。



基礎編



スケーラビリティ向上編



運用編



セキュリティ編

※ 当日ご覧になれなかった場合でも、後日のオンデマンド配信でご覧頂くことが出来ます

本セッションで扱わないこと

- デモでご紹介する AWS アカウントに対するセキュリティ対策の詳細や AWS におけるセキュリティの考え方については、セッションアーカイブから「今日からスタート！ AWS セキュリティはじめの一歩」をご覧ください。



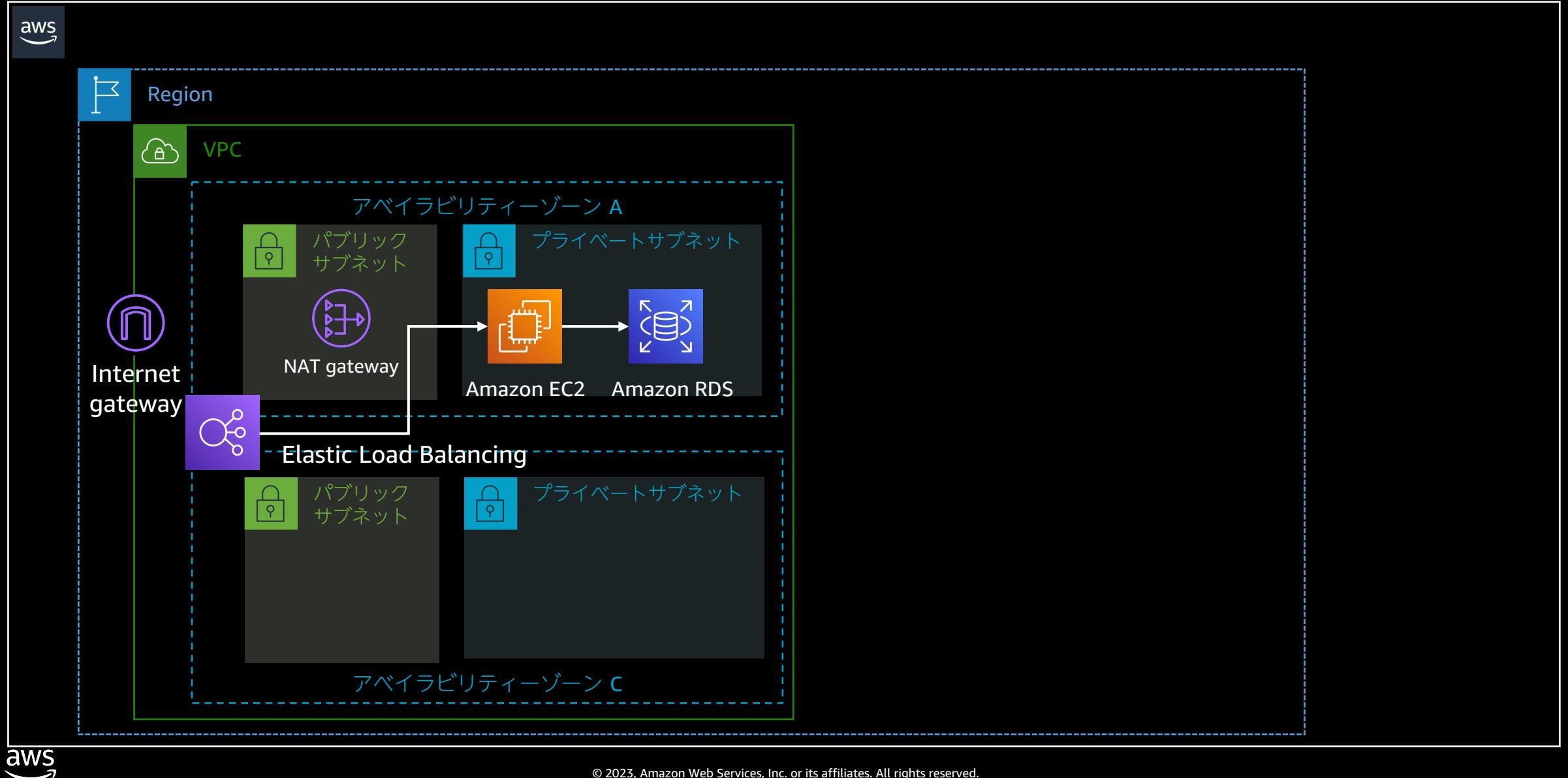
<https://youtu.be/cxCSY8DHXZA>



セキュリティ対策 全体の流れ



基本の Web システム



AWS アカウントをセキュアにする



AWS Identity and Access Management (IAM)

AWS リソースをセキュアに操作するための認証・認可を行う

- AWS リソースをセキュアに操作するための認証・認可を行う
- 日常作業に利用する IAM ユーザーの作成・管理が可能
- 特別な作業以外は、ルートユーザー^(※1)ではなく、IAM ユーザーを使う
- EC2 等のサービスに対する権限付与も可能（IAM ロール）

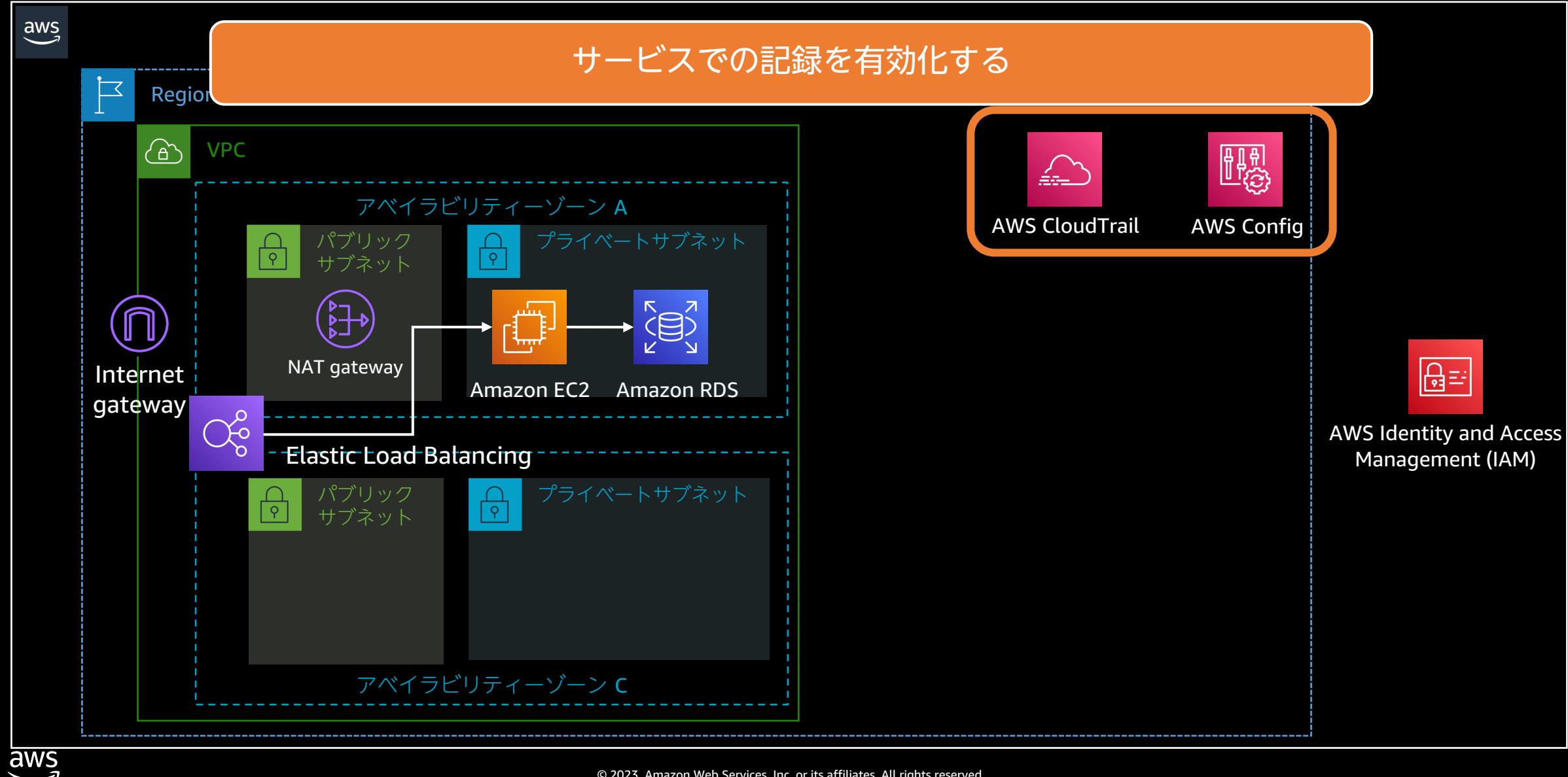


※1 ルートユーザー： AWS アカウント作成時に使用したメールアドレスとパスワードによるログイン

動画をご覧ください



AWS で起きた事実を記録する



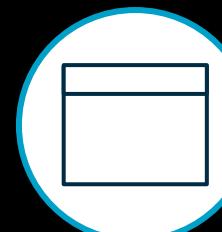
AWS CloudTrail

いつ、どこから、誰が、どんな操作を実行したかを記録し、セキュリティ分析などを容易に

- AWS アカウントにおける各種操作のログ記録、継続的なモニタリング、保持が可能
- いつ、どこから、誰が、どんな操作を実行したかを記録し、セキュリティ分析など容易に
- 設定により Amazon S3 に証跡を自動保存する



AWS
マネジメント
コンソール



AWS CLI, AWS SDK 等



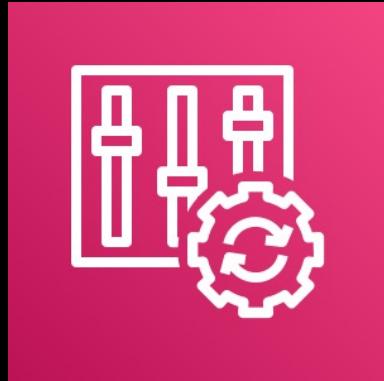
証跡

操作例：
EC2 インスタンス起動



AWS Config

構成情報の記録、評価を行うマネージドサービス



- AWS リソース構成情報の一元管理、および構成変更管理のためのフルマネージド型サービス
- 構成変更の追跡で、セキュリティ分析などを容易に

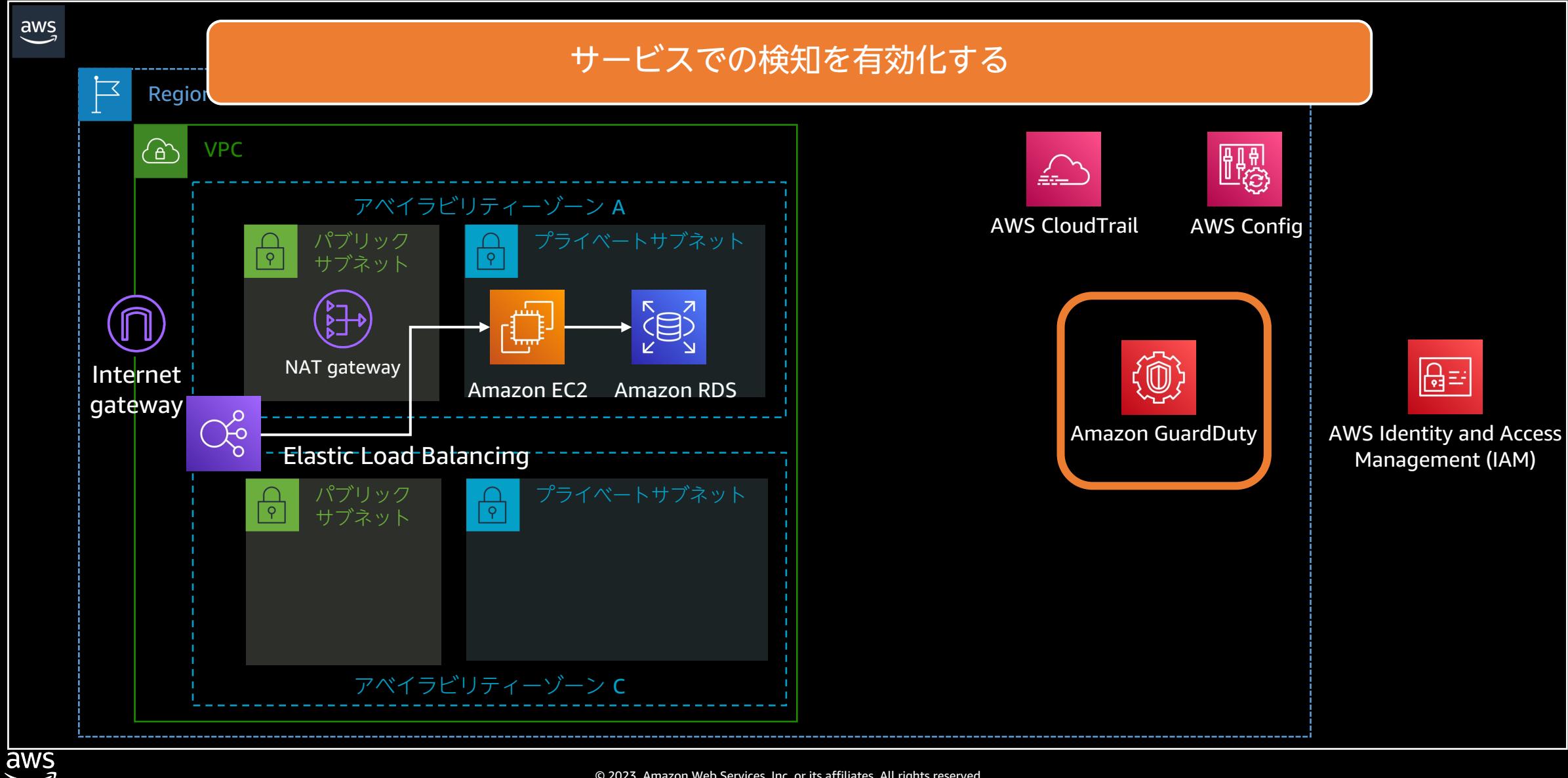
誰が、いつ、何をしたかを、自動で継続的に記録し、確認する



動画をご覧ください



セキュリティ脅威を自動的に検知する



Amazon GuardDuty

機械学習と豊富な脅威情報に基づく脅威検知で AWS 環境を保護



- 機械学習と豊富な脅威情報に基づいた脅威検知で、お客様の AWS 環境を保護
- AWS が管理する基盤で動作し、導入時の構成変更不要 & 性能影響なし
- 脅威検知手法は AWS が継続的に改善

セキュリティ、アイデンティティ、コンプライアンス

Amazon GuardDuty
アカウントとワークLOADの
ためのインテリジェントな脅
威保護

ワンクリックの脅威検出

1回クリックするだけで、Amazon GuardDuty は、AWS アカウント、データ、およびワークLOADのインテリジェントで継続的な脅威検出を使用して、リスクを軽減します。

GuardDuty を無料で試す

30 日間の無料トライアルで GuardDuty とその
脅威検出機能を評価できます。

今すぐ始める

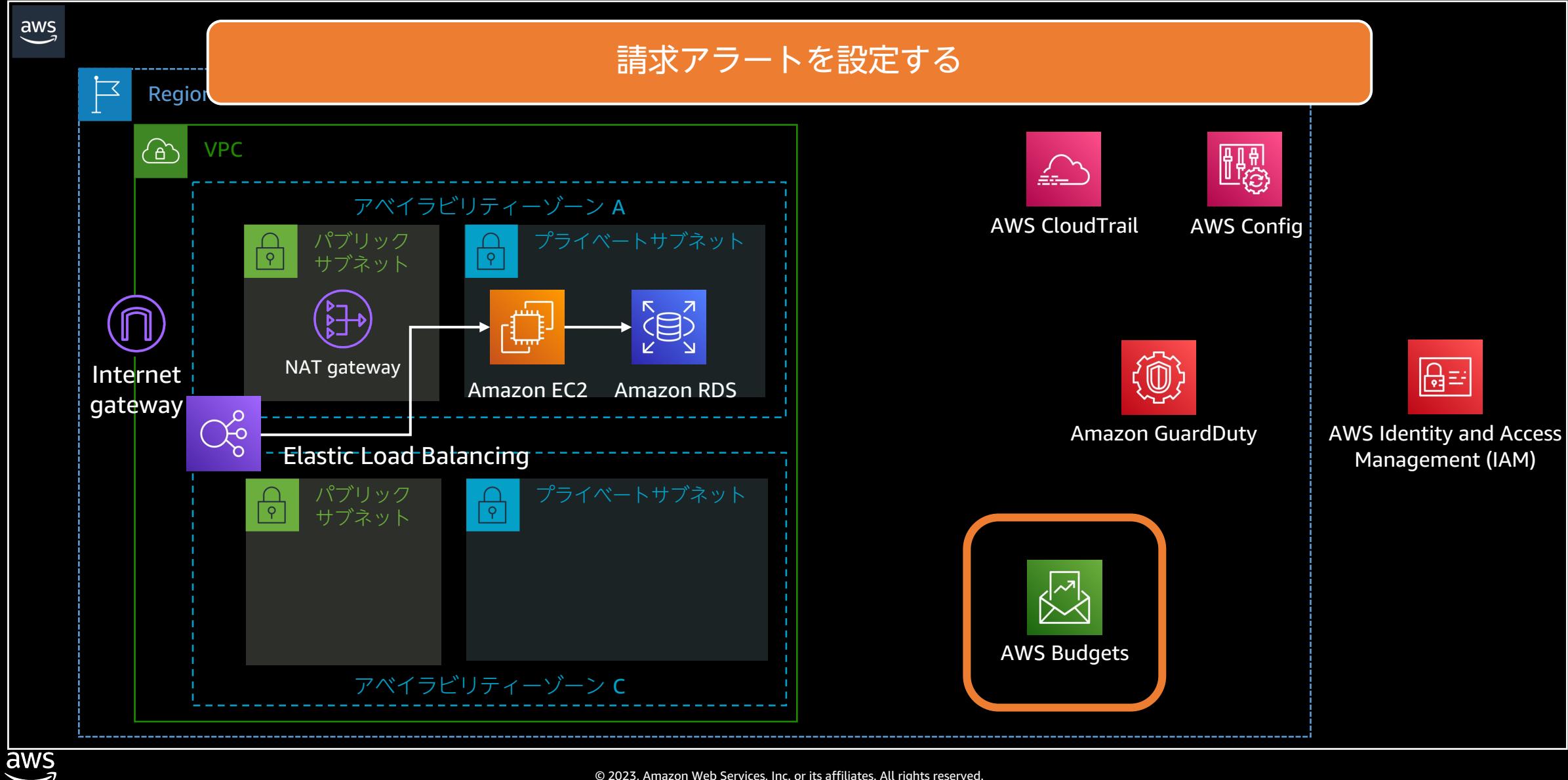
数クリックで利用開始

30 日間の無料トライアルでコスト感を把握

動画をご覧ください



コスト面での「安心」を確保する



AWS Budgets

柔軟な予算と予測による、計画とコストコントールの改善



- 実績または予測コストが、予算に対する「しきい値」を超えると警告メールで通知
- 予算の監視とアラート通知の受信は無料

AWS のコストと使用状況の追跡を開始する

予算を作成すると、AWS Budgets では、1 つの場所から予算の作成、支出の予測、コストと使用状況に対するアクションの実行が可能になります。

予算を作成する



予算タイプを選択 情報

予算タイプ

コスト予算 – 推奨
指定された金額に照らしてコストを監視し、ユーザークラウド支出を表します。例えば、ある事業部門に対す

使用量予算
指定された 1 つ、または複数の使用タイプまたは使用するときは、予算額が予想される使用量を表します



アラート番号 1

定義
予測コストが予算額(\$50.00) の 80% (\$40.00) を超えると、アラートのしきい値を超過します。

しきい値
 超過していません

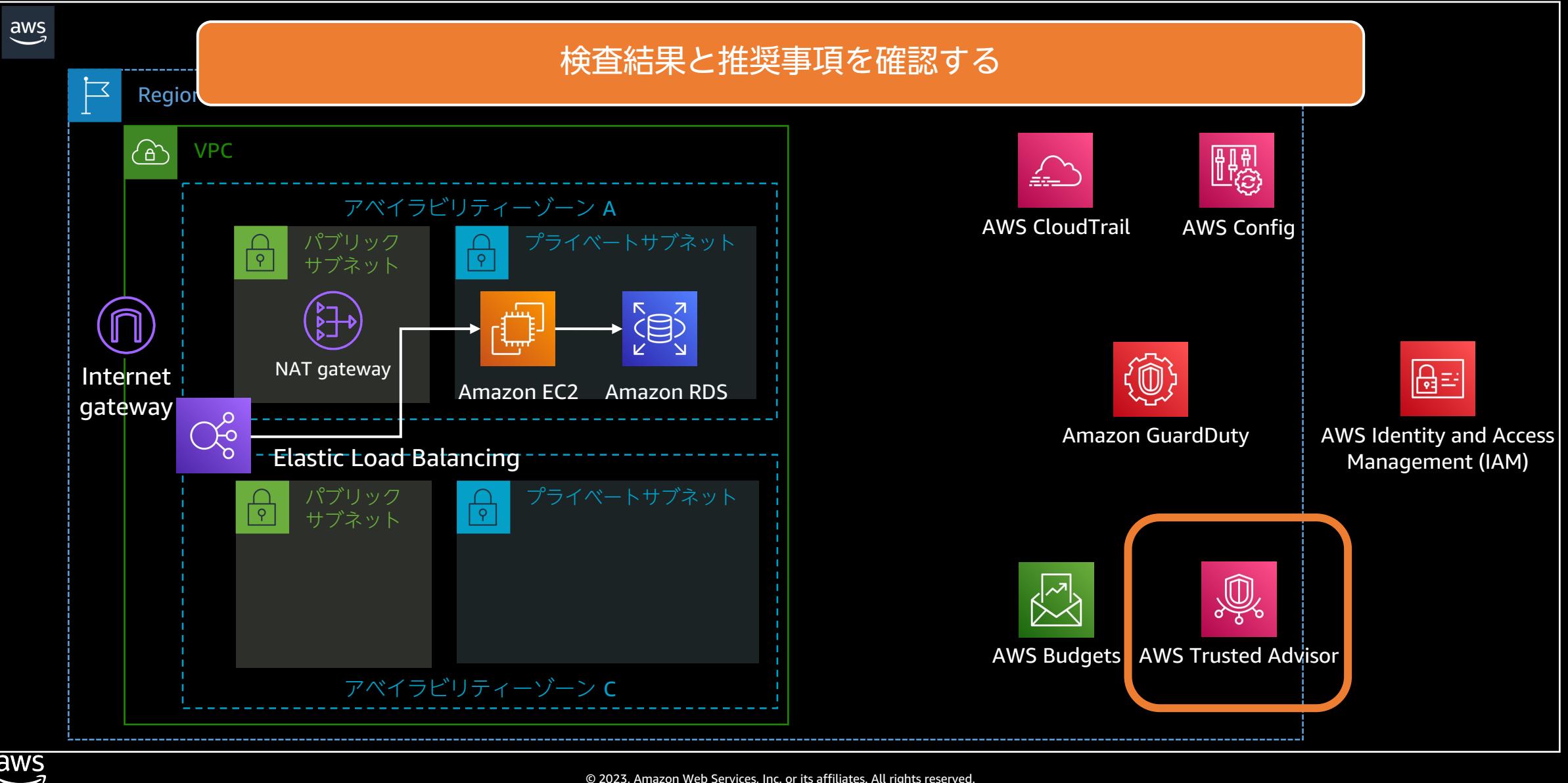
アクション
-

※ 同様のコストに関するアラートとして、機械学習を用いた AWS Cost Anomaly Detection は[こちら](#)

動画をご覧ください



継続的な改善へ取り組む



AWS Trusted Advisor

AWS のベストプラクティスに準拠するための推奨事項を提供



- AWS のベストプラクティスに準拠するための推奨事項を提供
- 5 つのカテゴリについてのチェックを実施
- ビジネス以上のサポート契約により全ての機能が利用可能

コスト最適化



パフォーマンス



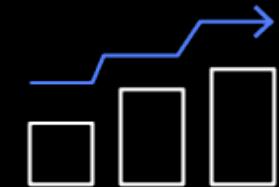
セキュリティ



耐障害性



サービスの制限

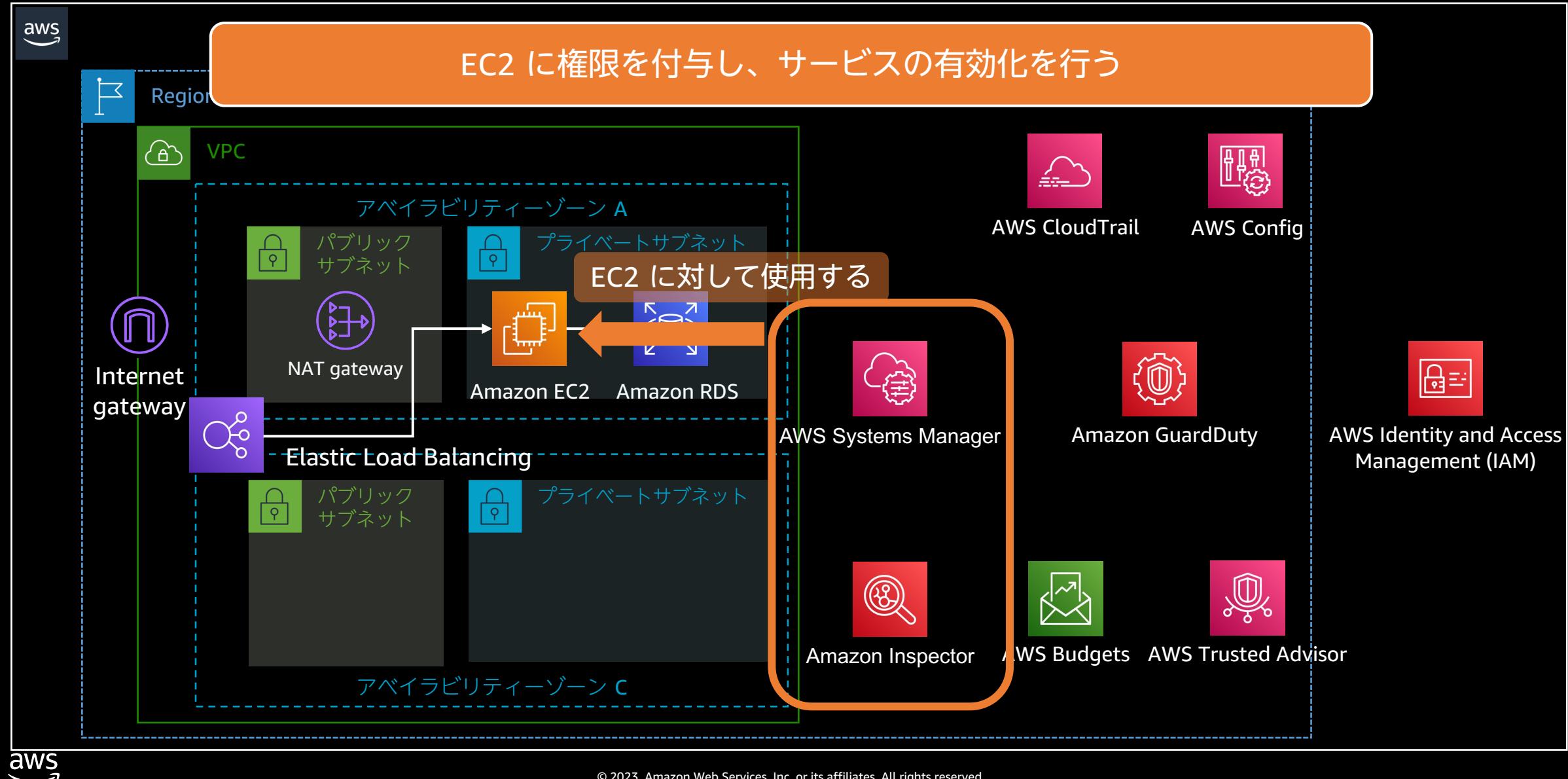


※ ベーシック及びデベロッパーサポートの場合には、セキュリティの一部とサービスの制限について利用できます

動画をご覧ください



仮想マシンの安全な運用を実現する



AWS Systems Manager (SSM)

AWS クラウドで実行されるアプリケーションとインフラストラクチャの管理に役立つ一連の機能を提供

運用編で更に詳しく扱います

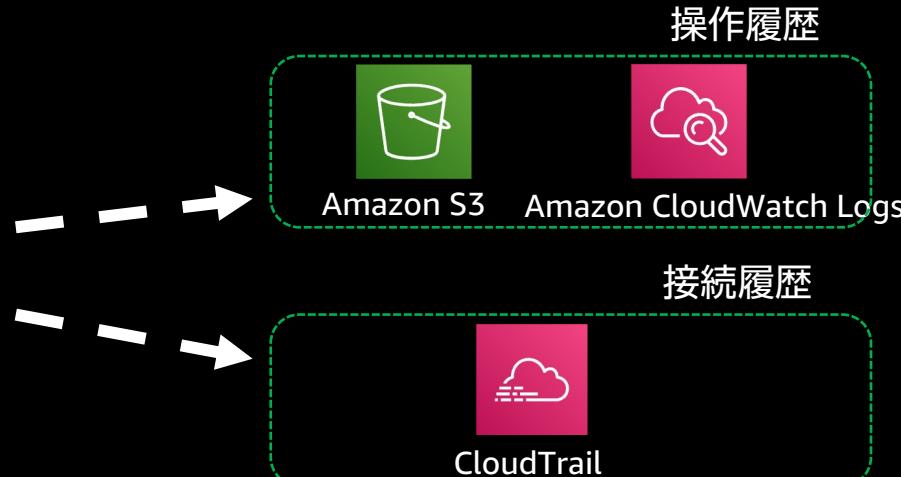


- AWS 環境の運用管理をスケーラブルかつコスト効率よく行うサービス群
- アプリケーションとインフラストラクチャを管理



エージェントを用いてマネージドインスタンス化

```
sh-4.2$  
sh-4.2$  
sh-4.2$ pwd  
/  
sh-4.2$ whoami  
ssm-user  
sh-4.2$ ps
```



SSM セッションマネージャによる
ブラウザからのシェル操作 (機能一例)

※ サーバーが Windows であれば、SSM Fleet Manager の機能を使用したリモートデスクトップ接続が使えます。

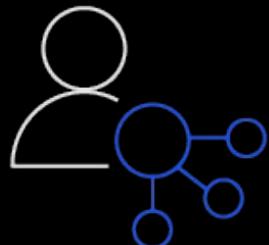
Amazon Inspector

自動化された脆弱性管理サービス

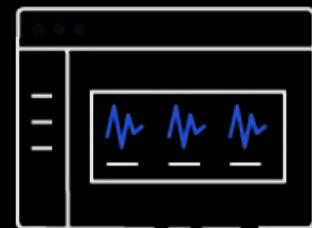


- ・自動化された脆弱性管理サービス
- ・対処すべき脆弱性リソースの優先順位付けを支援
- ・Amazon EventBridge や AWS Security Hub と統合し、脆弱性への対策措置のワークフローを自動化

シンプルで
大規模な管理



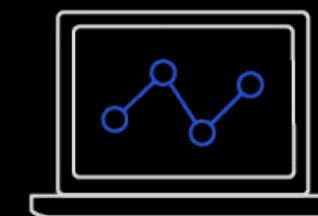
一元的に集約し
可視化



自動検出と継続的
なスキャン



スコア算出による
優先順位付け



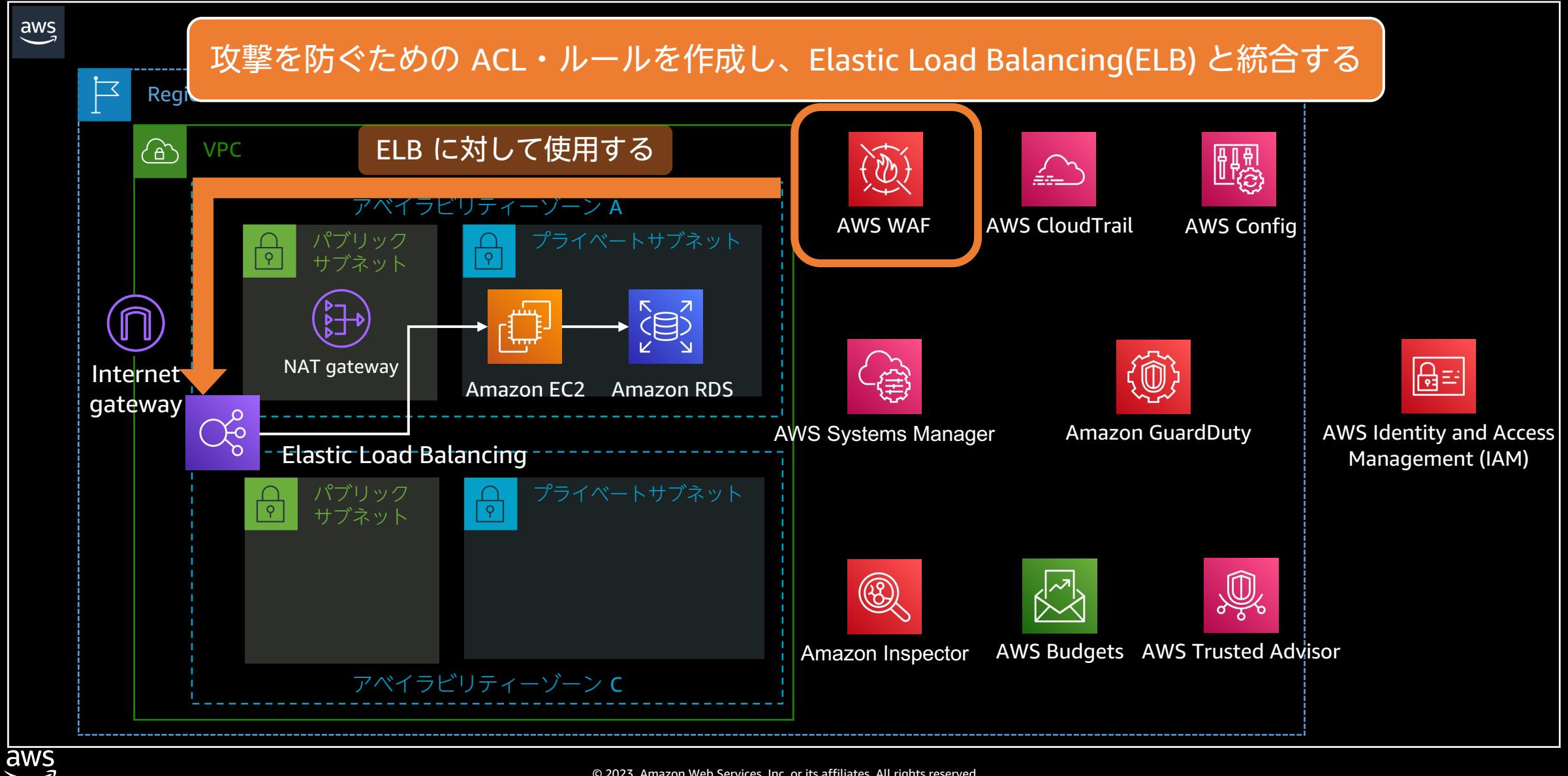
対策措置の
ワークフロー
自動化



動画をご覧ください



Web システムを攻撃から守る



AWS WAF

WEBアプリケーションの通信内容を検査し、不正なアクセスを遮断する



- ・ウェブアプリケーションの通信内容を検査し、不正なアクセスを遮断する
- ・マネージドルールの提供 (※自身でも作成できる)

悪意のあるリクエストのブロック



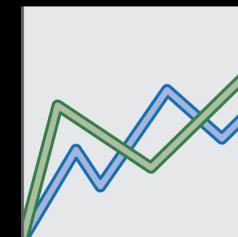
- ・SQLインジェクション
- ・クロスサイトスクリプト
- ・AWS、またはパートナー 提供のマネージドルール
- ・Bot Control
- ・Account Takeover Prevention

カスタムルールに基づいた Webトラフィックのフィルタ



- ・Rate-based rules
- ・IP & Geo-IP filters
- ・正規表現パターン、文字列
- ・サイズ制限
- ・アクション：許可/拒否
- ・Label

モニタリングとチューニング



- ・Amazon CloudWatch
- ・メトリクス/アラーム
- ・サンプルログ
- ・Full logs
- ・カウントアクション モード (検知モード)



動画をご覧ください



まとめ



おすすめしたいハンズオン

本セッションでご紹介した内容を、
具体的な画面とデモを見ながら進めることができるハンズオンです

AWS アカウントに対するセキュリティ対策



「Z1 関連資料」にて、今すぐお試し可能です

おすすめしたいハンズオン

本セッションでご紹介した内容を、
具体的な画面とデモを見ながら進めることができるハンズオンです

基本的な Web システムに対するセキュリティ対策

[ハンズオン]
AWS Systems Manager を使った
サーバ管理はじめの一歩編



※ Amazon Inspector は含みません

[ハンズオン]
Amazon CloudFront および AWS WAF を用いて
エッジサービスの活
用方法を学ぼう



※ Elastic Load Balancing は含みません

「Z1 関連資料」にて、今すぐお試し可能です



さいごに

- 数多くのセキュリティ施策から**厳選した対策**をデモを通して紹介
 - AWS アカウントをセキュアにしよう / AWS Identity and Access Management
 - AWS で起きた事実を記録しよう / AWS CloudTrail, AWS Config
 - セキュリティ脅威を自動的に検知しよう / Amazon GuardDuty
 - コスト面での「安心」を確保しよう / AWS Budgets
 - 継続的な改善へ取り組もう / AWS Trusted Advisor
 - 仮想マシンの安全な運用を実現しよう / AWS Systems Manager, Amazon Inspector
 - Webシステムを攻撃から守ろう / AWS WAF
- 今回ご紹介したサービスと機能を、
お客様のセキュリティを高めるための「基礎」としてご活用ください



AWS TRAINING & CERTIFICATION

AWS Skill Builder の 500+ の 無料デジタルコースで学ぼう

30以上のAWSソリューションの中から、自分に最も関係のあるクラウドスキルとサービスにフォーカスし、自習用のデジタル学習プランとRamp-Upガイドで学ぶことができます。

- 自分のペースでAWSクラウド上を活用した未来を切り開く
- 学習プランでスキルや知識を向上
- AWS認定資格でクラウドの専門知識を証明する



自分に合ったスキルアップ方法をで学びましょう
[EXPLORE.SKILLBUILDER.AWS »](https://explore.skillbuilder.aws)



AWS Builders Online Series に ご参加いただきありがとうございます

楽しんでいただけましたか? ぜひアンケートにご協力ください。
本日のイベントに関するご意見/ご感想や今後のイベントについての
ご希望や改善のご提案などございましたら、ぜひお聞かせください。



aws-apj-marketing@amazon.com



twitter.com/awscloud_jp



facebook.com/600986860012140



<https://www.youtube.com/user/AmazonWebServicesJP>



<https://www.linkedin.com/showcase/aws-careers/>



twitch.tv/aws



Thank you!

