目次

セキュリティ

この章ではセキュリティに関するサービスについて説明します。内容は以下の通りです。

- セキュリティサービスの概要
- WAFの設定
- GuardDutyの設定
- TrustedAdvisorの確認

※セキュリティについてテストをする場合、AWSへの申請が必要になります。そのため、本書ではセキュリティを設定するところまでハンズオンで行います。

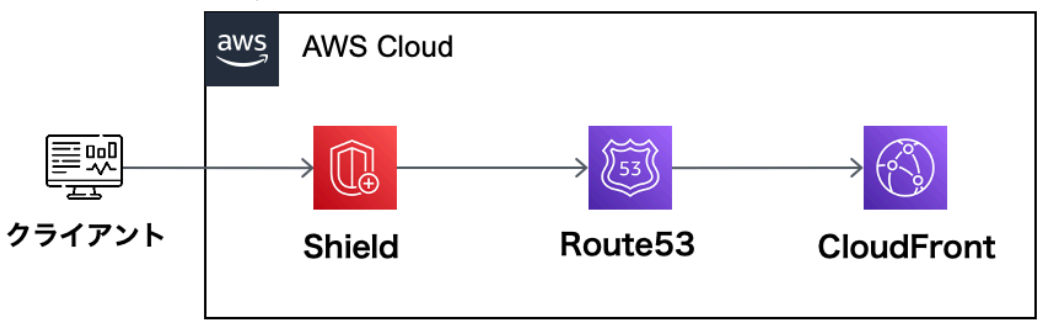
セキュリティサービスの概要

この節では、AWSの各種セキュリティサービスについて説明します。

AWS Shield

AWS Shield(以下、Shield)とは、DDos攻撃対策のサービスです。DDos攻撃とは、サーバーに大量のリクエストを送りつけて、サーバーを高負荷・停止させる攻撃のことです。AWSの発表では、DDos攻撃は年々増加しています。

Shieldはエッジロケーション上でDDos攻撃対策を行います。CloudFrontやDNSサービスであるRoute53の前に配置します。



■プラン

ShieldにはStandardとAdvancedの2つのプランがあります。Standardはデフォルトで有効化されています。Advancedは1年間の契約を前提とする有料のプランです。AdvancedはStandardよりも機能が豊富にあります。特に、DDos攻撃を受けた際のコスト保護機能があります。リクエスト急増によるリソース使用量が増加したとします。Standardではコストの支払いが必要となります。Advancedでは、コスト保護機能があります。

通常はStandardで十分です。DDos攻撃の対象になる可能性が高い場合、Advancedの導入を検討します。以下のサイトにて、StandardとAdvancedの比較表が載っています。

[保護計画を選択するためのヒント]

https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/ddos-overview.html#ddos-help-me-choose

■料金

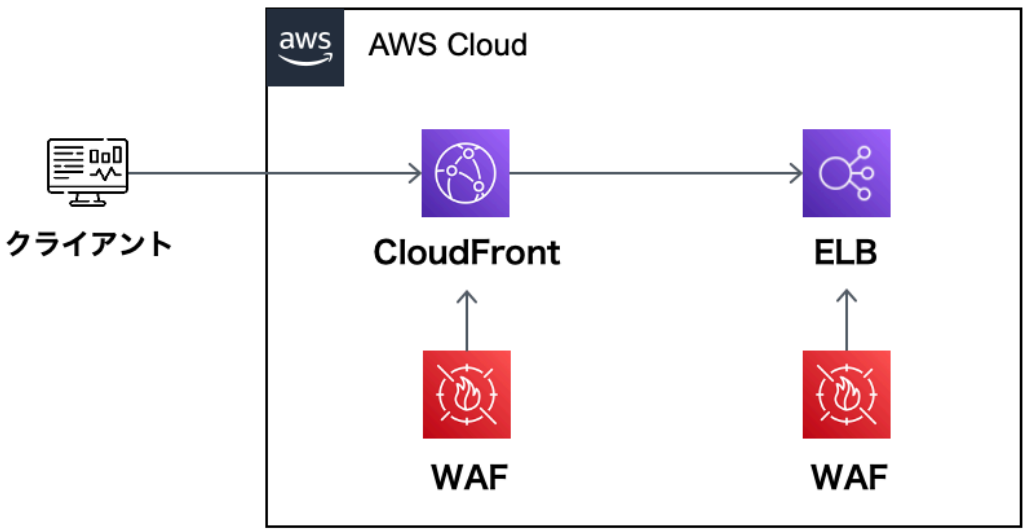
Standardは無料で利用できます。Advancedは月額の固定料金が発生します。また、Advancedではデータ転送量による従量課金が発生します。詳細は以下のサイトで確認できます。

[AWS Shield 料金]

https://aws.amazon.com/jp/shield/pricing/

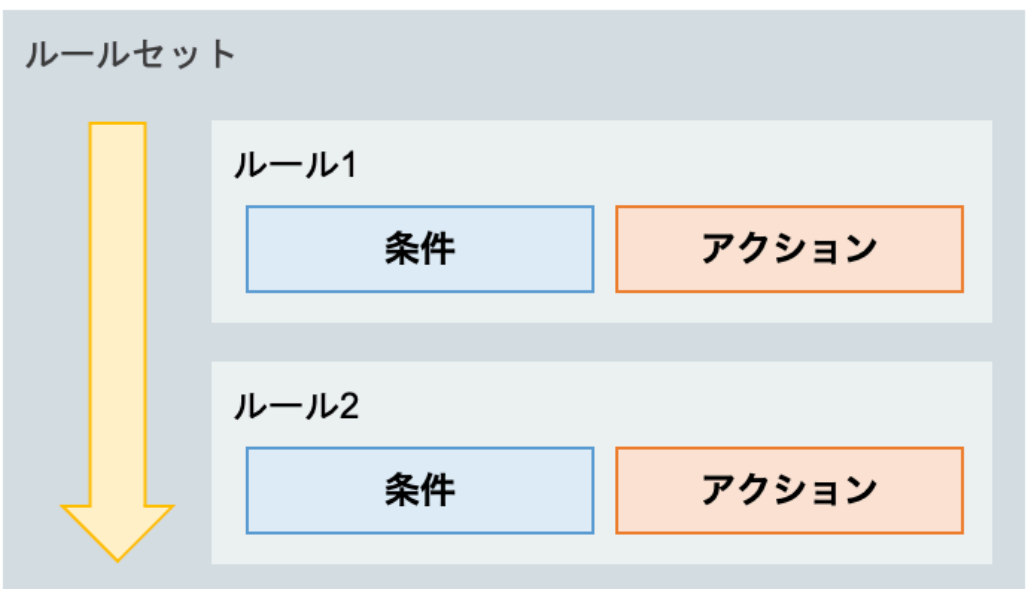
WAF

Web Application Firewall(以下、WAF)とは、通信内容を検査して、不正アクセスを遮断するセキュリティサービスです。CloudFrontなどに適用することで、セキュリティ対策をすぐに講じることができます。



■ルール

WAFでは、ルールベースのセキュリティ設定をします。ルールには条件とアクションを設定します。そして、それらのルールをまとめることで、ルールセットを作成できます。



■ルールの種類

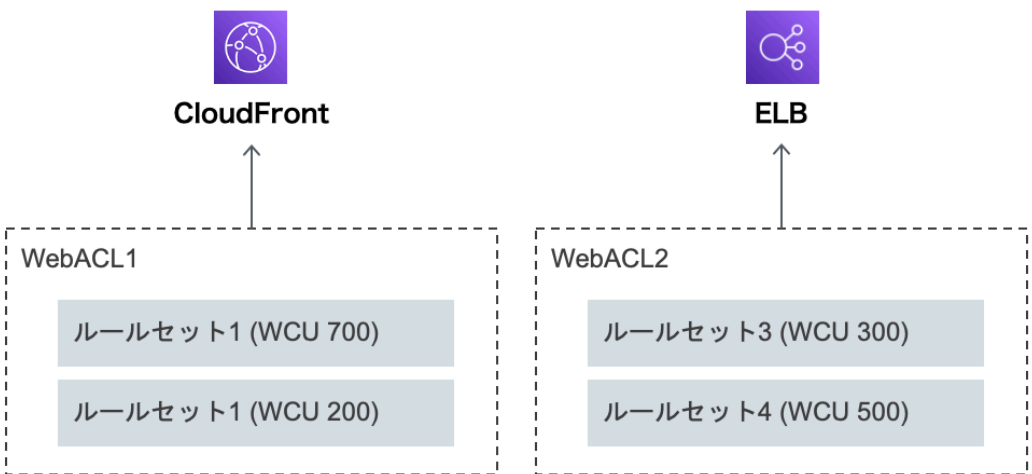
ルールにはカスタムルールとマネージドルールがあります。カスタムルールは、任意に作成したルールです。マネージドルールはAWSが用意しているルールです。

マネージドルールを使用すれば、一般的なセキュリティ対策(SQLインジェクションやクロスサイトスクリプティング)や、OWASP Top 10についての対策をすぐに設定できます。マネージドルールは定期的に更新されているため、セキュリティ対策についての運用も簡単になります。

> **補足: OWASP Top 10とは**
>
> OWASPはソフトウェアセキュリティを向上させることを目的とする非営利団体です。OWASP Top 10とは、Webアプリケーションについての10大リスクです。リスクがランキング形式で表されています。

■WAF Capacity Unit

WAFの設定単位のことをWebACLと言います。WebACLの中には複数のルールセットを持つことができます。ただし、ルールにはそれぞれポイントがあります。このポイントのことをWAF Capacity Unit(以下、WCU)と言います。1つのWebACL内で使用できるWCUの上限は1,500です。この上限を超えないようにルールセットを決定します。



CloudFrontとALB用に別々のWebACLを作成することもできます。

■対象リソース

WAFは以下のリソースにアタッチできます。

- CloudFront
- ALB
- API Gateway
- AWS AppSync

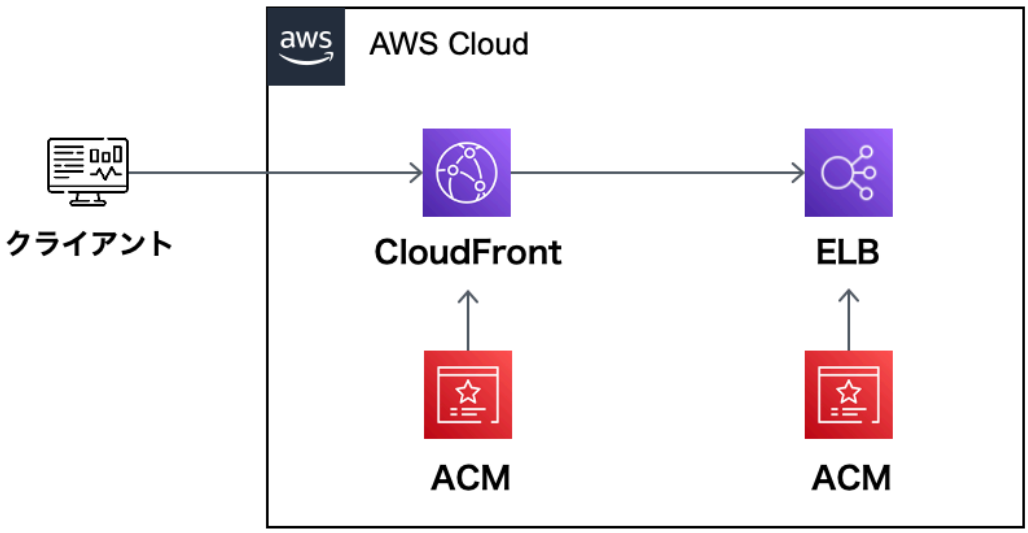
■料金

WAFは以下の使用量に応じて課金されます。

- WebACLの数
- ルール数
- リクエスト数

AWS Certificate Manager

AWS Certificate Manager(以下、ACM)は、SSL/TLS証明書を管理するサービスです。ACMでは証明書を簡単に取得できます。取得した証明書をCloudFrontなどに簡単にデプロイできます。



SSL/TLS証明書の使用は必須と言えます。Googleの検索エンジンでもHTTPSで通信できるサイトを優先表示するようになっています。

■対象リソース

ACMで証明書をデプロイできるリソースは以下になります。

- Route53
- CloudFront
- ELB
- API Gateway

※1つの証明書を複数のELBで使用することが可能です。

※Route53、CloudFrontでACMを使用する場合、米国東部(バージニア北部)でデプロイします。それにより、全てのエッジロケーションに証明書がプロビジョニングされます。

■証明書の自動更新

証明書には有効期限があります。有効期限が切れると通信ができなくなってしまいます。そのため、証明書の有効期限切れだけは起こさないように注意が必要です。ACMは証明書を自動で更新します。そのため、運用も簡単になります。ただし、自動更新には条件があります。詳細は以下のサイトをご確認ください。

[ACM 証明書のマネージド更新]

https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/managed-renewal.html

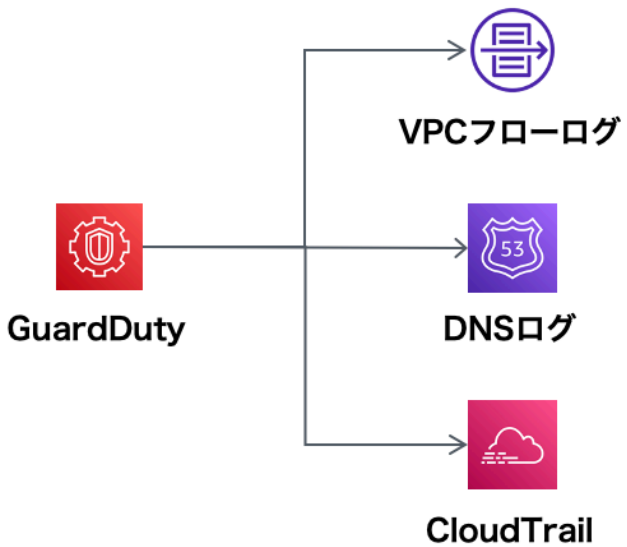
■料金

ACMは無料で使用できます。

GuardDuty

GuardDutyは、機械学習による監視、脅威の検知を行うサービスです。1クリックで有効化するだけで、セキュリティ監視の運用負荷を低減できます。なお、リージョン単位で有効化します。

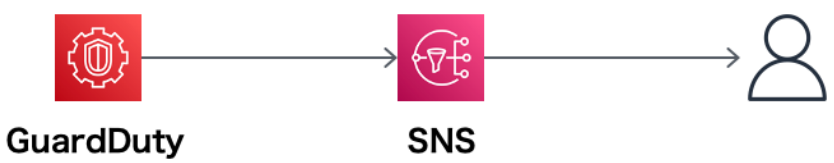
GuardDutyでは、VPCフローログ、DNSログ、CloudTrailを監視して脅威を発見します。



※VPCフローログなどを有効化しなくても、GuardDutyが監視してくれます。

■通知

脅威を検知して通知するためには、他サービスとの連携が必要です。



■料金

データソースの使用量によって課金されます。具体的には以下の使用量です。

- VPCフローログ(GB)
- DNSログ(GB)
- CloudTrailのイベント数

なお、GuardDutyを有効化して最初の30日間は無料で使用できます。

Trusted Advisor

AWS Trusted Advisor(以下、Trusted Advisor)とは、AWS環境を分析して、環境を最適化するためのベストプラクティスを提供するサービスです。以下のカテゴリーについてチェックされます。

- コスト最適化
- パフォーマンス
- セキュリティ
- フォールトトレランス
- サービス制限

ベストプラクティスに沿ってない設定があれば、ダッシュボードにアラート表示されます。

■プラン

Trusted Advisorがチェックする内容は、契約しているサポートプランにより異なります。ビジネス以上のプランであれば、全てのチェックを実施してくれます。

プラン	デベロッパー	ビジネス	エンタープライズ On-Ramp	エンタープライズ
Trusted Advisor	一部のみ	全てチェック	全てチェック	全てチェック

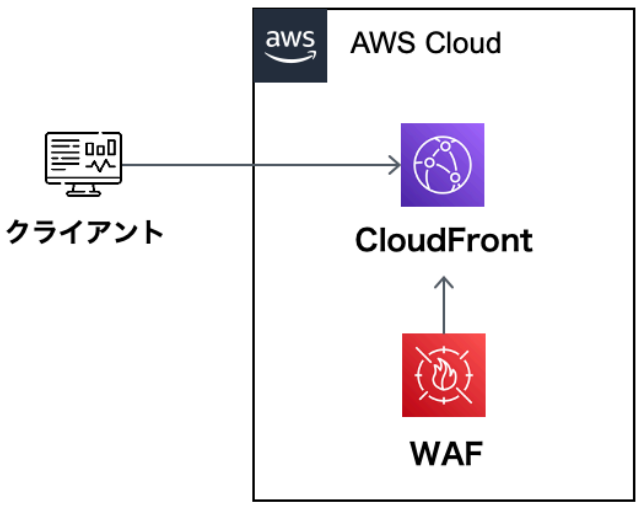
各プランの詳細は以下のサイトで確認できます。
[AWS Support プラン比較]
https://aws.amazon.com/jp/premiumsupport/plans/

■料金

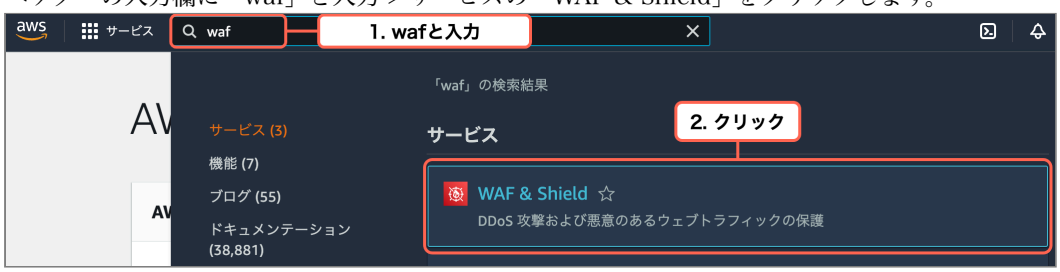
Trusted Advisorは無料で使用できます。

WAFの設定

この節では、WAFをCloudFrontに設定します。



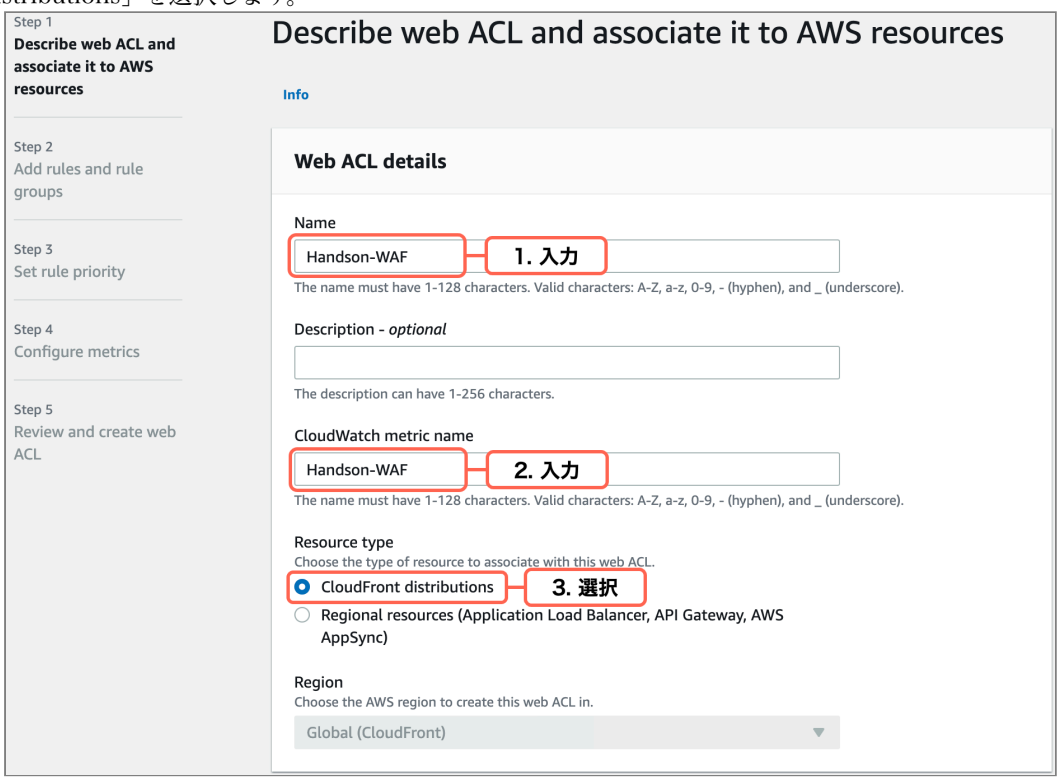
ヘッダーの入力欄に「waf」と入力 > サービスの「WAF & Shield」をクリックします。



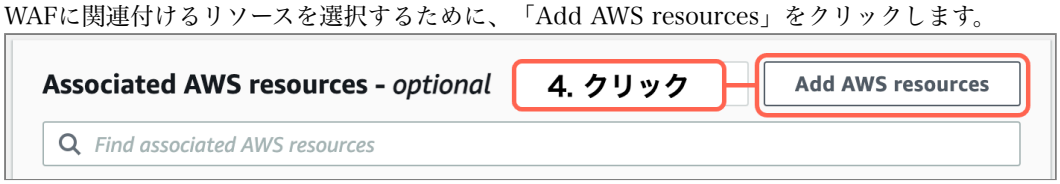
※執筆時点ではWAF & Shieldの画面が日本語対応していません。いずれ日本語対応されると思われます。

「Create web ACL」をクリックします。

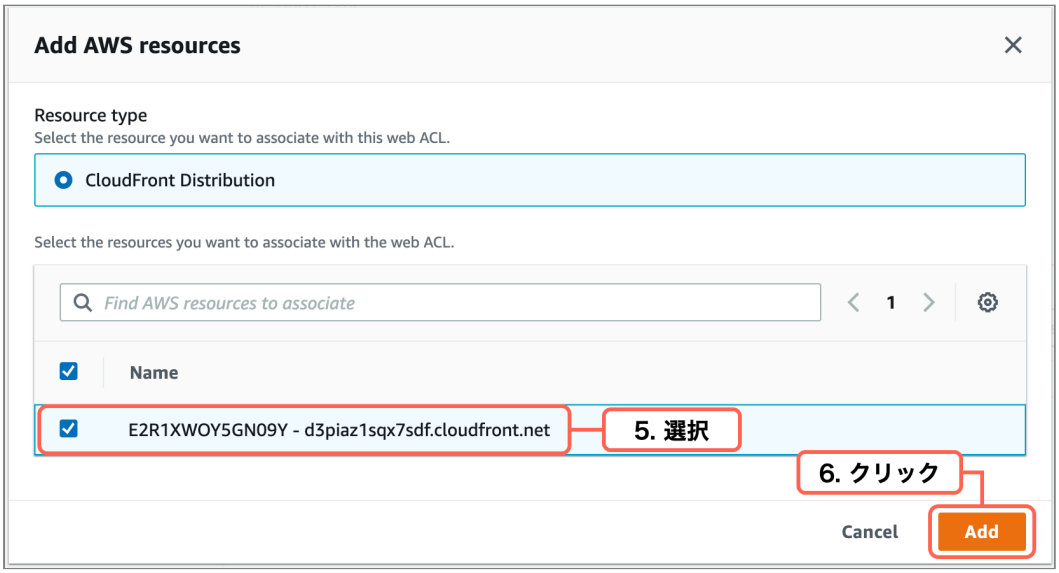
「Name」、「CloudWatch metric name」を入力します。Resouce typeで「CloudFront distributions」を選択します。



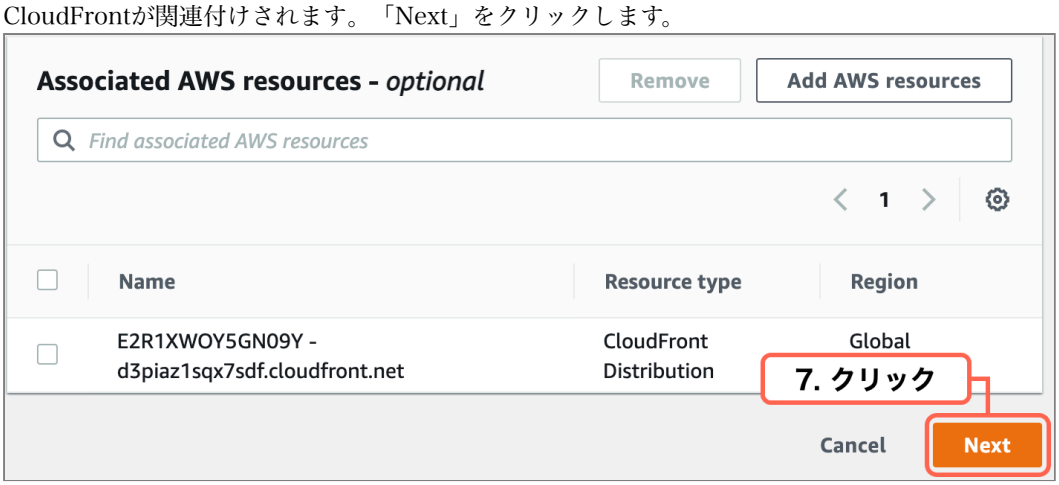
WAFに関連付けるリソースを選択するために、「Add AWS resources」をクリックします。



作成したCloudFrontのディストリビューションを選択 > 「Add」をクリックします。

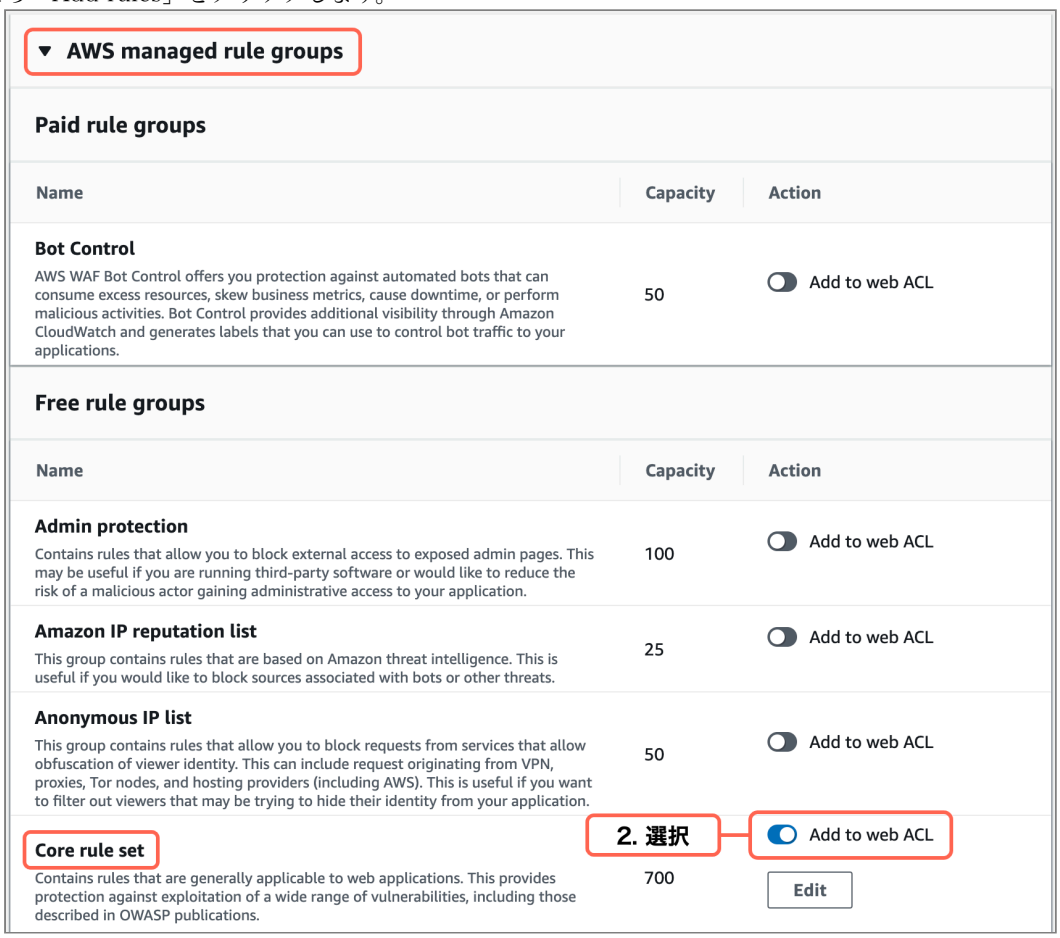


CloudFrontが関連付けされます。「Next」をクリックします。

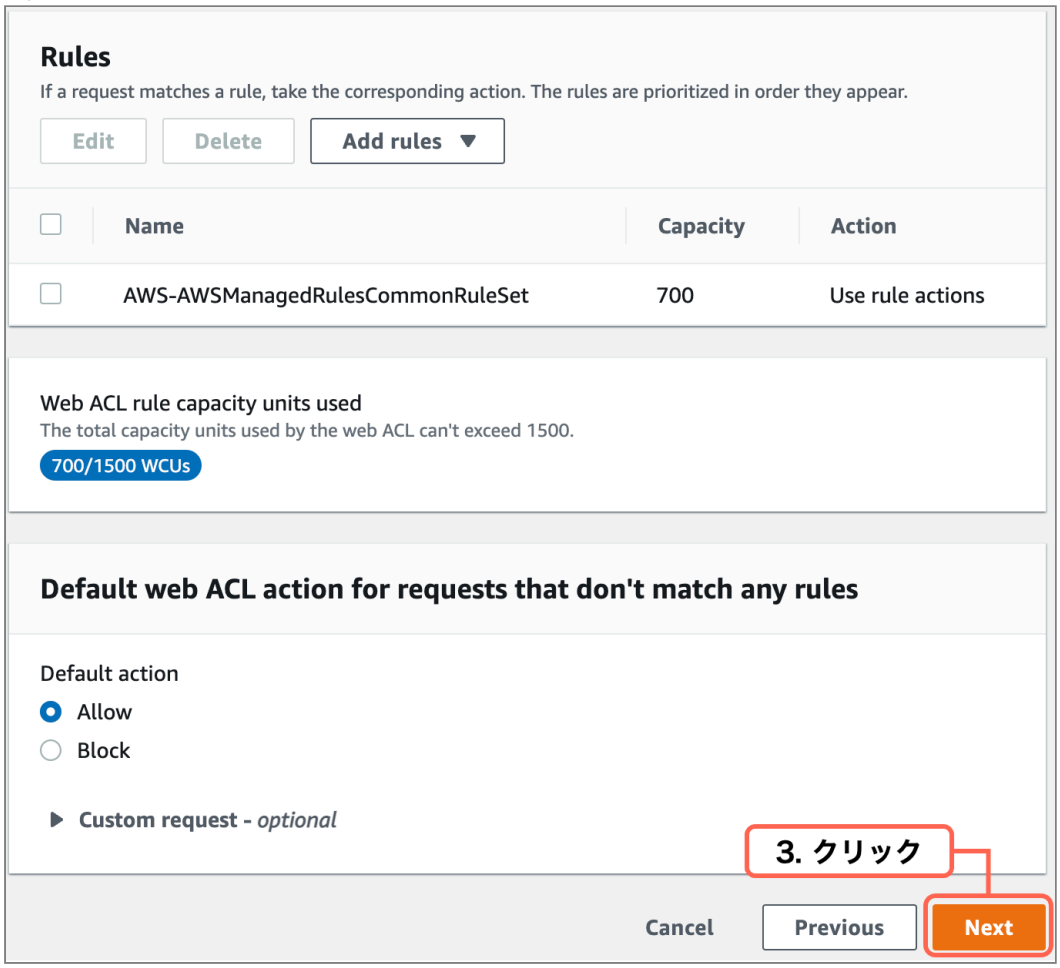


次の画面で適用するルールを設定します。本書では、AWSが用意しているルールを設定します。「Add rules」 > 「Add managed rule groups」をクリックします。

「AWS managed rule groups」 > 「core rule set」の「Add to web ACL」を選択します。選択したら「Add rules」をクリックします。



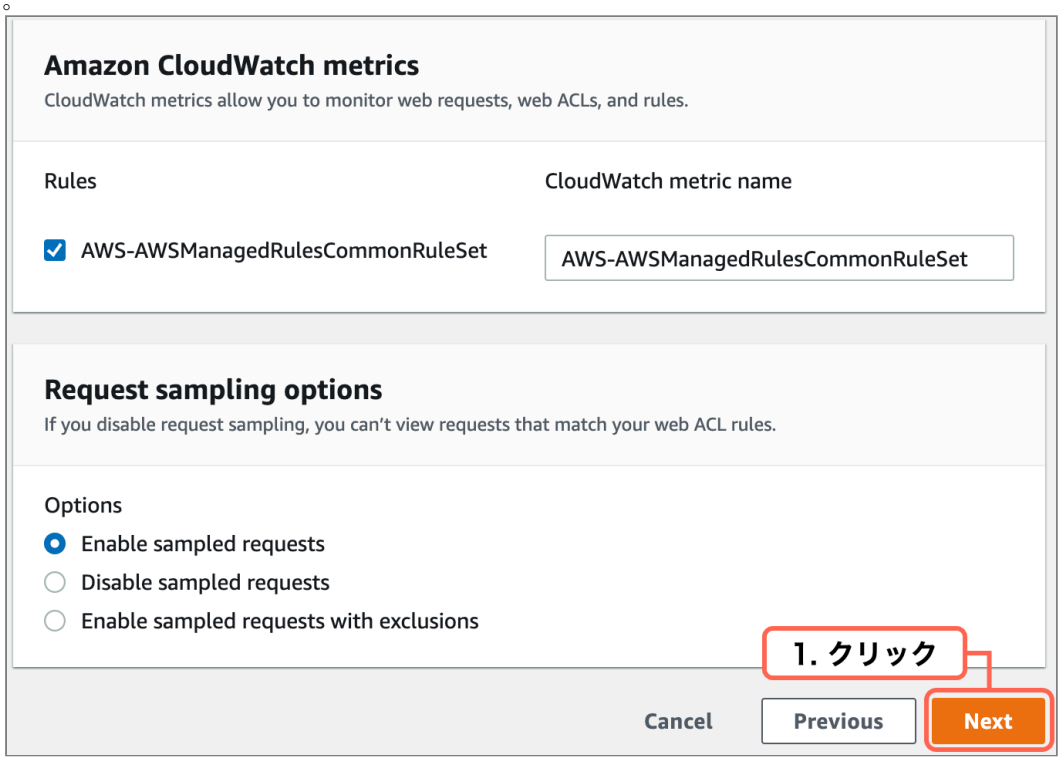
ルールが追加されて、WCUを700ポイント消費していることが分かります。「Next」をクリックします。



なお、ルールに一致しなかった場合のアクションをDefault web ACL Actionで設定できます。

ルールセットの優先順位を決める画面です。優先順位により、ルールセットが適用される順番を設定できます。ルールセットは1つしかないため、「Next」をクリックします。

CloudWatchのメトリクスなどを設定する画面です。設定を何も変更せずに「Next」をクリックします。



あとは確認画面が表示されます。問題なければWAFを作成します。

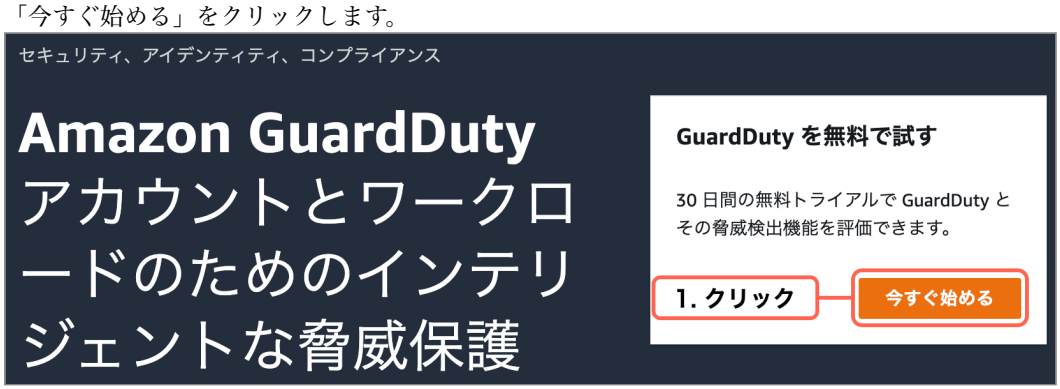
CloudFrontにWAFが関連付けされているか確認します。CloudFrontのディストリビューション一覧を表示します。作成したディストリビューションをクリックします。

ディストリビューションの詳細画面にて、WAFが関連付けされています。WAFが関連付けされるまでに数分かかります。これでWAFの設定は完了です。

GuardDutyの設定

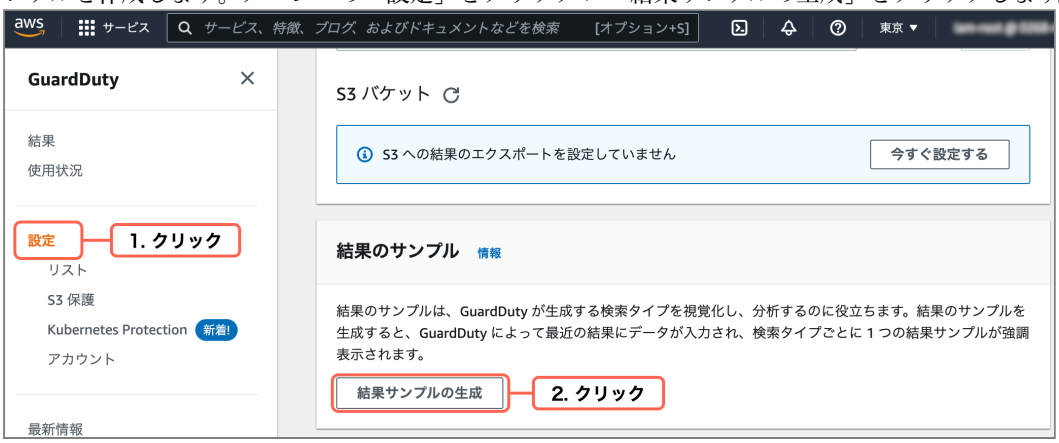
この節ではGuardDutyの設定を有効にします。ヘッダーの入力欄に「guard」と入力 > サービスの「GuardDuty」をクリックします。

「今すぐ始める」をクリックします。

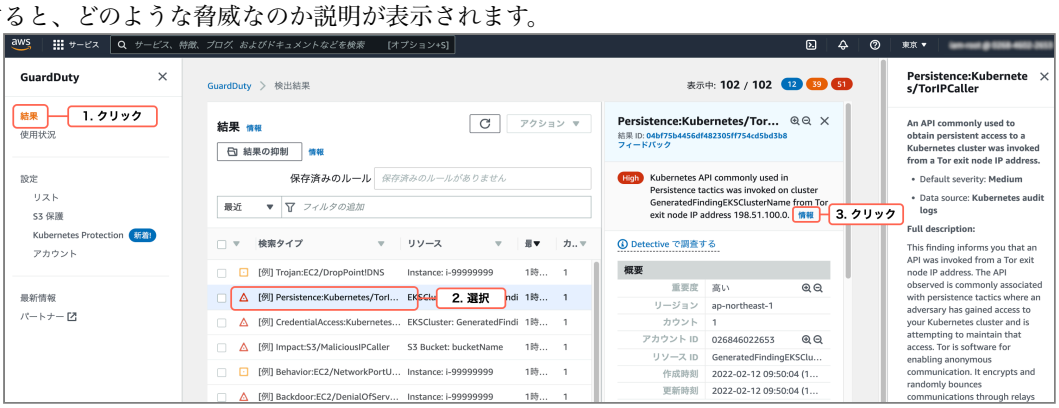


「GuardDutyの有効化」をクリックします。これで有効化は完了です。

有効化しただけでは、GuardDutyの使い方が分かりません。GuardDutyで脅威が検出された場合のサンプルを作成します。メニューの「設定」をクリック＞「結果サンプルの生成」をクリックします。



メニューの「結果」をクリックします。すると、検出された脅威の一覧(サンプル)が表示されます。試しに、一覧のどれかを選択します。すると、右側に脅威の詳細が表示されます。「情報」をクリックすると、どのような脅威なのか説明が表示されます。



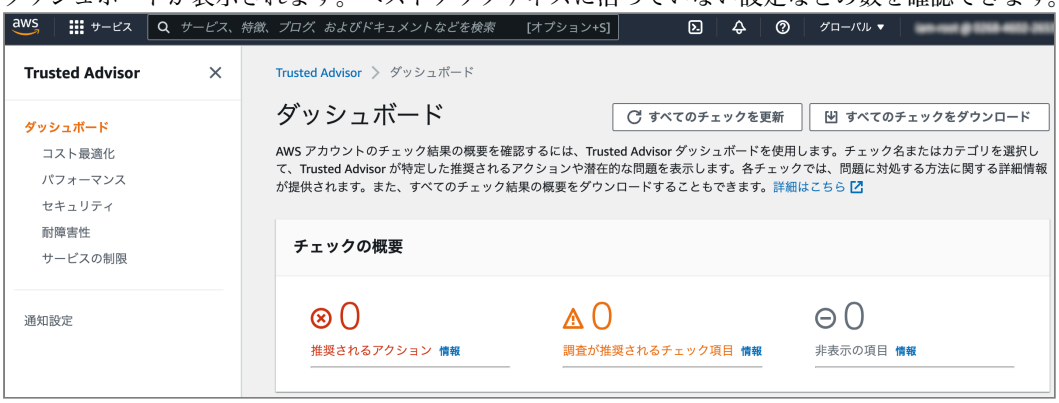
次にGuardDutyのコストを表示します。メニューの「使用状況」をクリックします。無料トライアル期間中は表示されませんが、GuardDutyにかかるコストについて確認できます。

これでGuardDutyの設定は完了です。

TrustedAdvisorの確認

この節ではTrustedAdvisorを確認します。ヘッダーの入力欄に「trust」と入力 > サービスの「Trusted Advisor」をクリックします。

ダッシュボードが表示されます。ベストプラクティスに沿っていない設定などの数を確認できます。

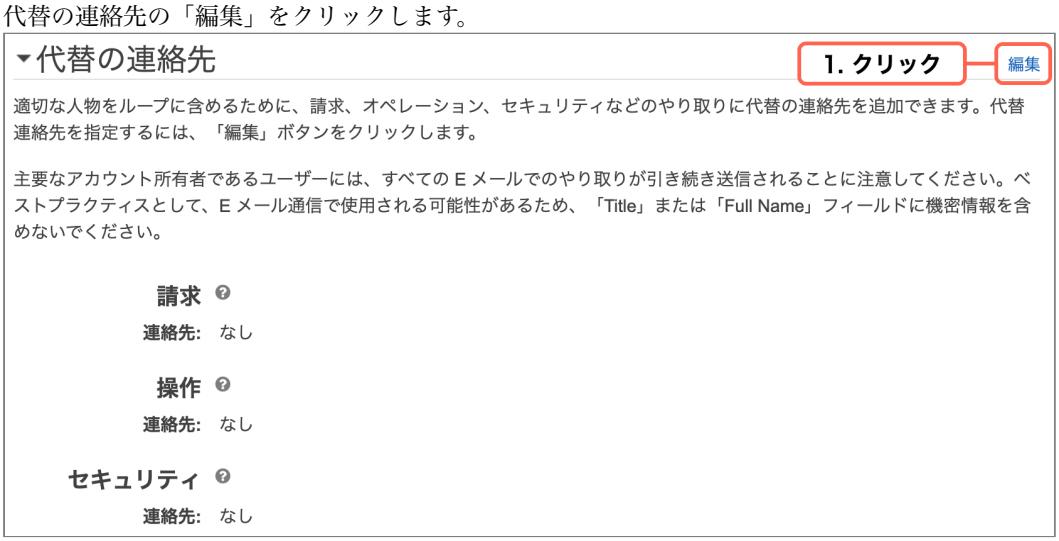


次にTrusted Advisorのチェック内容を表示します。メニューの「セキュリティ」をクリックします。Trusted Advisorがセキュリティ面でチェックしている内容と結果が一覧表示されます。

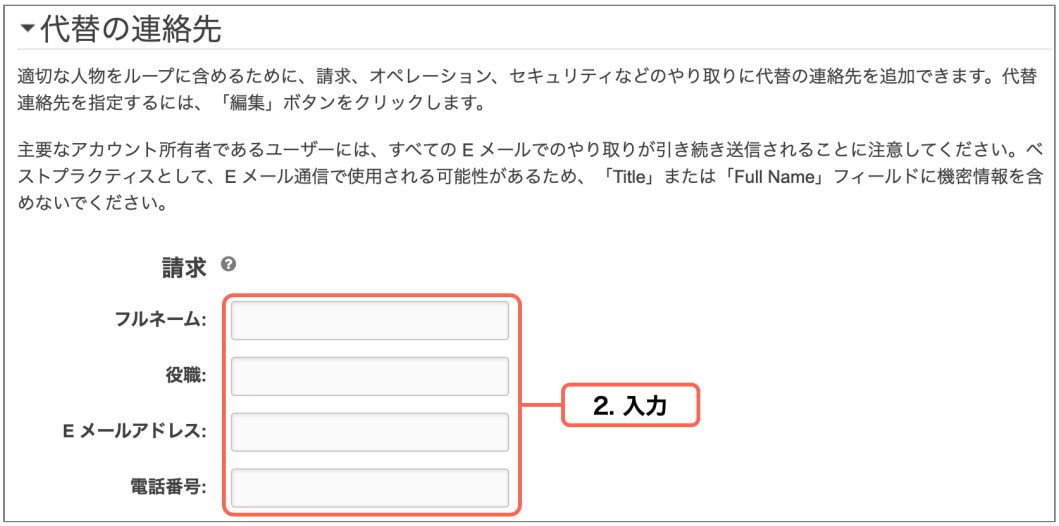
次にTrusted Advisorの通知設定を行います。この操作はIAMルートユーザーではなく、ルートユーザーで行います。設定する場合、ルートユーザーでログインし直してください。

メニューの「通知設定」をクリック＞「アカウント設定」をクリックします。

代替の連絡先の「編集」をクリックします。



代替の連絡先を入力して「更新」をクリックします。



Trusted Advisorの画面に戻って、画面をリロードします。通知したい連絡先にチェックを入れます。「メールの設定を保存」をクリックします。

これでTrusted Advisorの設定は完了です。

まとめ

この章で学んだ内容は以下の通りです。

[セキュリティサービスの概要]

- ACMはSSL/TLS証明書の管理を行うためのサービスです。
- WAFは、典型的なセキュリティ対策(XSS、SQLインジェクションなど)を行うサービスです。マネージドルールを使用すれば、すぐにセキュリティ対策ができます。
- ShieldはDDos攻撃対策を行うサービスです。Standard版がデフォルトで有効となっています。Standardは無料です。
- GuardDutyは、機械学習により脅威を検知するサービスです。VPCフローログ、DNSログ、CloudTrailの内容をチェックします。
- TrustedAdvisorを使用すると、ベストプラクティスに沿っているかどうかチェックできます。サポートプランによって、チェックできる内容が変わります。

リソース削除

この章では、今まで作成してきたリソースを削除します。サービスによっては、リソースを放置していても課金されてしまいます。

リソースを削除するためには、関連しているリソースから削除しなければいけないものがあります。そのため、以下の順番でリソースを削除していってください。

- GuardDuty
  - GuardDuty画面のメニューの「設定」をクリック > 「GuardDutyの無効化」をクリックします。

- WAF
  - WAF画面のメニューの「Web ACLs」を選択 > 「Global(CloudFront)」をクリック > 作成したWebACLをチェック > 「Delete」をクリックします。