このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報についてはサービス別資料もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar] AWS Shield Advanced

サービスカットシリーズ

Solutions Architect, Edge Services
岡　豊

2020/08/18

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

自己紹介

岡　豊（おか　ゆたか）

所属：Edge サービス担当ソリューションアーキテクト

好きなAWSのサービス：

- Amazon CloudFront
- AWS WAF
- AWS Shield Advanced
- AWS Certificate Manager

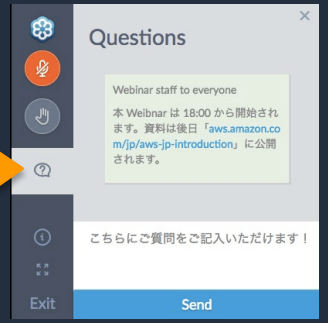
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
  お答えできませんのでご了承下さい

① 吹き出しをクリック
② 質問を入力
③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2020年08月18日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(http://aws.amazon.com) にてご確認ください。

- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。

- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

本セミナーの概要

- 本セミナーで学習できること
  - 典型的な DDoS 攻撃の手法と最近のDDoS 攻撃の傾向
  - AWS Shield Advanced とはどのようなサービスか
  - DDoS の耐性が高いアーキテクチャ
- 主な対象者
  - セキュリティ担当者
  - DDoS 対策に関心のある方
  - AWS Shield Advanced の導入をご検討されている方

本日のアジェンダ

1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS 耐性の高いアーキテクチャ
7. Firewall Manager の活用
8. 料金体系
9. まとめ

本日のアジェンダ

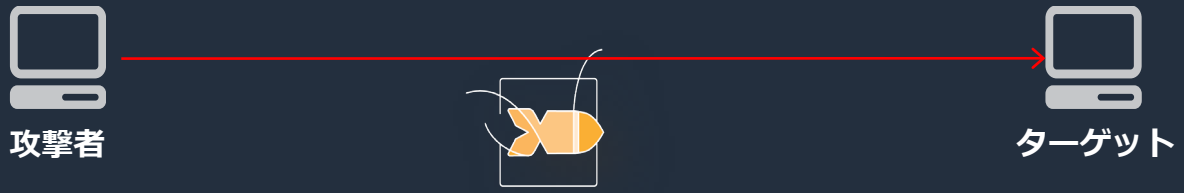
1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS Resiliency Architecture
7. Firewall Manager の活用
8. 料金体系
9. まとめ

インターネット上の脅威

誰でもアクセスが可能なインターネットでは攻撃者もアクセスができる

DoS

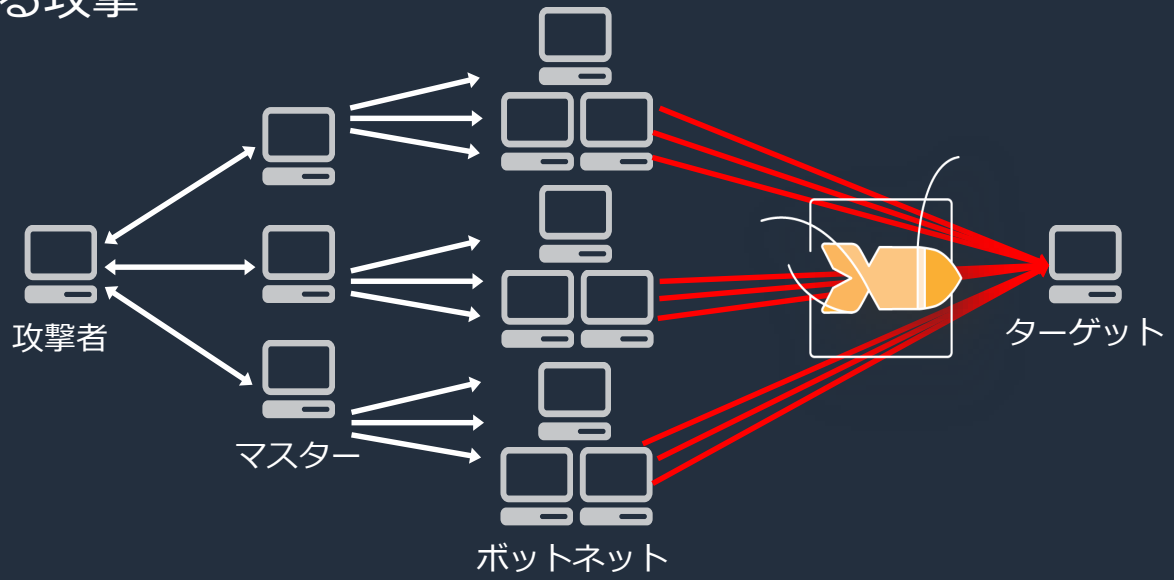
Denial of Service Attack (DoS 攻撃) のこと
サービスを不能にすることを目的とした、単一のリソースからターゲットに対する攻撃



DDoS (Distributed Denial of Service)

Distributed Denial of Service Attack

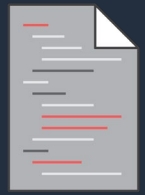
サービスを不能にすることを目的とした、分散された複数のリソースからターゲットに対する攻撃



1つ1つのリクエスト/パケットは悪意のあるものと区別がつかないケースがある
量が多いため攻撃の対策が難しい

攻撃の種類

DDoS



Application Attacks

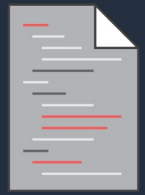
Bad Bots

	DDoS	Application Attacks	Bad Bots
Application Layer	HTTP floods Slowloris	SQL injection Application exploits	Crawlers Content scrapers Scanners & probes
Network/ Transport Layer	UDP floods SSL abuse SYN floods UDP reflection		

aws

攻撃の種類

DDoS



Application Attacks

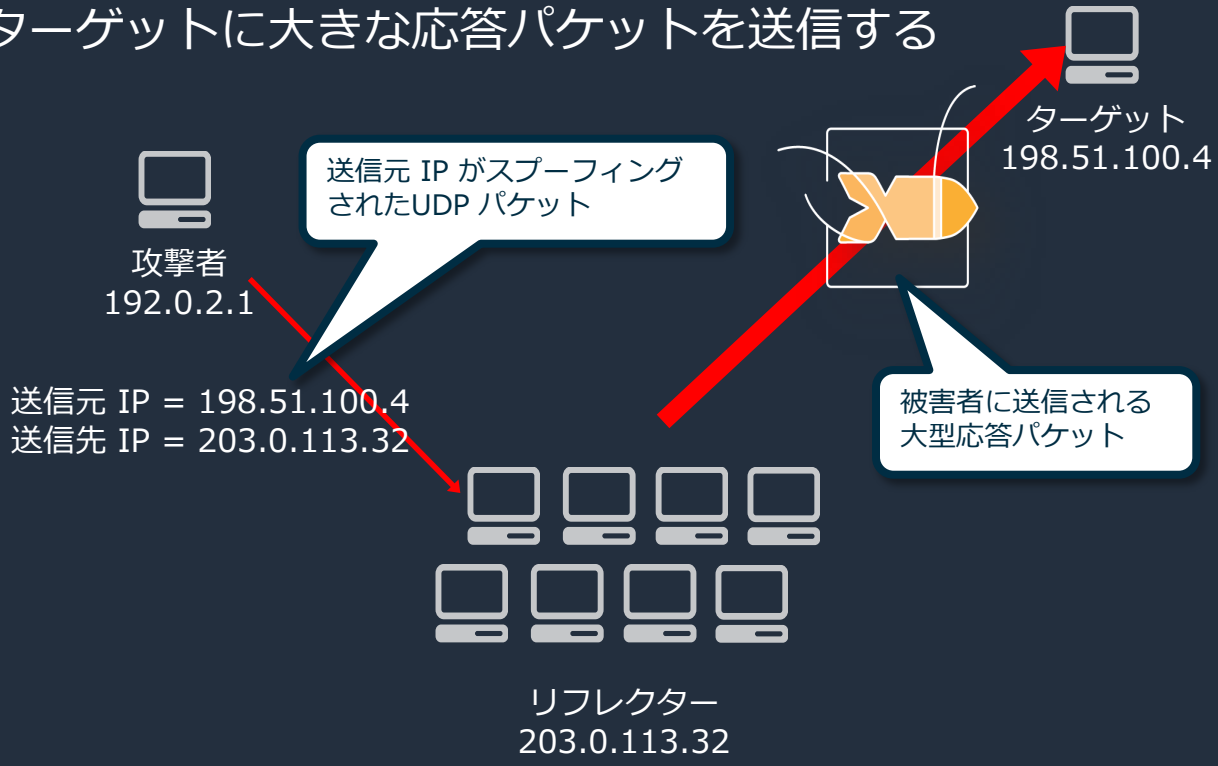
Bad Bots

	DDoS	Application Attacks	Bad Bots
Application Layer	HTTP floods Slowloris	SQL injection Application exploits	Crawlers Content scrapers Scanners & probes
Network/ Transport Layer	UDP floods SSL abuse SYN floods UDP reflection		

aws

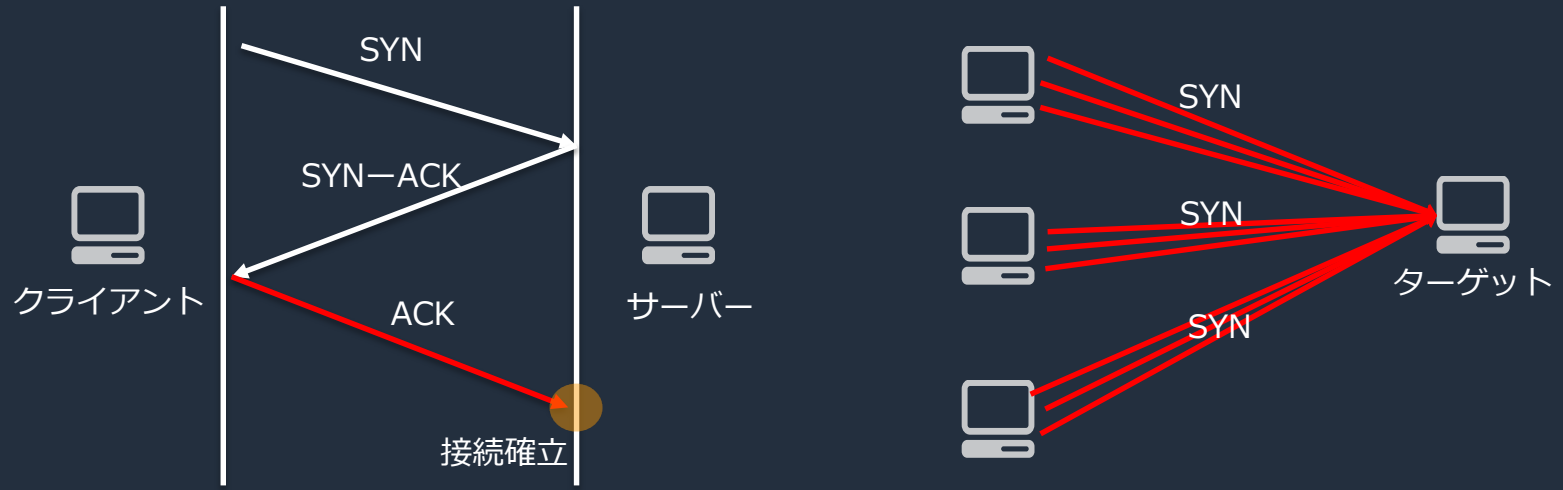
参考: UDP リフレクション攻撃

攻撃者が送信元 IP を偽装し、リクエストとレスポンスのパケットサイズの差を利用してターゲットに大きな応答パケットを送信する



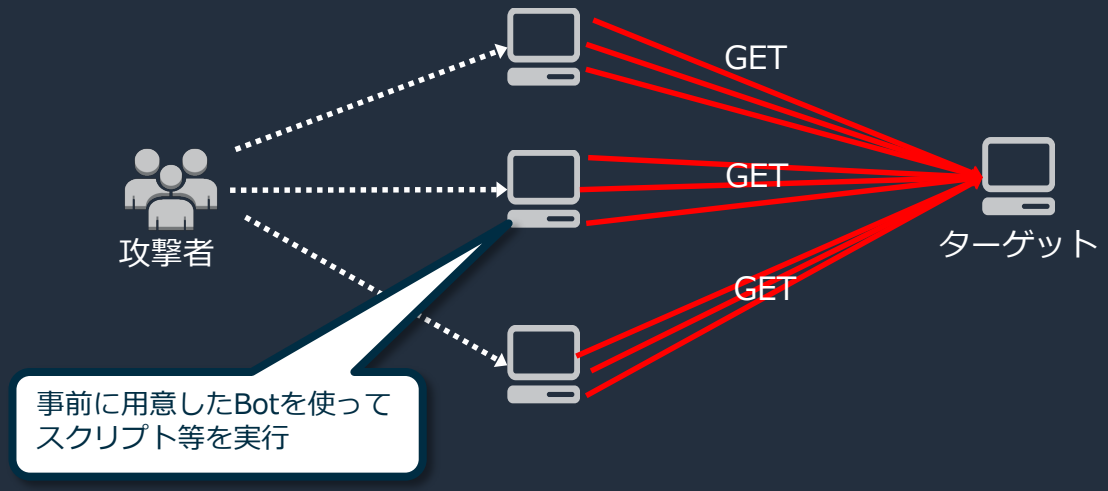
参考: SYN フラッド攻撃

攻撃者が大量の SYN パケットを送信するが、最後の ACK パケットを意図的に送信せず、サーバーは応答を待ち続けることにより、正規の接続のためのリソースを枯渇させる

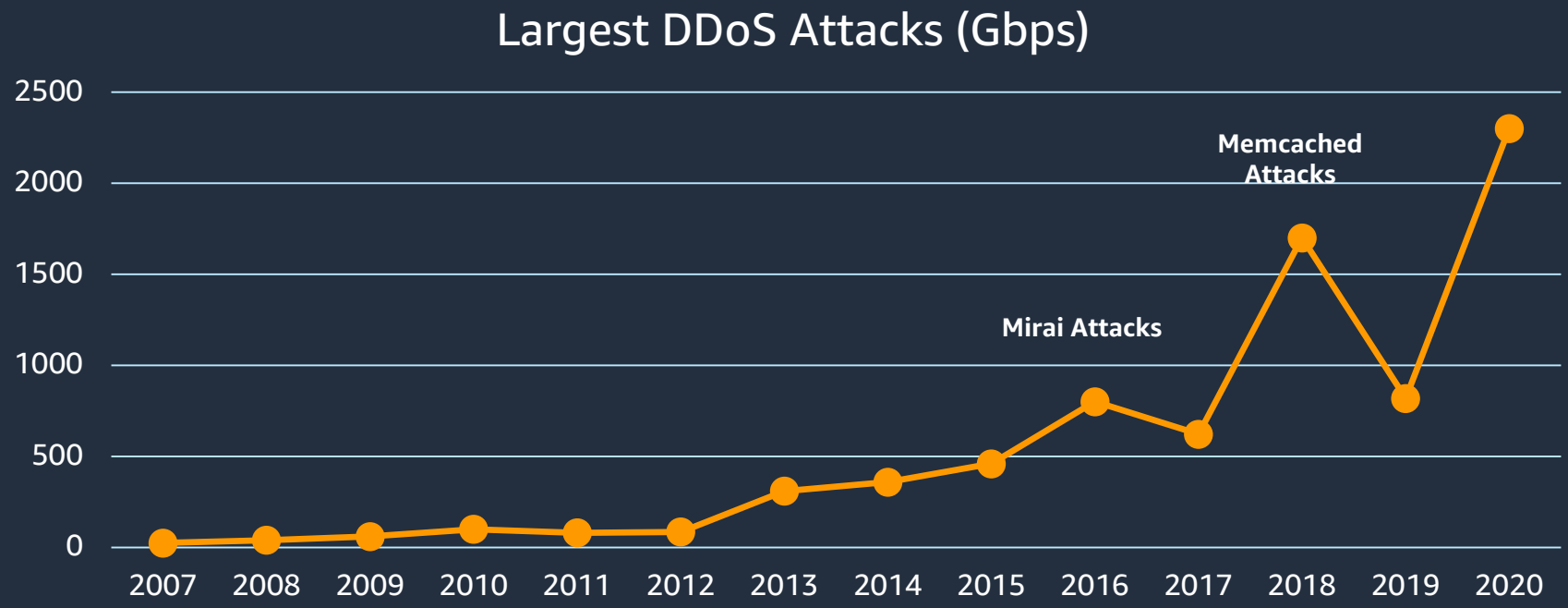


参考: HTTP フラッド攻撃

攻撃者はウェブアプリケーションの正規ユーザーから送られてきたように見える大量の HTTP リクエストをアプリケーションの特定の機能に対し送信。巧妙な HTTP フラッド攻撃の中には、人間のインタラクションを模倣するものもある



ボリューム型 DDoS 攻撃の推移



最近の DDoS 攻撃の状況（2020年Q1）

310,954 件

2020年 Q1 に観測された攻撃の数, 2019年 Q1と比較して 23% の増加

2.3 Tbps

2020年 Q1 に観測された最大規模の攻撃(ビット), 2019年 Q1と比較して 188% の増加

293.1 Mpps

2020年 Q1 に観測された最大規模の攻撃(パケット数), 2019年 Q1と比較して 13% の増加

694,201rps

2020年 Q1 に観測された最大規模の攻撃(リクエスト数) , 2019年 Q1と比較して 31% の減少

AWS Shield Threat Landscape report から抜粋　※2020年Q1（2020年 1-3月）

https://aws.amazon.com/jp/blogs/security/aws-shield-threat-landscape-report-now-available/

https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf

DDoS 対策の種類 - On-Premises / Cloud-Routed

オンプレミスによる DDoS 対策

- オンサイトで持つので可視性の担保と制御を自ら行うことが可能
- 初期費が高額になりやすく、維持コスト、運用担当者の確保などに課題を持つ
- 必要なキャパシティの想定が難しい

Cloud-Routed による DDoS 対策

- マネージドサービスを持つ他のネットワーク/装置にルーティングをすることによって緩和
- オンプレミスと比較して、より大規模なDDoS攻撃に対応し、初期投資やインハウスのリソースを持つ必要が無い
- レイテンシの増加や障害ポイントの増加につながることもある

DDoS 対策の種類 - 分散環境での DDoS 対策

Edge Location を利用することで大規模な攻撃に対してもより攻撃に近い箇所で緩和することで対応を行うため、オリジンへのインパクトが小さい

オンプレミスでは対応できない大規模な DDoS に対応しつつ、Cloud-Routed では対応できない低レイテンシを両立して実現

分散されたEdge Location と 各 AWS Regionの両方でDDoS対策が可能

217

Amazon CloudFront Points of Presence

12 Regional Edge Caches

84 cities,

42 countries

As of 8/1/2020

aws

本日のアジェンダ

1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS 耐性の高いアーキテクチャ
7. Firewall Manager の活用
8. 料金体系
9. まとめ

AWS Shield

- AWS Shield Standard
  - 一般的な DDoS 攻撃に対応したDDoS 攻撃緩和サービス
  - すべての インターネットに面したAWS のサービスに対して透過的に適用され、ネットワークレイヤーとトランスポートレイヤーに対する DDoS を自動的に緩和

- AWS Shield Advanced
  - 大規模かつ高度な攻撃に備えて、攻撃に対する可視性を高め、複雑な事例に関して DDoS レスポンスチームへの年中無休のアクセスが提供される DDoS 緩和サービス

プランの比較　https://aws.amazon.com/jp/shield/getting-started/

AWS Shield Standard and Shield Advanced

AWS Shield

ビルトインの DDoS 保護機能

オンボーディングウィザード

自動検出と一般的な DDoS 攻撃の緩和

攻撃時の迅速なカスタム緩和

DDoS レスポンスチームへの24時間のアクセス

CloudWatch メトリクスの提供

攻撃後の分析

グローバル脅威ダッシュボード

正常性ベース検出

AWS WAF が無料で利用可能
For protected resources

AWS Firewall Manager が無料で利用可能

コスト保護 (DDoS によるコストの吸収)

AWS Shield Advanced 機能拡張の歴史

- 2016年 AWS Shield Advanced リリース

2016

2017

- 2017年11月グローバル脅威環境ダッシュボードを提供、AWS 全体における DDoS 攻撃の傾向を把握
- 2017年11月 EC2 およびネットワークロードバランサーの高度な DDoS 保護を追加　（ EC2 インスタンスまたは NLB にアタッチされた AWS Elastic IP アドレス）

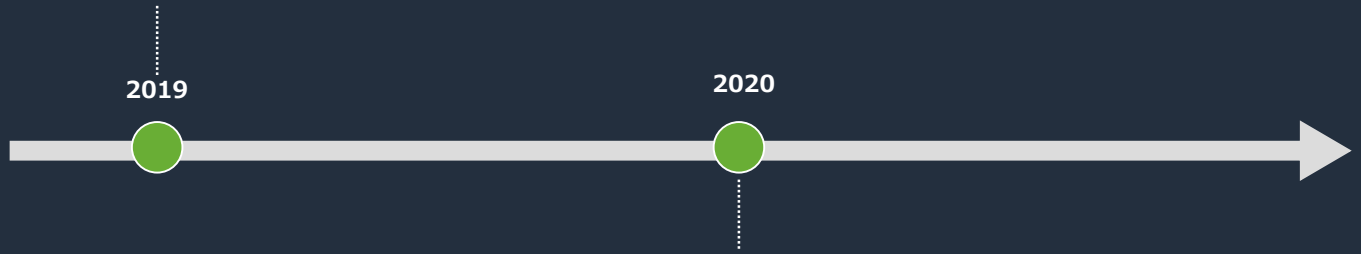
2018

- 2018年3月 すべてのリソースの保護が一度で可能となる
- 2018年3月 米国東部 (オハイオ) リージョンで利用可能となる
- 2018年6月 新しいオンボーディングウィザードを搭載
- 2018年8月 AWS Config を使用して、構成変更の記録が可能となる
- 2018年8月 AWS Shield Advanced からレートベースのルールと Amazon CloudWatch アラームを容易に作成可能となる
- 2018年12月 AWS Global Accelerator の高度な DDoS 保護を追加

※AWS Shield: What's newから抜粋
https://aws.amazon.com/shield/

AWS Shield Advanced 機能拡張の歴史

- 2019年2月 高度な保護のためのデフォルトのリソース制限を引き上げ
- 2019年3月欧州 (ロンドン)、欧州 (ストックホルム)、アジアパシフィック (シンガポール)、アジアパシフィック (ソウル)で利用可能になる
- 2019年3月 AWS Firewall Manager Support For AWS Shield Advanced の発表
- 2019年7月 欧州 (パリ)、カナダ (中央)、アジアパシフィック (ムンバイ)、南米 (サンパウロ) で利用可能になる



- 2020年2月 AWS Shield Advanced が正常性ベース検出のサポート
- 2020年4月 アジアパシフィック (香港) と中東 (バーレーン) で利用可能に
- 2020年6月 DDoSイベントへのプロアクティブな対応のサポートを開始

※AWS Shield: What's newから抜粋
https://aws.amazon.com/shield/

AWS Shield Advanced 対象のサービス

DNS

Amazon Route 53 上のゾーンを保護

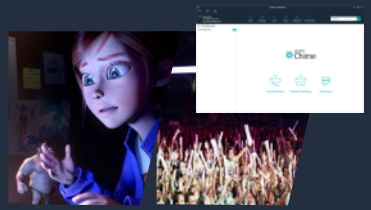
Amazon Route 53

Web アプリケーション

HTTP/HTTPSプロトコルを利用するWebサイトとAPI

Amazon CloudFront

Application Load Balancer



TCP/UDP アプリケーション

マルチプレイヤーのゲームアプリ、DNS、VOIPなどのUDPアプリケーション

AWS Global Accelerator

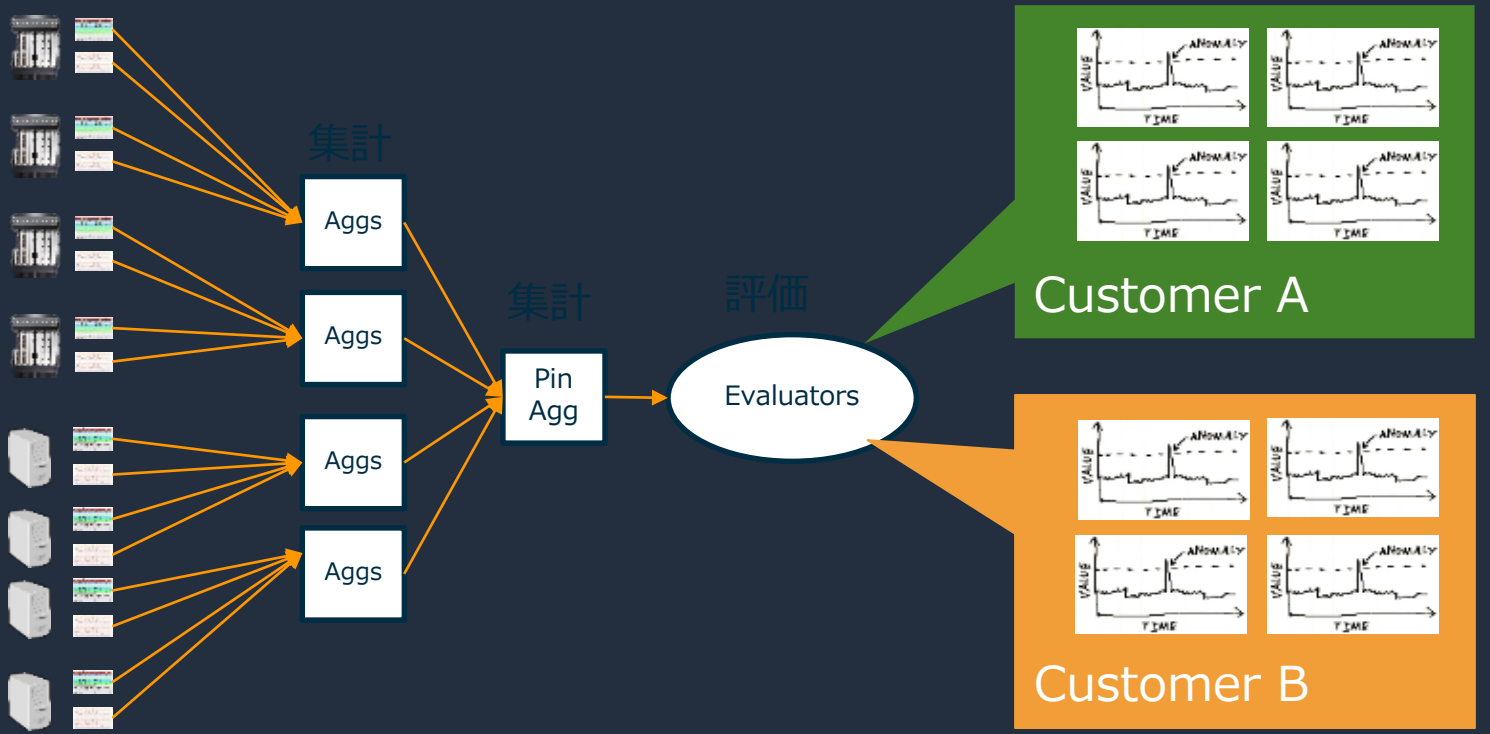
Elastic IP address

DDoS 攻撃の緩和

- Layer 3/4 の DDoS 攻撃緩和は自動で行われる
- Layer 7 については原則として WAF で行う（レートベースルールやIPブラックリスト等）
- 様々な DDoS 緩和手法を実装
- 統計情報を取得しベースラインを策定、異常値（Anomaly）の検知
- 設定の見直しやシグネチャの更新などを DDoS レスポンスチームが行い最新の状態に保つ
- 自動防御で対応できない場合は、 DDoS レスポンスチームが介在し対処を行う

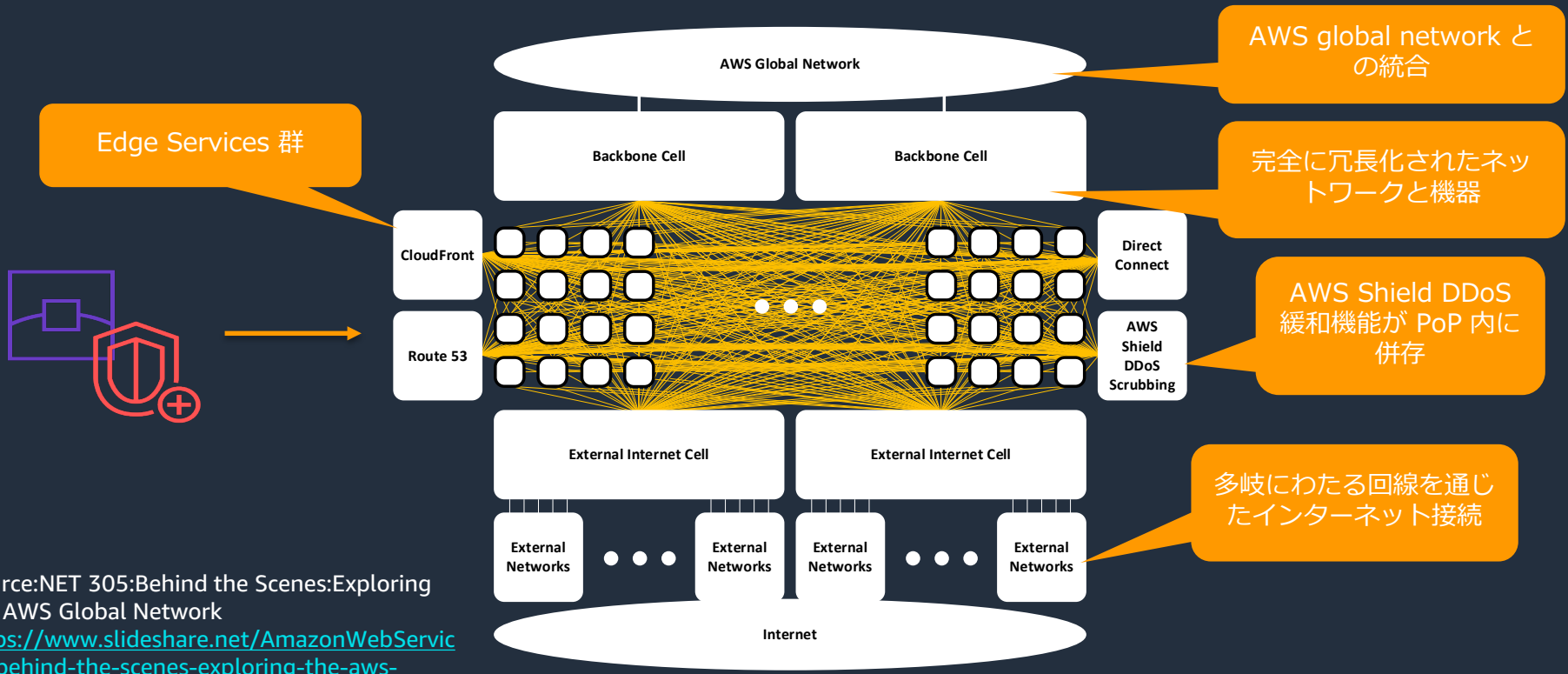
aws

参考: Anomaly Detection



統計情報を取得し、ベースラインの策定を行い、異常値（Anomaly）の検知を行う

参考: In-line DDoS Mitigation Inside an Edge POP

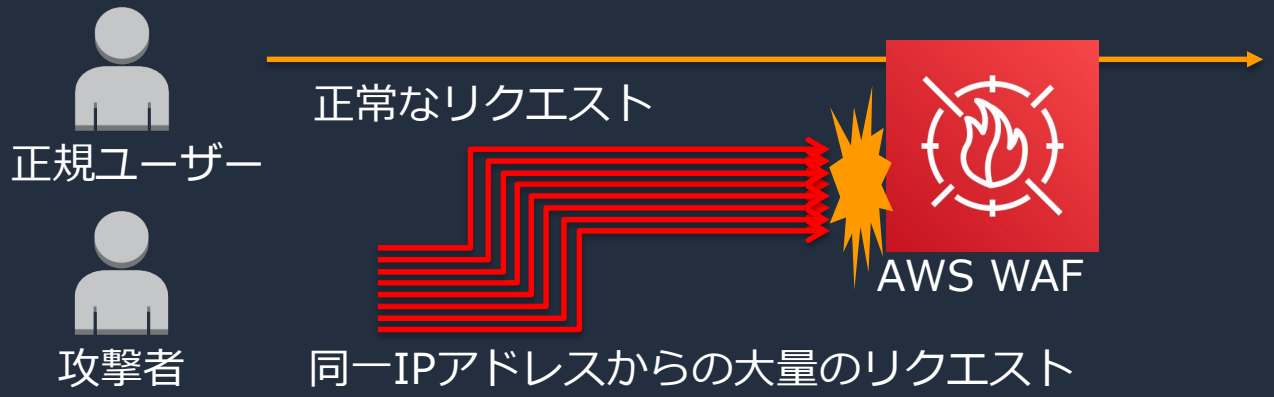


Source:NET 305:Behind the Scenes:Exploring the AWS Global Network
https://www.slideshare.net/AmazonWebServices/behind-the-scenes-exploring-the-aws-global-network-net305-aws-reinvent-2018

Layer 7 のDDoS対策

AWS WAF のレートベースのルールを利用　(Shield Advanced からも設定可能)

- 5 分間あたりの同一 IP アドレスからのリクエスト数が設定された閾値を超過したら、Block/Count する。（閾値の設定範囲は、100 ～ 20,000,000 ）
- 全てのリクエストを対象にするか、特定の条件に一致したリクエストだけを対象にするかを選択可能（特定の条件を指定する場合、AWS WAF側でルールを作成し、Shield Advancedでルールとリソースを関連づける）



本日のアジェンダ

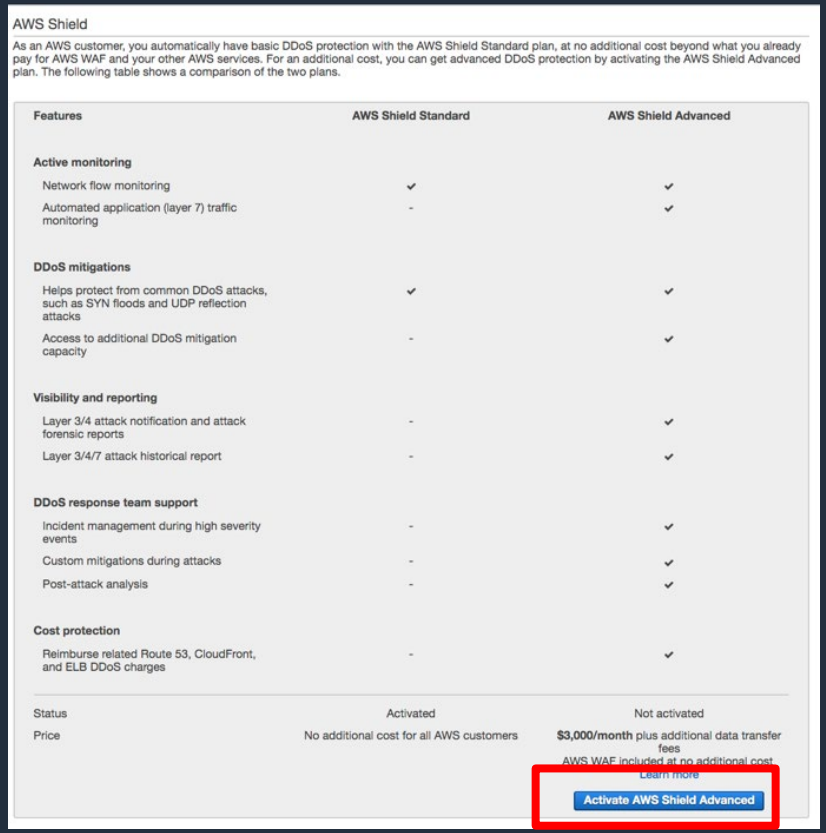
1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS 耐性の高いアーキテクチャ
7. Firewall Manager の活用
8. 料金体系
9. まとめ

AWS Shield Advanced の利用開始

マネージメントコンソールから WAF & Shield を選び、Shield Advanced のActivate AWS Shield Advanced をクリックする

Activate AWS Shield Advanced

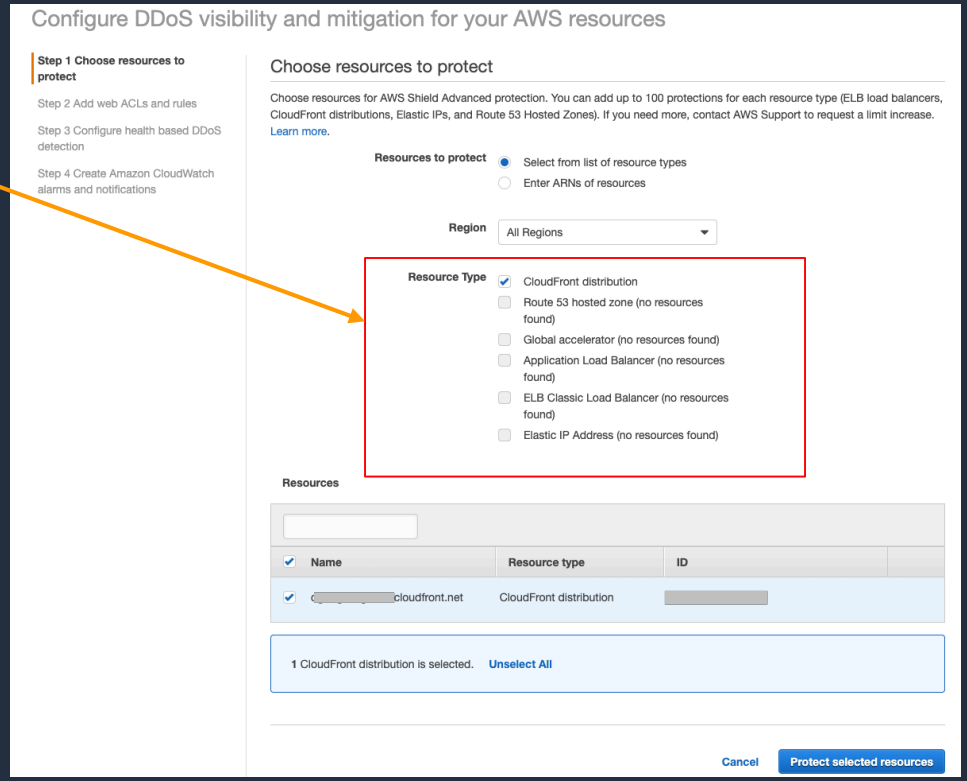
https://aws.amazon.com/shield/



Step-1 防御対象リソースの選択

Shield Advancedの防御対象としたいリソースを選ぶ

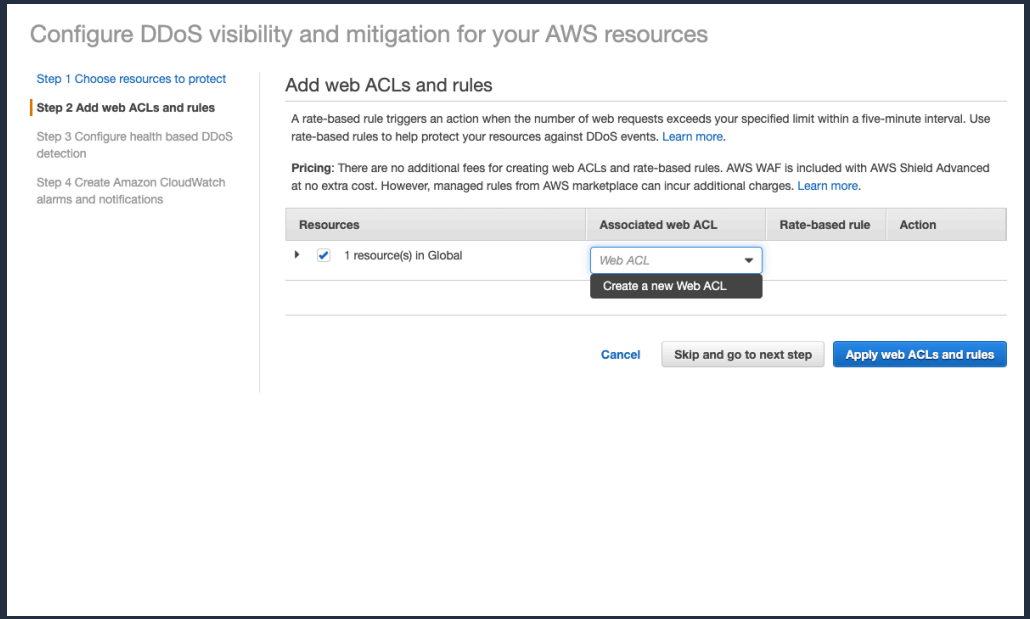
- デフォルトではすべてのリソースが選ばれるので、必要なリソースのみを選択する



Step-2 web ACL とルールの追加

WAF（Web ACL）との関連付け、新規作成などを行い L7 防御の設定を行う

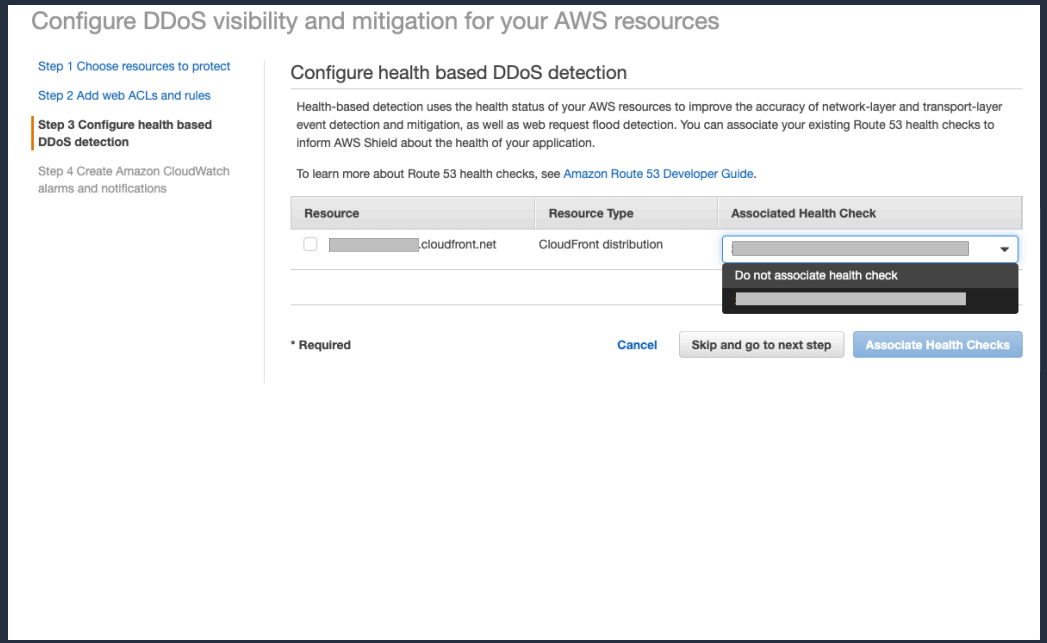
- 関連付けを行わない場合はLayer3/4の防御のみになる
- Shield Advanced の防御対象リソースは AWS WAFの費用は発生しない



Step-3 正常性ベース検出との関連づけ

正常性ベースの検出を使用するには、Route 53 でヘルスチェックを定義し、ここでリソースに関連づけると関連付ける

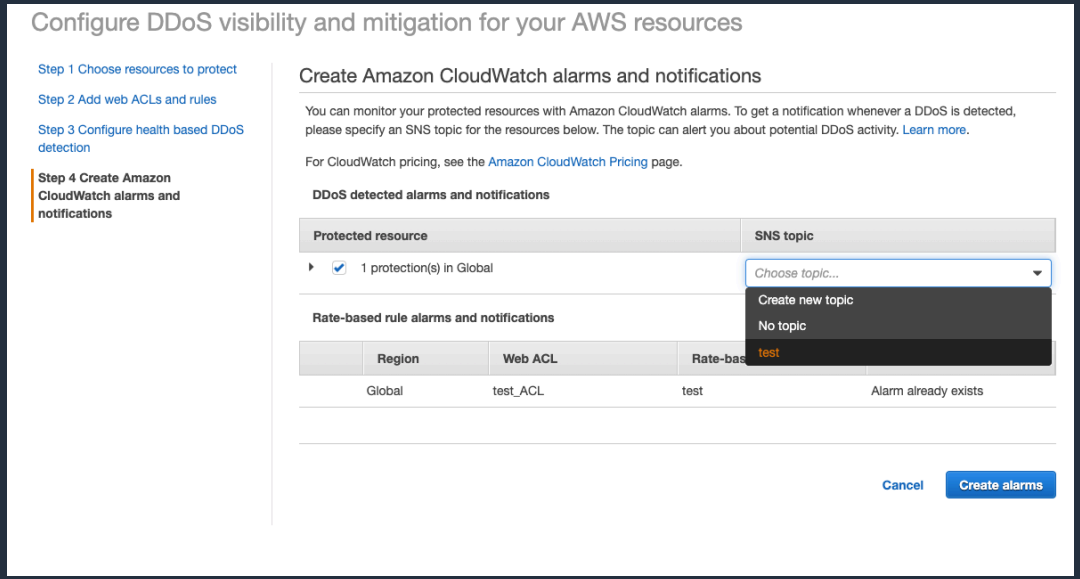
- 事前に Route 53 のヘルスチェックの設定が必要
- 後から変更することも可能



Step-4 Amazon CloudWatch アラームと通知設定

防御対象のリソースで
DDoSを検知した場合に送
るSNSトピックを設定する

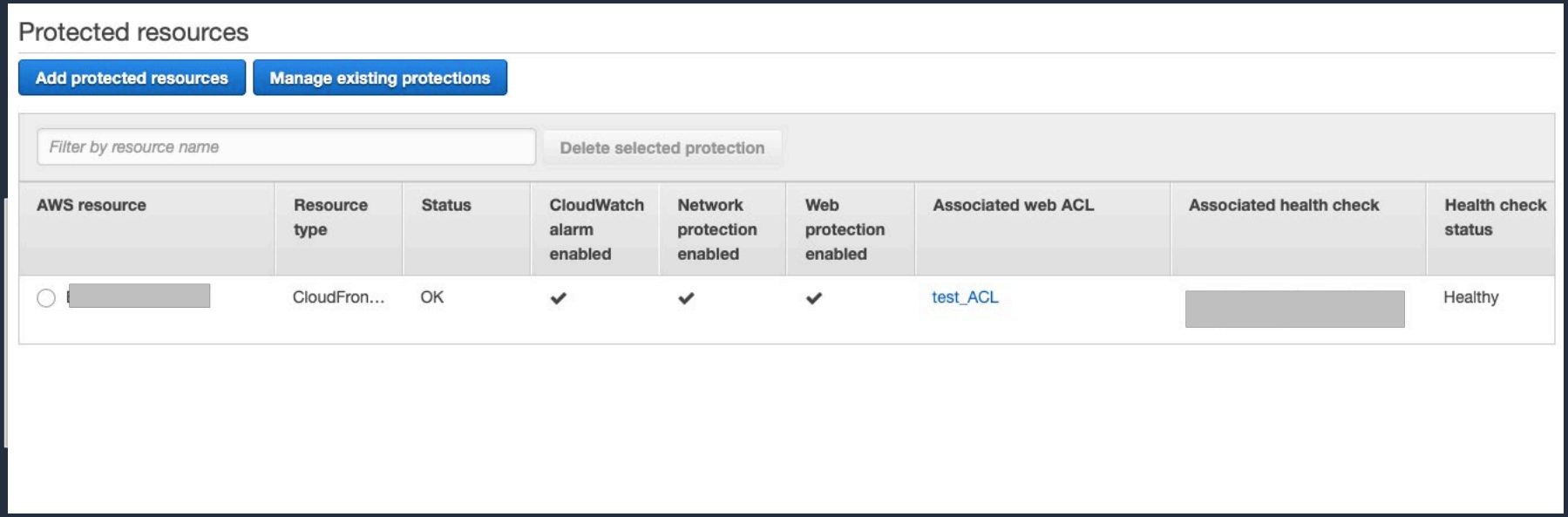
- DDoSDetected＞＝1の場合
  に検知するように設定される
- ここで関連付けを行わなず、
  自分で設定を行うことは可能



Protected Resources

防御対象（Protected Resources）としての設定が完了

- 設定内容は変更/削除可能

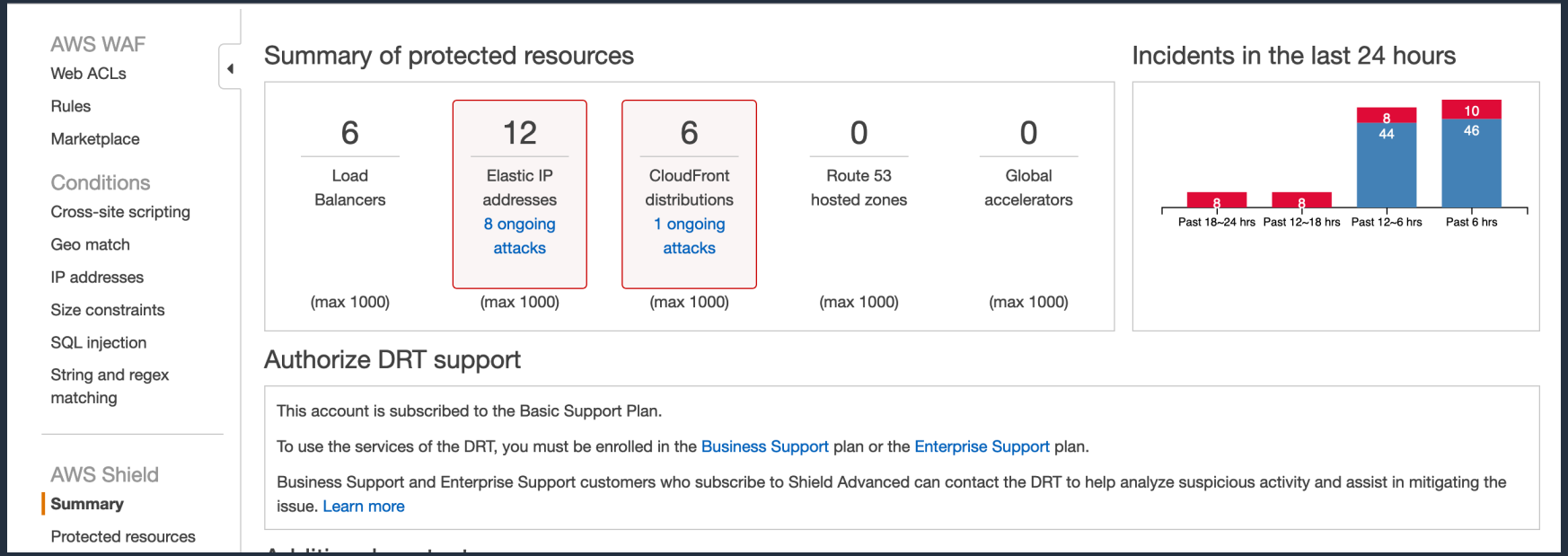


本日のアジェンダ

1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS 耐性の高いアーキテクチャ
7. Firewall Manager の活用
8. 料金体系
9. まとめ

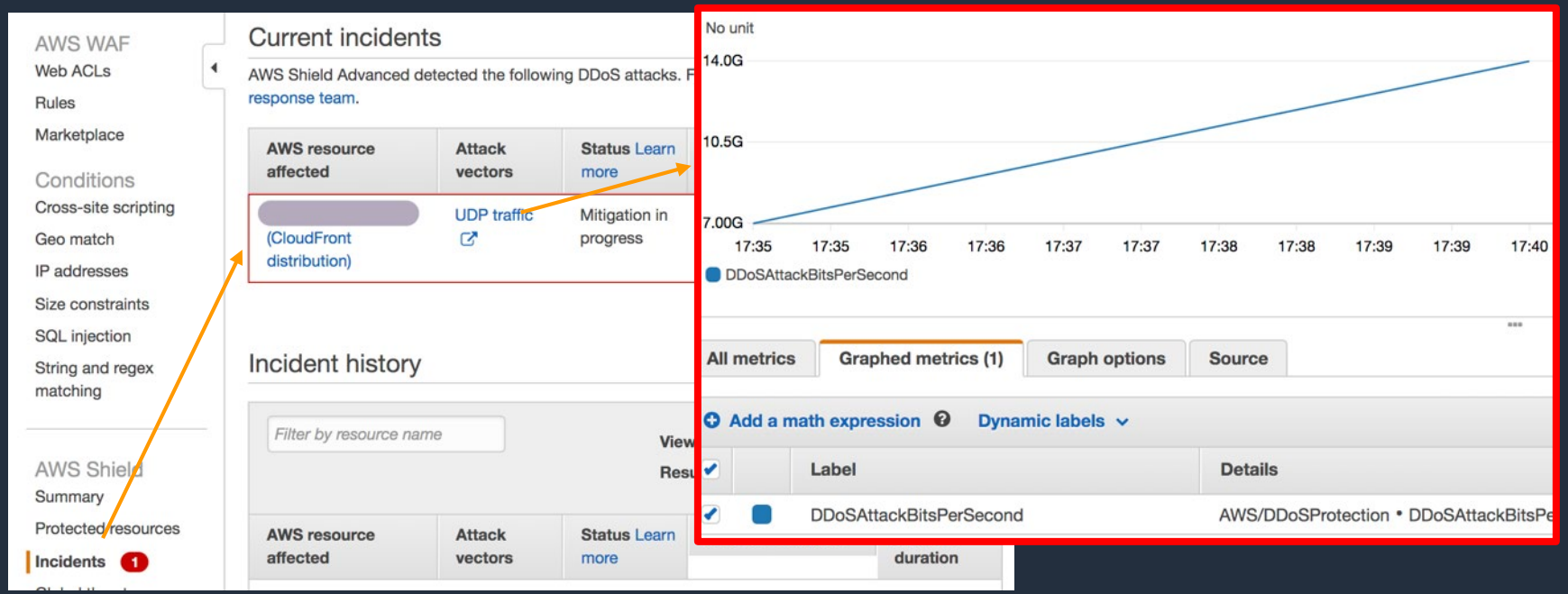
Summary

DDoS 緩和対象のリソースのサマリー



Incidents

現在進行中の攻撃内容と緩和状況を確認することが可能



参考: Amazon CloudWatch のメトリクス

メトリクス	内容
DDoSDetected	特定の Amazon リソースネーム (ARN) に対して DDoS イベントが進行中かどうかを示します。 このメトリクスの値は、攻撃中は 1、それ以外の場合は 0 です
DDoSAttackBitsPerSecond	特定の Amazon リソースネーム (ARN) の DDoS イベント中に認められたビット数。このメトリクスは、レイヤー 3 およびレイヤー 4 の DDoS イベントのみで使用できます。 このメトリクスは、攻撃中はゼロ以外の値を持ち、それ以外の場合は 0 です。
DDoSAttackPacketsPerSecond	特定の Amazon リソースネーム (ARN) の DDoS イベント中に認められたパケット数。このメトリクスは、レイヤー 3 およびレイヤー 4 の DDoS イベントのみで使用できます。 このメトリクスは、攻撃中はゼロ以外の値を持ち、それ以外の場合は 0 です。
DDoSAttackRequestsPerSecond	特定の Amazon リソースネーム (ARN) の DDoS イベント中に認められたリクエスト数。このメトリクスは、レイヤー 7 の DDoS イベントのみで使用できます。メトリクスは、特に重要なレイヤー 7 イベントのみについて報告されます。 このメトリクスは、攻撃中はゼロ以外の値を持ち、それ以外の場合は 0 です。

AWS Shield アドバンスド のメトリクス
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/monitoring-cloudwatch.html

Incident Summary

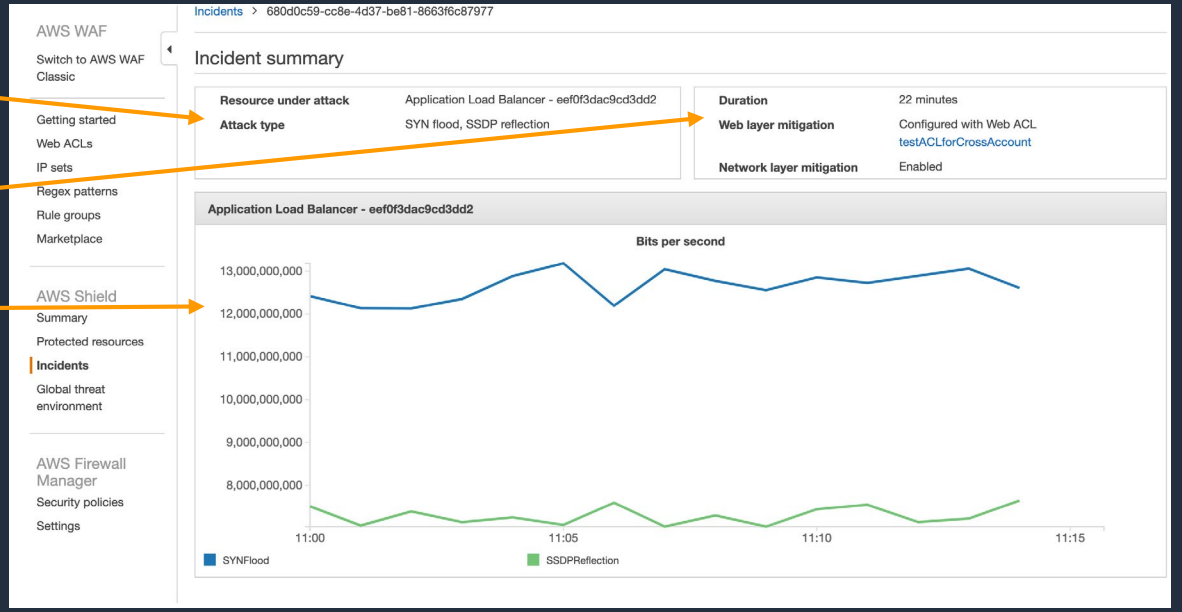
攻撃の種類

攻撃の発生期間

時系列グラフ

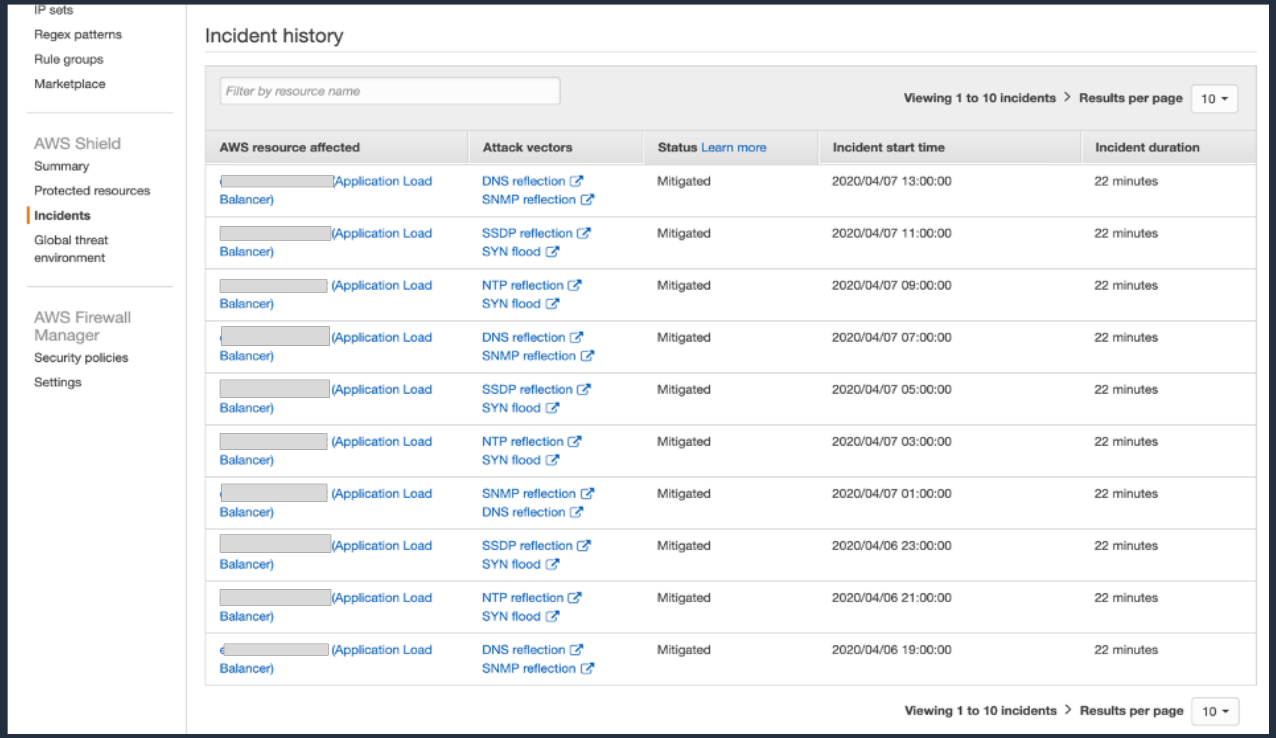
Bbs/pps/reqなど

攻撃元や攻撃対象の詳細情報

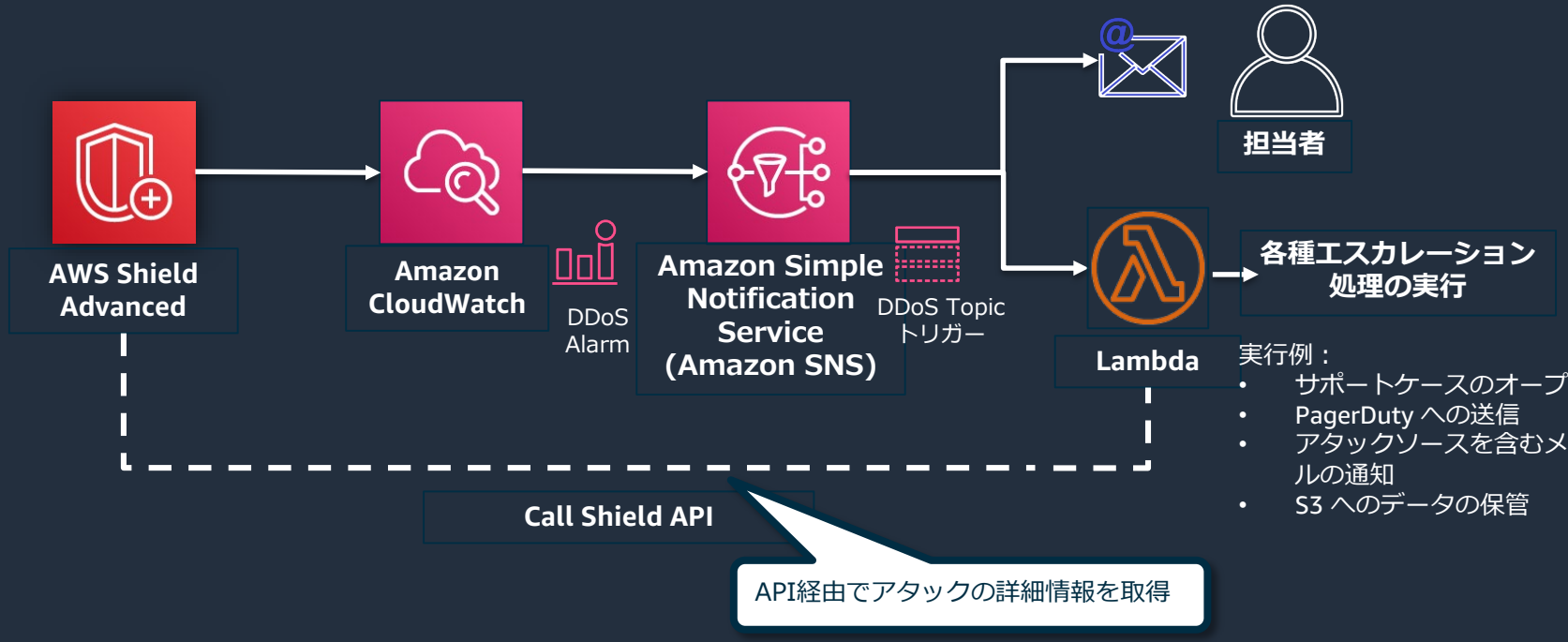


Incident History

- 過去13ヶ月分の攻撃の履歴が確認可能



DDoS の検知 / 通知



AWS Shield Engagement Lambda （サポートケースのオープン）
https://s3.amazonaws.com/aws-shield-lambda/ShieldEngagementLambda.pdf

参考: API で取得可能な情報

Data Types	内容
AttackDetail	DDoS 攻撃の全体の詳細
AttackProperty	攻撃の詳細 (攻撃レイヤー、攻撃対象のURL、リファラ、IPアドレス、など)
AttackSummary	指定した期間におけるすべての DDoS 攻撃の要約
AttackVectorDescription	攻撃の種類
Contributor	攻撃元の情報
EmergencyContact	プロアクティブエンゲージメントが有効になっている場合、DDoS レスポンスチームへのエスカレーション、およびプロアクティブなカスタマーサポートを開始するために、DDoS レスポンスチームがお客様に連絡するために使用する連絡先情報
Limit	作成できる保護対象のタイプ毎の最大数
Mitigation	DDoS 攻撃に適用される緩和策
Protection	DDoS 保護下にあるリソースを表すオブジェクト
SubResourceSummary	指定されたサブリソースの攻撃情報
Subscription	サブスクリプションに関する情報
SummarizedAttackVector	攻撃に関する情報の要約
SummarizedCounter	指定された期間のDDoS 攻撃のカウンタ
TimeRange	時間範囲　（開始時間、終了時間）

AWS Shield Advanced API リファレンス
https://docs.aws.amazon.com/waf/latest/DDOSAPIReference/API_Types.html

参考: API でサポートされるアクション一覧

AssociateDRTLogBucket
AssociateDRTRole
AssociateHealthCheck
AssociateProactiveEngagementDetails
CreateProtection
CreateSubscription
DeleteProtection
DeleteSubscription
DescribeAttack
DescribeDRTAccess
DescribeEmergencyContactSettings
DescribeProtection
DescribeSubscription
DisableProactiveEngagement
DisassociateDRTLogBucket
DisassociateDRTRole
DisassociateHealthCheck
EnableProactiveEngagement
GetSubscriptionState
ListAttacks
ListProtections
UpdateEmergencyContactSettings
UpdateSubscription

AWS Shield Advanced API リファレンス
https://docs.aws.amazon.com/waf/latest/DDOSAPIReference/API_Operations.html

AWS Shield CLI 実行例

```
$ aws shield list-attacks

{
   "NextToken": ”xxx=",
   "AttackSummaries": [
      {
         "EndTime": 1534529765.0,
         "ResourceArn": "arn:aws:ec2:us-west-2:111111111111:eip-
allocation/eipalloc-9a7556a6",
         "AttackId": "c04ab40d-a8e4-47c8-a132-ccccff3a22dd",
         "AttackVectors": [
            {
               "VectorType": "UDP_TRAFFIC"
            }
         ],
         "StartTime": 1534529460.0
      },

...
}
```

Attackidを取得

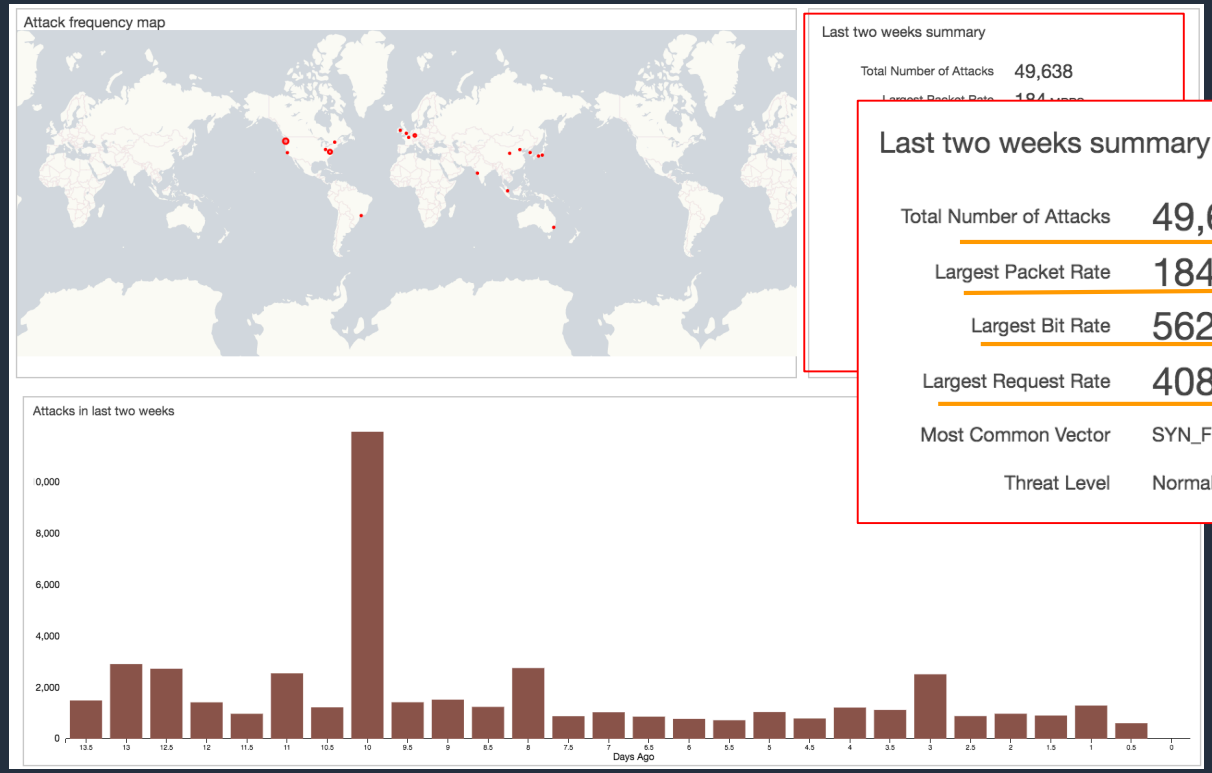
```
$ aws shield describe-attack --attack-id c04ab40d-a8e4-47c8-a132-ccccff3a22dd

{
   "Attack": {
      "Mitigations": [“us-west-2_20180817181136833_3925”],
      "ResourceArn": "arn:aws:ec2:us-west-2:111111111111:eip-allocation/eipalloc-
9a7556a6",
      "AttackId": "c04ab40d-a8e4-47c8-a132-ccccff3a22dd",
      "SubResources": [
         {
            "Type": "IP",
            "Id": "1.2.3.4",
            "AttackVectors": [
               {
                  "VectorCounters": [
                     {
                        "Name": "NA",
                        "Max": 5000000000.0,
                        "Average": 5000000000.0,
                        "N": 5,
                        "Sum": 25000000000.0,
                        "Unit": "BPS"
                     }
                  ],
                  "VectorType": "UDP_TRAFFIC"
               }]}],
      "StartTime": 1534529460.0,
      "EndTime": 1534529765.0
}}
```

Attackidを指定

攻撃の詳細を取得

Global threat environment



総アタック数

最大パケットレート

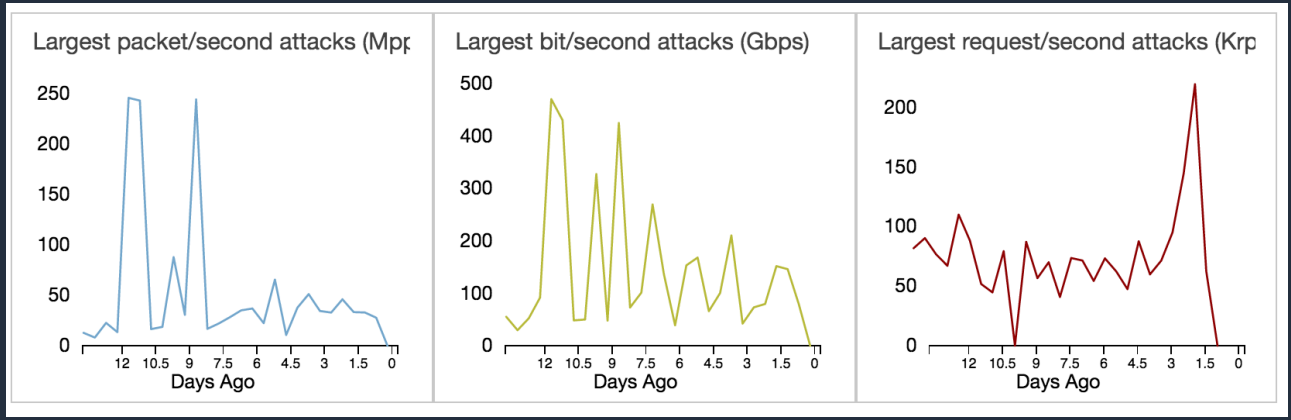
最大ビットレート

最大リクエストレート

aws

Global threat environment

3つのメトリクスそれぞれで時系列のグラフも表示される



Packet Rate

細かいパケットを送ることで CPU リソースを消費させる

必ずしもネットワークの帯域が枯渇するとは限らない

Bit Rate

帯域を消費することでネットワークを利用できなくさせる

一般的な DDoS のイメージ

Request Rate

HTTP リクエストを大量に送ることにより、アプリケーションのリソースを消費させる

ネットワーク帯域消費という観点では大きくなりにくい

本日のアジェンダ

1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS 耐性の高いアーキテクチャ
7. Firewall Manager の活用
8. 料金体系
9. まとめ

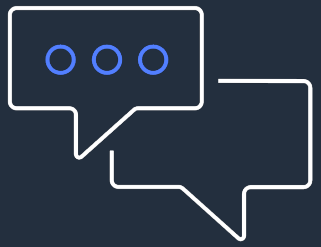
DDoS レスポンスチーム

AWS と Amazon.com を保護する知識と経験を持った DDoS 対策の専門家チーム

サポートケース経由でのアクセス

- 24x7で DDoSレスポンスチームへアクセス可能
- クリティカルで緊急の優先順位のケースは DDoS レスポンスチームに直ぐにルーティング
- お客様環境へのアクセスが承認されている場合、Layer 7 の DDoSの緩和を実施
- ビジネスサポートプランまたはエンタープライズサポートプランが必要必要

サポートケースのオープン



「AWS Shield」サービスでサポートケースを開く

アプリケーションの説明、影響の説明、ターゲットとなるリソースの特定

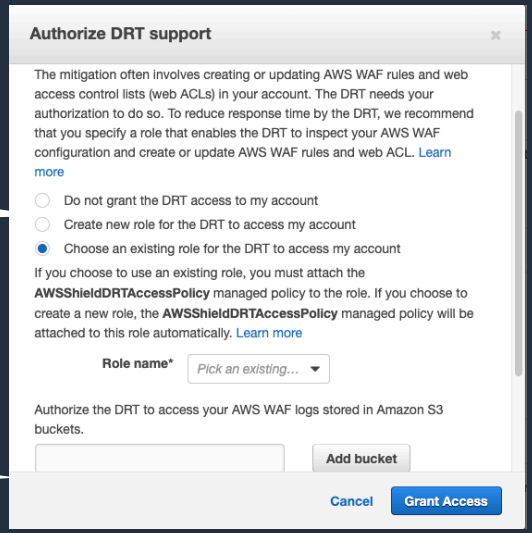
本番影響を受ける場合は、利用可能な最も高い優先度を選択し、ケースに明記

DDoS レスポンスチームからのアクセス許可

- DDoS レスポンスチームに対して Shield Advanced および AWS WAF API への制限付きアクセスと、AWS WAF ログを含む Amazon S3 バケットへのアクセスを許可する場合、ウェブアプリケーションレイヤーの攻撃イベントをDDoS レスポンスチームがサポートすることが可能
- DDoS レスポンスチームは、サポート契約の範囲に限定され、お客様の承認を得てお客様の API と AWS WAF ログにのみアクセスする

DRTがアカウントにアクセスするためのロールを選択

AWS WAF ログが保存されている Amazon S3 バケット



DDoS レスポンスチームへのエスカレーション例

お客様

AWS
サポート

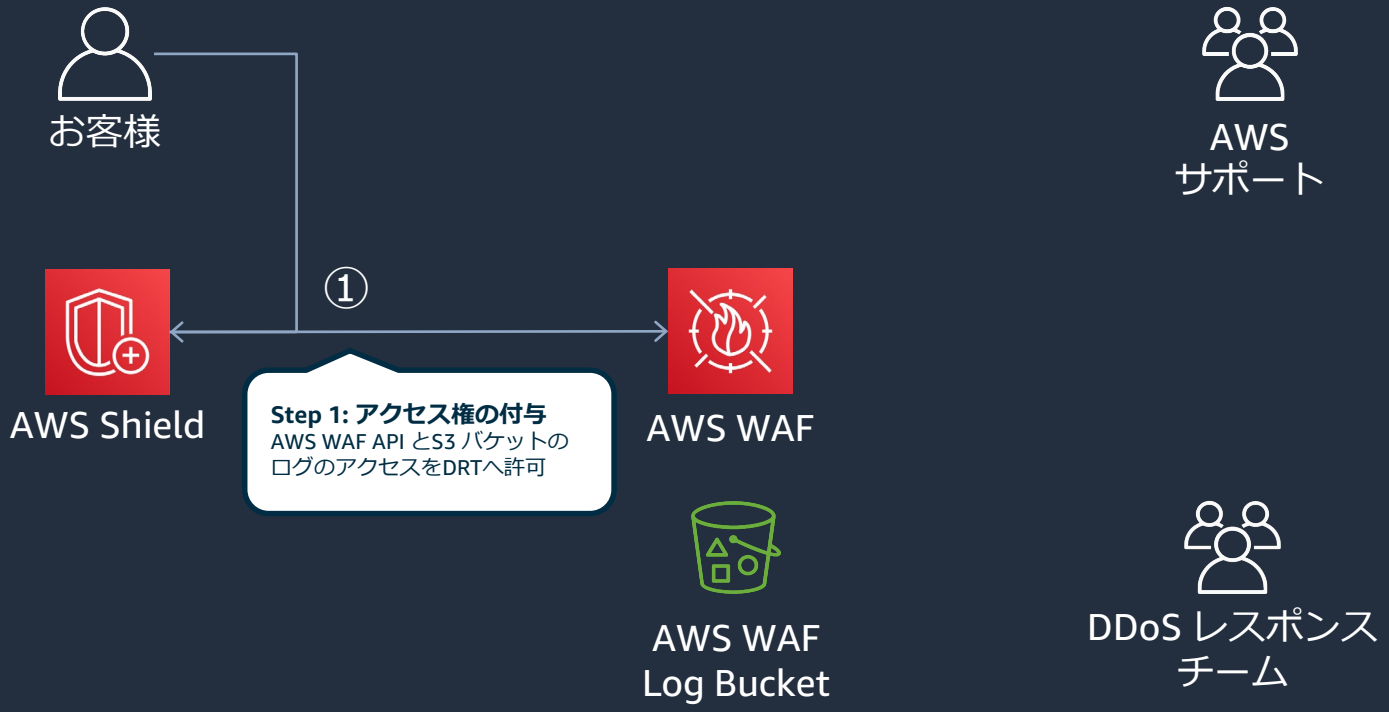
AWS Shield

AWS WAF

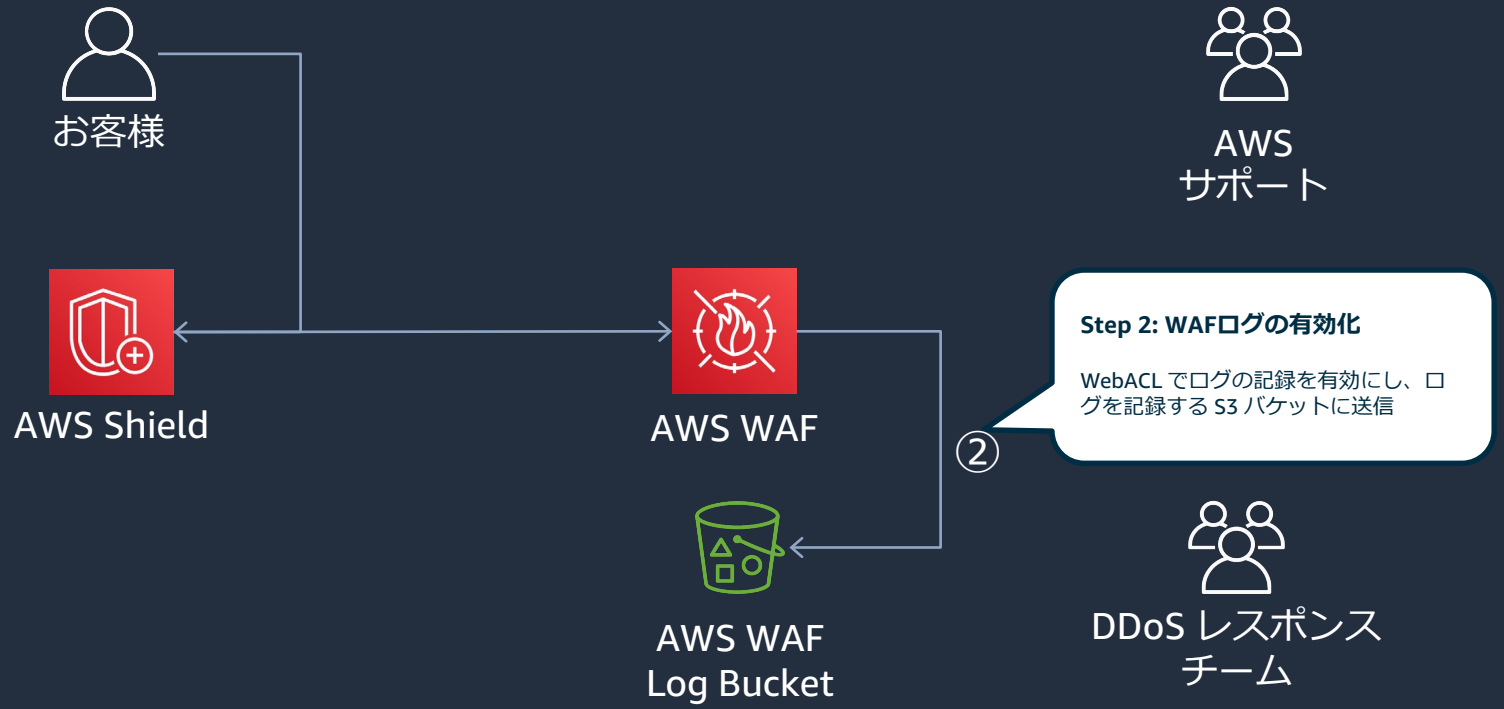
AWS WAF
Log Bucket

DDoS レスポンス
チーム

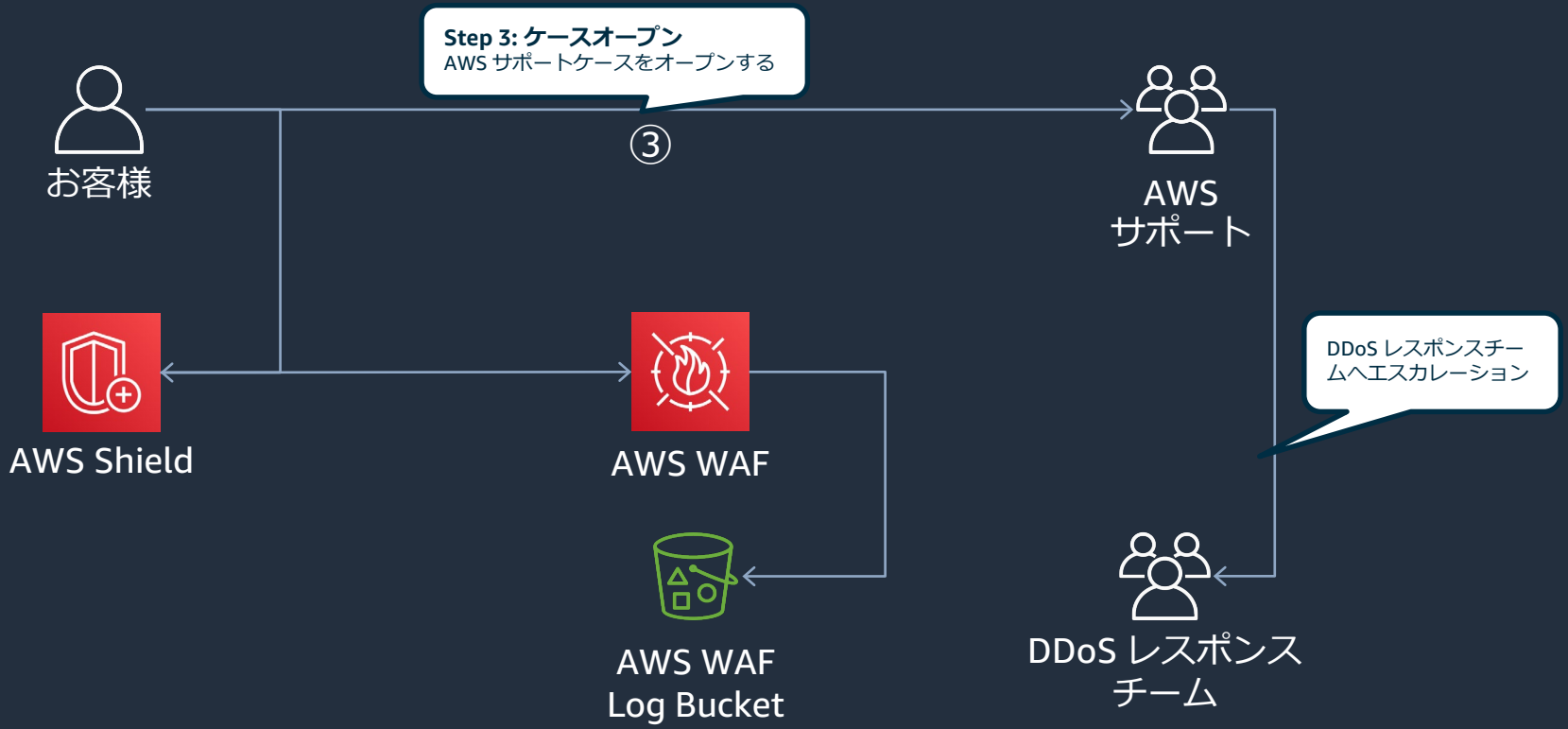
DDoS レスポンスチームへのエスカレーション例



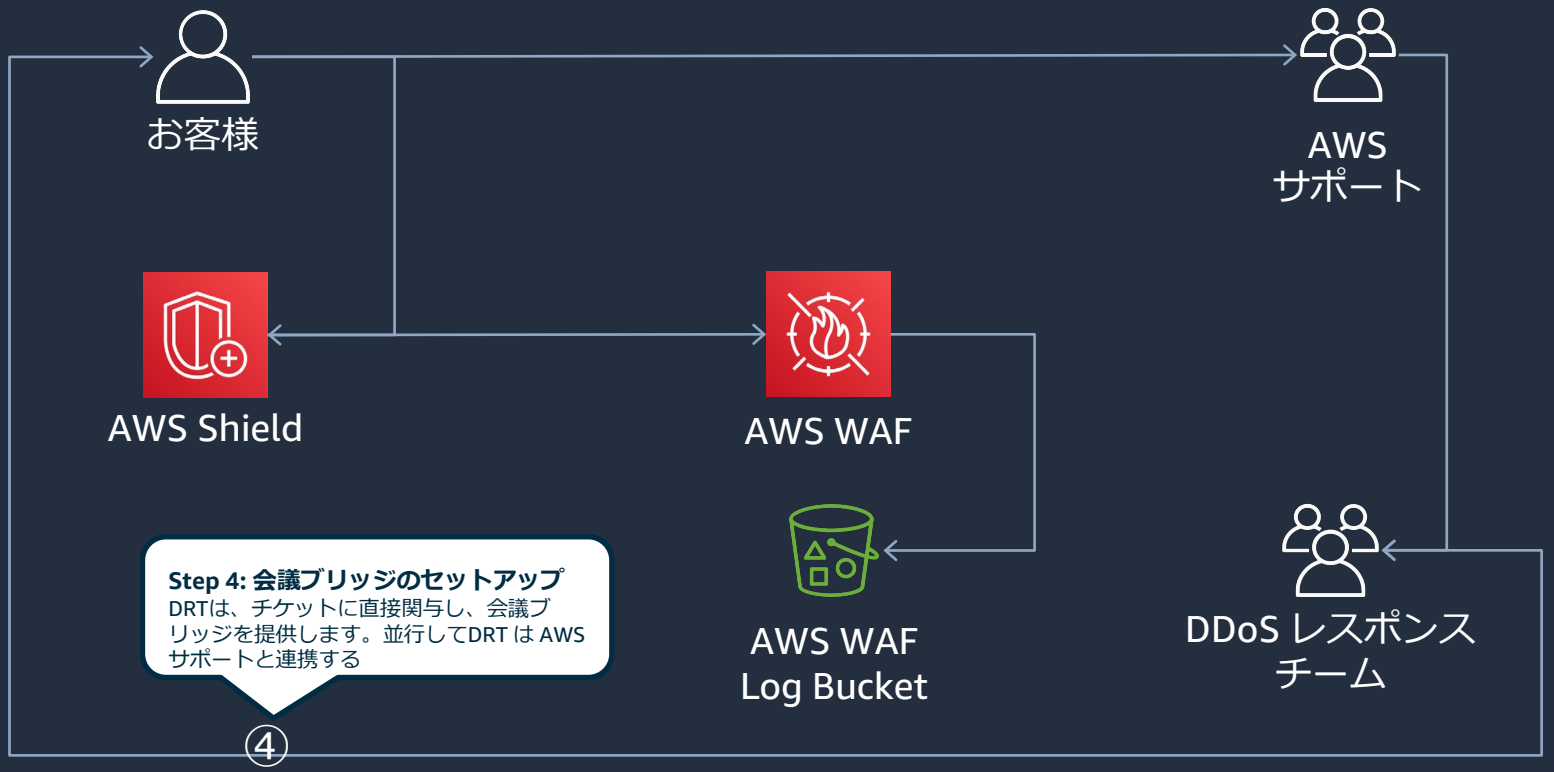
DDoS レスポンスチームへのエスカレーション例



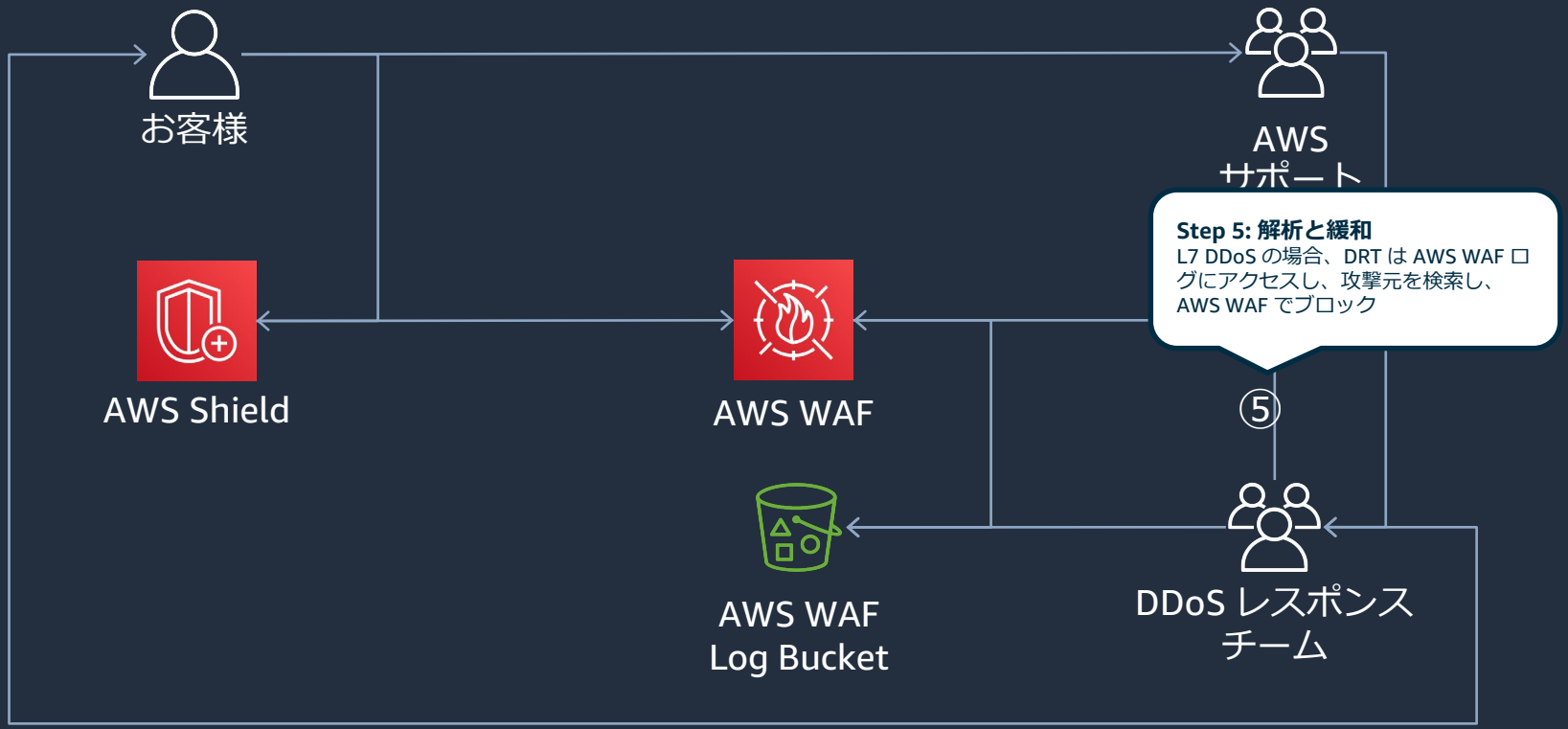
DDoS レスポンスチームへのエスカレーション例



DDoS レスポンスチームへのエスカレーション例

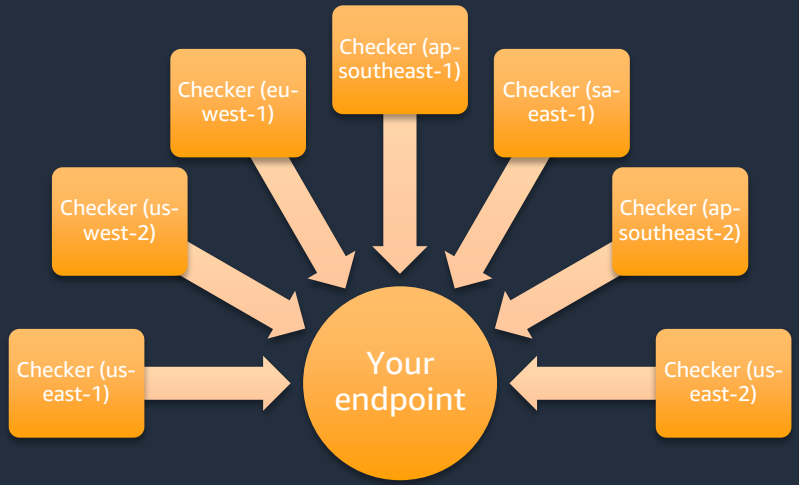


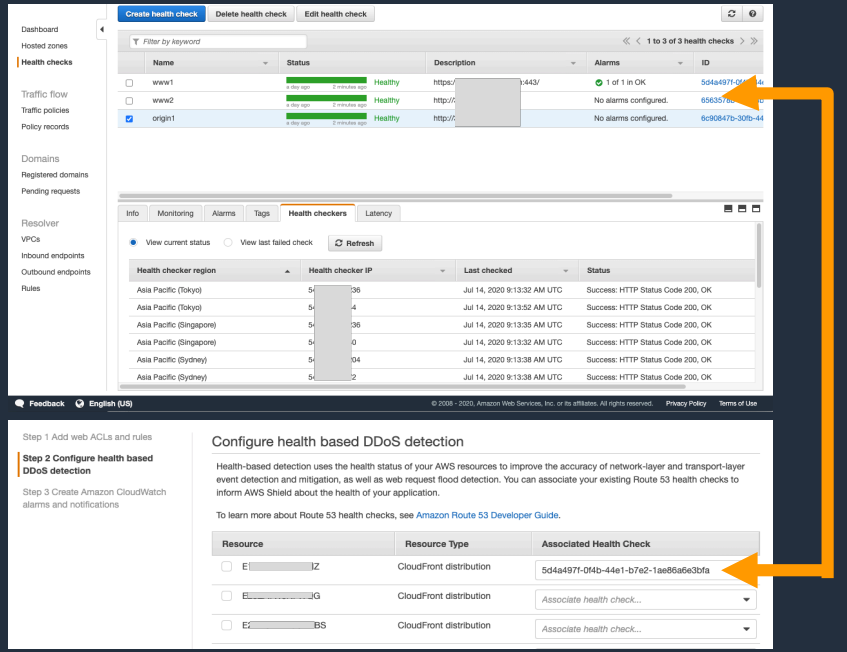
DDoS レスポンスチームへのエスカレーション例



正常性ベース検出との関連づけ

- 正常性ベースの検出を使用するには、Route 53 でヘルスチェックを定義し、それを Shield Advanced と関連付ける
- 攻撃の検出精度を向上することが可能

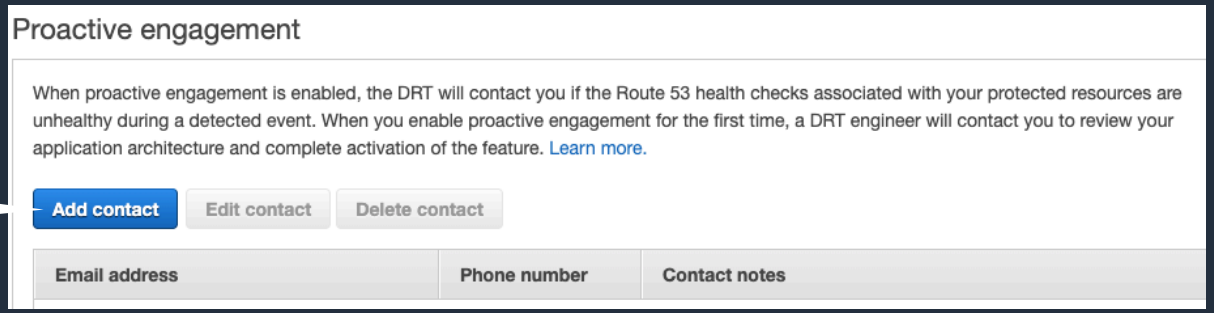




正常性ベース検出によるプロアクティブエンゲージメント

- Shield Advanced によって検出された攻撃イベント中に、保護されたリソースに関連付けられた Amazon Route 53 ヘルスチェックが異常になった場合、DDoS レスポンスチームはお客様と直接連携することができる
- DDoS レスポンスチームは、障害のある保護されたリソースに関連する攻撃イベントが検出されたとき、この情報を使用してお客様に連絡する
- ビジネスサポートプランまたはエンタープライズサポートプランが必要

アカウント毎に10個まで
登録可能



チェックリスト

- ✓ 保護すべきリソースを特定する
- ✓ Amazon CloudWatch の適切なアラーム設定
- ✓ レートベースルールの追加
- ✓ AWS WAF ロギングの有効化
- ✓ API およびS3 ログバケットへの DDoS レスポンスチームからのアクセス許可
- ✓ Route53 のヘルスチェック設定とリソースの関連付け
- ✓ プロアクティブエンゲージメントへのコンタクト先登録
- ✓ AWS Shield Engagement Lambda の設定（オプション）

https://s3.amazonaws.com/aws-shield-lambda/ShieldEngagementLambda.pdf

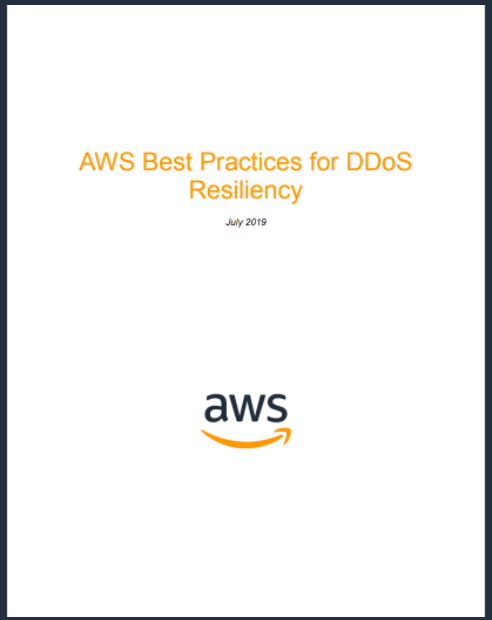
本日のアジェンダ

1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS 耐性の高いアーキテクチャ
7. Firewall Manager の活用
8. 料金体系
9. まとめ

DDoS 耐性の高いアーキテクチャ

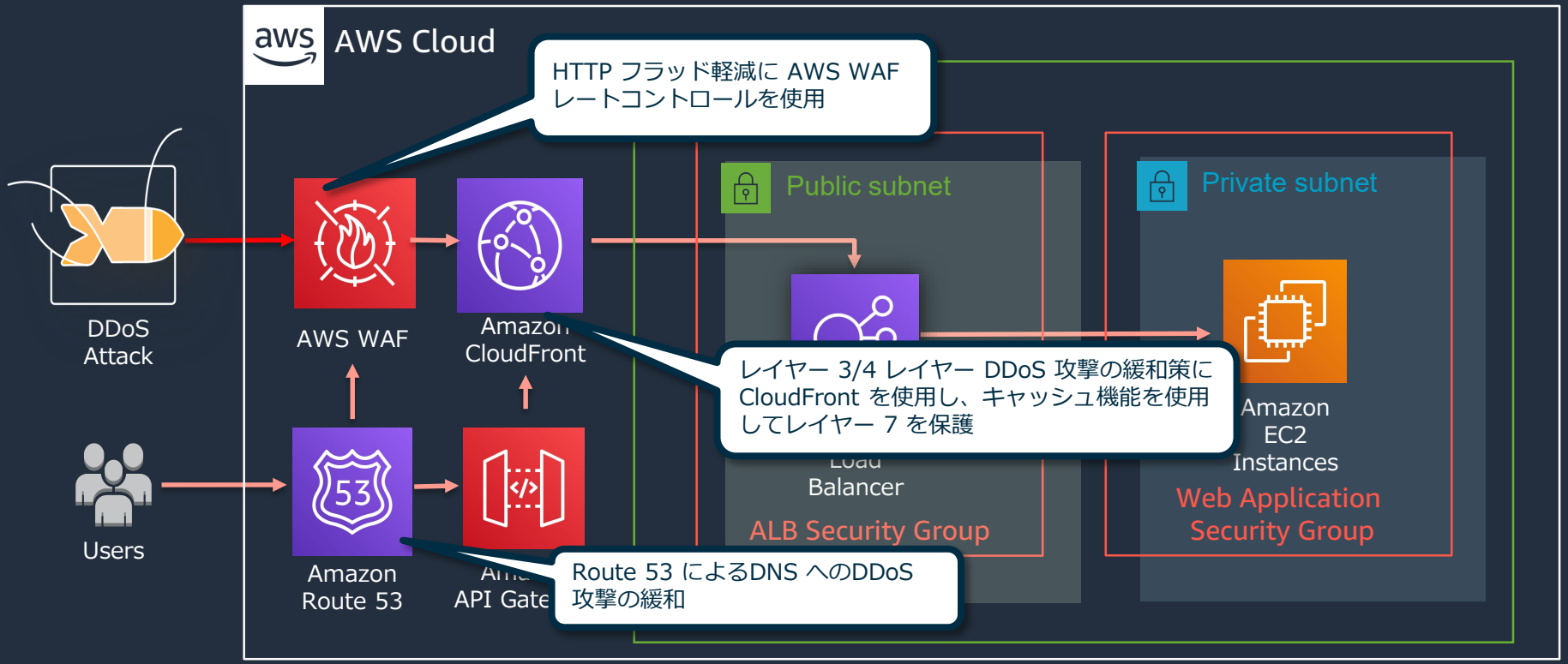
ベストプラクティスガイド：“AWS Best Practices for DDoS Resiliency”

- サービス拒否攻撃の定義
- インフラストラクチャ/アプリケーション層攻撃
- DDoS 緩和テクニック
    - インフラストラクチャ層の防御
    - アプリケーション層の防御
    - アタックサーフェースを減らす
    - AWSリソースの難読化
    - DDoS 緩和テクニック
- 運用テクニック
- 可視性

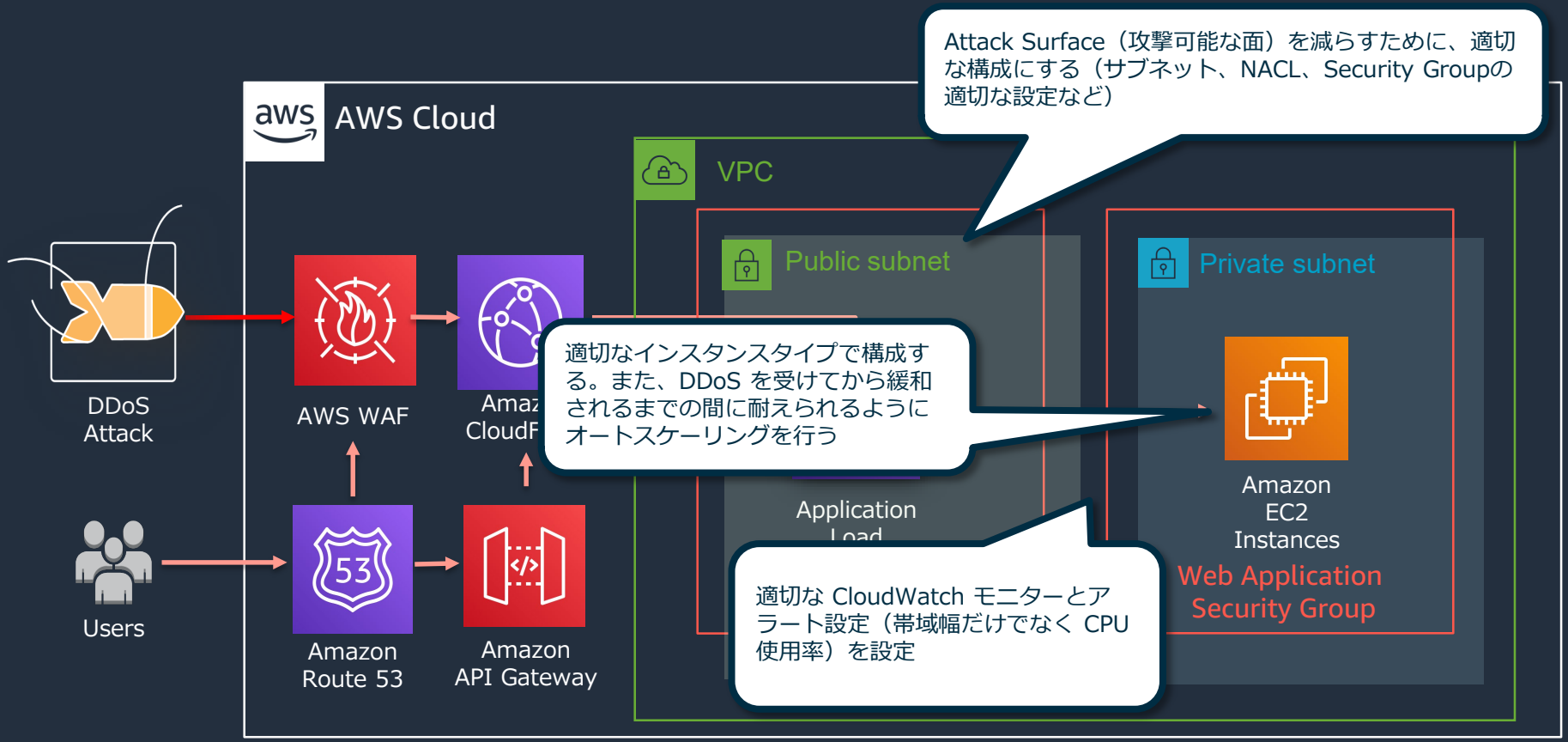


https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf
https://d1.awsstatic.com/whitepapers/jp/security/DDoS_White_Paper_Revised.pdf (日本語)

DDoS 耐性の高いアーキテクチャ



DDoS 耐性の高いアーキテクチャ



DDoS 耐性の高いアーキテクチャ

	AWS Edgeロケーション		AWS リージョン			
	Using Amazon CloudFront with AWS WAF	Using Amazon Route 53	Using Elastic Load Balancing with AWS WAF	Using Amazon API Gateway with AWS WAF	Using Security Groups and NACLs in Amazon VPC	Using Amazon EC2 with Auto Scaling
Layer 3 (for example, UDP reflection) attack mitigation	✓	✓	✓	✓	✓	✓
Layer 4 (for example, SYN flood) attack mitigation	✓	✓	✓	✓		
Layer 6 (for example, TLS) attack mitigation	✓	✓	✓			
Reduce attack surface	✓	✓	✓	✓	✓	
Scale to absorb application layer traffic	✓	✓	✓	✓	✓	✓
Layer 7 (application layer) attack mitigation	✓	✓	✓(*)	✓(*)	✓(*)	✓(*)
Geographic isolation and dispersion of excess traffic, and larger DDoS attacks	✓	✓				

** If used with AWS WAF*

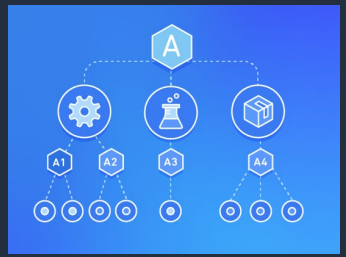
OAI…Origin Access Identity

本日のアジェンダ

1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS 耐性の高いアーキテクチャ
7. Firewall Manager の活用
8. 料金体系
9. まとめ

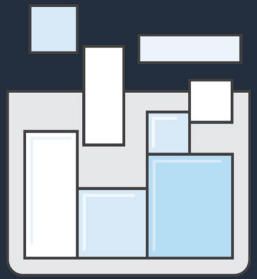
なぜ Firewall Manager を利用するのか

多数の AWS アカウントとリソースが存在



すべてのアカウントとリソースにわたってセキュリティポリシーを一元的に管理することが困難

常に新しいアプリケーションが作成される



すべてのアプリケーションを作成直後から一貫して保護することは困難

組織全体にわたる脅威の可視化

組織全体の脅威を監視して対応できる単一の場所がない

Firewall Manager & AWS Shield Advanced

アカウントとリソースにわたるセキュリティルールの管理を簡素化

- ✓ AWS Shield Advanced では追加料金なしで利用可能
- ✓ 新しいアカウントやリソースの作成時に自動的に検出し、DDoS 対策を有効化することが可能
- ✓ AWS Organizations と統合され、一元的にデプロイ可能
- ✓ すべてのアカウントに対する集約された Amazon SNS アラートにより、組織レベルの脅威の監視を実現

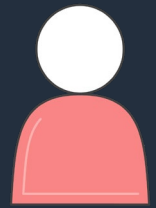
AWS Firewall Manager

AWS Shield

AWS Firewall Manager 利用の前提条件

1. AWS Organizations の有効化

2.すべてのアカウントで AWS Config を有効化

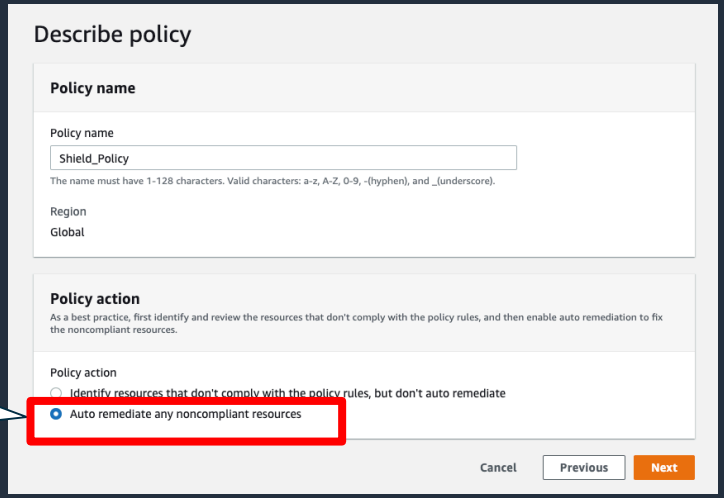


3. Firewall Manager の管理者アカウントを指定

Firewall Manager のポリシー設定

- Firewall Manager から、AWS Shield Advanced のポリシータイプを選択し、対象のスコープを定義。Organizations の複数のアカウント、複数のリソースに対し Shield Advanced を自動適用するよう設定可能

自動的に適用するよう設定することで、新たに作成されたリソースも漏れなくShield Advancedで保護する



本日のアジェンダ

1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS 耐性の高いアーキテクチャ
7. Firewall Manager の活用
8. 料金体系
9. まとめ

AWS Shield Advanced の料金

月額 3,000 USD の1年間サブスクリプション契約とデータ転送料金 （下表）

	データ転送量 ($ per GB)				
	Amazon CloudFront	ELB	Elastic IP	AWS Global Accelerator	Amazon Route 53
最初の 100 TB	$0.025	$0.050	$0.050	$0.050	追加料金なし
次の 400 TB	$0.020	$0.040	$0.040	$0.040	追加料金なし
次の 500 TB	$0.015	$0.030	$0.030	$0.030	追加料金なし
次の 4 PB	$0.010	お問い合わせ	お問い合わせ	お問い合わせ	追加料金なし
5 PB 超	お問い合わせ	お問い合わせ	お問い合わせ	お問い合わせ	追加料金なし

AWS Shield Advanced のデータ転送 (アウト) 使用料金 (GB あたり)
https://aws.amazon.com/jp/shield/pricing/

Shield Advanced 利用時の AWS WAF 課金の変化

1. Shield Advanced の保護対象とした場合は AWS WAF の費用が発生しなくなる
    - Shield Advanced の契約だけではなく保護対象としての設定が必要
    - WAF のパートナールールの費用は引き続き発生

2. Shield Advanced のSubscription 料金は組織（AWS Organizations）単位
    1. アカウント単位で3,000 USDではない
    2. データ転送量課金は各アカウント単位で発生

本日のアジェンダ

1. DDoS 攻撃とは
2. Shield Advanced のサービス内容
3. AWS リソース保護の設定 (Demo)
4. モニタリングとレポート
5. DDoS レスポンスチームとの連携
6. DDoS Resiliency Architecture
7. Firewall Manager の活用
8. 料金体系
9. まとめ

まとめ

- AWS Shield は、自動化され常に稼働している DDoS 緩和ソリューション
- Edgeサービスを利用することで分散環境での DDoS 緩和が可能
- AWS Shield Advanced は高度な DDoS 緩和と可視性を提供する
- Route53 ヘルスチェックとの関連づけにより、攻撃検出の応答性と精度を向上
- DDoS レスポンスチームからのプロアクティブな連携が可能
- DDoS 対策のためには、AWS Shield Advanced を使うだけではなくDDoS 耐性の高いアーキテクチャにすることが重要
- Firewall Manager により、複数のアカウントとリソースに対して一元的に DDoS 対策を適用し統制が可能

参考資料

- AWS Shield Advanced 開発者ガイド
  https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/ddos-overview.html
- AWS Shield Threat Landscape report
- https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf
- AWS Shield Advanced API リファレンス
  https://docs.aws.amazon.com/waf/latest/DDOSAPIReference/API_Operations.html
- AWS Shield Advanced の料金
- https://aws.amazon.com/jp/shield/pricing/
- AWS Best Practices for DDoS Resiliency
- https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf
- Behind the Scenes : Exploring the AWS Global Network
- https://www.slideshare.net/AmazonWebServices/behind-the-scenes-exploring-the-aws-global-network-net305-aws-reinvent-2018

Q&A

お答えできなかったご質問については
AWS Japan Blog 「https://aws.amazon.com/jp/blogs/news/」にて
後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に対策などを相談することも可能
- 申込みはイベント告知サイトから

(https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

ご視聴ありがとうございました

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive