CloudShift

Stylez

株式会社スタイルズ

2021年11月9日

30分でわかる！
AWSにおけるDDoS対策

aws partner network

aws partner network Advanced Consulting Partner

RANCHER PARTNER NETWORK

ZABBIX CERTIFIED PARTNER

Nextcloud Gold partner

vmware PARTNER PROFESSIONAL SOLUTION PROVIDER

自己紹介

- 馬場 潤一（Junichi Baba）

- 株式会社スタイルズ
  - AWS上でのアプリ開発・インフラ構築
    チームリーダー

- 好きなAWSサービス
  - CloudFormation、Systems Manager

本日、お話しする内容

対象

- AWSを使い始めた初級者
- DDoS攻撃対策に関して不安を持たれている方

ゴール

- DDoS攻撃がどのようなものかを理解する
- AWS上のシステムをDDoS攻撃からどのように保護するかを理解する

今回の内容：DDoS攻撃緩和対策を概要レベルで

次回の内容：WAFによる攻撃対策の設定手法

DDoS攻撃とは

DDoS攻撃とは

➢ 情報セキュリティにおける攻撃手法のひとつ

・ウェブサービスを稼働しているサーバやネットワークなどのリソース（資源）に
意図的に過剰な負荷をかけたり脆弱性を突いたりすることによって、
ネットワーク遅延やサイトアクセス不能といった妨害をする。

➢ 攻撃の目的

・抗議、嫌がらせ
・脅迫や金銭搾取

➢ 攻撃を受けた場合の被害

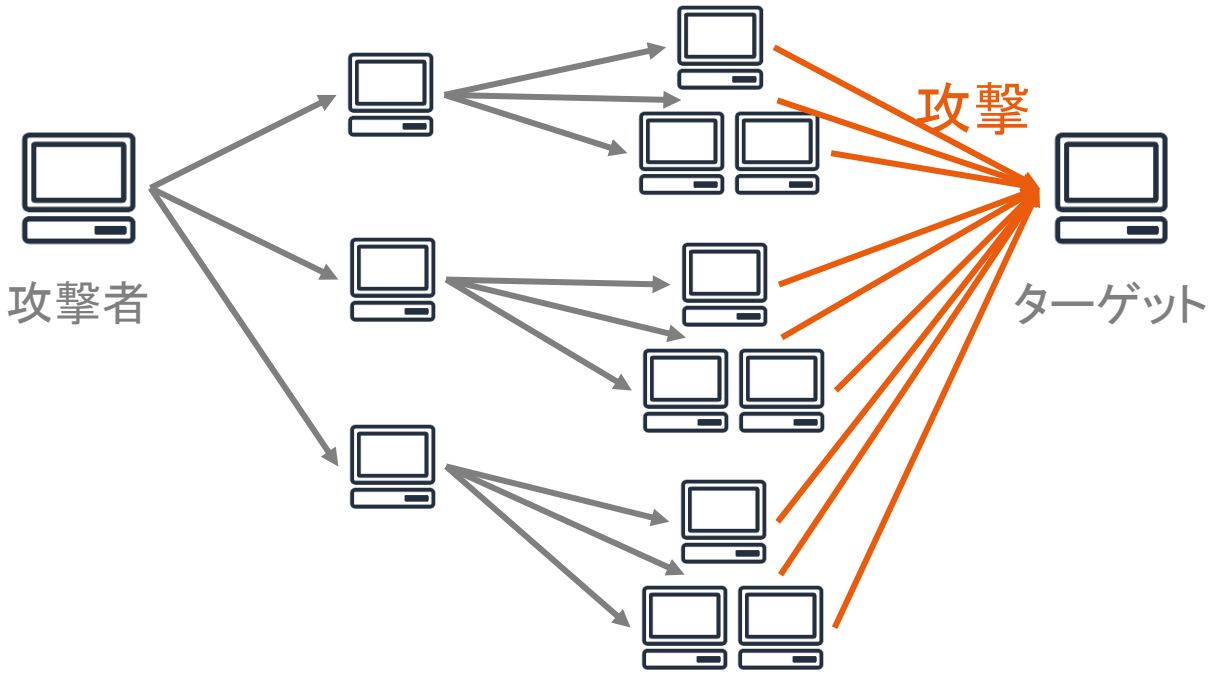
・サーバーダウン、サービス停止
・金銭的被害（クラウド利用料増加）
・情報漏洩やサイト改ざん

DDoS攻撃とは

➢ DoS攻撃とDDoS攻撃の違い

DoS（**D**enial **o**f **S**ervice attack）
単一のリソースからの攻撃

DDoS（**D**istributed **D**enial **o**f **S**ervice attack）
分散された複数のリソースからの攻撃



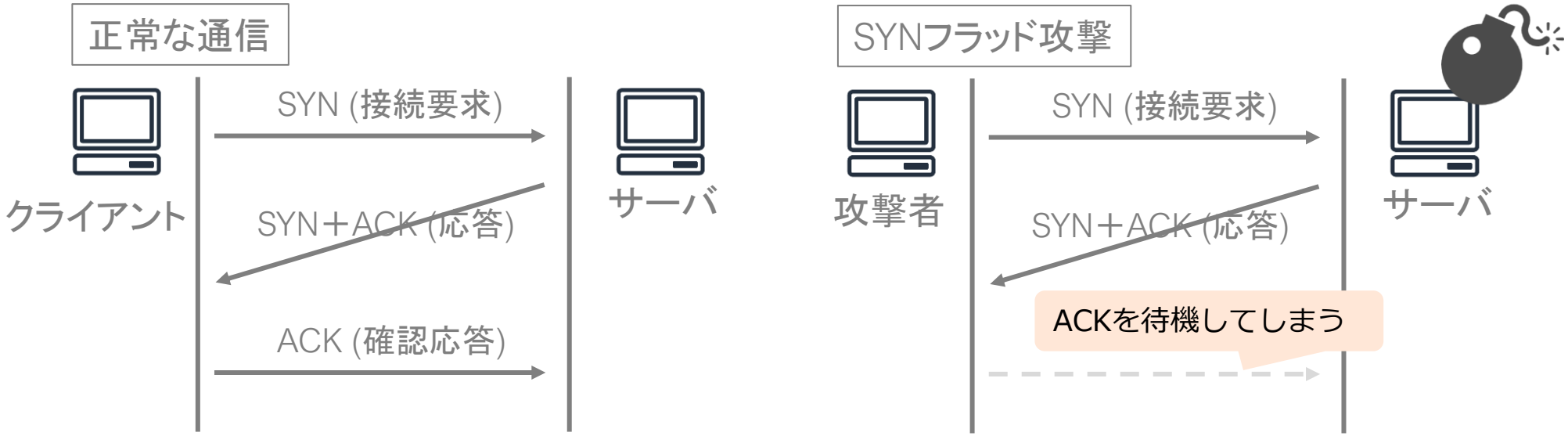
DDoS攻撃

【レイヤー】
OSI参照モデル
7階層のネットワーク標準規格

➢ 攻撃の種類

	DDoS	アプリケーション攻撃	ボット
アプリケーション（L7）レイヤー	HTTPフラッド	SQLインジェクション クロスサイトスクリプト	クロウラー Webスクレイパー
ネットワーク（L3）・トランスポート（L4）レイヤー	SYNフラッド UDPフラッド		

↑○○フラッド：特定の通信を大量に送りつける攻撃

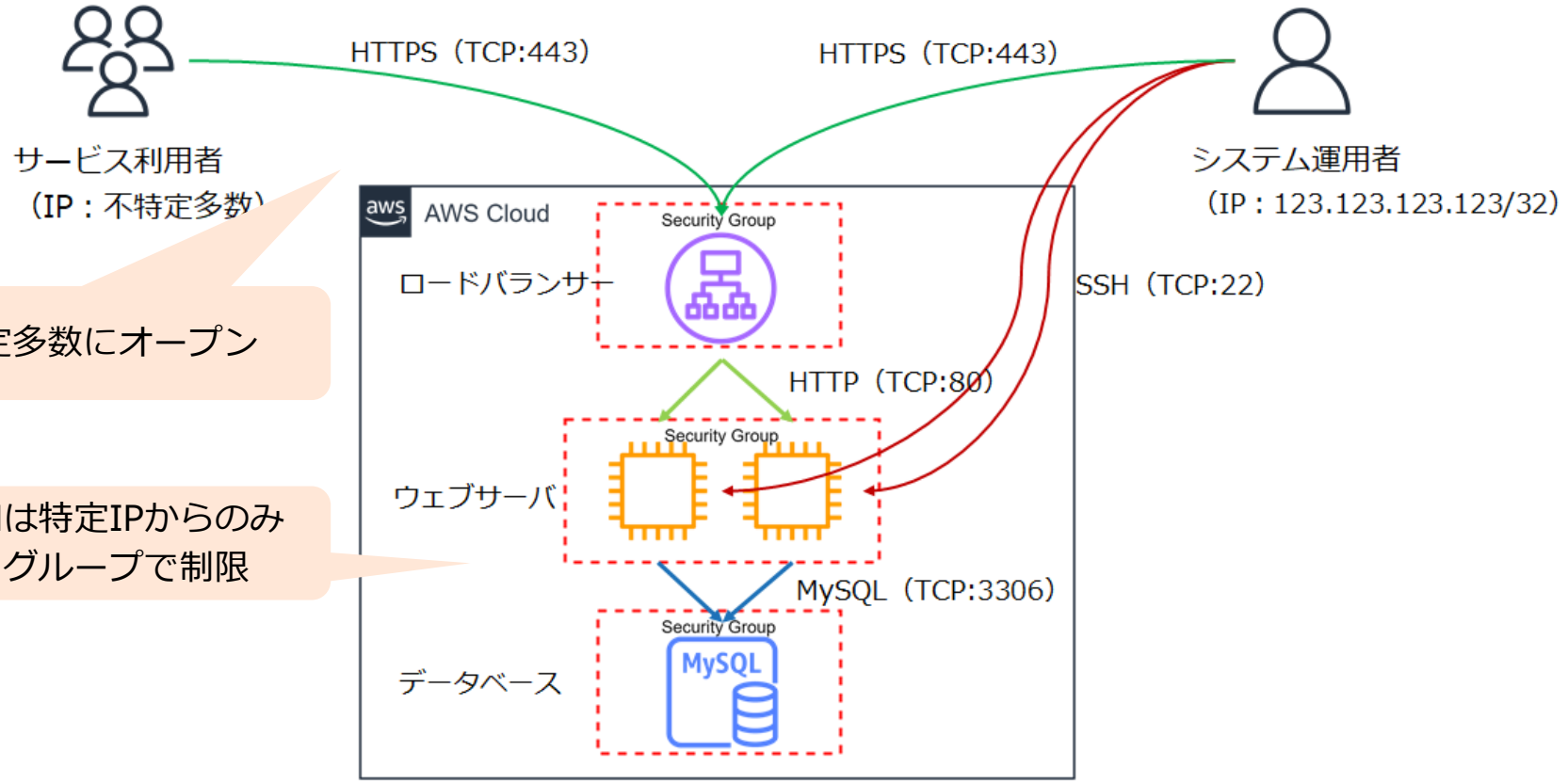


AWS上でのDDoS攻撃緩和対策

DDoS攻撃緩和対策

➢ 攻撃可能なポイントを削減

・インターネットからの接続が可能な構成を排除
・送信元IPアドレスによる制限



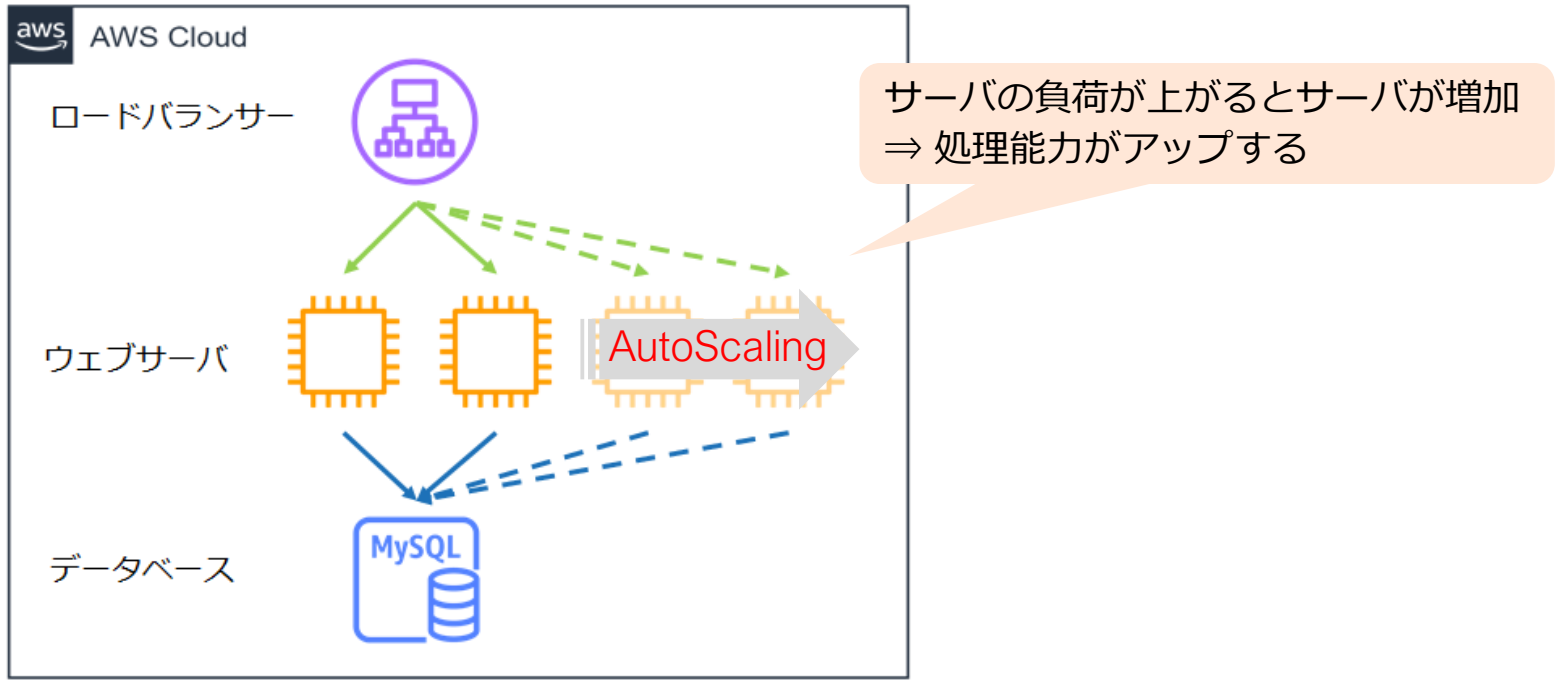
HTTPSは不特定多数にオープン

サーバへのSSHは特定IPからのみ
※セキュリティグループで制限

DDoS攻撃緩和対策

➢ サーバをスケールして攻撃を吸収する

・AutoScaling構成にし、サーバ負荷に応じてサーバ台数を自動増加
・攻撃を上回る構成を実装し、攻撃者側でより多くの時間とリソースを必要とさせる



DDoS攻撃緩和対策

➢ AWSサービスによる保護

・AWS提供サービスを利用し、公開リソースを保護

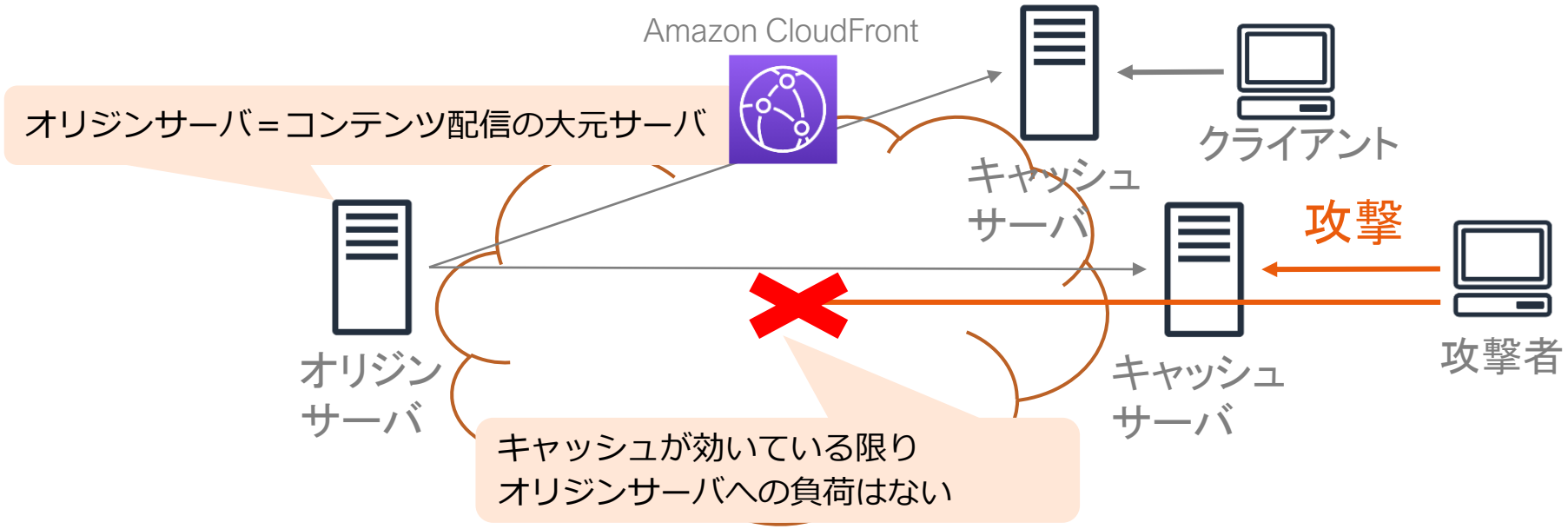
	DDoS	アプリケーション攻撃	ボット
アプリケーション（L7）レイヤー	HTTPフラッド	SQLインジェクション クロスサイトスクリプト	クロウラー Webスクレイパー
ネットワーク（L3）・トランスポート（L4）レイヤー	SYNフラッド UDPフラッド	AWS Shield	Amazon CloudFront AWS WAF

AWS Shield Advanced

DDoS攻撃緩和対策

Amazon CloudFront

・AWS提供のCDN(Contents Delivery Network)サービス
・世界中に配置されたキャッシュサーバからデータ応答
・キャッシュサーバが応答している限り、オリジンサーバに負荷がかからない
・キャッシュが効かない通信もある（アクセス毎に内容が変わるコンテンツ等）



DDoS攻撃緩和対策

AWS WAF

- AWS提供のWAF(Web Application Firewall)サービス
- アプリケーションレイヤーでの防御が可能
- 攻撃者と疑わしきIPリストからの制限
- HTTP接続に対するレート制限が可能
  （特定時間におけるクライアント毎の接続数の制限が可能）

DDoS攻撃緩和対策

AWS Shield

- AWS提供のDDoS攻撃対策サービス
- 全てのAWSアカウントに標準で適用済
- 無料
- ネットワーク（L3）トランスポート（L4）レイヤーでの攻撃から防御

アプリケーション（L7）レイヤーは防御できない

通知機能もない

DDoS攻撃緩和対策

➢ AWS Shield Advanced

・AWS Shieldの有料拡張版サービス

✓ DDoS Response Teamによる 24 x 365のサポート
- ・コンサルティング
- ・攻撃からの緩和
- ・事後分析

英語でのやり取りが前提

✓ DDoSによるコスト保護
- ・アプリケーション（L7）レイヤーでの攻撃はWAFで防御する
  この時WAF利用料は無料
- ・DDoS攻撃によりスケーリングされた場合の LB、
  CloudFront、Route53 のコストは請求対象外となる

DDoS攻撃緩和対策

➢ AWS Shield Advanced

✓ レポーティング
- 攻撃を受けた際のリアルタイム検知
- ダッシュボード画面の提供

■ サービス費用
- 月額費用：$3,000 (+データ転送量に伴う費用)
- 1年間のサービス利用をコミットが条件

DDoS攻撃に悩む大規模環境ではコストメリットがある

予算的に導入できない場合は、AWS Shield と AWS WAF を独自で導入するパターンが一般的

まとめ

まとめ

DDoS攻撃とは

- 攻撃手法の１つ
- 攻撃を受けてサービス停止や情報流出につながるリスクがある
- アプリケーションレイヤーとネットワークレイヤーそれぞれで攻撃が存在する

AWS上のDDoS攻撃緩和対策

- 攻撃可能なポイントの削減
- サーバのスケール可能な構成による攻撃吸収
- AWSサービスによる保護
  - CloudFront
  - WAF
  - Shield
  - Shield Advanced

実績豊富なエンジニア集団の技術と開発ツールで「開発期間/コスト削減」「品質向上」を実現

株式会社スタイルズ

https://www.stylez.co.jp

東京都千代田区神田小川町1-2　風雲堂ビル6階

Tel:03-5244-4111

オープンソースソフトウェア推進