aws SUMMIT

2-H1-1-17 / 2-H1-3-19

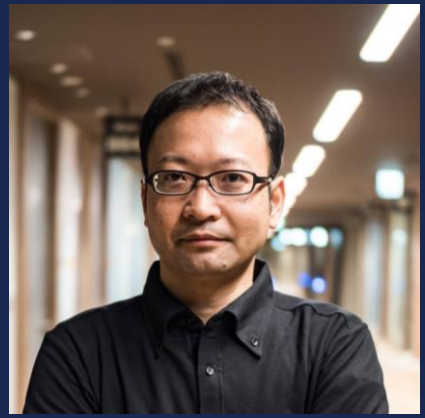
AWS の Edge ネットワーク入門

藤原 吉規
アマゾンウェブサービスジャパン 株式会社 技術統括本部 ソリューションアーキテクト

自己紹介

藤原 吉規 (ふじわら よしのり)

西日本担当 ソリューション アーキテクト



- AWS 大阪オフィスにいます
- 関西のビジネスチャットスタートアップ企業で 6 年間 AWS を活用
- Edge 系サービスを担当
- AWS サムライ 2013
- 好きな AWS サービス: **Amazon CloudFront, Lambda@Edge, AWS サポート**

想定するオーディエンス と セッションの目的

想定するオーディエンス

- Web サイトの高速化やセキュリティ対策に関心がある
- 基本的な Web 技術を理解している
    - URL、HTTP/HTTPS、リクエスト/レスポンス、DNS、DDoS 攻撃 等

セッションの目的

- AWS の Edge サービスとは何か、概要とメリットを理解する
- Edge サービスをどのようなシステムに活用できるか理解する

Agenda

- AWS の Edge サービス
- Web アクセスの仕組みと課題
- Amazon CloudFront
- Lambda@Edge
- AWS WAF
- まとめ

Amazon CloudFront

Lambda@Edge

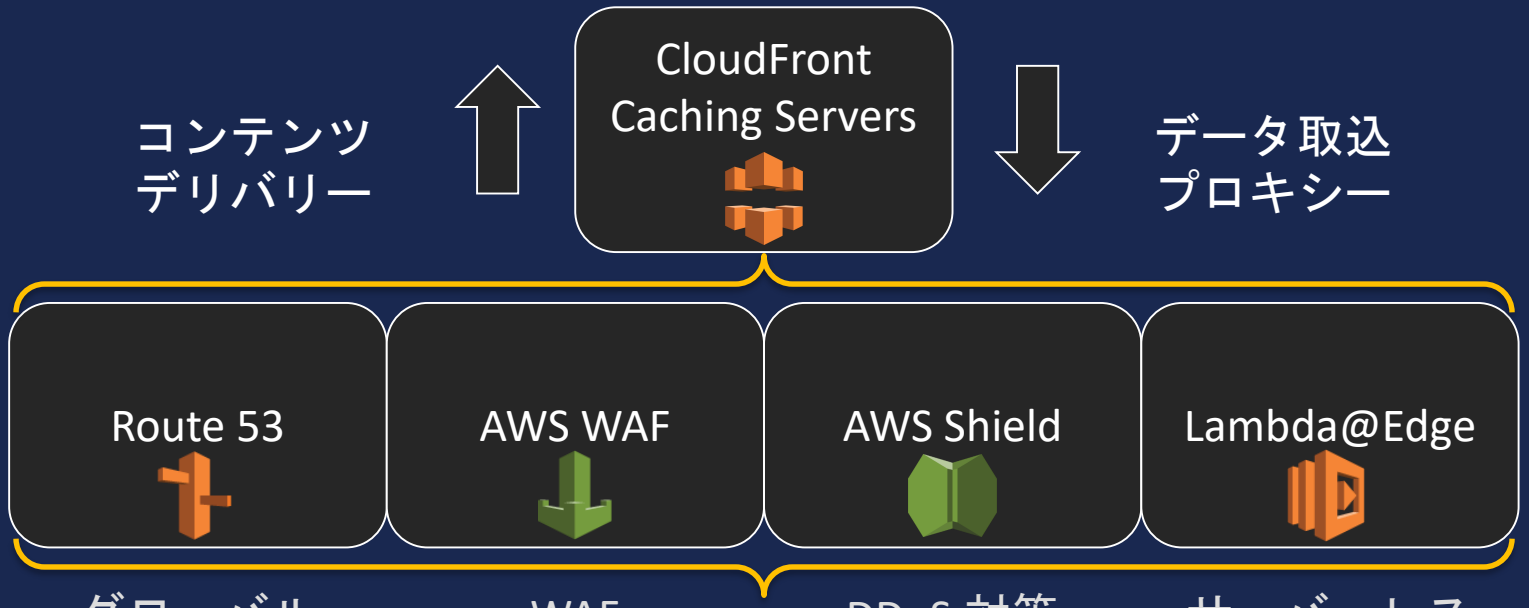
AWS WAF

aws SUMMIT

AWS の Edge サービス

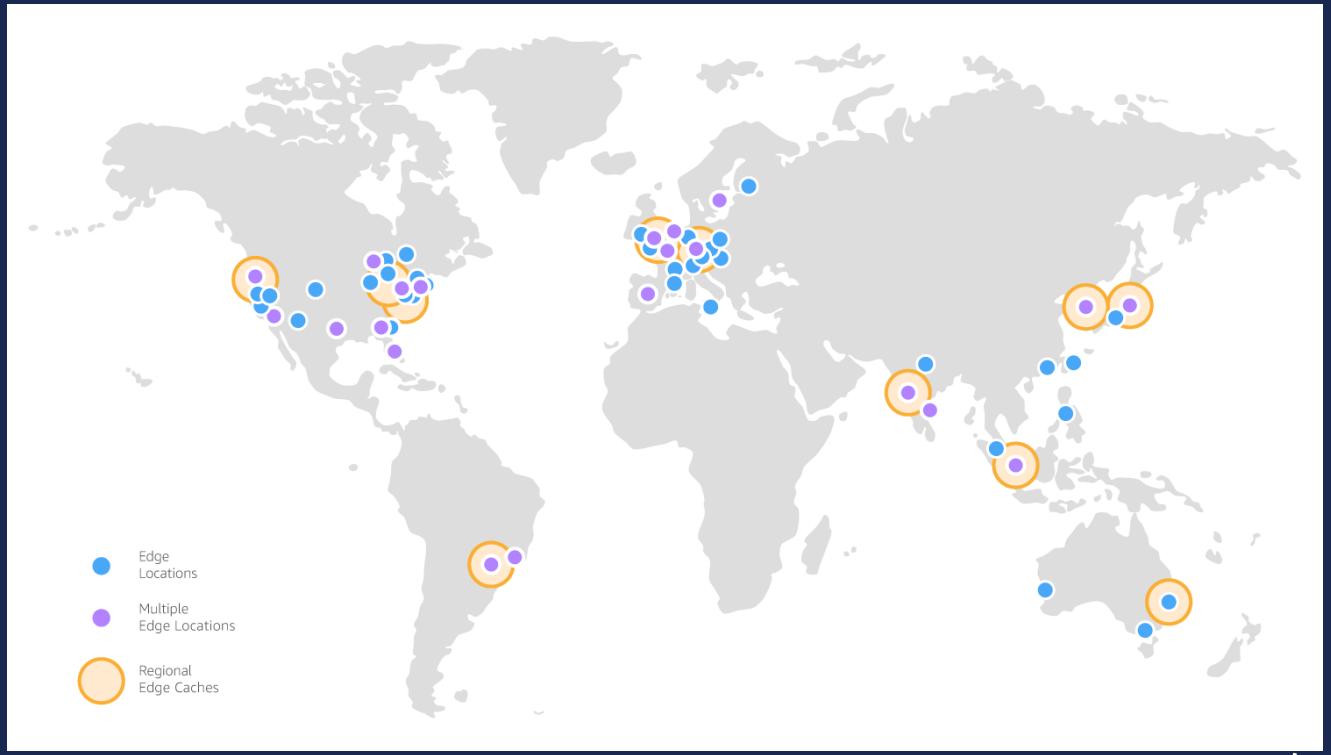
AWS の Edge サービス

AWS のエッジロケーションから提供されるサービス群
ユーザーが最初にアクセスするサービスをユーザーに近い場所から提供



エッジロケーション

117 PoPs (106 エッジロケーション + 11 リージョナルエッジキャッシュ) ※



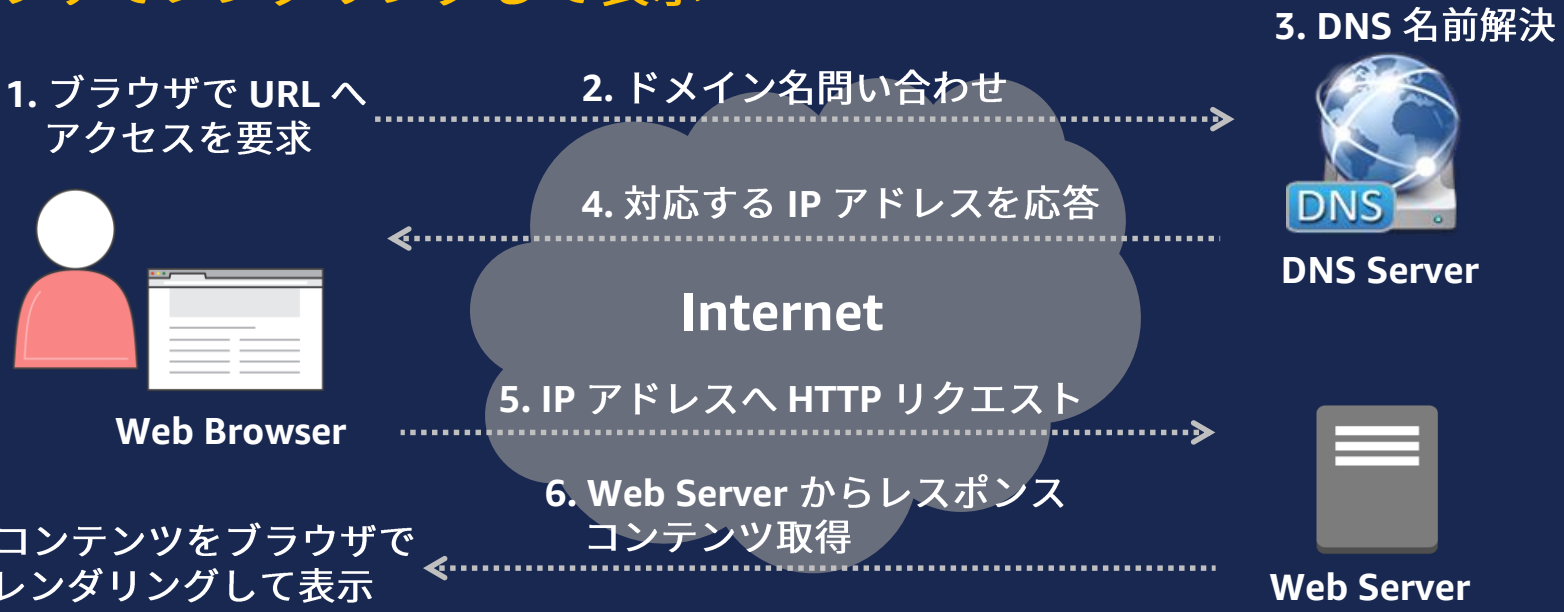
※ 2018 年 5 月末時点

aws SUMMIT

Web アクセスの仕組みと課題

Web アクセスの仕組み

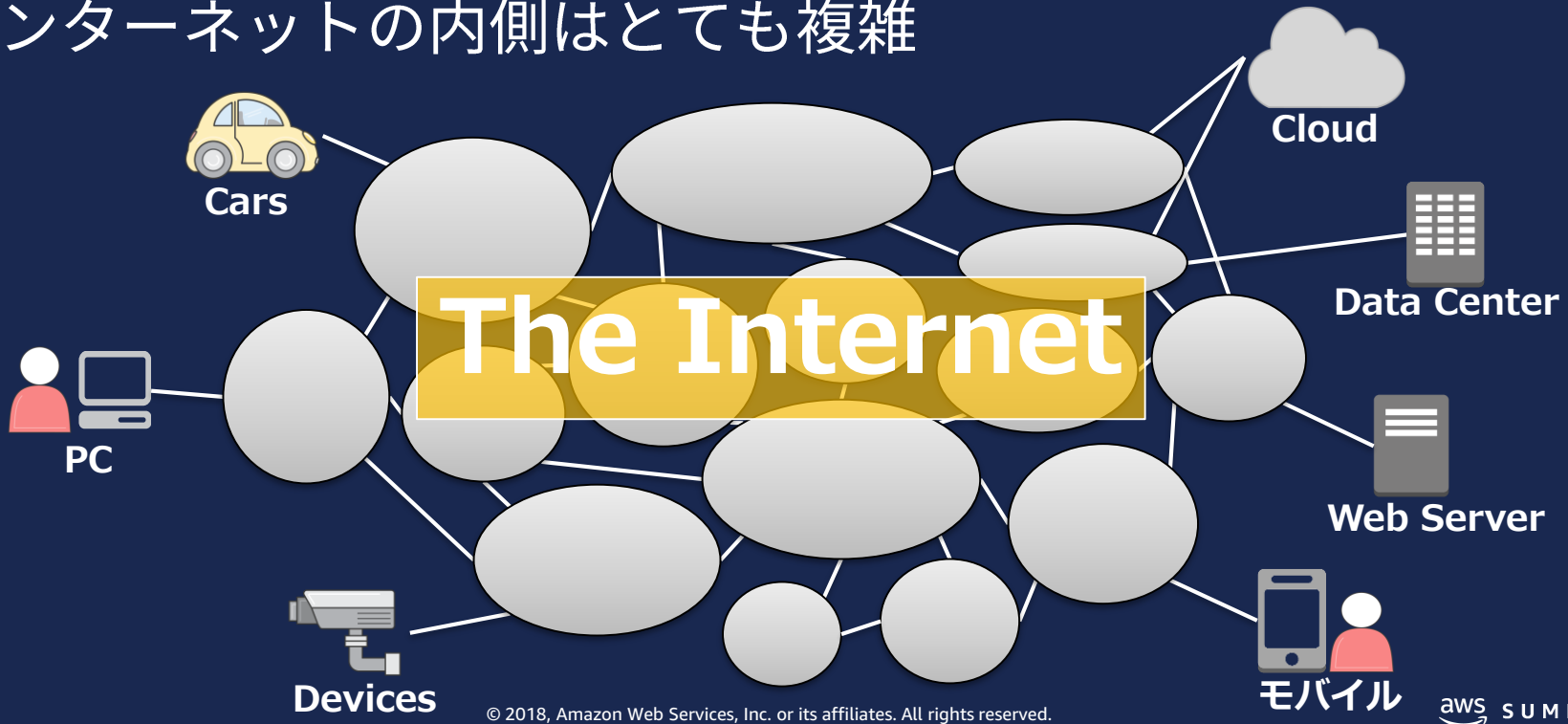
ブラウザから URL を指定してアクセス要求、名前解決を行い、
インターネット経由で Web サーバーに接続しコンテンツを取得、
ブラウザでレンダリングして表示



インターネットの仕組み

インターネットは、個別の組織によって管理されたネットワークを
複数相互に接続することで実現されている

インターネットの内側はとても複雑



インターネットの仕組み

高品質な通信の確保とセキュリティ脅威からの保護が課題

- ネットワークのネットワーク (Inter-network)
  - ISP 同士がピアリングやトランジットにより接続。ISP 毎のネットワークの品質 ※ は様々
  - 宛先までの経路は時々の状況により変化、**品質は常に一定ではない**
  - 特に、**距離の離れた通信は遅延の影響**を受けやすい
- 誰からでもアクセスできる
  - 同じプロトコル (IP) でアクセスでき、誰からでも情報がやり取りできることが、インターネットの大きなメリット
  - 逆に言うと、**誰からでも攻撃される可能性がある**ということ
  - 最近は**アプリ脆弱性をついた攻撃、DDoS 攻撃**も多い

※品質とは、遅延、スループット、損失率などを表す

大規模な Web サイトでの課題

インターネット経由で大規模な Web サイトを利用する場合は、
レスポンス、キャパシティ、アプリセキュリティ、DDoS 対策が課題

- レスポンスの遅延、不安定なレスポンス
- 大量アクセスへの対応
- アプリのセキュリティ対策
- DDoS 攻撃の対策

レスポンスの遅延、不安定なレスポンス

インターネット経由でのアクセスにおけるネットワーク遅延の影響

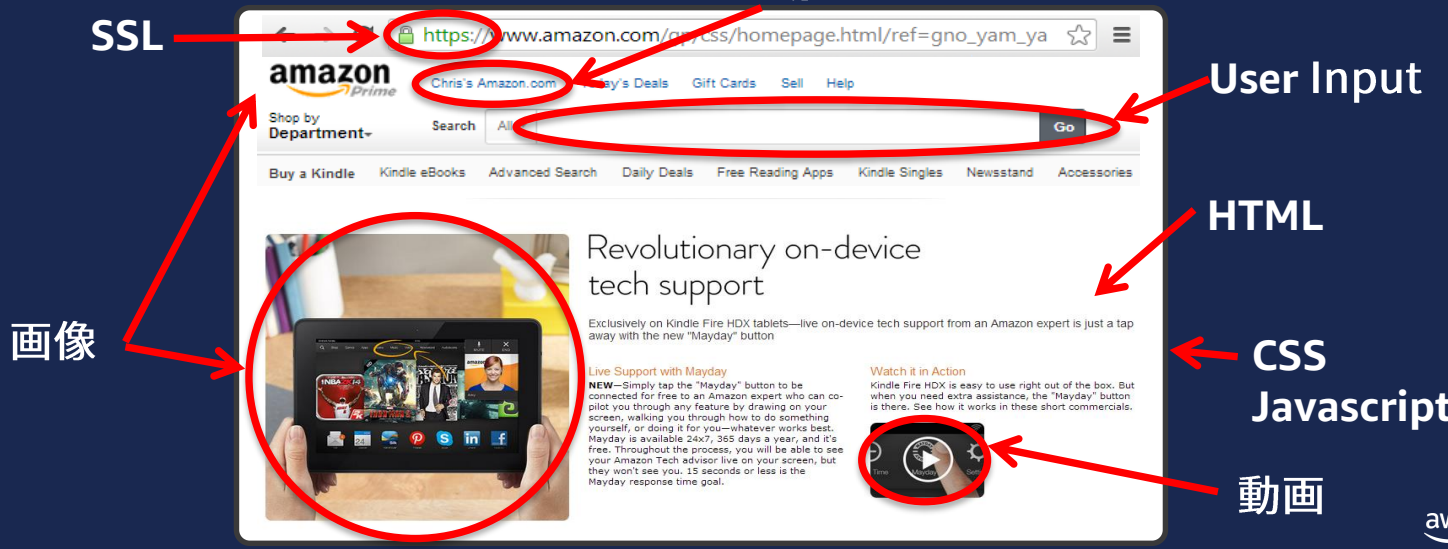
- ネットワーク遅延は、(物理的、ネットワーク的な)距離に依存
- コンテンツの元サーバー(オリジン)が遠いと、応答に時間がかかる
- 応答時間の多くが、ネットワーク転送の待ち時間を占める場合も

Resource Scheduling	TIME
Queueing	0.81ms
Connection Start	TIME
Stalled	3.49ms
DNS Lookup	113.03ms
Initial connection	650.28ms
SSL	544.69ms
Request/Response	TIME
Request sent	0.17ms
Waiting (TTFB)	452.97ms
Content Download	1.78ms
Explanation	1.22s

大量アクセスへの対応

大量のアクセスをさばくためには、不要なトラフィックをオリジンに到達させない効率的な仕組みが必要

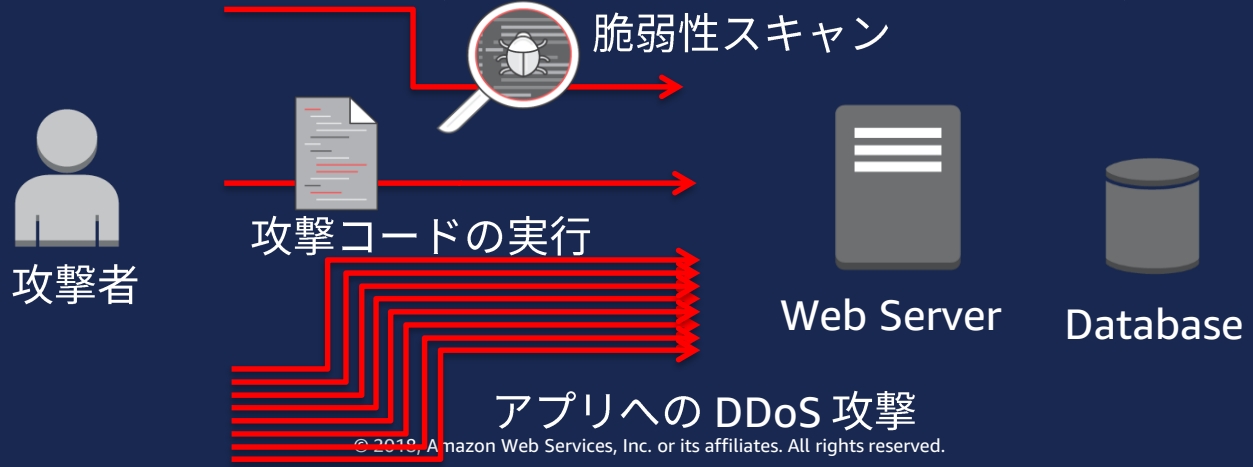
- Web コンテンツには、あまり**変化しない静的なデータ**が多く含まれる
  (画像・動画、CSS、JavaScript 等のファイル)
- 同じデータを何度も取得するのは、**ネットワーク帯域、サーバーリソースの無駄な消費**



アプリケーションのセキュリティ対策

社会的信用の失墜、サイト閉鎖による機会損失などを防ぐため
Web アプリケーションへの攻撃に対する対策が必要

- **アプリケーション脆弱性のスキャン:** 攻撃を仕掛けるターゲットを見極める
- **アプリケーション脆弱性をついた攻撃:** SQL インジェクション、クロスサイトスクリプティング等
- **アプリケーションに対する DDoS 攻撃:** 一見適切だが悪意のある要求でアプリケーションリソースを枯渇させる (HTTP GET、DNS クエリフラッド)



DDoS (Denial of Service) 攻撃の対策

サービスの可用性を確保するため DDoS 攻撃に対する対策が必要

- **Volumetric DDoS attacks**: 大量パケットでネットワークを輻輳させる
- **State exhaustion DDoS attacks**: ファイヤウォール、ロードバランサなど状態を管理するデバイスに負荷をかける

AWS の Edge サービスによる解決

大規模な Web サイトで AWS の Edge サービスを活用

ネットワーク遅延影響の低減

- ユーザーに近いロケーションからWebコンテンツを返す

オリジンでの無駄なリソース消費を低減

- 繰り返しアクセスされるデータをキャッシュし、オリジンへのアクセスを低減する

アプリケーションへの攻撃に対する対策

- パケットをアプリケーションレベルで監視し、不正なアクセスを遮断する

DDoS攻撃に対する対策

- DDoS攻撃に対応できるインフラにより、DDoS攻撃の影響を低減する

Amazon CloudFront

AWS WAF

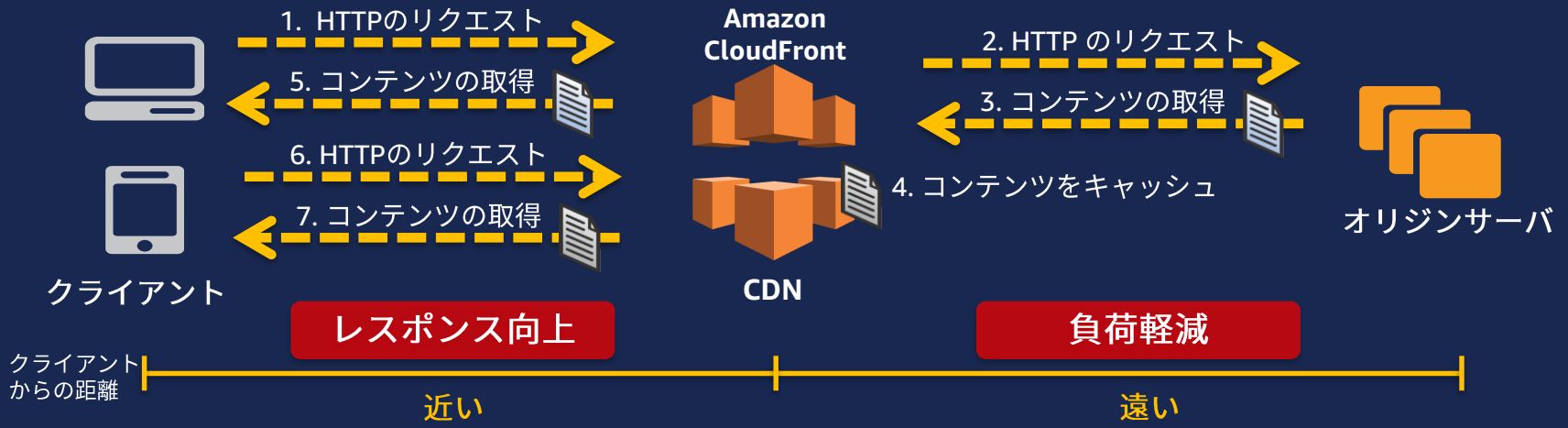
AWS Shield

Amazon CloudFront による CDN (Contents Delivery Network)

大容量キャパシティを持つ地理的に分散したサーバー群(エッジ)から
コンテンツをキャッシュしたり代理配信をするサービス

CDN 導入の利点

- ユーザーを一番近いエッジロケーションに誘導することで **配信を高速化**
- エッジサーバでコンテンツのキャッシングを行い **オリジンの負荷をオフロード**



AWS WAF による Web アプリケーションの保護

アプリケーションレベルでパケットを解析

不正なアクセスを遮断し、正しいアクセスのみを許可する

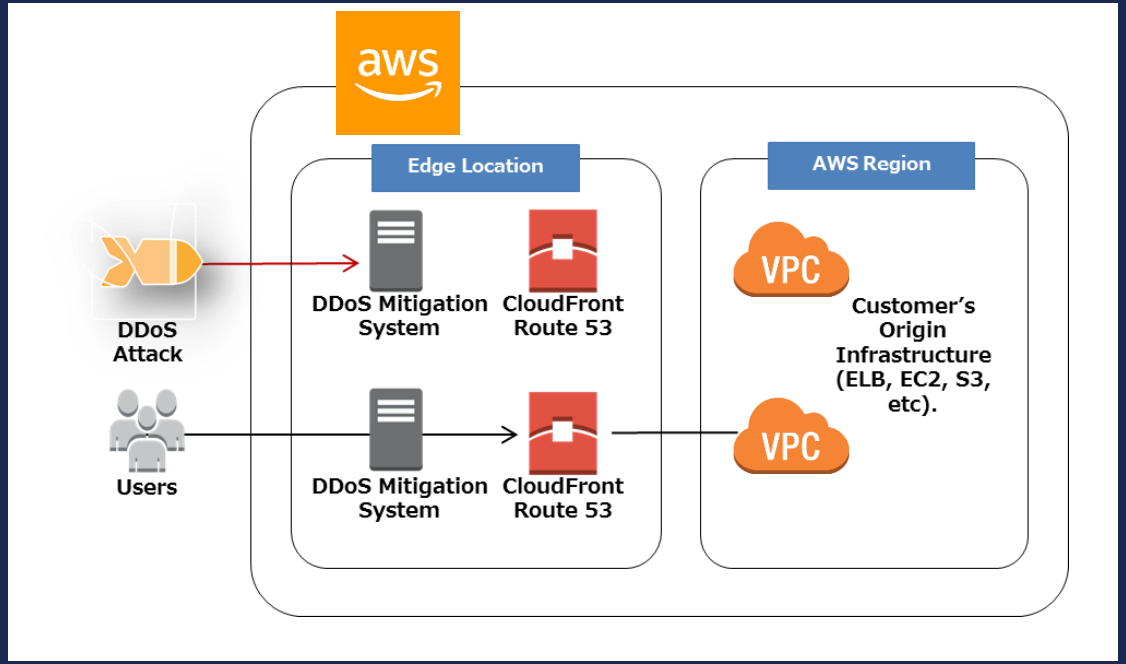
- Web サーバーのフロントに置かれる
- アプリレベルのトラフィックを監視 (HTTP, URL, Cookie, クエリ文字列)
- ルールに基づいて、不正なアクセスを遮断しレポート

AWS Shield による DDoS 攻撃対策

Amazonのノウハウを詰め込んだDDoS攻撃を緩和するサービス

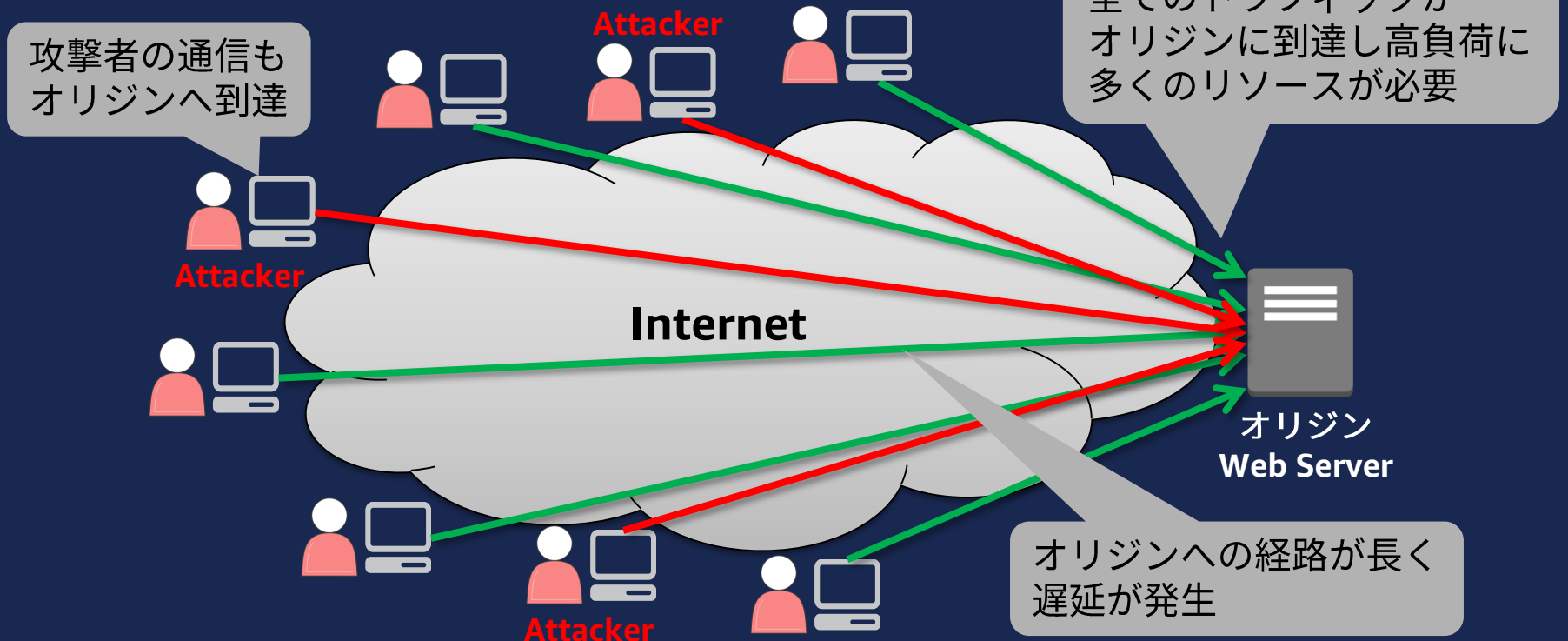
デフォルトで有効になっており無料で利用できる

- 自社製の DDoS 緩和システムでサービスベースの防御
- 全てのパケットは検査され、学習アルゴリズムでスコアリングされる
- 他ユーザートラフィックは、インラインシステムが可用性、スループット、レイテンシに影響を与えずに迅速に対応



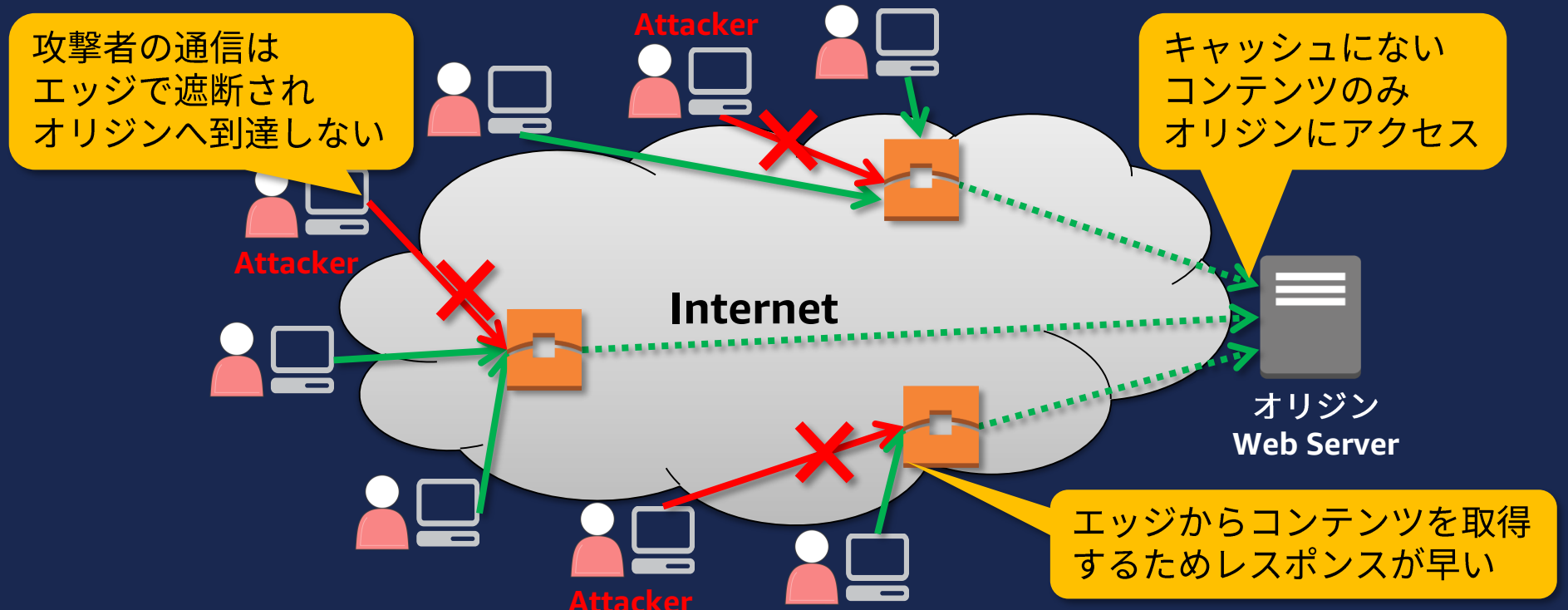
Edge サービス 導入前

攻撃を含む全てのトラフィックがオリジンに到達、オリジンが高負荷
長い経路で遅延が大きくレスポンスも悪い



Edge サービス 導入後

トラフィックはエッジから返され、オリジンへは一部のみ転送される
攻撃者からのアクセスはエッジロケーションで遮断される



様々な業界の多くの事例

メディア & エンターテイメント

ゲーム

ソーシャルメディア、デジタル広告、EdTech、ファイナンス

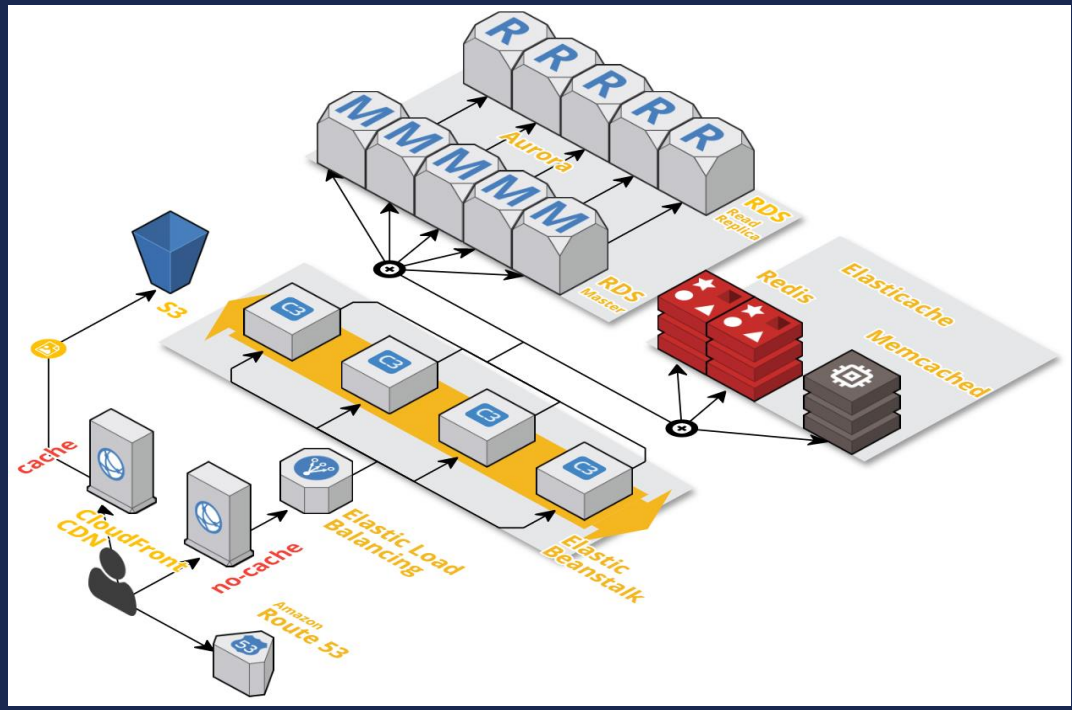
エンタープライズ

Eコマース

事例: ディライトワークス様

『 Fate/Grand Order 』の海外展開のため すべてのリクエストを CloudFront 経由に

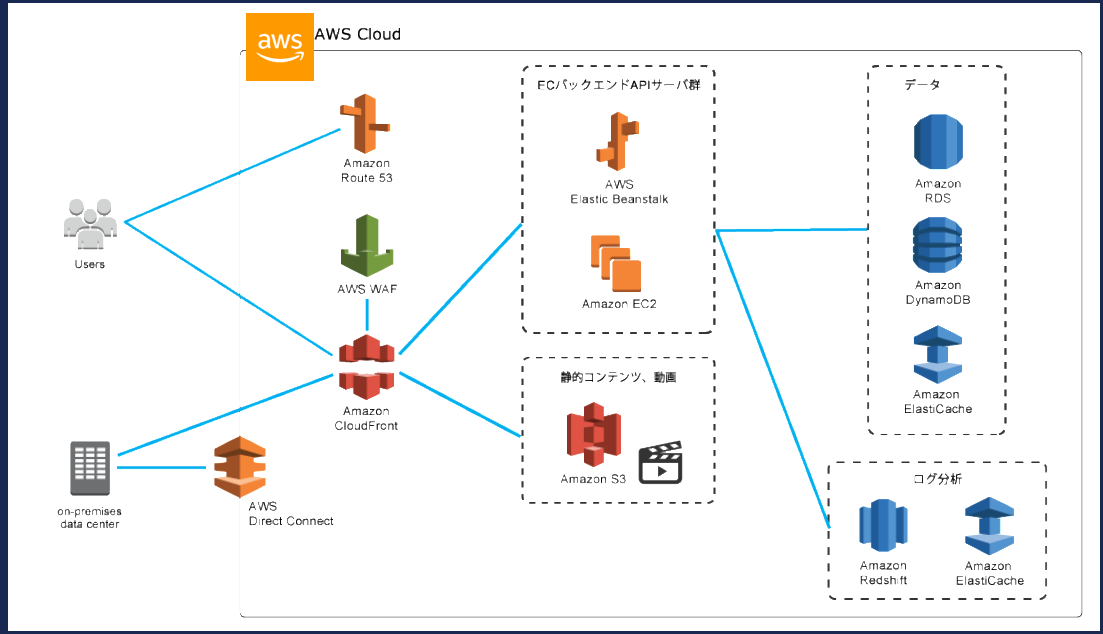
- CloudFront 経由のアプリケーション通信はキャッシュせず、通信の最適化のために利用
- Route 53 の Alias 機能を使用し DNS クエリ回数を削減
- 海外からの HTTPS 通信のレイテンシーが改善され、単一拠点での海外展開が可能に



事例: ジュピターショップチャンネル様

DC で運用していた EC サイトを AWS へ移行
サイトの性能限界が上昇し、ピーク時でもインフラの安定稼働が可能に

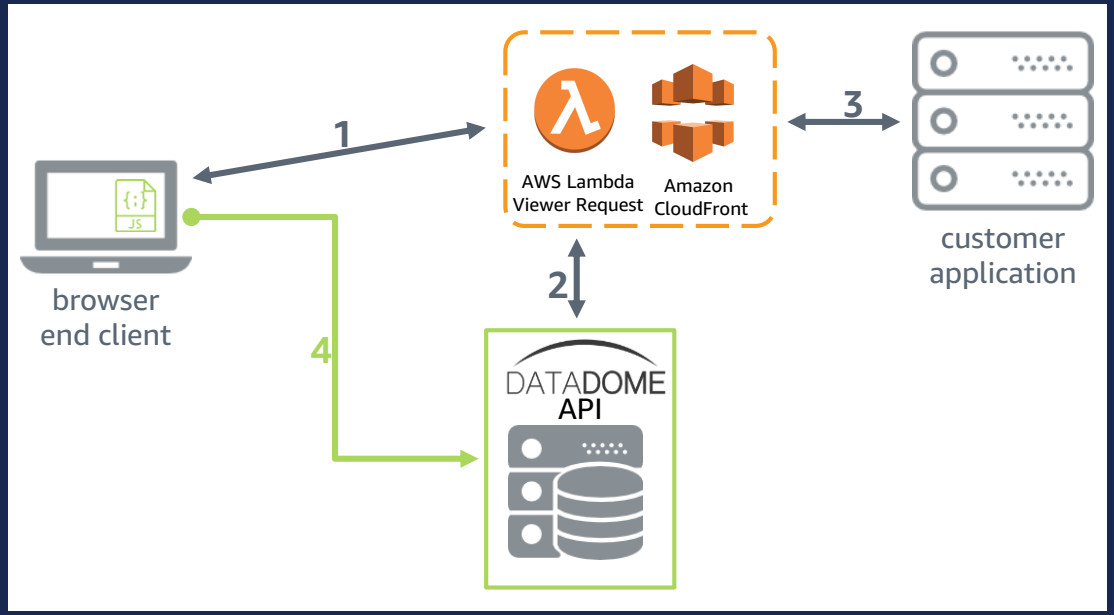
- CloudFront で、急務だったコンテンツ配信の課題を改善
- AWS WAF を利用して、悪意のあるアクセスの IP ブロックや、アプリ脆弱性をついた攻撃をブロック
- 標準機能で DDoS 攻撃からサイトを保護
- オリジンも AWS で統一することで高い拡張性が得られる点も高くご評価



事例: DataDome 様

Lambda@Edge と CloudFront を利用して
ボット対策セキュリティソリューションをワンクリックで利用可能に

- Lambda@Edge を使用することで、サーバーサイドモジュールのセットアップと JS タグの指定が不要に
- ユーザーは 1 回のクリックで 2 分以内に DataDome をアクティブにできるように
- 「エッジ」でウェブサイト、コンテンツ、ユーザー、API を保護



aws SUMMIT

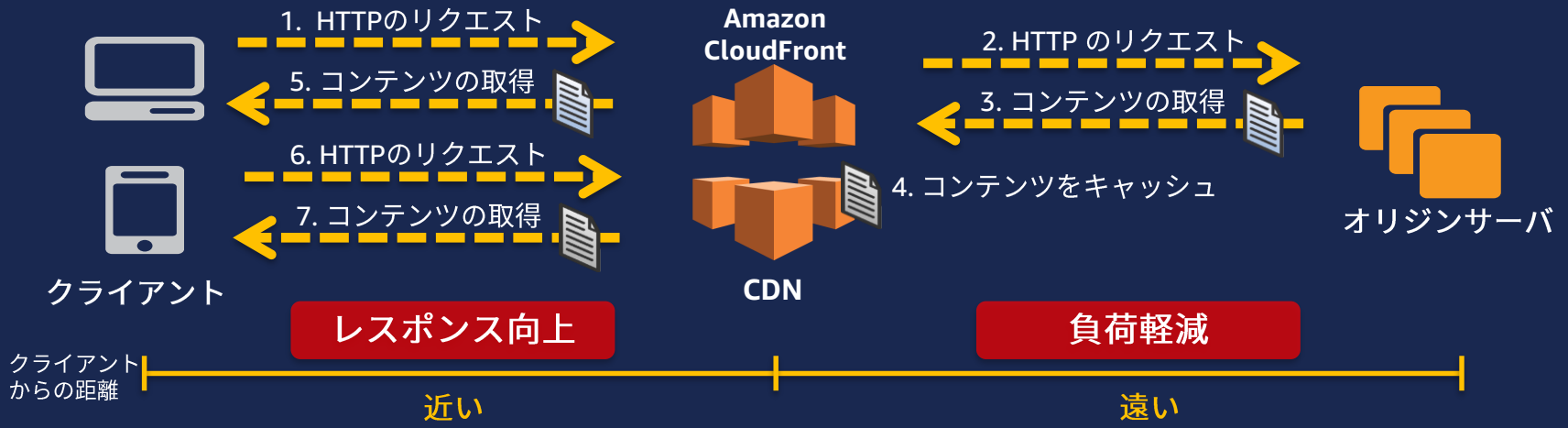
Amazon CloudFront
Contents Delivery Network

CloudFront の仕組み

大容量キャパシティを持つ地理的に分散したサーバー群(エッジ)から
コンテンツをキャッシュしたり代理配信をするサービス

CDN 導入の利点

- ユーザーを一番近いエッジロケーションに誘導することで **配信を高速化**
- エッジサーバでコンテンツのキャッシングを行い **オリジンの負荷をオフロード**

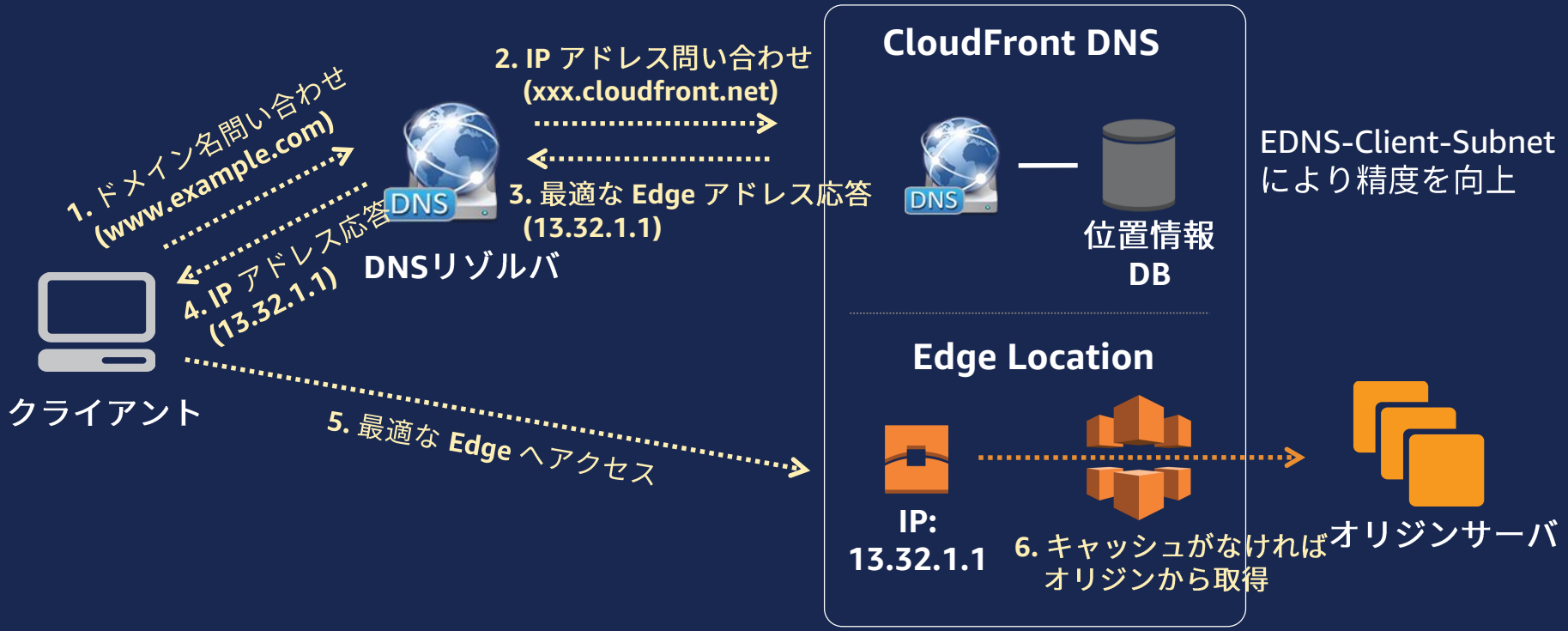


CloudFront の特徴

高性能な分散配信 (世界117拠点の接続ポイント) ※2018年5月末時点
高いパフォーマンス (高いパフォーマンスの実績)
キャパシティアクセスからの解放 (予測不可能なスパイクアクセスへの対応)
ビルトインのセキュリティ機能 (WAF 連携、DDoS 対策)
設定が容易で即時利用可能 (GUI からの設定で15 分程度でサービス利用可能)
充実したレポーティング (ログ、ダッシュボード、通知機能)
完全従量課金 (初期費用がなく安価、一時的な利用も可能)

最適なエッジロケーションの割当

DNS を応用した仕組みで最適なエッジロケーションを割当



CloudFront の様々な機能

- 動的コンテンツの配信 (フォワードオプション)
- 暗号化通信 (TLS/SSL、独自SSL証明書(3rd party, ACM※))
- プライベートコンテンツ提供 (署名付きURL/Cookie)
- フィールドレベル暗号化を使用した機密データの保護
- GZIP 圧縮
- アクセス元地域の制限
- カスタムエラーページ
- IPv6 サポート
- HTTP/2 サポート

※ Amazon Certificate Manager

aws SUMMIT

Lambda@Edge
エッジにおける
サーバーレスコンピューティング

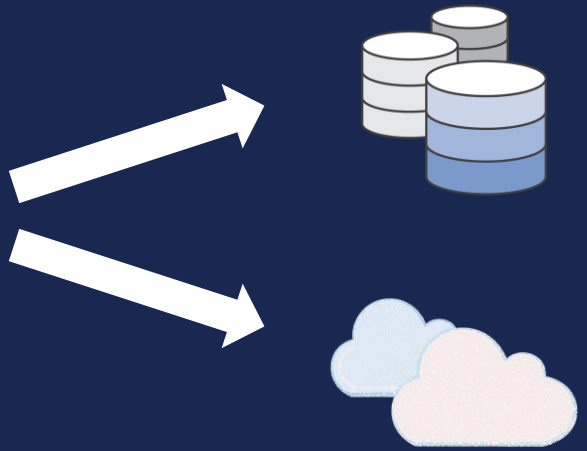
Amazon CloudFront

AWS Lambda

Lambda@Edge

サーバーレスと Lambda

イベントソース　　Lambda 関数　　あらゆるサービス

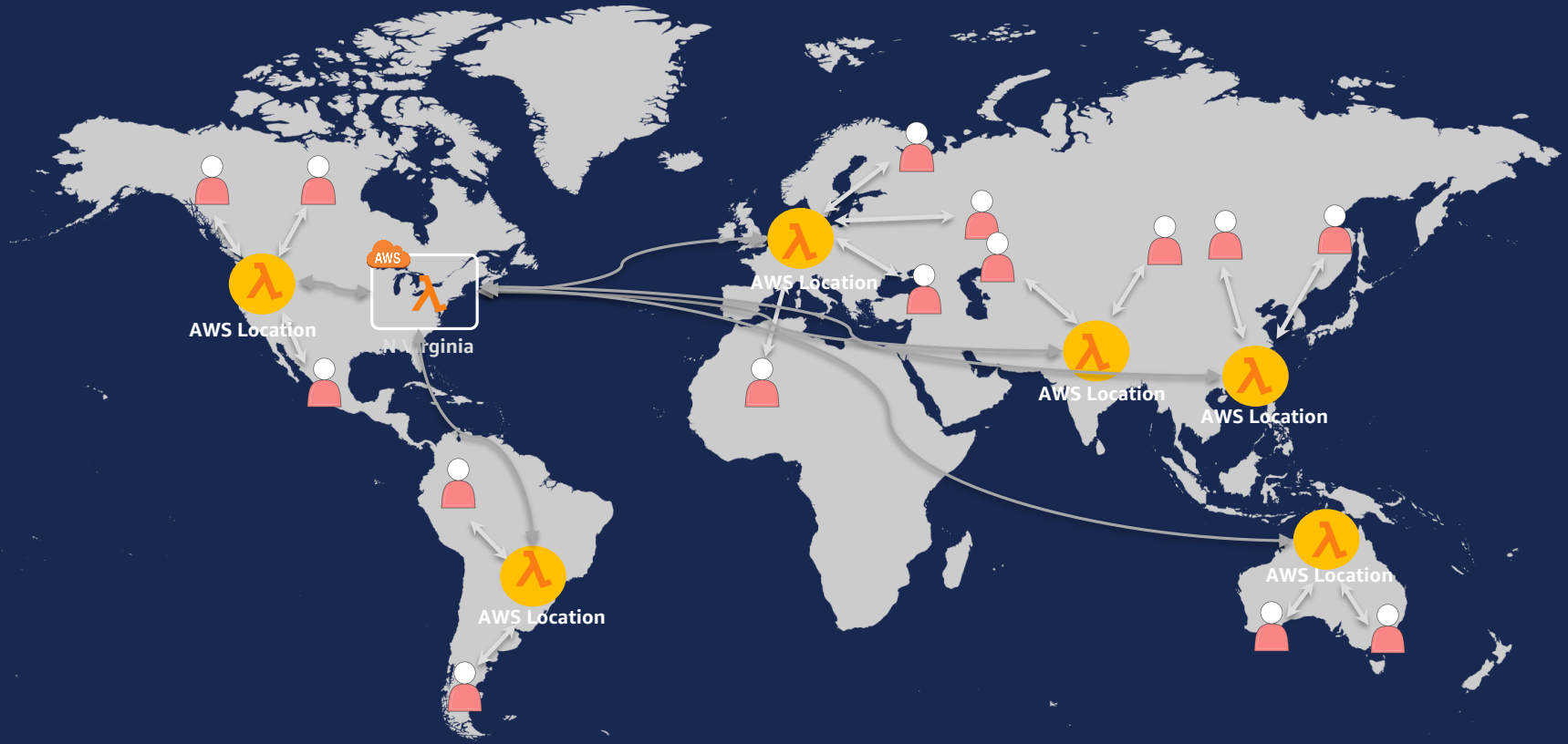


データ更新

リクエスト

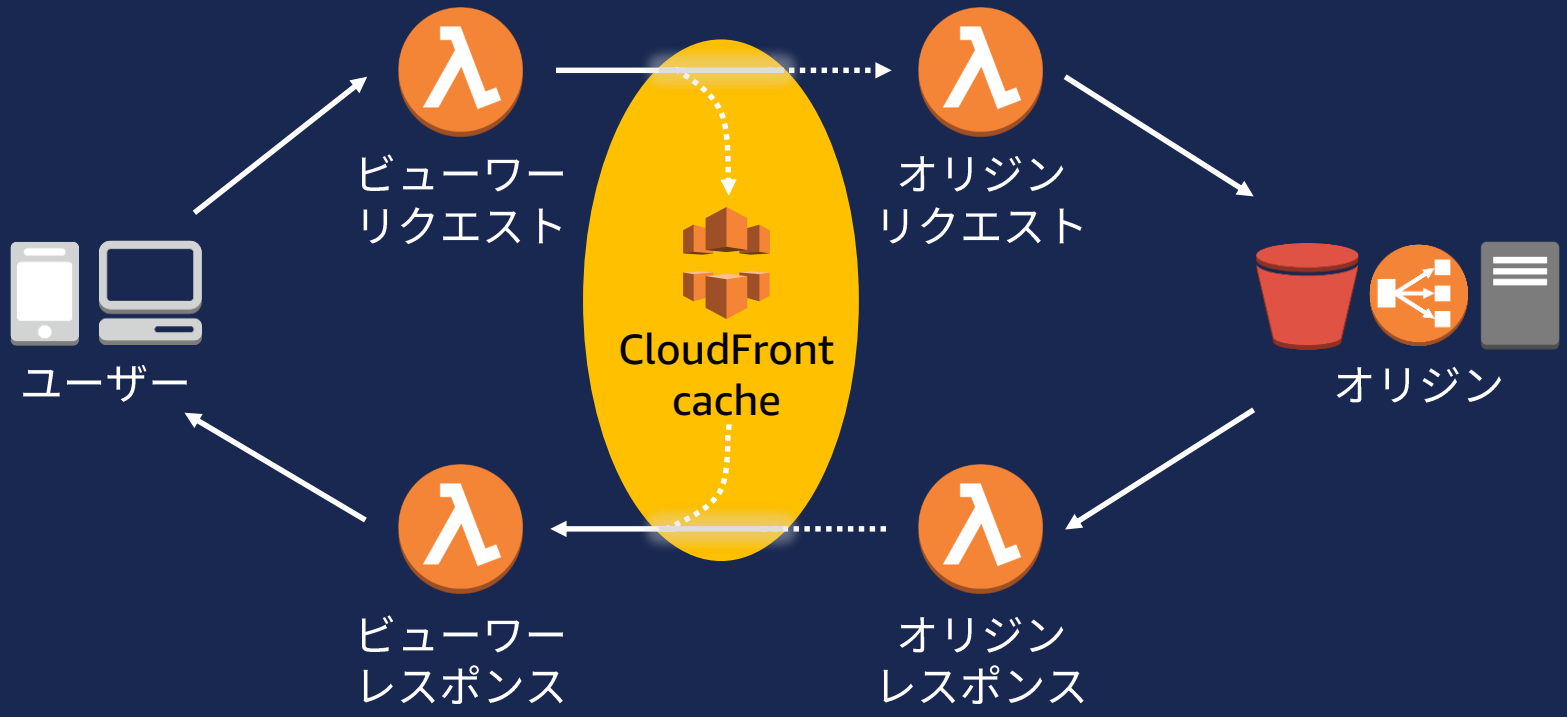
リソース
状態の更新

Lambda 関数をグローバルで実行可能



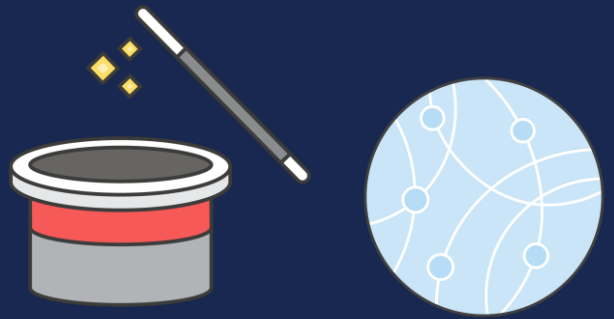
CloudFront トリガー

Lambda 関数を使用して CloudFront リクエストとレスポンスを変更



Lambda@Edge のユースケース

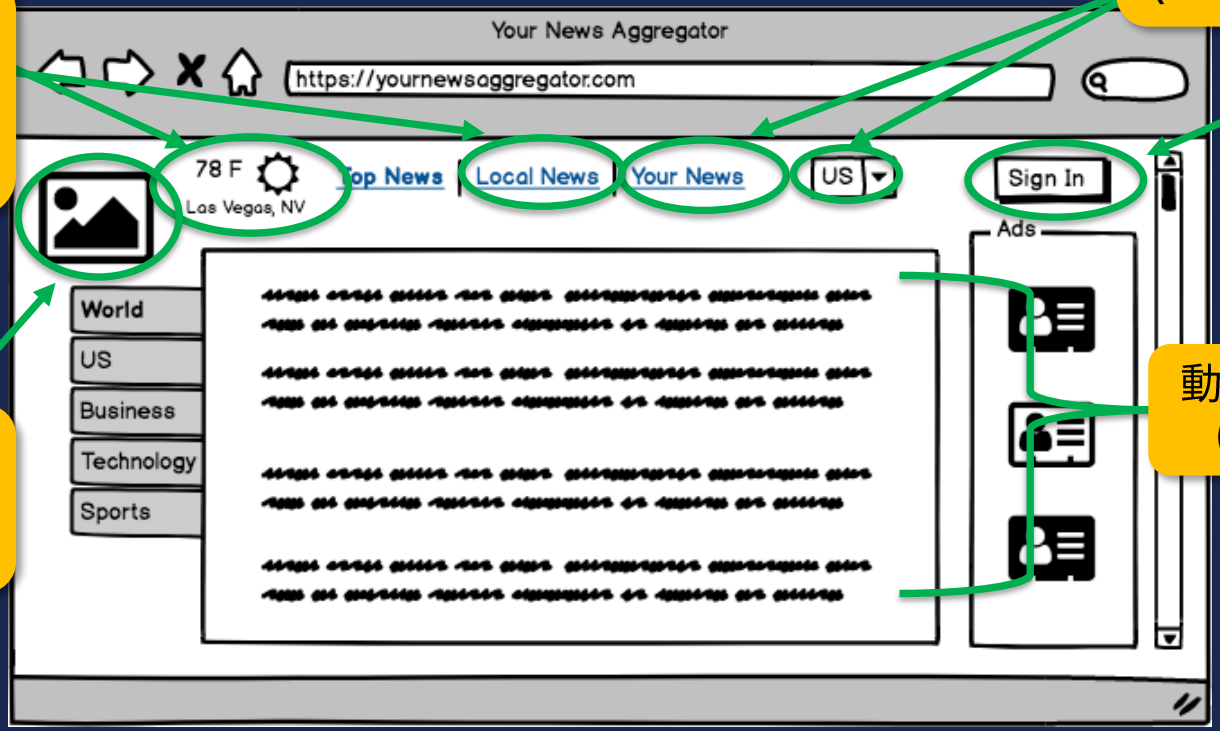
ユーザーエクスペリエンスの向上と
サイトアクセス時のパフォーマンスを両立



- キャッシュヒット率の向上
  - キャッシュコントロールヘッダの変更
  - クエリ文字列、ユーザーエージェントの正規化
  - ヘッダー / Cookie / クエリ文字列に基づき、複数のオリジンへ動的にルーティング
- コンテンツ生成
  - 画像リサイズ、HTMLページ生成
  - A/B テスト
- セキュリティ
  - JWT/MD5/SHA トークンハッシュを使用した認証
  - HSTS/CSP セキュリティヘッダ付与

Lambda@Edge のユースケース

コンテンツ生成や処理をエッジで実行



カスタマイズされた動的コンテンツ(ロケーション)

静的コンテンツ(images,HTML, JS,CSS,…)

動的なユーザーコンテンツ(パーソナライズ)

認証

動的コンテンツ(News feed)

aws SUMMIT

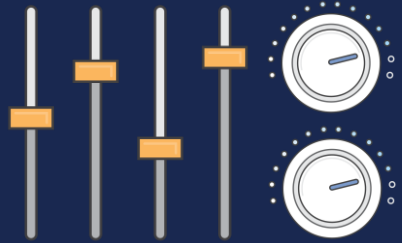
AWS WAF
Web Application Firewall

AWS WAF とは？

お客様の要望に応じて AWS が実現したマネージド WAF サービス

実践的な
セキュリティモデルを
簡単に導入

ルールを
フレキシブルに
カスタマイズできる



DevOps との統合

それらを AWS の「使っただけ」の支払い

なぜ WAF を使うのか

ファイアウォールや IPS/IDS で保護できないアプリへの攻撃や
難読化された攻撃から保護するために WAF を利用

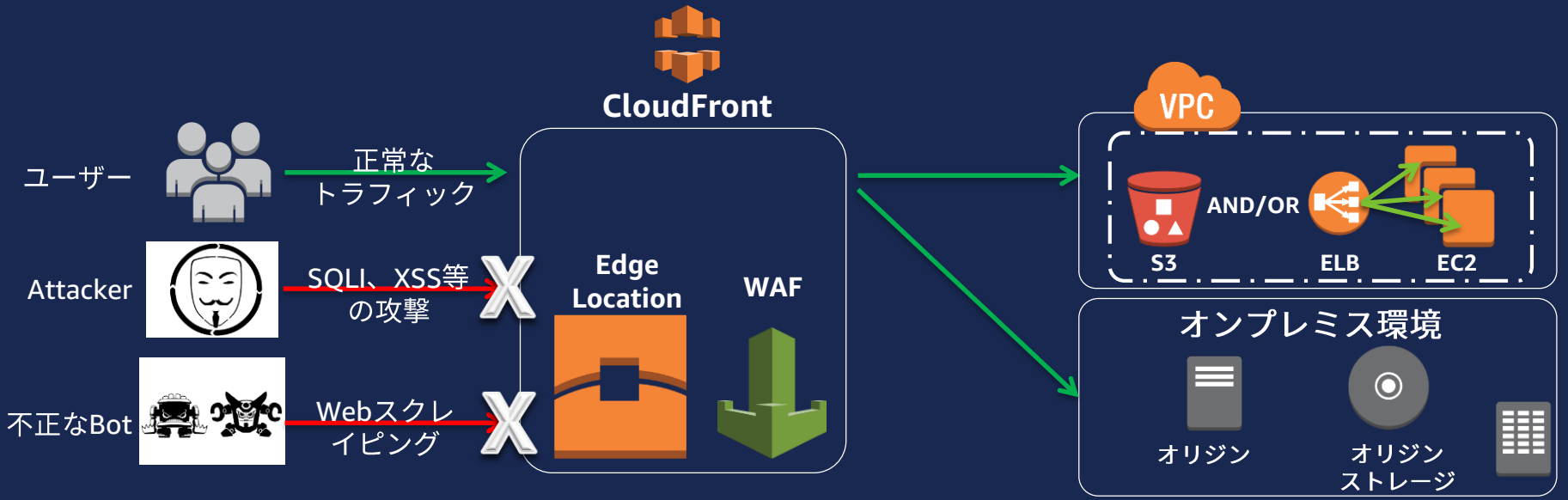
- WAF は、Web サイトやアプリケーションが、攻撃されてダウンしたりデータが流出したりすることがないように手助けをする
- WAF の一般的なユースケース
  - SQL インジェクション(SQLI)、クロスサイトスクリプティング (XSS) 対策
  - Web クローラ、スクレイピング等の BOT 対策
  - DDoS 緩和 (HTTP/HTTPS floods)
- PCI DSS 対応
  - PCI DSS のアプリケーション防護策の要件を満たす手法となっていることも、WAF が広く使われる理由の1つ

CloudFront with AWS WAF

不正なトラフィックはエッジロケーションにある WAF でブロック

サーバー管理やスケール対応は不要で WAF 機能のみ利用

- AWS 外のリソースでも OK
- 動的なコンテンツでも静的なコンテンツでも OK

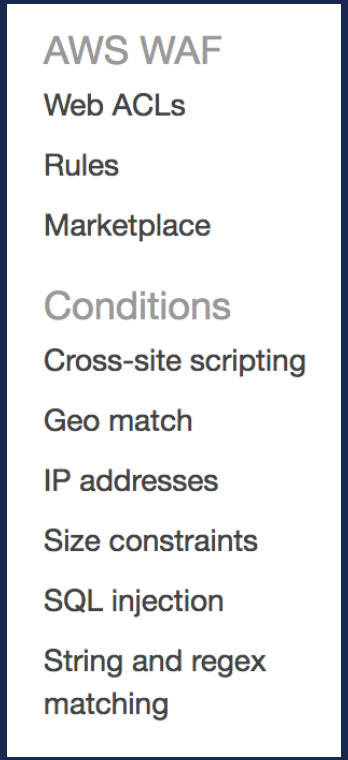


リクエストの判定条件

AWS WAF は複数の条件を組み合わせてリクエストの許可／拒否を判定

AWS WAF のリクエスト判定条件

- **クロスサイトスクリプティング**
  クロスサイトスクリプティング攻撃のチェック
- **アクセス元の地域**
- **IP アドレス**
  送信元IPアドレス、アドレスレンジ
- **サイズ制限**
  リクエストのサイズ (ヘッダー毎のサイズ、リクエストボディ)
- **SQL インジェクション**
  不正な SQL ステートメントのチェック
- **文字列、正規表現マッチング**
  URI, クエリ文字列, ヘッダー、リクエストボディに含まれる文字列



AWS WAF のマネージドルール

事前設定されたルールを利用して ウェブアプリケーションを保護

- パートナーが管理するマネージドルールを利用することで、ウェブアプリや API の保護を即座に開始
- Alert Logic, F5 ネットワークス, Fortinet, Imperva, Trend Micro, Trustwave などセキュリティのエキスパートがルールを提供
- AWS Marketplace を通じて調達でき、従量制の料金で利用可能、長期契約の必要なし
- ルールの適用は AWS WAF のコンソールからも可能

aws SUMMIT

まとめ

まとめ

- CloudFront はユーザーへのレスポンスを改善し、オリジンの負荷を削減
- CloudFront は AWS WAF との組み合わせや、組み込みの DDoS 対策により、高いセキュリティを実現
- CloudFront は Lambda@Edge と組み合わせる事により **ユーザーエクスペリエンスを向上**させることができる
- **大容量の配信や大量アクセスがある**サイトでの活用が有用
- 小規模でも **WAF/DDoS 等のセキュリティ対策**が必要なサイトで有用

aws SUMMIT

Thank you!