AWS Black Belt Online Seminar

Amazon CloudFront 基礎編

鈴木　隆昭

Professional Services

2025/07

AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
  アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
  - > https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - > https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

ご感想は X (Twitter) へ！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

- 本資料では資料作成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。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (https://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
- 技術的な内容に関しましては、有料の AWS サポート窓口 へお問い合わせください
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口 へお問い合わせください (マネジメントコンソールへのログインが必要です)

自己紹介

鈴木　隆昭

アマゾンウェブサービスジャパン
プロフェッショナルサービス
アプリケーション開発コンサルタント

AWS サービスを組み合わせたワークロードのプロトタイピングや、
開発チームの内製化支援を行なっています。

好きな AWS サービス

Lambda@Edge, Amazon Aurora, AWS Certificate Manager

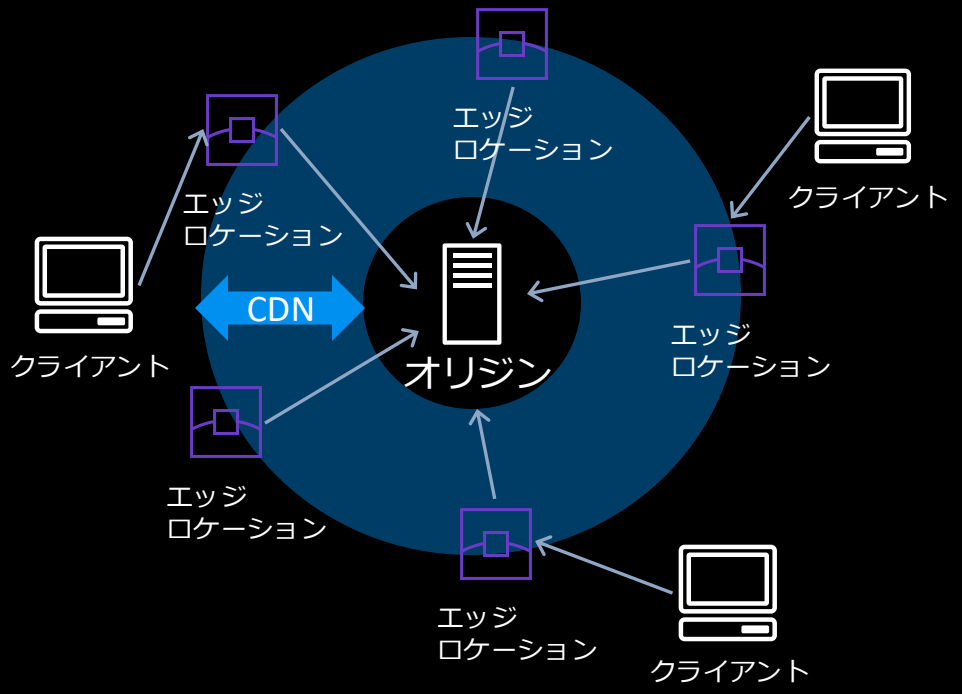
アジェンダ

1. Amazon CloudFront の概要
2. CloudFront の基本アーキテクチャ
3. CloudFront の設定の流れ
4. 主要機能についての補足
5. まとめ

Amazon CloudFront の概要

Content Delivery Network (CDN) とは

クライアントに地理的に近いエッジロケーションから、
速く・効率的にコンテンツ配信を行うネットワークを提供するサービス



グローバルに分散したエッジロケーション

- ✓ 広域な負荷分散
- ✓ 高可用なネットワークインフラストラクチャ
- ✓ 大容量の通信帯域、安定したネットワーク

＋

様々な付帯機能

キャッシュ：

- ✓ レスポンスタイムの削減
- ✓ オリジンの負荷軽減
- ✓ オリジンの保護

セキュリティサービスとの統合：

- ✓ DDoS 攻撃対策
- ✓ WAF

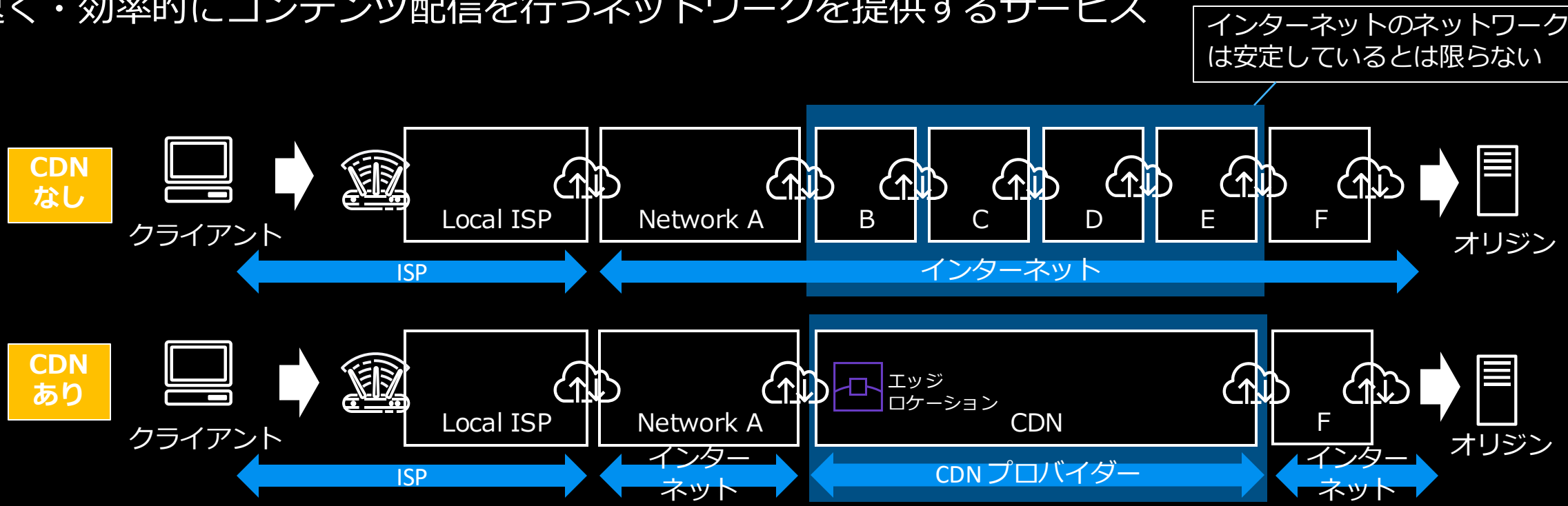
エッジコンピューティング：

- ✓ コンテンツの書き換え
- ✓ 認可処理

等

Content Delivery Network (CDN) とは

クライアントに地理的に近いエッジロケーションから、
速く・効率的にコンテンツ配信を行うネットワークを提供するサービス

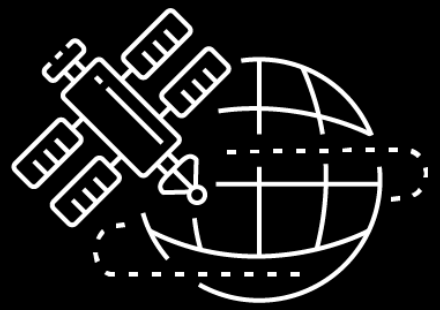


クライアント～オリジン間のネットワーク経路を、
CDN の最適化されたネットワーク経路に置き換え、
高速・安定した通信を実現する

Amazon CloudFront

Fast, highly secure and programmable content delivery network (CDN)
高い安全性と性能を実現するプログラム可能なコンテンツデリバリーネットワーク

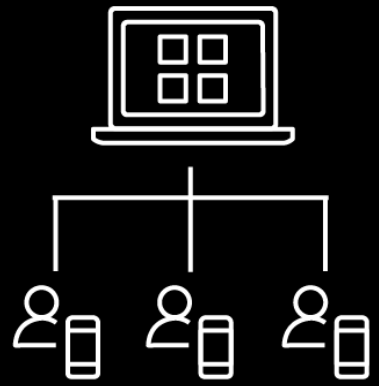
AWS のグローバル インフラストラクチャ



世界中から最適な経路での
高速・安定したアクセス

- ✓ ネットワークレイテンシーの低減
- ✓ ネットワーク帯域幅の確保
- ✓ 高可用なインフラストラクチャ

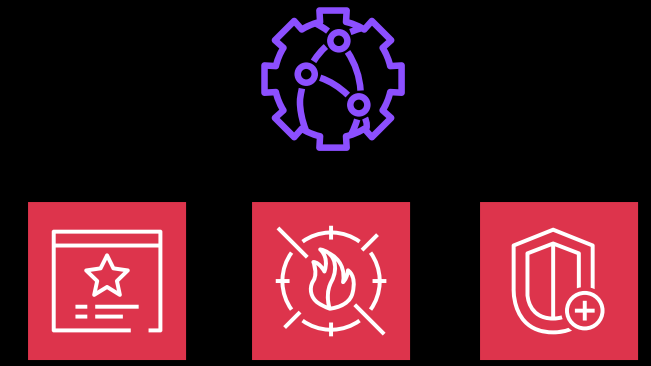
エッジロケーションを キャッシュサーバーとして活用



キャッシュされたコンテンツを
エッジロケーションから返却

- ✓ レスポンスタイムの低減
- ✓ サーバーのコンピュートリソースの節約
- ✓ ネットワークコストの節約

CloudFront の様々な機能や 他の AWS サービスとの連携



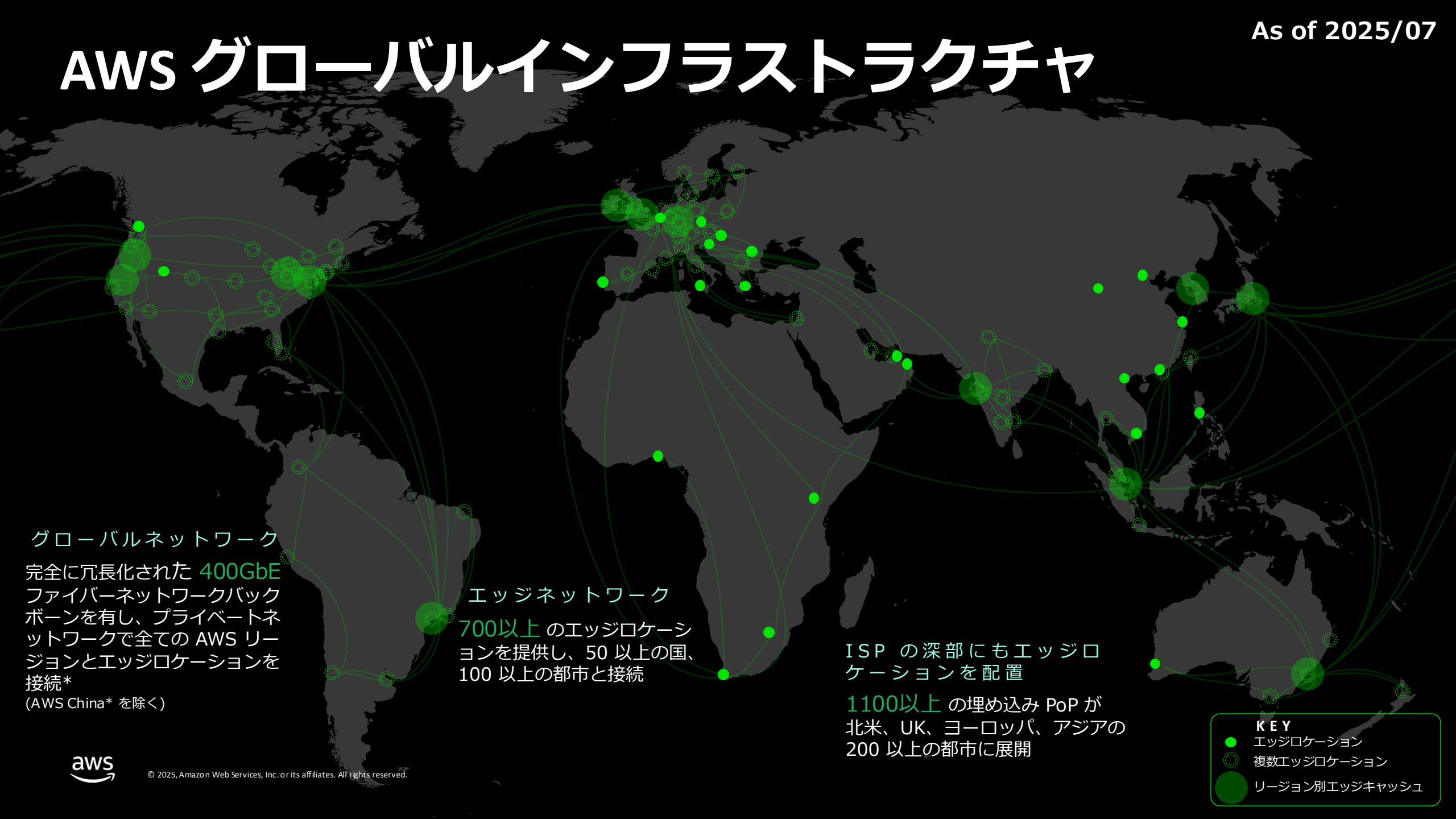
アプリケーションを変更をせず
動作をカスタマイズ

- ✓ エッジコンピューティング
- ✓ DDoS 攻撃対策、WAF
- ✓ SSL/TLS 終端　　等

CloudFront の基本アーキテクチャ

As of 2025/07

AWS グローバルインフラストラクチャ



グローバルネットワーク

完全に冗長化された 400GbE ファイバーネットワークバックボーンを有し、プライベートネットワークで全ての AWS リージョンとエッジロケーションを接続*
(AWS China* を除く)

エッジネットワーク

700以上 のエッジロケーションを提供し、50 以上の国、100 以上の都市と接続

ISP の深部にもエッジロケーションを配置

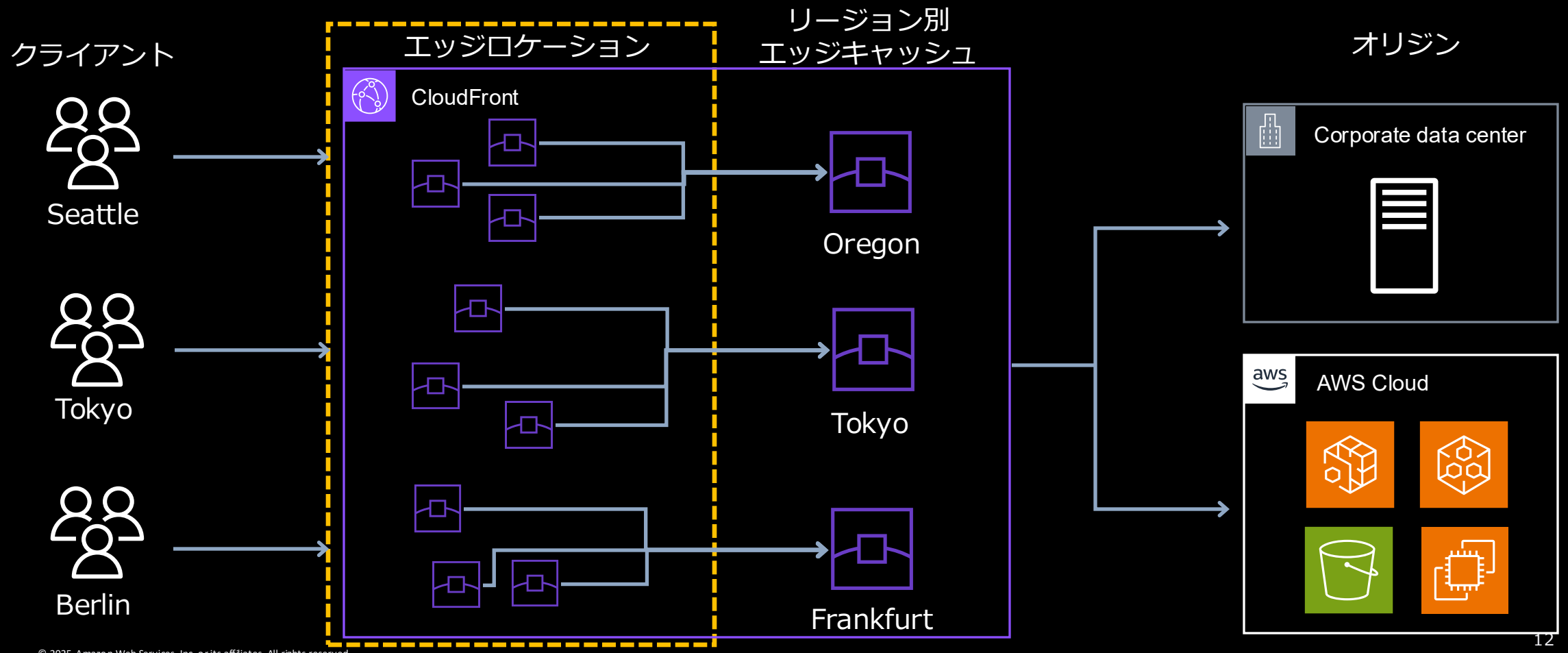
1100以上 の埋め込み PoP が北米、UK、ヨーロッパ、アジアの 200 以上の都市に展開

KEY
- エッジロケーション
- 複数エッジロケーション
- リージョン別エッジキャッシュ

aws

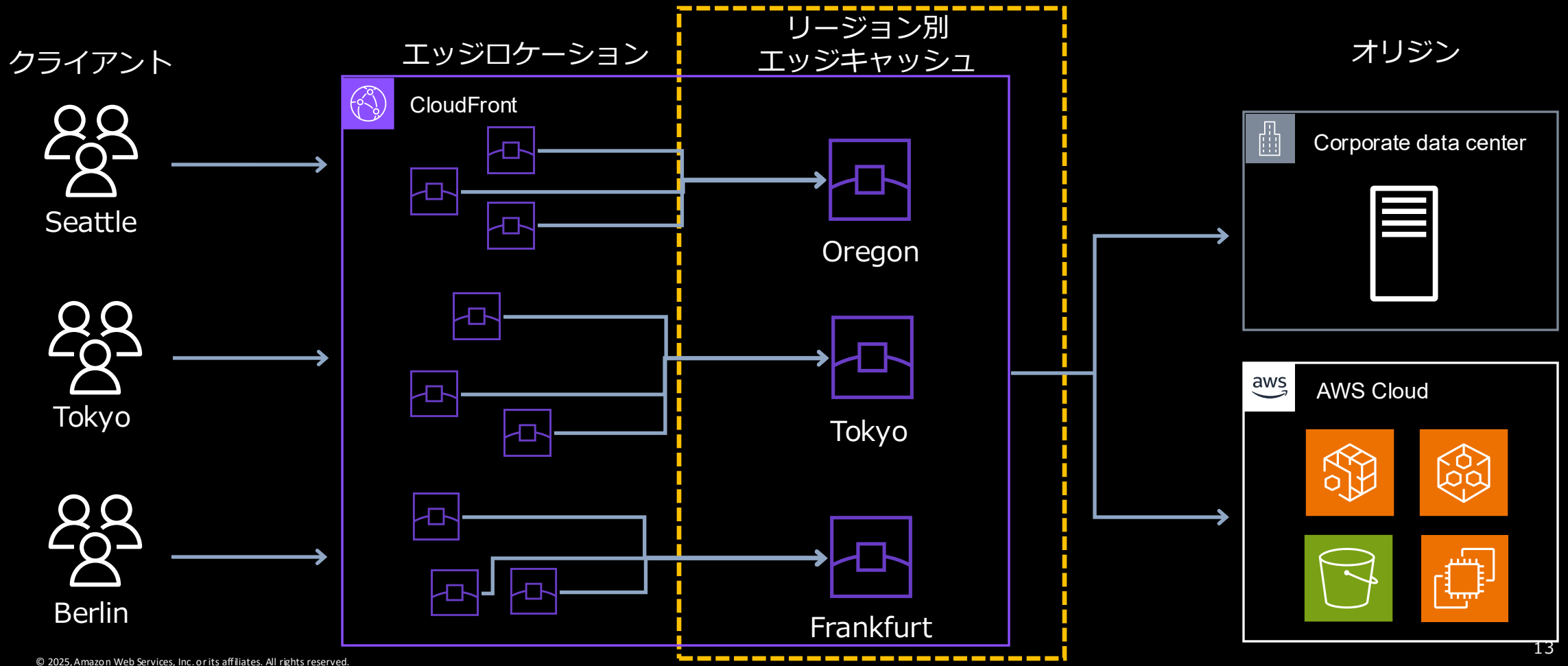
エッジロケーション

- ✓ クライアントに最も近い場所からコンテンツを配信
- ✓ 各エッジロケーションはキャッシュサーバーとして機能
- ✓ エッジロケーション以降のリクエストの低レイテンシー化を実現



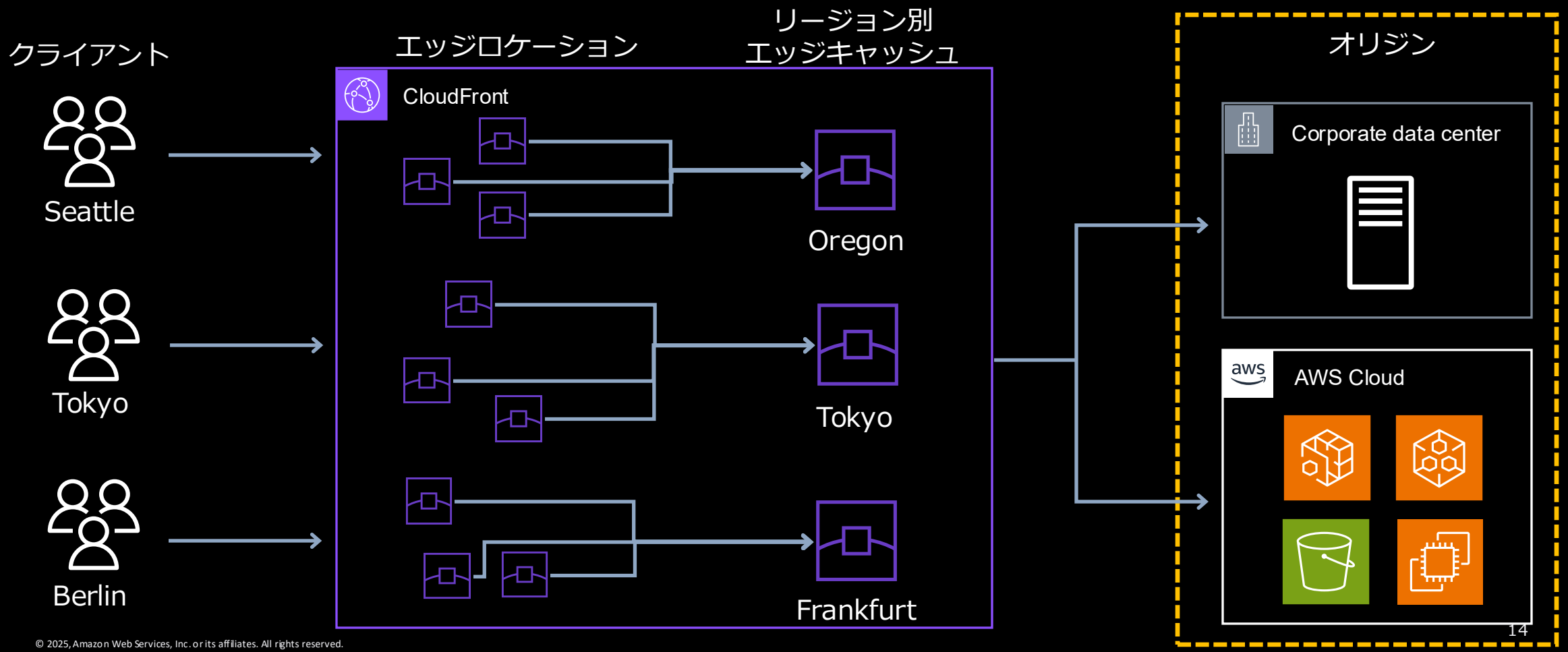
リージョン別エッジキャッシュ（REC）

- ✓ エッジロケーションとオリジン間に配置されるキャッシュ
- ✓ キャッシュ設定を無効化した場合、REC は使用されない
- ✓ 一部の HTTP メソッドはエッジロケーションから直接オリジンへ転送される



オリジン

- ✓ オリジナルのコンテンツを保持するソース
- ✓ CloudFront のキャッシュにヒットしなかった時にオリジンへのアクセスが発生
- ✓ オリジンは AWS リソースだけでなくオンプレミスサーバーも利用可能



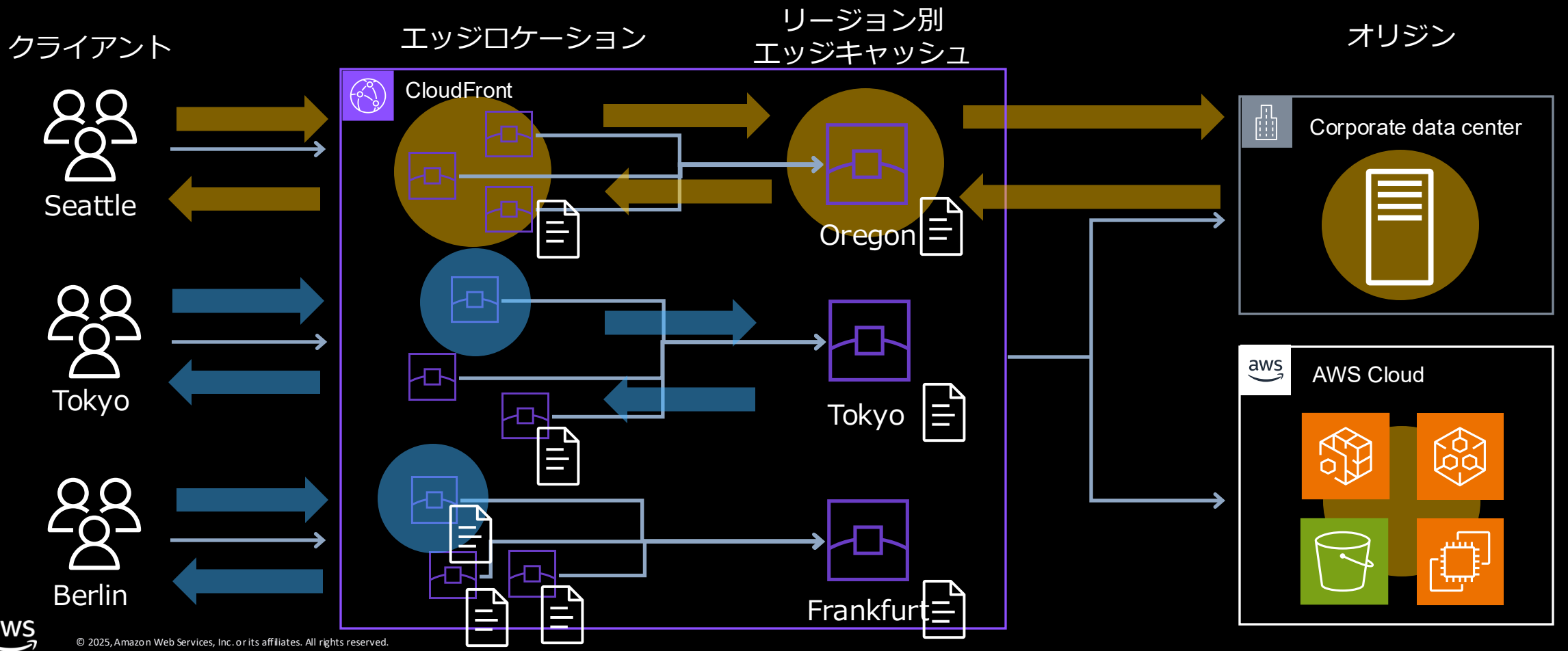
コンテンツ配信の仕組み

初回リクエスト時

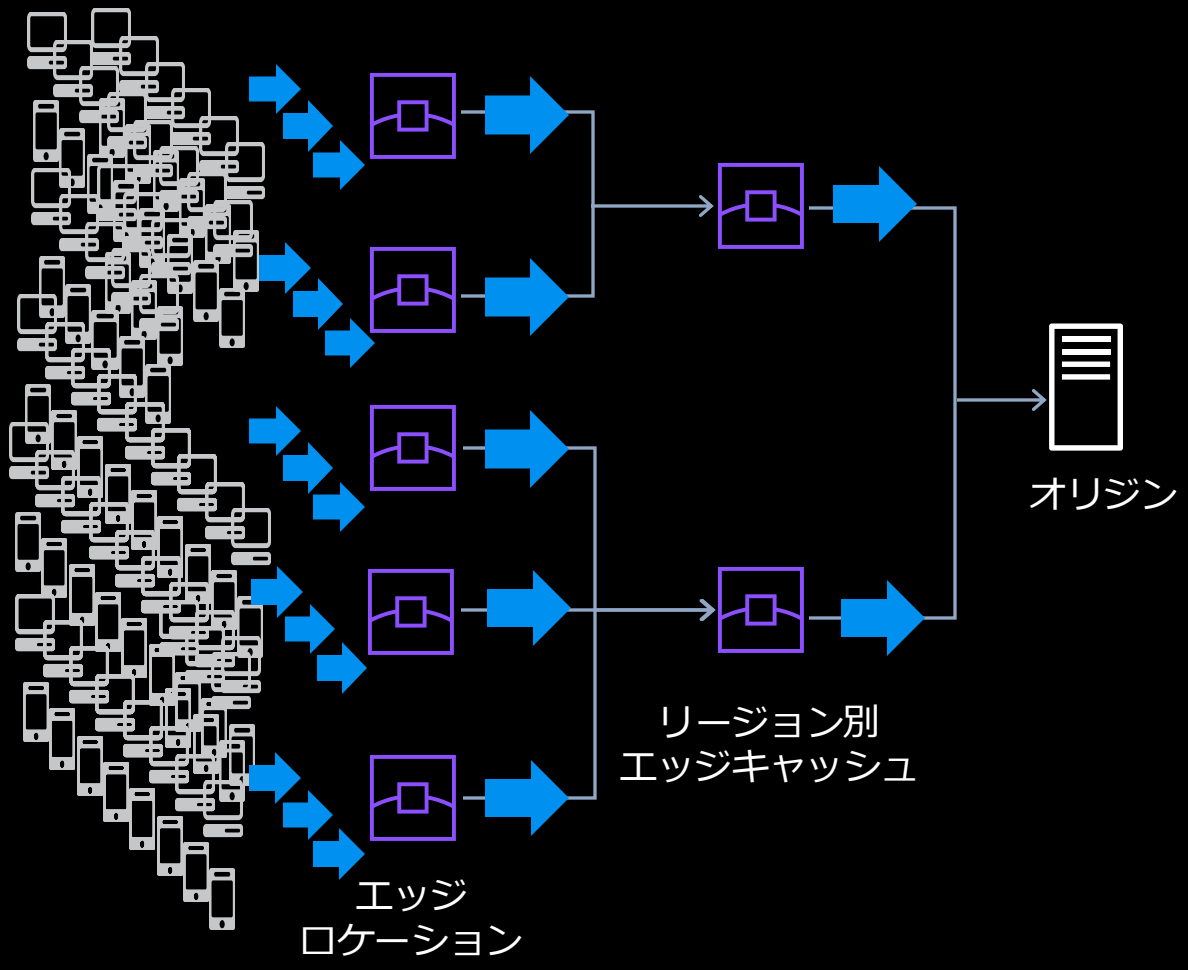
1. クライアントからのリクエストを最寄りのエッジロケーションが受信
2. エッジロケーションのキャッシュになければ、リージョン別エッジキャッシュを確認
3. リージョン別エッジキャッシュになければオリジンからコンテンツを取得
4. 取得したコンテンツをキャッシュしつつ、クライアントにレスポンス

2回目以降リクエスト時

1. クライアントからのリクエストを最寄りのエッジロケーションが受信
2. エッジロケーションのキャッシュからコンテンツを返却
   （なければリージョン別エッジキャッシュからコンテンツを返却）



"フラッシュクラウド" からのオリジンの保護



- 同時に大量リクエストが発生（フラッシュクラウド/Flash Crowd）した場合、最初のリクエストのみをオリジンに送り、負荷低減を実現する仕組み
- オリジンが AWS 上にある場合は AWS グローバルネットワークを使用
- AWS 以外のオリジンに対しても同様の機能を提供

CloudFront の設定の流れ

CloudFront：用語集

- **ビューワー**: ユーザー / クライアント / Web ブラウザ
- **ディストリビューション**: コンテンツ配信の設定単位
  CloudFront ドメイン名、代替ドメイン名毎に作成
  - **ビヘイビア**: 振る舞いの設定
    URL パスパターン毎に作成

    キャッシュ設定：
    キャッシュキー
    TTL
    コンテンツ圧縮

    リクエスト/レスポンス制御：
    ビューワー ～ CloudFront 間
    CloudFront ～ オリジン間

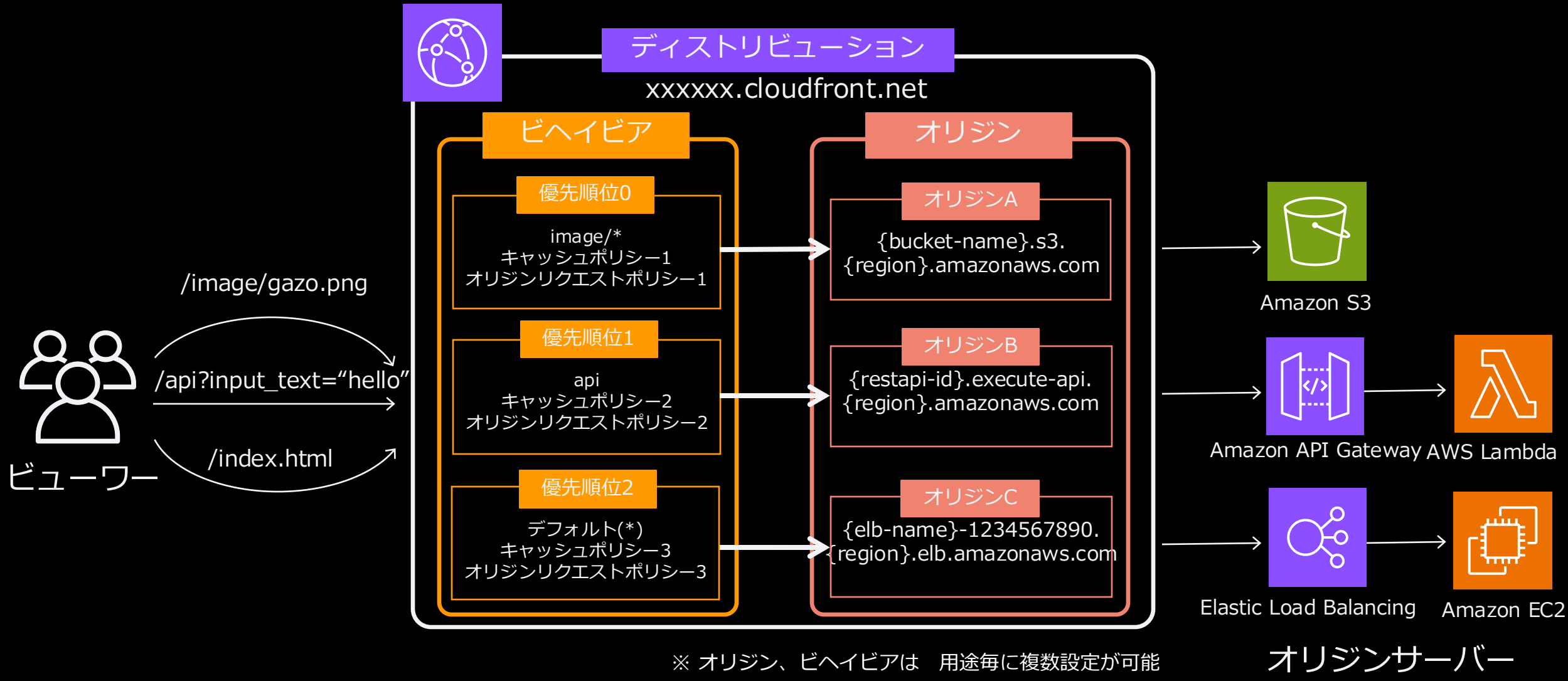
    エッジコンピューティングの関連づけ：
    CloudFront Functions
    Lambda@Edge

  - **オリジン**: コンテンツ提供元の設定
    コンテンツ提供元毎に作成

    カスタムオリジン:
    ALB、EC2 や Amazon API Gateway、
    Lambda 関数 URL、オンプレミスの Web サーバー 等

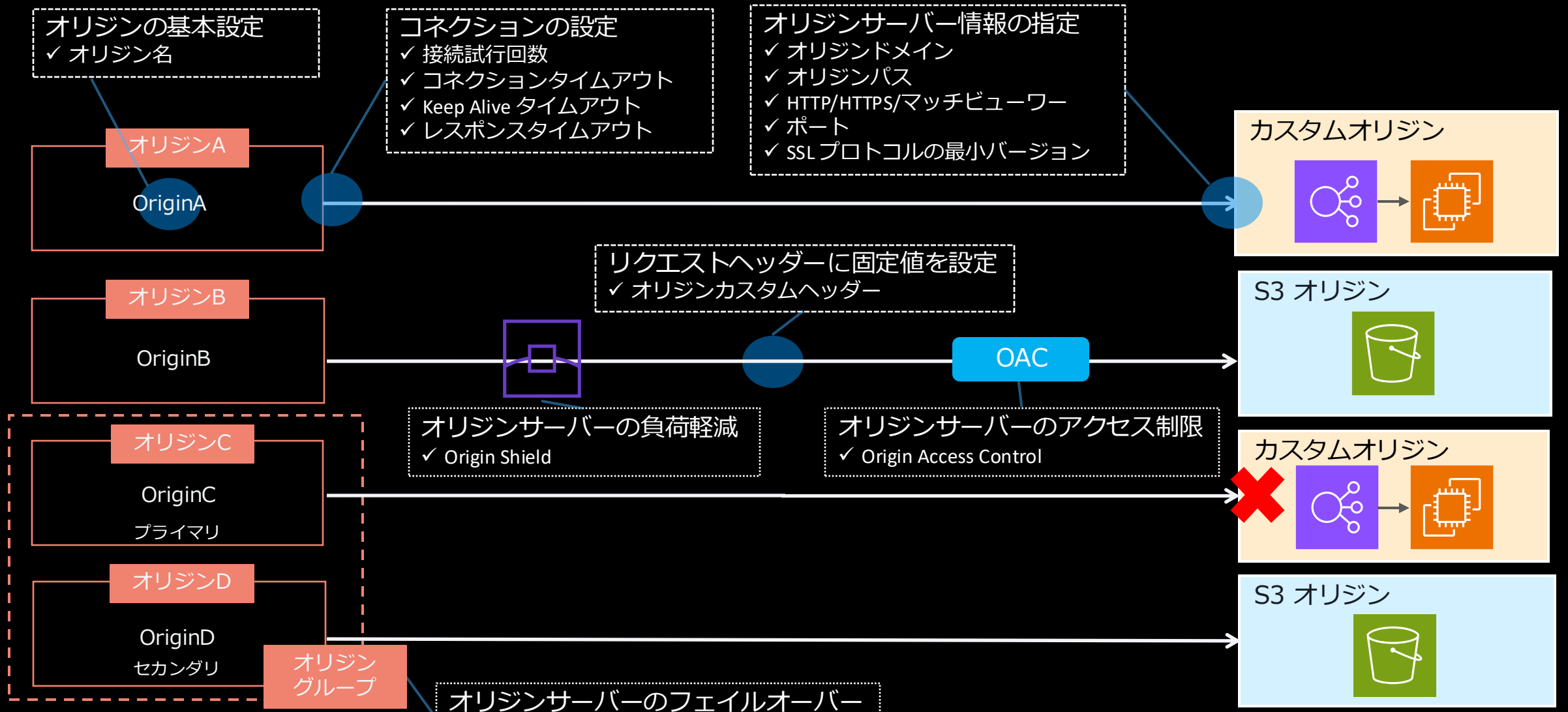
    S3 オリジン:
    静的コンテンツを提供する S3 バケット

CloudFront の構成要素イメージ



※ オリジン、ビヘイビアは　用途毎に複数設定が可能

オリジンの設定概要

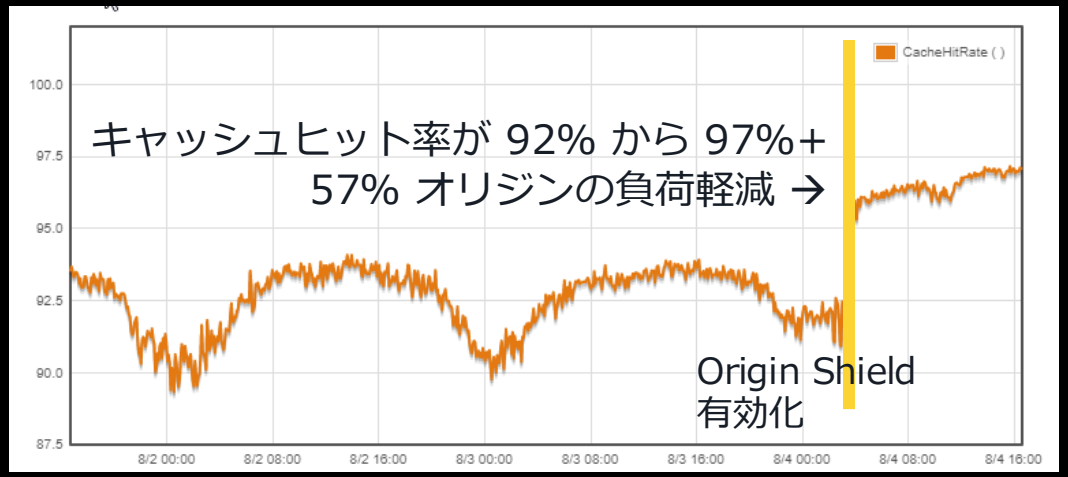


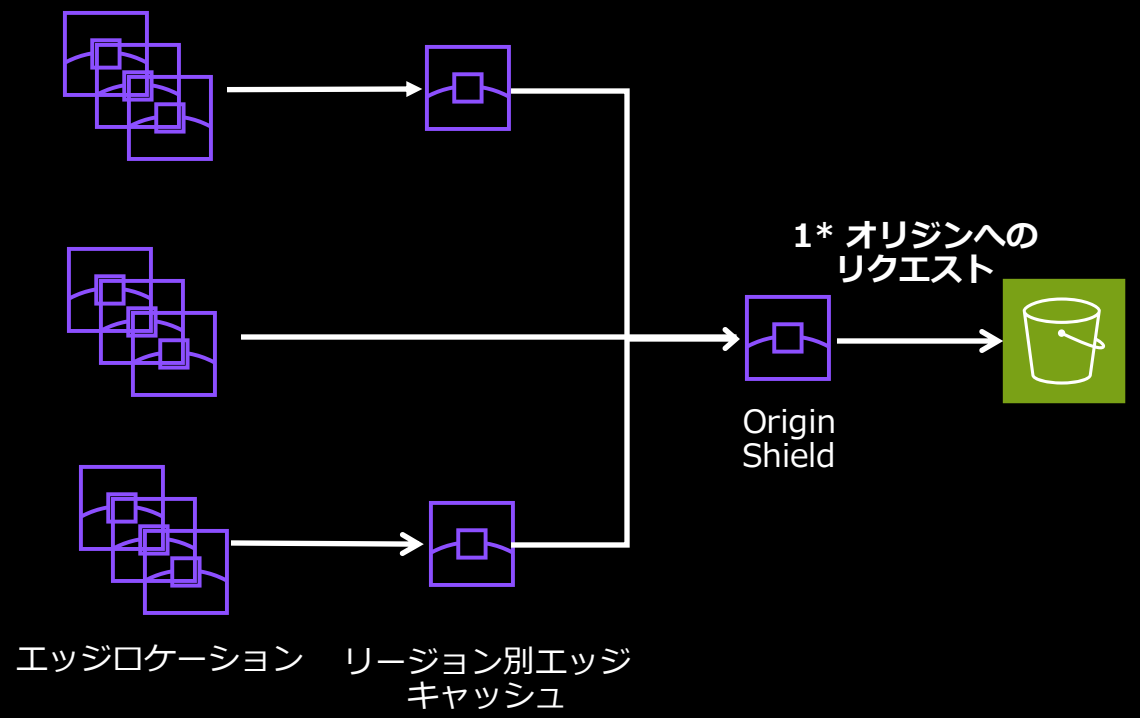
※ 接続先オリジンによって
指定不可な項目あり

Origin Shield による負荷軽減

オリジンに最も近いリージョン別エッジキャッシュにアクセス拠点を限定してオリジンへの負荷を最小限に

- リージョン間の重複したリクエストを集約
- キャッシュヒット率の向上
- オリジンのコスト最適化
  - リクエスト数削減
  - データ転送量削減



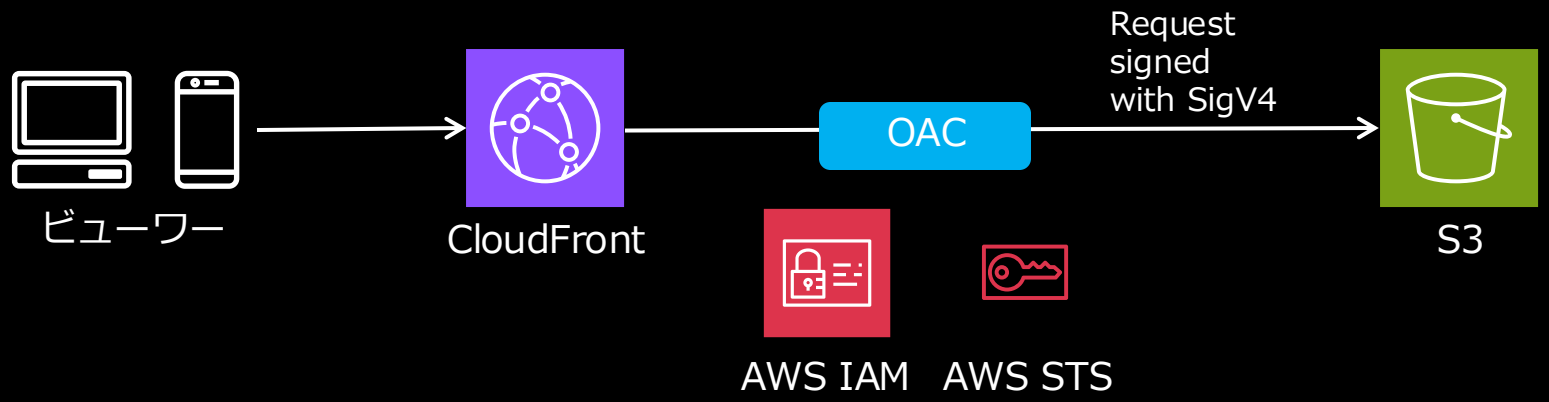


Amazon CloudFront Origin Shield の使用
https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/origin-shield.html

Origin Access Control (OAC)

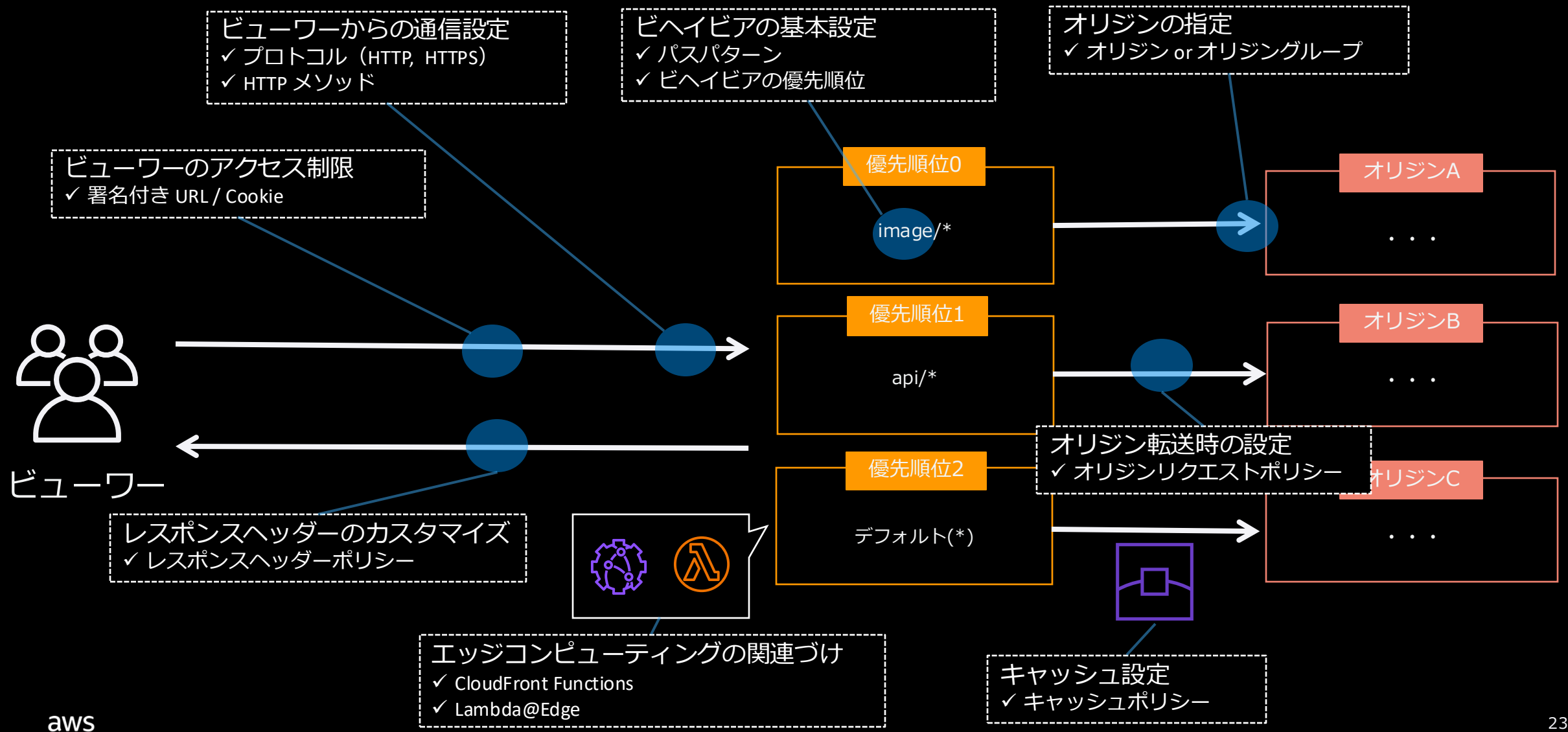
IAM Service Principal による一貫したアクセス制御

- 短期間のクレデンシャル、頻繁なクレデンシャルのローテーションおよびリソースベースのポリシーなど、強化されたセキュリティプラクティスを実装
- GET, HEAD, OPTIONS に加え、PUT, POST, PATCH, DELETE メソッドをサポート
- SSE-KMS で暗号化された S3 オブジェクトのダウンロード/アップロードをサポート
- Origin Access Identity (OAI) は 2022 年 12 月までに開始された既存の AWS リージョンでのみサポートされるため、OAC の利用を推奨



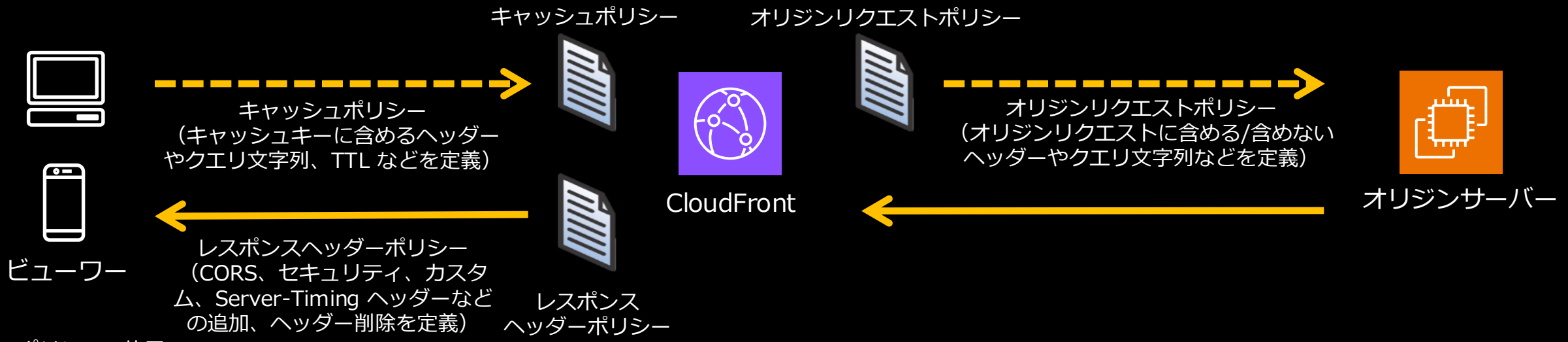
Amazon S3 オリジンへのアクセスの制限:
https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

ビヘイビアの設定概要

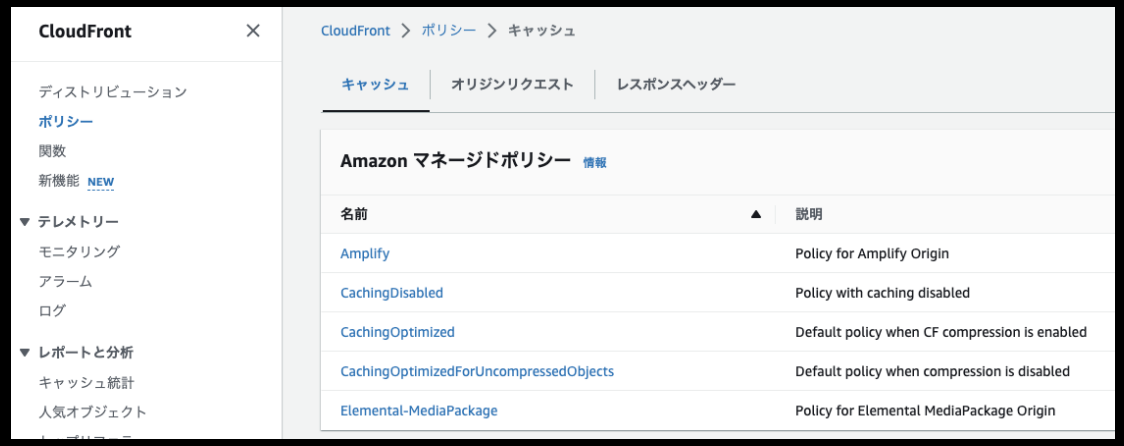


ポリシー（キャッシュ / オリジンリクエスト / レスポンスヘッダー）

定義済みのマネージドポリシー、再利用可能なカスタムポリシーを定義



ポリシーの使用:
https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/working-with-policies.html



- オリジンに転送するリクエストと
  キャッシュキーを分離して取り扱うことにより、
  柔軟なキャッシュ設定が可能
- レスポンスヘッダーのカスタマイズが可能

署名付き URL / Cookie

クライアントのコンテンツへのアクセス制限

- IAM アカウントで署名付き URL / Cookie のキー設定を行う
- 単一コンテンツアクセスの場合は署名付き URL、HLS 動画配信などの複数コンテンツアクセスの場合は、署名付き Cookie の利用を推奨

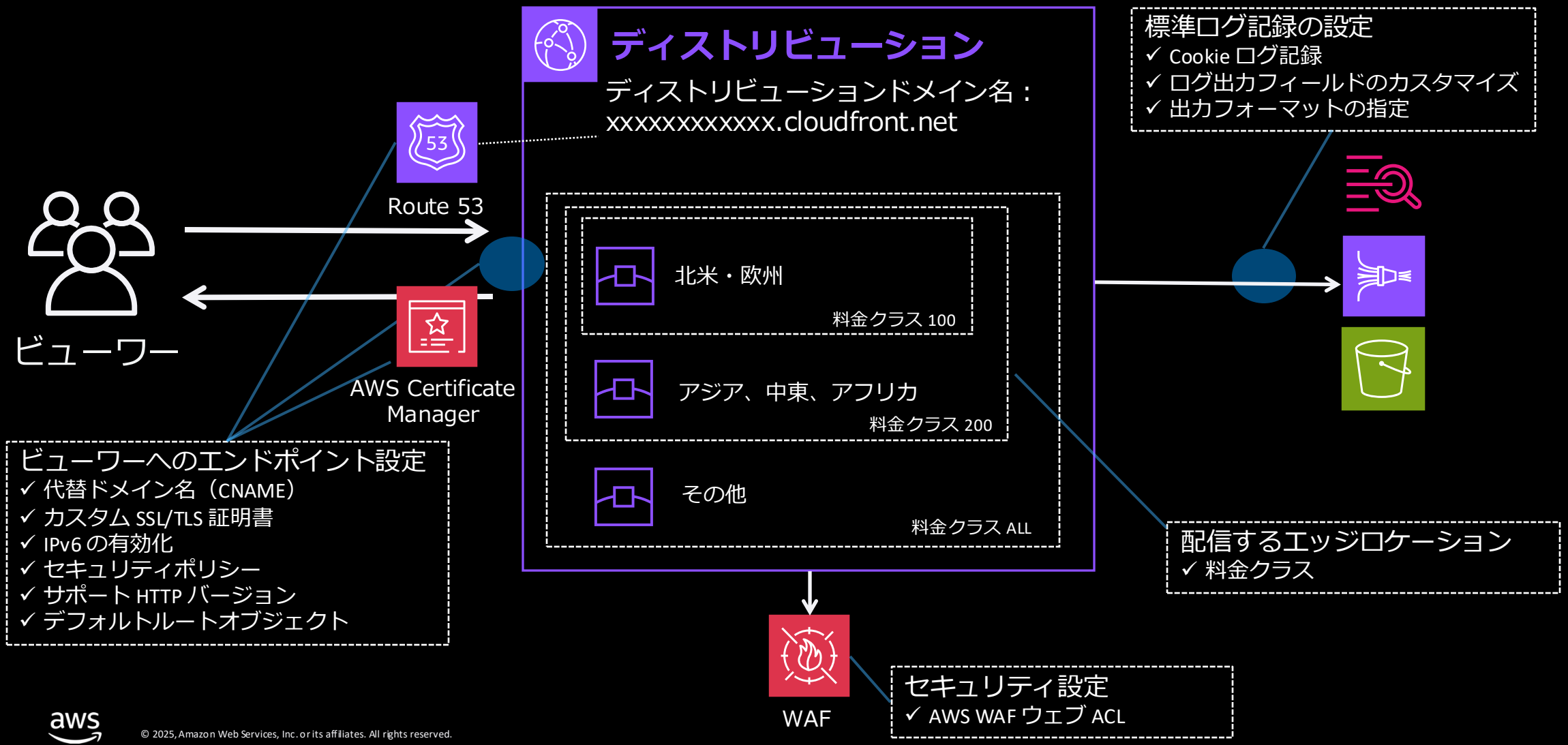
署名付き URL と署名付き Cookie を使用したプライベートコンテンツの提供
https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/PrivateContent.html

エッジコンピューティングの関連付け

ビューワーに近い場所で任意の処理を実行

- ビューワーに近いエッジロケーション/リージョン別エッジキャッシュで
  コードを実行するサービス
- HTTP(s) リクエストとレスポンスをトリガーする
- サーバーレスでインフラストラクチャの管理は不要
- トリガーに応じて自動でスケール
- 使った分だけの従量課金
- コンピューティングリソースをグローバルに利用可能

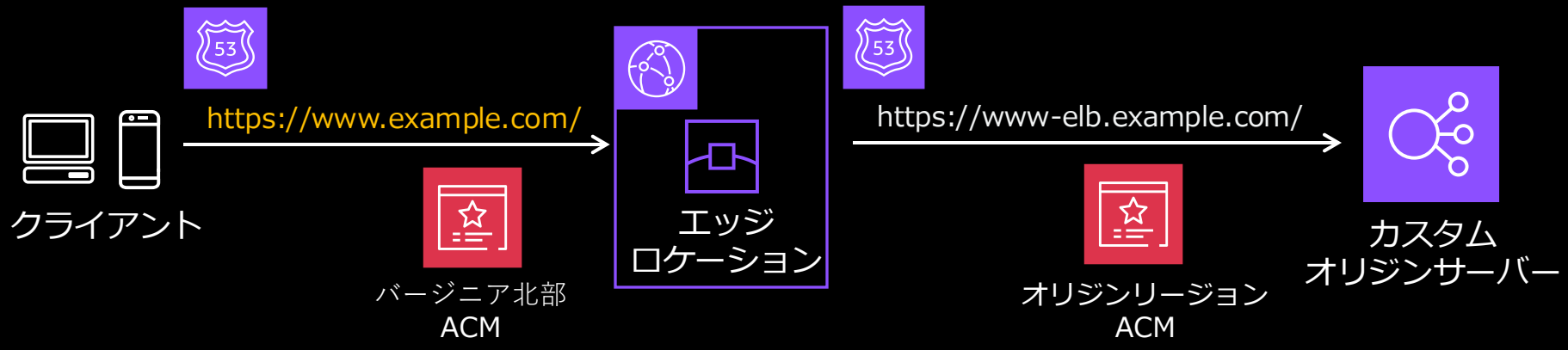
ディストリビューションの設定概要



代替ドメイン名、カスタム SSL/TLS 証明書の設定

独自のドメインでセキュアにコンテンツを配信

- クライアントからの SSL/TLS 接続はエッジロケーションで終端
- 代替ドメイン名 (CNAME) の追加には、ドメイン名を含む有効なカスタム SSL/TLS 証明書を設定する
  - > CloudFront は AWS Certificate Manager (ACM) と統合されており、無償のドメイン認証（DV）タイプ証明書を数分で発行、自動更新も可能
  - > ワイルドカード指定 (例: *.example.com) や、Route53 エイリアスレコードと組み合わせた Zone Apex (例: example.com) をサポート



As of 2025/07

サポート HTTP バージョン、セキュリティポリシー

CloudFront への接続要件を指定

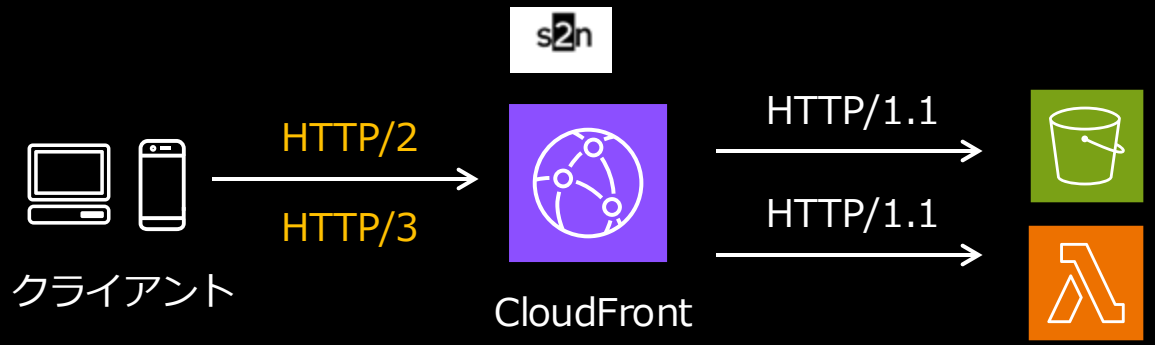
サポート HTTP バージョン

- TLS 1.3 クライアント接続をデフォルトサポート
- HTTP/1.0, HTTP/1.1, WebSocket プロトコルをデフォルトサポート
- HTTP/2, HTTP/3 の追加サポートが可能

セキュリティポリシー

- 最低限の SSL/TLS プロトコルと暗号の組み合わせ

✓ TLSv1.2_2021
✓ TLSv1.2_2019
✓ TLSv1.2_2018
✓ TLSv1.1_2016
✓ TLSv1_2016
✓ TLSv1
✓ SSLv3 (非推奨)

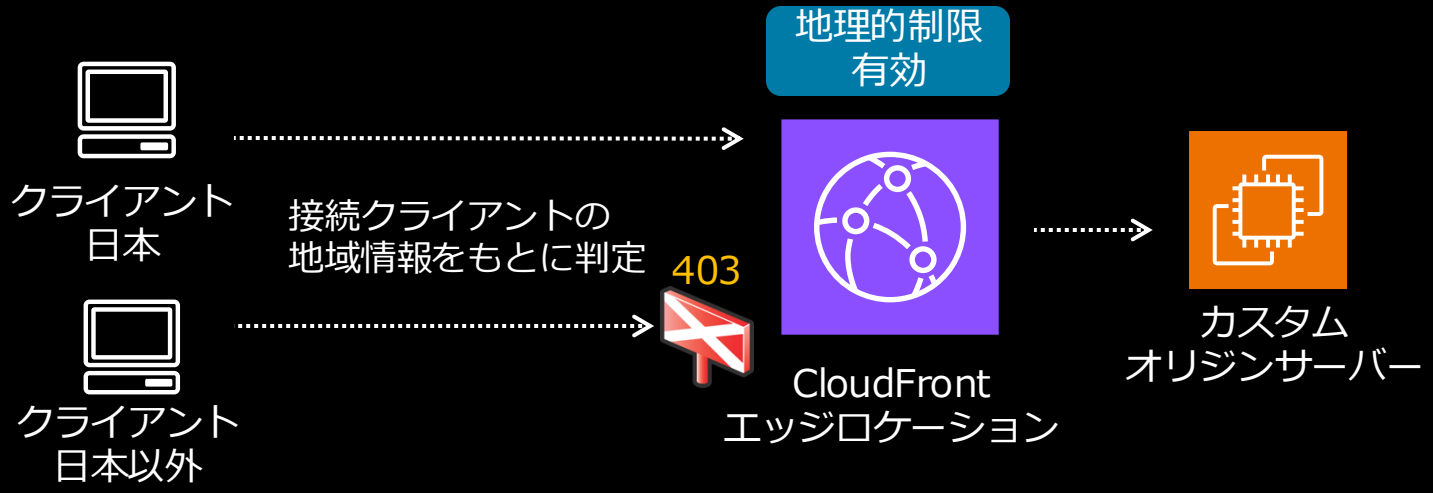


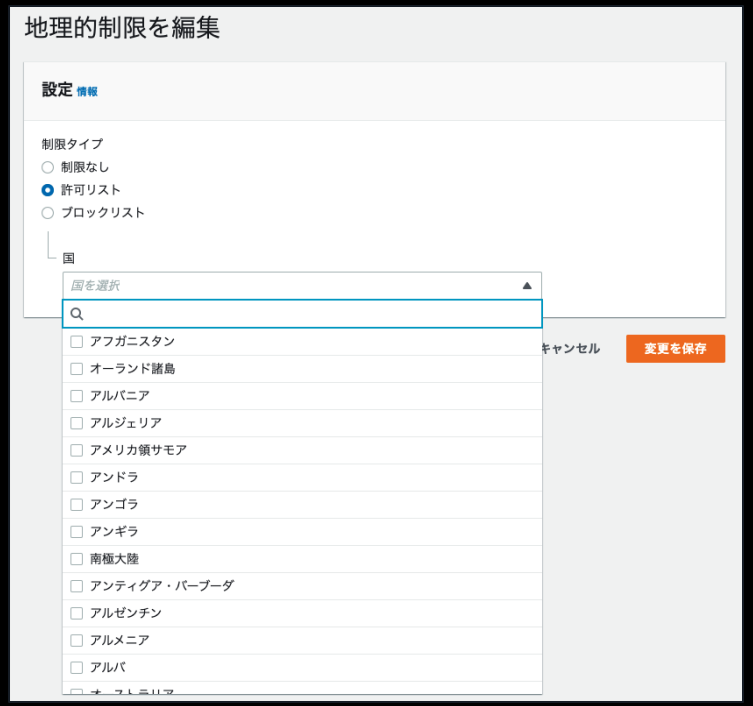
主要機能についての補足

地理的 (GEO) 制限

特定の国のユーザーに対するアクセス制御

- クライアント IP アドレスの地域情報を元に、エッジロケーションでアクセス判定
- 許可リストまたはブロックリストで指定可能
- ディストリビューション全体に適用される
- 制限されたアクセスには 403 を応答



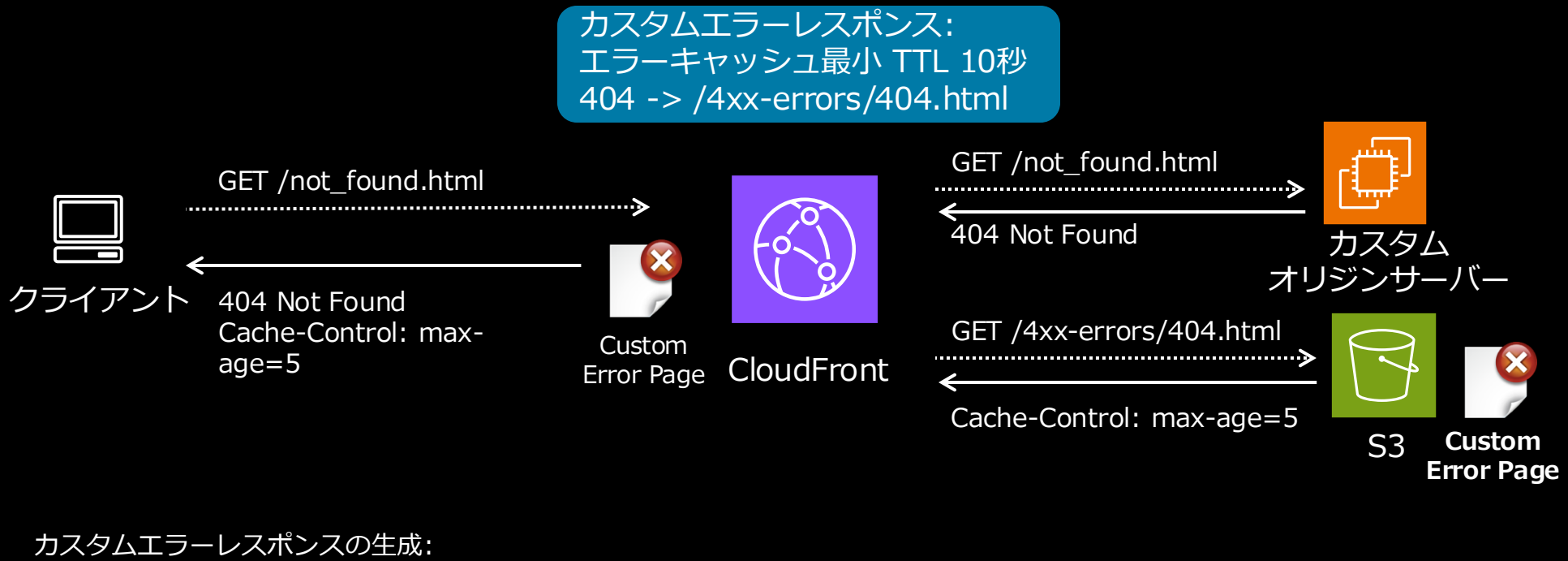


コンテンツの地理的ディストリビューションの制限
https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html

カスタムエラーレスポンス

オリジンサーバーのエラー受信時にレスポンスをカスタマイズ

- CloudFront は、エラーレスポンスをデフォルト 10 秒キャッシュ
- 4xx および 5xx ステータスコードそれぞれに対して、エラーレスポンスおよびレスポンスステータスコードのカスタマイズが可能



カスタムエラーレスポンスの生成:
https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/GeneratingCustomErrorResponses.html

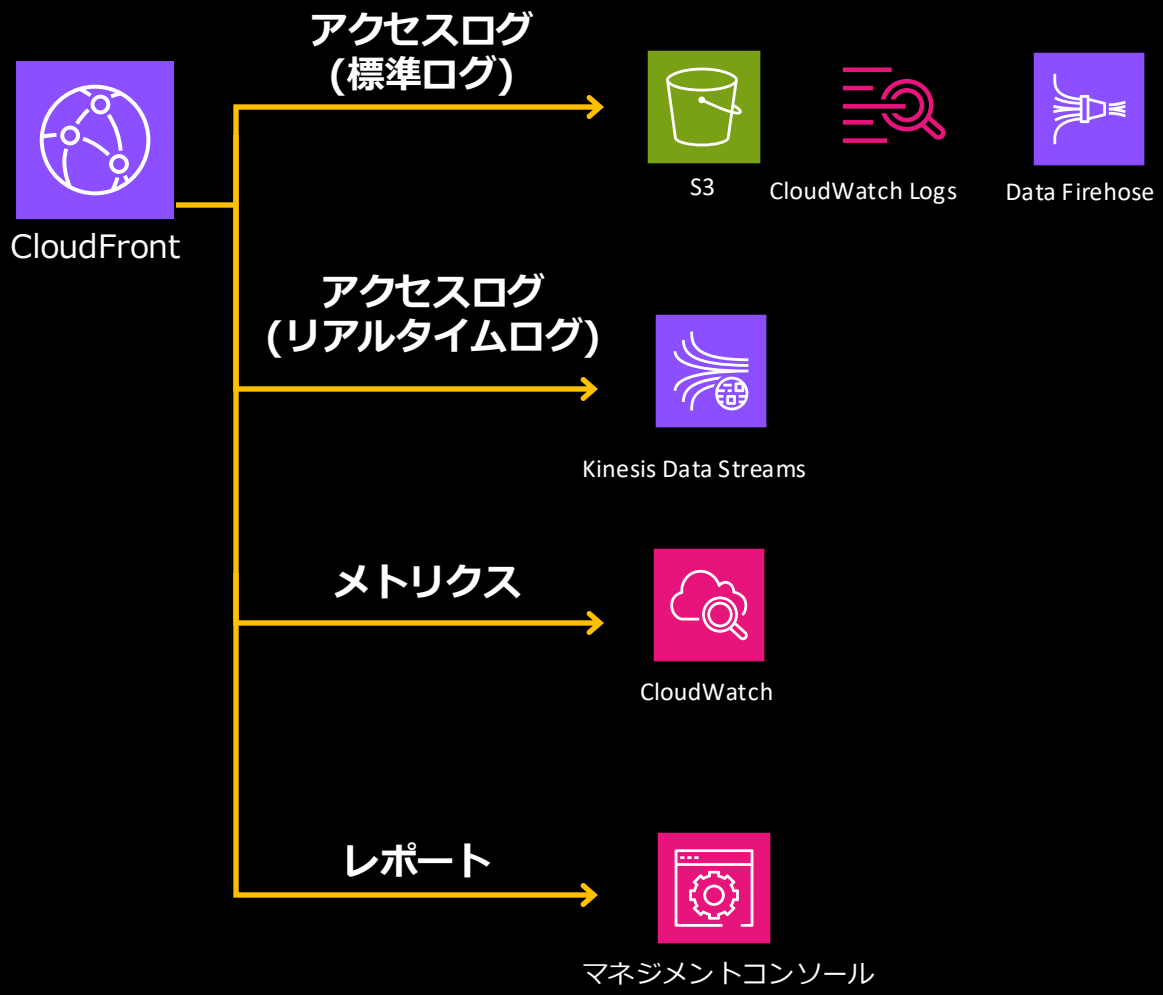
キャッシュファイルの無効化（Invalidation）

CloudFront のキャッシュをパス単位でパージ

- コンテンツ毎の無効化パス指定
  - 同時に最大 3,000 個までのパス指定が可能
- ワイルドカードを利用した無効化パス指定
  - 同時に最大 15 個まで無効化パスリクエストが指定可能
  - オブジェクト数は制限無く、1 無効化パスとして計算
- 月間最初の 1,000 パスまでは追加料金無し, それ以降は、無効をリクエストしたパスごとに $0.005

ファイルの無効化:
https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/Invalidation.html

ログ / メトリクス / レポート



アクセスログ
- 複雑なアクセスや利用傾向分析
- データの可視化と詳細な障害分析

モニタリング / アラーム
- 障害/異常検知や現状の利用確認
- ダッシュボードでの可視化
  - ディストリビューションメトリクス
  - エッジコンピューティングのエラーメトリクス
- CloudWatch Internet Monitor との統合
- CloudFront コンソールでのアラーム設定

アクセスや利用状況傾向の確認及び分析
- キャッシュ統計
- 人気オブジェクト
- トップリファラ
- 使用状況
- ビューワー

CloudFront ログのクエリ:
https://docs.aws.amazon.com/ja_jp/athena/latest/ug/cloudfront-logs.html

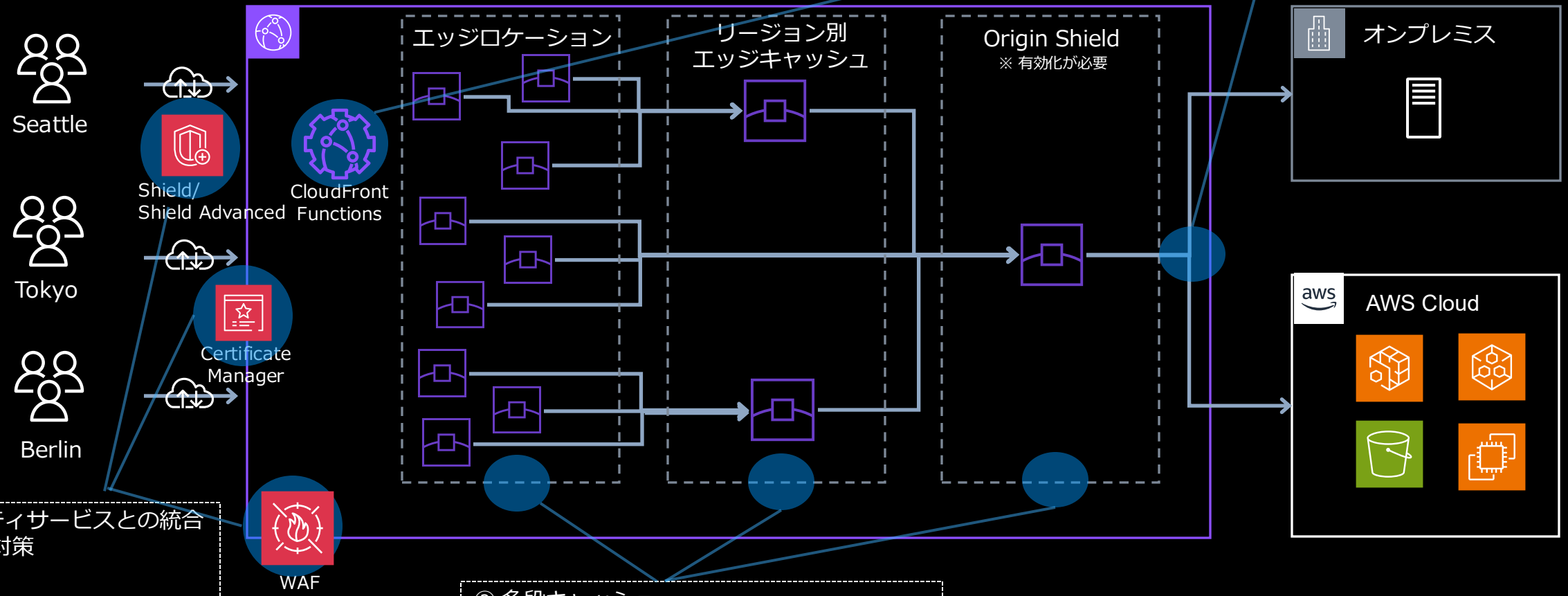
まとめ

CloudFront の特徴

① AWS グローバルネットワークの利用
- 高速かつ安定したネットワークでコンテンツ配信
- キャッシュしない動的コンテンツでも高速化が見込める

⑤エッジコンピューティングの利用
- CloudFront Functions
- Lambda@Edge

④オリジンへのアクセス制御
- OAC



③ セキュリティサービスとの統合
- DDoS 攻撃対策
- SSL 証明書
- WAF

② 多段キャッシュ
- レスポンスタイムの高速化
- オリジン負荷の低減
- フラッシュクラウドからのオリジン保護

CloudFront の設定

コンテンツ配信の設定単位
- 代替ドメインの設定
- セキュリティポリシー
- WAF, ACM の設定
- 標準ログ転送設定
- カスタムエラーレスポンス
- 地理的制限

ディストリビューション

ビヘイビア

優先順位0

image/*
キャッシュポリシー1
オリジンリクエストポリシー1

優先順位1

api
キャッシュポリシー2
オリジンリクエストポリシー2

オリジン

オリジンA

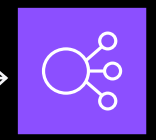
{bucket-name}.s3.
{region}.amazonaws.com

オリジンB

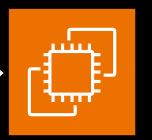
{restapi-id}.execute-api.
{region}.amazonaws.com

{elb-name}
{region}.elb.

Amazon S3



Elastic Load Balancing



Amazon EC2

ビューワー

/image/gazo.png

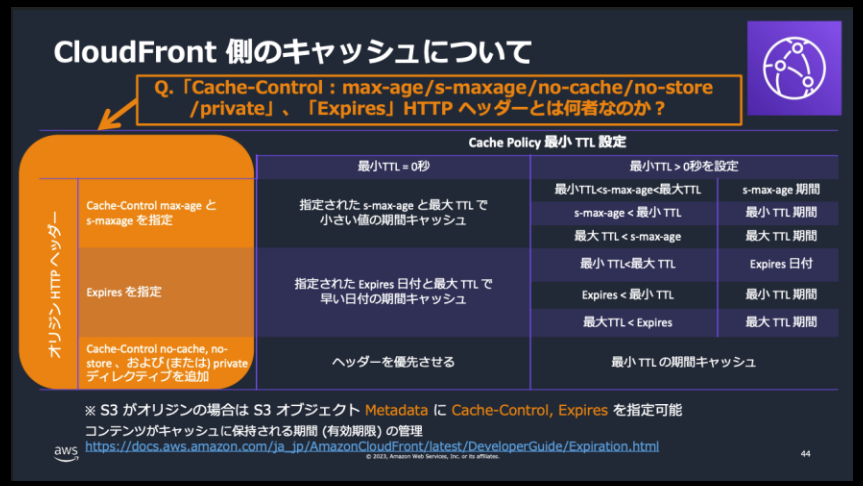
/api?input_text="hello"

/index.html

パスパターン毎にキャッシュ動作を指定
- 優先順位順の評価される
- プロトコルポリシー、許可されたHTTPメソッド
- キャッシュ / オリジンリクエスト / レスポンスヘッダーポリシー
- 署名付き URL / Cookie によるコンテンツのアクセス制限
- エッジコンピューティングの関連付け

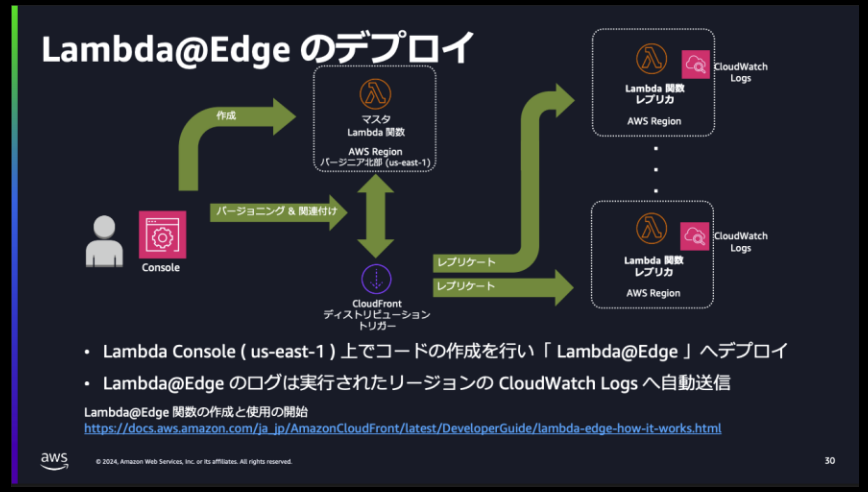
コンテンツ提供元のオリジンを設定
- オリジンプロトコルポリシー
- オリジンへのアクセス制御（OAC）
- Origin Shield によるオリジン負荷軽減
- レスポンス / KeepAlive タイムアウト
- オリジングループによるフェイルオーバー

CloudFront のテーマ別 Blackbelt の紹介



Cache Control 編

レポート / モニタリング / ロギング 編



Edge Computing 編

AWS サービス別資料

Thank you!