



AWS
Black Belt
Online Seminar

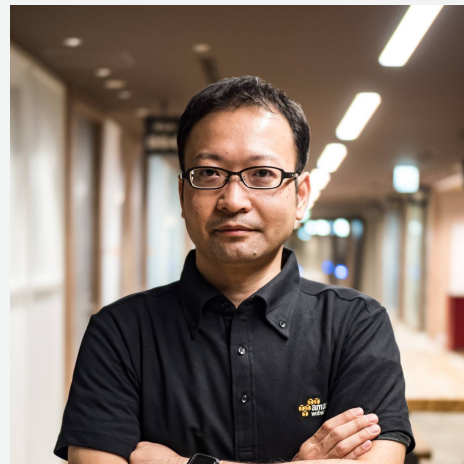
Amazon CloudFront AWS Lambda@Edge

アマゾン ウェブ サービス ジャパン株式会社
ソリューション アーキテクト 藤原 吉規
2017.09.27 (2017.10.03 Updated)

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: **AWS サポート**

内容についての注意点

- 本資料では2017年9月27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が東京リージョンを使用する場合、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.

Agenda

- Amazon CloudFront
 - Contents Delivery Network
 - 高速配信機能
 - セキュリティ機能
 - レポート & ロギング
- AWS Lambda@Edge
- まとめ



Amazon CloudFront



Contents Delivery Network



Contents Delivery Network

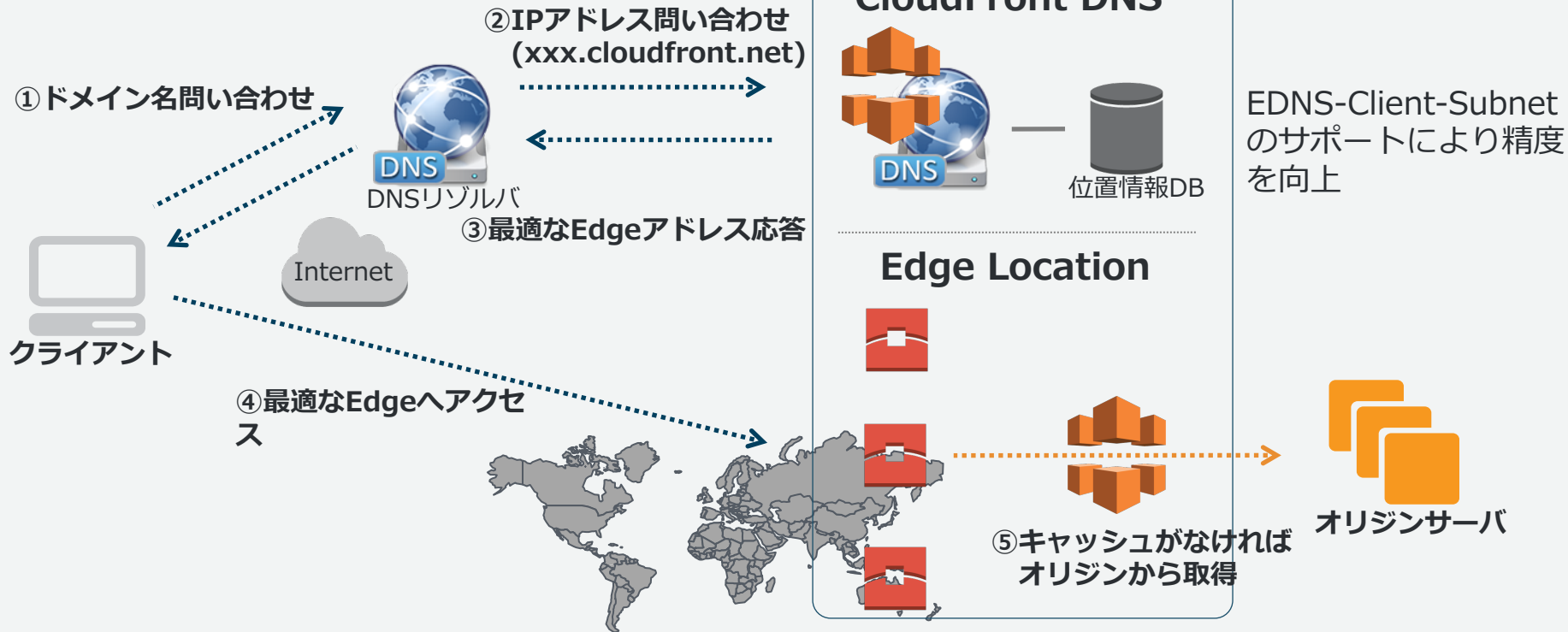
大規模なアクセスも世界中にあるエッジのキャパシティを活用して効率的かつ高速にコンテンツ配信が可能なサービス

- ユーザからのアクセスを最も近いエッジサーバに誘導することで**ユーザへの配信を高速化**
- エッジサーバでは、コンテンツのキャッシングを行い、**オリジンに負荷をかけず効率的に配信**



Contents Delivery Network

最適なエッジへの誘導



CloudFront の特徴



高性能な分散配信 (世界 84 拠点のエッジサーバ)

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かつスポットも利用可能)

サイトまるごと CloudFront

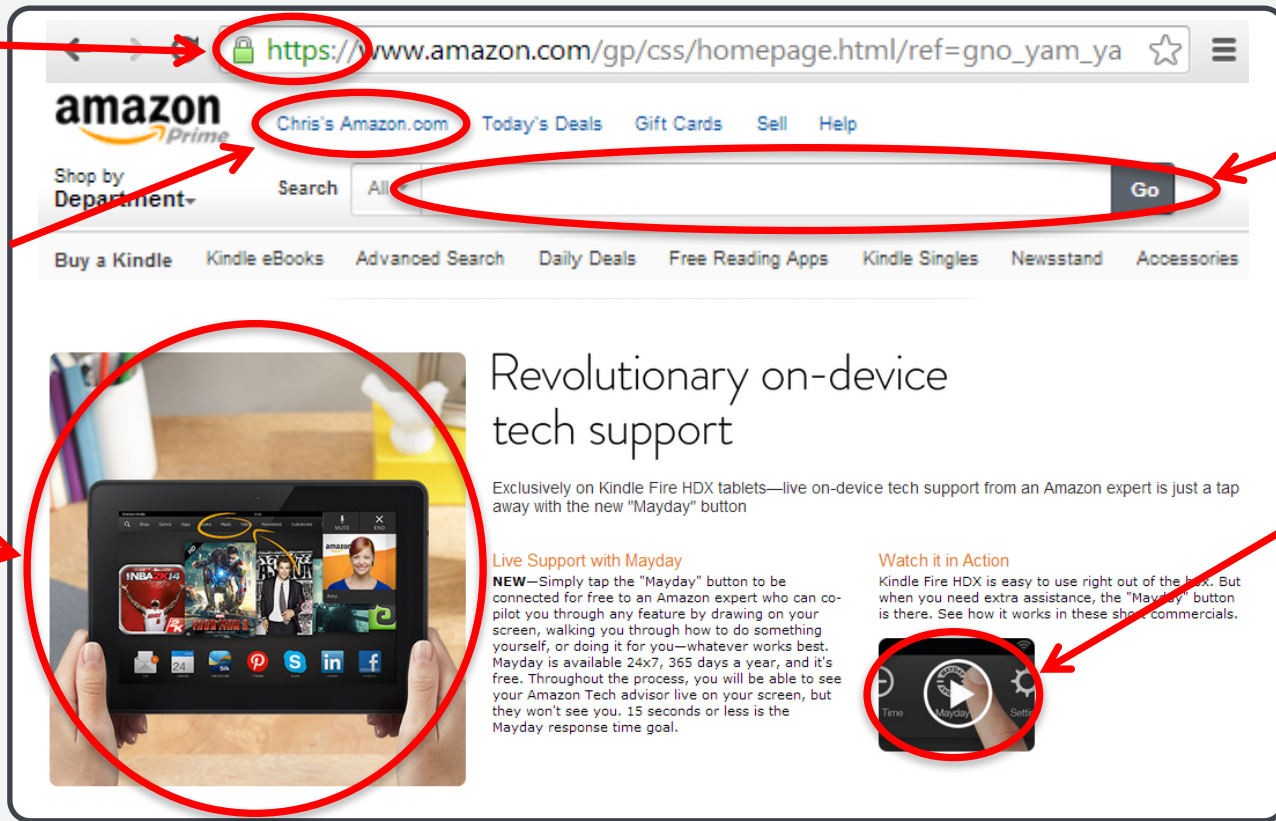
SSL

Dynamic

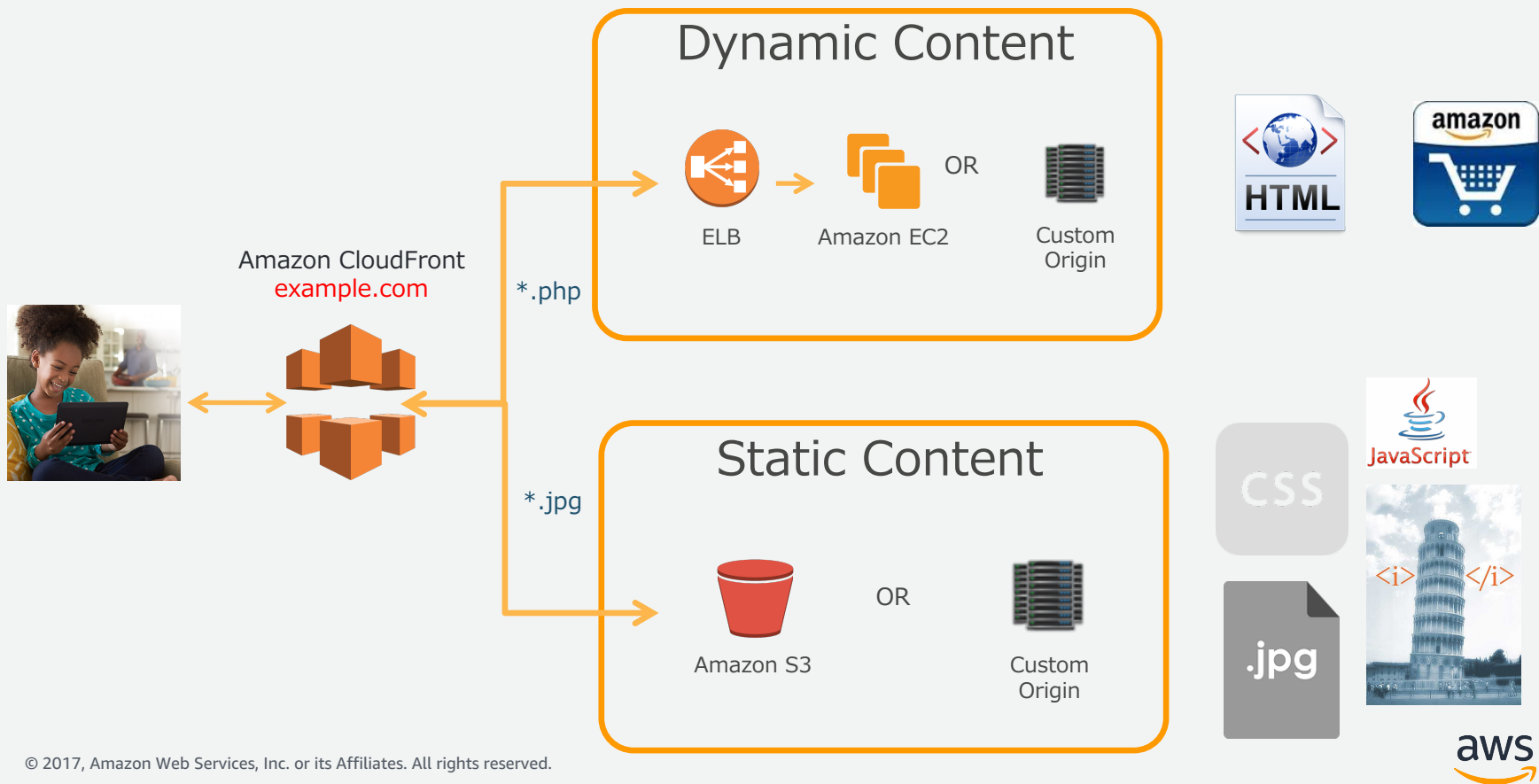
Static

User Input

Video

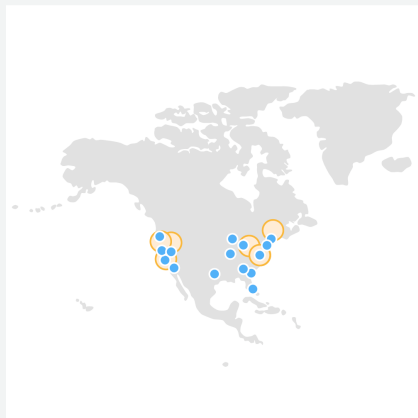


CloudFront 導入はバックエンドそのままで可能



エッジロケーション

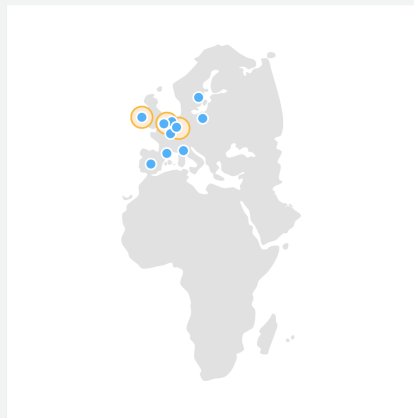
84 エッジロケーション (PoPs), **11** リージョナルエッジキャッシュ (PoPs), **50** Cities



North America
Cities: 20
PoPs: 32



South America
Cities: 2
PoPs: 3



Europe / Middle
East / Africa
Cities: 15
PoPs: 27



Asia Pacific
Cities: 13
PoPs: 22
Tokyo (4)
Osaka
...

CloudFront
リージョナルエッジキャッシュ

Tokyo, ...



Regional
Edge Cache



AWS Region /
Regional Edge
Cache



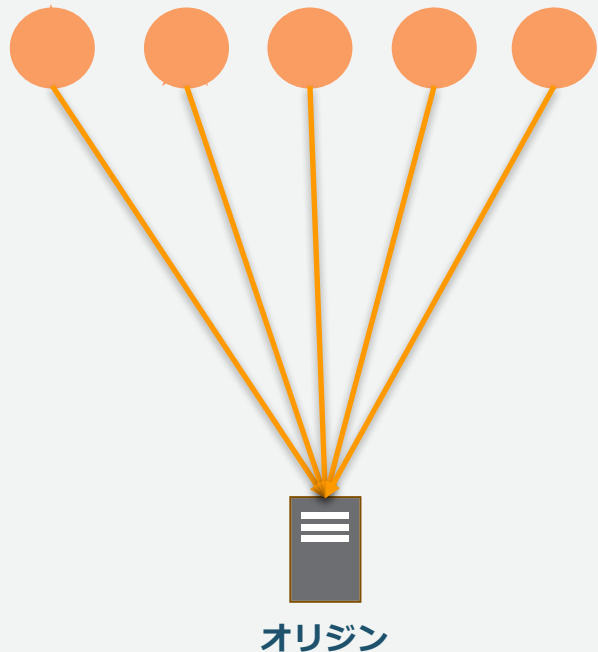
Edge
Location

CloudFront のリージョナルエッジキャッシュ



オリジンに対するコンテンツ取得を削減

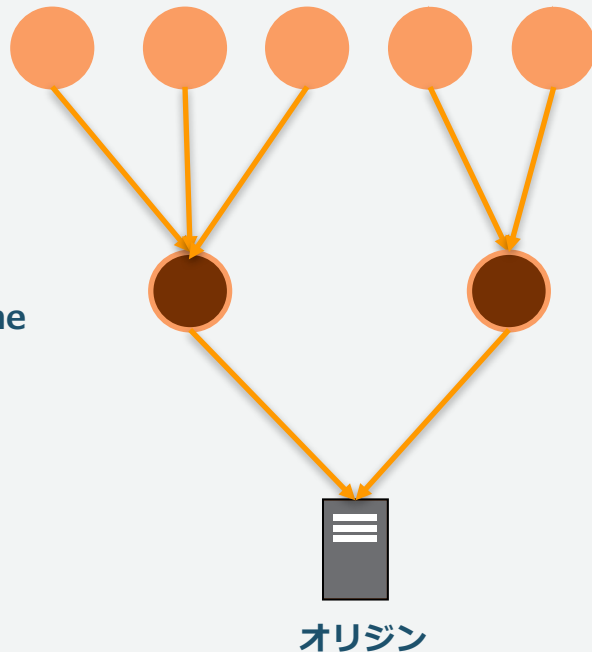
以前のアーキテクチャ



Edge Locations

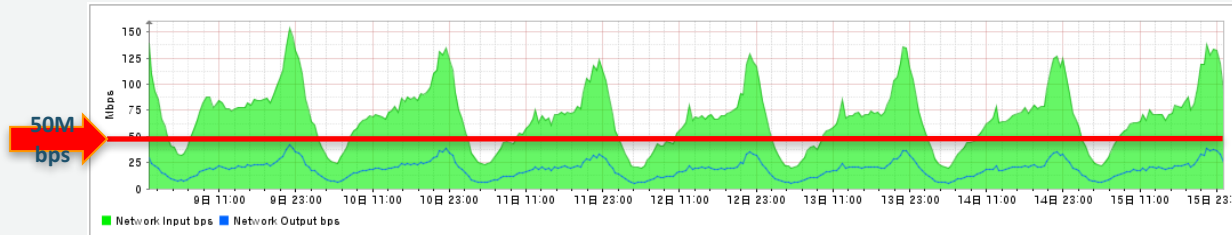
Regional Edge Cache

新しいアーキテクチャ

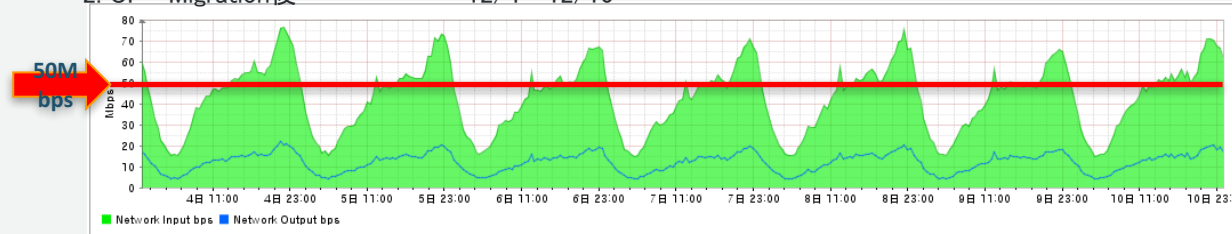


他 CDN から CloudFront に移行後オリジントラフィックが約 7 分の 1 に減少したお客様事例

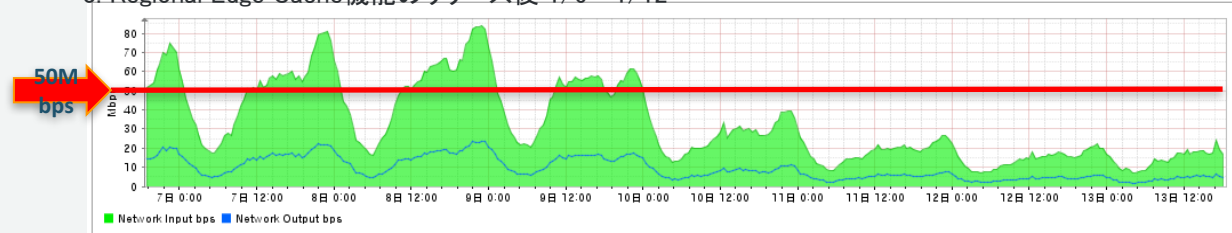
1. 他CDN使用時 10/9 ~ 10/15



2. CFへMigration後 12/4 ~ 12/10



3. Regional Edge Cache機能のリリース後 1/6 ~ 1/12



高速配信機能



CloudFront Distribution



Distribution

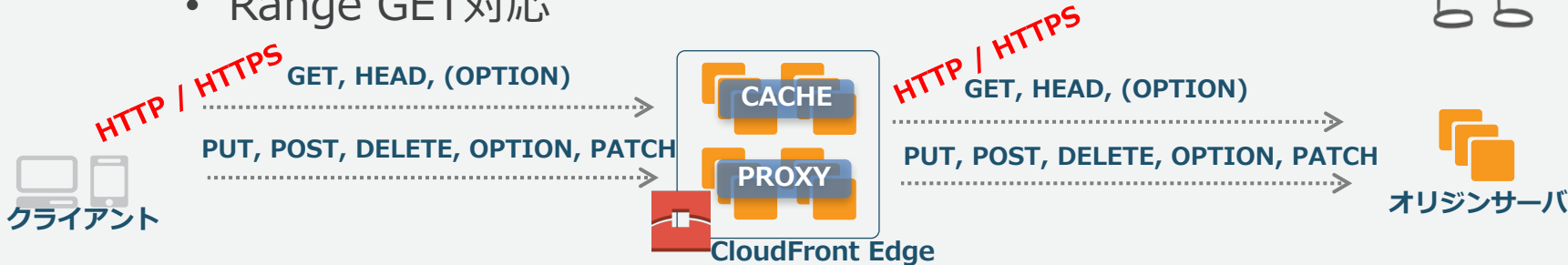
- ドメイン毎に割り当てられる CloudFront の設定
- AWS Management Console もしくは API で即時作成可能
- Web もしくは RTMP Distribution を選択可能
- Distribution あたりの使用量が最大 **40Gbps** もしくは **100,000RPS** を超える場合  は上限緩和申請が必要
- HTTP/1.0, HTTP/1.1, **HTTP/2** 対応 
 - HTTP/2 使用時はクライアントが TLS 1.2 以降と SNI (Server Name Identification) サポート必要
- **IPv6** 対応 
- デフォルトでは「xxxx.cloudfront.net」が Distribution のドメイン名として割り当てられる
 - CNAME エリアスを利用して独自ドメイン名の指定が可能
 - CNAME エリアスのワイルドカード指定もサポート (例: *.example.com など)
 - Route53 と組み合わせた Zone Apex (例: example.com など)が利用可能

Web Distribution



サポートプロトコル/HTTPメソッド

- HTTP / HTTPS 対応
 - GET, HEAD, OPTION(選択可能) (Cacheモード)
 - PUT, POST, DELETE, OPTION, PATCH (Proxyモード)
- オリジンへのアクセス
 - Internet経由でアクセスできることが必要
 - Range GET対応



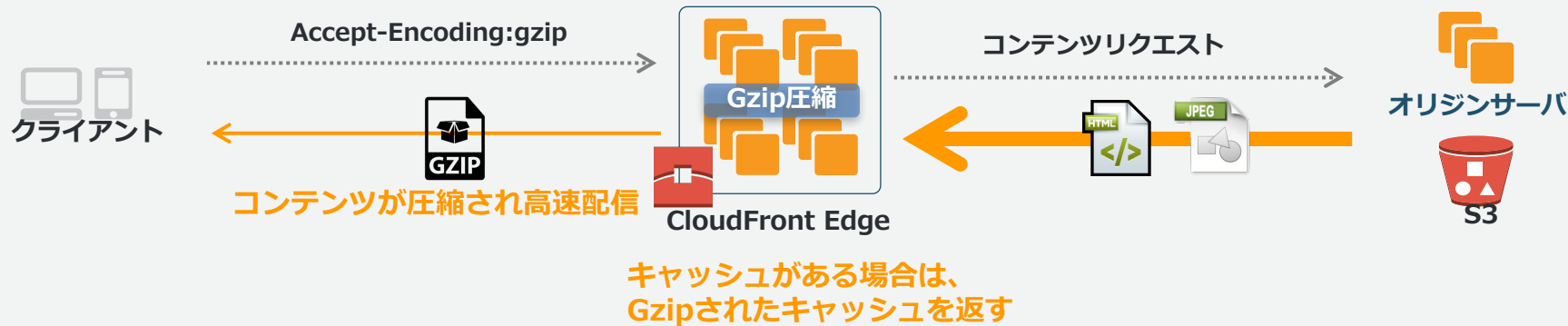
エッジでの Gzip 圧縮機能



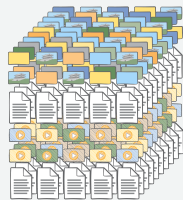
CloudFront エッジでコンテンツを Gzip 圧縮することでより高速にコンテンツを配信

リクエストヘッダーに Accept-Encoding:gzip が指定されており、オリジンが Gzip に対応していない場合は、CloudFront エッジにて Gzip 圧縮を行い配信

- Amazon S3 は Gzip 圧縮をサポートしていないため、有効なオプション



キャッシュコントロール機能



キャッシュコントロール

キャッシュヒット率を向上させることが CDN 導入におけるポイント

- GET / HEAD / OPTION(選択可能)のリクエストが対象
- 単一ファイルサイズのキャッシングは最大 20GB まで
- URLパス毎にキャッシュ期間指定が可能
- フォワードオプション機能による動的ページ配信 (Web のみ)
 - Header / Cookie / Query Strings

URLおよび有効化したフォワードオプション機能のパラメータ値の**完全一致**でキャッシュが再利用される

キャッシュコントロール機能



キャッシュコントロールヘッダーの挙動

- Object Caching により、キャッシュ時間のコントロールが可能
- オリジン側が HTTP キャッシュコントロールヘッダーを付与しない場合でも上書きが可能
- Behavior 毎にキャッシュ設定を行うことで、URL パス毎にキャッシュ期間を変えることも可能
 - デフォルト TTL : オリジンがキャッシュコントロールヘッダーを指定しない場合に利用(デフォルト 24 時間)
 - 最小 TTL : CloudFront 側でキャッシュすべき最小期間
 - 最大 TTL : CloudFront 側でキャッシュすべき最大期間

CloudFront Minimum TTL 設定				
		最小 TTL = 0 秒	最小 TTL > 0 秒を設定	
オリジン HTTP ヘッダー	Cache-Control max-age を指定	指定された max-age と最大 TTL で小さい値 の期間キャッシュ	最小 TTL < max-age < 最大 TTL max-age < 最小 TTL 最大 TTL < max-age	max-age 期間 最小 TTL 期間 最大 TTL 期間
	Cache-Control 設定なし	デフォルト TTL 期間キャッシュ (標準 24 時間)	最小 TTL またはデフォルト TTL で大きい値の期間 キャッシュ	

キャッシュコントロール機能(つづき)



CloudFront Minimum TTL 設定

		最小TTL = 0秒	最小TTL >0秒を設定	
オリジン HTTP ヘッダー	Cache-Control max-age と s-maxage を指定	指定された s-max-age と最大 TTL で小さい値の期間キャッシュ	最小TTL < s-max-age < 最大TTL	s-max-age 期間
			s-max-age < 最小 TTL	最小 TTL 期間
			最大 TTL < s-max-age	最大 TTL 期間
	Expires を指定	指定された Expires 日付と最大 TTL で早い日付の期間キャッシュ	最小 TTL < 最大 TTL	Expires 日付
			Expires < 最小 TTL	最小 TTL 期間
			最大 TTL < Expires	最大 TTL 期間
	Cache-Control no-cache, no-store を指定	キャッシュされない	最小 TTL の期間キャッシュ	

※HTML Meta タグの HTTP Cache-Control もしくは Pragma が指定されていても CloudFront のキャッシュコントロールでは利用されない
※オリジンが S3 で、オリジン側でヘッダー指定する場合は、Metadata に HTTP ヘッダーを指定

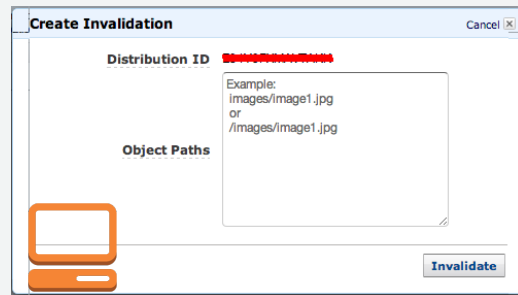
キャッシュコントロール機能

キャッシュの Invalidation(無効化)

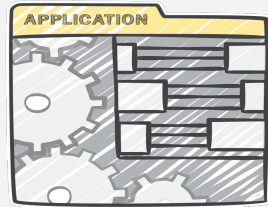
- コンテンツ毎の無効化パス指定
 - 同時に最大 3,000 個までのパス指定が可能
- ワイルドカードを利用した無効化パス指定
 - 同時に最大 15 個まで無効化パスリクエストが指定可能
 - オブジェクト数の制限無し
- AWS Management Console もしくは API で実行可能
- Invalidationの完了は 10-15 分程度



AWS SDK / CLI / API



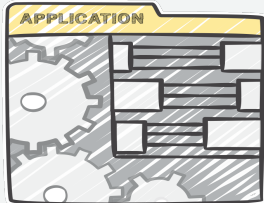
ダイナミックコンテンツ機能



動的コンテンツキャッシュへの対応

- オリジンサーバに対して Header, Cookie, Query Strings 情報をフォワードすることで、動的なページの配信にも対応
- URL パス (Behavior) と組み合わせ、きめ細かなキャッシュコントロールを実現
- Whitelist を利用して、必要最低限のパラメータのみをフォワード設定することで、キャッシュを有効活用することが重要
- キャッシュしないコンテンツでも、オリジンとの通信の最適化により配信の高速化を実現

ダイナミックコンテンツ機能

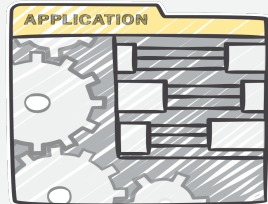


ヘッダーをオリジンへ転送

- オリジンに任意のヘッダー情報を転送することで動的なページ生成にも対応
- 全てのヘッダーをフォワードするとキャッシュ効率が大幅に低下するため必要最小限のヘッダーを指定することを推奨
- カスタムヘッダーにも対応
- CloudFront 独自ヘッダー
 - CloudFront 側でクライアントの情報を独自に判定し、オリジンにフォワード

Type	Header	詳細
接続プロトコル判定	CloudFront-Forwarded-Proto	HTTP もしくは HTTPS を設定
デバイス判定	CloudFront-Is-Mobile-Viewer CloudFront-Is-Tablet-Viewer CloudFront-Is-Desktop-Viewer	User-Agent をもとに、クライアントデバイスの情報を True/False で設定
地域判定	CloudFront-Viewer-Country	クライアントの IP アドレスをもとに、地域コードを設定 (ISO-3166-1 alpha-2 準拠)

ダイナミックコンテンツ機能

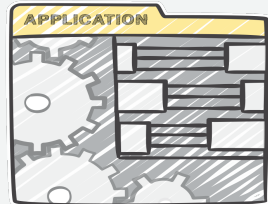


Cookie をオリジンへ転送

- オリジンに任意の Cookie 情報を転送することで動的なページ生成にも対応
- CloudFront は指定された Cookie 名と値をセットでキャッシュ
- 全ての Cookie をフォワードするとキャッシュ効率が大幅に低下するため必要最小限の Cookie を指定することを推奨
- 対象の Cookie 名はワイルドカードの指定も可能

Forward Cookies	Whitelist ▼	i	
	Whitelist Cookies	SESSION_* USERID	i

ダイナミックコンテンツ機能



クエリ文字列パラメータの値をオリジンへ転送

- オリジンに任意のクエリ文字列を転送することで動的なページ生成にも対応
- CloudFront は指定されたクエリ文字列パラメータと値をセットでキャッシュ
- 全てのクエリ文字列をフォワードするとキャッシュ効率が大幅に低下するため必要最小限のクエリ文字列を指定することを推奨



Query String Forwarding and Caching	Forward all, cache based on whitelist ▼	
Query String Whitelist	language w	
Valid characters: a-z, A-Z, 0-9, - . _ * + % Learn More		

パラメータの順序を常に統一する

パラメータ名とパラメータ値の大文字と小文字を常に統一する

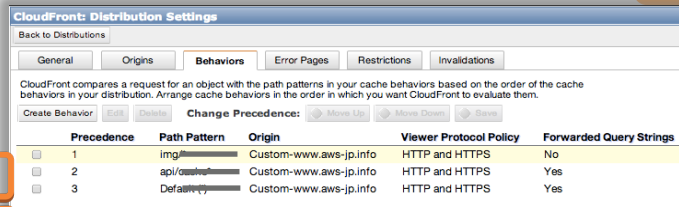
ダイナミックキャッシング

Behaviors を活用したマルチオリジンおよびキャッシュコントロールの個別設定

- クライアントからのリクエストパスパターンをもとに、キャッシュポリシーやオリジンへのアクセスルールの個別指定が可能

Behavior Cache TTL (正規表現)

http://www.aws.com/



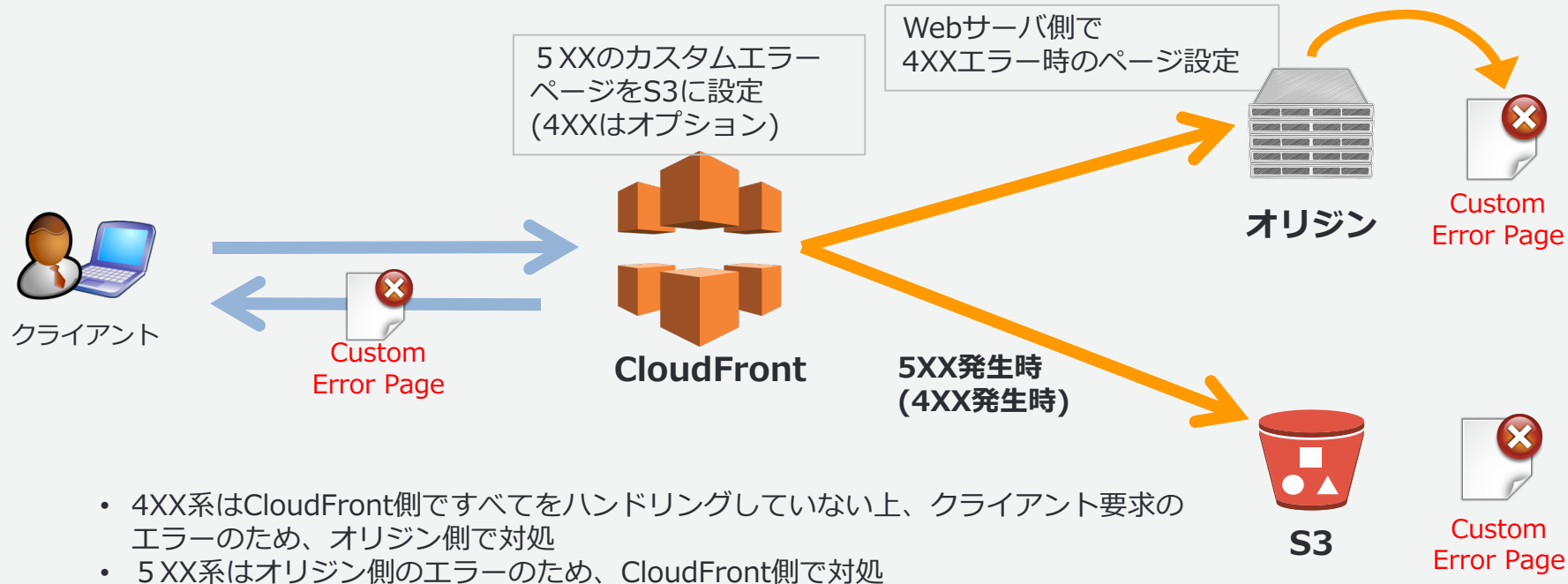
Behaviors Path Patternの記述方法

- 「*」 0もしくはそれ以上の文字列
- 「?」 1文字

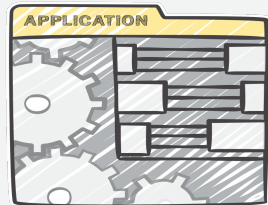
例) /*.jpg, /image/*, /image/a*.jpg, /a??.jpg

カスタムエラーページ

Amazon S3と組み合わせた構成例



カスタムオリジンのタイムアウト



オリジンの読み取りタイムアウト

- CloudFront がカスタムオリジンからの応答を待つ時間を指定
- ビジー状態の負荷を軽減したり、ビューアにエラー応答をより迅速に表示したりする場合は、読み取りタイムアウトを小さくする
- デフォルトのタイムアウトは 30 秒、 4～60 秒の範囲で設定可能

キープアライブタイムアウト

- 接続を閉じる前に CloudFront がカスタムオリジンサーバーとの持続的接続を維持する最大時間を指定
- デフォルトのキープアライブアイドルタイムアウト値は5秒、 1～60秒の範囲で設定可能

セキュリティ機能



セキュリティ機能

セキュア配信



- HTTPS 対応 (強制リダイレクト / HTTPS のみ許可)
- SSL 証明書
(デフォルト / SNI / 専用IPアドレス / Certification Manager)
- ビューワー接続 SSL セキュリティポリシー 
- オリジン暗号化通信
- オリジンカスタムヘッダー
- GEOリストリクション (Whitelist / Blacklist)
- 署名付き URL/Cookie (有効期間指定)
- AWS WAF 連携
- AWS Shield による DDoS 攻撃対策 

サポートする SSL 証明書



デフォルト証明書

- cloudfront.net ドメインの SSL 証明書は標準で利用可能

独自 SSL 証明書

- X.509 PEM 形式かつ認証チェーンが含まれること、鍵長は最大 2048bit
- 様々な証明書タイプをサポート
 - Domain Validated, Extend Validated, Wildcard, Subject Alternative Name 証明書 など
- ACM(AWS Certification Manager) で発行された証明書

SNI(Server Name Indication) SSL 証明書

- CloudFront の専用 IP アドレス費用を負担せず、独自ドメインでの SSL 通信が可能
- 一部古いブラウザは SNI 拡張をサポートしていないため注意が必要
 - フィーチャーフォンブラウザなど

専用IP アドレス SSL 証明書

- 専用IP アドレス使用時は CloudFront にて別途利用課金される

独自 SSL 証明書の利用

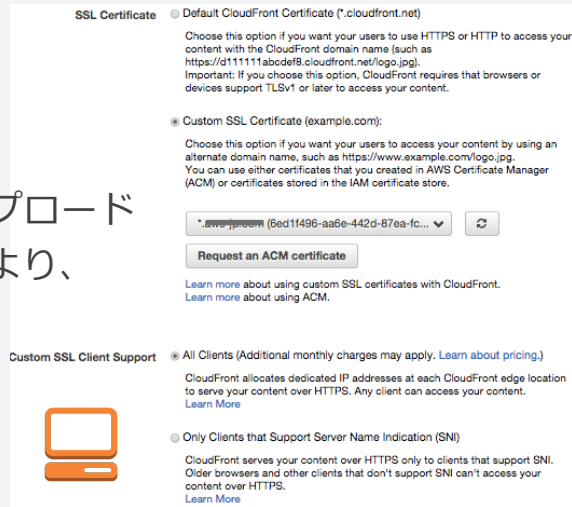


利用申請

- 専用IP アドレス SSL 証明書の利用には上限緩和申請が必要
※AWS アカウントあたり 2 がデフォルト上限

利用手順

- 1-1. 証明書機関で署名を受けた証明書を IAM CLI を利用してアップロード
- 1-2. AWS Certification Manager の Management Console 画面より、
生成したい証明書の FQDN を指定
※ホスト名にワイルドカードも指定可能
2. CloudFront の Distribution 設定画面にて登録した証明書を選択
3. 証明書と同じ CNAME に設定
4. SNI の有無を選択
5. 指定した CNAME と Distribution 作成時に生成される Domain 名を紐付けたレコードを DNS に登録

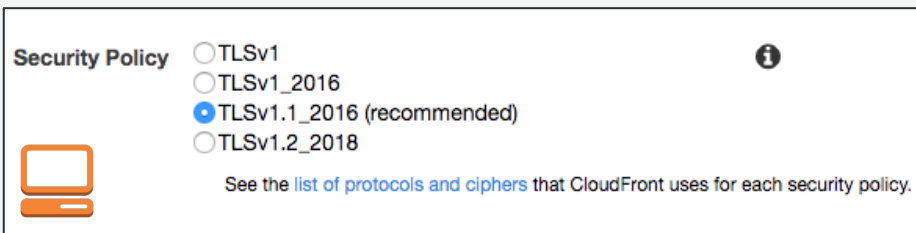


ビューワー接続 SSL セキュリティポリシー



クライアント と CloudFront 間の事前定義された SSL/TLS プロトコルと Cipher の組み合わせをサポート

- TLSv1.2_2018, TLSv1.1_2016(推奨), TLSv1_2016, TLSv1, SSLv3 から選択
- 独自 SSL 証明書 のみ指定可能
 - SNI SSL 証明書は TLSv1 以降のみ指定可能
 - SSLv3 は専用 IP アドレス SSL 証明書のみ指定可能

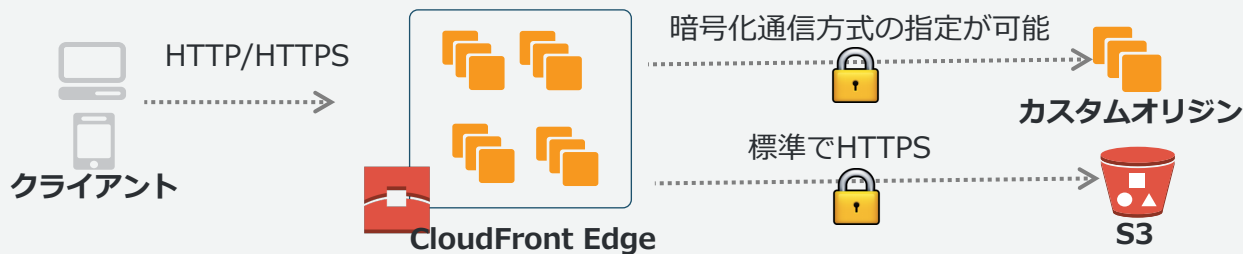


オリジン暗号化通信



CloudFront エッジとオリジン間の通信方式を制御

- SSL プロトコル方式
 - TLSv1.2, TLSv1.1, TLSv1, SSLv3 から複数指定可能
- オリジンとの通信プロトコル
 - HTTP のみ、HTTPS のみ、クライアントからの通信プロトコルに合わせる
- カスタムオリジンの場合のみ指定可能



Origin Settings

Origin Domain Name	httpbin.org
Origin Path	
Origin ID	Custom-httpbin.org
Origin SSL Protocols	☒ TLSv1.2 ☒ TLSv1.1 ☒ TLSv1 ☐ SSLv3
Origin Protocol Policy	☐ HTTP Only ☒ HTTPS Only ☐ Match Viewer



オリジンカスタムヘッダー



エッジからオリジンサーバへの通信でカスタム HTTP ヘッダーの追加

- オリジンサーバ毎に固定でヘッダーの追加もしくはクライアントからのリクエストヘッダーの上書きが可能

Origin Custom Headers	Header Name	Value	
	X-CloudFront-Distribution-Id	123	✕
	X-Shared-Secret	cf9db9688ff28c2624fdaa321948c51	⊕

- Shared-Secret
 - CloudFront とオリジン間で任意のヘッダーおよびヘッダー値を取り決め、オリジン側でヘッダー値のチェックを行うことで、カスタムオリジンは CloudFront からのアクセスのみに制御する
- リクエストヘッダーの調整
 - Cross-Origin Request Sharing(CORS) 通信時に、クライアントブラウザのバージョンなどにより、ブラウザが適切なヘッダーを付与しない場合に、強制的に設定

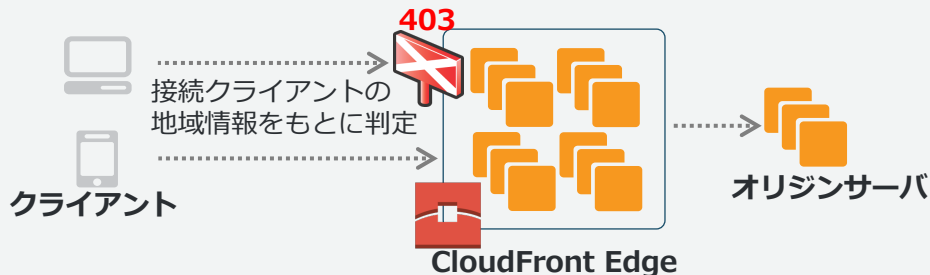
GEO リストリクション



地域指定によるアクセス制御

- 接続されるクライアントの地域情報を元に、エッジでアクセス判定
- Blacklist もしくは Whitelist で指定可能
- Distribution 全体に対して適用される
- 制限されたアクセスには **403** を応答

GEO Restriction有効



Edit Geo-Restrictions

Geo-Restriction Settings

Enable Geo-Restriction ☒ Yes ☐ No ⓘ

Restriction Type ☒ Whitelist ☐ Blacklist ⓘ

Countries ⓘ

IT -- ITALY
JM -- JAMAICA
JP -- JAPAN
JE -- JERSEY
JO -- JORDAN
KZ -- KAZAKHSTAN

Add >> << Remove

JP -- JAPAN

Cancel Yes, Edit

署名付き URL/Cookie



署名付き URL/Cookie を利用したプライベートコンテンツ配信

- Restricted Viewer Access を有効にするだけで、署名のないアクセスを全てブロック
 - Behavior 単位で指定可能
 - URL もしくは Cookie いずれかを利用可能
- 標準 (Canned Policy)
 - 有効期間 (時刻を秒単位指定)
 - 有効コンテンツパス
- オプション (Custom Policy)
 - アクセス元 IP アドレス制限
 - 有効開始時刻指定
 - 許可コンテンツのワイルドカード指定

Edit Behavior

Whitelist Headers ⓘ 2 header(s) whitelisted

Filter headers or enter a custom header

Accept
Accept-Charset
Accept-Datetime
Accept-Language
Authorization
CloudFront-Forwarded-Proto

Add Custom >>
Add >>
<< Remove

Object Caching ⓘ

☒ Use Origin Cache Headers ⓘ
☐ Customize [Learn More](#)

Minimum TTL ⓘ 60

Maximum TTL ⓘ 31536000

Default TTL ⓘ 86400

Forward Cookies ⓘ None (Improves Caching) ⓘ

Forward Query Strings ⓘ ☒ Yes ⓘ
☐ No (Improves Caching)

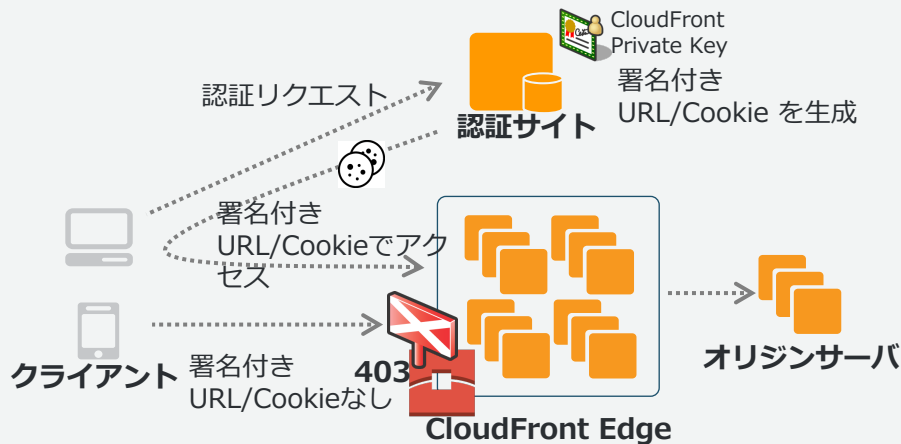
Smooth Streaming ⓘ ☒ Yes ⓘ
☐ No

Restrict Viewer Access ⓘ ☒ Yes ⓘ
☐ No
If you restrict viewer access, viewers must use CloudFront signed URLs or signed cookies to access your content. For more information, see [Serving Private Content through CloudFront in the Amazon CloudFront Developer Guide](#).

署名付き URL/Cookie

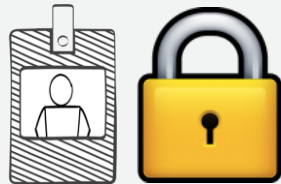


署名付き URL/Cookie を利用した際のアクセスフロー



- 単一コンテンツアクセスの場合は署名付き URL、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

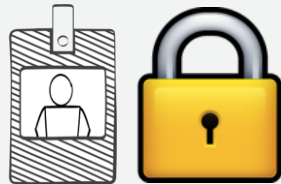
署名付き URL



- Web および RTMP 双方に対応
 - Web の場合は有効期間を最小化することを推奨
 - TCP コネクション確立中は対象コンテンツのダウンロードが可能
 - RTMP の場合は動画再生時間以上の有効期間の設定が必要
- 権限のないアクセスには 403 を応答
- URL の生成
 - 決められたフォーマットで Query Strings にパラメータ値を設定
 - Canned Policy:
`http://xxxx.cloudfront.net/file.jpg?Expires=XXX&Signature=XXX&Key-Pair-Id=XXX`
 - Custom Policy: `http://xxxx.cloudfront.net/file.jpg?Policy=XXX&Signature=XXX&Key-Pair-Id=XXX`
 - CloudFront の秘密鍵を利用して Signature のパラメータ文字列を署名
 - アクセス URL 毎に必ず署名が必要
 - サンプルソースコード (Perl / PHP / C# + .NET Framework / Java)
http://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/PrivateCFSignatureCodeAndExamples.html



署名付き Cookie



- Web ディストリビューションのみサポート
 - 許可コンテンツのワイルドカードパス指定ができるため、1つの Cookie で対象パス以下のコンテンツにアクセス可能
- Cookie の中に署名付き URL の Custom Policy と同様のパラメータをセット
 - CloudFront-Key-Pair-Id, CloudFront-Policy, CloudFront-Signature
- Set-Cookie 時のポイント
 - Domain 属性を利用して、CloudFront の Alternate Domain Name と同じドメイン名を指定することで、Cookieの有効範囲を制限
 - ExpireおよびMax-Age属性を利用しないことで、セッションCookieを作成
 - Secure属性を利用することでクライアントリクエスト時にCookieを含める際にCookieの暗号化を行う
- サンプルソースコード(Perl / PHP / C# + .NET Framework / Java)
https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-cookies.html#private-content-overview-sample-code-cookies



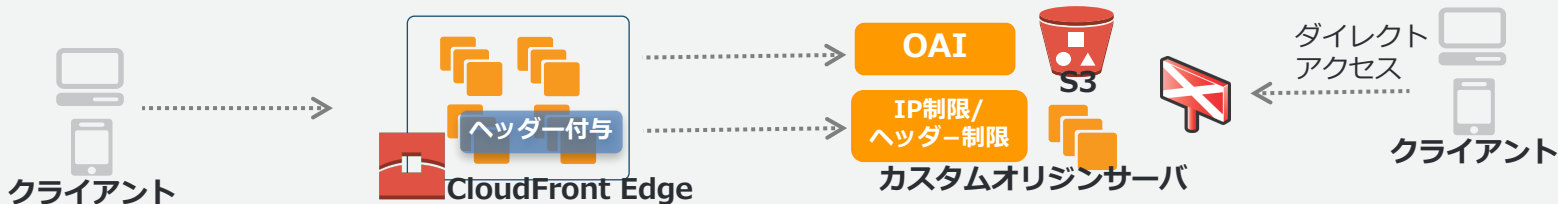
オリジンサーバの保護

オリジンが S3 の場合

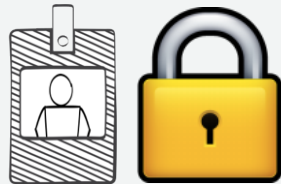
- Origin Access Identity(OAI) を利用
 - S3 の Bucket へのアクセスを CloudFront からのみに制限

カスタムオリジンの場合、下記の2種類が選択可能

- オリジンカスタムヘッダーを利用し、CloudFront で指定された任意のヘッダーをオリジン側でチェック
- オリジン側のアドレスを公開しないとともに、CloudFront が利用する IP アドレスのみの許可させる
 - CloudFront が利用する IP アドレスは下記 URL から取得可能
<https://ip-ranges.amazonaws.com/ip-ranges.json>
 - JSON フォーマット
 - » Service キーの “CLOUDFRONT” でフィルタすることで抽出可能

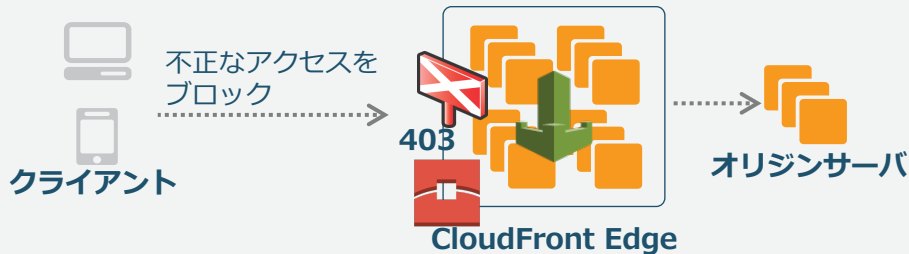


AWS WAF 連携



AWS WAF で定義した Web ACL を CloudFront Distribution に適用

- CloudFront をサービスの前段に配置することでサイトの保護を実現
- AWS WAF での制御
 - IP アドレス制限 / SQLインジェクション / ヘッダー, クエリ等の String マッチング
- AWS WAF の内容が即時反映
- ブロック時は 403(Forbidden) を応答



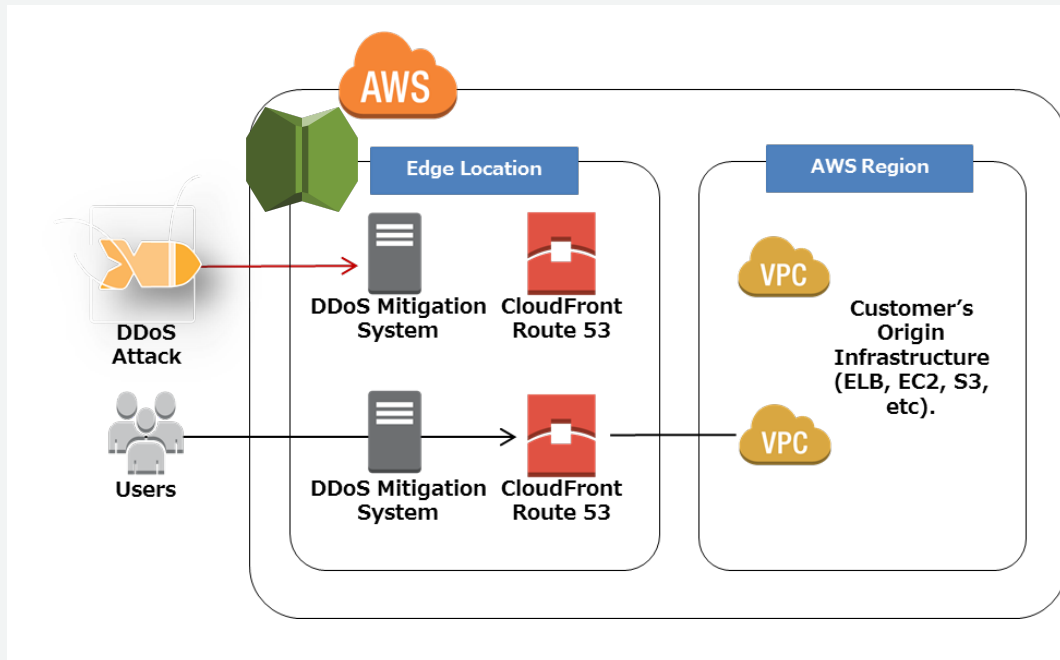
Edit Distribution	
Distribution Settings	
Price Class	Use All Edge Locations (Best Performance) ⓘ
AWS WAF Web ACL	None ⓘ
Alternate Domain Names (CNAMEs)	demo.com ⓘ
SSL Certificate	Default CloudFront Certificate (*.cloudfront.net)

AWS Shield による DDoS 攻撃対策

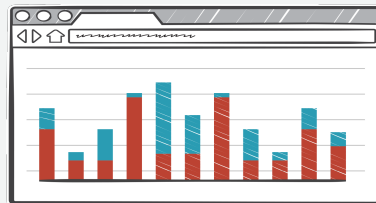


Amazon のノウハウを詰め込んだ DDoS 攻撃を緩和するサービス
デフォルトで有効になっており無料で利用できる

- Amazon 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



レポート & ロギング機能



CloudFront Reports & Analytics

Cache Statistics

- キャッシュの利用状況

Monitoring and Alarming

- リアルタイムモニタリングと通知

Popular Objects

- 人気コンテンツの統計情報

Top Referrers

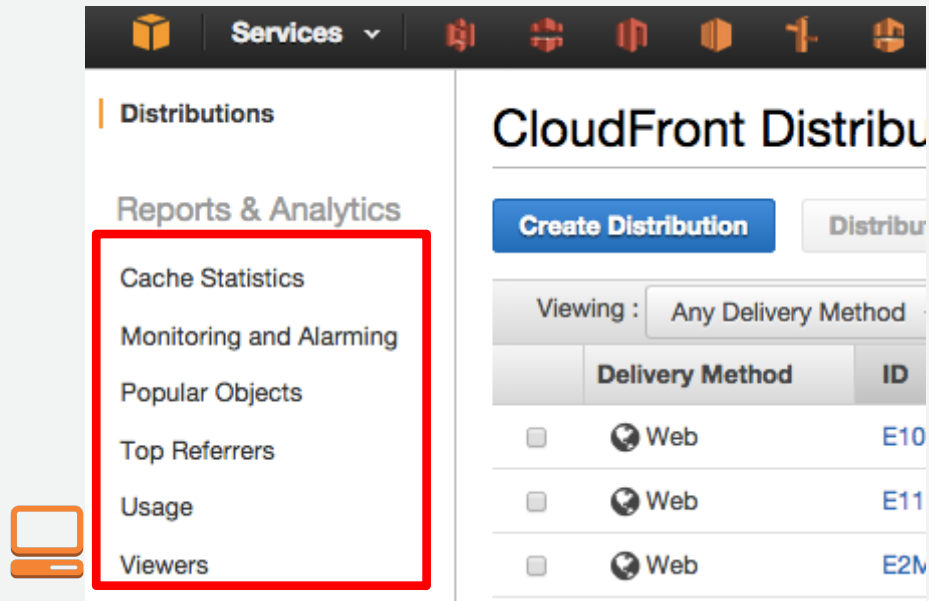
- リファラーの統計情報

Usage

- リクエスト数およびデータ転送量

Viewers

- クライアントデバイスの統計情報

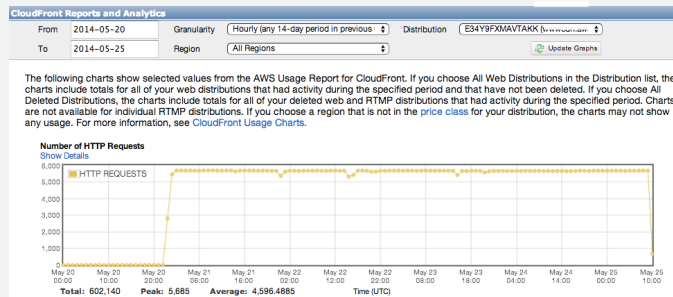


Cache Statistics / Popular Objects /
Top Referrers / Usage / Viewers は AWS
Management Console のみで参照可能

CloudFront Reports & Analytics

Cache Statistics / Popular Objects / Usage / Top Referrers / Viewers に関しては CloudFront の利用状況における傾向分析として利用

- 直近 60 日間のグラフが参照可能
- 1 時間単位もしくは日単位でのグラフ表示
- グラフへの反映までには 3 時間程度 Delay
- CSV へのエクスポートも可能
- フィルタリング
 - 全 Distribution もしくは Distribution 単位
 - 期間指定
 - エッジ地域



Monitoring and Alarming はリアルタイムの利用状況の確認により、アクセス状況のリアルタイム監視として利用

- 数分の遅延で利用状況を把握可能
- Cloudwatch のアラート機能を利用し、突発的なアクセスやエラーレートの上昇の検知による通知が可能
- 3~5 分程度の Delay で検知

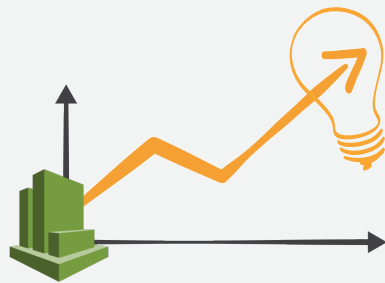
CloudFront Reports & Analytics

Cache Statistics

- Total Request
 - 全リクエスト数
- Percentage of Viewer Requests by Result Type
 - CacheのHit/Miss/Error の割合
- Bytes Transferred to Viewers
 - クライアントへの総データ転送容量
 - Miss Hit したリクエストに対する総データ転送容量
- HTTP Status Codes
 - 2XX, 3XX, 4XX, 5XX 毎の応答数
- Percentage of GET Requests that Didn't Finish Downloading
 - ダウンロードを完了出来なかった GET リクエストの割合

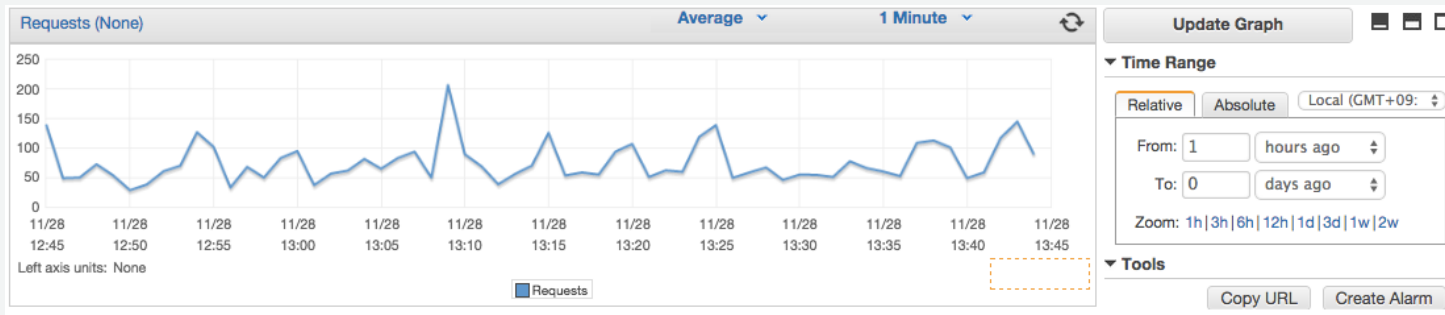


CloudFront Reports & Analytics



Monitoring and Alarming

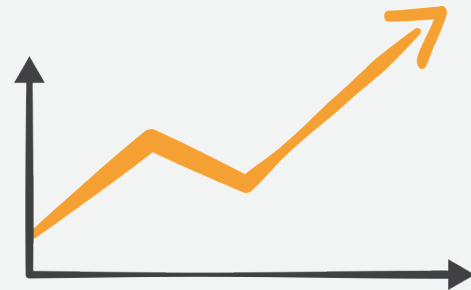
- CloudWatch を利用するため、しきい値設定によるアラート連携も可能
- CloudFront の CloudWatch メトリックスは Virginia リージョンに出力される
- メトリックス
 - 4xxErrorRate, 5xxErrorRate, TotalErrorRate
 - BytesDownloaded, BytesUploaded
 - Requests



CloudFront Reports & Analytics

Popular Objects

- Distribution 毎のリクエスト数の多いTop 50コンテンツリスト
 - Object
 - Requests
 - Hits, Hit %, Misses
 - Total Bytes, Bytes From Misses,
 - Incomplete Download, Response Code

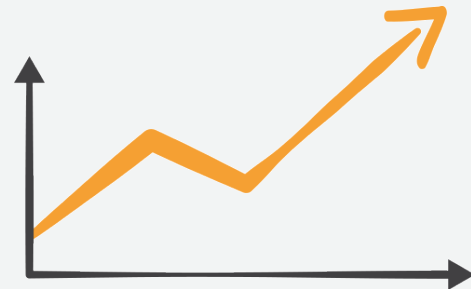


	Object	Requests	Hits	Misses	Hits %	Bytes From Misses (Adjusted)	Total Bytes (Adjusted)	Incomp	2xx	3xx	4xx	5xx
1	/index.php	309,642	306,711	2,818	99.08%	160.54 MB	17.20 GB	0	309,642	0	0	0
2	/	7	1	6	14.29%	350.25 KB	408.87 KB	0	7	0	0	0

CloudFront Reports & Analytics

Top Referrers

- Distribution 毎のリクエスト数の多い Top 25 のリファラードメイン
 - Referrers ドメイン
 - Request Count
 - Request %

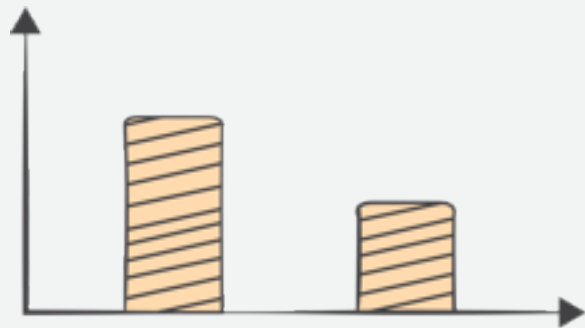


	Referrer	Request Count ▲	Request %
1	Not Specified	899,180	99.93%
2	320xsmadim510b.cloudfront.net	608	0.07%
3	www.in.aws-jp.info	20	0.00%

CloudFront Reports & Analytics

Usage

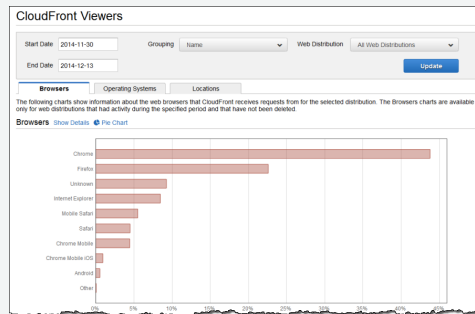
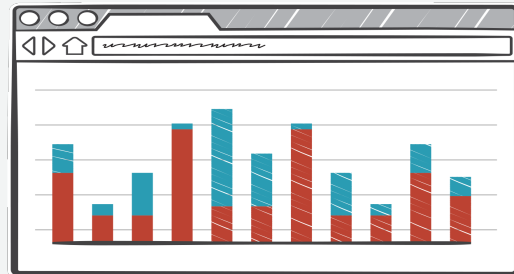
- Number of Requests
 - HTTP リクエスト数
 - HTTPS リクエスト数
- Data Transferred by Protocol
 - HTTP によるクライアントおよびオリジンに対して送信したデータ転送容量
 - HTTPS によるクライアントおよびオリジンに対して送信したデータ転送容量
- Data Transferred by Destination
 - CloudFront Edge からクライアントに送信したデータ転送容量
 - CloudFront Edge からオリジンに送信したデータ転送容量



CloudFront Reports & Analytics

Viewers

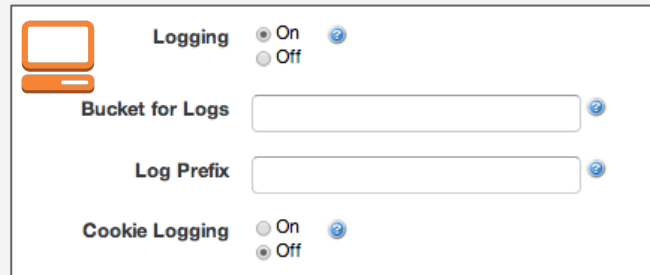
- Distribution 毎のクライアントデバイス情報
 - Devices
 - デバイス種別の比率
 - デバイストレンド(日単位でのデバイス毎のリクエスト数)
 - Browsers
 - ブラウザー種別の比率
 - ブラウザートレンド(日単位でのブラウザー毎のリクエスト数)
 - Operating Systems
 - OS 種別の比率
 - OS トレンド (日単位での OS 毎のリクエスト数)
 - Locations
 - Location トレンド(日単位での地域毎のリクエスト数)
 - Location 毎の比率 (Request Count/Request%/Bytes)



Access Log

CloudFront アクセスログ

- 任意の S3 Bucket に出力可能
- アクセスログの出力はタイムラグあり



Logging ☒ On ☐ Off

Bucket for Logs

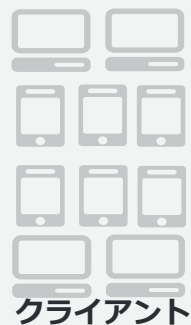
Log Prefix

Cookie Logging ☐ On ☒ Off

項目	説明
date	アクセス日(UTC)
time	アクセス時間(UTC)
x-edge-location	エッジロケーションID
sc-bytes	配信Byte数(ヘッダー含む)
c-ip	クライアントIPアドレス
cs-method	HTTPアクセスMethod
cs(Host)	CloudFront Distributinドメイン名
cs-uri-stem	リクエストURI
sc-status	レスポンスコード
cs(Referer)	リファラ
cs(User-Agent)	クライアントユーザエージェント
cs-uri-query	リクエストQuery Strings
cs(Cookie)	リクエストCookieヘッダー

項目	説明
x-edge-result-type	Hit : キャッシュヒット RefreshHit : キャッシュがExpireされていた Miss : キャッシュミス LimitExceeded: CloudFrontのリミットオーバ CapacityExceeded: エッジのキャパシティ不足 Error : クライアントもしくはオリジンによるエラー
x-edge-request-id	CloudFrontのリクエストID
x-host-header	リクエストHost Header
cs-protocol	リクエストプロトコル(http / https)
cs-bytes	リクエストByte数(ヘッダー含む)
time-taken	CloudFrontエッジがリクエストを受けて、オリジンからLastByteを取得するまでにかかった秒数
x-forwarded-for	ViewerがHTTPプロキシなどを利用した場合の元Viewer IP
ssl-protocol	クライアントとHTTPS通信をした際の利用したプロトコル
ssl-cipher	クライアントとHTTPS通信した際の利用した暗号化方式
x-edge-response-result-type	Viewerにレスポンスを返す直前の処理分類 ※分類はx-edge-result-typeと同様

CloudFront ログ & レポート

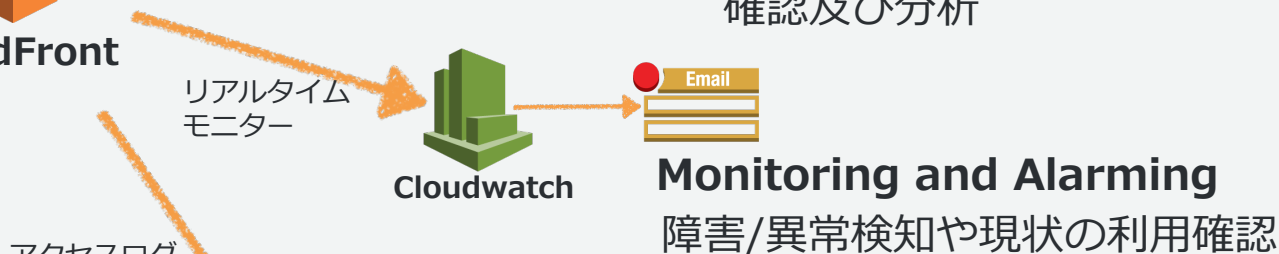


クライアント



Cache Statistics
Popular Objects
Top Referrers
Usage
Viewers

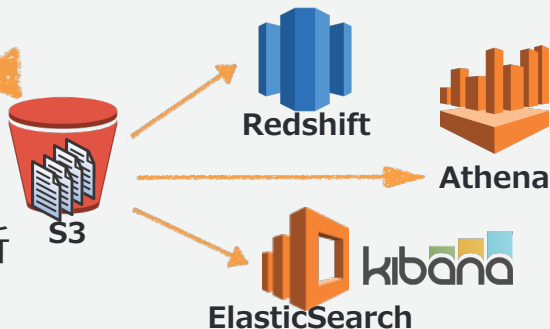
アクセスや利用状況傾向の
確認及び分析



アクセスログ

Access Log

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



TIPS

DNS名前解決の高速化

Route 53と連携したDNS Lookupの高速化

- CloudFront の Alternative Domain Name を Route53 を利用して名前解決する際は、レコードセット Type を **CNAME** ではなく **A レコードの Alias** 設定することでクエリ回数が削減

CNAME

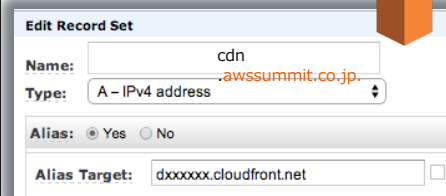
```
> nslookup cdn.awssummit.co.jp
Server:      192.168.2.1
Address:     192.168.2.1#53

Non-authoritative answer:
cdn.awssumit.co.jp canonical name =
dxxxx.cloudfront.net.
Name: dxxxx.cloudfront.net
Address: 54.230.234.XXX
Name: dxxxx.cloudfront.net
Address: 54.230.234.XXX
:
```

A Record + Alias

```
> Nslookup cdn.awssummit.co.jp
Server:      192.168.2.1
Address:     192.168.2.1#53

Non-authoritative answer:
Name: cdn.awssumit.co.jp
Address: 54.230.234.XXX
Name: cdn.awssumit.co.jp
Address: 54.230.234.XXX
Name: cdn.awssumit.co.jp
Address: 54.230.235.XXX
:
```

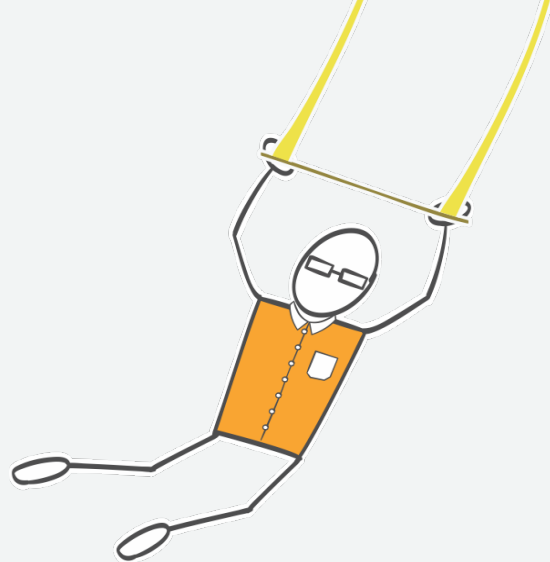


リアルタイム障害/異常検知



Cloudwatch Alarmの活用

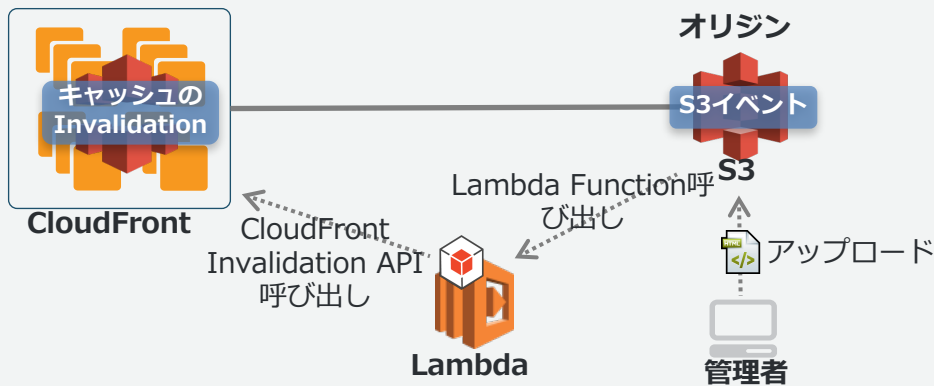
- Request メトリックス
 - 上限値アラーム設定による突発的なアクセス検知
 - 下限値アラーム設定によるアクセス障害検知
- TotalErrorRate メトリックス
 - 上限値アラーム設定によるオリジンエラー障害検知



Amazon S3オリジン自動キャッシュの無効化

Lambdaを活用した自動キャッシュの無効化

- S3 への最新コンテンツのアップロードに連動して、CloudFrontから対象コンテンツの Invalidation を自動発行
- S3 のイベントおよび Lambda を利用し、CloudFront の Invalidation API をコール



※Lambda Functionのプログラムは別途作成する必要あり

▼ イベント

イベント通知によって、アラートの送信やワークフローのトリガーを実行できます。通知は、Amazon Simple Notification Service (SNS) や Amazon Simple Queue Service (SQS) 経由で送信したり、Lambda 関数宛てに送信したりすることができます (バケットの場所によって決まります)。

名前	CloudFront Invalidation	?
イベント	Put	?
プレフィックス	e.g. images/	?
サフィックス	e.g. .jpg	?
送信先	☐ SNS トピック ☐ SQS キュー ☒ Lambda 関数	?
Lambda 関数の	Lambda 関数を選択/入力	

S3 はこのソースバケットから Lambda 関数を呼び出すのに必要なアクセス権限を追加します。『開発者ガイド』を参照してください。

AWS Lambda@Edge



Lambda@Edge の特徴



- Lambda@Edge は AWS Lambda の拡張、AWS のエッジロケーションでのコード実行を可能に
- コードをエッジロケーションに配置することで、エンドユーザーの近くでコンテンツをカスタマイズし、ユーザー体験を改善



**サーバー管理
が不要**



**継続的
スケーリング**



**ミリ秒単位
の課金**

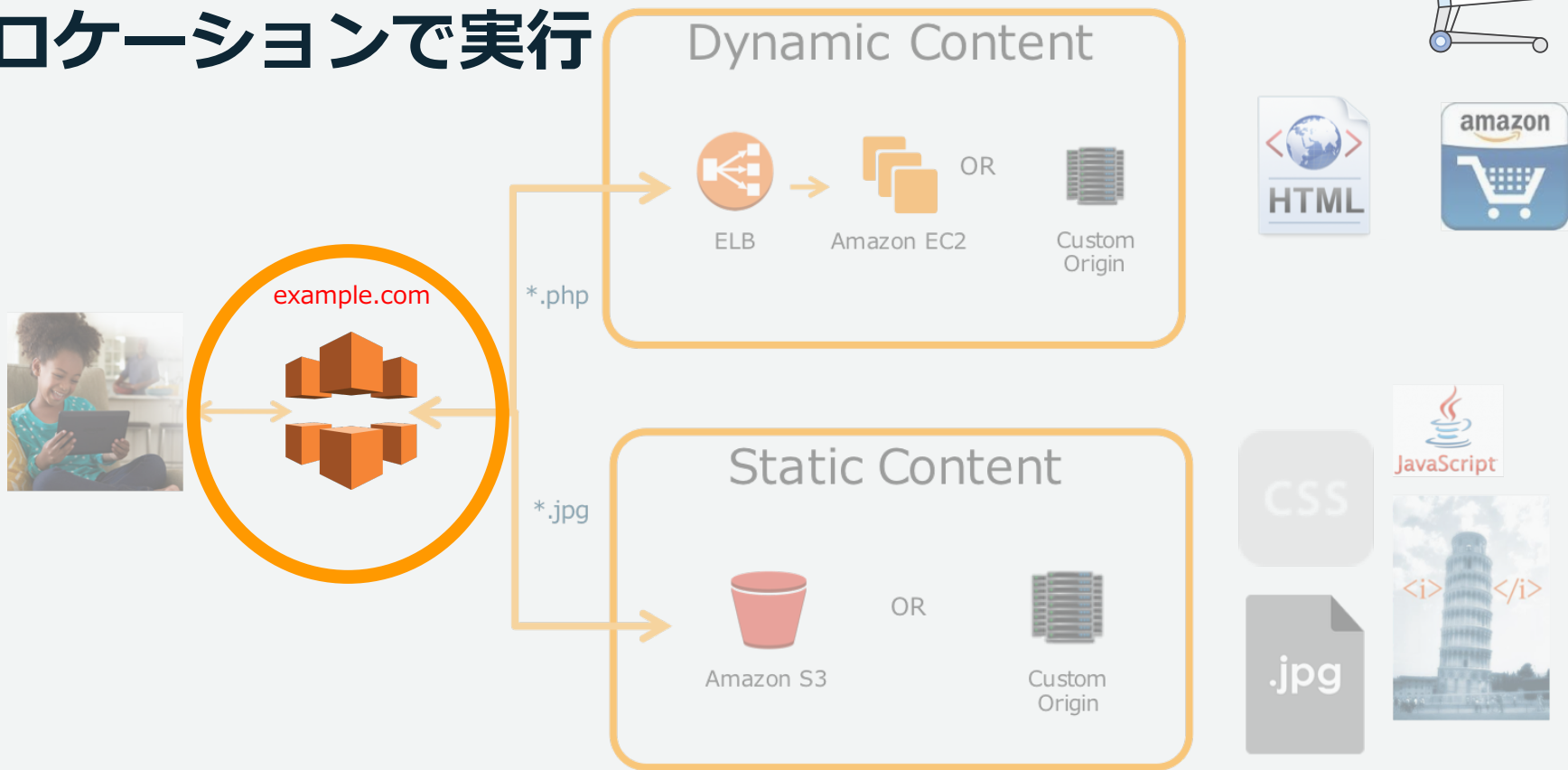


**グローバル
に分散**

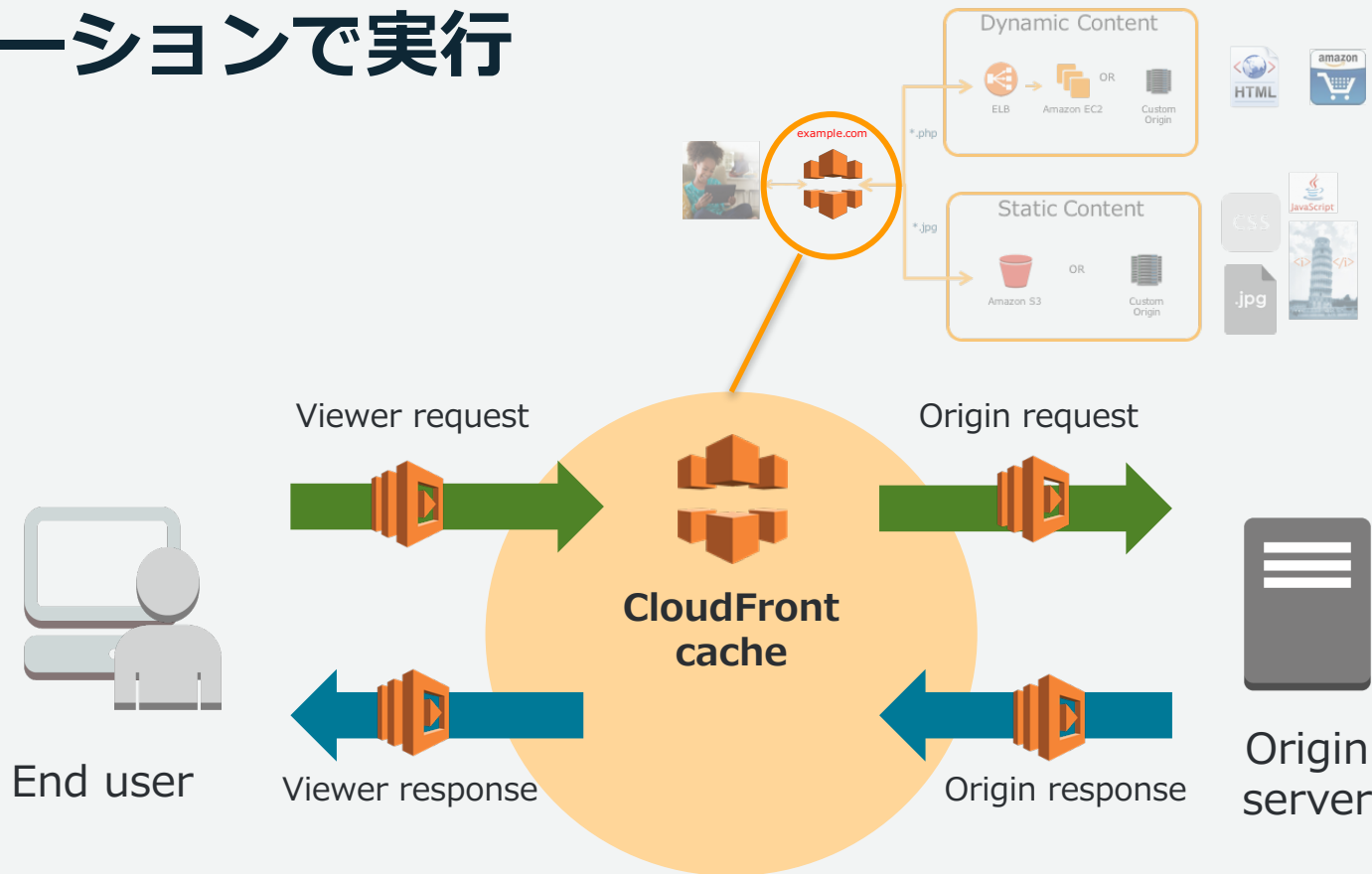
一度コードを書けば、どこでも実行可能



Lambda@Edge は CloudFront エッジロケーションで実行



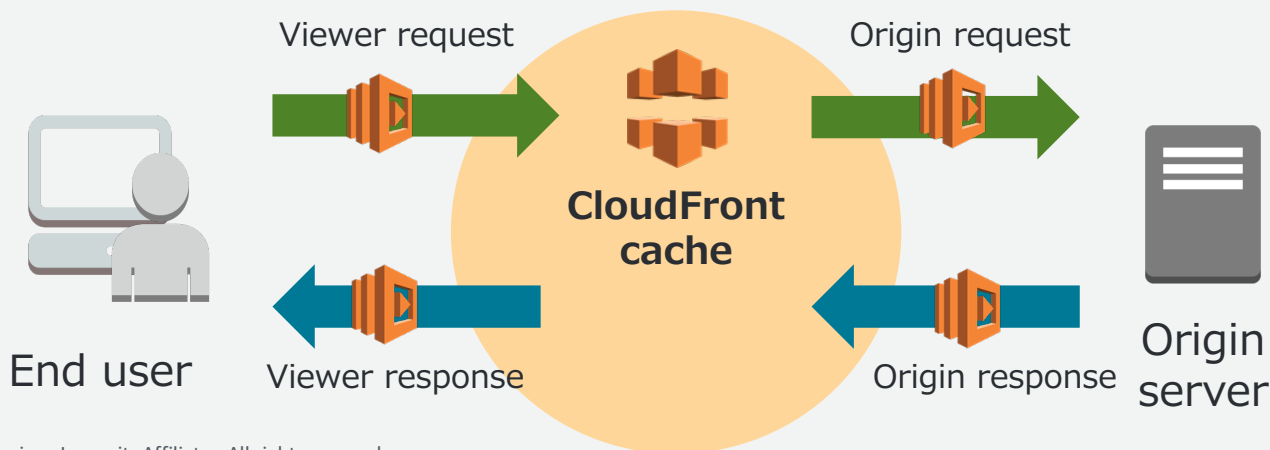
Lambda@Edge は CloudFront エッジロケーションで実行



CloudFront イベント



- Viewer request: リクエストが最初に閲覧者から届いたとき
- Origin request: オリジンへのリクエストを転送するとき
- Origin response: オリジンからの応答を受けるとき
- Viewer response: 閲覧者に応答する前



CloudFront イベントごとの対応機能



VIEWER

- Header 読み取り/書き込み
- URL 読み取り/書き込み
- Response 生成

- Header 読み取り/書き込み
- Request object 読み取り

REQUEST

- Header 読み取り/書き込み
- URL 読み取り/書き込み
- Response 生成
- Network 呼び出し
- 最大実行時間 3 秒

RESPONSE

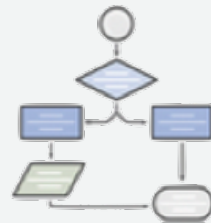
- Header 読み取り/書き込み
- Request object 読み取り
- Network 呼び出し
- 最大実行時間 3 秒

ORIGIN

Lambda@Edge のユースケース

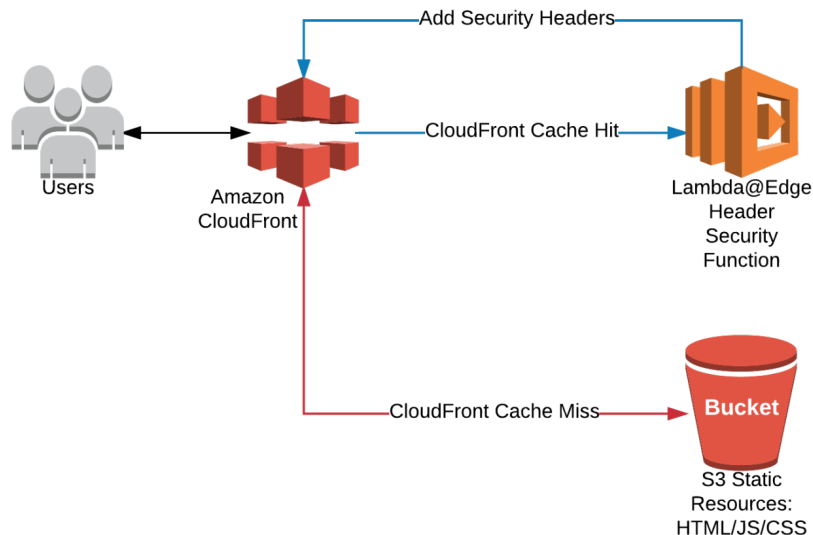


- 高度にパーソナライズされたウェブサイト
- ビューワーリクエストに応じたレスポンス生成
- URL の書き換え
- エッジロケーションでのアクセスコントロール
- リモートネットワークの呼び出し
- A/B テスト





Result: Secure and Scalable JS Delivery



TOZNY



Lambda@Edge Function Code

Node 6.10 Runtime

```
'use strict';
exports.handler = (event, context, callback) => {
  const headers = event.Records[0].cf.response.headers;

  headers['Strict-Transport-Security'] = [{key: "Strict-Transport-Security", value: "max-age=31 ..."}];
  headers['Content-Security-Policy'] = [{key: "Content-Security-Policy", value: "default-src ..."}];
  headers['X-Content-Type-Options'] = [{key: "X-Content-Type-Options", value: "nosniff"}];
  headers['X-Frame-Options'] = [{key: "X-Frame-Options", value: "DENY"}];
  headers['X-XSS-Protection'] = [{key: "X-XSS-Protection", value: "1; mode=block"}];
  headers['Referrer-Policy'] = [{key: "Referrer-Policy", value: "no-referrer"}];

  callback(null, event.Records[0].cf.response);
};
```



Returned HTTP Headers

```
ben — -bash — 102x33
Last login: Wed Aug 9 10:16:04 on ttys001
[ben@Bens-MacBook-Pro:~ $ curl -I https://console.tozny.com
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 2350
Connection: keep-alive
Content-Security-Policy: default-src 'self'; img-src 'self' *.tozny.com data;; script-src 'self' js.st
ripe.com *.tozny.com; style-src 'self' 'unsafe-inline' fonts.googleapis.com fonts.gstatic.com *.tozny.
com; font-src 'self' fonts.googleapis.com fonts.gstatic.com *.tozny.com; object-src 'none'; frame-src
js.stripe.com; connect-src js.stripe.com *.e3db.com; block-all-mixed-content;
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Tozny: We're looking for the kind of people who focus on details - like the headers returned in a se
cure request. Drop us a line: https://tozny.com/hiring/
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Age: 78653
Date: Mon, 17 Jul 2017 18:22:01 GMT
ETag: "9a8364b4600d4788f20d2b64e0110556"
Last-Modified: Mon, 17 Jul 2017 18:17:09 GMT
Server: AmazonS3
x-amz-id-2: nZIH4+nFsF1WExr86QKHmfJBDzL0Mbh8pjea10n8gqW3VH5ZQP0LDZc9p0Spe2+W9zJym06sdY=
x-amz-request-id: 2BA87BE81EF35800
X-Cache: Hit from cloudfront
Via: 1.1 17de248e6d780f737234d37cc490dbe3.cloudfront.net (CloudFront)
X-Amz-Cf-Id: UZjAmaE3y7-Eib0q9S0iZy69XqQZfKfCeFusfyrwMoUyTWGnz0_kFg==

ben@Bens-MacBook-Pro:~ $
```

TOZNY



Mozilla Observatory

OBSERVATORY by mozilla

[HTTP Observatory](#)[TLS Observatory](#)[SSH Observatory \(Beta\)](#)

Scan Summary



Host:	console.tozny.com
Scan ID #:	3980737 (unlisted)
Start Time:	June 23, 2017 3:53 PM
Duration:	77 seconds
Score:	15/100
Tests Passed:	5/11

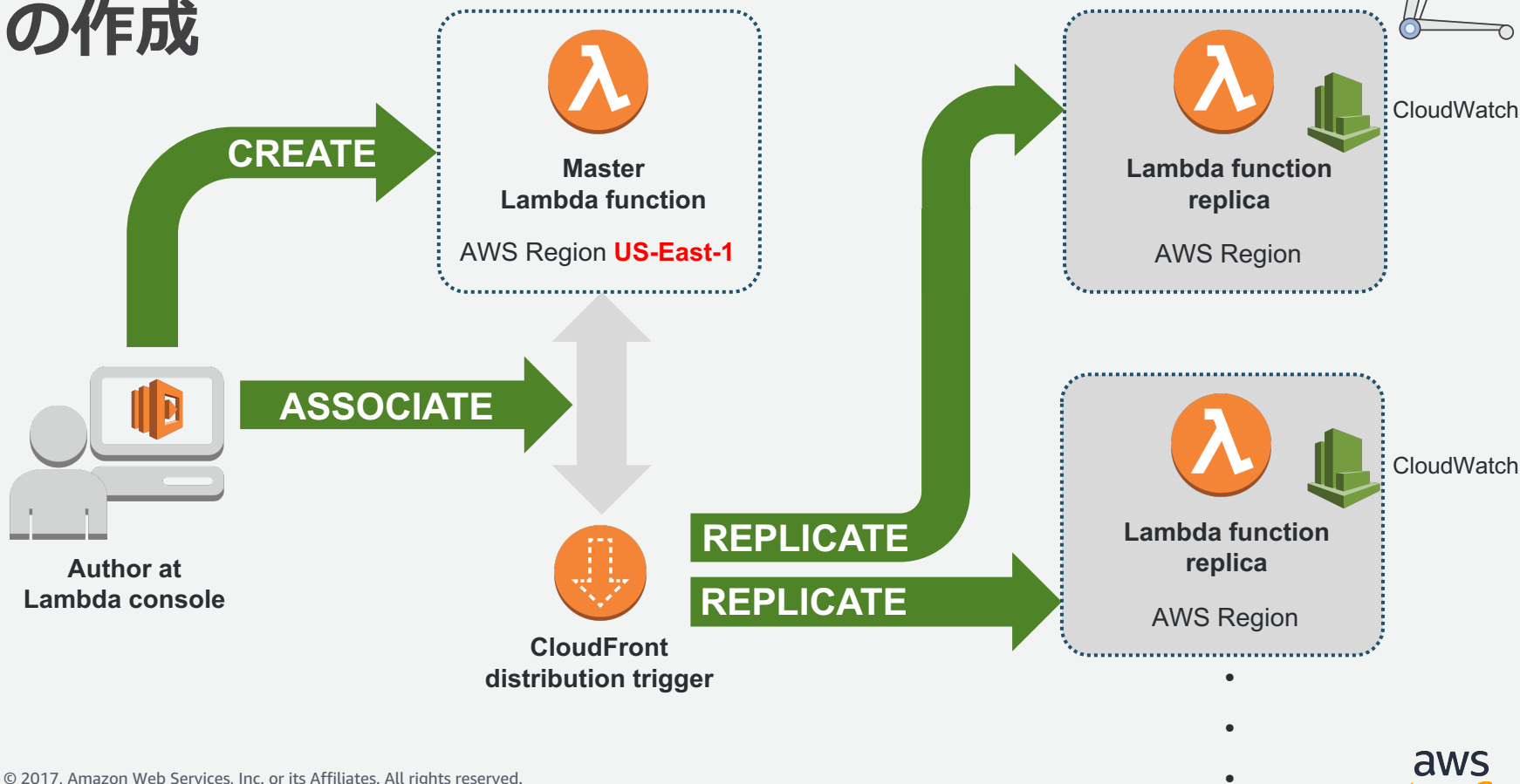
Scan Summary



Host:	console.tozny.com
Scan ID #:	4278570 (unlisted)
Start Time:	August 8, 2017 6:13 PM
Duration:	78 seconds
Score:	100/100
Tests Passed:	10/11

TOZNY

Lambda@Edge 用 Lambda Function の作成



CloudWatch Logs へのログ記録



- console.log()
- console.error()
- console.warn()
- console.info()

Lambda用ロールへの信頼関係を追加

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "edgelambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```



Lambda@Edge 実行環境



	Origin facing	Viewer facing
ランタイム	Node.js 6.10	←
メモリ	128 MB	←
最大実行時間	3 seconds	1 second
デプロイパッケージサイズ (zip/jar圧縮前)	1 MB	←
ネットワーク呼び出し	Yes	No
レスポンスサイズ (request events)	256 KB	40 KB
同時実行数のデフォルト (Region毎) ※上限緩和可能	1,000	←
/tmp, 環境変数, DLQ, VPC, X-Ray	使用不可	←

まとめ

まとめ

Amazon CloudFrontを活用することで

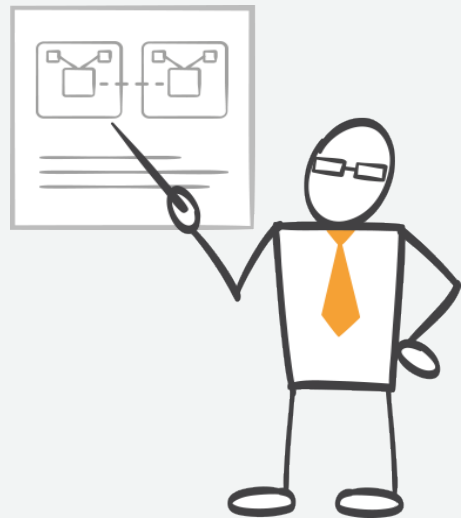
- 簡単にサイトの高速化とスケーラビリティを実現可能
- 動的コンテンツへの対応も可能
- プレミアムコンテンツもセキュアに配信
- レポート機能でアクセス傾向分析も可能
- いつでも、すぐに利用できる CDN サービス



まとめ

AWS Lambda@Edge は

- CloudFront イベントに応じて **AWS エッジロケーション**で **Lambda 関数を実行**
- パーソナライズ、レスポンス生成、URL書き換え、アクセスコントロール、リモートネットワーク呼び出し、A/Bテスト等、**多様なユースケース**



参考資料

Amazon CloudFront

- Amazon CloudFront 開発者ガイド
http://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/Introduction.html
- Amazon CloudFront よくある質問
<http://aws.amazon.com/jp/cloudfront/faqs/>
- Amazon CloudFront の料金表
<http://aws.amazon.com/jp/cloudfront/pricing/>

AWS Lambda@Edge

- AWS Lambda@Edge 開発者ガイド
http://docs.aws.amazon.com/ja_jp/lambda/latest/dg/lambda-edge.html
- Lambda@Edge よくある質問
<https://aws.amazon.com/jp/lambda/faqs/#edge>
- Lambda@Edge の料金詳細
<https://aws.amazon.com/jp/lambda/pricing/#edge>

Appendix

CloudFront 料金モデル

①データ転送アウト(GBあたり)

	米国	ヨーロッパ	香港,フィリピン,韓国, シンガポール,台湾	日本	南米	オーストラ ラリア	インド	予約容量の 価格
最初の 1 0 TB/月	\$0.085	\$0.085	\$0.140	\$0.140	\$0.250	\$0.140	\$0.170	問い合わせ
次の40TB/月	\$0.080	\$0.080	\$0.135	\$0.135	\$0.200	\$0.135	\$0.130	問い合わせ
次の100TB/月	\$0.060	\$0.060	\$0.120	\$0.120	\$0.180	\$0.120	\$0.110	問い合わせ
次の350TB/月	\$0.040	\$0.040	\$0.100	\$0.100	\$0.160	\$0.100	\$0.100	問い合わせ
次の524TB/月	\$0.030	\$0.030	\$0.080	\$0.080	\$0.140	\$0.095	問い合わせ	問い合わせ
次の4PB/月	\$0.025	\$0.025	\$0.070	\$0.070	\$0.130	\$0.090	問い合わせ	問い合わせ
次の5PB/月以上	\$0.020	\$0.020	\$0.060	\$0.060	\$0.125	\$0.085	問い合わせ	問い合わせ

②リクエスト(10,000件あたり)

	米国	ヨーロッパ	香港,フィリピン,韓国, シンガポール,台湾	日本	南米	オーストラ ラリア	インド	予約容量の 価格
HTTPリクエスト	\$0.0075	\$0.0090	\$0.0090	\$0.0090	\$0.0160	\$0.0090	\$0.0090	問い合わせ
HTTPSリクエスト	\$0.0100	\$0.0120	\$0.0120	\$0.0120	\$0.0220	\$0.0125	\$0.0120	問い合わせ

③専用IP 独自 SSL 証明書

Distributionに関連付けられた証明書1通につき、月\$600 ※SNIの場合は不要

④オリジンへのデータ転送アウト (GB あたり)

	米国	ヨーロッパ	香港,フィリピン,韓国, シンガポール,台湾	日本	南米	オーストラ ラリア	インド	予約容量の 価格
全てのデータ転送	\$0.020	\$0.020	\$0.060	\$0.060	\$0.125	\$0.100	\$0.160	問い合わせ

⑤ CloudFront へのデータ転送アウト (GB あたり)

別の AWS リージョンまたは Amazon CloudFront、\$0.000

⑥無効リクエスト

最初の 1,000 ファイルまで追加料金なし。それ以上はリクエスト毎に \$0.005

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



2017 年 9 月時点



CloudFront 料金クラス

Price Class を指定することで、安価なエッジロケーションのみを利用した配信が可能

- Price Class の変更により、ユーザへの配信速度に影響が出る可能性があるため利用の際は注意が必要

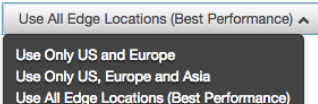
料金クラス All	料金クラス 200	料金クラス 100
米国	米国	米国
カナダ	カナダ	カナダ
欧州	欧州	欧州
香港、フィリピン、韓国、シンガポールおよび台湾	香港、フィリピン、韓国、シンガポールおよび台湾	
日本	日本	
インド	インド	
南米		
オーストラリア		

Distribution Settings

Price Class: Use All Edge Locations (Best Performance) 

Alternate Domain Names (CNAMEs) 

SSL Certificate: Default CloudFront Certificate (*.cloudfront.net)





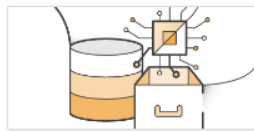
Q&A



オンラインセミナー資料の配置場所

AWS クラウドサービス活用資料集

- <http://aws.amazon.com/jp/aws-jp-introduction/>



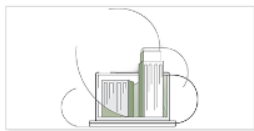
サービス別資料

無料オンラインセミナー「Black Belt Online Seminar」のサービスカット資料他、AWSのTechメンバーによる各サービスの解説資料がご覧いただけます。



ソリューション別資料

無料オンラインセミナー「Black Belt Online Seminar」のソリューションカット資料他、特定のソリューションについてのAWS活用方法がご覧いただけます。



業種別資料

無料オンラインセミナー「Black Belt Online Seminar」のインダストリーカット資料他、特定の業界のユースケースがご覧いただけます。



その他の資料

イベントに関する資料やアップデート情報などがご覧いただけます。

AWS Solutions Architect ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています
- <http://aws.typepad.com/sajp/>

AWSの導入、お問い合わせのご相談

AWSクラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は以下のリンクよりお気軽にご相談ください

<https://aws.amazon.com/jp/contact-us/aws-sales/>

お問い合わせ

日本担当チームへのお問い合わせ >

関連リンク

フォーラム

日本担当チームへのお問い合わせ

AWS クラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。

※ご請求金額またはアカウントに関する質問は[こちらからお問い合わせください](#)。

※Amazon.com または Kindle のサポートに問い合わせは[こちらからお問い合わせください](#)。

アスタリスク（*）は必須情報となります。

姓*

名*

※「AWS お問い合わせ」で検索してください

ご参加ありがとうございました

