Movable Type 7 で実現する
エンタープライズ向けのシステム構成

株式会社COLSIS
執行役員CTO 永谷 理

プロフィール

- 株式会社COLSIS
  執行役員CTO 永谷 理

- 2000年から地元北海道でWEB関連のディレクションや制作に関わる。2006年から東京にてECサイトやポータルサイトのサーバーサイドエンジニアとして大規模トラフィックを扱う技術を経験。現在はコルシス札幌支社に勤務しエンタープライズ系インフラ構築や、ECサイトなどのシステム開発に従事。

本日のアジェンダ

- サーバ運用
- オンプレミスのサーバ構成
- コンテンツ配信
- セキュリティ
- クラウドでのサーバ構成
- SmartSync Packのご紹介
- 事例のご紹介
- まとめ

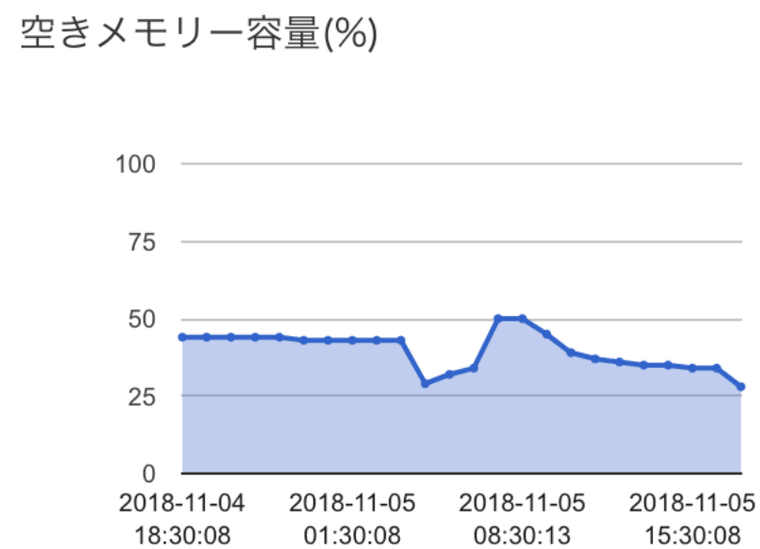
サーバ運用について

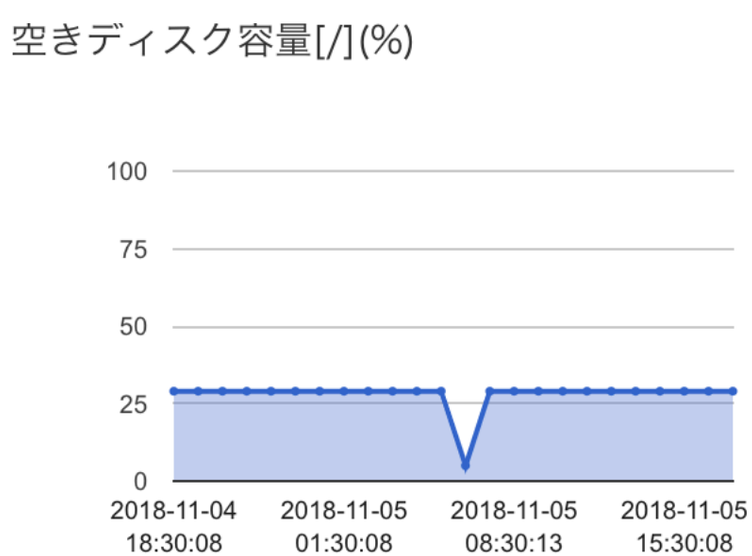
サーバ運用について

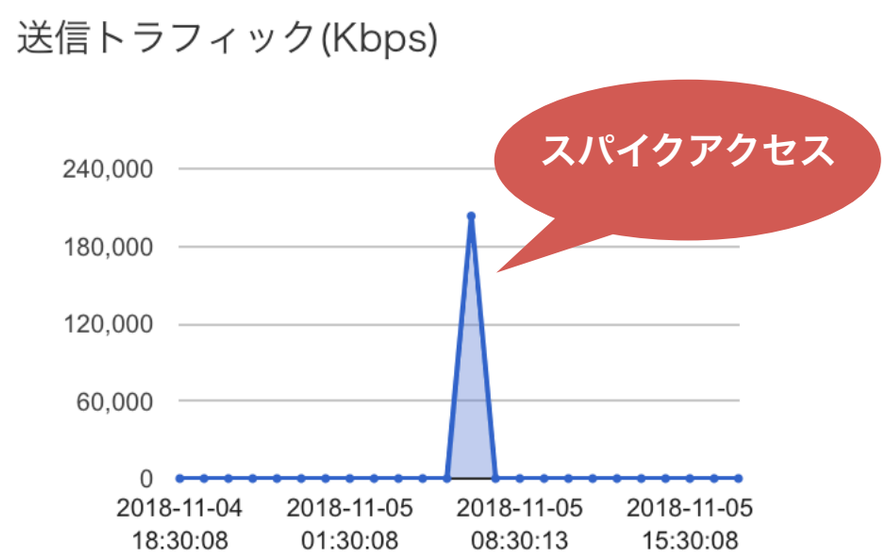
- 監視とは
  - Webサイトは24/365で異常の無い状態にしたい
  - 可動は可能な限り100%に近づけたい
  - 但し100%の構成は不可能
    - 例えばAzure Virtual Machinesでは99.9%のSLAになっています
  - 落ちる事を前提に監視を実施する
    - 異常系を検知し適切に対応する必要がある

監視

- リソース監視
  - 異常事態になる前に兆候を検知し事前に対応する







COLSIS

主な監視ポイント

種別	監視項目	備考
URL監視	ステータス監視	正常にコンテンツが取得できるのか、Webサーバを外部から監視する
リソース監視	メモリー	メモリーが足りているのか残容量を監視
	ロードアベレージ	サーバの処理が混み合っているのかの指標
	ディスク容量監視	ディスクが足りているのか残容量を監視
ログ監視	httpステータス監視	500ステータスなどの異常値を監視
	syslogの監視	sshへの不正アクセスなどを監視
ポート監視	80番ポートなど	apacheやpostfix等のサーバソフトウェアの監視
DB監視	データベースサーバ	コネクション、slow queryなどの監視

監視の問題

- 閾値が低すぎると見逃してしまう
  - 閾値を低く設定したためにアラートが沢山送信されてしまい、それが常習化することによって見逃してしまうケースも
- 監視項目が多い
  - 監視ポイントを増やす事でもれなく検知できるが、敷居と同じく見逃してしまう事も
- バランスを取り適切な設定をする事が必要です

バックアップ

- もしもの時にロールバック可能な状態にする
- 対象
  - データベース
  - コンテンツ
  - ログ
  - スナップショット（仮想環境のみ可能）
- 保存先
  - クラウドのオブジェクトストレージ（Azure Storage,AWS S3, GCP Storageなど）
  - サーバ内
  - 別サーバ内
- 頻度
  - 1日毎、1週間毎など

ロールバック

- スナップショット
  - サーバーの完全なロールバックが可能
  - すべてのデータがバックアップ時点にロールバックされてしまうため単一ファイルの修正などを行う場合は不便
- データベース
  - レプリケーションを行う事で、秒単位でのロールバックも可能
- コンテンツ
  - ファイル単位でのレストアが可能
  - サーバが破損した場合はコンテンツだけでは復旧はできない

COLSIS

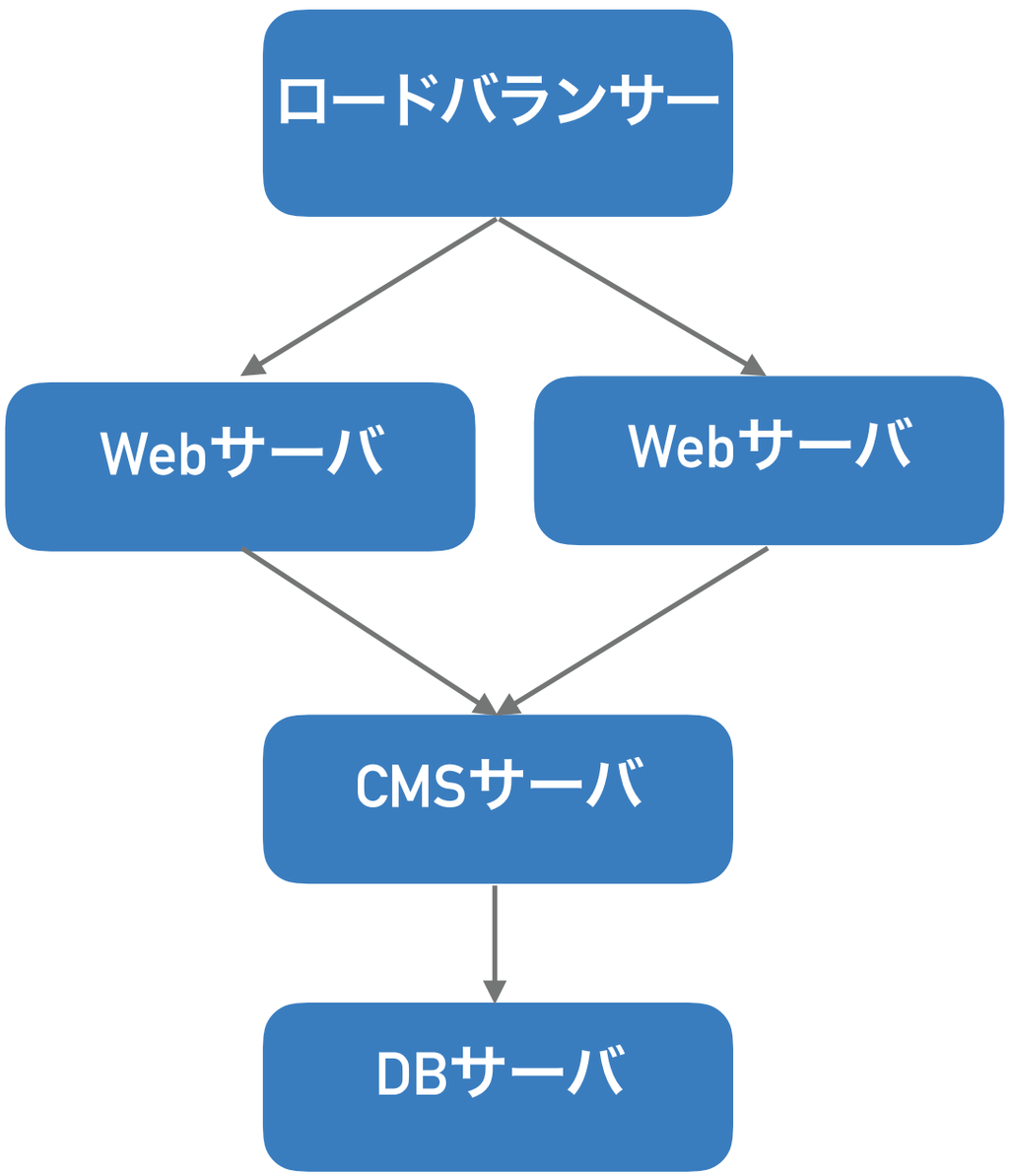
バックアップのまとめ

- バックアップローテーションの頻度は細かい方が良い
- 長い期間保持する方が良い
  - GWなど長期休み中に不具合があり、気がついた時にはバックアップが意味の無い場合も
- バックアップの種類は多いほうが良い
  - スナップショット、DBサーバの冗長化、クラウドストレージへの各種バックアップの保存

オンプレミスのサーバ構成について

従来の構成

➤ オンプレミス



- ハードウェアロードバランサー

  アクセスを各サーバに均等に割り振る

  とても高価

  *SSL*アクセラレーションを行う事も

- *Web*サーバ

  物理サーバとして設置

  設定ミスの場合ロールバックが難しい

  ハードウェアの故障を担保する必要がある

  保守が大変

- *CMS*サーバ

  *Movable Type*を設置するサーバ

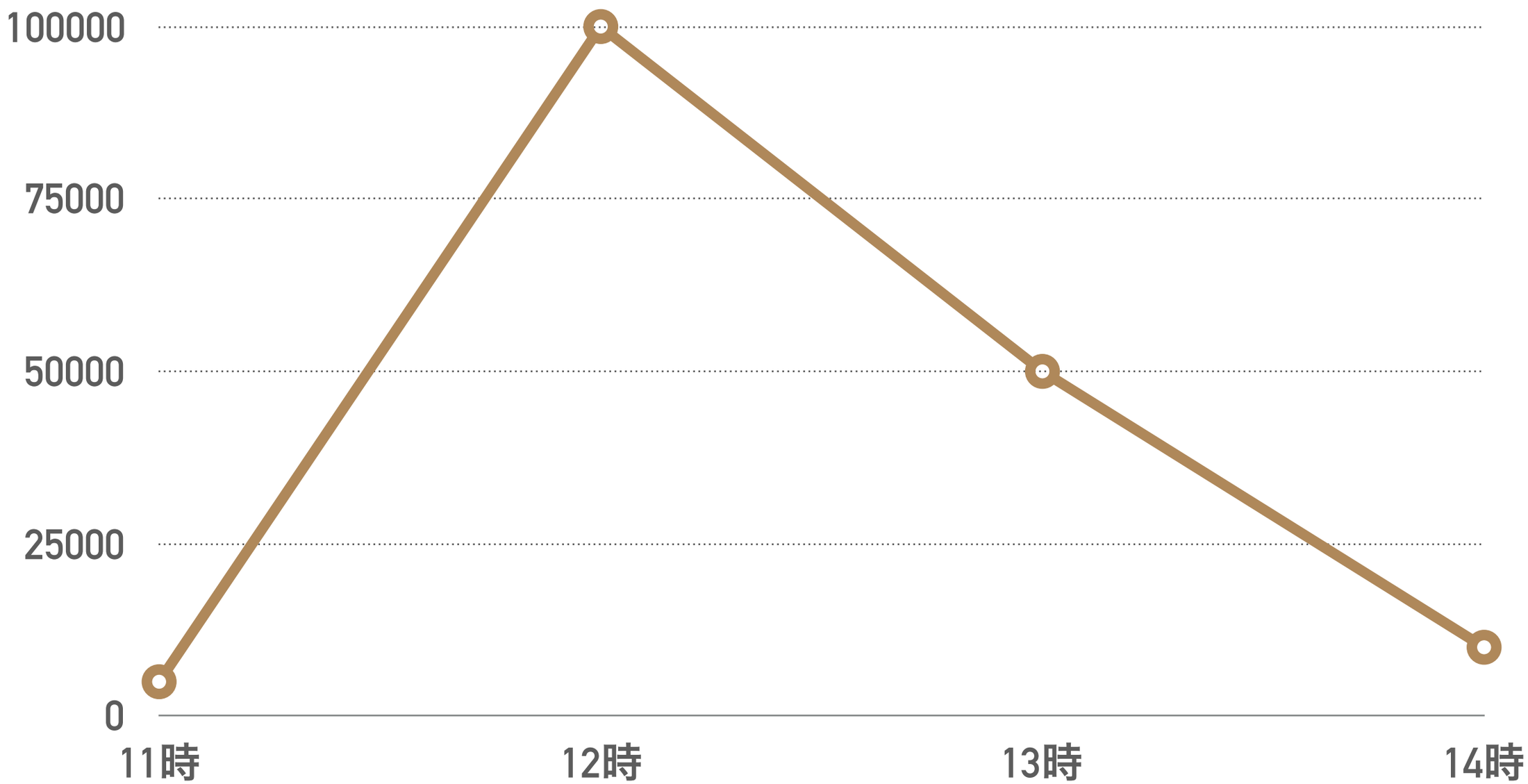
  特にセキュリティに気をつける必要がある

- *DB*サーバ

  *SQL*サーバや*MySQL*サーバを機動し*CMS*などのデータを格納する

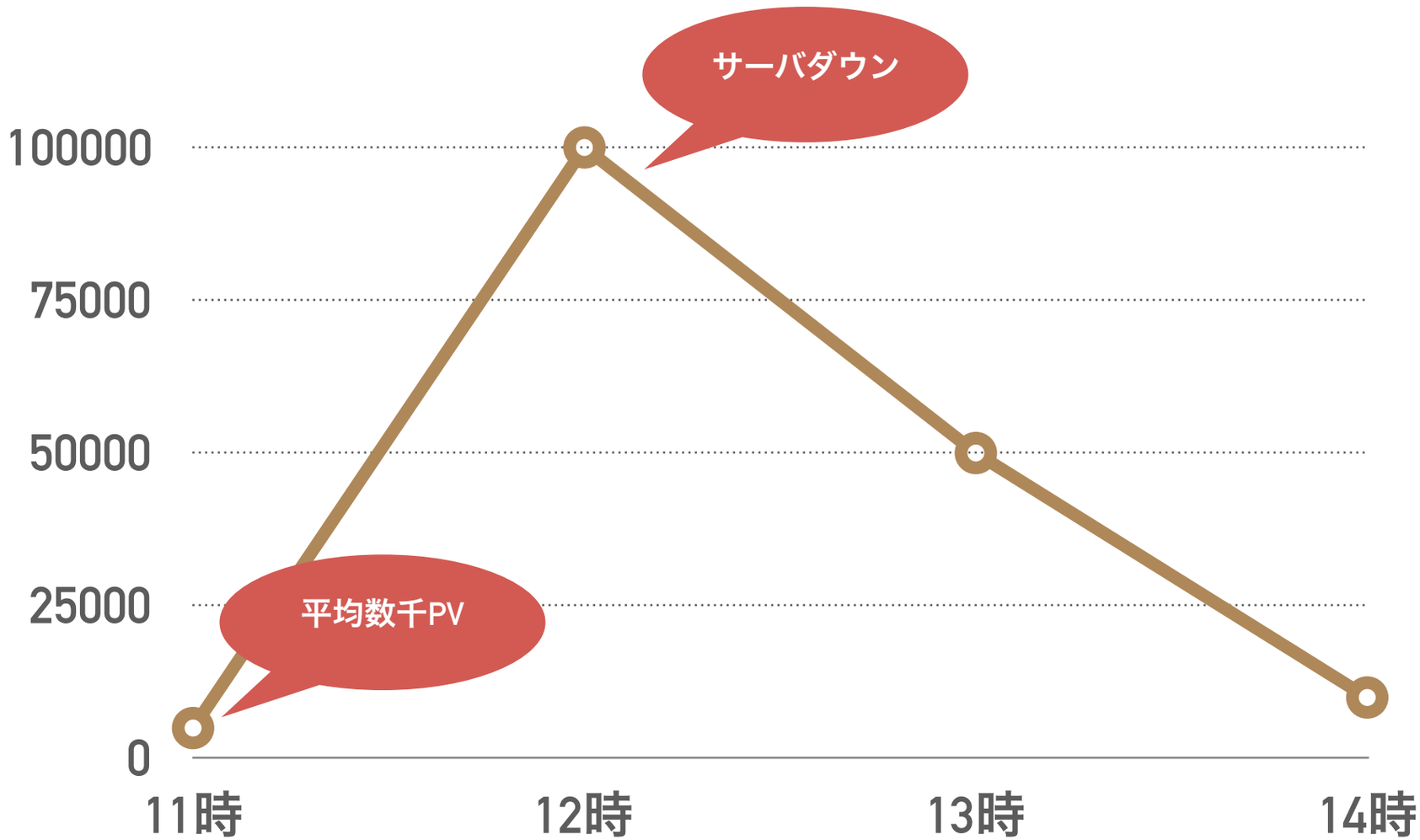
スパイクアクセス

- Yahoo、LINE、TV番組、、、での紹介



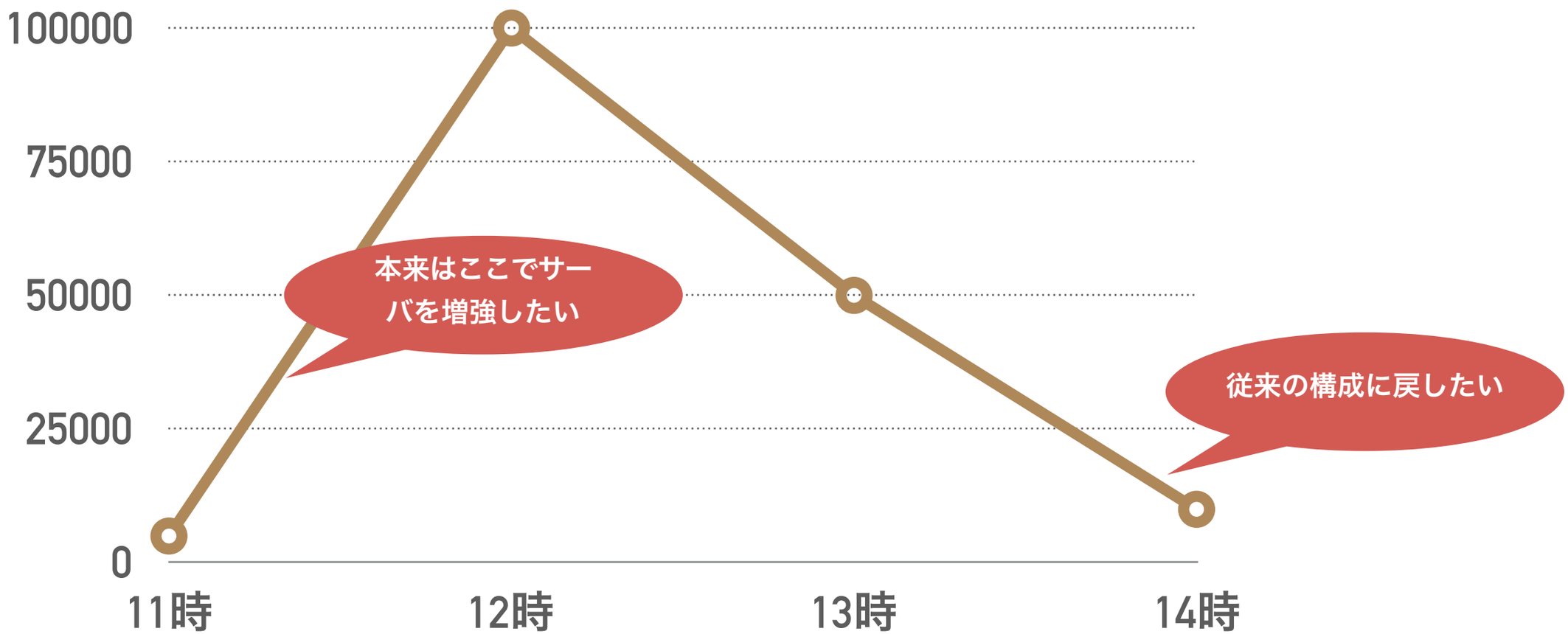
サイジング

- オンプレミスだとスパイクアクセスの対応ができず、サーバダウンが考えられる。平常時では利用されないスペックにサイジングする事が多い



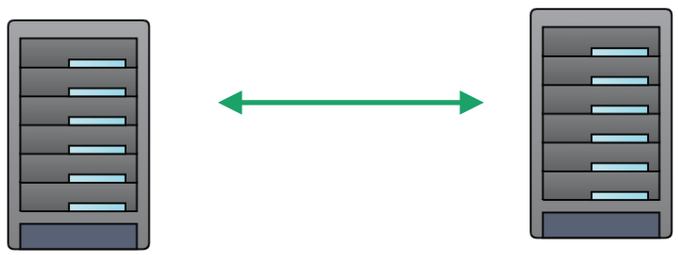
オンプレミスの限界

- ハードウエアで構成されるためラックの余りや、契約の上限など様々な問題で柔軟に構成を変える事はできない



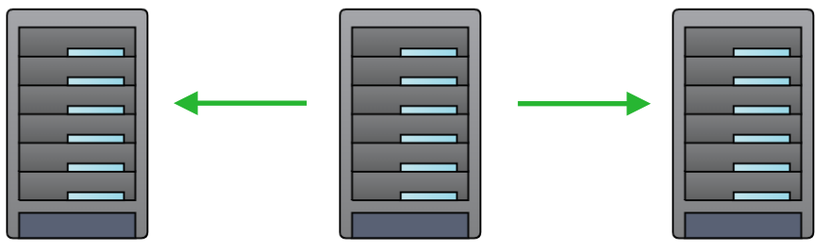
クラウドでは

- 柔軟なリソースコントロールが可能
  - スケールアップ/ダウン、スケールアウト
- オートスケールによる動的コンテンツのスパイク対策
- 従量課金によって常に低コストで利用可能



1コア・1Gメモリ　　*4コア・4Gメモリ*

スケールアップ



オートスケールなどで台数を調整

スケールアウト

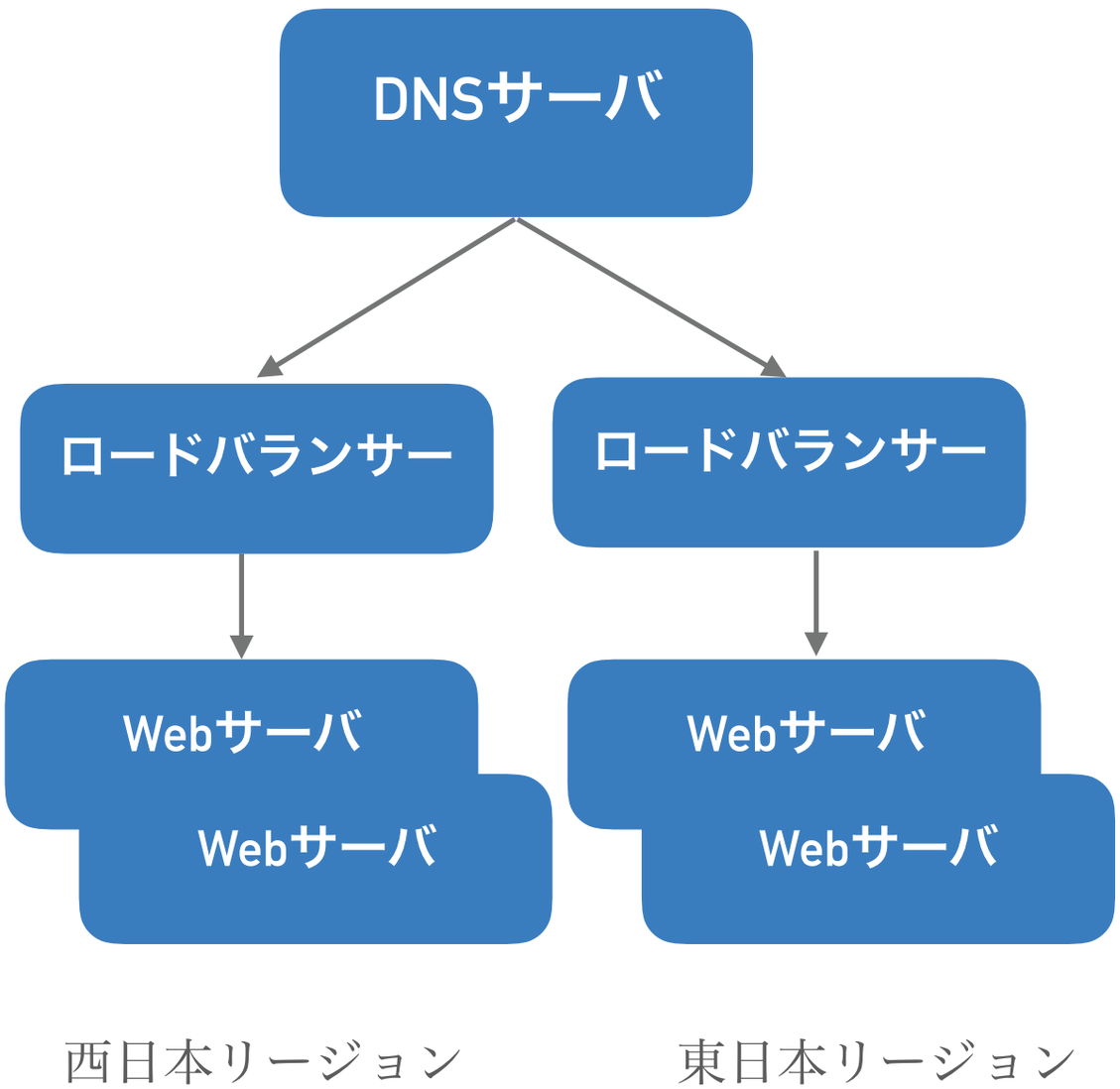
BCP / DRとは

- BCP
  Business Continuity Plan / 事業継続計画

- DR
  Disaster Recovery / 災害復旧

BCP / DR対策

➤ 地域を分けて複数のデータセンターにサーバを分散する

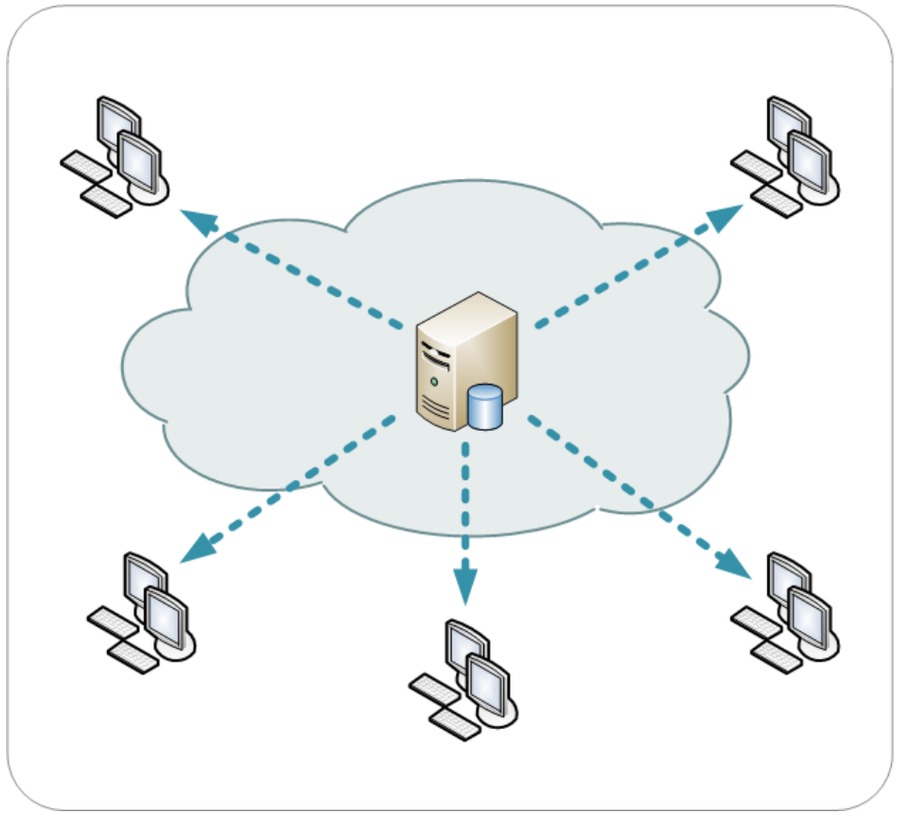


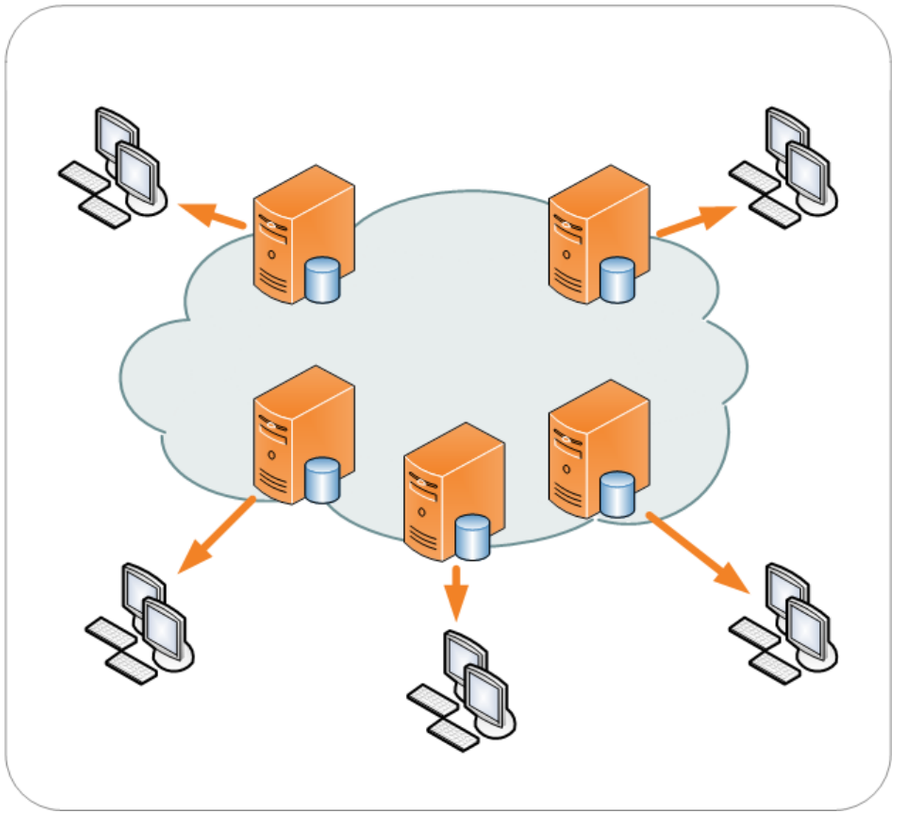
- *DNS*サーバ
  災害時には正常可動しているデータセンターへ*DNS*を切り変える
- データセンター
  複数データセンターでの運用となるためデータ同期が難しい
  オンプレでは*DRBD*+*Pacemaker*、*MySQL*レプリケーションなどを利用して構築する
- クラウド
  *Azrure Site Recovery*など、複数リージョンにコピーを設置する事で自動的に参照先を切り替える

コンテンツ配信について

CDNとは

- コンテンツデリバリネットワーク(英: content delivery network、CDN)とは、ウェブコンテンツをインターネット経由で配信するために最適化されたネットワークのことである。コンテンツ配信網とも。 (wikipediaから引用)





CDNのキャッシュを利用する事でスパイクアクセス対策を

CDNの製品について

➤ 以下のように各社から製品が出荷されています

開発元	製品名
Azure	Azure CDN
AWS	CloudFront
GCP	Cloud CDN
Akamai Technologies	Akamai

CDN導入について

- 新規サイトでは導入はほぼ必須
  - クラウドであれば転送料金が安くなる事も
- 既存サイトへの導入には注意が必要
  - 動的コンテンツはキャッシュすると個人情報の漏洩リスクも
  - 静的出力されたコンテンツのみキャッシュするなど工夫が必要

Movable Typeは静的にコンテンツを出力するのでCDNとの相性が良い

セキュリティについて

日々脆弱性は発見されています

JVN Japan Vulnerability Notes

最終
Engl

RSS に掲載する URL に関するお知らせ

新着リスト

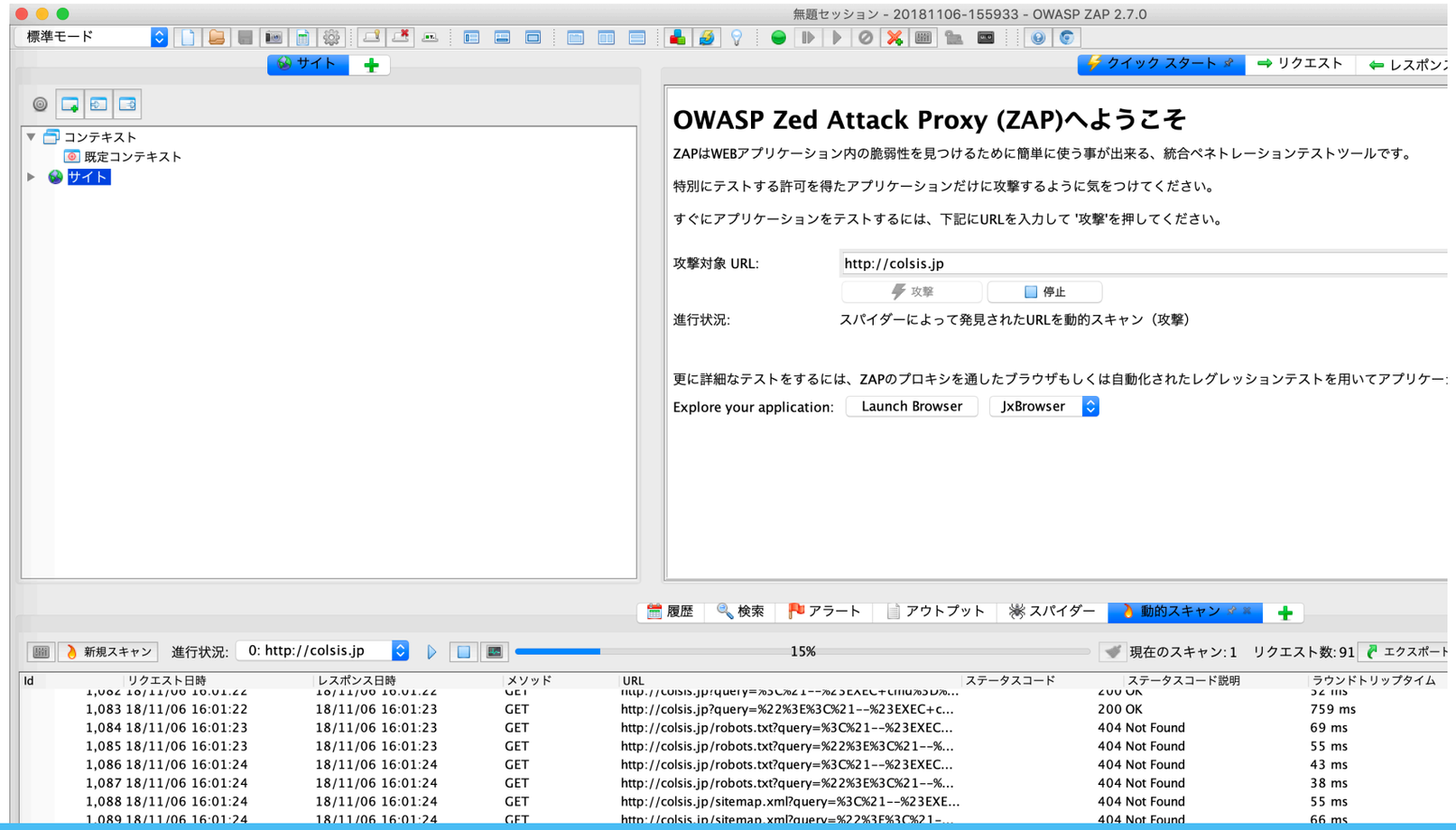
RSS

JVNVU#93295516:	Apache Struts2 に任意のコードが実行可能な脆弱性 [2018/11/06 11:50]（更新）
JVNVU#93409761:	IKEv1 のメインモードに総当たり攻撃に対する脆弱性 [2018/11/06 11:50]（更新）
JVNVU#93502675:	OpenSSL に複数の脆弱性 [2018/11/06 11:50]（更新）
JVNVU#91991349:	Apache Tomcat の複数の脆弱性に対するアップデート [2018/11/06 11:50]（更新）
JVNVU#98416507:	Apache HTTP Web Server における複数の脆弱性に対するアップデート [2018/11/06 11:50]（更新）
JVNVU#90211511:	Apache Tomcat の複数の脆弱性に対するアップデート [2018/11/06 11:50]（更新）
JVNVU#92830136:	OpenSSL に複数の脆弱性 [2018/11/06 11:50]（更新）
JVNVU#99304449:	Apache HTTP Web Server 2.4 における複数の脆弱性に対するアップデート [2018/11/06 11:50]（更新）
JVNVU#92250735:	Apache Tomcat の複数の脆弱性に対するアップデート [2018/11/06 11:50]（更新）
JVNVU#96365720:	複数の Apple 製品における脆弱性に対するアップデート [2018/11/05 12:50]
JVNVU#93926212:	Cisco ASA および FTD の SIP インスペクション機能におけるサービス運用妨害 (DoS) の脆弱性 [2018/11/02 15:30]
JVNVU#98767431:	Texas Instruments 製マイクロコントローラ CC2640 および CC2650 にバッファオーバーフローの脆弱性 [2018/11/02 15:00]
JVN#75738023:	WordPress 用プラグイン Event Calendar WD におけるクロスサイトスクリプティングの脆弱性 [2018/11/02 12:00]

サーバ内部は常に最新の状態にする必要があります

OWASPによる診断

- 定期的なサーバの脆弱性診断が重要になります
  - システムを作っても故意ではないミス（脆弱性）は気がつきにくい



OSSであるOWASP以外にも沢山の脆弱性検査ツールがあります

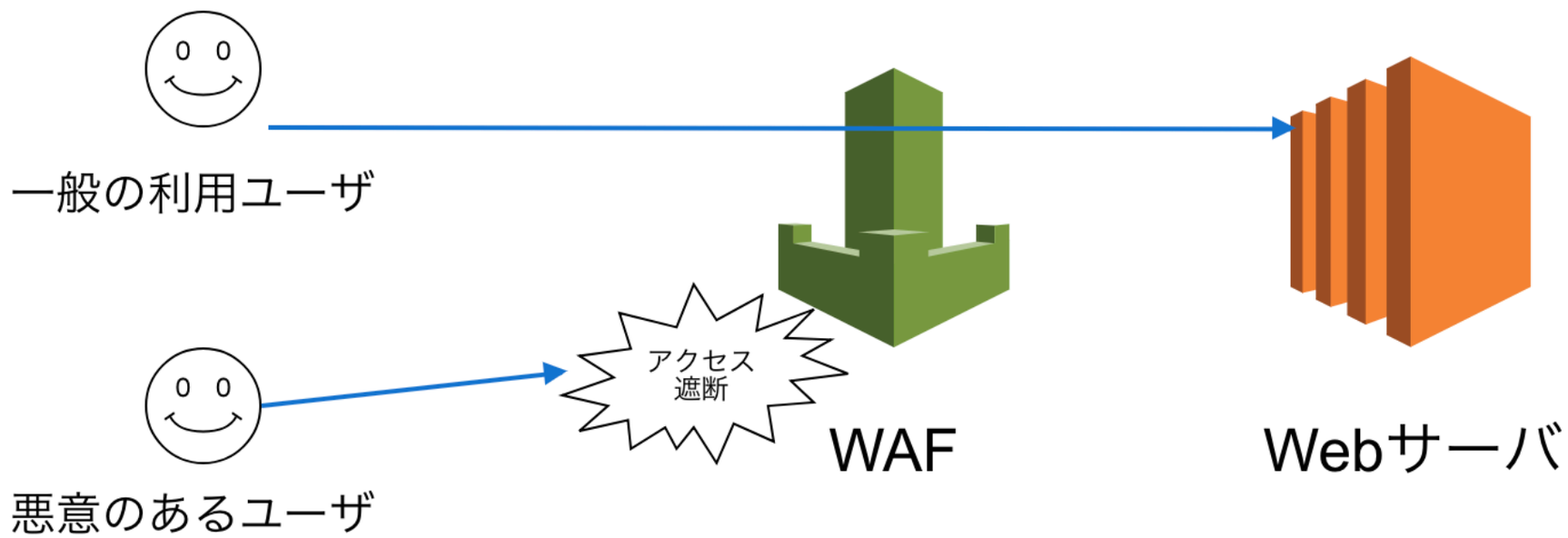
サーバーとシステムの保守

- 脆弱性情報を適切に処理する
  - 脆弱性情報の緊急度を確認し、システムへの影響度から適用タイミングを調整する
- 必ずステージングサーバーで確認してからシステムのアップデートを行う。CMSなどはバージョンアップにより不具合が出るケースも
- 可能な限り24/365の保守を検討した方が良い

ロードバランサーを導入する事で、アップデート後正常に動く事を確認してからサーバを切り替える事も可能

WEB APPLICATION FIREWALLとは

- ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護するセキュリティ対策の一つ。 WAFを導入するウェブサイト運営者は、検出パターンを設定することで、ウェブサイトとウェブサイト利用者との間の通信の内容を機械的に検査する (wikipediaから引用)



SQLインジェクション・クロスサイトスクリプティング
コマンドインジェクションなどからWebサイトを保護します

WAFの製品について

➤ 以下のように各社から製品が出荷されています

開発元	製品名
Azure	Application Gateway
AWS	AWS WAF
GCP	Cloud Armor
サイバーセキュリティクラウド	攻撃遮断くん
セキュアスカイ・テクノロジー	Scutum
Trend Micro	Deep Security

WAF導入について

- 新規サイトでは導入はほぼ必須
  - Webサイト側に問題があっても事前に遮断する事が可能
  - ゼロディ攻撃など、脆弱性を解消する手段が存在しない場合でも防げる場合も
- 既存サイトへの導入には注意が必要
  - 悪意の無いクエリーが誤検知され、Webシステムなどが動かなくなる可能性も

十分に検証を行ってから導入する必要がある

クラウドでのサーバ構成について

最小限のサーバ構成

➤最小限のサーバ構成

➤Webサーバ：Aapche,Nginx

➤DBサーバ：MySQL,SQLサーバ

➤CMS：Movable Type 7

一般的なコーポレートサイトなどでは問題の無い構成であるが、色々と不安の残る構成になります。

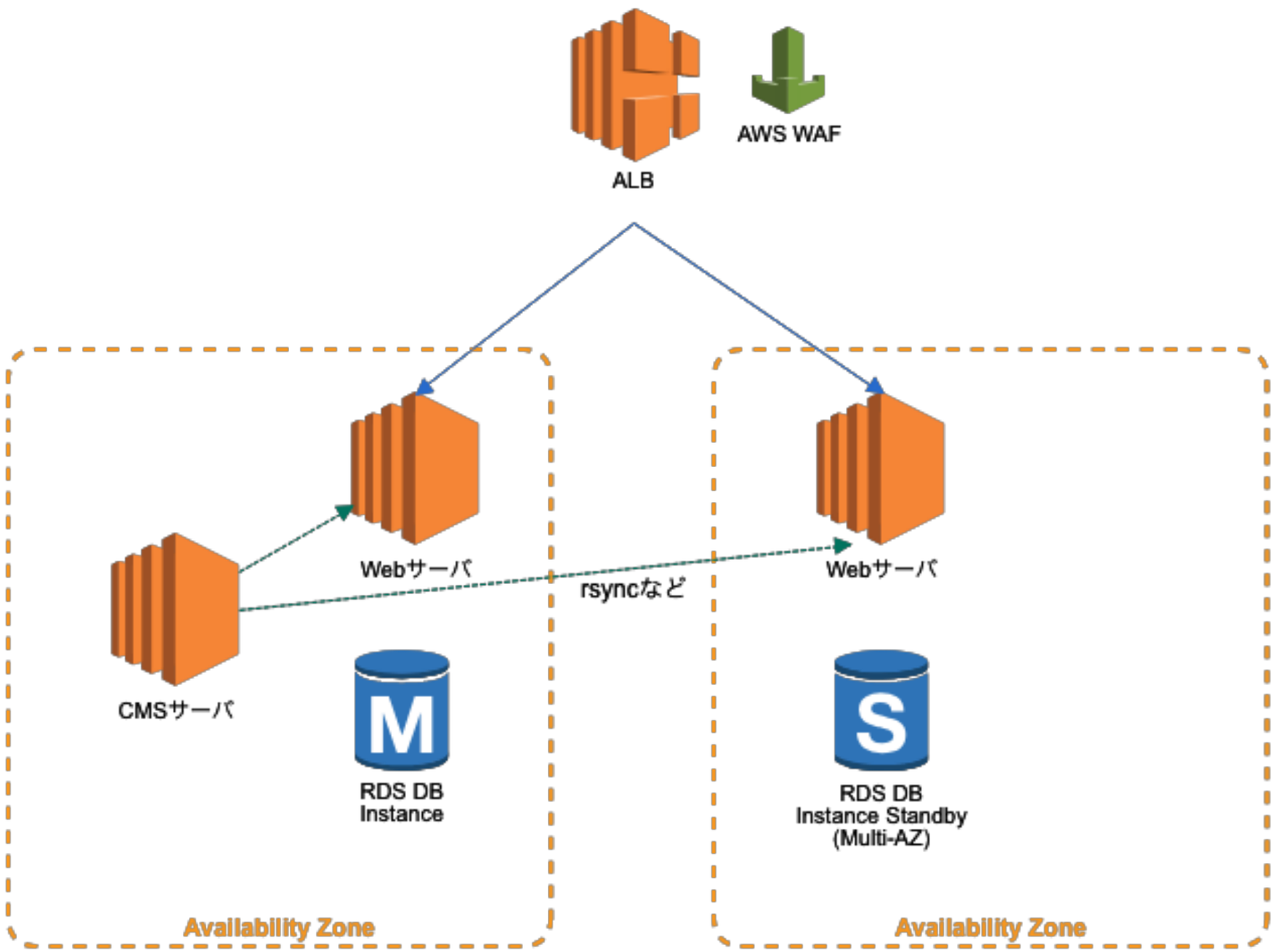
項目	内容
Firewall	セキュリティグループを利用して、適切なポートのみ開放する
スパイク対策	MT7では静的にコンテンツを出力するため大抵は問題ないが不安が残る
DB	Web/CMSとDBサーバが分離されていないのでセキュリティも不安
DR/BCP	1台構成なのでサーバダウンした場合にサイトが停止します
SSL	常時SSLの場合は処理速度が10分の1程度まで下がります

セキュリティに考慮したサーバ構成

*ALB*を前段に設置し、*WAF*を設置する事でセキュリティを向上し、さらに*DB*を*RDS*として切り離す事で情報漏えいリスクを軽減しています。

項目	内容
Firewall	前段にALBを導入したのでWebサーバへの直接アクセスがなくなりました。
スパイク対策	MT7では静的にコンテンツを出力するため大抵は問題ないが不安が残る
DB	RDSとして分離する事でセキュリティも向上
DR/BCP	1台構成なのでサーバダウンした場合にサイトが停止します
SSL	ALBでSSLターミネーション（復号化）を行う事でWebサーバの負荷を軽減

冗長性を考慮したサーバ構成



COLSIS

冗長性を考慮したサーバ構成

ALB配下にWebサーバ2台を冗長化して設置し、DBサーバもMultiAZで分離しています。CMSサーバを分離した事でCMSサーバへのアクセスをIPで完全に遮断できるようになりました。なお、サーバが増えましたがクラウドのログ収集システムを利用することでログを集約する事が可能です。

CMSサーバとWebサーバを分離したので、CMSサーバから静的に出力したコンテンツをWebサーバに設置しないといけません、今回は弊社商品であるSmartSync Packを利用しています。要はCMSサーバからrsync等でコンテンツを複数サーバへコピーしています。

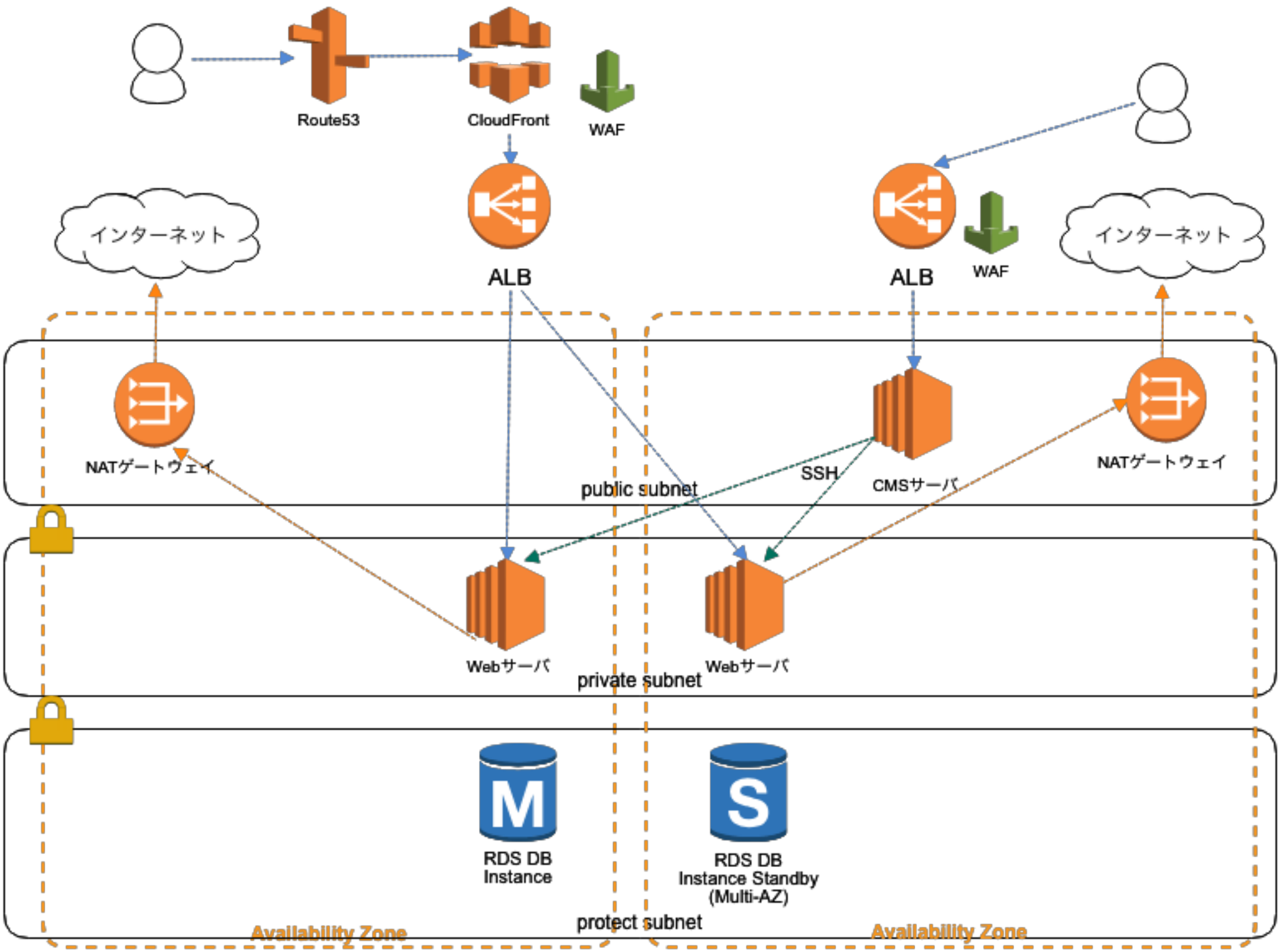
項目	内容
スパイク対策	冗長化されましたが、まだ不安が残ります
DB	RDSを冗長化したので、1台がダウンしてもサービスを継続可能です
DR/BCP	Web/DBは冗長化されましたので、基本的に問題ないと言えるでしょう

準サーバーレス構成

*CloudFront*と*S3*を利用しているので、セキュリティ・スパイクアクセスがほぼ完璧な構成です。但し、*S3*では柔軟なリダイレクトや動的コンテンツが動かないので注意が必要です。

項目	内容
CMSサーバ	MT7を動かすためのCMSサーバは必要になりますので完全なサーバーレスはできない
CloudFront	CDNを導入しているので、スパイアクセスもまったく問題ありません
S3	SLAが、99.999999999%なのでサービスダウンはほぼ無いと考えて良いでしょう

エンタープライズ向けの構成



冗長性を考慮したサーバ構成

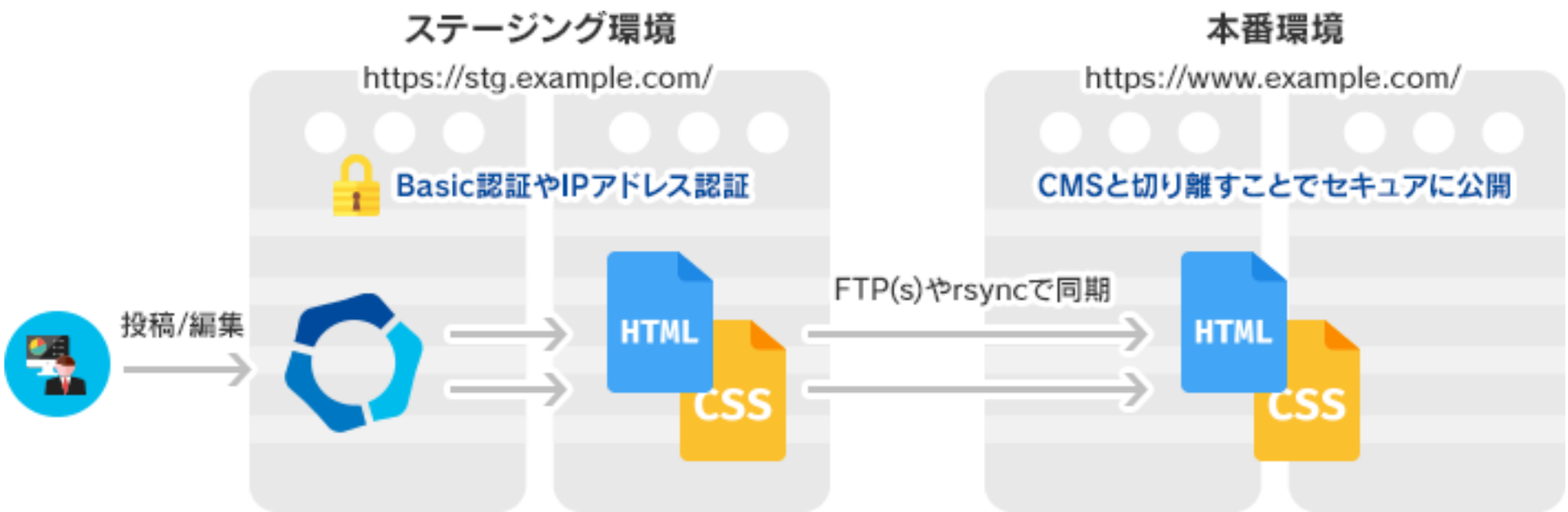
- CloudFront(CDN)を設置します。これによりオリジンサーバ（Webサーバ）への負荷がなくなった上にCloudFrontのおかげでスパイクアクセス、セキュリティともに向上が見込めます。ネットワークも見直しを行いWebサーバはElasticIPを付与せずに外部から見えない場所に設置します。この場合サーバから外部にアクセスできなくなるためAWSのマネージドNATゲートウェイを利用します(CMSサーバをNATインスタンスとして利用する事も可能)。CMSサーバもALB下に配置する事で安心感が向上されました

SmartSync Packのご紹介

SMARTSYNC PACKについて

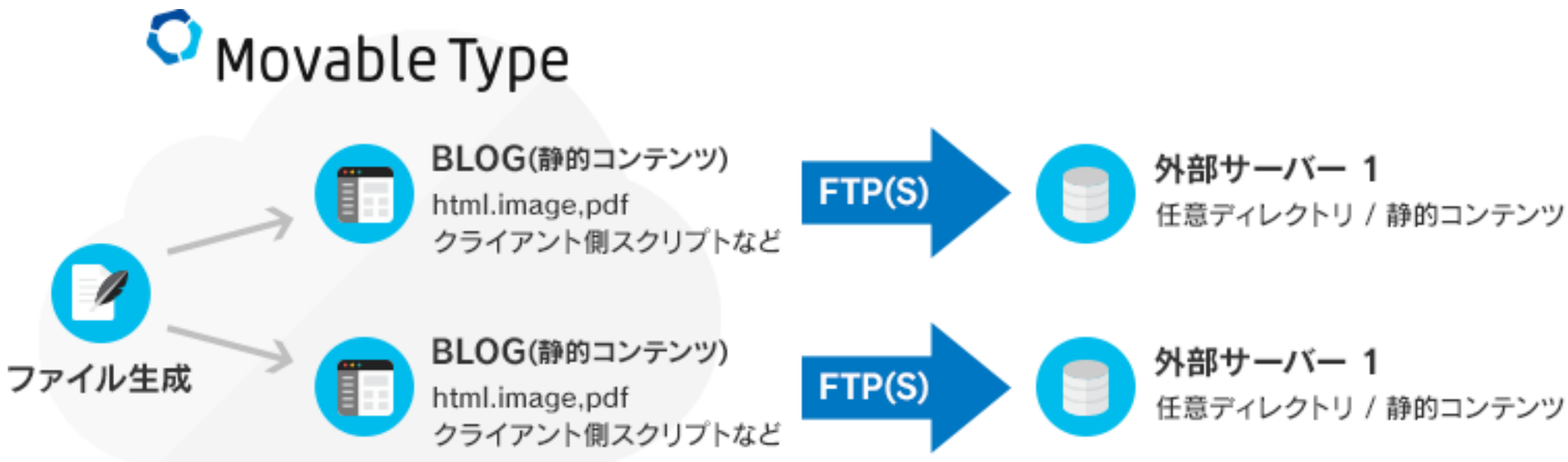
- サーバー配信・ワークフロー・CSVインポート・エクスポート等のエンタープライズ向けのMovable Type 7 拡張パッケージです。
  - サーバー配信機能
  - Workflowプラグイン
  - 管理画面カスタマイズ（MTAppjQuery2）
  - CSVインポート・エクスポート
  - ファイルアップロード拡張
- 必要最低限なエンタープライズ向けパッケージとして提供していきます。

サーバー配信機能



- サーバー配信機能を利用するとMovable Typeがインストールされたサーバーと外部サーバーと同期を取ることができます。公開するサーバーにMovable Typeをインストールしなくてもコンテンツを公開することができるため、セキュリティに配慮したサーバー構成を取ることができます。配信するプロトコルはFTP(s)とrsyncが利用できます。

同期単位



- ウェブサイト・ブログ単位でのサーバー配信
  - サーバー配信では、Movable Type で管理されているファイル（アップロードされたファイルや、再構築時に生成されるファイル）以外にも、選択されたウェブサイト又はブログのサイトパス以下のファイルやディレクトリがすべて配信の対象となります。

配信タイミング

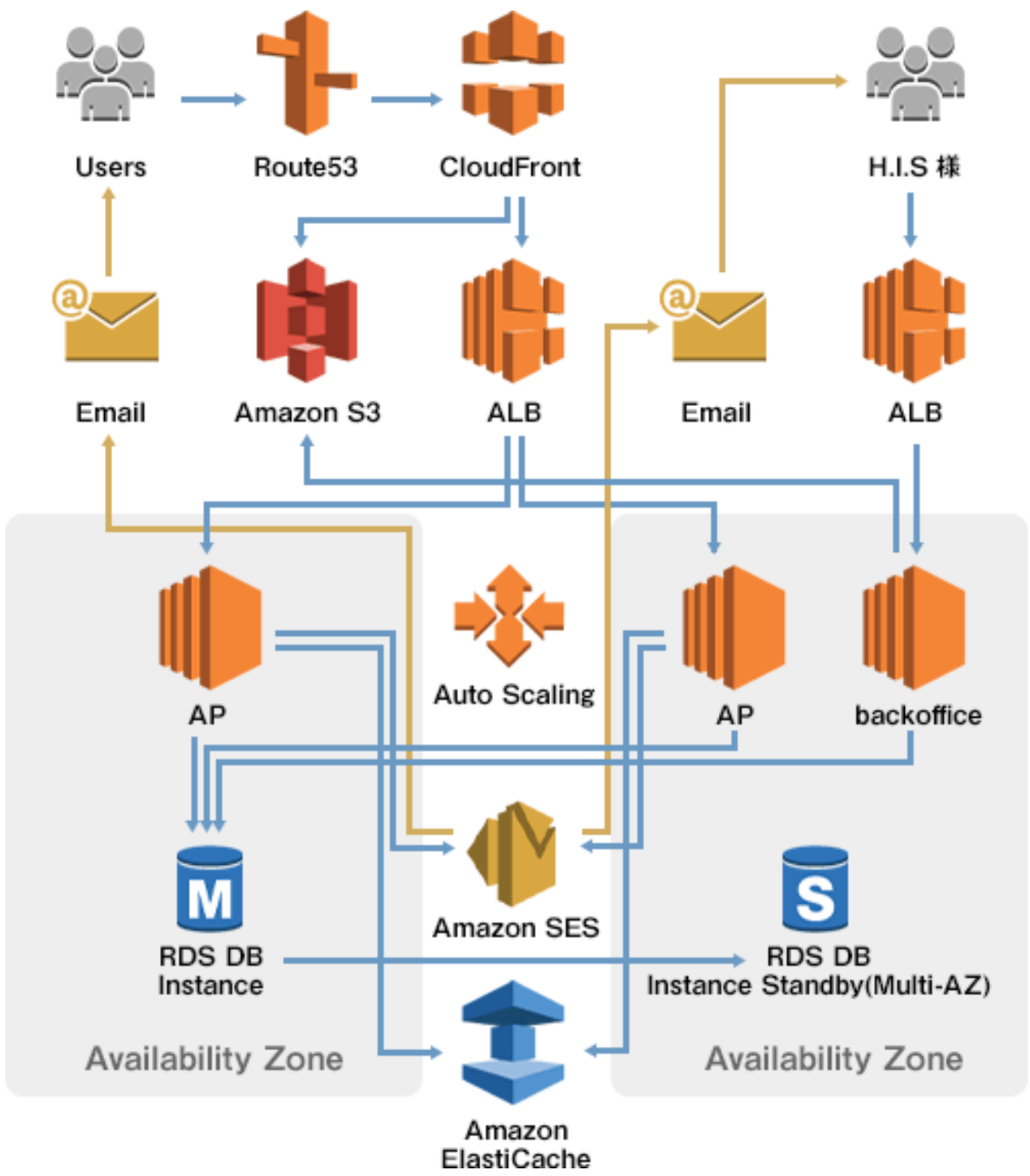
- 即時配信や日時指定配信も可能
  - サーバー配信の設定で指定された日時に、配信が実行されます。（サーバー上で、run-periodic-tasks が動作するように設定されている必要があります。）日時指定は通知設定を行えば、実行結果をメールで受け取ることができます

今後の機能追加について

- メール・ログ機能の改善
- ファイル個別転送機能
- クラウドサービスとの連携
  - 各種クラウドストレージへの配信
    - Azure,AWS,GCP,Alibabaを予定
- 各種CDNのキャッシュ削除
  - クラウドサービス以外ではAkamaiにも対応予定

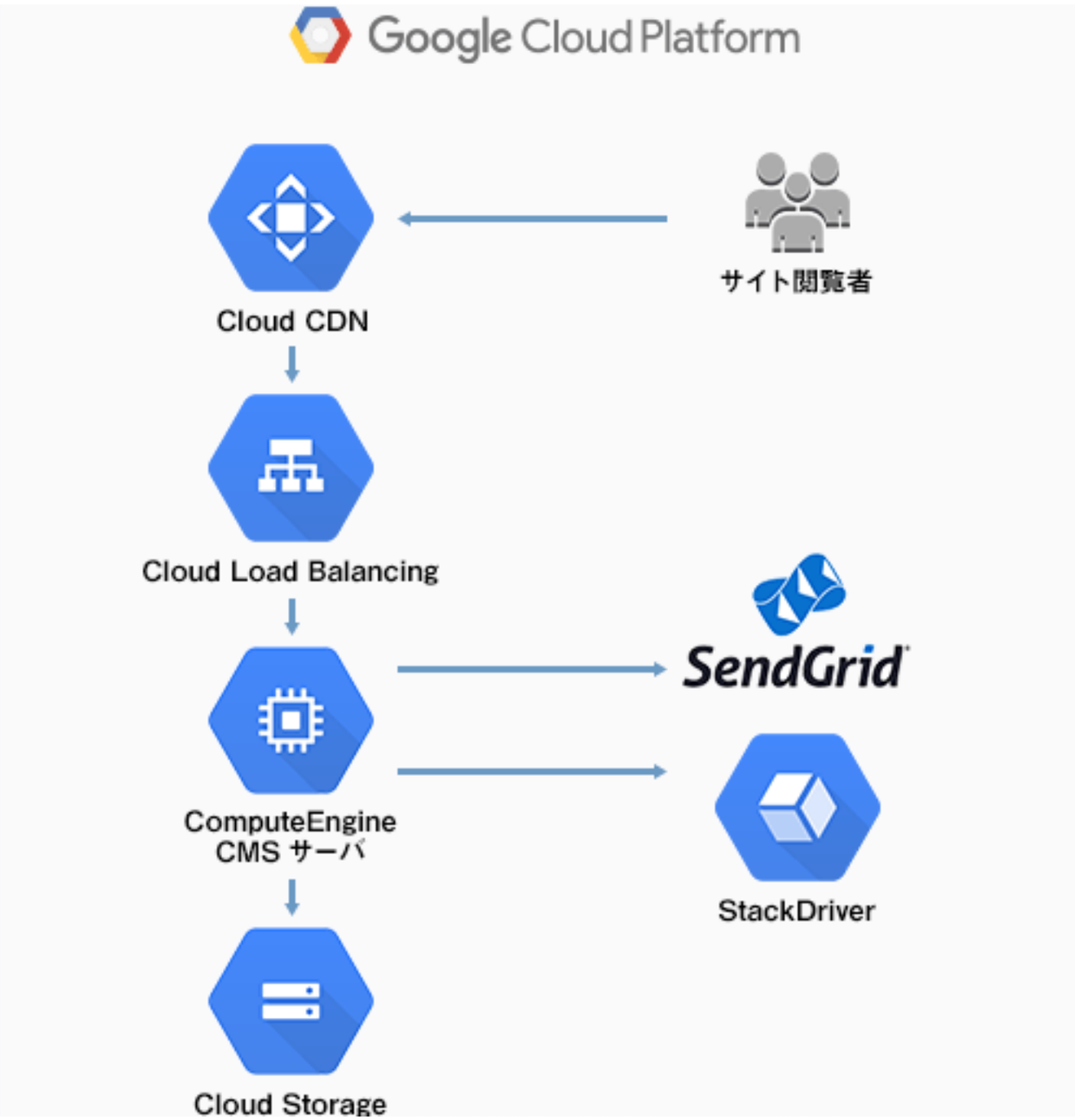
事例のご紹介

H.I.S様 「台湾現地ツアー予約サイト」の事例



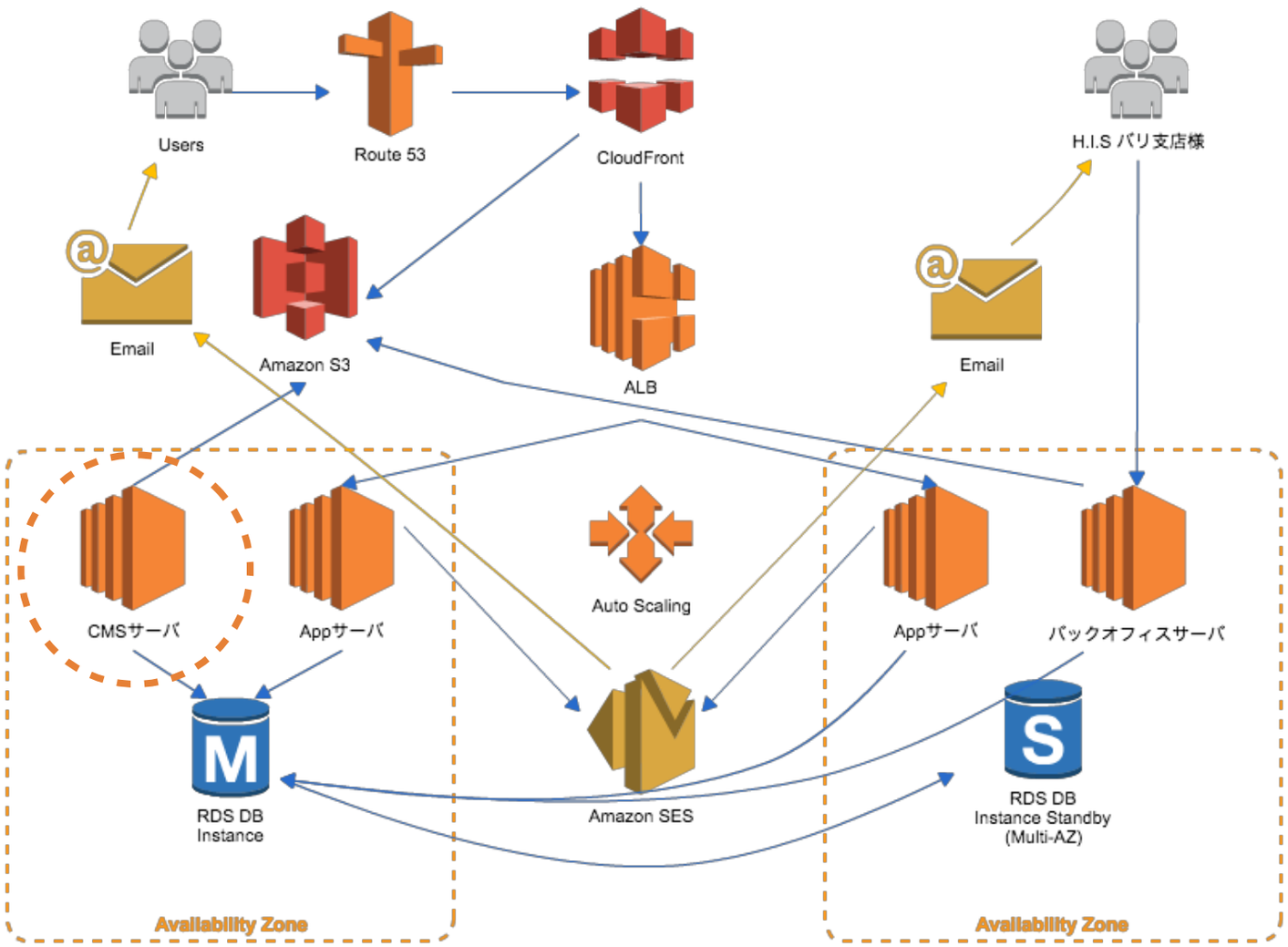
- ポイント
  - backoffice(管理系）サーバはIP制限を設定した上で、ALB下に設置
  - 画像や静的コンテンツはS3を利用した上でCloudFront経由で配信
  - アプリケーションサーバーはオートスケール設定を行い、自動的にサーバ台数を調整
  - メール配信はSESを利用して配信
  - DBはMultiAZのRDSとして冗長化

株式会社ピューズ様 「WEBサイト」の事例



- ポイント
  - CloudCDNを利用する事でスパイクアクセス対策を実施
  - Cloud Load Balancingを利用しCMS(Movable Type)サーバを運用
  - Cloud Storageにバックアップを保存

H.I.Sバリ支店様「現地ツアー予約サイト」の事例



- ポイント
  - ツアーシステムとは別にブログなどのコンテンツをMovable Typeで管理
  - Movable Typeから出力される静的コンテンツはS３経由でCloudFrontで配信

まとめ

まとめ

- セキュリティとバックアップ・冗長性に優れたエンタープライズ向けシステムを構築するには
  - クラウドだと短期間・低コストで構築が可能
  - 監視は適切に設定すること
  - バックアップは多くても困ることは無い
  - セキュリティは適切なネットワーク設計、WAFの導入を行うと安心
  - CDNを使う事でスパイクアクセスに対応する
    - Movable Typeは静的出力を行うので、オブジェクトストレージやCDNとの相性が抜群です

ご清聴頂きありがとうございました