



AWSがもたらすセキュリティイノベーション ーDevSecOps、Compliance as code、セキュリティ自動化ー

Shogo Matsumoto(matshogo@)
Amazon Web Services Japan
Professional Services Senior Security Consultant

松本照吾(Shogo Matsumoto)

Senior Security Consultant, AWS Professional Services

セキュリティソリューションのプロダクトSEを経て、セキュリティ専門のコンサルティング会社に転職。情報セキュリティ監査や事業継続計画（BCP）、PCI DSSの審査員（QSA）等を担当。2015年より現職。

AWS Summit Tokyo2016にてDevSecOpsセッションを担当。

AWS Summit Tokyo2017にてAWSセキュリティ入門セッションを担当。

得意分野

- ・セキュリティポリシー策定支援
- ・各種種コンプライアンス認証への適合支援

主なクライアント

- ・電気通信、金融、金融系スタートアップ（Fintech）などを多数担当

主な保有資格、活動

- ・AWS認定5資格（アソシエイト3資格、プロフェッショナル2資格）
- ・CISA、CISSP、MBA（University of Massachusetts Lowell）
- ・ISACA東京支部CISA委員会試験対策コース委員
- ・JASA（情報セキュリティ監査協会）クラウド監査実技WGリーダー
- ・ISO21500（プロジェクトマネジメントの国際規格）策定には国内対応委員として規格策定に参加。国際会議に出席
- ・JICA技術専門家派遣としてコロンビア政府土地返還プロジェクトにおける情報セキュリティマネジメント講師としての活動に従事（2016）



The background of the slide is a photograph of a river, likely the Arima River in Japan, with numerous pink cherry blossoms (sakaki) hanging from the banks over the water. The water is a calm, light brownish-grey color, and the sky is a pale, hazy blue. The overall mood is serene and beautiful.

本講演の狙い：New Normal
クラウドのセキュリティを“不安”から“加速”へ



本講演で話さないこと：AWS“の”セキュリティ

AWS のコントロール

AWS データセンターは、セキュリティを念頭に置いて設計されており、統制により具体的なセキュリティが実現されています。データセンターを構築する前に、潜在的な脅威を検討し、実装するシステム、テクノロジー、人員がリスクを軽減し得る統制となっているかどうか、膨大な時間を費やしてその設計、実装、テストについて実施しています。お客様自身の監査要件および規制要件を満たしていたために、当社の物理的および環境的コントロールに関するいくつかの具体的な情報を以下に示します。



AGENDA

- WHY AWS ?
- DevSecOpsとAWS
- AWSにおけるガバナンス
- AWSが加速させるセキュリティ自動化



WHY AWS?



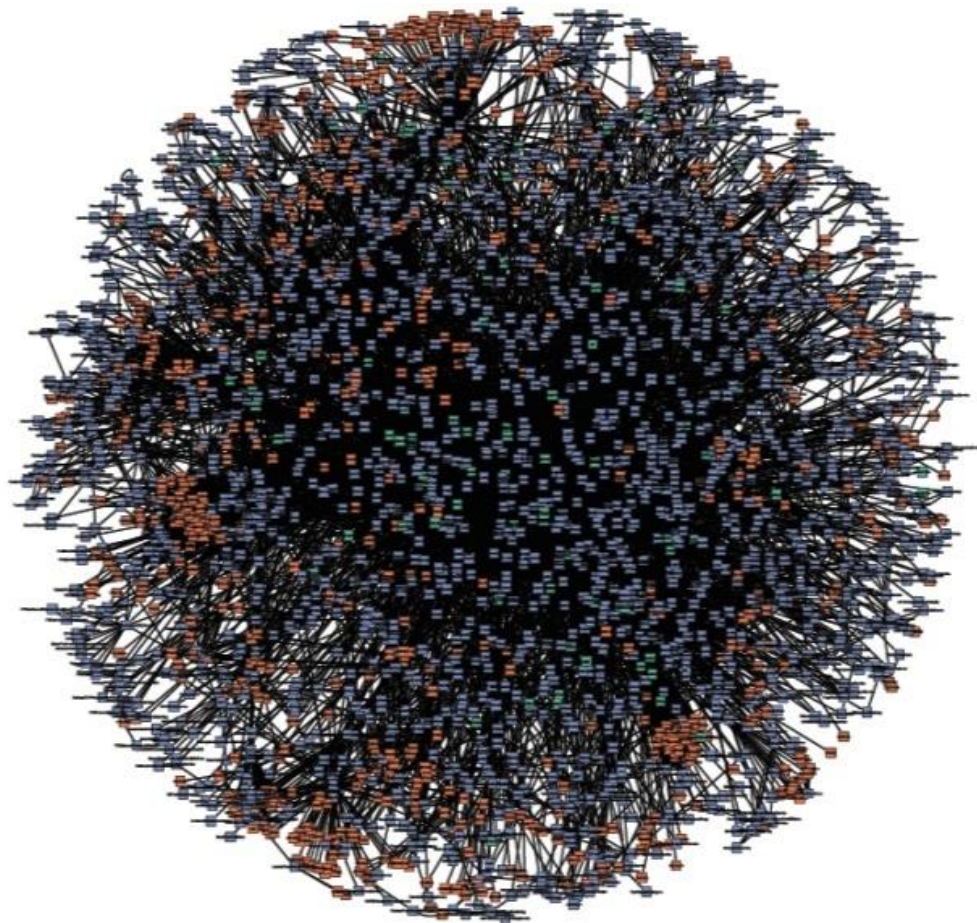
テストのあるべき姿ってなんだろう？

- テスト環境でのテスト
- 本番スケールでのテスト
- 本番環境でのテスト

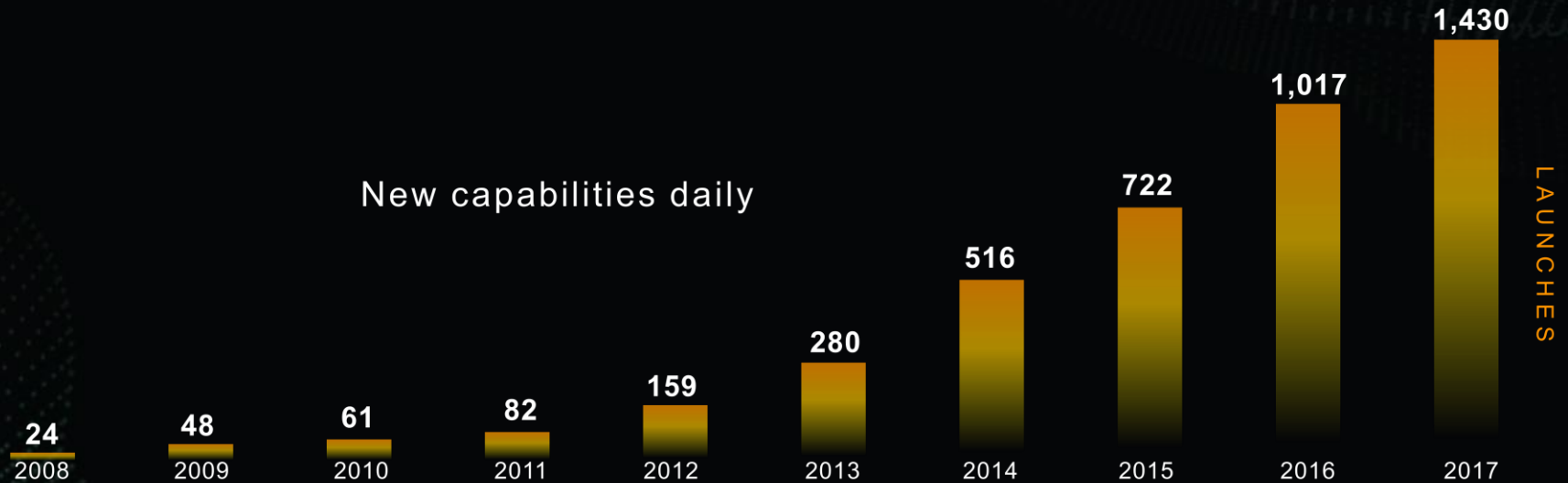
クラウドがもたらすもの
アジリティとスケーラビリティ



<https://medium.com/netflix-techblog>



Supported By Continued Pace Of Innovation



さて、セキュリティをテストするために

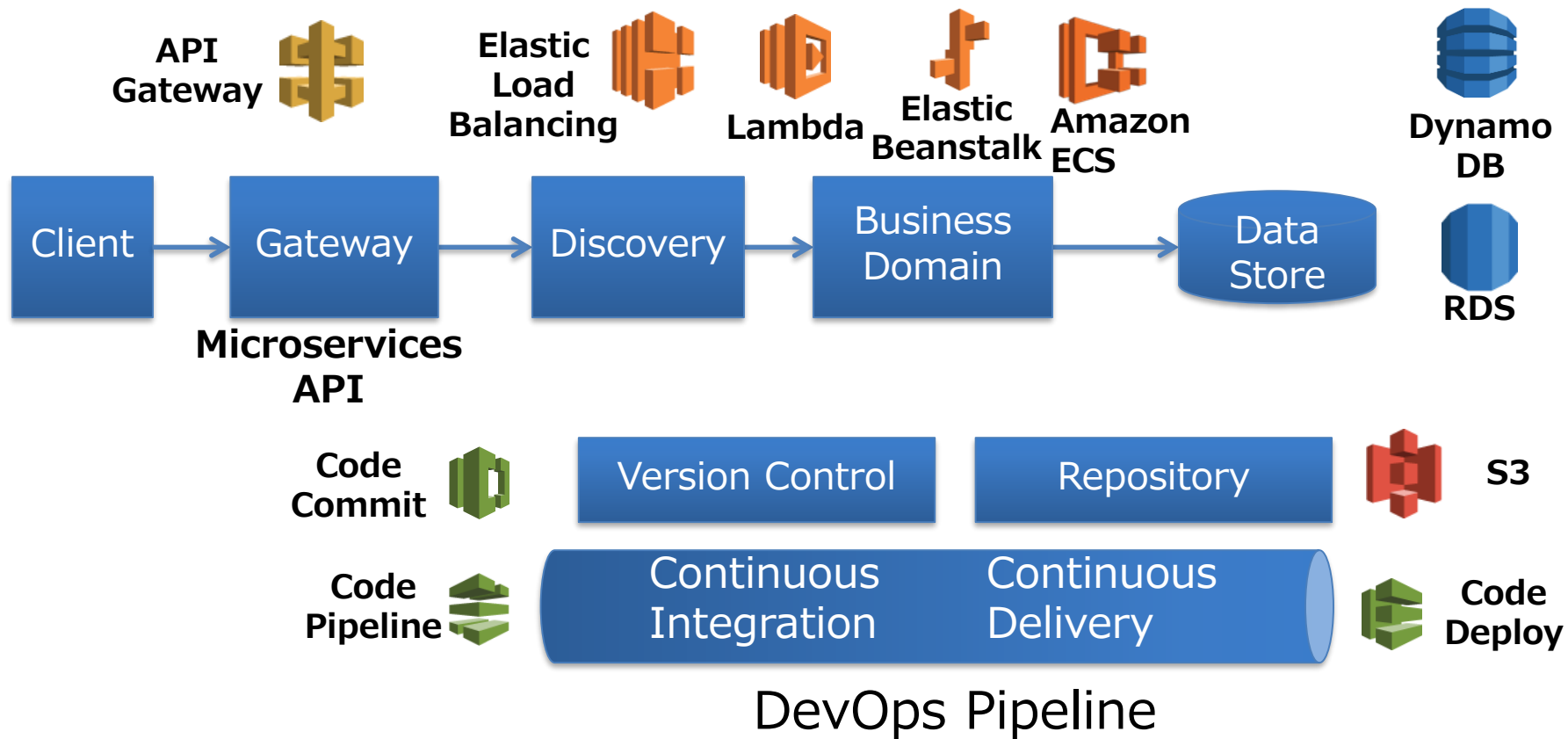
クラウドのセキュリティに不安はありませんか？

- クラウド＝不透明
- クラウド＝規格や法令への順守が困難
- クラウド＝セキュリティ管理が複雑

実際にクラウドがもたらすもの

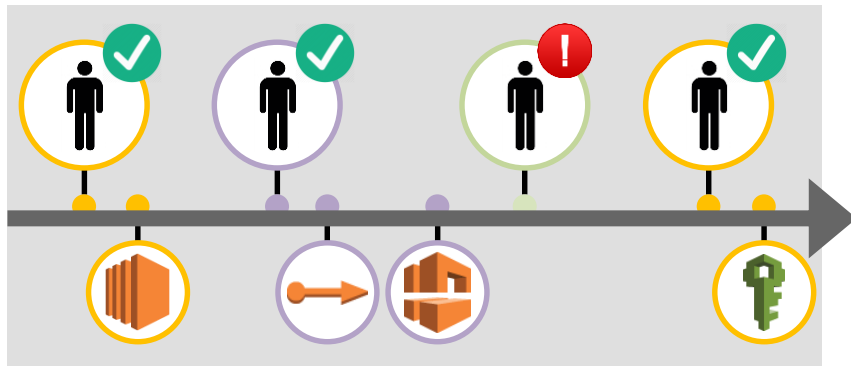
- クラウド＝インフラの透明化
- クラウド＝規格や法令順守のコードへの組み込み
クラウド＝セキュリティ管理の簡素化、自動化

Microservices & DevOps コンポーネント

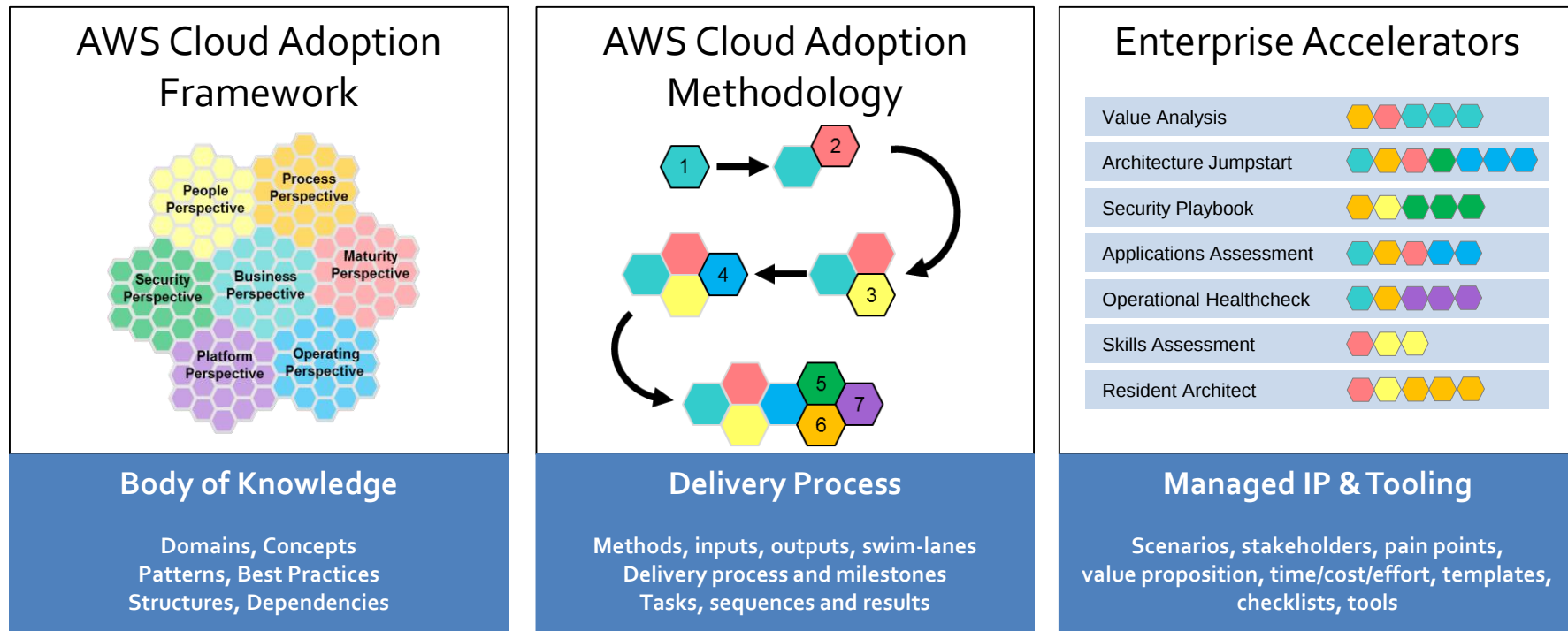


AWSがもたらすもの

- APIによる管理レイヤの抽象化および対応オペレーションの可視化、自動化
- マネージドサービスによるセキュリティ責任の低減
- AWSによるグローバルセキュリティインフラストラクチャ



AWS Cloud Adoption Framework (CAF)



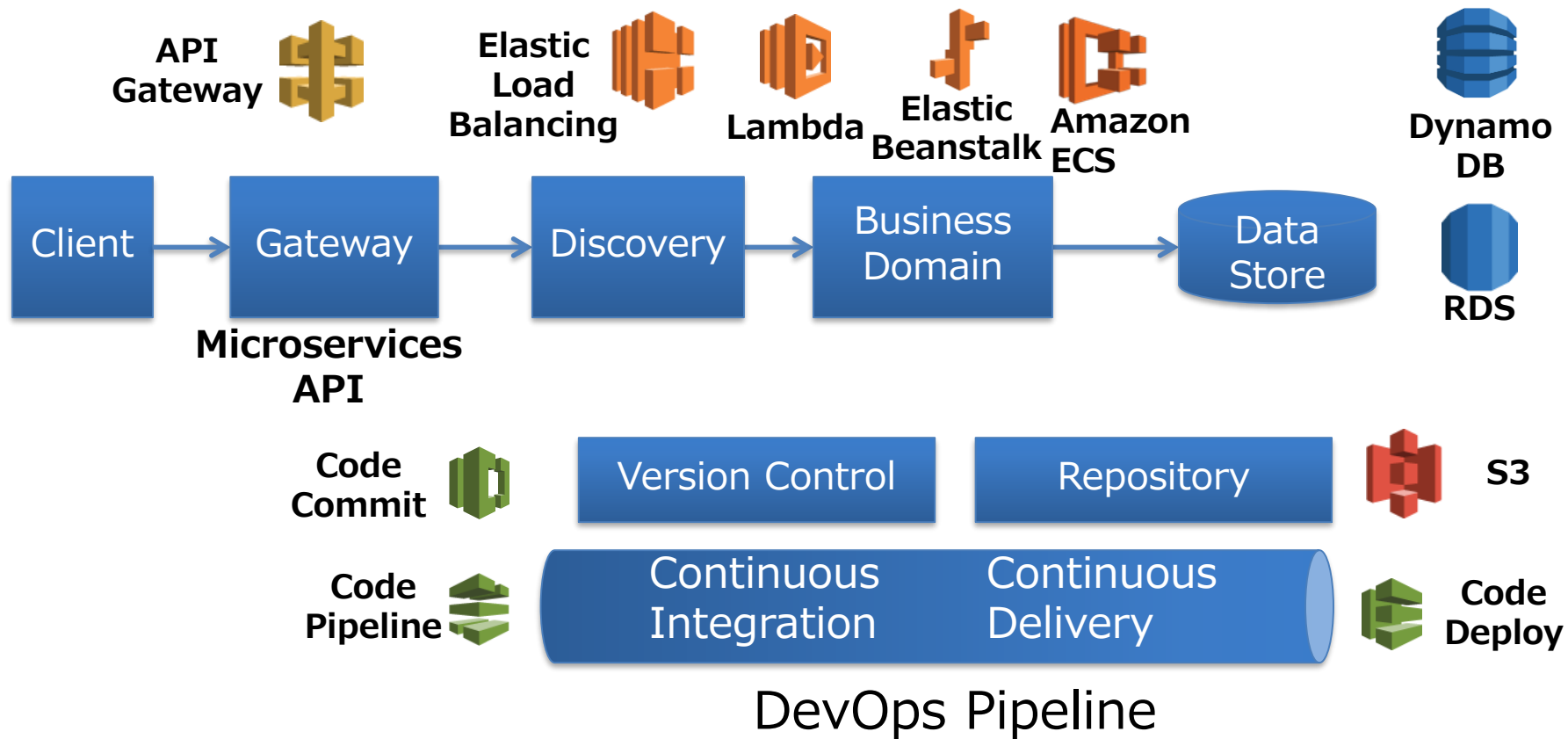
Download the CAF Whitepaper: http://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

Kindle versions also available: <https://aws.amazon.com/whitepapers/#cloud-adoption-framework>



DEVSECOPSとAWS

Microservices & DevOps コンポーネント



Microservices & DevOps コンポーネント

API
Gateway



Elastic
Load
Balancing



Lambda



Elastic
Beanstalk



Amazon
ECS



Dynamo
DB



RDS



マイクロサービス (脆弱性) 評価

Code
Commit



Version Control

Repository



S3

Code
Pipeline



Continuous
Integration

Continuous
Delivery



Code
Deploy

DevOps Pipeline

Amazon Inspector

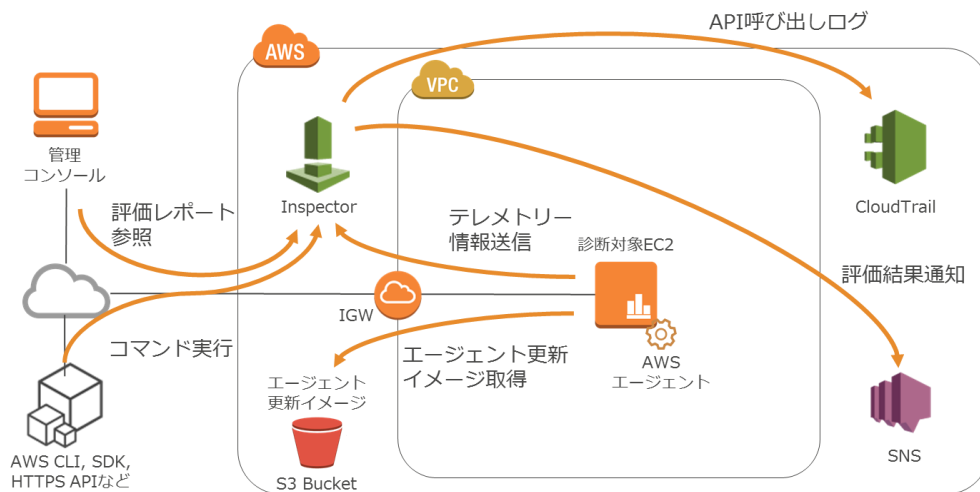
自動化されたセキュリティ評価サービス



特徴

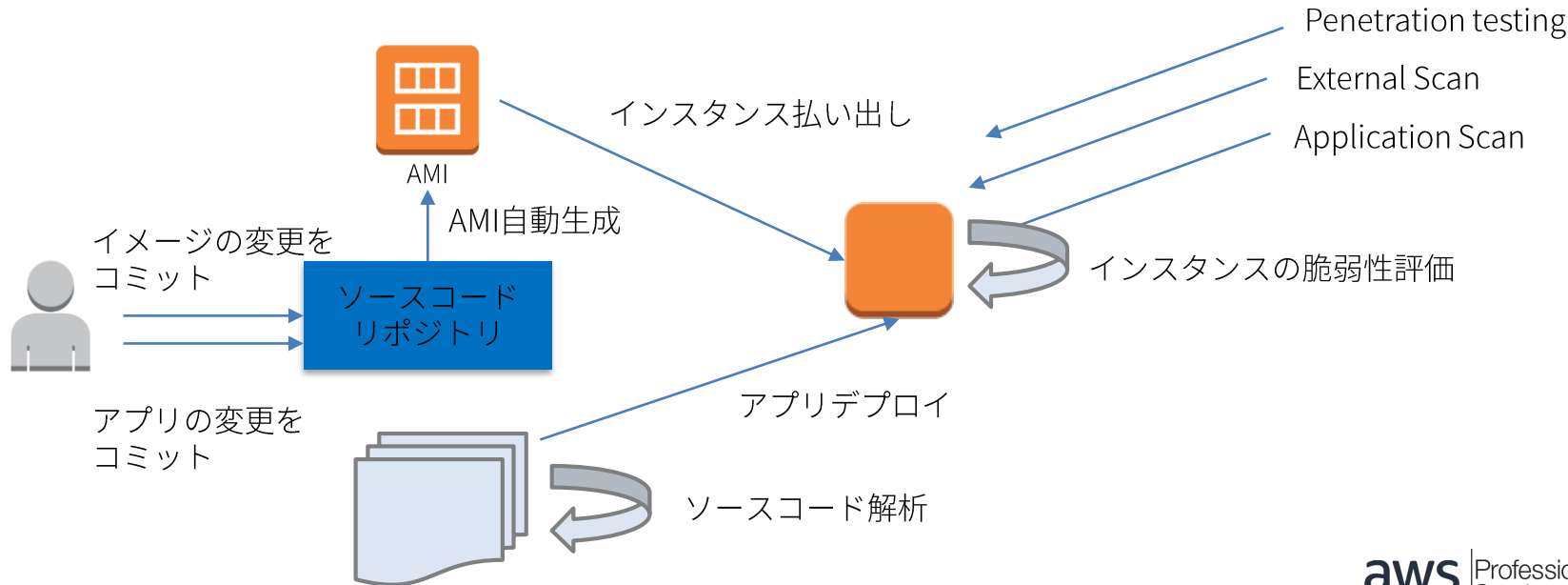
(<http://aws.amazon.com/jp/inspector/>)

- Amazon EC2にエージェントを導入し、セキュリティを評価するホスト型診断
- AWSへの事前申請の必要なし
- CVE(共通脆弱性識別子)、CIS業界ベンチマーク、AWSセキュリティベストプラクティスなどに基づくルールパッケージ
- 再利用可能な評価テンプレート
- エグゼクティブサマリー含めた評価レポート



デプロイ対象のアプリ/サーバレベルへの評価

- 様々なConfigurationの管理
- コードレベルの管理
- アクセスするアカウント/権限の管理
- 評価すべきルールセットの管理



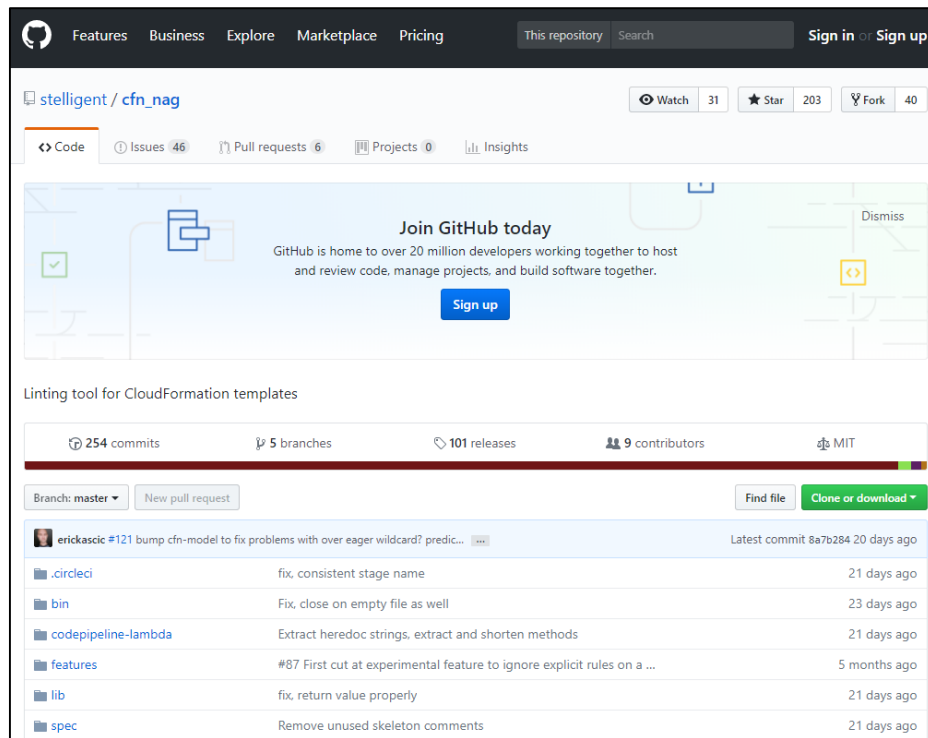
Infrastructure as code : API共通化のもたらす価値

- サービスは“常によりよく（継続的に改善）”するもの
- ハードウェアがソフトウェアになればネットワークもサービスも“取り換えられる”
- Blue-Green Deployment



Infrastructure levelの設定ミスは致命的にも

- 環境の再利用性は、
ミスの再生産にもなる
- リソースとしてGo live
になる前に検知、対応
- OSSのcfn_nagによるテンプレート検査の組み込み



https://github.com/stelligent/cfn_nag

```
$_POST['search_company_code_1_2']=$search_company_code_1_2;
$_POST['search_store_code_1_2']=$search_store_code_1_2;

$_POST['search_company_code_1_3']=$search_company_code_1_3;
$_POST['search_store_code_1_3']=$search_store_code_1_3;
/*
```

```
$_POST['search_company_code_2']=$search_company_code_2;
$_POST['search_store_code_2']=$search_store_code_2;

$this->get_default_prm();
/*
```

評価タイミングのスケジュール化、自動化

DevOpsの一步先を行く、SecureなCI/CD
(DevSecOps)



AWSにおけるガバナンス

セキュリティ部門の要求



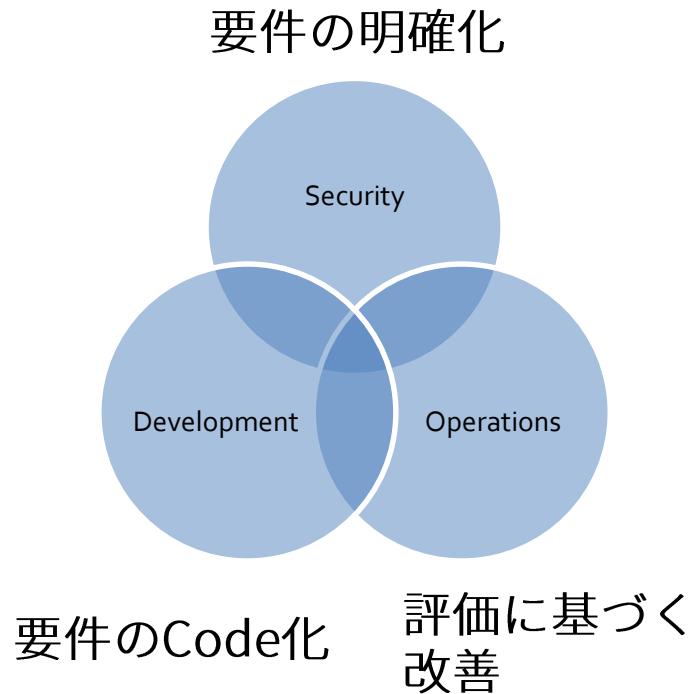
可監查性=Auditability



AWSにおけるガバナンス

Compliance評価を自動化

- 事実に基づく意思決定
- セキュリティ運用の負荷軽減
- DevSecOps文化の醸成



AWS Configとは

- AWSリソースの構成変更をロギング
- 履歴も保存
 - 構成情報は定期的にスナップショットとしてS3に保存
 - 必要に応じSNSを使った通知も可能
- ログはS3に保存
- あるべき状態の評価 (Rules)
 - AWSが適用するルール
 - 独自のルールを適用
- コスト
 - 記録される設定項目につき 0.003 USD (1回の設定として前払いのみ)



AWS Config
AWS Config Rules

セキュリティをボトルネックにしないために

- スタンダードチャータード銀行におけるコンプライアンス要件のコード化の取り組み事例
- AWSが組み込むマネージドルールその他にお客様によるカスタムルールの組み込みも
- AWS自体がカスタムルールの公開も※



<https://www.slideshare.net/AmazonWebServices/building-the-largest-repo-for-serverless-complianceascode-sid205-reinvent-2017>

※Custom rules: <https://github.com/aws-labs/aws-config-rules>



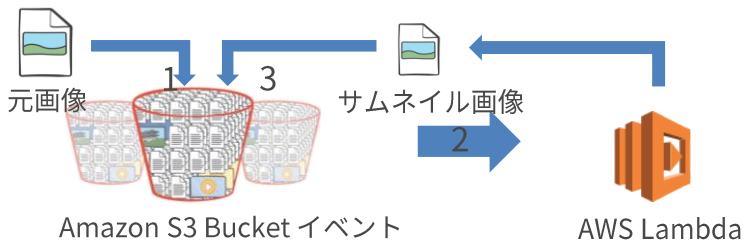
AWSが加速させるセキュリティ自動化

AWS Lambda

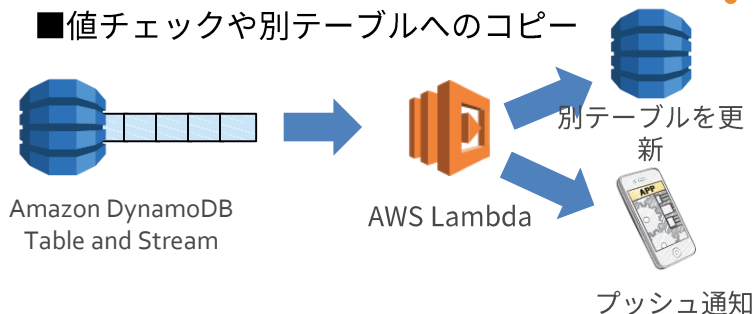


イベントをトリガーにコードを実行するコンピュータサービス

■イメージのリサイズやサムネイルの作成



■値チェックや別テーブルへのコピー



• 特徴 (<http://aws.amazon.com/jp/lambda/>)

- OS、キャパシティ等インフラの管理不要
- S3、Kinesis、SNS等でのイベント発生を元にユーザが用意したコード (Node.js) を実行
- ユーザアプリからの同期/非同期呼び出し

• 価格体系 (<http://aws.amazon.com/jp/lambda/pricing/>)

- コード実行時間 (100ms単位)
- Lambdaファンクションへのリクエスト回数
- 1月あたり100万リクエスト、400,000GB/秒が無料で利用可能

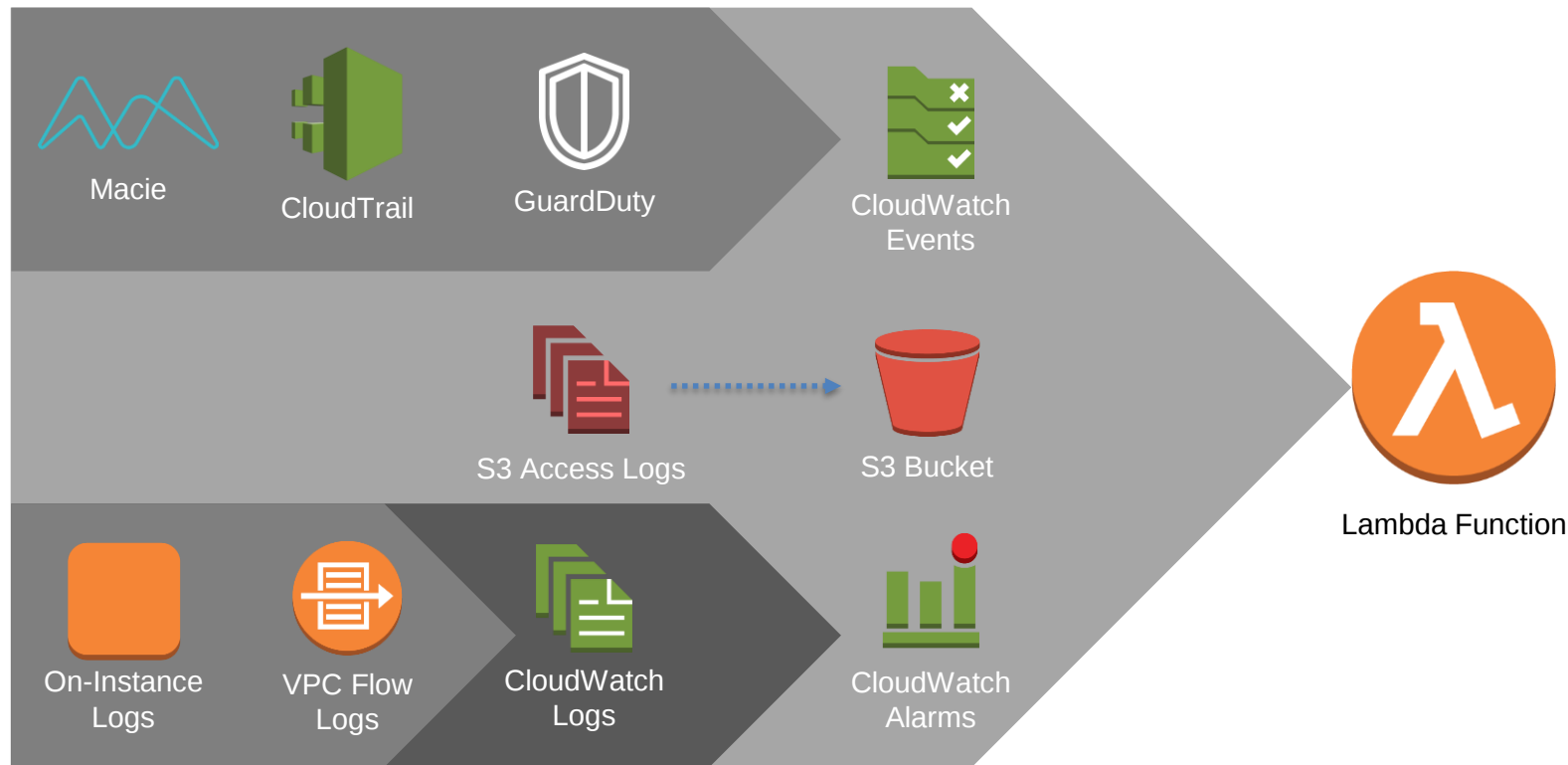
Lambdaがもたらすもの

- インフラ管理からの解放
- コストメリット
- イベント駆動型のコード実行
- サービス単位の分割＝マイクロサービス
- “テストしやすい”サービス



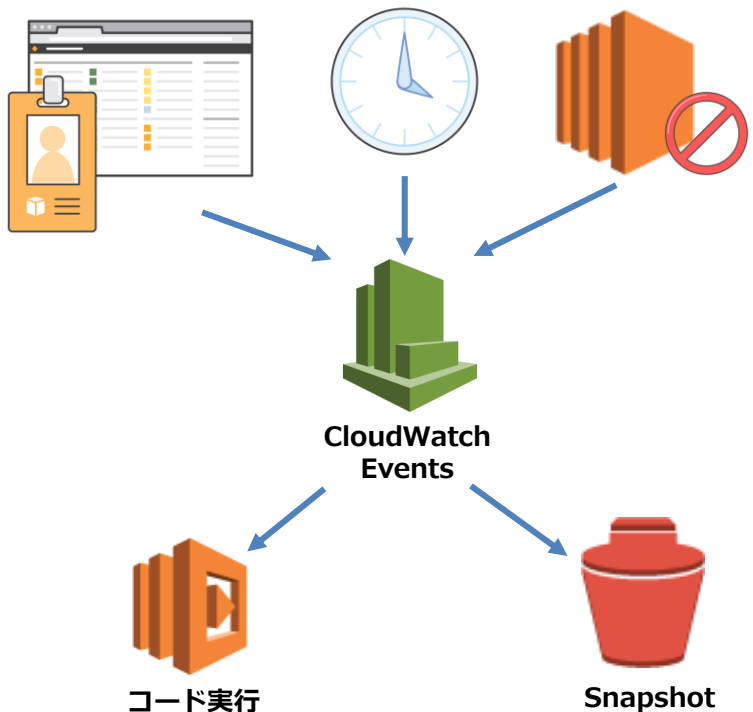
Lambda Function

Lambdaが実現するセキュリティ自動化



Amazon CloudWatch Events

AWSの様々なリソースの変更をリアルタイムに検知・アクション



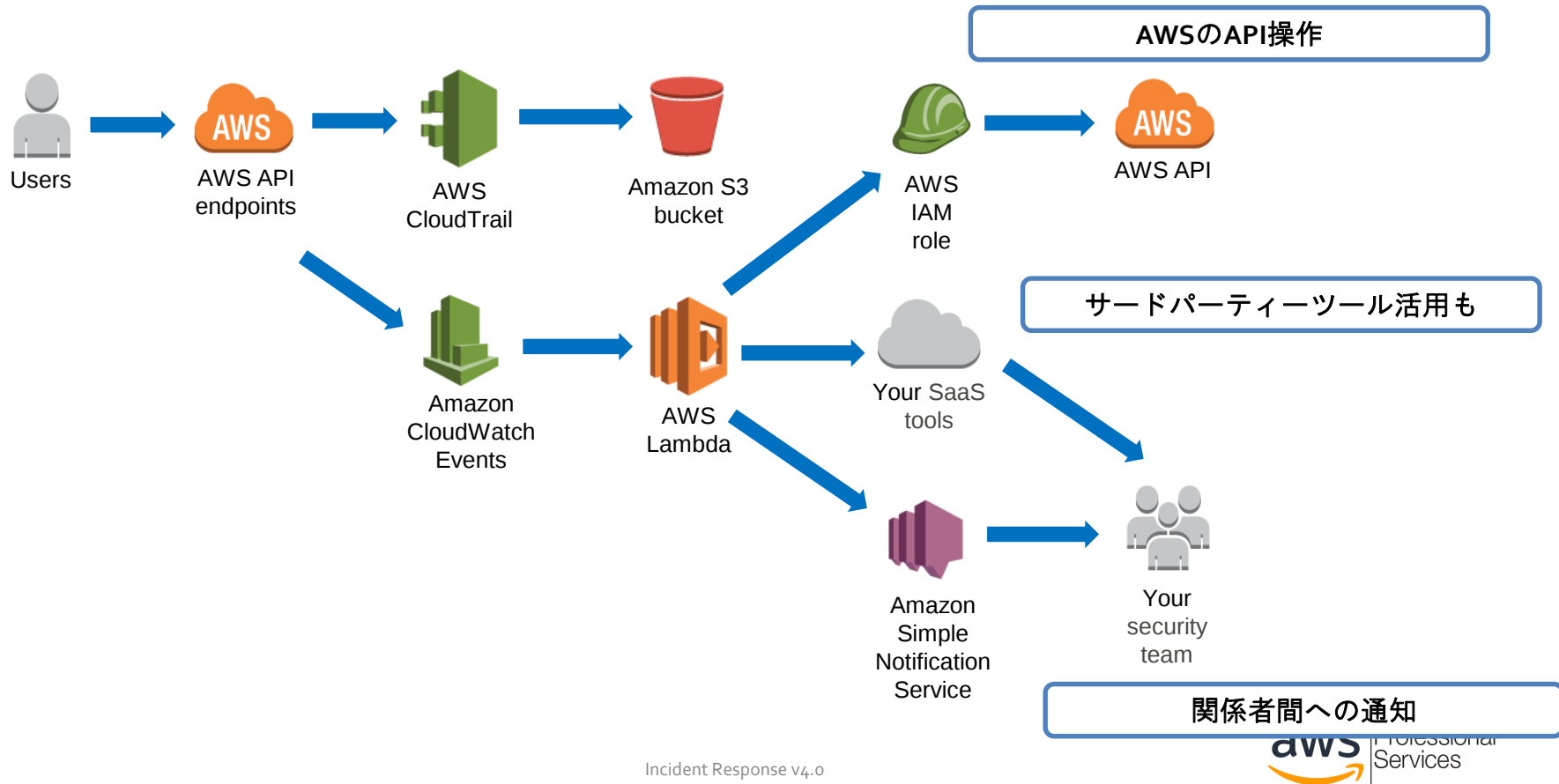
特徴

- AWSの様々なリソースに対するイベントをトリガーにアクションを実行
- 例) 特定ユーザーがログインしたらLambda関数の実行
- スケジュールベースでのアクションも可能
- EBSスナップショットの定期取得などのBlueprintを用意
- イベント、ターゲット、ルールで定義

価格体系 (<https://aws.amazon.com/jp/cloudwatch/pricing/>)

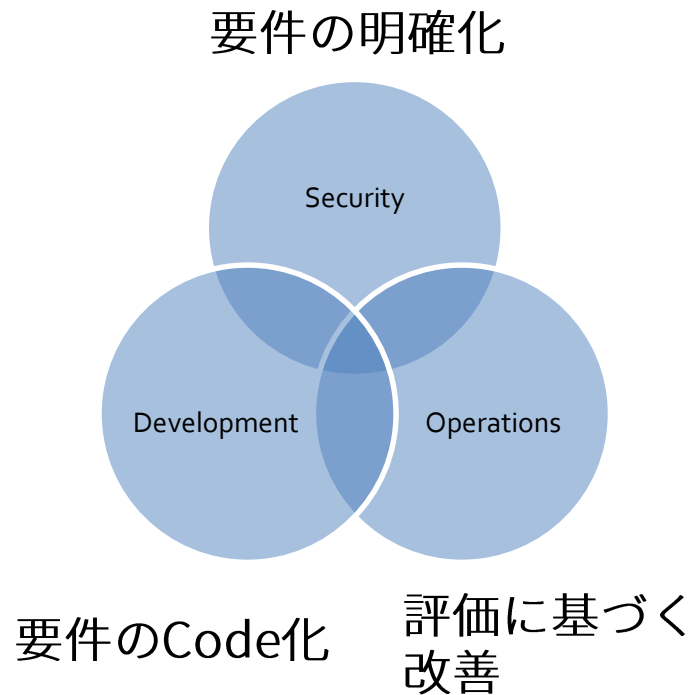
- 100万イベント/1ドル
 - カスタムイベントを作成した場合にはカウントに注意

自動化にむけた対応



DevOpsやDevSecOpsはツールではない＝文化

セキュリティ、コンプライアンス
のためのコードは誰が書くのか？

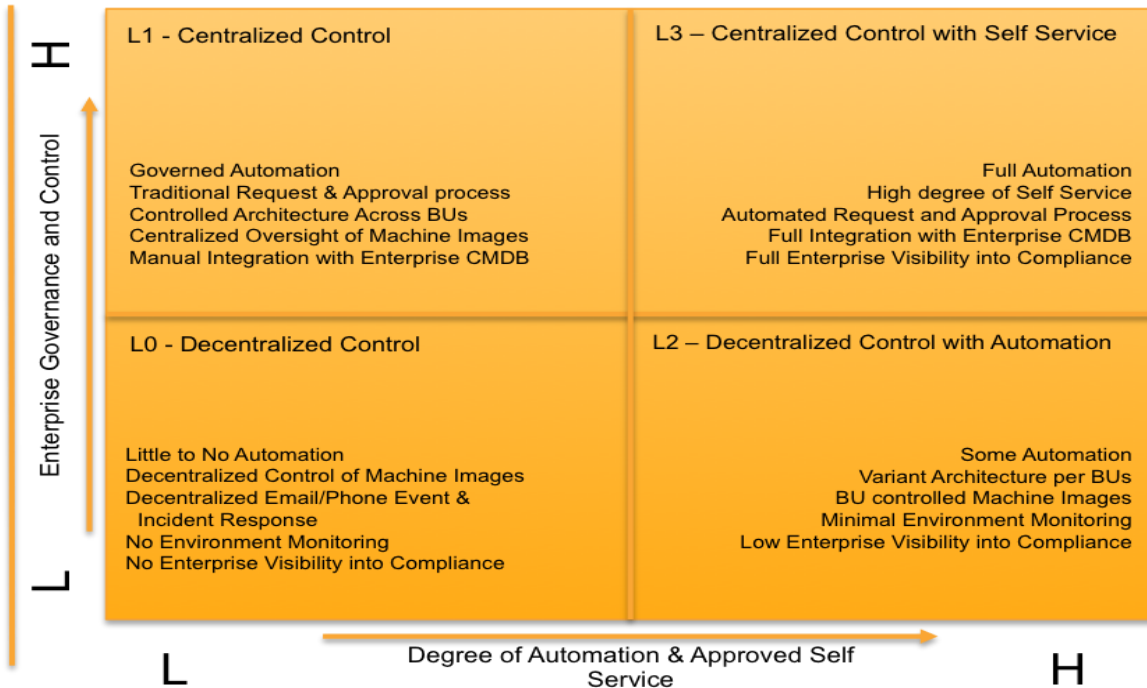


DevSecOps Governance Maturity

Maturity Assessment Key Questions

1. What is the level of interaction between the business unit and IT operations to provision cloud resources?
2. To what degree are the software development teams constrained by the ability to provision compute resources?
3. To what degree does the business unit have visibility into cost of cloud resources to support applications?
4. To what degree has the business unit developed preconfigured automation templates?
5. Are there automated integrations between cloud environments and your CMDB or Event Management systems?

Cloud Operations and Governance Maturity





まとめとして



Security Cloud Journey is always
Testing and Improving
Infrastructure, Apps, and Organization



2018 年 5 月 30 日 (水) ~ 6 月 1 日 (金)
グランドプリンスホテル新高輪

セッション選択・無料来場お申し込み »

日本最大級のクラウドコンピューティングカンファレンス AWS Summit Tokyo 2018 今年は 5 月 30 日 (水) ~ 6 月 1 日 (金) の 3 日間にわたり、品川にて開催！

AWS Summit はクラウドコンピューティングコミュニティが一堂に会して、アマゾン ウェブ サービス (AWS) に関する情報交換、コラボレーション、学習を行うことができる日本最大級のクラウドコンピューティングカンファレンスです。

AWS Summit は世界 23 カ国以上 33 か所以上の都市で開催され、東京では 2018 年 5 月 30 日~6 月 1 日、品川にて開催します。

AWS Summit Tokyo 2018 では、基調講演、お客様事例、ユースケースセッション、AWS の最新テクノロジー動向や多種多様な業種や企業規模でのクラウドサービス活用事例など、150 以上にもおよぶ AWS ならではのセッションをご提供します。また、展示スペースではスポンサー企業様のソリューションの他、AWS や Amazon の最新サービスについても見て、触れて、学べる展示を実施します。

クラウドに関する最新情報と最新実用事例を学び、AWS 利用者との人脈を築くことができるこの機会に、皆様ぜひご参加ください。

nal



THANK YOU FOR YOUR ATTENTION!

Shogo Matsumoto([matshogo@](mailto:matshogo@amazon.com))

Amazon Web Services Japan

Professional Services Senior Security Consultant