DevSecOps のユースケースと DevSecOps がもたらす未来

釜山 公徳　-Masanori KAMAYAMA-

日本クラウドセキュリティアライアンス　クラウドセキュリティWG リーダー

Self-introduction

- 釜山公徳（Masanori Kamayama）
- CSA Japan クラウドセキュリティWG リーダー
- その他所属・活動
  - ✓日本電気株式会社
    テクニカルエバンジェリスト兼クラウドコンサルタント
  - ✓CompTIA Subject Matter Experts
  - ✓Fin-JAWS 運営メンバー
  - ✓JNSA IoTセキュリティログ検討WG、他
- 著作

  NISC（内閣サイバーセキュリティセンター）
  「あなたの守りたい「モノ」は何ですか？どうやって守りますか？」、他

セキュリティィについての考え方

セキュリティは

コストではなく

投資！

1st Stepで大事なこと

守るべきモノを
定義する

参考）NISCのコラム

- 「あなたの守りたい「モノ」は何ですか？どうやって守りますか？」

参考：https://www.nisc.go.jp/security-site/month/h29/column/20180314.html

クラウドセキュリティWGの成果物

タイトル

CSA ガイダンス v4.0 を用いた
クラウドセキュリティリファレンス（OSS マッピング）

公開日

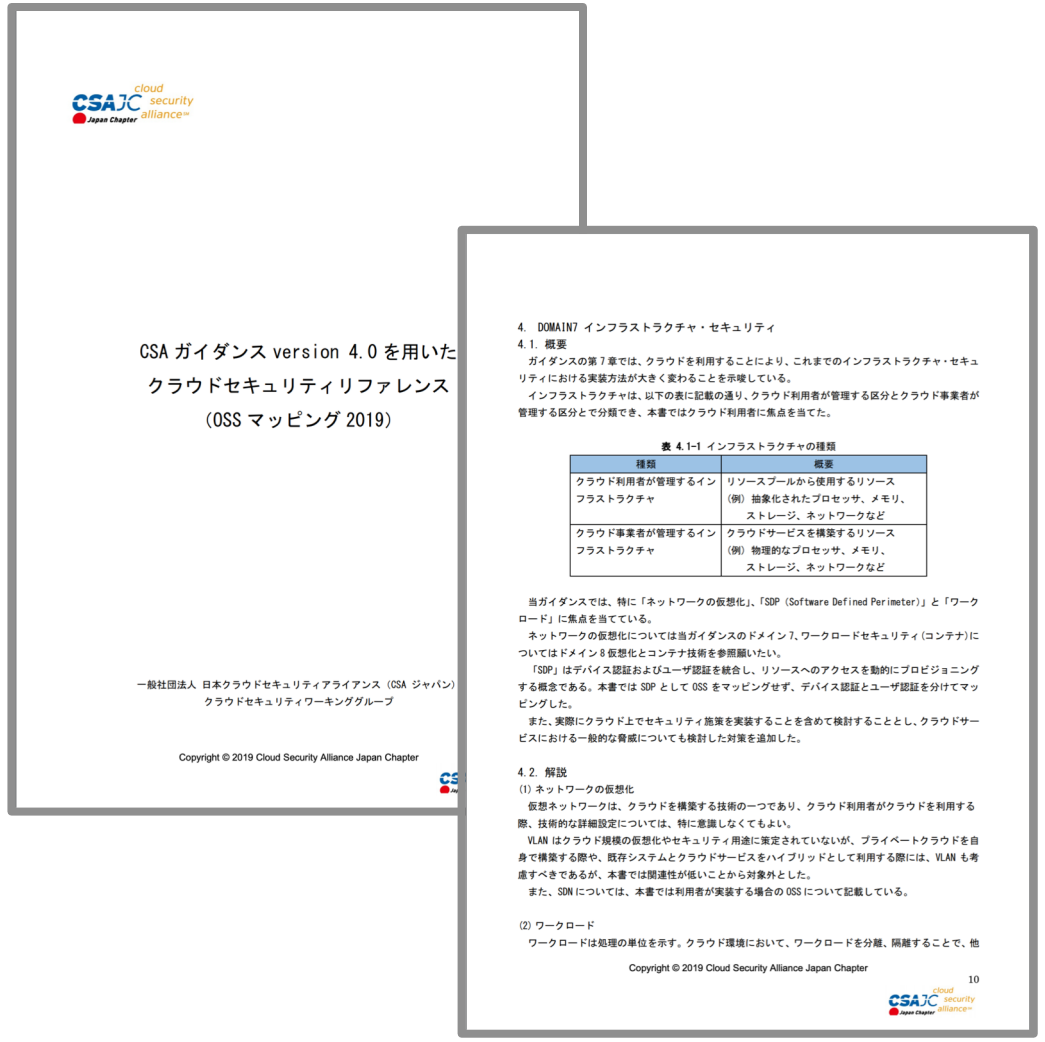
2019年2月26日

目的

実環境における設計や実装といったフェーズで具体的な検討をするにあたり、Open Source Software(OSS)とガイダンスをマッピングさせることで、具体的な施策のイメージへの一助になると考え作成

ダウンロードURL

https://www.cloudsecurityalliance.jp/site/WG_PUB/cloud security_WG/CSAguidance_mapping_20190226.pdf


CSA ガイダンス version 4.0 を用いた
クラウドセキュリティリファレンス
(OSS マッピング 2019)

一般社団法人 日本クラウドセキュリティアライアンス（CSA ジャパン）
クラウドセキュリティワーキンググループ

Copyright © 2019 Cloud Security Alliance Japan Chapter

4. DOMAIN7 インフラストラクチャ・セキュリティ
4.1. 概要
ガイダンスの第 7 章では、クラウドを利用することにより、これまでのインフラストラクチャ・セキュリティにおける実装方法が大きく変わることを示唆している。
インフラストラクチャは、以下の表に記載の通り、クラウド利用者が管理する区分とクラウド事業者が管理する区分とで分類でき、本書ではクラウド利用者に焦点を当てた。

表 4.1-1 インフラストラクチャの種類

種類	概要
クラウド利用者が管理するインフラストラクチャ	リソースプールから使用するリソース （例）抽象化されたプロセッサ、メモリ、ストレージ、ネットワークなど
クラウド事業者が管理するインフラストラクチャ	クラウドサービスを構築するリソース （例）物理的なプロセッサ、メモリ、ストレージ、ネットワークなど

当ガイダンスでは、特に「ネットワークの仮想化」、「SDP（Software Defined Perimeter）」と「ワークロード」に焦点を当てている。
ネットワークの仮想化については当ガイダンスのドメイン 7、ワークロードセキュリティ（コンテナ）についてはドメイン 8 仮想化とコンテナ技術を参照願いたい。
「SDP」はデバイス認証およびユーザ認証を統合し、リソースへのアクセスを動的にプロビジョニングする概念である。本書では SDP として OSS をマッピングせず、デバイス認証とユーザ認証を分けてマッピングした。
また、実際にクラウド上でセキュリティ施策を実装することを含めて検討することとし、クラウドサービスにおける一般的な脅威についても検討した対策を追加した。

4.2. 解説
(1) ネットワークの仮想化
仮想ネットワークは、クラウドを構築する技術の一つであり、クラウド利用者がクラウドを利用する際、技術的な詳細設定については、特に意識しなくてもよい。
VLAN はクラウド規模の仮想化やセキュリティ用途に策定されていないが、プライベートクラウドを自身で構築する際や、既存システムとクラウドサービスをハイブリッドとして利用する際には、VLAN も考慮すべきであるが、本書では関連性が低いことから対象外とした。
また、SDN については、本書では利用者が実装する場合の OSS について記載している。

(2) ワークロード
ワークロードは処理の単位を示す。クラウド環境において、ワークロードを分離、隔離することで、他

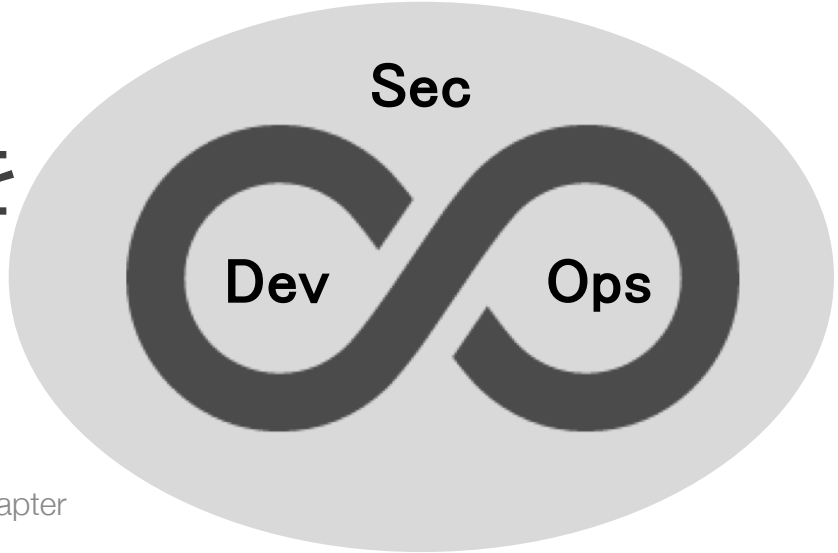
Copyright © 2019 Cloud Security Alliance Japan Chapter
10

参考）ワーキンググループの参加申込について

- 興味がある方は是非！

DevSecOps の定義

- DevOps に Security を加えた概念
- DevOps.com、DevSecOps.com、Gartner等、様々なところで重要性を叫ばれている
- DevOpsとは
  - ✓Dev(開発) と Ops(運用) を組み合わせ、継続的対応する考え
  - ✓主にアプリケーション開発視点
- Biz-DevSecOpsといったビジネスの視点を取り入れた概念も



Why DevSecOps?

- ビジネスアジリティの向上
- コスト最適化
- 時間対効果
- 情報漏洩リスク回避

よくある課題

定義が曖昧	DevOpsすらもよくわからない	目的がはっきりしない	そもそもどうすればよいかわからない

DevSecOps以前に検討すべき多くの事項

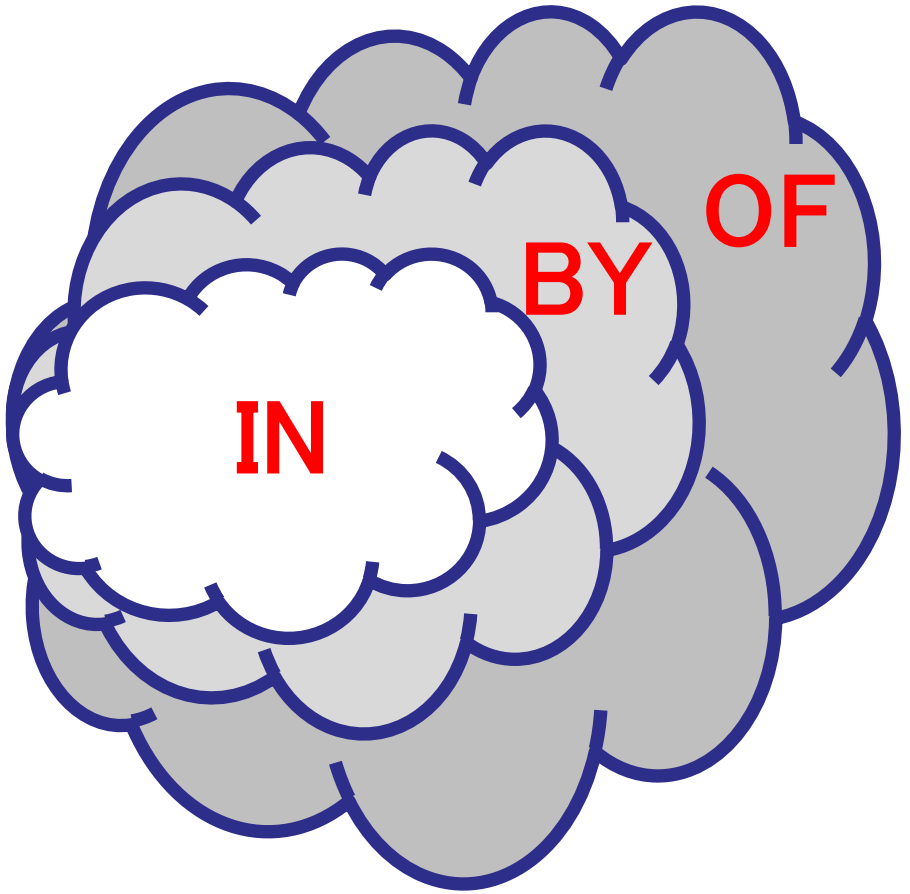
3つのセキュリティ領域（Security X Cloud）

- クラウドのセキュリティ領域を3つに分類
  1. Security **IN** Cloud

     利用者側で講じる領域
  2. Security **BY** Cloud

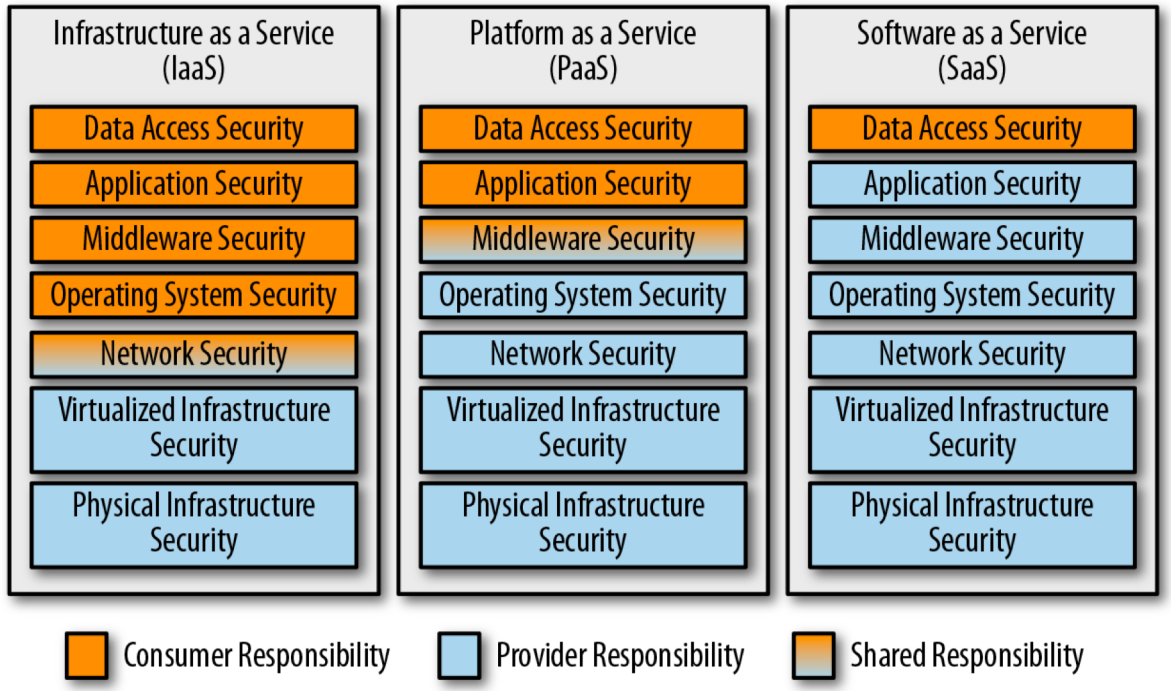
     クラウドベンダーやセキュリティベンダーが提供するセキュリティ
  3. Security **OF** Cloud

     クラウドベンダー側の責任範囲



Security X Cloud と 責任共有モデル

- カスタマー側の責任範囲
  - ✓Security **IN** Cloud
  - ✓Security **BY** Cloud
- クラウドベンダー側の責任範囲
  - ✓Security **OF** Cloud



https://www.oreilly.com/library/view/practical-cloud-security/9781492037507/ch01.html

Security by Design の 3 つの視点

アプリケーション開発

- SAST(静的分析)、DAST(動的分析)等

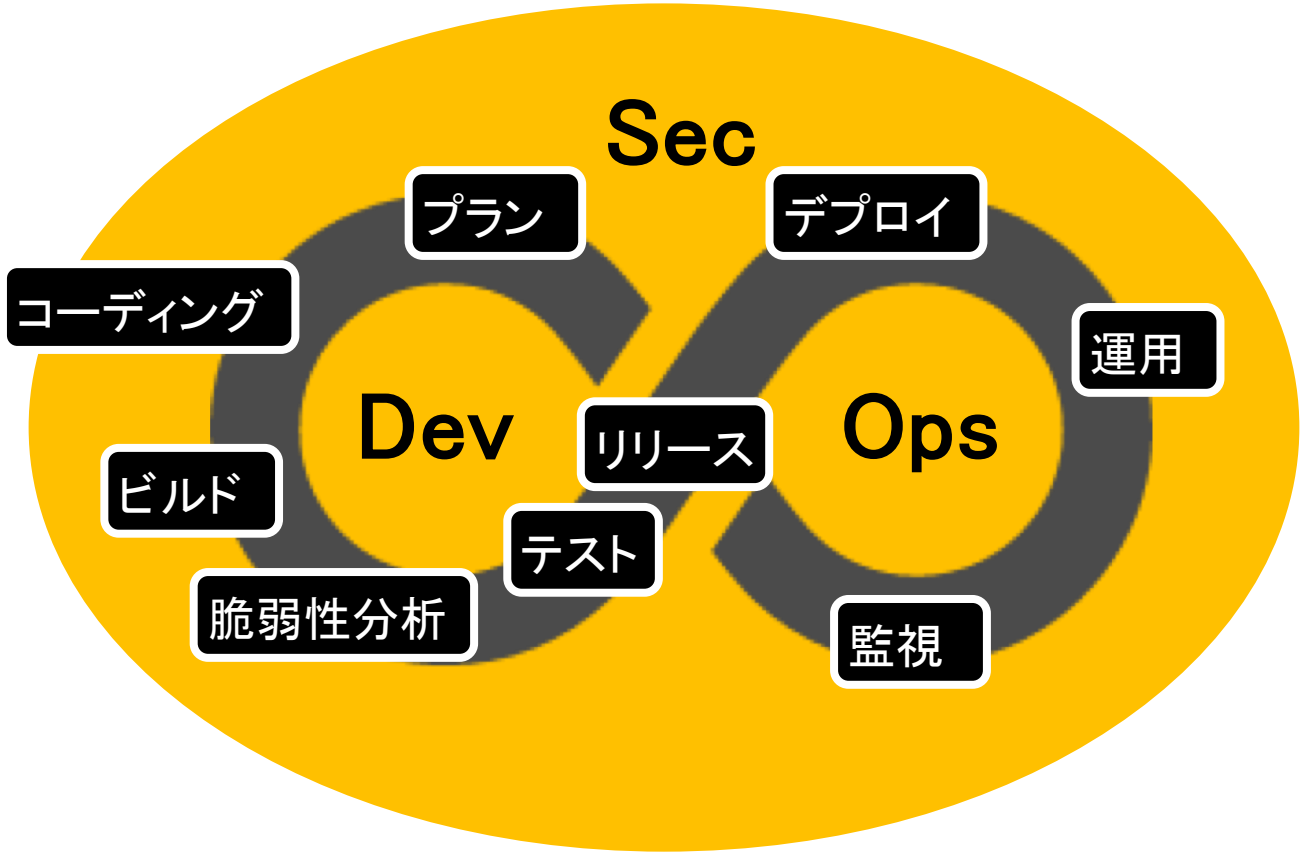
クラウドサービス

- クラウドベンダー、セキュリティベンダーが提供するセキュリティサービス

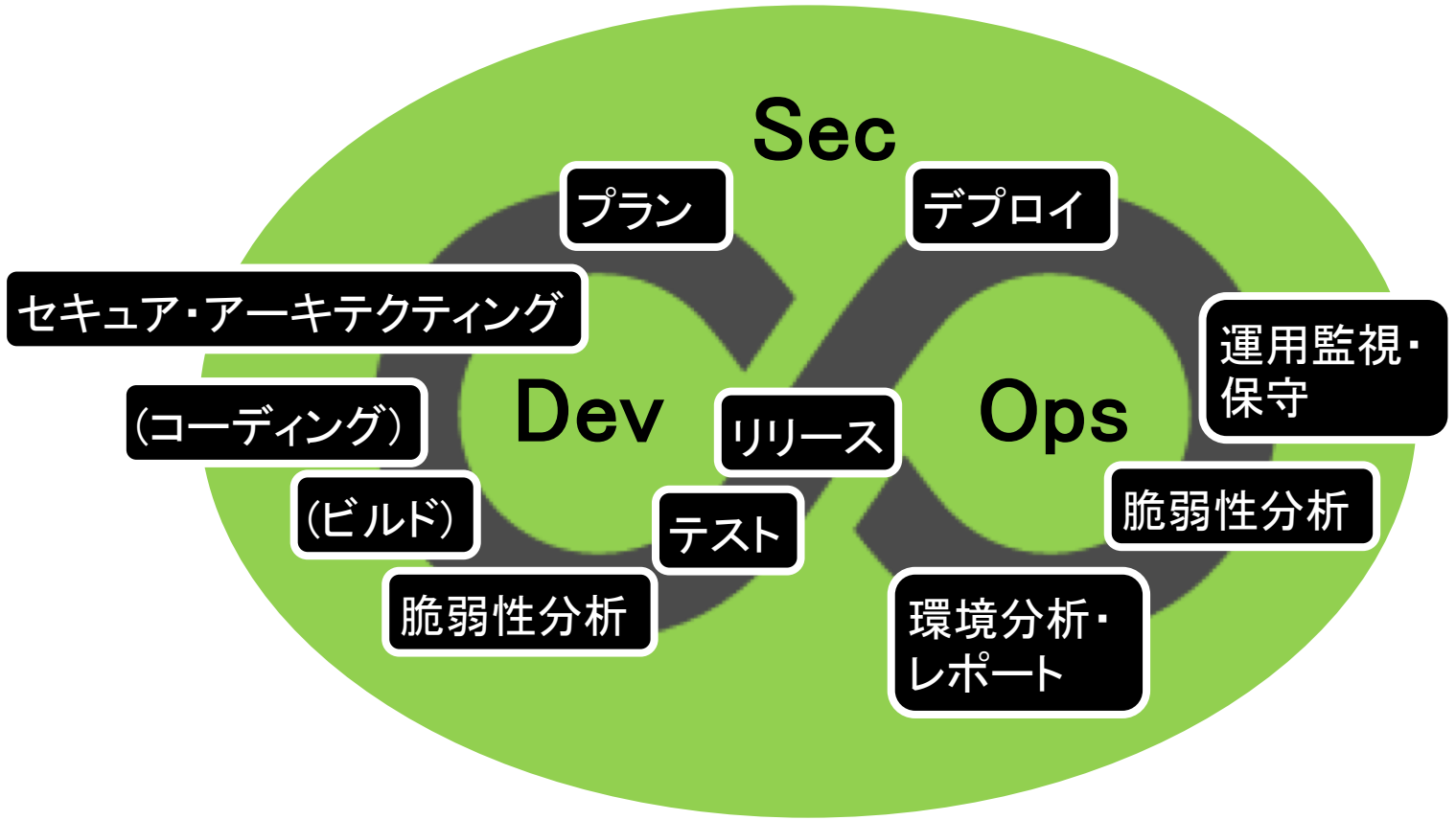
インフラストラクチャ

- Bastion、ファイアウォール、IDS/IPS、不要ポート閉塞等

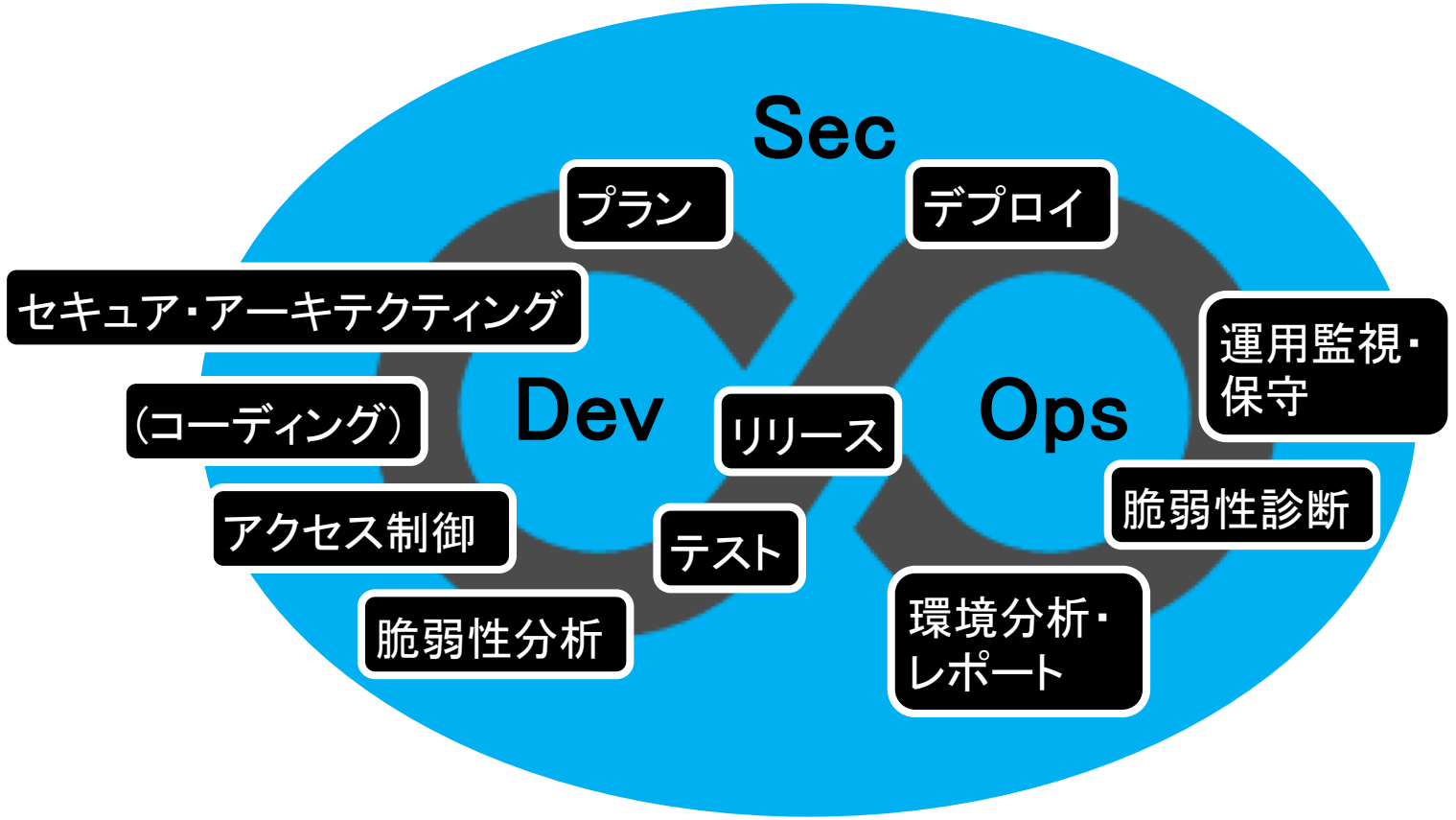
アプリケーション開発視点でのDevSecOps



クラウドサービス視点でのDevSecOps

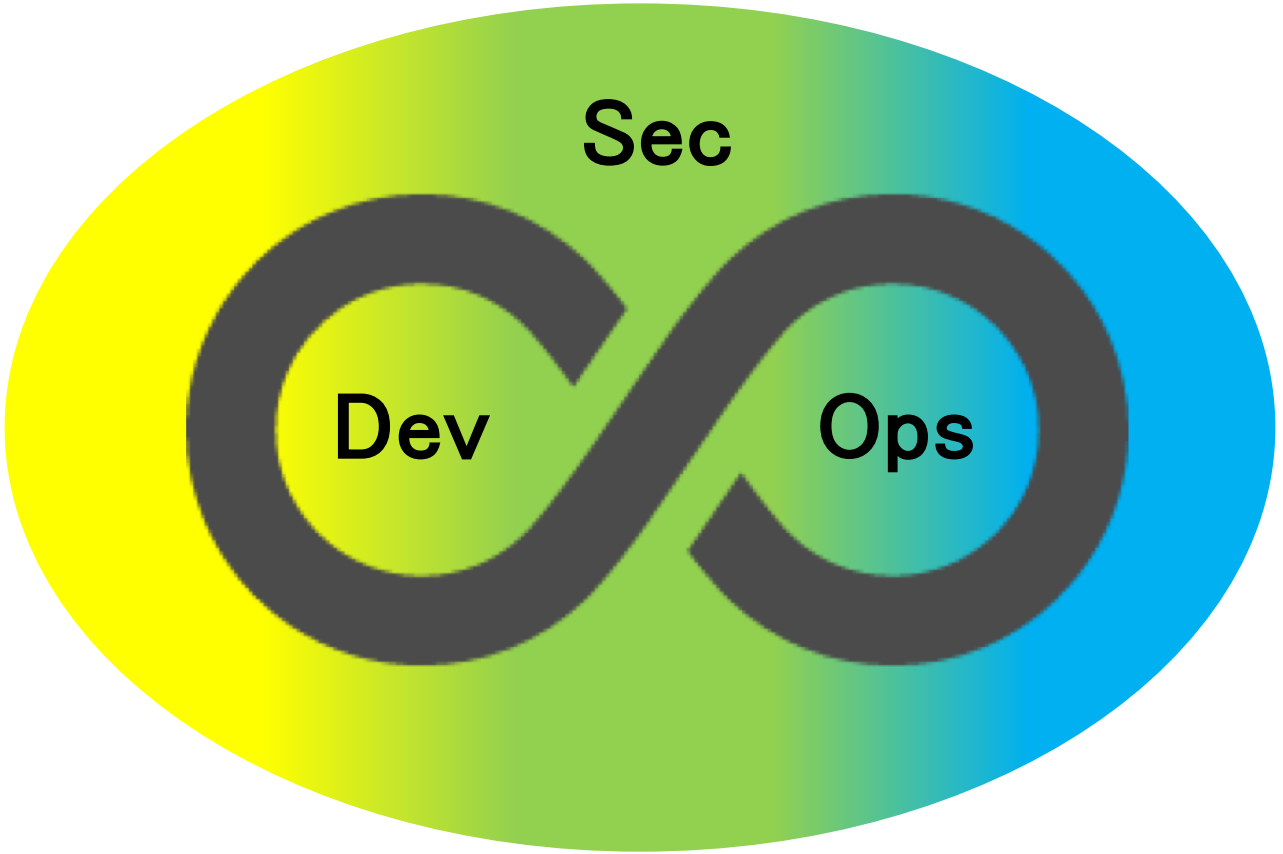


インフラストラクチャ視点でのDevSecOps



様々な視点のDevSecOpsをどうするか

- 守りたいモノにフォーカスし、必要な要素は全て取り入れる



セキュリティの脅威を起点に考える

- クラウド重大セキュリティ脅威 11の悪質な脅威

https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/10/top-threats-to-cloud-computing-egregious-eleven_J_20191031.pdf

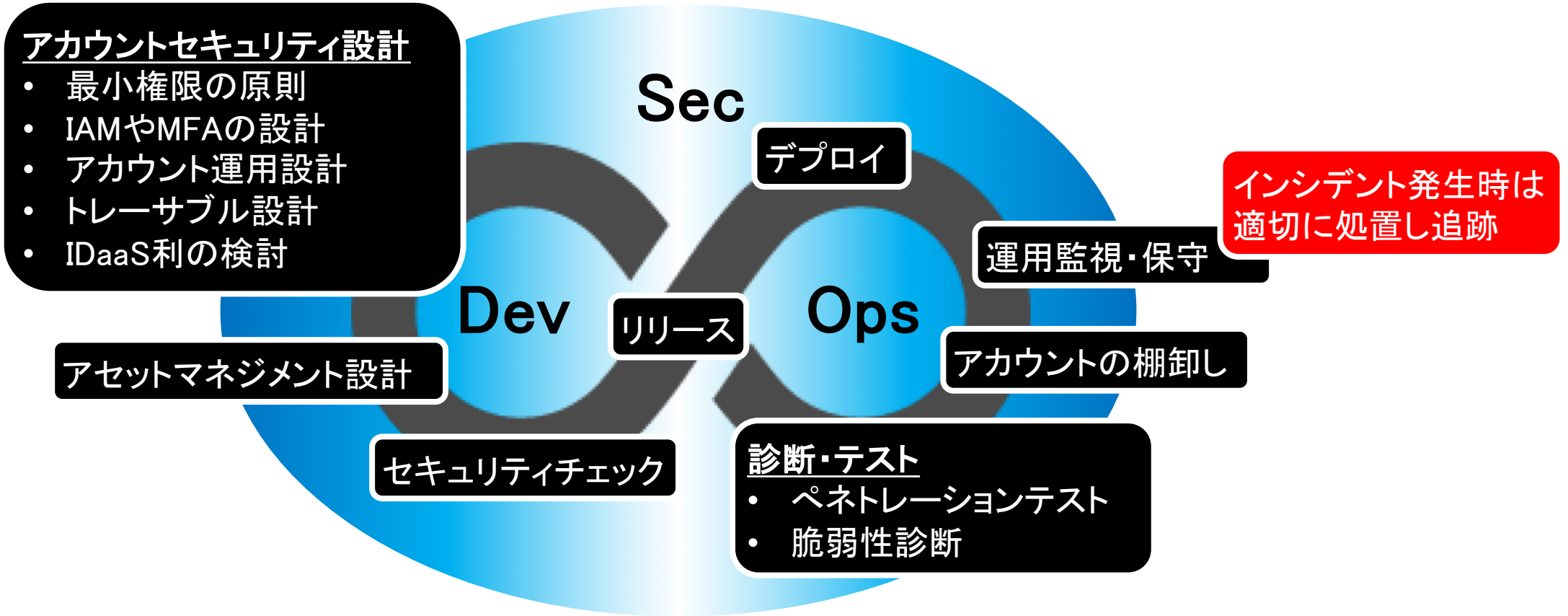
アカウントハイジャックのサマリー

- 脅威サマリー
  - アカウントやサブスクリプションを取得し、不正に操作する
- ビジネスインパクト
  - 評判の低下、ブランド価値の低下、法的責任の発生、機微な 個人情報やビジネス情報の開示につながるデータ漏洩
- 想定事例と事例
  - 2014年6月、Code Space 社のAWSアカウントが、管理コンソールを多要素認証で防御していなかったため、全ての情報資産が破壊され、事業が継続不能になった。
  - 2018年、Consumer Cloud Services社のデータがダークネット市場で大規模に販売された。
  - 2017年、特にMicrosoft Office 365のアカウントをターゲットとした攻撃が増加。
  - 2010年4月、アマゾンでクロスサイトスクリプティング（XSS）バグが確認された。2009 年には、非常に多くのアマゾン上のシステムがハイジャックされ、Zeus ボットネットの温床になった。

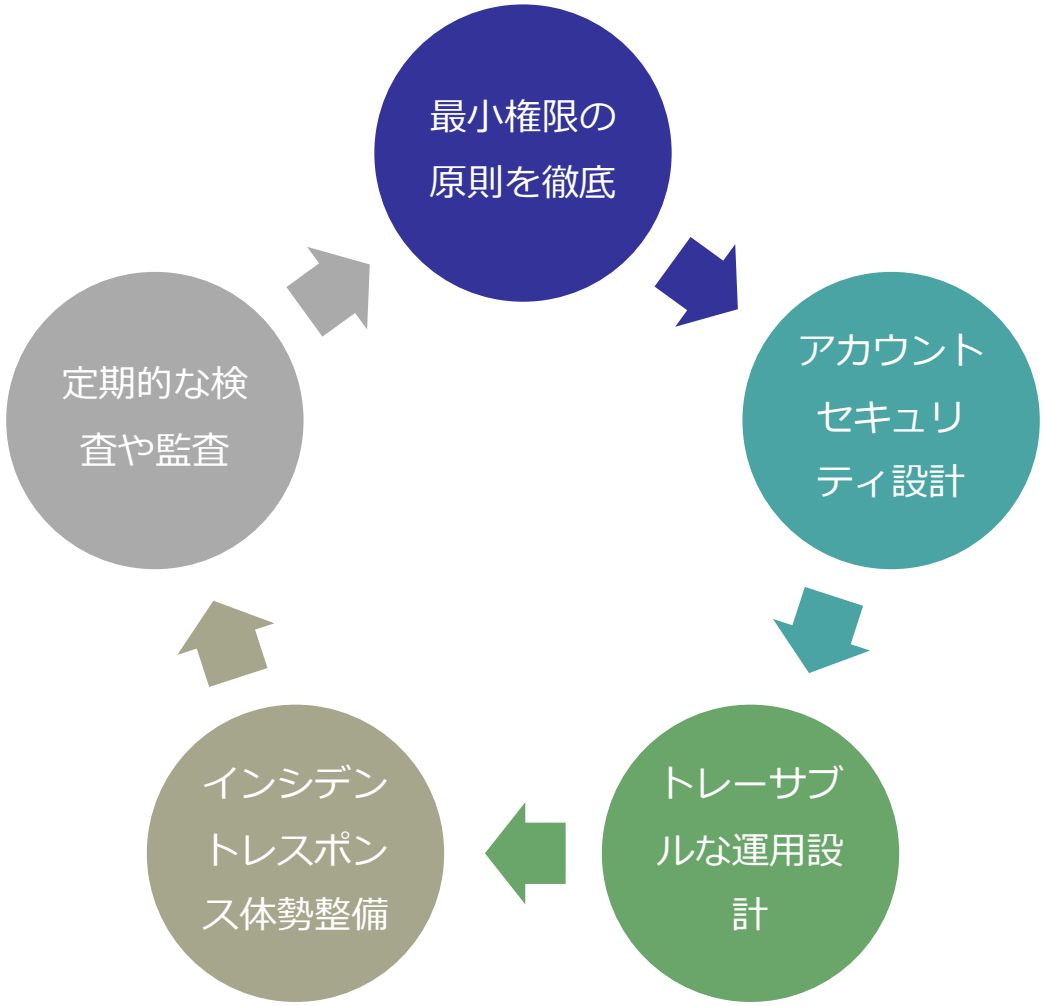
https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/10/top-threats-to-cloud-computing-egregious-eleven_J_20191031.pdf

アカウントハイジャックのDevSecOps

- アカウントにフォーカス



アカウントハイジャックのポイントまとめ



DevSecOpsの最適利用

- 視点
  - ✓Dev だけではダメ、Opsだけでもダメ、Secだけでもダメ
- 全レイヤーへセキュリティを実装
  - ✓アプリケーションやシステムを最適化
- ビジネスアジリティの向上
  - ✓売り上げ向上
  - ✓新領域への挑戦

※DevSecOps をスルーすると成長が望めないどころか衰退の恐れも!?

今後のDevSecOps

- DevSecOps に最適なツールやサービス
- DevSecOps に Biz をより適切に取り入れるスタイル
  - ✓Biz-DevSecOps
  - ✓BSOD (Biz-SecOpsDev)
    - よりBiz と Ops にフォーカス
- エンタープライズレディなアジャイルの採用
  - ✓エンタープライズアジャイルやハイブリッドアジャイル等
- より高度な組織設計
  - ✓CCoE (Cloud Center of Excellence) の多層化


cloud
CSA
security
alliance SM


cloud
CSAJC
security
alliance SM
Japan Chapter

Thanks!