CSA Mobile

CSA JC Japan Chapter cloud security alliance SM

クラウドファースト時代のモバイルアプリケーションセキュリティとDevOps

November 22, 2016
Eiji Sasahara, Ph.D., MBA
Mobile WG
Cloud Security Alliance

CSA Mobile

Agenda

1. CSAにおけるモバイルアプリケーションセキュリティの取組
2. 「クラウドファースト」がモバイルアプリケーション開発に及ぼす影響
3. DevOpsとは？
4. CSAにおけるDevOpsの取組
5. DevOpsを活用したセキュリティのエコシステム作りの課題

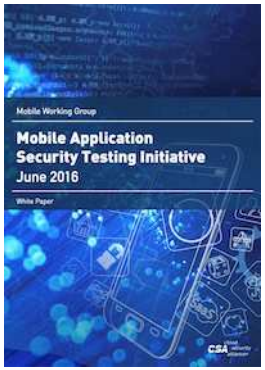
CSAJC cloud security alliance Japan Chapter

1.CSAにおけるモバイルアプリケーションセキュリティの取組(1)

- CSA Mobile Working Group
（https://cloudsecurityalliance.org/research/mobile/）
  - 代表幹事: David Lingenfelter
    Cesare Garlati
  - 過去の主な活動実績
    - 2012年9月：モバイルデバイスのライフサイクルセキュリティ管理における構成要素をまとめた「Mobile Device Management: Key Components, V1.0」を公表
    - 2012年10月：企業環境におけるモバイルデバイスセキュリティの脅威に関するアンケート結果をまとめた報告書「Top Mobile Threats」を公表
    - 2012年11月：モバイルの定義、モバイルコンピューティングの現状に加えて、Bring Your Own Device (BYOD)、認証、App Stores、モバイルデバイス管理（MDM）など、モバイル利用上の留意点を整理した「Security Guidance for Critical Areas of Mobile Computing V1.0」を公表
    - 2015年4月：IoTの初期導入企業・開発者向けのセキュリティ対策指針「New Security Guidance for Early Adopters of the IoT」を公表
    - 2016年6月：モバイルアプリケーション開発におけるセキュリティ／プライバシー・バイ・デザインを実現するためのフレームワークを整理した「Mobile Application Security Testing (MAST) Initiative V1.0」を公表

CSA Mobile

1.CSAにおけるモバイルアプリケーションセキュリティの取組(2)

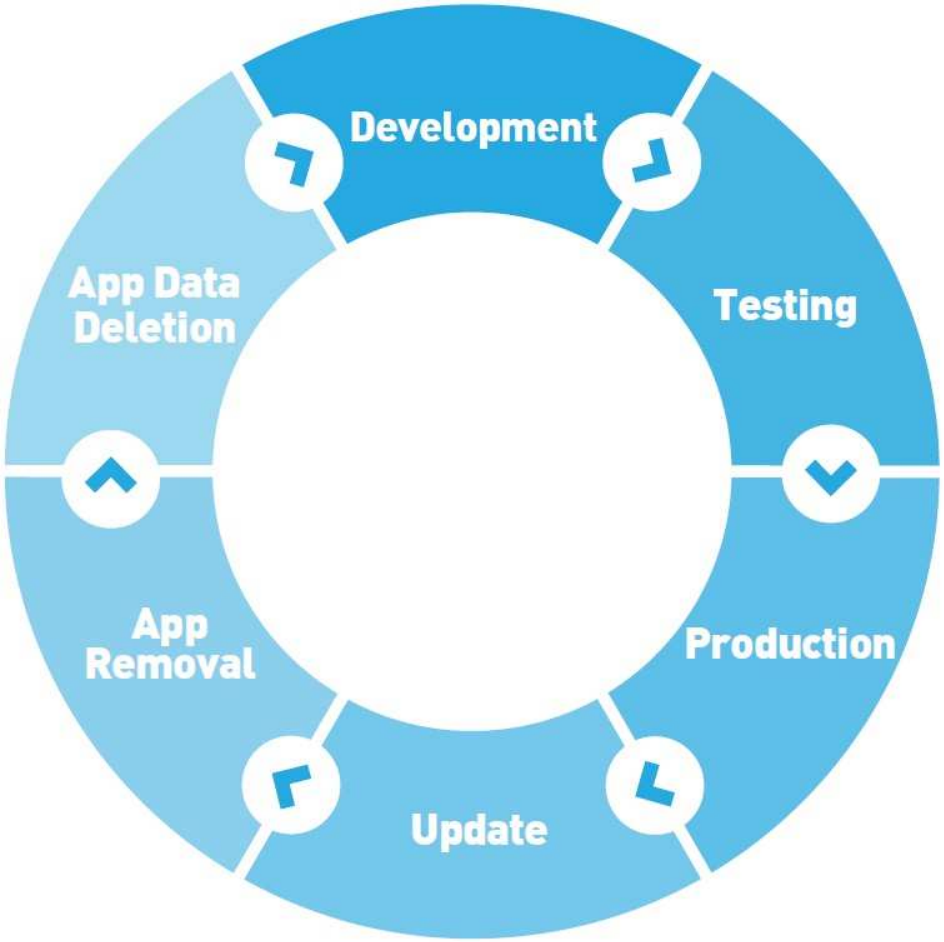


- 「Mobile Application Security Testing (MAST) Initiative V1.0」
  - 業務用モバイルアプリケーション開発にフォーカス
  - 参照規格
    - CSA Security Guidance for Critical Areas of Mobile Computing
    - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
    - NIST SP 800-163, Vetting the Security of Mobile Applications
    - OWASP Mobile Security Project 他

CSAJC Japan Chapter cloud security alliance℠

1.CSAにおけるモバイルアプリケーションセキュリティの取組(3)

- モバイルアプリケーションセキュリティ管理ライフサイクル



出典：CSA Mobile WG「Mobile Application Security Testing Initiative V1.0」（2016年6月）

CSA Mobile

1.CSAにおけるモバイルアプリケーションセキュリティの取組(4)


NIST Special Publication 800-163

Vetting the Security of Mobile Applications

COMPUTER SECURITY

NIST

- モバイルアプリケーションセキュリティの要求事項
  - プライバシーの取扱
    - パーミッションの悪用
      - 悪意のある目的のための不適正なパーミッション要求
      - 意図的に隠されたパーミッションの利用
      - カスタムメイドのパーミッション
    - 不適正な情報開示
      - 不適正な周辺情報の開示
      - アプリケーション内部の行為
  - ネイティブの問題
    - API/ライブラリ固有のリスク
      - 潜在的なAPIのリスク
      - 潜在的なライブラリのリスク
      - インジェクションのリスク
    - アプリケーションの共謀行為
      - データソース／宛先の共謀
      - ブロードキャストレシーバのコンポーネントもしくは同等のもの
      - データ生成／修正／削除
    - 開発難読化の懸念
      - ネイティブコード実行の難読化
      - コールのマッピングにおける問題
      - 娯楽としての難読化

CSA JC cloud security alliance Japan Chapter

1.CSAにおけるモバイルアプリケーションセキュリティの取組(5)

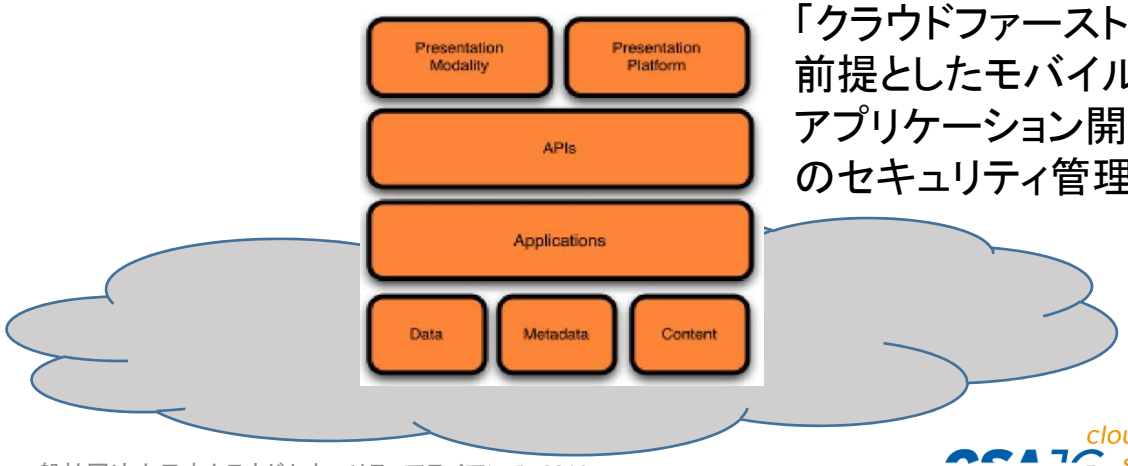
- モバイルアプリケーションセキュリティの要求事項（続き）
  - 保護の要求事項
    - コネクション暗号化強度
      - コネクションの保護
      - 暗号化強度と多要素認証
    - データストレージ
      - ストレージの機能とロケーション
      - プライベート・機微な情報の保護
  - 実行環境
    - 電力消費
      - CPU 使用率
      - I/Oの問題


NIST Special Publication 800-163

Vetting the Security of Mobile Applications

COMPUTER SECURITY

NIST



「クラウドファースト」を前提としたモバイルアプリケーション開発のセキュリティ管理策

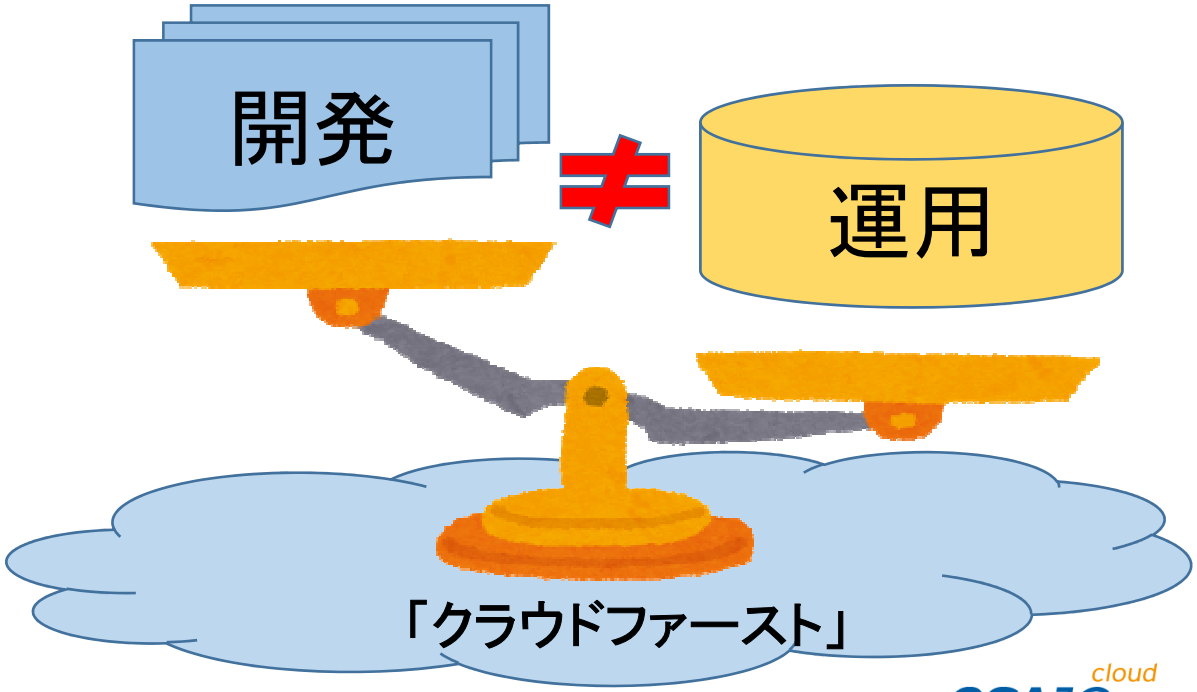
CSA Mobile

2.「クラウドファースト」がモバイルアプリケーション開発に及ぼす影響

- クラウドサービスプロバイダーのPaaS拡充策
  - 業務システムの開発から運用までPaaSで包括的にサポート
  - PaaSからマイクロサービス構築支援ツールへ
    （例）「Azure Service Fabric」
- 業務システムのモバイル化／マルチデバイス化
  - アプリケーションライフサイクルの短期化
  - 開発と運用の隙間がセキュリティのリスク要因に

・「運用でカバー」の時代の終焉

・開発から運用・廃棄までのライフサイクル管理を効率化するツールの登場
＝「DevOps」



CSA JC Japan Chapter cloud security alliance℠

CSA Mobile

3.DevOpsとは？

DevOpsの定義

・IDC：DevOpsは開発（Development）と運用（Operations）を組み合わせた用語で、開発担当者と運用担当者が連携して協力し、ビジネスからの要求に対して、アプリケーションの開発や導入を迅速かつ柔軟に行うこと。

・Gartner：ITシステムにおける迅速かつリーンな実践を通して、ITサービスデリバリをより速く実行することに焦点を当てたITカルチャーの変革。加えて人や文化を中心に据え、運用チームと開発チームのコラボレーションの改善、迅速性を重視した新たなITサービスデリバリのためのアプローチ。

CSAJC cloud security alliance Japan Chapter

CSA Mobile

4.CSAにおけるDevOpsの取組(1)

cloud CSA security alliance®

CSA Security Guidance for Critical Areas of Focus in Cloud Computing v.4(策定中)

≪Domain 10: Application Security≫

- DevOpsの普及と役割
  - 定義
  - デプロイパイプラインと継続的な導入／配布
  - セキュリティの意味合いと利点
    - 標準化
    - テストの自動化
    - 監査と変更管理の改善
  - SecDevOps、Rugged DevSecOps

CSAJC Japan Chapter cloud security alliance℠

CSA Mobile

4.CSAにおけるDevOpsの取組(2)

CSA各支部に広がるDevOpsの考え方

CSAJC cloud security alliance Japan Chapter

CSA Mobile

5.DevOpsを活用したセキュリティのエコシステム作りの課題

cloud CSA security alliance®

「クラウドファースト」環境におけるDevOpsの課題

- クラウド固有の特徴がDevOpsに及ぼす影響
  - 本番環境とその他の環境の間で簡単に切替できる
  - 仮想マシンを簡単に作成できる
  - RDB、NoSQLなど、様々なデータベースを複数利用できる
- DevOps利用時のセキュリティ留意事項
  - セキュリティ監査対応における開発と運用の調整
  - デプロイパイプラインの安全確保策
  - マイクロサービスアーキテクチャ固有の課題（例．コンポーネントのセキュリティ）