IBM **Watson** Summit 2017
Cognitive and Cloud

【E2-1】

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

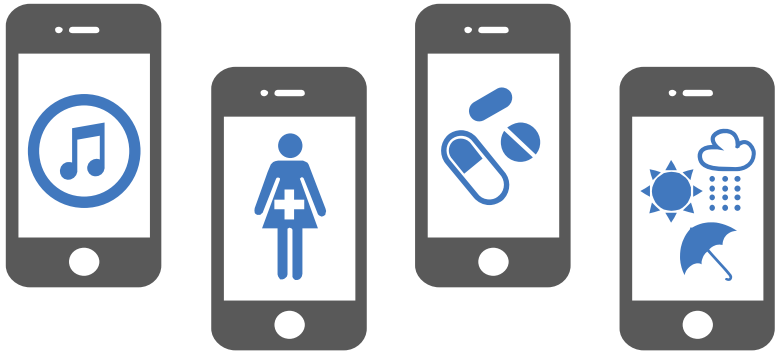
- 株式会社エムティーアイの概要
- モバイル・アプリは危険なのか?
- モバイル・アプリの脆弱性とは?
- 具体的な脆弱性診断の流れは?
- music.jp アプリが安全な理由！

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

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

「music.jp ®」「ルナルナ」をはじめとする多彩なアプリ



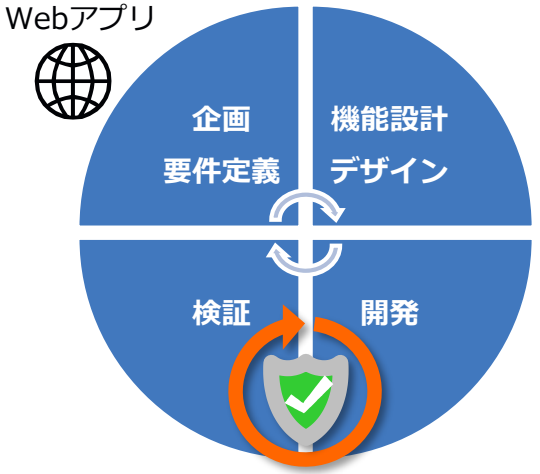
- 売上高 32,844百万円
- 営業利益 5,355百万円

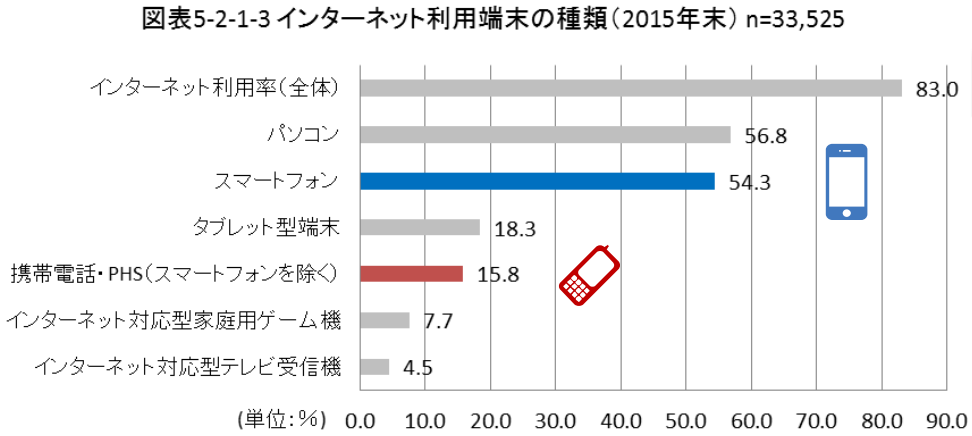
2016年9月期

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ー検証/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ネルが、Webベースから**モバイル・アプリ**へと大きくシフト





Source: 総務省 平成27年「通信利用動向調査」

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ー検証/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

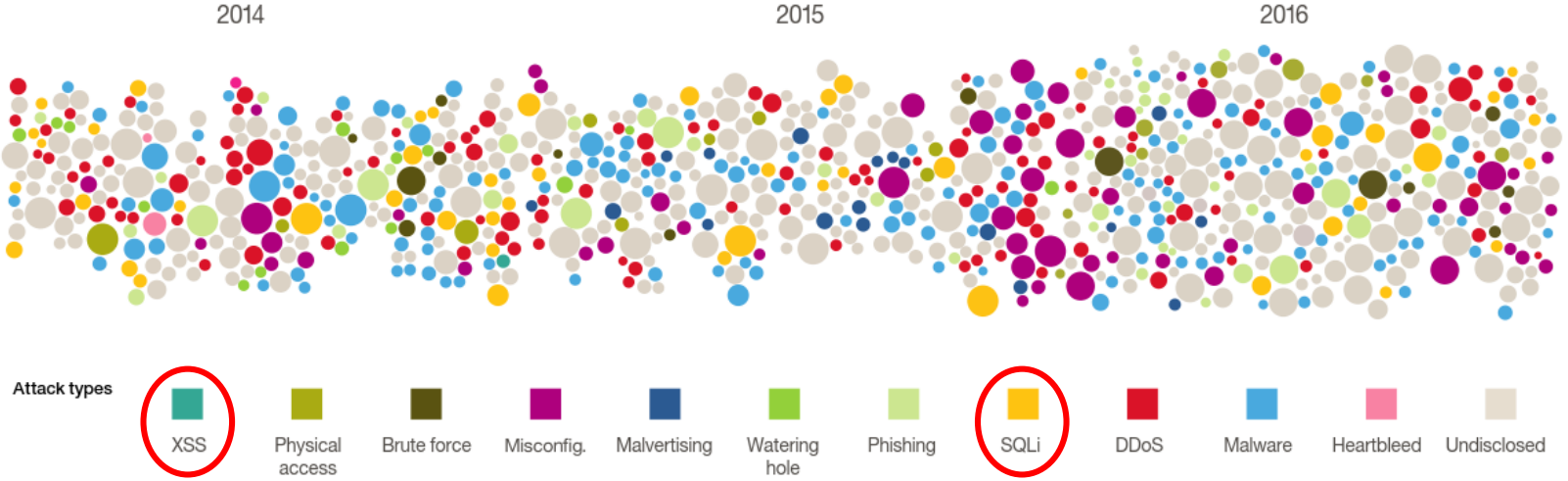
ライフ・エンターテインメント 事業本部
music.jpシステム統括部 システム運用部 部長
大久保 真勝 様　（2017年3月31日現在）

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 10億レコード以上の侵害	2015 前例のない 高価値ターゲットの侵害	2016 情報漏えいレコード数と発見された脆弱性が歴史的な件数に



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**

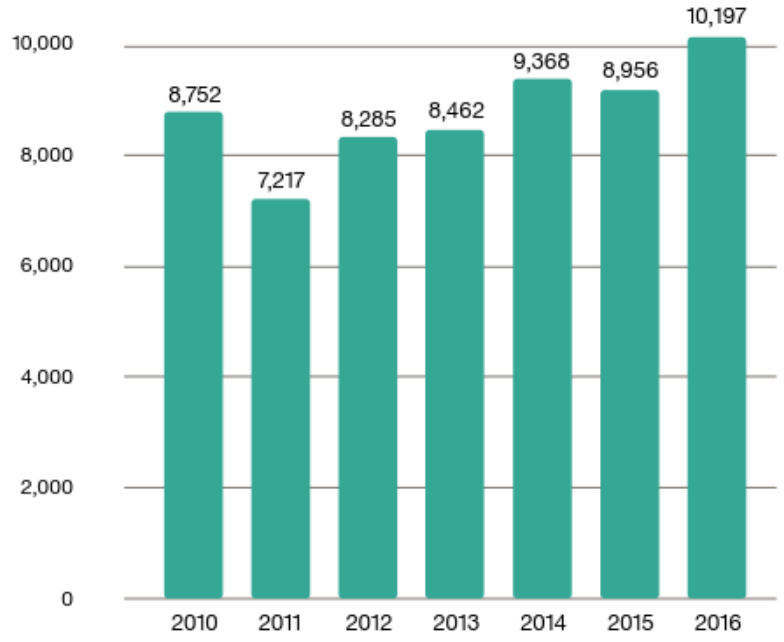
Source: The 10 Most Common Application Attacks in Action, April 2015

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**セキュリティー予算**を計上していない

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

セキュリティー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

★★½☆☆ 2.4

183 ユーザー

ストア認定
デベロッパー

100
万

ダウンロード

★★★★½ 4.3

14,968 ユーザー

セキュリティーはどうでしょう?

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

★★½☆☆ 2.4

183 ユーザー

ストア認定
デベロッパー

100
万

ダウンロード

★★★★½ 4.3

14,968 ユーザー

印象は...

Not Tested

Tested

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

★★½☆☆ 2.4

183 ユーザー

Not Tested

現実は...

ストア認定
デベロッパー

100 万

ダウンロード

★★★★½ 4.3

14,968 ユーザー

Not Tested

ストアの審査では脆弱性まで見つけてくれない

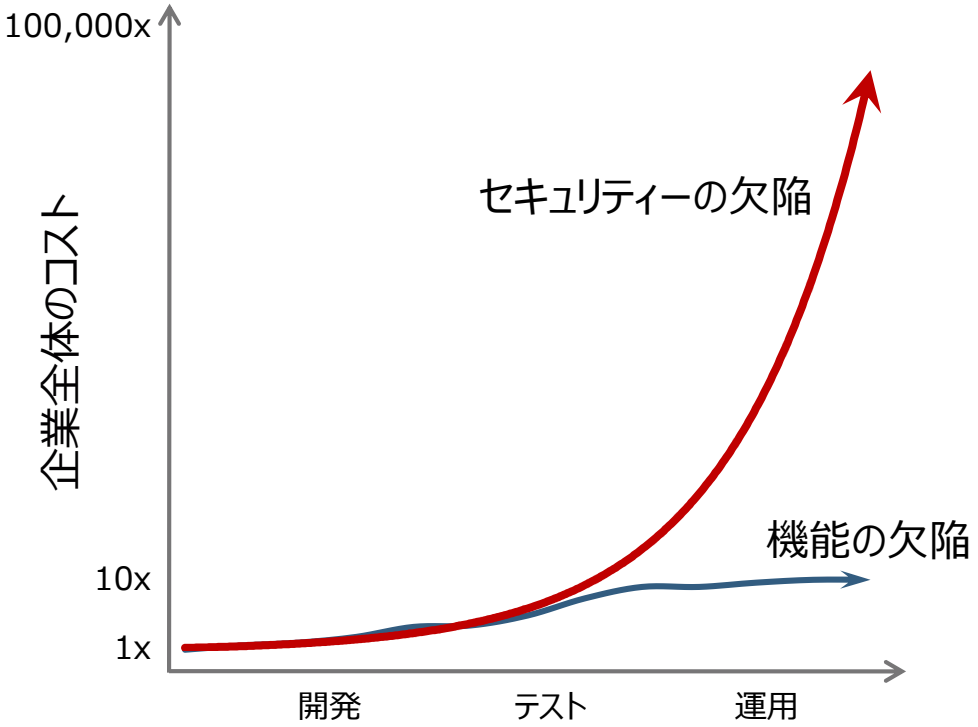
- マルウェアに感染していた場合
  ➔ 審査で (きっと) リジェクトされる

  …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がある！

セキュリティー欠陥は予期しないコストを発生させます



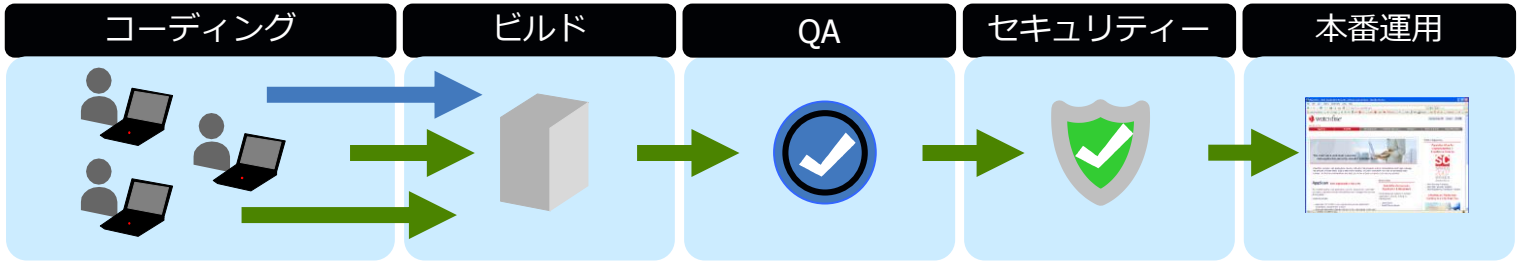
予期せぬコスト:

- 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 **

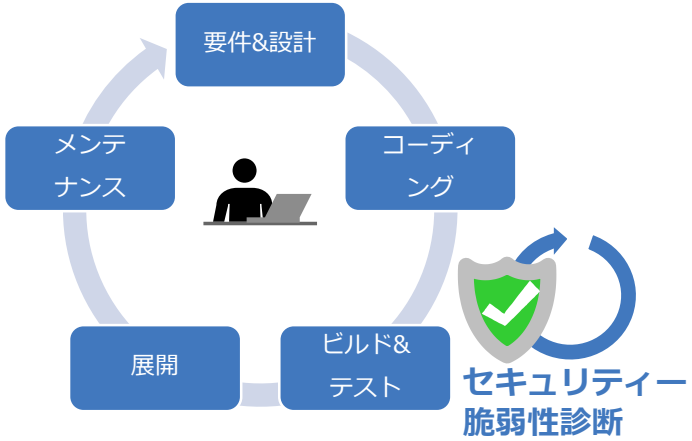


開発時の発見	ビルド時の発見	QA/テスト時の発見	リリース後の発見
問題ごとに $80	問題ごとに $240	問題ごとに $960	問題ごとに $7,600
アプリごとに $8,000 *	アプリごとに $24,000 *	アプリごとに $96,000 *	アプリごとに $760,000 *

** 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

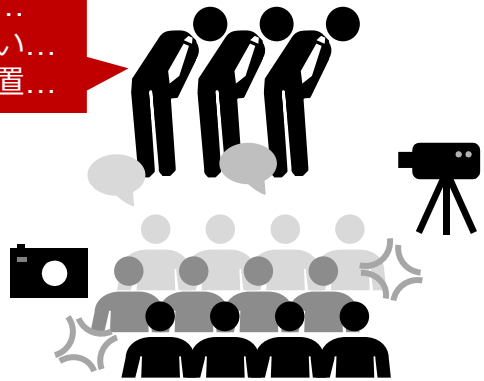
こちら?

それとも、こちら?

問題を放置した後に...

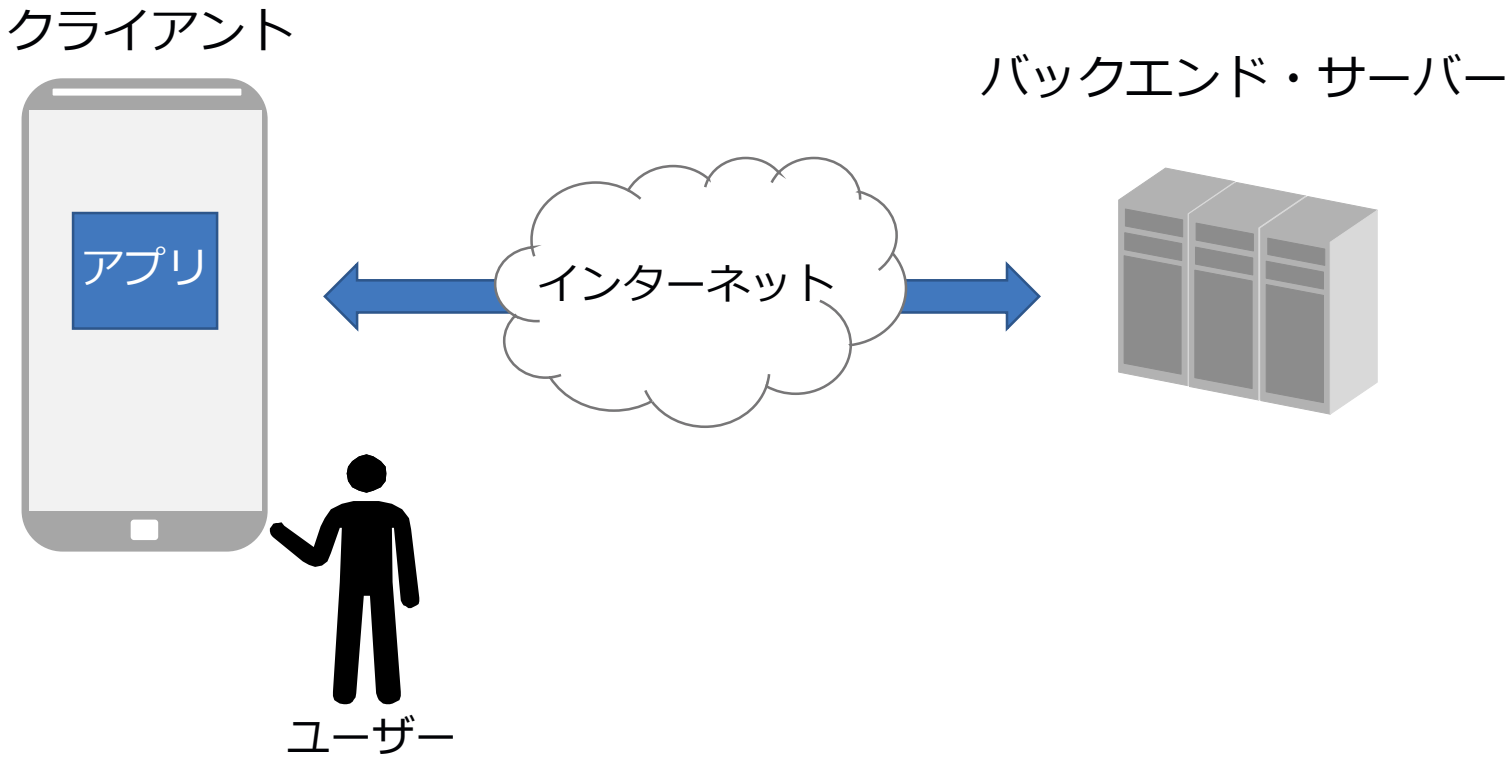
- 高コスト
- 大変な苦労
- 著しい混乱

個人情報…
データ漏えい…
脆弱性を放置…

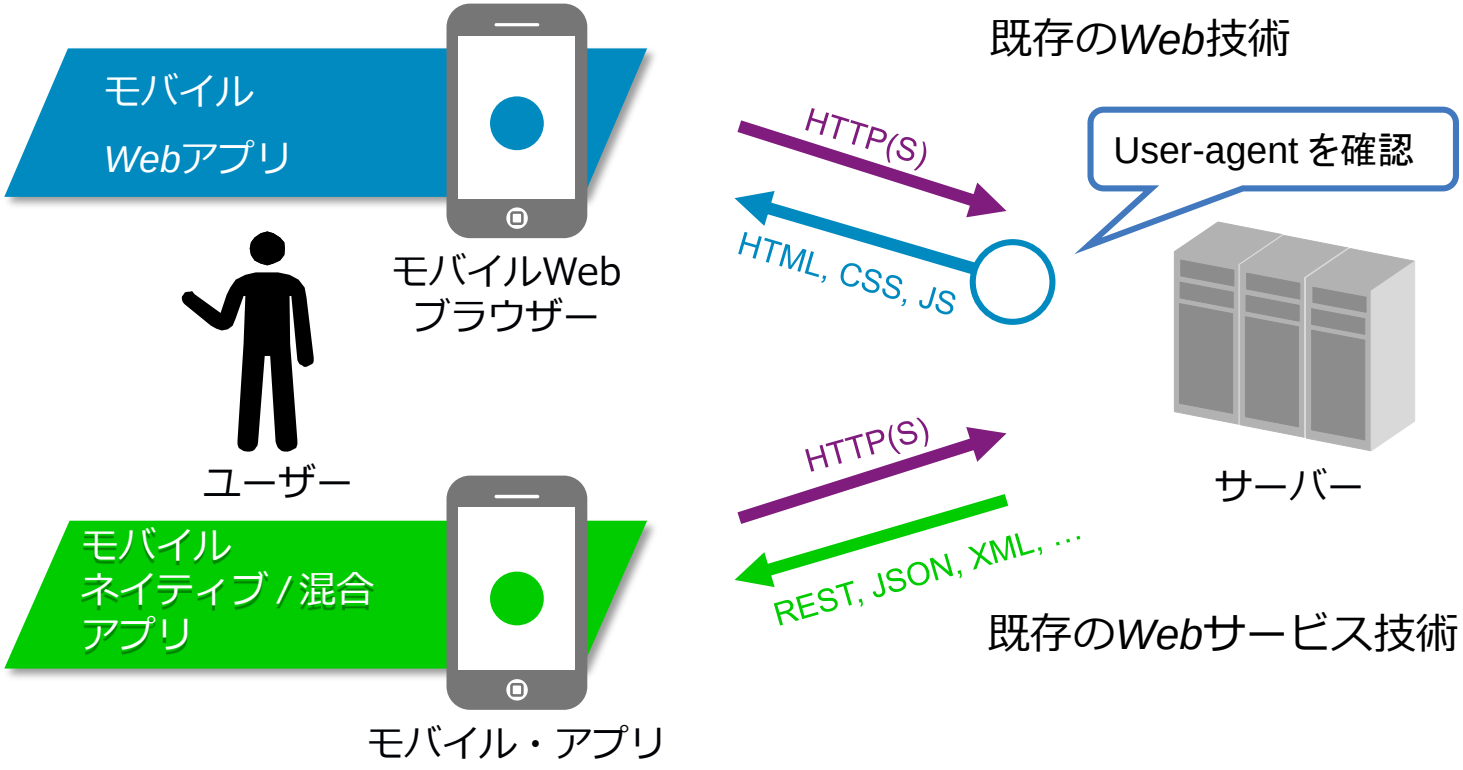


モバイル・アプリの脆弱性とは?

典型的なモバイル・アプリケーション



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

表示、操作、単一ユーザーのデータとアクション

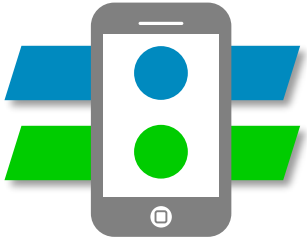
ビジネス・ロジック、多数のユーザー、*DB*、ログ、個人情報

- 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)

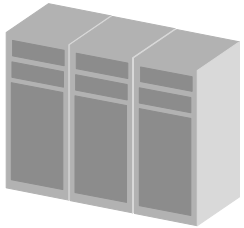
- Webサービス・インターフェース

モバイル・アプリケーションの脆弱性領域

クライアント



サーバー



新たな
クライアント側の
脆弱性:

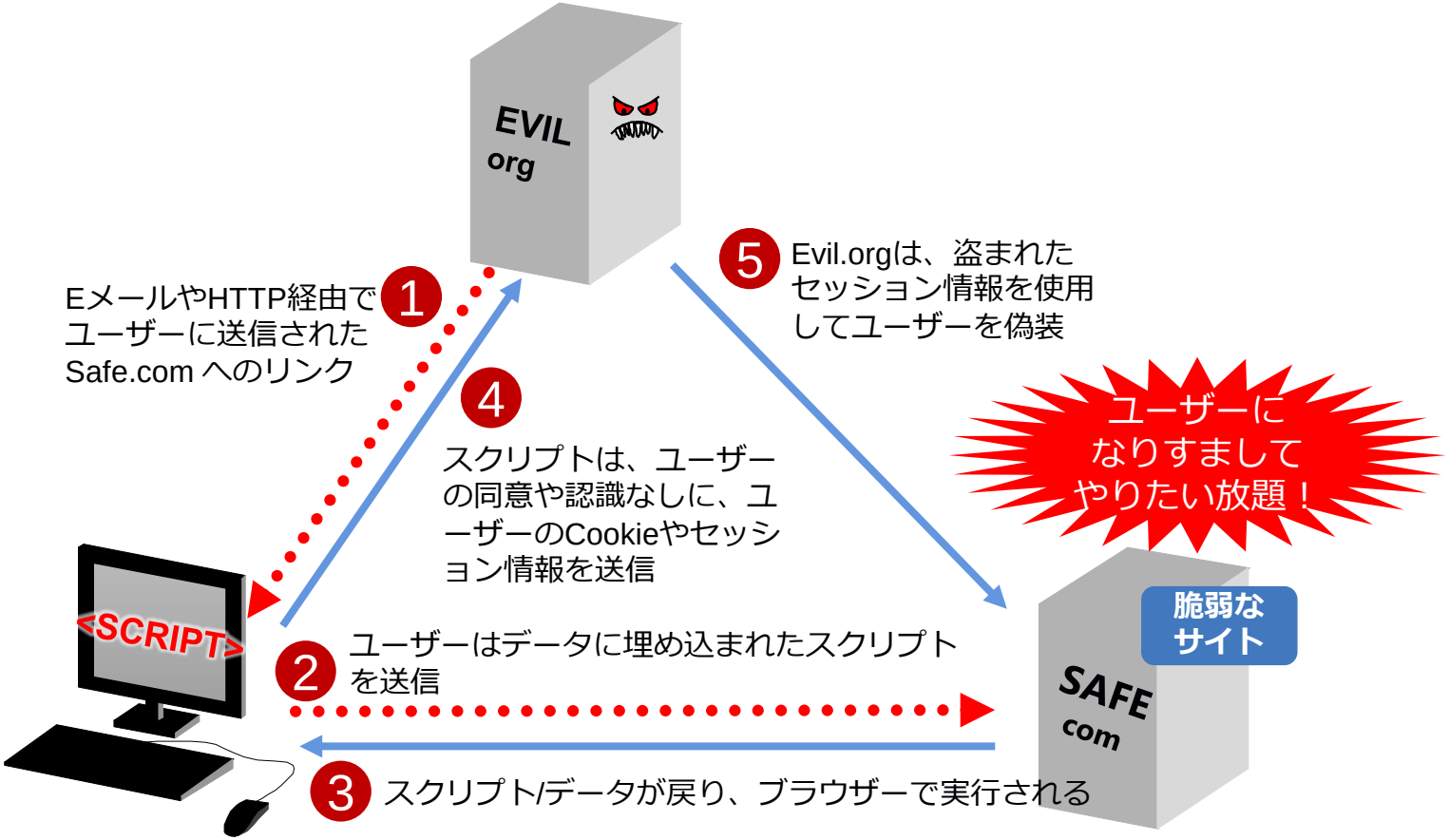
従来の
バックエンドの
脆弱性:

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

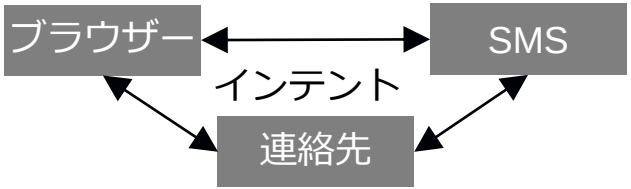
一般的なWebアプリと共通:
*SQL*インジェクション, パストラバーサル, 応答分割, *File Inclusion*, *OS*のコマンド実行 など

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?



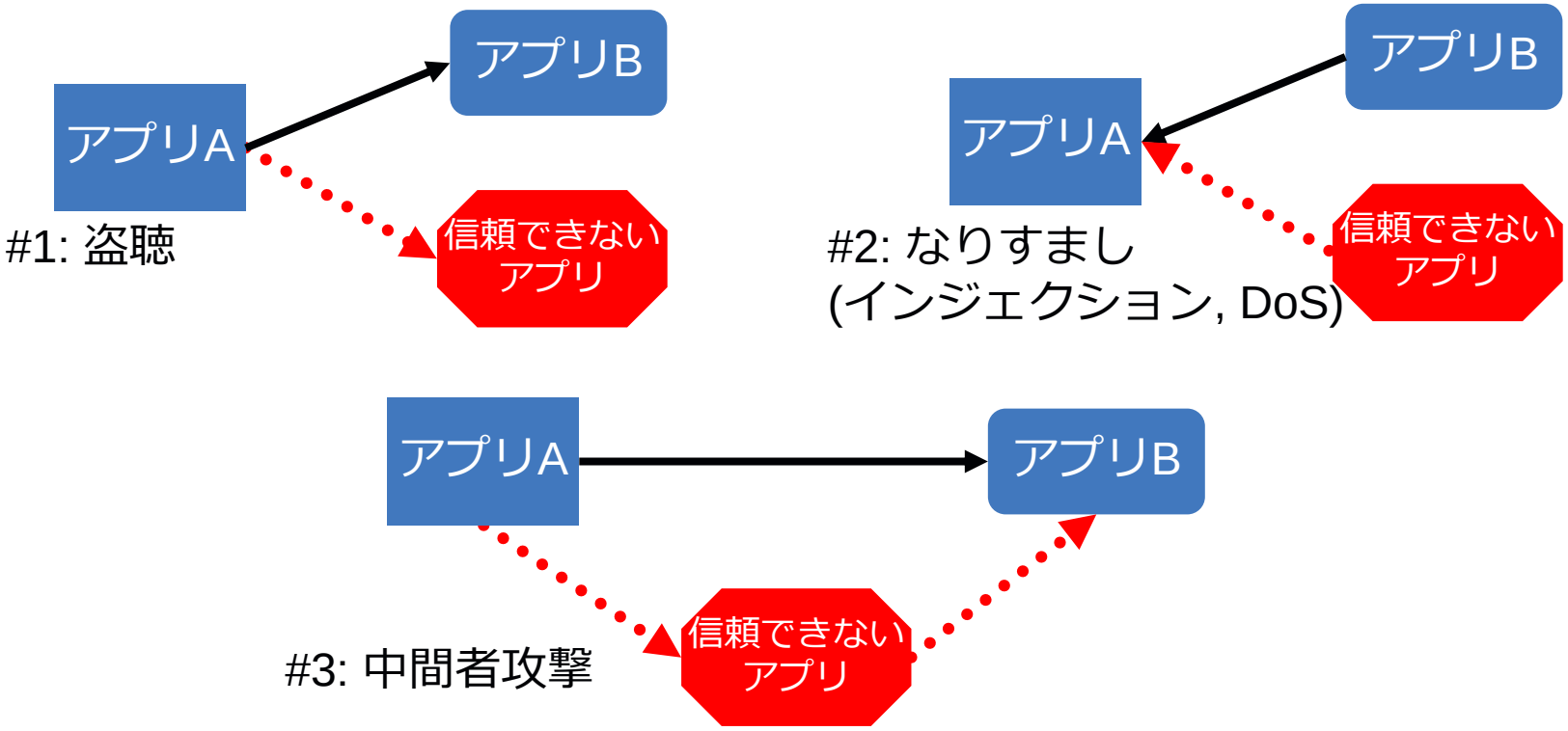
モバイル・アプリケーションのリスク (Android例)

- 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

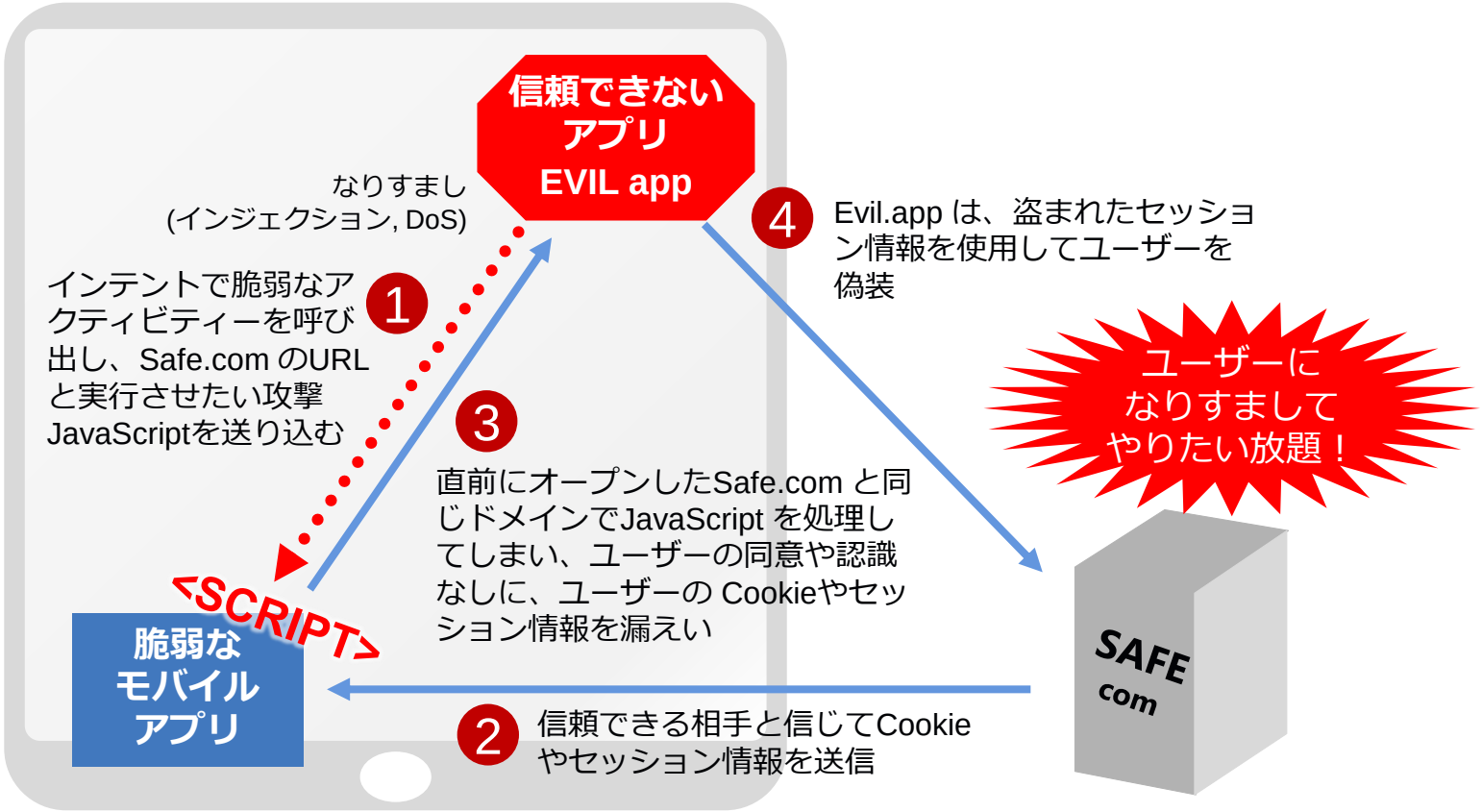
アプリケーション間通信を使った脆弱性のタイプ



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

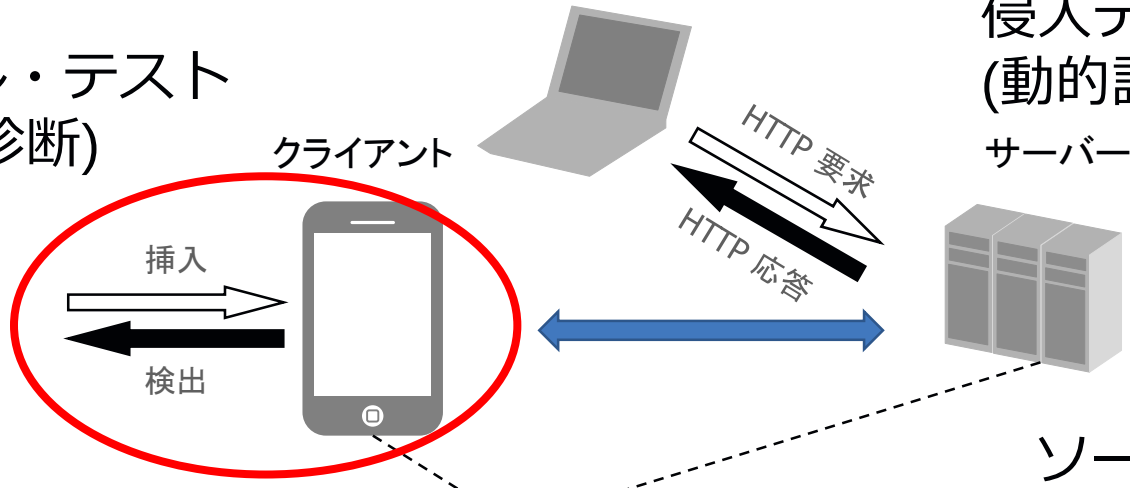
モバイル脆弱性の例：クロス・アプリケーション・スクリプティング (XAS) とは?

Android Browser XAS (CVE-2011-2357)



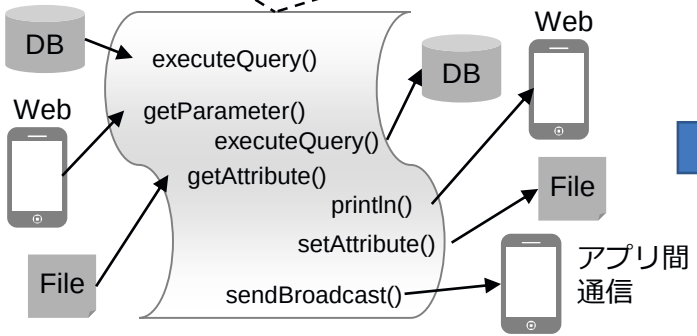
アプリケーションの脆弱性と診断方法

モバイル・テスト
(対話型診断)

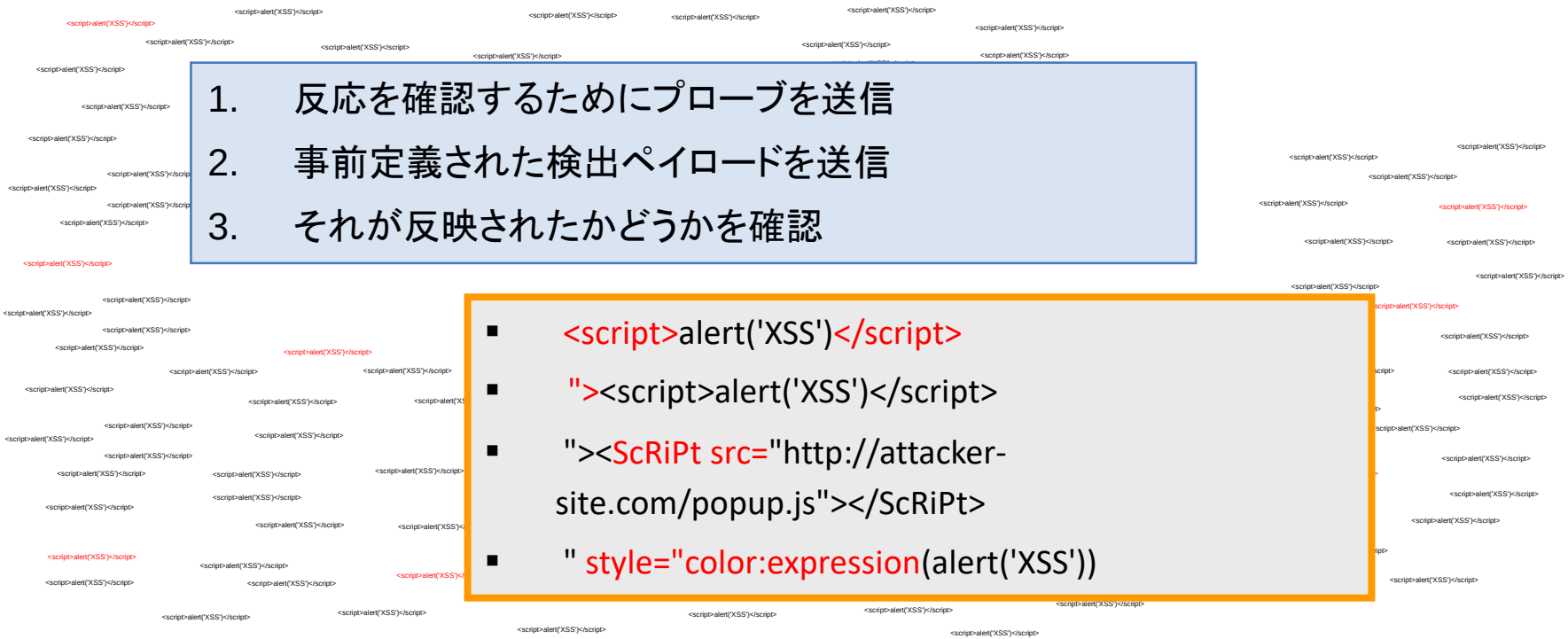


侵入テスト
(動的診断)

ソースコード・テスト
(静的診断)



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、動的にインテントのパラメーターを学習する

- **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インテントを送信する

- **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のセキュリティー・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、セキュリティー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のセキュリティー・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ーを呼び出します。
  - 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いものの、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?

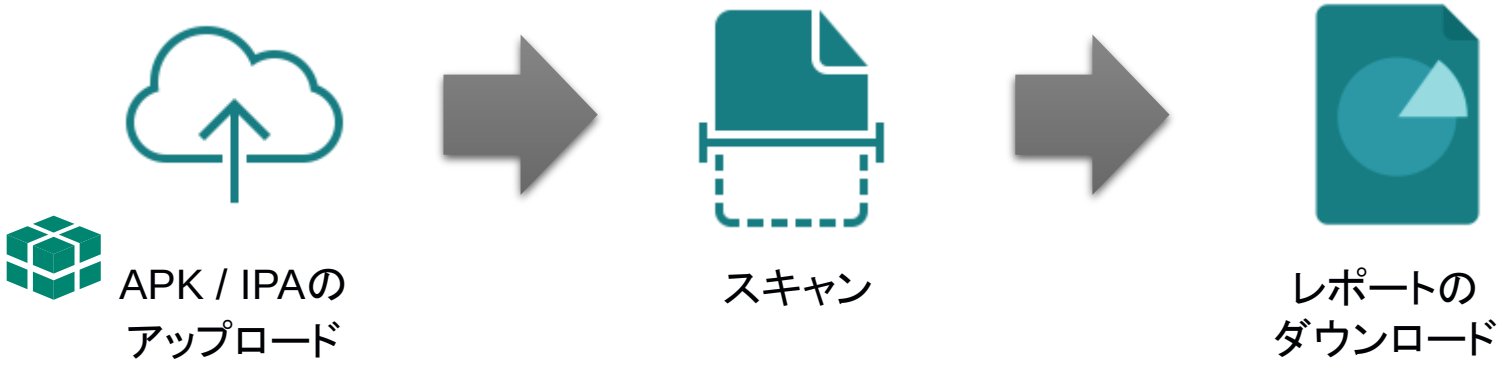
Application Security on Cloud (ASoC)

- 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

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

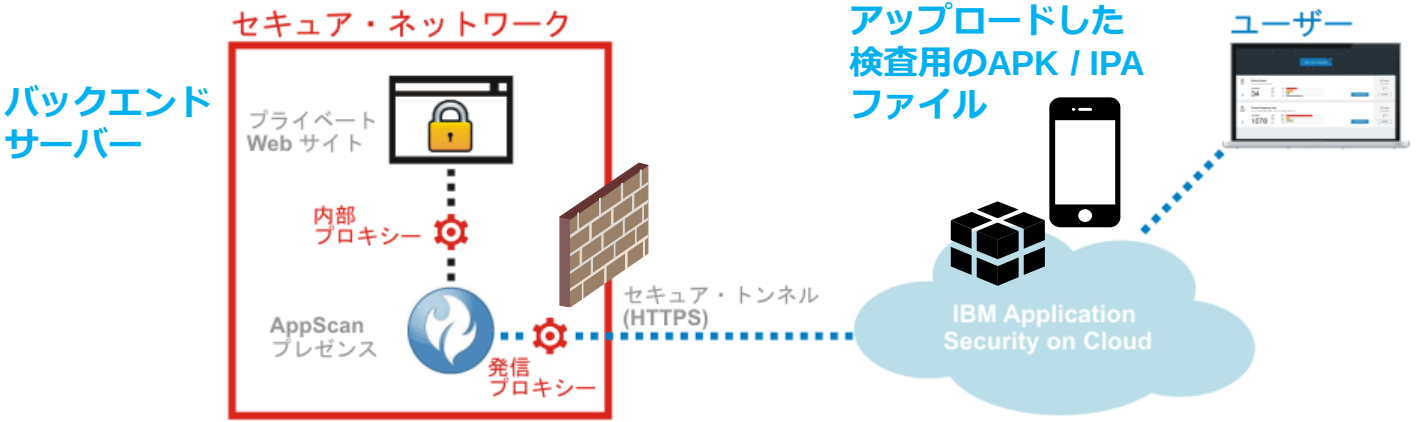
Mobile Analyzer：スキャンの流れ

- 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。

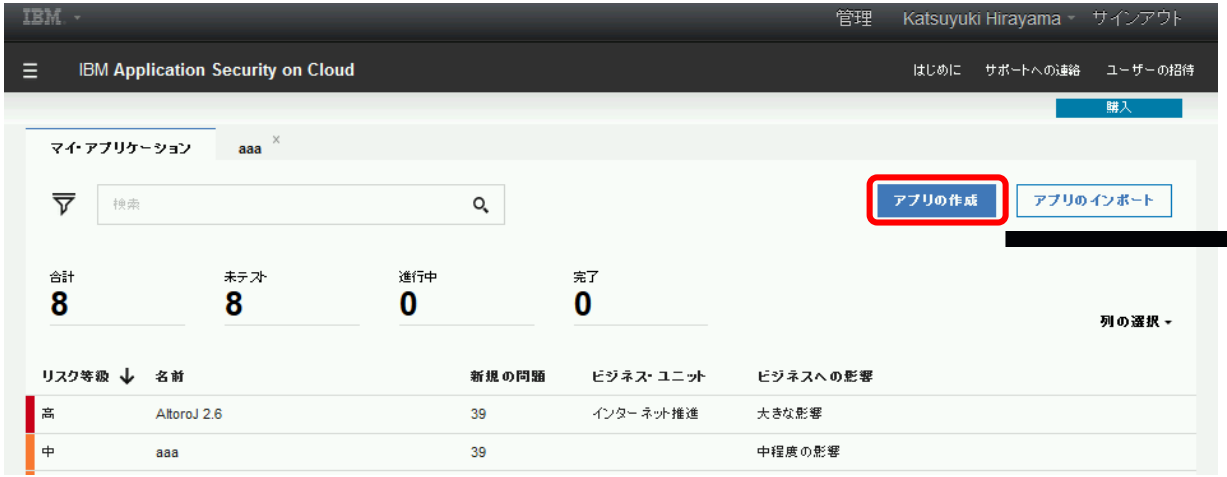


クラウドからイントラへの通信も可能

- 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プロキシーとして機能し、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ー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



サービスの使用：モバイルの場合

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)

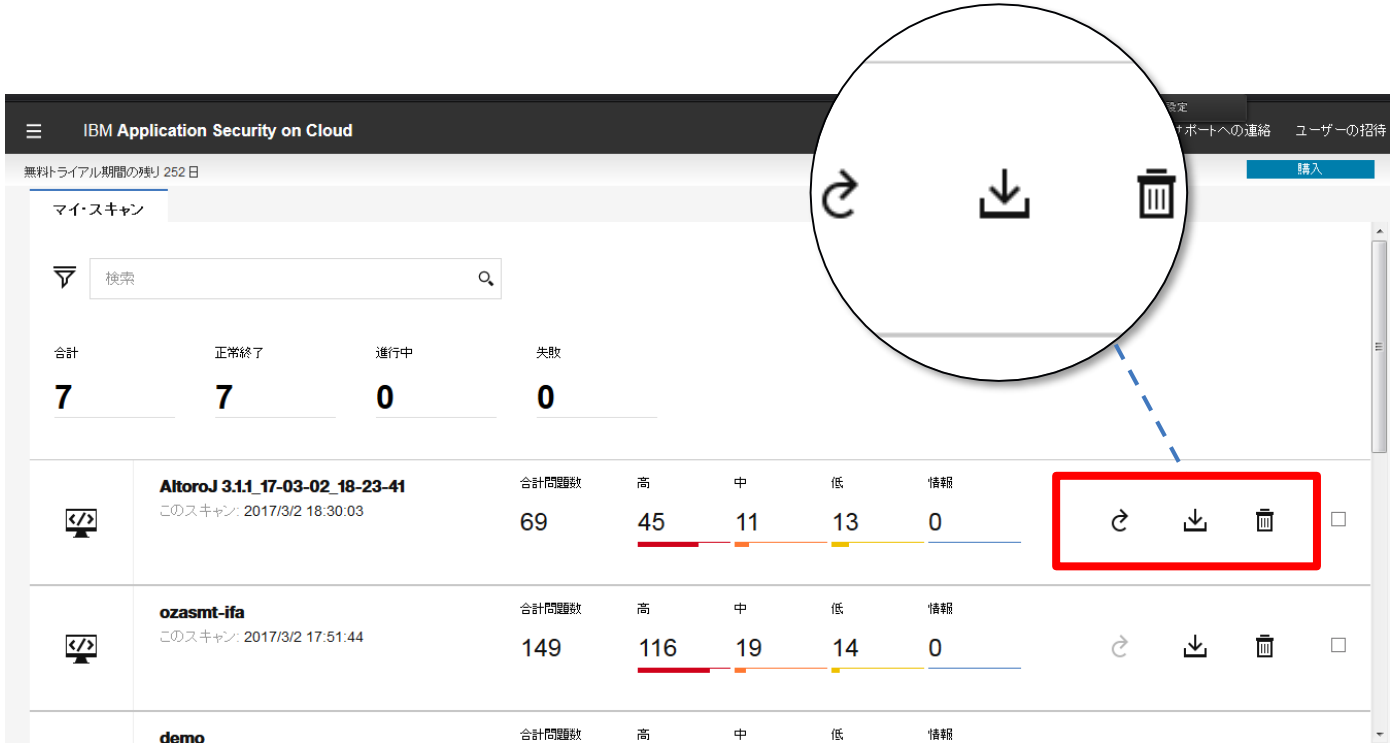
- スキャンに適切な任意の名前を付けます。初期値としてAPKファイル名が反映されています。
- 準備ができたら、「スキャン」をクリックします。

サービスの使用：スキャンの進行状況の表示

スキャン完了時にEメール通知を受けることができます。

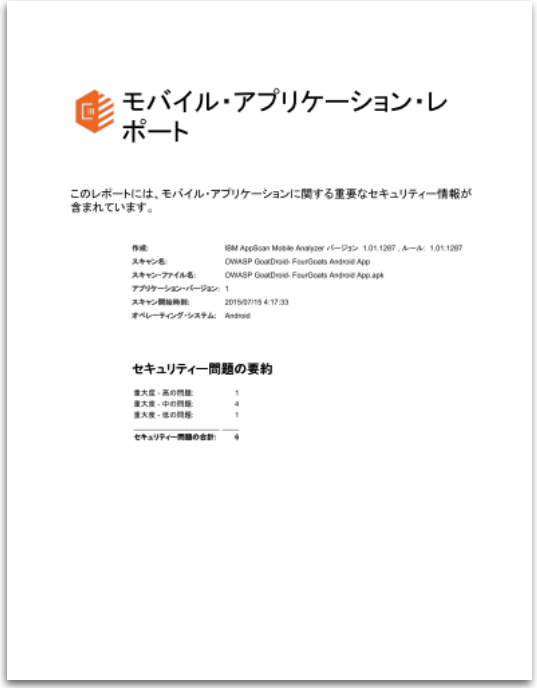
サービスの使用：レポートのダウンロード

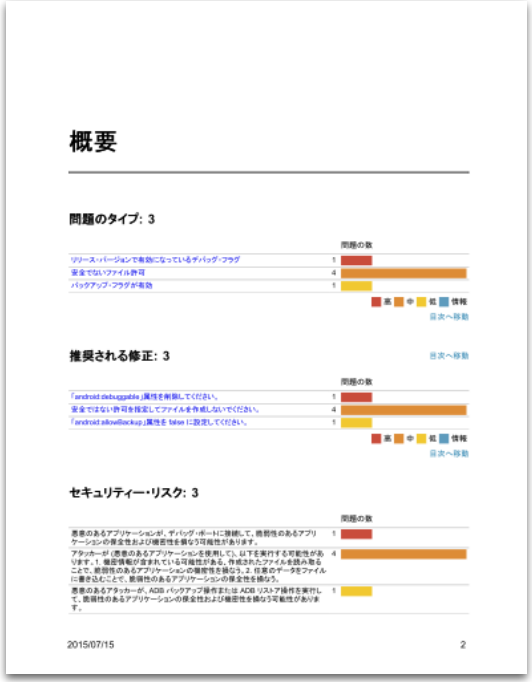
検出結果のHTML, XMLレポートをダウンロードできます。



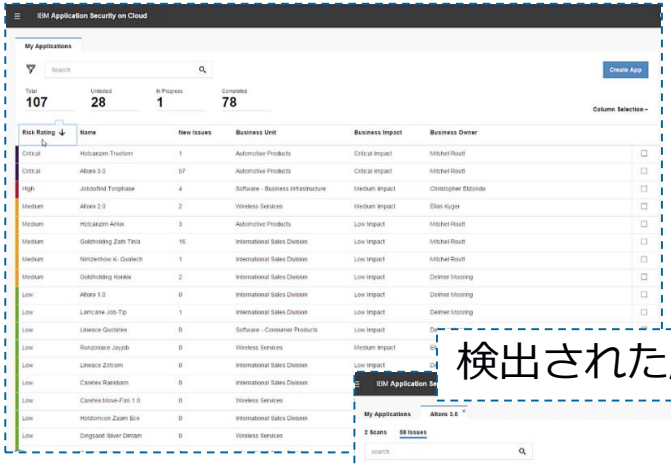
Mobile Analyzer：レポート・サンプル

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

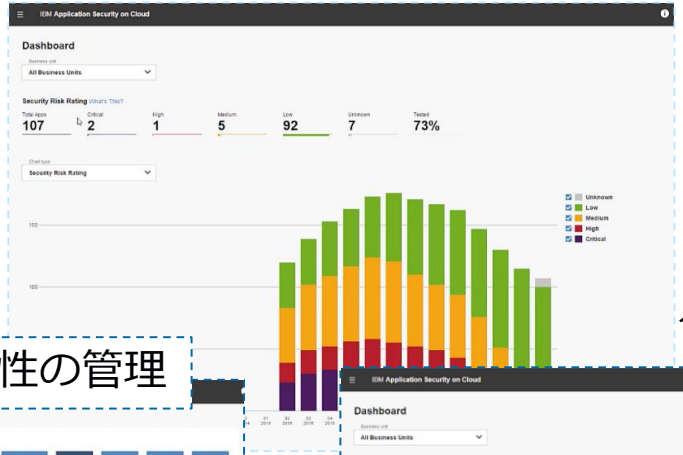




アプリケーション・セキュリティー管理を装備

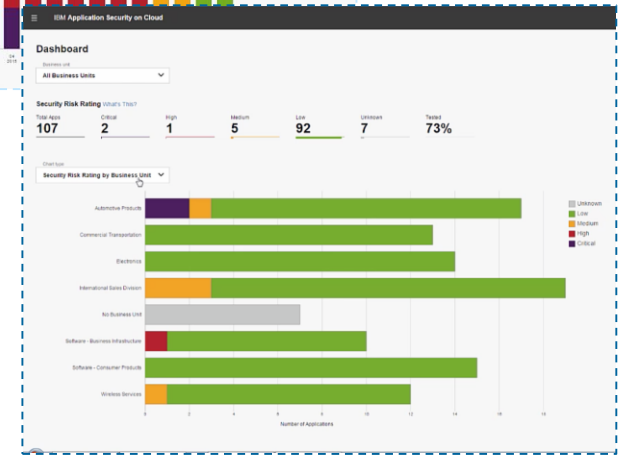


アプリケーション
インベントリーの管理

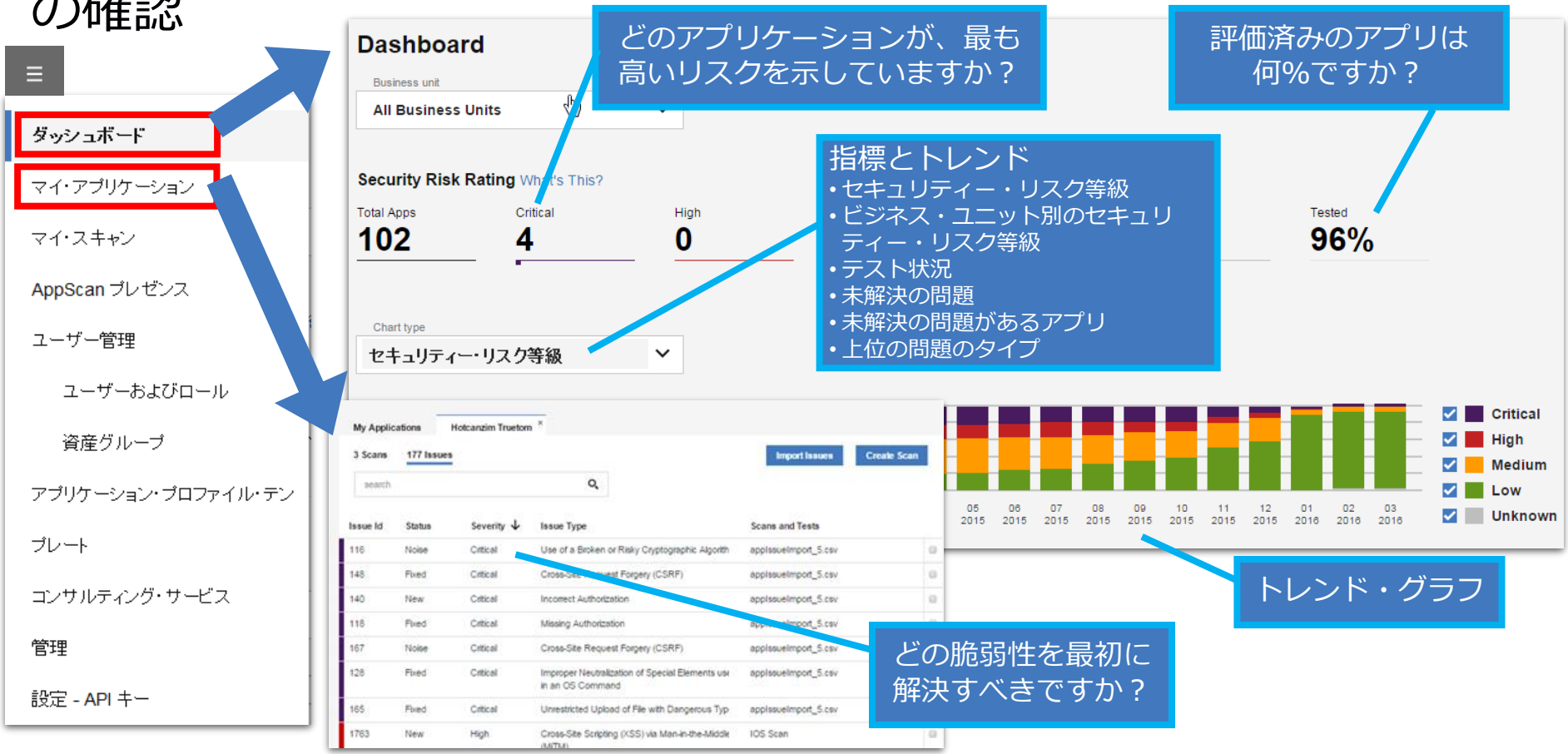


リスクベースの
ダッシュボード

検出された脆弱性の管理



ダッシュボード：アプリケーションのセキュリティー状態と進捗の確認



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

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）

- 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）

- 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ーの推進

- 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ー検証/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
セキュリティー脆弱性診断

- ✓ 初期投資はほとんど不要
- ✓ 最新サイバー攻撃への追随や 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?
- 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！**

- 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

- 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

- 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

- **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ものではなく、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も、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もなく、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も、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。