

平成24年度第1回学術情報基盤オープンフォーラム

スマートフォンの脅威

平成24年7月4日

株式会社ラック
山城 重成

アジェンダ

- ▶ 第一部：株式会社ラック 山城
 - ▶ スマートフォンプラットフォーム
 - ▶ Google Playのセキュリティ
 - ▶ スマートフォン侵入デモ
- ▶ 第二部：株式会社カスペルスキー 前田
 - ▶ マルウェアの統計情報
 - ▶ Androidマルウェアの実例紹介

スマートフォンプラットフォーム

スマートフォンプラットフォーム

▶ さまざまな OS



それぞれの特徴

	Android	iOS	BlackBerry
メーカー	複数	Apple 社	RIM 社
脆弱性対応	メーカーに依存	Apple が対応	RIM が対応
アプリケーションのインストール	<ul style="list-style-type: none">• Android マーケット• サードパーティのマーケット	App Store	BlackBerry App World
アプリ審査	なし	あり	あり

Jailbreak と root 化

- iOS と Android での制限を解除すること
 - Apple によるアプリケーション制限
 - テザリング制限
 - カスタマイズ制限
- やってることは脆弱性を攻撃し、権限昇格、システムの書き換え

iOS の場合

• Jailbreak (脱獄)

Android の場合

• root 化

Jailbreak と root 化

▶ メリット

▶ 各種制限の回避

- ▶ AppStore 以外のアプリケーションインストール
- ▶ テザリング
- ▶ OS レベルでの細かなカスタマイズ
- ▶ 端末情報の改変

▶ デメリット

▶ マルウェア感染の影響拡大

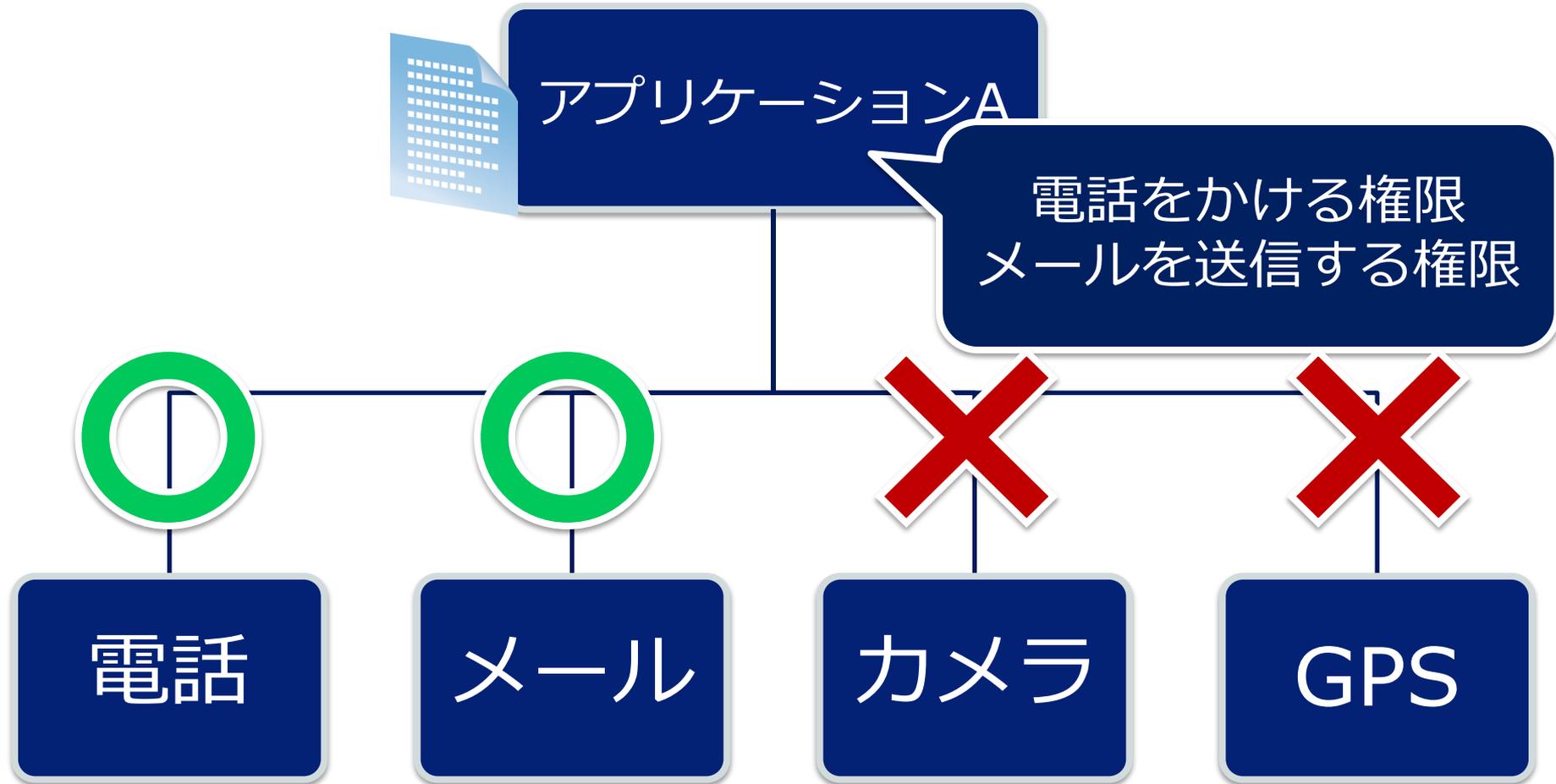
- ▶ システム権限で動作し最悪の場合復旧不可
 - ▶ ウイルス対策ソフトによる駆除も困難
 - ▶ キャリアによる交換・修理対応となる
- ### ▶ メーカーサポートが受けられなくなる可能性

パーミッションの要求

- ▶ アプリケーションをインストールする際に出てくる画面
 - ▶ 端末内データへのアクセス
 - ▶ インターネットへ通信
 - ▶ 設定の変更
 - ▶ 電話の発信
 - ▶ などなど
- ▶ (例) 名刺リーダーアプリ
 - ▶ 名刺画像取り込み -> 「カメラの利用」
 - ▶ アドレス帳へ登録 -> 「連絡先データへの書込」

アプリケーションとパーミッション

- ▶ 各種情報へのアクセスには「権限」が必要



パーミッション確認画面

 Skype SKYPE 同意してダウンロード	 Twitter TWITTER, INC.	 LACCO セキュリティ MOBILE ROADIE
許可	許可	許可
ハードウェアの制御 写真と動画の撮影, 録音, 音声設定	ネットワーク通信 完全なインターネットアクセス	ネットワーク通信 完全なインターネットアクセス >
アカウント アカウントの認証情報を使用, フォロワーを管理, アカウント認証システム	ストレージ USBストレージのコンテンツの変更/削除	システムツール 端末のスリープを無効にする >
個人情報 連絡先データの書き込み, 連絡先を同期	システムツール 同期設定の書き込み, 端末のスリープを無効にする	ストレージ USBストレージのコンテンツの変更/削除 >
ネットワーク通信 Bluetooth接続の作成, 完全なインターネットアクセス	現在地 精細な位置情報 (GPS)	ハードウェアの制御 写真と動画の撮影 >

ほとんどのアプリで要求されるため、見落としがち

アプリマーケット

Google Play

アプリ審査は基本的に無い

- 開発者登録時にクレジットカードカード番号を求める
- 開発者は好きなとき、好きなようにアプリケーションを公開できる
 - 中には「HelloWorld」のようなものも

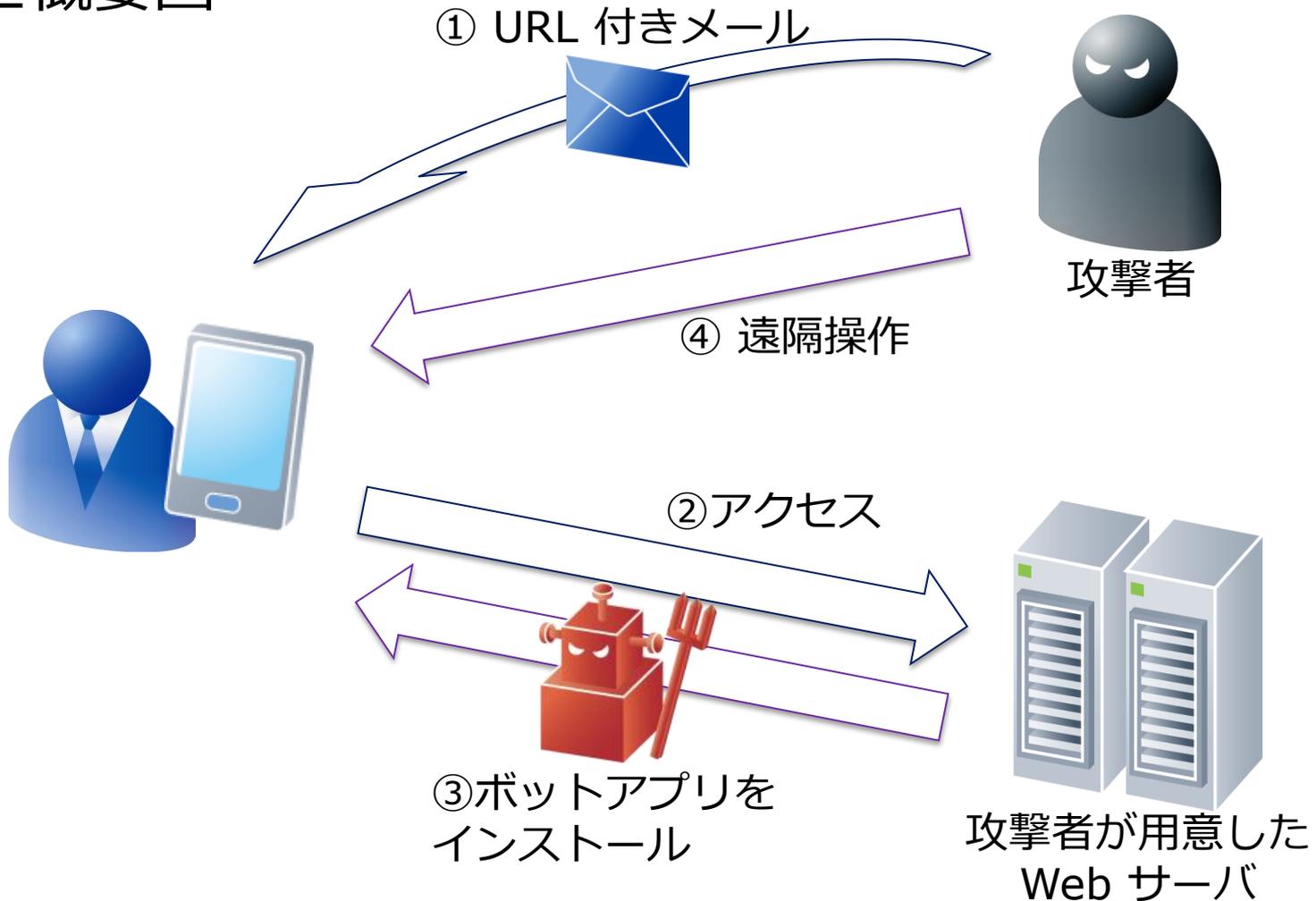
不正アプリの対策

- 報告されたマルウェアを削除
- Bouncer

スマートフォン侵入デモ

スマートフォン侵入デモ

▶ デモ概要図



Next -> Kaspersky 前田氏