スマートフォンセキュリティ

2011年10月5日　NSF in Kansai

ラックホールディングス株式会社
山城 重成

株式会社カスペルスキー
前田 典彦

目次

- スマートフォンのプラットフォーム
- スマートフォンマルウェアの実例
- アプリケーションの信頼性
- 不正アプリによる遠隔操作デモ
- 対策・まとめ

スマートフォンプラットフォーム

- AndroidiOS
- iOS
- WindowsPhone(旧Windows Mobile)

- BlackBerry
- Symbian
- 他 Palm, Brew....

それぞれの特徴

	Android	iOS	Windows Phone
メーカ	複数	Apple社	複数
脆弱性対応	メーカに依存	Appleが対応	端末・OSメーカ
インストール方法	Android Market On The Air キャリアマーケット	AppStore	MarketPlace
アプリ審査	なし	あり	あり

スマートフォンセキュリティモデル

- BlackBerryモデル
  - 通信、アプリケーションともにOSメーカーの一元管理をすることでセキュリティを担保
- iOS・Windows Phoneモデル
  - OSメーカーのアプリケーション審査によるセキュリティを担保
- Androidモデル
  - PCと同様に、ユーザにてセキュリティ対策を行う

iOS JailBreak

- iOSのアプリケーションはアップル社の「電子署名」が必須
- JailBreakはこの制限を外すことを指す
- JailBreakをすると....
  - アップル社が認可してない(しない)アプリケーションをインストール
  - 海賊版アプリケーションの動作
  - ホーム画面やロック画面をはじめ、UIそのものをカスタマイズ
  - などなど
- 当然、故障時はメーカサポートが一切受けられなくなる

Android rooted

- root化すると...
  - テザリングの利用
  - フォントやUIのカスタマイズ
  - CPUのクロック操作
  - などなど

- フォレンジック目的
  - メモリダンプ
  - /data 領域の参照

Jailbreak, root化による影響

- マルウェア感染の場合、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

- IMEI等の端末固有情報やOAuth認証情報等が変更が可能
  - アプリ開発者はID偽装を考慮しなければならない

（参考情報）Android端末における「識別番号」の種類

- 端末固有情報（IMEI：International Mobile Equipment Identity）
  - 端末そのものの識別番号
  - 端末内のバッテリを外すと書いてあることが多い

- 加入者識別番号（IMSI：International Mobile Subscriber Identity）
  - SIMカード内に格納されている識別番号

- Android ID
  - /data/data/com.google.android.googleapps/databases/accounts.db に格納された識別番号

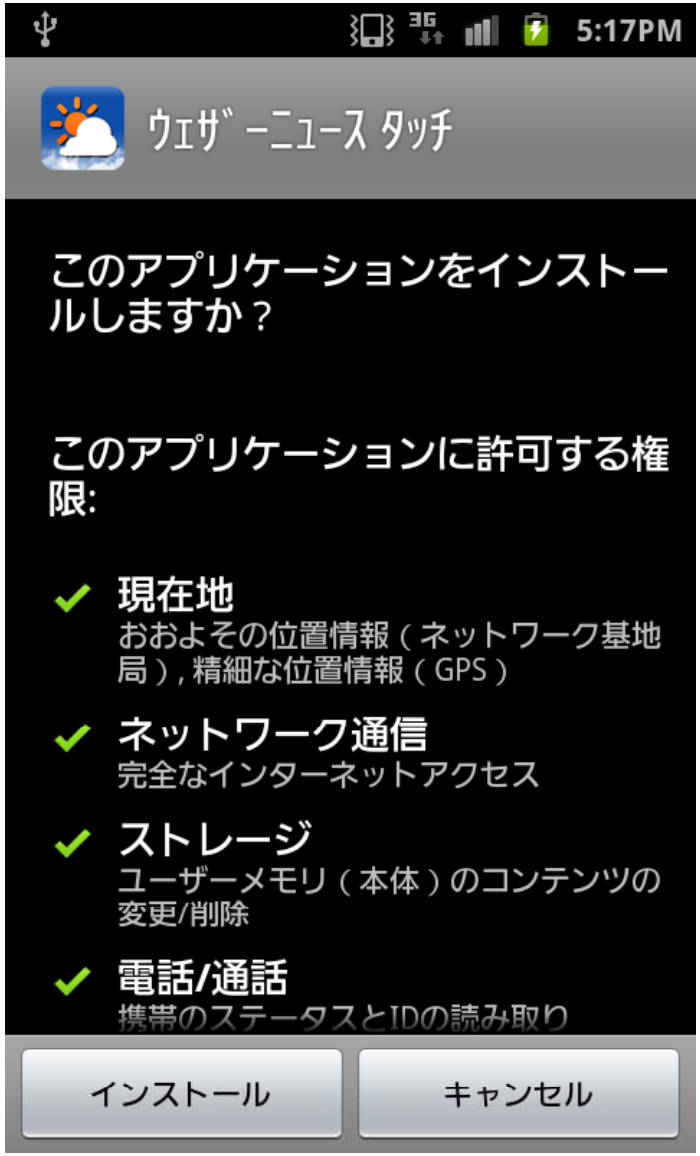
スマートフォンマルウェアの実例

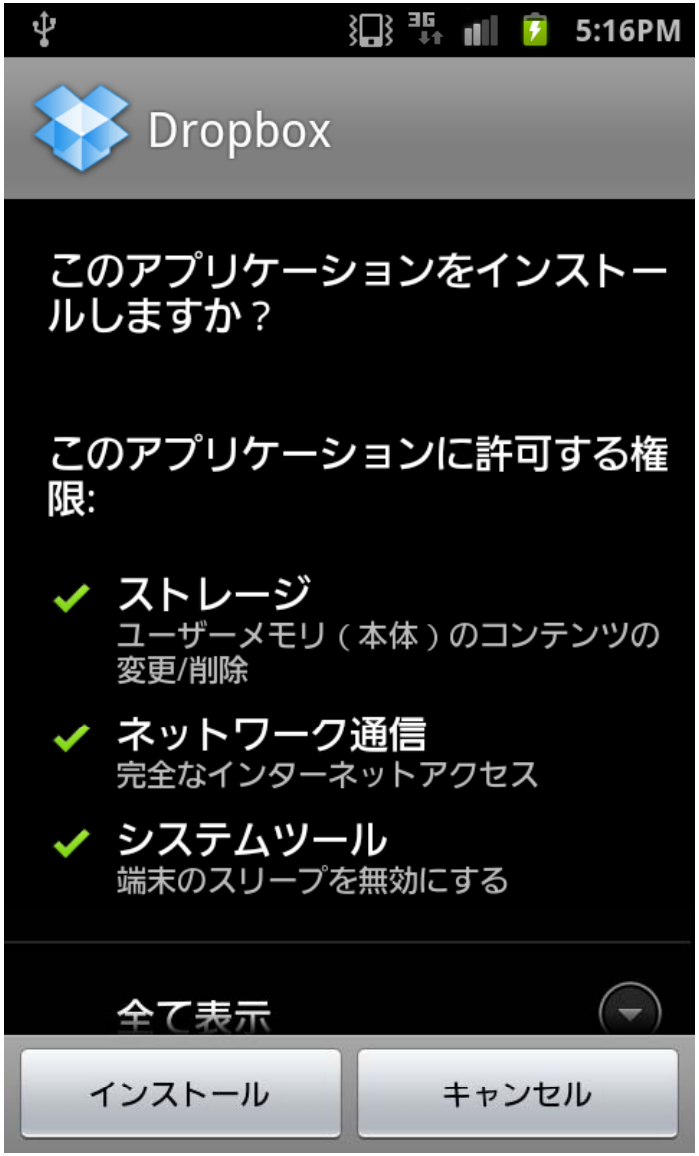
Androidアプリケーションの信頼性

パーミッション

- アプリケーション毎に使える機能を制限する
  - アプリケーションをインストールする際に表示される
    - 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
  - （例）名刺リーダアプリ
    - 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」

パーミッション確認画面



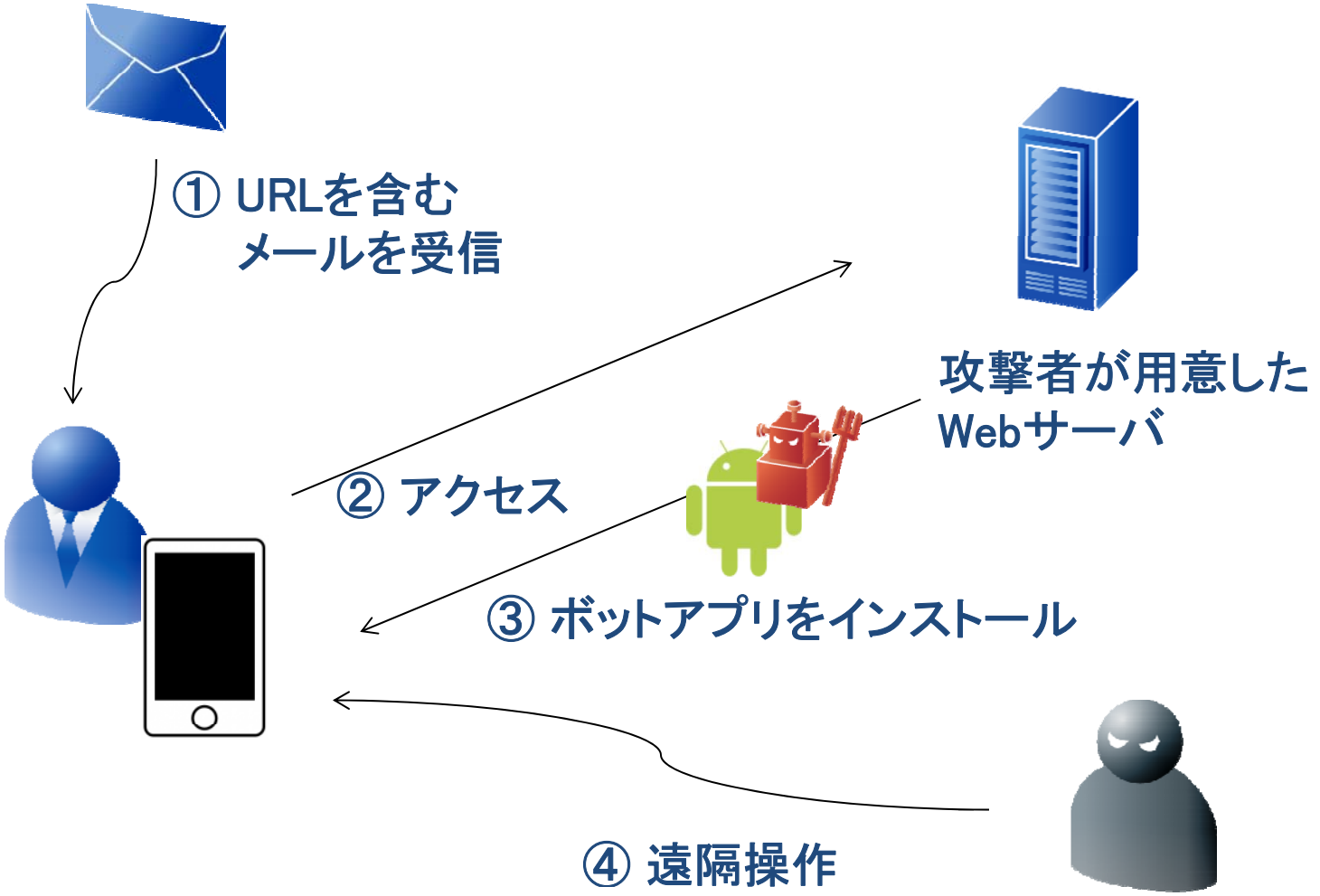


Android Market

- アプリケーションの審査は基本的には「無い」
  - 開発者登録の際にクレジットカードカード番号を求めている
- 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」なものも…
- DroidDream(Rootcager)が組み込まれていたアプリは50種類以上、アプリによっては20万件以上がダウンロードされた(http://goo.gl/Kd3UV/)

不正アプリによる
スマートフォン遠隔操作デモ

デモ概要



対策・まとめ

対策　キャリア編

- リモートロックサービス

- キャリアマーケット
  - au one market→KDDI研究所によるセキュリティチェック

- メールスキャン
  - docomo→spモードのメールにウイルススキャン

- ウイルス対策ソフトの提供
  - au→TrendMicro社製品をオプション提供
  - docomo→McAfee社製品を無償提供
  - SoftBank→McAfee社製品をオプション提供

対策　個人編

- ウイルス対策ソフトのインストール
- インストール予定のアプリケーションのレビューを確認し、信頼できるか判断
- キャリアマーケットの利用
- インストール時に表示されるアクセス許可の一覧を確認
- USBデバッグの無効化

まとめ

- 今のスマートフォンセキュリティは課題が多く、Androidに至っては利用者自身によるセキュリティ対策が必須

- とはいえ、難しいことをする必要もなく
  - 端末内のアプリケーションやOSそのもののバージョンアップを欠かさず行う
  - ウイルス対策ソフトをインストールする
  - アプリケーションは正規の手段、正規のものをインストールする
  - 興味本位でJailBreak、rootedを行わない

- 万が一に備え、クラウドサービスを活用する

- 企業ではMDM(Mobile Device Management)を活用する