NRI 未来創発 Dream up the future.

NRIセキュアテクノロジーズ

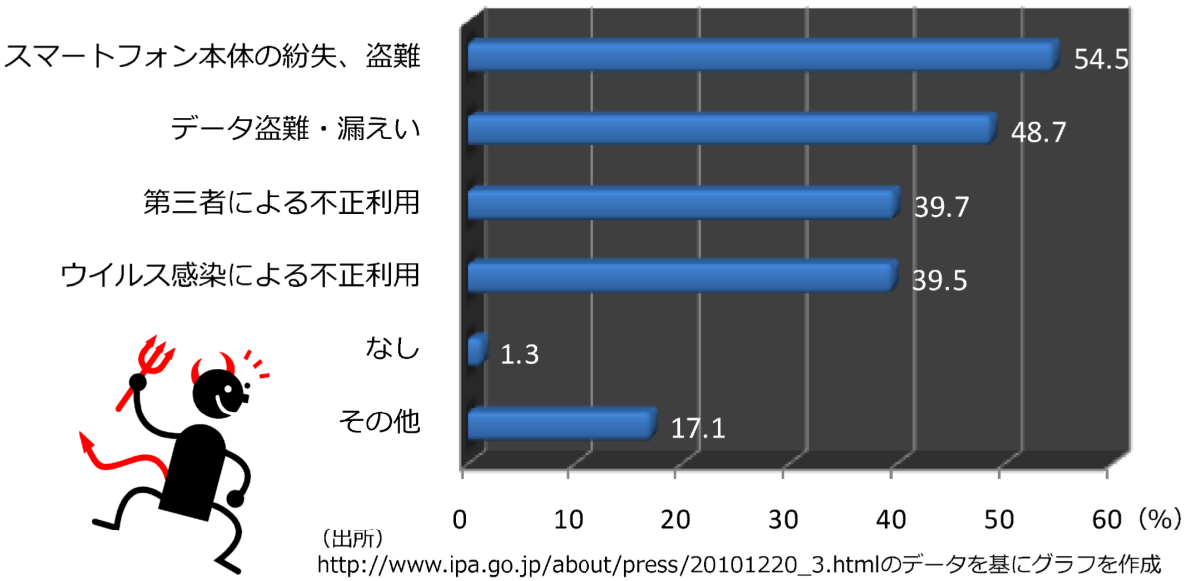
システム技術分科会 2011年度第1回会合

スマートフォンセキュリティ再考

2011年9月9日

NRIセキュアテクノロジーズ株式会社
コンサルティング事業本部
テクニカルコンサルティング部
西田 助宏
〒105-7113
東京都港区東新橋1-5-2 汐留シティセンター

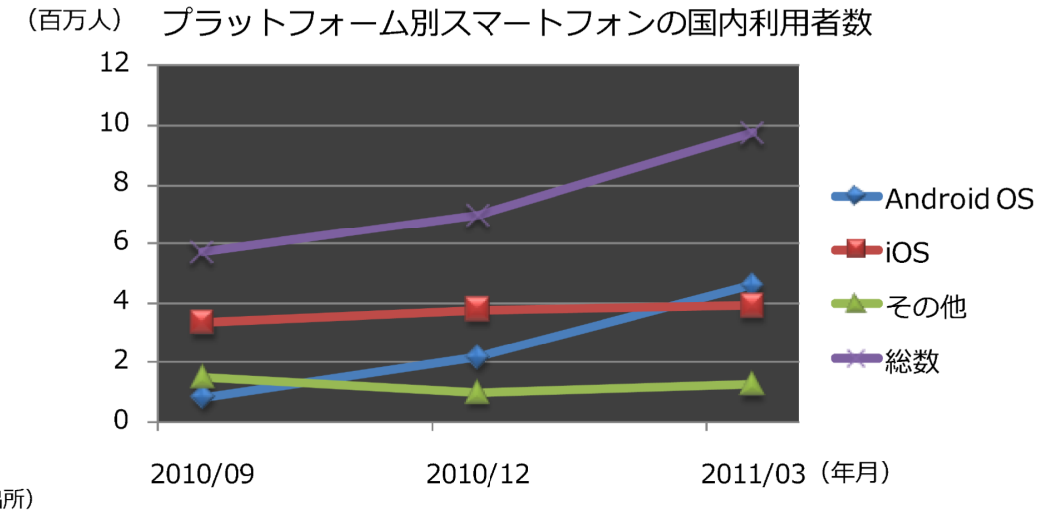
スマートフォン利用時の不安要素



（出所）
http://www.ipa.go.jp/about/press/20101220_3.htmlのデータを基にグラフを作成

2

スマートフォンのプラットフォーム別シェア
Android OS と iOS がシェアを二分（国内）

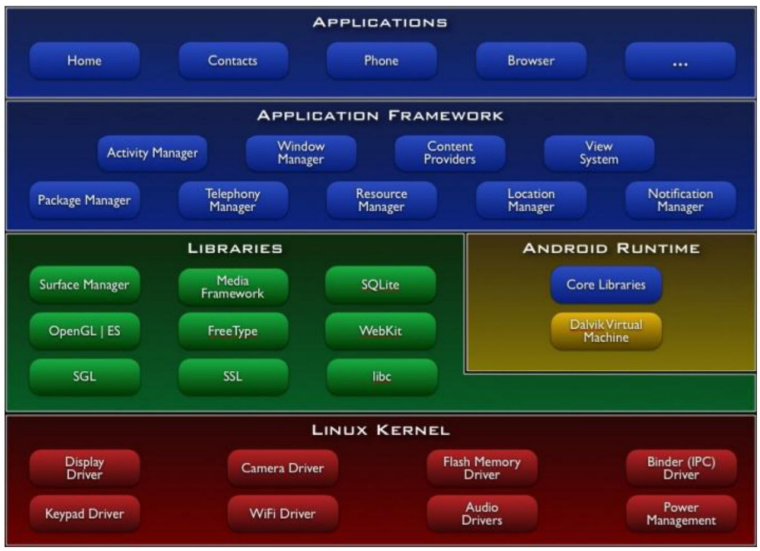


（出所）
http://www.comscore.com/jpn/Press_Events/Press_Releases/2011/6/Google_Android_Leads_Acceleration_in_Smartphone_Adoption_in_Japan のデータを基にグラフを作成

3

セキュリティを考慮すべきレイヤ

- ■ハードウェア
- ■OS
- ■アプリ
- ■利用方法
- ■アプリ配信
- ■…



（出所）
http://developer.android.com/images/system-architecture.jpg

4

今日お話しすること

■対象：
- ●Android OS、iOS搭載のスマートフォン

■脅威：
- ●情報漏洩、不正利用

■レイヤ
- ●アプリケーション（を中心にその周辺も少々）

■組織内でスマートフォンを利用する際の…
- ●利用面での考慮点
- ●アプリケーション開発時の考慮点

5

Android OS vs. iOS

マルウェアの脅威

対策と課題

Android OS/iOS のアクセスコントロール

- 一般的なOSとの違い
  - 利用者には管理者権限がない
  - コアな部分は保護されている
  - root化、Jailbreak…という選択
- アクセスコントロール
  - 物理的なアクセスからの保護
    - 暗号化
    - パスコード
  - 論理的なアクセスからの保護
    - Sandbox
    - アクセス権の要求

7

Android OS vs. iOS
～物理的なアクセスからの保護～

■暗号化

- ●iOS　iPhone 3GS～でハードウェアによる暗号化（AES-256）
  iOS4～で特定のデータを暗号化する機能
- ●Android OS　3.x系～を搭載する一部の端末で実装

- ●OSからはアクセス可能
  - ▪ 仮にパスコードを回避されると
  - ▪ JVNDB-2010-001678

■その他

- ●データのバックアップ
- ●パスコード、自動ロック、自動消去、リモートワイプ…

Android OS vs. iOS
～論理的なアクセスからの保護～

■利用者には管理者権限がない（再掲）

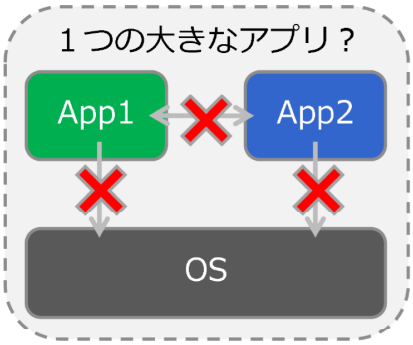
■Sandboxによる保護

- ●アプリ間のアクセス
- ●アプリ → OSへのアクセス

```
# ls -l /data/data/
ls -l /data/data/
drwxr-x--x app_0    app_0           2011-08-17 12:00 com.android.providers.
drwxr-x--x app_1    app_1           2011-08-17 12:00 com.android.speechreco
drwxr-x--x app_3    app_3           2011-08-17 12:00 com.android.inputmetho
drwxr-x--x app_4    app_4           2011-08-17 12:00 com.android.customloca
drwxr-x--x app_0    app_0           2011-08-17 12:00 com.android.inputmetho
drwxr-x--x system   system          2011-08-17 12:00 com.android.providers.
drwxr-x--x app_2    app_2           2011-08-17 12:00 com.android.providers.
```

■（例）ブラウザが侵害された場合

- ●ブラウザ経由のデータは盗まれる恐れがある
- ●ブラウザ以外のアプリのデータは保護される



■OSとアプリの関係（イメージ）

- ●OS ≒ 大きな1つのアプリ？
- ●アプリ ≒ アプリのプラグイン？

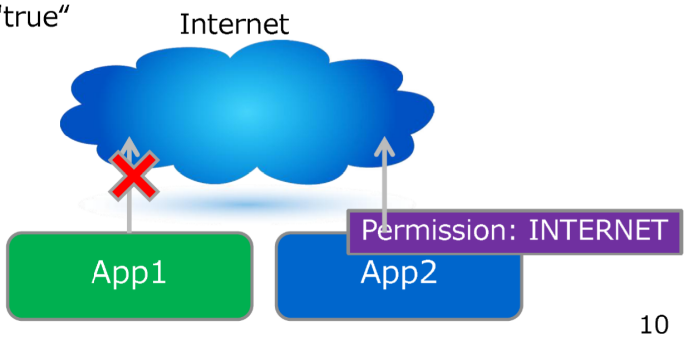
Android OS vs. iOS
～Android OS が実装するアクセスコントロール～

■各アプリに付与される権限が異なる
- ●4つのコンポーネントとインテント（詳細略）

■AndroidManifest.xml
- ●インストールするアプリが要求するアクセス権
  - ▪（例）uses-permission android:name="android.permission.INTERNET"
- ●他のアプリに対して許可するアクセス権
  - ▪（例）android:exported="true“

■インストールするアプリへの権限
- ●利用者が付与

■他のアプリへの権限
- ●開発者が付与



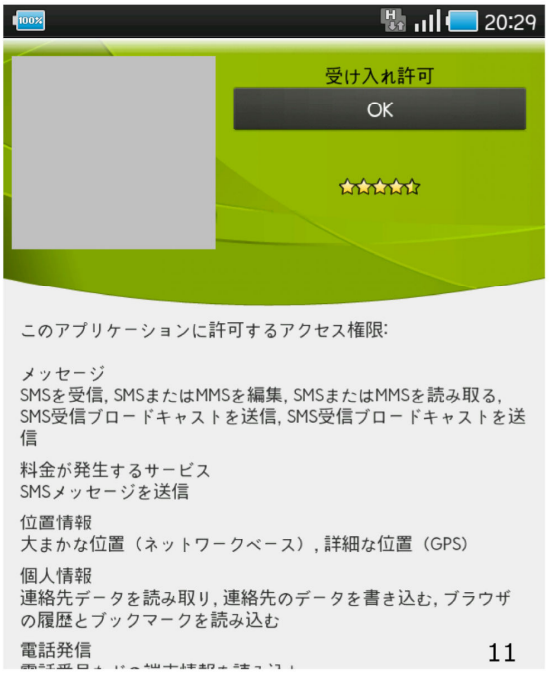
10

Android OS vs. iOS
～Android OS – 利用者に求められるアクセス権～

■アクセス権の要求
- ●アプリのインストール時
- ●すべて許可/拒否の２択

■例：マルウェア「Droid09」
- ●インターネットへのアクセス
- ●キーボードの入力
- ●…

■何をどう判断して「OK」する？



11

Android OS vs. iOS
～Android OS – データの保存場所～

■大きく3つ
- ●端末内部の保存領域
  - ▪ SharedPreferences
  - ▪ ファイルシステムの利用
  - ▪ データベース（SQLite）
  - ▪ Content Provider
- ●端末外部の保存領域
- ●ネットワーク経由で保存

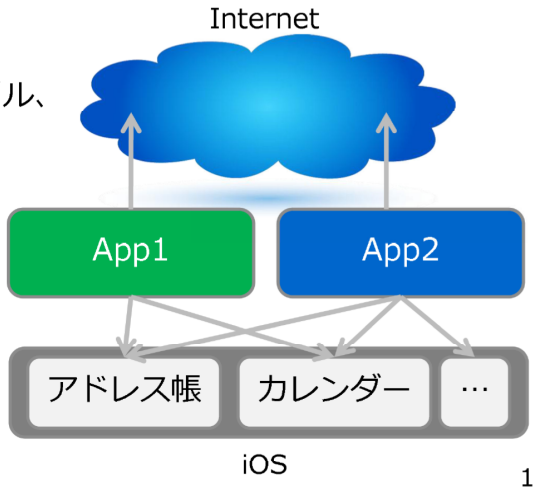
■アクセス権の設定不備
- ●Android版 Skype（CVE-2011-1717）
- ●Android版 Dropbox（v1.1.3）

■SDカードは簡単に取り外し可
- ●読み取る
- ●改ざんする

Android OS vs. iOS
～iOS が実装するアクセスコントロール～

■各アプリは同じ権限で動く

■OSの一部のリソースには利用者の許可なくアクセス可
- ●付与されるアクセス権（例）
  インターネット、アドレス帳、
  カレンダー、音楽/ビデオ/写真ファイル、
  safariの閲覧履歴、マイク/カメラ…
- ●例：Viber



Android OS vs. iOS
～iOS が実装するアクセスコントロール～

■アクセス権の要求
- ●アプリ初回起動時
  - ▪ GPSによる位置情報へのアクセス、Push通知
- ●都度
  - ▪ SMS/E-mailの送信、電話の発信

14

Android OS vs. iOS

マルウェアの脅威

対策と課題

マルウェアの脅威（１）

■Android OSを狙ったマルウェアが増加（2011年～）

- ●Android端末に感染する不正プログラムが半年で16倍に急増
  (http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20110706104118.html)
- ●400 Percent Increase in Android Malware Found Since Summer 2010
  (http://www.juniper.net/us/en/company/press-center/press-releases/2011/pr_2011_05_10-09_00.html)

■何故 Android OS が狙われる？

- ●アプリの流通経路の違い
- ●アーキテクチャの違い（？）

16

マルウェアの脅威（２）

年月	マルウェア名	年月	マルウェア名
2009/11	iPhoneOS.Ikee	2011/3	Android.Walkinwat
2009/11	Dutch 5€ ransom	2011/5	Android.Smstibook
2009/11	iPhone/Privacy	2011/5	Android.Trojan.DDLight
2010/08	AndroidOS.FakePlayer	2011/5	DroidKungFu
2010/08	AndroidOS.TapSnake	2011/6	Android.Jsmshider
2010/12	ANDROIDOS_GEINIMI	2011/6	Android.Tonclank
2011/2	Android.Pjapps	2011/6	Android.Ggtracker
2011/2	Android.Adrd	2011/7	Android.Trojan.GoldDream
2011/3	DroidDream	2011/7	Android.Hippo
2011/3	Android.Bgserv	2011/8	GingerMaster

：iOS　　：root権限を奪取するマルウェア

17

Android OS vs. iOS
～アプリケーションの流通経路～

■Android OS
- ●Android Market（Google社）
- ●その他たくさん
  - ▪ Android Marketから削除されたアプリ専用…
- ●アプリ自体（.apk）があればインストール可能
- ●自己署名
- ●開発者自身の隠蔽が比較的容易

■iOS
- ●基本的にApp Store経由
  - ▪ Jailbreakした端末は除く
- ●開発者用のプログラムもある
- ●事前審査

再パッケージ

■アプリの開発言語
- ●Android OS　Java
- ●iOS　Objective-C

■Android アプリの改ざん事例
- ●正規アプリに機能追加
- ●再度パッケージ化してマーケットへ

root権限で動作するマルウェア

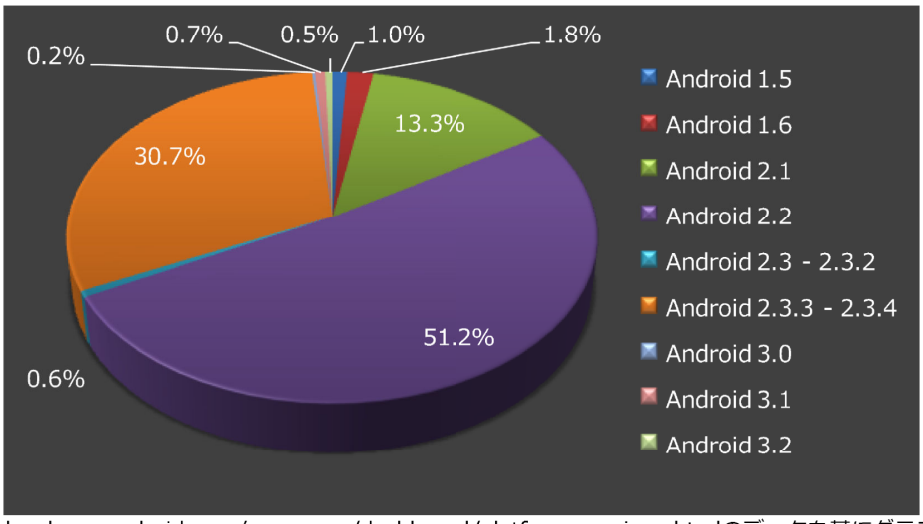
■一般権限 or 管理者権限

■Android
- ●DroidDream（2011年3月～） Android 2.2.1
- ●DroidKungFu（2011年5月～） Android 2.2
- ●GingerMaster（2011年8月～） Android 2.3.3
- ●再パッケージの手口

■iOS
- ●JailbreakMe（2007年～）
- ●ブラウザ経由で端末の管理者権限を取得

Android OS 搭載端末のOSバージョン

■Android OS のバージョンは端末メーカ依存



（出所）
http://developer.android.com/resources/dashboard/platform-versions.htmlのデータを基にグラフを作成
※ 2011/9/2時点の情報

アンチマルウェアソフト

■Android OS 向けに各社が提供
- ●iOS 向けにできること？

■現状のアンチマルウェアソフトの限界
- ●PC用　　管理者権限で動作
- ●Android OS用　その他アプリと同じ権限で動作
- ●Webアクセスのリアルタイムスキャン、全ファイルへのアクセス等は不可

■root権限で動作するマルウェア
- ●マルウェア ＞＞＞＞＞ アンチマルウェアソフト
- ●rootユーザのプロセスに対しては無力

22

Android OS　vs.　iOS

マルウェアの脅威

対策と課題

まとめ（本日の内容）

■Android OS vs. iOS
- ●暗号化
- ●アクセスコントロール
  - ▪ Android OS　利用者に要求、開発者が設定、データの保存場所
  - ▪ iOS　各アプリは同じ権限、デフォルトで一部のOSリソースを利用可

■マルウェアの脅威
- ●Androidを狙ったマルウェアが増加
- ●一般権限で動作するマルウェアとroot権限で動作するマルウェア

■再パッケージ
- ●悪意のあるコードを追加して、マーケットへ

対策と課題

■スマートフォンを利用
- ●バックアップとパスコード、自動ロック、自動消去、リモートワイプ…
- ●アプリのインストール制限？（マーケット、アプリのインストール自体）
- ●現時点でマルウェア対策ソフトの効果は限定的

■アプリを開発
- ●機微な情報は端末に残さない、残すとしても暗号化
- ●必要最小限のアクセス権（for Android OS）
- ●難読化処理

■提供者側に望まれること
- ●マーケット側での対策
- ●一定の権限を限定公開、プリインストール（？）

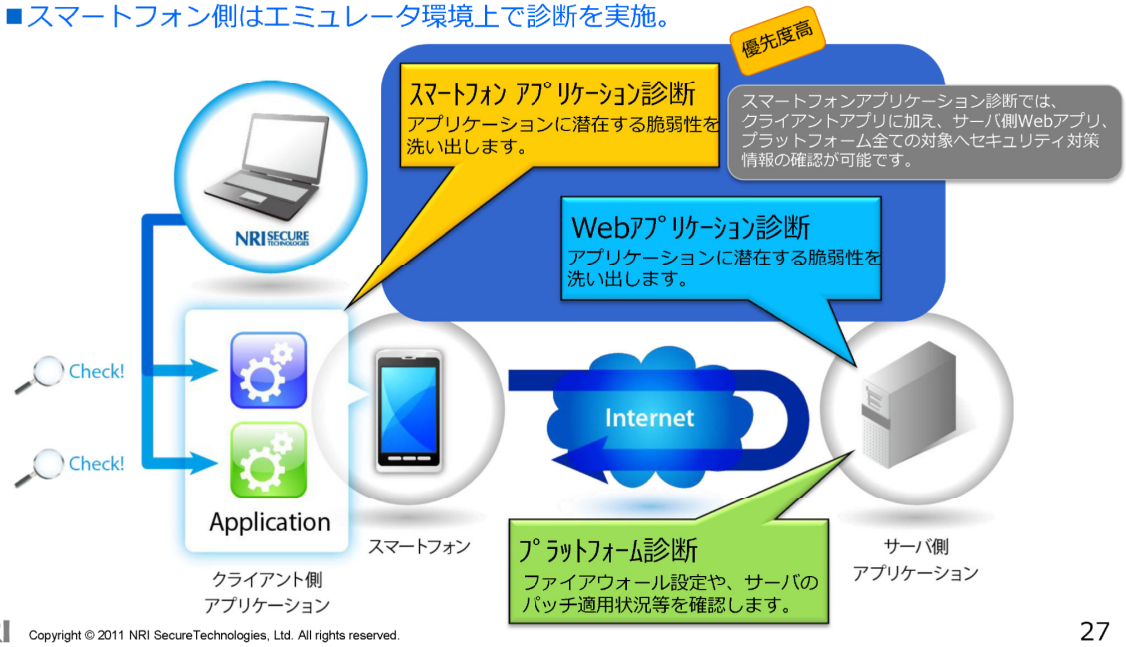
25

当社診断サービスのご紹介

スマートフォン関連の診断サービスメニュー

～クライアント/サーバの両面からセキュリティ対策状況をチェック～

- サーバ側はインターネット経由での実施（リモート診断）、貴社環境での実施（オンサイト診断）の2形態。
- スマートフォン側はエミュレータ環境上で診断を実施。



スマートフォンアプリケーション診断

■ 診断内容

- 動的解析・静的解析を組み合わせた診断
- マニュアルによる診断・分析によるフォロー

■ 弊社サービスの特長

- アプリケーションの実装方式、利用プラットフォーム、開発言語を考慮した診断を実施

■ 発見される脆弱性例

- パスワードが端末内に平文で保存されている
- 機微情報が暗号化せずに送信されている
- ソース内にログインID、パスワードが記載されている
- 他のアプリケーションから、機微情報にアクセス可能

など

分類	項番	評価項目
機微データの取り扱い	1.1	外部保存領域への機微情報の保存
	1.2	機微情報保存時の暗号化処理
	1.3	キャッシュデータの適切な処理
	1.4	適切なデータ削除処理
	1.5	アカウント情報の保存
	1.6	利用機能に関するユーザへの通知
暗号化処理	2.1	重要情報の平文での送信
	2.2	強度の弱い暗号化方式
	2.3	SSL/TLS通信時の証明書の検証
アクセス権の検証	3.1	過剰なアクセス権の付与
	3.2	明示的なアクセス権の付与
ソースコード解析	4.1	難読化処理
	4.2	ソースコード内の機微情報の保存

28

NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ

〒105-7113　東京都港区東新橋1-5-2　汐留シティセンター
TEL：03-6274-1011　E-mail：info@nri-secure.co.jp
HomePage：http://www.nri-secure.co.jp