スマートフォンとセキュリティ
～アプリ安全性検査とプライバシ保護～

KDDI研究所
竹森 敬祐 （Ph.D）

PCと何が違うの？
ポイントをおさえれば、事故は殆ど起きません。

1: はじめに
2: ちょっと気をつけるポイント
3: 端末堅牢化とアプリ安全性検査
4: プライバシ保護に向けて
5: おわりに

スマホ・タブレットとは

使い方

- 様々なアプリをインストールして機能アップさせる携帯端末。

OS

- PCに電話アプリが入っている携帯端末。
- アクセス制限（サンドボックス）の付いたPC。

構成

- 端末メーカや通信キャリアが管理するシステム領域と、
  アプリ開発者や利用者に解放されたユーザ領域が同居する。
- SIMカード、GPS、カメラなど特殊デバイスを持つ端末。

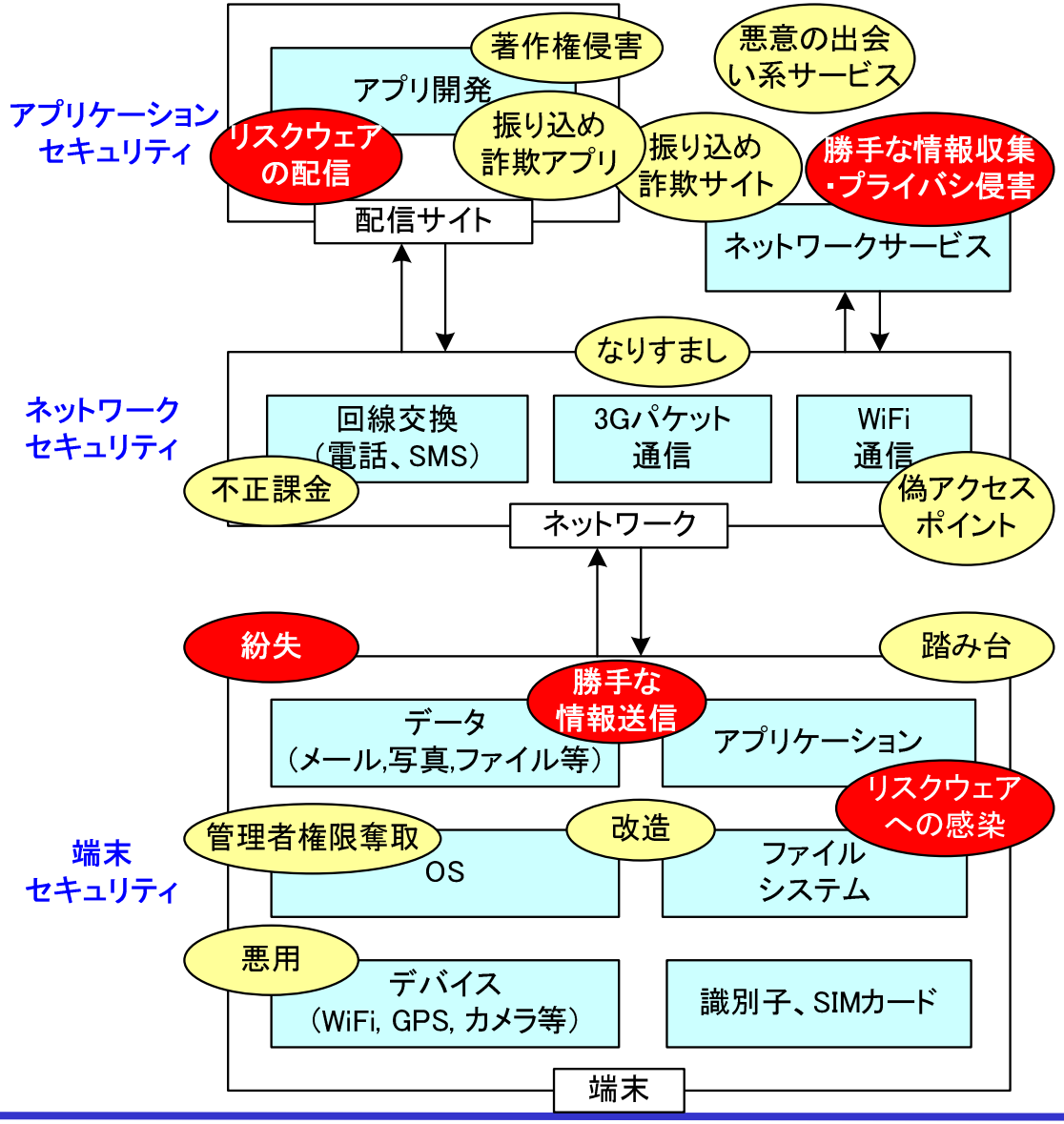
プライバシ問題

提供

- 端末メーカ、OSベンダ、通信キャリア、アプリベンダが混在する
  水平展開型のケータイサービス。

KDDI R&D LABS

スマホの脅威：全体マップ



スマホの脅威：ポイントの整理

■ スマホを取り巻く3つの脅威（法人：＋1つの法脅威）
- ◆ 端末の紛失 ⇒ リモートロック・ワイプ
- ◆ 悪性Webサイトの閲覧 ⇒ PC同様の問題、フィルタサービス
- ◆ リスクを伴うソフトウェア（リスクウェア）への感染

（◆ 利用者による不正利用 ⇒ アプリ制限、機能制限、ログ監査）

■ スマホにウイルス*なし
- ◆ PCのような自動的なウイルス感染はない。**

*ウイルスとは、ファイルやネットワークを媒介して自動感染（拡大）するもの。
**手動感染した後は、自動感染はありうる。

■ 利用者のリテラシ問題
- ◆ スマホOSには、安全に利用するための機構が施されている。

⇒ 安全機構を理解しないまま、従来の携帯電話の使い方をすることで脅威が生じる。

KDDI R&D LABS

安全性はアプリ配信サイトが肝

以降、オープンOSで議論しやすいAndroidを例に取り上げ説明します。

■ 主な感染源
- ◆ 悪性アプリの殆どは、非公式のアプリ配信サイトから出回る。
- ◆ アプリ配信サイトから駆除されると、感染拡大は止まる。

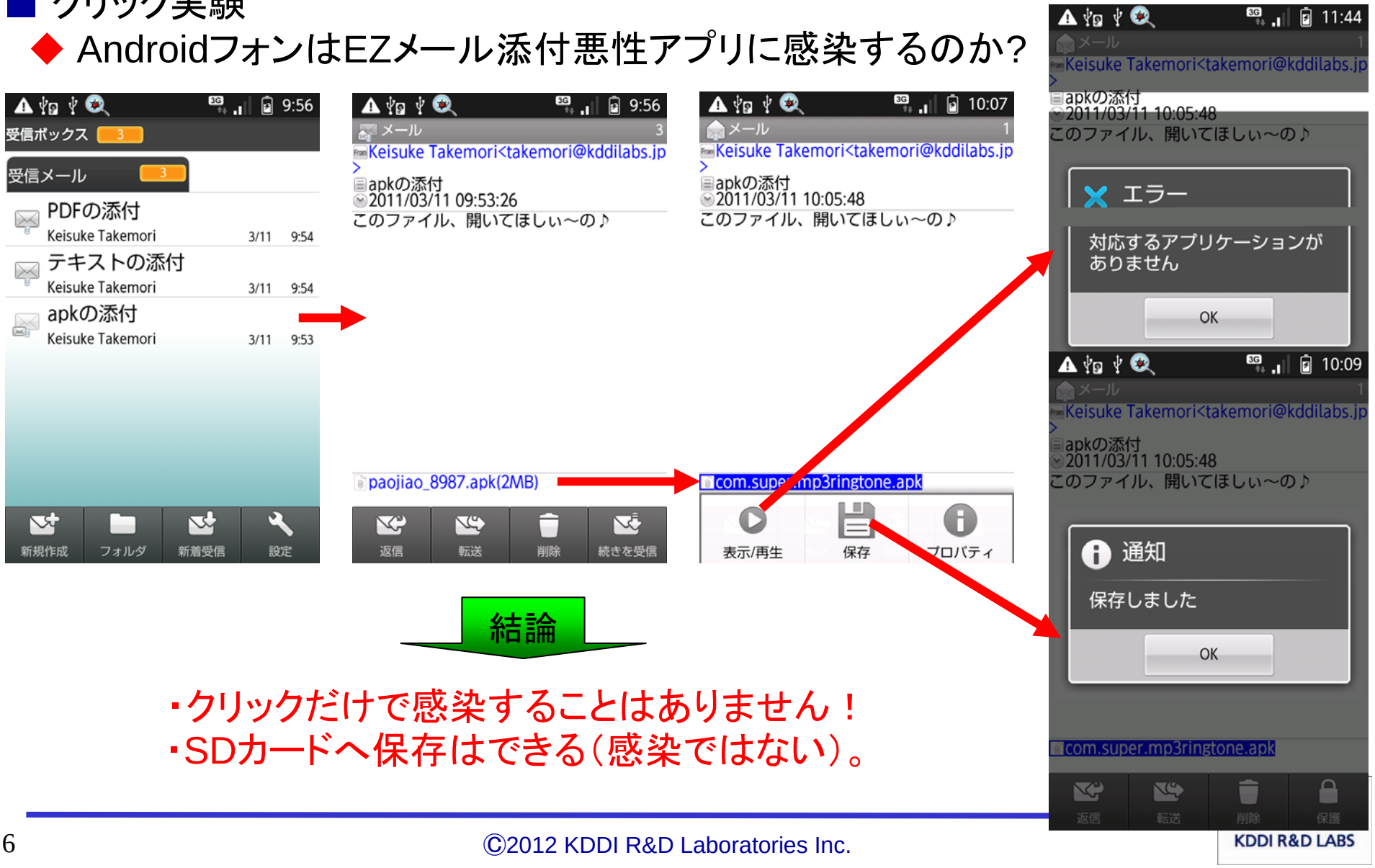
■ 僅かな感染源
- ◆ EZメール添付の悪性アプリをクリックしただけでは感染ない。
  （Gmail添付の場合、提供元不明アプリを解除後に手動感染）
- ◆ adbシェルから手動で感染できる。
- ◆ SDカード保存のアプリは、ファイル操作アプリを通じて感染できる。

au MarketやOSベンダの配信サイトをご利用頂ければ安心です。

メール添付の悪性アプリに感染？：EZメール編

■ クリック実験

◆ AndroidフォンはEZメール添付悪性アプリに感染するのか？



結論

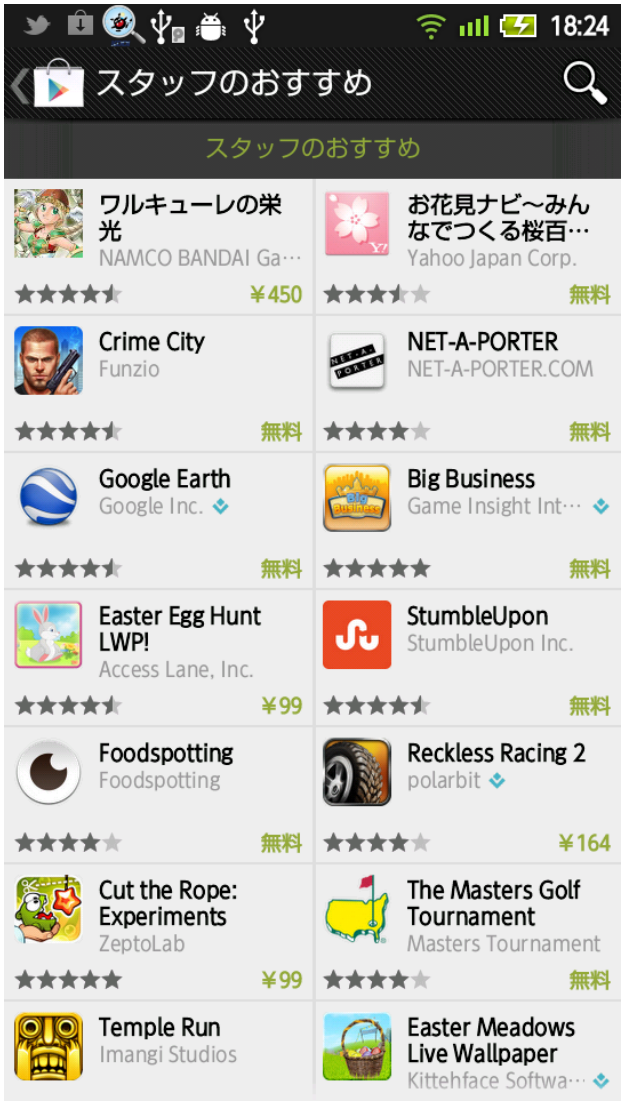
・クリックだけで感染することはありません！
・SDカードへ保存はできる（感染ではない）。

KDDI R&D LABS

Google Play™の安全への取り組み

- Google Play™の安全機構
  - 悪性アプリの事前検査、定期検査を担う”Bouncer” が導入されている。
  - ユーザからの指摘を受けて迅速に悪性アプリを駆除。
  - Google Play™では開発者登録としてクレジットカードを登録し$25を支払う。

一定の安全性は確保されてます。



ところで、悪性アプリの出現状況

統計情報（2011年）の提供元　株式会社カスペルスキー

悪性アプリ出現比　PC : Android™フォン ＝ 1000 : 1

■ 感染の危険度
- ◆ 非公式サイトからの感染には、言語の壁、端末設定の壁がある。
- ◆ 公開期間も短く、絶滅していることが殆ど。

スマホOSのアーキテクチャはPCよりもかなり安全！
安全機構を正しく理解すれば危険を回避できる。

KDDI R&D LABS

よくあるQ＆A

■ 世界の攻撃者が日本を狙う？　～無理です～
- ◆ 利用者の殆どはau MarketかGoogle Play™を利用する。
  - ・非公式アプリ配信サイトを初心者が利用するには手間を要する。
  - ・危険の多い中国やロシアのサイトは言語の壁がある。
  - ⇒ 公式サイト側でアプリをチェックすれば安全を維持できる。

■ 外部から端末への侵入？　～無理です～
- ◆ デフォルト状態の端末には、外部からの侵入口がない。
  - ⇒ 侵入口を開ける悪性アプリに手動感染しない限り影響なし。

■ OSの脆弱性を自動的に突いて管理者権限奪取？　～無理です～
- ◆ 攻撃アプリをインストールして実行する必要がある。
- ◆ PCに端末をUSB接続して不正コマンドを発行する必要がある。
  - ⇒ インストール操作を伴うため、自動的な管理者権限奪取はない。

KDDI R&D LABS

まとめ：スマホとPCのセキュリティ比較

	従来の携帯	Android™フォン	PC
OS/開発情報 （脆弱性）	クローズ （限定的）	オープン （多数が公知化）	汎用OS （多数が公知化）
API （サンドボックス）	限定的 （全アプリへ強制）	豊富＋ユーザ承認 （全アプリへ承認型）	豊富 （Webブラウザのみ）
端末識別子管理	強（堅牢に保護）	弱（APIアクセス可）	ー
コンソール	無	有	有
ディスクの暗号化	無	限定的	有
遠隔ロック・ワイプ	有	有	無
アプリ販売（Market）	クローズ	オープン	オープン
管理者権限アプリ	無	無 ＊	有
リスクウェア感染	限定的	有（手動）	有（手動 & 自動）
Webスクリプト攻撃	限定的	有	有
フィッシング	有	有	有
総合的な安全度	★★★	★★	★

＊想定外の管理者権限奪取や管理者権限利用のアプリがある。

最大の脅威

KDDI R&D LABS

スマートフォンとセキュリティ
～アプリ安全性検査とプライバシ保護～

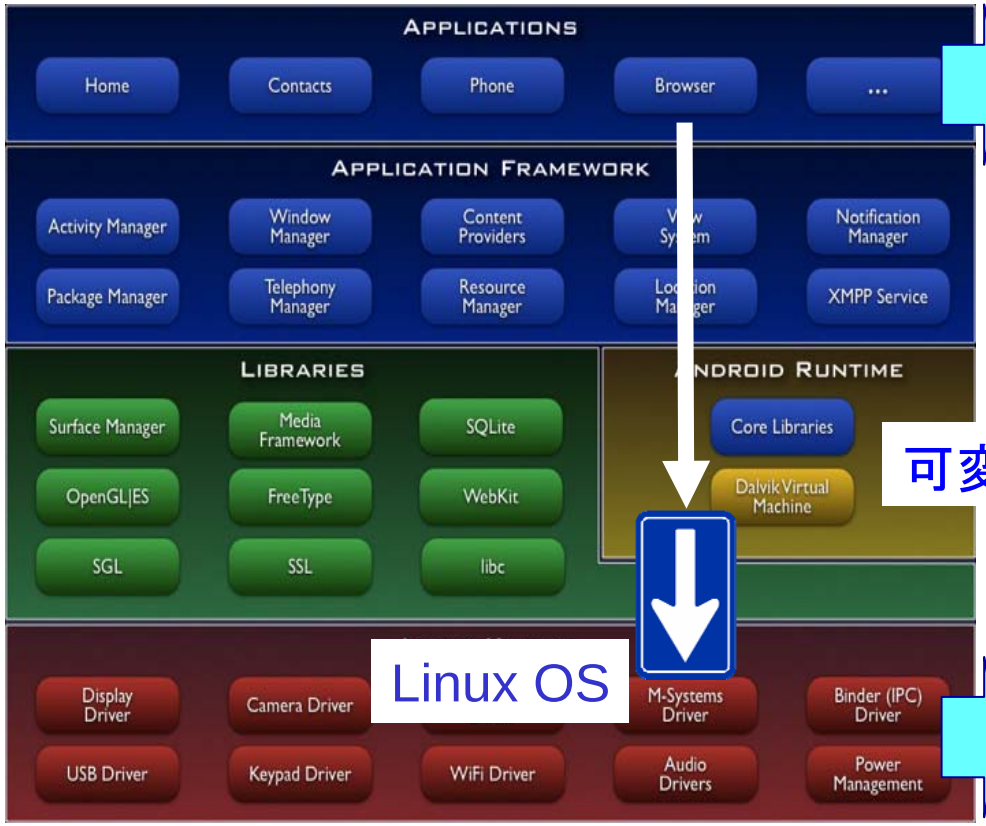
KDDI研究所
竹森 敬祐 （Ph.D）

PCと何が違うの？
ポイントをおさえれば、事故は殆ど起きません。

1: はじめに
2: ちょっと気をつけるポイント
3: 端末堅牢化とアプリ安全性検査
4: プライバシ保護に向けて
5: おわりに

Android™のセキュリティ機構

- Linux OS + サンドボックス
  - Linux上に、パーミッション可変型のサンドボックスを構築したOS。
  - アプリが利用する機能・情報を利用者が承認する。
    ⇒ 安全性と利便性のトレードオフをユーザに委託



- 事故の主原因（1）
  ⇒ 情報アクセスへの機能が豊富
  ⇒ 日本人に馴染みの薄い機能承認（パーミッション）の仕組み

可変型（利用者承認型）サンドボックス

- 事故の主原因（2）
  ⇒ Linux（PC）の脆弱性を含む
  ⇒ 管理者権限奪取でPC化

KDDI R&D LABS

ポイント：インストール時の承認

■ パーミッション機構

◆ アプリの機能（権限）を承認するインストール機構

⇒ 本来の目的から逸脱する機能の有無に注目してください。

KDDI R&D LABS

パーミッションの利用実態 ～統計調査（2011年8月）～

■ Android Market™の無料アプリ（14カテゴリ×70個＝980個）のパーミッション
- ◆ 携帯電話特有の情報を利用するアプリが多数ある。

参考：2010年	順位	合計 980	利用率	Android Permission	説明（au one Marketでの説明文）
→ 55.4%	1	882	90.0%	INTERNET	インターネットへのアクセス
	2	664	67.8%	WRITE_EXTERNAL_STORAGE	SDカードへの情報の書き込み
	3	575	58.7%	ACCESS_NETWORK_STATE	ネットワークへの接続状態の表示
→ 17.2%	4	567	57.9%	READ_PHONE_STATE	電話番号やSIM情報の読み取り
	5	287	29.3%	VIBRATE	バイブレーション機能
→ 15.8%	6	278	28.4%	ACCESS_COARSE_LOCATION	携帯電話基地局情報やWiFiアクセスポイントを使った位置情報の取得（精度低）
→ 15.2%	7	261	26.6%	ACCESS_FINE_LOCATION	携帯電話基地局情報やWiFiアクセスポイント、及び、GPSを使った位置情報の取得（精度高）
	8	243	24.8%	WAKE_LOCK	端末のスリープの無効
	9	160	16.3%	ACCESS_WIFI_STATE	Wi-Fiアクセスポイント情報の表示
	10	122	12.4%	RECEIVE_BOOT_COMPLETED	端末起動時にアプリケーションを自動的起動

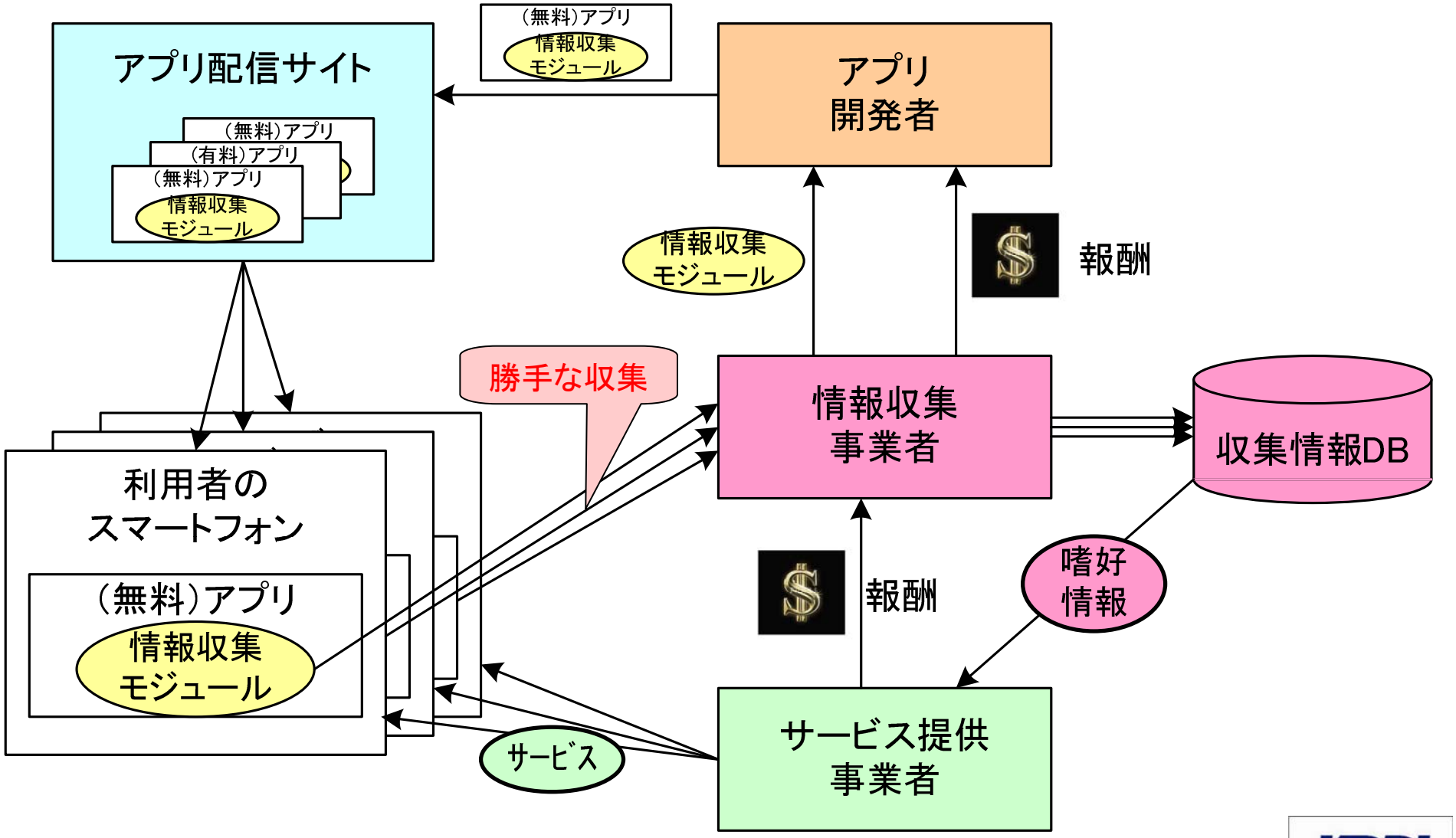
KDDI R&D LABS

リスクウェアの整理

分類	定義	具体例	
		悪性アプリ 参考：現時点の日本における脅威レベル	設計ミス・迷惑なアプリ 参考：現時点の日本における脅威レベル
情報漏洩	・勝手に利用者情報を送信するアプリ	・スパイウェア 主に海外の非公式配信サイトに掲載され日本の利用者への感染は殆ど無い。（脅威小） ・情報漏洩型の悪性Webサイト 悪性Webサイト閲覧による攻撃スクリプトの実行を通じた情報漏洩が想定される。（脅威小）	・説明/許諾のない情報収集 主にターゲティング広告の為であり、脅迫などの実被害の報告は無い。（脅威中） ・ファイル操作の設計ミスによる情報漏洩 外部から端末内ファイルを読み取れてしまう設計ミスのアプリがある。（脅威小）
不正課金	・勝手に料金の生じるサービスを利用するアプリ ・利用者を騙して金銭を要求するアプリ	・プレミアムSMS 日本にプレミアムSMSのサービスは無く実被害無し（脅威小） ・振込め/ワンクリック詐欺 多くは日本の成人向けWebサイトに掲載され自動感染は無いが、騙され易い。（脅威中）	・説明/許諾のないSMSの利用 リモート制御のためのSMS通信等であり、悪意の制御には至っていない。（脅威小）
踏み台	・端末を外部から不正に制御するアプリ	・ボット/バックドア 多くは海外の非公式配信サイトに掲載され、日本の利用者の感染は殆ど無い。（脅威小）	対象外
脱獄 （ﾊｯｷﾝｸﾞ）	・OS/ライブラリ/アプリ等の脆弱性を突くアプリ ・他のアプリが作った裏口や特権を利用するアプリ	・アタック 多くは海外の非公式配信サイトに掲載され、日本の利用者の感染は殆ど無い。（脅威小）	・制限された権限/コマンドの利用 非開放機能の活用であり直接的な被害は少ない。（脅威小）
悪用	・使い方によっては、法令に抵触するアプリ	対象外	・盗撮(消音)カメラ/ビデオ 使い方によっては被害者が出てしまう、もしくは機密情報の漏洩に至る。（脅威中）

KDDI R&D LABS

情報収集ネットワークの例



情報収集モジュールの実態

■ 情報収集ビジネス
- ◆ 広告を利用者がクリックすることで、アプリ開発者に報酬が入る。

⇒ 電話番号や位置情報を利用したターゲティング広告を配信する。

■ 望ましい姿
- ◆ 情報収集機能を組み込むアプリ開発者は利用者に対して、収集者、収集する情報、収集目的をアプリの中で説明すべき。

検索アプリ

■ 実態調査（KDDI研調べ：2011年8月）
- ◆ 980個の無料アプリを対象に、情報収集機能の含有調査を実施した。

	含有数	含有率
アプリ総計	558/980	56.9%
情報収集モジュール総計	1065/558	1.91個

KDDI R&D LABS

情報収集モジュールのアプリ例「許諾なし」

■ 送信実態

◆ 組み込んだ情報収集モジュールが送信。

■ 問題点

◆ アプリ内での利用者許諾なし。

◆ 送信情報は、端末ID（IMEI）と位置。

GET /kuAD_V2/InfoReceive.php?cmd=REG&apid=00000000e&ver=04&imei=354957031150819 HTTP/1.1¥r¥naccept: */*¥r¥ncontentType: charset=utf-8¥r¥nUser-Agent: Dalvik/1.4.0 (Linux; U; Android 2.3.4; Nexus One Build/GRJ22)¥r¥nHost: [redacted].com¥r

GET /kuAD_V2/InfoReceive.php?cmd=LBS&did=000000taEh&lat=35.87912053333333&lon=139.51742570000002&acc=66.0 HTTP/1.1¥r¥nUser-Agent: Dalvik/1.4.0 (Linux; U; Android 2.3.4; Nexus One Build/GRJ22)¥r¥nHost: [redacted].com¥r¥n

新聞早読みアプリ

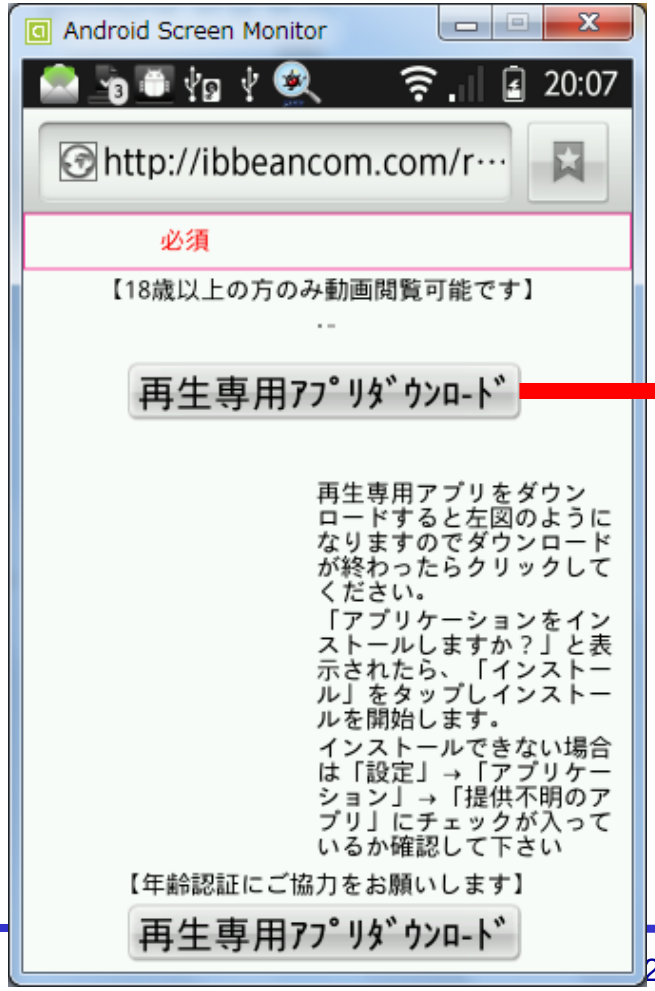
KDDI R&D LABS

悪性アプリ：振込め／ワンクリック詐欺

■ 非公式アプリ配信サイト

◆ 日本の成人向けWebサイトに偽の再生アプリが置かれた。

⇒「提供元不明アプリ」をデフォルト設定（OFF）にしておけば安心。



電話番号

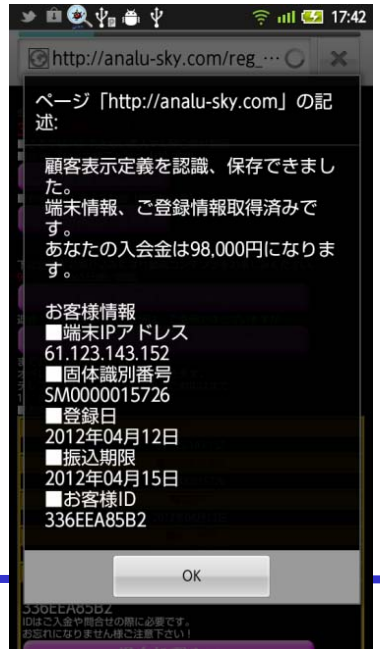
メールｱﾄﾞﾚｽ

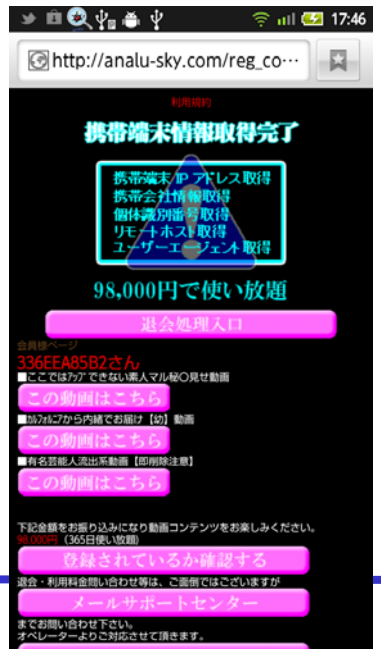
＋位置

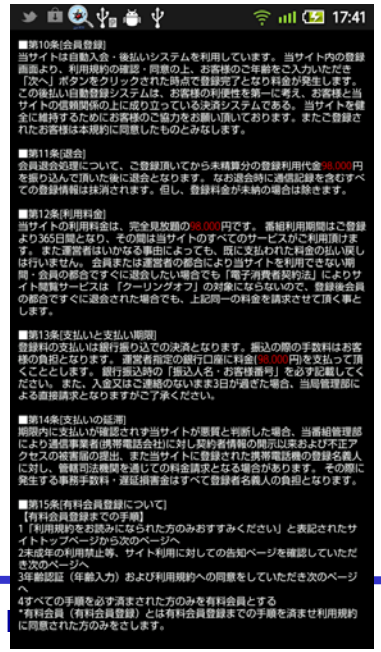
＋IMEI

KDDI R&D LABS

参考：悪性Webサイト：振込め／ワンクリック詐欺







- 無視してください
  - Webブラウザで閲覧しただけでは、個人情報が抜き取られることはありません。

KDDI R&D LABS

迷惑なアプリ：盗撮（消音）カメラ

■ 悪用アプリとは

◆ ユーザの使い方次第で、第三者に迷惑をかける恐れがあるアプリ。

◆ 消音カメラは、盗撮で被害者が出るなど社会問題になっている。

- 正しい使い方
  - 動物を撮影する。
  - 撮影許可のある美術館で撮影する。

- 問題のある使い方
  - 駅で盗撮をする。
  - 工場や研究施設を盗撮する。
  - 書籍を電子万引きする。

http://t0.gstatic.com/images?q=tbn:ANd9GcTuDn7nvVDQNPN3tDVOBtGaK3h-YM9AbowFtPUvxn6GtAO15wkoftTQnjkOhA

まとめ：インストール時に注意すべきパーミッション

■ 不正操作と情報漏洩の視点から

◆ 悪用されると危険が及ぶ、特に注意を要するパーミッションの一例を示す。

潜在脅威	パーミッション	分類	説明
不正操作	CALL_PHONE	料金の発生するサービス	電話番号発信
	SEND_SMS	料金の発生するサービス	SMSメッセージの送信
	AUTHENTICATE_ACCOUNTS	アカウント	アカウント認証システムとして機能
	USE_CREDENTIALS	アカウント	アカウントの認証情報を使用
情報漏洩	READ_PHONE_STATE	電話/通話	携帯のステータスとIDの読み取り
	READ_SMS	送受信したメッセージ	SMSの読み取り
	READ_CONTACTS	個人情報	連絡先データの読み取り
	READ_CALENDAR	個人情報	カレンダーデータの読み取り
	READ_LOGS	システムツール	システムログファイルの読み取り
	ACCESS_FINE_LOCATION	現在地	精細な位置情報（GPS）
	ACCESS_COARSE_LOCATION	現在地	大よその位置情報（ネットワーク基地局）
	READ_INPUT_STATE	ProtectionLevel：signature	入力や操作の記録

スマートフォンとセキュリティ
～アプリ安全性検査とプライバシ保護～

KDDI研究所
竹森 敬祐 （Ph.D）

PCと何が違うの？
ポイントをおさえれば、事故は殆ど起きません。

1: はじめに
2: ちょっと気をつけるポイント
3: 端末堅牢化とアプリ安全性検査
4: プライバシ保護に向けて
5: おわりに

はじめに　～セキュリティマップ～

(5) 運用のセキュリティ
- お客様への説明
- 情報発信

(4) ネットワークのセキュリティ
- ネットワークの安定化
- 認証

The Internet

通信キャリア
NW

3G

WiFi

(2) Marketのセキュリティ
- 掲載アプリの安心チェック
- アプリ情報の提供

(3) アプリのセキュリティ
- 開発者への啓発
- 著作権重視のアプリ

(1) 端末のセキュリティ
- 端末の堅牢化
- リモート管理(MDM)
- リモートロック／ワイプ
- セキュリティ対策ソフト

(0) 脆弱性の調査
- 端末への攻撃
- 悪性アプリ

一般端末のセキュリティ

端末の堅牢化

- 脆弱性への対応を進めることで、管理者権限を奪わせない。
- 端末メーカ、通信キャリアの領域である/systemを保護する（例/system/binにsuを置かせない）ことで攻撃の影響を最小化する。

攻撃の防止と、影響の最小化

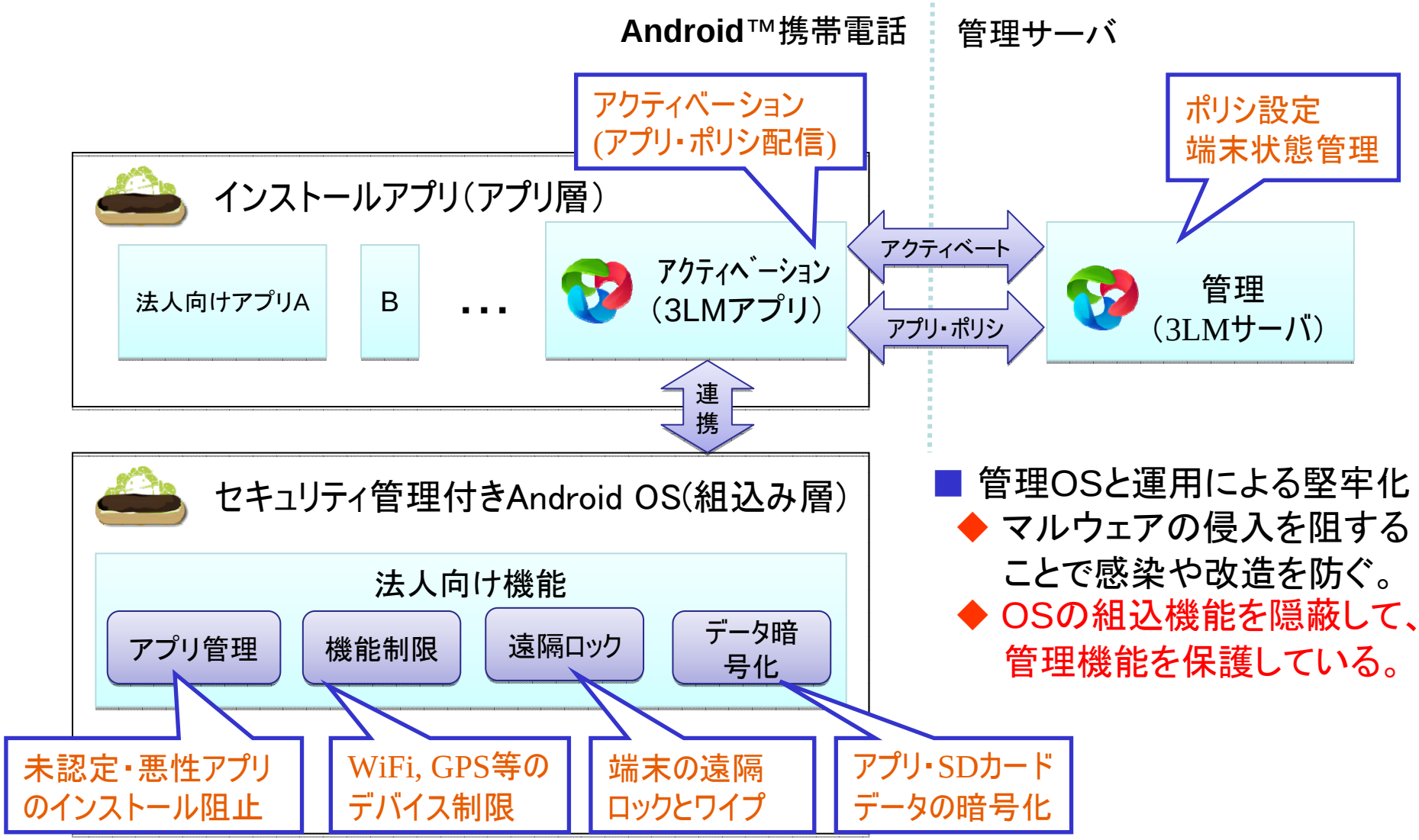
対応項目	事前対策	事後対策
脆弱性対応	•最新OSの搭載 •脆弱性情報の入手/対策 •独自仕様の最小化	•脆弱性情報の入手/対策 •パッチの作成 •パッチの配布
OS書換の保護	•セキュアブート •特定ROMの書換の禁止	

本表の提供元：シャープ（株）

効果

- グローバル悪性アプリの影響を受けず、踏み台になっていない。

法人端末のセキュリティ：OS層からの管理機構「3LM」



- 管理OSと運用による堅牢化
  - マルウェアの侵入を阻することで感染や改造を防ぐ。
  - OSの組込機能を隠蔽して、管理機能を保護している。

MDM: Mobile Device Management

法人端末のセキュリティ：OS型 vs アプリ型のMDM

OS型とアプリ型のMDM比較

- OS型（3LM）は、様々な機能を提供できるため高い安全性を実現できる。
- アプリ型MDMは、利用条件に従ってセキュリティ強度が変わる。

	セキュリティ対策・機能	3LM	某社のアプリ型MDM 制限は適度	某社のアプリ型MDM 制限を最大化
アプリ管理	アプリのホワイトリスト	高	低（root権限で改ざん）	高
	アプリ自動削除	高	無	無
	パーミッション実行制御	高	無	無
	アプリの遠隔配信	高	無	無
	アプリの暗号化	高	無	無
デバイス管理	各種デバイス制御	高	低(root権限で改ざん)	高
	外部メモリ暗号化	高	無	無
	電話の発信制限	無	低(root権限で改ざん)	高
遠隔ロック	遠隔ロック機能	高	低(root権限で解除)	高
データ暗号化	SDカードの暗号化	有	無	無
アプリ排除攻撃	制御アプリの無効化対策	高	低(root権限無くても可能)	高

＊高　セキュリティ強度が高い　低　セキュリティ強度が低い　無　機能がない

MDM: Mobile Device Management

KDDI R&D LABS

端末のセキュリティ：まとめ

■ 総合的な安全対策

◆ 端末の堅牢化とセキュリティ管理サービスの組み合わせで法人に適用できうる。

Player	要件	対策	詳細
端末メーカ	OS実装	ブートローダ保護	独自ディスク(ROM)への差替え阻止
		/system保護	/systemに対する改造阻止
	パッチリリース	パッチの適用	管理者権限奪取を阻止するパッチのリリース
MDMサービス	悪性Webサイト対策	URLフィルタ	URLのブラックリストを用いたフィルタリング
	マルウェア(悪性アプリ)対策	ブラックリスト(アンチマルウェア)	マルウェアのパターンファイルとの照合
		ホワイトリスト(認定アプリ)	アプリの安全性検証と認定 認定アプリのみインストールする制限機構
	社内網接続	VPN	暗号通信路＋認証による社内LAN接続
	ロック・ワイプ	リモートロック	ログインのためのパスワードのリモート制御
		リモートワイプ	工場出荷状態へ戻すリモート制御
	位置特定	GPS追跡	端末の位置情報をリモート監視
	機能制限	禁止機能の阻止	adbやWiFiなどのデバイス制限
	データの暗号化	データの暗号化	アプリデータを暗号化する機能
		SDカードの暗号化	SDカード全体に対する暗号化

MDM: Mobile Device Management

KDDI R&D LABS

Marketのセキュリティ: auスマートパスの「安心」

■ 安全性検査

◆ アプリ配信サイトが安全であれば、脅威の多くを取り除ける。

⇒ 事前検査と掲載中検査：auスマートパス向けアプリの全検査

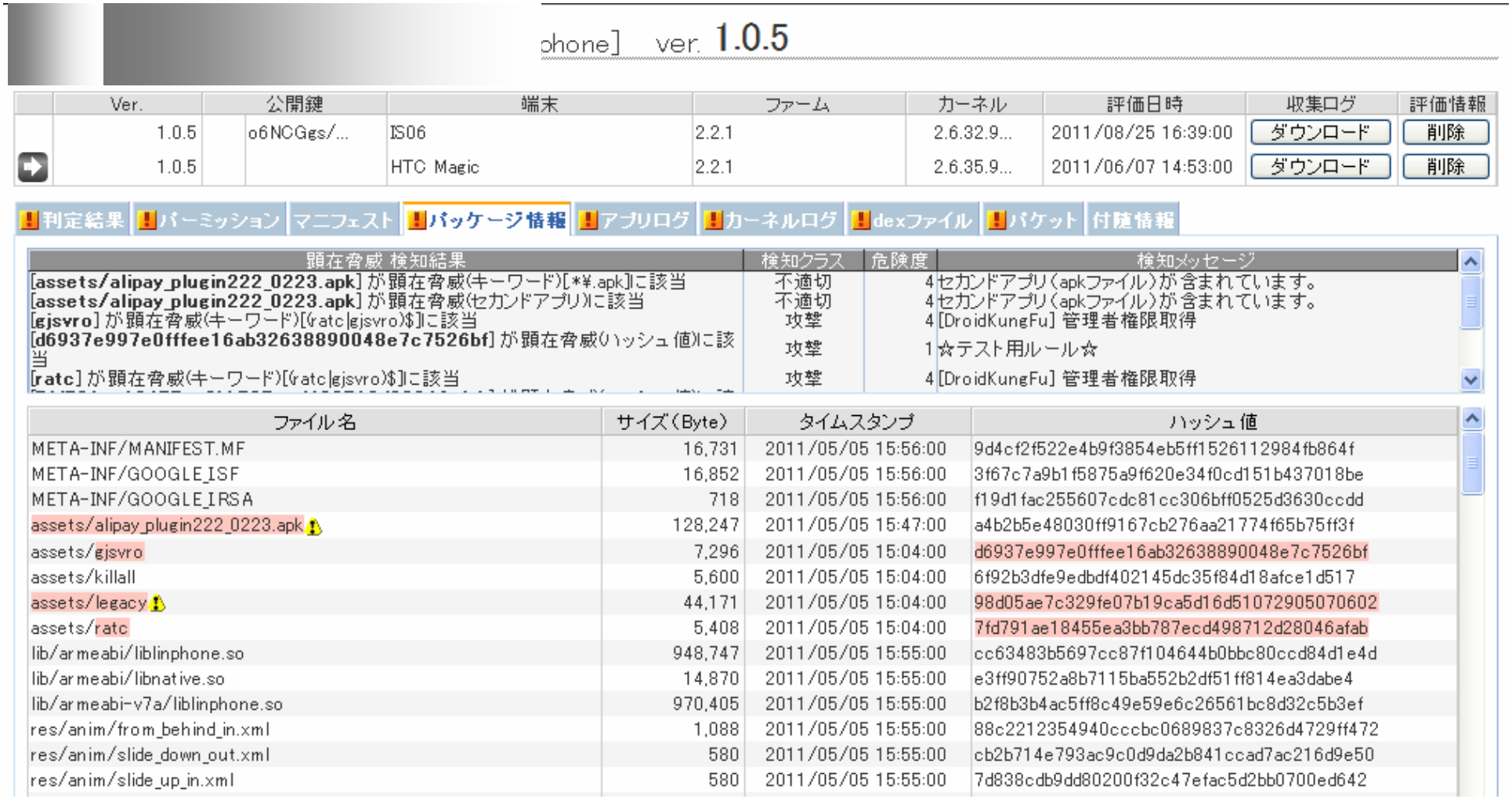
⇒ 静的解析と動的解析： アプリの機能や実行ログを確認

チェックのポイント

1. 機能（パーミッション）
2. 本来利用できない機能の有無
3. 利用者情報の勝手な送信の有無
4. 外部への不正アクセスの有無 etc

注意を要するものは、アプリ開発者へフィードバック
（二人三脚で安心アプリの提供に取り組んでいます。）

au Marketのセキュリティ検査：静的解析



phone]　ver. 1.0.5

	Ver.	公開鍵	端末	ファーム	カーネル	評価日時	収集ログ	評価情報
	1.0.5	o6NCGgs/...	IS06	2.2.1	2.6.32.9...	2011/08/25 16:39:00	ダウンロード	削除
➔	1.0.5		HTC Magic	2.2.1	2.6.35.9...	2011/06/07 14:53:00	ダウンロード	削除

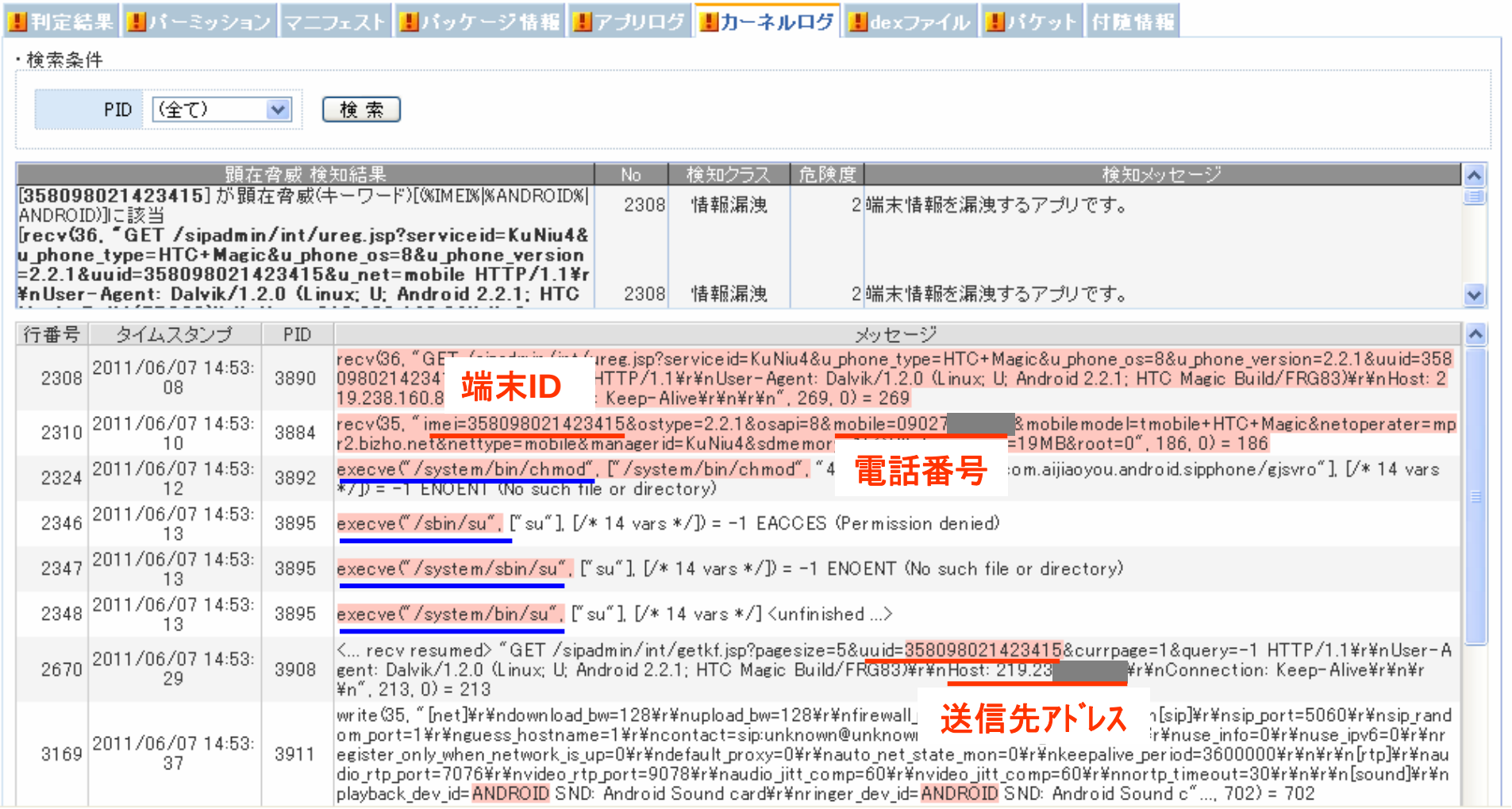
判定結果 | パーミッション | マニフェスト | パッケージ情報 | アプリログ | カーネルログ | dexファイル | パケット | 付随情報

顕在脅威 検知結果	検知クラス	危険度	検知メッセージ
[assets/alipay_plugin222_0223.apk] が顕在脅威(キーワード)[(*¥.apk)]に該当	不適切	4	セカンドアプリ(apkファイル)が含まれています。
[assets/alipay_plugin222_0223.apk] が顕在脅威(セカンドアプリ)に該当	不適切	4	セカンドアプリ(apkファイル)が含まれています。
[gjsvro] が顕在脅威(キーワード)[(ratc|gjsvro)$]に該当	攻撃	4	[DroidKungFu] 管理者権限取得
[d6937e997e0fffee16ab32638890048e7c7526bf] が顕在脅威(ハッシュ値)に該当	攻撃	1	☆テスト用ルール☆
[ratc] が顕在脅威(キーワード)[(ratc|gjsvro)$]に該当	攻撃	4	[DroidKungFu] 管理者権限取得

ファイル名	サイズ(Byte)	タイムスタンプ	ハッシュ値
META-INF/MANIFEST.MF	16,731	2011/05/05 15:56:00	9d4cf2f522e4b9f3854eb5ff1526112984fb864f
META-INF/GOOGLE_ISF	16,852	2011/05/05 15:56:00	3f67c7a9b1f5875a9f620e34f0cd151b437018be
META-INF/GOOGLE_IRSA	718	2011/05/05 15:56:00	f19d1fac255607cdc81cc306bff0525d3630ccdd
assets/alipay_plugin222_0223.apk	128,247	2011/05/05 15:47:00	a4b2b5e48030ff9167cb276aa21774f65b75ff3f
assets/gjsvro	7,296	2011/05/05 15:04:00	d6937e997e0fffee16ab32638890048e7c7526bf
assets/killall	5,600	2011/05/05 15:04:00	6f92b3dfe9edbdf402145dc35f84d18afce1d517
assets/legacy	44,171	2011/05/05 15:04:00	98d05ae7c329fe07b19ca5d16d51072905070602
assets/ratc	5,408	2011/05/05 15:04:00	7fd791ae18455ea3bb787ecd498712d28046afab
lib/armeabi/liblinphone.so	948,747	2011/05/05 15:55:00	cc63483b5697cc87f104644b0bbc80ccd84d1e4d
lib/armeabi/libnative.so	14,870	2011/05/05 15:55:00	e3ff90752a8b7115ba552b2df51ff814ea3dabe4
lib/armeabi-v7a/liblinphone.so	970,405	2011/05/05 15:55:00	b2f8b3b4ac5ff8c49e59e6c26561bc8d32c5b3ef
res/anim/from_behind_in.xml	1,088	2011/05/05 15:55:00	88c2212354940cccbc0689837c8326d4729ff472
res/anim/slide_down_out.xml	580	2011/05/05 15:55:00	cb2b714e793ac9c0d9da2b841ccad7ac216d9e50
res/anim/slide_up_in.xml	580	2011/05/05 15:55:00	7d838cdb9dd80200f32c47efac5d2bb0700ed642

KDDI R&D LABS

au Marketのセキュリティ検査：動的解析



附録：攻撃性チェックのレポート： まとめ

Androidアプリケーション安全性評価レポート 2011/07/11

KDDI

アプリケーション

極品美女v1.0
[com.GoldDream.pg]

バージョン	1.0

総合評価

危険	アプリを実行したときのログとアプリに潜在する能力を解析した結果、 危険な挙動と、悪用することで脅威となりうる機能が検出されました。

顕在脅威 － アプリの動作ログや構成要素に注目し、危険な挙動や攻撃的な機能を抽出しています。

危険	情報漏洩	個人情報を漏洩するアプリです。
		端末情報を漏洩するアプリです。
		モバイル広告を利用するアプリです。
	攻撃	未検出
	不適切	管理者権限を必要とする不正なコマンドを実行するアプリです。

潜在脅威 － アプリが利用する機能や情報に注目し、悪用された場合の脅威を評価しています。

危険	アプリケーションの削除
	アプリケーションを直接インストール
	電話番号発信
	SMSメッセージの送信
	おおよその位置情報（ネットワーク基地局）
	精細な位置情報（GPS）
	SMSの読み取り
	SMSの受信
	携帯のステータスとIDの読み取り
	発信の傍受
	起動時に自動的に開始

免責事項

- 本レポートは、評価時点の安全性を示すものであり、将来にわたりこれを保証するものではございません。
- 本レポートは、アプリ単体の評価であり、他のアプリと連携して攻撃するタイプや、外部からコードをダウンロード実行するタイプの悪性アプリを、対象外と致します。

KDDI R&D LABS

スマートフォンとセキュリティ
～アプリ安全性検査とプライバシ保護～

KDDI研究所
竹森 敬祐 （Ph.D）

PCと何が違うの？
煽る報道に惑わされないで！
通常利用では事故は殆ど起きません。

1: はじめに
2: ちょっと気をつけるポイント
3: 端末堅牢化とアプリ安全性検査
4: プライバシ保護に向けて
5: おわりに

プライバシ問題の整理

■ 従来携帯やPCブラウザから取得できなかった情報 ⇒ 利用者自らの提供
- ◆ スマホアプリからのグローバルIDの収集
  例） MACアドレス、端末ID（IMEI）、SIM ID（IMSI）、etc
  ⇒ 利用者側で書き換えできない。
  ⇒ 世界共通のIDによる、名寄せへの不安。
- ◆ スマホアプリによるプライバシ情報の収集
  例）電話番号、メールアドレス、アドレス帳、位置、通話履歴、アプリ一覧、etc
  ⇒ プライバシ侵害に対する不安。

■ ID単体の送信でも、、、
- ◆ スマホからグローバルIDのみが送信された場合でも、送信元アプリの起動という行動履歴にリンク付くため、プライバシ情報の送信とみなされる可能性がある。
- ◆ サイト側で閲覧ページなどの履歴とIDを紐付けると人物像が浮かび上がる。

■ 属性情報単体の送信でも、、、
- ◆ 属性情報が集まると、利用者を特定できる場合がある。⇒ID化

グローバルIDと独自ID

■ グローバルID
- ◆ 利用者側で破棄できない世界統一のID。
  ⇒ 従来携帯アプリから取得できなかった。PCブラウザから取得できなかった。

■ グローバルID'
- ◆ 事業者が独自に生成するIDであっても、複数の事業者で共有される場合には、グローバルIDとみなされることがある。

■ 独自ID（UUID: Universally Unique Identifier）
- ◆ 端末側のアプリ内で独自に生成することで、名寄せへの脅威のないID。
- ◆ 取得者（サーバ）側でも、利用者を特定できないID。
- ◆ Webブラウザでは、cookieが独自IDに近い。

ところで、、、

総務省）「スマートフォン プライバシ イニシアティブ案」(6/29)によると、透明性の確保の為、IDや属性情報を収集する場合には利用者への事前の説明/許諾が必要。

ネット指摘）グローバルIDは名寄せへの脅威があるため、たとえ許諾を得た場合でも収集すべきではない。

基本の提言

■ 目的に沿った最低限の情報収集
- ◆ 事業上、必要以上の情報を収集しないこと。

■ 利用者の認知
- ◆ 利用者が意識して送信する情報については、説明・許諾は必須ではない。
  例） ログイン、ネットアルバム、子供の見守りサービス

■ KDDI研は独自IDを推奨
- ◆ 名寄せへの不安のあるグローバルIDは、できる限り用いない。
- ◆ 独自IDの単独送信はプライバシ侵害の懸念は小さく説明/許諾は必須ではない。
- ◆ 但し、何らかの情報が送信されていることを不安に感じる利用者を考慮して、何処かにリンクを貼る形式で良いので、説明は行うべきである。

■ 制御

A 利用者（端末）側で独自IDを再生成できると、収集者（サーバ）側の情報が無効化する。⇒忘れられる権利

B 利用者側で情報送信の停止を設定できること。

- ◆ AとBのオプトアウト機能を持たず、アプリをアンインストールする手段しかない場合には、アプリの中でその旨を説明すること。

KDDI R&D LABS

アプリ開発者への提言

■ 利用者へ必須の説明
- ◆ 取得する利用者情報の項目・内容　⇒何の情報を
- ◆ 利用目的の特定・明示（アプリのサービス、広告配信か等）⇒何の目的で
- ◆ 情報を取得する事業者の名称、所在地、連絡先　⇒誰が
- ◆ 第三者提供はあるのか（提供の有無、有る場合：誰が、何の情報を、何の目的で）

■ 考慮の必要な点
- ◆ アプリによる端末情報の自動収集、サイト側での閲覧履歴の自動収集など、利用者の知らないところで収集される情報についての説明
- ◆ 利用者からの申告で、情報送信の停止、収集した情報の破棄に関する機構
  - ⇒ プライバシ侵害の不安が小さな場合は、説明によるオプトアウト方式
  - ⇒ プライバシ侵害の不安が大きな場合は、許諾によるオプトイン方式
- ◆ 問い合わせ窓口の設置
- ◆ プライバシ・ポリシの変更を行う場合の手続き

■ 外部の情報収集モジュールを組み込む場合
- ◆ 安全な情報収集モジュールを選ぶこと。
  - ⇒ 事業者は？　収集する情報は？　IDの特性（再生成、送信停止）は？

KDDI R&D LABS

情報収集モジュール提供者への提言

■ アプリ開発者と利用者への説明
- ◆「アプリ開発者への提言」を参照のこと

■ 考慮の必要な点
- ◆「アプリ開発者への提言」を参照のこと

■ 求められる啓発活動
- ◆ 説明はHPなどを通じてアプリ開発者と利用者に説明すること。
- ◆ アプリ開発者へ、アプリ内で情報収集モジュールについての説明を促すこと。

アプリ配信サイトへの提言

■ アプリとその開発者の事前審査
- ◆ プライバシ侵害を判断する基準の策定
  - ⇒ 利用者説明/許諾が必要となる情報の整理、線引き
  - ⇒ 利用者説明/許諾文を読み解き、実際に送信される情報との突き合わせ

■ 不適切なアプリ掲載への対応
- ◆ 不適切なアプリに関する通報窓口を設置する。
- ◆ 不適切なアプリ掲載が判明した場合には、利用者へ注意喚起を行う。

■ 啓発活動の推進
- ◆ アプリ開発者や情報収集モジュール提供者に対し、利用者への説明/許諾に関する対応を促すこと。
  - ⇒ アプリ開発ガイドライン（掲載基準）や講演会を通じた啓発

■ au Marketでは
- ◆ 総務省「スマートフォン プライバシ イニシアティブ」に沿い、アプリがIDや属性情報を送信する場合には、利用者への事前の許諾を求めている。

KDDI R&D LABS

スマートフォンとセキュリティ
～アプリ安全性検査とプライバシ保護～

KDDI研究所
竹森 敬祐 （Ph.D）

PCと何が違うの？
ポイントをおさえれば、事故は殆ど起きません。

1: はじめに
2: ちょっと気をつけるポイント
3: 端末堅牢化とアプリ安全性検査
4: プライバシ保護に向けて
5: おわりに

利用者（お客様）へ

スッピンのAndroidでもかなり安全ですが、あと少し気を付けましょう。

- 3つの脅威への対策
  - 悪性Webサイトの閲覧
    - ⇒ ウイルスバスター等が持つWebフィルタを適用しましょう。
  - 端末の紛失
    - ⇒ パスワードロック、USBデバッグのOFFを施しましょう。
    - ⇒ リモートロック・ワイプを申し込みましょう。
  - 悪性アプリへの感染
    - ⇒ アプリは信頼できる配信サイトから入手しましょう。
    - ⇒ パッチがリリースされたら、速やかに適用しましょう。

法人の管理者へ

スッピンのAndroidでもかなり安全ですが、あと少し気を付けましょう。

- ＋1つの脅威への対策
  - 社員の悪用
    - ⇒ アプリのインストール制限、機能制限
    - ⇒ ログ収集と監査

auのAndroid端末なら

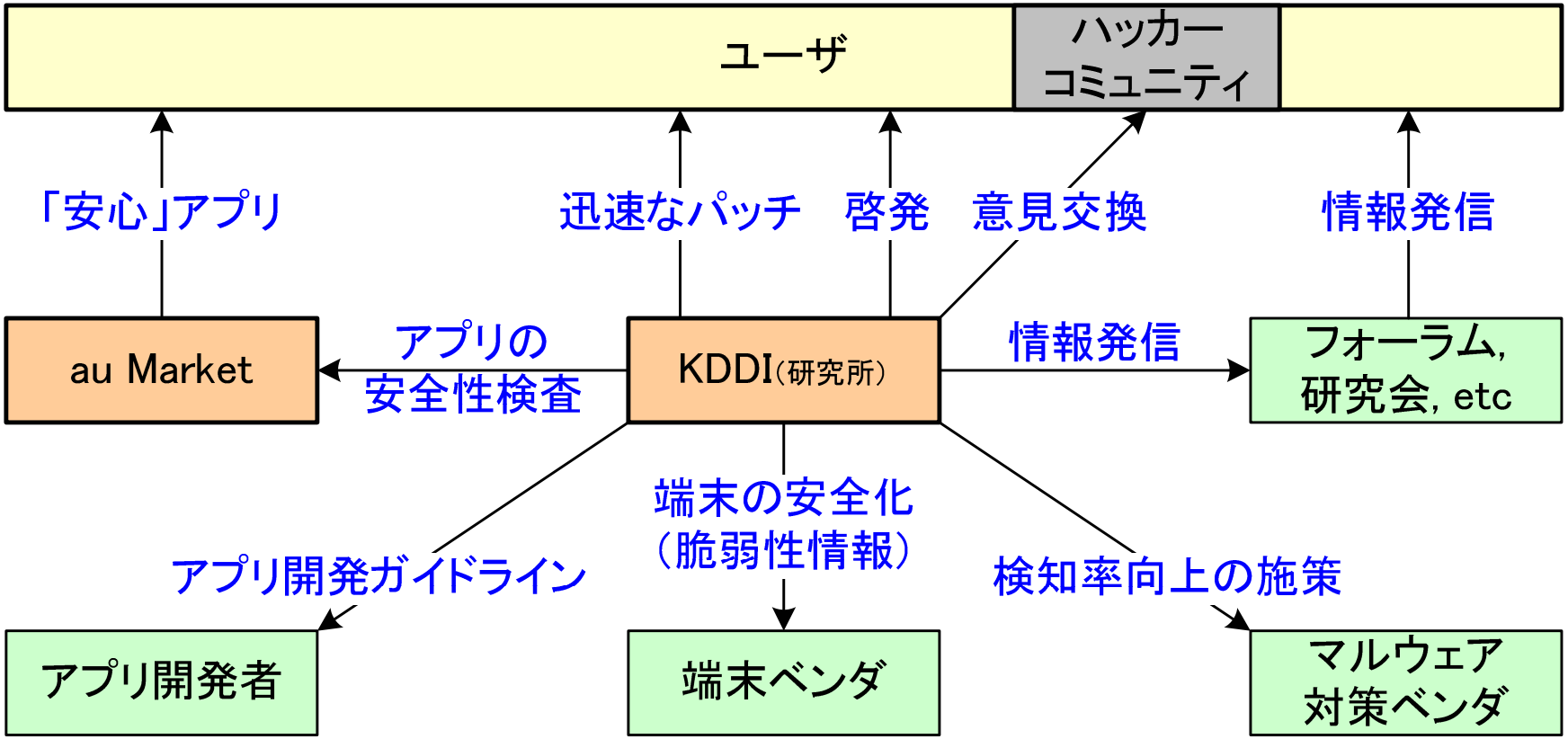
KDDI-3LMでOS層から安全に端末管理できます。

おわりに　～全体を通じて～

■ KDDIの取り組み

◆ 端末の堅牢化やau Market等を通じて、通信キャリアの安全品質を垂直展開

◆ 皆様との連携 ↓　注)「ハッカー」とは高度な知識を有する人材。攻撃者は「クラッカー」と呼ばれる。



スマートフォンセキュリティに関する通信事業者(KDDI)の取り組み