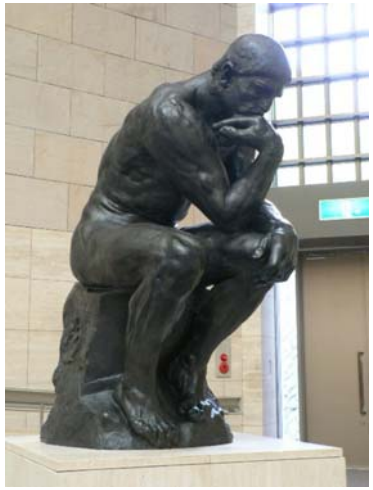
スマートフォンのセキュリティ

KDDI研究所　KDDI



KDDI R&D LABS

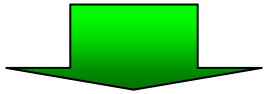
概要

■ スマートフォンの定義 （利便性）

(1) 誰もがアプリケーションの開発を行える。
(2) 誰もがアプリケーションのインストールを行える。
(3) PC向けの汎用OSをベースとした様々な処理機能を持つ。

■ セキュリティ対策 （安全性）

(1) アプリを安全に実行する制御の壁（サンドボックス）を設けている。
(2) 悪意のソフトウェア（マルウェア）への感染を防ぐアプリ配信（Marketプレイス）の安全化が図られている。
(3) PCと同様なセキュリティパッチの適用が行われている。



通常利用で脅威は少ないが、逸脱利用でPCと同様の脅威がある。

危険 ← PC ＜ スマートフォン ＜ 従来の携帯電話 → 安全

■ 展開モデル

◆ 垂直統合型（例：iPhone）：端末／OS／アプリ／通信をクローズドに管理
◆ 水平展開型（例：Android）：“ ”をオープン化して役割分担

KDDI R&D LABS

Android™フォンのセキュリティ

KDDI研究所　KDDI

1: はじめに
2: Android™OSのセキュリティ機構
　ユーザによる承認
　パーミッションの統計調査
　Android Market™
3: 参考：悪意のソフトウェア（マルウェア）

KDDI R&D LABS

はじめに

■ Android™OSの思想

(1) アプリが利用できる機能が豊富で、利便性の高いアプリを実現できる。
⇒ マルウェアを容易に開発できる。

(2) アプリの開発・販売の自由化を図りAndroid Market™に多数のアプリを集める。
⇒ Android Market™はアプリの事前審査は無く、マルウェアの掲載もある。

(3) Android™端末は、独自のセキュリティ機構を持ったPCである。
⇒ PCよりも低い確率で、PCと同様のインシデントが発生する。

■ Android™OSのセキュリティ仕様

(1) インストール時にアプリの機能が表示され、ユーザが承認を与える。
⇒ アプリの良性／悪性の判断は難しい。

(2) Windows PCのような自動的なマルウェア感染は殆ど無い。
⇒ ユーザ自らがマルウェアをインストールする行為に起因する。

(3) アプリはサンドボックスで隔離・実行されるため、端末への影響を抑止している。
⇒ 端末を完全に制御できるroot権限を奪うことによって、サンドボックスを越えた想定外の事象が発生する。

はじめに　～セキュリティ視点での比較～

	従来の携帯	Android™フォン	PC（汎用OS）
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）	オープン *1 （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 （無し *1）
コンソール	無	有	有
root権限アプリ	無	無 *2	有
マルウェア感染	限定的	有（手動）	有（手動 & 自動）
Webスクリプト攻撃	限定的	有 *3	有
フィッシング	有	有	有
端末認証子管理	強（堅牢に保護）	弱（APIアクセス可）	―
暗号化ディスク	無	限定的	有
リモートロック	有	有	無
リモートワイプ	有	有	無
総合的な安全度	★★★	★★	★

*1 一部例外あり
*2 Android OSの想定外であるが、Jailbreakを想定したroot権限利用アプリがある。
*3 PCのような自動的なマルウェア感染はないが、SDカードからの自動的な情報漏洩の可能性はある。

懸念

KDDI R&D LABS

Android™OSのセキュリティ機構

■ セキュリティ対策と脆弱性

◆ 仮想マシンを実装し、アプリをサンドボックス上で隔離・実行させる。

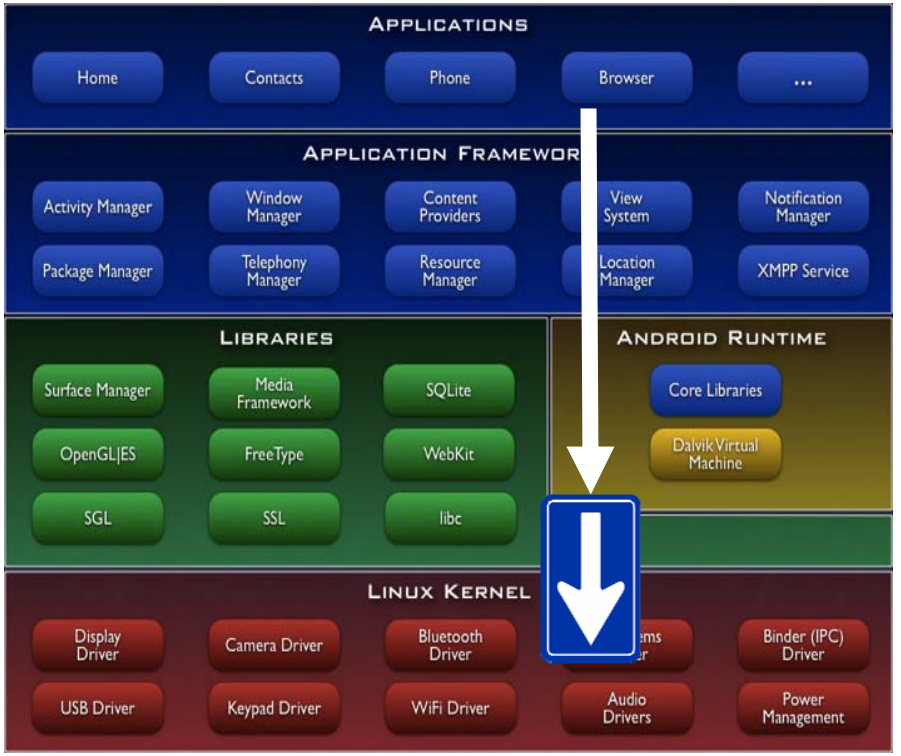
◆ アプリのインストールには、利用する機能の承認ボタンのクリックが必要である。

功 Windows™XPのような自動感染型ウイルス・ワームは殆どない。

罪 パーミッション承認で、仮想マシンに穴を開けることができる。

連鎖的なウイルス感染はない

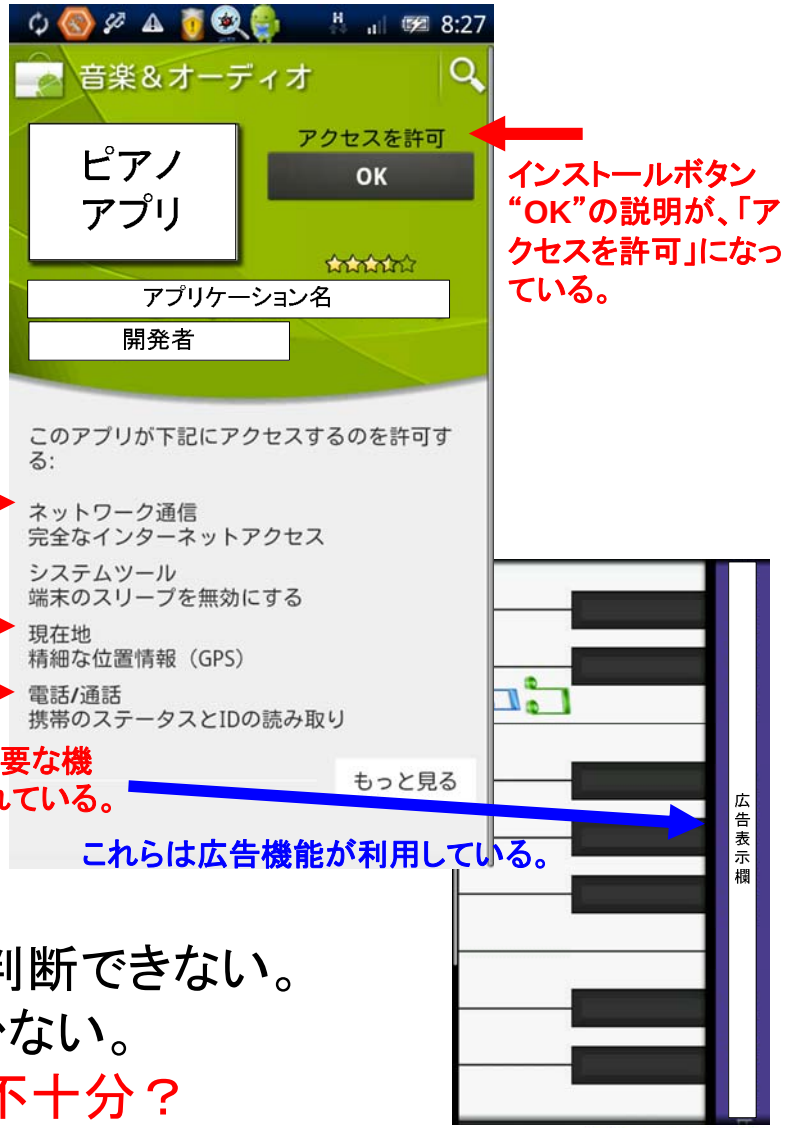
ユーザの誤操作によるマルウェア感染



KDDI R&D LABS

ユーザによる承認

■ パーミッション機構
- ◆ Android™OSからユーザに対して、アプリが利用する機能を表示して、インストールの可否を問うている。



インストールボタン“OK”の説明が、「アクセスを許可」になっている。

■ パーミッション機構の功罪
- 功 ユーザ承認で、個人情報や各種機能を利用する便利なアプリを組み込める。
- 罪 パーミッションに潜在する脅威を見抜けないユーザは、マルウェアに感染する。

ピアノに不必要な機能が列挙されている。

これらは広告機能が利用している。

■ 問題点
- ◆ 機能単位の利用申請であり、悪意の有無を判断できない。
- ◆ そもそもパーミッションを気にするユーザは少ない。

⇒ Android™OSのパーミッション機構だけでは不十分？

KDDI R&D LABS

パーミッションの統計調査

■ 調査

- ◆ Android Market™から646アプリを取得し、パーミッションの利用率を調査した。
- ◆ 携帯電話特有の情報へアクセスするアプリが多数あることが判明した。
  但し、情報アクセスに関するパーミッションの多くは、広告機能によるものである。

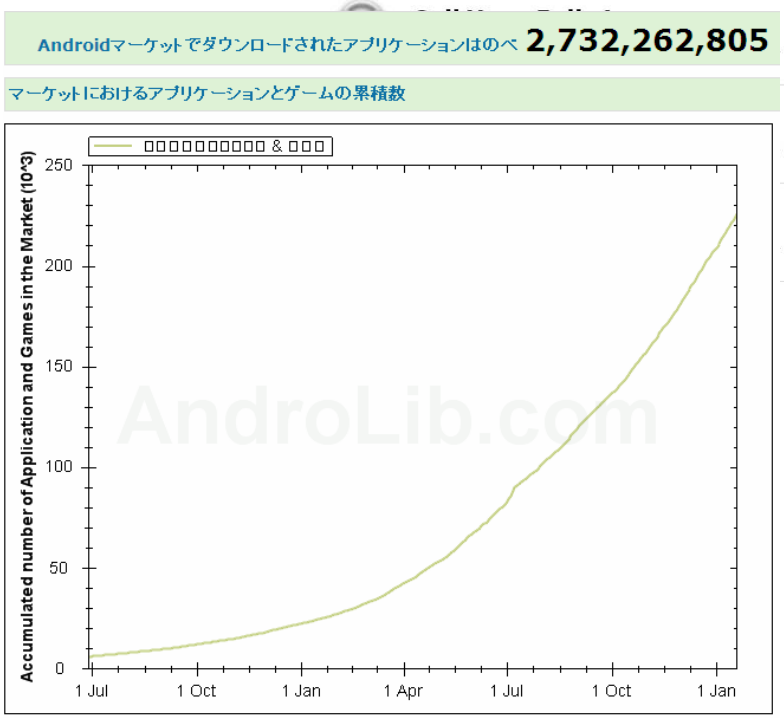
パーミッションの利用頻度（2010年7月調べ）

アプリ数 全646個	率 （%）	Android パーミッション	説明
358	55.4	INTERNET	ネット接続
127	19.7	VIBRATE	バイブレート機能
113	17.5	WAKE_LOCK	スリープの無効化
111	17.2	READ_PHONE_STATE	電話情報・IDの読取
102	15.8	ACCESS_COARSE_LOCATION	大よその位置取得
98	15.2	ACCESS_FINE_LOCATION	詳細な位置取得
83	12.9	ACCESS_NETWORK_STATE	ネット状態の取得
75	11.6	READ_CONTACTS	アドレス帳の読取
67	10.4	RECEIVE_BOOT_COMPLETED	自動起動の登録
46	7.1	WRITE_EXTERNAL_STORAGE	SDカードへの書込

Android Market™

- Android Market™上のアプリ(2011年1月中旬)
  - 20万以上のアプリが公開されている。
  - 延べ27億アプリがダウンロードされている。

- Googleの取り組み
  - Android Market™では、開発者登録を行う。
    >Google（Gmail）アカウントの登録
    >Googleチェックアウトでのクレジット支払
  - ⇒ マルウェアが掲載されることは殆ど無い。
  - ユーザからの申告を受けて、マルウェアを駆除する、迅速な事後対応を図っている。
  - ⇒ 直ぐに駆除されることで感染のリスクを低減。



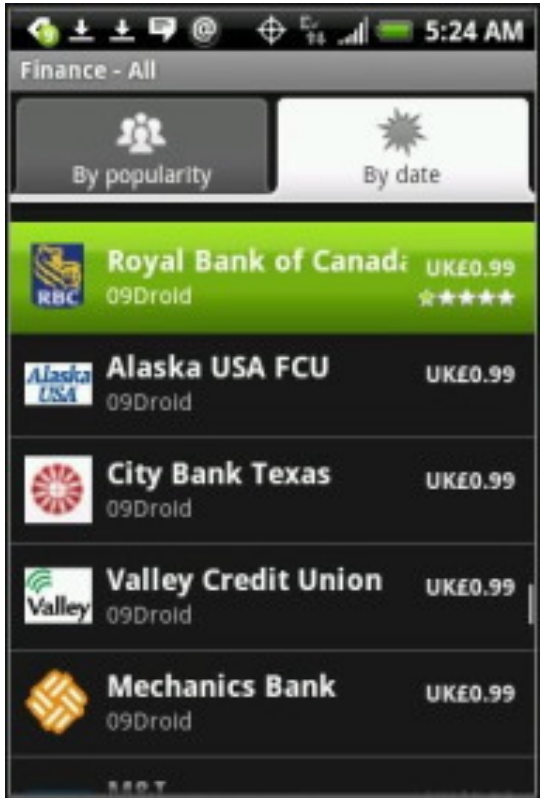
http://jp.androlib.com/appstats.aspx

KDDI R&D LABS

参考：フィッシング（キーロガー）アプリ

■ オンラインバンキング
- ◆ Droid09と呼ばれる匿名の開発者がリリースしたオンラインバンキングアプリにキロガーが内包されていたとの報告がある。

http://www.itmedia.co.jp/enterprise/articles/1001/12/news018.html
http://journal.mycom.co.jp/news/2010/01/14/019/index.html



■ キーロガー・パーミッション
- ◆ android.permission.READ_INPUT_STATE
  入力や操作の記録。別のアプリケーションへの入力（パスワードなど）でもキー入力を監視することをアプリケーションに許可します。
- ◆ 端末操作の記録には有効である。

■ 問題点
- ◆ キーモニタ・パーミッションを内包し、他のアプリを含む全てのキー操作を記録する。

KDDI R&D LABS

参考:情報漏洩アプリ

■ 表面上の機能

- ◆ 某マルウェア対策アプリは、端末内アプリをスキャンする。
- ◆ 本物のマルウェアは一つも検知できない。

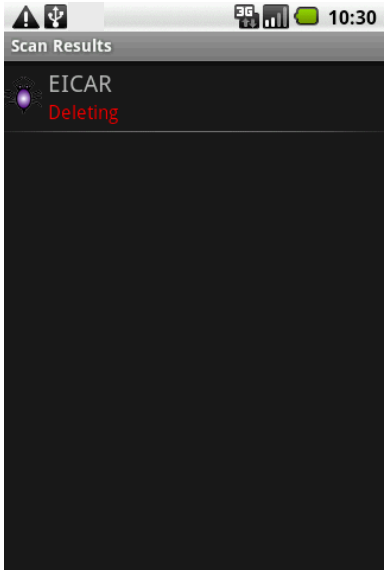
■ 31個のパーミッション

INTERNET、DELETE_PACKAGES、RESTART_PACKAGES、
READ_PHONE_STATE、RECEIVE_SMS、
READ_CONTACTS、WRITE_CONTACTS、CALL_PHONE、
READ_SMS、WRITE_SMS、SEND_SMS、GET_TASKS、
RECEIVE_BOOT_COMPLETED、INSTALL_PACKAGES、
ACCESS_NETWORK_STATE、WRITE_APN_SETTINGS、
PROCESS_OUTGOING_CALLS、INSTALL_SHORTCUT、
LOCATION、ACCESS_FINE_LOCATION、
ACCESS_LOCATION_EXTRA_COMMANDS、
ACCESS_MOCK_LOCATION、
ACCESS_COARSE_LOCATION、
ACCESS_COARSE_UPDATES、CALL_PRIVILEGED、
MODIFY_PHONE_STATE、GOOGLE_AUTH.mail、
WAKE_LOCK、WRITE_EXTERNAL_STORAGE、
USE_CREDENTIALS、VIBRATE

パーミッション承認

スキャンの様子

本物のマルウェアを非検知



■ 問題点

- ◆ 端末ID（IMEI）、契約 ID（IMSI）がアプリ作成者のサーバに送信される。

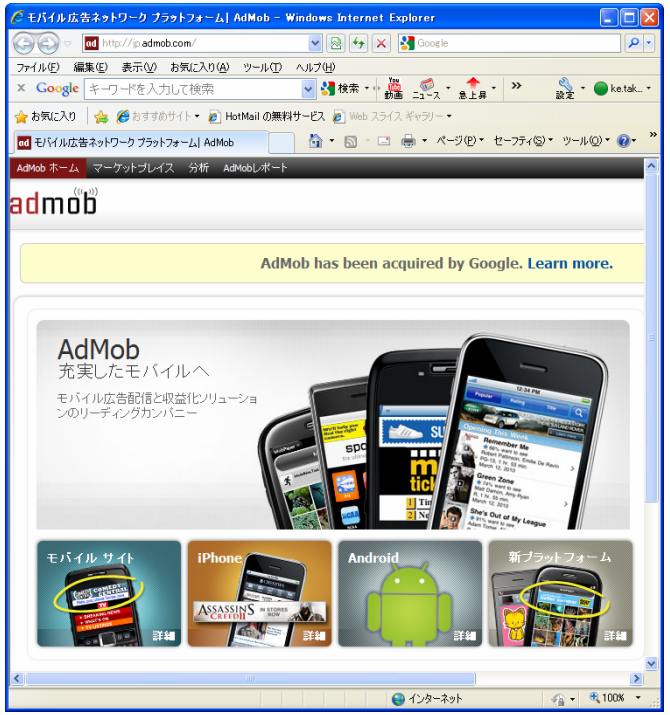
KDDI R&D LABS

参考:広告機能

- READ_PHONE_STATEアプリ
  - 本パーミッションを持つアプリの多くは、広告機能を内包している。
  - アプリ内の広告をユーザがクリックすることで、開発者に報酬が入る。

- 仕組み
  - 国コードで、適切な言語で広告を表示する。
  - 緯度・経度で、場所に応じた広告を表示する。
  - Android ID、IMEI、IMSI でユーザを識別する。

- 現状
  - 広告事業者は、パーミッションによる承認で、情報収集の可能性はユーザに確認済み。
  - ★ 収集する情報とその利用目的を知らせていない？



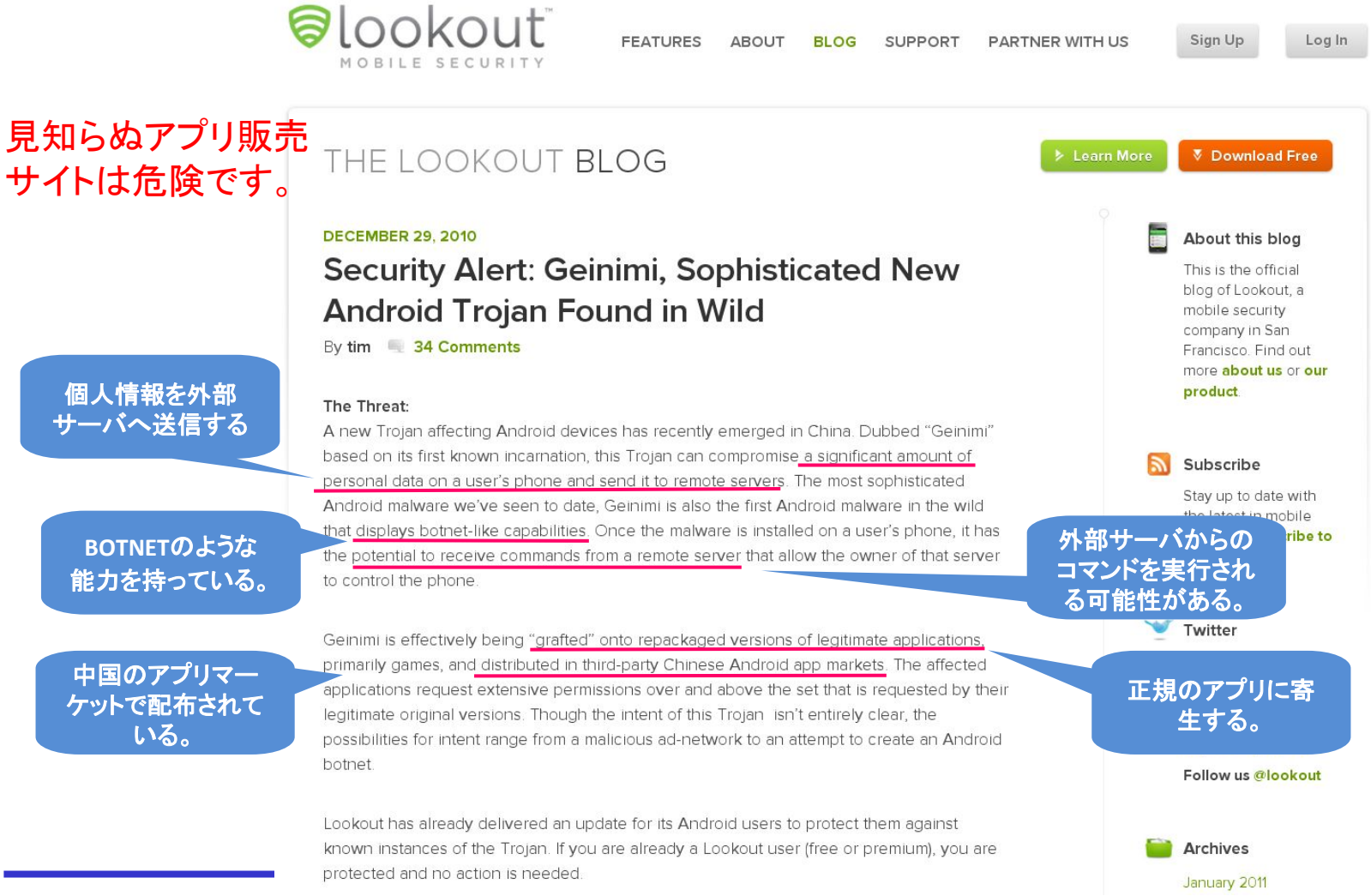
http://jp.admob.com/

KDDI R&D LABS

参考:トロイ型のボットアプリ

■ Android™端末を踏み台にするボットネット「Geinimi」が現れた。

http://blog.mylookout.com/2010/12/geinimi_trojan/



見知らぬアプリ販売サイトは危険です。

個人情報を外部サーバへ送信する

BOTNETのような能力を持っている。

中国のアプリマーケットで配布されている。

外部サーバからのコマンドを実行される可能性がある。

正規のアプリに寄生する。

KDDI R&D LABS

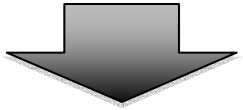
参考：root権限奪取

■ 参考：iPhone™のJailbreak http://www.f-secure.com/weblog/archives/00001814.html
- ◆ ユーザが、root権限のsshサービスを内包するJailbreakツールを組み込む。
- ◆ sshのログインID/PWDが既知のため、外部からroot権限でログインされ、ボット化する。

■ Android™のroot権限奪取
- ◆ iPhone™のJailbreakと同じく、ユーザが、sshサービスを内包するroot権限奪取ツールを利用して携帯電話を改造した場合、外部からroot権限でログインされ、ボット化する。

注1）OS（Linux)層に、不正なサービスを外部から自動的に組み込むことが可能である。
注2）アプリ（Dalvik）層の上にあるAndroid™アプリの自動インストールは不可能である。

■ root権限利用アプリ
- ◆ root権限を利用するアプリを組み込むことは、Google、端末ベンダ、通信キャリアが想定した操作を超えるため、不具合やインシデントの原因になりかねない。



★ 改造は、root 権限を、端末所有者のみならず、外部の攻撃者にも与える。
★ 公共の電波を制御する端末の改造行為は、電波法違反の可能性がある？！

Jailbreakは決して行わない！

Androidセキュリティに関する KDDIの取り組み

KDDI　KDDI研究所

1: はじめに
2: セキュアアプリ検証
3: アプリ開発ガイドライン
4: ユーザへの啓発
5: 端末の安全化

KDDI R&D LABS

はじめに

■ KDDIの分析

(1) 多くのユーザは、Marketプレイスを通じてマルウェアをインストールする。
(2) 一部のユーザは、端末を攻撃してソフトウェアを改造し、自分好みに設定する。
(3) 普及の初期段階では、Androidフォンのセキュリティの考え方が浸透していない。

■ KDDIの取り組み

(1) Marketプレイスを安全化すれば、多くの脅威を除去できる。
(2) OS・アプリの脆弱性の撲滅は不可能であり、改造抑止の啓発活動を進める。
(3) ショップや講演会などを通じて、危険なポイントの周知に取り組む。
通信キャリアとして、縁の下でユーザをフォローする。

セキュアアプリ検証　～日本品質の au one Market～

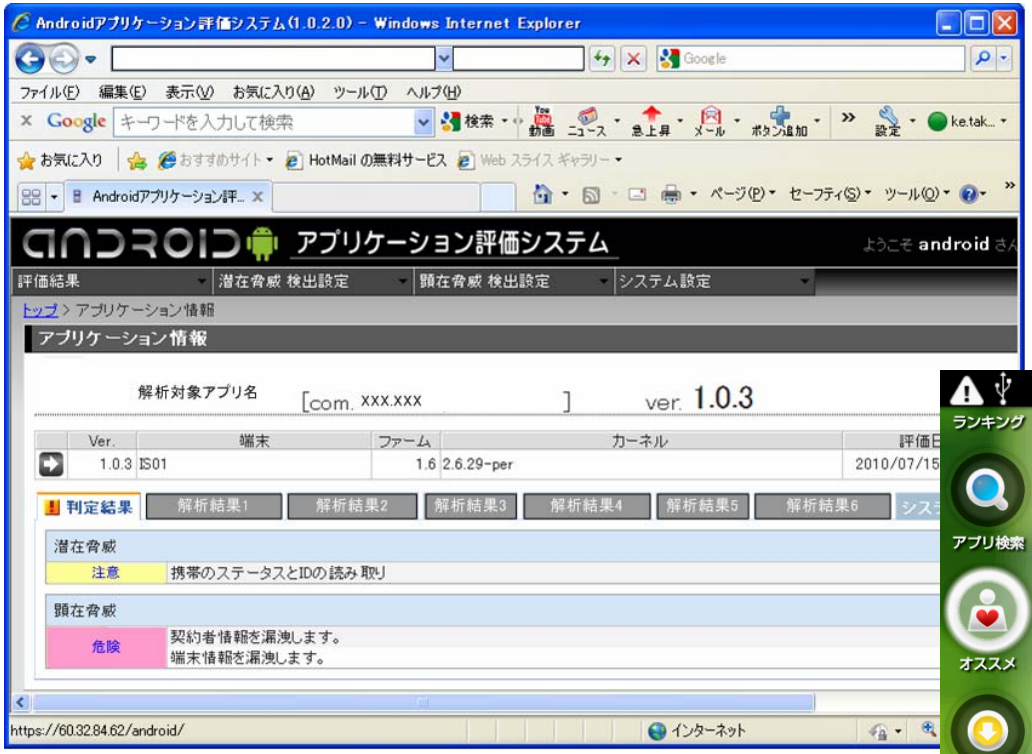
■ 安全なau one Marketサービス

★ Androidのセキュリティ事故の多くは、ユーザによるMarketからのマルウェアのインストールで生じる。

◆ 潜在脅威（静的解析）：難解なAndroidパーミッションの解読を、お客様に代わってKDDIが検証する。

◆ 顕在脅威（動的解析）：不審な挙動に注目して、お客様に代わってKDDIが検証する。

⇒ au one Marketセキュアアプリ検証を受けたアプリに、セキュアマークを付与している。



様々な独自技術でAndroid
アプリの安全性を評価

セキュアマーク

KDDI R&D LABS

アプリ開発ガイドライン

■ アプリ開発者への啓発活動

◆ au one Market™セキュアアプリ検証で確認するポイントを明確にすることで、安全なアプリ開発を促している。

au one Market™セキュアアプリの検証では、以下の点に関する確認を実施しています。

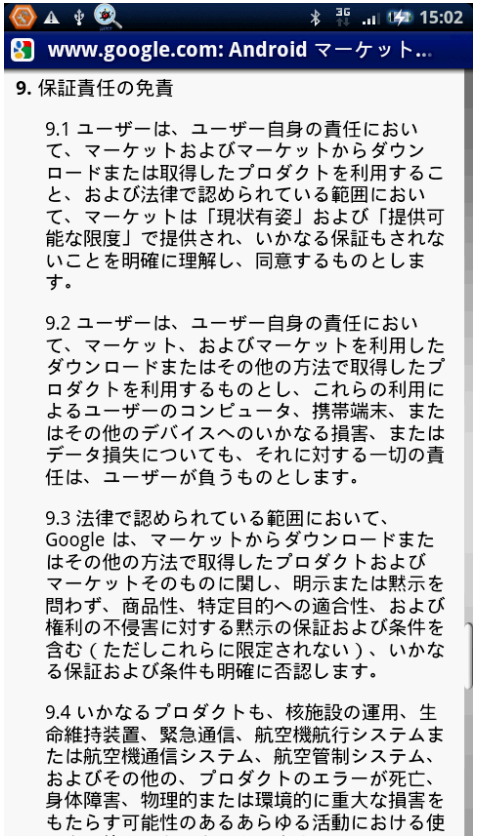
1. 利用を宣言した機能（セキュリティー権限）の確認。
2. KDDIが提供しているAndroid™アプリ配信サーバから配信していること。
3. KDDIから出荷されるAndroid™端末の標準設定で利用できない機能の有無の確認。
4. 顧客情報を漏洩する動作、もしくは、漏洩する恐れのある動作の有無。
5. 不必要な大量通信の有無、もしくは、外部への不正アクセス機能の有無。

◆ 特に、重要な情報を外部へ送信する場合には、アプリケーションのストーリの中で、ユーザ承認を求める許諾画面を設けるように指導している。

ユーザへの啓発

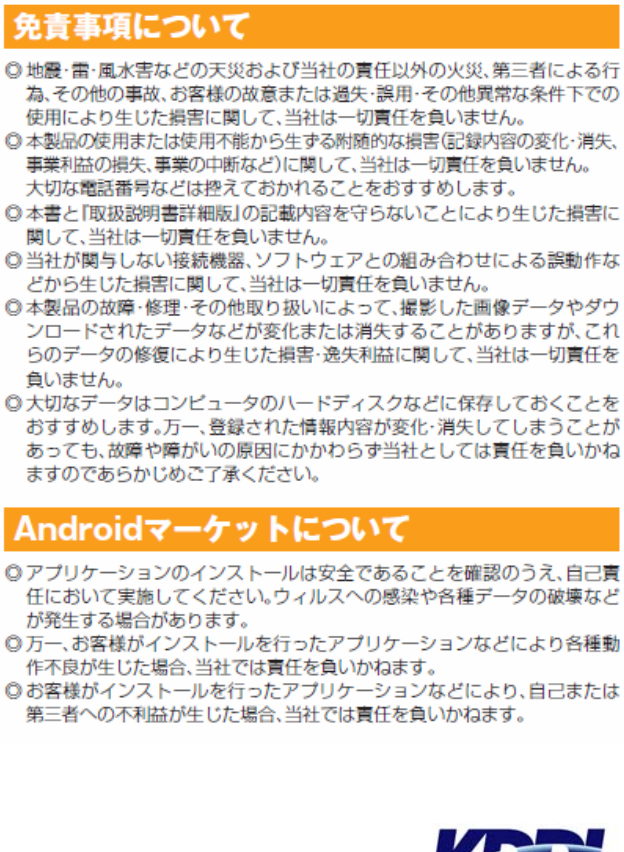
■ 利用規約を通じた啓発活動
- ◆ Market運用者は、ユーザ責任でアプリのインストール・利用について注意喚起している。
- ◆ KDDIは、さらに踏み込んで端末の取扱説明書での注意書きや、ショップでの口頭説明＋承認プロセスを設けて、Market利用の危険性に関する啓発活動に努めている。

Android Marketの免責



au one Marketの免責

IS01取扱説明書



免責事項について

◎地震・雷・風水害などの天災および当社の責任以外の火災、第三者による行為、その他の事故、お客様の故意または過失・誤用・その他異常な条件下での使用により生じた損害に関して、当社は一切責任を負いません。
◎本製品の使用または使用不能から生ずる附随的な損害（記録内容の変化・消失、事業利益の損失、事業の中断など）に関して、当社は一切責任を負いません。大切な電話番号などは控えておかれることをおすすめします。
◎本書と「取扱説明書詳細版」の記載内容を守らないことにより生じた損害に関して、当社は一切責任を負いません。
◎当社が関与しない接続機器、ソフトウェアとの組み合わせによる誤動作などから生じた損害に関して、当社は一切責任を負いません。
◎本製品の故障・修理・その他取り扱いによって、撮影した画像データやダウンロードされたデータなどが変化または消失することがありますが、これらのデータの修復により生じた損害・逸失利益に関して、当社は一切責任を負いません。
◎大切なデータはコンピュータのハードディスクなどに保存しておくことをおすすめします。万一、登録された情報内容が変化・消失してしまうことがあっても、故障や障がいの原因にかかわらず当社としては責任を負いかねますのであらかじめご了承ください。

Androidマーケットについて

◎アプリケーションのインストールは安全であることを確認のうえ、自己責任において実施してください。ウィルスへの感染や各種データの破壊などが発生する場合があります。
◎万一、お客様がインストールを行ったアプリケーションなどにより各種動作不良が生じた場合、当社では責任を負いかねます。
◎お客様がインストールを行ったアプリケーションなどにより、自己または第三者への不利益が生じた場合、当社では責任を負いかねます。

KDDI R&D LABS

端末の安全化 ～日本市場への浸透に向けて～

■ 脆弱性の調査・対策指導・研究

◆ 普及期では、グローバル端末をそのまま日本市場に投入するのは不親切と考えている。

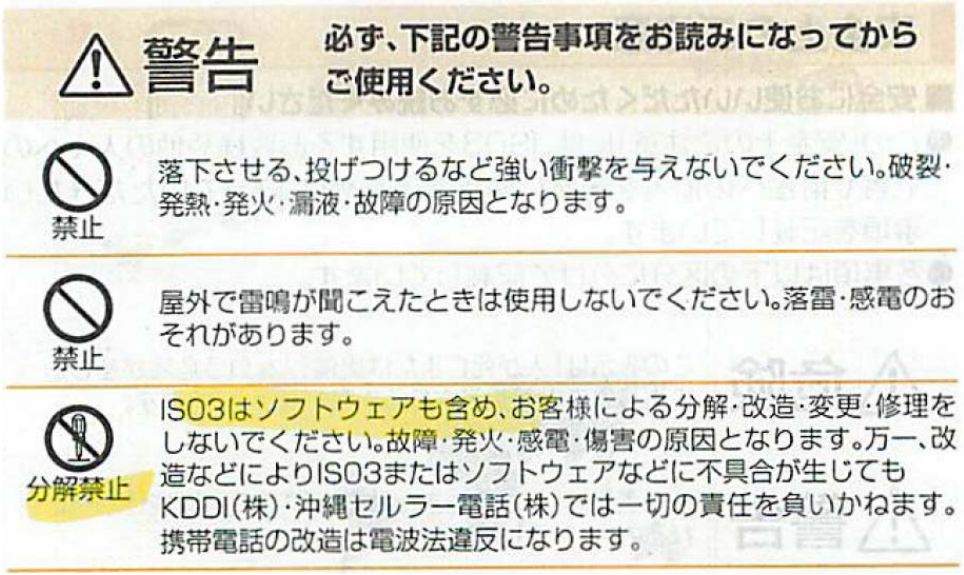
⇒ KDDI（研究所）は、セキュリティインシデントの調査・分析・対策指導を実施している。

⇒ Googleや端末ベンダへのフィードバックと、パッチの迅速なリリースを実施している。

⇒ Android™セキュリティに関する研究活動を積極的に推進している。

インシデントの収集・分析・対策者の特定（2008-2009）

年月	対象	脆弱性の詳細	原因	対策
2008/10	組込アプリ	Webブラウザの乗っ取り	WebブラウザのオープンソースのWebKitの脆弱性を突いたバッファオーバフローでブラウザプロセスが乗っ取られる。	最新のライブラリを利用する。
2008/11	Android (root奪取)	telnet経由のroot侵入	ターミナルソフトをインストールして、ここからtelnetdを起動する。G1端末のIPアドレスにtelnet接続すると、認証なしでログイン。	ターミナルをユーザに提供しない。不要なサービスを削除して出荷する。
2008/11	端末H/W	アプリに対するキー入力をOSが実行(OSコマンドインジェクション)	シリアルポート接続されたデバイスのキー入力を受け取るinit.rcの設定が残っており、キーボード入力をOSが直接受け取っていた。	シリアルポート経由のアクセス設定を見直す。
2008/11	端末H/W	ログイン認証の無効化	menuキーを押し続けるとセーフモードで起動する。この場合、ログイン機能やスクリーンロック機能がバスされる。	セーフモードで起動した場合でも認証機能を設けておく。
2009/01	組込アプリ	URLの非表示によるフィッシングサイトへの誘導	Gmailブラウザにおいて、ハイパーリンクを閲覧できない問題と、From:とReply-to:を閲覧できない問題がある。	Gmailブラウザ のURLやアドレス参照機能の設計に注意
2009/02	組込アプリ	Webブラウザの乗っ取り	Webブラウザのサブシステム(PacketVideo)が利用するOpenCoreライブラリの脆弱性を突いたバッファオーバフロー攻撃を受ける。	OpenCoreライブラリのパッチを適用する。
2009/05	Android	公開アプリ認証の不具合	Android-SDKに、公開アプリ間のデータ参照や制御を自由に行えてしまうアプリ間認証の不具合があった。	uidの制御を 修正するパッチをリリースした。
2009/05	Market	SDKにAndroid Market通信アプリのインストール	Android-SDKからでも、Android Marketと通信できるようにするSetupWizard.apk, gtalkservice.apk, Talk.apk, Vending.apkが公開。	Vending.apk(Market)アプリを公開させない。SDKと商用端末を見抜く機能が必要。
2009/08	Linux	ネイティブアプリのメモリダンプ	Linux用のメモリダンプツールを、ARM用にクロスコンパイルすることで、Android上のネイティブアプリのメモリダンプを取得できる。	秘匿性のある処理をメモリ上で行わない。ptraceなどの権限を最小化する。
2009/08	Linux (root奪取)	ファイルI/Oメモリ制御の不具合 (CVE2009-2692)	CVE2009-2692のLinuxのメモリ/Oの初期化不具合を突いて、端末にrootでログインするマルウェア"asroot"が公開。	Linuxのパッチを適用する。
2009/09	公開アプリ	Web・FTP系アプリの公開	Web・FTPサーバ系の公開アプリをインストールすると、通信Portがオープンする。FTPはパスワード無しでログイン可。	—
2009/10	Market	Marketアプリの PC へのダウンロード（なりすまし端末）	Android Marketのフリーアプリのダウンロードに利用する4つのID（assetID, userID, device ID, authToken）を偽装できてしまう。	有料アプリのダウンロードについて、クライアント認証の仕組みを確認すべき。
2009/10	Android	SMSとDalvikの脆弱性でリモートから端末停止(CVE2009-2999)	SMSの脆弱性と、Dalvik APIの脆弱性がある。特殊なSMSパケットをAndroid端末に送りつけると、Dalvik上のサービスが停止する。	SMSとDalvik APIのパッチを適用する。(HT-03AはSMSの影響なし)
2009/10	端末H/W (root奪取)	カスタムROMのインストール (Recovery Utilityの改造)	CVE2009-2682でrootを奪取したHT-03A(v1.5)に対して、SDカード起動を許可する改造で、root付きROMをインストールできる。	Recovery Modeを排除すること。
2009/11	端末H/W	SIMロックの解除	HT-03A(1.5)の場合、端末コード(IEME)にリンク付けられたSIMロックを解除コード(PIN)の計算手法が解読されている。	SIMロックの解除コードを入力させるインタフェースを排除すればよい。
2009/11	公開アプリ	WiFiやBluetoothのホットスポットになり3Gへのテザリング	WiFiやBluetoothデバイスと3Gデバイスを接続してテザリングした。後位端末を見抜くことが出来ない。	iptablesでWiFi⇒3G通信を規制する。
2009/12	端末H/W (root奪取)	OSアップデートイメージの認証手法が漏洩してOSをダウングレード	純正HT-03A端末では、OSの配布元とバージョンを確認する検証コードが付与されている。この検証コードのアルゴリズムが漏洩。	OSをダウングレードさせないバージョンチェックを組み込む。



■ 端末改造の抑止の呼びかけ

◆ ソフトウェアを含む端末の改造を禁止しています。

KDDI R&D LABS

スマートフォンセキュリティに関する今後の課題

KDDI研究所　KDDI

1: 日本基準を世界標準に
2: ユーザ意識の醸造

KDDI R&D LABS

日本基準の安全を世界標準に

■ マルウェアの定義

◆ 事業者間連携を図り、日本基準のマルウェアの定義を世界に発信することで、Marketプレイスやマルウェア対策ベンダの安全化へと、寄与すべき。

■ 水平展開モデルへの発言

◆ 端末／OS／アプリ／通信のプレーヤ毎に、セキュリティ対策を独自に判断している中で、事業者間連携で、日本の安全基準を垂直統合的に発言していくべき。

⇒ KDDIはお客様と共に、日本の安全に対する考え方をグローバルに発信します。

ユーザ意識の醸造

■ 汎用OSの意味
- ◆ スマートフォンは、PCで培われた汎用OSが搭載されている。
  - × 従来の携帯電話の高機能版
  - ○ PCに電話機能が付いたもの

■ 世界標準OSの意味
- ◆ アプリインストールのリスクは、PCと同じく、ユーザに判断が委ねられている。

■ 逸脱行為の意味
- ◆ 端末／OS／アプリ／通信の各プレーヤが適切に設定した端末を改造する行為は、本人のみならず、他のユーザへも迷惑を掛ける可能性がある。

■ 見知らぬMarketプレイスの意味
- ◆ セキュリティ管理のないMarketプレイスから、アプリを入手するのは危険である。
- ◆ 有料のアプリが、無料で配布されている場合、マルウェアの可能性が高い。