応用 一般

4

北島 真理子
ソニーエリクソンモバイルコミュニケーションズ（USA）Inc.

スマートフォン向け適正アプリの開発と配信サイト

日本の伝統ICT産業の危機

■ スマートフォンの光と影

アプリケーション（以後，アプリと略す）の実行プラットフォームであるスマートフォンが急速にシェアを伸ばす中で，専用端末で培われてきた日本の伝統ICT産業である家庭用ゲーム業界に危機が迫っている．スマートフォンのベースはPCであり，端末としての高い処理能力，アプリの高い移植性，ネットワークの接続性など，専用端末との垣根が薄らいでいる．いわゆる，ゲーム端末と電話機の融合である．特に，Androidにおける融合は，垂直管理されてきた品質保証のゲーム開発のスタイルから，世界の個人層にまで開発現場が拡がった水平展開への移行をも意味する．ここで注意すべきは，リテラシーやモラルの乏しいアプリ開発者による，不正コピーの氾濫や悪意のコード（マルウェア）の埋め込み，それを許すアプリ配信サイトの存在である．このような状況の中，日本のゲーム開発者にとって，Android向けアプリ市場に開発アプリを提供するリスクの高さ，低価格化が進むことでの収益の低下，低俗アプリに埋もれる懸念など，新たな潮流からの生き残り策が問われている．

本稿では，日本を元気に“保つ”ICTの例として，Android向けアプリ開発や配信における問題点を洗い出し，その対策や業界の取り組みを紹介する．特に，アプリ開発者への啓発とアプリ配信サイトが取り組むべきポイントについてまとめる．

■ 日本の伝統ICT産業の危機

スマートフォンの特徴

本稿で考えるスマートフォンの光と影を列挙してみる（図-1）．

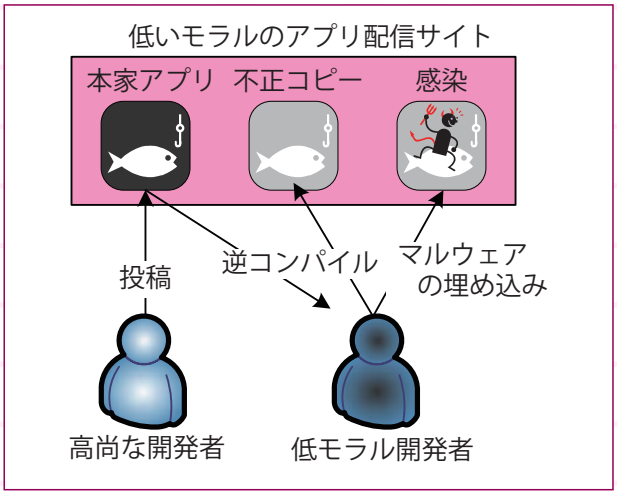

図-1　アプリ開発者にとっての光と影

（1）アプリ開発と配信が自由化された携帯端末
　-> 開発や配信が世界の個人層まで拡がり，アプリの品質や開発者のモラル低下が進む
（2）アプリ開発キットが充実
　-> 逆コンパイルツールによるコードの盗用
（3）PCに電話アプリが搭載されたネット端末
　-> 端末を踏み台にしたマルウェア感染

低品質アプリ

品質やセキュリティを管理しないアプリ配信サイトには，練習目的で作成した不具合だらけのアプリやユーザにとって脅威となり得るアプリがたくさん並んでいる．価格と品質が直接的に関連していないことや，利便性と安全性を備えたアプリを事前に知ることが難しいという問題がある．

日本のゲームアプリは，開発費を要するものの高

図-2　Android Marketで，左「sudoku」を検索，右「テトリス」を検索

品質なアプリが多く，価格もそれなりの額になる．低品質で無料アプリが並ぶ配信サイトでは，高額であるが高品質な日本のゲームアプリが埋もれてしまう問題がある．

偽物アプリ

日本のパズル制作会社のニコリが数独というゲームを開発した．世界的には，sudokuとして知られている．パズルゲームとして，画面構成の手軽さ，規則性の明解さから，世界中のアプリ開発者によって模倣されている．Android Marketで「sudoku」と検索するとたくさんのアプリがヒットし，20番目あたりに本家の無料版が，40番目あたりに本家の有料版が出てくる．海賊版に本家アプリが埋もれており，プロの開発者にとって，品質維持に重要な利益を見込めない状況にある（図-2左）．

次に「テトリス」と検索すると，やはりたくさんのアプリがヒットする．本家のテトリスを容易に探すことはできない．中には，本家でないテトリス同士で，画面イメージやプレイ機能がほとんど同じで，明確な差異は開発者（署名）だけというものまである（図-2右）．

Javaベースの開発環境を引き継ぐAndroidアプリの場合，逆コンパイルが容易であり，抽出したコードを再コンパイルしたものも正しく動作する．このため，他者が開発したアプリのコードを不正にコピーして，再署名した偽物アプリが氾濫しているものと推測される．日本の高度なゲームアプリは狙われやすく，注意が必要である．

感染アプリ

2010年12月に，世界初となるAndroid向けの踏み台型（以後，ボットと呼ぶ）アプリが現れた．これは，有料のゲームアプリを逆コンパイルして，ボットコードを埋め込んで再コンパイルし，中国の配信サイトを通じて無料で公開されたものである．ゲームとしての機能はそのままに，密かにボットとして動作するため，感染しても気づくことは難しい．こうした感染アプリが出回ることで，元となった本物のアプリが敬遠されてしまう問題がある．

■ 危機を救う対策

昨今，旧作ゲームの利用やカジュアルな導入機として，スマートフォンが代用できてしまう．この状況の中で，日本の高度な技術レベルであるゲーム開発のスタイルや業界そのものを保つためにも，世界のアプリ開発者への啓発と，高品質なアプリを適正価格で安心して供給できるアプリ配信サイトの運用は重要である．

アプリ開発者の啓発

❖ 法令・文化・著作権の遵守

Android向けアプリは，世界中で利用されることを念頭に，設計・開発する必要がある．つまり，利用されるすべての国の法令に遵守した設計とし，地域の文化や表示言語に配慮しなければならない．

逆コンパイルが容易であるものの，取り出したコードやイメージ画像の著作権はオリジナルの開発者にあることを忘れてはならない．

❖ 端末で管理される情報の収集のあり方

個人との結びつきの強いスマートフォンでは，ユーザに関する識別子や嗜好を活用したサービス提供が活発に行われている．こうしたユーザ情報を収集するモジュールを組み込む場合には，その特性を理

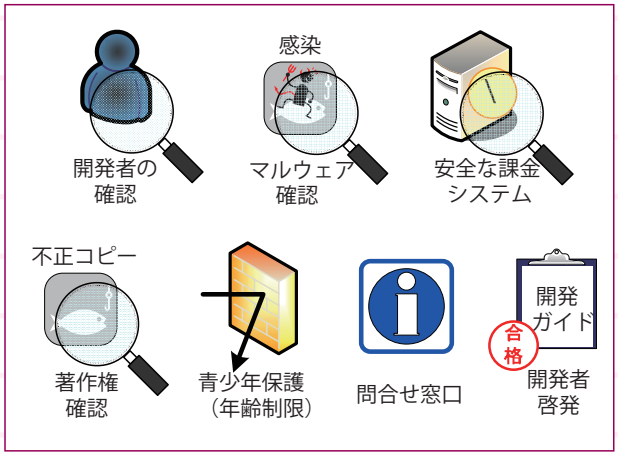

図-3　配信サイトの信頼向上のための運用像

解した上で，何の情報を，なぜ，誰が取得するのか，アプリのシナリオ中でユーザに説明を行い，許諾を得る仕組みを設ける必要がある．

適切な配信サイトの運用

アプリ配信サイトが，アプリ開発者およびユーザにとって安心でき，Androidサービス全体としての信頼性の向上に繋がる施策を紹介する（**図-3**）．

❖開発者の確認

配信サイトは，個人・法人にかかわらず配信アプリの開発者の実在と事業内容の確認が重要である．また，高品質で安全なアプリを開発する個人や法人を認定するなど，開発者認証の仕組みを設けるのもよい．

❖マルウェア感染の確認

配信するアプリについては，以下の項目などに注目したセキュリティ検査を行うとよい．なお，検査については，実行時の挙動に注目した動的解析や，アプリを構成するファイルやコードに注目した静的解析がある．

(a) 情報漏洩：勝手に識別子やプライバシーに関する情報を外部に送信していないか？

(b) 不正課金：勝手に料金の発生するサービス（電話やSMS）を利用していないか？

(c) 脱獄：本来利用できないコマンドやAPIを利用していないか？

-> OS・ドライバ・ライブラリなどに潜む脆弱性を突く攻撃を行っていないか？

-> 他のアプリが奪った特別な権限（管理者，システム）を利用する設計になっていないか？

(d) 違法性：容易に犯罪に利用され得る機能を具備していないか？

❖安全な課金システムの使用

ユーザが安心できる課金システムとして，課金に必要なユーザ情報の安全な管理や，ユーザの不注意によるアカウント情報の漏洩や不正利用が生じた場合の迅速な対応策を備える必要がある．

アプリ（コンテンツ）課金やアプリ内（アイテム）課金については，課金が発生する場合には，毎回ユーザ許諾を得る仕組みを設けるとよい．

❖著作権の適正な管理

開発元や提供元の名称や配信するアプリの名称が，別の事業者やアプリ名称に酷似している，またはユーザを惑わすような紛らわしい名称ではないことを確認する必要がある．イメージ画像やキャラクタについても，別の事業者が著作権を持つ画像やキャラクタに類似したものを持つアプリを配信しないように注意しなければならない．

誰もが行える方法だけで，ユーザ端末側でアプリを抜き取られて複製・実行されないよう，予防措置を持つことも重要である．

❖青少年利用に配慮した運用

青少年が利用することを考慮し，親権者からの同意を得る仕組み，年齢を考慮した閲覧制限や課金上限額の設定などに配慮することも重要である．

❖ユーザからの問合せ窓口の設置

質問，クレーム，不正アプリに関する連絡を受ける窓口を設置する必要がある．その際，窓口の連絡先や連絡方法が分かりやすく明記され，地域に適した言語で対応できることが求められる．

❖開発者へのサポート，注意喚起，啓発

アプリ開発者からの，要望，問合せなどに対応する窓口を設けるのもよい．また，ユーザからの情報や，アプリに関する啓発・教育など，開発者に有益な情報の提供を心がけるべきである．

■ 業界の取り組み

業界横断のフォーラム

日本スマートフォンセキュリティフォーラム（JSSEC）では，アプリ開発者に向けた啓発やアプリ配信サイトの適正な運用について，端末メーカ，通信キャリア，アプリ開発者などの業界横断的なメンバで，本稿で紹介した内容などの協議を行っている．協議の成果については，JSSECのWebサイト[1]を通じた情報公開や，ITU-T☆1などの国際連携を進めていく必要があると考えている．

アプリ販売サイトの取り組み

利便性で注目を集めるAndroidにおいて，先に紹介した取り組みを実践している配信サイトは少ない．そこで，高品質なアプリを安心して取得できる配信サイトを2つほど紹介する．ポイントは，アプリ開発者およびユーザの両者から信頼される配信サイト作りである．

KDDIが運用するau one Marketでは，前述の取り組みを進める中でも，特に研究開発で培ったアプリの攻撃性解析技術[2]を活用した，投稿アプリに対する事前のセキュリティ検査プログラムを設けている．

PlayStation Storeでは，専用端末で培ったプレイステーションクオリティのアプリをAndroid端末に提供するPlayStation Suiteプログラムを実施し，開発者サポートなどを通じて，上質なアプリ配信に向けた取り組みを進めている．

☆1 International Telecommunication Union, Telecommunication Standardization Sector.

参考文献
1） JSSEC, http://www.jssec.org/
2） 磯原，他：セカンドアプリ内包型Androidマルウェアの検知，情報処理学会，CSS2011 3B3-1 (Oct. 2011).

（2012年2月4日受付）

■ **北島 真理子**　Marie.Kitajima@sonyericsson.com
Sony Ericsson（USA）Inc. SCEIにてCell/B.EおよびPS3セキュリティ設計を経て，現在米国でアプリや個人情報運用の研究に従事．