資料1－2

Android端末向け
セキュリティ対策について

2011年2月24日

ソフトバンクモバイル株式会社

SoftBank

ソフトバンクモバイルの取り組み

弊社取り組み

1. アンドロイド端末購入者への
   セキュリティに関する注意喚起
2. アンドロイド端末用セキュリティ対策アプリの提供

1 購入者への注意喚起

Android端末をご購入いただくお客様へお渡しする『ご利用にあたっての注意事項 別紙(SoftBank スマートフォン用)』にて次の通り注意喚起および、すぐに利用できるセキュリティ対策アプリの紹介を行っています。

＜ウイルス対策＞

・SoftBank スマートフォンはインターネットへの接続やメール添付ファイルなどを通じて、ウイルスなどに感染する危険性があります。危険性軽減のためセキュリティソフトのご利用をおすすめします。

＜スマートセキュリティ powered by McAfee®＞

・スマートセキュリティ powered by McAfee® は、お客さまご自身でAndroidマーケットからダウンロードしていただく必要があります。
・スマートセキュリティ powered by McAfee® は、定期的に定義ファイルの更新を行う必要があります。海外で定義ファイルを更新する際は、携帯電話機のデータローミング設定をONにするか、Wi-Fiにて通信を行ってください。
※　データローミングを行った場合、パケット通信料が高額になる恐れがあります。
・スマートセキュリティ powered by McAfee® をインストールしているにもかかわらず万一ウィルス等に感染した場合であっても、当社ならびにマカフィー社は一切の責任を負いません。

2 セキュリティアプリの提供

マカフィー社のセキュリティソリューション「VirusScan Mobile」を弊社向けにカスタマイズした「スマートセキュリティ powered by McAfee®」を提供中です。

提供開始日： 2010年12月10日

月額使用料： スマートフォン基本パック 【498円/月】
スマートセキュリティ powered by McAfee®単体 【315円/月】

※ スマートフォン基本パックは3月末までは無料。
スマートセキュリティ powered by McAfee®単体提供は3月1日より開始予定

機能概要：
- アプリインストール直後のスキャン機能
- microSDカード挿入時のスキャン機能
- メール送受信時のスキャン機能
- 定義ファイルの自動更新機能（日次または週次）
- 定期スキャン機能（日次または週次）
- 手動による定義ファイル更新およびスキャン実施機能

2 アプリダウンロード・インストール導線

SoftBank

アンドロイドマーケットにすぐにアクセスできるよう、メールによりご案内を実施しています。

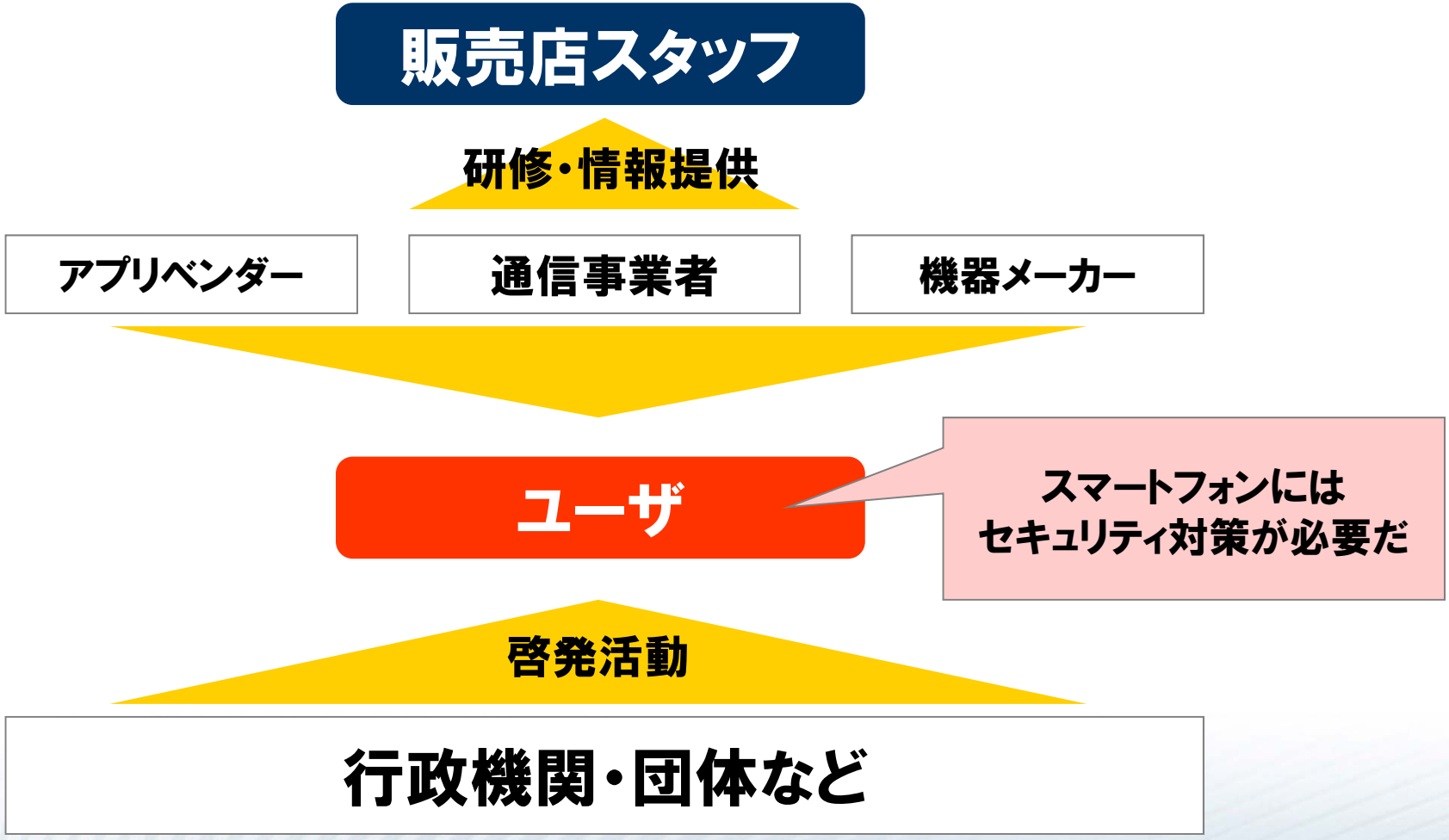
店頭でのコミュニケーション

スマートセキュリティ powered by McAfee®利用開始までの流れを記載したお渡し用チラシを配布。

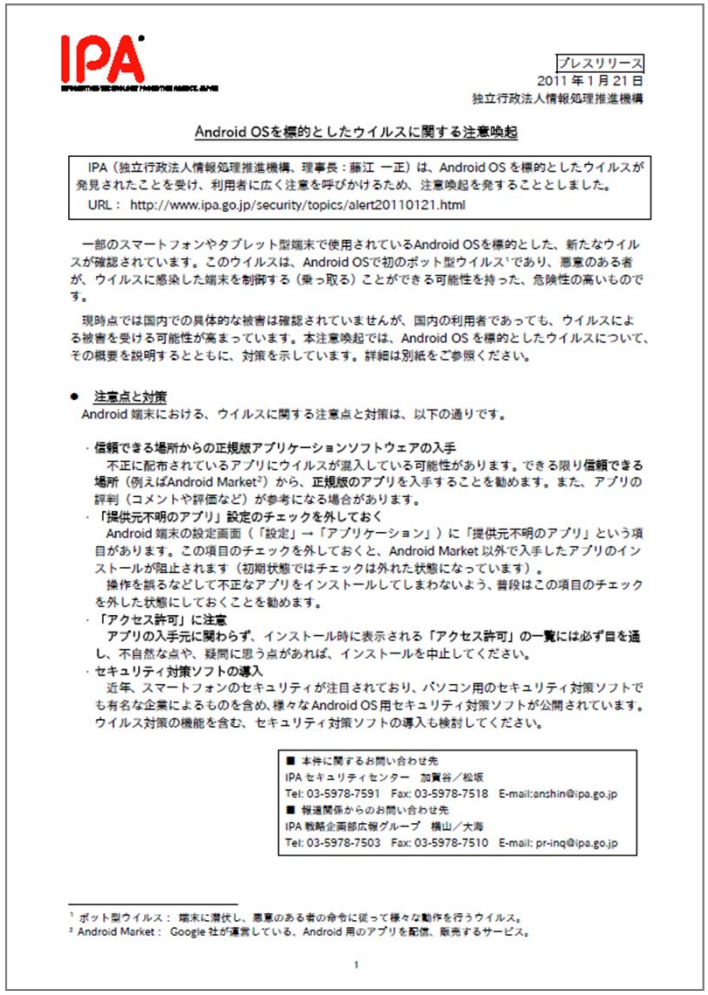
スマートフォンの安全性向上のために

セキュリティ対策の必要性認知の向上

PCと同様にスマートフォンにもセキュリティ対策が必要であることを
社会全体の共通認識とするような啓発活動が必要



【参考】 IPA プレスリリース(1月21日) 他



IPA

プレスリリース
2011年1月21日
独立行政法人情報処理推進機構

Android OSを標的としたウイルスに関する注意喚起

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、Android OS を標的としたウイルスが発見されたことを受け、利用者に広く注意を呼びかけるため、注意喚起を発することとしました。
URL： http://www.ipa.go.jp/security/topics/alert20110121.html

一部のスマートフォンやタブレット型端末で使用されているAndroid OSを標的とした、新たなウイルスが確認されています。このウイルスは、Android OSで初のボット型ウイルス[1]であり、悪意のある者が、ウイルスに感染した端末を制御する（乗っ取る）ことができる可能性を持った、危険性の高いものです。

現時点では国内での具体的な被害は確認されていませんが、国内の利用者であっても、ウイルスによる被害を受ける可能性が高まっています。本注意喚起では、Android OS を標的としたウイルスについて、その概要を説明するとともに、対策を示しています。詳細は別紙をご参照ください。

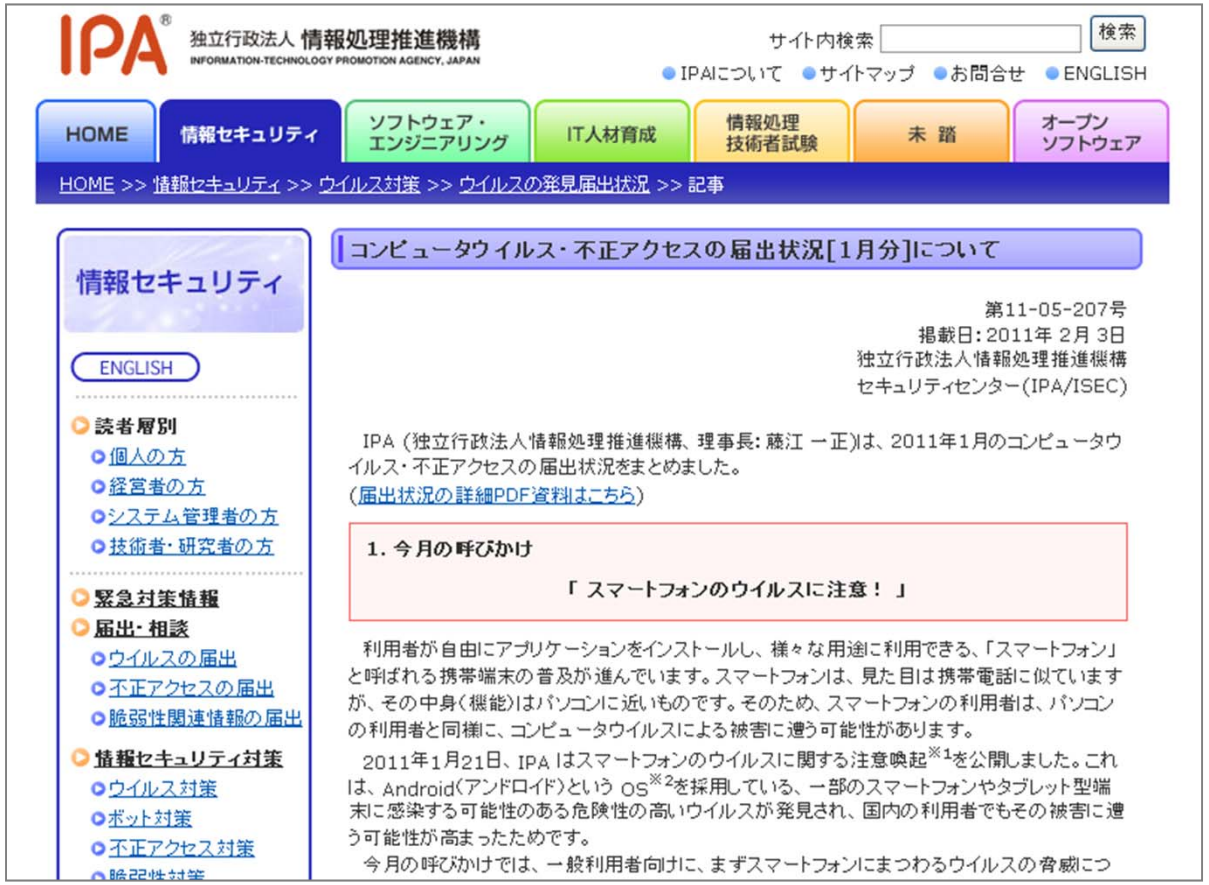
● 注意点と対策
Android 端末における、ウイルスに関する注意点と対策は、以下の通りです。

・信頼できる場所からの正規版アプリケーションソフトウェアの入手
不正に配布されているアプリにウイルスが混入している可能性があります。できる限り信頼できる場所（例えばAndroid Market[2]）から、正規版のアプリを入手することを勧めます。また、アプリの評判（コメントや評価など）が参考になる場合があります。
・「提供元不明のアプリ」設定のチェックを外しておく
Android 端末の設定画面（「設定」→「アプリケーション」）に「提供元不明のアプリ」という項目があります。この項目のチェックを外しておくと、Android Market 以外で入手したアプリのインストールが阻止されます（初期状態ではチェックは外れた状態になっています）。
操作を誤るなどして不正なアプリをインストールしてしまわないよう、普段はこの項目のチェックを外した状態にしておくことを勧めます。
・「アクセス許可」に注意
アプリの入手元に関わらず、インストール時に表示される「アクセス許可」の一覧には必ず目を通し、不自然な点や、疑問に思う点があれば、インストールを中止してください。
・セキュリティ対策ソフトの導入
近年、スマートフォンのセキュリティが注目されており、パソコン用のセキュリティ対策ソフトでも有名な企業によるものを含め、様々なAndroid OS用セキュリティ対策ソフトが公開されています。ウイルス対策の機能を含む、セキュリティ対策ソフトの導入も検討してください。

■ 本件に関するお問い合わせ先
IPA セキュリティセンター 加賀谷／松坂
Tel: 03-5978-7591 Fax: 03-5978-7518 E-mail:anshin@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ 横山／大海
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

[1] ボット型ウイルス： 端末に潜伏し、悪意のある者の命令に従って様々な動作を行うウイルス。
[2] Android Market： Google 社が運営している、Android 用のアプリを配信、販売するサービス。

1



IPA 独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

サイト内検索 検索
IPAについて サイトマップ お問合せ ENGLISH

HOME | 情報セキュリティ | ソフトウェア・エンジニアリング | IT人材育成 | 情報処理技術者試験 | 未 踏 | オープンソフトウェア

HOME >> 情報セキュリティ >> ウイルス対策 >> ウイルスの発見届出状況 >> 記事

情報セキュリティ

ENGLISH

読者層別
- 個人の方
- 経営者の方
- システム管理者の方
- 技術者・研究者の方

緊急対策情報

届出・相談
- ウイルスの届出
- 不正アクセスの届出
- 脆弱性関連情報の届出

情報セキュリティ対策
- ウイルス対策
- ボット対策
- 不正アクセス対策
- 脆弱性対策

コンピュータウイルス・不正アクセスの届出状況[1月分]について

第11-05-207号
掲載日：2011年 2月 3日
独立行政法人情報処理推進機構
セキュリティセンター(IPA/ISEC)

IPA (独立行政法人情報処理推進機構、理事長: 藤江 一正)は、2011年1月のコンピュータウイルス・不正アクセスの届出状況をまとめました。
(届出状況の詳細PDF資料はこちら)

1. 今月の呼びかけ

「 スマートフォンのウイルスに注意！ 」

利用者が自由にアプリケーションをインストールし、様々な用途に利用できる、「スマートフォン」と呼ばれる携帯端末の普及が進んでいます。スマートフォンは、見た目は携帯電話に似ていますが、その中身(機能)はパソコンに近いものです。そのため、スマートフォンの利用者は、パソコンの利用者と同様に、コンピュータウイルスによる被害に遭う可能性があります。

2011年1月21日、IPA はスマートフォンのウイルスに関する注意喚起※1を公開しました。これは、Android(アンドロイド)という OS※2を採用している、一部のスマートフォンやタブレット型端末に感染する可能性のある危険性の高いウイルスが発見され、国内の利用者でもその被害に遭う可能性が高まったためです。

今月の呼びかけでは、一般利用者向けに、まずスマートフォンにまつわるウイルスの脅威につ

【参考】 マカフィー社　ウィルス情報

SoftBank