不正アクセス防止対策に関する官民意見集約委員会（官民ボード）
行動計画宣伝ワーキンググループ企画　座談会

「スマートフォン利用における脅威とその対策とは？」

増加する一方のサイバー犯罪にあって、最近とくに注意が必要とされているのがスマートフォンにおける脅威の拡大です。ここ 1、2 年でスマートフォンは急速にそのシェアを伸ばし、ある調査会社の統計によれば、すでに国内でも携帯電話全体の出荷量の過半数を超えたとされています。この数字は今後、さらに伸びていくでしょう。

利用者が増えれば、犯罪者のターゲットも必然的にそこに移ります。現在、不正アクセス、情報漏えいや改ざん、ワンクリック詐欺、架空請求など、スマートフォンを媒介したサイバー犯罪の報告が急激に増えています。しかもスマートフォンは小型でどこにでも持ち運べるため、盗難/紛失するケースが PC よりも多く、より深刻な脅威となりつつあるのです。

増大するスマートフォンをめぐる脅威に対し、一般ユーザはどのように対応していくことが望ましいのでしょうか。今回、「スマートフォンのセキュリティ」をテーマに、情報セキュリティ業界を代表する有識者の方々にご参加いただき、官民ボード座談会を開催しました。その内容をここでご紹介します。（実施日：平成 24 年 6 月 19 日）

★参加者

・JPCERT/CC(JPC) 理事 真鍋敦士氏
・JPCERT/CC(JPC) 情報流通対策グループ 情報セキュリティアナリスト 熊谷裕志氏
・日本 IBM 経営品質・情報セキュリティ 情報セキュリティ推進室 シニアセキュリティアナリスト 守屋英一氏
・ラック 専務理事 セキュリティ事業本部 セキュリティ技術統括 西本逸郎氏
・産業技術総合研究所(産総研) 高木浩光氏
・日本情報システム・ユーザ協会(JUAS) / 富士ゼロックス 総務部 リスクマネジメントグループ グループ長 神林彰氏
・トレンドマイクロ(TM) コーポレートマーケティング部 セキュリティエバンジェリスト 染谷征良氏
・日本マイクロソフト(MS) チーフセキュリティアドバイザー 高橋正和氏
・トレンドマイクロ(TM) マーケティング本部 森屋幸英氏(モデレータ)
・警察庁 生活安全局情報技術犯罪対策課 情報技術犯罪捜査指導室長 岸田憲夫氏
・警察庁 生活安全局情報技術犯罪対策課 課長補佐 吉田光広氏
・警察庁 生活安全局情報技術犯罪対策課 課長補佐 人見 友章氏

■　スマートフォン利用における脅威の現状

TM 森屋: 本日はお忙しい中、お集まりいただきありがとうございます。今回は「スマートフォンのセキュリティ」をテーマに、業界を代表する有識者の皆さんのご意見を伺っていきたいと思います。本座談会ではひとつの意見に集約することを目的としません。スマートフォンのセキュリティにおけるさまざまな課題を洗い出すことで、一般の人々、とくに技術に詳しくない人々にとっての気づきにつながればと思っています。

まずは現在、スマートフォン利用にはどんな脅威が迫っているのか、その現状を確認していきたいと思います。今日は国内のセキュリティ状況を日々チェックしている JPCERT/CC から 2 名にご参加いただいておりますが、スマートフォンに関するセキュリティインシデントの数は実際、増える傾向にあると言ってもいいのでしょうか。

JPC 熊谷: そうですね。とくに Android のアプリに関する脆弱性の報告が年々増えているのを実感します。

JPC 真鍋: ちょうど 1 年前から急増している感じですね。数だけでなく、その内容も複雑化しています。スマートフォンアプリは PC のアプリケーションのような「1 ベンダ/1 ソフトウェア」という構図から外れるビジネスモデルなので、取り扱いが難しいという面もあります。

TM 染谷: トレンドマイクロはこの四半期(2012 年 1 月－3 月)だけでも 5,000 を超える不正 Android アプリを確認しています。不正アプリの内訳を見ると、不正に金銭を取得しようとするワンクリック詐欺や、正規のアプリに見せかけた偽アプリなどが多く見られます。高額な利用料が発生するサービスに SMS メッセージを送信するタイプの偽アプリも増えています。

MS 高橋: 欧州ではスマートフォンの不正アプリによって銀行口座の預金が盗まれ、数百億円レベルの被害が生じたという事例もあります。日本でも同様のことが起こる可能性は十分にあります。

産総研高木: スマホアプリの問題で難しいのはシロかクロかがはっきりしないものが多いという点です。グレーでもないというところがさらに悩ましい。作成者が悪意をもって作成したウイルスのようなソフトであればクロに分類できますが、「こんな機能があったらユーザにとって便利なのでは」と善意で実装した機能が、電話帳をサーバに送ったり、位置

情報を無断で開示したりする場合があります。ユーザは同意確認したあとにその事実を知ることがほとんどで、「勝手に情報を公開された」と怒る人も少なくありません。このように使い方によって、あるいは人によってシロにもクロにもなるアプリが多く、一概に分類するのが難しい状況にあります。

これらのアプリが怖いのは知らず知らずのうちに自分だけでなく友人などの情報も送信している可能性が高いことです。被害者になるだけでなく、加害者にもなってしまう。一般の人々はそこまで注意がいかないのが実情です。

IBM 守屋: スマートフォンとともに利用者数を伸ばしている Facebook もそうですね。Facebook のアプリは本来必要ない情報を取っていることが多い。しかしスマートフォン上で操作していると、あまりセキュリティなどを意識することなく、流れ作業的に承認ボタンを押してしまいがちです。高木さんが言われたシロ/クロ/グレーで言うならグレーのアプリが非常に多い。Facebook はアプリの拡散が速いので、不用意に渡してしまった情報がどこへ渡るかわからない怖さはあります。それがスマートフォンでさらに加速している感じですね。

JUAS 神林: 一ユーザの立場から言うと、たしかにソーシャルメディアをスマートフォンでぱらぱらと操作していると、不意に何かボタンを押してしまいそうになることはあります。実際、操作した覚えがないのにメールがソーシャルメディア経由で送信されてしまうことが周囲で起きていますから、ユーザが間違ってクリックしてしまう危険性は高いと思います。

TM 森屋: 神林さんは企業ユーザの立場でもあるわけですが、スマートフォンを業務で使うにあたり問題と感じることはありますか。

JUAS 神林: 紛失が心配ですね。これまで、携帯電話は紛失が多いのですが、スマートフォンは PC 並みに情報が蓄積される可能性があるので、被害としてはより深刻です。また、これまで PC では Web アクセスにフィルタをかけたり、インストールするソフトを制限するなど、イントラで端末と情報を守ってきました。それをスマートフォンがすべて壊してしまったとも言えます。携帯電話と同じ頻度で紛失が発生すると、情報漏えいのリスクは頭の痛い問題です。

ラック西本: 私の印象では、企業の経営層にはスマートフォン、とくに iPhone が好きな方が多いですね。なので個人で使用している iPhone や Android を業務にも持ち込もうとするの

ですが、社内の情シスに「セキュリティに問題があるから」と止められるという話をよく聞きます。これはいま流行りの BYOD(Bring Your Own Device: 業務に私物のスマートフォンやタブレットを使用すること)の問題とも絡んでくるのですが、スマートフォンの登場により、情シスがすべての端末を管理するという時代はもう終わったと個人的には感じています。

神林さんが言われたとおり、スマートフォンは"破壊者"です。イントラだけでなく、通信事業者が作り上げてきたフレームも、これまでのアプリケーションビジネスも、さらには医療、教育、金融といった国内法で守られてきた産業も、すべてを破壊するパワーをもっています。現在の国内法ではまだスマートフォンに対してさまざまな規制をかけていますが、段階的に外していかざるを得ないでしょう。最終的には他国と同様にほとんどのビジネスがスマートフォン上で解放されることになるのではないでしょうか。その分、不正プログラムなどのリスクも高まることは必至ですが。

IBM 守屋: 数年前、情報漏えい事件が相次いだとき、その反省から個人のデバイスを業務で使用してはいけないという流れができました。ところが、スマートフォンの登場でそれがまた揺り戻されたんですね。長引く不況もあって、経費削減の観点から個人のスマートフォンを業務で利用することを奨励している企業もあります。当然、それに伴ってセキュリティリスクは高くなっている。情報漏えいしていないかどうかをチェックしようにも、個人のデバイスをどこまでチェックしていいものかという問題もある。このあたりはまったくルール化されていないので、判断が非常に難しいと言えます。

TM 染谷:「スマートフォンの使い方がわからない」、「アプリが何をどうしているのか分からない」、という一般ユーザが大半で、しかもそれを理解するのは難しいのではと感じます。端末上で何が起こっているか、利用者には見えにくく、注意事項を読んでもわかりにくい。この不透明さが問題をさらにややこしくしているのではないでしょうか。

■　脅威から見えてくるスマートフォン利用の課題

TM 森屋: ひととおりスマートフォンのセキュリティをめぐる現状を挙げていただきましたが、もう少し議論を進めて、脅威に対する課題と考えられる対策を洗い出していきたいと思います。PC のソフトウェアベンダでセキュリティに関わっている高橋さんや染谷さんから見ると、スマートフォンの問題点はどこにあると思われますか。

MS 高橋: スマートフォンは"多様化"しすぎている、一言で言うとこれに尽きます。iPhone と Android という違いだけでなく、Android に至っては OS のバージョンごとによって機

能や動作がまったく異なる。したがってアプリを動かすためのドライバもすべて違ってくることになります。デバイスの種類だけ、アプリやドライバが存在し、さらにそれに紐付いた不正アプリが増えるという図式です。

TM 染谷:スマートフォンを利用した SNS 経由での情報流出の危険性も訴えたいですね。SNS 利用者が悪意はないものの、能動的に情報を外に発信していることにもうすこし気づくべきだと思います。とくに同意のない他人の顔写真や情報の公開はプライバシーという観点で問題です。

JPC 真鍋: スマートフォン以前は携帯電話のほとんどが国産で、たとえセキュリティに対する問題が発生しても国内でほとんどの場合、原因を特定して解決することできました。ところがスマートフォンはメジャーな 2 つのプラットフォームが海外製です。問題が発生しても、その原因は端末自体なのかアプリなのか、それとも回線の向こう側にあるクラウドにあるのかがわかりにくくなっています。

また、IT に詳しくないスマートフォン利用者が増えたことで、新たな問題も起こり始めています。たとえば IT に詳しくない人は「アドレス帳の同期」と言われても何のことだか意味がわからない。その程度のことも認識せずに使っている利用者が非常に多いのです。この"認識の欠如"は大きな課題だと言えます。

警察庁岸田: アプリの安全性を標準化するような動きは民間では起こってないのでしょうか。iPhone アプリに関しては Apple が審査していますが、Android アプリのレピュテーション(評価)システムがあれば、一般市民にとってはとてもありがたい存在になると思うのですが。「このアプリはこのくらい安全です」と言ってもらえるとスマートフォンアプリに対する信頼感も上がるように思います。

MS 高橋: パブリックなレピュテーションシステムは良い案だと思います。ただし、一般利用者からの報告をどのように受け付けるか、その線引きは難しいでしょうね。

ラック西本: あとは誰が評価を下すか、という点も大きな課題ではないでしょうか。

TM 染谷: 国内にも多くのアプリマーケットがあるだけでなく、海外発のアプリも多いので、海外のアプリマーケットともどう連携するかも課題になるかと。当社(トレンドマイクロ)のようなセキュリティベンダが、アプリの評価をしたりマーケットプレイスの運営を支援するというのも良いのかもしれません。

産総研高木: 個人的にはアプリのレピュテーションは非常に実現が難しいと思います。理由は、先ほども申し上げたように、たとえ一見セキュリティに問題がないアプリでも、使い方によってクロになるアプリが少なくないからです。たとえば小さな子供の行動をチェックするために母親が子供のスマートフォンに行動を監視するアプリを入れる。これは OK です。しかし同じアプリを自分の夫のスマートフォンにこっそり入れた場合はどうか。これはもう完全に真っ黒な使い方です。使い方まで含めたレピュテーションはかなり困難と言わざるを得ないでしょう。セキュリティにおいて、ブラックリストではなくホワイトリストを作成するというのは本当に難しいのです。

TM 森屋: スマートフォン上での詐欺行為対策についてはいかがでしょうか。どんな課題があると思われますか。

MS 高橋: スマートフォンがこれまでの携帯電話とも PC とも大きく違うのは、カメラと通信機能とアプリ、そして SNS がひとつのデバイスに載っているというところです。そういうデバイスを触っていると、魔が差しやすくなる。よくネット上で話題になる"炎上"といわれる騒動も、魔が差すことで起こりやすくなる。臨場感のある世界が突然ひらける感じですね。詐欺に巻き込まれるときも同じく、ふと魔が差してクリックしてしまうことから始まります。対策としては"よく見る習慣をつける"、これが最善ですね。

TM 染谷: ソーシャルエンジニアリングのような「美味しい話には気をつけよう」という原則はスマートフォンの世界でも同じです。今のままの流れが進めば、これまで PC の世界で起こっているアドウェア、スパイウェアといった問題や、美味しい話に便乗して不正プログラムを配信するような脅威がスマートフォンでも同様に確実に増えると感じています。

IBM 守屋: Facebook で表示される広告にも詐欺まがいのものがあるので注意が必要です。一般の人は「Facebook というパブリックな場に掲載されている広告だから、審査を通っているはず」と考えます。ところが実際には審査を通っていない。それを知らずにクリックすることで"ドライブバイダウンロード(Drive by Download: 利用者が気づかないうちにマルウェアをインストールさせられていること)"に感染するおそれもある。しかも Facebook には行動ターゲティング広告が採用されていますから、利用者がクリックして詐欺に巻き込まれる可能性も高くなっています。

産総研高木: 偽アプリの台頭もかなり悩ましい課題だと言えます。基本的に PC を中心とした Web の世界はセキュリティを厳しくする方向に向かっていました。ところがスマートフォンによってアプリのセキュリティレベルが微妙に退行している感を受けます。これによって偽アプリが増える下地ができてしまった。偽アプリは確認が非常に難しく、やっかい

な存在です。銀行口座を乗っ取るような悪質なものが出てきてもおかしくない状況にあります。産総研は偽アプリの被害が今後は拡大するのではと見ています。

■　求められるスマートフォンのセキュリティ対策

TM 森屋: ここまでで非常に有意義な意見がたくさん得られました。議論の最後に、皆さんから一般の方々に向けて、スマートフォンのセキュリティへの脅威に関して、一言ずつメッセージをいただければと思います。

MS 高橋: 私は大きく 4 つのポイントで気をつけてもらいたいと思っています。その 4 つとは、プライバシー、マルウェア、偽アカウント、(ネット上での)不適切な発言です。この 4 つが実生活に入り込むとどんな影響を及ぼすのか、マイクロソフトとしても具体的な形で伝えていこうと思っています。

JUAS 神林: スマートフォンにはいままでの携帯電話とはケタ違いの情報量が格納されていることを強く認識してほしいです。現在、PC のデータがどんどんスマートフォン上に移動しています。紛失/盗難という事態になれば、その被害は携帯電話の比較ではありません。持ち歩く必要のない情報は都度削除し蓄積しない等、なくなることを前提にリスク管理をするということが必要だと思いますが、もっと身近なところで言えば、たとえばスマートフォンベンダはストラップを付けられるようにするとか、そういう小さな工夫にも目を配ってもいいのではないでしょうか。

TM 染谷: ごく一般的なことになりますが、セキュリティソフトはスマートフォンにも必ず入れてください。そして"美味しい話"にはくれぐれも気をつけて。残念ですが不正アプリは今後もなくなることはありません。怪しいアプリ、信頼できないところからのアプリにはむやみやたらに手を出さないようにしてほしい。セキュリティベンダとして、トレンドマイクロも引き続きこの部分を啓発していきます。

IBM 守屋: Facebook はデフォルトの設定が"公開"です。これはこれまでの日本人の感覚と大きく異なります。事前に審査するのではなく、何かが起こったら利用者が申告する仕組みです。その部分のリスクをよく認識するべきです。ただ、最近は携帯電話の番号を Facebook 上で平気でオープンにしているような若い人を見ることが増えてきました。まだ被害に遭ってないからなのでしょうが、個人的には非常にリスクが高いと感じています。

ラック西本: 一般の方には「犯罪に加担しないで、被害に遭わないで」とアプローチしています。今日の議論でも出てきましたが、知らないうちにただの利用者から被害者に、そし

て加害者になってしまうケースが増えています。ラックとしても注意喚起を引き続き促していきます。

産総研高木: 提供元が不明のアプリを使うことはやめたほうがいいでしょう。あとはパーミッションもよく読むべきです。そして、アプリベンダに不快な思いをさせられたら、たとえばアドレス帳の送信などを勝手にされたのなら、きちんと声をあげてほしい。声を上げて糾弾することを苦手にしている日本人は多いですが、「そんなもんなのかな」と納得したりせず、きちんと怒るべきです。それがスマートフォンのセキュリティの向上にもつながります。

警察庁岸田: 非常に有益な議論ができたことを感謝します。本日はありがとうございました。

以上