スマートフォン情報セキュリティ最前線 ～業界の最新動向と今後の方向性～

総務省　情報流通行政局 情報セキュリティ対策室　課長補佐　中谷（なかたに）　純之（じゅんじ）

1．はじめに

2005年当時、第3世代の携帯電話（3G）を高速化する3.5世代の携帯電話[1]の技術基準を担当していた頃の著者は、正直、情報通信ネットワークの「土管」ばかり大きくしても、そこを流れるコンテンツや有効に活用する利用シーンが果たして現れるものかどうか、幾ばくかの違和感を覚えていた。ところが、この不安は幸いなことに見事に裏切られた。ひとたび「箱」ができてしまえば、それを活用して何か面白いことをしてやろうと人類が試みるということが、スマートフォンの台頭により再び証明されることになった。

2．スマートフォンの台頭と課題

スマートフォンは、従来の携帯電話とPC双方のメリットを兼ね備えた存在として利用者が増加しており、国内出荷台数は平成23年度2,417万台で、前年度比2.8倍、携帯電話端末の国内総出荷台数の56.6%を占めるに至っている（**図1**）。また、アプリケーションなどの領域を含め成長の著しい分野であり、その普及速度は、固定電話や携帯電話、インターネットの場合より大きい（**図2**）。

この場で改めて申し上げるまでもなく、様々な場面におけるスマートフォンの利活用への期待が高まっている。他方で、急速な普及による市場の拡大に伴い、スマートフォンをターゲットとしたマルウェア[2]が出現している。発見されているマルウェアの多くはAndroidを対象としたものであり、2012年後半から増加幅が拡大している（**図3**、**表1**）。

本稿では情報セキュリティについて論じるが、スマートフォンは、情報セキュリティに限らず関連する産業構造の激変や文化的影響にも波紋を投げかけている存在である。そのため、スマートフォンの急速な普及に遅れを取ることなく、情報セキュリティ確保のための検討や必要な方策に加え、社会的な受容性[3]に関する議論を推進していくことが重要ではないだろうか。

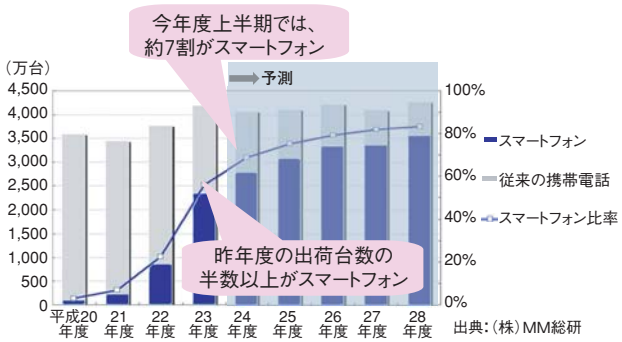
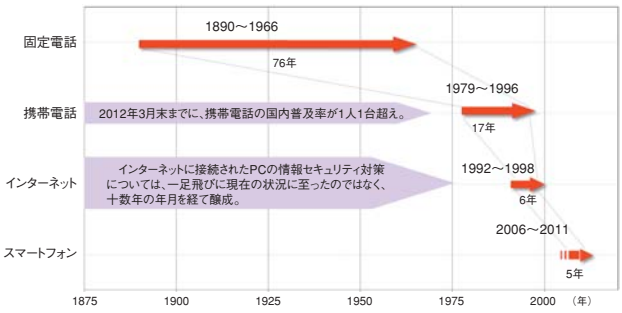


図1．国内の携帯電話端末の出荷台数



※　総務省「通信利用動向調査」及び「国勢調査」並びにNTT東日本「加入電話の推移」を基に演者が作成（固定電話及びインターネットは世帯普及率）

図2．我が国における新サービス開始から国内普及率が1割を超えるまでの期間

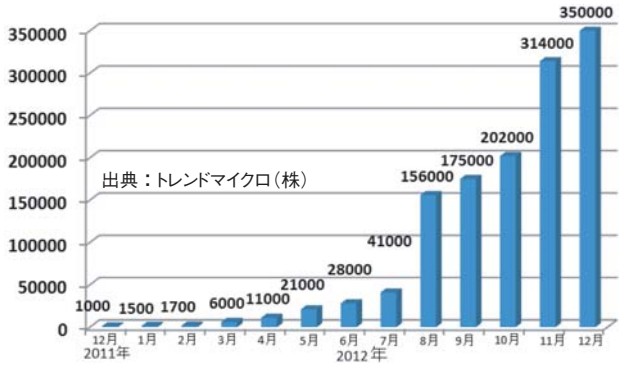


図3．Androidを対象としたマルウェアの件数（累計）

3．「スマートフォン・クラウドセキュリティ研究会」

総務省は2011年秋、著者が事務局の一員を務める「スマートフォン・クラウドセキュリティ研究会」（座長：山口英奈良先端科学技術大学院大学 教授）を立ち上げ、スマートフォンの情報セキュリティ上の脅威の洗い出しから議論を開始し、OS[4]、アプリケーション、通信路、端末内データ等に関する課題として整理した（**図4**）。

抽出された課題それぞれに対して、実施又は積極的な検

表１．マルウェアの事例

発見年月	名称	OS	概　要	備　考
平成21年11月	ikee	iOS	JailbreakしたiPhoneに感染し、勝手に壁紙を変更するワーム。	
平成22年8月	FakePlayer	Android	Androidを狙った初めてのマルウェア。ロシアのプレミアムSMSに勝手に送信する。	当該SMSには、ロシア国外からは送信できない。
平成22年12月	Geinimi	Android	Androidを狙った初めてのボットウイルス。インストール後、端末内の情報を収集し、サーバからの指令を待つ。	有料アプリケーションの海賊版に、このマルウェアを埋め込み配付。日本語版アプリケーションも存在。
平成23年2月	DroidDream	Android	OSのぜい弱性を突き、管理者権限を奪取するボットウイルス。起動時に、定期的にサーバと通信し、コマンドやアップデートを実行する。	有料アプリケーションに埋め込み、無料アプリケーションとして配付。Android Market（現Google Play）で提供するアプリケーションの中からも検出。
平成23年5月	Lightdd	Android	アプリケーション起動なしに端末を監視し、着信や受信、通話の終了などの際に悪性コードを実行し、外部に情報を送信する。	Android Market（現Google Play）で提供するアプリケーションの中からも検出。
平成24年1月	FakeTimer	Android	電話番号やメールアドレス等を外部に送信するとともに、これらの情報とともに架空の利用料金を請求するポップアップを画面に表示させる。	日本のワンクリック詐欺サイトで用いられ、アクセスすると動画を再生するアプリケーションと称して、端末内にインストールを促す。6月、警視庁は都内のIT関連会社役員らを、不正指令電磁的記録供用（ウイルス供用）と詐欺の疑いで逮捕。
平成24年4月	the Movie	Android	利用者の電話帳に登録された個人名や電話番号、メールアドレスなどの情報を外部に送信する。	警視庁は5月、IT関連会社などを、ウイルス供用容疑で家宅捜索。10月には同容疑で元経営者らを逮捕。その後、東京地検は、11月に処分保留で釈放、12月には不起訴。

（総務省調べ）

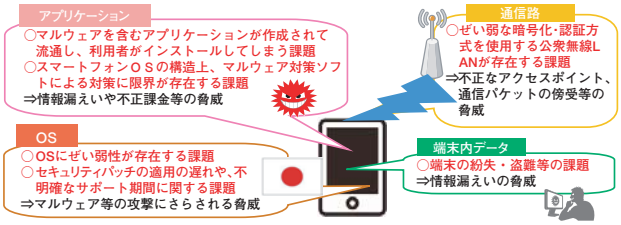


図４．我が国における脅威及び課題のうち主なもの

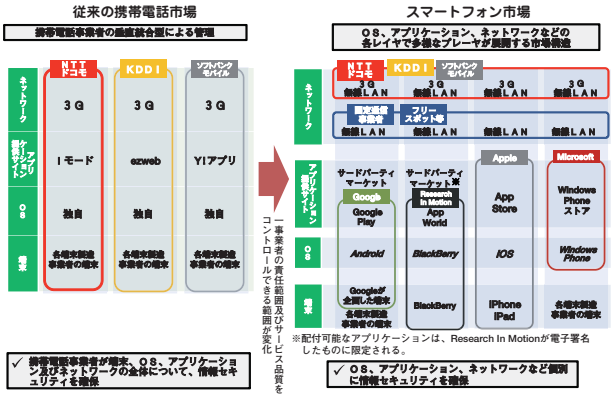


図５．我が国の携帯電話市場に起こったパラダイムシフト

討が望まれる対策に関する議論を行ったわけであるが、従来の携帯電話における対策との違いの一つに、対策を講ずべき主体の違いが挙げられる。従来の我が国の携帯電話は、携帯電話事業者が、情報セキュリティの確保を含めサービス全体を一元的に企画・設計・運営・管理してきたところ、今次のスマートフォンの台頭により、このサービス提供構造に変革が起きた（**図5、表2**）。

このパラダイムシフト等の環境変化を踏まえ、研究会がどのような議論の末に最終報告[5]に至ったのかについては、別の機会[6]に委ねることにし、本稿では、事業者、利用者及び政

表２．OS別の市場展開の状況

OSの種類	OS提供事業者	特　　徴
Android	（米）Google	○OS、端末及びアプリケーション提供サイトを水平分業型で展開しているため、複数事業者が、端末の製造、アプリケーション提供サイトの運営等に参入している。 ○オープンソースのOSであるため、端末製造事業者によるカスタマイズの自由度が高い。そのため、OSのバージョンが同一でも、機種に依存した動作を行うことがある。
BlackBerry	（加）Research In Motion	○基本的には、OS、端末及びアプリケーション提供サイトを垂直統合型で展開しているため、端末の製造は、OS提供事業者のみが行っている。 ○アプリケーション提供サイトの運営については、同社が電子署名したアプリケーションに限り、OS提供事業者以外の事業者が提供を行うことが可能である。
iOS	（米）Apple	○OS、端末及びアプリケーション提供サイトを垂直統合型で展開しているため、端末の製造及びアプリケーション提供サイトの運営をOS提供事業者のみが行っている。
Windows Phone	（米）Microsoft	○OS及びアプリケーション提供サイトを垂直統合型で展開しているため、アプリケーション提供サイトの運営を、OS提供事業者のみが行っている。 ○端末の製造は、水平分業型で展開しているため、複数事業者が参入している。（国内では現在1社）

（総務省調べ）

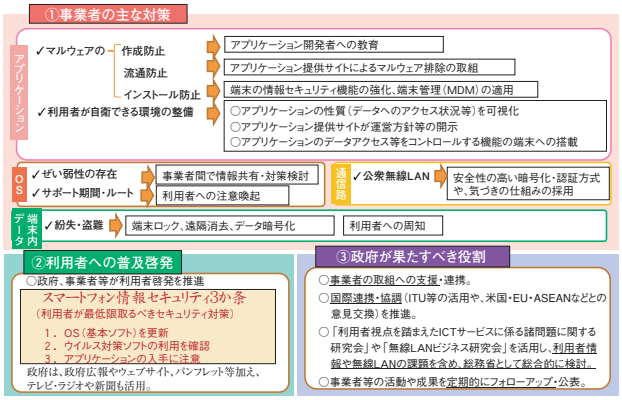


図６．研究会最終報告で提示した実施主体ごとの対策

府それぞれの役割を明確化した対策（図6）を示すに留め、その後の動向や取組、方向性に話を移したい。

4．研究会の最終報告取りまとめ後の動向・取組・方向性

4.1　「スマートフォン情報セキュリティ3か条」の周知

研究会の検討結果である最終報告は、あくまでサービス提供者側が取り組むべき方策を取りまとめたものであるが、利用者に最低限守っていただきたい事項を取りまとめた「スマートフォン情報セキュリティ3か条」[7]という国民への周知啓発ツールを含んでいる。このツールを活用し、総務省としては、ウェブサイトや広報誌、セミナーといった従来型の方法に加え、様々な年齢層・利用者層に効果的に訴求していくため、ラジオやインターネットテレビ、新聞記事や突出し広告等様々なマスメディアを駆使している[8]ほか、携帯電話事業者においても、「3か条」をパンフレットに掲載するなど、産官が協調して周知啓発に取り組んでいる。

4.2　「無線LAN情報セキュリティ3つの約束」の策定・周知

スマートフォンの普及に伴う通信量の増大（図7）により、

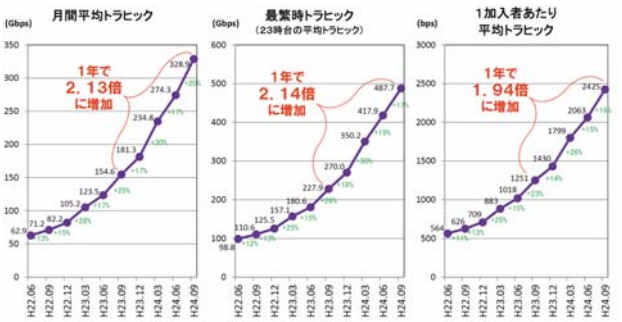


図７．携帯電話のデータ通信量の急速な増加

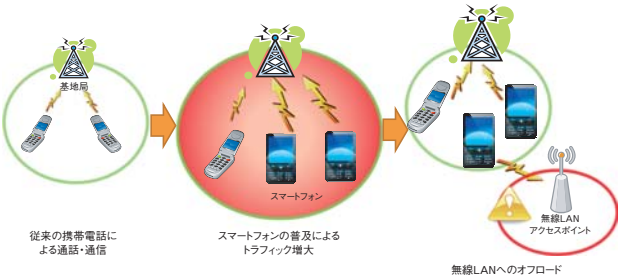


図８．スマートフォンの無線LANへのオフロード

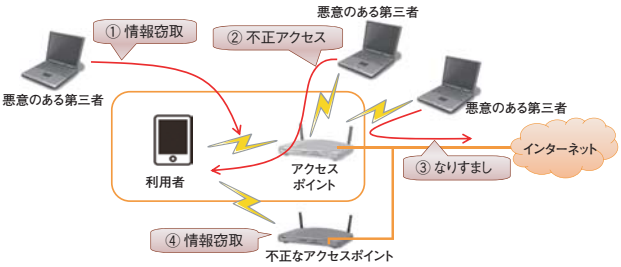


図９．無線LANの情報セキュリティ上の主な脅威

携帯電話事業者のネットワークがひっ迫している。そのため、携帯電話網から無線LANへのオフロード（図8）が進展しつつある。

ところが、無線LANには、一般に、①無線LAN区間における情報窃取、②他の端末からの不正アクセス、③利用者端末へのなりすまし、④不正なアクセスポイントによる情報窃取といった情報セキュリティ上の脅威が存在する（図9）ことから、総務省として、一般利用者が最低限取るべき情報セキュリティ対策として取りまとめた「無線LAN情報セキュリティ3つの約束」を含む一般利用者向けの手引書[9]を策定し、ラジオ等の政府広報や広報誌、新聞記事、セミナー等による周知を実施している。

なお、企業等の組織が無線LANを導入・運用する際の情報セキュリティ対策に関する手引書「企業等が安心して無線LANを導入・運用するために」も、2013年1月に取りまとめた[10]。

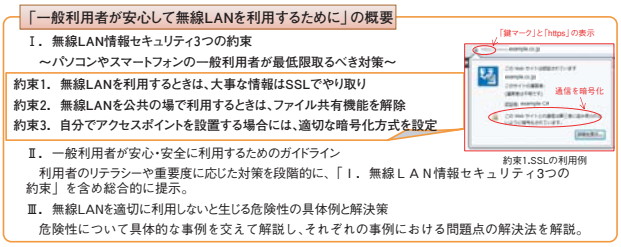


図10．無線LANの一般利用者向けの手引書

4.3　その他の動向と今後の方向性

研究会の最終報告に掲げられている対策の幾つかについては、実際に携帯電話事業者やOS提供事業者、業界団体等において実行に移されている。

例えば、アプリケーションごとに、データ・デバイスへのアクセスをOS側で制御[11]又は可視化[12]する機能が提供されるようになった。また、OSベンダにより、端末内におけるシステム権限によるマルウェアチェック機能が提供される、携帯電話事業者が提供する無線LANアクセスポイントにEAP-SIM/EAP-AKAなる強固な相互認証方式が採用されるなどの取組も進展している。さらに、一般社団法人日本スマートフォンセキュリティ協会（JSSEC）[13]において、OS等のぜい弱性について情報共有を行うとともに、外部の団体やOSベンダ、端末ベンダへの報告を行うなど、事業者団体における事業者連携が進展している。

アプリケーション提供サイトには、様々なものがあり、それぞれにおいてマルウェア排除の取組の継続・改善がなされている（**表3**及び**表4**）。利用者視点に立てば、サイトによらず、アプリケーション掲載の最低限の基準が可能な限り統一されていくことが望ましい。その意味で、例えば、社団法人電気通信事業者協会において、アプリケーション提供サイト運営者向けガイドラインの検討が進展していることから、携帯電話事業者が運営するアプリケーション提供サイトに対する安心感が醸成されることが期待される。

マルウェアとは別の課題であるぜい弱性を含むアプリケーションについては、現時点において大きなリスクとはなっていないものの、PCがたどってきた歴史や現在置かれている状況に鑑みれば、当該アプリケーションが攻撃者によって悪用されるという脅威が顕在化することを念頭に置くべきではないだろうか。しかしながら、ぜい弱性を含むアプリケーションは、作成後に第三者が当該ぜい弱性を発見することが技術的に高度でコストもかかることもあり、まだ対応が十分になされているとは言えない。そのため、広くアプリケーション開発者への啓発活動を行うとともに、アプリケーション提供サイト運営者において、JSSECが策定している開発者向けのセキュア設計・コーディングガイド（2012年6月、11月改訂[14]）、その他当該アプリケーション提供サイト運営者が用意するガイドを開発者に提示し、アプリケーションの作成段階という「入り口」で対処することが、現実的かつ効果的な方法であると考えられる。

いずれにしても、図2で示したように、サービス開始からたった時間からすれば、スマートフォンはまだ黎明期にあるとも言える。そのため、スマートフォンを取り巻く環境は日々変化しており、産学官連携、さらにはITUの場を活用するなどして国際的にも協調・連携し、脅威や課題に関する情報収集・共有を行い、対策について不断の検討を行っていくこ

表３．OS提供事業者が運営するアプリケーション提供サイトの概要

アプリケーション提供サイト			提供アプリケーション						
					掲載ポリシー				
					一般への公開		掲載時	掲載後	
運営者	名称	種別	提供対象	登録数	利用者向け	開発者向け	ポリシー違反の確認方法	ポリシー違反の検知	ポリシー違反判明時の対応
Google	Google Play	アプリケーション配信	Android端末	70万以上（平成24年10月）	○	○	アップロードされるとすぐに、アプリケーションを以下の方法で確認。 （1）開発者が過去にマルウェア等を配付していないか確認。 （2）静的解析により、既知マルウェアの検出。 （3）実行させその挙動を解析。	アプリケーションを随時自動チェックと、開発者及び利用者からの報告を基に調査。	アプリケーションの種別や違反内容に応じて、開発者への注意喚起や提供サイトからの削除など。
Research In Motion	BlackBerry World	アプリケーション配信	BlackBerry端末	約12万（平成24年11月）	×	○（英語）	掲載前に、アプリケーションの審査により確認。（審査方法は非公開）	利用者等からの報告を基に調査。	同上
Apple	App Store	アプリケーション配信	iPhone端末※1 iPad端末※1	約77.5万（平成25年1月）	×	×※2	掲載前に、アプリケーションの審査により確認。（審査方法は非公開）	人手によるアプリケーションの巡回チェック、開発者及び利用者からの報告を基に調査。	同上
Microsoft	Windows Phone ストア	アプリケーション配信	Windows Phone端末※1	約12万（平成24年10月）	×	○	掲載前に、公開されている要件をチェックリストとして人手による確認を行い、要件に適合しない場合には申請者にその理由や再現方法を記述したドキュメントを返信する。	開発者及び利用者からの報告を基に調査。	同上

※1　他のアプリケーション提供サイトからのインストールが不可。
※2　公開しているが、閲覧には開発者アカウント（有料）が必要。

（総務省調べ）

表４．携帯電話事業者が運営するアプリケーション提供サイトの概要

アプリケーション提供サイト			提供アプリケーション						
運営者	名称	種別	提供対象	登録数	掲載ポリシー				
					一般への公開		掲載時	掲載後	
					利用者向け	開発者向け	ポリシー違反の確認方法	ポリシー違反の検知	ポリシー違反判明時の対応
NTTドコモ	dマーケット	アプリケーション紹介	NTTドコモのAndroid端末	約1,000（平成24年12月）	×	×	掲載前に、人手によりアプリケーションを実行させて、動作を目視で確認。	人手によるアプリケーションの巡回チェック、及び利用者からの報告を基に調査。	提供サイトから削除。
	dメニュー	アプリケーション提供サイトの紹介	NTTドコモのAndroid端末	約6,300サイト（平成24年12月）	×	○	アプリケーション提供サイトの運営者が掲載ポリシーの説明に同意したことを確認し、同者の企画書を審査。	人手によるアプリケーションの巡回チェックと、ドコモあんしんスキャンによるウイルスチェック、及び利用者からの報告を基に調査。	アプリケーションの種別や違反内容に応じて、開発者への注意喚起や提供サイトからの削除など。
KDDI	au Market	アプリケーション配信	KDDIのAndroid端末	約8,500（平成25年1月）	×	○	アプリケーションを以下の方法で確認。 (1) 機能の自動解析 (2) 人手により実行させ、挙動記録を解析。 (3) 情報漏えいや不正課金につながる可能性がある場合には、アプリケーションから利用者へ提示される説明や許諾の妥当性を目視で確認。	(A) 利用者からの申告。 (B) 解析パターンファイル更新時に、掲載中の全アプリケーションに対して左記（1）の実施、掲載前に収集した左記（2）（3）の記録を再評価。	危険性が大きい場合、アプリケーション開発者に通知後、当該アプリケーションの配信を停止し、必要に応じて利用者へ連絡（これまで該当なし）。 危険性が小さい場合、アプリケーション開発者に修正を依頼し、差替え。
ソフトバンクモバイル	メニューリスト	アプリケーション及びウェブサイトの紹介	ソフトバンクモバイルのAndroid端末	約1,000（ウェブサイトを含む）（平成25年1月）	×	×※	アプリケーションを以下の方法で確認。 (1) アプリケーション開発者が掲載ポリシーの説明に同意したことを確認。 (2) 人手により申請内容に合致しているかを確認。	人手によるアプリケーションの巡回チェック、及び利用者からの報告を基に調査。	提供サイトから削除。

※　同社の規定する「プロバイダー向け機密情報開示申込規約」に同意し、同社からアカウントを発行した開発者のみ閲覧可能

（総務省調べ）

とが重要になってくる。

5．むすび

最後に、著者なりの考えを書かせていただき、本稿を締めくくることにする。実態を持つ「モノ」では、紛失や盗難により、所有者はその価値を失うとともに、そのモノを拾った又は盗んだ者に当該モノの価値が移転する。ドイツの思想家ヴァルター・ベンヤミンになぞらえて表現するなら、「モノ」はアウラ[15]の宿る絵画であるのに対し、「データ」はアウラの宿らない写真である。アウラなき「データ」が物理的な壁を越えて容易に複製・共有されることで、情報通信社会は加速度的に進化した。今後は、スマートフォンを利用する際にも、毀損して又は改ざんされて使えなくなると不都合が生じる情報[16]からなるデータと、意に反して複製され又は漏えいすると不都合が生じる情報[17]からなるデータとに区別して考える必要があるのではないだろうか。

また、スマートフォンを含むICTの利用者が、情報セキュリティを理解・意識せずに情報通信サービスを利用できた時代は、過去のものとなりつつあるのかもしれない。それとも、今やICT機器と化した自動車は、よほどの車好きでなければ利用者が修理をすることが困難であるが、ガソリンスタンドに持ち込めば専門家が点検・修理をしてくれるのと同じように、情報セキュリティのワンストップサービスが普及していくのだろうか。情報セキュリティを取り巻く世界がどのようなに変貌していくのかを見通せるわけではないが、その未来が少しでも明るいものとなるよう、今後とも汗を流していきたい。

註：本稿中、意見や推測にわたる部分は筆者の個人的見解であり、所属元や研究会の見解を代表・表明するものではない。

注

1　3.5世代の携帯電話では、余剰の拡散コードや送信電力の活用、変調方式の多値化により、3Gよりも高速なデータ通信速度を実現している。HSDPAやEV-DOなどの方式がある。

2　マルウェアとは、malicious softwareの短縮された語で、コンピュータウイルスのような有害なソフトウェアの総称。情報セキュリティ事業者により、定義や呼称は異なる。なお、刑法において、不正指令電磁的記録（人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録）の作成・供用等が禁止され、処罰の対象となっているが、刑法の謙抑主義・断片主義に則れば、スマートフォンのマルウェアと呼称されるアプリケーションやプログラムのすべてが、直ちに不正指令電磁的記録となるわけではない。

3　「スマ歩」が社会問題化しつつあるが、そのほかにも多くの課題を抱えている。ビジネスにおける打合せや会議の最中に、携帯電話等の着信音を鳴らすのは論外として、そもそも電話に出ることを疑問なしによしとすべきなのだろうか。友達とお茶をしている時や、彼氏とデートをしているのに、お互いの視線を自らの携帯電話に向けているのは自然なことだろうか。電車内で、堂々と通話するのは論外として、いつから、優先座席付近で、携帯電話の電源を付けておいてよくなったのか。これら武士道に反する振舞いは、従来の携帯電話でも「問題」となっていたことではあるが、スマートフォンの台頭により、助長されているきらいがある。

4　図4中にある「セキュリティパッチの適用の遅れ」とは、OS提供事業者から発行されたセキュリティパッチが、端末製造事業者による組込みや、携帯電話事業者による検証が必要となるため、利用者への提供に遅れが生じている事象を指す。特に我が国において、顕著な課題であると考えられる。

5　「スマートフォンを安心して利用するために」（スマートフォン・クラウドセキュリティ研究会編、クリエイト・クルーズ、2012）

6　例えば、一般財団法人ITU協会発行のNew Breeze Vol. 24 No. 4 Autumnにおける拙著（What Must be our Stance Toward Smartphones? ～Reflections from the “Study Group on Information Security Issues of Smartphone and Cloud Computing”～）がある。

7　「スマートフォン情報セキュリティ3か条」（http://www.soumu.go.jp/main_content/000139824.pdf）

8　政府広報の例として、ラジオ番組（http://www.gov-online.go.jp/pr/media/radio/bj/sound/20120728.html）、政府インターネットテレビ（http://nettv.gov-online.go.jp/prg/prg6690.html）、政府広報オンライン（http://www.gov-online.go.jp/useful/article/201207/2.html）がある。そのほか、総務省の周知啓発の取組として、総務省広報誌に特集（http://www.soumu.go.jp/menu_news/kouhoushi/koho/1202.html、http://www.soumu.go.jp/menu_news/kouhoushi/koho/02koho03_03000164.html）を組むほか、情報セキュリティ月間（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000017.html）等における講演、国内の頒布物や英文ジャーナルへの投稿等を実施している。

9　「一般利用者が安心して無線LANを利用するために」（総務省）（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000029.html）

10　「企業等が安心して無線LANを導入・運用するために」（総務省）（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000035.html）

11　iOS6では、位置情報サービス、連絡先、カレンダー、リマインダー、写真にアクセスするアプリケーションやシステムサービスを表示及び制御可能。（http://manuals.info.apple.com/ja_JP/iphone_user_guide_j.pdf）

12　NTTドコモの「個人データ確認支援（プライバシーチェック）」では、インストール済みアプリを対象に、個々のアプリがどのような個人データを取得しているのか一覧し、再確認することなどが可能（http://www.nttdocomo.co.jp/service/safety/docomo_anshin_scan/privacy_check/index.html）。また、KDDIでは、アプリケーションが収集し利用する可能性のある端末情報や個人情報について、そのリスクとともに表示する「プライバシースキャン」を提供予定。

13　一般社団法人日本スマートフォンセキュリティ協会は、スマートフォンの安全な利活用を図り普及を促進するために、スマートフォン関連企業等により設立された任意団体「日本スマートフォンセキュリティフォーラム」から、2012年4月に改組した。

14　「Androidアプリのセキュア設計・セキュアコーディングガイド」（JSSEC）（http://www.jssec.org/report/20121119_securecoding.html）

15　アウラ（aura）は、絵画や彫刻など、印刷、写真、データコピーなどによる複製で完全に同じものを作れない芸術作品に宿るとされるもの。ラテン語（英語のオーラの語源）に由来する。

16　機密性よりも、可用性・完全性が優先される情報。例えば、思い出の写真や、後で見ようと録画しておいたお気に入りのテレビ番組が該当すると考えられる。

17　機密性が、可用性・完全性よりも優先される情報。例えば、ID・パスワードや決済関連の情報、プライバシー性の高い情報が該当すると考えられる。