別紙

スマートフォン・クラウドセキュリティ研究会　中間報告

～スマートフォンを安心して利用するために当面実施されるべき方策～

平成２３年１２月１９日

目　　次

はじめに

情報セキュリティの重要性は従来から指摘されているが、昨今、ネットワークを通じたいわゆるサイバー攻撃による情報漏えいや業務妨害などが大きな社会問題となり、喫緊に取り組まなければならない課題として、より一層強く認識されるようになってきた。

スマートフォンは、従来の携帯電話とＰＣの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、アプリケーションなどの周辺領域を含め成長の著しい分野である。しかし、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[1]が出現するなど、情報セキュリティ上の課題が指摘されている。これまでに大きな被害は報告されていないものの、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る中、被害が拡大する前段階で対処する必要があるとの認識から、スマートフォンの情報セキュリティ対策について検討することとした。

新しい技術やサービスは、国民が安心してその恩恵を受けられなければ、結局、信頼を失ってしまう。利便性と情報セキュリティレベルの向上は相反する要請のように言われることがあるが、二者択一の発想ではなく、利便性を維持しながら、どのような情報セキュリティ対策を講ずべきかという視点で検討することが重要である。

このような観点から、スマートフォンの情報セキュリティレベルの向上、特にマルウェアや外部からの攻撃に対処するために早急に講ずべき対策として、携帯電話事業者及び端末製造事業者において導入を検討されるべき情報セキュリティ対策、及び利用者への普及啓発の内容や周知の方法について、有効かつ現実に即した方策を中間報告としてとりまとめた。

[1] マルウェアとは、malicious software の短縮された語。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。

第１章　スマートフォンを取り巻く状況

第１節　スマートフォンの急速な普及

（１）スマートフォンとは

スマートフォンとは、従来の携帯電話端末の機能に加え、高度な情報処理機能が備わった携帯電話端末である。ＰＣと同様に、使いたいアプリケーションを自由にインストールするなどして、利用者が自由にカスタマイズできることが特長であり、タッチパネルを搭載した製品が多い。

多様なアプリケーションの流通を背景に、個人や企業の活動における様々な場面において、利活用への期待が高まっている。

（２）スマートフォンの普及状況

スマートフォンの普及が急速に進展しており、平成２３年度上半期（４～９月）のスマートフォン国内出荷台数は1,004万台で、前年度比4.5倍、携帯電話端末の国内総出荷台数の49.5%を占めるに至っている。スマートフォン市場がいよいよ成長期を迎えつつある中、情報セキュリティ上の問題が発生した場合のインパクトの大きさに鑑みれば、情報セキュリティ対策の強化が急務である。

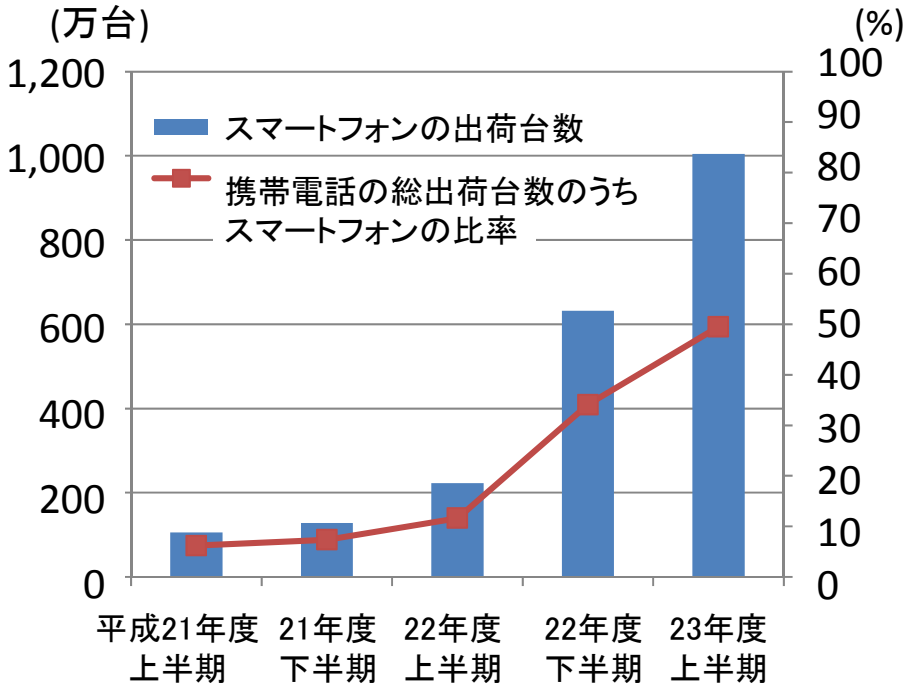


図１　スマートフォンの出荷台数等の推移

（株式会社ＭＭ総研のデータ（平成２３年１０月２７日、平成２３年５月１０日、平成２２年１０月２６日及び平成２２年４月２２日）を基に作成）

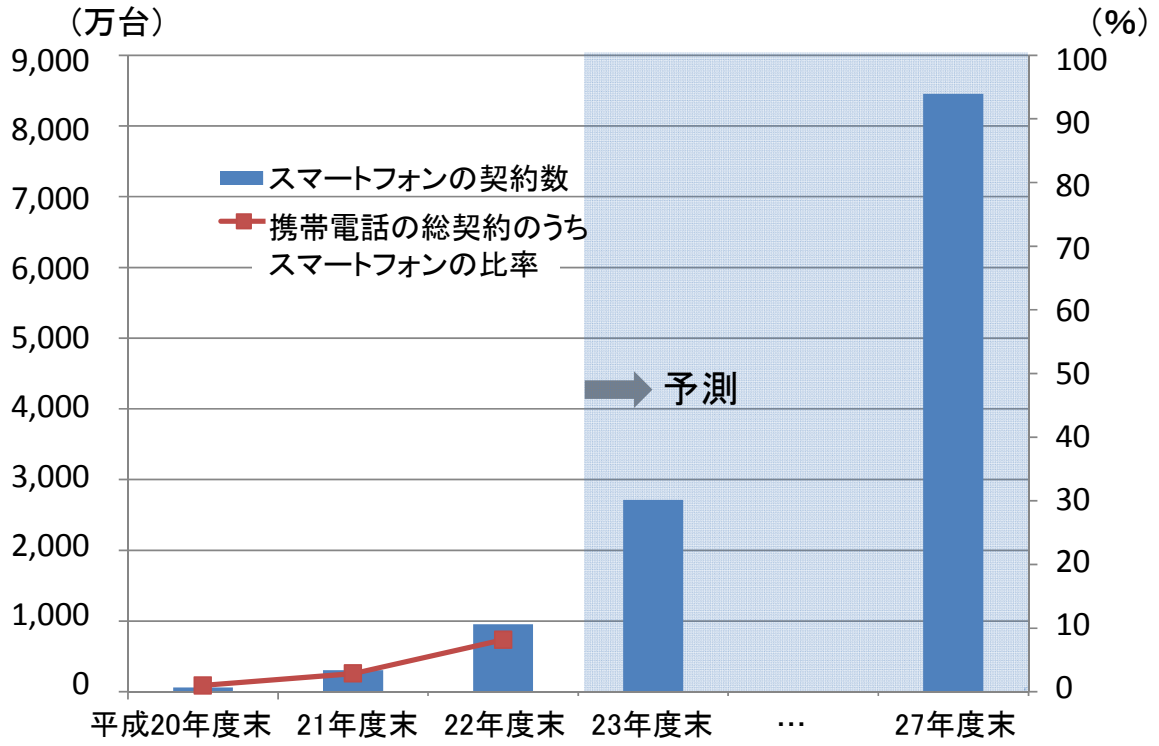


図２　スマートフォンの契約数等の推移
（株式会社ＭＭ総研のデータ（平成２３年７月７日）及び株式会社インプレスＲ＆Ｄのデータ（平成２３年１２月６日）を基に作成）

第２節　スマートフォンの特性

（１）ＰＣとの差異

スマートフォンは、ＰＣと比較すると、ハードウェアの処理能力が限られるため情報セキュリティに割けるリソースが少ない、ＯＳがシングルユーザを想定しているため利用者ごとの権限設定ができない、ファイルの暗号化などの機能に乏しいなど、ＰＣにはあるがスマートフォンにはない特性により、ＰＣでは可能な情報セキュリティ対策を取ることが困難になる可能性がある。他方、通話機能に加え、カメラやＧＰＳ等のデバイスが搭載されているなど、ＰＣにはない機能がスマートフォンに具備されていることにより、利便性が高いが故に新たな脅威が発生する、又は脅威が大きくなることがあるということにも留意する必要があると考えられる。

（２）セキュリティモデルの特徴

スマートフォン向けＯＳでは、アプリケーションを制限されたアクセス範囲でのみ動作させることによって、デバイスやデータが不正に操作されるのを防ぐセキュ

リティモデル（サンドボックス[2]）が使用されていることが多い。しかし、マルウェアが混入したアプリケーションに対し、過大なアクセス範囲を利用者が一旦承認してしまえば、当該セキュリティモデルが有効に機能しなくなるという側面を有している。

（３）多様な通信路

従来の携帯電話が基本的には携帯電話事業者のネットワークのみを使用するのに対し、スマートフォンでは、携帯電話事業者のネットワークと、無線ＬＡＮを経由することによりその他回線設置事業者のネットワークの双方が利用可能である。

通信路の多様化により、利用者の利便性が向上する一方、無線ＬＡＮ自体の情報セキュリティ上の課題が問題になる。

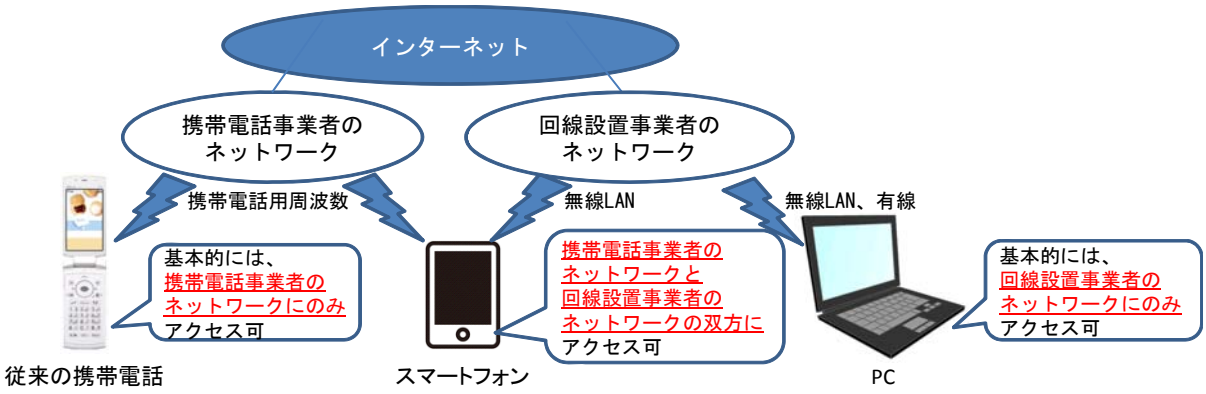


図３　通信路の多様化

（４）ビジネスモデルの変容

スマートフォンの台頭により、携帯電話を取り巻く状況が、我が国においても、従来の携帯電話事業者を中心とした垂直統合モデルから、ＯＳ提供事業者、端末製造事業者、携帯電話事業者等様々なプレーヤが複雑に関与するモデルに変容してきた。ＯＳ提供事業者及び端末製造事業者がグローバル展開し、グローバルモデルの製品を提供しており、ビジネスモデルの変容は、責任分界点やコントロール性の変化だけでなく、技術的な対策のあり方にも変化を及ぼしている。

第３節　スマートフォンに対する利用者の意識

（１）一般利用者の意識　―従来の携帯電話の延長としての認識―

スマートフォンは、従来の携帯電話端末と同じ売り場で購入、又は従来の携帯電話端末からの機種変更により利用者が入手することが多い。そのため、多くの一般

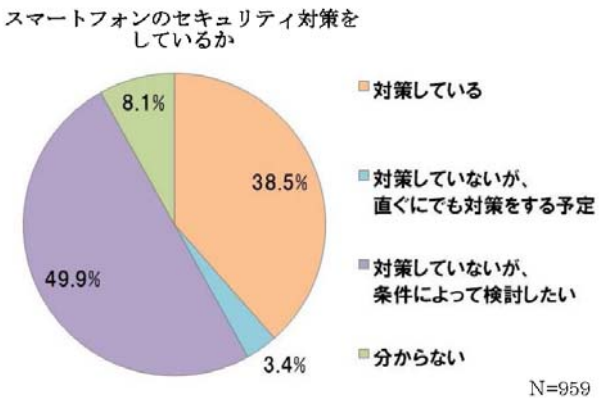
[2] サンドボックス（sandbox）とは、外部から受け取ったプログラムを保護された領域で動作させることによって、システムが不正に操作されるのを防ぐセキュリティモデルのこと。

利用者は、スマートフォンを、従来の携帯電話の延長や高機能な携帯電話端末という意識で利用していると考えられる。

アンケート調査によれば、スマートフォンの情報セキュリティ対策を取っている利用者は約４割との結果（図４－１）もあり、従来の携帯電話端末と同レベルで安全であるという意識を持っている利用者が多数存在するのが実態である。さらに、スマートフォンの情報セキュリティ対策を取らない利用者のうち、４割以上が「必要だが実際に何をすればよいか分からない」との結果（図４－２）もある。

したがって、携帯電話事業者等はこれまでにも、スマートフォン向け情報セキュリティ対策についての利用者啓発の取組を行ってきてはいるが、一般利用者は、スマートフォンに係る脅威及び対策手法を必ずしも十分に認知していないと考える必要がある。

情報セキュリティ対策を怠ることは、自らのスマートフォンがリスクにさらされるだけでなく、ボット化[3]してネットワークや他の利用者に影響が及ぶ可能性があることから、利用者の情報セキュリティ対策に関する意識の向上を図ることが必要である。



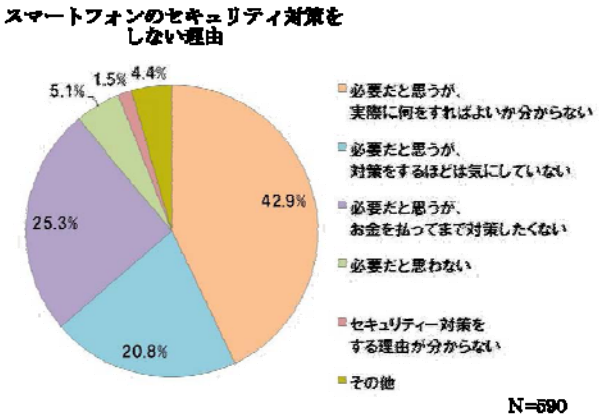


図４－１　　図４－２

スマートフォンのセキュリティに関する調査

（株式会社ネットマイル（平成２３年１２月６日））

（２）ビジネス利用者の認識

ビジネスシーンでは、これまで利用していたＰＣの代わりにスマートフォンを使用する形態もあることから、ビジネス利用者は、スマートフォンをＰＣに通話・通信機能が付加されたものとして捉えていることも想定される。しかしながら、スマートフォンが最近急速に普及したことや、その機能が日々高度化していることなどもあり、ビジネス分野においてスマートフォンを業務システムの中にどう組み込む

[3] ボット化しているとは、感染したコンピュータを遠隔で操作する機能を持ったコンピュータウイルス（ボットウイルス）に感染した状態のこと。操作された状態が、ロボット（Robot）に似ているところから、ボット（ＢＯＴ）と呼ばれている。

かのモデルは必ずしも確立できていない状況にある。

このような問題意識の下、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「日本スマートフォンセキュリティフォーラム」（ＪＳＳＥＣ）では、業務上でスマートフォンを利用する場合の情報漏えい対策など、ビジネスユースにおける情報セキュリティ上の脅威とその対策の検討を行っている。その成果として、管理者向けガイドラインとして、「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン　～その特性を活かしたワークスタイル変革のために～【第１版】」（平成２３年１２月１日）を公開している。本ガイドラインは、ビジネス分野においてスマートフォンを活用する際に参考となるものである。

第４節　情報セキュリティ上の脅威

（１）スマートフォンを対象としたマルウェアの出現

スマートフォンの急速な普及に伴い、スマートフォンをターゲットにしたマルウェアが出現している。

平成２２年８月にAndroidを対象とした初のマルウェアが発見されて以来、スマートフォンを対象としたマルウェアは増加傾向にあり、これらのマルウェアの中には、ボットウイルスもあり、勝手に電話を発呼するもの、遠隔操作によりデータを窃取するもの等が報告されている。平成２３年２月には、日本語のアプリケーションでマルウェアが混入したものが発見されている。

また、図５に示すように、利用者が最も不安に感じている情報セキュリティ上の不安は、ウイルスなどのマルウェア感染であるとのアンケート結果もある。

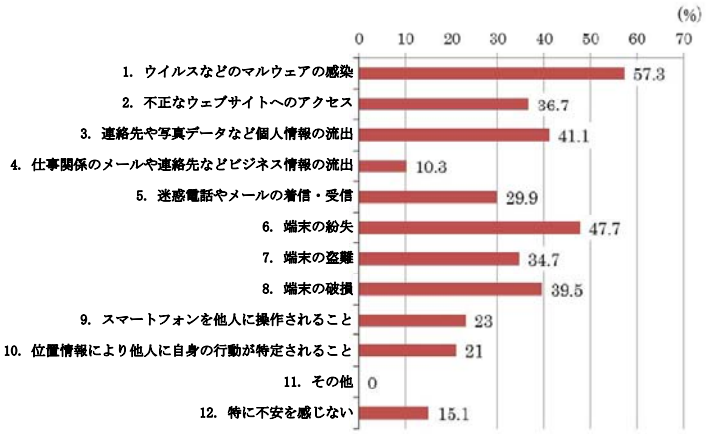


図５　スマートフォン利用にあたり、セキュリティについて感じる不安
出典：スマートフォン利用におけるセキュリティ意識（マカフィー株式会社）
（平成２３年９月１２日）

（２）無線ＬＡＮ利用による脅威

スマートフォンで無線ＬＡＮを利用する場合、インターネットが持つ情報セキュリティ上の脅威一般にさらされることになり、なりすましアクセスポイント、通信パケットの傍受や、それを契機とした利用者になりすました不正アクセスといった脅威が発生する。

無線ＬＡＮを利用することに伴ってスマートフォンに発生するリスクは、ＰＣの場合と同様であるとの考え方もあるが、スマートフォンに機能的な制約があること

や、利用者が意識しないままに無線ＬＡＮを利用するという事象が発生しやすい、利用者のリテラシーレベルがＰＣに比べて低い場合があるといった諸点から、ＰＣにおける無線ＬＡＮ利用の場合よりも、よりそのリスクが顕在化しやすい性質を持っていることに留意することが重要である。

（３）利用者が意図しない利用者情報の外部送信等

スマートフォンは、従来の携帯電話同様に日常的に持ち運ばれ、外出中であっても頻繁に利用される。そのため、スマートフォンは、ＰＣと比較して利用者との接触時間が長くなる傾向があり、アプリケーションや位置情報の使用が増えるため、これらに付随する利用者に関する幅広い情報が、利用者が意識しないままにスマートフォンに蓄積されている。

これらの利用者情報を、利用者の意図しない形で、外部に送信する機能を持つアプリケーションやデーモン[4]等のプログラムが出現している。

[4] デーモンとは、マルチタスクＯＳにおいてバックグラウンドで動作するプログラム。

第２章　スマートフォンの情報セキュリティ対策の考え方

第１節　情報セキュリティ上の課題

前章で述べたような情報セキュリティ上の脅威が現れている状況を踏まえ、情報セキュリティ上の課題を整理する。検討領域と各領域間の情報のやり取りを図示すると、図６のようになる。

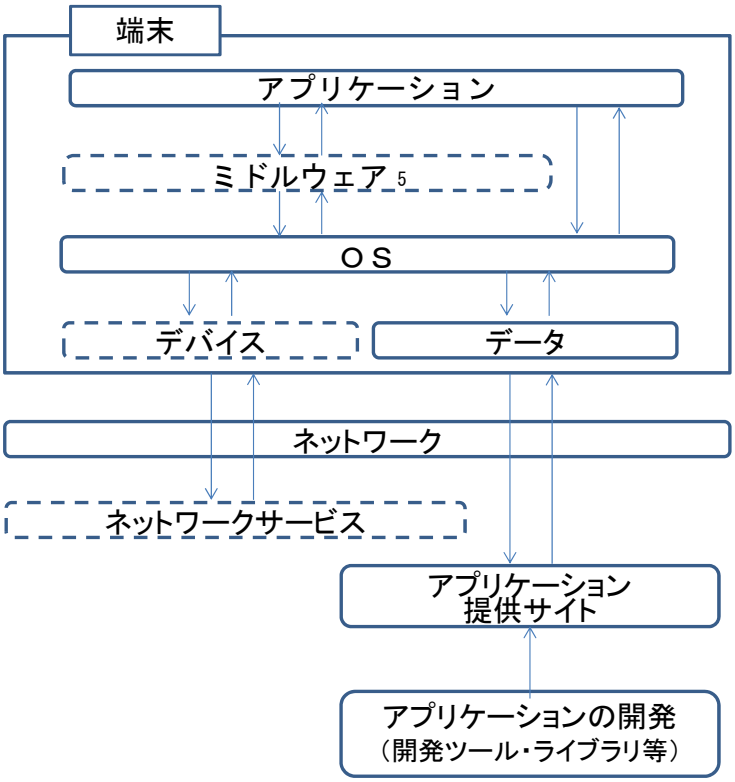


図６　スマートフォンのセキュリティ対策に関する検討領域

（１）ＯＳの課題

ア　ぜい弱性に関する課題

ＯＳのぜい弱性を狙うマルウェアにより、ＯＳ上の管理者権限が不正に取得され、ＯＳ自体やシステムファイルが書き換えられてしまうリスクが指摘されている。

イ　ＯＳのバージョンに付随する課題

新しいバージョンのＯＳは、ＯＳ提供事業者により独自に開発・公開され、その影響は、当該ＯＳを搭載する端末製造事業者や、その端末により利用されるネットワークを提供する携帯電話事業者にも及ぶ。

特に、端末製造事業者が、利便性や情報セキュリティレベルを向上させるた

[5] ミドルウェアとは、ＯＳとアプリケーションの間で動作するソフトウェアのこと。アプリケーションに共通する処理を集約し、各アプリケーションにその機能を提供する。

めに、ＯＳを独自にカスタマイズしている場合には、新しいバージョンのＯＳに対しても、別途カスタマイズを行うことが必要となるため、開発には、相応の工数と期間を要する。

さらに、ＯＳのセキュリティパッチ[6]については、ＯＳ提供事業者から発行された後に、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、利用者への提供の遅れが発生しているとの指摘もある。そのため、マルウェア等によりぜい弱性を悪用される可能性がある期間が、結果的にＰＣより長くなる傾向にある。

（２）アプリケーションの課題

スマートフォンのアプリケーションは、従来の携帯電話のアプリケーションとは異なり、利用者に付与された権限を自由に用いた機能実現が可能である。

この特性を用いて、悪意ある動作をするアプリケーションやマルウェアが作成されている。利用者がこれらをインストールすることは、情報セキュリティ上危険性が高いと指摘されている。

ア　悪意ある動作をするアプリケーションの問題

悪意ある動作をするアプリケーションには、アプリケーション作成者が意図的にマルウェア等を組み入れる場合と、ＳＤＫ[7]により組み込まれたモジュールにマルウェア等が含まれている場合とがある。前者が許されないのは当然であるが、後者の場合は、アプリケーション作成者も、組み込んだモジュールがどのような動作をしているのかを十分認識していないことがある。例えば、個人情報を収集するモジュールの場合、ＳＤＫ作成者がどのような目的で利用者情報を収集・蓄積しているのかといったことや、それらの情報がどのように管理・利用されているのかが、アプリケーション作成者にとって不明な場合がある。

イ　アプリケーションの開発方法の課題

アプリケーション開発者のセキュリティ軽視や知識不足により、意図しないうちに、ぜい弱性を持ったアプリケーションを提供してしまうことや、利用したＳＤＫにより情報の不正取得・流通に荷担してしまうおそれがあるという課題も指摘されている。このようなアプリケーション開発者による問題の発生を防ぐためには、アプリケーション開発者に対し、アプリケーションの安全な開発方法を浸透させていくことも重要である。

ウ　セキュリティ対策ソフトの課題

セキュリティ対策ソフトは、マルウェア対策として有効である。他方で、サ

---

[6] セキュリティパッチとは、ＯＳ等のぜい弱性を修正するプログラムのこと。

[7] ＳＤＫ（Software Development Kit）とは、ソフトウェア開発のためのツールのセット。

ンドボックスを採用しているセキュリティモデルの特徴から、アプリケーションの一種であるセキュリティ対策ソフトは、他のアプリケーションの動きや内容を原則として監視することができないという限界を構造上抱えている等の課題が指摘されている。

エ　ウェブ連動型アプリケーションの課題

多くのアプリケーションがウェブサービスと連動して機能するため、ウェブサービス側のセキュリティも課題である。

（３）ネットワークの課題

スマートフォンの普及による通信量の増大により、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、携帯電話事業者は、利用者の利便性を向上させるべく、トラヒックの一部を逃がす（オフロード）先である無線ＬＡＮの基地局増設やサービスの無料提供を表明している。

スマートフォンでは、携帯電話事業者設備以外の公衆無線ＬＡＮ等を利用することがあるため、従来の携帯電話と異なり、携帯電話事業者の取組だけでは、十分な情報セキュリティ対策が困難であるという課題がある。

（４）端末内のデータに関する課題

スマートフォン端末には個人情報を含む多くの情報が集約されていることから、端末の紛失・盗難等によって、データの紛失や第三者に情報を抜き取られるリスクや、他人が再利用できない仕組みの必要性が指摘されている。現在、遠隔消去や自己消去機能[8]等が対策として挙げられることが多いが、遠隔消去による対策は、端末に電源が入っており、かつ通信状態が良好な場合にしか効果が期待できない点に留意する必要がある。

また、スマートフォンの外部記憶媒体として、ＳＤカードが広く利用されているが、端末の盗難・紛失等によって、当該ＳＤカードごと盗まれてしまうことがある。さらに、当該ＳＤカードに蓄積されたデータが、ネットワーク経由又はＰＣに接続することにより抜き取られるリスクも指摘されている。

（５）利用者の普及啓発に関する課題

第１章第３節で述べたとおり、スマートフォンの情報セキュリティについて、利用者の意識の向上が必要である。このためには、利用者に対し、「何を」啓発すべきかということに加え、「いかなる方法で」利用者に対する啓発を行うのかについても工夫が必要である。

（６）利用者情報に関する課題

8 自己消去機能とは、既定のパスワード入力回数を超えた場合に、システムの消去などを行う機能。

第１章第４節（３）で述べたとおり、位置情報等の利用者情報を、利用者の意図しない形で外部に送信するアプリケーションが問題となっている。これについては、インストール時における利用者への適切な同意取得のあり方、マルウェアや問題のあるアプリケーションの客観的判断基準をどうすべきかなどの課題が明らかになっているところである。

（７）ビジネスモデルの変容に伴う課題

ＯＳ提供事業者及び端末製造事業者がグローバル展開し、グローバルモデルの製品を提供しているため、これらの事業者に対して、我が国単独の要望として情報セキュリティ上の措置を求めることが困難であることも認識する必要がある。

（８）本中間報告で取り上げる課題

（１）～（７）の課題のうち、本中間報告では、当面早急に講ずべき対策を取りまとめる観点から、ＯＳ、アプリケーション、ネットワーク及び利用者啓発に関する事項を中心に取り扱うこととし、残りの課題については、最終報告に向けて引き続き検討することとする。

なお、利用者情報に関する課題については、技術的な切り口もさることながら、保護すべき情報そのものに関する議論が必要となることから、別途検討の場を設けるなどして、詳細な検討を進め、本研究会の検討と連携を図っていくことが適当である。

第２節　対策の検討に当たっての基本的考え方

（１）ＯＳ等による対策の違い

現在、スマートフォンのＯＳとしては、Android、BlackBerry、iOS及びWindows Phoneが存在するところ、ＯＳによって、その設計思想やビジネスモデルが異なることから、その特徴に応じた対策を講ずることが適当である。

なお、インターネットに接続されたＰＣの情報セキュリティ対策については、一足飛びに現在の状況に至ったのではなく、十数年の年月を経て醸成されてきたものである。そのため、スマートフォンについても、情報セキュリティ対策が技術的に成熟し、それが十分に利用者に受け入れられるまでには、相応の時間がかかることも予想される。かかる事情に鑑み、次章以下では、ビジネスモデルやスマートフォンのスペック等様々な制約により、実施者や端末によっては速やかな実現が困難な対策についても、その困難性をもって検討範囲から外すことはせず、情報セキュリティ対策に含めている。

（２）連携の重要性

スマートフォンの情報セキュリティ対策に限らず、一般に、情報セキュリティに関する対応については、企業や研究機関、行政等の間で、情報セキュリティ上の事案に関する情報を共有するなど、連携が求められている。

情報セキュリティ対策においては、携帯電話事業者、端末製造事業者等によって、ＯＳのカスタマイズ状況、情報セキュリティ対策自体やその手法に関する考え方、保有する技術、端末のスペックなどが異なることがあるため、横並びの対策が難しいことは事実である。しかし、速やかな情報セキュリティ対策の強化のためには、スマートフォンの情報セキュリティレベル向上等について、事業者団体の場を活用するなどして、可能な範囲で情報の共有を図ることが重要である。

また、新端末の発売を急ぐあまり、情報セキュリティ上の大きな課題を残したまま端末が発売されるなど、スマートフォン産業の健全な発展を歪めることがあってはならないという観点から、最低限必要な対策については、いずれの事業者においても講じられるようにすることが重要である。

（３）利便性の確保

国内の取組や、ガイドラインなど事業者団体等における自主規制については、常にグローバルな市場との関係性や、スマートフォンの利便性や我が国の事業者の競争環境を低下させることがないように留意する必要がある。

また、本中間報告は、スマートフォン産業の健全な発展を下支えすることを企図したものであり、「はじめに」で述べたように、利便性を維持しながら、どのような情報セキュリティ対策を講ずべきかという観点が重要である。そのため、情報セキュリティ対策を利用者に受け入れてもらうために、例えば、ＯＳの動作や、バッテリーの保ちなどに配慮し、スマートフォンの利便性を損なわないよう配慮するこ

とも重要である。

（４）海外との協調

我が国が単独で対策を実施するだけでなく、我が国のグローバルな発言力を強化するという観点も重要である。そのため、国際社会の理解を得ながら、対策手法等について情報交換を行うとともに、場合によっては国際標準化を進めていくことも有益である。

また、政府及び事業者は、国内における検討、国際社会における活動の双方で、事業者団体の動きと協調していくことが重要である。

以上の基本的考え方を踏まえ、本中間報告においては、当面早急に講ずべき対策をとりまとめる観点から、携帯電話事業者及び端末製造事業者において対応が可能な対策、及び一般利用者に対する普及啓発策に焦点を絞り、有効かつ現実に即した対策を取りまとめた。

第３章　事業者において導入を検討されるべき対策

第２章で整理した情報セキュリティ上の課題に対して、携帯電話事業者及び端末製造事業者において対応が可能な領域に焦点を絞り、以下に対策をとりまとめた。

第１節　ＯＳにおける対策

（１）ＯＳのバージョンに付随する対策

ＯＳのぜい弱性に対応したセキュリティパッチが、ＯＳ提供事業者により発行された場合には、優先順位を付けて、可能な限り速やかな利用者への通知やＦＯＴＡ[9]対応などにより利用者端末に適用すべく、携帯電話事業者との連携を含め、端末製造事業者の取組が引き続き求められる。ただし、ＯＳの機能性等に関する不具合への対応も、利用者の利便性を高める上で重要であるばかりか、不十分な形でパッチを提供することにより、かえってＯＳの情報セキュリティレベルを落とすことになっては本末転倒であることに留意すべきである。

また、ＯＳのぜい弱性情報や、そのぜい弱性に起因する被害状況を、ぜい弱性情報の悪用防止という見地から、既存の取組と事業者団体とが連携して把握し、対応方策も連携して検討した上で、ＯＳ提供事業者に提供する取組も有効と思われる。さらに、ぜい弱性を早期に検出するため、検査ツールなどの研究開発も重要である。

（２）ぜい弱性に関する対策

現状のセキュリティ対策ソフトは、問題のあるアプリケーションの侵入を防ぐことに主眼があるが、一部に防御が難しい攻撃が存在することから、防御の効果を高めるためには、アーキテクチャやソフトウェアの構造を含めた対策の検討を行うことが有効である。

いずれにしても、完ぺきなセキュリティ対策は存在しないことを前提に、万が一情報セキュリティが破られてしまった場合の被害最小化のための対策についても、併せて検討を行うことが重要である。対策の一例として、アプリケーションやミドルウェアを乗っ取られた場合に備えた権限最小化、管理者権限を奪取された場合に備えたＯＳ機能最小化（不必要なコマンドの削除等）、システムファイル書換えに備えた改ざん検出・機能凍結などの対策、さらには、カーネル部への情報セキュリティ対策により、ＯＳが持つ安全性を向上させること等が挙げられる。

これらの対策を複数組み合わせることで、ＯＳの堅牢性をより強化し、かつ特定の対策が破られた場合の被害最小化を図ることが可能であるとの指摘がある。

[9] ＦＯＴＡ（Firmware Over-the-Air）とは、スマートフォンのＯＳ等の更新を無線通信で行うこと。

第２節　アプリケーションにおける対策

（１）アプリケーション提供サイトにおける審査

マルウェアの侵入経路は、マルウェアを含むアプリケーションをインストールすることにより引き起こされる場合が多いとされている。アプリケーションの審査におけるセキュリティチェックの方法は、アプリケーション提供サイトによって異なっていることから、その審査状況を踏まえ、信頼のおける提供サイトからのアプリケーションの入手を推奨することが適当である。

（２）セキュリティ対策ソフト

マルウェアを含むアプリケーションを、利用者が誤ってインストールしてしまうことを防ぐため、マルウェアのインストールを検知できるセキュリティ対策ソフトの提供や導入の推奨は、有効な対策である。

（３）関係者の連携や総合的な対策の必要性

アプリケーションのインストールを十分注意して行い、かつセキュリティ対策ソフトを導入してもなお、情報セキュリティ上の脅威を防ぎきれない可能性もあることから、事業者団体の場を活用するなどして、脅威の動向について関係者が連携して把握し、その対策に努めるとともに、前節で掲げた対策等と合わせて、総合的な対策を講ずることが肝要である。

第３節　ネットワークにおける対策

（１）無線ＬＡＮ利用の情報セキュリティ対策

ＷＰＡ[10]やＷＰＡ２[11]、ＳＳＬ[12]やＶＰＮ[13]といった認証や暗号化の標準的な技術の活用に加え、接続先を識別し、回線の信頼度に応じて保護レベルを変更できる仕組みの導入が考えられる。

また、利用者が無意識のうちに保護されていない無線ＬＡＮを利用することを避けるためには、当該無線ＬＡＮを利用する際に、利用者の承認を求めるというように気づきを与える仕組みも、引き続き有効となる。

---

[10] ＷＰＡ（Wi-Fi Protected Access）とは、従来の無線ＬＡＮの暗号化方式であるＷＥＰ（Wired Equivalent Privacy）のぜい弱性を補強したもの。なお、現在では、ＷＥＰの利用は推奨されていない。

[11] ＷＰＡ２とは、ＷＰＡと比較して、より強固な暗号を用いた無線ＬＡＮの暗号化方式のこと。

[12] ＳＳＬ（Secure Socket Layer）とは、インターネット上でデータを暗号化して送受信するプロトコルのこと。オンラインショッピングやウェブメールなど、個人情報や機密情報を扱うサービスにおいて広く使用されている。

[13] ＶＰＮ（Virtual Private Network）とは、データを送受信する拠点間の通信経路を暗号化し、インターネット等の公衆回線で、専用回線並みのセキュリティを実現するサービスのこと。

第４章　一般利用者への普及啓発のあり方

第１節　普及啓発の内容

スマートフォンは、利用者の目的に応じてソフトウェアや端末機能をカスタマイズする自由が一定程度確保されていることなどにより、サービス提供者側の対策のみによって安全性を確保することが困難な場合もあることから、利用者自身が必要なリテラシーを身に付け、適切な情報セキュリティ対策を取ることが必要である。昨今、様々な主体により普及啓発活動が行われるようになってきているが、社会全体として早急に利用者全体のセキュリティ意識を高め、各個人による対策の実施を促すため、次のような事項について普及啓発を行うことが検討されるべきである。

【普及啓発を行うべき事項】

（１）スマートフォンの性質について

スマートフォンは、従来の携帯電話端末の機能に加え、高度な情報処理機能を持ち、利用者の目的に応じて様々なカスタマイズが可能な携帯電話端末であることから、従来の携帯電話とは異なり、事業者による対策に加え、利用者自身でも情報セキュリティ対策に留意することが重要である。

（２）利用者に実施を促す事項

ア　スマートフォンＯＳやアプリケーションに含まれるぜい弱性を放置することは、マルウェア感染、情報漏えいなどの危険性を高めることから、それらのソフトウェアのパッチや更新版が提供された際には、速やかにインストールを行う。

イ　誤ってマルウェア等の混入したアプリケーションをインストールすることを避けるため、セキュリティ対策ソフトをインストールすることが推奨される。

また、携帯電話事業者の提供する通信時のセキュリティチェックサービス、クラウドサービス事業者が提供する事業者管理サーバに保存されたデータに対するセキュリティチェックサービスを活用することも有効である。

ウ　事前審査の行われていない又は十分でないアプリケーション提供サイトにおいては、マルウェア等の混入したアプリケーションが発見される例があることから、アプリケーションを入手する際には、ＯＳ提供事業者又は携帯電話事業者等が安全性の審査を行っているアプリケーション提供サイトを利用することが推奨される。

（３）利用者の認識を促す事項

ア　ＯＳのぜい弱性を突くなどの手段により、ＯＳ提供事業者により設定されていた制限を外す行為（いわゆる“Jailbreak(脱獄)”）は、ＯＳのセキュリティレベルを下げる可能性がある。

イ　無線ＬＡＮは、暗号や認証の仕組みが導入されていない場合があり、安全な通信が確保できるかどうかが不明であるため、そこに接続して行う通信が外部に内容を読み取られる可能性があることを認識する必要がある。

（４）その他

（１）～（３）のほか、従来の携帯電話も含む携帯電話端末全般の取扱いに関する情報セキュリティ対策として、盗難・紛失時における第三者による利用を防ぐための対策（端末ロック、遠隔消去等）、データのバックアップ、プライバシーフィルターの利用等についても、併せて複合的に実施することが推奨される。

以上の事項は、スマートフォンの一般利用者向けに、利用者自身が取るべき情報セキュリティ対策について、政府及びスマートフォン関係事業者（携帯電話事業者、端末製造事業者、アプリケーション提供サイト運営者等）等が普及啓発を行う際に、取り上げるべき標準的事項をまとめたものである。ただし、ＯＳや端末の種類によっては必ずしも当てはまらない項目もあることから、各ＯＳや端末の特性を見極めた上で、対象者や普及啓発の場面ごとに取捨選択の上、普及啓発を行うことが望ましい。

【スマートフォン情報セキュリティ３か条】

上述の普及啓発事項に加え、本研究会としては、スマートフォンが幅広い年齢層の利用者に普及している現状を踏まえ、具体的で分かりやすく現実的な事項に重点化するべきとの基本的な考え方に立ち、利用者が最低限取るべき情報セキュリティ対策を、「スマートフォン情報セキュリティ３か条」（別添）としてとりまとめた。これについて、関係者の協力により、早急に利用者に対して啓発を行っていくことが必要である。

第２節　普及啓発の方法

利用者への普及啓発に当たっては、政府、スマートフォン関係事業者（携帯電話事業者、端末製造事業者、アプリケーション提供サイト運営者等）やスマートフォン関係事業者等から構成される事業者団体等が、既存の取組を活用しながら、相互に連携し、効果的に普及啓発を行うことが必要である。

以下では、取組の主体別に、これまでの普及啓発活動及び今後の取り組むべき方

向性についてまとめる。

（１）携帯電話事業者の取組

各携帯電話事業者は、これまでにも、スマートフォン契約時の注意事項の説明、企業ウェブサイトや各社独自のアプリケーション提供サイトにおける情報セキュリティ関連コンテンツの掲載などスマートフォン向けセキュリティ対策についての利用者啓発の取組を行ってきている。その内容は、主に各社が独自にセキュリティ事業者等と提携して提供している各種セキュリティサービスの利用を推奨するものとなっている。

一方で、「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」の中の「電気通信サービス利用者の利益の確保・向上に関する提言（案）」（平成２３年１０月２８日）において、スマートフォンを従来の携帯電話端末同様に安全であるという認識しか持たない利用者の存在は、携帯電話事業者による広告表示等での説明が十分ではないことによる部分があるとの指摘も行われている。

このことを踏まえ、携帯電話事業者は、今後、以下のような取組を行っていくことが考えられる。

ア　脅威についての分かりやすい説明

契約時の説明においては、例えば免責事項の一部としてマルウェア感染の可能性等に言及するだけではなく、利用者が的確に情報セキュリティ上の脅威の大きさを把握できるような説明を行う等の工夫が望ましい。

イ　基本的な情報セキュリティ対策の資料化

利用者自身が行うべき基本的な情報セキュリティ対策についてまとめた情報を、端末製造事業者と協調して、端末取扱説明書等に追加することや、初心者向けスタートアップマニュアル等として資料化することが、引き続き重要となる。

ウ　販売店への協力依頼等

販売店等に対して協力を求めるなど、利用者がどのようなチャネルを通じて商品を購入する際にも、情報セキュリティ関連の説明を受けられるよう徹底する方策なども検討されるべきである。

（２）アプリケーション提供サイト運営者の取組

現在、スマートフォンにおいてセキュリティ上最も危険性が高いとされるのが、マルウェアの混入されたアプリケーションをインストールすることであることから、アプリケーション提供サイトにおいては、以下のような取組を行っていくことが効果的と考えられる。

ア　情報セキュリティ関連コンテンツの掲載

情報セキュリティ関連コンテンツを掲載し、トップページにバナーを設ける

など、利用者の目につきやすい場所に配置する。

イ　サイトの運営方針等の開示

事業者自身の努力として、運営するサイトから不正アプリケーションを排除する取組を継続的に進めるとともに、そのようなサイトの運営方針や取組状況等、利用者がサイトの安全性について判断することが可能になるための情報を開示していく。

（３）事業者団体の取組

民間企業間の自主的な取組として、企業や組織がスマートフォンを業務利用する際のガイドラインや、アプリケーション及びアプリケーション提供サイトの安全性評価を行うための基準などを策定する活動が進められている。利用者が安全なサービスを選択する際の一つの目安を示すものとして、こうした取組が推進され、またより広範な啓発主体と連携していくことが期待される。

（４）政府の取組

「情報セキュリティ２０１１」（平成２３年７月情報セキュリティ政策会議決定）では、急速に普及しているスマートフォンについて、総務省を含む関連省庁が「従来の携帯電話端末、ＰＣ等との特性の違いを踏まえ、スマートフォン普及に伴って発生する問題点について利用者周知を行う」こととされている。

既に総務省においては、前述の「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」の中の「電気通信サービス利用者の利益の確保・向上に関する提言（案）」においても検討が行われ、同研究会の指摘も踏まえ、本研究会では、普及啓発事項として前節の内容をとりまとめた。今後は、これらの取組について、政府広報、情報セキュリティの普及啓発に関するウェブサイトへの掲載、パンフレット作成、消費生活センター等との連携等を通じ、普及啓発を促進することが重要である。

（５）その他全体に共通する事項

スマートフォンの情報セキュリティ対策についての啓発資料は充実しつつあり、利用者が求めれば一定程度の情報が入手可能になっている一方、セキュリティ対策の必要性を感じていない層への訴求が課題となっている。政府、各事業者、事業者団体等は、関連する展示会、講演会、セミナー等の機会を通じて、積極的に情報セキュリティ対策の必要性を発信していくべきである。

また、青少年へのスマートフォンの安全な利用方法に関する啓発は、従来の携帯電話の場合のように、重点を置いて取り組まれることが望ましい。

あとがき

本研究会は、平成２３年１０月以降、スマートフォンの利用に際する情報セキュリティ上の課題について、その抽出及び整理を行った上で、当面、早急に講ずべき対策として、携帯電話事業者及び端末製造事業者において対応が可能な領域に焦点を絞って、当面実施されるべき事項につき集中的に検討し、結果を中間報告としてとりまとめた。

平成２４年１月以降は、最終報告に向けて、本中間報告で課題として指摘した事項や、スマートフォンを取り巻く中長期的な課題や対策等について、新たな状況の変化も踏まえつつ、引き続き検討を実施していく予定である。その際、「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」や事業者団体における検討や取組と、引き続き歩調を合わせて連携を図っていくことが重要であると認識している。

加えて、一つの大きな潮流として、企業の情報資産等の移行が進むウェブサービス等のクラウドサービスについて、スマートフォンを通じた利用が進み、利用主体・形態や取り扱われる情報の多様化が予想されることから、これに付随する課題や対策について、本研究会において検討していく。

本中間報告が、各事業者による情報セキュリティ対策に活かされるとともに、利用者への周知が徹底され、スマートフォンの健全な発展が図られることを期待する。

参　考

「スマートフォン・クラウドセキュリティ研究会」構成員名簿

（敬称略、五十音順）

阿佐美 弘恭	株式会社エヌ・ティ・ティ・ドコモ 執行役員 スマートコミュニケーションサービス部長
岡村 久道	国立情報学研究所 客員教授・弁護士
内田 義昭	KDDI株式会社 理事 運用本部長
大畠 昌巳	シャープ株式会社 執行役員 通信システム事業本部 本部長
齋藤 衛	株式会社インターネットイニシアティブ サービス本部 セキュリティ情報統括室 室長
佐古 和恵	日本電気株式会社 サービスプラットフォーム研究所 主席研究員
塩崎 哲夫	富士通株式会社 クラウドビジネスサポート本部 チーフアーキテクト
菅原 英宗	エヌ・ティ・ティ・コミュニケーションズ株式会社 アプリケーション＆コンテンツサービス部長
瀬野尾 修二	株式会社日立製作所 セキュリティ･トレーサビリティ事業部 ソリューション本部 本部長
竹内 正樹	ソニー・エリクソン･モバイルコミュニケーションズ株式会社 ソフトウェア部門　部門長
丹波 廣寅	ソフトバンクモバイル株式会社 プロダクト・サービス本部 本部長
中尾 康二	情報通信研究機構 ネットワークセキュリティ研究所　主管研究員
西本 逸郎	株式会社ラック 取締役ＣＴＯ
萩原 英二	パナソニック モバイルコミュニケーションズ株式会社 常務取締役
三輪 信雄	総務省 情報化統括責任者（ＣＩＯ）補佐官
山口 英	奈良先端科学技術大学院大学 教授【座長】

（オブザーバ）

近藤 玲子	内閣官房情報セキュリティセンター　企画調整官【第３回～】
江口 純一	経済産業省商務情報政策局　情報セキュリティ政策室長
関根 久	経済産業省商務情報政策局　情報家電戦略室長

検討経緯

第１回（平成２３年１０月１９日）
〇スマートフォンに関する各社の情報セキュリティ対策の現状の整理
〇スマートフォンの情報セキュリティに関する課題の洗い出し

第２回（平成２３年１１月４日）
〇日本スマートフォンセキュリティフォーラム（ＪＳＳＥＣ）の活動のヒアリング
〇スマートフォンの情報セキュリティに関する検討課題の整理
〇スマートフォン利用者への情報セキュリティ対策の普及啓発策の検討

第３回（平成２３年１１月２９日）
〇消費生活センターに寄せられたスマートフォンの情報セキュリティに関する相談の主な事例
〇スマートフォンの情報セキュリティに関する検討課題の整理
〇中間報告骨子（案）の検討

第４回（平成２３年１２月１９日）
〇中間報告（案）の検討