別紙１

スマートフォン・クラウドセキュリティ研究会　最終報告（案）

～スマートフォンを安心して利用するために実施されるべき方策～

平成２４年４月２７日

目　　次

はじめに

一般に、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。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、昨年１０月から、本研究会においてスマートフォンの情報セキュリティ対策に関する検討を開始した。

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、まずは、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、並びに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、昨年１２月に中間報告としてとりまとめた。

その後、各事業者や政府が、本中間報告を踏まえた技術的対策や普及啓発活動等に取り組んできたところではあるが、その一方で、利用者から実際の被害に関する相談・報告が寄せられるなど、脅威が現実のものとなっている。

今般、これらの取組や新たな状況の変化を踏まえて、中間報告の内容を拡充するとともに、スマートフォンからのクラウド利用に付随する課題やその対策、スマートフォンを安全に利用するためにクラウドを活用する方策を含めて、最終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いる。平成２３年度の国内のスマートフォン出荷台数は、前年度比2.7倍の2,340万台で、携帯電話端末総出荷台数の55.8%を占め、通期で初めてスマートフォンが過半数に達している見込みである[2]（図１）。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影響の大きさや、実際に被害に関する相談・報告が寄せられ始めていることに鑑みれば、情報セキュリティ対策の強化が急務である。

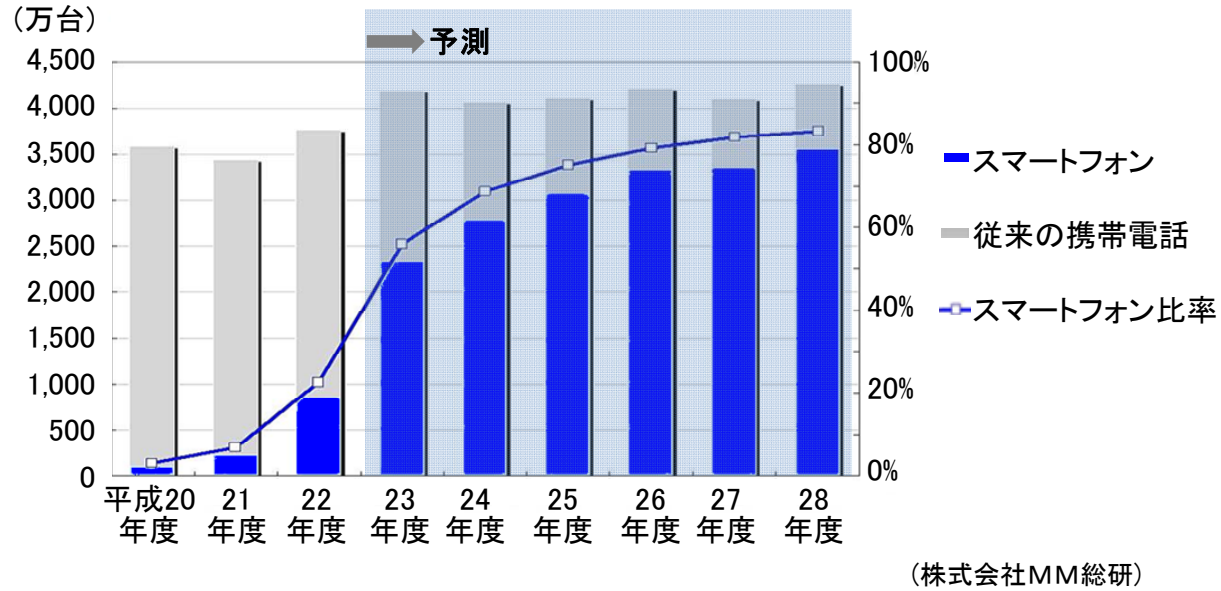
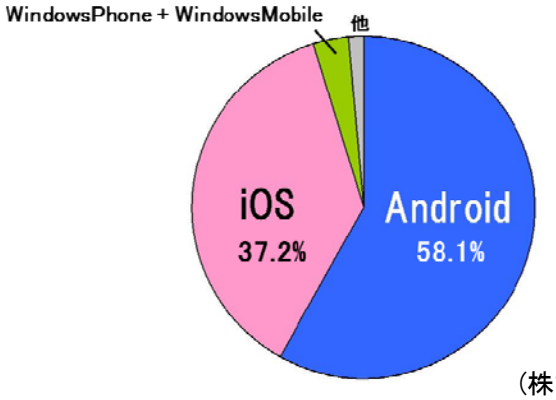


図１　国内の携帯電話端末（従来の携帯電話＋スマートフォン）の出荷台数

[2] 株式会社MM総研ニュースリリース（平成２４年３月１３日）
（http://www.m2ri.jp/newsreleases/main.php?id=010120120313500）

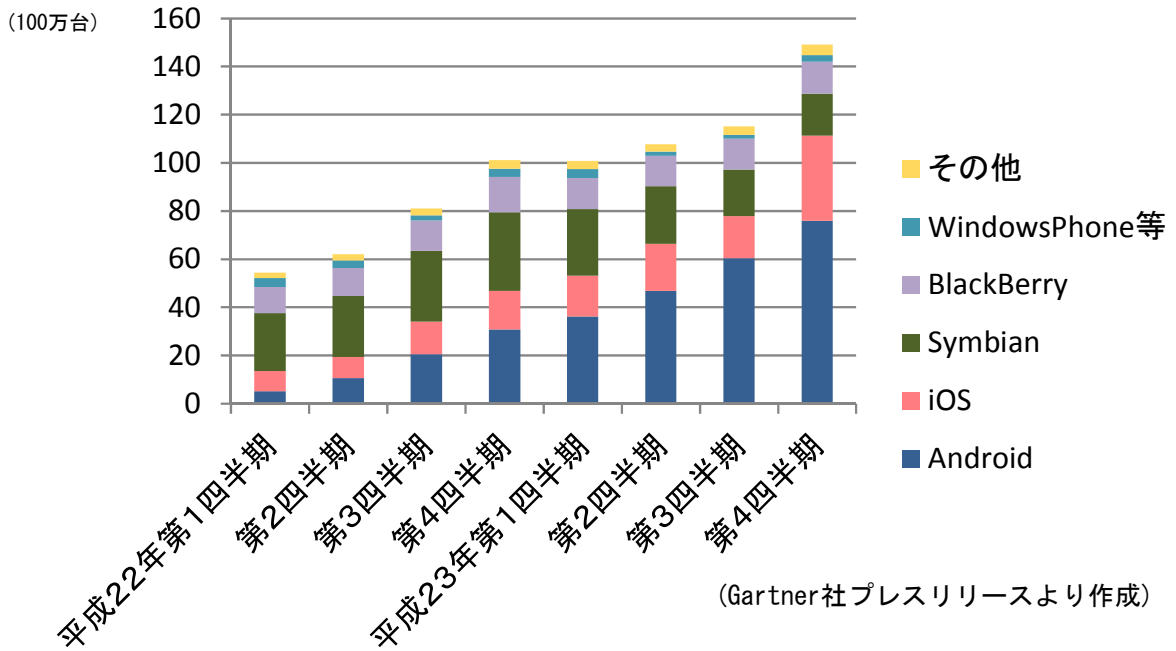
また、平成２３年１２月末時点での国内におけるスマートフォンの契約数のＯＳ別シェアは、Androidが58.1%、iOSが37.2%となっている（図２）。



（株式会社ＭＭ総研）

図２　国内におけるスマートフォンの契約数のＯＳ別シェア

スマートフォンは、従来の携帯電話とは異なり、ＯＳ及び端末が世界共通の仕様であるグローバルモデルの端末が国内市場にも多く投入されている。Android及びiOSは、世界的に見てもシェアを拡大[3]（図３）しており、海外で発生した脅威が国内に波及する可能性も考えられることから、まだ国内では顕在化していない情報セキュリティ上の脅威も含め、課題の抽出及び対策の検討を行うことが必要である。



(Gartner社プレスリリースより作成)

図３　世界のスマートフォン等[4]のＯＳ別出荷台数

[3] Gartner 社プレスリリース(http://www.gartner.com/it/page.jsp?id=1924314)等
[4] Symbian OS等には従来型の端末も含まれる。

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性質により、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）情報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情報セキュリティモデル（サンドボックス[5]）が使用されていることが多い。そのため、ＯＳの設計としては、一般的にＰＣより安全性が高いとされている。

しかし、マルウェアを含む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、当該情報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がある。

（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（図４）。

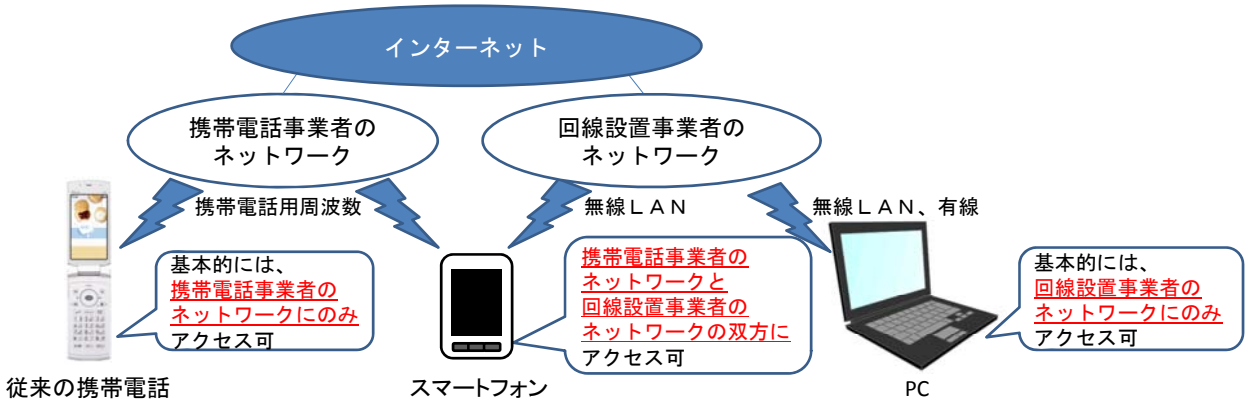


図４　通信路の多様化

[5] 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情報セキュリティモデルのこと。

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が問題になる。

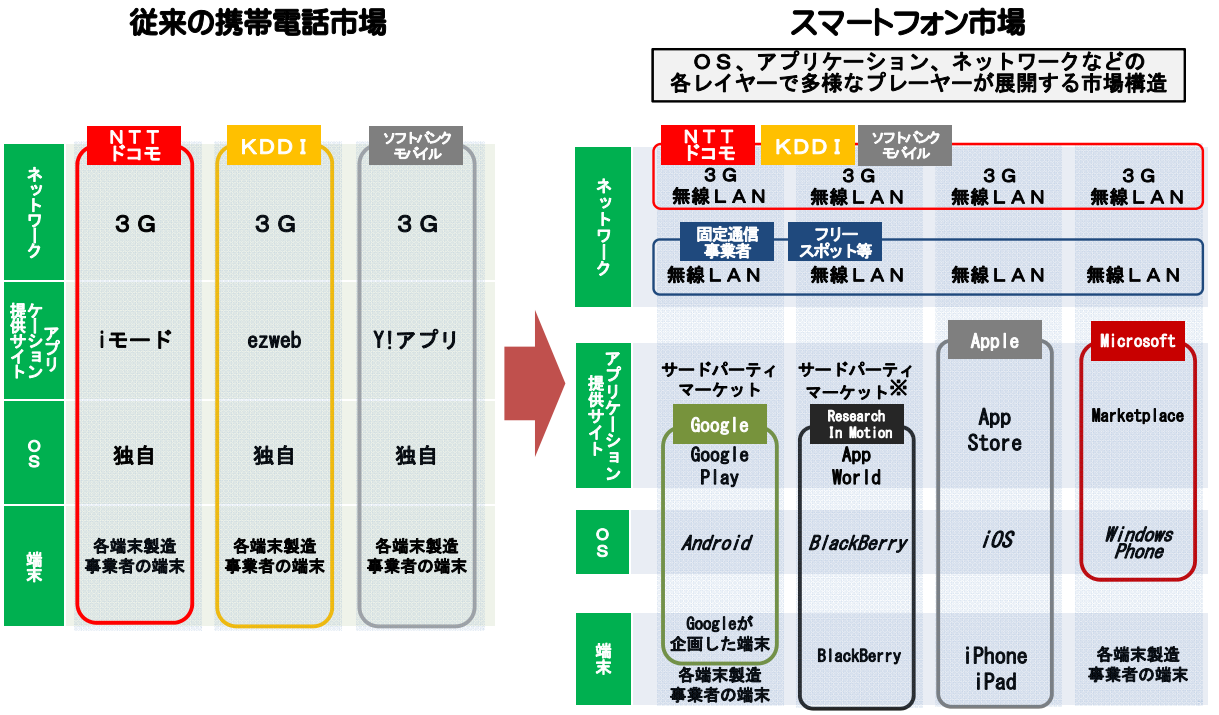
（４）ビジネスモデルの変容

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（表１及び図５）。また、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いる。このようなビジネスモデルの変容は、利用者に届けられるサービスに対する各事業者の責任範囲や一事業者がコントロールできる範囲の変化だけでなく、技術的な対策のあり方にも変化を及ぼしている。

表１　ＯＳ別の市場展開の状況

ＯＳの種類	ＯＳ提供事業者	平成２３年度国内出荷台数(万台)※	特　　徴
Android	(米)Google	1,766	○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	8	○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	390	○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	12	○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）

（事務局調べ。ただし、※は矢野経済研究所提供データ）



※配付可能なアプリケーションは、Research In Motionが電子署名したものに限定される。

図５　ビジネスモデルの変容

第３節　スマートフォンに対する利用者の意識

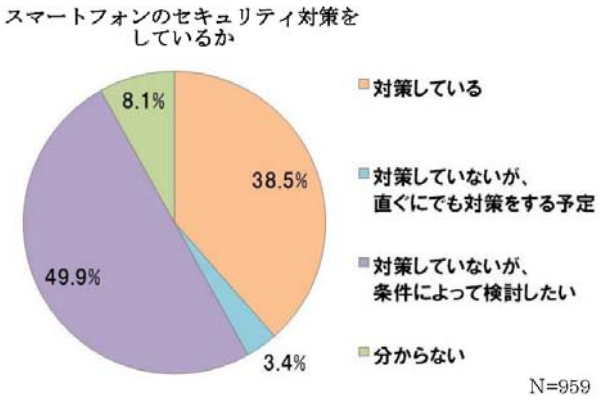
（１）一般利用者の意識

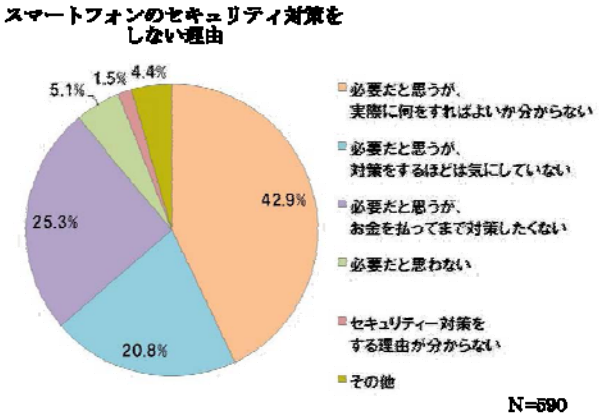
一般利用者は、従来の携帯電話端末と同じ売り場で購入、又は従来の携帯電話端末からの機種変更により、スマートフォンを入手することが多い。そのため、スマートフォンを、従来の携帯電話の延長や高機能な携帯電話端末という意識で利用している利用者も依然多いと考えられる。

民間調査会社のアンケート調査[6]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６－１）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６－２）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危険にさらされるだけでなく、ボット化[7]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。





（株式会社ネットマイル）

図６－１　　図６－２

スマートフォンの情報セキュリティに関する利用者の意識

---

[6] 株式会社ネットマイル「スマートフォンのセキュリティに関する調査」（平成２３年１２月６日）（http://research.netmile.co.jp/voluntary/2011/pdf/201112_1.pdf）

[7] 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。

（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かのモデルは必ずしも確立できていない状況にある。特にスマートフォンの業務利用において、勤務先からの支給端末を用いるのか、又は個人所有の端末を業務に活用する（ＢＹＯＤ[8]と呼ばれる。）戦略を取るのか、ＢＹＯＤを採用する場合の情報セキュリティポリシーをどのように設計するかは企業等における懸案事項となっている。

このような状況の下、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）[9]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、ビジネス利用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。

[8] Bring Your Own Deviceの略。

[9] 名称は当時。同組織は平成２４年４月、任意団体から「一般社団法人日本スマートフォンセキュリティ協会」（ＪＳＳＥＣ）に改組した。

第２章　スマートフォンの情報セキュリティ上の脅威と課題

第１節　スマートフォンの情報セキュリティ上の脅威

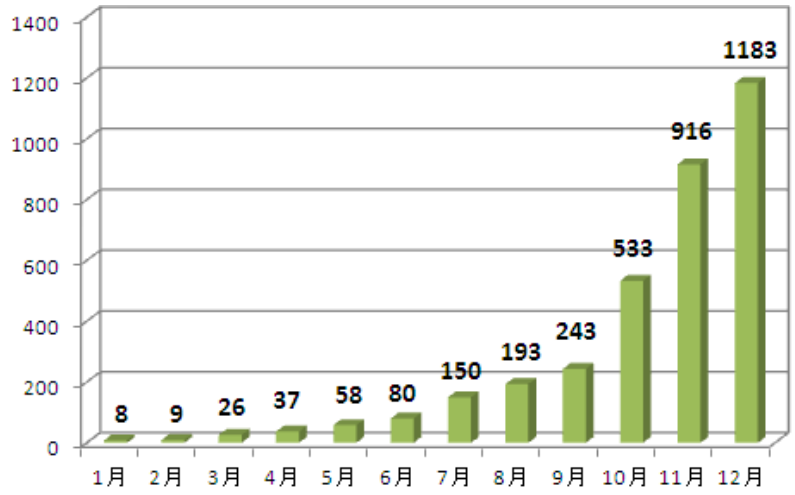
（１）情報セキュリティ上脅威のあるアプリケーション

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、スマートフォンの急速な普及に伴い様々なアプリケーションが開発されているが、その中に、利用者にとって情報セキュリティ上脅威のあるアプリケーションが一部存在している。これらのアプリケーションの中には、①マルウェアを含むアプリケーション、②ぜい弱性を含むアプリケーション、③利用者が明確に意図しない形で利用者情報を外部に送信する機能を持つアプリケーション等が存在するとされている。

ア　スマートフォンを対象としたマルウェア

スマートフォンを対象としたマルウェアが出現しており、その種類は増加傾向にある。現在、発見されているものはAndroidを対象としたものが大半であり、平成２３年後半に大幅な増加を示している[10]（図７）。

一方で、平成２３年前半のマルウェア出現数をＰＣとスマートフォンで比較した場合、スマートフォンのマルウェア数はＰＣの4,000分の１に過ぎないとの調査結果[11]もあり、現状、深刻な被害が蔓延する状態には至っていないと考えられる。



（平成２３年１月１日～１２月３１日／累計）

（トレンドマイクロ株式会社）

図７　Android 端末に感染するマルウェア[12]を検出するパターンファイル数

[10] トレンドマイクロ株式会社「インターネット脅威年間レポート 2011 年度」（http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20120106083242.html）

[11] 総務省「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 スマートフォンを経由した利用者情報の取扱いに関するＷＧ」第１回資料。

[12] 情報セキュリティ事業者により定義・呼称は異なる。

これまでに発見されているマルウェアには、不正課金、情報漏えい、不正操作や管理者権限奪取などを行うものがある（表２）。

表２　マルウェアの事例

発見年月	名称	ＯＳ	概　要	備　考
平成１９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。

（事務局調べ）

マルウェアの脅威は、ＯＳごとに状況が異なる。

iOS及びWindows Phoneについては、ＯＳ提供事業者により設定されている制限を外す行為（いわゆる“Jailbreak(脱獄)”）を行わない限り、ＯＳ提供事業者が運営する公式アプリケーション提供サイト以外からはアプリケーションをインストールできない仕様となっている。BlackBerryについては、公式アプリケーション提供サイト以外からの入手も可能であるが、同社が電子署名したアプリケーションしか端末にインストールできない仕様となっている。また、これら各ＯＳの公式サイトは、独自の基準に基づき、掲載アプリケーションの安全性の事前審査を行っている。以上のことから、BlackBerry、iOS及びWindows Phoneについて、これまでに脱獄をしない通常の端末のマルウェア感染事例は確認されていない。

Androidについては、Google Play（Android Marketを継承した公式サイト）以外のアプリケーション提供サイト（サードパーティマーケット[13]と呼ばれる。）を通じて配布されるアプリケーションも多数作成され、利用者側の端末の設定変更

[13] 携帯電話事業者等が運営するサイトから、個人が運営するサイトまで、様々な種類のアプリケーション提供サイトが存在する。

[14]により、インストールが可能になっている。これまでに発見されたAndroidを狙ったマルウェアは、海外のサードパーティマーケットで発見されたものが多い。

Android Market（当時）に掲載されるアプリケーションについて、Googleは従来、公式サイト側で事前審査は行わない（アプリケーション開発者がAndroid Marketの掲載ポリシーに合致していることを自己審査）という方針を取っているため、過去にマルウェアを含むアプリケーションが掲載された例があるが、発見され次第、公式サイト及びダウンロードした利用者端末から削除する措置がとられていたため、本研究会の中間報告の時点では大きな被害が確認されていなかった。さらに、平成２４年２月、Googleは公式サイトからマルウェア等を排除するため、アプリケーションの自動解析を行うシステム[15]を稼働させていることを表明した。

一方、平成２４年１月、Androidを対象とした架空請求詐欺アプリケーションで、ウェブサイトにおいてインストールを促すものが我が国で確認され、平成２４年３月現在、消費生活センター等に感染の疑いのある相談が寄せられる事態が生じている[16]。

イ　ぜい弱性を含むアプリケーション

ぜい弱性には、コーディング[17]上の問題に起因するものと、仕様・設計上の問題に起因するものなどがある。

例えば、コーディングのミスにより生じたアプリケーションのメモリ関連のぜい弱性を悪用し、ＯＳのぜい弱性への攻撃、不正な情報アクセス等を行う悪意のあるプログラムを実行させることが可能となる。ＯＳのぜい弱性を攻撃された場合には、管理者権限奪取の脅威が、不正に情報にアクセスされた場合には情報漏えいの脅威が存在する。

また、仕様・設計上のミスにより、重要なデータの格納場所や暗号化設定などが不適切な場合、情報漏えいを引き起こす脅威が存在する。

ウ　利用者が意図しない利用者情報の外部送信を行うアプリケーション

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スマートフォンに蓄積されている。

---

[14] Android端末の設定画面で「提供元不明のアプリ」という項目にチェックを入れることで、Google Play以外のアプリケーション提供サイトからのインストールが可能になる。（初期状態では当該チェックは入っていない。）

[15] Google Japan Blog（平成２４年２月６日付記事）
（http://googlejapan.blogspot.jp/2012/02/android.html）

[16] 東京都広報（http://www.shouhiseikatu.metro.tokyo.jp/sodan/kinkyu/120323.html）

[17] ソフトウェアの仕様や設計に基づきプログラムを記述する作業。

これらの利用者情報を、利用者が明確に意図しない形で、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[18]等のプログラムが存在すると指摘されている。平成２４年４月には、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してしまうアプリケーションの存在が確認されている。

（２）端末の紛失等によるデータの漏えい等の脅威

スマートフォンで取り扱うデータに関しては、アプリケーション等による漏えい以外にも、紛失・盗難等による端末内に保存されたデータの紛失・漏えいなどの脅威が存在する。

（３）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脅威は、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、よりその脅威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。

[18] 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節　スマートフォンの情報セキュリティ上の課題

前節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問題点、すなわち解決すべき課題を整理する。検討領域と各領域間の情報のやり取りを図示すると、図８のようになる。

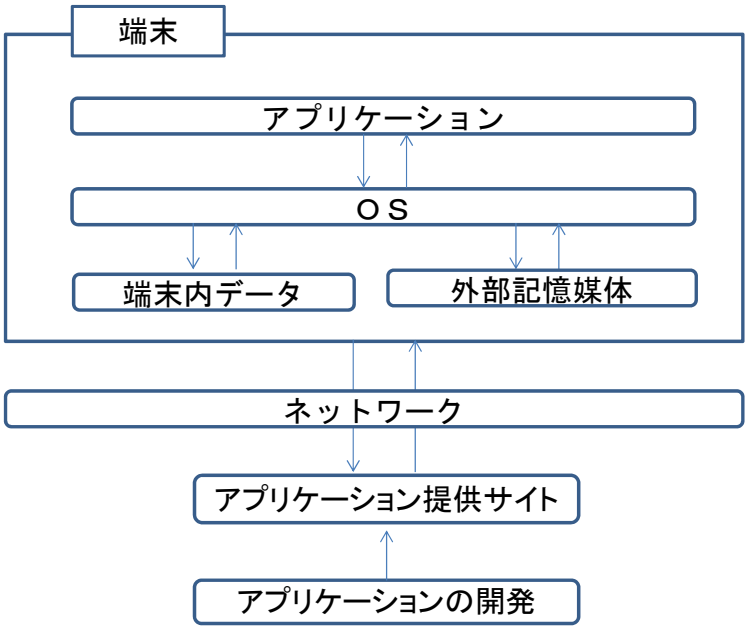


図８　スマートフォンの情報セキュリティ上の課題の検討領域

また、本節以降で、Ａ、Ｂ、ｉ及びＷとあるのは、それぞれ、Android、BlackBerry、iOS及びWindows Phoneに関する事項であることを示している。なお、この記述は、現時点におけるものであり、新たな脅威の発生等により変更される可能性がある。

（１）ＯＳの課題

ア　ぜい弱性に関する課題【Ａ、Ｂ、ｉ、Ｗ】

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危険性が指摘されている。

イ　ＯＳのバージョンアップ・セキュリティパッチへの対応に関する課題【Ａ、Ｗ】

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[19]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。そのため、マルウェア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。

ウ　ＯＳのサポート期間に関する課題【Ａ、Ｂ、ｉ、Ｗ】

現在、新しいバージョンのＯＳが公表された後に、旧バージョンのＯＳに対してセキュリティパッチの提供をいつまで行うかなど、旧バージョンのＯＳのサポート期間が不明なＯＳも存在する。利用者が同じ端末を長期間使用する場合など、端末の制約により新しいＯＳへのバージョンアップができず、旧バージョンのＯＳのままのスマートフォンが使用され続けるケースが想定されるが、その際、仮にサポート期間が終了すると、利用者が、その後セキュリティパッチの提供が行われないＯＳを使用し続けるという課題が発生する[20]。

エ　ＯＳのサポートの提供ルートに関する課題【Ａ、Ｂ】

ＯＳのセキュリティパッチの提供形態として、携帯電話事業者のネットワークを通じた配布のみが行われている場合がある。そのようなＯＳの端末については、携帯電話事業者との解約後に、原則、ＯＳのサポートが受けられないという課題がある。

高機能なスマートフォン端末に関しては、携帯電話事業者との解約後にも、携帯電話事業者のネットワークを用いた通話・通信以外の機能を使い続ける利用者の存在が指摘されている。これらの機能のうち、特に無線ＬＡＮ機能が引き続き使用可能であることにより、携帯電話事業者との解約後の端末が、ＯＳのサポートを受けられないままに、マルウェアへの感染等による情報漏えいの危険性にさらされるという課題が発生する[21]。

（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、利用者にとって情報セキュリティ上脅威のあるアプリケーションが一部で作成されており、利用者がこれらをインストールすることが、現時点において、情報セキュリティ上最も危険性が高いと指摘されている。

前節の脅威の中でも述べた通り、利用者にとって脅威のあるアプリケーションには、マルウェアを含むアプリケーション、ぜい弱性を含むアプリケーション、利用

[19] 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。
[20] 端末の仕様や端末製造事業者のセキュリティ機能強化対策等により、当該セキュリティパッチに関するＯＳのぜい弱性が顕在化しないこともある。
[21] 同上。

者が意図しない利用者情報の外部送信を行うアプリケーション等が存在する。このうち、利用者情報の外部送信を行うアプリケーションについては、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ある。これらの課題については、本研究会の中間報告にて指摘し、保護すべき情報そのものに関する議論の必要性から、別途検討の場を設けて詳細な検討を進めることが適当であるとしたところ、その後、総務省の「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」の下の「スマートフォンを経由した利用者情報の取扱いに関するＷＧ」において検討が行われていることから、以下では前二者、すなわちマルウェアを含むアプリケーション及びぜい弱性を含むアプリケーションに関する課題を取り扱うこととする。

ア　マルウェアやぜい弱性を含むアプリケーションの作成に関する課題【Ａ、Ｂ、ｉ、Ｗ】

マルウェアやぜい弱性を含むアプリケーションが作成される原因については、悪意ある開発者が意図的にマルウェアを組み入れる場合のほか、開発者の知識・認識不足が原因となり、意図的でなく、マルウェアを含んだモジュール等を組み入れてしまう場合や、ぜい弱性を残してしまう場合がある。そのため、開発者の技術レベルの向上やモラル教育などが課題となっている。

イ　マルウェアやぜい弱性を含むアプリケーションの流通に関する課題【Ａ、Ｂ、ｉ、Ｗ】

マルウェアやぜい弱性を含むアプリケーションに対するチェック機能が不完全な場合、アプリケーション提供サイトにそれらが流通する課題が存在する。新しいマルウェアやぜい弱性が今後も作成されることが想定される状況に鑑みれば、これらのチェック機能を完全に担保することは困難であるが、関係者の努力により、流通を可能な限り阻止していくための方策を講ずることが必要である。

ウ　マルウェアやぜい弱性を含むアプリケーションのインストールに関する課題【Ａ、Ｂ、ｉ、Ｗ】

利用者が、マルウェアやぜい弱性を含むアプリケーションをインストールしてしまう課題が存在する。

マルウェア対策ソフトが提供されているＯＳでは、その使用が、マルウェアやぜい弱性を含むアプリケーションのインストール防止対策として一定程度有効である。しかし、サンドボックスを採用しているスマートフォンＯＳの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マルウェア対策ソフトは、原則として他のアプリケーションの動きや内容を監視することができないという構造上の限界を抱えている等の課題が指摘されている。

（３）ネットワークの課題【Ａ、Ｂ、ｉ、Ｗ】

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について、そのアクセスポイントの増設やサービスの無料提供を表明している。その他、市中には携帯電話事業者以外の事業者が設置する公衆無線ＬＡＮも多数存在する。

スマートフォンから公衆無線ＬＡＮを利用する機会は今後も拡大していくと見込まれるが、現状、公衆無線ＬＡＮの中には、ぜい弱性が指摘されている暗号方式や認証方式を使用しているものが存在するという課題がある。また、従来の携帯電話が、基本的に携帯電話事業者の通信設備を利用する通話・通信のみを行っていたのに対し、スマートフォンでは、携帯電話事業者以外の事業者が設置する公衆無線ＬＡＮを利用することが可能であり、その無線ＬＡＮに対しては、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【Ａ、Ｂ、ｉ、Ｗ】

スマートフォンは常に携帯して使用するという性質上、紛失・盗難に遭う危険性はＰＣよりも高い。また、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危険性や、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[22]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危険性も指摘されている。

（５）スマートフォンが外部ネットワークに及ぼす影響【Ａ、Ｂ、ｉ、Ｗ】

スマートフォンの利用者側から見て、利用者自身の端末及び情報を守る観点からの課題だけではなく、スマートフォンの情報セキュリティ対策が不十分であるために、スマートフォンが様々なサイバー攻撃やサイバー犯罪に利用される可能性が存在するという課題、スマートフォンの通信が帯域ひっ迫を引き起こすこと等の視点からの課題も存在する。

現在、大規模な事象の発生は報告されてはいないが、スマートフォンが不正に操作されるマルウェアに感染した場合には、同様のマルウェアに感染したＰＣ同様、当該スマートフォンがDDoS攻撃やＰＣ等へのマルウェア感染活動等サイバー攻撃の踏み台に利用されるという危険性も想定される。また、スマートフォンによる

[22] 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などに、システムの消去などを行う機能。

Wi-Fiテザリング[23]の機能が利用されるようになってきているが、接続の設定を適切に行わなければ、付近の想定していない端末からの接続を許し、同様に、様々なサイバー犯罪の踏み台として利用される危険性も想定される。

（６）ビジネスモデルの変容に伴う課題【Ａ、Ｂ、ｉ、Ｗ】

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を認識する必要がある。

[23] スマートフォンを無線ＬＡＮのアクセスポイントとして利用し、携帯電話事業者のネットワーク等を使って、無線ＬＡＮ対応のパソコンやゲーム機器等をインターネットに接続させること。

第３章　事業者及び政府における対策

本章では、第２章第２節で述べたスマートフォンが直面する課題ごとに、事業者及び政府において取られるべき対策、積極的な検討が望まれる対策等を提示する。

第１節　対策の検討に当たっての基本的考え方

（１）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るようにすることが重要である。

（２）利用者の意識向上の重要性

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が大きな利点となっている。一方で、その利点により、サービス提供者側の対策のみによってスマートフォンの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講ずることが必要である。

したがって、事業者及び政府は、自らが情報セキュリティ対策に関する取組を実施することに加え、利用者に対し情報セキュリティ対策の必要性や具体的方法等に関する啓発を行い意識を向上させるとともに、利用者が情報セキュリティ対策を取りやすい環境整備を行うなど、サービス提供者側における対策と利用者側における対策とを車の両輪として推進していくことが重要である。

（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、本最終報告は、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の動作性や、バッテリーの消耗などに配慮し、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）ＯＳ等による対策の違い

スマートフォンＯＳ（Android、BlackBerry、iOS及びWindows Phone）は、ＯＳによって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、次節以下では、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。

第２節　課題に関する事業者における対策

本節及び次節では、第２章第２節で指摘した課題ごとに具体的な対策を提示する（次ページ図９）。本節では、特にＯＳ提供事業者やアプリケーション提供サイト運営者と断らない限り、携帯電話事業者、端末製造事業者、情報セキュリティ事業者等における対策を提示することとする。また、本節で提示した対策を一覧にしたものを別添１とした。

（１）ＯＳに関する対策

ア　ＯＳのぜい弱性の修正とその修正版の提供【Ａ、Ｗ】

ＯＳのぜい弱性は、ＯＳのバージョンアップや、ＯＳ提供事業者により発行されるセキュリティパッチにより修正されるため、それらを可能な限り速やかに利用者端末に適用していくことが求められる。

この課題に対しては、ぜい弱性の内容に応じて優先順位を付ける、携帯電話事業者との連携を強化するなど、可能な限り速やかな利用者への通知やＦＯＴＡ[24]対応を実現することが、端末製造事業者の取組として引き続き求められる。その際、ＯＳのバージョンアップやセキュリティパッチが不十分な形で提供され、かえってＯＳの情報セキュリティレベルが落ちることにならないように留意すべきである。

イ　ＯＳのぜい弱性情報の発見と共有【Ａ、Ｂ、ｉ、Ｗ】

ＯＳのぜい弱性への早期対応を行うとの観点から、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、事業者団体の枠組みにおいて事業者が連携して把握し、対応方策を検討する取組が有効である。その際、ぜい弱性情報の悪用防止という見地から、情報共有の範囲は厳密に取り扱い、既存のソフトウェアのぜい弱性情報共有の取組との連携に十分に留意する必要がある。

さらに、ぜい弱性を早期に検出するため、検査ツールなどの開発も重要である。

ウ　ＯＳのサポート期間に関する対策【Ａ、Ｂ、ｉ、Ｗ】

サポート期間を過ぎたＯＳを利用者が知らずに使用し続ける危険性を軽減させるため、ＯＳ提供事業者は、サポートを終了する場合には事前に公表することが望ましい。

エ　ＯＳのサポートの提供ルートに関する対策【Ａ、Ｂ】

携帯電話事業者との解約後にＯＳのサポートが受けられない等の課題に対しては、解約時に、携帯電話事業者から利用者に対して、注意喚起を行うことが必要である。

---

[24] 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。

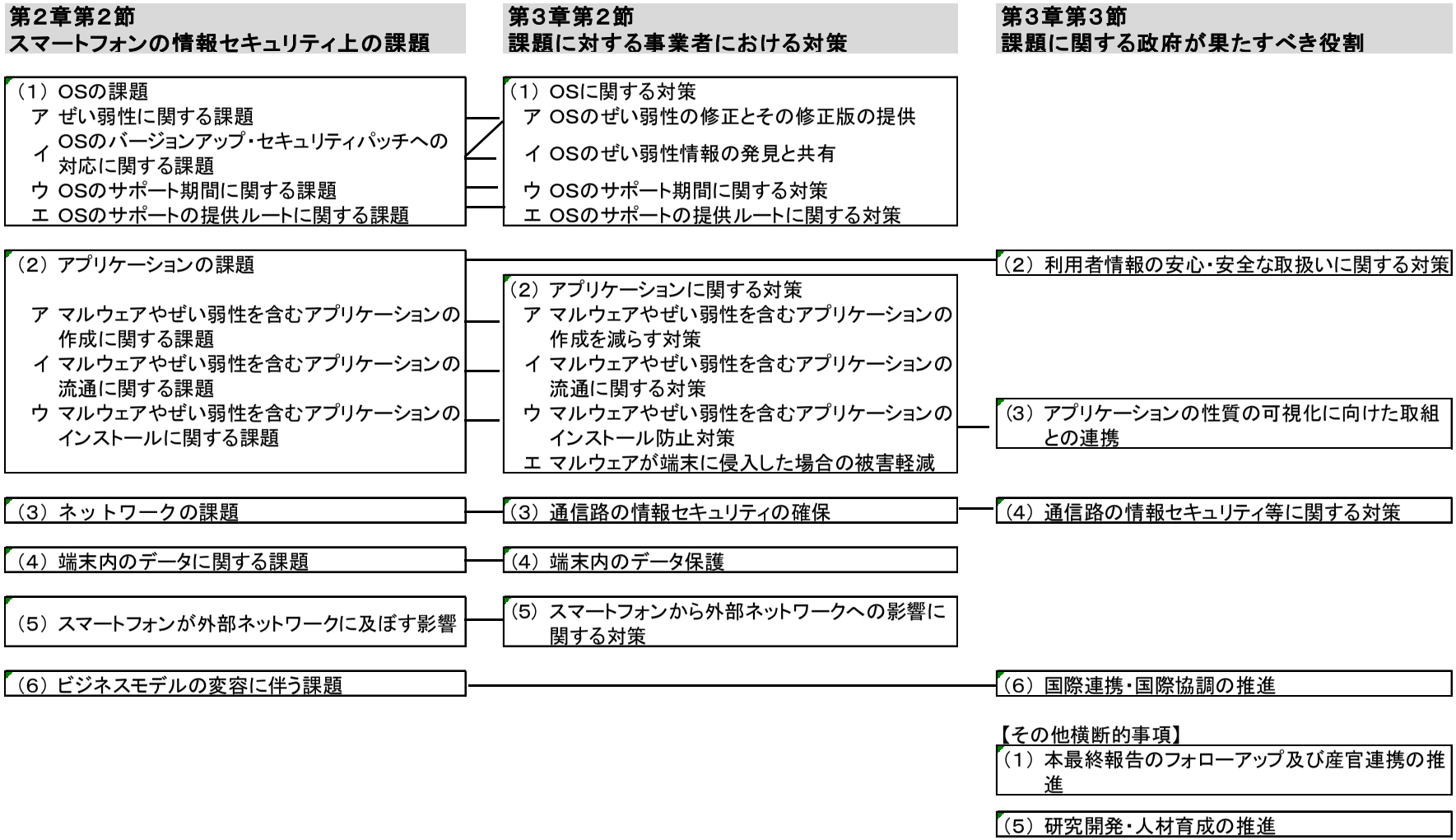

第２章第２節
スマートフォンの情報セキュリティ上の課題
第３章第２節
課題に対する事業者における対策
第３章第３節
課題に関する政府が果たすべき役割
（１）OSの課題
ア ぜい弱性に関する課題
イ OSのバージョンアップ・セキュリティパッチへの対応に関する課題
ウ OSのサポート期間に関する課題
エ OSのサポートの提供ルートに関する課題
（１）OSに関する対策
ア OSのぜい弱性の修正とその修正版の提供
イ OSのぜい弱性情報の発見と共有
ウ OSのサポート期間に関する対策
エ OSのサポートの提供ルートに関する対策
（２）アプリケーションの課題
ア マルウェアやぜい弱性を含むアプリケーションの作成に関する課題
イ マルウェアやぜい弱性を含むアプリケーションの流通に関する課題
ウ マルウェアやぜい弱性を含むアプリケーションのインストールに関する課題
（２）アプリケーションに関する対策
ア マルウェアやぜい弱性を含むアプリケーションの作成を減らす対策
イ マルウェアやぜい弱性を含むアプリケーションの流通に関する対策
ウ マルウェアやぜい弱性を含むアプリケーションのインストール防止対策
エ マルウェアが端末に侵入した場合の被害軽減
（２）利用者情報の安心・安全な取扱いに関する対策
（３）アプリケーションの性質の可視化に向けた取組との連携
（３）ネットワークの課題
（３）通信路の情報セキュリティの確保
（４）通信路の情報セキュリティ等に関する対策
（４）端末内のデータに関する課題
（４）端末内のデータ保護
（５）スマートフォンが外部ネットワークに及ぼす影響
（５）スマートフォンから外部ネットワークへの影響に関する対策
（６）ビジネスモデルの変容に伴う課題
（６）国際連携・国際協調の推進
【その他横断的事項】
（１）本最終報告のフォローアップ及び産官連携の推進
（５）研究開発・人材育成の推進

図９　課題と対策の対応

（２）アプリケーションに関する対策

ア　マルウェアやぜい弱性を含むアプリケーションの作成を減らす対策【Ａ、Ｂ、ｉ、Ｗ】

開発者の知識・認識不足によりマルウェアやぜい弱性を含むアプリケーションが作成されてしまう課題については、セキュアプログラミング技術やモジュール[25]に関する知識などについて、開発者への教育・啓発行っていくことが有効である。開発者は、個人から企業等の技術者まで様々な層からなるため、多くの層の開発者に対する具体的な教育・啓発が重要となる。

ＪＳＳＥＣでは、サンプルコードを含むセキュアプログラミングガイドの作成が行われている。具体的な手法やプログラムを、幅広い開発者層が習得できるようにするため、同団体のウェブサイト、セミナーや専門誌など開発者の目に触れやすい媒体を駆使して、この種の最新のガイドを掲載していくことが推奨される。また、ＯＳやＳＤＫ[26]、モジュールは絶えず新しいバージョンが出現することから、ガイドやサンプルコードの内容は、継続的に検証・見直しが行われることが適当である。

さらに、アプリケーション提供サイト運営者や端末製造事業者は、ウェブサイトを通じたプログラミングガイドや開発関連ツールの提供、開発者向け説明会の取組の中で、情報セキュリティ確保の観点からの情報提供を行っていくことが推奨される。くわえて、現在、市場におけるスマートフォンのアプリケーション開発者の需要は伸びており、プログラミング技術者を抱える企業による社員教育や、開発者コミュニティ[27]による自主セミナー等の活動も活発化していることから、これらの機会も活用して、開発者の情報セキュリティレベル向上に資する知識の教育・啓発に取り組むことが奨励される。

イ　マルウェアやぜい弱性を含むアプリケーションの流通に関する対策【Ａ、Ｂ、ｉ、Ｗ】

ＯＳ提供事業者や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では、マルウェアやぜい弱性を含むアプリケーションを排除するための取組が行われている（表３及び表４）。現状、アプリケーションの掲載基準等について国内外に統一的な標準はなく、各アプリケーション提供サイト運営者が独自のアプリケーション掲載方針に基づき、運営を行っている。

アプリケーション提供サイト運営者には、安全なアプリケーションを求める利用者からの期待に配意し、引き続き各自の取組を継続・改善していく努力が求められる。また、利用者がそれぞれのアプリケーション提供サイトの信頼性を判断できるようにするため、各サイトは、自社サイトの運営方針やアプリケーション掲載方針について、利用者への情報開示を行うことが望ましい。

---

[25] モジュールとは、ひとまとまりの機能を実現する部品に相当するプログラムのこと。

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

[27] 「日本アンドロイドの会」等のコミュニティが存在する。

さらに、アプリケーション掲載にあたっての最低限の基準については、今後、各アプリケーション提供サイト運営者が連携して、利用者の視点に立ち、可能な限り統一していくことが望ましい。

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				
運営者	名称	種別	提供対象	登録数	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
Google	Google Play	ｱﾌﾟﾘｹｰｼｮﾝ配信	Android端末	45万以上（平成24年3月）	○	○	掲載されるとすぐに、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もとに調査。	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	App World	ｱﾌﾟﾘｹｰｼｮﾝ配信	BlackBerry端末	約6万（平成24年3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もとに調査。	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。
Apple	App Store	ｱﾌﾟﾘｹｰｼｮﾝ配信	iPhone端末※1 iPad端末※1	約58.5万（平成24年2月末）	×	×※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、及び利用者からの報告をもとに調査。	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。
Microsoft	Market-place	ｱﾌﾟﾘｹｰｼｮﾝ配信	Windows Phone端末※1	約6.4万以上（平成24年3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。	開発者等からの報告をもとに調査。	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。

※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。

（事務局調べ）

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						
					掲載ポリシー				
運営者	名称	種別	提供対象	登録数	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	ｱﾌﾟﾘｹｰｼｮﾝ紹介	ＮＴＴドコモのAndroid端末	約1,000（平成24年3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もとに調査。	提供サイトから削除。
	dﾒﾆｭｰ	ｱﾌﾟﾘｹｰｼｮﾝ提供ｻｲﾄの紹介	ＮＴＴドコモのAndroid端末	約4,800サイト（平成24年3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、ﾄﾞ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もとに調査。	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	ｱﾌﾟﾘｹｰｼｮﾝ配信	ＫＤＤＩのAndroid端末	約7,500（平成24年4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繋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、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（これまで該当無し）。 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。
ｿﾌﾄﾊﾞﾝｸﾓﾊﾞｲﾙ	@アプリ	ｱﾌﾟﾘｹｰｼｮﾝ紹介	ソフトバンクモバイルのAndroid端末	約2,000（平成24年4月）	×	×※	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。	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もとに調査。	提供サイトから削除。

※　開発者アカウントの登録画面で公開しているが、当該画面のＵＲＬはアカウント申請者のみに個別に通知。（当該画面のＵＲＬ自体には誰でもアクセス可能）

（事務局調べ）

ウ　マルウェアやぜい弱性を含むアプリケーションのインストール防止対策

①　マルウェア対策ソフト【Ａ、Ｂ】

マルウェア対策ソフトは、マルウェアを含むアプリケーションのインストール防止対策として一定程度有効である。したがって、マルウェア対策ソフトの機能の向上を図るとともに、その普及に努める必要がある。

マルウェア対策ソフトが構造上の制約を抱えている課題については、システム部分への特権的なアクセス権限を付与する端末を開発するという解決策が検討されている。一方で、その取組について、特権的なアクセス権限の付与は、ＯＳ本来の情報セキュリティモデルを変更することになるため、当該マルウェア対策ソフトにぜい弱性が存在した場合等に新たな脅威を生むという指摘も存在する。今後の取組にあたっては、当該指摘を考慮した慎重な検討が必要であろう。

また、別の解決策として、端末開発に際してカーネル部への情報セキュリティ対策を強化することで、通常のマルウェア対策ソフトとの併用により、特権的なアクセス権限を付与されたマルウェア対策ソフトを要することなく、それと同等の効果を実現することを志向する事業者も存在する。

②　モバイル端末管理（ＭＤＭ）【Ａ、Ｂ、ｉ、Ｗ】

マルウェア対策ソフト以外の対策として、ビジネスで利用されるモバイル端末管理（ＭＤＭ）の概念を個人利用端末に応用できないかという検討課題がある。企業においてスマートフォンを業務に利用する際には、当該企業のシステム管理者が、自社の情報セキュリティポリシーに従い、業務に利用される端末[28]の設定、ソフトウェアのバージョン管理、導入アプリケーションの制限等を総合的に行うモバイル端末管理を採用し、それによりマルウェアの感染等を防止している場合がある。このような統一的なポリシーに基づくスマートフォンの管理ソリューションは、まだ一般利用者の端末向けに提供されている例は少ないが、実現されれば高いレベルの情報セキュリティを確保することができると考えられる。

したがって、一般利用者向けのモバイル端末管理の手法について、検討していくことが重要である。その際、多様な端末を保持する一般利用者への対応を行うにあたっては、ＭＤＭ提供事業者が常に最新バージョンのＯＳに対応する必要があるなど、実現に向けた課題も多いと指摘されているため、留意が必要である。

③　アプリケーションの性質の可視化の枠組み【Ａ】

Androidでは、公式サイトGoogle Play以外の多くのサードパーティマーケッ

[28] 企業支給端末を利用する場合と、私物端末を業務にも利用する場合（ＢＹＯＤ）とがある。

トや一般のウェブサイトにおいても、アプリケーションが自由に掲載され、そこからインストールされている。そのため、「イ」で述べたアプリケーション提供サイト運営者による取組に加え、アプリケーションそのものの性質を利用者が把握できる枠組みを構築し、当該性質を利用者にも公開していくことが検討されるべきである。

また、アプリケーションの性質の解析や可視化等のツールなどの開発も検討されるべきである。

エ　マルウェアが端末に侵入した場合の被害軽減

完ぺきな情報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軽減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。

①データやデバイスへのアクセスに関するＯＳによる動的制御【Ａ、Ｂ、ｉ、Ｗ】

アプリケーションのインストール時に、利用者の承認を経て、サンドボックスモデルが有効に機能しなくなる場合がある。その場合に備え、ＧＰＳや無線ＬＡＮの利用のON/OFF機能に加えて、電話帳データや端末内に保存されているデータ、発呼機能やＳＤカード等へのアクセスについても、利用者がＯＳの設定変更でアプリケーションごとに柔軟にON/OFFできるようになれば、マルウェアやぜい弱性を含むアプリケーションを万が一インストールしてしまった場合でも、その被害を軽減することが可能となる。

これらの対策を各端末製造事業者が実施することは困難又は非効率的であると考えられるため、ＯＳ提供事業者により、ＯＳへの実装が検討されることが望ましい。ただし、その検討に当たっては、データやデバイスへのアクセスを前提として設計されているアプリケーションが存在することに留意することが必要である。

②カーネル部への情報セキュリティ対策【Ａ】

カーネル部への情報セキュリティ対策として、アプリケーション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を軽減することが可能となる。

（３）通信路の情報セキュリティの確保【Ａ、Ｂ、ｉ、Ｗ】

公衆無線ＬＡＮの情報セキュリティ向上の前提として、ＷＰＡ[29]やＷＰＡ２[30]といった暗号技術を活用した無線ＬＡＮのアクセスポイントについて、その普及を無線ＬＡＮアクセスポイント提供事業者[31]等が推進することが重要である。同時に、情報セキュリティレベルを向上させるために、ＳＳＬ[32]やＶＰＮ[33]等の活用を広く進めることが重要である。

端末製造事業者における対策としては、例えばスマートフォン端末側で接続先を識別し、回線の信頼度に応じて保護レベルを変更できる仕組みを端末に導入することが考えられる。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、引き続き実装していくことが適当である。

（４）端末内のデータ保護【Ａ、Ｂ、ｉ、Ｗ】

紛失・盗難対策として、まずは普段からパスワード等による端末ロックを設定しておくことが必須である。次に、実際に紛失・盗難に遭った際には、遠隔消去や自己消去機能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。これらの事項について、事業者から利用者に対して、第４章に述べる啓発の際に併せて伝えることが適当である。

端末内やＳＤカードからの情報漏えいという課題への対策としては、端末内やＳＤカード内のデータを暗号化し、データが漏出しても内容が知られることのない仕組みを端末に導入することが有効である。

（５）スマートフォンから外部ネットワークへの影響に関する対策【Ａ、Ｂ、ｉ、Ｗ】

スマートフォンを踏み台にした攻撃の可能性について、事業者から利用者に対して、第４章に述べる啓発の際に併せて伝えることが検討されるべきである。

その上で、利用者は、自身の端末を守る観点からと同様に、端末へのマルウェアの侵入・感染の防止対策等を行うことが必要である。そのほか、スマートフォンによるWi-Fiテザリングの機能を利用する場合には、無線ＬＡＮルータ同様に、強固

---

[29] 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。

[30] 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。

[31]オフロード先としての無線ＬＡＮアクセスポイントの場合、携帯電話事業者が設置主体となりうる。

[32] 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。

[33] 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、専用回線並みの情報セキュリティを実現するサービスのこと。

な暗号化方式を用いる、適切にパスワードを管理する等、設定や取扱いに留意することが必要である。

第３節　課題に関する政府が果たすべき役割

本節では、第２章第２節で指摘した課題のうち、前節で対策を示したもの以外の課題等について、政府が果たすべき役割を提示する。

（１）本最終報告のフォローアップ及び産官連携の推進

第４章で述べる普及啓発方策について、自ら引き続き積極的に推進するとともに、事業者等が協調して普及啓発を実施することを促進することも重要である。また、事業者における技術的な対策やその検討における連携を促すことも重要である。

したがって、技術的な対策や利用者への普及啓発等ついて、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ほか、事業者や政府等の取組を、半年に１回程度事務局が調査しその結果を公にしていくことが適当である。

また、事業者等が中心となって検討する施策に関しても、将来に亘り事業者等だけでは十分な成果が期待できない場合には、政府による支援策も検討する必要がある。

（２）利用者情報の安心・安全な取扱いに関する検討

総務省の「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」の下の「スマートフォンを経由した利用者情報の取扱いに関するＷＧ」においては、平成２４年１月から、スマートフォンにおける利用者情報が安心・安全な形で活用され、利便性の高いサービス提供につながるよう、現状と課題や必要な対応等について調査・検討を行い、同年４月に中間取りまとめを公表したところである。今後は、利用者情報の性質・分類、事業者による利用者情報の適切な取得・管理・利用のあり方[34]等について、引き続き検討を進めるとともに、検討結果を踏まえた対応を行うこととしている。

（３）アプリケーションの性質の可視化に向けた取組との連携

アプリケーションのインストールに関する課題については、前節で、アプリケーション提供サイト運営者による掲載方針に関する取組や、それに加えて事業者団体によるアプリケーションの性質の可視化に関する取組を提示したところであるが、政府は、調査研究や必要な協力を通じて、これらの取組との連携を図っていくことが適当である。

（４）通信路の情報セキュリティ等に関する対策

無線ＬＡＮに関しては、近年公衆無線ＬＡＮがさまざまなサービス主体により提供されるようになり、同時にオフロード、ビジネス活性化、地方活性化、災害対応

[34] 具体的には、スマートフォンのサービス構造において関与する多様な事業者や各関係者において、個人情報に関する法令遵守やプライバシーの保護、利用者の不安感に対する配慮等の観点から利用者情報の取り扱いをどのように行う必要があり、また望ましい取組はどのようなものであるか検討を深める。

等の観点から積極的な活用が期待されている。本年３月には、無線ＬＡＮの現状を整理し、安心・安全な利用や普及に関する課題及び必要な方策の検討を目的として、「無線ＬＡＮビジネス研究会」が総務省に設置され、情報セキュリティ対策及び利用者啓発についても検討対象とされたところである。

総務省としては、「無線ＬＡＮビジネス研究会」における検討を進めるとともに、検討結果を踏まえた対応を行っていくことが重要である。また、利用者が安全に無線ＬＡＮを利用するための手引書として、「安心して無線ＬＡＮを利用するために」を策定しているが、技術動向の変化やスマートフォンからの利用、スマートフォンによるWi-Fiテザリングの機能の利用が進んでいることなどから、同研究会の動向・成果も踏まえながら、同手引書の改訂を行うことが必要である。

（５）研究開発・人材育成の推進

スマートフォンの情報セキュリティ上の脅威は、今後、高度化・複雑化が想定されることから、政府は、利用者保護の観点から求められる技術等について積極的に研究開発を推進するとともに、新たな脅威に的確に対応するため中長期的な視点から人材育成策に取り組むべきである。

（６）国際連携・国際協調の推進

スマートフォンのＯＳや端末のビジネスモデルは、ひとつの国や地域に閉じたものになっていないことから、世界共通の仕様であるグローバルモデルの端末が国内市場にも多く投入されているため、スマートフォンの情報セキュリティ上の脅威は、国や地域に関わりなく、スマートフォンを利用する上で共通のものであり、共有できるものでもある。また、スマートフォンにおいて扱われるアプリケーションやサービスは、国や地域を越えたビジネスとなっていることから、そこに存在する情報セキュリティの課題の中には、我が国だけでは解決できないものも存在する。

そのため、具体的な脅威やそれに関する課題や対策について、海外との情報交換や意見交換を行っていくことは重要であり、これらは、国際的な枠組みで論じられるべき内容である。また、単に情報セキュリティに関連する情報を国際的に共有するだけでなく、認識される課題を国際的な枠組みの中で解決していく取組も重要となる[35]。その際、我が国のグローバルな発言力を強化するという観点から、脅威や課題について問題提起を行うことにより、国際社会の理解を得ながら、対策手法等についての情報交換や意見交換を継続的に行っていくことが重要である。さらに、

[35] これらの取組のひとつとして、国際標準化に向けた活動を挙げることができる。ＩＴＵ－Ｔ（国際電気通信連合電気通信標準化部門）では、スマートフォンの情報セキュリティという視点で議論が開始されており、具体的な国際標準の勧告化に向けて、次に関する寄書が提出されている。
○スマートフォンにおける情報セキュリティに関する事項（脅威、課題、対策例）
○スマートフォンで扱うアプリケーションの管理、運用に関するガイドライン
これらの活動は、現在のところ、日本、韓国などのアジア圏のメンバが主導しているが、今後、欧州（ＧＳＭ関連）や米国（ＮＩＳＴ（米国国立標準技術研究所）等）が関わる形で進んでいくと考えられる。

国際標準化団体の機能を活用し、我が国の知見や海外から情報をもとに、スマートフォンの情報セキュリティ対策に関するベストプラクティスをとりまとめることや、状況に応じ、利用者保護のあり方等に関する国際標準等も視野に入れていくことが適当である。

したがって、政府は、国内における検討だけでなく、国際社会における活動も常に視野に入れ、国際会議や二国間会合の場[36]を捉え、引き続き、積極的な情報交換や意見交換に努め、国際的な協調を図っていくことが重要である。

[36] 昨年１１月の日・ＡＳＥＡＮ情報セキュリティ会議において我が国から問題提起を行い、本年１月には、米国との政府間会合において、スマートフォンの情報セキュリティに関する意見交換を開始。

第４章　一般利用者への普及啓発

第２章で述べた具体的な課題の解決に当たっては、利用者側の意識の向上も必要である。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という観点から、第１節で普及啓発の内容、第２節でその方法について提示する。

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講ず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情報セキュリティに関する意識を高め、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の更新の際には、機能修正・追加のほかに、ぜい弱性の修正が行われることもある。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　Android利用者は、誤ってマルウェアを含むアプリケーション等をインストールすることを避けるため、マルウェア対策ソフトをインストールすることが推奨される。携帯電話事業者が提供する通信時の情報セキュリティに関する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、マルウェアを含む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、携帯電話事業者等が一定の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。インストールする際には、アプリケーションが使用する機能・利用者情報について、内容を理解した上で行うことが重要である。

（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（“Jailbreak(脱獄)”）は、ＯＳの情報セキュリティレベルを下げる可能性があることを認識する必要がある。

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。

ウ　端末の設定において、ＧＰＳの利用をON/OFFする機能が存在することを認識する必要がある。ＧＰＳの利用をOFFにすると、ソーシャル・ネットワーキング・サービス（ＳＮＳ）やアプリケーション等に対して利用者のＧＰＳ情報を秘匿できる一方、遠隔消去等のＭＤＭが有効に機能しない可能性がある。したがって、その選択に当たっては、これらを十分に吟味すべきであるということを、正しく認識することが必要である。

（４）その他

（１）から（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。

迷惑電話や迷惑メールへの対策については、従来の携帯電話と同様の対策[37]が有効である。

以上の事項は、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。

その上で、中間報告では、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、研究会として利用者が最低限取るべき情報セキュリティ対策を、別添２の「スマートフォン情報セキュリティ３か条」[38]としてとりまとめ、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と結論づけた。

---

[37] 各携帯電話事業者のウェブサイトや、迷惑メール対策については、一般財団法人日本データ通信協会迷惑メール相談センターのウェブサイト（http://www.dekyo.or.jp/soudan/index.html）等が参考になる。

[38] 「スマートフォン情報セキュリティ３か条」においては、利用者にとり理解しやすい文言を使用するとの観点から、「マルウェア対策ソフト」のことを、より一般的に使用されている名称である「ウイルス対策ソフト」と記載している。

その後、前述の「スマートフォンを経由した利用者情報の取扱いに関するＷＧ」において、利用者が自らのプライバシーを守るために少なくとも知っておくべきこと、とるべき行動について検討がなされ、「スマートフォン プライバシー ガイド」が取りまとめられた。また、第２章第３節で述べた利用者向けの無線ＬＡＮ利用の手引書である「安心して無線ＬＡＮを利用するために」については、内容の改訂が行われる見込みである。

今後は、本研究会の「スマートフォン情報セキュリティ３か条」と「スマートフォン プライバシー ガイド」及び「安心して無線ＬＡＮを利用するために」を組み合わせながら、利用者に対して、より伝わりやすく効果的な啓発に努め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重要である。

以下では、取組の主体別にその取り組むべき方向性を示すとともに、それぞれの主体が共通に認識すべき事項、及びフォローアップの方法について述べる。

（１）携帯電話事業者の取組

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いる。その内容は、主に各社が独自に情報セキュリティ事業者等と提携して提供している各種情報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、総務省の「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」がとりまとめた「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」（平成２３年１２月２１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が行われている。

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有益であると考えられる。

ア　情報セキュリティ対策の必要性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存在と情報セキュリティ対策の必要性を把握できるような説明を行う等の工夫を行う。

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を行う。

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

策を講ずる。

（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情報セキュリティ上最も危険性が高いとされるのが、情報セキュリティ上脅威のある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情報開示

第３章で提示したように、運営者自身の努力として、運営するサイトからマルウェアやぜい弱性を含むアプリケーションを排除する取組を継続・改善するとともに、そのようなサイトの運営方針やアプリケーション掲載方針について、一般利用者に対し情報を分かりやすく開示していく。このことにより、利用者が自らアプリケーション提供サイトの運営方針に関する情報に接し、判断することや、情報セキュリティの重要性について認識を深める機会となることが期待される。

（３）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、本研究会の中間報告でとりまとめられた「スマートフォン情報セキュリティ３か条」等について、利用者への普及啓発活動を、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、パンフレット作成等を通じて実施[39]してきたところであるが、新聞・雑誌やテレビなどのメディアの活用などを含め、普及啓発をより一層促進していくことが重要である。

---

[39] 昨年１２月の中間報告のとりまとめ以降、政府において実施した主な周知啓発の取組以下のとおり。

○政府インターネットテレビの番組において情報セキュリティに関するテーマを扱い、「スマートフォン情報セキュリティ３か条」を紹介（平成２４年２月～）

○総務省広報誌において、スマートフォンの特徴及び安全な利用に関する特集テーマを掲載（平成２４年２月及び４月）

○情報セキュリティ月間を中心とした全国のセミナー・講演会の場において、「スマートフォン・クラウド３か条」を活用し、スマートフォンの情報セキュリティ対策の重要性を啓発する講演等を実施（平成２４年１月～）

○総務省ウェブサイト「国民のための情報セキュリティサイト」に、「スマートフォン情報セキュリティ３か条」を掲載（平成２４年１月～）

（４）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るが、普及啓発にあたっては、利用者が情報セキュリティに関する情報を欲した際に、容易に入手可能である環境が整備されることが重要である。他方、情報セキュリティに関心のない利用者が情報を入手する際に、情報セキュリティに対する意識を高める情報が目に留まるようにすることも重要である。

前者については、政府、関係事業者、報道機関などから情報発信がなされるようになってきているが、引き続き、サービスの現状や脅威についての正確な情報を継続的に発信する努力が求められる。

後者については、特に、①ＩＣＴリテラシーが未成熟である就学年齢の青少年、②経済的に自立し、自律的な消費者として活動を始める20代前半の成人、③ＩＣＴ利用経験や知識の少ない高齢者、これらの層への情報発信が、他のＩＣＴの安全な利活用方策と同様に、重要であると考えられる。

①については、既存の取組として、民間団体、政府や携帯電話事業者が、学校などの教育機関やＰＴＡ等を対象とした講習会や教材配布の取組[40]を行っており、その内容として、スマートフォンの情報セキュリティ対策を盛り込んでいくことが有効である。

②及び③については、消費者相談等の実事例を豊富に蓄積している消費者団体等との連携を強化していくことが重要である。特に若い世代に対しては、具体的な事例を踏まえながら、インターネット等の若者の利用頻度の高いメディアを通じた情報発信が有効であると考えられる。そのほか、一般に、ＩＣＴの利活用については、世代を問わず身近の詳しい人間に相談するという行動を取る人が多く存在することから、地域社会において、周囲の人々を知識面からサポートできるような人材を育成していく取組[41]も重要である。

（５）関係者の取組のフォローアップ

今後、スマートフォンの情報セキュリティに関する情報発信は発信主体・量・質ともに増加していくことが予想されるため、それらの情報や活動を定期的に取りまとめ、俯瞰することは、取組をより効果的なものとしていくために有効であると考えられる。そのため、技術的な対策や利用者への普及啓発策等について、定期的に情報を発表することにより、関係者による普及啓発の取組等が効果的・継続的に実施されることを期待する。

---

[40] ｅーネットキャラバン（総務省・文部科学省）、安心ネットづくり促進協議会の全国各地域でのシンポジウム、インターネット安全教室（経済産業省）、ケータイ安全教室（ＮＴＴドコモ）、ＫＤＤＩケータイ教室（ＫＤＤＩ）、「考えよう、ケータイ～情報モラル授業プログラム～」（ソフトバンクモバイル）等

[41] このような取組を行っている団体として、例えば「セキュリティ対策推進協議会（ＳＰＲＥＡＤ）」がある。

第５章　スマートフォンからのクラウド利活用に関する情報セキュリティ

本章では、スマートフォンとクラウドとの関係性の視点から、スマートフォンからクラウドを利用した場合のクラウド上のデータ保護に関する脅威、課題及び対策（第２節～第４節）、並びにクラウドをスマートフォンの情報セキュリティ対策の一環として活用する方策（第５節）という二つの観点から考察を行う。

第１節　スマートフォンとクラウドサービスとの親和性

スマートフォンの急速な普及に先行する形で、クラウドサービスの利用が進展している。元来は、企業のＩＴ資源を外部委託化するホスティングサービスに、仮想化技術や高度リソース活用技術を適用することにより、クラウドサービスが誕生した。その後、個人利用者向けのクラウドサービスであるパーソナルクラウドが登場し、更にその市場を拡大している[42]。

スマートフォンは端末としてのデータ格納容量がＰＣに比べ少ない一方、移動先でも多様な通信路からインターネットに接続可能であるという特性を持つことから、データをクラウド上に保存して利用するという形態との親和性が高い（図１０）。現実に、ウェブアプリケーションを介して、スマートフォンからクラウドを利用する形態が増加している。

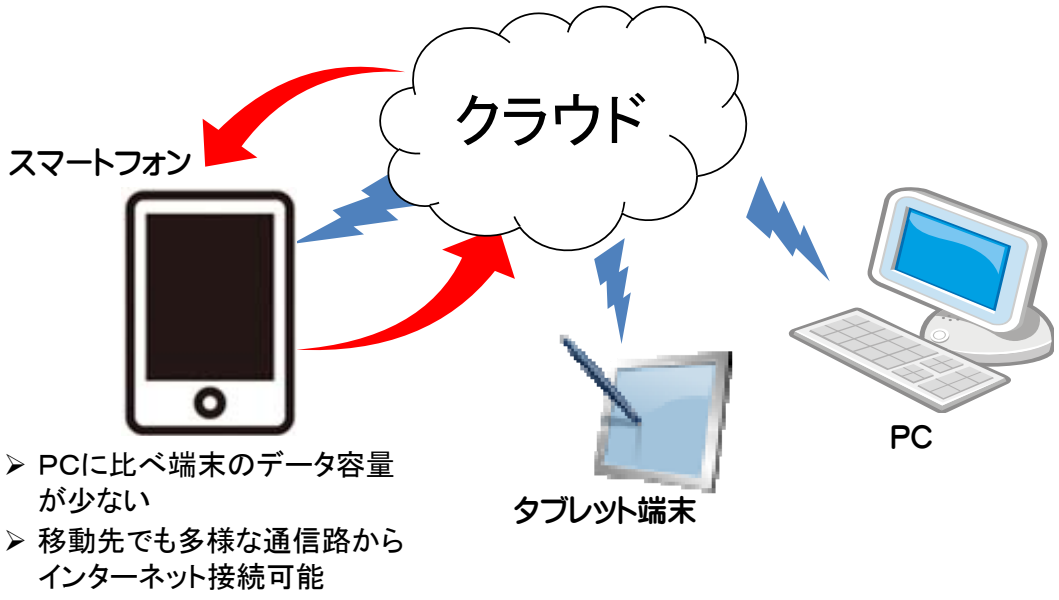


図１０　スマートフォンのクラウドサービスとの親和性の高さ

[42] 平成２３年１０月に株式会社ＩＣＴ総研が公表した調査結果（http://www.ictr.co.jp/topics_20111004.html）によれば、平成２２年度末時点の国内のパーソナルクラウド利用者数は1,472万人。同社は、平成２３年度に利用者総数は33%増の1,965万人、平成２７年度には平成２２年度比3.8倍の5,601万人に達すると予想。

第２節　スマートフォンからのクラウド利用に関する脅威

クラウドサービスの情報セキュリティ上の脅威・課題・対策については、様々なところで議論が進展している[43]。企業利用者から見た場合、自社で管理していた情報資産を外部のクラウド事業者の管理下に移すことにより、ガバナンスの喪失（クラウド事業者のシステム構成がブラックボックス化し安全性を確認できない等）、コンプライアンス違反（クラウドサービス事業者の監督が十分にできない等）、急なサービス終了やサービス終了時の不完全なデータ削除、海外拠点へのデータ保存等の脅威が存在する。

個人利用者から見た場合も、クラウドの情報セキュリティレベルがクラウド事業者側に依存するため、クラウド事業者が適切な情報セキュリティ対策を取っていなかった場合などに、クラウド上に保存した情報が漏えい及び毀損することが主要な脅威であると考えられる。その上で、特に、スマートフォンからクラウドを利用する際には、脅威を拡大しかねない以下のような要素が存在する。

（１）利用者情報の保存

クラウドサービスが主にビジネス利用やＰＣ向けに提供されていた数年前と比較すると、スマートフォンを経由してクラウド上に保存されるデータは、幅広い利用者情報を含む。

（２）多様な端末経由で保存されたデータとの連動

利用者がＰＣその他の多様な端末経由で保存したデータをクラウド上で集約できることが、クラウド利用のメリットとなっている。一方、スマートフォンはＰＣに比べ紛失・盗難等の危険性が高く、仮に紛失した端末からクラウドへの不正アクセスが発生すると、ＰＣなど他の端末から保存したデータを含む利用者のすべての情報が漏えいする可能性もある。

第３節　スマートフォンからのクラウド利用に関する課題

本節では、前節の脅威を踏まえ、今後期待されるスマートフォンからのクラウド利用に関する課題について概観する。

（１）利用者が無意識にクラウドを利用する課題

クラウドを利用するスマートフォンのアプリケーションの中には、利用者にそのことを意識させないインターフェースを持つものが存在するため、利用者が無意識に情報をクラウド上に保存するということが起こりうる。その場合、利用者が、情

[43] 国内では総務省、経済産業省、ＡＳＰＩＣ（特定非営利活動法人ASP・SaaS・クラウドコンソーシアム）、ＩＰＡ（独立行政法人情報処理推進機構）等により各種ガイドラインが策定されているほか、ＮＩＳＴやＥＮＩＳＡ（欧州ネットワーク情報セキュリティ庁）のガイドラインも参照されることが多い。その他、ＩＴＵ等の国際会議において議論が進められている。

報の毀損や漏えいという危険性一般を認識していても、機密性の高いデータをクラウド上に保存しないという選択をすることが困難になるという課題が存在する。

（２）情報セキュリティ対策が不十分なクラウドを利用するアプリケーションに関する課題

クラウドサービスは、市場拡大に伴い、価格、サービス、情報セキュリティ対策のそれぞれの面において様々なレベルのサービスが提供されるようになっており、特に情報セキュリティ対策が不十分なクラウドには情報の漏えいや毀損の危険性が存在する。そのため、クラウド事業者の情報セキュリティレベルが重要となるが、現状では、アプリケーションが利用するクラウド事業者の情報セキュリティレベルについて、利用者やアプリケーション提供サイト運営者、場合によってはアプリケーション開発者自身でも把握することが困難であるという課題がある。

（３）クラウド上のデータの暗号化に関する課題

クラウド事業者における情報漏えい対策としては、クラウドサーバのぜい弱性検査、クラウドサーバに不正アクセスされた場合の証跡確保、データの暗号化等の対策を取ることなどが有効であると言われる。このうち、クラウド上に保存されるデータを暗号化する対策については、既に実用化されているが、データ処理に当たってクラウド上で暗号文を復号するため、サービスの内容によっては、クラウド事業者等がデータの内容を把握できてしまうという課題がある。

（４）クラウドサービス利用時の認証に関する課題

クラウドへのアクセスの認証方式として、スマートフォンの端末認証を用いている場合や、利便性向上のため、ＩＤ・パスワード等の認証情報がスマートフォン端末内にキャッシュされている場合がある。利用者の利便性を重視する観点からは、これらの方法が一概に否定されるものではないが、一方で、仮にスマートフォンが紛失やボットウイルスの感染等により他者の支配下におかれてしまうと、簡単にクラウドへのアクセス認証が突破されることにより、他者によるクラウドへのアクセスやなりすましを可能にする端末としてスマートフォンが悪用されるおそれがある。

第４節　スマートフォンからのクラウド利用に関する対策

本節では、前節で指摘した課題について、対策の方向性を提示する。

（１）利用者が無意識にクラウドを利用することを防止する対策

スマートフォン利用者が、無意識にクラウド上に情報を保存することを避けるためには、アプリケーション提供サイトにおけるアプリケーションの選択時に、当該アプリケーションがクラウドを利用するか否かが表示されていることが有効であ

る。

（２）情報セキュリティ対策が不十分なクラウドを利用するアプリケーションに関する対策

現状、クラウド事業者の安全性について、それを第三者が客観的に評価する共通的な基準がなく、サービスの進展も速いため、契約の当事者は、事業者の規約その他を吟味し判断を行っている。

アプリケーションが、情報セキュリティ対策が不十分なクラウドを利用しないようにするためには、一義的には、アプリケーション開発者が、アプリケーションの設計に当たって、安全性の高いサービスを提供するクラウド事業者を選択するよう努めることが重要である。その上で、利用者にとっての安全性をより高めるため、アプリケーション提供サイト運営者における取組として、アプリケーションが利用するクラウドの情報を、アプリケーション開発者からの申告などにより収集するよう努めるとともに、クラウド関連の業界団体などから発信されるクラウド事業者の安全性に関する情報と組み合わせることにより、アプリケーションの安全性をクラウドを含めて総合的に判断できるようになれば、対策として有効である。

また、第３章で提示したアプリケーションの性質の可視化に向けた事業者団体の取組の中で、個々のアプリケーションがどのような情報をクラウドに送信しているかを明らかにすることができれば、当該アプリケーションが利用するクラウドの情報及びクラウド事業者の安全性に関する情報と合わせて、アプリケーションの総合的な評価に活用することが可能になると考えられる。

（３）クラウド上のデータの暗号化に関する対策

クラウド上で暗号文を復号するため、クラウド事業者等がデータの内容を把握できてしまうという課題を克服するために、クラウド上のデータを暗号化したまま一部の処理が可能な要素技術が確立されている。本技術が実用化されれば、復号過程を経ないため、復号したデータから情報漏えいする危険性を排除することが可能になる。ただし、当該要素技術において実行できる演算種別や速度に制限があることなどから、スマートフォンからのクラウド利用に関する即時性のある対策とは言い難い。

今後、暗号に関する要素技術を更に高度化し、実用に供するための技術開発を推進することが重要である。

（４）クラウドサービス利用時の認証に関する対策

スマートフォンによる端末認証や認証情報のキャッシュが利用される際には、他者による不正利用を防ぐため、利用者がより意識して、端末の紛失・盗難対策（端末ロック等）を行うことが必要になる。また、現在の認証方式とは別に、安全なアクセス実現のためのスマートフォン用の認証方式の検討も重要であると考えられる。

第５節　クラウドを活用したスマートフォンの情報セキュリティの確保

本節では、前節とは別の観点から、クラウドをスマートフォンの情報セキュリティ対策の一環として活用する可能性について考察する。

（１）クラウド上へのデータの保存

スマートフォン端末の紛失・盗難に遭った場合、情報漏えいの危険性を軽減するという観点から、遠隔消去機能などによりデータの抹消を行う対策が取られることがあるが、日頃からデータのバックアップを取っておくことが必要になる。

さらに、そもそも取り扱うデータを端末やＳＤカード内に保存するのではなく、積極的にクラウド上に保存することで、情報漏えいやデータ紛失の危険性を軽減できるとの指摘がある。

しかし、後者の方策には、利用者がデータの保存先を意識できないままにクラウドを利用するという状況に対する不安、通信環境が整っていない場所でスマートフォンを利用する場合の利用継続性、通信量増大による帯域ひっ迫の助長、クラウド側からの情報漏えいの危険性等、別の課題も含まれているため、両者を比較衡量した上での選択が重要である。また、そのようなクラウド上のストレージサービスを利用する際には、利用者が、クラウド事業者の規約等からクラウドの安全性を自身で一定程度判断することや、データの性質を見極め、クラウド上に保存するデータを選択することも重要である。

（２）スマートフォン端末のシンクライアント化

現状のスマートフォンは、通常、端末内でＯＳ、アプリケーションを動作させるが、今後、クラウドサービスとの連携が更に進展すれば、PaaS、SaaS等の機能を用いて、スマートフォンのＯＳ、アプリケーションに相当する機能をクラウド上で動作させ、手元の端末を、クラウド上の動作結果の表示装置として利用するというサービス形態が登場することが想定され、このことにより、端末からのデータ漏出の危険性を著しく軽減できる。

このサービス形態においては、クラウド上のＯＳのバージョンアップ、セキュリティパッチの適用はクラウドサービス事業者側で実施されることになり、利用者から見れば最新の情報セキュリティが確保されたＯＳを利用することが可能になる。

他方、このサービス形態には、必然的にクラウド利用に関する課題が付随することになるため、この方策の採用にあたっては、その有効性と課題を見極めることが必要である。

最後に、スマートフォンからのクラウド利用に関する情報セキュリティに関しては、利用が始まったばかりであり、今後様々な問題が発生する可能性があることから、情報収集や脅威・課題の的確な把握に努めるとともに、産学官連携、国際連携の枠組みを有効に活用しながら、対応策を検討することが望まれる。

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及びスマートフォンからのクラウド利活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、事業者や政府における当該課題の解決のための対策について検討を行い、結果を最終報告としてとりまとめた。

今後、最終報告のフォローアップという位置付けで、技術的な対策や利用者への普及啓発等ついて、事業者や政府等の取組を、半年に１回程度事務局が調査しその結果を公にしていくこととする。本フォローアップは、事業者間等の切磋琢磨を促すとともに、取組を検証する機会となることが期待される。同時に、スマートフォンを取り巻く環境は、正に日進月歩であることから、本研究会終了後も、産学官が連携して、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とが重要である。

本最終報告が、各事業者やアプリケーション開発者等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、スマートフォン及びクラウド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（あさみ ひろやす）	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（おかむら ひさみち）	国立情報学研究所 客員教授・弁護士
内田 義昭（うちだ よしあき）	KDDI株式会社 理事 運用本部長
大畠 昌巳（おおばたけ まさみ）	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（さいとう まもる）	株式会社インターネットイニシアティブ サービスオペレーション本部 セキュリティ情報統括室 室長
佐古 和恵（さこ かずえ）	日本電気株式会社 Ｃ＆Ｃイノベーション推進本部 イノベーションプロデューサー
塩崎 哲夫（しおざき てつお）	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（すがはら ひでむね）	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（せのお しゅうじ）	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（たけうち まさき）	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【～第６回】
玉井 久視（たまい ひさし）	ソニー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 プロダクトソフトウエア部 統括部長【第７回～】
丹波 廣寅（たんば ひろのぶ）	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（なかお こうじ）	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（にしもと いつろう）	株式会社ラック 取締役ＣＴＯ
萩原 英二（はぎわら えいじ）	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（みわ のぶお）	総務省 情報化統括責任者（ＣＩＯ）補佐官
山口 英（やまぐち すぐる）	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（こんどう れいこ）	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（えぐち じゅんいち）	経済産業省商務情報政策局　情報セキュリティ政策室長【～第６回】
上村 昌博（うえむら まさひろ）	経済産業省商務情報政策局　情報セキュリティ政策室長【第７回～】
関根 久（せきね ひさし）	経済産業省商務情報政策局　情報家電戦略室長

（事務局）

佐藤 健治（さとう けんじ）	総務省情報流通行政局　情報セキュリティ対策室長
中谷 純之（なかたに じゅんじ）	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

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、とりまとめ

第５回（平成２４年２月１日）
〇事業者における取組状況の確認
〇クラウドの利用・活用を含めた課題及び対策の洗出し

第６回（平成２４年３月９日）
〇ＯＳ提供事業者からのヒアリング
〇最終報告に向けた課題と対策の整理

第７回（平成２４年４月３日）
〇最終報告の意見招請案の検討

第８回（平成２４年４月２６日）
〇最終報告の意見招請案の検討、とりまとめ

第９回（平成２４年６月〇〇日）
〇最終報告のとりまとめ

事業者における対策一覧

別添１では、第３章第２節において提示した事業者における対策について、それを一覧にした上で、現時点で想定される実施主体を示した。実施主体は、本一覧に限定されるものではなく、今後の状況の変化等に応じて、柔軟に取り組むことが望ましい。なお、事業者は、その業態によって、複数の実施主体に分類される場合がある。

対策の項目	携帯電話事業者	端末製造事業者	事業者団体	アプリケーション提供サイト運営者	その他ＯＳ提供事業者	情報セキュリティ事業者	対策の内容
（１）ＯＳに関する対策							
ア　ＯＳのぜい弱性の修正とその修正版の提供 【Ａ、Ｗ】	○	○					ＯＳ提供事業者により発行されるセキュリティパッチを可能な限り速やかに利用者端末に適用。
イ　ＯＳのぜい弱性情報の発見と共有 【Ａ、Ｂ、ｉ、Ｗ】			○				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連携して把握し、対応方策を検討。
		○	○			○	ぜい弱性を早期に検出するため、検査ツールなどの開発。
ウ　ＯＳのサポート期間に関する対策 【Ａ、Ｂ、ｉ、Ｗ】					○		サポートを終了する場合には事前に公表。
エ　ＯＳのサポートの提供ルートに関する対策 【Ａ、Ｂ、Ｗ】	○						携帯電話事業者との解約後にＯＳのサポートが受けられない旨、利用者に注意喚起。

対策の項目	携帯電話事業者	端末製造事業者	事業者団体	アプリケーション提供サイト運営者	その他ＯＳ提供事業者	情報セキュリティ事業者	対策の内容
（２）アプリケーションに関する対策							
ア　マルウェアやぜい弱性を含むアプリケーションの作成を減らす対策【Ａ、Ｂ、ｉ、Ｗ】			○				セキュアプログラミングガイドやサンプルコードの内容を、継続的に検証・見直しを行い、開発者の目に触れやすい媒体に最新のガイドを掲載。
		○		○			ウェブサイトや開発者向け説明会の取組の中で、情報セキュリティ確保の観点から情報提供。
イ　マルウェアやぜい弱性を含むアプリケーションの流通に関する対策【Ａ、Ｂ、ｉ、Ｗ】				○			マルウェアやぜい弱性を含むアプリケーションを排除するための取組を継続・改善。
				○			サイトの運営方針やアプリケーション掲載方針について、利用者への情報開示。
ウ　マルウェアやぜい弱性を含むアプリケーションのインストール防止対策							
①　マルウェア対策ソフト【Ａ、Ｂ】	○	○				○	マルウェア対策ソフトの導入、機能向上。
		○				○	システム部分への特権的なアクセス権限を付与する端末を開発。
		○					端末開発に際してカーネル部への情報セキュリティ対策を強化し、通常のマルウェア対策ソフトと併用。
②　モバイル端末管理（ＭＤＭ）【Ａ、Ｂ、ｉ、Ｗ】					○	○	端末の設定、ソフトウェアのバージョン管理、導入アプリケーションの制限等を総合的に行うモバイル端末管理を採用。
③　アプリケーションの性質の可視化の枠組み【Ａ】			○				アプリケーションそのものの性質を利用者が把握できる枠組みを構築。
			○	○		○	アプリケーションの解析ツールの開発。

対策の項目	携帯電話事業者	端末製造事業者	事業者団体	アプリケーション提供サイト運営者	その他ＯＳ提供事業者	情報セキュリティ事業者	対策の内容
エ　マルウェアが端末に侵入した場合の被害軽減							
①データやデバイスへのアクセスに関するＯＳによる動的制御 【Ａ、Ｂ、ｉ、Ｗ】					○		電話帳データや端末内に保存されているデータ、発呼機能やＳＤカード等へのアクセスについて、ＯＳ側で柔軟にON/OFFする機能。
②カーネル部への情報セキュリティ対策 【Ａ】		○					アプリケーションに付与する権限の最小化、ＯＳ機能最小化（不必要なコマンドの削除等）、改ざん検出・機能凍結。
（３）通信路の情報セキュリティの確保 【Ａ、Ｂ、ｉ、Ｗ】	○						暗号技術を活用した無線ＬＡＮのアクセスポイントの普及を推進。
		○					スマートフォン端末側で接続先を識別し、回線の信頼度に応じて保護レベルを変更できる仕組みを端末に導入。
		○			○		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。
（４）端末内のデータ保護 【Ａ、Ｂ、ｉ、Ｗ】	○	○	○	○		○	事業者から利用者に対する啓発の際に、紛失・盗難対策やその留意点について、併せて伝達。
		○					端末内やＳＤカード内のデータを暗号化し、データが漏出しても内容が知られることのない仕組みを端末に導入。
（５）スマートフォンから外部ネットワークへの影響に関する対策 【Ａ、Ｂ、ｉ、Ｗ】	○	○	○	○		○	事業者から利用者に対する啓発の際に、スマートフォンを踏み台にした攻撃の可能性について併せて伝達。

別添２

スマートフォン情報セキュリティ３か条

（利用者が最低限取るべき情報セキュリティ対策）

スマートフォンは、アプリケーションを活用することで、様々な機能を自由に追加できる便利な携帯電話です。しかし自由さの反面、その中には危険なアプリケーションが混じっている場合もあります。利用者自身で情報セキュリティ対策を取ることが必要です。

盗難・紛失対策や他人による不正利用防止対策など、従来の携帯電話と同様の対策が必要です。さらにスマートフォンにおいては、次の３つの対策が大切です。

１．ＯＳ（基本ソフト）を更新

スマートフォンは、ＯＳの更新（アップデート）が必要です。古いＯＳを使っていると、ウイルス感染の危険性が高くなります。更新の通知が来たら、インストールしましょう。

２．ウイルス対策ソフトの利用を確認

ウイルスの混入したアプリケーションが発見されています。スマートフォンでは、携帯電話会社などによってモデルに応じたウイルス対策ソフトが提供されています。ウイルス対策ソフトの利用については、携帯電話会社などに確認しましょう。

３．アプリケーションの入手に注意

アプリケーションの事前審査を十分に行っていないアプリケーション提供サイト（アプリケーションの入手元）では、ウイルスの混入したアプリケーションが発見される例があります。ＯＳ提供事業者や携帯電話会社など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ようにしましょう。インストールの際にはアプリケーションの機能や利用条件に注意しましょう。