別紙

平成２５年３月２９日
総　　務　　省

スマートフォン・クラウドセキュリティ研究会最終報告のフォローアップ

スマートフォン・クラウドセキュリティ研究会（以下、「本研究会」という。）は、最終報告（平成２４年６月公表。以下、「本最終報告」という。）において、事業者における具体的な情報セキュリティ対策や利用者への普及啓発策のほか、関係事業者や政府等が当面、重点的に実施すべき事項を「スマートフォン情報セキュリティ行動計画」（以下、「本行動計画」という。）として示した。以下では、本最終報告で掲げられた事項の中から、特に重要と考えられるものについて、各節において最新の動向のフォローアップを行い、今後の方向性を提示する。

まず第１節において、スマートフォンの情報セキュリティ上、最も危険性が高いのは、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、それらアプリケーションのインストール防止に向けた各関係者の取組について重点的に取り上げる。

次に第２節では、スマートフォンを安心して利用するためには、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あることから、現在までの各関係者の取組について重点的に取り上げる。

最後の第３節では、本行動計画に沿った現在までの関係事業者及び政府等の取組状況について取り上げる。

なお、以下の記述は、特に断りのない限り、Android に関する事項である。

第１節　情報セキュリティ上脅威のあるアプリケーションに関する対策

情報セキュリティ上脅威のあるアプリケーションに関する対策には、第３節の行動計画（３）でも触れるように、情報セキュリティ上脅威のあるプリケーションについて（A）作成そのものを減らす取組、（B）アプリケーション提供サイト等に流通することを防止する取組、（C）利用者がインストールする際に危険性に気づき、インストールを回避することができるようにする取組、(D)インストール後に脅威に気づき、対処可能とする取組という各段階が存在する。

また、本最終報告では、情報セキュリティ上脅威のあるアプリケーションを、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に分類した。

以下では、各段階及びアプリケーションの分類を踏まえ、各取組主体ごとに対策の状況や今後の方向性について取り上げる。

（１）携帯電話事業者の取組

【最終報告】

携帯電話事業者（アプリケーション提供サイト運営者としての役割を含む。）に期待される次の取組が挙げられた。

・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として、アプリケーション開発者に対する情報セキュリティ確保の観点からの情報提供を行う。
・マルウェアやぜい弱性を含むアプリケーションの流通防止に関する取組として、アプケーション提供サイト運営者として、これらのアプリケーション排除の取組を継続・改善する。
・利用者がアプリケーション提供サイトを信頼性の観点から選択できるよう、アプリケーション掲載方針等について、情報開示を行うとともに、事業者間の連携により最低限の基準の統一を行っていく。
・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に向けた対策として、マルウェア対策ソフトの普及等に努める。

【最新動向】

携帯電話事業者各社は、自らがアプリケーション提供サイトを運営するに際し、掲載ガイドラインを策定し、アプリケーション開発者への遵守を求めることにより各社運営サイトの品質維持に努めるとともに、各社の基準で安全性の確認を行う取組を継続してきた。しかし、アプリケーション掲載方針等の一般利用者への情報開示や、アプリケーション提供サイト運営者間で連携した基準の作成はなされていなかった。

かかる状況下において、平成２４年１０月、社団法人電気通信事業者協会（ＴＣＡ）の移動電話委員会の下に、スマートフォンの利用者情報等に関する適正な取組に向けて、「スマートフォンの利用者情報等の適正利用促進検討部会」[1]が設置され、携帯電話事業者により「アプリケーション提供サイト運営事業者向けガイドライン」の検討が開始された。同ガイドラインは、アプリケーション提供サイトを運営する携帯電話事業者が、プライバシー及び情報セキュリティの観点から適切でないアプリケーションを提供サイトから排除し、アプリケーション提供サイトを適正に運用すること、利用者への周知啓発を行うことを目的として、各事業者による実施が推奨される取組を記載しているものであり、平成２５年３月に策定・公表された[2]。

ＴＣＡのガイドラインには、マルウェア及びぜい弱性を含むアプリケーションへの対策に関しては、次の記載がある。

「スマートフォンアプリケーション提供サイト運営事業者向けガイドライン」における関連の記載（抜粋）

５　アプリケーション提供サイト運営事業者向けガイドライン

[1] 同部会の目的・活動内容は、「『スマートフォン プライバシー イニシアティブ』で示された『スマートフォン利用者情報取扱指針』を踏まえて、スマートフォンの利用者情報等の適正な利用を促進するため、構成員間の情報共有、必要なガイドライン等の施策の検討・策定・運用、利用者への周知・啓発、外部関係団体・関係省庁・関係会議等への対応等に関する事項を取扱う。」こととされている（「スマートフォンの利用者情報等に関する連絡協議会」第３回会合（平成 24 年 12 月 11 日）TCA 提出資料）。

[2] http://www.tca.or.jp/topics/2013/0329_561.html

（1）アプリケーション提供者等に対する支援

②アプリケーションに関するセキュリティの確認

○　アプリケーション提供者等に対する周知啓発活動において、マルウェア対策関連の情報提供を行うことが期待されます。

○　アプリケーション登録やリンク掲載の前に、各運営事業者の基準に従ってセキュリティ上の確認を行うとともに、事後的にも定期的にチェックすることが望まれます。

　加えて、配信型事業者の場合には、上述したアプリケーションの事前審査を実施する際に、セキュリティの観点からも検証を行うことが求められます。

○　アプリケーション提供サイト運営事業者の掲載ガイドライン等において、アプリケーション開発にあたっては、セキュアコーディングガイドライン（一般社団法人日本スマートフォンセキュリティ協会（JSSEC）のセキュアコーディングガイド等）を参考に、脆弱性を排除する旨を記述する等し、アプリケーション提供者等に対して啓発を行っていくことが望まれます。

③適切ではないアプリケーションが判明した場合の対応

○　利用者からの通報や運営事業者自らによる検知、他の団体等からの情報提供等によって、不適切なアプリケーションが判明した場合、アプリケーション提供サイト運営事業者は、当該アプリケーションの自社サイトからの迅速な削除や利用者への注意喚起、関係事業者間の情報共有等、適切に対応することが求められます。

　また、各社の具体的な取組としては、マルウェア対策ソフト提供事業者と提携した各社ブランドのウイルススキャンを行うアプリケーションを、事前に端末にインストールするなどして出荷し、顧客が携帯電話事業者へ申込手続きのみで、簡単にウイルス対策ができるように配慮している。またこれらの各社ブランドのアプリケーションにおいて、顧客がダウンロードするアプリケーションの性質の可視化に向けたサービスを提供する動きが見られる。（（2）のマルウェア対策ソフト提供事業者の取組を参照。）

【今後の方向性】

　これらの取組は、本最終報告において示された事項を具現化するものであり、本ガイドラインを踏まえた各社の一層の取組の推進が期待される。それにより、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が、利用者にとって一層信頼のおけるものとなることが期待される。

（2）マルウェア対策ソフト提供事業者の取組

【最終報告】

　マルウェア対策ソフトの機能向上と普及とが必要とされた。

【最新動向】

マルウェア対策ソフト提供事業者において、スマートフォン向けマルウェアの検知率の向上や新しいマルウェアへの対応のため、検体収集等の取組が継続されている[3]。

また、一部のマルウェア対策ソフト提供事業者では、利用者情報を不適切に収集・利用するアプリケーションに対処するための機能の追加を進めている。例えば、ある対策ソフトではアプリケーションの取得するパーミッションをインストール後に確認できる機能を設けている[4]。また、別の対策ソフトでは、アプリケーションの事前評価データベースに基づき、個々のケースに応じ、利用者情報を不適切に取得していると判断した場合、マルウェアとは別に当該アプリケーションを検知結果に含める[5]などの対応が進められている。

その他、携帯電話事業者を含むアプリケーション提供サイトやアプリケーションレビューサイト[6]におけるアプリケーションの評価に対して、技術協力を行う取組が進められている。

【今後の方向性】

我が国においては、現時点では、スマートフォンを狙うマルウェアの事例に利用者情報を不適切に取得するものも多く含まれることから、マルウェア対策ソフト等におけるそれらアプリケーションのへの対応等の進展が期待される。

（３）端末製造事業者の取組

【最終報告】

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に向けた対策として、マルウェア対策ソフトに特権的なアクセス権限を付与する端末の開発や、端末自身の情報セキュリティ対策の強化等の解決策の検討が例示された。

【最新動向】

マルウェア対策ソフトに強化したアクセス権限を付与する端末や、端末自身の情報セキュリティ対策を強化した端末が開発されている。

また、プライバシーへの懸念の対処方策として、一部機種に、アプリケーションが電話帳機能へアクセスする際にそれを通知したり、特定のアプリケーションから電話帳データへのアクセスをブロックする機能の導入が開始された[7]。

---

[3] 株式会社カスペルスキーでは、「カスペルスキーモバイルセキュリティ for Android」において、利用者の端末にインストールされたアプリケーションのスキャン時に得られる情報をマルウェアの動向分析などに活用しているほか、ヒューリスティックスキャン（類推検知）などを併用し、ブラックリストのみに依存しない多層的保護機能を提供している。

[4] マカフィー株式会社では「McAfee Mobile Security」にアプリケーションがアクセスするデータと端末機能をアイコンで表示する機能を搭載。株式会社ＮＴＴドコモでは同機能を、自社ブランドの「ドコモあんしんスキャン」の追加機能として提供中。

[5] トレンドマイクロ株式会社では、「ウイルスバスター モバイル for Android」にアプリケーションが個人情報を取り扱うかを確認して、漏えいの可能性があることを警告する「プライバシースキャン」機能を搭載。ＫＤＤＩ株式会社では同機能を、今後「ウイルスバスター for au」の機能の一部として提供することを検討中。

[6] 「アプリ情報サイト『アンドロイダー』」 https://androider.jp/topic/about/

[7] シャープ株式会社「電話帳アクセスモニター」
https://sh-dev.sharp.co.jp/android/modules/others/

【今後の方向性】

端末レベルにおいても、情報セキュリティ対策の取組の継続・充実が望まれる。

（４）ＯＳ提供事業者の取組

【最終報告】

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、各自の取組を継続・改善していく努力が求められた。

また、マルウェアが端末に侵入した場合の被害軽減措置として、データやデバイスへのアクセスをアプリケーションごとに柔軟に設定できる措置がＯＳレベルで実装されることが検討されることが望ましいとされた。

【最新動向】

Android4.2 以降のバージョンに、危険性のあるアプリケーションをインストール前にチェックする機能や、アプリケーションが有料ＳＭＳサービスにメッセージを送ろうとしたときに利用者に通知する機能を設けたと公表されている[8]。

なお、iOS については、iOS6 において「プライバシー」セクションが設けられ、個別のアプリケーションごとに、位置情報、電話帳、カレンダー、リマインダー、写真等へのアクセスについて、利用者がインストール後に制御できる機能が搭載された。また新規にダウンロードしたアプリケーションがこれらの機能に最初にアクセスする際には、ポップアップで同アクセス許諾の可否を利用者に確認する機能を備えている。

【今後の方向性】

ＯＳ提供事業者は最大のアプリケーション掲載数を誇るアプリケーション提供サイト運営者でもあることから、その安全性向上や、ＯＳレベルの情報セキュリティ機能の強化は、スマートフォンの危険性の低減に最も効果的であることから、今後も取組の継続・充実が期待される。

（５）その他事業者団体の取組

【最終報告】

アプリケーションの作成段階で、マルウェアやぜい弱性を含むアプリケーションを減らす取組として、アプリケーション開発者への教育・啓発や、セキュアプログラミングガイド等の具体的な啓発資料の作成を対策として提示し、JSSEC において作成されているセキュアプログラミングガイドについては、ガイドの継続的な検証・見直しと各種媒体を駆使した周知が行われることが適当とされた。

【最新動向】

JSSEC のセキュアコーディンググループでは、「Android アプリのセキュア設計・セキュアコーディングガイド」初版を平成２４年６月に公表したのち、同年１１月に改訂するなど、Android 向けアプリケーションのぜい弱性の動向を踏まえた見直し・拡充等の取組を継続的

[8] http://developer.android.com/about/versions/jelly-bean.html

に実施している。同ガイドは多くの関係者に参照されており、複数の携帯電話事業者やアプリケーション開発企業において、社内アプリケーション開発者への教育や自社提供アプリの設計・自己診断に活用されているほか、ＫＤＤＩ株式会社が運営するアプリケーション提供サイトにおいて、平成２５年３月より、提携先のアプリケーション開発者への推薦資料としても活用されるようになっている。

【今後の方向性】

アプリケーションのぜい弱性については、アプリケーション作成後に第三者がぜい弱性を発見することは技術的に高度で高コストであること、また従来からソフトウェアのぜい弱性は、発見者から直接あるいは調整機関を通じてアプリケーション開発者に通知され、対策が取られた後に公表されるスキームが確立されていることから、今後も個別のアプリケーションのぜい弱性の有無を、アプリケーション開発者自身の確認なしに利用者に対して表示するサービスが登場することは想定しづらく [9]、アプリケーション開発段階でぜい弱性を作り込まないことが今後も対策の中心となると考えられる。そのため、今後も、セキュアコーディングガイドの見直し・拡充等の取組の有益性が参加団体間で確認され、業界団体としての取組が継続されることが望まれる。

一方で、現在のスマートフォンに対する攻撃は単体のマルウェアによるものが中心であり、ぜい弱性を利用した実際の被害の事例は国内ではまだ報告がない [10]ことから、アプリケーション自体が持つぜい弱性への対策について、業界全体で機運が高まっているとは言い難い。しかし、ＩＰＡによれば、スマートフォンの普及に伴い、スマートフォンのアプリケーションのぜい弱性の報告件数は増加しており [11]、また報告されたアプリケーションの中には、ダウンロード数が 100 万件を超える日本語の人気アプリケーションも含まれていたことが確認されている [12]。ＰＣ向けのソフトウェアにおいては、情報セキュリティ対策の進展に伴い、攻撃の手段が単体のマルウェアからソフトウェアのぜい弱性を突くものに移行していった歴

---

9 ぜい弱性を含むアプリケーションの検証・評価については、現状、ぜい弱性診断サービス提供事業者等が、有料でアプリケーション開発者向けに提供しているサービスが中心となっている。

10 海外では、ドイツの大学の研究チームが、GooglePlay 上の無料アプリケーションの多くに、アカウント情報の不正取得が可能な SSL のぜい弱性が含まれていることを明らかにしたとの報道などがある。
http://www.computerworld.jp/topics/563/205247

11 脆弱性対策情報データベース JVN iPedia の登録状況[２０１２年第４四半期（１０月～１２月）] http://www.ipa.go.jp/security/vuln/report/JVNiPedia2012q4.html

12 ある事例では、悪意のあるマルウェアに利用された場合、端末内の画像を勝手にＳＮＳに投稿される可能性のあるぜい弱性や、別の事例では、ＳＮＳアプリ上の友人の発言情報がＳＤカードに保存されていたため、他のアプリケーションから読み取ることができる可能性のあるぜい弱性が含まれていたという。出典「スマートフォン セキュリティ シンポジウム２０１２」（２０１２年１１月２１日）（主催：日本スマートフォンセキュリティ協会）における「Android アプリの脆弱性（セキュリティホール）を防ぐ、JSSEC のセキュア設計・セキュアコーディングガイド」（技術部会 セキュアコーディンググループリーダー 松並勝氏発表資料）
http://www.jssec.org/dl/1121/05_secure%20cording.pdf

史があることを踏まえると、今後スマートフォン向けアプリケーションにおいても、アプリケーションのぜい弱性を突くマルウェアや攻撃ツールが登場する可能性は否定できない。

以上のことから、深刻な被害がまん延する前に先手を打つべく、開発者に対しセキュアコーディングの知識の啓発を進め、開発段階からぜい弱性を作り込まないようにする取組が強化されていくべきであると考えられる。

第２節　利用者に対する普及啓発の取組

スマートフォンを安心して利用するためには、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あることから、以下では、普及啓発を実施する各主体ごとの取組について取り上げる。なお、利用者の意識向上策については、第３節の行動計画（５）においても触れる。

（１）総務省の取組

【最終報告】

メディアの活用を含め、普及啓発をより一層促進していくことが重要であるとされた。

また、スマートフォンから公衆無線ＬＡＮを利用する機会の拡大が見込まれる一方で、情報セキュリティ上危険性のある公衆無線ＬＡＮアクセスポイントへの対策として、サービス提供者側で安全性の高い無線ＬＡＮアクセスポイントの設置を進めるとともに、無線ＬＡＮの安全な利用方策に関する手引書の改訂等により、利用者のリテラシーを高めていくことが必要であるとされた。

【最新動向】

総務省では、スマートフォンの特性及び利用上の注意点・対策のポイントについて、「スマートフォン情報セキュリティ３か条」（平成２３年１２月）及び「スマートフォン プライバシー ガイド」（平成２４年４月）をとりまとめ、政府広報やウェブサイトへのコンテンツ掲載等を通じた啓発を開始している。

平成２４年７月以降、政府広報の各種媒体（インターネットテレビ、ラジオ、オンラインテキスト、新聞広告等）を通じて、「スマートフォン情報セキュリティ３か条」及び「スマートフォン プライバシー ガイド」の周知広報を実施した。また、平成２４年９月の「スマートフォン安心・安全利用促進プログラム」の策定以降、関係機関とも協力しながら、各種セミナーでの紹介、啓発資料作成、雑誌等への寄稿等を通じて、利用者に対する周知啓発を推進している。

無線ＬＡＮに関しては、利用者が安全に無線ＬＡＮを利用するための手引書を改訂し、平成２４年１１月「一般利用者が安心して無線ＬＡＮを利用するために」として公表した[13]。これについても同様に、政府広報の各種媒体（ラジオ、オンラインテキスト、モバイルテキスト広告、広報誌等）や、セミナー等の機会を通じて同手引書の周知に努めている。

【今後の方向性】

引き続き、スマートフォンにおける脅威の動向や、利用者の意識の変化を把握しながら、啓発事項の見直しや啓発対象の重点化を進めるなど、関係事業者とも協力しながら、効果的

[13] http://www.soumu.go.jp/main_content/000183224.pdf

な普及啓発を推進すべきである。

無線ＬＡＮに関しては、現在、スマートフォンによる通信量の急激な増大と携帯電話周波数のひっ迫が課題となっていることを踏まえ、電波の有効利用の観点からも、利用者への普及啓発が必要である。具体的には、利用者に対して、オフロードの効用とともに、スマートフォンからの無線ＬＡＮの適切な使用方法や情報セキュリティ対策について、周知・広報していくことが必要である。併せて総務省では、平成２５年度からは、アクセスポイント設置者側の情報セキュリティ対策についても、啓発資料の作成及び啓発事業を実施していくこととしている。

（２）携帯電話事業者等の取組

【最終報告】

携帯電話事業者については、契約時に利用者が的確に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などの工夫を行うことや、利用者自身が行うべき基本的な情報セキュリティ対策を資料化することが有益であるとされた。アプリケーション提供サイト運営者については、利用者の目につきやすい場所に情報セキュリティ関連情報を掲載するといった取組を行うことが効果的であるとされた。

【最新動向】

平成 24 年 11 月には、社団法人電気通信事業者協会（ＴＣＡ）の移動電話委員会にて、携帯電話事業者の連携による統一的啓発資料が作成され [14]、携帯電話事業者のアプリケーション提供サイト等からリンクを掲載して周知が行われている。

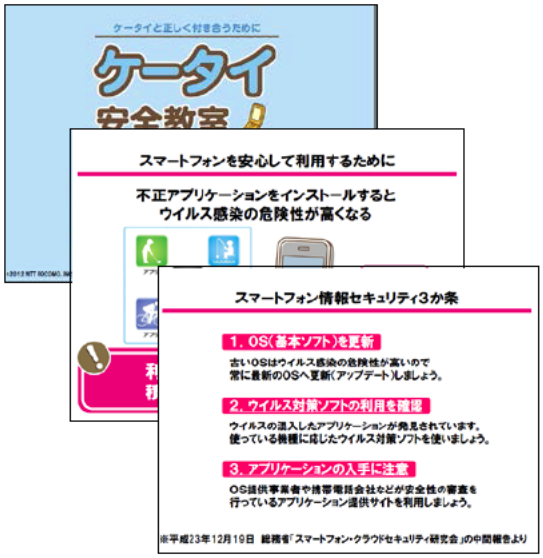
「スマートフォン（スマホ）ご利用にあたっての注意事項」
（社団法人電気通信事業者協会）

14　社団法人電気通信事業者協会 2012 年 11 月 2 日付プレスリリース「～安心・安全なスマートフォンのご利用への取り組み～ 『スマートフォン（スマホ）ご利用にあたっての注意事項』の作成について」　http://www.tca.or.jp/press_release/2012/1102_537.html

携帯電話事業者における利用者啓発の取組としては、契約時配布資料への「スマートフォン情報セキュリティ３か条」の掲載（株式会社ＮＴＴドコモ及びＫＤＤＩ株式会社）、携帯電話事業者各社が提供するウイルス対策サービスの紹介、一般利用者向けの啓発教室におけるスマートフォンの情報セキュリティ対策の盛込み等の取組が進められている。

契約時配布資料（株式会社ＮＴＴドコモ）

契約時配布資料（ＫＤＤＩ株式会社）



ケータイ安全教室資料（株式会社ＮＴＴドコモ）

さらに、これら啓発活動については、第１節で取り上げたＴＣＡの「スマートフォンアプリケーション提供サイト運営事業者向けガイドライン」５（２）において、スマートフォン契約時等における利用者への周知啓発 [15]、様々なリテラシーの消費者（青少年、高齢者）へ

15 本最終報告及び「スマートフォン プライバシー イニシアティブ」を踏まえて、ＴＣＡによるガイドラインにおいては、スマートフォンと従来型の携帯電話の端末との違い、スマートフ

の対処を行っていくことが望ましいとして明記されている。

【今後の方向性】

携帯電話事業者においては、スマートフォンの情報セキュリティ対策に関して、今後も引き続き利用者へのわかりやすい説明の取組を継続することが求められる。また、携帯電話事業者間や関連の事業者団体等との間で、情報セキュリティ上の脅威についての情報共有を促進し、実態を踏まえた啓発コンテンツの刷新をはかっていくことが望まれる。

無線ＬＡＮに関しては、携帯電話事業者自身が無線ＬＡＮのアクセスポイントの安全性向上を進めるとともに、利用者に対して無線ＬＡＮの情報セキュリティ対策について、総務省の手引書その他を活用しつつ、啓発を行うことが望まれる。

第３節　「スマートフォン情報セキュリティ行動計画」に基づく取組

行動計画（１）事業者団体における対応方策検討 情報セキュリティ関連の事業者団体の枠組みにおいて、ＯＳのぜい弱性情報等を事業者が連携して把握し、対応方策を検討する取組を、平成 24 年中に開始する。

【最終報告】

スマートフォンの情報セキュリティ上の課題の１つとして、ＯＳのぜい弱性が指摘され、バージョンアップなどによるＯＳのぜい弱性の修正の迅速化や、ぜい弱性情報を事業者間で連携して把握・検討する取組が有効であるとされた。

【最新動向】

本最終報告公表後、携帯電話事業者等において、自社の販売端末に関するぜい弱性対応の進捗管理方法が改善された。また、平成２４年１１月には、ソフトウェアのぜい弱性情報ハンドリングを行う機関である一般社団法人 JPCERT コーディネーションセンター、携帯電話事業者及び端末製造事業者の間で、初の事例としてスマートフォンのＯＳのぜい弱性情報の取扱いに関する調整が行われるなど、ＯＳのぜい弱性対応の円滑化に向けた取組が進められている。

また、ぜい弱性情報の共有に関しては、一般社団法人日本スマートフォンセキュリティ協会（JSSEC）の脆弱性ＷＧにて、ＯＳのぜい弱性情報を事業者間で共有し、対策の検討を行う活動や、必要に応じて独立行政法人情報処理推進機構（ＩＰＡ）、ＯＳ提供事業者等の関係者に報告を行う活動が平成２４年中から実施されている。

【今後の方向性】

端末ごとにＯＳのカスタマイズが行われている我が国の状況において、関係者間で着実に推進されているＯＳのぜい弱性対応の迅速化に向けた取組が、継続されることが期待される。

ォンにおける様々な利用者情報の取扱いと注意点、スマートフォンにおける情報セキュリティ対策について周知啓発を行うことが求められるとしている。

行動計画（２）利用者保護の観点から求められる技術の研究開発

独立行政法人情報通信研究機構は、暗号技術やモバイル環境を含め情報セキュリティに関する研究開発に総合的に取り組んでいる知見を生かし、スマートフォンで取り扱われる利用者情報のクラウドへの安全な格納方法や、スマートフォンのアプリケーションによるデータやデバイスへのアクセスに関する情報セキュリティ対策や評価手法等、スマートフォンの情報セキュリティ確保に資する研究開発に平成２４年中に取り組む。

【最終報告】

独立行政法人情報通信研究機構（ＮＩＣＴ）において、スマートフォンのアプリケーションの情報セキュリティ確保に資する研究開発に取り組むこととされた。

【最新動向】

ＮＩＣＴでは、平成２４年に、スマートフォンアプリの解析手法や解析ツールの比較検討の調査を実施した。また、これまでにＮＩＣＴでは、利用者のネットワーク利用方法に着目し、リスク分析結果の可視化と情報セキュリティ対策を提示するための「セキュリティ知識ベース」と分析エンジンの研究開発に取り組んできている。この知見を活かし、スマートフォンのアプリケーションが、アカウント情報等の機密性の高いデータの送受信を行う際の情報セキュリティ要件について、その検討を進めている。

【今後の方向性】

ＮＩＣＴは、官民の叡智を集めたオールジャパン体制での研究を実施する機関として、機密性の高いデータを取り扱うアプリケーション開発者との連携を視野に入れながら、スマートフォンのアプリケーションにおけるリスク分析とリスク可視化に関する研究開発を行っていくことが期待される。

行動計画（３）アプリケーションの性質の可視化の枠組みの整備

アプリケーションにマルウェアが含まれているか否かや利用者情報の取扱い方法、アプリケーションが外部と通信する際の通信路が暗号化されているか否かなど、アプリケーションの性質について、それを利用者に分かりやすく提示する事業者団体等の枠組みについて、総務省は、その整備に関する必要な調査研究等を実施し、平成２４年度中に一定の結論を得る。また、総務省は、事業者団体等によって整備された枠組みについて、その取組の普及を支援していく。

【最終報告】

総務省において、アプリケーションの性質を利用者にわかりやすく提示する事業者団体等の枠組みについて、必要な調査研究等を実施するとともに、整備された枠組みの普及を支援することとされた。

【最新動向】

平成２４年始め頃から、我が国においてもスマートフォンを対象とした情報セキュリティ上脅威のあるアプリケーションによる被害が現実のものとなったことから、アプリケーションの性質の可視化に対する社会的ニーズが高まっていると考えられ、さまざまな主体がアプ

リケーションの性質の可視化に向けた対策に取り組み始めている。

総務省では、平成２４年度に民間調査会社に委託し、アプリケーションの検査・評価の手法や業界団体等の検討状況について調査を実施した。本調査結果を踏まえ、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の作成、流通、インストールの防止等に関する現在までの取組と今後の対策の方向性について、詳細は第１節で取り上げた通りである。

特に我が国においては、携帯電話事業者が、各社の運営するアプリケーション提供サイトにおける安全性の向上のほか、アプリケーション開発者及び利用者に対する情報提供、利用者への情報セキュリティ対策ツールの提供等において中心的な役割を果たしており、スマートフォンのアプリケーションの安全性向上に向けた各種の取組を推進している。

【今後の方向性】

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おいては、継続して取組が行われることにより、一層安心・安全にアプリケーションを利用できる環境の整備が進展することが期待される。その他のアプリケーション提供サイトについても、マルウェア対策ソフト等の提供、アプリケーションの評価・レビューサービスの拡充、アプリケーション開発者への啓発等の重層的な取組により、アプリケーションに関する必要な情報が利用者にとってよりわかりやすく表示されるようになることが望まれる[16]。

行動計画（４）国際連携・国際協調の推進 総務省は、内閣官房情報セキュリティセンターや関係省庁と連携して、国際会議や二国間会合の場を通じ、引き続き、脅威や課題、対策手法等について積極的な情報交換や意見交換に努め、利用者保護のあり方等に関する国際標準化を視野に入れながら、国際的な協調を図っていく。

【最終報告】

スマートフォンのＯＳや端末、サービス構造がグローバルモデルとして我が国の市場に投入されている状況を踏まえ、具体的な脅威や課題、対策について、諸外国との情報共有が重要とされた。

【最新動向】

本研究会終了後、総務省では、インターネットエコノミーに関する日米政策協力対話（平成２４年１０月）、日 EU・ICT 政策対話、日 EU インターネット・セキュリティフォーラム（平成２４年１１月）、第 5 回日・ASEAN 情報セキュリティ政策会議（平成２４年１０月）、日仏 ICT 政策協議（平成２５年２月）等において、スマートフォンの情報セキュリティ及び利用者情報の取扱いに関する双方の取組の情報交換を行った。

特に、日米政策協力対話では、スマートフォンのセキュリティ確保のためのベストプラクティス及びスマートフォンにおける利用者情報の取扱いやプライバシーに関する国際的な取

16 なお、第三者による検証の在り方等については、「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」に設置された「スマートフォン時代における安心・安全な利用環境の在り方に関するＷＧ」（平成２４年１２月）において検討が行われている。

組への対応について情報共有を継続することで合意している。

【今後の方向性】

スマートフォンの情報セキュリティ上やプライバシー上の脅威は、主要国において共通の課題として関心が高まっていることから、引き続き二国間・多国間の国際枠組み等を通じて、連携・協調を図ることが必要である。

行動計画（５）スマートフォン利用者への総合的な普及啓発の実施

スマートフォンにおける情報セキュリティや利用者情報等に関する対策等について、利用者に必要な情報を総合的に提供するため、総務省は、「スマートフォン安心安全プログラム（仮称）」を早急にとりまとめ、関係事業者や事業者団体等と協力して継続的に推進する。また、その内容については、取組の進捗や状況の変化等を踏まえ、必要に応じて見直しを行う。

【最終報告】

スマートフォンの情報セキュリティ上の課題を解決し、スマートフォンを安心して利用するためには、利用者の意識向上が不可欠であることから、携帯電話事業者やアプリケーション提供サイト運営者、政府等が継続的に利用者に情報提供を推進すべきとされた。

【最新動向】

関係者間の連携を確保し、総合的な啓発を行う観点から、総務省は、本行動計画及び「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」（以下、「諸問題研究会」という。）の提言である「スマートフォン プライバシー イニシアティブ」（平成２４年８月公表）[17]を踏まえ、平成２４年９月に「スマートフォン安心・安全利用促進プログラム」を策定し、公表した[18]。

各主体ごとの普及啓発の取組状況については、第２節で詳細を取り上げた通りである。

【今後の方向性】

引き続き、各主体における普及啓発の取組が継続されることが期待されるとともに、普及啓発の効果及び利用者の意識の現状を捉えるため、スマートフォン利用者を対象とした意識調査を行うことが有効である。

また、スマートフォンからの無線ＬＡＮの適切な使用方法や情報セキュリティ対策等についても、周知・広報していくことが必要である。

行動計画（６）本最終報告の定期的なフォローアップ

本最終報告に掲げた技術的な対策や利用者への普及啓発等ついて、関係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。同時に、スマートフォンを取り巻く環境は、日々変化していることから、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とする。

17 総務省報道資料 http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html
18 総務省報道資料 http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000091.html

【最終報告】

本最終報告では、関係者による取組の実施を促すため、行動計画（６）として、総務省による定期的なフォローアップと、関係者間の情報共有・連携の継続が謳われている。

【最新の動向】

総務省では、これまでに JSSEC の場を通じて、スマートフォンに関する脅威や対策に関する民間事業者等と検討課題を共有してきた。また、平成２４年１０月には、総務省の諸問題研究会の提言等を踏まえ、スマートフォンのアプリケーション開発者やアプリケーション提供サイト運営事業者、セキュリティ関連事業者等の幅広い関係者が集まり、「スマートフォンの利用者情報等に関する連絡協議会」が設立された[19]。この場を通じて、利用者情報を不適切に収集する情報セキュリティ上脅威のあるアプリケーションの実態や、民間企業におけるアプリケーションの評価・認定に向けたさまざまなアプローチの取組状況等について、産学官で情報共有を進めている。

【今後の方向性】

今後も、スマートフォンに関連し、新たな情報セキュリティ上脅威のあるアプリケーションの発生等、脅威の状況が変化していくことが予想されることから、脅威及び事業者による対策の状況について、引き続き情報共有を実施していくことが必要である。

[19] スマートフォンの利用者情報等に関する連絡協議会　http://jssec.org/spsc/index.html