別紙２

「スマートフォン・クラウドセキュリティ研究会」の最終報告（案）に対する意見及びこれに対する研究会の考え方

平成２４年６月２９日

「スマートフォン・クラウドセキュリティ研究会」の最終報告（案）に対する意見募集で寄せられたご意見について

○ 意見募集期間：平成24年4月28日～平成24年5月28日

○ 提出意見総数： 10件

（１） 個人 ５件
（２） 法人・団体 ５件

受付順	法人・団体意見提出者
1	日本ユニシス株式会社
2	日本ベリサイン株式会社
3	北陸無線データ通信協議会
4	特定非営利活動法人　日本ネットワークセキュリティ協会
5	ヤフー株式会社

項目	頂いたご意見	ご意見に対する考え方
【意見1】「はじめに」において、本最終報告（案）が、何のために誰が何をすることを示した文書であるかを明示すべき。		
全体、特に「はじめに」	＜意見＞ 誰を対象読者とし、何のために何を訴えるのかが分かりにくい。 ＜説明＞ 本報告書は、携帯電話事業者、端末製造事業者、政府等の各主体における課題や施策を網羅的に示している点でよくまとめられているとの印象を受ける。一方、「はじめに」において、本研究会の問題意識や報告書作成までの経緯には触れられているが、結果のアウトプットとして、何のために誰が何をすることを示した文書かが明示されていない。（P3）また、スマートフォン利用者の個人情報に関わる問題や無線LANのセキュリティに関わる問題は、各々の検討主体に委ねることとして（P35）おり、その点の対策主体があいまいな印象を受ける。 このような点が、本意見のような印象をもたらすものと考量する。従って、「はじめに」にそのような点を明示する文章が補われるよう要望する。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、最終報告（案）「はじめに」を次の通り修正します。 「（略）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、関係事業者や政府等が取り組むべき方策を、最終報告としてとりまとめた。」
【意見2】スマートフォンの定義を記載すべき。		
全体	スマートフォンの定義が見当たらないので、定義していただきたい。 （理由）SIMカードが入っていなくても、Skypeアプリを載せたスマート端末は、本書で言うところのスマートフォンと機能的には差異が無いと思われます。 【日本ユニシス】	第1章第1節（1）において、「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。」としております。
【意見3】電話機能を持たないスマート端末（タブレット端末やSIMカードの入っていないスマートフォン等）も本研究会の検討対象とするべき。		
全体	本書は、携帯電話事業者が提供するスマートフォン（SIMカード付）のみを対象としているようであるが、電話機能を持たないスマート端末も対象としていただきたい。 （理由）タブレット端末やSIMカードの入っていないスマートフォン等のスマート端末もWi-Fi接続でインターネットに接続するため、これら端末についても本書で言うスマートフォンと同様な脅威が存在する。検討するのであれば両者をまとめて議論した方が、読み手に親切であると思います。 【日本ユニシス】	本研究会は、高度な情報処理機能が備わった携帯電話端末であるスマートフォンの情報セキュリティ対策を検討対象としておりますが、最終報告（案）で提示された対策の多くは、タブレット端末等のスマート端末の情報セキュリティ対策としても有効であると考えます。
【意見4】災害時の対応を検討項目に含めるべきではないか。		
全体	災害時の対応検討が全くありませんので、これは考慮すべき最重要項目と考えます。 【個人1】	災害時の通信の確保については重要な課題と認識しております。総務省では、「大規模災害等緊急事態における通信確保の在り方に関する検討会」において、緊急時・災害時における音声通話、メール、インターネット等の通信手段の確保や充実・改善について、携帯電話からの利用の場合も含めて検討を行い、平成23年12月に最終取りまとめを公表しております。 また、ご指摘を踏まえ、最終報告（案）第5章第5節（1）を次の通り修正します。 「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~~や~~や災害時に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。」
【意見5】携帯電話事業者側でログ情報を収集し、利用者に無償もしくは安価で公開する仕組みを作るべき。		
全体	インターネットのセキュリティで最も大切なものの一つが、ログ情報であることははっきり各種テキストに書かれてあるとおりである。携帯電話では、ログを残すことができないため、携帯電話側でログ情報を収集し、利用者に無償、もしくは安価で公開するような仕組みを作るべきである。これらは、かつて、電話番号を保持することが問題という運動に影響されていると思われるが、こういう考えも、完全に通信業者が保持するなと言うのではなく、通信の秘密の保持を守ってほしいと言うだけのことであり、ログに関しては業者ではなく消費者に『選択権を与えるべき』で、『業者が消費者の知らないところで勝手にログを残すな』というものに過ぎないと考える。 【個人2】	ご意見については、今後の参考とさせていただきます。
【意見6】サポートセンターにおける消費者からの問い合わせ内容も、セキュリティ向上につながるのではないか。		
全体	サポートセンターにおける消費者からの問い合わせ内容も、セキュリティ向上につながる。 【個人2】	消費者からのお問合せ内容については、各サポートセンター運営主体において、情報セキュリティやサービス向上のために適切に活用されているものと理解しております。
【意見7】スマートフォンにおいてもリカバリーができる仕組みを確立すべき。		
全体	パソコンにおけるリカバリーがスマートフォンにおいてできないのは問題である。また、リカバリーをHDD内でなく、店舗等において所持するデータなどで外部から行う仕組みも確立させるべきである。 【個人2】	スマートフォンにおいても、端末の工場出荷状態への初期化や、事前に外部にバックアップしておいたデータによる端末の復旧は可能です。

項目	頂いたご意見	ご意見に対する考え方
【意見８】スマートフォンの操作場面における危険性を指摘する記載をすべき。スマートフォンの利用基準の策定が必要。		
第１章第１節	タッチパネルを搭載した製品が主流であることから、従来の携帯電話に比べて「両手を使用した操作」が圧倒的に多く、セキュリティも重要であるが、その前に操作場面における危険性を記載した方がいいかと思います。理由は、利用時に使用者が停止している場面は少ないため、歩行などの移動中に操作し転倒事故などを起こしていることから、セキュリティ以前に使用者の生命にかかわる事象の増加が予想されるためです。この観点から見るとスマートフォンそのものの利用基準の策定が必要と考えます。 【個人１】	スマートフォン使用時の物理的な事故等への対策は、本研究会の検討課題である「スマートフォンの情報セキュリティ対策」の対象範囲からは外れますが、今後の参考とさせていただきます。
【意見９】スマートフォンが、サンドボックスを使用していることにより、PCに比べ安全性が高いとする記述を修正すべき。また、スマートフォンのOSの設計が一般的にPCより安全性が高いとされているとする記述を修正すべき。		
第１章第２節（２）	①サンドボックスを使用することによりPCに比べ安全性が高いと読める点は再考する必要があるのではないでしょうか。 （理由）スマートフォンの優位性としてサンドボックスの利用を説明していますが、サンドボックスはWindowsやMacOSでも一般的に採用されています。 【日本ユニシス】 ②「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。」は言い過ぎではないでしょうか。 （理由）前提条件、環境条件、使用方法等によってリスクは変化するので、「一般的にも安全」とは言い切れないと考えます。 【日本ユニシス】	ご指摘のように、広義のサンドボックスは、PCでも採用されています。他方、本研究会では、スマートフォンの多くのOSが採用しているサンドボックスを扱っているため、本最終報告（案）におけるサンドボックスの定義を、次の通り、より明確にしました。 第１章第２節（２）脚注 「※ここでいうサンドボックス（sandbox）とは、1台のコンピュータの中に、複数のコンピュータを仮想的に模擬する技術を用いて、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情報セキュリティモデルのこと。サンドボックスを採用することによって、プログラムは互いの保護された領域にアクセスできなくなるため、ことによって、システムが不正に操作されるのを防ぐ効果がある情報セキュリティモデルのこと。」 PCのOSでは仮想化技術を用いていないため、最終報告（案）におけるサンドボックスに該当しません。 また、本研究会では、上記定義に基づくサンドボックスを前提に設計されたOSの方が、他のOSよりも一般的に安全性が高いと認識しております。ただし、第2章第2節（2）ウにおいて記載したように、スマートフォンのマルウェア対策ソフトが、原則として他のアプリケーションの動き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ところであり、これを踏まえた対策を、第3章第2節（2）ウ及びエに掲げています。
【意見１０】「マルウェアを含むアプリケーションに対する過大なアクセス範囲の承認」に関する記述を修正または削除すべき。		
第１章第２節（２）	①「マルウェアを含んでいたり、過大な情報提供を要求するアプリケーションに対し、・・・」とされては如何でしょうか？ （理由） 過大なアクセス範囲を要求するものとして、マルウェアだけではなく、マルウェア感染が無くても、悪意のあるプログラムが存在します。 【日本ユニシス】 ②「しかし～機能しなくなるという側面がある。」という記述は、無いほうが良いのではないでしょうか。 （理由） スマートフォンの特性として説明していますが、マルウェアによる不正操作の影響はPCも同様であり、記述した場合誤解が起きる恐れがあります。 【日本ユニシス】	①のご意見を踏まえ、第１章第２節（２）を次の通り修正します。 「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。」
【意見１１】外国から持ち込まれる国内電波法の認証を得ていないスマートフォンに関する考察が必要ではないか。		
第１章第２節(３)	賛同するが追加する項目も必要。 報告書にあるとおり、無線LAN自体のセキュリティについてはWPS(Wifi Protect Setup)の策定以降進歩も無く世界的に放置されたと言っても過言ではない。国としてこの問題を忘れないという事いついては長足の進歩すら感じている。 しかしながら特に外国人が持ち込むスマートフォン、一部業者が輸入販売するスマートフォンに搭載される無線LANが国内法である電波法に係る認証を得てない機器に間する配慮も必要ではないのか。世界的競争の中で、特にアメリカ合衆国対全世界の制度の違いが際立ってきており、アメリカ合衆国おFCC（連邦通信委員会）の認可を取ったスマートフォンでハイパワー機が日本国内の電波法・総務省令に適合は今後とも見込みが立たない以上、2.4GHz帯・5GHz帯における各国の制度の違いに配慮した記述が必要だと指摘する。 【北陸無線データ通信協議会】	最終報告（案）に賛成のご意見として承ります。 その他のご指摘については、今後の参考とさせていただきます。

項目	頂いたご意見	ご意見に対する考え方
【意見12】無線LANに関する脅威として、ノイズや不要パケットをばらまく行為等の通信妨害の脅威を考慮すべき。		
第1章第2節(3)	該当項目の文書を以下の文章への変更を提案する 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や中間者攻撃の一つであるDisconnectパケットによる強制切断という脅威がある。電波利用特有の問題としてノイズ発生器を悪用し意図的にノイズをばら撒く行為そして多数の無線LAN搭載端末を使用して大量の不要パケットをばら撒く混信妨害の脅威も忘れてはならない。 理由：電波利用上、回線接続が脅かされるという脅威について配慮を求める。 【北陸無線データ通信協議会】	ご意見については今後の参考とさせていただきます。
【意見13】悪意を持ったソフトの作成者に法的な罰則規定を設けることが必要。		
第1章第2節	スマートフォンのOSについてはAndroidが主流であるが、Androidのバージョンとデバイスとの組合せにより、動作環境および利用できるソフトに差異が見られます。またSDKの普及によりAndroidのソフトは個人作成できるため、悪意を持ったソフトの発生は防止できません。よって、ソフト作成者に対し、法的な罰則規定を設けることが必要と考えます。 【個人1】	刑法第百六十八条の二及び第百六十八条の三では、「正当な理由がないのに、人の電子計算機における実行の用に供する目的で、」「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」を作成、提供、供用、取得又は保管した者を罰する規定が設けられています。 スマートフォンのソフトウェア作成者でも、上記の要件に該当する場合には、同法の規定が適用されることになります。
【意見14】「スマートフォン」と「端末」という用語が同じ意味で使用されており、統一すべき。		
第1章第2節(4)、第2章第2節	「スマートフォン」と「端末」という用語が同じ意味で使用されており、用語のゆらぎがあるので統一していただきたい。 (理由)「スマートフォン」を意味する「端末」という用語は、全て「スマートフォン」に統一するほうが読みやすいと思われる。 【日本ユニシス】	スマートフォンを構成する要素としてOS、端末(ハードウェア)、アプリケーションを区別して記述しているため、現状の記載を維持させていただきます。
【意見15】やむを得ずスマートフォンを購入している利用者の有無の調査が必要。		
第1章第3節(1)	従来の携帯電話の延長線上でスマートフォンを購入するのは、携帯電話業者がスマートフォンを主力に提供しているという事情があることから、「止むを得ずスマートフォンを購入している」利用者の有無を調査する必要があると考えます。 【個人1】	本研究会では、購入動機に関わらず、現にスマートフォンを利用している者を対象とした情報セキュリティ対策について検討を行っております。
【意見16】過去のセキュリティ事故事例の調査等を通じて、従来の携帯電話がマルウェアの影響を受けないかの検証が必要。		
第1章第3節(1)	また利用者側のセキュリティ意識ですが、「従来の携帯電話は本当にマルウェアの影響を受けないのか？」の検証が欠如していますので、メール洪水などを含めた従来の携帯電話のセキュリティ事故の過去事例を含めて調査が必要と考えます。 【個人1】	本研究会では、スマートフォンの情報セキュリティ対策を検討対象としております。 なお、従来の携帯電話は、携帯電話事業者が、情報セキュリティの確保を含め一元的に企画・設計・運用を行っていたため、スマートフォンと比較し高い安全性を有していると考えます。
【意見17】iKeeの発見年月日の事実関係を修正すべき。		
第2章第1節(1)表2	iKeeの発見年月日は平成21年(2009年)ではないでしょうか。 http://www.f-secure.com/weblog/archives/00001814.html 【日本ユニシス】	ご指摘を踏まえ、第2章第1節(1)表2のikeeの発見年月を「平成21年11月」に修正いたします。
【意見18】iOS及びWindowsPhoneの脱獄を行う主体を明記すべき。		
第2章第1節(1)ア	①「iOS及び～制限を外す行為～仕様となっている」について、制限を外す行為の主体は利用者かマルウェアか、また両方か明記したほうが良いのではないでしょうか。 (理由)「脱獄」は利用者が意図的に行う場合と、マルウェアによって強制的に行われる場合の両方があります。仕様上、マルウェアによるものは予防不可と思います。 【日本ユニシス】	ご指摘の通り、「脱獄」は利用者が意図的に行う場合と、マルウェアによって強制的に行われる場合の両方がありえますが、原文のままとさせていただきます。
【意見19】iOSについて、脱獄をしない通常の端末のマルウェア事例		
第2章第1節(1)ア	②「iOS～脱獄をしない～感染事例は確認されていない」について、感染の事実(報道)がありますので、記述をみなおされたほうが良いのではないでしょうか。 (理由)iPhoneは、2010年にPDFの脆弱性を突いたウイルス感染事例があります。 【日本ユニシス】	ご指摘の報道を確認いたしましたが、本研究会では、感染の事実は確認されていないものと認識しております。
【意見20】「Android Market(当時)」とされている記述を、最新の情報に更新するため、「Google Play」とすべき。		
第2章第1節(1)ア	「Android Market(当時)」→「Google Play」 最新の情報に更新した方がよいと思います。 【日本ユニシス】	この文脈では、「Android Market」という名称であった当時の公式サイトについて記載しているため、原文のままとさせていただきます。

項目	頂いたご意見	ご意見に対する考え方
【意見21】スマートフォンを対象としたマルウェアにより「深刻な被害が蔓延する状況には至っていない」という記述は、利用者にそれほど心配する必要はないという誤解与えるため、改めるべき。		
第2章第1節（1）ア	第2章　第1節の ア　スマートフォンを対象としたマルウェア　に記載の以下の記述における見解は、修正したほうが良いと思います。 「深刻な被害が蔓延する状況には至っていないと考えられる」 理由は、PCのマルウェアの量とスマートフォンのマルウェアの量の単純な比較からの考察のようですが、IPAが発表している「今四半期までに合計34件が届出られています」に提示されているグラフをみると、無視できない件数が届けられているからです。 http://www.ipa.go.jp/security/vuln/report/vuln2012q1.html#L6 スマートフォン以外の届け出は、94件です。マルウェアの量が少ないにもかかわらず、届け出件数が多いことは注目すべきです。 　また、PCにおける被害とスマートフォンにおける被害を比較した場合、PCと比較するとスマートフォンの方が、より機微なデータをより多く端末内に保管しているので注意喚起を行うのが、必要と考えます。しかし、「深刻な被害が蔓延する状況には至っていないと考えられる」との記述では、業界関係者のみならず、利用者においてもそれほど、心配することはないんだなと認識してしまうと思われます。 　具体的な悪意ある行動においても、差が出てきます。ワンクリック詐欺においては、PCの場合、悪徳業者から電話が直接かかってくることはないですがスマートフォンの場合、電話番号の取得もメールアドレスの取得も比較的簡単な為、悪徳業者からの電話によるアプローチが行われることが容易に想像できます。 （PCの場合、IPアドレスを記録したとかISP業者を特定したとかの脅し文句が使われますが、スマートフォンの場合、電話番号を特定したと脅すだけでなく、実際の番号を表示すると思います。もちろん、電話番号を利用したSMも送ってくると思われます） 　以上の観点から、修正すべきと考えます。 【個人5】	最終報告（案）では、第2章においてスマートフォンの情報セキュリティ上の脅威・課題について、PCとの比較も含め詳細に検討し、また第4章において利用者への普及啓発の必要性を訴えており、全体として、利用者にスマートフォンの情報セキュリティ対策を心配する必要がないという誤解を与える内容にはなっていないと考えます。また、本研究会終了後も、関係事業者や政府等において今後の動静を注視し、必要な方策を講じていきます。
【意見22】改ざんされたアプリケーションの被害を最小限に抑えるため、Android向けのアプリケーションは、Java言語の利用及び多くの解析ツールの流通により、容易に改ざん可能なアプリケーションしか作れないという事実を、業界関係者及び利用者に提示すべき。		
第2章第2節(2)	①第2章　第2節の（2）アプリケーションの課題に、アプリケーションの課題として　ア、イ、ウの3つ定義されています。その中で 　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 が記されていますが、ここに記載されている以外に、以下の事項を広く知らしめておくべきと思います。 　端末が、Androidに限定されますが、簡単に改ざん可能なアプリケーションしか作れないという事実を課題として提示しておくことが必要と思います。これは、開発者の知識・認識不足ではなく、Java言語を利用していることと、多くの解析ツールが、流通している事が原因です。 　では、なぜこの事実を、広く知らしめるべきと考えているかというとPC、Webで問題となっているフィッシングサイトへの誘導が実に簡単に行えるからです。このような課題を業界関係者のみならず利用者も知ることにより、あらゆる被害を最小限に抑えるチャンスが拡大するのではないかと考えています。 【個人4】 ②「Androidに限定すると、簡単に改ざんされてしまうアプリケーションしか作れない」という事実は、33ページ以降の　「第4章　一般利用者への普及啓発」においても明記するべきと考えます。意見1においても述べましたが、被害を必要最小限にする効果が期待できると思います。 Androidアプリケーションから、フィッシングサイトに誘導されているかもしれないという視点で、画面に表示されたWEBページを閲覧する利用者が増えることが期待できると考えます。 【個人4】	最終報告(案)では、改ざん等により作成された不正なアプリケーションによる被害防止のため、第3章第2節（2）において関係事業者における対策、第4章において利用者への普及啓発のための対策を、それぞれ記載しております。 プログラム言語の性質に起因する課題に関するご指摘は参考として承ります。なお、OSによる違いについては、第3章第1節（4）において、対策の基本的考え方として「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。」と記載しています。
【意見23】マルウェア対策ソフトに関する記述について、わかりやすい記述に修正すべき。		
第2章第2節(2)ウ	『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』・・・「その」がマルウェア対策ソフトを指すのかOSを指すのか分りにくい。「OSでは」という必要があるのか。「場合には」とするほうが一般には分りやすくないか。 『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』これは専門家でないと意味がつかみにくい表現と思われる。 全体として、マルウェア対策ソフト、OS、検査対象となるソフトウェアの関係の説明が整理されておらず、何が問題なのか分りにくい文章となっていると思われる。全体を再整理して記述されることが望ましい。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、次の通り修正します。 「マルウェア対策ソフトが提供されているOSでは、当該マルウェア対策ソフトその使用が、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。」

項目	頂いたご意見	ご意見に対する考え方
【意見24】公衆無線LANでは十分な情報セキュリティ対策が困難であり、現在の公衆無線LANのサービス展開には課題がある。		
第2章第2節(3)	公衆無線LANはほぼ全て暗号方式が脆弱であり、たとえWPA-PSKを使用したとしてもパフスレーズがSSIDに記述してある公衆無線LANサービスもある。鍵が公開されている公衆無線LANサービスにおける暗号化は無線LANセキュリティ上では意味は為さない。同様の事例が多く公衆無線LANの解説基準の制度の新設など既存の制度の変更を求めるしかない。公衆無線LANは十分なセキュリティ対策が困難、いや「出来ない」という前提があり、この問題はビジネス利用や普及の大きな妨げである。事業者は利潤追求・利便性追求がベースであり当方は多くの事業者の「過剰な宣伝」を目の当たりにしている。由々しき事態である。 免許を与えられて携帯電話事業者は踏み込むできで無いサービスが公衆無線LANであり、免許不要の無線局を「ビジネス利用」をするという危険性は未知数であり脅威のサブマリン化が益々進み現在、その脅威が国民の目にさらされる事は遠くないものと考える。 十分なセキュリティ対策が困難であることはLASDECや石川県・金沢市には何度も実例を交えて説明を行っておりセキュリティ上では在ってはならないダブルスタンダード(内と外)という現実を生み出し、無線LAN利用の実態の混乱を加速させている。 【北陸無線データ通信協議会】	ご意見については今後の参考とさせていただきます。
【意見25】「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」という記述について、補足説明を行うべき。		
第2章第2節(4)	『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』・・・ネットワーク経由とは、携帯回線または無線LAN経由で当該スマートフォンに不正アクセスすることによって、という趣旨かと思われるが、少し唐突で分りにくいと思われるので、若干言葉を補うことが望ましい。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、次の通り修正します。 「(略)当該SDカードに蓄積されたデータ~~が、ネットワーク経由~~は、アプリケーション等からのアクセスコントロールが困難であることから、アプリケーションにより抜き取られる危険性や、外部記憶媒体として~~又は~~PCに接続することにより抜き取られる危険性も~~あ指摘されてい~~る」
【意見26】通信を強制もしくは意図的に遮断するマルウェア、他の無線LAN利用者を妨害するマルウェアを考慮すべき。		
第2章第2節(5)	スマートフォンが他の無線LAN利用者を妨害する妨害電波を発射するマルウェアも考慮願いたい。通信を強制もしくは意図的に遮断するマルウェアも存在が予想されており、確認を求めたい。非常通信でこの様な事が起こった場合は人命にかかわる事でもあり、接続する事だけでなく遮断・切断されるという事についても言及して頂きたい。 【北陸無線データ通信協議会】	ご意見については今後の参考とさせていただきます。
【意見27】「グローバル展開するOS提供事業者及び端末製造事業者に、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」という認識は修正すべき。		
第2章第2節(6)	「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。」のくだりは、認識が間違っていると考えられる。 措置の実現方法は様々あるので個別具体的な要求は困難であるが、必要なセキュリティについての「機能要件」は求めることができるはずと考えます。 【日本ユニシス】	本研究会では、グローバル展開するOS提供事業者及び端末製造事業者による情報セキュリティ対策の必要性も重視しており、第3章において、個別の課題に対して事業者において取られるべき対策や積極的な検討が望まれる対策を提示しております。 今後も、国際連携等を通じて、我が国の要望を発信していくことが重要であると考えますので、意見募集後に追記した第6章において、次の通り記載しております。 「(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。」
【意見28】無線LANが日本の国内法を無視して提供される事例があり問題である。		
第2章第2節(6)	無線LANについては当方として「WiFi」という言葉で大きなごまかしが起こっていると認識している。WiFiは無線LAN機器の相互接続性を確認する為に成立したものであり、各国法の国内法に適合したというものではない。無線LANは日本では電波法及び総務省令により小電力データ通信システムという名前が与えられている。通信事業者の中にはARIB(電波産業会)で定義された表示義務を無視する事業者が存在し、ARIBの注意文書を無視し、スマートフォンブームを当て込んでARIBの表示義務無視という事実を隠して該当する何十万台の無線LAN機器を公衆無線LAN機器とこっそり交換して処理したという実例がある。 グローバルモデルのビジネスモデルでは主権国家としての日本の国内法を無視して当然という風潮があり、その象徴の言葉が「WiFi」であると当方は認識している。 国家の主権を脅かす行為を放置した総務省の公衆無線LANへの監理監督については失策と糾弾されるに十分である。グローバルビジネスモデルの前に屈服したと同義である。無線LANは国家による保護・監理を放棄したと受け取られて当然であり、今回の研究会は何かのブラックジョークでは無いのかと言われても致し方ない。 【北陸無線データ通信協議会】	ご意見については今後の参考とさせていただきます。

項目	頂いたご意見	ご意見に対する考え方
【意見29】「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。」の「最低限」の意味を明確化すべき。		
第3章第1節（1）	「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。」の「最低限」の意味を明確化していただきたい。 利用者の立場から事業者がどの程度の対策を行っているかを評価するために、「最低限必要な対策」とは何かを知っておく必要があるため。 【日本ユニシス】	ご指摘を踏まえ、第3章第1節（1）を次の通り修正します。 「（略）スマートフォン関連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、適切な情報セキュリティ対策を講じる~~にす~~努めることが重必要である。」
【意見30】対策の柱の一つに利用者の意識向上を掲げるのではなく、基本的には「事業者が対策を提供する」という方向性を示すべき。		
第3章第1節（2）	「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、・・・」ではなく、基本的には「事業者が対策を提供する」という方向性が望ましい。 現実には、お年寄りや子供を含め、ITリテラシの無い利用者が大多数であるため、一部を除いて利用者への啓発はほとんど期待できないと認識すべきと考えます。 【日本ユニシス】	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という利点をもつ反面、利用者においてもリテラシーを身につけ利用することが必要になる端末です。本研究会では、スマートフォンの情報セキュリティ確保のためには、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を車の両輪として推進していくことが重要であると考えています。
【意見31】字句の修正の指摘。		
第3章第2節(2) ア	「啓発行っていく」の「啓発」の後ろの「を」が抜けていると思われる。 【日本ベリサイン株式会社】	ご指摘の通り修正します。
【意見32】「当該指摘を考慮した慎重な検討が必要であろう」という記述に賛同する。		
第3章第2節 (2)ウ、 第4章第1節	「当該指摘を考慮した慎重な検討が必要であろう」の部分です。これは、まさにその通りだと思います。 その理由は、【意見1】にも関係するのですが、マルウェア対策ソフト自身が簡単に改ざんされるという事実があるからです。有料のマルウェア対策ソフトが改ざんされて、無料で配布された場合の被害は、想像するだけで恐ろしいものがあります。 傍証として、ある会社のマルウェア対策ソフトは、今年5月の時点でSDKに付属している難読化ツールをもちいて、改ざんされにくくするということさえもおこなっていないようです。他のマルウェア対策ソフトは、難読化処理はおこなっているようですがこれらのマルウェア対策ソフトも改ざんは、可能です。 この意見も、意見1で述べた「Androidに限定すると、簡単に改ざんされてしまうアプリケーションしか作れない」ということから派生しています。Android端末に限定される意見を2つ述べましたが、12ページの表2　マルウェアの事例　でも、1つを除いて、Android の事例ばかりですので、意見として差しさわりがないと判断しました。 【個人4】	最終報告（案）に賛成のご意見として承ります。
【意見33】文意の明確化のため文章を修正をすべき。MDMの機能について脚注等で情報を補足すべき。		
第3章第2節(2) ウ②	①『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』・・・先ず文章の構造として、主語である「システム管理者」に対応する述語として、「制限等を総合的に行う」または「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」の2通りの読み方ができてしまう。文意は後者であると思われるが、読者にMDMに関する知識が乏しいと戸惑う恐れがあるので、前者のように取られない構文に修正すべきと思われる。 ②　次に、MDMの機能については、一般に、資産管理、コンプライアンス管理、リモート管理（ロックやワイプ）を行うソフトウェアもしくはサービス、を指すものと理解されている。ここでは資産管理、コンプライアンス管理の機能によるマルウェア感染や脆弱性について語っているわけだが、2行目に『MDMの概念』という語が使われた直後にその機能の一部の記述が続く構造から、読者にMDMに関する知識が乏しいとその機能の理解に対する誤解が生じる恐れがある。脚注等を使って情報を補うような策を講じることが望ましいと思われる。 　なお、この②の最後に『留意が必要である』という語が登場するが、何に対する留意か明記されていないので分りにくくなっている。（主語も不明確） 【日本ネットワークセキュリティ協会】	①について、ご指摘の通り文意は後者であり、特段の紛れは生じないと考えます。 ②について、ご意見を踏まえ、モバイル端末管理（MDM）に次の脚注を付し、また本文を次の通り修正します。 「*MDM（Mobile Device Management）とは、企業等の情報セキュリティポリシーに基づいて、スマートフォンを一元的に管理する仕組みのこと。MDMの利用により、様々な場所にあるスマートフォンのシステム等の状況の把握や、情報セキュリティ確保の観点等から特定の機能の利用を制限する設定等を、管理者が遠隔で行うことが可能となる。」 「（略）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~~。」

項目	頂いたご意見	ご意見に対する考え方
【意見34】文意の明確化のため文章を修正をすべき。		
第3章第2節(2) エ①	『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』・・・アプリケーションのインストールに際してインストーラーが聞いてくる設定に関する問いへの回答如何で、という趣旨と思われるが、この文章ではユーザが直接サンドボックスの有効無効を選択する結果のように読める。この項目における主題に直接関わる内容なので、もう少し具体的で分りやすい書き方が望まれる。 また、続いて『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。』と述べられているが、文章が長く二つのことを言っているので、上記とも関連してわかりにくい。このままではサンドボックスが機能しなくなることと情報が流出することの間に直接の因果関係があるように読めてしまう。この文章は以下のように替えるとわかりやすくなるのではないだろうか。 「その結果、マルウェアやぜい弱性を含むアプリケーションがインストールされ、端末内部のユーザ情報が不当に流出する恐れがある。そのような場合でも、GPSや無線LANの利用のON/OFF機能に加えて、利用者がOSの設定変更をすることで、アプリケーションごとに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、柔軟にON/OFFできるようになれば、情報の不正入手や流出を防止することができる。」 【日本ネットワークセキュリティ協会】	ご意見を踏まえ、次の通り修正します。 「アプリケーションのインストール時に、過大なアクセス範囲を利用者~~の~~が承認~~を経て~~してしまえば 、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。その結果、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た後、端末内部のデータ漏出やデバイスへのアクセスといった脅威にさらされることがある。そのような場合に備え、 GPSや無線LANの利用のON/OFF機能が実用化されている。これに加えて、利用者がOSの設定を変更することにより、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。」
【意見35】スマートフォンにおいて、電源、および、通信(3G、WIFI)のONOFFを物理的にできるようにすることも検討すべき。		
第3章第2節(2) エ①	よく言われるのが、データ通信のONOFFが物理的にできないことである。エイサーというパソコンではないが、電源、および、通信(3G、WIFI)のONOFFを物理的にできるようにすることも検討すべきである。 【個人2】	現在のスマートフォン端末の中にも、端末の設定により3G、Wi-FiのON/OFFをできるものが増えています。
【意見36】ソフトウェアの利用条件や特に重要なリスク事項が、利用者にとってわかりやすく簡潔に表示されるよう法令等で義務づけるべき。		
第3章第2節(2)	明らかなマルウェアに関する対策のみならず、通常のソフトでも無用に利用者の位置情報等を入手しているものがあり、ソフトウェアの利用者がインストール時およびその後もリスクをよく理解したうえで自己責任で利用することができるように、ソフトウェアの利用条件や特に重要なリスク事項が利用者にとってわかりやすく簡潔に表示することを義務づけるべきと考えます。現在は、長々とした約款が提示されるだけで誰も読む気がせず、よく理解しないまま利用条件に承諾している実態がある。約款は約款として必要としても、その中の重要事項を法令等で列挙し、簡潔に表示させるルールが必要と考えます。 【個人3】	ソフトウェアの利用条件や特に重要なリスク事項が利用者にとってわかりやすく簡潔に表示されるように、行政や事業者等が取り組んでいくことは重要であると考えます。 最終報告(案)第3章第2節(2)イでは、「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。」と記載しているほか、同節ウ③では「アプリケーション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。」と記載しているところです。 なお、ソフトウェアの利用条件の表示については、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」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」において検討が進められております。
【意見37】オフロードという用語に注釈を付すべき。		
第3章第2節(3) 注釈31	「オフロード」について、括弧書きで注釈を追記されたほうが良いのではないでしょうか。 (理由) わかりにくい用語なので、注釈を付けた方がよいと思います。 【日本ユニシス】	ご指摘を踏まえ、初出である第2章第2節(3)に次の脚注を付します。 「ここでいうオフロード(offload)とは、携帯電話事業者のネットワークの負荷を軽減させるため、スマートフォンのデータ通信トラヒックを、無線LANなどの携帯電話事業者以外の通信ネットワークに迂回させること」

項目	頂いたご意見	ご意見に対する考え方
【意見38】無線LANアクセスポイント提供事業者等の推進施策として、証明書を用いたアクセスポイントの認証強化を加えるべき。		
第3章第2節(3)	無線LANアクセスポイント提供事業者等の推進施策として、WPA、WPA2等のクライアント認証技術の表記のみにとどめず、証明書を用いたIEEE 802.1Xによるアクセスポイントの認証についても、加味する必要がある。公共空間において、2.4GHZ帯域の混信とユーザが意図しないアクセスポイントにアクセスしてしまう問題、特になりすましの不正アクセスポイントや、WPA・WPA2のクラッキングツールが存在することから、証明書による認証強化は有効な策の一つと思われる。 【日本ベリサイン株式会社】	まずはWPA、WPA2への移行が進むことが重要であると考えます。認証方式の違い等については、次の通り本文及び脚注を修正します。 「公衆無線LANの情報セキュリティレベルの向上の前提として、WPA[31] やWPA2[32] といった暗号技術仕様 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 等が推進することが重要である。」 「※31 WPA(Wi-Fi Protected Access)とは、従来の無線LANの暗号化方式情報セキュリティの仕様であるWEP(Wired Equivalent Privacy)のぜい弱性を補強し、より強固な暗号化方式(TKIP:Temporal Key Integrity Protocol)及び認証方式を包含したもの仕様のこと。認証方式には、認証サーバを構築して認証するIEEE 802.1X方式や、事前共有鍵(PSK:Pre-Shared Key)による方式がある。なお、現在では、WEPの利用は推奨されていない。 ※32 WPA2とは、WPAと比較して、より更に強固な暗号化方式(CCMP:Counter-mode CBC-MAC Protocol)を標準とした無線LANの情報セキュリティの仕様暗号化方式のこと。」
【意見39】公衆無線LANの情報セキュリティの確保方策として、推奨する技術及び運用方法の記述を修正するべき。		
第3章第2節(3)	意見:当方が公衆無線LANを考える上で貴研究会が公衆無線LANの実態を理解していないという根拠になる部分があり、以下の通りに文章を変更する事を強く求める。 (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には限界があり、WPA-PSK/WPA2-PSKではパスフレーズを固定にして利用者に公開している。パスフレーズが公開されている事は、第三者に容易に通信内容が漏れる事になり厳密には情報セキュリティ上意味をなさない。事業者はより安全性の高いWPA-EAP/WPA2-EAPに移行を進める必要がある。非通信事業者が開設する公衆無線LANでは最低限の情報セキュリティの措置として極めて短い期間(1日～2週間)で定期的にパスフレーズの変更が必要なシステムを構築する必要がある。その上で情報セキュリティレベルを向上させるために、SSLやVPN等の活用を広く進めることが重要である。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。 【北陸無線データ通信協議会】	無線LANの情報セキュリティの確保のためには、安全性の高い技術を採用するとともに、パスフレーズを公開しない等の適切な運用を行うことが重要というご指摘として承ります。ご意見については今後の参考とさせていただきます。
【意見40】文意の明確化のため語句の修正をすべき。		
第3章第3節(1)	『自ら』・・・文意((1)の前にあるリード)から「政府が」の趣旨と思われるが、やや唐突の印象を受けるので「政府自ら」と明記してはどうか。 【日本ネットワークセキュリティ協会】	ご指摘の通り修正します。
【意見41】アプリケーションの性質という言葉の意味がわかりにくいため、例を補うべき。		
第3章第3節(3)	『アプリケーションの性質』という語が使われているが、何を意味するのかわかりにくいと思われるので、例を補う等があればよいと思う。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、最初にアプリケーションの性質について記載している第3章第2節(2)ウ③の記述を次の通り修正します。 [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。]
【意見42】「オフロード」に脚注を付すべき。		
第3章第3節(4)	『オフロード』は一般にはなじみのない言葉と思われるので脚注等で説明を補っていただきたい。 【日本ネットワークセキュリティ協会】	【意見37】への回答を参照。

項目	頂いたご意見	ご意見に対する考え方
【意見43】「人材育成策」における人材がどのような人材であるかを具体的に記述すべき。		
第3章第3節(5)	『人材育成策』とあるが、どのような人材なのか不明確であると思われる。具体的記述があるとわかりやすい。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、次の通り修正します。 「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べきである。~~またともに~~、新たな脅威に的確に対応するため、スマートフォンサービスを提供する事業者、情報セキュリティ事業者、研究機関等において活躍する高度情報セキュリティ人材について、中長期的な視点から引き続き育成やあり方に関する検討を進め、その~~人材~~育成策に取り組むべきである。」
【意見44】無線LANの現状に大きな課題がある。		
第3章第3節(5)	公衆無線LANの現状については「惨憺たる実態」を口頭にて無線LANビジネス研究会に伝え、現在当方として資料整理中である。ワールドワイドのビジネスモデルに国の主権を侵されている事も考慮しない研究会の存在価値に疑問を持ちつつこれまで蓄積した国として痛い実例の数々を文章として報告する予定である。たとえITU-Tで協議中であったとしても、各国の電波の出力や周波数が異なる事実は乗り越える事は絶望的と言い切って良い。 端的にいえば、日本がアメリカの仕様に合わせれば、無線LANの混信妨害による利便性の著しい低下は加速的に進む事になる。つまり活性化どころかパワー競争の結果、通信事業者が地域・空間の共用を排除し力を持って地域・空間を占拠し、事業者の無線LAN傍の近隣の利用者は利用を制限される事になり、急速な衰退を招く。福井県福井市のCATV局が行おうとしている無線LANメッシュネットワークは、設置自由という無線LANの原則を著しく制限する事になりかねず、衰退に至る住民と事業者との深刻なトラブルを経て無線LAN利用の衰退を加速させる原因にもなりかねない。上記の様な暴力的な占拠に国がお墨付きを与えて無線LAN設置の自由を制限するにはその代償を必要とするが、免許事業でも無い為に総務省が直接介入することは著しく困難であり自治体も根拠となる法律が存在しない事もあり対応はできません。この項目は無線LANビジネス研究会が担当するものとみられるが 、現在のところ住民視点に立った発表がなく、この意見書を緊急に無線LANビジネス研究会に送付する。 【北陸無線データ通信協議会】	ご意見については今後の参考とさせていただきます。
【意見45】違法無線LAN排除機能を公衆無線LAN事業者に義務付けすべき。		
第3章第3節(6)	総務省は電波法を放棄する事を意味するか。無線LANと言え国内法が優先される事であり、事業者の言う無線LANのビジネスモデルは国家が消滅もしくは電波に関する主権を放棄して初めて出来る事です。では、国家主権を確保するという意味で公衆無線LANの「違法機検出機能」は絶対必要であり、ビジネス推進の基礎中の基礎の機能の機能です。この論議が全くなされず、無線LANビジネス研究会で発表される国家主権の放棄を前提とした事業者の言葉に怒りを禁じえない。そして過去の総務省の政策は無線LANに関しては放置同然であった事を考えれば、その失策失政は厳しく糾弾しなければならい。また事業者の制度の「タダ乗り」は無責任極まりない暴挙であり、市民の電波のルールに関する知識・理解が無い為にこの様な事態に至ったのは総務省の監理・監督から無線LANを重視していないことの表れであり、更なる深い論議が必要である。当方としても9年以上にわたって蓄積したデータ及び事例は多数にのぼり、制度不備がどの様な事態を招いたのかを示すものになっている。当方の調査活動はあくまでボランティアベースであり、公の公表を問題されるものが非常に多い。情報の公開について政府・国会の同意が必要になるものであるがその道のりが遠い。日本が無線LAN問題にイニシアチブを取るということであれば、当方のこれらのデータはITUを始め各国の注目の的になるのは自明である。世界の無線LANの制度を一気に変革させるに充分だと当方は評価する。その上で政府・総務省がどの様な判断を当方として見極める必要がある。 電波に関わる法律・制度は、「国家(Nation)の主権の専権事項であり、既にアメリカ合衆国が突出した自由度を確保している。全世界共通ということであれば、アメリカ合衆国の国民がその権利・権益を取り上げられることになり、電波の主権放棄は行う事はないと容易に判断できる。その上で覇権国家に屈し、違法無線LANを放置しているのが今の日本国ではないのか。日本が国際社会に協調を勧めるのであれば、国内法に則った「違法無線LAN排除機能を公衆無線LAN事業者に義務付け」をする事によって漸く国際社会に発言権を得る事になると確信する。 【北陸無線データ通信協議会】	ご意見については今後の参考とさせていただきます。

項目	頂いたご意見	ご意見に対する考え方
【意見46】スマートフォン利用者の個人情報の安全対策についても本最終報告で具体的に言及すべき。一般利用者への普及啓発施策の実施主体を明示すべき。		
第4章 全般	＜意見＞ スマートフォン等の利用者である個人に属する情報の安全対策についても本報告書で言及し、その対策について具体的に、実施主体も含め、示していただきたい。 ＜説明＞ 本報告書では、スマートフォン等の利用者である個人に属する情報の安全、ならびに無線LANの利用に伴うセキュリティ課題については簡略に触れるにとどめ、各々のワーキンググループや研究会から出されるガイドや報告、並びにそれら主体による取組との組合せにより対策することとしている。(P35) が、利用者の視点に立ったときに、本報告書が主として取り上げている脆弱性やマルウェアの問題と、個人情報やプライバシーの保護の問題並びに無線LANに関わるセキュリティ問題は連関し、全体として個人にとってのセキュリティ・プライバシー対策の対象となる一連の課題と捉えられるべきである。従って、利用者個人に届く情報としてそれらが総合的、体系的に編集されて伝わることが望ましい。今回の本報告書におけるスタンスは、連携や組み合わせという表現はあるものの、これら課題の一体化や一貫性についての言及がない。 それゆえ、本報告書のみを見る者にとっては、利用者の個人情報やプライバシーの保護について、問題とされていないかの印象を受ける。本報告書においても、この課題への言及を期待したい。 ＜意見＞ 一般利用者への普及啓発のための施策の実施主体を明示されたい。 ＜説明＞ 上記の課題に関して、実際に個人に対してメッセージングや啓発活動を行う場合には、スマートフォン等の利用者である個人に属する情報の安全、無線LANの利用に伴うセキュリティ課題、そして本報告書が取り上げる、スマートフォン自体やそのアプリの脆弱性並びにマルウェアの問題の全てについて、それらが一体化して同時に伝えられるよう図られる必要がある。ばらばらに、別々の機会に、別々の主体から発信された場合には、一般利用者は何をどこまでやればいいのかわかりにくく、混乱する恐れがある。 従って、利用者の視点に立って、情報が整合して一体的に伝えられるように、対策主体者が統一的立場で対応する必要があると考える。この点の取組に、本研究会並びに事務局がイニシアティブを発揮して当たられることを期待したい。 【日本ネットワークセキュリティ協会】	意見募集後に追記した第6章において、次の通り記載しております。 「(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の面の脅威や対策について、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)」を早急に取りまとめ、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。」
【意見47】スマートフォンが反社会的、公序良俗に反する行為への悪用や、犯罪の道具として利用される危険に対する課題とその対策の必要についても言及すべき。		
全体、 第4章　全般	＜意見＞ 反社会的、公序良俗に反する行為への悪用や、犯罪の道具として利用される危険に対する課題とその対策の必要についても言及いただきたい。 ＜説明＞ 近年、情報弱者を狙った経済犯罪や性的犯罪等の深刻化が見られる。いわゆる振り込め詐欺、ワンクリック詐欺、援助交際、イジメや仲間内の恐喝等の事例が頻繁に聞かれるところである。これらの犯罪の道具として、携帯電話やネットアクセスが広く巧妙に使われていることも公知の事実である。スマートフォンは、携帯電話機能に加え、いわゆるネットゲーム等の利用により適し、かつより高度の利用を可能とする。そのため、従来以上にこの種の犯罪に悪用され、被害の拡大や深刻化を招く可能性が懸念される。 本報告書では、この問題についての言及が見られなかった。スマートフォン利用者の安全対策という意味では、この点の啓発と被害の予防も重要な課題である。本報告書においても、「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」を副題として掲げる立場からは、この点に対する言及がされることが望ましいと考える。 【日本ネットワークセキュリティ協会】	本研究会では、スマートフォンの情報セキュリティ対策を検討対象としており、ご指摘のスマートフォンが犯罪等に利用される可能性については、第2章第1節(1)において、スマートフォンのマルウェアの事例に関連して記載するにとどめております。 ご意見については今後の参考とさせていただきます。

項目	頂いたご意見	ご意見に対する考え方
【意見48】無線LANから外部に読み取られたデータが記録蓄積される可能性があることにも言及すべき。		
第4章第1節(3) イ	意見：該当箇所イ部分は非常に重要であるが不十分な内容である。 以下に修正を求める。 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データとして記録蓄積される可能性があることを認識する必要がある。 この文書を持って真のユーザーへの啓発としたい。読み取られるだけでなく記録蓄積される危険性をもつ無線LANを利用するという「リスク」について政府に再評価して頂きたく存じます。 データとして記録蓄積という指摘をもって現行制度における無線LAN利用の最大かつ致命的欠点を明らかにし、政府の無線LANを安全・安心を確立する最大の壁であり、無線LANにおいて安全性確保は非常に困難であり設置・利用については明確に制限する必要がある。 国家機関・地方公共団体・法律で守秘義務を課せられている「弁護士・医師・会計士等」では無線LANの利用は原則禁止が最も適当である。その点では、現在東京・霞が関になる日本弁護士連合会が設置する無線LANアクセスポイントは法律家の電波利用に関するブラックジョークでしかなく、通信内容の解読の可能性及び第三者に大量に通信データを蓄積されるリスクを「否定」し現在のいわゆる無法状態の肯定の象徴となっていると考える。2010年には一度注意をしたが、その指摘を無視し現在でも設置運用が続いている。当方の判断では「問題があっても、問題視されずリスクは著しく低い場合は無視で構わない。」 と考えているのではないのか。 その考えに対する反論は「堤防の白アリ」であり、現在その白アリが急速に拡大し、大事な情報を外部に垂れ流し始めている。その行く末は組織の崩壊そして国家崩壊です。 IP通信レベルで暗号化をすれば問題は無いという反論があるが、組織的に外部の第三者に無線LANデータの傍受により大量の情報を取られ認証に必要なID,PASSも不正な手段によって取得され解析に供されるリスクは絶対に無いと断言できるのでしょうか。 つまるところ、スマートフォン・クラウドにおいて職種・利用形態別に無線LAN利用の抜本的な見直しを求めるしかないと意見致します。 余談になりますが、昨年11月に一部通信事業者には、各国の通信制度の違いを考慮してGPSにて日本国である事を検知した時には自動的に無線LANの周波数・パワー等を強制的に変更する機能が必要になると提案しています。　国境を跨ぐとその国に適合したスマートフォンに変化する。この機能を実現したという話は平成24年5月現在、該当の通信事業者から聞いておりません。 【北陸無線データ通信協議会】	一般に情報が外部に不正に取得された場合、その次の段階における情報の取り扱われ方としては、記録・蓄積、第三者への提供、犯罪への転用などさまざまなケースが想定されます。ここでは、取得後の情報がどのように取り扱われるかに因らず、通信内容が読み取られる可能性があるという点が無線LANの直接的な脅威である旨を指摘しているものです。
【意見49】『データのバックアップ』に加え「データの暗号化」も記載したほうがよいのではないか。		
第4章第1節(4)	『データのバックアップ』に加え「データの暗号化」も記載したほうがよいのではないか。 【日本ネットワークセキュリティ協会】	第4章第1節は一般利用者に対して認識・実施を促す内容について記述しております。データの暗号化機能は、現時点において一般的に利用可能な機能として普及しているとは言えないため、追加することは適当ではないと考えます。
【意見50】クラウドサービスの成立の過程について、1つのパターンに限定しない記述に修正すべき。また「パーソナルクラウド」という語の使用を控		
第5章第1節	クラウドサービスの成立の沿革について、ホスティング＋仮想化の構図が示されているが、そのような事例に限らず様々な背景や技術によって様々なサービスモデルが開発され提供される中で、総称としてクラウドという呼称が定着したと考えるべきで、原文のように一つのパターンだけを限定的に書くことはミスリーディングではないか。 また『パーソナルクラウド』という語が登場するが、先ず企業向けとサービスとの時系列としてはアマゾンのS3はどちらかといえば個人向けから発祥しているし、これも断定的にいうべきでないと考える。 更に「パーソナルクラウド」という語自体が社会的認知を得ておらず、引用された調査が独自的につけた語のように思われる。これもミスリーディングの恐れという趣旨から使用は控えられるのが望ましいと思う。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、次の通り修正します。 「~~元来は、~~企業の~~IT~~情報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。その後や~~、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~~が拡大している。」
【意見51】タブレット端末もスマートフォンと同様のセキュリティが必要。		
第5章第1節	タブレット端末もスマートフォンと同様のセキュリティが必要と考えます。 【個人1】	本研究会は、スマートフォンの情報セキュリティ対策を検討対象としておりますが、最終報告（案）で提示された対策の多くは、タブレット端末の情報セキュリティ対策としても有効であると考えます。

項目	頂いたご意見	ご意見に対する考え方
【意見52】スマートフォンの普及に伴い通信の輻輳発生の恐れがあるため、一概にクラウドとの連携を行ってよいか、再検討が必要。		
第5章第1節	クラウドとの連携については、スマートフォンの普及とともにデータ通信量が膨大になるため、網輻輳発生の恐れがあります。現実に東日本大震災時には網輻輳の発生で、従来の携帯電話もスマートフォンもメールなどデータの送受信機能がほとんど使用できなかったことを踏まえると、一概にクラウドとの連携を行っていいのか、再検討が必要と考えます。 【個人1】	ご指摘の点については、本研究会でも検討を行っており、第5章第5節（1）において、データのクラウド上への保存という方策について、「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。」と記載しているところです。
【意見53】クラウド上に保存した情報に対する主要な脅威として、可用性の喪失や情報改ざんの可能性についても記載すべき。スマートフォンからのクラウド利用に関する課題として、情報の改ざんや可用性の喪失も認識すべき。		
第5章第2節、第5章第3節（2）	①クラウド上に保存した情報に対する主要な脅威に対する記載が不十分ではないか。 情報の漏えいと毀損以外にも、クラウド上のAPIの障害によってサービスの可用性が失われる事例は多い。また、JPCERT/CCインシデント報告対応レポートによるとウェブサイトが改ざんされる事例は後を絶たない。これらの脅威はPC特有のものではなく、スマートフォンにも当てはまるものである。 【日本ベリサイン株式会社】 ②課題として情報の漏えいと毀損にしか言及しない事でリスクが過小評価されている。 情報の改ざんや可用性の喪失も課題として認識すべきである。クラウドに利用者のデータが集中管理されることは多く、特に強固なセキュリティが求められるコンポーネントであるため、リスクが過小評価されることは避けるべきである。 【日本ベリサイン株式会社】	ご指摘を踏まえ、第5章第2節柱書きを次の通り修正します。 「（略）クラウド上に保存したデータから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。また、クラウドに保存したデータに、障害発生時などにアクセスできないという脅威も存在する。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。」
【意見54】クラウドサービスの利用について、ビジネス利用やPC向けが先行していたとは必ずしも言えないのではないか。		
第5章第2節(1)	①『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、』・・・クラウドサービスの利用についてビジネス利用やPC向けが先行していたという見方については、異論がある可能性がある。特に比較的早くから提供されていたGメールはクラウド型サービスと言われるが、個人がモバイル端末から利用する比率が高い可能性がある。有償サービスに限れば、企業先行、個人追随、という流れは考えられるが、無償や廉価なサービスを念頭に置くと一概にそうは言い切れないと考える。 ② 次に『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』については、「スマートフォンを経由して」と言うよりは「スマートフォンを使うことにより」という趣旨かと思われる。なお「含む」で終る文章は、「比較すると」を受けていないので例えば「様々な利用者情報を幅広く含むようになってきている」等に変えてはいかがだろうか。 ③ また、この節の趣旨からはこの項のタイトルも『利用者情報の保存』というよりは、「利用者情報の収集と蓄積」とすべきではなかろうか。ネット上の購買履歴や位置情報等が、利用者の認識の外で事業者に蓄積されることや、プライバシー情報が勝手に送信されること自体の問題もあるが、更に蓄積されたデータが集積分析されることで新たに発生するプライバシー侵害のリスクもある。この項では、その2点についてより詳しく丁寧に指摘すべきではないかと考える。 【日本ネットワークセキュリティ協会】	①について、ご意見を踏まえ、次の通り修正します。 「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るクラウドサービス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について、特段文意に紛れが生じないため、修正の必要はないと考えます。 ③ここで言う利用者情報は、利用者が意図的に保存したものか、事業者が収集したものかを区別せず、クラウド上に利用者情報が保存されていることを述べているため、修正の必要はないと考えます。
【意見55】第三者に侵入されたスマートフォンまたは、マルウェアに感染したスマートフォンからクラウドを利用することでクラウド側に発生する侵入やマルウェア感染というリスクについても考察すべき。		
第5章第2節	スマートフォンからのクラウド利用に関する脅威としては、第三者に侵入されたスマートフォンまたは、マルウェアに感染したスマートフォンからクラウドを利用することで、クラウドに侵入されたり、クラウド側にマルウェア感染が拡大する脅威も指摘すべきではないかと考える。 クラウドのマルチテナント環境やスケーラブルなリソースを考えると、マルウェアの性質によっては、大きな社会的脅威になる可能性がある。 この問題に言及されるよう提言したい。 【日本ネットワークセキュリティ協会】	ご指摘の点に関しては、第5章第3節（4）において、「仮にスマートフォンが紛失・盗難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。」と記載しているところです。 また、スマートフォンからのクラウド利用については、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、ご意見については今後の参考とさせていただきます。
【意見56】文意の明確化のため文章を修正をすべき。		
第5章第3節(1)	『その場合、利用者が、情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』・・・流れが悪く分りにくいので「その場合、情報の毀損や漏えいという危険性一般を認識している利用者であっても、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の機会が得られず、そのような判断をすることが困難になる」としてはいかがだろうか。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、次の通り修正します。 「その場合、利用者が、情報の毀損や漏えいや毀損という危険性一般を認識している利用者であっても、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の機会が与えられず、そのような判断をすることが困難になるという課題が存在する」

項目	頂いたご意見	ご意見に対する考え方
【意見57】クラウドからの情報漏えいの可能性があるため、個人情報をクラウドサービスに預けることを禁止すべき。		
第5章第3節(3)	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成21年10月9日厚生労働省・経済産業省告示第2号）では、「個人情報」について「事故または違反」があった場合の対処として、主務大臣等への報告が規定されていますが、ここで、「個人情報」とは、「個人に関する情報」であれば暗号化等によって秘匿化されているかどうかを問わない(2-1-1.「個人情報」)とされています。 この事から考えると、預けるデータが個人情報の場合は、クラウドサービスを利用してはならないと思います。暗号化してデータを預けたとしてもです。 その理由を以下に列挙します。 ・クラウドサービスを利用する個人／企業が暗号化したデータをフルコントロールできない。 （データの実体がどこにあり、アクセス権はどうなっているのか、 バックアップ媒体が実際どのように管理されているのか、 バックアップ媒体の破棄の方法はどうなっているのか、 バックアップテープなどがコピーされて流出していない という保証は？など） ・最近問題になっている標的型攻撃のすさまじさを考えるとクラウドサービス先のサーバーから、データが流出するリスクは低いとはとても言えない。 ・「事故または違反」があったか否かが、クラウドサービスを利用する側ではわからないという点も問題です。 さらに、同じページに記載されている （4）クラウドサービス利用時の認証に関する課題 で、提示されているリスクを勘案すると、クラウドサービスの利用においては個人情報（例えば、電話帳データ）を預けることは、禁止すべきと思います。（認証コードが盗まれると、データが盗まれたこともわかりません） 【個人4】	クラウドサービスを活用し、個人情報を含むさまざまな情報を管理・処理することにより得られる利便性の大きさを考慮すると、個人情報をクラウドサービスに預けることを一律禁止することは適当ではないと考えます。クラウドサービスの信頼性を向上させるため、クラウド事業者等の関係者による努力を継続していくことが必要であると考えます。
【意見58】クラウド事業者のウェブアプリケーション開発に関する技術レベルやモラル教育等も課題となる。クラウド事業者によるデータの暗号化のみを課題として取り上げることでリスクが過小評価されている。またアプリケーション提供サイト事業者は、ウェブアプリケーションの脆弱性や真正性をも審査対象とする必要がある。		
第5章第3節(3)	「クラウド上のデータの保護（「暗号化」ではなく）に関する課題」とすべきである。スマートフォンにとってクラウド事業者とはスマートフォンAPIとなるウェブアプリケーションを開発するSaaS提供者（アプリケーション開発者が兼ねる場合もある）と考えられる。スマートフォンのアプリケーションがAPIを参照する場合、ウェブアプリケーションと連動することになるため、第2章第2節で言及されているアプリケーション開発者同様、クラウド事業者のウェブアプリケーション開発に関する技術レベルやモラル教育等も課題となる。また、前項で指摘した通り、クラウドには利用者のデータが集中管理されることは多く、特に強固なセキュリティが求められる。つまりクラウド事業者はアプリケーションの開発や運用において情報の漏えい、毀損、可用性の喪失、改ざんが発生しないようアプリケーション開発者以上に万全な対応が求められるが、クラウド事業者によるデータの暗号化のみを課題として取り上げることでリスクが過小評価される。さらにアプリケーション提供サイト事業者はスマートフォンアプリケーションの脆弱性だけでなくウェブアプリケーションの脆弱性や真正性をも審査対象としなければ大きな抜け道が残ったままとなる。 【日本ベリサイン株式会社】	ご指摘を踏まえ、次の通り修正します。 「（3）クラウド上のデータの~~暗号化~~保護 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、クラウドサーバやその上で動作するウェブアプリケーションのぜい弱性検査、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技術的対策や、クラウド事業者のコンプライアンス確保を図~~を取~~ることなどが有効である~~と言われる~~。 　このうち、ウェブアプリケーションのぜい弱性については、クラウド事業者からクラウドサーバを借りて、その上にウェブアプリケーションを構築する者の対策も必要となるため、クラウド事業者による対策だけでは不十分であるという課題がある。 　また、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ものの~~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場合が多いため、そのような~~ため、~~サービス~~の内容によっては~~には、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。」

項目	頂いたご意見	ご意見に対する考え方
【意見59】「クラウド事業者等がデータの内容を把握できてしまう」という課題の本質は、暗号化の限界の問題というより、クラウド事業者のモラル、信頼性、ガバナンスの問題と捉えるべきである。		
第5章第3節(3)	この項で指摘している課題の本質は、暗号化の限界の問題よりは、クラウド事業者のモラル、信頼性、ガバナンスの問題である。例え暗号化していても復号化された瞬間盗み見や窃取が可能であるという論点は、そのような意思の存在そのものがクラウドのセキュリティ問題であると捉えるべきで、暗号化されないデータはそれ以上にリスクにさらされるわけである。すなわちこれはデータの暗号化以前の課題であり、『暗号化に関する課題』として取り上げるのは適当でないと考える。 なお、情報漏洩対策としての暗号化の問題は別のところにあると考える。通常、暗号化によるデータ保護は、その確実な実施と鍵管理の問題から、アプリケーションやシステムが自動的に行い、利用者やアプリケーションに対しては、自動的に復号化して返す構造が一般的であり、そのことによって暗号化という対策の有効性(確実に安全に機能する)が担保されている。人手と手動に委ねることの方がリスクが高いと考えるべきである。しかし、それは成りすましその他で正規のユーザと同じ立場で不正アクセスに成功した悪意ある行為者にとっては、防御としては機能しないというパラドックスがある。これはクラウドにもスマートフォンにも固有の課題ではないが、暗号に関する限界として認識しておく必要がある。暗号化は、あくまでも正規以外の手段によってディスクやファイルが持ち去られた場合でも、復号ができないために情報の価値が守られる、という構造の中で初めて威力を発揮する対策である。 【日本ネットワークセキュリティ協会】 『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』・・・単にデータを保存するタイプのクラウドサービスでは、暗号化した状態で保存する場合や、第三者等によって二重に暗号化して保存するサービス等も検討されている(これらのサービスでは、データの移動や共有設定の変更等のデータ処理が可能である)。従って、原文のように、データ処理に当たってクラウド上で暗号文を復号することを断定できない。したがって、この文は「データ処理に当たってクラウド上で暗号文を復号する場合が多い、そのようなサービスでは」等のように修正することが望ましいのではないか。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、次の通り修正します。 「(3)クラウド上のデータの暗号化保護 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、クラウドサーバやその上で動作するウェブアプリケーションのぜい弱性検査、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技術的対策や、クラウド事業者のコンプライアンス確保を図を取ることなどが有効であると言われる。 このうち、ウェブアプリケーションのぜい弱性については、クラウド事業者からクラウドサーバを借りて、その上にウェブアプリケーションを構築する者の対策も必要となるため、クラウド事業者による対策だけでは不十分であるという課題がある。 また、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もののいるが、データ処理に当たってクラウド上で暗号文を復号する場合が多いため、そのようなため、サービスの内容によってには、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。」 なお、第5章第3節(2)において、クラウド事業者の情報セキュリティレベルの重要性について記載しております。
【意見60】スマートフォンが他者の支配下に置かれる状況として、ボットウイルス感染より一般的な紛失・盗難という要素に触れるべきである。		
第5章第3節(4)	スマートフォンが他者の支配下に置かれる状況としてより一般的と思われるのが紛失・盗難である。通常、パスワードによるログオン認証で保護されるべきところだが、設定していなかったり強度が低い場合には容易に乗っ取りを許すことになる。この要素にも触れられることが望まれる。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、次の通り修正します。 なお、紛失や盗難への対策については、第4章第1節(4)に記載しております。 「(略)一方で、仮にスマートフォンが紛失・盗難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、(略)」
【意見61】アプリケーション提供サイトにおいて、クラウド利用の有無だけでなく、クラウド事業者も表示されることを有効とすべき。		
第5章第4節(1)	クラウドの利用有無のみではなく、クラウド事業者も表示されることを有効とすべきであろう。クラウド事業者のセキュリティレベルは異なる上、明示することでクラウド事業者のモラル向上が期待できる。 【日本ベリサイン株式会社】	第5章第4節(2)において、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とクラウド事業者の安全性に関する情報を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旨、考察しております。
【意見62】クラウド利用者としてのアプリケーション開発者における対策として、経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を参照すべき。		
第5章第4節(2)	ここでのアプリケーション開発者は経済産業省発表の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン(以下ガイドライン)」で記されている「クラウド利用者」と考えられる。つまり草案に記載の対策に加えて多くの課題に対する対策として「クラウド利用者」の立場でガイドラインを参照することが望ましい。 【日本ベリサイン株式会社】	ご指摘のガイドラインは、組織事業の基礎を成す情報資産の多くを、外部組織であるクラウド事業者が提供するクラウドサービスにゆだねようとする組織が、「JIS Q 27002:2006情報技術—セキュリティ技術—情報セキュリティマネジメントの実践のための規範」に規定された管理目的を達成するための管理策を実施しようとする場合に適用することとされております。ここで言うアプリケーション開発者が、当該ガイドラインにおけるクラウド利用者に直ちに該当するとは言えないため、当該ガイドラインの参照は適切ではないと考えます。
【意見63】クラウド事業者が取り得る対策として、経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」内の「クラウド事業者の実施が望まれる事項」を参照することが望ましい。		
第5章第4節(3)	クラウド事業者が取り得る対策としてガイドライン内の「クラウド事業者の実施が望まれる事項」を参照することが望ましい。クラウド事業者によってはすべての対策を取ることが時間的・経済的な制約から困難な場合でも、例えば弊社で提供しているウェブサイト向け認証サービス付属のマルウェアスキャン及び脆弱性診断機能を活用することにより、通常の脆弱性検査と比べて格段に安価にウェブサイトの安全性維持とユーザ保護に貢献できる。 【日本ベリサイン株式会社】	クラウド事業者側において、各種ガイドラインを参照することは望ましいと考えます。本最終報告(案)では、第5章第2節柱書きの脚注において、各種ガイドラインの存在に言及しております。

項目	頂いたご意見	ご意見に対する考え方
【意見64】本節で対象とする、スマートフォン利用者がクラウド上に保存する「情報」について、性質を限定すべき。		
第5章第4節(1)	【意見】 該当箇所では、クラウド上に「情報」を保存するアプリケーション（以下「対象アプリ」という。）については、アプリケーション提供サイト（以下「マーケット」という。）において、対象アプリがクラウドを利用するかを明示すべき（この明示を、以下「本件対応」という。）であるとされている。 この点、1）対象とされる「情報」についての限定がないこと、2）対象アプリについては一律に明示すべきであるとされていること、3）表示場所の選択の余地がないこと、4）有効性の検証が難しいこと、5）実効性の確保がむずかしいことが、それぞれ懸念される。以下、詳述する。 1） 対象とされる「情報」についての限定がないこと 一般に、アプリケーションの利用により生成されるデータは、①利用者が能動的に作成・保存するデータ、②他の利用者と通信することにより受け取るデータ、③アプリケーションを利用し事業者のサービスを利用することで発生する利用ログ等に分けられるが、パブコメ対象案については、これら情報の特性に応じた分析がなされておらず、包括的に本件対応を実施すべきと読めることが懸念される。 まず、②については、メーラアプリやメッセンジャーアプリを利用して受け取る情報が典型的であるが、当該情報は一次的には送信元が保存先を含めた処分内容を決めることができる情報であること、当該情報を介在する事業者に対しては既に電気通信事業法等により厳格な情報管理の義務が課されていることから、対象アプリやマーケットの提供者の負担において、情報を受け取る側に対して、本件対応を実施する理由に乏しい。 次に、③については、利用するサービスの提供事業者が対象アプリの提供者である場合とそうでない場合があるが、後者においては、アプリ事業者で情報の蓄積管理状況が把握できるとは限らず、むしろ当該他社サービスにおいて説明するのが望ましいし、いずれにしても、既に個人情報保護法及び関連ガイドラインが整備されており、当該情報を事業者側に蓄積するためには、法令に基づき事業者が開示するプライバシーポリシーによって、事業者側で蓄積する情報の種類及び蓄積の目的が開示されているところである。なお、実務上は、法令による定めより詳細かつ厳格に当該開示がされているのが一般的と思われることを付言する。 一方で、①においては、利用者において、情報の蓄積場所を確認した上で利用したいというニーズはあり得るところでもあるが、それを前提としても、次項以降で述べる懸念がある。 したがって、本報告においても、対象となる「情報」を定義することが望ましいと考える。 【ヤフー株式会社】	アプリケーションの利用により生成されるデータについて、①の場合に限らず、②や③の場合であっても、スマートフォン利用者が、自らのサービス利用行動に伴う情報の保存先について、意識できるようになることは望ましいと考えます。 　ただし、ご指摘のように表示の要否や方法については、アプリケーションの特性により相違がありうることから、次の通り修正します。 「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等に、当該アプリケーションがクラウドを利用するか否かについて、当該アプリケーションの特性に応じたが表示をすされている ことが有効である。」
【意見65】利用者が自身で生成したり保存操作を行うアプリについては、保存先が自明の場合があり得るため、「アプリの特性に応じ、適切に利用者に説明することが望ましい」とすべき。		
第5章第4節(1)	2） 対象となるアプリケーションについては一律に明示すべきであるとされていること 特に利用者が自身で、生成したり保存操作を行うアプリについては、保存先が自明の場合があり得る。例えば、ファイルストレージサービスを利用するためのアプリであれば、保存しようとするファイルがクラウドに格納されることは自明であり、本件対応を行うことが必須ではないと思われる。 したがって、本報告においても、「アプリの特性に応じ、適切に利用者に説明することが望ましい」といった表現にすることが望ましいと考える。 【ヤフー株式会社】	【意見64】への回答を参照。
【意見66】アプリケーションのクラウド利用の有無の表示場所を、マーケット上での表示に限定しない記載とすべき。		
第5章第4節(1)	3） 表示場所の選択の余地がない記載となっていること 対象箇所の記載によれば、本件対応の実施場所がマーケット上での表示に限定されている。 この点、しかし、仮に本件対応を実施するとしても、アプリの特性に合わせて、例えば、クラウドで保存するタイミングでポップアップアラートを表示することや、アプリの利用開始に先立ち閲読及び同意を要するアプリ自体の利用条件内で規定することなど、適切な表示にはバリエーションがあり得る。 したがって、本報告においても、表示方法及び表示場所を限定しない形で、記載されることが望ましいと考える。 【ヤフー株式会社】	【意見64】への回答を参照。

項目	頂いたご意見	ご意見に対する考え方
【意見67】アプリケーションのクラウド利用の有無を表示することによる定量的な効果が示されていないため、事業者の負担増や提供サービスの柔軟性に見合う効果の有無が検証されるべき。また、利用者側のアプリ選択時の判断基準についての啓発が進み、情報がどこに蓄積されるかの説明対応を丁寧に行っているアプリが競争上有利になることが望ましい。		
第5章第4節(1)	4) 有効性の検証がないこと 本報告が提出された場合、事実上対象アプリの提供者が依って立つべき指針となり得ると思われる。 この点、一般に国民の安心安全を守るための消極目的の行政目的を法令によって実現するためにはその立法事実が厳格に審査されるべきであるとされているところ、本件のような「報告」であっても事業者にとって事実上の指針となり得るのであれば、当該報告の公表に足る根拠事実が厳格に検討されるべきと思われる。 しかし、報告案においては、本件対応を実施することによる定量的な効果が何ら示されておらず、なんら根拠事実が示されていない。もし、客観的データなどによる裏付けもなく会議体の構成員の意見のみで案文が決まっているのであれば、指針の根拠として十分なものではないと考える。また、本件対応を実施した場合の、事後的な検証についても特に言及されておらず、この点においても、事業者の負担の増加や提供サービスの柔軟性に見合う効果の有無が検証されることが望まれる。 一方で、情報がどこに蓄積されるかという点に関心を持つ利用者が(潜在的にも)一定数存在することは否めないため、「アプリを選択する上で、情報がどこに蓄積されるかについても判断基準になる」ことに関する理解が一般に広がることは歓迎される。そこで、上記理解についての啓蒙を進めることにより、本件対応を丁寧に行っているアプリが、競争上有利になり、その結果本件対応の実施が進むというアプリ間競争が健全に為されたうえで、本件対応を行っているアプリが、シェアを取っていくことが望ましいと考える。 【ヤフー株式会社】	クラウドと連動したスマートフォン向けアプリケーションの利用は普及しはじめたばかりであり、今後様々な問題が発生する可能性があることから、ご意見については今後の参考とさせていただきます。
【意見68】アプリケーションのクラウド利用有無の表示について、国内事業者と海外事業者との間での対応の差が生じると利用者の混乱を招くことが懸念されるため、海外事業者も従う形で対策を実施すべき。		
第5章第4節(1)	5) 実効性の確保が難しいこと 対象アプリの提供者としては、国内事業者のみならず、海外事業者も多く存在する。 この点、仮に前述のとおり、本件対応の実施がアプリ提供者にとって事実上依って立つべき指針となるとしても、海外事業者にまで当該指針を浸透させて実施させるのは、海外関連機関との連携なしには不可能と言わざるを得ない。 一方で、国内にいる対象アプリの利用者は、国内外を問わずアプリ提供者が本件対応を実施していると期待し得ると思われるため、結果として、アプリ提供時の記載として本件対応が実施されていない場合、それがクラウドに情報を蓄積しないアプリであるからなのか、それともクラウドに情報を蓄積するにもかかわらず本件対応を実施していないのかを判断することができず、結果として利用者のアプリ選択時の混乱を呼びかねないことが懸念される。 したがって、対象箇所の記載を実施するのであれば、海外事業者もこれに従うような建付けで実施するエンフォースメント体制の下に進めるべきである。 【ヤフー株式会社】	クラウドと連動したスマートフォン向けアプリケーションの利用は普及しはじめたばかりであり、ご意見については今後の参考とさせていただきます。
【意見69】「クラウド上で暗号文を復号する場合が多いため」とすべき。文意の明確化のため文章を修正をすべき。		
第5章第4節(3)	『クラウド上で暗号文を復号するため』・・・上記18.項での指摘の通り、データ処理に当たってクラウド上で暗号文を復号することを断定できないため、を「クラウド上で暗号文を復号する場合が多いため」に修正することが望ましい。 また、3行目の『本技術』は、前後の文脈及び用語の一貫性を考えると「本要素技術」に修正することが望ましい。 【日本ネットワークセキュリティ協会】	ご指摘の通り修正します。
【意見70】一般に安全度の高い認証方式として推奨されている2要素認証をクラウド側に導入することに言及すべき。		
第5章第4節(4)	スマートフォン用とは限らないが、一般に安全度の高い認証方式として2要素認証が推奨されている。スマートフォンに固有の新たな方式への言及も否定しないが、少なくともここではクラウド側に二要素認証を導入することにも言及されてはいかがだろうか。 【日本ネットワークセキュリティ協会】	ご意見を踏まえ、次の通り修正します。 「また、二要素認証の導入の検討や、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。」
【意見71】スマートフォン端末をシンクライアント化する場合、アプリケーションのバージョンアップ、セキュリティパッチの適用もクラウドサービス事業者側の責務であることに言及すべき。		
第5章第5節(2)	『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』・・・PaaS、SaaSのサービスにおいては、特にSaaSはアプリケーションまでのバージョンアップ、セキュリティパッチの適用もクラウドサービス事業者側の責務であるので、そのことに関する言及があった方が、この項の趣旨にかなうと思われる。 【日本ネットワークセキュリティ協会】	ご指摘を踏まえ、次の通り修正します。 「このサービス形態においては、クラウド上のOS・アプリケーションのバージョンアップ、や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、(略)」
【意見72】字句の修正の指摘。		
第5章第5節(1)	『衡量』→『考量』? 【日本ネットワークセキュリティ協会】	いずれの言葉も存在しますが、メリットとデメリットをはかりにかけて勘案するとの趣旨から、原文のままとさせていただきます。

項目	頂いたご意見	ご意見に対する考え方
【意見73】OSのぜい弱性について、その他OS提供事業者の対策を追記すべき。		
別添1 表(1)ア、イ	「その他OS提供事業者」に〇を追記していただけないでしょうか。 （理由）OSの脆弱性についてはOS提供事業者こそが対応すべき、と考えます。 【日本ユニシス】	アについては、OS提供事業者から発行されるセキュリティパッチについて、携帯電話事業者及び端末製造事業者が可能な限り速やかに利用者端末に適用することを述べたものですので、OS提供事業者は実施主体に含まれません。 イについてはご指摘の通り修正します。
【意見74】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について、その他OS提供事業者の対策を追記すべき。		
別添1 表(2)ア	「その他OS提供事業者」に〇を追記していただけないでしょうか。 （理由）セキュアなプログラミングガイドはOS提供事業者こそが提供すべき、と考えます。 【日本ユニシス】	ご指摘の通り修正します。
【意見75】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について、携帯電話事業者の対策を追記すべき。		
別添1 表(2)ウ①	携帯電話事業者欄が2箇所空白となっているが、〇を追記していただけないでしょうか。 （理由）携帯電話事業者は、スマートフォンをOS（Android）の改造を含めて端末メーカに作らせているため、いかなる機能も実装可能である、と考えます。 【日本ユニシス】	端末への情報セキュリティ対策については、一義的には端末製造事業者が対応すべきものと考えます。
【意見76】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について、その他OS提供事業者の対策を追記すべき。		
別添1 表(2)ウ①	「その他OS提供事業者」に〇を追記していただけないでしょうか。（3行目のみ） （理由）カーネル部への情報セキュリティを強化するのはOS提供事業者も対応すべき、と考えます。 【日本ユニシス】	OSは端末開発用に自由度の高い形で提供される場合があり、カーネル部への情報セキュリティ対策については、一義的には、端末への実装を行う端末製造事業者が対応すべきものと考えます。
【意見77】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について、携帯電話事業者の対策を追記すべき。		
別添1 表(2)ウ②	携帯電話事業者欄が空白となっているが〇を追記していただけないでしょうか。 （理由）現実に携帯電話会社が、OS（Android）にエージェントを組み込んだMDMサービスを提供しつつあるため。 【日本ユニシス】	ご指摘の通り修正します。
【意見78】マルウェアが端末に侵入した場合の被害軽減について、携帯電話事業者及び端末製造事業者の対策を追記すべき。		
別添1 表(2)エ①	携帯電話事業者欄と端末製造時業者欄のいずれも空白であるが〇を追記していただけないでしょうか。 （理由）携帯電話事業者と端末製造事業者のいずれもOS（Android）の改造が可能なため。 【日本ユニシス】	データやデバイスへのアクセスに関するOSによる動的制御については、一義的にはOS提供事業者により対応されることが望ましいと考えます。
【意見79】マルウェアが端末に侵入した場合の被害軽減について、携帯電話事業者の対策を追記すべき。		
別添1 表(2)エ②	携帯電話事業者欄が空白となっているが〇を追記していただけないでしょうか。 （理由）携帯電話事業者は、スマートフォンをOS（Android）の改造を含めて端末メーカに作らせているため、いかなる機能も実装可能である、と考えます。 【日本ユニシス】	カーネル部への情報セキュリティ対策は一義的には端末製造事業者が対応すべきものと考えます。
【意見80】マルウェアが端末に侵入した場合の被害軽減について、その他OS提供事業者の対策を追記すべき。		
別添1 表(2)エ②	「その他OS提供事業者」に〇を追記していただけないでしょうか。 （理由）権限の最小化やOS機能最小化はOS提供事業者も対応すべき、と考えます。 【日本ユニシス】	OSは端末開発用に自由度の高い形で提供される場合があり、カーネル部への情報セキュリティ対策については、一義的には、端末への実装を行う端末製造事業者が対応すべきものと考えます。