別紙２

「一般利用者が安心して無線ＬＡＮを利用するために」（案）の意見募集に対する御意見及びそれらに対する検討会の考え方

平成 24 年 11 月２日

「一般利用者が安心して無線ＬＡＮを利用するために」（案）の
意見募集に対する御意見

○　意見募集期間：
平成 24 年９月 21 日（金）～平成 24 年 10 月９日（火）

○　意見提出総数
（１）　個人８件
（２）　法人・団体４件（受付順）
◇ イー・アクセス株式会社
◇ 日本ユニシス株式会社
◇ 北陸無線データ通信協議会
◇ 独立行政法人産業技術総合研究所セキュアシステム研究部門セキュアサービス研究グループ

	御意見の概要	御意見に対する考え方
個人①	とてもよい文書だと思います。 したがって、この文書をより一般に普及させるため、WEBで公開し、十分なSEO対策（検索エンジン最適化対策）をとるべきだと思います。 また、技術の進歩に伴い、適切に改訂していくべきだと思います。	本手引書は、総務省「国民のための情報セキュリティサイト」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm）に掲載することとしております。なお、当該サイトはSEO対策を実施する予定です。 また、御指摘のとおり、技術の進歩、無線LANを取り巻く状況の変化等を踏まえ、必要に応じて本手引書を改訂していく予定です。
個人②	別紙2： 5頁 脚注9に、 メールソフト Evolution3.4.4 グループウェアスイートにおけるメールの受信の設定及び Android 端末における Gmail 設定を追加。	メールソフトは様々なものが普及しており、設定方法も多岐に亘るため、本手引書においてそれらを網羅的に記載することは困難です。そのため、本手引書５ページ脚注９の記載のとおり「POP3s、IMAP4s、SMTPs を利用するための設定は、契約しているプロバイダーのマニュアルをよく読む」ことが適切と考えております。 よって、原案のとおりとさせていただきます。
	別紙2： １１頁 表２のレベル１（必須対策）の設定内容に、「WPA2-PSK 暗号化方式については、AES 及び TKIP を選択します。」を追加。	WPA2をはじめとする暗号化方式については、本手引書 12 ページで概要を示しております。 よって、原案のとおりとさせていただきます。
個人③	以下の危険性についての対策提示を要望。 1)スマートフォン向けのアプリケーションは、それ自体がスマートフォンの情報を要求しアプリケーション作成者に送信される仕組みになっているため、安全なアクセスポイントに接続しても、アプリケーションの入手中にハッキングされる恐れがある。しかも、アプリケーションをダウンロードする直前まで分からない場合が多い。 2)スマートフォンや PC でもレガシーOS を使用しているユーザーは多いので、必ずしもハッキング対策を実施できるとは限らない。しかも脆弱性が判明してから OS のアップデートソフトの提供という流れでは、それ以前に被害に遭っていても気づかない。 3)アプリケーション入手後、バージョンアップを行う際に、通常とは異なる Web サイトに接続することがある。アクセスポイントは安全でも、その先に繋がる Web サイトが悪意を持ったものであったら、ハッキングされる恐れはある。しかも、Web サイトに接続するまで悪意を持った Web サイトなのかどうか判断ができない。	スマートフォン向けのアプリケーション等に関する御意見は、本意見募集の範囲を超えていますので、検討会としての考え方を示すことは致しません。 なお、スマートフォンにおける利用者情報の取扱いについては、「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」の下に本年１月に設置した「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、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、諸外国の動向を含む現状と課題を把握し、利用者情報の取扱いに関して必要な対応等について検討し、提言（http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html）を取りまとめ、公表しております（平成 24 年８月）。 おって、スマートフォンに関する情報セキュリティについては、「スマートフォン・クラウドセキュリティ研究会」（平成 23 年 10 月～平成 24 年６月）において、スマートフォンやスマートフォンを通じたクラウドサービスの利用に当たっての情報セキュリティ上の課題を抽出するとともに、安全・安心なスマートフォンの利用環境の構築のために講ずべき対策について検討し、最終報告（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html）を取りまとめており、本手引書においても引用しております。
個人④	通信キャリヤやプロバイダの提供している公衆無線 LAN の端末、アクセスポイント間の WPA/WPA2 による暗号化を義務付けるべき。さらに WPA/WPA2 を実装していない端末や無線 LAN 機器は製造、輸入販売自体を規制すべき。	義務付け及び販売規制に関する御意見は、本意見募集の範囲を超えていますので、検討会としての考え方を示すことは致しません。 なお、無線LANの情報セキュリティの確保に当たっては、事業者や業界団体である Wi-Fi Alliance 等において、種々の取組が行われていくものと理解しております。
	公務員試験に高度な通信セキュリティーの問題を載せるべき。	公務員試験に関する御意見は本意見募集の範囲を超えていますので、検討会としての考え方を示すことは致しません。
個人⑤	スマートフォンなど機器側に「使う人のレベルに自動設定する機能」を搭載すべきと提言致します。	情報セキュリティ対策を自動的に施す機能としては、WPS(Wi-Fi Protected Setup)が既に存在しております。本手引書においても、10 ページの脚注 16 で「無線LAN機器の情報セキュリティに関する設定を自動で行う機能のことです。スマートフォンでは、携帯電話事業者がアプリケーションとしてこの機能を提供しています。」と解説しております。 なお、情報セキュリティの確保に当たっては、利用者自身が情報セキュリティに関する意識を高めることが重要であるとの観点から、本手引書の策定・周知を行うものです。
個人⑥	ステルス SSID 機能は推奨するべきではありません 一見、ステルス SSID 機能は安全性が向上するように感じられます。しかし実態は概ね逆であり、この機能を使うことでセキュリティリスクは増大します。 ステルス SSID 機能を利用する場合、利用者はほぼ間違いなく「SSID が隠されている」場合でも、手動で SSID を打ち込んで探すのではなく、自動で接続を行うように設定するでしょう。SSID を隠している AP であっても、近づけば自動接続するようにしたい、というユーザが殆どのはずです。 ステルス SSID に対し自動接続を許可する設定を行っている場合、クライアントは常に「隠された SSID が存在しないか？」問い合わせを行いますので、常時「隠された SSID を含んだパケット」を送信することになります。つまりステルス SSID 機能を使うことで、逆に隠された SSID をばら撒く結果となります。さらにもしこのクライアントが WEP 暗号を使用していた場合、Cafe Latte Attack や Hrite Attack により、WEP キー自体が抜かれかねません。 有線 LAN を引けずに無線で中継通信を行う場合で、AP とクライアントがそれぞれ移動しない場合は、自動接続が不要ですので、ステルス SSID の機能が有効です。	SSIDがステルス化されている場合、端末がアクセスポイントを検知するためSSIDを含むパケットを発信することは事実ですが、ステルス化時の特有の事象でございません。 よって、原案のとおりとさせていただきます。

	しかしそのようなケースは多くありません。ですので、一般の通知としてはステルス SSID の機能はむしろ、使わないように推奨した方が好ましいぐらいです。 ステルス SSID 機能は推奨するべきではありません。 参考: http://en.wikipedia.org/wiki/SSID#Security_gains_of_SSID_hiding	
	WEP 暗号への警告をより強く もはや WEP は暗号化されていないも同然です。 このような機器の使用の更新・停止が「一般利用者が安心して使うためには」推奨されるでしょう。	WEPの危険性については、12 ページに記載しております。 よって、原案のとおりとさせていただきます。
個人⑦	別紙2の資料に賛同します。しかし、無線LAN機器メーカーの取扱説明書には同様のことが既に記載(またはホームページ上)されています。 総務省殿の資料を活かすには次の点が必要ではないでしょうか。 この別紙2の資料(内容)が多くの利用者に届く(理解される)手法の検討。	本手引書は、総務省「国民のための情報セキュリティサイト」(http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm)に掲載し、WEBで公開することとしております。また、関係団体の皆様にも御協力をお願いし、広く周知を行っていく予定です。
	の別紙2の資料を理解できても、技術面が不足な利用者支援対策の検討。 例:この別紙2の「表 2　自分でアクセスポイントを設置するときの情報セキュリティ対策」における内容において、利用者がレベル3を要求したとき、利用者が上級者でない場合。	本手引書を超える内容については、御利用の機器の特性、サービスの実態等の詳細を把握する必要があるため、事業者にお問い合わせいただくことが適切と考えております。 よって、原案のとおりとさせていただきます。
	上記に関連して ・公的な機関の相談窓口は存在するのでしょうか。 ・民間が相談窓口の場合(販売業者、施工業者、通信事業者などのサービス業)、その業者を信頼できる証はないのでしょうか。 利用者が不安無く信頼できる他人に費用を払いサービスを受ける環境整備の検討。 この場合の例:工事担任者DD何種?、無線従事者何級?、民間資格のNISM?情報ネットワークプランナーなど誰が信頼できるのか。 ・平成 21 年2月の IP ネットワーク管理・人材研究会報告では、無線LANの設定は工事担任者や民間資格のNISMや情報ネットワークプランナーなどに委ねる旨の報告がありましたが、その後検討はどうなりましたか。	本手引書に対する御意見ではないため、検討会としての考え方を示すことは致しません。 なお、国家資格である工事担任者や無線従事者は、それぞれの資格が対象とする範囲で信頼性を証するものであり、民間資格についても、それぞれの実施主体が信頼性を証するものと理解しております。 御指摘の研究会の報告書のとおり、情報セキュリティ等の確保に当たっては、国家資格等を取得するなど専門知識を有する事業者を活用することが一般的に望ましいと理解しております。
個人⑧	かなり入念な対策は書いてありますが、それでも悪意のあるハッカーらとしてはいとも簡単に情報を盗むことは容易でしょう。 ですので最後にこう付け加えることを提案します。 上記のような対策を立てても完全ではない旨ご了解ください。 情報は盗まれる危険性があるのでクレジットカード等の重要情報は有線のものを使用して送ってください。	クレジットカード等の重要情報については、2、3及び4ページにおいて言及しております。 よって、原案のとおりとさせていただきます。
イー・アクセス株式会社	スマートフォンの急速な普及に伴い無線LANの利用者層が拡大している中で、一般利用者向けに特化した手引書を策定することは適切な施策であると考えます。 手引書の内容については概ね問題ないと考えますが、情報セキュリティ対策の具体的な手順がいくつか紹介されている箇所については(P.7「ファイル共有機能の解除の手順」、P.8「接続しているアクセスポイントの確認手順」等)、例えばOSがバージョンアップし画面表示が大幅に変更になるような場合等は、適切なタイミングで内容の更新を行う必要があると考えます。	ご指摘のとおり、技術の進歩、無線LANを取り巻く状況の変化等を踏まえ、必要に応じて本手引書を改訂していく予定です。
	本手引書が広く一般ユーザの目に触れるよう、関係事業者および業界団体(安心ネットづくり促進協議会、電気通信事業者協会、等)のホームページにリンクを貼るなど、効果的かつ効率的な周知を行っていくことが重要であると考えます。	本手引書については、総務省「国民のための情報セキュリティサイト」(http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm)に掲載し、WEBで公開することとしております。また、関係団体の皆様にも御協力をお願いし、広く周知を行っていく予定です。
日本ユニシス株式会社	P5　欄外記述の8 (意見内容) 「電子証明書が信頼のおける認証局から発行されている場合に、当該電子証明書に記載のあるウェブサイトやサーバが、偽造されたものではなく、その管理者によるものであることを保証する仕組みです。」との記述があるが、最後部を「その管理者によるものであることを推定する仕組みです。」と記述するのが適当であると考えます。 (提出理由) 電子署名及び認証業務に関する法律によると、法的には推定の効力(第 3 条)しか付与されていないため。 また、正規の認証局から不正な証明書が発行される事故(DigiNotar 社など)も現実に発生しているので「当該電子証明書に記載のあるウェブサイトやサーバが、偽造されたものではない」ということは保証できないと考えます。	当該箇所は、電子証明書の法的な効力を示したものではなく、技術的な仕組みを説明したものです。 よって、原案のとおりとさせていただきます。
	P10　囲み記事 (意見内容) ＜スマートフォンのデザリング機能での注意点＞の中の用語「ステルス機能」については欄外で補足説明の追記が望ましいです。 (提出理由)	ご指摘を踏まえ、以下のとおり脚注として説明を補足しました。 SSID[17]のステルス機能[18]に対応していない場合があります。 (脚注追加のため、以下の脚注番号もあわせて変更)

	一般利用者には「ステルス機能」がどういうものであるか、知らない人もいると思われるため。	[18] 無線LANのアクセスポイントは自身の存在を端末側に知らせるために、SSIDを周囲に発信しています。ステルス機能とは、このSSIDの発信を停止し、無線LANのアクセスポイントの存在を隠ぺいする機能です。
	P11　表2の最下段の設定内容欄 （意見内容） 「アクセスポイントに．．．」は「同一のアクセスポイントに．．．」が正しいです。 （提出理由） 同じアクセスポイントに接続する場合の話であるため。	ご指摘のとおり、修正します。
北陸無線データ通信協議会	■今回の（案）はガイドラインとして既に破たん状態 I.無線 LAN 情報セキュリティ3つの「約束」という言葉は行政の横暴で不適当 この無線 LAN セキュリティガイドラインは国と国民との契約書なのでしょうか。 日本国民及び在住外国人との間で同意を確認できない約束は有効な約束とは言えません。 世の中にある SSL に対応していない Web サイト・メール BOX は「約束破り」のサイト・メールサーバーとして日本政府は無線 LAN を使用し閲覧・利用してはいけないと強要している事を示す。個人サイトやブログは無線 LAN では見ていけませんと無線 LAN 接続前提のスマートフォンに強要もしくは誤解を招く事になる。そしてサービス提供側は決して破られる事はないセキュリティを確保していると幻想を振りまくガイドライン。約束できない事を約束させる事自身、現場や実例を見ない行政の横暴でしか無い。国内外の全ての Web サイト、メールやファイル転送・クラウドサービスに対し多額の税金を投入して SSL 対応を促すという「覚悟」と「計画」をお持ちなのか伺いたい。 当方としての見解は、「約束」という言葉を使った時点、このガイドラインは確認作業ができない空約束であり破綻しています。	本手引書において、「約束」とは「種々のとりきめ」（広辞苑第六版）の意味であり、契約行為を指すものではございません。 よって、原案のとおりさせていただきます。 なお、本手引書のような用例については、既に複数の行政機関が発する文書において使用されております。
	■電波法において犯罪性が否定されている傍受そのものを「盗み取る」と摩り替えたガイドラインは認められない 第三者による傍受を「悪人による盗聴」と決めつけるような電波法を扱う主管庁として如何なものと言える表現があり、電波を扱うプロフェッショナルとは到底考えられない概念が入り込んでいる。このガイドラインが電波法の概念を理解していない事務局・ガイドライン作成担当者が勝手に作り上げた「作文」と決めつけることができる。 「第三者による傍受」による大量の通信データの記録について考慮させないガイドラインは電波利用において不適切であり、無線 LAN の危険性を国民に理解させるに不十分だと考える。 今回の（案）ではサービス提供側はこの「第三者による傍受」による大量の通信データの記録について、無線 LAN 利用者ではなくサービス提供側に責任が移るという事を意味し、将来 SSL が解読され危険視される事態になった場合、サービス提供側が訴訟を受け多額の賠償請求が発生するものと理解して宜しいだろうか。	本手引書は法令文書でないことから、一般の方々により分かりやすい表現を用いております。 よって、原案のとおりとさせていただきます。 その他の御意見については、今後の参考とさせていただきます。
	■SSL（Secure Socket Layer）至上主義は極めて危険 SSL 至上主義という概念が入り込み、SSL に対応しないサービスは無線 LAN では使うべきでないとなる。SSL はサービスを提供する側が行う暗号化サービスであるが無線 LAN はあくまで自律的にその危険性を判断して使うものである。これは無線 LAN もサービス側がコントロールして制御下に置くことも意味するものであり、サービス側に公金投入の口実を作るものであり如何なものか。 また、SSL は日本政府・総務省がその安全性を担保する暗号実装の技術としたことはもろ刃の剣である事を改め認識して頂きたい。 その上で、以下に示す文章を付け加えて頂きたい。 「SSL は現在の技術水準では解読が難しいものですが、将来に渡って解読が出来ないと保証するものでありません。安全性を確保するための技術水準の時代変化に対応する為ガイドラインは改訂されます。」 この文章を入れない場合は、政府・総務省は SSL の安全性について評価を誤ったとして訴訟において不利になり混乱と不安を招くものになると考えます。	今後の参考とさせていただきます。
	■総務省は原則に立ち戻って無線 LAN を考え直すべき 当方としては、無線 LAN 利用はあくまでも利用者本人の自覚が原則であり、SSL は利用者がサービス提供を受けないとその対応・対策すら利用者は出来ない。この矛盾を抱えてしまった今回の案は「約束」という言葉を使いサービス提供者側に税金投入を行うための作文になったと判断する。つまり、利用者の自律という原則を捻じ曲げて破綻したものであると結論付ける。しかも、通信事業者は世界的競争にさらされ訴訟リスクを増大さ数多くの犯罪に巻き込まれる事になる。その対応に疲弊しているサービス提供者の救済のための税金投入に使用される理由書でしかないのか。 訴訟や混乱を政府として回避するには、無線 LAN 利用について本来政府は「お願い」しかできないのであり、免許不要局として「監	今後の参考とさせていただきます。

	理」をこれまで放置してきた結果を踏まえて以下の様に書き替えて頂きたい。これは今回のガイドラインの初期から関わってきた当方の数多くの観測データ・事例から導き出された当方の結論でもある。 さらに、＜お願い4＞として数多くの行政機関や団体・民間企業が古い無線 LAN を運用もしくは「放置」し、しかも放置の実態を把握できていない事例がある。この為、お願い4を追加する。 I.無線 LAN 情報セキュリティ4つの日本国政府・総務省からのお願い お願い1. 無線 LAN を利用する時は、大事な情報は SSL でやりとり電波法の下では無線 LAN 利用時には通信内容を第三者に見られる事を前提として考えなければなりません。その為、無線 LAN 利用時の全ての通信は SSL でやりとりする事が望ましいが、ID・パスワード等のログイン情報、クレジットカード番号やセキュリティコード、暗証番号といった決済に関する情報や個人情報・プライバシー性の高い情報等社会通念上大事な情報は SSL により暗号化されている事を確認する事をお願いします。 SSL は現在では強固な暗号とされていますが、技術の進展で将来解読される事も予想されています。常に無線 LAN の通信内容は第三者に見られている可能性がある事を忘れないでください。 （サービス提供側については SSL 利用について必ずそのサービスを利用中であることを画面及び画面の色・形を大きく変化させ利用者に SSL 利用中を認識させる事を努力する事を求める。） お願い2. 無線 LAN を公共の場で利用するときは、ファイル共有機能を解除 公共の場で無線 LAN を利用する際に、ファイルの共有機能が有効になっている。他人からパソコンやスマートフォン内のファイルが読み取られたり、ウイルスなどの不正なファイルが送り込まれたりすることがあります。 ファイル共有機能の利用は、予めファイル共有機能を利用する事を許可した家庭や職場の LAN のみにして見知らぬ第三者が利用する無線 LAN では避けることをお願いします。意識的に ON・OFF に自信の無い利用者は自動的に LAN のタイプを区別してファイル共有機能を ON・OFF できる端末もしくはアプリケーションの利用をお願いします。 お願い3. 自分でアクセスポイントを設置する場合には、適切な暗号化方式を設定 自分で設置したアクセスポイント（親機）でも、電波の届くところから気が付かないうちに通信内容が第三者に見られたり通信内容を勝手に保存されたり、無断でウイルスの配布などに悪用されたりする危険性があります。そのため、家庭の無線 LAN の親機やモバイル Wi-Fi ルータ、スマートフォンのテザリング機能を設定する場合は、WPA2（AES）により暗号化する事をお願いします。その際、アクセスポイントと端末との間に設定するパスフレーズ（パスワード）は、記号（！”＃＄％）等を含むなるべく長い（２１文字以上）ものをお願いします。また WEP(Wired Equivalent Privacy)の利用・設置は出来る限り避けて下さい。 お願い4. 古い無線 LAN 機器は電源を OFF するか捨てましょう。 古い無線 LAN 機器には暗号化機能が WEP のみしか設定できないものや自動暗号化機能があっても十分な強度を持たない機器があります。暗号化機能の設定が煩雑なものがあり、暗号化無しで運用される事例も見られます。無線 LAN 機器が安価になり暗号化機能も進歩しています。この為、古い無線 LAN の利用を止め、破棄する様お願いします。	
	■各ページについて問題点を言及します。 今回の案は「サービス提供側」「利用者側」が区別されていない乱暴極まりないガイドラインであり、無線 LAN セキュリティガイドラインと一般国民に向けるのであれば利用者側の視点に立って記述が必要になる。この視点から整理すると以下の通りになる。 1. 大事な情報は SSL でやりとり 問題点： この問題はあくまでもサービス提供側が問題であり、無線 LAN セキュリティ対策とは言い難い。 無線 LAN セキュリティのガイドラインとして SSL は無線 LAN 以外でも一般的な対応であり、敢えて示す必要があるのか疑問。問題は通信を「第三者に簡単に傍受され蓄積される事」であり、あくまでも電波を使う以上、通信内容は第三者が容易に知り、蓄積できることを強く言えば良い。この原則を無視したガイドラインは繰り返しになるが「破綻」しているとしか言えない。 付け加えるなら、サービス提供者側が行わなければならない項目を別に作りレベル0としてサービス提供側の義務としなければならない。ただこの項目は無線 LAN セキュリティガイドラインとして考える場合、極めて不自然な項目であり今回の改訂はサービス事業者中心のガイドラインであるとしか言えない。 また SSL の証明書は RSA1024/2048 及び SHA-1 を使う証明書が未だに大多数であり、これらは日々進歩している GPGPU や CUDA	今後の参考とさせていただきます。

	等の安価な高速デスクトップPCでもその解読の可能性が現実味を帯びてきている。事実、13文字の0～9、A～Fまでの文字列を使用したN社製自動暗号化機能で対策されたWPA仕様の無線LANアクセスポイントは、現状手に入る高速なデスクトップ PC 上では 100 年以下で解読可能という事が実験データから推測できるまでに至った。これは 1000 台あれば0．1年つまり1ヶ月程度で全ての認証鍵パターンを検索できる事を意味する。ガイドラインでも基準を明確にしていないパスフレーズ（パスワード）の問題点であり、被害が出た場合はもはやガイドラインを制定した総務省・及び研究会の責任を問わなければならない。 解読の危険性が日々高まっている以上、無線LANによる金融機関のサイトへのアクセスや、他人に知られなくない情報を通信路として使用する事は極力避けましょうという呼びかけが一番適当である事を意見として付記する。 本来、一部通信事業者が「免許を受けない無線局」である無線LANを事業遂行の為に便利な通信路として活用とする事自身が間違い。この為の対応として、教育啓蒙は十分に行きわたっているとは言えず、マスコミ・メディアも通信事業者の広告宣伝に配慮し無線 LAN を利用した事件・情報漏えい事故を報道しない事になっており、教育啓蒙の障害になっている。	
	P.7 ○論理的欠陥を抱える部分 現行法では知らないアクセスポイントには接続する事は違法とは言えないが、「無断利用」は社会生活を営むこの社会においては基本的には窃盗や所有権の侵害にあたり罰せられて当然の行為である。この（3）はこのガイドラインに於いては理解に苦しむ内容でありこの記述は一切認められない。 以下の様に変更すべきである。 （3）知らないアクセスポイントには接続しない 無断で知らないアクセスポイントには接続しない様お願いします。 第三者の所有物を勝手に利用する行為は不正行為と見なせます。 その不正行為を逆に利用し、アクセスポイントに接続してくる無線LANの通信を盗み取られる可能性もあります。 また第三者に勝手に利用されるような無線 LAN アクセスポイントの設置も行わないでください。悪意で無断利用された場合、設置者も加害者になり罰の対象になる可能性もあります。	本手引書でいう「知らないアクセスポイント」とは、「誰でも利用可能とされているが、利用者が設置者等の管理情報の詳細を確認、又は推測できないアクセスポイント」を指しており、御指摘は当たらないと考えております。 よって、原案のとおりとさせていただきます。
	P.3 1．無線 LAN を利用する時の情報セキュリティ対策 ではなく 1．無線 LAN 経由した通信を利用する時の情報セキュリティ対策 もしくは 1．無線 LAN を利用したサービスを利用する場合の情報セキュリティ対策 に変更すべきではないのか。電波利用という原則を無視したにも拘らず「無線 LAN を利用」という言葉を使うのは本末転倒で無線 LAN の実態を理解していないと批難されるに十分である。	今後の参考とさせていただきます。
	P.10 大きな問題点が以下の文である。 2．自分でアクセスポイントを設置する時の情報セキュリティ対策 一般個人を指す「自分」という単語を使用するのは、今回のガイドラインがサービス提供側の視線で一般（市民）の設置を見ているものであり、奇異すら感じる。 アクセスポイントの設置は利用者が自営で設置した後で通信事業者が公衆無線 LAN として割込んできたものであり、自営の設置について明確な単語が出来なかった事がこの「自分」という極めて異様な言葉が出てきた背景にあると考える。 つまり以下の様に書きなおす必要がある 2．（通信事業者の公衆無線 LAN 以外の）無線 LAN アクセスポイントを設置する時の情報セキュリティ対策 と、態々通信事業者が設置した公衆無線 LAN を除外した書き方をしなければならない。ただし、過去のガイドラインで設置者の判断で第三者に提供する店舗開放型の無線 LAN を公衆無線 LAN と言うのか問題が多い。それは通信事業者との回線利用契約では第三者への貸し出しを禁止した契約を交わす事例が多い事もあり、第三者への貸し出しについて無断も同意も関係ない空気が作られている。実際に第三者への貸し出しを禁止した事を知る無線 LAN 設置者はどれだけいるのか。間違いなく極少数であると考える。 不特定多数の利用者を考える場合でも、通信事業者側は通信の秘密を振りかざしてフィルタリングを義務化出来ない社会環境は異様と言えよう。行政は国民の生活の安全確保ができるのか、疑問が深まるばかりである。 当方の無線 LAN 問題において、公衆無線 LAN は「通信事業者として登録の無いもしくは、第三者への回線の貸し出しに関し研修を受け登録しない団体・個人の無線 LAN は禁止する。」しかない。さらに、「無料」は責任の所在を管理者・設置者が訴訟による賠償を逃	今後の参考とさせていただきます。

	れるためのテクニックであり問題。基本的にサービスの対価を利用者に請求すべきである。	
	P.11 についても電波法の原則や WPA/WPA2 では「パスフレーズ」という用語を使用するが「パスワード」と WPA/WPA2 の体系を無視する様な単語を使用し態々市場を混乱させる為に勝手に「パスワード」という言葉を使ったのではないのかと疑われても仕方がない。 またパスフレーズ（パスワード）の設定の基準についても明確に示さない等、ガイドラインとして技術的な検討が成されたとは言い難い記述。 スマートフォンに内蔵されている無線 LAN 機能の情報セキュリティ対策を意味した記述であり、これらは「別研究会」もしくは「サービス提供側だけでなく一般の利用者視点で技術的背景を明確化もしくは再検討」を意見します。 総務省のガイドラインが一般国民にも行き渡らず、さらに地方公共団体や日本を代表する方々にも無視されているという現状を鑑み、これらのガイドライン及びの在り方そのものを再考して頂きたい。	今後の参考とさせていただきます。
	中国語・韓国（朝鮮）語・英語版の翻訳は政府として行い発表する事は必要である。更に World Wide 対応ということであればポルトガル語・スペイン語・ロシア語・イタリア語・ポーランド語・タガログ語ら東南アジアの諸言語版も最低限必要である。	今後の参考とさせていただきます。
	国民的な議論を通して立法府（国会）を通し刑事罰の罰則を伴う無線 LAN 保護法（仮称）を制定する必要を主張します。 業務・個人、公衆・個人、サービス提供者・利用者そして無線 LAN における屋外と屋内、国外と国内と区分区別がいい加減であいまいな通信システムの蔓延は安全安心を考える上で懸念でしかない事を最後に付け加えます。	本意見募集の範囲を超えていますので、検討会としての考え方を示すことは致しません。
独立行政法人 産業技術 総合研究所 セキュア システム 研究部門 セキュア サービス 研究グループ	表 1(4)の対策を削除するべきではないか。 理由： 表 1(4)で対策として「公衆無線 LAN サービスのログイン画面に電子証明書エラーが表示されたら接続しない」とありますが、このような説明は、「公衆無線 LAN サービスのログイン画面で電子証明書エラーが表示されなかったなら、正規のアクセスポイントである」との誤解を誘引するものであると考えられます。偽アクセスポイントを用いて盗聴を試みる攻撃者は、電子証明書エラーが出ないよう、そもそもログイン画面を出さずに接続を受け入れるように偽アクセスポイントを設置することが可能です。その場合、利用者からすれば、「正規のアクセスポイントを使っているつもりが、気づかない間に偽アクセスポイントに切り替わっていた」という事態となるため、対策としては不適切であると考えます。 このような攻撃は、偽アクセスポイントで ・SSID を公衆無線 LAN サービスのものと同一の名前に設定 ・事前共有鍵を当該公衆無線 LAN サービスのものと同一の鍵（鍵は同サービスの利用者全員で共通のものであるため、公知の情報）に設定することで可能となります。この攻撃手法は「Evil Twin」と呼ばれ、古くから知られている攻撃です。 http://en.wikipedia.org/wiki/Evil_twin_%28wireless_networks%29 本攻撃が行われる可能性がある状況で、対策となり得るのは、表 1(1)の対策「SSL でやりとり」することです。この対策を徹底することにより、公衆無線 LAN の使用は安全になります。(4)は対策とはなっておらず、さらには安全でない場合を安全だと誤解させる危険があるので、削除することを提案します。 それに伴い、p.7 の(4)の節も削除することを提案します。 p.7 の(4)にある「SSL が使われてない場合や、SSL が使われていても電子証明書のエラーが表示される場合には、偽のアクセスポイントに接続している危険性があります。「公衆無線 LAN サービスにログイン画面が表示されるときには SSL という通信方法が使われていることを確認しましょう。」との記述は、「SSL が使われていることを確認してエラーが出ていなければ偽アクセスポイントではない」との誤った理解を招く危険性が高いです。実際には、攻撃者は、偽アクセスポイントに接続させた後、任意の Web サイト上に正規のサーバ証明書を設置して偽のログイン画面を設置することや、そもそもログイン画面など出さずに接続を継続させて盗聴することが可能です。(4)の対策を回避できる攻撃がありますので、本対策を記述するのは不適切であると考えます。 また、p.18 の記述も改める必要があります。この部分では、「同一の名称（SSID）、暗号化方式、パスワードが設定されると、それが本来接続するべき正しいアクセスポイントなのか、正しいアクセスポイントになりすました不正なアクセスポイントなのか判別できない	表 1(4)は、「公衆無線LANサービスのログイン画面に電子証明書エラーが表示」された場合は、明白な危険があることを示すものであり、「エラー画面が表示されていない」ことを「安全」であると述べているものではありません。 よって、原案のとおりとさせていただきます。

	ことがあります。」として、上記の「Evil Twin」の問題が想定されているにもかかわらず、事例のエピソードでは、「「証明書エラー」という画面が表示されたがよくわからなかったので」と、あたかも、証明書エラーによって偽アクセスポイントを見分けることができるかのように書かれています。「Evil Twin」が行われている状況では、偽アクセスポイントを見分けることはできないので、このような記述は削除するべきと考えます。 同様に、p.18 の黄色の囲み「＜問題点＞」の部分でも、「証明書エラーが表示されるなど、いつもと違う様子に気づかないまま、不正なアクセスポイントに接続したため」と書かれていますが、このような記述は、読者に、「いつもと違う様子に気づけば不正なアクセスポイントへの接続を発見できる」と誤った理解をさせる危険が高いものであり、削除するか他のエピソードに変更する必要があると考えます。	
	表 1(5)の対策を削除するべきではないか。 理由： 表 1(5)で対策として「接続しているアクセスポイントを確認」とありますが、どのようにすれば確認できるのかが具体的に示されていません。同一の SSID、同一の事前共有鍵で動く偽アクセスポイント（意見 1 参照）を、本物と見分けることは現実的に不可能です。このような対策を掲げることは、「SSID が正しいので正規のアクセスポイントである」という誤解、それに基づく誤った対策法の流布等を招く危険性があるため、本記述を削除することを提案します。 それに伴い、p.7 の(5)の節も削除することを提案します。 「どのアクセスポイントに接続しているか確認しましょう。」との記述がありますが、何をどのように確認すれば安全であるかが示されていません。また、p.7 には「公衆無線 LAN サービスを利用するときには、偽のアクセスポイントでないか、サービス事業者のアクセスポイント検索やステッカーなどで、その場所で本当にサービスが提供されているのか確認することも有効です。」と書かれていますが、そのような確認を実施することは現実的ではありません。本物のアクセスポイントがある場所で、偽のアクセスポイントを設置して盗聴する攻撃があり得るため、対策としては不適切であると考えます。	偽のアクセスポイントを判断することは困難であることは承知しておりますが、本手引書の7ページで示した「公衆無線 LAN サービスを利用するときには、偽のアクセスポイントでないか、サービス事業者のアクセスポイント検索やステッカーなどで、その場所で本当にサービスが提供されているのか確認する」ことは、一定の効果が期待できるものと理解しております。 よって、原案のとおりとさせていただきます。
	表 1(6)の対策を削除するべきではないか。 理由： 表 1(6)で対策として「アクセスポイントが暗号化に対応していることを確認」とありますが、暗号化されていることを確認しても、そのアクセスポイントが、正規のものと同一の SSID、同一の事前共有鍵で動く偽アクセスポイント（意見 1 参照）であった場合には、通信内容は盗聴されてしまいます。このような対策を掲げることは、「アクセスポイントが暗号化に対応しているから大丈夫だろう」という誤解、それに基づく誤った対策法の流布等を招く危険性があるため、削除することを提案します。 それに伴い、p.8 の(6)の節も削除することを提案します。 SSL の必要性と SSL が利用されていないときの危険性については、既に p.4 に書かれています。	表 1(6)においては、偽のアクセスポイントではなく、通信内容を盗み見られることへの対策を記載しております。 よって、原案のとおりとさせていただきます。
	P.5 のコラム内、メールサーバへの接続で SSL の利用を必須とするべきではないか。 公衆無線 LAN サービスを利用する場合、SSL による暗号化が必須であるところ、メールサーバへの接続で送信されるパスワードをどう守るかが問題となります。この点について、p.5 の「SSL について詳しく知りたい方へ」のコラムと脚註 9 で触れられているものの、「ご利用の電子メールサービスが SSL に対応している場合には（略）通信を暗号化できます。」という表現で書かれており、必須の要件としては書かれていません。 メールサーバのパスワードは、他のサービスのパスワードと同じ文字列であることが少なくないと考えられることから、メールサーバへの SSL 接続は必須である旨を明確に打ち出すべきです。利用中のメールサービスが SSL に対応していない場合については、公衆無線サービスを利用しないよう促すべきです。 このことは、コラム内で簡単に触れるのではなく、p.4 の本文中に記載することを提案します。	メールのSSL対応はWEBと比較して一般的でないため、必須とはしません。ただし、御指摘の趣旨を踏まえて、当該部分はコラムに記載することとし、文章を以下のとおり修正します。 電子メールの内容やパスワードなどが知られることを防ぐことができます~~。~~<u>ので、積極的に利用しましょう。</u>
	表 2(2)の対策を削除するべきではないか。 理由： 自分でアクセスポイントを設置するときの対策として、SSID を推測困難に設定し、ステルス機能を活用することが挙げられています。	SSIDのステルス化が万全の対策でないことは承知しておりますが、管理の不備等によりパスフレーズが漏えいした場合においても、SSIDのステルス化によりアクセスポイントへの接続を防止できるなど、一定の効果が期待できるものと考えております。 同対策を回避する手法もございますが、回避に当たっては専門的

	しかし、表 2 の「備考」にも書かれているように、ステルス機能を用いてもその SSID を完全に隠すことはできません。したがって、ステルス機能を対策として挙げることは不適切であると考えます。また、SSID を推測困難なものにすることも、完全に隠すことができないわけですから、対策として不適切であると考えます。 表 2 には「メーカ名が推測できる SSID にしていると、攻撃を受ける危険性が高くなります。」との記述がありますが、なぜ高くなるのかが具体的に示されていません。SSID をランダムに設定しても、MAC アドレスからメーカーを推定することが可能です。続いて、「SSID を簡単には推測又は検出されないようにすることで、他人から無断で利用されるなどの危険性を低くすることができます。」との記述がありますが、表 2(1)の対策、すなわち WPA 等で適切な暗号化設定をしていれば、「他人から無断で利用される」ことは、盗聴されないのと同等の確実さで防止することが可能です。「他人から無断で利用される」リスクとその対策については、表 2(1)の対策の解説中で書くの適切であると考えます。 なお、「SSID として自分の名前などを設定すると、他人の興味を不用意に惹く危険性があります。」との点については、プライバシー等の問題として重要な点であり、解説しておくことが望まれますが、盗聴や無断利用といったセキュリティ上の問題とは別の問題であることから、表 2 の中に記載するのではなく、コラム等の欄外で記載するのが望ましいと考えます。	な知識が必要であることから、一定の効果が期待できるものと考えております。 また、SSIDがメーカー名の場合、当該メーカーの製品に特有のぜい弱性が確認された場合、攻撃を誘引する危険性があります。MAC アドレスからのメーカー名の推測も専門的な知識が求められることから、一定の効果が期待できるものと考えております。 また、「SSIDとして自分の名前などを設定すると、他人の興味を不用意に惹く危険性があります。」との記述は、プライバシーの観点だけでなく、攻撃対象となる潜在的危険性を低減するとの意味がありますので、情報セキュリティ対策として取り扱うことが適当かと存じます。 表 2(1)では既に、「アクセスポイントの無断利用の危険性」について言及しております。 よって、原案のとおりとさせていただきます。
	表 2(4)の対策は削除するべきではないか。 理由: 自分でアクセスポイントを設置するときの対策として、MAC アドレスフィルタリングの利用が挙げられています。しかし、表 2 の「備考」にも「この対策では防止できません。」と書かれているように、それを回避できる方法がありますので、対策として書くのは不適切であると考えます。 表 2 には「アクセスポイントは他人に無断で悪用される危険性があります。」との記述がありますが、表 2(1)の対策、すなわち WPA 等で適切な暗号化設定をしていれば、「他人から無断で利用される」ことは、盗聴されないのと同等の確実さで防止することが可能です。「他人から無断で利用される」リスクとその対策については、表 2(1)の対策の解説中で書くの適切であると考えます。	MACアドレスフィルタリングが万全の対策でないことは承知しておりますが、管理の不備等によりパスフレーズが漏えいした場合においても、MACアドレスフィルタリングによりアクセスポイントへの接続を防止できるなど、一定の効果が期待できるものと考えております。 同対策を回避する手法もございますが、回避に当たっては専門的な知識が必要であることから、一定の効果が期待できるものと考えております。 また、表 2(1)では既に、「アクセスポイントの無断利用の危険性」について言及しております。 よって、原案のとおりとさせていただきます。
	事前共有鍵をランダムで長いものとすることを必須とし、その長さの目安を示すと有用ではないか。 理由: 表 2(1)の対策の説明で、「パスワードはなるべくランダムで長いものにします」との記述がありますが、今日では、オフライン攻撃による事前共有鍵の復元攻撃が広く知られていることから、「なるべく」ではなく必須とし、長さの基準を明確にするのが読者にとって有用ではないでしょうか。 事前共有鍵のことを「パスワード」と表現すると、一般の読者は、Web サイトで用いるパスワードと同様のものを連想してしまい、例えば 8 文字程度で十分に強固なものと誤解してしまう危険性があります。Web サイトで用いるパスワードの場合では、オフライン攻撃の危険性がなければ、多過ぎるパスワード試行をロックすることによりオンライン攻撃を防止できるため、8 文字程度のパスワードでも十分であるのに対し、無線 LAN の事前共有鍵の場合は、傍受したパケットを元にオフライン攻撃によって事前共有鍵を復元する手法が知られているため、より長くランダムな鍵を設定する必要があります。 ランダムな英数字と記号で設定する場合何文字以上必要か、数字だけならば何桁以上必要か、長い文章ならば何文字以上必要かといった目安を示してもらえると、読者は適切に対策し易くなると考えます。 また、無線 LAN の話題において「パスワード」の語を用いると、パスワードが何を表しているのか混乱を招くおそれがあります。無線 LAN において「パスワード」と表現され得るものは少なくとも 3 つあります。 (a) 事前共有鍵 (b) 公衆無線 LAN サービスにおける利用者認証のログイン画面用のパスワード (c) 自分で設定するアクセスポイントの管理者設定用のパスワード	御指摘を踏まえ、御意見中の事前共有鍵の意で使用している「パスワード」については、無線LANの規格書「IEEE802.11™–2012」等に準拠して「パスフレーズ」に修正し、2ページに脚注としてパスフレーズに以下の説明文を加えます。 アクセスポイントと端末との接続に必要な鍵で、事前に共有しておきます。なお、本鍵はパスフレーズのほか、暗号化キー、暗号キー、共有キー、事前共有キー、ネットワークキー、パスワード、Pre Shared Key 等と呼ばれています。 また、2ページの「約束3」及び 11 ページの表2(1)の「設定内容」の説明文から「なるべく」の文言を削除し、脚注としてパスフレーズの長さについて説明文を追加しました。 推奨されるパスフレーズの長さについては、文献により異なりますが、無線LANの規格書(IEEE802.11™, 2012)には、「A key generated from a passphrase of less than about 20 characters is unlikely to deter attacks.」と記載されており、おおよそ 20 文字以上を推奨しています。

	混乱を招かないように、表 2(1)の対策で「パスワード」としているものが(b),(c)のことではなく(a)のことである旨がわかるように記述すべきであると考えます。	
	隣人が平然と不正アクセス禁止法違反行為をするというエピソードを用いるのは避けるべきではないか。 p.15 で事例として、「A さんのメールの ID とパスワードを知ることができた。C さんは A さんのメールを受信し、A さんが温泉に行ったことを知った。」という記述がありますが、C さんは不正アクセス禁止法で禁止されている不正アクセス行為をしたという話のように聞こえます。このような扱いは、他人の ID とパスワードを用いてメールを受信する行為が犯罪でないかのように誤解を与えるものであると考えます。ID とパスワードを傍受したストーリーではなく、A さんが受信中のメールを C さんが傍受したストーリーに改めてはどうでしょうか。 また、「A さんは近所では誰にも話していない温泉の話を C さんが話題に出したので驚き、メールが覗かれていると思った。」というエピソードが用いられていますが、A さんの立場からすれば、C さんに「温泉行ったんでしょ？」と言われただけの段階では、他にも様々な可能性があるのであり、そこでメールの盗み読みをまず疑うのは不健全であると感じます。この文書を読んだ国民が、こういう状況でメールの盗み読みを疑うようになるというのは、よくないことだと考えますので、エピソードを抜本的に変更してはどうでしょうか。	御指摘を踏まえ、以下のとおり修正します。 Aさんの~~メール~~~~のIDとパスワードを知る~~を見る~~ことができた。Cさんは~~A~~さんの~~メール~~~~を受信し~~~~の内容から~~、先週Aさんが温泉に行ったことを知った。 なお、本項においては、無線LANの利用時に考え得る危険性について直截に伝えることを目的としているため、現行のストーリーとなっています。 よって、原案のとおりとさせていただきます。