別紙２

公衆無線 LAN セキュリティ分科会報告書（案）に対して提出された意見及び
その意見に対する公衆無線 LAN セキュリティ分科会の考え方
（意見募集期間：平成 30 年２月２日～平成 30 年２月 21 日）

提出意見：10 者
　法人：３者
　　（無線 LAN ビジネス推進連絡会、トレンドマイクロ株式会社、エヌ・ティ・ティ・ブロードバンドプラットフォーム株式会社）
　個人：７者
　　（個人 A～個人 G）

【総論】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見１　報告書案で示されている一連の方策は、現実を踏まえた検討が行われており、関係者が着実に対応することができるもの。	考え方１	
○　報告書案で示されている一連の方策は、現実を踏まえた検討が行われており、関係者が着実に対応することができるものであると考えられます。 　これら一連の方策の実施によって、公衆無線 LAN のセキュリティレベルの向上、公衆無線 LAN に関するリテラシーの向上等が図られ、公衆無線 LAN の一層の発展が期待できるものと考えます。 　公衆無線 LAN の発展は、当連絡会の目的とも整合するものであり、当連絡会としても報告書案の実行に向け、できるものから順次取り組むこととしたいと考えております。 【無線 LAN ビジネス推進連絡会】	報告書（案）に対する賛同の意見として承ります。	無

【第１章　公衆無線 LAN の現状】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見２　災害時の無線 LAN サービス「00000JAPAN」を初めて知った。「00000JAPAN」というサービスがあることについて、広く情報発信すべき。	考え方２	
○　私は色々な情報をインターネットで収集しているが、00000JAPAN という災害時の無線 LAN サービスは正直初めて知った。マスメディアでも見たことなければ雑誌でも見たことが無かった。恐らく都市部から離れれば離れるほど認識率は低いと考えられる。特に「のど元過ぎれば熱さを忘れる」ので災害時以外でも常日頃からテレビ CM、広告を発信、そして各通信キャリアを通じて広めていく事が肝要。 【個人 B】 ○　00000JAPAN の事は寡聞にして知りませんでした。 　公式発表や報道への要請などで繰り返し発進されるべき事項かと存じます。 　Wi-Fi の安全性確保は急がれるべきですが、あまり行政が躍起になってでしゃばる事例でも無い様に思えます。昨今行政の私物化が騒がれますが、気が付いたら安全強化が退職公務員の再就職受け入れにすり替わっていたり、安全のためと称して常時通信内容の監視がこっそり盛り込まれたりとならないようご注意願います。 【個人 E】	報告書（案）に示したとおり、「00000JAPAN」の認知に関するアンケート調査によれば、「知らなかった」との回答が 40.4%であり、今後、民間事業者等において「00000JAPAN」について認知度の向上が図られることが望まれます。	無
意見３　アクセスポイントとインターネット間（有線区間など）での盗聴及び改ざんについても、記していただきたい。	考え方３	
○　【P8】 　図について、○5 として、アクセスポイントとインターネット間での盗聴及び改竄について、特に記していただきたい。アクセスポイントとインターネット間のどこか（アクセスポイント-直近ルータ間、直近ルータ-ゲートウェイ用ルータ間等）で、UTP ケーブル接続かつ非暗号化通信が行われている場合は、容易に盗聴が行える事態が発生しうるので（無線 LAN 端末-アクセスポイント間は高強度暗号でもそこから先にパケット取得が容易に行える素の UTP ケーブル 1000Base-T 通信区間がある、などという事態はありうると思われる。(2 年程前からネット	報告書（案）では、専ら無線区間における脅威を例示しています。 　なお、公衆無線 LAN サービスの全体像を捉えた場合には、アクセスポイントの先のネットワークにも脅威が存在することから、さまざまな脅威が存在することを踏まえたセキュリティ対策を行うことが必要であると考え	無

ワーク機器はSFP端子等が一般化してきたのであるし、そもそも本来は国がメタルケーブルではなく光ケーブルへの移行を積極的に推進すべきなのであるが。))、店舗の無線LAN環境の有線部分構築事業者とネットワーク構築状況が不明な場合は有線部分を意識して注意するよう、記していただきたい。無線LANを使っている時でも、そのバックには（場合により非常に無防備な）有線LANが存在する事を意識するのは、重要であると考える。(P10等にも記載があるが、P8において「(詳細は1.3)」の様な案内を付して、公衆無線LAN末端利用者あるいは市井一般向けに注意喚起を行っていただきたい。) 【個人G】	ます。	

【第２章　公衆無線LANのセキュリティ対策のあり方】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見４　セキュリティの向上のためには、SSIDはAny（見える）から見えないにし、暗号化は現時点最高の方式(WPA2、今後登場するWPA3)を利用し、プライバシーセパレータはオンにし、利用者認証は偽装しにくいSMS連携とした方がよい。また、匿名性の高い公衆無線LANでは、利用者を追跡しつつ安全な環境提供が必要。さらに、IoTでは必ずデフォルトパスワードを利用しないこと。利用者側の意識向上として、公衆無線LANに最初接続した際には、Webのトップページにマニュアルダウンロードを表示させることも必要。	考え方４	
○　暗号化していない企業が多いのには驚愕した。プライバシーセパレータなどのネットワーク分離機能を利用しているので問題ないが、もしそこに脆弱性があった場合はパケットキャプチャーツールなどによって盗聴が可能となる。 空港は国の出入口であり、人も大量にいる。こんな場所でネットワークに関する攻撃があれば被害は甚大。監視カメラがあるとしてもトイレなどの個室からネットワークを利用されればますます犯人の特定は難しいのではないか。 SSIDはAny（見える）から見えないにし、暗号化は現時点最高の方式(WPA2、今後登場するWPA3)を利用、プライバシーセパレータはオン、利用者認証は偽装しにくいSMS連携とした方がセキュリティは向上する。 匿名性の高い公衆無線LANは提供するだけでなく、利用者を追跡しつつ安全な環境提供が必要である。前記は飽くまで無線LANの機器側だが、通信経路に対し「通信範囲の制限(Proxy)」、「水際の攻撃防御」、「経路追跡」が必要になる。利用者の利用範囲によってネットワークを制限する場合はProxyでWeb閲覧制限を行い、攻撃防御はIPS/IDS及びサンドボックス型のマルウェアチェックを行う。そして経路追跡は利用者認証に結びつけたログを取得する。 IoTを実施する際は必ずデフォルトパスワードを利用しない事。Mirai等のマルウェアのターゲットになるからである。 暗号化方式としてWPA2があり、これには脆弱性があるといわれている。今後WPA3を利用する事ができるものの、海外からの旅行者等の端末でこれが利用できるか、シェアを考える必要もある。	報告書（案）は、特定の暗号化方式、認証方式等を定めるものではなく、本分科会は、利便性と安全性のバランスに配慮しつつ、提供形態や利用シーンに応じて、提供者が多様な認証方式や暗号化方式による公衆無線LANサービスを提供するなど、利用者に与える選択肢を増やし、利用者がそれらのサービスを適切に選択することが可能な環境を整備することが必要であると考えます。 合わせて、利用者や提供者が、どのような利用シーンにおいてどのようなセキュリティ対策を講ずればよいか、適正な対策方法について、周知・啓発を図ることや、優良事例となるセキュアな公衆無線LAN環境の普及を図ることで、様々な利用シーンにおいて最適な選択が行われるよう支援して	無

利用者側に対する公衆無線 LAN の意識向上だが、これは公衆無線 LAN に最初接続した際に Web のトップページに（マニュアルダウンロードを）表示させるといった半ば強制的な事も必要だと考える。 【個人 B】	いくことが必要であると考えます。	
意見５　利便性と安全性のバランスに配慮しつつ検討が行われていることについては、公衆無線 LAN サービスの健全な普及・発展に向けて、大変意義のある取組。 公衆無線 LAN サービスが例えばインターネット上の掲示板への誹謗中傷の書き込み等に悪用されることを防止するために、認証に加え、利用ログの収集・保管も含めたトレーサビリティを確保し、市場全体として利用ログを収集・保管する取組を広げていくことが、公衆無線 LAN サービスの健全な普及・発展に向けて重要。	考え方５	
○　公衆無線 LAN セキュリティ分科会において、公衆無線 LAN サービスのセキュリティ対策のあり方とセキュリティに配慮した公衆無線 LAN サービスの普及策について、利便性と安全性のバランスに配慮しつつ検討が行われていることについては、公衆無線 LAN サービスの健全な普及・発展に向けて、大変意義のある取組みであると考えております。 分科会においては、公衆無線 LAN サービスのキュリティ対策のあり方として、認証方式のあり方、暗号化方式のあり方が検討課題として挙げられておりますが、弊社としては、公衆無線 LAN サービスが例えばインターネット上の掲示板への誹謗中傷の書き込み等に悪用されることを防止するために、認証に加え、利用ログの収集・保管も含めたトレーサビリティを確保していくことが重要と考えております。 したがって、利用ログの収集・保管を既に行っている電気通信事業者が提供するサービスであるか否かにかかわらず、市場全体として利用ログを収集・保管する取組みを広げていくことが、公衆無線 LAN サービスの健全な普及・発展に向けて重要であると考えております。 なお、弊社は、選択式のセキュリティ機能の提供についても積極的に取組み、利用者が利用目的等に応じて適切なサービスを選択できる環境の整備に努めていく考えです。 また、弊社は、「Japan Connected-free Wi-Fi」（Japan Wi-Fi）アプリを提供し、既に全国約 16 万アクセスポイントに「ワンタップ」「ワン認証（1 回のみの	報告書（案）では、利便性と安全性・プライバシーのバランスに配慮した検討を行うこととしており、報告書（案）に対する賛同の意見として承ります。 なお、民間事業者等による健全な利用を促進するような公衆無線 LAN サービスの工夫が期待されます。	無

利用登録）」で接続することができる環境を提供しておりますが、引き続き、公衆無線 LAN サービスの利便性向上、普及促進に応えていく考えです。 【エヌ・ティ・ティ・ブロードバンドプラットフォーム株式会社】		
意見６　安全性を確保する一つの手段として、政府、ISP や携帯電話事業者等がアクセス用 VPS（Virtual Private Server：仮想専用サーバ）を運用し、当該 VPS との VPN を無料で公衆無線 LAN 利用者に提供してはどうか。	考え方６	
○　【P15】 やや禁じ手的な趣きもあるのであるが、例えば、政府あるいは ISP や携帯電話キャリア等が、インターネット上で、アクセス用 VPS を運用して、当該 VPS との VPN を無料で公衆無線 LAN 利用者に提供するというのは、安全性を確保する一つの手段であると考える。この様にすれば、公衆無線 LAN 設置事業者が信用できなくても、ある程度の安全性を確保できるはずである。（なお、そもそも、携帯電話キャリアにおいては、一般的に、その様なものを契約者向けに無料で提供するべきであると考える。たとえばスマートフォンで無線 LAN あるいは携帯電話回線での通信を行う際に、VPN を用いれば、セキュリティ状況についてかなりの向上が行えるはずであり、そしてキャリアにはその様な事を行う能力や余裕があるのであるから、契約者の安全を考慮するのであれば、その様な事は相当程度に当然行うべきはずである。） 【個人 G】	報告書（案）は、特定の提供形態を定めるものではなく、本分科会は、提供者のビジネス環境等を配慮し、提供形態や目的に応じたセキュリティ対策のあり方について、検討結果をまとめています。 なお、民間事業者等によるセキュリティに配慮した公衆無線 LAN サービスの提供形態の工夫が期待されます。	無
意見７　公衆無線 LAN サービスの利用者がマルウェアに感染する等の被害を防ぐため、サービス提供者側でのセキュリティ対策も必要。	考え方７	
○　【報告書（案）16 ページ　(3) 公衆無線 LAN サービス全体像】 アクセスポイントの安全性確認や Wi-Fi 通信の暗号化等の対策のみならず、Wi-Fi 網を経由して危険な Web サイト等へアクセスすることで、Wi-Fi 利用者がマルウェアに感染するなどの被害を防ぐ為、サービス提供者側でのセキュリティ対策も必要。 【トレンドマイクロ株式会社】	公衆無線 LAN サービスには、様々な脅威が存在することから、報告書（案）に示したとおり、利用者や提供者がどのようなセキュリティ対策を講ずればよいか、適正な対策方法について、周知・啓発を図ることが必要であると考えます。	無
意見８　認証について信頼性は置けないが、認証はあるべき（EAP-SIM について、安全性が低くなる場合がある。）。接続アプリについて、単に接続を行うだけで VPN 機能を備えていないものやバックドアに情報提供するものがあるので、無条件に無線区間の暗号化も実現できるものではない。	考え方８	

○ 【P18】 認証については、結局、MAC アドレスから何から何まで偽造出来るわけであるので、そもそもそこまでの信頼性は置けないと考えるべきである。一般的な利用者についてはよいのであるが、不正な利用者への抵抗力はそこまで無い。勿論、認証によるトレーサビリティや不正利用防止措置、利用者記録等は行った方が望ましいが、攻撃の意図ある者にはあまり有効に機能しない場合がある事を前提とすべきであると考える。ただ、認証はあるべきであると考える。 ○ 【P19】 EAP-SIM 等についてであるが、SIM（中国製である事が多い）について携帯電話ショップ（なお、NTT ドコモを筆頭として、自社法人で運営されているショップは殆ど無い。酷い話、無責任な話であるが。）店頭奥等で組織的にコピーされていた場合（大量であったりもするであろう。直営以外で安全な SIM は無いのではないかと考える。）、安全性等は当然低くなると考える。 なお、接続アプリについては、単に接続を行うだけで VPN 機能を備えていなかったり、あるいはバックドアに情報提供したりするものがあるので、無条件に「無線区間の暗号化も実現できる」などという誤解を招く様な発言をするのは慎まれたい。あくまでそのアプリの実装する機能による事こそ周知させていくべきである。 【個人 G】	認証については、報告書（案）に示したとおり、脆弱な認証方式が採用されている場合、公衆無線 LAN サービスを踏み台にした攻撃やなりすましによる不正アクセス等の不正なサービス利用のおそれがあることに留意し、一律に、特定の認証方式を推奨するのではなく、提供形態や利用シーンに応じて、提供者は多様な認証方式による公衆無線 LAN サービスを提供するなど、利用者に与える選択肢を増やし、利用者がそれらのサービスを適切に選択することが可能な環境を整備することが必要であると考えます。 また、接続アプリについては、報告書（案）に示したとおり、その信頼性を担保する仕組みが必要であるとともに、利用者においては、接続アプリの機能を踏まえた利用が求められると考えます。	無
意見９　VPN について、端末からインターネットのクラウド上までの通信を暗号化するコンシューマ向けのサービスが存在することを明示すべき。	考え方９	
○ 【報告書（案）21 ページ （2）考え方 ③】 VPN について、一般に VPN というと拠点間であったり、端末から会社までの間の暗号化をイメージすると思われるため、端末からインターネットのクラウド上までの通信を暗号化するコンシューマ向けのサービスが存在する事を明示すべき。 【報告書（案）29 ページ 2 段落目 注 28 および 29】 主な有償の VPN サービスとして以下のものがある au の Wi-Fi セキュリティ、シマンテックのノートン Wifi プライバシー、トレンドマイクロのフリー Wi-Fi プロテクションなどが提供されている。 【トレンドマイクロ株式会社】	ご指摘を踏まえ、報告書（案）21 ページに、「VPN サービスの形態として、端末からインターネットのクラウド上までの通信を暗号化する利用者向けのサービスがある。」旨を明記いたします。 なお、有償の VPN サービスがあることについては、参考として承ります。	有

意見 10　VPN については、携帯電話キャリア及び無線 LAN 提供事業者が、ゲートウェイホスト周辺あるいはインターネット上にそのためのサーバを設置し、標準でその機能を提供すべき。 VPN については、別に、アプリに頼らずとも、スマートフォン等の場合は、ネットワーク設定で、L2TP/IPsec 等を指定することによって使えるはず。	考え方 10	
○ 【P20】 VPN については、携帯電話キャリア及び無線 LAN 提供事業者が、ゲートウェイホスト周辺あるいはインターネット上にそのためのサーバを設置し、標準でその機能を提供すべきであると考える。（有料事業者であれば、普通にそういうものを提供していていいはずであるが、していないのは、SI・NE 関係事業者の不善であると考える。数多くの有料サービスオプションがあったりするのであるから、VPN は標準または安価に、ごく当然のオプション又は無料初期オプションとして、提供されるべきであると考える。）なお、VPN については、別に、アプリに頼らずとも、スマートフォン等の場合は、ネットワーク設定で、L2TP/IPsec 等を指定する事によって使えるはずである事を指摘しておく。（なお、基本的に、不要なアプリケーションをインストールする事は危険である。） 【個人 G】	本報告書（案）は、特定の提供形態を定めるものではなく、本分科会は、提供者のビジネス環境等に配慮し、提供形態や目的に応じたセキュリティ対策のあり方について、検討結果をまとめています。 利用者が VPN サービスを利用する場合には、利便性と安全性のバランスに配慮しつつ、VPN アプリの利用やネットワーク設定が求められます。	無
意見 11　TLS については、現在の最新バージョンも示すべき。	考え方 11	
○ 【P21】 脚注 20 の TLS については、現在の最新バージョンも示すべきであると考える。SMBC の IB などは未だに TLSv1.0 を使っているのであるが、これだと GCM が使えない等の問題があるし、概ね暗号スイートも低劣な状態である。サーバ管理者向けに OpenSSL やその設定の更新等を促すためにも、バージョンについても記載されたい。 【個人 G】	ご指摘を踏まえ、報告書（案）21 ページに、「2018 年３月時点において、TLS1.2 が最新バージョンである。」旨を明記いたします。	有

【第３章　セキュリティに配慮した公衆無線 LAN サービスの普及策】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見 12　「公衆無線 LAN 版安全・安心マーク」制度について、利用企業が少ない。本当に安全で健全な無線 LAN を提供すべきであれば、国を挙げて基準を作り、資格として公開すべき。	考え方 12	
○　「公衆無線 LAN 版安全・安心マーク」制度についてだが、注釈を見る限りあまりにも利用企業が少なすぎる。本当に安全で健全な無線 LAN を提供すべきであれば国を挙げて基準を作り、資格として公開するべき。特にオリンピックの様なグローバルイベントがある場合はその地域は全て強制するとした方が無難。公衆無線を利用した攻撃（テロ）等があれば国の面子が立たなくなる。 【個人 B】	報告書（案）に示したとおり、公衆無線 LAN 版安全・安心マークの周知・普及を図ることが必要と考えます。 こうした民間の取組を通じて、健全な公衆無線 LAN サービスの普及が期待されます。	無
意見 13　利用者が暗号化あり／無しのサービスを選択可能な選択式のセキュリティ機能の提供は不要。	考え方 13	
○　選択式セキュリティは特に不要。何故自らセキュリティを外してまで無線 LAN を利用させるのか疑問。問題があれば提供者の責任と利用者は言いかねない。 セキュリティとかけ離れているが海外の端末に対する技適はどうするのか。問題のある端末を持ち込む可能性はないのか。 確かにセキュリティの向上は利便性とのトレードになるだけでなく、コストとのトレードともなります。ただ、安全で誰でも平和に利用していく公衆無線 LAN を実現していくためには必要な事だと存じております。 【個人 B】 ○　【「第３章 セキュリティに配慮した公衆無線 LAN サービスの普及策」「３．１ 公衆無線 LAN のセキュリティに対する利用者・提供者の意識向上」「（２） 民間主体によるセキュアな公衆無線 LAN の取組」「イ） 選択式のセキュリティ機能の提供」（24～25 頁）】 不適切な内容と考えます。 ここでいう、「無線区間の暗号化」は WPA2-PSK を想定されていて、無線通信の傍受を防いで利用者を保護する意図であると思料しますが、現実には保護されず、暗号化の設定による利便性低下を上回るメリットが見出せないためです。	暗号化については、ご指摘のとおり、PSK 方式においては、PSK の暗号化キーが公知である場合、通信が傍受されるおそれがあることから、提供者においては、PSK の暗号化キーの受渡しに留意する等の運用を行うことが求められます。 その上で、報告書（案）に示したとおり、提供形態や利用シーンに応じて、提供者は多様な暗号化方式による公衆無線 LAN サービスを提供するなど、利用者に与える選択肢を増やし、利用者がそれらのサービスを適切に選択することが可能な環境を整備すること等が必要であると考えます。 合わせて、利用者や提供者が、どのような利用シーンにおいてどのようなセキュリティ対策を講ずればよいか、適正な対策方法について、周知・啓発を図ることが求められます。	無

理由１）無線通信の傍受が容易に可能であり、利用者保護にならないこと。 これは、WEP に見られたような脆弱性によって解読が可能であるような話ではなく、そもそも暗号の原理からして傍受が防止できないからです。 元々、PSK 方式は、家庭や職場等、限られた利用者間で鍵を共有し、鍵を知らないと接続・傍受ができないようにするためのセキュリティです。 しかし、公衆無線 LAN サービスの場合は、PSK の暗号鍵が公知であることが多く、誰でも接続・傍受が可能です。 どんな優れた暗号方式であっても、復号する方式やそれに必要な鍵が知られていれば、全く用をなしません。方式については、標準化されていることから誰でも利用できるものですので、鍵が公知であると、もはや暗号とは言えません。 著名なネットワークアナライザーである Wireshark を利用すると、暗号鍵を入力するだけで WPA2-PSK で暗号化された無線 LAN も容易に内容を知ることが可能です。暗号化されていない無線 LAN と手間は何ら変わりません。 参考）セキュリティ大実験室 2017 パスワードが公開された公衆無線 LAN、暗号化されていても盗聴できる？ cf）http://itpro.nikkeibp.co.jp/atclact/active/17/100300158/100300008/ 理由２）利用者・設置者に誤った認識を与えて、かえってセキュリティリスクを増大させること。 このような内容の報告書が公になると、上記の理由により無線区間が保護されないにも関わらず、「無線区間を暗号化していれば安全安心である」と誤った認識が流布されかねません。 そもそも、インターネットそのものが秘匿性が全くない通信手段であり、無線 LAN を利用していなくても、通信経路のどこかで傍受される可能性が否定できないものです。暗号を利用する場合には、VPN や SSL/TLS など end-to-end で利用する必要があります。 もちろん、暗号方式の脆弱性や、偽サイト、偽証明書などのリスクはありますが、これは無線 LAN に限ったことではありません。 これらのセキュリティリスクは、報告書でも触れられているように周知啓蒙が必要である点は異論ありませんが、無線区間の暗号化によって誤った安心感を与えることはかえってセキュリティリスクの増大を招くと危惧します。		

理由３）設置者のコスト増大を招き、普及の足かせになること。 直接セキュリティの問題ではありませんが、公衆無線 LAN の普及の観点による理由です。 無線区間の暗号化設定を行うと、利用する場合に端末側の設定が必要となります。 このため、設置者のサポートのコスト上昇を招きます。同じサポートコストを負担するのであれば、end-to-end の暗号化や、WPA2-EAP の導入などより効果的な対策にコストを振り向けるべきです。 また、暗号化の有無で複数の SSID を使う場合、設置環境によってはアクセスポイントの増設など、物理的コストも上昇する恐れがあります。アクセスポイントは、設定できる SSID に上限があり、既に複数の SSID が設定されている場合、暗号化の有無で２倍の数の SSID が仕様上設定できないケースが想定されます。 これらにより、公衆無線 LAN サービスの普及にブレーキとなる懸念が生じます。 まとめ） 以上の理由により、「選択式のセキュリティ機能の提供」の部分は不適切であり、削除、あるいは代案の記載が必要であると考えます。 事実上意味がない対策（無線区間の PSK 暗号化）よりも、より効果のある対策（EAP 暗号化の導入、認証の強化、認証連携による利便性向上、等）に注力する方が、総合的なセキュリティ強化に繋がるものと思料します。 【個人 D】		
意見 14　データ利活用と連携したセキュアな公衆無線 LAN サービスの普及においては、利用者への接続・認証方法の事前周知を図ることが求められる。	考え方 14	
○　【３．２ データ利活用と連携したセキュアな公衆無線 LAN サービスの普及】 既存の（１）の次に、次の１節を追加することを提案する。 《案》 （２）利用者への接続・認証方法の事前周知 宿泊施設、観光施設、スタジアム、交通機関などあらかじめ利用者が計画して利用する施設については、予約時等に（１）のアプリの提供を含む接続・認証方法を案内することで、アプリのインストールや認証アカウントの取得など事前準備を促し、ユーザーの利便性の向上を図ることが考えられる。 《理由》 ２．１節（１）マル１でも指摘されているとおり、公衆無線 LAN のセキュリ	利用者への接続・認証方法の周知の方法については、ご提案いただいた方法やそれ以外の方法も含め、提供者において様々な工夫がなされることが期待されます。	無

ティ対策の検討においては、利便性と安全性のバランスに配慮することが重要である。安全性の確保のために認証やアプリの使用を求めるのであれば、それを事前に周知し準備を促すことで、現地に行って初めてそれに気付く場合に比べユーザーの障壁を下げ、利便性を向上することができる。 《参考事例》 ・JAL 国内線機内 Wi-Fi サービス（日本航空株式会社） https://www.jal.co.jp/dom/wifi_free/index.html 事前に接続方法を案内し、認証アカウントの取得やアプリのインストールも促している。 ・Taipei Free（台北市） https://www.tpe-free.tw/TPE/index_jp.aspx 日本をはじめ主な外国からの来訪者に対し、自国電話番号による SMS 連携方式の無料アカウントの取得を促している。 【個人 C】		
意見 15　さまざまなコンテンツサービスのアプリの機能と連携はやめて頂きたい。個人情報保護の観点からは、連携は望ましくない。	考え方 15	
○　【P26】 (1) さまざまなコンテンツサービスのアプリの機能と連携、などと恐ろしい事を言うのは止めていただきたい。個人情報コントロール権の侵害を推奨する様なものである。 (2) それは普通の認証ではないのか。なお、個人情報保護の観点からは、あまり連携は望ましくないと考える。 なお、認証について、なりすましについての記述をした同じ文書で、利用者の属性情報を認証に用いるとする事は、あまり賛成しない。 なお、チェックイン等については、旅館法等に則って手続きを行うべきである。身分証の提示（及び現在変更される可能性があるとなっているが、台帳への登録）無き場合は、旅館法等により宿泊不可としていただきたい。 【個人 G】	報告書（案）に示したとおり、地域活性化や利用者への新たな価値創造を加速し、セキュアな公衆無線 LAN サービスの普及を図る観点から、さまざまなコンテンツサービスのアプリの機能との連携は適当であり、その際には、プライバシーに配慮することが必要であると考えます。	無
意見 16　利用者側で公衆無線 LAN の接続先が安全なものであるかを確認することができるサービスについて例示されているが、必ずしも安全性を確認できているとは思えないものもあり、有効性を論じる必要がある。	考え方 16	

○　【P29】 　おそらくMACアドレス他traceroute結果等いくつかの情報で判断しているのだと思われるが、それらを全て偽れる事については意識していただきたい。国内基幹に近いネットワーク位置にあるサーバと事前調査のために施設等で用いる端末相互のやり取りがあれば、セーフ Wi-Fi による安全確認は容易に突破される事になるのではないかと察する（もし、各ルータやその配下の管理用端末等に機構を設けてドコモサーバとの暗号化通信による正当性確認を独自に行っているのであれば話は異なってくるが、それはなかなかにハードルが高いので、おそらくドコモはそのハードルを越えない方式を取っているかと思われる。あるいは、McAfreeの技術を用いているとの事であるので、それより更に簡単なMcAfee提供のブラックリスト方式での運用を行っているかもしれないと考える。）。 　また、FFRIのものは単に暗号プロトコルの確認をしているだけで、即Wi-Fiスポットの安全性の確認が出来ている事にはならないと思われる。 　「セーフWi-Fiアプリ」「Wi-Fi安全確認アプリ」の様なものについては技術的内容を把握して、その技術についての概要を示してから、その有効性について論じるようにしていただきたい。 　なお、SSIDを掲載する利便性についてはともかく、SSIDも偽れる事については国民に注意していただきたい。 【個人G】	利用者側で公衆無線LANの接続先が安全なものであるかを確認することができるサービスの一例を挙げたものです。	無

【その他】

意　見	考え方	提出意見を踏まえた案の修正の有無
意見17　一定程度の年数が経った時に、明らかなセキュリティホール等のあるスポットが多くなると思われる。	考え方17	
○　無線LANでは提供事業者にはセキュリティ面もだが、観光などやインフラで考えるなら一定以上の年数が経った時に明らかなセキュリティホールやまたは通信電波帯域を使うのに明らかに回線などが速度が遅い、接続不安定などと言うスポット、もしくはセキュリティでも接続問題があるスポットが多くなるというのは何とかしなければならないと思う 　こういうのがうまく提供できるようにすることはインバウンド政策やIoTやビッグデータ、マネーレス決済活用時代に非常に重要なインフラになると思う。また公衆無線スポットだけでなく充電や電源スポットなども公共施設などで整備、や広める必要があると思われます。（観光、防災、産業活用などいろんな面で有効） 【個人A】	自治体・民間事業者等が提供する公衆無線LANサービスについては、適切にセキュリティ対策を講ずる等、健全な公衆無線LANサービスの提供が望まれます。	無
意見18　PSKの暗号化キーを「パスワード」と呼称としている記述がある。「ログインパスワード」と混同しないよう記述を見直すべき。	考え方18	
○　PSKの暗号鍵を「パスワード」と呼称としている記述が一部にありますが、「ログインパスワード」と混同しない様記述を見直されることを希望します。 　NISC「情報セキュリティハンドブック」第2章に、「パスワード」と呼称されるものには3種類あり、「パスワードと呼ばれていることもあるけれど、本当はファイルや通信内容を暗号化するための暗号鍵として使われているもの（ZIPファイルのパスワード、WordやExcel、PowerPointの保護パスワード、Wi-Fi機器の暗号化キー、暗号キー、パスフレーズ、セキュリティキー、ネットワークキー）」という記述があります。 　資料11の7項PSKの脆弱性欄と対策欄にある「パスワード」はPSKの暗号鍵のことを指していると思われます。 　資料14のPSKの説明も「ID・パスワード」とは「SSID・暗号鍵」を指しているように見えます。	ご指摘を踏まえ、資料11の7項PSKの脆弱性欄と対策欄にある「パスワード」については、「パスフレーズ」と修正いたします。 　資料12及び資料14において、PSKの暗号化に関する箇所は「ID・パスワード」は「SSID・パスフレーズ」と修正いたします。 　なお、資料12の事例は、無線LANのネットワークセグメントから校務管理用のネットワークに侵入できたことが問題であったと考えます。	有

資料 12 の説明中の「ID・パスワード」は「ログインパスワード」のことを指していると思われますが、一方で校内アクセスポイントへの侵入について無線 LAN の設定等にも問題があったのかこの資料では判断しかねます。 また、P11「公衆無線 LAN 機器（ルータ等）の ID やパスワード」についても、文脈からルータ等機器の管理画面へのログインパスワードのことと判断できますが、可能であれば説明を補足されることを望みます。 【個人 F】	11 ページの「公衆無線 LAN 機器（ルータ等）の ID やパスワード」は、ルータ等機器の管理画面へのログインパスワードのことを指しており、アンケート調査の質問項目として記したものです。	
意見 19　各資料についての修正意見。	考え方 19	
【資料 1】 IEEE 規格名を示されたい。 【資料 10】 アクセスポイント-ゲートウェイルータ等の間の記述が抜けている。この間の暗号化が無かったり、UTP ケーブルだったり、あるいはハブが無防備に晒されていたり、などといった事がありうるので、その注意を行われたい。（なお、資料作成者は、故意にこの様な図を用い、日本人を嘲笑っている側の人間であると判断した。） 【資料 11】 ここで KRACKs についても記されたい。 【資料 20】 回線設備提供者の提供機器等には、IEEE802.1X 等の機能があるのであろうか。でなければ、アクセスポイントと回線設備提供者提供機器の間の通信は保護されていないものになると考える。この間で通信の漏洩や改竄がされる危険性がある事の注意喚起を行っていただきたい。 【資料 25】 上でも書いたが、VPN インターネットアクセスサービスについては、携帯電話キャリアや ISP、無線 LAN 事業者等が提供すべきものであると考える。VPN の利用は概ね望ましいものであるので、下部（※）で危険性をうたうよりも、それらの事業者への期待を表明すべきであると考える。 なお、無線 LAN 接続においても DNS の問題があるが、アクセスポイントが端末に伝える DNS についても問題が無いものとするよう、資料全体のうちどこかで記していただきたく思う。 【資料 30-32】 国民としては、IoT おもてなしクラウドと結びついたルーシー・ブラックマン	資料 1 は、公衆無線 LAN（Wi-Fi）の特徴を示しており、無線 LAN の規格の動向（IEEE802.11）や IEEE802.11ai の概要については、資料４及び資料５に記しています。 資料 10 は、考え方３のとおりです。 資料 11 は、公衆無線 LAN における主な攻撃の分類とその対策を示しており、WPA2 の脆弱性（KRACKs）については、資料 27 に記しています。 資料 20 は、公衆無線 LAN の提供形態の概念図を示したものであり、セキュリティ対策については、資料 14 及び資料 15 に一例を記しています。 資料 25 は、考え方 10 のとおりです。 資料 30～資料 32、資料 35 及び資料 36 に関するご意見は、本報告書（案）に直接関係ないものです。	無

さん事件の様な事態が発生する事を危惧するのであるが、同時に、奇妙な「おもてなし」を行おうとするよりも、素直なサービスの提供（当然、変なてらい無く適切なものである事が重要である。）を行った方が望ましいのではないかと考える。（どうせ、この様な「おもてなし」を提供しようとするのは低精神年齢の持ち主であり、あまり望ましいサービスを提供出来ないであろうという推測からもそう考える。（大体、「おもてなし」というのが使われ方として呪言（マントラ）地味ていて感心しない。夜郎自大でもある。）） 【資料 35】 既に行われる事になっているこの制度であるが、不法な者に金までやって国民個人情報・使用端末情報を収集させようとする凶事としか思えないので、すぐ止められたい。 誰が行わせようとしたのかはは不明であるが、愚かの一言である。 【資料 36】 デジタルサイネージには Sharp が押し込まれるという予測をしておく。経済産業省はその様な省庁となっているので。 【個人 G】		