○無線LANビジネスガイドライン（案）への御意見及びそれらに対する総務省の考え方

別添1

頁	項目	意見提出者	提出意見	総務省の考え方
3	1. はじめに			
		無線LANビジネス推進連絡会	無線LANビジネス推進連絡会といたしましては、当連絡会に期待された事項など、本ガイドラインの記載を真摯に受け止め、無線LANの健全な普及・発展に向けた一層の取組を図って参る所存です。	賛同の御意見として承ります。
5	2. 公衆無線LANサービス提供に当たっての法令上の留意事項			
5	2.1 事業開始等の際の法令上の手続			
		個人④	本項目は電気通信事業法についての解説がされているが、有線電気通信法についても解説をしていただきたい。 有線電気通信法では「無線通信用の有線連絡線」も「有線電気通信設備」に含め、その設置の届出を求めているが、AP や、APと上流回線との接続設備は「無線通信用の有線連絡線」に該当するようにも読める。 よって、この点につき、有線電気通信法の解釈適用についての解説をしていただきたい。	有線電気通信法（昭和28年法律第96号。以下「有電法」という。）上、有線電気通信設備を設置しようとする者は、原則として同法第3条第1項に基づく設備の設置等の届出を総務大臣に提出しなければなりません。しかし、一方で、同法第3条第4項により、当該設備が、電気通信事業法（昭和59年法律第86号。以下「事業法」という。）第44条第1項に規定する事業用電気通信設備に該当する場合や、その設備の一の部分の設置の場所が他の部分の設置の場所と同一の構内（これに準ずる区域内を含む）又は同一の建物内であるものについては、上記の届出は不要となっています。したがって、基本的には、公衆無線LANサービスを提供する事業者等において、上記の有電法上の届出の対応が実際に必要になるケースは想定されにくいと考えられます。 なお、個別の解釈や適用について御不明点がございましたら、最寄りの各総合通信局等にお問い合わせください。
5	2.1.1 総論			
		日本ユニシス株式会社	総合的な内容として、事業者と設備提供者が異なる場合の明記がなされておりませんでした。 ぜひ、明記していただきたい。	「2.1 事業開始等の際の法令上の手続」については、事業法上の登録・届出の要否が分かりにくいとの指摘があったことを踏まえて、今回ガイドラインに記載を設けたものです。御指摘のような事業者と設備設置者が異なる場合については、電気通信設備の調達方法如何にかかわらず、電気通信事業を営む事業者において登録・届出の要否を本件ガイドラインの記載を基に判断の上、適切な手続をとるようにしてください。
5	2.1.2 電気通信事業法に基づく登録又は届出が不要なもの			
		日本ユニシス株式会社	不要なものについての明記があることで明確な表現となっており賛同します。	賛同の御意見として承ります。
		日本ユニシス株式会社	記述が判りにくいので、特に段落「この場合、・・・」以下のくだりについて説明を追加していただきたい。また、当該ケースを図示していただくと、より判りやすくなると思われる。	2.1.2(3)の記載については、特定の事業者が独特の形態で提供しているサービスについて為念的に記載したものです。コミュニティメンバー自身は登録・届出不要であることは文末から明らかであり、原案のままとします。

10		2.2.3 端末設備等規則に関する留意事項			
			個人②	【案】上記2.1.4.1(2)に該当する場合、電気通信回線設備に無線LAN機器を接続するためには、端末機器の技術基準適合認定等を取得する（又は接続先の電気通信事業者の接続の検査を受ける）必要がある。また、2.1.3(1)及び2.1.4.1(1)において、無線LAN機器を電気通信事業の用に供する端末設備として用いる場合、当該機器は、端末設備等規則の該当条項を満たす必要がある。（事業用電気通信設備規則第37条） 【意見】 工事担任者や無線従事者が必要な場合とそれの参考として条文を載せていただきたい。（主に電気通信事業法第71条関係） ・端末設備の接続工事には、利用者が工事担任者に作業を任せる必要がある場合と、不要の場合の説明が必要と思われる。 ・モジュラージャック方式で容易に設置できる場合と自営端末設備に通信ケーブルを加工・工事するときの留意点の説明が必要。 無線従事者が必要な場合とそれの参考として条文を載せていただきたい。 ・屋外用の便利な一部の機器（例：IEEE802．11j）に申請・登録が必要なAPがある。 ・電気通信事業者においては無線通信で無線従事者が必要な領域があることの説明が必要と思われる。	御指摘のとおり、IEEE802.11j等の登録局を開設し運用する場合には、免許を要する無線局と同様に、無線従事者資格が必要となります。 IEEE802.11jについては、公衆無線LANという観点ではエンドユーザが直接使うことは想定されませんが、公衆無線LANをメッシュ的に構築する際の中継回線として使われることもあるので、脚注に上記趣旨を追記することとします。なお、技術基準や工事資格等に関する条文は多岐にわたるため、これを掲載した場合、逆に煩雑になることが予想されるため、原則掲載しないこととします。 【追記する脚注】 電波法上の技術基準適合証明を有するなどの条件を満たした無線LANの運用に関しては、一般に無線従事者資格は不要であるが、登録局の5GHz帯無線アクセスシステム(IEEE802.11j)を開設し運用する場合は、無線従事者資格が必要となる。
10		2.3.1 個人情報の保護に関する事項			
			日本ユニシス株式会社	2.3.1ではプライバシーポリシーをあらかじめ定めて公表することが求められているが、ポリシー策定においてプライバシー情報の定義が必要なので、この定義を追記いただきたい。 また、プライバシーポリシー策定において、個人識別性のないプライバシー情報をも対象とするべきか否かを明確にしていただきたい。	「プライバシー情報」については、形式的に個人識別性を有しない情報であっても、プライバシー保護の観点から実質的に個人識別性を有する場合は、保護の対象とすべきと考えますが（※）、その該当性については、個別の事情に基づき判断する必要があると考えます。 ※「パーソナルデータの利用・流通に関する研究会」報告書（平成25年6月12日総務省公表）第3章第1節「2．保護されるパーソナルデータの範囲」を参照ください。
11		2.3.2 通信の秘密の保護に関する事項			
			個人④	電気通信事業者以外の者が提供する公衆無線 LAN サービスの通信の秘密の保護についても解説をしていただきたい。 本項目は、冒頭で「公衆無線 LANサービスを提供する電気通信事業者は」とあるように、電気通信事業者が自らが提供する電気通信役務の秘密を侵すことについて解説されている。 しかし、項目 2.1.2 にもあるように、電気通信事業者とはならない公衆無線 LANサービス提供者も存在しうるところ、当該提供者が自らが提供する電気通信役務の秘密を侵すことも考えられる。 実際に、電気通信事業者ではないとされる公衆無線 LANサービス提供者に対して、総務省が指導をした事例もある（http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000071.html、平成24年4月4日）。 電気通信事業法各条では「電気通信事業者の取扱中に係る通信」について規定しているが、電気通信事業者以外の者が提供する電気通信役務に対しての当該各条の適用関係は判然としない。 よって、電気通信事業者以外の者が提供する公衆無線 LAN サービスの通信の秘密の保護についての解説をしていただきたい。	平成24年4月4日の指導の対象となった者は、電気通信事業者となるべき者であったため、事業法に基づく指導を行ったところです。 なお、事業法における通信の秘密の保護については、電気通信事業者の取扱中に係る通信以外に、事業法第164条第1項各号に該当する電気通信事業を営む者の取扱中に係る通信も対象となり（事業法第164条第2項）、何人であっても通信の秘密を侵した場合は事業法第179条の罰則の対象となります。 また、電気通信事業者以外の者が提供する公衆無線 LAN サービスについては、有線電気通信部分における通信の秘密は、有電法第9条、第14条により、無線通信部分における通信の秘密は、電波法（昭和25年法律第131号）第59条、第109条及び第109条の2により保護されることとなります。 同趣旨を脚注として追記するとともに、参照条文を追加します。

			個人④	ウェブ認証の正当業務行為性についての解説をしていただきたい。 公衆無線 LAN サービスは、利用開始時に利用者の確認としてウェブ認証を行うことが多いと思われる。 通常のネットワーク回線であれば、回線接続時に認証を行い、回線接続が確立した後に個々の通信が行われる。 一方ウェブ認証では、何らの認証なく回線接続を確立させ、その後に個々の通信が発生した段階で、当該通信の内容を改変し、本来の通信の応答の代わりに利用者確認を求めるページを利用者端末に送信することで認証を行うものである。 項目 3.1 の「利用の際の画面表示」はこれを指していると思われる。 個々の通信に対して操作を行う手法であるため、形式的には通信の秘密の侵害に該当するところ、電気通信役務の提供に必要な範囲で行われる限りにおいては、正当業務行為として違法性が阻却されるものと推察する。 しかし、どの範囲であれば許容されるのかは明らかでない。 認証と同時に広告宣伝等を行う場合や、認証に要するページのほか、ポータルサイトの閲覧等の所定のアクセスについては認証前でも通信を許可する場合など、応用的な利用方法も考えられる。 また、個々の通信には、その相手先に係る認証情報等の特に機密性の高い情報が含まれていることもありえるところ、ウェブ認証に伴って通信内容を改変する際に、当該通信内容に元々属する情報がウェブ認証のログとして取り扱われることがないよう、技術的基準が必要になると考える。 よって、これらの点につき、ウェブ認証の正当業務行為性についての解説をしていただきたい。	項目 3.1 の「利用の際の画面表示」はこれを指していると思われるとの御指摘ですが、この記載は、利用中に公衆無線LANのサービス品質（速度、情報セキュリティ等）が広く画面で確認できることを念頭に置いており、特にウェブ認証を意識したものではありません。 なお、一般的にウェブ認証自体は、通信の秘密の保護との関係上問題となることはないと考えます。
			日本ユニシス株式会社	P11の図（個人情報と通信の秘密との関係）では、プライバシー情報との関係性についてなんら表示されていない。 プライバシーポリシー策定の参考とするため、プライバシー情報の範囲（個人識別性がある場合とない場合の双方について）を当該図に明示いただきたい。	「プライバシー情報」については、形式的に個人識別性を有しない情報であっても、プライバシー保護の観点から実質的に個人識別性を有する場合は、保護の対象とすべきと考えますが（※）、その該当性については、個別の事情に基づき判断する必要があると考えます。 ※「パーソナルデータの利用・流通に関する研究会」報告書（平成25年6月12日総務省公表）第3章第1節「2．保護されるパーソナルデータの範囲」を参照ください。

14	3. 利用者との関係における留意事項				
17		3.3 オフロードの取組を進める携帯電話事業者の留意事項			
			個人①	現状公衆無線LANの局数増加はLTEネットワークからのデータオフロードにあると理解しているが、残念なことに携帯通信事業者の特定のサービス(いわゆるスマートホン)の契約が必須であり、それ以外の端末との接続は禁止しているところがほとんどである。 ISMバンドでありながらキャリアによる囲い込み、キャリア同士による設置合戦のために「バンドが汚れ」PC・およびTablet端末が安価に公衆バンドの恩恵を受けられない事態が起こっている。 無線LANはキャリアのトラヒックオフロードのためだけに存在しているのではない。 恢聞するところによると他キャリア、バンドの利用状況について碌な調整も調査も行われず、10メートルおきに設備を打ち、設備からの通信をHSPAやWiMaxで収容するという本末転倒な事例が数多くある。 電波法の精神にあるとおり「電波は国民の有する有限の財産」なのであるから、このような行為は即刻禁止されるべきであり、ISMバンドをあたかも自らに無償で割り振られたような海賊的活動は法令などで厳しく制限をかけられるべきである。 (電波法4条局に対しても82条の弾力的かつ厳格な運用が必要である) 少なくとも、自社スマートホンだけではなく、PCやWWANのないタブレット型機器に対しても、安価な接続契約・ローミングを義務付けるべきである。 また、KDDI・ソフトバンクモバイルが個人・法人事業者店舗に対し、自社の固有製品サービスのみサポートという重大な制約事項を説明せず、結果として個人事業者が期待するサービスと実情との乖離がおきている。 このままでは新産業が既存の通信事業者によるLTEオフロードのみに擂り潰され、幅広くビジネス化されることが困難になる他、近隣の構内利用者・個人、および同帯域を利用するBluetoothのようなサービスのレベル低下を招くこととなる。 (特に無線LANを利用したPOSといった自営端末通信・デジタルサイネージについては実害が生じている) 電気通信事業者による設置に対しては、他事業者や構内利用者・個人に対しエリア設計を義務付けるとともに、特定端末以外の排除の禁止・輻輳発生時における自動的な出力やチャネルバルキングの縮退、ローミングの義務付けや無線LANのみの契約が可能になるよう法レベルで定めるべきであるとともに、例えば2.4GHz帯においては同時に3チャネルしか使えないことを一般の事業者や個人に啓発すべきであると考える。 無線LAN単体でも事業を行っている事業者に対し、携帯通信事業者の上記のような自社特定端末以外を締め出す行為は不正競争であるといわざるをえない。 このような現状をガイドラインにしっかりと記載し、国家として明確な「配慮」をもとめ、指導していくべきであると考える。	御指摘のような点も踏まえて、今回ガイドラインに「3.3 オフロードの取組を進める携帯電話事業者の留意事項」の記載を設けたり、「4.1 5GHz帯の利用促進」の記載を行っているところです。 個々の論点については、今後の行政運営上の参考とします。

17	4. 利用しやすい無線LANとするための留意事項				
18		4.1.1 アクセスポイント側の対応			
			日本ユニシス株式会社	5GHz帯の場合は、DFS/TPC機能による電波影響もございますので、周知していただきたい。	御指摘のとおり、5.3GHz帯及び5.6GHz帯の無線LANについては、国際的な基準によりDFS/TPC機能を具備することが求められており、適正な無線LAN機器を使用している場合は、気象レーダー等の電波を感知したときに、設置者の意図には関係なく自動的に機能します。 DFS/TPC機能を具備する5GHz帯の無線LANの特性については、本ガイドライン4.1に以下の脚注を追記します。 【追記する脚注】 5.3GHz帯及び5.6GHz帯の無線LANについては、国際的な基準により DFS/TPC機能を具備することが求められている。このため、同周波数帯において無線LANを運用した場合、気象レーダー等の電波を感知したときは、設置者の意図に関係なく自動的にチャネル変更等が行われることがある。 DFS（Dynamic Frequency Selection）：無線LANがレーダーと周波数を共用して使用するための機能 TPC（Transmitter Power Control）：無線LANの一の通信系における平均の空中線電力を3dB下げる機能
			日本ユニシス株式会社	『また、APは、IEEE802.11グループにおいて検討されている次世代無線LAN規格が実用化された場合に、ソフトウェアの更新やモジュールの追加等により、AP自体を交換することなく対応できるものであると望ましいと考えられる。』との記載がありますが、無線LANベンダーが限られる記載に受け取ることができますので、削除していただきたい。	一般的にAPの物理的更改よりソフトウェアの更新等によって対応が可能である方がコストも低廉となり、設備更改も迅速に行われることが期待されるため、無線LANの発達の観点から望ましいと考えた記載ですが、御指摘等も踏まえ、当該部分は削除することとします。

18		4.2 アクセスポイントの設置等			
			日本ユニシス株式会社	昨今、パブリックスペースでのアクセスポイントが乱立しているため、隣接する一般企業内やテナント等に電波の輻輳など影響が出ております。そのため、パブリックスペース等における共用型アクセスポイントの普及を強く推進していただきたい。	御指摘のような状況を踏まえ、本ガイドラインにも共用型アクセスポイントの活用推進が望まれる旨を記載しているところです。
19	5. 大規模災害発生時に備えた留意事項				
			日本ユニシス株式会社	事前に検討・準備すべき事項としては、大規模災害のみならず、テロ対応についても同様なので、テロ発生時に備えた推奨される対応としての留意事項を追記していただきたい。	大規模災害発生時における公衆無線LANの活用については、一定の効果が確認されているため、本ガイドラインに記載を設けたものです。 一方、テロリズムについては、大規模災害と比べて被害地域が限定される場合が多いと考えられることや、公衆無線LANの無料開放等が有効であるか現時点では不明であることから、特段の記載を設けておりません。 ただし、大規模災害発生時に関する本ガイドラインの記述と同様に、各事業者等の自主的な判断により、テロリズム発生時に個別の取組を行うことが考えられます。
21	6. 地域活性化、ビジネス活性化に向けた無線LAN活用における留意事項				
21	7. アクセスポイントの設置場所となる店舗等オーナーの留意事項				
22	別添1 公衆無線LANサービスの提供における個人情報の保護及び通信の秘密の保護について				
			日本ユニシス株式会社	(2)の1行目に、「個人識別性を有する場合には、個人情報の取得に該当することから、個人情報保護法及び個人情報保護ガイドラインに基づく適切な取扱いが求められる。」旨が記述されている。 プライバシー情報についても個人識別性を有する場合には、個人情報保護法で対応できるが、個人識別性をもたないプライバシー情報についての対応方法は不明確なので、どのような取扱いをすればよいのかを追記していただきたい。	「プライバシー情報」については、形式的に個人識別性を有しない情報であっても、プライバシー保護の観点から実質的に個人識別性を有する場合は、保護の対象とすべきと考えますが(※)、その該当性については、個別の事情に基づき判断する必要があると考えます。 ※「パーソナルデータの利用・流通に関する研究会」報告書(平成25年6月12日総務省公表)第3章第1節「2. 保護されるパーソナルデータの範囲」を参照ください。
			日本ユニシス株式会社	【意見】 アクセスポイントの盗難防止に関する記載がありませんので下記のように追記していただきたい。 【案】 アクセスポイントは、盗難防止チェーンでロックするか、盗難防止ケースに入れるなどの対策をすることが望ましい。また、万が一盗難されても設定情報が見えない、などの配慮を実施することが必要である。	アクセスポイントの盗難防止措置は、ガイドラインに記載するまでもなく、各事業者等が注意して行うものと考えられることから、参考意見として承ります。
			日本ユニシス株式会社	事業者と設備提供者が異なる場合、事業者側の意図しない、帯域制御が設備提供者より与えられている場合などはどのように解釈をしたらよいのか記載していただきたい。	帯域制御に関する各論については、本ガイドラインでも紹介している「帯域制御の運用基準に関するガイドライン」を適宜参照ください。

26	別添2 無線LANアクセスポイントを置く店舗等のオーナーに知っておいていただきたいこと				
			個人②	【意見】 次の内容の追記を検討いただきたい。 利用者の情報リテラシーの参考になるような資格の掲載 例として工事担任者資格や無線従事者資格などがスキル標準の参考になる。有資格者管理により公衆無線LANの端末利用者の安心・安全が保つ活動ができる。（他にはネットワークスペシャリスト、情報セキュリティなど）。利用者または利用者が委託した設置業者が有資格者監督の施行による通信事故などの予防・防止。 ・将来的には「利用者が企業」「開放型店舗」の経営者が定める管理者要件の参考とする。	参考意見として承ります。
			個人⑤	現在、公衆無線LANサービスの認証方法（本人確認方法）については、 事業者等により、セキュリティのレベルの高いものから、低いものまで、 各種の方法が採用されている状態です。 （中には認証していないところもあります） そのため、事業者等に理解をしていただくため、認証方法（本人確認方法）に関する具体的なガイドラインとして、 ・各種認証方法の整理 ・推奨する認証方法（最低限すべき対策、理想的な対策） を「別添2 無線LANアクセスポイントを置く店舗等のオーナーに知っておいていただきたいこと」内の「3.(2) 情報セキュリティ対策の実施」 に、1項目として追加し、明記してはいかがでしょうか。	御意見いただいたような問題意識を踏まえて、「別添2 無線LANアクセスポイントを置く店舗等のオーナーに知っておいていただきたいこと」中、「3. 安心・安全な利用を確保するための情報セキュリティ対策について」のなお書きにおいて、当省が策定・公表している「一般利用者が安心して無線LANを利用するために」を適宜参照頂きたい旨を呼びかけているものです。本記載がより参照しやすくなるように、リンクを追加することとします。

その他意見					
			個人①	・電波法59条の原則(傍受窃用の禁止)を原則に、電気通信事業法との関連を1節に分けて解説・記述すべきである。特に傍受窃用の禁止ははっきりと明記すべきです。 ・特に設置者がISMバンドのことを理解していないと思われます。802.11の他にもBluetooth・WirelessUSB・気象レーダーなどISMバンド利用の他サービスが存在することを周知し、配慮するべきであるということを明記すべきである。 ・草創期の街頭無線LANの中には出力を可変させずに最大で利用し、個人や構内利用の法人に多大な迷惑をかけている例がある。無線カバレッジを上げるには出力を限界まで上げるのが最適だが、さまざまな事業者が参入している以上、動的なチャネル・出力の制御は必須である。 ・旧規格の.b.gは基地局から見えないため、CSMA/CDすら働かず、公衆無線LANによって迷惑を蒙っている。特にコンピュータ制御の寿命が長い産業機械は未だに.bを使っていることが多い。 ・電波法59条の(傍受窃用の禁止)は電気通信事業法よりも範囲が広いと認識しているので、電波法の精神を原則としつつ事業法との関係を1節を分けて解説すべきである。(Macヘッダのみならず、ビーコンなども対象に含まれうる。)明確化すべき。 ・.jを通信事業者に勧めるとともに、.jを次世代に拡張することを提案すべき。 ・稠密地では2.4G帯の一部チャネル利用を遠慮させるべきだと思います。POSなどレイテンシが厳しい使い方をしているところはかなり存在します。 ・公衆無線LANにおけるチャネルボンディングは他事業者やそれ以外の個人に迷惑をかける可能性があるので、LTEオフロードを兼ねた有償サービスについてはチャネルボンディング数を制限すべきです。1Gbpsは明らかに不要でしょう。 ・とにかく自営無線LAN・他の通信方式に影響を極力与えないよう、ISMバンドの清浄性を保つために最大の努力を払うべきである。今後登場する可能性のあるISMバンド利用のサービスを阻害してはならないと思います。	全体的に賛同の意見として承ります。 なお、事業法における通信の秘密の保護については、電気通信事業者の取扱中に係る通信以外に、事業法第164条第1項各号に該当する電気通信事業を営む者の取扱中に係る通信も対象となり(事業法第164条第2項)、何人であっても通信の秘密を侵した場合は事業法第179条の罰則の対象となります。また、電気通信事業者以外の者が提供する公衆無線 LAN サービスについては、有線電気通信部分における通信の秘密は、有電法第9条、第14条により、無線通信部分における通信の秘密は、電波法第59条、109条及び第109条の2により保護されることとなります。 同趣旨を「2.3.2 通信の秘密の保護に関する事項」の脚注として追記するとともに、参照条文を追加します。 電波の輻輳等への配慮については、APの設置については、本ガイドライン4.2においても記述しているところです。
			個人③	「無線LANビジネスガイドライン」などというタイトルだが、こんなビジネスは存在しないのではないか？と考える。アクセスポイントから末端までしか対象にしないのだから、ネットワークビジネスとして完成出来ない、つまり顧客とのネットワーク契約が結べないことを意味する。そもそも無線LANとは、LANケーブルの無線化であり、基本は、local Aria Networkという狭域である。つまり、個人や学校、会社など、身元が安全なメンバーだけのネットワークとして、ファイアウオールの中での世界としているのが、LANである。それを一般に開放するということは、LANでは無くなる。大事なものは、アクセスポイントとなるルーターである。これを野放しにして設置してしまうと、大変なことになるかも知れない。少なくても、情報通信技術の知識を持った人に設置工事を義務付けしなければセキュリティー性は保てないはずである。行政手続で届出をさせても立会い確認は不可能なのだから、事件が起きる前に、きちんと技術基準を定義し規制すべきと提言する。	無線LANアクセスポイント等を設置して公衆向けに電気通信事業を営む業態が存在するため、今回ガイドラインを策定したものです。その現状については、無線LANビジネス研究会報告書「第1章 無線LANの現状、3無線LANサービスの分類」をご参照ください。 なお、セキュリティについては、「3.2.1 適切な情報セキュリティ対策」において記載しております。