別紙２

「企業等が安心して無線ＬＡＮを導入・運用するために」（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 25 年 1 月 30 日

「企業等が安心して無線ＬＡＮを導入・運用するために」（案）の
意見募集に対する御意見

○　意見募集期間：

平成24年12月14日（金）～平成25年１月４日（金）

○　意見提出総数

（１）　個人３件

（２）　法人・団体１件

◇ 北陸無線データ通信協議会

	御意見の概要	御意見に対する考え方
個人①	無線端末が固定IPでの運用であれば問題ないが、DHCPの場合、DHCPサーバへのアクセス時に攻撃を受けIPアドレスをハッキングされる恐れがあるため、DHCPでの運用は不可とする旨記載した方がよいと思う。	WPA又はWPA2を適切に設定することにより、DHCPサーバとのやりとりは暗号化されるため、DHCPの利用は問題ありません。 よって、原案のとおりとします。
	携帯電話にSIMカードの情報が残存することからSIMカードを利用する認証方式は推奨できないと考える。	端末にSIMの情報が残存することはないため、御指摘は当たらないと考えます。 よって、原案のとおりとします。
	RADIUSを採用している場合は、RADIUSサーバに対しパケット洪水攻撃等、トラフィックに影響を与える攻撃を避ける仕掛けや運用が必要と考える。	トラヒック等に影響を与えることにより通信を妨害する攻撃については、既に「無線IDS／IPS等の導入」等の対策を記載しています。 よって、原案のとおりとします。
	アクセスポイントについては電源確保時にノイズが混じると正常に機能しない恐れがあるため、アースの取り付けは必須と考える。	御指摘の点は電気製品の使用に当たって重要なことですが、本手引書が対象とする無線LANの情報セキュリティ対策ではありません。 よって、原案のとおりとします。
	最も怖いのはアクセスポイントを利用する端末そのものが攻撃を受けることなので、クラウドなどの利用で端末に情報を一切残さない運用や、アクセスポイントへの接続時には端末情報を初期化してしまう機能の搭載が望まれる。	情報セキュリティ対策の一つとして、クラウド等を利用することが有効な場合がありますが、その利用については個々の企業等の組織がセキュリティポリシーを踏まえて判断する事項です。 よって、原案のとおりとします。
個人②	ISO/IEC27001(JIS Q 27001)においては、すでに「情報資産」という用語は使われておらず、「資産」で統一されていたかと思う。 「無線LAN」ということから、物理資産やサーピスなどの資産に対する脅威や脆弱性ではない、という理由からだとは思うが、あえて「情報資産」と限定して対象を狭くしなくても良いと考える。	御指摘のとおり、「情報資産」を「資産」に変更します。
個人③	商業ビルなどでフリーのSSIDがずらずらと読み込まれるという状態だと、他の一般客のhotスポットなどの利用に不都合が生じるので、外部の人間（たとえば来訪者）のために無線LANのフリーSSIDを作るのはやめてほしい。	本手引書は、p1及び2に示すとおり、組織の構成員のみが利用する形態の無線LANを対象としています。 よって、原案のとおりとします。
	干渉でつながらなくなるため、アクセスポイントの電波の出力も極力絞って運用してほしい。	電波の伝搬範囲の設定については、既にp9等に記載しています。 よって、原案のとおりとします。
北陸無線データ通信協議会	1．電波を利用するという観点及び丁寧な説明が無い 日本国内での無線LAN機器の設置・運用に於いては技術基準適合認証を受けた無線LAN機器を使用しなければならない。技適認証の無い機器を運用した場合は電波法4・110条違反として刑事罰として罪に問う可能性がある事を国として警告すべきである。	本手引書は、無線LANの情報セキュリティ対策を対象としており、電波を利用すること及び電波法令を遵守していることを前提としています。 よって、原案のとおりとします。
	2．IEEE802.11-2012に定義されたセキュリティ機能に関する記述が不足 IEEEE802.11-2012で追加されたBIP(Broadcast/Multicast Integrity Protocol)の記述がない。少なくとも802.11-2012を踏まえ分り易く説明文を入れる必要がある。	BIP(Broadcast / Multicast Integrity Protocol)は、IEEE802.11wに含まれる機能であり、その内容については既にp8に記載しています。 よって、原案のとおりとします。
	3．802.11フレームが抱える大きな欠陥とも言える部分について示していない MACヘッダーにはSource、Destination, APとSSID用の4つのMACがフレームに含まれるがこの多数の無線LAN機器の特定、データの流通経路を割り出すことができ、Broadcastが流れた場合同一セグメントに存在する機器のMAC情報は第三者に簡単に知れ渡るという事を意味する。第三者にネットワークの構成が機種も含めて簡単に分ってしまうという事を意味する。	IEEE802.11のフレームから特定可能な情報は、ネットワークの末端にある機器の一部の情報のみであり、御指摘は当たらないと考えます。 また、やりとりされるデータは暗号化、接続は認証で保護されることから、情報セキュリティ上の脅威には当たらないと考えます。 よって、原案のとおりとします。
	4．ビーコンフレーム・SSID（Service Set ID）について明瞭ではない BSSID、SSIDの情報は通信の秘密で保護されるものであり、SSIDの取扱いについて個人情報の類をSSIDに使わないようにすべきだと言うべきところが成されていない。	個人情報等が類推可能なSSIDを設定することはプライバシー保護の観点から避けるべきと考えますが、本手引書が対象とする無線LANの情報セキュリティ対策ではありません。 よって、原案のとおりとします。
	5．外部委託する場合の注意事項、免責について 無線LANビジネス推進者には積極的にこの様なただ乗りができる無線LANを除去して頂く様お願いし、総務省には不正利用の無い安全で混信妨害の無い無線LAN利用環境を構築する為に法の整備及び教育・安全対策の為に税金を投入して頂くしかない。当然無線LANビジネス推進者には負の遺産である危険な古い無線LAN機器を無料回収・交換して頂くしかない。	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しません。
	6．今後多発する事が間違いない無線LAN傍受データの大量収集による被害を注意喚起するに不十分である。 無線LANを使用した電波の傍受により簡単に該当のネットワーク機器の存在や機種が特定できその無線データを大量に蓄積できるという無線ならではの特徴を真っ先に挙げて注意を喚起するべきである。つまり、悪意の第三者からの攻撃に弱いネットワークを推進する理由は無いと言い切って良い。	暗号化等の適切な情報セキュリティ対策が取られている場合、無線LAN傍受データの大量収集は現実的なリスクとはなりません。 よって、原案のとおりとします。
	○「窃取」という言葉は軽すぎる 「第三者による傍受及び通信データの大量記録」に置き換え無線・電波を利用の大きな欠点を強調すべきである。	データを「ひそかにぬすみ取ること」は「窃取」と表現することが適当と考えます（広辞苑第六版）。 よって、原案のとおりとします。
	○無線LANへの侵入 これは「無線LAN機器への侵入」です。	御指摘を踏まえ、「無線LANへの侵入」については、「無線LANを経由した内部ネットワークへの侵入」に修正します。

	□P.2 ARIB T66/71の記述を入れる事。	本手引書は、無線LANの情報セキュリティ対策を対象としており、電波法令について言及するものではありません。 よって、原案のとおりとします。
	□P.2 周波数・電波形式を定義しているIEEE802.1acを追加する事が必要	IEEE802.11acは、平成25年1月時点で規格として正式に発効されていないため、記載していません。 よって、原案のとおりとします。
	□P.2 屋外利用できない周波数を明記すべき 例 5.2～5.3GHz帯もしくはチャンネルNo. 36,40,44,48、52,56,60,64ch	本手引書は、無線LANの情報セキュリティ対策を対象としており、電波法令について言及するものではありません。 よって、原案のとおりとします。
	□P.2 表1の最大通信速度は不適当。理論上の最大通信速度に修正を強く要求する。	「最大通信速度」には、理論値であることが含意されています。 よって、原案のとおりとします。
	□P.3 ジャミング（妨害）電波の発信による通信妨害が抜けている 実際に違法機であるが妨害電波発生装置は市場で市販されている。	p3等に該当する記述が既にございます。 よって、原案のとおりとします。
	□P.3 ①無線線LAN区間における通信内容の傍受と大量蓄積、及び通信データ改ざん等のMITM（中間者攻撃（Man in the Middle)をうけるおそれがある。 に変更を求める。	データを「ひそかにぬすみ取ること」は「窃取」と表現することが適当と考えます（広辞苑第六版）。また、無線LAN区間における通信内容の窃取及び改ざんは、中間者攻撃に限定されるものではありません。 よって、原案のとおりとします。
	□P.3 ④悪意のある第三者により不正なアクセスポイントが設置され、当該アクセスポイントを正規のアクセスポイントと誤認させられた利用者の端末が接続することで、通信内容が大量に蓄積されるおそれがある。 に変更を求める。	データを「ひそかにぬすみ取ること」は「窃取」と表現することが適当と考えます（広辞苑第六版）。 よって、原案のとおりとします。
	□P.3 ⑤通信の妨害 悪意のある第三者によって、大量のパケット等が送信されることによるDoS（Denial of Service）攻撃、例えば制御信号を詐称して切断コマンドを送るMITM(Man In The Middle)攻撃,不正もしくは違法な電波発生源が設置されることによる電波干渉等により、通信速度が低下し又は通信が不可能となるおそれがある。 に変更を求める	中間者攻撃は、正当な二者間の通信に介入する攻撃の呼称であることから、改ざんした管理フレームを繰返し送信する攻撃はDoS攻撃と分類することが適当と考えます。 よって、原案のとおりとします。
	□P. 4 通信の妨害の項目に △ 設置時に電界強度マップを作成し混信妨害が発生した場合のトラブルシューティング時のリファレンスとする を追加して頂きたい。	御指摘の内容については、「電波状況の監視」及び「無線IDS／IPS」に含まれています。 よって、原案のとおりとします。
	□P.5 2.1 （1）に WEPの使用しない事を強く推奨する。 を追加して頂きたい。	御指摘の内容については、p5及び12で既に記載しています。 よって、原案のとおりとします。
	□P.5 端末及びアクセスポイントにおいて事前に設定・共有される共通の鍵として使用されるパスフレーズにより に変更を求める。PSKとパスフレーズの使い方に混乱が見られる。PSK （Pre-Shard Key)とパスフレーズをこの一文で「すり替え」ている点に非常に違和感と今回の担当者の信用にかかわる部分であり危険を感じた。 Passphraseはパスワードの文字数が多くなったもの指す言葉でありPre-shard Keyは事前共有鍵である。意味が異なる。	御指摘を踏まえ、次のとおり修正します。 PSK認証は、端末及びアクセスポイントにおいて事前に設定・共有~~される共通の鍵であるPSK（パスフレーズ）により、~~されているパスフレーズから、それぞれPSKと呼称される鍵を生成し、
	□P.7 SIMそのものがコピーや改ざんの手法が確立される可能性が捨てきられない以上この表現は不適当。SMの利用は機器認証の高速化とUSBや、カード読み取り機を必要としないため小型化が可能であるという点が主であり、コピーされた同一IDのものが出回るリスクは排除できない。この記述は削除が適当。	SIMカードがコピー及び改ざんされた事例は確認されておりませんので、御指摘は当たらないと考えます。 よって、原案のとおりとします。
	□P.8 IEEE802.11wはMITM（Man In The Middle）攻撃を低減する為である。 制御フレームの偽装とMACアドレスが暗号化される事が無い為、802.11wの効力は限定的であり更に対応した端末は圧倒的に少数である。 その旨、改めて記述する必要がある。	中間者攻撃は、正当な二者間の通信に介入する攻撃の呼称であることから、改ざんした管理フレームを繰返し送信する攻撃はDoS攻撃と分類することが適当と考えます。 また、IEEE802.11wにより、管理フレームの暗号化及び改ざん検知が可能となるため、IEEE802.11wは有効な情報セキュリティ対策です。 よって、原案のとおりとします。
	□P.9 このような偽装した管理フレームを繰り返し送信することにより、MITM（Main In The Middle）攻撃が可能となる。そこで、IEEE802.11wを活用することにより、管理フレームの正当性を判断できるようになり、この種のMITM攻撃によって無線LANの接続が遮断されることを防ぐことができ DoSは一般に大量のリクエストデータを該当する端末・サーバーに繰り返し送り、処理を遅延させる事や不正な命令を送ってサービス	中間者攻撃は、正当な二者間の通信に介入する攻撃の呼称であることから、改ざんした管理フレームを繰り返し送信する攻撃はDoS攻撃と分類することが適当と考えます。 よって、原案のとおりとします。

	を止める意味に使われる。無線ではDisconnect Packetの偽装送信はMITM攻撃特有のものであり一般の有線通信におけるDoSとは性質が異なるものと考える。	
	□P.9 MultiSSIDは空間へのビーコンフレームがSSID分増える事も示し2.4HGzの場合、2Mbpsの低速かつ広範囲に電波をばら撒くこと混信に拍車をかける原因にもなりかねない。 この点を注意事項として加えるべき。	「マルチSSIDによる通信量の増大が通信速度等に与える影響は、ノイズ等と比較して小さいと考えます。 よって、原案のとおりとします。
	□P.9 以下に修正するべきである (1) 電波の伝搬範囲の適切な設定 サービス継続の確保する為、通信の傍受、無線LAN機器への侵入、電波干渉による通信速度低下及び切断等の危険性を低減するため、アクセスポイントの電波の伝搬範囲を制限する。具体的には、次のような対策が考えられる。 － 窓、外壁付近等にアクセスポイントを設置しない。 － アクセスポイントの電波出力を調整する。 － アクセスポイントのアンテナとして指向性を有するものを使用する。 － 無線LANの利用区画と非利用区画の間に電波遮蔽シート等を使用する。 なお、設置時に電界強度マップの作成を推奨する。混信妨害が発生した場合迅速なトラブルシューティングを行う為に有効である。電波の伝搬範囲は、アクセスポイントの設置箇所周辺の状況等の影響を受けるため、定期的に時間毎の電界強度マップを作成し確認すべきである。	「電波の伝搬範囲の適切な設定」は、攻撃を受ける蓋然性を低減させる効果はありますが、暗号化等のように情報セキュリティ上の脅威に対する直接的な対策とはなり得ません。 よって、原案のとおりとします。 「無線LANへの侵入」については、御指摘を踏まえ「無線LANを経由した内部ネットワークへの侵入」と修正します。 また、電界強度マップの内容については、「電波状況の監視」及び「無線IDS／IPS」に含まれています。 よって、原案のとおりとします。
	□P.10 以下に変更する事を求める (4) 電波状況の監視 無線LANを運用する付近の電波を定期的に監視し、許可なく設置されたアクセスポイント及び不正なアクセスポイントが存在しないか確認を行う。 例えば、無線LANの通信機能を備えたパソコンに、無線LANの電波状況を確認するソフトウェアをインストールすることにより、周囲のアクセスポイントのSSID、MACアドレス、電界強度等の電波伝搬の状況を確認する。ただし、SSID及びMACアドレスは偽装することが可能であることを留意する必要がある。パソコンベースの検知ソフトでは一度に検知できる無線LANに制限があり20~30台までである。大規模な運用を行う場所（APが20以上が目安）では専用の無線LAN測定装置を使用することが望ましい。	御指摘を踏まえ、次のとおり修正します。 ~~アクセスポイント~~無線LANを構築・運用している場所及びその周辺の電波状況を定期的に監視し、許可なく設置されたアクセスポイント及び不正なアクセスポイントを検知する。 例えば、無線LANの通信機能を備えたパソコンに、無線LANの電波状況を確認するソフトウェアをインストールすることにより、周囲のアクセスポイントのSSID、MAC（Media Access Control）アドレス、電波強度等の電波状況を確認する。また、多数のアクセスポイントを設置し、大規模な無線LANを構築・運用している場合には、専用の機器を利用し詳細に確認することが適当である。ただし、SSID及びMACアドレスは偽装することが可能であることを留意する必要がある。 なお、アクセスポイント以外の不正な電波発生源を検知するためには、スペクトルアナライザ等の専用の機器が必要となる。
	□P.10 （5）アドホックについて Ad-hocモードは暗号化ではWEPのみしか対応していない事を明記するべき。 WiFi-Directを脚注に持ってくるべきではない。	IBSSのアドホックモードにおいても、暗号化方式としてWPAを利用可能な機器も存在していることから、御指摘は不正確と考えます。 また、Wi-Fi Directは、アドホックモードの利用を禁止することが適当であるとした上で、参考と紹介しているものであることから、脚注に記載しています。 よって、原案のとおりとします。
	□P.11 暗号化方式には、WEP、TKIP及びCCMPの3つの規格がある。 IEEE802.11-2012にあるBIPについて記述必要。	WEP、TKIP及びCCMPはデータフレームを暗号化する方式の名称であり、一方、BIPは管理フレームの完全性を確認する方式の名称であることから、同列に扱うことは不適当です。 よって、原案のとおりとします。
	□P.12 以下に修正すべきと提案する。 ④ 電波の伝搬範囲の設定 通信の傍受、無線LAN機器への侵入、電波干渉による通信速度低下及び切断等の危険性を低減するため、無線LANを利用できる場所として設定した範囲を超えて電波が漏出しないよう、電波の伝搬範囲を限定する。電波の伝搬範囲を限定するためには、窓側及び外壁付近を避け、なるべく中央にアクセスポイントを設置するなどの工夫を行うことが考えられる。また、より積極的な対策として、指向性のあるアンテナの利用、アンテナの向きの調整、電波出力の調整、電波遮蔽シートの使用等も有効である。電波伝搬のチェックの為に電界強度マップを作成する事を推奨する。	「電波の伝搬範囲の適切な設定」は、攻撃を受ける蓋然性を低減させる効果はありますが、暗号化等のように情報セキュリティ上の脅威に対する直接的な対策とはなり得ません。 よって、原案のとおりとします。 「無線LANへの侵入」については、御指摘を踏まえ、「無線LANを経由した内部ネットワークへの侵入」と修正します。
	□P.12 VPN（Virtual Private Network）についての手引が必要になる。多くの形式があり未だにTDES等古いタイプが使用されている場合がある。 社外からの運用を定義できない手引書は手引書の存在意義を問われるものになる。 国・総務省に求められるのは社外モバイル運用の指針と責任範囲であり、それが示されなければ検討中等の前向きな対応や図解を含めた丁寧な説明を求める。	ここでは参考としてVPNを紹介しており、詳細について記載することは本手引書の範囲を超えることになります。また、社外モバイル運用についても同様です。 よって、原案のとおりとします。
	携帯電話のデータ通信領逼迫を緩和する為は免許局の不当な不正利用と考えられないのか。通信の秘密を確保する上で無線LANほど普及した脆弱な機器は無い。 今後、独占的に利用できる周波数を割り当てられた事業者には無	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しません。

	線LANを使用しない様行政が指導するべきであると考える。	
	電波を利用する場合においては、第三者に傍受されることを前提としなければならい。 何故なら電波は公共のものであり、通信の秘密を担保するのは暗号技術と傍受した側の規律に頼るしか無い。この2つが不安定で技術革新や研究や社会的要因が重なり当てにならない事は歴史が証明する事であり強く啓発する文章が必要。	御指摘の前提に立ち、本手引書では種々の情報セキュリティ対策について記載しています。 よって、原案のとおりとします。
	公的に無線LANでビジネスを推進するのであれば、無線LANで収益を得る事業者は高額な教育費用の提供や過去に販売した古い機器の無償交換に応じるべきである。	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しません。