別紙1

「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第１版)」(案)についての意見募集の結果

○ 意見募集期間：平成 31 年3月2日（土）から4月1日（月）まで

○ 意見の件数：10 件

意見提出者	代表者氏名等	
一般財団法人電気通信端末機器審査協会	理事長	木村　順吾
ヴィタネット・ジャパン株式会社	代表取締役	山田　健雄
トレンドマイクロ株式会社	代表取締役社長（CEO）	エバ・チェン
一般社団法人デジタルライフ推進協会	代表理事	細野　昭雄
サイバートラスト株式会社	代表取締役	眞柄　泰利
個人 A		
個人 B		
個人 C		
個人 D		
個人 E		

「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第１版)」(案)
に対して寄せられた意見及びこれに対する考え方

No.	意見対象箇所	提出された意見	意見に対する考え方	修正の有無
●ガイドライン全体 関連				
0-1	全体	総務省が電気通信事業法に定める技術基準適合認定等の適用に関するガイドラインを策定され、その対象機器の範囲及び審査方法等について明定されることを積極的に評価致します。 ガイドライン施行後は、登録認定機関（登録外国適合性評価機関を含む。以下同じ。）における適確な遵守運用が確保されるべく、総務省がその執行状況を調査監督され、登録認定機関に対し適切に指導されることを期待致します。 【一般財団法人電気通信端末機器審査協会】	本ガイドライン(案)に賛成の御意見として承ります。	無
●第１章（IoT 機器のセキュリティ基準に係る技術基準適合認定等について） 関連				
1-1	1.セキュリティ基準に係る認定等の対象機器の範囲（P2）	2ページの枠内は、新規則の条文の抜粋であること、原文に加筆をしていることを注記として記載したほうがよいと思います。 【個人 C】	御指摘を踏まえ、新規則の条文の抜粋である旨を追記します。	有
1-2	1.セキュリティ基準に係る認定等の対象機器の範囲（P3 1 ポツ(1)）	3ページの米印2の2行目「端末設備等規則」は、「新規則」ではなく改正前の端末設備等規則を指していると理解してよろしいか？（米印3についても同様） 【個人 C】	御指摘の点については、省令改正による変更がないため、「端末設備等規則」と表記しています。	無
1-3	1.セキュリティ基準に係る認定等の対象機器の範囲（P3	１の対象機器の範囲ですが、（１）と（２）の部分は近距離無線通信技術（Bluetooth や Zigbee)を用いた機器が対象から外れてしまいます。近距離無線通信技術では、実際には殆ど使われていない6LoPAN 以外はインターネットプロトコルを使いません。それと、一般に近距離無線通信技術を使った機器は「恒常的に既に認定等を受けてい	本ガイドライン(案)は、情報通信審議会一部答申「IoT の普及に対応した電気通信設備に係る技術的条件」(平成 30 年9月 12 日）（以下	無

	1 ポツ(2))	る機器（以下「既認定機器」という。）を介さずにデジタルデータ伝送用設備 ※2に直接接続される端末機器」に当てはまりません。 さて、現実の IoT の多くを占める IP アドレスを持たない、IP プロトコルをサポートしない機器を今回の基準に含まないわけにはいかないと考えます。現在の案では、例として家庭での IoT しか意識していないように見受けられますが、オフィスや製造設備での IoT 機器とクラウドを組み合わせた利用は今後加速的に増えるとされています。 例えば、認証されたルータ（IoT ハブ、ゲートウェイ等多様な呼び方がされています）と Bluetooth の端末装置が接続された場合、Bluetooth の機器になりすまして誤った情報をルータに送る攻撃が考えられます。認証されたルータが誤った情報をサーバに転送してその誤った情報を基に施設運用・制御をするとシステム或いは設備の運用に重大な支障を来す可能性があります。悪意を持ってい送り込まれた異常な数値に基づいて設備の運用を停止するなどが考えられます。IoT の時代では、所謂ハッキングでシステムに侵襲して悪意の操作をしなくても、個人・法人・社会に悪意の影響を与えることが可能です。端末機器とルータの相互認証と通信の暗号化が防御の第一歩ですので、この点を基準認証に付加する必要があります。 まとめると、IP アドレスを持たない IoT 機器も適用の範囲とし、IoT 機器とルータ等との相互認証と通信の暗号化の実装を基準認証に加えることを強く進言いたします。その際、強度まで設定する必要はなく、各無線技術の持つ認証機能と暗号化が利用されていれば充分とすべきだと考えます。現状は、無線技術の用意する機能を利用しない実装も多く見受けられます。 蛇足ながら、ヘッドセットは、サーバがデータをヘッドセットから受け取り何かを制御することが意図されていませんので、上記の提言には含まれません。 以上、 【ヴィタネット・ジャパン株式会社】	「情通審答申」という。）を受けて、平成 31 年3月1日に公布された「端末設備等規則及び電気通信主任技術者規則の一部を改正する省令（平成 31 年総務省令第 12 号）」による改正後の端末設備等規則（以下「新規則」という。）において、インターネットプロトコルを使用し、電気通信回線設備に直接接続され、備えられた電気通信の送受信に係る機能の設定変更ができる IoT 機器を対象としてセキュリティ基準が定められたことを受けて、その運用・解釈の明確化を図ることを目的としたものです。 御指摘のような、インターネットプロトコルを使用しない IoT 機器の取扱いについては、今後の検討課題とさせていただきます。	
1-4	1.セキュリティ基準に係る認定等の対象機器の範囲（P3	本ガイドライン案の対象は、IP 通信が実装されている通信機器に限られるものであり、非 IP プロトコルやアナログ通信プロトコルで通信を行う IoT 機器は対象とはならないとされている。 しかしながら IoT 機器を対象とする攻撃は多々あり、その中でも今後増えることが想		無

	1 ポツ(2))	定される機器の乗っ取りに関する「なりすまし」や「踏み台」を防御していくためには、末端の端末への対策が不可欠と考えられる。 　つまり通信回線からみてファイアウォール/ルータ経由で接続される、PLC(プロブラマブルロジックコントローラ)等制御装置やゲートウェイ機器、および、下位のレイヤに散在するあらゆる IoT 機器が攻撃対象となることが想定されるため、IP 通信を実装する機器だけではなく幅広い IoT 機器を対象としたガイドラインも併せて整備すべきではないかと思われる。 【サイバートラスト株式会社】		
1-5	1.セキュリティ基準に係る認定等の対象機器の範囲（P3 1 ポツ(3))	・該当箇所 　右肩 3 ページ （3） ・意見 　「端末機器に備えられた電気通信の送受信に係る機能」と記載されていますが、この場合、送受信に係らないような設定変更を許容する機器は対象にならないようにも読むことができます。 【トレンドマイクロ株式会社】	新規則に定めるとおり、端末機器に備えられた電気通信の送受信に係る機能の設定変更ができるものがセキュリティ基準の対象となります。	無
1-6	1.セキュリティ基準に係る認定等の対象機器の範囲（P3 1 ポツ(4))	「PCやスマートフォン等がこれに該当し、セキュリティ基準の対象外となる。」とあるが、必ずしもすべてのデバイスにおいてソフトウェア更新機能が搭載されているわけではない。(Linux ベースの PC など) 　そこで「各号((5)～(7))に相当する機能を実装済みの PC やスマートフォン等がこれに該当し、セキュリティ基準の対象外となる。」と明記した方が良いと思われる。 【サイバートラスト株式会社】	御指摘の点については、情通審答申において、PC やスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能であり、それによりセキュリティ要件に関する機能が出荷時とは異なるものになることが想定される機器については、セキュリティ要件を適用することが馴染まないことから対象外とすることが適当とされたことを踏まえ、本ガイドライン（案）のとおり整理しています。	無

1-7	1.セキュリティ基準に係る認定等の対象機器の範囲（P3 2 ポツ）	本ガイドラインでは、ルータ等を介して、間接的にデジタルデータ伝送用設備に接続される IP 通信が実装されている通信機器は対象外とされているが、一般家庭等において、ルータのアクセス制御が適切に設定されていない場合、ルータ配下の機器の管理画面が、インターネット上からアクセスできてしまうケースが想定されるため、IP 通信が実装されている機器については、直接／間接接続を問わず、対象とすべきと思われる。 【サイバートラスト株式会社】	本ガイドラインの目的等は 1-3 に示すとおりです。 御指摘のような、電気通信回線設備に直接接続されない IoT 機器の取扱いについては、今後の検討課題とさせていただきます。	無
1-8	1.セキュリティ基準に係る認定等の対象機器の範囲(P3 2 ポツ)	第 1 章第 1 節について、電気通信事業法に基づく端末機器のセキュリティ基準の対象となる機器が明確化されており、この点において本案に賛同いたします。 一方で、対象機器の該当条件においては「既認定機器を介して接続されており、電気通信回線設備に直接接続して使用されない機器は、認定等を要しない」とされており、家庭内においてセキュリティ要件が該当する機器が実質ゲートウェイ(ルータ)機器のみとなり、今回作られた制度において対象とされなかった家庭内の機器がセキュリティ脅威から守られない懸念がございます。 例えば、近年の家庭内のネットワーク対応機器はクラウド連携により高機能を実現するようなもののうち、少なくない数の機器がゲートウェイ(ルータ)機器の制御を受けずに直接インターネットと通信を行う機能(UPnP プロトコル等が代表例として挙げられます)が動作することを前提に設計されており、ゲートウェイ(ルータ)がそれらの機器を含め家庭内の機器を防御することには限界があると考えられます。 サイバーセキュリティ対策は総務省・経済産業省が中心となり複数の制度整備の組み合わせによって設計される由方向性が示されておりますが、それらを含め家庭内のネットワーク機器を包括したセキュリティ対策制度をご検討いただければと存じます。 【一般社団法人デジタルライフ推進協会】		無
1-9	1.セキュリティ基準に係る認定等の対象機器の範囲(P3 2 ポツ)	・該当箇所 右肩 3 ページ 「既認定機器を介して接続されており、電気通信回線設備に直接接続して使用されない機器は、認定等を要しない」	本ガイドライン(案)において、既認定機器であるルータを介して接続されており、電気通信回線設備に直接接続して使用されないゲーム機やウェブカメラ等の機器につい	無

		・意見 　UPnP やユーザの操作によってルータの設定を変更させ、ポートを開けて利用することをメーカーが前提とした機器は、今回の要件に該当しますか。 具体的には、PlayStation 4 などのゲーム機や Web Camera などがあります。 https://www.jp.playstation.com/op/codbo3/playersinfo/2016/03/3-network-device.html https://bouhancamera-choice.com/networkcamera-connect/ 　今回のケースは、「（3）電気通信回線設備を介して接続することにより当該専用通信回線設備等端末に備えられた電気通信の機能（送受信に係るものに限る。）に係る設定を変更できるもの」には該当するが「既認定機器を介して接続されており、電気通信回線設備に直接接続して使用されない機器は、認定等を要しない」ものになります。 【トレンドマイクロ株式会社】	ては、認定等を要しないものと整理しています。	
1-10	1.セキュリティ基準に係る認定等の対象機器の範囲(P3 3ポツ)	3 ページの最期の項目で、「直接接続して使用できない旨を記載する等の措置を講ずる必要がある。」との記載があるが、不十分ではないか？直接接続しようとしてもできないように設計することを義務付けるべきではないか？ 【個人 E】	御指摘の点については、情通審答申において、利用者が認定等を取得していない機器を誤って直接接続しないようにするため、例えば、取扱説明書等において、①当該機器は既認定機器に接続する必要があることや、②電気通信事業者の電気通信回線設備に直接接続する場合には、電気通信事業者による検査が義務付けられていることを記載すること等をガイドライン等により明示することについて検討する必要があるとされたことを踏まえ、本ガイドライン(案)のとおり整理しています。	無

1-11	2.セキュリティ基準の内容・解説(P5 1ポツ(6))	識別符号の初期値の変更を促す機能について、「機器ごとに異なるものが付されていることが満たされれば、変更機能は無くて良い」とされているが、これは安全な形で識別符号が格納されていることが前提となる。 そこで、「識別符号の保管先は、難読化等、耐タンパ技術によって、容易に読みだせないような対策を講じることが望ましい。」というコメントを追加することを提案する。 【サイバートラスト株式会社】	御指摘を踏まえ、識別符号が安全に保管されることが推奨されるべきことをセキュリティ基準の解説に追記します。	有
1-12	2.セキュリティ基準の内容・解説(P5 1ポツ(7))	ファームウェア更新機能の義務化が規定されているが、ファームウェア自体の安全性については、「推奨」にとどめられている。 しかし、昨今ファームウェア更新におけるウィルス感染が問題視されていることから、コード署名によりファームウェアが改ざんされていないことを証明し、安全性なアップデートを担保する仕組みやマルウェアを判別する機能もガイドラインに含めることが望まれる。 【サイバートラスト株式会社】	御指摘の点については、情通審答申において、ソフトウェアの更新は安全かつ自動で行われることが推奨されるが、IoT 機器は多種多様であり、更新の手法は機器の種別毎に異なることから、安全かつ自動の更新までは要件としないことが適当とされたことを踏まえ、本ガイドライン(案)のとおり整理しています。 御指摘のような、ソフトウェアの安全な更新を担保する仕組みについては、今後の検討課題とさせていただきます。	無
1-13	2.セキュリティ基準の内容・解説(P6(9))	CC 認証(ISO/IEC15408)と同等のセキュリティ強度を目指すのであれば、ST(セキュリティターゲット)の審査基準や適合要素のマトリクスなど開示も必要だと考えられる。 【サイバートラスト株式会社】	御指摘の点については、情通審答申において、CC 認証などの国際標準に基づくセキュリティ認証を取得した複合機など、アクセス制御機能、ID/ﾊﾟｽﾜｰﾄﾞの適切な設定を促す等の機能及びファームウェアの更新機能と同等以上のセキュリティ機能を有すると認められるものについては、セキュリティ要件を満足す	無

			るものとみなすことが適当とされたことを踏まえ、本ガイドライン(案)のとおり整理しています。	
1-14	その他（全体）	「サイバーセキュリティー対策」におけるソフトウェアーの「アップグレード（更新）」を主流としても、ハードウェアーのデバイス技術に対し、「容量（キャパシティー）」での「限界値（リミッター）」が有ると、私は考えます。 具体的には、「センサー技術、ネットワーク技術、」から成る「CPS（サイバーフィジカルシステム）」を導入する事で、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される事と、私は考えます。 例えばですが、「Dos 攻撃」及び「DDoS 攻撃」が主流と、最新では、「ボット（機械による自動での送受信システム）」等は、時間的な要素を追求が出来る事で、ファイアーウォールを掻い潜る事により、「NTP（ネットワークタイムプロトコル）」の対策が必要と、私は考えます。 要約すると、サイバーセキュリュテイー対策には、構造の事例が有ります。（ア）「通信衛星回線（サテライトシステム）」における「DFS（ダイナミックフレカンシーセレクション）」での構造の部分。（イ）「電話回線（テレコミュニケーション）」における「SIP サーバー（セレクションイニテェーションプロトコル）」での構造の部分。（ウ）「インターネット回線（ブロードバンド）」における「DNS サーバー（ドメインネイムシステム）」での構造の部分。（エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」等による融合での構造の部分。 要するに、サイバーセキュリティー対策とは、「フィジカル空間（物理空間）での「AP（アクセスポイント）」の構造に対し、「サイバー空間（情報空間）」での「中継点（リレーポイント）」における「VPN（バーチャルプライベートネットワーク）」の構造と、私は思います。 【個人 A】	本ガイドラインの目的等は 1-3 に示すとおりです。	無
1-15	その他（全体）	「サイバーセキュリティー対策」における構造では、ソフトウェアーでの「アップデート（更新）」を施しても、デバイス的な部分での無駄な事と、私は思います。 例えばですが、ハードウェアー及びソフトウェアーでの「モジュール（交換の部品）」	本ガイドラインの目的等は 1-3 に示すとおりです。	無

		の「Assy 基板（実装基板）」における「CPU 及び IC（マイコン制御）」での「ファームウェアー（ハードウェアー及びソフトウェアーの組み込み）」の事と、私は思います。 　具体的には、「情報技術（IT）」及び「人工知能（AI）」の分野が構造的に、区別が有ると考えます。（ア）IT ネットワークの分野では、「ビックデーター（BD）」から成る「データーベース（DB）」おけるクラウドコンピューティングが主流に成る事。（イ）AI ネットワークの分野では、Web 上での「MTML（ハイパーテキストマークアップラングエッジ）」から成る「HTTP（ハイパーテキストロランスファープロトコル）」通信での「API（アプリケーションプログラミングインターフェイス）」におけるエッジコンピューティングが主流に成る事。 　要約すると、クラウドコンピューティングの場合では、電話回線の基地局制御サーバーでの「SIP サーバー（セッションイニテーションプロトコル）」及びインターネット回線の ISP サーバーでの「DNS サーバー（ドメインネイムシステム）」の分野での「企業側（キャンパニー）」の「運用及び管理」をしたネットワークサーバーの事と、私は考えます。エッジコンピューティングの場合では、IoT 機器に接続をした「ユーザー側（個人利用者）」の事と、私は考えます。 　要するに、「ポート通信（IP アドレスの通信）」の事を提唱すると、「通信衛星回線（サテライトシステム）」における「DFS（ダイナミックフレカンシーセレクション）」に対しても、サイバーセキュリティー対策が必要と、私は考えます。 【個人 A】		
●第2章（電波を使用する端末機器に係る技術基準適合認定等について） 関連				
2-1	1.技術基準適合認定等の対象機器の範囲及び審査方法等(P9 2 ポツ)	9ページの16行目「平成 6 年郵政省告示第 424 号」の名称は、「端末設備等規則の規定に基づく識別符号の条件等」ではないのか？ 【個人 C】	御指摘を踏まえ、「平成 6 年郵政省告示第 424 号」の名称を追記します。	有
2-2	1.技術基準適合認定等の対	9ページの9行目、最下行の「端末設備等規則」は、「新規則」ではなく改正前の端末設備等規則を指していると理解してよろしいか？	御指摘の点については、省令改正による変更がないため、「端末設	無

	象機器の範囲及び審査方法等(P9 2ポツ、4ポツ)	【個人C】	備等規則」と表記しています。	
2-3	1.技術基準適合認定等の対象機器の範囲及び審査方法等(P9 3ポツ)	9ページの最下行から上に2行目「関係規定」の名称を記載したほうがよいと思います。 【個人C】	御指摘を踏まえ、「関係規定」の名称を追記します。	有
2-4	1.技術基準適合認定等の対象機器の範囲及び審査方法等(P9 3ポツ)	9ページの22行目「または」は、他の箇所と同様に「又は」と記載したほうがよいと思います。 【個人C】	御指摘を踏まえ、「又は」に修正します。	有
2-5	その他(全体)	匿名を希望いたします。 端末設備規則第九条には「端末設備を構成する一の部分と他の部分相互間において電波を使用する端末設備」とありますので、総務省の見解通りコードレス電話以外の Wi-Fi や Bluetooth 等に適用するのは無理があると考えています。 Wi-Fi ホットスポット等を想定した無線で提供される電気通信回線に接続することができる Wi-Fi(子機)については、端末設備規則第三十四条の八および平成23年3月22日 総務省告示第87号を適用することが明確であるかと思います。 上記より、ガイドライン第2章の内容に賛成いたします。 また、審査方法として以下を提案いたします。 端末設備規則第六条の絶縁抵抗／絶縁耐力につきまして、これは無線で事業用電気通信設備に接続する端末設備には要求されないと解釈できるようガイドラインに盛り込めないでしょうか。 登録認定機関による機器の認定に際しては、Wi-Fi や Bluetooth 機器についても端末設備規則第六条の要求をされますが、これは電気通信回線と何ら電気的な接続が	本ガイドライン(案)に基本的に賛成の御意見として承ります。 なお、御指摘の点については、本ガイドライン(案)において、既認定機器を介して接続されており、電気通信回線設備に直接接続して使用されない機器については、認定等を要しないものと整理しており、端末設備等規則第6条も適用されないこととなります。 この点については、登録認定機関における実運用等を踏まえつつ、適切に周知して参ります。	無

		ない無線接続端末については明らかに不当な要求かと思います。 　端末設備規則第六条第１項の本来の趣旨は、端末設備側の電源回路等の絶縁不足で、メタルで提供される事業用電気通信回線に異常な電圧を印加しないことで、第２項の趣旨は、電気通信回線側からの感電を防止するユーザーに対する危険防止ではないでしょうか。 【個人 B】		
○その他				
3-1	ー	＞全般的に 　国民としては、いい加減に、PPP（PPPoE）において、CHAP 又は PPP ではなく、EAP を使いたいのであるが、こういう事については、この様なガイドラインで何とかならないものなのであろうか。 　2005 年頃には CHAP ではなく EAP を使う・使える様に各事業者がしていくべきだったと思われるのであるが、PPP（PPPoE）の通信が CHAP 止まりの現状は全世界的に見て頭がおかしいものであると考える。 　どこに何度言っても、どこもこの状況を変える気は無い様子なのであるが（ただ、無線 LAN についてはその通信に普通に EAP が用いられているが。また、簡易 RADIUS 的な管理・端末制限が行える機能が無線 LAN ルータにおいても通常備わっているが。…何故それを有線で行わないのであろうか？ネットワーク業界関係者は全員が全員頭がおかしいのであろうか？他の分野のエンジニアが見ると「何をやっているのだ？こいつらは。」としかならないのであるが。大きな疑問である。）、かくなる上は国が主導して（=事業者の尻を叩いて…叩かれるのが然るべき者達であるはずである。NTT などは日本の恥であって誇りではない。）状況を変えていっていただきたいと考える。 　時代は PPPoE から IPoE へと移りつつある様な気もするのであるが（しかしおかしな話である。IPv6 については PPPoE を用いてアクセスしてもいいはずであるのだが…。NTT 東西のひかり電話を用いつつ、各 ISP に IPv6PPPoE でアクセスして（PPP でカプセル化し、それを NTT 局でデカプセル化すると、あまり IPoE と速度的に変わらないのではないかと思われるのであるが…。どうせ L2 層では MAC アドレスは変更が必要な	本ガイドラインの目的等は 1-3 に示すとおりです。	無

		のであるし、よってパケットを直接そのままの形で用いるのは IPoE でも無理なのであるから、基本として速度に大差が出る事は考え辛い。）、IPv4（PPPoE での IPv4overIPv6）及び IPv6 でサービス提供が行われるというのが、素直な形ではないのか。何故、日本国民が、KDDI 系の JPNE 配下に収められるなどという事になるのがメジャーな事態になったりするのであろうか？ネットワーク業界関係者事情は複雑怪奇であると言わざるを得ない。道理では考え辛いものである。必ず KDDI 系（トヨタ系である。）の陰謀があるはずである（あまりにもその根拠が確固たる陰謀論は陰謀論と言うのであろうか？）。）、PPP は依然として重要なものであるので、CHAP 又は PPP などの原始的な手段に替えて、EAP を用いれるように国としてしていっていただきたい。 意見は以上である。 【個人 D】		