

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2版)

2020 年9月1日

総務省

目次

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	3
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	10

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

情報通信審議会からの一部答申(平成30年9月12日)及び情報通信行政・郵政行政審議会からの答申(平成31年1月25日)を受けて、IoT機器の技術基準にセキュリティ対策を追加するため、総務省において「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)」を公布(平成31年3月1日)。(端末設備等規則の一部改正については令和2年(2020年)4月1日施行。)

同省令による改正後の端末設備等規則(昭和60年郵政省令第31号、以下「新規則」という。)第34条の10の規定(以下「セキュリティ基準」という。)に関する電気通信事業法(以下「法」という。)の規定による技術基準適合認定(法第53条第1項)、設計認証(法第56条)又は技術基準適合自己確認(法第63条)(以下「認定等」という。)の運用について明確化する観点から、以下のとおり整理する。

○端末設備等規則(「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)〈抜粋〉

(インターネットプロトコルを使用する専用通信回線設備等端末)

第三十四条の十 (1)専用通信回線設備等端末(デジタルデータ伝送用設備に接続されるものに限る。以下この条において同じ。)であつて、(2)デジタルデータ伝送用設備との接続においてインターネットプロトコルを使用するもののうち、(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。以下この条において同じ。)に係る設定を変更できるものは、次の各号の条件に適合するもの又は(9)これと同等以上のものでなければならない。ただし、(4)次の各号の条件に係る機能又はこれらと同等以上の機能を利用者が任意のソフトウェアにより随時かつ容易に変更することができる専用通信回線設備等端末については、この限りでない。

一 (5)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に係る設定を変更するためのアクセス制御機能(不正アクセス行為の禁止等に関する法律(平成十一年法律第百二十八号)第二条第三項に規定するアクセス制御機能をいう。以下同じ。)を有すること。

二 (6)前号のアクセス制御機能に係る識別符号(不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号をいう。以下同じ。)であつて、初めて当該専用通信回線設備等端末を利用するときあらかじめ設定されているもの(二以上の符号の組合せによる場合は、少なくとも一の符号に係るもの。)の変更を促す機能若しくはこれに準ずるものを有すること又は当該識別符号について当該専用通信回線設備等端末の機器ごとに異なるものが付されていること若しくはこれに準ずる措置が講じられていること。

三 (7)当該専用通信回線設備等端末の電気通信の機能に係るソフトウェアを更新できること。

四 (8)当該専用通信回線設備等端末への電力の供給が停止した場合であつても、第一号のアクセス制御機能に係る設定及び前号の機能により更新されたソフトウェアを維持できること。

1. セキュリティ基準に係る認定等の対象機器の範囲

- セキュリティ基準に係る認定等を求める対象は、新規則第 34 条の 10 柱書に定める以下の(1)から(3)までの全てに該当し、同条ただし書に定める(4)を除く端末機器である^{*1}。セキュリティ基準に係る認定等の対象機器の範囲のイメージは図 1 のとおり。

※1 例えば、ルータ、ウェブカメラ等がこれに該当する。IPを使用しない機器や専用線のみにつながる機器は含まれない。

(1) 専用通信回線設備等端末(デジタルデータ伝送用設備に接続されるものに限る。)

恒常的に既に認定等を受けている機器(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のことであり、専ら専用通信回線設備^{*3}に接続される端末機器は含まれない。

※2 「デジタルデータ伝送用設備」とは、電気通信事業の用に供する電気通信回線設備であって、デジタル方式により、専ら符号又は映像の伝送交換を目的とする電気通信役務の用に供するものをいう。(端末設備等規則第2条第2項第 15 号)

※3 「専用通信回線設備」とは、電気通信事業の用に供する電気通信回線設備であって、特定の利用者に当該設備を専用させる電気通信役務の用に供するものをいう。(端末設備等規則第2条第2項第 14 号)

(2) デジタルデータ伝送用設備との接続においてインターネットプロトコルを使用するもの

デジタルデータ伝送用設備との接続においてインターネットプロトコル(IP)を使用する端末機器のことである。

(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

端末機器に備えられた電気通信の送受信に係る機能について、電気通信回線設備を介して接続することにより設定変更(操作)できるものである。例えば、インターネット側からアクセスし操作可能なネットワークサービス(web 管理、telnet 等)などがこれに該当する。

(4) 次の各号の条件に係る機能又はこれらと同等以上の機能を利用者が任意のソフトウェアにより随時かつ容易に変更することができる専用通信回線設備等端末

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。なお、PC及びスマートフォン等の利用者においてアンチウィルスソフトを導入する等の適切な対策が行われることが推奨される。

- 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^{*4}。

※4 例えば屋外に持ち出して使用されない機器(エアコン、冷蔵庫、洗濯機、照明、テレビ、複合機等)がこれに該当するが、これらの機器が電気通信回線設備に直接接続して使用される場合は、この限りでない。

- 利用者が誤って電気通信回線設備に直接接続しないようにするため、認定等を受けていない機器については、取扱説明書(取扱説明書の追補その他の書面及びウェブ上の情報提供を含む。)に電気通信事業者の電気通信回線設備に直接接続して使用できない^{*5}旨を記載^{*6}する等の措置

を講ずる必要がある。

※5 法において、認定等を受けていない機器については、電気通信事業者による検査を受けない限り、電気通信回線設備に直接接続して使用できないこととされている。

※6 記載例として「本製品は電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダ等）の通信回線（公衆無線 LAN を含む）に直接接続することができません。本製品をインターネットに接続する場合は、必ずルータ等を経由し接続してください。」等が考えられる。

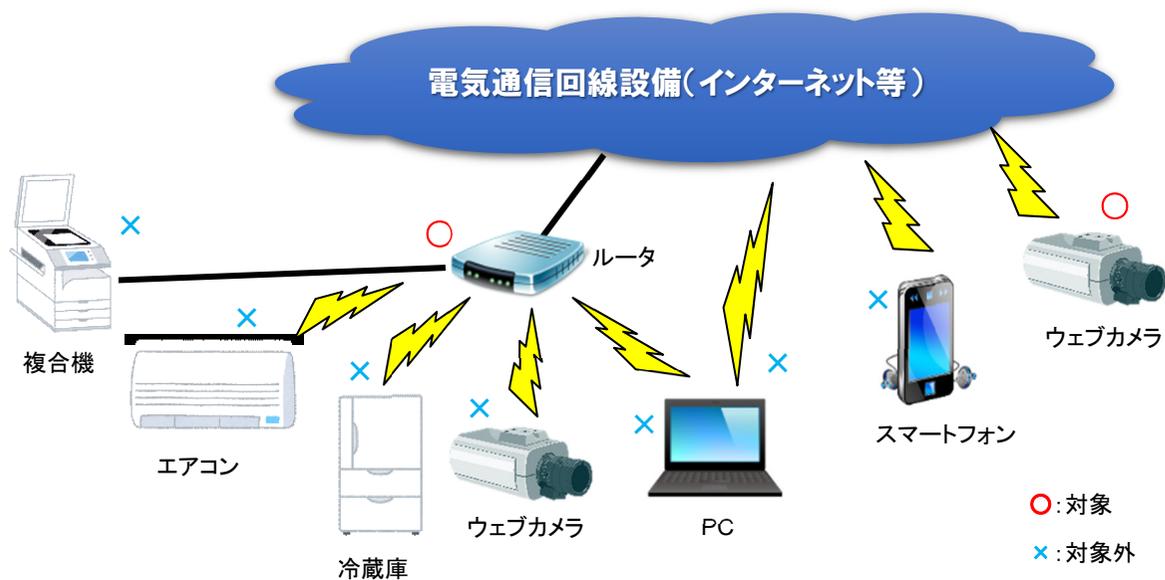


図1 セキュリティ基準(新規則第34条の10)に係る技術基準適合認定等の対象機器の範囲のイメージ

2. セキュリティ基準の内容・解説

- セキュリティ基準においては、対象機器が、新規則第 34 条の 10 各号に定める以下の(5)から(8)までの条件又は同条柱書に定める(9)の条件を満たさなければならないこととしている。

(5) 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に係る設定を変更するためのアクセス制御機能(不正アクセス行為の禁止等に関する法律(平成十一年法律第百二十八号)第二条第三項に規定するアクセス制御機能をいう。以下同じ。)を有すること

電気通信回線設備を介して接続されることにより、端末機器に備えられた電気通信の送受信に係る機能が不正に設定変更(操作)されないことを目的として、当該設定変更(操作)の前にアクセス制御を行うことができる機能を有していなければならないものである。このアクセス制御機能は、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(操作)を正規の利用者等以外の者ができないよう制限するための機能であり、利用者に識別符号(機器の利用にあたって用いられる符号であって利用者を区別して識別するために用いるものであり、具体的にはパスワード又はパスワードと ID を組み合わせたもの等をいう。以下同じ。)の入力を求め、正しい識別符号が入力された場合にのみ当該設定変更(操作)の制限を自動的に解除し、正しい識別符号ではなかった場合には設定変更(操作)を拒否する機能である。

(6) 前号のアクセス制御機能に係る識別符号(不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号をいう。以下同じ。)であつて、初めて当該専用通信回線設備等端末を利用するときにあらかじめ設定されているもの(二以上の符号の組合せによる場合は、少なくとも一の符号に係るもの。)の変更を促す機能若しくはこれに準ずるものを有すること又は当該識別符号について当該専用通信回線設備等端末の機器ごとに異なるものが付されていること若しくはこれに準ずる措置が講じられていること

アクセス制御の際に使用する識別符号が他人から容易に推測できないものとして設定されることを目的として、識別符号の初期値(例えばパスワードと ID の両方による認証や複数のパスワードによる認証など、複数の符号の組合せにより初期値が設定されている場合は、少なくとも一の ID 又はパスワードの初期値)の変更を促す機能があり、若しくは機器ごとに別の識別符号(ID/パスワード)が付されており、又は、これらに準じる機能・措置が講じられているものでなければならないものである。これらの場合において、識別符号が安全に保管されることが推奨される。なお、取扱説明書等に識別符号の初期値の変更を促す記載をすることは、これらに準ずる措置として認められない。

(7) 当該専用通信回線設備等端末の電気通信の機能に係るソフトウェアを更新できること

端末機器に記憶されている電気通信の送受信の機能に係るソフトウェアの更新を行うことができる機能(ファームウェアの更新機能)を有していなければならないものである。なお、IoT 機器は多種多様であり、当該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でなければならないことまではセキュリティ基準として求めないが、当該更新は安全かつ自動で行われることが推奨される。

(8) 当該専用通信回線設備等端末への電力の供給が停止した場合であつても、第一号のアクセス制御機能に係る設定及び前号の機能により更新されたソフトウェアを維持できること

端末機器への電力供給が停止して電源オフになった後、電力供給が再開されて電源オンに戻って電気通信の機能が復帰した際に、アクセス制御の際に使用する識別符号の設定及び更新された電気通信の送受信の機能に係るソフトウェアが、出荷時の初期状態に戻ることなく、電源オフになる直前の状態を維持できるものでなければならないものである。

(9) これと同等以上のもの

新規則第 34 条の 10 各号の条件に適合するものと同等以上のセキュリティ対策が講じられていると認められる場合は、セキュリティ基準を満たすこととしている。具体的には、対象機器が国際標準 ISO/IEC15408 に基づくセキュリティ認証(CC 認証)を受けた機器などがこれに該当する。

3. セキュリティ基準に係る技術基準適合認定等の審査方法

- セキュリティ基準の対象機器が、セキュリティ基準を満たしていることについての確認は、製品を対象として、技術基準適合認定(法第 53 条第 1 項)、設計認証(法第 56 条)又は技術基準適合自己確認(法第 63 条)のいずれかの方法により行う。

技術基準適合性の確認方法	技術基準適合認定 (法第 53 条第 1 項)	設計認証 (法第 56 条)	技術基準適合自己確認 (法第 63 条)
書面による確認	<p>・申請者がセキュリティ基準に適合するための機能又は措置の内容^{*1}について、以下の書類により、登録認定機関に申請する。</p> <ul style="list-style-type: none"> ○ 名称、用途、構成、機能及び仕様の概要を説明した資料 ○ 外観、構造及び寸法を記載した外観図 ○ 接続系統図 ○ ブロック図 ○ 機器の取扱い及び操作の方法を説明した資料 ○ 端末機器のセキュリティ基準に係る試験結果(各機能を具備しており正常に動作することがわかる以下の資料①～④全て) ①設定画面の写し ②メーカーの動作確認結果 ③メーカーの製造手順書 ④セキュリティ基準に適合するために機能性をどのように実現しているのかがわかる資料^{*2} <p>・これらを基に、端末機器が技術基準に適合していることについて登録認定機関が審査する。 【端末機器(個体)が対象】</p>	<p>・申請者がセキュリティ基準に適合するための機能又は措置の内容^{*1}について、以下の書類により、登録認定機関に申請する。</p> <ul style="list-style-type: none"> ○ 名称、用途、構成、機能及び仕様の概要を説明した資料 ○ 外観、構造及び寸法を記載した外観図 ○ 接続系統図 ○ ブロック図 ○ 機器の取扱い及び操作の方法を説明した資料 ○ 端末機器のセキュリティ基準に係る試験結果(各機能を具備しており正常に動作することがわかる以下の資料(①、③、④は必須、実機による動作確認を行う場合は②は不要)) ①設定画面の写し ②メーカーの設計段階での動作確認結果 ③メーカーの製造手順書 ④セキュリティ基準に適合するために機能性をどのように実現しているのかがわかる資料^{*2} ○ 端末機器が設計に合致することの確認方法書 <p>・これらを基に、端末機器が技術基準に適合していることについて登録認定機関が審査する。 【端末機器の設計(量産向け)が対象】</p>	<p>・申請者がセキュリティ基準に適合するための機能又は措置の内容^{*1}及びこれらが技術基準に適合していることの自己確認の結果について、以下の書類により、総務大臣に届け出る。</p> <ul style="list-style-type: none"> ○ 名称、用途、構成、機能及び仕様の概要を説明した資料 ○ 外観、構造及び寸法を記載した外観図 ○ 接続系統図 ○ ブロック図 ○ 機器の取扱い及び操作の方法を説明した資料 ○ 端末機器のセキュリティ基準に係る試験結果(各機能を具備しており正常に動作することがわかる以下の資料①～④全て) ①設定画面の写し ②メーカーの設計段階での動作確認結果 ③メーカーの製造手順書 ④セキュリティ基準に適合するために機能性をどのように実現しているのかがわかる資料^{*2} ○ 端末機器が設計に合致することの確認方法書
実機による試験	<p>・申請者が希望すれば、登録認定機関において、実環境下でPC等に接続し、各機能が正常に動作することを確認するための試験を行うことも可能。</p>		—

※1 認定等の対象機器が、国際標準 ISO/IEC15408 に基づくセキュリティ認証(CC 認証)を受けている場合は、その旨を証する書類を添付することで足りる。

※2 セキュリティ基準に適合するための各機能の本質的な内容は変わらないが、ソフトウェアのアップデート等により、各機能の設定画面等に変更が生じる場合は、認定等の申請の際にその旨を明確化することにより、当該変更に起因する再度の認定等は要さないこととする。

4. 適合表示端末機器を組み込んだ端末機器の扱い(通信モジュール等の扱い)

- 既に端末設備の接続の技術基準(セキュリティ基準を除く。)に係る認定等を受けて表示が付されている端末機器(適合表示端末機器)を組み込んだ製品がセキュリティ基準の対象機器である場合は、当該製品を対象として、端末設備の接続の技術基準(セキュリティ基準を含む。)に係る認定等を受けることとなる^{※1}。

その場合は、セキュリティ基準への適合性については上記3.の方法で確認を行うとともに、認定等の申請書類においてセキュリティ基準以外の技術基準への適合性を示す資料(適合表示端末機器の認定番号、認定書の写し等の認定を証する書類及び登録認定機関が必要とする場合は認定等に係るデータ等)を添付することとする。

※1 当該製品に付される技術基準適合認定番号、設計認証番号又は届出番号(以下「認定等番号」という。)は、組み込む前の適合表示端末機器に付された認定等番号とは異なるものとなる。

- なお、新規則の施行日前に認定等を受けた端末機器については、なお従前の例によることができているところ、適合表示端末機器を組み込んだ端末機器についての新規則の施行日後におけるセキュリティ基準に係る認定等の扱いについては、次表のとおり。

モジュール単体での認定等取得時期	施行前 (~R2.3.31)	施行後 (R2.4.1~)		【参考】 施行前に販売済みの製品
モジュール単体でのセキュリティ認定等の有無		あり	なし	
モジュールを組み込んだ端末機器のセキュリティ基準に係る認定取得の要否	要	不要 ^{※2}	要	不要 ^{※3}

※2 モジュール単体での認定取得時とセキュリティ関連の設計が異なる場合には、組み込み後の端末機器での認定取得が必要。

※3 必要に応じてセキュリティ基準についての認定等を取得することも可能。

5. その他(市場調査等の活用)

- 総務省においては、認定等を受けて市場に流通する端末機器(一定数)を抽出して技術基準への適合性を確認し、当該技術基準への適合性が認められない場合は必要な措置を講ずる制度(法第 54 条、第 59 条、第 67 条等)も活用する。

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

電波を使用する端末機器に係る認定等の対象範囲や審査方法等の運用について、関係者(登録認定機関、端末機器メーカー等)間の認識の共通化の観点から、以下のとおり整理する。

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

(1) Wi-Fi 及び Bluetooth を搭載した端末設備

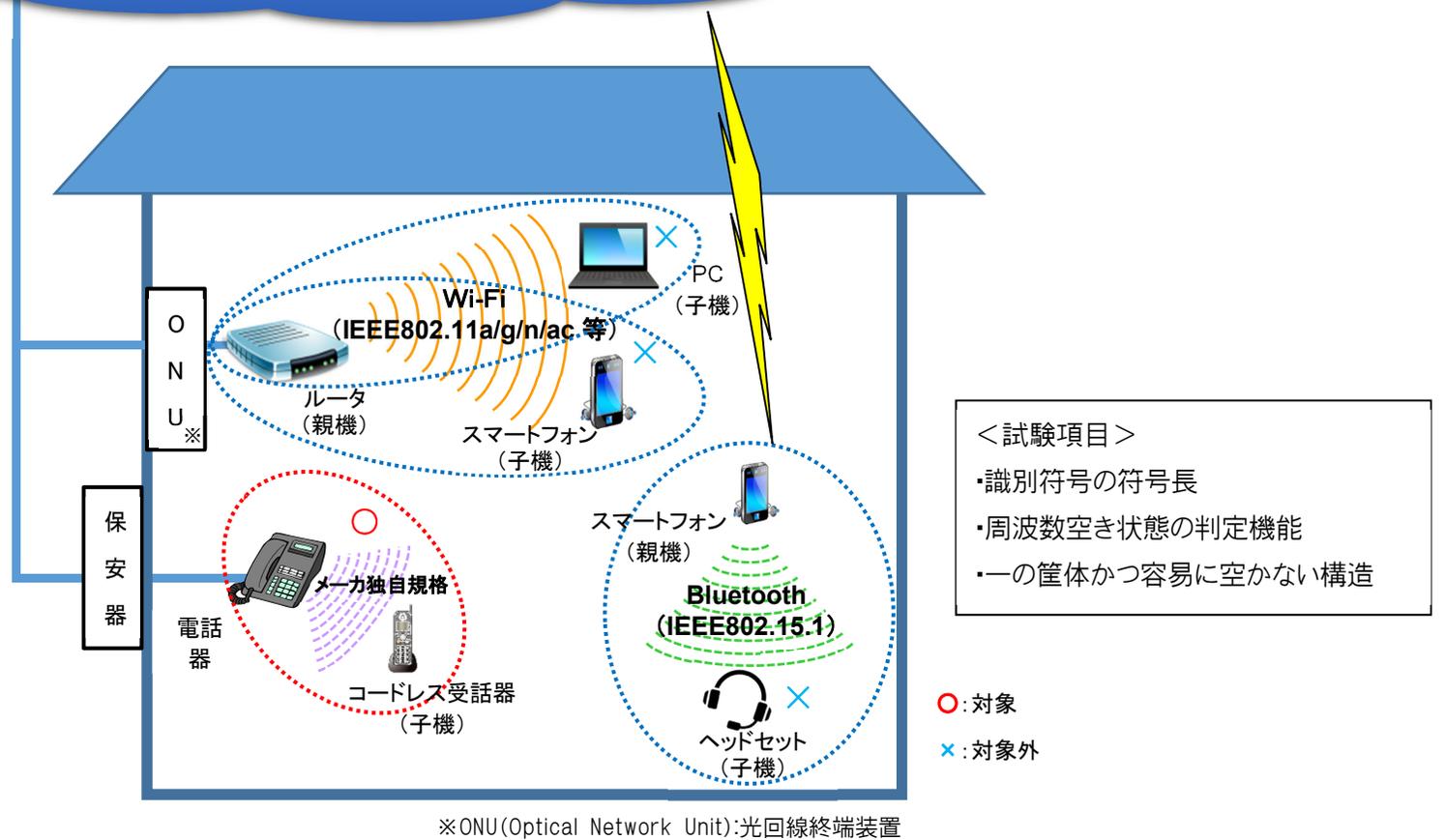
- 第1章で述べたとおり、既認定機器を介して接続されており、電気通信回線設備に直接接続して使用されない機器については、認定等を要しない。一方、電気通信回線設備に直接接続して使用される機器については、認定等を受けることが必要である。
すなわち、Wi-Fi や Bluetooth 等の通信機能を搭載した PC やスマートフォンなど電波を使用する端末機器についても、電気通信回線設備に直接接続して使用することが十分想定される機器については、認定等を受けることが適当である。
- また、端末機器が電気通信回線設備に直接接続されるか否かという観点以外に、端末設備等規則第9条(端末設備内において電波を使用する端末設備)との関係において、「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」としての試験を行う必要性についても留意が必要である。
同条の規定は、電波を介して親機と子機が一体・不可分で使用されるコードレス電話について、その誤接続・誤課金の防止を目的として導入したもので、以降、類似の懸念が想定される端末設備が対象に追加されてきた経緯があり、その試験は親機と子機を一体で行うことを想定しているものである。(例えば、現状のコードレス電話の試験は、組み合わせで使用される可能性のある親機と子機のセットでのみ行われている。)。
したがって、そのような懸念が想定されないような端末設備については必ずしも同条を根拠とした試験を必要としないものであり、これまでの運用等を踏まえると、例えば、平成6年郵政省告示第424号(端末設備等規則の規定に基づく識別符号の条件等)における「小電力データ通信システムの無線局の無線設備」のうち、Wi-Fi の親機(ルータ)と子機(PC等)の組み合わせについては、Wi-Fi は国際標準規格(IEEE)に基づくものであり誤接続防止等に係る信頼性が高く、当該規格に準拠している限り親機と子機は様々な組み合わせで使用され、一体性が相対的に低いと考えられるため、Wi-Fi Alliance の認証を受けた旨の表示(認定ロゴ)があるものについては、同条を根拠とした親機と子機一体での試験を行う必要はなく省略可能とすることが適当である(当該規定の趣旨から子機のみ試験を行う必要はない。))。
- また、Bluetooth の親機(携帯電話)と子機(ヘッドセット等)の組み合わせについても、上述の Wi-Fi と同様に国際標準規格(IEEE)に準拠していること等から、Bluetooth SIG の認証を受けた旨の表示(認定ロゴ)があるものについては、親機と子機一体、又は子機のみ試験を行う必

要はなく省略可能とすることが適当である。

なお、Bluetooth ヘッドセットが平成 16 年総務省告示第 95 号(技術基準適合認定及び設計についての認証の対象となるその他端末機器)により認証を要するアナログ電話用設備又は移動電話用設備に接続される「音声補助装置」に当たるかどうかについては、有線接続のヘッドセットと同様に認証の対象とはならない。

- 端末設備等規則第9条に係る試験の要否のイメージは図 2 のとおり。

電気通信回線設備(インターネット等)



- <試験項目>
- ・識別符号の符号長
 - ・周波数空き状態の判定機能
 - ・一の筐体かつ容易に空かない構造

図2 端末設備等規則第9条に係る試験の要否のイメージ

(2) sXGP デジタルコードレス電話

- sXGP デジタルコードレス電話システムが PHS の後継システム的な位置づけのものであると考えた場合、システム構成は次の図 3 のようなものが考えられ、責任分界点は A に示す箇所にあると考えるのが通常である。

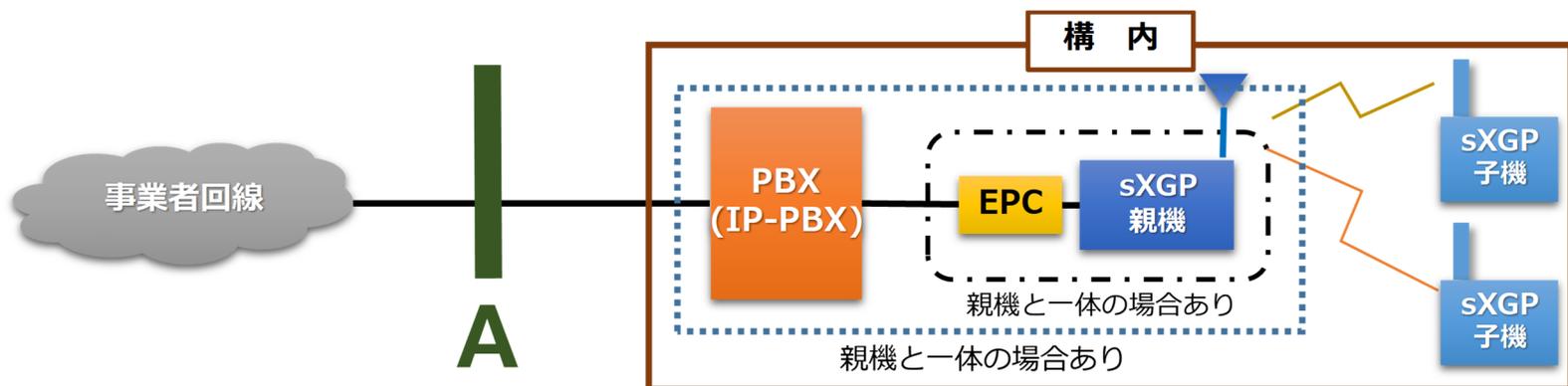


図 3 PHS の後継システムとして導入される場合の sXGP デジタルコードレス電話システムの構成例

- しかしながら、図 4 のように IP-PBX が VPN 接続で構外に設置されている場合など、実際のシステム構築では様々な接続形態が考えられる。
- 一方で、IP-PBX は sXGP デジタルコードレス電話で使用される以前に、既に必要な認定等を受けていることが考えられる。また、認定等を受けていない IP-PBX については、sXGP デジタルコードレス電話システムで使用するか否かにかかわらず認定等が必要である。
- 以上を踏まえ、VPN 回線などを介して接続される sXGP デジタルコードレス電話に関する認定を行う際の責任分界点を図4の B2 にあるものとし、考え方を整理する。責任分界点 B2 は EPC 及び sXGP 親機に接続されるデジタルデータ伝送端末(D 端末)となる。ただし、B2 は sXGP デジタルコードレス電話に関する認定等の考え方の整理のための分界点とし、全ての端末設備の認定等における責任分界点を示すものではない。

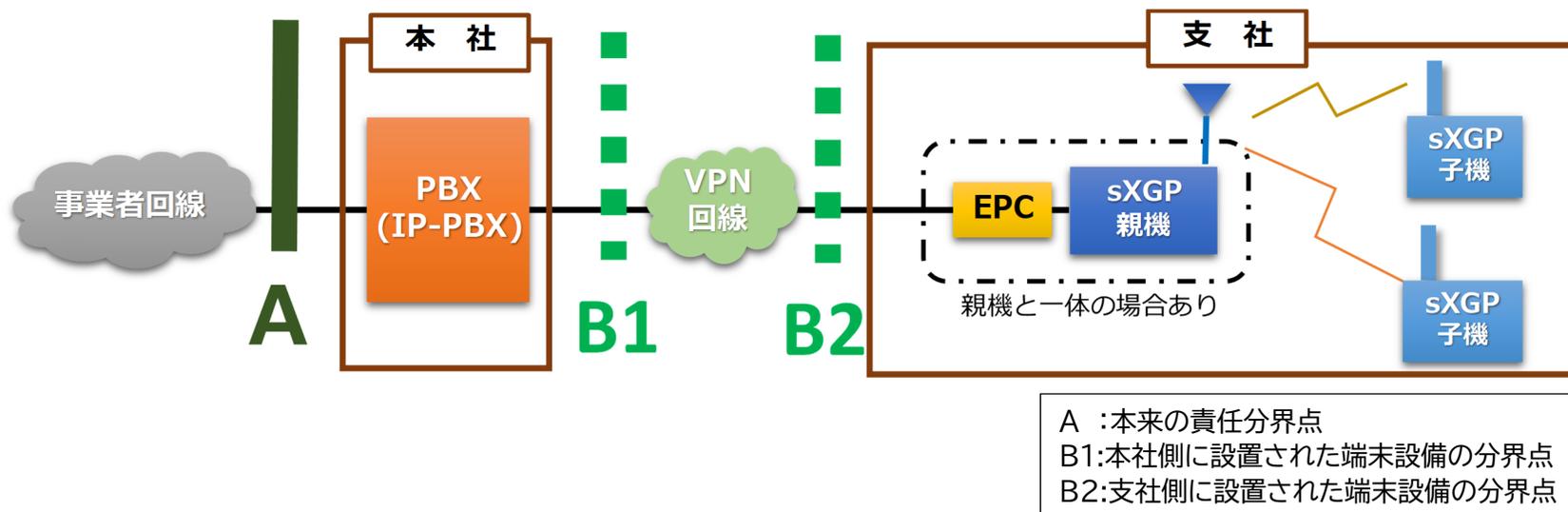


図4 実際の sXGP デジタルコードレス電話システムの構成例

- sXGP デジタルコードレス電話システムについては、前述のとおり様々な構成が考えられる。また、使用される子機も専用端末ではなく、スマートフォンやタブレット端末など、汎用性の高いものが想定される。このことから、親機・子機の多様な組み合わせが生じることとなり、全ての端末を特定して親機・子機一体で認定等することは現実的に困難であると考えられる。
- このことから、sXGP デジタルコードレス電話については、従来どおり親機・子機一体での認定等に加え、親機、EPC、子機それぞれ単体での認定を行うことも可とする。
- 単体で認定する場合の考え方は、次表のとおり。

親機	① 「専用設備又はデータ通信用設備に接続される端末設備」としての認定等（D 認定）が必要。 ② 親機と EPC が一体となっているものについては、EPC の認定等に準ずる。 ③ 端末設備等規則第 9 条に基づく検査が必要。
EPC	「専用設備又はデータ通信用設備に接続される端末設備」としての認定等(D 認定)が必要。
子機	端末設備規則第 9 条に基づく検査が必要。(D 認定)

2. その他

- なお、上記の取扱いについて、総務省が定期的実施する端末機器の市場調査等において不適切な事例等が判明した場合には、適宜見直しが必要である。