別紙2

平 成 31 年 1 月 25 日

総 務 大 臣
石 田　 真 敏 殿

情報通信行政・郵政行政審議会
会 長　 多 賀 谷　 一 照

答　申　書

平成30年10月26日付け諮問第3107号をもって諮問された事案について、審議の結果、下記のとおり答申する。

記

１　本件、端末設備等規則等の一部改正については、諮問のとおり改正することが適当と認められる。

２　なお、提出された意見及びそれに対する当審議会の考え方は、別添のとおりである。

以上

別　添

端末設備等規則等の一部を改正する省令案に寄せられた御意見及び御意見に対する考え方

意見募集期間：平成 30 年 10 月 27 日（土）から 11 月 26 日（月）まで
提出された御意見の件数：５件

意見提出者	代表者氏名等	
一般財団法人日本データ通信協会	理事長	酒井　善則
個人A		
個人B		
個人C		
個人D		

No.	意見提出者	提出された意見	意見に対する考え方	修正の有無
1	一般財団法人日本データ通信協会	今回、端末設備等規則にセキュリティに関する基準が新たに設けられることについては賛成です。 しかしながら、IoT 機器が乗っ取られてサイバー攻撃に悪用され、インターネットに障害を及ぼす事案の発生原因は、パスワードの不適切な設定など IoT 機器のセキュリティ上の脆弱性の悪用であることから、端末機器が今回新たに設けられるセキュリティに関する基準を満足する機能を有していることだけでは不十分であり、利用者がセキュリティ対策の機能を有効にさせることが必要であると考えております。 したがって、今後検討されるガイドラインにおいて、その具体的な対策を盛り込むこととして頂きたい。 　例えば セキュリティに関する知識のない利用者が、業者等他者に依頼してセキュリティ設定を行う場合は、セキュリティに関する知識を有する者（資格者）に依頼すること。 依頼された者がパスワードの設定などセキュリティ対策をした場合は、その設定内容及び資格者名などを記載した書面を利用者に手渡すこと。 など、利用者が安心してインターネットを使用でき、他の利用者に迷惑（踏み台となる）をかけないような具体的でかつ効果のある対策をガイドラインに盛り込むことをお願いしたい。 【理由】 　平成 28 年 7 月策定の「IoT セキュリティガイドライン ver1.0（IoT 推進コンソーシアム、総務省、経済産業省）」において、「端末機器のみにセキュリティ対策をゆだねるのではなく、システム・サービスの構築・接	本改正案に賛成の御意見として承ります。 　なお、本改正案に係る運用について明確化するためのガイドラインについては、総務省において、関係者の意見を考慮しながら検討・策定を進めていくことが適当と考えます。	無

		続・運用・保守時に取り組むべき対策の必要性」が記載されているとともに、「一般利用者のためのルール」として利用者が行うべき対策が盛り込まれており、ネットワークやセキュリティなどの知識のない利用者も安心してセキュリティ対策の実施ができるようにすることが重要であると考えているため。		
2	個人A	「総務省総合通信基盤局電気通信事業部電気通信技術システム課」が提唱している内容では、IoT 機器に接続する「LPWA（ロウパワーワイドエリア）」の事と考えます。具体的には、「3G（第 3 世代）」における「3GPP（W-CDMA 及び GSM）」での「サテライトシステム（通信衛星）」の事と考えます。サイバー対策での IoT 機器におけるセキュリティー対策に関する技術基準の事と考えます。要約すると、プロバイダー側は、「携帯電話事業者（モバイルホーンオペレーター）」及び「ISP（インターネットサービスプロバイダー）」が、提供し管理している「基地局サーバー及び IT サーバー」を、IT クラウドサーバーにおける IT クラウドコンピューティング技術を使う事で、ユーザー側が保有している IoT 機器のセキュリティー対策する事が望ましいです。セキュリティー対策を促す事では、プロバイダー側の責任にすれば良い事です。	近年インターネットにつながる IoT 機器がサイバー攻撃に悪用される事案が増加しており、その原因としてはパスワードの不適切な設定など IoT 機器のセキュリティ上の脆弱性を悪用するケースが多いことが課題となっています。 こうした課題については、電気通信事業者による対応も期待されますが、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）では、電気通信事業者は原則として通信内容を確認できないためその通信内容から通信の正常性を判別できないこと、マルウェアに感染した IoT 機器のみの通信を止めることが技術的に困難であることなど取り得る対応には制約があることも踏まえ、IoT 機器を含む端末設備の技術基準にセキュリティ対策を追加することが適当とされたことを受け、本改正案によりこれを整備するものです。	無
3	個人B	＞端末設備等規則の一部を改正する省令案 本改正に賛成である。 この様な仕様の提示は望ましいものであると考える。	本改正案に賛成の御意見として承ります。	無

		＞電気通信主任技術者規則の一部を改正する省令 本改正に賛成である。 LPWA についての追記は適切なものと思われた。		
4	個人C	近年に開発・出荷されている IoT 機器装置において、技術基準適合証明取得済みの通信モジュールが組み込まれて使用される構造になっているものが多くあります。通信モジュール自体に独自のファームウェア(アクセス制御機能を持ち、そのための ID/パスワードを有する)が存在しており、このモジュールに対して今回のセキュリティ対策に関する技術基準を満足すべきという趣旨は理解します。 通信モジュールが組み込まれた IoT 機器装置全体に目を向けたとき、この装置は一見は通信回線設備に接続されているように見えます。しかし実際には通信モジュール内にアクセス制御機能が存在・動作しており、IoT 機器そのものの OS 上で動作する機能が通信事業者のネットワークに直接晒されることにはなりません。こうしたケースでは、アクセス制御を行う通信モジュールを(一般家庭やオフィス環境における)ルーターと同様の存在と見做すことができます。 「情報通信審議会答申(本年 9 月 12 日)」において「セキュリティ対策が追加された技術基準適合認定等を求める対象範囲は、電気通信回線設備に直接接続される端末機器とし、恒常的に既認定機器を介して接続する機器（例えば、大型白物家電など、屋外に持ち出す等により電気通信事業者の回線設備に直接接続して使用することを全く想定していない機器)については技術基準適合認定等の対象外とすることが適当としており、今後、ガイドラインにおいて明確化する予定。」とされておりました。アクセス制御機能を持つ通信モジュール(モジュールそのものがファームウェア更新の機能を持つ)を内包した構造の装置では、同様に「アクセス制御機能を持つ通信モジュールが、電気通信回線設備に直接接続される端末機器である」と考えても、今回の制度整備の趣旨に反することはないと考えます。	本改正案は、近年インターネットにつながる IoT 機器がサイバー攻撃に悪用される事案が増加しており、その原因としてはパスワードの不適切な設定など IoT 機器のセキュリティ上の脆弱性を悪用するケースが多いことが課題となっていることを背景として、電気通信回線設備に直接接続される端末設備の技術基準に最低限のセキュリティ対策を追加するものです。 なお、本改正案に係る運用について明確化するためのガイドラインについては、具体的な製品に組み込まれて使用される通信モジュールが有する機能の実態等も踏まえ、総務省において、関係者の意見を考慮しながら検討・策定を進めていくことが適当と考えます。	無

		十分なセキュリティ機能を有したモジュールを利用することによって、IoT 機器開発スピードの鈍化が避けられるとすれば大変有用です。こうしたモジュール内蔵型の装置も想定した形で、ガイドラインで技術基準適合認定範囲を明確化していただけないでしょうか。		
5	個人D	社会構造、教育、外国人高度人材等に関する政策の御提案（要約）	本改正案は、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）を受け、IoT 機器を含む端末設備のセキュリティ対策に関する技術基準の整備及び LPWA サービスに係る電気通信主任技術者の選任義務の緩和を行うものです。	無