資料91－２

IPネットワーク設備委員会報告（案）についての意見募集の結果　概要

令　和　７　年　１　１　月　２　７　日
ＩＰネットワーク設備委員会
総　　務　　省

意見募集の概要

1. 意見募集期間：令和7年10月4日（土）～同年11月4日（火）まで
2. 提出意見件数：8件（電気通信事業者1件、法人1件、団体1件、個人5件）
   注：提出意見数は、意見提出者数としています。

<意見提出者>

- 一般社団法人電子情報技術産業協会
- 株式会社ラック
- KDDI株式会社
- 個人

賛同のご意見

本報告案に賛同する。

＜主なご意見＞

- 改正後の端末規則の施行から５年が経過したことで、効果測定を行い技術基準の見直しを行うこと、賛同いたします。
  【一般社団法人電子情報技術産業協会】
- 情報通信審議会IPネットワーク設備委員会において、サイバー攻撃の増加、ランサム攻撃による大規模被害の発生等を踏まえ、端末機器の技術基準等への適合性に係るセキュリティ基準の見直しの検討は、大変時宜を得たものと存じます。【株式会社ラック】
- 今回の報告（案）で示されたとおり、IDパスワードの設定機能等所要な機能に関するセキュリティ強化を図るものの、技術基準という性格上、市場や利用者に与える影響が大きいことから、セキュリティリスクを注視しつつ個別の対応を取るなどの経過措置等を検討いただいており、報告（案）に賛同いたします。【株式会社ラック】
- IoT機器のセキュリティもとても大切なので、レベルを上げることを推進していただきたいと考えています。【個人A】
- 充電ケーブルなどから、外部から操作される危険への対策　自ら信号を送る危機もある　21-22 不要な通信はぜひ遮断していただきたいです。【個人A】

考え方（案）

○　賛同のご意見として承ります。

ID/パスワード設定機能の見直しについて①

変更を強制する対象について。

＜主なご意見＞

・ 変更を強制するのは、パスワードのみとし、IDについては、変更しなくてもよいのではないか？ 【個人B】

考え方(案)

○ 現在の端末設備等規則では、

・当初より端末機器ごとに一意の識別符号(ID/パスワード)が付されていること

又は

・当初より設定されている識別符号(ID/パスワード)の少なくとも1つについて変更を促す機能

を求めております。

今回の検討結果は、後者の場合において、識別符号(ID/パスワード)の少なくとも1つについて変更を「させる」機能を求めることが適当であるとの趣旨であり、ご意見のように、パスワードのみ変更をさせ、IDの変更はしないケースも許容されるものとなっております。

その上で、3.1.3の2行目中、【パスワードの変更を】は【ID/パスワードの少なくとも1つの変更を】に修正いたします。

【修正箇所（赤字部分の追記）】
委員会報告P.18「3.1.3 検討結果」

現状及び課題を踏まえ、現行規定の「②当初より設定されているID/パスワードの変更をユーザに促す機能」については、ID/パスワードの少なくとも１つの変更を「促す」ことを求める機能ではなく、変更を「させる」ことを求める機能へ見直すことが適当である。

ID/パスワード設定機能の見直しについて②

パスワード管理に関するノウハウの活用について。

＜主なご意見＞

・ 無線LANルータ等では、出荷時にランダムなパスワードを設定する運用が一般化しております。これは本報告で懸念されている脆弱性対策として有効な手法であり、今後の技術基準策定において積極的に取り入れていただくことを要望いたします。【個人C】

考え方（案）

○ ご提示いただいた具体的な手法等については、その内容を検討の上、「電気通信事業法に基づく端末機器の基準認証ガイドライン」へ反映することが適当であると考えます。

＜主なご意見＞

・ 企業系のIoT機器の場合、複数人でアカウントを共有することが一般的な運用です。複雑なパスワードを必須とすると、覚えることができずメモを共有するなどの運用をしてしまい結果的にセキュリティレベルが低くなることが想定されます。総当たり攻撃のリスクヘッジには、連続loginに対するloginプロンプトを遅くしたりlockをしたりなどの手法が効果的と考えられ、パスワードの複雑性はある程度緩和し、login施行の繰り返しの制限をいれるほうがバランスとしてはよくなるのではないかと考えます。【個人D】

考え方（案）

○ ID/パスワードに関する規定の見直しについては、第三者から容易に推測されないものとすべき趣旨を規定することが適当としつつ、「ID/パスワードの文字数や入力規則等のルールについては、省令・告示で規定することにより内容の硬直化・陳腐化を招くおそれがあることから、JC-STARにおける適合基準も参考としつつ、セキュリティ対策の変遷に柔軟に対応できるよう、端末ガイドラインにて提示することが適当」としております。また、ご提示いただいた具体的な手法等については、その内容を検討の上、「電気通信事業法に基づく端末機器の基準認証ガイドライン」へ反映することが適当であると考えます。

ID/パスワード設定機能の見直しについて③

新たな認証技術への対応について。

＜主なご意見＞

・ 近年、パスキー(FIDO2等)をはじめとする、ID/パスワードに依存しない多くの認証方式が普及しつつあります。端末ガイドラインにおいては、特定の認証方式に限定することなく、「十分なセキュリティ強度を持つ認証手段を実装すること」といった、より広範な要件として記述していただくことで、将来的な技術革新にも柔軟に対応できる枠組みとしていただくことをご考慮いただきたく、お願い申し上げます。【一般社団法人電子情報技術産業協会】

考え方(案)

○ ご意見のとおり、セキュリティ対策としてID/パスワードに依存しない認証方式の普及が進んでおります。現行の技術基準(端末設備等規則)では、アクセス制御機能及びアクセス制御機能に用いるID/パスワード等の識別符号に関する規定があります。当該規定では、規定に明示された措置のほか、「これに準ずる措置」を講ずることが認められていることから、現時点においても将来的な技術革新にも柔軟に対応できる枠組みになっていると考えます。

ID/パスワード設定機能の見直しについて④

国際整合性の確保について。

＜主なご意見＞

・ グローバルな市場において製品を展開する事業者にとって、各国・地域で異なる独自要件への対応は大きな負担となります。端末認証ガイドラインの策定にあたっては、サイバーセキュリティに関連する国際的な標準化の動向や、欧州サイバーレジリエンス法等の主要国の規制動向を参考にしていただき、可能な限り国際的に整合性のとれた内容としていただくことをお願い申し上げます。【一般社団法人電子情報技術産業協会】

考え方（案）

○ 今回の検討において、欧州のサイバーレジリエンス法並びにETSIの「EN 303 645」で規定されている内容を参考にしております。今後も、検討に当たっては国際的に整合性の取れた内容としていくことが適当であると考えます。

「電気通信事業法に基づく端末機器の基準認証ガイドライン」の定期的な見直しについて。

＜主なご意見＞

・ セキュリティ技術は急速に進化するため、端末認証ガイドラインについても、定期的な見直しの機会を設けていただくことをご検討いただけますと幸いです。【一般社団法人電子情報技術産業協会】

考え方（案）

○ ご意見のとおり、セキュリティ対策のための技術は、日々進化しており、これらの技術との整合性の観点から、「電気通信事業法に基づく端末機器の基準認証ガイドライン」の定期的な見直しを行うことが適当であると考えます。

ファームウェア更新機能の見直しについて①

ファームウェアの自動更新について。

＜主なご意見＞

・ ファームウェアのアップデートにより不具合が起こり、まともに使えなくなる経験もしております。p.20-21にもありますが、ネットを使わなくてよい機材については使わない選択、ファームウェアにより不具合が起こらないか確認してから手動でアップデートできるようにもしていただきたいと強く願います。 【個人A】

考え方（案）

○ ファームウェアのアップデートについては、いただいたご意見のような懸念が存在することから、「アップデート前のソフトウェアの完全性の確認機能」の具備を求めることが適当としています。また、効果的なセキュリティ対策となるためには、更新の徹底が必要であることを踏まえつつ、自動更新については、「推奨するが要件としない」としています。なお、「ネットを使わなくてよい機材」について、電気通信回線設備に接続しない機器については、今般の検討対象とはなっておりません。

＜主なご意見＞

・ 自動更新について、無線を利用する端末設備が弱電界となる場所に設置されている場合等、設置環境によってはユーザーが更新の自動化を希望した場合でも、ファームウェアの更新が失敗するケースが考えられます。従って、今後、自動更新を必須要件とする場合には、そのような場合を考慮した要件であることが適当と考えます。 【KDDI株式会社】

考え方（案）

○ 頂いたご意見については、今後の参考とさせていただきます。

ファームウェア更新機能の見直しについて②

機能の実現方法(手段)について。

<主なご意見>

- "「最新のソフトウェアがインストールされていることを確認する手段」及び「アップデート前のソフトウェアの完全性の確認機能」の具備" とあるが、「確認手段はWeb等でユーザが確認する手段があればよい」を希望します。

理由: (1) すべての機器がインタラクティブなインタフェースを持っているとは限らない。

(2) 装置を操作する人が確認するとは限らない。

【個人D】

考え方(案)

○ 機能を具備する手段については、端末機器に対して実装する方法のほか、ご意見のようなWeb等によりユーザが確認できるようにする方法も考えられます。

不要なインタフェースへの物理/論理アクセスに関する機能について

対象の明確化について。

<主なご意見>

・ IoT機器はIP通信のみならず、LPWA等の多様なプロトコルで稼働しております。報告書ではtelnet利用の脆弱性が例示されておりますが、対象とする無線通信・ネットワーク通信規格の範囲が不明確でございます。今後の制度設計においては、対象とする通信規格を明確化し、現場の混乱を防ぐための指針を示していただきますようお願い申し上げます。【個人C】

考え方(案)

○ 「対象とする無線通信・ネットワーク通信規格の範囲」については、当委員会での議論でも「論理的インタフェースはマルウェア侵入等に使われる代表的なポートを予め明示」すべきといったご意見をいただいており、今後の制度設計においては、無効化するインタフェースおよびその確認方法等について明確化することが適当と考えます。

その他①

本報告での検討対象について。

＜主なご意見＞

・ 本報告書では「セキュリティ問題」と広く記載されておりますが、実際に課題とすべきはIoT機器の乗っ取りや踏み台化によるサイバー攻撃の防止であると認識しております。現状の記述では、具体的な脅威や対策対象が不明瞭であり、政策目的の明確化が望まれます。今後は、乗っ取り・踏み台化等の具体的なリスクを明示し、対策の優先順位を明確化いただきたく存じます。 【個人C】

考え方（案）

○ 今回の検討は、平成29年に問題となっていた「Webカメラやルータ等のIoT機器が乗っ取られ、DDoS攻撃等の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ような事案が増加していた」（委員会報告（案）1.2）ことに対する検討結果（技術基準の策定）の「妥当性の検証を行い、より実効性のある内容を強制規格として規定すべきかどうかを行うことを目的としている。」（委員会報告（案）第3章）ものとなります。このため、ご認識いただいている、「IoT機器の乗っ取りや踏み台化によるサイバー攻撃の防止」を課題としていることは明示しているため、案の記載のままとさせていただきます。

＜主なご意見＞

・ ネットを切っても家電は使えるようにして欲しい　車など乗っ取られると命に関わる機器はネットに繋がない選択ができるように強く望みます 【個人A】

考え方（案）

○ 頂いたご意見については、今後の参考とさせていただきます。

その他②

今後の制度設計に当たっての留意点について。

＜主なご意見＞

・ 新たな技術基準の導入は、IoT機器開発事業者へのコスト転嫁となる懸念がございます。特に中小企業や海外製品に対しては、国際競争力の低下や国内市場のガラパゴス化を招く恐れがございます。制度設計にあたりましては、政府・省庁による支援策や国際標準との整合性確保を強くご検討いただきたく存じます。【個人C】

考え方(案)

○ 今回の検討において、欧州のサイバーレジリエンス法並びにETSIの「EN 303 645」で規定されている内容を参考にしております。制度設計に当たっては国際的に整合性の取れた内容としていくことが適当であると考えます。また、各機能に対して具体的に求める基準等については、経済産業省とIPAにおいて策定された任意規格において定めている個々の適合基準と大きく乖離しない方向で見直しを行うことが適当であると考えます。

セキュリティ体制の構築について。

＜主なご意見＞

・ SPI（Stateful Packet Inspection）を用いたフィルタリングがIoT機器、ルータ・スイッチ、電気通信事業者、サーバ事業者等の各所で適用出来る・概ね標準的に適用されているような体制を国全体で構築するようにされたい。【個人E（意見要旨）】

考え方(案)

○ 頂いたご意見については、今後の参考とさせていただきます。