資料 91－１

「情報通信審議会 情報通信技術分科会 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

意見募集期間：令和７年 10 月４日（土）～令和７年 11 月４日（火）
提出されたご意見の件数：８件

※提出意見数は、意見提出者数としています。

No.	意見提出者（提出順）
1	個人
2	個人
3	個人
4	一般社団法人電子情報技術産業協会
5	株式会社ラック
6	個人
7	KDDI 株式会社
8	個人

「情報通信審議会 情報通信技術分科会 IP ネットワーク設備委員会 報告（案）」に対して寄せられた意見及びそれに対する考え方（案）

意見 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
1	第３章 3.1	3.1 について、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？	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。	有
2		平素より我が国の情報通信分野の安全・		

		信頼性向上にご尽力いただき、誠にありがとうございます。 「IP ネットワーク設備委員会 報告（案)」に関し、下記の通り意見を申し述べます。		
	全般	1. セキュリティ問題の主語について 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。	1. について 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。	無
	第３章	2. 対象とする通信規格の範囲について 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	2. について いただきましたご意見は、「3.3　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」に対するものと承りました。	無

		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。	いただきました、「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	3. IoT 機器開発に関わる金銭的負担について 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。	3. について 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。	無
	第３章	4. パスワード管理に関するノウハウの活用について 無線 LAN ルータ等では、出荷時にランダム	4. について ご意見にある出荷時にランダムなパスワードを設定することは、現行の端末設備等	無

		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。	規則において、ID/パスワードに求める「端末の機器ごとに異なるものが付されている」ための手法の１つであると考えられます。 　このため、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」へ反映させることが適当と考えます。	
3	全般	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。	賛同のご意見として承ります。	無
	第３章	一方で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。	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。	無
	第３章	充電ケーブルなどから、外部から操作され	不要なインタフェースへの物理/論理ア	無

		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。	クセスについて、製造者が提供する意図を持つ通信機能以外についてあらかじめ無効化しておくことを技術基準として規定することに賛同のご意見として承ります。	
	その他	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	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。	無
4	全般	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。	賛同のご意見として承ります。	無
	第３章 (3.1.3)	第三者から容易に推測されないための ID/パスワードの文字数や入力規則等のルールについて、省令・告示で規定せず、「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」（以下「端末認証ガイドライン」）に反映することで、セキュリティ対策の変遷に柔軟に対応するという方針に賛同します。 一方で、以下の点につきまして、ご検討いただけますと幸いです。	賛同のご意見として承ります。また、いただいたご意見に関しては、以下のとおりと考えます。	
		1. 国際整合性の確保について グローバルな市場において製品を展開する	1.に関して： 今回の検討において、欧州のサイバーレ	無

		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。	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。	
		2. 新たな認証技術への対応について 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。	2.に関して： 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。	無
		3. ガイドラインの定期的な見直しについて セキュリティ技術は急速に進化するため、	3.に関して： 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	無

		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。	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。	
	第３章 (3.1.3)	第三者から容易に推測されないための 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・告示で規定せず、セキュリティ対策の変遷に柔軟に対応できるよう、端末認証ガイドラインに反映することに賛同します。	賛同のご意見として承ります。	無
	第３章 (3.2.3)	ファームウェアには、セキュリティ機能のほかに、通信機能、アプリケーション機能等複数の機能があります。製品の使用環境によってはアプリケーションの機能更新は禁止されている場合もあります。一律に最新版のファームウェアを適用することは難しいため、推奨規定として頂くことに賛同します。	賛同のご意見として承ります。	無
	第３章 (3.2.3)	不正なファームウェアを誤って更新しないために、ファームウェアの完全性をアップデート前に確認できる仕組みを規定化することに賛同します。	賛同のご意見として承ります。	無
	第３章	セキュリティ向上のために製造者が提供を	賛同のご意見として承ります。	無

	(3.3.3)	意図しないインタフェースの無効化に賛同します。 製造業者・登録認定機関双方の認識相違を防ぐため、認証審査時に、インタフェース無効化していることを宣言する方法や、審査規程で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頂くことで、より確実なインタフェース無効化を図ることを希望します。		
	第３章 (3.4)	書面審査対応に賛同します。 社内検査を活用できる書面審査により、審査時間の短縮につながると考えます。	賛同のご意見として承ります。	無
	第４章	強制規制は今まで通り、電気通信回線網と直接接続する機器を規制対象とすることに賛同します。 JC-STAR のような任意規格で間接接続する機器をカバーすることで、より安全な通信環境が構築できると考えています。	賛同のご意見として承ります。	無
	第５章	従来と同様の経過措置を設定頂くことに賛同します。 経過措置を受けない場合、機器購入者が購入時点の意図とは異なる形で電気通信事業者から接続を拒まれる可能性が出てしまい、不利益を与えてしまう可能性がありま	賛同のご意見として承ります。	無

		す。 周知活動についても賛同します。周知活動によって買替等の効果がありますので、地道な取組にはなりますが、周知活動、キャンペーンを行って置き換えの推進を行うのが良いと考えます。		
	第６章	世界的な動向、JC-STAR 等の国内各種セキュリティ制度との整合を取りながら、情報通信ネットワークの安全・信頼性を確保する取り組みに賛同します。	賛同のご意見として承ります。	無
5	全般	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。 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。 各種のサイバーセキュリティ事業に取り組むとともに、情報リテラシーの向上に取り	賛同のご意見として承ります。	無

		組んでいる弊社としましても、報告（案）を踏まえ、IoT 機器の安全性向上に努めてまいります。		
6	第３章 (3.1.3)	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。	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。	無
	第３章 (3.2.3)	″「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	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。	無

		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。		
7	第３章 (3.2.3)	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。	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。	無
8	全般	・意見要旨 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。 ・意見 SPI（Stateful Packet Inspection）を用いたフィルタリングについて、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ように、電気通信事業者・ネットワーク機器事業者・OS及びソフトウェアの各開発者・事業者に	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。	無

		おいて実装していくべきではないかと考える。 SPI は TCP プロトコルによる通信を用いる限り、相当に有効なセキュリティ技術ではないかと考えるのであるが、有効である事に加えて、色々な所で用いれる事も特徴である（スイッチ等で透過的に用いる事も可能であろう。）。 注意点として、幾つかのサービスが利用出来なくなる可能性がある事や（サービスで使用する通信による。）、ネットワークの遅延によっての影響が発生しがちになる事が挙げられるが、それを除いては SPI を用いたフィルタリングはかなりあてになる（未知の危機を含む）セキュリティ危機への対応方法であり、ローカル的なネットワークにおけるウイルス等の蔓延やネットワーク経由の攻撃を防ぐための手段となるものであろう。 電気通信事業者・サーバ事業者・ネットワーク機器事業者などは、電気通信回線利用者、ISP・VNE サービスの利用者（ISP・VNE 事業者を介してインターネットとの通信を行う際に SPI を用いたフィルタリングが可能であろう。）、レンタルサーバ・IaaS 利用者などに、簡単な操作・設定で用いれるような SIP を用いたフィルタリング方法を提		

		供し（もちろん、その無効化や例外の設定なども行えるべきであろう。）、それを標準で有効なの設定として提供する事で（既存の利用者については強制的な適用をしなくてもよいと考えるが。）、少なくとも新規の利用者については、ネットワーク経由での攻撃の危機を相当防御出来るようになるのではないかと思われるが、どこもここもがSPI を用いたフィルタリングで防御されていると、ネットワーク・インターネットの危機は大きく減ずるのではないかと考える。（サーバを設置する者は、ネットワークに関する知識を知っているべきはずであるし、また SPI を用いたフィルタリングについても知らないのであればサービス提供を行うべきではないと考えるのであるが、そのような者はネットワークに関する知識を十分に持ちつつ SPI を用いたフィルタリングにサービス提供に必要な例外を設定する事で問題の発生が無いように出来ると思われるし、ネットワーク通信を用いるアプリケーションについても、クライアント側から開始するプロトコル（チャネルを作成するもの含む）を用いる事で、通常、問題の発生が無いように出来るのではないかと思われる。） SPI を用いたフィルタリングは、おそら		

		く、技術的に容易かつ依然として有用・有効なものではないかと思われるが、これは合理的・効率的に、ネットワーク・インターネットにおいてのウイルス等によっての問題を減らす効果があるものと考える。 日本国は、合理的・効率的に、ネットワーク・インターネットに関しての安全性を向上させるため、SPI を用いたフィルタリングがほぼどこででも適用されているような状態を構築するようにされたい。日本政府はそのような施策を行うようにされたい。		