（別紙２）

# 「円滑なインターネット利用環境の確保に関する検討会 対応の方向性（案）」に対する意見募集で寄せられた御意見に対する考え方

２０１８年２月

# 「円滑なインターネット利用環境の確保に関する検討会　対応の方向性（案）」に対する意見募集で寄せられた御意見

○　意見募集期間：2017年12月27日（水）～ 2018年1月18日（木）

○　意見提出数：10件

※意見提出数は、意見提出者数としています。

| 受付順 | 意見提出者 |
|---|---|
| 1 | 一般財団法人日本データ通信協会 |
| 2 | ダイキン工業株式会社 |
| 3 | 一般社団法人デジタルライフ推進協会 |
| 4 | アルテリア・ネットワークス株式会社 |
| 5 | 凸版印刷株式会社 |
| 6 | 一般社団法人日本電気工業会スマートホーム委員会 |
| 7 | 一般社団法人日本ケーブルテレビ連盟 |
| 8 | 一般社団法人電子情報技術産業協会 |
| 9 | ＫＤＤＩ株式会社 |
| １０ | 一般社団法人ビジネス機械・情報システム産業協会 |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| １：政府における今後の取組の在り方等に関する御意見 | |
| 意見１<br>サイバー攻撃に関しては、政府、各府省庁及び協議会等の様々な組織において検討が行われている。関係者において適切に情報共有や検討の一元化を行うとともに、政府全体として横断的に対策を実施していくことが必要。 | |
| パブコメでは、「IoT 機器のセキュリティ対策はこれまで民間企業の独自の取組みに依存してきた」（P14）の記述の他、「今後有効な対策を講じていくためには、関係者間で必要な情報を共有し、相互に連携していくことが必要」（P4）、「国民のセキュリティ意識のさらなる向上を図ることも必要」（P5）との記載があります。このように幅広い対応を行うためには、総務省や通信事業者だけでなく、関係省庁及び事業者全体での情報共有と意見収集の体制が必要と考えますので、重ねてご配慮の程、お願い申し上げます。<br>【一般社団法人日本電機工業会スマートホーム委員会】 | 政府では、サイバーセキュリティ戦略本部において、各府省庁の施策の総合調整等を行うとともに、関係府省庁において、民間の協議会等の関係者とも連携しながら具体的な施策を検討、実施しています。今後とも関係府省庁や民間の協議会等と適切に情報共有を行いながら施策の検討、実施をしていくことが重要と考えます。 |
| 「円滑なインターネット利用環境の確保に関する検討会対応の方向性(案)」につきまして、賛同いたしますとともに、これをお纏め頂いた主査・構成員の皆様に、敬意を表する次第です。<br>ケーブルテレビは、地域に根差したメディアとして、災害情報、地域情報、コミュニティチャンネル(自主放送)を提供するとともに、地上波、ＢＳ、ＣＳ多チャンネル放送などの他地域からの放送コンテンツを提供しています。さらに、インターネット、電話サービスなどを提供することによって、地域内の情報流通をより円滑に行えるようにする役割も担っています。<br>ケーブルテレビ業界のインターネットサービスの提供世帯数は 2017 年 3 月末時点で約 870 万世帯となっており、地域密着のプロバイダとして加入者も増加を続けています。また、IoT の導入に取り組むケーブル局が増えており、家の見守りや家電機器のコントロールなど多様なライフスタイルに合わせた生活総合サポートサービスの充実も図られようとしています。<br>このような状況の下、IoT 機器等を踏み台とした DDoS 攻撃等によるインターネットの障害を回避し、円滑なインターネット利用環境を確保するために、通信ネットワークに係るもの全体が連携して対応をすすめていく本方向性(案)に期待するとともに、ケーブル業界としても協力してまいります。<br>なお、サイバー攻撃対策については、国、省庁、協議会など複数の組織で検討が行われていますので、同様な取組みは可能な限り一元化することや、本方向性の全体に対する位置づけの明確化をあわせてお願い致します。<br>【一般社団法人日本ケーブルテレビ連盟】 | |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| （セキュリティ対策検討の一本化について）<br>総務省において、2017 年 10 月 3 日付にて公表された「IoT セキュリティ総合対策」は、“IoT システムのセキュリティ対策に際しては、部分最適ではなく、システム全体を俯瞰した全体最適を実現する観点から総合的な対策を講じていく必要があり、IoT システムのセキュリティ対策の総合的な推進に向けて取り組むべき課題について整理されたもの”という主旨で纏められている。また“対策の推進に際しては、NISC や経済産業省をはじめ、関係する府省庁との連携の下に進めていく必要がある”とも述べられている。また、経済産業省においても、2017 年 12 月 27 日に、我が国の産業界が直面するセキュリティの課題を洗い出し、関連政策を推進していくため、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される「産業サイバーセキュリティ研究会」を設置され第 1 回会合が開催されている。<br>http://www.meti.go.jp/press/2017/12/20171226004/20171226004.html<br>IoT 機器は、センサーから家電、自動車、インフラ設備まで様々なものがあり、機器の特性や利用環境により異なるリスクが存在し、機器を狙った攻撃についても、DDoS 攻撃だけではなく、様々な脅威が存在する。DDoS 攻撃に限っても、「Mirai」の亜種など次々に新たな脅威が出現している状況である。対策の推進にあたっては、様々な脅威を踏まえた上で行う必要がある。また、IoT 機器の対策も単体で考えるだけではなくシステム全体でセキュリティを確保できるような対策の在り方を検討すべきではないか。併せて、政府調達含む機器・システム調達時のセキュリティ対策の要件化や攻撃発生時の責任分界等、セキュリティ対策を実装した機器・システムが広く普及し、正しく運用されるフレームワークの検討も、我が国の経済社会の活力の向上、国際競争力の確保の観点からも必要ではないか。<br>以上のことから、ネットワークを基盤とする ICT システムのセキュリティ対策は、省庁の所掌を跨がった対応が必須である。例えば近い将来自動車も IoT 機器となることが想定され、総務省、経済産業省だけでなく国土交通省、警察庁等も関係する。ICT システムのセキュリティについては現在の省庁の所掌を横断する対応が求められる。<br>重要インフラと一般家庭内のセキュリティ対策のレベル感等、様々な角度での検討や国、企業、団体、一般の方々等各主体が果たすべき役割もあると考える。<br>総務省や経済産業省等、関係府省庁で連携頂き、政府として一本化してセキュリティ対策を検討していただきたい。<br>【一般社団法人電子情報技術産業協会】 | |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 「通信ネットワークを含めた IoT セキュリティを確保するための活動としては IoT 推進コンソーシアムの IoT セキュリティワーキンググループの中で検討されること、検討会での検討はこうした IoT コンソーシアムでのセキュリティ対応の一環として位置づけられ、全体として調整が取られること」を明記いただきたい。<br><br>（理由）<br>「インターネット上の脅威」に対する対策として、「電気通信事業者が提供する回線設備の安定稼働」を図るという、限られた領域の中での可用性の確保だけでは不十分であることは明らかであり、IoT セキュリティ全体としての、機密性、完全性を含めた対策は、この検討会とは別に行われることを明記し、全体の IoT セキュリティの推進と本検討会の関係を明確にすることにより、IoT セキュリティ対策全体の中での本検討会の位置づけを明らかにしていただきたい。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| ２：全体に関する御意見／語句の修正に関する御意見 | |
| 意見２－１<br>インターネット障害が世に与える影響の大きさ、昨今の脅威の深刻さから「対応の方向性（案）」の施策は概ね妥当なものと考える。 | |
| インターネット障害が世に与える影響の大きさ、昨今のセキュリティ上の脅威の深刻さから「対応の方向性（案）」の施策は概ね妥当なものと考える。<br>【アルテリア・ネットワークス株式会社】 | 対応の方向性（案）に賛成の御意見として承ります。 |
| 意見２－２<br>サイバー攻撃に対しては、関係者全体での取組が重要。国民のセキュリティ意識向上のための施策も推進すべきである。 | |
| サイバー攻撃に対しては、利用者・メーカー・通信事業者等の全体での取り組みが重要であり、国民のセキュリティ意識向上のための施策も推進していくべきと考えます。<br>【ＫＤＤＩ株式会社】 | 対応の方向性（案）４、５頁において、通信ネットワークに関わる者全体での取組の重要性と国民のセキュリティ意識向上の必要性を記述しているところと同旨であり、対応の方向性（案）に賛成の御意見として承ります。 |
| 意見２－３<br>本検討会の審議内容について、今後さらに情報提供を進めてもらいたい。 | |
| 今回のパブコメには「通信ネットワークを保護するためには、電気通信事業者のみならず、端末設備の製造者、セキュリティベンダ、利用者等の通信ネットワークに関わる者全体が連携しながら対応を進めていくことが極めて重要である」（P4）と記載されております。当会としましても今回設立された検討会の審議内容について、当初から高い関心を持っておりますが、検討内容の情報公開は上部の検討会やパブコメに限られております。今後は、一層の情報提供についてご配慮をお願いいたします。<br>【一般社団法人日本電機工業会スマートホーム委員会】 | 本検討会においては、具体的なサイバー攻撃の手法や各事業者における対策手法等を公開することによりサイバー攻撃が誘発されることを防止する等の観点から、一部資料及びWGの会議自体は非公開としていますが、事後的に公開が可能と判断できた資料や議事概要についてはいずれも公表しており、今後も公開が可能な情報については提供を行っていきます。 |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 意見２－４<br>「企業におけるセンサー機器」との語句を「企業における設備機器や、一般家庭のエアコンや洗濯機等の白物家電」と修正されたい。 | |
| 【１．検討の背景】第三段落<br>「企業におけるセンサー機器のように」を「企業における設備機器や、一般家庭のエアコンや洗濯機等の白物家電のように」に修正されたい。<br><br>（理由）<br>企業におけるセンサー機器とは何を指すのか明確でない。また、一般家庭への IoT 機器の普及も無視できない。<br>寿命の長い機器の例として、より具体的イメージが掴みやすいように記載することで、これらの機器を提供する事業者の取組がより進むことを期待した提案。<br>【ダイキン工業株式会社】 | 御指摘の趣旨を踏まえ、「企業における設備機器や一般家庭における家電製品」と修正します。 |
| 意見２－５<br>「通信ネットワークを保護する」を「通信ネットワークの安定稼働を確保する」と修正し、「インターネットの障害に関する規定」を「電気通信事業者の回線設備の安定稼働を守るための技術基準」に修正するなど、いわゆるサイバーセキュリティの対応ではないことを明示すべき。 | |
| 【２．基本的な考え方】第一段落<br>「通信ネットワークを保護する」を「通信ネットワークの安定稼働を確保する」に変更いただきたい。<br><br>（理由）<br>円滑なインターネットの利用環境を保護するために、電気通信事業者の通信ネットワークを保護することの趣旨について、先日貴局とのヒアリングの中で「電気通信事業者が提供する回線設備が安定稼働することを確保すること」でありいわゆるサイバーセキュリティ対策の議論との混同を避けたいとご説明いただいた。通常、「通信ネットワークを保護する」と記載されている場合、物理的な損傷から通信ネットワークを守ることの他に、データを転送する機能が維持されることが含まれ、その場合にデータが完全性を保ち転送されることや、外部から覗かれたり傍受されたりしないという機密性が確保されていることも前提として考えるのが通常である。<br>「セキュリティ」との混同を避けるためにも、本検討会での検討範囲を「電気通信事業者が提供する回線設備が安定稼働すること」に限定し、いわゆるサイバーセキュリティの対応とは一線を画すことを要望する。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | 本検討会は、円滑なインターネット利用環境の確保に向けて、いわゆるサイバー攻撃のうち通信ネットワークに障害を与えるようなものへの対策を検討対象としており、電気通信事業者が提供する回線設備の安定稼働のみに限定して検討したものではないことから、原案のとおりとします。 |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 【５．IoT 機器を含む脆弱な端末設備への対策（２）今後の対応の方向性】第一段落<br>「サイバー攻撃等によるインターネットの障害に関する規定」を「インターネット上の脅威から電気通信事業者の回線設備の安定稼働を守るための技術基準」に変更していただきたい。<br><br>（理由）<br>通常、端末設備に関して「サイバー攻撃等によるインターネットの障害」という用語が使用される場合、そこで守られるべき機能は「デバイスやサービスが継続稼働すること」（可用性）の他に、デバイスやサービスで扱われるデータの保護、例えばネットワーク通信回線が乗っ取られないことや、他人からのぞかれないこと等（機密性、完全性）も含んで考えることが一般的である。したがい、こうした機能の保護を想起させる用語を使用することは、不要な誤解や混乱を生じさせることとなるため、「インターネット上の脅威から電気通信事業者の回線設備の安定稼働を守るための技術基準」と明記し、いわゆるサイバーセキュリティの対応ではないことを明確にされることを要望する。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | |
| 意見２－６<br>「セキュリティ対策」という用語を「電気通信事業者が提供する回線設備の安定稼働に必要な防御対策」に変更いただきたい。 | |
| 【２．基本的な考え方】第二段落、第五段落<br><br>「セキュリティ対策」という用語を「電気通信事業者が提供する回線設備の安定稼働に必要な防御対策」に変更いただきたい。<br><br>（理由）<br>一般に、IoT 機器等の「セキュリティ対策」という用語がインターネット上の脅威との関係で使用される場合、そこで守られるべき機能は「デバイスやサービスが継続稼働すること」（可用性）の他に、デバイスやサービスで扱われるデータの保護、例えばネットワーク通信回線が乗っ取られないことや、他人からのぞかれないこと等（機密性、完全性）も含むと考えることが一般的である。したがい、こうした機能の保護を想起させる「セキュリティ」等の用語を使用することは、不要な誤解や混乱を生じさせることとなるため、「電気通信事業者が提供する回線設備が安定稼働するための防御対策を講じる」と明記し、いわゆるサイバーセキュリティの対応ではないことを明確にされることを要望する。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | 本検討会は、円滑なインターネット利用環境の確保に向けて、いわゆるサイバー攻撃のうち通信ネットワークに障害を与えるようなものへの対策を検討対象としており、その中には IoT 機器を含む脆弱な端末設備の乗っ取りを抑止するためのセキュリティ対策も含まれ、御指摘の可用性に限定して検討したものではないことから、原案のとおりとします。 |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 意見２－７<br>「サイバー攻撃等によるインターネットの障害に関する規定」を「インターネット上の脅威から電気通信事業者の回線設備の安定稼働を守るための技術基準」に変更していただきたい。 | |
| 【５．IoT 機器を含む脆弱な端末設備への対策（２）今後の対応の方向性】　第一段落<br><br>「サイバー攻撃等によるインターネットの障害に関する規定」を「インターネット上の脅威から電気通信事業者の回線設備の安定稼働を守るための技術基準」に変更していただきたい。<br><br>（理由）<br>通常、端末設備に関して「サイバー攻撃等によるインターネットの障害」という用語が使用される場合、そこで守られるべき機能は「デバイスやサービスが継続稼働すること」（可用性）の他に、デバイスやサービスで扱われるデータの保護、例えばネットワーク通信回線が乗っ取られないことや、他人からのぞかれないこと等（機密性、完全性）も含んで考えることが一般的である。したがい、こうした機能の保護を想起させる用語を使用することは、不要な誤解や混乱を生じさせることとなるため、「インターネット上の脅威から電気通信事業者の回線設備の安定稼働を守るための技術基準」と明記し、いわゆるサイバーセキュリティの対応ではないことを明確にされることを要望する。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | 御指摘の箇所は、事実関係を記述したものであるため、原案のとおりとします。 |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| ３：　「３．電気通信事業者の取り得るDDoS攻撃等への防止措置」に関する御意見 | |
| 意見３－１<br>電気通信事業者の取り得るDDoS攻撃等への防止措置の検討、実施にあたっては、電気通信事業者に対して過度な負担とならないようにすべきであり、政府においても予算措置やセキュリティ技術者の育成等の施策を併せて講じるべきである。 | |
| マルウェアの通信を検出、対策へつなげることは予防処置として高い効果が期待できると考える。しかしながら、実施においては通信事業者における設備面／運用面等への負荷が非常に大きくなる恐れがある。検出方法や効果を十分に検証したうえで、事業者に対して過度な負担とならないことが必要と考える。<br>【アルテリア・ネットワークス株式会社】 | 今後の政府施策や民間団体等における検討において事業者負担に留意すべき旨の御意見として承ります。<br>御意見については、今後政府や民間において種々の検討を行う際に、参考とすることが適切と考えます。 |
| ケーブルテレビ事業者の規模は大手から中小まで様々であり、とりわけ中小事業者が過半を占めております((一社)日本ケーブルテレビ連盟の正会員事業者373社のうち、総接続世帯数の規模が1万未満が約4割(162社)、1～5万未満が約3割(114社))。<br>DDoS攻撃等を実施している端末やC&Cサーバと通信をしている端末等の検知、C&Cサーバ等の検知などの対策には賛同いたしますが、その検知にはトラフィックのモニタリングを行う高価なネットワーク機器やセキュリティの知見が必要と思われ、これらの対応を事業者一律に求められるのはかなりの負担となります。このため、対策実施の検討にあたり、端末やC&Cサーバの検知を行う事業者は一定の規模以上の事業者、対応する事業者には予算措置を行う、セキュリティ技術者の育成施策の実施等の配慮をお願い致します。また、攻撃元が海外である場合も多く、その際の対処の方向性も検討いただくようお願い致します。<br>【一般社団法人日本ケーブルテレビ連盟】 | |
| 意見３－２<br>電気通信事業者の取り得るDDoS攻撃等への防止措置の検討、実施にあたっては、利用者の通信の秘密やプライバシー保護等との関係について十分な議論を行うべきであり、また利用者に不安を与えないような広報等を行うことも必要である。 | |
| これまで以上に通信の秘密に当たる情報を取り扱うことになるため、広く議論を深めたうえでガイドラインを作成／公開し、ガイドライン作成後の広報も積極的に実施するなどすることで、インターネット利用者へ不安や不信を与えないことが必要と考える。<br>【アルテリア・ネットワークス株式会社】 | 対応の方向性（案）９頁等において、通信の秘密、プライバシー保護等の観点から実施方法や留意事項を精査すべき旨を記述しているところと同旨であり、対応の方向性（案）に賛同する御意見として承ります。 |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 通信事業者がマルウェア感染の端末の特定を行い、利用者に対して注意喚起をするため、通信の秘密やプライバシー情報に関して整理することに賛同します。<br>【ＫＤＤＩ株式会社】 | |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| ４：　「４．電気通信事業者その他の関係者における情報共有」に関する御意見 | |
| 意見４－１<br>DDoS 攻撃等に係る通信情報について、第三者機関を結節点とした情報共有の枠組を設計するに当たっては、電気通信事業者にとって過度な負担とならず、できるだけ多くの者が参加できるような枠組にすべきである。 | |
| 情報共有は非常に重要である為、広く事業者が積極的に参加出来るようにすべきであり、その為にも事業者に対して過度な負担とならないこと事が必要と考える。<br>【アルテリア・ネットワークス株式会社】 | 法制度や具体的な実施枠組を検討するに当たっては、御指摘の点についても十分に留意しながら検討を進めることが重要と考えます。 |
| DDoS 攻撃等に係る通信情報について、第三者機関を結節点とした情報共有基盤の促進、制度整備する事に異論ございませんが、情報共有の枠組みに参画する事業者に過度な負担とならないようご配慮をお願いします。例えば、DDoS 攻撃等を実施している端末等の検知を行わない事業者であっても、セキュリティ確保のために必要な範囲での利用や DDoS 攻撃等の防止措置を実施すること等を条件として、広く共有されることを要望します。<br>【一般社団法人日本ケーブルテレビ連盟】 | |
| 意見４－２<br>第三者機関を通じた情報共有の枠組みを作ることに賛同する。<br>情報共有の枠組を設計するに当たっては、通信の秘密への十分な配慮等を行うべきである。 | |
| サイバー攻撃に係る情報を関係事業者間で共有するためには、第三者機関を通じた情報共有の枠組みを作る事に賛同します。枠組みの検討に際しては、通信の秘密への十分な配慮、情報提供のタイミング、共有対象の情報の明確化等への留意が必要と考えます。<br>【ＫＤＤＩ株式会社】 | 対応の方向性（案）12 頁等において、第三者機関の体制、情報提供の範囲、実施方法等について通信の秘密やプライバシー保護等との関係を踏まえて整理すべき旨記述しているところと同旨であり、対応の方向性（案）に賛同する御意見として承ります。 |

| 頂いた御意見 | 御意見に対する考え方 |
|---|---|
| ５：　「５．IoT 機器を含む脆弱な端末設備への対策」に関する御意見 | |
| 意見５－１<br>　ＩｏＴ機器を含む脆弱な端末設備への対策により、脆弱な端末設備に対するセキュリティ対策が進むことを期待。検討に当たっては、許容可能な実装・運用等のコストについても考慮する必要性がある。 | |
| 方向性(案)の指針に対し賛同いたします。<br>家庭内における端末設備を広く保護するホームゲートウェイの役割は重要であり、該当機器設計メーカの業界団体たる当協会は対策の検討にあたり協力させていただきたく存じます。<br>また、検討において「技術的な観点から専門的な検討を行っていく」過程にあたり、許容可能な実装・運用等のコストに関しても十分考慮する必要性がある点、意見とさせていただきます。<br>【一般社団法人デジタルライフ推進協会】 | 対応の方向性（案）に賛同する御意見として承ります。<br>なお、今後の検討に当たっては、許容可能な実装・運用等のコスト等についても、十分に留意することが適切と考えます。 |
| マルウェア Mirai やその亜種による感染に至る機器の注意喚起や無線 LAN ルータの脆弱性などに対し、ケーブルテレビ事業者がホームページへの掲載、ユーザへの周知や個別対処等が必要な事例が増えており、事業者の負荷になっております。また、前述のように、IoT の導入に取り組むケーブルテレビ事業者が増えております。<br>このため、「IoT セキュリティガイドライン ver1.0」の順守や本方向性に従った検討の加速化などにより、機器ベンダが脆弱な端末設備に対するセキュリティ対策を徹底することや、ユーザ(国民)のセキュリティ意識の醸成が進むことも期待いたします。<br>【一般社団法人日本ケーブルテレビ連盟】 | |
| 意見５－２<br>IoT 機器を含む脆弱な端末設備への対策については、国際競争力確保の観点から、日本独自の規制による輸入障壁とならないよう、適切な対応水準に向けて検討を行うとともに、国際的な連携を行っていくことが必要であり、その旨を示すために【５．IoT 機器を含む脆弱な端末設備への対策】の（２）に「なお、端末設備に関して『インターネット上の脅威から電気通信事業者の回線設備の安定稼働を守るための技術基準』を検討する場合は、電気通信事業者のネットワークに対するリスクの大きさや端末設備の国際競争力の確保、諸外国の状況や技術的な観点等を併せ考慮し、適切な対応水準となるように検討する」との記載を追加すべきである。 | |
| セキュリティ対策は、海外の動向も見ながら検討を行う必要があります。「諸外国の検討状況や技術の動向等十分に踏まえた上で、通信事業者、IoT 機器メーカ等の関係者から広く意見を聴取し、慎重に検討を進めていくことが求められる。」（P15）との記載がありますが、日本独自の規制が輸入障壁となったり、逆に日本製品の競争力の低下を起すことがないよう、ご留意戴きたいと存じます。<br>【一般社団法人日本電機工業会スマートホーム委員会】 | 対応の方向性（案）14 頁において、IoT の発展は、我が国の経済社会の活力の向上、国際競争力の確保の観点からも、極めて重要なものであり、現在、IoT 機器のセキュリティ対策については、諸外国においても様々な議論が行われ |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 【５．IoT 機器を含む脆弱な端末設備への対策(3)海外製品のセキュリティ対応及び国際的な連携の必要性について】<br>IoT 機器には既に多数の海外製品が存在するため、コスト増加も伴うセキュリティ対策は、国内ベンダだけでなく、海外ベンダへの実装も必要。日本独自の施策、対応は、わが国市場で事業を行う海外ベンダの反発を招くのみならず、市場の成長を損なう。このためセキュリティ検証方法は、海外ベンダにも適用される国際標準又はそれに準ずる標準を採用すべきであり、我が国固有の基準であってはならない。<br>また、国境のないサイバー空間において、グローバル規模で行われるサイバー攻撃にわが国単独で対応することは難しい。従って、諸外国の制度とのすり合わせ等を行い、国際的な連携による取組みを行うことが必要である。<br>【一般社団法人電子情報技術産業協会】 | ていることから、情報通信ネットワークの安全・信頼性を確保するための IoT 機器のセキュリティ対策については、こうした国際動向を踏まえた上で、IoT サービスや機器の普及の阻害とならないように慎重に検討を行う必要がある旨記述しているところと同旨であり、対応の方向性（案）に賛成する御意見として承ります。<br>なお、既に上記記述が存在することから、御意見にある修正は行わず、原案のとおりとします。 |
| 【５．IoT 機器を含む脆弱な端末設備への対策（２）今後の対応の方向性】<br>「なお、端末設備に関して『インターネット上の脅威から電気通信事業者の回線設備の安定稼働を守るための技術基準』を検討する場合は、電気通信事業者のネットワークに対するリスクの大きさや端末設備の国際競争力の確保、諸外国の状況や技術的な観点等を併せ考慮し、適切対応水準となるように検討する」を追加いただきたい。<br><br>（理由）<br>直接に電気通信事業者のネットワークに接続することを想定して設計されている製品であっても、例えば、常時電源オンではない機器のリスクは小さい可能性があるため、こうしたリスクの大きさを無視し一律に規制等をかけるべきではなく、また新たな技術の採用などによりリスクが回避される場合もあるため、こうした実際のリスクの大きさが考慮された適切な対応水準を設定いただき、国際競争力の確保という産業要求が併せて確保されるよう検討いただきたい。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 意見５－３<br>IoT 機器のセキュリティ対策の要件は、可用性だけではなく、機密性、完全性等の確保のための対策も検討すべき。また、一律の対策を避け、重要度や各機器の特性に応じた対策を講じるべき。 | |
| （1）偏りのないセキュリティ対策の必要性について<br>本方向性（案）は全体的に、円滑なインターネット利用環境を確保するという観点にて、主に DDoS 攻撃を防止するために、主に電気通信事業者が取るべく対応を纏められており、ネットワークを管理する立場にある総務省のセキュリティ対策であることを理解する。<br>しかし、ICT システムを構成する IoT 機器を開発・販売するベンダにはネットワークを主体とする ICT システムの可用性だけでなく、総合的なセキュリティ対策が求められるが、本方向性（案）は、機密性、完全性等の確保のための対策が示されていない。<br>これらのセキュリティ対策の要件は、相互に密接な関係を持つため、可用性だけを考慮したセキュリティ機能の実装は、他のセキュリティ機能及びそれらの実装のタイミング等で不整合を起こす可能性がある。セキュリティ対策は、一面に偏った対策ではなく、機密性や完全性等を確保するための対策も検討すべきである。<br>また IoT のセキュリティ対策はネットワーク全体、個々の対象機器、運用等極めて幅広く影響が及ぶが、一律的な対策を避け、重要度や各機器の特性に応じたメリハリある対策を講じるべきである。<br>【一般社団法人電子情報技術産業協会】 | 本検討会は、円滑なインターネット環境確保に向けて、IoT 機器が DDoS 攻撃等のサイバー攻撃に悪用され、インターネットに対する脅威が増大していることから、電気通信事業者の回線設備の障害の防止のため、端末設備への対策を検討対象としてきたものです。<br>御指摘のように、これらの対策は、IoT 機器の特性を考慮することが必要であり、対応の方向性（案）15 頁において、こうした観点から情報通信ネットワークの安全・信頼性を確保するための IoT 機器のセキュリティ対策について、技術的な観点から専門的な検討を行っていくことを求めています。<br>なお、御指摘の IoT の総合的なセキュリティ対策の検討については、政府では、サイバーセキュリティ戦略本部において、各府省庁の施策の総合調整等を行うとともに、関係府省庁において、民間の協議会等の関係者とも連携しながら具体的な施策を検討、実施しており、今後とも関係府省庁や民間の協議会等と適切に情報共有を行いながら施策の検討、実施をしていくことが重要と考えます。 |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 意見５－４<br>IoT 機器を含む脆弱な端末設備への対策については、電気通信事業者の回線設備に障害を与えないといった観点から、利用者が行うべき対策を記載するとともに、その対策や目的等について十分周知を行うべきであり、その旨を明示的に記載すべきである。 | |
| 【５．IoT 機器を含む脆弱な端末設備への対策（１）端末設備におけるセキュリティ対策の必要性】<br><br>”　”部分を追記されたい。<br><br>このため、利用者に対して IoT 機器のセキュリティ対策に関する啓発活動”（利用者が端末設備に対する責任を負うことも含む。）”を行うことに加え、IoT 機器等の端末設備においても、情報通信ネットワークの安全・信頼性を確保する観点から、”端末設備、自営電気通信設備の構築、接続、運用、保守、廃棄の各ライフサイクルで”一定のセキュリティ対策が必要と考えられる。<br><br>（理由）<br>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）」においても「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、それらの点についても本方向性（案）に記載することが重要である。<br>【一般財団法人日本データ通信協会】 | 本検討会は、円滑なインターネット環境確保に向けて、IoT 機器が DDoS 攻撃等のサイバー攻撃に悪用され、インターネットに対する脅威が増大していることから、電気通信事業者の回線設備の障害の防止のため、端末設備への対策を検討対象としてきたものです。<br>対応の方向性（案）15 頁において、情報通信ネットワークの安全・信頼性を確保するための対策について、技術的な観点から専門的な検討を行うことを求めていますが、利用者に対して IoT 機器のセキュリティ対策に関する啓発活動を行うことの必要性についても指摘しており、いただいた御意見にも留意しつつ、今後具体的な検討がなされる必要があると考えます。<br>なお、修正の御意見については、上記記述と同旨であることから、原案のとおりとします。 |
| 【５．IoT 機器を含む脆弱な端末設備への対策（２）今後の対応の方向性】<br><br>”　”部分を追記されたい。<br><br>通信事業者、IoT 機器メーカ等の関係者から”だけでなく、利用者の立場として消費者団体等にも”広く意見を聴取し、”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ができる体制（例えば、資格者による構築、接続、運用、保守、廃棄）の構築も含めて、”検討を進めていくことが求められる。 | |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| （理由）<br>4ページ　”２．基本的な考え方”において、電気通信事業者のみならず、・・・利用者等の通信ネットワークに関わる者全体が連携しながら対応を進めていきことが極めて重要である。“としているが、実際の端末設備の所有者である利用者に対する対応が啓発活動のみとなっていることから、利用者が行うべき対応についても記載するとともに、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構築ができるようにすることが重要である。<br>【一般財団法人日本データ通信協会】 | |
| 【５．IoT 機器を含む脆弱な端末設備への対策（２）今後の対応の方向性】　第二段落<br><br>「また、端末設備に関して『インターネット上の脅威から電気通信事業者の回線設備の安定稼働を守るための技術基準』を追加する場合には、これが「端末設備の安全性」のための基準ではなく、「電気通信事業者の回線設備の安定稼働の確保」のための基準であることを、利用者に正確に伝える必要がある。」を追加していただきたい。<br><br>（理由）<br>インターネット上の脅威に対応するための技術基準として説明された場合、通常利用者は、こうした基準に適合している「端末設備」がデータの安全保護を含むセキュリティに強い製品であると認識するのが一般である。こうした誤った認識により、利用者をミスリードし市場に混乱が生じるだけでなく、IoT セキュリティ全体の推進という点においても障害となりかねないため、如何に正確に利用者に対してアピールするかについての十分な検討が必要である。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | |
| 【５．IoT 機器を含む脆弱な端末設備への対策（２）今後の対応の方向性】<br><br>「あわせて、利用者に対して「直接電気通信事業者のネットワークに接続することを想定して設計されている製品」以外については、ゲートウェイの中で使用することが求められていること、直接電気通信事業者のネットワークに接続することを想定して設計されている製品については基準認証等の措置の有無を確認したうえで接続することのアピールを徹底する活動が必要である。」を追加いただきたい。 | |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| （理由）<br>電気通信事業者の通信ネットワークの稼働安定性確保にあたっては、最終的には利用者が適切な環境で端末設備を利用するようリードすることがポイントとなるので、まずは、こうした法律や基準についての端末設備利用者の理解レベルを向上させることや運用方法を工夫することが必要と思われる。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | |
| 意見５－５<br>簡易的なＩＤ・パスワードの他、セキュリティ・モジュールを活用したＭ２Ｍサービスのセキュリティ対策についても検討対象とすべき。また、ＩｏＴ機器メーカ以外にも、アプリ配信事業者、Trusted Service Managers（ＴＳＭ）なども検討対象とすべき。 | |
| 今回の検討ではインターネット上で最近発生している事例として「ＩＤ・パスワード」の流出事例が取り上げられております。<br>しかし，海外では放送用ＳＴＢ端末のセキュリティ機能を偽造し，真正なユーザではないユーザが視聴できる等の被害が発生しています。また，国内でもＢＣＡＳカードの偽造被害が発生しました。<br>そのため，今後のＩｏＴ機器の発展の中で現在の簡易的なＩＤ・パスワードの他，セキュリティ・モジュールを活用したＭ２Ｍサービスも考えられることから，これらも検討対象とすべきではないか。<br>【凸版印刷株式会社】 | 御意見については、情報通信ネットワークの安全・信頼性を確保するための IoT 機器のセキュリティ対策に関して、技術的な観点から専門的な検討を行う際に参考とすることが適切と考えます。 |
| セキュリティ対策を実現するためには，ここで利用される IoT 機器の他，最適なセキュリティレベルを実現する信頼関係（セキュリティ・トラスト）を実現する必要があります。そのため，予め端末に暗号鍵等のセキュリティ情報を格納しておくこと，これに加えてユーザに対応するユーザ鍵を改めて格納することなどが行われます。（簡単な事例ではＳＩＭにＩＤ及び通信用暗号キーが格納される場合など）<br>今後のＩｏＴ機器の発展に合わせて，これらの端末に格納される暗号鍵等の秘密情報を運用に合わせて柔軟に管理することが求められることから，ＩｏＴ機器メーカばかりでなくアプリ配信事業者，Trusted Service Managers（ＴＳＭ）といった鍵配信・管理についてもご検討を頂きたい。<br>【凸版印刷株式会社】 | |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 意見５－６<br>ネットワークに接続されるデバイスそのものが扱うデータの保護を検討の対象範囲外とすることを明記していただきたい。 | |
| 【２．基本的な考え方】　第五段落<br><br>基本的な考え方として、ネットワークに接続されるデバイスそのものが扱うデータの保護を検討の対象範囲外とすることを明記していただきたい。<br><br>（理由）<br>インターネット上の脅威との関係でデバイスの防御対策について説明される場合、「サイバーセキュリティ」対策と混同して受け止められることが一般的であるため、こうした不要な誤解や混同を避けるために、本来、サイバーセキュリティとして議論されるような「通信回線」を通じてやりとりされる「データ」の保護は検討の対象外であることを明記いただきたい。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | 本検討会は、円滑なインターネット環境確保に向けて、IoT 機器が DDoS 攻撃等のサイバー攻撃に悪用され、インターネットに対する脅威が増大していることから、電気通信事業者の回線設備の障害の防止のため、端末設備への対策を検討対象としてきたものです。<br>上記の観点を踏まえ、今後、技術的な観点から専門的な検討を行っていく上では、端末設備におけるデータの保護の必要性についても留意することが必要です。<br>したがって、御意見にある修正は行わず、原案のとおりとします。 |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| 意見５－７<br>「電気通信事業法等で求められる基準認証等の措置を講じた端末設備を通信ネットワーク回線に接続したにもかかわらず「電気通信事業者の回線設備の安定稼働」が損なわれた場合の責任分界について、電気通信事業法の下でどのように取り扱われるべきかについても検討する必要がある」を追加いただきたい。 | |
| 【５．IoT 機器を含む脆弱な端末設備への対策（２）今後の対応の方向性】<br><br>「電気通信事業法等で求められる基準認証等の措置を講じた端末設備を通信ネットワーク回線に接続したにもかかわらず「電気通信事業者の回線設備の安定稼働」が損なわれた場合の責任分界について、電気通信事業法の下でどのように取り扱われるべきかについても検討する必要がある」を追加いただきたい。<br><br>（理由）<br>昨今のセキュリティ攻撃の進化の状況から、たとえ基準認証等の措置が取られたとしても、必ずしも「電気通信事業者の通信ネットワークの稼働安定性」が確保されることにはならない。<br>回線設備の稼働安定性を継続して確保していくために、電気通信事業者と端末設備事業者間で情報が共有され、円滑に検討がすすめられるような体制を構築いただきたい。<br>【一般社団法人ビジネス機械・情報システム産業協会】 | 御意見の趣旨が必ずしも明らかではありませんが、利用者の接続する端末設備と電気通信事業者の設備との間の責任の分界については、電気通信事業法第 52 条第２項に基づき、電気通信事業者の設置する電気通信回線設備と利用者の接続する端末設備との責任の分界が明確であるようにすることを確保する技術基準が定められています。<br>したがって、御意見にある修正は行わず、原案のとおりとします。 |

| 頂いた御意見 | 御意見に対する考え方 |
| --- | --- |
| ６：　「６．2017 年８月に我が国で発生した大規模なインターネットの障害に関する検証と今後の対策」に関する御意見 | |
| 意見６－１<br>報告の在り方の変更について、単なる基準の変更ではなく、共有の効果が高まり、かつ、事業者の運用に過度な負担とならないよう検討が必要と考える。 | |
| 報告の在り方の変更について、単なる基準の変更ではなく、共有の効果が高まり、かつ、事業者の運用に過度な負担とならないよう検討が必要と考える。<br>【アルテリア・ネットワークス株式会社】 | 御意見については、インターネットの障害に関する情報共有体制の整備等を検討する際に参考とすることが適切と考えます。 |