資料91－４

IPネットワーク設備委員会報告（案）概要
－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－

令和７年１１月２７日
IPネットワーク設備委員会
総務省

検討の背景・内容（委員会報告（案） 第1,2章）

【検討背景】

○ 電気通信事業法では、端末設備等規則（端末規則）において、電気通信回線設備に直接接続する端末機器に関する技術基準（強制規格）を規定。

○ IoT機器のセキュリティ対策については、Webカメラやルータなどの IoT機器が乗っ取られ、インターネットに障害を及ぼすようなDDoS攻撃等のサイバー攻撃に悪用される事案が増加したことを受け、情報通信審議会において検討（平成29-30年）を行い、省令（端末規則）を改正（令和2年4月施行）。

【セキュリティ基準施行後の動向】

○ IoT機器のセキュリティ対策に係る規定に基づき技術基準適合認定等を受けた機器であっても、NICTが行っている調査（NOTICE）によって「サイバー攻撃に悪用される脆弱性のあるIoT機器」として検知される事案が発生している状況。

○ 端末機器に関する技術基準に関連する制度として、令和4年より、経済産業省及びIPAにおいて、任意規格として、IoT製品に対するセキュリティ適合性評価制度（JC-STAR）の検討が進められ、令和7年3月、【★1】のラベリングについて受付を開始。

【IoT機器のセキュリティに関する海外の動向】

○ 市場に流通されるIoT機器のサイバーセキュリティ確保等を目的とした法律が各国において発行されている（IoT Cybersecurity Improvement Act（米）, PSTI Act（英）, Cyber Resilience Act（欧） 等）。

○ 各国において、IoT機器に対するラベリング制度（任意）を設け、運用している（U.S Cyber Trust Mark（米）, Cybersecurity Labelling Scheme（星）等）。

IoT機器のセキュリティ対策に関する省令を施行して5年が経過したことを踏まえ、内容の妥当性（NOTICEによる調査結果との比較等）を検証し、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等について検討する。

【検討内容】

1. アクセス制御機能、ID・パスワードの適切な設定に関する機能（デフォルトパスワード及びその更新　等）

○ セキュリティ基準施行後に販売された機器が、NOTICEにおいて検知される要因の分析を踏まえた、制度の見直し要否を検討。

2. インタフェース無効化機能、ファームウェア更新機能について

○ （サプライチェーンの複雑化により）機器の製造者が把握していない通信機能が機器に存在する場合があり、サイバー攻撃の対象となるおそれ。対策として、機器の利用上不要なインタフェースの無効化を求めるかどうか（セキュリティ基準に追加するかどうか）を検討。

○ ファームウェア更新機能について一部規定しているが、より具体的な内容を規定することの要否を検討。

3. その他

○ 1. 及び2. に記載の機能の他、端末規則、関係告示、ガイドライン等に追加すべきセキュリティ基準の有無を検討。

検討結果①（セキュリティ基準の見直し）（委員会報告（案）第3章）

○ アクセス制御の際に使用するID/パスワードの設定機能及びファームウェアの更新機能の見直し、並びに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を追加することが適当。

○ 各機能に対して、具体的に求める基準等（※1）については、JC-STAR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。

○ セキュリティ基準に関する技術基準適合認定等の審査方法について、登録認定機関における実機による試験を義務付けることは、申請者に対して過剰な負荷となることから、書面による確認（※2）とすることが適当。

※1 パスワードに求める「容易に推測されない」の確認方法、無効化するインタフェースおよびその確認方法　等
※2 技術基準適合認定等の申請者がセキュリティ基準に係る試験結果等を提出し、登録認定機関が申請書類を基に審査する形式

機能の見直し・追加

機能	端末規則（現行）	検討結果（見直しの方向性）
アクセス制御の際に使用するID/パスワードの設定機能	<どちらか1つを実装することを求めている> ① 当初より端末機器毎に一意のID/パスワードが付されていること ② 当初より設定されているID/パスワードの少なくとも1つの変更をユーザに促す機能	デフォルトID/パスワードの設定及び当該ID/パスワードからの変更にあたって「第三者から容易に推測されない」ものを設定・変更するよう技術基準に規定（詳細はガイドラインに規定） 左欄②は、「変更を促す」ではなく、「変更させる」ことを求める
ファームウェアの更新機能	ファームウェアの更新が可能であること	以下のような具体的な基準・指標を規定 ・最新のファームウェアがインストールされていることを確認する手段を有すること ・ソフトウェアをネットワーク経由でアップデートする際、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有すること
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	規定なし	インタフェースへのアクセスに対しては、製造者が提供する意図を持つ通信機能以外について無効化しておくことを技術基準として規定

機能の見直し・追加に向けた検討のポイント（委員会報告（案）第3章）

検討内容	現　状	課　題
アクセス制御機能、ID/パスワード設定機能の見直し	○ NOTICEにおけるID/パスワード設定の脆弱性調査において、セキュリティ基準を含む技術基準適合認定等を取得した端末機器であっても脆弱性のある機器として検知されるケースが存在。 ○ 要因として、「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」を具備している場合において、 ・端末機器メーカが出荷時のデフォルトID/パスワードが簡便なもの、かつ、ユーザがそのまま使用しているケース。 ・機器側のパスワードルールが厳しくないなどの理由により、ユーザによって脆弱なID/パスワードが設定されるケース。 が考えられる。	○「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」を具備していても、ID/パスワードの変更を行わずに端末機器を利用できるケースが考えられる。 ○ ユーザが変更したID/パスワードについては、文字数などの規定が存在せず、たとえ一文字のID/パスワードであっても端末規則の規定を満足していることになる。 ○「当初より端末機器毎に一意のID/パスワードが付されていること」の規定を含め、ID/パスワードに係る規定は、第三者から容易に推測されないものであることを目的として導入されたものの、当該目的については現時点ではガイドラインに記述があるのみで、法律上規定されていない。
ファームウェア更新機能の見直し	○ 年を追うごとに狙われる脆弱性の数が増加している状況であり、ルータが特に攻撃の対象となっている。また、機器個別の脆弱性が狙われるようになっている。 ○ アクセス制御機能、ID/パスワード設定機能（第三者から容易に推測されないパスワード設定）は、悪意のある攻撃者からの侵入を一定程度防ぐことに対して効果的だが、端末機器の脆弱性に起因する侵入・感染を防ぐことは困難であり、端末機器そのものの脆弱性対策を講じることが重要。	○ 端末機器に対するファームウェア更新により、機器の脆弱性を突いた攻撃への対策をとることが可能となるが、脆弱性は日々発見されることから、ファームウェアは最新のものが適用されていることが必要。また、ファームウェア更新が徹底されない古い端末機器の脆弱性は狙われ続けるため、更新の徹底が必要。 ○ 端末規則では「更新が可能」であることが要件となっており、自動的に更新される端末機器も存在するが、大部分はユーザが自発的に更新作業を行うことが必要。最新の脆弱性対策が適用されることでリスク軽減につなげるため、当該更新について、具体的な基準（指標）の規定が必要。
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	○ 端末規則に規定されていない。	○ サプライチェーンの複雑化により、製造者も把握・想定していない通信機能が端末機器に存在（物理的な接続端子だけでなく、プロトコルのポート等も含む。）。 ○ 当該通信機能は、製造者に放置されている形となり、サイバー攻撃の対象となるリスクが高いことから、製造者は自らの製品に対して、提供しようとしている通信機能以外の機能が存在しているか確認し、存在している場合、悪意ある第三者によって利用されない措置を講じておくことが必要。 ○ 現行の端末規則において、機器の設定を変更する際のアクセス制御機能を規定しているが、機器の設定を変更する機能は、機器の製造者が意図的に実装するものであり、自ら実装した機能については、適切な確認を行うことができると考えられるが、それ以外の通信機能の確認は十分になされていないおそれ。

検討結果②（対象範囲、経過措置）（委員会報告（案）第4,5章）

○ 見直し後のセキュリティ基準が適用される端末機器は、これまでと同様、電気通信回線設備に直接接続されるものとすることが適当。

○ 制度改正前に技術基準適合認定等を取得した端末機器には、これまでと同様の経過措置を設けることを基本とし、周知活動等において置き換えの推進を行っていくこととした上で今後、置き換えの状況や、既存機器の接続によるセキュリティリスクについて継続的に注視し、必要に応じて対策を講ずることが適当。セキュリティリスクの高い機器が出てきたような場合には個別に対応することを検討することが適当。

対象機器の範囲

【現状】

○ 現行のセキュリティ基準では、電気通信回線設備に直接接続される端末機器を技術基準の適用対象としている。

【主な意見】

○ 電気通信回線設備に間接的に接続する機器には任意規格を活用しつつ、直接接続する機器には端末規則（強制基準）を強化して適用する方向の対応が望ましい。

【検討結果】

○ 対象機器の範囲は、これまでと同様に、電気通信回線設備に直接接続される端末機器とすることが適当。

○ 間接的に接続される機器への技術基準適用の要否は、今後の状況を踏まえ、改めて検討することが適当。

経過措置

【現状と課題】

○ 累次の制度改正において、制度改正前に技術基準適合認定等を受けた端末機器に対して経過措置を規定。

○ 具体的には、制度改正等により技術基準に追加された機能を実装して再度認定等を受けることを求めない措置（従前の技術基準を適用可）を規定。

○ 令和元年以前に発売された端末機器がNOTICEの脆弱性調査で「脆弱な機器」として判断される件数の83～96%を占めている。

【主な意見】

○ 経過措置により機器を接続可能とし、注意喚起を継続することが一般ユーザの多さを考えると妥当である。一方で、非常に大きなリスクがある場合には、個別に取り扱っていくべき。

○ 家庭用の端末設備は利用者・管理者が多様に混在しているため、法的効力をもって利用停止や置き換えを強いるのではなく、（周知活動、キャンペーンの活用等による）利用者・管理者の自発的な置き換えを促すことが望ましい。

【検討結果】

○ これまでと同様の経過措置を設けることを基本とし、周知活動等において置き換えの推進を行っていくこととした上で今後、置き換えの状況や、既存機器の接続によるセキュリティリスクについて継続的に注視し、必要に応じて対策を講ずることが適当。

○ セキュリティリスクの高い機器が出てきたような場合には個別に対応することを検討することが適当。

今後の検討課題（委員会報告（案）第6章）

○ 対象機器の範囲や、経過措置（制度見直し前に技術基準適合認定等を取得した機器への措置）に関して示された意見を踏まえ、今回の検討結果が反映された端末規則の施行後、状況経過について継続的に注視し、必要に応じて対策を講じることが適当。

○ 今後も、上記の継続的な注視状況を踏まえつつ、電気通信事業法の主旨に基づき取り組んでいる総務省内の関連施策や、関係者の取組と連携を図るとともに、整合のとれたものとなるよう、不断の見直しを行うことが望ましい。

関係意見

・電気通信回線設備に間接的に接続される端末機器もIPで接続されている現状を踏まえ、セキュリティ対策に関する技術基準が対象とする端末機器の範囲について、電気通信回線設備に直接接続されるものに限定せず、インターネットに接続されるものを対象とすること。

・令和2年4月に施行された、端末機器に対するセキュリティ基準が適用される以前に認定等を受けた端末機器や、現在のセキュリティ基準に適合していると認定等を受けた端末機器に対して、今回の検討結果を踏まえた見直し後の技術基準に適合することを求めること。