資料88-1

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について
（有識者ヒアリング　参考資料）

令　和　７　年　６　月　２　４　日
ＩＰネットワーク設備委員会
総　　務　　省

検討内容（第86回IPネットワーク設備委員会資料より）

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。

【考えられる要因】

①ID、パスワードがデフォルトかつ、容易に推測できるもののまま使用
パスワード変更に関して【後で変更】する機能が用意されていることなど。

②ユーザーによって脆弱なパスワードが設定
複雑性を強要していない、8文字以下のパスワードを許容するなど、機器側のパスワードルールが厳しくないこと。

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、端末設備等規則、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。

（参考） 上記の検討内容に関する現行技術基準の規定内容

機能	端末設備等規則（現行）	（参考）JC-STAR制度（★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	<どちらか1つを実装することを求めている> ・機器ごとに別の識別符号（ID/パスワード）が付されていること（第三者から容易に推測されないもの） ・少なくとも1つの識別符号（ID/パスワード）の変更を促す機能（第三者から容易に推測されないものを目的としているが文字数規定などの制限はなし）	【デフォルトパスワードの設定】＊ 機器毎に異なる一意の値で、容易に推測可能でない6文字以上 【デフォルトパスワードの更新】＊ 初回起動時にユーザによるパスワード変更（8文字以上）を強制 【その他】 総当たり攻撃からの保護　等 ＊はいずれか一方を満たす必要がある
インタフェース無効化機能	規定なし	不要かつリスクの高いインタフェースの無効化
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	・ファームウェアの更新が可能であること ・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できる機能 ・アップデート前にファームウェアの完全性を確認できる機能　等

端末機器に関する技術基準（セキュリティ基準の部分）とJC-STAR制度の比較

制度の建付け

※利用者が任意のソフトウェアにより随時かつ容易に変更することができる機器（PCやスマートフォン等）を除く

	端末設備等規則のセキュリティ基準	JC-STAR制度
対象機器（※）	・インターネットプロトコルを使用（データ通信） ・電気通信回線設備に直接接続	・インターネットプロトコルを使用（データ通信） ・インターネットに接続（直接・間接とわず）
位置づけ	・強制規格（技術基準適合認定等に必須）	・任意規格 ・IoT製品として共通して求められる最低限のセキュリティ要件（★1）
規定・制度の目的	・電気通信回線設備に障害を与えない ・他の利用者に迷惑を及ぼさない　等 【電気通信事業法第52条第2項に規定】	・共通的な物差しでIoT製品のセキュリティ機能を評価・可視化し、適切なセキュリティ対策が講じられているIoT製品が広まる仕組みの構築 ・IoT製品に具備されたセキュリティ機能を評価・可視化することで、安全なIoT製品の選定・調達・購入を容易とする　等
適用開始	令和2年4月1日施行	令和7年3月受付開始（★1）

制度の目的（保護対象等）に差異あり。

規定の内容

IoT機器がマルウェア等に感染してDDoS攻撃の踏み台となることへの対策を検討、制度整備されたもの

カテゴリ	端末設備等規則のセキュリティ基準	JC-STAR制度
認証・識別 アクセス制御	・アクセス制御機能 ・ID/PWの適切な設定を促す等の機能	・適切な認証に基づくアクセス制御 ・容易に推測可能なデフォルトパスワードの禁止、パスワードの変更機能 等
ソフトウェア更新	・ファームウェアの更新機能	・ソフトウェアのアップデート機能、アップデート前の完全性の確認機能　等
レジリエンス向上	・上記設定等の電力供給停止時の維持	同左
インタフェースへの論理アクセス	－	・不要かつリスクの高いインタフェースの無効化
（IoT機器内の） データ保護	－	・製品に保存される守るべき情報の保護（保存データの暗号化　等） ・ネットワーク経由で伝送される守るべき情報の保護　等
情報提供	－	・ユーザへのセキュアな利用・廃棄方法に関する情報提供　等
その他	－	・製品本来の機能の保護 ・人的資産（利用者の健康など、利用者の物理的安全性）の保護 ・物理的資産（製品本体や関連する物理的機器）の保護　等 （★2以上で規定される予定）

端末設備等規則におけるセキュリティ基準の規定（2020年4月1日施行）

（インターネットプロトコルを使用する専用通信回線設備等端末）

第三十四条の十　専用通信回線設備等端末（デジタルデータ伝送用設備に接続されるものに限る。以下この条において同じ。）であつて、デジタルデータ伝送用設備との接続においてインターネットプロトコルを使用するもののうち、電気通信回線設備を介して接続することにより当該専用通信回線設備等端末に備えられた電気通信の機能（送受信に係るものに限る。以下この条において同じ。）に係る設定を変更できるものは、次の各号の条件に適合するもの又はこれと同等以上のものでなければならない。ただし、次の各号の条件に係る機能又はこれらと同等以上の機能を利用者が任意のソフトウェアにより随時かつ容易に変更することができる専用通信回線設備等端末については、この限りでない。

一　当該専用通信回線設備等端末に備えられた電気通信の機能に係る設定を変更するためのアクセス制御機能（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第三項に規定するアクセス制御機能をいう。以下同じ。）を有すること。

二　前号のアクセス制御機能に係る識別符号（不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号をいう。以下同じ。）であつて、初めて当該専用通信回線設備等端末を利用するときにあらかじめ設定されているもの（二以上の符号の組合せによる場合は、少なくとも一の符号に係るもの。）の変更を促す機能若しくはこれに準ずるものを有すること又は当該識別符号について当該専用通信回線設備等端末の機器ごとに異なるものが付されていること若しくはこれに準ずる措置が講じられていること。

三　当該専用通信回線設備等端末の電気通信の機能に係るソフトウェアを更新できること。

四　当該専用通信回線設備等端末への電力の供給が停止した場合であつても、第一号のアクセス制御機能に係る設定及び前号の機能により更新されたソフトウェアを維持できること。

アクセス制御機能

アクセス制御の際に使用するID/パスワードの適切な設定を促す等の機能

ファームウェアの更新機能

端末への電力共有が停止した場合でも、更新されたソフトウェアや変更されたアクセス制御の設定内容を維持

端末設備等規則におけるセキュリティ基準の考え方①
（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(第2版)より）

○　セキュリティ基準においては、対象機器が、端末設備等規則（以下「規則」という。）第34 条の10 各号に定める以下の一から四までの条件又は同条柱書に定める五の条件を満たさなければならないこととしている。

一　当該専用通信回線設備等端末に備えられた電気通信の機能に係る設定を変更するためのアクセス制御機能（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第三項に規定するアクセス制御機能をいう。以下同じ。）を有すること

電気通信回線設備を介して接続されることにより、端末機器に備えられた電気通信の送受信に係る機能が不正に設定変更(操作)されないことを目的として、当該設定変更(操作)の前にアクセス制御を行うことができる機能を有していなければならないものである。このアクセス制御機能は、端末機器に備えられた電気通信の送受信に係る機能の設定変更（操作）を正規の利用者等以外の者ができないよう制限するための機能であり、利用者に識別符号（機器の利用にあたって用いられる符号であって利用者を区別して識別するために用いるものであり、具体的にはパスワード又はパスワードとIDを組み合わせたもの等をいう。以下同じ。）の入力を求め、正しい識別符号が入力された場合にのみ当該設定変更（操作）の制限を自動的に解除し、正しい識別符号ではなかった場合には設定変更（操作）を拒否する機能である。

二　前号のアクセス制御機能に係る識別符号（不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号をいう。以下同じ。）であつて、初めて当該専用通信回線設備等端末を利用するときにあらかじめ設定されているもの（二以上の符号の組合せによる場合は、少なくとも一の符号に係るもの。）の変更を促す機能若しくはこれに準ずるものを有すること又は当該識別符号について当該専用通信回線設備等端末の機器ごとに異なるものが付されていること若しくはこれに準ずる措置が講じられていること

アクセス制御の際に使用する識別符号が他人から容易に推測できないものとして設定されることを目的として、識別符号の初期値（例えばパスワードとID の両方による認証や複数のパスワードによる認証など、複数の符号の組合せにより初期値が設定されている場合は、少なくとも一のID 又はパスワードの初期値）の変更を促す機能があり、若しくは機器ごとに別の識別符号（ID/パスワード）が付されており、又は、これらに準じる機能・措置が講じられているものでなければならないものである。これらの場合において、識別符号が安全に保管されることが推奨される。なお、取扱説明書等に識別符号の初期値の変更を促す記載をすることは、これらに準ずる措置として認められない。

端末設備等規則におけるセキュリティ基準の考え方②
（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(第2版)より）

三　当該専用通信回線設備等端末の電気通信の機能に係るソフトウェアを更新できること

端末機器に記憶されている電気通信の送受信の機能に係るソフトウェアの更新を行うことができる機能（ファームウェアの更新機能）を有していなければならないものである。なお、IoT 機器は多種多様であり、当該更新の手法は機器の種別毎に異なることから、安全かつ自動の更新でなければならないことまではセキュリティ基準として求めないが、当該更新は安全かつ自動で行われることが推奨される。

四　当該専用通信回線設備等端末への電力の供給が停止した場合であつても、第一号のアクセス制御機能に係る設定及び前号の機能により更新されたソフトウェアを維持できること

端末機器への電力供給が停止して電源オフになった後、電力供給が再開されて電源オンに戻って電気通信の機能が復帰した際に、アクセス制御の際に使用する識別符号の設定及び更新された電気通信の送受信の機能に係るソフトウェアが、出荷時の初期状態に戻ることなく、電源オフになる直前の状態を維持できるものでなければならないものである。

五　これと同等以上のもの

規則第34 条の10 各号の条件に適合するものと同等以上のセキュリティ対策が講じられていると認められる場合は、セキュリティ基準を満たすこととしている。具体的には、対象機器が国際標準ISO/IEC15408 に基づくセキュリティ認証(CC認証)を受けた機器などがこれに該当する。

JC-STAR制度 ★1セキュリティ適合基準

JC-STAR説明会（2024.11.28/12.2/12.6、独立行政法人情報処理推進機構（IPA））より。

★1で考慮する主な脅威			脅威に対抗するために★1で求める適合基準			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づく**アクセス制御**[1-3,5-5] (2)**容易に推測可能なデフォルトパスワードの禁止**[1-2,1-1] (3)パスワード等の認証値の変更機能[1-4] (4)ネットワーク経由のユーザ認証に対する**総当たり攻撃からの保護**[1-5]	情報提供	(16)ユーザへの**セキュアな利用・廃棄方法に関する情報提供**（初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等）[17-12,17-3,17-5,17-8,17-10]
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6)ソフトウェアコンポーネントのアップデート機能[3-1,3-2] (7)**容易かつ分かりやすいアップデート手順**[3-3] (8)アップデート前のソフトウェアの完全性の確認機能[3-7,3-2,3-10] (10)ユーザが製品型番を認識可能とする記載・機能[3-16]	情報・問合せの受付、情報提供	(5)連絡先・手続き等の**脆弱性開示ポリシーの公開**[2-1] (9)セキュリティアップデートの優先度決定方針の文書化[3-8]
	③未使用インタフェースの有効化により、		インタフェースへの論理アクセス	(13)**不要かつリスクの高いインタフェースの無効化**（物理的・論理的な通信ポート等）[6-1]	―	―
	①～③共通		データ保護	(11)製品に保存される守るべき情報の保護（**保存データの暗号化、物理的保護による保存、OSセキュア管理**等）[4-1]	―	―
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12)ネットワーク経由で伝送される守るべき情報の保護（**通信の暗号化、保護された通信環境の利用**等）[5-1,5-7]	―	―
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15)**製品内に保存される守るべき情報の削除機能**[11-1] ※(11)も含む	情報提供	※(16)に含む
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンス向上	(14) 停電・ネットワーク停止等からの復旧時の**認証情報やソフトウェア設定の維持**（初期状態に戻らないこと）[9-1]	―	―

※「適合基準の概要」欄の末尾の”[N-N]”は対応するセキュリティ要件の項目番号（複数の場合、代表的な要件を先頭に記載）を示す。セキュリティ要件は17個の大項目に分類。
※ 複数の脅威に対応するための適合基準もあるが、代表的なものにマッピングしている。