資料86-2

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

令和７年５月１３日
IPネットワーク設備委員会
総務省

検討の背景

○ 電気通信事業法では、端末設備等規則において、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（端末設備等規則）を改正（令和2年4月施行）。

○ 一方、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。

○ また、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制度）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。

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

	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、自己宣言（★1）
規定の趣旨	・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	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） 等
項目（概要）	・アクセス制御機能 ・ID/PW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 ・上記設定等の電力供給停止時の維持	・左記項目（一部の項目では、より詳細な規定） ・インタフェースへの論理アクセス ・（IoT機器内の）データ保護 ・製品ベンダーに関する適合基準
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）

※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

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。

【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

検討スケジュール

スケジュール（案）

令和７年	５月	６月	７月	８月	９月	10月以降
情報通信技術分科会						一部答申 → 答申内容を踏まえた省令改正等
IPネットワーク設備委員会	5/13 ・検討の背景 ・検討事項説明	ヒアリング	論点整理	報告書（案）の検討	意見募集 報告書（案）の決定	

ヒアリング（案）

対象者候補：NICT（NOTICE関係）、IPA（JC-STAR関係）、学識経験者、端末機器関係団体

ヒアリング内容：検討内容に対する考え方、その他端末設備のセキュリティ対策強化に向けて必要と考える取組・規律等

参考資料

端末設備に係る技術基準の概要

技術基準の考え方

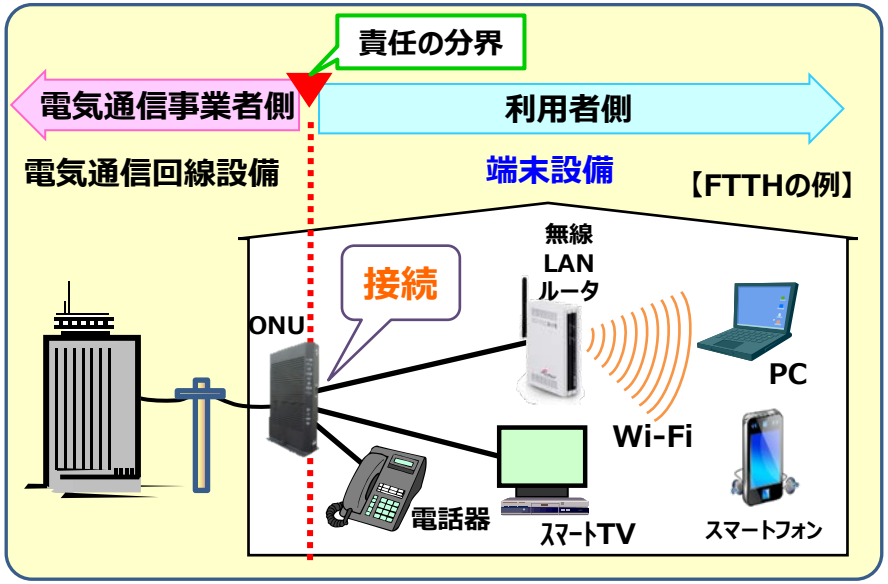
電気通信事業法では、電気通信回線設備に端末設備を接続する際の損傷や機能障害の発生を防止する目的から、次の３つの事項を確保するものとして、**総務省令（端末設備等規則）**に定める技術基準に適合することを求めている。

電気通信事業法（第52条第2項）

1) 電気通信回線設備を損傷し、又はその機能に障害を与えないようにすること

2) 電気通信回線設備を利用する他の利用者に迷惑を及ぼさないようにすること

3) 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を明確であるようにすること



- 「端末設備」は、電気通信回線設備の一部に接続される電気通信設備であって、その設置の場所が同一構内又は同一建物内であるもの。
- 「自営電気通信設備」は、電力会社や鉄道会社等の自営通信システムなど端末設備以外のものであって、電気通信役務の提供に用いるものではない電気通信設備。
  「自営電気通信設備」の接続に係る技術基準は、端末設備に係るものを準用。

- 技術基準は**端末設備**に適用
- 技術基準適合認定等は**端末機器**※が対象

※ 端末機器の技術基準適合認定等に関する規則第３条で定める種類の端末設備の機器

※ 電気通信回線設備：送信の場所と受信の場所との間を接続する伝送路設備及びこれと一体として設置される交換設備並びにこれらの附属設備

端末設備の接続と技術基準の確保

電気通信事業者は、利用者から端末設備をその電気通信回線設備に接続すべき旨の請求を受けたとき、その接続が技術基準に適合しない場合等を除き、その請求を拒むことができない（電気通信事業法第52条）。

利用者は、**技術基準に適合し表示（技適マーク）が付された適合表示端末機器を接続する場合等を除き**、電気通信事業者による接続の検査を受け、技術基準に適合する端末設備と認められなければ、**当該設備を使用できない**（電気通信事業法第69条）。

端末設備等規則の構成

（端末設備に求められる基準全般）

第１章　総　則（第１条・第２条）

第２章　責任の分界（第３条）

第３章　安全性等（第４条～第９条）

（個別の端末設備に係る規定）

第４章　電話用設備に接続される端末設備

第２節　移動電話端末（第１７条～第３２条）

第３節　固定電話端末（第３２条の２～第３２条の９）

第４節　インターネットプロトコル移動電話端末
（第３２条の１０～第３２条の２５）

第５章　無線呼出用設備に接続される
端末設備（第３３条・第３４条）

第７章　専用通信回線設備又はデジタルデータ
伝送用設備に接続される端末設備
（第３４条の８～第３４条の１０）
＊IoT機器の端末設備はここに該当

第８章　特殊な端末設備（第３５条）

（その他）

第９章　自営電気通信設備（第３６条）

・責任の分界

・漏えいする通信の識別禁止　・鳴音の発生防止
・絶縁抵抗等　・過大音響衝撃の発生防止
・配線設備等
・端末設備内において電波を使用する端末設備

・基本的機能　・発信の機能　・緊急通報機能　等

・無線呼出端末固有情報の変更を防止する機能　等

・電気的条件等　・漏話減衰量
・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
－アクセス制御機能
－ID/PW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
－上記設定等の電力供給停止時の維持機能

IoT機器を含む端末設備のセキュリティ対策（情通審答申（2018.9.12）より）

■　近年、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て、インターネットに障害を及ぼすような事案が増加。

■　情報通信ネットワークの安全・信頼性を確保するため、IoT機器を含む端末設備の技術基準に最低限のセキュリティ対策を追加することについて検討。

検討結果（概要）

＜端末設備の接続の技術基準に追加すべきセキュリティ対策の内容＞

・　インターネットプロトコルを使用する端末設備であって、電気通信回線設備を介して接続することにより当該設備に備えられた電気通信の送受信に係る機能を操作可能なものについて、大量感染を防ぐための最低限のセキュリティ要件として、①アクセス制御機能、②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、③ファームウェアの更新機能（又はそれらと同等以上の機能※）が必要。

※ 同等以上の機能を持つものとしては、ISO/IEC15408に基づくセキュリティ認証(CC認証)を受けた複合機等が含まれる。

・　なお、PCやスマートフォン等については、当該セキュリティ要件の規定の対象外とするが、利用者においてアンチウィルスソフトを導入する等の適切な対策を行うことが求められる。

＜技術基準適合認定等の対象機器の範囲＞

・　現在、技術基準適合認定等は、基本的に電気通信回線設備に直接接続される端末機器を対象に実施しており、セキュリティ要件が追加された場合においても、ネットワーク側からサイバー攻撃を受けた際に乗っ取られるリスクが特に高いのは、電気通信事業者の電気通信回線設備に直接接続される端末機器であることから、技術基準適合認定等の対象は、従来と同様に電気通信回線設備に直接接続可能な端末機器とする。

・　但し、恒常的に既認定機器を介して接続する機器（例：大型白物家電等）は、今後、認定等の対象外とする。

＜その他の対策等＞

・　IoTセキュリティを確保するためには、本対策だけではなく、改正電気通信事業法等に基づく電気通信事業者の情報共有等の新たな取組みや、ガイドラインの活用や周知啓発など総合的な対策が必要。

・　IoTのグローバル市場への展開や国際競争力確保等の観点から、今後もIoTセキュリティ対策に関する国際動向把握が必要。

端末設備等規則におけるセキュリティ関係の規定（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

JC-STAR制度概要

強制規格である端末設備等規則におけるIoT機器のセキュリティ基準に加えて、経済産業省及び独立行政法人情報処理推進機構（IPA）において、より範囲を拡大した任意規格として「JC-STAR」制度を2025年３月より開始。

※2024年11月「特定分野システムのIoT製品におけるJC-STAR制度活用ガイド（経済産業省）」から抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20241106.html

JC-STAR制度の概要

- 2022年11月より検討会[1]を開催し、2024年3~4月のパブリック・コメントを経て、8月に制度構築方針[2]を公表しました。それに従い、9月30日にIPAから**「JC-STAR」という制度名にて制度開始の案内**[3]を実施しました。
- **★１については2024年度中の制度開始**を予定しています。また、**政府調達等の要件**等とすべく関係省庁と議論を行っているほか、**米欧等の諸外国との制度調和**を図るため議論を行っています。

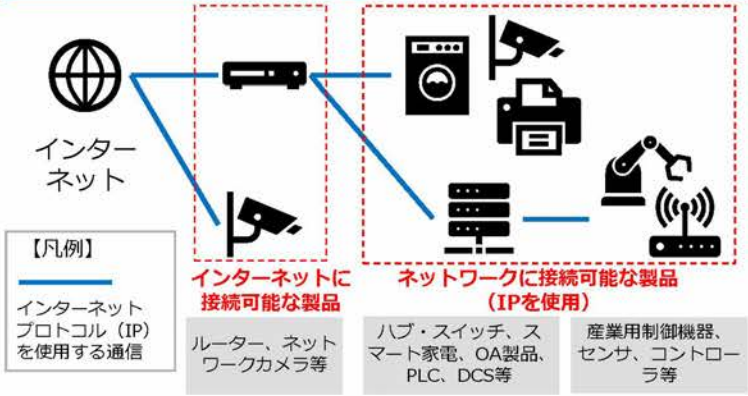
制度名称・ロゴ・ラベル

セキュリティ要件適合評価及びラベリング制度
JC-STAR
(Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements)

JC-STAR

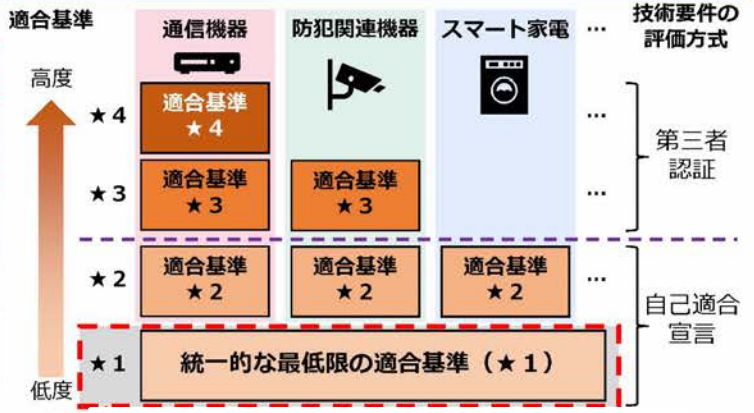
JAPAN CYBERSECURITY LABEL
★★★★
JC-STAR
Registered ID: 0123456789012345

対象製品の概要



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

制度の概要（イメージ）



1: 経済産業省「ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会）」 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html
2: 経済産業省「IoT製品に対するセキュリティ適合性評価制度構築方針（2024年8月23日）」 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html
3: IPA「IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」 https://www.ipa.go.jp/pressrelease/2024/press20240930.html

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。