資料 91－３

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）

―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

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）　目次

Ⅰ　検討事項

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（以下「委員会」という。）では、平成 17 年 11 月より、情報通信審議会諮問第 2020 号「ネットワークの IP 化に対応した電気通信設備に係る技術的条件」（平成 17 年 10 月 31 日諮問）について検討を行ってきている。

本報告は、「ネットワークの IP 化に対応した電気通信設備に係る技術的条件」のうち、「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、本年５月から~~９月~~ 11 月にかけて開催された委員会（第 86 回、第 88～第 9~~0~~1 回）において検討された結果を取りまとめたものである。

Ⅱ　委員会の構成

委員会の構成は、別表１のとおりである。

Ⅲ　検討経過

これまで、委員会（第 86 回、第 88 回～第 90 回）を開催して IoT 機器等の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等について検討を行い、報告を取りまとめた。

(1) 委員会での検討

① 第 86 回委員会（令和７年５月 13 日）

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、検討すべき内容を確認し、外部有識者等の関係者に検討課題に対するヒアリングを行うことを決定した。

② 第 88 回委員会（令和７年６月 24 日）

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検討課題について、外部有識者、関係団体等からヒアリングを行った。

③ 第 89 回委員会（令和７年８月４日）

ヒアリングの結果を踏まえ、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に関する論点整理を行った。

④ 第 90 回委員会（令和７年９月 29 日）

論点整理等の結果を踏まえた、IP ネットワーク設備委員会報告（案）の検討を

行った。また、同報告（案）を意見募集に付すこととした。

⑤　第 91 回委員会（令和 7 年 11 月 27 日）

委員会報告（案）に対する意見募集の結果について検討した。検討の結果、案のとおり（／一部修正の上）、情報通信技術分科会に報告することとなった。

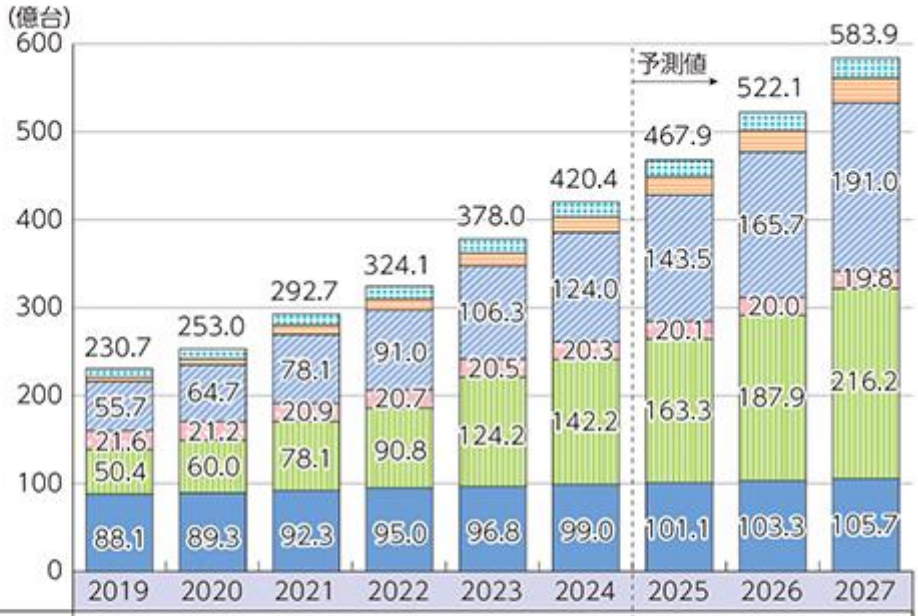
Ⅳ　検討結果

第１章　検討の背景

1.1　通信サービスの重要性とセキュリティ対策の重要性

パソコンやスマートフォンなど、従来のインターネット接続端末に加え、家電や自動車、ビル、工場など、世界中の様々なものがネットワークにつながるようになっている。特に、インターネットから操作可能な家電・スマートメータ等において IoT（IoT サービス）の果たす役割は大きく、民間調査会社の推定によれば令和６年度時点でデバイス数は約 420 億台、令和９年度には約 1.4 倍の約 584 億台に達すると予測されており、通信の果たす役割は今後ますます高くなっている。

40. 世界のIoTデバイス数の推移及び予測



	2019	2020	2021	2022	2023	2024	2025	2026	2027
合計	230.7	253.0	292.7	324.1	378.0	420.4	467.9	522.1	583.9
自動車・宇宙航空	9.8	11.3	12.7	14.2	15.7	17.3	19.1	20.9	22.7
医療	5.1	6.5	10.7	12.5	14.6	17.5	20.7	24.3	28.6
産業用途	55.7	64.7	78.1	91.0	106.3	124.0	143.5	165.7	191.0
コンピュータ	21.6	21.2	20.9	20.7	20.5	20.3	20.1	20.0	19.8
コンシューマ	50.4	60.0	78.1	90.8	124.2	142.2	163.3	187.9	216.2
通信	88.1	89.3	92.3	95.0	96.8	99.0	101.1	103.3	105.7

(出典)Omdia

図 1.1　世界の IoT デバイス数の推移及び予測
（情報通信白書令和７年版[1]　データ集[2]より）

一方、サイバー攻撃による被害も企業・個人問わず増加傾向にある。国立研究開発

[1] https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/pdf/index.html

[2] https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html

法人情報通信研究機構（以下「NICT」という。）が運用している大規模サイバー攻撃観測網（NICTER[3]）のダークネットで確認された令和６年の総観測パケット数は、平成 27 年観測時と比べて約 11 倍に増加しており（図 1.2）、IoT 機器を狙った通信が全体の３割を超えている（図 1.3）。

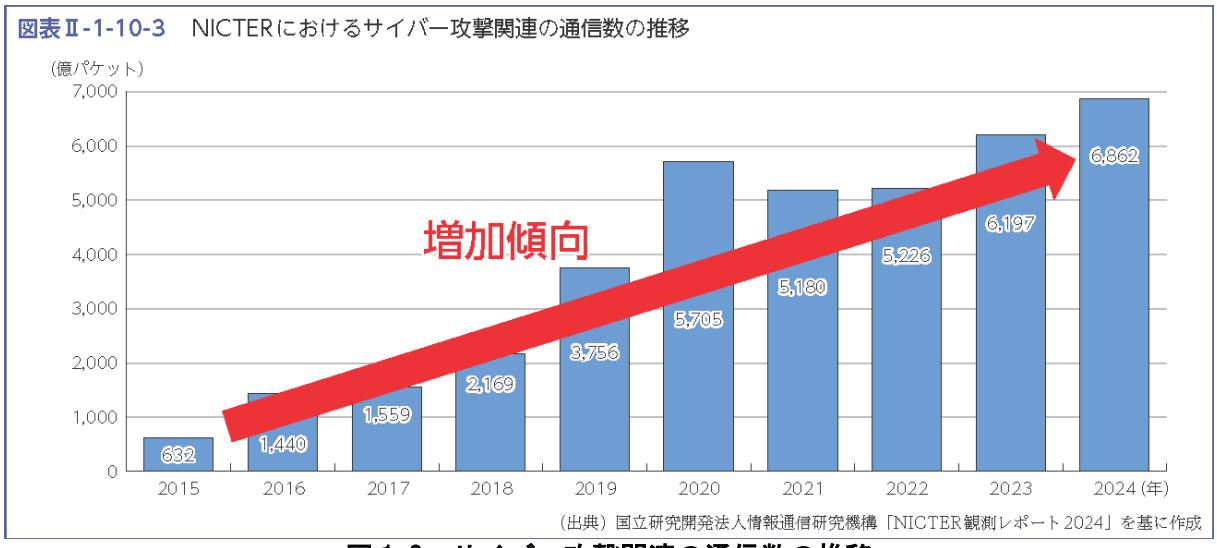


図 1.2　サイバー攻撃関連の通信数の推移
（情報通信白書令和７年版より）

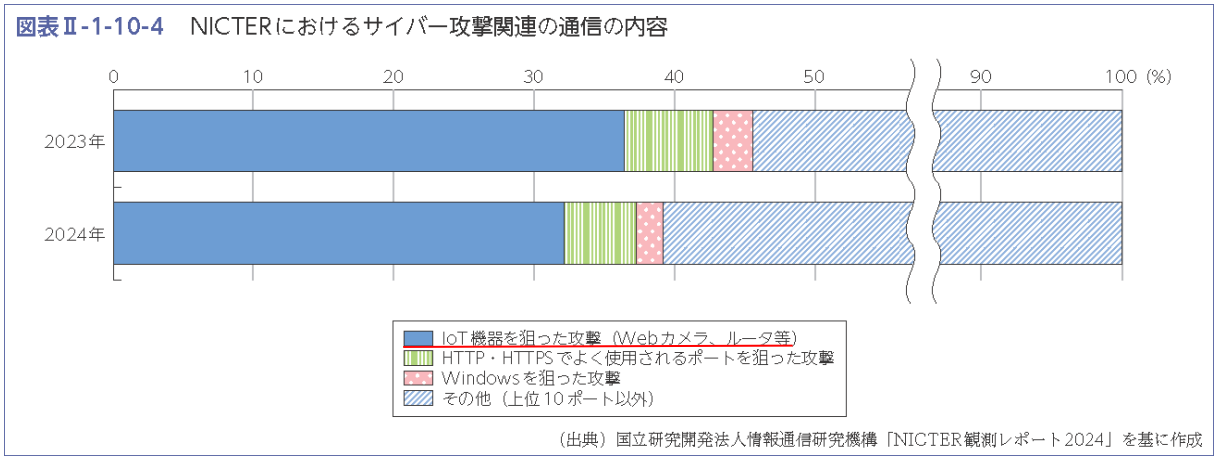


図 1.3　サイバー攻撃関連の通信の内容
（情報通信白書令和７年版より）

また、令和６年末から令和７年にかけて民間企業等で発生したセキュリティインシデントとして、ランサムウェアや不正アクセス、DDoS 攻撃によるものが確認されているが、DDoS 攻撃は利用者の端末機器も加害者になり得ることが想定されるため、端末機器を接続している電気通信事業者だけでなく利用者自身もセキュリティ対策を講じていくことがますます重要となっている。

[3] Network Incident analysis Center for Tactical Emergency Response

1.2　現行のセキュリティ基準の策定経緯

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ことを踏まえ、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、IP ネットワーク設備委員会において平成 29 年から平成 30 年にかけて検討を行い、平成 30 年９月に情報通信審議会の一部答申を得た。

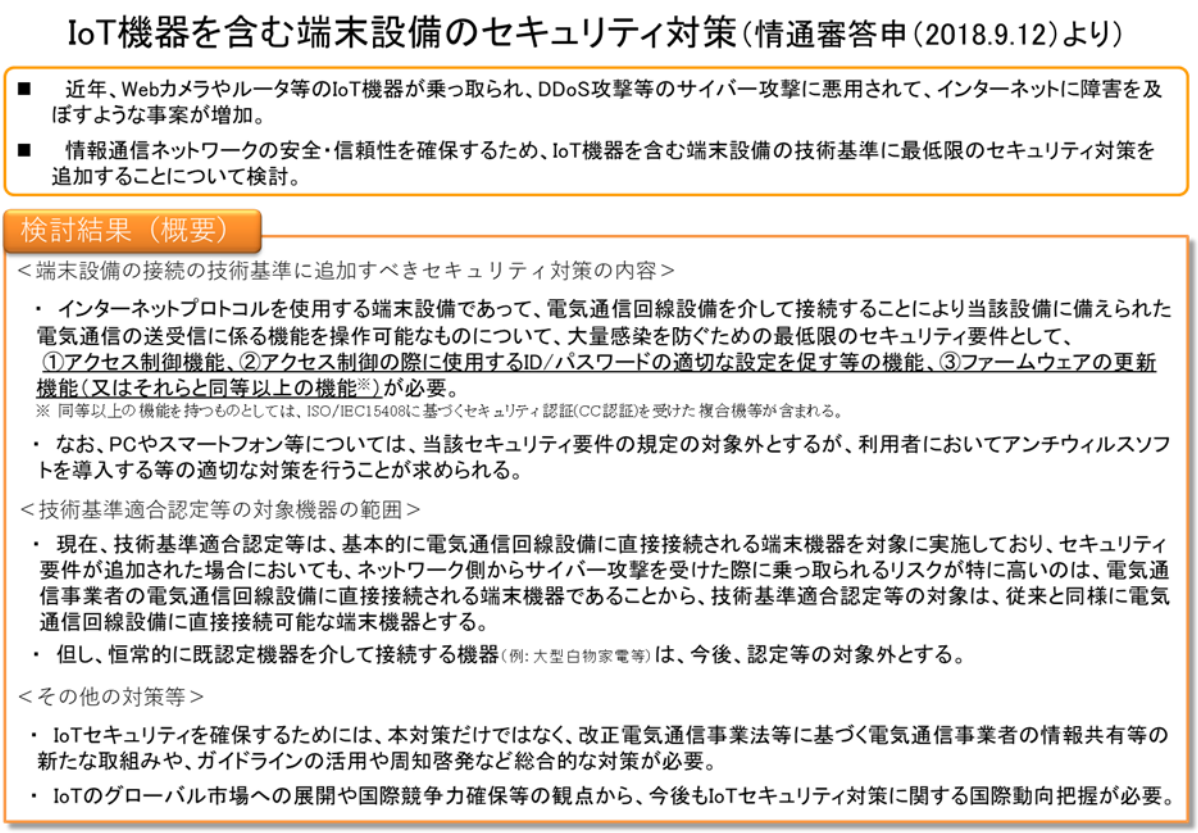


図 1.1　端末機器に対するセキュリティ対策概要（平成 30 年の検討結果）
（第 86 回委員会 事務局資料（資料 86-2）より）

総務省は、情報通信審議会の一部答申を踏まえた端末設備等規則（以下「端末規則」という。）の改正を行い、平成 31 年３月に公布、令和２年４月に施行された。現在の端末規則では、電気通信回線設備に直接接続される IoT 機器[4]に対して、以下のセキュリティ対策が技術基準として規定されている。

①　アクセス制御機能

端末機器に設けられている設定変更機能等を実施するにあたって、あらかじめ設定されて（して）いる ID/パスワードによる認証を行い、承認を得た場合に当該機能の実施を認める。

②　ID/パスワードの適切な設定を促す等の機能

[4] 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端末（パソコン、スマートフォン等）を除く。

ID/パスワードの設定にあたっては、（ア）端末機器毎に一意の ID/パスワードを設定すること、（イ）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のいずれかを実装すること。

③　ファームウェアの更新機能

端末機器の通信機能に係るソフトウェアの更新が可能であること。

④　その他（①～③の機能設定内容を電力供給停止時も維持する機能）

1.3　セキュリティ基準の見直しの検討に係る経緯

改正後の端末規則の施行から５年が経過し、技術基準として規定されたセキュリティ対策を講じた端末機器が市場にも流通している。

一方で、当該対策を講じているとして技術基準適合認定等を受けた機器であっても、NICT による IoT 機器調査（2.1 参照）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」として検知されるケースが発生している（3.1.1 参照。）。また、端末機器に関する技術基準に関連する制度として、経済産業省及び独立行政法人情報処理推進機構（以下「IPA」という。）において、任意規格として、IoT 製品に対するセキュリティ要件適合評価及びラベリング制度が令和７年３月より運用されている（2.2 参照。）。

こうした状況や新たな取組等を踏まえ、今回、現行の端末規則で規定されている技術基準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等について検討することとした。

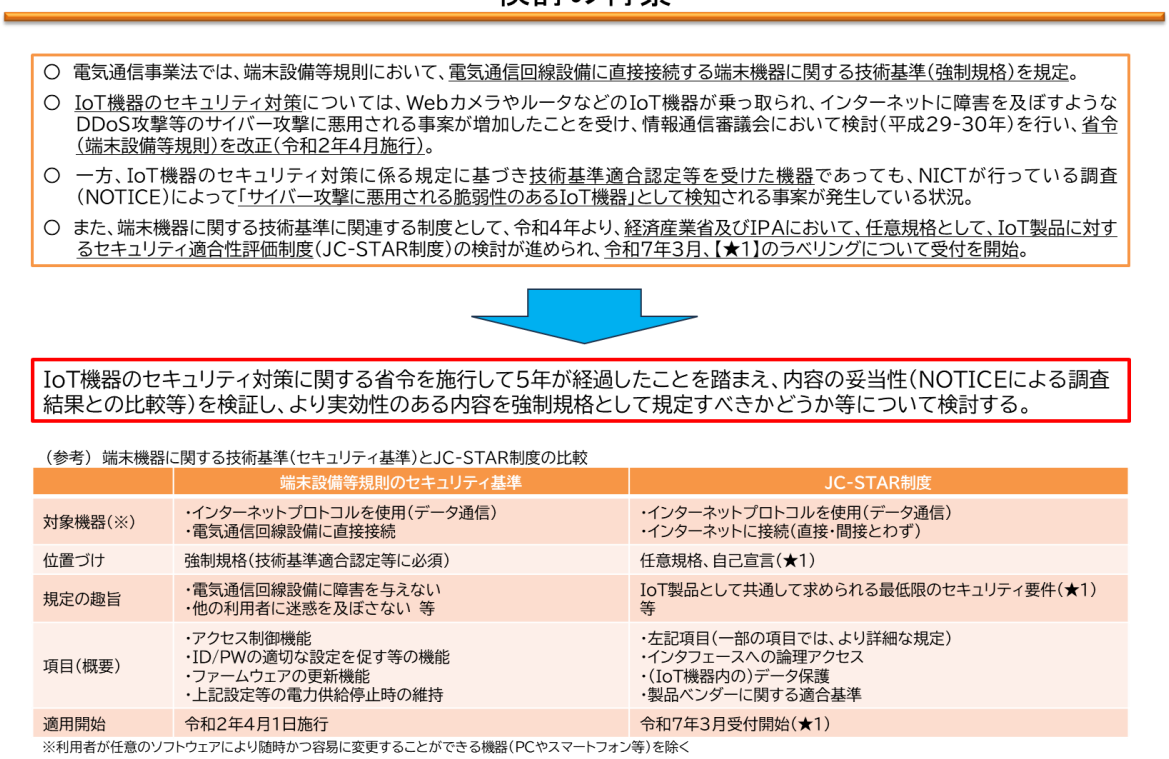


図 1.2　端末セキュリティ対策見直し検討の背景
（第 86 回委員会 事務局資料（資料 86-2）より）

第２章　IoT 機器のセキュリティ対策に関する取組状況等

2.1　IoT 機器調査（NOTICE[5]）の実施

総務省では、NICT、一般社団法人 ICT-ISAC、インターネットサービスプロバイダ（以下「ISP」という。）、IoT 機器メーカ、SIer および業界団体が連携し、IoT 機器のセキュリティ対策向上を推進することにより、サイバー攻撃の発生や、その被害を未然に防ぐためのプロジェクト（NOTICE）を平成 31 年（2019 年）２月より実施している。

NOTICE では、サイバー攻撃の予防や、被害の最小化を目的として以下の３つの活動に取り組んでいる。

- IoT 機器のセキュリティリスクの啓発と対策習慣の浸透
- IoT 機器のセキュリティ対策に関する充実した情報提供
- 危険性が高い IoT 機器の観測と管理者・利用者への注意喚起

このうち「危険性が高い IoT 機器の観測と管理者・利用者への注意喚起」については、NICT と ISP が連携を図って取り組んでいる（図 2.1）。

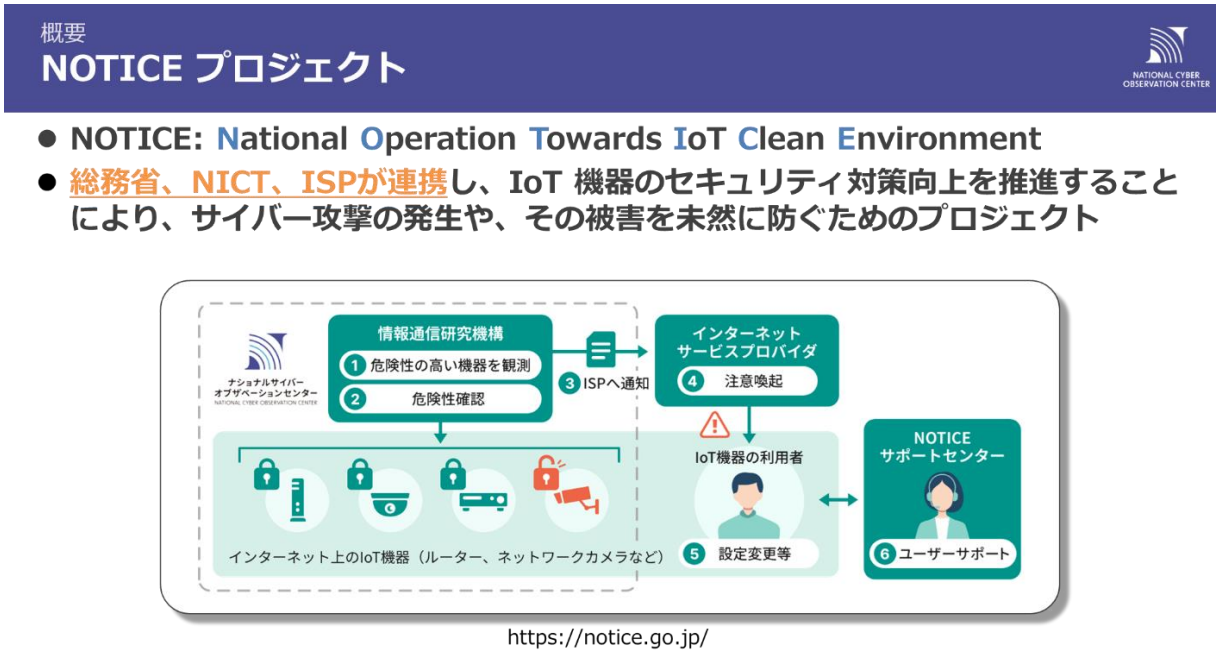


図 2.1　NOTICE 概要
（第 88 回委員会 NICT 衛藤オブザーバ説明資料（資料 88-2）より）

【実施手順[6]】

①　NOTICE に協力している ISP のネットワークに直接接続されている IoT 機器を定期的に観測（パソコンやスマホは観測の対象外）

②　①で観測した IoT 機器のうち、サイバー攻撃に悪用されている、または悪用さ

[5] National Operation Towards IoT Clean Environment

[6] https://notice.go.jp/about

れるおそれがある IoT 機器を、危険性が高い IoT 機器として特定

③　②で特定した危険性が高い IoT 機器の、グローバル IP アドレスや脆弱性などの情報を ISP に通知

④　NICT から通知を受けた ISP が当該 IoT 機器の管理者・利用者に対して、電子メールや郵便で注意喚起を実施

⑤　注意喚起を受けた IoT 機器の管理者・利用者は、IoT 機器の設定変更などのセキュリティ対策を行う

⑥　サポートが必要な方には、NOTICE サポートセンターが IoT 機器設定方法などを案内

NOTICE においては、令和７年４月時点で、毎月平均で約 1.25 億件の IoT 機器を観測している。そのうち、注意喚起の対象となったものとして、端末規則において技術基準が規定されている機能との関係では、ID/パスワードに関するもの（容易に推測可能なものを設定）が約 1.5 万件、ファームウェアに関するもの（高リスクの脆弱性がある）が約４千件観測されているなど、セキュリティリスクのある端末機器が十分な対策を講じられずにインターネットに接続されていると推測される（図 2.2）。

図 2.2　NOTICE での観測結果
（第 88 回委員会 NICT 衛藤オブザーバ説明資料（資料 88-2）より）

2.2　IoT 機器セキュリティラベリング制度（JC-STAR[7]）

JC-STAR は、令和６年（2024 年）８月に経済産業省が公表した「IoT 製品に対するセキュリティ適合性評価制度構築方針」に基づき構築された制度で、インターネットとの通信が行える幅広い IoT 製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的としている[8]。

本制度では、利用先に求められるセキュリティ水準に応じて、★１（レベル１）から★４（レベル４）を定め、適合が認められた製品には、二次元バーコード付きの適合ラベルを付与することで、製品詳細や適合評価、セキュリティ情報・問合せ先等の情報を調達者・消費者が簡単に取得できるようにしている（図 2.3、2.4）。

図 2.3　JC-STAR 概要
（第 88 回委員会　IPA 神田オブザーバ説明資料（資料 88-4）より）

[7] Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements

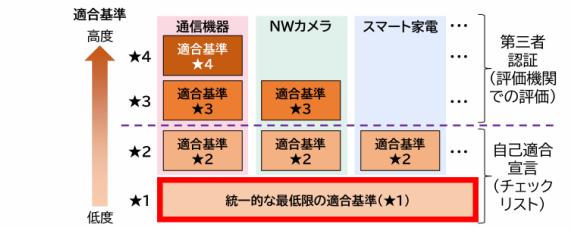
[8] https://www.ipa.go.jp/security/jc-star/index.html

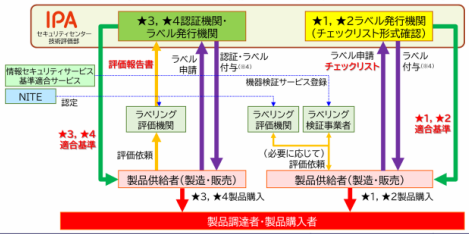
適合ラベルの適合基準

IPA

ETSI EN 303 645やNISTIR8425等とも調和しつつ、独自に定める適合基準（セキュリティ技術要件）に基づき、IoT製品に対する適合基準への適合性を確認・可視化する日本の制度

●**求められるセキュリティ水準に応じたセキュリティ技術要件**として、最低限の脅威に対応するための製品共通の適合基準・評価手順（★1）と製品類型ごとの特徴に応じた適合基準・評価手順（★2～★4）を設定





レベル	位置付け	適合基準	評価方式
★4	政府機関等や重要インフラ事業者、地方自治体、大企業の重要なシステムでの利用を想定した製品類型ごとに	製品類型別	第三者認証
★3	★1、★2に追加して汎用的なセキュリティ要件を定め、それを満たすことを独立した第三者が評価して示すもの		
★2	製品類型ごとの特徴を考慮し、★1に追加すべき基本的なセキュリティ要件を定め、それを満たすことを製品ベンダーが自ら宣言するもの		自己適合宣言
★1	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を定め、それを満たすことを製品ベンダーが自ら宣言するもの	製品類型共通	

IPAネットワーク設備委員会資料(25.06.24)　©2025 独立行政法人情報処理推進機構(IPA)　5

図 2.4　★１～★４の適合基準
（第 88 回委員会　IPA 神田オブザーバ説明資料（資料 88-4）より）

★１の適合基準は、最低限の脅威に対抗できるものとして設定されており、また、適合基準への評価は、製造者の自己適合宣言で対応できるものとなっている。★１で実現すべき対策（図 2.5）は、端末規則で求めている技術基準の内容のほか、データ保護やセキュリティに関する情報提供まで広範に及んでおり、一部の対策については、電気通信事業法に基づく端末機器セキュリティに係る技術基準を含めた技術基準適合認定等を取得していれば、★１の適合基準に適合しているとみなされる。

★1のセキュリティ要件・適合基準

IPA

★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。

IPAネットワーク設備委員会資料(25.06.24)　©2025 独立行政法人情報処理推進機構(IPA)　10

図 2.5　JC-STAR ★１で IoT 機器に求める適合基準
（第 88 回委員会　IPA 神田オブザーバ説明資料（資料 88-4）より）

2.3　IoT 機器のセキュリティ対策に関する海外の状況

機器を対象としたセキュリティ認証については、政府調達機器の一部に関して、国際標準 ISO/IEC15408 に基づく CC（Common Criteria）認証がある。CC 認証は、情報技術セキュリティの観点から、情報技術に関連した製品およびシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格であり、日本を含む認証国（18 ヶ国）で認証された認証製品は CCRA 加盟国（36 ヶ国）で相互承認される。端末規則においても、当該認証を受けている端末機器はセキュリティ基準を満たすこととしている。

また、IoT セキュリティ対策に関する国際標準は、ISO/IEC JTC 1/SC 27 および ISO/IEC JTC 1/SC 41 において検討が進められていたが、我が国からの提案[9]が国際標準規格として成立し、令和３年５月に出版された。

2.3.1　米国における動向

米国では、令和２年 12 月に「IoT サイバーセキュリティ改善法（IoT Cybersecurity Improvement Act）」が成立した。この法律では、米国国立標準技術研究所（NIST）に対して、

① IoT デバイスの安全な開発、ID 管理、パッチ適用、および構成管理などのガイドライン発行

② 米国行政管理予算局（OMB）がガイドラインに基づく活動を行っているかのチェック

を求めている。NIST では上記①を踏まえ、IoT サイバーセキュリティの目的、リスク、脅威の分析および国際標準化状況を整理した「NIST IR 8200」を基に、政府調達における適切なセキュリティ管理の推奨事項を示した「NIST IR 8259」を令和２年５月に公表した[10]。

上記法令（連邦法）のほか、各州で適用される州法において規制しているものもあり、その１つであるカリフォルニア州 IoT セキュリティ法では、直接/間接的にインターネットに接続される製品に対して、ローカルエリアネットワーク外への認証手段を備える場合、以下のいずれかを実装することを求めている。

- 製品ごとにプログラムされたユニークなパスワード設定
- 利用開始前に、ユーザにパスワードを設定させる機能

2.3.2　英国における動向

英国では、消費者向け IoT 製品の設計段階で安全性が確保され、製品の開発、製

[9] ISO/IEC JTC 1/SC 41 に提案していた、「ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes」

[10] IoT サイバーセキュリティ改善法による①に基づき、令和３年 12 月に連邦政府機関が IoT 機器を調達する際に調達先に求めるべき要件を示した「NIST SP 800-213 文書群」を公表し、その中で「NIST IR 8259」を参照する形式をとっている。

造、販売に携わる利害関係者を支援することを目的として「消費者向け IoT 製品のセキュリティに関する行動規範」を平成 30 年に作成した[11]。この行動規範では、初期パスワードの設定や脆弱性に関する情報の公開方針、ソフトウェアの定期的な更新等の 13 項目のガイドラインを規定している。

また、IoT 製品のサイバーセキュリティ対策、通信インフラ強化を目的として「PSTI 法（Product Security and Telecommunication Infrastructure Act)」が令和４年 12 月に成立、令和６年４月に施行された[12]。この法律では、IoT 機器に対して設定するパスワードは、以下のいずれかであることを必須としている。

- 機器毎に一意であること[13]
- 機器の利用者によって設定されること

2.3.3 欧州における動向

欧州では、欧州電気通信標準化機構（ETSI）が、IoT 機器の開発・製造に関わる関係者に対し、製品をセキュアにするガイダンスを提供するため、「民生用 IoT 機器のサイバーセキュリティ：基本要件（Cyber Security for Consumer Internet of Things: Baseline Requirements、以下「EN 303 645」という。)」[14]を令和２年に作成した。EN 303 645 では、ネットワークインフラに接続される民生品 IoT 機器に対して、14 のサイバーセキュリティ規定・データ保護規定を設定している。

また、欧州市場に流通される IoT 機器のサイバーセキュリティ確保を主な目的として、「サイバーレジリエンス法（Cyber Resilience Act)」が令和６年 12 月に発行され、令和９年 12 月から EU 域内で適用予定となっている[15]。サイバーレジリエンス法は強い強制力を持っており、デジタル要素を含む製品全般を対象として、設計から廃棄までのライフサイクル全般にわたるセキュリティ対策を義務化しており、当該法に準拠しない製品は、EU の市場での販売は不可となる。

2.3.4 IoT 機器に対するラベリング制度

IoT セキュリティに関して、任意規格となるラベリング制度により確認・担保している国がある。そのうちの１つであるシンガポールにおいて、令和２年より運用されている「サイバーセキュリティラベリングスキーム（Cybersecurity Labelling Scheme)」[16]は、EN 303 645 を参考にした評価基準により、民生用 IoT 機器全般に対する格付けを行っている。ラベルを付与された機器はホームページ等で確認するこ

---

[11] https://assets.publishing.service.gov.uk/media/605e41e7d3bf7f717efe1f2f/054718_DCMS_IoT_Code_of_Practice_JAPANESE_V2.pdf

[12] https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

[13] 「一意であること」の例示ついても法律で示している。

[14] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

[15] https://www.cyberresilienceact.eu/ja/

[16] https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about

とができる[17]（図 2.6）。

IoTセキュリティに関する海外の状況について②

○ IoT機器に対するラベリング制度（一部）

	アメリカ	シンガポール	（参考）欧州
制度名	U.S. Cyber Trust Mark （2025年～）	Cybersecurity Labelling Scheme （2020年～）	ETSI EN 303 645（規格名）
対象機器	インターネット接続機器、消費者向けスマートデバイス等（制度開始時は無線機器を対象）	Wi-Fiルータ、スマートホームハブ、IPカメラ、スマートプリンター等の消費者向けIoT機器全般	ネットワークインフラに接続される民生用IoT機器
評価基準	以下の基準を満たす機器にラベル付与 ・一意で強力なデフォルトパスワードの使用 ・適切なデータ保護 ・適切なソフトウェアの更新 ・インシデント検出機能 ※技術的な適合基準は、NISTが公表したIR 8425（Profile of the IoT Core Baseline for Consumer IoT Products）に準拠	機器が受けた試験・評価に応じて以下の格付け レベル１：基本的なセキュリティ要件（固有のデフォルトパスワード設定、ソフトウェアアップデートの提供等） レベル２：レベル１＋セキュリティ・バイ・デザインの原則に基づいた製造 レベル３：レベル２＋第三者機関によるソフトウェア・バイナリ評価 レベル４：レベル３＋第三者機関による構造化ペネトレーションテスト ※EN 303 645を参考	14のサイバーセキュリティ規定・データ保護規定を設定 ・汎用のデフォルトパスワードを使用しない ・ソフトウェアを最新の状態に保つ ・セキュア通信 ・露出した攻撃面の最小化 ・ソフトウェアの完全性確保 ・停止に対してレジリエントなシステム 等
確認方法	ラベルにはQRコードが付与されており、デフォルトパスワードの変更手順やデバイスを安全に構成する手順、自動更新の詳細、デバイスのアップデートを提供していない場合の通知情報等を確認可	ラベルにはQRコードが付与されており、製品情報やセキュリティポリシー、サポート期間、アップデート情報等を確認可	－
その他	・ラベルの使用を認証するサイバーセキュリティラベル管理者として11社を認定 ・BestBuy, AMAZON等が消費者向けに同制度の啓蒙を行い、ラベル製品が目立つように陳列・表示（予定）	・サイバーセキュリティラベリングの相互承認に関して、類似の取組を行っているフィンランドとMOU、ドイツおよび韓国とMRAを締結（ドイツはレベル2以上、フィンランドと韓国はレベル3以上）	・欧州をはじめ世界各国で採用

図 2.6　IoT 機器に対する各国のラベリング制度
（第 89 回委員会 事務局資料（資料 89-2）より）

[17] https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/product-list/

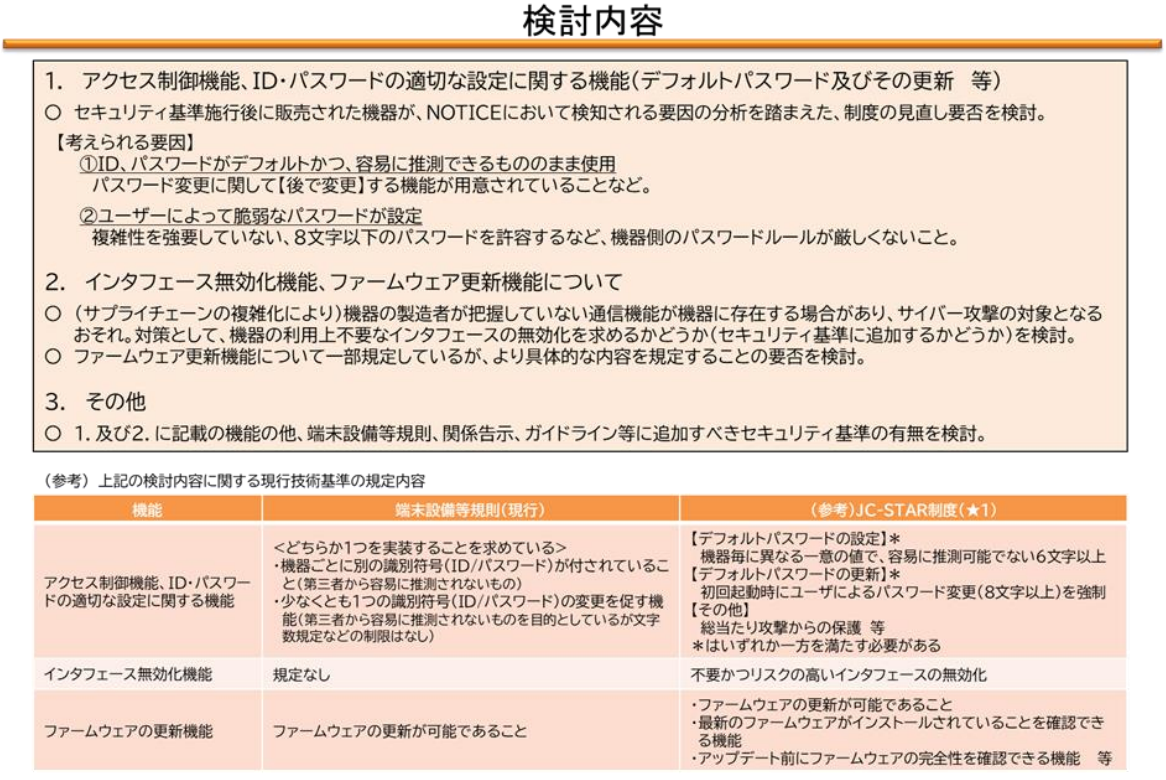
第３章　端末設備の技術基準に追加すべきセキュリティ基準の内容

今回の検討は、現行の端末規則で規定されているセキュリティ対策に関する技術基準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。

このため、現在規定されている技術基準の見直しの要否や、新たに端末規則で要求すべきセキュリティ対策の有無を把握するため、以下の項目について、外部有識者及び関係団体からヒアリングを行い、検討を実施した。

- アクセス制御機能、ID/パスワードの設定機能について
- ファームウェアの更新機能について
- インタフェースの無効化機能について
- その他（上記機能の他、端末規則や関係告示、「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（以下「端末ガイドライン」という。）」[18]等に規定すべき事項等）

各機能に関する検討結果について、3.1 から 3.3 までにそれぞれ記載する。また、各機能に共通して、同一の機能（要件）に対する基準は、端末規則で規定される技術基準と JC-STAR で規定されている適合基準とで同一にすることが望ましいとの意見が、委員会構成員、外部有識者及び関係団体から多数見られた。



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

図 3.1　セキュリティ基準の見直しにあたり検討する内容
（第 88 回委員会 事務局資料（資料 88-1）より）

[18] https://www.soumu.go.jp/main_content/000705080.pdf

3.1　アクセス制御機能、ID/パスワード設定機能の見直し

3.1.1　現状

アクセス制御機能､アクセス制御の際に使用する ID/パスワードの設定機能のうち、ID/パスワード設定機能については、端末規則において以下の要件のいずれかを具備することを求めている。

①　当初より端末機器ごとに一意の 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/パスワードの変更をユーザに促す機能

また、当該機能は、アクセス制御の際に使用する識別番号（ID/パスワード）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いる旨が端末ガイドラインに記載されている。

一方、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している。

この要因として、主に上記②の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に設定した ID/パスワード（デフォルト ID/パスワード）が簡便なものであり、かつ、ユーザがそのまま使用しているケースが考えられる。これは、端末機器がユーザに ID/パスワードの変更を促しているものの、後で変更する機能が用意されている[19]ことなどによるものである。また、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（図 3.2）。

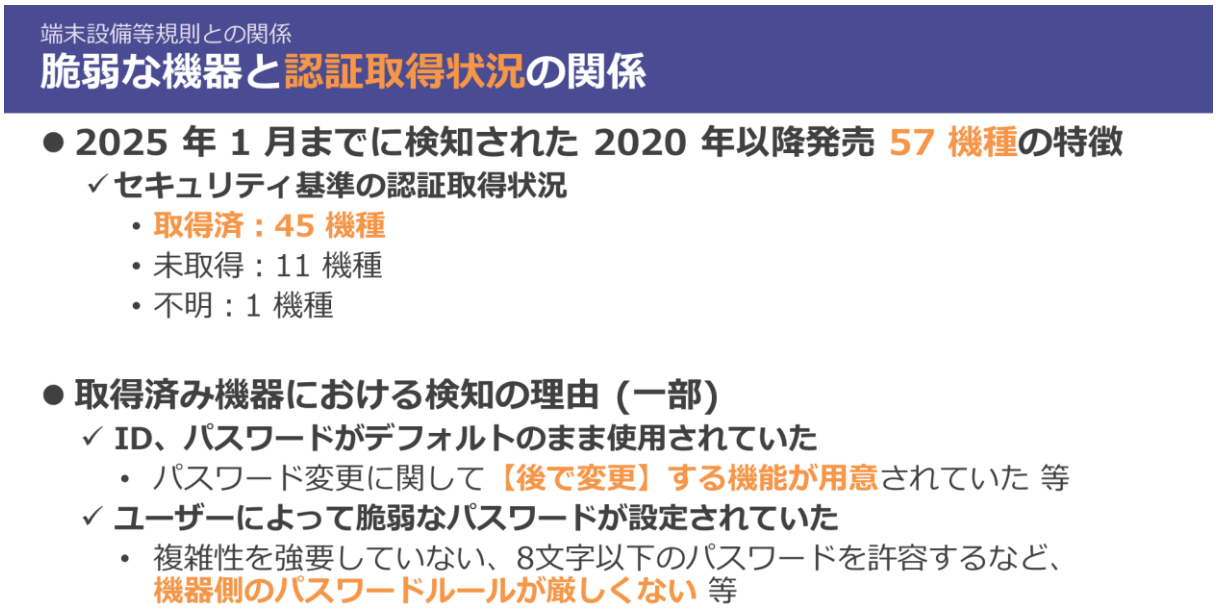


図 3.2　セキュリティ基準認証取得済み機器が検知される理由
（第 88 回委員会 NICT 衛藤オブザーバ説明資料（資料 88-2）より）

[19] 「後で変更する」のボタン等を押下すれば変更を行わずとも利用し続けることが可能となる。

3.1.2　課題

3.1.1 に記載されているように、端末規則の規定に基づき、「②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ため、現行の技術基準は、セキュリティ対策として脆弱性があると考えられる。その上、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ため、セキュリティ対策として脆弱性があると考えられる。

また、「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」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端末ガイドラインに記述があるのみで、法令上規定されていない。

3.1.3　検討結果

現状及び課題を踏まえ、現行規定の「②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」については、ID/パスワードの少なくとも１つの変更を「促す」ことを求める機能ではなく、変更を「させる」ことを求める機能へ見直すことが適当である。また、デフォルト ID/パスワードの設定および当該 ID/パスワードからの変更にあたっては、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明示することが適当である。

ただし、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[20]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である。

3.2　ファームウェア更新機能の見直し

3.2.1　現状

IoT 機器のサイバー攻撃を観測した調査結果では、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（図 3.3）。また、機器個別の脆弱性が狙われるようになっている。3.1 項で検討したアクセス制御機能、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であるが、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になってくる。

[20] JC-STAR においては、①メーカが設定するデフォルトパスワードは IoT 機器毎に異なる一意であり、６文字以上（覚えやすい人名、地名などを用いない等の制約あり）とすること、②IoT 機器の初回起動時にユーザによるパスワード変更を必須とし、文字数も８文字以上を強制させる機能のいずれかを実装することを求めている。

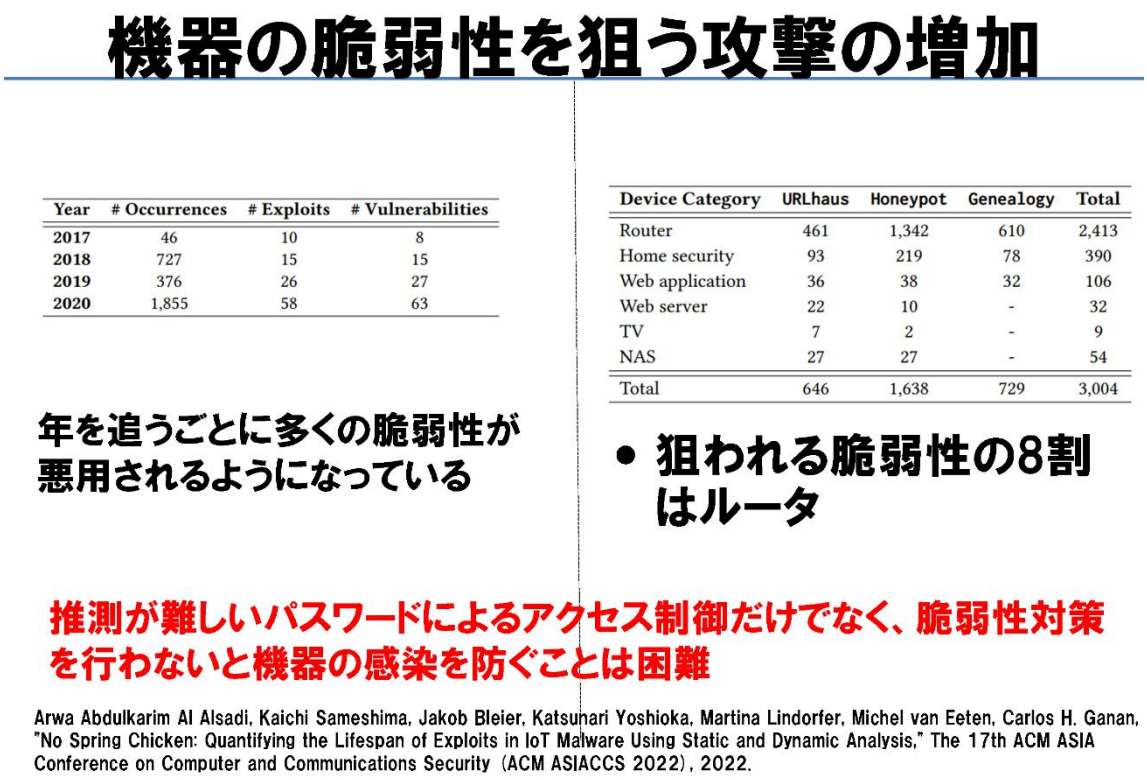


図 3.3　IoT 機器のサイバー攻撃を観測した調査結果
（第 88 回委員会 横浜国立大学 吉岡オブザーバ説明資料（資料 88-3）より）

機器個別の脆弱性対策として有効であるファームウェアの更新機能については、端末規則において「電気通信の機能に係るソフトウェアを更新できること」と規定されている。また、端末ガイドラインにおいて、「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」とされている。

3.2.2　課題

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となる。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、更新の徹底が必要である（図 3.4）。

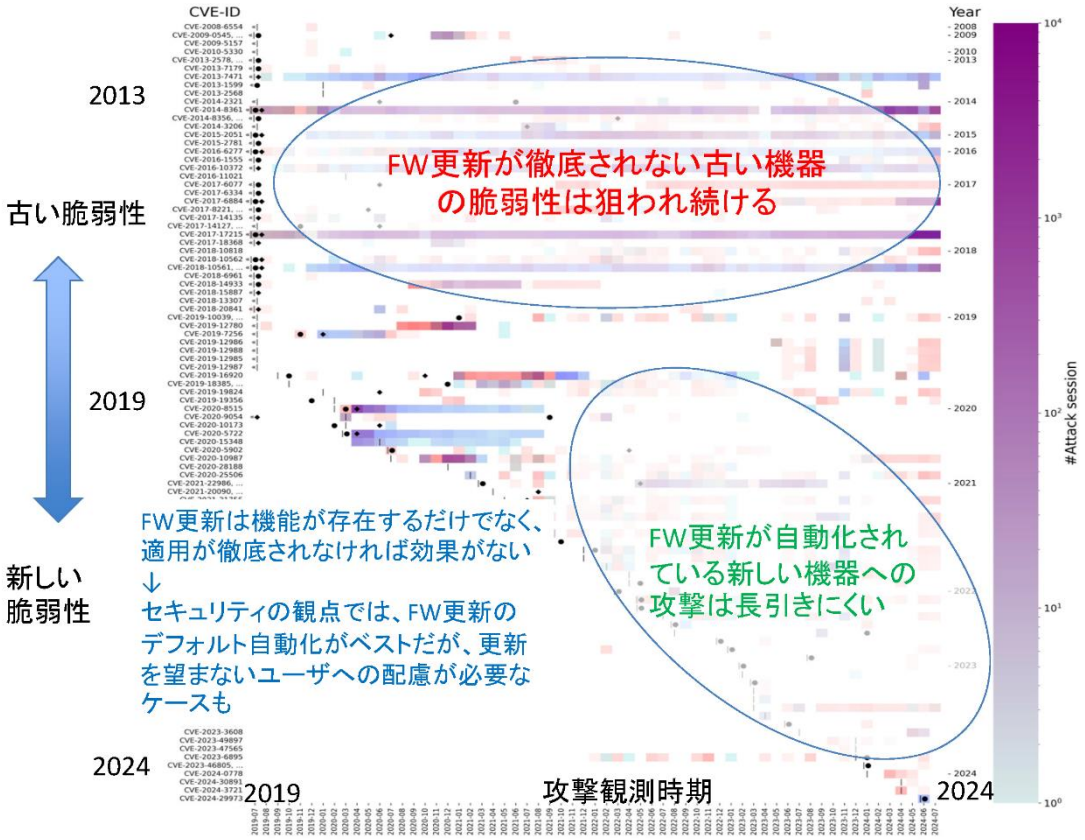


図 3.4　ファームウェア更新による脆弱性対策効果
（第 88 回委員会 横浜国立大学 吉岡オブザーバ説明資料（資料 88-3）より）

この点、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になる。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には、当該更新について、具体的な基準（指標）を規定する必要がある。

3.2.3　検討結果

現状及び課題を踏まえ、ファームウェアの更新にあたっては、ユーザが自発的に（脆弱化対策にかかる）ファームウェア更新を行うことができる（更新が徹底される）よう、「更新できる」機能に加えて、「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[21]の確認機能」の具備を求めることが適当である。その際、容易かつ分かりやすい手順でユーザがアップデートを実行可能とすることが望ましい。

また、脆弱性対策という観点ではセキュリティに関するファームウェア更新は自動的に実施されるようにすることが効果的な方策であると考えられる。これについては、平成 30 年のセキュリティ基準検討の際に、「更新は安全かつ自動で行われることが推奨されるが、IoT 機器は多種多様であり、更新の手法は機器の種別毎に異なることか

[21] 開発されたソフトウェアが、その仕様や要求に対して正確に動作すること。

ら、安全かつ自動の更新までは要件としない。」と整理[22]し、3.2.1のとおり、現在の端末規則では規定されず、端末ガイドラインに当該整理の趣旨が記載される形となっている。

今般の検討においても、ファームウェア更新には、脆弱性対策だけでなく更新対象となる端末機器の機能拡張・改善のために実施されるものも含まれ、端末機器の機能拡張・改善に関するものはユーザの判断に依存する（更新を望まないユーザも存在）ものであるとの意見や、ファームウェアの更新はセキュリティ以外の機能に影響を及ぼすことがあり、最新版の適用がそぐわない場合もあるとの意見があった。

これらを踏まえ、自動更新については（平成30年の検討結果と同じく）「推奨するが要件としない」こととすることが適当であるが、（代替手段として）ユーザが更新の自動化を希望する場合に対応できる機能を実装することが望ましい[23]。

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

3.3.1 現状

不要なインタフェースへの物理的/論理的なアクセスに関する規定は、端末規則に規定されていない。これは、平成30年の検討では、当時発生していたマルウェア「Mirai」による大規模DDoS攻撃（IoT機器のマルウェア大規模感染）を防止することを目的とするセキュリティ対策について、電気通信事業法における端末設備の接続の技術基準の枠組み（電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさない）の中で、最低限の技術基準の追加を検討したためである。

3.3.2 課題

現在、製造されている端末機器は、他社から調達したチップセットを組み込む、外注により製造する等、サプライチェーンの複雑化により、製造者（技術基準適合認定等を受けようとする者）も把握・想定していない通信機能が当該機器に存在（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。）していることがある（図3.5）。

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である。

この点に関連して、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。しかしながら、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、前段のような通信機能についての確認は十分になされ

[22] 検討の際、更新主体（だれが責任を持つのか）や更新手段（ネットワーク経由、保守、回収）も含めた議論を行った。

[23] ETSI「EN 303 645」において、ファームウェア更新自動化に対して求める要件として「セキュアアップデートメカニズムの１つは、自動化するように設定可能であるべきである。」、「初期化中に、消費者向けIoTデバイスは、ユーザの同意を得た後、自動で安全な更新メカニズムを有効化することが望ましい。」とある。

ていないおそれがある。

事例：大学内の脆弱IoT機器調査

- 横浜国大内で動作する機器について網羅的な調査を実施（2021-2022）
- Telnetが動作するIoT機器116件（36モデル）を検出
- マニュアルが取得できたTelnetが動作する機器30モデルのうち、15モデルでTelnetに関する記載が全くなし．5モデルではTelnet利用目的の記載なし．
- 22モデルについて、Telnetの利用目的を問い合わたところ，5モデルは目的不明、1モデルはTelnet自体を知らないと回答．
- メーカであっても、自社製品で動作するネットワークサービス（通信機能）を完全に把握している訳ではない（チップベンダ提供のFW利用や開発の外注が背景）
- 過去に横浜国大がマルウェア感染の注意喚起を行った際、製造者が自社製品で動作するTelnetを認識していなかった事例が多く存在（ルータ等）

Device Type	Telnet or FTP	Telnet	FTP
Smart card reader	53 (2)	53 (2)	53 (2)
Printer/Multi-function printer	38 (27)	21 (16)	36 (25)
Electric current monitor	13 (2)	13 (2)	11 (1)
Display controller	11 (1)	0 (0)	11 (1)
NAS	11 (10)	1 (1)	10 (10)
Announcement broadcast system	8 (1)	0 (0)	8 (1)
Data logger	6 (2)	0 (0)	6 (2)
Earthquake early warning system	6 (2)	6 (2)	0 (0)
L2 switch	5 (2)	5 (2)	0 (0)
Wireless LAN access point	4 (2)	4 (2)	0 (0)
UPS	4 (2)	4 (2)	1 (1)
Wireless LAN controller	3 (1)	0 (0)	3 (1)
Energy monitor	3 (1)	0 (0)	3 (1)
Router	3 (1)	3 (1)	0 (0)
Network adapter for printer	2 (2)	2 (2)	2 (2)
Web camera	2 (2)	1 (1)	2 (2)
Black and white printer	2 (1)	0 (0)	2 (1)
Paperless recorder	1 (1)	0 (0)	1 (1)
HPLC controller*	1 (1)	1 (1)	0 (0)
Web conferencing system	1 (1)	1 (1)	0 (0)
Power supply Control	1 (1)	1 (1)	0 (0)
Backup storage	1 (1)	0 (0)	1 (1)
Total (IoT devices identified model No.)	179 (66)	116 (36)	150 (52)

* High-Performance Liquid Chromatography (HPLC) controller

Takayuki Sasaki, Takaya Noma, Yudai Morii, Toshiya Shimura, Michel van Eeten, Katsunari Yoshioka, and Tsutomu Matsumoto, "Who Left the Door Open? Investigating the Causes of Exposed IoT Devices in an Academic Network," Proc. 45th IEEE Symposium on Security and Privacy (IEEE S&P 2024), 2024.

図 3.5　不要なポートの設定状況調査
（第 88 回委員会 横浜国立大学 吉岡オブザーバ説明資料（資料 88-3）より）

3.3.3　検討結果

現状及び課題を踏まえ、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が適当である。

その際、物理的なインタフェースの無効化の確認は比較的容易に行うことができるが、プロトコルのポート等の論理的なインタフェースについては確認が難しいため、マルウェアの侵入等に使われる代表的なポートを明示し、当該ポートの無効化について確認することとすべきとの意見や、製造者の宣言では実効性の確認が困難な面があるとの意見があったことから、これらの意見も踏まえた制度とすることが適当である。

3.4　その他

今回 3.1 から 3.3 までにおいて検討した各機能に対して具体的に求める基準等（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）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である。

また、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は、現在、

端末ガイドラインにおいて、書面による確認の方法が記載されている。今回の検討に基づく見直しによって、インタフェースの無効化や、ファームウェア更新に関する追加の確認事項等について新たに技術基準が追加されるにあたり、これらの事項について、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、今回検討した各機能に対する審査方法についても、書面による確認（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、端末機器が技術基準に適合していることを審査する形式）とすることが適当である。

その際、セキュリティ要件の対象となる機器の審査が円滑に行われるよう、その審査方法等について、電気通信事業者、機器メーカ等の関係者の意見も踏まえて、端末ガイドラインに記載することが適当である。

第４章　技術基準適合認定等の対象機器の範囲（電気通信回線設備に間接的に接続する端末機器の扱い）

現在の端末規則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。

セキュリティの観点では、図 4.1 中央のルータ（無線 LAN ルータ）を介して電気通信回線設備に接続される端末機器（間接的に接続される端末機器）を含む、インターネットプロトコルを使用する全ての機器に対し、セキュリティ対策を求めることが理想的であるが、平成 30 年のセキュリティ基準検討の際に、「現状において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、セキュリティ要件が追加された技術基準適合認定等の対象についても、従来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である。」と整理したものである。

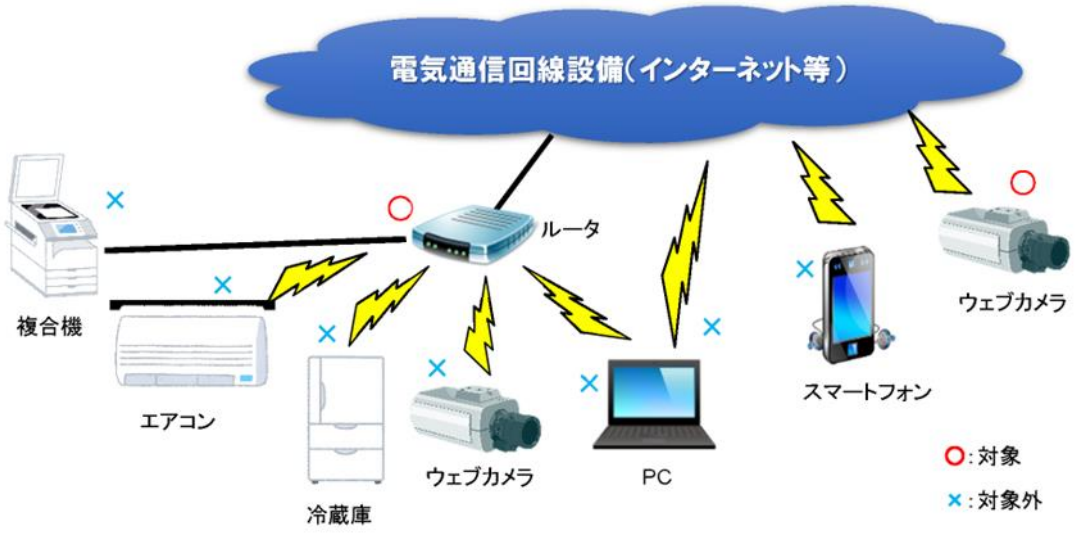


図 4.1　電気通信事業法における技術基準適合認定の対象となる端末機器
（電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第２版）より）

今回の技術基準の見直しの検討にあたり、電気通信回線設備に間接的に接続される端末機器への技術基準適用の要否についても検討を実施した。その際、JC-STAR が直接・間接を問わずインターネットにつながる機器を対象としていることも踏まえ、電気通信回線設備に間接的に接続する端末機器のセキュリティ対策には JC-STAR を活用しつつ、電気通信回線設備に直接接続する端末機器のセキュリティ対策については、端末規則に規定する技術基準を強化していくという方向の対応が望ましい等の意見があった。

これを踏まえ、技術基準の見直し後における端末規則のセキュリティ基準の対象機器の範囲は、現在と同様に、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である。なお、電気通信回線設備に間接的に接続される端末機器への技術基準適用の要否については、技術基準の見直し後における NOTICE 等での検知状況等も活用しつつ、電気通信回線設備に直接接続される機器のセキュリティ対策の改善状況や、間

接的に接続される機器に関するリスクを検証した上で、改めて検討することが適当である。

第５章　セキュリティ基準の追加・見直しに係る経過措置

端末規則では、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は、制度改正等により技術基準に具備すべき新たな機能が追加された場合であっても、当該新たな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（「従前の技術基準とすることができる」旨を規定した経過措置）を講じてきた。

端末機器のセキュリティ基準については、平成 30 年の検討の際に以下①、②の経過措置を設けることが適当であるとされ、②に基づき、セキュリティ基準を含めた技術基準適合認定等を受けなくても従前の技術基準適合認定等が有効であると扱われる経過措置[24]が講じられた。

① 端末設備の接続の技術基準へのセキュリティ要件の規定の追加が制度化された場合には、IoT 機器メーカや登録認定機関等の対応を考慮して、一定の期間を設けて施行することとなるが、その期間は１年から２年程度とすることが適当

② 従来の制度に基づき、新制度の施行前に取得した技術基準適合認定等については、施行後も引き続き有効であり、当該認定等に基づく機器も引き続き使用することを可能とすることが適当

今般、技術基準の見直しの検討にあたり、経過措置の要否についても検討を実施した。その際、第３章に記載したヒアリングにおいて、端末規則のセキュリティ基準が施行される前に当たる令和元年以前に発売された端末機器が NOTICE の ID/パスワードの脆弱性調査で「脆弱な機器」として判断される件数の 83～96%を占めていることが説明された（図 5.1）。

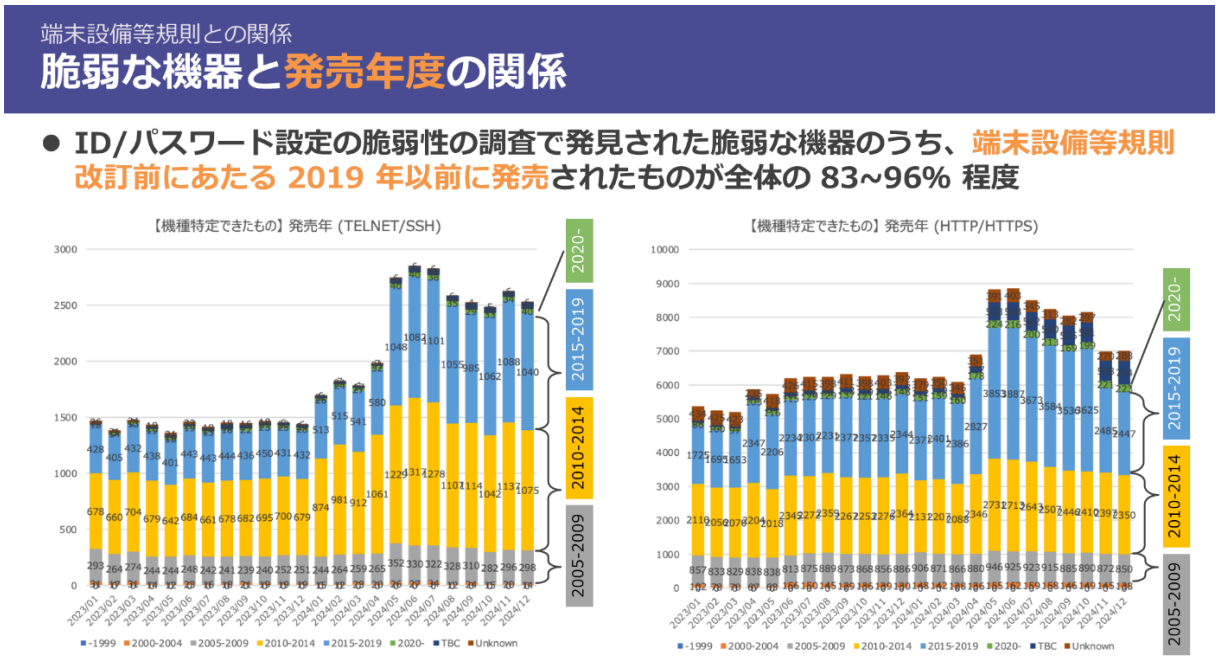


図 5.1　セキュリティリスクが高いと判断された端末機器と発売年度の関係
（第 88 回委員会 NICT 衛藤オブザーバ説明資料（資料 88-2）より）

[24] ②について措置が講じられたほか、①に関し、端末規則にセキュリティ基準を追加する省令改正は平成 31 年（2019 年）３月に公布され、令和２年（2020 年）４月に施行されており、制度化までに一定の期間が設けられた。

これまでの経過措置が一因となってこのような状況が発生していることも踏まえ、今般の経過措置の要否について、以下の意見があった。

（構成員意見）

- 電波法のスプリアス規定において、技術基準が変更されると古い機器（変更前の技術基準に対応していた機器）は（変更された技術基準に対応しない限り）使うことができない規定となっていることから、電気通信事業法においても同じような制度とすることが可能ではないか。
- 技術基準変更前に技術基準適合認定等を取得している機器で重大なインシデントが発生した場合、その原因が新しい技術基準を満たさないことによるものであれば、新しい技術基準に基づき、再度技術基準適合認定等を取得する必要があるという形にするのも考え方の一つ。
- 経過措置により、新しい技術基準を満たしていない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はないか。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。

（関係団体意見）

- 古い機器で特にセキュリティ要件を満たしていないものへの対策としては、周知活動によって買替等の効果があるので、地道な取組にはなるが、周知活動、キャンペーンを行って置き換えの推進を行うことで対応できればよいと考える。
- 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、トラブルを回避するためにも法的効力をもって利用停止や置き換えを強いることの無いよう、利用者・管理者の自発的な置き換えを促すことが最も有効な政策ではないか。

経過措置を設けることに対する要否の判断については、①経過措置を設けない場合において、新しい技術基準を導入して一定期間後には当該技術基準を満足しない端末機器は電気通信事業者から接続を拒まれ得ることとなる場合の影響と、②経過措置を設ける場合において、新しい技術基準を満たさないことになる既存の端末機器を接続可能とすることによるリスクを比較して検討を行うことが考えられる。

上記意見を踏まえて比較すると、①については、多様な利用者・管理者に大きな影響を及ぼすおそれがあるのに対し、②については、NOTICE の ID/パスワード設定の脆弱性調査において検知された端末機器について、これまでも注意喚起を通じて脆弱な機器が有意な件数減少することを確認できていること、端末機器の製造等に係る業界団体において、サポート期間が終了した脆弱な端末機器の案内を実施しているほか、脆弱なルータを「自発的に買い換えて頂く」促進運動を計画中であることなどから、一定のリスクの軽減が見込まれる。

よって、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である。また、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である。

第６章　今後の検討課題

今回の検討では、現行の端末規則で規定されているセキュリティ対策に関する技術基準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実施した。

検討を進めるにあたり、意見のあった以下の点については、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である。

- 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（第４章関係）
- 令和２年３月以前（端末規則に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、現在の端末規則で求めている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（第５章関係）

また、今回の検討は、情報通信ネットワークの安全・信頼性を確保するため、電気通信事業法に規定された端末設備の接続の技術基準における IoT 機器のセキュリティ対策の枠組みの中で見直しの検討を行ってきたものであることから、今後も、上記の継続的な注視状況を踏まえつつ、情報通信ネットワークの安全・信頼性を確保に向けて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。

別表１　IP ネットワーク設備委員会 構成員

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 構成員

（敬称略　五十音順）

	氏　名	所　属
主査	相田　仁	東京大学 特命教授
主査代理	森川　博之	東京大学 大学院 工学系研究科　教授
委員	江崎　浩	東京大学 大学院 情報理工学系研究科 教授
専門委員	朝枝　仁	国立研究開発法人情報通信研究機構 ネットワークアーキテクチャ研究室長
	石井　義則	一般社団法人情報通信ネットワーク産業協会 常務理事
	岩田　秀行	一般社団法人情報通信技術委員会 代表理事専務理事
	内田　真人	早稲田大学 理工学術院 教授
	河内　達哉 （第 91 回～）	一般財団法人　電気通信端末機器審査協会　理事長
	武居　孝 （～第 86 回）	一般財団法人　電気通信端末機器審査協会　理事長
	田中　絵麻	明治大学 国際日本学部 専任准教授
	宮田　純子	東京科学大学 工学院情報通信系 准教授
	矢入　郁子	上智大学 理工学部 情報理工学科 教授
	矢守　恭子	朝日大学　経営学部　経営学科　教授