資料89-2

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（論点整理）

令　和　７　年　８　月　４　日
ＩＰネットワーク設備委員会
総　　務　　省

セキュリティ基準見直しに係る主な意見等①

○ 第86回(5月13日)、第88回(6月24日)のIPネットワーク設備委員会において、委員会構成員、外部有識者及び端末機器関係団体の方から以下のようなご意見・ご見解をいただいた。

① 端末設備等規則の現行のセキュリティ基準に関する課題について

・ 2020年以降に販売され、セキュリティ基準の認証を所得した機器が、ID/パスワード設定の脆弱性の調査（NOTICE）において、脆弱性のある機器として発見されるケースが存在。要因としては、パスワード変更について、後で変更する機能が用意される、機器側のパスワードルールが厳しくない、などがある。

・ 端末メーカーが認識している設定・サービスだけでなく、把握していない通信機能が機器に存在する場合があり、それらが実際にサイバー攻撃の対象となっている。現在の確認手順で、そのようなケースを発見できるか確認が必要であり、不要なサービス・インタフェースが動いていないかを認定の際には確認する必要がある。

・ ファームウェア更新が徹底されない古い機器の脆弱性は狙われ続ける。ファームウェア更新は、機能が存在するだけでなく、運用が徹底されなければ効果がない。

② セキュリティ基準適用前に認定を受けている端末機器への対応について

・ 発見された脆弱な機器のうち、端末設備等規則改訂前にあたる2019年以前に発売されたものが全体の83-96%程度。

・ 現在の電気通信事業法では、一度、技術基準適合認定等を取得した端末機器は、技術基準が変わっても接続できる規定になっている。電波法では規格が変わると古いものは使えない規定になっているので、電気通信事業法においてもそのような形にすることができないか。

・ 技適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、再度技適の認証を取る必要があるという形にするのも考え方の一つ。

・ 企業に関しては、組織のガバナンスの問題として、買換えなどを含めて促していくということは大いに効果が期待できるが、個人に関しては、注意喚起をしても、用語に関する知識がなく、何をどうすればいいのか分からないとか、通知を送っても、すぐにメールを破棄されるというケースも多く見られる。周知啓発などに取り組んできた結果として、検出される2009年以前の機器の数は相対的に小さくなっているので、そのような地道な活動も必要と考える。

・ 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は、周知活動によって効果があるという、有意的な結果も示していただいたので、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。

セキュリティ基準見直しに係る主な意見等②

③ 端末設備等規則とJC-STARとの連携について

・検討を進めるにあたり、経済産業省とIPAで実施しているJC-STARとの連携を引き続き図っていただきたい。
・JC-STARで規定している適合基準の方が、サイバーセキュリティの観点では、端末設備等規則の技術基準よりも進んだものとなっている。この内容を参考にすることは問題ないが、お互いの基準が矛盾することのないように進めていただきたい。
・端末設備等規則が対象とする端末機器とJC-STARが対象とする端末機器に同じ基準が適用されることとなった場合、義務化されることによるインパクトも考慮する必要がある。
・JC-STARで規定している事項を端末設備等規則でも使うというご意見をいただいたと認識。その方向で検討を進めていただきたい。特にファームウェアのアップデートをどこまで強制とするかは、端末設備等規則の見直しの中で議論を具体化するのがよいと考える。
・間接的に接続する機器にはJC-STARを使って、直接接続する機器に対しては基準を強化していくという方向の対応が望ましいのではないか。

④ IoTセキュリティに関する海外の状況について

・技術基準を見直す場合はWTO手続きを経ることになり、過度に厳しい基準とすると、昨今話題となっている非関税障壁の話も出てくるため、諸外国の状況も踏まえた検討や規制の対象を絞るといった考え方もあるのではないか。

⑤ その他

・上位法令で義務化すると硬直化・時代の進展に合わなくなる可能性がある。
・健全な国内市場の維持、不適合機器の排除の観点から、（今般の見直し事項の一部がガイドラインに記載される場合、）ガイドラインが公開されている認証を取るときの審査基準であり、ガイドラインに従わなければ電気通信事業法の技術基準適合認定等は取れないという強制力のある形で規定されることを想定。

セキュリティ基準の見直しに係る論点

○ アクセス制御・ID/パスワード設定機能

- 現行の基準は、①デフォルトパスワードの変更を「促す」ことが要件とされている、②ユーザが変更するパスワードに複雑性を求めていない（パスワードのルールが厳格ではない）ことが、NOTICEでの脆弱性検知理由となっていると考えられる。
- そのため、より具体的な基準（指標）を規定することが適当ではないか（例：ID/パスワードは「容易に推測されない」もの、パスワードについては変更を「促す」ではなく「させる」機能の実装　等）。ただし、具体的な数値等を規定する場合、セキュリティの考え方の変遷に柔軟に対応できるよう、ガイドラインに記載することが適当ではないか。

○ ファームウェア更新機能

- ファームウェア更新機能について、最新の脆弱性対策が適用されることで攻撃対象となるリスク軽減につながることから、当該機能についても具体的な基準（指標）を規定することが適当ではないか（例：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を有すること、アップデート前のソフトウェア完全性の確認機能を有すること　等）。
- また、ファームウェア更新が自動化されている新しい機器への攻撃は長引きにくいという調査結果を踏まえ、「ファームウェア更新のデフォルト自動化」を求めることについてどう考えるか。その際、以下の点を考慮する必要がある。
  - ✓ 更新を望まないユーザへの配慮や、ユーザの判断に依存する機能拡張・改善のための更新とセキュリティアップデートが区別困難なこと
  - ✓ 「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と
  - ✓ 現行基準の検討時、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）も含めた議論となった結果、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として、自動更新は推奨されるが要件とはしないと整理されたこと

○ 不要なインタフェースの無効化機能

- 機器製造者自身が把握していない通信機能がサイバー攻撃の対象になることを防止するため、「不要かつリスクの高いインタフェースの無効化機能」を新たな技術基準として規定することが適当ではないか。

○ その他

- 各機能の技術基準の詳細は、インターネットに直接/間接的に接続されるIoT機器での採用が進められている、任意基準であるJC-STARで定めている個々の適合基準と大きく乖離しない（同じ端末機器であっても、使い方により電気通信回線設備に直接的にも間接的に接続される現状を踏まえた）方向で見直しを行うことが適当ではないか。（「同一の要件は同一の基準」の観点）
- 対象とする端末の範囲は、前回のセキュリティ基準検討時と同様、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ではないか。間接的に接続される端末については、今回の見直し後に実施されるNOTICE等での検知状況等を踏まえ、間接的に接続する端末機器への技術基準適用について改めて検討することが適当ではないか。
- 登録認定機関等の審査は実機テストにて行うか、書面にて行うか（現行のセキュリティ規定は書面にて確認）。

【参考】端末設備等規則とJC-STARの規定の比較

①現行のセキュリティ基準に存在する項目

	端末設備等規則（現行）	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	<デフォルトパスワードおよびその更新についてどちらか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およびその更新についてどちらか1つを実装することを求めている> ・機器毎に異なる一意の値で、容易に推測可能でない6文字以上のパスワードであること ・初回起動時にユーザによるパスワード変更を必須とする機能を実装し、当該機能において設定可能なパスワードとして、8文字以上のパスワードを強制させる
	-	IoT機器に対するネットワークを介したユーザ認証の仕組みについて、以下のいずれかに類する仕組み又はそれ以上の仕組みにより総当たり攻撃を困難とすること ・認証試行の連続失敗に対し、認証試行制限の対応をしている ・多要素認証が使用されている
ファームウェア（ソフトウェア）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する手段を有すること。 ・ユーザがアップデートを適用する際、容易かつ分かりやすい手順でファームウェアのアップデートを実行可能とすること ・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。

②現行のセキュリティ基準に存在しない項目

カテゴリ	JC-STAR制度（★１）
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（物理的、論理的な通信ポート等）
（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、物理的保護による保存　等） ・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） ・製品内に保存される守るべき情報の削除機能

セキュリティ基準適用前に認定を受けている端末機器への対応について

【論点】

○ 制度改正等により、技術基準に変更があった場合の措置

・ 現行の技適制度では、一度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をとってきている（「経過措置」により従前の技術基準によることができることを規定。）。

・ 今般、技術基準を見直した場合に、以下の機器について、同様の経過措置を規定するべきか。それとも、見直し後の技術基準への対応を求めるべきか。

  ✓ 現在の技適制度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

  ✓ セキュリティ基準施行前（2020年３月以前）に認定等を受けた端末機器（脆弱性を持ち続けているおそれ）

・ 上記の検討に当たっては、新技術基準導入の一定期間後には当該基準を満たさない機器は接続を拒まれ得ることとなる場合の影響と、（新技術基準を満たさない可能性のある）既存機器を接続可能とすることによるリスクの比較が必要ではないか。その際、以下の点も考慮し、これまでと同様の経過措置を規定することを基本とし、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はないか。

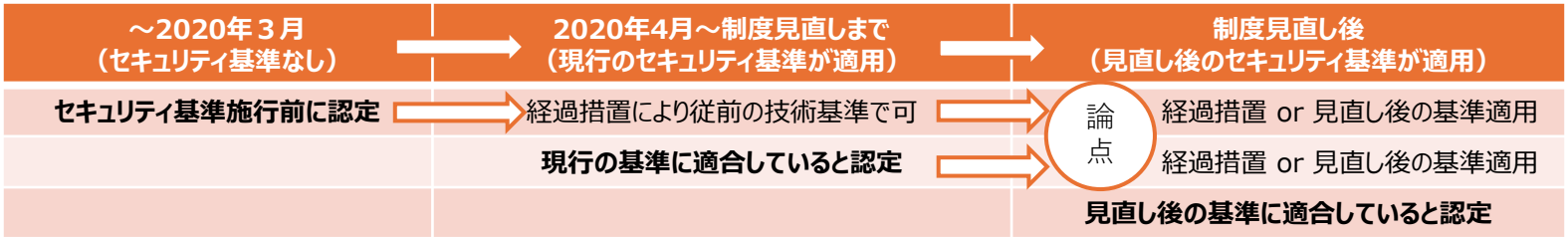
  ✓ ID/パスワード設定の脆弱性調査において、注意喚起を通じて脆弱な機器が有意な件数減少することを確認できていること

  ✓ 既存機器にも新技術基準を適用する場合、それにより技術基準を満たさなくなった端末機器を利用者が接続することを防止できるような、実効性のある制度の構築・運用が困難（技術基準を満たしていない機器が使用され続けるおそれ）

  ✓ 電波法の「無線設備のスプリアス発射の強度の許容値」においても、平成17年12月の新たな許容値の適用に当たり、旧スプリアス規格の無線設備の使用期限は令和４年11月30日（後に、当分の間延長）とされている

○ 古い機器の脆弱性について、利用者の認識を高める方策（ベンダー等の協力も得た周知の強化 等）

（参考）JC-STARでは、適合ラベルの有効期間は２年（延長申請可能）。また、有効期間内はセキュリティに関するアップデートを義務付け



（参考）現行のセキュリティ基準策定時に設定した「経過措置」

この省令による改正前の端末設備等規則の条件に適合する端末設備又は自営電気通信設備であって、第一条の規定の施行の日前に電気通信事業法（以下「法」という。）第五十三条第一項に規定する技術基準適合認定、法第五十六条第一項に規定する設計認証、法第六十九条第一項の規定による端末設備の接続の検査若しくは法第七十条第二項の規定による自営電気通信設備の接続の検査を受け、又は法第六十三条第三項の規定による技術基準適合自己確認の届出を行ったものの技術基準については、なお従前の例によることができる。

【参考】電気通信事業法における端末機器の接続等に関する主な規定

（端末設備の接続の技術基準）

第五十二条　電気通信事業者は、利用者から端末設備（中略）に接続すべき旨の請求を受けたときは、その接続が総務省令で定める技術基準（中略）に適合しない場合その他総務省令で定める場合を除き、その請求を拒むことができない。

2　前項の総務省令で定める技術基準は、これにより次の事項が確保されるものとして定められなければならない。

一　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。

二　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。

三　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。

（表示が付されていないものとみなす場合）　※設計認証に基づく端末機器については、第61条で準用

第五十五条　登録認定機関による技術基準適合認定を受けた端末機器であつて第五十三条第二項又は第六十八条の八第三項の規定により表示が付されているものが第五十二条第一項の総務省令で定める技術基準に適合していない場合において、総務大臣が電気通信回線設備を利用する他の利用者の通信への妨害の発生を防止するため特に必要があると認めるときは、当該端末機器は、第五十三条第二項又は第六十八条の八第三項の規定による表示が付されていないものとみなす。

2　総務大臣は、前項の規定により端末機器について表示が付されていないものとみなされたときは、その旨を公示しなければならない。

（表示の禁止）

第六十条　総務大臣は、次の各号に掲げる場合には、認証取扱業者に対し、二年以内の期間を定めて、当該各号に定める認証設計又は設計に基づく端末機器に第五十八条の表示を付することを禁止することができる。

一　認証設計に基づく端末機器が第五十二条第一項の総務省令で定める技術基準に適合していない場合において、電気通信回線設備を利用する他の利用者の通信への妨害の発生を防止するため特に必要があると認めるとき（第六号に掲げる場合を除く。）。　当該端末機器の認証設計

二～五　（略）

六　第五十二条第一項の総務省令で定める技術基準が変更された場合において、当該変更前に設計認証を受けた設計が当該変更後の技術基準に適合しないと認めるとき。　当該設計

（同一の表示を付することができる場合）

第六十八条の二　第五十三条第二項（第百四条第四項において準用する場合を含む。）、第五十八条（第百四条第七項において準用する場合を含む。）若しくは第六十五条又は第六十八条の八第三項の規定により表示が付されている端末機器（第五十五条第一項（第六十一条、前条並びに第百四条第四項及び第七項において準用する場合を含む。）の規定により表示が付されていないものとみなされたものを除く。以下「適合表示端末機器」という。）を組み込んだ製品を取り扱うことを業とする者は、総務省令で定めるところにより、製品に組み込まれた適合表示端末機器に付されている表示と同一の表示を当該製品に付することができる。

（端末設備の接続の検査）

第六十九条　利用者は、適合表示端末機器を接続する場合その他総務省令で定める場合を除き、電気通信事業者の電気通信回線設備に端末設備を接続したときは、当該電気通信事業者の検査を受け、その接続が第五十二条第一項の総務省令で定める技術基準に適合していると認められた後でなければ、これを使用してはならない。これを変更したときも、同様とする。

2　電気通信回線設備を設置する電気通信事業者は、端末設備に異常がある場合その他電気通信役務の円滑な提供に支障がある場合において必要と認めるときは、利用者に対し、その端末設備の接続が第五十二条第一項の総務省令で定める技術基準に適合するかどうかの検査を受けるべきことを求めることができる。この場合において、当該利用者は、正当な理由がある場合その他総務省令で定める場合を除き、その請求を拒んではならない。

3・4　（略）

【参考】端末設備等規則の構成

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セキュリティに関する海外の状況について①

○ 各国におけるIoT機器に対するサイバーセキュリティに関する法制度

	法律・ガイドライン名	概要
米国	The IoT Cybersecurity Improvement Act（NIST）	2020年12月成立。 ・NISTが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を発行 ・アメリカ合衆国行政管理予算局（OMB）がガイドラインに基づく活動を行っているかをチェック
	Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords（CISA）	セキュア・バイ・デザインの一環として、製造業者が製品に設定するデフォルトパスワードを廃止して顧客を保護するように促すガイダンス
	SB-327（California）	2020年1月施行。 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る ・製品ごとにプログラムされたユニークなパスワードを設定 ・利用開始前に、ユーザにパスワードを設定させる機能
欧州	EU Cyber Resilience Act	2024年12月発行。 ・EU市場に上市されるデジタル製品について、サイバーセキュリティ要件を満たすようにデジタル製品が設計、開発及び製造されていることを保証（第三者のコンポーネントを組み込む場合、当該製品のデュー・デリジェンスを実施し、デジタル製品のセキュリティリスクを高めるものではないことを確認） ・デジタル製品を上市する際、デジタル製品と共に型式やシリアル番号等の一定の情報を提供
	2014/53/EU	無線機器指令（RED）。2022年1月に更新。 以下の製品にサイバーセキュリティ、個人情報、プライバシー保護を義務づけ（2025年8月より） ・直接/間接的にインターネットに接続する製品 ・個人情報、トラフィックデータ、または位置情報を処理する製品 ・ユーザーが金銭、貨幣価値、または仮想通貨の送金が可能な製品
英国	Product Security and Telecommunication Infrastructure Act	2022年12月成立。 ・出荷時の共通パスワード設定の禁止（機器固有のパスワード設定で出荷するか、製品を使用する前にユーザが強固なパスワードを設定しなければ使い始められない仕様とすること） ・脆弱性情報の報告方法の提供 ・製品のセキュリティサポート期間の明示
シンガポール	Safer Cyberspace Masterplan 2020	サイバーセキュリティ戦略（2016）に基づき策定。以下の3つの柱で構成 ・中核となるデジタル・インフラの安全確保 ・サイバースペースでの活動を保護 ・サイバーに精通した人々の育成

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

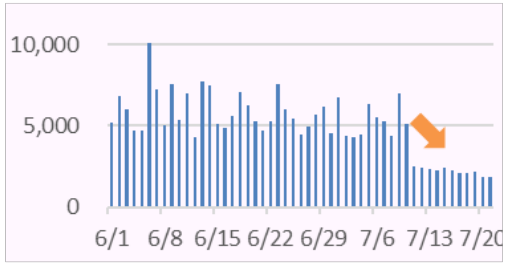
【参考】ソフトウェア脆弱性調査（有識者ヒアリング（NICT資料）より）

- 3 件のファームウェア脆弱性の調査を開始し、計 60,155 件の通知を実施
- その後の製品ベンダと連携した対処により対象とする脆弱性に関して顕著な観測数の減少を確認

国内ベンダ製無線ルータ

主な用途：家庭等において、インターネットに接続し、無線LAN等を提供するための機器
脆弱性詳細：Web設定画面がインターネット上からアクセス可能かつ、Web設定画面の脆弱性を用いて任意のコマンドが実行可能。

ベンダから対策済みファームウェアの配信とNOTICE による注意喚起が始まると、**平均6,000ホストから2,000ホストまで減少**

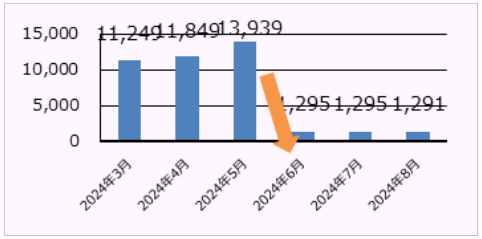


マルウェアからの感染拡大通信の観測数
（NICTERによる観測）

海外ベンダ製壁埋め込み型ルータ

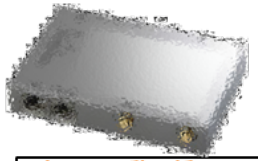
主な用途：家庭等において、インターネットに接続し、無線LAN等を提供するための機器
脆弱性詳細：脆弱性を有する管理画面がインターネットからアクセス可能な場合、管理画面に攻撃を行うことでルーターの悪用が可能になる。

当該機器を導入しているマンション向け ISP がインターネットからのアクセス制御を実施したことで、6月から検知数が**約 1/10 に減少**



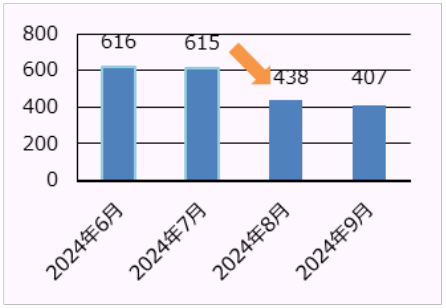
脆弱性のあるD-Link社製壁埋め込み型ルータの観測数
(NOTICEによる観測)

国内ベンダ製モバイルルータ



主な用途：
IoT機器等をインターネットに接続し、機器を遠隔で保守するための装置

実機の挙動解析により侵入経路を明らかにし、該当するポート番号 (6666/tcp) を NOTICE の調査対象に追加して注意喚起を行った結果、脆弱性のある当該国内ベンダ製モバイルルータの観測数が減少。



脆弱性のある国内ベンダ製モバイルルータの観測数
（NOTICEによる観測）

【参考】ETSI「EN 303 645」におけるセキュリティ基準の規定内容（論点に関する部分を抜粋）①

セキュリティ項目	「EN 303 645」における規定内容（規定(Provision)のみ記載）
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	**規定 5.1-1** パスワードが使用され、工場出荷時のデフォルト以外の状態にある場合、すべての民生用IoT機器のパスワードは、機器ごとに固有であるか、又はユーザによって定義されるものでなければならない。 **規定 5.1-2** プリインストールされた、機器毎に固有のパスワードを使用する場合、パスワードは機器のクラス又はタイプに対する自動化された攻撃のリスクを軽減するメカニズムで生成されなければならない。 **規定5.1-2A** パスワードを機器間の認証に使用するのは望ましくない。 **規定 5.1-3** 機器に対してユーザを認証するために使用される認証メカニズムは、技術、リスク、及び用途の特性に適したベストプラクティスの暗号技術を使用していなければならない。 **規定 5.1-4** ユーザが機器に対して認証できる場合、機器は、使用される認証値を変更するためのシンプルなメカニズムを、ユーザ又は管理者に提供しなければならない。 **規定 5.1-5** 機器が制約のある機器ではない場合、ネットワークインタフェースを介したブルートフォース攻撃を実行不可能にするメカニズムを持たなければならない。
ファームウェア（ソフトウェア）の更新機能	**規定5.3-1** 民生用IoT機器に含まれるすべてのソフトウェアコンポーネントは、セキュアにアップデート可能であることが望ましい。 **規定5.3-2** 制約のある機器でない場合、アップデートをセキュアにインストールするためのアップデートメカニズムを備えていなければならない。 **規定5.3-3** アップデートは、ユーザが簡単に適用できるものでなければならない。 **条項5.3-4A** 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なければならない。 **条項5.3-4B** 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。 **規定5.3-5** 機器は初期化後、定期的にセキュリティアップデートが利用可能かどうかを確認することが望ましい。 **規定5.3-6A** 民生用IoT機器が自動アップデートをサポートする場合、ユーザは、自動アップデートの仕組みを有効化および無効化し、自動アップデートの仕組みを通じて提供されるアップデートのインストールを延期することができるものでなければならない。 **規定5.3-6B** 民生用IoT機器が更新通知をサポートしている場合、ユーザは更新通知を有効化および無効化できなければならない。 **規定5.3-7** 機器は、セキュアなアップデートメカニズムを容易にするために、ベストプラクティスの暗号技術を使用しなければならない。 **規定5.3-8** セキュリティアップデートは、適時でなければならない。 **規定5.3-9** 機器は、ソフトウェアアップデートの真正性と完全性を検証することが望ましい。 **規定5.3-10** アップデートがネットワークインタフェースを介して配信される場合、機器は、信頼関係を介して各アップデートの真正性及び完全性を検証しなければならない。 **規定5.3-11** 製造業者は、セキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明らかな方法でユーザに通知することが望ましい。 **規定5.3-12** ソフトウェアアップデートの適用により、機器の基本的な機能が阻害される場合には、機器からユーザに通知することが望ましい。 **規定5.3-13** 製造業者は、定められたサポート期間を、ユーザにとって明確で透明性のある方法で公表しなければならない。 **規定5.3-14** ソフトウェアアップデートできない制約のある機器については、製造業者は、ソフトウェアアップデートができない根拠、ハードウェア交換のサポート期間と方法、及び定められたサポート期間を、ユーザにとって明確で透明性のある方法で公表することが望ましい。 **規定5.3-15A** ソフトウェアアップデートができない機器については、民生用IoT機器は分離可能でなければならない。 **規定5.3-15B** ソフトウェアアップデートができない機器については、民生用IoT機器のハードウェアは交換可能でなければならない。 **規定5.3-16** 民生用IoT機器のモデル名称は、機器上のラベル又は物理的インタフェースを介して、明確に認識可能でなければならない。

【参考】ETSI「EN 303 645」におけるセキュリティ基準の規定内容（論点に関する部分を抜粋）②

セキュリティ項目	「EN 303 645」における規定内容（規定(Provision)のみ記載）
インタフェース無効化	**規定5.6-1** すべての未使用のネットワークインタフェース及び論理インタフェースは無効化しなければならない。 **規定5.6-2** 初期化状態において、機器のネットワークインタフェースは、認証されていないセキュリティ関連情報の開示を最小化しなければならない。 **規定5.6-3** 機器のハードウェアは、物理インタフェースを不必要に攻撃にさらすことは望ましくない。 **規定5.6-4A** デバッグ・インタフェースは、無効にするか、ベストプラクティスの認証またはアクセス制御メカニズムによって保護されなければならない。 **規定5.6-4B** 物理ポートであるデバッグ・インターフェースは、デバイスによって物理的に保護されることが望ましい。 **規定5.6-5** 製造者は、民生用IoT機器の意図された使用または操作に使用される、または必要とされるソフトウェアサービスのみを有効にしなければならない。 **規定5.6-6** コードは、民生用IoT機器の動作に必要な機能のみに最小化しなければならない。 **規定5.6-7** ソフトウェアは、セキュリティと機能の両方を考慮し、必要最小限の権限で実行されることが望ましい。 **規定5.6-8** 民生用IoT機器は、メモリのハードウェアレベルのアクセス制御メカニズムを含むことが望ましい。 **規定5.6-9** 製造者は、民生用IoT機器に導入されるソフトウェアの安全な開発プロセスに従わなければならない。
設定済内容の電力供給停止時の維持機能	**規定5.9-1** データネットワークと電源の停止の可能性を考慮して、レジリエンスを民生用IoT機器とサービスに組み込むことが望ましい。 **規定5.9-2** 民生用IoT機器は、ネットワークアクセスが失われた場合にも動作を維持し、ローカルで機能し続けることが望ましく、電源損失が回復した場合にも正常に回復することが望ましい。 **規定5.9-3** 民生用IoT機器は、インフラの能力を考慮し、期待された、運用可能な安定した状態で、秩序ある方法でネットワークに接続することが望ましい。