本資料は、総務省の「令和５年度 重要IoT機器のセキュリティ対策に係る調査の請負」事業（受託者：NTTコミュニケーションズ）により作成したものを、総務省で公表するものです。

本資料に関するお問合せ等は総務省サイバーセキュリティ統括官室までお願いいたします。

メールアドレス:notice@ml.soumu.go.jp

令和5年度 0049-0219

「令和５年度 重要IoT機器のセキュリティ対策に係る調査の請負」

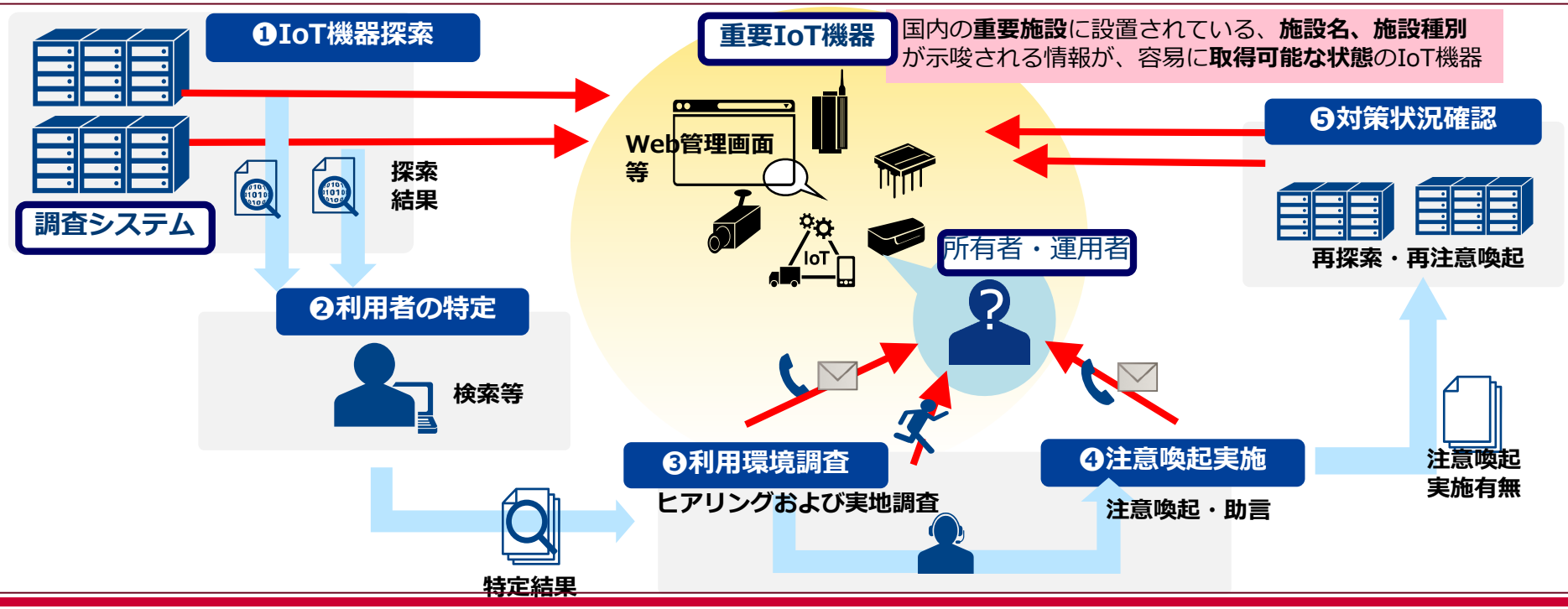
IoT機器チェックリスト

2024年3月29日

NTTコミュニケーションズ

目次

1．「令和５年度 重要IoT機器のセキュリティ対策に係る調査の請負」概要について

目的	IoT機器の安心・安全かつ適正な利用環境の構築を目指し、注意喚起による重要IoT機器利用者のリテラシーを向上させること。
実施対象	**社会的に影響を及ぼすリスクを伴った使用**をしている機器のうち、**国内の重要施設に設置されたIoT機器**（重要IoT機器）の利用者。 なお、社会的に影響を及ぼすリスクを伴った使用とは、**施設名、施設種別**が示唆される情報が、認証が不要な範囲でも**取得可能な状態**であることとする。
実施内容	施設名、施設種別が示唆される情報が取得可能な重要IoT機器を特定し、その利用者に対して以下の４つ観点による注意喚起を実施する。 • 施設名、施設種別が示唆される情報が、認証が不要な範囲でも取得可能な状態である • 国内ユーザー認証あるいはアクセス制御(IPフィルタ等含む）の導入が必要である • パスワードがデフォルトや特定されやすい（弱い）文字列となっている • 機器あるいはWebサーバーに脆弱性が存在する
全体像	

2．「令和５年度 重要IoT機器のセキュリティ対策に係る調査の請負」調査結果について

実施プロセス		実施結果
フェーズ	目的	
① IoT機器 探索	利用者名称や用途がインターネット上から容易に判別できる状態に置かれているIoT機器を特定するため、日本国内のIPアドレスに対して、探索を行う	• **2,883件**の対象機器を発見 →R2年度（962件）と比較し探索結果は増大。今後もIoT機器としては増加の見通し **増大するIoT機器**
② 利用者 特定	探索によって取得したIoT機器が重要施設に設置されているかの判別を行い、重要施設のIoT機器（重要IoT機器）に対しては連絡先を調査する。また、利用環境調査・注意喚起に向けたトリアージをするため、重要IoT機器ごとにスコアリングを実施する	• **1,122件（39%）**の連絡先候補を特定 →重要IoT機器でないとしたもの含め、60%にはリーチできていない **未リーチ層**
③ 利用環境 調査	個別に適切な対策案を提示するため、利用者にヒアリングを実施し、それぞれの重要IoT機器の利用・運用状況やセキュリティ対策がどの程度行われている調査を行う	• **868件（77%）**の利用環境調査を実施 →リスクを受容した利用、リテラシーがあまり高くはない層の利用を確認 **リスクを受容** **低いリテラシー**
④ 注意喚起	利用環境調査で判明したセキュリティ対策状況に応じて対策を検討し、注意喚起（対策案の提示、助言）を実施する。また、対策対応状況の管理を行い、実行を促進する	• **868件（77%）**の注意喚起を実施 「A.施設名、メーカー名等の表示を変更」、「B.特定利用者へアクセス制御」、「C.適切なパスワード設定」、「D.ファームウェア更新体制の準備」について注意喚起実施
⑤ 対策状況 確認	対策実施率を向上させるため、注意喚起を受けた対策の実施有無を確認し、実施できていない場合は再度の注意喚起を行うことで対策実施を促進する	• **802件（92%）**の改善を確認 ※再探索で抽出できない、及び一部対策済みを含む →対策が進まない事業者も確認 **対策未実施者**
補完	注意喚起対象とならなかった事業者、及び今後もさらに増大するインターネットを介して遠隔監視等を行うIoT機器利用者等をターゲットとし、本調査の注意喚起内容をチェックリストにて参照することでセキュリティリテラシーを向上し、適正なIoT機器の利用を促進する。またサイバー攻撃の影響は自組織だけでなく、他組織にも影響を及ぼす可能性があることの理解を進めたい。	

3. 本チェックリストのターゲットについて

ターゲット	インターネットを活用し、遠隔監視等の目的で、IoT機器を利用している方

「令和５年度 重要IoT機器のセキュリティ対策に係る調査の請負」にて調査対象の**90%を超えるIoT機器が、「インターネット上から（管理画面、施設名等の情報を）確認できることを意図していない」**との調査結果となりました。これらの結果からも、インターネットを介してIoT機器を利用しているユーザーの多くは、**IoT機器の利用に関してセキュリティリテラシーがあまり高くない**ことを示しています。その他、実証実験等での一時的な利用も含み、構築や運用コストを考慮し、**リスクを受容した利用**者であることが分かってきています。

本調査では、インターネットを活用し、IoT機器を利用する日本国内のユーザーを対象に、「インターネット上から（管理画面、施設名等の情報を）確認できる」機器を探索を行い、短期間ではあるが、2,883件もの施設名等が確認できる機器を発見しました。

その探索されたIoT機器に関する情報から、利用者を特定し、868件の注意喚起を行いました。

その結果、本調査注意喚起の４つの観点に関して、１以上の何らかの対策を実施したIoT機器は802件（92%）となりました。

しかしながら観点毎に「対策完了および対策予定」を合わせた、対策率についてを見てみると、「**施設名、施設種別が示唆される情報の修正、又は削除**」は17%、「**アクセス制御の導入**」に関しては18%という結果となりました。「**推測されにくい適切な（強度の高い）パスワードの設定**」、「**ソフトウェア更新体制の構築**」関しては、それぞれ87%、88%と高い結果を示したことから、比較的に対策のしやすい項目、又はソフトウェアの脆弱性に関する対応への理解は高まったといえます。その一方前述の2つの観点に関しては、今後のさらなる改善、働きかけが必要になると考えています。

本調査の注意喚起にて活用した内容をまとめチェックリストとすることで、施設名の表示に関する対策のみならず、４つの観点に関するセキュリティリテラシーの向上のため、本チェックリストがその一助となることを期待します。

4. 事前に確認いただきたい事項

本チェックリストの確認にあたり、以下の内容を事前に確認の上、A～Dのチェックを進めてください。

項番1	□ **チェックリストの確認に伴い、所有者、構築者、運用者、利用者等のステークホルダを定義し、確認結果をそのメンバーに共有、協議するための準備を行う。**

項番2	□ **インターネットを介して当該IoT機器へアクセスを行う必要があるか、部外者に閲覧又は操作してもらうことを意図しているか確認を行う。**

→ 本調査結果として、「インターネット上から機器が確認できることを意図していなかった」という回答が90%を超えている状況であり、インターネットからの利用が本当に必要なものであるか、再度確認をお願いします。

項番3	□ **所属する業界において機器設定や運用に関する「指針」「ガイドライン」等がないか確認を行い、ある場合は併せて活用する。**

→ 様々な業界において、該当する機器利用に応じて、ガイドラインや指針が示されている可能性があります。どのような情報が公開されているかについて確認し、必要な対応をご確認ください。

4. 事前に確認いただきたい事項

「令和５年度 重要IoT機器のセキュリティ対策に係る調査の請負」における注意喚起事項に則った、IoT機器利用に際して推奨される対応は下記の通りです。全ての対応をすることが望ましいですが、一部の対応を進めるだけでも、安心・安全な社会の実現に向けた第一歩となりますので、ご検討ください。

項番４	□　**下記の項目に対して、必要な対応を確認し、それぞれの項目に関する確認を行う。**

- ユーザー認証あるいはアクセス制御(IPフィルタ等含む）の導入を行う　→　5. チェック項目Aへ
- 施設名、施設種別が示唆される情報が、認証が不要な範囲でも取得可能な状態にしない　→　6. チェック項目Bへ
- パスワードがデフォルト設定や特定されやすい（弱い）文字列とならない　→　7. チェック項目Cへ
- 機器あるいはWebサーバーに脆弱性が存在しないよう更新体制を整備する　→　8. チェック項目Dへ

※4つの観点における対策の中では、項番Aにあるアクセス制御の実現により、必要なユーザーにしか見えなくなることが期待されます。そのため、一部しか実施できない場合、優先的に実施すべき対策と考えるため、以降のチェックリストでは、アクセス制御の導入に関する項目を最初に実施する構成とします。

5. A：ユーザー認証あるいはアクセス制御(IPフィルタ等含む）の導入を行う

インターネット上から確認可能な画面にアクセスする際には、ユーザー認証やアクセス制御など、必要なユーザーのみがアクセスを行えるような対応が望ましいです。

項番 A1	□ **画面内容が直接閲覧できるような状態にせず、ID及びパスワードによるログイン認証等、何らかのユーザー認証画面を設定しているか。**

項番 A2	□ **機器を利用するユーザーが、不特定多数ではなく、限られたユーザーのみある場合、ユーザーを限定したアクセス制御を設定することができるか。**

→ 機器を利用するユーザーが、不特定多数ではなく、限られた一定のメンバーであるか確認し、インターネット環境との境界となるルーター、Webサーバー（IoT機器）、またはファイアウォールを含むUTM機器でアクセス制御を行うことが可能か、検討ください。
詳細については、機器ごとに対応が異なるため、機器マニュアル、または構築者、運用者等のメンバーとご相談の上確認ください。主な確認事項としては、以下が想定されます。

- アクセスを行うユーザー数の確認
- アクセスユーザーのIPアドレスの確認
- アクセス制御を実施可能な機器の確認と設定する機器の確定（ルーター、Webサーバー、ファイアウォール等UTM機器、等）
- 機器の設定方法の確認
- 機器の設計
- アクセス制御設定の実施
- 動作確認試験後の運用開始

6. B：施設名、施設種別が示唆される情報が、認証が不要な範囲でも取得可能な状態にしない

管理画面等、インターネット上から確認可能な情報として、施設名、地域名、機器名、機器のバージョン、またはそれらを推測させる情報が見える状況になっていることで、何も情報が無い場合と比較し、攻撃者の興味を引き、攻撃の対象となる可能性があり、変更することが望ましいです。

項番 B1	□ **更改されているログイン画面、管理画面に攻撃者の対象となりやすい情報（「施設名」「地域名」「機器名」「機器のバージョン」「またはそれらを推測させる情報」等）を表示していないか確認する。**

→　施設名、地域名、機器名、機器のバージョン、またはそれらを推測させる情報が見える状況になっていることで、何も情報が無い場合と比較し、攻撃者の興味を引き、攻撃の対象となる可能性があります。

　記号など利用者にしか分からない情報に変更することで攻撃のリスクを下げる可能性があるため、記号等、利用者のみが判別可能な情報への変更、または削除についてご検討ください。

7. C：パスワードがデフォルト設定や特定されやすい（弱い）文字列とならない

ログイン画面認証を設定しているにもかかわらず、強度の低いパスワードを設定している場合、認証を第三者に突破される可能性が高まるため、適切な運用が必要となります。

項番 C1	□ **ログイン時のID及びパスワードは「工場出荷時の初期設定あるいは容易に推測される値」ではないか確認を行う。**

→　ご利用のIoT機器の設定マニュアル等を参照し、第三者に推測されない複雑なパスワードを設定ください。

項番 C2	□ **ID及びパスワードは複数の利用者で共有せず、必要な利用者分の払い出し、設定ができているか？**

→　一般的にID及びパスワードの使いまわし、共有により、 ID及びパスワードが漏洩する危険性が高くなると言われます。
そのため共用は行わず、必要なユーザー分払いだすことが推奨されます。

8. D：機器またはWebサーバーに脆弱性が存在しないよう更新体制を整備する

機器運用において、機器メーカーから提供されるソフトウェアを適切に管理・更新することは、機器を安全に運用する上で重要な要素となるため、そのための体制構築が望ましいです。

項番 D1	□ **構成する機器（ルーター、Webカメラ等のIoT機器、およびサーバー等）のネットワーク構成、各設定内容を管理できているか**
項番 D2	□ **構成する機器（ルーター、Webカメラ等のIoT機器、およびサーバー等）の台数、メーカー名、型番、ファームウェア等ソフトウェアのバージョンを一元管理できているか**
項番 D3	□ **機器あるいはWebサーバーのソフトウェア」に対して最適なバージョンを判断し、最新のものに更新する体制があるか**

→ 構築後の機器をそのまま運用するだけでなく、更新されるソフトウェアの情報を機器ごとに確認し、最新化することが望まれます。そのためには、機器情報の管理、更新情報の確認、最新ソフトウェアの更新を行うための体制の維持が必要となります。

重要なセキュリティに関する更新が公開される場合もあり、最新化することがサイバー攻撃の可能性を下げる重要な要素となります。

9. 最後に

体制、対応コスト、機器運用上の制限がある等、直ちにセキュリティ対策を実施することができない場合も想定されます。

サイバー攻撃等の対象となった場合、自身に関する施設やIoT機器に対して被害が出る可能性はもちろんのこと、他者の攻撃に利用されてしまう可能性があることご理解ください。IoT機器の運用に関するセキュリティリテラシーを向上し、IoT機器の安心・安全かつ適正な利用環境の構築を目指していきましょう。