IoT セキュリティチェックシート解説編

～IoT を企業へ導入するために考慮すべきこと～

【第 2.1 版】

2020 年 2 月 27 日

一般社団法人 日本スマートフォンセキュリティ協会（JSSEC）
利用部会　IoT 調査・研究タスクフォース

文書管理番号 JSSEC-R-IoT20200201-1

はじめに

超スマート社会を目指す「Society 5.0」を実現していくために、日本の第四次産業革命としてのコンセプトが「Connected Industries」となる。「Connected Industries」実現のためには「IoT によるデジタルデータ化」を起点に、集めたデータを分析し活用するための「ビッグデータ、AI」、さらには「ロボット」との連携や協調がコアテクノロジーとなり、これらコアテクノロジーをいかに活用できるか、我が国の産業全体に求められている。

IoT の普及によるセキュリティ対策の対象範囲拡大と被害防止が社会全体として重要な課題となって来たことを受け、一般企業が IoT を導入する視点からセキュリティ面で考慮すべき点の検討を進めて来た。

■IoT セキュリティチェックシート第 2 版の特徴

IoT セキュリティチェックシートは、一般企業が IoT を導入する時、セキュリティ面で考慮すべきことを網羅的に A3 両面 1 枚にまとめ、企業の情報セキュリティ（IT）と設備システム（OT）の両担当者が理解しやすくした。本チェックシートは、社内の IoT 導入関係者の検討や IoT 構築ベンダーとの確認用、さらに経営層へ理解を深めるに国際的サイバーセキュリティフレームワーク 1.1（NIST の CSF）からみた対策レベルのものさしとして利用することを想定し作成した。

※NIST：National Institute of Standards and Technology（米国国立標準技術研究所）

※引用先：NIST CSF1.1（IPA 翻訳版 2019 年 1 月発行）

■本解説編

本編は、「JSSEC IoT セキュリティチェックシート第 2 版」をより理解してご活用いただくために、以下のポイントで解説を記載している。

①なぜ検討すべきかの背景や目的

②なに検討すべきかのポイント

■免責・注意事項

※ JSSEC 並びに執筆関係者は、チェックシートおよび解説編などに関するいかなる責任も負うものではありません。全ては自己責任にて対策などをお願いします。

※ 本解説編に登場する商品名・サービス名は、一般に各社の商標または登録商標です。

※ 社内文書などに引用する場合、著作権法で認められた引用の範囲内でご利用ください。また、その際は必ず出典を明記してください。

■IoT セキュリティチェックシート改定の経緯

第 2.0 版(2019 年 2 月)：NIST のサイバーセキュリティフレームワーク 1.1（CSF）をもとに利用者側の網羅性を高めた。

第 2.1 版(2020 年 2 月)：チェック項目の検討主体（IT 又は OT）及び、連携（IT と OT）が重要な項目を明記した。

※項目 No.表示を色分けし明記（①：IT が主体的、❶：OT が主体的、❶：IT と OT の連携が重要）

※【注意】：主体的とは連携は必要となるがリードする側を表し、連携とは互いに議論するなど密に連携が重要な項目を表している。又チェックシートを活用する企業の体制により主体や連携すべき項目は変わってくるので、検討をはじめる段階で連携の方法を議論する事を推奨する。

■本解説編（第 2.1 版β）の主な変更点

・IoT セキュリティチェックシート改定に合わせ、項目 No.表示の色分けを反映した。

■制作■

利用部会 IoT 調査・研究タスクフォース

§第 2.1 版（2020 年 2 月　チェックシートと解説編の改定）

リーダー	後藤 悦夫	（株式会社ラック）
サブリーダー	三池 聖史	（ユニアデックス株式会社）
メンバー	笠原 正弘	（ソフトバンク株式会社）
（五十音順）	北村 裕司	（サイバートラスト株式会社）
	坂田 孝昭	（株式会社日立システムズ）
	瀬川　紘	（セコムトラストシステムズ株式会社）
	中村 丈洋	（株式会社 SHIFT SECURITY）
	中村 康洋	（シャープ株式会社）
	藤崎 卓哉	（株式会社ラック）
	不破 崇博	（凸版印刷株式会社）
	本間 輝彰	（KDDI 株式会社）
	松下 綾子	（アルプスシステムインテグレーション株式会社）

§第 2 版（2019 年 2 月　チェックシート改定と解説編発行）

リーダー	後藤 悦夫	（株式会社ラック）
サブリーダー	三池 聖史	（ユニアデックス株式会社）
メンバー	笠原 正弘	（ソフトバンク株式会社）
（五十音順）	北村 裕司	（サイバートラスト株式会社）
	坂田 孝昭	（株式会社日立システムズ）
	瀬川　紘	（セコムトラストシステムズ株式会社）
	中村 丈洋	（株式会社 SHIFT SECURITY）
	中村 康洋	（シャープ株式会社）
	藤崎 卓哉	（株式会社ラック）
	不破 崇博	（凸版印刷株式会社）
	本間 輝彰	（KDDI 株式会社）
	松下 綾子	（アルプスシステムインテグレーション株式会社）

§第 1 版（2018 年 3 月　チェックシートのみ発行）

リーダー	後藤 悦夫	（株式会社ラック）
サブリーダー	三池 聖史	（ユニアデックス株式会社）
メンバー	笠原 正弘	（ソフトバンク株式会社）
（五十音順）	北村 裕司	（サイバートラスト株式会社）
	坂田 孝昭	（株式会社日立システムズ）
	瀬川　紘	（セコムトラストシステムズ株式会社）
	中村 丈洋	（株式会社 SHIFT SECURITY）
	中村 康洋	（シャープ株式会社）
	藤平 武巳	（エヌ・ティ・ティ・コミュニケーションズ株式会社）
	松下 綾子	（アルプスシステムインテグレーション株式会社）

文書管理番号　JSSEC-R-IoT20200201-1

目 次

1. 識別（ID）

1.1. 資産管理（ID.AM）

01)IoT 機器、IoT システムの守りたい機能と守りたい情報を明確にする

❶ 守るべき機能（人に被害を与えないなど）を明確にする
② 守るべき情報（蓄積情報、流れる情報、設定情報など）を明確にする

IoT 機器は基本的に、本来の機能に「つなげる機能」が追加されている。これまで機器単体で完結していたものが、通信機能を介して外部から操作や制御を行えたり、データを収集したりする。こうした「IoT 化」によって追加された部分を認識し、「守るべき機能」と「守るべき情報」を洗い出して明確にする必要がある。

守るべき機能とは、機器が持つ本来の機能はもちろん、事故や誤作動が発生した際にユーザの身体や生命、財産を守るための機能も含まれる。また、守るべき情報とは、生成されるセンサーデータやログについての情報で、個人情報や設定情報など重要な情報となる。守るべき機能と情報を洗い出し、リスクを認識する。必要があれば、機器のメーカーや通信事業者などにも確認し、必要に応じて重要度を整理する。

02)IoT 機器、IoT システムの基本的な構成情報を把握する

① ハードウェア、ソフトウェアの情報を把握する
② 通信とデータの流れを把握する

IoT 機器やシステムの構成情報は、リスクアセスメントを実施するために必要な最低限の情報となる。また、脆弱性管理やインシデント管理の基礎情報にもなるため、構成情報の把握は非常に重要である。IoT 機器がどこにあるのか、どのメーカーの製品なのか、ファームウェアのバージョンなどの情報とともに把握し、図や表などにして保管する。IoT システムも同様に棚卸しを行う。

また、通信とデータの流れも把握する。IoT 機器やシステムが、それぞれどのような通信で接続されているか、どのようなデータが送信されるのかを把握しておく。

＜補足＞
ハードウェアでは、構成部品や初期状態、不具合が発生したときの挙動などを把握する。
ソフトウェアでは、脆弱性が作り込まれていないことが重要となる。
例えば、汎用のオープンソース・ソフトウェアパッケージに脆弱性が発見される可能性もあるため、注意が必要である。通信とデータの流れを把握することも重要な要素となる。たとえ IoT 機器がセキュアに製作されていたとしても、通信経路が多岐にわたるケースでは通信経路を把握することも重要である。

03)IoT 機器、IoT システムの関係者の役割を把握する

❶ IoT 機器、IoT システムの管理責任者の役割
❷ IoT 機器メーカーや IoT システム提供者の役割、および利用企業の役割
❸ IoT 機器、IoT システム運用や保守担当の役割
❹ CSIRT/PSIRT などインシデント対応関係部署の定義と役割（IoT 機器などインシデント発生時の連携先）

IoT の運用には、様々な人や組織が関わる。誰がどのような役割で関わっているかを明確にすることで、インシデントが発生しても適切な対応を行えるようになり、被害や影響の拡大を阻止できる可能性が高くなる。リスク分析などを通じあるべき役割を検討するため、現時点の IoT 導入・運用の体制と役割を把握する。

＜補足＞
IoT 機器、IoT システムの関係者には、IoT 機器、IoT システムの管理責任者、IoT 機器メーカーや IoT システムサービス提供企業の担当者および利用企業、IoT 機器、IoT システム運用や保守担当、CSIRT/PSIRT などインシデント対応関係部署などが挙げられる。具体的には、インシデント対応全体のハンドリング、原因究明、インシデントの影響範囲の見極め、関係者間の調整、原因の対処（機器の交換など）、エンドユーザへの対応、インシデントの発生に関する広報など、担当と役割を連絡先も含めて明確にしておく必要がある。

1.2. ビジネス環境（ID.BE）

04)IoT 機器、IoT システムがどのビジネスに関係しているか調査し守るべきビジネスを把握する
❶ IoT 機器、IoT システムがどのビジネスに影響を与えるか把握する
❷ IoT 機器、IoT システムが重要なビジネスまたは基幹ビジネスに大きな影響を与えないか調査する

IoT の問題が原因でビジネスがダメージを受ける可能性がある。このため、導入する IoT が自社のどのようなビジネスに影響を与えるか把握することが重要になる。調査の際には、影響を与える可能性のあるビジネスの重要度も加味する。重要度は詳細にレベル分けする必要はないが、重要なビジネスや基幹ビジネスに影響を与える可能性がある際には、その影響範囲を特に詳しく調査する必要がある。

1.3. ガバナンス（ID.GV）

05)企業へ IoT 機器を導入しネットワークに接続する時に検討すべき内容を方針として明確にする
1 IoT のリスク（リスクアセスメント）を認識し、経営層に提言し現状セキュリティポリシーの見直しをする
2 IoT の特性（数が多い、機器と一体、持ち出しやすい、人への安全に関わるなど）を考慮する
3 必要な体制を整備し、人材を確保して育成する

十分な検討を行わないまま IoT を導入してしまうと、想定していなかった深刻な問題が発生する可能性がある。そこで、新たに IoT 機器を導入しネットワークに接続する際には、あらかじめ前項のようにビジネスへの影響について調査し、リスクを認識する。特に、数が多い、機器と一体、持ち出しやすい、人への安全に関わるなど、IoT 機器の特性を考慮してリスクを洗い出す。

また、現状のセキュリティポリシーと比較し、必要があれば経営層に提言し、改訂を行う。そのためには経営層を巻き込むことも必要となるので、的確にリスクを説明できるようにしておく。さらに、必要な体制を整備し、人材を確保する。人材には IoT だけでなくセキュリティの知識も必要になるため、教育や育成を検討する。リスクアセスメントについては次項の 1.4 を参照のこと。

06)IoT 導入に伴い遵守すべき法令などを把握する
❶ 関連する適用法令及び契約上の要求事項を特定する
❷ 認可されているソフトウェア及び使用許諾されている製品だけを利用する

IoT 機器やシステムは、ハードウェアとしてのデバイスや、デバイスが収集するデータ、通信を行うネットワーク、全体として提供するサービスなど、複数の要素で成り立っている。それぞれの要素に該当する法令などがあるため、これらを遵守する必要がある。

＜補足＞

例えば電化製品がベースになっている場合は、電気用品安全法が適用され、販売するためには「PSE マーク」を表示する必要がある。また、使い方を誤ると危険なものなどは「特定電気用品」に分類され、登録検査機関による検査が必要となる。さらに、遠隔操作機能を実装する場合には、その技術基準を満たす必要がある。こうした法令は業界ごとに存在する。

個人を特定できるような情報を収集する場合には、いわゆる個人情報保護法を遵守する必要があるし、データの収集を海外で行う場合にはデータ移転に関する国ごとの法律を守る必要がある。

IPA などが提供しているガイドラインを参考に、関連する適用法令および契約上の要求事項を特定し、遵守することを確認する。法令やガイドラインなどに準拠しているソフトウェア、および使用許諾されている製品だけを利用するよう意識することも重要である。

1.4. リスクアセスメント（ID.RA）

07)つながることにより攻撃を受けるリスクを想定する
① ソフトウェアやハードウェアの設定の不備（ミス）による外部からの攻撃を想定する
② 保守ポートからの攻撃を想定する
③ 不正な相手に接続するリスク（乗っ取りを含む）を想定する

IoT 機器は、すでに脅威にさらされており、実際にサイバー攻撃を受け被害も発生している。リスク対策を行わないまま運用を開始すると、思わぬサイバー攻撃を受け、場合によっては加害者になってしまう可能性もある。リスク対策を行うためには、IoT 機器やシステムを構成するソフトウェアやハードウェアに設定ミスがある場合、どのような攻撃を受ける可能性があるかを想定する。

また、保守用のポートが攻撃を受けたり、侵入口となったりする可能性もある。最悪の場合は、IoT 機器やシステムを乗っ取られてしまうこともあるので、どのようなことをされてしまうかを想定する。そのためには、IoT 機器に関連する過去のサイバー攻撃事例などを調べ、IoT が攻撃を受ける可能性や影響、対策を把握することが重要となる。ただし、上記の 3 点はあくまで例であり、網羅的にリスクを想定することが重要だ。

08)保守作業時のリスクを想定する
❶ 保守員の悪意を想定する
❷ 保守ツールからのマルウェア感染を想定する

保守作業は、IoT 機器やシステムの設定を変更することが可能な作業なので、作業ミスや悪意のある操作がリスクとなる可能性が大きい。マルウェアを設置して感染を広げるような操作も可能となる。保守作業の多くは人間が行うことなので、信頼できる保守員の起用や、保守の立ち会いなどの検討が必要である。

保守ツールにマルウェアが潜んでいる可能性もあるので、保守ツールからマルウェアが侵入した際の影響を想定する。

09)つながることで異常が伝播し意図せず攻撃するリスクを想定する
① ソフトウェアやハードウェアの設定の不備（ミス）による外部への攻撃を想定する

IoT 機器やシステムが原因で、外部からサイバー攻撃を受けるだけでなく、それを足がかりに外部へサイバー攻撃を行う可能性がある。この場合、被害者のはずの自社が加害者になってしまうため、注意が必要となる。

マニュアルや正常な設定値などを用意しておき、異常を検出した際には再チェックを行うなど、設定のミスを起こさないようにする。また、IoT 機器やシステムがどのようなシステムにつながっているかを把握し、サイバー攻撃を受けた際に影響が伝播する範囲も特定しておく。

10)脆弱な IoT 機器がつながることで異常が伝播するリスクを想定する
❶ 連携する機器やシステムに影響を与えるリスクを想定する
❷ マルウェアなどが波及するリスクを想定する
❸ 既存機器（セキュリティ対策が不十分な組込系など）への影響を与えるリスクを想定する

IoT 機器やシステムを導入する環境のセキュリティ対策が不十分であると、IoT 導入によるリスクが増加する。IoT 機器やシステムは、複数のシステムにつながっていることが多いので、例えば、マルウェアに感染した場合に、どのシステムにどれだけの影響を与える可能性があるのかを想定する必要がある。

また、既存環境のセキュリティ対策レベルを確認し、IoT 機器やシステムからの影響をどれだけ食い止めることができるか、IoT 導入による影響を確認する。同様に、IoT 機器やシステムを原因とするトラブルにはどのようなものがあるか、どこまで影響を受ける可能性があるか、その範囲も把握する。

11)IoT 機器の盗難・紛失・破壊などのリスクを想定する
❶ 盗難・紛失時のリスクを評価し、対策が必要な場合には検討する

IoT 機器やシステムが第三者に容易に触れられる場所にある場合や、紛失や盗難によって悪意ある第三者の手に渡ってしまった場合は、不正アクセスや情報漏えいなどのリスクが生じる。特に IoT 機器やシステムを構成するセンサーやデバイスは小型のものが多いため、盗難や紛失のリスクを想定しておく必要がある。同様に、屋外に設置されるものもあるので、悪天候などにより破壊されるリスクもある。あらかじめ盗難や紛失が発生した際の影響範囲を特定し、対応策を検討する。

盗難・紛失・破壊などのリスクの想定には、例えば IoT 機器やシステムにどのようなデータが保存されているのか、個人情報など重要なデータが保存されていないか、保存されているデータは暗号化されているのか、暗号化されている場合、その強度は十分なのかなどを確認し、これらのデータが漏れた場合のリスクを評価する。

12)IoT 機器の破棄や転売時に情報を読み出されるリスクを想定する
① 個人情報・秘密情報などが漏えいするリスクを想定する

廃棄や売却したパソコン、あるいは HDD（ハードディスクドライブ）などにデータが残っていて、情報が漏えいしてしまう事件が発生している。これは、IoT 機器でも同様だ。IoT 機器の中には多くのデータを記録しているものがあり、個人情報や機微な情報が含まれていることもある。

マニュアルや製造元の Web サイトなどでどのようなデータが記録されているのかをチェックし、情報の重要度に応じた既存の情報管理の枠組みが、導入しようとしている IoT デバイスにも準用可能であるかを確認する。

13)中古の IoT 機器購入のリスクを想定する
① マルウェアや不正な設定情報が組み込まれているリスクを想定する

中古の IoT 機器を使用したことで、マルウェアに感染したり、不正な設定情報により誤作動などが発生する可能性がある。これは中古パソコンでも発生しており、中古品を扱う業者が初期化を十分に実施していないことが原因と思われる。

IoT 機器は使用される環境が多様なため、様々な種類の業者が中古品を取り扱う可能性があり、IoT 機器がマルウェアに感染することさえ知らない業者も多いと考えられる。設定においても同様で、買い取ったままの状態で販売する業者も多いと考えられる。中古品は信頼できる業者から購入することが前提となるが、中古品として想定されるリスクを許容できる環境のみで使用する、あるいは外部と通信しない閉域網で使用することが望ましい。

14)IoT 機器について内部不正やミスのリスクを想定する
① 内部関係者の不正（故意）や設定・操作ミス（過失）を想定する

どんなに堅牢なセキュリティ対策を構築しても、悪意を持った内部者が不正を行うことも想定される。また、故意ではなくても人的ミスは起こりえる。こうした内部者による不正やミスは、基本的に権限を持つ人間の操作なので、把握しづらいという問題もある。

内部不正やミスの発生を脅威として捉え、発生した場合の影響と原因を想定する。原因としては、例えば不正を可能にする検知や防御面での手薄さ、不正により得られる利益から導かれる動機の高さなどを想定し、それらに見合った対策状況であるかどうかを検討し、追加的措置の必要性を評価する。

1.5. リスクマネジメント戦略（ID.RM）

15)リスク対応計画（方針）を策定する
❶ リスクアセスメントの結果を受け、自組織への影響と許容範囲から対応策を検討する
❷ マネージメントレビューを実施し計画を確定する

IoT 機器やシステムは様々な業界で使用され、設置する場所も多岐にわたる。そのため、リスクアセスメントを行うと、非常に多くのリスクが潜在している結果になりやすい。しかし、想定されるリスクの全てに対応することは難しい。そこで、それぞれのリスクについてビジネスへの影響などを考慮し、優先度を決定する。そして、適切なリスク対策を計画する。

具体的には、リスクアセスメントにより洗い出したリスクに対し、ビジネスの観点も含めて対応を判断し、ビジネスに影響を与える重要なリスクや、許容範囲のリスクなどにランク分けを行う。これらの情報を元にリスクマネジメントを回していく。また、決定したリスクマネジメントの運用方針が適切に実施されているかを経営陣が判断するマネージメントレビューを実施し、リスクマネジメントを評価する。ISMS では年に一回の実施が義務づけられている。

16)信頼出来る IoT 機器（認証や実績）、IoT システムか確認をする
❶ 実績が多く評価の高い IoT 機器、IoT システムであるか確認する
❷ 第三者による評価や監査を受けている信頼性の高い IoT 機器、IoT システムであるか確認する

今後、IoT 機器やシステムは参入企業が増え、多くの機器やシステムが登場し、玉石混交となる可能性が高い。そうなったときに、例えば単純に価格だけで IoT 機器やシステムを選んでしまうと、思わぬリスクを抱えてしまうこともあり得る。

そこで、IoT 機器やシステムを選定する際には、豊富な実績や導入事例があるかどうか、あるいはインターネット検索でその機器やシステムの評価を調べる。特に、IoT やセキュリティに関連する第三者の評価や監査を受けているような、信頼性の高い機器やシステムの利用を検討する。

17)データの種類により経路や保管場所のルールを定める
① データの社外保管ルールに従う（ルールがなければ定める）
② ネットワークの経路（インターネットや国外経由など）のルールに従う（ルールがなければ定める）

IoT 機器やシステムは様々な場所に設置され、通信を行う。複数の通信を経由する場合には、通信を盗聴される可能性のあるポイントも増える。特に、重要なデータを収集する場合には、情報漏えいのリスクも高まる。そのため、リスクマネジメントの結果から、漏えいなどの可能性のあるデータの転送経路や保管場所を確認し、避けるようにする。

また、機器やシステムが社外にある場合には、データの社外保管ルールを適用する。ルールがない場合には策定する。同様に、ネットワークの経路に対してもルールを適用する。こちらもルールがない場合には策定する。

18)重要な事項が Web、マニュアルなどに記載されているか確認する（契約書など）
① 個人情報やプライバシーを取り扱う場合は保護などが記載されているかを確認する
② 集めた情報の使われ方や第三者提供および利用目的などを確認する
❸ サポート期間、問い合わせ先などを確認する

IoT 機器やシステムで収集したデータの管理に、社外のサービスを利用することもある。この場合、そのサービスから重要なデータが漏えいしたり、失われたりする可能性がある。サービスを利用する際には、重要な事項が Web サイトやマニュアル等に記載されているかを確認する。

特に、個人情報やプライバシーなど重要なデータを取り扱う場合には、不正アクセス対策やデータの暗号化など、具体的な保護手段を確認する。また、データの第三者提供の有無などを確認する。第三者提供を行う場合には、その使われ方や利用目的、匿名化の有無などを確認する。もちろん、サービスのサポート期間や問い合わせ

先なども把握しておきたい。

1.6. サプライチェーンリスクマネジメント（ID.SC）

19)IoT で繋がったビジネスパートナーとのリスクを把握する
❶ ビジネスパートナーに影響をあたえるリスクを把握する ❷ ビジネスパートナーから影響を受けるリスクを把握する

IoT 機器やシステムを利用または提供する場合には、複数の企業と連携することが多い。それはビジネスパートナーであったり、サプライチェーンであったりする。サプライチェーンとは、原材料や部品の調達、製造、在庫管理、物流、販売までの一連の商流、およびこの商流に関わる複数の組織群を指す。こうした連携の中では、インシデントが発生すると影響が広がりやすい。

自社がパートナーに影響を与えてしまうこともあれば、パートナーから影響を受けることもある。ビジネスパートナーやサプライチェーンを構成する企業それぞれのリスクを想定し、自社にどのような影響があるかを把握する。同様に、自社で問題が発生した際にビジネスパートナーやサプライチェーンに与えてしまう影響についても把握する。特に、機器やシステムの不具合や、サイバー攻撃、情報漏えいといったインシデントは影響が広範囲にわたる可能性が高い。

20)IoT システムの提供者関係における情報セキュリティを把握する
① IoT システム提供者の情報セキュリティマネジメント状況を確認検証、評価する

外部の IoT システムを利用する場合には、そのシステムの提供者のリスク管理体制も重要になる。サービス提供者のリスク管理が甘いと、利用する側のリスクも高まり、最悪の場合はサービスが停止し事業が成り立たなくなってしまう。そこで、IoT システムの提供者の情報セキュリティマネジメント状況に問題がないか確認する。

具体的には、サービスの契約時に情報セキュリティマネジメントの状況を確認したり、サービス提供者の Web サイトで情報セキュリティへの取組状況を確認する。また、サービス提供者についてインターネットで検索を行い、評判などを把握することも方法のひとつとなる。

21)IoT 機器、IoT システムの提供者の提供リスクを把握する
❶ IoT 機器、IoT システム提供の継続性を確認する ❷ 障害などへの対応能力や体制を確認する ❸ データ所有権を確認する ❹ IoT 機器、IoT システム提供者のサプライチェーンのセキュリティリスク管理を確認する

外部から IoT 機器やシステムを調達する場合には、それらを利用する際のリスクを把握する必要がある。提供者の信頼性が低いと、それらを利用したサービスも不安定になり、継続性が下がってしまうことになる。

継続性においては、脆弱性の有無やファームウェアなどのアップデート状況、評判などを調査する。対応能力や体制については、提供者の Web サイトで情報を確認する。例えば提供者が自社で CSIRT を構築している場合は、ある程度の信頼性があると判断できる。これらには、IoT 機器やシステムの提供者のサプライチェーンについても確認し、どのようなセキュリティリスク管理体制を構築しているかも確認する。事前に Web サイトで確認するほか、契約の際に直接確認することが重要である。

2. 防御（PR）

2.1. アイデンティティ管理、認証／アクセス制御（PR.AC）

22)IoT 機器の機能及び用途に応じてネットワークへ接続する方針や条件を検討する
① IoT 機器のインターネットへの接続が必要か否か検討する（閉域網の検討） ② IoT 機器をネットワークへ接続する際には、認証および暗号化によるセキュリティ対策を実施する ③ セキュリティ対策が不十分な IoT 機器を直接インターネットに接続しないように留意する

IoT 機器やシステムに対するセキュリティ意識はまだ低く、十分な対策がなされていないケースが多い。そのため昨今では IoT 機器やシステムを狙うサイバー攻撃が増加している。まずは、IoT 機器やシステムにインターネット接続が必要かどうかを検討する。インターネットに接続する必要がないなら、閉域網で接続し、インターネットに接続するリスクを回避する。

IoT 機器をネットワークに接続する際には、認証（VPN の認証機能や MAC 認証）および暗号化によるセキュリティ対策を実施し、不正アクセスや情報漏えいを防ぐ。

23)IoT 機器、IoT システムの不要なサービスやポートは停止するなど必要最小限の設定を行う
① デフォルトで有効になっている不要な機能やサービスは無効にする ② IoT 機器やシステムに必要のない不要なポートは停止する

不要なサービスが動いていたり、不要なポートが開いていると第三者からの攻撃などを受けるリスク高くなるので、不要なものは必ず停止することが重要である。

特に IoT 機器やシステムでは、メンテナンス用ポートが初期設定で開いたままになっていたり、不要なサービスが有効になっていたりすることもあるので、使用開始前に IoT 機器の設定から有効な機能やサービスを確認し、不要なものは無効に設定する。

24)IoT 機器への外部からの不正アクセスを防止する
① ファイアウォールなどにより外部からのアクセス制御を行う

インターネットに直接接続している IoT 機器は、例えばインターネットに接続されている機器を検索する「Shodan」や「Censys」といったサービスを利用することで、インターネット上からその存在を容易に確認することができる。実際に、インターネットに直接接続している家庭用のブルーレイレコーダーなどに不正アクセスを行い、マルウェアに感染させることでボット化し、DDoS 攻撃に利用するケースが増加している。こうした不正なアクセスを防ぐため、IoT 機器は直接インターネットに接続せず、ファイアウォールやルータを経由するとともに、適切なアクセス制御を行う。

25)IoT 機器、IoT システムの管理者権限・利用者権限の ID とパスワードの設定及び管理を適切に行う
① ID とパスワードを初期設定のままとせず、適切に変更（変更後の文字数、文字種別などにも留意）する ② 第三者に知られないよう厳重に管理する ③ ID とパスワードを権限のないユーザと共有しない ④ ID とパスワードを他システムと使いまわししない

IoT 機器の初期設定内容は、比較的容易に知ることができる。多くの場合、IoT 機器のメーカーは説明書などの資料を Web サイトで公開しているためだ。これにより、初期設定の ID やパスワードを誰でも確認できる。サイバー犯罪者は、こうした情報を元に不正アクセスを行っている。そのため、ID とパスワードを初期設定のままで変更していない IoT 機器は、常に不正ログインのリスクが存在することになる。

IoT 機器を使用する際には、必ず設定を確認し、ID とパスワードを初期設定のものから別のものに変更する。変更の際には、設定できる文字数や文字種別も確認し、なるべく推測しづらい組み合わせにする。また、ID とパスワードは厳重に管理し、権限のないユーザとの共有を避ける。パスワード漏えいなどの影響範囲を限定するため、パスワードを別のサービスやシステムで使い回さないことも重要だ。

26)IoT 機器、IoT システムに対して適切な認証機能を利用する

① IoT 機器の認証を検討する（電子証明書、IoT 機器識別子など）
② 利用者（ユーザ）の認証機能を検討する（ID/パスワード、IC カード、生体認証など）
③ IoT システム（クラウドなど）の認証を検討する（電子証明書など）

IoT 機器やシステムには、「なりすまし」のリスクが存在する。なりすましには、不正な IoT 機器が正規の IoT 機器のようになりすますケースと、不正なユーザが正規のユーザのようになりすますケースがある。前者は不正な IoT 機器にアクセスしたユーザのプライバシー情報が漏えいする危険性があり、後者は IoT 機器や IoT システムの不正操作による情報漏えいや運用妨害の危険性がある。

ネットワークを利用した接続には公開鍵認証やクライアント証明書による認証、IoT 機器の識別子による認証などにより対策を行う。ID とパスワードのみの認証では辞書攻撃などにより破られる可能性があるため、物理的な認証には ID とパスワードだけでなく、IC カードや生体認証との併用による多要素認証の導入を検討する。認証を IoT 機器で行わず、OAuth2 などの電子証明書を用いたクラウド上の認証サービスを活用することも有効だ。

27)物理的なセキュリティ対策を検討する

❶ 第三者の入室制限など検討する
❷ 通信ケーブル及び電源ケーブルの配線は、傍受、妨害または損傷から保護する

サイバー攻撃はネットワーク経由のみとは限らない。悪意ある人物が建屋などに侵入し、直接 IoT 機器の設定を変更するなどの不正を行う可能性もある。実際に、高度な標的型攻撃では、清掃員などになりすましてオフィスに侵入し、ネットワークに盗聴器を仕掛けるといったケースもある。サイバーだけでなく、フィジカル（物理）セキュリティも検討する。

IoT 機器は IC カードなどで入退室が管理されたエリアに設置するなどの方法が挙げられる。また、重要なデータの場合は、サーバルームやセキュリティボックスなどに配置し、より厳密にアクセスを管理することも考えられる。さらに、重要なデータを扱う機器では、配線からデータをモニタする盗聴方法もあるため、ケーブルのシールドやケーシングなどの保護も検討する。

2.2. 意識向上およびトレーニング（PR.AT）

28)リスクを社内利用者へ周知する

❶ 禁止事項（機器が壊れるなど、「この様な使い方はしない」こと）
❷ 重要な説明事項（個人情報やプライバシーに関わること、生命や重大事故につながること）
❸ システム全体に影響を及ぼす事項

IoT 機器には非常に小さいものもあるが、精密機器に変わりはない。設定や衝撃などにより誤動作や故障が発生する可能性がある。また、外的な要因による影響も考えられる。IoT 機器は様々な場所に設置されるため、動作条件の確認も重要となる。使用温度域や振動、水濡れなども誤動作や故障の原因となるため、設置前に確認しておく。そして、こうした禁止事項や重要な説明事項を社内利用者への周知を行う。

IoT システムが個人情報や利用者の行動などを収集する場合、その旨を利用者に周知する必要がある。また、個人情報やプライバシーが保護されるよう、利用者には適切な利用方法や注意事項などの説明が必要となる。同様に、生命や重大事故につながる恐れがある場合には禁止事項を行った場合に想定される事故や影響についても周知し、注意事項を徹底する。

29)IoT 機器、IoT システムの関係者に役割を周知する

❶ IoT 機器、IoT システムの管理責任者の役割
❷ IoT 機器メーカーや IoT システム提供者の役割、および利用者の役割
❸ IoT 機器、IoT システム運用や保守担当の役割
❹ CSIRT/PSIRT、またはインシデント対応関係部署の定義と役割（IoT 機器などインシデント発生時の連携先）

IoT には多くの関係者が存在し、しかもその関係は複雑という特徴がある。この関係を整理しておかない

と、迅速さが求められるインシデント対応において遅れを招く要因となり、被害の拡大につながる恐れがある。そこで、サービスの開始時までに IoT 機器やシステムの関係者の役割分担を明確にして、利用者、関係者に周知する必要がある。

特に IoT の場合は、業種や分野によって想定されるインシデントやリスクが大きく異なり、関係者も異なってくる。まず、全体の管理を行う責任者を決め、役割やインシデント発生時の連絡先などを明確にする。そして、IoT 機器やシステムの提供者の担当者を明確にするとともに、役割を認識してもらう。同様に、システム運用者や保守担当の役割、CSIRT/PSIRT あるいはインシデント対応関係部署の定義と役割を明確にする。これらを文書化しておくことで、インシデント対応の効果をより高めることができる。

30)関係者の役割に従った手順をトレーニングする
❶ 関係者の役割に従った手順を明確にする
❷ 関係者の役割に従った手順をトレーニングする

IoT 機器やシステムの設定や障害対応は、文書化だけではいざというときに十分な対応ができないことがある。前項で明確にした関係者とその役割をもとに、実際のインシデント対応における手順を組み立て、それも各自に認識してもらう。

また、インシデント発生時の仮想シナリオを用意して対応のシミュレーションを行うことも重要だ。手順に沿って各自が役割を果たす予行演習のようなものであるが、実施してみると様々な問題が浮かび上がることが多い。担当者が休みであったり、必要な情報をすぐに得られなかったりする。トレーニングを定期的に繰り返し、問題点を修正していくことで、より確実で迅速なインシデント対応が可能になる。

2.3. データセキュリティ（PR.DS）

31)守るべきデータが暗号化されているか確認する
① IoT 機器、IoT システムに保管されている情報が暗号化されているか確認する

IoT 機器はその性質上、様々な場所に設置されることが多く、盗難や紛失などのリスクがある。また、Wi-Fi などの無線通信を利用することが多く、無線経由で情報が漏えいするリスクもある。特に、重要なデータを扱う IoT 機器やシステムでは、常に最悪のケースを想定して対策を行う必要がある。

紛失や盗難、盗聴などにより発生する情報漏えい対策には、データの暗号化が効果的となる。データは常に暗号化するようシステムで対応する。また、暗号化の強度にも注意する。

32)IoT 機器の接続、IoT システムのゲートウェイ経由の接続などの環境に応じた暗号化を検討する
① Wi-Fi ネットワークへの接続を設定する際には、より強い暗号方式を使用する
② 可能な場合、有線での接続も検討する
③ Telnet ログインを無効にし、可能な限り SSH を利用する

IoT 機器やシステムは、有線接続や Wi-Fi など、通信経路が多様であることが特徴。特に、Wi-Fi による無線通信の場合は、データを盗聴される危険性がある。そこで、Wi-Fi ネットワークに接続する際には暗号化を行い、より強い暗号方式を設定する。ただし、現時点でもっとも強い暗号強度である「WPA2」には脆弱性が確認されており、Wi-Fi 機器やデバイスがこの脆弱性を解消しているかどうかを確認する必要がある。また、2018 年に後継となる「WPA3」が正式に承認されたため、今後は WPA3 対応機器が登場してくる。なるべく WPA3 対応機器を使用したい。なお、場合によっては有線接続も検討する。

IoT 機器やシステムをゲートウェイ経由で接続する際にも、暗号化を検討する必要がある。なお、Telnet は認証情報を含むすべての通信を暗号化せず、平文で行うため、多くの情報漏えい事件の原因となっている。Telnet 対応とうたっていなくても使用できることが多いため、Telnet ログインは無効にし、暗号化された SSH を可能な限り利用する。

33)IoT 機器側でセキュリティ対策が難しい場合、別途セキュリティ製品を導入し全体でセキュリティを確保する
① セキュリティ対策が困難な IoT 機器は、セキュアなゲートウェイを経由する

IoT 機器は CPU やメモリといったリソースが少なく、新たなセキュリティ対策ソフトなどをインストールできないことが多い。一方で、サイバー犯罪者はよりサイズの小さいマルウェアを開発している。
そこで、個々の IoT 機器でセキュリティ対策を行うのではなく、ゲートウェイなど、ネットワーク上のセキュリティ製品で対策を行うことが有効となる。

34)設定情報が改ざんや変更されないようにする
① 管理者以外による IoT 機器、IoT システムの設定変更を禁止する

IoT 機器やシステムにおける設定は非常に重要で、管理者以外の内部者による設定ミスや、外部者による悪意ある設定変更により、IoT 機器やシステムの誤作動や情報漏えいが発生する可能性がある。そこで、管理者以外による IoT 機器やシステムの設定変更を禁止する。
対策の例としては、管理者以外が設定変更できないようシステム上で制御することや、許可された人間以外による設定変更の禁止を運用ルールとして文書化することが挙げられる。

35)IoT 機器の廃棄や再利用時の対策を行う
① 個人情報・秘密情報を完全に消去する方法を提供者に確認する ② 廃棄時は完全消去又は物理破壊、組織内再利用時には初期化、売却は完全消去が可能時のみとする ③ 中古など再利用する場合は、不正に改造がされていないか提供者に確認する

廃棄や売却した IoT 機器にデータが残っていて、情報が漏えいしてしまう可能性がある。逆に中古品などを再利用する際にリスクの高い設定がなされていたり、改造されている可能性もある。IoT 機器を廃棄や売却する際には、データを完全に消去する正しい方法を提供者に確認し、実行する。なお、データを完全に消去が出来ない場合は、売却をせず物理破壊を行う。また、外部業者に作業を委託する場合は、作業完了のエビデンスを取得する。
同様に、中古品などを再利用する際には、初期化を行うとともに、正しい初期状態を提供者に確認する。多くの場合、IoT 機器を提供している企業の Web サイトなどでマニュアルを確認できるので、改造されていないかも合わせて確認する。

2.4. 情報を保護するためのプロセスおよび手順（PR.IP）

36)IoT 機器、IoT システムの使用期間とサポート期間を確認する
❶ IoT 機器、IoT システムのサポート期限（EOL/EOSL）が提示される/されているか確認する ❷ アップデート可能な期間を確認する

IoT 機器やシステムに脆弱性があると、それを悪用され被害を受ける可能性がある。また、サポート期間が設定されている IoT 機器やシステムでは、サポート終了（EOL/EOSL）後は脆弱性が確認されても修正されない。セキュリティ対策を行わないまま IoT 機器やシステムを使い続けると、脆弱性を悪用されるリスクが高まる。
脆弱性には様々な種類があり、種類によっては外部から IoT 機器やシステムを乗っ取られたり、情報漏えいを引き起こされる可能性もある。そこで、IoT 機器やシステムを使用する際には、サポート期間を確認する。また、アップデートが可能な（修正パッチやアップデートが提供される）期間を確認する。

37)IoT 機器のアップデート手順を確認し策定する
① アップデート情報やアップデートファイルの入手方法やアップデート手順を確認する ② アップデート時の安全性（改ざん防止やアップデートファイルの暗号化など）を確認する ❸ アップデートする判断基準を定める ❹ 安全にアップデートする手順とアップデート後の動作確認手順を策定する ❺ アップデートの不具合があった時の戻し手順を策定する

IoT 機器やシステムのソフトウェアなどに脆弱性が確認された場合、サポート期間内であれば基本的に提供者からアップデートやパッチが提供される。これを適用することで、脆弱性を悪用したサイバー攻撃から IoT 機器やシステムを保護することができる。パソコンやサーバであれば、パッチやアップデートの通知が

あったり、自動的に適用される機能があったりするが、IoT 機器やシステムでは、提供元によって通知方法や適用方法が様々である。

まずは、自社で使用している IoT 機器やシステムごとに、アップデータやパッチの提供方法を確認する。また、パッチやアップデートの多くは脆弱性の修正も含まれているため、基本的にパッチやアップデートの適用は必須である。修正される脆弱性の内容を確認して重要度や影響といったリスク判断を行い、適用するタイミングを決定する。そして、適用手順や適用後の動作確認手順も策定しておく。アップデートに不具合があった場合も想定し、適用前の状態に戻す手順も確認、策定しておく。

38)インシデント発生時の対応計画と復旧計画を策定する
❶ インシデントの基本的な対応手順を策定する ❷ インシデント対応後の基本的な復旧手順を策定する ❸ 復旧のためのデータバックアップ計画を策定する

インシデント発生時の対応手順が策定されていないと、対応が後手に回ってしまい、被害が拡大して業務に影響を及ぼしたり、自社が加害者になってしまうこともある。インシデント対応は企業の事業継続性にも影響を及ぼす重要な問題なので、平常時からインシデント発生時の対応手順をあらかじめ策定しておき、関係者に周知しておく。

インシデント対応には、システムの対処や復旧を行う担当や、サプライチェーンと連携する担当、利用者や監督省庁への通知や告知を行う担当、全体をハンドリングする担当などが必要で、システムを止める判断のために経営層も巻き込む必要がある。また、対応後の復旧手順においても、同様に策定・周知する。復旧のためには、日頃から必要に応じた頻度でデータのバックアップを実行しておく必要がある。

39)IoT 機器メーカーや IPA、JPCERT/CC、ISAC などの脆弱性情報を収集・分析と対応手順を策定する
① 不具合や脆弱性などの情報を提供者に確認する（Web サイトやメールなど） ② IPA などの機関から発信される情報を確認し、自社の構成に類似していたら提供者に影響を確認する ③ 提供者から通知が行われた脆弱性の影響（自社利用への影響）を特定する ④ 利用制限などの暫定対策とアップデートなど恒久対策を検討する

脆弱性の多くは、公的機関やセキュリティベンダ、機器やシステムの開発元から情報発信が行われる。これを見過ごして適切な対応を行っていないと、脆弱性を悪用する攻撃を受けたり、深刻な不具合が発生したりする可能性がある。脆弱性情報を日頃からチェックしておくことが必要だ。IoT 機器やシステムを利用している場合は、脆弱性が発見された際に提供元からメールなどによる通知が行われるかどうかを確認し、必要があれば契約を行う。Web サイトでの告知が行われるかどうかも確認しておく。脆弱性が発表され立木には、早急な対応を行う。

また、IPA や JPCERT/CC、ISAC などでも都度、情報が公開される。IoT 機器や IoT システムで利用している構成情報などから、該当している脆弱性があったら、提供者に影響を確認するなどの対応も必要となる。システムが複雑な場合は、アップデートが他のアプリケーションなどに影響を与えることもあるので、リスク判断による対策実施の検討や、利用制限などによる暫定対策の検討、アップデートなどの恒久対策の検討を行う。

2.5. 保守（PR.MA）

40)IoT 機器のソフトウェアを最新のバージョンにアップデートする
❶ IoT 機器の導入時点で最新のソフトウェアにアップデートする ❷ 継続的に IoT 機器のソフトウェアを最新のバージョンにアップデートする

IoT 機器を導入した時点で、すでにソフトウェアが古くなっていることがある。その場合は、脆弱性が存在している可能性が高く、そのまま使用してしまうとサイバー攻撃を受ける可能性がある。

IoT 機器を導入したら、まずソフトウェアのバージョンを確認し、開発元などの Web サイトで最新のバージョンを調べ、古いようならアップデートを行う。使用開始後もバージョン情報を定期的にチェックし、最新のバージョンを保つようにする。

41)IoT 機器、IoT システムの構成情報を最新にする
❶ IoT 機器、IoT システムの構成情報（設置場所、台数、使用用途、稼動有無など）を管理する

管理されていない IoT 機器やシステムは、意図しない情報漏えいの原因になったり、サイバー攻撃の侵入口になったりする可能性がある。定期的に自社にある IoT 機器やシステムについて棚卸しを行い、それぞれの設置場所や台数、使用用途、稼働の有無、ソフトウェアやファームウェアのバージョン、担当者などを明確にする。

42)保守作業時の手順を明確にする
❶ 許可されたツールを使用する
❷ 遠隔保守の不正アクセス対策を実施する
❸ 保守の履歴を管理する

保守作業には複数のリスクが伴う。保守ツールそのものにマルウェアなどが紛れ込んでいるケースや、遠隔保守機能を悪用され不正アクセスされるケースもある。まずは保守を行う担当者を決め、保守のために IoT 機器やシステムの設定項目を変更できる権限を与える。

また、使用する保守ツールの信頼性を確認する。遠隔保守を行う場合には、不正アクセス対策を行う。また、保守の履歴を残して管理することも、問題や障害が発生した際の原因究明に役立つため重要な作業となる。

2.6. 保護技術（PR.PT）

43)IoT 機器の必要なログが取れるか確認する
① 故障やエラー情報（セーフティ解析用）が取れるか確認する
② 動作環境の情報（リライアビリティ解析用）が取れるか確認する
③ 攻撃や認証の情報、アクセス履歴（セキュリティ解析用）が取れるか確認する
④ ログのタイムスタンプなど時刻を合わせる
⑤ 必要なログ、保管期間などを決める
⑥ センシティブな情報のログ出力をしない（センシティブな情報を含む場合は暗号化する）

ログを保存しておき、定期的に確認することで、攻撃や不正、不具合の痕跡や予兆を見つけ出せる可能性が高くなる。これにより攻撃や不具合を事前に対策できたり、事後の原因究明にも役立つ。IoT 機器やシステムからログを取得できるかを、まず確認する。ログを取得できる場合は、どのようなログを取得できるかを調べ、必要なログを保存する。

必要なログには、セーフティ解析用の故障やエラー情報、リライアビリティ解析用の CPU 負荷、ネットワーク負荷、リソース使用量などの動作環境の情報、セキュリティ解析用の攻撃や認証の情報、アクセス履歴などが挙げられる。その上で、取得するログを決定し、保管する期間を定める。関連する IoT 機器やシステム間でログの記録時間が整合するように、タイムスタンプの時刻を合わせることも重要となる。ただし、センシティブな情報のログは出力しないことが理想だが、ログにセンシティブな情報が含まれる場合は、暗号化するなどの対策を行う。

44)IoT 機器の必要なログが安全に保管されるか確認する
① 不正アクセス対策がされていること（改ざん・消去対策）を確認する
② ログへのアクセス権限の設定を確認する
③ ログの暗号化を確認する
④ 保管場所を確認する

巧妙なサイバー攻撃では、ログを改ざんして痕跡を消していくこともある。唯一の手がかりを消されることのないように、ログの保管には万全を期したい。ログに関する対応事項としては、ログへの不正アクセス対策を行い、改ざんや消去を行われないようにする。ログへのアクセス権限の設定を確認し、権限のある者のみがログにアクセスできるようにする。ログの暗号化を確認する。IoT 機器の中には低機能のため、大量のログの管理や暗号化などの対策が難しい場合があるので、他にログを管理するための専用の機器（サーバ

など）を用意するなどの対策も検討するといったことが挙げられる。

3. 検知（DE）

3.1. 異常とイベント（DE.AE）

45)IoT 機器、IoT システムの異常を把握する
❶ IoT 機器のログやインベントリ情報から異常の検知方法を検討する（異常はなにかを定義）
❷ 異常として検知するしきい値を検討する
❸ 異常の影響を把握する

IoT 機器やシステムに異常が発生すると、必要なデータを取得できなくなり、業務に影響を及ぼすこともある。こうした異常には、一刻も早く気づき、対応を行う必要がある。IoT 機器やシステムの「異常な状態」を定義し、それを検知できる方法をしきい値も合わせて確認する。また、異常が発生した場合の影響範囲を把握しておくことも重要となる。

3.2. セキュリティの継続的なモニタリング（DE.CM）

46)ネットワーク機器や IoT システムの異常を継続的に監視する
① 設置した IoT 機器のログなどをモニタリングし異常を検知する仕組みを検討する
② 設置した IoT 機器にマルウェアなどが存在しないか調査する仕組みを検討する
③ 異常を検知する仕組みを継続的に運用しモニタリングする

異常を検知できる仕組みがないと、異常が発生しても気づくことができず、IoT 機器やシステムの破壊や情報の搾取、リモート操作などの被害につながることがある。常に IoT 機器やシステムの状況をモニタリングし、いち早く検知できる仕組みが必要となる。IoT 機器やシステムに異常が発生していないか、マルウェアが侵入していないかを調査できる仕組みを検討する。

運用においては、継続してモニタリングを行い、異常を検知できる仕組みを検討する。

47)設置した IoT 機器の脆弱性を調査する
① 脆弱性検出（脆弱性スキャン）ツールによる IoT 機器の脆弱性を調査する

IoT 機器やシステムに脆弱性があると、それを悪用され被害を受ける可能性がある。脆弱性にも様々な種類があるが、機器やシステムを乗っ取られるような危険性の高い脆弱性もある。脆弱性を把握するためには、定期的にスキャンツールを使用して検出を行い、脆弱性が存在していないかを確認する。

発見された脆弱性に対しては、その影響度や危険度を調べ、重大な脆弱性には迅速に対処を行う。最近では、IoT に対応した脆弱性診断サービスも登場しているので、こうしたサービスを活用することも有効だ。

3.3. 検知プロセス（DE.DP）

48)検知した異常を関係者に伝達する
❶ 検知した情報を異常として判断する体制を明確にする
❷ 異常と判断した情報を速やかに伝達する

IoT 機器やシステムに異常が確認された場合、それを適切に判断し、適切な人間に伝えないと、影響が拡大する危険性がある。IoT 機器やシステムの「異常な状態」を定義し、判断できるようにする。異常と判断した場合には、その情報を速やかに伝達する必要がある。それを誰に伝えるのか、伝える内容も合わせて決めておく。

4. 対応（RS）

4.1. 対応計画（RS.RP）

49)IoT 機器、IoT システムのインシデントに対応する
❶ 速やかに発生事象を把握し、状況（影響など）、証拠（ログなど）を収集する
❷ インシデントの基本的な対応手順をもとに、発生した事象にあわせ対応手順を検討する
❸ インシデントの原因に対処し被害拡大を防止する
❹ 全ての対応活動を記録する

IoT 機器やシステムにセキュリティインシデントが発生した場合、対応手順や対応人員がいないと影響が拡大し、業務にも影響が及ぶ可能性がある。平常時からセキュリティインシデントを定義し、発生した際の対応手順や報告先、被害の拡大防止策などを策定しておく。

インシデントが発生した際には、速やかに発生事象を把握し、状況（影響など）、証拠（ログなど）を収集する。また、インシデントの原因に対処し被害拡大を防止する。深刻な場合には対応チームをすぐに編成できるようにしておき、全ての対応活動を記録する。これにより、収束後の評価が可能になり、改善点を明らかにできる。

4.2. コミュニケーション（RS.CO）

50)インシデント情報を関係者に伝達する
❶ 発生状況の第一報を連絡する
❷ 被害拡大防止など対応策を伝達する

インシデント発生時の報告先を明らかにしていないと、適切な対応を行えず、深刻な事態に発展しやすい。インシデントの発生を確認した場合、誰に伝えるのか、伝達手段とともに明らかにしておく。なるべく短時間で、必要な関係者に連絡が行き渡るよう工夫する。

担当者が不在の場合を考慮し、代理の担当者も決めておくことも重要。連絡を受けた担当者は、その場でできる被害拡大の防止策を伝達できるようにしておく。インシデント発生時の現場での一次対応手順を文書化しておくことも有効な対策となる。

51)インシデント情報を IoT 機器メーカーや提供者に連絡する
❶ インシデントの発生状況をメーカーのサポート窓口へ連絡する

インシデントが発生した際にメーカーのサポート窓口に連絡することで、有効な情報を得られることがある。IoT 機器やシステムのメーカーのサポート連絡先は、すぐに確認できるようにしておく。また、サポート窓口に伝えるべき内容をテンプレート化しておくことも重要。

例えば、使用している IoT 機器の製品名や型式番号、ファームウェアのバージョンなどをあらかじめ用意しておけば、サポート窓口も対応しやすい。

52)IoT 機器、IoT システムのインシデント情報を通知する
❶ CSIRT/PSIRT と連携し報告範囲や内容を検討する

セキュリティインシデントの発生時には、必要な連絡先に通知や報告を行う。業種や業界によっては義務化されていることもある。CSIRT/PSIRT と連携して、セキュリティインシデント発生時の通知先、報告先をあらかじめリストアップしておくとともに、報告する内容についても検討する。業界ごとのガイドラインがある場合には、その内容に沿うようにする。

4.3. 分析 (RS.AN)

53)IoT 機器、IoT システムの管理者、運用担当者の作業ログを確保する
① 管理者及び運用担当者の作業を記録し、そのログを保護し確保する

セキュリティインシデントや不具合が発生した際には、その IoT 機器やシステムの管理者や運用担当者の作業ログを参照することで、原因を特定しやすくなる。IoT 機器やシステムの管理者および運用担当者の作業内容をログとして記録し、参照できるようにしておく。ログを記録しておくことで、担当者の設定ミスや不正行為を可視化できるようになる。

54)IoT 機器、IoT システムのイベントログなどを分析し異常を特定する
① 検知システムからの通知を調査する
② フォレンジック調査などを実施し証拠の保全と原因を推定する
❸ インシデントの判定とその影響を把握する

セキュリティインシデントや不具合が発生した際には、その IoT 機器やシステムのイベントログを分析することで、原因を特定しやすくなる。そのため、平常時からイベントログを記録しておくことは重要。記録したイベントログを分析することで、検知システムからの通知がどのようなもので、いつ通知されたかなどを把握できる。

また、記録したイベントログを参照できるようにしておくことで、フォレンジック調査も迅速に行うことができ、原因の推定もしやすくなる。フォレンジックは証拠保全にも有効なので、警察の捜査や裁判での証拠などにも活用できる。さらに、インシデントの判定とその影響を把握することで、今後の対策や再発生の防止に役立てられる。

55)IoT 機器、IoT システムのインシデントのリスク対応方針を決定する
❶ IoT 機器、IoT システムのインシデントを評価し、対応方針を決定する

IoT 機器やシステムに起こりえるインシデントを想定し、それぞれのリスク評価を行う。また、評価によって対応方針を決定する。これにより、発生したインシデントの種類によって適切な対応が可能となる。例えば、軽微なインシデントは現場の判断で対応することや、重大なインシデントの場合は経営層まで情報を伝達することで、適切で迅速な対応を実現できる。

特に大事なことは、IT の人間と OT の人間の意識の統一を図ることである。特にインシデント対応の考え方が根本的に異なる。例えば、機器にトラブルが発生した場合、OT の人間は故障やバグとして捉えるが、IT、特に情報セキュリティの人間はマルウェア感染を疑う傾向が強い。そのため、OT の人間はインシデント発生時に再起動を行ってしまい、メモリに残った証拠を消してしまう。認識の違いは大きなリスクを生むこと

になるので、リスク対応における意識の統一は非常に重要となる。

4.4. 低減（RS.MI）

56)被害拡大を低減する
❶ ネットワークを遮断しマルウェアの拡大を防止する
② マルウェアを駆除する
③ 脆弱性対応のアップデートを行う

インシデントを放置してしまうと、影響がみるみる拡大してしまう。まずはネットワークを遮断し、マルウェアの拡大を防止する。この際、無線でつながっている場合には、どのようにネットワークを遮断するかを検討しておく。また、マルウェアを駆除するとともに、その感染原因を調査し、脆弱性を悪用されていた場合にはパッチやアップデートなどの対処を行う。またこの際には、権限を持つ適切な担当者へ迅速に連絡できるよう、伝達系統や手段も決めておく。

4.5. 改善（RS.IM）

57)IoT 機器、IoT システムのインシデントから学習する
❶ 対応計画の見直し改善に利用する

一連のインシデントが収束し、原状復旧が完了したら、原因から発生、伝播状況などをまとめ、再発防止に取り組む。特に発生時の対応計画については見直しを行い、より迅速、確実な対応を行えるよう改善していく。評価には経営層も参画してもらい、インシデント対応の重要さを理解してもらうことも重要。必要があればインシデント対応における企業のポリシーの変更なども行う。

5. 復旧（RC）

5.1. 復旧計画（RC.RP）

58)IoT 機器、IoT システムをインシデント発生前の状態に復旧する
❶ インシデントの基本的な復旧手順をもとに、発生した事象にあわせ復旧手順を検討する
❷ 復旧体制と復旧費用を検討し承認を得る
❸ 復旧が完了したことを確認する
❹ インシデントの原因に対処し被害拡大を防止する

インシデントの収束後には、IoT 機器やシステムを発生前の状態に復旧する。あらかじめ策定された基本的な復旧手順をもとに、発生したインシデントに合わせて最適な復旧手順を検討する。

復旧手順が固まったら、必要な体制や費用などを算出し、上層部の承認を得る。復旧後は問題がないか再確認を行い、再びインシデントが発生しないよう対処を行う。特に、同じ原因で再びインシデントが発生しないよう、十分な対策を行う。

5.2. 改善（RC.IM）

59)IoT 機器、IoT システムのインシデントから再発防止を検討する
❶ インシデントから得た情報を再発防止に活用する
❷ 同種のインシデントが他の IoT 機器、IoT システムで発生しないか確認する
❸ 復旧計画の見直し改善に利用する

復旧が完了したら、発生したインシデントから得られた情報をもとに、再発防止策を検討する。また、同種のインシデントが他の IoT 機器やシステムで発生する可能性がないかを確認する。

さらに、復旧計画や手順なども見直し、インシデント対応から得られた知見を追加し、改善を行う。再発防止のために新たな担当や権限を設けたり、報告の伝達経路なども再整備する。

5.3. コミュニケーション（RC.CO）

60)IoT 機器、IoT システムのインシデント情報を通知する
❶ 利用者にインシデントの存在又は関連するその詳細を通知する
❷ 同種のインシデントがサプライチェーンの中で発生しないか関連会社に伝達する
❸ CSIRT/PSIRT と連携しステークホルダーに報告する

IoT 機器やシステムにインシデントが発生した際には、利用者にもインシデントの存在や関連情報を通知し、影響や今後の対応などについて説明責任を果たす。また、自社で発生した IoT 機器やシステムのインシデントは、サプライチェーンでも発生する可能性がある。

このため、インシデントの内容や対応手順、復旧手順などの情報をサプライチェーンと共有し、未然に防ぐ努力をする。さらに、CSIRT/PSIRT と連携しステークホルダーに報告することも重要な対応となる。

発行者 ： 一般社団法人 日本スマートフォンセキュリティ協会（JSSEC）利用部会

連絡先 ： 一般社団法人日本スマートフォンセキュリティ協会　事務局
TEL 03-6757-0159　　https://www.issec.org/　（お問い合わせ先参照）