

第6回

IoTチェックシート活用

～IoT機器導入に使ってみる～

2020年9月15日

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TF

本間 輝彰（KDDI株式会社）

前回までのおさらい

第1回

セミナーの概要と受講の進め方

～安心・安全にIoTを活用するために～

第2回

チェックシートの特徴と セキュリティの重要性

～安心・安全にIoTを活用するために～

第3回

チェック項目「識別」の解説

～ビジネス環境やIoT資産を把握し、
リスクの想定と対応方針を定める～

第4回

チェック項目「防御」の解説

～リスク対応方針に基き、物理面、人的面、
技術面から防護策を実施する～

第5回

チェック項目 「検知」「対応」「復旧」の解説

～異常を検知するしくみの構築から
被害拡大の防止・復旧まで～

本コンテンツは、IoTセキュリティチェックシート入門第1回～第5回を視聴された方が対象となっておりますので、まだの方は先に視聴する事をお勧めします

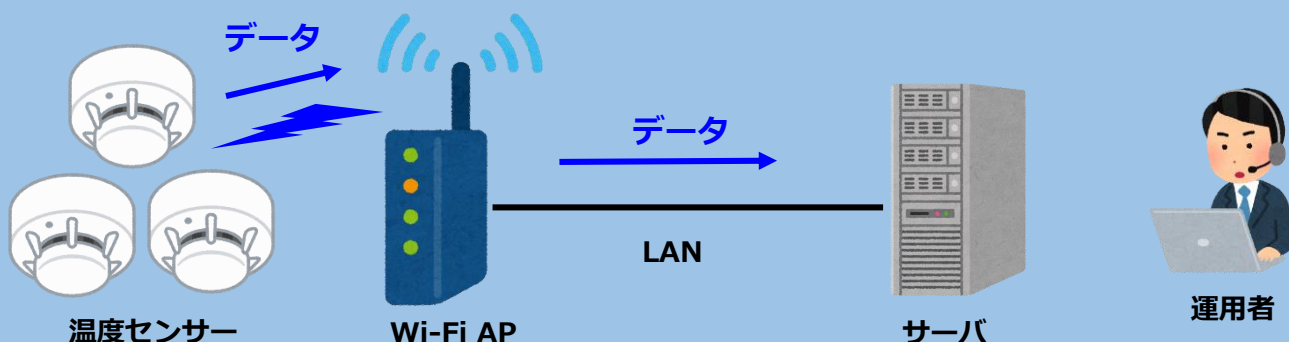
JAPAN
SMARTPHONE
SECURITY
ASSOCIATION

今回は、IoT機器を導入するにあたり、IoTセキュリティチェックシートをどのように使えばいいか、実践的な説明をします

さっそく始めてみましょう！

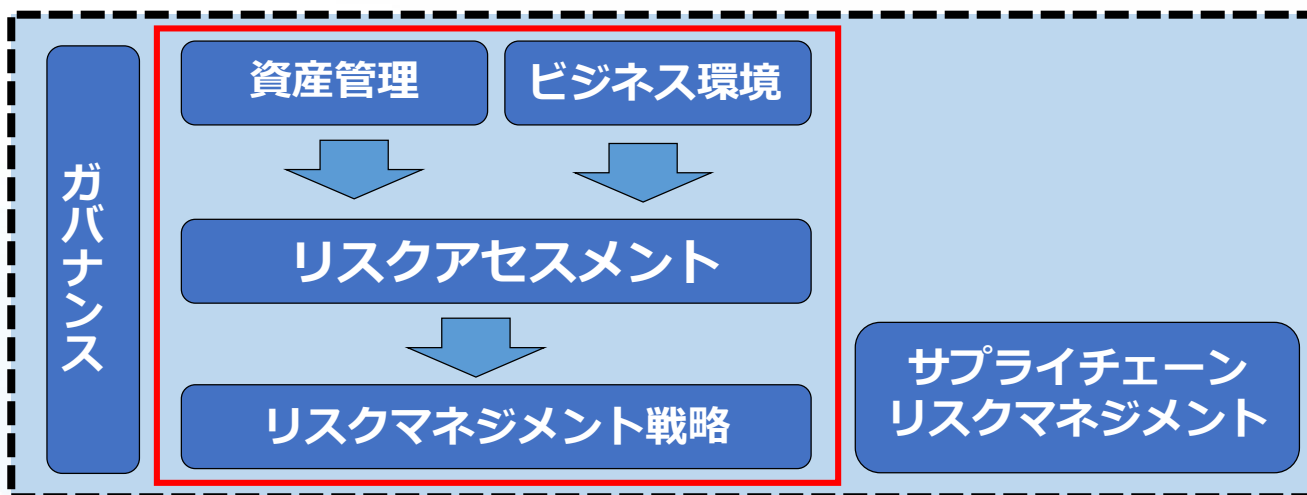
今回は**初級編**として、市販の**温度センサー**導入を想定した説明となります
また、本格的なIoTの導入として**基幹ビジネス**を想定し、**チェックシート活用のポイント**を中心に紹介します

温度センサーはWi-FiでWi-Fi APに接続され、データはWi-Fi APとLANで接続されたサーバに送信され、そのデータを監視者が監視するケースで考えます。また、監視する情報は工場内の温度となります



用途レベル毎の推奨項目		
PoC又は 補助的	基幹 ビジネス	重要 ビジネス

“識別”のポイントは、**ビジネス環境やIoT資産を把握し**、システム、人員、資産、データに関するセキュリティの**リスク管理を理解することになります**

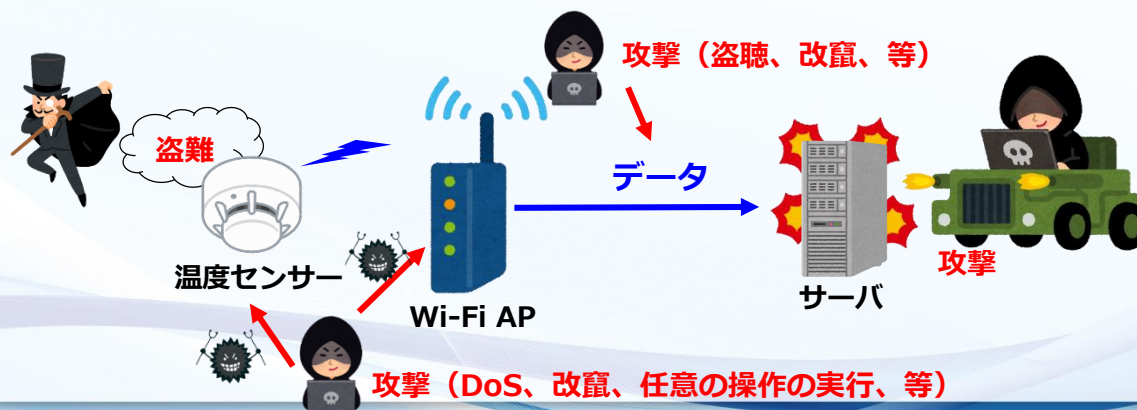


IoTのセキュリティ対策を進める上で、“**識別**”が十分でない場合、以後の検討が無意味になる可能性があるので、確実に実施する事を推奨します

■ビジネス環境やIoT資産を把握するには、システム構成を明確にし、扱うデータ、データの流れを理解します。また、異常が発生した場合にどのような影響があるかも明らかにします



■リスク管理を理解するために、想定されるリスク（攻撃手段）を抽出し、その結果を踏まえて対策を立てます

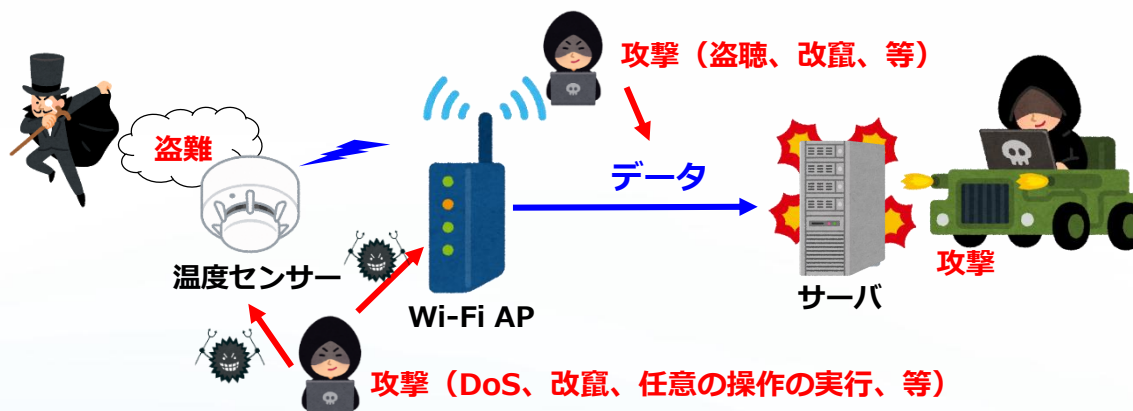


■ビジネス環境やIoT資産を把握するには、システム構成を明確にし、扱うデータ、データの流れを理解します。また、異常が発生した場合にどのような影響があるかも明らかにします



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
	①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
	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
	03)IoT機器、IoTシステムの関係者の役割を把握する
	①IoT機器、IoTシステムの管理責任者の役割
	②IoT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
	③IoT機器、IoTシステム運用や保守担当の役割
	④CSIRT/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）
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
	①IoT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
	②IoT機器、IoTシステムが重要なビジネス又は基幹ビジネスに大きな影響を与えないか調査する

■ リスク管理を理解するために、想定されるリスク（攻撃手段）を抽出し、その結果を踏まえて対策を立てます

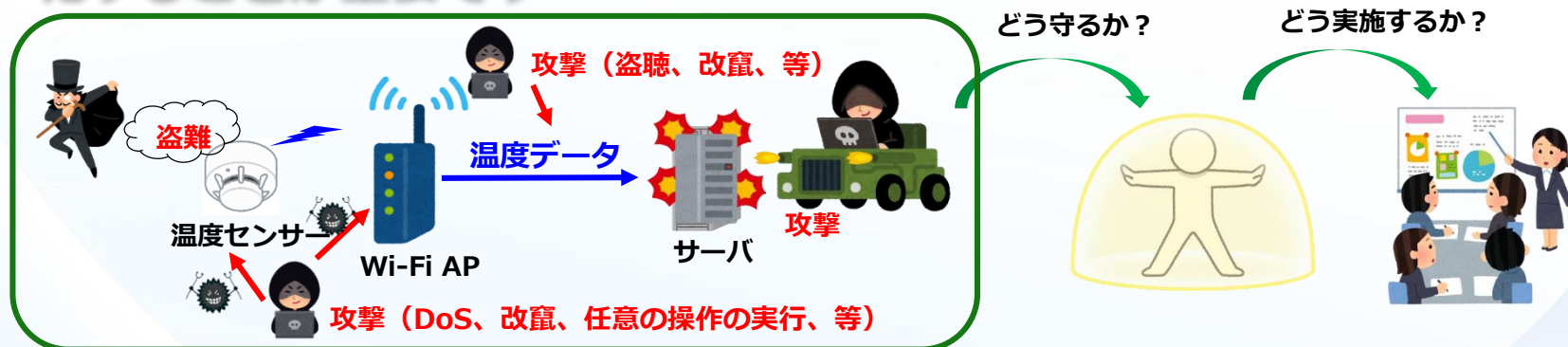


リスクアセスメント (ID.RA)

- 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
- 08) 保守作業時のリスクを想定する
 - ① 保守員の悪意を想定する
 - ② 保守ツールからのマルウェア感染を想定する
- 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
- 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
 - ① 連携する機器やシステムに影響をあたえるリスクを想定する
 - ② マルウェアなどが波及するリスクを想定する
 - ③ 既存機器（セキュリティ対策が不十分な組込系など）へ影響をあたえるリスクを想定する
- 11) IoT機器の盗難・紛失・破壊などのリスクを想定する
 - ① 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
- 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
- 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
- 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

“防衛”では、**攻撃を防ぎ、リスクを軽減する方法**を物理的、人的、技術的の多層的に検討します。また、防衛策の策定・実施は**ITとOTが協力**して行う

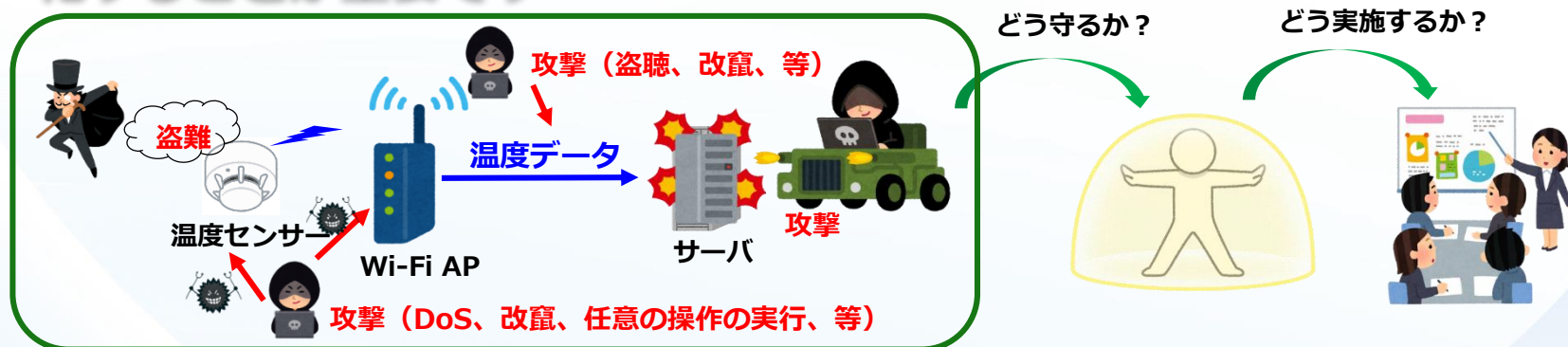
■守りの基本は、ID/パスワードを正しく管理し、不正アクセスされないように必要のないアクセス手段は閉じ、万が一に備えて暗号化することが重要です



■新たな脆弱性の対策として、ソフトウェアのアップデートを定期的に更新し、安全な環境を維持します

“防衛”では、**攻撃を防ぎ、リスクを軽減する方法**を物理的、人的、技術的の多層的に検討します。また、防衛策の策定・実施は**ITとOTが協力**して行う

■守りの基本は、ID/パスワードを正しく管理し、不正アクセスされないように必要のないアクセス手段は閉じ、万が一に備えて暗号化することが重要です



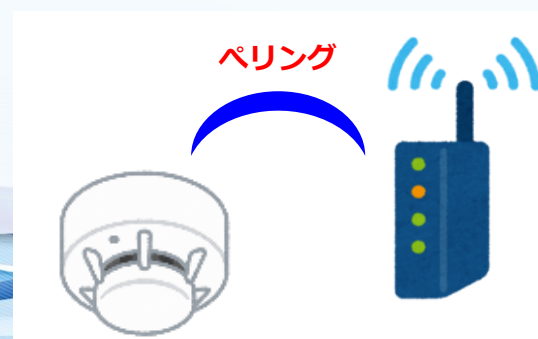
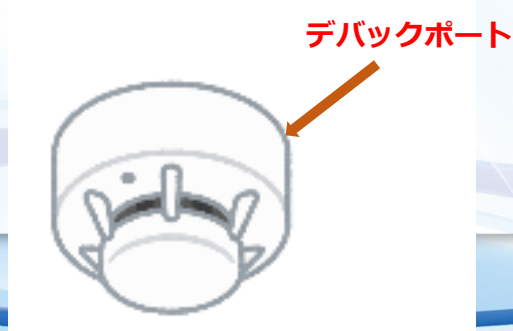
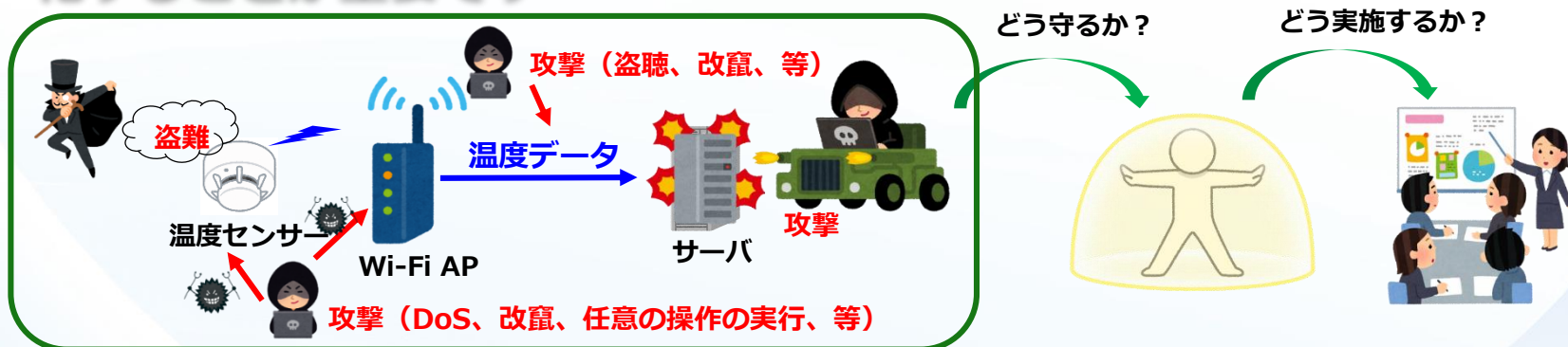
アイデンティ
ティ管理、認証
／アクセス制御
(PR.AC)

- | |
|---|
| 22)IoT機器の機能およ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 |
| ①IoT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） |
| ②IoT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 |
| 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サービスに必要な不要なポートは停止する |
| 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 |
| 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および管理を適切に行う |
| ①ID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 |
| ③IDとパスワードを権限のないユーザと共有しない |
| ④IDとパスワードを他システムと使いまわししない |

防衛

“防衛”では、**攻撃を防ぎ、リスクを軽減する方法**を物理的、人的、技術的の多層的に検討します。また、防衛策の策定・実施は**ITとOTが協力**して行う

■守りの基本は、ID/パスワードを正しく管理し、不正アクセスされないように必要のないアクセス手段は閉じ、万が一に備えて暗号化することが重要です



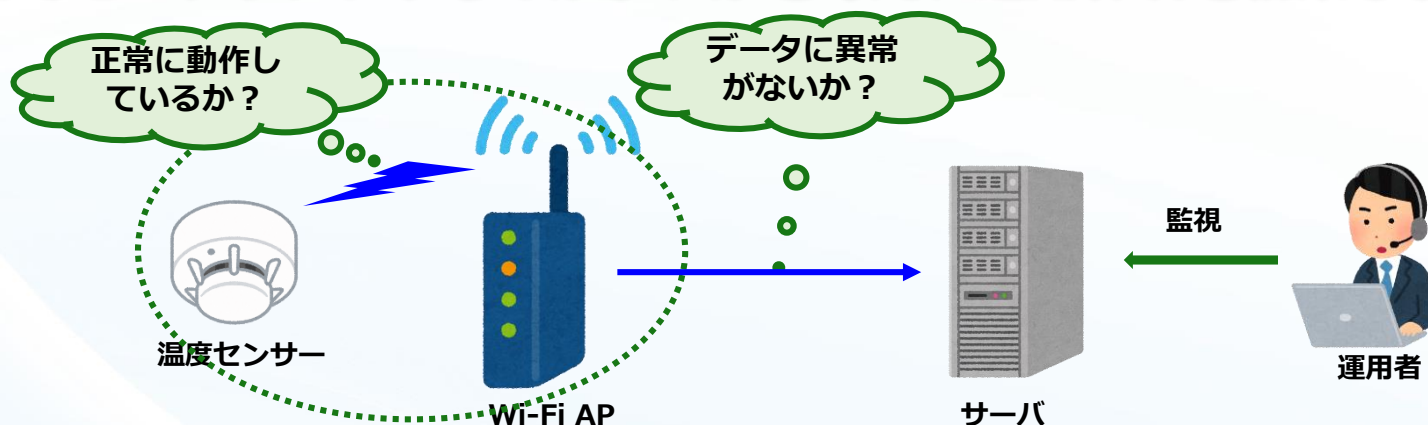
■ 新たな脆弱性の対策として、ソフトウェアのアップデートを定期的に更新し、安全な環境を維持します

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
	①IoT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
	②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
	41)IoT機器、IoTシステムの構成情報を最新にする
	①IoT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
	42)保守作業時の手順を明確にする
	①許可されたツールを使用する ②遠隔保守の不正アクセス対策を実施する ③保守の履歴を管理する

検知

“検知”では、異常をタイムリーに発見するために、**異常を検知する手段を確立し、継続的なモニタリング**することで実現可能になります

■ 異常を検知するには、どの情報をどう検証するかを考え、監視する方法を考えます。また、異常時の影響を考慮し、どのような周期でモニタリングするのがよいかを考え、運用体制を構築します

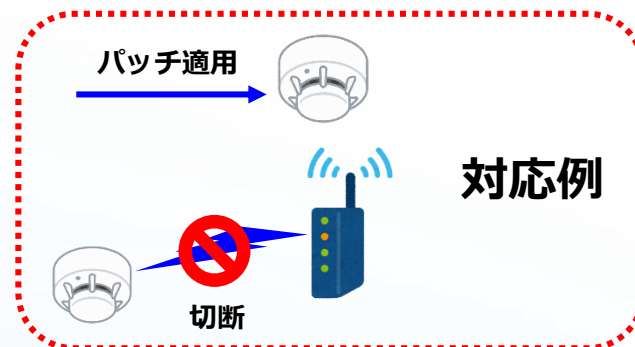


異常とイベント (DE.AE)	45)IoT機器、IoTシステムの異常を把握する
	①IoT機器のログやインベントリ情報から異常の検知方法を検討する（異常はなにかを定義）
	②異常として検知するしきい値を検討する
セキュリティの 継続的なモニタ リング (DE.CM)	③異常の影響を把握する
	46)ネットワーク機器やIoTシステムの異常を継続的に監視する
	①設置したIoT機器のログなどをモニタリングし異常を検知する仕組みを検討する
	②設置したIoT機器にマルウェアなどが存在しないか調査する仕組みを検討する
	③異常を検知する仕組みを継続的に運用しモニタリングする
	47)設置したIoT機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

対応・復旧

“対応”は、検知した異常に対して速やかに対応を行い、**被害拡大を防止**することが目的となります

■異常が発生したら、必要な情報を集めながら、迅速に適任者に引継ぎをします、適任者は状況を判断し、必要な対応を実施します



“復旧”では、異常を全てクリアにし、適切な処理を行い**システムを健全な状態に戻す**こととなります

■復旧では、問題が発生したシステムのみの対処ではなく、情報展開や振り返りによる再発防止も重要です



対応・復旧

“対応”は、検知した異常に対して速やかに対応を行い、**被害拡大を防止**することが目的となります

■異常が発生したら、必要な情報を集めながら、迅速に適任者に引継ぎをします、適任者は状況を判断し、必要な対応を実施します



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 ①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 ②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 ③インシデントの原因に対処し被害拡大を防止する ④全ての対応活動を記録する
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管理者およ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 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 ③インシデントの判定とその影響を把握する 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 ①IoT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
低減 (RS.MI)	56)被害拡大を低減する ①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

“復旧”では、異常を全てクリアにし、適切な処理を行い**システムを健全な状態に戻す**こととなります

■復旧では、問題が発生したシステム
のみの対処ではなく、情報展開や振り
返りによる再発防止も重要です



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

- ① 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
- ② 復旧体制と復旧費用を検討し承認を得る
- ③ 復旧が完了したことを確認する
- ④ インシデントの原因に対処し被害拡大を防止する

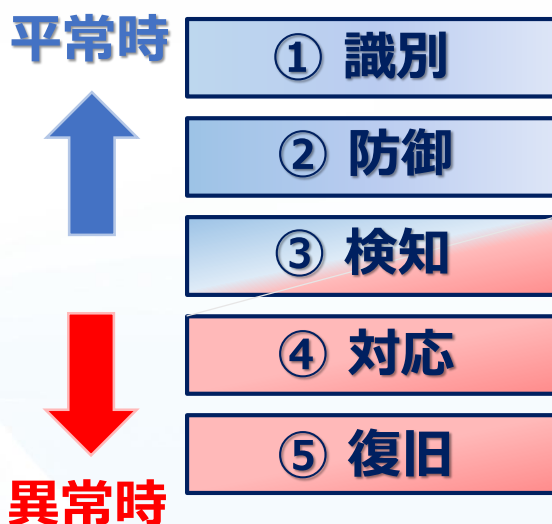
改善 (RC.IM)

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

- ① インシデントから得た情報を再発防止に活用する
- ② 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
- ③ 復旧計画の見直し改善に利用する

まとめ

- ①IoT機器は後追いでセキュリティ対策をする事は困難である
- ②情報セキュリティと組込み系システム担当の協調が必要である



“識別”で導入するIoT機器に適したやり方を見極め、適切な“防御”を行い、万が一に備えて、“検知”、“対応”、“復旧”の手順を定め**バランスよく実施する**のが重要



特に、重要システムでは**最悪**を想定して、検知・対応・復旧の検討をすることが大事です

用途レベル毎の推奨項目		
PoC又は 補助的	基幹 ビジネス	重要 ビジネス

■ IoTセキュリティチェックシートなど資料の入手

- ① 受講に必要な資料をJSSECホームページよりダウンロード（登録不要、無料）して下さい。

<https://www.jssec.org/iot>

■ IoTセキュリティチェックシート 第2.1版（PDF版）

JSSEC



JSSEC IoTセキュリティチェックシート第二版 ダウンロードページ

利用部会の成果物
「JSSEC IoTセキュリティ
チェックシート第二版」が
以下よりダウンロード
出来ます。

- ①IoTセキュリティチェックシート 第二版（2019年2月28日）
 - チェックシートPDF版
 - チェックシートExcel版
- ②IoTセキュリティチェックシート 第二版 解説編（2019年4月1日）
 - 解説編
 - FAQ
- ③ご質問や勉強会、セミナー講師派遣などの問い合わせ
 - 問い合わせフォーム



JAPAN
SMARTPHONE
SECURITY
ASSOCIATION

