JAPAN SMARTPHONE SECURITY ASSOCIATION

第4回

チェック項目「防御」の解説

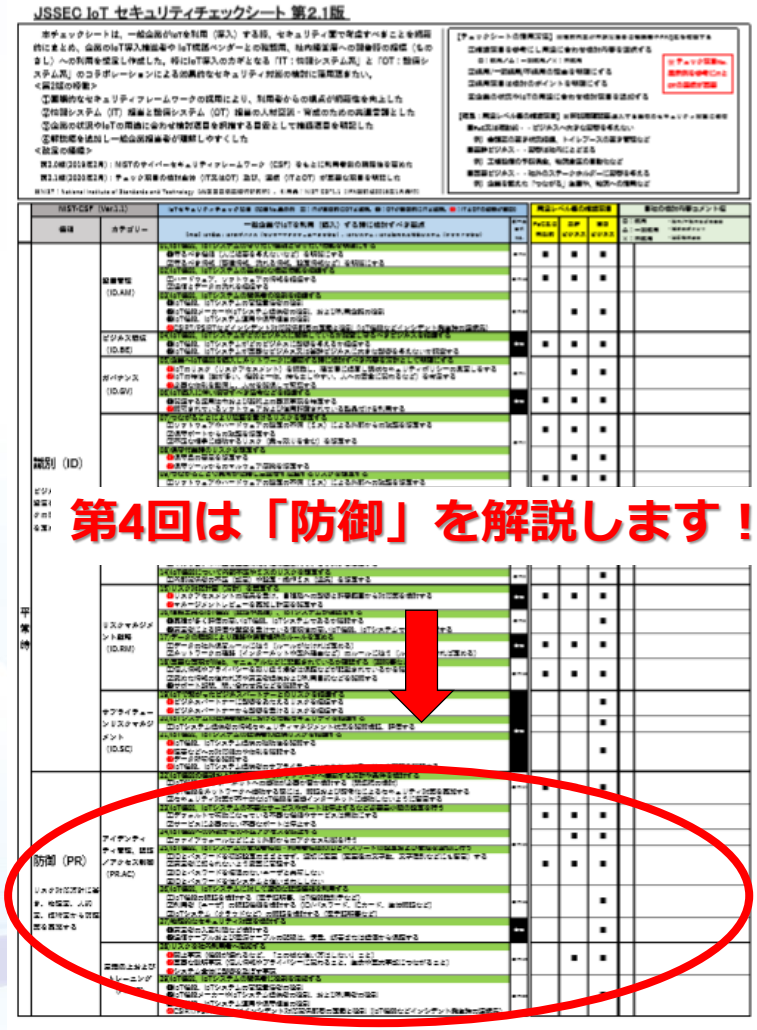
～リスク対応方針に基き、物理面、人的面、技術面から防護策を実施する～

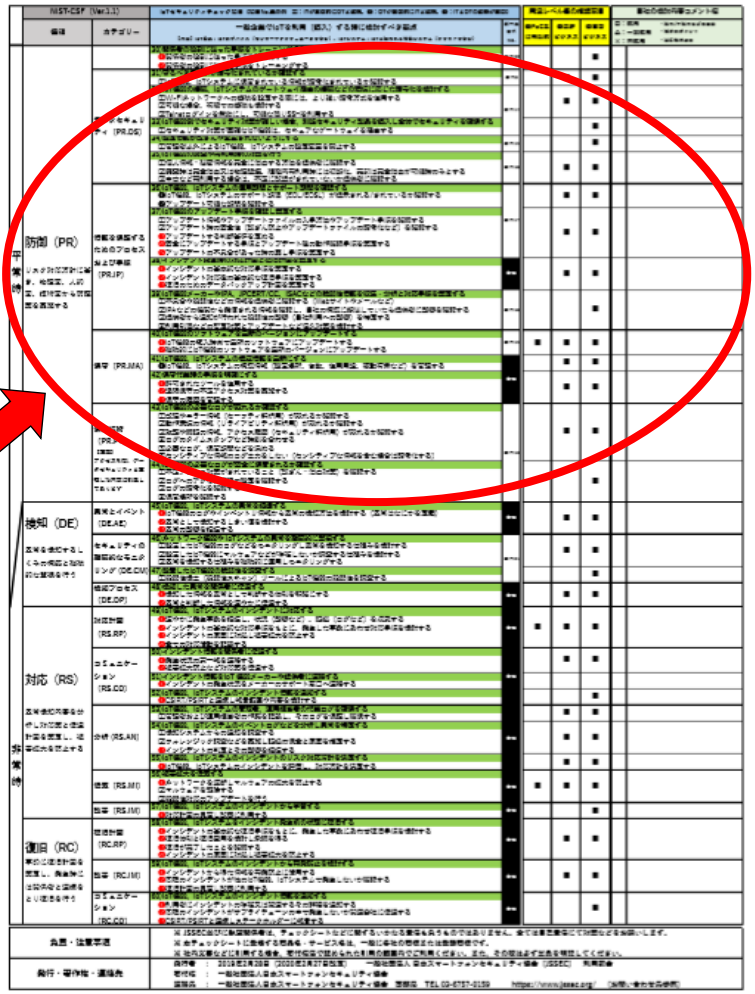
2020年9月1日

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
中村 丈洋（株式会社 SHIFT SECURITY）

IoTセキュリティチェックシート

JAPAN SMARTPHONE SECURITY ASSOCIATION





チェック項目「防御」

JAPAN SMARTPHONE SECURITY ASSOCIATION

❶NIST-CSFの分類：平常時、6カテゴリー
(1)アイデンティティ管理、認証／アクセス制御 (2)意識向上およびトレーニング
(3)データセキュリティ (4)情報を保護するためのプロセスおよび手順
(5)保守 (6) 保護技術
❷企業のIoT推進者や管理者の視点で検討すべき点：23項目
❸IoT用途レベル毎の推奨項目：3つの重要度に分類
❹各社の検討内容　採用理由／追加項目：検討結果の見える化
❺検討主体（IT又はOT）及び、連携（ITとOT）が重要な項目を明記

❶ ❺ ❷ ❸ ❹

NIST-CSF（Ver.1.1）		IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】		用途レベル毎の推奨項目			自社の検討内容コメント欄	
機能	カテゴリー	一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.	PoC又は補助的	基幹ビジネス	重要ビジネス	◎：採用　・採用/不採用などの理由 △：一部採用　・検討のポイント ×：不採用　・追加検討項目	
防御（PR） 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	アイデンティティ管理、認証／アクセス制御（PR.AC）	(2)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）	要点14	■	■	■		
		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						
		(3)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サービスに必要のない不要なポートは停止する						
		(4)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	要点15		■	■		
		(5)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						
		(6)IoT機器、IoTシステムに対して適切な認証機能を利用する						
		①IoT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）	要点16			■		
		③IoT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）						
		(7)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	新規			■		
		❷通信ケーブルおよ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						
		(8)リスクを社内利用者へ周知する						

防御について

JAPAN SMARTPHONE SECURITY ASSOCIATION

- 「攻撃を防ぎリスクを軽減するための活動」をチェック
- 防御策の策定・実施はITとOTが協力して行う
- IoTの防御は 物理的、人的、技術的 と多層的に行う
- 「防御」は6つのカテゴリに分類される
  - ①ID管理、認証／アクセス制御
  - ②意識向上およびトレーニング
  - ③データセキュリティ
  - ④情報を保護するためのプロセスおよび手順
  - ⑤保守
  - ⑥保護技術
- 以下、ひとつづつ見ていきましょう。

ID管理、認証/アクセス制御

JAPAN SMARTPHONE SECURITY ASSOCIATION

IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】 一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.	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
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	要点14			
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	要点15			
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サービスに必要のない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				
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	要点16			
①IoT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）				
③IoT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）				
27)物理的なセキュリティ対策を検討する	新規			
❶第三者の入室制限など検討する				■
❷通信ケーブルおよ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				

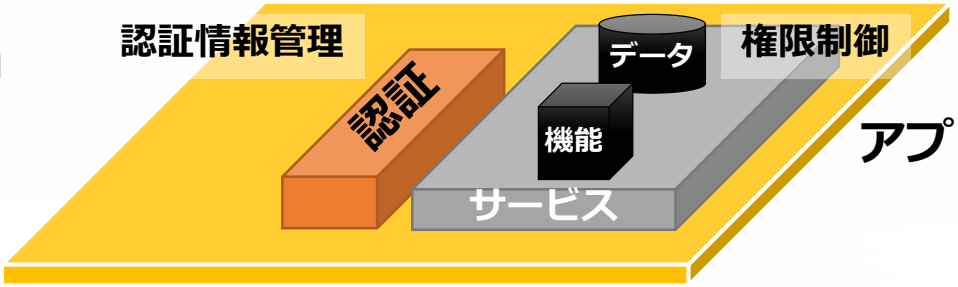
■不正アクセスの防止策を策定・実施

- 適切なID/パスワードの管理（No.25）
- 認証による資産の保護（No.26）
- 論理的（No.22, 23,24）、物理的（No.27）なアクセス制御

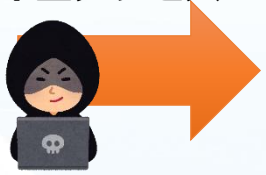
ID管理、認証/アクセス制御　ケーススタディ

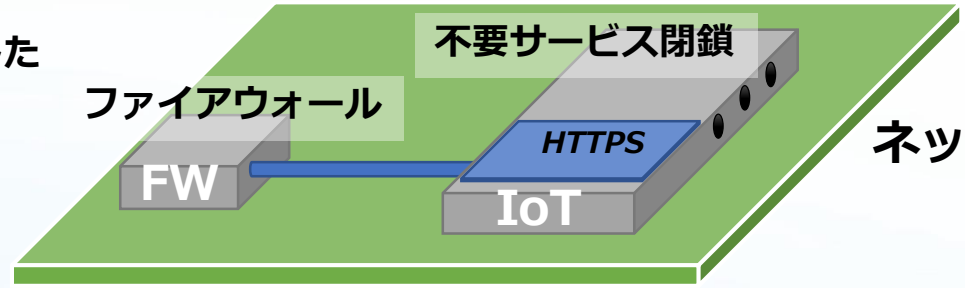
JAPAN SMARTPHONE SECURITY ASSOCIATION

弱い認証を利用した
不正アクセス 認証制御

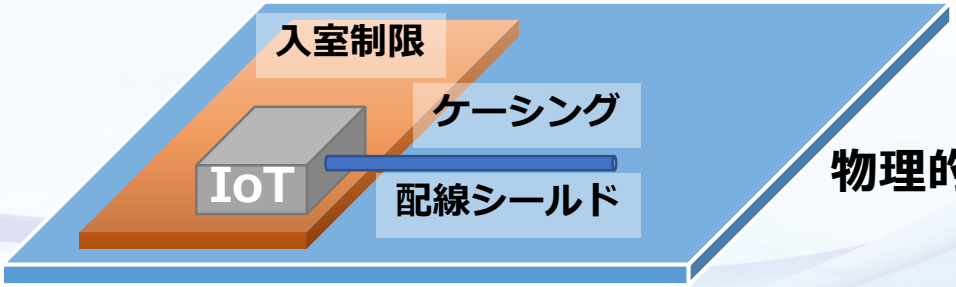


既知の脆弱性を利用した
不正アクセス





物理的な侵入により
不正アクセス



意識向上およびトレーニング

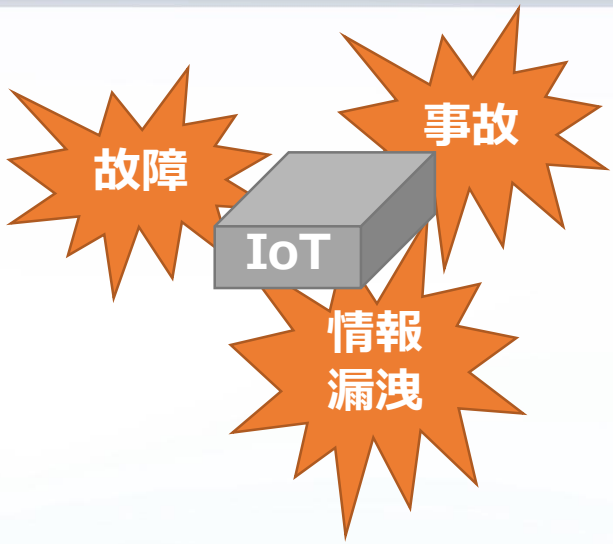
JAPAN SMARTPHONE SECURITY ASSOCIATION

IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】 一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.	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
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）	要点19		■	■
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				
29)IoT機器、IoTシステムの関係者に役割を周知する				
❶IoT機器、IoTシステムの管理責任者の役割	要点20			■
❷IoT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				
❸IoT機器、IoTシステム運用や保守担当の役割				
❹CSIRT/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				
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	要点20			■
❷関係者の役割に従った手順をトレーニングする				

■組織の構成員に対するセキュリティ規則の周知、意識造成とトレーニング

- **利用者への注意・禁止事項の周知する（No.28）**
- **関係者（各運用担当者、管理者等）に役割を周知する（No.29）**
- **役割に従った手順策定とトレーニングの実施（No.30）**

意識向上およびトレーニング　ケーススタディ



機器の誤動作が重大事故につながることも

禁止事項・注意事項 を定める

インシデント発生時の役割を明確化

システム運用者、保守担当者と
情報セキュリティ部門、CSIRTの協調が重要

「定める」だけでなく「守る」活動が必要

周知徹底とトレーニング

実践してみるとルールや手順の問題点も見えてくる。
定期的なトレーニングにより担当者のセキュリティ意識を育てる。

データセキュリティ

JAPAN SMARTPHONE SECURITY ASSOCIATION

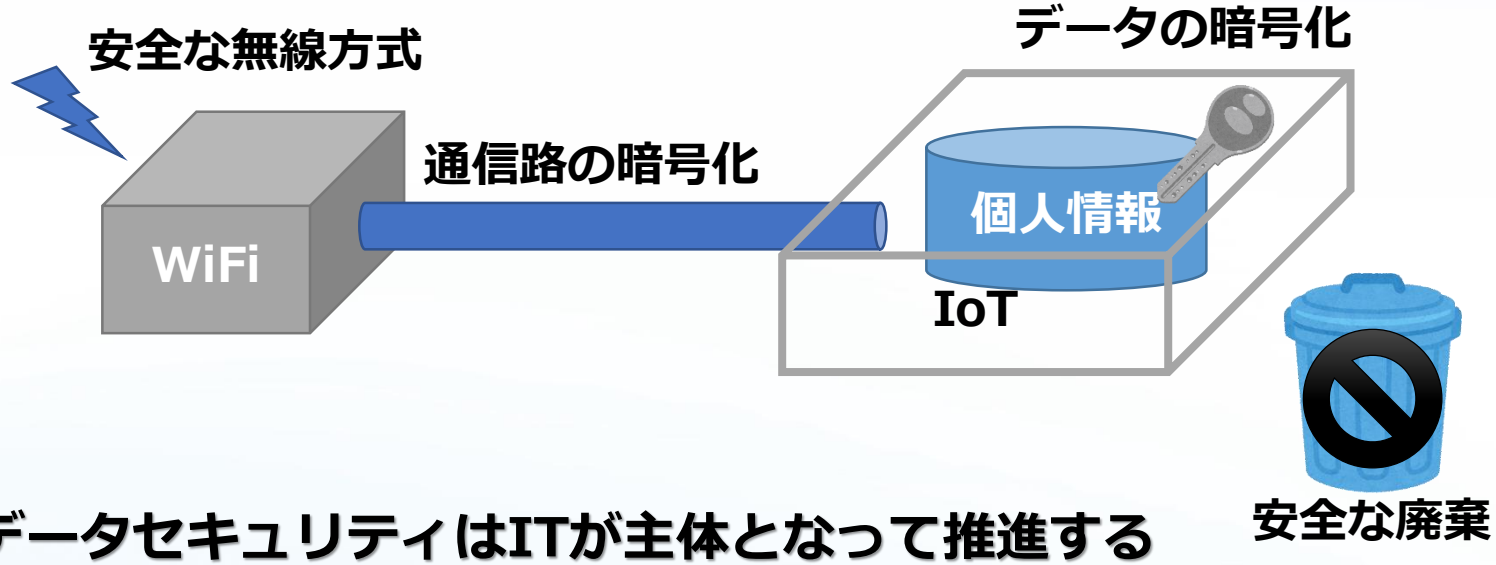
IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】 一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.	用途レベル毎の推奨項目 PoC又は補助的	基幹ビジネス	重要ビジネス
31)守るべきデータが暗号化されているか確認する	要点8			
①IoT機器、IoTシステムに保管されている情報が暗号化されているか確認する			■	■
32)IoT機器の接続、IoT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	要点14			
①Wi-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				
③Telnetログインを無効にし、可能な限りSSHを利用する				
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				
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				■
34)設定情報が改ざんや変更されないようにする	要点15			
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				■
35)IoT機器の廃棄や再利用時の対策を行う	要点18			
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				

■**IT主体でデータの機密性・完全性・可用性を確保**
- **データの暗号化（No.31）と通信路の暗号化（No.32）**
- **機器自体での暗号化が困難な場合の代替策の検討（No.33）**
- **管理権限の明確化（No.34）**
- **廃棄のデータ消去と再利用時の安全確保（No.35）**

データセキュリティ　ケーススタディ

JAPAN SMARTPHONE SECURITY ASSOCIATION

IT主体での「データ」の保護



データセキュリティはITが主体となって推進する

- ■データや通信路の暗号化
- ■無線機器利用時の安全な方式選定

etc.

情報保護のプロセス

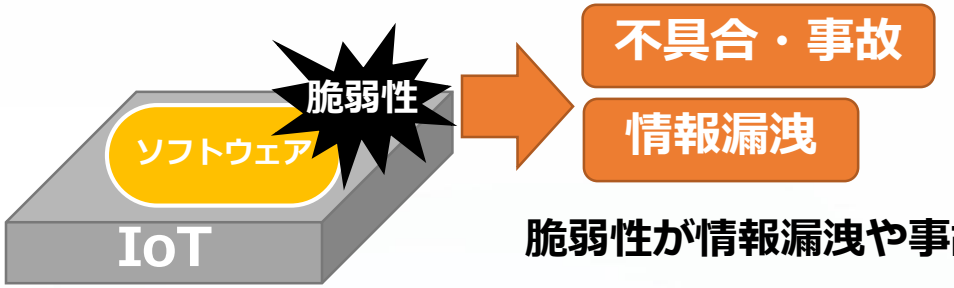
JAPAN SMARTPHONE SECURITY ASSOCIATION

IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】 一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.	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
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				
❶IoT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				
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	要点17			
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				
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	新規			
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				
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）				
②IPA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	要点18			■
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				

■セキュリティ方針、プロセス、手順による情報の保護
- 機器/システムの保守についての計画と手順化（No.36, 37）
- インシデント対応時の対応/復旧の計画策定（No.38）
- セキュリティ情報収集の計画（No.39）

情報保護のプロセス　ケーススタディ

IoTのシステムはハードウェア以外にも様々なソフトウェアで構成される。
例）ファームウェア、OS、アプリケーション



脆弱性が情報漏洩や事故に発展する場合も

IoTシステムの維持にはソフトウェアのアップデートが重要

■「いつまで」アップデートが提供されるか… エンドオブライフ=EOLを認識

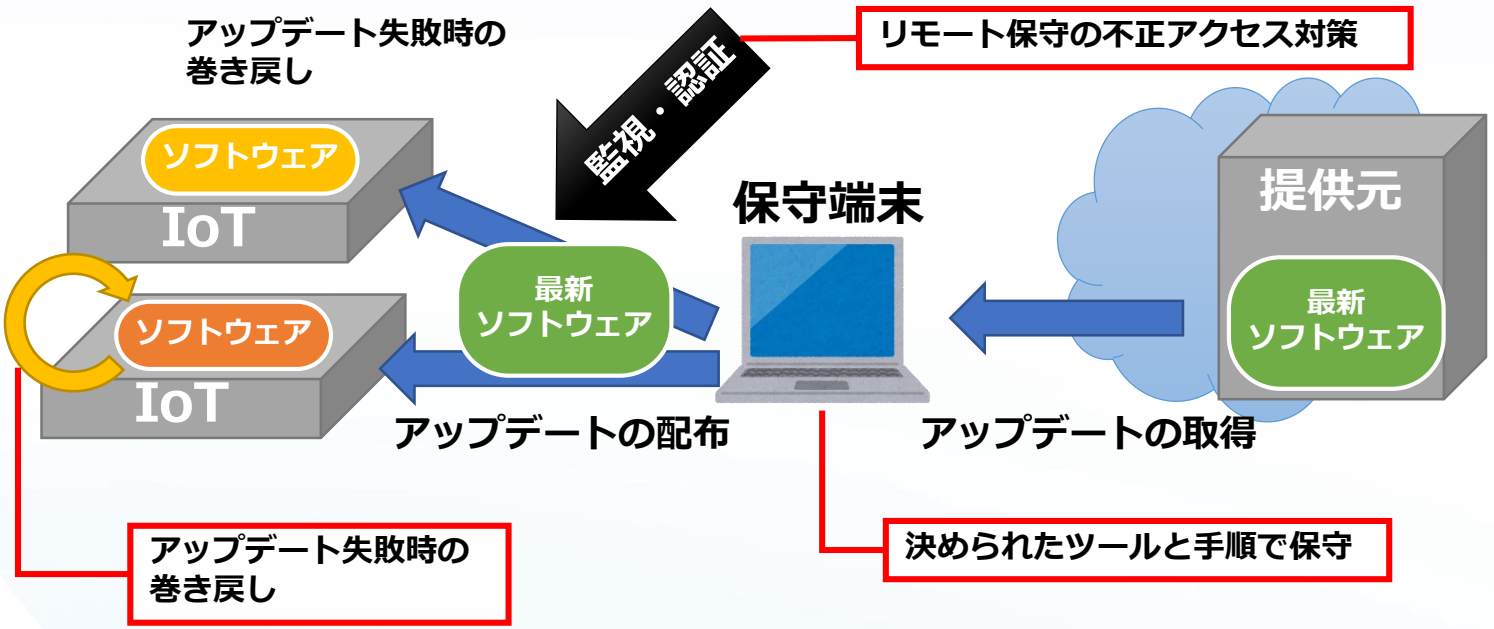
①「いつ」アップデートするか？
　■保守のタイミング・頻度を定める
②「どうやって」アップデートするか？
　■閉環境におけるアップデート方法など、特殊な場合も生じうる

保守

IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】 一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.	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
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				
❶IoT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	要点15	■	■	■
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				
41)IoT機器、IoTシステムの構成情報を最新にする				
❶IoT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	新規			
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				

■「情報保護のプロセス」で定めた方針にそった保守の実施
- ソフトウェアの更新（No.40）
- 構成情報の更新（No.41）
- 保守作業の明確化（No.42）

保守　ケーススタディ

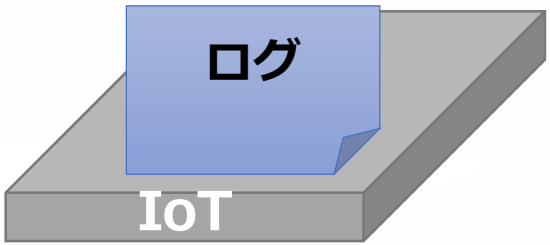

アップデート失敗時の
巻き戻し
リモート保守の不正アクセス対策
監視・認証
ソフトウェア
IoT
ソフトウェア
IoT
保守端末
最新
ソフトウェア
提供元
最新
ソフトウェア
アップデートの配布
アップデートの取得
アップデート失敗時の
巻き戻し
決められたツールと手順で保守

保護技術

IoTセキュリティチェック項目【項目No.表示例　①：ITが主体的にOTと連携、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】 一般企業でIoTを利用（導入）する時に検討すべき観点 【用語】IoT機器：IoTのデバイス（センサーやアクチュエータを含む）、IoTシステム：IoTに使われる情報システム（クラウドを含む）	第一版要点No.	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
43)IoT機器の必要なログが取れるか確認する	要点13			
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）				
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				

■前述以外のシステムを保護するための技術
ここでは主に証跡による利用者/システムの保護に着目
・ログを収集・保管する（No.43, 44）※ IT主体

保護技術　ケーススタディ



アクセス・操作履歴やシステムエラー等を
「ログ」として保管

■問題の予兆を検知
■問題発生時の原因/影響範囲を把握

ログを取ることは有用であり、重要だが、
「個人情報」等がログに含まれる場合には扱いに注意が必要
■ 記録対象の選択、個人情報のマスキング、暗号化

次回の紹介

JAPAN SMARTPHONE SECURITY ASSOCIATION

■IoTセキュリティチェックシート入門

■次回は「チェック項目 検知・対応・復旧」になります。

⑤検知・対応・復旧
■異常を検知する仕組みを構築します
■被害拡大を防止し、システムを復旧するための対策を定めます

次回の受講おまちしております。

ご覧頂きありがとうございました

JAPAN SMARTPHONE SECURITY ASSOCIATION

～安心・安全にIoTを活用するために～