JAPAN SMARTPHONE SECURITY ASSOCIATION

「IoT導入に必要なセキュリティ対策をどう進めるか？」

～JSSEC IoTセキュリティチェックシートの活用方法～

2019年11月12日

日本スマートフォンセキュリティ協会 （JSSEC）
利用部会 部会長　後藤　悦夫 （株式会社ラック）

当事業は「公益財団法人 電気通信普及財団」による助成を受けております。

本日の内容

JAPAN SMARTPHONE SECURITY ASSOCIATION

<概要>
企業でIoTの活用推進していくためには、IoTを安心・安全に利用することが求められる。今回IoTを利用する企業の視点からセキュリティ対策のポイントを解説する。

1. IoTセキュリティチェックシート概要
①セキュリティチェックシート検討の経緯
②なぜNIST-CSFを採用したか
③チェックシートの構成と特徴

2. IoT導入のためのチェックシート活用方法
①企業のIoT活用とセキュリティ対策の大切な点
②チェックシート活用のポイント

3. IoTセキュリティ対策向上のための活動
①啓発活動への取組
②人材育成のために

JSSEC利用部会の紹介

JAPAN SMARTPHONE SECURITY ASSOCIATION

一般社団法人　日本スマートフォンセキュリティ協会

https://www.jssec.org/

会員：86社＋30法人（特別会員、オブザーバー ） <2019年5月現在>

スマートフォンの**安全な利活用を図り普及を促進する**ために2011年5月設立

➔ **４年前からスマホセキュリティの知見をIoTセキュリティに活かす活動**

利用部会　技術部会　啓発事業部会　ＰＲ部会

「企業を中心とした利用者の視点で活動」

IoT調査・研究TF　利用ガイドラインWG　事例研究WG

テーマ：「スマホを機軸としたIoT時代のセキュリティ」

・IoT時代、ユーザとの窓口はスマートフォンが担う

・IoTもスマートフォンも、使われ方に合わせたセキュリティ

自己紹介

■ **株式会社　ラック**（本社：東京、名古屋/福岡に事業所）
サイバー・グリッド・ジャパン　ICT利用環境啓発支援室

■ **一般社団法人　日本スマートフォンセキュリティ協会**
利用部会　部会長

後藤　悦夫　etsuo.goto@lac.co.jp

＜業務の経歴＞

～2015/3　　トヨタ自動車株式会社　情報部門
- 情報インフラ系の企業間EDI基盤、社内情報共有、DC災害対策など
- 情報セキュリティのポリシーやルールの策定、働き方変革の推進など

2015/4～　　株式会社　ラック　サイバー・グリッド研究所　客員研究員
- JSSEC活動を中心にIoTの調査・研究（主に利用企業の視点）

＜JSSECの経歴＞

2011/5～　　JSSEC発足と同時に　利用部会　ガイドラインWGに参加
2013/4～　　JSSEC　利用部会　副部会長
2015/4～　　JSSEC　利用部会　部会長

はじめに

JAPAN SMARTPHONE SECURITY ASSOCIATION

①IoTは、知らないうちに使われる…

■PCが企業の中に入って来た時を思い出そう!

➔ 個人PCを 会社に持ち込み業務利用、など

■スマホはどうでした？

➔ 会社メールを勝手に自分のスマホに転送、など

■IoTも同じことが起こると思った方が…

- 設備の更新時に新しい機能を追加（導入担当者の思い）
- つながる機能があたりまえに（作り手、売り手側の事情）

➔ つながらない機器は、入手できなくなる
例：カメラなしスマホは入手出来ないように

IoTセキュリティ問題の顕在化

日本の監視カメラ、6000台もの映像が見られてる

ロシアのウェブサイトに公開

このサイトでは、街中や店内、
自宅玄関など、世界120か国の
監視カメラが撮影している映像
をリアルタイムで見れてしまう。

日本国内の監視カメラもおよそ6000か所。デパートやコーヒーショップ歯医者やホテルなど、顔がくっきり映っているものまである。

これらの監視カメラは、**「購入時に初期パスワードを変更せず」**
使っているカメラの映像であった。

出典：iMedi（2016）

はじめに

JAPAN SMARTPHONE SECURITY ASSOCIATION

②他人事ではないIoTセキュリティ

■IoTを標的にしたサイバー攻撃が急増

➔ **攻撃するターゲットの50%がIoT関連**
セキュリティリスク ＝ 重要な経営課題に…

■製造業に学ぶ作業安全活動（作業安全＝経営課題）

- 知らない、出来ない、やらない（日々啓発、訓練、改善）

➔ **短期では浸透しないのが安全活動**

- IoT時代は、サイバー攻撃が作業者の安全にも関ってくる
- IoTセキュリティの放置 ＝「野良IoT」化を招く

先ずは「早めに考える風土」＝ 「知る・気づく」

製造業に学ぶ安全作業啓発の重要性

JAPAN SMARTPHONE SECURITY ASSOCIATION

安全に作業が出来ない「要因」は…

■ **知らない**

・なにが危険か、どうすれば安全か知らない ➔ 啓発

➔ 知る（気づく）ことで多くの危険作業が減る

■ **出来ない**

・どうすれば安全か知っているが、
安全な作業手順が出来ない ➔ 訓練

■ **やらない**

・安全な作業手順が出来るが、
やらなかった ➔ 改善

1．IoTセキュリティチェックシート概要

JAPAN SMARTPHONE SECURITY ASSOCIATION

1．IoTセキュリティチェックシート概要
- ①セキュリティチェックシート検討の経緯
- ②なぜNIST-CSFを採用したか
- ③チェックシートの構成と特徴

2. IoT導入のためのチェックシート活用方法
- ①企業のIoT活用とセキュリティ対策の大切な点
- ②チェックシート活用のポイント

3. IoTセキュリティ対策向上のための活動
- ①啓発活動への取組
- ②人材育成のために

チェックシート検討の経緯

JAPAN SMARTPHONE SECURITY ASSOCIATION

■2017年度

「IoTセキュリティチェックシート第１版」発行(2018/3)
- IoT推進コンソーシアムのガイドラインを利用者の視点で見直し
- チェックシートの有用性を確認（有用であるとの手応え）

■2018年度

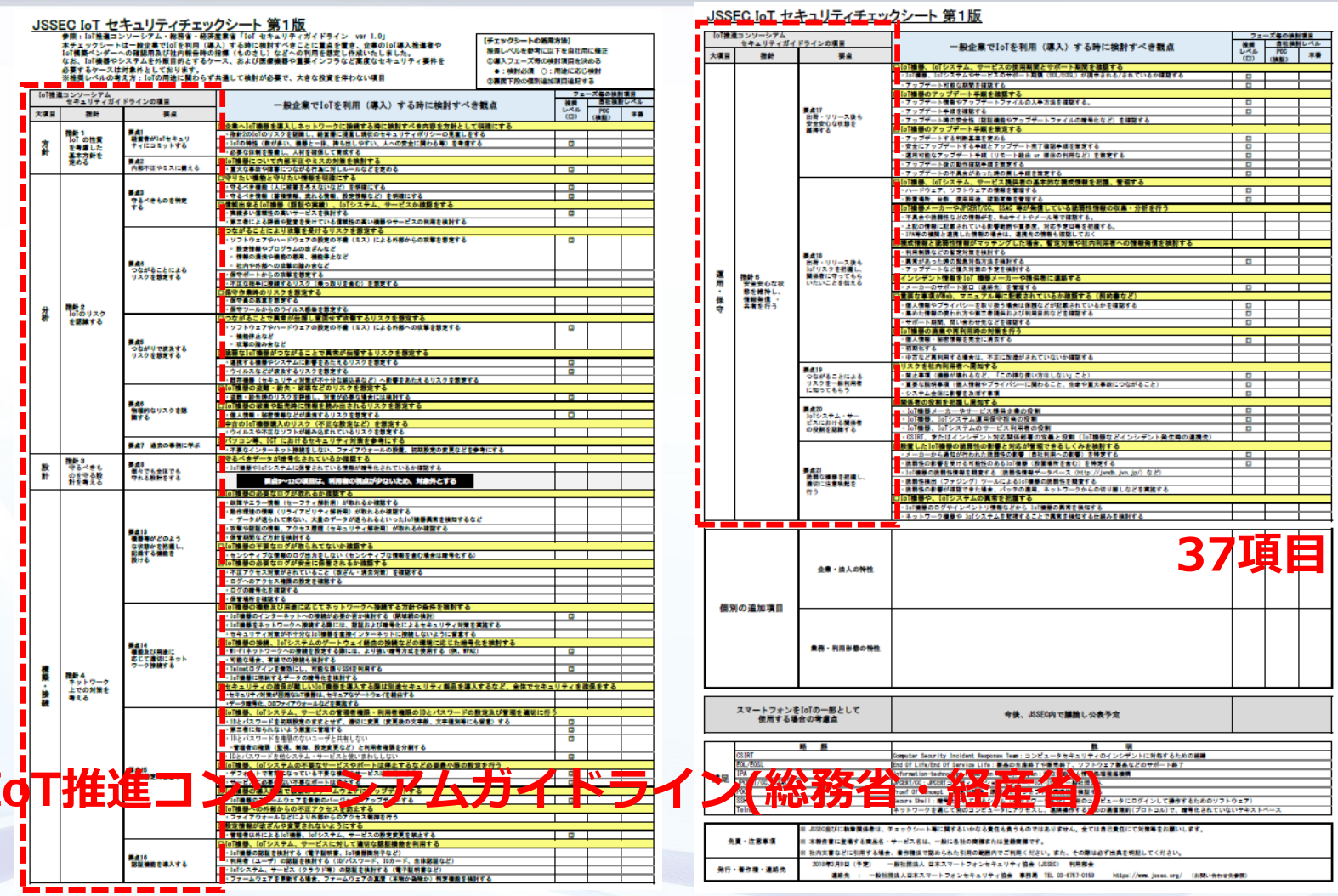
「IoTセキュリティチェックシート第２版」発行(2019/2)
- 国際性と網羅性の向上：NIST-CSF採用（米サイバーセキュリティフレームワーク）
- 一般利用者活用のための解説書を発行

■2019年度

「安心・安全なスマート社会のために」
- **IoTセキュリティの重要性などの啓発活動**（チェックシート活用）
  - ➔ **ものづくり現場など、企業の新たなセキュリティ課題を・・**

チェックシート第１版のイメージ

JAPAN SMARTPHONE SECURITY ASSOCIATION



チェックシート第１版の評価

JAPAN SMARTPHONE SECURITY ASSOCIATION

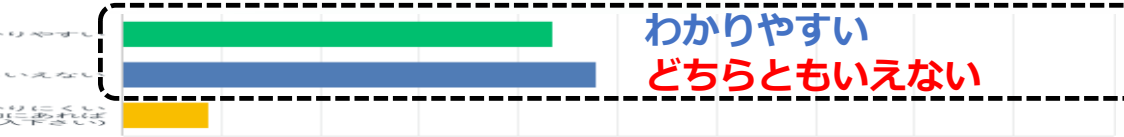
■第１版有用性の確認　IoT推進コンソーシアム会員アンケート（26社）

Q1: チェック項目の分量はいかがですか？

少ない ←網羅性の向上が必要

丁度良い

Q2: チェック項目の内容について分かりやすいですか？

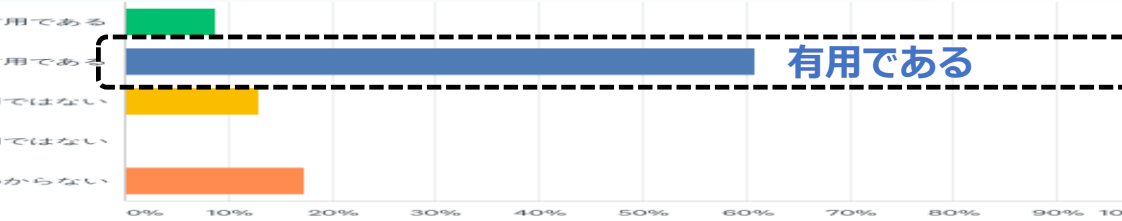


わかりやすい

どちらともいえない

←解説編が必要

Q3: 本チェックシートは有用だと思いますか？



有用である

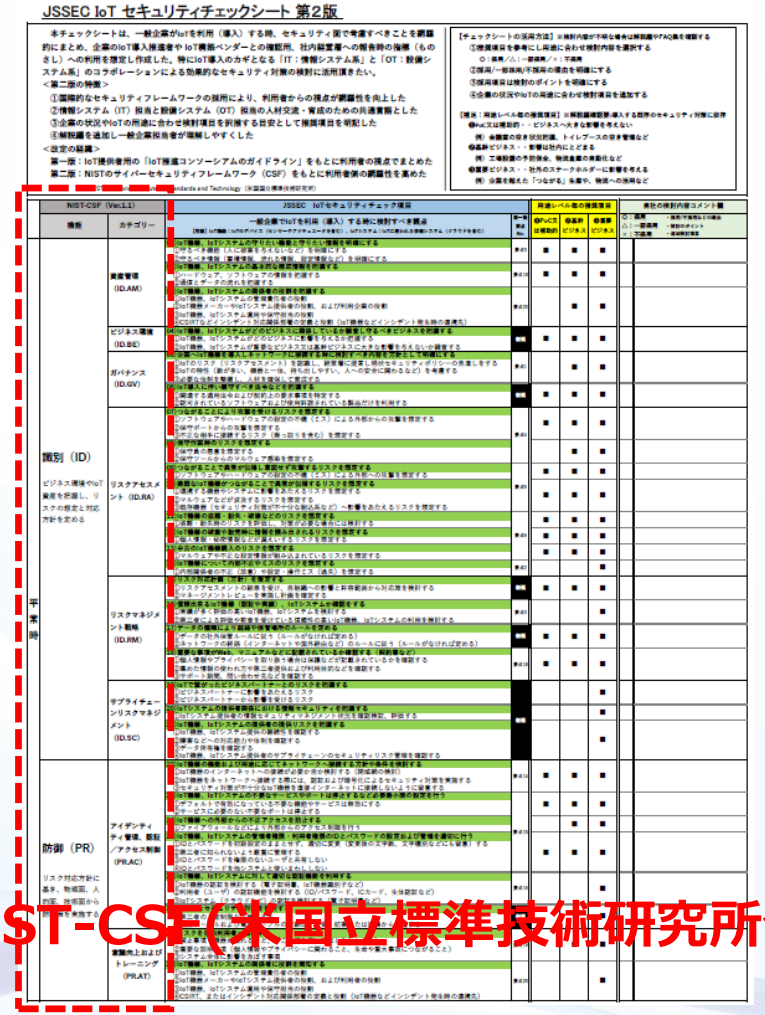
Q4: 自社での利用、お客様へのご紹介等活用してみたいですか？

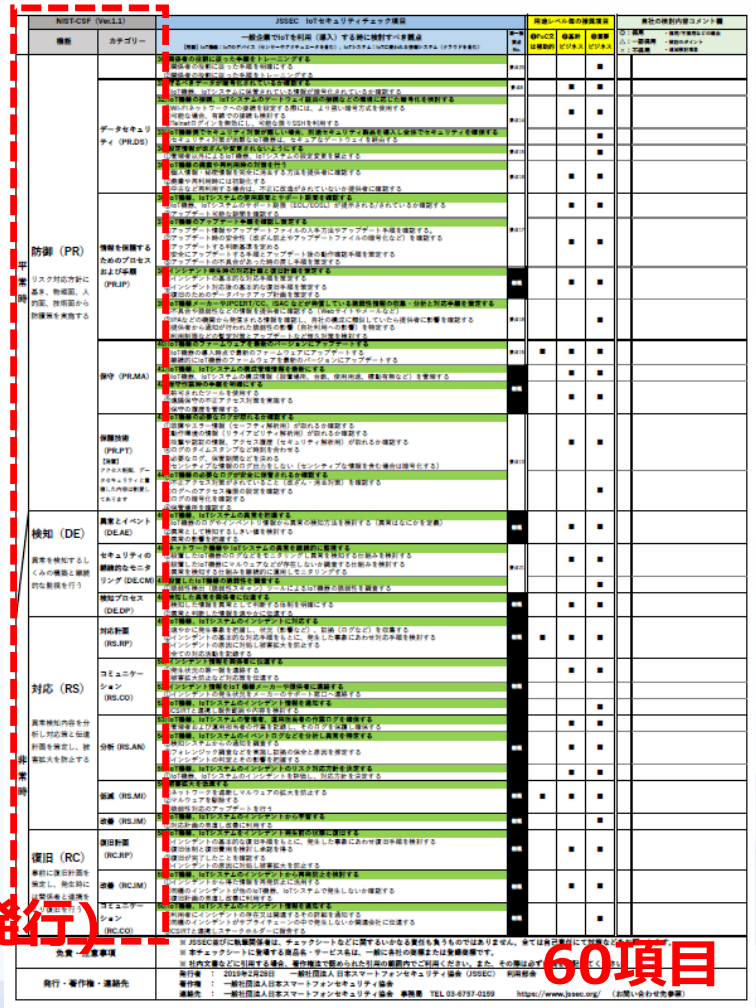
自社で使ってみたい

紹介したい

チェックシート第２版（網羅性）

JAPAN SMARTPHONE SECURITY ASSOCIATION





チェックシート第２版（解説編）

JAPAN SMARTPHONE SECURITY ASSOCIATION

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～

【第二版】

2019 年 4 月 1 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-k)

目 次

Page-4

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

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（管理情報、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

① IoT 機器、IoT システムの管理責任者の役割
② 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
③ IoT 機器、IoT システム運用や保守担当の役割
④ CSIRT 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 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。

Page-5

なぜNIST-CSFを採用したか

JAPAN SMARTPHONE SECURITY ASSOCIATION

■NIST-CSFとは・・

米国国立標準技術研究所（NIST）発行の「重要インフラのサイバーセキュリティを改善するためのフレームワーク」

参考）CybersecurityFrameworkVersion 1.1　日本語版IPAよりダウンロード可能

出典：米国国立標準技術研究所（NIST）

①組織的連携のための共通言語
- **インフラ設備担当**
- **サイバーセキュリティ担当**

②防御一辺倒ではない
- **セキュリティは破られる**
- **検知、対応、復旧など網羅的**

③平常時と異常時など運用面の視点
- **利用企業に分かりやすい**

チェックシートの構成と特徴①

JAPAN SMARTPHONE SECURITY ASSOCIATION

①NIST-CSFの分類：　5機能（識別、防御、検知、対応、復旧）
23カテゴリー(サブカテゴリーは参照に留めた)
②企業のIoT推進者や管理者の視点で検討すべき点：　60項目
③IoT用途レベル毎の推奨項目：　3つの重要度に分類
④各社の検討内容　採用理由／追加項目：　検討結果の見える化

チェックシートの構成と特徴（補足）

JAPAN SMARTPHONE SECURITY ASSOCIATION

③ 用途レベル毎の推奨項目

❶PoC又は補助的・・ビジネスへ大きな影響を与えない
例）会議室の空き状況把握、トイレブースの空き管理など
❷基幹ビジネス・・影響は社内にとどまる
例）工場設備の予防保全、物流倉庫の自動化など
❸重要ビジネス・・社外のステークホルダーに影響を与える
例）企業を超えた「つながる」生産や、物流への活用など

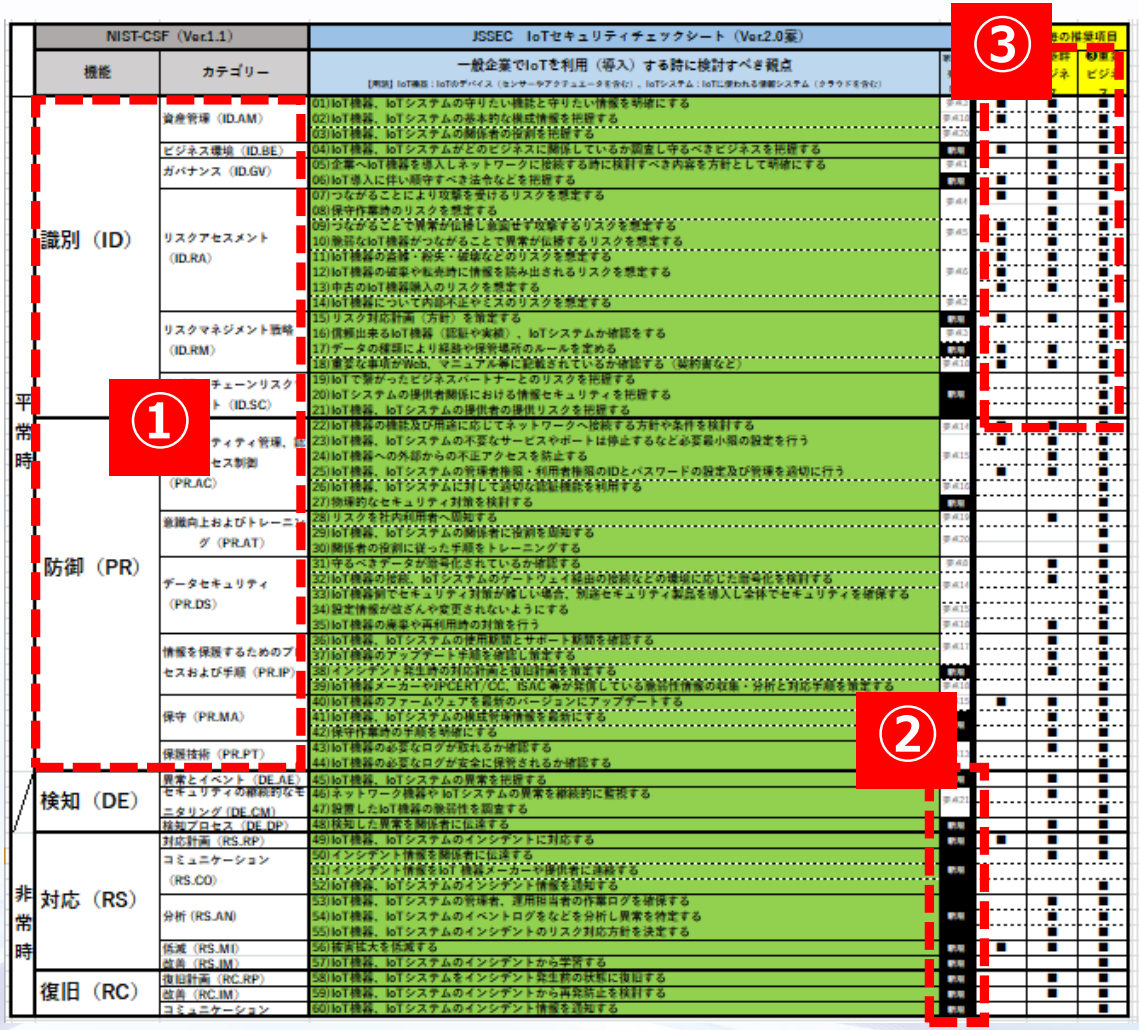
④ 自社の検討内容コメント欄 （活用はEXCELでセル拡大）

➔ IoTは長期間の利用を想定し、検討結果を継承することが重要

①「◎」採用/「△」一部採用/「×」不採用の理由を明確にする
②採用項目は検討のポイントを明確にする
③企業の状況やIoTの用途に合わせ検討項目を追加する

チェックシートの構成と特徴②

JAPAN SMARTPHONE SECURITY ASSOCIATION



①平常時からの備え
・識別と防御で2/3

②運用面の網羅性向上
・NIST-CSFの効果

③識別は出発点
・用途レベルに関らず

チェックシートの構成と特徴③

JAPAN SMARTPHONE SECURITY ASSOCIATION

■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
- **識別は用途レベルに関らず**、実施することを推奨（防御のベース）
- **踏み台にならないため**の、リスク想定が重要
- **サプライチェーンリスク**（ビジネスパートナー、システムや機器提供者）

NIST-CSF（Ver.1.1）		JSSEC　IoTセキュリティチェックシート（Ver.2.0案）	
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.
識別（ID）	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	要点3
		02)IoT機器、IoTシステムの基本的な構成情報を把握する	要点18
		03)IoT機器、IoTシステムの関係者の役割を把握する	要点20
	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	新規
	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	要点1
		06)IoT導入に伴い順守すべき法令などを把握する	新規
	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 08)保守作業時のリスクを想定する	要点4
		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 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	要点5
		11)IoT機器の盗難・紛失・破壊などのリスクを想定する 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 13)中古のIoT機器購入のリスクを想定する	要点6
		14)IoT機器について内部不正やミスのリスクを想定する	要点2
	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	新規
		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	要点3
		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	新規
		18)重要な事項がWeb、マニュアル等に記載されているか確認する（契約書など）	要点18
	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 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 21)IoT機器、IoTシステムの提供者の提供リスクを把握する	新規

チェックシートの構成と特徴④

JAPAN SMARTPHONE SECURITY ASSOCIATION

■リスク対応方針に基き、**物理面、人的面、技術面から防護策**実施
- **防御は用途レベルにあわせIT/OT部門が連携し**対策を検討することが重要
- **IoTは使用期間が長い（情報機器に比べ）**、サポート期間の確認も重要
- **IoTは情報の他、本来の機能や物理面の防御**も重要となる

NIST-CSF（Ver.1.1）		JSSEC　IoTセキュリティチェックシート（Ver.2.0案）	
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.
防御（PR）	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	要点
		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 24)IoT機器への外部からの不正アクセスを防止する 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	要点15
		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
		27)物理的なセキュリティ対策を検討する	新規
	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	要点19
		29)IoT機器、IoTシステムの関係者に役割を周知する 30)関係者の役割に従った手順をトレーニングする	要点20
	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	要点8
		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 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	要点14
		34)設定情報が改ざんや変更されないようにする	要点15
		35)IoT機器の廃棄や再利用時の対策を行う	要点18
	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	要点17
		37)IoT機器のアップデート手順を確認し策定する	
		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
		39)IoT機器メーカーやJPCERT/CC、ISAC 等が発信している脆弱性情報の収集・分析と対応手順を策定する	要点18
	保守（PR.MA）	40)IoT機器のファームウェアを最新のバージョンにアップデートする	要点15
		41)IoT機器、IoTシステムの構成管理情報を最新にする 42)保守作業時の手順を明確にする	新規
	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	要点13
		44)IoT機器の必要なログが安全に保管されるか確認する	

チェックシートの構成と特徴⑤

JAPAN SMARTPHONE SECURITY ASSOCIATION

■**完璧な防御はない**と考え、**異常は発生する事を前提**に備える
- 検知（DE）：**異常を検知**し継続的な監視を行う**＜異常の分類＞**
- 対応（RS）：異常検知内容を分析し対応策と伝達計画を策定し、**被害拡大を防止**する**＜人的被害防止＝作業安全＞**
- 復旧（RC）：事前に復旧計画を策定し、発生時には**関係者と連携をとり復旧**を行い、**再発防止**を実施する

NIST-CSF（Ver.1.1）		JSSEC　IoTセキュリティチェックシート（Ver.2.0案）	
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.
検知（DE）	異常とイベント	45)IoT機器、IoTシステムの異常を把握する	新規
	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 47)設置したIoT機器の脆弱性を調査する	要点21
	検知プロセス（DE.DP）	48)検知した異常を関係者に伝達する	新規
対応（RS）	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	新規
	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 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 52)IoT機器、IoTシステムのインシデント情報を通知する	新規
	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 54)IoT機器、IoTシステムのイベントログをなどを分析し異常を特定する 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	新規
	低減（RS.MI）	56)被害拡大を低減する	新規
	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	新規
復旧（RC）	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	新規
	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	新規
	コミュニケーション	60)IoT機器、IoTシステムのインシデント情報を通知する	新規

2. IoT導入のためのチェックシート活用方法

JAPAN SMARTPHONE SECURITY ASSOCIATION

1. IoTセキュリティチェックシート概要
   - ①セキュリティチェックシート検討の経緯
   - ②なぜNIST-CSFを採用したか
   - ③チェックシートの構成と特徴

2. IoT導入のためのチェックシート活用方法
   - **①企業のIoT活用とセキュリティ対策の大切な点**
   - **②チェックシート活用のポイント**

3. IoTセキュリティ対策向上のための取り組み
   - ①啓発活動への取組
   - ②人材育成のために

日本のものづくりと政策の動向

JAPAN SMARTPHONE SECURITY ASSOCIATION

国策：「超スマート社会」と「第四次産業革命」をめざす

「Society 5.0」＝　超スマート社会（新たな付加価値の創出）

「Connected　Industries」

＝　日本版・第四次産業革命

①サイバー空間とフィジカル空間が高度に融合した産業社会

②コアテクノロジーはIoTを起点にビックデータやAIとの連携

➔経産省：サイバー・フィジカル・セキュリティ対策フレームワーク

「企業のスマート化」←スマートフォンの知見

①スマート〇〇（工場、物流、ショップ、オフィス）

②コアテクノロジーはIoT

➔　IoTを安全・安心に活用するために・・

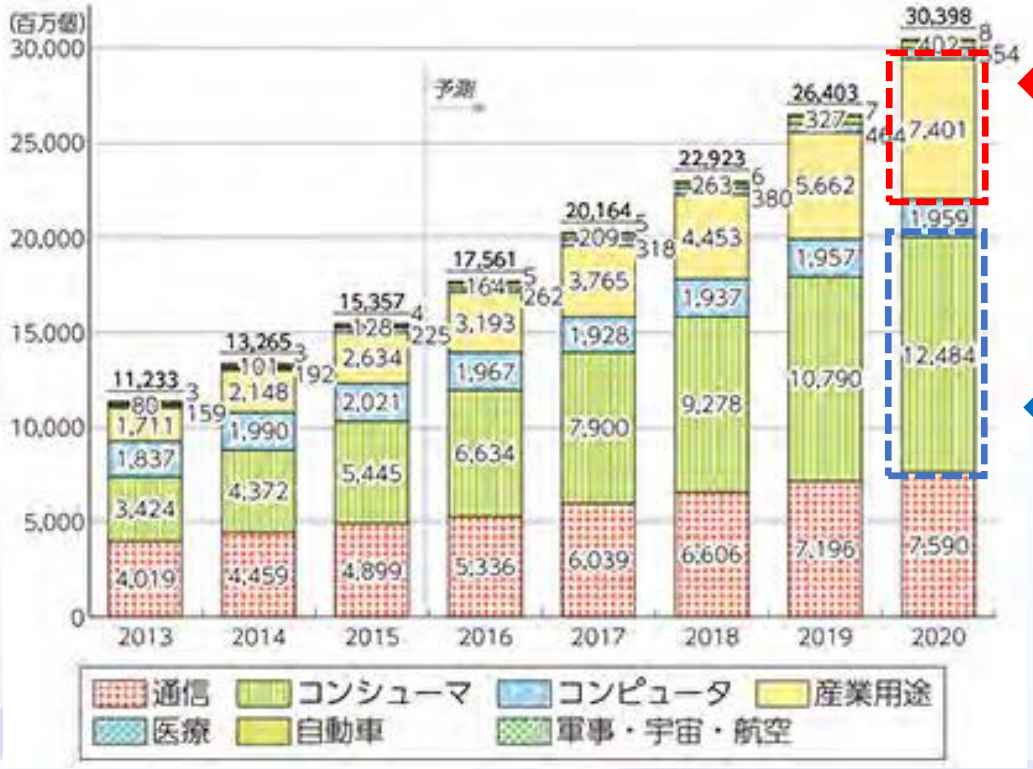
「IoTセキュリティチェックシート」

コアテクノロジーは（IoT）

JAPAN SMARTPHONE SECURITY ASSOCIATION

■世界のIoTデバイス数の推移及び予測

➔ 2020年には300億個を超えるとも



（出典：平成28年版情報通信白書）

➔ 産業用途

※IoT機器の普及は

スマホ同様、コンシューマ市場がけん引し産業用途に影響していくのでは？

➔ コンシューマ

コアテクノロジーは（５G）

JAPAN SMARTPHONE SECURITY ASSOCIATION

■第５世代移動通信（5G）は社会を変える

➔ 2020年サービス開始、低遅延と多数同時接続に注目

（出典：総務省「将来のネットワークインフラに関する研究会」報告書概要）

IoTセキュリティの大切な点①

JAPAN SMARTPHONE SECURITY ASSOCIATION

■IoTセキュリティと情報セキュリティの違い
・サイバー空間とフィジカル空間の融合に注意

①ネットを通じモノが制御される
・機密を守るから動作（制御）を守る
◎求められる事　➔　Security by Design

②モノがつぶやく
・自分の情報（位置、活動、画像など）が集められる
◎求められる事　➔　Privacy by Design

③長く使われる/モノが進化する
・スマホは3～5年、車や設備系は10年以上
◎求められる事　➔　長期的なアップデート

④多種多様な使われ方
・使う人、管理する人がセキュリティをあまり意識しない
◎求められる事　➔　ユーザーへの啓発やサポート

IoTセキュリティの大切な点②

JAPAN SMARTPHONE SECURITY ASSOCIATION

- **機密性**（Confidentiality）
- **完全性**（Integrity）
- **可用性**（Availability）
- **信頼性**（Reliability）
- **責任追跡性**（説明可能性）（Accountability）
- **真正性**（認証性）（Authenticity）

今までの情報セキュリティで重視されていた３要素

IoT時代のセキュリティでは、
➔ 更に３要素が重視される

IoTセキュリティの大切な点③

JAPAN SMARTPHONE SECURITY ASSOCIATION

■セキュリティとセーフティの両面

セキュリティ *(security)*
意志のある危険から身体や財産等を守る

セーフティ *(safety)*
意志のない危険から身体や財産等を守る

IoTセキュリティの大切な点④

JAPAN SMARTPHONE SECURITY ASSOCIATION

■サプライチェーンリスクが問われる

・高度に協業が進む時代「安心・安全」が求められる

①共同研究や開発を委託する時

・守秘義務契約（ND）や知的財産権などの締結

・重要な機密情報の取り扱い＝人の管理が重要

②設備やソフト調達する時

・設備やソフトの調達可能な期間や品質

・不正なソフトが組み込まれていない＝人の管理が重要

③保守や運用を委託する時

・事業の継続性や信頼性の確認

・保守や運用には大きな権限付与が必要＝人の管理が重要

④ビジネスパートナーと取引する時

・取引の継続や品質管理

・サイバー攻撃の波及＝セキュリティ対策（踏み台にならない）

チェックシート活用のポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ **どこからはじめるか,最低限やる事**

➔A3チェックシート参照

JSSECの「IoTセキュリティチェックシート」の
「用途レベル毎の推奨項目」の「**❶PoC又は補助的**」
を参考に「どこからはじるか、最低限やることは」
など活用のポイントを解説する

どこからはじめるか,最低限やる事

JAPAN SMARTPHONE SECURITY ASSOCIATION

■識別（ID）のポイント

ポイント①

01) なにを守るべきかを決める ➔ **①守るべき機能（=OT:事例参）**
02) 守るものを決めるためのシステム面の情報と
04) ビジネス面への影響を整理する
06) 法令への適用などを整理する

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 02)IoT機器、IoTシステムの基本的な構成情報を把握する 03)IoT機器、IoTシステムの関係者の役割を把握する
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
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 06)IoT導入に伴い順守すべき法令などを把握する
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 08)保守作業時のリスクを想定する 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 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 11)IoT機器の盗難・紛失・破壊などのリスクを想定する 12)IoT機器の廃棄や転売時に情報を読み出され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 14)IoT機器について内部不正やミスのリスクを想定する

ポイント②

07) 繋がることのリスクはなにかを想定する ➔ **①設定（=IT）**
09) 意図せず攻撃してしまう
10) 脆弱な機器がつながり、異常が他に伝搬してしまう
11) 機器の盗難や破壊されてしまう
12) 機器の廃棄や売却時に情報が漏えいしてしまう
13) 中古機器に不正なソフトが組み込まれてしまう

守る機能を考えることが重要（旅行中発見）

JAPAN SMARTPHONE SECURITY ASSOCIATION

■情報セキュリティにはなかったことへの気づき

①ホテルの部屋のTVから…

➔ コインランドリーの空きがわかる

①

②守るものはなにか…考えられてる

➔ ドアがセキュリティロック

②

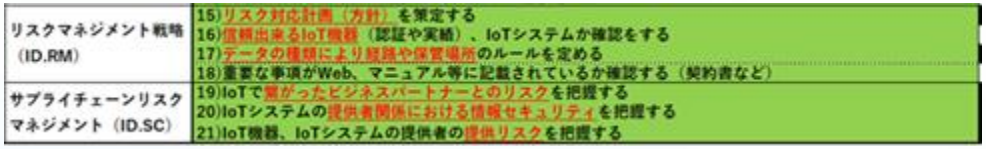
どこからはじめるか,最低限やる事

JAPAN SMARTPHONE SECURITY ASSOCIATION

■識別（ID）のポイント

ポイント③

15) 想定されるリスクへの対応方針を決める ➔ **①身の丈に合わせ**
16) 信頼できる機器やシステムの利用方針 ➔ **重要用途**
17) データの経路や保管場所の基準
18) サポート期間など重要事項の確認や契約



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 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 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 18)重要な事項がWeb、マニュアル等に記載されているか確認する（契約書など）
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 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 21)IoT機器、IoTシステムの提供者の提供リスクを把握する

ポイント④

19) サプライチェーンのリスクへの対応を決める ➔ **重要用途**
20) 機器やシステム提供者のセキュリティレベル確認
21) 機器やシステム提供者の能力や体制の確認

どこからはじめるか,最低限やる事

JAPAN SMARTPHONE SECURITY ASSOCIATION

■防御（PR）のポイント

ポイント⑤

22) 用途に応じてネットワーク接続条件を検討する

➔ **①なんでもインターネットへ接続しない**

23) ネットワークへの接続設定は必要最小限にする

➔ **①IoT機器はポート設定に注意（デバッグ用など空いてる）**

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 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 24)IoT機器への外部からの不正アクセスを防止する 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 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 27)物理的なセキュリティ対策を検討する
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 29)IoT機器、IoTシステムの関係者に役割を周知する 30)関係者の役割に従った手順をトレーニングする
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 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 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 34)設定情報が改ざんや変更されないようにする 35)IoT機器の廃棄や再利用時の対策を行う
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 37)IoT機器のアップデート手順を確認し策定する 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 39)IoT機器メーカーやJPCERT/CC、ISAC等が発信している脆弱性情報の収集・分析と対応手順を策定する
保守（PR.MA）	40)IoT機器のファーム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システムの構成管理情報を最新にする 42)保守作業時の手順を明確にする
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 44)IoT機器の必要なログが安全に保管されるか確認する

ポイント⑥

25) IDとパスワードの管理を適切に

➔ **①初期設定のままとしない**

40) ファームウエアーを最新にアップデート

➔ **①古いバージョンは狙われる**

どこからはじめるか,最低限やる事

JAPAN SMARTPHONE SECURITY ASSOCIATION

■対応（RS）のポイント

ポイント⑦

49) インシデント（異常）へ対応できるようにする

➔ **①被害拡大防止のため状況確認手順を考えておく**

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
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 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 52)IoT機器、IoTシステムのインシデント情報を通知する
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 54)IoT機器、IoTシステムのイベントログをなどを分析し異常を特定する 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
低減（RS.MI）	56)被害拡大を低減する
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

ポイント⑧

56)インシデント（異常）発生時は被害拡大を防止する

➔ **①ネットワークから切り離すなど被害拡大防止策を考えておく**

3. IoTセキュリティ対策向上のための活動

JAPAN SMARTPHONE SECURITY ASSOCIATION

1. IoTセキュリティチェックシート概要
   - ①セキュリティチェックシート検討の経緯
   - ②なぜNIST-CSFを採用したか
   - ③チェックシートの構成と特徴

2. IoT導入のためのチェックシート活用方法
   - ①企業のIoT活用とセキュリティ対策の大切な点
   - ②チェックシート活用のポイント

3. IoTセキュリティ対策向上のための活動
   - **①啓発活動への取組**
   - **②人材育成のために**

日本のものづくりと政策の動向

JAPAN SMARTPHONE SECURITY ASSOCIATION

■我が国製造業を巡る現状と課題

「ものづくり基盤技術振興基本法」に基づき経産、厚労、文科共同執筆（2019年6月発行）

➔ 第四次産業革命として「見える化」レベルは一部で取り組みがはじまった

第四次産業革命の進展

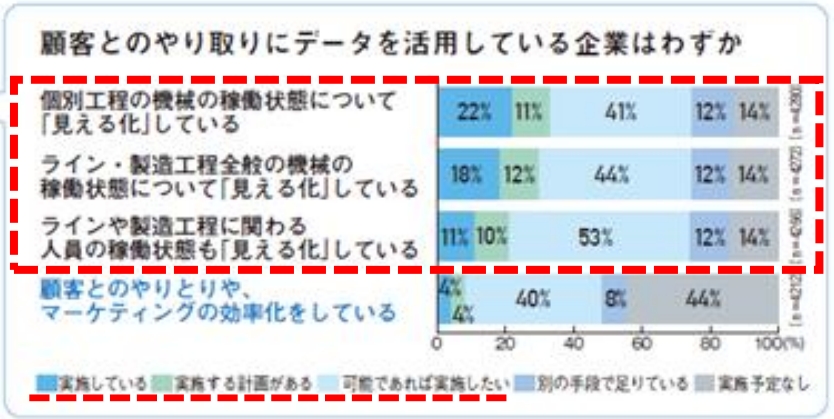
- 製造ラインでのデータ活用の動きは拡大。
- 今後は、顧客とのやり取りなど
  バリューチェーン全体を見据えた取組が求められ、
  製造業のデジタル化は第二段階へ。

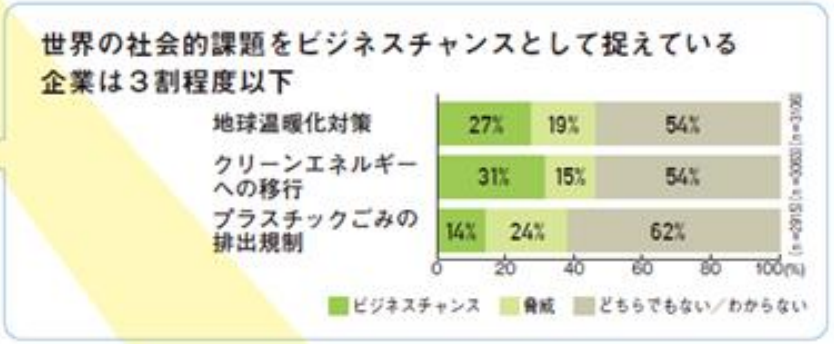
グローバル化の展開と保護主義の高まり

- グローバル化の動きは年々進展。
- 一方、保護主義の動きが高まり、グローバルなサプライチェーンの在り方について戦略的な対応が課題に。

ソーシャルビジネスの加速

- 世界では社会的課題の解決に向けた投資気運の高まりが見られる。日本の製造業が自社の強みを活かせる分野も存在。
- しかしながら、こうした動きをビジネスチャンスだと考えている企業はわずか。





（出典：経済産業省 2019年版ものづくり白書のポイント）

日本のものづくりと政策の動向

JAPAN SMARTPHONE SECURITY ASSOCIATION

■競争力強化に向けた４つの方策

➔ **①IoTなどの「新たなものづくり人材」の育成と活躍の場**
②ものづくり現場のデジタル化を急げ（熟練技能者が残っているうちに）

1 世界シェアや現場データを活かした新しいビジネスモデルの展開

- 現場の良質なデータを蓄積し、共有知化
- 自社製品の世界シェアを活かしたサービスの提供
- 世界の社会的課題をはじめとする新たな顧客ニーズに対応

例 製品に組み込まれている部品の世界シェアを背景に、そこからデータを収集・分析。新たなサービスソリューションの提供を目指す

2 重要部素材の強みを活かした世界市場の開拓・拡大

- 日本製造業の部素材での強みや、高い技術力・品質力を背景に、自社製品を事実上の「標準規格」化
- 海外企業を含む完成品メーカーへも積極的に提案

例 第四次産業革命を牽引する完成品の重要部素材において、自社の技術力を活かして世界の市場を開拓・拡大

① スキル人材が活躍できる場・組織の構築

- ものづくりとAI・IoTを組み合わせることのできるスキル人材が活躍できる環境の有無がデジタル化の成否を分ける
- 若手の積極登用や評価システムの見直し、横断的部門の新設などの場作り・組織改革を実施

例 企業内にデジタル専門部隊を組織し、予兆検知モデルの作成や技能継承のデジタル化などの取組を加速

② 技能のデジタル化・徹底的な省力化の実施

- 熟練技能者が現場に残っているうちに、将来を見据えた対策を行うことが急務
- 深刻な人手不足を追い風に変え、AI、IoT、ロボットの活用による現場の徹底的な省力化を推進

例 大学と連携しながら職人の暗黙知を力学センサにより計測・デジタル化し、技能習得を効率化

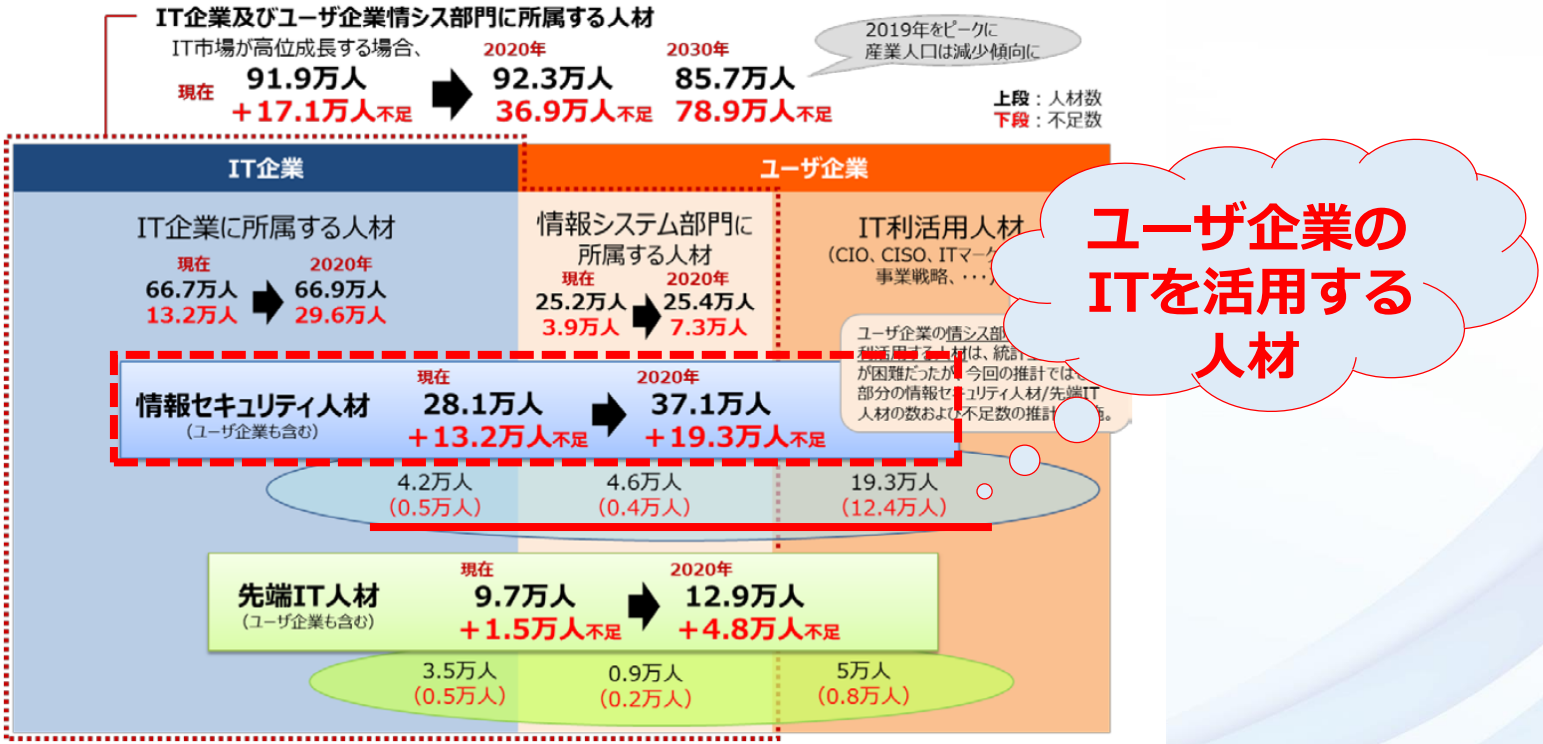
（出典：経済産業省 2019年版ものづくり白書のポイント）

IoTセキュリティ人材

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ IoTを安全・安心に活用するためには

➔ **OTが分かるセキュリティ人材**と
セキュリティが分かるOT人材の育成が課題



出典：経済産業省　参考図1. IT 人材の需給に関する推計結果の概要

人材育成へのチェックシート活用

JAPAN SMARTPHONE SECURITY ASSOCIATION

啓発（気づき）

IoTに関る人を対象にセキュリティの重要性を…

- IT系　：情報セキュリティとIoTセキュリティの違い
- OT系：IoTセキュリティの重要性
- どこからはじるか,最低限やることは

将来

人材育成（訓練）

人材育成へのチェックシート活用（ワークショップ）

- IoTセキュリティ実践のための講義・講演
- IoTのモデルを題材にチェックシートで討議
- ５人の小グループ×数組　➔　発表

人材育成へのチェックシート活用

JAPAN SMARTPHONE SECURITY ASSOCIATION

■チェックシート(PDF、Excel）、解説を無償公開

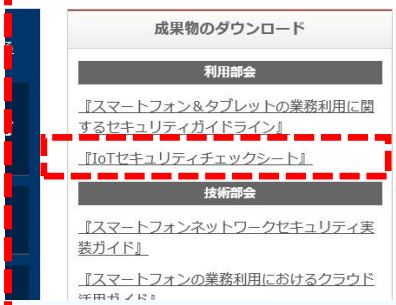
JSSEC IoTセキュリティチェックシート第二版 ダウンロードページ

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



https://www.jssec.org/

https://www.jssec.org/iot

参考）IoTの啓発計画の検討状況

JAPAN SMARTPHONE SECURITY ASSOCIATION

■連携先との調整(2019年5月～9月)

①地方版IoT推進ラボのと連携調整（全体事務局IPA、主体は各自治体）
- 愛知県、三重県、横浜市訪問し現地側の要望などヒアリング実施

②岐阜県IoTコンソーシアム（ソフトピアジャパン事務局）との連携調整
- 中小企業など約１３０社の会員が参加し活動がはじまっている
- 会員企業からセキュリティについて相談も増えて来た
- 今年度はものづくり企業を中心に啓発セミナー実施（ 2019年8月）

③日本エンジニアリング協会
- ものづくり関係のエンジニアにITやセキュリティのスキルも重要に

④IoTセキュリティ人材育成に向けた啓発セミナー
- 電気通信普及財団様の助成事業（2019/10～2020/9）

参考）関連先ヒアリング結果

JAPAN SMARTPHONE SECURITY ASSOCIATION

- IoTに関る人は、IT系とOT系などものづくりなど現場に近いひとたちの両面が重要、特にセキュリティから遠いOT系やものづくり現場への啓発が課題

- ものづくりに携わる人たちにも、ITやセキュリティの知見が今後重要になるが、ここが弱い

- ものづくりなどの現場に近い人たちへは、まずセキュリティとはなにか、どんなことが重要かなど入り口の勉強会をより広く開催する事が重要、ワークショップなど人材育成には啓発など土台づくりが必要

関連先との連携した活動予定

JAPAN SMARTPHONE SECURITY ASSOCIATION

■本年度は普及・啓発を中心に連携（詳細は今後調整）

①IT系のセキュリティセミナー

1) ジャパンセキュリティ・サミット（2019/11）
2）JSSECセキュリティフォーラム（2020/2～）
3）地方開催の総通局・セキュリティ勉強会

②OT系の啓発セミナー

1) 愛知県IoT推進ラボへ講師派遣（2019/12 名古屋）
2) 日本エンジニアリング協会へ講師派遣（2019/12 東京）
3) 今後全体の事務局IPAと協議し、活発な地方5ヶ所ほど選定

■人材育成セミナーの検討(来年度の予定)

①人材育成ワークショッププログラムの検討予定

1) 愛知県IoT導入人材育成支援講座（先進事例調査）

おわりに

JAPAN SMARTPHONE SECURITY ASSOCIATION

■**提供者に求められる事　➔　Security by Design**
（設計段階からセキュリティを検討する）

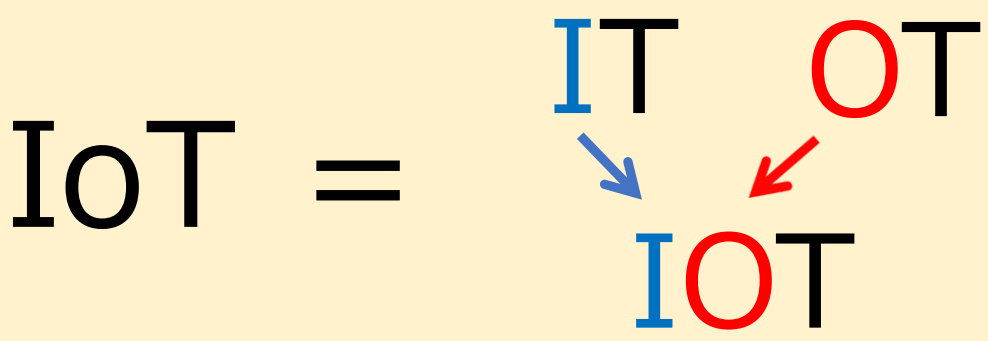
■**企業へ導入するときに求められる事は？？？**

①**「Security by POC」**

➔ **検証段階からセキュリティを検討することで気づきを…**

②**「Security by IOT」**

➔ **「IT」と「OT」のコラボレーションで効果的対策を…**



ご清聴ありがとうございました

JAPAN SMARTPHONE SECURITY ASSOCIATION

※本日の講演資料を以下でも公開予定です