JAPAN SMARTPHONE SECURITY ASSOCIATION

2017年度　利用部会成果発表

「企業へIoTを導入する場合のセキュリティ検討事項」

～JSSEC IoTセキュリティチェックシート～

2018年3月9日

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（株式会社ラック）

本日の内容

企業へIoTを導入する場合のセキュリティ検討事項（チェックシート）

＜講演概要＞
スマートファクトリーをはじめ、企業へのIoT導入事例も出はじめ、今後本格的に企業への導入が進むと思われる。一方、セキュリティ面の課題が今までの情報セキュリティとは異なるのか、何を検討すべきか明確になっていない。JSSEC利用部会で、**企業がIoT導入するためにセキュリティ面で何を検討すべきか**、IoT推進コンソーシアムの「IoTセキュリティガイドライン」を深読みし、企業利用者の視点から検討した**「IoTセキュリティチェックシート」**を紹介する。

■**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？？？**

JSSEC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

会員：104社　＋　28法人（特別会員、オブザーバー ）
<2018年2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月に任意団体としてスタートし、2012年4月より一般社団法人として活動

利用部会	技術部会	啓発事業部会	ＰＲ部会
利用者の視点で活動	提供者の視点で活動	ｼﾞｭﾆｱ層への啓発活動	JSSECのPR活動

主な成果物

利用部会:スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン
技術部会：Androidアプリのセキュア設計・セキュアコーディングガイド
啓発事業部会：スマートフォンセキュリティ・ワークショップレポート 2015

◆ **http://www.jssec.org/ ⇒ 「部会･WGからの報告 / 成果物」 からダウンロード可能**

利用部会の運営体制

JAPAN SMARTPHONE SECURITY ASSOCIATION

■部会長　　後藤　悦夫（ラック）
■副部会長　　北村　裕司（サイバートラスト）
■ガイドラインWG
・リーダー　　松下　綾子（アルプスシステムインテグレーション）
■事例研究WG
・リーダー　　坂田　孝昭（日立システムズ）
・サブリーダー　藤平　武巳（NTTコミュニケーションズ）
■IoT調査・研究TF
・リーダー　　後藤兼務
・サブリーダー　三池　聖史（ユニアデックス）
・メンバー（上記副部会長、WGのリーダ、サブリーダに加え）
笠原　正弘（ソフトバンク）
瀬川　　紘（セコムトラストシステムズ）
中村　康洋（シャープ）
中村　丈洋（SHIFT SECURITY）

利用部会の中期活動方針

JAPAN SMARTPHONE SECURITY ASSOCIATION

■ ２点に重点を置き活動

①「一億総活躍時代のモバイルワークとセキュリティ」
- 在宅勤務も含めた新たな働き方
- モバイルデバイスの進化に合わせたセキュリティ

②「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
- スマートフォンの使われ方の変化に合わせたセキュリティ

IoT時代のスマートフォンの役割変化

「つながる世界」 と 「人をつなぐ」

➔JSSECでは、「スマートフォンを機軸とした IoTセキュリティ」へ活動を拡大

IoT調査・研究TFの本年度計画

JAPAN SMARTPHONE SECURITY ASSOCIATION

IoT調査研究TFの活動計画

■**発行されているガイドラインを分析する**
・IoTコンソーシアムガイドラインを読み込み
・利用企業として検討すべき項目を洗い出す

■**利用者に関係する部分を抽出、不足分を追加する**
・企業への導入＝利用と考える

■**JSSEC利用部会として発信するイメージ案を作成する**
・ IoT全体を網羅し、スマホとの関連を取り上げる
・**第１ステップ：チェックシートイメージ作成**
➔利用可否をトライし、解説編を検討する

2017年度の活動スケジュール

JAPAN SMARTPHONE SECURITY ASSOCIATION

5月	JSSEC幹事会	（各部会の活動計画案）
6月	JSSEC　総会	（各部会の活動計画）
7月	利用部会	（メンバー募集）
	第１回TF	
8月	第２回TF	
9月	第３回TF	
10月	第４回TF	
11月	利用部会・技術部会　合同成果報告会（中間報告）	
	※総務省へ相談（IoTコンソーシアム資料活用など）	
12月	第５回TF	
	※経済産業省へ相談（IoTコンソーシアム資料活用など）	
1月	第６回TF	
3月	JSSEC　セキュリティフォーラム2018（成果発表）	
	➔　講演資料とチェックシートを公開（ホームページ）	

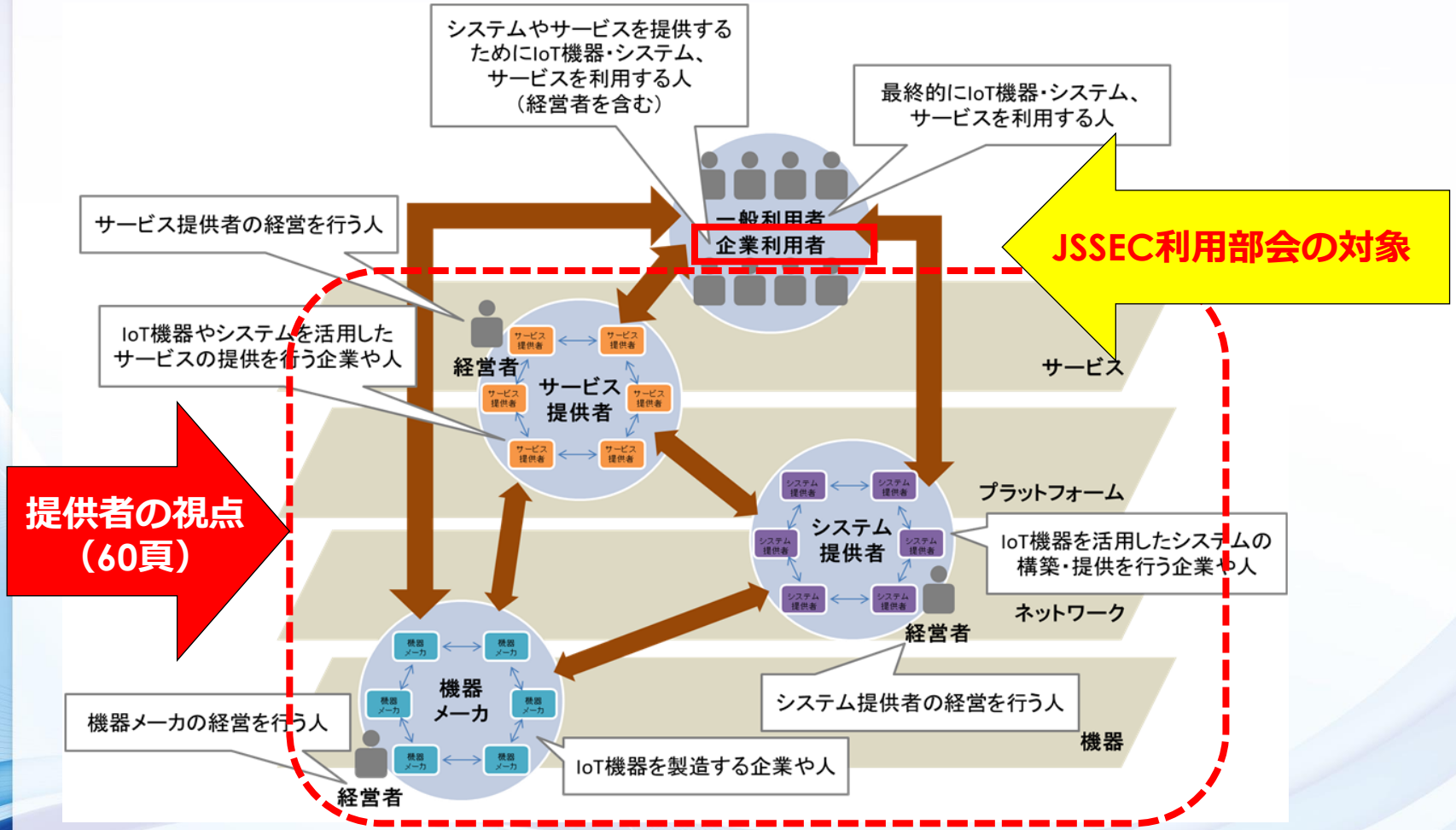
IoT推進コンソーシアムGL選定理由

JAPAN SMARTPHONE SECURITY ASSOCIATION

選定理由：IoTの利用対象分野が全般的で、網羅性が高い。

団体	ガイドライン名	発行日	評価		
			利用者視点	網羅性	位置付け
IoT推進コンソーシアム	セキュリティガイドラインver1.0	2016/7/5	△：一部あり	○：IoT サービス関係者全レイヤ向け	IPA「つながる世界の開発指針」を参考に対象者を広げ、一般化
IPA	つながる世界の開発指針	2016/3/24 第2版： 2017/6/30	×：開発者向け	○：IoTに関連する様々な製品分野・業界において分野横断的に活用	IoT製品の安全性・セキュリティに関するリスクとその対策に着眼
IPA	IoT開発におけるセキュリティ設計の手引き	2016/5/12	×：開発者向け	△：対象（デジタルテレビ、ヘルスケア機器、スマートハウス、コネクテッドカー）	IPA「つながる世界の開発指針」に対し、具体的なセキュリティ設計と実装を実現するための手引き
CCDS	製品分野別セキュリティガイドライン	2016/6/8 第2版： 2017/5/29	×：開発者向け	△：対象（車載、IoTゲートウェイ、金融端末、決裁端末）	IPA「つながる世界の開発指針」を各分野の視点で脅威やリスクをより具体化
JNSA	コンシューマ向けIoTセキュリティガイド	2016/6/24	×：開発者向け	△：対象（スマートテレビ、ウェアラブルデバイス、ネットワークカメラ、汎用マイコンボード）	コンシューマ向け IoT 製品の開発者が考慮すべき事柄
CSAジャパン	IoT早期導入者のためのセキュリティガイダンス	2016/2/24	○：導入者の視点	△：課題と管理策が細かい。理解するのが大変。	CSA本部が公開している資料（2015年４月）の翻訳

IoT推進コンソーシアムGLの対象読者



IoT 推進コンソーシアム「IoT セキュリティガイドラインver1.0」より

IoT推進コンソーシアムGLの概要

JAPAN SMARTPHONE SECURITY ASSOCIATION

方針	指針1 IoT の性質を考慮した基本方針を定める	要点1. 経営者がIoT セキュリティにコミットする 要点2. 内部不正やミスに備える
分析	指針2 IoT のリスクを認識する	要点3. 守るべきものを特定する 要点4. つながることによるリスクを想定する 要点5. つながりで波及するリスクを想定する 要点6. 物理的なリスクを認識する 要点7. 過去の事例に学ぶ
設計	指針3 守るべきものを守る設計を考える	要点8. 個々でも全体でも守れる設計をする 要点9. つながる相手に迷惑をかけない設計をする 要点10. 安全安心を実現する設計の整合性をとる 要点11. 不特定の相手とつなげられても安全安心を確保 要点12. 安全安心を実現する設計の検証・評価を行う
構築・接続	指針4 ネットワーク上での対策を考える	要点13. 機器等がどのような状態かを把握し、記録する機能を設ける 要点14. 機能及び用途に応じて適切にネットワーク接続する 要点15. 初期設定に留意する 要点16. 認証機能を導入する
運用・保守	指針5 安全安心な状態を維持し、情報発信・共有を行う	要点17. 出荷・リリース後も安全安心な状態を維持する 要点18. 出荷・リリース後もIoT リスクを把握し、関係者に守ってもらいたいことを伝える 要点19. つながることによるリスクを一般利用者に知ってもらう 要点20. IoT システム・サービスにおける関係者の役割を認識する 要点21. 脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール （第3章として2頁補足的に記載）		ルール1）問合せ窓口やサポートがない機器やサービスの購入・利用を控える ルール2）初期設定に気をつける ルール3）使用しなくなった機器については電源を切る ルール4）機器を手放す時はデータを消す

提供者の視点が中心のため割愛

IoT推進コンソーシアムGL（方針）

JAPAN SMARTPHONE SECURITY ASSOCIATION

要点		ガイドラインに記載されているポイント	
1	経営者がIoT セキュリティにコミットする	①	IoT セキュリティの基本方針を企業として策定し周知するとともに、継続的に実現状況を把握し、見直す。また、そのために必要な体制、人材を整備する。
2	内部不正やミスに備える	①	IoT の安全を脅かす内部不正の潜在可能性を認識し、対策を検討する。
		②	関係者のミスを防ぐとともに、ミスがあっても安全を守る対策を検討する。

説明は省略

IoT推進コンソーシアムGL（分析）

JAPAN SMARTPHONE SECURITY ASSOCIATION

要点		ガイドラインに記載されているポイント	
3	守るべきものを特定する	①	IoT の安全安心の観点で、守るべき本来機能や情報などを特定する。
		②	つなげる機能について、本来機能や情報の安全安心のために、守るべきものとして特定する。
4	つながることによるリスクを想定する	①	クローズドなネットワーク向け機器やシステムでも、IoT機器・システムとして使われる前提でリスクを想定する。
		②	保守時のリスク、保守用ツールの悪用によるリスクも想定する。
5	つながりで波及するリスクを想定する	①	セキュリティ上の脅威や機器の故障の影響が、他の機器とつながることにより波及するリスクを想定する。
		②	特に、対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。

IoT推進コンソーシアムGL（分析）

要点		ガイドラインに記載されているポイント	
6	物理的なリスクを認識する	①	盗まれたり紛失した機器の不正操作や管理者のいない場所での物理的な攻撃に対するリスクを想定する。
		②	中古や廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。
7	過去の事例に学ぶ	①	パソコン等のICT の過去事例から攻撃事例や対策事例を学ぶ。
		②	IoT の先行事例から攻撃事例や対策事例を学ぶ。

説明は省略

IoT推進コンソーシアムGL（設計）

要点		ガイドラインに記載されているポイント	
8	個々でも全体でも守れる設計をする	①	外部インタフェース経由／内包／物理的接触によるリスクに対して個々のIoT 機器・システムで対策を検討する。
		②	個々のIoT 機器・システムで対応しきれない場合は、それらを含む上位のIoT 機器・システムで対策を検討する。
9	つながる相手に迷惑をかけない設計をする	①	IoT 機器・システムの異常を検知できる設計を検討する。
		②	異常を検知したときの適切な振る舞いを検討する。
10	安全安心を実現する設計の整合性をとる	①	安全安心を実現するための設計を見える化する。
		②	安全安心を実現するための設計の相互の影響を確認する。

説明は省略

IoT推進コンソーシアムGL（設計）

要点		ガイドラインに記載されているポイント	
11	不特定の相手とつなげられても 安全安心を確保できる設計をする	①	IoT 機器・システムがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する。
12	安全安心を実現する 設計の検証・評価を行う	①	つながる機器やシステムは、IoT ならではのリスクも考慮して安全安心を実現する設計の検証・評価を行う。

説明は省略

IoT推進コンソーシアムGL（構築・接続）

要点		ガイドラインに記載されているポイント	
13	機器等がどのような状態かを把握し、記録する機能を設ける	①	機器等の状態や他の機器との通信状況を把握して記録する機能を検討する。
		②	記録を不正に消去・改ざんされないようにする機能を検討する。
14	機能及び用途に応じて適切にネットワーク接続する	①	機能及び用途に応じてネットワーク接続の方法を検討し、構築・接続する。
		②	ネットワーク接続の方法を検討する際には、IoT 機器の機能・性能のレベルも考慮する。
15	初期設定に留意する	①	IoT システム・サービスの構築・接続時や利用開始時にセキュリティに留意した初期設定を行う。
		②	利用者へ初期設定に関する注意喚起を行う。

IoT推進コンソーシアムGL（構築・接続）

要点		ガイドラインに記載されているポイント	
16	認証機能を導入する	①	IoT システム・サービス全体でセキュリティの確保を実現する認証機能を適用する。
		②	IoT 機器の機能・性能の制約を踏まえた適切な認証方式を使用する。

説明は省略

IoT推進コンソーシアムGL（運用・保守）

要点		ガイドラインに記載されているポイント	
17	出荷・リリース後も安全安心な状態を維持する	①	IoTの提供者等は、セキュリティ上重要なアップデート等を適切に実施する方法を検討し、適用する。
18	出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える。	①	脆弱性情報を収集・分析し、ユーザや他のシステム・サービスの供給者・運用者に情報発信を行う。
		②	セキュリティに関する重要な事項を利用者へあらかじめ説明する。
		③	出荷・リリース後の構築・接続、運用・保守、廃棄の各ライフサイクルで関係者に守ってもらいたいことを伝える。
19	つながることによるリスクを一般利用者に知ってもらう	①	不用意なつなぎ方や不正な使い方は、自分や他人に被害を与えたるなど守ってもらいたいことを一般利用者に伝える。

IoT推進コンソーシアムGL（運用・保守）

要点		ガイドラインに記載されているポイント	
20	IoT システム・サービスにおける関係者の役割を認識する	①	IoT 機器メーカやIoT システム・サービス提供者及び一般利用者の役割を整理する。
21	脆弱な機器を把握し、適切に注意喚起を行う	①	ネットワーク上でIoT 機器を把握する仕組みを構築し、脆弱性を持つIoT 機器の特定を行う。
		②	脆弱性を持つIoT 機器を特定した場合には、該当するIoT 機器の管理者へ注意喚起を行う。

説明は省略

IoT推進コンソーシアムGL（一般利用者）

一般利用者のためのルール		ガイドラインに記載されているポイント	
1	問合せ窓口やサポートがない機器やサービスの購入・利用を控える	①	問合せ窓口やサポートがない（もしくはサポート期限が切れた）機器やサービスの購入・利用は行わないようにしましょう。
2	初期設定に気をつける	①	機器を初めて使う際には、ID、パスワードの設定を行いましょう。
3	使用しなくなった機器については電源を切る	①	使用しなくなった機器や不具合が生じた機器は電源を切りましょう。
4	機器を手放す時はデータを消す	①	機器を手放す際は、自分や家族等の利用者のプライバシー情報が漏れないよう、情報を確実に削除しましょう。

※第3章として2頁補足的に記載されている

アウトプットイメージ（目標）

JAPAN SMARTPHONE SECURITY ASSOCIATION

◆想定する対象者：
- 企業のIoT導入推進者

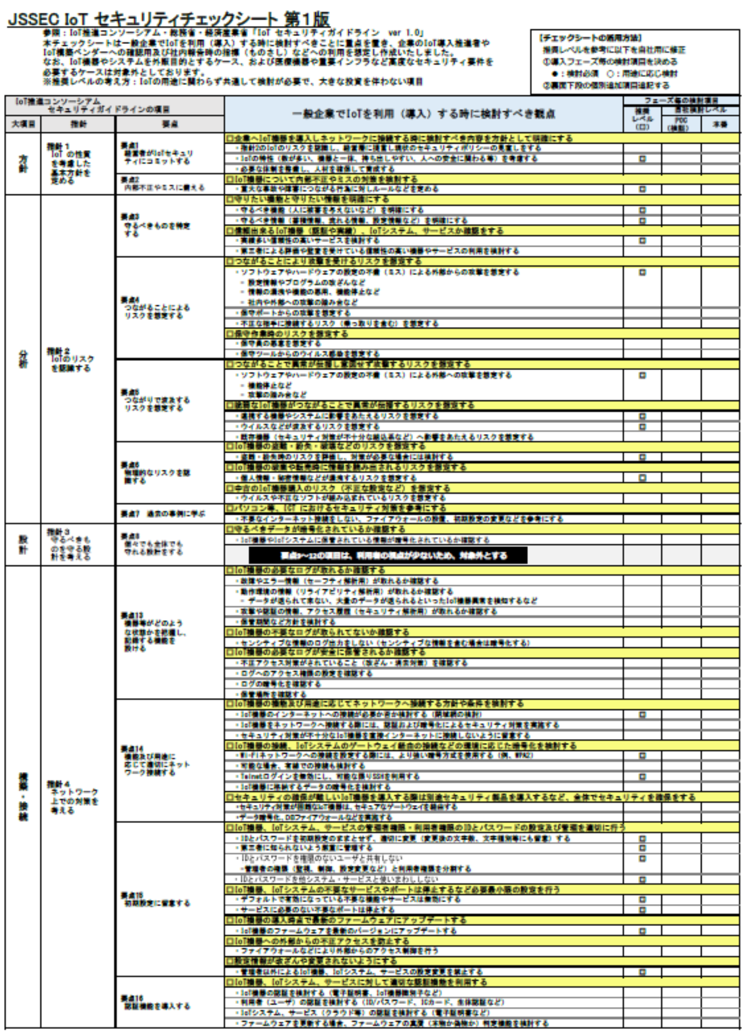
◆発信する内容：
- 一般企業がIoT導入する時、サイバーセキュリティ面の検討項目一覧（チェックシート）

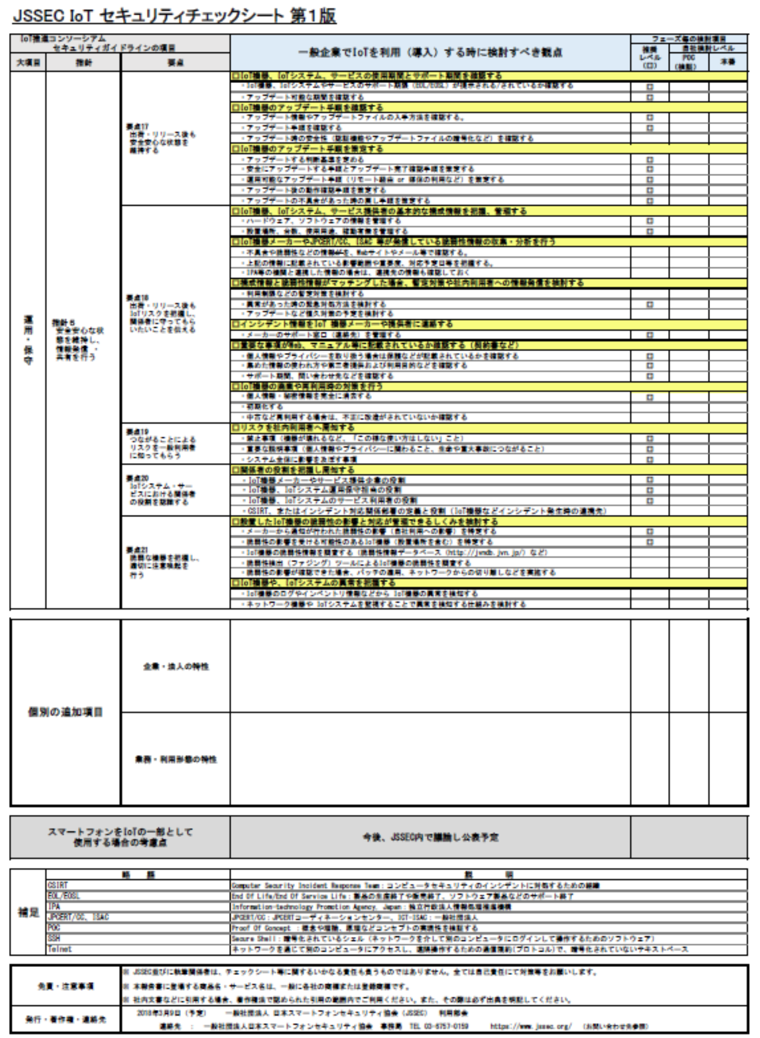
◆想定する活用イメージ：
- 社内IoT導入推進者の検討のベース
- 社内の経営層などへの報告時の指標（ものさし）
- IoT構築ベンダーとの確認用

◆チェックシート構成上の工夫：
- 早い段階（POCなど検証）からの検討着手を促す
- 共通して検討すべき推奨項目を明記
- 企業/法人の特性や利用形態の特性に合わせ項目追加可能

チェックシートイメージ

JAPAN
SMARTPHONE
SECURITY
ASSOCIATION





チェックシート構成

JAPAN SMARTPHONE SECURITY ASSOCIATION

JSSEC IoT セキュリティチェックシート 第1版

①IoTチェックシートの使い方

参照：IoT推進コンソーシアム・総務省・経済産業省「IoT セキュリティガイド
本チェックシートは一般企業でIoTを利用（導入）する時に検討すべきことに重点を置き、企業のIoT導入推進者や
IoT構築ベンダーへの確認用及び社内報告時の指標（ものさし）などへの利用を想定し作成いたしました。
なお、IoT機器やシステムを外販目的とするケース、および医療機器や重要インフラなど高度なセキュリティ要件を
必要するケースは対象外としております。
※推奨レベルの考え方：IoTの用途に関わらず共通して検討が必要で、大きな投資を伴わない項目

推奨レベルを参考に以下を自社用に修正
①導入フェーズ毎の検討項目を決める
●：検討必須　○：用途に応じ検討
②裏面下段の個別追加項目追記する

IoT推進コンソーシアム セキュリティガイドラインの項目			一般企業でIoTを利用（導入）する時に検討すべき観点	フェーズ毎の検討項目		
大項目	指針	要点		推奨レベル（□）	自社検討レベル POC（検証）	自社検討レベル 本番
方針	指針1 IoT の性質を考慮した基本方針を定める	要点1 経営者がIoTセキュリティにコミットする	□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			
			・指針2のIoTのリスクを認識し、経営層に捉直し現状のセキュリティポリシーの見直しをする			
			・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等）を考慮する	□		
			・必要な体制を整備し、人材を確保して育成する			
		要点2 内部不正やミスに備える	□IoT機器について内部不正やミスの対策を検討する			
			・重大な事故や障害につながる行為に対しルールなどを定める	□		
			□守りたい機能と守りたい情報を明確にする			
			・守るべき機能（人に被害を与えないなど）を明確にする	□		
			・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	□		
			□信[illegible]			
			・[illegible]	□		
			□つ[illegible]			
			・[illegible]			
			□保[illegible]			
			・[illegible]			
			□つ[illegible]			
			・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 －機能停止など －攻撃の踏み台など	□		
			□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			
			・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	□		
			・ウイルスなどが波及するリスクを想定する	□		
			・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			
			□IoT機器の盗難・紛失・破壊などのリスクを想定する			
			・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			
			・個人情報・秘密情報などが漏洩するリスクを想定する	□		
			□中古のIoT機器購入のリスク（不正な設定など）を想定する			
			・ウイルスや不正なソフトが組み込まれているリスクを想定する			
			□パソコン等、ICT におけるセキュリティ対策を参考にする			
			・不要なインターネット接続をしない、ファイアウォールの設置、初期設定の変更などを参考にする			
		要点6 物理的なリスクを認識する				
		要点7 過去の事例に学ぶ				

②IoTコンソーシアムガイドラインの指針と要点

※開発時のライフサイクルで導入時のライフサイクルと異なるが今回は対比に重点を置き枠組みは変更していない

③深読みし、企業のIoT推進者や管理者の視点で検討すべき点
□：検討すべき観点
・：チェック項目
ー：補足説明

④フェーズ毎の検討事項
□：推奨レベル
POC ⇒　本番

チェックシート構成（裏面下部）

JAPAN SMARTPHONE SECURITY ASSOCIATION

個別の追加項目	企業・法人の特性 業務	⑤IoTの使われ方などに合わせ、各企業で追加頂く項目 ※IoTが利用される分野や形態は多様であり、特性にあわせ検討項目を追加する形態とした			
スマートフォンをIoTの一部として使用する場合の考慮点		今後、JSSEC内で議論し公表予定			

	略　語	説　明
補足	CSIRT	Computer Security Incident Response Team：コンピュータセキュリティのインシデントに対処するための組織
	EOL/EOSL	End Of Life/End Of Service Life：製品の生産終了や販売終了、ソフトウェア製品などのサポート終了
	IPA	Information-technology Promotion Agency, Japan：独立行政法人情報処理推進機構
	JPCERT/CC、ISAC	JPCERT/CC：JPCERTコーディネーションセンター、ICT-ISAC：一般社団法人
	POC	Proof Of Concept ：概念や理論、原理などコンセプトの実現性を検証する
	SSH	Secure Shell：暗号化されているシェル（ネットワークを介して別のコンピュータにログインして操作するためのソフトウェア）
	Telnet	信規約(プロトコル)で、暗号化されていないテキストベース

⑥補足、注意事項や連絡先など

免責・注意事項	※ JSSEC並びに[illegible]責任にて対策等をお願いします。 ※ 本報告書に登場する商品名・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。
発行・著作権・連絡先	2018年3月9日（予定）　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.jssec.org/　（お問い合わせ先参照）

チェックシート活用のポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION

➔ 配布いたしました、A3両面の資料にて以下説明致します。

JSSEC IoT セキュリティチェックシート 第1版

参照：IoT推進コンソーシアム・総務省・経済産業省「IoT セキュリティガイドライン ver 1.0」
本チェックシートは一般企業でIoTを利用（導入）する時に検討すべきことに重点を置き、企業のIoT導入推進者やIoT構築ベンダーへの確認用及び社内報告時の指標（ものさし）などへの利用を想定し作成いたしました。
なお、IoT機器やシステムを外販目的とするケース、および医療機器や重要インフラなど高度なセキュリティ要件を必要するケースは対象外としております。
※推奨レベルの考え方：IoTの用途に関わらず共通して検討が必要で、大きな投資を伴わない項目

【チェックシートの活用方法】
推奨レベルを参考に以下を自社用に修正
①導入フェーズ毎の検討項目を決める
●：検討必須　○：用途に応じ検討
②裏面下段の個別追加項目追記する

<ポイント>
・POC（検証）のフェーズからセキュリティを考慮する。
・チェックシートを参考に共通して検討すべき項目を決める。
・各社独自に検討すべき項目を追加する。

チェックシート活用のポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION

方針	要点1 経営者がIoTセキュリティにコミットする	□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 ・指針2のIoTのリスクを認識し、経営層に提言し現状のセキュリティポリシーの ・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等） ・必要な体制を整備し、人材を確保して育成する
	要点2 内部不正やミスに備える	□IoT機器について内部不正やミスの対策を検討する ・重大な事故や障害につながる行為に対しルールなどを定める
分析	要点3 守るべきものを特定する	□守りたい機能と守りたい情報を明確にする ・守るべき機能（人に被害を与えないなど）を明確にする ・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 □信頼出来るIoT機器（認証や実績）、IoTシステム、サービスか確認をす ・実績多い信頼性の高いサービスを検討する ・第三者による評価や監査を受けている信頼性の高い機器やサービスの利用を検
	要点4 つながることによるリスクを想定する	□つながることにより攻撃を受けるリスクを想定する ・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 – 設定情報やプログラムの改ざんなど – 情報の漏洩や機能の悪用、機能停止など – 社内や外部への攻撃の踏み台など ・保守ポートからの攻撃を想定する ・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 □保守作業時のリスクを想定する ・保守員の悪意を想定する ・保守ツールからのウイルス感染を想定する
	要点5 つながりで波及するリスクを想定する	□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 ・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 – 機能停止など – 攻撃の踏み台など □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 ・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 ・ウイルスなどが波及するリスクを想定する ・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

＜要点１：ポイント＞
・IoTの特性やリスクを認識し情報セキュリティとの違いをセキュリティポリシーに反映し、体制整備を行う

＜要点３：ポイント＞
・守るべきものに機能が加わる
・信頼性のある機器などを選定

＜要点４：ポイント＞
・つながらない前提の組込み系からの意識改革が必要
・保守（USBも含め）は要注意

＜要点５：ポイント＞
・既にインターネットでIoTによる不正な通信が多数発生
・社内も含め、攻撃したり、されたりするリスクが増加

チェックシート活用のポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION

分析	要点6 物理的なリスクを認識する	□IoT機器の盗難・紛失・破壊などのリスクを想定する			
		・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			
		・個人情報・秘密情報などが漏洩するリスクを想定する			
		□中古のIoT機器購入のリスク（不正な設定など）を想定する			
		・ウイルスや不正なソフトが組み込まれているリスクを想定する			
	要点7　過去の事例に学ぶ	□パソコン等、ICT におけるセキュリティ対策を参考にする			
		・不要なインターネット接続をしない、ファイアウォールの設置、初期設定の変			
設計	要点8 個々でも全体でも守れる設計をする	□守るべきデータが暗号化されているか確認する			
		・IoT機器や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			
		要点9~12の項目は、利用者の視点が少ないため、対象外とす			
構築・接続	要点13 機器等がどのような状態かを把握し、記録する機能を設ける	□IoT機器の必要なログが取れるか確認する			
		・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			
		・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			
		– データが送られて来ない、大量のデータが送られるといったIoT機器異常を検			
		・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			
		・保管期間など方針を検討する			
		□IoT機器の不要なログが取られてないか確認する			
		・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			
		□IoT機器の必要なログが安全に保管されるか確認する			
		・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			
		・ログへのアクセス権限の設定を確認する			
		・ログの暗号化を確認する			
		・保管場所を確認する			

＜要点６：ポイント＞
・スマホ等と同様、紛失・盗難
廃棄・中古品の利用に注意

＜要点８：ポイント＞
・保管データの暗号化について
「設計」にしか書かれていない
いため、ここに記載
（今後の改定で利用の視点
から構築に移動）

＜要点13：ポイント＞
・ログの保管について検討する

チェックシート活用のポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION

構築・接続	要点14 機能及び用途に応じて適切にネットワーク接続する	□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
		・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）
		・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
		・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
		□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
		・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
		・可能な場合、有線での接続も検討する
		・Telnetログインを無効にし、可能な限りSSHを利用する
		・IoT機器に格納するデータの暗号化を検討する
		□セキュリティの確保が難しいIoT機器を導入する際は別途セキュリティ
		・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
		・データ暗号化、DBファイアウォールなどを実施する
	要点15 初期設定に留意する	□IoT機器、IoTシステム、サービスの管理者権限・利用者権限のIDとパス
		・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
		・第三者に知られないよう厳重に管理する
		・IDとパスワードを権限のないユーザと共有しない -管理者の権限（監視、制御、設定変更など）と利用者権限を分割する
		・IDとパスワードを他システム・サービスと使いまわししない
		□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
		・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
		・サービスに必要のない不要なポートは停止する
		□IoT機器の導入時点で最新のファームウェアにアップデートする
		・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
		□IoT機器への外部からの不正アクセスを防止する
		・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
		□設定情報が改ざんや変更されないようにする
		・管理者以外によるIoT機器、IoTシステム、サービスの設定変更を禁止する
	要点16 認証機能を導入する	□IoT機器、IoTシステム、サービスに対して適切な認証機能を利用する
		・IoT機器の認証を検討する（電子証明書、IoT機器識別子など）
		・利用者（ユーザ）の認証を検討する（ID/パスワード、ICカード、生体認証な
		・IoTシステム、サービス（クラウド等）の認証を検討する（電子証明書など）
		・ファームウェアを更新する場合、ファームウェアの真贋（本物か偽物か）判定

<要点14：ポイント>
・インターネットに接続する必要があるか検討する。
・IoT機器への攻撃の多くがTelnetが使われるので、可能であれば無効にする

<要点15：ポイント>
・パスワードの初期設定を必ず変更する
・管理者パスワード管理が重要
・不要なポートは必ず止める
・ファームウェアを最新にする

<要点16：ポイント>
・ユーザ、機器、サービスの認証を検討する
・ファームウエアが本物か判定できるかを確認する

チェックシート活用のポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION

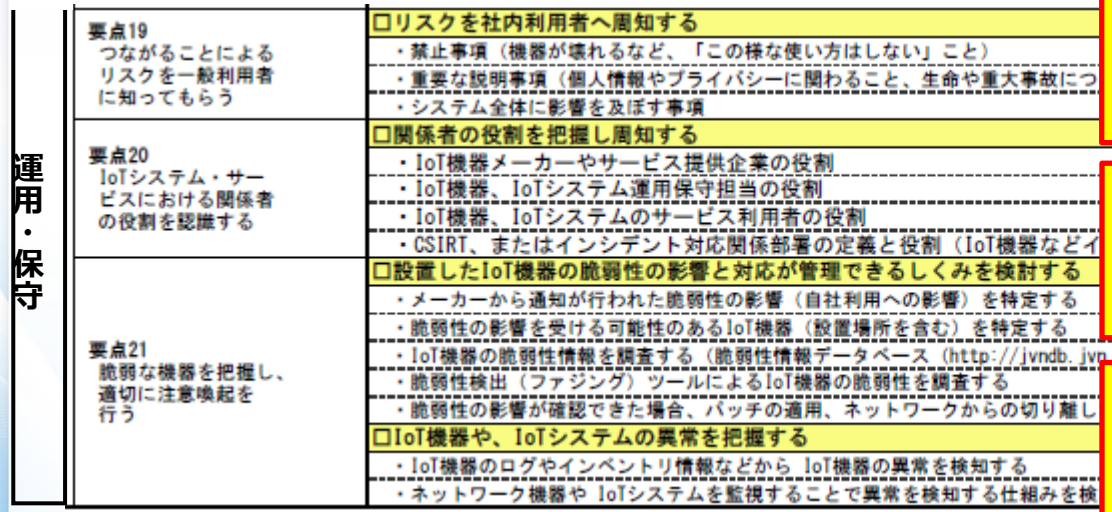
運用・保守	要点17 出荷・リリース後も安全安心な状態を維持する	□IoT機器、IoTシステム、サービスの使用期間とサポート期間を確認する
		・IoT機器、IoTシステムやサービスのサポート期限（EOL/EOSL）が提示される/さ
		・アップデート可能な期間を確認する
		□IoT機器のアップデート手順を確認する
		・アップデート情報やアップデートファイルの入手方法を確認する。
		・アップデート手順を確認する
		・アップデート時の安全性（認証機能やアップデートファイルの暗号化など）を
		□IoT機器のアップデート手順を策定する
		・アップデートする判断基準を定める
		・安全にアップデートする手順とアップデート完了確認手順を策定する
		・運用可能なアップデート手順（リモート経由 or 媒体の利用など）を策定する
		・アップデート後の動作確認手順を策定する
		・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
	要点18 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える	□IoT機器、IoTシステム、サービス提供者の基本的な構成情報を把握、管理する
		・ハードウェア、ソフトウェアの情報を管理する
		・設置場所、台数、使用用途、稼動有無を管理する
		□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
		・不具合や脆弱性などの情報を、Webサイトやメール等で確認する。
		・上記の情報に記載されている影響範囲や重要度、対応予定日等を把握する。
		・IPA等の機関と連携した情報の場合は、連携先の情報も確認しておく
		□構成情報と脆弱性情報がマッチングした場合、暫定対策や社内利用者への
		・利用制限などの暫定対策を検討する
		・異常があった時の緊急対処方法を検討する
		・アップデートなど恒久対策の予定を検討する
		□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
		・メーカーのサポート窓口（連絡先）を管理する
		□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
		・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
		・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
		・サポート期間、問い合わせ先などを確認する
		□IoT機器の廃棄や再利用時の対策を行う
		・個人情報・秘密情報を完全に消去する
		・初期化する
		・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確認する

＜要点17：ポイント＞
- 機器のサポート期間、ファームウェアのアップデート期間を確認する
- アップデート、動作確認、戻しなどの手順を策定する

＜要点18：ポイント＞
- システム構成を管理する
- 機器の不具合、脆弱性の情報を外部から収集する
- IoT機器の廃棄の時、初期化など情報を削除する
- 中古機器を使う場合、不正に改造されていないか確認する（具体的には難しいが）

チェックシート活用のポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION



運用・保守	要点19 つながることによるリスクを一般利用者に知ってもらう	□リスクを社内利用者へ周知する ・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） ・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 ・システム全体に影響を及ぼす事項
	要点20 IoTシステム・サービスにおける関係者の役割を認識する	□関係者の役割を把握し周知する ・IoT機器メーカーやサービス提供企業の役割 ・IoT機器、IoTシステム運用保守担当の役割 ・IoT機器、IoTシステムのサービス利用者の役割 ・CSIRT、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
	要点21 脆弱な機器を把握し、適切に注意喚起を行う	□設置したIoT機器の脆弱性の影響と対応が管理できるしくみを検討する ・メーカー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 ・脆弱性の影響を受ける可能性のあるIoT機器（設置場所を含む）を特定する ・IoT機器の脆弱性情報を調査する（脆弱性情報データベース（http://jvndb.jvn.jp/）など） ・脆弱性検出（ファジング）ツールによるIoT機器の脆弱性を調査する ・脆弱性の影響が確認できた場合、パッチの適用、ネットワークからの切り離し □IoT機器や、IoTシステムの異常を把握する ・IoT機器のログやインベントリ情報などから IoT機器の異常を検知する ・ネットワーク機器や IoTシステムを監視することで異常を検知する仕組みを検

<要点19：ポイント>
・社内利用者へ禁止事項などを周知する

<要点20：ポイント>
・CSIRTとの連携などの体制を検討する

<要点21：ポイント>
・脆弱性の影響を特定できる様に設置場所などを管理する
・IoT機器のログ分析や異常監視を検討する

チェックシート活用のポイント

JAPAN SMARTPHONE SECURITY ASSOCIATION

個別の追加項目	企業・法人の特性	
	業務・利用形態の特性	

＜個別追加：ポイント＞
・業種や企業風土の違いによるセキュリティ要求レベルの差にあわせ、検討すべき項目を追加
・IoTの利用分野や用途にあわせ、検討すべき項目を追加

スマートフォンをIoTの一部として使用する場合の考慮点	今後、JSSEC内で議論し公表予定	

補足	略　語	説　明
	CSIRT	Computer Security Incident Response Team：コンピュータセキュリティのインシデントに対処するための組織
	EOL/EOSL	End Of Life/End Of Service Life：製品の生産終了や販売終了、ソフトウェア製品などのサポート終了
	IPA	Information-technology Promotion Agency, Japan：独立行政法人情報処理推進機構
	JPCERT/CC、ISAC	JPCERT/CC：JPCERTコーディネーションセンター、ICT-ISAC：一般社団法人
	POC	Proof Of Concept ：概念や理論、原理などコンセプトの実現性を検証する
	SSH	Secure Shell：暗号化されているシェル（ネットワークを介して別のコンピュータにログインして操作するためのソフトウェア）
	Telnet	ネットワークを通じて別のコンピュータにアクセスし、遠隔操作するための通信規約(プロトコル)で、暗号化されていないテキストベース

免責・注意事項	※ JSSEC並びに執筆関係者は、チェックシート等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等をお願いします。 ※ 本報告書に登場する商品名・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。
発行・著作権・連絡先	2018年3月9日（予定）　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.jssec.org/　（お問い合わせ先参照）

今後の予定

JAPAN SMARTPHONE SECURITY ASSOCIATION

1．第１版の公開
- 本日の資料、チェックシートをJSSECホームページ掲載
- ご意見、ご指摘など募集予定
- 説明会、意見交換会など開催予定

➔　ご要望などありましたら、JSSEC事務局までご連絡下さい

2．チェックシートの有効性検証
- チェックシートが役立つか
- トライの時、最低限やらねばと感じる点
- 個別に追加された項目の収集

3．　解説編の発行
- 企業の方が活用しやすい工夫
- チェック項目の見直し

4．スマートフォンをIoTの一部として使用する場合の考慮点
- JSSEC内で検討し、チェックシートへ反映

おわりに

■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？？？

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

■企業へ導入するときに求められる事は
➔　Security by POC
（検証段階からセキュリティを検討する）

JAPAN SMARTPHONE SECURITY ASSOCIATION

ご清聴ありがとうございました