

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～

2020年8月20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

部会長 後藤 悦夫（株式会社 ラック）

セミナーの概要

■ IoTセキュリティチェックシート入門

・内 容

一般企業向けに作成した、セキュリティチェックシートの特徴を紹介

IoTセキュリティの共通する課題を
網羅的に解説（セキュリティの気づき）

IoTセキュリティの対策を効果的に
取り組むためのヒントや活用方法を
紹介（チェックシート活用のイメージ）

JAPAN
SMARTPHONE
SECURITY
ASSOCIATION

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

[illegible]

チェックシート解説編

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28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・研究スタッフフォーラム

文書管理番号 JSSEC-49-40

目次

1. 識別 (ID)	
1.1. 資産管理 (ID.AM)	
1.2. ビジネス継続 (ID.BE)	
1.3. ガバナンス (ID.GV)	
1.4. リスクアセスメント (ID.RA)	
1.5. リスクマネジメント戦略 (ID.RM)	
1.6. サプライチェーンリスクマネジメント (ID.SC)	
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)	
2.2. 監視向上およびトレーニング (PR.AT)	
2.3. データセキュリティ (PR.DS)	
2.4. 侵害を保護するためのプロセスおよび手順 (PR.IP)	
2.5. 保存 (PR.MA)	
2.6. 保護技術 (PR.PT)	
3. 検知 (DE)	
3.1. 異常とイベント (DE.AE)	
3.2. セキュリティの継続的なモニタリング (DE.CM)	
3.3. 検知プロセス (DE.DP)	
4. 対応 (RS)	
4.1. 対応計画 (RS.EP)	
4.2. ミニコミュニケーション (RS.CO)	
4.3. 分析 (RS.AN)	
4.4. 遮断 (RS.MI)	
4.5. 改善 (RS.IM)	
5. 復旧 (RC)	
5.1. 復旧計画 (RC.EP)	
5.2. 改善 (RC.IM)	
5.3. ミニコミュニケーション (RC.CO)	

Page 4

1. 識別 (ID)

1.1. 資産管理 (ID.AM)

01IoT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 (資産情報、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、通信機能を通じて外部から操作や制御を行ったり、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、事故や動作異常が発生した際にユーザーの身体や生命、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。

02IoT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盤情報にもなるため、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、ソフト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システムも同様に把握を行う。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、従来のオープンソース・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。たとえばIoT機器がセキュリティに脆弱とされていたとしても、通信経路が複数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。

03IoT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システム提供企業の役割、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/PISRTなどインシデント対応関係者の定義と役割 (IoT機器などインシデント発生時の連絡先)

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防止できる可能性がある。リスク分析などを進めるべき役割を検討するため、関係者のIoT導入・運用の体制と役割を把握する。

<補足>

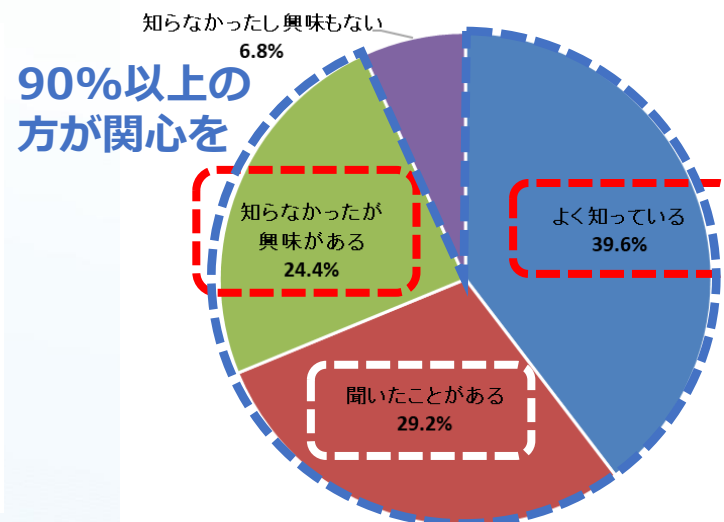
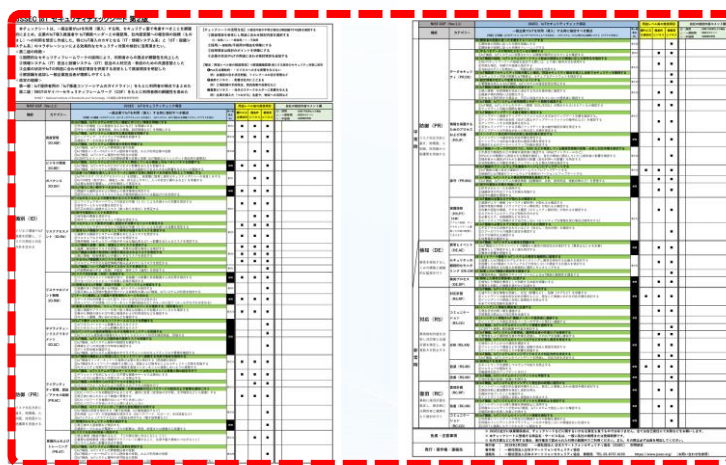
IoT機器、IoTシステムの関係者には、IoT機器、IoTシステムの管理責任者、IoT機器メーカーやIoTシステムサービス提供企業の担当者および利用企業、IoT機器、IoTシステム運用や保守担当、CSIRT/PISRTなどインシデント対応関係者などが挙げられる。具体的には、インシデント対応全体のハンドリング、原因究明、インシデントの影響範囲の見極め、関係者間の調整、原因の対応 (情報の交換など)、エンドユーザーへの対応、インシデントの発生に関する広報など、役割と役割を連絡先を含めて明確にしておく必要がある。

Page 5

Webアンケート結果

■アンケート調査結果

Q:IoTの情報セキュリティについては、注意すべき点や対処方法を示したガイドラインやチェックシートが国や専門団体から公表されています。たとえば下図のようなIoTセキュリティチェックシートについてご存じですか？



出典：JSSEC PR部会調査分析WG Webアンケート 詳細調査として2020年1月実施（N= 442複数回答/807調査依頼）

セミナーの対象と目標

■IoTセキュリティチェックシート入門

・対 象 IoTを導入する**一般企業の方**で
セキュリティに馴染が少ない方

・目 標 **IoTを安心・安全に活用するた**
めにセキュリティの概要を知る

JSSECの取り組み①

■スマートフォンとIoTの関係は？

JSSECでは、2011年より「スマートフォンを安心・安全に使うためのセキュリティ」をテーマに活動しております。

2016年より「**スマートフォンを基軸としたIoTセキュリティ**」への取り組みをはじめました。

JSSECのロゴは、IoT時代にスマートフォンの役割はどうなっているのかを表しております。



すべてのモノがつながるIoT時代、スマートフォンは「つながる世界と、私たちをつなぐ」大切な役割を担う．．

JSSECの取り組み②

■IoTセキュリティチェックシート発行経緯

2017年度：

IoTセキュリティチェックシート第1版
一般企業がIoTを利用する時に検討すべき観点

2018年度：

IoTセキュリティチェックシート第2版
米国の基準を採用し国際性と網羅性を高めた

2019年度：

IoTセキュリティチェックシート第2.1版
普及・啓発でITとOTの連携がより伝わるよう改訂

JSSECの取り組み③

■IoTセキュリティの普及・啓発への取り組み

大きく2つの分野へ普及・啓発

①IT（Information Technology）系のセミナー
情報セキュリティの知見をIoTセキュリティに活かす

②OT（Operational Technology）系へのセミナー
制御系やものづくりの現場に近い方々を対象に

**IoTセキュリティを効果的に取り組むためには、
①ITと②OTの担当の方の連携が重要となります**

セミナーの概要

■IoTセキュリティチェックシート入門

・セミナーの構成（各回10分程度）

①第1回：セミナー概要と受講の進め方

②第2回：チェックシートの特徴とセキュリティの重要性

③第3回：チェック項目「識別」の解説

④第4回：チェック項目「防御」の解説

⑤第5回：チェック項目「検知・対応・復旧」の解説

⑥第6回：チェックシートの活用例

セミナーの概要

■ IoTセキュリティチェックシート入門

① 動画セミナー概要と受講の進め方（ご覧頂いている動画）

- セミナーの対象者や、目標と**セミナー全体の概要**と使用する資料や、入手先など**受講の進め方**を紹介いたします。

② チェックシートの特徴とセキュリティの重要性

- IoTセキュリティ**チェックシートの構成と、どのような活用を想定して**作られているか紹介します。
- 使われている**用語の解説**や、IoTセキュリティ**対策の重要性**などを紹介いたします。

セミナーの概要

■ IoTセキュリティチェックシート入門

③ 識別（各項目の概要）

- 識別は検討の出発点で「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**」の項目を紹介します。
- 関係者が**現状を共有することが重要です**。

④ 防御（各項目の概要）

- 防御は③の「リスク対応方針に基き、物理面、人的面、技術面から**防御策を実施する**」の項目を紹介します。
- **事前に被害防止と軽減の対策が基本です**。

セミナーの概要

■ IoTセキュリティチェックシート入門

⑤ 検知・対応・復旧（各項目の概要）

- 異常を**検知**し、速やかに**被害拡大防止**の対処を行い、その後、復旧や再発防止を行う項目を紹介します。
- セキュリティ対策に完璧はなく、「**異常は発生する前提で備える**」ことが重要です。

⑥ チェックシートの活用例

- **初級編**として、**温度センサー**の導入を想定し、チェックシートの活用例を紹介します。
- 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**を紹介します。

■ 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）

※A3カラー（両面または2頁）で印刷し手元に準備して頂くと、よりスムーズに受講できます。



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。

A thumbnail image of the JSSEC IoT Security Checksheet 2nd Edition. It is a table with multiple columns and rows, containing various security-related information and checkboxes. The table is organized into sections, with some rows highlighted in green.

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

受講の進め方

■ 動画セミナーの受講

② JSSECホームページより、受講セミナーを掲載している動画サイト「YouTube」へ移動し受講して下さい。

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

■ 動画セミナー受講
→YouTubeへのリンク

■ セミナー資料
→HPよりダウンロード



※直接YouTube検索「JSSECchannel」でも受講可能です。

次回の紹介

■ IoTセキュリティチェックシート入門

■ 具体的な内容は次回からになります。

ぜひ次回の②をご覧ください、IoTセキュリティの「気づき」を感じて頂ければ幸いです。

② チェックシートの特徴とセキュリティの重要性

■ IoTセキュリティ **チェックシート**の構成と、どのような活用を想定して作られているか紹介します。

■ 使われている **用語**の解説や、IoTセキュリティ **対策**の重要性などを紹介いたします。

次回の受講おまちしております。