JAPAN SMARTPHONE SECURITY ASSOCIATION

# 2018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第二版～

2019年3月14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

JAPAN SMARTPHONE SECURITY ASSOCIATION

**「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第二版」**

- **改定の経緯とねらい**
- **チェックシート概要**
- **今後の計画**

■**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？？？**

# 利用部会「IoT調査・研究TF」の紹介

JAPAN SMARTPHONE SECURITY ASSOCIATION

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

**「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

・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

笠原　正弘（ソフトバンク）
中村　丈洋（SHIFT SECURITY）
不破　崇博（凸版印刷）
本間　輝彰（KDDI）
藤崎　卓哉（ラック）
瀬川　紘（セコムトラストシステムズ）
中村　康洋（シャープ）
北村　裕司（サイバートラスト株式会社）
松下　綾子（アルプスシステムインテグレーション）
坂田　孝昭（日立システムズ）

# 改定の経緯

JAPAN SMARTPHONE SECURITY ASSOCIATION

## ■2017年度の活動（合計６回TFを開催）

７月　　利用部会　　（TFメンバー募集）

➔「IoT推進コンソーシアムGLを利用者視点で一覧化・・」

11月　　利用部会・技術部会　合同成果報告会（中間報告）

３月　　JSSEC　セキュリティフォーラム2018（成果発表）

➔「チェックシート第一版」公開

## ■2018年度の活動（合計８回TFを開催）

➔「チェックシート第一版」の有用性の確認

※IoT推進コンソーシアム会員（約3千社）に配布、勉強会・意見交換

７月　　利用部会　　（TFメンバー募集）

➔「NIST-CSFを参照し国際性と網羅性向上、解説編・・」

11月　　利用部会　　（第二版の中間報告）

３月　　JSSEC　セキュリティフォーラム2019（成果発表）

➔「チェックシート第二版」公開

# 改定の経緯

## 第一版発行の進め方とねらい

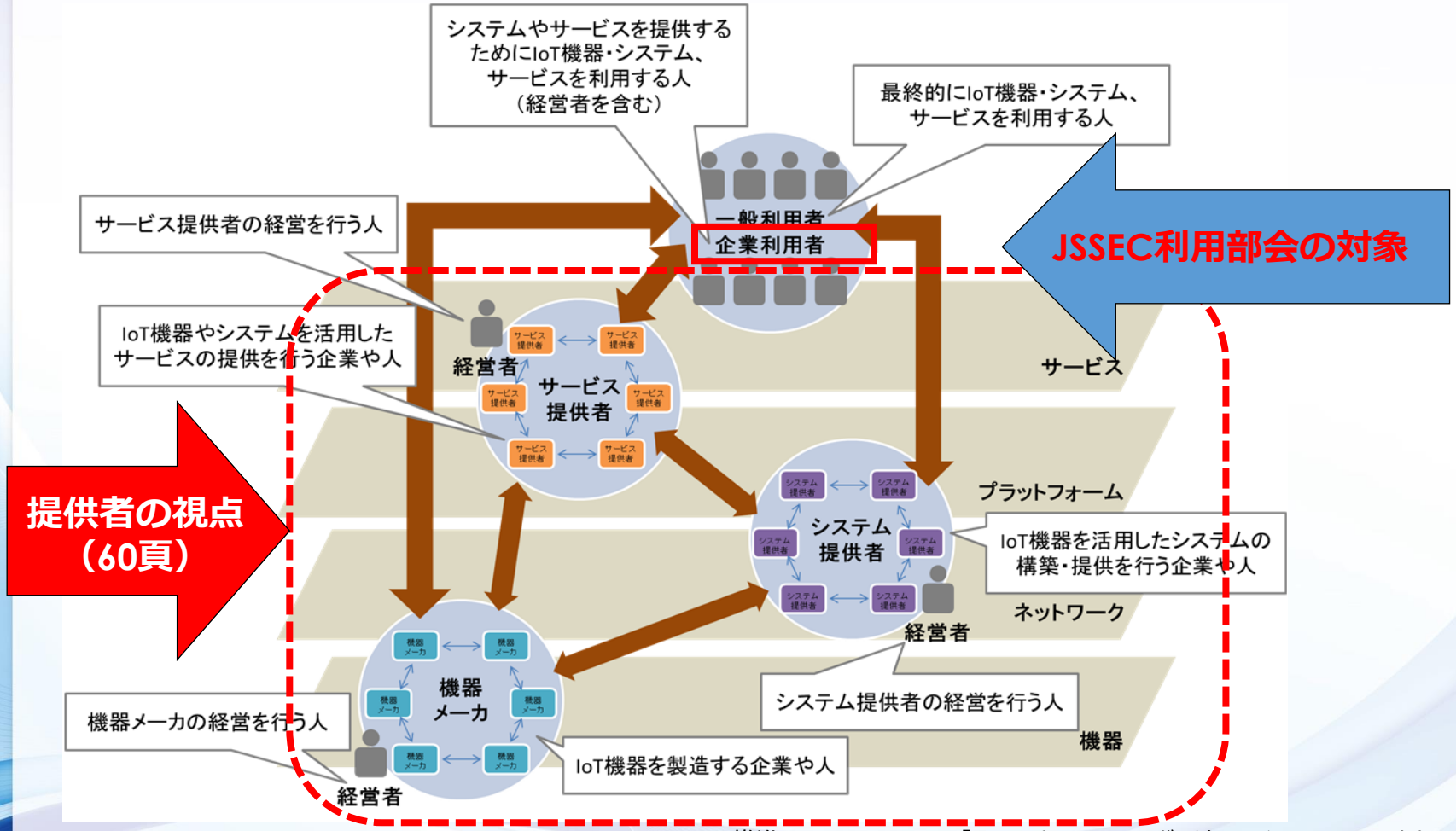
■**発行されているガイドラインを分析する**
- **IoT推進コンソーシアムガイドライン**を読み込み
- 利用企業として検討すべき項目を洗い出す

■**利用者に関係する部分を抽出、不足分を追加する**
- 企業への導入する**利用者視点からのガイドが存在しない**

■**JSSEC利用部会として発信するイメージを作成する**
- IoT全体を網羅し、その後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**
  ➔**利用可否を評価し、改定と解説編を検討する**

# 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

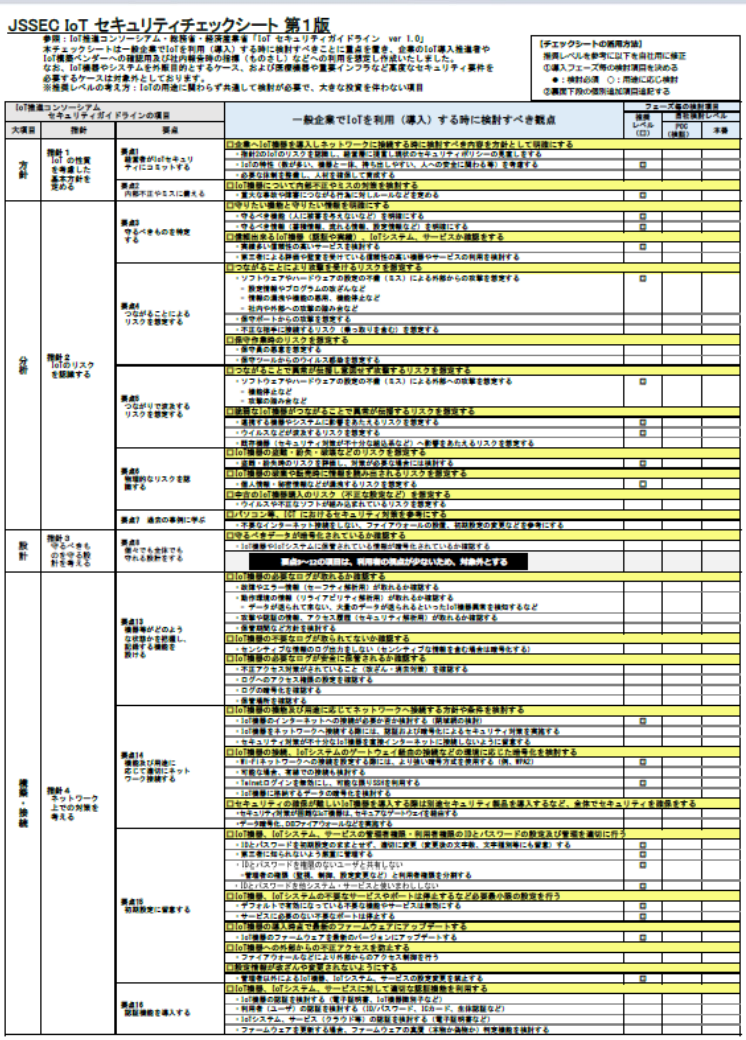
JAPAN SMARTPHONE SECURITY ASSOCIATION

| | | |
|---|---|---|
| **方針** | 指針1<br>**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<br>要点2. 内部不正やミスに備える |
| **分析** | 指針2<br>**IoT のリスクを認識する** | 要点3. 守るべきものを特定する<br>要点4. つながることによるリスクを想定する<br>要点5. つながりで波及するリスクを想定する<br>要点6. 物理的なリスクを認識する<br>要点7. 過去の事例に学ぶ |
| **設計** | 指針3<br>**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<br>要点9. つながる相手に迷惑をかけない設計をする<br>要点10. 安全安心を実現する設計の整合性をとる<br>要点11. 不特定の相手とつなげられても安全安心を確保<br>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<br>**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<br>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<br>要点15. 初期設定に留意する<br>要点16. 認証機能を導入する |
| **運用・保守** | 指針5<br>**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<br>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<br>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<br>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<br>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**<br>（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<br>ルール2）初期設定に気をつける<br>ルール3）使用しなくなった機器については電源を切る<br>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**

# チェックシート第一版のイメージ

JAPAN SMARTPHONE SECURITY ASSOCIATION



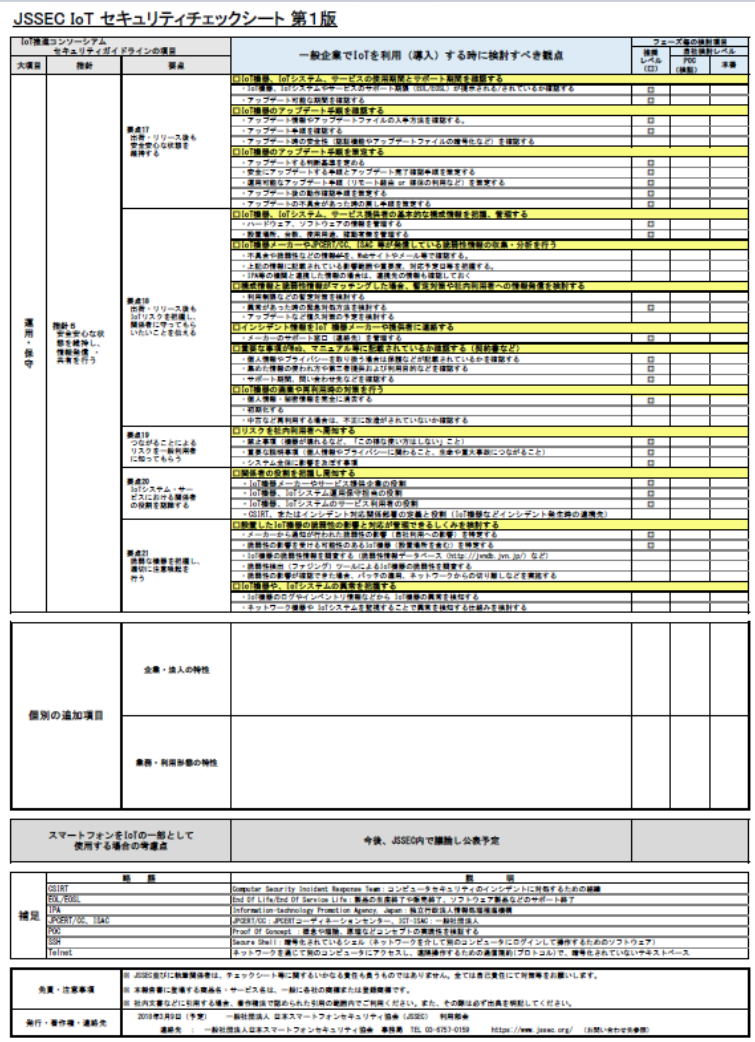
JSSEC IoT セキュリティチェックシート 第1版

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と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導入フェーズ等の検討項目を決める
●：検討必須　○：用途に応じ検討
②募集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着眼点 | フェーズ毎の検討項目 | | |
|---|---|---|---|---|---|---|
| | | | | 推奨レベル（□） | 自社検討レベル PDC（検証） | 本番 |
| 大項目 | 指針 | 要点 | | | | |
| 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際に検討すべき内容を方針として明確にする | | | |
| | | | ・設計ミスやリスクを把握し、経営者による検討のセキュリティポリシーの策定をする | | | |
| | | | ・IoTの特性（数が多い、場所と一体、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、人材を確保して実施する | | | |
| | | 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作業に対しルールなどを定める | □ | | |
| 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 | □守りたい機能と守りたい情報を明確にする | | | |
| | | | ・守るべき情報（人に被害を与えないなど）を明確にする | □ | | |
| | | | ・守るべき技術（重複情報、流れる情報、設定情報など）を明確にする | □ | | |
| | | | □侵害される(IoT機器（設備や装置）、IoTシステム、サービスの)価値をする | | | |
| | | | ・異常多い通信先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通信先の高い機器やサービスの利用を検討する | | | |
| | | 要点4 つながることによるリスクを認識する | □つながることにより脆弱性を受けるリスクを認識する | | | |
| | | | ・ソフトウェアやハードウェアの設定のの不備（ミス）による外部からの攻撃を想定する | □ | | |
| | | | ・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 | | | |
| | | | ・他やサポートからの攻撃を想定する | | | |
| | | | ・不正な端末に接続するリスク（乗っ取りを含む）を想定する | | | |
| | | | □振弊作業時のリスクを想定する | | | |
| | | | ・他やPCの感染を想定する | | | |
| | | | ・他や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他機に波及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他機するリスクを想定する | | | |
| | | | ・通信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端末など）へ影響をあたえるリスクを想定する | | | |
| | | 要点6 情報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機器の設定や動作時に情報が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 | □ | | |
| | | | □本当のIoT機器侵入のリスク（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、IT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 | | | |
| 設計 | 指針3 守るべきものの守るべき方法を考える | 要点8 | □守るべきデータが特定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の種類や比率されているか確認する | | | |
| | | | 重点ケースの実現は、利用者の満足がないため、対象外とする | | | |
| 構築・接続 | 指針4 ネットワーク上での対策を考える | 要点9 機器や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機器異常を検知するなど | | | |
| | | | ・故障や脆弱の情報、アクセス履歴（セキュリティ解析用）が取れるか確認する | | | |
| | | | ・保管期間などが妥当検討する | | | |
| | | | □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まめ場合は暗号化する） | | | |
| | | | □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・漏洩対策）を確認する | | | |
| | | | ・ログへのアクセス権限の設定を確認する | | | |
| | | | ・ログの確保先を確認する | | | |
| | | | ・保管場所を確認する | | | |
| | | 要点10 機器の接続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 | □IoT機器の接続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 | | | |
| | | | ・IoT機器のインターネットへの常時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、経路および暗号化によるセキュリティ対策を実施する | | | |
| | | | ・ネットワーク（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検討する | | | |
| | | 要点11 機能及び用途に応じて適切にネットワーク接続する | □IoT機器の接続、IoTシステムのゲートウェイ経由の接続などの通信先を検討する | | | |
| | | | ・到着ネットワークへの接続を許可する際には、より強い暗号方式を使用する（例、WPA2） | □ | | |
| | | | ・可能な場合、常時での接続を検討する | | | |
| | | | ・Telnetログインよりも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 | | | |
| | | | □セキュリティの提供が難しいIoT機器を導入する際は別途セキュリティ製品を導入するなど、全体でセキュリティを提供をする | | | |
| | | | ・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、DDoSファイアウォールなどを実施する | | | |
| | | 要点12 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・利用者権限の初とパスワードの設定及び管理を適切に行う | | | |
| | | | ・初とパスワードを初期状態のままなど、適切に変更（変更後の文字数、文字種別にも留意）する | □ | | |
| | | | ・第三者に知られないような管理と管理する | □ | | |
| | | | ・初とパスワードを複数のないユーザと共有しない | □ | | |
| | | | ・管理者の権限（変更、削除、設定変更など）と利用者権限を分割する | | | |
| | | | ・初とパスワードを他システム・サービスと使いまわしをしない | □ | | |
| | | | □IoT機器、IoTシステムの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 | | | |
| | | | ・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 | □ | | |
| | | 要点13 機器の導入時及び最後のファームウェアにアップデートする | □IoT機器の導入時及び最後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 | □ | | |
| | | 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 | | | |
| | | | □脆弱情報が公表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15 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機器の脆弱を検討する（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、生体認証など） | | | |
| | | | ・IoTシステム、サービス（クラウド上等）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正（末端か識別か）利用機能を検討する | | | |



JSSEC IoT セキュリティチェックシート 第1版

| 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着眼点 | フェーズ毎の検討項目 | | |
|---|---|---|---|---|---|---|
| | | | | 推奨レベル（□） | 自社検討レベル PDC（検証） | 本番 |
| 大項目 | 指針 | 要点 | | | | |
| 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 | □IoT機器、IoTシステム、サービスの提供期間とサポート期間を設置する | | | |
| | | | ・IoT機器・IoTやシステム・サービスのサポート期限（EOL/EOS）が提供されているか確認する | □ | | |
| | | | ・アップデート対応な期間を確認する | □ | | |
| | | | □IoT機器のアップデート手順を設置する | | | |
| | | | ・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。 | □ | | |
| | | | ・アップデート通知を確認する | □ | | |
| | | | ・アップデート時の安全性（改ざん検知やアップデートファイルの署名など）を確認する | | | |
| | | | □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実行確認手順を策定する | □ | | |
| | | | ・運用可能なアップデート手順（リリース前後 or 稼働の判断など）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・リリース後も安全安心な状態を維持する | □IoT機器、IoTシステム、サービス提供者の基本的な機能情報を把握、管理する | | | |
| | | | ・ハードウェア、ソフトウェアの情報を管理する | □ | | |
| | | | ・脆弱場所、装置、使用用途、稼動年数を管理する | □ | | |
| | | | □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・分析を行う | | | |
| | | | ・不具合や脆弱性などの情報収集、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やの情報と連携した情報の場合は、連携先の情報も確認して行く | | | |
| | | | □脆弱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情報発信を検討する | | | |
| | | | ・利用制限などの暫定対策を検討する | | | |
| | | | ・異常があった時の監視対応方法を検討する | □ | | |
| | | | ・アップデートなど個人対策の予定を検討する | | | |
| | | | □インシデント情報をIoT 機器メーカーや関係者に連絡する | | | |
| | | | ・メーカーにサポート窓口（連絡先）を確認する | □ | | |
| | | 要点19 つながることによるリスクを社内利用者へ周知する | □重要な事項が多い、マニュアル等に記載されているか確認する（契約書など） | | | |
| | | | ・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する | □ | | |
| | | | ・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機器の異常や異例時時の対策を行う | | | |
| | | | ・個人情報・秘密情報を第三者に渡する | □ | | |
| | | | ・初期にする | | | |
| | | | ・中古などで異例時する場合は、不正に改造がされていないか確認する | | | |
| | | | □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） | □ | | |
| | | | ・重要な脆弱事項（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） | □ | | |
| | | | ・システム停止に影響をおよぼす事項 | | | |
| | | 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 | □関係者の役割を認識し周知する | | | |
| | | | ・IoT機器メーカーやサービス提供企業の役割 | □ | | |
| | | | ・IoT機器、IoTシステム運用管理者の役割 | □ | | |
| | | | ・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者の交換と役割（IoT機器などインシデント発生時の連携含） | | | |
| | | 要点21 脆弱な機器を把握し、適切に注意喚起を行う | □脆弱した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 | | | |
| | | | ・メーカーから最低が作られた脆弱性の影響（自社利用への影響）を検討する | □ | | |
| | | | ・脆弱性の影響を受ける可能性のあるIoT機器（脆弱機能含む）を検討する | □ | | |
| | | | ・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（フィジング）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る場合、パッチの適用、ネットワークからの切り離しなどを実施する | | | |
| | | | □IoT機器や、IoTシステムの異常を把握する | | | |
| | | | ・IoT機器のログやイベントト情報などから、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討する | | | |
| 個別の追加項目 | | 企業・法人の特性 | | | | |
| | | 業務・利用形態の特性 | | | | |
| 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：製品の在庫終了や保守終了、ソフトウェア更新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。
※ 本資料書に記載する商品名・サービス名は、一般に各社の商標または登録商標です。
※ 社内文書などに利用する場合、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）　利用規約
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）

# チェックシート第一版の構成

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
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、経営層に提言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 | | | |
| | | | ・守 | | | |
| | | | ・守 | | | |
| | | | □信頼 | | | |
| | | | ・来 | | | |
| | | | ・第 | | | |
| | | | □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定する | | | |
| | | | －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 | | | |
| | | | □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 | | | |
| | | 物理的なリスクを認識する | | | | |
| | | 要点7 過去の事例に学ぶ | | | | |

②IoT推進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

④フェーズ毎の検討事項
POC ⇒　本番

# チェックシート第一版の構成（裏面下部）

JAPAN SMARTPHONE SECURITY ASSOCIATION

| | | |
|---|---|---|
| 個別の追加項目 | 企業・法人の特性<br>業務 | ⑤IoTの使われ方などに合わせ、各企業で追加頂く項目<br>※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 | |

| 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 | 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　　願いします。<br>※ 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。<br>※ 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<br>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） |

# 第一版の有用性確認（１）

JAPAN SMARTPHONE SECURITY ASSOCIATION

■JSSEC会員のIoTシステム提供者との意見交換
- 良くねられており、分かりやすい
- 自分たちが考えていた事と同じことも多く、安心できた
- 終了期限や廃棄期限について、気付きがあった
- 項目の内容へのご意見
  - ①「実績の多い」は実績が少ない現時点、うまく伝わらない
    - セキュリティに不安を感じるものを避けるで同感
  - ②設置環境などあってもいいのでは
    - IoTの物理的な設置場所・環境（ほこり、可燃性など）
  - ③ネットワーク構成の確認の重要性を感じている
    - 暗号化がなく盗聴されやすい
    - 海外にパケットが飛んで行くネットワークものもある
    - エッジのメーカーによっては、データ通信が国外に送付
- 独自追加項目「データが国内に留まっているか」が考えられる

# 第一版の有用性確認（２）

JAPAN SMARTPHONE SECURITY ASSOCIATION

■一般企業のセキュリティ担当者と意見交換
- 情報セキュリティから工場セキュリティを検討中、参考になる
- 分かりやすくまとまっている
- 解説があると、企業担当者でも理解できるのでありがたい
- さらに対策のヒントがあると助かる

■セキュリティ専門家（CISSP）勉強会での質問

Ｑ１：ITとOTの協力関係はどのようにすれば良いか？

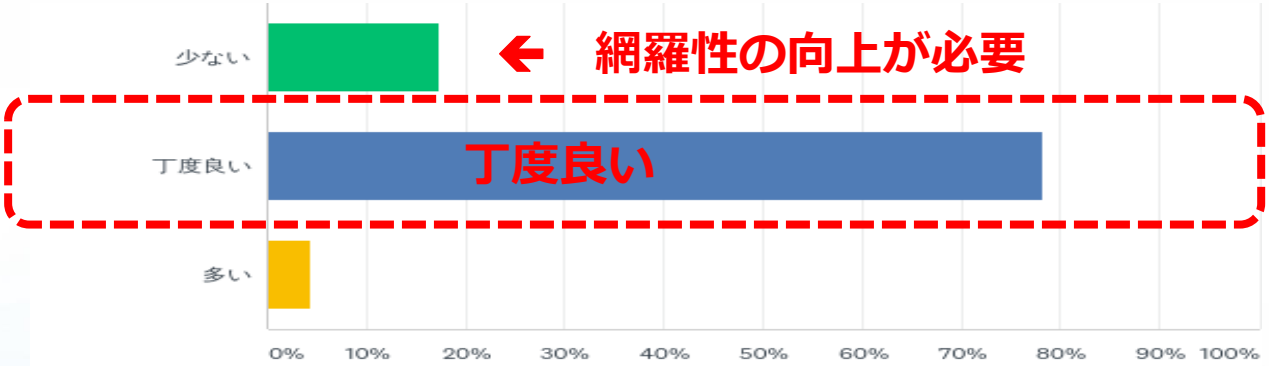
Ｑ２：国際的な動向へは、どのように対応していくのか？

# 第一版の有用性確認（３）

JAPAN SMARTPHONE SECURITY ASSOCIATION

## ■IoT推進コンソーシアム会員アンケート（26社）

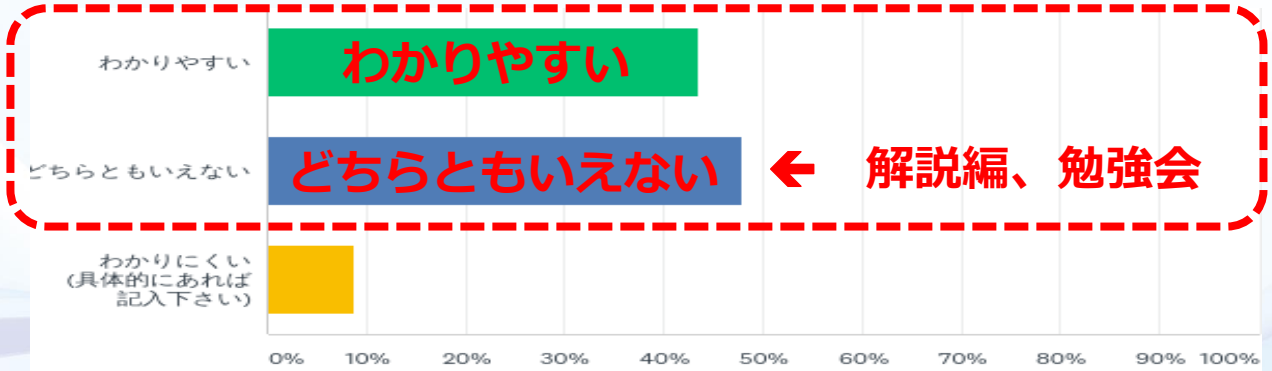
### Q1: チェック項目の分量はいかがですか？




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

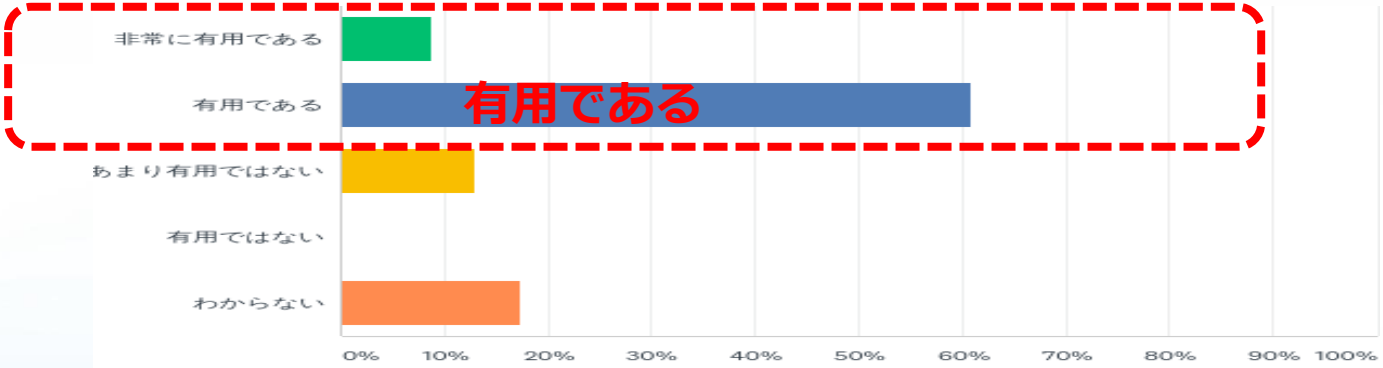
解説編、勉強会

# 第一版の有用性確認（３）

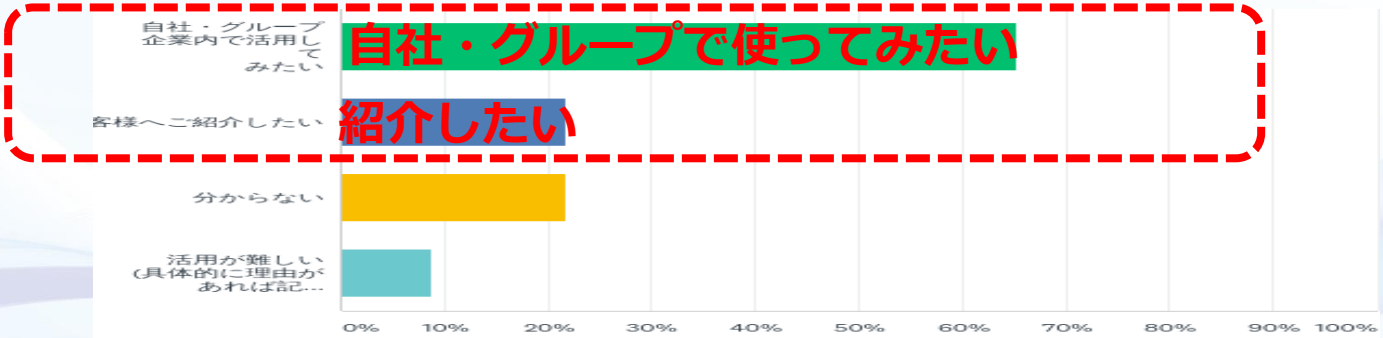
JAPAN SMARTPHONE SECURITY ASSOCIATION

## ■IoT推進コンソーシアム会員アンケート（26社）

**Q3: 本チェックシートは有用だと思いますか？**




**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？**



# チェックシート改定の進め方

JAPAN SMARTPHONE SECURITY ASSOCIATION

## ■NISTのCSFを縦軸に活用

**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**

**①Ver.1.1(2018/4)でIoTへの適用も・・と明記された**

2018 年 4 月 16 日　　サイバーセキュリティフレームワーク　　1.1 版

コミュニティにおいても、サイバーセキュリティ強化のための国際協力のモデルとして活用できる。

*フレームワーク*は、サイバーセキュリティの物理的側面、サイバー的側面、人的側面に対する効果を含め、柔軟にサイバーセキュリティに取り組むための方法を示す。*フレームワーク*は、サイバーセキュリティの主な焦点が、情報技術（IT）であるか、産業用制御システム（ICS）であるか、サイバーフィジカルシステム（CPS）であるか、あるいはモノのインターネット（IoT）等の一般的な接続デバイスであるかに関わらず、技術に依存する組織に対して適用可能なものである。*フレームワーク*は、サイバーセキュリティが顧客、従業員、その他の関係者に対して影響を及ぼす中で、組織がサイバーセキュリティに取り組んでいくのを支援する。さらに、*フレームワーク*に示された成果は、労働力の開発・発展活動の目標としても活用できる。

出典：IPA（NIST-CSF　Ver1.1日本語訳 2019.1発行）

# チェックシート改定の進め方

JAPAN SMARTPHONE SECURITY ASSOCIATION

## ■NISTのCSFを縦軸に活用

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

**②セキュリティ対策を進める視点が利用者に分かりやすい**

2014 年 2 月 12 日　　サイバーセキュリティフレームワーク　　バージョン 1.0

表 1: 機能の一意の識別子とカテゴリーの一意の識別子

| 機能の一意の識別子 | 機能 | カテゴリーの一意の識別子 | カテゴリー |
|---|---|---|---|
| ID | 特定 | ID.AM | 資産管理 |
| | | ID.BE | ビジネス環境 |
| | | ID.GV | ガバナンス |
| | | ID.RA | リスクアセスメント |
| | | ID.RM | リスク管理戦略 |
| PR | 防御 | PR.AC | アクセス制御 |
| | | PR.AT | 意識向上およびトレーニング |
| | | PR.DS | データセキュリティ |
| | | PR.IP | 情報を保護するためのプロセスおよび手順 |
| | | PR.MA | 保守 |
| | | PR.PT | 保護技術 |
| DE | 検知 | DE.AE | 異常とイベント |
| | | DE.CM | セキュリティの継続的なモニタリング |
| | | DE.DP | 検知プロセス |
| RS | 対応 | RS.RP | 対応計画の作成 |
| | | RS.CO | 伝達 |
| | | RS.AN | 分析 |
| | | RS.MI | 低減 |
| | | RS.IM | 改善 |
| RC | 復旧 | RC.RP | 復旧計画の作成 |
| | | RC.IM | 改善 |
| | | RC.CO | 伝達 |


出典：IPA（NIST-CSF　Ver1.0 日本語訳 ）

# 第二版の概要（ねらい）

本チェックシートは、**一般企業がIoTを利用（導入）**する時、**セキュリティ面で考慮すべきことを網羅的にまとめ**、・・・

**◆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**

特に**IoT導入のカギとなる「IT：情報システム系」と「OT：設備システム系」のコラボレーションによる効果的なセキュリティ対策**の検討に活用頂きたい。

# 第二版の概要（特徴）

JAPAN SMARTPHONE SECURITY ASSOCIATION

①**国際的なセキュリティフレームワーク**の採用により、利用者からの視点が網羅性を向上した

②**情報システム（IT）担当と設備システム（OT）担当の人材交流・育成のための共通言語**とした

③企業の状況や**IoTの用途に合わせ検討項目を択推する目安**として推奨項目を明記した

④**解説編を追加**し一般企業担当者が理解しやすくした

# 第二版の概要

JAPAN SMARTPHONE SECURITY ASSOCIATION

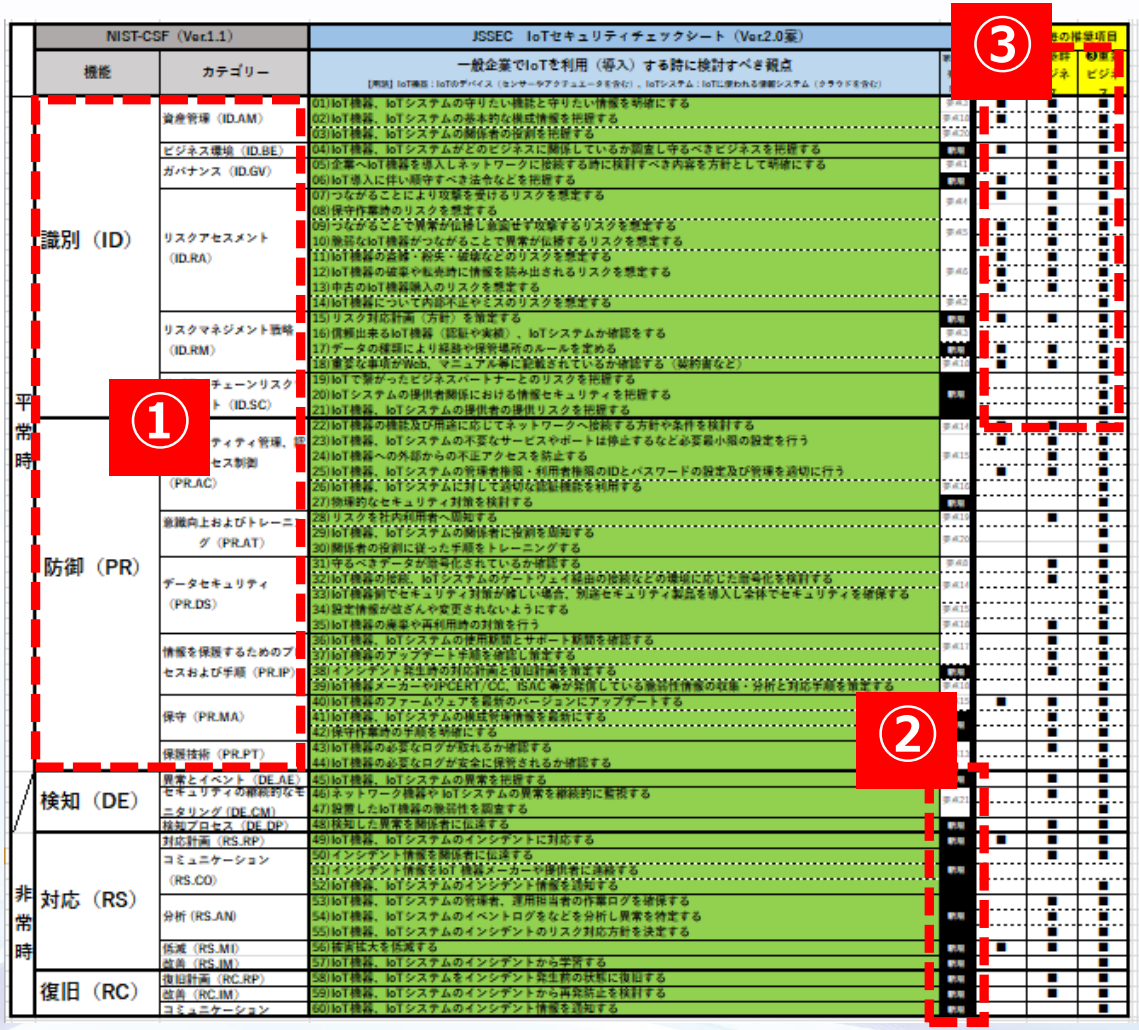
①NIST-CSFの分類：　5機能（識別、防御、検知、対応、復旧）
23カテゴリー(サブカテゴリーは参照)

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

# 第二版の概要




**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**

# 第二版の概要（識別）

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、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<br>【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<br>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<br>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<br>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<br>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<br>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<br>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 |

# 第二版の概要（防御）

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**を実施する

- **防御は用途レベルにあわせ**、対策を検討することが重要
- **IoTは使用期間が長い**、サポート期間の確認も重要

| 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<br>【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<br>24)IoT機器への外部からの不正アクセスを防止する<br>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<br>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<br>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<br>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<br>44)IoT機器の必要なログが安全に保管されるか確認する | 要点13 |

# 第二版の概要（検知・対応・復旧）

JAPAN SMARTPHONE SECURITY ASSOCIATION

検知（DE）：**異常を検知**するしくみの構築と継続的な監視を行う

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

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**をとり復旧を行う

| 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<br>【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<br>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<br>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 | 新規 |
| | | 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<br>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<br>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 |

# 今後の予定

## 1．第二版の公開

・JSSECホームページへ掲載（2/28）
①チェックシート（PDF/EXCEL）
②解説編（β版）、FAQ
③ご質問、講師派遣などの問い合わせ

**➔解説編（β版）へのご意見お願いします**

https://www.jssec.org/iot


## 2．来年度の予定

・普及・啓発を中心に活動予定

**➔勉強会やセミナーへの講師派遣を今後検討**

# 今後の予定

JAPAN SMARTPHONE SECURITY ASSOCIATION

## JSSEC　IoTセキュリティチェックシートの位置づけ

「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
➔サイバー・フィジカル・セキュリティ対策フレームワーク

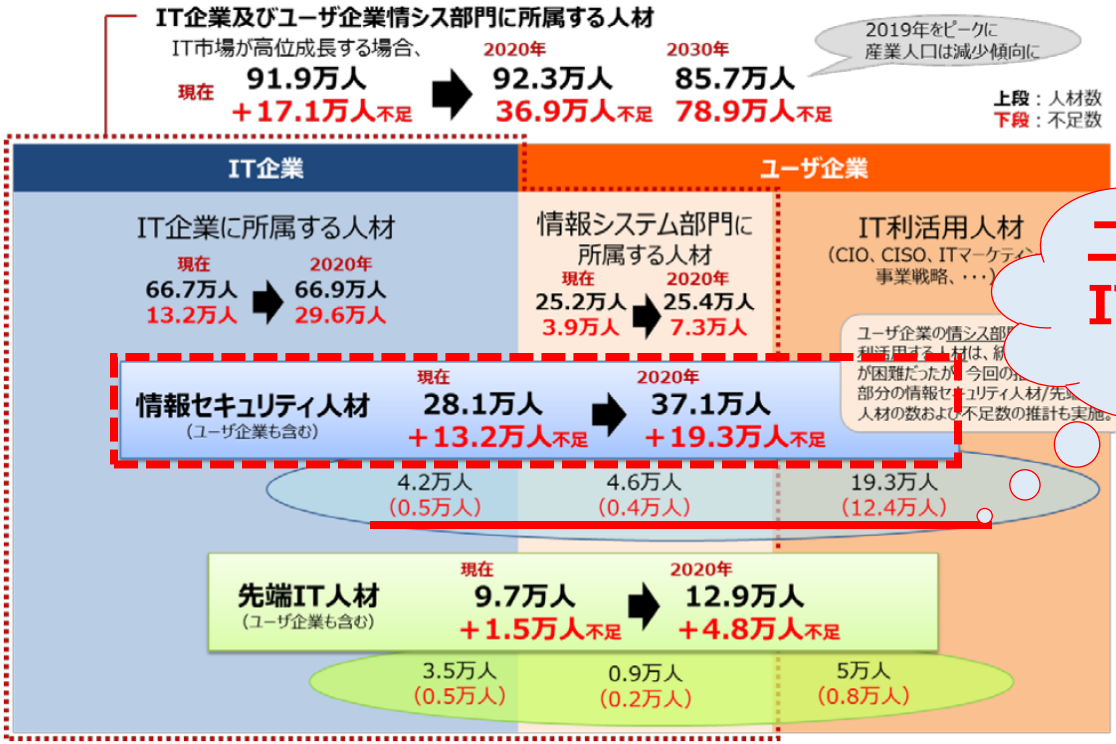
「企業のスマート化」
①スマート○○（工場、物流、ショップ、オフィス）
②コアテクノロジーはIoT
➔　IoTを安全・安心に活用するために・・
「IoTセキュリティチェックシート」

# 今後の予定（課題認識）

JAPAN SMARTPHONE SECURITY ASSOCIATION

## IoTを安全・安心に活用するためには

## ➔ セキュリティ人材育成が必須




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

# 今後の予定（啓発の重要性）

JAPAN SMARTPHONE SECURITY ASSOCIATION

製造業の安全作業活動に学ぶ、啓発の重要性

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

着目点 ＝ 知る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

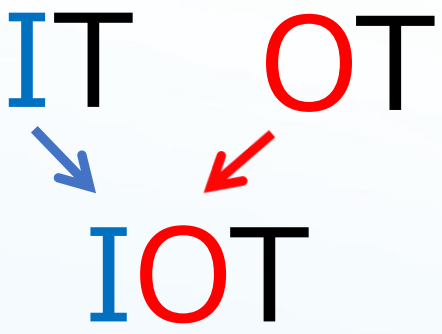
・安全な作業手順が出来るが、
やらなかった ➔ 改善

# 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？？？**
**①「Security by POC」**
（検証段階からセキュリティを検討する）

IoT ？




**②「Security by IOT」**
（「IT」と「OT」のコラボレーション）

JAPAN SMARTPHONE SECURITY ASSOCIATION

# ご清聴ありがとうございました