JSSEC IoT セキュリティチェックシート 第2版

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、企業のIoT導入推進者や IoT構築ベンダーとの確認用、社内経営層への報告時の指標（ものさし）への利用を想定し作成した。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。

＜第二版の特徴＞

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

＜改定の経緯＞

第一版：IoT提供者用の「IoT推進コンソーシアムのガイドライン」をもとに利用者の視点でまとめた
第二版：NISTのサイバーセキュリティフレームワーク（CSF）をもとに利用者側の網羅性を高めた

※NIST：National Institute of Standards and Technology（米国国立標準技術研究所）

【チェックシートの活用方法】※検討内容が不明な場合は解説編やFAQ集を確認する

①推奨項目を参考にし用途に合わせ検討内容を選択する
◎：採用／△：一部採用／×：不採用
②採用/一部採用/不採用の理由を明確にする
③採用項目は検討のポイントを明確にする
④企業の状況やIoTの用途に合わせ検討項目を追加する

【補足：用途レベル毎の推奨項目】※解説編確認要:導入する既存のセキュリティ対策に依存

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

	NIST-CSF（Ver.1.1）		JSSEC　IoTセキュリティチェック項目		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.	❶PoC又は補助的	❷基幹ビジネス	❸重要ビジネス	◎：採用 △：一部採用 ×：不採用	・採用/不採用などの理由 ・検討のポイント ・追加検討項目
平常時	識別（ID） 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	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（蓄積情報、流れる情報、設定情報など）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 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	要点18	■	■	■		
			03)IoT機器、IoTシステムの関係者の役割を把握する ①IoT機器、IoTシステムの管理責任者の役割 ②IoT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 ③IoT機器、IoTシステム運用や保守担当の役割 ④CSIRT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）	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** ①IoT機器、IoTシステムがどのビジネスに影響を与えるか把握する ②IoT機器、IoTシステムが重要なビジネス又は基幹ビジネスに大きな影響を与えないか調査する	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** ①IoTのリスク（リスクアセスメント）を認識し、経営層に提言し現状セキュリティポリシーの見直しをする ②IoT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など）を考慮する ③必要な体制を整備し、人材を確保して育成する	要点1		■	■		
			06)IoT導入に伴い順守すべき法令などを把握する ①関連する適用法令および契約上の要求事項を特定する ②認可されているソフトウェアおよび使用許諾されている製品だけを利用する	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** ①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 ②保守ポートからの攻撃を想定する ③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	要点4	■	■	■		
			08)保守作業時のリスクを想定する ①保守員の悪意を想定する ②保守ツールからのマルウェア感染を想定する			■	■		
			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 ①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	要点5	■	■	■		
			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 ①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 ②マルウェアなどが波及するリスクを想定する ③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		■	■	■		
			11)IoT機器の盗難・紛失・破壊などのリスクを想定する ①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	要点6	■	■	■		
			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 ①個人情報・秘密情報などが漏えいす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 ①マルウェアや不正な設定情報が組み込まれているリスクを想定する		■	■	■		
			14)IoT機器について内部不正やミスのリスクを想定する ①内部関係者の不正（故意）や設定・操作ミス（過失）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** ①リスクアセスメントの結果を受け、自組織への影響と許容範囲から対応策を検討する ②マネージメントレビューを実施し計画を確定する	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 ①実績が多く評価の高いIoT機器、IoTシステムを検討する ②第三者による評価や監査を受けている信頼性の高いIoT機器、IoTシステムの利用を検討する	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 ①データの社外保管ルールに従う（ルールがなければ定める） ②ネットワークの経路（インターネットや国外経由など）のルールに従う（ルールがなければ定める）	新規	■	■	■		
			18)重要な事項がWeb、マニュアルなどに記載されているか確認する（契約書など） ①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 ②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 ③サポート期間、問い合わせ先などを確認する	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** ①ビジネスパートナーに影響をあたえるリスク ②ビジネスパートナーから影響を受けるリスク	新規			■		
			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 ①IoTシステム提供者の情報セキュリティマネジメント状況を確認検証、評価する				■		
			21)IoT機器、IoTシステムの提供者の提供リスクを把握する ①IoT機器、IoTシステム提供の継続性を確認する ②障害などへの対応能力や体制を確認する ③データ所有権を確認する ④IoT機器、IoTシステム提供者のサプライチェーンのセキュリティリスク管理を確認する				■		
	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）	**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** 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	要点14	■	■	■		
			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 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	要点15	■	■	■		
			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 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）	要点16			■		
			27)物理的なセキュリティ対策を検討する ①第三者の入室制限など検討する ②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	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** ①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） ②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） ③システム全体に影響を及ぼす事項	要点19		■	■		
			29)IoT機器、IoTシステムの関係者に役割を周知する ①IoT機器、IoTシステムの管理責任者の役割 ②IoT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 ③IoT機器、IoTシステム運用や保守担当の役割 ④CSIRT、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）	要点20			■		

	NIST-CSF（Ver.1.1）		JSSEC　IoTセキュリティチェック項目		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.	❶PoC又は補助的	❷基幹ビジネス	❸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	
平常時	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		**30)関係者の役割に従った手順をトレーニングする** ①関係者の役割に従った手順を明確にする ②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** 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	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 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	要点14		■	■		
			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 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 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	要点15			■		
			35)IoT機器の廃棄や再利用時の対策を行う 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廃棄や再利用時には初期化する 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	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** ①IoT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 ②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。 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 ③アップデートする判断基準を定める ④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 ⑤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17		■	■		
			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 ①インシデントの基本的な対応手順を策定する ②インシデント対応後の基本的な復旧手順を策定する ③復旧のためのデータバックアップ計画を策定する	新規		■	■		
			39)IoT機器メーカーやJPCERT/CC、ISAC など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 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 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	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** ①IoT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 ②継続的に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 ①IoT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	新規		■	■		
			42)保守作業時の手順を明確にする ①許可されたツールを使用する ②遠隔保守の不正アクセス対策を実施する ③保守の履歴を管理する			■	■		
		保護技術（PR.PT） 【注意】 アクセス制御、データセキュリティと重複した内容は割愛してあります	**43)IoT機器の必要なログが取れるか確認する** 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）	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 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				■		
	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	異常とイベント（DE.AE）	**45)IoT機器、IoTシステムの異常を把握する** ①IoT機器のログやインベントリ情報から異常の検知方法を検討する（異常はなにかを定義） ②異常として検知するしきい値を検討する ③異常の影響を把握する	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** ①設置したIoT機器のログなどをモニタリングし異常を検知する仕組みを検討する ②設置したIoT機器にマルウェアなどが存在しないか調査する仕組みを検討する ③異常を検知する仕組みを継続的に運用しモニタリングする	要点21		■	■		
			47)設置したIoT機器の脆弱性を調査する ①脆弱性検出（脆弱性スキャン）ツールによるIoT機器の脆弱性を調査する				■		
		検知プロセス（DE.DP）	**48)検知した異常を関係者に伝達する** ①検知した情報を異常として判断する体制を明確にする ②異常と判断した情報を速やかに伝達する	新規		■	■		
非常時	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	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** ①速やかに発生事象を把握し、状況（影響など）、証拠（ログなど）を収集する ②インシデントの基本的な対応手順をもとに、発生した事象にあわせ対応手順を検討する ③インシデントの原因に対処し被害拡大を防止する ④全ての対応活動を記録する	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** ①発生状況の第一報を連絡する ②被害拡大防止など対応策を伝達する			■	■		
			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 ①インシデントの発生状況をメーカーのサポート窓口へ連絡する						
			52)IoT機器、IoTシステムのインシデント情報を通知する ①CSIRTと連携し報告範囲や内容を検討する				■		
		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** ①管理者および運用担当者の作業を記録し、そのログを保護し確保する			■	■		
			54)IoT機器、IoTシステムのイベントログなどを分析し異常を特定する ①検知システムからの通知を調査する ②フォレンジック調査などを実施し証拠の保全と原因を推定する ③インシデントの判定とその影響を把握する			■	■		
			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 ①IoT機器、IoTシステムのインシデントを評価し、対応方針を決定する			■	■		
		低減（RS.MI）	**56)被害拡大を低減する** ①ネットワークを遮断しマルウェアの拡大を防止する ②マルウェアを駆除する ③脆弱性対応のアップデートを行う	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** ①対応計画の見直し改善に利用する				■		
	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	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** ①インシデントの基本的な復旧手順をもとに、発生した事象にあわせ復旧手順を検討する ②復旧体制と復旧費用を検討し承認を得る ③復旧が完了したことを確認する ④インシデントの原因に対処し被害拡大を防止する	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** ①インシデントから得た情報を再発防止に活用する ②同種のインシデントが他のIoT機器、IoTシステムで発生しないか確認する ③復旧計画の見直し改善に利用する	新規		■	■		
		コミュニケーション（RC.CO）	**60)IoT機器、IoTシステムのインシデント情報を通知する** ①利用者にインシデントの存在又は関連するその詳細を通知する ②同種のインシデントがサプライチェーンの中で発生しないか関連会社に伝達する ③CSIRTと連携しステークホルダーに報告する	新規			■		

免責・注意事項	**※ JSSEC並びに執筆関係者は、チェックシートなど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などをお願いします。** **※ 本チェックシートに登場する商品名・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	**発行者　：　2019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** **著作権　：　一般社団法人日本スマートフォンセキュリティ協会** **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）**