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

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		
				推奨レベル（□）	自社検討レベル	
大項目	指針	要点			POC（検証）	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	□		
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る			
			・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討する			
		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			
		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			
		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、初期設定の変更などを参考にする			
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	**□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機器異常を検知するなど			
			・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・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検討する**			
			・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ティ対策を実施する			
			・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			
			□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			
			・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（例、WPA2）	□		
			・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製品を導入するなど、全体でセキュリティを確保をする			
			・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、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とパスワードの設定及び管理を適切に行う**			
			・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、文字種別等にも留意）する	□		
			・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	□		
			□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、生体認証など）			
			・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観点	フェーズ毎の検討項目		
				推奨レベル（□）	自社検討レベル	
大項目	指針	要点			POC（検証）	本番
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/されているか確認する	□		
			・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・分析を行う			
			・不具合や脆弱性などの情報がを、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ながること）	□		
			・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機器などインシデント発生時の連携先）			
		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　　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）