

JSSEC IoTセキュリティチェックシート第二版



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
 部会長 後藤 悦夫(株式会社ラック サイバー・グリッド・ジャパン)



1) チェックシート発行のねらい

一般企業がIoTを利用(導入)する際、セキュリティ面で考慮すべきことを網羅的にまとめ、企業への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り、効果的なセキュリティ対策の検討に貢献する

2) 活動の経緯

第一版<2018/3発行>:IoT推進コンソーシアムのガイドライン(提供者の視点)を深読みし一般企業の視点で検討すべきセキュリティ項目をまとめた。
 第二版<2019/3発行>:米国NISTのCSFを参照し改定、国際動向の反映と利用者の網羅性を向上、解説編を発行しIT側、OT側の共通認識や啓発などへ活用出来るようにした。

3) チェックシートの概要と特徴

- 一般企業がIoT導入時に考慮すべき項目を俯瞰的にA3両面60項目にまとめた!
- ① 国際的なセキュリティフレームワーク(NIST-CSF)の採用し網羅性を向上
 - ② ITとOT担当の人材交流・育成のための共通言語としてわかりやすくまとめた
 - ③ 企業の状況やIoTの用途に合わせ推奨項目参考に検討項目を選択できる
 - ④ 解説編の発行し普及・啓発に活用する
- 今後は普及・啓発(勉強会・セミナーへの講師派遣)に重点をおき活動予定

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	一般企業がIoTを利用(導入)する時に検討すべき観点	第一版 要 点 No.	①PoC又は 補助的	②基幹 ビジネス	③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	
①NIST-CSFの分類 (識別、防御、検知、 対応、復旧)	ビジネス環境 (ID.BE)	【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)							
		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 (不具合発生時(人)に被害を与えないなど)を明確にする	要 点 3	■	■	■			
		積情報、流れる情報、設定情報などを明確にする							
		システムの基本的な構成情報を把握する	要 点 18	■	■	■			
		ソフトウェアの情報を把握する							
		それを把握する							
		システムの関係者の役割を把握する							
		システムの管理責任者の役割	要 点 20		■	■			
		IoTシステム提供者の役割、および利用企業の役割							
		システム運用や保守担当の役割							
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)									
②企業のIoT推進者や管理者の視点 で検討すべき点	ガバナンス (ID.GV)	06)IoT導入に伴い順守すべき法令などを把握する	新 規	■	■	■			
		①関連する適用法令及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及び使用許諾されている製品だけを利用する							
		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							
		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)つながることによって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									
②マルウェアなどが波及するリスクを想定する									
10)脆弱なIoT機器がつながることによって異常が伝播するリスクを想定する	要 点 5	■	■	■					
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									
③IoT用途レベル 毎の推奨項目	識別 (ID)								
④各社の 検討内容	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								

ご自由にA3両面資料(Z折)をお取り下さい