

第5回 チェック項目 「検知」「対応」「復旧」の解説

～異常を検知するしくみの構築から
被害拡大の防止・復旧まで～

2020年9月1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

不破 崇博（凸版印刷株式会社）

JAPAN
SMARTPHONE
SECURITY
ASSOCIATION

第5回は「検知」「対応」「復旧」を解説します

「識別」「防御」までの相違点

平常時



① 識別

② 防御

③ 検知

④ 対応

⑤ 復旧

異常時



機能の識別子	機能	カテゴリの識別子	カテゴリ
ID	識別	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	リスクマネジメント戦略
		ID.SC	サプライチェーンリスクマネジメント
PR	防御	PR.AC	アイデンティティ管理とアクセス制御
		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	コミュニケーション
		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	コミュニケーション

セキュリティ対策に完璧はありません。

異常は発生することを前提で備えることが重要です。

チェック項目「検知」

- ① NIST-CSFの分類：平常時/異常時、3カテゴリー
(1)異常とイベント (2)セキュリティの継続的なモニタリング (3)検知プロセス
- ② 企業のIoT推進者や管理者の視点で検討すべき点：4項目
- ③ IoT用途レベル毎の推奨項目：3つの重要度に分類（「①PoC又は補助的」はなし）
- 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
- ⑤ 検討主体（IT又はOT）及び、連携（ITとOT）が重要な項目を明記

NIST-CSF (Ver.1.1)		IoTセキュリティチェック項目【項目No.表示例 ①：ITが主体的にOTと連携、②：OTが主体的にITと連携、③：ITとOTの連携が重要】		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		第一重要点 No.	①PoC又は補助的	②基幹ビジネス	③重要ビジネス	
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）	5)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		新設		■	■	
	セキュリティの継続的なモニタリング（DE.CM）	6)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適用しモニタリングする		要点2		■	■	
	検知プロセス（DE.DP）	7)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 ②検知した異常を関係者に伝達する ③検知した情報を異常として判断する体制を明確にする ④異常と判断した情報を速やかに伝達する		新設		■	■	

「検知」について

サイバーセキュリティイベントの発生を識別するのに適した対策を検討し、実施すること。

- ・「検知」機能はサイバーセキュリティイベントのタイムリーな発見を可能にする。
- ・「検知」機能の成果カテゴリーには、「異常とイベント」「セキュリティの継続的なモニタリング」「検知プロセス」がある。

検知：異常とイベント・セキュリティの継続的なモニタリング・検知プロセス

IoTセキュリティチェック項目【項目No.表示例 ①：ITが主体的にOTと連携、②：OTが主体的にITと連携、③：ITとOTの連携が重要】			用途レベル毎の推奨項目		
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.	①PoC又は 補助的	②基幹 ビジネス	③重要 ビジネス
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 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	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 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		■	■

▶ 異常とイベント（No.45）

：業務に支障をきたすような異常の定義と検知の方法を検討し、影響範囲を把握する。

▶ セキュリティの継続的なモニタリング（No.46, No.47）

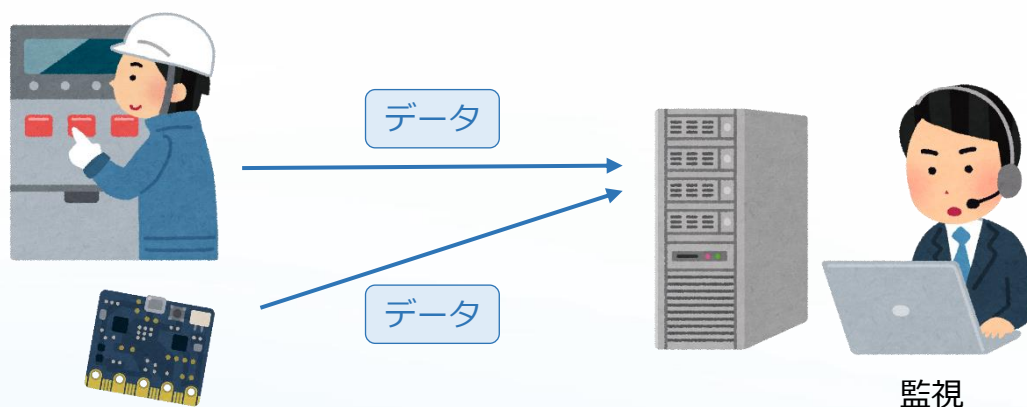
：IoT機器のログの監視や脆弱性スキャンなどにより、異常を監視・調査できるようにする。

▶ 検知プロセス（No.48）

：検知した異常を報告する体制を整備し、関係者で共有する。

継続的なモニタリング

(例) 生産装置やセンサーの状態監視をシステム的に行い、異常な値などを検知できるようにする。



これを実施しないと...

サイバー攻撃を受けたときに、気づくことが難しい。

攻撃者はなるべく痕跡を残さないように、「情報搾取」や「リモート操作」などの活動を行います。したがって、大量のデータから異常を検知する仕組みがないと、攻撃に気づくことすらできない。

チェック項目「対応」

- ① NIST-CSFの分類：異常時、5カテゴリー
 - (1)対応計画 (2)コミュニケーション (3)分析 (4)低減 (5)改善
- ② 企業のIoT推進者や管理者の視点で検討すべき点：9項目
- ③ IoT用途レベル毎の推奨項目：3つの重要度に分類
- 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
- ⑤ 検討主体（IT又はOT）及び、連携（ITとOT）が重要な項目を明記

NIST-CSF (Ver.1.1)		IoTセキュリティチェック項目【項目No.表示例 ①：ITが主体的にOTと連携、②：OTが主体的にITと連携、③：ITとOTの連携が重要】		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に変わる情報システム（クラウドを含む）		第一重要点 No.	③PoC又は補助的	②基幹 ビジネス	①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
対応 (RS)	対応計画 (RS.RP)	⑤IoT機器、IoTシステムのインシデントに対応する ①②③④⑤⑥⑦⑧⑨⑩⑪⑫⑬⑭⑮⑯⑰⑱⑲⑳㉑㉒㉓㉔㉕㉖㉗㉘㉙㉚㉛㉜㉝㉞㉟㊱㊲㊳㊴㊵㊶㊷㊸㊹㊺		■	■	■	■	
	コミュニケーション (RS.CO)	⑤IoT機器、IoTシステムのインシデントに対応する ①②③④⑤⑥⑦⑧⑨⑩⑪⑫⑬⑭⑮⑯⑰⑱⑲⑳㉑㉒㉓㉔㉕㉖㉗㉘㉙㉚㉛㉜㉝㉞㉟㊱㊲㊳㊴㊵㊶㊷㊸㊹㊺		■	■	■	■	
	分析 (RS.AN)	⑤IoT機器、IoTシステムのインシデントに対応する ①②③④⑤⑥⑦⑧⑨⑩⑪⑫⑬⑭⑮⑯⑰⑱⑲⑳㉑㉒㉓㉔㉕㉖㉗㉘㉙㉚㉛㉜㉝㉞㉟㊱㊲㊳㊴㊵㊶㊷㊸㊹㊺		■	■	■	■	
	低減 (RS.MI)	⑤IoT機器、IoTシステムのインシデントに対応する ①②③④⑤⑥⑦⑧⑨⑩⑪⑫⑬⑭⑮⑯⑰⑱⑲⑳㉑㉒㉓㉔㉕㉖㉗㉘㉙㉚㉛㉜㉝㉞㉟㊱㊲㊳㊴㊵㊶㊷㊸㊹㊺		■	■	■	■	
	改善 (RS.IM)	⑤IoT機器、IoTシステムのインシデントに対応する ①②③④⑤⑥⑦⑧⑨⑩⑪⑫⑬⑭⑮⑯⑰⑱⑲⑳㉑㉒㉓㉔㉕㉖㉗㉘㉙㉚㉛㉜㉝㉞㉟㊱㊲㊳㊴㊵㊶㊷㊸㊹㊺		■	■	■	■	

「対応」について

検知されたサイバーセキュリティのイベントに対処するための適切な対策を検討し、実施すること。

- ・「対応」機能は、発生する可能性のあるサイバーセキュリティインシデントがもたらす影響を封じ込めるのを支援する。
- ・「対応」機能の成果カテゴリーには、「対応計画の作成」「コミュニケーション」「分析」「低減」「改善」がある。

対応：対応計画・コミュニケーション

カテゴリー	IoTセキュリティチェック項目【項目No.表示例 ①：ITが主体的にOTと連携、②：OTが主体的にITと連携、③：ITとOTの連携が重要】		用途レベル毎の推奨項目		
	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.	①PoC又は補助的	②基幹ビジネス	③重要ビジネス
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/PSIRTと連携し報告範囲や内容を検討する	新規		■	■

▶ 対応計画（No.49）

：インシデントが発生したと考えられる場合、速やかに状況の把握し、対応手順を検討する。そして原因の対処を行い、被害拡大の防止に努める。その際、対応活動は全て記録しておく。

▶ コミュニケーション（No.50, No.51, No.52）

：必要な関係者に第一報を伝達する。また必要に応じて、メーカーのサポートに連絡する。また、社内にCSIRTやPSIRTが設立されているようなら協力を求める。

ケーススタディ 対応計画・コミュニケーション

迅速なコミュニケーション

(例) インシデント発生時の報告先を明らかにしておく。



これを実施しないと...

適切な対応が行えず、深刻な事態に発展しやすい。

インシデントが発生した際は、なるべく早い段階で処置を行うことが求められる。場当たり的な対応を行うと、返って被害が拡大することもあるので、適任者を報告先に構えさせておくことが望ましい。

対応：分析・低減・改善

IoTセキュリティチェック項目【項目No.表示例 ①：ITが主体的にOTと連携、②：OTが主体的にITと連携、③：ITとOTの連携が重要】		用途レベル毎の推奨項目			
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.	①PoC又は補助的	②基幹 ビジネス	③重要 ビジネス
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	新規		■	■
	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			■	■
	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		■	■	■
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	新規			■

▶ 分析 (No.53, No.54, No.55)

：ログやシステム通知などを調べて、異常を特定する。それに応じた対応方針も決定する。
対応方針を決める際は、IT担当者とOT担当者間の意識統一を図ろう。

▶ 低減 (No.56)

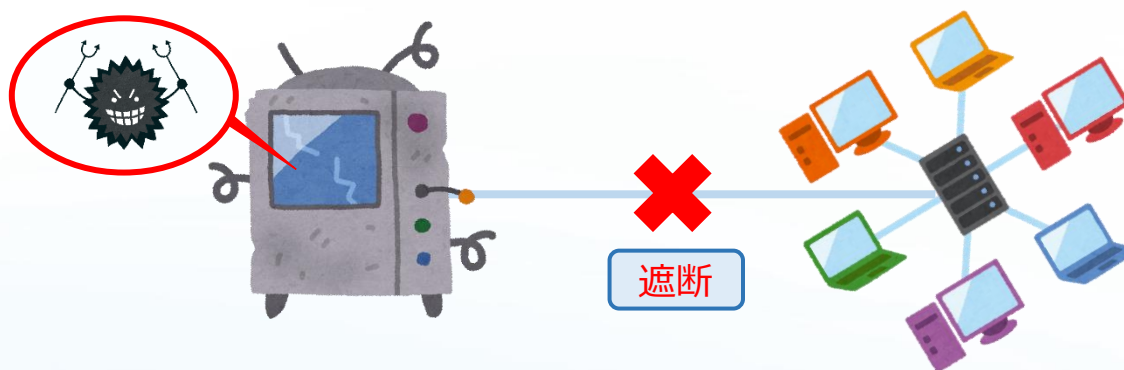
：マルウェア対策や脆弱性パッチを適用するなど、被害拡大の防止に努める。

▶ 改善 (No.57)

：インシデントが収束を向かえたら、再発防止策の取り組みを行う。

被害拡大の低減

(例) ネットワークを遮断しマルウェアの拡大を防止する。



これを実施しないと...

接続されている他の機器も、マルウェアに感染する。

自己増殖するマルウェアも多く、他の機器への感染活動も行います。

世界的にも話題となったランサムウェアはネットワークを通じて感染を拡大させました。

チェック項目「復旧」

- ① NIST-CSFの分類：異常時、3カテゴリー
(1)復旧計画 (2)改善 (3)コミュニケーション
- ② 企業のIoT推進者や管理者の視点で検討すべき点：3項目
- ③ IoT用途レベル毎の推奨項目：3つの重要度に分類（「①PoC又は補助的」はなし）
- 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
- ⑤ 検討主体（IT又はOT）及び、連携（ITとOT）が重要な項目を明記

NIST-CSF (Ver.1.1)		IoTセキュリティチェック項目【項目No.表示例 ①：ITが主体的にOTと連携、②：OTが主体的にITと連携、③：ITとOTの連携が重要】		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 要項 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
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）	8/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		新機		■	■	
	改善（RC.IM）	9/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 復旧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		新機		■	■	
	コミュニケーション（RC.CO）	10/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 関係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 ③ SIRT/PSIRTと連携しステークホルダーに報告する		新機			■	

「復旧」について

レジリエンス（回復力）を実現するための計画を策定・維持し、サイバーセキュリティイベントによって阻害されたあらゆる機能やサービスを元に戻すための適切な対策を検討し、実施すること。

- ・「復旧」機能は、サイバーセキュリティインシデントがもたらす影響を軽減するために、通常の運用状態へタイムリーに復旧するのを支援する。
- ・「復旧」機能の成果カテゴリーには、「復旧計画の作成」「改善」「コミュニケーション」がある。

復旧：復旧計画・改善・コミュニケーション

カテゴリー	IoTセキュリティチェック項目【項目No.表示例 ①：ITが主体的にOTと連携、②：OTが主体的にITと連携、③：ITとOTの連携が重要】 【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.	用途レベル毎の推奨項目		
			①PoC又は補助的	②基幹ビジネス	③重要ビジネス
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/PSIRTと連携しステークホルダーに報告する	新規			■

▶ 復旧計画 (No.58)

：インシデント収束後には、まずIoT機器やシステムを元の状態に復旧する。
その際、同じ原因で再びインシデントが発生しないように十分に配慮する。

▶ 改善 (No.59)

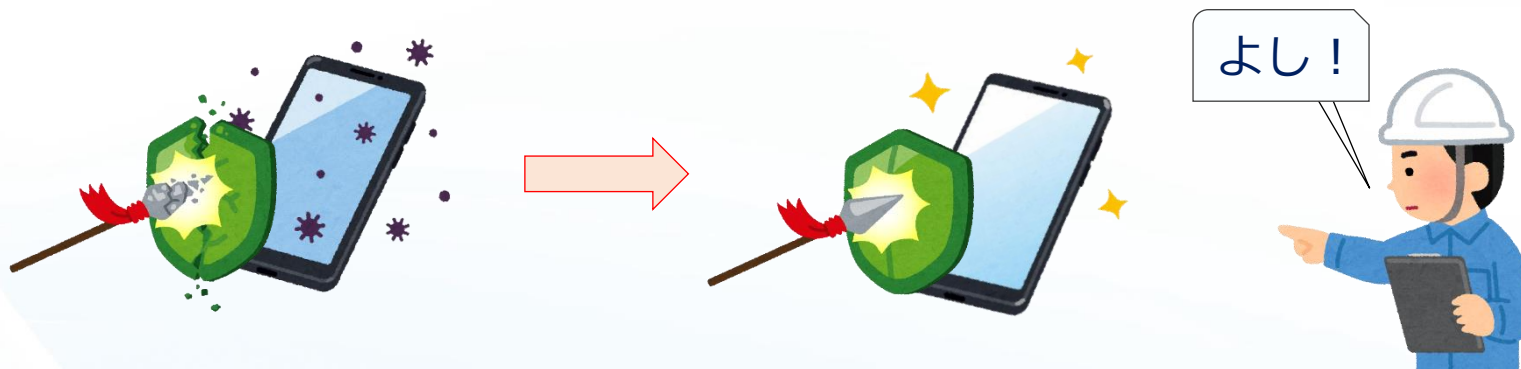
：復旧が完了したらインシデントから得た教訓を活かし、「復旧計画」や「手順」の見直し、「権限付与」など新たに必要と思われる事を追加する。

▶ コミュニケーション (No.60)

：必要な関係者にインシデント情報を通知する。

再発防止策の実施

(例) 脆弱性を突かれた機器とは、別の機器に同様の脆弱性が存在しないかを確認し、存在するようならその対策を実施する。



これを実施しないと...

別の機器を標的とした攻撃により、同様のインシデントが再び発生する。

標的型攻撃と呼ばれる攻撃では、組織は執拗に攻撃される。そのため別の端末に存在する脆弱性を確認して、そこから侵入されないなどの対策を施すことは再発防止につながる。

次回の紹介

■ IoTセキュリティチェックシート入門

- 次回は「IoTチェックシート活用」になります。
ぜひ次回の⑥をご覧ください、IoTセキュリティチェックシートを実際に活用してみましょう！

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。

次回の受講おまちしております。