JAPAN SMARTPHONE SECURITY ASSOCIATION

第3回

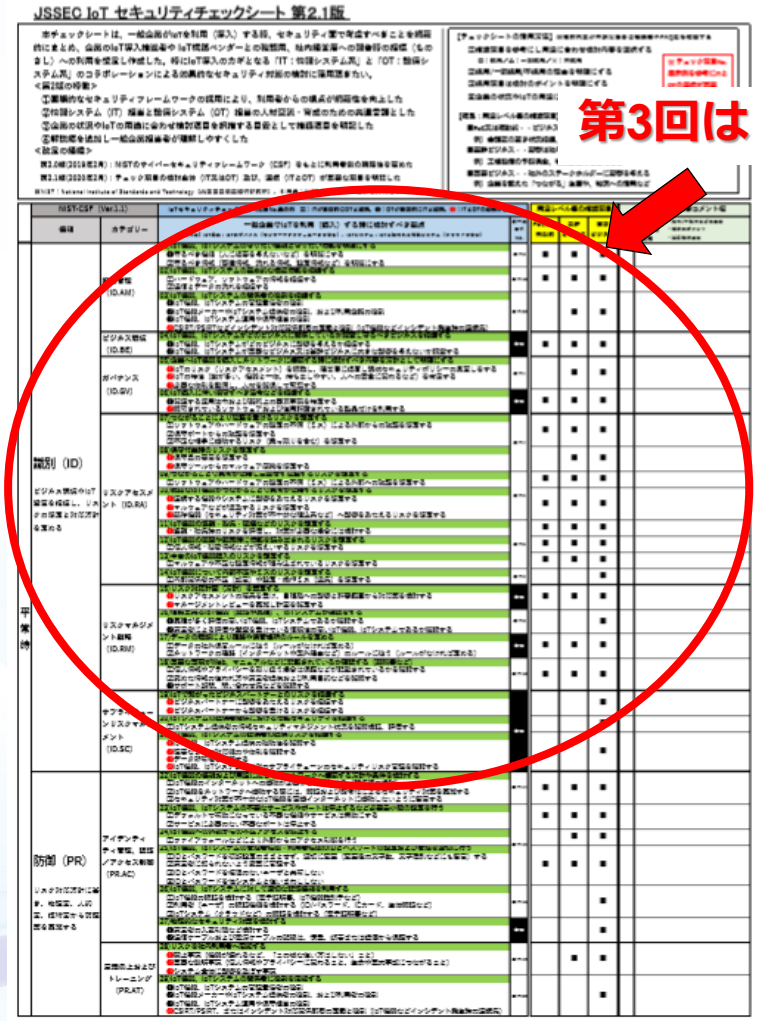
チェック項目「識別」の解説

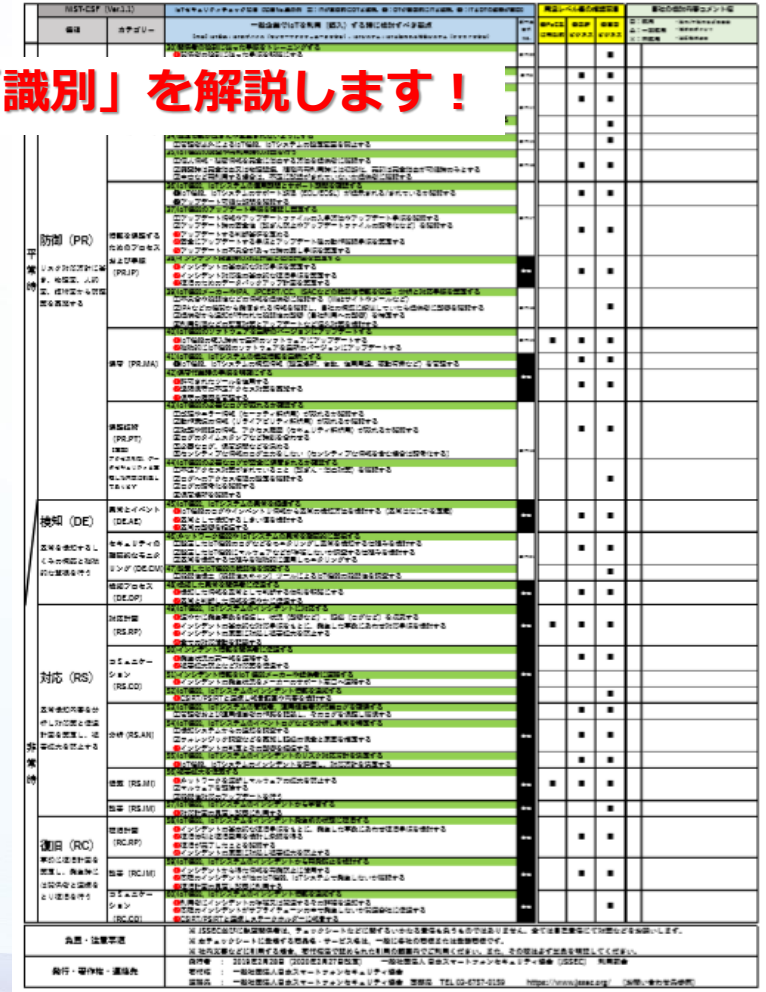
～ビジネス環境やIoT資産を把握し、リスクの想定と対応方針を定める～

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
三池 聖史（ユニアデックス株式会社）

IoTセキュリティチェックシート

JAPAN SMARTPHONE SECURITY ASSOCIATION





チェック項目「識別」

JAPAN SMARTPHONE SECURITY ASSOCIATION

❶NIST-CSF（米国国立標準技術研究所のサイバーセキュリティフレームワーク）の分類：平常時、6カテゴリー
(1)資産管理 (2)ビジネス環境 (3)ガバナンス (4)リスクアセスメント
(5)リスクマネジメント戦略 (6)サプライチェーンリスクマネジメント

❷企業のIoT推進者や管理者の視点で検討すべき点：21項目

❸IoT用途レベル毎の推奨項目：3つの重要度に分類

❹各社の検討内容 採用理由／追加項目：検討結果の見える化

❺検討主体（IT又はOT）及び、連携（ITとOT）が重要な項目を明記

❶ ❺ ❷ ❸ ❹

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、❶：OTが主体的にITと連携、❶：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）	第一版要点No.	PoC又は補助的	基幹ビジネス	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
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 ❶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 ❶IoT機器、IoTシステムの管理責任者の役割 ❷IoT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 ❸IoT機器、IoTシステム運用や保守担当の役割 ❹CSIRT/PSIRT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 ❶IoT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 ❷IoT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 ❶IoT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 ❷IoT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 ❸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 ❶関連する適用法令および契約上の要求事項を特定する ❷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	■	■	■	
		(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 ❶保守員の悪意を想定する ❷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		■	■	■	

識別について

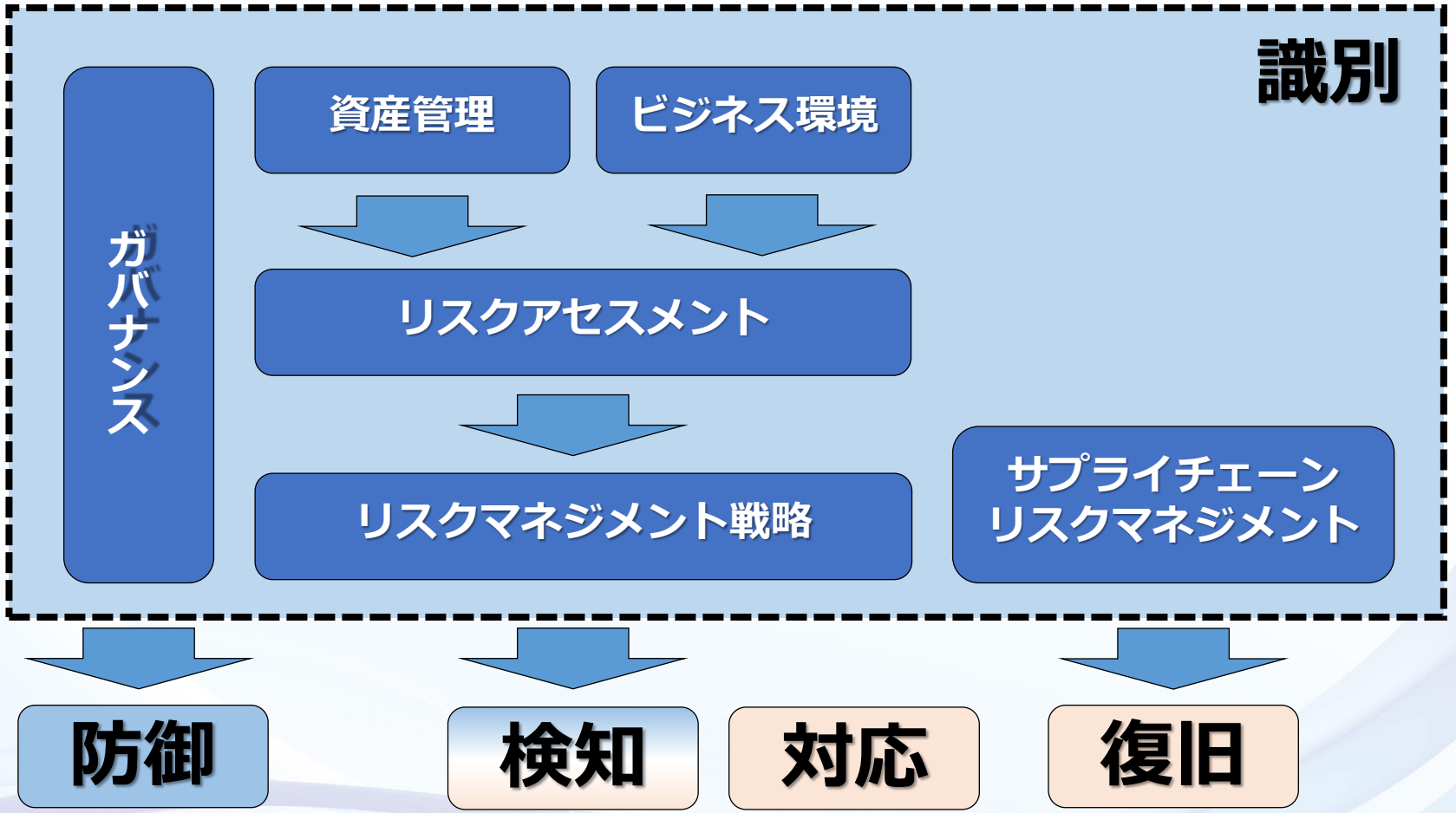
JAPAN SMARTPHONE SECURITY ASSOCIATION

■識別とは、
システム、資産、データ、機能、人員に対するセキュリティに関する
リスク管理を理解する

■このセッションの検討すべき項目は、チェックシートを効果的に
活用する上での基本となる

■自組織がセキュリティリスクを管理する上での優先順位付けが
できるようになります

識別のカテゴリー


識別
ガバナンス
資産管理
ビジネス環境
リスクアセスメント
リスクマネジメント戦略
サプライチェーン
リスクマネジメント
防御
検知
対応
復旧

資産管理

JAPAN SMARTPHONE SECURITY ASSOCIATION

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、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】 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.	用途レベル毎の推奨項目 PoC又は補助的	基幹ビジネス	重要ビジネス	自社の検討内容コメント欄 ◎：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
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					
❶守るべき機能（人に被害を与えないなど）を明確にする	要点3	■	■	■	
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					
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	要点18	■	■	■	
②通信とデータの流れを把握する					
03)IoT機器、IoTシステムの関係者の役割を把握する					
❶IoT機器、IoTシステムの管理責任者の役割					
❷IoT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	要点20		■	■	
❸IoT機器、IoTシステム運用や保守担当の役割					
❹CSIRT/PSIRT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）					

IoTシステム、IoT機器の・・・

■守るべき機能、守るべき情報を明確にする

■ソフトウェア、ハードウェア、データの流れを把握する

■管理責任者、提供者、利用者、運用/保守担当者、インシデント対応者の役割を把握する

⇒　資産の重要性に応じて管理する

ビジネス環境

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、❶：OTが主体的にITと連携、❶：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	
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.	PoC又は補助的	基幹ビジネス	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	
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	■	■	■		
❶IoT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						
❷IoT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						

IoTシステム、IoT機器が・・・

■影響を与えるビジネスを把握する

■他の重要なビジネス、基幹システムに影響を与えないか調査する

⇒　リスクマネジメントでの意思決定に使用される

ガバナンス

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、❶：OTが主体的にITと連携、❶：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	
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.	PoC又は補助的	基幹ビジネス	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	
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						
❶IoT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	要点1		■	■		
❷IoT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						
❸必要な体制を整備し、人材を確保して育成する						
06)IoT導入に伴い順守すべき法令などを把握する						
❶関連する適用法令および契約上の要求事項を特定する	新規	■	■	■		
❷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						

IoT導入に伴い・・・

■**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**
IoTの特性を考慮する

■**関連する適用法令、契約上の要求事項を特定し、認可されている**
ソフトウェア、使用許諾されている製品を利用する

⇒　**セキュリティポリシーを見直す**

リスクアセスメント

JAPAN SMARTPHONE SECURITY ASSOCIATION

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、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】 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.	用途レベル毎の推奨項目 PoC又は補助的	基幹ビジネス	重要ビジネス	自社の検討内容コメント欄 ◎：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
07)つながることにより攻撃を受けるリスクを想定する	要点4				
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					
❶保守員の悪意を想定する			■	■	
❷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	要点5	■	■	■	
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					
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					
❶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		■	■	■	
❷マルウェアなどが波及するリスクを想定する					
❸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	要点6	■	■	■	
❶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					
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	要点2			■	
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					

想定するリスクは・・・

- **ソフトウェア、ハードウェアの設定不備**
- **保守要員の悪意、保守ツールからのマルウェア感染**
- **脆弱なIoT機器が連携するシステム、既存のシステムへ及ぼす影響**
- **盗難、紛失、破壊**
- **破棄や転売による個人情報、機密情報の漏えい**
- **内部関係者の不正**

リスクマネジメント戦略

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、❶：OTが主体的にITと連携、❶：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
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.	PoC又は補助的	基幹ビジネス	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
15)リスク対応計画（方針）を策定する	新規	■	■	■	
❶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					
❷マネージメントレビューを実施し計画を確定する					
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			■	
❶実績が多く評価の高いIoT機器、IoTシステムであるか確認する					
❷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システムであるか確認する					
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	■	■	■	
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）					
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）	要点18	■	■	■	
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					
❸サポート期間、問い合わせ先などを確認する					

リスクアセスメントの結果を受けて・・・

■**リスク対応計画**を策定する

■IoT機器、システムの**実績**、**第三者による評価や監査**を確認する

■IoT機器、システムのマニュアルなどを確認する
- **個人情報やプライバシー保護**
- **情報の利用目的や第三者提供**
- **サポート期間や問合せ先**

サプライチェーンリスクマネジメント

JAPAN SMARTPHONE SECURITY ASSOCIATION

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、❶：OTが主体的にITと連携、❶：ITとOTの連携が重要】 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.	用途レベル毎の推奨項目 PoC又は補助的	基幹ビジネス	重要ビジネス	自社の検討内容コメント欄 ◎：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
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					
❶ビジネスパートナーに影響をあたえるリスクを把握する				■	
❷ビジネスパートナーから影響を受けるリスクを把握する					
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	新規				
21)IoT機器、IoTシステムの提供者の提供リスクを把握する					
❶IoT機器、IoTシステム提供の継続性を確認する					
❷障害などへの対応能力や体制を確認する				■	
❸データ所有権を確認する					
❹IoT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					

IoTで繋がったビジネスパートナーに対して・・・

■影響を**あたえるリスク**を把握する

IoTシステム提供者に対して・・・

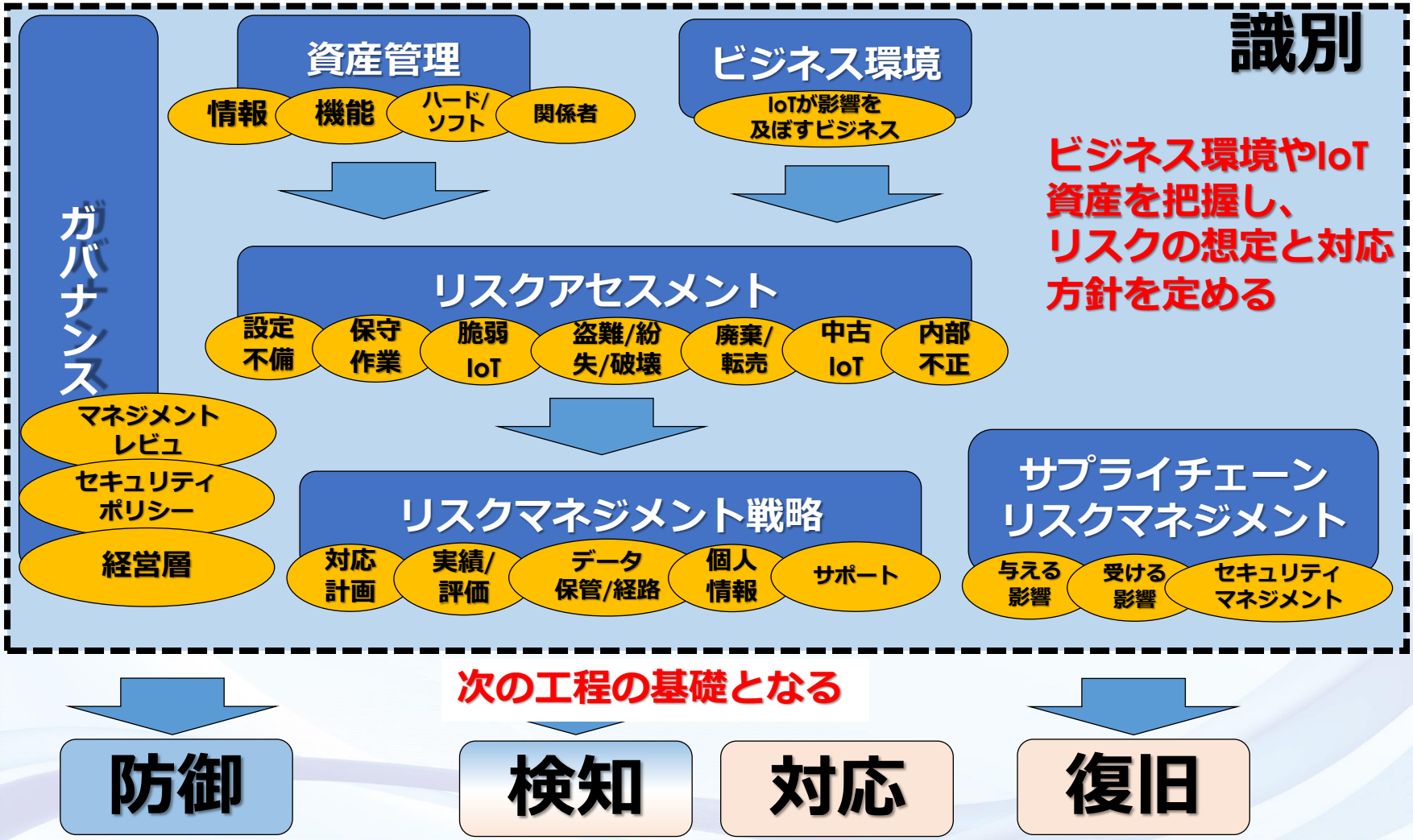
■**情報セキュリティマネジメント状況**を確認、評価する

■IoT機器、IoTシステム提供の**継続性**を確認する

■障害などへの**対応能力**や**体制**を確認する

■**データ所有権**を確認する

識別のまとめ


識別
ガバナンス
マネジメントレビュ
セキュリティポリシー
経営層
資産管理
情報
機能
ハード/ソフト
関係者
ビジネス環境
IoTが影響を及ぼすビジネス
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
リスクアセスメント
設定不備
保守作業
脆弱IoT
盗難/紛失/破壊
廃棄/転売
中古IoT
内部不正
リスクマネジメント戦略
対応計画
実績/評価
データ保管/経路
個人情報
サポート
サプライチェーンリスクマネジメント
与える影響
受ける影響
セキュリティマネジメント
次の工程の基礎となる
防御
検知
対応
復旧

次回の紹介

JAPAN SMARTPHONE SECURITY ASSOCIATION

■IoTセキュリティチェックシート入門

■次回はチェック項目「防御」になります。

④防御（各項目の概要）

■防御はIoTシステム／サービスの提供を確実にするための適切な保護対策を検討し、実施します。

■発生する可能性のあるセキュリティイベントがもたらす影響を抑制するのを支援します。

次回の受講おまちしております。