資料 3

HITACHI
Inspire the Next

2025/3/ 4

工場におけるサイバーセキュリティガバナンスについて

（株）　日立製作所　制御プラットフォーム統括本部　セキュリティエバンジェリスト
国立大学法人　名古屋工業大学　客員教授

中野利彦

講師紹介

氏名：中野利彦　博士（工学）

所属：（株）日立製作所の制御プラットフォーム統括本部　セキュリティエバンジェリスト
　　国立大学法人　名古屋工業大学　社会工学類　客員教授

業務履歴：　制御システム向けのミドルウェアやツールの開発、技術サポート
　　制御システムおよび情報システムに関連するセキュリティエンジニアリング
現在：　制御システムセキュリティに関するコンサルテーション及び講師
　　IPA　ICSCoEでのビジネスマネージメント、BCP/BCM講師

主な委員
政府

2010年～2011年	経済産業省サイバーセキュリティと経済研究会特別委員
2010年～2012年	経済産業省制御システム情報セキュリティ研究会委員
2012年～2013年	経済産業省制御システムセキュリティ検討タスクフォース委員
2013年～	経済産業省情報マネジメントシステム適合性評価制度の委員会委員
2013年～2014年	経済産業省次世代電力システムに関する電力保安調査委員会
2018年～	経済産業省産業サイバーセキュリティ研究会WG1 ビルサブワーキンググループ委員　工場サブワーキンググループ委員

政府関連団体

2012年～2018年	技術研究組合制御システムセキュリティセンター運営委員研究開発委員長
2014年～	一般財団法人日本情報経済社会推進協会（JIPDEC）　制御システムＳＭＳ技術分科会委員長
2015年～	一般社団法人日本経済団体連合会サイバーセキュリティ委員会　サイバーセキュリティ強化WG委員
2015年～	日本電気協会情報専門部会委員（電力制御システムセキュリティガイドライン、スマートメータセキュリティガイドライン制定）
2018年～	スマートメータセキュリティ監査制度運営委員会委員

サイバーセキュリティ範囲について

工場の現場へのセキュリティ展開のポイント

HITACHI
Inspire the Next

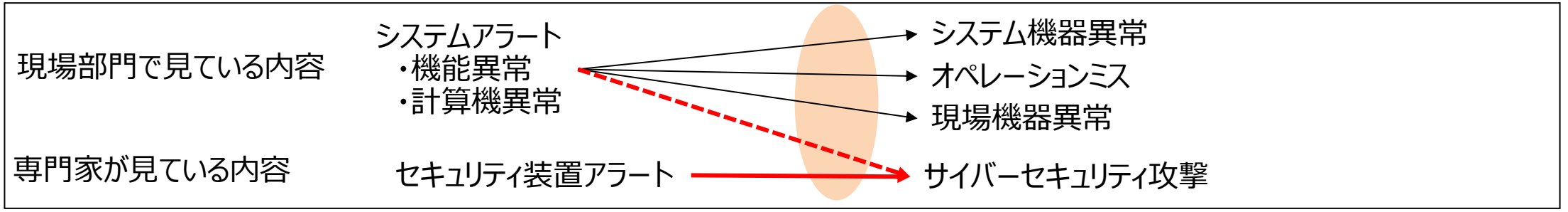
2つの融合：セイフティ、現場業務

◆セイフティ（安全）とセキュリティの融合

区分	安全（セイフティ）	[IT/OT]セキュリティ
定義	**許容できないリスクがないこと** （ISO/IEC GUIDE 51:2014）	**人為的な攻撃から[IT/OT]システムを保護すること** （ISO/IEC27000、ISO/IEC62443など）
例	・労働災害からの保護（感電事故防止、転落防止） ・自然災害からの保護（台風による破損防止）	・情報漏洩による信頼失墜 ・システム攻撃による業務停止
特徴	災害をある程度類型化が可能（台風、地震…） 過去の実例の蓄積し、活用できる範囲が大きい	攻撃方法が絶えず進化 攻撃対象（IT機器、ソフトウェアなど）も絶えず変化
対策	発生する可能性がある災害を**整理**し対策 ・内容　・影響度　・頻度	攻撃対象ごとに攻撃される可能性を**推定**し対策 ・攻撃対象　・狙われるところ　・攻撃方法

◆現場業務（故障対応等）とセキュリティ業務（検知、対応）の融合

従来の要因による異常と、セキュリティ攻撃による異常を複合的に判断



セキュリティガバナンスの領域

HITACHI
Inspire the Next

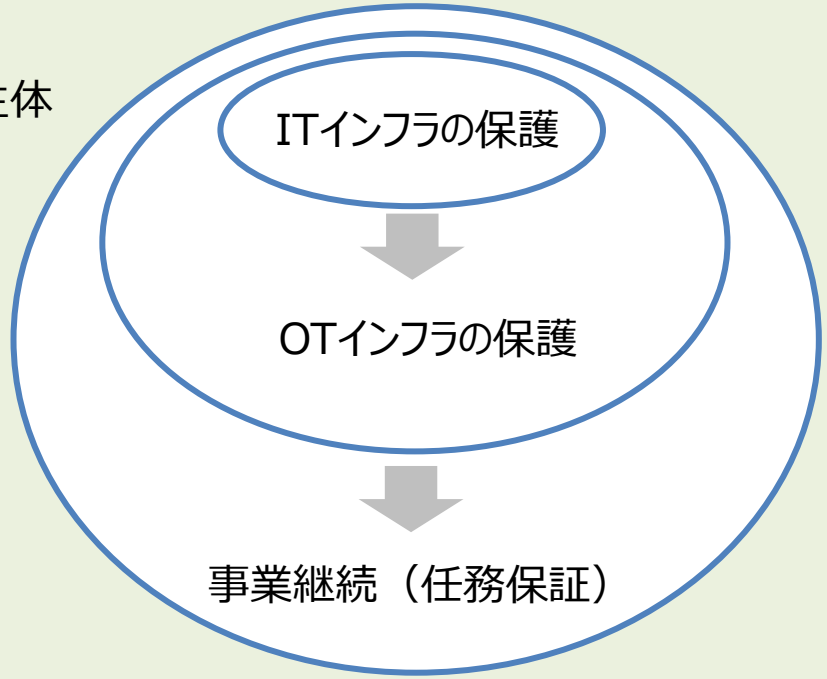
変化するサイバーセキュリティのガバナンス領域

組織のガバナンス

情報システム部門主体

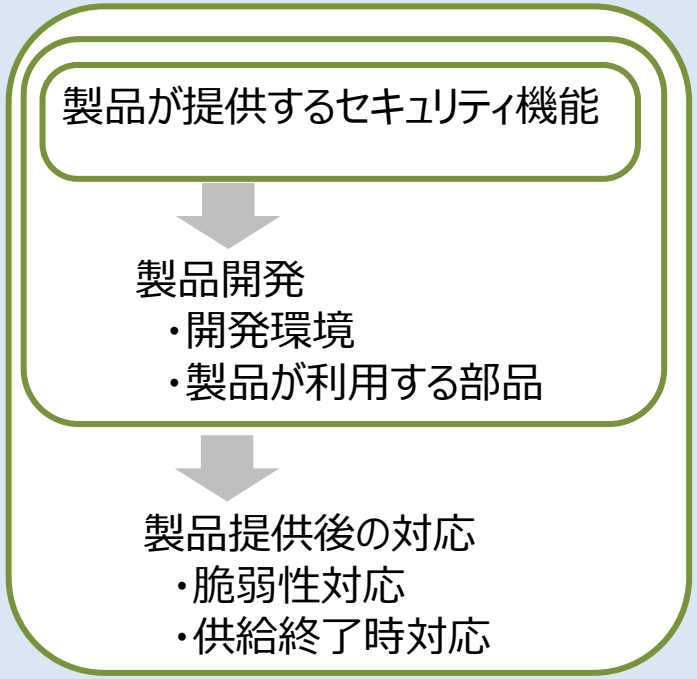
現場部門主体

経営部門主体



事業者 → グループ会社 → 取引先

製品のガバナンス



製品仕様

開発プロセス

製品ライフサイクル全般

個別製品担当 → 製品部署 → 全社

組織のガバナンス：NIST CSF V2.0

HITACHI
Inspire the Next

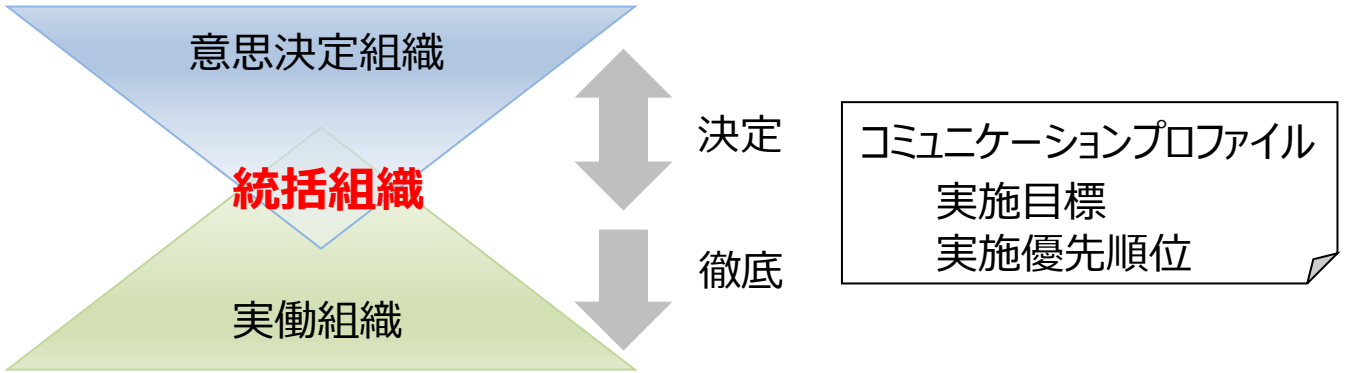
より組織的な統制を考慮した内容に改定

変更ポイント

- フレームワークの適応範囲の拡大あらゆる規模の組織に適用
- 新たに「統治（Govern）」という区分が追加（分散して記載されていたものを集約）
- サプライチェーンリスクマネジメントの強化
- コミュニティプロファイル（決定内容の徹底とフィードバック）の追加

	統治（Govern）
事前	特定（Identify）
	防御（Protect）
運用	検知（Detect）
	対応（Respond）
	復旧（Recover）

コミュニケーションフレームワーク（説明者アレンジ）



組織のガバナンス：企業のサイバー攻撃対策評価制度

外部から各企業のセキュリティ対策状況を判断することが難しい
⇒満たすべき各企業の対策を 業界間の互換性を確保しながら対策状況を可視化する仕組みを検討

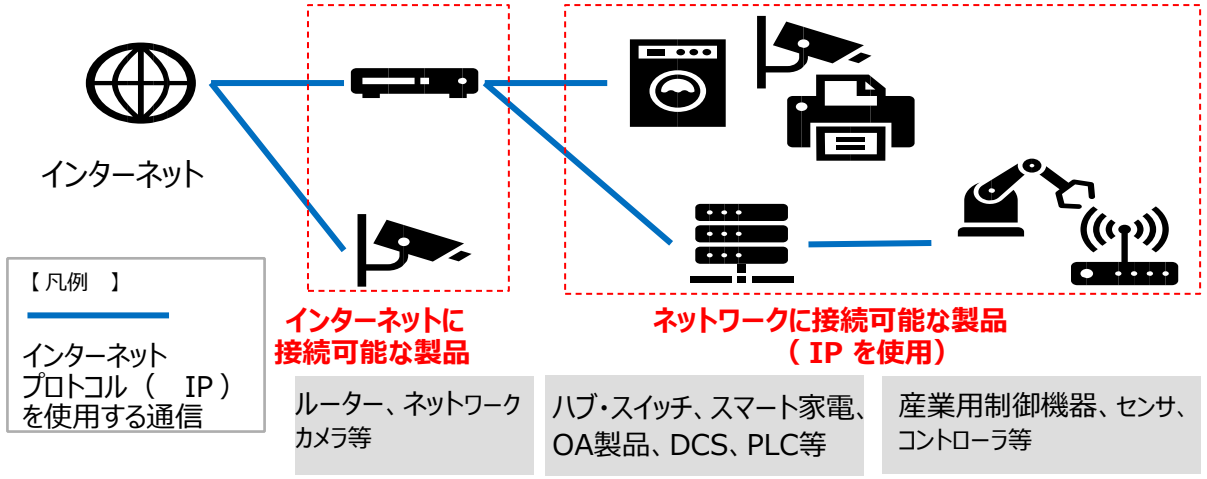
	三つ星（★3）	四つ星（★4）	五つ星（★5）
	・ ビジネス観点（データ保護、事業継続）及びシステム観点で取引先を評価し、重要度に応じて★3/4/5に区分		
(1) 対象事業者のイメージ	・原則としてサプライチェーンを形成するすべての者	・ビジネス観点：重要度中　または ・システム観点：接続あり	・ビジネス観点：重要度大
(2) 対策の適用範囲（組織、システム）	・組織的対策 ・システム的対策（自社IT基盤）	・組織的対策 ・システム的対策（自社IT基盤に加えて、発注者内部NWへの接続点）	追加の組織的対策は無し（★４取得が前提） ・システム的対策（自社IT基盤への高度な対策上乗せ、OT等業務システムへの対策の追加）
	・ NISTサイバーセキュリティフレームワーク2.0の６分類に、サプライチェーン対策である「取引先管理」を加えた７分類で検討		
(3) 対策の基本的な考え方	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策として、基礎的な組織的対策とシステム防御策を中心に構成	上記に該当する企業等が、標準的に目指すべきセキュリティ対策として、ガバナンスからシステム防御・検知、インシデント対応等包括的な対策にて構成	上記に該当する企業等が、高度なサイバー攻撃への対処を念頭に目指すべきセキュリティ対策として、侵入の早期検知と被害の極小化などシステムに対するより高度な対策にて構成
(4) 評価スキームの考え方 (5) 取得のターゲット（目標）費用		※既存のガイドラインや認証制度など活用可能なスキームを検討 （次回以降提示）	

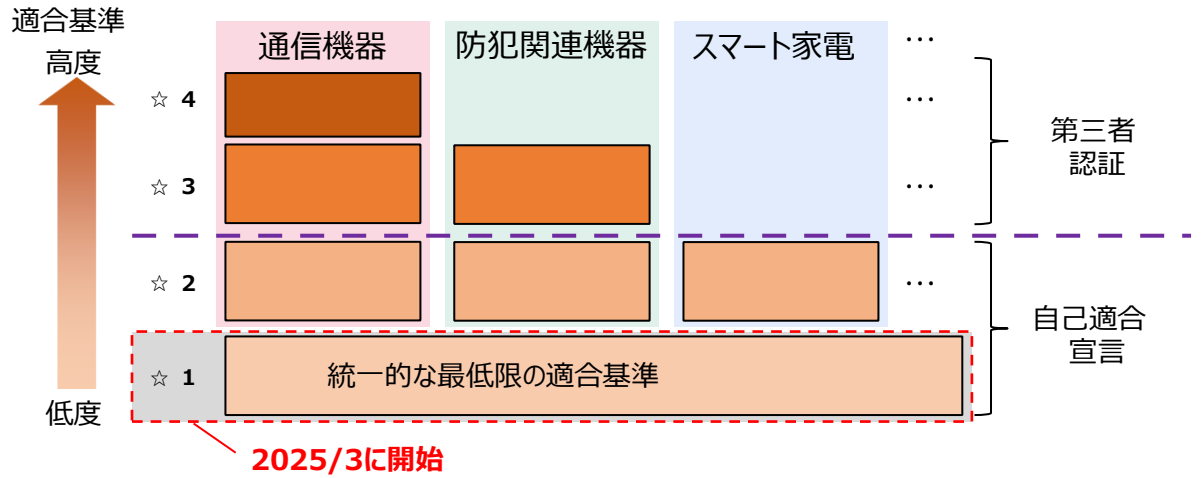
産業サイバーセキュリティ研究会WG1サプライチェーン強化に向けたセキュリティ対策評価制度に関するSWG[サプライチェーン強化に向けたセキュリティ対策評価制度の構築について]から抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/pdf/001_05_00.pdf

製品のガバナンス：IoT製品に対するセキュリティ適合性評価制度（JC-STAR）

HITACHI
Inspire the Next

対象
インターネットに直接接続されない製品も含め、インターネットプロトコルを使用する通信機能を持つIoT製品
消費者向け、企業・産業向けを問わず対象





米国：U.S. Cyber Trust Markを実施
欧州：CRAが2027年から実施

JC-STAR：Labeling Scheme based on Japan Cyber-Security Technical Assessment セキュリティ要件適合評価及びラベリング制度）

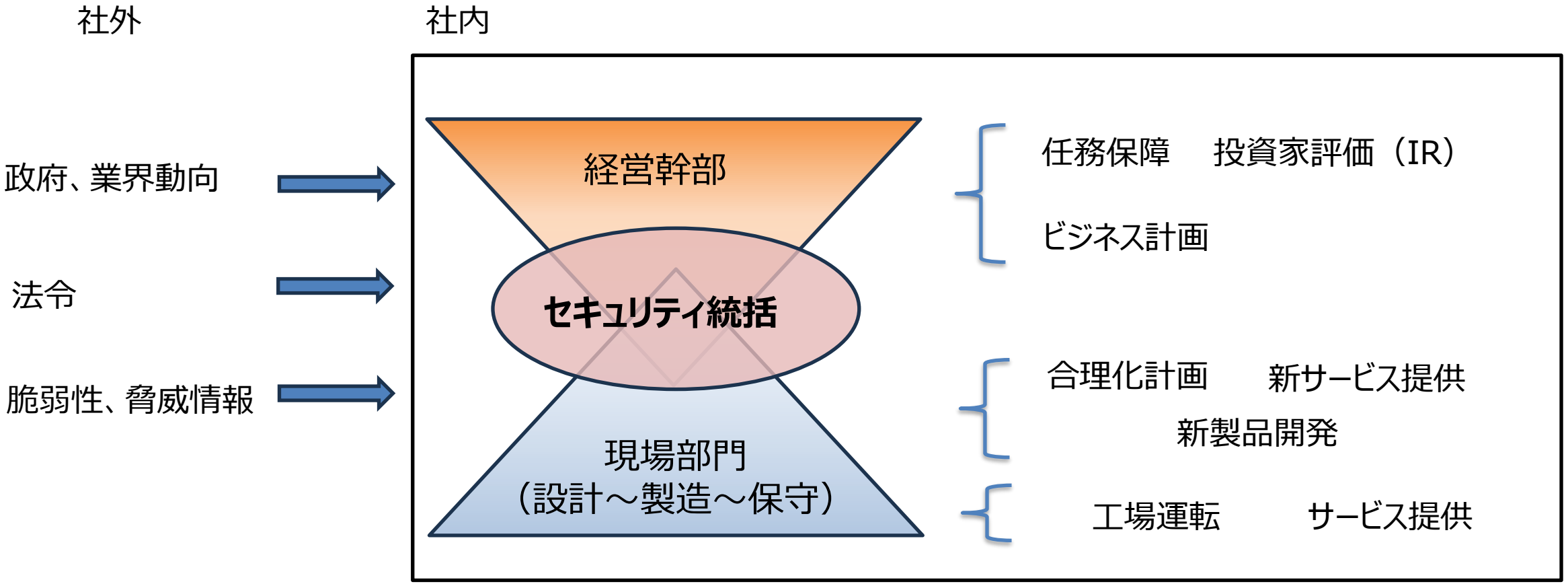
IPA JC-STAR制度説明資料から抜粋：https://www.ipa.go.jp/security/jc-star/material.html

組織のガバナンス

セキュリティ統括組織の位置づけ

HITACHI
Inspire the Next

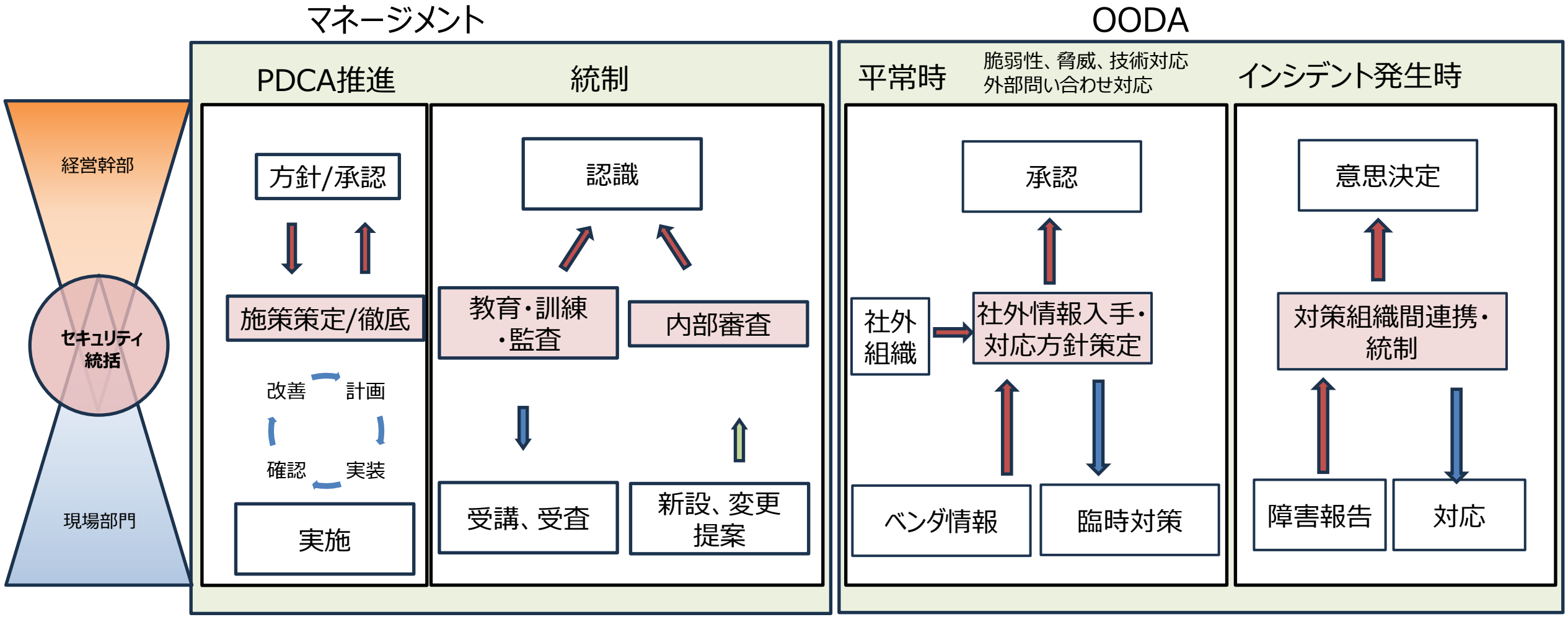
現場を含めた組織全体の「セキュリティ統括を担う」組織が不可欠



9

組織のガバナンス

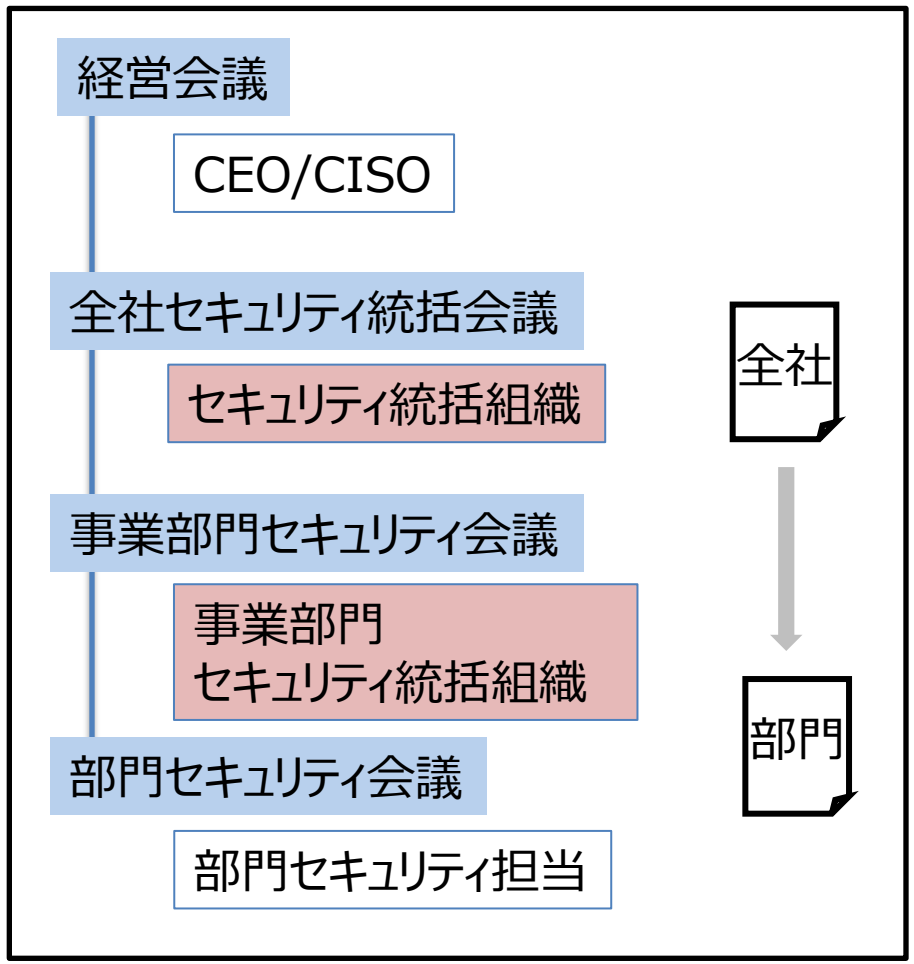
主な内容は下記を組織全体で円滑に
・サイバーセキュリティのマネージメントプロセス（PDCA） &統制（徹底）
・平時の予防保全、インシデント発生時の対応（OODA）



何を整備すべきか？

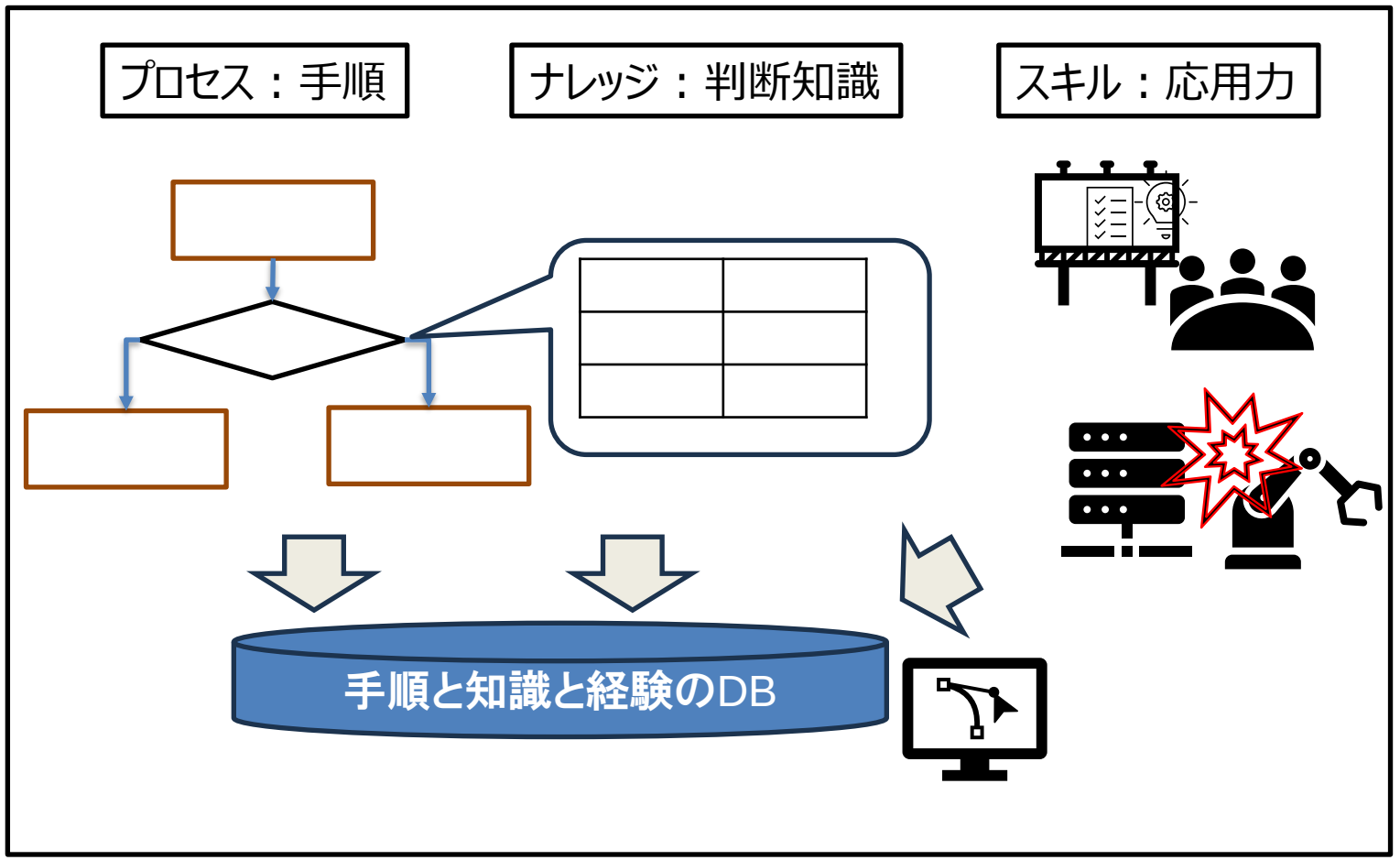
マネージメント

・ガバナンス体制の確立
・統一基準/ルール（規則）の整備



OODA（Observe（観察）・Orient（判断）・Decide（決定）・Act（実行））

活動コンピテンシー（活動能力）の確保
・プロセスとナレッジの整備、蓄積
・個々人、組織のスキル（応用力）向上



施策の策定

HITACHI
Inspire the Next

検討手順

ステップ1 → ステップ２ → ステップ３

内外要件（経営層の取組や法令等）や業務、保護対象等の整理

ステップ1-1

セキュリティ対策検討・企画に必要な要件の整理

（１）外部要件の整理

（２）内部要件／状況の把握

ステップ1-2 業務の重要度の設定

ステップ1-3 保護対象の重要度の設定

ステップ1-4 PDCA,ガバナンス体制の確認

ステップ1-5 OODA状況の確認

セキュリティ対策の立案

ステップ2-1 セキュリティ対策方針の策定

ステップ2-2

外部要件および想定脅威に対するセキュリティ対策立案

（１）ガバナンス、PDCA

- 組織体制、権限
- 統制ルール
- システム構成

（２）OODA

- 組織体制、権限
- 訓練

ステップ2-3　整備計画

- 組織、規定
- システム、運用
- サプリチェーン契約（条項、監査）

セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

ライフサイクルでの対策サプライチェーンを考慮した対策

(1)ライフサイクルでの対策

①運用・管理面のセキュリティ対策

A)サイバー攻撃の早期認識と対処（OODAプロセス）

B)セキュリティ管理(ID/PW管理、機器の設定変更など)

C)情報共有

②維持・改善面のセキュリティ対策

- セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
- 組織・人材のスキル向上（教育、模擬訓練等

(2) サプライチェーン対策

- 取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」をベースに講師が一部変更

組織としてのガバナンス例

HITACHI
Inspire the Next

CSF V2 サプライチェーン

区分		内容
SC-1	策定	• リスク管理プログラム（計画、ポリシー、手順）策定と合意 • 連携方法の確立
SC-2	徹底	• 役割と責任を文書化 • 目標の設定と定期的な実施評価 • 情報共有の方策を規定
SC-3	全体リスク管理との統合	• サイバーセキュリティリスク管理とサプライチェーンセキュリティリスク管理との融合
SC-4	優先順位付け	• サプライヤーの重要度の設定 • 重要度に基づく優先順位付
SC-5	契約条項定義	• 重要度に応じたセキュリティ要件の設定 • 要件と検証方法の契約 • 下層サプライヤとの情報共有の方策を規定 • リスクが顕在化された場合のための要件を規定 • SLAでセキュリティ要件の定義と監視 • 契約期間中のセキュリティ情報の開示 • 最新の製品（バージョン）の提供 • サプライヤー従業員の守秘義務 • セキュリティ実施の証拠の提供義務付け • サプライヤーの権利と責任の明記
SC-6	事前評価	• 事前のデューデリ、リスク管理の事前評価
SC-7	対象品のリスク管理・評価	• 第三者の評価 • 重要なサプライヤはライフサイクル全体での評価
SC-8	インシデント対応への組み込み	• 対応と復旧活動連携のための方策を規定 • 訓練と共有
SC-9	全体実施策でのサプライチェン施策の実施と監視	• 履歴管理と正しさの確認 • メンテナンスに不正がない
SC-10	契約終了後のリスク管理	• 終了時の要件を明確化

制定が必要な施策

規則規程
- 統合リスク管理規程
- 組織間の連携方法規程
- 組織評価と統制方法規程

評価
- 統合リスク評価と管理（サプライヤ、事業継続）
- 組織の評価と管理

要件規定
- 徹底の要件
  - ・事業継続視点
  - ：

検証
- 組織検証（監査、認証の活用）
- 製品・サービス検証（認証の活用）

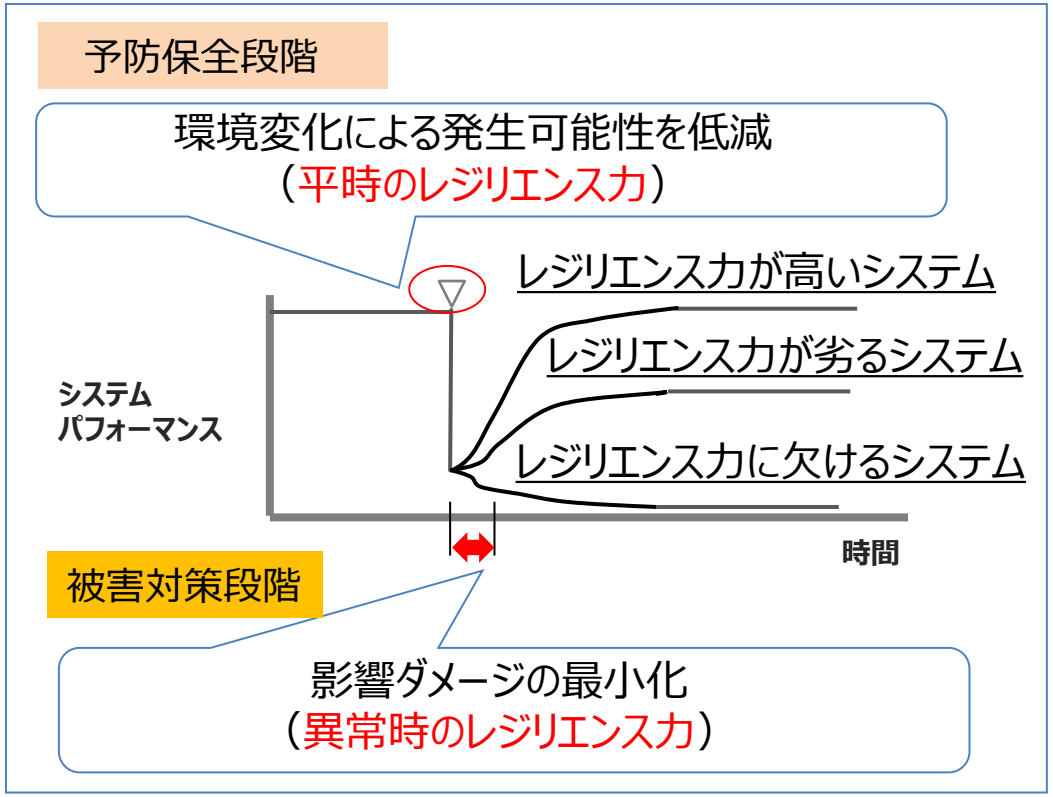
契約終了後
- クロージング

OODA検討例

HITACHI
Inspire the Next

レジリエンスが高いシステムの実現

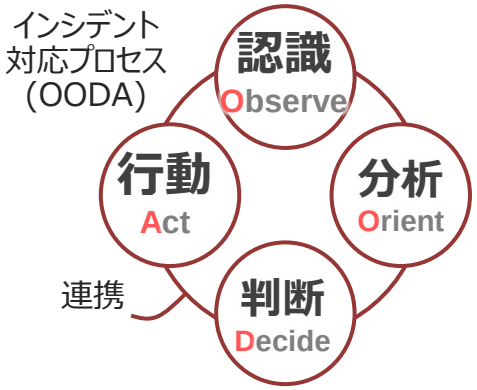
セキュリティ関連異常の早期発見、的確な対応

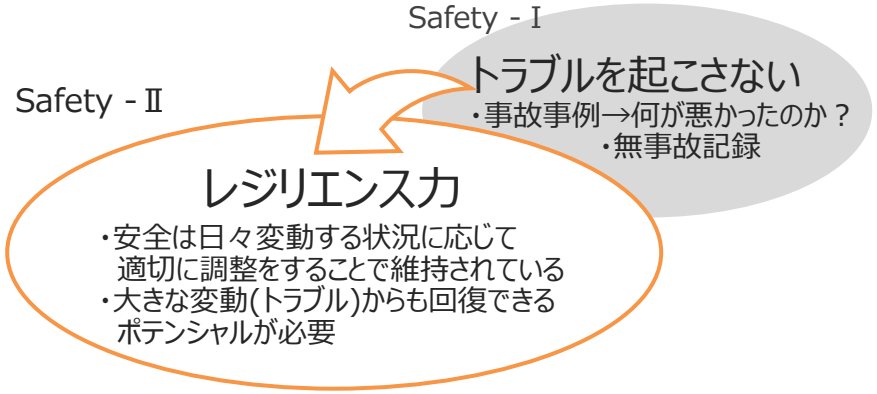


区分		活用例
予防保全	Observe　観察	関連する脆弱性、攻撃情報の収集
	Orient　分析	関連するアセットの導出、業務影響度の創出
	Decide　決定	連絡情報の生成
	Act　行動	進捗状況の管理支援
被害対策	Observe　観察	異常兆候の導出
	Orient　分析	障害との切り分け、関連する情報の提示
	Decide　決定	対応策の影響度生成、連絡情報の生成
	Act　行動	進捗状況の管理

セキュリティを意識した運用に何が必要か

レジリエンス実現に必要なスキル





プロセス（ルール）

インシデント対応のいち場面において人・組織は何をしている？
または何をしなくてはいけない？

- 認識：発生事象の認識する手順を理解している
- 分析：仮説の有効性を確認する手順を理解している
- 判断：意思決定する手順を理解をしている
- 行動：判断に従って実行する手順を理解している
- 連携：各プロセスが円滑に機能するために連携する手順を理解している

ポテンシャル（知識）

その時回復に向かうために必要な知識・ポテンシャルは？

- 基本：プロセスを実施するために必要な知識がある
- 適用：対処する知識を持ち的確に知識を適用できる
- 予見：発生事象から新たな知識を想像する
- 学習：事例をベースに応用可能な形で記憶

スキル（解決力）

それは具体的に何が出来れば発揮されたといえるか？
または発揮するためには何が必要か？

テクニカルスキル：
人として専門的な知識や技術、技能を活用

(例)
システム異常を即座に発見適切な封じ込め策を判断した

ノンテクニカルスキル：
組織として人と人の関係性を重視したスキル

(例)
齟齬なく情報が伝わった
リーダーシップが発揮された
リソースを的確に割り振った

セキュリティを意識した運用に何が必要か

HITACHI
Inspire the Next

計画的な技術・スキルと組織活動能力をベースにした成熟度（より高度な対応力）の向上訓練（演習）

組織＼技術・スキル	基本	応用	実践
社内外組織連携	**・社内外組織での確認** -BCP(総務ほか)組織との連携確認 -社外組織との連携確認	**・実践的なインシデントを想定し社内外組織での対応確認** -BCP組織とのやり取り内容確認 -社内外組織とのやり取り内容確認	**・高度インシデント（未知な、複合）のでの社内外組織での対応確認** -高度事象による対応
関連部署連携	**・社内組織間での確認** -サイバーセキュリティ組織の確認 -手順の確認	**・実践的なインシデントを想定し複数組織での対応確認** -複数組織での有機的連携 ・情報連携　・行動連携	**・高度インシデント（未知な、複合）の複数組織間での対応確認** -高度事象による対応
当該組織内	**・基本の確認** -インシデントの体感 -手順の確認 -ツールの理解 -セキュリティ基礎	**・実インシデントを想定した行動確認** -各プロセスでの知識活用 -ツールの活用 -チームでの行動確認	**・高度インシデント（未知な、複合）の対応確認** -知識応用 -プロセス応用 -ツール連携

製品のガバナンス

IoT製品に対するセキュリティ適合性評価制度

HITACHI
Inspire the Next

国名	制度名	概要
日本	IoTセキュリティ適合性評価制度	2025年3月から登録開始。 IoT機器のセキュリティ基準を満たすことを求める認証制度。
EU	EUサイバーセキュリティ認証制度（EUCC）	2024年2月に公布。 デジタル製品・サービスのサイバーセキュリティ認証制度。
	EUサイバーレジリエンス法（EU CRA）	2027年から適用開始。 デジタル製品のライフサイクル全体にわたってサイバーセキュリティの必須要件を認証。
アメリカ	U.S. Cyber Trust Mark	2021年5月の大統領令に基づき、IoT機器のセキュリティ基準とラベル制度を推進。 2024年度中にCybersecurity Labeling Programを開始予定。
イギリス	PSTI法（製品セキュリティおよび通信インフラストラクチャー規制法）	2024年4月29日に施行。 デフォルトパスワードの禁止やセキュリティアップデート提供期間の明示などを義務付け。
シンガポール	Cybersecurity Labelling Scheme (CLS)	2020年10月制度開始。 消費者向けIoT機器に対する任意のセキュリティラベリング制度。 ドイツ、フィンランドの類似制度と相互承認。

経済産業省　ワーキンググループ３（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会資料を参考に作成）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html

IoT製品に対するセキュリティ適合性評価制度（JC-STAR）

HITACHI
Inspire the Next

具備要件（Star 1 より報告者が抜粋）

区分	内容
認証	・パスワード強度のチェック ・セキュアな認証 ・認証ミス回数の制限
脆弱性対策	・優先度方針の文書化とポリシーの開示 ・脆弱性対策の実施 ・アップデートを可能に
インタフェース	・不要なインタフェースの削除
データ保護	・保持データの保護 ・伝送データの保護 ・情報の削除機能具備
レジリエンス	・復電、ネットワーク復旧時の設定維持
製品情報開示	・型式 ・免責、サポート期限、廃棄時のリスク

製品に対するセキュリティ適合性評価制度（EU　CRA）

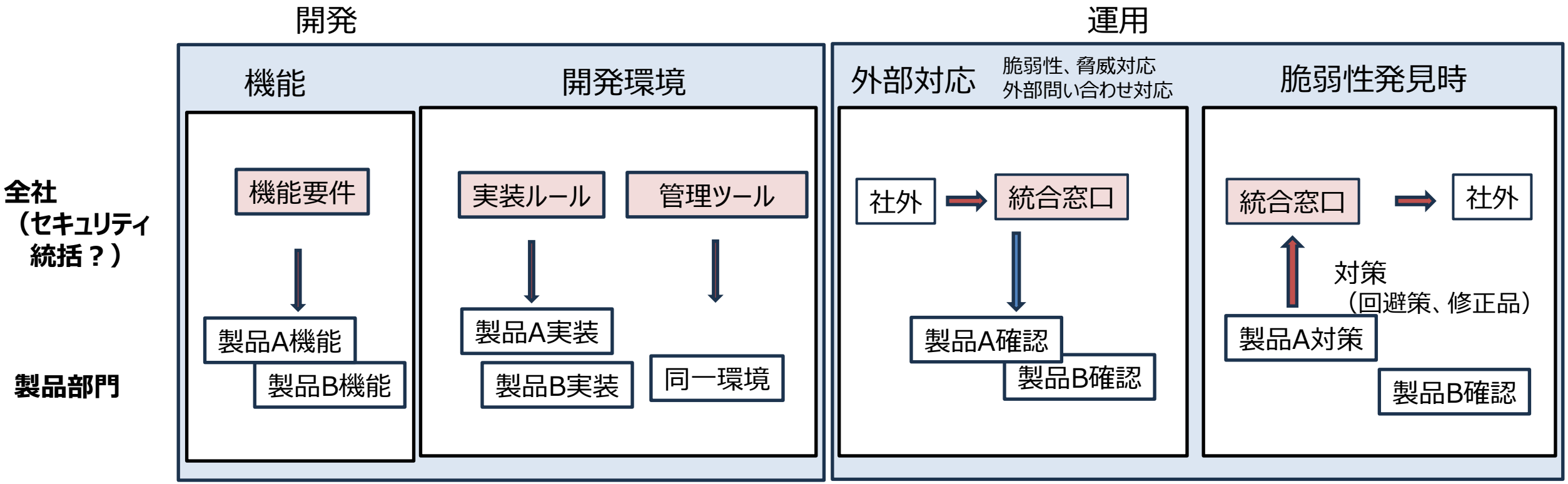
HITACHI
Inspire the Next

利用者が脆弱性対応を円滑に行うためにライフサイクル全般を統制（報告者が抜粋）

区分	内容
リスクアセスメント	・アセスメント手順 ・結果と対応策　　等
製品セキュリティ機能	・アクセス管理 ・通信：不正通信、暗号化　　等
開発プロセス	・設計～製作～検証 ・構成管理　　等
製品情報掲示	・SBoMでの情報提示 ・型式、連絡先 ・サポート時期　　等
脆弱性対応	・ポリシー ・手順　　等
インシデント対応	・EU連絡 ・情報、対策開示期限　等

製品のガバナンス

主な内容は下記を組織全体で円滑に
・製品に対するセキュリティ認証が進展
・製品のセキュリティ機能以外にも開発環境や問い合わせ対応が要件に
・EU　CRAではペナルティが、全社売上ベースで高額（５００万～１５００万ユーロ、全世界の年間総売上高の１%～2.5%）



HITACHI
Inspire the Next

まとめ

まとめ

組織ガバナンス
セキュリティの範囲は、従来のIT保護の視点から、事業継続の視点への拡大
・ガバナンスのためには、全社横断のセキュリティ統括組織が不可欠
・幹部から現場まで意思疎通できる枠組みが必要
現場の思い（HSEやSQDC）との融合
・統一されたポリシー～手順書までが不可欠
・計画的なスキル向上を目指した訓練が不可欠

製品ガバナンス
認証に向けてガバナンスの重要性が向上
・製品ライフサイクルを企業全体としてのガバナンスが不可欠
・製品内のソフトウェア構成（利用）部品の管理（サプリチェーン）
・脆弱性情報の組織的管理（取得、分析、発信）

HSE：IEC 62443**での評価軸：**Health , Safety , Environment
SQDC：Safety , Quality , Delivery , Cost

HITACHI

Inspire the Next