修士論文審査会

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

製造業のOT/FAにおいて情報セキュリティガバナンスを強化するために経営層が確認すべき重要事項の提案

2023年2月18日

後藤研究室　博士前期課程 2年
5508502　梅田真子

目次

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

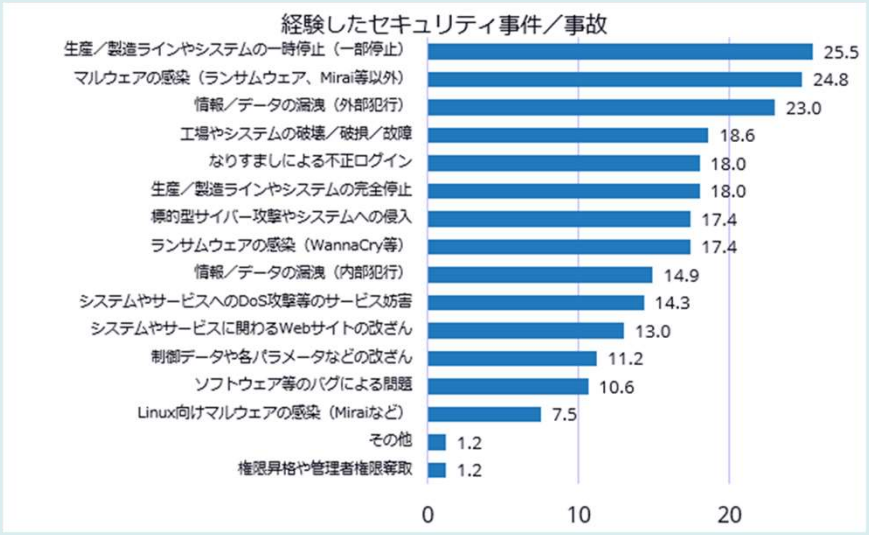
1. 研究の背景・動機

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 研究の背景・動機

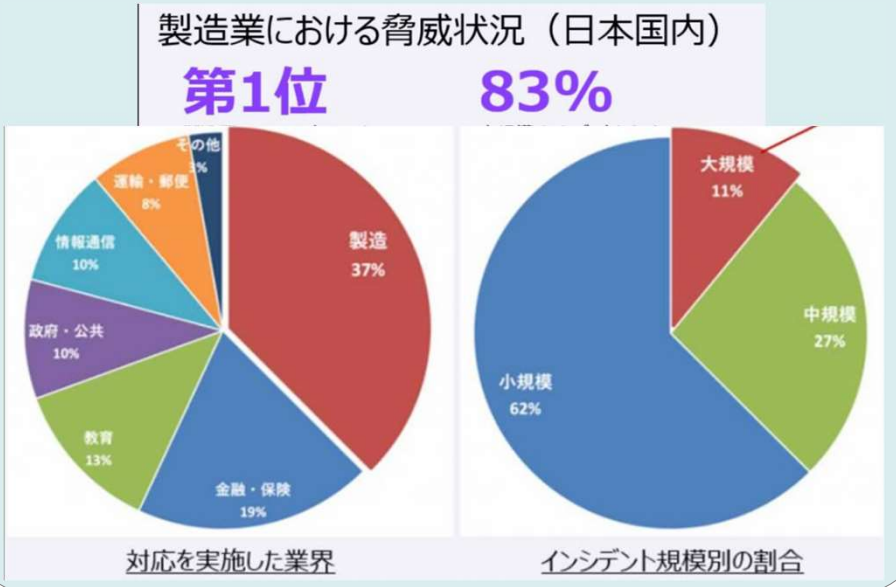
近年、製造業へのサイバー攻撃が増加傾向にある。OT/FAにおける体制や構造の複雑性が、製造業の情報セキュリティガバナンスを困難なものにしているひとつの要因であることが、本研究における有識者ヒアリングからも分かっている。OT/FAの速やかなセキュリティ対策の底上げには、情報セキュリティガバナンス強化の観点から、企業の決定権を握る経営層の意思決定につなげる事項がシンプルで明確になっている必要がある。そこで、本研究では、OT/FAのインシデント事例から問題点を抽出し、情報セキュリティガバナンスに必要な具体策とともに重要事項を考察しチェックリスト化することで、解消のための提案とする。

IoT/IIoT OTに関わるシステム特有の
セキュリティ事件/事故を36.4%の企業が経験



［出典］IDC「2021年 国内企業のIoT/OTセキュリティ対策実態調査結果」

2020年攻撃対象として業界1位となった製造業



［出典］IBM「X-Force脅威インテリジェンス・インデックス2021」

2. 研究目的と方針

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 研究の目的

サイバー攻撃が増加傾向にある国内製造業におけるOT/FAのセキュリティ対策の底上げをしたい。

■ 目指すところ

経営層の意思決定につなげる、OF/FAの情報セキュリティガバナンスに必要な重要事項をチェックリストとして提言する。

■ 事例考察とチェックリストの作成

・過去インシデント事例から抽出した問題点と、OT/FAの情報セキュリティガバナンスに必要な具体策とともに考察する。

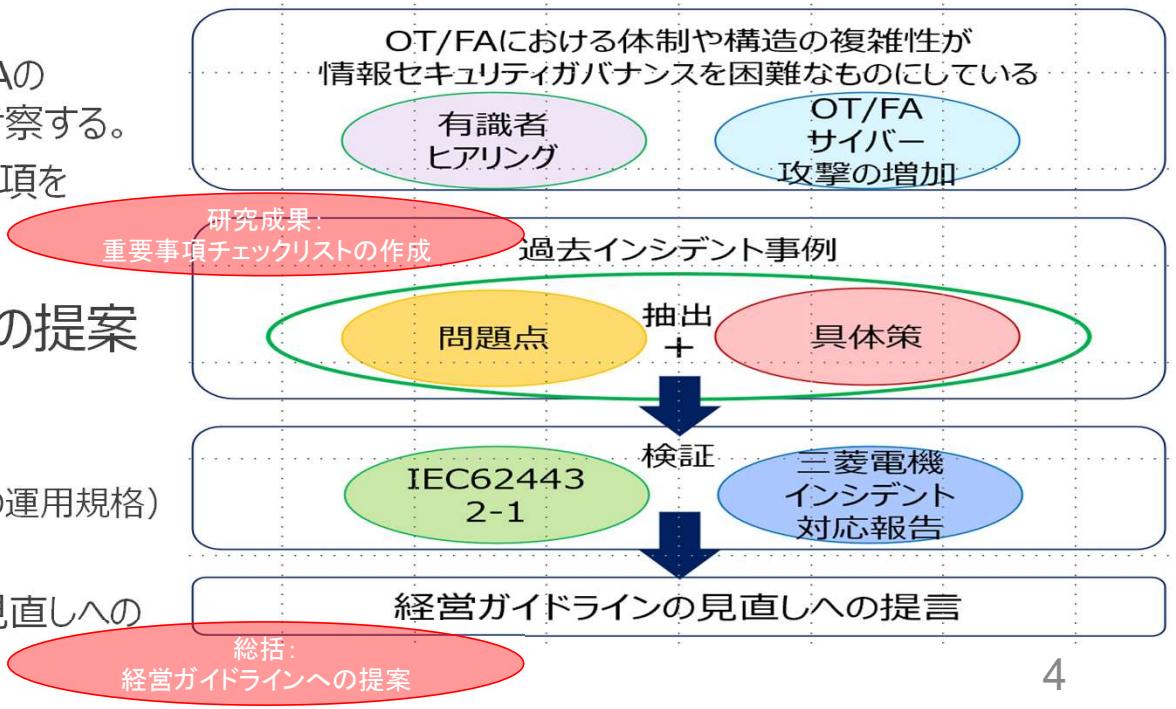
・OF/FAの情報セキュリティガバナンスに必要な重要事項をチェックリスト化する。

■ チェックリストの検証と経営ガイドラインへの提案

・3つの観点によりチェックリストの充足性を検証する。

- ✓有識者ヒアリング
- ✓OTの国際規格IEC62443-2-1（アセットオーナーの運用規格）
- ✓三菱電機のサイバー攻撃報告

・チェックリストの充足性を検証し、経営ガイドラインの見直しへの提言を総括する。

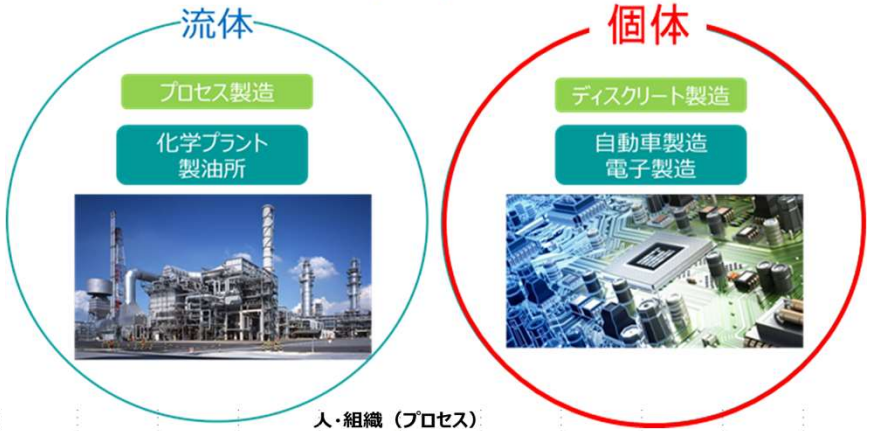


3. 対象の環境・範囲とフレームワーク

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

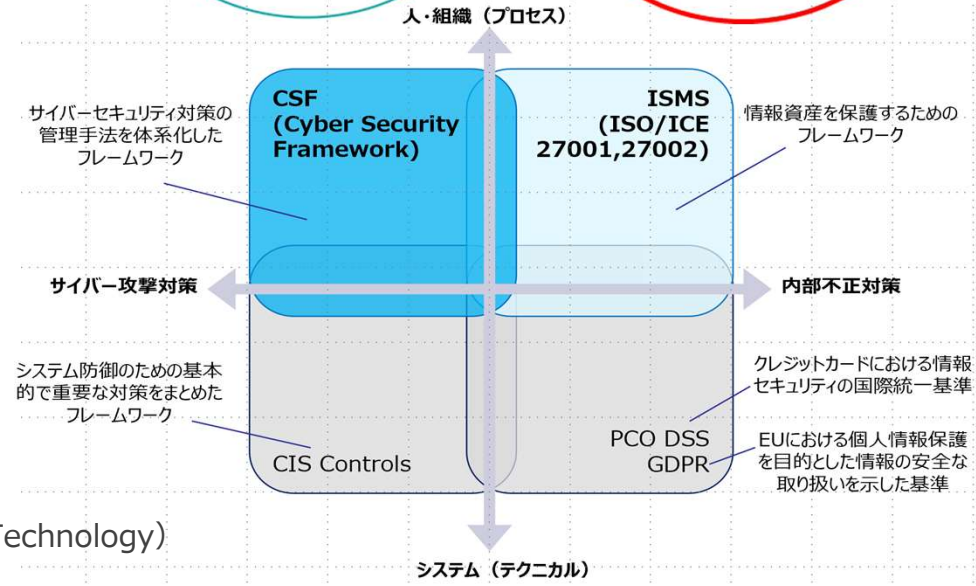
■ 対象環境と取扱い範囲

- ✓ 対象とするOT/FA環境：組織内に工場を保有し，機械部品「個体」を組み合わせて製造するディスクリート製造
- ✓ OT/FA環境の取扱範囲：産業システム(ICS)、スマートセンサー、スマートアクチュエータなどのITソリューション(IIoT)含む



■ フレームワーク

- ➢ 組織・人のフレームワーク（CSF・ISMS）
  - ✓ 人や組織の対策管理プロセスを体系化したNIST CSF*1
  - ✓ サイバー攻撃対策と内部不正対策の要素を示したISMS（ISO/IEC27001，27002）



［出典］ManageEngineの「代表的なフレームワークとの比較」

*1 NIST CSF : 米国国立標準研究所（National Institute of Standards and Technology）発行のCyber Security Framework

4. 参照するOT/FAの国際規格

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 制御システム（OT）の国際規格

- ➢ 分野・分類別に国際標準や業界標準の規格が存在する。
- ✓ 対象分野：IT，OT，電力システム，スマートグリッド，鉄道システム，石油化学
- ✓ 対象分類：組織，システム，コンポーネント

対象	情報システム（IT）	制御システム（OT）		電力システム	スマートグリッド	鉄道システム	石油化学
組織	ISO/IEC 27000	IEC 62443		NERC CIP	NIST IR7628	ISO/IEC 62278	WIB
システム			SDLA SSA				
コンポーネント			CSA	IEEE 1686			

［出典］IPA「制御システムにおけるセキュリティマネジメントシステムの構築に向けて」

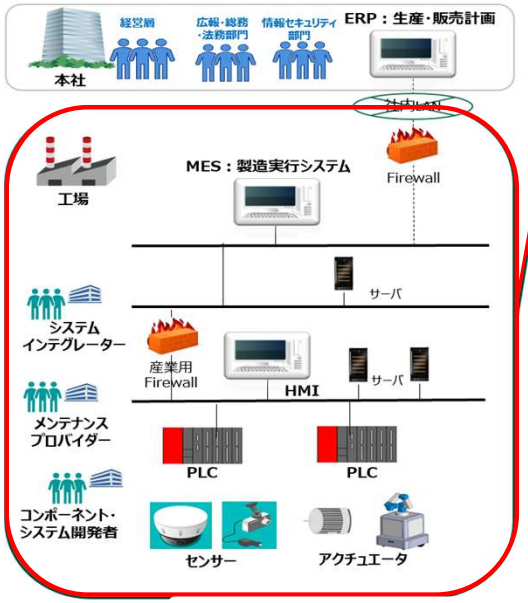
■ アセットオーナーの国際規格（IEC62443-2-1）

- ➢ IEC62443規格は役割別にシリーズ発行されている。本研究では，OTの組織（アセットオーナー）を対象にしているため、IEC62443-2-1を参照する。

<IEC62443シリーズ>

- ✓ IEC62443-2-1 ：アセットオーナー（IACS*2 全体の管理者，運用者）
- ✓ IEC62443-2-4,3-3 ：システムインテグレーターやメンテナンスプロバイダーなどのサービスプロバイダー
- ✓ IEC62443-3-3,4-1,4-2：コンポーネントやシステム開発者

*2 IACS：、産業用制御システム（IACS：Industrial Automation and Control System）



OT：IEC62443	
役割	規格
アセットオーナー IACS全体の管理者、運用者	IEC62443-2-1 運用
サービスプロバイダー ・システムインテグレーター ・メンテナンシプロバイダー	IEC62443-2-4 プロセス
	IEC62443-3-3 システム
プロダクトサプライヤー ・コンポーネント・システム開発者	IEC62443-4-1 プロセス
	IEC62443-4-2 コンポーネント

［出典］テュフズードジャパン「IEC62443概要」

5. 先行研究

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 3層構造の検証モデルと構成要素

- 本研究にてOT/FAにおける組織構造を検証するにあたり、RAMI4.0*3 の多層構造概念を用いた。
- また、IPA「重大な経営課題となる制御システムのセキュリティリスク」（P.15）の構成にRAMI4.0をイメージ展開し、経営計画システム（ERP）・製造実行システム（MES）・製造工程の自動化や制御監視システム（PLC）の3層構造モデルを作成した。このモデルを用いて過去インシデント事例の問題点を多層的・複合的に検証した。
- このモデルを用いることは、製造業の特徴でもある、OT環境だけではない多岐に渡るステークホルダーが「つながる関係」として視点を持つ重要性を意味している。

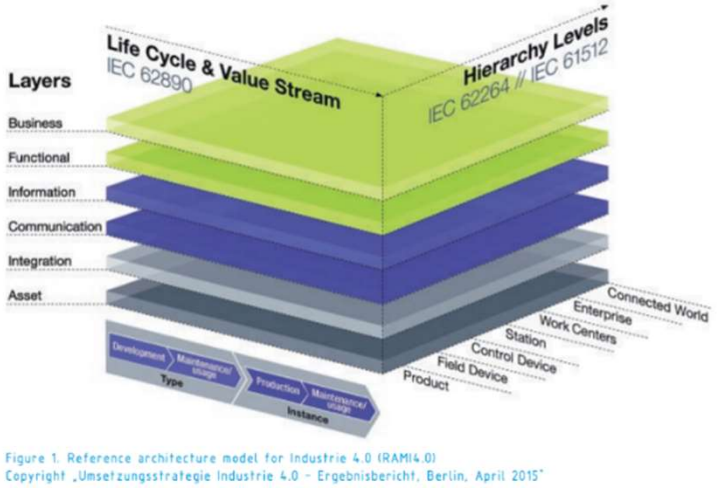
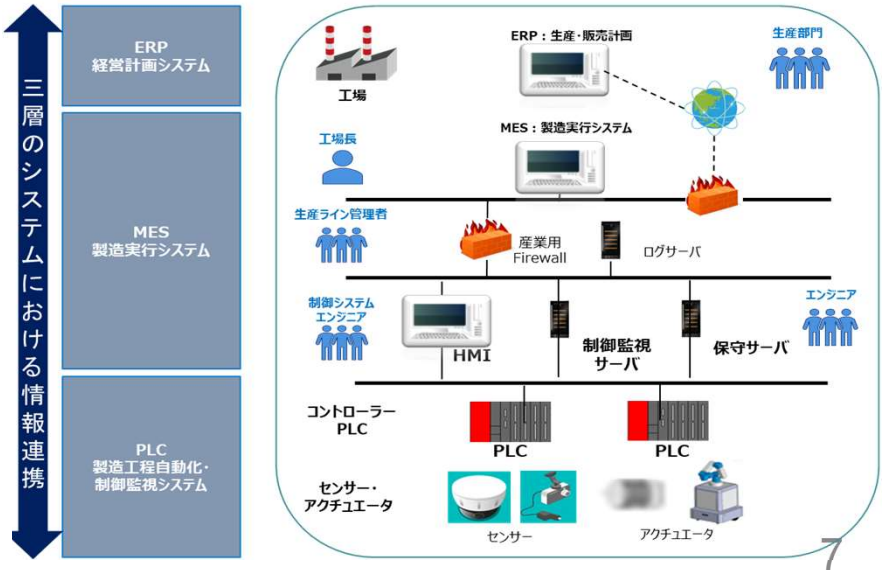


Figure 1. Reference architecture model for Industrie 4.0 (RAMI4.0)
Copyright „Umsetzungsstrategie Industrie 4.0 - Ergebnisbericht, Berlin, April 2015"

［出典］ZVEI Reference Architectural Model Industrie 4.0, 2015

展開イメージ



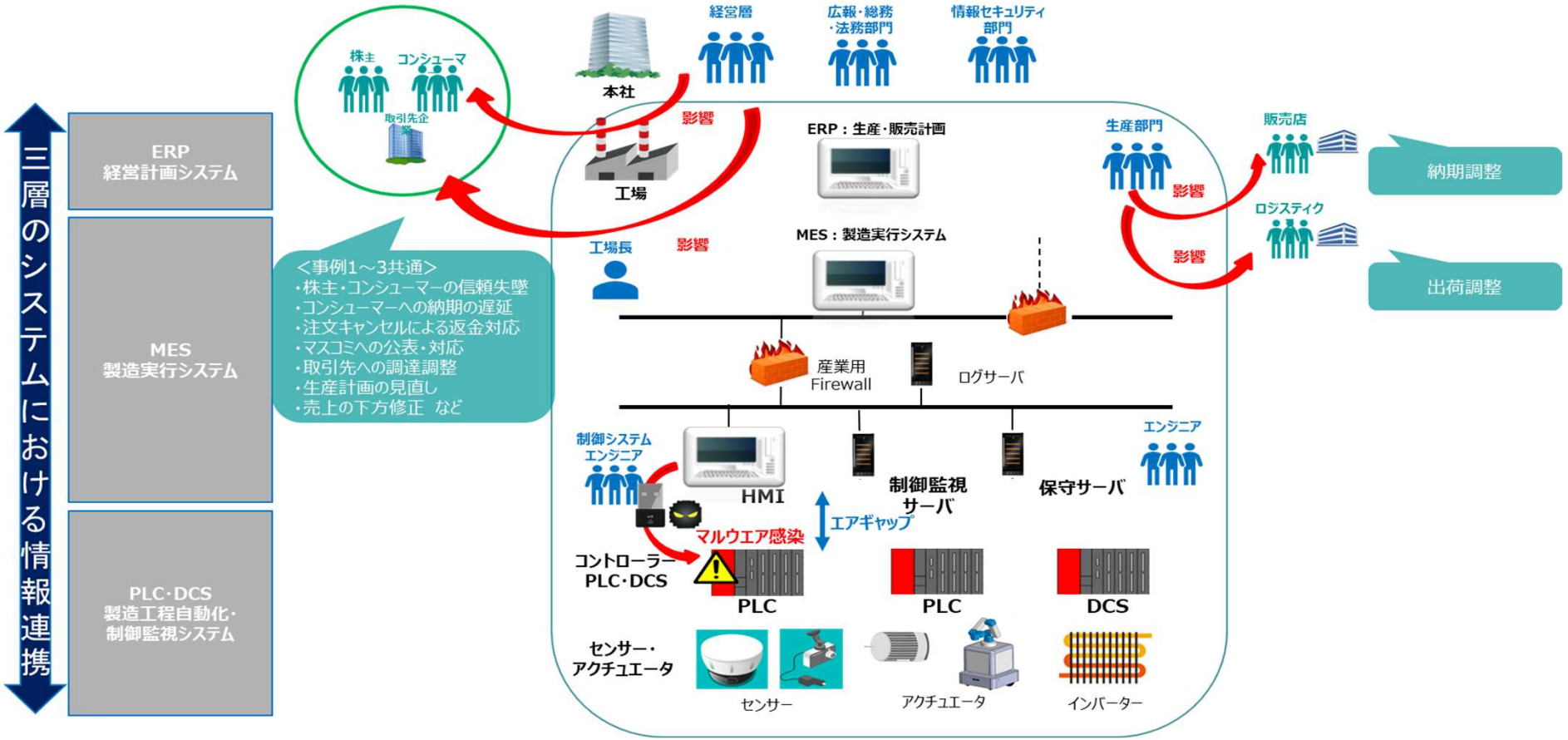
*3 RAMI4.0：ドイツ産業団体ZVEI、VDMA、BITKOMが提唱するモデル。インダストリー4.0（第4次産業革命）において、従来の生産工場の製造プロセスとのIoT既存の標準を再構成し、標準間で欠けているリンクを見つけ出し、さらに標準化が必要な分野について言及する枠組み。

6. 実例検証

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 3層構造の検証モデルをベースにサイバー攻撃実例を役割への影響へ落とし込み、対策課題を可視化し、検証を行った。

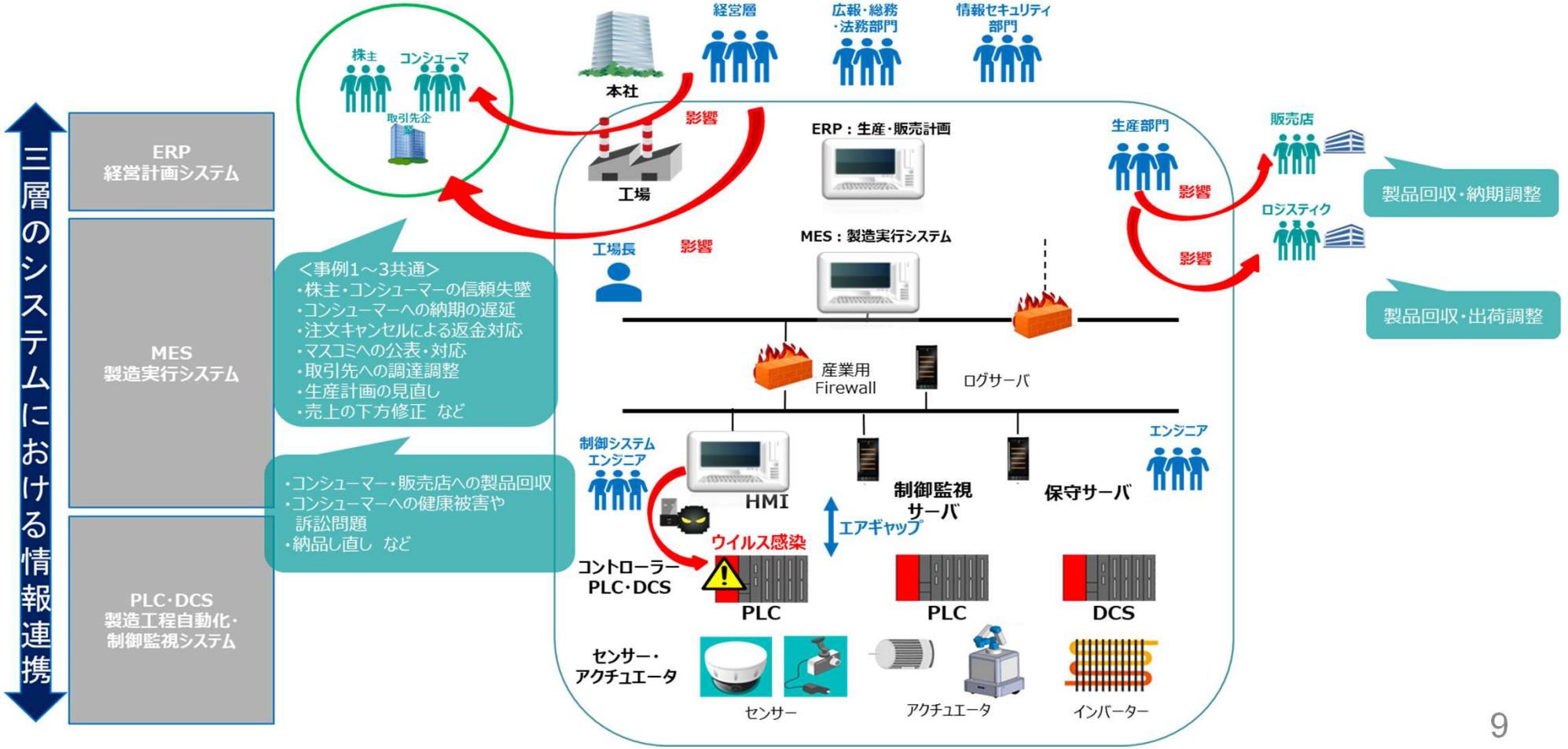
実例⑴　制御システムを標的とするマルウェアStuxnetによる攻撃事例（制御システム稼働不能）



6. 実例検証

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

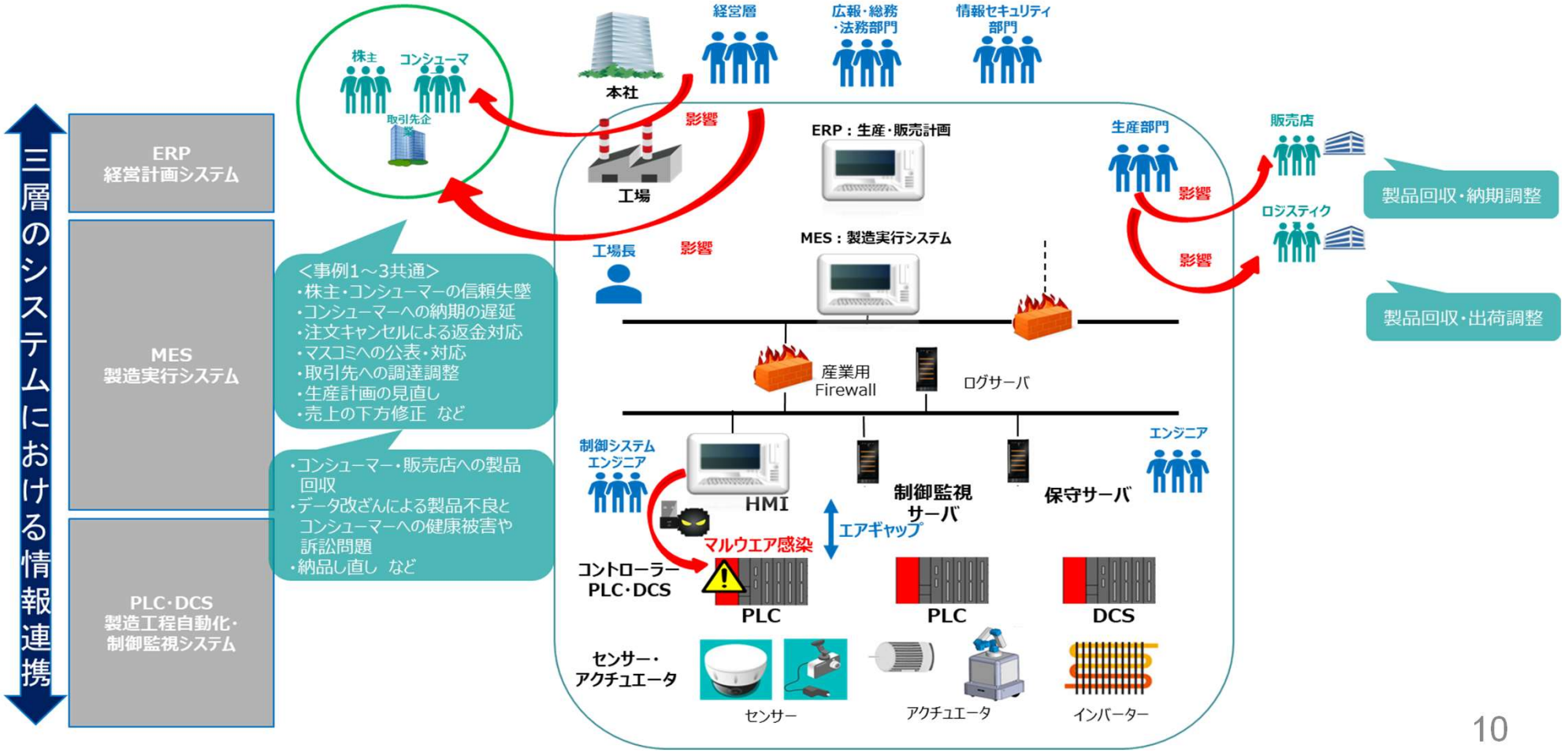
実例⑵　半導体製造企業のランサムウェアWannaCry の亜種による攻撃事例（生産ライン停止・品質検査システムへの影響）



6. 実例検証

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

実例⑶　水道橋への不正侵入と飲料水汚染未遂⇒アクセス権奪取とデータ改ざんによる不正侵入・遠隔操作



7. 重要項目の洗い出し

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 対策課題の可視化・検証から導出した課題

対象	攻撃による結果	課題
組織全体	事例⑴：マルウェア攻撃による制御システムへの感染の広がり **→工場の制御システムの稼働が停止に追い込まれ、Availability（可用性）が阻害された。** 事例⑵：品質を管理する制御システムへのウイルス侵入による機能不全 **→品質不良の製品が出荷され、Integrity（完全性）が阻害された。** 事例⑶：攻撃者による制御システムへのアクセス権奪取 **→制御システムのアクセス権が奪われConfidentially（機密性）が阻害された。**	**危機管理体制の見直し・再構築・適正な運用の確認の実施**
社長（経営層） 工場長	事例⑴：生産ラインの停止 事例⑵：品質不良の製品を出荷 事例⑶：外部からの不正アクセス **→信用の失墜・株価への影響、納期遅延、制御システムのデータ改ざんによる製品安全性への不安や実被害により、生産計画の下方修正等、対外的な責任が問われる。**	**経営層、工場長の危機管理体制に対する積極的な関与と指示の実施**
情報セキュリティ部門	**エンジニア向けのセキュリティリスクへの指導不足・教育不足が露呈した**	**（情報セキュリティ教育とは別に）制御システムにおけるセキュリティ教育の実施**
現場技術部門	**制御システムへの基本的なセキュリティ対策の理解不足が露呈した**	**制御システム固有に起こりうるリスクの洗い出しとセキュリティ教育の実施**

7. 重要項目の洗い出し

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 対策課題の可視化・検証から導出した課題に対するセキュリティ対策見直し案

課題	対策項目	具体策
組織全体 危機管理体制の見直し・再構築・適正な運用の確認と意識の醸成	**危機管理体制の見直し・再構築・適正な運用の確認の実施 IT環境とOT環境の違いを把握したうえで、OT環境が組織全体にもたらす影響を見直す** ＜見直しポイント＞ ・世の中の動向に合わせて、Availability（可用性）が阻害される主な要因を把握しているか （環境：情報収集と情報共有） ・組織全体で危機管理体制が確立されているか、既に確立されていても現状に応じ更新されているか （体制：体制の確立） ・制御システムの運用におけるリスクアセスメントを行い、実態把握と従業員のリスク認識を分析しているか （教育：リスク分析と教育）	**＜環境＞** 情報収集と情報共有として、他社との情報共有の体制づくり **＜体制＞** ・CSIRTやOT-SIRTの社内体制づくりと役割分担の明確化、 ・OT固有の資産の洗い出しとリスクアセスメントの方法・運用の確立 **＜教育＞** OTセキュリティ知識を持つ人材の育成
社長（経営層）、工場長 危機管理体制に対する積極的な関与と指示の実施	**経営層自らによる組織内のコミュニケーション活性化とセキュリティ対策への予算確保を行う** ＜見直しポイント＞ ・組織内の情報連携・情報収集においては、日ごろから縦横の垣根を超えたコミュニケーションの活性化が重要となり、組織内のイベント等を通じて経営層が従業員と、また従業員同士の交流の場を設け積極的に参加しているか ・経営層は組織全体のセキュリティ体制構築を推進し、自ら指示をおこなっているか	**＜社長（経営層）、工場長＞** 工場長がOTセキュリティにおいて理解しておくべき事項の整理 ・OTセキュリティに対する必要な戦略の見直し（予算を含む）
情報セキュリティ部門（IT） 教育プログラムの見直し （ITセキュリティ教育とは別に） OTセキュリティのプログラム計画	**制御システムにおけるセキュリティ教育の実施 IT、OTの特性に合わせたセキュリティ教育担当・体制を確立する** ＜見直しポイント＞ 下記2つのような教育・体制の検討を行っているか ・情報セキュリティは情報セキュリティ部門が主担当、制御システムセキュリティは技術部門が主担当となり、双方が窓口としてセキュリティ教育・体制に取り組む ・技術部門から情報セキュリティ部門へ担当者を移籍させ、情報セキュリティ部門が窓口一本となり部内でセキュリティ教育の展開を計画する	**＜情報セキュリティ部門（IT/OT）＞** IT/OT各システムセキュリティに対する体制の計画（CSIRT/OT-SIRTの構築）
現場技術部門（OT/FA） 制御システム固有リスクの洗い出しとセキュリティ教育の実施	**取り扱う制御システムやUSBメモリ、PC接続に対するセキュリティマニュアルの整備や遵守状況のアセスメントチェックシートの整備を行う** ＜見直しポイント＞ ・制御システムの運用におけるリスクアセスメントを行い、実態把握と従業員のリスク認識を分析しているか ・ルールを守れているかだけではなく、リスク対策の認識と必要性を理解した上で運用しているか	**＜現場技術部門（OT/FA）＞** ・OT固有の資産の洗い出し ・OTのリスクアセスメントの方法・運用づくり

8. 研究成果

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 経営層が確認すべき重要事項と情報セキュリティガバナンスを強化するためのチェックリスト

経営層が確認すべき重要事項

2原則

経営者は，下記の2原則を認識し，対策を進めることが重要である.

原則1. 経営層・工場長は，危機管理体制の構築及び継続的強化及び重要　　な情報資産の防衛強化のために，IT環境とOT環境の違いを把握したうえで，OT環境が組織全体にもたらす影響を見直すことが必要

原則2. 経営層・工場長は，継続的強化・改善のための積極的な関与と指示のために，自らサイバーセキュリティ対策予算や組織内コミュニケーションの活性化へ積極的に関与することが必要

情報セキュリティガバナンス強化のためのチェックリスト

＜危機管理体制の構築及び継続的強化，重要な情報資産の防衛強化＞

（国内外の情勢把握）

・世の中の動向やインシデントを注視し，OT環境におけるCIA阻害要因を常に把握し続けること

（体制の確立または見直し）

・組織全体でセキュリティリスク管理体制を構築し，必要に応じて都度更新していくこと

（リスク分析）

・OT環境におけるリスクアセスメントを行い，重要資産の把握とそれに対する運用実態のリスク分析をすること

＜継続的強化・改善のための積極的な関与＞

・情勢，体制，リスク分析を踏まえた改善計画の立案と指示をすること
・リスクジャッジやサイバーセキュリティ対策の投資において，バランスを保った判断や予算配分を行うこと
　また，緊急事態に備えサイバーセキュリティ対策に関わる予備費を確保すること
・日ごろから組織内の垣根を超えたコミュニケーションの活性化を図り，経営層が従業員の声に積極的に耳を傾けること
・工場長はステークホルダー（従業員，委託先，取引先，設備業者など）に対して，悩みや不満などにアンテナを張り，コミュニケーションと心のケアに努めること

8. 研究成果

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ OT/FAにおける情報セキュリティガバナンスを強化するためのチェックリスト

指示1　教育：
制御システムに携わる従業員に向けたセキュリティ教育・研修プログラムの実施

- 従業員向けに，OT/FA固有のセキュリティリスクに関する教育を実施すること
- 重要資産の取り扱いルールや基準を決め，関係者へ周知すること

指示2　体制：
OT環境におけるセキュリティ体制の確立（CSIRT/OT-SIRT/F-SIRT）

- インシデント対応チーム，体制を確立すること

指示3　規程・ルール：
OT/FAにおけるセキュリティ基準の整備と標準化

- （ディスクリート型を対象に）全社に共通するセキュリティ規程を整備・展開すること

指示4　OT環境特有のセキュリティリスクに対する技術・運用の対策

（MES）

- 不要なアプリケーションの禁止措置を行うこと
- USBメモリの禁止や代替措置を取り入れること
- 操作用PCや保守PCを接続する際には，マルウェアなどの簡易ウイルス検査を実施すること

（PLC）

- OT/FAにおけるデフォルトパスワードは必ず変更してから使用すること

（ネットワーク）

- OT/FAの構成見直しや構成管理をすること
- 外部からの不正侵入を防ぐために，ファイアウォールなどでIT/OTの通信を切り分け，さらに制御装置ネットワーク上に産業用ファイアウォールを設置すること
- FAの無線LANは暗号化などの対策をすること
- OTネットワークに接続されている機器を常時監視し，異常を早期発見できるような対策を行うこと

（システム全体）

- サイバー攻撃や内部不正に備え，ログ収集・分析の行える体制を構築すること

9. 充足性の検証 (1) 有識者ヒアリング

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

現場製造部門

OT/FAのセキュリティガバナンス強化は、製造業のセキュリティ対策の底上げにつながるため興味深い。
近年のサイバーセキュリティ情勢を踏まえると非常に重要な取り組みであり評価する。

重要項目に対して、対策ポイントに対する理解が深まる具体例をもったチェックリストとなっており，自社のOT/FAのセキュリティ対策を推進するうえで活用したい。

本社IT部門

9. 充足性の検証 (2) OT固有のセキュリティ要件（IEC62443-2-1）

結果：n=15項目（必須要件）

- 要件充足：9項目
- 要件不足：2項目
- 要件定義不十分：4項目
- OT固有のセキュリティ要件に含まれていなかった本提案要件：3項目

✓ **OT固有のセキュリティ要件に不足している2項目の追加検討が必要と分かった。**

✓ **OT固有のセキュリティ要件定義が不十分な4項目の見直しが必要と分かった。**

カテゴリ	項目名
4.2.3 リスクの識別,分類及びアセスメント	単純なネットワーク図の策定
	物理的リスクのアセスメントの結果とHSE上のリスクのアセスメントの結果とサイバーセキュリティリスクのアセスメントの結果の統合
	IACS のライフサイクル全体にわたるリスクアセスメントの実行
4.3.2 セキュリティポリシー組織及び意識向上	セキュリティ組織の確立
	訓練プログラムの経時的な改訂
4.3.3 選択したセキュリティ対策	補助的な物理的セキュリティ及びサイバーセキュリティポリシーの確立
	重要資産の暫定的保護のための手順の確立
	不要なアカウントの一時停止又は削除
	システム管理及びアプリケーション構成での強い認証方法の要求
	IACS 装置にアクセスするための適切な論理的及び物理的許可方法の確立
4.3.4 実行	システムの開発又は保守による変更に対するセキュリティポリシーの要求
	ポリシー及び手順のレビュー及び維持管理
	インシデント対応計画の伝達
	発見された問題点に対する対処及び修正
4.4.3 CSMS の見直し，改善及び維持管理	CSMS に対する変更を管理及び導入するための組織の割り当て

充足性の結果	OT固有のセキュリティ要件（カテゴリ）
要件不足：2項目	「単純なネットワーク図の策定」「不要なアカウントの一時停止または削除」
要件定義不十分：4項目	「物理的リスクアセスメントとHSE上のリスクアセスメント結果の統合」 「JACSライフサイクル全体のリスクアセスメントの実行」 「システム開発または保守による変更へのセキュリティーポリシーの要求」 「ポリシー、手順のレビュー、維持管理」
OT固有のセキュリティ要件にない要件：4項目	「OT/FA固有のセキュリティリスクに関する教育の実施」「不要なアプリケーションの禁止措置の実施」「外部記憶媒体に対するウイルス対策」

9. 充足性の検証 (3) 三菱電機の実例対策への充足性

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

＜三菱電機の3強化対策＞

［出典］「不正アクセスによる個人情報と企業機密の流出可能性について（第3報）」

三菱電機の対策	
①グループ全体の情報セキュリティ体制の強化	迅速な判断とインシデント発生時のお客様や関係機関との早期情報共有を実現するため，情報セキュリティ全般の企画・構築・運営の機能を一元化した社長直轄組織の「CRO」「リスクマネジメント統括室」を新たに設置
②技術的対策の強化	**4つの視点**でサイバーセキュリティ対策および監視体制を強化する多層防御態勢を整備 **＜侵入防止＞** ■ 未公開脆弱性対策 ・地域間・拠点間ネットワークのアクセス制限の強化 ・全サーバのネットワークレベルアクセス制御を厳格化 ■ 標的型攻撃対策 ・挙動検知機能を全端末に配備 **＜拡散防止＞** ■ グループ内感染防止対策 ・地域間・拠点間ネットワークのリアルタイム監視 ・端末リアルタイム監視と，感染端末の即時遮断 **＜流出防止＞** ■ 出口対策 ・不正アクセス先への通信遮断機能の強化 **＜グローバル対応＞** ■グローバルセキュリティーレベル向上 ・防御・監視機能のグローバル一元管理 ・MELCO-CSIRT 機能の強化
③文書管理の徹底	従来定めている，個人情報保護・企業機密管理に関する規則（情報の重要度に応じた文書の保管場所，暗号化に関する運用）について，改めて管理状況の再点検，従業員教育の充実による厳格な運用，特定事業・業務における特性を踏まえた文書管理の徹底を推進

充足性の結果	三菱電機の強化対策
要件不足：なし	「情報セキュリティ体制強化」「技術的対策の強化」「文書管理の徹底」
要件定義不十分：2項目4要素	拡散防止　　：「地域間・拠点間ネットワークリアルタイム監視」「感染端末の即時遮断」 グローバル対応：「防御・監視機能のグローバル一元管理」「グローバルCSIRT 機能の強化」

10. まとめ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

＜OT固有のセキュリティ要件に対するチェックリストの考察＞

カテゴリ	項目名	考察
4.2.3 リスクの識別,分類及びアセスメント	**単純なネットワーク図の策定**	**不足している。**
	物理的リスクのアセスメントの結果とHSE上のリスクのアセスメントの結果とサイバーセキュリティリスクのアセスメントの結果の統合	**経営者原則2に記載あるが，明確に定義できていない。**
	IACSのライフサイクル全体にわたるリスクアセスメントの実行	**経営者原則2に記載あるが，明確に定義できていない。**
4.3.2 セキュリティポリシー，組織及び意識向上	セキュリティ組織の確立	経営者原則2にて明確に定義されている。
	訓練プログラムの経時的な改訂	経営者原則1にて定義されている。
4.3.3 選択したセキュリティ対策	補助的な物理的セキュリティ及びサイバーセキュリティポリシーの確立	規程・ルールにて定義されている。
	重要資産の暫定的保護のための手順の確立	体制にて定義されている。
	不要なアカウントの一時停止又は削除	**不足している。**
	システム管理及びアプリケーション構成での強い認証方法の要求	PLCネットワークにて定義されている。
	IACS 装置にアクセスするための適切な論理的及び物理的許可方法の確立	対策⑩にて定義されている。
4.3.4実行	**システムの開発又は保守による変更に対するセキュリティポリシーの要求**	**教育,MES,にて記載あるが，明確に定義できていない。**
	ポリシー及び手順のレビュー及び維持管理	**規程・ルールにて記載あるが，明確に定義できていない。**
	インシデント対応計画の伝達	体制にて定義されている。
	発見された問題点に対する対処及び修正	体制にて定義されている。
4.4.3 CSMS の見直し，改善及び維持管理	CSMS に対する変更を管理及び導入するための組織の割り当て	経営者2にて定義されている。

10. まとめ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

＜三菱電機の3強化対策に対するチェックリストの考察＞

三菱電機の対策	チェックリスト該当項目	考察	
①グループ全体の情報セキュリティ体制の強化	**経営者の原則** 組織全体でセキュリティリスク管理体制を構築	「情報セキュリティ全般の企画・構築・運営の機能を一元化」により実現するという点で，チェックリスト項目案で掲げた経営者の原則「組織全体でセキュリティリスク管理体制を構築」に該当している。	
②技術的対策の強化	**技術対策** MES/PLC/ネットワーク/システム全体の強化	②全体	「（侵入/拡散/流出/グローバル対応の）4つの視点でサイバーセキュリティ対策および監視体制を強化する多層防御態勢を整備」により実現するという点で，チェックリストで掲げた対策「MES/PLC/ネットワーク/システム全体」の技術対策に該当している。
		＜侵入防止＞ ＜流出防止＞	侵入防止・流失防止対策は、インシデント事例があって初めて設定レベル見直しができるため未然防止策とはならないのではないかと考える。むしろ、経営者が継続的な強化・改善のための積極的に関与するために、経営者の原則「世の中の動向やインシデントを注視し，CIA阻害要因を常に把握し続ける（国内外の情勢把握）」「情勢，体制，リスク分析を踏まえた改善計画の立案と指示をすること」の方が、根本的な強化対策になるのではないかと考える。
		＜拡散防止＞	「ネットワークに接続されている機器を常時監視し，異常を早期発見できるような対策を行うこと」に該当する。 製造業に関してはサプライチェーンリスクの観点で地域間・拠点間ネットワークが重要となる。このため「⑫地域間・拠点間ネットワーク，ならびにネットワークに接続されている機器を常時監視し，異常を早期発見できるような対策を行うこと」と提案のチェックリスト文章に追記したほうが良いと考える。
		＜グローバル対応＞	グローバル対応：製造業は海外拠点も多く連携することによるリスクも高いため，現提案の「③インシデント対応チーム，体制を確立すること」の基本的な記載ではなく、「国内外拠点間の防御・監視機能の一元管理を実装すること」を項目として追加すべきとの考える。
③文書管理の徹底	**教育** 重要資産の取り扱いルールや基準の決定と関係者への周知	「規則管理状況の再点検，従業員教育による厳格な運用，特性を踏まえた文書管理の徹底」により実現するという点で，教育で掲げた「重要資産の取り扱いルールや基準を決め，関係者へ周知する」に該当する。また，従業員教育や特性を踏まえた（文書）管理という点で「固有のセキュリティリスクに関する教育を実施する」にもつながるものと考え充足するものと考える。	

11.総括

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 本研究の成果

サイバーセキュリティ経営ガイドラインVer2.0をベースに、OT/FAの情報セキュリティガバナンス強化のために、経営層が確認すべき重要事項をチェックリストとして作成した。

■提言

本研究で作成したチェックリストの検証・考察結果より、以下についてサイバーセキュリティ経営ガイドラインVer2.0への提言としてまとめる。

- OT/FAの情報セキュリティガバナンスを考慮する上では，IEC62443-2-1の制御システムを対象とした制御システム向けのセキュリティマネジメントシステム（CSMS）のOT固有セキュリティ要件を考慮する必要がある。

- 本研究でサイバー攻撃実例から問題点を抽出し対策をチェックリスト化した研究成果と「まとめ」で示した充足性の考察結果をもとに、今後、サイバーセキュリティ経営ガイドラインなどでの議論に貢献できることを期待する。

サイバー攻撃実例の各役割への影響・対策課題の可視化

■ 制御システムを標的とするマルウェアStuxnetによる攻撃事例（制御システム稼働不能）

役割	攻撃による影響	対策課題
組織全体	マルウェア攻撃による制御システムへの感染の広がりにより、工場の制御システムの稼働が停止に追い込まれ、Availabillity（可用性）が阻害される	危機管理体制の見直し・再構築・運用確認の実施
社長（経営層） 工場長	生産ラインの停止による信用の失墜・株価への影響、納期遅延による生産計画の下方修正等、対外的な責任が問われる	経営層、工場長の危機管理体制に対する積極的な関与と指示の実施
情報セキュリティ部門	エンジニア向けのセキュリティリスクへの指導不足・教育不足が露呈する	（情報セキュリティ教育とは別に）制御システムにおけるセキュリティ教育の実施
現場技術部門	制御システムへの基本的なセキュリティ対策の理解不足が露呈する	制御システム固有に起こりうるリスクの洗い出し（アセスメント）の実施
コンシューマー 販売代理店	生産ラインの停止による納期調整や注文取消しによる売上げ損失が発生する	ー
ロジスティクス	生産ラインの停止によるコンシューマーや販売店への出荷計画の修正が発生する	ー

サイバー攻撃実例の各役割への影響・対策課題の可視化

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 半導体製造企業のランサムウェアWannaCry の亜種による攻撃事例
（生産ライン停止・品質検査システムへの影響）

役割	攻撃による影響	対策課題
組織全体	ウイルスが品質を管理する制御システムに侵入し正常に機能しなくなった場合、品質不良の製品が出荷され、Integrity（完全性）が阻害される	危機管理体制の見直し・再構築・運用確認の実施
社長（経営層） 工場長	品質不良の製品を出荷したことによる信用の失墜・株価への影響、納期遅延による生産計画の下方修正等、対外的な責任が問われる	経営層、工場長の危機管理体制に対する積極的な関与と指示の実施
情報セキュリティ部門	エンジニア向けのセキュリティリスクへの指導不足・教育不足が露呈する	（情報セキュリティ教育とは別に）制御システムにおけるセキュリティ教育の実施
現場技術部門	制御システムへの基本的なセキュリティ対策の理解不足が露呈する	制御システム固有に起こりうるリスクの洗い出し（アセスメント）とセキュリティ教育の実施
コンシューマー 販売代理店	品質不良による製品回収の手配と納期の再調整によるコスト増と注文取消しによる売上げ損失が発生する	ー
ロジスティクス	品質不良によるコンシューマーや販売店への製品回収および出荷計画の修正が新たに発生する	ー

サイバー攻撃実例の各役割への影響・対策課題の可視化

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 半導体製造企業のランサムウェアWannaCry の亜種による攻撃事例
（生産ライン停止・品質検査システムへの影響）

役割	攻撃による結果	対策課題
組織全体	攻撃者の不正アクセスにより、制御システムのアクセス権が奪われ、Confidentially（機密性）が阻害される	危機管理体制の見直し・再構築・運用確認の実施
社長（経営層） 工場長	外部からの不正アクセスによる信用の失墜・株価への影響、制御システムのデータ改ざんによる製品安全性への不安や実被害、生産計画の下方修正等、対外的な責任が問われる	経営層、工場長の危機管理体制に対する積極的な関与と指示の実施
情報セキュリティ部門	エンジニア向けのセキュリティリスクへの指導不足・教育不足が露呈する	（情報セキュリティ教育とは別に）制御システムにおけるセキュリティ教育の実施
現場技術部門	制御システムへの基本的なセキュリティ対策の理解不足が露呈する	制御システム固有に起こりうるリスクの洗い出しとセキュリティ教育の実施
コンシューマー 販売代理店	品質不良による製品回収の手配と納期の再調整によるコスト増と注文取消しによる売上げ損失が発生する	ー
ロジスティクス	品質不良によるコンシューマーや販売店への製品回収および出荷計画の修正が新たに発生する	ー

4. 問題点の提示

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 経営ガイドラインVer2.0の要件定義
  - 付録 D「重要１０項目と ISO/IEC27001、27002 の関係性(P.4,27)」が示すように，ISO/IEC27001の情報セキュリティマネジメントシステム（ISMS）を基準に作成されている。
- 問題点
  - OT/FAの情報セキュリティガバナンスを考慮する上では，IEC62443-2-1の制御システムを対象とした制御システム向けのセキュリティマネジメントシステム（CSMS）のOT固有セキュリティ要件を考慮する必要がある。

付録Ｄ　国際規格 ISO/IEC27001 及び 27002 との関係

重要１０項目	ISO/IEC 27001（●）、ISO/IEC 27002（・）	
指示１　サイバーセキュリティリスクの認識、組織全体での対応方針の策定	●5.1 ●5.2	リーダーシップ及びコミットメント 方針
指示２　サイバーセキュリティリスク管理体制の構築	●5.3 ・6.1.1	リスク及び機会、責任及び権限 情報セキュリティの役割及び責任
指示３　サイバーセキュリティ対策のための資源（予算、人材等）確保	●7.1 ●7.2	資源 力量
指示４　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	●6.1 ●6.2 ・5.1.1 ・5.1.2	リスク及び機会に対処する活動 情報セキュリティ目的及びそれを達成するための計画策定 情報セキュリティのための方針群 情報セキュリティのための方針群のレビュー
指示５　サイバーセキュリティリスクに対応するための仕組みの構築	・6.2 ・9 ・10 ・11 ・12 ・13	モバイル機器及びテレワーキング アクセス制御 暗号 物理的及び環境的セキュリティ 運用のセキュリティ 通信のセキュリティ
指示６　サイバーセキュリティ対策における PDCA サイクルの実施	●7.4 ●8.1 ●8.2 ●8.3 ●9.1 ●9.2 ●9.3 ●10.1 ●10.2 ・17.1.1 ・17.1.2 ・17.1.3 ・18.1.1 ・18.2.1 ・18.2.2 ・18.2.3	コミュニケーション 運用の計画及び管理 情報セキュリティリスクアセスメント 情報セキュリティリスク対応 監視、測定、分析及び評価 内部監査 マネジメントレビュー 不適合及び是正処置 継続的改善 情報セキュリティ継続の計画 情報セキュリティ継続の実施 情報セキュリティ継続の検証、レビュー及び評価 適用法令及び契約上の要求事項の特定 情報セキュリティの独立したレビュー 情報セキュリティのための方針群及び標準の順守 技術的順守のレビュー
指示７　インシデント発生時の緊急対応体制の整備	・16.1.1 ・16.1.2 ・16.1.3 ・16.1.4 ・16.1.5	責任及び手順 情報セキュリティ事象の報告 情報セキュリティ弱点の報告 情報セキュリティ事象の評価及び決定 情報セキュリティインシデントの対応
指示８　インシデントによる被害に備えた復旧体制の整備	・17.1.1 ・17.1.2 ・17.1.3	情報セキュリティ継続の計画 情報セキュリティ継続の実施 情報セキュリティ継続の検証、レビュー及び評価
指示９　ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	●8.1 ・15.1.1 ・15.1.2 ・15.1.3 ・15.2.1 ・15.2.2	運用の計画及び管理 供給者関係のための情報セキュリティの方針 供給者との合意におけるセキュリティの取扱い ICT サプライチェーン 供給者のサービス提供の管理及びレビュー 供給者のサービス提供の変更に対する管理
指示１０　情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	・6.1.3 ・6.1.4	関係当局との連絡 専門組織との連絡