一般公開資料

Rev 1.0

SMKL セキュリティに関する白書

～工場ネットワークのセキュリティ対策レベルの見える化～

2025/11/26

IAF (Industrial Automation Forum)

SMKL Project

SMKL セキュリティ SWG

目次

1. 用語集

#	用語	意味・概要	初出箇所
1	ランサムウェア (Ransomware)	「身代金（ransom）＋ソフトウェア（software）」の造語で、悪意あるプログラムの一種。	2.1
2	レガシーシステム	古くから使われているコンピューターシステムやソフトウェアのこと。古い技術で作られているため新しいシステムとの接続性が低く、保守に課題がある。	2.1
3	ガバナンス体制	組織を適切に運営・管理するための仕組みやルールのこと。	2.2
4	NIS2 指令	EU が定めたネットワークと情報セキュリティに関する法令。	2.2
5	CISA（Cybersecurity and Infrastructure Security Agency）	2018 年に設立されたアメリカ国土安全保障省（DHS）傘下の政府機関で、その目的は、国家のサイバーセキュリティと重要インフラの保護。	2.2
6	NIST Cybersecurity Framework	NIST が策定したサイバーセキュリティのフレームワーク。	2.2
7	SP 800-82	産業制御システム向けのセキュリティガイドライン。	2.2
8	KPI（Key Performance Indicator）	目標達成の進捗を測るための「重要な指標」で、数値で把握するために使われる。	3
9	IEC 62443	産業用制御システム（ICS/OT）のセキュリティに関する国際規格。	3.1
10	Security Level	セキュリティ対策の強度を示す指標。IEC 62443 で定義。	3.1
11	Protection Level	SL と ML に基づいて定義される保護レベル。	3.1
12	Maturity Level	セキュリティ対策の成熟度を示す指標。	3.1
13	Purdue Model	製造業の階層構造を定義するネットワークアーキテクチャモデル。	3.2
14	ISA-95	製造業の情報システムと制御システムの統合を定義する国際規格。	3.2
15	ROI（投資利益率）	「Return on Investment」の略で、投資に対してどれだけ利益が出たかを示す指標。	4.1
16	ISO（International Organization for Standardization）	世界共通のルールや基準（規格）を作る国際機関。	4.1
17	IEC（International Electrotechnical Com-mission）	電気・電子技術に関する国際規格を作る団体。	4.1
18	ネットワークセグメント(Network Segment)	ネットワークを論理的または物理的に分割した「一区切り」のこと。	4.2
19	アーキテクチャ (Architecture)	システムやネットワーク、ソフトウェアなどの構造や設計の枠組み。	4.2
20	Field Network	工場やプラントなどの現場で使われる制御機器同士をつなぐ通信ネットワーク。	4.2
21	Field Bus	工場やプラントの現場機器をつなぐ通信ネットワークの一種。従来の個別配線方式に代わり、1 本の通信線で複数の機器を接続できるため、配線の簡素化と制御の効率化を実現。	4.2
22	IP Network	インターネットプロトコルを用いた通信ネットワーク。	4.2

23	Industrial DMZ（De-militarized Zone）	工場内ネットワークと工場外ネットワークの境界に設けるセキュリティゾーン。	4.2
24	脆弱性対策	システムやソフトウェアに存在するセキュリティ上の弱点（＝脆弱性）を見つけて、悪用されないように防ぐ取り組み。	4.2
25	みえる化	SMKL において単純に「可視化」だけではなく、分析という意味での「観える化」、改善の意味での「診える化」を意味する。	4.4
26	Enterprise System	企業や官公庁などの組織全体で使われる、大規模で中核的な情報システム	5.1
27	対応（緩和・改善）	インシデントへの対処とネットワーク保護の実施。	5.2
28	SNMP（Simple Network Management Protocol）	ネットワーク機器の監視・管理に使われる通信プロトコル。	5.3
29	Syslog	システムログを収集・転送するための標準プロトコル。	5.3
30	Managed SW	管理機能を持つネットワークスイッチ。	5.3
31	NMS（Network Manage-ment System）	ネットワーク全体を監視・管理するシステム。	5.3
32	OT-IDS	OT 環境向けの侵入検知システム。	5.3
33	SOC（Security Opera-tion Center）	セキュリティ監視・対応を行う専門組織。	5.3
34	CSIRT（Computer Secu-rity Incident Re-sponse Team）	インシデント対応を担う専門チーム。	5.3
35	リスク分析	何が問題になる可能性があるかを事前に見つけて、どれくらいの影響があるかを評価すること。	6.1.2
36	ギャップ分析	現状と目標の差異を分析する手法。	6.1.2
37	セキュリティポリシー	組織のセキュリティに関する基本方針。	6.1.2
38	インシデント対応プロセス	セキュリティ事故発生時の対応手順。	6.1.2
39	3C 分析	顧客（Customer）、競合（Competitor）、自社（Company）の視点で分析するマーケティング手法。	6.2.1
40	リスク許容度	組織が受容可能とするリスクの度合い。	6.2.2
41	製品ポートフォリオ	提供する製品群の構成と戦略。	6.2.4
42	定量的評価	数値などを使って客観的に評価する方法。主観ではなくデータに基づく判断ができる。	7.2.1
43	foundational require-ments（FRs）	IEC 62443 で定義されている基本的な 7 つのセキュリティ要件。	7.2.2
44	ベンチマーク	比較や評価の基準となる指標や値のこと。	7.2.2
45	開発ライフサイクル	製品やシステムの設計、開発、運用、廃止までの一連の過程。	7.2.2
46	マネージドスイッチ	ネットワークの通信設定や監視を管理者が制御できるスイッチ。	7.2.3
47	評価対象範囲	評価の対象とする範囲（システム、拠点、組織など）。	7.2.3

48	エンドポイント機器	ネットワークの末端に位置する機器。	8.2.1
49	スマートファクトリー	AI（人工知能）、IoT（モノのインターネット）、センサー、クラウドなどの技術を使って、工場のあらゆる工程をデジタルで管理・最適化する仕組み。	8.2.2
50	クラウドファースト	IT システムの構築や更新を行う際に、オンプレミス（自社サーバー）ではなく、まずクラウドサービスの利用を第一に検討する戦略。	8.2.2
51	エッジ AI	端末（エッジ）側に AI を組み込み、データをその場で処理する技術。	8.2.2
52	ゼロトラスト	「一度認証されたからといって、ずっと信頼するのは危険」という考え方に基づき、常に「誰が」「何に」「なぜ」アクセスしようとしているのかを確認し続けるセキュリティモデル。	8.2.4

2. 「SMKL セキュリティ」策定の背景

本章においては、なぜ製造業でサイバーセキュリティ対策が必要なのか、「SMKL セキュリティ」策定に至る背景を説明します。

2.1 製造業を取り巻くサイバー攻撃の現状

製造業は、近年世界的にサイバー攻撃の主要な標的となっています。従来は金融や小売といった情報資産を多く抱える分野が中心でしたが、IoT／OT（Operational Technology）の普及や生産ネットワークのデジタル化が進んだことで、工場そのものが攻撃対象となりました。特にランサムウェアによる操業停止、サプライチェーンを経由した侵入、知的財産の窃取など、事業継続に直接影響を及ぼす事例が増えています。

IBM が発表した「Threat Intelligence Index 2025」によれば、製造業は 4 年連続で最も狙われている産業であり、攻撃者からの注目度が非常に高い状況にあります【1】。

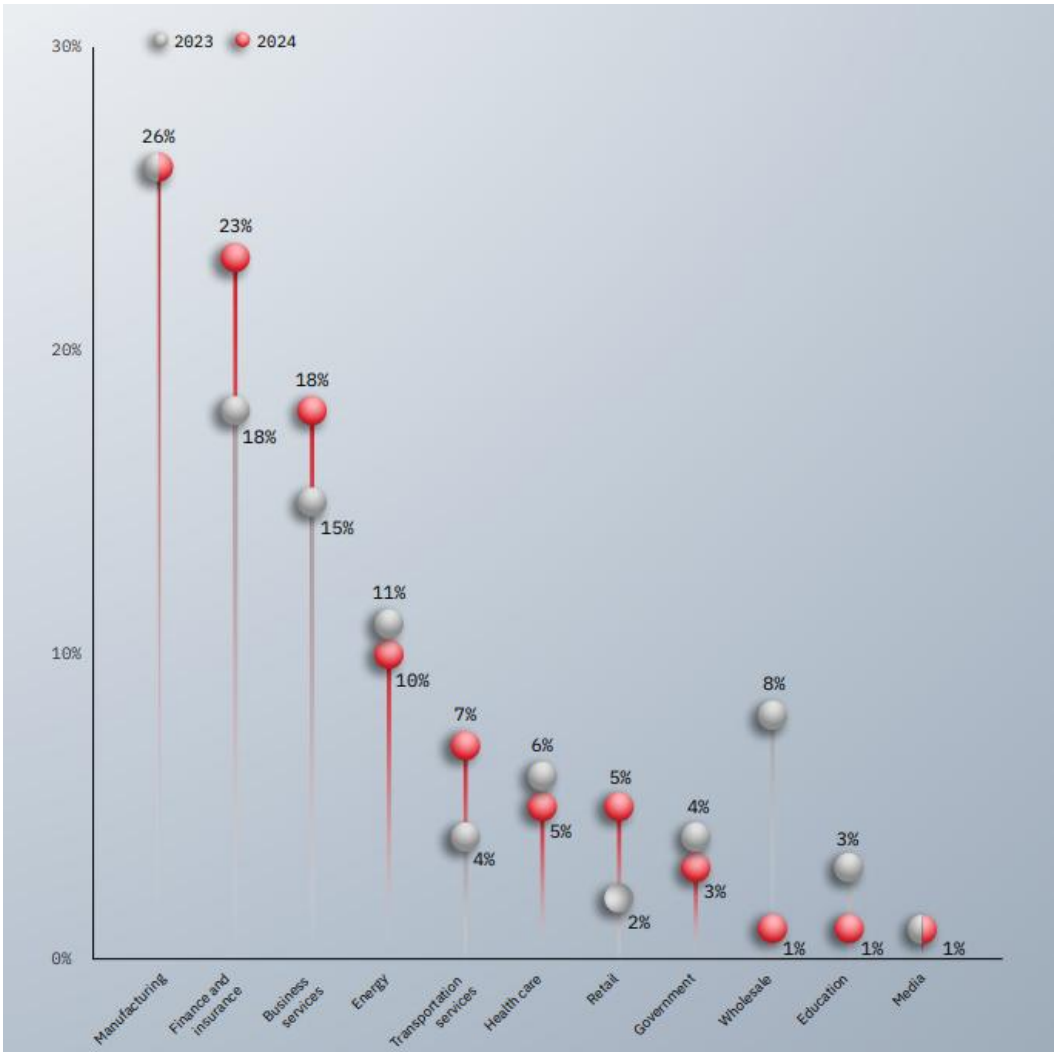

図 1

引用：「Threat Intelligence Index 2025」Share of attacks by industry, 2023-2024

その背景として、レガシーシステムの存在、有効アカウントの悪用、複雑なサプライチェーン、攻撃の高度化、そしてアジア太平洋地域を中心とする製造拠点の集中などが指摘されています。こうした要因が重なり、製造業は攻撃の成功率が高く、被害が広がりやすく、攻撃者としても活動が行いやすい、構造的な特徴を持っています。

さらにIBMの「Cost of a Data Breach Report 2023」によると、世界全体のデータ侵害の平均被害額は445万ドルに達しており、製造業は金融業界に次いで被害額が大きい産業とされています【2】。また、侵害の検知から封じ込めまでに平均277日を要しており、被害が長期化することで損害が拡大しています。これらの調査結果は、製造業におけるサイバー攻撃が、単なる情報漏えいの問題にとどまらず、経営リスクそのものに直結していることを示しています。

2.2 国際的な規制と標準化の動向

このような背景を受け、各国では製造業を含む重要インフラ分野に対する規制や標準化の取り組みを強化しています。

欧州連合（EU）では2023年に「NIS2指令（Network and Information Security Directive 2）」が施行され、リスク管理、インシデント報告、ガバナンス体制の整備が義務化されました。違反した企業には高額な制裁金が科される仕組みも導入され、法令対応が企業経営に直結する状況となっています。特にNIS2指令では、サプライチェーン全体を考慮したセキュリティ確保が求められており、国際的に事業を展開する製造業にとって大きな課題となっています【3】。

米国においても、2021年の大統領令（Executive Order 14028）を契機に、CISA（Cybersecurity and Infrastructure Security Agency）が中心となって重要インフラ分野への対策を推進しています。NIST（National Institute of Standards and Technology）は「NIST Cybersecurity Framework」や「SP 800-82（ICS向けガイドライン）」を提示し、産業制御システムに適した標準を整備しています【4】。これらは政府調達や契約条件に組み込まれることで、事実上の義務化として浸透しています。

さらに国際標準化の面では、IEC 62443シリーズが産業オートメーション分野における国際的な基準として確立されつつあります。NIS2やNISTガイドラインとも整合性を持つこの標準は、グローバルサプライチェーンにおける信頼性確保の要件となりつつあり、今後は準拠が競争力の前提条件となる可能性があります。

2.3「SMKLセキュリティ」策定の必要性

このように、製造業は攻撃者にとって魅力的な標的であり、国際的にも規制や標準化の動きが加速しています。しかし、こちらも前述の通り従来の国際規格やガイドラインは高度に専門的であり、特に中小規模の製造現場にとっては理解や実装が難しいという課題がありました。IEC 62443をはじめとする規格は包括的で有用であるものの、専門用語や多数の要件を含むため、現場担当者が直感的に「何をどこまで実施すればよいのか」を把握することが困難です。

この結果、多くの企業ではセキュリティの重要性を認識しながらも、実際の取り組みに踏み出せない状況に陥っています。特に人材や予算の制約がある中小企業では、現実的かつ段階的に取り組める仕組みが求められています。

そこで本白書では、SMKL の「みえる化」の考え方を応用し、製造現場におけるセキュリティ対策の成熟度を分かりやすく評価できる指標として「SMKL セキュリティ」を策定しました。SMKL セキュリティは、現場担当者が自社の取り組み状況を直感的に把握できることを目的とし、関係者間で共通言語として活用できる仕組みを提供します。これにより、中小企業でも現実的なステップを踏みながら継続的に対策を強化でき、結果として産業界全体の底上げにつながることを目指しています。

3. 「SMKL セキュリティ」策定の趣旨

この章では、「SMKL セキュリティ」の概要を説明します。ここでいう「SMKL セキュリティ」とは、SMKL（Smart Manufacturing Kaizen Level：工場のスマート製造化を“みえる化”する KPI 体系）に基づき、製造工場におけるセキュリティ対策の現状把握と将来的な方向性の検討を目的とした評価ツールです。SMKL の詳細については、以下の白書をご参照ください：

- 日本語版
- 英語版：Microsoft Word - SMKL_White_paper_Factory_introduction_version1_0_english.docx
- 中国語版：Microsoft Word - SMKL_White_paper_v1_0_chinese.docx

本白書を発行する IAF（Industrial Automation Forum）は、製造業ユーザーのビジョン実現に向けた情報連携とシステム構築の開発・普及を推進しており、その活動の一環として SMKL プロジェクトを展開しています。SMKL は、デジタル化された情報を可視化し、経営層・管理層・現場作業者・SIer・IoT ベンダーなどが活用できる共通基盤を提供しています。その派生として「SMKL セキュリティ」が開発されました。

この「SMKL セキュリティ」は、次節 3.1 および 3.2 で示す 2 つの観点を念頭に策定されており、これらは他の規格やガイドラインには見られない独自の特徴と考えています。

3.1 中小企業の現場でも使えるセキュリティ対策の指標策定を目指す

工場におけるセキュリティ対策とは、「工場内の重要な有形・無形資産をセキュリティリスクから守るための取り組み」を指します。これには、不法侵入を防ぐ物理的対策、システム構成に関する技術的対策、組織体制の整備、人材育成・教育など、多岐にわたる要素が含まれます。これらの側面に対しては、統括的な指針が国際的にも国内でも公開されています。代表的なものとして、IEC62443 などの国際規格、あるいは官庁・業界団体が策定した国内指針が挙げられます。

しかし、これらの標準規格は多面的な要素を網羅しているため、既に 2 章で述べたようにしばしば利用者にとっては理解が難しく、実際に対策を講じる際に「何をどの程度行えば、どこまでセキュリティを担保できるのか」が分かりづらいという課題があります。（表 1 参照）

表 1 IEC62443 シリーズの適用範囲

（2025 年 4 月時点で発行されている IEC62443 の概要を筆者が和訳し、まとめたもの）

領域	文書記号	文書名	発行年
全般的共通事項 General	62443-1-1	用語、概念およびモデル(Terminology, concepts and models)	2009
	62443-1-5	IEC62443セキュリティ・プロファイルのスキーム(Scheme for IEC62443 security profiles)	2023
ポリシーと手順 Policies & Procedures	62443-2-1	IACSアセットオーナーのためのセキュリティプログラム要求事項(Security program requirements for IACS asset owners)	2024
	62443-2-2	IACSセキュリティ保護スキーム(IACS security protection scheme)	2025
	62443-2-3	IACS環境内のパッチ管理(Patch management in the IACS environment)	2015
	62443-2-4	IACSサービスプロバイダーに対するセキュリティプログラム要求事項(Security program requirements for IACS service providers)	2023
システム System	62443-3-1	産業用オートメーションおよび制御システムのためのセキュリティ技術(Security technologies for IACS)	2009
	62443-3-2	システム設計のセキュリティリスクアセスメント(System risk assessment for system design)	2020
	62443-3-3	システムセキュリティ要求事項およびセキュリティレベル(System security requirements and security levels)	2013
コンポーネント Component	62443-4-1	安全な製品開発ライフサイクル要求事項(Secure product development lifecycle requirements)	2018
	62443-4-2	IACSコンポーネントの技術的セキュリティ要求事項(Technical security requirements for IACS components)	2019
評価方法論 Evaluation Methodology	62443-6-1	IEC62443-2-4のためのセキュリティ評価方法論(Security evaluation methodology for IEC62443-2-4)	2024
	62443-6-2	IEC62443-4-2のためのセキュリティ評価方法論(Security evaluation methodology for IEC62443-4-2)	2025

製造現場でセキュリティ指標の活用が難しいとされる主な理由は以下の通りです：

（1）セキュリティ技術に関する専門用語が多用されている。

（2）多領域を包括的に扱うため、規格が非常に複雑である。

（3）実施すべき項目が多く、計画立案が困難。Security Level、Protection Level、Maturity Level の関係性が直感的に理解しづらい。（図 2 参照）

（4）自社での評価が難しく、継続的な対策が困難。

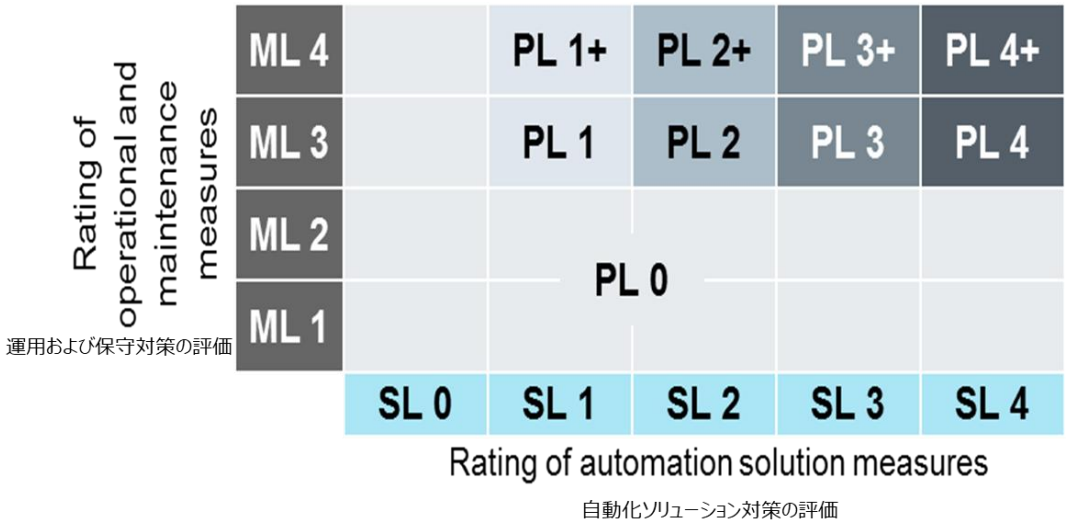

図 2 IEC62443-2-2 に記載の Security Level(SL)と Maturity Level(ML)により規定される Protection Level(PL)の関係

これらの規格は技術的な正確性を重視しているため、難解な用語や複雑な関係性の理解がユーザーにとって大きな負担となり、結果として対策の実施に踏み出せない企業も少なくありません。

特に、専門組織や人材の確保が難しい中小企業ではその傾向が顕著であり、セキュリティの重要性を認識しながらも、実際の活動に移せない状況が続いています。

このような課題を踏まえ、中小企業、特に製造現場でも容易に活用できる指標の検討を進めました。製造現場を重視する理由は、日常的に製造装置や制御装置を扱う部署であり、セキュリティが破られた際に最も影響を受けるからです。また、IT 部門とは異なり、これまでサイバー攻撃の対象となる機会が少なかったため、セキュリティ対策が浸透しづらい背景もあります。

3.2 SMKL の特性を活かした工場のセキュリティ対策の成熟度を可視化

3.1 で述べたような分かりやすい指標を検討した結果、SMKL のシンプルな構成と明確な基準設定が最適であると判断しました。具体的には以下の通りです：

（1）3×4 のマトリクス構成で、横軸（3 レベル）は対象範囲を示します。これは Purdue Model や ISA-95 で規定される製造工程の階層とその階層間をつなぐネットワークに対応しています。

（2）縦軸（4 レベル）は「見える化」レベルを示し、セキュリティ対策の進捗や達成度合いを表します。すなわち、この指標はセキュリティ対策の成熟度を可視化した指標です。

（3）SMKL セキュリティは、横軸で定義された対象範囲（例：制御ネットワーク等）におけるセキュリティ対策の成熟度を可視化するツールです。

（4）現状のレベルを判定し、将来的にどのレベルまで成熟度を高めるか、あるいは対象範囲を広げるかといった計画が立てやすくなります。

セキュリティ対策には多くの部署が関与するため、頻繁な調整が必要です。その際、SMKL セキュリティを共通指標とすることで、製造現場の担当者はもちろん、セキュリティに詳しくない方でも「どの対象範囲（横軸）」の話か、「どの成熟度レベル（縦軸）」の話かを理解しやすくなります。これにより、部署間の誤解が減り、より円滑な対策の推進が可能となります。

ただし、SMKL セキュリティは「分かりやすさ」や「コミュニケーションのしやすさ」を重視しているため、学術的な厳密性には一部劣る点があります。また、縦軸の**「見える化」レベルを達成したからといって、リスクを完全に回避できると保証するものではない**ことにご留意ください。

4. 「SMKL セキュリティ」策定の方針

本書第 3 章で述べたように、これまでに発表されている規格やガイドラインにおいて、製造現場での活用がなかなか進まない状況を改善すべく、本書では大きく分けて以下の 2 点を検討することにしました。

（1） SMKL の仕組みを用いて、直感的に分かりやすく、かつ使いやすい評価指標とする。

（２） 様々な評価対象を省き、的を絞って「SMKL セキュリティ」を策定する。

この（１）については 4.1 で、（２）については 4.2 で詳細を説明します。

4.1 SMKL の活用 - SMKL とは? -

SMKL（Smart Manufacturing Kaizen Level）は、IAF（Industrial Automation Forum）が推進するプロジェクトで、製造現場のスマート化を段階的に評価・改善するための指標体系です。

（１）SMKL の概要

目的：スマート製造の「みえる化」レベルを診断し、改善（Kaizen）を促進します。

対象：経営層、現場作業者、SIer、IoT ベンダーなど多様な関係者が共通の評価基準で活用可能です。

評価方法：IoT 化の進捗を 16 マスのマトリクスで評価し、現状と目標のギャップを明確化します。

（２）4 つの「みえる化」レベル

SMKL のみえる化レベル（縦軸）は、以下の 4 段階で成熟度を評価します：

表 2 SMKL のみえる化レベル

レベル	名称	内容
a	データ収集(Collecting)	自動または簡易操作で必要なデータを電子的に収集・蓄積。
b	見える化(Visualizing)	データを表やグラフで自動表示。
c	観える化(Analyzing)	AI や分析ツールを活用して目標との差異を分析し、自動通知。
d	診える化(Optimizing)	AI などを活用し、差異に対する改善処置を生産システムや設備、人へ自動フィードバック。

※データ収集をしていない状態はレベル０

（３）管理対象レベル

SMKL の管理対象レベル（横軸）は、SMKL を適用する業種や分野によって設定ができます。

表 3 SMKL の管理対象レベル

レベル	製造業（組立）	製造業（カーボンニュートラル）	製造業（セキュリティー）	農業	教育
1	設備・人	工場	本書で定義	初期	初級
2	ライン・工程	ライン・工程	同上	中期	中級

3	工場	設備・人	同上	後期	上級
4	サプライチェーン	サプライチェーン	同上	―	―

※投資が少ない管理レベルから定義する事で、費用対効果(ROI)についても検討が可能です

（4）活用のメリット

・ROI（投資収益率）を考慮した改善計画が立てられます。
・中小企業でも導入しやすいように、簡易診断ツールやホワイトペーパーも提供しています。
・国際標準化（ISO/IEC）への提案も進行中ですので、SMKL を世界中で活用できます。

（5）詳しく知りたい方へ

下記 Web ページを参照ください。

・IAF 公式サイトの SMKL プロジェクトページ
・三菱電機による SMKL の紹介ページ

スマート製造に興味があるなら、SMKL はまさに「今どこにいて、どこへ向かうか」を可視化するコンパスのような存在です。導入を検討している企業や技術者にとって、非常に有益なツールであり。興味があれば、簡易診断ツールもお試しください。

・SMKL 簡易診断ツール

4.2　評価対象の限定

本白書で扱う「評価対象」とは、「SMKL セキュリティ」が適用される範囲を指します。図 3 に示すように、製造業の構成の中でも「工場内の製造現場と倉庫」に限定しています。

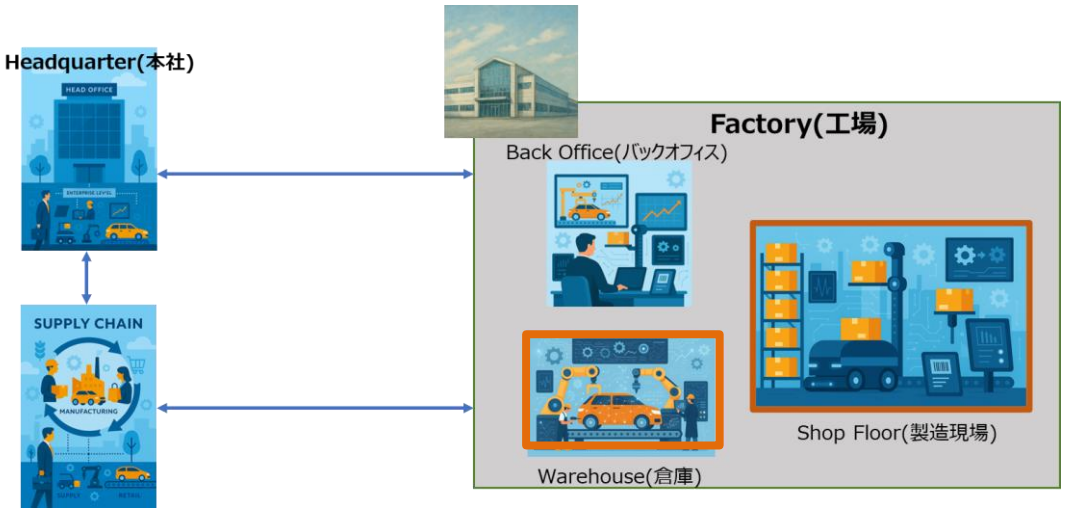

図 3 本白書で扱う領域

さらに、製造現場におけるネットワークセキュリティに焦点を絞っています。ネットワークセキュリティとは、ネットワークに接続された情報資産と、それを支えるネットワーク基盤を不正アクセスやサイバー攻撃から守るための防衛策です。

本白書の「SMKL セキュリティ」では、製造工場における工程およびその工程間での情報流通に関し、以下の要件を満たすことを求めています。

（1） 機器や設備における情報はデジタル化されている。

（2） 機器や設備間の情報はネットワークを介してやり取りされる。

（3） 一つの工程や機能の塊を一つのネットワークセグメントとして分離させている。

ただし、上記 3 項目を工場全体で実施することは必ずしも必要ではなく、セキュリティを担保したい部分だけに実施するだけでも「SMKL セキュリティ」を用いる条件は満たしています。上記のような条件の下で、「SMKL セキュリティ」は Purdue Model を基盤とした ISA-95 を参照し、ネットワークのセグメンテーションと機器階層構造を明確に定義しています。このフレームワークにより、企業はエンタープライズシステムと運用システム間の一貫した通信を維持しつつ、柔軟で拡張性の高いアーキテクチャを構築できます。

図 4 は、ISA-95 の階層モデルを基に、工場内の管理機能・生産機能・データ交換に使われるソフトウェアシステムを区分し、それらを接続するネットワーク構成を模式的に示したものです。このネットワークにおいては、ISA-95 の Level0 および Level1 においては、従来から産業用プロトコルにより通信を行う Field Network(あるいは Field Bus)が使われています。

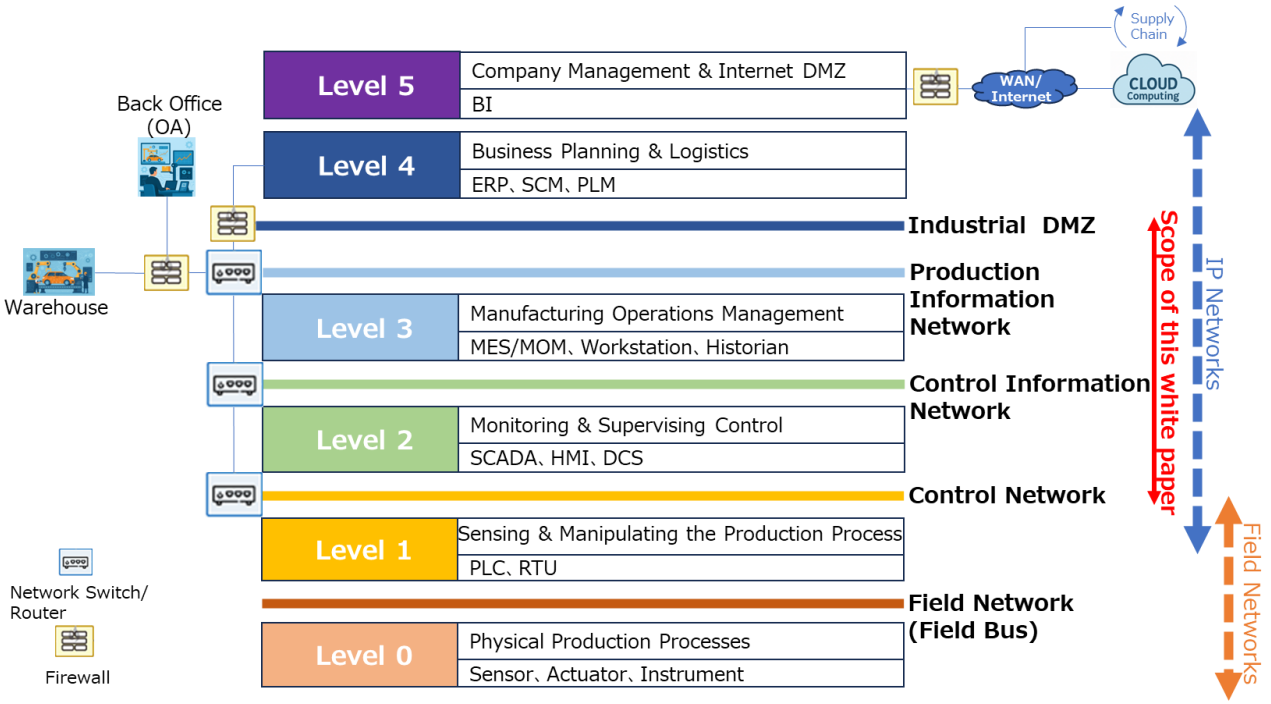

図 4 ISA-95 の階層モデルを基に作成した工場内ネットワーク構成

本白書では、ISA-95 の Level1 以上において主に IP Network が使用されていることを踏まえ、「Control Network」「Control Information Network」「Production Information Network」「Industrial DMZ」までを対象としています。

なお、IoT/DX 時代においてそもそも図 4 で示したような階層構造が成り立つのかという疑問もあるかと思います。その点については、8 章で検討していますので、そちらを参照ください。

このように対象範囲を限定することで、第 2 章で述べた評価指標の複雑性を回避し、現場での実装を容易にすることを目指しています。なお、本白書では、工場内機器の脆弱性対策や物理的侵入リスクについては扱っていません。

4.3　評価対象範囲の限定

SMKL の横軸では、工場内を「設備・作業者」「ライン・工程」「工場全体」「サプライチェーン全体」の 4 つのレベルに区分していますが、SMKL セキュリティでは工場内ネットワークに評価対象範囲を限定しているため、「サプライチェーン全体」は対象外となります。

また、工場ネットワークのデータフローや扱うデータの種類を考慮し、基本的な 3 つの階層に分けて評価する方針としています。この 3 階層については第 5 章で詳しく説明します。

4.4　評価要件の限定

SMKL セキュリティの縦軸レベルを判定する「評価要件」についても、評価対象を限定することで、製造現場での自己評価が可能になると考えました。

元の SMKL では、IoT/DX の達成度合いを「みえる化」することが目的ですが、SMKL セキュリティでは、工場ネットワークにおけるセキュリティ対策機能の「みえる化」に特化しています。これは、セキュリティ設計や運用、識別・認証などの要素は含まないという意味です。

また、評価項目が多すぎると、判定に時間がかかるだけでなく、すべての項目をクリアしなければそのレベルに到達できないという印象を与えてしまいます。これは、製造現場におけるモチベーションの低下につながる恐れがあります。

そこで本白書では、各レベルの評価項目を 2 項目のみに絞り込み、簡潔かつ明確な判定が可能となるよう設計しました。これにより、現場担当者が自らの取り組み状況を把握しやすくなり、継続的な改善への意欲を維持しやすくなります。

次の章で詳細の説明を行います。

5.　SMKL セキュリティマトリクスの定義

5.1　横軸の定義

管理対象のレベルである横軸は、SMKL では工場内を「設備・作業者」「ライン・工程」「工場全体」「サプライチェーン全体」の 4 つのレベルに区分していますが、SMKL セキュリティにおいては、4.2 で述べたように工場内のネットワークに評価対象範囲を限定していますので、「サプライチェーン全体」は範囲外となります。

また、工場内ネットワークのセキュリティのみを対象としていますので、工場ネットワークのデータフローおよび扱うデータの種類を考慮して、「生産情報ネットワーク」「制御情報ネットワ

ーク」「制御ネットワーク」の基本的な 3 つの階層に分けることにしました。この 3 階層については、ISA-95 を参考に決めています。

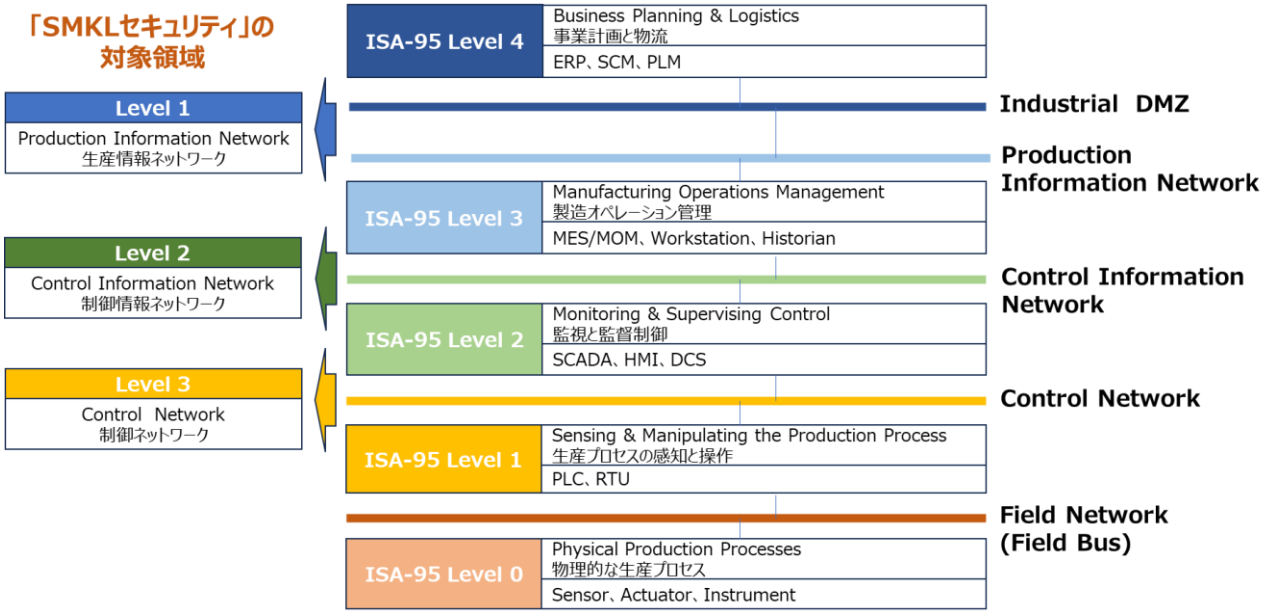

図 5 ISA-95 を参考に決めた SMKL セキュリティの管理対象レベル

レベルの順番については、工場のセキュリティ対策を検討する際は Enterprise System との接続分離から実施し、上位層から内部のセキュリティ対策を検討していくことが効果的なため、レベル 1「生産情報ネットワーク」→レベル 2「制御情報ネットワーク」→レベル 3「制御ネットワーク」としました。

5.2 縦軸の定義

みえる化のレベルである縦軸は、SMKL ではレベル a「データ収集」、レベル b「見える化（可視化）」、レベル c「観える化（分析）」、レベル d「診える化（改善）」と定義しています。SMKL セキュリティでは、4.4 で述べたように工場ネットワークにおけるセキュリティ対策機能のみえる化であることを踏まえ、レベル a「ログの収集」、レベル b「モニタリング（ネットワーク/アセットの状態や識別の可視化）」、レベル c「分析（セキュリティリスクの継続的な監視）」、レベル d「対応（緩和、改善）」として定義します。

横軸の定義と組み合わせると SMKL セキュリティ・マトリックスは表 4 のように表すことができます。

表 4 SMKL セキュリティ・マトリックス

レベルd	対応(緩和、改善)			
レベル c	分析(セキュリティリスクの継続的な監視)			
レベルb	モニタリング(ネットワーク／アセットの状態や識別の可視化)			
レベル a	ログの収集			
みえる化レベル		レベル1	レベル2	レベル3
管理対象レベル		生産情報ネットワーク	制御情報ネットワーク	制御ネットワーク

5.3　評価要件とみえる化レベル

各みえる化レベルにおける評価要件は次の通りとします。

（1） レベル a「ログの収集」

・ログデータを自動的に収集し（SNMP,Syslog 等）、継続的な監視に利用できるようになっている。
・ポートミラーリング機能を持っている。
※ログの収集は一元化されていなくてもよい。
典型的な対策の例としては Managed SW の導入が挙げられます。

（2） レベル b「モニタリング（ネットワーク/アセットの状態や識別の可視化）」

・ネットワークを常に監視して新しいハードウェア、ソフトウェアを検出する。
・稼働状況を検知する仕組みをもっている。
典型的な対策の例としては NMS の導入が挙げられます。

（3） レベル c「分析（セキュリティリスクの継続的な監視）」

・自動化された手段を使用して、選択されたサイバーセキュリティ要件への準拠を継続的に評価する。
・ネットワークを監視して、異常、侵害の兆候を検出する。
典型的な対策の例としては OT-IDS の導入が挙げられます。

（4） レベル d「対応（緩和、改善）」

・インシデントの拡大を防ぎ、封じ込めを実行する手段を持っている。
・通信及び制御ネットワークを保護する手段を講じている。
典型的な対策の例としては SOC/CSIRT の継続運用が挙げられます。

6. 「SMKL セキュリティ」の活用

6.1 工場での活用

SMKLセキュリティは、工場現場におけるネットワークセキュリティ対策の「見える化」を実現するための評価ツールです。特に中小企業の製造現場では、専門人材の不足や複雑な規格への対応が困難であるため、SMKL のシンプルな構造と直感的な評価指標が有効に機能します。本節では、工場現場における SMKL セキュリティの活用方法を、以下の 4 つの観点から整理します。

6.1.1 現状把握と目標設定のためのツール（活用①）

SMKL セキュリティは、工場内のネットワークセキュリティ対策の現状を客観的に評価するためのツールです。専門知識がなくても、現場担当者が自社のセキュリティ対策の成熟度を把握できるよう設計されています。

ステップ 1：現状のポジション把握

工場内の設備構成、ラインの接続状況、ネットワークの階層（例：ISA-95 に基づく Level 1〜3）を確認し、SMKL マトリクス上で現在の位置を特定します。

例えば、「生産情報ネットワーク」レベルで「ログ収集」まで達成しているが、「制御情報ネットワーク」では未着手、というように、対象範囲と成熟度を明確にします。

ステップ 2：目標設定の最適化

工場の規模、IT/OT リソース、リスク許容度、事業継続性などを踏まえ、現実的かつ段階的な目標レベルを設定します。

すべての領域で最高レベルを目指すのではなく、重要度や ROI を考慮し、優先順位をつけた目標設定が可能です。

このプロセスにより、現場主導でのセキュリティ対策の方向性が明確になり、関係者間の共通認識形成にもつながります。

6.1.2 セキュリティロードマップ策定における活用（活用②）

SMKL セキュリティは、工場の中長期的なセキュリティ強化計画の策定にも活用できます。現場の実情に即した改善ステップを明確にすることで、継続的な対策推進が可能になります。

フェーズ 1：基本設計

現状評価をもとに、リスク分析とギャップ分析を実施。SMKL マトリクス上での目標レベルに向けて、セキュリティポリシーや基本方針を策定します。

フェーズ 2：運用体制の確立

インシデント対応プロセスの整備、現場での運用ルールの明文化、担当者の役割分担など、日常運用に必要な体制を構築します。

フェーズ 3：最適化・高度化

セキュリティ対策の自動化（例：ログ監視、アラート通知）、改善サイクルの導入、他拠点との連携強化など、継続的な高度化を図ります。

このように、SMKL を軸にしたロードマップは、現場の実行力を高め、無理なく段階的にセキュリティレベルを向上させることができます。

6.1.3 自社活動のポジショニングと戦略的活用（活用③）

工場内でのセキュリティ活動を SMKL セキュリティマトリクス上にマッピングすることで、現場の強み・弱みを可視化できます。これにより、社内の改善活動や外部ベンダーとの連携が円滑になります。

・各部署の取り組み（例：IT 部門の監視体制、製造部門の装置管理）を SMKL 上で整理し、どのレベルに対応しているかを明確化。

・改善の優先順位を定めることで、限られたリソースでも効果的な対策が可能。

・他工場との比較やベンチマークにも活用でき、グループ全体でのセキュリティレベル向上にも貢献。

このようなポジショニングは、社内の意思統一や外部との協業にも役立ちます。

6.1.4 改善活動・運用プロセスにおける SMKL の活用（活用④）

SMKL セキュリティは、工場内の改善活動や運用プロセスにおいても、関係者間の意識合わせに有効です。定期的な評価とフィードバックを通じて、セキュリティ対策の継続的な改善を支援します。

・提案フェーズ：現場での課題共有と改善案の提示。SMKL を使って、どの範囲・どのレベルの話かを明確にし、関係者の理解を促進。

・導入フェーズ：施策の実装状況を SMKL で可視化。進捗管理や関係者への報告にも活用可能。

・運用フェーズ：定期的な評価とロードマップの見直し。環境変化に応じた柔軟な対応が可能。

このように、SMKL は単なる評価ツールではなく、改善活動の「共通言語」として機能し、現場の自律的なセキュリティ運用を支援します。

6.1.5 おわりに

SMKL セキュリティは、工場現場におけるセキュリティ対策の「見える化」を通じて、現場主導の改善活動を支援するツールです。専門知識がなくても活用できる構造により、現場の自律的なセキュリティ強化を促進します。今後、より多くの工場での導入が進むことで、製造業全体のセキュリティレベル向上に貢献できると考えています。

6.2　インテグレータでの活用

6.2.1 はじめに

システムインテグレーター、セキュリティベンダー、コンサルタントなどのインテグレータにとって、SMKL は単なる評価ツールではなく、顧客との意識合わせの共通言語として活用でき、包括的なセキュリティ戦略を策定・実行するための強力な手段となります。

本節では、インテグレータにおける４つの活用方法について説明します。

またこれらの活用方法を実践するとインテグレータ商材の３Ｃ分析が可能になりますので、商材の改善や新規開発など上手く活用して、貴社による提供価値を高めてください。

6.2.2 顧客の現状把握と目標設定のためのツール（活用１）

インテグレータは、SMKL セキュリティを活用することで、客観的に製造業顧客のセキュリティ状況を評価し、共通認識を形成することができます。

この顧客のセキュリティ評価の過程は以下のステップで進めることが効果的と言えます。

同時に目標とする範囲やレベルについても議論できると更に効率的な評価につながります。

ステップ１：現状のポジションを把握

顧客の工場やネットワークシステムの現状を調査し、SMKL 上でどの位置にいるのかを特定します。このヒアリングを通じて、顧客のセキュリティ対策の強み・弱みが明確になります。例えば、顧客から人材育成や組織体制が不十分であることの相談や、技術面ではどのような対策をすればいいかわからない。このようなお悩み事をお聞きできるとより対策方針が明確になってきます。

ステップ２：設定する目標の最適化

顧客の事業特性、リソース、リスク許容度などを考慮し、適切な目標位置を SMKL セキュリティ上で定義します。重要なのは、最高レベルを一律に目指すのではなく、事業継続性とセキュリティ対策のバランスを取りながら、顧客にとって具体的かつ最適な目標設定の提案を行う事です。

6.2.3 顧客のセキュリティロードマップ策定における活用（活用２）

SMKL セキュリティは、中長期的なセキュリティ強化計画の策定に特に有効です。まずは、顧客の事業形態や環境変化などの特性を捉えて、対策の優先度を決めていく必要があります。この顧客と優先度を決めていく過程の中で、おのずとセキュリティ対策の範囲やレベルは決まってくると考えます。

（１）顧客特性の整理

セキュリティ対策を優先順位付けする際、以下の顧客特性を考慮する必要があります。

- 事業変革の状況（M&A、新工場建設、グローバル展開など）
- 組織規模と人員構成（従業員数、OT 人材の IT リテラシーの度合など）
- 拠点数と拠点毎の接続先（顧客先接続の有無、クラウド利用の有無など）
- 業界固有の規制要件と標準（業界セキュリティガイドライン対応など）
- 既存システムの状態と更新サイクル（更新時期に合わせたコスト削減など）

顧客特性を加味した上で対策の優先度設定ができたのち、インテグレータは以下のようなアプローチで目標達成に向けた計画表（ロードマップ）を作成し、今回、何をどこまで進めるのか顧客と合意形成を図っていく必要があります。各推進フェーズに分けて、フェーズ毎のアウトプットを明確にしながら推進することで、顧客の協力が得られやすくセキュリティ対策を計画的に進める事ができます。

（２）セキュリティ対策 実装設計

SMKL セキュリティのどのセルを通過する道筋にするか、セキュリティ対策の範囲と深さについて、顧客と相談しながら顧客特性を踏まえたロードマップを作成し、段階的な実装計画として提案します。

フェーズ 1: セキュリティポリシーの基本設計

- リスク評価とギャップ分析
- セキュリティポリシーの策定・見直しなど

フェーズ 2: セキュリティ強化の運用検討

- 運用体制の確立
- インシデント対応プロセスの整備など

フェーズ 3: 最適化・高度化などの継続推進

- 自動化・効率化の推進
- 継続的改善サイクルの構築など

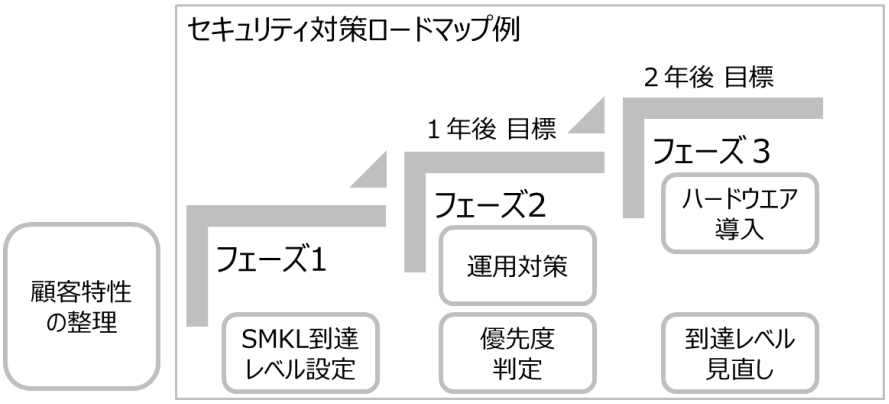

図 6 ロードマップ化イメージ（住友電設オリジナル）

6.2.4 自社ソリューションのポジショニングと戦略的活用（活用３）

インテグレータは、SMKL セキュリティを自社製品・サービスのポジショニングと顧客提案に活用できます。

活用３は、主に製品開発部門が実施することで、営業部門や他部門との意思疎通がしやすくなります。製品販売においては、社内や顧客折衝での認識のずれが少なくなるなどのメリットがありますので、プロセス１、２を行う事をお勧めします。

プロセス３については、包括的な提案を行いたいインテグレータが取り組んでみると良いと思います。

プロセス１：ソリューションマッピングによる価値明確化

自社が提供する製品・サービス・ソリューションを SMKL セキュリティ上にマッピングすることで、以下のメリットが得られます。

- 各商材がどの段階に対応しているかの明確化　　(社内認識の統一)
- 製品ポートフォリオの強みと弱みの可視化　　(強みを生かした提案)
- 顧客の目標に対する機能・技術の明確化　　(提案力の向上)

プロセス２：自社分析とアライアンスの推進

SMKL セキュリティ上で自社商材とアライアンス企業の商材の対応範囲を可視化することで、以下のビジネス拡大の機会を明確化できます。

- 自社製品・サービスでカバーできていない領域　（製品開発のニーズ把握）
- 他社との協業による補完が必要な領域　（アライアンスの推進）
- 競合との差別化が可能な独自強化領域　（自社優位性の確立）

プロセス３：ワンストップソリューションの構築

顧客にとって理想的なのは、複数ベンダーとの調整を必要とせず、セキュリティ対策に関して予算整合性や一貫性をもって１社が提供してくれることも大きなメリットにつながります。

- 自社グループ内の製品・サービスの組み合わせによる包括的なソリューション提案
- 協業先との戦略的提携によるソリューション範囲の拡大
- マネージドサービスとしての包括的な対策提供など

これらのプロセスを実施する事により、顧客にインテグレータの提供範囲やレベルなどが伝わりやすいことや、営業活動において誤った説明にならないなど自社製品に対する理解度の向上に繋がります。

またインテグレータによるワンストップでのセキュリティ対策提供という新しいビジネス価値を生むことも可能です。

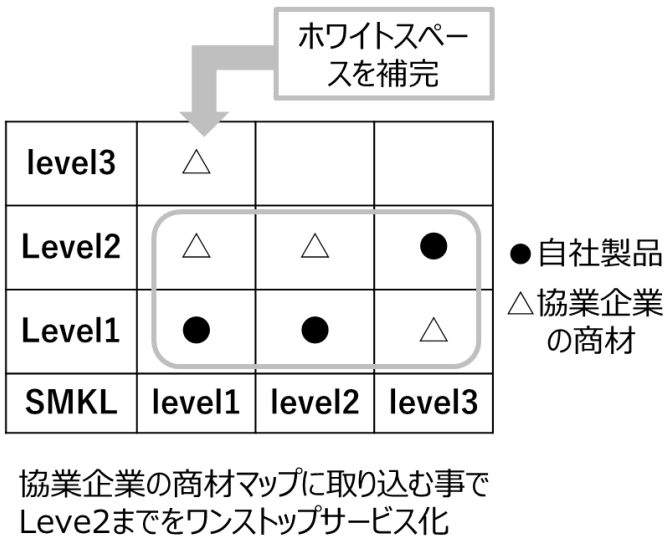

図７ ワンストップサービス化イメージ（住友電設オリジナル）

事例：住友電設のサイバーセキュリティワンストップサービス

https://www.sem.co.jp/inet/solution/csos

6.2.5 提案・導入プロセスにおける SMKL の活用（活用４）

事業活動として顧客との営業活動や社内プロジェクト実行においても、SMKL セキュリティは、現状を可視化し関係者との意識合わせに有効活用できます。

以下、各フェーズでの具体的な利用イメージをご紹介します。

（１）提案フェーズでの活用

- SMKL を用いた現状分析ワークショップの実施
- 可視化された目標に向けた対策手段の提示
- 顧客向けの投資優先度説明など

（２）導入フェーズでの活用

- 各施策の実装状況を SMKL セキュリティで可視化
- 目標達成状況の確認と評価
- プロジェクトの進捗管理と関係者への報告

（３）運用・改善フェーズでの活用

- 定期的なセキュリティ成熟度の評価
- 環境変化に応じたロードマップの見直し
- 継続的改善サイクルの実行管理

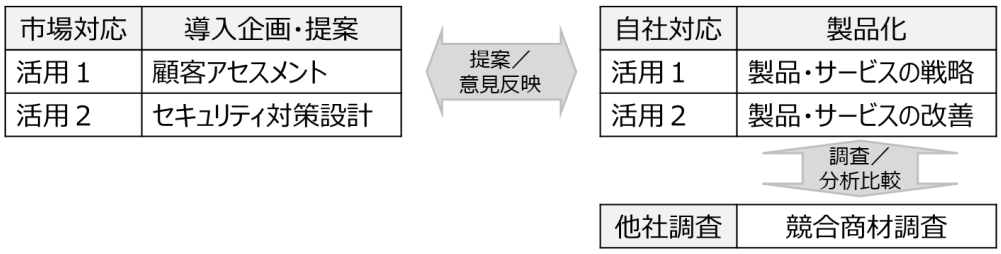

図８　インテグレータの継続的改善（住友電設オリジナル）

6.2.6 セキュリティ対策の顧客提案における３つのポイント

インテグレータの SMKL セキュリティ活用について４つの活用方法を説明しました。上手く活用することで、顧客への訴求ポイントの明確化や、自社製品の見直しなどが進みます。しかし、セキュリティ対策は目に見えないので顧客の導入が進みにくいことがあります。

そこで提案から導入に向けて、自社製品を顧客へ訴求する３つのポイントをご紹介いたしますので、参考頂けますと幸いです。

（1）顧客の経営視点に立った提案

- セキュリティ対策を企業価値や事業価値向上の文脈で説明
- コスト面だけでなく、事業継続性や競争力の観点からの価値提示など

（2）実装可能性への配慮

- 到達すべき理想形ではなく、現実的な対策の提示
- 顧客リソースと優先度を鑑みた段階的な実装計画

（3）顧客との継続的な関係を構築

- 定期的なアセスメントと改善提案の実施
- セキュリティ勉強会や訓練などの提案

6.2.7 おわりに

SMKL セキュリティは、インテグレータにとって顧客との対話を促進し、価値ある提案を行うための強力なツールです。単なるセキュリティ対策の提供者ではなく、顧客のビジネス目標達成を支援するパートナーとしての立場を確立するために、このフレームワークを積極的に活用することが推奨されます。

製造業のデジタル化が進む中で、セキュリティ対策は避けて通れない課題となっています。

インテグレータは、SMKL を活用することで、顧客へより明確で体系的なセキュリティ戦略の提示ができ、共に実行していくパートナーになることが可能と考えます。

７． SMKL セキュリティの活用展開

7.1 製品マッピング

ここまで、「SMKL セキュリティ」の仕様や活用について述べてきましたが、実際に「SMKL セキュリティ」を用いて工場内のセキュリティ対策を講じる場合、どのような対策があるか分かるような資料が必要となります。

そこで、「SMKL セキュリティ」検討チームでセキュリティ対策製品、ソリューションあるいはサービス等を SMKL セキュリティのマトリクスにマッピングすることを試行してみました。

レベルd	対応（緩和、改善） インシデントの拡大を防ぎ、封じ込めを実行する手段を持っている 通信および制御ネットワークを保護ずる手段を講じている	SOC/CSIRTの継続運用 SOC:Security Operation Center CSIRT:Computer Security Incident Rescue Team	・SOCサービス ・CSIRT運用支援サービス ・セキュリティ監視サービス	・CSIRT運用支援サービス ・OT向けセキュリティ監視サービス	・OT向けセキュリティ監視サービス
レベルc	分析（セキュリティリスクの継続的な監視） 自動化された手段を使用して、選択されたサイバーセキュリティ要件への準拠を継続的に評価する ネットワークを監視して、異常や侵害の兆候を検知する	OT-IDSの導入 OT-IDS:Operational Technology Intrusion Detection System	・サイバーセキュリティ・ワンストップサービス ・SOC AI脅威分析基盤サービス／脅威インテリジェンス・資産インテリジェンスサービス ・IPS装置 ・IDS装置 ・セキュアルータ ・UTM装置 ・OT向けIDS装置	・SOC AI脅威分析基盤サービス／脅威インテリジェンス・資産インテリジェンスサービス ・IPS装置 ・IDS装置 ・セキュアルータ ・UTM装置 ・OT向けIDS装置	・SOC AI脅威分析基盤サービス／脅威インテリジェンス・資産インテリジェンスサービス ・IPS装置 ・IDS装置 ・セキュアルータ ・OT向けIDS装置
レベルb	モニタリング（ネットワーク／アセットの状態や識別の可視化） ネットワークを常に監視して新しいハードウェア、ソフトウェアを検出する 稼働状況を検知する仕組みを持っている	NMSの導入 NMS:Network Management System	・監視クラウド ・統合型サイバーセキュリティ監視／侵入検知システム／資産・通信可視化 ・ネットワーク管理ツール（SNMPマネージャ） ・UTM装置 ・OT向けIDS装置	・統合型サイバーセキュリティ監視／侵入検知システム／資産・通信可視化 ・ネットワーク管理ツール（SNMPマネージャ） ・UTM装置 ・OT向けIDS装置	・統合型サイバーセキュリティ監視／侵入検知システム／資産・通信可視化 ・ネットワーク管理ツール（SNMPマネージャ） ・OT向けIDS装置
レベルa	ログの収集 ログデータを自動的に収集し（SNMP,Syslog等）、継続的な監視に利用できるようになっている ポートミラーリング機能を持っている	Managed Switchの導入	・エンドポイントセンサー ・ファイアウォール ・マネージドスイッチングハブ ・IPS装置 ・IDS装置 ・セキュアルータ	・エンドポイントセンサー ・マネージドスイッチングハブ ・IPS装置 ・IDS装置 ・セキュアルータ	・PLC組込型エンドポイントセンサー ・マネージドスイッチングハブ ・IPS装置 ・IDS装置 ・セキュアルータ
みえる化レベル	要件定義 ＼ 管理対象レベル	典型的な対策	レベル1 生産情報系ネットワーク	レベル2 生産管理系ネットワーク	レベル3 制御系ネットワーク

図 8 SMKL マトリクスへの製品マッピング

図 8 の使い方としては、まず横軸の「管理対象レベル」を決め（どこのセキュリティ対策を行いたいか）、その管理対象が現状どの「みえる化レベル」にあるか要件定義を基に判定します。また、管理対象のセキュリティレベルをどこまで向上させるか方針を決定します。その後、この図を参考にセキュリティ対策ソリューションの具体策を検討することになりますが、一つのソリューションで複数の「管理対象レベル」及び「みえる化レベル」に対応するものがありますので注意が必要です。利用する管理対象やみえる化で条件が異なるため、ソリューションの設定等事前に検討する必要があります。

また、本来の SMKL のように、ROI(Return on Investment)を考慮することがセキュリティ分野でも求められると思います。その場合は、IAF の SMKL プロジェクトの Web サイト（SMKL プロジェクト ｜ IAF）にある「SMKL 投資計画書.docx」を用い、「SMKL 投資計画書事例.pdf」を参考に費用対効果を検討することをお勧めします。

なお、この図は「製品マッピング」を試行したものですので、ここに提示したソリューションが全てという意味ではありません。今後も継続してセキュリティ製品、サービス、ソリューションを追加あるいは統合していく予定です。

7.2 成熟度点数化の試案

7.2.1 本章の位置づけ

本章では、セキュリティ対策の成熟度を可視化する指標である SMKL を活用し、現状のレベルを定量的に評価する方法について 1 つの試案を紹介します。

定量的な評価を行うことは、多岐にわたる関係部署間、複数にちらばる拠点間で、俯瞰的にセキュリティ対策の現状のレベルを把握し、将来目標とすべきレベルについて明確な共通認識を持つことを促します。

なお、定量的評価の手法は様々考えられるため、本試案は一つの参考として取り扱いください。

7.2.2 基本的な考え方

試案を紹介する前に、試案で参考としている IEC 62443-4-1 で述べられている maturity model(成熟度モデル)と IEC 62443-3-3 や 4-2 などで述べられている foundational requirements(FRs)について紹介します。【5】【6】【7】

maturity model では、表 5 に示すとおり 4 段階の maturity level が定義されており、IEC 62443-4-1 の 47 要件に対し、組織がプロセスや手順を整備し、どの程度、安全な製品を設計し実装することができる態勢ができているかどうかを定義するためのベンチマークを提供します。

Maturity model は、製品を設計および実装など製品の開発ライフサイクルへの適用を想定したモデルですが、本試案では、この maturity model の考え方を拡大・準用します。

表 5 maturity model

Level	IEC 62443-4-1	IEC 62443-4-1 Description
1	Initial	製品サプライヤは通常、アドホックで文書化されていない(または完全に文書化されていない)方法で製品開発を行う。その結果、プロジェクト間の一貫性とプロセスの再現性が不可能になる可能性がある。
2	Managed	このレベルでは、製品サプライヤは文書化された方針(目的を含む)に従って製品の開発を管理する能力を有する。製品サプライヤはまた、プロセスを実行する担当者が専門知識を持ち、訓練され、またはそれを実行するために書面の手順に従う。 ただし、このレベルでは、組織はすべての書面によるポリシーに準拠した製品を開発した経験がない。これは、組織がこの文書に準拠するようにその手順を更新したが、まだすべての手順を実際に実施していない場合に当てはまる。 成熟度レベル2に反映されている開発規律は、ストレス時でも開発慣行が再現可能であることを保証するのに役立つ。これらの慣行が整ったら、それらの実行は文書化された計画に従って実行され管理される。 注：このレベルでは、CMMIとIEC 62443-4-1の成熟度モデルは基本的に同じであるが、IEC 62443-4-1はプロセスの定義/形式化と実行(実施)の間にかなりの遅れがあることを認識している。 従って、CMMI-DEVレベル2の実行関連の側面はレベル3に延期される。
3	Defined (Practiced)	レベル3の製品サプライヤの実績はサプライヤの組織全体で再現可能であることを示すことができる。プロセスは実践されており、これが発生したことを示す証拠が存在する。 注：このレベルでは、CMMIとIEC 62443-4-1の成熟度モデルは基本的に同じであるが、CMMI-DEVレベル2の実行関連の側面がここに含まれている。従って、レベル3のプロセスは、サプライヤが少なくとも1つの製品に対して実施したレベル2のプロセスである。
4	Improving	このレベルでは、パート4-1はCMMI-DEVレベル4と5を組み合わせたものである。適切なプロセスメトリクスを使用して、製品サプライヤは製品の有効性と性能を管理し、これらの分野で継続的な改善を示す。

参考: IEC 62443-4-1 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements を基に筆者訳・加筆

また、foundational requirements は、IEC 62443-3-3 や 4-2 で産業オートメーションおよび制御システムにおける基本的で重要なセキュリティ要件として表 6 に示す 7 つの要件が定義されています。

foundational requirements は、産業オートメーションおよび制御システムに対するセキュリティ要件ですが、本試案では、この foundational requirements の考え方を拡大・準用します。

表 6 foundational requirements

IEC 62443-4-2 FRs	要件	機能例
Identification and authentication control (IAC)	識別/認証制御	ユーザ認証、アカウント管理など
Use control (UC)	使用制限	アクセス制御、イベントログ生成など
System integrity (SI)	システムの完全性	データ改ざん防止など
Data confidentiality (DC)	データの機密性	データ漏洩防止など
Restricted data flow (RDF)	データフローの制限	ネットワークのセグメント化など
Timely response to events (TRE)	イベントへのタイムリーな対応	監査ログアクセス制限など
Resource availability (RA)	リソースの可用性	バックアップなど

参考： IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
を基に筆者訳・加筆

ここからは、maturity model や foundational requirements をどのように拡大・準用し、成熟度を点数化していくかの考え方を「Level a ログの収集」を例にとって説明します。(図 9 参照)

「Level a ログの収集」を実現する対策として(A)を実施していると仮定します。

大まかな考え方としては、対策(A)に対して評価対象範囲における

①対策(A)の導入状況

②対策(A)の 管理・運用状況(成熟度)

の観点で点数化を行います。

①に関して、対策(A)の導入状況をそれぞれ「未導入(0.0)」、「一部導入(1.5)」、「導入済(3.0)」(カッコ内の数値は配点例)と定義し、評価対象範囲における導入状況を評価します。

②に関して、対策(A)の 管理・運用状況(成熟度)として、対策(A)について、foundational requirements で定義される 7 つのセキュリティ要件がそれぞれ管理・運用されているかを評価します。

評価においては、maturity model を参考として「未管理/その場しのぎ(0.0)」、「ルール化している(1.0)」、「運用している(2.0)」、「システム更新に合わせて見直ししている(3.0)」(カッコ内の数値は配点例)と定義し、7 つの要件それぞれについて評価し、それぞれの和を求めます。

①に関して導出された導入点と、②に関して導出された成熟度点を乗じることで、点数化を行います。

以上の説明内容を図 9 に示します。

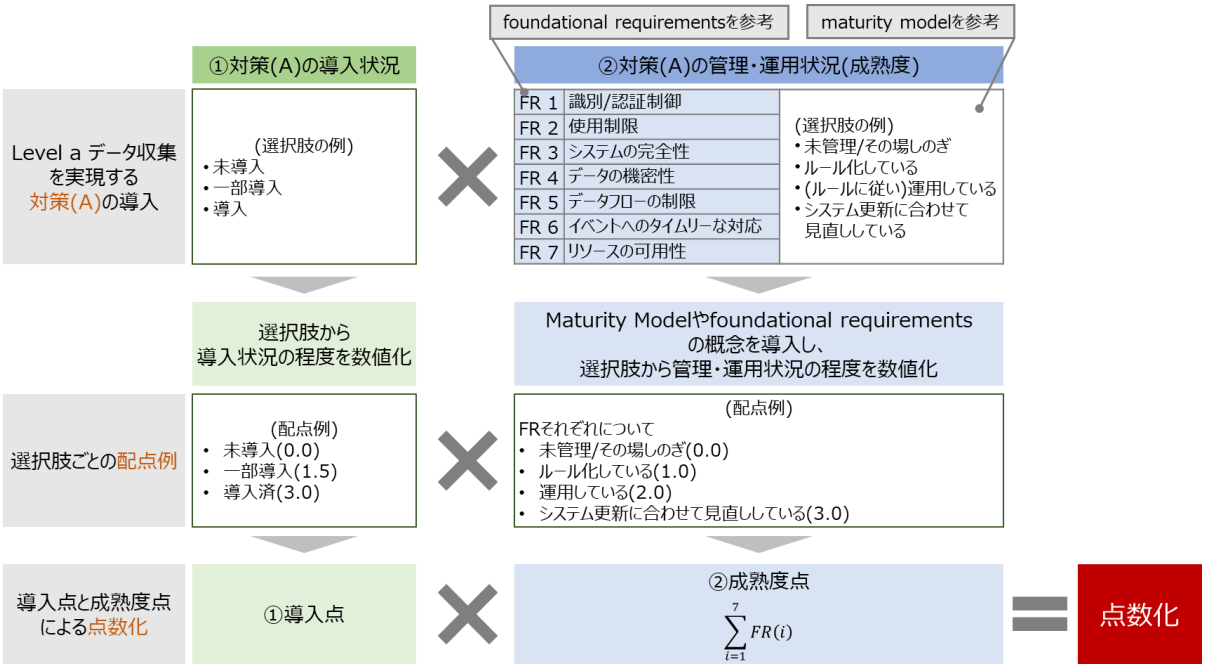

図 9 点数化の考え方

7.2.3 点数化試案

本項では、7.2.2 で対策(A)とした対策をマネージドスイッチと仮定して点数化試案を示します。

図 10 に示すように、①対策(マネージドスイッチ)の導入状況、及び②対策(マネージドスイッチ)の管理・運用状況(成熟度)の観点で評価を進めます。

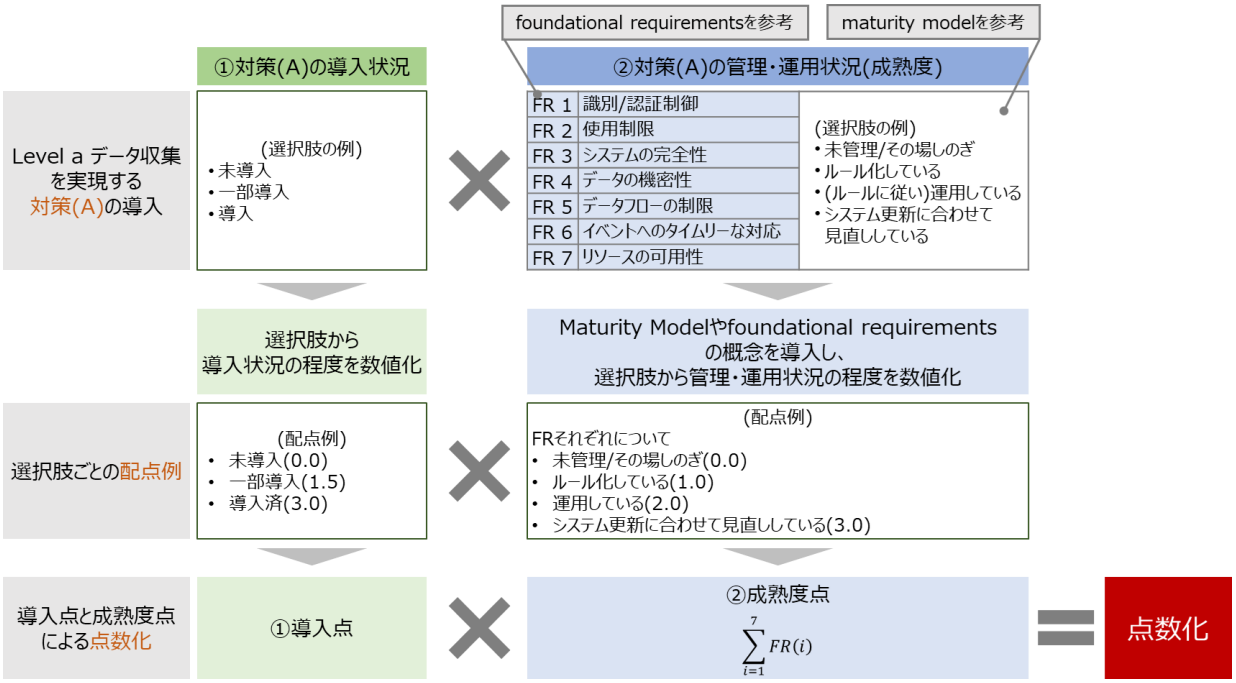

図 10 点数化の試案

【評価項目及び選択肢/配点の作成】

①対策(マネージドスイッチ)の導入状況の評価項目を定めます。図 10 の例示では、「対策(マネージドスイッチ)は導入されているか？」という評価項目を定めたとします。併せて、導入状況の程度に応じた配点を定めます。

また、②対策(マネージドスイッチ)の管理・運用状況(成熟度)について、FR1～7 それぞれの観点に対する評価項目を定めます。本項では、図 10 に示す評価項目を定めたとします。併せて、管理・運用状況に応じた配点を定めます。

【評価の実施】

① 対策(マネージドスイッチ)の導入状況の評価項目に対して、評価対象範囲における評価を実施します。図 7.3 の例示では、仮に対策が一部導入されているケースを想定すると、「一部導入(1.5)」(カッコ内の数値は配点例)という評価が得られます。

また、②対策(マネージドスイッチ)の管理・運用状況(成熟度)について、FR1～7 それぞれの観点に対する評価を実施します。図 10 の例示では、評価項目に対する管理・運用状況として、「未管理/その場しのぎ(0.0)」、「ルール化している(1.0)」、「運用している(2.0)」、「システム更新に合わせて見直ししている(3.0)」(カッコ内の数値は配点例)の中から、評価結果を得たと仮定します。

【点数化の実施】

① 対策(マネージドスイッチ)の導入状況については、評価結果に対応する点数そのものが点数となります。図 10 の例示では、1.5 点となります。

また、②対策(マネージドスイッチ)の管理・運用状況(成熟度)については、FR1～7 それぞれの評価結果に対応する点数の和を計算します。図 10 の例示では、10.0 点となります。

最後にそれぞれの点数を乗じた値を求めます。これが最終的な評点となります。図 10 の例示では、15.0 点です。

7.2.4 点数化における留意点

7.2.3 の例示では、15.0 点という値が得られましたが、この値自体には特段の意味を持ちません。このため、値自体の高低に一喜一憂することなく、同じ評価尺度に基づき継続的に評価を行い、目指すべき成熟度に達成するための改善を行うことが肝要であることにご留意ください。

7.2.5 活用方法の例

前項までで説明した点数化試案に基づき、

・複数拠点で評価を行い、高評点の拠点の取り組みを分析し、取り組みの好事例を他の拠点にフィードバックする

・目標とする評点を定め、定期的に評価を実施しながら目標との差について分析を行うことで強化する分野(FRs)を定め改善を図る

といった活用方法が考えられます。図 11 に活用イメージを示します。

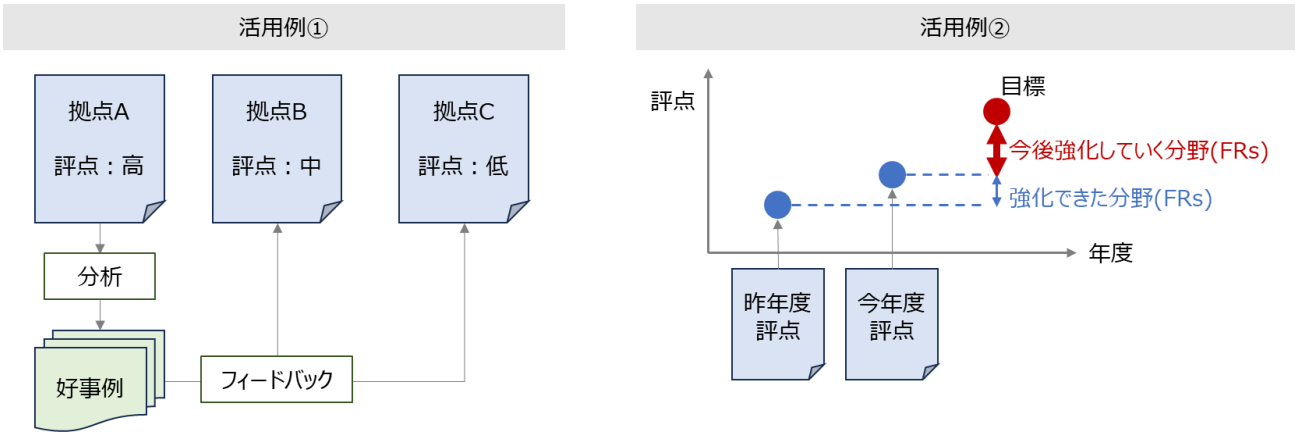

図 11 活用例イメージ

8. まとめ

8.1 現状での「SMKL セキュリティ」のまとめ

本白書では、現時点における「SMKL セキュリティ」について、その策定背景と目的、仕様定義を説明するとともに、具体的な活用事例を紹介しました。さらに応用展開として、「製品マッピング」および「成熟度点数化の試案」を提示し、現場での実用性を高める内容を盛り込みました。

本書における「SMKL セキュリティ」は、工場内ネットワークのセキュリティに特化し、分かりやすさ・使いやすさを重視したコミュニケーション・ツールとして設計されています。その検討にあたっては、SMKL の仕組みと特長を積極的に活用しました。

「SMKL セキュリティ」の主な目的は、製造現場で実際に活用可能なセキュリティ評価指標を提供することにあります。ただし、技術的な厳密性については一定の簡略化を行っているため、詳細な効果測定には IEC 62443 や NIST Cybersecurity Framework など、国際的な基準との併用を推奨します。すなわち、SMKL セキュリティは、セキュリティ対策の導入初期における現状把握や改善方針の検討に適しており、具体的な技術検証には IEC 62443 等の標準を活用するという使い分けが有効です。また、対策実施後も継続的な状況の観察・監視は、セキュリティ維持において極めて重要であり、そのためにも簡易かつ直感的な指標の存在が不可欠です。

図 12 では、SMKL セキュリティを用いて工場ネットワークのセキュリティを確保する際の留意点を示しています。多くの製造現場では、製造品目の変更、品質向上、効率化などに伴い、ネットワークや製造システムが常に変化しています。そのため、一度セキュリティ対策を講じて成果を得たとしても、こうした変化によりセキュリティ環境が変動する可能性を常に考慮する必要があります。特に、縦軸で示される「みえる化レベル」については、継続的な評価が求められます。

さらに、セキュリティ分野では新種のウイルスなど予測困難な脅威が突発的に発生する可能性があり、これまでの対策が無効化されるリスクも存在します。したがって、継続的な監視と評価は不可欠です。新たな脅威への対応においても、まずはレベル a のログの収集によって現状を把握し、脅威の有無を確認したうえで、既存の対策が有効かどうかをレベル a からレベル d まで再評価する必要があります。

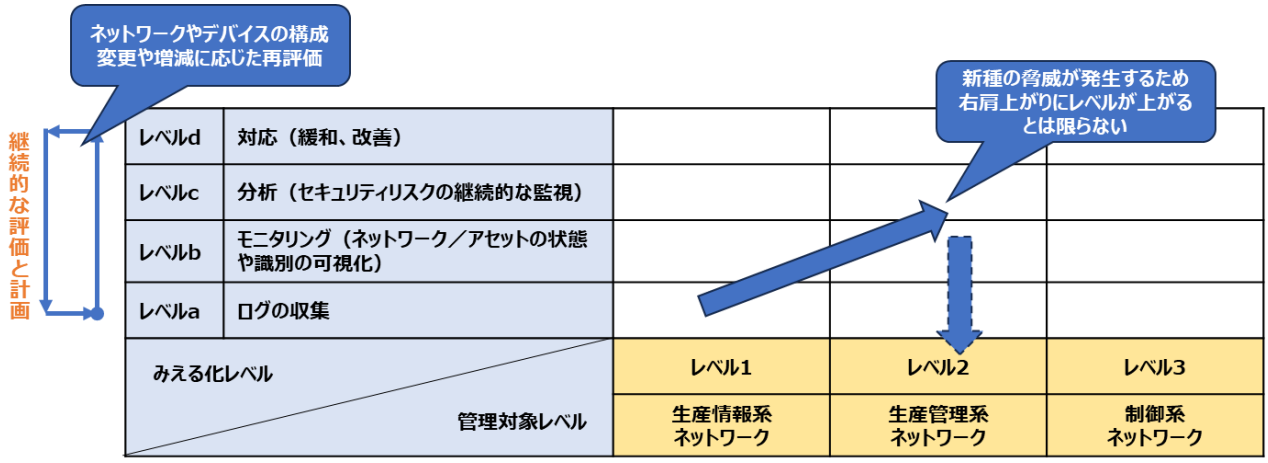

図 12 SMKL セキュリティマトリクスの使い方

8.2. SMKL セキュリティの今後の対応

8.2.1 SMKL セキュリティの展開

SMKL セキュリティの将来を考えるうえで、本白書で取り上げた「工場ネットワークのセキュリティ」だけでなく、以下のような広範な視点から定義を見直すあるいは新たに定義することを検討しています。

① エンドポイント機器（PC やセンサーなど）のセキュリティ（→管理対象レベル 3）

② サプライチェーン全体のセキュリティ（→管理対象レベル 4 を追加）

③ 工場施設などの物理的なセキュリティ（→みえる化レベルの変更）

④ 認証・暗号化の仕組み（→みえる化レベルの要件を変更）

⑤ セキュリティ人材の育成、教育、組織体制の整備（→全面見直し）

⑥ IT/OT 統合などの新たな概念へ対応できる指標（→要検討）

⑦ セキュリティ KPI の定義とそれに基づく SMKL セキュリティの活用方法（→要検討）

ここでは、⑥「IT/OT 統合などの新たな概念へ対応できる指標」について、SMKL セキュリティの観点から考察します。

8.2.2 セキュリティ環境の変化

製造業ではスマートファクトリーの推進が重要課題となっており、各社がその実現に取り組んでいます。これに伴い、OT（制御技術）と IT（情報技術）の統合や、モジュール型・クラウド対応アーキテクチャの導入、モバイルデバイス（スマートフォンやタブレット等）や IoT デバイスの活用などが今後顕著になると予想されています。それにより、従来とは異なるセキュリティ対策が求められるようになることが想定されます。また、セキュリティ対策そのものも本白書で用いた階層

防御ではなく、ゼロトラストのような新たな概念がOTにも適用されることが予想されています。これらのことに対して、SMKLセキュリティも対応していく必要があります。

まず、上記のような環境変化は具体的にどのような変化を生じるのかを考察します。考えられる変化としては以下のようなことが挙げられます。

① 企業IT（ERP等）と現場OT（PLC、SCADA、MES等）が統合され、データと制御が双方向に連携する。

② MES、SCADA、ERPなどの機能がモジュール化され、標準化されたインタフェースで相互接続される。それにより、柔軟にモジュールを組み合わせる設計思想が生まれる。

③ ERP、MESがクラウドベースで運用される。（クラウドファースト）

④ センサーや装置の近傍で推論を行うエッジAIの活用が進む。

⑤ モバイルデバイスやIoTデバイスによる設備の状態監視、在庫管理や品質管理・検査記録などがさらに普及する。リモートでの作業を可能とするために、有線ばかりではなく無線の活用も進む。

これまでのISA-95では、隣接する階層とのみ通信を行うという前提でした。しかし、上記の5つの変化によって、そうではないデータの流れが生じることが分かります。①では、レベル3とレベル4の垣根がなくなります。②でも、レベル3とレベル4の間の垣根がなくなると想定できます。また、③ではレベル3とレベル4の機能要素が外部に出てしまいます。さらに、④や⑤ではレベル1からレベル3、レベル4あるいはクラウドへ直接データが送信される、あるいはその逆のデータフローも生じます。

このような変化に対して、SMKLセキュリティとしてはどのように対応すべきか大まかな検討を試みました。

8.2.3 SMKLセキュリティの多層防御モデル

SMKLセキュリティでは、工場内部を複数の層（SMKLセキュリティマトリクスの横軸）に分け、それぞれの層に対して個別のセキュリティ対策を講じることで、全体の成熟度（SMKLセキュリティマトリクスの縦軸）を定義しています。これは「多層防御」によって重要な機器やデータを守るという考え方です。

しかし、最近のインシデントでは以下のような人的・運用的な要因が原因となるケースが多く見られます：

①工場内での不正操作や誤操作

②セキュリティ機器の設定ミス

③不正な媒体・機器の接続

④権限情報の漏洩

ネットワーク外部からの攻撃に加え、これら内部要因において工場内ネットワークに侵入された後、内部で自由にアクセスされてしまうリスクが大きな問題となっています。

8.2.4 ゼロトラストという新たな考え方

こうした課題に対し、IT 分野では「ゼロトラスト」（Zero Trust）という新しいセキュリティモデルが注目されています。ゼロトラストでは、工場の内部と外部を区別せず、すべての機器やアプリケーションに対して、通信のたびに認証と検証を行います。

図 13 では、従来型の「境界防御」を城と堀に例え、ゼロトラストを「城内にも警備員がいる」状態として説明しています。つまり、城（工場）に入った後も、常に身分証の確認や行動のチェックが行われ、自由に動けない仕組みです。

ただし、ゼロトラストの導入には以下のような課題もあります：

①環境構築・運用に時間とコストがかかる

②認証手続きが煩雑になり業務効率が低下する可能性

③生産性や利便性への影響

④レガシーシステムでは、ゼロトラストに不可欠なコンポーネントを実装する能力が不足

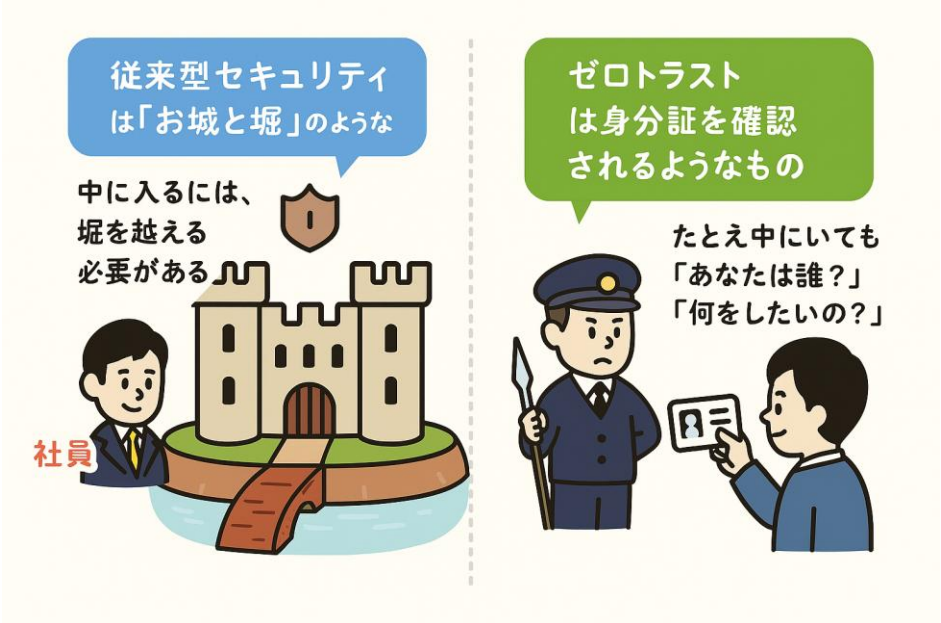

図 13 従来型（境界防御型）とゼロトラストの違い

そのため、工場全体に一斉導入するのではなく、重要工程をセグメント化し、部分的に導入する形が現実的です。SMKL セキュリティとしては、こうした新たな概念に向けた要件定義や対象範囲の明確化が求められます。

8.2.5 新たな SMKL セキュリティの検討

8.2.2 から 8.2.4 で述べた工場におけるセキュリティ環境の変化をまとめると、以下のようになります。

（1）データフローとして、片方向ではなく双方向の通信を考慮する必要がある。

（2）データフローとして縦方向だけではなく、横方向の展開も考慮する必要がある。

（3）データが階層を跨いで伝送されることを考慮する必要がある。

（4）ゼロトラストのように、階層を意識しないセキュリティ対策も考慮する必要がある。その一方で、従来の多層防御採用の対象もあるため両方に対応できる必要がある。

このような環境変化に対して、ISA-95 は 2025 年版（ANSI/ISA-95.00.01-2025）でそれらへの対応を公開しています。【5】また、ユーザー主導のプロセスオートメーションの標準化団体である NAMUR においても、NOA（NAMUR Open Architecture）として、従来のプロセスオートメーションに新たな通信経路を追加することで、既存設備に影響を与えずにデータ活用を可能にするアーキテクチャを発表しています。【6】両活動では、共に階層構造を用いつつ柔軟性と拡張性を併せ持つようにしています。今後、このような活動・普及が盛んになってくるものと思われます。

そうした中、SMKL セキュリティはどのように対応すればよいでしょうか？ISA-95 に基づいた階層構造を継承してうまくセキュリティ対策の成熟度を表現できるでしょうか？これまでの物理的階層ではなく、論理・機能的階層としてこれを横軸に据え、その論理・機能的階層のネットワークセキュリティの要件を縦軸に取ることで解決を図れるのではないかと考えています。このようにすれば、物理的階層を跨ぐ通信やゼロトラストにも対応可能になる可能性があると考えます。

今後も、製造業の進化に合わせて、8.2.1 の①～⑦の項目に対して、優先順位を立てて SMKL セキュリティのアップデートを継続していく方針です。

以上

9. 参考文献・参照

【1】 IBM Security, Threat Intelligence Index 2025, https://www.ibm.com/downloads/documents/us-en/1227cc9e83cb97ae（2025 年 9 月 22 日時点）

【2】 IBM Security, Cost of a Data Breach Report 2023, https://www.ibm.com/reports/data-breach（2025 年 9 月 22 日時点）

【3】 European Union, Directive (EU) 2022/2555 on measures for a high common level of cyber-security across the Union (NIS2 Directive), 2023.

【4】 NIST, Guide to Industrial Control Systems (ICS) Security, SP 800-82 Rev.3, 2023.

【5】IEC 62443-4-1 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements (Edition 1.0 2018-01)

【6】IEC 62443-3-3 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels (Edition 1.0 2013-08)

【7】IEC 62443-4-2 Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components (Edition 1.0 2019-02)

【8】Industrial Cyber, New ISA-95 standard enhances IT/OT convergence for industrial automation, April 14,2025, https://industrialcyber.co/regulation-standards-and-compliance/new-isa-95-standard-enhances-it-ot-convergence-for-industrial-automation/

【9】NAMUR, NAMUR Open Architecture Overview, https://www.namur.net/fileadmin/media_www/fokusthemen/20200710_NAMUR_NOA_ Overview_EN.pdf

SMKL セキュリティに関する白書
～工場ネットワークのセキュリティ対策レベルの見える化～

発行日：２０２５年１１月２７日

発行者：Industrial Automation Forum(IAF)

制御層情報連携意見交換会（CLiC）　SMKL プロジェクト

筆　者：SMKL プロジェクト・SMKL セキュリティ　サブワーキングメンバー

第１章		朝日奈　弘典（三菱電機）
第２章		長澤　宣和（Moxa Japan）
第３章		植田　信夫（クリエーティブ・コンセプト・システムズ）
第４章	4.1 節	藤島　光城（三菱電機）
	4.2 節	植田　信夫（クリエーティブ・コンセプト・システムズ）
	4.3 節	植田　信夫（クリエーティブ・コンセプト・システムズ）
	4.4 節	植田　信夫（クリエーティブ・コンセプト・システムズ）
第５章		山崎　幸治（NTT ドコモビジネス）
第６章	6.1 節	種田　大地（アライドテレシス）
	6.2 節	安藤　公詔（住友電設）
第７章	7.1 節	植田　信夫（クリエーティブ・コンセプト・システムズ）
	7.2 節	朝日奈　弘典（三菱電機）
第８章		植田　信夫（クリエーティブ・コンセプト・システムズ）

IAF 事務局：城下　哲郎（一般財団法人 製造科学技術センター内）
連絡先：〒105-0004 東京都港区新橋 3-4-10 新橋企画ビルディング 4 階
e-mail ：jim-iaf@mstc.or.jp
TEL　：０３－３５００－４８９１
URL　：http://www.mstc.or.jp/iaf/