

デジタル化する工場のサイバーセキュリティ

工場(OT)領域におけるセキュリティ人材



PwCコンサルティング合同会社 ディレクター 上村 益永
PwCコンサルティング合同会社 シニアアソシエイト 河合 菜央

OT(Operational Technology: 生産ラインやシステムの制御・運用技術)環境のセキュリティ確保を行う上で、セキュリティ管理の推進や実行を担う人材の確保は重要な論点です。優れたルールや対策が実装されても、それらを正しく運用し、環境の変化に合わせて最適化できる人材が揃っていないければ、無用の長物と化してしまうことは明白です。今回は、OT環境のセキュリティ確保に必要な人材要件と、そうした人材の獲得戦略について解説します。

1. 主役はセキュリティスペシャリストではない？OT環境に求められるセキュリティ人材とは

セキュリティ人材と聞くと、高度な専門知識や実行能力を有する「セキュリティスペシャリスト」を想像するかもしれませんが、OTセキュリティにおいては、セキュリティスペシャリストが担う役割はごく一部に留まります。

IT／OTに関わらず企業がセキュリティに取り組むためには、ルールや仕組みを建て付けて監督する管理的な役割と、ルールの実現のために技術的対策を実装・運用する役割の両方が必要です。ITとOTで異なるのは、特に技術的な対策を行う際に必要になる知識・スキルの部分です。ITの場合、セキュリティを実装するシステムにおいては標準化された技術が使用されています。一方でOTの場合、自組織の製品生産に特化した設備やシステムが利用されていることが多く、セキュリティ対策の実装・運用のためには、自組織の設備やシステムの技術を理解し、最適化して実装することが求められます。

上記の前提に基づいて、OT環境におけるセキュリティ人材を以下の3種類と定義し、それぞれの要件を整理します。

■ 管理人材

セキュリティのルールや仕組みを建て付け、その実行状況を確認し、改善を推進する人材です。

一般的なセキュリティ管理要件を、自組織の事業や設備の特性を考慮してルールとして最適化した上で監督・推進することが求められるため、セキュリティ管理の基礎知識と自組織の事業や組織に対する深い理解が必要です。

■ 技術人材(OTシステム専門)

OTシステムの設計開発や運用・保守にセキュリティ対策を実装し、遂行する人材です。

OTシステムの設計開発や運用・保守業務にセキュリティ要件を組み込み、運用することが求められるため、同システムとその運用・保守に関する技術的な専門性を有していることを前提に、セキュリティ専門性も備えている必要があります。また、多くの企業・組織ではシステムが各拠点で異なり、運用業務もオンサイトで実施されることが多いことから、本人材は各拠点に配置され、人数も最も多くなります。

■ 技術人材(セキュリティ専門)

セキュリティ監視(Security Operation Center)や高度分析など、技術的なセキュリティ専門業務を遂行する人材です。

セキュリティに関する高度な専門性が必要である反面、事業や設備の専門性はあまり求められません。

図1. 知識・スキル別のOTセキュリティ人材分類



2. 鍵は外部ではなく社内人員の育成。 OTセキュリティの人材獲得戦略とは

前述のように、OTセキュリティ人材の多くには、自社の事業や組織またはOTシステムやその運用・保守に関する専門性が求められます。そうした人材の獲得のためには、外部からセキュリティ人材を登用するのではなく、既に自社の事業や組織またはOTシステムやその運用・保守の専門性を持っている社内人員を活かして、セキュリティ知識をアドオンしていくことが、人材戦略として望ましいと考えられます。また一般的には、高度な専門性が求められるほど、また知識／スキルが標準的であればあるほど、外部リソースを有効活用しやすくなります。自社固有の知識の必要性がない領域においては、アウトソースや外部人員の登用も積極的に検討することが望まれます。

上記の考えをもとに、各人材の獲得戦略を以下のように整理することができます。

■ 管理人材

自組織の事業特性を理解し、OT関連の施策を推進できる立場の人材(社内のOT関係者とリレーションを持つ人材など)に対して、セキュリティ管理に関する基礎的な知識を教育することが効果的です。

管理人材をどのような組織単位で配置していくのか組織のガバナンス戦略に沿って検討することが望ましいと考えられます。(「工場(OT)におけるセキュリティガバナンス」参照)

■ 技術人材(OTシステム専門)

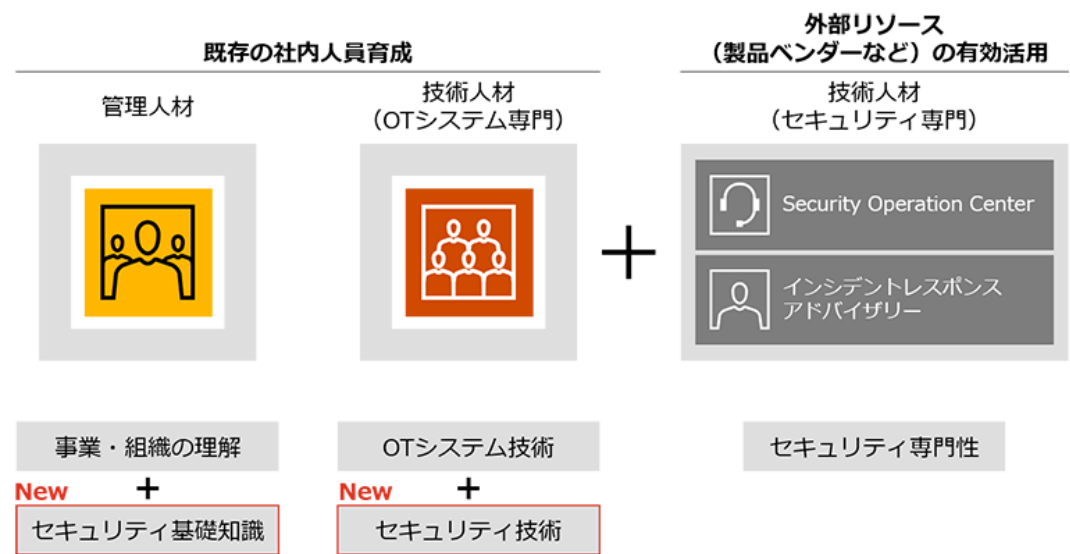
OTシステムやその運用・保守に関する技術的な専門性を持つ社内人材に対し、知識のみならずオペレーションスキルを含めたセキュリティ専門性を教育することが求められます。前述のように、多くの企業では各事業や各拠点独自でOTシステムを実装・運用していることから、本人材は各拠点で育成していく必要があります。

■ 技術人材(セキュリティ専門)

高度なセキュリティ専門性が求められること、また自組織固有の知識の必要性が少ないことから、外部人材の登用やアウトソースを有効に活用できます。また自組織のIT部門で活用している人材のシェアを検討することも、効率的かつ効果的な人材獲得戦略であると考えられます。

図表2もご参考にしていただきながら、それぞれの獲得戦略に沿った教育計画や外部委託計画を検討・実践し、OT環境のセキュリティ確保に努めていただければ幸いです。

図2. 各人材の獲得戦略



お問い合わせ

PwCコンサルティング合同会社
〒100-6921 東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel : 03-6250-1200 (代表) Mail : jp_cyber_inquiry@pwc.com