デジタル化する工場のサイバーセキュリティ

工場（OT）におけるセキュリティガバナンス
～ 現場の実力を重視した管理態勢の構築

PwCコンサルティング合同会社 シニアマネージャー 上村 益永

1. OTセキュリティにおけるガバナンスの重要性

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管理を目指した場合、その統括を担う組織は、OT環境で使用されているOTシステムの構築、運用・保守、および業務利用を担う部門、工場や研究所の物理環境を管理する部門など、工場や研究所で働く従業員を統制する必要性に直面します。

しかし、従来のITセキュリティの管理態勢は、実態として主にオフィスワーカーやIT部門を統制することを目的に設計・運用されてきました。またITセキュリティでは、ITシステムの設定をコントロールしたり、セキュリティ対策製品を導入したりすることで、組織や従業員の統制を一部代替することが可能でした。しかし厄介なことに、OTシステムはその性質上、製品や業務ごとにニッチなシステムが多数存在するため、設定の標準化やセキュリティ対策製品による統制も一筋縄ではいきません。

OTシステムの構築、運用・保守、業務利用を担う従業員に対して、OTセキュリティに関する会社の方針やルールを実現可能な方法で確実に伝達し、定期的に管理態勢を確認し、必要に応じて是正を促す――。こうしたOTセキュリティ管理の一連のプロセスを、既存の管理の仕組みを活用して適切に運用することは、OTセキュリティ管理と既存の管理の性質や対象の違いから難しいと言わざるを得ません。

こうした現実に鑑み、OTセキュリティ管理の実現に向けては、ITセキュリティの管理態勢とは別に、OT独自のセキュリティガバナンスを設計し、実装する必要があります。以後は、OTセキュリティガバナンスの設計・実装（第1段階）、成熟化（第2段階）を実現する上で重要になる論点を解説します。

2. OTセキュリティガバナンスの重要論点

一般に、ガバナンスは、方針・ルール、制度・仕組み、組織・人の3つの手法によって達成されます。OTセキュリティガバナンスにおいても、適切なセキュリティ管理のためにそれらの手法を採用する必要がありますが、その設計や実装においては、OTセキュリティの性質に十分配慮する必要があります。

（ア）制度に軸足を置いたガバナンス構築を

企業におけるOTセキュリティガバナンスは、難しい状況に置かれています。OT環境はあらゆる事業と拠点に存在しますが、企業としては全体で1つのガバナンスによって遍く統制する必要があります。そのため、全体として設定した標準的なルールに基づき、各事業部門や各拠点の自発的努力によって、ルール遵守の達成に向けて運用ルールや手順、管理の仕組みの開発を期待したいところです。

一方で、前述の通り、OTシステムには製品や業務ごとにニッチなシステムが多数存在します。こうしたOTセキュリティというテーマの特殊性・新規性に鑑みると、各事業や拠点が自力でOTセキュリティの目的や適切な手法を正しく理解して、全体で定められたルール通りにセキュリティ管理を実現・実施することが困難であることは想像に難くありません。

こうした状況である以上、OTセキュリティガバナンスにおいては、ルールではなく制度・仕組みに軸足を置くべきと考えます。もちろん全体で標準化されたルールは必要です。ただし、OTセキュリティガバナンスを主導するOTセキュリティの統括組織は、ルールを設定し遵守を促すだけの一方的で形式的なガバナンスの構築ではなく、それを具体的な制度・仕組みに落とし込み、現場の制度・仕組みの実態に鑑みて全体の方針・ルールが対話的に協調する現実的なガバナンスの構築を目指すことが肝要です。

（イ）拠点のケイパビリティを重視する

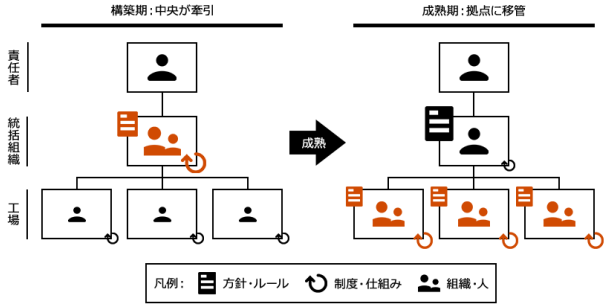
デジタル化やオープン化の進展と共にOT環境の標準化が進んではいるものの、依然として事業や拠点ごとに、固有プロトコルや尊重すべき固有の事情を抱えた環境が多く存在しています。こうした背景を踏まえると、企業におけるOTセキュリティガバナンスのあり方としては、全体で共通のポリシーに基づきながらも、拠点ごとの事情を適切に勘案してセキュリティ管理態勢に落とし込み、実践する姿が望まれます。そのためには、OTセキュリティガバナンスの中核を担うOTセキュリティの統括組織の設計においては、事業部門および拠点が自発的に活動できるように権限を与え、かつ、権限を適切に執行できるだけのケイパビリティを備えさせることが重要です。具体的には、全体の統制を担う中央の要員よりも、拠点のOT環境に精通し、拠点内での管理・運用を担う要員の割合を多くするなどによって、現場におけるセキュリティ管理の実効性を担保することが必要です。また、方針や基準を明確にすることで各拠点が一定の統制の中で裁量を発揮しやすくする、手厚い教育を提供することで立ち上りを支援するといった方策も有効です。

（ウ）成熟度に応じたガバナンスモデルの採用を

セキュリティガバナンスの建て付けから成熟に至る過程を既に経験された企業のセキュリティ担当者は、成熟したセキュリティガバナンスのモデルをOTセキュリティにも適用しようとされるかもしれません。しかし、そうした成熟したモデルは、想定通りに機能しないことが予想されます。セキュリティガバナンスは要員のセキュリティの理解度やセキュリティ管理のための仕組みの整備状況、システム化の程度、守るべき環境の多様性などによる影響を強く受けます。OTセキュリティにおいては、セキュリティの目的や必要性を理解する従業員や技術的な対策が施された環境は少なく、ITセキュリティのように従業員が基礎知識を有しており、さまざまなセキュリティ管理を目的とした制度や仕組みが日常の業務や技術的な対策として埋め込まれている状況とは大きく異なるためです。ガバナンスのあり方に影響する現実のさまざまな要因が未成熟な状態にも関わらず、ガバナンスの設計だけ成熟したものを取って付けると、上手く噛み合わず、機能しないのです。

OTセキュリティガバナンスの整備においては、各々の実情に沿って、その時点で適切なガバナンスのあり方を模索すべきです。通常、ガバナンスの成熟には長期間を要します。例えば、OTセキュリティに取り組み始める時点では、最低限のルールを標準化し全体管理の仕組みと体制を立ち上げ、活動の中で従業員のセキュリティ管理や知識水準の向上や制度・仕組みの拡充・深化を図り、組織のOTセキュリティ管理の成熟に応じてガバナンスのあり方を見直す、というアプローチを取ることで、OTセキュリティガバナンスのあり方を継続的に最適な状態に保つことができます。

図表1：OTセキュリティガバナンスの変遷例



3. OTセキュリティ統括組織が果たすべき役割

上述の通り、組織におけるOTセキュリティ管理の取り組みを主導するOTセキュリティ統括組織は重要な役割を担うことになります。自らはOTセキュリティの必要性を正しく認識し、組織にとって新しい機能となるOTセキュリティの重要性を提唱し、必要なリソースを獲得して取り組みを推進する。そんな役割が期待されます。

経営層や各事業の本社部門に対してOTセキュリティに必要な投資に関する理解を醸成し、各現場で協力を得られるよう後方支援を取り付ける一方で、OTセキュリティの最前線である工場に赴き、本業に集中したい現場に対してセキュリティの重要性とビジネスにおける効用を説いて周ることも重要な活動です。さらに、既存のITセキュリティ体制との役割分担や連携を整理し、OTを含むセキュリティ管理を組織全体で無駄なく、抜け漏れなく実現する必要があります。

これからの時代の重要な経営課題であるOTセキュリティガバナンスにおいて、OTセキュリティ統括組織はまさに八面六臂の活躍が期待され、相応の陣容をもって取り組みに臨むことが求められるのです。

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