# デジタル化する
# 工場のサイバーセキュリティ

pwc

www.pwc.com/jp

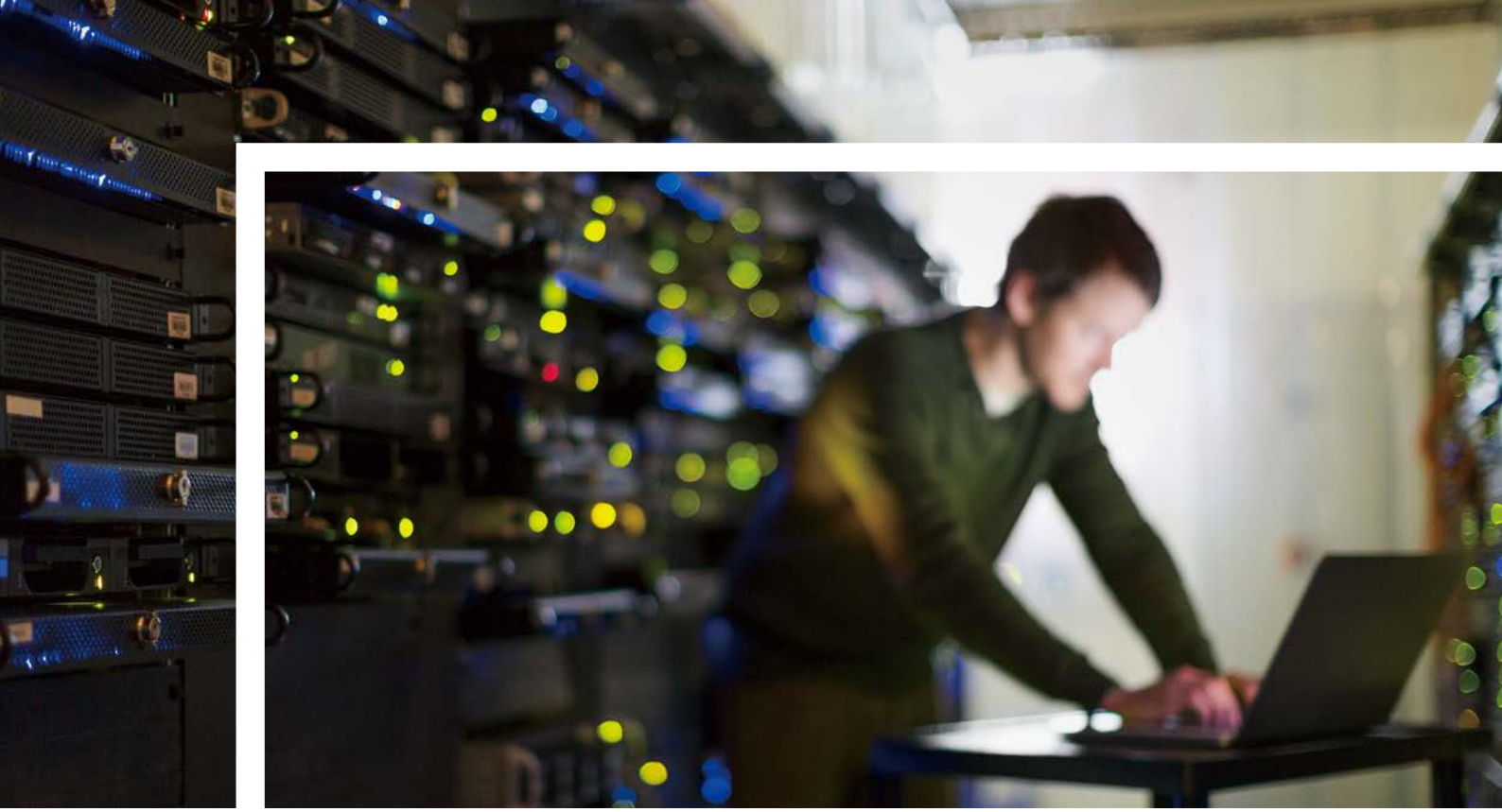
# 目次



# 1 はじめに

デジタル化が進む昨今、サイバー攻撃は企業活動の根幹をなすOT（Operational Technology：生産ラインやシステムの制御・運用技術）環境にまで及んでいます。日本国内においても、工場をはじめとするOT環境でのサイバーセキュリティインシデント（以下、OTセキュリティインシデント）が発生していることは周知のとおりです。PwCは、企業の存在意義すらも脅かすOTセキュリティインシデント、およびその発生を防止するOT環境におけるサイバーセキュリティ（以下、OTセキュリティ）を重要な経営課題と捉えています。

OTセキュリティは知見が不足している傾向にあり、サプライチェーンや製造拠点を抱える企業がその推進に苦労されています。本稿では、企業がOTセキュリティを推進していく際に考えないといけないポイント、観点について解説し、安全・安心な事業推進の一助となることを目指します。



# 2 工場（OT）環境の類型整理とOTセキュリティ

## OT環境の類型整理

### OT環境の大別

OT環境である工場や研究所ではICS（Industrial Control System：産業制御システム）が使用されていることから、OTのサイバーセキュリティは従来の情報セキュリティやITセキュリティとは別の取り組みとして考えられることが一般的です。

OT環境は、大別するとFA（Factory Automation）環境とPA（Process Automation）環境に分類できます。FAは、主に物理的な組み立て・加工などを行うプロセスを自動化することを目的としたシステムからなる環境です。一方、PA環境は、主に化学的な合成・精製などを行うプロセスを自動化することを目的としたシステムからなります。

その他にも、BA（Building Automation）や送電網、通信網など、ICSを使用したサービスシステムは多数あります。しかし、そうした環境はユーザーにサービスを直接提供するために使用されているなど、いわゆる工場や研究所といった企業内部の事業活動に使用される環境とは異なる性質を持つため、ここでは取り扱わないこととします。

なお、本稿はOTセキュリティに係る環境全体の類型化に焦点を当てる目的から、例外が多数存在することは認識した上で、一般的な状況を前提としています。

### FA環境とPA環境の特徴と主な違い

OTセキュリティを大局的に考えると、全ての環境で可用性が最優先であるといった誤解や、構成変更が難しいことから技術的な対策は何もできないといった錯覚に陥ることがあります。しかし、実際のOT環境は個々に性質が異なり、OA（Office Automation）環境のように全体として1つの傾向を語ることは難しいと言えます。FA環境とPA環境に大別するだけでも、一般に下表（図表1）のような違いがあります。

**図表1：OT環境の類型整理**

| カテゴリ | 指標 | 参考）OA環境 | FA環境 | PA環境 |
|---|---|---|---|---|
| 機能や実状 | 構成変更の容易性 | 容易 | 比較的容易 | 困難 |
| | 要求される出力品質精度 | 低（ベストエフォート） | 高 | 中 |
| | 規格 | TCP／IP | TCP／IP＋<br>固有プロトコル | TCP／IP＋<br>固有プロトコル |
| | 運用体制 | IT部門で全社的に<br>一元化 | 製造部門ごとに<br>細かく分散 | 運用ベンダーにて<br>一定程度一元化 |
| セキュリティ | 守るべき対象 | 情報資産 | プロセスおよび<br>プロセスを担う設備 | プロセスおよび<br>プロセスを担う設備 |
| | 最優先される<br>セキュリティ要素 | 機密性 | 可用性 | 完全性 |
| | セキュリティ侵害時の<br>影響 | データの損失 | 環境・安全・製品・<br>設備の侵害 | 環境・安全・製品・<br>設備の侵害 |

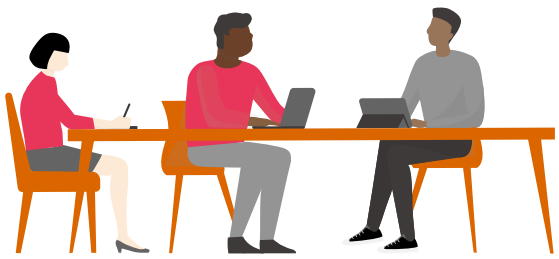
出所：PwC作成

## OTセキュリティにおける留意点

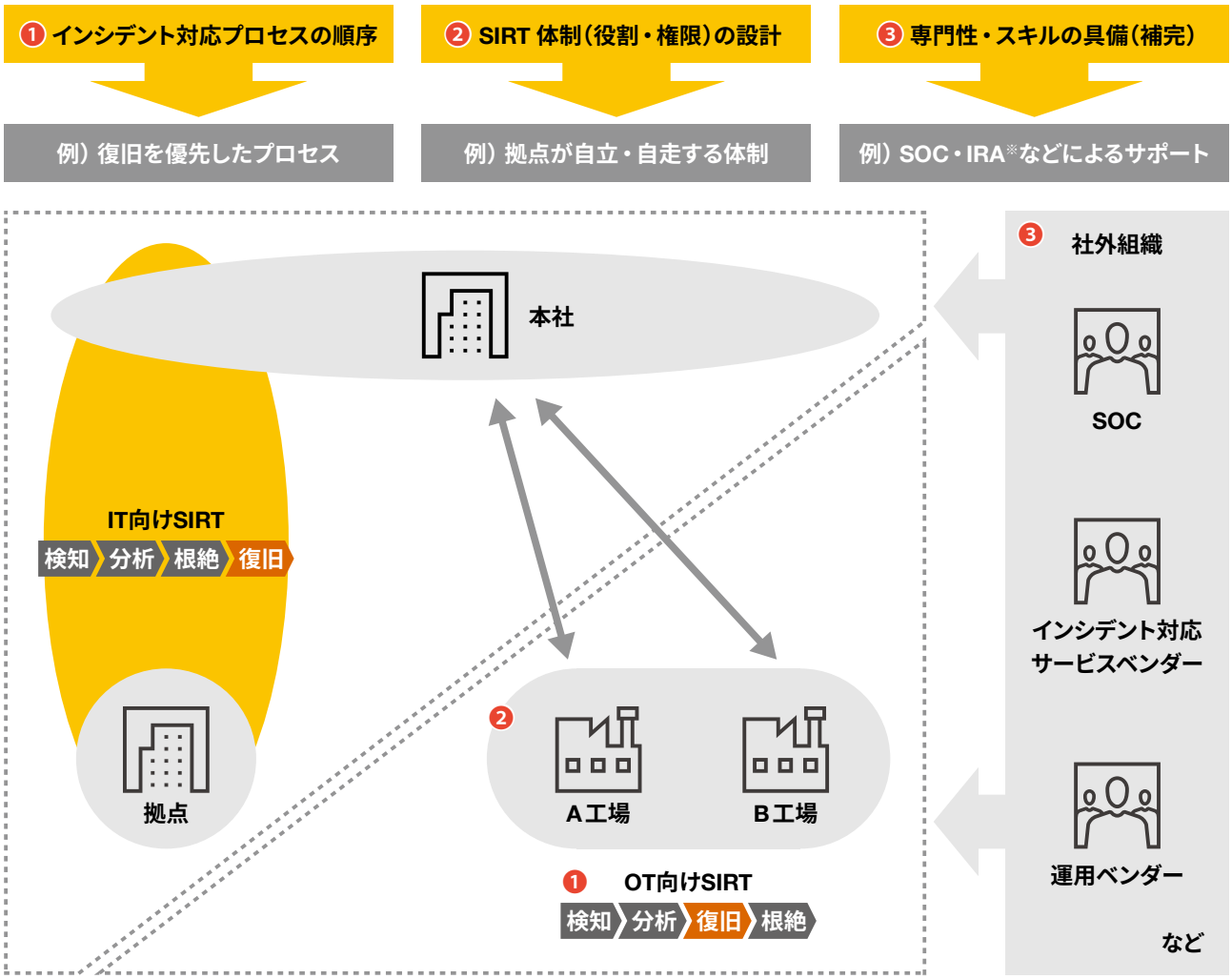
日本企業の多くは、これから自社のOTセキュリティ管理のあり方の検討（体制、プロセス、技術的対策）と、あり方の実現に向けた施策（制度や仕組み、対策製品の導入）の企画を進められることでしょう。その際、自社で保有する個々のOT環境が目指している機能や実際の状況を適切に理解するとともに、従来の情報セキュリティ・ITセキュリティの考え方とOTセキュリティの考え方の違いを認識することが重要です。

例えば、インシデント対応体制のあり方を考えてみましょう。プロセス面では、OT環境の特性に鑑みると、設備の稼働の維持または復旧を優先したいため、被害を受けた設備の隔離を前提としたプロセスではなく、稼働継続を前提としたプロセスとする必要があります。次に体制面では、OT環境はITのようにシステムやその管理が一元化されていないことから、状況把握や初動対応、切り分け、場合によってはトリアージなども、インシデントが発生している拠点の体制・人員で実施する必要があります。

しかしながら、こうした拠点の体制・人員は、本来セキュリティ管理を目的としたものではないため、セキュリティの専門性が経験・スキル面ともに不足します。その中で、トリアージや案件の切り分けといったセキュリティの知識・スキルを要するプロセスを有効に機能させるためには、拠点の体制・人員をサポートする外部サービスの利用や簡易的な判断基準の整備などの検討も必要です（図表2）。



図表2：インシデント対応体制における留意点と検討例




※SOC：Security Operation Center
IRA：Incident Response Advisory

出所：PwC作成

# 3 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セキュリティ管理体制の構築

### OTセキュリティにおけるガバナンスの重要性

OT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。

従来のITセキュリティの管理体制は、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、定期的に管理体制を確認し、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体制とは別に、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となる論点を解説します。

## 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つの手法によって実現されます。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、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。

### 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た運用ルールや手順、管理の仕組みの開発を期待したいところです。

一方で、前述のとおり、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どお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。

### 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ともに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体制に落とし込み、実践する姿が望まれます。

そのため、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がりを支援するといった方策も有効です。

### 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立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、想定どお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かかわらず、ガバナンスの設計だけ成熟したものを取って付けると、うまく噛み合わず、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意識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ための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。

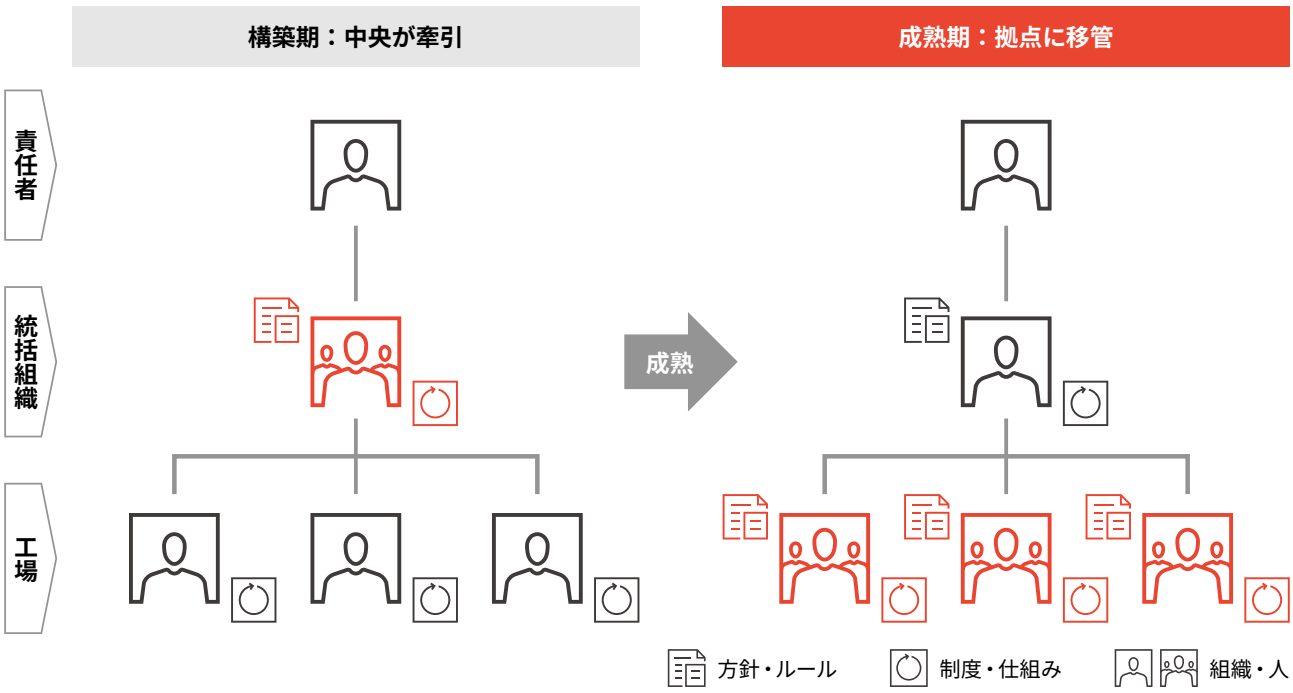
## OTセキュリティ統括組織が果たすべき役割

上述のとおり、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。そのため自らは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まわ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。

これからの時代に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むことが求められるのです。

**図表3：OTセキュリティガバナンスの変遷例**




出所：PwC作成

# 4 ATT&CK for ICSを利用した攻撃者視点のOTセキュリティ評価

## 攻撃者視点のOTセキュリティ評価の必要性

なぜ攻撃者視点でOTセキュリティを評価することが必要なのでしょうか。その理由として以下の3点が挙げられます。

### OT環境の制約から離れた視点の獲得

OT環境はOA環境と比べて制約事項が多く、セキュリティ対策が制限されている現実があります。例えば、設備の稼働に影響する可能性がある対策では実施できないレガシーOSが残存しており、最新のセキュリティ対策が適用できないなどのケースが考えられます。しかし、攻撃者は対策する側の事情は考慮せず、対策に穴があればそこから侵入し攻撃するのです。

攻撃者の視点を持ち、OT環境の制約事項をいったん無視してOTセキュリティを評価することで、対策すべき脆弱な箇所を特定することができます。その上で、脆弱な箇所に対策を追加する、直接対策できない場合は攻撃の経路上で対策するなど、制約の範囲で有効な対策をとることができれば、防御力の向上につながります。

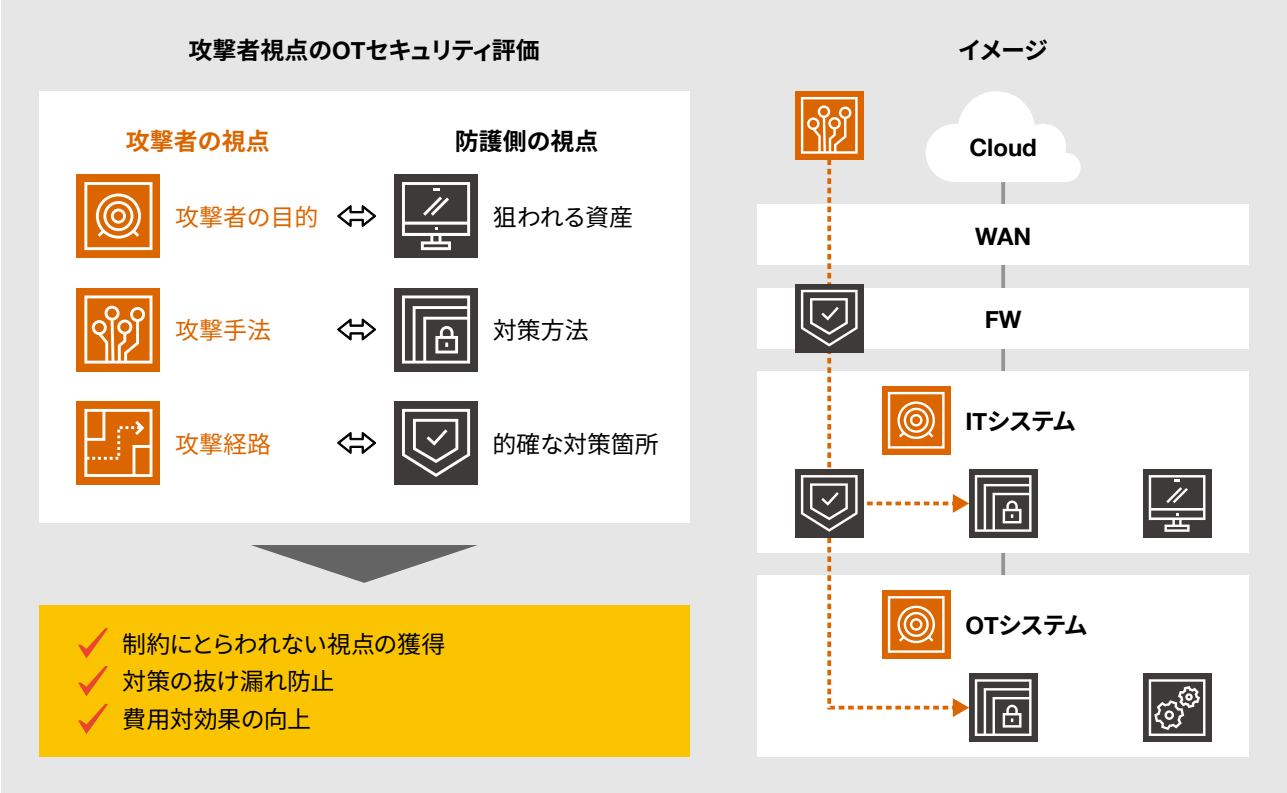
### 対策の抜け漏れ防止

もしセキュリティ対策を行う際に想定するサイバー攻撃に抜け漏れがあれば、適切な対策を行うことはできません。自社のOT環境で発生する可能性のあるサイバー攻撃を網羅的に想定した上でOTセキュリティを評価することにより、対策の抜け漏れを防ぎ、有効な結果を得ることができます。

### 費用対効果の向上

セキュリティ対策は、スコープや効果の異なる複数の対策を組み合わせて実装されます。全てのサイバー攻撃に対して高いレベルでの対策をとるためには、守りたい対象の全てに対して十分すぎるほどのセキュリティ対策を実装することとなり、費用や時間の制約などから現実的ではありません。そこで、攻撃者の視点で攻撃のしやすさ、攻撃による成果を考慮しながら対策を評価することで、より必要性の高い対策や重点的に守るべき攻撃経路を把握することができ、費用対効果を上げることが可能です。

**図表4：攻撃者視点のOTセキュリティ評価の必要性**




出所：PwC作成

## 評価における留意点

ここからは、攻撃者視点でのOTセキュリティ評価を行う上で留意すべきポイントを紹介します。

### 攻撃シナリオの網羅性の担保

何よりもまず、OT環境で起こり得るサイバー攻撃を網羅的に把握することが必要です。サイバーセキュリティに関する信頼に足る専門組織・機関が、OT環境におけるサイバー攻撃の一覧を公開しています。これを利用することにより、コストをかけずに網羅性を担保することができるでしょう（その代表例である「ATT&CK for ICS」について後述します）。

### 評価の正確性の担保

OT環境は個々に性質が異なるため、発生する可能性のあるサイバー攻撃も環境ごとに異なります。また、サイバー攻撃が発生した場合の影響についても環境によってさまざまです。したがって、正しい評価を得るためには、対象のOT環境の詳細を把握することが必要です。これによって、評価対象のOT環境で実際に起こり得るサイバー攻撃の発生可能性や攻撃による影響を、正しく見積もることができます。

把握すべきOT環境の詳細な内容としては、例えばネットワーク構成やUSBメモリの利用状況、各システムの役割と関係性、復旧の容易性、それらを踏まえた上での守るべきもの（守りたいもの）の優先順位付けなどが挙げられます。

### 継続的な評価の実施と対策の改善

サイバー攻撃の手法は常に進化しています。したがって、定期的に評価を行い、最新の攻撃手法に対してセキュリティ対策が十分かどうかを把握することが必要です。また、自社のOT環境の変化によって発生する可能性のあるサイバー攻撃が変わり、結果として必要なセキュリティ対策が変化することも考えられます。ネットワーク構成を変更したり、新たな技術の利用を開始したりする場合は、その前にセキュリティ評価を実施し、セキュリティ対策の変更要否についても検討するべきでしょう。継続的な評価の実施と、評価結果に基づく対策の改善によって、対策の有効性を維持・向上することができます。

## OTセキュリティ評価に役立つATT&CK for ICS

最後に、OTセキュリティ評価に有用であろう参考資料を紹介します。「ATT&CK（アタック）」は、米国の非営利団体が作成している、攻撃者の戦術・攻撃手法に関するナレッジベースです。2013年に発表されて以降、継続的にアップデートされています。2020年1月には、産業制御システム版である「ATT&CK for ICS」が新たに公開されました。OT環境に対するサイバー攻撃が網羅的・体系的にまとめられており、これを活用することで抜け漏れのないOTセキュリティ評価をすることが可能になるでしょう。以下にその特徴を簡単に記します。

### 機能レベルと資産

ATT&CKは従来、エンタープライズ向けとモバイル向けのそれぞれが存在していました。ATT&CK for ICSには、これらと異なるOT環境特有の要素が2点追加されています。

#### Levels（機能レベル）

ATT&CK for ICSが対象とする領域は、パデューモデル[1]の機能レベルによって示されています。基本的には、レベル0から2がATT&CK for ICSの範囲になります（レベル3・4はATT&CK for Enterpriseの範囲）。自社のOT環境をパデューモデルに沿って理解することで、ATT&CK for ICSの対象範囲を把握することができます。

#### Assets（資産）

OT環境には多様な資産が存在します。ATT&CK for ICSでは、それらの資産を一般化してAssetsとしてリストアップしています。Assetsの内容を理解し、個々の攻撃手法が自社環境のどの資産に影響するかを把握することで、対策に役立てることができます。

### Tactics（戦術）とTechniques（攻撃手法）

ATT&CK for ICSのもう一つの特徴は、Matrixと呼ばれる形式で攻撃者の戦術と攻撃手法が整理されている点です（図表5）。

Matrixの横軸にはTactics（戦術）が、縦軸にはそれぞれのTacticsで使用されるTechniques（攻撃手法）が一覧化されています。攻撃はTacticsの左から右に向かって行われます。起こり得る攻撃を段階ごとに網羅的に把握できる点で非常に有益と考えられますが、いくつかのステップがスキップされたり、Tacticsの右端のImpactに至る以前に攻撃者の目的が達成されたりするケースも考えられるので、必ずしも全ての手順が踏まれるわけではないことに注意が必要です。

こうした資料をもとにすることで、効率的に対策を練ることができるようになるでしょう。攻撃手法の具体的な事例や緩和策を把握することもできる実用的な内容ですので、理解を深められてはいかがでしょうか。

1　CIM（Computer Integrated Manufacturing：コンピュータ統合生産）のためのエンタープライズアーキテクチャの標準モデル。

## 図表5：MITRE ATT&CK for ICS Matrixにおける戦術と攻撃手法の整理

攻撃者の戦術的な目的、左から右に向けて進行

Tactics

それぞれのTacticsで使用される攻撃手法

Technique

| Initial Access | Access Execution | Persistence | Privilege Escalation | Evasion | Discovery | Lateral Movement | Collection | Command and Control | Inhibit Response Function | Impair Process Control | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 techniques | 9 techniques | 6 techniques | 2 techniques | 6 techniques | 5 techniques | 7 techniques | 11 techniques | 3 techniques | 14 techniques | 5 techniques | 12 techniques |
| Drive-by Compromise | Change Operating Mode | Hardcoded Credentials | Exploitation for Privilege Escalation | Change Operating Mode | Network Connection Enumeration | Default Credentials | Adversary-in-the-Middle | Commonly Used Port | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Exploit Public-Facing Application | Command-Line Interface | Modify Program | Hooking | Exploitation for Evasion | Network Sniffing | Exploitation of Remote Services | Automated Collection | Connection Proxy | Alarm Suppression | Modify Parameter | Denial of Control |
| Exploitation of Remote Services | Execution through API | Module Firmware | | Indicator Removal on Host | Remote System Discovery | Hardcoded Credentials | Data from Information Repositories | Standard Application Layer Protocol | Block Command Message | Module Firmware | Denial of View |
| External Remote Services | Graphical User Interface | Project File Infection | | Masquerading | Remote System Information Discovery | Lateral Tool Transfer | Data from Local System | | Block Reporting Message | Spoof Reporting Message | Loss of Availability |
| Internet Accessible Device | Hooking | System Firmware | | Rootkit | Wireless Sniffing | Program Download | Detect Operating Mode | | Block Serial COM | Unauthorized Command Message | Loss of Control |
| Remote Services | Modify Controller Tasking | Valid Accounts | | Spoof Reporting Message | | Remote Services | I/O Image | | Change Credential | | Loss of Productivity and Revenue |
| Replication Through Removable Media | Native API | | | | | Valid Accounts | Monitor Process State | | Data Destruction | | Loss of Protection |
| Rogue Master | Scripting | | | | | | Point & Tag Identification | | Denial of Service | | Loss of Safety |
| Spearphishing Attachment | User Execution | | | | | | Program Upload | | Device Restart/ Shutdown | | Loss of View |
| Supply Chain Compromise | | | | | | | Screen Capture | | Manipulate I/O Image | | Manipulation of Control |
| Transient Cyber Asset | | | | | | | Wireless Sniffing | | Modify Alarm Settings | | Manipulation of View |
| Wireless Compromise | | | | | | | | | Rootkit | | Theft of Operational Information |
| | | | | | | | | | Service Stop | | |
| | | | | | | | | | System Firmware | | |

出所：MITRE ATT&CK for ICS Matrixをもとに PwCが作成

# 5 工場（OT）環境におけるセキュリティアーキテクチャのリファレンスモデル化の重要性

## OTセキュリティに求められるもの

OT環境にセキュリティアーキテクチャを実装する際、まずは企業に存在する制約条件を認識することが重要です。以下に代表的な例を挙げます。

### 制約条件

#### 1つ目：工場の機能要件を優先する必要がある

工場では、組み込み系のシステムに使用されているレガシー OS上でしか動作しないソフトウェアを使用し続けることがあります。事業を営む上でそのソフトウェアの使用を優先せざるを得ず、OSのアップグレードができないといった側面があるからです。加えて、製品の生産性を重視するため、費用対効果の観点でセキュリティ専任の人員を各工場に常駐させることが困難となることも、こうした制約を生む要因です。

#### 2つ目：生産に影響を与えることができない

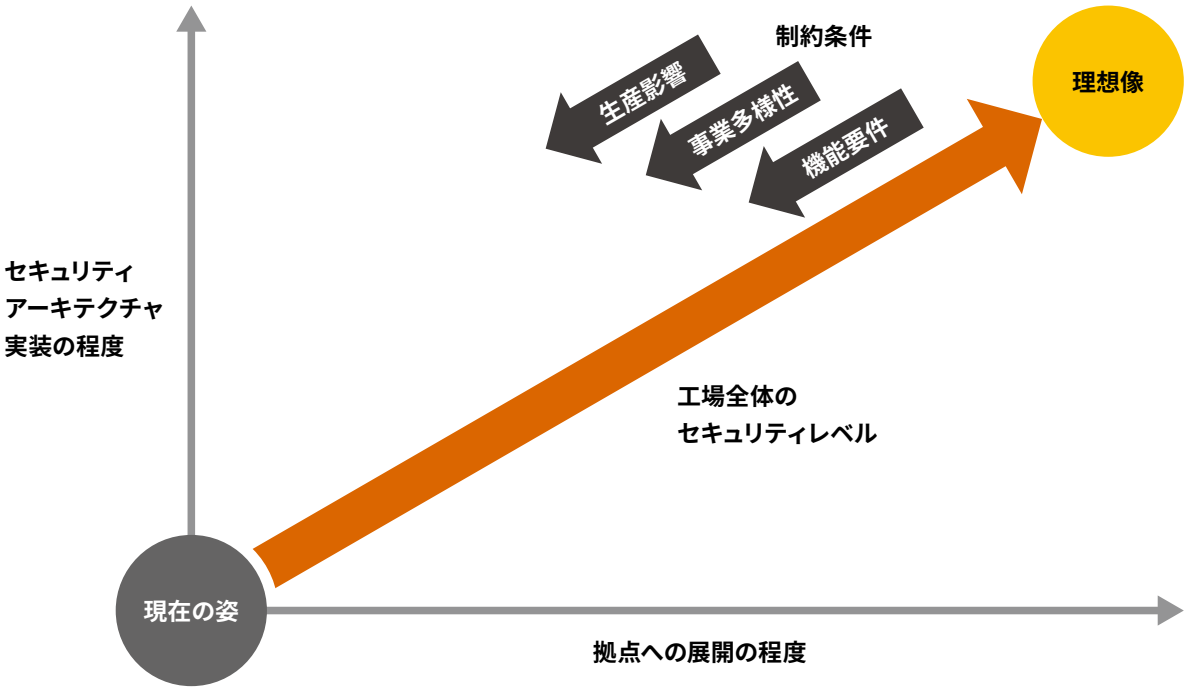
企業の多くは製品を生産・加工するために工場を稼働させています。このことから、セキュリティアーキテクチャの実装により、工場の稼働を遅延、停止することは避ける必要があります。

#### 3つ目：工場ごとに事業や規模が異なる

企業の多くは生産効率や人件費削減などの理由から、国内外に複数の工場を持っています。そして、その規模や事業内容、ロケーションは各々異なります。つまり、特定の工場だけにセキュリティアーキテクチャを実装して終わりではなく、工場全体に実装していくことを考慮した設計や実装が求められるのです。

こうした工場が持つ制約条件を考慮した上で、機能要件を満たしつつ、国内外の複数工場を対象にOTセキュリティ水準を向上させる複合的な取り組みが求められます。セキュリティインシデントが発生した場合の包括的かつ迅速な対応も重要な要件となります。

**図表6：OTセキュリティの理想像と制約条件の関係**




出所：PwC作成

## リファレンスモデル化による恩恵

OT環境特有の制約条件下でセキュリティアーキテクチャを実装するには、膨大な期間とコスト、運用負荷がかかることが想定されます。そこで、セキュリティアーキテクチャの設計と実装をリファレンスモデル化することで、工場の特徴に応じて柔軟に設計・実装をすることが可能になります。以下にリファレンスモデル化による主な恩恵を記します。

### セキュリティ品質の安定化

リファレンスモデルを活用することで設計や実装が一定レベルで共通化されるため、工場の規模の大小や事業の特徴に関わらず、セキュリティの品質が安定します。

### コスト削減

毎回個別に設計や実装をする必要がないため、これまで工場ごとの個別設計・実装に要したコストを削減できます。

### 時間短縮

前述のとおり、個別に設計や実装をする必要がないため、セキュリティアーキテクチャ実装のスピードアップにつながります。

### レスポンスの迅速化

設計や実装を共通化しておくことで、セキュリティアーキテクチャ実装後の運用も工場全体で共通化することが可能になります。万が一、複数の工場でインシデントが発生した場合でも、リファレンスモデルをベースに共通認識を持った状態で工場間のコミュニケーションがとれるため、被害が発生している端末の情報から類似端末を特定したり、必要な対応をとったりしやすくなります。

## リファレンスモデルが達成すべき要件

では最後に、セキュリティアーキテクチャをリファレンスモデル化するための要件について考えてみましょう。

### 規模や業務内容に縛られない設計・実装方針

各工場の規模や業務内容によって設計・実装方針が変わってしまうと、工場ごとに作業の重複が発生してしまい、セキュリティアーキテクチャの品質が安定しません。そのため、規模や業務内容などに縛られない設計・実装方針であることが求められます。

### 基本設計と詳細設計の区分け

一方、リファレンスモデルで全てを共通化してしまうと、実装がうまくいかない工場が出てくる可能性があります。そのため、基本設計までを共通化し、工場の特性を考慮して詳細設計できるようにしておくことが望ましいです。これにより、工場全体の設計と実装の品質を安定させた状態で、コストの削減や期間の短縮が可能になります。

### 実装の優先度を決める判断基準の明確化

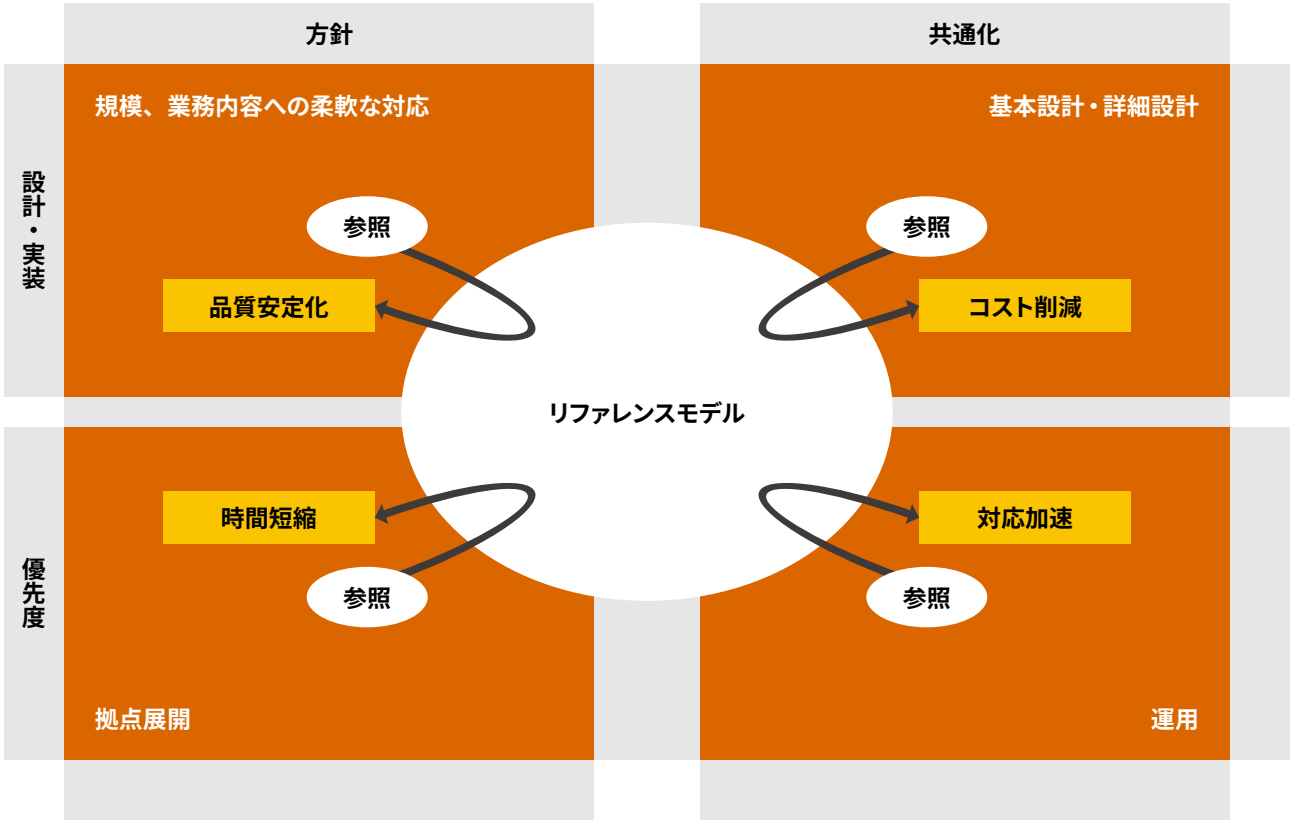
工場が多ければ多いほどリファレンスモデルが有効性を発揮しますが、やみくもに工場全体への実装を進めても非効率になってしまいます。長期的な目線で工場への展開にレバレッジをかけるために、工場の規模や業務内容などを判断要素とし、どの工場に展開していくべきかの優先度を決めるための判断基準を持つことが求められます。

### 根幹となる運用の共通化

実装後の運用について考えてみると、もちろん枝葉の運用は工場によって差異はありますが、根幹となる運用は共通化しておく必要があります。インシデント発生時の被害拡大を防止することを想定して、有事の際はネットワークを分断できるようにしておき、生産を停止しないことや守るべき資産を守れるような体制を構築することが必要です。つまり、セキュリティアーキテクチャの設計・実装にあたり、優先度に基づいたインシデント対応ができるよう考慮しておくことが重要になります。

多くの企業が日本国内外に工場を持つ一方、工場へのセキュリティ人員の配置や設計・実装に費やすことができるリソースは限られています。このような中で工場全体へセキュリティを浸透させていくためには、セキュリティアーキテクチャのリファレンスモデル化が有益です。

**図表7：リファレンスモデルが達成すべき要件と恩恵**




出所：PwC作成

# 6 工場（OT）領域におけるセキュリティ人材

## OT環境に求められるセキュリティ人材

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とどまり、主役ではありません。

IT／OTにかかわらず企業がセキュリティ対策に取り組むためには、ルールや仕組みを立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立て付け、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）

SOC（Security Operation Center：セキュリティ監視）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。

**図表8：知識・スキル別のOTセキュリティ人材分類**


出所：PwC作成

## OTセキュリティの人材獲得戦略

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生かして、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。つまり、カギは外部ではなく社内人員の育成です。また一般的には、高度な専門性が必要になればなるほど、さらに知識／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（P7「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）

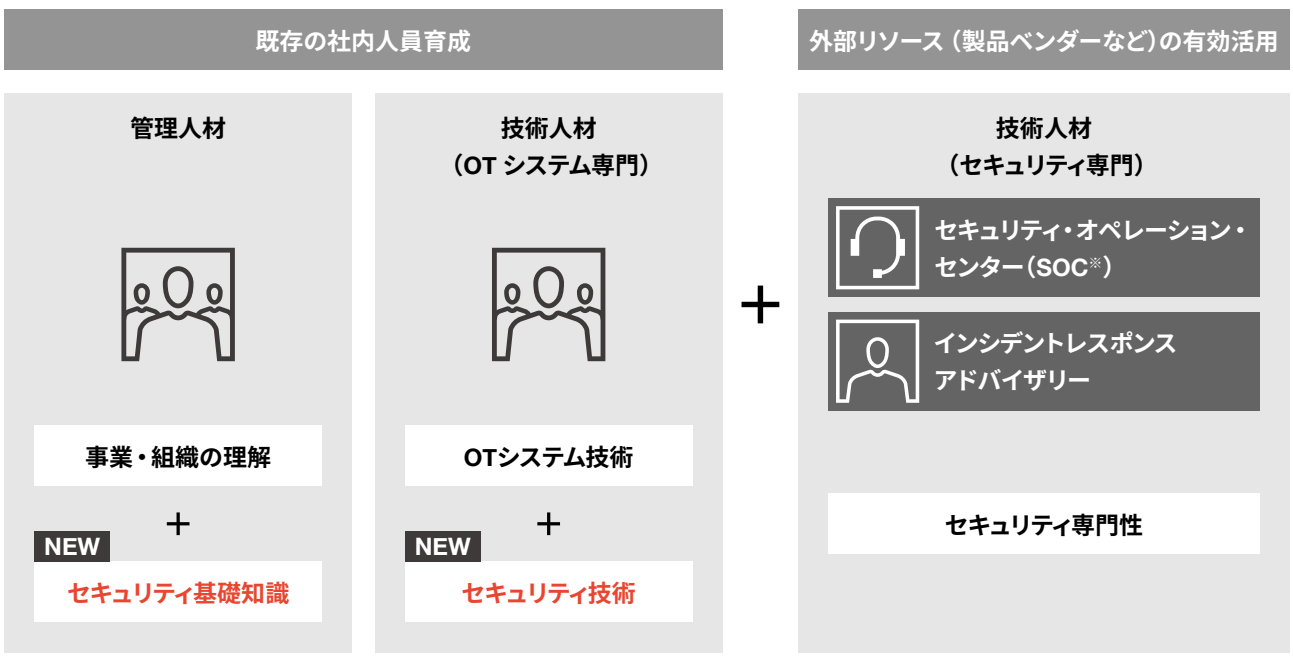
OTシステムやその運用・保守に関する技術的な専門性を持つ社内人材に対し、知識のみならずオペレーションスキルを含めたセキュリティ専門性を教育することが求められます。前述のように、多くの企業では各事業や各拠点独自でOTシステムを実装・運用していることから、本人材は各拠点で育成していく必要があります。

### 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。さらに自組織の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9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。

**図表9：各人材の獲得戦略**




※SOC（Security Operation Center）
出所：PwC作成

# 7 OT環境を狙った高度なサイバー攻撃とその対策

## 米国の政府機関が注意喚起

米国の国家安全保障局（NSA）は2022年4月、産業制御システムを対象として破壊や混乱を引き起こすAPT（Advanced Persistent Threat：高度標的型攻撃）ツールに対する注意喚起の声明を、DOE（Department of Energy：エネルギー省）、CISA（Cybersecurity and Infrastructure Security Agency：サイバーセキュリティ・インフラセキュリティ庁）、FBI（Federal Bureau of Investigation：連邦捜査局）と共同で発表しました。

2010年以降、欧米や中東を中心に発電所や水道施設などの重要インフラ、鉄や化学物質の工場などにおけるセキュリティインシデント発生件数が増加傾向にあり、APTツールによる攻撃は、これらの中東やウクライナで発生した特に強力だった攻撃に匹敵すると見なされています。

**図表10：OT環境に極めて重大な被害をもたらしたサイバー攻撃**

| | |
|---|---|
| 2010年 | イランの核燃料施設で、PLCの設定が改ざんされ、同施設の稼働が一時的に停止 |
| 2015年～2016年 | 送電の遮断とシステムの破壊によりウクライナの電力設備で大規模停電が発生 |
| 2017年 | 中東の重要インフラで、安全計装システムの緊急停止機能が不正に作動 |

出所：PwC作成

## どのような攻撃で何が高度なのか

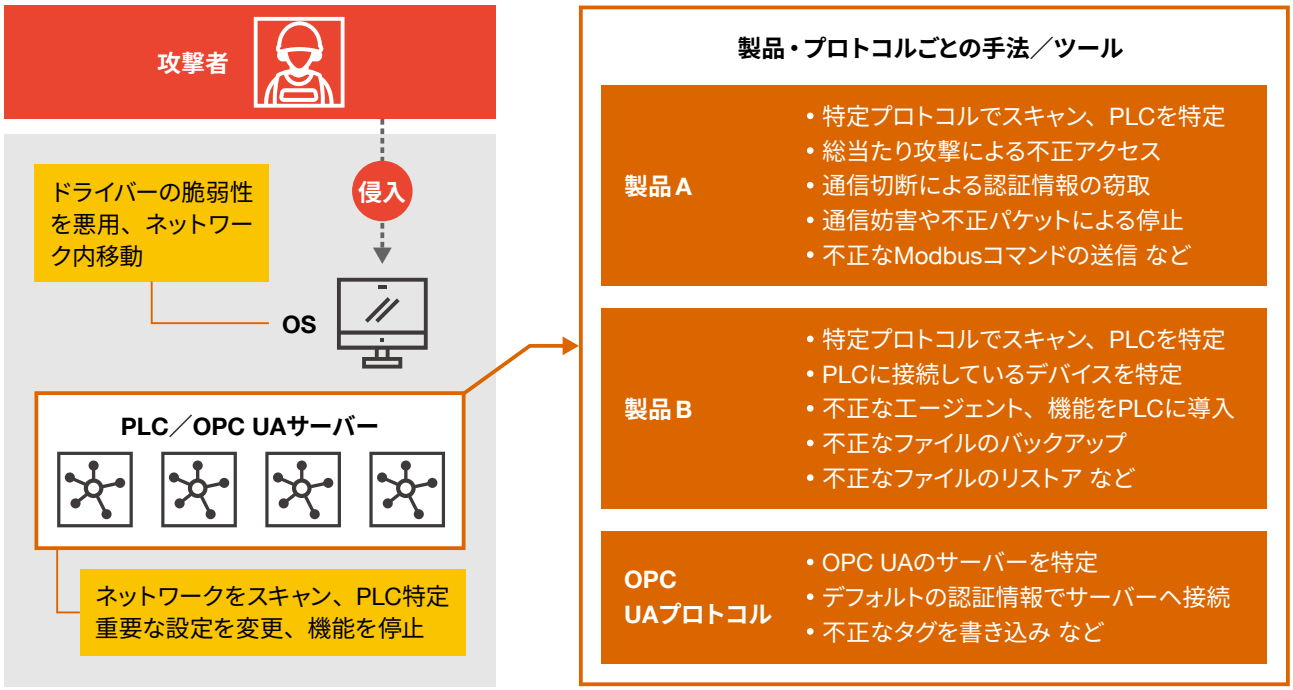
これらの攻撃が重大な被害をもたらした理由として、IT環境からのもらい事故（偶発的にマルウェアなどが流入した）ではなく、攻撃者が産業プロセスや製造設備に詳しく、OT環境そのものを狙った攻撃だった点が挙げられます。

APTツールによる攻撃もそれと同様に、OT環境の特定の製品やプロトコルを狙ったものであるため、特に注意が必要です。

### 攻撃手法の特徴

- OSのデバイスのマザーボードドライバーの脆弱性（CVE-2020-15368）を悪用し、OT環境内のネットワークでアクセスを拡大する
- プログラマブルロジックコントローラ（PLC）の特定の製品や特定のプロトコル（OPC UA）の仕様に則して開発したツールを用いて、破壊や停止を引き起こす

**図表11：脆弱性の悪用～ PLCなどに対する攻撃のイメージ**




出所：PwC作成

## どのように守るべきか

これらの攻撃への備えとして特に重要なのが、「認証による防御」と「悪意のある通信や振る舞いの検知」です。

ただ、これら以外にも、防御、検知、対応、復旧と幅広く推奨される対策がNSAなどによる声明には記載されており、サイバー攻撃が発生した際の耐性や回復力を意味する「サイバーレジリエンス」が重要であることが分かります。

**図表12：代表的な推奨策（太字：特に重要なもの）**

| | |
|---|---|
| 防御 | • **リモートアクセスするデバイスに多要素認証を実装**<br>• **パスワードの初期値を禁止、強固なものに変更**<br>• OTとIT／インターネット間の分離、必要最小限の通信以外禁止<br>• 必要最小限のアプリケーションやドライバーのインストール<br>• 必要最小限の権限の付与<br>• OSのセキュリティ機能とEDRによるデバイスの堅牢化 など |
| 検知 | • **悪意のある通信（脆弱性の悪用やマルウェアの横感染など）を検知**<br>• **悪意のある振る舞い（業務上利用しないアプリケーションやドライバーなどのインストールなど）やサービス停止の兆候となる事象（通信や処理の遅延、再起動など）を検知 など** |
| 対応 | • インシデント対応の計画を策定<br>• インシデント対応の訓練をIT部門／OT部門などの関係者と定期実施<br>• デバイスのログの収集および保管 など |
| 復旧 | • オフラインバックアップの取得<br>• ファームウェアやコントローラの構成ファイルのハッシュチェックによる完全性の確保 など |

出所：PwC作成

## 参考文献


1 米国の国家安全保障局（NSA）によるプレスリリース「APT Cyber Tools Targeting ICS/SCADA devices」2022年4月13日（2022年5月13日閲覧）

2 米国の国家安全保障局（NSA）、米国のエネルギー省（DOE）、サイバーセキュリティ・インフラセキュリティ庁（CISA）、連邦捜査局（FBI）による共同アドバイザリー「APT Cyber Tools Targeting ICS/SCADA Devices」2022年4月13日（2022年5月13日閲覧）

3 IPAの攻撃事例資料「制御システム関連のサイバーインシデント事例1 ～2015年 ウクライナ 大規模停電～」2019年9月（2022年5月13日閲覧）

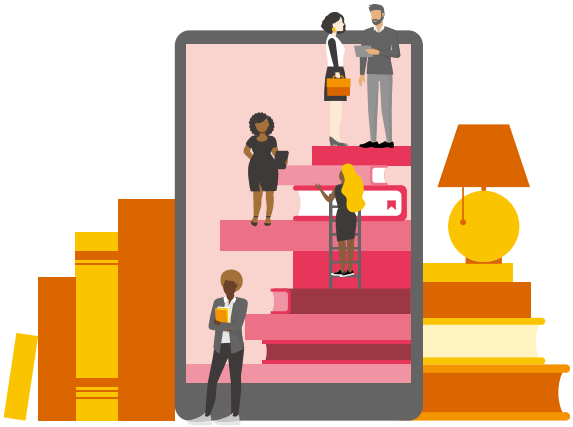
4 IPAの攻撃事例資料「制御システム関連のサイバーインシデント事例2 ～2016年 ウクライナ マルウェアによる停電～」2019年7月（2022年5月13日閲覧）

5 IPAの攻撃事例資料「制御システム関連のサイバーインシデント事例3 ～2017年 安全計装システムを標的とするマルウェア～」2019年7月（2022年5月13日閲覧）

6 IPAの攻撃事例資料「制御システム関連のサイバーインシデント事例4 ～Stuxnet：制御システムを標的とする初めてのマルウェア～」2020年3月（2022年5月13日閲覧）

8 MANDIANT BLOG「INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems」2022年4月14日（2022年5月13日閲覧）

9 DRAGOS Whitepaper「PIPEDREAM: CHERNOVITE'S EMERGING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS」2022年4月（2022年5月13日閲覧）

# 8 最後に

組織のOTセキュリティ管理を立て付けていく上で、従来の情報セキュリティ・ITセキュリティとは随所で異なる対応が求められます。例えば、多くの企業が具備しているインシデント対応体制1つを例にとっても、その違いは明白です。万が一、OTセキュリティ特有の考え方や環境を考慮せずOTセキュリティ管理に係る制度や仕組み、技術的対策を設計した場合、実効性が伴わないだけでなく、無駄な投資と運用コストの発生も懸念されます。

一方、サイバー攻撃は金銭を狙うような「犯罪」の範疇を超え、サイバー空間における国家間の「紛争」の手段にまで拡大しています。このことからも、攻撃者は重要インフラや重要な事業に関わる工場やプラントで使われる設備やプロトコルの理解をさらに深め、高度な攻撃手法・攻撃ツールを開発し、強力な攻撃を仕掛けてくることが予想されます。

PwCは、OT環境のセキュリティリスクに対して、アセスメントや技術的対策の設計・実装をはじめとする包括的なサービスを提供しています。また、企業のOTセキュリティを直接的に支援するだけでなく、そうした支援を通じて得た知見を広く社会に共有することで、安全・安心な事業活動の実現と企業の持続的な成長に基づくより良い未来に貢献します。

# 執筆者

**上村 益永**
PwCコンサルティング合同会社
パートナー

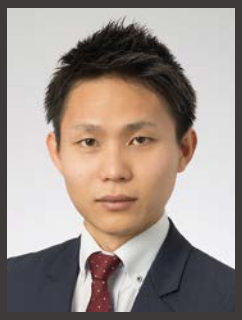
**茂山 高宏**
PwCコンサルティング合同会社
ディレクター

**布目 亮**
PwCコンサルティング合同会社
シニアマネージャー

**大貫 経介**
PwCコンサルティング合同会社
マネージャー

**河合 菜央**
PwCコンサルティング合同会社
マネージャー

**木佐森 幸太**
PwCコンサルティング合同会社
マネージャー



**金田 侑也**
PwCコンサルティング合同会社
マネージャー

# お問い合わせ先

**PwC Japanグループ**
https://www.pwc.com/jp/ja/contact.html

**www.pwc.com/jp**

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約11,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界152カ国に及ぶグローバルネットワークに328,000人以上のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。

発刊年月：2023年12月　　管理番号：I202309-02