OTセキュリティ対策ガイド

OTセキュリティとITセキュリティは何が違う？

OTセキュリティ対策を効率的に進めるとで重要なのは、ITセキュリティとの違いを把握しておくことです。「OTのシステムにITのセキュリティ製品・運用を適用すればいいのでは？」と考えている方も多いかもしれませんが、OTシステムの技術や特性を理解していなければOTセキュリティ対策は上手く進みません。
本記事では、OTセキュリティ対策を進めるとで重要な前提知識である、OTセキュリティとITセキュリティの違いから見るOTセキュリティ対策の課題について解説します。

目次

OTセキュリティとITセキュリティの違い

	IT 情報システム部門	OT 製造部門
主な目的	情報の管理や利活用	生産性や品質の向上
利用技術	Windows/Linux、Ethernet など	PLC、産業ネットワーク など
保護対象	個人や企業の機密情報	生産状況、 モノ（設備、製品）サービス（連続稼働）
セキュリティの考え方	情報漏洩の防止を重視	生産の維持、情報漏洩防止の両方を重視
稼働時間	通常業務時間内	24時間365日
システム更新	3～5年	10～20年

セキュリティ対策を考える上でOTとITではいくつかの違いがあり、上の表にまとめています。
今回は、これらの違いを「管理部門の違い・セキュリティの考え方の違い・利用技術/運用の違い」の3つの観点から解説します。

管理部門の違い

OTとITの違いとして、まずは管理部門の違いが挙げられます。
一般的にOT領域の管理は製造部門、IT領域の管理は情報システム部門が担当しているケースが大半を占めます。管理対象は、OT・ITそれぞれの領域で利用している機器や運用ルールなどです。

多くの企業はすでにITセキュリティ対策を講じており、情報システム部門が主導しています。では、OTセキュリティも情報システム部門が対応すれば問題ないでしょうか？実際は、OTセキュリティは情報システム部門だけで進めるのが難しいという実状があります。
例えば情報システム部門は製造現場に関する十分な知識があるとは言い切れず、生産設備や現場の運用の実態を必ずしも全容把握しているわけではありません。また、PLC（Programmable Logic Controller）やSCADA（Supervisory Control And Data Acquisition）といった制御機器やシステムがどのような通信・データをやり取りしているのか、計画通りに製品を生産するために製造現場でどのような運用がなされているのかを知らない場合が多いです。このような状況で情報システム部門がOT領域にセキュリティ対策を進めても、上手く適用できない・運用できないといった事態に陥ります。

一方で、製造部門は現場の機器や運用については詳しいですが、セキュリティに関する知識が不足しがちです。したがって製造部門がOTセキュリティを進めようとしても、まず何から始めていいのかわからなくなります。また情報システム部門と製造部門は密にコミュニケーションをとっておらず、お互いのことをほとんど把握していないケースが多いです。

その結果、OTセキュリティ対策を進めるときに「誰がOTセキュリティ対策を推進するのか？」が明確に定まらないという問題が発生してしまいます。

OTセキュリティ対策の課題

- **OT領域の管理は製造部門が担当することが一般的だが、セキュリティについては知識が不足しがちなため対策を主導するのは難しい**
- **情報システム部門はOT機器の知識や可用性意味の理解などが乏しいためOT領域のセキュリティ対策を主導するのは難しく、結果的にどの部門の誰が主導するのかが定まらない**

セキュリティの考え方の違い

OTとITでは、セキュリティにおいて重視する考え方も異なっています。

まず、ITの領域では情報セキュリティの基本的な考え方として、機密性・完全性・可用性の3要素をバランス良く維持・向上することが求められます。またサイバー攻撃事例でよく耳にするように、外部に機密情報などが漏洩してしまうといった事故を防ぐためには、機密性を十分に確保することが求められます。

機密性	正当な権利を持った者だけが情報にアクセス・使用できる状態にすること
完全性	保有する情報が正確であり、完全である状態を保持すること
可用性	情報をいつでも安全に利用できることを確保する（＝システムの稼働の継続性を確保する）

一方、OTの領域では生産現場の高い生産性が求められ、OTシステムの稼働をとめずに生産し続けられる「可用性」が特に重視されます。そのため、たとえセキュリティ対策を講じてサイバー攻撃の被害に遭うリスクは抑えられたとしても、それによって工場の稼働が止まったり、生産活動に影響が発生したりするようでは本末転倒と言えます。また、そもそも工場の稼働が優先なのでセキュリティ対策製品を導入することすら敬遠される場合もあります。

メンテナンスや障害などによるシステム停止が容認されやすいITに対し、OTでは現場の可用性を考慮した対策導入、運用ルールを考えていく必要があります。

OTセキュリティ対策の課題

- **ITとOTではセキュリティの考え方において重要とされる要素が異なる（ITセキュリティは機密性、OTセキュリティは可用性を重視）**
- **可用性を軽視したセキュリティ対策は、リスクを軽減できても、生産効率を下げることにつながるため、継続的な運用はできない**

利用技術/運用の違い

最後に、それぞれの領域で利用している技術の違いです。

OT機器とIT機器では、それぞれの目的や使われている技術が異なり、同じセキュリティ対策を適用することは難しいとされています。一般的にOT機器は生産設備など機器やプロセスを制御・監視するのに対し、IT機器は情報技術を活用してデータの処理や通信を行います。それぞれの目的が違うため、通信に使用されているプロトコルやその性質も異なります。
例えばIT機器はインターネット接続を前提としており、TCP/IPと呼ばれる標準プロトコルで通信が行われます。一方で、OT領域ではPLCをはじめとしたFA製品が使用され、メーカ独自のプロトコルや制御ネットワークプロトコルで通信しています。このようにOT領域とIT領域では通信プロトコルが異なり、セキュリティ上のリスクや対策方法も異なります。

ほかにも、IT機器は3～5年といったスパンでのOS更新や頻繁なセキュリティアップデートにより脆弱性対策がなされている一方で、OT機器は「製造現場の稼働が優先で、セキュリティアップデートのために機器を止めることができない」「製造用ソフトウェアが古いOSでないと動かない」といった理由でOS・セキュリティのアップデートができず、脆弱性を抱えたまま運用しているケースが多く見られます。

このようなOT領域のシステム・技術の特性について理解が不足していると、OTセキュリティ対策がうまく進められないという課題が出てきます。

OTセキュリティ対策の課題

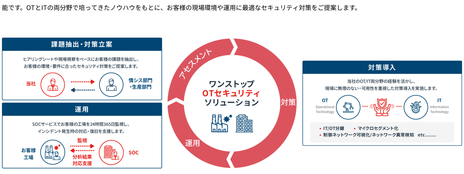
- **IT領域とOT領域では利用されている技術が異なり、OT領域にITセキュリティと同じ対策を講じることが難しい**
- **OT機器の特性について理解が不足していると、セキュリティ対策の何をどこから実施すればよいのか分からない状態に陥る**

まとめ

この記事では、OTセキュリティとITセキュリティの違いからみるOTセキュリティ対策の課題について説明しました。OTセキュリティ対策を効果的に講じるためには、それらの課題を把握したうえで検討をすすめる必要があります。

OTとITの違い	OTセキュリティ対策の課題
管理部門	・OT領域の管理は製造部門が担当することが一般的だが、セキュリティについては知識が不足しがちなため対策を主導するのは難しい ・情報システム部門はOT機器の知識や可用性意味の理解などが乏しいためOT領域のセキュリティ対策を主導するのは難しく、結果的にどの部門の誰が主導するのかが定まらない
セキュリティの考え方	・ITとOTではセキュリティの考え方において重要とされる要素が異なる（ITセキュリティは機密性、OTセキュリティは可用性を重視） ・可用性を軽視したセキュリティ対策は、リスクを軽減できても、生産効率を下げることにつながるため、継続的な運用はできない
利用技術	・IT領域とOT領域では利用されている技術が異なり、OT領域にITセキュリティと同じ対策を講じることが難しい ・OT機器の特性について理解が不足していると、セキュリティ対策の何をどこから実施すればよいのか分からない状態に陥る

当社のOTセキュリティソリューションでは、お客様が抱えるOTセキュリティのお悩みを解決するべく課題の抽出から対策導入、運用までをワンストップで提供可能です。OTとITの両分野で培ってきたノウハウをもとに、お客様の現場環境や運用に最適なセキュリティ対策をご提案します。



出典：三菱電機サイトより転載

OTセキュリティ 対策サービスに関するお問い合わせ

三菱電機デジタルイノベーション株式会社
https://go.digief.mitsubishielectric.co.jp/medigital/contact/inquiry_ot-security

お問い合わせ