機能安全とサイバーセキュリティ間のギャップを埋める

潜在的なセキュリティの脅威が増える中、産業プラントの安全性確保は重要な課題です。OT（Operational Technology)におけるサイバーセキュリティを向上させるには、組織がリスクを把握し適切な対策をとることが求められます。
OTサイバーセキュリティの対策や体制づくりの課題についてQ&A形式でまとめましたので、ぜひお役立てください。

サイバーセキュリティが機能安全に与える影響は？
技術の進歩に伴い、ますます多くの産業プラントがIPベースのソリューションを採用しています。これにより、サイバーイベントやインシデントに対する脆弱性が高まる可能性があります。TRITON攻撃などによる安全計装システム（SIS）への標的型攻撃はすでに起こっており、今後さらに増えるでしょう。

このTRITON事件では、幸いにも攻撃は失敗に終わり安全システムは適切に対応することができました。
IEC 61508などの安全規格は、全体的な安全性評価の一部としてサイバーセキュリティリスク対応を要求しています。

TÜVRheinland®
Precisely Right.

機能安全とサイバーセキュリティのバランスを実現しますか？
機能安全とサイバーセキュリティは、切り離せない関係です。最も重要な安全性とサイバーセキュリティを確保するために、限られた予算をあてて、リスクベースのアプローチを採用する必要があります。そのためには、OTマネージャーがビジネスリスク、安全性リスク、およびサイバーセキュリティリスクを詳細に理解し、予算に優先順位を付けることが重要です。

参考：調査結果「産業セキュリティとサイバーセキュリティトレンド2020」

サイバーセキュリティ対策にどのくらい投資すべきでしょうか？
サイバーセキュリティ対策はビジネスリスクに依存し、NISTサイバーセキュリティフレームワークやIEC 62443などの客観的なフレームワークを使用して評価を行う必要があります。評価を実施することにより、ビジネスリスクの問題や、サイバーセキュリティ管理の欠落、不十分な管理についての概要が示されます。
サイバーセキュリティ対策への投資は、リスクに比例する必要があります。最初に重要な問題に対処し、次に残りの問題に対処するプロセスを作成します。これが1回のプロセスで実現できる可能性は低く、個々のビジネスあるいは既存のサイバーセキュリティレベルの成熟度によって、効果的なプロセスを作成するのに2～3年かかる場合があります。リスク評価は、サイバーセキュリティの脅威の絶え間なく変化する性質を反映するために定期的に行われることが必須です。

産業用サイバーセキュリティの分野で最大の課題は何ですか？
セキュリティを優先する組織や文化造りは、多くの組織にとって最大の課題です。新しいIP対応テクノロジーは、プラントの効率を大幅に向上させることができますが、今まで考慮していなかった関連リスクを伴うこともあります。さらに、セキュリティの経験豊富なエンジニアが不足しているため、企業が産業プロセス、OT、サイバーセキュリティを理解している人材を見つけることは困難です。

産業プロセスにおけるスタッフまたは専門家をOTサイバーセキュリティのスペシャリストとしてトレーニングするべきですか？
ITスタッフが産業プロセス、エンジニアリング、および重要性を理解している場合は、OTサイバーセキュリティの専門家として、ITスタッフをトレーニングすることが近道です。ベストなOTサイバーセキュリティチームは、ITスタッフ、OTプロセスエンジニア、資産所有者、およびOTサイバーセキュリティの専門家で構成されます。このアプローチにより、知識と経験の共有と交換が可能になり、非常に優れたチームになります。テュフ ラインランドは、チームメンバーがOTサイバーセキュリティチームの機能を強化するために、コーチングやトレーニングを提供します。

チーフインフォメーションセキュリティオフィサー（CISO）/チーフセキュリティオフィサー（CSO）のIT・OTに関わる機能や役割を統合して、リスクと攻撃を最小化する最善の方法は？
サイバーセキュリティ、IT、OTの専門知識を習得するには、何年もの経験が必要です。経験と知識を蓄積する間、テュフ ラインランドのような第三者機関を上手に活用することも一つの方法です。テュフ ラインランドは、サイバーセキュリティに関するテクノロジーや課題に対し、長期的にトレーニングを提供することができます。

OT固有のチーフセキュリティオフィサー（CSO）は必要ですか？
多くの組織は、CSOが責任者としてITとOTのサイバーセキュリティチームが緊密に連携する集中型アプローチに移行しています。しかし、そのようなCSOの専門家を見つけるのが難しいため、中期的なソリューションとして別のCSOを持つことがよいでしょう。

TÜVRheinland®
Precisely Right.

OTをランサムウェアから保護する上で重要な要素は何ですか？

ランサムウェアは、コンピューターシステムを暗号化する悪意のあるソフトウェアです。多くの場合、フィッシングメールを介して配信され、攻撃者はデータを復号化するために支払いを要求します。支払われても、復号化プロセスは失敗することも多々おこります。ITシステムとOTシステムはリンクされていることが多いため、ランサムウェアインシデントが発生すると、生産施設に直接的な影響が生じ、生産とシステムの稼働が失われる可能性があります。

パッチの適用、適切なバックアップ、セグメント化されたネットワークは、ランサムウェアの防止に役立つ優れた対策であり、また、ユーザーへの適切な教育、電子メールのフィルタリングおよび管理もランサムウェア対策に役立ちます。OTのリソースは文書化し、ITシステムとどのように連携されているかも十分に理解しておく必要があります。適切に構成されたファイアウォールを使用することも役立ちます。ランサムウェアインシデントが発生した場合、バックアップからシステムを復元することが重要なことですが、これにはOTシステムを含める必要があります。また、バックアップは同じランサムウェアによって誤って暗号化されないように保護する必要があります。適切なインシデント対応と復旧計画を準備するとともに、インシデントに対処する人材や、プロセス、テクノロジーの備えを確実にすることが必要です。

外部サービスプロバイダーや第三者機関を利用すると、どのようにリスクを最小化できますか？

第三者機関を利用する場合は、まず責任を定義し、適切な契約を結んだうえでサポートしてもらうことが重要です。企業は、サプライヤーとの関係を築く最初の段階において、そして契約が署名される前にサイバーセキュリティについて検討する必要があります。

第三者機関による定期的な監査は、サイバーセキュリティ対策が契約期間全体を通じて維持されていることを確認するために最も重要です。

自動車業界のTISAX監査プログラムは、サイバーセキュリティ保証プログラムがどのように機能するかを示しています。これは、情報セキュリティを評価し、共有するシステムで、サイバーセキュリティの評価結果を参加企業間で相互に受け入れることができます。顧客からの機密情報を処理する場合、または自社のサプライヤーの情報セキュリティを評価する場合、TISAXはこれを実現する方法の非常に良い例です。

ビジネスリスクの懸念とOTサイバーセキュリティリスクはどのように関連していますか？

OTシステムは、サイバーセキュリティ対策が他の主要なビジネスリスクと共に考慮されるように、ビジネスの**ガバナンス、リスク**、および**コンプライアンス**（**GRC**）戦略と統合している必要があります。テュフ　ラインランドは、OTの稼働においてGRC戦略を統合した新しいソリューション「継続的適応リスクモニタリング（CARM）を提供します。詳しくはお問い合わせください。

インシデントによってOTデータが失われることの重大性は？
生産機能が失われることによってどのような結果を招きますか？

生産システムの可用性を保護することは、人・環境保護同様に、この分野のOTサイバーセキュリティの専門家にとって主な懸念点です。生産停止による財務への影響は計り知れず、企業に長期的な損害を与える可能性があります。OTデータを失うことは決して無視できません。例えば、OTプロセス情報や機能ブロック図、企業秘密などが盗まれたり紛失すると、風評被害や重要な契約解消に至ることもあり得ます。したがって、OTデータと生産機能の損失は重大課題で、サイバーセキュリティ管理とプロセス構築は、避けられないインシデントに対応するために非常に重要です。

複雑な産業環境の中、ITからOTへの移行はどの時点で行われるのですか？

ITとOTの間の移行点は、ビジネスの構成または問題となるOTシステムによって異なります。Purdue Reference モデルは、これを説明する良い方法を示しています。多くの場合、IT / OT移行はモデルのレベル3または4から行われます。レベル4のシステムは通常、日常のビジネスオペレーションを処理し、プロセスレベルから切り離されています。レベル3には、運用管理が含まれ、監視制御であるレベル2から切り離されています。時代の流れとともにOTの世界が発展するにつれ、本来のPurdueモデルの使用は困難になるかもしれませんが、現時点では、有用な「理想的な」論理構造でしょう。

テュフ ラインランド ジャパン株式会社
カスタマーサービス
info@jpn.tuv.com

東日本地域Tel: 045-470-1850
西日本地域Tel: 06-6355-5400

横浜市港北区新横浜 3-19-5
新横浜第二センタービル
Tel. 045-470-1860 Fax 045-473-5221

TÜVRheinland®
Precisely Right.