参考情報

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern,
Germany
Deutschland/Germany
www.pilz.com

2025年10月

企業、機械、製品の保護

安全と産業サイバーセキュリティ –
ワンストップショップ

2025年10月、オストフィルダン -
セキュリティ・インシデントは、もはやITシステムだけではなく、生産環境（OT）にも大きな影響を与えるものになりつつあります。産業サイバーセキュリティのインシデントには目標を定めた攻撃のほかに、意図せぬ不正操作もあります。生産における産業サイバーセキュリティの使命は、機械のデータや処理の完全性・機密性はもちろんのこと、設備と機械の可用性をも保証することです。しかし、最も確実に保護すべきものは機能安全にほかなりません。なぜなら、最終的には企業がデータの主権を握らなければ、企業と従業員の安全を危険にさらすことになるからです。セキュリティなくして安全はなく、安全なくして人を守ることはできません！

EU域内では、脅威が日増しに高まっているという認識に基づいた法規制の改正が進んでいます。企業レベルでは、**NIS 2指令**により、EU全体で共通レベルの高いサイバーセキュリティを実現するため、例えば情報セキュリティ管理システムを活用するなどの対策をとるよう求めています。

機械規則2023/1230では、設備と機械を改ざんから保護するための規定を設け、機械の機能安全に影響する部分に対する産業サイバーセキュリティ対策を要求しています。

サイバーレジリエンス法（CRA）は、デジタル要素を伴う製品のセキュリティ対策を要求するもので、コントローラ、IOシステムやその他の、機械類に使用されるコンポーネントが対象です。

企業、機械、製品 –
すべてのレベルで、機械のメーカとオペレータはさまざまな課題と法的枠組みに対処しなくてはなりません。

最先端のセキュリティ

たとえ法律で産業サイバーセキュリティが義務付けられていなくても、この問題に早期に取り組み、アドバイスを受けるべき十分な理由はいくつもあります。機械を操作するための既存のプロセスや条件は、定期的に見直しをしないと不正操作を許してしまうおそれがあります。例として、耐用期間の長い機械では対応システムが旧式化して、やがて最新のセキュリティ基準を満たせなくなるという状況がしばしば起こり、システムには埋めることのできないセキュリティギャップが生じます。サプライヤはセキュリティの更新の提供をやめてしまっているからです。多くの場合、末端の機器にはマルウェアに対する保護を実装できなくなります。機器が古すぎ、無理に実装すれば、性能が低下して生産のダウンタイムの原因となるおそれがあります。

段階的な産業用セキュリティの強化

最終目標は事業運営を確実に保護し続けることですが、そのためには、企業はさまざまな課題を克服しなければなりません。適用される法的要件の特定から、システム内の脆弱性の検出と修正、そして従業員の意識向上とトレーニング、その後の管理体制の施行まで、課題は多岐にわたります。セキュリティの目標は絶えず変化し続けるので、機械の産業サイバーセキュリティの状態を定期的にチェックすることも欠かせません。社内の責任分担を明確にして、必要な

専門知識を集積するなどの体系的なアプローチを確立することが大切です。

オートメーション企業ピルツは、そうした要求に対応するべく準備を整え、世界中の機械メーカとユーザのニーズに応える、人と機械の保護に役立つあらゆる要素を統合したサービスポートフォリオを開発しました。ピルツの専門家は最新の法的要件と標準化要件を熟知しており、それらを取り入れたアドバイスをします。そして最後に、企業がセキュリティの知識を自ら構築・更新していけるよう、トレーニングを提供します。ピルツの製品ソリューションは、より高い安全性と産業セキュリティを実現するIdentification and Access Management（I.A.M.）システムなどの、実用的な実装にも使用されています。

正しい基礎作り

自社の機械を産業サイバーセキュリティの脅威から守るには、機械エンジニアリング分野のスペシャリストが法規制や適用規格に関する基礎知識を持つことが重要です。ピルツの専門家が、「産業サイバーセキュリティの中級」トレーニングで、そのノウハウを伝授します。トレーニング参加者は、機械とネットワークセキュリティの観点から、セキュリティの脅威と適切な保護対策、ベストプラクティスを学びます。そのため、セキュリティ初心者でも、生産現場で稼動する機械をサイバー攻撃や不正操作から守るための効果的な対策を身につけることができます。

ピルツは「CESA - Certified Expert for Security in Automation（オートメーションにおけるセキュリティの認定エキスパート）」の資格を有しており、2日間のエキスパートコースをご用

意しています。このコースの参加者は、特にIEC 62443シリーズ（「産業用通信ネットワーク-ネットワークおよびシステムのITセキュリティ」）などの最新規格に沿ったセキュリティの深い知識を習得できます。さらに、このトレーニングでは、セキュリティリスクを防止するためのアクセス管理や技術的手段と組織的対策によるネットワークセキュリティの向上など、実践的なリスク低減対策も網羅しています。参加者は、この規格を正しく適用する方法や、自社のオートメーション・システムがサイバーセキュリティ要件を満たしていることを証明する方法を学べます。試験に合格すると、参加者は世界的に認められているTÜV NORDの「CESA - Certified Expert for Security in Automation（オートメーションにおけるセキュリティの認定エキスパート）」の認定証を取得できます。

理論から実践へ

理論的な基礎ができ、トレーニングを完了したら、産業サイバーセキュリティを強化するための次のステップは、構造化された実践的なプロセスを適用することです。OT（Operational Technology）についてのコンサルティングでは、理論的な土台から実行可能な戦略を導き出すための橋渡しをします。産業サイバーセキュリティサービスは段階的なアプローチを用いて、複雑なシステムの脆弱性を特定し、リスクを最小限に抑えるための対策を練ります。それらをもとに総合的なセキュリティのコンセプトが形成されます。

産業サイバーセキュリティを強化する4つのステップ

OTセキュリティプロセスは「保護要件分析」、「産業サイバーセキュリティのリスクアセスメント」、「産業サイバーセキュリティのコンセプト」、「産業サイバーセキュリティシステムの検証」の4つのステップで構成されます。

保護要件分析では、その企業の設備や機械の個々の「資産」について、保護要件と保護目標を特定します。第2のステップの「リスクアセスメント」では、システムのライフサイクル全体を通じての各サブセクションのすべてのリスクを、発生確率も含めて考慮します。さらに次のステップでは、攻撃、不正操作、オペレーターのミスなどによって生じるリスクを防御し、軽減するための戦略と対策を盛り込んだ産業サイバーセキュリティのコンセプトを細部にわたり、まとめあげます。また、システムのセキュアな動作や構造を継続的に保証するための方策や規則、ガイドラインも作成します。最後のステップ、「産業サイバーセキュリティのシステム検証」では、実装された対策の有効性を確認します。

セキュアな機械の可用性

産業サイバーセキュリティサービスのプロセスは、サイバー攻撃を軽減または防止するのに役立ちます。意図せずして起こるセキュリティインシデントも減らすことができます。そうすることで機械の稼働率を向上させ、経済効率を維持しながら、最終的なコスト削減を実現できます。

このアプローチでは適切なセキュリティ対策を用いて、主として機械に関わる人員を保護します。なぜなら、セキュリティインシデントは安全対策の妨げにもなるからです。たとえば、機械の前にライトカーテンを設置し、オペレータが危険ゾーンに立ち入らないよう

にしていても、攻撃者が関連のコントローラやメカニズムを侵害することで、ライトカーテンの保護機能が無効化されないとも限らないのです。セキュリティは安全を守ります！

上記のような理由から、機械に実装する際には、安全とセキュリティを合わせて検討するのが理にかなっています。セキュリティなくして安全はなく、安全なくして人を保護することはできないからです！

明確な管理: 誰が機械で何をできるか？

機械とオペレータの安全は、対象が人であろうとネットワークであろうと、ひとえにアクセス制御にかかっています。たとえば、機械の運転中には誰も危険ゾーンに入れないようにするために、入口を不正なアクセスから保護しなくてはなりません。たとえ善意でも、誰かが同時に現場で、あるいはネットワークを介して操作やメンテナンスを行えば、重大な結果を招きかねません。

「Identification and Access Management」(I.A.M.)はそのための重要な要素の1つで、企業における設備や機械への権限やアクセスを明確に管理するものです。その中には、組織的な対策および仕様に加えて、適切な安全機能とセキュリティ機能が含まれます。ピルツのPITreaderのようなアクセス許可システムは、これらの機能を備えた最適な製品コンポーネントです。ユーザは従業員の保護、賠償責任保護、最大生産性、データ保護の観点から、各種の要件を達成できます。

安全とセキュリティに対する総合的なアプローチだけが、人と機械全体の保護を保証します。今後、企業はセキュリティへの取り組みの要否や範囲を自ら決定することはできません。今日ではセキュリ

ティは法的要件の1つなのです。エンジニアリングにおける産業サイバーセキュリティとしてのセキュリティはIT部門だけの仕事ではなく、設計・製造の切り離せない一部です。あとからセキュリティを実装するのは複雑であり、たいていの場合、使いやすさ、機能、生産性の面でマイナスになります。

((文字数: 9,784))

((囲み記事:))

EUの産業サイバーセキュリティ法の概要

特にヨーロッパでは、立法府が脅威レベルに対応する一連の法律を制定しており、その結果、ヨーロッパでは世界のどこより厳格な要件が適用されます。しかし他の国々でもすでに合意は成立していて、いずれ法律として導入される見通しです。産業サイバーセキュリティのグローバルな整合化が進むものと予想されます。

NIS 2: 企業の義務の拡大

NIS (Network and Information Security)はサイバーセキュリティの強化を目的とする欧州連合指令です。2016年に制定され、これまではエネルギー、交通、銀行・金融、健康、飲用水の供給・販売、デジタルインフラといった重要インフラの提供者に適用されていました。そうした分野のサービス提供者は「適切なセキュリティ対策」を導入し、サイバーセキュリティに関わる重大インシデントを報告する義務がありました。新しいNIS 2指令（(EU) 2022/2555 ...

EU全体で共通レベルの高いサイバーセキュリティを実現するための措置）の要件により、将来、サイバーセキュリティのリスク管理対策を求められる企業の数は大幅に増加します。NIS 2では対象分野が拡大され、製造/生産業者、たとえば電気機器のエンジニアリングや製造を行う企業も含むことになります。

要件には情報システム、サプライチェーンの保護、人員の安全に関するリスク分析とセキュリティコンセプトなどに関わるものがあります。アクセス制御や設備管理のコンセプト、さらには管理のためのトレーニングも要求事項に含まれています。

NIS
2指令は2022年の終わりに欧州議会およびEU理事会で採択されました。すべてのEU指令と同様、直ちに個々のEU加盟国で発効して拘束力を持つわけではなく、各国の国内法に統合される必要があります。企業にとって賢明なのは、できるだけ早くNIS
2に対応し、自社の包括的なセキュリティ評価を実施することでしょう。情報セキュリティ管理システム（ISMS）の開発はその一例です。この観点から、情報セキュリティ規格であるISO
27001の認証を取得することは有用です。

例 - 風力タービンの使用に関するNIS 2: NIS
2では将来、発電設備(例:風力タービン)メーカなどの機械製造業者も要件への適合を求められます。そして風力タービンの製造者には、オートメーション用ソリューション、コントローラ、センサなどが必要です。一定規模以上の電気部品メーカにもNIS
2が適用されます。また、NIS
2の規定ではサプライヤーも考慮されるため、ピルツのような企業は安全なサプライチェーンを心がけ、サプライヤーに遵守を求めなけ

ればなりません。このようにNIS
2はサプライチェーン全体に影響します。

新しい機械規則: セキュリティなしではCEマークもなし

機械指令2006/42/ECは、機械の機能安全に関して特に重要です。

機械類をヨーロッパに輸入する場合、機械メーカはこれまで必ず適切な適合性評価の手順を経て、CEマークを表示する必要がありました。

2023年6月に機械規則として再発行されたことを機に、仕様が最新技術に更新されました。法的規則なので、国内法への変換は不要です。機械メーカは新たな要求事項に対応するための移行期間を与えられ、2027年1月20日からはそれらを遵守しなくてはなりません。

この機械規則は現行の機械指令に代わるもので、サイバーセキュリティを必須の義務としている点が機械指令との大きな違いです。機械指令は純粋に安全性を評価するものであるのに対し、新規則はセキュリティ保護の目標を「破損や改ざんからの保護」(Protection against corruption)の章の「必須健康安全要求事項」(Essential health and safety requirements:
EHSR)に定めています。機械の安全機能は、事故や作為による破損や改ざんによる不具合から守られなくてはなりません。

このCEマーキングへの新たな道のりは機械のメーカとオペレータに新たな課題を課すものであり、これまでの安全とセキュリティの概念の見直しを迫るものといえます。

サイバーレジリエンス法: 製品のライフサイクル全体のセキュリティ

企業と機械類の総点検をすることに加えて、セキュリティ対策を装置(制御システムなど)に直接実装することも絶対に必要です。2022年9月、欧州委員会は製品のサイバーセキュリティ強化を目的とする規則のドラフトを提出しました。サイバーレジリエンス法(CRA)の対象は、他製品との通信が可能なデジタル要素(ハードウェアとソフトウェア)を伴う製品の製造業者です。スマートフォンやロボット掃除機のようなB2Cセグメントの製品も、コントローラやセンサ、オペレーティングシステムなどの純粋なソフトウェア製品、機械本体といったB2Bセグメントの製品と同様に、この影響を受けます。

製造業者に対する悪用された脆弱性の報告義務は、2026年9月11日から適用されます。デジタル要素を含む製品をEU市場に投入できるようにするには、2027年12月11日以降、CRAの要件を満たす必要があります。CRAはEU規則であるため、EU加盟国で直ちに有効となります。

実際にCRAの影響がどれほどあるかは、製品を分類するために最終的に設けられる基準によって異なります。CRAの規定によると、適切なレベルのサイバーセキュリティが保証された製品以外は市場に出すことができません。これは製品のライフサイクル全体にわたって適用されます。つまり、セキュリティは製品開発時から始まるのです。こうした理由から、ピルツは数年かけて、開発プロセスをIEC 62443-4-
1「産業用オートメーションおよび制御システムのセキュリティ - 第4-1部:
「安全な製品開発ライフサイクル要求事項」に適合させ、十分なセ

キュリティが実証されたSecurityBridgeなどの製品を開発してきました。

((文字数: 6,062))

Pilz – The Spirit of Safety

ピルツは、オートメーション技術分野の製品、システム、サービスを提供するグローバルサプライヤーです。安全オートメーションの先駆者として、人、機械、環境の安全を創造し続けています。同族企業ピルツの設立は1948年に遡り、現在ではオストフィルダンの本社を拠点として世界各国に42の現地法人・支店、2,500名の従業員を擁しています。

業界の技術リーダーであるピルツは、機械の安全と産業サイバーセキュリティを実現するためのトータルなオートメーションソリューションを提供しています。そのポートフォリオには、センサ、コントローラ、ドライブ技術に加え、産業用通信、診断、視覚化を目的としたシステムが含まれます。また、コンサルティング、エンジニアリング、トレーニングを含む各種サービスも国際的に提供しています。ピルツのソリューションは、機械エンジニアリングの業界にとどまらず、社内物流、包装、鉄道技術、ロボティクスなど、多くの業界で採用されています。

www.pilz.com

ピルツのソーシャルメディア:

ピルツのソーシャルメディアチャネルでは、当社に関する情報やピルツの社員、オートメーション技術の最新ニュースをお知らせし

プレス向け連絡先：

Martin Kurth

企業および技術プレス
電話：+49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

技術および企業プレス
電話：+49 711 3409-7009
s.skaletz-karrer@pilz.de