ICS環境の現場から考える検知・対応の難しさと解消に向けた対応の例

February 2023

pwc

自己紹介、はじめに

エンジニア

PwC

IT

OT (ICS)

ICS環境は業務もシステムも多様です。
また、昨今、サイバー攻撃も巧妙化し、
セキュリティインシデントを100%防ぐことは
できません。

本日は、そのようなICSセキュリティの難しさについて、
経験した内容から、課題や解消の考え方の一例を
ご紹介します。

本内容が皆様の一助になると幸いです。

Agenda

- ICS環境の動向とセキュリティ強化の高まり
- インシデント検知・対応態勢の重要性
- インシデント検知・対応態勢の主な難しさと解消の方向性
- インシデント検知・対応態勢の強化でフォーカスするモノ
- インシデント検知の仕組みの実装（例）
- インシデント検知・対応の手順・教育の実装（例）

ICS環境の動向とセキュリティ強化の高まり

スマートファクトリーをはじめとする生産活動や研究のDX化が進み、ICS環境やそれとつながるサプライチェーンを狙う攻撃が増えています。これを受け、ICSセキュリティ強化の重要性が高まっています。

生産／研究のDX化

IT／ICS環境のDXは、企業の成長の動力
コネクティビティの急増は、リスクをも急増させる

- IoTセンサー、タブレットなどによる生産活動の効率／品質向上
- AIを活用した生産データの分析・制御・最適化　など

脅威の活発化

攻撃者が対策が施されているIT環境から、
マネタイズしやすいICS環境へシフト、手法も巧妙化

- ICS環境におけるランサムウェアの被害事例
- 制御機器やカメラへの不正アクセスの被害事例　など

社会的な気運の高まり

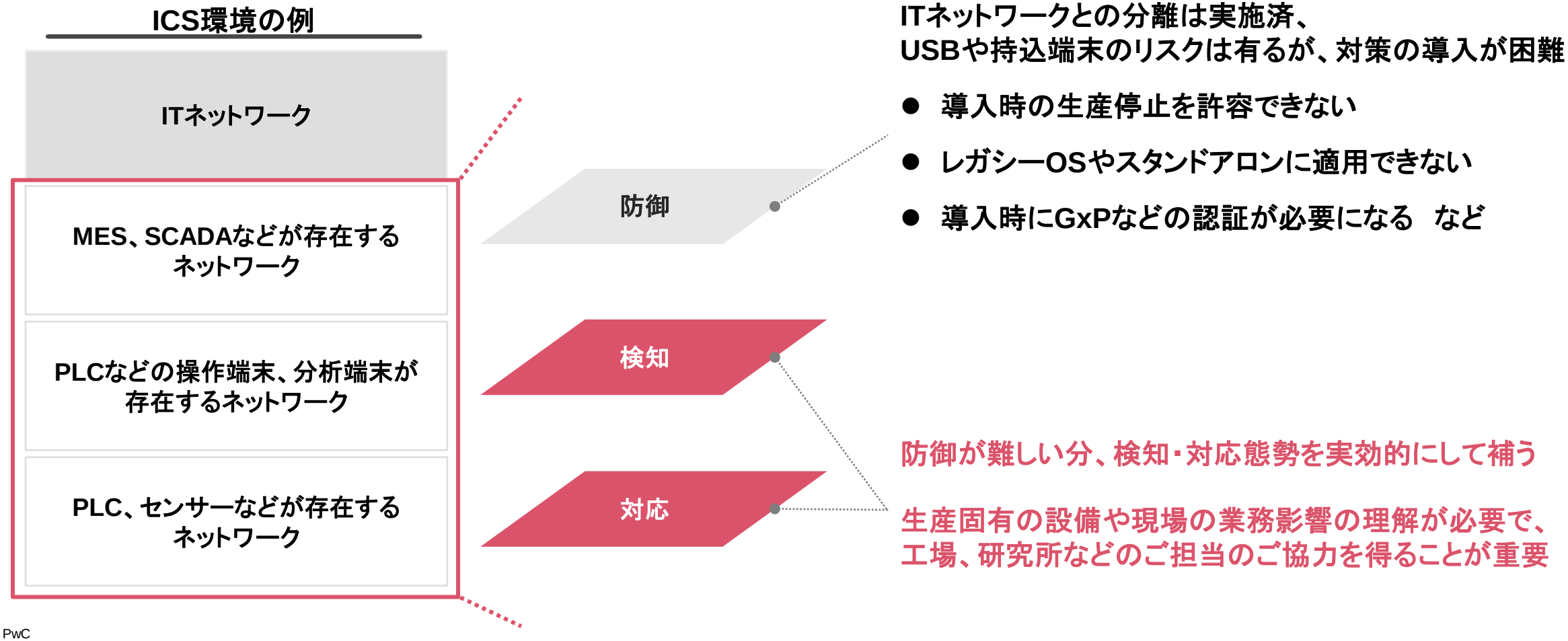
生産／研究のDX化や脅威の活発化を受け、
社会的にICSセキュリティ強化の気運が高まっている

- 各機関から規制やガイドラインが公開
- 取引先との委託契約における要件の追加　など

ICS環境のセキュリティ強化の重要性が高まる

インシデント検知・対応態勢の重要性

ICS環境では生産を停止できないという制約が有り、防御を目的とした技術的な対策の導入が困難であることから、インシデント検知・対応態勢にフォーカスすることも効果的な強化の戦略です。



ITネットワークとの分離は実施済、
USBや持込端末のリスクは有るが、対策の導入が困難

- 導入時の生産停止を許容できない
- レガシーOSやスタンドアロンに適用できない
- 導入時にGxPなどの認証が必要になる　など

防御が難しい分、検知・対応態勢を実効的にして補う

生産固有の設備や現場の業務影響の理解が必要で、
工場、研究所などのご担当のご協力を得ることが重要

インシデント検知・対応態勢の主な難しさと解消の方向性

ICS環境は企業、工場毎に多様であるものの、インシデント検知・対応態勢整備における主な難しさの解消に向けて、リスクベースで対象を絞るアプローチも有効です。

	主な難しさ	解消の方向性
プロセス	工場、研究所のシステム環境を考慮した上で、調査／隔離などの対応手順を整備するための**マンパワーや専門性が不足している** **社内外ステークホルダー連携の整備が難しい**	**攻撃者に狙われやすく、利用が多いシステム**に絞り、手順を整備し、工場、研究所横断で展開する 上記手順を整備する際、**どのタイミングでどのような情報**があれば、説明性を確保できるのか考慮する
ヒト	工場、研究所で調査／隔離などの対応を担う**マンパワーや専門性が不足している**	**攻撃者に狙われやすく、利用が多いシステム**に絞り、教育や採用などを実施する
モノ	防御策が導入されておらず、**アラートを送信できる対策**が無い	**システムに標準で搭載されている機能**（ログなど）を使う

インシデント検知・対応態勢の強化でフォーカスするモノ

攻撃の起点となり、工場／研究所横断で導入数が多いシステムや設備はWindowsである場合が多く、それを対象に態勢を整備する方法も考えられます。

ICS環境の例

ITネットワーク

MES、SCADAなどが存在するネットワーク

PLCなどの操作端末、分析端末が存在するネットワーク

PLC、センサーなどが存在するネットワーク

PLCなどが攻撃者から直接攻撃を受けることは稀

フォーカスするモノの例

Windowsにフォーカスすると良いのではないか

PCのOSとして最も利用が多い

PwCが確認した各種事例において、Windowsが工場で占める割合は70%以上

- PLCなどのプログラムを作成・書き込むソフトウェアの導入OSとして広く用いられている
- 研究や分析などで使うソフトウェアの導入OSとして広く用いられている

攻撃者に狙われやすい

PCが不正に操作され、そこからその奥にある設備が攻撃されることが多い

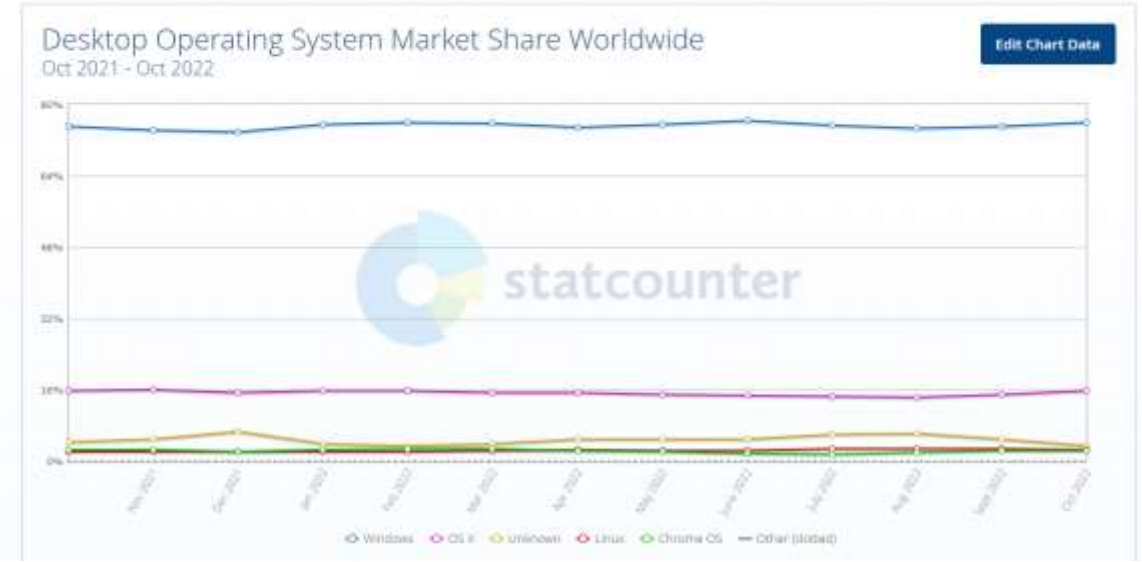
- USB接続、外部（IT／インターネット）接続、メールなど侵入口である
- 世間的に知られている脆弱性が多い

ご参考）PCやタブレットのOSのシェア

PCのOSのシェアはWindowsが多い

Windows	OS X	Unknown	Linux	Chrome OS	FreeBSD
75.93%	15.74%	3.34%	2.6%	2.38%	0.01%

Desktop Operating System Market Share Worldwide - October 2022



タブレットのOSのシェアは他のOSが多く、Windowsは少ない

iOS	Android	Linux	Windows	Unknown	BlackBerry OS
50.7%	49.18%	0.05%	0.03%	0.03%	0.01%

Tablet Operating System Market Share Worldwide - October 2022

タブレットのシェアという視点だとまだ少ないものの、
HMIやPLCでWindowsの活用が出てきている

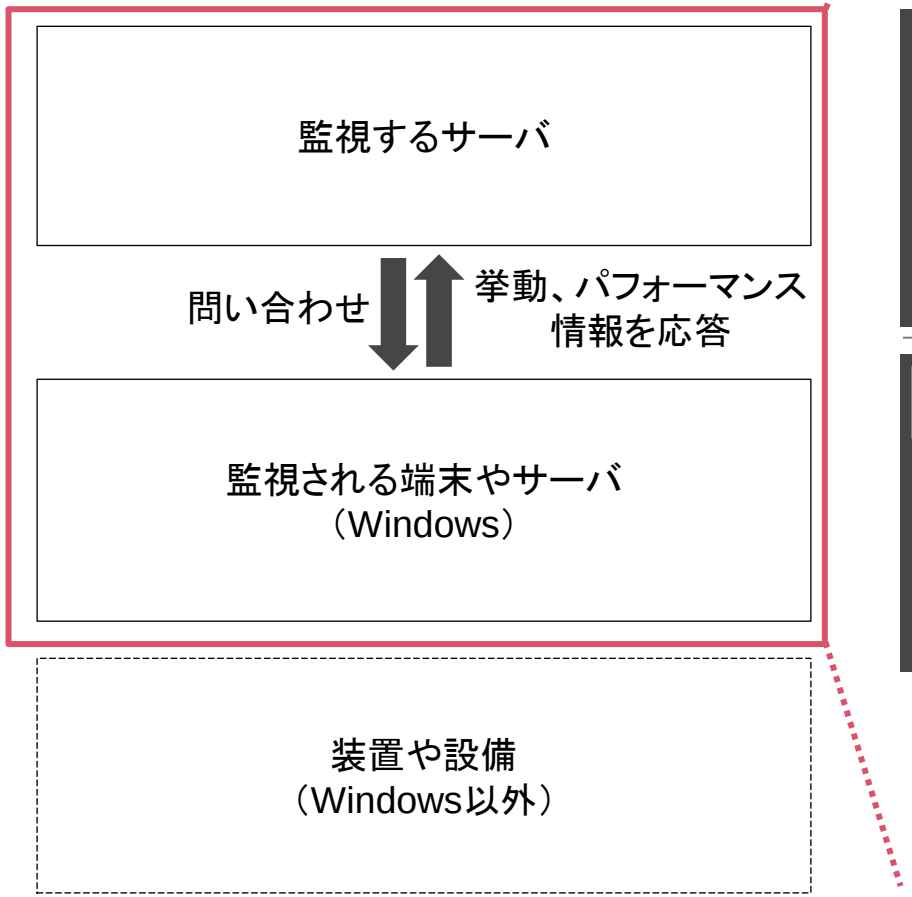
Statcounter, 2022, “Desktop Operating System Market Share Worldwide | Statcounter Global Stats” Accessed Nov 30, 2022. https://gs.statcounter.com/os-market-share/desktop/worldwide

Statcounter, 2022, “Tablet Operating System Market Share Worldwide | Statcounter Global Stats” Accessed Nov 30, 2022. https://gs.statcounter.com/os-market-share/tablet/worldwide

インシデント検知の仕組みの実装（例）

生産影響や規制、研究や生産設備の仕様の影響を受け、ソフトウェアの導入が難しいことから、Windowsの標準機能であるリモート管理のAPIやイベントログなどを用いて監視します。

構成イメージ



実装方法

監視

Windows標準のリモート管理のAPIを用い、
イベントログやパフォーマンスを監視

検知

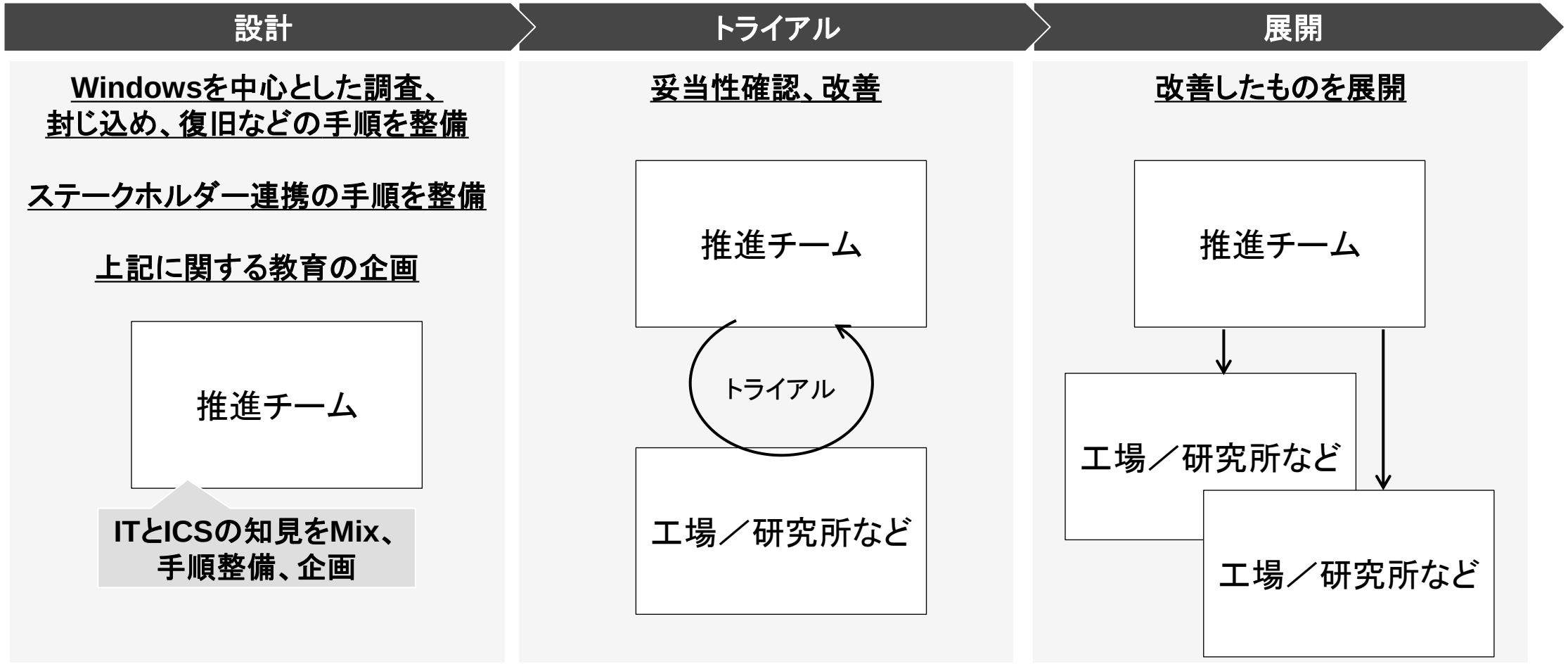
通常業務で発生しない、または
通常業務で発生することが稀であれば、異常と検知

- 業務上利用しないアカウントの利用
- 業務上利用しないサービスの起動
- CPUやメモリの高騰　など

工場／研究所は定型プロセスが確立していることがあり、
そこからの逸脱はインシデント懸念と見なすことができるのではないか

インシデント検知・対応の手順・教育の実装（例）

調査、封じ込め、連携などの対応手順や教育を推進チームにて整備し、特定の工場／研究所でトライアル、その後、展開するといったアプローチでIT、ICS、本社、工場／研究所などが協力して推進します。



クロージング

ICSセキュリティには様々な難しさが有りますが、
インシデント検知・対応態勢は論点が多く、
特に難易度が高い活動だと思います。

今回は、システム的な例を中心としましたが、
社内の危機管理態勢、社外の消費者や取引先への
情報公開の内容やタイミングなども整備が必要です。

大変さは有るものの、インシデント検知・対応態勢は、
製品生産や研究への被害の低減に直結する
重要なもので、**ICSのご担当、ITのご担当で協力し合い、リスクベースでポイントを絞る**ことで、
難しさを軽減して取組むことができるのではないでしょうか。

本内容が皆様の一助になると幸いです。ご清聴ありがとうございました。

Thank you

www.pwc.com/jp