制御システムにおける
CTEMを活用したリスク低減策

2025/2/5(水) 14:05～14:35
制御システムセキュリティカンファレンス2025

Claroty Ltd. APJ Sales
Solution Engineer 加藤 俊介

発表者紹介

NCEES
FE Exam

TÜVRheinland®
FS Engineer

ISA/IEC 62443 CYBERSECURITY EXPERT ISA

クラロティ　アジア太平洋・日本地区 営業部
シニアソリューションエンジニア

加藤　俊介

2015年4月~ 2018年3月 (3年)
化学メーカーエンジ 計装・制御システムエンジニア

2018年4月~2022年5月 (4年)
制御機器メーカー 安全計装システムエンジニア

2022年5月～現在
現職

CLAROTY

目次

1. 会社紹介
2. セキュリティ対策の全般の課題
3. CTEMについて
4. CTEMの制御システムへの適用
5. まとめ

CLAROTY

会社紹介

当社プロフィール

CLAROTY(クラロティ)

Clarity (透明性・明瞭さ) + OT (Operation Technology)

2015年
設立年

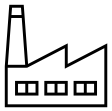
$735M
資金調達

+680
従業員数

59カ国
展開地域・国

+$100M
年間定期利益

20%
グローバルでの実績
(Fortune500)



+10,000
導入工場数

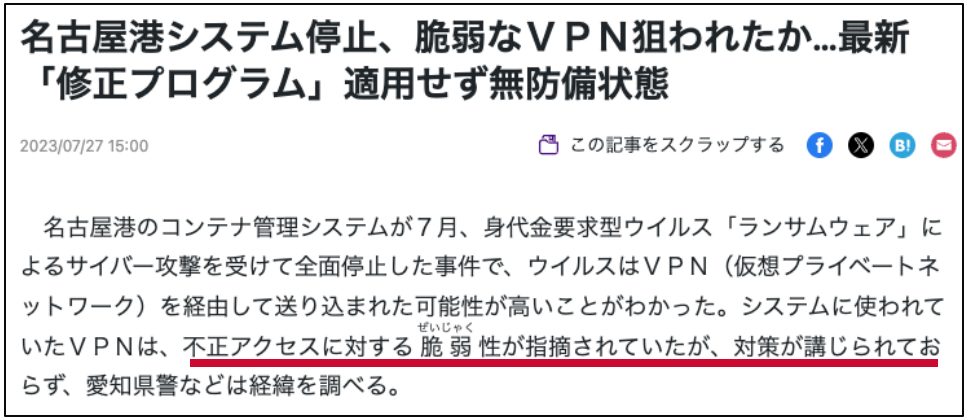
3600%
国内市場成長率

セキュリティ対策の全般の課題

CLAROTY

セキュリティ製品を入れれば、安心?

事業インパクトを見据えた上での脆弱性対策が必要



名古屋港システム停止、脆弱なＶＰＮ狙われたか…最新「修正プログラム」適用せず無防備状態

2023/07/27 15:00

この記事をスクラップする

名古屋港のコンテナ管理システムが７月、身代金要求型ウイルス「ランサムウェア」によるサイバー攻撃を受けて全面停止した事件で、ウイルスはＶＰＮ（仮想プライベートネットワーク）を経由して送り込まれた可能性が高いことがわかった。システムに使われていたＶＰＮは、不正アクセスに対する脆弱性（ぜいじゃく）が指摘されていたが、対策が講じられておらず、愛知県警などは経緯を調べる。

JAXA、23年の不正アクセス詳細公表　VPN機器の脆弱性突かれ、Microsoft 365のアカウント情報など盗まれていた

2024年07月05日 15時41分 公開

[ITmedia]

印刷　見る　Share　47　1

JAXA（宇宙航空研究開発機構）は7月5日、2023年に受けた不正アクセスの詳細を発表した。VPN機器の脆弱性を狙った攻撃による不正アクセスを受け、職員の個人情報を含む一部の情報が漏えいしていたという。漏えいした情報の詳細は「相手方との関係もあることから差し控える」としている。

脆弱性対応の未実施による事業インパクトに関する意識がなかったのでは?

このような事業インパクトが想定されていれば、脆弱性対応も優先度が高かったはず。

CLAROTY

ICSセキュリティの現在地

OTシステムをターゲットとした攻撃のインパクトは大きい

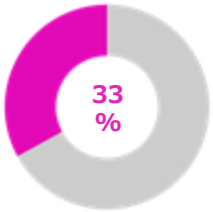
財政的なインパクト

インパクトの主な要因

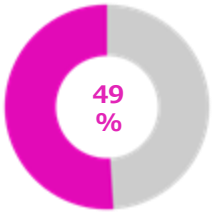
- 売上の喪失
- 復旧コスト
- 従業員の残業コスト

53% 暗号化されたシステムへのアクセスを回復するため、50万ドル以上の身代金要求に対応した

操業に関わるインパクト

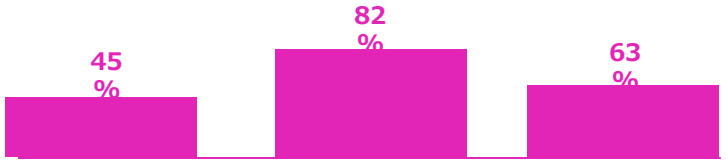


丸１日もしくはそれ以上の操業停止が報告されている



12時間以上のダウンタイムが発生し、復旧に1週間以上要した

リモート&第三者からのアクセス



自組織のCPSの少なくとも半数がインターネットに接続されていると回答。

第三者からのアクセスにるサイバー攻撃を少なくとも一度は経験している

CPSネットワークへのサードパーティの接続について、部分的にしか理解していない。

https://claroty.com/ja/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions

ICSを標的としたサイバー攻撃の結末は最悪

インシデントの後にアクシデントが発生し得る

生産プロセスの中断

サイバー攻撃やシステム障害により、生産ラインが停止する可能性が増大。これにより、工場で作業する従業員の安全性が脅かされるだけでなく、製品の品質や納期にも影響を及ぼす。

装置やシステムの誤動作

サイバー攻撃によって産業用制御システムが操作されると、装置が誤作動するリスクがある。例えば、温度や圧力の制御が失われることで、火災や爆発のリスクが高まる。

安全対策の無効化

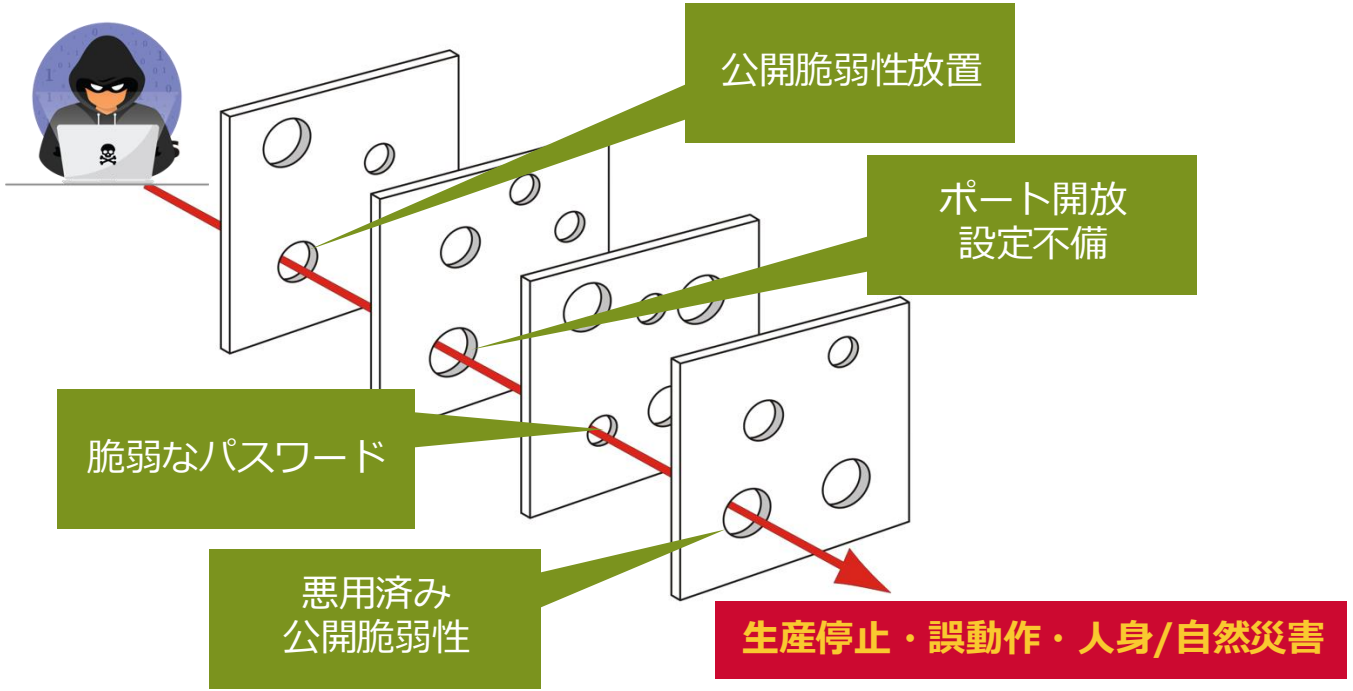
攻撃者が安全システムや緊急停止装置を無効にすることで、事故が発生した際の被害が拡大する可能性が増大。リスクを軽減するための仕組みが機能しなくなることで、重大な人的被害につながる。

人命または環境への直接的な危険

特定のセクター(化学工場や発電所など)では、重要インフラへの攻撃が人命に直接的な危険をもたらす可能性が増大。毒性物質の漏洩や電力供給の停止が発生すると、従業員や地域住民に対して深刻な影響を及ぼす。

事業インパクトを見据えた対策が必要

システム全体を捉えた予防保全対策・設定不備確認が必要



https://ja.wikipedia.org/wiki/%E3%82%B9%E3%82%A4%E3%82%B9%E3%83%81%E3%83%BC%E3%82%BA%E3%83%A2%E3%83%87%E3%83%AB

CTEMについて

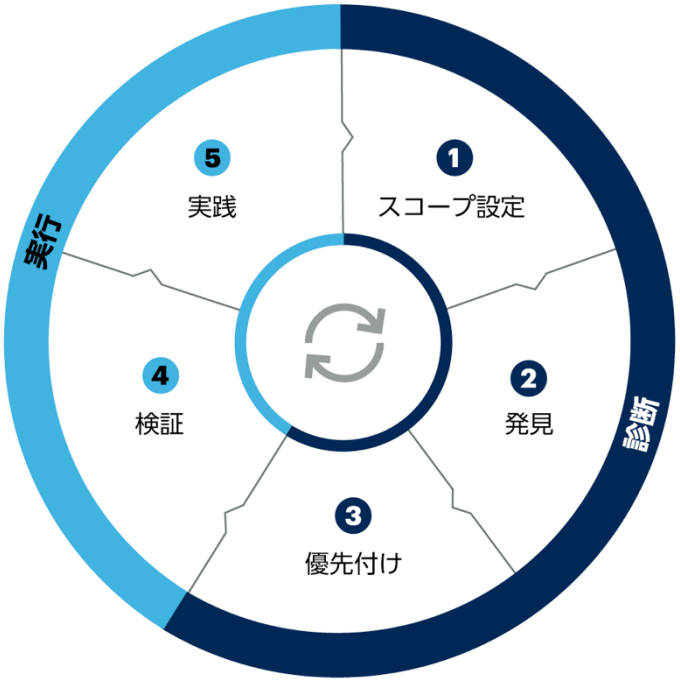
CTEM: 継続的エクスポージャー管理とは?

動的にセキュリティ体制を評価し、優先順位付けをした対策

CTEMとは?

ガートナーによって提唱されている、組織がサイバーリスクを継続的に管理し、セキュリティ態勢を改善するための、反復的なプロセス。

CTEMプログラムに基づいてセキュリティ投資を優先する組織は、侵害を受ける可能性が3分の1になると予測されています



CTEM プログラムの導入、2022年、ガートナー社

CTEMが提唱されている背景

攻撃対象の広がりや高度化する脅威への追従

従来の対策限界

従来のセキュリティ対策は、特定の脅威に焦点を当て、定期的な評価に依存する傾向。しかし、サイバー攻撃は高度化・多様化し、従来の対策では変化する脅威に対応しきれなくなった。

攻撃対象の拡大

ITシステムだけでなく、OT（運用技術）、IoT（モノのインターネット）デバイスなどの接続性が増加。
従来のセキュリティ対策では管理が難しく、新たな脆弱性や攻撃の入り口となっている。

事業継続性の重要性

サイバー攻撃によるシステム停止や情報漏洩が、事業継続に大きな影響を与えることが明らかになっている。特に、重要インフラを支える制御システムは、攻撃を受けると社会全体に甚大な被害をもたらす可能性がある。

リスクマネジメント強化

国際標準規格や各国のセキュリティガイドライン等においても、リスクアセスメントの実施が求められており、CTEMはこれらの要請に対応。

従来の脆弱性対策との比較

これまでの脆弱性対策との異なり、動的な評価で継続的に実施

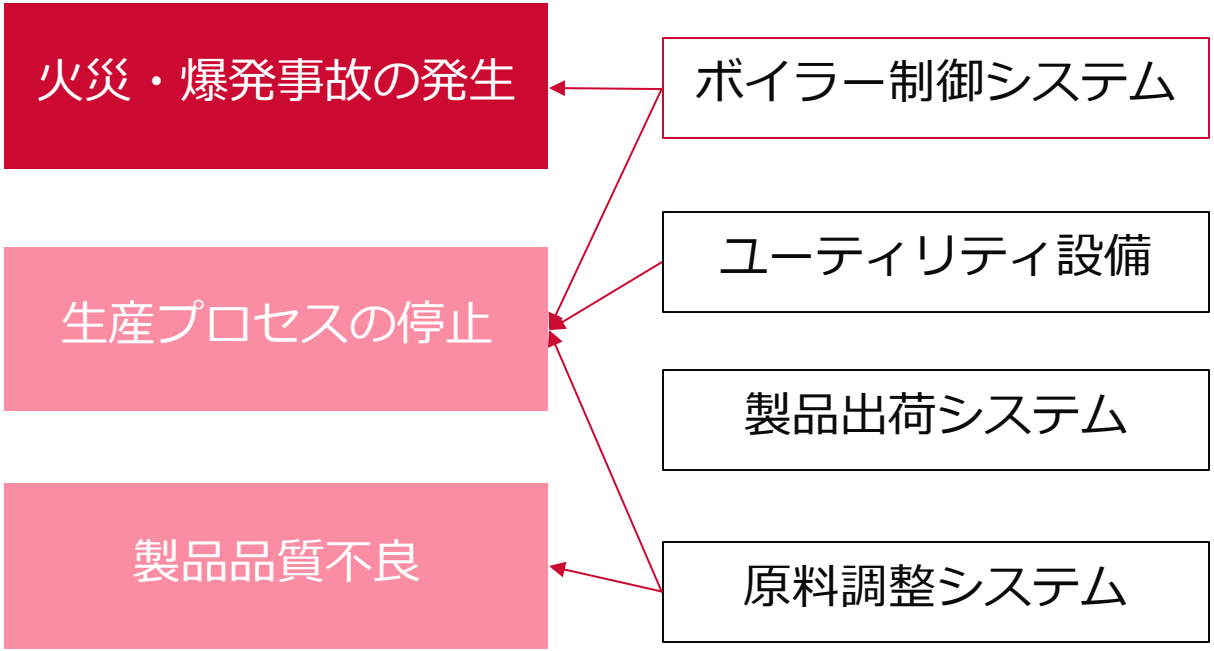
項目	CTEM	従来の方法(SSVC/ICS-Patch)
目的	全体的なリスク管理	個別脆弱性への対応
評価基準	事業インパクト重視	技術的要素を中心
運用方法	継続的・動的	一度きりの意思決定
対応範囲	広範な攻撃対象領域と多様なシステム	限定的（特定の脆弱性や資産）
リスク評価の視点	マクロ視点 (事業全体を俯瞰)	ミクロ視点 (個別の脆弱性)
継続性	高い 環境の変化に対応し継続的に見直し	低い 評価後の再検討が少ない

CTEMの制御システムへの応用

CLAROTY

フェーズ1: スコープ設定

例えば想定事業被害ベースでの範囲設定

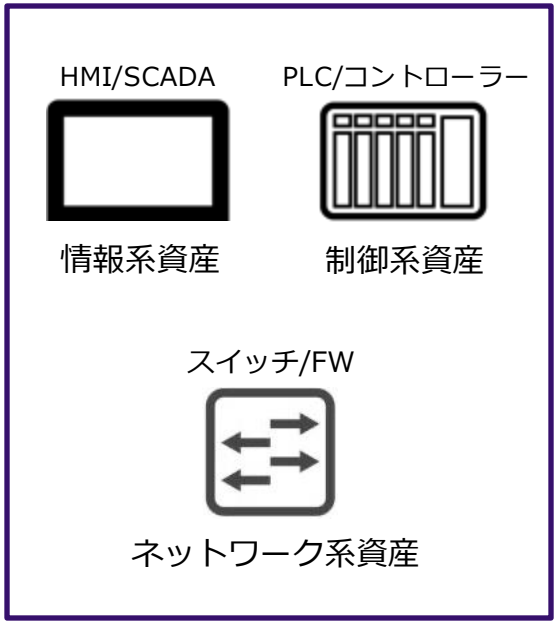


フェーズ2: 発見

範囲設定したシステムを構成する、資産情報を収集

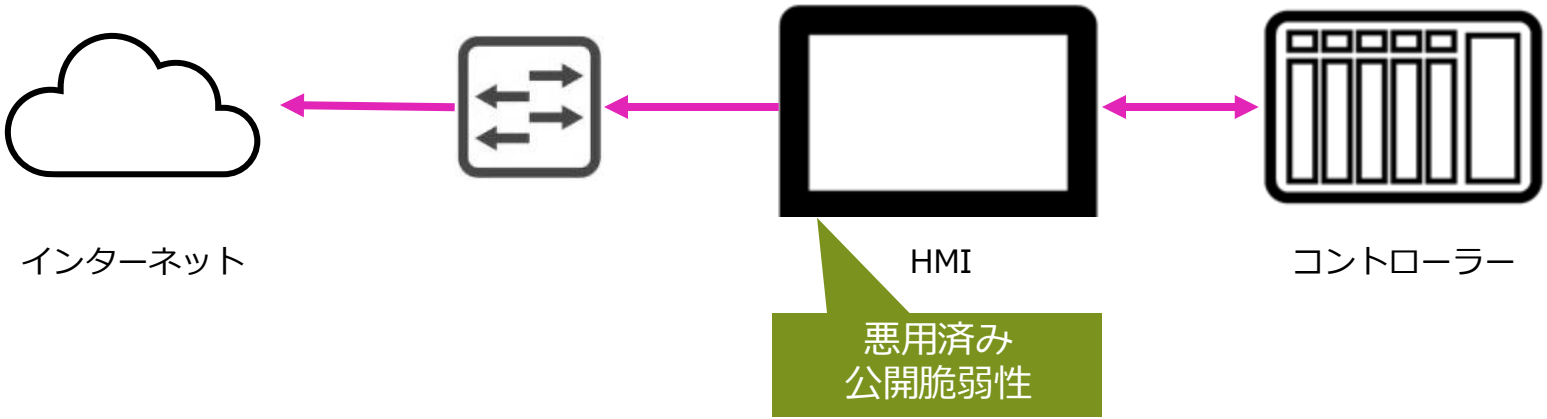
資産情報	**接続性**	**運用**
資産名	回線種類	定常稼働・非定常稼働
資産種別	接続先ネットワーク	設置場所
機能	管理ポートの接続先	構築ベンダー
IP/MACアドレス	使用するプロトコル	資産の担当者/責任者
操作I/Fの有無	データの種類と経路	
機器メーカー	無線機能の有無	
OS種類/バージョン		
▼	▼	▼
事業インパクトや脆弱性判断に必要	攻撃経路や通信の脆弱性判断に必要	実践フェーズにおいて対策を講じる際に必要

資産種別例



フェーズ3: 優先付け (状態ベース)

デバイス種類 + 公開脆弱性 + データフロー(通信状況)の組合せ



現状　資産種類がHMIで、悪用済みの公開脆弱性が該当し、インターネットに対して通信している。

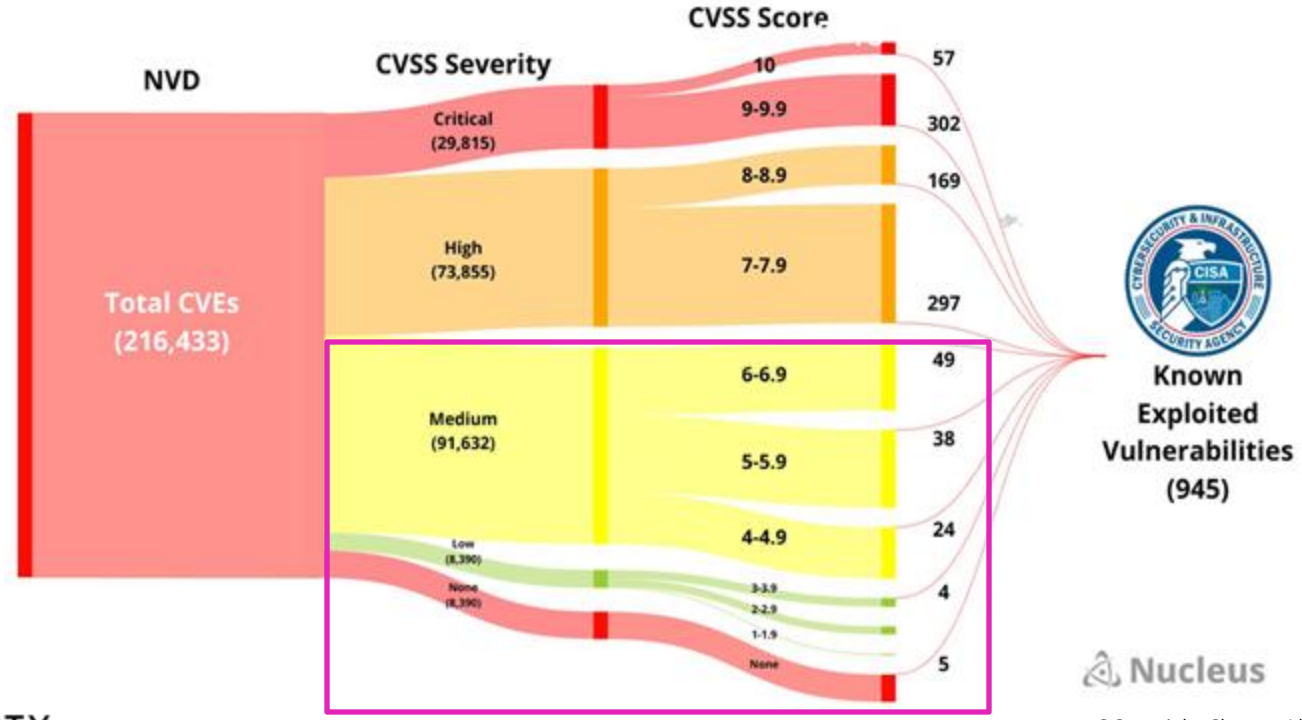
シナリオ　外部から脆弱性を付いた攻撃がされ、HMI端末が乗っ取られ、コントローラーを不正に操作される。

事業インパクト　コントローラーに不正な制御値が書き込まれ、制御対象が危険な状態に遷移し、爆発が発生する。

CLAROTY

優先付け時に参考にしたい指標

CVSSスコアHigh以上だけの対策では、悪用される脆弱性が見逃される



見逃されてる!

フェーズ3: 優先順位付け (リスク値ベース)

リスク値を定量化することで、その定量値に基づき優先順位付け

対象システムを構成する資産群

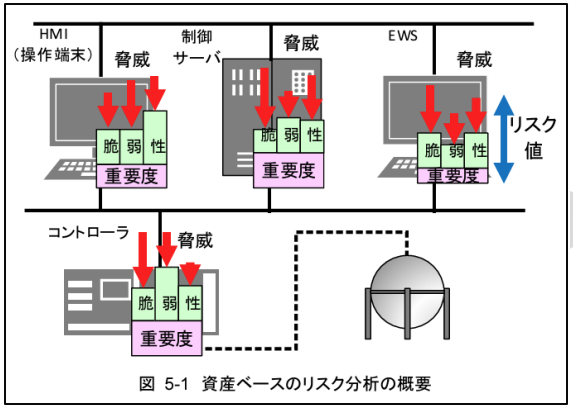


図 5-1 資産ベースのリスク分析の概要

https://www.jpa.go.jp/security/controlsystem/ug65p900000019b kg-att/begoj900000 00hpm8.pdf

資産ベースのリスク分析

資産情報	リスクスコア
HMI	68
SCADA	65
EWS	48
PLC	38
RTU	28

優先度高

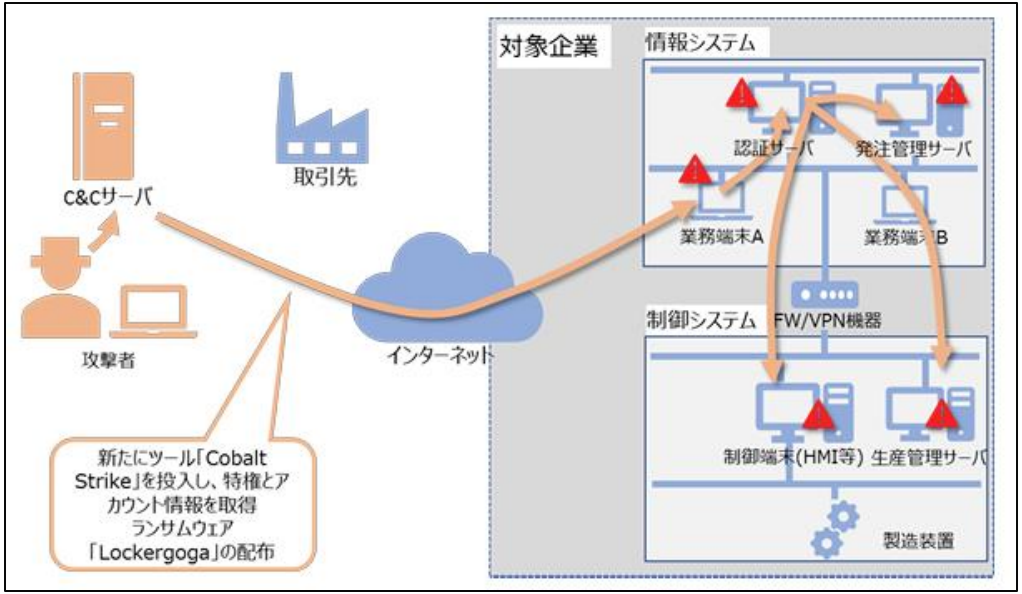
各資産のリスクスコア化

フェーズ4: 検証

本当に攻撃が可能かを検証

- 一般的なセキュリティ対策では、ペネトレーションテストなどが方法として考えられる。
- しかしICSにおいては実施できるタイミングが限られており、可用性への影響懸念が大きい。
- 机上ベースで各種ネットワークパケットや設定ファイルなどのエビデンスベースでの検証が現実的

エビデンスの例:
- PLCの設定ファイル
- 情報系資産のホストFW設定
- ネットワークパケットキャプチャ

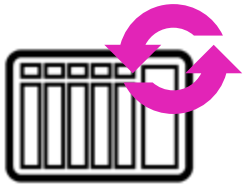


https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000080702.pdf

フェーズ5: 実践

エンドポイントもしくはネットワークベースでの対策

エンドポイント側の対策



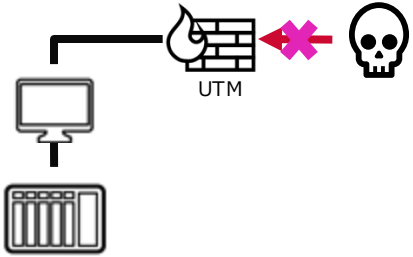
本質的対策

- ファームウェア更新
- セキュリティパッチ適用

ハードニング

- ポート/プロトコル制限
- IPアドレス制限

ネットワーク側の対策



対策

- セグメント化(VLAN)
- エンドポイント間のポート/プロトコル制限
- IPアドレス制限

- 仮想パッチ
- IPSシグニチャーの有効化

フェーズ5: 実践 (PLC)

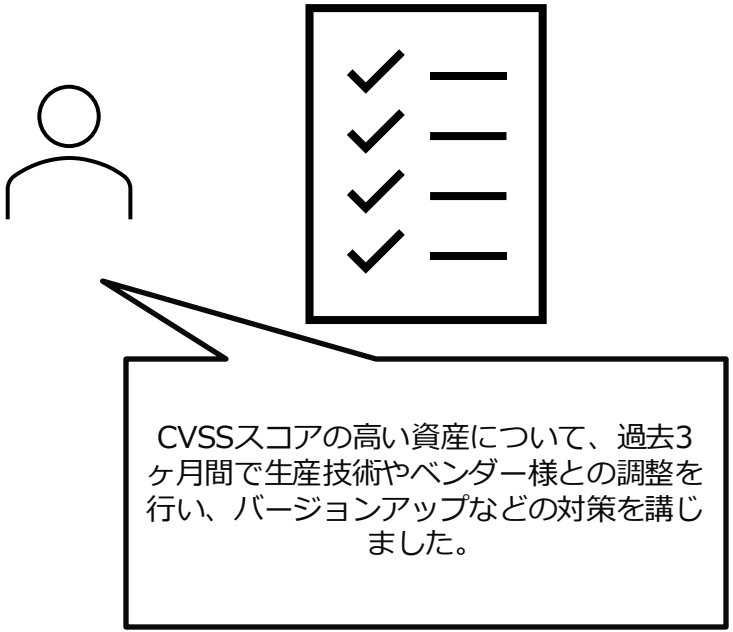
Secure PLC coding Practiceによるコントローラーの対策例

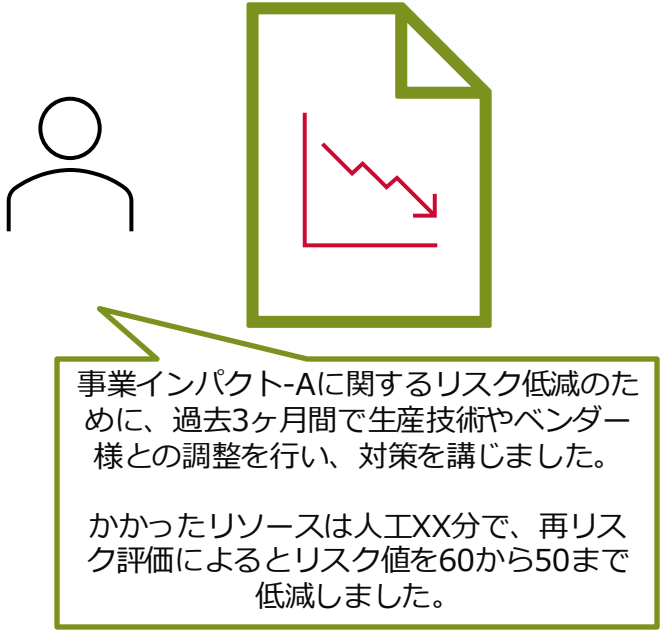
対策項目	対策の目的
運転モードの追跡	RUNモードであることを常時監視、異常な状態を検知 不正なコード変更のリスクを低減 プラント内の作業状況を把握
HMI入力のPLCレベルでの検証	HMIからの入力をPLCレベルで検証し、不正な値をブロックします。 これにより、悪意のある攻撃者がPLCに不正な値を送信するのを防ぎます
PLC再起動時の安全なプロセス状態の定義	PLCの再起動時に、プロセスが安全な状態になるように構成します。 予期しない再起動が発生した場合でも、プロセスが安全に再開できるようにします。

https://plc-security.com/content/Top_20_Secure_PLC_Coding_Practices_V1.0.pdf

フェーズ5: 実践 (レポーティング)

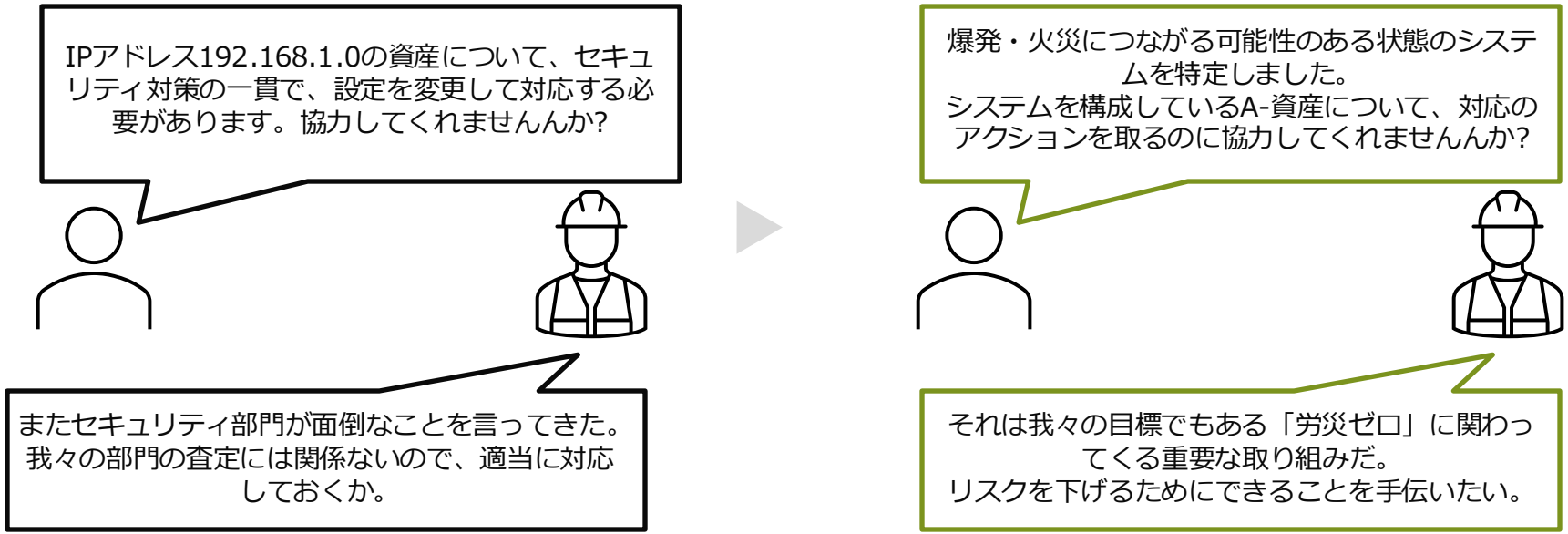
リスク低減を軸にしたROIのわかるレポートは効果的





フェーズ5: 実践 (対策実施時のステークホルダー)

事業インパクトは部門・組織間を超えた会社としての共通目的



CLAROTY

まとめ

CLAROTY

制御システムにおけるCTEMを活用したリスク低減策

継続的なセキュリティの改善活動のために

1. 対策実施によりセキュリティが担保されるという時代ではなくなってきているため、継続的な状況把握が必要。

2. 1つの脆弱性や1つの資産でなく、システム全体で見た上で、優先順位付けして対策を講じ、最大のリターン(リスク低減)を狙うことはできる。リスクスコアはその指標となり得る。

3. 事業被害などの企業にとってのビジネスインパクト起点で、セキュリティ対策を考えることで、合理性が見せやすくなる。

CLAROTY

ありがとうございました。

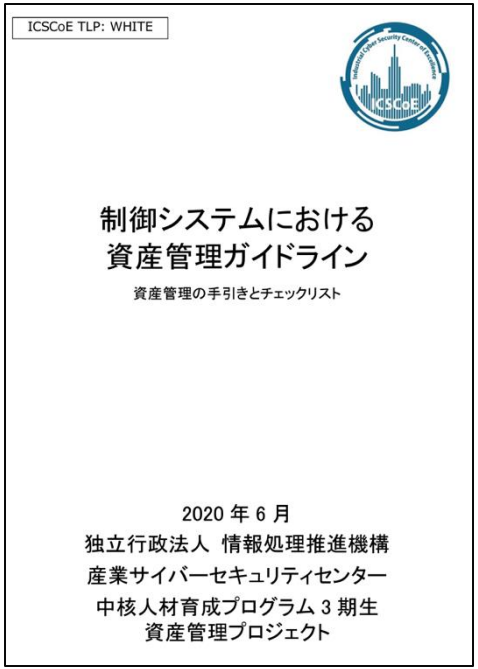
Contact information here

CLAROTY

参考文献

https://www.ipa.go.jp/security/controlsystem/ssf7ph0000009qnw-att/000069438.pdf

https://www.ipa.go.jp/security/controlsystem/ug65p900000019b-kg-att/begoj900000h pm8.pdf



https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2020/ng93u0000002jif-att/000083594.pdf