制御システムの脆弱性管理の課題とグローバルにおける事例

2024/2/7(水) 制御システムセキュリティカンファレンス

Claroty Ltd.

APJ Sales / Solution Engineer

加藤　俊介

目次

1. 会社・発表者紹介
2. 脆弱性管理を取り巻く状況と重要性
3. 脆弱性管理の課題(特定、追従、優先付け)
4. グローバルにおける事例
5. まとめ

1. 会社・発表者紹介

クラロティとはどんな会社？

会社の名前の由来

Clarity (透明性・明瞭さ) + OT (Operation Technology: 工場などの生産システム)

当社はOT含むXIOT向けにセキュリティソリューションを提供するアメリカのスタートアップ企業です

製造業

公共設備

石油/ガス

化学

自動車

食品＆飲料

ビルオートメーション

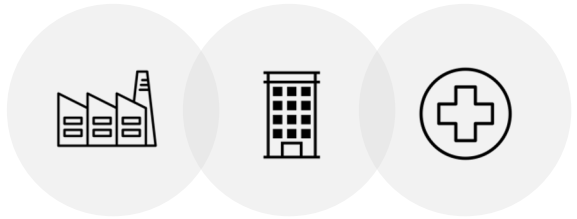
ヘルスケア・
ライフサイエンス

会社概要

本社: 米ニューヨーク	設立年: 2015年	資本金: $640M (約857億)	導入実績: +10,000
従業員数: 500+	収益成長率: 1,139%	拠点: ロンドン、フランクフルト、シンガポール、ソウル、メルボルンなど	

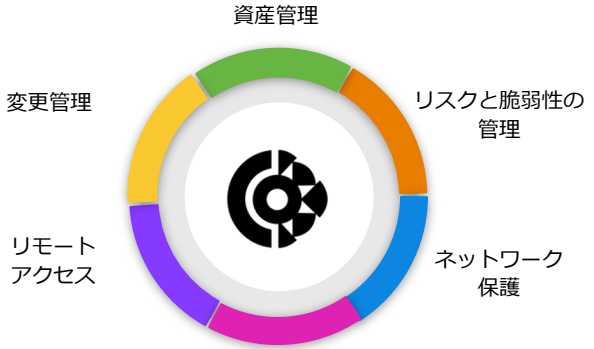
業界最高水準の専門知識

拡張型IoT(XIoT)



インダストリアル　エンタープライズ　ヘルスケア

包括的なソリューション



グローバルにおける実績

顧客数800+, 導入:10,000+, 国: 50+, 業界: 25+

第三者からの高い評価

SC 2022 awards EUROPE

DEVELOPMENTAL TESTING AND EVALUATION DESIGNATION SAFETY ACT

FORRESTER WAVE LEADER 2021 Industrial Control Systems (ICS) Security Solutions

BEST IN KLAS HEALTHCARE IOT SECURITY 2021 / 2022 / 2023

500 Technology Fast 500 2022 NORTH AMERICA Deloitte.

READERS' CHOICE AWARDS 2022 CYBERSEC CLAROTY Best in OT, IoT & Supply Chain Security 2022

自己紹介

ミッション: セーフティーxセキュリティでDXを推進する

クラロティ　アジア太平洋・日本地区 営業部
ソリューションエンジニア
加藤　俊介

2015年4月~ 2018年3月: 国内大手化学メーカー
計装・制御システムエンジニア

2018年4月~2022年5月: 海外大手制御機器メーカー
安全計装システムエンジニア

2022年5月～現在:現職

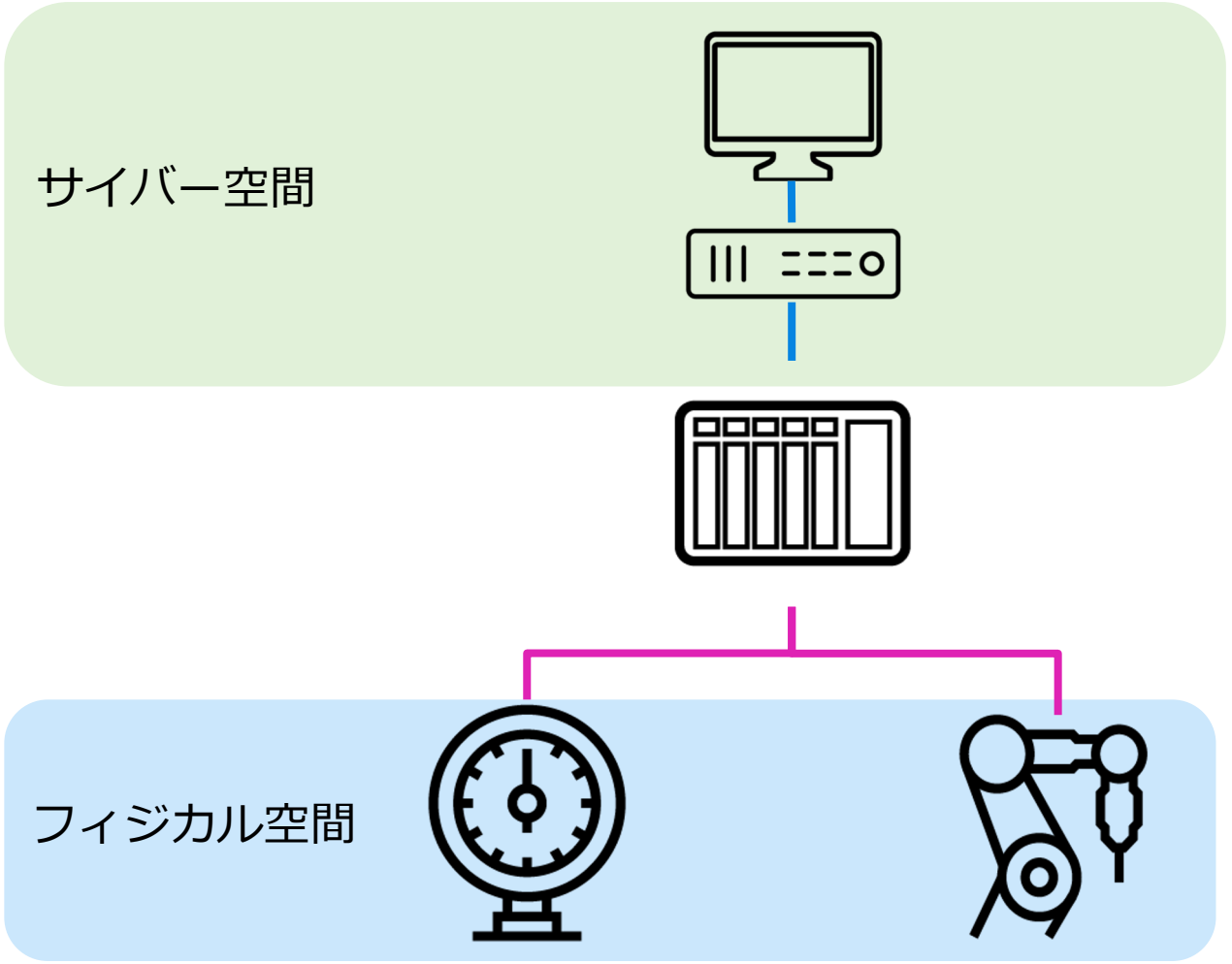
2. 脆弱性管理を取り巻く状況と重要性

制御システムの性質

DCSやPLC, RTUはフィジカル空間(現実世界)とサイバー空間を隔てるデバイスである。

現実世界に影響を与えられる。
例) ポンプを起動する、アームを動かす

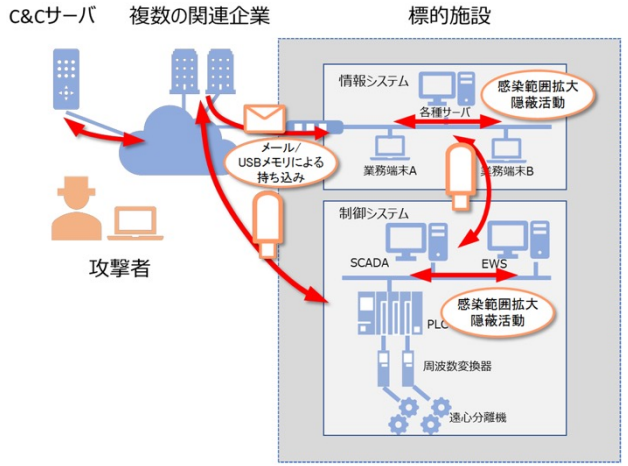
誤った動作は環境破壊・人身事故などを引き起こす可能性がある。



制御システム本体の脆弱性を悪用した攻撃は、環境・経済・安全への影響がある。

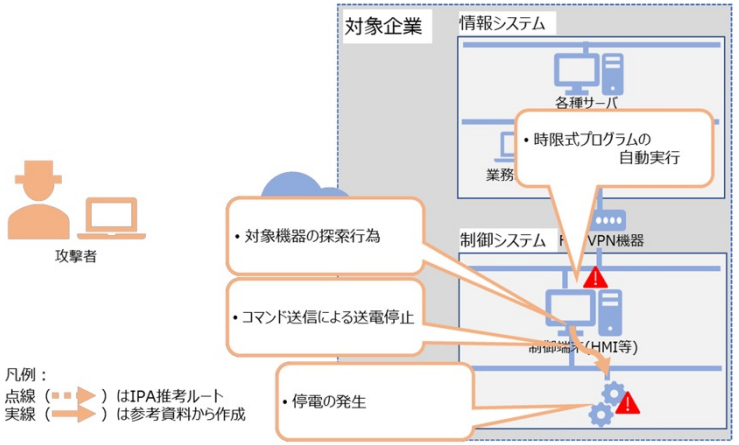
制御システムが被害・標的となったインシデント事例

2010: Stuxnet



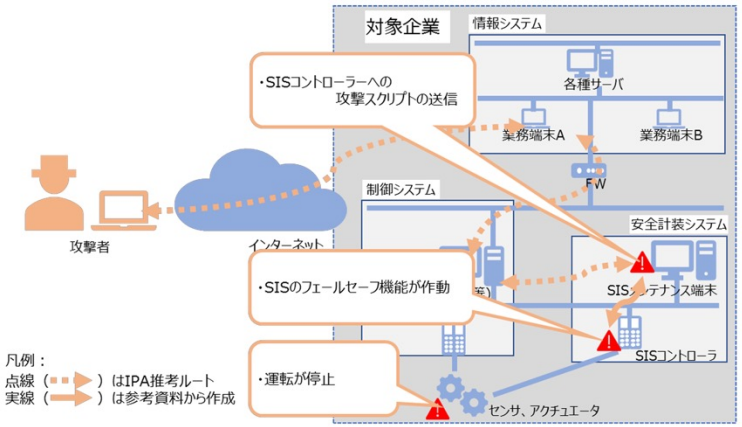
ドイツのSiemens社の**PLCの脆弱性を標的**とし、遠心分離機の回転周波数を変更した。

2016: Industroyer



遮断器に対して直接制御コマンドを送信し、遮断器を開閉した。ドイツのSiemens社の**PLCに対してDoS攻撃**をしかけるプログラムも含まれていた。

2017: HatMan



メンテナンス端末に導入した不正プログラムから**攻撃用スクリプトが安全PLC**に対して送信、書き込みが行われた。

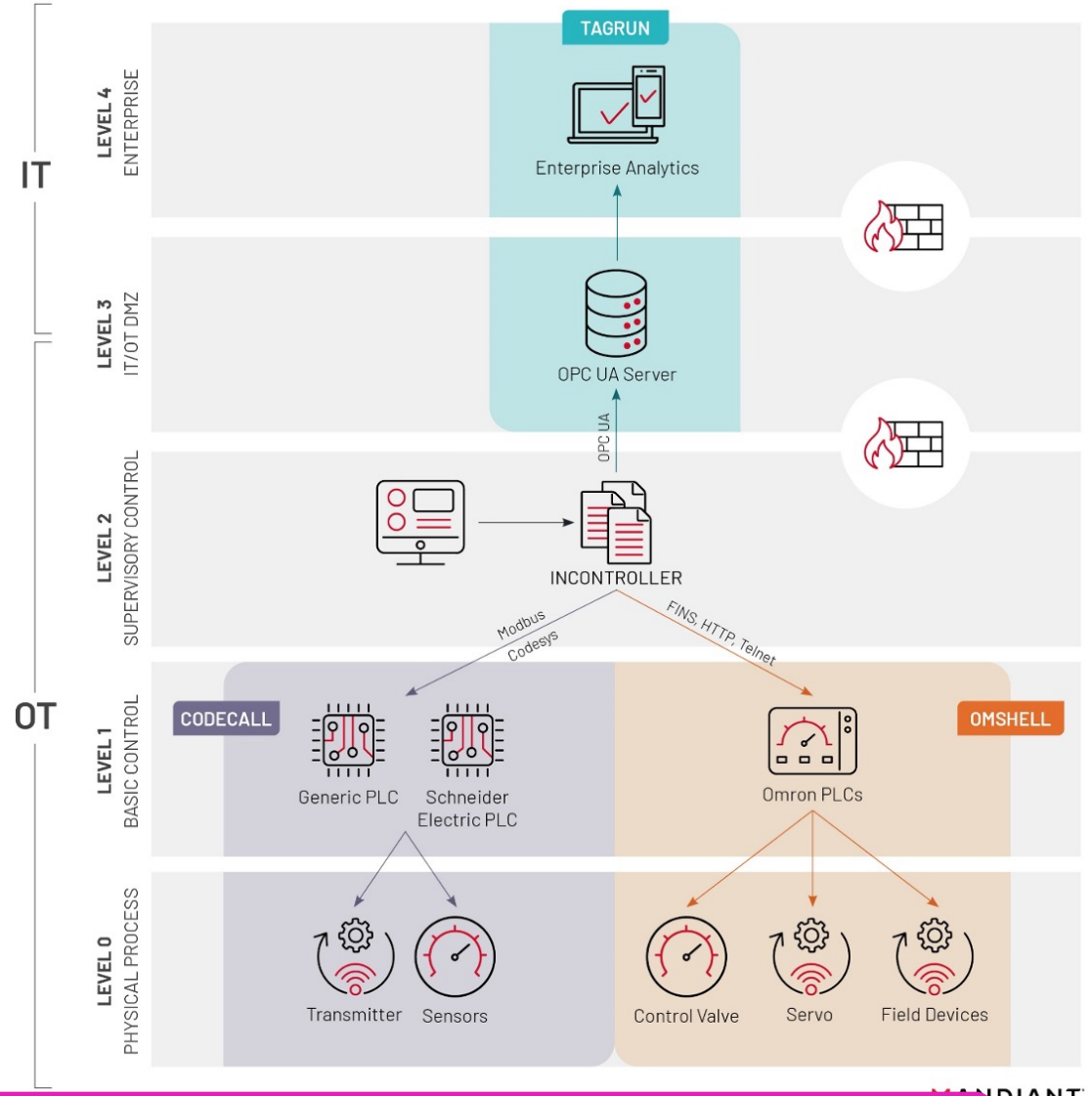
引用元:
https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000080701.pdf
https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000076756.pdf
https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000076757.pdf

コントローラーレベルのICS脆弱性を悪用した攻撃はすでに成功している。

制御システムの脆弱性をつく攻撃ツール開発は活発化

2022年4月13日、米国のエネルギー省と国土安全保障省のサイバーセキュリティ・インフラストラクチャー・セキュリティ庁（CISA）、国家安全保障局（NSA）、連邦捜査局（FBI）が新たなハッキングツールの発見について共同勧告を実施

ツールは産業用制御システムを標的とした、複数のマルウェアを一体化したものでした。
(通称:Pipedream)



引用元:https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool

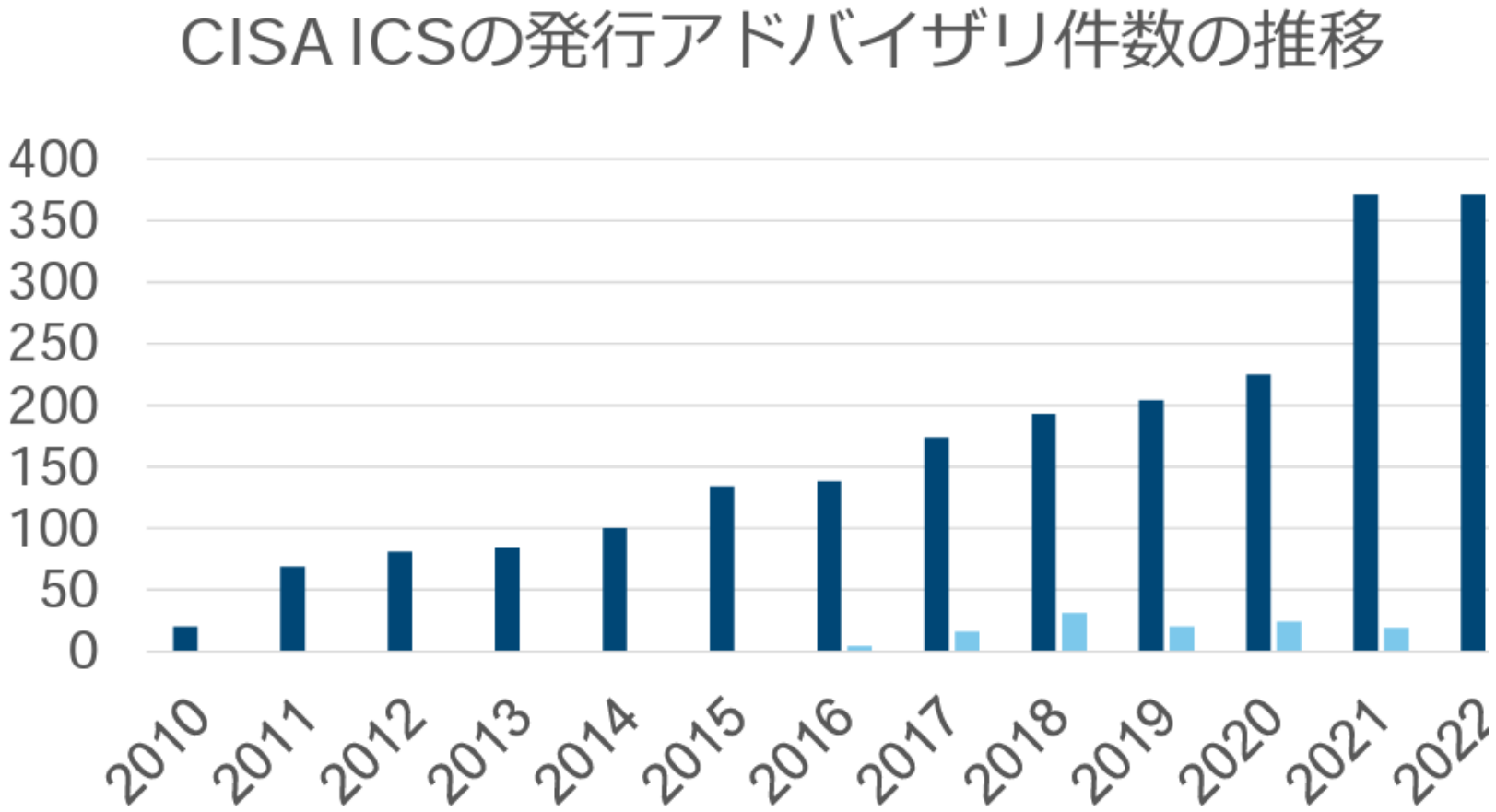
ICS脆弱性を悪用した攻撃のハードルは下がってきている。

脆弱性公表数の推移とイベント

PLCを含むOT機器の脆弱性公表数は年々増加傾向にある。

2022年後期は**ベンダーからの公表が、その他の機関からの公表数を超えた。**

ベンダー側の意識が高まっていると推察できる。



引用元:https://www.jpcert.or.jp/present/2023/ICSR2023_01_JPCERTCC.pdf

ICSベンダー側も予防措置として、脆弱性を発表する傾向が強くなってきている。

脆弱性管理はコンプライアンス遵守事項

組込機器(PLC や IoT 機器など)のモデル情報やファームウェア情報の把握及び**脆弱性情報の定期的な確認等**)

CPG
Cross-Sector Cybersecurity Performance Goals
分野横断的なサイバーセキュリティパフォーマンス目標
2023年3月更新版

Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of **confirmed security vulnerabilities in their assets** within a risk-informed time frame as determined by the organization.

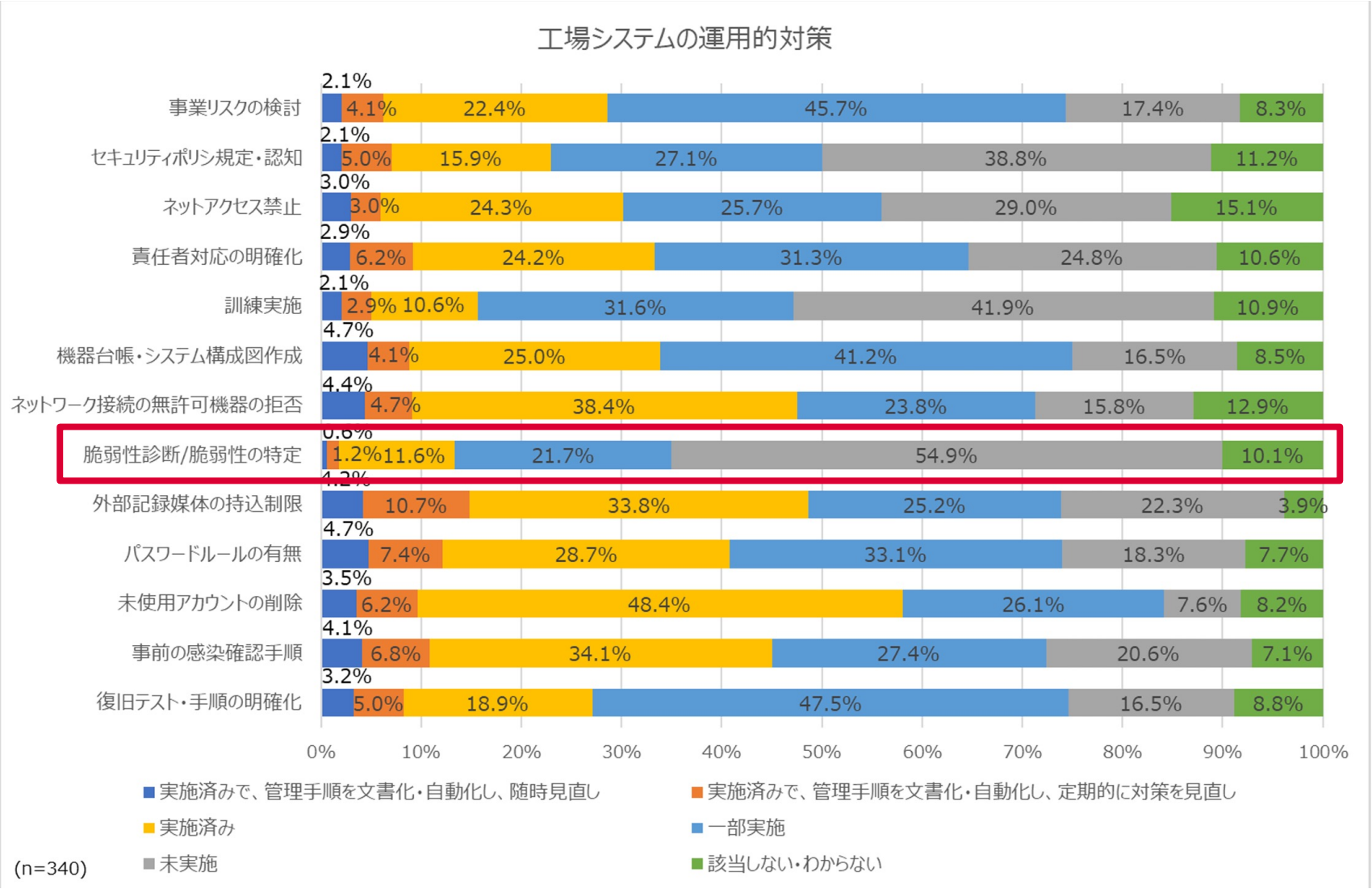
NIS2 Directive

(e) security in network and information systems acquisition, development and maintenance**, including vulnerability handling and disclosure**

引用元:
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.0.pdf
https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
https://www.exalens.com/post/navigating-nis2-for-eu-businesses-ensuring-compliance-and-seizing-opportunities-in-the-eus-evolving-cybersecurity-landscape

各国における規制・ガイドラインにも脆弱性把握、管理は要求されている。

脆弱性管理は喫緊の課題



引用元:https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/pdf/005_s01_00.pdf

インシデント発生時における脆弱性情報の有効活用

今朝、とある建物にて保管されていた10億円が何者かによって盗み出されました。盗み出された当初の建物の状態は不明です。

出荷設備を動かすPLCのバルブ制御が正しく行われず、出荷プロセスが停止しました。

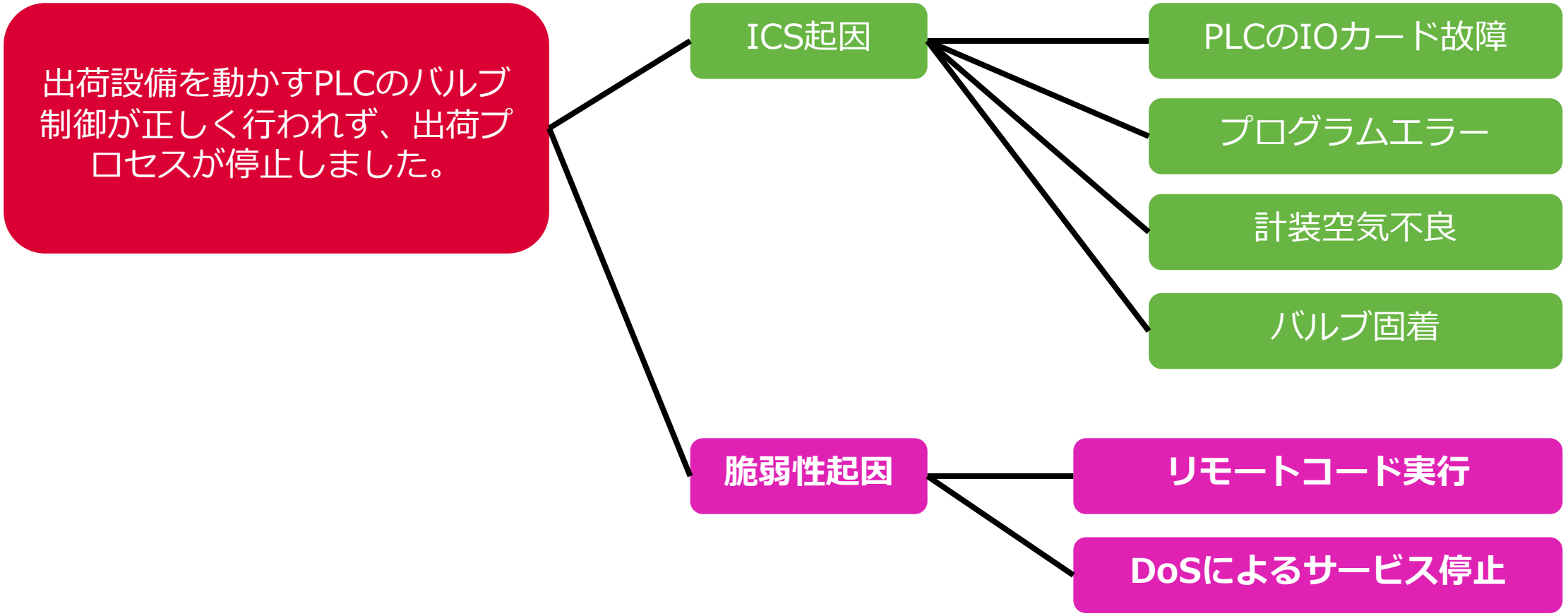
今朝、とある建物にて保管されていた10億円が何者かによって盗み出されました。盗み出された当初の建物は、鍵があいた状態のドアが設置されており、ドアは設置されてから約30年が経過した木製のドアでした。

出荷設備を動かすPLCのバルブ制御が正しく行われず、出荷プロセスが停止しました。
このPLCには公開脆弱性であるCVE-XXX, YYY, ZZZが該当すると確認されており、リモートでのコード実行やDDoS攻撃を受ける可能性がありました。

原因調査のヒントが多い!

CLAROTY

インシデント原因の特定事例



脆弱性管理の取り巻く状況と重要性

1. ICS、得にコントローラーはサイバー空間とフィジカル空間を隔てる機器のため、影響度が甚大かつ重要度が高い。

2. ICSを狙った脅威は高まっており、ベンダー側からも積極的に脆弱性情報を開示され、規制・ガイドラインからも脆弱性管理がますます求められている。

3. 脆弱性情報を管理することで、インシデント後の原因調査にも活用できるため、把握と管理は必要である。

3. 脆弱性管理の課題(特定、追従、優先付け)

公開脆弱性からの該当資産の特定

JVNVU#97061687
複数の CODESYS 製品に複数の脆弱性

概要

複数の CODESYS 製品には、複数の脆弱性が存在します。

影響を受けるシステム

CVE-2021-30186、CVE-2021-30188、CVE-2021-30195

CPU タイプやオペレーティングシステムに関わらず、以下の CODESYS V2 ランタイムシステム

- CODESYS Runtime Toolkit 32-bit full v2.4.7.55 より前のバージョン
- CODESYS PLCWinNT v2.4.7.55 より前のバージョン

CVE-2021-30187

以下の製品をベースにした Linux 上で動作するすべてのランタイムシステム

- CODESYS V2 Runtime Toolkit 32-bit full Version 2.4.7.55 より 前のバージョン

CVE-2021-30189、CVE-2021-30190、CVE-2021-30191、CVE-2021-30192、CVE-2021-30193、CVE-2021-30194

スタンドアロンまたは CODESYS ランタイムシステムとして動作する以下の製品

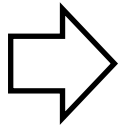
- CODESYS V2 web server Version 1.1.9.20 より前のバージョン

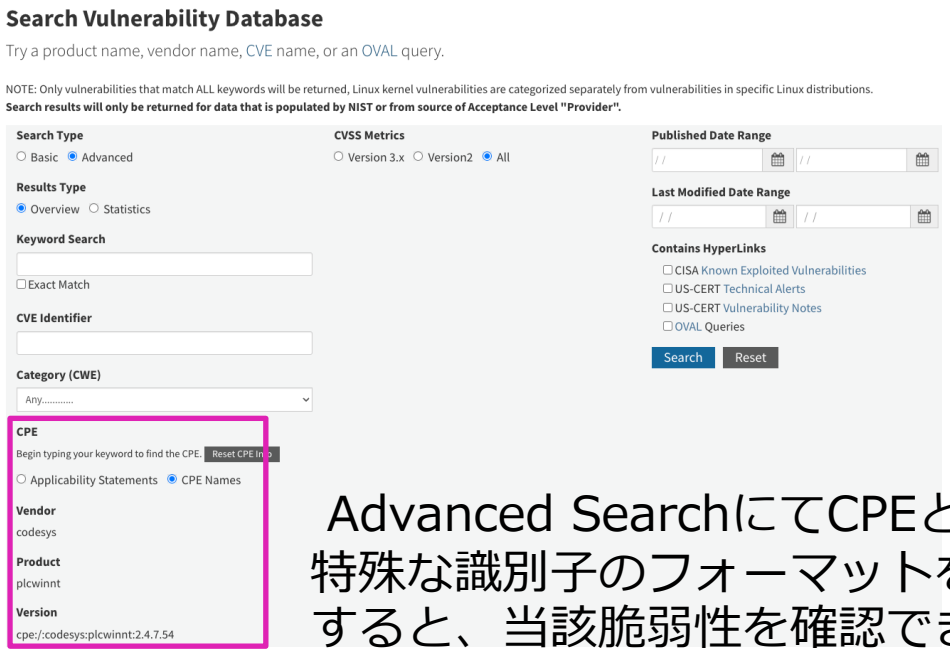
引用元: https://jvn.jp/vu/JVNVU96883262/

該当する資産を把握するためには、詳細な資産台帳が必要

資産台帳があっても該当CVEの紐づけは困難

ベンダー名	モデル番号	バージョン	数量
CODESYS	Runtime Toolkit 32-bit full	V2.4.7.55	5
CODESYS	PLCWinNT	V2.4.7.55	10
CODESYS	V2 Runtime Toolkit 32-bit full	Ver. 2.4.7.55	10

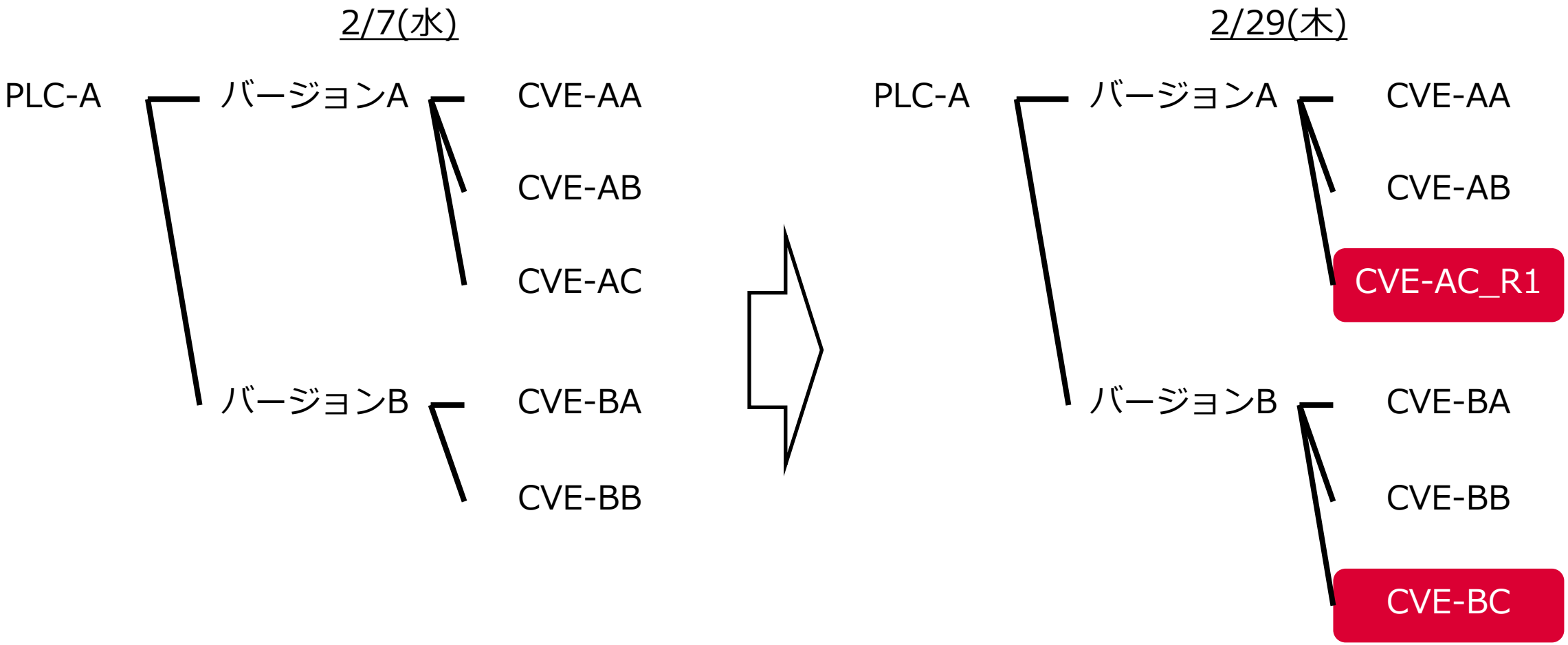




Advanced SearchにてCPEという特殊な識別子のフォーマットを使用すると、当該脆弱性を確認できる。

資産情報から、該当する脆弱性を検索可能だが、非常に多くの手間がかかる。

日々追加、修正される脆弱性情報



日々追加・修正される脆弱性情報を手動で追従するのには限界がある。

該当する脆弱性情報は把握できたが、優先度が見え辛い

脆弱性管理番号	CVSS 基本値	深刻度	該当する資産数
CVE-2021-34527	8.8	重要	4
CVE-2021-33742	7	重要	42
CVE-2021-34448	6.8	警告	7
CVE-2020-0787	7.8	重要	5
CVE-2021-27502	7.8	重要	12
CVE-2021-27504	7.8	重要	14
CVE-2021-22636	7.8	重要	54
CVE-2021-27429	7.8	重要	35
CVE-2021-22680	9.8	重要	1

脆弱性情報が把握できたものの、どの脆弱性から対応すべきか把握し辛い。

脆弱性管理の課題(特定、追従、優先付け)

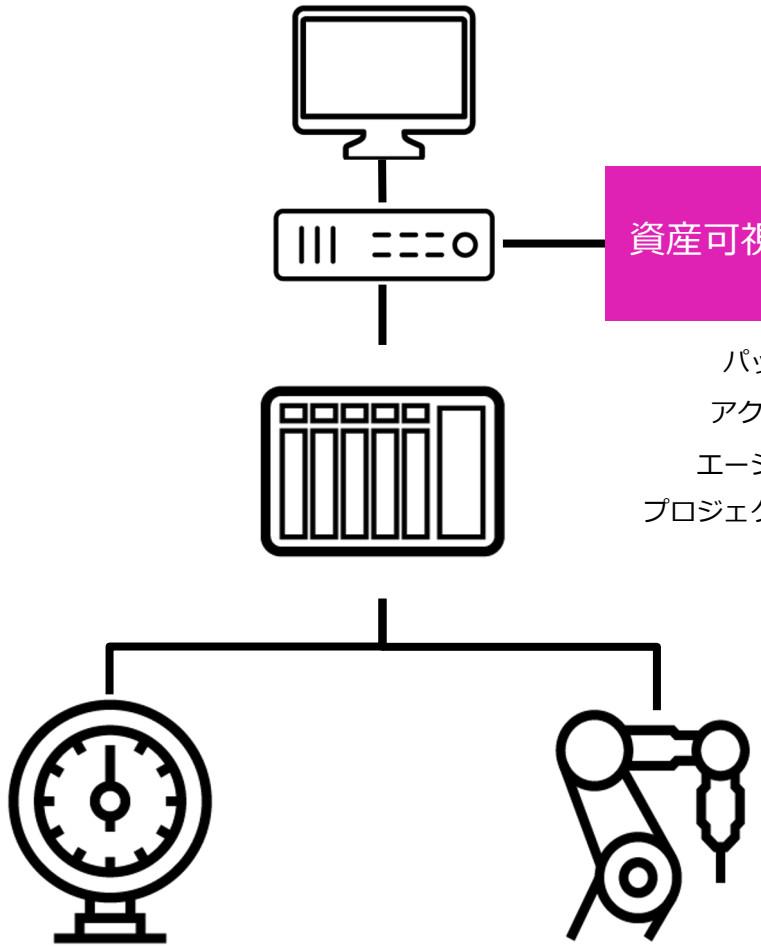
1. 保有している資産と公開脆弱性情報の紐づけには、まず保有資産の詳細な把握(資産棚卸)が必要になる。

2. 紐づけ後の追加・修正情報への追従については、人手で実施するのは非常に困難なため、ツールの導入が合理的である。

3. 脆弱性対応について優先順位をつける指標が複数あるため、優先順位をつけるポリシーや指針が必要になる。

4. グローバルでの事例

資産可視化ツールによる資産台帳作成と脆弱性管理



資産可視化ツール

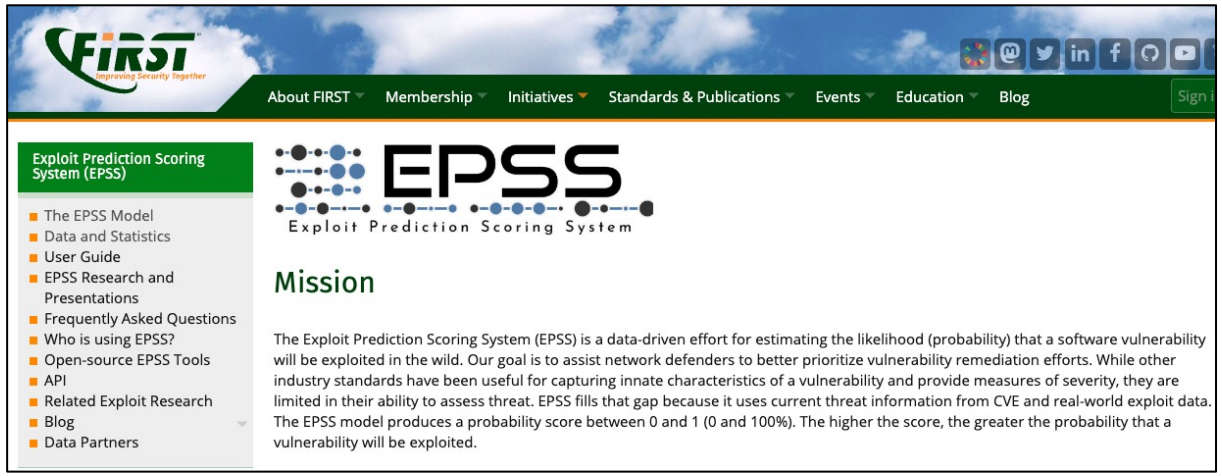
パッシブ
アクティブ
エージェント
プロジェクトファイル

管理番号	ベンダー名	モデル番号	バージョン	数量
1	CODESYS	Runtime Toolkit 32-bit full	V2.4.7.55	5
2	CODESYS	PLCWinNT	V2.4.7.55	10
3	CODESYS	V2 Runtime Toolkit 32-bit full	Ver. 2.4.7.55	10

脆弱性管理番号	CVSS 基本値	深刻度	該当する資産数
CVE-2021-34527	8.8	重要	4
CVE-2021-33742	7	重要	42

実データに基づく資産棚卸しと、脆弱性自動紐づけ、追従をツールによって自動化

脆弱性の優先度をつける指針



EPSS

FIRSTという団体が管理する管理する脆弱性悪用スコアシステム。

今後30日間にその脆弱性が悪用される確率を0~100%で算出

KEV

CISAが公開している実際に悪用が確認された脆弱性のリスト。

攻撃の試み、攻撃の成功が観測されたことがリスト掲載の条件

引用元:
https://www.first.org/epss/
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

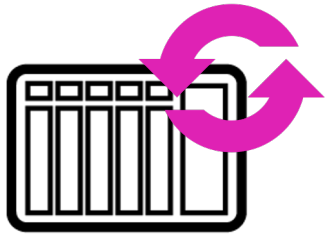
実際に悪用される可能性のある脆弱性情報は、一般に公開されている。

脆弱性情報に指標を加えて対応の優先付け

脆弱性管理番号	CVSS 基本値	深刻度	該当する資産数	EPSS	KEV
CVE-2021-34527	8.8	重要	4	96.7%	あり
CVE-2021-33742	7	重要	42	27.3%	あり
CVE-2021-34448	6.8	警告	7	15.9%	なし
CVE-2020-0787	7.8	重要	5	0.7%	あり
CVE-2021-27502	7.8	重要	12	4.0%	なし
CVE-2021-27504	7.8	重要	14	10.0%	なし
CVE-2021-22636	7.8	重要	54	30.0%	なし
CVE-2021-27429	7.8	重要	35	14.9%	なし
CVE-2021-22680	9.8	重要	1	98.0%	あり

EPSSが高いことと、KEVが存在することから高確率で脆弱性を付かれる可能性有り
=> 優先順位”高”として対応

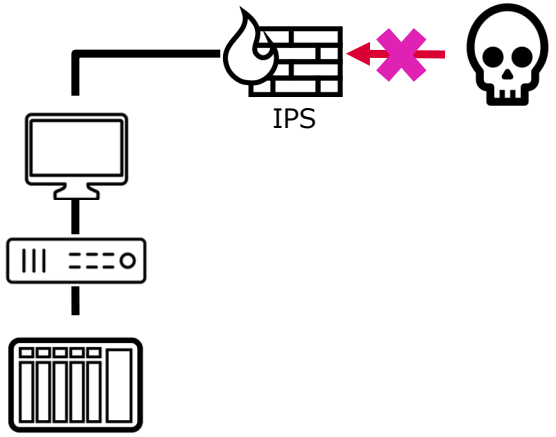
脆弱性対応の例



パッチ適用やファームウェア更新により脆弱性をなくす(本質的対策)

⇩

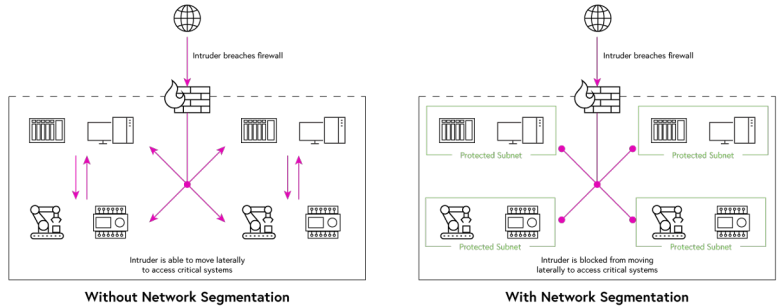
ICS運用環境においては、**実施できるタイミングは限られており**、タイムリーには対応が出来ない。



脆弱性を悪用する攻撃コマンドを、シグニチャーとして登録しIPS実装(仮想パッチ)

⇩

攻撃が確認されてからでないと、**シグニチャーとして配布されない**可能性がある。



セグメントを区切り、セグメント間の通信ポリシーを設定する。(マイクロセグメンテーション)

⇩

通信内容の正しい把握とポリシーの段階的適用が必要となる。

応急処置としてネットワーク側で補正対策をする。

全体のまとめ

1. 効率的な脆弱性管理の運用には、保有資産の把握から脆弱性情報の紐づけ、追従が出来るツールが必要である。

2. CVEにある情報だけでなく、EPSS, KEVとの紐づけを行うことで、悪用される可能性の高さをベースに優先付けできる。

3. ICSにおいては脆弱性対応として、本体側で対応することよりもネットワークセキュリティとして補正制御を行う方が現実的である。

ありがとうございました。