



PLCやIoT機器の脆弱性管理の重要性

2023/10/19(木) Edgecross 工場セキュリティガイドライン啓発・連続セミナー

クラロティ
アジア太平洋・日本地区
ソリューションエンジニア
加藤 俊介

目次

- 自己・会社紹介
- PLCやIoT機器の脆弱性管理が何故重要なのか？
- 実際に管理する上での課題と考察
- まとめ

A photograph of an industrial manufacturing environment. In the foreground, a large orange robotic arm is positioned over a silver car chassis. The arm is actively welding, creating a dense spray of bright yellow and white sparks that radiate outwards. In the background, other robotic arms and car chassis are visible, suggesting a busy factory floor. The lighting is bright, highlighting the metallic surfaces and the intense heat of the welding process.

CLAROTY INDUSTRIAL

自己・会社紹介

自己紹介

ミッション: セーフティ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



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

本講演テーマ選択に至るまでの背景

工場セキュリティガイドライン 付録E チェックリスト
運用的対策(システム関連等) 2-8

システムへの侵入を可能とする攻撃手法や脆弱性を特定し、脆弱性へ対応している、又は緩和策を講じている。

(脆弱性を特定する手法の例:
定期的な脆弱性診断やペネトレーションテスト(侵入可否検査)、
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)



脆弱性スキャナやツールによる診断、ペンテストは高度な技術と高いコストを要する。

モデルやファームウェアからの脆弱性把握を行おうとしている組織が多いと仮定

一方で自組織の組込機器の脆弱性を、適切に把握できている組織もまだ少ないはず

PLCやIoT機器の脆弱性管理が何故重要な のか?

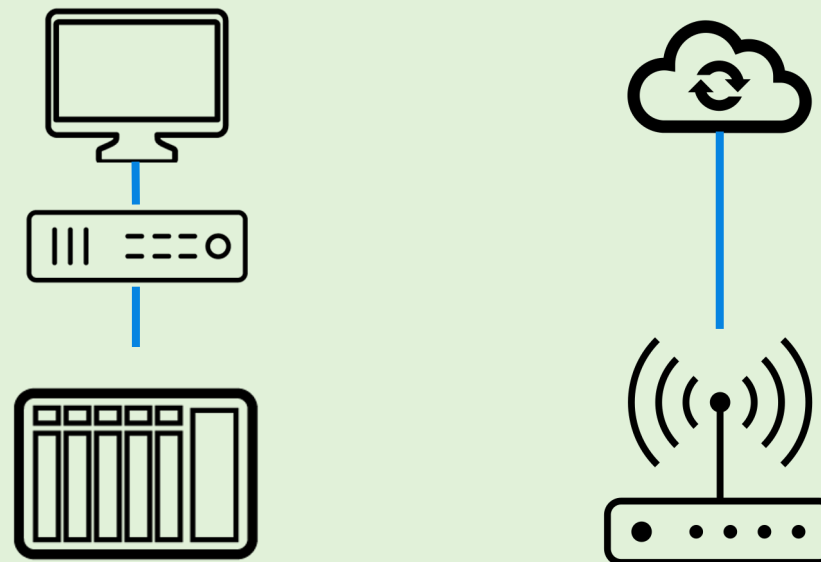
PLC, IoT機器の性質

PLCやIoT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。

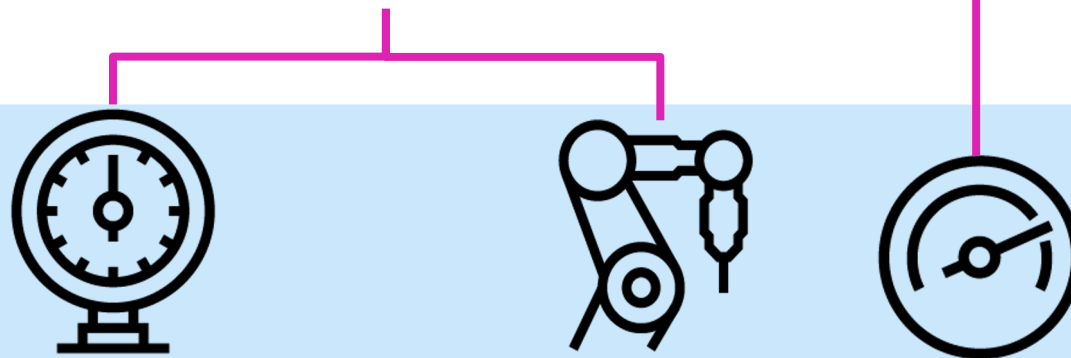
現実世界に影響を与えられる。
例) ポンプを起動する、アームを動かす

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。

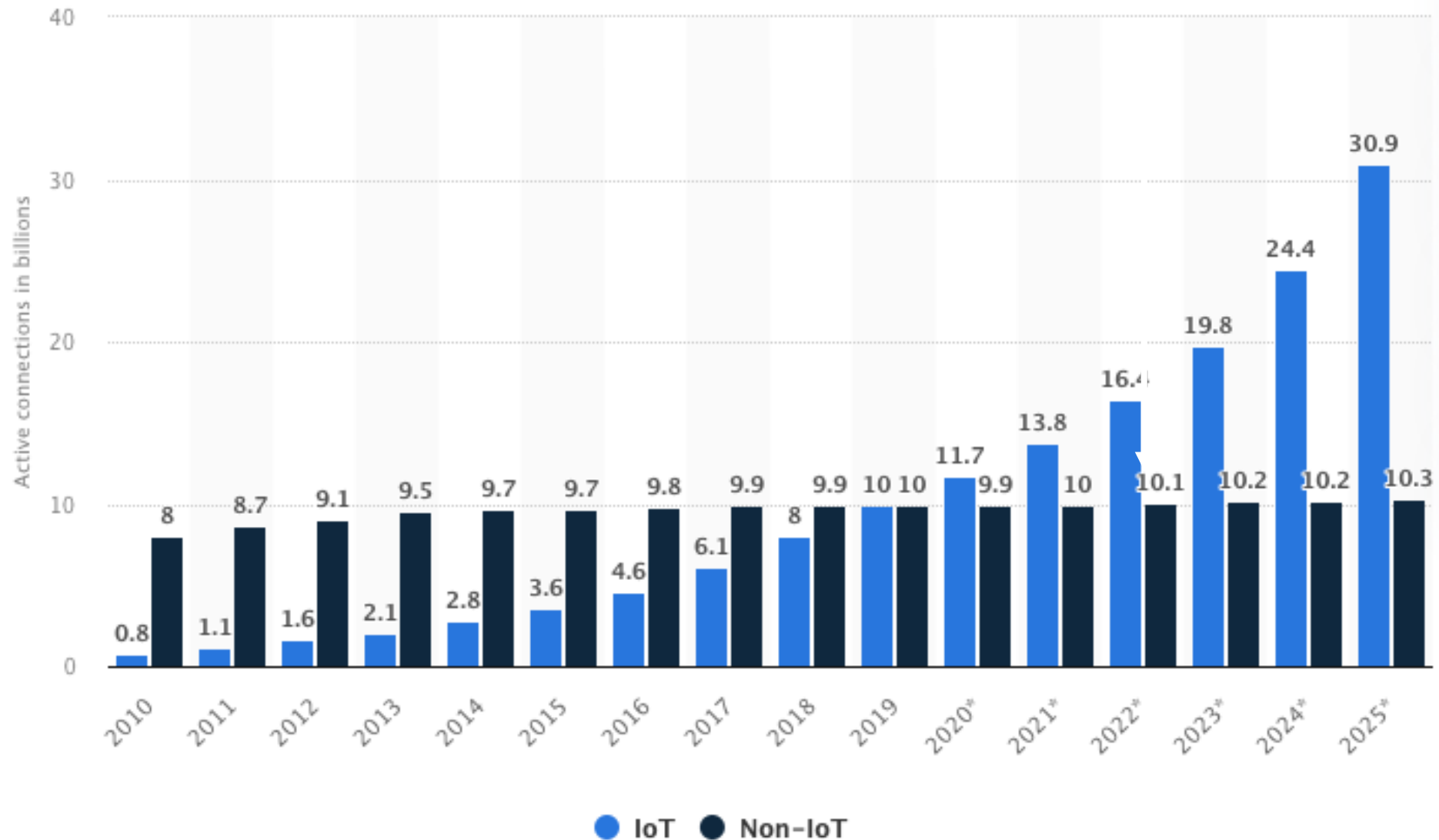
サイバー空間



フィジカル空間



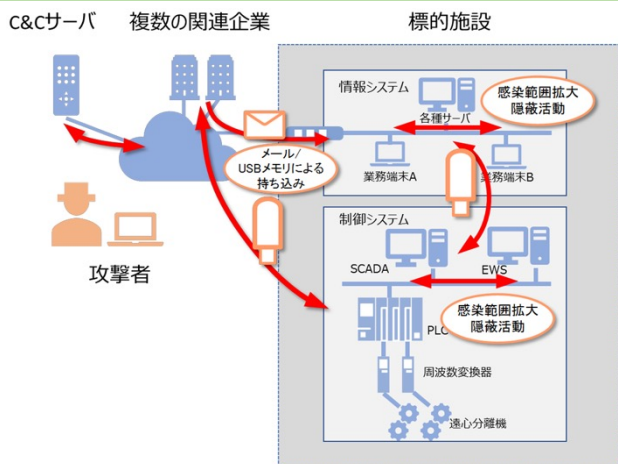
フィジカル空間・サイバー空間を隔てるデバイスは増加



引用元:<https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/>

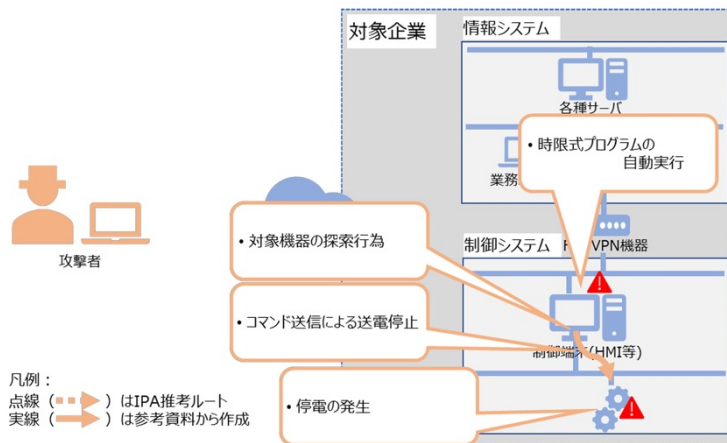
組込機器が被害・標的となったインシデント事例

2010: Stuxnet



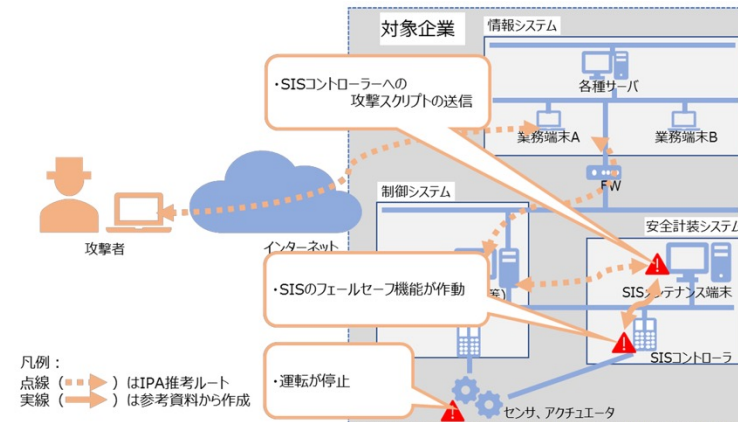
ドイツのSiemens社のPLCの脆弱性を標的とし、遠心分離機の回転周波数を変更した。

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をフランスのSchneider Electric社の安全PLCに対して送信、書き込みが行われた。

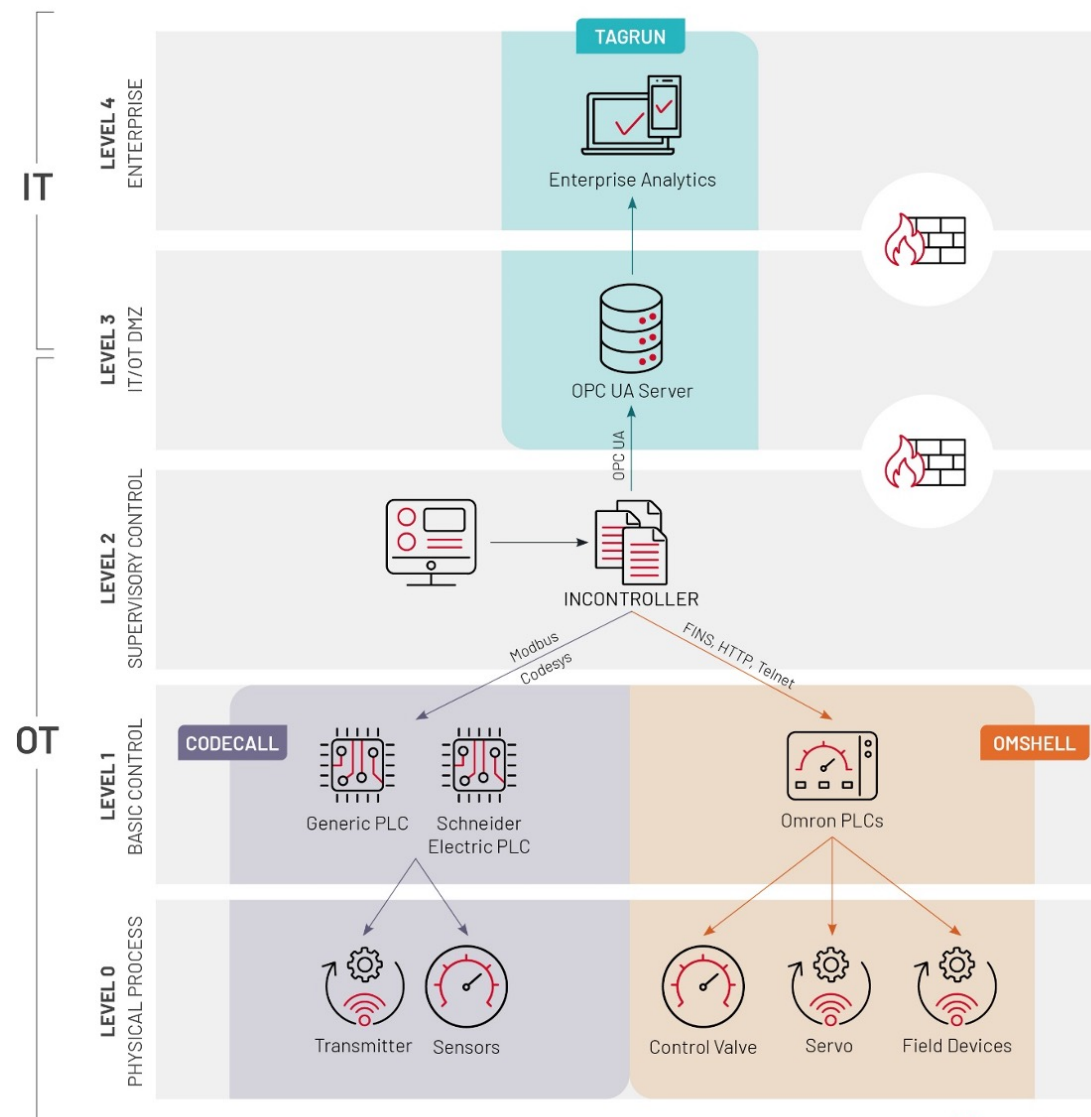
フェールセーフ機能によりプラントはシャットダウンした。

引用元:
<https://www.ipa.go.jp/security/controlsystem/uq65p900000197wa-att/000080701.pdf>
<https://www.ipa.go.jp/security/controlsystem/uq65p900000197wa-att/000076756.pdf>
<https://www.ipa.go.jp/security/controlsystem/uq65p900000197wa-att/000076757.pdf>

組込機器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 (通称:Pipedream)



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

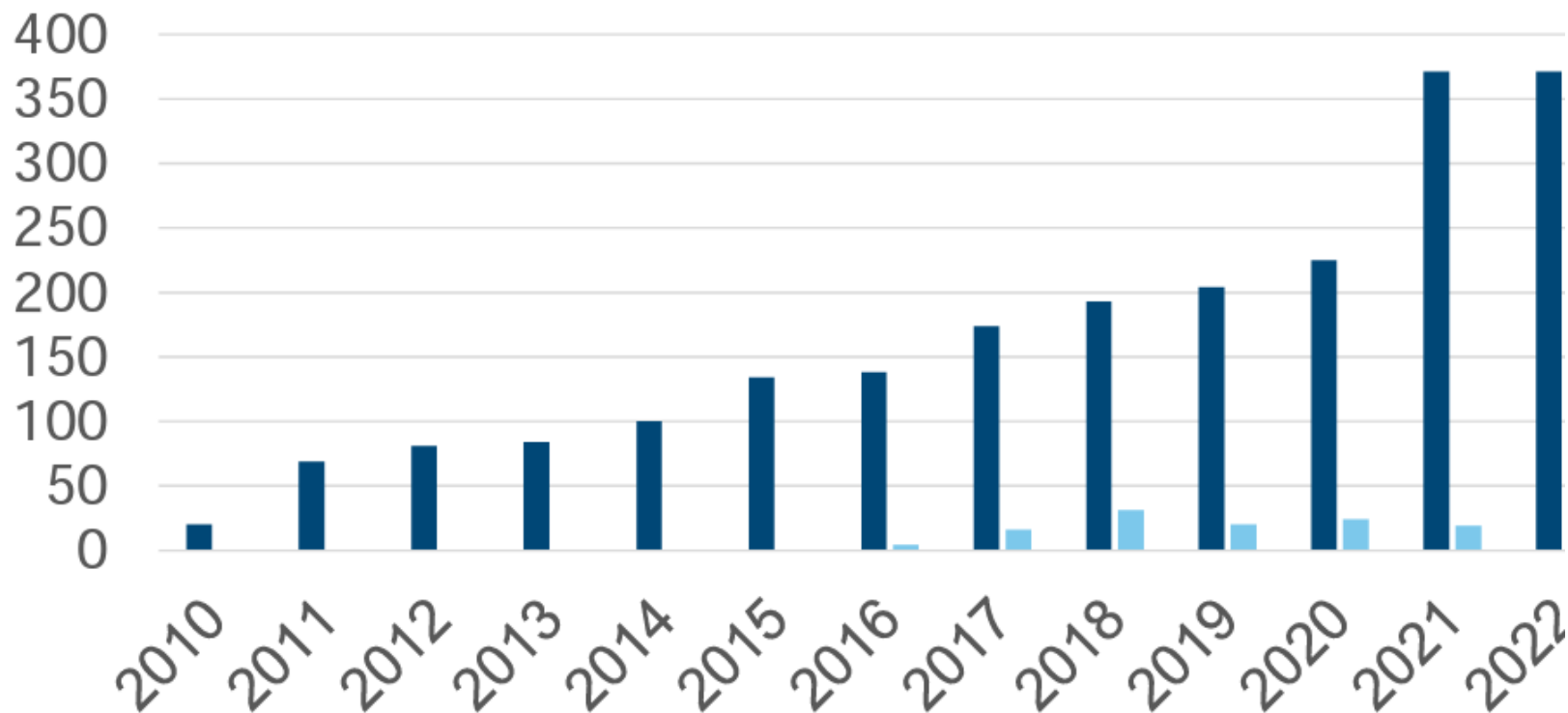
脆弱性公表数の推移とイベント

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。

CISA ICSの発行アドバイザーリ件数の推移



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。

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。



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。

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。



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。

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。



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。



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。

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。



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。



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す。

原因調査のヒントが多い!

PLCやIoT機器の脆弱性管理が何故重要なのか？

- 1 サイバー空間とフィジカル空間を隔てる機器のため、何かあった場合の影響度が甚大であり、その数はますます増えていく
- 2 これらの機器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するようになってきている。
- 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。

A photograph of an industrial manufacturing environment. In the foreground, a large orange robotic arm is positioned over a silver car chassis. The arm is actively welding, creating a dense spray of bright yellow sparks that fills the right side of the frame. In the background, other car chassis and robotic arms are visible, suggesting a busy factory floor. The lighting is bright and industrial.

CLAROTY INDUSTRIAL

実際に管理する上での課題と考察

所有している機器と公開脆弱性の紐づけ(CVE => 資産)

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

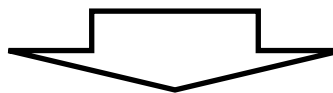
- CODESYS V2 web server Version 1.1.9.20 より前のバージョン

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

該当する脆弱性情報を見つけるためには、モデル名とバージョンが必要

所有している機器と公開脆弱性の紐づけ(資産 => CVE)

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



単純なベンダー名検索では、該当する脆弱性情報にたどり着くのが難しい

所有している機器と公開脆弱性の紐づけ(資産 => CVE)

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.

Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type
 Basic Advanced

CVSS Metrics
 Version 3.x Version2 All

Published Date Range
//

Last Modified Date Range
//

Contains HyperLinks
 CISA Known Exploited Vulnerabilities
 US-CERT Technical Alerts
 US-CERT Vulnerability Notes
 OVAL Queries

Results Type
 Overview Statistics

Keyword Search

 Exact Match

CVE Identifier

Category (CWE)
Any.....

CPE
Begin typing your keyword to find the CPE.
 Applicability Statements CPE Names

Vendor
codesys

Product
plcwinnt

Version
cpe:/:codesys:plcwinnt:2.4.7.54

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。

所有している機器と公開脆弱性の紐づけ(ChatGPT)

Default (GPT-3.5)

S

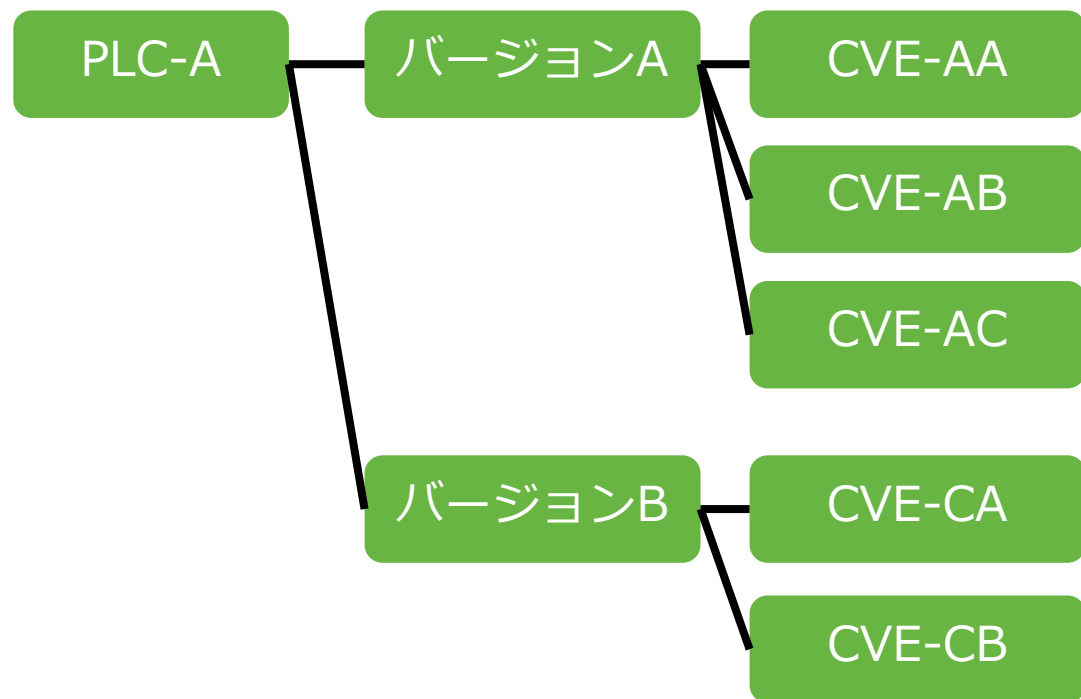
CODESYS製、PLCWinNTのバージョン2.4.7.55に該当する脆弱性情報を教えてください



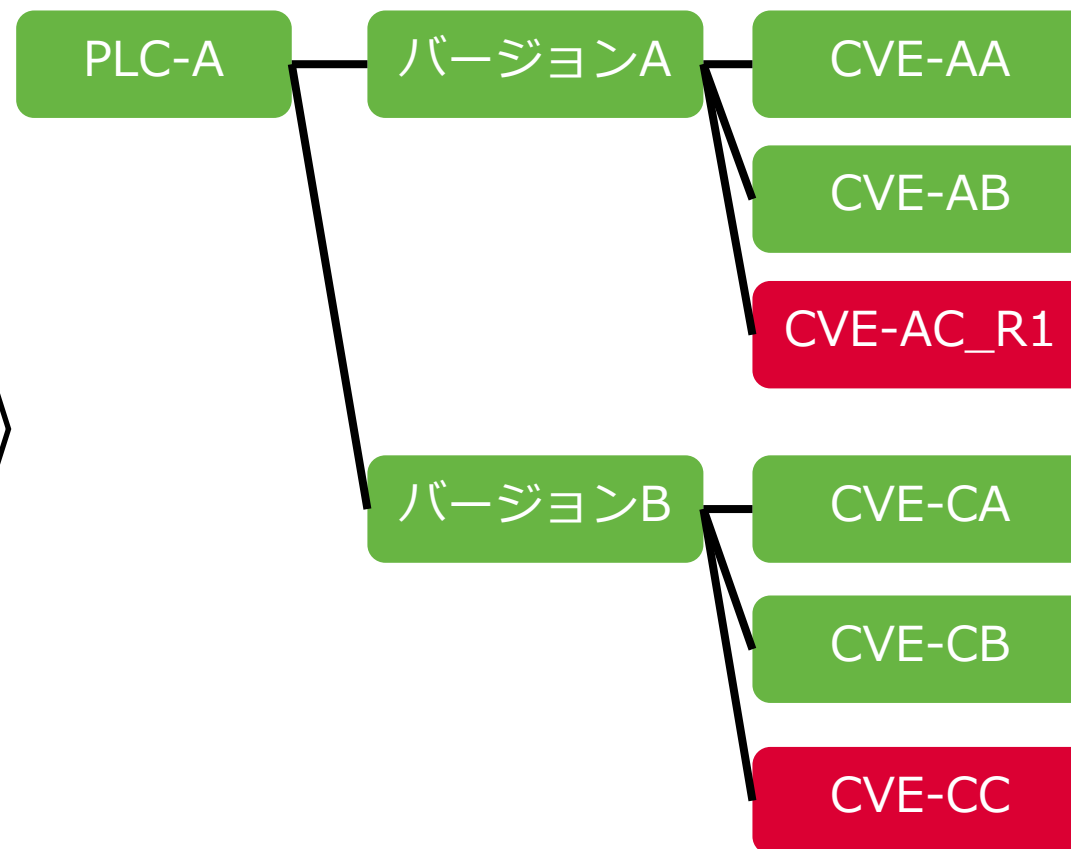
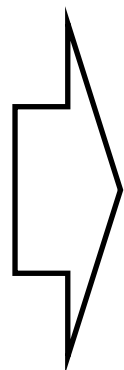
申し訳ございませんが、私のデータベースには特定のバージョンや日付に関連する具体的な脆弱性情報は含まれていません。また、情報の提供日時から既知の脆弱性情報も最新のものではないかもしれません。PLCWinNTのバージョン2.4.7.55に関する最新の脆弱性情報を入手するためには、CODESYSの公式ウェブサイトやセキュリティ情報提供者のウェブサイト、セキュリティブログ、またはベンダーに直接問い合わせる情報入手をお勧めします。セキュリティアップデートや修正プログラムが利用可能であれば、それらを適用することが重要です。また、システムを最新のセキュリティベストプラクティスに従って設定し、セキュリティポリシーを遵守することも重要です。



日々追加、修正される脆弱性情報(最新情報追従)



10/19(木)



10/31(火)

脆弱性情報に優先順位をつけるための指標

脆弱性管理番号	CVSS 基本値	深刻度	該当デバイスの重要度	攻撃容易性スコア	EPSS	KEV
CVE-2021-34527	8.8	重要	高	2.8	96.7%	あり
CVE-2021-33742	7	重要	中	2.8	27.3%	あり
CVE-2021-34448	6.8	警告	中	2.8	15.9%	なし
CVE-2020-0787	7.8	重要	低	1.8	0.7%	あり

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

実際に管理する上での課題と考察

- 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が必要
- 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
- 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、対応に関するポリシー・指針が必要



ありがとうございました。



A photograph of an industrial manufacturing environment. In the foreground, a large orange robotic arm is positioned over a silver car chassis. The arm is actively welding, creating a dense spray of bright yellow sparks that fills the right side of the frame. In the background, other robotic arms and car chassis are visible, suggesting a busy factory floor. The lighting is bright and industrial.

CLAROTY INDUSTRIAL

補足資料

クラロティについて

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

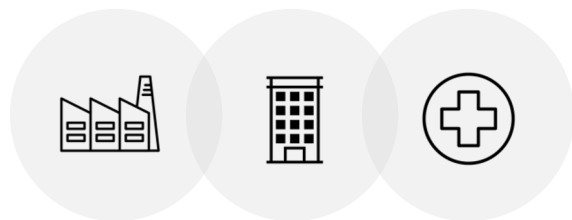
包括的なソリューション

グローバルにおける実績

拡張型IoT(XIoT)

資産管理

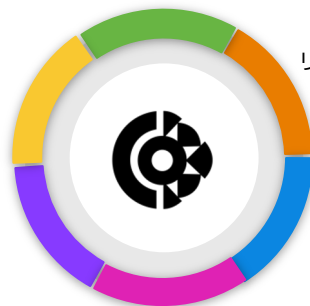
顧客数800+, 導入:10,000+, 国: 50+, 業界: 25+



インダストリアル エンタープライズ ヘルスケア

変更管理

リモート
アクセス



脅威検出

リスクと脆弱性の
管理

ネットワーク
保護



第三者からの高い評価

