ICS関連製品の脆弱性情報の分析を通じて見えてきた課題

JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ
堀　充孝

今回話す内容

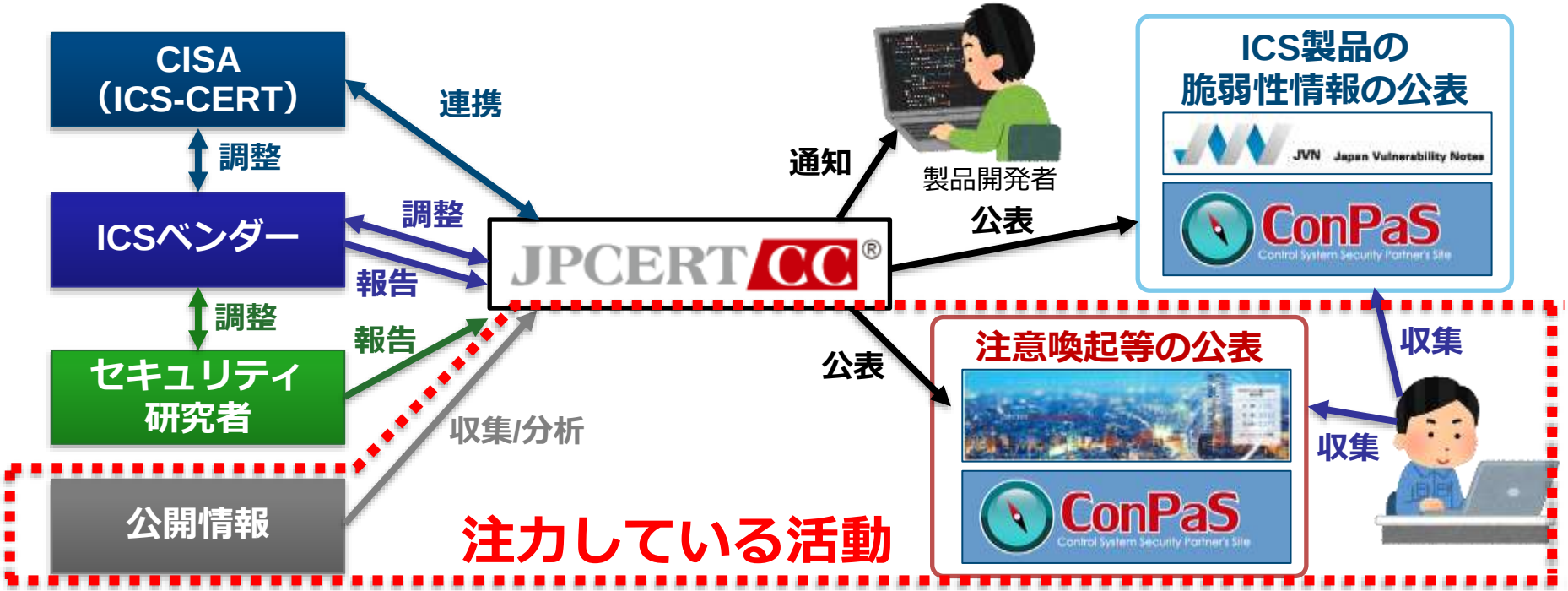
- はじめに
- ICS関連製品の脆弱性情報の分析事例
- 分析事例の振り返りと課題
- 脆弱性管理に関する参考情報
- 最後に
  - J-CLICS 攻撃経路対策編の紹介

はじめに

・担当業務および分析活動
・今回の講演の趣旨

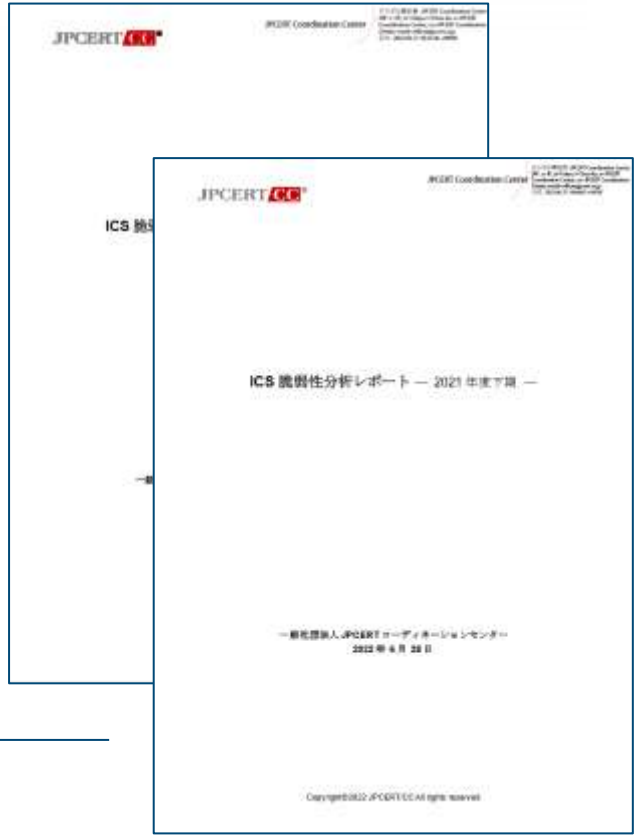
担当業務および分析活動

- 2020年度からインターネット等の公開情報からのICS製品の脆弱性情報の収集・分析に注力



担当業務および分析活動（続き）

- ICS脆弱性分析レポートの公表
  - ICSユーザー組織向けの文書
  - 半期ごとにJPCERT/CCが注目したICS関連製品の脆弱性情報を1つ取り上げて詳細に解説
    - CVSSなどの情報の読み解き方
    - ICS全体への影響
    - ICSユーザー組織で実施可能な対策
    - その他、注目した脆弱性情報の一覧
      など



参考：JPCERT/CC
ICS脆弱性分析レポート
https://www.jpcert.or.jp/ics/ics-vuls-analysis-report.html

今回の講演の趣旨

ICSユーザーでの脆弱性情報のトリアージの参考として

- ICS関連製品の脆弱性情報の分析事例の紹介
  - どのような情報を収集していくか
  - 脆弱性情報の読み解き方
  - ICSユーザー組織で情報を分析する上で注意すべき点と課題

- 脆弱性管理に関する参考情報
  - ICSユーザー組織で対応要否の判断を支援する分析手法

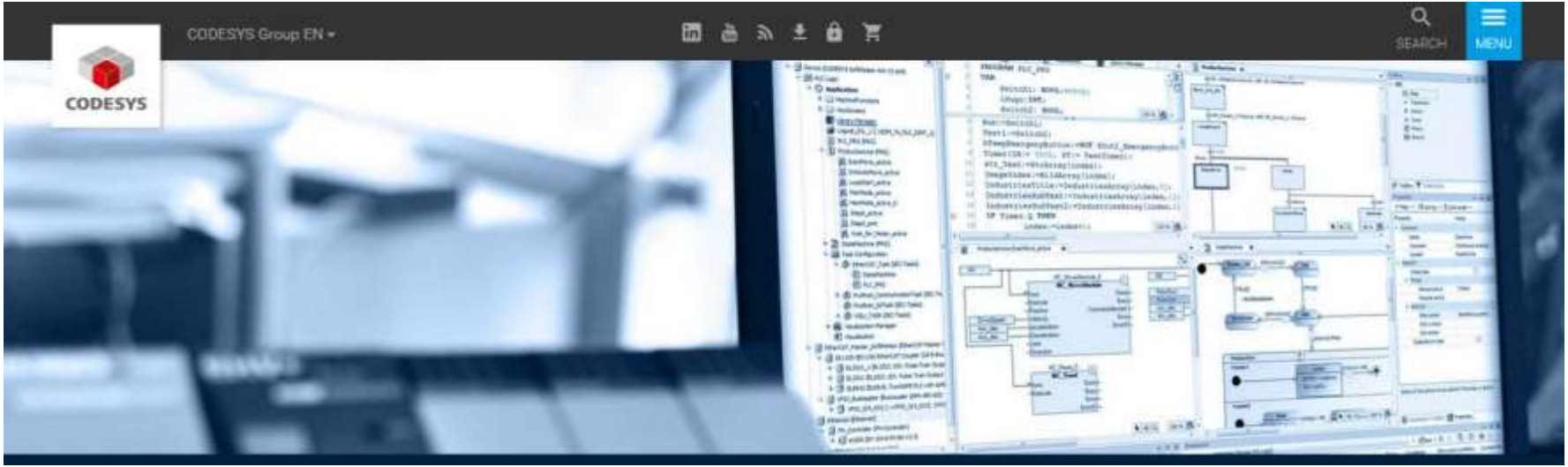
ICS関連製品の脆弱性情報の分析事例

「ICS脆弱性分析レポート - 2021年度下期 -」より

CODESYS の脆弱性（CVE-2021-34593）

CODESYSとは

- IEC 61131-3に準拠したソフトウェアPLC・HMI等の開発ライブラリ
  - エンジニアリングツールも提供されている



引用：CODESYS
CODESYS Inside
https://www.codesys.com/the-system/codesys-inside.html

今回の脆弱性（CVE-2021-34593）に注目した理由

- CODESYSは500社を超えるメーカーに採用されており、CODESYSが組み込まれたデバイスは国内でも流通している
- セキュリティベンダーから詳細な情報が公表されていた

引用：SEC Consult
Denial of service & User Enumeration in WAGO 750-8xxx PLC
https://sec-consult.com/vulnerability-lab/advisory/denial-of-service-user-enumeration-in-wago-750-8xxx-plc/

CVE-2021-34593の公表の経緯

■ 公表の経緯は次のとおり

日付	公表の状況
2021/10/18	CODESYS社がCODESYS v2.x系のライブラリに関する脆弱性情報を公表 ※ アップデートの提供はなく、一般的なセキュリティ対策の実施の推奨のみ記載
2021/10/25	CODESYS社が本脆弱性に対応したアップデートを公開
2021/11/16	CERT@VDEが本脆弱性の影響を受けるWAGO社のPLCに関する情報を公表 ※ アップデートの提供予定は2022年1月とのこと
2022/01/26	WAGO社のアップデートの公開とあわせて、**SECConsult社が詳細情報を公表**

■ 詳細情報の公表を受けて、悪用の可能性についての調査を実施

CVE-2021-34593の内容

影響を受けるシステム	次のCODESYS v2ランタイムシステムに含まれるCODESYS TCP/IP通信ドライバーが影響を受ける ・CODESYS Runtime Toolkit 32bit full v2.4.7.56より前のバージョン ・CODESYS PLCWinNT v2.4.7.56より前のバージョン
脆弱性の内容	CWE-755：例外的な状態の不適切な処理 　CODESYS v2ランタイムシステムで提供されているエンジニアリングツールと通信するためのサーバー機能の処理に問題があり、細工されたリクエストを受信するとそのリクエストに対するメモリの割り当てに失敗する。
想定される影響	遠隔の第三者によって、エンジニアリングツールと通信するためのサーバー機能をサービス運用妨害（DoS）状態にされる。
CVSS v3による評価	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H（基本値：7.5）
対策	・脆弱性に対応したアップデートが提供されている ・本脆弱性に特化したワークアラウンドは無く、一般的なセキュリティ対策の実施を推奨

参考：CODESYS
Advisory 2021-16：Security update for CODESYS Control V2 TCP/IP communication driver
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16877&token=8faab0fc1e069f4edfca5d5aba8146139f67a175

CVSS v3基本評価基準の説明

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H　基本値: 7.5

■ 「攻撃の成立条件」に関わる項目

評価項目	値	内容
攻撃元区分 （AV：Attack Vector）	N：ネットワーク	ネットワーク経由でリモートから攻撃可能
攻撃条件の複雑さ （AC：Attack Complexity）	L：低	特別な攻撃条件を必要としない
攻撃に必要な特権レベル （PR：Privileges Required）	N：不要	特別な権限（認証）を必要としない
利用者の関与 （UI：User Interaction）	N：不要	ファイルを開く、リンクを開くなどのユーザーによる操作を必要としない

※JVNでは上記条件の場合、想定される影響に「遠隔の第三者によって」と記載されていることが多いです

CVSS v3基本評価基準の説明（続き）

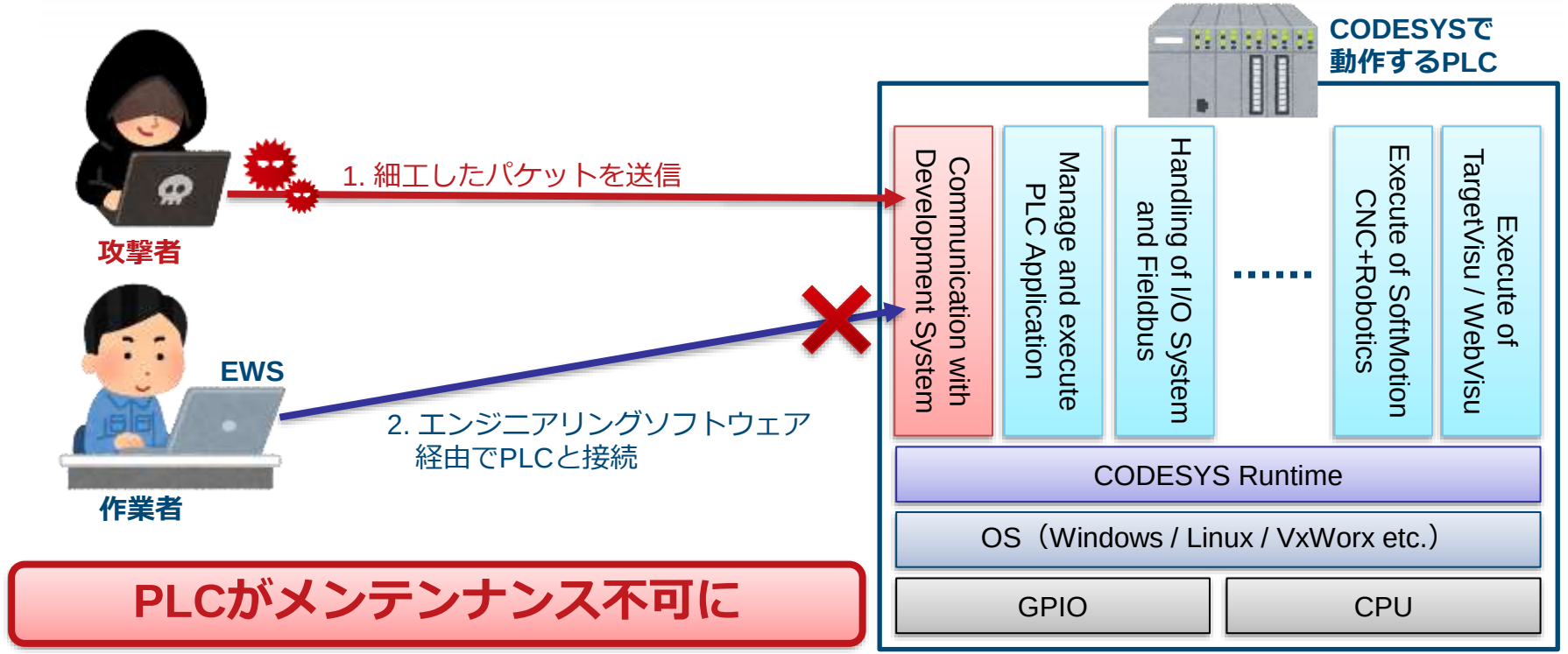
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H　基本値: 7.5

■ 「想定される影響」に関わる項目

評価項目	値	内容
影響の想定範囲（S：Scope）	U：変更なし	影響範囲は脆弱性のあるコンポーネントが帰属するオーソリゼーションスコープに留まる
機密性への影響（C：Confidentiality）	N：なし	機密性への影響はない
完全性への影響（I：Integrity）	N：なし	完全性への影響はない
可用性への影響（A：Availability）	H：高い	リソースを完全に枯渇させたり、完全に停止させたりすることができる

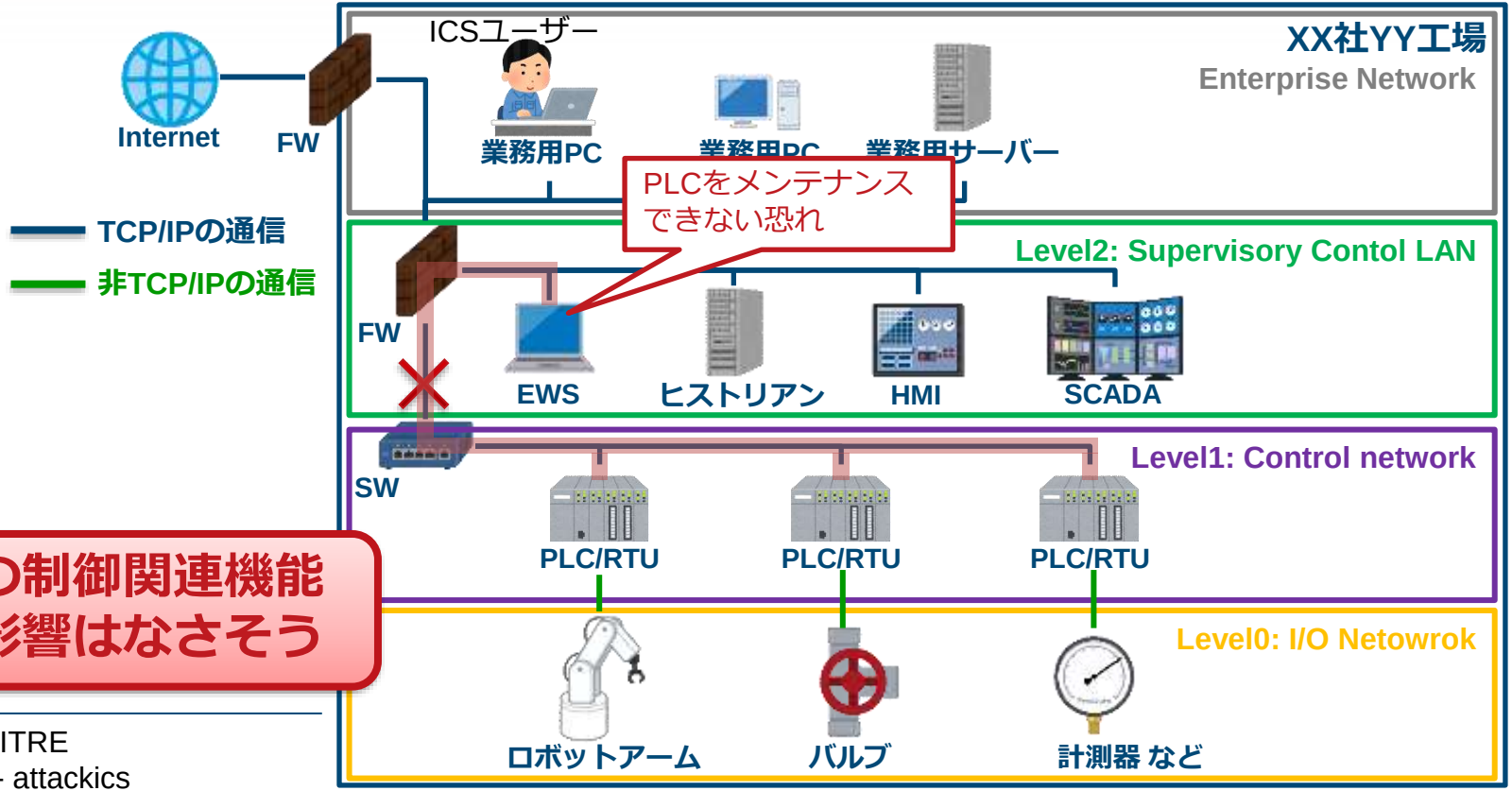
※JVNでは上記条件の場合、想定される影響に「サービス運用妨害（DoS）状態にされる」と記載されていることが多いです

CVE-2021-34593のまとめ（図説）



参考：CODESYS
CODESYS RUNTIME
https://www.codesys.com/products/codesys-runtime.html

ICS全体としての影響を考えると…



PLCの制御関連機能への影響はなさそう

参考:MITRE
Levels - attackics
https://collaborate.mitre.org/attackics/index.php/All_Levels

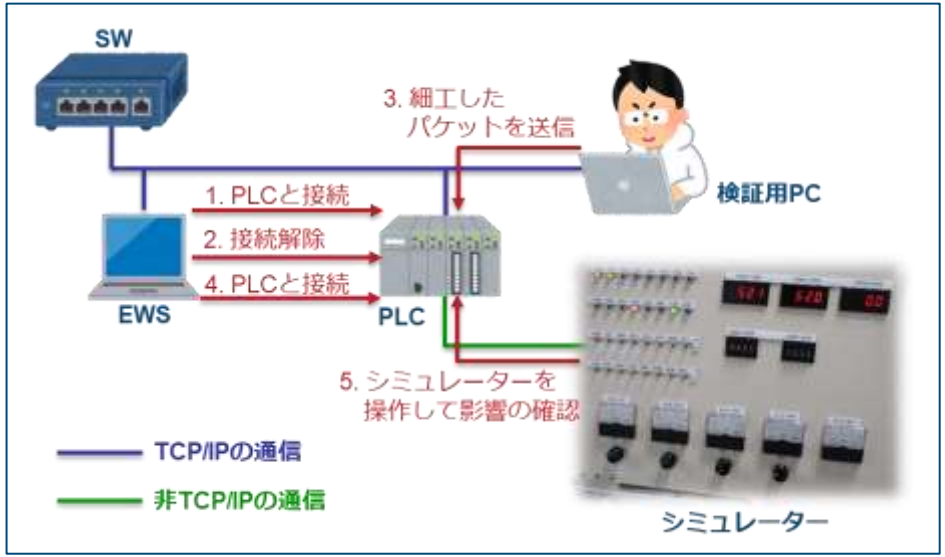
CVE-2021-34593の検証

- SECConslut社の詳細情報にもとづいて検証を実施
  - 想定される影響を再現できるか
  - 本当に監視・制御への影響はないのか

検証に使用した機器一覧

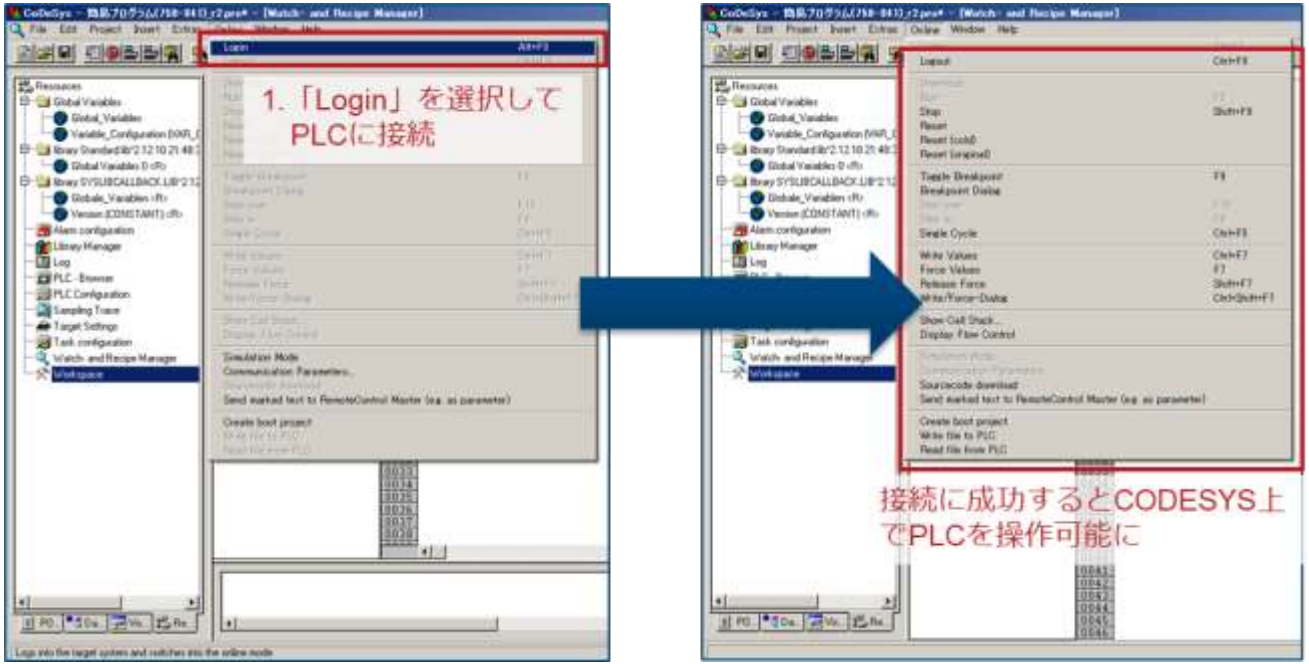
スイッチ（SW）	NETGEAR製GS108Ev3
EWS	CODESYS v2.3.9.35
PLC	WAGO製750-841 v04.01.06（19）
検証用PC	Pythonが動作するPC
シミュレーター	フィールド機器の動作を シミュレートする装置

検証環境および手順



CVE-2021-34593の検証結果 - 脆弱性の再現

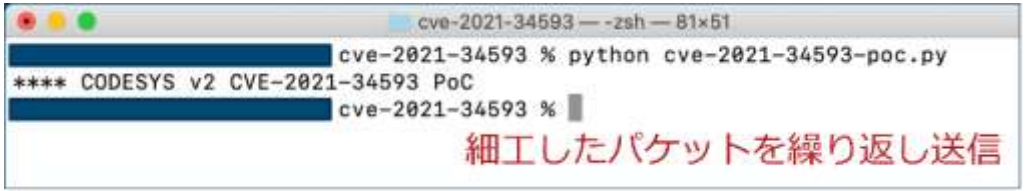
- 細工したパケットを送信する前にエンジニアリングワークステーションからPLCへの接続が問題なくできることを確認



細工したパケットの送信前：CODESYS開発環境とPLCが接続可能

CVE-2021-34593の検証結果 - 脆弱性の再現（続き）

- 検証用PCから細工したパケットをPLCに送信



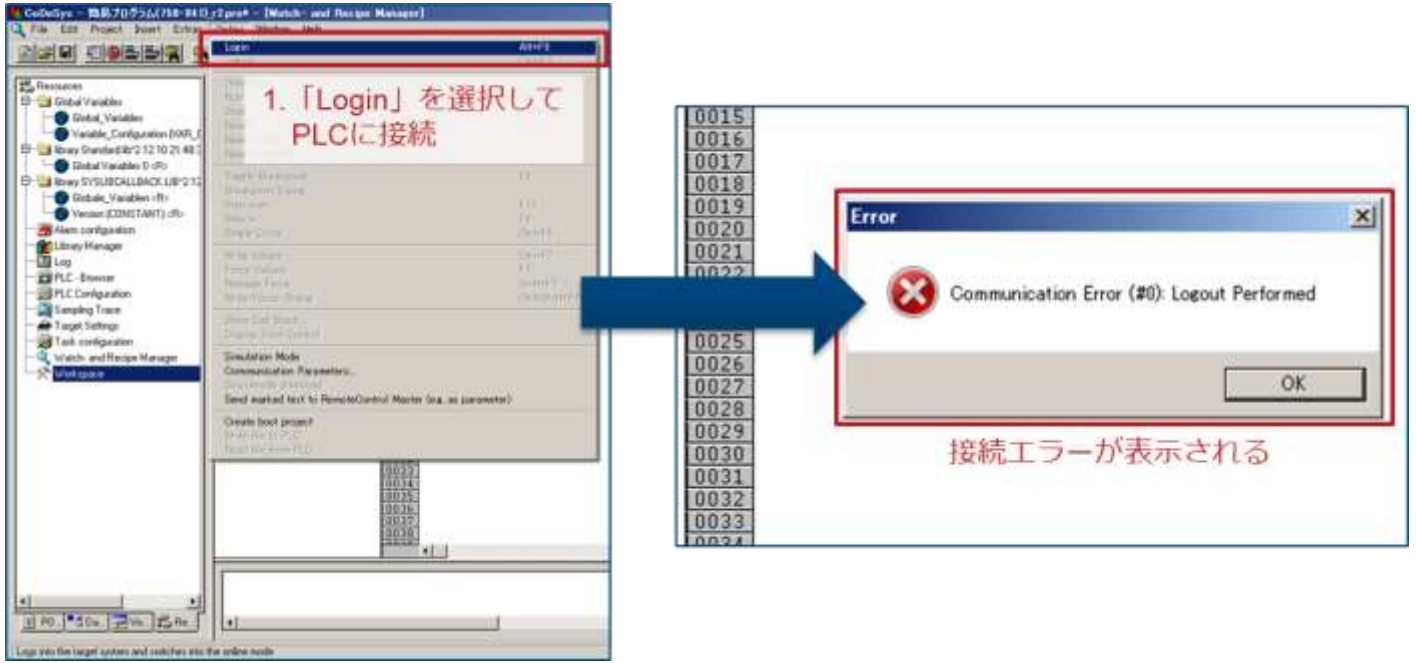
検証機からPLCに細工したパケットの送信

SECConsult社の詳細情報によると…

- ✓ 最大値のパケットサイズ（4GB相当：0xffffffff）が定義されているヘッダー情報を持つCODESYSプロトコル（port 2455/tcp）のパケットを機器に送信すると、機器側でメモリの確保に失敗し、処理が中断される
- ✓ ソケットが作成されたままになり閉じられない
- ✓ CODESYSでは最大接続数が決まっているため、繰り返しパケットを送信することで新たな接続を受け入れられない状態になる

CVE-2021-34593の検証結果 - 脆弱性の再現（続き）

- 細工したパケットを送信した結果、CODESYS開発環境とPLCの接続ができなくなったことを確認（復旧には機器の再起動を要する）



細工したパケットの送信後：CODESYS開発環境とPLCが接続不可に

CVE-2021-34593の検証結果 - 監視・制御への影響

■ PLCの制御関連機能への影響はないことを確認

― シミュレーター上で操作した結果はそのままランプや表示機に反映された

EWSとPLCが接続不可になった直後の
シミュレーターの状態

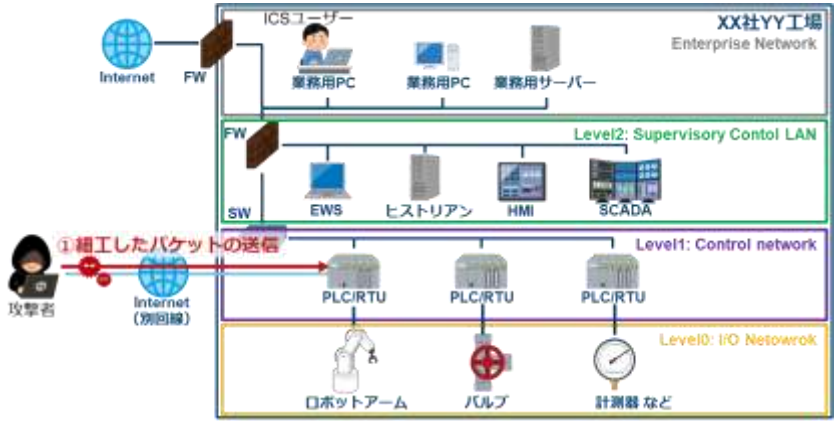
シミュレーターを操作してランプの点灯状態や
表示機の数字が変更された状態

細工したパケットの送信後：PLCの制御関連機能への影響確認

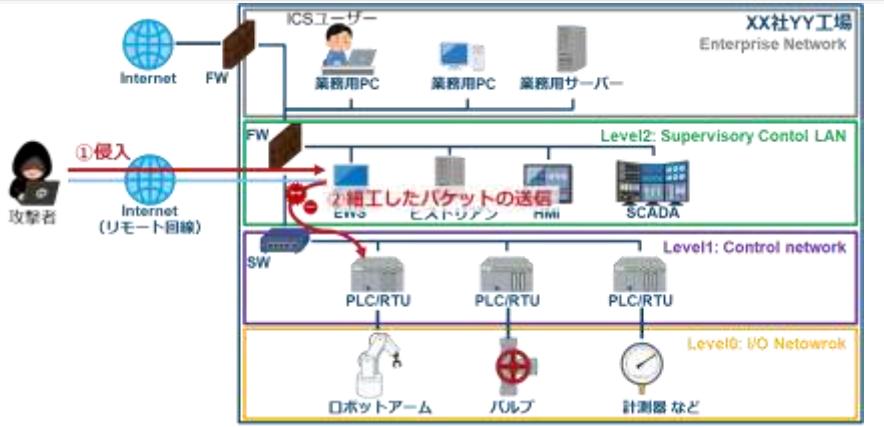
CVE-2021-34593を使用した攻撃シナリオ

- 次のようなケースが想定されます
  1. インターネット経由でアクセス可能なPLCに対して、攻撃者が細工したパケットを送信する
  2. 攻撃者が何らかの方法（例：リモートメンテナンス回線経由など）で制御系ネットワーク（Level2 / Level1）に侵入し、そこからPLCに対して細工したパケットを送信する

想定される攻撃シナリオ1



想定される攻撃シナリオ2



対策について

- 第三者にネットワーク経由で影響を受ける機器にアクセスされないようにする
  - 不要な場合はインターネットから切り離す
  - インターネット経由でアクセスする場合はVPNなどのセキュアな通信を使用する（VPN製品のセキュリティパッチの最新化も）
  - ネットワーク経由での当該機器へのアクセスを必要最小限にする
  - 当該機器をリモートメンテナンスをする場合は、リモート回線の接続をメンテナンス作業時のみに留める　など

- ICS機器ベンダーからアップデートが提供されている場合は、影響を確認した上で適用する
  - 現時点でアドバイザリ―公表しているICS機器ベンダーはWAGO社のみ

CVE-2021-34593のまとめ

- 誰に攻撃されるか
  - ネットワーク経由で当該機器にアクセス可能な第三者
- 攻撃された際の影響
  - エンジニアリングワークステーション（CODESYS開発環境）から当該機器へのアクセスができず、メンテナンス作業ができなくなる
  - 監視・制御の機能への影響はなさそう
- 攻撃に転用可能な実証コード
  - なし（ただし、詳細情報からスクリプトを作成することは容易）
- 悪用事例
  - なし
- 対策
  - CODESYS社のアップデートが提供されている
  - 対策が提供されているICS機器ベンダーはWAGO社のみ

本件については、ICS機器ベンダーに情報を提供

分析事例の振り返りと課題

今回の脆弱性の対応の必要性について

- この脆弱性の影響を受ける製品があった場合、どうしますか？
  - 皆さんも一緒に考えてみてください

今回の脆弱性の対応の必要性について（続き）

- 緊急対応を要すると判断した人はいないのではないでしょうか

ICSユーザーが対応要否判断のために必要な情報とは

- 自組織で影響を受ける製品を使用しているかどうか
- 対策方法の有無
- 当該脆弱性を使用した攻撃が行われた場合のICS全体への影響
- 当該脆弱性を使用した攻撃の可能性

自組織で影響を受ける製品を使用しているかどうか

■ 資産管理が脆弱性管理の第一歩

- 脆弱性情報には影響を受ける製品の名称・型番、バージョン情報が記載されているため、この情報との付け合わせが必須
- 今回は、CODESYSライブラリに起因する脆弱性なので、当該ライブラリを使用しているICS機器ベンダーから公表された情報が必要

参考：制御システムにおける資産管理ガイドライン

- ✓ IPA ICSCoE 中核人材育成プログラム 3期生 資産管理プロジェクトの成果物
- ✓ 資産管理の範囲、収集すべき情報、資産情報の収集方法など、具体的な内容が記載されている
- ✓ 資産管理チェックリストも添付されており、資産管理に対する自組織の成熟度を確認できるようになっている

参考：IPA 産業サイバーセキュリティセンター
制御システムにおける資産管理の効率化
https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/assetmanagement.html

対策方法の有無

- ICS機器ベンダーから提供されている対策を確認
  - セキュリティパッチ（根本対策）
  - ワークアラウンド（リスク軽減策）

- まずはワークアラウンドの実施を検討
  - 製品特有のワークアラウンドが脆弱性情報に記載されていない場合は、一般的な対策の実施を検討する

  ※ 一般的な対策については、ICS機器ベンダーの脆弱性情報に記載されている場合があります

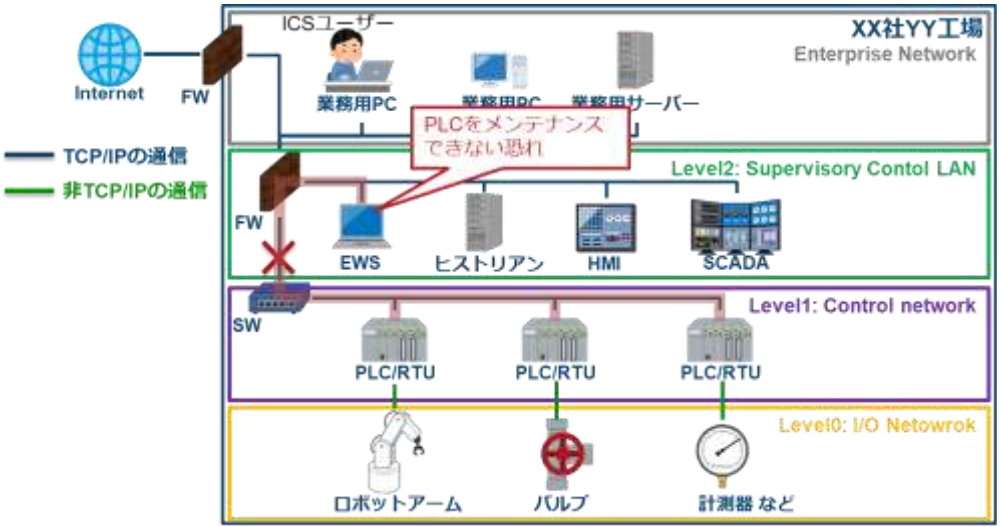
- セキュリティパッチの適用には慎重な確認を
  - 設備の動作上の問題だけでなく、変更管理上問題ないかも確認が必要

  ※ 一部の業界では、設備の変更管理に係る法規制が存在します

当該脆弱性を使用した攻撃が行われた場合のICS全体への影響

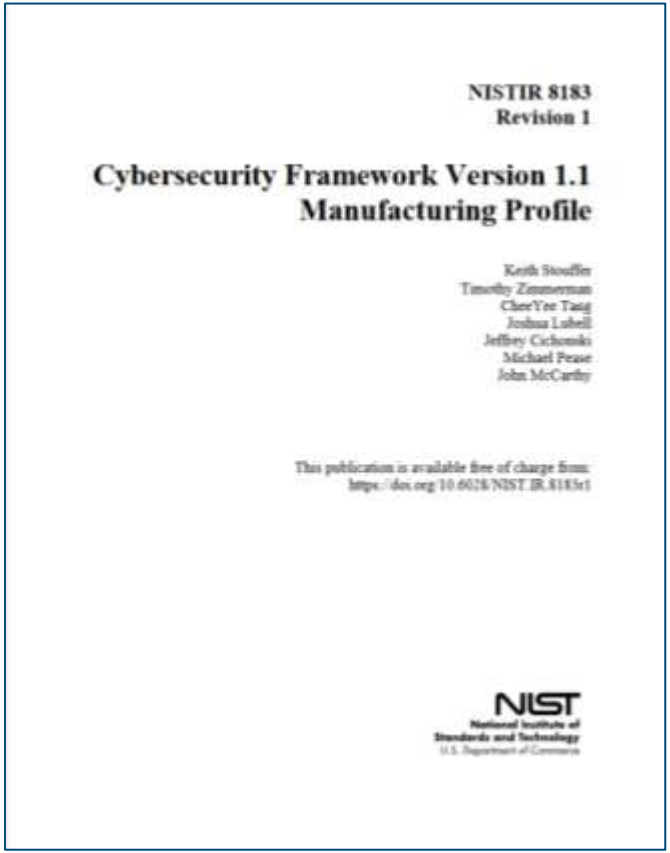
- CVSS v3の評価を過信しない
  - 今回、CVSS v3基本値は7.5（重要）と評価されているが…
    - 影響範囲は制御機器とエンジニアリングツール間の通信に限定
  - ICS全体の影響を踏まえた判断が必要

- 対応すべき脆弱性とは？
  - 引き起こされる恐れのある事象、事故の観点で考える
  - 安全対策（機能安全、本質安全）との兼ね合いも必要
  - 緊急停止判断に要する事象は避けたい



参考：CSF v1.1 Manufacturing Profile

- 2020年10月にNISTから公表された文書
- 製造業共通のビジネス上の目標として次の5つが定義されています
  - 環境安全の維持
  - 人的安全の維持
  - 製品品質の維持
  - 生産目標の維持
  - 機密情報の保護
- これらを阻害する事象となり得るかが判断のポイント


NISTIR 8183
Revision 1

Cybersecurity Framework Version 1.1
Manufacturing Profile

Keith Stouffer
Timothy Zimmerman
CherYee Tang
Joshua Lubell
Jeffrey Cichonski
Michael Pease
John McCarthy

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

参考：NIST
NISTIR 8183 Rev.1 Cybersecurity Framework Version 1.1 Manufacturing Profile
https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/final

当該脆弱性を悪用した攻撃が行われるか

- 脆弱性情報の公表だけでは判断できない
  - 脆弱性の公表はあくまでも「可能性」（あくまでも有るか、無いか）
  - 機器の自然故障のように「確率」は一定ではなく、状況に応じて変化する
    - 客観的事実にもとづいて発生確率（蓋然性）の高さを評価する必要がある
- 脆弱性を取り巻く状況の例
  - 脆弱性に関する詳細な解説が公表される
  - 脆弱性の存在を実証するコード（PoCコード）が公表される
  - 脆弱性の存在を確認するスキャンが観測される
  - 脆弱性を悪用した攻撃パケットが観測される
  - 脆弱性を悪用した攻撃によりインシデントが発生する
- インシデント調査によって製品の脆弱性が発見され、公表されるケースも

ICSユーザーの視点で整理すると…

攻撃によってもたらされる被害（損害）が大きい
被害（損害）を想定した際、ビジネス上の目標を大きく阻害する可能性がある

攻撃の機会がある
追加の対策を講じないと攻撃に晒される可能性がある

攻撃が容易である
詳細な解説やPoCコードがあり、攻撃コードを容易に作成される可能性がある

現実的な攻撃シナリオがある
どのように攻撃されるかを踏まえ、自組織の環境において、現実的な攻撃シナリオがある

※この図は報告者と開発者の間で調整された上で公表されたケースを想定

※公表時点でPoCコードが公表されていたり、攻撃活動が始まっていたりする場合も

※蓋然性の高まりを評価する上で確認する事項は順不同

参考：JPCERT/CCの注意喚起では…

- 「蓋然性の高まり」～「攻撃活動」に関連する情報として次のような記載がされている場合があります

記載例（一部）：

- ✓ JPCERT/CCは、YYYY年MM月DD日に本脆弱性を実証するコード（PoC）が公開されていることを確認しています。
- ✓ JPCERT/CCは、本脆弱性を悪用する実証コードが公開されていること、および国内にて本脆弱性の悪用を試みる通信を確認しています。
- ✓ XXXX（製品開発元）は次の脆弱性について悪用の事実を確認していると公表しています。
- ✓ XXXX（セキュリティベンダー）によると、MM月DD日から脆弱性の有無を調べる通信が、MM月DD日には脆弱な環境に不審ファイルを配置することを目的とした通信がそれぞれ観測されており、実際にファイルが配置される事例も確認されているとのことです。

注意喚起には「被害予防」と「被害拡大防止」の2つ目的があります

振り返りのまとめ：ICSユーザーによる対応要否の判断

- 想定される影響（リスク）の評価
  - どのように製品が使用されているかによって攻撃の成立条件や想定される影響は変わる
  - 安全対策（機能安全、本質安全）との兼ね合いも含めて考える
- 脆弱性を悪用した攻撃が差し迫ったリスクかどうかの確認
  - 蓋然性が高まっているか、偵察行動または攻撃活動が行われているか
- 実施済のセキュリティ対策との整合
  - 追加の対策が必要かどうかを判断する

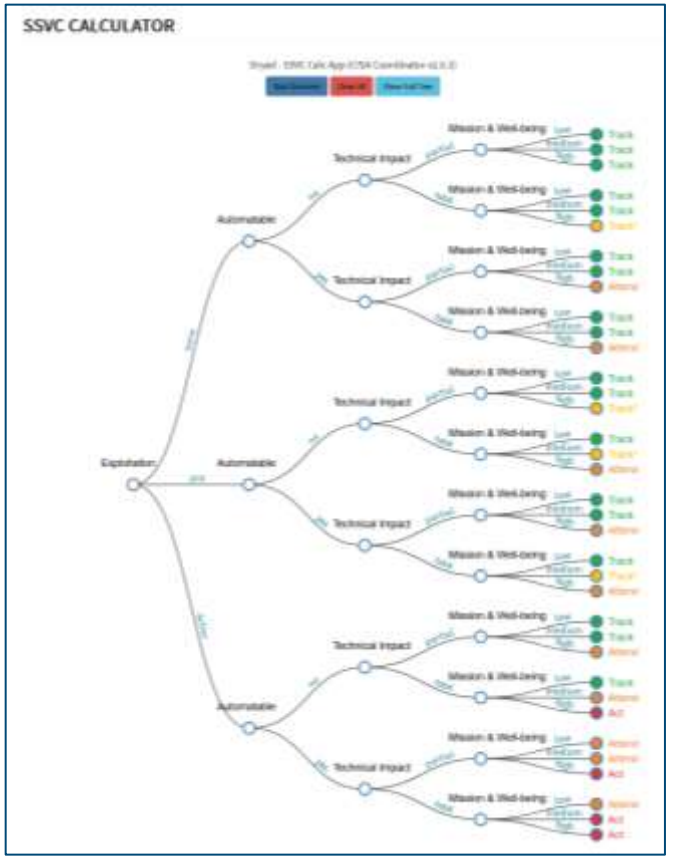
リスクと蓋然性のバランスを勘案しながら、いつ対策を実施するか判断する

脆弱性管理に関する参考情報

- CISA SSVC（Stakeholder-Specific Vulnerability Categorization）
- ICS-Patch

CISA SSVC（Stakeholder-Specific Vulnerability Categorization）

- SSVCは2019年にCISAとカーネギーメロン大学ソフトウェア工学研究所が共同で作成した脆弱性分析手法
- 米国では2020年に政府機関や重要インフラ向けにカスタマイズしたSSVC決定木「CISA SSVC」を開発、導入
- 2022年11月にWebで使用可能なツール「CISA SSVC Calculator」を公開



参考：CISA
Stakeholder-Specific Vulnerability Categorization
https://www.cisa.gov/ssvc

CISA SSVCで導出される判断

■ CISA SSVC決定木では、次の4通りの判断があります

判断	説明
Track	現時点での対処は必要なし。脆弱性を継続的に追跡し、新たな情報を入手次第再評価を行う。この判断となった脆弱性は標準的な更新スケジュールの中で対応することを推奨している。
Track*	脆弱性に特定の特性があるため、状況の変化をより綿密に監視する必要がある。この判断となった脆弱性は標準的な更新スケジュールの中で対応することを推奨している。
Attend	組織内の管理者による注意を要する。必要なアクションとして、支援の要求や脆弱性に関する情報の要求が含まれ、社内外への通知の公表を伴う場合がある。この判断となった脆弱性は標準的な更新スケジュールよりも早く対応することを推奨している。
Act	組織内の管理者、指導者による注意を要する。必要のなアクションとして、支援の要求や脆弱性に関する情報の要求、社内外への通知の公表などがある。通常、社内のグループで全体的な対応策を決定するための会議を開き、合意した対応策を実施することになる。この判断になった脆弱性は、できるだけ早く対応することを推奨している。

参考：CISA
CISA Stakeholder-Specific Vulnerability Categorization Guide
https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide%20508c.pdf

CISA SSVCにおける判断要素

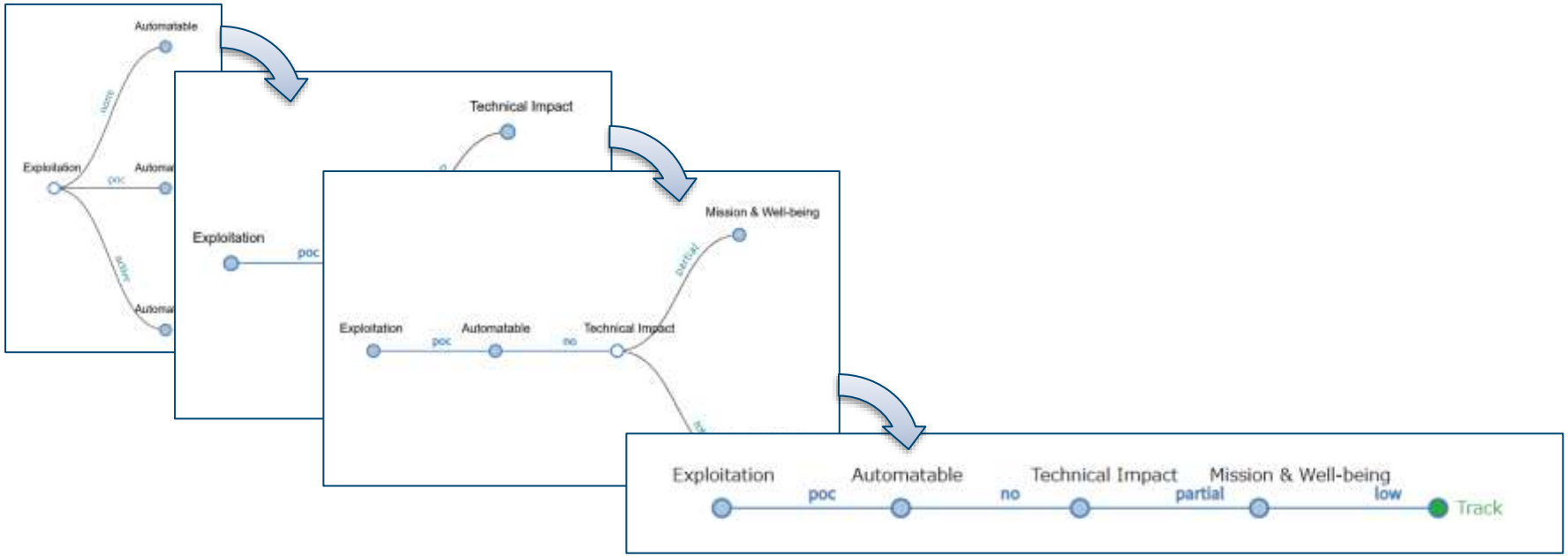
- 最終的な判断に至るために必要な要素は次の5つです

必要な要素	説明
Exploitation 現時点での悪用の状況	その脆弱性が悪用された形跡があるか、PoCの公開されているかどうか
Technical Impact 技術的影響	影響を受けるコンポーネントを完全に制御できるかどうか
Automatable 攻撃の自動化の可否	攻撃が自動化されているかどうか
Mission Prevalence 事業への影響	組織において通常業務の中断の間に継続する、または速やかに再開しなければならない重要な機能（Mission Essential Functions）への影響の度合い
Public Well-Being Impact 公共への影響	身体的および精神的被害、環境被害、財産的損害といった公共への影響の度合い

参考：CISA
CISA Stakeholder-Specific Vulnerability Categorization Guide
https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide%20508c.pdf

CISA SSVC Calculator

- それぞれの要素について状況を選択し、判断を導出します



参考：CISA
SSVC Calculator
https://www.cisa.gov/ssvc-calculator

ICS-Patch

- ICS特有の事情を考慮したSSVCベースの決定木
  - s4で生まれたプロジェクト
  - 2020年9月に公表されたバージョンはv0.5（最新版）

- ICS-Patchの特徴
  - 1つの要素を除き、ICSの資産情報にもとづく要素で判断を導出できる
  - 導出される判断は3つ（defer、scheduled、ASAP）になっている
  - 決定木の図は読みやすさを重視して、3つに分割されている

参考：Linkedin – Dale Peterson
ICS-Patch: What To Patch When?
https://www.linkedin.com/pulse/ics-patch-what-patch-when-dale-peterson

ICS-Patchで導出される判断

- ICS-Patchの決定木では、次の3通りの判断があります

判断	説明
Defer	リスク低減を目的としたサイバー資産へのセキュリティパッチの適用を実施しない、または予定を立てない（ICSユーザーは、システムのサポートを維持するためにメンテナンスの一環としてセキュリティパッチの適用を選択できる）
Scheduled	次回予定されているパッチ適用のタイミングでサイバー資産へのセキュリティパッチを適用する。ICSによっては、年1回または半年に1回の定期メンテナンス時になる場合があったり、四半期毎や月毎のパッチ適用がルール化されたりする場合もある
ASAP	サイバー資産のセキュリティパッチを安全な方法でできるだけ早く適用する

※ASAPは「As Soon As Possible」の略

参考：Dale Peterson
ICS-Patch
https://dale-peterson.com/wp-content/uploads/2020/10/ICS-Patch-0_1.pdf

ICS-Patchにおける判断要素

■ 最終的な判断に至るために必要な要素は次の5つです

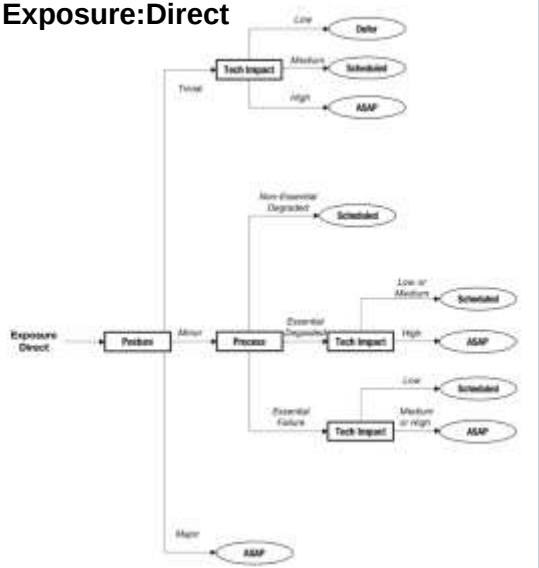
必要な要素	説明
Exposure 資産の露出度	そのサイバー資産が、設置されているゾーンからより信頼度の低いゾーンに直接的または間接的にアクセスできるかどうか
Safety Impact 安全への影響	監視・制御対象のプロセスの安全性に影響を与えるかどうか
Security Posture Change セキュリティ態勢の変更	パッチを適用することで攻撃者の目標達成がより困難になるかどうか ※多方面で脆弱なサイバー資産にパッチを適用しても効果があるかどうか
Process Impact プロセスへの影響	サイバー資産の可用性、完全性が毀損された場合にプロセスに与える影響
Technical Impact 技術的影響	CVSS v3スコアにもとづく判断項目 ※資産情報にもとづかない唯一の項目はこれ

参考：Dale Peterson
ICS-Patch
https://dale-peterson.com/wp-content/uploads/2020/10/ICS-Patch-0_1.pdf

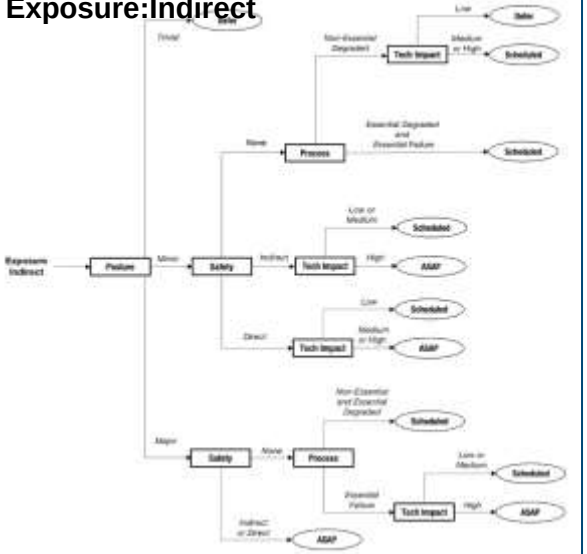
ICS-Patchの決定木は3種類

- ICS-Patchでは「Exposure」の結果にもとづく3つの決定木が存在
  - 残りの4要素を選択することで判断を導出します

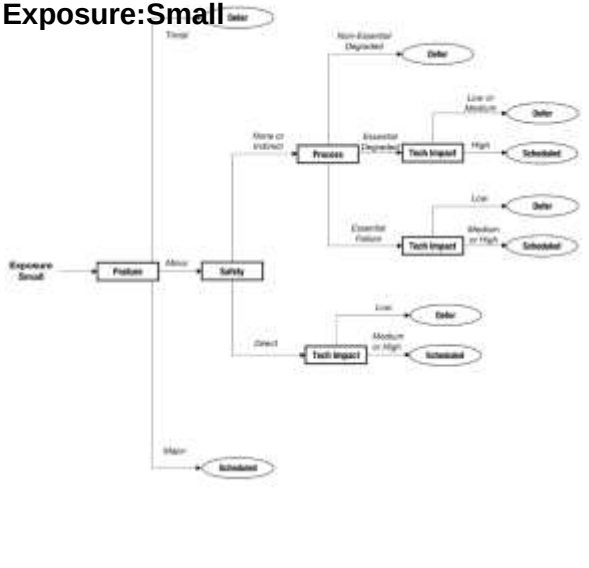
Exposure:Direct



Exposure:Indirect



Exposure:Small



参考：Dale Peterson
ICS-Patch
https://dale-peterson.com/wp-content/uploads/2020/10/ICS-Patch-0_1.pdf

参考情報について

分析事例の振り返りと照らしあわせてみるとどうでしょうか。

ぜひ、脆弱性管理を実施する上での参考にしてください。

最後に

- J-CLICS 攻撃経路対策編の紹介
- 講演の終わりに

J-CLICS 攻撃経路対策編の紹介

- SICE/JEITA/JEMIMAセキュリティ調査研究合同WGにて作成が進められてきた文書
  - JPCERT/CCは同WGにオブザーバーとして参加しています

- 制御システムとの接続点を攻撃経路と定義し、外部からの主な攻撃経路（4経路）の攻撃手順に対して実施すべきセキュリティ対策を検討した結果から作成された次の3つの文書で構成
  - 19問のチェックリスト
  - 設問項目ガイド
  - 対策マップ

J-CLICS 攻撃経路対策編　設問項目ガイド

※デザインは変更される可能性があります

STEP1／STEP2と攻撃経路対策編の違い

- STEP1／STEP2との位置づけの違いや掲載内容の違いは次のとおりです

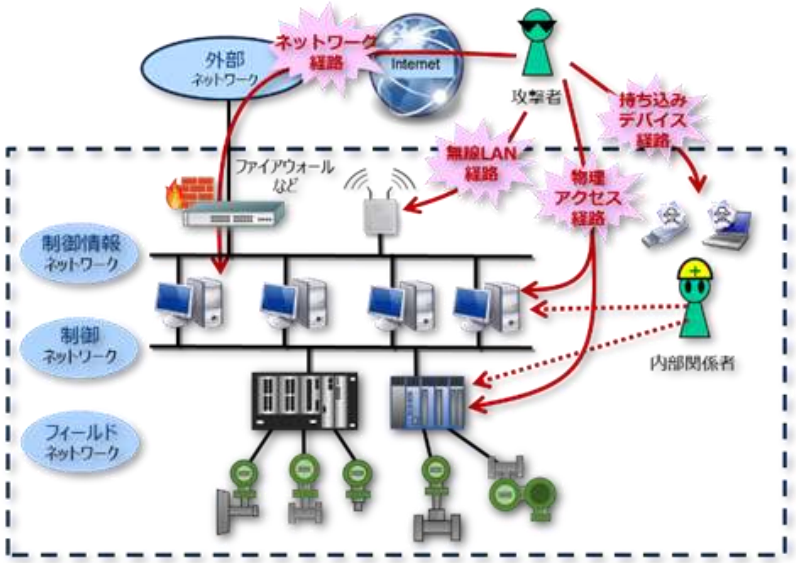
項目	J-CLICS STEP1／STEP2	J-CLICS 攻撃経路対策編
位置付け	セキュリティ対策の最初のステップ	セキュリティ対策の次のステップ
提供情報	とりあえず何をするべきか	何を何のためにやるべきか
掲載内容	実施しやすく，高い効果が期待できる推奨対策を掲載	優先度と過不足がわかる形で推奨対策を掲載
着目点	対策の実施難易度・重要度	攻撃経路・手順・成立条件

保護対象として想定されるシステム

- 「フィールドネットワーク」「制御ネットワーク」「制御情報ネットワーク」からなる3層モデルの制御システム

- 保護対象のシステムに対する代表的な攻撃経路と攻撃手法の分析を行い、その結果に基づいてセキュリティ対策を選定

- よりつながる制御システムへの備えとして、まずは自組織で統制できる制御システムの保護に重点を置いた



保護対象として想定されるシステム

4つの攻撃経路と19の設問

優先度：高 → 低

ネットワーク	無線LAN	持ち込みデバイス	物理アクセス
QN0： 外部ネットワーク接続の最小化	QR0： 無線LAN使用の最小化	QD0： 持ち込みデバイス使用の最小化	
QN1： ネットワーク構成情報の秘匿	QR1： 無線LAN構成情報の秘匿	QD1： ウイルス対策の実施	QP1： セキュリティ区画の設定
QN2： 境界防衛の実施	QR2： 電波状況の把握と管理	QD2： 持ち込みデバイスの限定	QP2： 入退管理の実施
QN3： 強力な認証の実施	QR3： 無線LAN機器のセキュリティ確保	QD3： 持ち込みデバイス内のデータの制限・検査	QP3： 施錠管理の実施
QN4： 内部ネットワークの分類	QR4： 認証管理の実施	QD4： エンドポイントセキュリティ対策の実施	
QN5： エンドポイントセキュリティ対策の実施			

J-CLICS 攻撃経路対策編の全文書（3点）

J-CLICS 攻撃経路対策編
チェックリスト

・○×形式でのチェックリストにより
対策状況を可視化
・設問項目は具体的かつ簡潔に記載

J-CLICS 攻撃経路対策編
設問項目ガイド

・攻撃経路ごとの対策の考え方や、
設問項目の背景、目的、想定される
攻撃、対策内容を分かりやすく解説

※デザインは変更される可能性があります

J-CLICS 攻撃経路対策編　対策マップ

・各攻撃経路ごとにシートを作成
・攻撃手順、攻撃の成立条件を整理
・成立条件ごとの対策（防御策、検知策、緩和策、
回復策）と各設問項目との関連性をマッピング

2022年度中の公開を予定

講演の終わりに

今回の講演は、ICSユーザーがICS関連製品の脆弱性情報をトリアージすることを念頭においた内容にしました。

しかしながら、ICSの脆弱性の管理や対処については、さまざまな課題があることを認識しています。

今回の講演を踏まえ、少しでも問題解決の一助になれば幸いです。

私の講演に関するアンケートで、脆弱性の管理や対応に関する皆さまの課題や悩みなどを是非お聞かせください。

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/