JPCERT CC®

JPCERT/CCにおける制御システム製品の脆弱性情報の収集及び分析

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（ICSR）
堀　充孝

本講演の趣旨

ICSユーザー組織のセキュリティ担当者が制御システム（以降「ICS」）製品の脆弱性への対応を考える機会に

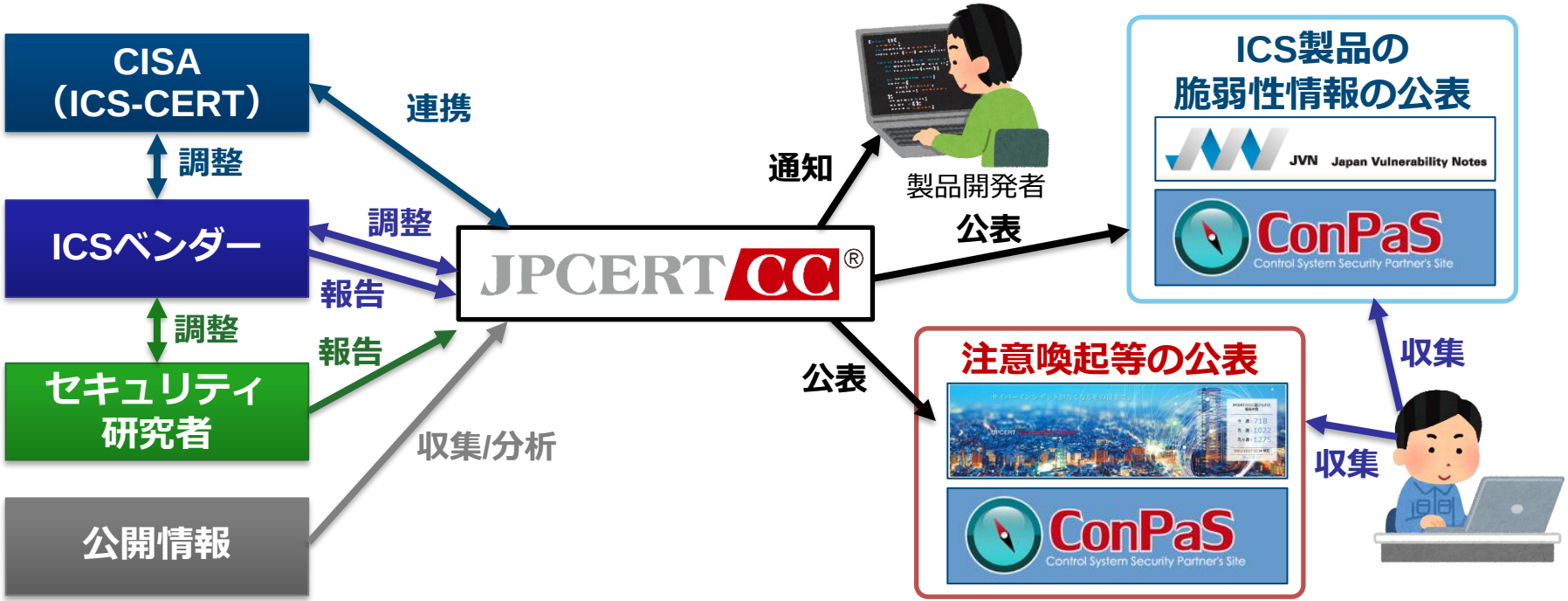
アジェンダ

- JPCERT/CCの活動のご紹介
  - ICS製品の脆弱性をユーザー組織に適切に提供するための活動
  - ICS製品の脆弱性情報の収集・分析
- 今回注目した制御システム製品の脆弱性情報
- まとめ

ICS製品の脆弱性をユーザー組織に適切に提供するための活動

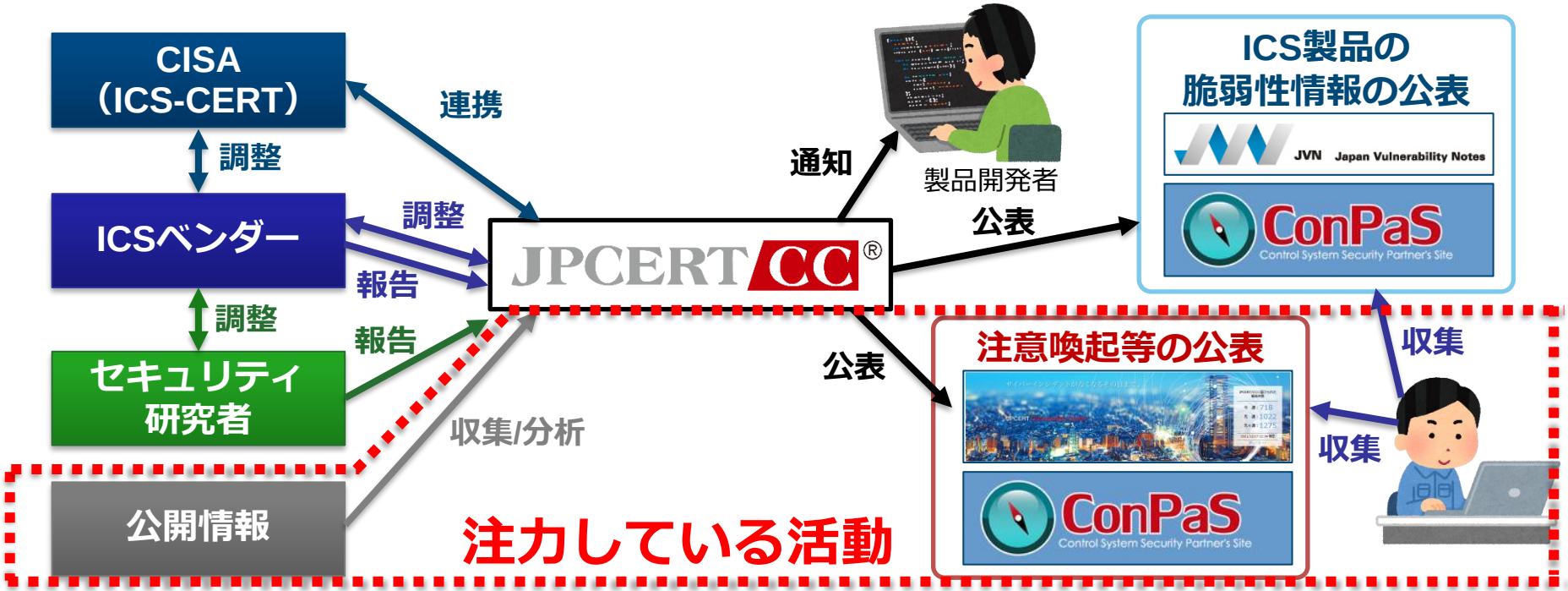
ICS製品の脆弱性情報の適切な流通を目指して

- JPCERT/CCでは、ユーザー組織に向けてICS製品の脆弱性情報を適切に提供するための活動を実施



ICS製品の脆弱性情報の適切な流通を目指して

■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



なぜ注力するのか

■ICS製品の脆弱性情報の公表経緯はさまざま

開発者　調整機関　報告者

ICSベンダーと報告者の間に調整機関が入り公表

報告者　開発者

ICSベンダーと報告者で直接やり取りして公表

発見者（報告者）

報告から長期間経過する等により、対策されないまま発見者が公表

発見者（報告者）

対策されないまま発見者がPoCコードを含めてフォーラム等に投稿

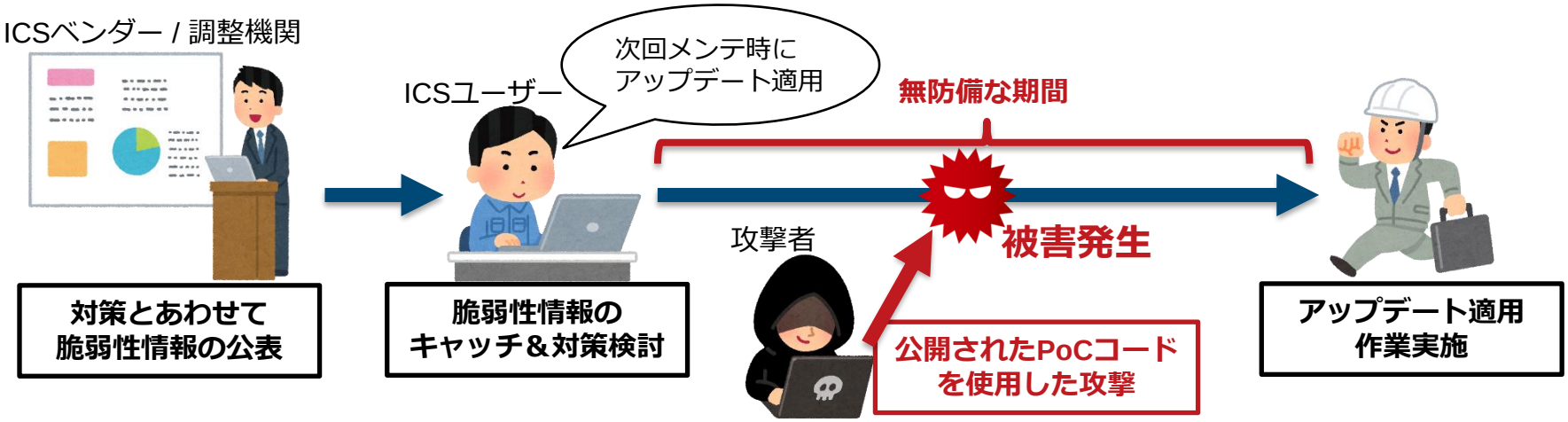
■ICS製品の脆弱性情報が公表される場所もさまざま

— 調整機関、ICSベンダー、セキュリティベンダー など

公開情報から広く脆弱性情報を収集する必要がある

なぜ注力するのか

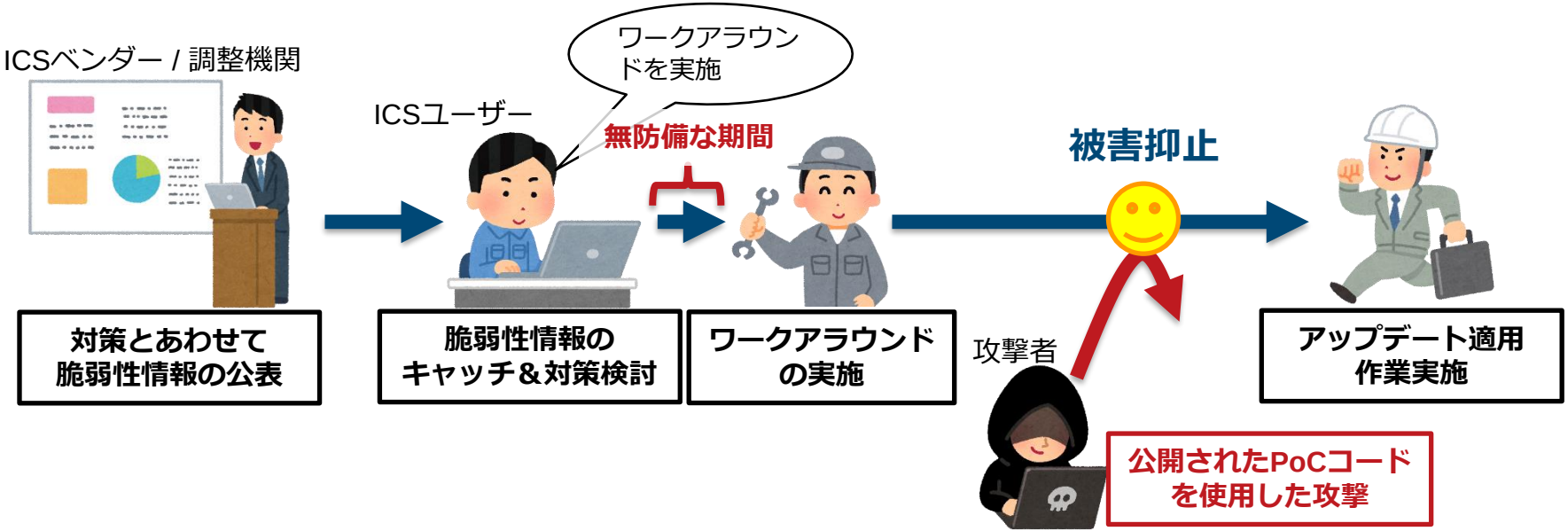
- ICSでは、対策とあわせて脆弱性情報が公表されてもすぐにアップデートを適用できない場合が多い
  - その間に脆弱性の存在を実証するコード（PoCコード）が公表されるとサイバー攻撃につながる恐れがある



脆弱性の悪用が容易な状況かどうかを把握する必要がある

緊急度の高いICS製品の脆弱性情報が出た場合に…

■ユーザー組織側でまず対応できることはないか
　― リスク軽減策（ワークアラウンド）の実施



攻撃に備えてICSユーザーが直ちに講じれる措置を提供する

ICS製品の脆弱性情報の収集・分析

収集から情報発信までの流れ

- 公開情報から広くICS製品の脆弱性情報を収集し、二段階の分析（簡易分析、詳細分析）を行った上で発信を検討

- 「注意喚起」相当の情報でない場合、その情報を必要とする組織に「参考情報」として情報提供する場合もある

簡易分析について

- 詳細分析の要否を判断するため、主に次の点を確認
  - その脆弱性を使用した攻撃が容易に可能な状況か
    - ✓ どのような経路で攻撃が行われるか
    - ✓ 攻撃の実施には認証が必要か
    - ✓ PoCコードが公開されているか など
  - その脆弱性を使用した攻撃が行われた際に想定される影響
    - ✓ ICSの可用性に大きな影響を及ぼす恐れがあるか
  - 影響を受ける製品の国内流通の状況
    - ✓ 国内に影響を与える可能性が低い情報の提供はノイズになる
  - 対策（ワークアラウンド、アップデート）の提供の有無
    - ✓ ユーザー組織側で取れる対策はあるか

攻撃につながる恐れがある情報は詳細分析で深掘り

詳細分析について

- 簡易分析の結果を踏まえ、複数の公開情報にもとづいて技術的な観点で更なる分析を行います

- 例えば…
  - 影響を受ける製品の用途
  - 影響を受ける製品で使われている技術
  - 脆弱性の原因、想定される影響、CVSS v3評価の妥当性
  - PoCコードの精査
  - インターネット経由でアクセス可能な製品の有無の確認 など

詳細分析の結果を踏まえて情報発信の検討を行う

詳細分析を行った中から注目した脆弱性情報

ICS関連ソフトウェアのファイル読み込みに関する脆弱性

- 今回注目した理由
  - 緊急性はなかったものの、対策がされないまま公表される脆弱性が散見された
  - その中でもエンジニアリングソフトウェアの脆弱性が多かった

- 以降、実際に詳細分析を行った脆弱性情報を例に解説
  - ユーザー組織の担当者は改めて自組織の運用をご確認ください

ICS関連ソフトウェアの
ファイル読み込みに関する脆弱性の解説

詳細分析例:

Delta Electronics製DOPSoftの
ファイル読み込みに関する脆弱性

参考：JVN
「JVNVU#92650134：Delta Electronics 製 DOPSoft に境界外読み取りの脆弱性」
https://jvn.jp/vu/JVNVU92650134/

Delta Electronics製DOPSoftとは

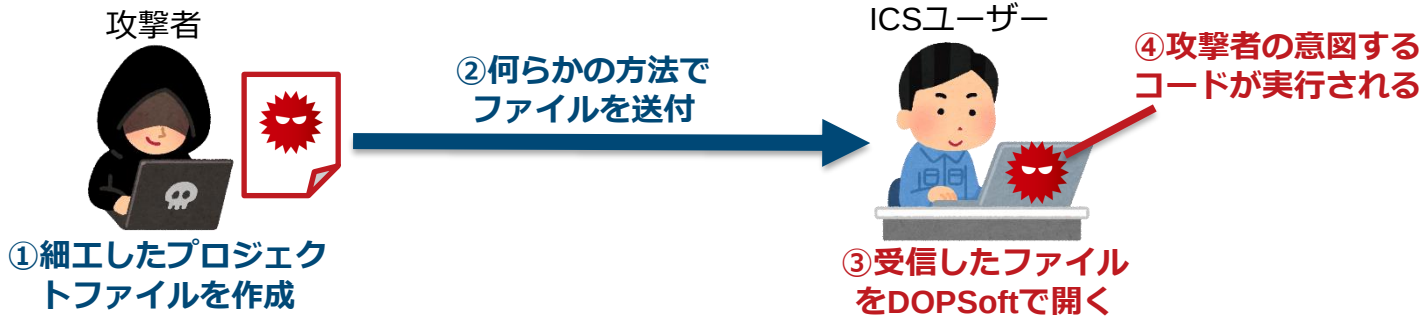
- Delta Electronics製のHMI機器「DOPシリーズ」専用の画面設計用ソフトウェア
  - ― エンジニアリングソフトウェアに相当

データのやり取りはUSBまたはEthernetなどを経由する

参考：Delta Electronics
「DOPシリーズ」
http://www.delta-japan.jp/Products/CategoryListT1.aspx?CID=0603&PID=ALL&hl=ja-JP

どのような脆弱性が見つかったのか

- プロジェクトファイル（DPAファイル）を読み込む際にファイルのデータが適切に検証されない
  - これにより割り当てられたメモリ領域（バッファー）の末尾を超えた読み込みが行われ、任意のコードが実行される



DOPSoftをインストールしたPCが乗っ取られる恐れ

CVSS v3基本評価基準を見ると…

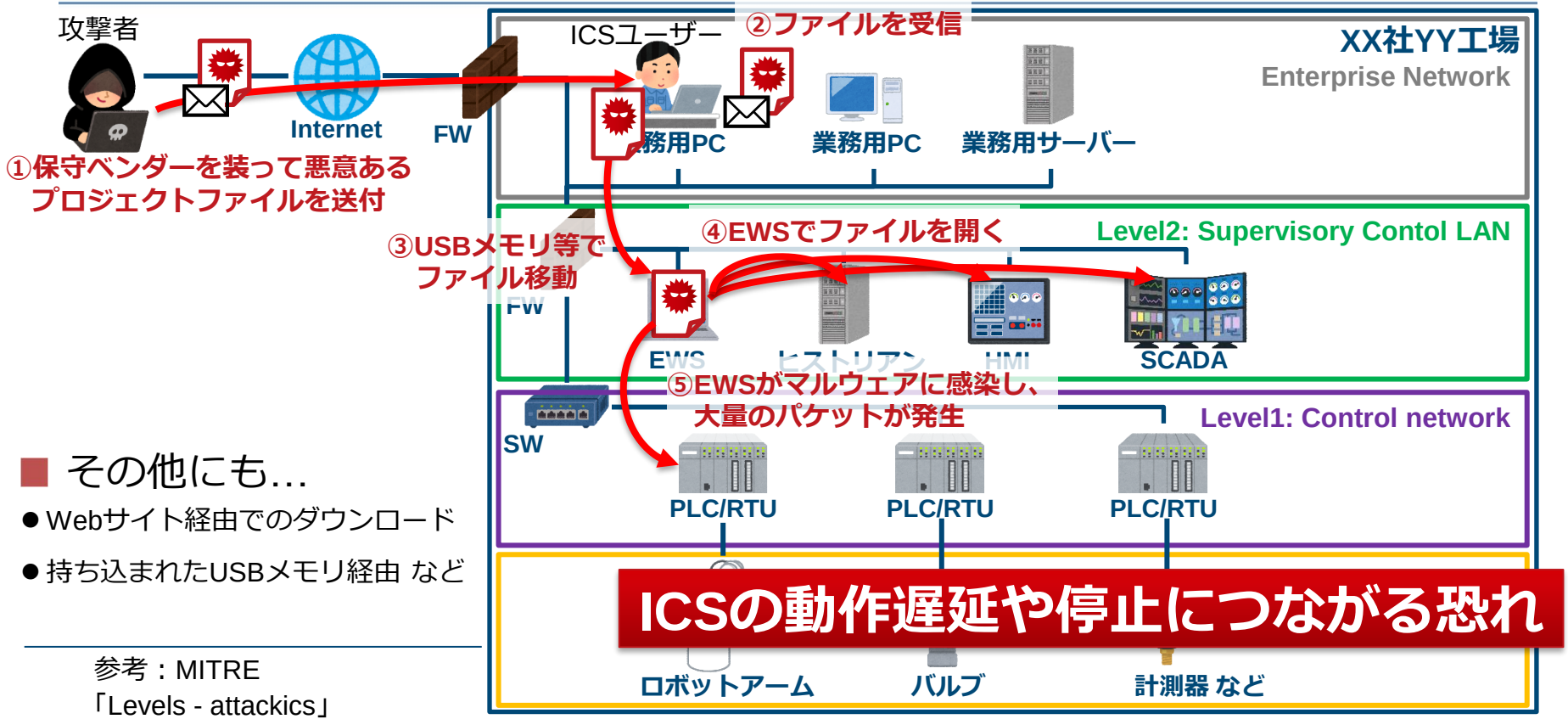
CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H　基本値: 7.8

基本評価基準	値	基本評価基準	値
攻撃元区分（AV）	ローカル（L）	スコープ（S）	変更なし（U）
攻撃条件の複雑さ（AC）	低（L）	機密性への影響（C）	高（H）
必要な特権レベル（PR）	不要（N）	完全性への影響（I）	高（H）
ユーザ関与レベル（UI）	要（R）	可用性への影響（A）	高（H）

- 攻撃者がこの脆弱性を悪用して攻撃を行う場合、複数のステップを踏む必要がある

参考：IPA
「共通脆弱性評価システムCVSS v3概説」
https://www.ipa.go.jp/security/vuln/CVSSv3.html

想定される攻撃（標的型メール攻撃）



■ その他にも…

- Webサイト経由でのダウンロード
- 持ち込まれたUSBメモリ経由 など

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

ワークアラウンド（軽減策）と根本対策

ワークアラウンド

- 信頼されたファイルのみを読み込む
  - ✓ 所定のフォルダーに保存されている正規のファイルのみを開く
  - ✓ DOPSoftをインストールしたPCの使用者を必要最小限に限定する
  - ✓ メールでプロジェクトファイルをやり取りしている場合は、不審なメールの添付ファイルは開かない など
    ※メールの対策はIPAの「標的型サイバー攻撃対策」の各コンテンツをご参考ください

根本対策

- ICSベンダーからアップデートが提供されている場合は、ICSへの影響をICSベンダーなどに事前確認した上で適用する
  - ✓ 本脆弱性に対応したDOPSoft（v4.0.11.22）がリリースされています

参考：IPA「標的型サイバー攻撃対策」
https://www.ipa.go.jp/security/ta/index.html

ICS関連ソフトウェアの
ファイル読み込みに関する脆弱性についてのまとめ

- 今回紹介したものは、エンジニアリングソフトウェアだが、他にも次のようなICS関連ソフトウェアがある
  - SCADA/HMIソフトウェア
  - リモート監視用ソフトウェア
  - 産業用ネットワーク機器の統合管理ソフトウェア
  - 3D設計用のソフトウェア など

ICS関連ソフトウェアのファイルの運用を改めてご確認ください

- ✓ **ファイルの取り扱いに関するルールは定められているか**
- ✓ **ソフトウェアの使用者は必要最小限か**
- ✓ **外部組織や他部署とのファイルのやり取りの方法 など**

まとめ

まとめ

- JPCERT/CCの活動の紹介
- 脆弱性情報の分析について
- ICSユーザーへのお願い

最後に

- ICS製品の脆弱性情報のより適切な分析や提供のため、提供いただける情報がございましたら、連絡先までご連絡いただけますと幸いです

- 連絡先

  一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）

  制御システムセキュリティ対策グループ

  Email：icsr@jpcert.or.jp

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/

ご清聴ありがとうございました