ICS 脆弱性分析レポート ― 2021 年度上期 ―

一般社団法人 **JPCERT** コーディネーションセンター

2022 年 **3** 月 **28** 日

JPCERT CC®

目次

1. はじめに

1.1. JPCERT/CC における ICS 関連製品の脆弱性情報の取り扱い

一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」）では、ICS 関連製品の脆弱性情報を JVN（Japan Vulnerability Notes）[1]や制御システムセキュリティ情報共有ポータルサイト ConPaS[2]に掲載しています。これらは、米国 CISA[3]や JPCERT/CC が国内の ICS ベンダーと調整した案件が主な情報源ですが、最近では他の CERT 組織や国内および海外のセキュリティベンダー、ICS ベンダーなどからも脆弱性情報が公表されています。このような状況を踏まえ、JPCERT/CC では ICS 関連製品の脆弱性情報をインターネットなどの公開情報から積極的に収集し、深刻かつ影響範囲が広いと思われる脆弱性情報が公表された場合には、「注意喚起 [4]」と呼ばれる情報を発行して利用者に広く対策を呼びかけています。また、「注意喚起」の基準に満たないものの国内で利用が認められている ICS 関連製品の脆弱性情報は、関係する ICS ユーザー組織や ICS ベンダー組織に適宜提供しています。

「注意喚起」の発行を検討する際は、脆弱性の内容や想定される影響、脆弱性の悪用が容易な状況になっていないかなど、脆弱性そのもののリスクを評価し、影響を受ける製品の日本国内での流通状況や、ICS ユーザー組織での該当製品の利用状況などを公開情報の範囲で収集、分析した上で情報提供の可否を判断しています。そのため、JPCERT/CC から公表される ICS 関連製品の「注意喚起」は、ICS ユーザー組織の担当者にもぜひ収集いただきたい情報です。

1.2. 本文書の目的

本文書は、2021 年度上期において JPCERT/CC が「注意喚起」の発行を検討するために詳細分析を行った ICS 関連製品の脆弱性情報の中から特に注目すべき情報を解説したものです。本文書を通じて、ICS ユーザー組織のセキュリティ担当者が、ICS 製品の脆弱性への対応を検討する上での参考になれば幸いです。

---

1 Japan Vulnerability Notes（JVN）
https://jvn.jp/

2 制御システムセキュリティ情報共有ポータルサイト ConPaS - JPCERT/CC
https://www.jpcert.or.jp/ics/ics-community.html

3 Industrial Control Systems - CISA
https://www.cisa.gov/uscert/ics

4 注意喚起 - JPCERT/CC
https://www.jpcert.or.jp/at/2022.html

2. 2021 年度上期に詳細分析を行った ICS 関連製品の脆弱性情報

2021 年度上期に JPCERT/CC が「注意喚起」の発行を検討するために詳細分析を行った ICS 関連製品の脆弱性情報は、表 1 のとおり 23 件でした。これらの脆弱性情報は、インターネットなどの公開情報から収集したものの中から「想定される影響」「CVSS v3 基本評価基準による評価結果」「脆弱性の存在を実証するコード（以下「PoC コード」）の公開状況」「製品の国内流通状況」「対策の提供状況」を踏まえた簡易分析を行い、日本国内の ICS ユーザー組織に直ちに影響が出る恐れがあると判断したものです。これらの情報に対し、「影響を受ける製品の詳細情報（用途や使われ方、使用されている技術など）」「影響を受けるコンポーネントの範囲」「攻撃が行われた場合に想定される被害」などの技術的な観点から詳細分析を行いました。

［表 1：2021 年度上期に JPCERT/CC が詳細分析を行った ICS 関連製品の脆弱性情報一覧］

情報確認日	タイトル
2021/04/19	DNS の実装に関する脆弱性群「NAME:WRECK」
2021/04/26	Advantech WebAccess/HMI のファイル読み込みに関する脆弱性
2021/05/03	OpenPLC v3 の Web サーバー機能にリモートコード実行の脆弱性
2021/05/10	Delta Electronics 製 DOPSoft のファイル読み込みに関する脆弱性
2021/05/13	Siemens 製 Solid Edge Viewer のファイル読み込みに関する脆弱性
2021/05/19	BELDEN 製 HiOS および HiSecOS に認証回避の脆弱性
2021/05/19	Moxa 製 NPort IA5000A シリーズに複数の脆弱性
2021/05/20	CODESYS 製 CODESYS V2 Web サーバーに関する脆弱性
2021/05/20	Advantech 製 BB-ESWGP506-2SFP-T にハードコードされた認証情報の使用の脆弱性
2021/05/25	CODESYS 製 CODESYS V3 関連製品の脆弱性
2021/06/02	B&A Automation 製 Automation Runtime に Ntpd 関連の脆弱性
2021/06/03	Kornix Technology 製産業用スイッチに複数の脆弱性
2021/06/15	Solar-Log 製 Solar-Log 500 に複数の脆弱性
2021/06/15	Wibu-Systems 製 WibuKey Runtime に引用符で囲まれていない検索パスまたは要素の脆弱性
2021/06/29	Wibu-Systems 製 CodeMeter のバッファエラーの脆弱性
2021/06/30	Phoenix Contact 製 PLCNext、ILC 2050 BI、FL MGUARD DM UNLIMITED、TC ROUTER、CLOUD CLIENT に OpenSSL 関連の脆弱性
2021/07/08	Advantech 製 WebAccess Node に複数の脆弱性
2021/07/13	Ricon Mobile 製産業用 LTE ルーター S9922XL に OS コマンドインジェクションの脆弱性
2021/07/20	Advantech 製 R-SeeNet に複数の脆弱性
2021/07/27	Advantech 製 WebAccess/NMS に関する重要な機能に対する認証の欠如の脆弱性
2021/08/17	Delta Electronics 製 DOPSoft のファイル読み込みに関する脆弱性

情報確認日	タイトル
2021/08/31	富士電機製 Tellus Lite のファイル読み込み関する脆弱性
2021/09/06	Moxa 製鉄道用無線アクセスコントローラー等に複数の脆弱性

2021 年度上期においては、これらの詳細分析の結果から「注意喚起」の発行につながる脆弱性情報はなかったものの、ICS ユーザー組織に向けて公表すべき情報として、表 2 のとおり JVN に掲載しました。

［表 2：ICS 関連製品の脆弱性情報の詳細分析から情報提供に至った脆弱性情報の一覧］

公表日	タイトル
2021/05/12	JVNVU#98262671: Advantech 製 WebAccess/HMI Designer に複数の脆弱性
2021/05/12	JVNVU#92650134: Delta Electronics 製 DOPSoft に境界外読み取りの脆弱性
2021/05/26	JVNVU#91051134: Siemens 製品に対するアップデート (2021 年 5 月) ※一部情報の更新

その他の脆弱性情報は、適宜その情報が必要と思われる組織に情報を提供しています。

3. 2021 年度上期における注目すべき ICS 関連製品の脆弱性情報

表 1 に示したように 2021 年度上期には複数の ICS 製品のファイル読み込みに関する脆弱性情報が ICS ベンダーから対策が提供されない状態で公表されました。そのことから、ここでは、当該脆弱性情報について、特定の情報の例をとりあげ、その分析から情報提供にまで至った経緯を解説します。

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

3.1.1. 情報が公表された経緯

Delta Electronics 社が提供する DOPSoft は、同社の HMI 製品「DOP シリーズ」専用の開発ソフトウェア[5]です。2021 年 5 月 6 日に海外セキュリティ組織によって、本製品に関する複数の脆弱性情報[6]が公表されました。これらの脆弱性は、海外セキュリティ組織から Delta Electronics 社および CISA に報告され、CISA と Delta Electronics 社の間で調整が行われていましたが、報告から長時間が経過したことにより海外セキュリティ組織の情報公開ポリシーに従って公表されています。そのため、公表時点において Delta Electronics 社からアップデートやワークアラウンドは提供されていませんでした。

3.1.2. 本脆弱性に対する簡易分析

3.1.2.1. 想定される影響

複数公開された脆弱性情報の中で悪用された場合のリスクが一番高いとされる脆弱性は、「境界外読みとりの結果、DOPSoft を実行する権限の範囲で任意のコードを実行される可能性がある脆弱性（ZDI-21-517）」です。

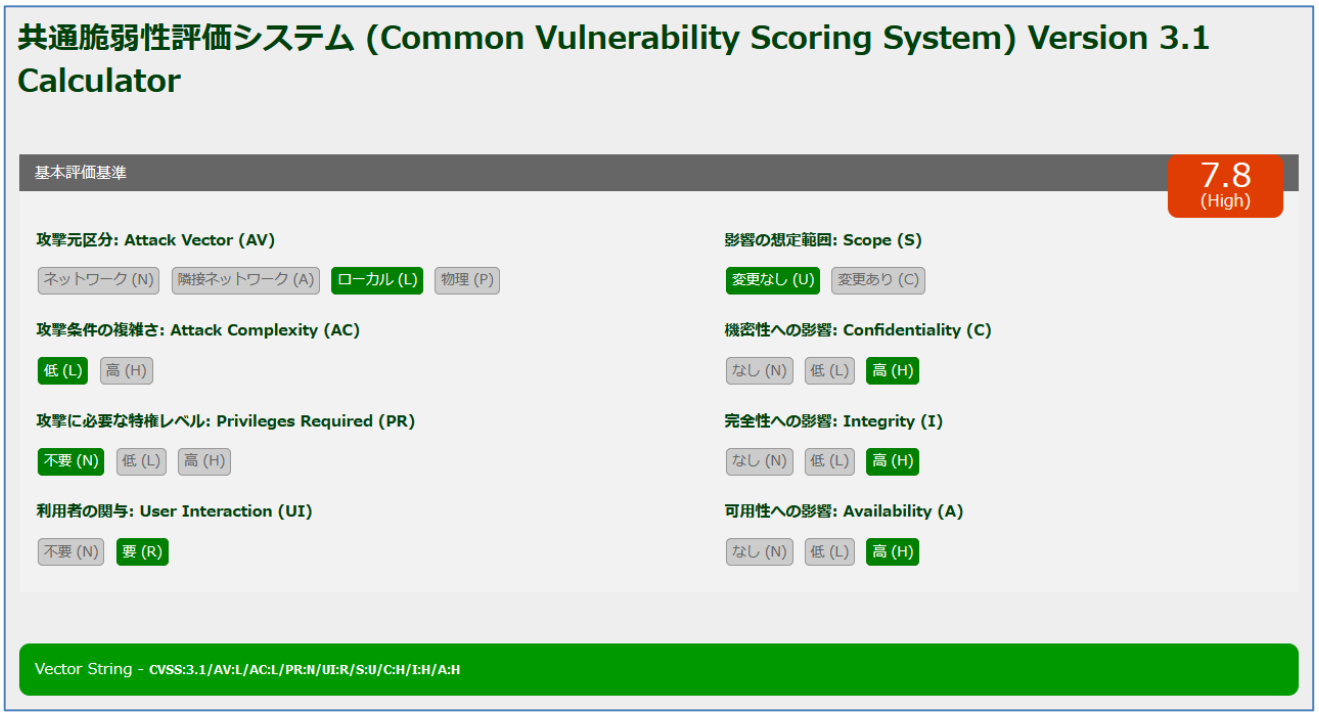
3.1.2.2. CVSS v3 基本評価基準による評価結果

共通脆弱性評価システム（CVSS）Version 3 による本脆弱性の評価結果は図 1 のとおりです。

---

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

[6] 参考：(0Day) Delta Industrial Automation DOPSoft DPA File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability
https://www.zerodayinitiative.com/advisories/ZDI-21-517/
(0Day) Delta Industrial Automation DOPSoft DPA File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability
https://www.zerodayinitiative.com/advisories/ZDI-21-510/
https://www.zerodayinitiative.com/advisories/ZDI-21-511/
https://www.zerodayinitiative.com/advisories/ZDI-21-512/
https://www.zerodayinitiative.com/advisories/ZDI-21-513/
https://www.zerodayinitiative.com/advisories/ZDI-21-514/
https://www.zerodayinitiative.com/advisories/ZDI-21-515/
https://www.zerodayinitiative.com/advisories/ZDI-21-516/
https://www.zerodayinitiative.com/advisories/ZDI-21-518/
https://www.zerodayinitiative.com/advisories/ZDI-21-519/



［図 1：共通脆弱性評価システム（CVSS）Version 3 による本脆弱性の評価結果 [7]］

本脆弱性の攻撃元区分はローカル（AV：L）、攻撃に必要な特権レベルは不要（PR：N）、利用者の関与は必要（UI：R）です。この評価結果から、第三者が本脆弱性を使用した攻撃を行うためには、攻撃対象の PC を直接操作するか、ユーザーを騙して攻撃対象の PC を操作させる必要があります。

3.1.2.3. PoC コードの公開状況、製品の国内流通状況、対策の提供状況、簡易分析の結論

攻撃に転用可能な PoC コードは公開されていませんでした。そのため、本脆弱性が直ちに攻撃につながるものではないと考えられます。しかし、CVSS 評価結果からシステムの可用性への影響が高い（A：H）ことや、Delta Electronics 社から対策が公表されない状態で海外セキュリティ組織から脆弱性情報が公表されたこと、同社が日本国内に向けて HMI 製品の販売を行っていることから詳細分析を行いました。

3.1.3. 本脆弱性に対する詳細分析

詳細分析では、脆弱性の具体的な ICS への影響や攻撃シナリオについて分析しました。

3.1.3.1. 影響を受ける製品の詳細情報、影響を受けるコンポーネントの範囲

DOPSoft v4.0.10.17 およびそれ以前のバージョンには、専用のプロジェクトファイル（DPA ファイル）

[7] 引用元：共通脆弱性評価システム (Common Vulnerability Scoring System) Version 3.1 Calculator
https://jvndb.jvn.jp/cvss/ja/v31.html#CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

を読み込む際にデータの検証が適切にされず、メモリの境界外に及ぶ読み取り[8]が発生する脆弱性が存在します。そのため、第三者が意図するコードを組み込んだプロジェクトファイルをユーザーが DOPSoft 上で読み込ませることにより、DOPSoft が実行されている権限で第三者によって組み込まれたコードを実行される可能性があり、その結果 PC を不正に操作されるなどの恐れがあります。

DOPSoft のようなエンジニアリングソフトをインストールした PC は、PLC や HMI などの制御機器をメンテナンスするため、制御システムネットワーク上に設置されている場合[9]があります。その場合、本脆弱性を使用してエンジニアリング PC を不正に操作し、そこからアクセス可能な制御システム関連のサーバーや PLC や HMI といった制御機器などに影響を与える恐れがあります。

3.1.3.2. 攻撃が行われた場合に想定される被害

第三者が本脆弱性を使用した攻撃を行う場合、ローカル環境から攻撃する必要があること、ファイルを開くというユーザーの操作が必要であることから、次のような攻撃シナリオが想定されます。

(1) フィッシングメールに添付された不審なファイルをユーザーが DOPSoft で開く
(2) Web サイトからダウンロードした不審なファイルをユーザーが DOPSoft で開く
(3) 外部から持ち込まれた USB メモリに保存されている不審なファイルをユーザーが DOPSoft で開く
など

3.1.3.3. 詳細分析の結論

攻撃に転用可能な PoC コードは簡易分析後も公開されていなかったため、詳細分析においても直ちに攻撃につながる脆弱性ではないという結論になりました。

3.1.4. 情報提供

以上の分析結果から、本脆弱性が直ちに攻撃につながるものではありません。しかし、Delta Electronics 社から対策が提供されない状態で公表された脆弱性であることや国内での流通度を鑑みて JVN で情報を発信しました。

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

---

[8] CWE-125: Out-of-bounds Read - CWE
https://cwe.mitre.org/data/definitions/125.html
[9] 参考：Levels - MITRE ATT&CK for ICS
https://collaborate.mitre.org/attackics/index.php/All_Levels

4. ICS ユーザー組織への推奨事項およびお願い

4.1. 3.1 で解説した脆弱性への対策として推奨する事項

ICS 関連ソフトウェアにおけるファイル読み込みの脆弱性を使用した攻撃は、攻撃者によって細工されたファイルをユーザーが ICS 関連ソフトウェアで開いたタイミングで成立するため、本脆弱性に対するリスク軽減策は「信頼されたファイルのみを開くこと」になります。そのため、所定のフォルダーに保存されているファイルのみを開く、ICS 関連ソフトウェアをインストールした PC やサーバーの使用者を必要最小限にする、メールで ICS 関連ソフトウェアの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を開かないなどの対策を推奨しています。また、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 ベンダーに事前確認した上で適用することを推奨しています。

ICS 関連ソフトウェアの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、ICS ソフトウェアの使用者は必要最小限になっているか、外部組織との ICS 関連ソフトウェアのファイルのやり取り方法など、ICS 関連ソフトウェアのファイルの運用について改めてご確認ください。

4.2. JPCERT/CC から入手した ICS 製品の脆弱性情報への対応について

ICS は、容易に停止できないかつ 1 点もののシステムであること、設備の変更管理を厳格に行う必要があることなどから、ICS ベンダーから脆弱性に対応したアップデートが提供されてもすぐに適用できません。そのため、即時の対応が必要な脆弱性については、ワークアラウンドの実施を検討することになります。脆弱性への対応の可否や優先度を決めるにあたっては、ICS ごとに影響を受ける製品がどのように設置されているかを確認した上でリスクを評価する必要があります。例えば、ネットワーク経由でリモートから攻撃が可能な脆弱性の情報が公表されても、その製品がインターネットから直接アクセス可能な状態でなければ脆弱性が悪用されるリスクは下がります。

JPCERT/CC では、日本国内の影響を公開情報の範囲で調査した上で「注意喚起」を発行していますが、影響を受ける製品が実際にどのように使われているかは ICS 環境ごとに異なります。そのため、ICS ユーザー組織のセキュリティ担当者が、JPCERT/CC から提供される「注意喚起」などの脆弱性情報を収集した際には、改めて自組織の ICS 環境を踏まえた評価をいただけますと幸いです。また、日々の ICS 製品に関する脆弱性情報の収集には、JVN や ConPaS をご利用ください。

Japan Vulnerability Notes（JVN）
https://jvn.jp/
制御システムセキュリティ情報共有ポータルサイト ConPaS
https://www.jpcert.or.jp/ics/ics-community.html

なお、本文書で解説した「2021 年度上期における注目すべき ICS 関連製品の脆弱性情報」や表 1 に記載されている脆弱性情報などにつきまして、提供いただける情報がございましたら JPCERT/CC までご連絡ください。

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