当社製品の TCP プロトコルスタックにおけるなりすましの脆弱性について

公開日 2020 年 8 月 31 日
最終更新日 2024 年 6 月 13 日
三菱電機株式会社

■概要

複数の当社製品の TCP プロトコルスタックにおいて、セッション管理の不備があるため、なりすましの脆弱性が存在することが判明しました。これらの脆弱性を悪意のある攻撃者に悪用された場合、正規の機器になりすまし、任意のコマンドを実行されることにより、情報の漏えい、情報の破壊・改ざん等の影響を受ける恐れがあります。(CVE-2020-16226)

現時点で判明している本脆弱性の影響を受ける製品名を以下に示しますので、対策又は軽減策・回避策の実施をお願いいたします。本脆弱性の影響を受ける製品名、対策及び軽減策・回避策は、順次更新いたします。

■脆弱性の説明

複数の当社製品の TCP プロトコルスタックでは、セッション管理の不備があるため、攻撃者によって、正規の機器になりすまされ、任意のコマンドを実行されることにより、情報の漏えい、情報の破壊・改ざん等の影響を受ける恐れがあります。(CWE-342)

■脆弱性がもたらす脅威

悪意のある攻撃者に脆弱性を悪用された場合、正規の機器になりすまされ、任意のコマンドを実行されることにより、情報の漏えい、情報の破壊・改ざん等の影響を受ける恐れがあります。

■影響を受ける製品、対策方法及び軽減策・回避策

[1]【シーケンサ MELSEC】

型番	対策及び軽減策・回避策
NZ2FT-MT, 全バージョン NZ2FT-EIP, 全バージョン	<お客様での対応> 対策版のリリース予定はございませんので、軽減策・回避策にて対応をお願いいたします。 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ルータ、ファイアウォール等の設置や仮想プライベートネットワーク(VPN)の利用などにより、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからのアクセスをファイアウォールでブロックする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

型番	対策及び軽減策・回避策
Q03UDECPU, シリアルの上 5 桁 22081 以前 Q24DHCCPU-V, シリアルの上 5 桁 24031 以前 Q24DHCCPU-VG, シリアルの上 5 桁 24031 以前 QnUDEHCPU (n=04/06/10/13/20/26/50/100), シリアルの上 5 桁 22081 以前 QnUDVCPU(n=03/04/06/13/26), シリアルの上 5 桁 22031 以前 QnUDPVCPU(n=04/06/13/26), シリアルの上 5 桁 22031 以前 LnCPU(-P)(n=02/06/26), シリアルの上 5 桁 22051 以前 L26CPU-(P)BT, シリアルの上 5 桁 22051 以前	<お客様での対応> 軽減策・回避策にて対応をお願いいたします。下記のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできませんので、後継機種であるMELSEC iQ-R シリーズへの移行のご検討もお願いいたします。 <製品での対応> 以下のバージョンで対策しております。 Q03UDECPU, シリアルの上 5 桁 22082 以降 Q24DHCCPU-V, シリアルの上 5 桁 24032 以降 Q24DHCCPU-VG, シリアルの上 5 桁 24032 以降 QnUDEHCPU (n=04/06/10/13/20/26/50/100), シリアルの上 5 桁 22082 以降 QnUDVCPU(n=03/04/06/13/26), シリアルの上 5 桁 22032 以降 QnUDPVCPU(n=04/06/13/26), シリアルの上 5 桁 22032 以降 LnCPU(-P)(n=02/06/26), シリアルの上 5 桁 22052 以降 L26CPU-(P)BT, シリアルの上 5 桁 22052 以降 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
RnCPU(n=00/01/02), Ver. 18 以前	<対策> Ver. 19 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
RnCPU(n=04/08/16/32/120), Ver. 50 以前 RnENCPU(n=04/08/16/32/120), Ver. 50 以前	<対策> Ver. 51 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

型番	対策及び軽減策・回避策
RnSFCPU(n=08/16/32/120), Ver. 22 以前 RnPSFCPU(n=08/16/32/120), Ver. 05 以前	<お客様での対応> 軽減策・回避策にて対応をお願いいたします。下記のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできません。 <製品での対応> 以下のバージョンで対策しております。 ・RnSFCPU(n=08/16/32/120),Ver.23 以降 ・RnPSFCPU(n=08/16/32/120), Ver.06 以降 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
RnPCPU(n=08/16/32/120), Ver. 24 以前	<対策> Ver. 25 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
R12CCPU-V, Ver.13 以前 RD55UP06-V, Ver. 09 以前 RD55UP12-V, Ver. 01	<お客様での対応> 下記バージョンをお使いの方は、以下サイトより次項に記載の対策版をダウンロードしたうえで、アップデートしてください。 https://www.mitsubishielectric.co.jp/fa/download/index.html R12CCPU-V, Ver. 09～13 RD55UP06-V, Ver. 07～09 RD55UP12-V, Ver. 01 R12CCPU-V, Ver. 08 以前または RD55UP06-V, Ver. 06 以前をお使いの方は、軽減策・回避策にて対応をお願いいたします。下記のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできません。 <製品での対応> 以下のバージョンで対策しております。 R12CCPU-V, Ver. 14 以降 RD55UP06-V, Ver. 10 以降 RD55UP12-V, Ver. 02 以降 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

型番	対策及び軽減策・回避策
Q06CCPU-V, 全バージョン	〈お客様での対応〉 対策版のリリースがございませんので、後継機種となります Q12DCCPU-V 又は R12CCPU-V の使用を検討ください。または、軽減策・回避策にて対応をお願いいたします。 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
RJ71GN11-T2, Ver. 11 以前	〈対策〉 Ver. 12 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
RJ71EN71, Ver.48 以前	〈対策〉 Ver. 49 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
RD78Gn(n=4,8,16,32,64), Ver.14 以前 RD78GHV, Ver.14 以前 RD78GHW, Ver14 以前	〈対策〉 Ver. 16 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

型番	対策及び軽減策・回避策
QJ71E71-100, シリアルの上5桁21092以前 LJ71E71-100, シリアルの上5桁21092以前 QJ71MT91, シリアルの上5桁20082以前	<お客様での対応> 軽減策・回避策にて対応をお願いいたします。下記のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできません。 <製品での対応> 以下のバージョンで対策しております。 QJ71E71-100, シリアルの上5 桁 22102 以降 LJ71E71-100, シリアルの上5 桁 22102 以降 QJ71MT91, シリアルの上5 桁 22102 以降 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
QJ71MES96, 全バージョン QJ71WS96, 全バージョン	<お客様での対応> 対策版のリリースおよび後継機種はございませんので、軽減策・回避策にて対応をお願いいたします。 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
FX5U(C)-〇〇M□/△△ [1]製造番号 17X****以降の場合: Ver.1.210 以前 [2]製造番号 179**** 以前の場合: Ver.1.070 以前	<対策> [1]ファームウェアバージョン 1.211 以降で対策しております。 [2]ファームウェアバージョン 1.071 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

型番	対策及び軽減策・回避策
FX5UC-32M□/△△-TS, Ver.1210 以前	<対策> ファームウェアバージョン 1.211 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
FX5UJ-〇〇M□/△△, Ver. 1.000	<対策> ファームウェアバージョン 1.001 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
FX5-ENET, Ver. 1.002 以前 FX5-ENET/IP, Ver. 1.002 以前	<お客様での対応> 軽減策・回避策にて対応をお願いいたします。下記のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできません。 <製品での対応> 以下のバージョンで対策しております。 FX5-ENET, Ver.1.003 以降 FX5-ENET/IP, Ver.1.003 以降 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

型番	対策及び軽減策・回避策
FX5-CCLGN-MS, Ver. 1.000	〈対策〉 ファームウェアバージョン 1.001 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
FX3U-ENET-ADP, Ver. 1.22 以前 FX3U-ENET, Ver. 1.14 以前 FX3U-ENET-L, Ver. 1.14 以前 FX3U-ENET-P502, Ver. 1.14 以前 FX3GE-〇〇M□/△△, シリアルの上 3 桁 20X 以前	〈お客様での対応〉 軽減策・回避策にて対応をお願いいたします。下記のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできませんので、後継機種である iQ-F シリーズ CPU ユニットへの移行のご検討もお願いいたします。 〈製品での対応〉 以下のバージョンで対策しております。 FX3U-ENET-ADP, Ver.1.24 以降 FX3U-ENET, Ver.1.16 以降 FX3U-ENET-L, Ver.1.16 以降 FX3U-ENET-P502, Ver.1.16 以降 FX3GE-〇〇M□/△△, シリアルの上 3 桁 20Y 以降 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
NZ2GACP620-60, Ver.1.03D 以前 NZ2GACP620-300, Ver.1.03D 以前	〈対策〉 サンプルコードバージョン 1.04E 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

●お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、代理店にご相談ください。

[2]【データ収集アナライザ MELQIC】

型番	対策及び軽減策・回避策
IU1-1M20-D, 全バージョン	〈お客様での対応〉 対策版のリリースおよび後継機種はございませんので、軽減策・回避策にて対応をお願いいたします。 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

●お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、代理店にご相談ください。

[3]【テンションコントローラ】

型番	対策及び軽減策・回避策
LE7-40GU-L, 画面パッケージデータ V1.01 以前	〈対策〉 画面パッケージデータ V1.02 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、画面パッケージデータをアップデートしてください。 https://www.mitsubishielectric.co.jp/fa/download/index.html 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

●お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、代理店にご相談ください。

[4]【表示器 GOT】

型番	対策及び軽減策・回避策
GOT1000 シリーズ GT14 モデル, 全バージョン	〈お客様での対応〉 対策版のリリースがございませんので、後継機種となります GT2505(HS)-VTBD の使用を検討ください。または、軽減策・回避策にて対応をお願いいたします。 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

型番	対策及び軽減策・回避策
GOT2000 シリーズ GT21 モデル, Ver 01.44.000 以前 GS シリーズ GS21 モデル, Ver 01.44.000 以前	<対策> 基本システムアプリケーションのバージョン 01.45.000 以降で対策しております。 GT Designer3 Version1(GOT2000) Ver.1.275M 以降に同梱されています。 以下サイトより、上記バージョンの GT Designer3 Version1(GOT2000)をダウンロードしたうえで、基本システムアプリケーションをアップデートしてください。 https://www.mitsubishielectric.co.jp/fa/download/index.html <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
GT25-J71GN13-T2, Ver.03 以前	<対策> Ver. 04 以降で対策しております。 以下サイトより対策版をダウンロードしたうえで、アップデートください。 https://www.mitsubishielectric.co.jp/fa/download/index.html <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

●お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、代理店にご相談ください。

[5]【インバータ FREQROL】

型番	対策及び軽減策・回避策
FR-A800-E シリーズ，発売開始から2020 年 12 月生産分 FR-F800-E シリーズ，発売開始から2020 年 12 月生産分	<お客様での対応> 軽減策・回避策にて対応をお願いいたします。下記のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできません。 <製品での対応> 2021 年 1 月生産分以降で対策しております。 <製品の識別方法> インバータ本体の定格名板、もしくは梱包箱の梱包名板内に記載した製造番号（SERIAL）の、左から 2 文字目が製造年(西暦の末尾 1 桁)、3 文字目が製造月(1～9、X(10 月)、Y(11 月)、Z(12 月))を表します。 【対策済み製品の製造番号（SERIAL）例】 □11○○○○○○：2021 年 1 月製 □12○○○○○○：2021 年 2 月製 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。（例：鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付） ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。
FR-A8NCG，発売開始から 2020 年 8 月生産分	<お客様での対応> 軽減策・回避策にて対応をお願いいたします。下記のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできません。 <製品での対応> 2020 年 9 月生産分以降で対策しております。 <製品の識別方法> インバータ本体の定格名板、もしくは梱包箱の梱包名板内に記載した製造番号（SERIAL）の、左から 2 文字目が製造年(西暦の末尾 1 桁)、3 文字目が製造月(1～9、X(10 月)、Y(11 月)、Z(12 月))を表します。 【対策済み製品の製造番号（SERIAL）例】 □09○○○：2020 年 9 月製 □0X○○○：2020 年 10 月製 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。（例：鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付） ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

型番	対策及び軽減策・回避策
FR-E800-EPA シリーズ，発売開始から 2020 年 7 月生産分 FR-E800-EPB シリーズ，発売開始から 2020 年 7 月生産分	<お客様での対応> 軽減策・回避策にて対応をお願いいたします。下記のとおり対策済み製品をリリースしておりますが、対策版へのアップデートはできません。 <製品での対応> 2020 年 8 月生産分以降で対策しております。 <製品の識別方法> インバータ本体の定格名板、もしくは梱包箱の梱包名板内に記載した製造番号(SERIAL)の、左から 3,4 文字目が製造年(西暦の末尾 2 桁)、5 文字目が製造月(1～9、X(10 月)、Y(11 月)、Z(12 月))を表します。 【対策済み製品の製造番号(SERIAL)例】 □□208○○○○○○:2020 年 8 月製 □□209○○○○○○:2020 年 9 月製 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

●お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、代理店にご相談ください。

[6]【ロボット MELFA】

型番	対策及び軽減策・回避策
コンベアトラッキングアプリケーション APR-nTR3FH/ APR-nTR6FH/ APR-nTR12FH/ APR-nTR20FH(n=1/2)，全バージョン（19 年 4 月生産中止品）	<お客様での対応> 対策版のリリースおよび後継機種はございませんので、軽減策・回避策にて対応をお願いいたします。 <軽減策・回避策> 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

●お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、代理店にご相談ください。

[7]【AC サーボ MELSERVO】

型番	対策及び軽減策・回避策
MR-J4-TM, 全バージョン MR-JE-C, 全バージョン	〈お客様での対応〉 対策版のリリースおよび後継機種はございませんので、軽減策・回避策にて対応をお願いいたします。 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

●お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、代理店にご相談ください。

[8]【三菱省エネデマンド監視サーバ E-Energy】

型番	対策及び軽減策・回避策
MES-DM500, 全バージョン MES-DM1000, 全バージョン	〈お客様での対応〉 対策版のリリースがございませんので、後継機種となります MES3-255B-DM 又は MES3-255C-DM の使用を検討ください。または、軽減策・回避策にて対応をお願いいたします。 〈軽減策・回避策〉 本脆弱性が悪用されることによるリスクを最小限に抑えるため、三菱電機は以下に示す軽減策を講じることを推奨します。 ・当該製品をインターネットに接続する場合には、ファイアウォールや仮想プライベートネットワーク(VPN)等を使用し、不正アクセスを防止する。 ・LAN 内で使用し、信頼できないネットワークやホストからアクセスできないようにする。 ・当該製品が接続されたネットワーク上のネットワーク機器への物理的なアクセスを制限する。(例:鍵付きキャビネットへの格納、不使用 Ethernet ポートへのシール貼付) ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載する。

●お客様からのお問い合わせ先
製品をご購入いただいた当社の支社、代理店にご相談ください。

[9]【バス乾燥・暖房・換気システム】

型番	対策及び軽減策・回避策
V-141BZ-HM-SL V-141BZ-HM-YH V-141BZ-HM-SYH V-143BZL-HM V-143BZL2-HM V-243BZL-HM V-243BZL2-HM	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・インターネットからの不正アクセスを困難とし、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 有線 LAN の設定についてはルーターメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

型番	対策及び軽減策・回避策
V-241BZ-RC 上記型番の無線 LAN アダプターのソフトウェアバージョン Ver0.47 以前	＜対策＞ 無線 LAN アダプターのソフトウェアバージョン Ver0.48 以降で対策しております。「MyMU」アプリ、または「バスカラット REMOTE」アプリより対策版にアップデートください。 MyMU をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「MyMU」アプリの「登録機器」にある「アダプター情報」から行ってください。詳細は以下サイトにある無線 LAN アダプターのソフトウェア更新方法（取扱説明書・別冊）をご覧ください。 https://www.mitsubishielectric.co.jp/home/mymu/entry_ib2.html バスカラット REMOTE をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「バスカラット REMOTE」アプリの「機器情報」にある「アダプターソフトウエアバージョン」から行ってください。詳細は以下サイトにあるバスカラット REMOTE 取扱説明書をご覧ください。 https://www.mitsubishielectric.co.jp/ldg/ja/air/products/ventilationfan/bath/IB/pdf/bathkaratremote.pdf ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなど、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定についてはルーターメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[10]【ダクト用換気扇】

型番	対策及び軽減策・回避策
V-18ZMVC2-HM V-18ZMVC3-HM V-150CRL-D-HM VD-15ZFVC2-HM VD-15ZFVC3-HM VD-15ZFVC5-HM VD-18ZFVC2-HM VD-18ZFVC3-HM VD-18ZFVC5-HM	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・インターネットからの不正アクセスを困難とし、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 有線 LAN の設定についてはルーターメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[11]【レンジフードファン】

型番	対策及び軽減策・回避策
V-6047S-HM V-754S-HM V-904S-HM	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・インターネットからの不正アクセスを困難とし、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 有線 LAN の設定についてはルーターメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[12]【ロスナイセントラル換気システム】

型番	対策及び軽減策・回避策
VL-11ZFHV-HM VL-20ZMH3-L-HM VL-20ZMH3-R-HM	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・インターネットからの不正アクセスを困難とし、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 有線 LAN の設定についてはルーターメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[13]【太陽光発電システム　カラーモニター　エコガイド】

型番	対策及び軽減策・回避策
PV-DR006L-SET-Y PV-DR006L-IFU-GW-Y	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・インターネットに接続する場合、計測ユニットは据付工事説明書に従い、製品に同梱の情報収集ユニットに接続してご使用下さい。エコガイドでは、悪意のある攻撃者に対して、情報収集ユニットが本脆弱性の影響を軽減します。 情報収集ユニットより上流のルーターなどの機器については、下段共通項目をご参照ください。
PV-DR006L-IFU-MRC-Y	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・本製品はインターネット経由の攻撃の影響を受けることはありません。ただし、当社指定の情報収集ユニットを追加購入してインターネットに接続する場合は、計測ユニットは据付工事説明書に従い、情報収集ユニットに接続してご使用下さい。エコガイドでは、悪意のある攻撃者に対して、本脆弱性の影響を軽減します。 （当社指定以外の HEMS ユニット、市販のルーターなどには直接接続をしないでください。） 情報収集ユニットより上流のルーターなどの機器については、下段共通項目をご参照ください。

型番	対策及び軽減策・回避策
上記 3 機種の共通項目	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ■情報収集ユニットを接続しているルーターが有線の場合は以下をご確認ください。 ・インターネットからの不正アクセスを困難とし、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 有線 LAN の設定についてはルーターメーカーにお問い合わせください。 ■情報収集ユニットに無線 LAN イーサネットコンバータを接続して無線 LAN でご使用の場合は以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなど、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定についてはルーターメーカーにお問い合わせください。 ■パソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[14]【エネルギー計測ユニット】

型番	対策及び軽減策・回避策
HM-EM02 HM-EM03-E	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・エネルギー計測ユニットをインターネットに接続される場合は、直接ルーターへは接続せず、情報収集ユニットを介して接続ください。HM-EM02 は情報収集ユニット HM－GW02 に接続し、HM-EM03-E は情報収集ユニット HM-GW03 に接続してください。 ・インターネットからの不正アクセスを困難とし、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 有線 LAN の設定についてはルーターメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[15]【ルームエアコン】

型番	対策及び軽減策・回避策
MSZ-FZ4020S/5620S/6320S/7120S/8020S/9020S MSZ-ZW2220/2520/2820(S)/3620(S)/4020S/5620S/6320S/7120S/8020S/9020S MSZ-FZV4020S/5620S/6320S/7120S/8020S/9020S MSZ-ZXV2220/2520/2820(S)/3620(S)/4020S/5620S/6320S/7120S/8020S/9020S MSZ-EM2220/2520/2820/3620/4020/5620/6320/7120/8020/9020E8(S) 上記型番の無線 LAN ソフトウェアバージョン Ver30.00 あるいは Ver31.00	＜対策＞ 無線 LAN ソフトウェア Ver32.00 以降で対策しております。 「霧ヶ峰 REMOTE」アプリより対策版にアップデートください。 ソフトウェアのバージョン確認およびアップデートは、「霧ヶ峰 REMOTE」アプリの「エアコン管理」-「(部屋名称)」にある「無線 LAN ソフト更新」から行ってください。 詳細は以下サイトにある霧ヶ峰 REMOTE 取扱説明書をご覧ください。 https://www.mitsubishielectric.co.jp/home/kirigamine/function/remote/ib.html ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなど、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定についてはルーターメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先

三菱電機お客さま相談センター　0120-139-365(無料)　携帯・PHS　0570-077-365(有料)

フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[16]【HEMS 対応アダプター、LAN アダプター】

型番	対策及び軽減策・回避策
GT-HEM4 上記型番の製造番号 0****** (7 桁の数字の先頭の一桁目が“0”) GT-RA1 GT-RA2 上記型番のアダプターソフトウェアバージョン 00.45 以前	＜対策＞ GT-RA1、GT-RA2 については、アダプターソフトウェアバージョン 00.46 以降で対策しております。 「MyMU」アプリ、または「DIAHOT REMOTE」アプリより対策版にアップデートください。 MyMU をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「MyMU」アプリの「登録機器」にある「アダプター情報」から行ってください。詳細は以下サイトにある無線 LAN アダプターのソフトウェア更新方法（取扱説明書・別冊）をご覧ください。 https://www.mitsubishielectric.co.jp/home/mymu/entry_ib2.html DIAHOT REMOTE をご使用の方 ソフトウェアのバージョン確認およびアップデートは、「DAHOT REMOTE」アプリの「機器情報」にある「アダプターソフトウェアバージョン」から行ってください。詳細は以下サイトにある DIAHOT REMOTE 取扱説明書をご覧ください。 https://www.mitsubishielectric.co.jp/home/ecocute/function/remote/ib.html 対策ソフトウェアが無い機種については、軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ 無線ルーターの設定について、以下をご確認ください。 ・無線 LAN の暗号キーは、数字の連番や MAC アドレスなどから推測できる設定を避けて、文字と数字を複合した推測されにくい安全なパスワードをご使用ください。 ・無線 LAN の暗号方式は WEP あるいは Open を使用しないでください。 ・インターネットからの不正アクセスを防止するため、PING 応答を無効に設定するなど、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 無線 LAN の設定についてはルーターメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。
GT-HEM3-E GT-HEM4-E MAC-894IF	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・インターネットからの不正アクセスを困難とし、インターネット上での存在が特定されないようにしてください。 ・管理画面へのログインパスワードを推測されにくいものに変更ください。 有線 LAN の設定についてはルーターメーカーにお問い合わせください。 自宅でパソコンやタブレット等を使用の場合は、以下をご確認ください。 ・ウイルス対策ソフトを最新版にアップデートしてご使用ください。 ・信頼できない発信元や出処が不明な添付ファイルやハイパーリンクは開かないように注意してください。

●お客様からのお問い合わせ先
三菱電機お客さま相談センター　0120-139-365(無料)　携帯・PHS　0570-077-365(有料)
フリーダイヤル，ナビダイヤルをご利用いただけない場合　03-3414-9655(有料)

[17]【空調管理システム / 集中コントローラー】

型番	対策及び軽減策・回避策
G-50 全バージョン G-50-W 全バージョン GB-50 全バージョン G-150AD 全バージョン GB-50AD 全バージョン	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・インターネット等の外部と接続する場合は、VPN ルーター等を使用し、セキュリティを確保した環境でご使用ください。 ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載してください。 ・該当製品へのアクセスを、信頼できるネットワークやホストからのアクセスに制限してください。

●お客様からのお問い合わせ先
三菱電機冷熱相談センター 0037-80-2224(無料) 携帯・IP 電話 073-427-2224(有料)

[18]【空調管理システム / 拡張コントローラー】

型番	対策及び軽減策・回避策
PAC-YG50EC 全バージョン	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・インターネット等の外部と接続する場合は、VPN ルーター等を使用し、セキュリティを確保した環境でご使用ください。 ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載してください。 ・該当製品へのアクセスを、信頼できるネットワークやホストからのアクセスに制限してください。

●お客様からのお問い合わせ先
三菱電機冷熱相談センター 0037-80-2224(無料) 携帯・IP 電話 073-427-2224(有料)

[19]【空調管理システム / BM アダプター】

型番	対策及び軽減策・回避策
PAC-YW01BAC 全バージョン PAC-YW51BAC 全バージョン	＜対策＞ 軽減策・回避策を実施されることを推奨いたします。 ＜軽減策・回避策＞ ・インターネット等の外部と接続する場合は、VPN ルーター等を使用し、セキュリティを確保した環境でご使用ください。 ・該当製品へアクセス可能なパソコンにウイルス対策ソフトを搭載してください。 ・該当製品へのアクセスを、信頼できるネットワークやホストからのアクセスに制限してください。

●お客様からのお問い合わせ先
三菱電機冷熱相談センター 0037-80-2224(無料) 携帯・IP 電話 073-427-2224(有料)

■謝辞

この問題をご報告いただいた Trend Micro 社の Zero Day Initiative と連携する Trend Micro 社 TXOne IoT/ICS Security Research Labs Ta-Lun Yen 様に感謝いたします。

■更新履歴

2024 年 6 月 13 日
影響を受ける製品において下記の製品の＜軽減策・回避策＞を更新
[1]【シーケンサ MELSEC】全製品
[2]【データ収集アナライザ MELQIC】全製品
[3]【テンションコントローラ】全製品
[4]【表示器 GOT】全製品
[5]【インバータ FREQROL】全製品
[6]【ロボット MELFA】全製品
[7]【AC サーボ MELSERVO】全製品
[8]【三菱省エネデマンド監視サーバ E-Energy】全製品

影響を受ける製品において、下記の製品の＜対策＞を＜お客様での対応＞及び＜製品での対応＞に見直し
[1]【シーケンサ MELSEC】NZ2FT-MT、NZ2FT-EIP、Q03UDECPU、Q24DHCCPU-V、Q24DHCCPU-VG、
QnUDEHCPU (n=04/06/10/13/20/26/50/100)、QnUDVCPU(n=03/04/06/13/26)、
QnUDPVCPU(n=04/06/13/26)、LnCPU(-P)(n=02/06/26)、L26CPU-(P)BT、

RnSFCPU(n=08/16/32/120)、RnPSFCPU(n=08/16/32/120)、R12CCPU-V、RD55UP06-V、
RD55UP12-V、Q06CCPU-V、QJ71E71-100、LJ71E71-100、QJ71MT91、QJ71MES96、
QJ71WS96、FX5-ENET、FX5-ENET/IP、FX5-CCLGN-MS、FX3U-ENET-ADP、
FX3U-ENET、FX3U-ENET-L、FX3U-ENET-P502、FX3GE-〇〇M□/△△

[2]【データ収集アナライザ MELQIC】IU1-1M20-D
[4]【表示器 GOT】GOT1000 シリーズ GT14 モデル
[5]【インバータ FREQROL】FR-A800-E シリーズ、FR-F800-E シリーズ、FR-A8NCG、FR-E800-EPA シリーズ、
FR-E800-EPB シリーズ
[6]【ロボット MELFA】コンベアトラッキングアプリケーション APR-nTR3FH/ APR-nTR6FH/ APR-nTR12FH/
APR-nTR20FH(n=1/2)
[7]【AC サーボ MELSERVO】MR-J4-TM、MR-JE-C
[8]【三菱省エネデマンド監視サーバ E-Energy】MES-DM500、MES-DM1000

2023 年 6 月 29 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
[1]【シーケンサ MELSEC】 Q06CCPU-V、QJ71MES96、QJ71WS96
[2]【データ収集アナライザ MELQIC】 IU1-1M20-D
[4]【表示器 GOT】GOT1000 シリーズ GT14 モデル
[6]【ロボット MELFA】コンベアトラッキングアプリケーション
[7]【AC サーボ MELSERVO】MR-J4-TM、MR-JE-C

2022 年 9 月 22 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
[3]【テンションコントローラ】 LE7-40GU-L

2022 年 5 月 24 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
[1]【シーケンサ MELSEC】 Q24DHCCPU-V、Q24DHCCPU-VG
[4]【表示器 GOT】 GOT2000 シリーズ GT21 モデル、GS シリーズ GS21 モデル

2021 年 8 月 24 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
[1]【シーケンサ MELSEC】RD78Gn(n=4,8,16,32,64)、RD78GHV、RD78GHW

2021 年 5 月 18 日
影響を受ける製品において、下記の製品の対策方法の情報を追加
[1]【シーケンサ MELSEC】RJ71EN71、QJ71E71-100、LJ71E71-100、QJ71MT91、NZ2GACP620-60、NZ2GACP620-300
[4]【表示器 GOT】GT25-J71GN13-T2

2021 年 02 月 18 日
影響を受ける製品において、下記の製品のバージョン情報や対策方法の情報を追加
[9]【バス乾燥・暖房・換気システム】V-241BZ-RC
[15]【ルームエアコン】MSZ-FZ4020S/5620S/6320S/7120S/8020S/9020S、MSZ-ZW2220/2520/2820(S)/3620(S)/4020S/
5620S/6320S/7120S/8020S/9020S、MSZ-FZV4020S/5620S/6320S/7120S/8020S/9020S、MSZ-ZXV2220/2520/2820(S)/
3620(S)/4020S/5620S/6320S/7120S/8020S/9020S、MSZ-EM2220/2520/2820/3620/4020/5620/6320/7120/8020/
9020E8(S)
[16]【HEMS 対応アダプター、LAN アダプター】GT-HEM4、GT-RA1、GT-RA2

2021 年 01 月 26 日
影響を受ける製品を追加 ([16])
影響を受ける製品において、下記の製品の対策方法の情報を追加
[1]【シーケンサ MELSEC】R12CCPU-V、RD55UP06-V、RD55UP12-V、RJ71GN11-T2、Q03UDECPU、QnUDEHCPU、
QnUDVCPU、QnUDPVCPU、LnCPU(-P)、L26CPU-(P)BT、RnSFCPU、RnPCPU、RnPSFCPU、FX5-ENET、FX5-ENET/IP、
FX3U-ENET-ADP、FX3GE-〇〇M□/△△、FX3U-ENET、FX3U-ENET-L、FX3U-ENET-P502 および FX5-CCLGN-MS
[5]【インバータ FREQROL】FR-A800-E シリーズ、FR-F800-E シリーズ、FR-A8NCG、FR-E800-EPA シリーズおよび FR-
E800-EPB シリーズ

2020 年 09 月 24 日
影響を受ける製品を追加 ([9]～[19])