空調管理システムの暗号化通信における情報漏えい、改ざんおよびサービス拒否（DoS）の脆弱性

公開日 2022 年 6 月 7 日
三菱電機株式会社

■概要

三菱電機製の空調管理システムの暗号化通信において、複数の情報漏えい、改ざんおよびサービス拒否（DoS）の脆弱性が存在することが判明しました。これら脆弱性を悪用された場合、攻撃者が暗号化された通信伝文を盗聴することにより、当該機器の一部の情報が漏えいする可能性があります（CVE-2022-24296、CVE-2016-2183、CVE-2013-2566、CVE-2015-2808）。また、攻撃者は、中間者攻撃により、暗号化された通信伝文に不正なメッセージを挿入したり、対象をサービス停止(DoS)状態に陥らせることができる可能性があります。（CVE-2009-3555）。

三菱電機製の空調管理システムにおいては、後述の「■脆弱性の説明」にて記載のシステム構成例 1、2 のように、ビル内ネットワークでご使用、もしくは、VPN ルータなどでセキュリティを確保された構成でのご使用を前提としております。ご使用中のシステムが、当社の推奨する適切な構成となっていることをご確認いただけますよう、お願いいたします。

■CVSS スコア

CVE-2022-24296 CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N 基本値: 3.1
CVE-2016-2183 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値: 7.5
CVE-2013-2566 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値 5.9
CVE-2015-2808 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N 基本値 5.9
CVE-2009-3555 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H 基本値 7.4

■該当製品の確認方法

＜製品とバージョン＞

表の見方・・・〇：該当、×：非該当

型番	バージョン	CVE-2022-24296	CVE-2016-2183	CVE-2013-2566	CVE-2015-2808	CVE-2009-3555
G-150AD	Ver.3.21 以前のバージョン	〇	〇	〇	〇	〇
AG-150A-A	Ver.3.21 以前のバージョン	〇	〇	〇	〇	〇
AG-150A-J	Ver.3.21 以前のバージョン	〇	〇	〇	〇	〇
GB-50AD	Ver.3.21 以前のバージョン	〇	〇	〇	〇	〇
GB-50ADA-A	Ver.3.21 以前のバージョン	〇	〇	〇	〇	〇
GB-50ADA-J	Ver.3.21 以前のバージョン	〇	〇	〇	〇	〇
EB-50GU-A	Ver.7.10 以前のバージョン	〇	〇	〇	〇	×
EB-50GU-J	Ver.7.10 以前のバージョン	〇	〇	〇	〇	×
AE-200J	Ver.7.97 以前のバージョン	〇	〇	×	×	×
AE-200A	Ver.7.97 以前のバージョン	〇	〇	×	×	×
AE-200E	Ver.7.97 以前のバージョン	〇	〇	×	×	×
AE-50J	Ver.7.97 以前のバージョン	〇	〇	×	×	×
AE-50A	Ver.7.97 以前のバージョン	〇	〇	×	×	×
AE-50E	Ver.7.97 以前のバージョン	〇	〇	×	×	×
EW-50J	Ver.7.97 以前のバージョン	〇	〇	×	×	×
EW-50A	Ver.7.97 以前のバージョン	〇	〇	×	×	×
EW-50E	Ver.7.97 以前のバージョン	〇	〇	×	×	×
TE-200A	Ver.7.97 以前のバージョン	〇	〇	×	×	×
TE-50A	Ver.7.97 以前のバージョン	〇	〇	×	×	×
TW-50A	Ver.7.97 以前のバージョン	〇	〇	×	×	×

＜バージョン確認方法＞

・G-150AD、AG-150A-A、AG-150A-J、GB-50AD、GB-50ADA-A、GB-50ADA-J、EB-50GU-A、EB-50GU-J の場合
WEB 画面のログイン画面にて「オプション機能のライセンス登録」を選択すると、バージョンを確認できます（図 1 参照）。

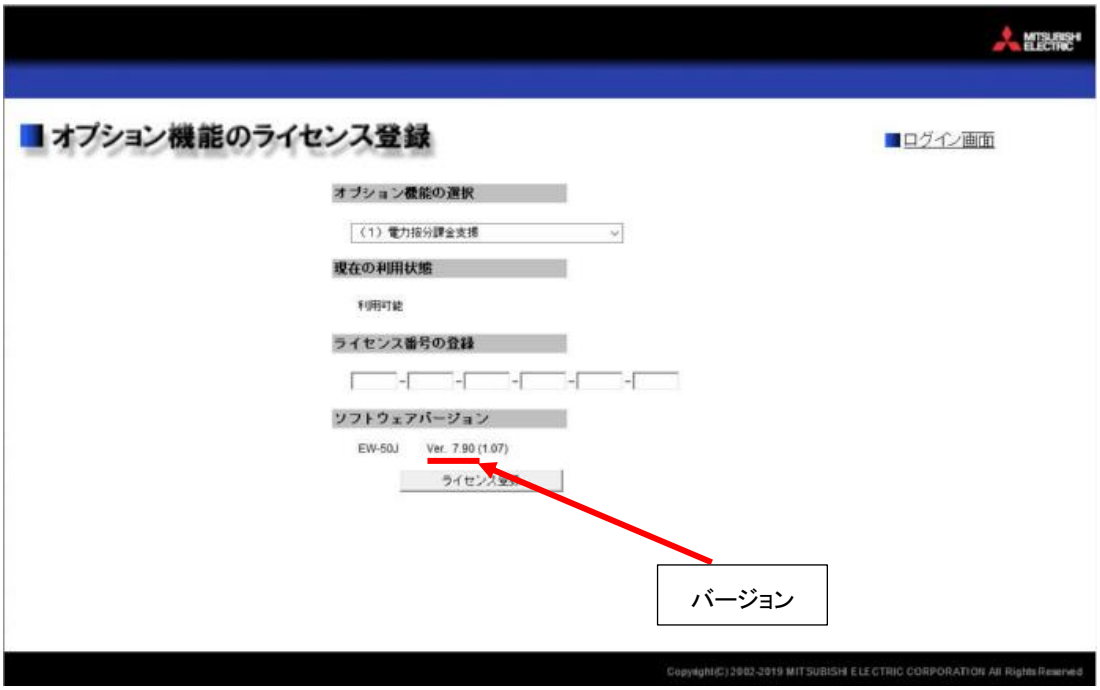

図 1　バージョン確認方法

（G-150AD、AG-150A-A、AG-150A-J、GB-50AD、GB-50ADA-A、GB-50ADA-J、EB-50GU-A、EB-50GU-J の場合）

・AE-200J、AE-200A、AE-200E、AE-50J、AE-50A、AE-50E、EW-50J、EW-50A、EW-50E、TE-200A、TE-50A、TW-50A の場合
WEB 画面にて、管理者アカウントでログイン後、ホーム画面の設定タブよりライセンス登録の画面を選択すると、バージョンを確認できます（図 2 参照）。

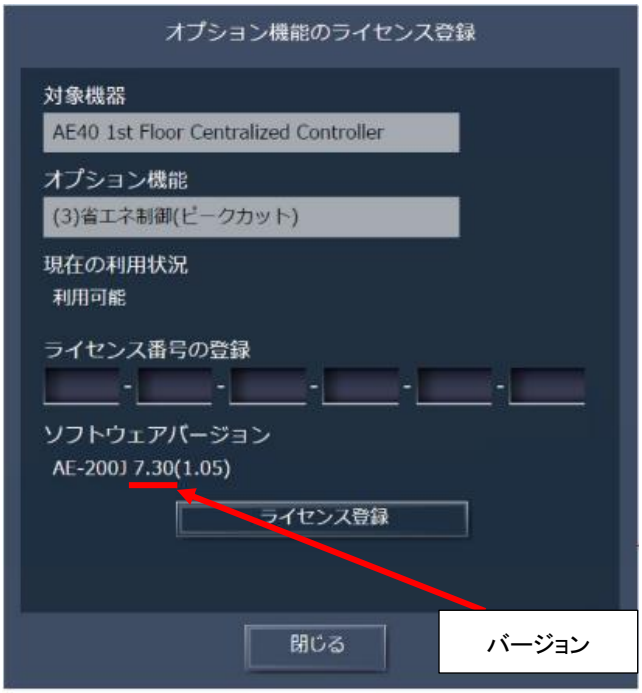

図 2　バージョン確認方法

（AE-200J、AE-200A、AE-200E、AE-50J、AE-50A、AE-50E、EW-50J、EW-50A、EW-50E、TE-200A、TE-50A、TW-50A の場合）

・G-150AD、AG-150A-A、AG-150A-J、AE-200J、AE-200A、AE-200E、AE-50J、AE-50A、AE-50E、TE-200A、TE-50A の本体画面からのバージョン確認方法

通常画面の右上の設定変更  をタッチしてログイン画面を表示しますと、バージョンを確認できます（図 3 参照）。

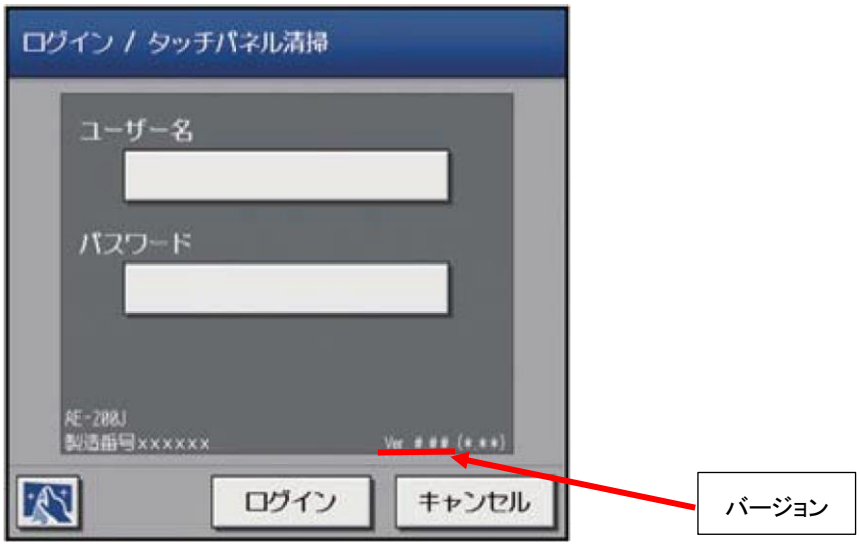

図 3 バージョン確認方法

（G-150AD、AG-150A-A、AG-150A-J、AE-200J、AE-200A、AE-200E、AE-50J、AE-50A、AE-50E、TE-200A、TE-50A の本体画面の場合）

■脆弱性の説明

三菱電機製の空調管理システムの暗号化通信において、以下の複数の情報漏えいの脆弱性（CVE-2022-24296、CVE-2016-2183、CVE-2013-2566、CVE-2015-2808）および情報の改ざん、サービス拒否（DoS）の脆弱性（CVE-2009-3555）が存在します。

・CVE-2022-24296：不完全、または危険な暗号アルゴリズムの使用（CWE-327）
・CVE-2016-2183：情報漏えい（CWE-200）
・CVE-2013-2566：不完全、または危険な暗号アルゴリズムの使用（CWE-327）
・CVE-2015-2808：不完全、または危険な暗号アルゴリズムの使用（CWE-327）
・CVE-2009-3555：中間者攻撃問題（CWE-300）

システム構成例 1 や 2 の場合、外部の第三者がインターネットから悪用を試みても、これら脆弱性への攻撃は成功しません。

システム構成例 3 の場合、外部の第三者がインターネットから悪用を試みるとこれら脆弱性への攻撃が成功する可能性がございますので、VPN ルータ等、当社が推奨する適切な環境でご使用ください。

システム構成例 1 空調管理システムをビル内のネットワークで使用している構成（図 4 参照）

図 4 システム構成例 1

システム構成例 2 空調管理システムが VPN ルータを介してビル外の PC がアクセス可能な構成（図 5 参照）

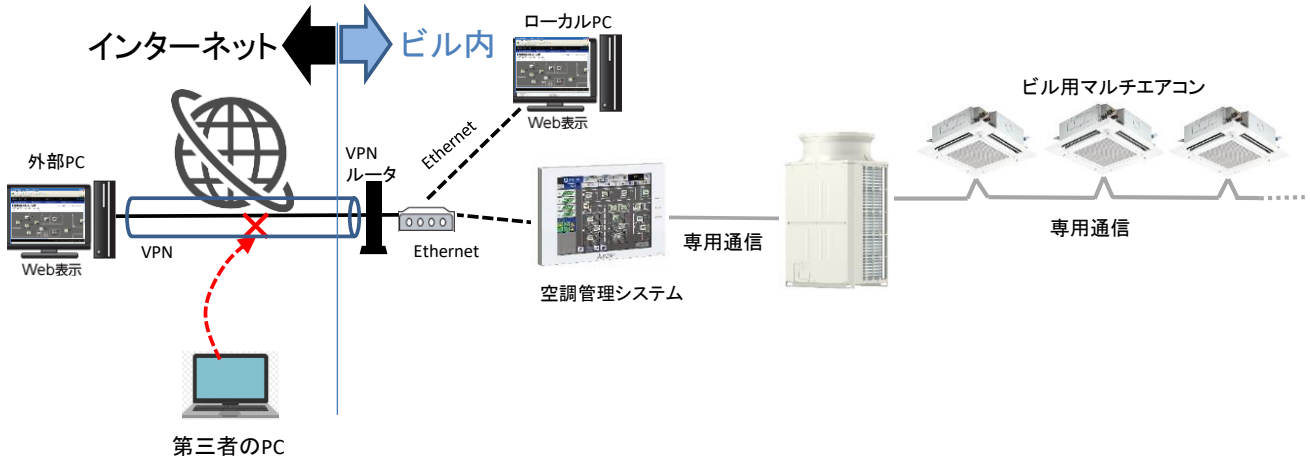

図 5 システム構成例 2

システム構成例 3 空調管理システムが VPN 無しでビル外の PC がアクセス可能な構成（不適切な構成、図 6 参照）

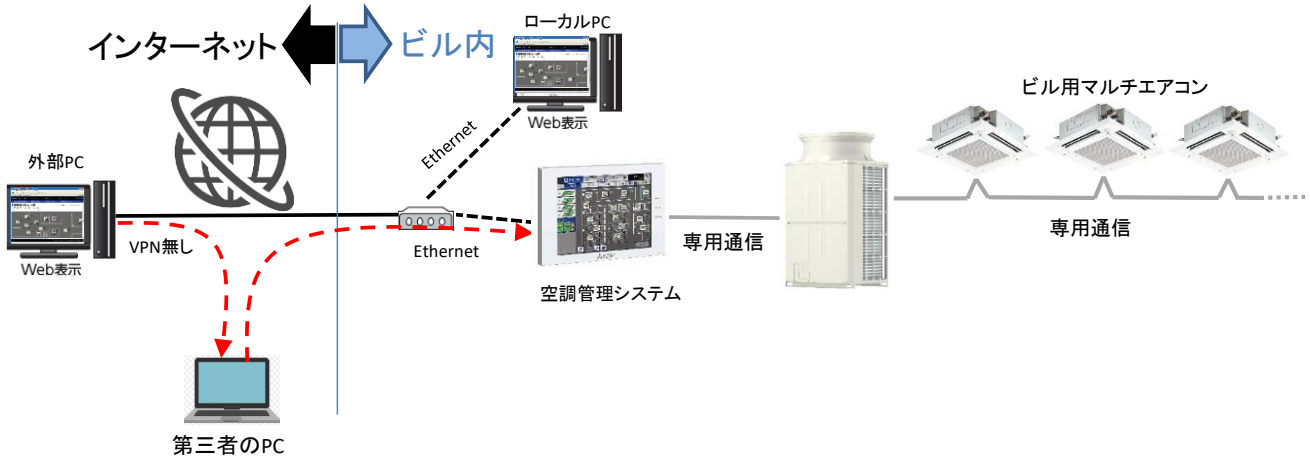

図 6 システム構成例 3

■脆弱性がもたらす脅威

これら脆弱性を攻撃者に悪用された場合、当該機器との通信情報の一部が漏えいしたり、改ざんされたり、対象が DoS 状態に陥る可能性があります。

■対策方法

各製品の対策済のバージョンは以下の通りです。

＜製品とバージョン＞

型番	バージョン
G-150AD	AE-200J、AE-50J、EW-50J Ver.7.98 以降へ機器を更新してください。
AG-150A-A	AE-200A、AE-50A、EW-50A Ver.7.98 以降へ機器を更新してください。
AG-150A-J	AE-200E、AE-50E、EW-50E Ver.7.98 以降へ機器を更新してください。
GB-50AD	AE-200J、AE-50J、EW-50J Ver.7.98 以降へ機器を更新してください。
GB-50ADA-A	AE-200A、AE-50A、EW-50A Ver.7.98 以降へ機器を更新してください。
GB-50ADA-J	AE-200E、AE-50E、EW-50E Ver.7.98 以降へ機器を更新してください。
EB-50GU-A	Ver.7.11 以降のバージョン
EB-50GU-J	Ver.7.11 以降のバージョン
AE-200J	Ver.7.98 以降のバージョン
AE-200A	Ver.7.98 以降のバージョン
AE-200E	Ver.7.98 以降のバージョン
AE-50J	Ver.7.98 以降のバージョン
AE-50A	Ver.7.98 以降のバージョン
AE-50E	Ver.7.98 以降のバージョン
EW-50J	Ver.7.98 以降のバージョン
EW-50A	Ver.7.98 以降のバージョン
EW-50E	Ver.7.98 以降のバージョン
TE-200A	Ver.7.98 以降のバージョン
TE-50A	Ver.7.98 以降のバージョン
TW-50A	Ver.7.98 以降のバージョン

＜アップデート方法＞

ご購入いただいた販売代理店にお問合せください。ご不明点がございましたら、下記の三菱電機冷熱相談センターにお問い合わせください。

また、ファームウェアをアップデートするとともに、使用しているパソコンの OS とブラウザを最新にしてください。パソコンの OS やブラウザが古い場合、もしくはセキュリティ設定を変更している場合、製品アップデート後に以下のような画面(図 7)が表示され、接続できなくなる可能性がございます。

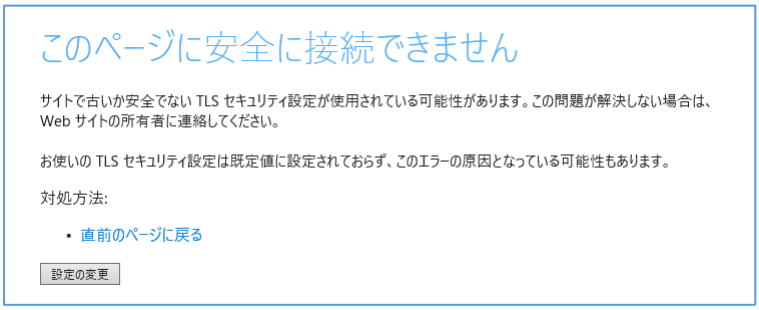

図 7 ブラウザ画面におけるエラー例

■回避策

これらの脆弱性が悪用されることによるリスクを回避するため、当社が推奨する適切な環境でご使用ください。また、以下に示す回避策を講じることを推奨します。

・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。
・アクセス元のパソコンの OS や WEB ブラウザを最新のバージョンに更新し、ウイルス対策ソフトを搭載してください。

■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 TEL 0037-80-2224(携帯電話・PHS の場合 TEL 073-427-2224)