MITSUBISHI ELECTRIC
Changes for the Better

NEWS RELEASE

（経営 No.2005）

2020 年 2 月 12 日
三菱電機株式会社

不正アクセスによる個人情報と企業機密の流出可能性について（第 3 報）

三菱電機株式会社は、1 月 20 日に公表した不正アクセス事案（「不正アクセスによる個人情報と企業機密の流出可能性について」）について、攻撃を受けた可能性のあるすべての端末を精査する中で、流出可能性のあるファイルとして、防衛省の指定した「注意情報」があることを 2 月 7 日に発見し、同日、防衛省に報告の上、2 月 10 日に第 2 報として公表いたしました。当社の調査が完全でなく、国の防衛に関わる情報が流出した可能性があるという事態を引き起こし、深く反省しております。防衛省をはじめ、皆さまにご迷惑とご心配をおかけしていることを、深くお詫び申し上げます。

以下に 2 月 10 日に公表した第 2 報についてあらためてご報告するとともに、サイバーセキュリティーに資する情報の共有を図るべく、攻撃手法や当社での検証プロセスなどを、合わせてお知らせします。

電力・鉄道などの社会インフラに関する機微な情報、機密性の高い技術情報や取引先との契約で定められた重要な情報は、攻撃を受けた可能性のあるすべての端末からアクセス可能な範囲に含まれておらず、流出していないことを再確認しました。
現在、1 月 20 日に公表した個人情報が流出した可能性のある方々へのご報告を終え、流出した可能性のある企業機密に関係するお客様への一次報告も終えております。

該当の方々や関係するお客様に多大なるご迷惑とご心配をおかけしていることを、あらためてお詫び申し上げます。また、当社が端末の不審な挙動を認識してから公表に至るまで、半年以上を要したことを反省いたします。

当社グループ全体の情報セキュリティー体制強化に向け、迅速な判断とインシデント発生時のお客様や関係機関との早期情報共有等を目的に、情報セキュリティー全般の企画・構築・運営の機能を一元的に担う社長直轄の統括組織を 2020 年 4 月 1 日付にて新設する予定です。

当社は、今回の事案を教訓として、社会全体のセキュリティーレベル向上に貢献してまいります。

流出した可能性のある防衛省が指定した「注意情報」について

攻撃を受けた可能性のある端末のフォレンジック調査結果から流出可能性のあるファイルを抽出し、調査作業を進めてまいりましたが、防衛省への詳細報告を準備する中で、アクセス可能範囲を再精査したところ調査範囲が拡大し、流出可能性のある情報として、防衛省の指定した「注意情報」があることが判明しました。当該情報は、貸与された紙のまま、専用の部屋に保管すべきでした。
今後、調査を継続するとともに、防衛省にご指導いただきながら、保全措置を徹底してまいります。

他の事業もアクセス可能範囲を再精査し、電力・鉄道などの社会インフラに関する機微な情報、機密性の高い技術情報や取引先との契約で定められた重要な情報は流出していないことを再確認しました。

報道関係からのお問い合わせ先	〒100-8310 東京都千代田区丸の内二丁目 7 番 3 号　TEL 03-3218-2332　FAX 03-3218-2431 三菱電機株式会社　広報部

確認された不正アクセスの概要

当社は、米国国立標準技術研究所（NIST）の規格である「サイバーセキュリティーフレームワーク※1」の考え方に則り、当社の事業内容に応じたサイバーセキュリティー対策を講じていましたが、今回の事象は従来の監視や検知をすり抜ける高度かつ巧妙な手法であったため、残念ながら攻撃を完全に防御することはできませんでした。

昨年 6 月 28 日、各端末に導入しているウイルス対策ソフトの挙動検知機能が、不審な挙動を検知し、調査したところ、マルウエア感染が判明したため、感染拡散防止・マルウエア駆除作業などを行いました。マルウエアは、マイクロソフト Windows®の標準機能である PowerShell を使用したファイルレスマルウエアで、当社を狙った標的型サイバー攻撃であると考えています。未公開脆弱性情報・マルウエア情報・不正通信先アドレス情報などについては、一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）をはじめとするサイバーセキュリティーの専門機関に報告しました。

なお、感染の疑いのある端末台数は国内外含め 132 台で、そのうち個人情報やお客様への報告が必要と思われる重要情報に関わる端末は国内 9 台です。海外拠点の中では、中国の拠点で感染の疑いのある端末が確認されています。当該端末からアクセス可能な範囲には、機密性の高い技術情報や取引先との契約で定められている重要な情報は含まれておらず、流出していないことを確認しておりますが、お客様に報告すべき内容の有無を精査しているところです。他の海外地域の拠点については本件に関わる攻撃を受けていないことを確認済みです。

※1　重要インフラのサイバーセキュリティー対策を改善するためのフレームワーク

1. 当社のセキュリティー対策

これまで当社では「サイバーセキュリティーフレームワーク」の考え方に則り、当社の事業内容に応じたサイバーセキュリティー対策を講じています。情報システム環境の多層防御機能として標的型メールの挙動検知をはじめ、インターネット出入口の制御・監視、社内ネットワーク内アクセス制御、パッチ管理を含むサーバー・端末のグローバルでの構成一元管理などを実装し、インシデント発生時の緊急対応体制（MELCO-CSIRT※2）を運用しております。

※2　Mitsubishi Electric Corporation Computer Security Incident Response Team

2. 対応経緯と攻撃手法

＜対応経緯＞

(1) 昨年 6 月 28 日、ウイルス対策ソフトの挙動検知機能が、国内拠点の端末で不審な挙動を検知。
(2) 同年 7 月 8 日、当該端末で不審な挙動として検出されたファイルは Windows®標準プログラム（以下、PowerShell）のファイル名をウェブブラウザソフトの実行ファイル名に書き換えられたもので、ファイルレスマルウエアを実行するための機能として利用されていたことを確認し、不正アクセスと断定。
(3) 同年 7 月 10 日、当社グループの国内外約 24.5 万台の端末とサーバーを共通管理している構成管理ツールで各端末内のプログラム構成を調査したところ、ファイル名を書き換えられた PowerShell が他の複数の端末にも存在することが確認され、国内外の複数拠点にまたがる不正アクセスの可能性が高いと判断。
(4) 同年 7 月 17 日までに、不正な通信先を全て特定して遮断。以降、不正アクセスは確認されておらず、封じ込め完了と判断。
(5) 同年 8 月 1 日に、保全が完了した端末から順次、フォレンジック調査を含む詳細な解析を進めるとともに通信とサーバーログ解析との突合調査を 11 月 15 日まで継続し、技術面での発生事象と問題点を洗い出し。
(6) 同年 8 月 29 日に、未公開脆弱性情報・マルウエア情報・不正通信先アドレス情報などを、JPCERT/CC に報告。
(7) 同年 8 月 31 日に、技術面での調査に加えて、情報管理の観点で各端末からアクセス可能なファイルの洗い出しを開始し、フォレンジック調査が完了した端末から順次、流出可能性ファイルの仕分けを実施。

＜攻撃手法＞

昨年 6 月 28 日に不審な挙動を検知してから感染端末や通信ログの調査を行い、判明した攻撃手法について時系列に示します。

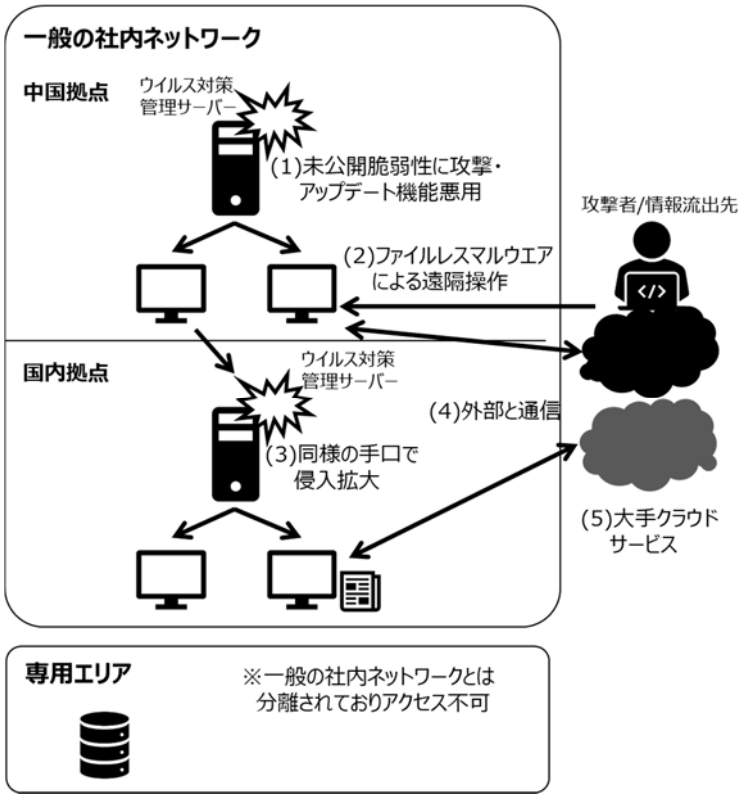
(1) 昨年 3 月 18 日に、当社の中国拠点内ネットワークにあるウイルス対策管理サーバーが、外部から未公開脆弱性を突いたゼロデイ攻撃を受け、パターンファイルアップデート機能を悪用される形で同拠点の端末に侵入が拡大。ウイルス対策管理サーバーへの攻撃者の送信元アドレスが詐称されていることから、攻撃者の特定は難航（調査継続中）。

(2) 同日以降、当該端末のメモリー内で活動するファイルレスマルウエアが PowerShell を用いて実行され、外部からの遠隔操作（攻撃）を確立し、当社の中国内他拠点に感染が拡大。

(3) 同年 4 月 3 日に、攻撃者は中国拠点の端末を介して、日本国内にあるウイルス対策管理サーバーを 3 月 18 日と同じ手口で攻撃し、ファイルレスマルウエアを用いて、国内複数拠点の端末に侵入を拡大。

(4) 同日以降、攻撃者はウイルス対策管理サーバーの機能を悪用し、ウイルス対策クライアントソフトが導入されている国内拠点のサーバーの一部に不正アクセスし、さらに端末に侵入。端末が外部と通信。

(5) これらの攻撃において、攻撃者はファイルレスマルウエア実行のプラットフォームとして、複数の大手クラウドサービスを利用。

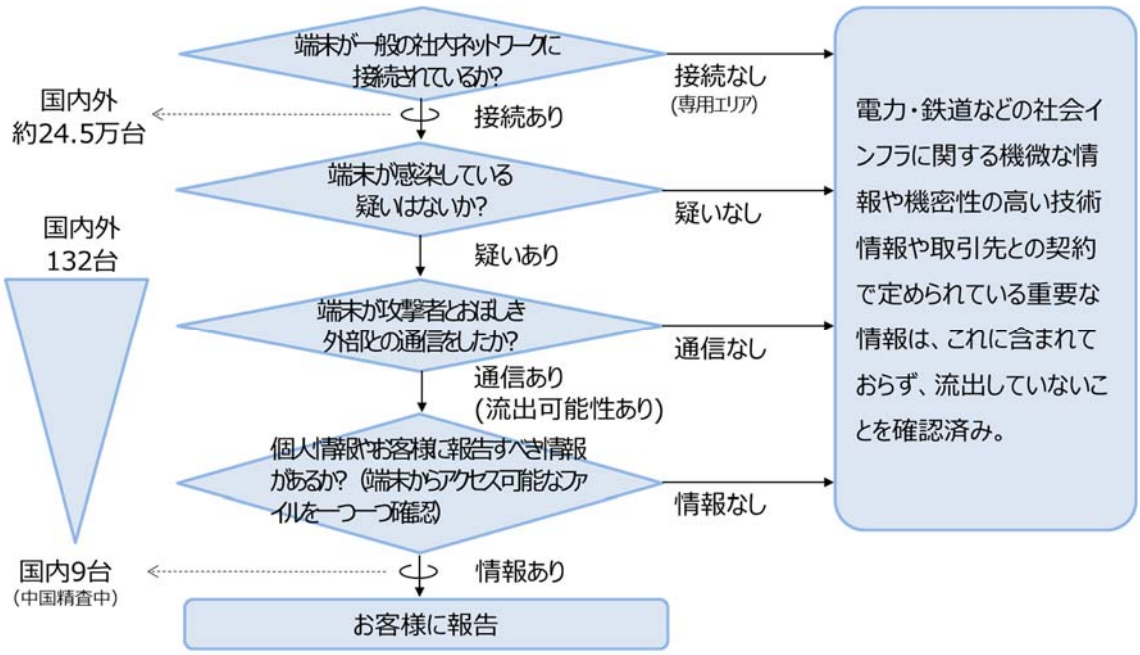


当社における検証プロセスと対応

サイバー攻撃に関わる影響の検証は、一般の社内ネットワークに接続しているすべての端末（約 24.5 万台）を対象に以下のプロセスで行いました。具体的には、マルウエア感染の疑いの有無、攻撃者とおぼしき特定の外部との通信有無を精査し、通信があった全端末を絞り込みました。当該端末からアクセス可能なすべての情報を精査した結果、電力・鉄道などの社会インフラに関する機微な情報や機密性の高い技術情報や取引先との契約で定められた重要な情報は、これに含まれておらず、流出していないことを確認しました。

感染の疑いのある端末台数は国内外含め 132 台で、そのうち個人情報やお客様への報告が必要と思われる重要情報に関わる端末は国内 9 台です。海外拠点の中では、中国の拠点で感染の疑いのある端末が確認されています。当該端末からアクセス可能な範囲には、機密性の高い技術情報や取引先との契約で定められている重要な情報は含まれておらず、流出していないことを確認しておりますが、お客様に報告すべき内容の有無を精査しているところです。他の海外地域の拠点については本件に関わる攻撃を受けていないことを確認済みです。

＜検証プロセス＞



流出した可能性のある個人情報については、該当する方々へのご報告を終え、お問い合わせに対応しているところです。

また、流出した可能性のある企業機密は、当社内の技術資料、設備投資計画や月次・週次の進捗報告、受注状況など、ほとんどが社内向けの資料です。お客様からいただいた資料やお客様に関係する社内向け資料については、お客様へ一次報告を終えております。

サイバーセキュリティー対策強化に向けた今後の取り組み

今般の不正アクセス事案について、端末・サーバー共に緊急対策を講じておりますが、本事案のような高度かつ巧妙な手法を用いた標的型攻撃を防御するには、これまで以上の多層防御態勢を整備していく必要があります。具体的には、「侵入防止」「拡散防止」「流出防止」「グローバル対応」の 4 つの視点でサイバーセキュリティー対策および監視体制の強化を行い、再発防止を図ります。加えて、文書管理の徹底や情報セキュリティー体制の強化により、総合的なサイバーセキュリティー対策強化を図ってまいります。

1．技術的対策

項目	主な対策
侵入防止	■未公開脆弱性対策 ・ 地域間・拠点間ネットワークのアクセス制限の強化 ・ 全サーバーのネットワークレベルアクセス制御を厳格化 ■標的型攻撃対策 ・ 挙動検知機能を全端末に配備
拡散防止	■グループ内感染防止対策 ・ 地域間・拠点間ネットワークのリアルタイム監視 ・ 端末リアルタイム監視と、感染端末の即時遮断
流出防止	■出口対策 ・ 不正アクセス先への通信遮断機能の強化
グローバル対応	■グローバルセキュリティーレベル向上 ・ 防御・監視機能のグローバル一元管理 ・ MELCO-CSIRT 機能の強化

2. 文書管理の徹底

当社では個人情報保護・企業機密管理に関する規則に、情報の重要度に応じた文書の保管場所や暗号化に関する運用を定めております。今回の事案を教訓に、文書管理状況の再点検と従業員教育の充実により、規則に沿って厳格に運用してまいります。

特定の事業や業務については、その特性を踏まえた文書管理を徹底いたします。

3. 体制強化

当社グループ全体の情報セキュリティー体制強化に向け、迅速な判断とインシデント発生時のお客様や関係機関との早期情報共有等を目的に、情報セキュリティー全般の企画・構築・運営の機能を一元的に担う社長直轄の統括組織を 2020 年 4 月 1 日付にて新設する予定です。

当社は、今回の事案を教訓として、社会全体のセキュリティーレベル向上に貢献してまいります。