MITSUBISHI ELECTRIC
Changes for the Better

三菱電機グループ　情報セキュリティ報告書 2022

目次

■ 目次・編集方針 …… 1

■ ごあいさつ …… 2

■ サイバー攻撃事案の教訓と情報セキュリティ強化
- 事案の概要 …… 3
- 事案から学んだ教訓 …… 3
- 今後の取り組み …… 3

■ 情報セキュリティの基本的な考え方
- 情報セキュリティの基本方針 …… 4
- 情報セキュリティの体制 …… 5

■ 情報セキュリティマネジメント
- マネジメントの考え方 …… 6
- 情報セキュリティにかかわる規則・ガイドライン …… 7
- 情報セキュリティの点検 …… 7
- 情報セキュリティの教育 …… 8
- 個人情報保護の取り組み …… 8
- その他の施策 …… 10

■ 情報セキュリティに対する取り組み
(技術的・物理的安全管理措置)
- サイバー攻撃対策 …… 11
- 物理セキュリティ …… 14

■ 製品・サービスのセキュリティ品質に対する取り組み
- 三菱電機PSIRTの役割 …… 15
- 三菱電機PSIRTの体制 …… 15

■ 第三者認証
- プライバシーマーク取得状況 …… 16
- ISMS認証取得状況 …… 16
- その他の第三者認証 …… 17

編集方針

本報告書は三菱電機グループが「活力とゆとりある社会の実現」に貢献するために日々取り組んでいる情報セキュリティの取り組みについて、ステークホルダーの皆様にご報告することを目的として発行しています。

報告期間

2021年度(2021年4月1日～2022年3月31日)

報告範囲

三菱電機グループの情報セキュリティの取り組み

報告書の発行時期

2022年7月発行

お問い合わせ先
情報セキュリティ統括室
〒100-8310
東京都千代田区丸の内二丁目7番3号〈東京ビル〉

情報セキュリティ報告書に関する
お問い合わせ

ごあいさつ

情報セキュリティへの対応を経営上の重要な課題と捉え取り組んでいきます。

三菱電機株式会社
常務執行役
情報セキュリティ担当
三谷 英一郎

三菱電機グループでは、過去に発生した不正アクセスによる情報漏えいの事案について深く反省し、サイバーセキュリティが重要な経営問題であることを再認識いたしました。それを踏まえて、2020年4月には、三菱電機グループの情報セキュリティ施策を統括する「情報セキュリティ統括室」を設置いたしました。

近年、テレワークの急増やクラウド活用事業の増加などに伴い、業務や事業環境が変化し、DX（デジタルトランスフォーメーション）推進が経営課題となっております。また、紛争に伴う地政学的な情報セキュリティリスクも高まってきております。そのため安心・安全にデータを活用できる環境が必要になってきており、情報セキュリティ統括室では、そうした状況の変化に備えるために必要な施策を立案し、三菱電機グループ全体へ展開しています。

企業にとってサイバー攻撃は、年々、大きな脅威となってきています。巧妙かつ多様化するサイバー攻撃に対して三菱電機グループ全体で対抗すべく、知見を共有していきます。

また、三菱電機グループでは、企業機密管理宣言ならびに個人情報保護方針を制定し、企業機密・個人情報の適切な取り扱いを徹底する企業風土の醸成にも努めています。これらの理念を具体化すべく、規則と体制の整備、全従業員への定期的な教育、ITを活用した総合対策を実施するとともに、点検活動を含めたPDCAサイクルにより常に改善を重ねています。

さらに、製品・サービスのセキュリティ品質に対する取り組みを強化しており、これらを通じて安心・安全な社会の実現に貢献してまいります。

ますます巧妙かつ多様化するサイバー攻撃への備えのほか、グローバルな視点での法令規制や経済安全保障の観点から、海外地域におけるリスクの判断とその対応を加速し、三菱電機グループの情報セキュリティに関する取り組みが、皆様のご期待に添えるものとなるよう、今後も推進してまいります。

本報告書は、三菱電機グループの情報セキュリティ活動をご紹介するものです。ご覧いただき、皆様のお役に立つことができれば幸いです。

サイバー攻撃事案の教訓と情報セキュリティ強化

三菱電機グループでは、標的型攻撃やランサムウエアなどの脅威に対する情報セキュリティ対策を重要な経営課題と捉え、当社グループを狙ったあらゆるサイバー攻撃に対して堅牢化し、ステークホルダーの皆様または当社に不利益を及ぼすおそれのあるすべての情報を守るべく対策に取り組んでいます。

事案の概要

これまで三菱電機グループでは、標的型攻撃によるマルウエア感染、クラウドサービスを介した不正アクセス、当社が管理するネットワークへの不正アクセスが発生いたしました。

標的型攻撃によるマルウエア感染については、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、それを調査したところ、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、かつ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。この攻撃によるマルウエア感染が国内外の端末で確認されました。

クラウドサービスを介した不正アクセスについては、当社が導入しているクラウド監視システムが、当社契約のクラウドサービスに対する通常とは異なるアクセスを検知しました。当社は直ちに当該の不正アクセスを遮断するなどの対策を講じましたが、当社の国内お取引先の金融機関口座に関わる情報などが外部へ流出したことが確認されました。不正アクセスは、中国にある当社子会社への不正アクセスを契機として、第三者が当社および当社国内子会社の一部の従業員のクラウドアクセス用アカウント情報を窃取し、当社が契約しているクラウドサービスおよび関連サーバーを攻撃したものであることが判明しました。マルウエアによる侵害やソフトウエアの脆弱性を突いた攻撃ではなかったため、正常な利用を含む多くのログの中から不正アクセスを探索する必要があり、全容の調査に時間を要しました。

当社が管理するネットワークへの不正アクセスについては、通常とは異なる海外からのアクセスを検知し、関係会社の機密情報が外部へ流出したことが確認されました。

事案から学んだ教訓

今回、サイバー攻撃事案を受けて3つの教訓を得ました。

まず1つ目は、特定部分の対策をしていれば攻撃から守られるとは限らないということです。従来の対策だけでは防ぐことのできない高度かつ巧妙な攻撃に対しては、さらに複数の防御対策を講じて何重にも守ることが必要になります。

2つ目は、境界防御による対策だけでは守り切れないということです。社内のIDやパスワードの情報を窃取し、それらの情報を使用した不正アクセスに対しては、すべてのアクセスを信頼しないゼロトラスト※1の考え方で対策を講じる必要があります。

3つ目は、事案の発生に対して迅速に原因を特定し対策を講じるために、一元管理の概念が重要であるということです。管理すべき情報が複数の場所に分散していたり、複数の場所で調査・分析をしていたりすると、一貫して管理することができず、総合的な判断にも時間を要して報告が遅れ、被害も大きくなってしまいます。

※1 社内外すべてを信用できない領域とし、すべての通信を検査し認証を行うという考え方

今後の取り組み

事案を受けて、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ると考えています。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攻撃対策と監視体制を強化し、再発を防止します。加えて、文書管理の徹底や情報セキュリティ体制の強化により、総合的にサイバー攻撃対策を強化してまいります。

また、不正アクセスを受けたクラウドサービスに対する監視をさらに強化するとともにゼロトラストセキュリティ対策を加速し、再発防止を徹底いたします。国内外のネットワークアクセス制御の強化、端末のセキュリティ対策や多要素認証を含む認証基盤、監視の強化など、総合的な多層防御によるセキュリティ対策の強化を当社グループ全体で加速し、今後も関係機関と連携しながら、さらなる強化に継続的に取り組んでまいります。

さらに、対策においては一元管理の概念を導入し、一貫したセキュリティ対策に取り組んでまいります。

情報セキュリティの基本的な考え方

情報セキュリティの基本方針

三菱電機グループでは、不正アクセスによる情報漏えい事案の再発を防止すべく、サイバー攻撃対策の強化に加え、情報管理・運営体制などの継続的な強化に取り組みます。具体的な目標としてサイバーセキュリティ成熟度モデル（CMMC）※2のレベル3以上を目指します。

なお、三菱電機のステークホルダーの皆様からお預かりした情報、営業情報や技術情報、知的財産などの企業機密については、2005年2月に制定した「企業機密管理宣言」の考えに基づき管理していましたが、過去の事案の反省を踏まえて、本宣言を、改めて深く三菱電機グループ内へ浸透させ、さらなる情報の保護・管理を徹底していきます。

※2 米国防総省が発行する、サイバーセキュリティ成熟度モデルの認証の枠組み。レベル3以上は優れたセキュリティ対策・管理体制を表す

企業機密管理宣言

当社は事業活動の根幹をなす情報資産に関して社外に開示すべき情報については適時適切に開示する一方、企業機密については適正な管理を徹底します。

皆様からお預かりした貴重な情報や企業機密が万一漏えいすれば、当社にお寄せいただいた信用・信頼を失墜するのみならず、その不正な使用により、国家・社会・個人の安全が脅かされかねません。

企業機密の適正な管理は当社が完遂すべき社会的責任の1つであると認識し、当社の全従業員が以下の企業機密管理方針を遵守することを宣言します。

1. 法令・規則遵守による企業機密の適正な管理
   当社は、事業活動に関連するすべての企業機密を、法令及び当社規則に従い適正に管理します。
   企業機密とは、当社が保有する技術上又は営業上の有用な情報及び漏えい・不正使用により当社又はステークホルダーの皆様に不利益を及ぼすおそれのある情報（個人情報、社外から得た情報、インサイダー情報等を含む。）を指し、企業機密を具現している物理的対象物も管理の対象とします。

2. 安全管理措置の徹底
   当社は、企業機密の保護・管理のため、適切な安全管理措置を講じます。
   安全管理措置とは、組織的・人的・技術的・物理的諸対策を指し、企業機密のレベルに応じた措置を徹底します。

3. 情報システムセキュリティ対策の強化
   当社は、企業機密に対する不正アクセス・侵害、不正使用の防止等の観点から、情報システムセキュリティ対策を強化し、ITを活用した総合的な対策を実施します。

4. 全従業員に対する教育の実施
   当社は、企業機密に携わる個々の従業員の意識向上こそが管理の基本であるとの認識に基づき、企業機密管理の重要性と企業機密管理に向けた当社の取組につき、全従業員を対象とする教育を定期的に実施します。

5. PDCAサイクルによる継続的な管理向上
   当社は、企業機密管理に関するマネジメントシステムを構築し、PDCA（Plan・Do・Check・Act）のサイクルによる主体的かつ継続的な管理向上を図ります。

6. 適時適切な情報開示の実施
   上記1.～5.により、企業機密については適正な管理を徹底するとともに、社外に開示すべき情報については適時適切に開示します。

制定日　2005年2月16日
改正日　2021年7月28日
三菱電機株式会社
執行役社長　漆間　啓

情報セキュリティの体制

2020年4月に、社長直轄組織として情報セキュリティ統括室を設け、「企業機密管理・個人情報保護」「情報システムセキュリティ」「製品セキュリティ」の三機能を統合し、情報セキュリティ管理活動全般を統括しており、2021年4月には同組織の体制と陣容を強化拡充しています。また、500億円超を投資し、サイバーセキュリティ対策を強化するとともに、情報管理・運営体制などの継続的な強化に努め、サイバーセキュリティ成熟度モデルのレベル3以上を目指します。

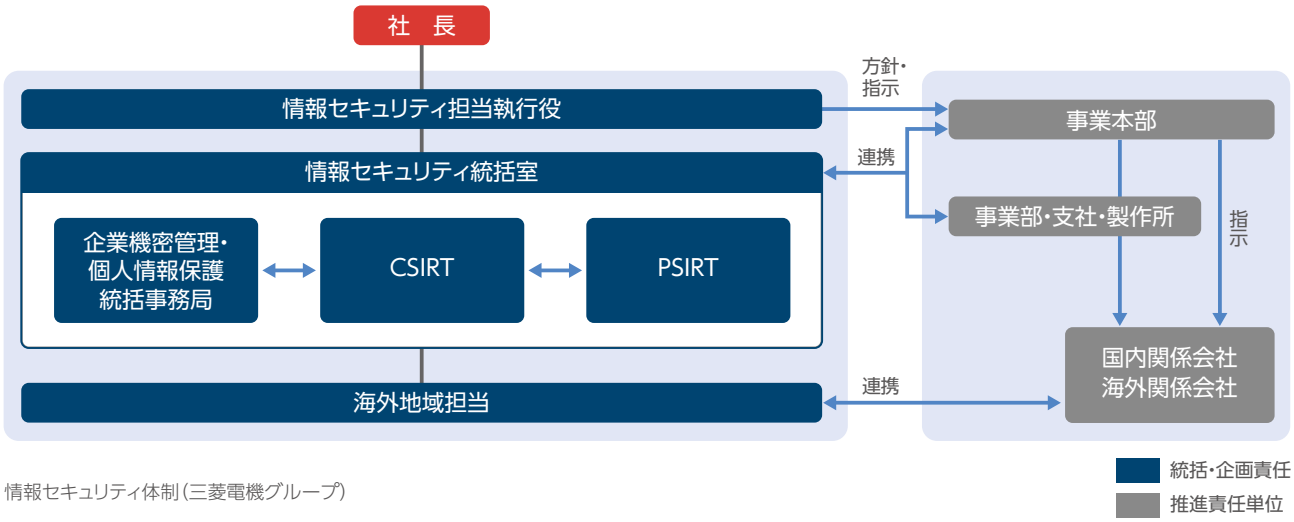
情報セキュリティ担当執行役は情報セキュリティ管理全般を統括し、情報セキュリティ統括室はその指示のもと、三菱電機グループの情報セキュリティ管理の仕組み、ルール、情報システムのセキュリティ確保に関して企画・推進しています。各情報、システムを利活用・管理する各事業本部、事業所に設置するCSIRT※3が相互に連携し、情報セキュリティの確保に努めています。

また、工場の生産に影響を与えるようなサイバー攻撃が他社で発生していることから、三菱電機においても工場セキュリティを担当するグループを設置し、体制を強化しています。

加えて、製品セキュリティ施策を推進するPSIRT活動※4は2020年11月にCNA※5として認定され、三菱電機製品に影響を与える脆弱性に自らCVE ID※6を付与し、公表しております。これにより、社外ステークホルダーとの効率的な脆弱性ハンドリングを実践する体制を強化しています。確認された脆弱性は、この体制に沿って報告・指示され、二次被害を防ぐなどの適切な対応をとります。

国内外の関係会社については、事業本部・事業所（事業部・支社・製作所）から情報セキュリティに関して指示・指導をしています。特に海外の関係会社については、地域ごとの事情、特性を考慮すべく情報セキュリティ統括室が米州・欧州・中国・アジアの各拠点の海外地域担当と情報セキュリティ確保のためにより一層の連携を深めていきます。

※3 CSIRTはComputer Security Incident Response Teamの略
※4 PSIRTはProduct Security Incident Response Teamの略。
製品・サービスのセキュリティ品質に対する取り組み
※5 CVE Numbering Authority、CVE採番機関。CVEとはCommon Vulnerabilities and Exposuresの略
※6 国際的に使用されている脆弱性の識別子



情報セキュリティ体制（三菱電機グループ）

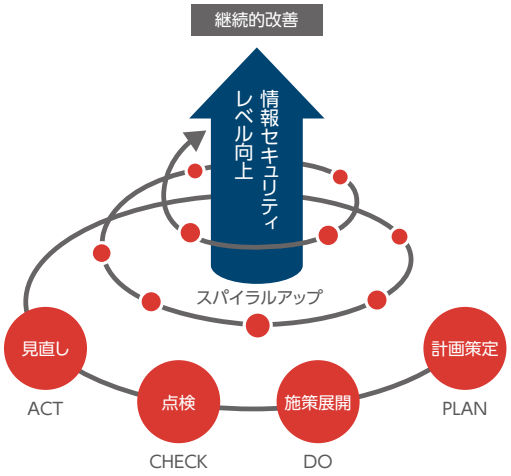
情報セキュリティマネジメント

マネジメントの考え方

三菱電機グループでは企業機密管理及び個人情報保護の活動をPDCA(Plan-Do-Check-Act)サイクルによる継続的な改善活動として取り組み、企業機密・個人情報を守るために、海外における個人データの取り扱いなどの外的環境も考慮して、組織的・人的・物理的・技術的からなる4つの安全管理措置を実施しています。

PDCAサイクル

年度初めに年度方針に基づく計画を策定(Plan)し、各種情報セキュリティ施策の展開や従業員への教育を行った(Do)上で、情報セキュリティの運用状況を確認(Check)し、その結果を基に施策などを見直す(Act)ことで、情報セキュリティのレベルがスパイラルアップするよう努めています。



PDCAサイクルによる継続的改善

4つの安全管理措置

「組織的」安全管理措置は、管理体制、社内規則、社内監査など企業機密・個人情報を守るための仕組みであり、業務環境の変化などによりその有効性が失われないよう必要に応じて、都度見直しています。

「人的」安全管理措置は、情報セキュリティの施策を従業員に徹底するための教育や労務管理です。

「物理的」安全管理措置は、無関係な第三者が事業所内に入って企業機密や個人情報に触れることを防ぐ入退室管理や機器などの物理的保護です。

「技術的」安全管理措置は、サイバー攻撃対策などの情報システムセキュリティです。

4つの安全管理措置

グローバルでの取り組み

海外関係会社を含めたグループ全体で情報セキュリティレベルを維持・向上すべく、関係会社向けの企業機密管理・個人情報保護に関するガイドラインを制定し、情報セキュリティの体制に則り、各種点検を実施しています。

情報セキュリティにかかわる規則・ガイドライン

企業機密管理宣言、個人情報保護方針を実現するために、情報セキュリティにかかわる規則・ガイドラインを4つの安全管理措置に沿って整備し、現行の法律に則り、適宜見直しています。

また、個人情報保護についても同様のルールを定め、関係会社に対しても適用しています。

項目		基本的な規則
安全管理措置	組織的安全管理措置	企業機密管理規則／個人データ保護ガイドライン
	人的安全管理措置	社員就業規則
	物理的安全管理措置	物理セキュリティガイドライン
	技術的安全管理措置	情報システムセキュリティ管理規則

業務環境の変化に対する対応

基本となる上記規則類に加えて、業務環境の変化に応じて「公開ウェブサイトの開示に関する規則」、「スマートフォンの使用に関する規則」、サプライチェーン上の情報セキュリティを強化するための管理基準などを必要に応じて適宜設けています。

情報セキュリティの点検

三菱電機グループでは、グループ全体の企業機密管理・個人情報保護活動が適切になされているか、またどのようなレベルにあるかを確認するために、PDCAサイクルの中のC（Check）として、本社コーポレート部門、事業本部、事業所及び関係会社にて次の点検活動を実施しています。

これにより、施策などを見直し、PDCAサイクルのA（Act）につなげていきます。

これらの点検活動については、三菱電機を対象とした「企業機密管理規則」及び国内外関係会社を対象とした「情報セキュリティ管理規則ガイドライン」に定めています。

分類	名称	内容など
自己チェック	企業機密管理・個人情報保護に関する自己点検	三菱電機グループ各社でチェックリストを用いて、情報セキュリティの取り組みを自己点検しています。
第三者チェック	企業機密管理・個人情報保護に関する第三者点検	三菱電機事業所間では相互に情報セキュリティの運用状況を確認しています。関係会社の情報セキュリティの運用状況は三菱電機が確認しています。
	個人情報保護の監査（PMS監査）	三菱電機では、三菱電機執行役社長から指名された個人情報保護監査責任者の指示の下、全社で個人情報の保護状況を確認しています。プライバシーマークを付与された国内関係会社では、各社の監査責任者により同様の確認をしています。

情報セキュリティの教育

三菱電機では、企業機密・個人情報の適切な取り扱いを徹底する企業風土の醸成に努めています。例えば、不正アクセスによる情報漏えい事案を踏まえ、機密等級に応じたファイルのサーバー保管や暗号化など具体的な安全管理措置を従業員が着実に実施できるよう下記の教育プログラムを実施しています。

全従業員への教育

約5万人の全従業員などを対象に情報セキュリティの教育を年一回、eラーニングで実施し、三菱電機の方針、情報漏えい事故概況、個人情報保護関連法令、不正競争防止法、一人ひとりが認識すべき安全管理措置（組織的・人的・物理的・技術的）を周知徹底します。また、テレワークの急増やクラウド活用による業務形態・環境の変化に伴い、適宜従業員向け教育資料を展開しています。

キャリアパスに沿った教育

新入社員教育、新任課長研修の中で、各階層で求められる役割を果たすために必要な企業機密管理・個人情報保護の教育を実施しています。

不審メール対処予行演習

サイバー攻撃対策として、三菱電機では役員を含む全従業員を対象に「不審メール対処予行演習」を実施し、定期的に不審メールへの対処方法を確認しており、国内関係会社の従業員も同演習に参加できるようにしています。海外関係会社については、地域担当の下、米州、欧州、中国で地域の実情に合わせて予行演習を実施しています。

その他の個別教育

海外赴任者に対しては赴任前研修の中で、企業機密管理・個人情報保護に関する海外でのリスク、海外での情報漏えい事故の事例について教育しています。

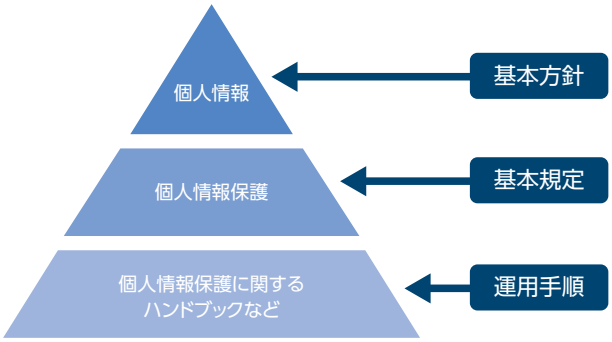
個人情報保護の取り組み

個人情報保護

三菱電機では、2001年10月に「個人情報の保護に関する規則」を制定の上、三菱電機従業員及びその他関係者に個人情報保護を周知徹底し、個人情報保護活動に取り組んでいます。

2004年には「個人情報保護方針」を制定し、日本工業規格「JIS Q 15001：2006個人情報保護マネジメントシステム―要求事項」に準拠した個人情報保護活動として整備しました。2008年1月には、個人情報について適切な保護措置を講ずる体制を整備していることを認定するプライバシーマークを取得し、以後、継続して更新しています。

また、2022年4月に施行された改正個人情報保護法に適切に対応すべく、社内の規則などを見直しています。



個人情報保護のルール体系

各種アンケートやお買い上げいただいた製品の登録、アフターサービスなどを通じて入手したお客様の個人情報は、「個人情報保護方針」の考えに基づき管理しています。さらに、三菱電機ではプライバシーマークを取得しており、個人情報の適正な取り扱いに努めています。

個人情報保護方針

三菱電機（以下、「当社」といいます。）は、技術、サービス、創造力の向上を図り、活力とゆとりのある社会の実現に貢献していきます。このような活動を通じて、当社はお客様や関係の皆様から、様々な情報をお預かりしており、個人情報については個人の重要な財産であることから、法律に則って適切に保護し、正確かつ安全に取扱うことは企業の社会的責務と考えます。当社は、経営の一環として個人情報保護マネジメントシステムを確立し、当社従業員（役員・社員・パートタイマー・アルバイト・派遣社員などを含む）及びその他関係者に個人情報保護を周知徹底させて以下の取り組みを実行するとともに、改善・維持に努めてまいります。

1. 個人情報保護の目的
   個人情報を適正かつ効果的に活用し、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とします。

2. 個人情報の利用目的
   ご本人様に明示した利用目的の範囲内で、事業遂行上必要な場合のみ個人情報を利用します。また、目的外の利用を行わないために必要な措置を講じています。

3. 個人情報の取得
   適法かつ公正な手段によって個人情報を取得します。直接、ご本人様より取得する場合は、利用目的等の必要事項を明示し、同意を頂きます。

4. 個人情報の開示・提供
   委託業務や協業等に際して第三者に個人情報を開示・提供する場合には、ご本人様の同意を取得します。

5. 個人情報の取り扱い
   (1) 個人情報保護に関する法令等の遵守
   当社は、個人情報保護に関する法令、国が定める指針及びその他規範を遵守します。
   (2) 個人情報の漏えい・滅失又は毀損の防止（安全管理措置等）及び是正に関すること
   個人情報への不正アクセス、紛失、破壊、改ざん及び漏えい等を未然に防止するため、合理的な安全対策とともに、必要な安全管理措置を講じます。また、毎年、個人情報の取り扱い状況について、全部門を対象に監査を実施し、是正処置を実施しています。この監査では、最新の漏えいリスクや課題を全部門で再確認し、同様の事象が発生しないよう改善に努めています。
   (3) 個人情報保護マネジメントシステムの構築・運用
   当社は、「JISQ15001 個人情報保護マネジメントシステム−要求事項」を基に個人情報保護マネジメントシステムを構築し、運用しています。一般財団法人 日本情報経済社会推進協会の審査を受審し、個人情報の適切な取り扱いを行う事業者に与えられる「プライバシーマーク」の付与認定を受けています。今後も、個人情報マネジメントシステムを継続的に改善しながら、個人情報を保護します。

プライバシーマーク

6. 個人関連情報の取り扱い
   当社のウェブサイト等にて、位置情報・IPアドレス・クッキー情報等の個人関連情報を取り扱う場合は、ご本人様に利用目的を通知し、同意を取得することがあります。

7. ご本人様からのお問い合わせへの対応
   ご本人様から個人情報の開示、訂正、削除、利用停止等を求められたとき、及び苦情、相談等のお問合せを受けたときは、遅滞なく対応いたします。また、個人情報を正確かつ最新の状態に保つよう努めます。

制定日　2004年4月16日
改正日　2022年4月 1 日
三菱電機株式会社
執行役社長　漆間　啓

個人情報の適切な取り扱い

個人情報は利用目的を特定するなど適切に取得し、利用するときは「利用目的の範囲を超えて利用しない」、「第三者に提供するときはあらかじめ本人の同意を得る」など、個人情報を適切に取り扱っています。また、サイバー攻撃による流出リスクにも備えるべく、サーバー保管や暗号化対策などの安全管理措置を一層強化していきます。

プライバシーマーク

三菱電機及び「第三者認証」に記載の国内関係会社では、プライバシーマークを取得しています。

マイナンバーへの対応

マイナンバー制度に対応した社内規定に則り、厳格な管理と適切な取り扱いに努めています。マイナンバーを取り扱う従業員に対して、個別に教育しています。

EU一般データ保護規則(GDPR)、中国個人情報保護法への対応

EUにおけるプライバシー保護の枠組みとして2018年5月に施行されたEU一般データ保護規則(GDPR;General Data Protection Regulation)に従い、三菱電機グループとしてEU個人データを適切に取り扱っています。また、欧州以外においては中国で個人情報保護法が2021年11月1日に施行されるなど、個人データの越境移転は規制される動向にあり、適切に対応していきます。

その他の施策

取引先・委託先管理

企業機密・個人情報を委託する際は、適切に秘密保持契約を締結した上で、セキュリティ上の理由から取引・委託先に求めるべき事項があれば契約書に記載しています。委託先に渡した企業機密・個人情報が適切な管理のもとで取り扱われていることを確認するために、委託先が適切な保護水準を維持しているか評価・選定し、契約後も定期的に利用及び管理状況の報告を受けるなど、適切に監督しています。さらに、個人情報の取り扱いを他社に委託するときは、個人情報保護に留意した取り扱い事項を規定した契約をしています。

情報セキュリティに対する取り組み（技術的・物理的安全管理措置）

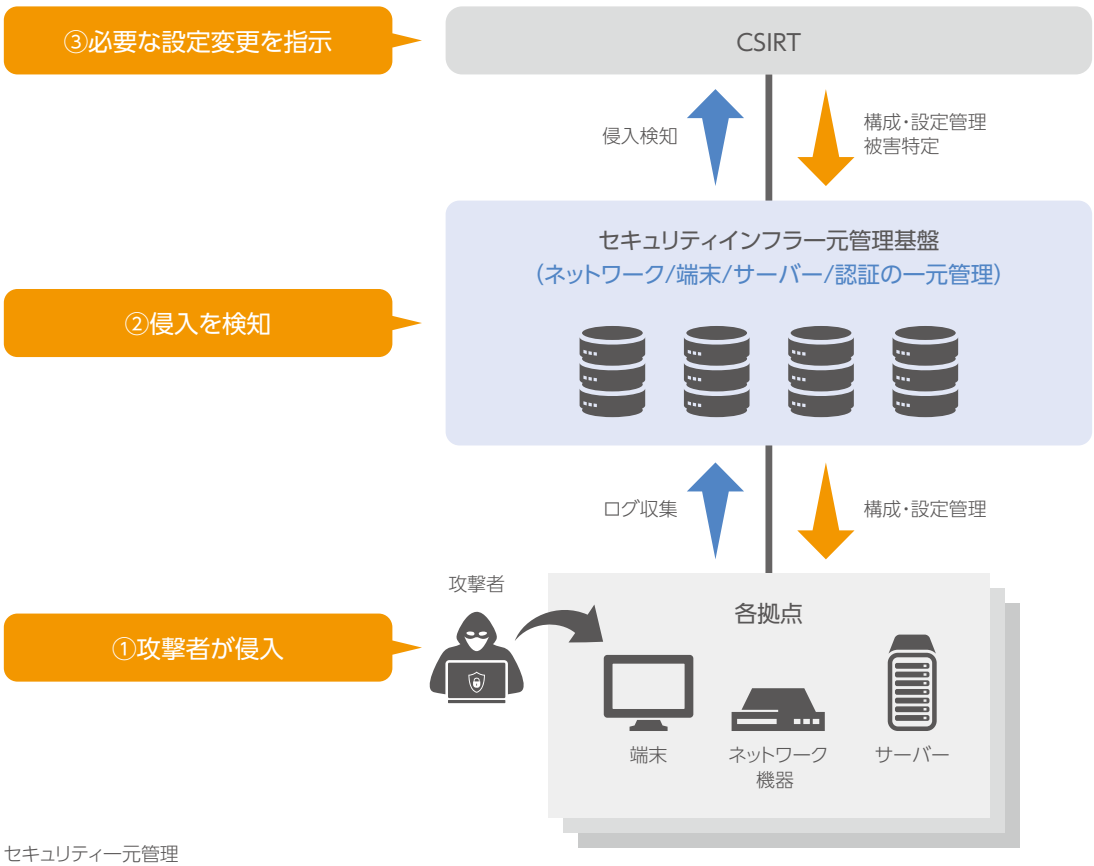
三菱電機グループでは、情報セキュリティに対する取り組みとして、ITインフラのサイバー攻撃対策や物理的なセキュリティ対策を行っております。

サイバー攻撃対策

企業に対するサイバー攻撃は、年々、巧妙かつ多様化しており、大きな脅威となっています。

三菱電機グループでは、クラウドサービスの利用、テレワークの普及に伴い巧妙かつ多様化するサイバー攻撃への対策として、ネットワークや端末、サーバー（クラウド）の一元管理と、ゼロトラストセキュリティの考え方に基づく「多層防御」の導入に取り組んでいます。「多層防御」によりサイバー攻撃の防御、不審な兆候及び侵入の検知を可能とし、さらに、即時対応する体制を整えることで、被害を防止するとともに、最小化しています。

また、オフィスのほか、テレワーク、出張先からのアクセスによる業務に対応するため多要素認証を導入し、認証を一元的に管理しています。さらに、常に外部から多くの脅威にさらされているインターネット公開ウェブサイトについては、セキュリティレベルを保つために三菱電機が認定したウェブサイトのみを公開しています。



セキュリティー元管理

多層防御

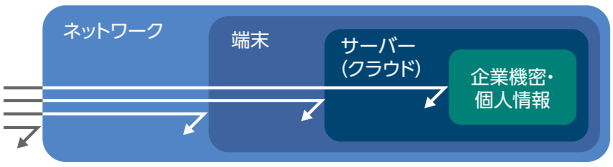
三菱電機グループでは、「多層防御」として「ネットワーク」、「端末」、「サーバー（クラウド）」の3階層の技術的なセキュリティー対策を実施しています。

ネットワークでのセキュリティー対策では、インターネットと社内ネットワークの接続点に様々なセキュリティー対策機器を配置し、メールやウェブなどの通信を制御・監視します。それにより、外部から社内への不正なアクセスやマルウエアの侵入を遮断することや、社内から外部へ情報が漏えいすることを防ぎ、今後もこの通信遮断機能を強化していきます。

端末のセキュリティ対策では、マルウエア対策ソフトによるマルウエアの検知・駆除や、ソフトウエアの脆弱（ぜいじゃく）性を修正するセキュリティパッチの適用を行います。それにより、端末へのマルウエア感染を防ぎ、攻撃を抑制するとともに、被害を局所化します。そのために、端末を一元的に管理し対策を徹底しています。また、今後不審なふるまいを検知する機能を全端末に配備し、対策を強化していきます。

クラウドの活用が進むサーバーに対しては、脆弱性の定期的な診断の他、通信やクラウドの運用を監視します。それにより、重要な情報が格納されるサーバー（クラウド）において堅牢な環境を維持できるようにしていきます。

サーバーやクラウドに格納される企業機密・個人情報に対しては、「最小権限の原則」に基づいたアクセス制御と暗号化を適用します。これらの情報管理については、規則の整備と徹底、従業員教育、点検活動もあわせて実施しています。

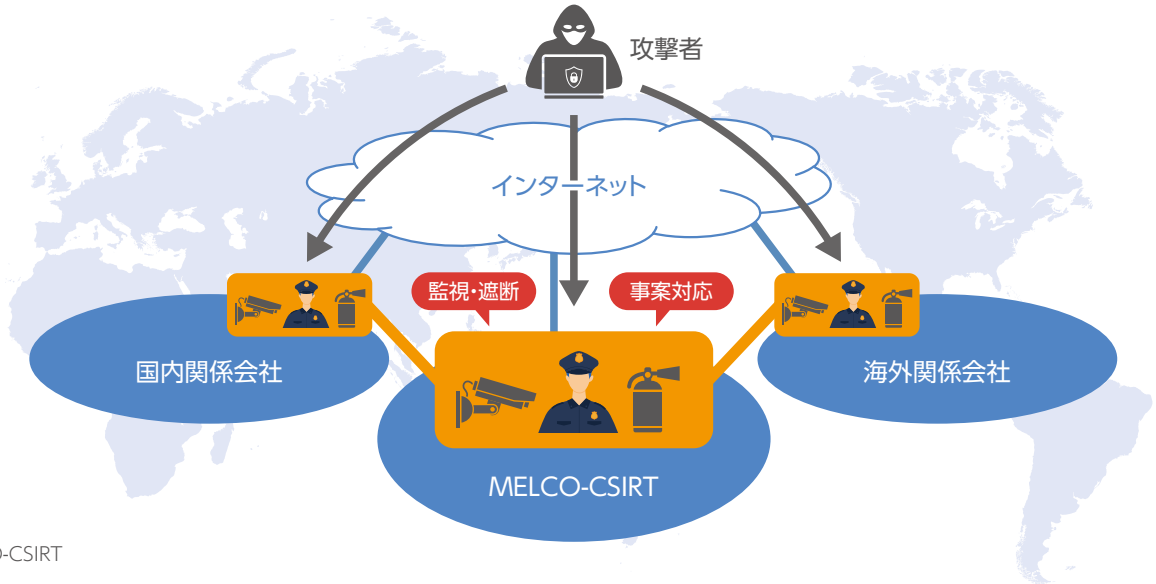


多層防御

緊急即応体制

三菱電機グループでは、サイバー攻撃に対する監視と事案発生時の即時対応のため、MELCO-CSIRT（Mitsubishi Electric Corporation Computer Security Incident Response Team）を設置しています。

従来は対応が不十分であった国内外の関係会社に対する監視体制も整えました。前述の「出入口対策」で通信を監視することにより、不審な挙動を検出、安全性を確認することでサイバー攻撃をいち早く検出し遮断します。また、「端末セキュリティ対策」により、マルウエアの検知情報や端末のセキュリティ対策状況などを収集、把握することができます。万一、事案が検出された場合は、上記の仕組みを駆使することで、即座に被害状況を把握し、緊急で適切な対処、復旧を行い、被害を可能な限り抑えます。その後、事案を詳細に分析し、事案発生部門による恒久対策の実施を支援します。



MELCO-CSIRT

テレワーク時のセキュリティ対策

出張時のモバイル勤務以外にも在宅勤務やサテライトオフィスの利用など、多様化するワークスタイルに対応してテレワークの活用が進んでいます。また、近年では新型コロナウイルス感染対策として在宅勤務の機会が大幅に増加し、テレワークの活用はますます増え、より一般的な働き方として浸透していくと思われます。

一方で、ネットワークやクラウドの活用によって業務環境も多様化し、従来の社内システムとインターネットとの境界を防御するセキュリティ対策では十分に対応できない状況も起こり得ます。そこで、VPN（仮想専用通信網）接続により通信を暗号化し、安全性を確保するとともに、多要素認証も導入し、より強固なセキュリティ対策を行っています。

我々は、在宅勤務、サテライトオフィス勤務、モバイル勤務（出張）のいずれに対しても、ゼロトラストの考え方を導入し、サイバー攻撃から防御するためのセキュリティ対策にひき続き取り組んでいきます。

インターネット公開ウェブサイト管理

三菱電機グループでは、過去に発生した不正アクセスによる事故を契機に、セキュリティレベルを保つために三菱電機が認定したウェブサイトのみを公開しています。

事前にセキュリティ検査を実施して不具合を解消したウェブサイトでなければ、公開を許可していません。また、インターネット上の公開ウェブサイトを定期的に点検して、管理状況を把握することで、不要なウェブサイトを廃止する他、セキュリティ対策が不十分なウェブサイトについてはセキュリティ対策を強化しています。あわせて、未許可のウェブサイトを見つけた場合は、速やかにセキュリティ検査を実施しています。

物理セキュリティ

三菱電機グループでは、不審者が事業所内に立ち入って企業機密に触れることがないよう、事業所内の敷地、廊下、執務室、会議室、サーバーエリア、資料室など、人が活動する場である物理領域（エリア）を区画化し、エリアごとにセキュリティのレベル（エリアレベル）を定めています。

エリアレベル

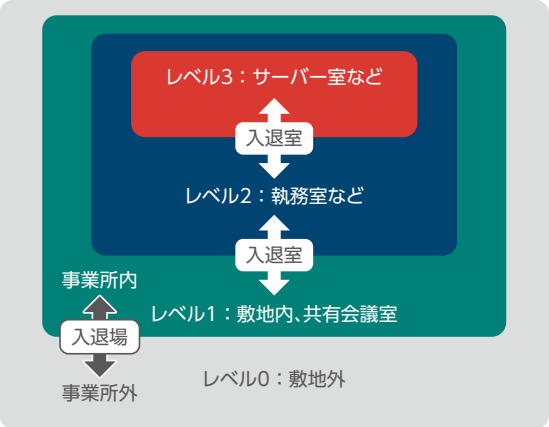
エリアレベルの考え方は以下の表のとおりです。エリアレベルに応じたセキュリティのルールを定めています。

	レベル	判断基準	例	
高	エリアレベル3	事業所内で、限定された従業員のみが利用・アクセス可能なエリア	サーバー室、資料室、開発室	事業所内
	エリアレベル2	事業所内で、原則従業員のみが利用・アクセス可能なエリア	執務室	
	エリアレベル1	事業所内で、入場手続きを済ませた従業員関係会社社員（代理店含む）やお客様が利用できるエリア	敷地、共用会議室、廊下	
低	エリアレベル0	事業所外	敷地外	事業所外

エリアレベルの考え方

入退室（場）管理

エリアレベルの異なるエリアに入る際は、認められた者しか入れないよう入退室（場）を管理しています。特に、三菱電機の事業所においては、IDカードによる認証システムを導入することで、入退管理の効率化とセキュリティーの確保を実現しています。



入退室（場）管理

製品・サービスのセキュリティ品質に対する取り組み

三菱電機PSIRTの役割

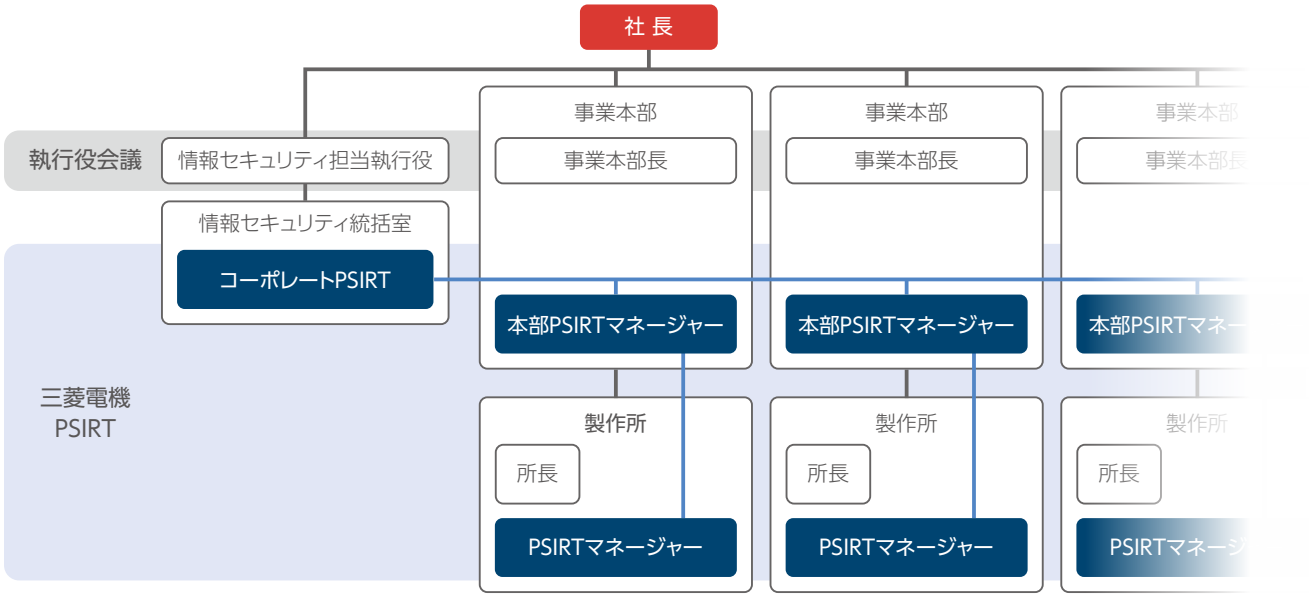
三菱電機では、製品・サービスのセキュリティ品質に対応する社内の体制として三菱電機PSIRT（Product Security Incident Response Team）を構築し、製品・サービスの情報セキュリティに対し全社で取り組んでいます。

三菱電機PSIRTは、以下を実施することを役割としています。

- お客様へ提供している製品・サービスの脆弱性に関する情報収集
- 製品の設計・製造部門及びサービスの運用部門と連携し発見された脆弱性への迅速な対応
- 製品やサービスを提供する前の段階で脆弱性を作り込まないようにするための設計・開発手法の導入推進
- 製品・サービスの開発に関係するすべての役員及び従業員に対する必要なセキュリティに関する教育
- 脆弱性に関する情報・対策のお客様への公開

三菱電機PSIRTの体制

三菱電機では、すべての事業本部と事業所に、製品・サービスのセキュリティにおける責任者（PSIRTマネージャー）を配置し問題への対応などリスク低減を推進しています。また、情報セキュリティ統括室に全体を統括するコーポレートPSIRTを設置し、製品・サービスのセキュリティ品質向上に対して取り組んでいます。



三菱電機PSIRTの体制図

第三者認証

三菱電機及び国内関係会社では、個人情報や情報セキュリティに関連する第三者評価・認証の取得を推進しています。

プライバシーマーク取得状況

プライバシーマーク取得状況（2022年3月30日現在）	
三菱電機株式会社	三菱電機インフォメーションシステムズ株式会社
アイテック阪急阪神株式会社	三菱電機インフォメーションネットワーク株式会社
株式会社アイプラネット	三菱電機クレジット株式会社
エムビーテクノ株式会社	三菱電機ITソリューションズ株式会社
株式会社ガウス	三菱電機保険サービス株式会社
西菱電機株式会社	メルテック・ビジネス株式会社
株式会社ダイヤモンドパーソネル	株式会社栗菱コンピューターズ
株式会社ビーシーシー	

ISMS認証取得状況

ISMS※7認証取得状況（2022年3月30日現在）
三菱電機株式会社（インフォメーションシステム統括事業部）
三菱電機株式会社（鎌倉製作所）
三菱電機株式会社（通信機製作所）
アイテック阪急阪神株式会社
青森三菱電機機器販売株式会社（関連組織：株式会社シンク）
株式会社シンリョー
西菱電機株式会社（猪名寺事業所・鳥取西菱電機株式会社）
通菱テクニカ株式会社
株式会社ビーシーシー
三菱電機インフォメーションシステムズ株式会社、株式会社テクノウェア
三菱電機インフォメーションネットワーク株式会社
三菱電機エンジニアリング株式会社（伊丹事業所）
三菱電機エンジニアリング株式会社（鎌倉事業所）
三菱電機システムサービス株式会社 第3本部
三菱電機特機システム株式会社（東部事業部（鎌倉地区、北海道工場、三沢出張所、築城出張所、佐世保出張所、郡山事務所））
三菱電機特機システム株式会社（西部事業部（三田地区、伊丹地区、岩国地区、沖縄地区））
三菱電機ITソリューションズ株式会社、エムビーテクノ株式会社
三菱電機プラントエンジニアリング株式会社
三菱プレシジョン株式会社（1.営業本部における以下製品の防衛・宇宙分野向け営業、2.鎌倉事業所における航空・宇宙・慣性・電波機器及びシミュレーションシステム並びに駐車場システムの製造及び保守）
株式会社栗菱コンピューターズ（本社）
菱栄テクニカ株式会社（品証事業部計測管理部校正サービスセンター）
菱電商事株式会社（新事業推進室）

※7 ISMSはInformation Security Management Systemの略

その他の第三者認証

国際標準規格「IEC 62443-4-1」認証取得

FA システム事業の開発・製造拠点である名古屋製作所と産業メカトロニクス製作所が、産業用オートメーションと制御システムのセキュリティ開発ライフサイクルに関する国際標準規格「IEC※8 62443-4-1」の認証を取得しました。

「IEC 62443-4-1」は、産業用オートメーション、制御システムおよびそれらの開発プロセスを対象としたセキュリティに関する国際標準規格です。

今回の認証取得により、両製作所の製品の開発・生産・保守のライフサイクル全般において、国際標準のセキュリティ要件を満たしていることが認められました。

今後も当社は、取得した認証に基づく企業活動を継続し、セキュリティ機能を強化した製品※9とサービスの提供を推進していきます。

※8 IECはInternational El ectrotechnical Commission（国際電気標準会議）の略

※9 シーケンサ、産業用PC、FAセンサー、表示器、サーボアンプ、インバーター、ロボット、CNC、放電加工機、レーザ加工機、関連ソフトウエアなど

三菱電機株式会社
www.MitsubishiElectric.co.jp