情報セキュリティ

基本的な考え方

三菱電機グループでは、急速に高度化、巧妙化が進むサイバー攻撃の脅威に対応するため、サイバーセキュリティと、情報管理・運営体制などのガバナンスの継続的な強化に取り組んでいます。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 ver.2)*のレベル2以上を目指します。

三菱電機の顧客や取引先等をはじめとした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、知的財産等の企業機密については、「企業機密管理宣言」の考えに基づき管理しています。

* 米国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2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

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設置された情報セキュリティ統括室は、「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・運営体制等の継続的な強化に努めています。

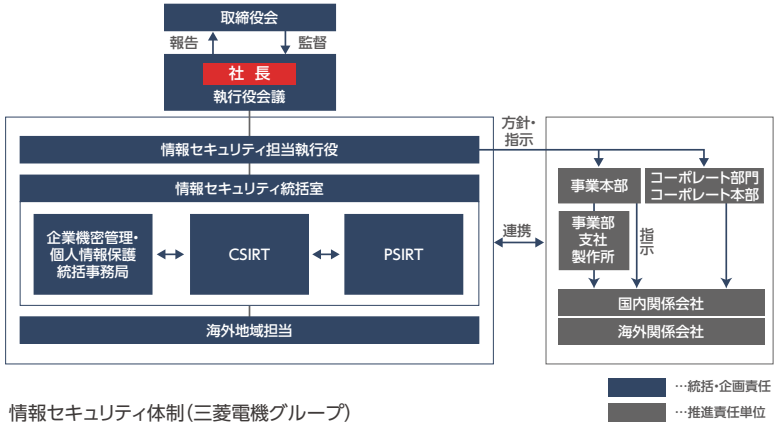
情報セキュリティ担当執行役は情報セキュリティ管理全般を統括し、情報セキュリティ統括室はその指示のもと、三菱電機グループの情報セキュリティ管理の仕組み、ルール、情報システムのセキュリティ確保、個人情報保護に関する法令遵守や取組みに関して企画・推進しています。各情報、システムを利活用・管理する各事業本部、事業所に設置するCSIRT*1が相互に連携し、情報セキュリティの確保に努めています。

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*2活動は2020年11月にCNA*3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*4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、二次被害を防ぐ等適切に対応します。

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や特性を考慮すべく、情報セキュリティ統括室が米州・欧州・アジアの各拠点の海外地域担当とより一層の連携を深めていきます。

*1 Computer Security Incident Response Team
*2 Product Security Incident Response Team。製品・サービスのセキュリティ品質に対する取組み
*3 CVE Numbering Authority、CVE採番機関。CVEとはCommon Vulnerabilities and Exposuresの略
*4 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)

個人情報保護

三菱電機では、2001年10月に「個人情報保護に関する規則」を制定の上、三菱電機従業員等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:個人情報保護マネジメントシステム—要求事項」に準拠した体制を構築・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事業者として認定を受け、プライバシーマークを取得しました。2024年1月には、8回目の更新手続きを完了しています。

個人情報保護方針

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。その対策として、三菱電機グループではネットワークや端末、サーバー(クラウド)の一元管理と「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、最小化しています。

また、オフィスのほか、テレワークや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するように取り組んでいます。