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 2025

目次

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行っている情報セキュリティの取り組みについて、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

2024年度
(2024年4月1日～2025年3月31日)
2025年4月以降の方針や目標・計画等についても一部記載しています。

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

2025年10月発行

お問い合わせ先
三菱電機株式会社
デジタルイノベーション戦略室
IT・セキュリティガバナンスユニット
〒100-8310
東京都千代田区丸の内2-7-3　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

サイバー空間を守ってデジタルイノベーションを促進し、お客様の成長と多様化する社会課題の解決に貢献します。

三菱電機株式会社
専務執行役
CIO（情報セキュリティ担当）

武田　聡

AI活用やデータサイエンス、DXの進展が著しい一方で、サイバー攻撃の手口は巧妙化し、世界中で脅威が高まってきています。三菱電機グループは、国内外で幅広い事業を展開しており、サイバーセキュリティを重要な経営課題と認識して取り組んでいます。

三菱電機グループでは、お客様から得られたデータをデジタル空間に集約・分析するとともに、グループ内が強くつながり、知恵を出し合う事で新たな価値を生み出し、社会課題の解決をする「循環型　デジタル・エンジニアリング企業」となることを目指しています。そして、この変革を加速するため、DX・IT・セキュリティ関連組織を再編し、2025年4月1日にデジタルイノベーション事業本部及び三菱電機デジタルイノベーション株式会社を新設しました。

幅広い分野・領域で培った、大規模プロジェクトやグローバル対応の豊富な実績を活かした高度なインテグレーション力に加え、三菱電機グループの情報セキュリティ強化施策で得たノウハウを活かし、最新のデジタル技術を組合せ最適なソリューションサービスと、多様化するセキュリティリスクに対し、ITからOTまでの幅広いセキュリティの統合的対策とO＆M（Operation＆Maintenance）のフルレンジのサービスを提供します。

三菱電機グループに向けては、情報セキュリティ統括部門が牽引することにより、現在のセキュリティレベルの維持・向上に努めています。近年サイバー攻撃はさらに複雑化しており、お客様のセキュリティ対策に加え、製造分野などでのOTセキュリティの重要性も増してきているため、本対策として、2024年10月に事業部門（事業部・事業所）も含めたFSIRT体制を構築しました。これにより、情報セキュリティ（CSIRT※1）、製品セキュリティ（PSIRT※2）、工場セキュリティ（FSIRT※3）及び企業機密管理・個人情報保護の4本の柱にてお客様、株主・投資家・取引先の皆様、従業員など、様々なステークホルダーを支えてまいります。

また、グローバルに目を向けると欧州のNIS2指令やサイバーレジリエンス法をはじめとして、各国でセキュリティに関する法規制が強化されています。そのため、各国の法令動向を調査・分析し、必要な対策を講じていきます。そして、情報セキュリティ統括部門と事業部門、特に海外関係会社との連携を強化し、三菱電機グループ全体で法令を遵守するよう取り組んでいきます。

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。

※1 CSIRT：Computer Security Incident Response Team
※2 PSIRT：Product Security Incident Response Team
※3 FSIRT：Factory Security Incident Response Team

三菱電機グループのビジョン・戦略

近年、サイバー攻撃は高度化・巧妙化が加速しており、世界を脅かす見えざる脅威になっています。私たちは、国境を越えたチームワークでこの脅威に立ち向かい、健全なサイバー空間を守ってデジタルイノベーションを促進し、活力とゆとりある社会の実現を目指します。そして、三菱電機が掲げている「循環型デジタル・エンジニアリング企業」への変革に向けて、お客様の重要なデータやシステムを守るため、製品・システムのライフサイクル全体にわたるセキュリティ対策を講じ、顧客の安心・安全を確保し、持続可能な社会の実現に貢献していきます。サイバー攻撃は日々進化しているため、現在推進している施策にて三菱電機グループのサイバーセキュリティ対策が完了するわけではありません。最新の攻撃動向や法令の変化を常に監視し、セキュリティ対策に継続して取り組んでいます。

ワンストップセキュリティソリューション

三菱電機グループのセキュリティ強化に向けた取り組みでは、三菱電機グループ向けに推進している企画・統括部門と、お客様向けに、製品やサービスを安心・安全に導く取り組みを行っているセキュリティ事業部門があります。2025年4月の組織再編によって、この両部門の連携を強化しています。それぞれの部門が持っている強みである、情報セキュリティ、工場セキュリティ、製品セキュリティ、セキュリティガバナンス、監視・運用、コンサルティングの技術を融合し、ワンストップセキュリティソリューションとして提供していきます。

グローバル人財育成

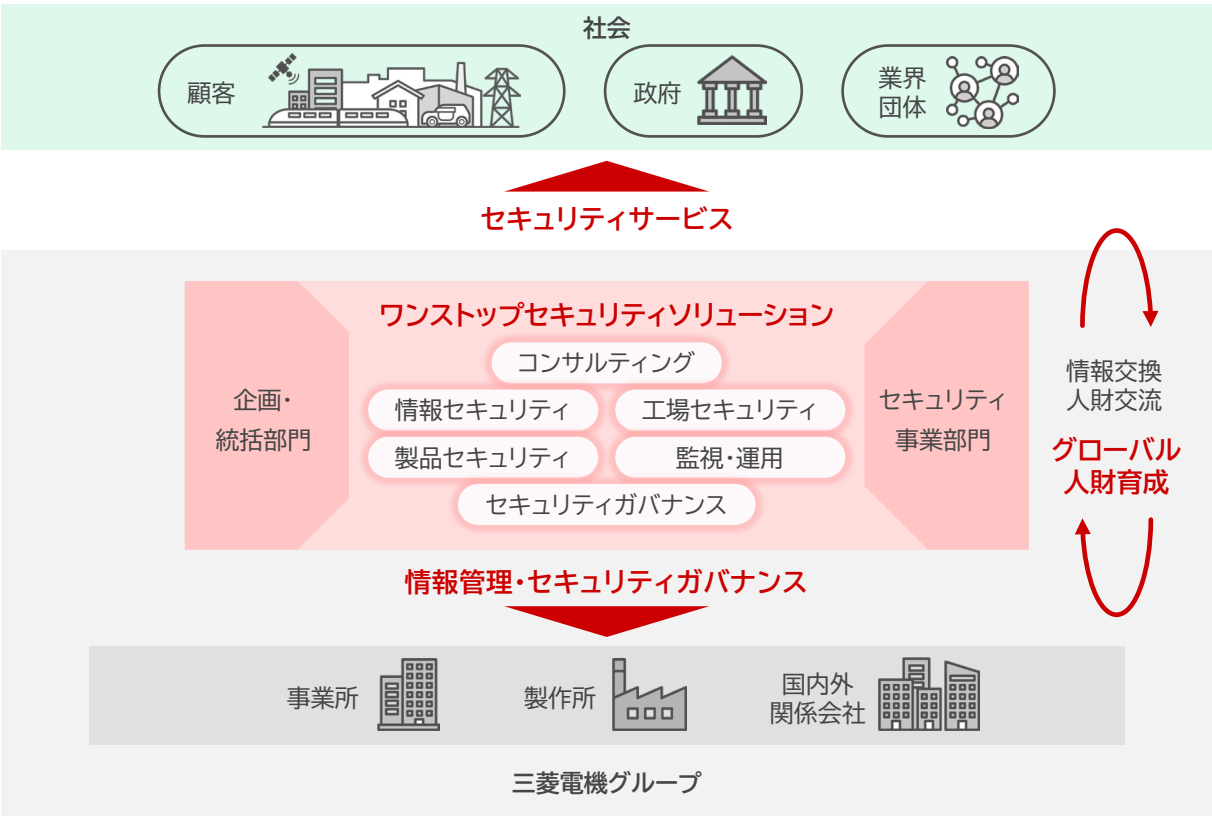
グローバルに展開している様々な事業を安全に進めるために、セキュリティ対策を推進する人財の育成が非常に重要であると考えています。それぞれの立場や役割に応じた情報管理・セキュリティ人財育成プログラムを用意して受講を進めています。また、三菱電機グループ内のグローバルなローテーションの活性化、産学官での人財交流も積極的に行っています。

情報管理・セキュリティガバナンス

三菱電機グループ全体が一体化して施策を進めるため、体制や役割を明確化し、高度化・巧妙化が加速するサイバー攻撃への対策とデータ利活用の両立を、効果的かつ効率的に牽引・支援していきます。そのために、最新の脅威を踏まえ、リスクの大きさや優先度に応じた柔軟で実効性の高いセキュリティ対策を進めます。

セキュリティサービス

三菱電機グループの情報セキュリティ強化施策の成果を活かしたIT/OT/製品のワンストップセキュリティソリューションにより、サプライチェーンセキュリティの安全・安心に貢献していきます。幅広いセキュリティの統合的な対策と立案、高度なセキュリティ対応力により、お客様の不安や不満を全面的に解決するパートナーを目指します。



情報セキュリティマネジメント

情報セキュリティの基本方針

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・運営体制等のガバナンスの継続的な強化に取り組んでいます。

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。

企業機密管理宣言

当社グループ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を含む企業機密が万一漏えいすれば、当社グループ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グループが完遂すべき社会的責任の1つであると認識し、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。

なお、企業機密とは、当社グループ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、当社グループ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（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。

1. 法令・規則遵守による企業機密の適正な管理
   当社グループは、事業活動に関連するすべての企業機密を、法令及び当社グループの規則に従い適正に管理します。
2. 安全管理措置の徹底
   当社グループは、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
   当社グループは、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
   当社グループは、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グループの取組につき、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
   当社グループは、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　2025年5月26日
三菱電機株式会社
執行役社長　漆間　啓

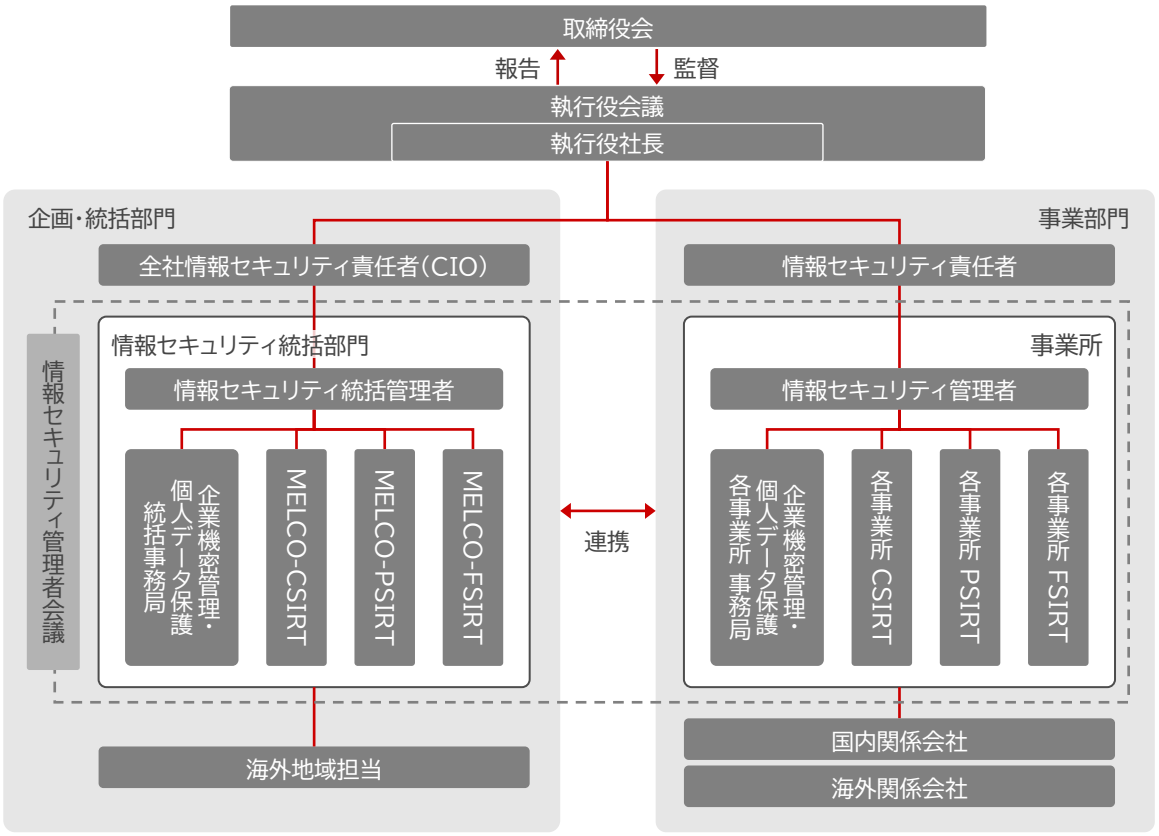
情報セキュリティの体制

三菱電機グループの情報セキュリティ体制は、執行役社長を情報セキュリティ管理に関する最高責任者とし、情報セキュリティ管理を企画・統括する部門と事業活動において情報セキュリティに関わるリスクを所有し責任を持つ事業部門から構成されています。企画・統括部門では、全社情報セキュリティ責任者に任命された情報セキュリティ担当執行役が、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管理者がその指示のもと、顧客のサプライチェーン要求事項や遵守すべき国際規準・慣行等に対して適切な対応を進めるとともに、活動内容について定期的に報告します。事業部門では、情報セキュリティ責任者のもと、情報セキュリティ管理者が傘下の関係会社を含めた自部門に関する情報セキュリティを管理します。

全社情報セキュリティ責任者が定期的に開催する情報セキュリティ管理者会議では、情報セキュリティ管理者に対して三菱電機グループ全体の情報セキュリティ方針の策定や施策の企画等について展開・連携します。

各部門に、情報管理、CSIRT、PSIRT、FSIRTの機能を持たせ、情報セキュリティ統括部門が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り組みに関して企画・推進しています。また、インシデント発生時には事業部門と連携し、事業状況を踏まえた総合的な状況判断のもと、迅速に意思決定を行い、インシデント対応を進めます。

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部門が米州・欧州・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。



MELCO:Mitsubishi Electric Corporation

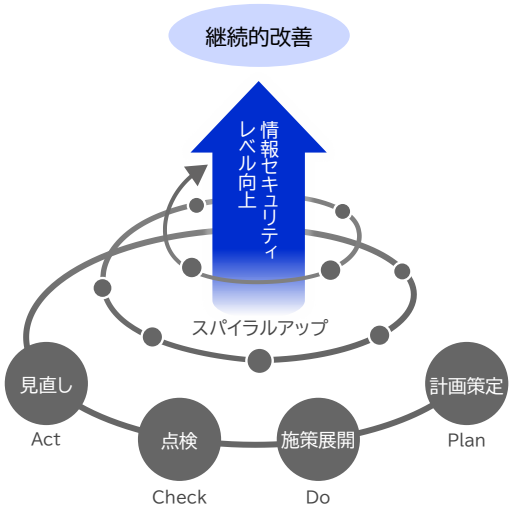
情報セキュリティ体制(三菱電機グループ)

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、海外における個人情報の取り扱いなどの外的環境も考慮して、組織的・人的・技術的・物理的からなる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点検(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

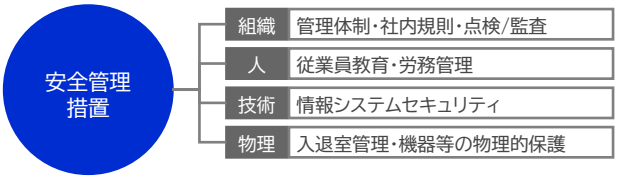
4つの安全管理措置

「組織的」安全管理措置は、管理体制、社内規則、点検/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、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。

「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。

「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。



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。また、日々変化するNIS2指令やサイバーレジリエンス法をはじめとする、グローバルなサイバーセキュリティ関連法令を定期的にモニタリングし、三菱電機グループ一丸となって対応を進めています。

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自国の法令、適用を受ける第三国・地域の法令の遵守はもとより、三菱電機グループにおける共通のガイドラインを関係会社に対しても適用し、個人情報を適切に取り扱い、グローバルレベルで保護します。

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
	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
	物理的安全管理措置	物理セキュリティガイドライン

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。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1回、eラーニングで実施し、三菱電機の方針、情報漏えい事案の概況、個人情報保護関連法令、不正競争防止法、一人一人が認識すべき安全管理措置(組織的・人的・技術的・物理的)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、新任課長、個人情報資産管理者、運営に関わる事務局向けの研修などを通して、各階層や担当業務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、アジア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案の事例について教育しています。

三菱電機グループの個人情報保護への取り組み

基本姿勢

三菱電機グループは、企業理念を「私たち三菱電機グループは、たゆまぬ技術革新と限りない創造力により、活力とゆとりある社会の実現に貢献します」と定め、様々な事業を展開しています。私たちは、お客様、株主・投資家、取引先、従業員など、様々なステークホルダーから貴重な情報をお預かりしています。その中でも、個人情報等は特に重要な財産のひとつであり、私たちは個人情報を適切に取り扱うことを社会的責務と考えています。

三菱電機グループは、各国・地域の法律に基づいた8つの原則に従って個人情報を取り扱い、体制の確立と適切な取り組みによって改善・維持に努めています。

個人情報の取り扱いに関する原則

三菱電機グループでは、お客様からお預かりした大切な個人情報を以下の原則に従って取り扱います。

(1)適法性の原則:関係法令に従い、適切に個人情報を取得し、取り扱います。

(2)公平性及び透明性の原則:個人情報の取り扱いについて、お客様の観点に立って適切なタイミングで、容易な手段を用いて分かり易くお知らせします。

(3)取り扱い目的の制限の原則:明確かつ適法な目的の下で個人情報を取得し、その目的の範囲内において取り扱います。

(4)データの最小化の原則:取り扱い目的の範囲において必要なものに限定して個人情報を取り扱います。

(5)正確性の原則:可能な限り個人情報を正確に保ちます。必要な場合にはデータを更新します。

(6)保存制限の原則:取り扱い目的に応じて定めた必要な保存期間の中で個人情報を取り扱い、保存期間が終了した際には、適切な方法で削除します。

(7)完全性及び機密性の原則:不正アクセスや紛失、破壊、改ざん、漏えいなどから保護するために、個人情報に対して必要なセキュリティ対策を講じます。

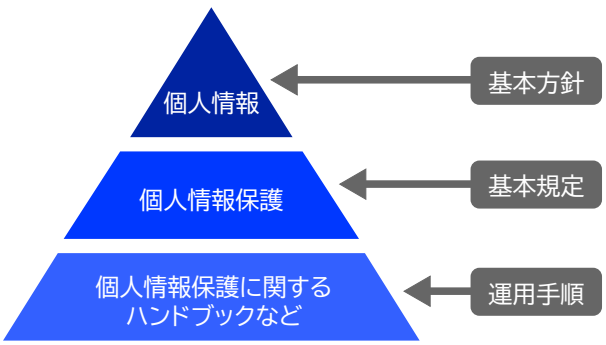
(8)企画段階でのプライバシー保護の原則:個人情報を取り扱う企画の段階から、上記の原則を遵守するために保護措置を講じます。

三菱電機の個人情報保護の取り組み

個人情報保護マネジメントシステムの構築

三菱電機では、「個人情報保護方針」及び「個人情報の保護に関する規則」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。

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、「JIS Q 15001: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P23「第三者評価・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一般データ保護規則(GDPR※1:2018年5月施行)や中国個人情報保護法(2021年11月1日施行)等、三菱電機において各国・地域法が定義する個人情報を移転、取り扱う場合には当該国・地域法令の要求に従い、適切に保護します。

※1 GDPR:General Data Protection Regulation

その他の施策

取引先・委託先管理

企業機密・個人情報を他社に委託する際は、適切に秘密保持契約を締結した上で、セキュリティ・個人情報保護上の理由から取引・委託先に求める事項を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下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。

AIでの予兆検知による漏えい対策

経済安全保障の観点及び企業競争力維持の観点から、重要な情報の保護への重要性が高まる中、「人を介した情報漏えい」への対策強化が一層必要とされています。

従業員の職務環境の安心・安全を確保し、当社技術情報・資産の保全を強化するため、AIを活用したメール確認など予兆検知型の漏えい対策を導入しています。

サイバーセキュリティに対する取り組み

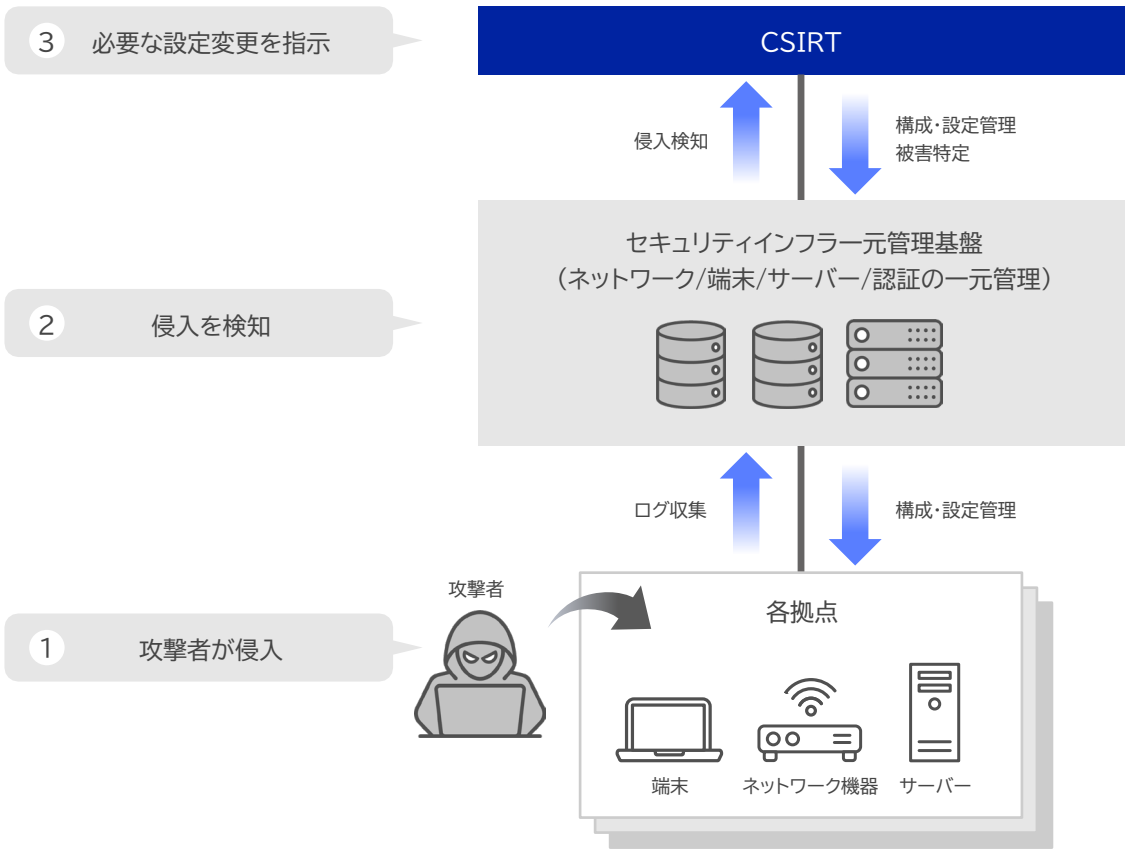
三菱電機グループでは、情報セキュリティに対する取り組みとして、ITインフラのサイバー攻撃対策や物理的なセキュリティ対策を行っております。

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。

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。



セキュリティー元管理

多層防御

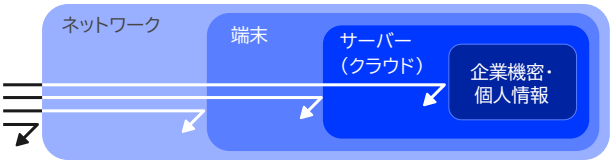
三菱電機グループでは、「多層防御」として「ネットワーク」、「端末」、「サーバー(クラウド)」の3階層の技術的なセキュリティ対策を実施しています。

ネットワークでのセキュリティ対策では、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、社内への不正アクセスやマルウエアの侵入を遮断し、外部への情報漏えいを防止しています。さらに社内ネットワークでは端末とサーバー間、異なる製作所間での通信を厳密に制御・管理することで、被害の局所化に努めており、今後もこれらの対策を強化していきます。

端末のセキュリティ対策では、端末へのマルウエア感染を防ぐために、端末を一元的に管理し、マルウェア対策ソフトによるマルウェア検知・駆除や、ソフトウエアの脆弱性を修正するセキュリティパッチの適用を徹底しています。また、不審なふるまいを検知する機能(EDR※1)を全端末に配備し、対策を強化しています。さらに、情報システムにアクセスする際には2つ以上の要素の認証を組み合わせる多要素認証(端末認証)を導入し、セキュリティ対策を強固にしています。

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。



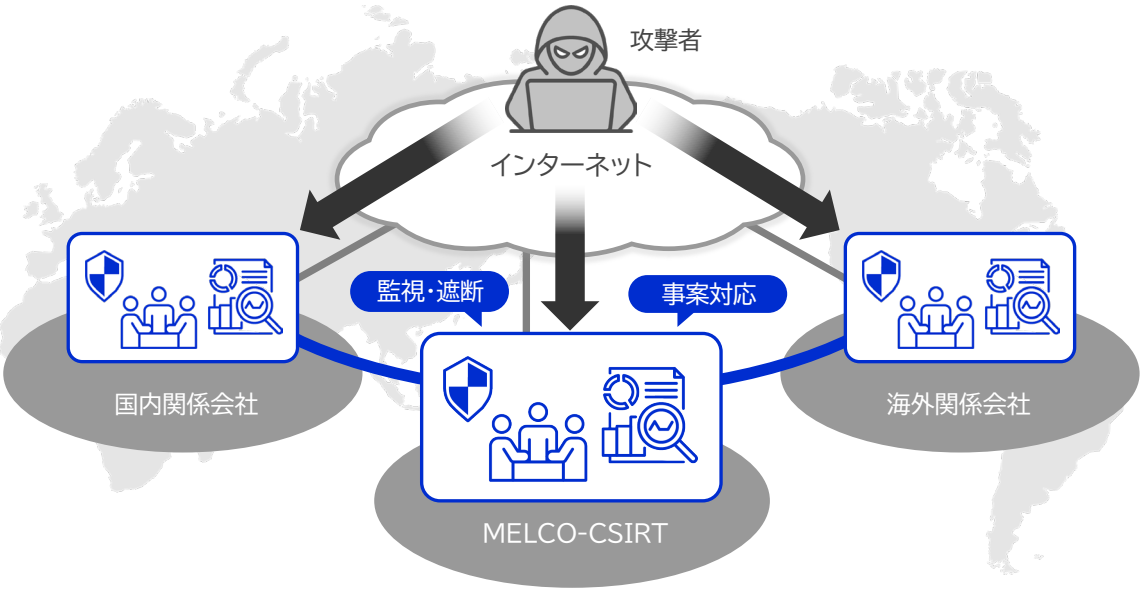
多層防御

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。前述の通信監視により不審な挙動を検知することでサイバー攻撃をいち早く見つけ、遮断します。また、端末側では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、事案が発生した場合は、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、迅速で適切な対処・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。

※1 EDR:Endpoint Detection and Response



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。

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。そのため、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、サイバー攻撃から防御するためのセキュリティ対策に引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案を契機に、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公開するように取り組んでいます。

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。

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

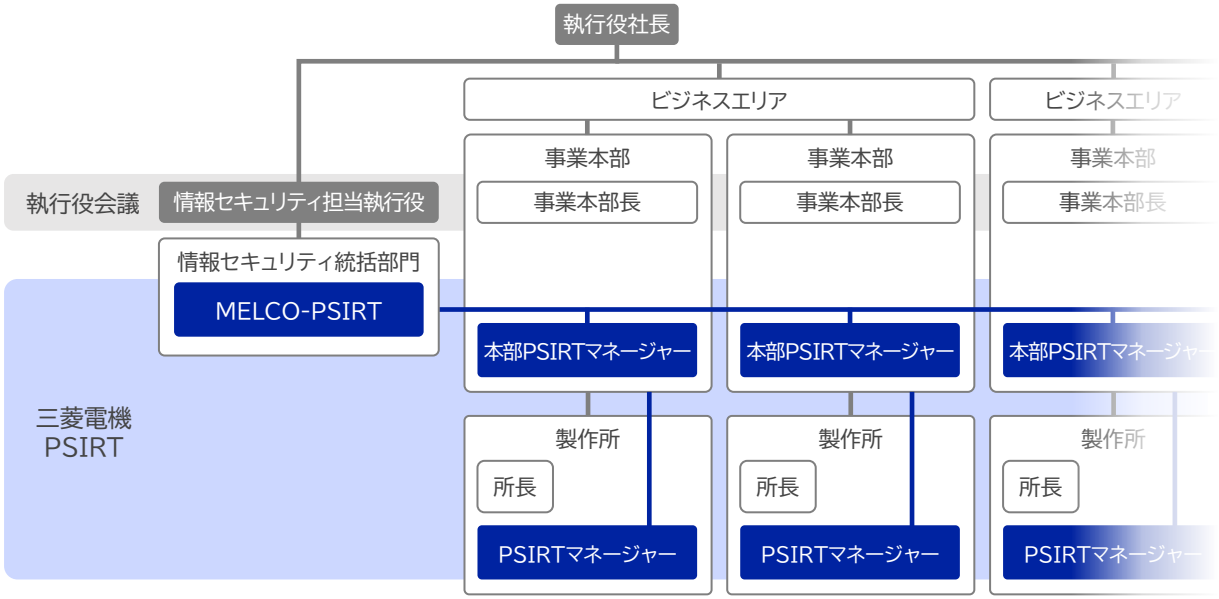
三菱電機では、製品・サービスのセキュリティ品質に対応する社内の体制として三菱電機PSIRT（Product Security Incident Response Team）を構築し、製品・サービスの情報セキュリティに対し全社で取り組んでいます。

三菱電機PSIRTは、右記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・開発手法の導入を推進
- 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、本社に対外的な窓口となるMELCO-PSIRT(Mitsubishi Electric Corporation Product Security Incident Response Team)を設置し、各事業本部に本部PSIRTマネージャーを配置し、さらに全ての製作所にPSIRTマネージャーを配置して、全社で製品・サービスのセキュリティ品質に対して取り組んでいます。



三菱電機PSIRTの体制図

製品セキュリティに関わる法令対応

近年、デジタル化の進展に伴い、サイバー攻撃による社会への影響が増大していることから、EUのCyber Resilience Actを始め、各国で製品のセキュリティ対応を求める法規制が強化されています。三菱電機では、製品・サービスのセキュリティ品質への対応に加えて、各国の法令要件を遵守すべく、事業横断で対応に取り組んでいます。

工場(OTセキュリティ)に対する取り組み

OTセキュリティ対策の推進

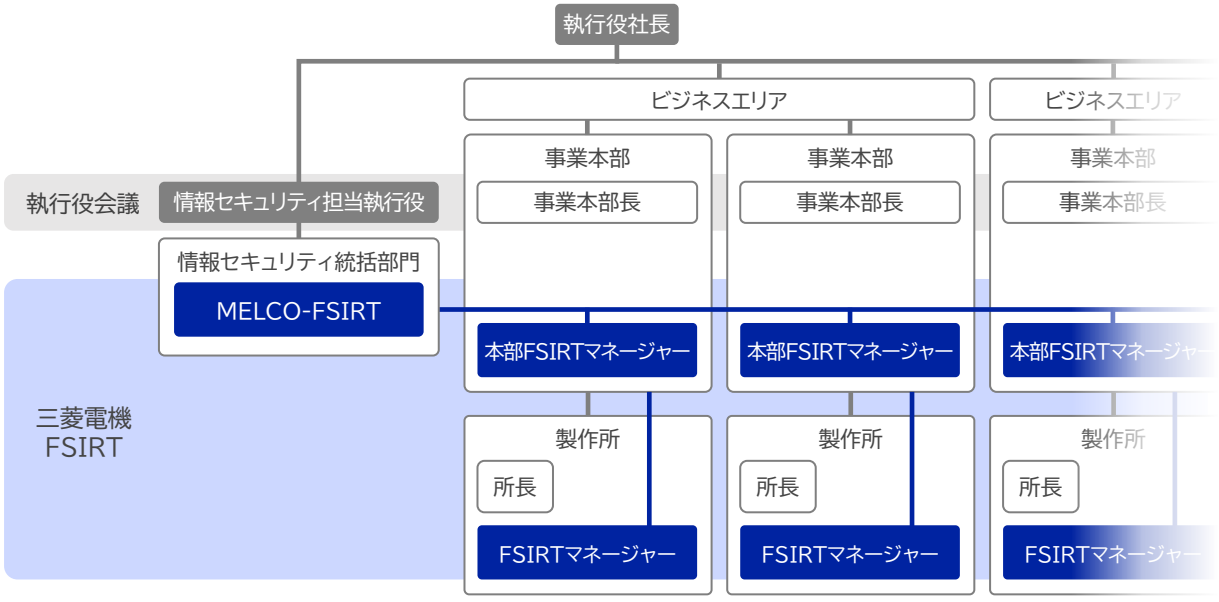
インターネットなど外部との接点を持たずクローズした環境で稼働していた工場の現場にも、IoTやDX、テレワークといった様々な新技術、環境変化の流れが押し寄せてきており、工場もオープンな環境で稼働するようになってきました。

その結果、今まで無縁だったサイバー攻撃の脅威が工場にまで及び、工場停止など重大な被害が近年多発しています。

当社では、三菱電機FSIRT(Factory Security Incident Response Team)を構築し、当社グループの工場に対するサイバーセキュリティ対策の強化に全社で取り組んでいます。三菱電機FSIRTは、情報セキュリティ統括部門内に組織するMELCO-FSIRT(Mitsubishi Electric Corporation Factory Security Incident Response Team)、各事業本部に配置する本部FSIRTマネージャー、各製作所に配置するFSIRTマネージャーにより構成されます。

各組織の役割としては、MELCO-FSIRTが全体統括を担い、全社で発生した問題解決を支援します。また、その対応をとおして得た知見やノウハウを蓄積し、全社の取り組みを改善します。FSIRTマネージャーはMELCO-FSIRTと連携し、製作所内の関係部門をとりまとめます。平時では自組織の状況に合わせ、対策の検討と推進を担い、有事ではインシデント対応を主導します。本部FSIRTマネージャーもMELCO-FSIRTと連携し、インシデントが発生した製作所の後方支援を行います。また事業本部が管轄する関係会社のOTセキュリティに関わる業務をとりまとめます。

各組織は、平時・有事で組織間連携ができる体制としており、OTセキュリティ対策を当社として適切かつ円滑に推進できるよう活動しています。



三菱電機FSIRTの体制図

OTセキュリティソリューションとの連携

当社グループ向けのOTセキュリティ対策推進活動において、実際に当社グループの製作所に技術的対策を導入しております。導入や運用で出てきた様々な課題は現場の部門と連携しながら解決してきました。得られたノウハウなどは、お客様向けのOTセキュリティソリューションにも活用できるよう取り組んでいます。詳しくは、本誌の「OTセキュリティソリューション」の内容をご参照ください。

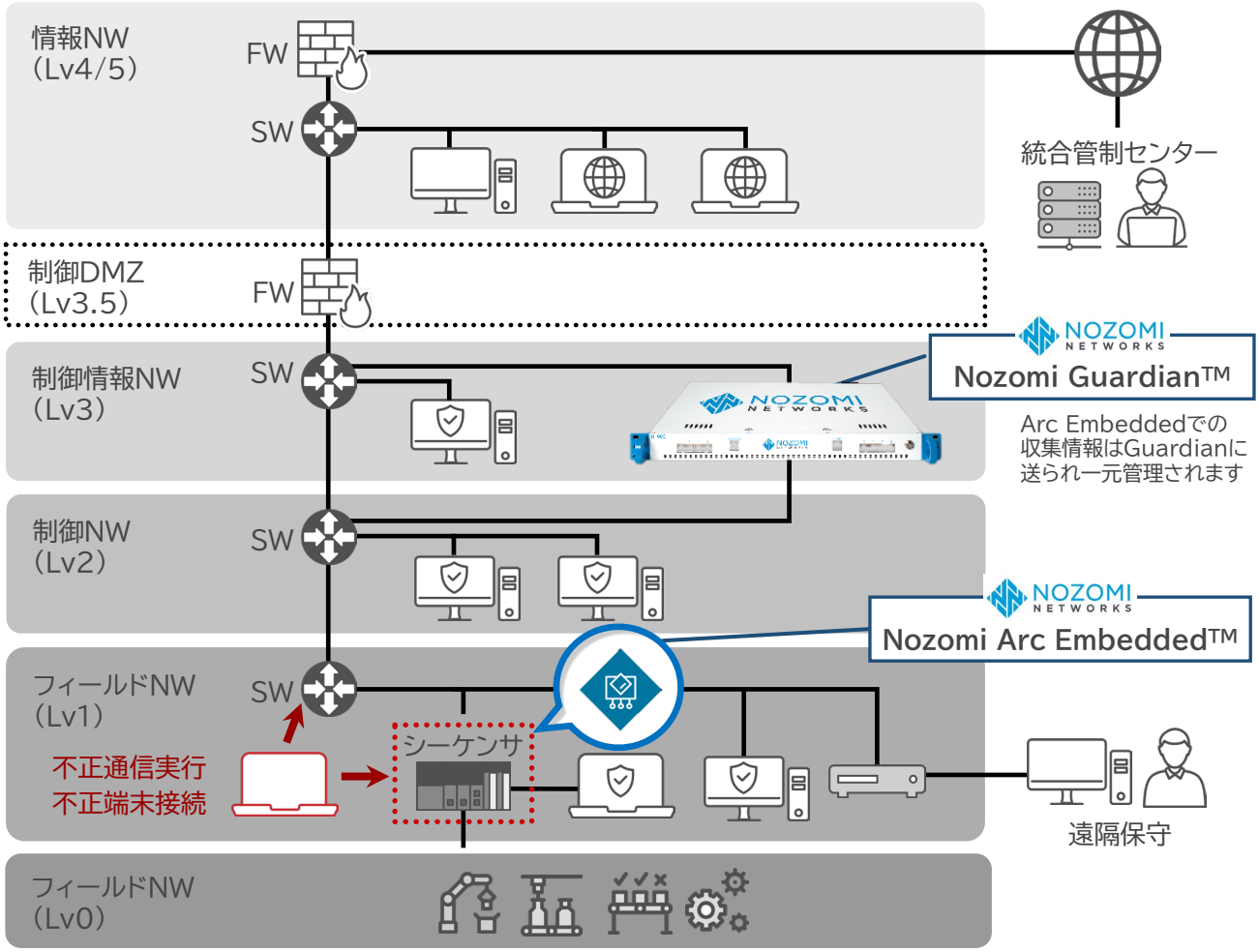
情報セキュリティソリューションの提供

OTセキュリティソリューション

製造現場や社会インフラのIoT化に伴い、OTセキュリティ対策の重要性が増しています。OTセキュリティにおいては、システムがシーケンサやロボットなどの多種多様な制御機器で構成されているため全体の把握が難しいこと、データの盗聴・漏えい対策に加えてシステムの連続稼働が重視されることから、ITセキュリティのような一律の対策適用や異常検出時のシステム停止・切り離しが容易にできない難しさがあります。また、工場などの現場では、インターネットと接続せずクローズドな環境を維持することでセキュリティリスクを回避していたため、現場の資産やネットワークの可視化は十分に行われていませんでした。DXの先進企業ではITとOT環境の接続に伴い、その境界の可視化の重要性が認識されていますが、OT環境の深い層の可視化については多くの企業で本格的に着手されておらず、それを実現するソリューションも発展途上にあります。

これに対し、三菱電機は、自社のOTセキュリティ対策を通して蓄積した知見と、金融業界をはじめとする各分野向けに培ってきたITセキュリティ技術を融合し、「課題抽出・対策立案」→「対策導入」→「運用」のサイクルをワンストップで提供します。

特にOT環境の可視化については、 OTセキュリティソリューションを提供するNozomi Networks社（以下、Nozomi）の代表的な製品であるNozomi Guardianを活用したソリューションを顧客に提供するとともに、更なる精緻な現場の可視化を目指し、共同開発の「Nozomi Arc Embedded」をシーケンサMELSEC iQ-Rシリーズに搭載可能としました。



三菱電機が提供するOTセキュリティソリューション

三菱電機では、Nozomiの製品とOT及びIT両分野での豊富な経験を活用し、製品導入だけではなく、継続的に最適な運用が可能なソリューションを提供します。

OTネットワーク可視化・監視ソリューション

Nozomiの製品を導入することによりOTネットワークの詳細情報を一元的に収集・管理し、資産や脅威を可視化します。また、シーケンサの資産情報などを可視化するとともに、シーケンサに対する異常通信も検知します。

■ Nozomi Guardian

Nozomi Guardianは、OT環境向けのIDS※1製品です。ネットワークから得られる情報をもとに、

1. ネットワーク・構成機器可視化
2. 脆弱性・リスク管理
3. ネットワーク異常検知

の機能を提供します。

■ Nozomi Arc Embedded

Nozomi Arc Embeddedは、シーケンサに組み込まれたセキュリティセンサであり、以下の機能があります。

1. シーケンサの製品情報の取得(形名、型番、ファームウェアバージョン等)
2. シーケンサの通信モニタリング(シーケンサ通信相手識別、異常な通信検知)
3. シーケンサの内部状態変化の検知

これにより、シーケンサを中心とする深い層の資産や脅威をさらに可視化できます。

導入支援サービス

初期状態では多様なセキュリティアラートが検知されるために、現場に合わせたチューニングが必要です。当社工場内で培ったノウハウを活かし、機器の設計、構築、導入から、IDSの機能を最大限活用するために、現場に合わせて可視化範囲やアラートのチューニングを行います。ネットワークで発生しやすい各種アラートへの対応サポートサービスを提供します。

運用支援サービス

いつ狙われるか分からないサイバー攻撃に対しては、専門技術者による常時の監視が欠かせません。セキュリティ運用支援サービス(専門技術者による24時間365日監視)を活用いただくことで、お客様のセキュリティ運用をサポートします。

※1 IDS:Intrusion Detection System

マネージドセキュリティサービス

三菱電機デジタルイノベーション株式会社

リモートワークやDX化が進む一方で、サイバー攻撃の脅威は日々ますます拡大しており、攻撃リスクへの対策が急務となっています。そして、機器の監視・設定変更・脆弱性対応など日々の運用に加え、インシデント発生時には迅速な検知・対応が必要となり、より組織的な対応力と高い専門性が求められています。

当社は、セキュリティの診断から監視・運用に加え、インシデントの対応・復旧までNIST※1のサイバーセキュリティフレームワークで定義されるセキュリティサイクル全体をワンストップで支援する様々なサービスを提供します。お客様が対応することが困難なセキュリティ監視・運用は、SOC※2とCFC※3の 運用・サポートチームの強固な運用体制でご支援し、お客様のビジネスの安定的な発展に貢献します。

最適なセキュリティ対策をワンストップでご提供

お客様のセキュリティ要件に合わせ、最適なセキュリティ機器のご提案から構築、設定変更・稼働監視・保守対応などのセキュリティ維持のための日々の運用業務までをワンストップで対応します。

高度なセキュリティ監視

SOCの経験豊富なアナリストが24時間・365日体制でお客様の対応を支援します。複数の機器のログを組み合わせて攻撃の兆候を検出し、高度な標的型攻撃にも対応可能です。インシデントを検知した場合は、当社の専任技術者が影響範囲調査や推奨対策の提示を行い、お客様のインシデント対応を支援します。

セキュリティ対策の維持・運用支援

ネットワーク診断サービスやWeb/スマートフォンアプリ診断サービスにて、お客様システムに内在する脆弱性を診断します。また、脆弱性情報提供サービスにて日々公開される多数の脆弱性情報の中から日次でお客様システムに影響のある脆弱性をお知らせすることで、手間のかかる情報収集・影響判断運用をお任せいただけます。

※1 NIST:National Institute of Standards and Technology（米国国立標準技術研究所）
※2 SOC:Security Operation Center
※3 CFC:Cyber Fusion Center

CyberMinder XSIRT

サイバー攻撃の被害拡大を抑制し、早期復旧を行う支援サービス
専門家が、詳細調査から復旧まで一貫して対応を支援します。

- CSIRT運用支援
- フォレンジック調査
- 個別運用対応

CyberMinder IoT

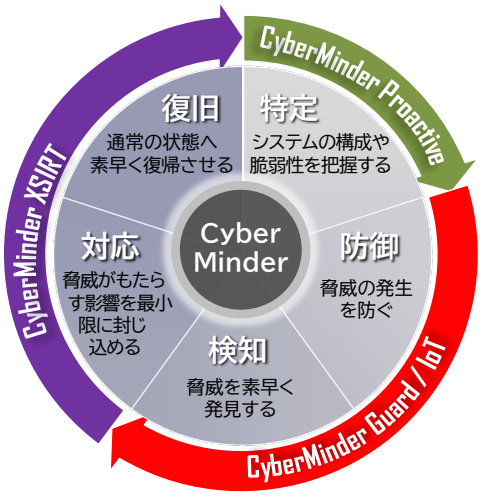
制御系システム・製造現場向けのネットワークセキュリティサービス
お客様の製造工場の状況に合わせ 最適なセキュリティ施策を提案します。

- Firewall-UTM構築・運用
- 通信可視化
- ホワイトリスト型通信制御
- 持込媒体セキュリティ対策
- 不正端末接続制御
- OTセキュリティアセスメント

CyberMinder Proactive

脆弱性診断や従業員の訓練など、サイバー攻撃を未然に抑制するサービス
リスクを低減させ、お客様の環境を守ります。

- ネットワークセキュリティ診断
- Web/スマホアプリ診断
- ペネトレーションテスト
- 脆弱性情報提供
- 標的型メール訓練
- 脆弱性管理
- 標的型攻撃対策訓練・教育



CyberMinder Guard

お客様の業務環境全体をカバーするセキュリティサービス
お客様の環境や情報資産を保護する製品の導入と監視運用を提供します。

- クラウドWAF
- マネージドSASE
- クラウドセキュリティ
- 標的型攻撃対策
- SWGセキュリティ監視
- Firewall-UTM構築・運用
- 不正アクセス監視
- マネージドNDR
- マネージドEDR

セキュリティサービス CyberMinder

セキュリティログ分析サービス

三菱電機デジタルイノベーション株式会社

近年、加速度的に増大し高度化するサイバー攻撃が企業経営の大きなリスクとなっています。特に、標的型攻撃のような巧妙な脅威には、多様なログを統合的に分析するSIEM※1の活用と、攻撃の兆候を捉える高度な検知ルールの整備が重要です。一方で、SIEMの導入・運用にはコストや技術的な複雑さが伴うため、導入を躊躇する企業も少なくありません。当社は、SIEM導入支援を強化するとともに、「標的型攻撃対策サービス」との連携による高度なセキュリティ運用監視の実現にも対応しました。SIEMとSOCを組み合わせることで、包括的で強固なセキュリティ対策をワンストップで提供します。

多様なログ形式に対応したSIEMの安定運用が可能

SIEM市場で長年高いシェアを誇り、多様なログ形式に対応可能なSplunk LLC（以下「Splunk社」）のSplunk Cloud（以下「Splunkソフトウエア」）を採用しています。SaaS提供によるお客様の導入負荷軽減に加え、当社のSplunk技術者が基盤モニタリングを行い、SIEM基盤の運用支援を行います。例えば、契約ログ量の超過状況を継続的に監視することで、利用料の適正化に貢献します。これにより、SIEM基盤の運用効率が向上し、安定したセキュリティ運用が可能となります。

※1 SIEM:Security Information and Event Management
（収集したログのリアルタイム分析、検知アラート、レポート出力などにより異常を分かりやすく可視化する仕組み）

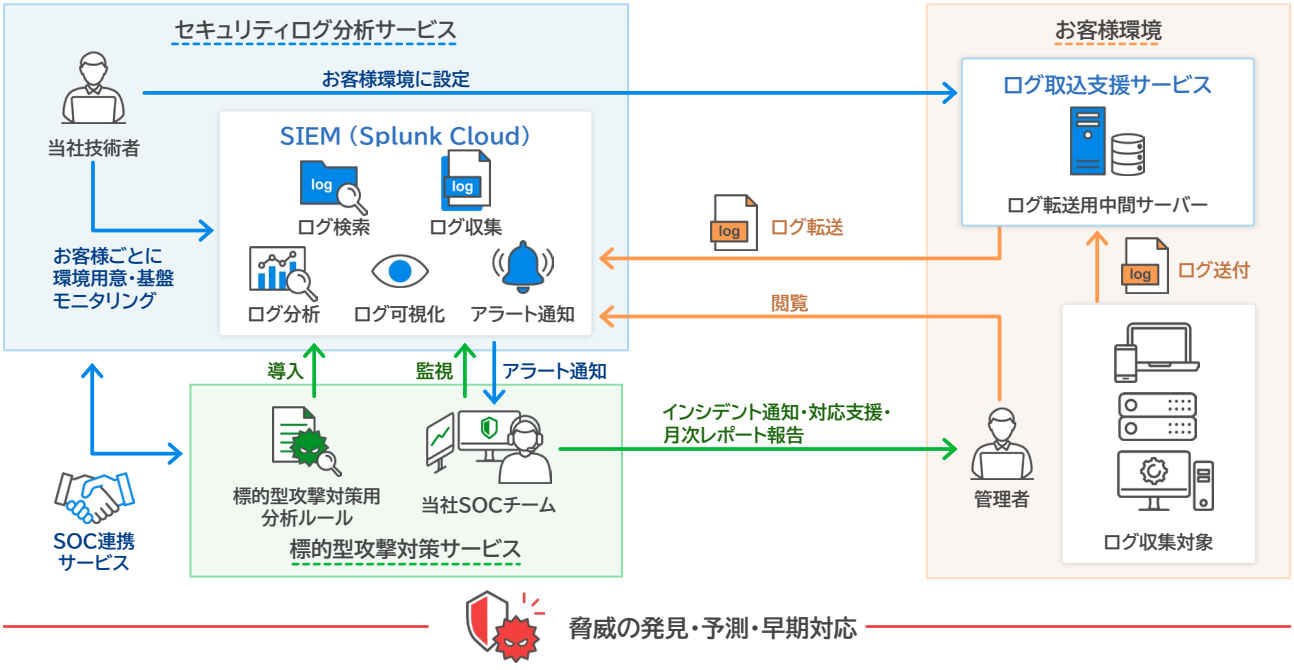
Splunkソフトウエアへのログ取り込みを支援

SIEM導入時に課題となるログ取り込みを支援するオプションサービスを提供します。お客様環境のログ転送用の中間サーバーに、Splunk Heavy Forwarderと呼ばれるクライアントソフトウエアを導入・設定することで、ログのフィルタリングや変換が可能となり、取込むログ量を調整できます。これにより、Splunkソフトウエアの利用料軽減に繋がります。

「標的型攻撃対策サービス」との連携による高度なセキュリティ運用監視の実現

「標的型攻撃対策サービス」の提供を通じて培った高度な検知ルールを、セキュリティログ分析サービスのSIEMに取り込むことで、標的型攻撃の検知が可能になります。これにより、お客様は従来のセキュリティ対策では見逃されがちな巧妙な攻撃を早期に把握し、被害の拡大を未然に防ぐことが可能です。さらに、検知されたインシデントに対して、当社SOCが、24時間365日体制で運用監視します。25年以上の運用実績を持つ当社SOCでは、専門アナリストがセキュリティインシデントを継続的に監視・分析し、お客様のインシデント対応力の向上を支援します。

今後、Splunk技術に関するノウハウをもとに、さらなる支援サービスを展開することで、高度化する脅威への対策強化を支援します。



セキュリティログ分析サービス　利用イメージ

研究開発

三菱電機では、安定した社会活動を継続可能にするために、当社製品やサービスのセキュリティ向上に向けた研究開発に取り組んでいます。昨今、課題となっている内部脅威による情報漏えいや、システムに組み込まれたセンサーへのサイバー攻撃に対する研究を紹介します。

おとりを用いた内部犯検知システム

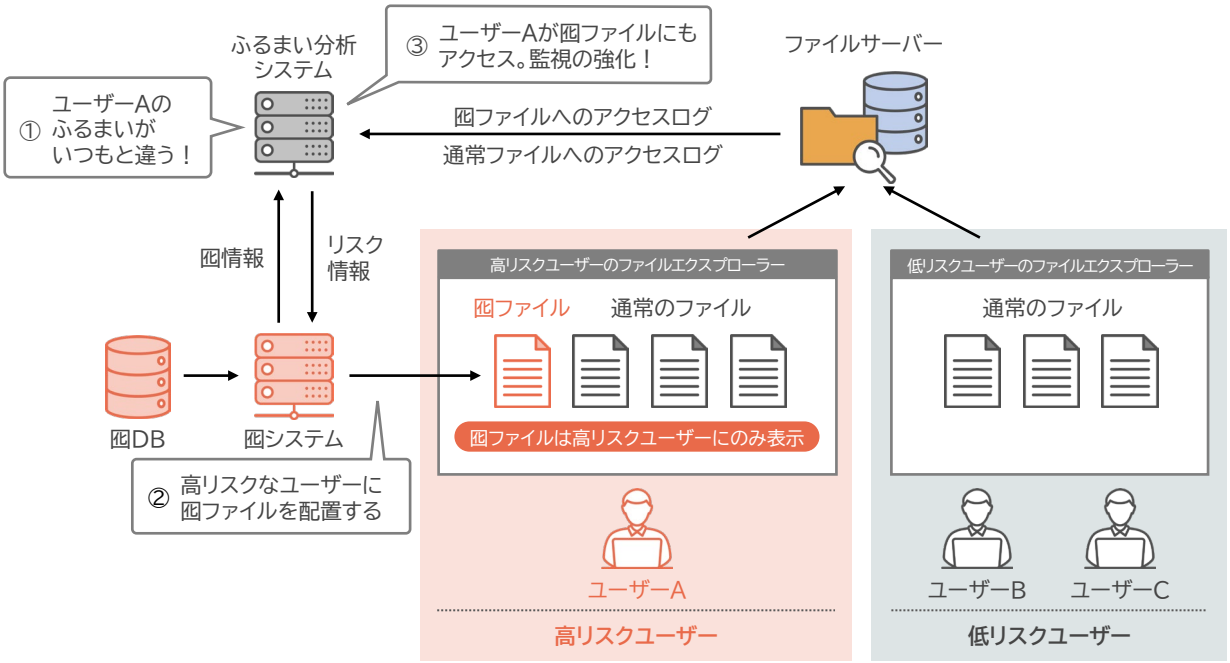
サイバー攻撃による情報漏えいへの対策が課題だと言われていますが、内部犯による情報漏えいも数多く発生しています。内部犯は正規の権限を有する悪意を持ったユーザーであるため、認証されたユーザーを信用する従来のセキュリティ対策では、その兆候を捉えることが難しいという課題があります。

そこで、三菱電機では、受動的に観測できる情報から内部犯と正規ユーザーとを切り分けるのではなく、内部犯が積極的に行うであろう行為を防御側が能動的に誘発させることで、内部犯の悪意を顕在化させて、おとり(囮)を用いて悪意に関連する行為を観測するというアプローチを採用しました。悪意を持ったユーザーにとって興味を引きそうな囮ファイルを動的に配置し、ファイルへのアクセス傾向を基に内部犯を絞り込むというのが、提案方式のコンセプトです。そして、この提案方式の試作を行い実現可能性を示しました。

本手法では、ふるまい分析システムでファイルアクセスのログなどを分析し、ふるまいの異常をリスク値として算出、リスクが高いユーザーを特定するとともに、ファイルのアクセス状況からそのユーザーが興味をひくトピックを推測しておきます。そして、リスクの高いユーザーに対して、興味をひくトピックに関連した魅力的な囮のファイルを動的に表示し、ファイルへのアクセス状況の監視を強化します。囮ファイルへのアクセスの状況をリスク値へフィードバックすることで、内部犯の候補として絞り込んでいきます。

高リスクのユーザーに絞って囮ファイルを配置することで、普段どおりの業務をしている正規ユーザーへの業務阻害を軽減することができます。万が一、正規ユーザーが高リスクと判定されて囮ファイルが配置されたとしても、普段使っているファイル以外へは積極的にアクセスすることは無いと考えられ、業務阻害の可能性は低いと期待されます。

参考文献：山本　匠他、“おとりを用いた内部犯検知システムの提案”、SCIS2024



提案方式の概要

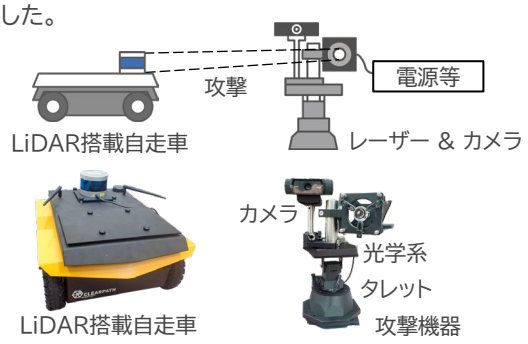
自律走行車用LiDARへの妨害攻撃が及ぼす影響評価

レーザーによって周囲環境を測定するLiDAR※1は、自己位置の推定と3D地図生成を行うSLAM※2技術と組み合わせて、安心安全な自律走行の実現に大きく寄与しています。計測セキュリティの分野では、センサーデータの取得時点のセキュリティを確保するため、LiDARへの妨害攻撃によって、LiDARから得られる情報がどのように変化するかの評価と対策の研究が進められています。

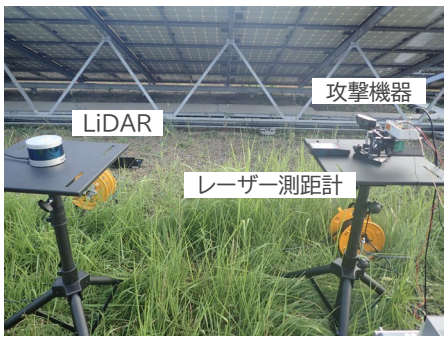
今回、LiDARの物体検出において検知されない後方からのレーザー照射に着目した妨害攻撃によって、SLAMの地図生成処理が重大な影響を受け、自律走行車が誤った経路を走行する可能性があることを、妨害攻撃実験及びシミュレーションで明らかにしました。

妨害攻撃実験とシミュレーション

屋内、屋外での2つの妨害攻撃実験にて実世界での攻撃の制約やセンサー信号処理への影響を算出し、その結果をシミュレーターに反映させてLiDARへの意図的な攻撃を再現しました。その結果、自己位置に誤差が生じ、自律走行車が車線から逸脱する軌道計画が作成されることが確認できました。

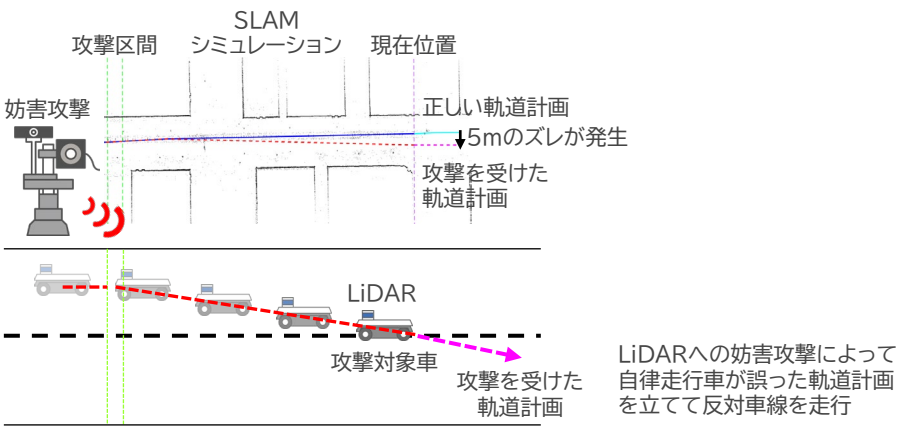


屋内照射攻撃実験



屋外照射攻撃実験

妨害攻撃実験の様子



シミュレーション結果

妨害攻撃への対策

このような妨害攻撃への対策として、①二次センサーの活用、②360°全方位の物体検出、③ハードウェアに関する防御が挙げられます。

今後の取り組み

今回のシミュレーションは特定の場面に限定されており、今後更に妨害攻撃への堅牢性を評価するには、傾斜のない平坦なエリアなど他の設定での攻撃に対する検証が必要です。

当社では、このシミュレーション結果に基づいて、LiDARへの妨害攻撃に対する有効な対策を検討し、さらに安心安全な自律走行の実現に貢献します。

※1 LiDAR:Light Detection and Ranging
※2 SLAM:Simultaneous Localization and Mapping

参考文献:Fukunaga, M., et al.: Random Spoofing Attack against LiDAR−Based Scan Matching SLAM

第三者評価・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（2025年4月1日現在）	
三菱電機株式会社	三菱電機デジタルイノベーション株式会社
株式会社アイプラネット	三菱電機ソフトウエア株式会社
エムビーテクノ株式会社	三菱電機フィナンシャルソリューションズ株式会社
株式会社ダイヤモンドパーソネル	三菱電機保険サービス株式会社
株式会社ビーシーシー	メルテック・ビジネス株式会社

ISMS認証取得状況

ISMS※1認証取得状況（2025年4月1日現在）	
三菱電機株式会社（神戸製作所横浜地区）	
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）	
三菱電機デジタルイノベーション株式会社（芝浦事務所）	
三菱電機デジタルイノベーション株式会社（三田事務所（株式会社テクノウェア含む））	
三菱電機デジタルイノベーション株式会社（中野事務所（エムビーテクノ株式会社含む））	
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）	
三菱電機ソフトウエア株式会社（電子システム事業統括部）	
三菱電機システムサービス株式会社（第3本部）	
三菱電機プラントエンジニアリング株式会社（24時間オンコールサービス、西日本本部、技術管理部）	
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
三菱電機ディフェンス＆スペースステクノロジーズ株式会社（東部事業部（鎌倉地区、北海道工場））	
三菱電機ディフェンス＆スペースステクノロジーズ株式会社（西部事業部（三田地区、伊丹地区、岩国地区、沖縄地区））	
通菱テクニカ株式会社	
株式会社ビーシーシー	

※1 ISMS：Information Security Management System

三菱電機株式会社
www.MitsubishiElectric.co.jp