

情報セキュリティ

基本的な考え方

太陽誘電は、情報セキュリティを事業継続および中長期的な企業価値の維持・向上に関わる重要な経営課題の一つとして位置付けています。情報セキュリティ方針の下、グローバルな管理体制を構築し、全社的な取り組みを推進しています。

情報セキュリティ方針

[情報セキュリティ方針](#)

戦略

太陽誘電では製造プロセスや技術情報を始めとする各種情報資産、並びに顧客情報を競争優位の源泉となる重要資産と位置付け、リスクに応じた適切な管理・保護を行っています。

特に生産現場におけるサイバーリスクは製品の安定供給や品質に直結することから、生産設備を含むOT領域※において多層的なセキュリティ対策を講じ、製造基盤のレジリエンス強化に取り組んでいます。

※ OT:Operational Technology(運用技術)。工場などの現場で設備や生産プロセスを監視・制御する領域。

情報セキュリティ認証

国内の統括拠点(本社および高崎グローバルセンター)にて取得していた「ISO/IEC 27001」認証を、2026年6月までに国内営業拠点5カ所および海外販売子会社6社へ拡大しました。また、TISAX認証を太陽誘電本社および玉村工場の2カ所で取得しました。

推進体制

責任者として情報セキュリティ担当役員(CISO)が、全社の情報セキュリティ施策およびインシデント対応を統括しています。

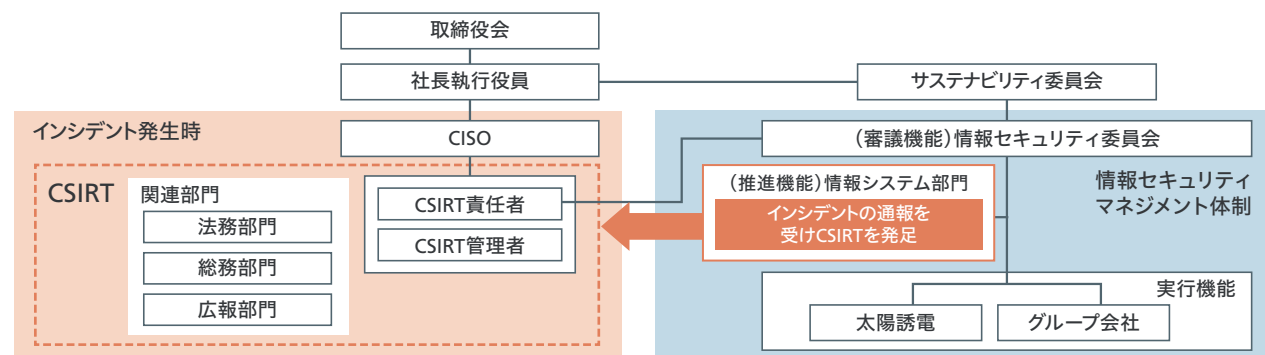
CISOを委員長とする情報セキュリティ委員会を定期的開催し、情報セキュリティ方針、各種対策の進捗、インシデント対応状況等を審議しています。これらの審議内容および重要事項はサステナビリティ委員会に年2回報告され、経営の意思決定および監督に反映されています。

実務面では、情報システム部門が事務局としてグループ全体の情報セキュリティマネジメントを推進しています。

インシデント発生時の対応

対応チーム(CSIRT)が中心となり、初動対応、影響範囲の把握、封じ込めおよび是正措置を実施します。

状況は速やかにCISOへ報告され、必要に応じて情報セキュリティ委員会での審議を経てサステナビリティ委員会へ報告されます。これにより、現場対応から経営レベルまで一貫した判断・指示が行われる体制を整えています。



リスク管理

情報資産に関するリスクを継続的に評価し、組織的・人的・物理的・技術的対策を組み合わせた多層的な管理を行っています。

情報セキュリティに関わるグループ規定を整備するとともに、入社時教育や全従業員向けの定期教育、役割別教育および不審メール・インシデント対応訓練等を通じて、情報セキュリティリテラシーの向上を図っています。

また、サーバーールームや生産工程等の重要エリアにおける入退室管理に加え、マルウェア対策や脆弱性対策、ネットワークセキュリティ対策等の多層防御、アクセス権限管理や暗号化を組み合わせた統合的なセキュリティ対策を実施しています。