TOKYO ELECTRON

Information Security Report 2026

東京エレクトロン
情報セキュリティ報告書 2026

編集方針

情報セキュリティ報告書の発行にあたって

東京エレクトロンは、ステークホルダーの皆さまに当社の情報セキュリティに関する活動をご報告することを目的として、情報セキュリティ報告書を発行しています。本報告書では、当社が実施している包括的な情報セキュリティ対策の取り組み状況をご説明しています。当社は、今後も情報セキュリティ脅威の動向を注視し、継続的なセキュリティ強化に取り組むとともに、ステークホルダーの皆さまへの適切かつ透明性の高い情報開示に努めてまいります。

対象範囲

報告の対象範囲および関連データについては、東京エレクトロングループ (連結26社) としていますが、一部は日本国内のグループ会社のみを対象としています。

発行時期

2026年8月

対象期間

2026年3月期 (2025年4月1日～2026年3月31日)

Contents

ご挨拶

樋口 公博
東京エレクトロン株式会社
情報セキュリティ委員長

当社は、「最先端の技術と確かなサービスで、夢のある社会の発展に貢献します」という基本理念のもと、半導体産業の発展に向けて日々取り組んでいます。社会の持続的な発展を支える半導体において、当社は技術革新を真摯に追求し、付加価値の高い最先端の装置と技術サービスを継続的に創出することで、中長期的な利益の拡大と企業価値の持続的な向上を目指していきます。

一方、これらの活動を進める上で、情報セキュリティの確保は極めて重要な課題です。わが国を取り巻く地政学的状況の変化、情報セキュリティに関する法規制の強化、グローバルサプライチェーンの拡大、ビジネス環境のDXの進展やAI技術の急速な発展、さらにはこれらに対するサイバー脅威の増加など、情報セキュリティを取り巻くリスクはますます複雑化しています。当社が事業を確実に継続するためには、安全・安心にデータを活用できる環境の整備が欠かせません。

当社は、半導体市場の発展を支える業界のリーディングカンパニーとして、情報セキュリティを重要な経営課題に位置づけています。強固な情報セキュリティの確保は、事業継続の基盤であると同時に、激化する市場環境を勝ち抜くための差別化要因であり、品質やコンプライアンスと並ぶ当社の事業競争力の源泉であると考えています。

こうした状況を踏まえ、当社では、東京エレクトロングループ情報セキュリティ委員会を中心にグループ全体で情報セキュリティ対策の強化に取り組んでいます。お客さまやお取引先さまの情報や先端技術に関する機密情報を保護し、サイバー攻撃、内部不正、製品セキュリティ、工場セキュリティなど、多岐にわたるリスクに対処するため、高度な専門能力を有する専門部署を設置し、リソースの拡充を図りながら対策を強化しています。また、従業員一人ひとりに情報セキュリティに関する教育を実施し、インシデントの未然防止に努めています。

当社は、これらのセキュリティ強化への取り組みをさらに加速させ、東京エレクトロングループとして、株主さま、お客さま、お取引先さま、そして社会全体のご期待に応えるべく、今後も努力を続けてまいります。本報告書では、東京エレクトロングループの情報セキュリティ活動を紹介しております。ぜひご一読いただけますと幸いです。

当社における情報セキュリティの位置づけ

あらゆる産業でデジタル化が進展する中、半導体・半導体製造装置産業の重要性は一層高まっています。一方、その重要性の高まりに伴い、半導体・半導体製造装置事業を取り巻く情報セキュリティの脅威が深刻化しています。当社では、情報セキュリティの確保を経営上の重要課題と位置づけ、お客さまやお取引先さまの情報や先端技術に関する機密情報を保護するため、情報セキュリティ強化に向けた取り組みを積極的に推進しています。

世界をリードする先端技術を有する企業は、絶えず外部ネットワークからの不正アクセスや社内からの機密情報漏えいなどの情報セキュリティの脅威に直面しています。半導体製造装置の市場において60年以上の歴史をもち、他社をしのぐ先進技術情報を多数保持しつつ、未来を見据えた研究開発が注目されている当社も例外ではありません。当社では、業務上必要なすべての情報および情報を取り扱う環境 (以下、情報資産) において、その機密性・完全性・可用性の確保を徹底することで、以下の情報セキュリティの実現を目指しています。

- 機密情報の保護管理、流出防止とお客さまの満足度の維持向上
- 情報資産の改ざん防止と正確な情報に基づくビジネス実施環境の確保
- インシデントに対するレジリエンス (回復力) の強化によるビジネス継続性の確保
- 情報セキュリティに関する法令、社会規範、倫理基準の遵守と社会的責任の履行
- セキュリティソリューションを用いたデジタルトランスフォーメーション (DX) とセキュリティの両立

当社は、これらの取り組みの実現に向けて、グループ全体の情報セキュリティ体制やサイバー攻撃への対策を強化しています。これらの活動を通して、お客さまやお取引先さまからお預かりした情報資産および当社の情報資産をセキュリティの脅威から守るとともに、セキュアな製品の提供に努めています。当社は、常に変化し続けるセキュリティリスクを分析し、セキュリティ対策の見直しを重ねながら、リスクを適切にコントロールすることで、半導体技術の発展と豊かな社会の実現に貢献していきます。

主な活動


情報セキュリティ体制

情報セキュリティマネジメント


サプライチェーンセキュリティ


セキュリティ脅威への対応


工場・製品のセキュリティ

レジリエンスの強化

情報セキュリティのガバナンス

半導体需要の高まりを背景に、当社の事業と組織は拡大を続けています。一方、情報セキュリティの領域では、最もセキュリティが弱い部分 (Weakest Link) が脆弱性となり、重大なインシデントに発展するリスクがあります。

さまざまな国に拠点をもつ東京エレクトロングループは、国ごとに異なる言語や法規制への対応を考慮し、本社およびグループ全体で情報セキュリティを確保していくことが必要です。当社は、「ONE TEL」を合言葉に、グループ全体で高い情報セキュリティを確保するためのガバナンス体制を構築しています。

1 情報セキュリティ推進体制

当社のコーポレートガバナンスを統括する取締役会は、情報セキュリティ部門から適時、情報セキュリティに関する活動報告を受け、最新の情報セキュリティリスクを踏まえて、日々のコーポレートガバナンス活動を実施しています。

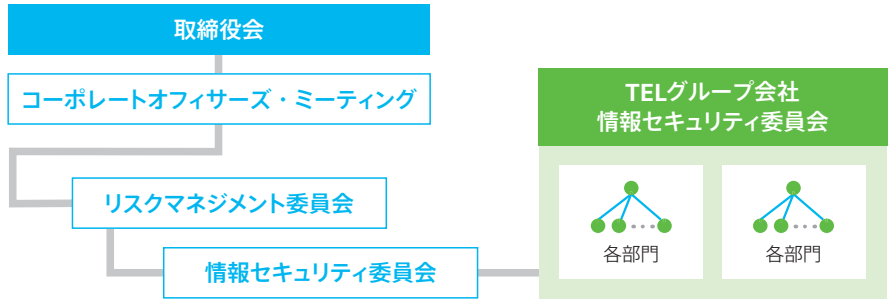
また、当社では取締役会およびコーポレートオフィサーズ・ミーティングの下部組織として、本社の情報セキュリティ担当執行役員が委員長を務める「東京エレクトロングループ　情報セキュリティ委員会」を設置しています。本委員会は、グループ全体の情報セキュリティガバナンスを推進し、グループ全体にわたる情報セキュリティの方針の決定や、各グループ会社のセキュリティ対策状況の管理をおこなっています。

本社では、情報セキュリティ担当執行役員の指示のもと、情報セキュリティ部がグループ全体にわたる情報セキュリティの管理、施策の実行、ならびにグループ会社を横断するセキュリティオペレーションを遂行しています。

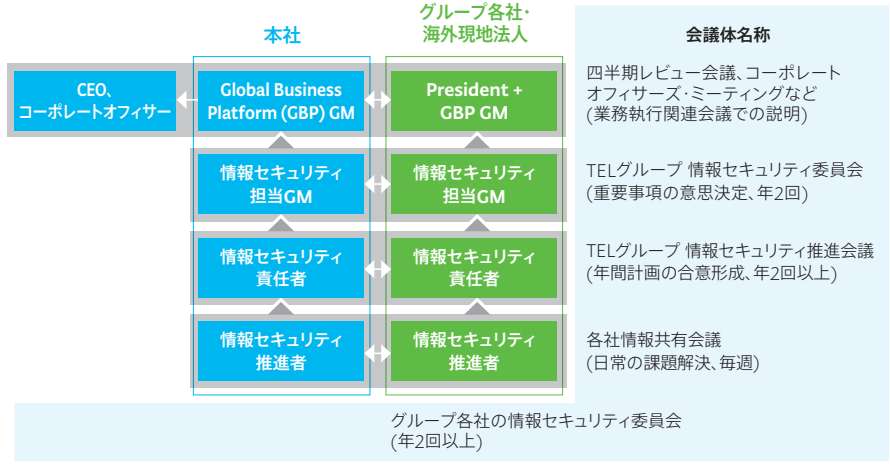
加えて、各グループ会社内では、情報セキュリティ担当のGM (General Manager) の指揮のもと、任命された情報セキュリティ責任者および情報セキュリティ推進者が各社内の情報セキュリティ委員会を組織し、情報セキュリティに関する実効的なガバナンスを構築しています。各社内で議論を重ね、横断的な連携を図ることで、グループ全体で共通の認識をもちながら、セキュリティ強化に取り組んでいます。

これらの体制を通じて、グループ全体での統一的な情報セキュリティレベルを確保するとともに、本社の統括のもと、グループ全体の情報セキュリティの管理状況を把握し、各種セキュリティ施策を迅速に展開できる体制を構築しています。

情報セキュリティ管理体制図



各社の情報セキュリティ体制



情報セキュリティのガバナンス

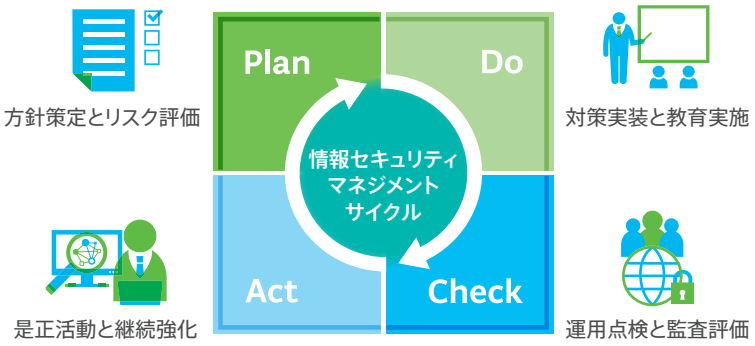
2 情報セキュリティ活動のフレームワーク

情報セキュリティリスクは常に変化し続けており、最新の動向を反映した組織全体での継続的な取り組みが不可欠です。当社では、情報セキュリティ活動を情報セキュリティマネジメントに基づくPDCAサイクルに則り、体系的に実施しています。

Planフェーズでは、各組織において情報資産の洗い出しやリスクアセスメントを実施し、必要な施策を決定します。続くDoフェーズでは、従業員を対象とした教育や啓発活動、セキュリティ施策の展開を実行します。Checkフェーズでは、点検や内部監査を通じて、セキュリティ対策の運用状況を評価します。Actフェーズでは、実施された点検や内部監査の結果を分析し、是正措置やルール・施策の見直しをおこないます。

こうした継続的な取り組みにより、当社は情報セキュリティを効果的に維持しています。さらに2025年3月期からは、グループ全体で共通の情報セキュリティ水準を確保する観点から、本社部門より順次、第三者認証機関による審査を通じて情報セキュリティマネジメントシステムの国際規格であるISO/IEC 27001:2022の認証取得を段階的に進めています。今後も継続的な改善を通じて、お客さまやお取引先さまからの信頼に応えていきます。

情報セキュリティマネジメント活動



3 機密情報の管理と情報セキュリティ事故への対応

当社では、当社が保有する重要な技術情報、およびお客さまやお取引先さまからお預かりした情報など、多くの重要な情報資産を取り扱っています。当社では、事業活動において有用であり、機密に保持する必要がある情報をすべて機密情報として取り扱い、厳格に管理しています。機密情報は、情報管理部門長が情報管理責任者として機密区分を指定し、認識ミスや管理漏れが発生しないよう、各情報資産へのラベリングを徹底しています。この機密区分に基づき、厳格なアクセス制御がおこなわれたサーバーへの格納や情報資産の持ち出しの監視、強固な暗号化などの措置を講じています。また、社外組織と情報を共有する必要がある場合は、強固なセキュリティが確保されたオンラインストレージサービスを利用しています。

万が一、機密情報の漏えいなどのインシデントが発生した場合には、インシデント管理システムに入力をおこなうことで、直ちにリスク管理部門等の関係部門に状況が共有され、組織全体で速やかな対処をおこなう体制を整えています。またインシデントの経緯や発生状況については情報セキュリティ部門が分析し、組織全体での振り返りと再発防止につなげています。

なお、従業員個人に起因する機密情報の漏えいなどのインシデントが発生した場合には、故意・不注意を問わず、就業規則に基づき厳正に対応しています。

情報セキュリティのガバナンス

東京エレクトロンのガバナンスと情報セキュリティ

峰島 孝之
情報セキュリティユニット GM、CISO (Chief Information Security Officer)
東京エレクトロン株式会社

「Chapter 2 当社における情報セキュリティの位置づけ」で記載のとおり、半導体・半導体製造装置事業を取り巻く情報セキュリティの脅威は、近年急速に高まっています。カンファレンスなどで米国を含む、同業他社のCDO (チーフデジタルオフィサー) やCIO (チーフインフォメーションオフィサー) と会話をすると、真っ先に話題に上がるのは、情報セキュリティです。この領域において、各社は「競争ではなく、協調して取り組むべき」という共通認識をもち、業界全体としてセキュリティ強化に取り組んでいく必要性を確認しています。当社も、半導体業界において日本をリードする立場であるという使命感をもっており、各メンバーが責任をもって活動に取り組んでいます。

Accelerate Global IS Orchestration!

Orchestration of:
- Strategy
- Technology
- Security
- Governance (Process)
- Organization & People

東京エレクトロングループでは、情報セキュリティを含むIT活動指針として、「Accelerate Global IS Orchestration!」を掲げています。この指針には、本社およびグループ会社のITと情報セキュリティに関わるメンバーが一体となり、オーケストラが奏でるように調和を取りながら推進する、という思いが込められています。最優先事項として位置づけられている情報セキュリティおよびITガバナンスについて、グループ横断で足並みを揃えた活動が真っ先に進んでいます。さらに、調和の取れた活動を促進するため、日本本社の情報セキュリティ部から海外の各現地法人へ赴任者を派遣し、本社との橋渡しとして連携を強化しています。

4 情報セキュリティポリシー

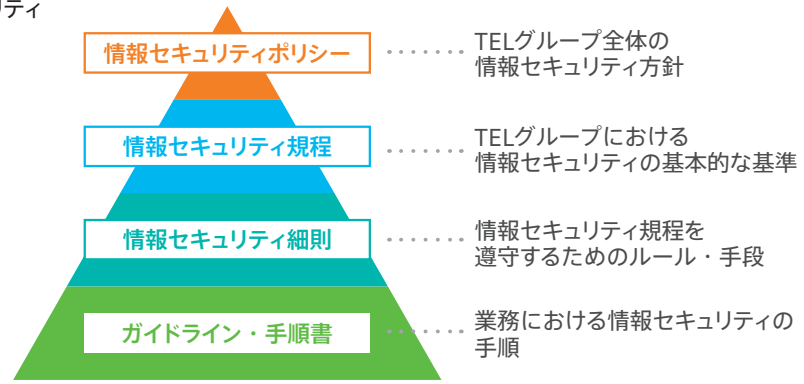
グローバル企業である東京エレクトロングループにおいて、本社とグループ会社が同じ水準でセキュリティ対策を実施することが重要です。それを実現するために、グループ全体としての情報セキュリティ文書をセキュリティポリシーとして策定しています。

当社の情報セキュリティ文書は、右図に示す体系により構成されています。第一階層では、グループ全体のセキュリティ方針を定めた情報セキュリティポリシーを制定しています。この下の第二階層では、当社の基本的なセキュリティ対策の基準を定めた情報セキュリティ規程を整備し、さらに第三階層で、情報セキュリティ規程を遵守するための詳細なルールや手段を定めた情報セキュリティ細則を制定しています。また、第四階層には、各業務における情報セキュリティの具体的な実施手順を示すセキュリティガイドラインや手順書類を整備しています。

これらの情報セキュリティ文書は、外部のセキュリティ規格や国際標準で定められた要件を参考にして策定されています。また、セキュリティの脅威や技術動向の変化を踏まえ、定期的な見直しや規定の追加をおこなうことで、最新の情報セキュリティ脅威に対応しています。

グループ全体で統一的なセキュリティレベルを確保するため、これらの情報セキュリティ文書は、社内のポータルサイトに多言語で掲載され、当社で業務をおこなうすべての従業員が常に閲覧できるようになっています。

情報セキュリティ文書体系



情報セキュリティのガバナンス

5 情報セキュリティの教育と意識啓発

情報セキュリティを確保する上では、情報セキュリティポリシーを定め、物理的対策、技術的対策などのさまざまな情報セキュリティ対策を講じつつも、最終的には、「人」が最後の防衛線となってきます。従業員一人ひとりが日々の業務において取り扱う情報の重要性や自身が担う責任の大きさを理解し、情報セキュリティ規程が定めるさまざまな対策を意識した行動を取ることが重要です。

当社では、すべての役員、従業員を対象に、毎年情報セキュリティ規程に関する教育を実施しています。内容はグローバル共通となっており、現地スタッフが理解しやすいよう多言語で提供するとともに、情報セキュリティ規程を分かりやすくまとめた情報セキュリティハンドブックを、すべての従業員のPC上に配置し、速やかに最新版を閲覧できるようにしています。また、メールの誤送信や情報の持ち出しなど、事例別の教育コンテンツも整備しています。

並行して、管理職や工場の担当者など役割別でのセキュリティ教育をおこなうとともに、新入社員やキャリア採用の方向けのオンボーディング研修でも情報セキュリティを重要コンテンツとして取り入れています。また、従業員の情報セキュリティに関する意識を高めるために、社内向けの情報を集約したポータルサイトの運営や情報セキュリティニュースレターの配信などをおこなっています。

加えて、工場や海外子会社では、各社の業務状況に密着した独自のセキュリティ教育を実施するとともに、現場のリスクに応じたサイネージやポスター掲示、注意喚起などの啓発活動をおこない、従業員一人ひとりが情報セキュリティのキーポイントを正しく理解するための取り組みを推進しています。

6 情報セキュリティ演習

情報セキュリティの脅威は日々高まり続けており、万が一、情報セキュリティに関する事案が発生した際には、各従業員が速やかに社内関係部門にエスカレーションをおこなうことが重要です。特に、当社の従業員や情報資産を狙ったフィッシング攻撃は日常的に発生しており、従業員が悪意のあるメールを開封するなどの行為によって、会社全体を巻き込んだ大規模なインシデントに発展してしまうケースも想定されます。

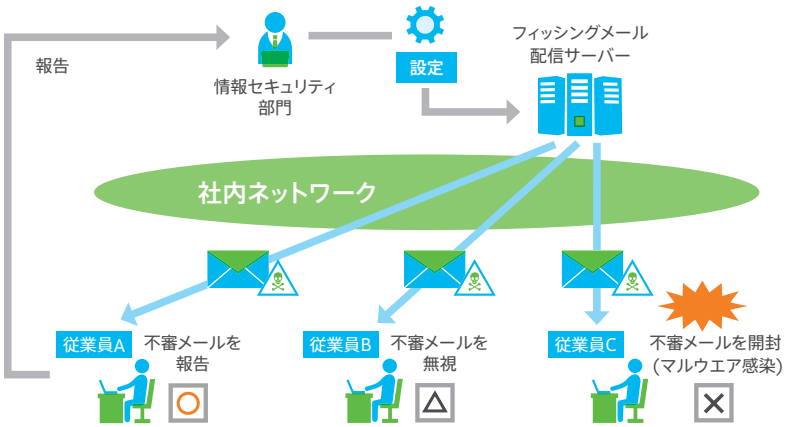
こうした背景から、当社では、全従業員を対象にフィッシングメール演習を継続的に実施しています。実際の攻撃を模したフィッシングメールを実体験することで、リスクに対する理解を深め、不審メールを見分ける基本的なリテラシーの向上を図っています。しかし、「人」である以上、不審メールを完璧に見極めることは困難です。そのため、フィッシング攻撃を受けた際にはセキュリティ部門に情報を共有し、迅速な初動対応や同様の攻撃を未然に防ぐ行動が重要となります。そのため、開封率より報告状況を重視し、組織全体でのフィッシング攻撃への耐性向上を目指しています。

また、当社を標的としたサイバー攻撃が発生した場合に、適切な情報共有や迅速な初動対応ができるよう、システム担当者やセキュリティ関連部門では、インシデント対応演習を実施しています。演習では、あらかじめ準備したサイバー攻撃のシナリオに基づき、インシデントの発生を想定した各種対応を関係者がおこないます。その際、演習中に見つかった課題を記録し、今後の改善につなげています。情報共有は、実際のインシデントを想定し、ウェブ会議やチャット、対面会議など実践的な形でおこないます。

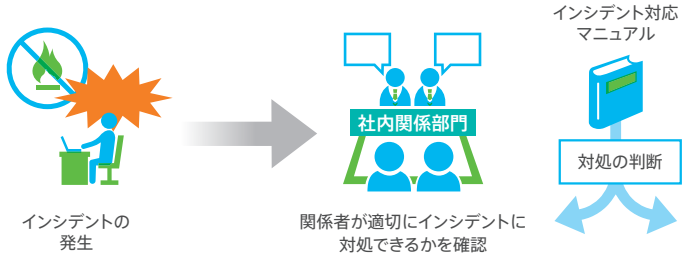
こうした情報セキュリティ演習を継続的に実施することで、組織全体のセキュリティレジリエンスを高め、実際にインシデントが発生した際にも、速やかな復旧対応が可能となるよう努めています。

情報セキュリティのガバナンス

フィッシングメール演習



インシデント対応演習



7 情報セキュリティに関する監査と点検

情報セキュリティ規程や教育プログラムが整備されていても、日々の業務の中でルールが形骸化してしまうリスクがあります。当社では、情報セキュリティ規程の遵守を徹底するため、以下のような監査と点検を実施しています。

情報セキュリティに関する内部監査

当社では、当社の社員だけでなく、派遣社員や委託社員が所属する多くの部門がさまざまな情報資産を取り扱っています。このため、情報セキュリティ規程が各部門で適切に遵守されているかを確認する目的で、毎年、情報セキュリティに関する内部監査を実施しています。

本監査では、社内の情報セキュリティ規程に従い、情報資産が適切に保護されているか、各組織内で情報セキュリティ活動が適切に実施されているかを確認しています。監査結果は責任者に報告され、不備があった場合は、対策の見直しや改善をおこなっています。

社内情報システムおよびクラウドサービスのセキュリティ対策状況の点検

当社では、事業遂行のために多くの社内情報システムを運用しています。当社が構築･運用する情報システムに関しては、情報セキュリティ規程に基づき、適切なパッチ適用、認証やアクセス制御、マルウエア対策、バックアップなど必要なセキュリティ対策が実施されているかを確認しています。不備が確認された場合には速やかに是正をおこないます。

また、DXの進展やビジネス環境の変化に迅速に対応するため、社外のクラウドサービスを利用するケースが増加しています。こうした場合は、外部の専門会社と連携し、当該クラウドサービスに対するセキュリティ審査を実施しています。セキュリティ審査で不備が発見された場合は、当該クラウド事業者に是正を依頼し、対応が困難な場合は、よりセキュアなクラウドサービスに切り替えるなど、厳格な管理を徹底しています。

情報セキュリティのガバナンス

お取引先さまへの情報セキュリティ点検

当社の半導体製造装置は、多くのお取引先さまのご協力を得て生産されています。情報セキュリティの脅威からサプライチェーン全体を守るため、当社はお取引先さまと一体となり、セキュリティ対策の継続的な向上に取り組んでいます。

お取引先さまには、毎年情報セキュリティに関するアセスメントをお願いし、当社にて情報セキュリティ対策が適切におこなわれているかを確認しています。具体的には、セキュリティチェックシートに基づく書類での確認に加え、現地での確認が必要なお取引先さまに対しては、セキュリティ部門の専門監査員による訪問点検も実施しています。

点検で明らかになった不備については、速やかにお取引先さまにフィードバックをおこない、改善を依頼しています。また、脅威の動向やインシデントの状況を踏まえ、各種点検項目の定期的な見直しを実施しています。

書類点検

訪問点検

情報セキュリティのガバナンス

グローバルでの情報セキュリティガバナンスの課題

佐々木 誠
情報セキュリティ部　推進グループリーダー
東京エレクトロン株式会社

東京エレクトロンの情報セキュリティガバナンスを進める上での課題は何ですか？

情報セキュリティガバナンスを推進するにあたり、私たちはコミュニケーションの重要性を強く認識しています。

現在、セキュリティ対策の現状を把握するために、自社を含むグループ会社や主要なお取引先さまに対してセキュリティアセスメントを実施し、必要な是正措置を支援しながら、統一的なガバナンスの確立に向けた取り組みを進めています。しかし、国内外の異なる文化や言語、時差、規制、技術的な違いをもつ国々のメンバーと連携しながら統一的なガバナンスを確保することは、大きな課題です。こうした課題に対応するため、担当者との定期的な会議や教育プログラムの展開を通じて共通認識を醸成し、柔軟なアプローチを心掛けています。

また、外部の専門家や各種団体との積極的な連携も欠かせません。最新の情報やトレンドを取り入れることで、セキュリティガバナンスの質をより高めることができます。私自身も、外部の方々との情報交換を通じて得た知見をどのように自社へ反映させるか、日々担当者と議論を重ねています。

これらの課題を解決するためには、独自の取り組みを進めるだけでは不十分です。東京エレクトロングループ全体、さらにはサプライチェーン全体で協力して、情報セキュリティガバナンスのさらなる改善を目指していきたいと考えています。

鈴木 雄大
Information Security Analyst
Tokyo Electron U.S. Holdings, Inc.

生成AIなども昨今、大きな話題ですが、どのようにガバナンスに取り組まれていますか？

従来、目的別に導入されてきたCRMや教育などの各種サービスにおいても、生成AIや高度な機械学習技術を活用した分析・支援機能の実装が進み、AIの活用領域は業務プロセス全体へと急速に拡大しています。こうしたAIの高度化・汎用化は業務効率や付加価値の向上に寄与する一方で、技術進展や利用形態の変化を踏まえたガバナンスの定期的な見直しが重要な課題となっています。

東京エレクトロンでは、情報セキュリティを中核に、ITガバナンス、コンプライアンス、法務、知的財産などの関係部署が連携し、AI活用を含むデジタル技術に対する横断的なガバナンスルールの整備を継続的に進めています。

また、グループで標準的に利用する生成AIについては、情報システム部門の管理のもと、情報セキュリティ部がトライアル段階から参画する運用とすることで、企画・導入の早期段階からセキュリティリスクの低減を図っています。

今後もこれらの取り組みを継続することで、セキュアな生成AI活用の基盤を維持・強化し、東京エレクトロングループの持続的な価値創造に貢献してまいります。

技術的・物理的対策

標的型攻撃やランサムウエアなどサイバー攻撃による被害の報道は後を絶たず、企業の事業継続における大きな脅威です。さらに、地政学的緊張の高まりを背景に、国家支援型のハッカー組織によるサイバー攻撃や、ビジネスモデルとして確立されたサイバー犯罪組織による活動が活発化しており、その手法はますます巧妙化しています。また、従業員の内部不正によって機密情報が流出するケースや、悪意ある者が企業の施設内に立ち入って、情報資産の窃取や破壊などをおこなうリスクも懸念されます。

こうした脅威に対応するため、当社では、技術および物理的対策の強化に日々取り組んでいます。

1 セキュリティ監視について

当社が保有する情報資産や従業員を標的とした不正通信や不審メールは、日々確認されています。当社のSOC (Security Operation Center) では、専門のセキュリティ技術者が24時間365日の体制でインシデントを監視しています。

各従業員のPCやサーバーに導入されたEDR (Endpoint Detection and Response) などのセキュリティ監視機器が出力するログをSIEM (Security Information and Event Management) により集約し、不審なイベントが検出された場合は、迅速に調査や分析をおこなっています。加えて、従業員のアカウントを狙う攻撃も大きな脅威の1つです。SOCでは、外部からの不正ログイン試行やアカウント不正利用などの不審なアクティビティについても常時監視をおこなっています。

さらに、社外からのサイバー攻撃に加え、従業員による内部不正や不注意によるインシデントも重大事案に発展するリスクを伴います。従業員へのセキュリティ教育を徹底する一方で、従業員が意図的に規定に違反して機密情報を社外に持ち出す、あるいは、セキュリティ意識の低い従業員が私物の機器を持ち込んでマルウエア感染が発生するなどのリスクにも対応が求められます。

当社では、このような従業員の不適切行為を防止するため、厳格なアクセス制御と常時監視をおこなっています。不適切行為が発覚した場合は、当該者に対して厳正な対処を取る運用を実施しています。

こうしたセキュリティ監視により、当社の重要な情報資産をさまざまなセキュリティ脅威から保護しています。

セキュリティ監視

技術的・物理的対策

2 SIRTの取り組み

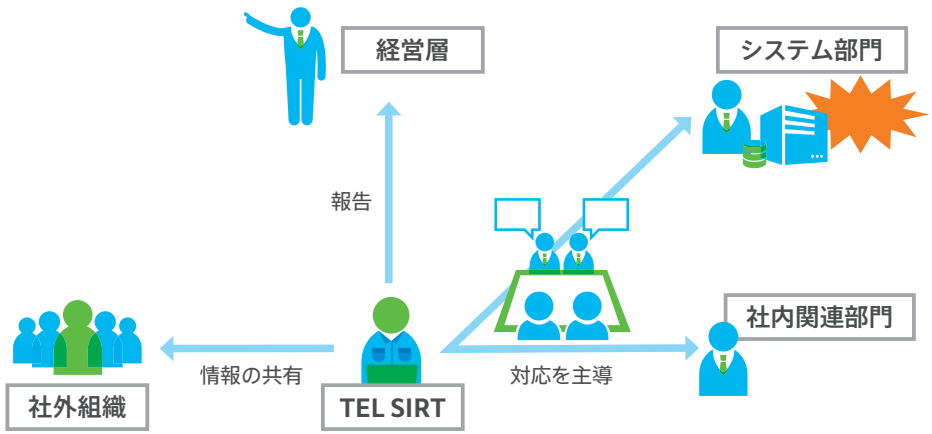
当社は、攻撃者にとって価値のあるさまざまな技術や製品に関する機密情報を保有しています。一方で、組織規模や事業領域が多岐にわたるため、攻撃対象となりうる範囲 (アタックサーフェス) は、極めて広範囲です。サイバー攻撃を「攻撃側」と「防御側」という構図から見た場合、攻撃と防御は非対称であるため、攻撃側が常に有利な状況にあります。攻撃側は、広大な対象範囲の一点を任意のタイミングで突破すればよいのに対し、防御側はすべての対象範囲を継続的に守り抜く必要があるからです。こうした状況を踏まえると、サイバー攻撃を100%防ぐことは難しいといえます。そのため、当社は、インシデントの発生を想定し、速やかにインシデントを特定、復旧・対処をおこなうレジリエンスの体制を確保することが重要であると考えています。

SIRT (Security Incident Response Team) は、インシデントの発生時にSOCと連携して対処するチームです。当社では、2020年に「TEL SIRT」を設置し、グループ全体のセンターオブエクセレンスとして活動しています。

「TEL SIRT」は、SOCからの連絡を受け、対応が必要と判断されたインシデントについて、通信の遮断や被害拡大の防止、証拠保全と調査、原因の分析などの一連の対応を主導します。インシデントが発生した場合は、事態の収束に向けて、社内関連部門や社外組織との連携が不可欠です。そこで、専門組織である「TEL SIRT」が全体の統制を図ることで、迅速なインシデント対応を可能としています。

「TEL SIRT」は、平常時はセキュリティの情報サイトやダークウェブなどのさまざまな情報源から、サイバー攻撃集団のプロファイルや攻撃手口などのインテリジェンス情報およびサイバー攻撃に悪用される最新の脆弱性情報を収集しています。収集された脅威情報は、セキュリティリサーチャーによって分析され、日々のセキュリティ監視やセキュリティ対策の改善などに活用される他、全社への注意喚起や是正指示などの活動にも役立てられます。

TEL SIRTによるインシデントレスポンス

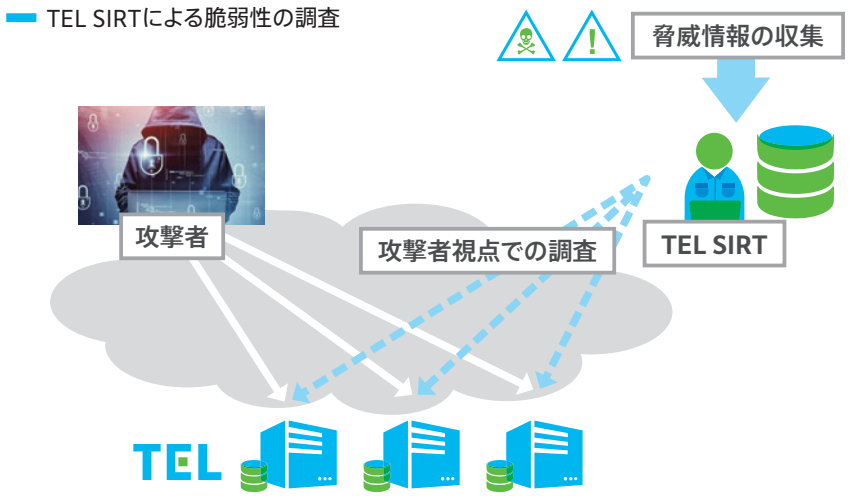


技術的・物理的対策

また、「TEL SIRT」では、攻撃者の視点をもち、攻撃者に先んじて当社がサイバー攻撃を受けるリスクがないかを調査する活動も重要であると考えています。当社が運用管理するシステムに対しては、「TEL SIRT」が事前に脆弱性診断を実施しています。また、脆弱性は日々新たに発見されるため、定期的な脆弱性のチェックをおこなうとともに、意図せず公開されているシステムがないかの巡回調査も併せておこなっています。

加えて、攻撃者が用いることの多いOSINT (Open Source Intelligence) など、インターネット上に公開されている情報を活用して当社に関連する脆弱性や設定不備の有無についての探索を実施しています。また、重要なシステムに対しては、ペネトレーションテストと呼ばれる疑似的な不正侵入テストもおこない、不正侵入につながる脆弱性の有無を調査しています。

「TEL SIRT」は、防御側と攻撃側の両方の視点を兼ね備えたサイバーセキュリティのスペシャリストとして、当社の情報セキュリティを守るために重要な役割を果たしています。



TEL SIRTによるサイバーセキュリティ強化の取り組み

藤川 晃央
情報セキュリティ部　TEL SIRT　社内セキュリティグループリーダー
東京エレクトロン株式会社

昨今、さまざまなインシデントが大きく報道されており、非常に大変な仕事だと思いますが、どのようなところにやりがいを感じますか？

サイバー攻撃は24時間365日いつ発生するか分からず、なかなか気が休まることはありませんが、日々激化するサイバー攻撃から、われわれTEL SIRTが当社を守る防波堤になっているという点に大きなプレッシャーと同時にやりがいを感じています。また、半導体市場の発展を支える当社をサイバー攻撃から守り抜くことは、半導体が支える豊かな社会の実現に貢献できる極めて重要な仕事だと感じています。

TEL SIRTのメンバーとして心掛けていることは何ですか？

日々進化するサイバー攻撃技術に対抗するためには、私たちSIRTメンバーのスキル向上が欠かせません。メンバー全員が高い意識をもって、日々のセキュリティ関連の情報収集はもちろん、社外のセキュリティ技術研修にも積極的に参加し、TEL SIRTの監視技術やインシデント対応能力の向上に役立てています。自社内にとどまらず、外部のイベントへの参加や社外のセキュリティチームとの交流などを積極的に進めて、より高度な技術を磨いていきたいと思っています。

技術的・物理的対策

3 ネットワークセキュリティ対策

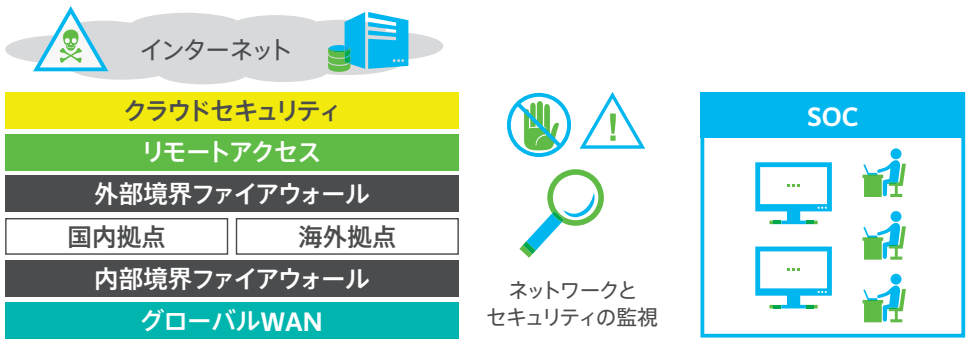
当社では、DXを推進していく上で多くのクラウドサービスを利用しており、インターネット上のクラウド環境に保管されているデータを安全に活用することが重要な課題です。また、当社の従業員は、グローバルな環境で、テレワーク・オフィスワークを問わずハイブリッドなワークスタイルで働いています。

このような状況下で当社は、統一されたネットワークセキュリティポリシーに基づき、グローバル拠点でばらつきのない運用を実現するため、セキュアなグローバルネットワーク基盤を構築しています。

各拠点に次世代型ファイアウォールを設置し、リスクの高い通信のフィルタリングや監視をおこなうとともに、すべての拠点へクラウドセキュリティサービスを導入し、ネットワークとセキュリティの継ぎ目のない運用をおこないながら、クラウド環境利用時のセキュリティを強化しています。さらに、全世界の従業員が、セキュリティを確保しながら快適な働き方ができるよう多要素認証によるリモート接続の環境を整備しています。

また、前述のEDRと同様にこれらのネットワークや機器もSOCで一元的に監視し、不審なイベントが発生した場合は、直ちに通信遮断などの対応をおこないます。加えて、機器故障によるネットワーク障害が発生した際も各拠点と連携して迅速にサポートできる体制を整備しています。

グローバルネットワーク基盤



4 物理セキュリティ対策

当社は、部外者が事業所内に立ち入って情報資産に接触することのないよう、事業所内を区画化し、エリアレベルに応じた入退管理を実施しています。

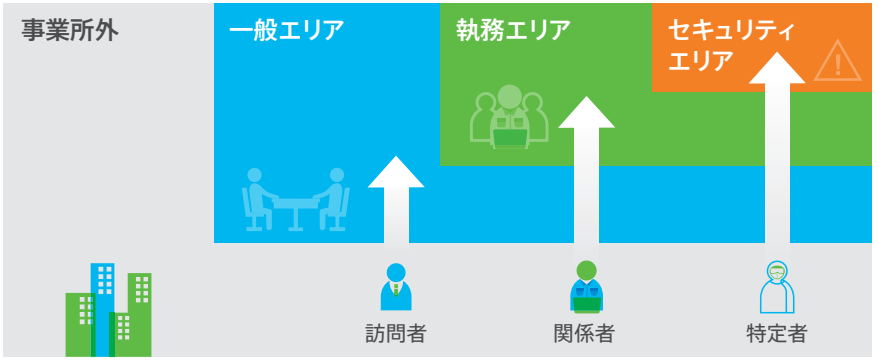
一般エリアは、事業所から離れた会社の敷地内の屋外通路や駐車場、玄関、来客用会議室、カフェテリアなどが該当します。このエリアは、フェンスや警備員による監視体制が取られています。

執務エリアは、従業員と事前に許可された関係者のみが入場可能なエリアであり、物理認証システムによる入退管理が徹底されています。

セキュリティエリアは、当社の技術情報などの高機密情報を取り扱うエリアです。このエリアには、従業員であっても事前にエリア管理者に許可された特定の者しか立ち入ることができず、カメラ付きスマートフォンなどの持ち込みも禁止されています。さらに、監視カメラによる常時監視がおこなわれており、一部の特定エリアでは、こうした対策に加えて生体認証システムも導入されています。

当社では、情報セキュリティを考慮した厳格な物理認証システムを用いることで、不審者による情報資産へのアクセスを厳重に制限しています。

エリア別の運用管理



生産拠点や製品のセキュリティ対策

半導体製造装置を手掛ける当社にとって、生産および開発の拠点である工場のセキュリティ強化は喫緊の課題です。当社では、各工場が安全かつ安定的に稼働するよう、工場セキュリティの強化に取り組んでいます。

また、お客さまに納入する製品については、SEMI E187/E188※1をはじめとする業界標準や、EUサイバーレジリエンス法※2 をはじめとする各国の法規制を踏まえたセキュリティ対策を実施しています。これにより、お客さまの半導体製造工場の安定稼働に資する製品セキュリティの確保にも取り組んでいます。

※1 SEMI E187/E188: SEMI E188とは、パッチ適用やメンテナンスなどにより工場内システムへのマルウエア感染を防止することを目的とした装置の規格。SEMI E187とは、半導体製造に関わるデータの保護を目的としたファブ (Fab) 装置 (半導体製造装置) のサイバーセキュリティ規格
※2 EUサイバーレジリエンス法 (EU CRA) とは、欧州連合 (EU) でデジタル製品のセキュリティ対策を製造者に義務づける法律

1 工場セキュリティ強化

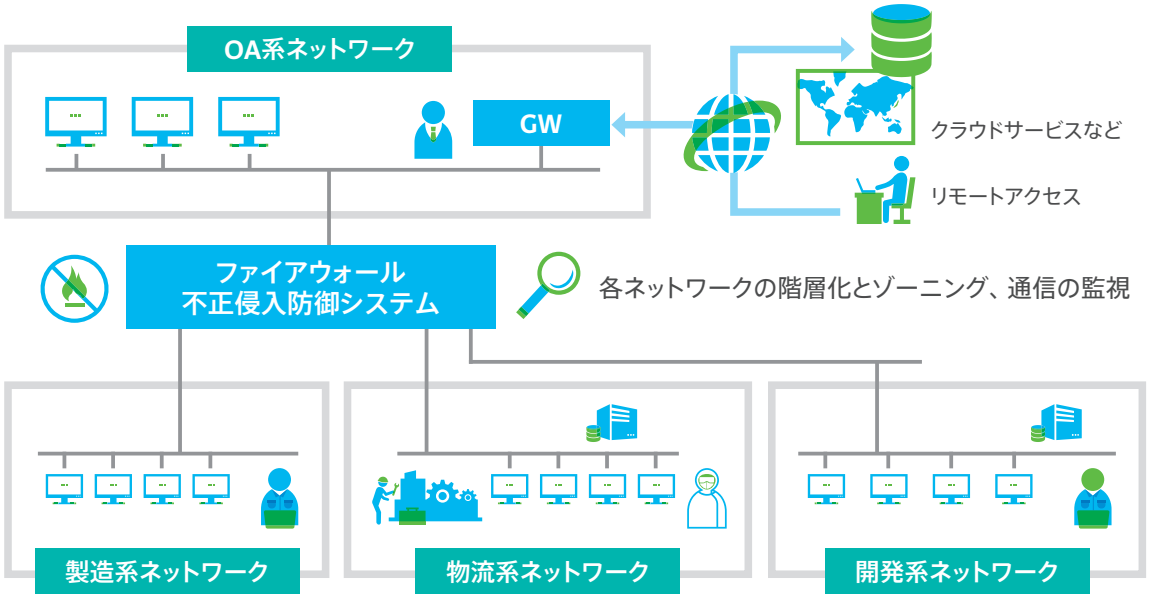
従来はクローズドな環境であった工場ネットワークにおいても、オープン化やDXが進み、サイバー攻撃やランサムウエア感染などの情報セキュリティのリスクが高まっています。

工場では、一般的なオフィス環境やOAネットワーク向けに定められた情報セキュリティ対策をそのまま適用することが難しい場合があります。このため、当社では、工場セキュリティの知見を有するメンバーを中心に工場セキュリティ強化のための専担チームを編成しています。また、国際標準などを参考に工場セキュリティのガイドラインを制定し、本ガイドラインに基づき、各工場が安全かつ安定的に稼働するよう、グループを横断するソリューションの導入と監視をおこなっています。

工場における製造系ネットワークや物流系ネットワークおよび開発系ネットワークは、OA系のネットワークとはファイアウォールや不正侵入防御システムにより明確に分離され、通信の監視がおこなわれています。加えて、各ネットワークは、VLANで細かくセグメンテーションされており、万が一、インシデントが発生した場合の被害を最小限に抑える設計です。また、各種ネットワークに接続される機器はインベントリ管理されており、インシデントが発生した場合は、SOC/SIRTチームと工場現地のメンバーが連携して、迅速に対処します。

こうした取り組みにより、各工場の生産および開発業務を停止させることなく、安定的な事業の継続を実現しています。

工場ネットワークのセキュリティ強化



生産拠点や製品のセキュリティ対策

2 製品セキュリティ強化

製品セキュリティを取り巻く状況と当社の基本方針

製品セキュリティは、現代のデジタル社会においてますます重要性を増しており、その確保は企業にとって不可欠な課題です。

製品セキュリティを取り巻く状況としては、EUサイバーレジリエンス法（EU CRA）が成立し、2027年12月から適用が開始される予定です。また、米国でも法令化の動きが進んでおり、2023年3月に公表された国家サイバーセキュリティ戦略において法令化が明示されています。このような背景から、SEMIスタンダードに対するお客さまからの問い合わせや要求が増加しています。加えて、半導体工場のスマート化の進展により、サイバーセキュリティの重要性は一層高まっています。半導体工場におけるサイバーセキュリティリスクは、マルウエア感染による生産への影響、ランサムウエアによる金銭要求や機密漏えい、機密情報の窃取、手順の改ざんや不正な制御による生産の妨害など、多岐にわたります。

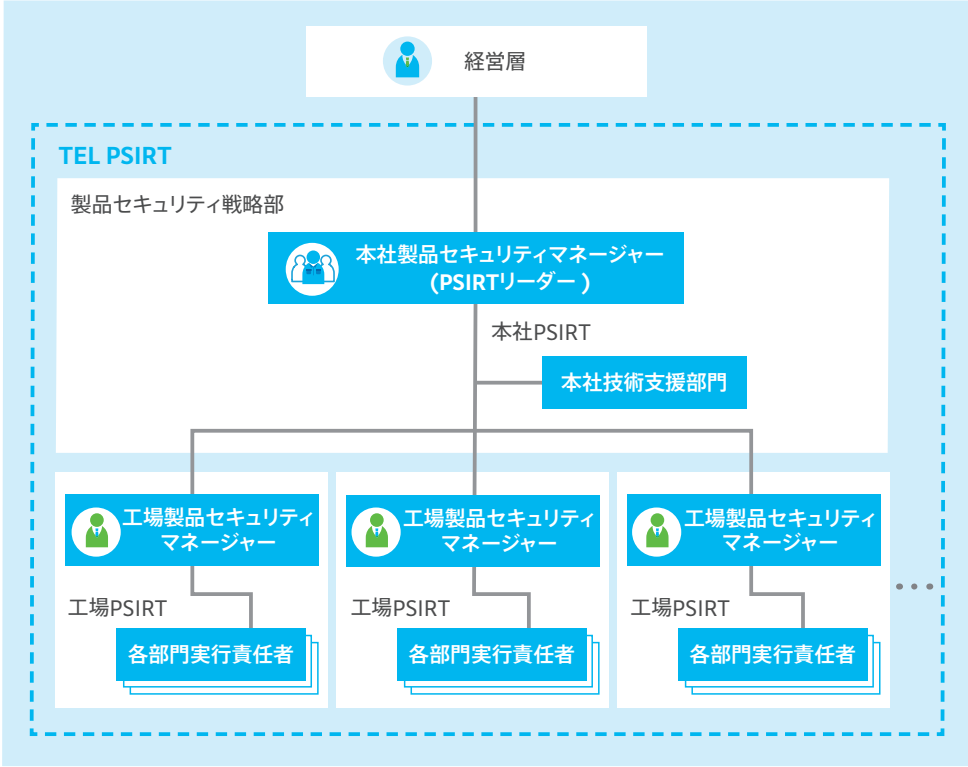
当社は、お客さまに安心して製品・サービスをご利用いただけるように以下のとおり製品セキュリティ基本方針を定め、製品そのものの強固なセキュリティと製造およびフィールドサポートにおける確実なセキュリティ対策を実施しています。

製品セキュリティ基本方針

- 当社製品への攻撃による半導体デバイス製造の妨害を防ぐ
- 当社製品を踏み台にした攻撃を防ぐ
- 顧客の情報資産、当社に属する情報資産を守る

製品セキュリティ推進体制

当社は、すべての製品におけるセキュリティを確保するための司令塔として、「製品セキュリティ戦略部」を立ち上げました。この部門は、社内外のさまざまなステークホルダーを取りまとめ、製品セキュリティに関する最新情報や技術、ノウハウを集約することによって、当社全体で統一したルールやプロセスの確立をおこなっています。加えて、脆弱性の発見やインシデントの発生といった有事の際に迅速に問題解決ができるよう、本社だけでなく国内外の全工場にPSIRT（Product Security Incident Response Team）を設置し、機動的に連携する体制づくりを進めていきます。

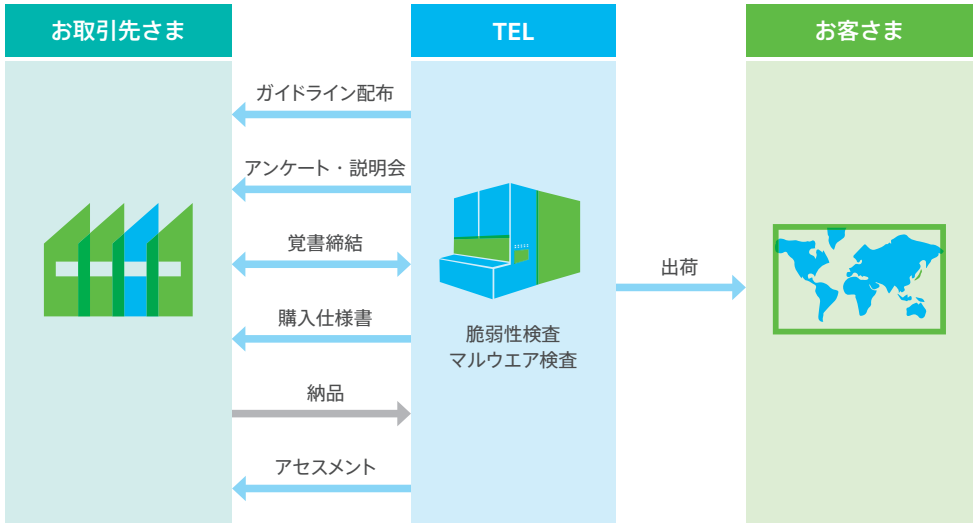


生産拠点や製品のセキュリティ対策

お取引先さまへの対応

当社では、お取引先さまから購入する部品 (ハードウエア部品だけでなくソフトウエアも含む) によって当社製品のセキュリティが損なわれることを防ぐため、お取引先さまに対して製品セキュリティの観点から定期的なアセスメントを実施しています。このアセスメントを通じて、課題の是正と製品セキュリティ対策の改善を促しています。

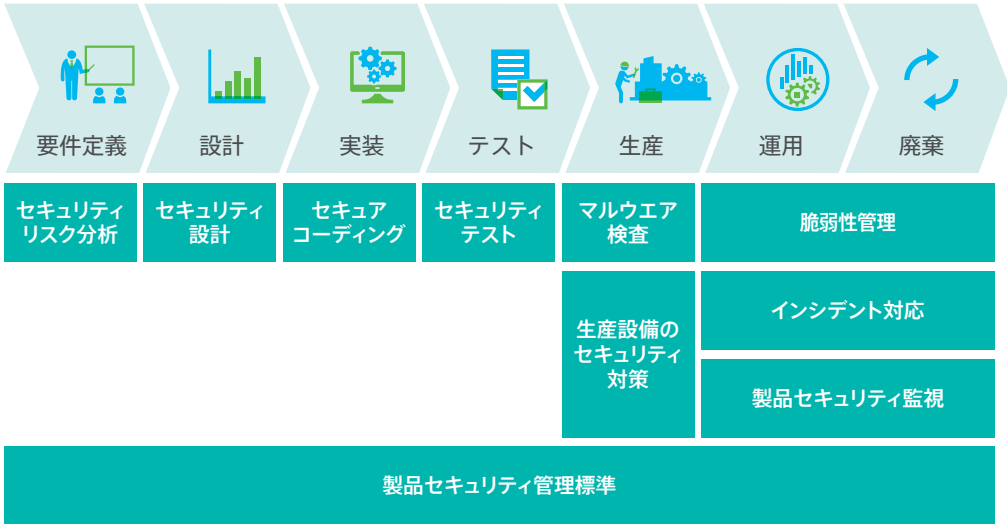
具体的には、当社からの協力依頼事項をまとめたお取引先さま向け製品セキュリティガイドラインを発行し、説明会の開催やアンケート実施などによりお取引先さまの理解度の向上と確認をおこなうとともに、その遵守など製品セキュリティ要件を定めた覚書を締結します。また、購入仕様書にガイドラインに沿った具体的な要件を明記するとともに、定期的に現地アセスメントを実施して、問題点が確認された場合には必要な是正措置を講じています。



セキュアな製品・サービス開発

当社では、製品開発の各段階において適切に製品セキュリティが考慮され、セキュリティが確保された製品を実現するための製品開発プロセスを確立しています。

EUサイバーレジリエンス法 (EU CRA) をはじめとするセキュリティ関連の法令では、セキュアな機能を実装するだけでなく、セキュリティを考慮した製品開発プロセスの整備が求められています。それに対応するため、各部門の業務フローに、セキュア製品開発プロセスを組み込む必要があります。具体的には、製品開発ライフサイクルに関する国際規格を参照し、当社の製品に合わせた開発プロセスに関する文書を作成します。その文書を各部門の既存文書に反映させることで、新たなプロセスの実践を推進しています。これらの取り組みは、製品のセキュリティ向上と信頼性の確保に寄与することを目指しています。

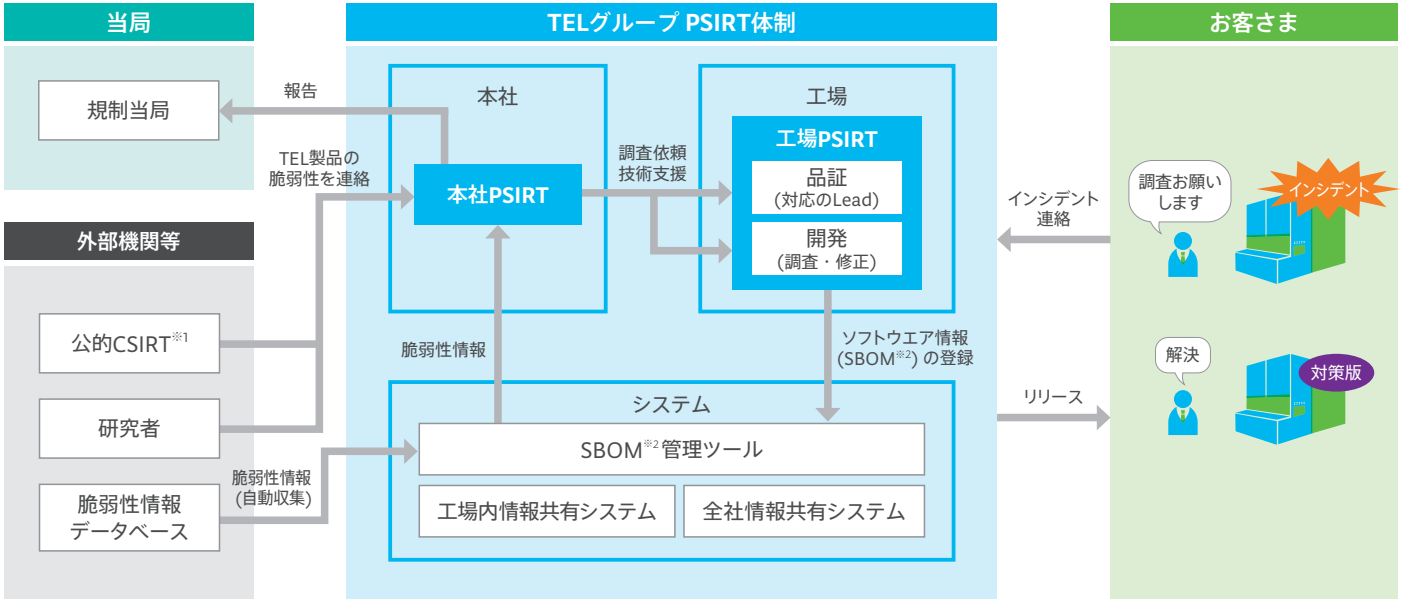


生産拠点や製品のセキュリティ対策

脆弱性およびインシデントへの対応

製品のセキュリティを維持するためには、平時から最新の脆弱性情報を収集し、製品への影響の有無を見極めた上で、サイバー攻撃による脆弱性の悪用を未然に防ぐことが重要です。当社では、本社と工場に設置したPSIRTが連携する脆弱性対応フローを確立し、脆弱性の収集および検知、影響分析、そして優先度に基づく対策を実施しています。

また、サイバー攻撃によるインシデント発生に備え、平時からインシデント対応訓練を実施し、対応フローの確認と改善を継続的におこなっています。これらの取り組みにより、万が一、インシデントが発生しても、PSIRTが中心となって被害の最小化と迅速な復旧、関係者への情報開示、原因究明と再発防止策の検討などを円滑に進めるための体制を構築していきます。



※1 公的CSIRT: 各国でサイバー攻撃や脆弱性に対応し、情報の収集・共有や調整をおこなう公的な専門組織
※2 SBOM (Software Bill of Materials): ソフトウエアの部品表

業界の規範となる連携モデルの確立を目指して

森 英雄
製品セキュリティ戦略部　エキスパート
東京エレクトロン株式会社

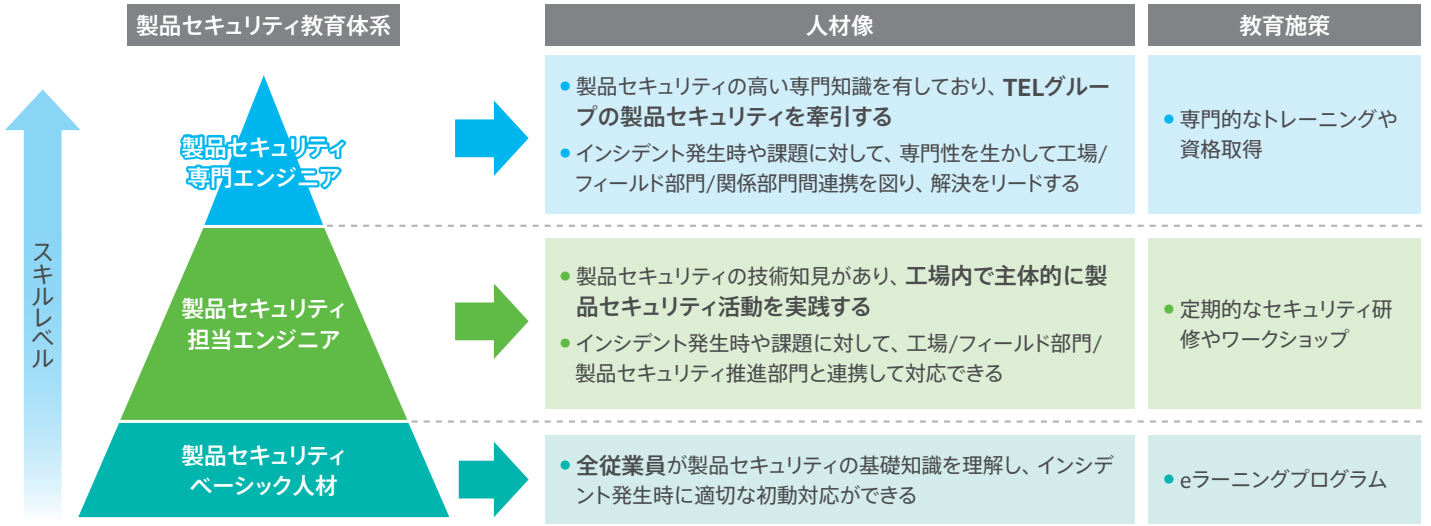
半導体製造装置は多様な機器で構成されています。各機器にはさまざまなソフトウエアが搭載されており、当社単独でオープンソースソフトウエア (OSS) も含めたすべてのソフトウエアを把握し、脆弱性に対処することは非常に困難です。そこで当社では、お取引先さまと連携し、脆弱性情報の共有や連携の枠組みの構築を通じてサプライチェーン全体としての信頼性を高め、セキュリティリスクの低減を目指しています。この連携に向けては、技術面、運用面で多くの課題がありますが、お取引先さまとの連携に向けたトライアルや社外セキュリティ有識者との議論・共創などを通じて業界の規範となる連携モデルを確立し、半導体業界のさらなる発展に貢献していきます。

生産拠点や製品のセキュリティ対策

製品セキュリティ人材育成

当社の製品セキュリティを確保するためには、従業員一人ひとりが確実に製品セキュリティ対策を実施することが必要です。そのため、製品セキュリティに関する人材区分と目指すべき人材像を設定し、それに基づいた教育施策をおこなっています。全従業員向けの基礎教育、製品セキュリティの開発や運用に携わるエンジニア向け教育、製品セキュリティインシデントに対応する専門チーム向け教育などを実施しています。

さらに、専門的な知識やスキルをもち、製品セキュリティをリードできる人材の育成にも取り組んでいます。今後も教育施策を継続強化し、当社全体の製品セキュリティレベルの向上を図っていきます。



“攻め” の製品セキュリティ強化活動

飯嶋 織行
製品セキュリティ戦略部　部長
東京エレクトロン株式会社

半導体は重要な戦略物資であることから、半導体工場におけるサイバーセキュリティ対策の重要性は今後さらに高まることが予想されます。当社では、強固なセキュリティや対応体制が、お客さまにとって製品価値の一部になることを目指して、製品セキュリティ活動に取り組んでいます。その活動の中心を担うのが、私たち製品セキュリティ戦略部です。私たちは、グループ全体の製品セキュリティに関する方針の策定と実行を担っています。サイバーセキュリティ対策というと“守り” のイメージですが、広く深く製品セキュリティに携わるという点では非常にチャレンジングな業務であり、むしろ “攻め” の活動です。お客さまにセキュアな製品および付加価値の高いサービスを提供できるように、全社一丸で製品セキュリティに取り組んでまいります。

社外活動と情報セキュリティ人材の強化

当社は半導体製造装置事業における技術力や事業規模に加え、情報セキュリティの分野においてもリーディングカンパニーとなることを目指しています。当社は世界的に激化するサイバー攻撃に対抗するため、高度な防御体制を構築し、規範を示すことで、半導体業界の持続的な成長に貢献することを使命と考えています。その一環として、半導体業界におけるセキュリティ対策の標準化や社外連携にも積極的に取り組んでいます。

また、情報セキュリティの根幹を支えるのは「人」です。社会全体でセキュリティ人材の不足が深刻化する中、当社では情報セキュリティを最重要課題の1つと位置づけ、セキュリティ組織を強化していきます。

1 社外でのセキュリティ活動

当社は、世界の半導体業界に属する企業や団体が参画するSEMIにおいて、サイバーセキュリティの強化を検討する事業体であるSMCC (Semiconductor Manufacturing Cybersecurity Consortium) の活動を牽引しています。当社は、2023年12月に設立されたこの事業体のGoverning Councilのメンバーに選出され、事業体の運営に関して意思決定・監督する役割をもち、加えて全ワーキンググループに議長もしくはメンバーとして参画し、議論の中心的役割を担っています。

また、SEMI主催の各国で開催されるカンファレンスにおいて、SMCCの活動を牽引する立場で、SMCCの活動および当社のサイバーセキュリティの取り組みについて精力的に講演をおこなっています。SEMICON Japanにて毎年開催されるサイバーセキュリティフォーラムにおいては、2023年から2025年の3年間、SEMIとともに実行委員としてプログラムを企画し、Opening Remarksと当社の取り組みに関する講演をおこなっています。加えて、半導体業界の将来を見据えた技術標準化戦略を議論するために初めて開催されたグローバルスタンダードサミットでは、SMCC代表としてサイバーセキュリティの標準化戦略について講演し、他の標準化団体の代表者とともにパネルディスカッションをおこなうなど、半導体業界全体のセキュリティ強化に貢献しています。

また、昨今のサイバー攻撃は業種や規模を問わずあらゆる企業で発生しており、ある組織で発生した攻撃と同様の手法が別の組織で再び利用されることも多くあります。こうした脅威に迅速に対応するためには、単独での対応ではなく、同様の課題を抱える組織間で信頼関係を構築し、横の連携を強化することが不可欠です。

当社のTEL SIRTは、こうしたセキュリティの連携強化に賛同し、産官学などの多様な組織が参加する社外セキュリティ団体にも加入しています。こうした活動を通して、脅威情報の収集やさまざまなセキュリティ情報の共有を推進しています。

当社が所属するセキュリティ団体

- 日本シーサート協議会: 国内のシーサート (CSIRT: Computer Security Incident Response Team) 間での緊密な連携を図り、シーサートにおける課題解決に貢献するための組織。
- FIRST (Forum of Incident Response and Security Teams): 世界中のシーサート間での緊密な連携を図り、シーサートにおける課題解決に貢献するための世界最大のシーサート組織。企業、政府機関、学術機関などさまざまな組織で構成される。
- 日本ネットワークセキュリティ協会 (JNSA): ネットワークセキュリティに関する啓発、教育、調査研究および情報提供に関する事業をおこなう、特定非営利活動法人。
- セキュリティ・トランスペアレンシー・コンソーシアム: サプライチェーンセキュリティリスクの低減に向け、可視化データ (SBOM等) の活用促進に資する知見の共創に取り組む任意団体。

社外活動と情報セキュリティ人材の強化

2 情報セキュリティ人材の強化

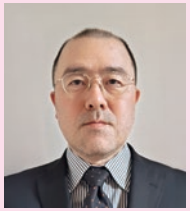
昨今の情報セキュリティに関わる脅威の高まりを背景に、セキュリティ人材の需要はますます拡大しています。また、セキュリティ業務は多岐にわたるため、一言でセキュリティ業務といっても、その内容は多様です。

例えば、日々のセキュリティ監視をおこなうアナリスト、製品や工場セキュリティの対策強化をおこなうエンジニアなど、技術的な業務だけではなく、セキュリティマネジメントやセキュリティ監査をおこなう人材には、セキュリティの法令や規格に関する知識も必要です。より専門的な領域では、外部の専門パートナーの知見を借りることもありますが、事業会社として基盤を支える部分は、従業員が対応していく必要があります。当社では、業界トップクラスのセキュリティ体制構築を目指し、セキュリティ人材の採用と育成を強化しています。

また、情報セキュリティ領域は変化のスピードが非常に速く、日々のスキルアップが重要な課題です。セキュリティ部門では、日々のOJTに加え、体系的に情報セキュリティを学べる仕組みを整備しています。具体的には、CISSP (Certified Information Systems Security Professional) などのセキュリティ資格の取得や大学が開催するセキュリティ講座での社会人学習を推奨しています。加えて、インターンシップを通じて、当社でセキュリティを学ぶ楽しさや最先端技術に触れる機会を提供し、セキュリティに関心の高い優秀な学生に当社のセキュリティへの取り組みを伝える活動にも取り組んでいます。

当社は、事業を支えるセキュリティ、そしてセキュリティを支える「人」の採用と育成に積極的に取り組み、セキュリティ人材育成の強化を推進していきます。

社外団体の活動と情報セキュリティ人材の強化



萩尾 英二
情報セキュリティ部　部長
東京エレクトロン株式会社

昨今の半導体に関する世界的な需要の増加、そして地政学的観点からも半導体業界・企業のセキュリティリスクは注目されていますが、東京エレクトロングループはどのような立場でこうした課題に取り組まれているのでしょうか？

半導体業界の国際団体であるSEMIは、昨今のセキュリティの重要性を踏まえ、サイバーセキュリティコンソーシアムであるSMCCを立ち上げ、業界全体としてセキュリティ強化に取り組んでいます。SMCCには、現在8つのワーキンググループがあり、そのうち、サプライチェーンのセキュリティ評価手法を策定するワーキンググループでは、私が議長を務めています。定例会議を通じて、業界の各社とともにチェックリストの素案を作成し、SEMIの正式文書として公開しました。また、2024年7月に開催された SEMICON Westのサイバーセキュリティセッションでは、日本企業で唯一、講演をおこなっています。半導体業界への貢献に加えて当社のプレゼンス強化と、業界のリーディングカンパニーとして日本の半導体業界のサイバーセキュリティの存在価値を海外にアピールすることを念頭に活動を推進しています。

こうした状況を踏まえ、東京エレクトロングループでは、どのようにセキュリティの組織を強化していく予定でしょうか？

私たちは、東京エレクトロングループ全体の情報セキュリティ強化を牽引するという重大なミッションを担っています。今後のセキュリティ強化のロードマップを策定し、それに基づいて対策の強化や人材の採用・育成を進めていきます。その人材確保と育成に対する思いは、自社の採用サイトや採用エージェント企業のインタビューでも明記しており、共感いただける方と次の東京エレクトロングループのセキュリティを共創していきたいと考えています。当社は、セキュリティ対策の強化、人材の確保と育成、プレゼンスの強化という3本柱で、名実ともに業界最先端のサイバーセキュリティを実現し、半導体サプライチェーンの安全確保に貢献していく考えです。

東京エレクトロン概要

1 会社概要 (2026年3月31日時点)

社名	東京エレクトロン株式会社
本社所在地	〒107-6325 東京都港区赤坂5-3-1 赤坂Bizタワー
設立	1963年11月11日
従業員数	20,236名 (グループ全体)

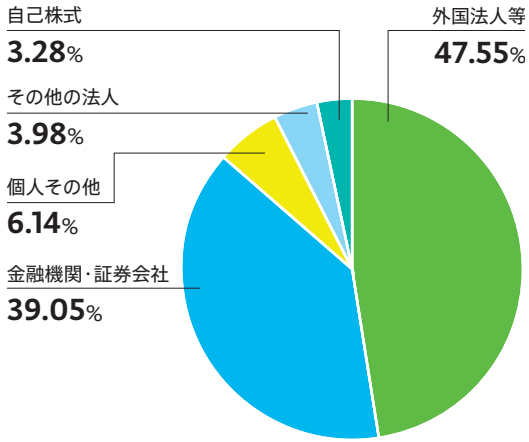
2 株式の状況

上場証券取引所	東京証券取引所プライム市場
発行可能株式総数	900,000,000株
発行済株式総数	471,632,733株
株主総数	114,525名

大株主の状況

株主名	持株数 (千株)	持株比率 (%)
日本マスタートラスト信託銀行株式会社 (信託口)	111,481	24.43
株式会社日本カストディ銀行 (信託口)	46,224	10.13
株式会社TBSホールディングス	15,112	3.31
THE CHASE MANHATTAN BANK, N.A. LONDONSECS LENDING OMNIBUS ACCOUNT	14,891	3.26
STATE STREET BANK AND TRUST COMPANY 505001	11,569	2.53
HSBC HONG KONG-TREASURY SERVICES A/C ASIAN EQUITIES DERIVATIVES	7,408	1.62
GOVERNMENT OF NORWAY	6,738	1.47
JP MORGAN CHASE BANK 385781	6,644	1.45
BNYM AS AGT/CLTS NON TREATY JASDEC	6,418	1.40
JP MORGAN CHASE BANK 385642	5,678	1.24

所有者別株式分布状況



東京エレクトロン株式会社

〒107-6325
東京都港区赤坂5-3-1 赤坂 Bizタワー
Tel.03-5561-7000
www.tel.co.jp