産業サイバーセキュリティ研究会 WG1 工場SWG
第2回会合
JEITA半導体部会発表資料

2022年2月28日

①業界を取り巻く状況（DXの状況、工場システムの概要、国内外の法令等による工場セキュリティへの要求事項等）（1）

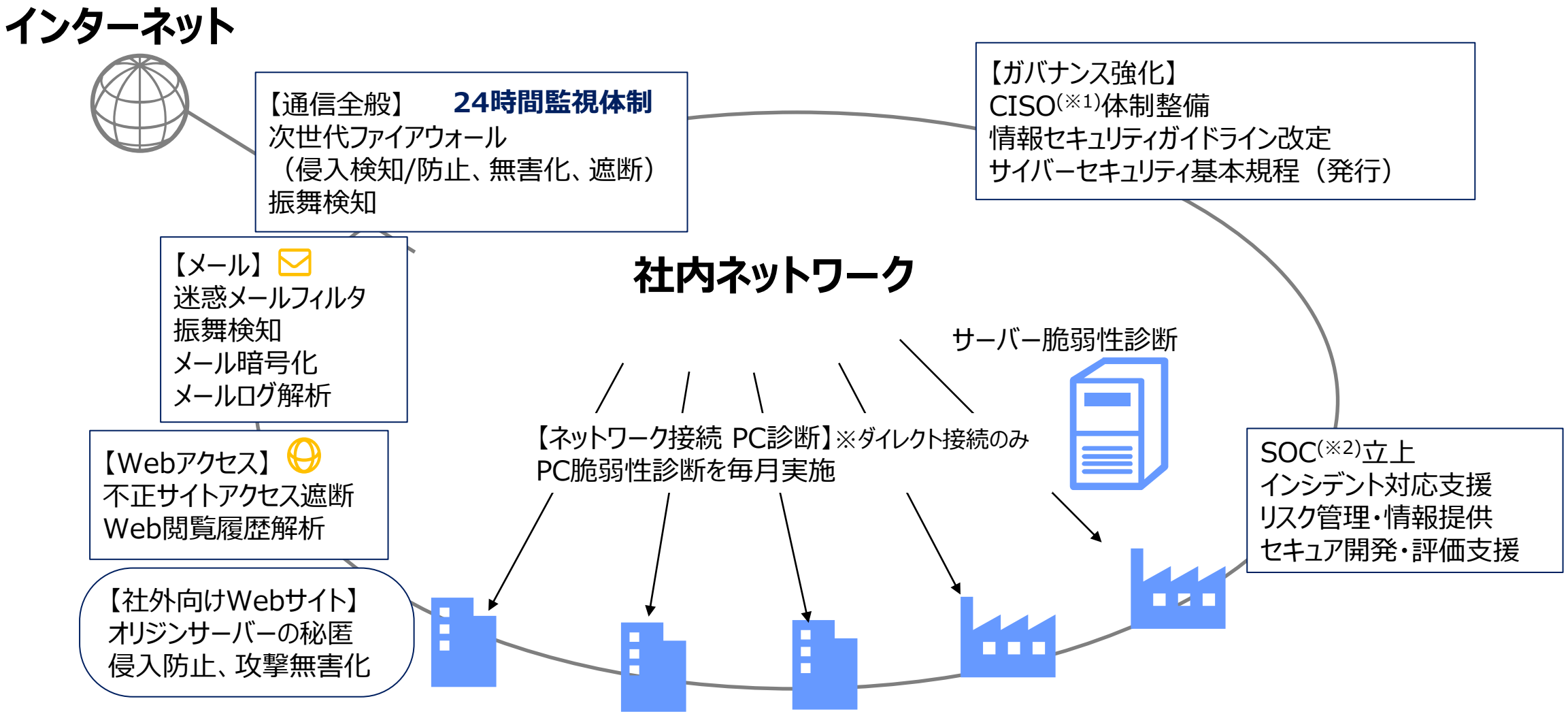
➢ DXの状況

- 生産効率向上のため国内と海外の生産データを一元管理し、全工場の見える化を実施している。
- 高度シミュレーション/スケジューリングシステムを用いて生産性を最大化している。
- DXを推進部署を設立。半導体量産工場での品質改善や業務効率改善などを推進している。

➢ 工場システムの概要

- イントラネットの中で半導体製造に必要なシステムを展開している。
- SEMI規格によるオンライン自動運転で運用している。
- スタッフ・技術のOAネットワークと製造側ネットワークを分離しており、製造側にMES、装置稼働モニター等を配している。

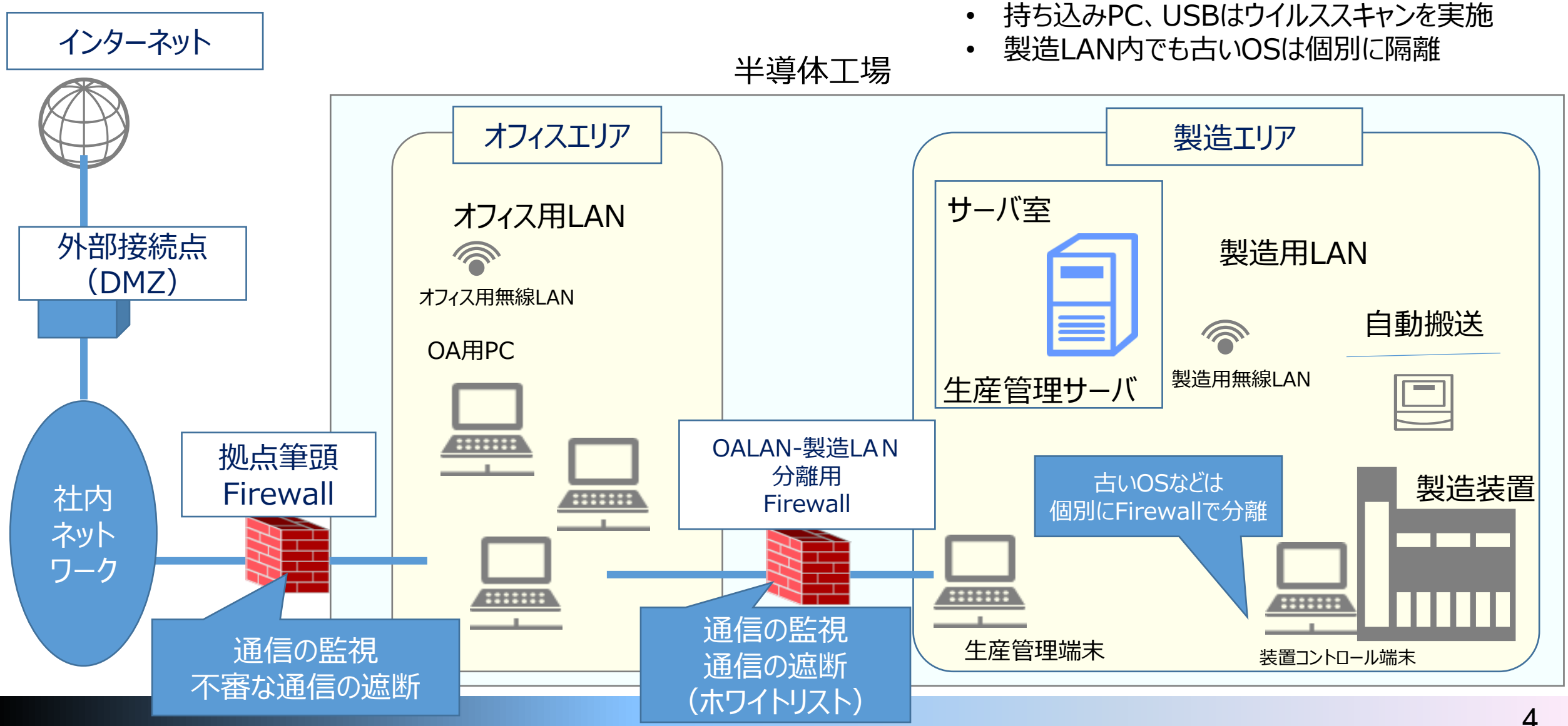
社内ネットワーク　セキュリティ対策（一部）



※1 CISO Chief Information Security Officer 情報セキュリティ統括責任者
※2 SOC Security Operation Center 24時間365日体制で、ネットワーク・デバイスを監視し、サイバー攻撃の検出・分析・対策を行う組織

半導体工場におけるセキュリティ対策（一部）

- オフィス用LANと製造LANを分離
- 持ち込みPC、USBはウイルススキャンを実施
- 製造LAN内でも古いOSは個別に隔離



①業界を取り巻く状況（DXの状況、工場システムの概要、国内外の法令等による工場セキュリティへの要求事項等）（2）

➢ 工場セキュリティへの要求事項

- 車載顧客をはじめ、セキュリティ対策に積極的な顧客からの要望が増え、設計、工場におけるセキュリティに対する要求レベルは高まってきている。
- 欧州自動車業界の情報セキュリティの審査基準（TISAX）の認証取得を顧客から求められている。
- 顧客よりNISTをベースとした要求事項が提示され、契約内にもセキュリティに対する条項が盛り込まれている。
- ISMS（情報セキュリティマネジメントシステム）の規格取得や、それに準ずる施策の実施を顧客より求められており、CSRのアセスメント／サーベイ等でも質問に上がってくる。

顧客からのチェックシート（例、一部）

【要求事項】　サーバ等の設置エリアには、物理的セキュリティ対策を行っている。

【達成条件】　サーバ等の設置エリアは、入場可能なひとを定めている。

【達成基準】　規則でサーバ等を設置するエリアに入場可能な者を定めること。

顧客からの設問

【自己評価】　対策済み。

【評価根拠】　入場可能な者を以下に制限している。
- 事前に管理者の承認を得た従業員。
- 社内のシステム運用保守責任者・担当者、メンテナンス業者。
- メンテナンス業者については、入退場時に台帳で立ち入り記録をつけ、都度社内責任者の承認を取得するとともに、入場可能な社内担当者の立ち合いを必須としている。

ベンダーの回答

②各社における工場セキュリティの取組状況（自社工場での取組、下請中小企業や海外企業を含めたサプライチェーン大での取組等）（1）

➢ 自社工場での取組はさまざまなレベルで行われている

- 自社工場での取り組みは、ネットワークセグメント分割が主な対策。
- 工場ネットワーク(OT)と一般用ネットワーク(OA)をFirewallで論理的に分離し、必要な通信のみに限定している。
- ラインは建屋毎、ライン毎等にもFirewallを設置している。
- NIST Cyber Security Framework、ISO 27001等に準拠したセキュリティ対策を実行している。
- マルウェアの感染を想定し、コミュニケーションパスや、対応方法を確認するサイバー・セキュリティ・インシデント対応訓練を、経営陣も参加して実施している。
- コロナ禍で設備メーカーのエンジニア来訪が難しくなり、設備メーカーによるリモートメインテナンスへの要求が高まり、新たにセキュリティガイドラインと審議プロセスを構築して対処した。
- その他
  社内端末以外のネットワーク接続禁止、Removableメディアの利用禁止、フィッシングメールに対する定期的なドリルの実施、サーバーなどへのアクセス権管理の実施、入退室管理（持込・持出、監視カメラ、X線検査など）の実施など。

②各社における工場セキュリティの取組状況（自社工場での取組、下請中小企業や海外企業を含めたサプライチェーン大での取組等）（2）

➢ サプライチェーンでの取組はばらつきがある

- 自社ルールを装置ベンダー、保守ベンダーに展開し、協力を要請している。
- パートナー企業の中には、加工委託などを行ってもらい、分離したネットワークで接続している委託先もある。情報機器の棚卸を含めて、ネットワークの利用方法などを定期的に監査している。
- 部材メーカーなどサプライヤーについてセキュリティ要件を策定中。

③各社における工場セキュリティを取り巻く課題(1)

➢ 各社ともさまざまな課題を抱えている

- 製造装置は、導入時のシステムのまま使われることが多く、バージョンアップなどセキュリティ対策が実質できない。
- セキュリティ対策ソフトは、装置動作の保証ができないとの装置ベンダーからの回答があり、導入が困難。そのため直接的な保護、検疫ができない。
- 製造装置の保守時に装置や関係するベンダーによるコンピュータウィルスの持ち込みリスクがある。
- 製造装置の修理のためハードディスクなどの記憶媒体を修理に出した際、コンピュータウィルスの混入リスクがある。
- リモート診断・支援などが進む場合、社外からのアクセスに伴うセキュリティ対策をユーザー単独として対策することに限度がある。また、様々なツール、方式が乱立することにより、対応がより複雑になる。
- 導入したセキュリティソリューションにより工場システムへ予期しない影響が発生することがある。
- Cloudベースのセキュリティソリューションでは、自社でコントロールできない問題が発生して、工場のオペレーションに影響を及ぼす。
- 新たな技術/デバイスの登場に対するセキュリティ対策が追い付かない(IoT、Cloud、Mobile etc)。

③各社における工場セキュリティを取り巻く課題(2)

- 生産装置付帯PCは、古い設備があり、サポート切れOSなどセキュリティが準拠できない機器が一部残っている。
- 新規設備についても、設備の動作の保証ができないとのことで、ウイルス対策ソフト未導入の生産装置付帯PCが多く存在する。
- 設備メーカーのウイルスに対する認識が甘く、ウイルスに対する対策が不十分である。
- 外部からの持ち込みツールの検査を基本とする侵入対策を中心に実施しているが、装置ベンダーによる修理、メンテナンスの際は持ち込みツールのVirusチェックをベンダーの自己申告により提出されたツールに対して実施しているのが現状であり、悪意や申告漏れで持ち込まれるリスクへの対策が困難である。
- 設備を停止できるタイミングが年に1度程度しかなく、実機テストやシステム導入の計画が立てにくい。
- 24時間365日稼働している工場であり、脆弱性などが発見された場合、パッチをあてるタイミングが難しい。
- OA系は情報システム担当、FA系は製造担当の責任分解点があり、セキュリティ対策は情報システム担当が推進するが、利害関係が一致しない。
- 人材不足のため、体制が十分に組めない。専門スキルを持った要員の補充も難しい(特に地方は深刻)。

④各社の今後の取組(ガイドラインと各社取組との関連性、ガイドラインの活用展望等)(1)

➢ **全体的にガイドラインに対して肯定的な受け止めが多かった**

- 「製造業／工場の事業／業務にとって重要な価値軸:BC／SQDC に対して、セキュリティリスクがどのような影響を及ぼすのかを結びつけ、リスク対応の優先度を整理した上で、必要最小限の基本的なセキュリティ対策は何か、及び対策導入・適用の 進め方を論じています。」 正に、この考え方に沿いたい。
- 2022年度に工場セキュリティの社内規定の制定を予定しており、当ガイドラインに従い対策方法を決めたいと考えている。社内規定制定の目的は、国内、海外、各工場毎のバラバラなセキュリティ対策方法の標準化。対策レベルの最低ラインを定義し、過剰投資の抑制、対策漏れの防止を図りたい。
- 工場セキュリティガイドラインの内容は、今まで弊社で行ってきた工場セキュリティへの取組における課題に対して非常に関連性が高く、今後の活動におけるバイブルとして活用できるものであると思う。
- ガイドラインはよく出来ていると思う。業界を横断した取組とすることで、材料メーカ、OSAT(Outsourced Semiconductor Assembly & Test)などと連携した取組となることを期待する。
- サプライヤー管理の参考となる。
- お客様やサプライヤーの要求や実力を測るため、ガイドラインに記載のレベルやチェックリストを共通の指標として用いられるような環境になることを期待する。
- 会社としてセキュリティ意識の醸成をどのように進めていくとよいのかの参考となる。

④各社の今後の取組(ガイドラインと各社取組との関連性、ガイドラインの活用展望等)(2)

➢ 具体的な活用箇所としては次のようなものが挙がった

- ガイドラインを最低限のベースに装置ベンダー、保守ベンダーとのセキュリティ対応について活用し、自社・自工場に特有な状況については、ガイドラインに加えた対応で活用。
- セキュリティ専門チームによる対策の推進。
- 生産ライン内でのウイルス感染の早期検知。
- Firewallでウイルス検知(セキュリティアラート検知)時の処置と対応策の確立。
- AI技術や設備情報収集技術の活用に伴い、生産ライン内からインターネットへの接続が必要になってきており、これらのセキュリティ対策の強化。
- 高機能化する制御システム(シーケンサ等)のウイルス対策。
- 社内システムでの不足部分の検討。
- 工場セキュリティの教育資料作成。
- 弊社の工場セキュリティを考えるに当たって、他社やサプライヤーの相場観の確認。

⑤ガイドラインへの指摘・ニーズ・要望（1）

➢ 指摘

- ガイドラインの各章に書かれていることはとてもよく理解できたが、工場のセキュリティ対策を進めていく活動の全体像（対応フロー、ステップ）がわかりにくいと感じた。「工場セキュリティを進めるための全体の作業/検討フロー図」と「各フローの作業でガイドラインのどの部分を参照すればよいのか」をマッピングさせる情報があると、リテラシーが低い読者であってもより活用できるものになると思う。
- ガイドライン記載内容の「4.脅威」についてだが、標的を特定したサイバー攻撃を事例とした場合、中小や一般の企業から見てその対策と現状に大きな隔たりを感じ、現実感のないものに映るかと思う。より身近な脅威となる無作為なVirusへの感染による業務ツールのフリーズ、第三者への情報漏洩事故による社会的批判など、身近な脅威が入口の対策目標となるかと考える。さらに、この脅威のレベルと対策のレベルを紐付けできるとよいと考える。
- 「セキュリティ要求レベル」に対して、どのような施策を適用するとよいのかのガイドがあるとよりよいと思われる。
- 政府購入要件等、要件遵守の項目があるとよいと思われる。
- NISTベースでの成熟度アップのための施策レベルや手順があるとよりよいと思われる。
- ガイドラインの冒頭に適用範囲、言葉の定義があればわかりやすいと思う。

⑤ガイドラインへの指摘・ニーズ・要望(2)

➢ 要望

- P.77 図6-1 対策例の具体的実施例、表6-1の主要対策以外の実施例も紹介いただきたい。
- 制御ゾーン(生産現場)の生産ライン内の設備に対するウイルス対策方法について記載いただきたい。
- 調達先に対して、デバイスメーカーごとの要望ではなかなか対策をお願いすることが難しいので、必要な対応については統一した依頼、対応ができるガイドライン制定をお願いしたい(装置の対策ガイド、外部からの機器持ち込みガイド、外部からの遠隔診断サービスガイド)。
- 将来の工場セキュリティに対する考え方の相場観を示していただきたい。従来型の侵入防止対策に加え、異常検知に対する考え方(どこまでやるのか)や、さらに今後はゼロトラストを基本とする考え方に移行すべきなのかどうかの指針をいただけるとありがたい。
- 「基準となる標準規格やセキュリティガイドラインが整備されつつあります。今後、日本の製造業／工場も海外の取引先やユーザを始めとする要求に応じる ことが必須となり、国内でも法規制や業界標準などの要求が定められていくと見られます。」 ガラパゴス(日本特有)な内容ではなく、グローバルで通用する世界基準に適合した内容としていただきたい。
- セキュリティ施策は日進月歩であり、ガイドラインに対する推奨施策の見直しなどがあるとよりよいと思われる。
- 取り巻く環境の変化に追従できる継続的なガイドライン改定をお願いしたい。

⑤ガイドラインへの指摘・ニーズ・要望(3)

➢ 期待

- 過剰なセキュリティ対策ガイドラインの公開は、顧客や社会からの過剰な要求となり、製造業をモダナイズする上での経済性そのものに悪影響を与えるものとなるので、サプライチェーン全体で守れる内容となることを期待する。
- 第6章について、具体的な対応策の事例をもっと厚くしていただき、業界全体での事例共有に期待する。
- 認証制度を作成し、海外の認証制度と相互認証などにできないか。

➢ その他

- ガイドラインにはそぐわないかもしれないが、悪意を持ったサイバーアタックの事例の公開とアタック元情報の公開/検索を可能とすることもご検討いただきたい(下記の効果を期待)。
  ①社内ブラックリストによるブロック
  ②社会的に模倣犯の抑止を期待(デジタル庁によるアタック元の特定など)