産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）工場 SWG（第 5 回）議事要旨

日時　　：令和 5 年 3 月 10 日（金）9 時 30 分～11 時 15 分

構成員　：

（座長）	江崎　浩	東京大学大学院 情報理工学系研究科教授
	市岡　裕嗣	三菱電機株式会社名古屋製作所ソフトウエアシステム部部長 （代理：松田　規、柴田　陽一）
	岩﨑　章彦	一般社団法人電子情報技術産業協会 セキュリティ専任部長
	榎本　健男	一般社団法人日本工作機械工業会 技術委員会標準化部会電気・安全規格専門委員会委員 （三菱電機株式会社名古屋製作所ドライブシステム部 専任）
	桑田　雅彦	日本電気株式会社 デジタルネットワーク事業部門　兼　テクノロジーサービス部門 サイバーセキュリティ事業統括部 シニアプロフェッショナル（サイバーセキュリティ） （Edgecross・GUTP 合同工場セキュリティ WG リーダー）
	斉田　浩一	ファナック株式会社 IT 本部情報システム部五課 課長
	佐々木　弘志	フォーティネットジャパン合同会社 OT ビジネス開発部 部長 （IPA ICSCoE 専門委員）
	斯波　万恵	株式会社東芝 サイバーセキュリティ技術センター 参事 （ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
	高橋　弘宰	トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
	中野　利彦	株式会社日立製作所 制御プラットフォーム統括本部 大みか事業所 セキュリティエバンジェリスト
	藤原　剛	DMG MORI Digital 株式会社 制御開発本部コネクティビティー部 副部長
	松原　豊	名古屋大学大学院 情報学研究科准教授
	村瀬　一郎	技術研究組合制御システムセキュリティセンター 事務局長
	渡辺　研司	名古屋工業大学大学院 社会工学専攻教授

議題　：

１．　開会

２．　制御システムにおけるセキュリティ対策推進の取組について

３．　ガイドラインの普及について

４．　令和４年度に行った調査結果及び今後の取組について

５．　自由討議

６．　閉会

要旨　：

1.　制御システムにおけるセキュリティ対策推進の取組について

・　資料３を IPA 高見様より説明

2.　ガイドラインの普及について

・　資料４を高橋委員より説明

3.　令和４年度に行った調査結果及び今後の取組について

・　資料５を事務局より説明

4.　自由討議

（1）調査結果を踏まえた取り組みの方向性に関するご意見

・　本社のポリシーと現場のオペレーションに乖離があることが多々ある。アンケート結果について、本社のポリシーと現場オペレーションの乖離が認識できるよう、回答者の属性ごとの分析を行ってほしい。

・　経済産業省による各業界団体向けセミナーの実施や SC3 との連携等により、業界団体を通じて広く企業に周知できるとよい。より具体的な例や、実際の対策など、業界団体から、より具体的な対策を展開いただくことが有効な普及策になりうる。

・　各業界特有のリスクと設備や製造等守るべきものの優先度に応じた対策の検討をするべきであ

る。また、半導体業界や自動車業界等、同じ業界の事業者間で情報を共有できるような場を作ってほしい。

- KYT（危険予知トレーニング）のようなわかりやすい手法は、セキュリティ面で現場の底上げに資するものである。セキュリティを検討している者や経営層と、現場とのギャップが明確になる点でも有効である。
- 事業者毎にリスクが異なる点について、BCP の考え方やシステムの差異を踏まえた工場システムのマトリックスを整理することで、ガイドラインの活用ができるのではないか。
- 製薬会社等、セキュリティに対する関心が高い業界にもアプローチしてほしい。IPA はもちろん、JPCETRT/CC とも連携してほしい。
- 工場 SWG でも発表いただいた半導体とプラント等の業界にもアプローチを進めていただきたい。

（2）工場のスマート化に向けた対応（仮説）に関するご意見

- デジタル臨調は、現状のアナログベースの工場のオペレーションを、どのようにデジタル化していくかという観点でテクノロジーマップを作り、要求条件を整理している。IoT デバイス等やシステムのセキュリティ要件を提示した上で、スマート化を進めるという考え方。経済産業省所管の業界と情報交換をしながらデジタル臨調の検討を進めていけば、各社の内規を含めた見直しが必要になるのでデジタル臨調の取組と経済産業省の歩調を合わせて、戦略的に検討できるとよい。
- Society5.0 を背景としたスマート化やサプライチェーン上の脅威の観点は重要。工場を持つ顧客から聞くと、対策が IT・OT 間にファイアウォールを設置して完了することが多いようだが、PC や USB メモリ等により工場内部で感染する場合もある。工場のスマート化においても工場の内部対策について検討できるとよい。アンケート結果からデータ利活用が進められていることが明らかになったが、日本の工場のほとんどがオンプレミスのデータセンターでデータ利活用を行っており、クラウドの活用が進んでいない現状がある。クラウドにどのように移行するとよいか、そもそもクラウドに移行する必要があるか、クラウド化により本当に儲かるか等を今後議論する必要がある。また、スマート化は大手を想定していると思うが、中小企業では取引先から要請されて OT・IT を切り離しているケースも多い。どのように安全に OT・IT を繋げるかを示せると、中小規模の方々の DX 化を推進できるのではないか。
- 自動化に完全に移行する形に近づいた際、プログラム的には正しいが、製品として正しくない事態を人間がどう確認するかが重要であり、全体の枠組みの中にスマート化した結果を検証する人材を入れていく必要がある。工場では、熟練工としてのノウハウを少ない人数に継承する流れがあるが、自動化の落とし穴にはまらないよう注意する必要がある。人間のノウハウや匠の知恵を考慮する点について記載できるとよいのではないか。

・ スマートファクトリーを議論の対象にするという点は重要。資料で記載されているスマート化とスマート化により発生するリスクについての共通理解が重要と考える。具体的な例が入るとわかりやすい。配送関係の工場であると、ロボット間・工場間の連携が高まることでサイバーセキュリティのリスクの対象範囲が広がり、人材が減ることでインシデント対応の必要性が高まる。また、製造業の場合は、これまで人とロボットの間に仕切りを置くことで安全性を担保してきたが、スマート化によりロボットと人間の距離が近くなると、ロボットの停止だけではなく人に危害を与えるリスクが高くなる。従来のリスクと、スマート化した際のリスクを深掘りできるとよい。

・ 海外進出に重きを置く事業者が多いと考えるが、日本のセキュリティ対策が海外でも通用するということを、データを基に示せるとよい。国によって労働者の意識も異なり、適切なセキュリティ対策も異なる。日本の工場の海外進出を後押しできるとよい。

・ 大規模システムにおける人間とシステムの関係においては、人間を重視した考え方や人間の日頃の判断力が大切であるということも記載できるとよい。

・ 自動化が進展すると、異常やシステム障害に対する人間の対応能力の養成が求められる。資料の多様なインシデントの経験に類するが、異常をいかに検知し、どのようにリカバリーをするかは重要であり、そのために演習・訓練が有効である。異常な事態に対応できる能力の養成に向けた人材教育・訓練の必要性を強調いただきたい。

・ 重要インフラ保護の観点では技術の研究開発に注力しがちだが、運用技術をどのように養成していくかも非常に重要である。CSTI の研究開発においても、運用という観点での研究開発と、それを実現するためのソフトウェアを含めた人材の必要性を指摘している。運用での人材開発はスマート化の中でも強調する必要がある。

・ セキュリティの専門人材だけではなく、DX に関わるクラウドや AI など幅のある人材の育成が重要。

・ スマート化について、大企業以外の Tier2・3 サプライヤーや中小企業では人材・金銭的制約があるものの、サプライチェーン上で対策が求められているのが実態である。スマート化以前のセキュリティ対策でも同様だが、具体的な対策方法に加え、有効なアウトソーシング先や人とお金に限りがある中でどのような対策が有効か示せると、よい支援になるのではないか。

・ 今後自動化システム系を納める際に、お客様への説明に向けてクラウド化の指針を示せるとよい。中小企業においてクラウド化に対して拒否反応がある現状、そのような指針を示すことで、企業が次のステップに進む後押しができると考える。

・ クラウド化の成功事例があると理解してもらいやすい。今後、可能な範囲で成功事例について共有いただけるとよい。

・ スマート化により外部との接続が増え、サプライチェーンでの連携が増していく中、個々のセキュリ

ティ対策の連動をどのように行うか検討していただきたい。

・ プロダクトやコンポーネントに対するセキュリティ対策も諸外国の法規制によって要請されており、工場側の義務にも影響しているので諸外国の規制を踏まえて検討する必要がある。

・ Tier2・3 や中小企業の状況を紹介すると、ある工程にセンサーを付けて、データを取りながら、なぜ不良が生じるか等の分析をし始めたところであるが、人間が見るとすぐわかる不良を AI はまだ判別できず、人間と AI のギャップがあるのが現状である。人口減少の中で DX 化が進み、セキュリティ対策の必要があるが、Society5.0 のような世界を実現するために、どのように Tier2,3 サプライヤーを巻き込めるか、どのように底上げしていくかを常に念頭に置いて検討を進める必要がある。

・ 中小企業を含め支援することが重要である。Tier2・3 がセンサーを導入しつつある段階であれば、セキュリティが確保されたセンサーを導入いただく方向に誘導することも、工場 SWG の重要なミッションである。

（以上）