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 6 回）議事要旨

日時　　：令和 5 年 10 月 6 日（金）10 時～12 時

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
	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 プラットフォーム・テクノロジーサービス事業部門セキュリティ事業統括部 IoT/OT セキュリティグループ ディレクタ （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四課 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 大セキュリティエバンジェリスト （名古屋工業大学 ものづくり DX 研究所 客員教授）
	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．　工場のスマート化に関する取組について

３．　スマート工場におけるセキュリティ対策推進の取組について

４．　ガイドラインの拡充版について

５．　ガイドラインの普及啓発について

６．　自由討議

7.　閉会

要旨　：

1.　工場のスマート化に関する取組について

・　資料３を経済産業省製造産業戦略企画室より説明

2.　スマート工場におけるセキュリティ対策推進の取組について

・　資料４を IPA 高見様より説明

3.　ガイドラインの拡充版について

・　資料５を事務局より説明

4.　ガイドラインの普及啓発について

・　資料６を事務局より説明

・　資料７を今野様（TXOne）より説明

・　資料８を桑田委員より説明

・　資料９を斯波委員より説明

5. 自由討議

(1) 工場のスマート化に対する取組に関するご意見

- ソフトウェア分野においても、構成が複雑化している状況においてソフトウェア部品の情報を共有する SBOM という仕組みが国際連携の中で求められている。製造業においてもこのような仕組みがあれば活用すべきであるし、ないのであれば仕組み化を進めていかないと、サプライチェーンから断絶するリスクを把握することが難しいと考える。

(2) ガイドラインの拡充版に関するご意見

- 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインの付録 E のチェックリストを活用しているという顧客が多い。拡充版についても同様のチェックリストを追加いただけると良い。
- ガイドラインの読者は、スマート化に対して異なるイメージを持つことが想定される。セキュリティ対策の重要性を認識いただくためにも、スマート工場やスマート化という言葉の定義を明確にする必要がある。
- 経済産業省サイバーセキュリティ課において検討されている IoT 機器に対して求められるセキュリティ要件や、デジタル臨時行政調査会におけるテクノロジーマップに定義される DX におけるセキュリティ要件等、他の取り組みと足並みを揃える必要がある。工場に IoT 機器が導入される場合にこれらの要件を参照するようにすると、整合性が取れるのではないか。
- 現状スマート工場のレベル分けが 5 段階でなされているが、それぞれのレベルでどのようなリスクが発生するかを示せると良い。例えば、レベル 1・2・3 では、データのやり取りにおいてクラウド利用がなされると、セキュリティが関連する。レベル 4 になると、ロボットの動作による人の安全の影響や、無人化された工場の障害発生時の対応等を検討する必要がある。各レベルの具体的なリスク例を提示できると、読者にとってわかりやすいのではないか。
- 読者は工場全体がレベル 3・4 になるイメージを持つ可能性もある。しかし、ゾーニングにより、同じ工場内でも部分的にレベル 3・4 にレベルアップができる。中小企業を 1 つのゾーンのように捉え、中小企業が連携することもできる。スマート化のレベルを工場全体で考えるのではなく、システムや実現したい事項毎に検討できると良いのではないか。
- 中小企業では、工場内の一部のシステムをロボット化して自動化を進める一方で、IT ネットワークを接続していない等、部分的なスマート化の取り組みに止まり、全体としてはまだスマート化が進展していないケースもある。そのような企業でもガイドラインを参照しやすいようにしていただきたい。
- ユースケース含めて整理いただけるとより使いやすくなると考えられる。

・ 工場 SWG 委員ではない作業部会メンバーについては、工場 SWG にオブザーバーとして参加いただけると良い。

・ SEMI Taiwan のように、調達要件としてセキュリティ認証やガイドラインへの準拠を求める事例が増えているように見える。ガイドラインにおいて、調達要件としてセキュリティが求められる動向を示せると良い。調達要件を国がトップダウンで仕組み化することはあり得ると考える。国の調達要件として求められると、関連する産業がその調達要件を参考にすることもあり、特定の業界で起きたことが別の業界でも導入される可能性はある。特定の業界に関する情報だけでも有益であるため、今後も調達動向に関する情報共有ができると良い。

(3) ガイドラインの普及啓発に関するご質問・ご意見

・ 普及活動を行う上で、製造業の大半は中小企業である。普及啓発においては中小企業を巻き込むことが重要であり、IPA のサイバーセキュリティお助け隊サービス制度等と同様に、各地域の商工会議所とも連携できると良い。

・ 1 点目、サプライチェーンに関する議論に、中小企業の工場（含む町工場）における DX 推進とセキュリティ強化を両輪とした取り組みをどのような仕組み・やり方で展開するかという論点をより強く織り込む必要がある（業界別のガイドライン簡易版や取組みに係る経済的インセンティブ等）。2 点目、IT セキュリティ人材よりも絶対的に不足している OT セキュリティ人材をどのように確保するのか、産官学それの役割で、短期的対応と中長期的対応を戦略的に組み合わせた対策を行動に移すことが急務と考える。3 点目、サイバー攻撃関連のインシデントレスポンスの際に有効な警察への通報、及びそれ以前に相談できる体制をどのように各地域で確立し、その実効性を担保・向上できるのか、といった議論も必須ではないものの必要だと考える（特に対中小企業）。

（以上）