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 1 回）議事要旨

日時　　：令和 4 年 1 月 6 日（月）14 時 00 分～16 時 00 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
	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　兼　サイバーセキュリティ事業部　兼 デジタルプラットフォーム事業部　シニアエキスパート ソフトウェアアドバンストテクノロジスト(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株式会社　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
	西雪　弘	三菱電機株式会社 FA ソリューションシステム部　部長
	藤原　剛	ビー・ユー・ジーDMG 森精機株式会社 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. 産業サイバーセキュリティ研究会 WG 1 工場 SWG の議事運営について
2. 産業サイバーセキュリティ研究会 WG1 工場 SWG の設置について
3. 経済産業省委託調査「令和 2 年度スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査」結果概要の紹介
4. 東大グリーン ICT プロジェクト・Edgecross「工場セキュリティガイドライン(案)概要編」の紹介
5. 自由討議

要旨　：

1. 産業サイバーセキュリティ研究会 WG 1 工場 SWG の議事運営について

- 資料 3『本会議の運営について（案）』の通り。
- 本会議の運営方針に関して、委員からの意見・質問はなし。

2. 産業サイバーセキュリティ研究会 WG1 工場 SWG の設置について

- Society5.0 では、新たな付加価値が増加する一方、サイバーセキュリティのリスクが増加している。
- 経済産業省では、産業サイバーセキュリティ研究会を設置し、これに紐づき 3 つの WG を設置している。今回の工場 SWG は WG1 に紐づく形の位置付け。
- Edgecross・東大合同 WG が 2 月を目途にガイドラインを発行する予定であり、現在発行に向けた作業を行っているものと承知。このガイドラインを本 SWG の検討でも参照させていただきつつ、工場 SWG のガイドラインとして発行するにあたり必要な点について議論いただきたい。
- なお、当該ガイドライン案については、3 月に開催を予定している第 3 回 SWG で取りまとめることを想定している。

3. 経済産業省委託調査「令和 2 年度スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査」結果概要の紹介

- スマートファクトリーにおけるセキュリティを検討するため、工場におけるデータ利活用の状況、セ

キュリティ脅威と対策、ステークホルダー、関連法制度や規格等についての調査を行った。

- 従来の工場、データ利活用が進みつつある工場、インダストリー4.0 に代表される工場では求められるセキュリティが異なるため、データ利活用の段階毎にレベルを設定した。
- データ利活用のユースケースを定め、取り扱われるデータ、そのデータが脅威にさらされた場合のリスク、必要なセキュリティ対策例を整理した。また、データ利活用のシステムモデルを元に想定脅威を整理した。
- ガイドライン策定にあたり取り込むべき観点として、新設工場と既設工場、工場規模、データの利活用の段階等が挙げられた。また、リスクベースで検討を行うことが重要であり、国際規格と調和する形で、サイバー・フィジカル・セキュリティ対策フレームワークを踏まえて整理することが受け入れられやすいのではないかとの意見が得られた。
- スマートファクトリーのステークホルダーは様々であり、各々がセキュリティについて実施すべきことを進める必要がある。

4. 東大グリーン ICT プロジェクト・Edgecross「工場セキュリティガイドライン(案)概要編」の紹介

- 工場のセキュリティを推進させるため、セキュリティの必要性・危機意識の啓発、対策方法の説明、アウトソースという選択肢の掲示を基本コンセプトとしてガイドラインの素案を作成した。
- 想定読者は、システム及びセキュリティの調達要件を作成する方、工場 FA/OT システムの利用者、経営者、システムの構築者・管理者、システムのメーカーの方などである。
- IT 側のガイドラインはすでにあるため、本ガイドラインは FA/OT システム固有の課題に絞って執筆した。新設/既設のその両方を対象としている。古い機器を置き換える動機付けをする内容と、古い機器を継続利用しなければならない際に注意すべきことを併記している。
- 以上の内容を工場セキュリティガイドライン概要編の第 1 章にまとめた。第 2 章では工場 FA システムのセキュリティに対する基本的な考え方を示し、読者が第 3 章以降を読み進める予備知識として、考え方の全体像を把握できるように努めた。第 3 章では典型的な工場 FA システムを想定しシステムの全体像・構成を設定した。
- 第 4 章以降は、具体的なセキュリティの内容となる。第 4 章では、保護対象、脅威・影響をまとめた。第 5 章では、工場内のセキュリティだけではなく、法規制・標準規格・ガイドライン準拠や各ステークホルダーからの要求など、工場を取り巻く社会的セキュリティ要件をまとめた。
- 第 6 章でセキュリティ対策の全体像および具体例を示した。物理面・システム構成面、OODA・PDCA・サプライチェーンというように多面的な内容となっている。また、自社にセキュリティの技術が無くとも、セキュリティベンダが提供する製品・サービスを活用する方法があることも記

載した。

- 最後に、中小企業でもセキュリティを導入できるよう、補足となる考え方を第 7 章に示した。
- 付録にこのガイドラインに沿ったチェックリスト、調達仕様テンプレートを記載した。
- さらに、事例紹介を行う別冊を作成する予定である。

5. 自由討議

（１）ガイドラインの目的・スコープについて

- 東大グリーン ICT プロジェクト・Edgecross ガイドラインは大手の電子機器メーカーがユースケース例として記載されているが、本 SWG 第二回のヒアリングには、自動車、家電、半導体、医療機器・ヘルスケア、鉄鋼が予定されている。スコープを明示的に変えていくということか。
  - ➢ 一つのガイドラインにすべての分野を盛り込むのは困難。共通的に必要となる事項を概要版として取りまとめてはどうかと考えている。他方、業界ごとに状況が異なり、業界によっては個別に議論が進んでいるものと認識。各業界で本ガイドラインをどう使っていただけるかについても、第 2 回のヒアリングでも確認できればと考えている。
- 初版は準備編ないし計画導入編の位置づけとすると、事業継続の観点をどう入れるかも重要。素案では OODA や PDCA などは軽く触れられているのみだが、全体像を広く浅く見据えるのか、準備・導入を深く記載するのかによって、タイトルも変えた方がよい。
- 次版以降、インシデントレスポンスやリカバリーについて、工場単体ではなく、事業継続の観点での工場の役割が頭出しできると良い。例えば、多数の工場を保有するメーカーでは、ある工場が機能不全となった場合、能動的に他の工場に振り替えても事業を継続しなければいけない。
- 本社からの命令を実施するのみでは工場のセキュリティは守れない。本社の方針の確認やその調整をするなどを含めて、現場が上から言われたことをこなすだけという構図を変えた方が良い。指示に対して具体的なチェック方法が書かれていると良い。
- 中小・零細企業のセキュリティ対策については、部屋の施錠などの物理的対策も不十分である可能性がある。それらを実施した上でネットワークやサイバーセキュリティの必要性に訴求する方が良い。
- 今回のガイドラインは、中小企業を含めたセキュリティの底上げも目的となり得る。高度な標的型攻撃もあるがそれはごく一部であり、むしろ人為的ミスでウイルスが混入してしまうことなどを前提にして書けると良い。攻撃者のレベルやその対策のレベルの意識合わせをすべきである。

- 概要編で高いレベルのセキュリティを示すと、既存の工場の実態と合わない可能性がある。本ガイドラインでは既存のシステムにフォーカスを当て、将来的にシステムを拡張することとするのが良いのではないか。
- スコープや範囲は早い段階で適切に整理しておく必要がある。対策には物理セキュリティとサイバーセキュリティの両方が含まれているが、資産や保護対象はサイバーセキュリティに偏っている。特に物理的な対策をどこまで含めるのかを議論すべき。
- 目的はサイバーセキュリティの確保だけでなく、セーフティやクオリティなどの確保なので、物理セキュリティを含むことは必然。
- 物理的対策について、水道に関する記載が不足している。冷却水や機器の稼働に必要な水など、水の循環は最近米国でも意識されている。
- 同じ工場の敷地内であっても製造するものの変更や人の入れ替えが生じることなどを考えると、工場のライフサイクルマネジメントは製品のライフサイクルと一緒に変化するのではないか。
- ベンダー企業の立場から見ても、日本では小さい規模の企業がまだ多く、セキュリティ担当がいない企業さえある。そのような企業もスムーズに理解できるようなガイドラインになると良い。
- 昨年度の委託調査結果の中で、工場におけるデータ利活用の段階をレベル 0～レベル 4 と示していたように、工場の置かれている状況によって、やるべきことや対策方法は異なる。来年度以降、レベルに応じて求められる対策や考慮すべき事項を検討する活動ができると良い。

（２）ガイドラインの構成について

- 概要編にしてはボリュームが多い。例えば Part1 に要求事項を記載し、次に対象のシステム、共通的なセキュリティ実施事項、運用面での対策、組織面での対策等をよくある手順に沿って書くなど整理してはどうか。
- チェックリストやテンプレートはぜひ各社に知恵を出していただきたい。RRI でも調達時のチェックリストを作っているので参考にするとよい。附属書を充実化させる方向性も一案。
- 専門家でない方が読んだ時に、事例が無いと理解が難しいのではないか。
- 自動車、半導体、鉄鋼、医療等の業界における状況とこのガイドラインで想定するユースケースとがどう異なるのかを整理したうえで、ユースケースごとの読み替えや参考をつけた方が良い。
- 生産現場の実態、例えば、ものづくり日本大賞や GOOD FACTORY 賞を取った企業に事例を紹介するのはどうか。

（3）他のガイドライン・リファレンスモデルとの対応について

- ISO/IEC JTC 1 でスマートマニュファクチャリングに関するリファレンスモデルやフレームワークアーキテクチャの検討が進められている。
- ステークホルダーからセキュリティ対策を要求される時に、標準やガイドラインへの準拠を求められ得る。それらは常に更新されるので、オリジナルを参照するのが実用的。
  - グローバルサプライチェーンの観点もあり、海外の事業にて活用できるようにするためには、国際規格との対応関係についても今後議論が必要。
- 自動車分野だと WT29 で OT ファクトリーに関する言及がある。自動車会社がどのようなことを OT ファクトリーに求めているか意見をいただき、それに対応できるようなガイドラインになると良い。
- 欧州等の諸外国と相互に認証し合うなどのレベルまで作成できれば、中小企業もカバーできるようなガイドラインになるのではないか。
  - 国際的な枠組みについて、これまでも産業サイバーセキュリティ研究会の関連ガイドラインは英訳して海外にも発出してきた。RRI との連携も重要になると考えている。

（4）公開について

- 工場には多くのステークホルダーがいるので、完成度を上げるには時間がかかる。ガイドラインは世の中に早く出して、色々な立場の方から意見を得ながらブラッシュアップすることが重要である。
- 日本におけるガイドラインが経済産業省から発出されて、リファレンスになっていくことが重要である。

（5）普及・啓発活動について

- 6 月以降に普及啓発という線表だが、ルートや媒体について次回以降議論できると良い。業界団体やベンダーからのアプローチと、フィールドである経済産業局や中小企業診断士など、様々なルートが考えられる。どのような普及啓発ができるのか、選択肢を整理できるとよい。
  - 工場でセキュリティ対策を進めているのは、IoT 活用や AI 分析などをしたいというモチベーションで、一緒にセキュリティ対策に投資をしているケースが多い。それゆえ、DX を推進する経済産業省の組織などと連携を高めて行ければ良い。ガイドラインのユーザーとなり得る方々から、どのような形であれば受け取りやすいか、各業界での議論も進めていただいている中でどう活用いただけるのかご意見を伺いたく、それが普及に向けた最初のステップと考えている。その上で、これをどう周知するのが適切か、様々なチャネルを考えていきたい。産

業界の方々とは、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）の関係団体を集めた枠組みも活用できるのではないか。

（以上）