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 2 回）議事要旨

日時　　：令和 4 年 2 月 28 日（月）16 時 00 分～19 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
	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．　開会

２．　製造業における DX について

３．　工場セキュリティに関する取組みについて

４．　工場セキュリティに関する動向について

５．　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」について

６．　自由討議

７．　閉会

要旨　：

1.　製造業における DX について

・　資料３を経済産業省製造産業局より説明

2.　工場セキュリティに関する取り組みについて

・　資料４－１を日本自動車工業会より説明

・　資料４－２を電子情報技術産業協会半導体部会より説明

・　資料４－３を NEC プラットフォームズより説明

・　資料４－４をパナソニックより説明

・　資料４－５を日本鉄鋼連盟より説明

・　資料４－６を日本医療機器産業連合会より説明

・　資料４－７を日本工作機械工業会より説明

3.　工場セキュリティに関する動向について

・　資料５を重要生活機器連携セキュリティ協議会（CCDS）より説明

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」について

・ 資料 6『工場セキュリティガイドライン改版状況共有資料』を桑田委員より説明

5. 自由討議

（1）発表者への質問

・ 自動車工業会ではガイドラインを作成しているが、具体的な議論は自動車工業会で行われているのか。また、本ガイドラインに同業他社と情報共有するべきと記載すべきかご意見を伺いたい。

・ 自動車工業会の発表の中の重点項目について、これらが出てきた背景は何か。

・ 昨年、台湾で SEMI の 6506 が出た。半導体業界では議論が進んでいるのか。

・ 工場での生産設備・機器のセキュリティの強化として、設備メーカーにセキュリティの対策の要求は何かしているのか。

（2）スコープについて

・ 本ガイドラインのスコープは今回ヒアリングを行う業界以外もカバーできるとよい。食品、医薬品などの業界では、サイバー攻撃が消費者の健康に影響する可能性がある。

・ 前回、セキュリティの観点から冷却水が重要という議論があった。工場では品質などにフォーカスしがちになるが、排水、排気などは工場の周りの環境に影響する。これらの要因はガイドラインの中で共通に扱えるのではないか。

（3）ガイドラインの読みやすさについて

・ 本ガイドラインの読み進め方を冒頭に作成してはどうか。読者の課題に対応する章・節を示す方法、別紙に誘導する方法、想定読者と読んで欲しい個所を図や表で示す方法などがある。

・ 自ら対策可能な企業と外部に頼らざるを得ない企業がいること、また、産業をどう強くしていくかという観点がある。ガイドライン記載の対策を行うことで、新しい産業ができるようになるとよいという意見が以前の産業サイバーセキュリティ研究会であった。これらを意識して読み進め方を作成するとよい。

・ 必要最低限やるべきことが不明確であるという意見が一部の発表者からあった。

・ 必要最低限何をすればよいかという事項を勧告なのか推奨なのかわかるように区別して作成し

た方がよい。

- ガイドラインに対する解説書や現場向けにセキュリティの心得を作成している団体があった。このような良い点は、本ガイドラインにも取り入れていきたい。

（４）事業継続性について

インシデントが起きた際、工場で対策を行っている状況で、全社的には事業継続性の観点から工場の稼働を能動的に停止するという判断もありうる。BCP の観点でこのような考え方もわかるようにガイドラインの記載ぶりを工夫すべきではないか。

（５）情報共有組織（Information Sharing And Analysis Center: ISAC）について

- 現状把握のため ISAC が重要。各団体ライフサイクルマネージメントの観点で取り組んでいる印象を受けたが、ISAC は手薄に感じた。
- ガイドラインでは、ISAC のような取組も含め、業界を通した情報連携の必要性について記載がされればポジティブな対策になるのではないか。
- 本 SWG は、今後も多くの団体の方にご参加いただき、業界をまたいだ情報共有の機能も果たすことができれば、さらによいものとなるのではないか。

（６）情報提供

- CCDS からドローンに対するセキュリティガイドラインが発行される予定。最新の情報をふまえ、最低限必要な要件やリスクアセスメントなどを含んだガイドラインを発刊する。
- CCDS は現在 OSS のセキュリティの調査をしている。これも本ガイドラインに役に立つ内容となるだろう。

（７）その他ガイドラインに対するコメント

- 国際標準の参照先が正しいか、参照漏れが無いかの再確認が必要である。
- 法令や国際標準に基づく対策と本ガイドラインとの位置づけの明確化が必要である。
- サプライチェーンのコストも鑑みた最適化が必要である。
- ガイドラインの定期的なメンテナンスが必要である。

・ リスク例に対する対応が不明瞭である。

・ 要求を受ける窓口が異なることで、コンフリクトが発生しないか懸念する。

・ Edgecross コンソーシアムメンバー以外の企業のソリューションの競争力が削がれる懸念があるという声もあることから、相応の配慮が必要。

（以上）