経済産業省

資料４

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

経済産業省

サイバーセキュリティ課

産業機械課

１．産業サイバーセキュリティ研究会、WG１と
　　工場SWGの位置づけ

２．工場関係のサイバーセキュリティを取り巻く現状

３．工場SWGの設置について

４．ご議論いただきたい点

１．産業サイバーセキュリティ研究会、WG１と工場SWGの位置づけ

２．工場関係のサイバーセキュリティを取り巻く現状

３．工場SWGの設置について

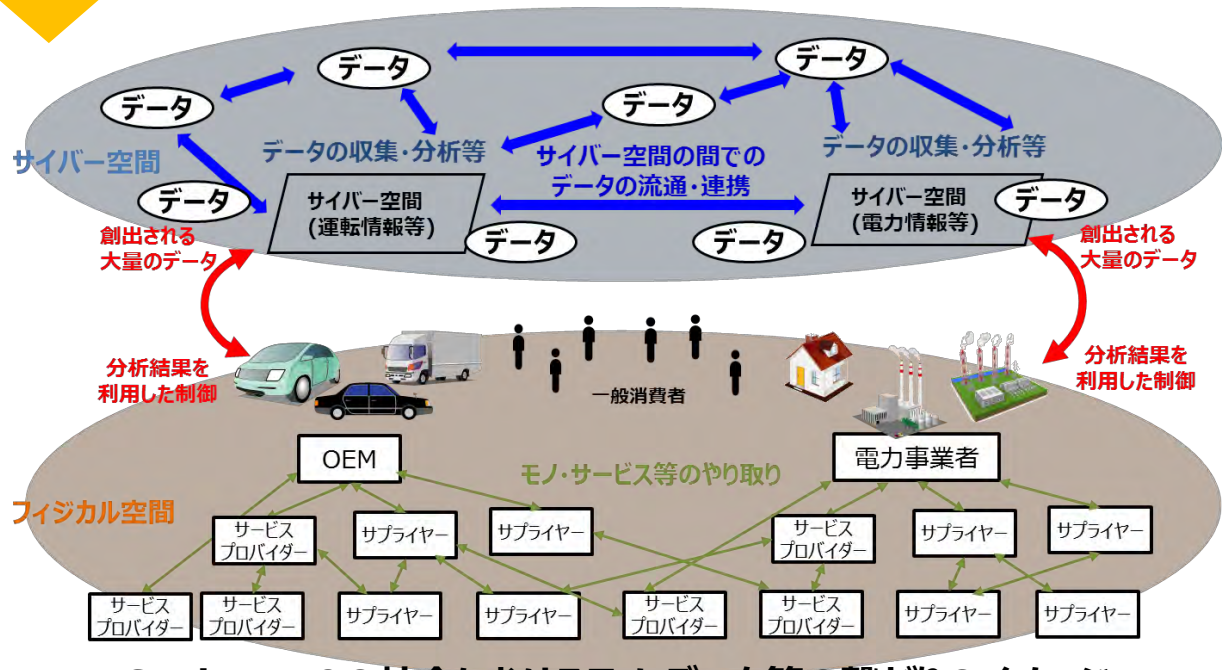
４．ご議論いただきたい点

サイバー・フィジカル・セキュリティ対策フレームワークの策定
＜サプライチェーン構造の変化＞

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**となる。

「Society5.0」以前

個々の企業主体の定型的なつながりで価値を生み出す



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

産業サイバーセキュリティ研究会WG１の位置づけ

- 平成29年12月27日、産業サイバーセキュリティ研究会第1回を開催。**我が国の産業界がサイバーセキュリティに関して直面する課題に対応していくためのＷＧの一つとして、制度・技術・標準化を検討するWG１を設置**。

産業サイバーセキュリティ研究会　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/

■政策の方向性を提示

ＷＧ１　制度・技術・標準化

■制度・技術・標準化を一体的に政策展開する戦略を議論

ＷＧ２　経営・人材・国際

■サイバーセキュリティ政策全体の共通基盤となる経営・人材・国際戦略を検討

ＷＧ３　サイバーセキュリティビジネス化

■セキュリティサービス品質向上と国際プレーヤー創出に係る政策を検討

連携

中小企業政策審議会基本問題小委員会等

■中小企業の生産性向上に資するIT利活用支援策とともに検討

分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化 とテーマ別TFにおける検討

- **産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、3つの**タスクフォース（TF）を設置**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

- **ビルSWG**
  - ガイドライン第1版の策定(2019.6)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - 2021年11月に第3回を開催
- **工場SWG（新設）**

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
データの信頼性確保に向け「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」骨子案のパブリックコメントを実施。

ソフトウェアTF：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

検討事項：
OSSの管理手法に関するプラクティス集の策定、SBOM活用促進に向けた実証事業（PoC）を検討。

『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。

＜参考＞２層TF：IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

- **用途や使用環境によって課題が異なるIoT機器・システムに対するセキュリティ対策を、複数のステークホルダー間で合意する**際に活用できる**「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」を2020年11月5日に公開。**
- 本フレームワークで、IoT機器・システムをカテゴライズし、カテゴリごとに求められるセキュリティ・セーフティ要求の観点を把握・比較することにより、**それぞれに求める対策の観点・内容の整合性を確保できる**。

フィジカル・サイバー間をつなげる
機器・システムのカテゴライズのイメージ

カテゴリに応じて求められる
セキュリティ・セーフティ要求の観点のイメージ

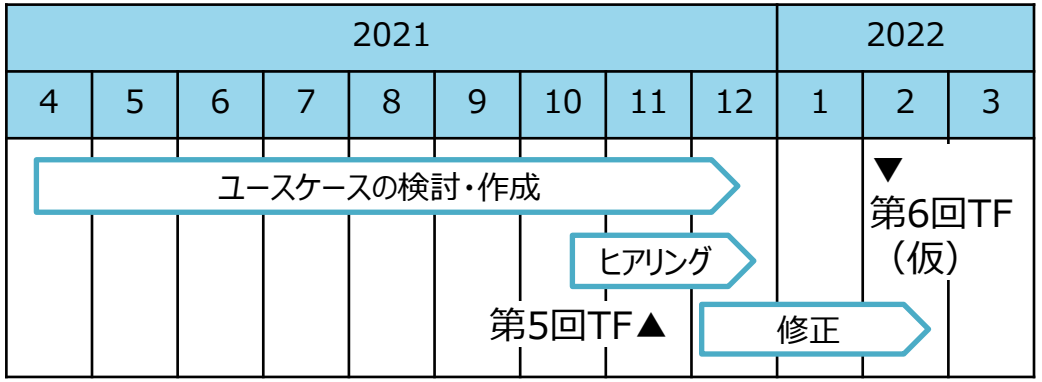
※　同じ機器・システムでも使用形態などによってマッピング先が異なり得る。
例えば、機器ｇと機器ｈが同じ機器で異なる使用形態である場合などがあり得る。）

＜参考＞2層TF：IoT-SSFのユースケース作成

- R3年度内に、IoT-SSFのユースケース集を作成し、IoT-SSFの付属文書として公表予定。

＜作成スケジュール＞

- 令和3年度内に、5つ程度のユースケースを検討・作成する。
  （ユースケースの対象については、
  次頁以降を参照のこと。）
- ユースケースの作成前後に、各ユースケースに関連する企業等へヒアリングを行う。



＜アウトプットイメージ＞

- ユースケース集（詳細をまとめた文書と概要スライド）を、IoT-SSFの付属文書として公表予定。

文書の目次（案）

1. 本文書の位置付けと構成
   - 1-1「IoTセキュリティ・セーフティ・フレームワーク」の概要
   - 1-2 本文書の目的と構成
   - 1-3 想定読者
2. 「IoTセキュリティ・セーフティ・フレームワーク」実践に係るユースケース集
   - 2-1 対象となるユースケース
   - 2-2 ユースケースにおける記載事項
   - 2-3 具体的なユースケース

添付A 対策要件
添付B 対策例

＜参考＞2層TF：ユースケース一覧（検討中）

- 前頁の考え方に基づき、詳細化を進める対象として、以下の6ケース（※）を選定した。

No	ユースケース	IoT機器を導入する現場	（参考）リスクの大きさ	
			回復困難性の度合い	経済的影響の度合い
1	ガス給湯器の遠隔操作（ガス給湯器）	消費者現場	大	小
2	ドローンを活用した個人による写真撮影（ドローン）	消費者現場	小	小
3	物流倉庫における自動ピッキング（ピッキングロボット）	物流現場	小	大
4	プラント施設内の設備（プラント設備）	製造現場	大	大
5	工場における部材加工作業の自動化（例：溶接ロボット）	製造現場	小	中
6	金属製造現場における状態監視用機器（例：温度センサー）	製造現場	小	中

１．産業サイバーセキュリティ研究会、WG１と
　　工場SWGの位置づけ

２．工場関係のサイバーセキュリティを取り巻く現状

３．工場SWGの設置について

４．ご議論いただきたい点

情報セキュリティ10大脅威　2021

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	標的型攻撃による機密情報の窃取
3	テレワーク等のニューノーマルな働き方を狙った攻撃
4	サプライチェーンの弱点を悪用した攻撃
5	ビジネスメール詐欺による金銭被害
6	内部不正による情報漏えい
7	予期せぬIT基盤の障害に伴う業務停止
8	インターネット上のサービスへの不正ログイン
9	不注意による情報漏えい等の被害
１０	脆弱性対策情報の公開に伴う悪用増加

出典：IPA資料（https://www.ipa.go.jp/files/000089239.pdf）

情報セキュリティ10大脅威　2021

【1位】ランサムウェアによる被害
～組織を狙ったランサムウェアの攻撃が増加～

IPA

- 2020年の事例/傾向②
  - 特定の組織に特化したランサムウェア(※1)
    - ・自動車メーカーがサイバー攻撃から大規模システム障害
    - ・国内外の工場で出荷が一時停止
    - ・従業員のPCが使えなくなる等オフィス系ネットワークシステムにも影響

【出典】
※1　ホンダを標的に開発か、ランサムウェア「EKANS」解析で見えた新たな脅威
https://xtech.nikkei.com/atcl/nxt/column/18/00989/062400028/

出典：IPA資料（https://www.ipa.go.jp/files/000089239.pdf）

工場におけるサイバー攻撃事例

- アルミニウム工場のマルウェア感染（2019年、ノルウェー）

事象

- ✓ ノルウェーのアルミニウム製造大手で大規模なマルウェア感染
- ✓ 「LockerGoga」と呼ばれるランサムウェアに感染
- ✓ 発生直後、プレス加工等の一部生産、オフィス業務に影響
- ✓ プラントは影響拡散防止のためシステムから分離
- ✓ 被害は、最初1週間で3億～3億5000万ノルウェークロネ（4000万ドル相当）と推定

- 石油化学プラントの安全計装システムを狙ったマルウェア（2017年、中東）

事象

- ✓ 中東の石油化学プラントで使用されていた Schneider Electric 社製の SIS コントローラー(Triconex)がマルウェア感染
- ✓ SISのエンジニアリング・ワークステーションへのリモートアクセスを取得、SISシステムのゼロデイ脆弱性を利用して改ざん
- ✓ プラントが緊急停止

- 自動車工場（ホンダ）のマルウェア感染（2017年、日本）

事象

- ✓ 大手自動車メーカーの工場でコンピュータがWannaCryに感染
- ✓ 工場に据え付けの設備に付属するパソコンが感染
- ✓ 生産ラインの制御システムに影響が発生し、一時的にラインを停止
- ✓ 約1千台の車両生産に影響

１．産業サイバーセキュリティ研究会、WG１と
　　工場SWGの位置づけ

２．工場関係のサイバーセキュリティを取り巻く現状

３．工場SWGの設置について

４．ご議論いただきたい点

工場SWGの設置

【現状認識・課題】

- 経済産業省は、産業・社会の変化に伴うサイバー攻撃の増大に対し、リスク源を適切に捉え、検討すべき対策を漏れなく提示するための新たなモデルとして「**サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）**」を提示した。このCPSFを実現するため、フィジカル空間とサイバー空間を繋ぐ機器・システムに対するセキュリティについても検討を行っている。
- 従来の工場内システムはインターネットには曝されないことを前提に設計されてきたが、IoT化の流れの中で、**フィジカル空間に存する個別の機械やデバイスやその関連センサーといった末端部分が直接サイバー空間のインターネットに接する**ことにより、知らない間にセキュリティホールが生じるなど、**新たなセキュリティリスク源が増加**しつつある。
- 今後、データの見える化や、遠隔制御、自動化等の進展に伴い、**IPアドレスを保有するデバイス・機器がサプライチェーンの一層広域にまで広がる**ことに鑑み、**足元でのリソースや危機意識に乏しい中小企業も含め**、**工場におけるセキュリティリスク対策は一層重要**になってくるものの、**ステークホルダー間の相互信頼の土台となる考え方が整理できているとは言い難い状況**。

【方向性】

- このため、今年度、工場のサイバーセキュリティ対策の推進に向けた**ガイドラインを取りまとめる**ことを目標とし、産業サイバーセキュリティ研究会ＷＧ１に紐づける形で、**工場のサイバーセキュリティ関係者により構成する「工場ＳＷＧ」を設置する**。

当面のスケジュール（イメージ）

2022年

- **１月６日　第１回**
  - 経産省委託調査結果の紹介
  - 進行中の取組の紹介
  - 今後の方向性について

- **２月　第２回**
  - 工場ユーザーからのヒアリング（業界ごとの取組状況、課題、ニーズ等）
  - 工場セキュリティガイドラインのとりまとめに向けた整理

- **３月　第３回**
  - 工場セキュリティガイドラインのとりまとめ
  - 令和４年度以降の進め方

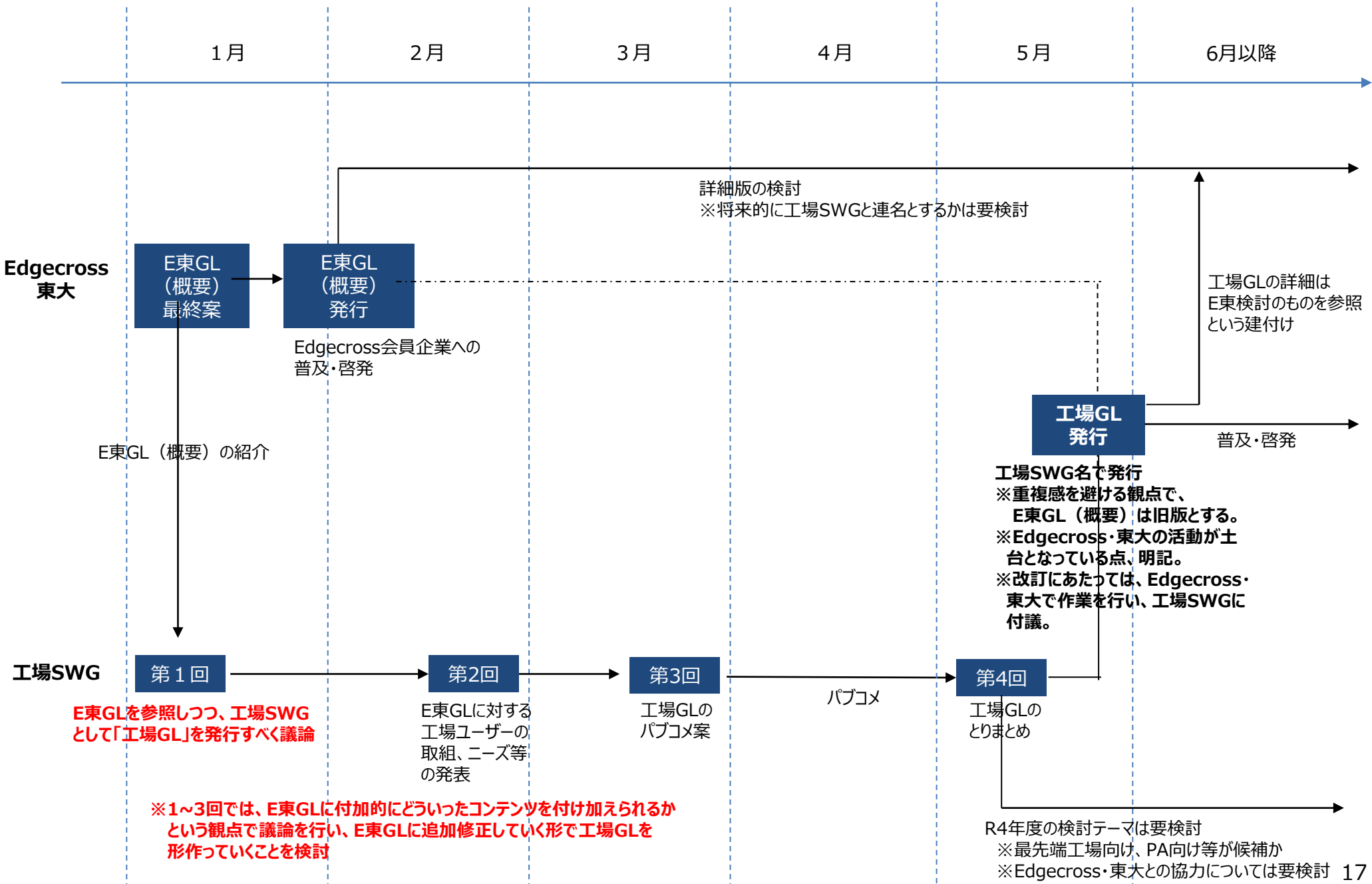
１．産業サイバーセキュリティ研究会、WG１と
　　工場SWGの位置づけ

２．工場関係のサイバーセキュリティを取り巻く現状

３．工場SWGの設置について

４．ご議論いただきたい点

Edgecross・東大合同WGと工場SWGのスケジュールイメージ



第２回でのユーザーヒアリング対象（イメージ）

- 製品・部品の加工や組立等を行う工場（FA）を持つユーザーを基本的には対象とし、原料製造等の際に流量、温度、圧力等を管理する工場（PA）を持つユーザーは関心に応じて対応を行う。
- その上で、生産方式や産業の性質等を勘案し、ヒアリング対象業界を選定。
- 各業界の中で、本SWGに対する興味関心が高い個社から、本ＳＷＧで、取組状況、課題、ニーズ等について発表していただくことを想定。

【ヒアリング対象業界のイメージ】

- 自動車
- 家電
- 半導体
- 医療機器・ヘルスケア
- 鉄鋼

４．ご議論いただきたい点

- 我が国の工場セキュリティに関する取組の課題
- Edgecross・東大合同WGガイドライン
  - Edgecross・東大合同WGのガイドラインに、本SWGでの議論も踏まえ付加的にエッセンスを付け加える形で、工場SWGとしてガイドラインを発行してはどうか。
  - その際に、ユーザー目線での重複を避ける観点で、Edgecross・東大合同WGのガイドラインを引き継ぐ形で工場SWGのガイドラインを発行してはどうか。
  - その場合に、より広範なユーザーに行き届くことを念頭に置くと、どのような事項を付加していくべきか。

【留意事項】
- 工場SWGガイドライン発行の際には、Edgecross・東大合同WGのガイドラインは旧版として扱うものの、Edgecross・東大合同WGの活動が土台になっていることがわかるようにする（例：連名で発行、前書き等本文中での言及）。
- 工場ＳＷＧガイドライン改訂の必要が生じた際には、改訂作業をEdgecross・東大合同WGが行い、改訂案を工場SWGに付議することとする。

- スケジュール
  - 足下でガイドラインをとりまとめつつ、来年度以降、各者においてどのような取組が必要となるか（ガイドライン策定・改訂の方向性、普及・啓発等）。
- ユーザーヒアリング対象
  - ヒアリング対象とすべき業界、ヒアリング内容（取組内容、課題、ニーズ等）について。