産業サイバーセキュリティ研究会
WG1『第2層：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
（第3回）議事要旨

1．日時・場所

日時：令和2年2月26日（水）～3月6日（金）（書面開催）

2．委員等

委員　　：松本委員（座長）、青木委員、石原委員、伊藤委員、岩崎委員、荻野委員、梶屋委員、
神余委員、北澤委員、戸枝委員、西貝委員、野口委員、松元委員、渡部委員

オブザーバ：内閣官房　内閣サイバーセキュリティセンター、警察庁、総務省、厚生労働省、防衛装備庁、
国立研究開発法人産業技術総合研究所、独立行政法人情報処理推進機構、
技術研究組合制御システムセキュリティセンター、独立行政法人製品評価技術基盤機構、
一般財団法人電気安全環境研究所、電子商取引安全技術研究組合、
一般財団法人日本情報経済社会推進協会、一般財団法人日本品質保証機構

3．配布資料

資料１　議事次第・配布資料一覧
資料２　委員名簿
資料３　『第２層：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の検討の方向性
資料４　フィジカル空間とサイバー空間のつながりの信頼性を確保するためのフレームワーク（案）

4．議事内容

書面審議の結果、委員からの主な意見は以下のとおり。

- タイトルについて、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）を分かっている人には何のことか理解できるが、そうでない人には伝わりにくい。また、本フレームワークを広めていくためにはCPSF のような呼びやすい略称が必要。IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）はどうか。
- 資料４図２の「限定的なダメージ（リカバリが容易）」の例として「名前等の個人情報の漏えい」とあるが、一般には名前と何かしらの情報がセットで漏えいすることが多く、その場合はリカバリが容易とは言えないのではないか。
- 資料４図４で第１軸（赤）と第２軸（緑）が一直線上に並んでいるのは分かりにくいのではないか。
- 同じシステムや機器でも、脅威によって被害は異なるので、資料４図５は誤解を招く可能性がある。同じ機器を複数配置したほうがいいのではないか。
- 同じ機器でもマッピング先が異なり得ることを、図に関連させて記載した方が分かりやすいのではないか。
- 資料４図６の青い軸は、「セキュリティ・セーフティの強度」とあるが、実際には「観点」ではないか。

- 資料４3-3-2の第２の観点「フィジカル・サイバー間をつなぐ機器・システムの運用中の確認要求」について、3-3-3 と明確に区別するために、「運用中のフィジカル・サイバー空間をつなぐ機器・システム」と表現した方がいい。

各委員から頂いた意見を踏まえて座長に相談し、フレームワーク案に修正を加えた上で、産業サイバーセキュリティ研究会ワーキンググループ1及び同分野横断サブワーキンググループに報告することで了承を得た。

以上

お問合せ先

商務情報政策局　サイバーセキュリティ課
電話：03-3501-1253