産業サイバーセキュリティ研究会
第6回 ワーキンググループ1（制度・技術・標準化）
第4回 WG1分野横断サブワーキンググループ
合同会議
議事要旨

1. 日時・場所

日時：令和3月9日(月)～3月17日(火)（書面開催）

2. WG1委員等

委員　　：佐々木委員（座長）、岩見委員、上原委員、江崎委員、太田委員、岡村委員、
片山委員、九野委員、小松崎委員、白石委員、其山委員、高倉委員、坂委員、
平田委員、松尾委員、松本委員、渡部委員

専門委員　：瓜生専門委員、坂下専門委員、田中専門委員

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、金融庁、総務省、外務省、
文部科学省、厚生労働省、農林水産省、国土交通省、防衛装備庁

3. 分野横断SWG委員等

委員　　：佐々木委員（座長）、青木委員、石原委員、岩﨑委員、大久保委員、岡田委員、
粕谷委員、川口委員、桑名委員、後藤（俊）委員、後藤（里）委員、古原委員、
谷委員、中尾委員、平田委員、舟山委員、洞田委員、山田委員、吉田委員、米田委員

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、総務省、防衛装備庁

4. 配布資料

資料１　議事次第・配付資料一覧
資料２　WG1 委員名簿
資料３　WG1 分野横断 SWG 委員名簿
資料４　サイバーセキュリティに関連する海外の動き
資料５　サブワーキンググループ、タスクフォース等の検討状況
資料６　IoT セキュリティ・セーフティ・フレームワーク　～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～（案）

5. 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。

- 第 2 層のフィジカル空間とサイバー空間のつながりにおいては、フィジカル空間側には必ずヒトが存在しており（モノが存在する場合もあるが、その場合でも必然的にそれを扱うヒトが存在する）、IoT の使用がヒトに対して企業活動等による効用をもたらしたり、インシデントによる損失や責任を生じさせたりすることを、総論部分

において明確化してはどうか。

- IoT 機器の想定外の使用はどのように位置づけられるか。いくら機器側で対策をしても、想定外の使用をされるとどうしようもない面もある。
- 観点が積み重なり、第 1 軸と第 2 軸のリスクが増大するにつれて棒グラフが上位の観点へ伸びる資料 6 図 6 の表現は、上部に行くにつれ、高リスクの際の対策のように見えてしまう。実際は、状況に応じてそれぞれの確認要求を検討し採用・実施することから、適切な表現に修正した方がいいのではないか。
- IoT 機器に対して、誰がどのような対策を検討・実施していくのか、各ステークホルダーの役割や責任分界点についても追記した方がいいのではないか。
- 第 1 軸と第 2 軸にカテゴライズされる機器やシステムを例示した方が理解しやすいのではないか。
- 転写機能を有してはいるが、IoT 機器とは言い切れないものも存在するため、本フレームワークのスコープは IoT 機器に限定されると受け止められる表現にしない方がいいのではないか。
- 本フレームワークに基づいて具体的な対策を検討するためには、原因や発生確率の分析・評価が必要であることを考えると、JIS Q 31000 等の既存のプロセスの過程の中で本フレームワークの考え方を取り入れる事例を示せると良いのではないか。

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、パブリックコメントを実施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