経済産業省

IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

令和2年11月５日

経済産業省　商務情報政策局

サイバーセキュリティ課

テーマ別TFの検討状況

- 平成31年4月、**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）**を策定。
- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）にて議論。**

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
- **電力SWG**
  - 既存ガイドラインの強化
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドラインを公表
- **スマートホームSWG**
  - ガイドライン案パブコメ
- ・・・

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：
データマネジメントを俯瞰するモデルを提案し、データの信頼性確保に求められる要件を検討

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等

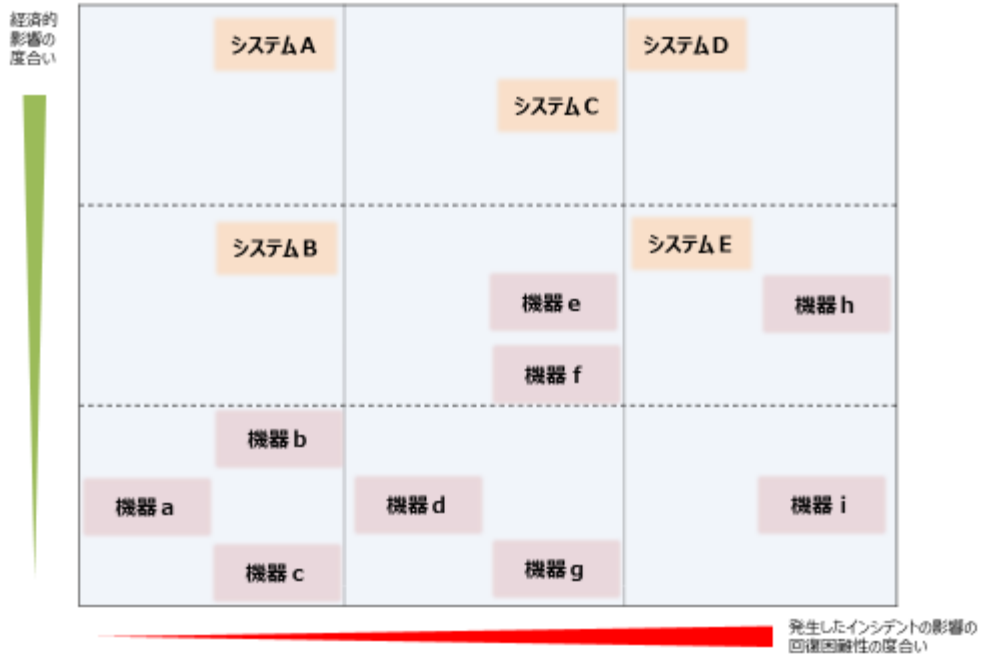
『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

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)」のドラフト策定

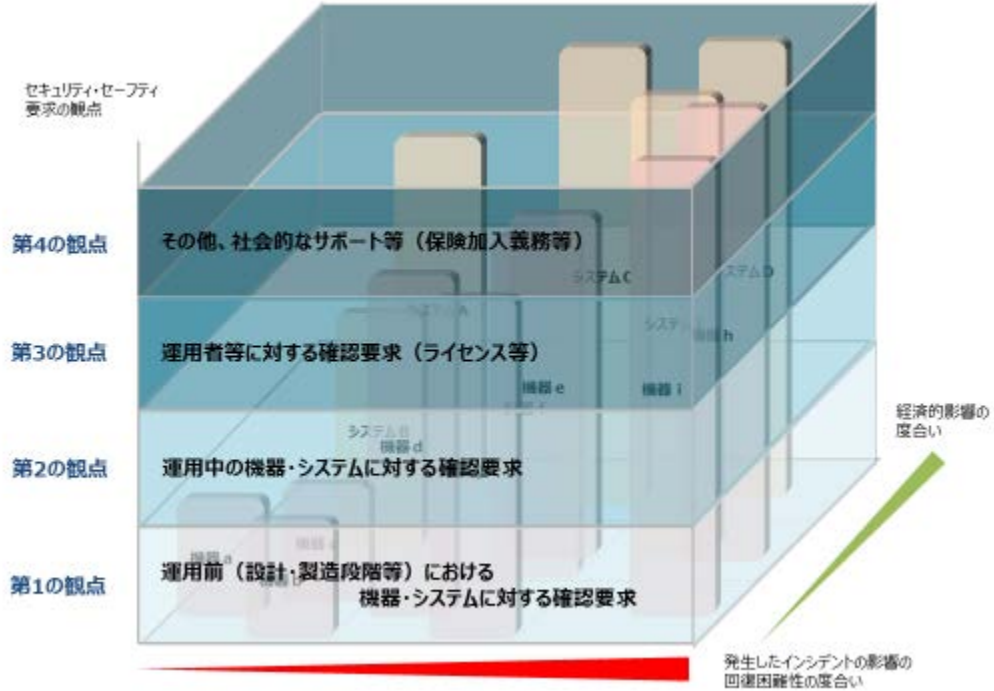
IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）について

- サイバー空間とフィジカル空間が高度に融合した「Society5.0」、「Connected Industries」では、サイバー空間とフィジカル空間の境界において、情報が正確に変換されること、つまり転写機能の正確性を確保することが極めて重要。
- IoT機器・システムの性質や利用環境によって課題が一様ではないことに着目し、IoT機器・システムをリスクに応じてカテゴライズした上で、それぞれに対するセキュリティ・セーフティ要求を検討することに資するフレームワーク「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」を策定。

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。）

IoTセキュリティ・セーフティ・フレームワークのパブコメ概要

- **IoTセキュリティ・セーフティ・フレームワーク**の原案に対するパブリックコメントを令和2年3月31日～6月24日に実施。
- 海外からの関心が高く、英語版パブコメも実施。
- **国内15、海外10の組織・個人より、約100件の意見提出**あり。

主な御意見

① **IoT-SSFのコンセプトやスコープ**に関する御意見
② **リスクに基づく機器・システムのカテゴライズ**に関する御意見
③ **求められるセキュリティ・セーフティ要求の観点**に関する御意見
④ **具体的な実装や要求事項**に関する御意見
⑤ **国際規格やガイドライン等との関係**に関する御意見
⑥ **用語の定義**に関する御意見
⑦ **今後の取り組み**に関する御意見