サイバー・フィジカル・セキュリティ対策フレームワーク（案）の修正概要

資料３

8月3日第3回WG1でお示しした見直し方針

フレームワークの考え方の明確化

- 目的、適用範囲、対象、想定する読者等を冒頭で明示
- 価値創造過程の定義や信頼の確保の考え方についてコンセプトの説明を行う部分に記載
- 6つの構成要素で整理する根拠、目的を追記
- マルチステークホルダーの考え方を明記

国際規格等との対応関係の整理

セキュリティ対策例のレベル分け

今回の修正点

０．全体構成の見直し

第Ⅰ部　コンセプト：サイバー空間とフィジカル空間が高度に融合した産業社会における産業分野のサイバーセキュリティのあり方
第Ⅱ部　ポリシー　：リスク源の洗い出しと対策要件の特定
第Ⅲ部　メソッド　：セキュリティ対策要件と対策例集

１．フレームワークの考え方の明確化

（１）冒頭にフレームワークの使い方等に関する考え方を整理
（２）コンセプトの説明の充実
（３）三層構造アプローチと6つの構成要素を利用したリスク源の洗い出し方法の提示

＜リスク源の洗い出しのポイント＞
① バリュークリエイションプロセスに関わるステークホルダーとの関係の整理
② IoT機器を介したサイバー空間とフィジカル空間の融合により発生する新たなリスクの把握
③ 組織を跨るデータの流通の仕方の把握
④ 各層における信頼性の基点の確保

（４）ユースケースの作成

２．国際規格等との比較

（１）NIST CSF、NIST SP800-171、ISO/IEC 27001の各管理策等と本フレームワークの対策要件の関係の整理
（２）その他、NIST SP800-161等の主な国際規格の内容も参照

３．コストも考慮したレベル別の対策例の作成

（１）High、Middle、Lowで対策例を提示