経済産業省

資料6

WG1の今後の進め方（案）

平成30年8月3日

経済産業省　商務情報政策局

サイバーセキュリティ課

1. パブリックコメントを受けたサイバー・フィジカル・セキュリティ対策フレームワークの見直し

2. 分野横断SWG（仮称）の設置

3. 今後のスケジュール

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見直し方針

- 国内外からのパブリックコメントの意見を踏まえ「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）の記載・構成を以下の観点から見直す。

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の記載位置を変更（前方に移動）
- 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

国際規格等との対応関係の整理

- グローバルハーモナイゼーションの観点から、各対策項目と、既存の海外主要規格等との対応関係を明確にする。
- 特に、**米国政府が国際標準化を推進する『NIST Cybersecurity Framework』の機能分類と対比**した上で、**対策項目の整序や統合を含む再構成を実施**する。

対応する海外主要規格等の記載（案）

- 『サイバー・フィジカル・セキュリティ対策フレームワーク』の各対策項目に、海外主要規格等の対応するサブカテゴリーを記載
- 海外主要規格等のサブカテゴリーを基準として、対応する各対策項目を整理

NIST CSFの機能分類との対比（案）

- NIST CSFの5つの機能分類にあわせて、本フレームワークの対策項目をマッピング
- 各層内の対策項目を分類するカテゴリーを追加し、対策項目を整序

	識別(ID)	防御(PR)	検知(DE)	対応(RS)	復旧(RC)
第1層	L1.001 L1.002 L1.003 ⋮	L1.005 L1.006 L1.012 ⋮	L1.003 L1.004 L1.010 ⋮	L1.003 L1.008 L1.013 ⋮	L1.002 L1.008 L1.009
第2層	L2.001 L2.003 L2.010 ⋮	L2.002 L2.013 L2.014 ⋮	L2.007 L2.008 L2.015 ⋮	L2.006 L2.009 L2.018 ⋮	(第1層の上記項目を参照)
第3層	L3.001 L3.008 L3.022	L3.002 L3.011 L3.017 ⋮	L3.001 L3.006 L3.015 ⋮	L3.004 L3.008 L3.015 ⋮	(第1層の上記項目を参照)

セキュリティ対策例のレベル分け

- 「各事業者がオペレーションレベルで活用できる」「セキュリティ対策の必要性とコストの関係を把握できるようにする」ことを目標として、**対策による効果やコスト等を考慮しながら、具体的な対策例を示す。**
- なお、産業分野ごとに守るべきものやリスクは異なる場合があるため、詳細な検討については各SWGにおいて検討する。

対策例の記載イメージ

現状の記載例

…

■構成要素毎の対策例

〇組織

- IoT機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。
- IoT機器やソフトウェアのサプライヤーを特定し、そのサプライヤーから正規品を導入する。

〇ヒト

…

各対策例に、効果やコスト等による重み付けがなされていない

対策例のレベル分け

分類後のイメージ（案）

…

■構成要素毎の対策例

〇組織

【レベル３】

- 製造システムの仕様、設計、開発、実装及び変更にセキュリティエンジニアリングの原則を適用する。開発過程におけるバグや脆弱性の修正課程が追跡可能な状態を維持する。

【レベル１】

- システム開発時にセキュリティの考慮事項を明確に含むライフサイクルが考慮されており、外部コンポーネントの導入時にはセキュリティ要

…

〇ヒト

…

【レベル分けの例】

レベル３：高いセキュリティ水準、国際規格等（ISO/IEC27002, SP800-171等）への対応

レベル２　　ʃ

レベル１：セキュリティ対策として最低減求めたい事項

1. パブリックコメントを受けたサイバー・フィジカル・セキュリティ対策フレームワークの見直し

2. 分野横断SWG（仮称）の設置

3. 今後のスケジュール

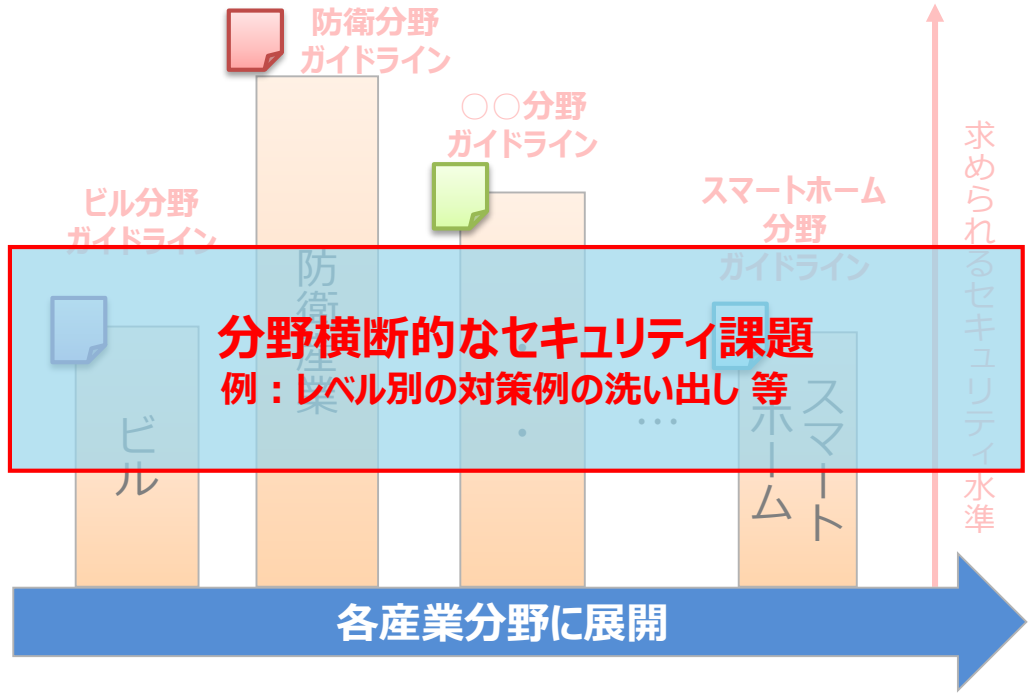
分野を横断して共通するセキュリティ課題への対応

- サイバー空間とフィジカル空間が高度に融合する「Society5.0」では、産業分野を横断した企業間のつながりやデータの流通、サービスの提供がなされることも事実。
- 産業分野別の課題や対策等を相互に持ち寄り、**分野を横断して共通するセキュリティ課題の洗い出しやその対策について検討するSWGを設置。**
- 検討結果は、**産業分野別の検討にフィードバックする**とともに、**「サイバー・フィジカル・セキュリティ対策フレームワーク」へ反映する等の取組を進める。**

サイバー・フィジカル・セキュリティ対策フレームワーク

三層別アプローチ	必要な対策のポイント
1. 企業間のつながり (主体の信頼)	セキュリティポリシーの策定、体制の整備
	事業継続計画又はコンティンジェンシープランへの反映
	・・・
2. フィジカル空間とサイバー空間のつながり (機能の信頼)	セキュリティ対策が施されたIoT機器の導入
	セキュリティバイデザインの実践
	・・・
3. サイバー空間におけるつながり (データの信頼)	信頼できるサービスサプライヤーの選定
	サイバー空間における接続相手の認証
	・・・

産業分野別のサイバー・フィジカル・セキュリティ対策



1. パブリックコメントを受けたサイバー・フィジカル・セキュリティ対策フレームワークの見直し

2. 分野横断SWG（仮称）の設置

3. 今後のスケジュール

今後のスケジュール（案）

- 本日いただいたご意見も踏まえ、『**サイバー・フィジカル・セキュリティ対策フレームワーク**』**（第二案）**に向けた修正を実施。第二案についてもパブリック・コメントを実施し、国内外から広く意見を募る。
- 並行して、分野横断SWGを設置し、分野横断的なセキュリティ対策の議論を進める。

今後のスケジュールのイメージ