経済産業省

資料４

産業サイバーセキュリティ研究会WG1
分野横断SWGの設置について

平成30年10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

1. 産業サイバーセキュリティ検討会、WG1の検討経緯

2. 分野横断SWGの設置

サイバーセキュリティ政策の方向性

1. 産業政策と連動した政策展開

① **重要インフラの対策強化**
－情報共有体制強化　等

② **IoTの進展を踏まえたサプライチェーン毎の対策強化 (Industry by Industry)**
－防衛関係、自動車、電力、スマートホーム等の分野別検討と技術開発・実証の推進

③ **中小企業のサイバーセキュリティ対策強化**

2. 国際ハーモナイゼーション

① **日米欧間での相互認証の仕組みの構築**

② **民間主体の産業活動をゆがめる独自ルールの広がり阻止**

3. サイバーセキュリティビジネスの創出支援

① **産業サイバーセキュリティシステムを海外に展開**

② **サービス認定創設、政府調達などの活用**

4. 基盤の整備

① **経営者の意識喚起**

② **多様なサイバーセキュリティ人材の育成（ICSCoE等）**

③ **サイバーセキュリティへの過少投資解決策の検討**

産業サイバーセキュリティ研究会とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催

→ **産業サイバーセキュリティ強化へ向けた**
アクションプラン（４つの柱）を提示

構成員

※第2回開催時点

石原　邦夫　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、
東京海上日動火災保険株式会社相談役

鵜浦　博夫　日本電信電話株式会社代表取締役社長

遠藤　信博　日本経済団体連合会情報通信委員長、
日本電気株式会社会長、サイバーセキュリティ戦略本部員

小林　喜光　経済同友会代表幹事、
株式会社三菱ケミカルホールディングス取締役会長

中西　宏明　株式会社日立製作所会長、
(日本経済団体連合会会長)

船橋　洋一　アジア・パシフィック・イニシアティブ理事長

宮永　俊一　三菱重工業株式会社社長

村井　純(座長)慶應義塾大学教授、サイバーセキュリティ戦略本部員

渡辺　佳英　日本商工会議所特別顧問、
大崎電気工業株式会社取締役会長

オブザーバー

NISC、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、防衛省

サイバーセキュリティ基本法
改正にて対応（NISC）

3/9
閣議決定

WG１
（制度･技術･標準化）

第１回　2/7
第２回　3/29
第３回　8/3

１．サプライチェーン強化パッケージ

WG２
（経営･人材･国際）

第１回　3/16
第２回　5/22

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３
(サイバーセキュリティビジネス化)

第１回　4/4
第２回　8/9

４．ビジネスエコシステム創造パッケージ

産業分野ごとの検討の促進：分野別のSWGの設置

- WG1で検討する『サイバー・フィジカル・セキュリティ対策フレームワーク』を、産業分野別に順次展開し、具体的適用のためのセキュリティポリシーを検討。

1. 産業サイバーセキュリティ検討会、WG1の検討経緯

2. **分野横断SWGの設置**

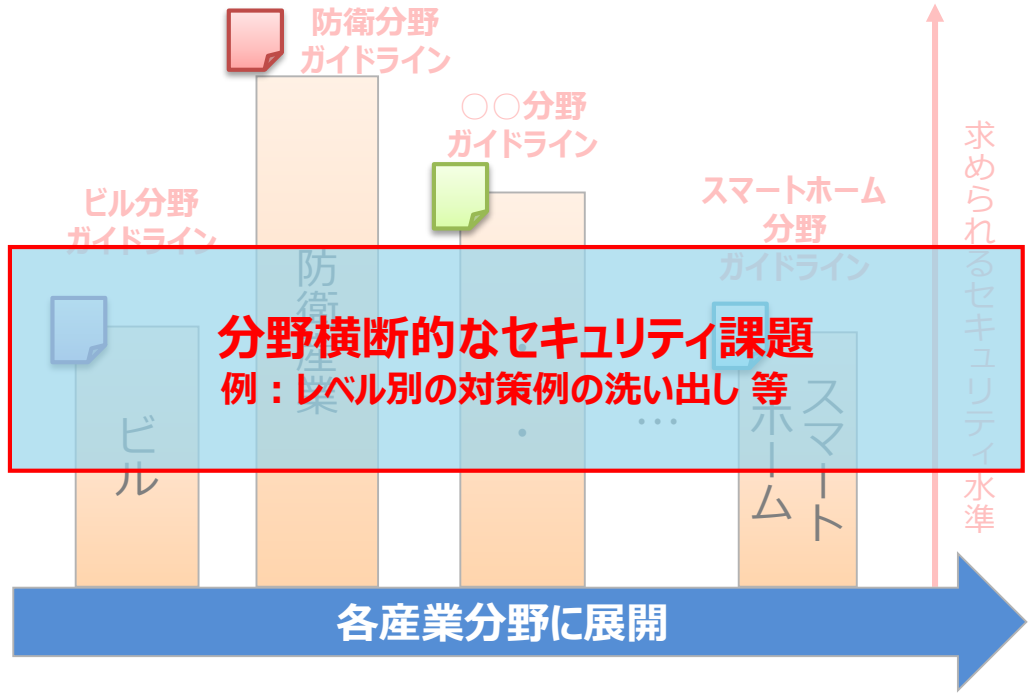
分野を横断して共通するセキュリティ課題への対応

- 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

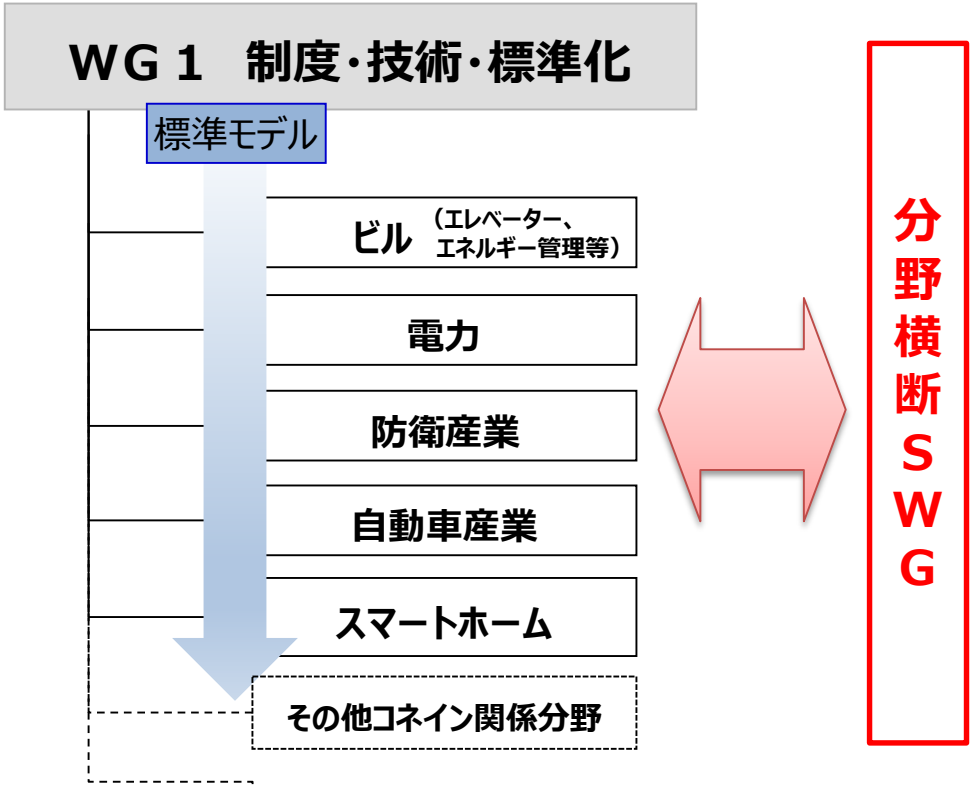
三層別アプローチ	必要な対策のポイント
1. 企業間のつながり (主体の信頼)	セキュリティポリシーの策定、体制の整備
	事業継続計画又はコンティンジェンシープランへの反映
	・・・
2. フィジカル空間とサイバー空間のつながり (機能の信頼)	セキュリティ対策が施されたIoT機器の導入
	セキュリティバイデザインの実践
	・・・
3. サイバー空間におけるつながり (データの信頼)	信頼できるサービスサプライヤーの選定
	サイバー空間における接続相手の認証
	・・・

産業分野別のサイバー・フィジカル・セキュリティ対策



分野横断SWGの検討事項と進め方（案）

- 各産業分野における検討から、分野を横断して共通するセキュリティ課題を洗い出した上で、その対策の方向性等を『サイバー・フィジカル・セキュリティ対策フレームワーク』に具体的に反映するための検討を実施する。検討の結果は、適宜、産業分野別SWGにフィードバックする。
- 当面は、産業分野別SWGの検討状況も踏まえ、現在の『サイバー・フィジカル・セキュリティ対策フレームワーク』の見直しを中心とした検討を実施する。
- 分野横断SWGの開催に加えて、検討事項に応じてメールベースでの議論も予定。



1. **分野を横断して共通するセキュリティ課題の検討**
   - 産業分野別SWGの検討状況に応じて、検討課題を選定する
   - 検討結果は産業分野別SWGにフィードバック
2. **現在の『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**
   - 国内外からのパブリックコメントの意見を踏まえた修正について検討

分野横断SWGの検討スケジュール（案）

➢ 10月5日（本日）第1回

- 『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。

➢ 11月下旬～12月上旬　第2回

- 『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。
- 産業分野別SWGの検討における課題の共有。

12月中旬 第4回 WG1
- **『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）の議論**

12月下旬～来年１月上旬
- **『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）のパブリックコメント実施**

➢ 来年2月上旬以降 第3回

- パブリックコメントを踏まえた『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。