経済産業省

資料５

『サイバー・フィジカル・セキュリティ対策フレームワーク』について

平成30年９月4日

経済産業省

サイバーセキュリティ課

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策定する目的

- 「Society5.0」、「Connected Industries」の実現へ向けて、**産業構造、社会の変化に伴うサイバー攻撃の脅威の増大に対応することが必要**。
- **このため、産業に求められるセキュリティ対策の全体像を整理**し、**産業界が活用できる『サイバー・フィジカル・セキュリティ対策フレームワーク』の策定**を進めている。

１．各事業者がフレームワークを活用することで期待される効果

- **「Society5.0」、「Connected Industries」の実現に求められるセキュリティの確保**
- **製品・サービスのセキュリティ品質を差別化要因（価値）にまで高めることによる競争力の強化**

２．フレームワークの特徴

①　各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる

- 社会として目指すべき概念だけではなく、各事業者が実際にセキュリティ対策を実施するうえで活用できる内容にする。

②　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

- サプライチェーン全体を構成する中小企業を含めた事業者が、実際に対策を行えるよう、想定されるリスクと必要な対策のコストのバランスをイメージできるような内容にする。
- セキュリティレベルを保ったままでコストを圧縮できるような内容にする。
- リスクシナリオベースの考え方も考慮した内容にする。

③　グローバルハーモナイゼーションを実現する。

- グローバルサプライチェーンの中で、日本における製品・サービスのセキュリティ対策が海外からも認められるよう、諸外国の動きをよく取り入れ、ISMSやNIST Cybersecurity Frameworkなど米欧などの主要な認証制度との整合性を確保し、相互承認を進めていくことができる内容にする。

フレームワークの構造～「Society5.0」型サプライチェーン“価値創造過程”への対応

- **「Society5.0」（人間中心の社会）、「Connected Industries」では、製品/サービスを生み出す工程（サプライチェーン） も従来の定型的・直線的なものとは異なる、多様なつながりによる非定型の形態を取る。**
- 本フレームワークでは、このような**「Society5.0」型サプライチェーンを**これまでのサプライチェーンとは区別して認識するため、**価値創造過程（バリュークリエイションプロセス）と定義**。

本フレームワークは、価値創造のための活動が営まれる産業社会を、 **三層構造**と**6つの構成要素**で捉え、包括的にセキュリティポイントを整理し、それらに対応するための指針を示す。

◆三層構造

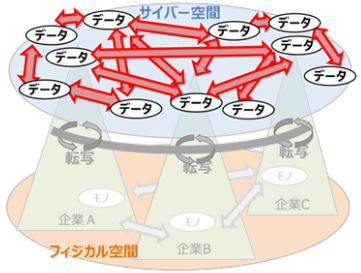
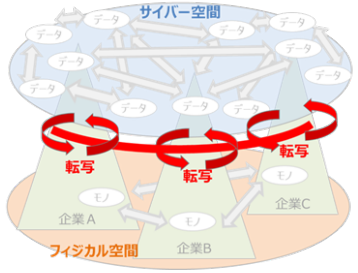
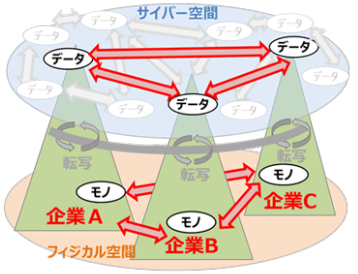
第3層－　サイバー空間におけるつながり

第2層－　フィジカル空間とサイバー空間のつながり

第1層－　企業間のつながり（従来型サプライチェーン）

◆６つの構成要素

－組織、ヒト、モノ、データ、プロシージャ、システム

三層構造	概念図
サイバー空間におけるつながり 【第３層】	
フィジカル空間とサイバー空間のつながり 【第２層】	
企業間のつながり （従来型サプライチェーン） 【第１層】	

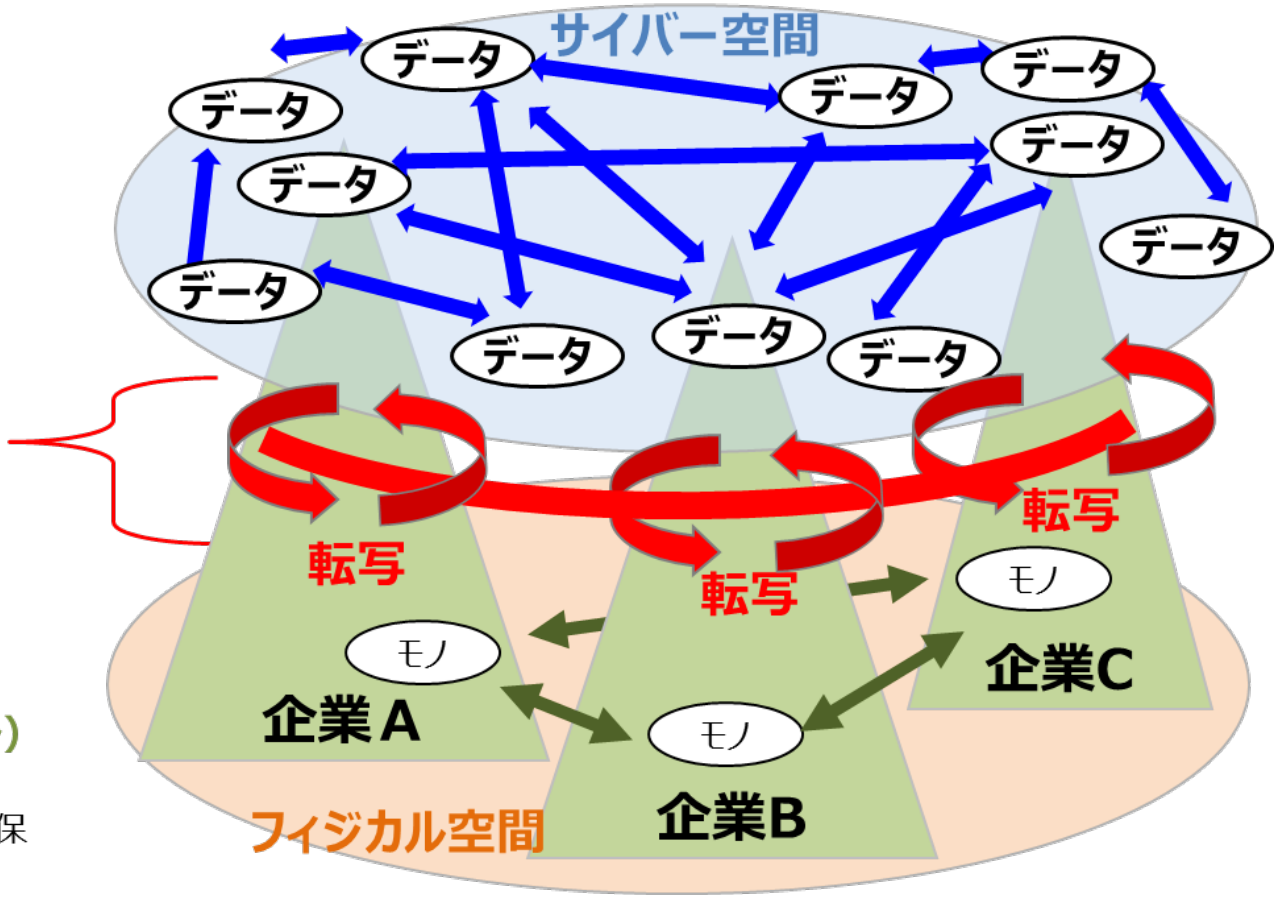
三層構造アプローチの意義

- 各層には、価値創造過程において確保されなければならない機能・役割が存在。
- 本フレームワークでは、各層で創造される価値の持つ特徴を踏まえた対応の方針を示す。

サイバー空間におけるつながり
【第３層】
- 自由に流通し、加工・創造されるサービスを創造するためのデータの信頼を確保

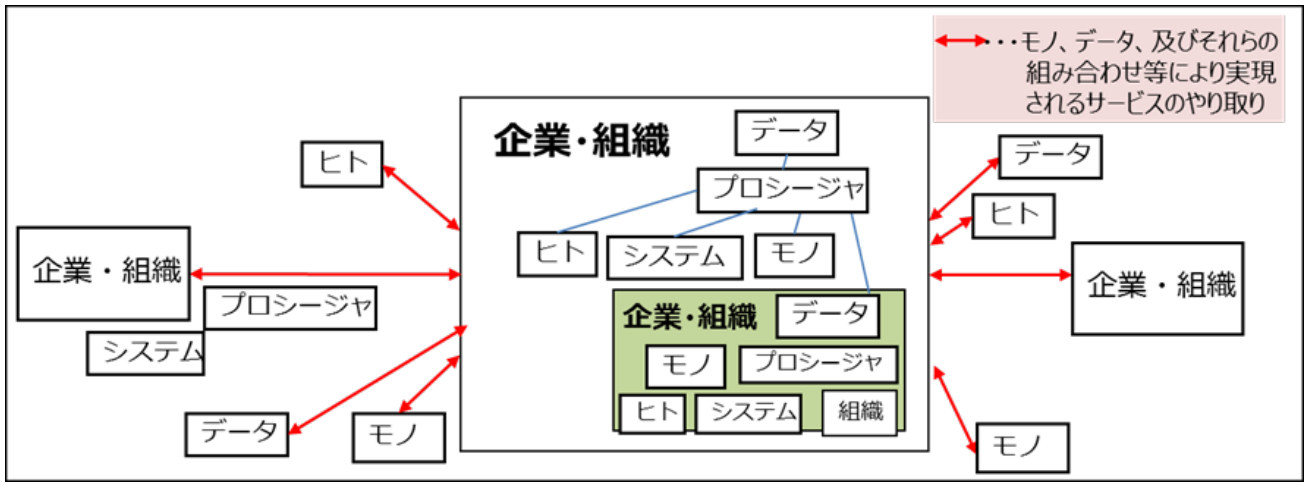
フィジカル空間とサイバー空間のつながり
【第２層】
- フィジカル・サイバー間を正確に“転写”する機能の信頼を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり（従来型サプライチェーン）
【第１層】
- 適切なマネジメントを基盤に各主体の信頼を確保

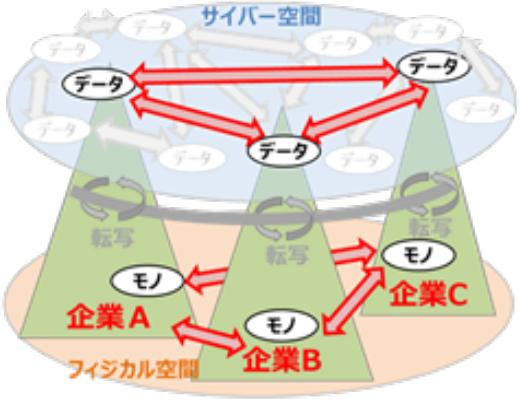
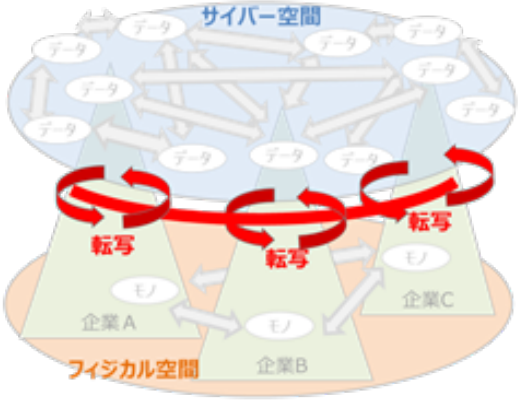
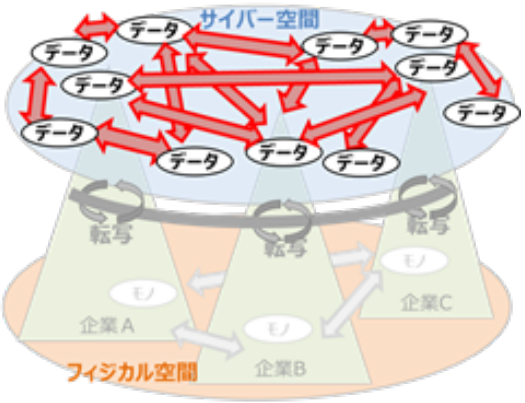


価値創造過程に関わる６つの要素と構成要素の関係

構成要素	定義
組織	• 価値創造過程（特に、従来型サプライチェーン）に参加する企業・団体
ヒト	• 組織に属する人、及び価値創造過程に直接参加する人
モノ	• ハードウェア、ソフトウェア、及びそれらの部品
データ	• フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	• 定義された目的を達成するために要求される定型化された一連の活動
システム	• サービスを実現するためにモノで構成される仕組み・インフラ



各層におけるセキュリティ対策の概要

	企業間のつながり（従来型サプライチェーン）【第１層】	フィジカル空間とサイバー空間のつながり【第２層】	サイバー空間におけるつながり【第３層】
新たなサプライチェーン構造の整理			
守るべきもの	・仕様どおりの製品、サービス ・組織の信頼	・正確な転写機能 ・レジリエンス	・セキュアなデータ流通 ・サイバー上での信頼あるデータサービス
セキュリティリスクの洗い出し	・製品へのマルウェア混入 ・組織からの情報漏えい	互いに関係 ↔ ・計測データの改ざん ・制御機能への攻撃	互いに関係 ↔ ・ネットワーク上でのデータ改ざん ・偽称されたデータサービス
具体的な対策の提示（構成要素ごとに整理）	■納品されたモノの検証 ■マネジメントルールの徹底	■セキュリティバイデザイン ■セキュアなIoT機器等の導入 ■安全とセキュリティのためのシステム運用	■暗号化によるデータ保護 ■データ提供者の信頼性確認

フレームワークにおける信頼の確保の考え方

- サイバーフィジカルシステムのセキュリティを確保するため、それぞれの構成要素についての**セキュリティの確保(信頼の創出)とその確認(信頼の証明)を繰り返し行い、信頼のチェーンを構築、維持することで、価値創造過程全体のセキュリティを実現**。

１．信頼の創出

・セキュリティ要件を満たすモノ・データ等の生成
・対象のモノ・データ等が要件を満たした形で生成されたことの確認

２．信頼の証明

・対象のモノ・データ等が正常に生成されたものであることを確認できるリスト(トラストリスト)の作成と管理
・トラストリストを参照することで対象のモノ・データ等が信頼できるものであることの確認

３．信頼のチェーンの構築と維持

・信頼の創出と証明を繰り返すことで信頼のチェーンの構築(トレーサビリティの確保)
・信頼のチェーンに対する外部からの攻撃等の検知・防御
・攻撃に対するレジリエンスの強化

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パブコメ概要

- 平成30年4月27日～5月28日でパブリックコメントを実施。
- 海外からの関心が高く、英語版パブコメも実施。
- 国内23、海外10の組織・個人より、300以上の意見提出あり。肯定的な御意見が9割弱。

- **国内からの主な御意見**
  - Society5.0における信頼の確保へ向けた取組として、**フレームワークの趣旨に賛同**。
  - **既存の国際規格等があるので、対応関係を明確化**してほしい。
  - NIST SP800-171と比較して、**対策の強度は低いが準拠するためのコストが掛かる**ことを懸念。

- **海外からの主な御意見**
  - **フレームワーク案を広く支持**。サイバーセキュリティと経済活動を両立する上で効率的な、マルチステークホルダーアプローチやリスクベースアプローチに合致する多数の概念や対策が含まれている。
  - **国際規格であるIEC 62443 への言及が少ないように見える。**
  - **中小企業にとっても活用しやすいガイドラインを期待**。

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

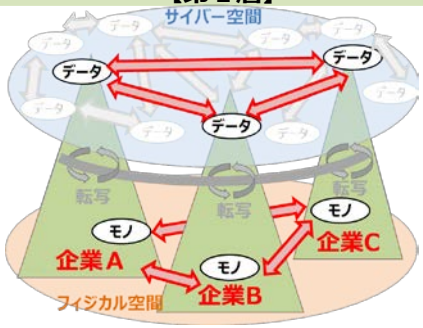
国際規格等との対応関係の整理

セキュリティ対策例のレベル分け

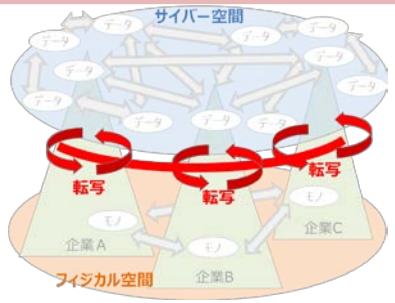
フレームワークの構成の新たな考え方

マネジメントモデル

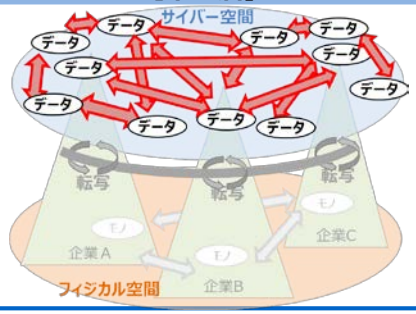
企業間のつながり（従来型サプライチェーン）【第１層】



フィジカル空間とサイバー空間のつながり【第２層】



サイバー空間におけるつながり【第３層】



三層構造でリスクを整理するための
リスクマネジメントモデル。

リスク・対応ポリシー

【L1.001】セキュリティポリシーの策定、体制の整備
- リスク：
  - 組織内で統一的なセキュリティ対策が取れない。
- 対応ポリシー：
  - セキュリティポリシーの策定と運用。

・・・

【L3.003】サイバー空間への不正ログイン対策
- リスク：
  - サイバー空間の情報(データ)への不正アクセス。
- 対応ポリシー：
  - 多要素認証の実装。

・・・

モデルに基いて、リスク・対応ポリシーを整理。
一般標準。分野により性能要求の形で規制になり得る粒度。

セキュリティ対策例

・・・

【L1.001】【L3.003】
関係者、特に特権を持つユーザーに対して、セキュリティ上の役割と責任を正しく理解させる。

・・・

【L3.003】
特権を持つユーザー等の認証に、適切な強度を有した認証方式を採用する。

・・・

各対応ポリシーに対処するための個別対策例。
リスク・対応ポリシーとの接続関係を示す。
個別認証はここを参照。

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

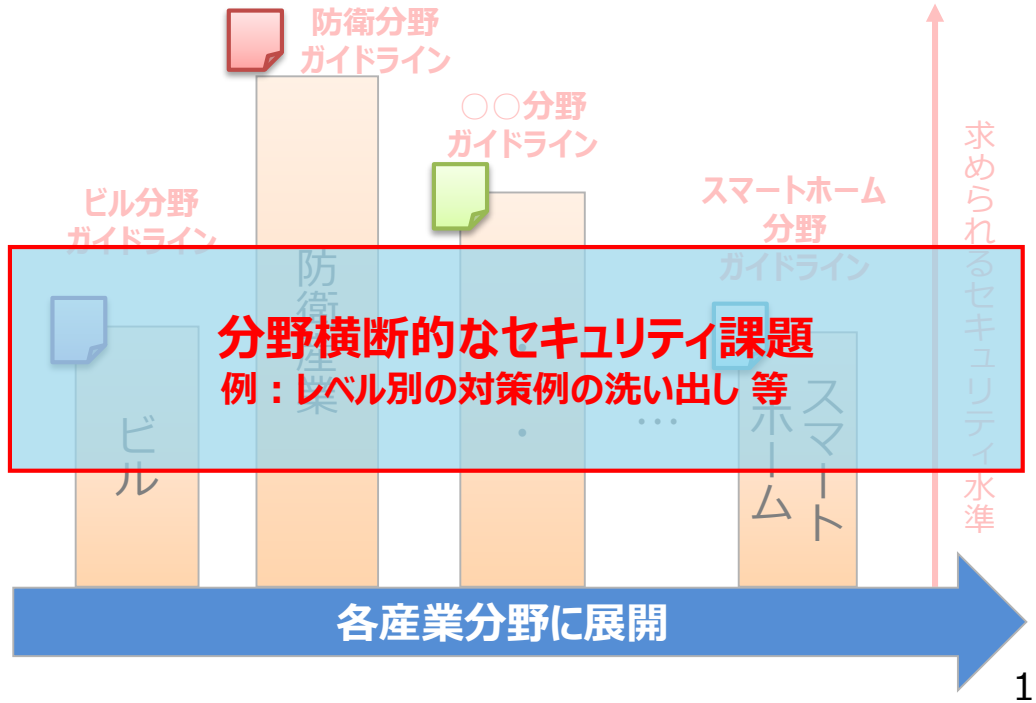
分野を横断して共通するセキュリティ課題への対応

- 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
	・・・

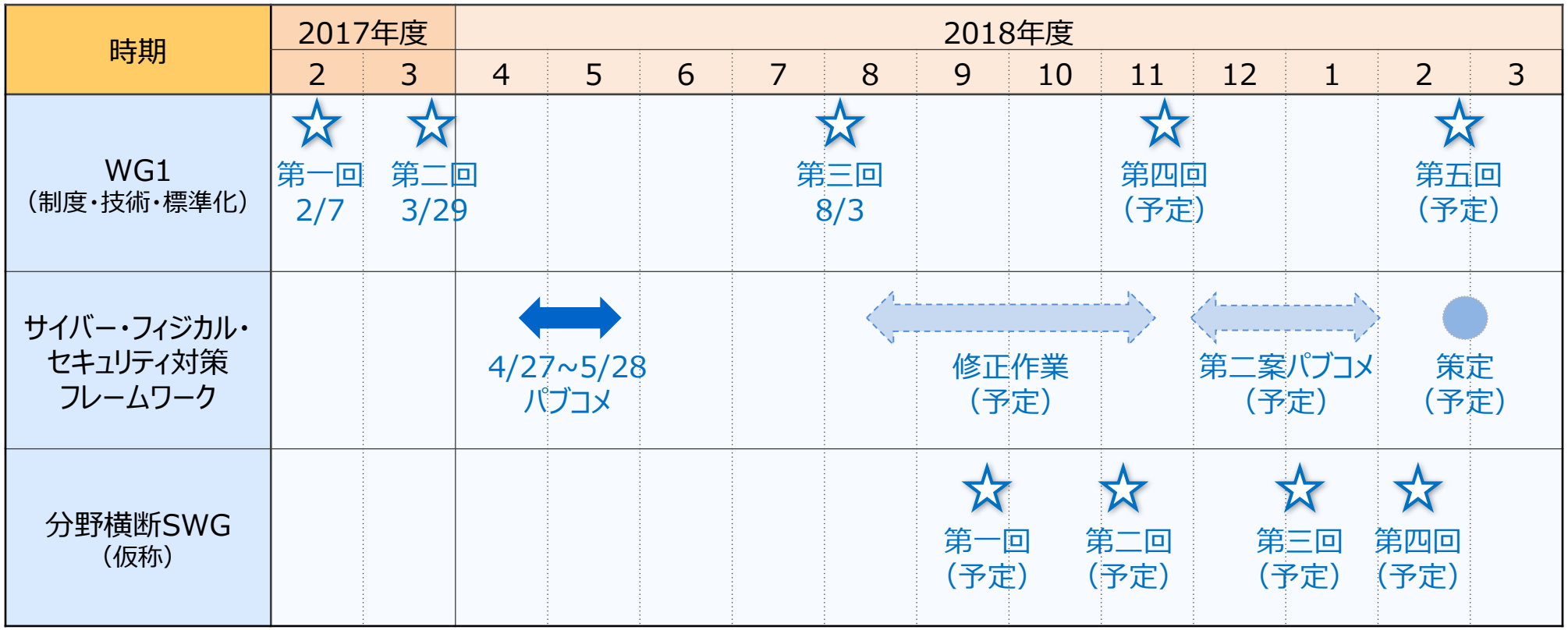
産業分野別のサイバー・フィジカル・セキュリティ対策



今後のスケジュール（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』（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



【参考】
各サブワーキンググループ等の設置・検討状況

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。

WG１　制度・技術・標準化

2/7 第1回会合, 3/29 第2回会合,
8/3 第3回会合開催

標準モデル

Industry by Industry で検討 (分野ごとに検討するためのSWGを設置)

ビル（エレベーター、エネルギー管理等）	**2/28 第1回会合, 4/16 第2回会合, 6/11 第3回会合, 7/12 第4回会合, 8/10 第5回会合開催**
電力	**6/12 第1回会合開催**
防衛産業	**3/29 第1回会合開催** **(防衛装備庁 第6回情報セキュリティ官民検討会)**
自動車産業	設置に向けて検討
スマートホーム	**3/13 第1回会合, 4/5 第2回会合, 6/13 第3回会合, 7/18 第4回会合開催** **(JEITA スマートホーム部会 スマートホームサイバーセキュリティWG)**
その他コネイン関係分野	

コラボレーション・プラットフォーム

Cross-Industry で検討 (分野を横断して共通する課題を検討するためのSWGを設置)

分野横断	設置に向けて準備中

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実装の方向性

- 『サイバー・フィジカル・セキュリティ対策フレームワーク』は、**対策の枠組み(チェックポイント)を示したものであり、セキュリティ水準(対策の強度)を示すものではない。**
- 産業分野ごとに守るべきものやリスクに違いも存在するため、**産業分野別にセキュリティ水準の検討を進めていく。**また、分野ごとの検討を進めた上で、**分野横断的課題を相互にフィードバックし、各産業分野に共通する対策を洗い出す等の取組を進めていく。**

『サイバー・フィジカル・セキュリティ対策フレームワーク』と分野別におけるセキュリティ対策のイメージ

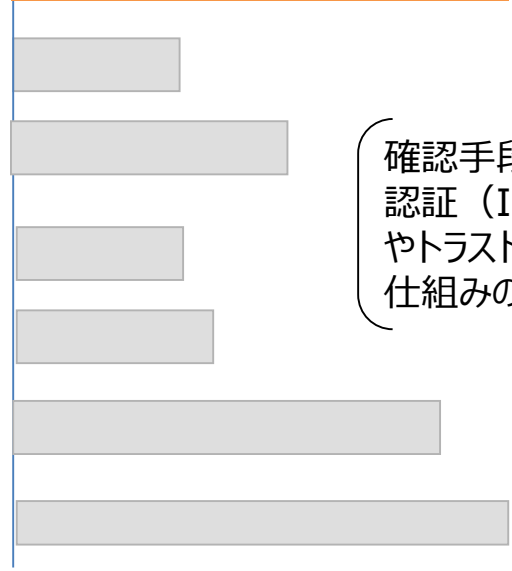
サイバー・フィジカル・セキュリティ対策フレームワーク

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
	・・

対策のポイントを踏えて産業分野ごとに検討

また、分野ごとの検討を踏まえて、分野横断的課題を相互にフィードバックしながら取り組みを推進

産業分野別セキュリティガイドライン



確認手段として、認証（ISMS、CC等）やトラストリスト等の仕組みの検討

ビルSWG（座長：江崎 浩 東京大学 教授）

- ビルの管理・制御システムに係る各種サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理し、ビルに関わるステークホルダーが活用できる**ガイドラインをとりまとめる。**
- オリパラに向けて、**各事業者において実施できる分野から実装**を目指す。

＜構成員＞

有識者、ビルオーナー、ゼネコン、サブコン、設計事務所、個別システム事業者（ビル管理、空調、エレベーター、ビデオ監視、電力・熱供給 等）、自治体、関係省庁 等

＜ガイドラインのとりまとめイメージ＞

- ビルシステム全体に**共通する最低限の要求**をまとめたもの＋**より詳細な方策**を示したものの二階建て構成
- ガイドラインでは、多くの事業者の取組の参考となるよう**優先順位を示した選択肢を提供**

内容項目例

・ビルに係わるサイバーセキュリティ上の脅威の現状
・ビルシステムに対して起こりえる攻撃とその影響の予測
・サイバーセキュリティ確保のための対策の概要
・対策の具体的内容
・対策実施に向けたチェックリスト

フェーズ	主な要求概要	関係するステークホルダー
設計	機器、ネットワーク、物理セキュリティへの要求	設計事務所、オーナー、ゼネコン、サブコン、ベンダー
施工／建築	機器単位、システム単位の施工プロセスへの要求	ゼネコン、サブコン、ベンダー
竣工検査	全体管理体制、管理結果、受入検査への要求	ベンダー、ゼネコン、サブコン、オーナー、設計事務所
運用・保守	管理体制への要求	オーナー、サブコン、ベンダー

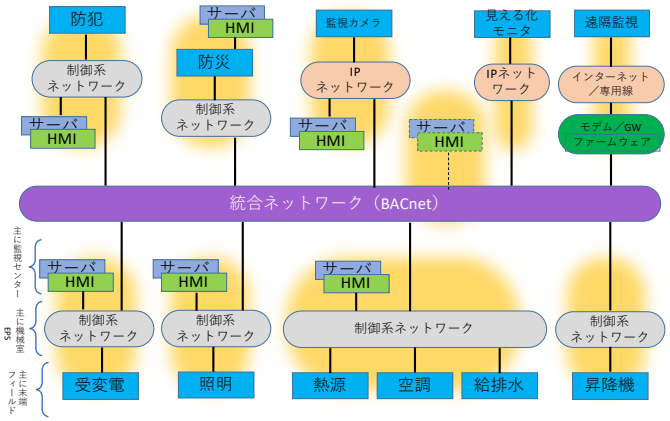
＜検討スケジュールイメージ＞

- **2018年夏：ガイドライン共通編・仮セット版（β版）を作成**
- 2018年度中：仮セット版を用いたモデル評価（2サンプル程度）とフィードバック、詳細検討を行い、ガイドライン共通編の完成
- 2019年度以降：ガイドライン共通編（完成版）の本格活用開始、個別編のモデル評価とフィードバック、完成

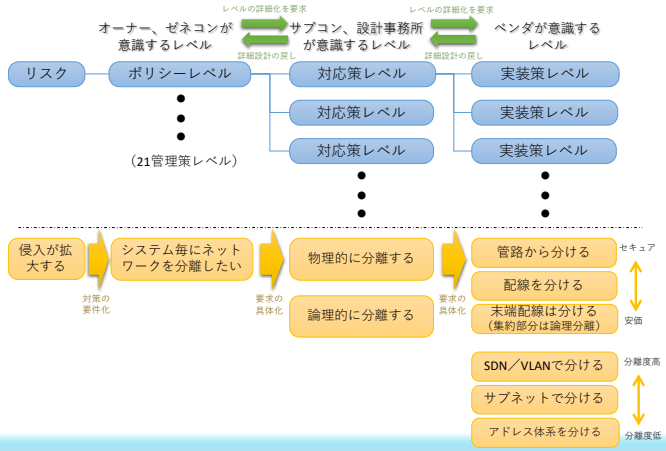
ビルSWG：最新の進捗状況

- 少人数の作業グループでガイドラインの叩き台作成に向けた作業を実施。
- 作業結果をもとにSWGにおいて議論を行い、**ガイドライン共通編・仮セット版（β版）を作成する。**

1．検討の前提として標準的なモデル構成を整理



2．対策の階層構造とステークホルダの関係を整理



3．ビルのライフサイクルを意識した対策の整理

4．ポリシーレベルでの対策の列挙

今後さらに．．．

- 各ライフサイクルのステージ毎の対策への展開
- ポリシーレベルから対応策レベルへの対策案の具体化

防衛産業SWG（防衛装備庁 情報セキュリティ官民検討会）

● 我が国の防衛調達におけるセキュリティ強化の方策について検討

我が国の防衛調達における情報セキュリティ強化の方策について、防衛装備庁と主要な防衛関連企業（２２社４団体）との間で「**防衛調達における情報セキュリティ強化に関する官民検討会**」を開催

＜検討の背景＞

１．我が国におけるサイバー攻撃の増大

・ 高度化するサイバー攻撃により、我が国のサプライチェーンが標的となる可能性。

２．米国の情報セキュリティ強化の動き

・ 米国の新標準（NIST SP800-171(※)）を満たすことが、今後の米国をはじめとする国際共同研究・開発への参加を継続する最低条件となる可能性。

（※）非政府機関がＣＵＩ（注）を扱う場合について、その機密性の確保のために推奨される14分野、110項目の具体的なセキュリティ要件を明らかにしたもの

（注）Controlled Unclassified Information　機密指定はされていないが管理が必要な情報

＜対応方針＞

契約企業が保護すべき情報を取り扱う際に適用される情報セキュリティ基準を、**米国の新標準と同程度まで強化した新情報セキュリティ基準を策定**する。

＜開催の状況＞

平成３０年３月までに計６回の検討会を開催。

第６回検討会より、経済産業省産業サイバーセキュリティ研究会と連携を図るため「**産業サイバーセキュリティ研究会WG1防衛産業SWG** 」として実施。

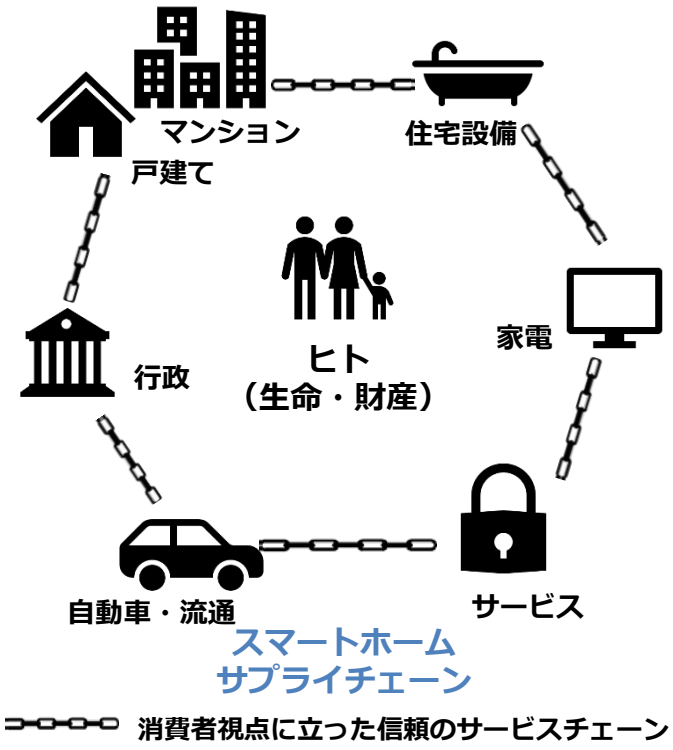
	開催日	検討テーマ
第１回	平成２９年　２月２８日	米国の防衛調達における情報セキュリティ強化の動向
		我が国の防衛調達における情報セキュリティ強化の方向
第２回	平成２９年　４月　５日	情報セキュリティ強化のためのルールのあり方
第３回	平成２９年　５月１９日	
第４回	平成２９年　６月１５日	中間的論点整理
第５回	平成２９年１１月２８日	これまでの振り返り及び現在の検討状況
第６回	平成３０年　３月２９日	新基準適合に向けた取り組み

スマートホームSWG（座長：小松崎 常夫 セコム株式会社 顧問）

- JEITA スマートホーム部会内にスマートホームサイバーセキュリティWGを新たに設置
- ハウスメーカ、システム・インテグレータ、機器メーカ等の住まいに関わる企業、業界団体が参加

＜構成員＞

企業）家電・AV関連、IT・通信関連、車載関連、住宅設備・サービス関連
団体・機関）住宅・住宅設備分野、電機・通信分野、医療分野、研究機関
スマートホーム部会長の丹 康雄教授（北陸先端大）も委員として参画



＜検討項目＞

Step1 “スマートホーム産業”に求められるセキュリティ対策像を整理し、**住宅・住設・家電・サービス等のスマートホームサプライチェーンで活用できる「サイバー・フィジカル・セキュリティ対策フレームワーク」**を策定する。

Step2 「サイバー・フィジカル・セキュリティ対策フレームワーク」を概念としてだけではなく、各事業者が実際のセキュリティ対策オペレーションレベルで活用できるよう、実効的な施策について検討を行い、必要に応じて、政府への政策提言を行う。

Step3 実運用に向けて、消費者へのリスク周知や免責事項、モニタリングの在り方、事業者間の信頼の創出方法等について検討。さらには、スマートホームからスマートライフ分野（街・社会インフラ）に対応したセキュリティ対策についても検討を進めていく。