

サブワーキンググループ、タスクフォース等 の検討状況

令和3年3月

経済産業省 商務情報政策局

サイバーセキュリティ課

分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化とテーマ別TFにおける検討

- 6つの産業分野別サブワーキンググループ(SWG)を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、3つのタスクフォース（TF）を設置

産業サイバーセキュリティ研究会WG 1（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(2019.6)

電力SWG

- ・ 小売電気事業者ガイドライン策定(2021.2)

防衛産業SWG

自動車産業SWG

- ・ ガイドライン1.0版を公表(2020.12)

スマートホームSWG

- ・ ガイドライン案パブコメを実施(2020.7-8)

宇宙産業SWG

- ・ 2021年1月に第1回を開催

...

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、SBOM活用促進に向けた実証事業（PoC）を検討

『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)」を公開

1. 産業分野別SWG

2. 第3層タスクフォース

3. ソフトウェアタスクフォース

4. 第2層タスクフォース

5. CPSFの国際規格化

産業分野別SWGの検討状況

- 各産業分野別SWGにおいて、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）を参考にしつつ、各産業分野の特性に応じたセキュリティ対策の検討が進んでいる。

WG 1 制度・技術・標準化

2018/2/7 第1回会合開催
2021/3/15 第8回会合開催

標準モデル

Industry by Industryで検討

ビル

2018/2/28 第 1回会合開催
2020/2/13 第10回会合開催

電力

2018/6/12 第 1回会合開催
2021/2/15 第11回会合開催

防衛産業

(防衛装備庁 情報セキュリティ官民検討会)

2018/3/29 第 1回会合開催
2019/8/26 第 4回会合開催

自動車産業

2019/3/29 第 1回会合開催
2021/3/5 第23回会合開催

スマートホーム

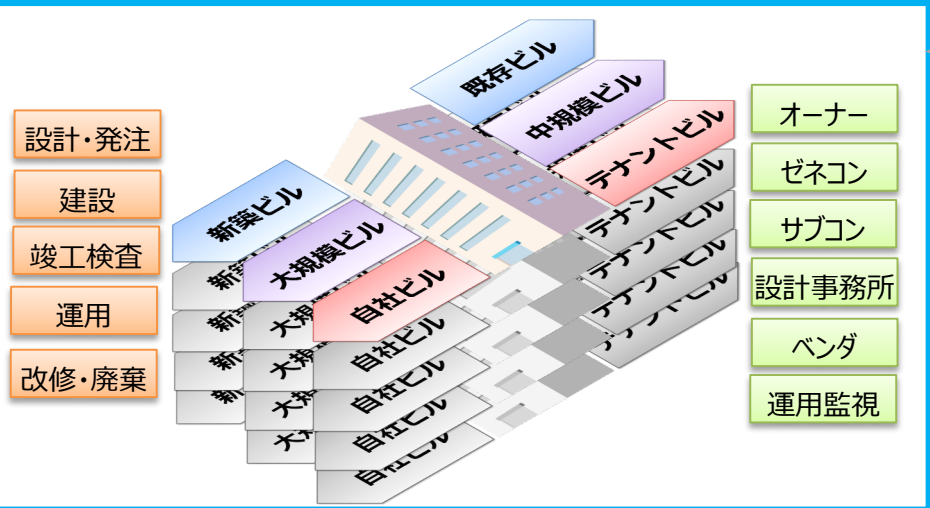
2018/3/13 第 1回会合開催
2021/3/8 第21回会合開催

宇宙産業

2021/1/15 第 1回会合開催
2021/3/3 第 2回会合開催

ビルSWG（座長：江崎 浩 東京大学 教授）

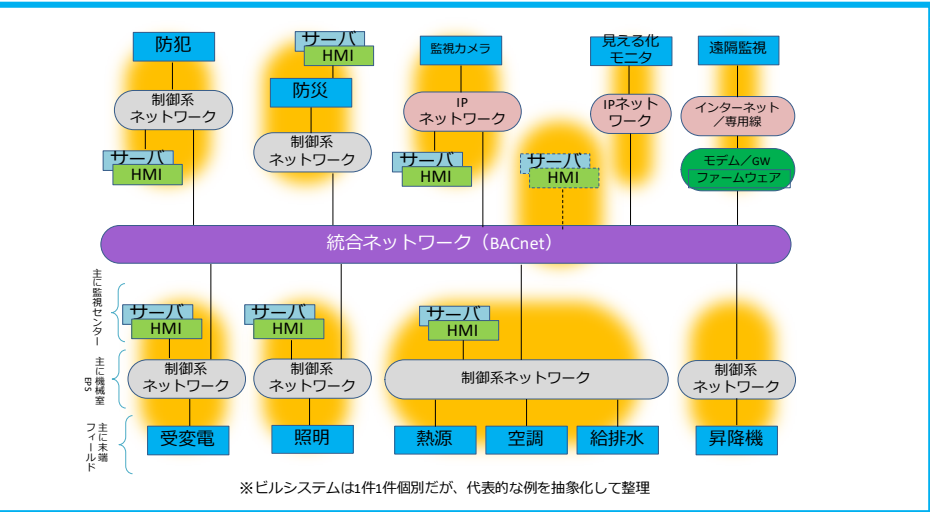
- ビルの管理・制御を行うビルシステムに係る各種サイバー攻撃のリスクと、それに対するサイバーセキュリティ対策を整理し、2019年6月17日付でガイドライン第1版を公開。
- 記述充実化と個別編(空調編)作成を実施中。関係者間の情報共有の在り方についても検討中。



ビルシステムは、様々な種類のビルに、多種多数のステークホルダが関与し、多種の設備システムが稼働し、複数ステージからなる長期間のライフサイクルを持つ、という特徴を持つ。

モデル的なビルシステムを設定。

ビルシステムの置かれる場所、個々の機器等に応じたリスクに対し、ライフサイクルを意識した対策を整理。



※ビルシステムは1件1件個別だが、代表的な例を抽象化して整理

場所	機器	リスク	ライフサイクル別対策要件				
			設計時	構築時	竣工時	運用時	長期運用 (改修時)
ネットワーク		リスク					
監視センター	HMI						
機械室	サーバ (BA装置)						
EPS							
末端の設置場所							
その他							

5つのライフサイクルに渡って、対策が引き継がれていく形で整理

電力SWG（座長：渡辺 研司 名古屋工業大学大学院 教授）

- 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、**官民が取り組むべき課題と方向性**について、**短期・中長期という時間軸を加味**しつつ、広く検討。
- CPSFも踏まえ、さらに取組が加速している諸外国の動きも視野に、電力分野における様々なセキュリティの課題への対応を強化していく。

<構成員>

有識者（大学教授、弁護士等）、電気事業者、業界団体

<検討項目>

- **大手電気事業者**のサイバーセキュリティ対策について
 - 大手電気事業者におけるサイバーセキュリティの対策状況に係る実態把握について、**国内外のフレームワークを踏まえた共通枠組みによるアセスメントの実施**
 - 2020年東京オリンピック・パラリンピック**に向けた対応策を継続検討
- **新規プレーヤー**のサイバーセキュリティ対策について
 - 小売電気事業者**の取り組むべきサイバーセキュリティ対策を取りまとめた**ガイドラインの策定**
 - 太陽光や風力等の小規模発電事業者等**への**実態調査**を実施
 - グリッドコード**において、**太陽光等の発電設備の系統への接続に係るサイバーセキュリティ要件を導入**
- **サプライチェーンリスクへの対応**について
 - 国際的な検討枠組みへの参加及び最新動向も踏まえた**サプライチェーンリスクへの対応**の継続検討

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（23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。

＜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＞

	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
第7回	平成30年 9月 5日	防衛調達におけるサイバーセキュリティの強化に向けて
第8回	平成31年 2月28日	サイバー攻撃に関する留意事項、米国企業のNIST SP800-171対応状況
第9回	令和 元年 8月26日	新情報セキュリティ基準（案）

自動車産業SWG（一般社団法人 日本自動車工業会 総合政策委員会）

- 日本の自動車業界として対象のセキュリティフレームワーク・ガイドライン・実現レベルを定め、活用を推進することで、適切なセキュリティ対策の実施を図る。
- 2020年12月、エンタープライズ領域（会社全体のベースとなるOA環境）において業界全企業が実施すべき事項を規定した「自工会／部工会サイバーセキュリティガイドライン1.0版」を公開。

＜メンバー構成＞

日本国内の乗用車、二輪車、商用車生産の14社

＜開催状況＞

- ・ 2019年4月16日 第1回 電子情報委員会／サイバーセキュリティ部会を開催。
- ・ 2020年12月4日 第1回 総合政策委員会／ICT部会／サイバーセキュリティ分科会を開催。
（自工会の組織体制変更に伴い名称変更）

＜2020年度進捗＞

- ・ 2020年5月、部工会と共同で、国内外のフレームワークやガイドライン、国際標準規定をベースとした「自工会／部工会サイバーセキュリティガイドライン0.9版」を作成し公開。
公開後、0.9版のチェックシートを用いたトライアルを業界内各社で実施。
- ・ 2020年12月、0.9版によるトライアルの結果を踏まえて内容を充実させ、「自工会／部工会サイバーセキュリティガイドライン1.0版」を公開。2021年には英語版も公開予定。
- ・ 今後、ガイドライン対応状況の集約・分析、レベルアップに向けたガイドラインの項目拡充、工場セキュリティに関する課題対応、脆弱性/脅威情報に関する各社の情報共有等について検討を深める。

スマートホームSWG (JEITA スマートホーム サイバーセキュリティWG)

- スマートホームにおける安全で安心な生活の実現のため、スマートホームの提供事業者から住まい手まで、幅広いステークホルダに求められる最低限のセキュリティ対策をまとめたガイドラインを取りまとめた。

◆ガイドラインの対象

- スマートホーム向けIoT機器、スマートホーム向けサービス、スマートホーム（住宅）の開発・生産・販売・供給・サポート等を行う事業者
- スマートホーム化された区分所有型集合住宅および賃貸型集合住宅の管理者
- スマートホームの住まい手

<メンバー構成>

企業）家電・AV関連、IT・通信関連、住宅設備・サービス関連

団体・機関）住宅（戸建て／マンション）・住宅設備分野、電機・通信分野、医療関係、健康関連分野、研究機関

<開催状況>

2018年3月より、JEITA スマートホーム サイバーセキュリティWGとして開催。

<2020年度進捗>

- ・ 2019年度に作成したガイドライン案について、2020年7月末から8月にパブコメを実施。
- ・ パブコメで提出された意見も踏まえて修正を行い、2021年3月、「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」第一版として取りまとめた。

スマートホームガイドラインの策定

- 2018年3月からスマートホームSWGにおいて議論。2019年度にとりまとめたガイドライン原案について、2020年7月末から8月にかけてパブコメを実施。提出された意見等を踏まえて修正を行い、「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」として取りまとめた。本WG1での議論を経て、ver1.0として公開したい。
- スマートホームにおけるステークホルダーは多様であり、セキュリティに関する知識・バックグラウンドも様々であるため、必要なセキュリティ対策を階層的に示している。
- なお、策定後は、ガイドラインの管理をSWGの事務局を務めたJEITAに移管し、業界の実態を踏まえて改訂版を作成・公開・周知いただくこととしてはどうか。

1. はじめに

- 1.1. ガイドラインを策定する目的
- 1.2. ガイドラインの対象者
- 1.3. 対象とするスマートホーム（戸建、共同）
- 1.4. ガイドライン作成の背景
- 1.5. サイバー・フィジカル・セキュリティ・対策フレームワークとの関係

2. セキュリティ対策の検討の考え方

- 2.1. 各ステークホルダーに対するセキュリティ対策を導出する流れ
- 2.2. 脆弱性の要素
- 2.3. 想定されるインシデントと脅威から脆弱性を抽出する観点

3. スマートホームにおけるセキュリティ上の脅威

- 3.1. データと脅威
- 3.2. 物理手的なモノを含めた管理上の脅威

4. スマートホームに求められる最低限のセキュリティ対策

- 4.1. (1)スマートホーム向けIoT機器の事業者

- 4.2. (2)スマートホーム向けのIoT機器を遠隔から管理する事業者、
- (5)スマートホーム向けにメンテナンスやサポートを行う事業者
- 4.3. (3)スマートホーム向けのサービス事業者
- 4.4. (4)スマートホームを供給する事業者
- 4.5 (6)スマートホーム化された分譲共同住宅・団地や管理受託会、
- (7)スマートホーム化された賃貸住宅の所有者や管理受託会社
- 4.6 (8)スマートホームの住まい手

5. おわりに

添付

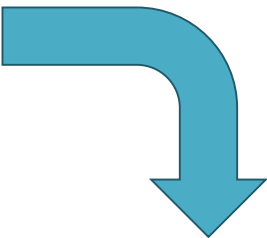
- 添付 A ステークホルダーにおける機能／想定されるインシデント／リスク源／対策要件
- 添付 B 対策の整理と、国際規格などの各種規格との対応
- 添付 C ステークホルダーに向けたガイドと対策要件の対応関係
- 添付 D サイバー攻撃と脆弱性の事例
- 添付 E 用語集
- 添付 F 参考文献

スマートホームガイドラインのポイント

- 知識やバックグラウンドが様々なステークホルダーに対応するため、シンプルな対策ガイド（4章）から、具体的な対策要件や他の標準との対比（添付）まで、セキュリティ対策を階層的に整理。

<4章 スマートホームに求められる最低限のセキュリティ対策> ※抜粋

- 4.1.(1)スマートホーム向けIoT機器の事業者
- ・ IoT機器は出荷時や初期状態からセキュリティを確保する
 - ・ セーフティを考慮する
 - ・ ソフトウェアをアップデートするための仕組みを提供する
 - ・ 利用者にIoT機器の使い方や使用環境をガイドする、セキュアに利用するための情報を提供する



誰でも読みやすいように本編はシンプルな対策ガイドに抑え、より詳細な検討が必要な者が参照できるよう添付において詳述することで、セキュリティ対策を階層的に整理。

<添付A ステークホルダーにおける機能／想定されるインシデント／リスク源／対策要件> ※抜粋

機能	想定されるインシデント	リスク源			対策要件ID	対策要件の例
		脅威	脆弱性ID	脆弱性		
下記の機能 ・フィジカル空間の物理事象を読み取り、デジタル情報へ変換し、サイバー空間へ送る機能 ・サイバー空間での処理の結果により、IoT機器を制御する等のためにサイバー空間から受ける機能 ・外部からの管理機能	事前に想定されていない動作をする （IoT機器およびIoT機器を含むシステムにより提供されるサービスや機器の種類により、想定されていない動作は異なり、情報漏洩や不正な制御といった、人体・健康・住宅・防犯・環境・利便性・エネルギーメーターなどに影響するものがある）	・ソフトウェアの脆弱性やハードウェアの脆弱性を悪用してIoT機器内部に不正アクセスされる	MV.1	・利用されないネットワークポートやサービスなどが利用可能な状態のままとなっている	MO.1	・IoT機器およびIoT機器を含むシステムでの不要なネットワークポート、その他USBやシリアルポートなどを物理的または論理的に閉塞すること。 ・IoT機器およびIoT機器を含むシステムが提供する機能、サービス、アプリケーション、アカウントについては必要に応じて停止、変更、削除が可能なようにすること。

<添付B> : 対策要件IDと国際規格との対応、 <添付C> : 4章と添付Aの対応

宇宙産業SWG の設立について

- 宇宙分野における民間事業者の役割拡大や、米国等における官民の取組を踏まえ、我が国でも、2021年1月に産学の有識者を委員に、宇宙産業SWGを設立。

＜背景＞

- 宇宙分野における民間事業者の役割拡大
- 国内外で宇宙分野のセキュリティインシデントが多発
 - 1986-2020年に国内外で90件以上
- 米国等において宇宙分野のセキュリティ対策を促進するための官民の取組が活発化
 - 国家安全保障システム委員会（CNSS）によるCNSSP12『安全保障任務に用いられる宇宙システムのための国家情報保証方針』（07年3月発行。18年2月最終改訂）
 - 民主導による『商用宇宙システムセキュリティガイドライン』発行（20年5月）

＜委員一覧＞

鹿志村 修	宇宙システム開発利用推進機構(JSS) 研究開発本部長
片岡 晴彦	(株)IHI 顧問（元防衛省航空幕僚長）
木下 仁	IPAセキュリティセンター主任研究員
栞原 聡文	東北大学大学院工学研究科 航空宇宙工学専攻 宇宙ロボット研究室 准教授
小山 浩	三菱電機(株) 電子システム事業本部 主席技監
坂下 哲也(座長)	JIPDEC 常務理事
佐々木 弘志	マカフィー(株) シニア・セキュリティ・ アドバイザー
名和 利男	(株)サイバーディフェンス研究所 専務理事・上級分析官
丸山 満彦	PwCコンサルティング パートナー
満永 拓邦	東洋大学 情報連携学部 准教授
吉松 健三	CSSC

宇宙産業SWG（座長：坂下 哲也 JIPDEC 常務理事）

- 民間事業者向けの宇宙システムに係るサイバーセキュリティ対策のガイドラインを令和3年度中を目標に開発予定。

<メンバー構成>

宇宙産業事業者、宇宙関係の業界団体・NPO、有識者（大学、産業サイバーセキュリティ専門家等）

<開催状況>

2021年1月に第1回、3月に第2回を開催。

<目標・検討内容>

- ・ 民間事業者向けの宇宙システムに係るサイバーセキュリティ対策のガイドラインを令和3年度中を目標に開発予定。開発するガイドラインは自主的な対策を促すためのものとする。（ただし、規制官庁が当該ガイドラインを参照することは妨げない。）
- ・ 宇宙産業SWGの下に実務者からなる作業部会を設置。作業部会には30以上の組織が参加。第一回を2021年2月に開催。
- ・ 本SWG及び作業部会には、宇宙分野の専門家、産業サイバーセキュリティの専門家の双方が参加し、お互いの専門領域について理解を深めることを通じ、「宇宙×サイバー」のコミュニティへと発展させることを目指す。

1. 産業分野別SWG

2. 第3層タスクフォース

3. ソフトウェアタスクフォース

4. 第2層タスクフォース

5. CPSFの国際規格化

第3層タスクフォースの検討の方向性

● タスクフォースの目標

- 主体間を転々流通するデータのセキュリティ対策を検討するにあたり、
ステークホルダー間の議論に際し、リスクを適切に把握することに資する枠組みの提供
- 組織を越えてデータを活用するバリュークリエイションプロセス（価値創造過程）において、本枠組みを用いてデータの流通プロトコルや連携APIの在り方を明確にすることで
データの囲い込みを回避（アンバンドル化）し、多様な価値創造を促進。

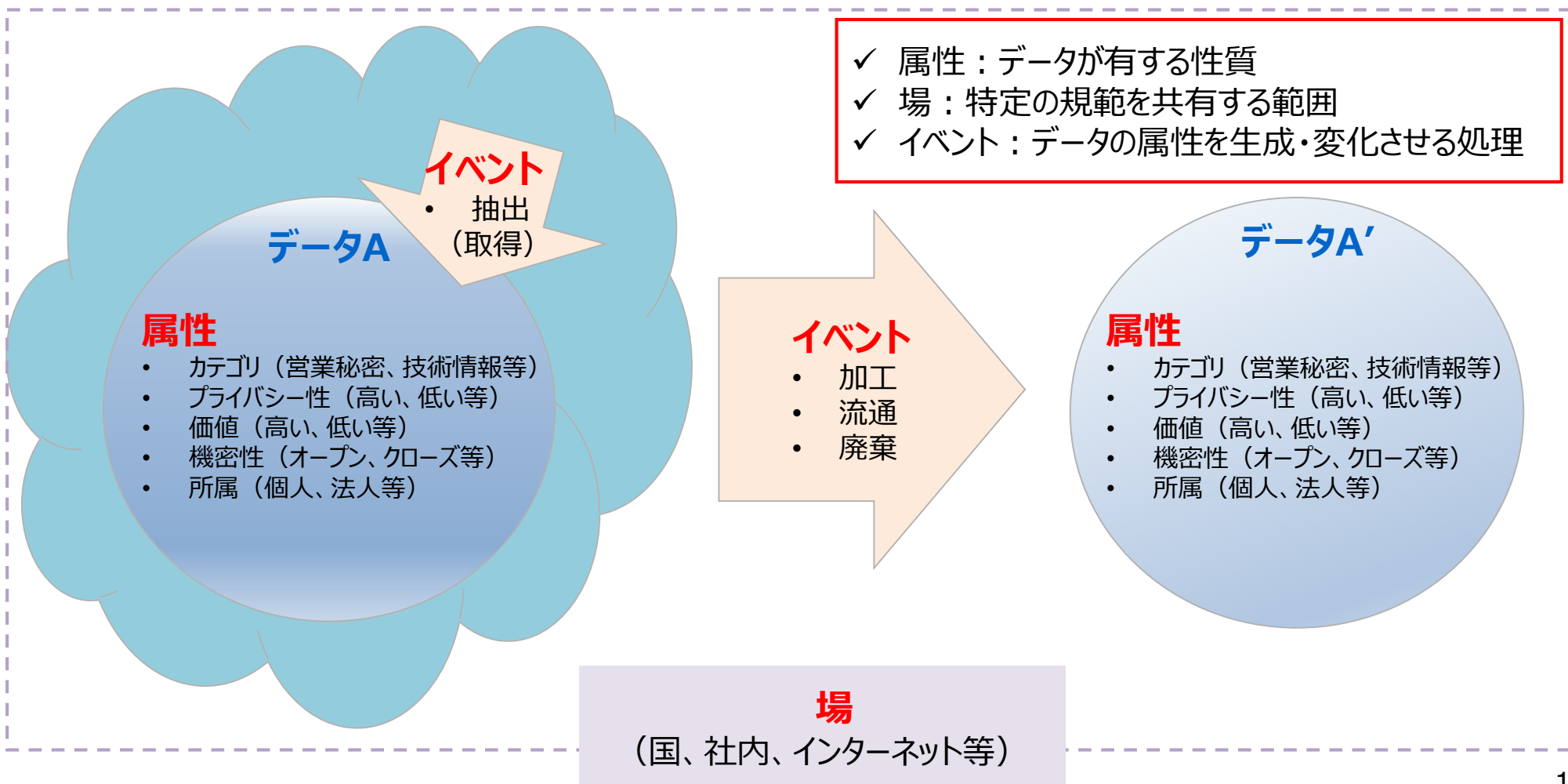
● データマネジメントの捉え方：

「データの属性が場におけるイベントにより変化する過程をライフサイクル全体にわたって管理すること」という定義を提案

➡ こうしたプロセスにて、「検証可能な方法でステークホルダーの期待を満たす」
のが「信頼性」を確保すること

データマネジメントの新たな捉え方

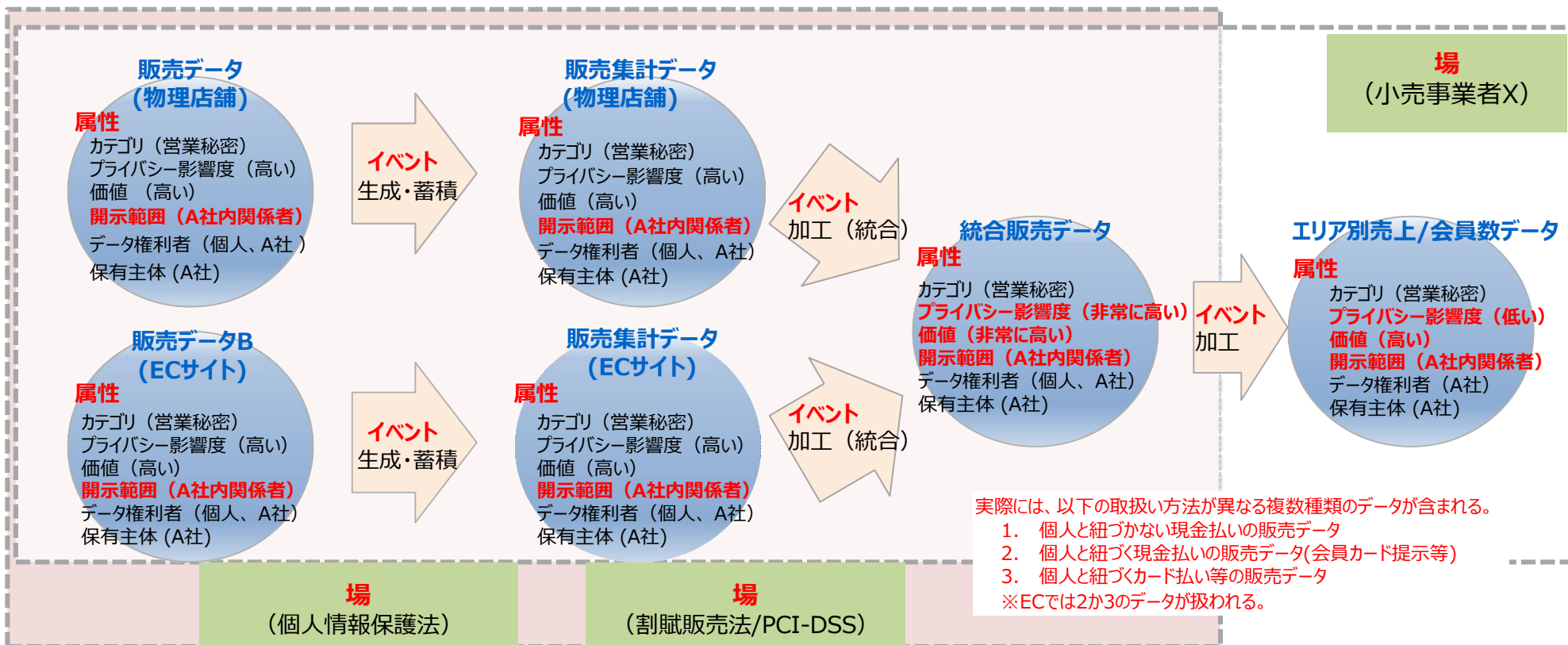
- 既存のデータマネジメント等の考え方を参考にしつつ、第1回タスクフォースの議論を踏まえ、データマネジメントとは、「データの 属性 が 場 における イベント により変化する過程を ライフサイクルを踏まえて管理すること」とここでは捉える。



データマネジメントの新たな捉え方の拡張（イメージ）

- 第3回TF（2021年3月開催）において、データマネジメントの新たな捉え方を、主体間を転々流通するデータのセキュリティ対策の検討に適合する形に拡張することとした。
- 様々な主体の間を転々と流通して付加価値を高めていくデータフローを可視化し、ステークホルダー間でリスクベースのデータマネジメントの在り方を合意することの重要性について合意。

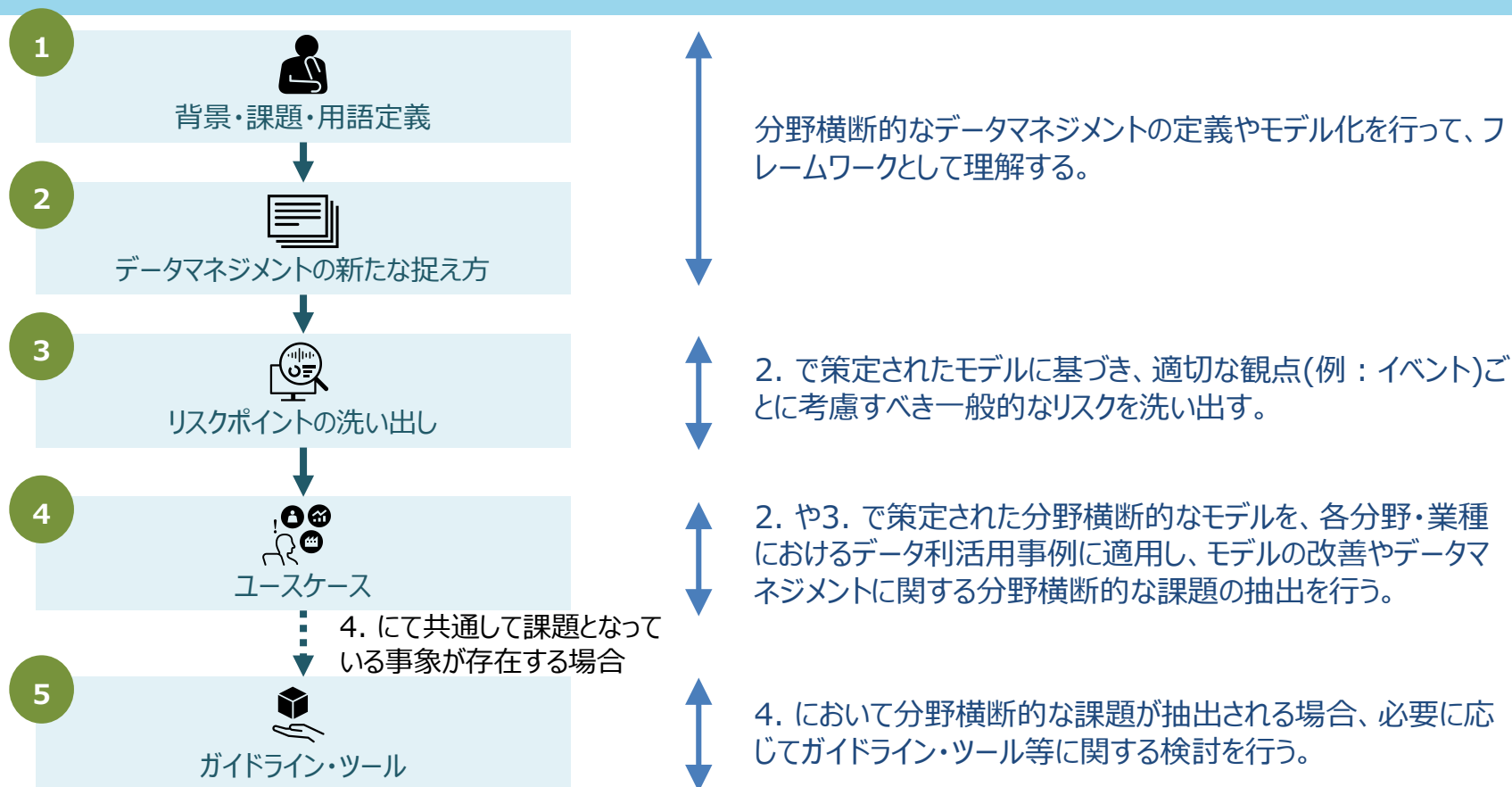
小売業におけるPOSデータの活用事例



それぞれの状態のデータにおいて、データ権利者や属性の変化に留意しつつ、
どのようなセキュリティ対策を講じるべきかについて、ステークホルダー間で合意することが重要なのではないかと。

第3層タスクフォースのアウトプットイメージ

- 第三層TFの目標を、主体間を転々流通するデータのセキュリティ対策を検討するにあたり、ステークホルダー間の議論に際し、リスクを適切に把握することに資する枠組みの提供と設定。
- データマネジメントの新たな捉え方をまとめ、それに基づきリスクポイントの洗い出し、具体的なユースケースの検討を行った後、分野横断的な課題が抽出された場合にガイドラインやツール等を検討する。



「リスクポイントの洗い出し」のプロセスの整理

- 主体間を転々流通するデータに関するデータマネジメントは、下記の4ステップで「新たな捉え方」に当てはめることで、リスクポイントの洗い出しを実施することが可能となる。
- イベントごとにリスクを洗い出す際は、いくつかの観点（CIA等）を示し、それぞれに懸念事項を列挙する方法が考えられるのではないかな。

「新たな捉え方」への当てはめのステップ

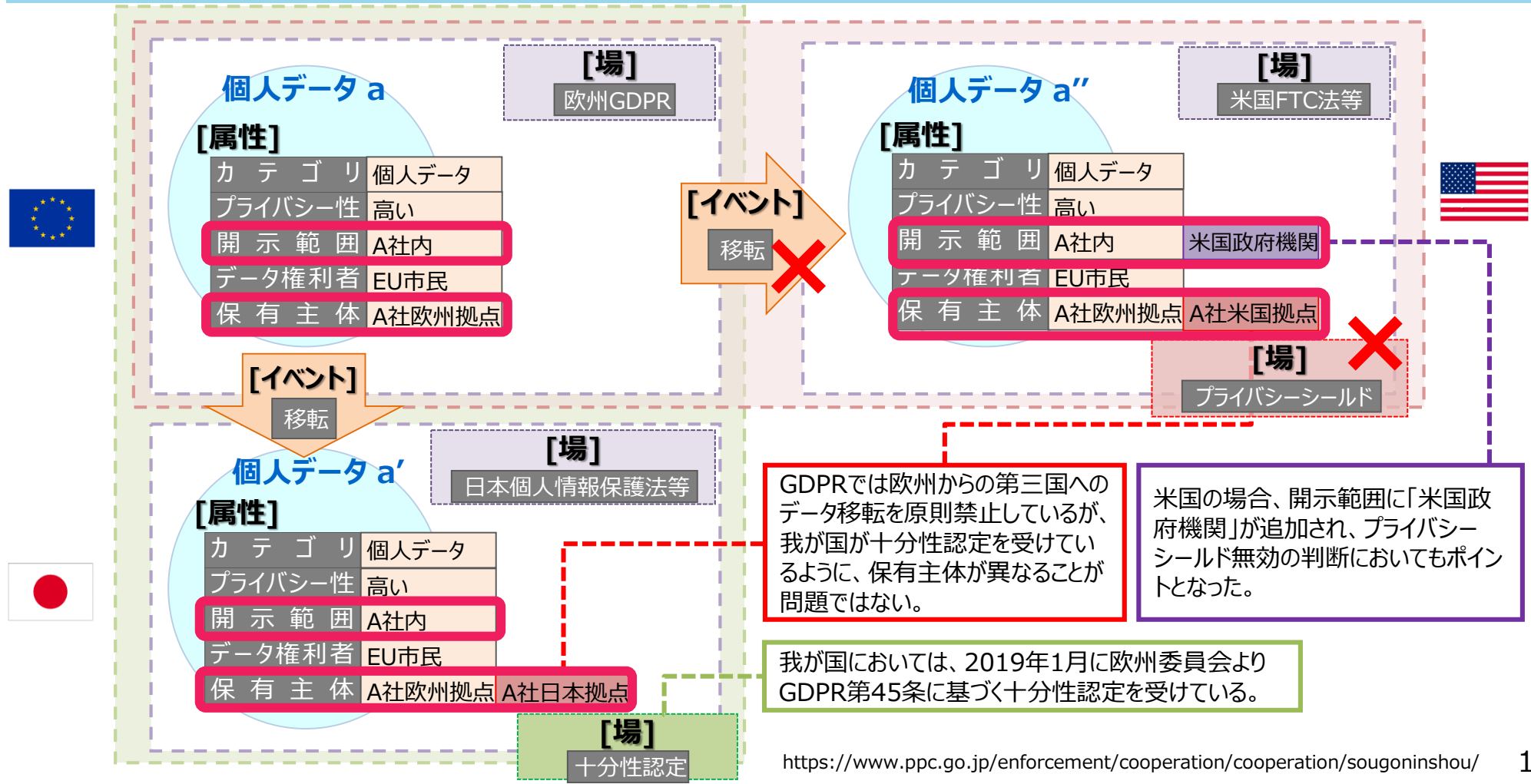


イベントごとのリスクの洗い出しの枠組み（イメージ）

対象イベント	観点及び想定される懸念事項(例)
 生成・取得	機密性 生成・取得過程でデータが漏えいする。
	完全性 データが生成・取得過程で不正に改ざんされる。
	可用性 システムの障害等によりデータの生成・取得が停止する。

第3層TFで議論しているモデルの活用 ～各国等のルール間のギャップ把握～

- データの取扱いに関する各国・地域のルールに対し、データマネジメントのフレームを当てはめることで、各国・地域のルール間のギャップ（凸凹）を把握しリスクポイントを可視化することが可能に。
- GDPRに関するSchrems II 判決の事例では、欧州からの個人データの移転に関し、プライバシーシールドが無効と判断された米国と、十分性認定を受けている我が国の制度の違いを可視化可能。



1. 産業分野別SWG

2. 第3層タスクフォース

3. ソフトウェアタスクフォース

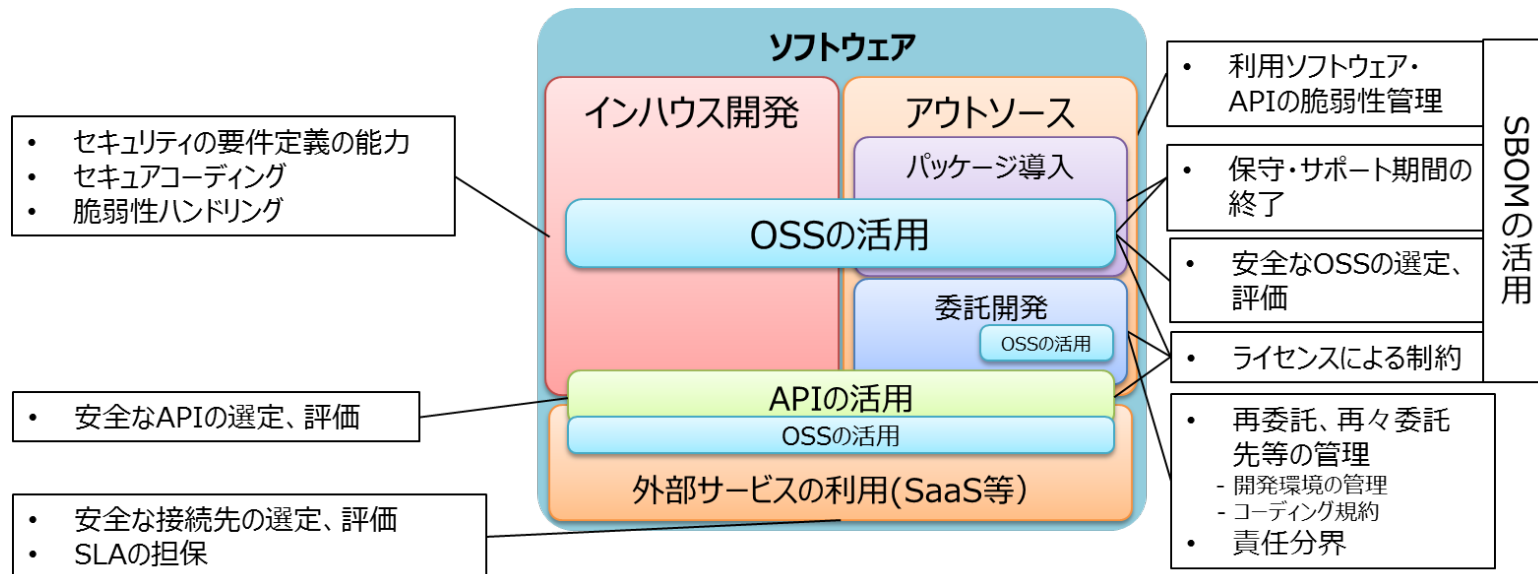
4. 第2層タスクフォース

5. CPSFの国際規格化

ソフトウェアタスクフォースの検討の方向性

- 仮想化技術の進展などにより、OSSを含むソフトウェア技術への依存が高まる中で、ソフトウェアの管理手法、脆弱性対応やライセンス対応等の重要性が増している。
- 2018年、米国NTIA（電気通信情報局）は、「Software Component Transparency」を設立し、ソフト部品構成表であるSBOM（Software Bill of Material）の活用に関する議論を推進。
- ソフトウェアタスクフォースでは、適切なソフトウェア（特にOSS）の管理手法、脆弱性対応やライセンス対応等を検討。

ソフトウェアを利用する際に考慮すべき観点



OSS管理手法に関する事例集の作成

- 3回のタスクフォースでの議論を経て「**OSSの利活用及びセキュリティ確保に向けた管理手法**」の事例集作成に着手。**参考となる事例を共有し、企業における適切なOSS利用を促進**する。
- 担当者が自社のOSS管理等を検討する際の参考資料や、経営層への説明時の補足資料等として活用されることを想定。

章	タイトル	作成方針（案）
1	目的	• 本書を作成する目的を、これまでのTFにおける資料・議論を基に取りまとめる。 ✓ OSS利活用に関する課題の観点を整理し、その観点ごとに各種事例をとりまとめて公開することにより、「OSS利活用及びセキュリティ確保に向けた管理手法」の参考情報を提供する。 ✓ 事例を自社の取組みの参考にしてもらうことで、<u>OSSの留意点（ライセンス遵守、脆弱性対応等）を考慮した適切なOSS利用を促進</u>する。 ✓ また、<u>企業のOSS利用の障壁を取り除くことで更なるOSS利用を促し、OSSのメリットを享受し競争力向上につながることを期待</u>。 • 事例集が、OSS管理等検討時の参考資料、経営層への説明の補足資料等として活用されることを想定。
2	OSSの概要	• 読者の理解を助けるために、OSSの基礎的な情報を取りまとめる。 ✓ 「OSSとは何か」「OSS利活用の長所・短所（リスク）」「OSSライセンスの概要」「OSSコミュニティ活動の利点」「OSSに関する課題」「インシデント事例」等。 • 併せて政府・関係機関のこれまでの取り組みも紹介する。
3	整理方法	• 事例を紹介するにあたり、読者の理解を助けるために、本書で取り上げる事例の分類・整理を示す。 • 各事例の種類を一覧で示す。
4	事例	• 各社の事例を順次記載する。

事例集の作成状況

- 昨年度から今年度にかけて、本TF委員からの推薦や公開情報の調査等を踏まえ、OSSの管理手法等で参考になる取組を実施している企業に対しヒアリングを実施。
- ITベンダ／サービス、金融、自動車／電機メーカー等の業種から10社以上にヒアリング。

OSS利活用における留意事項の観点

プロセス別観点	選定評価・ライセンス ✓ 安全なOSS選定が困難 ✓ 協力会社にOSS選定を一任してよいか判断がつかない ✓ 機能（品質）と安全性、信頼性のバランス ✓ 改変によるライセンス違反 ✓ OSSライセンスを評価できていない	脆弱性管理 ✓ ソフトウェア管理の粒度のばらつき ✓ 製品構成（部品やOSS等）や、脆弱性の把握が困難 ✓ 費用対効果（労力、コスト） ✓ 脆弱性告知、適用手段、サポートが不適切 ✓ レガシーな機器やシステム、IoT機器	保守・品質保証 ✓ サポート終了したOSSの放置 ✓ 運用、保守計画が立てづらい ✓ ロングタームサポートの必要性 ✓ 障害時等の賠償、免責の設定 ✓ 廃棄、利用終了時の対応
	サプライチェーン管理 ✓ 網羅的な調整が困難 ✓ OSS前提ではない取引慣行 ✓ SBOMの活用が進んでいない ✓ 全てのサプライチェーン内のOSS管理及び脆弱性体制の確保 ✓ 契約による明文化の必要性 ✓ 企業ごとの対応能力のばらつき		
人・組織に関する観点	個の能力・教育 ✓ 経営者のリスク管理不足 ✓ 判断基準、対応基準が未整備 ✓ リテラシー不足・知識不足 ✓ 人依存・コミュニティ依存の対応		
	組織体制 ✓ OSS利活用をサポートする社内体制がない ✓ 脆弱性発生時の対応が不安定 ✓ 多くのメーカーでPSIRTが立ち上がっていない		
コミュニティに関する観点	✓ コミュニティの評価 ✓ 活動の社内認知、理解の醸成 ✓ 活性化、発言力UP（海外含む）		

国内でのSBOMの活用促進に向けて（実証事業（PoC）の実施）

- 米国NTIAが主導するSoftware Component Transparencyでは、ヘルスケア分野におけるPoC等を通じて、ベストプラクティス等を記した成果物が作成・公表されつつある。
- 他方、ソフトウェア分野における業界構造や商習慣が異なる日本においては、総論としてSBOMの有用性は理解されているものの、実際の活用促進に向けては、導入コストをはじめとして様々なハードルがある。
- 第4回TF（2021年1月）において、適切なSBOMの活用を推進するために、実証事業の実施および検証事項等について議論いただいた。

NTIAが公開したドラフト文書の概要（10月22日時点）

Requirements for Sharing of Vulnerability Status Information ("VEX") v0.1

SBOMによって明らかになる脆弱性が必ずしも悪用可能であるわけではないため、そのexploitabilityを評価する仕組みの検討等を示唆

Playbook for SBOM Consumers

SBOMを受領したソフトウェア利用者がそのSBOMをセキュアに管理するための観点（契約や知的財産等）、ソースコード納品の場合/バイナリ納品の場合それぞれのSBOMの完全性の検証、特にコンパイルやコンテナ実行時などに追加の依存関係が生じることへの注意など、実践的な内容を多く含む

HDO SBOM PoC 2.0 Quick Start Guide v1.2

ヘルスケア部門におけるPoCにおいて、活用した技術、SBOMに含まれる項目、SBOMの取込から脆弱性/リスク管理等、ユースケースに基づく情報を紹介

SBOMのPoCで示したい内容

$$\left[\text{SBOMの導入にかかるコスト} \right] < \left[\text{SBOM導入により削減できる脆弱性対応・ライセンス管理のコスト} \right]$$

SBOMの活用促進に向けて検証すべき事項（仮説）

●適切なSBOMの活用レベル

- ・自社におけるSBOMの活用
- ・サプライチェーンにおけるSBOMの共有
- ・共有したSBOMの活用 etc.

低
高

- ・ 導入コスト
- ・ コスト削減効果

●適切なSBOMの活用・共有の範囲

業界、サプライチェーン、個社 etc.

●SBOMの導入に適した分野

業界構造・商慣習等を踏まえる必要がある etc.

●SBOM導入に向けた技術的検討が必要な観点

SBOM生成・共有・検証・管理手法
各コンポーネントの名称等、フォーマットの統一方法 etc.

●その他

実効性の担保方法（契約への盛り込み、ガイドライン等）

1. 産業分野別SWG

2. 第3層タスクフォース

3. ソフトウェアタスクフォース

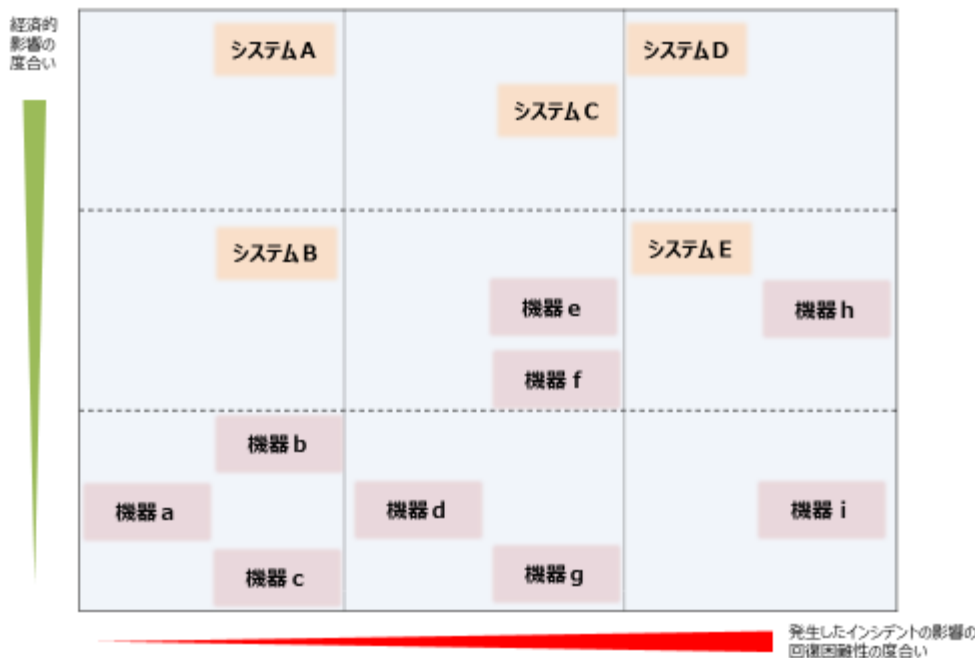
4. 第2層タスクフォース

5. CPSFの国際規格化

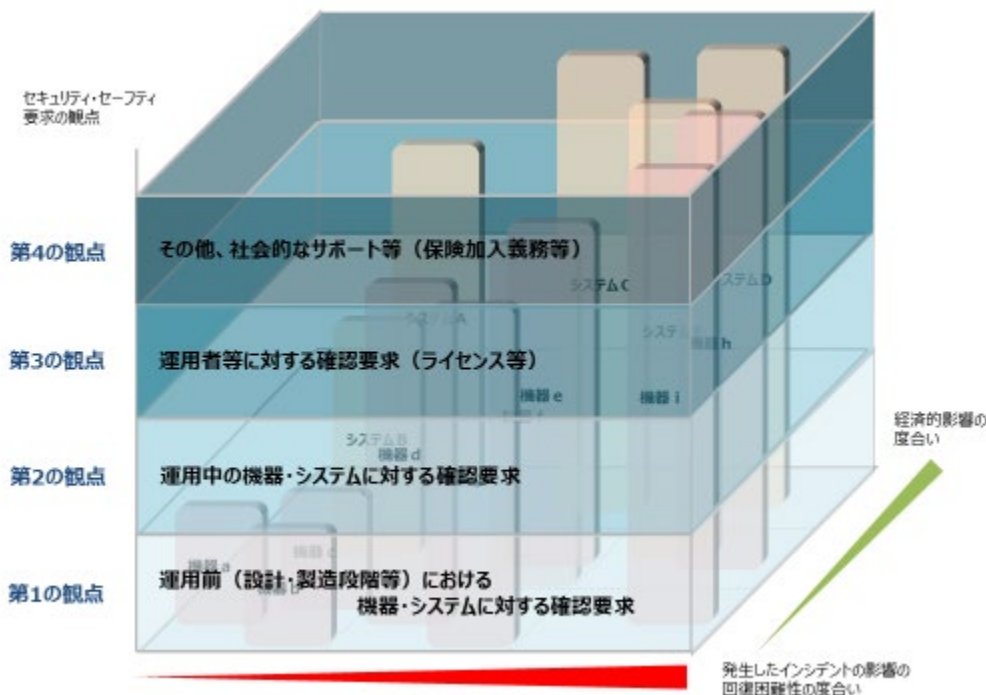
IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

- IoT機器・システムの性質や利用環境によって課題が一樣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。
- 世界中から幅広く意見を収集するため、日本語版・英語版のパブコメを実施。国内外から約100件の意見が寄せられた。パブコメの意見を反映した上で、2020年11月5日にver1.0を公表。

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。）

セキュリティとセーフティの融合への対応 ～製品安全分野における検討

- 欧州では、各NLF関連指令・規則にサイバーセキュリティの要素を盛り込む検討が進行。国際電気標準会議(IEC)においても、遠隔通信を行うIoT機器にサイバーセキュリティの要素を要求する動き。
- 日本では、平成30年度よりIoT化が進む製品を中心に製品安全確保の在り方に関する検討会及び業界団体等によるワーキンググループを設置。令和2年度末以降、ガイドラインを取りまとめる予定。

欧州：各NLF関連指令の検討状況（例）

NLF関連指令	検討状況
無線指令(RED)	・2021年Q2に改正予定 ・EN 303 645(消費者IoTに係る欧州標準)の参照を検討中。
機械指令 (MD)	・2021年Q1に改正予定。 ・IEC 62443の参照を検討中。
一般製品安全指令 (GPSD)	・2021年Q2に改正予定 ・サイバーセキュリティ要素の導入を検討中

製品安全分野におけるサイバーセキュリティ関係の動き

規格	主な要求事項
IEC60335-1 (家庭用及びこれに類する電気機器の安全性 第1部：通則)	・2020年9月発行 ・公衆ネットワークを介した遠隔通信に関する権限承認、暗号技術の適用等の製品安全に係るセキュリティ要求等を整理。

日本：製品安全分野における検討

IoT化を念頭にした製品安全対策を検討する有識者会議を設置。ガイドラインをとりまとめる予定。

● 検討の背景

従来の製品安全対策では想定されていなかったインターネットを介した遠隔操作を念頭に、生命・身体に危害等が及ばぬよう追加すべき対策などを整理する。

● 委員構成

セーフティ及びセキュリティ分野の専門委員、業界団体 等

● 検討内容

IoT化が進展している製品を中心に、インターネットを介し遠隔操作された場合のリスクシナリオ及びユースケースの検討を実施。

● 令和2年度の実施

製品設計上の対応、安全機能のあり方などを整理。IoT化等製品の安全確保の在り方に関するガイドラインを策定検討。今後公表する予定。

1. 産業分野別SWG

2. 第3層タスクフォース

3. ソフトウェアタスクフォース

4. 第2層タスクフォース

5. CPSFの国際規格化

CPSFをインプットとした国際規格の策定

- 国内エキスパートへ協力を仰ぎ、ISO/IECにおいてCPSFのモデル等をインプットとした国際規格の策定を推進。
- 他国の関連文書も考慮しながら、CPSFのモデルをサイバー・フィジカル・システム（CPS）をとらえるモデルの一つとして位置づけ、SC27/WG4 にTechnical Report（TR）を提案している。
- 他SCの国内外エキスパートとも連携しながら、PWI（予備業務項目）としての議論を継続中。

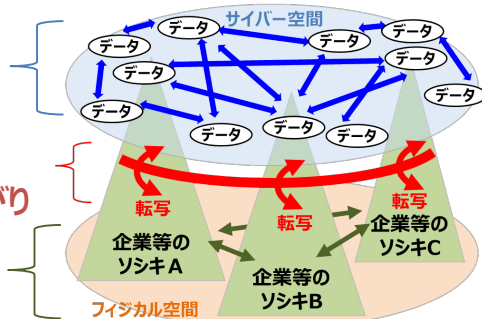
CPSFのモデル

<3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

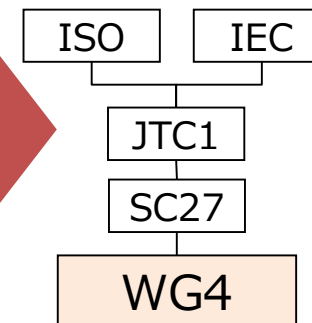


<6つの構成要素>

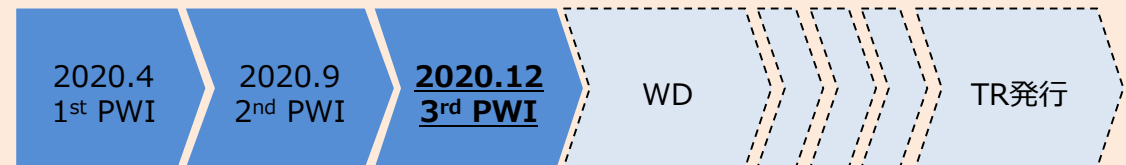
ソシキ	ヒト	モノ
データ	プロシージャ	システム

国際標準化団体へ提案

・「3層構造」
・「6つの構成要素」
というCPSFのモデル等を
インプットとしたTRを提案



SC27/WG4において、これまでにPWIとして3度の意見募集を実施。さらに議論を深め、国際規格（TR）の策定を目指す。



※今後のスケジュールは経済産業省および対応中のエキスパートによる想定

(参考) Like-mindedの関係強化

- 日本の取組を国際的なものとするため、CPSFや産業分野別/分野横断課題への検討成果を海外へ発信し国際的な議論に貢献。

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 (CPSF)

産業分野別の検討	ビル SWG	ビルシステムガイドライン
	自動車 SWG	自工会/部工会・サイバーセキュリティガイドライン
	スマートホーム SWG	スマートホームガイドライン
分野横断的な課題の検討	第3層 TF	データマネジメントの新たな捉え方 (案)
	ソフトウェア TF	OSSの利活用に関する事例集
	第2層 TF	IoTセキュリティ・セーフティ・フレームワーク (IoT-SSF)

英語版公開／公開予定

国際標準化団体へ提案

成果を海外へも発信。
米国・欧州との対話を継続し、
共通認識のレベルを深め、
議論の仲介を図る。

