経済産業省

資料３

『第３層：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の検討の方向性

令和３年３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. 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）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するセキュリティインシデント事例

3. データマネジメントを巡る制度・システムの動向

4. 本タスクフォースの検討事項

＜三層構造と６つの構成要素＞
サイバー・フィジカル一体型社会のセキュリティのためにCPSFで提示した新たなモデル

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造**と**６つの構成要素**）を提示。

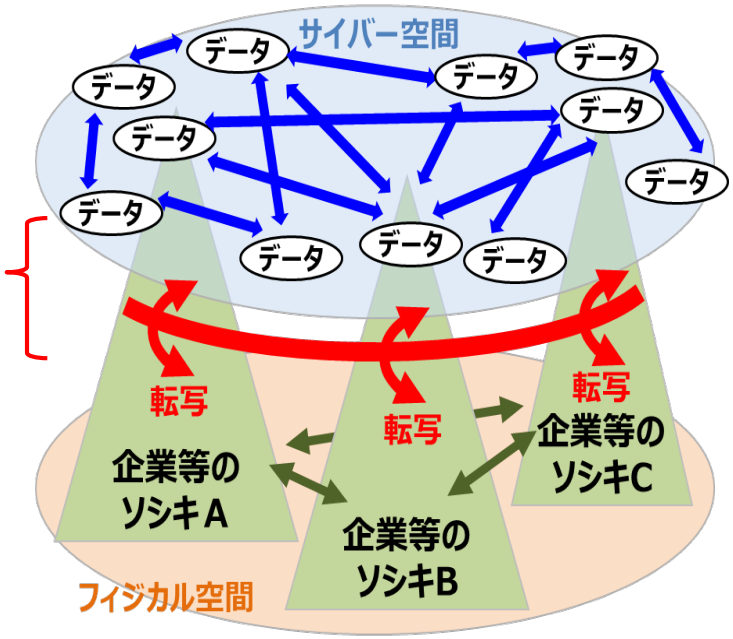
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

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**データの信頼性**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”する機能の信頼性**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
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保



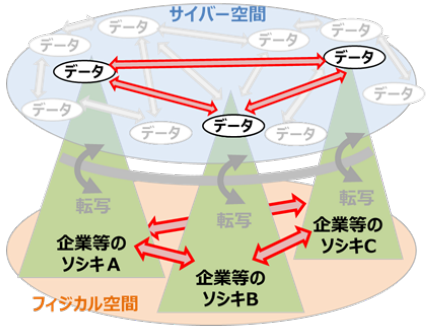
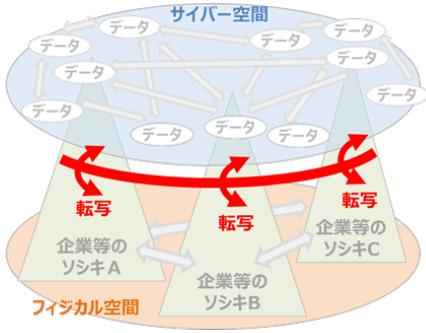
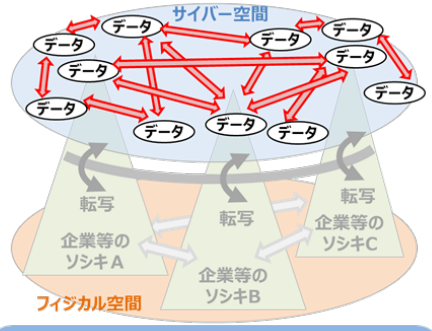
６つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を６つに整理**

構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	ハードウェア、ソフトウェア及びそれらの部品、操作する機器を含む
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の一連の活動の手続き
システム	目的を実現するためにモノで構成される仕組み・インフラ

＜CPSFの全体概要＞
三層構造モデルに基づきリスク源、対策要件等を提示

- サプライチェーンの信頼性を確保する観点から、産業社会を３つの層から捉え、それぞれにおいて**守るべきもの、直面するリスク源、対策要件**等を整理。

	企業間のつながり【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			
機能（守るべきもの）	• 平時及び緊急時のリスク管理・対応体制の構築と運用 • 企業内及び企業間のリスク管理・対応体制の構築と運用	• フィジカル空間とサイバー空間の境界における情報の正確な転写及び正確な転写の証明	• データの加工・分析 • データの保管 • データの送受信
セキュリティインシデント	• 保護すべき資産の棄損 • 他組織のセキュリティ事象発生に起因する事業停止	• 不正確なデータの送信 • 安全に支障をきたす動作	• 保護すべきデータの漏えい • なりすまし等による不正な組織からのデータ受信
リスク源（構成要素ごとに整理）	• セキュリティリスクに対するガバナンスの欠如 • 他組織との連携状況の未把握	• 不正なIoT機器との接続 • 許容範囲外の入力データ	• 通信経路が保護されていない • 通信相手を識別していない
対策要件	■ マネジメントルールの徹底 ■ 関係者との役割分担	■ 接続相手の認証 ■ 安全なIoT機器の導入	■ 暗号化によるデータ保護 ■ データの提供者の信頼性確認

テーマ別TFの検討状況

- **<u>6つの産業分野別サブワーキンググループ(SWG)</u>**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、**<u>3つのタスクフォース（TF）を設置</u>**

産業サイバーセキュリティ研究会ＷＧ１（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**
  - 既存ガイドラインの強化
- **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. 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）とその実装へ向けた取組の方向性

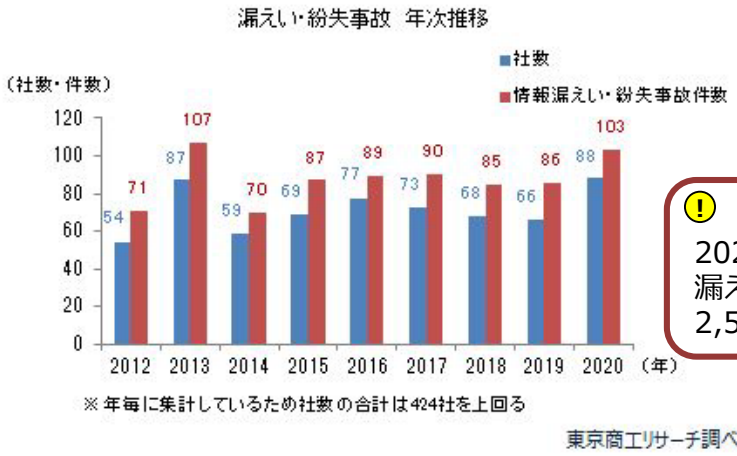
2. サイバー空間のつながりに関するセキュリティインシデント事例

3. データマネジメントを巡る制度・システムの動向

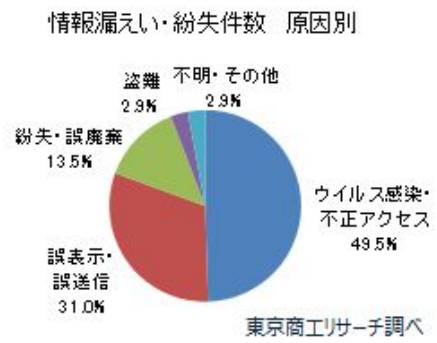
4. 本タスクフォースの検討事項

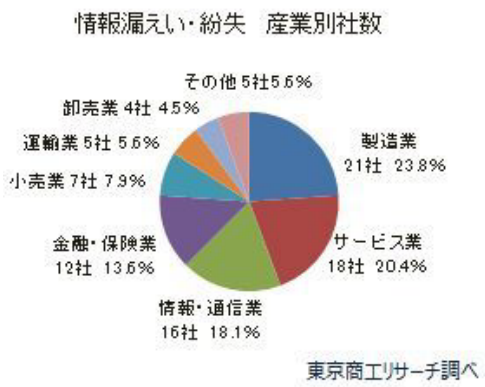
個人情報の流出事案

- 2020年の個人情報の流出事案は、公表社数、件数ともに増加傾向。
  2013年の107件に次いで2番目に多い水準で、7年ぶりに100件を上回った。
- 原因の約5割が、ウイルス感染・不正アクセスで、次いで誤表示・誤送信で約3割を占める。



2020年は88社103件、漏えいした個人情報は2,515万47人分





米国ホテルチェーンの事例（2020年4月）

攻撃者

不正アクセス

①フランチャイズホテルの従業員
ログイン情報を取得(※1)
②ホテルチェーンのシステムにアクセス

米国ホテルチェーン

・推定520万人の個人情報が流出。
・同ホテルチェーンは2018年にも3億8300万人分の個人情報流出により、欧州当局から約132億円の罰金が科された。
＜流出した情報＞
氏名、住所、メールアドレス、電話番号、ロイヤリティプログラムのアカウント詳細、部屋の好み等

※1:ログイン情報の取得経路は明らかになっていない。

国内スマホ決済サービスの事例（2020年12月）

攻撃者

不正アクセス

アクセス権限の設定不備を
突いて社員しか閲覧できないはずの
情報を閲覧

加盟店データベース管理サーバ

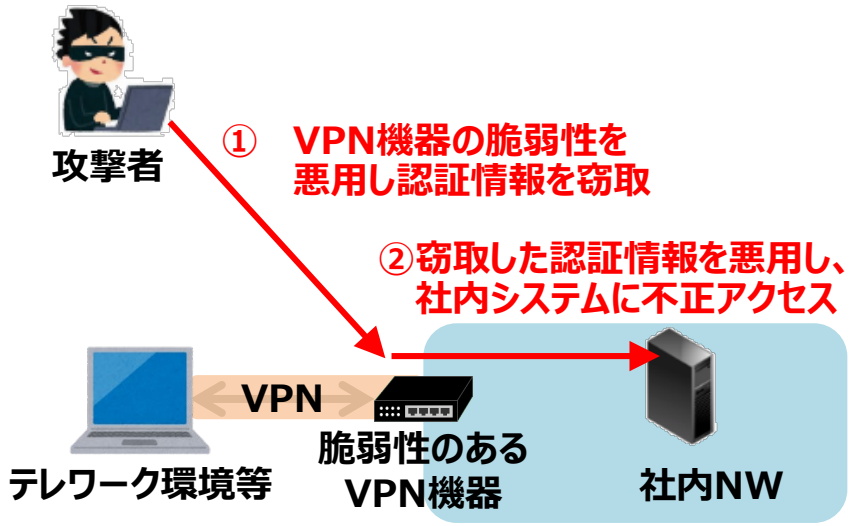
・260万店舗の加盟店などの営業情報が最大2007万件流出。
・発表時点でデータの不正利用は確認されていない。
＜流出した情報＞
加盟店の店名、住所、電話番号、代表者名、代表者生年月日、契約日、売り上げ振込先、営業対応履歴、加盟店営業先の店名、所属、役職、連絡先 等

https://www.tsr-net.co.jp/news/analysis/20210115_01.html
https://pc.watch.impress.co.jp/docs/news/1293581.html
https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident

ネットワーク貫通型：VPN機器の脆弱性を悪用したネットワークへの侵入

- VPN機器の脆弱性が相次いで報告され、そうした脆弱性を悪用するコードが公開されるなど深刻な状況が発生。攻撃者はこうした脆弱性を通じて直接的に社内ネットワークへ侵入し、攻撃を展開。
- 2020年8月、Pulse Secure製VPN機器の脆弱性が悪用され、**国内外900以上の事業者からVPNの認証情報が流出**。2020年11月、Fortinet製品のVPN機能の脆弱性の影響を受ける**約5万台**の機器に関する情報が公開。 **認証情報等が悪用されることで容易に侵入されるおそれ。**
- どちらのケースも既に悪用されている可能性があるため、機器のアップデートや多要素認証の導入といった事前対策に加え、事後的措置として**侵害有無の確認や、パスワード変更等の対応**が必要。

VPN機器に対する不正アクセス



Pulse Secure製VPN機器の脆弱性

2019年4月	脆弱性情報公開
2019年8月	脆弱性の悪用を狙ったとみられるスキャンを確認
2019年9月	脆弱性を悪用したとみられる攻撃を確認
2020年8月	国内外900社（国内は38社）の認証情報が公開

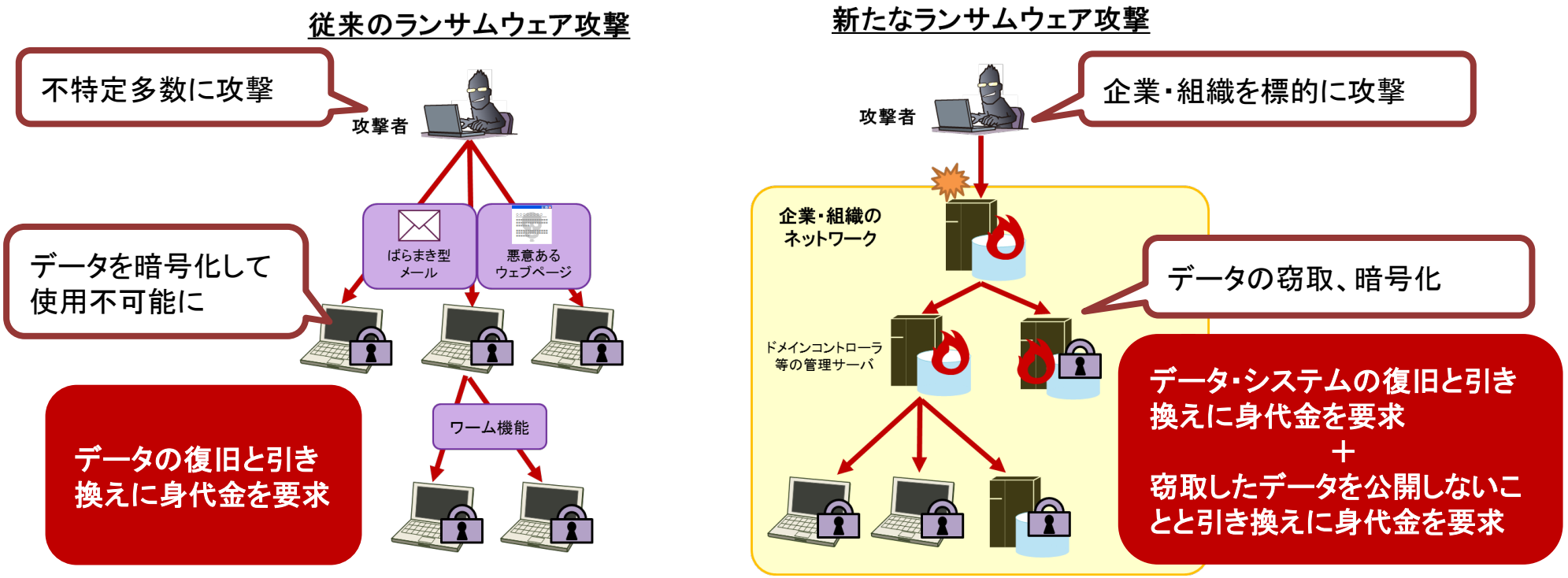
Fortinet製FortiOSの脆弱性

2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等

https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.html

ランサムウェアとその手口の変化（二重の脅迫）

- ランサムウェアは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。
  感染したパソコンのデータを暗号化するなど使用不可能にし、その**解除と引き換えに金銭を要求**する。
- **新たな（標的型）ランサムウェア攻撃（二重の脅迫）とは**
  - ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを窃取した後に一斉に暗号化してシステムを使用不可能にし、脅迫をするサイバー攻撃。
  - システムの**復旧に対する金銭要求**に加えて、窃取した**データを公開しない見返りの金銭要求**も行うので、**二重の脅迫**と恐れられる。窃取された情報に顧客の情報や機微情報を含む可能性がある場合には、被害組織はより困難な判断を迫られることになる。



1. 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）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するセキュリティインシデント事例

3. データマネジメントを巡る制度・システムの動向

4. 本タスクフォースの検討事項

プライバシーシールド無効化に関する動向（概要）

- 米国が2016年にEUと締結していたプライバシーシールドに対して、2020年7月にEU司法裁判所は無効とする判決を下した。

背景

米国はEUに対してプライバシーシールドを締結（2016年）
プライバシーシールドとは、EUのプライバシー原則を遵守することを個別企業が米国商務省に登録した場合に、個人データをEU域外へ持ち出せるとしたもの

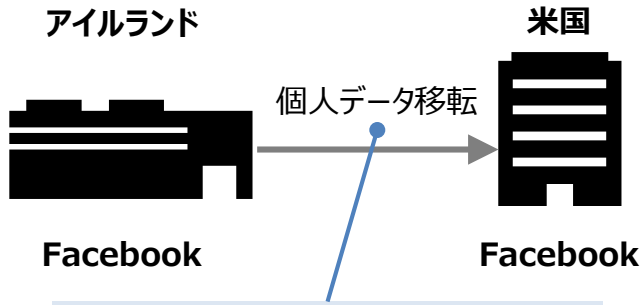
EUにてGDPRが施行（2018年）
GDPRでは原則EU域内から個人データを移転させることは違法とした。

個人データ移転についてEU司法裁判所に申し立て
本申し立てはEU在住ユーザがFacebookに対して行ったものである。

動向の概要

- 2020年7月16日に、EU司法裁判所はEU市民の情報が十分に保護されないとの理由から、EUから米国への個人データの移転を認めるプライバシーシールド決定を無効とする判決を出した。
- プライバシーシールドとは、米国が2016年にEUと締結したものであり、企業はEUのプライバシー原則を遵守すると米国商務省に登録した場合、EU域内から個人情報を移転できるとしたものである。
- 一方で、EU司法裁判所は標準的契約条項（Standard contractual clauses：SCC）と呼ばれるデータ移転契約のひな形を利用することにより、個人データ移転は可能とした。

プライバシーシールドの例（例：Facebook）



プライバシーシールドにおいては米国商務省に事前登録した場合、個人データ移転を認めるとしていた。

標準的契約条項
(Standard contractual clauses：SCC)
欧州委員会が決定したデータ移転契約のひな型で、個人データの移転をGDPR上適法化するためのもの。なお、以下の3つのひな型が用意されている。

- 域内管理者・第三国管理者間のモデル条項 (Decision 2001/497/EC)
- 域内管理者・第三国管理者間のモデル条項 (Decision 2004/915/EC)
- 域内管理者・第三国処理者間のモデル条項 (Decision 2010/87/EU)

(出所)　JETRO" EU司法裁、米国との個人データ移転に関する「プライバシー・シールド」を無効と判断"(2020/7/17)、"標準的契約条項（Standard contractual clauses：SCC）（欧州委員会資料の仮訳）"（2018/3/28）等を参考に作成

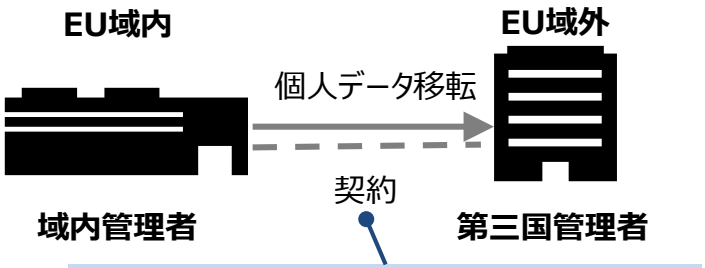
プライバシーシールド無効化に関する動向（企業への影響）

- 個人データをEU域内から移転する企業は契約の再締結が必要となる他、場合によってはデータ移転を中止しなければならない可能性がある。また、日本企業への影響は限定的であるが対応が必要となる場合がある。

契約の締結

- EU司法裁判所は個人データの移転をGDPRの内容に沿った形で実施するためのルールである標準的契約条項のひな形を使用することは認めたため、企業はデータ移転契約を締結する必要が生じた。

<域内管理者・第三国管理者間の場合>

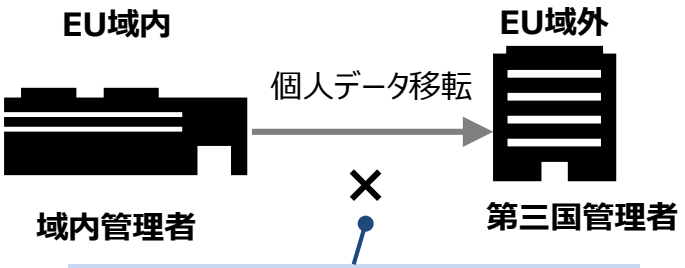


データ移転契約を結ぶ必要がある。

データ移転の中止

- 個人データをEU域内から移転する企業はデータ輸入者が標準的契約条項を守れないと判断した場合には、個人データ移転を中止する必要が発生する。

<域内管理者・第三国管理者間の場合>



データ移転を中止する場合がある。

＜日本企業への影響＞

- 日本とEUは2019年1月に相互に十分性認定をしていることから、**影響は限定的**と見られる。
- ただし、日本に対する十分性認定も欧州委員会による見直しにおいて厳しく審査される可能性があるため、従来、日本への移転を十分性認定のみに基づき行っていた場合は**標準的契約条項を併用することがより安全**と思われる。

(出所) JETRO" EU司法裁、米国との個人データ移転に関する「プライバシー・シールド」を無効と判断"(2020/7/17)等を参考に作成

カリフォルニア州消費者プライバシー法施行に関する動向（概要）

- 個人データに関する問題をきっかけに、米国カリフォルニア州にて2020年1月1日に「カリフォルニア州消費者プライバシー法」が施行された。
- 消費者データのプライバシー規制については、バーモント州（2018年12月施行）、ネバダ州（2019年10月施行）、メイン州（2020年7月施行）等でも制定されている。

背景

カリフォルニア州で通称「Shine the Light」法施行（2005年）

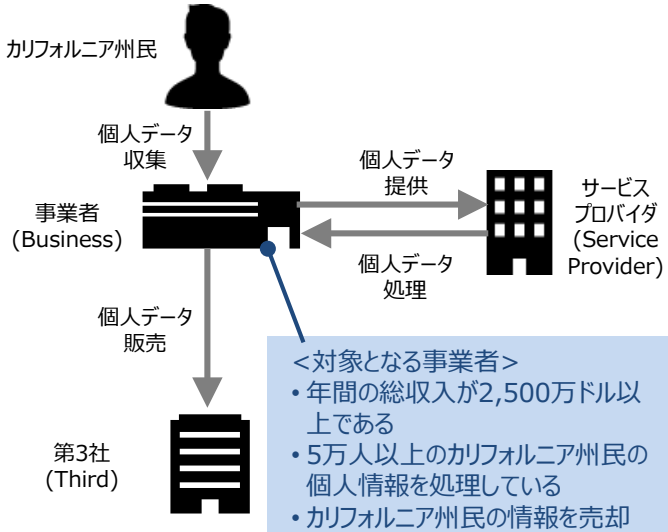
「Shine the Light」法とは、企業がマーケティングを目的として第三者と共有する個人情報の内容を請求する権利を、年1回に限りカリフォルニア州の居住者に付与するものである。

ケンブリッジ・アナリティカ問題（2018年）

2018年3月、Facebookから大量の個人データが流出したことが発覚した際、コンサルティング会社であるケンブリッジ・アナリティカ社がそれらを集め、2016年米大統領選などに使っていたことが明らかとなった。

動向の概要

- 2020年1月1日に、カリフォルニア州はプライバシー権及び消費者保護の強化を目的として、カリフォルニア州消費者プライバシー法を施行した。
- カリフォルニア州消費者プライバシー法では、一定の条件を満たしたカリフォルニア州民の個人情報を収集する事業者を対象としており、消費者に対して以下に示す5つの権利を認めた。



＜対象となる事業者＞
- 年間の総収入が2,500万ドル以上である
- 5万人以上のカリフォルニア州民の個人情報を処理している
- カリフォルニア州民の情報を売却することで年間の収入の50%を得ている

消費者の5つの権利

No	内容
1	企業が収集した個人情報のカテゴリー、情報源、情報の用途および収集した情報の開示先など、**企業のデータ収集の運用について開示請求する権利**
2	消費者による請求から過去12カ月の間にその消費者について収集した具体的な**個人情報のコピーを受け取る権利**
3	**本人の個人情報を削除してもらう権利**（ただし、例外有）
4	企業のデータ売却の運用について知り、その消費者の**個人情報を第三者に売却しないよう求める権利**（いわゆるオプトアウト）
5	消費者らがカリフォルニア州プライバシー法により付与された新たな権利を行使したことに基づいて**差別されない権利**

（出所）JETRO"施行が迫る「カリフォルニア州消費者プライバシー法」（米国）"（2019/6/6）等を参考に作成

カリフォルニア州消費者プライバシー法施行に関する動向（影響）

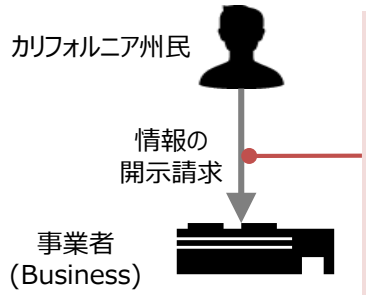
- カリフォルニア州消費者プライバシー法施行によって、企業は個人情報取扱いに関する義務を負った。また、情報開示請求へ対応できなかった場合の罰金規定も設けられており、罰金が高額になる可能性がある。

発生する義務への対応

- 企業として法令を順守するため、主に以下の内容に対応する必要がある。
  - ◆ プライバシーポリシーを更新すること
  - ◆ 請求している消費者の本人確認をする手順を実施すること
  - ◆ 45日以内に情報開示するために社内で個人情報を特定・発見することができるようにすること
  - ◆ 特定の情報開示を電子的に行う方法を開発すること
  - ◆ 売却禁止を求める消費者のオプトアウト（16歳未満の消費者に関してはオプトイン）に対応すること　等

罰金規定への対応

- 消費者からの情報開示請求に対して1件あたり最大2,500ドルの罰金（故意だと認定される場合には最大7,500ドル）を科せられる可能性があり、請求数によっては罰金が高額となる可能性があるため対応が必要となる。



45日以内に事業者は情報を開示する必要がある。
仮に、この情報開示請求に対応がされず、カリフォルニア州長官より受ける通知に対して是正がなされない場合、事業者に対して罰金が科される可能性がある。

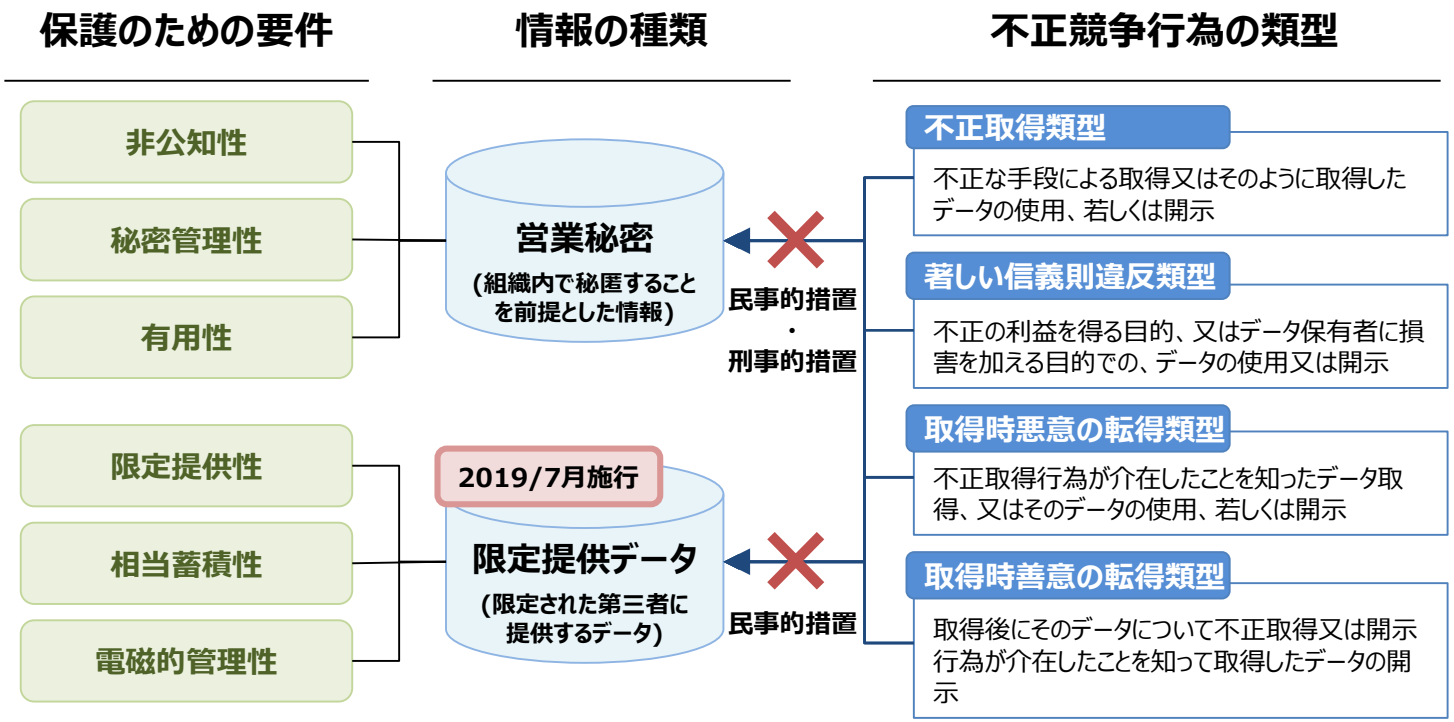
＜日本企業への影響＞

- 今後、日本企業・組織が米国国内においてビジネスを行っていく上では、説明責任の一環として、例えば「**カリフォルニア州消費者プライバシー法の適用を受けるか否か**」、（受ける場合）「**どのようにカリフォルニア州消費者プライバシー法を遵守しているか**」、（受けない場合）「**なぜカリフォルニア州消費者プライバシー法の適用を受けないと判断をしたか**」について、説明できるように準備する必要がある。

（出所） JETRO ”施行が迫る「カリフォルニア州消費者プライバシー法」（米国）”(2019/6/6)、”カリフォルニア州消費者プライバシー法(CCPA)実務ハンドブック”（2019/12/25）等を参考に作成

不正競争防止法 [営業秘密/限定提供データ関連規定の概要]

- 不正競争防止法(日本)では、従来から「非公知性」、「秘密管理性」、「有用性」の3要件を満たすような組織内で秘匿することを前提とされた情報を営業秘密として法的に保護。
- 2018年の改正において、事業者等が取引等を通じて第三者に提供するデータを念頭に新たに「限定提供データ」を定義し、不正競争行為に対する保護の範囲を拡大。
- すなわち、不正競争防止法上の保護を得るためには、法で定められた要件を満たすデータの管理が求められる。



(出典)「『第３層：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の検討の方向性」(2019年7月)

米国の輸出管理規制（ECRA）

- 米国における安全保障の確保を目的として、2018年に輸出管理改革法(ECRA)が制定された。
- 特に企業のデータマネジメントに大きな影響を与えうるのは「みなし輸出規制」（次ページに詳細）

輸出管理改革法 (ECRA)

概要

- 輸出管理法に代わるものとして2018年に制定され、米国の商取引上のデュアルユース(軍民両用)、軍事物質、ソフトウェア及び技術の輸出、再輸出に対する規制を確立。
- 特徴として、AI・量子技術などエマージング・基盤技術(Emerging and Foundational Technologies)に関する輸出管理を強化。

エマージング技術 (Emerging Technologies)	基盤技術 (Foundational Technologies)
次に示す技術分野はエマージング技術に含まれる。（バイオテクノロジー、ＡＩ・機械学習、測位技術、マイクロプロセッサー、先進コンピューティング、データ分析、量子情報・量子センシング技術、輸送関連技術、付加製造技術(3D プリンタ等)、ロボティクス、ブレインコンピュータインターフェース、極超音速、先端材料、先進セキュリティ技術）	具体的対象品目は明らかになっていないものの、既存の未規制技術で、米国が優位性を確保する上で重要なものという観点より、基盤技術が指定されるものと想定される。

輸出管理改革法の下位法令

- 輸出管理改革法の下位法令として輸出管理規則が位置付けられており、具体的な規制内容が規定されている。
- 輸出管理規則の規制対象となるのは以下の4パターン。なお、「技術」を例としている。

輸出規制	
米国から米国に存する技術を外国に輸出する場合	
再輸出規制	
米国原産の技術を米国の輸出先国から更に第三国に輸出する場合	
みなし輸出規制	
米国内において外国籍者に技術を開示する場合 [次ページに詳細を記載]	
みなし再輸出規制	
米国からの輸出先において、輸出先国以外の国籍に技術を開示する場合	

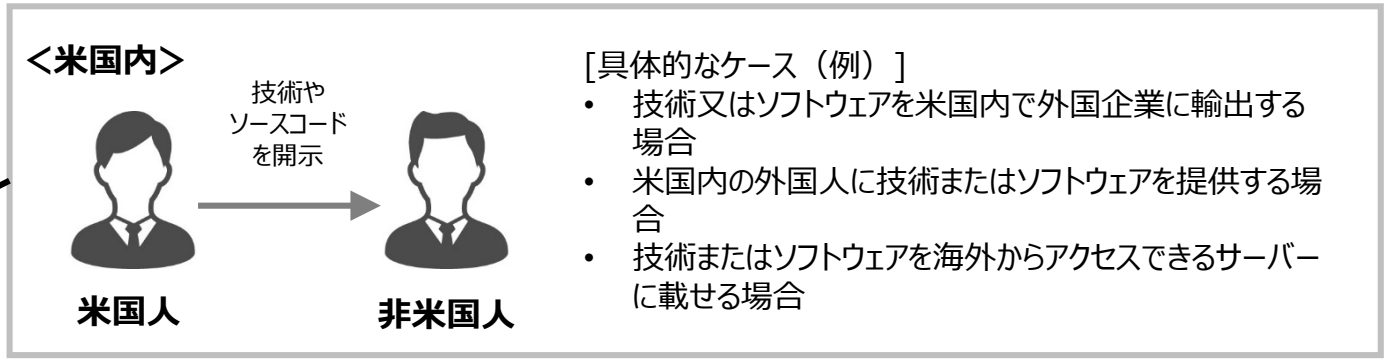
（出所）CISTEC"米国輸出管理改革法（ECRA）に関する基本的 QA"(2019/3/19)等を参考に作成

米国の輸出管理規則における「みなし輸出」

- 米国の輸出管理規則では、米国内にて米国人から非米国人に対して技術等が開示される場合にはみなし輸出と判断され、輸出管理の対象となる。

みなし輸出のイメージ

- みなし輸出の対象者は「人」であり国籍にて判断する。なお、以下はみなし輸出の対象から除外される。
  - ✓ 永住権資格を持つ者
  - ✓ 米国の市民権を持つ者
  - ✓ 保護されている個人"としての資格を与えられた者
- 技術とは、製品の“開発”、“製造”又は“使用”に必要となる特定の情報と定義する。



[具体的なケース（例）]
- 技術又はソフトウェアを米国内で外国企業に輸出する場合
- 米国内の外国人に技術またはソフトウェアを提供する場合
- 技術またはソフトウェアを海外からアクセスできるサーバーに載せる場合

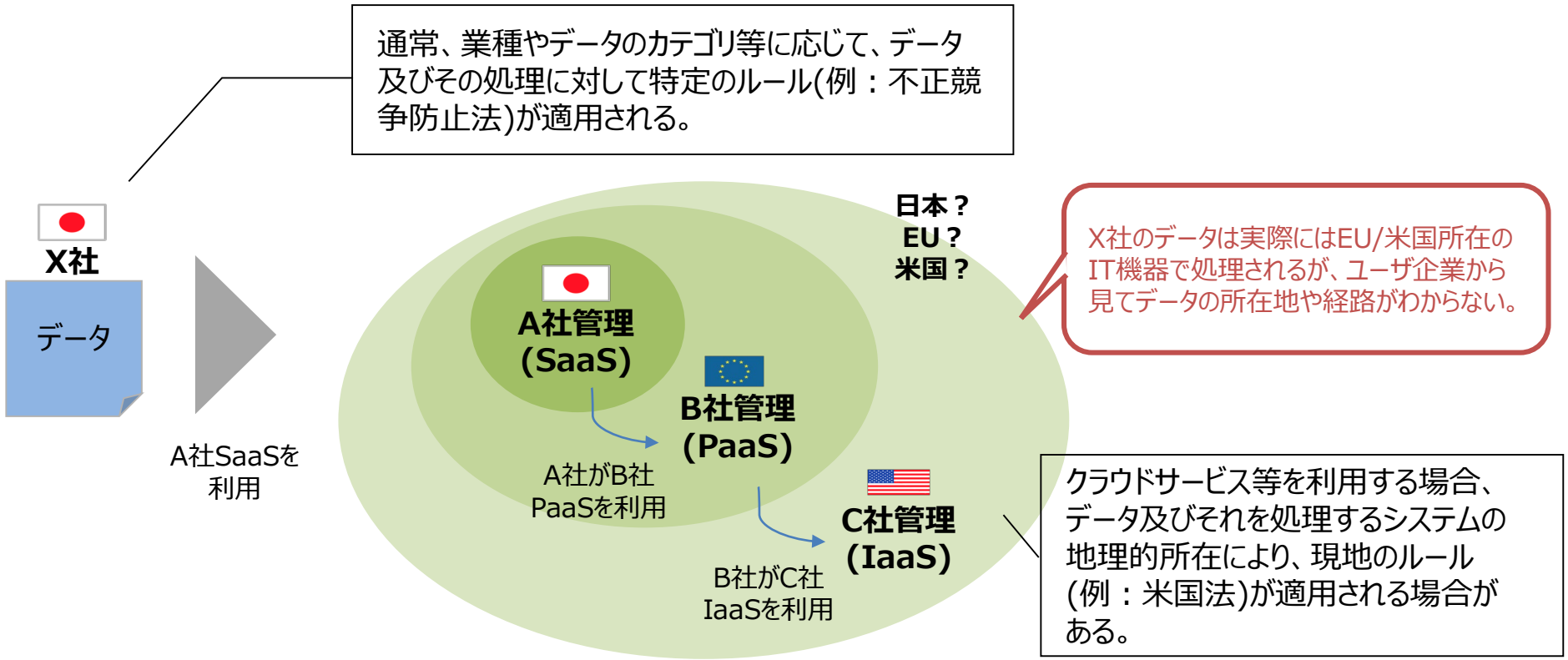
∨

みなし輸出と判断し、輸出許可が必要となる

(出所) CISTEC”EAR Q&A” 等を参考に作成

システム構成の多層化・重層化によるデータマネジメントの複雑化

- クラウドサービスの利用の進展により、データが生成され価値を生む場所と実際にデータが処理される場所が異なることがあるなど、**<u>システムの多層化・重層化が進展している</u>**。
- システムの複雑性が増すほど、データが取り扱われる「場」がフィジカル空間と乖離することがある。



1. 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）とその実装へ向けた取組の方向性

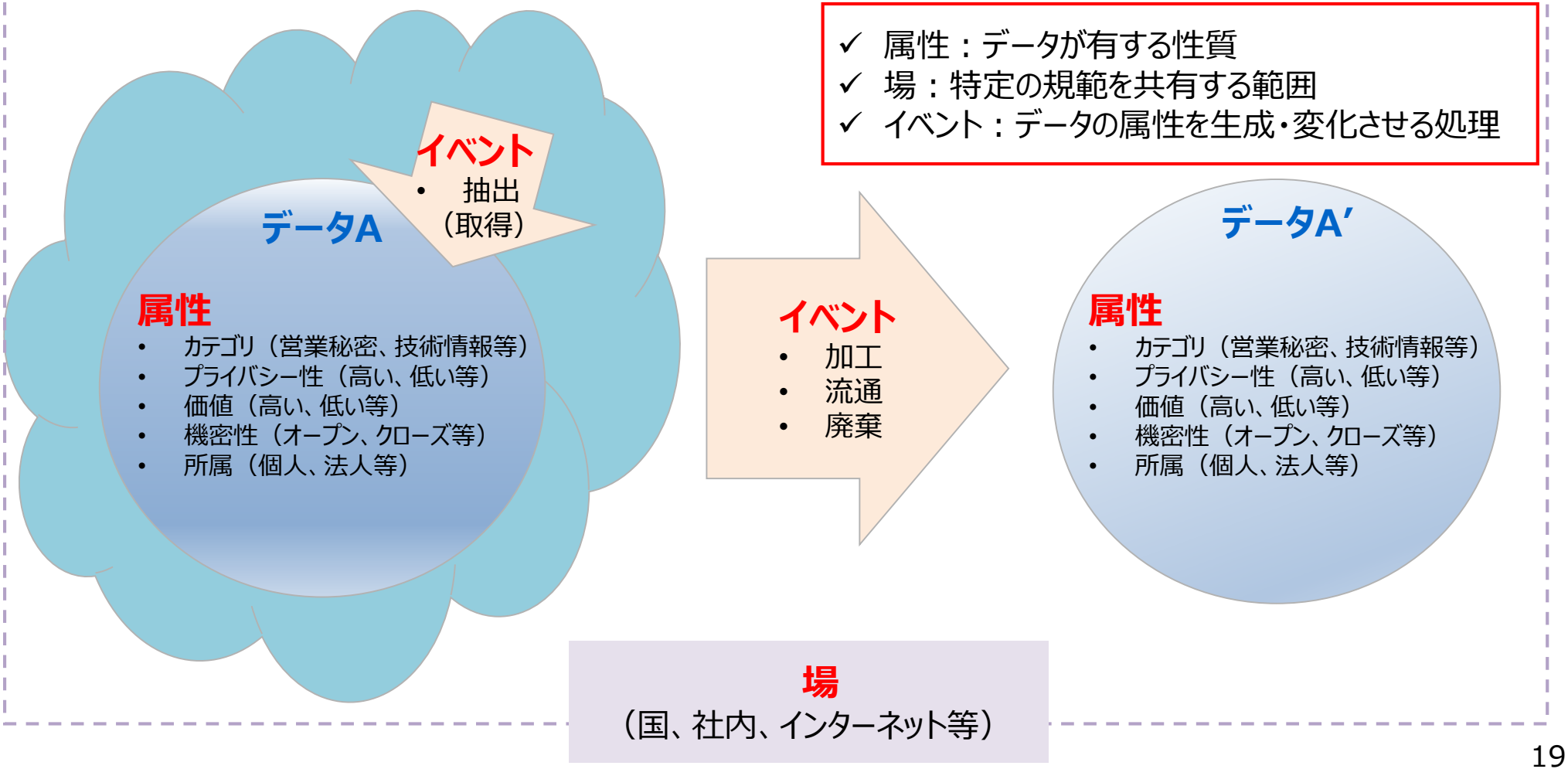
2. サイバー空間のつながりに関するセキュリティインシデント事例

3. データマネジメントを巡る制度の動向

4. 本タスクフォースの検討事項

データマネジメントの新たな捉え方（第２回TF資料再掲）

- 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に関するこれまでの議論

- 第2回タスクフォースにおいて、委員から多くの御意見をいただいたが、その多くは、「データが転々流通することにより、その属性を変えながら付加価値を生み出していく」ことを捉えきれていないのではないか、という観点での御指摘であった。

第２回で頂いた御意見（抜粋）

- IoTデバイスで取得したデータも、データの利用目的が必ずしも初期の目的のままであるとは限らない。トレーサビリティが課題。
- データを客観的に見ただけでは付加属性はわからないが、一方でその付加属性こそが、法的な意味が強いことがある。
- モデルの中に主体という概念を入れた方がいいのではないか。
  ある人から見れば営業秘密で、ある人から見れば個人情報のように、主体によって属性が変わってくることがある。
- データが転々と譲渡されるに従って、データを取得して扱う時に何を気にしなければならないかという情報が消えてしまい、非常に間違った使われ方をしてしまうリスクも上がってくる。
- 信頼性が高い方が良いものだという一方向の議論にならないように、トレードオフの部分は必ず考えておかなければならない。

➡ **御意見を踏まえ、本モデルを「データが転々流通する社会」に適合する形に拡張する**

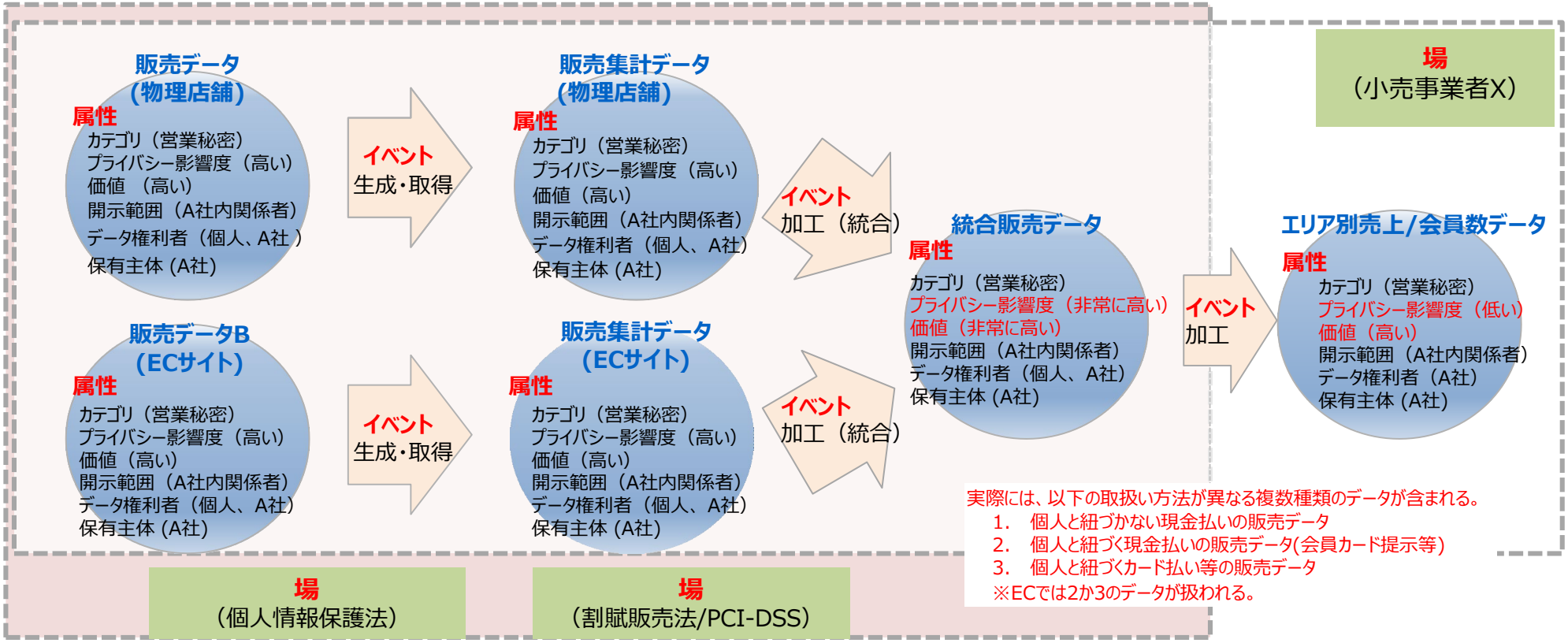
拡張のイメージ

- あるデータに対して、**複数主体間にまたがる複数のイベントが連続して発生すること**を捉える。
- データ属性の中で、**データを保有・管理している主体とは別に、当該データに対して権利が生じている主体**（例：個人Aの個人情報が企業Xに渡った後も個人Aは企業Xが保有するデータに対する権利を有する）を位置づける。（データ権利者）

データマネジメントの新たな捉え方の拡張（ケース1）

- 前ページの内容を踏まえ、データマネジメントの新たな捉え方を拡張したイメージは下記のとおり。
- 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**が重要なのではないか。

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。

データマネジメントの新たな捉え方の拡張（ケース2）

- 高齢者生活支援（見守りや健康アドバイス）提供のため、家電や健康器具各社が提供するデバイス等のデータを集約する課程で、データが転々流通する形態を念頭に整理すると下記の通り。

高齢者生活支援事業イメージ（想定）

場
（個人情報保護法、不正競争防止法）

場
A社ポリシー

室温、人の動き、映像
属性
カテゴリ（住民Xの個人関連情報）
プライバシー性（高い）
価値（高い）
開示範囲（A社内関係者）
データ権利者（住民X、A社）
保有主体（A社）

イベント
生成・取得

統合データ(A社保有)
属性
カテゴリ（住民の個人関連情報、A社の限定提供データ）
プライバシー性（高い）
価値（非常に高い）
開示範囲（A社内関係者）
データ権利者（住民、A社）
保有主体（A社）

イベント
移転

家庭血圧、測定日時
属性
カテゴリ（住民Xの個人関連情報）
プライバシー性（高い）
価値（高い）
開示範囲（B社内関係者）
データ権利者（住民X、B社）
保有主体（B社）

イベント
生成・取得

統合データ(B社保有)
属性
カテゴリ（住民の個人関連情報、B社の限定提供データ）
プライバシー性（高い）
価値（非常に高い）
開示範囲（B社内関係者）
データ権利者（住民、B社）
保有主体（B社）

イベント
移転

場
B社ポリシー

統合データ（PF事業者保有）
属性
カテゴリ（住民の個人関連データ、各社、PF事業者の限定提供データ）
プライバシー性（高い）
価値（非常に高い）
開示範囲（PF内関係者）
データ権利者（住民、各社、PF）
保有主体（PF事業者）

イベント
加工・利用

高次データ（PF事業者保有）
属性
カテゴリ（住民の個人関連データ、各社、PF事業者の限定提供データ）
プライバシー性（高い）
価値（非常に高い）
開示範囲（PF内関係者）
データ権利者（住民、各社、PF）
保有主体（PF事業者）

イベント
移転

高次データ（サービス事業者保有）
属性
カテゴリ（住民の個人情報、各社、PF事業者の限定提供データ）
プライバシー性（高い）
価値（非常に高い）
開示範囲（サービス事業者内）
データ権利者（住民、各社、PF）
保有主体（サービス事業者）

場
PF事業者ポリシー

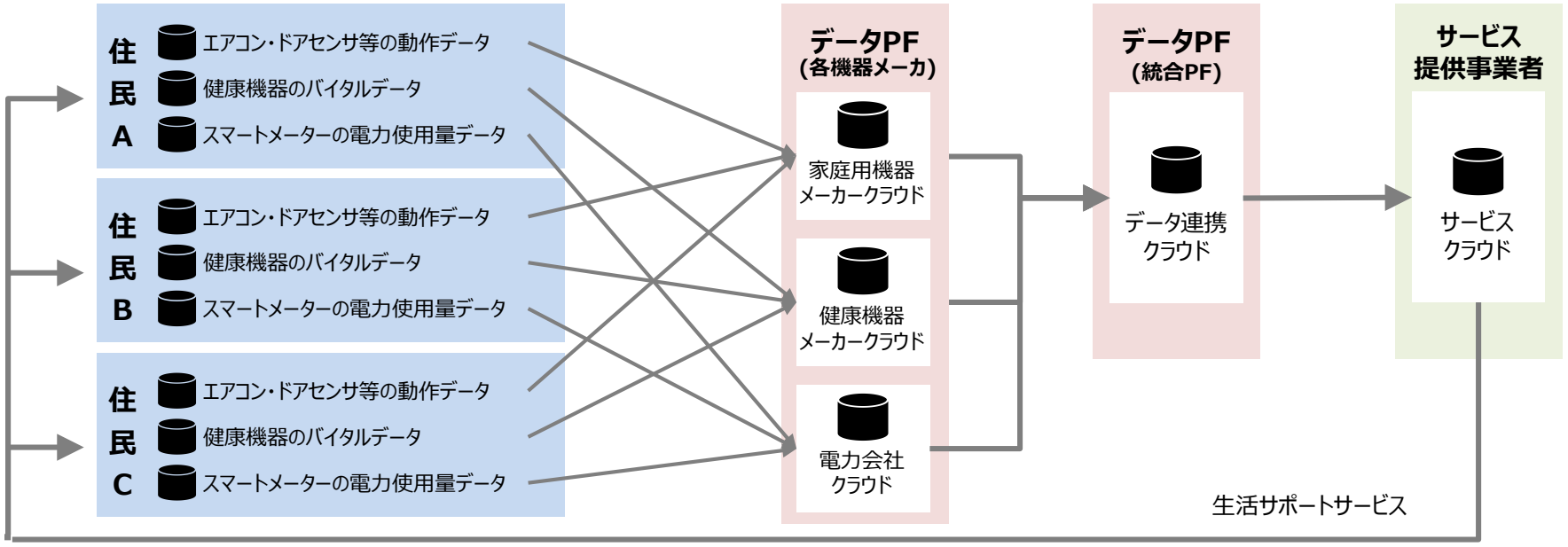
場
サービス事業者ポリシー

場
（データ取扱い規定(契約)）

参考：ケース2 概要

- 高齢者生活支援（見守りや健康アドバイス）提供のため、家電や健康機器各社が提供するデバイス等のデータを集約する課程で、データが転々流通する形態の事業イメージは下記の通り。

- データ連携クラウド上にて蓄積した機器データ群を分析・統合し、高齢者の生活をサポートするサービス提供事業者に対して有効な高次データを生成するのに加え、当該データを、サービス提供事業者に提供する。
- 機器データとして、ベッド上での呼吸状況・活動状況、ドア開閉、人体の通過など高齢者の動き情報、体重、家庭血圧などのバイタルデータを各機器メーカが運用するクラウド上に転送した後、データ連携クラウドに集約する。
- データ連携クラウドから、高次データとして、例えば、高齢者の生活リズムの情報(睡眠環境、トイレ回数など)やリハビリ効果把握に資する情報を、在宅の高齢者の生活をサポートするサービス提供事業者(ケアマネジャー、栄養士など)へ提供する。
- 上記を通じて、これまで把握困難であった在宅高齢者の生活リズムなどの把握が可能となり、在宅高齢者の生活全般を支えうるサービスの提供が可能となる。



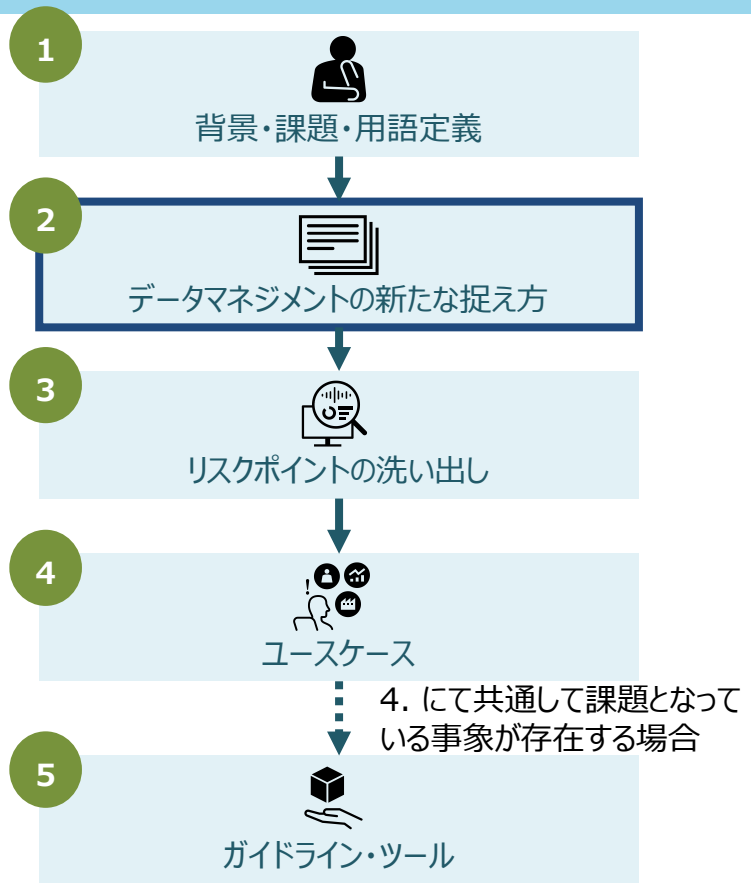
タスクフォースの検討の方向性

- **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利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

本タスクフォースのアウトプットイメージ

- 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。
- 本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する。



分野横断的なデータマネジメントの定義やモデル化を行って、フレームワークとして理解する。

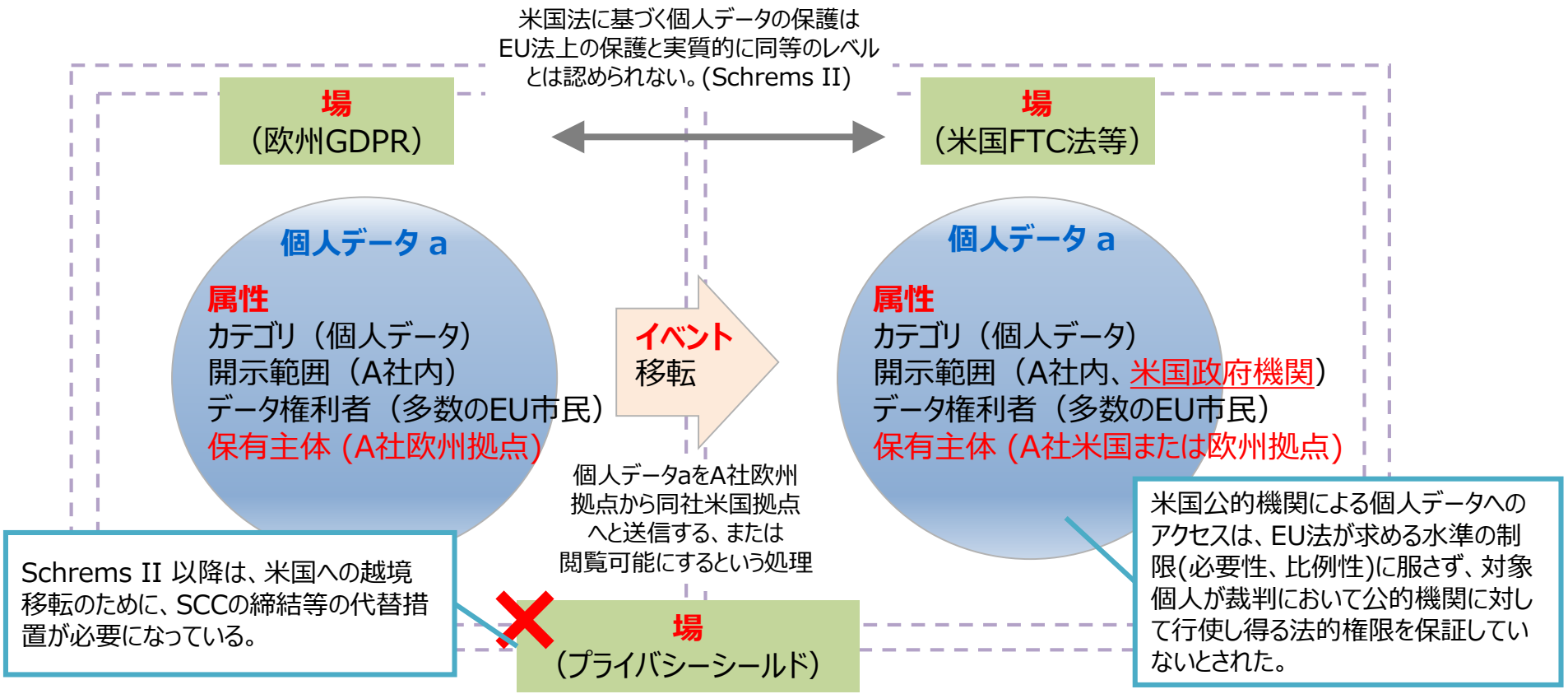
2. で策定されたモデルに基づき、適切な観点(例：イベント)ごとに考慮すべき一般的なリスクを洗い出す。

2. や3. で策定された分野横断的なモデルを、各分野・業種におけるデータ利活用事例に適用し、モデルの改善やデータマネジメントに関する分野横断的な課題の抽出を行う。

4. において分野横断的な課題が抽出される場合、必要に応じてガイドライン・ツール等に関する検討を行う。

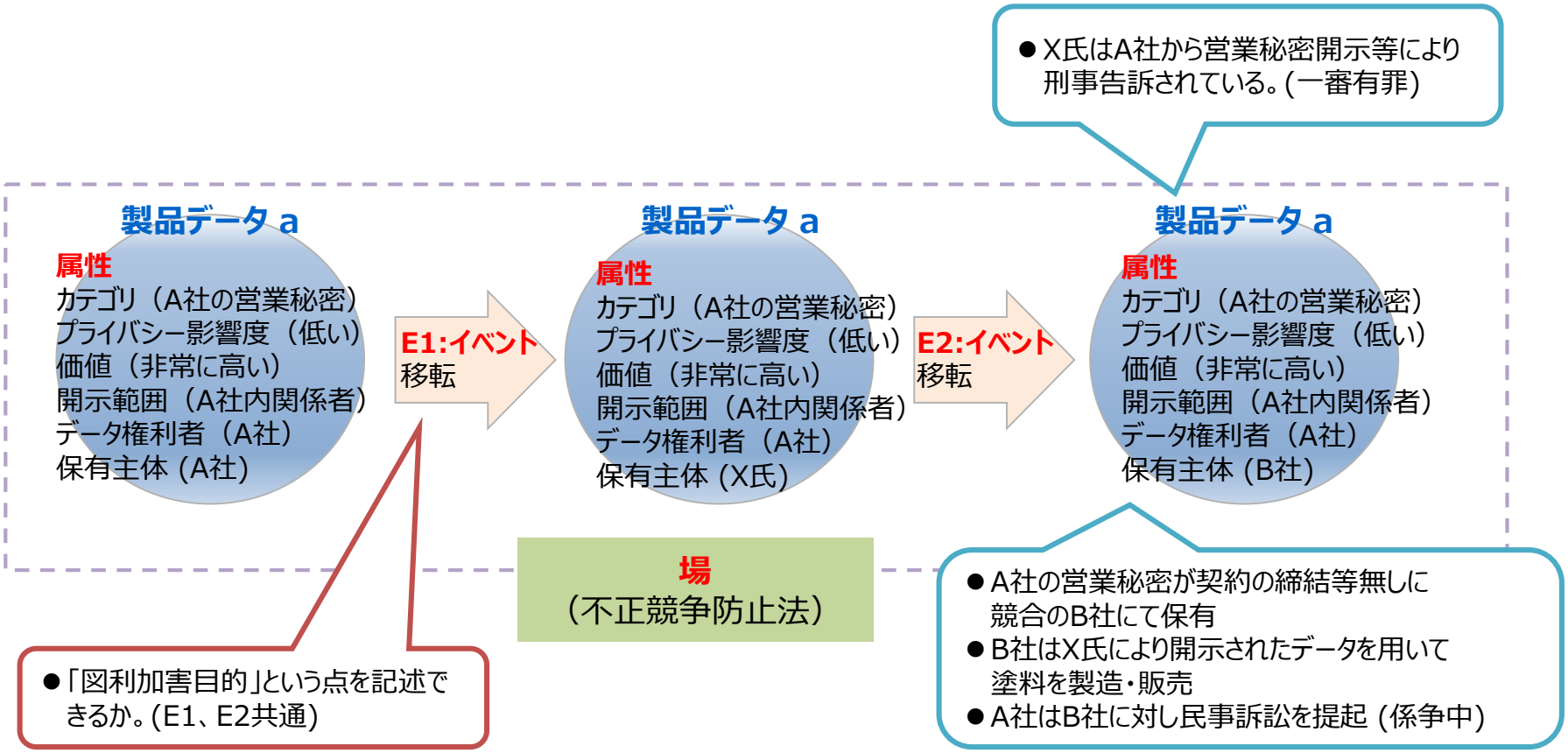
「データマネジメントの新たな捉え方」への当てはめ　①シュレムス判決

- 欧州域内で収集された個人データを米国拠点へ送信するケースについて、米欧の枠組みとしてのプライバシーシールドが有効だった際は、係るケースは容認されたが、同枠組みが有効でないという判断が下された後は別の枠組み(例：SCC、BCR) が必要となっている。(cf. Schrems II)
- **域外適用等の関係で、「場」というものが、伝統的な場（フィジカル空間）とは大きく異なっている**ことに注意が必要である。



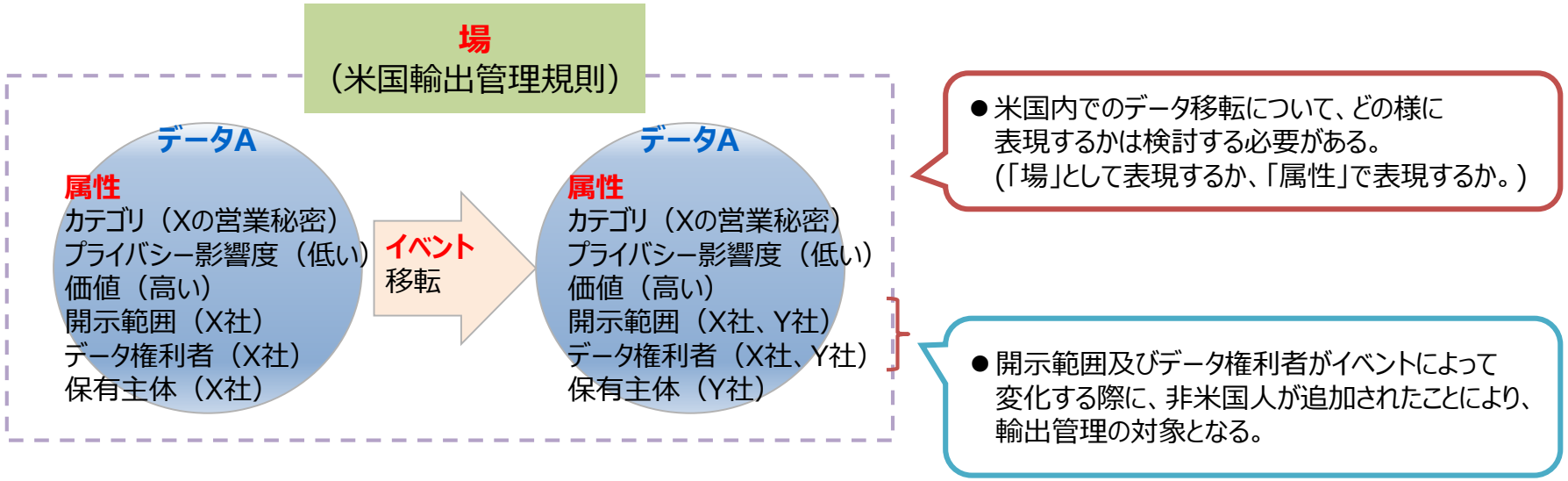
「データマネジメントの新たな捉え方」への当てはめ　②不正競争防止法

- 大手塗料メーカー(A社)の元執行役員である被告人(X氏)が、塗料の商品設計に関する情報(D1：製品データ a)をUSBメモリーに複製して保存(E1)し、競合企業(B社)に転職後、書面やメールで開示した行為(E2)が、営業秘密の領得・開示に当たるとして、懲役2年6月、執行猶予3年、罰金120万円が科された(名古屋地判令 2.3.27)



「データマネジメントの新たな捉え方」への当てはめ　③米国輸出管理制度

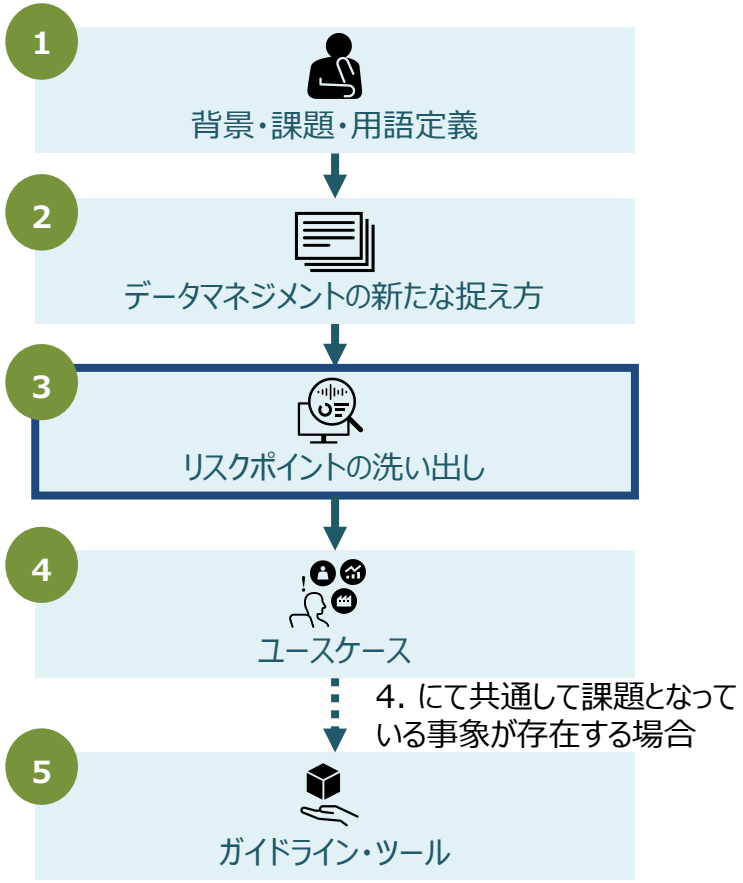
- 米国内にてX社に属する米国人AがY社に属する非米国人Bに対して、技術を提供する。
  なお、ここで指す技術とは製品の開発、製造、使用等に必要となる特定の情報(営業秘密)とする。



みなし輸出と判断する際には、開示範囲やデータ権利者のステータスを確認する必要がある。

「データマネジメントの新たな捉え方」を活用したリスクポイントの洗い出し

- データマネジメントの新たな捉え方を活用したリスクポイントの洗い出しの手順のイメージを整理する。



分野横断的なデータマネジメントの定義やモデル化を行って、フレームワークとして理解する。

2. で策定されたモデルに基づき、適切な観点(例：イベント)ごとに考慮すべき一般的なリスクを洗い出す。

2. や3. で策定された分野横断的なモデルを、各分野・業種におけるデータ利活用事例に適用し、モデルの改善やデータマネジメントに関する分野横断的な課題の抽出を行う。

4. において分野横断的な課題が抽出される場合、必要に応じてガイドライン・ツール等に関する検討を行う。

「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。

「新たな捉え方」への当てはめのステップ

（後のページに各ステップのイメージを記載）

STEP 1 データ処理フローの可視化

STEP 2 必要な制度的な保護措置(場)の整理

STEP 3 「属性」の具体化

STEP 4 イベントごとのリスクの洗い出し

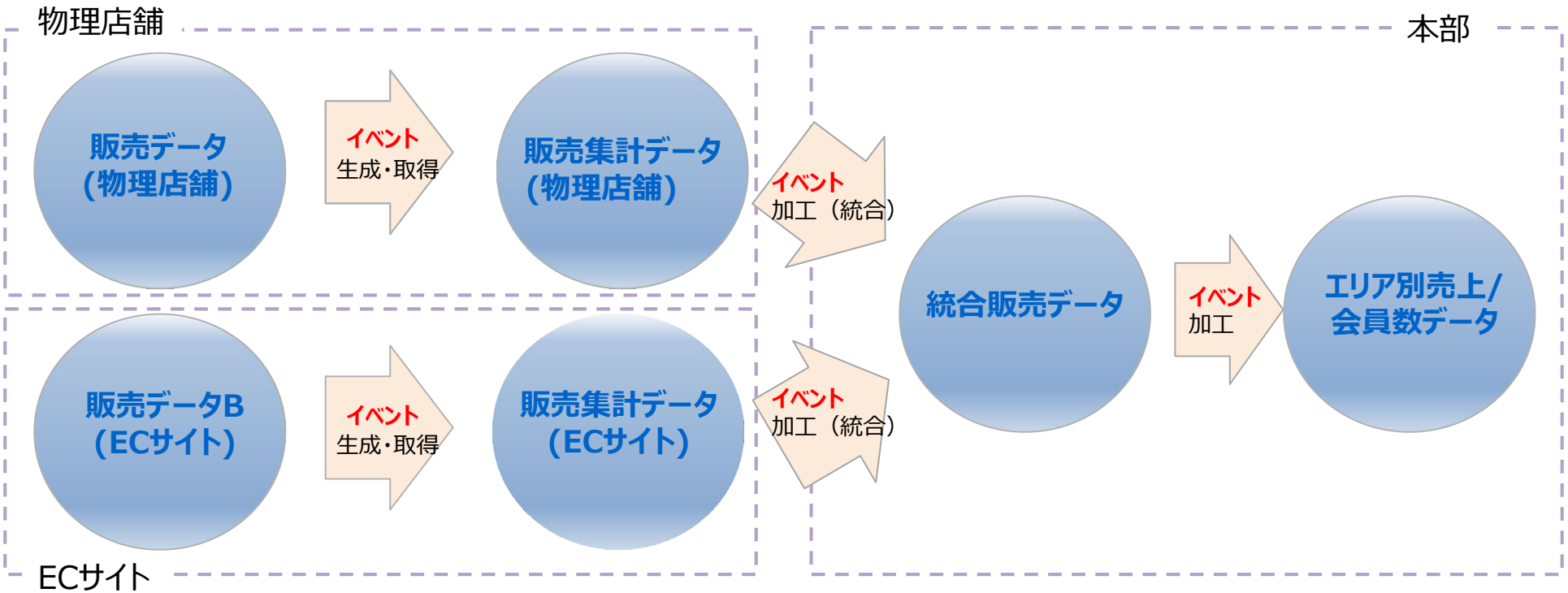
イベントごとのリスクの洗い出しの枠組み（イメージ）

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。

POSデータ活用を例にした「データマネジメントの新たな捉え方」への当てはめプロセス (1/4)

- **小売業において、販売店舗とECサイトからPOSデータを取得、統合した後、データを加工してエリア別売上や会員数を集計するケース**を想定する。
- はじめに、想定されるデータ利活用プロセスにおける大まかなデータフロー及びイベントを可視化する。

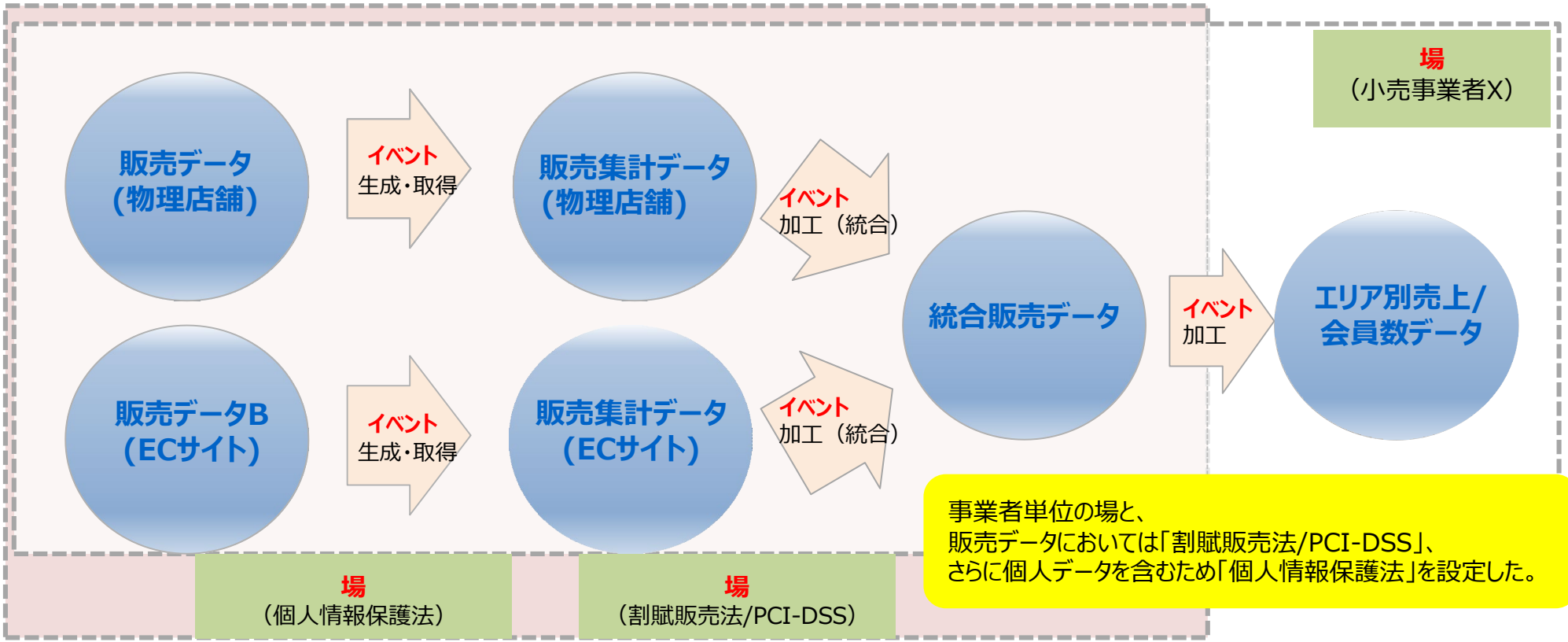
STEP 1 データ処理フローの可視化 → **STEP 2** 必要な制度的な保護措置(場)の整理 → **STEP 3** 「属性」の具体化 → **STEP 4** イベントごとのリスクの洗い出し



POSデータ活用を例にした「データマネジメントの新たな捉え方」への当てはめプロセス (2/4)

- 次に、データ保護に資する「場」を検討し、法律・契約の観点から適切なものを設定し、必要に応じてイベント等を追加する。

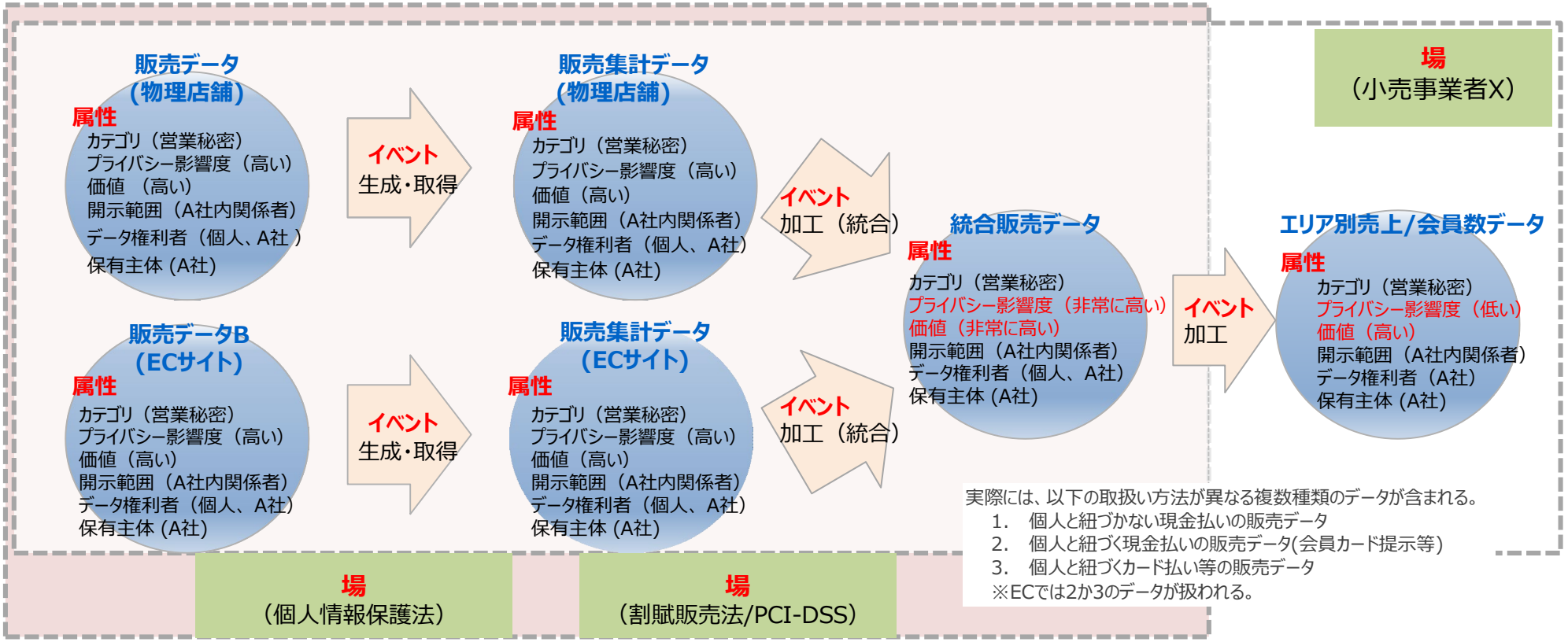
STEP 1 データ処理フローの可視化 → **STEP 2** 必要な制度的な保護措置(場)の整理 → **STEP 3** 「属性」の具体化 → **STEP 4** イベントごとのリスクの洗い出し



POSデータ活用を例にした「データマネジメントの新たな捉え方」への当てはめプロセス (3/4)

- 従前に設定されたデータや「イベント」、「場」に基づいて、管理上あるべき「属性」を特定する。

STEP 1 データ処理フローの可視化 → **STEP 2** 必要な制度的な保護措置(場)の整理 → **STEP 3** 「属性」の具体化 → **STEP 4** イベントごとのリスクの洗い出し



実際には、以下の取扱い方法が異なる複数種類のデータが含まれる。

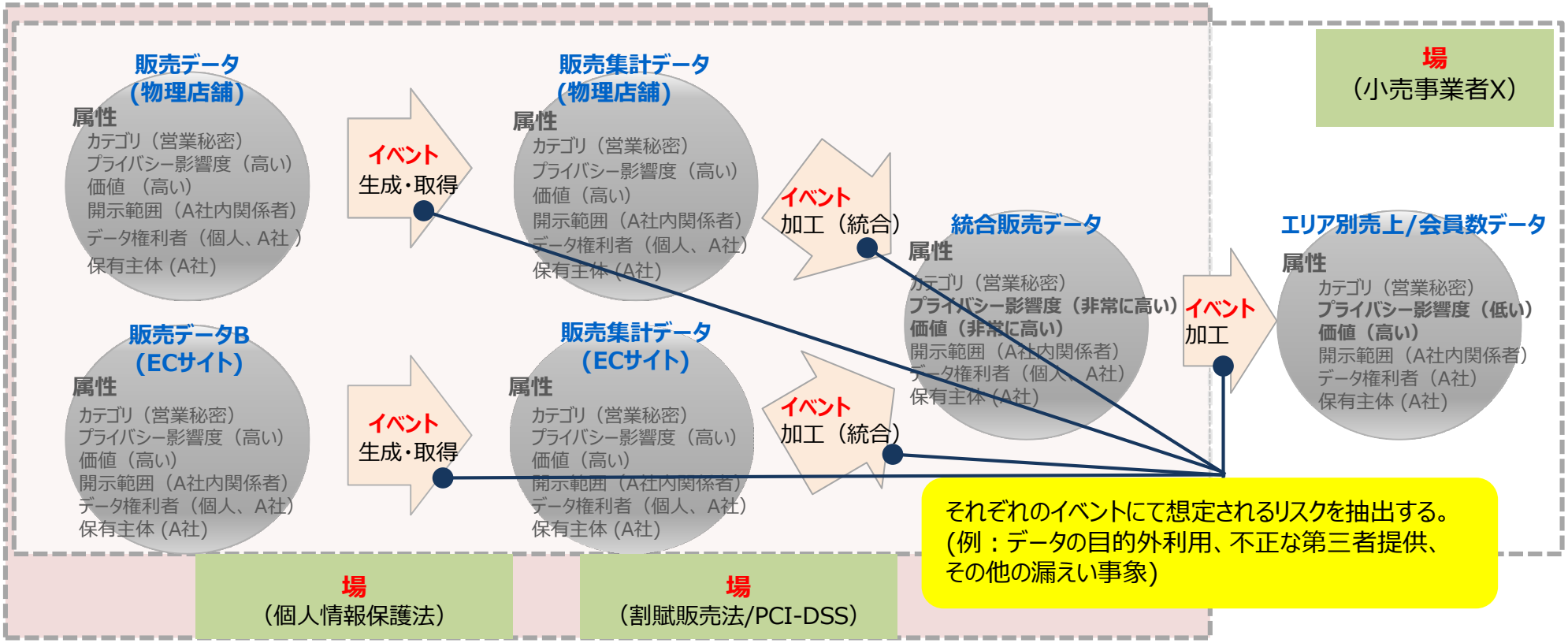
1. 個人と紐づかない現金払いの販売データ
2. 個人と紐づく現金払いの販売データ(会員カード提示等)
3. 個人と紐づくカード払い等の販売データ

※ECでは2か3のデータが扱われる。

POSデータ活用を例にした「データマネジメントの新たな捉え方」への当てはめプロセス (4/4)

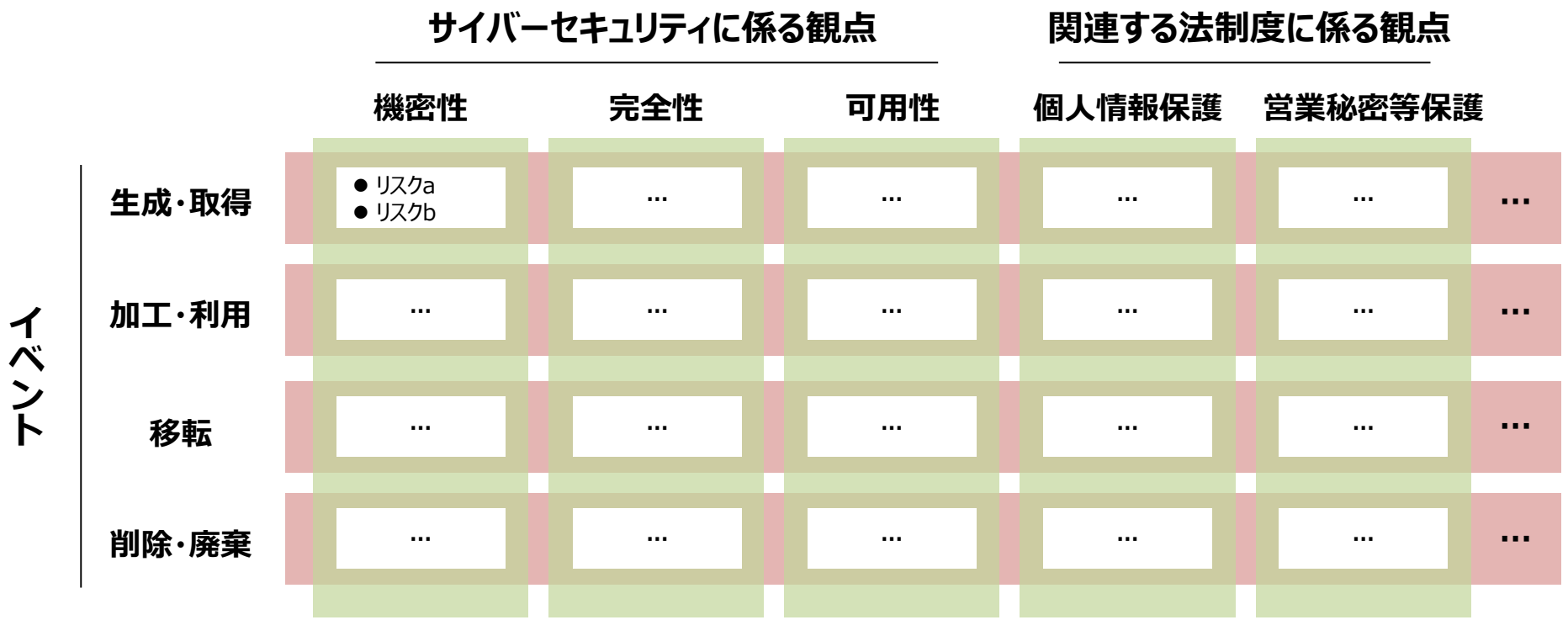
- 設定された「場」という観点から、各イベントごとに想定されるリスクを抽出し、設定した「属性」をレビューする。※次ページに例。

STEP 1 データ処理フローの可視化 → **STEP 2** 必要な制度的な保護措置(場)の整理 → **STEP 3** 「属性」の具体化 → **STEP 4** イベントごとのリスクの洗い出し



イベントごとのリスク洗い出し（イメージ）

- イベントの類型ごとに、サイバーセキュリティやその他の観点からリスクを抽出する。



- 機密性、完全性、可用性に加え、リスク抽出の際には、真正性や責任追跡性等についても考慮する。
- データ保護に係る代表的な法制度を考慮する。

リスクポイントの洗い出しに向けて整理すべき事項の議論イメージ

イベント類型

- **生成・取得**
- **加工・利用**
- **移転**
- **廃棄**

論点1：
イベントをどのように類型化すべきか。

考慮すべき属性(例)とその効用

論点2：
どのような属性を考慮すべきか。

カテゴリ	主に法的な観点からデータの取扱いを明確化できる。
プライバシー影響度	当該データが侵害された際の個人のプライバシーに対するリスクの大きさを明確化できる。
価値	当該データが侵害された際の関係する事業者に対するリスクの大きさを明確化できる。
開示範囲	機密性の観点からデータの取扱い範囲を明確化できる。
データ権利者	当該データの管理に直接的または間接的に関わる主体を特定できる。
保有主体	当該データの管理に直接的に関わる主体を特定できる。

懸念事項を抽出する際に考慮すべき観点

機密性	認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性。
完全性	正確さ及び完全さの特性。
可用性	認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。

論点3：
リスクの洗い出しの際に考慮すべき観点にはどんなものがあるか。

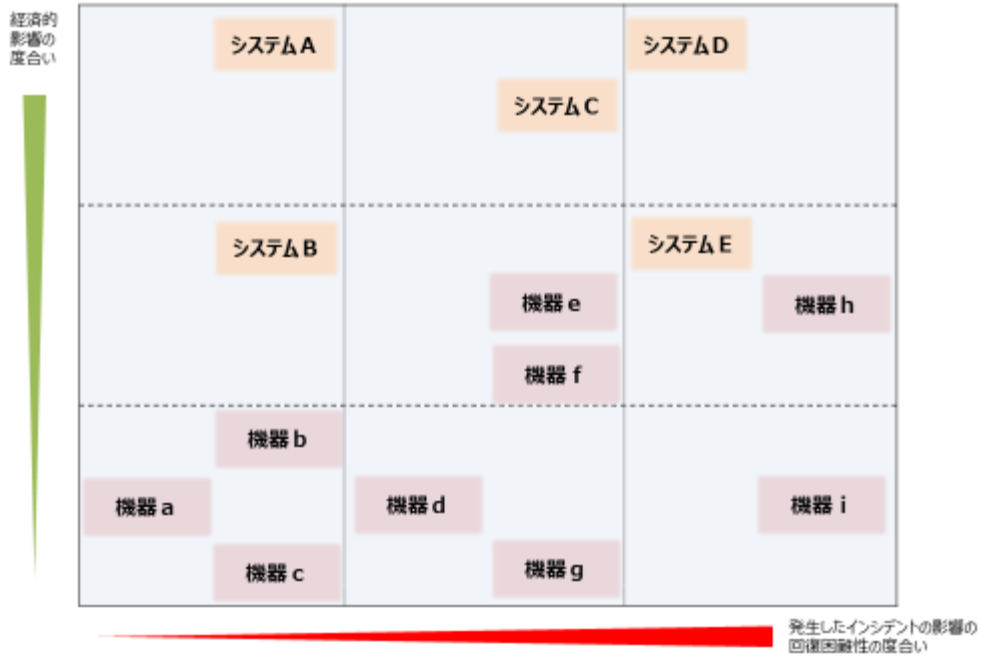
なお、対策を検討するに当たっては、下記の４つの観点も参考になる。

✓ **真正性**	エンティティは，それが主張するとおりのものであるという特性。
✓ **責任追跡性**	あるエンティティの動作が、どの動作から動作主のエンティティまで一意に追跡できることを確実にする特性。
✓ **信頼性**	意図する行動と結果とが一貫しているという特性。
✓ **否認防止（安全性）**	主張された事象又は処置の発生，及びそれを引き起こしたエンティティを証明する能力。（重要ではあるが、第２層（フィジカル空間とサイバー空間のつながり）で考慮すべき観点）

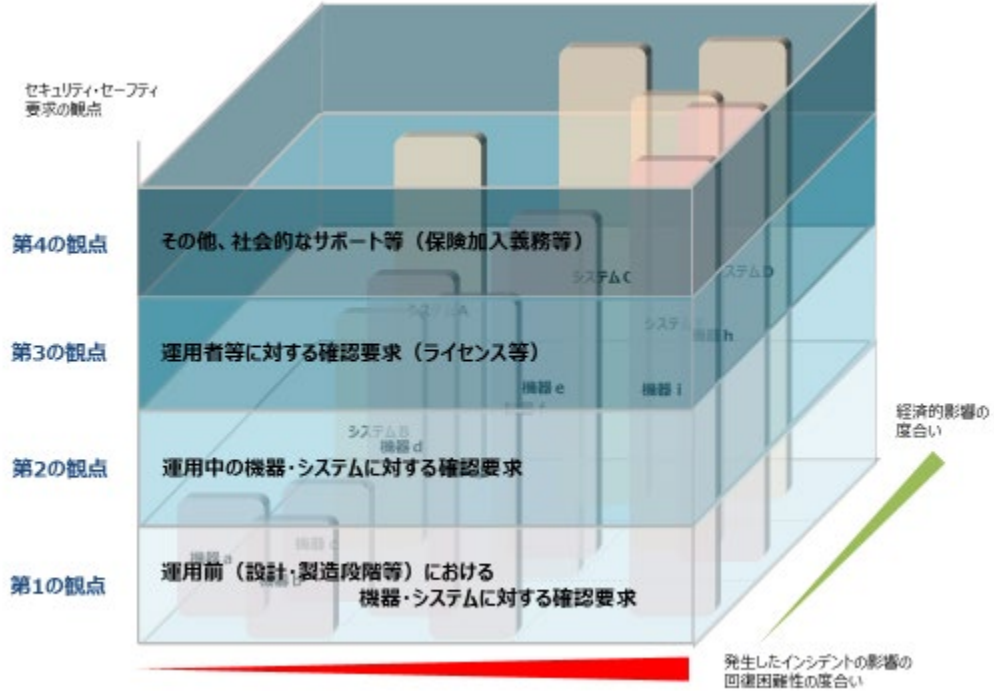
参考：第２層 IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の策定

- IoT機器・システムの性質や利用環境によって課題が一様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。）

イベントごとのリスクポイント洗い出しのイメージ

- イベントに着目し、考慮すべき観点に基づいて懸念事項と対処ポイントを抽出することが可能ではないか。
- イベントの類型や懸念事項等の具体化のレベル等について御意見をいただきたい。

対象イベント	観点及び想定される懸念事項(例)	リスク(例)	懸念事項への対処ポイント(例)
 **生成・取得**	**機密性** 生成・取得過程でデータが漏えいする。	●不正アクセス ●盗聴 ●マルウェア感染 ●内部犯行 ●過失 他	●取得元と取得者との通信において、安全なバージョンのSSL/TLS暗号通信プロトコルを利用する。(盗聴等を想定)
	完全性 データが生成・取得過程で不正に改ざんされる。		●取得元と取得者との通信において、安全なバージョンのSSL/TLS暗号通信プロトコルを利用する。(MITMを想定)
	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。		●取得元と取得者との間の契約において、サービスレベルに関する条項を設け、双方で合意する。

参考：今後のTFでの議論の叩き台となる資料

属性の定義と概要（叩き台）

- 適正なデータ管理のために考慮すべき「属性」として、以下の事項を抽出した。

属性の定義と概要

属性類型	概要	パラメータ例
カテゴリ	関連する法制度に基づいて適用され得るデータの分類を記載する。	● 個人情報保護法：個人情報(要配慮個人情報を含む)/個人情報(要配慮個人情報を含まない)/匿名加工情報/仮名加工情報/非個人情報 ● 不正競争防止法：〇〇の営業秘密/〇〇の限定提供データ/上記以外
プライバシー影響度	個人情報主体および/または個人情報主体のグループのプライバシーに及ぼされる影響の度合いを記載する。	● 高/中/低
価値	データの機密性、完全性又は可用性が損なわれた際に生じうる影響の度合いを記載する。	● 高/中/低
開示範囲	提供者に前もって知らせなくても、購入者がデータを開示してよいかを記載する。	● 制約あり/特に制約なし
利用目的	利用を認める用途に制約があるか、あるとすればどのような制約かを記載する。	● 商用利用/研究利用/教育利用/その他/特に制約なし
処理根拠の有無	データの取扱いを正当化する法制度的な根拠の有無を記載する。	● 根拠あり/根拠なし/根拠必要なし
保有期限	年月の経過や制度改定によって、データが無効になることはあるかどうかを記載する。	● 保有期限の制約あり/制約なし
データ権利者	データに適法にアクセスし、その利用をコントロールできる事実上の地位、または契約によってデータの利用権限を取り決めた場合にはそのような債権的な地位を保有する主体を記載する。	● A社/B社/個人X
保有主体	実際にデータを保有する主体を記載する。	● A社/B社

イベントの定義と概要(叩き台)

- データのライフサイクルを踏まえて、「イベント」を「生成・取得」、「加工・利用」、「移転」、「廃棄」の4つに整理することができるのではないか。

イベントの定義と概要

イベント類型	概要	該当する処理例
生成・取得	物理的なインターフェースからの入力等に基づき、データが自動的/非自動的に生成・取得され加工、利用が可能となるプロセス	● IoT機器によるセンシング ● 手動によるデータ入力
加工・利用	特定の利用目的を達成するために、生成・取得されたデータが論理演算され、加工済みのデータや分析結果等のアウトプットが生成されるプロセス	● データ構造の加工(例：抽出、結合、分割) ● マスキング ● データ解析(例：回帰、決定木、クラスタリング) ● ダッシュボードを通じた可視化 ● 上記の結果を活用した業務改善、意思決定等
移転	ネットワーク、その他の経路を通じて、データが認可された内外のエンティティへ移転され、加工・利用が可能となるプロセス	● 可搬媒体(例：USBメモリ、CD)を通じた移転 ● 電子メールを通じた移転 ● ファイル共有サービスを通じた移転 ● REST APIを通じた移転
廃棄	想定されるリスクの大きさに対して妥当と考えられるデータの除去、破壊等の処置を通じて、当該データの加工・利用が不可能となるプロセス	● 専用ソフトによる消去 ● 専用装置による消去 ● HDDの物理的破壊

データの分類及び関連する法令（例）

- 「場」を検討するにあたり、それぞれの法令ごとに考慮すべきデータの分類の一例として以下がある。

データの分類に関連する法令

法令	保護措置等の検討に際して考慮すべきデータの分類(例)	概要
個人情報保護法	特定個人情報/要配慮個人情報/個人データ/仮名加工情報/匿名加工情報	個人情報の取扱いに関する基本法と個人情報取扱事業者に対する義務等を定める。当該義務の中に個人データの安全管理措置義務が含まれる。
不正競争防止法	営業秘密/限定提供データ	不正競争の防止を目的の一つとしており、営業秘密や限定提供データの保護や、技術的制限手段の無効化、回避の禁止等を定める。
著作権法	著作物	プログラムを含む著作物の保護と複製権をはじめとする著作権等について規定している。
民法	個々の秘密保持契約等にて定められる秘密情報	契約に関する規律や、不法行為に基づく損害賠償求等を規定している。個々の秘密保持契約等にて定められる秘密情報

（参考）その他、企業の内部統制等に係るサイバーセキュリティ関係法令

会社法	・・・	取締役に対し、サイバーセキュリティを確保するための体制を含む内部統制システム構築義務を課している。
労働基準法	・・・	労働基準を定める法律であり、企業の就業規則に関する規定などを置いている。その他、労働契約に関する基本的な事項を定める労働契約法（平成19 年法律第128 号）等がある。
独占禁止法	・・・	私的独占、不当な取引制限、不公正な取引方法などについて規定している。カルテルや優越的地位の濫用、データの独占等に該当するとして、データの取扱いに対しても規律が及ぶ場合がある。
刑法	・・・	不正指令電磁的記録に関する罪（いわゆるウィルス罪）をはじめとするサイバー犯罪を処罰する規定を含む刑罰が規定されている。
不正アクセス禁止法	・・・	不正ログインといった不正アクセス行為や、いわゆるフィッシング行為を処罰する旨が規定されている。

(出所) 内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）『サイバーセキュリティ関係法令Q&Aハンドブック Ver1.0』(令和2年3月) 等を参考に、経済産業省作成