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６月３０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の動向

4. 本タスクフォースの検討事項

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**
  - 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1.0版を公表(2021.4)
- **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の動向

4. 本タスクフォースの検討事項

クラウドサービスの設定不備を原因とする不正アクセス

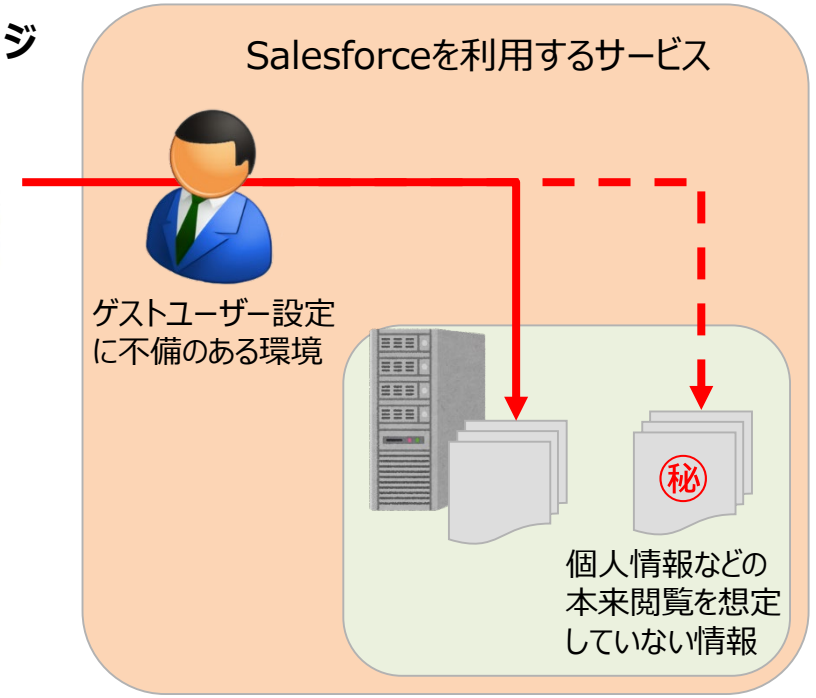
- 2020年12月25日、セールスフォース・ドットコムは、同社が提供するサービスにおける**ゲストユーザーに対する情報共有に関する設定が適切に行われていない場合、一部情報が第三者より閲覧できる**事象の発生を公表。また、**複数の国内事業者が本事象による不正アクセス及び個人情報漏えいの発生**を公表。
- 本サービスを組み込んだシステムがパッケージとして複数の顧客に提供され、同時に被害が発生したケースも。
- クラウドサービスを活用する際には、サービスの利用状況や各種設定の確認・見直しを行うなど、適切なセキュリティ対策を講ずることが重要。

◆不正アクセスがあったと公表した事業者等

- キャッシュレス決済サービス事業者
- サービス事業者
- クレジットカード事業者
- 小売事業者
- 玩具メーカー
- ガス事業者
- 地方自治体
- 独立行政法人　　他

◆攻撃イメージ

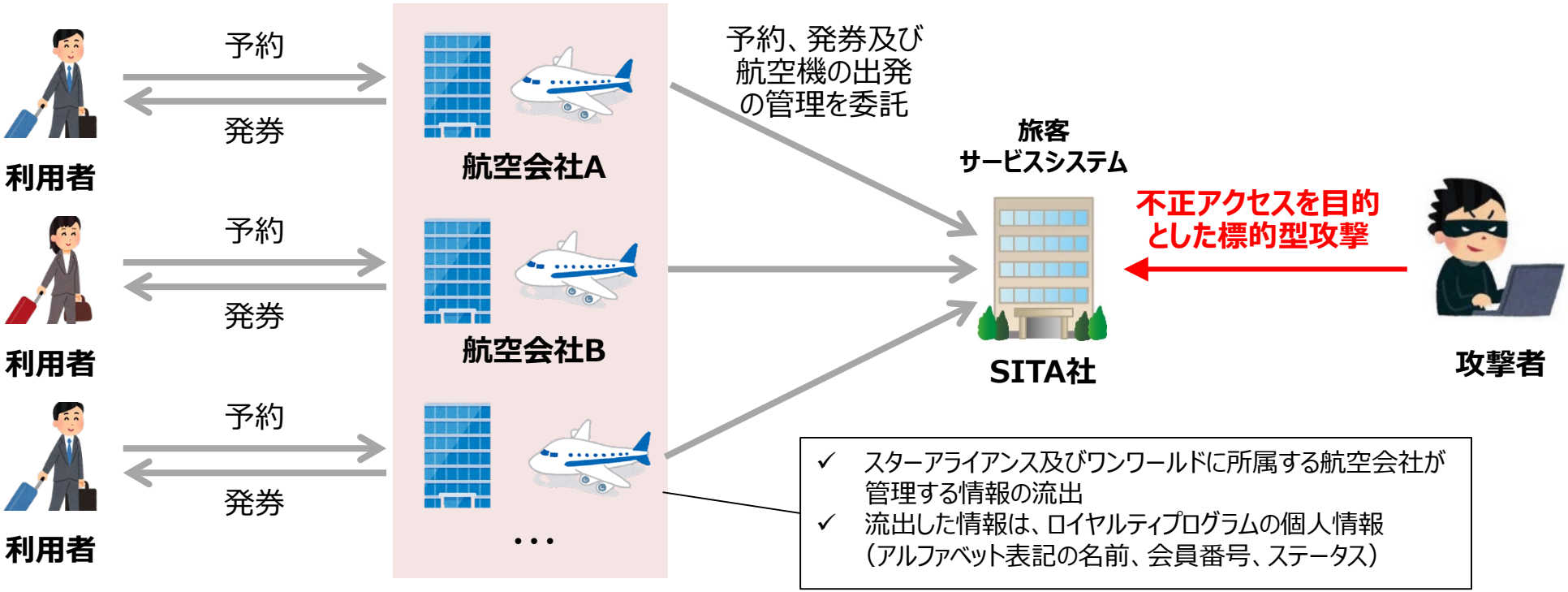
攻撃者



（出典）各種公開情報に基づき経済産業省作成

航空会社から委託を受けた企業における情報流出事例

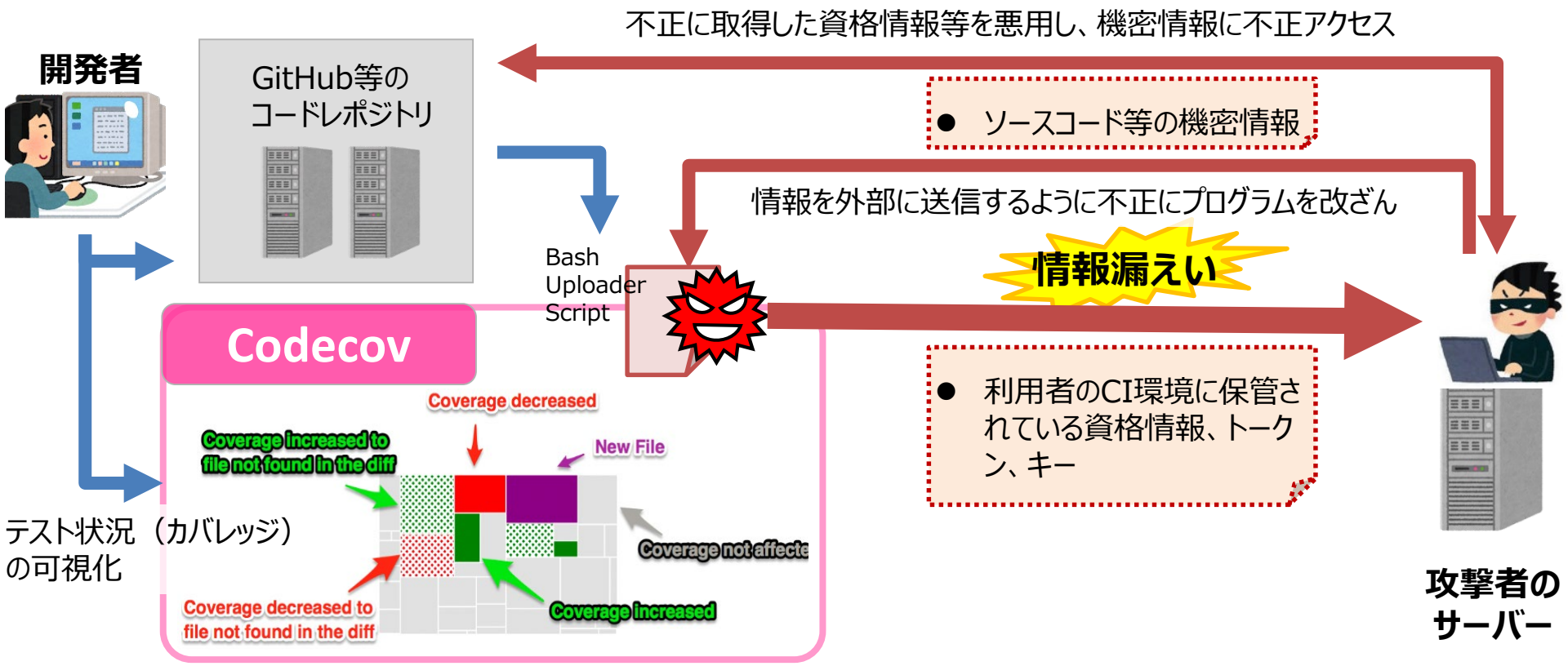
- サプライチェーンの中のある企業が標的型攻撃を受けることにより、被害が広範囲に広がる事例が増えている。
- 2021年2月、航空会社の旅客サービスシステムを提供する**SITA社（本社：ジュネーブ）が標的型攻撃を受け、**ANAやJALなどの日系企業を含む、**世界中の航空会社が保有する個人情報が流出**した。なお、SITA社は世界の航空会社の90%にサービスを提供しているとされる。
- 全体では約3000万件、このうちANAでは約100万件、JALでは約92万件の会員情報が流出したとされる。



（出典）各種公開情報より作成

ソフトウェア開発のテスト支援ツール”Codecov”にバックドア

- “Codecov”は、世界中で2.9万の組織、100万人以上に利用される（2021年4月時点）CI/CD(継続的インテグレーション／継続的デリバリー)を実現するためのテスト支援ツール。ソースコードのテスト状況を可視化する。
- 2021年4月、Codecovに含まれるBash Uploader Scriptが不正に書き換えられ、**利用者の資格情報等が不正に外部に送信され、ソースコードなどの機密情報が漏えいするリスクがある**ことが利用者指摘により発覚。
- Bash Uploader Scriptが書き換えられていた可能性があるのは、2021年1月31日～2021年4月1日の期間であり、国内でも**不正取得された資格情報等を悪用したソースコードや顧客情報の漏えい事案**が確認されている。



https://about.codecov.io/security-update/

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

国家のサイバーセキュリティの改善に係る米国大統領令の署名

- 2021年5月12日、バイデン大統領は、連邦政府機関におけるサイバーセキュリティ改善に係る大統領令に署名。
- **官民での脅威情報の共有**、**ソフトウェアサプライチェーンセキュリティ対策**の強化、**ゼロトラストアーキテクチャ**への移行等を通じて、連邦政府機関のサイバーセキュリティ対応能力の向上を図っている。

本大統領令における主な指示事項

1 **官民の脅威情報共有における障害の除去** (Section 2)	● ITサービスプロバイダーが連邦政府と確実に脅威情報を共有できるようにした上で、特定のインシデント情報の共有を義務づける。
2 **連邦政府におけるより強力な標準の近代化と導入** (Section 3)	● FedRAMP改定等を通じて、**連邦政府が安全なクラウド及びゼロトラストアーキテクチャに移行することを支援**し、多要素認証と暗号化の導入を義務づける。
3 **ソフトウェア・サプライチェーンのセキュリティ向上** (Section 4)	● NISTを通じて**政府が調達するソフトウェアの開発に関するセキュリティ基準(安全な開発環境の確保や構成要素に関する詳細（SBOM）の開示等を含む)を確立**し、特に**重要なソフトウェアに対して一定の対策を義務づけ**る。 ● 商務省は、既存のラベル表示などを参考にして、消費者向けの情報提供に関するパイロット制度を開始する。
4 **サイバー安全審査委員会の創設** (Section 5)	● 国土安全保障省は、**重大なインシデントが生じた際に政府と民間事業者が共同議長を務める「サイバー安全審査委員会」を設置**し、サイバーセキュリティ向上に向けた具体的な提言を行う権限を与える。
5 **インシデント対応のための標準プレイブックの策定** (Section 6, 7)	● 国土安全保障省は、連邦政府機関によるインシデント対応のためのプレイブックを策定する。 ● 連邦政府機関は、エンドポイント検知・対応(EDR)イニシアチブを展開し、インシデントの検知、積極的なサイバーハンティング、有事対応をサポートする。
6 **調査及び修復能力の向上** (Section 8)	● 連邦政府機関に対してセキュリティイベントログの要件を設け、侵入を検知し、対処する組織能力の向上を支援する。

（出典）各種公開情報より作成

新欧州サイバーセキュリティ戦略

- 2021年3月、欧州理事会は、EU加盟国を適用対象にサイバー脅威へレジリエンスの強化、デジタルサービスの信頼性確保、国際標準化のリーダー的地位の構築を目指した新欧州サイバーセキュリティ戦略を採択した。（草案は2020年12月公表）

達成すべき目的
欧州市民の安全保障/基本的権利・自由に対するリスクに対処するための強力なガードレールを備えた、グローバルかつオープンなインターネットを確保すること

上記の目的を達成するため、以下の行動分野に対して、規制、投資、政策手段という3つの方法でアプローチ

レジリエンス、技術的主権、リーダーシップ

- **ネットワーク・情報システム（NIS）指令の改正**
- セキュアなIoTのための規制措置
- CCCNを通じ、2021年から2027年の間に官民合わせて最大45億ユーロの投資を実施
- **AI活用SOC及び量子技術を利用した超安全な通信インフラに関するEUレベルでのネットワーク**
- **中小企業への献身的な支援を通じたサイバーセキュリティ技術の普及**
- インターネットアクセスのための安全でオープンな代替手段としてのEU DNSリゾルバサービスの開発
- 2021年の第2四半期までの5Gツールボックスの適用完了

予防、抑止、対応のための運用能力の構築

- **サイバーセキュリティ危機管理の枠組みを完成させ、共同サイバーユニット設立のためのプロセス、マイルストーン、タイムラインを決定**
- 安全保障戦略の下でのサイバー犯罪アジェンダの実施を継続
- 加盟国のサイバー情報作業部会の設立を奨励、促進
- 悪意ある活動を予防、抑止、対応するためのEUのサイバー抑止態勢推進
- **サイバー防衛政策の枠組み見直し**
- EU「作戦領域としてのサイバー空間に関する軍事ビジョンと戦略」の策定促進
- 民間、防衛、宇宙産業間の相乗効果を支援
- 重要な宇宙インフラのサイバーセキュリティを強化

グローバルで開かれたサイバー空間の推進

- 国際標準化プロセスにおける一連の目標を定義し、国際レベルで推進する。
- サイバー空間における国際的な安全保障と安定を促進
- サイバー空間における人権と基本的自由の適用に関するガイダンスを提供
- 子どもを性的虐待等から保護するとともに、子どもの権利に関する戦略を策定
- ブダペスト条約の第二追加議定書の作業を含む、サイバー犯罪に関するブダペスト条約の強化、促進
- 非公式のEUサイバー外交ネットワークを含む、第三国、地域、国際機関とのEUサイバー対話の拡大
- マルチステークホルダー・コミュニティとの交流強化
- EU対外サイバー能力構築アジェンダおよびEUサイバー能力構築委員会の提案

（出典）各種公開情報より作成　※ 赤字で協調しているイニシアチブは同戦略のプレスリリース中にて直接的に言及されているもの

欧州ePrivacy規則

- ePrivacy規則は、 GDPRの特別法と位置づけられており、域内における制度・運用の不統一を解消することを目的として、現行の**ePrivacy「指令」を「規則」に引き上げ、執行及び制裁を大幅に強化**するものであり、策定へ向けたプロセスが進んできた。
- 2019年12月に欧州理事会常任委員会（COREPER）にて同ドラフトが否決されたものの、**2021年3月規則案が欧州理事会にて合意**された。

ePrivacy規則 策定に係るこれまでのプロセス

2017年1月 欧州委員会がePrivacy規則ドラフトを発表

2017年10月 欧州議会LIBE(市民的自由・司法・内務委員会)で修正採択

2018年5月 欧州一般データ保護規則(GDPR)施行

2019年9月 欧州理事会議長が、ePrivacy規則の修正版ドラフトを発表

2019年12月 欧州理事会常任委員会（COREPER）が同ドラフトを否決

電子通信メタデータやクッキー等の技術により収集した情報の取り扱い（例：取り扱い可能な法的根拠、犯罪防止等を目的とした使用などの例外規定）が争点となっていた

2020年2月 欧州理事会が ePrivacy規則案（改訂版）を公表

2021年3月 **欧州理事会で ePrivacy規則案が合意**

ePrivacy規則案の主なポイント

規制対象	● 電子通信サービスに関連して実行される電子通信コンテンツ及び電子通信メタデータの処理 ● エンドユーザーの端末機器情報(例：クッキー) ● 電子通信サービスのユーザーの公開ディレクトリ提供 ● エンドユーザーへのダイレクトマーケティング
地理的な適用範囲	● 域外適用あり(処理の場所や事業者の所在地を問わない)
通信データの保護	● 「電気通信コンテンツ」(通信されるデータそのもの)と「電気通信メタデータ」(コンテンツの通信のために処理される日時・種類等のデータ)の秘密性を規定
クッキーの取扱い	● 同意を得ている場合や、要求されるサービスの提供に必要がある場合等の例外を除いて原則として禁止
ダイレクトマーケティングの実施	● 原則としてエンドユーザーの同意を得る必要がある
ブラウザ等による本人同意	● **ブラウザ／アプリの設定によるクッキー設定等への同意を有効な同意と認める。**ただし、利用者が直接表明した同意は、ソフトウェアの設定に優先する
執行と制裁	● **違反した条項に応じて、下記いずれかが適用**される。 - 1000万ユーロ以下、又は前会計年度の全世界年間売上高の2%以下のいずれか高い方 - 2000万ユーロ以下、又は前会計年度の全世界年間売上高の4%以下のいずれか高い方

（出典）各種公開情報より作成

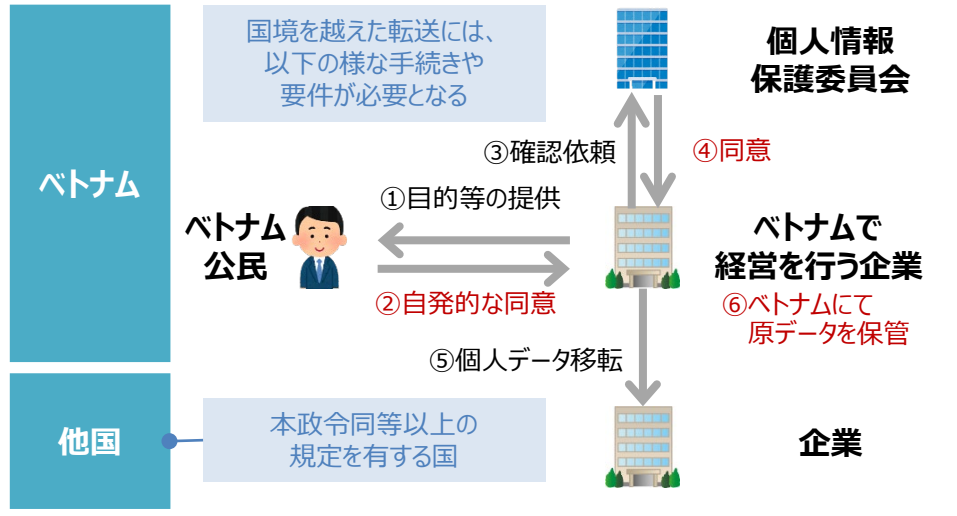
ベトナムの個人情報保護に関する政令草案

- 2021年4月を締め切りとして意見募集された個人情報保護に関する政令草案は、ベトナムで経営活動を行う国内外全ての組織、企業、個人を適用対象に、ベトナム公民の個人情報を保護することをすることを目的とした法令である（2021年12月1日施行予定）。
- **機微な個人情報を取り扱う場合にはベトナム個人情報保護員会への登録**や、個人情報を取り扱う場合には本人同意が必要になる他、**ベトナム公民の個人情報を越境移転する場合には、ベトナム個人情報保護委員会の同意が必要となる**。
- 違反が複数回に及び被害が大きい場合にはベトナムでの売り上げの最大5%の罰金が科されるなど、厳しい罰則を設けている。

個人情報保護に関する政令草案の目次

章	目次
1	一般規定
2	個人データの処理
3	**個人データの保護措置**
4	個人データ保護委員会
5	機関、組織、個人の責任
6	実施規定

第21条 個人データの国境を越えた転送



（出典）各種公開情報より作成

中国における主なデータ保護関連法規

- 中国では、2017年6月のサイバーセキュリティ法施行を皮切りに、サイバーセキュリティ審査弁法や自動車データ安全管理規定等の付随規定が盛んに策定されていることに加え、特に2020年以降、同法とともにデータ管理の法的枠組みを構成するデータセキュリティ法、個人情報保護法の検討が進んでいる。

2017年6月施行

中国サイバーセキュリティ法
[中华人民共和国网络安全法]

- 国家の安全保障を目的として、個人情報の保護、機密情報の保全、国外へのデータ移転規制、セキュリティ製品の認証、法的責任と罰則等について規定
- 同法は内容が原則的であり、詳細は下位の法令(右記)にて明確化する見込み

個人情報域外持出安全評価弁法 **2019年3月改訂草案公表**

- 中国国内で収集した個人情報及び重要データを国外へ移転する際に実施する安全評価の具体的な要求及び手順を規定

サイバーセキュリティ審査弁法 **2020年6月施行**

- 重要情報インフラ事業者が特定のIT製品・サービスを調達する際に、国が実施する審査に係る申請手続等を規定

自動車データ安全管理規定 **2021年5月草案公表**

- 自動車産業に関連する個人情報及び重要データについて、国内保存の義務づけ、国外移転時の国による安全評価等を規定

⋮

2021年6月成立、9月施行予定

データセキュリティ法
[中华人民共和国数据安全法]

- 中国国内におけるデータの収集、保存、加工、使用、提供、取引、公開等の行為(データ処理活動)に関連して、政府によるデータ分類・等級分類及び重要データ管理に関する制度の構築、事業者のデータセキュリティ保護に係る義務等を規定
- 2020年7月に初案公開された後、2021年5月に第2次審議稿を公表、2021年6月に成立

2021年5月第2次審議稿公表

個人情報保護法
[中华人民共和国个人信息保护法]

- 個人情報に関する権利利益を保護しつつ合理的な利用を促進するため、個人情報の処理や越境移転に係る規則、個人が行使できる権利等を規定
- 2020年10月に初案が公開された後、2021年5月に第2次審議稿を公表

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

タスクフォースの検討の方向性（第3回TF資料再掲）

- **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

データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク

- これまでのタスクフォースでの議論を踏まえて拡張したデータマネジメントの捉え方を用いた「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮題）」の骨子案を作成。
- 第4回タスクフォースでは、フレームワーク骨子の内容およびフレームワーク策定に向けた進め方についてご議論いただきたい。

＜目次＞

フレームワーク骨子案の概要：第3層の位置づけ

- 第3層においては**データが信頼性の基点**
  - Society 5.0において、サイバー空間におけるつながりが展開される場が第3層であり、そこでは物理特性に依存しないデータが付加価値を創造（バリュークリエイション）している。
  - データは基本的にシステムや組織に対して中立性を持つものであり、それが求められる規範等に則って適切に扱われることによって、自由に流通・活用される。
- データのライフサイクルには**様々な主体が関与**
  - 関与した主体による不適切な措置によって誤ったデータが流通し活用されることになれば、有害な結果をもたらすことにもつながりかねない。
- **データのライフサイクルは第3層の中に閉じるものではない。**
  - サイバー空間から発信されたIoTシステムへの動作指令が誤った内容であるならば、第2層における“転写”する機能の信頼性を確保することに成功していたとしても、IoTシステムはサイバー空間から届いた誤った指令を“正しく”転写して忠実に動作することで物理的な損害を発生させてしまうかもしれない。
  - データが生成される場所については第3層ではなく第2層に属する場合があり、第3層と第2層とを組み合わせることでデータ生成における信頼性が確保できる。（第2層TFで策定したIoT-SSFと連動）

フレームワーク骨子案の概要：データマネジメントの考え方の確立

＜データマネジメントの捉え方＞

- **データのライフサイクルの各工程において発生する様々な形の“関与”**

＜３つの視点＞

① データマネジメントについて確立した定義は存在しない

- 他の機関等において整理されたデータマネジメントの定義を持ち込むのではなく、CPSFを基礎としてセキュリティ対策を検討するために必要なデータマネジメントの考え方を示す。

② データを軸に置く

- データがライフサイクルの各工程においてどのような関与を受けるかという視点で整理すべき。

③ 関与する主体は同一・単一の主体に限られるものではない

- データマネジメントは複数の主体による協同的活動**（Collective Action）になる**ことを排除しない。例：クラウドサービス

フレームワーク骨子案の概要：本フレームワークの目的・想定読者

＜ 本フレームワークの目的 ＞

（as isの対策）

- データを軸に置き、**データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、**そのセキュリティを確保するために、ガバナンスを含めた必要な措置を**ステークホルダーが協調して実施する**。
- 洗い出されたリスクへの措置はDMBOK等の既存文書を参照。

（to beの対策）

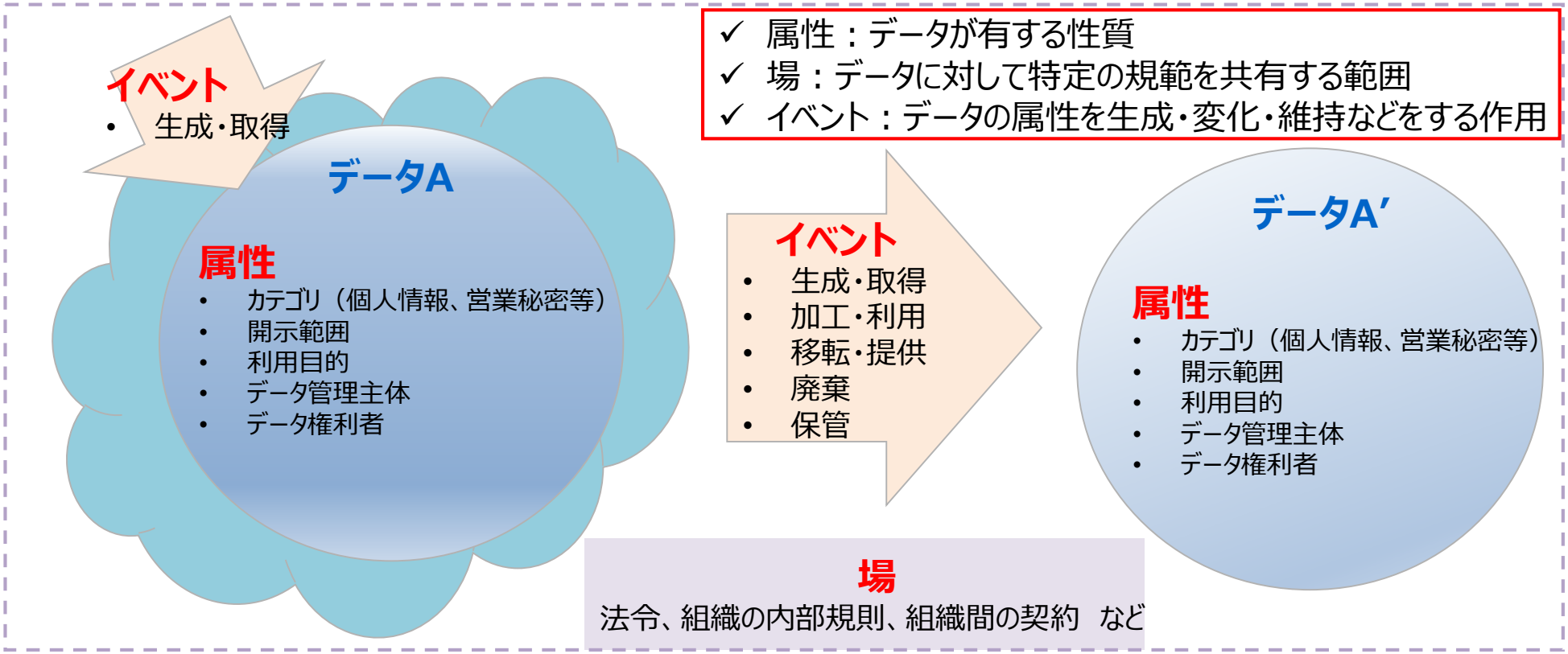
- データの流通を促進するために必要な条件を明確化。プロトコルの設計が容易に。
- 強い立場にあるシステムが**プロトコルのブラックボックス化によって「バンドル」することを難しく**させ、**オープン化された環境でデータ連携やシステムの組み合わせの自由を確保することを可能に**。
- 主体の在り方などを過度に考慮することなく、データに対して本来求められる要求事項を歪めることなく整理することが可能であり、**各国の制度間のギャップ分析**を行い必要な調整措置を明らかに。

＜ 本フレームワークの想定読者 ＞

- バリュークリエイションプロセスに参加する者
- データ交換のプラットフォームサービスを提供する者
- データ交換プラットフォームとなるシステムの設計・構築・運用に関わる者
- トラストサービスを提供しようとする者
- データセキュリティに関わるガイドライン等のルール設定に関わる者

フレームワーク骨子案の概要：データマネジメントのモデル化の概要

- データマネジメントを「**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**」と定義。
- **「属性」「場」「イベント」の3つの要素はそれぞれが相互に影響**しあう関係。
- データの遷移による**データの変化に関する一定の予見可能性を確保、ステークホルダーの間で認識を共有しやすく**なる。
- 共通の理解に基づいてそれぞれの主体が実施すべき措置についての検討を進めることが可能となり、**ステークホルダー全体で適切なデータマネジメントを実施していくことができる環境を実現**していく。



フレームワーク骨子案の概要：リスク分析手順

- **下記の4つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化**。
- 「属性」、「場」、「イベント」が相互に依存する関係にあることから、STEP1～3の**各ステップは不可逆的なものではなく、互いにフィードバックをかけながら検討されることが適切**。
- リスクの洗い出しに当たっては、機密性・完全性・可用性といったサイバーセキュリティに係る観点の他、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す必要。

STEP 1
データ処理フロー（「イベント」）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

フレームワーク骨子案の概要：モデル化（「イベント」）～ 生成・取得、加工・利用 ～

- データの属性を生成・変化・維持などをする作用である「イベント」に関しては、**大きくは「生成・取得」「加工・利用」「移転・提供」「保管」「廃棄」の5つに区分することが可能**。
- 5つの「イベント」はそれぞれ重複する性質を持つ場合があり、目的に応じて適切に「イベント」を捉え、リスクの洗い出しを実施する必要（例：閲覧は加工・利用だが移転・提供の要素を含み得る）。

＜ 生成・取得 ＞

- バリュークリエイションプロセスにおいて、サイバー空間でやりとりされるデータは、**何らかの形で生成・取得されることによってそのライフサイクルが始まる**。
- サイバー空間とフィジカル空間が高度に融合し、フィジカル空間の情報が大量にサイバー空間に転写され、リアルタイムに共有されるようになると、サイバー空間のつながりにおけるデータの信頼性を検討する場合、従来はデータを管理する範疇に捉えられていなかった、**データの生成・取得に関わる機器・システムなどの信頼性についても検討する必要**。
  - 代表的なリスク：計測結果が実際と異なる、計測機器をなりすまされる等の転写の失敗など。

＜ 加工・利用 ＞

- データに**付加価値を生み出すための作用を加工・利用と捉える**。
  - ✓ 分析過程や保管されたデータセットから**データの一部の項目や要素、レコードなどを取り除く作用については、加工の一形態として捉える**ものとし、後述する廃棄とは区別する。
  - ✓ データを保有しない者が**データにアクセスする作用（閲覧）については、利用の一形態として捉える**ことが適切であるが、リスクを洗い出す際は**移転的な要素を考慮**に入れる必要。
  - 代表的なリスク：データの目的外利用、不適切な加工など。

フレームワーク骨子案の概要：モデル化（「イベント」）～ 移転・提供 ～

＜ 移転・提供 ＞

- サプライチェーンを動的に構成する場合、効果を最大限に引き出すためには**より自由にデータの移転・提供を実施できる環境にすること**、**リスクに対してより効果的に対応すること**が求められる。
- 特定の移転・提供事象について、国・地域、組織・ヒト、システム・サービス、機器という**4つの単位で整理**。
- **イベントをどの程度詳細に記述するかは、データフローの整理の目的に応じて調整する必要**。

単位	考慮すべき事項	単位ごとのリスク(例)
国・地域	データの移転・提供に関連する国・地域及び、当該国・地域におけるデータ保護関連の政策、法令、ガイドライン等	● データの移転元/移転先に相当する国・地域にデータ保護関連法令が存在しない又は内容として不十分な場合、移転元/移転先間における保護水準の不整合が生じる結果、移転先で移転元の保護水準が確保できない。
組織・ヒト	データの移転・提供の関係主体となる組織及びヒト、当該主体におけるデータ保護関連の方針、体制等	● 組織のセキュリティポリシーが存在しない又は内容として不十分な場合、データ移転に関わるステークホルダ間にてセキュリティ水準の不整合が生じる結果、移転先で移転元の保護水準が確保できない。
システム・サービス	複数の機器から構成され、データの移転・提供を実行するシステムと提供されるサービス	● システム・サービスにおけるセキュリティ実装が十分でないことにより以下のようなセキュリティ上のリスクが生じうる。 - ネットワーク上での盗聴 - 送信元/送信先のなりすまし
機器	データの移転・提供を実行するサーバ、IoT機器、ネットワーク機器等のデータを物理的に取り扱う単体のシステムコンポーネント	● 機器におけるセキュリティ実装が十分でないことにより以下のようなセキュリティ上のリスクが生じうる。 - 機器内の不正なコンポーネントを通じた意図しないデータ移転 - DDoS攻撃等のサービス拒否攻撃による機器の稼働停止

フレームワーク骨子案の概要：モデル化（「イベント」）～ 保管、廃棄 ～

＜ 保管 ＞

- **保管は、他のイベントに付随して必ず生じる「イベント」**である。データはライフサイクルの様々な段階において、ネットワークに接続されたストレージ機器・サービスやクライアントのハードディスク、USBメモリのような可搬媒体や、機器の一時記憶領域等に保管され得る。
- データの取扱に関してリスクを洗い出し、セキュリティ対策を検討する上では、**移転・提供、加工・利用されるデータとは異なるリスクが生じうる**ことから、「イベント」の一類型として整理し、リスクの洗い出しを実施することが適切。

＜ 廃棄 ＞

- 本フレームワークにおける**廃棄は、データセット全体について、完全に、使用不可能な状態とすること**を指す。
- 同意に基づいて収集したパーソナルデータに関して、特定の個人が同意を撤回する等により、当該個人のデータをデータセットから除外する行為は、加工・利用の一形態として捉えるのが適切。
  - 代表的なリスク：廃棄すべきデータが残存して漏えいする、本来は廃棄すべきでないデータまで廃棄してしまうなど。

フレームワーク骨子案の概要：モデル化（「場」）

- 「場」の設定は個別の事情によるところが大きく、一律に設定方法を提示することは困難。
- 例えば、「場」を構成する重要な要素の一つに法令等があるが、**「場」の設定を行うに当たって、必要な観点を漏らすリスクを低減**しながら検討するために、**下記のような4つのカテゴリから整理**。
- 4つのカテゴリは、「場」が、データに関して何らかの共通の取扱を求める法令等と連動して設定されることを背景に、**データに共通の取扱を求める目的としてはどのようなものが考えられるか、という観点から整理**。

- **パーソナルデータの保護**
  - 「場」の例：個人情報保護法（日本）、GDPR（欧州関係）、個人情報を取得する際に当該個人が同意した利用目的
  - 規定される「属性」の例：カテゴリ（個人情報、匿名加工情報）、データ権利者、データ管理主体
- **知的財産・営業秘密保護**
  - 「場」の例：不正競争防止法、著作権法、主体間の契約（NDA等）
  - 規定される「属性」の例：カテゴリ（営業秘密、限定提供データ）、開示範囲、データ権利者
- **機微技術管理**
  - 「場」の例：外為法、米国輸出管理規則
  - 規定される「属性」の例：カテゴリ（輸出管理等対象技術）、開示範囲、データ管理主体
- **適切な社会機能の維持**
  - 「場」の例：金融商品取引法（インサイダー取引）、各種守秘義務関係
  - 規定される「属性」の例：開示範囲

フレームワーク骨子案の概要：モデル化（「属性」）

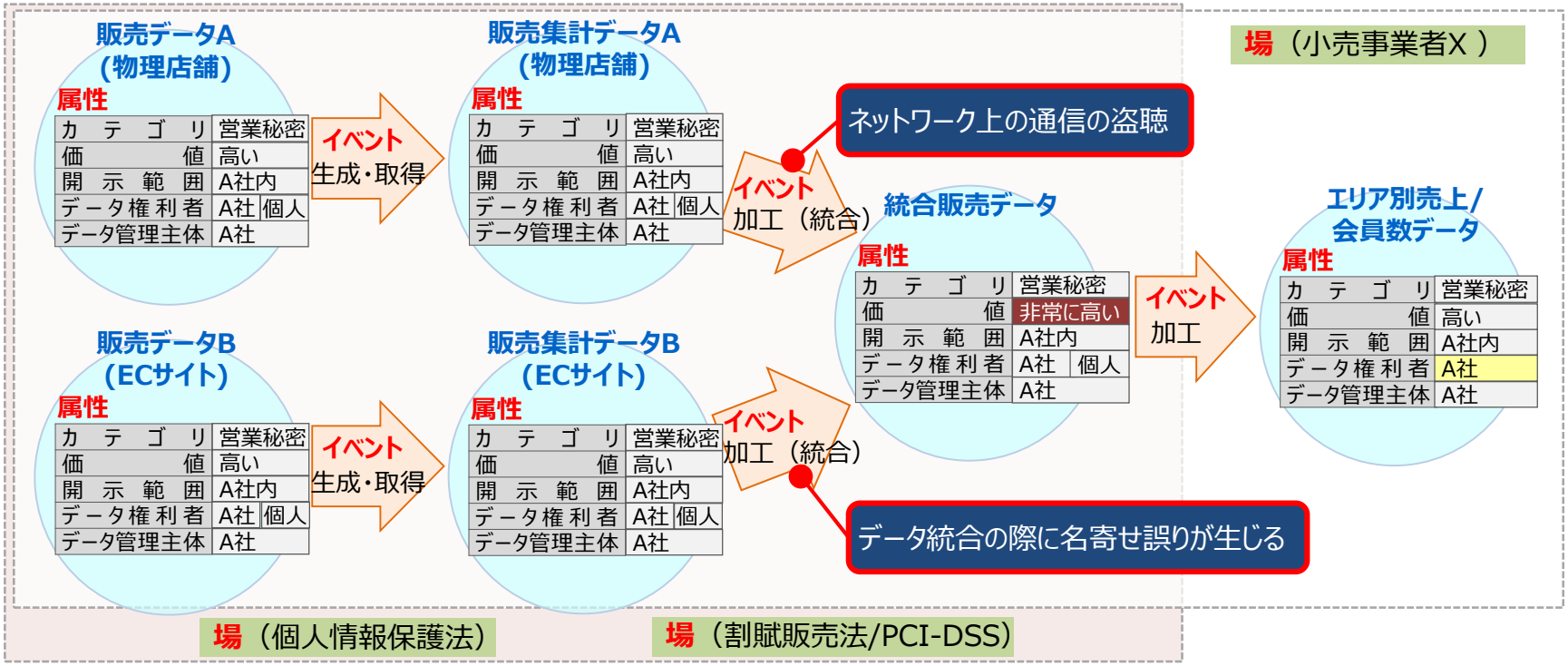
- 代表的な「属性」やパラメータ、整理のポイントを示す。
- 整理した「場」からデータに対する要求を検討し、関連する「属性」を適切に具体化することが重要。

- **<u>カテゴリ</u>**
  - 特に「場」と連動して、データに対して特別な作用（「イベント」）を求める場合（個人情報・匿名加工情報、営業秘密・限定提供データなど）、カテゴリとして法令等における位置づけを整理する。
- **<u>開示範囲</u>**
  - 民法上の契約や組織内規則も含め、データに定められている開示範囲を整理する。その際、組織内での取扱であっても、国・地域間での移転が伴う場合や、米国輸出管理法上のみなし輸出に該当する場合等、開示範囲の制限が複層的に適用される可能性がある点に留意。
- **<u>利用目的</u>**
  - 個人情報やライセンスなど、法令等に基づいて利用目的に制限が設けられている場合、当該利用目的の範囲内で取り扱われる必要があることから、「属性」として明示しておく必要がある。
- **<u>データ管理主体</u>**
  - データに軸を置く本フレームワークにおいては、データに作用を及ぼす主体についても、データが転々流通する過程で移り変わるものであり、あくまで「属性」の一つとして整理する。
- **<u>データ権利者</u>**
  - データが個人情報である場合、企業の競争力に関わる場合など、データ管理主体とは別に、データに対して権利を有する主体が存在することがある。移転・提供が行われて別の主体がデータを取得した場合でも、データ権利者は当該主体の管理下にあるデータに対して引き続き権利を有すると考えられるため、管理主体が転々と移っていく過程でも、「属性」として管理する必要がある。

フレームワーク骨子案の概要：活用方法
～ サプライチェーンを構成するステークホルダー間での活用 ～

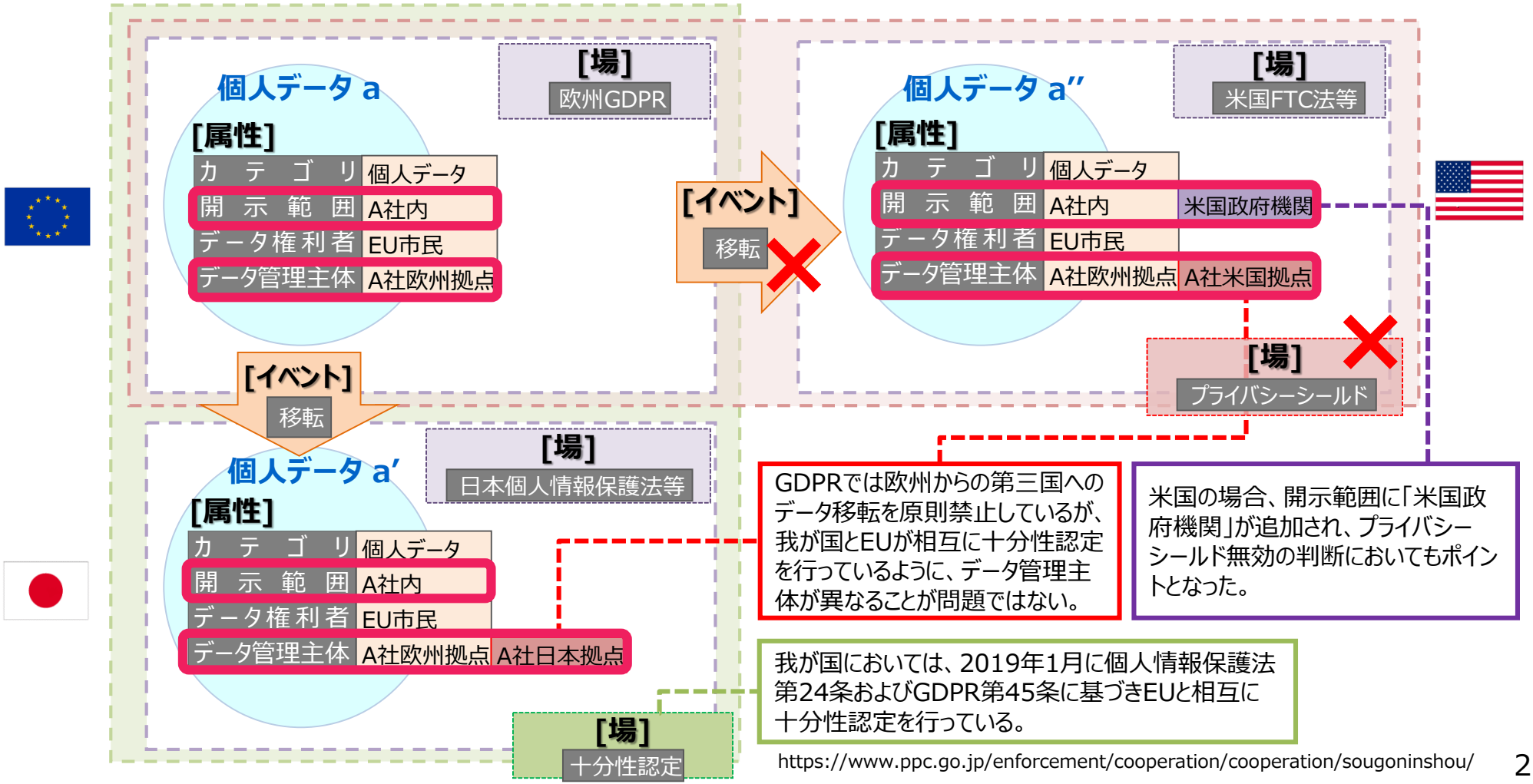
- バリュークリエイションプロセスに関わるステークホルダーの間で、データのライフサイクルの各工程においてリスクを可視化した上で、各主体がそれぞれ実施すべき対策を他の主体と合意形成しながら取り組むことにより、データの信頼性を確保することが期待される。
- 可視化されたリスクに対して各主体が実施すべきセキュリティ対策は、これまでに公表されてきた情報セキュリティに関する様々な国際標準等を参照。
- **将来的には経営者によるITガバナンス（デジタルガバナンス）の検討への活用も期待。**

小売業におけるPOSデータの活用事例



フレームワーク骨子案の概要：活用方法　～ルール間のギャップの分析 ～

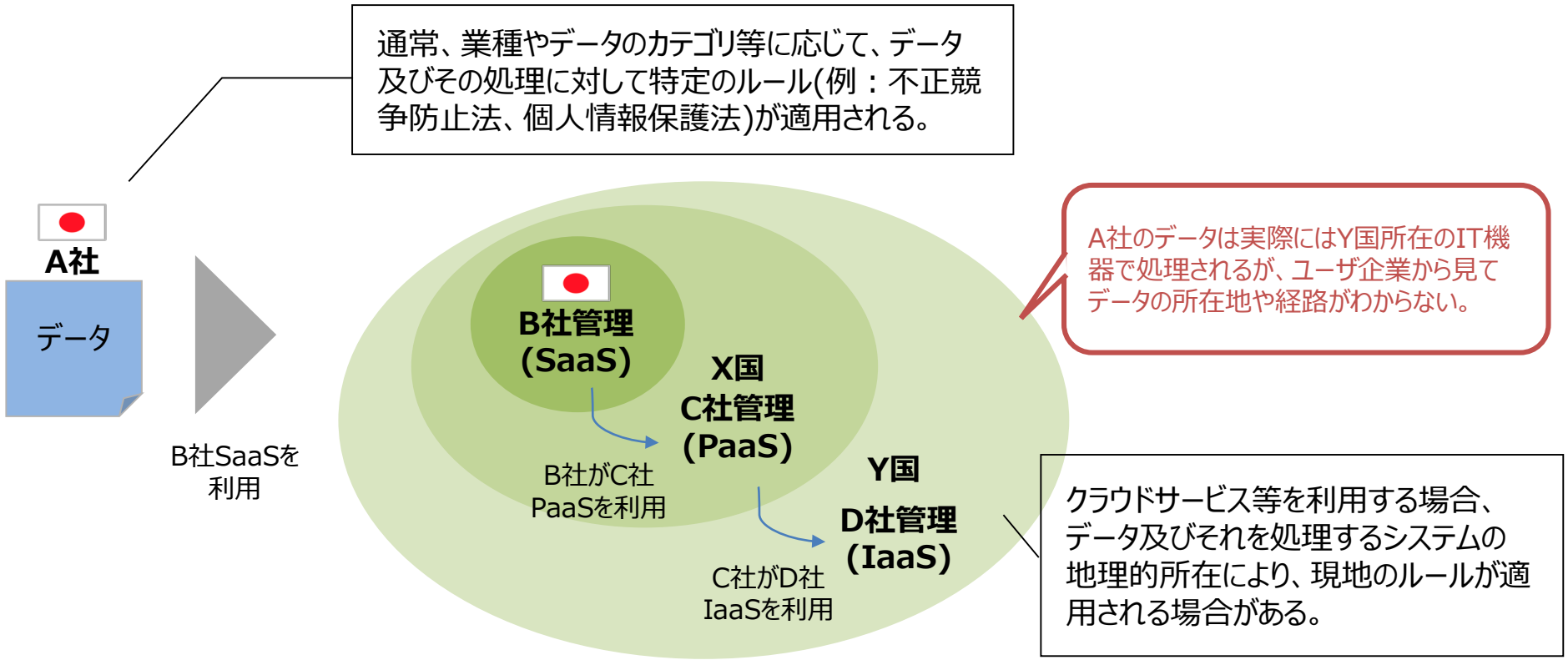
- 本フレームワークは、**データ管理に関わる制度間における、データのセキュリティの確保のために要求されている条件や措置の相違（ギャップ）を明確化するためのモデルとしての活用も可能**。
- データに関する**「場」や「属性」の変化を可視化することで、**データのセキュリティの確保のために**要求されている条件や措置の相違を把握**することにつながる。



https://www.ppc.go.jp/enforcement/cooperation/cooperation/sougoninshou/

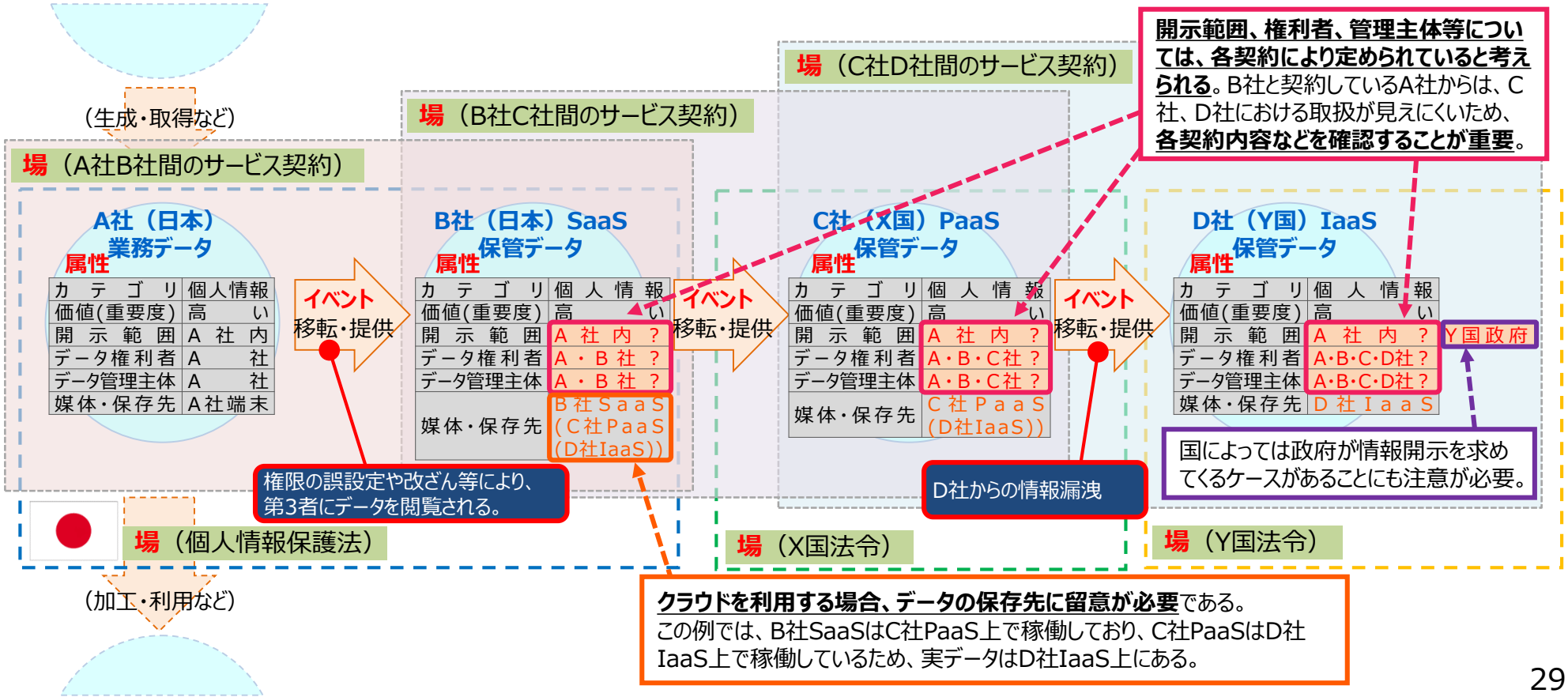
（参考）システム構成の多層化・重層化によるデータマネジメントの複雑化 ※第3回TF資料から一部修正

- 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。



（参考）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

- B社SaaSはC社PaaS上で、C社PaaSはD社IaaS上で稼働している場合等において、**A社がB社と契約してデータを保管する際**、A社から見たデータの保存先はB社SaaSだが、**実際のデータの保存先はD社IaaSとなり、A社・B社間の関係だけからは見えないリスクが内在**する。
- このような複雑なケースがあることを認識した上で、扱うデータの機微性等に応じてバリュークリエイションプロセスの**データフローを可視化し、サービス契約の約款や契約相手へ確認することが重要**。



特にご議論いただきたい内容

- 今後の進め方について、フレームワーク骨子案をパブリックコメントにかけることとしてよいか。
- 骨子案の2-2以降はパブリックコメントと並行して詳細化作業を進めるが、「場」を整理する際のカテゴリやフレームワークで例示すべき「属性」等について、ご意見をいただきたい。

フレームワーク骨子案について、特にご意見をいただきたい事項

- **「場」の設定にあたって参考となる4つのカテゴリ**を示しているが、リスクの洗い出しに必要な観点を漏れなく検討するにあたり、どのような整理が考えられるか。（P.24関係）
- フレームワークで代表例として示すべき**「属性」として、他にどのようなものがあるか**。（P.25関係）

今後の進め方（案）