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

令和元年12月17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わるセキュリティインシデント事例

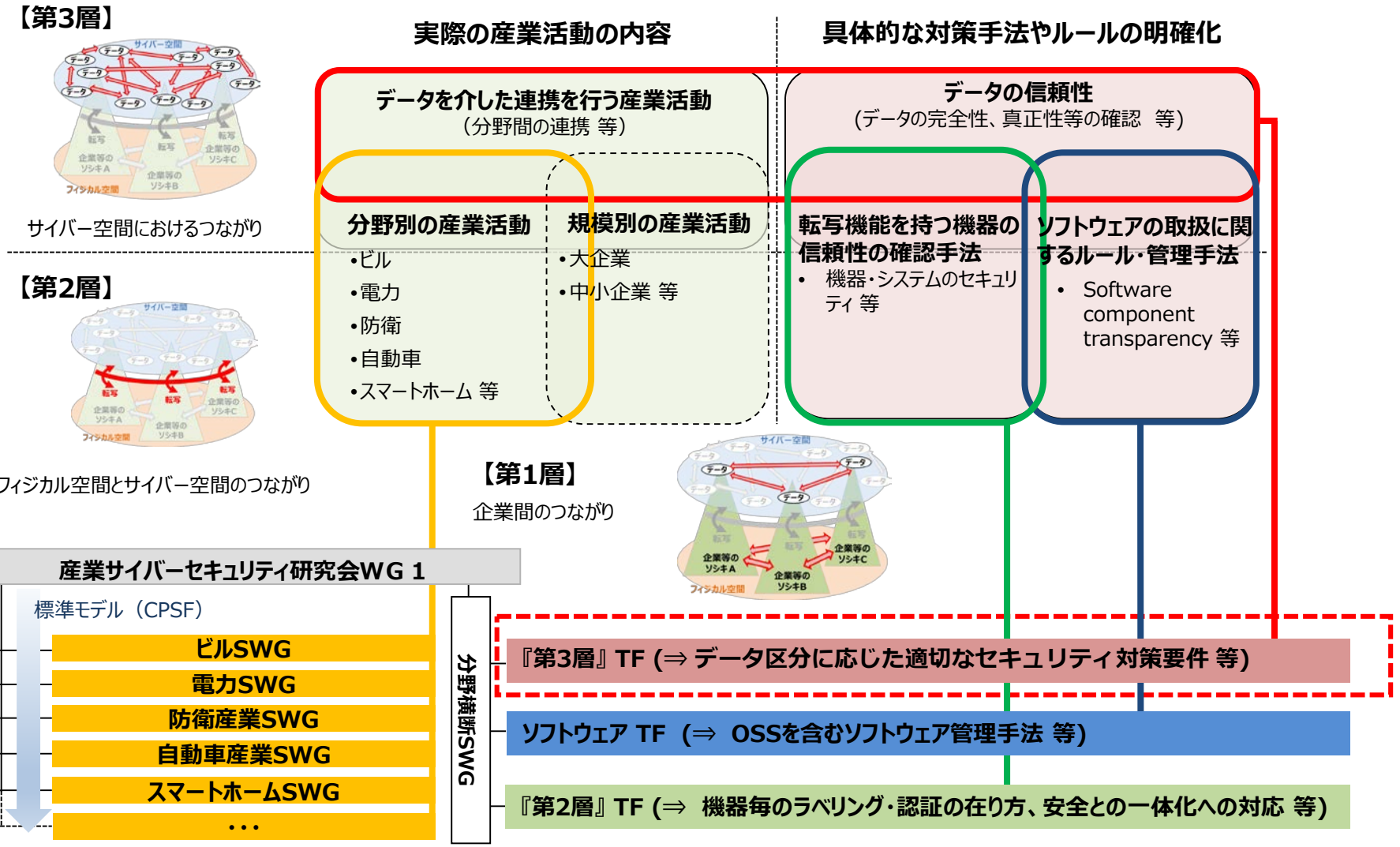
３．データを守るための海外の取組事例

４．データマネジメントに関する既存のフレームワーク等

５．本タスクフォースの検討事項

CPSFに基づくセキュリティ対策の具体化・実装の推進

- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）を新たに設置**。



テーマ別TFの検討状況

- CPSFに基づくセキュリティ対策の具体化・実装を推進するため、検討すべき項目ごとに焦点を絞った**タスクフォース（TF）を新たに設置**。

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
- 電力SWG
- 防衛産業SWG
- 自動車産業SWG
- スマートホームSWG
- ・・・

分野横断SWG

『第3層』TF

データの信頼性確保のために、データの区分に応じた適切なセキュリティ対策要件及びデータの信頼性の確認手法を検討する。
7/31の第１回TFでは、プライバシーを含むデータの属性やデータに対する処理、データを扱う場等によって要求されるセキュリティが異なり得ること等を議論。

ソフトウェア TF

ソフトウェア管理手法、脆弱性対応、OSSの利活用等について検討する。
9/5の第1回TFではSBOM等を用いたソフトウェア管理手法について、11/6の第2回TFでは脆弱性対応について、 12/4の第3回TFではOSSの利活用についてそれぞれ論点の洗い出しを行った。

『第2層』TF

サイバー・フィジカル間の転写機能を持つ機器等について、自己適合宣言・認証等の確認の在り方等を検討するとともに、産業保安・製品安全も考慮したセキュリティ対策の在り方について検討する。
8/2の第1回TF及び11/27の第2回TFでは、安全とセキュリティを併せて考えることの重要性や求められるセキュリティに応じて機器をカテゴライズする必要性等について議論。

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わるセキュリティインシデント事例

３．データを守るための海外の取組事例

４．データマネジメントに関する既存のフレームワーク等

５．本タスクフォースの検討事項

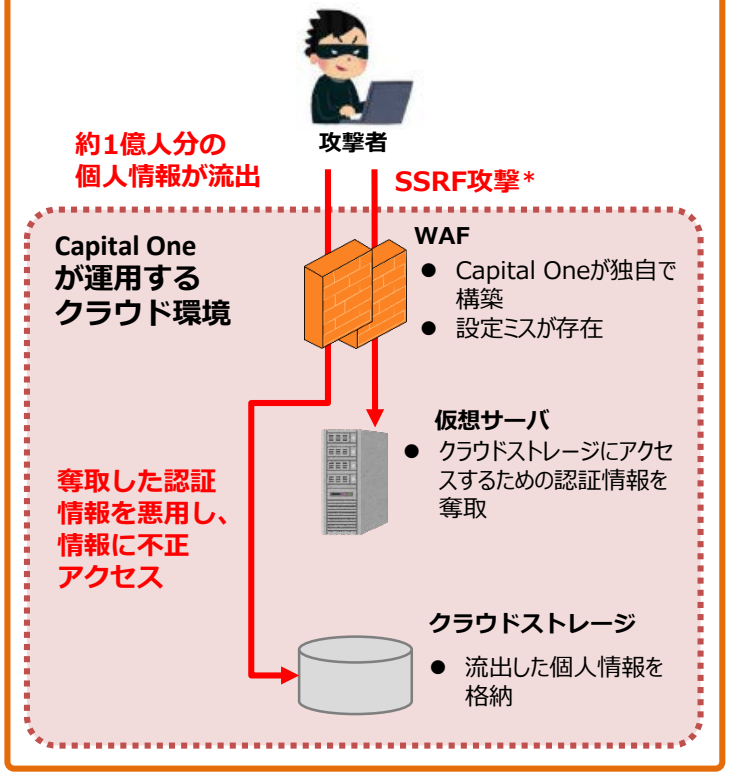
Capital One社における個人情報漏えい事例

- 2019年7月29日、**米国の金融大手Capital One は、不正アクセスにより1億人を超える個人情報**(クレジットカードへの申し込みをした消費者や中小企業の氏名/名称、住所、郵便番号、電話番号、メールアドレス等)**が流出したと発表**した。
- 原因の一つは、 Capital Oneがクラウド環境に独自で構築した**ウェブ・アプリケーション・ファイアウォール(WAF)の設定ミス**とされる。

本事例の詳細（原因・影響等）

- 2019年7月29日、米国の金融大手Capital One は、不正アクセスにより1億人を超える個人情報が流出したと発表した。
- 流出した情報は、クレジットカードへの申込みを行った消費者及び中小企業の氏名/名称、住所、郵便番号、電話番号、メールアドレス等で、クレジットカード番号、ログイン情報は含まれないとされる。
- Capital Oneがクラウド環境に独自で構築したウェブ・アプリケーション・ファイアウォール(WAF)の設定ミスにより、仮想サーバに割り当てられたクラウドストレージにアクセスするための認証情報を奪取されたことがインシデント発生の原因の一つとされる。
- 攻撃者は、奪取した認証情報を悪用し、個人情報を格納したクラウドストレージへアクセスした。そこから、外部アクセス可能なクラウドストレージにデータをコピーすることにより、結果的に約1億人分の個人情報を流出させた。
- 本件に関して、Capital Oneに加えて、漏えいしたデータがサイト上で公開されたGitHubも被告とした複数の集団代表訴訟(クラスアクション)が提起されている。

事例のイメージ



＊：Server Side Request Forgeryの略。公開サーバから内部のサーバにリクエストを送信することにより、内部のサーバを攻撃する手法。

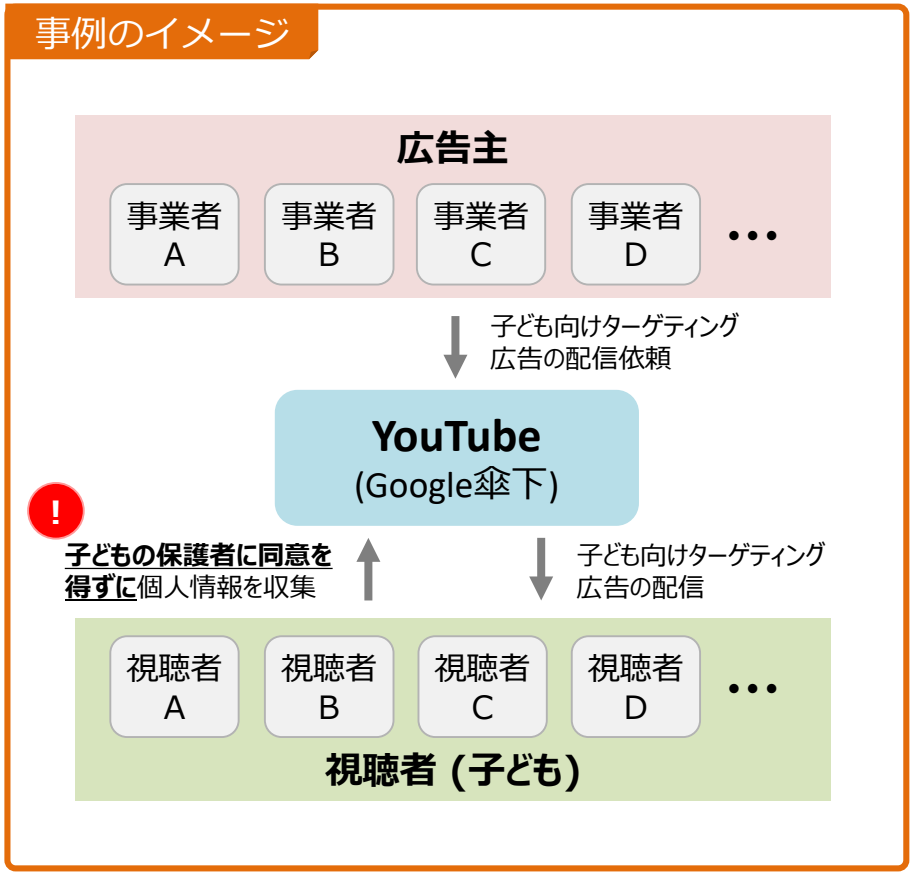
米国児童オンラインプライバシー保護法違反事例 (YouTube)

- 2019年9月4日に、**米国連邦取引委員会(FTC)は、Googleと傘下のYouTubeに、児童オンラインプライバシー保護法(COPPA)違反に対する和解金として1億7000万ドル(約180億円)を課すと発表**した。
- YouTube上の子ども向けチャンネルの視聴者(子ども)に対して、その**保護者に同意を得ずにクッキーを使い個人情報を収集していたことがCOPPA違反**とされた。

本事例の詳細（原因・影響等）

- YouTubeで配信されるチャンネルの内、COPPAの対象となる13歳未満の子どもが視聴する可能性が高いものについて、保護者に無断で子どもの個人情報を収集しマーケティングに利用している疑いが生じていた。
- 2018年4月に、子どもの人権やプライバシーの擁護に取り組む団体や消費者団体など20の団体がFTCに対し、YouTubeをCOPPA違反の疑いで捜査するよう求める請願書を共同で提出した。
- 上記を受けて、FTCとニューヨーク司法長官は、Googleと傘下のYouTubeが、子ども向けチャンネル視聴者に対して、保護者に同意を得ずにクッキーを使い個人情報を収集していたことをCOPPA違反と申し立てた。
- 2019年9月4日にFTCが発表した和解条件は、和解金1億7000万ドル(約180億円)の支払いと、子ども向けコンテンツ関係者向けのCOPPA順守トレーニング及び、COPPA対応に向けたシステム改善の実施である。

事例のイメージ



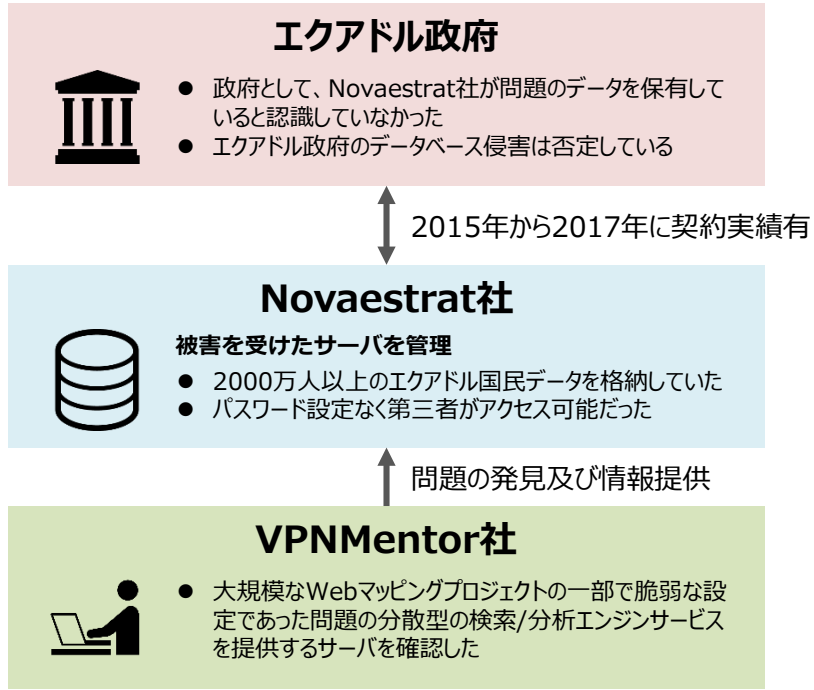
エクアドル全国民情報流出の可能性

- 2019年9月16日、VPNサービスのレビュー等を行うvpnMentorは、**エクアドル全国民分に相当する大量のデータがインターネット上で漏洩している疑いがあることを発表**した。
- 同国のコンサルティング企業が、検索/分析エンジンサービスを提供するサーバを、**パスワードなしで誰でもデータにアクセスできる状態にしていたことが原因**とされる。

本事例の詳細（原因・影響等）

- 2019年9月16日、エクアドル政府は、同国民2000万人超(故人を含む)の情報が流出した疑いがあることを明らかにした。
- サーバに保存されていたデータには、エクアドル国民2000万人超の個人情報のほか、750万件の金融関連の情報や250万件の自動車の所有者情報が含まれていた。
- Novaestrat社と呼ばれる同国のコンサルティング企業が、分散型の検索/分析エンジンサービスを提供するサーバを、パスワードなしで誰でもデータにアクセスできる状態にしていたことが原因とされている。
- 2015年から2017年にかけて、エクアドル政府は、複数の契約を同社との間で結んでいたが、同社が流出の疑われる当該データを保有する契約ではなかった。

事例のイメージ



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わるセキュリティインシデント事例

３．データを守るための海外の取組事例

４．データマネジメントに関する既存のフレームワーク等

５．本タスクフォースの検討事項

【米国における取組事例①】
NIST SP800-171 のアップデート及びSP 800-171Bの策定

- 2019年6月に、**SP 800-171の第2版(ドラフト)と、重要性の高いプログラムや価値の高い資産で扱われるCUIを高度な標的型攻撃から保護する追加の対策を示すSP 800-171B(ドラフト)が公開**された。
- SP 800-171 第2版(ドラフト)では、110項目のセキュリティ要件は変更されていないが、使いやすさ向上のために、付録Fに記載されていたディスカッションセクションが、セキュリティ要件に併記される形となっている。

SP 800-171及び関連文書の策定状況

SP 800-171 Rev. 2 (2019年6月 ドラフト公開)
連邦政府外のシステムと組織における管理された非格付け情報(CUI)の保護

- 対策要件は変更されていないが、付録Fに記載されていたディスカッションがセキュリティ要件に併記される形となった。

SP 800-171A (2018年6月 公開)
管理された非格付け情報向けセキュリティ要件の評価

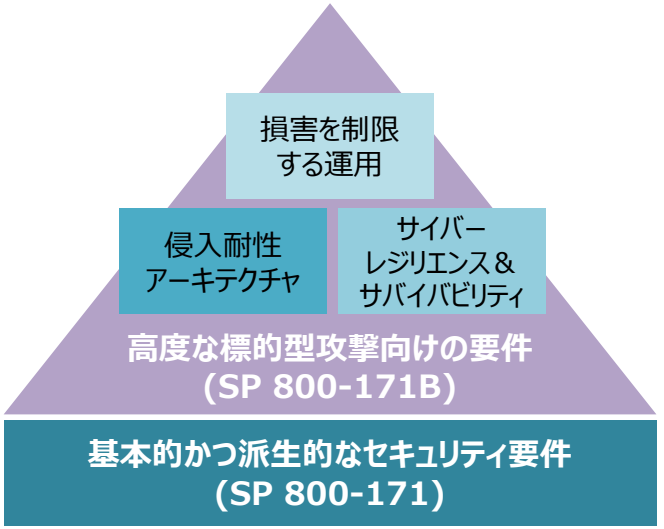
- SP 800-171で提示されているセキュリティ要件への準拠を評価するための評価手順及び方法論を提供する。

SP 800-171B (2019年6月 ドラフト公開)
CUIを処理する重要性の高いプログラム及び価値の高い資産向けの高度なセキュリティ要件

- 重要性の高いプログラムや価値の高い資産で扱われるCUIの機密性保護のために推奨される高度なセキュリティ要件を提供する。

SP 800-171とSP 800-171Bとの関係

- SP 800-171Bは、高度な標的型攻撃(APT攻撃)からCUIを保護するため、SP 800-171が提示する要件を補完する。
- SP 800-171Bが提示する要件は、「損害を制限する運用」、「侵入耐性アーキテクチャ」、「サイバーレジリエンス＆サバイバビリティ」の3点をサポートし、価値の高い資産の保護を実現する。



出典：Draft NIST Special Publication 800-171B

【米国における取組事例②】

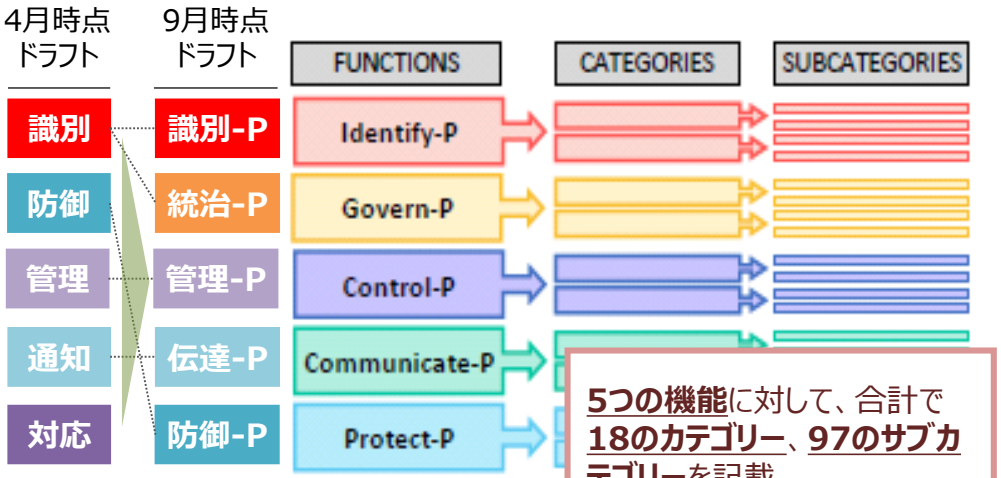
プライバシーデータを守るためのセキュリティ対策：NISTプライバシーフレームワーク

- NISTでは、2019年4月に公表された**NISTプライバシーフレームワーク(ディスカッション・ドラフト)の意見募集の結果等を反映し、9月に予備ドラフトを公開**(10月24日まで意見募集を実施)。
- NISTサイバーセキュリティフレームワーク(CSF)を踏襲した全体の枠組みは堅持しつつ、個々の機能やカテゴリーにおいてディスカッションドラフトから修正がなされている。
- 既に広く利用されているNIST CSFとの棲み分けをより強く意識したリスクの整理等がなされている。

プライバシーフレームワークの構造

NIST Cybersecurity Frameworkと同様の構造を採用。

- 基本的な構造は5月時点のドラフト(discussion draft)から変更なし。
- 5つの機能は、discussion draftから変更され、「対応」を削除し、「統治-P」を追加した。



-P：CSFの5分類と区別するため追記

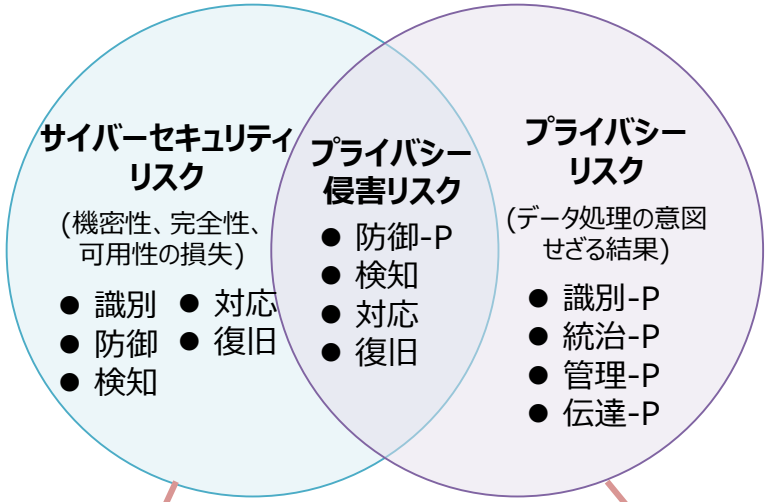
5つの機能に対して、合計で**18のカテゴリー**、**97のサブカテゴリー**を記載。

出典：NIST Privacy Framework Preliminary Draft

サイバーセキュリティフレームワーク(CSF)との関係

CSFとの併用をより意識した構成に変更。

- サイバーセキュリティリスクとプライバシーリスクの関係を整理し、網羅的なリスク対応が可能となるようにCSFとプライバシーフレームワーク(PF)の機能をマッピングしている。



「サイバーセキュリティリスク」にはNIST CSFで対応する

「プライバシーリスク」にはNIST PFで対応する

【欧州における取組事例①】
欧州におけるクラウドインフラ構築の動き：Gaia-X プロジェクト

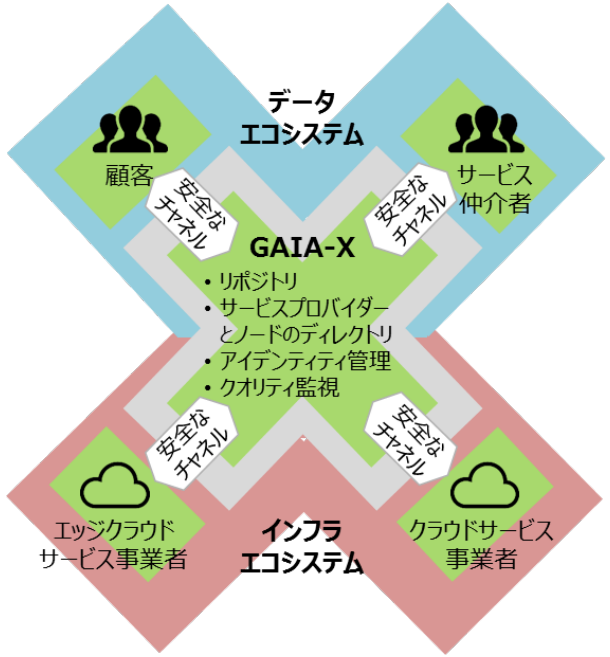
- 2019年10月29日、**ドイツ政府とフランス政府は、EU規模でのデータの共有や利活用を支援するため、クラウドサービスのインフラを構築する構想(GAIA-X プロジェクト)を発表**した。
- 当初はドイツとフランスで構想を主導し、2020年に他の欧州諸国に具体的な提案を行う予定である。なお、現時点では、投資額などの詳細は言及されていない。

取組の背景と目的

背景	● IoTが進展する中、様々なIoT機器等から収集したデータを、組織横断で活用することが重要になると見られている。 ● 既存のクラウドサービス市場は欧州外のプレイヤーに席巻されている。
目標	● データの主権確立 (data sovereignty：データに対する完全なコントロール及びデータへのアクセス権限に関する自由な決定) ● 特定サービスへの依存の減少 (reduce dependencies) ● より幅広い層に対するクラウドサービスの魅力増進 (make cloud services attractive on a broad basis) ● イノベーションのためのエコシステムの創出 (creating an ecosystem for innovation)
取組	ドイツ、EU規模での安全かつ連携したデータ・インフラの創出 (creating a secure and federated data infrastructure in Germany and in Europe more broadly)

取組の全体像

- Gaia-Xは、複数の異なるクラウドサービス間のリンクとして機能することで、組織を跨いだ安全なデータの共有や各種サービスの利用を可能にする。



出典：　”Project GAIA-X：A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem”

【欧州における取組事例②】
ePrivacy規則の策定

- **<u>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</u>**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。
- しかし、**<u>2019年11月、欧州理事会常任委員会（COREPER）が同ドラフトを否決</u>**したことから、2020年に、変更または撤回を選択する必要がある。

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
  - (この間、業界団体等による意見提出や閣僚理事会による複数回のドラフト公表を実施)
- **2019年7月**：議長国のフィンランドが修正版ドラフトを発表
- **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11月**：欧州理事会常任委員会（COREPER）が同ドラフトを否決

ePrivacy規則ドラフトの主なポイント

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。
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ほう - 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ほう

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わるセキュリティインシデント事例

３．データを守るための海外の取組事例

４．データマネジメントに関する既存のフレームワーク等

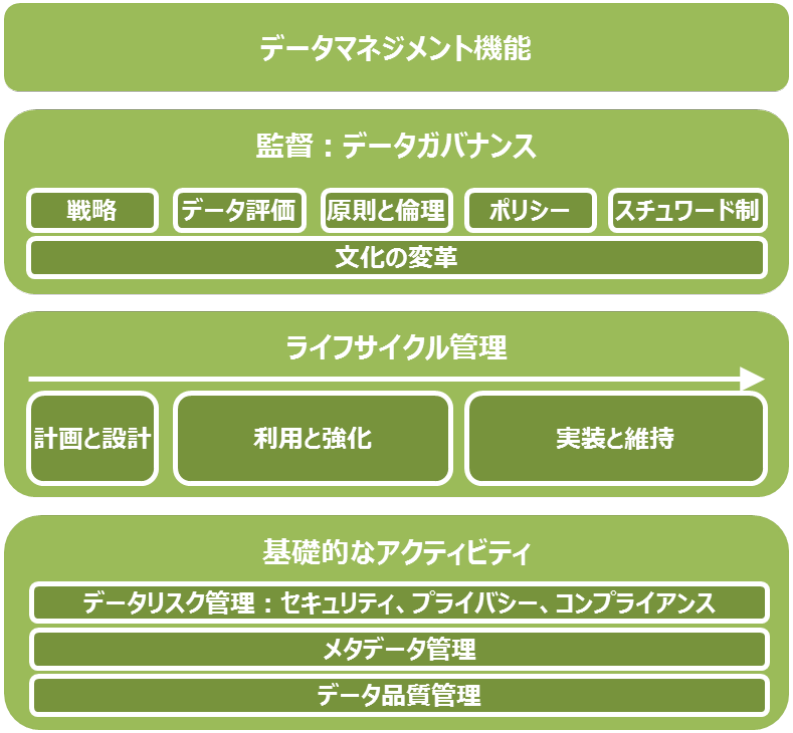
５．本タスクフォースの検討事項

データマネジメントに関する既存のフレームワーク (DAMA DMBoK)

- 国際データマネジメント協会（DAMA International)作成のデータマネジメント知識体系ガイド(DMBoK)では、**データマネジメントを「データや情報の価値を、データ・情報のライフサイクルを通じて(継続的に)創出・維持・保護・改善するための、計画・社内規定・(業務)プログラム、(業務)ルーチンの、開発、実行及び監視である」**とし、組織がデータマネジメントを実践する際に参照すべき枠組みや手法、評価方法等を提供。

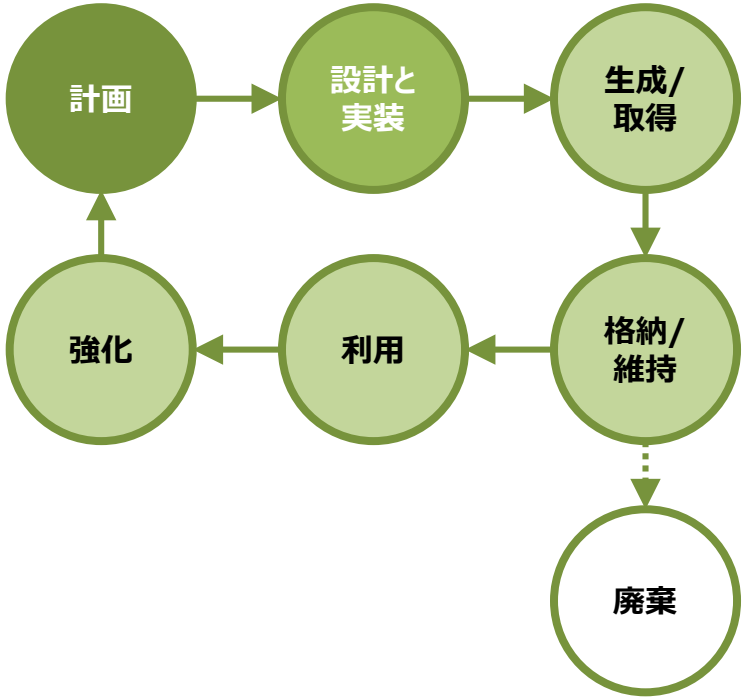
データマネジメント機能フレームワーク

- DMBoKでは、データマネジメントの機能を大きく、データガバナンス、ライフサイクル管理、基礎的なアクティビティに分類している。



データライフサイクルの主要アクティビティ

- データ資産を効果的に管理するためには、データライフサイクルを理解し、計画を立てる必要がある。

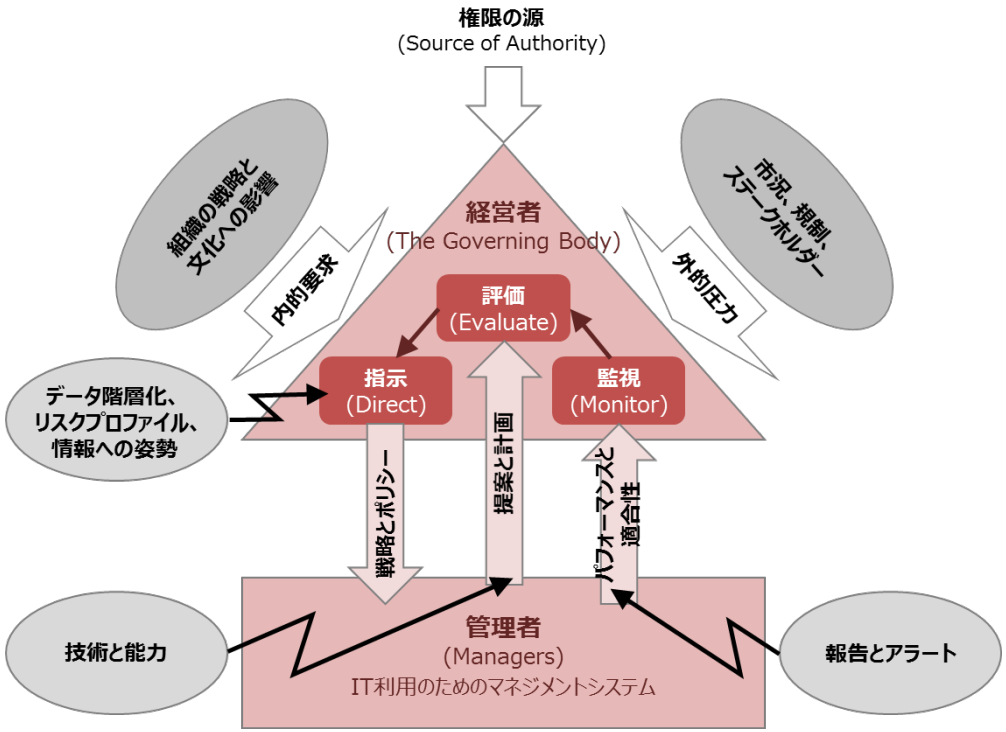


出典：DAMA International “データマネジメント知識体系ガイド 第2版”

データガバナンスに関する既存のモデル (ISO/IEC 38505-1:2017)

- **ISO/IEC 38505-1:2017は、データガバナンス**(組織のデータの現在及び将来の利用を指示し、管理するシステム)**のモデルを提示**し、①経営者が実施すべきガバナンスのタスク、②経営者が行うべき原則、③データを利活用する際の特殊性を規格化している。

ISO/IEC 38505-1におけるデータガバナンスモデル



データガバナンスモデルの概要

- データは、EDMモデル(①**評価**(Evaluate)、②**指示**(Direct)、③**監視**(Monitor))に基づき管理する必要がある。
  - **評価**：現在と将来のデータ利用について評価する。
  - **指示**：データの利用が組織のビジネス目標に合致するよう、計画とポリシーを策定し、実施する。
  - **監視**：ポリシーへの準拠と計画に対する達成度を監視する。
- EDMモデルに基づいたデータの管理を行う際、経営者は、組織の戦略や文化といった内的要求と、市況や規制といった外的圧力を考慮する必要がある。
- データ管理者は、評価の際、新たなデータ管理技術が組織に及ぼす影響について経営者に説明し、経営者は、データの利用に係る戦略やポリシーについて管理者に指示する。
- 有効なデータガバナンスを実施することにより、組織は、以下のような利点を得ることができる。
  - データの所有者やユーザーから見て信頼できる組織になれる。
  - 知財及びその他のデータ由来の価値を適切に保護できる。
  - データ侵害の影響を最低限にするよう準備できる。

出典： ISO/IEC 38505-1:2017 Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data

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わるセキュリティインシデント事例

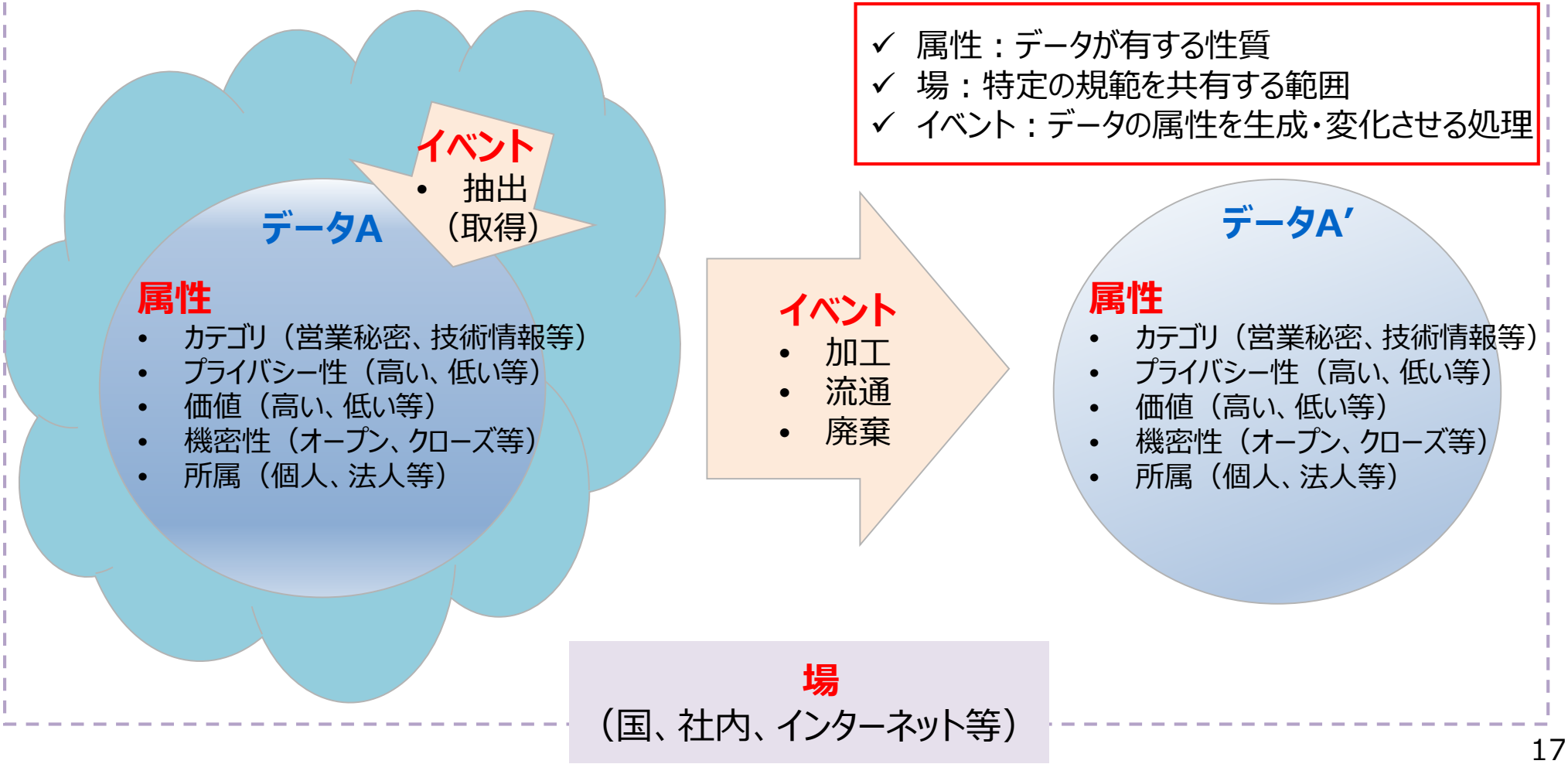
３．データを守るための海外の取組事例

４．データマネジメントに関する既存のフレームワーク等

５．本タスクフォースの検討事項

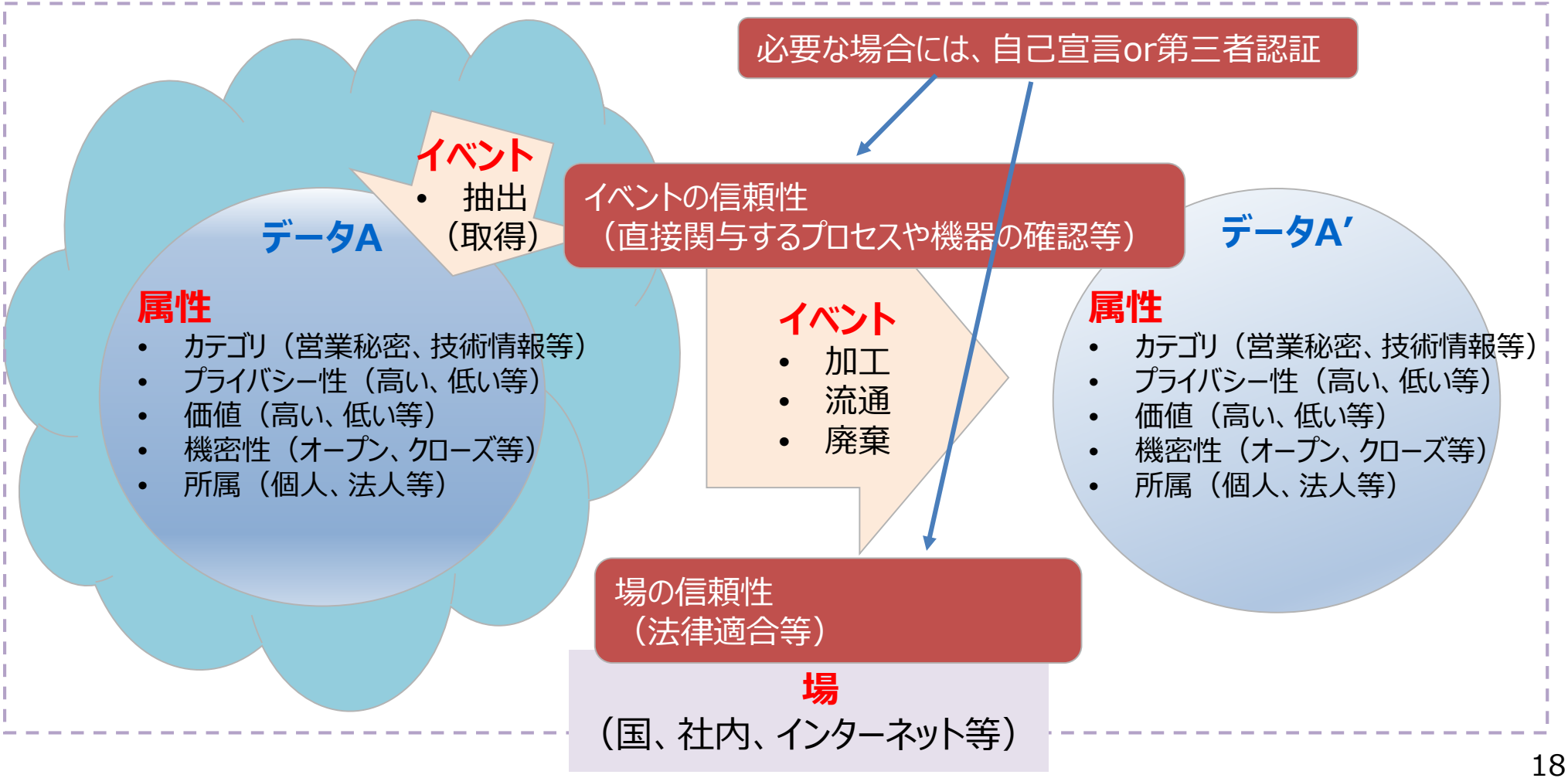
データマネジメントの新たな捉え方

- 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。



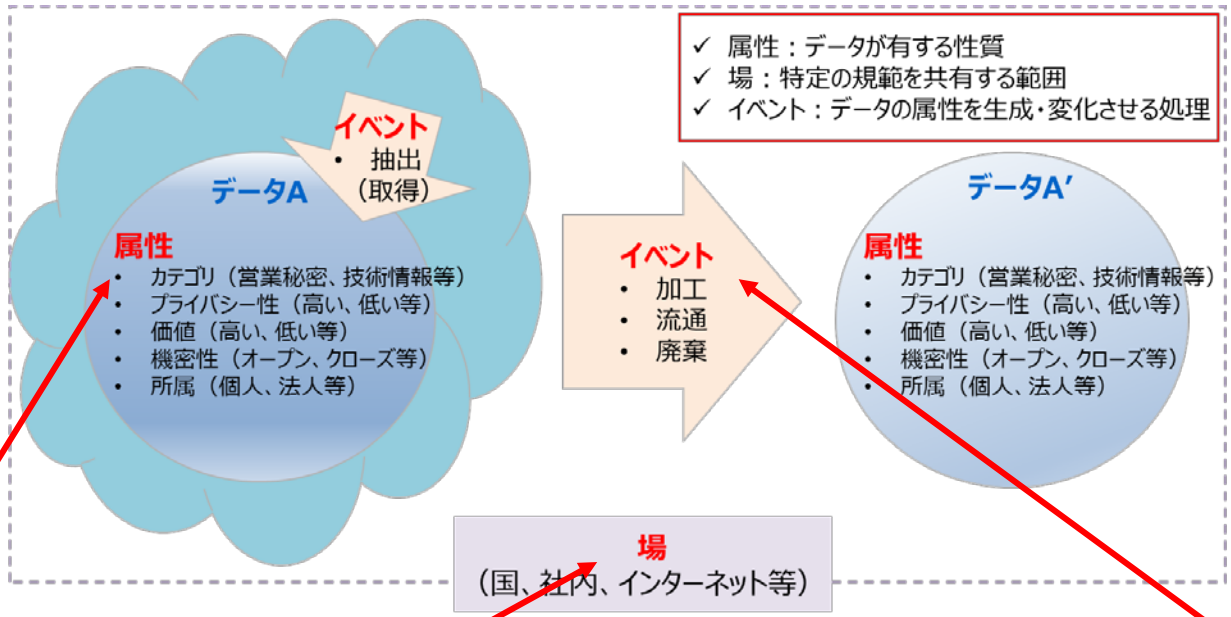
データの信頼性の考え方

- データの信頼性とは、データの属性に応じて、イベントの信頼性及び場の信頼性を適切に確保すること、と考えてはどうか。



データマネジメントに関連するキーワードのマッピング

- 今回提示した新たな捉え方に沿って、データマネジメントに関連するキーワードを、第1回タスクフォースで委員の皆様から挙げられたものを中心にマッピングすると、以下のようになるのではないか。



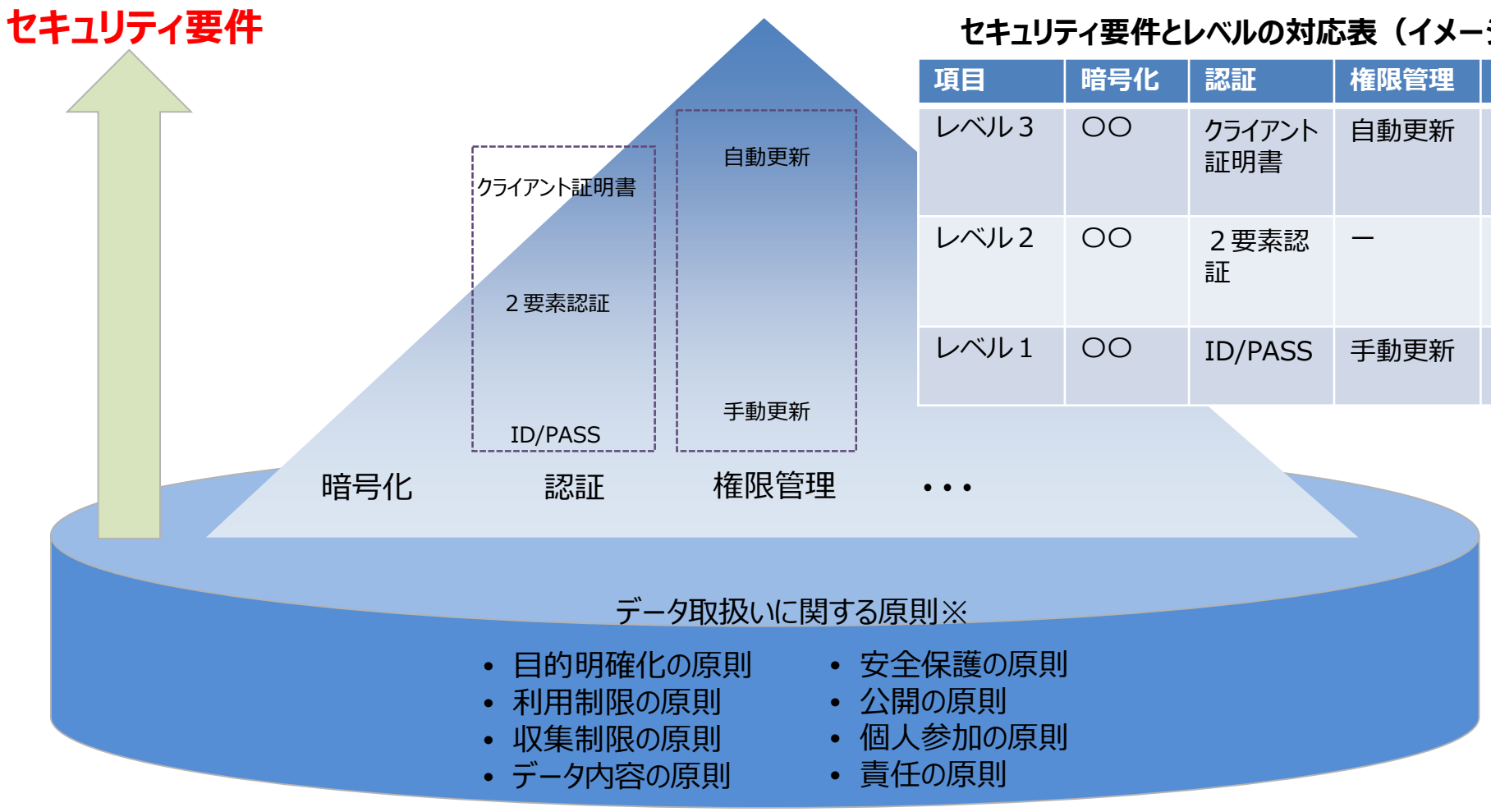
- 技術情報
- CUI
- プライバシーの観点
- オープンデータ
- データの帰属

- 個人情報保護法
- GDPR
- SP800-171
- 制度的裏打ち
- 業界基準的なセキュリティ要件
- プロバイダーと利用者の関係
- インターネット
- データ交換基盤

- 加工技術
- データの加工
- データの付加価値創造
- エンティティの真正性
- トレーサビリティ
- プロセスの信頼性

セキュリティ要件の考え方

- データに対する適切なセキュリティ要件を示すことができれば、データを流通させる際のセキュリティ基準が明確になり、データ有効活用の更なる拡大につながるのではないか。



セキュリティ要件とレベルの対応表（イメージ）

項目	暗号化	認証	権限管理	…
レベル３	○○	クライアント証明書	自動更新	
レベル２	○○	２要素認証	ー	
レベル１	○○	ID/PASS	手動更新	

※　OECDプライバシーガイドラインにおける8原則。データ取扱いに関する原則については、P24以降参照。

セキュリティ要件の考え方

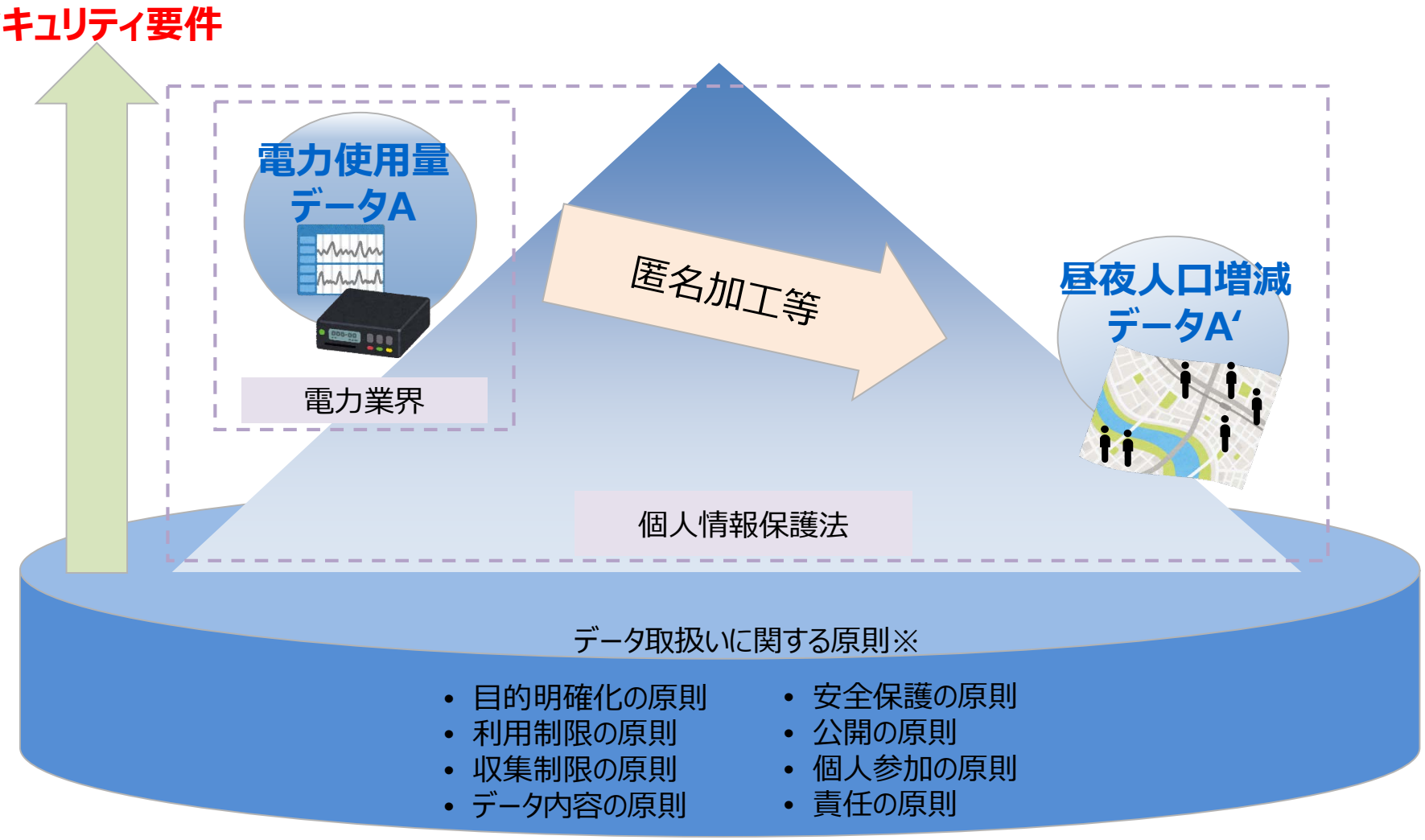
- セキュリティ要件は、データAの**属性**及び対応する**場**、並びに、データA‘へ処理するための**イベント**の影響を受けて決まるのではないか。

電力使用量データから防災等に活用するための昼夜人口増減データへの匿名加工化の想定（イメージ）

✓ 属性：データが有する性質
✓ 場：特定の規範を共有する範囲
✓ イベント：データの属性を生成・変化させる処理

セキュリティ要件の考え方

- セキュリティ要件は、データAの**属性**及び対応する**場**、並びに、データA‘へ処理するための**イベント**の影響を受けて決まるのではないか。



※　OECDプライバシーガイドラインにおける8原則。データ取扱いに関する原則については、P24以降参照。

第2回タスクフォースにおける論点

- 今回提案したデータマネジメントの新たな捉え方及びセキュリティ要件の考え方について、御議論いただきたい。

データマネジメントの新たな捉え方

- **データマネジメントの定義**
- **データマネジメントの3つの構成要素（属性･場･イベント）**
- **属性･場･イベントにおける要素**
- **信頼性の考え方**

セキュリティ要件の考え方

- **セキュリティ要件の項目**
- **セキュリティ要件のレベル**

（参考）【データ取扱いに関する原則の例】
OECDプライバシーガイドラインにおける8原則

- OECDが1980年9月に採択した「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」で以下の8つの原則が定められている。
- 本原則は、世界各国の個人情報保護やプライバシー保護に関する法律の基本原則として取り入れられている。

名称		概要
1	目的明確化の原則	収集目的を明確にし、データ利用は収集目的に合致するべき
2	利用制限の原則	データ主体の同意や法律に基づく場合以外は、目的以外に利用使用してはならない
3	収集制限の原則	適法・公正な手段により、かつ、情報主体に通知又は同意を得て収集されるべき
4	データ内容の原則	利用目的に沿ったもので、かつ、正確、完全、最新であるべき
5	安全保護の原則	合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護するべき
6	公開の原則	データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき
7	個人参加の原則	自己に関するデータの所在及び内容を確認させ、又は異議申立てを保障するべき
8	責任の原則	管理者は諸原則実施の責任を有する

（参考）【データ取扱いに関する原則の例】
GDPRにおける適法な個人データ処理の要件 (第5条)

- 個人データを処理するに当たり、管理者は6つの原則(適法性、公平性及び透明性/目的の限定/データの限定/正確性/保管の限定/完全性と機密性)を遵守する義務を負っている。これに加えて、管理者はその遵守を証明できなければならない(アカウンタビリティ)。

遵守する原則(第5条第1項)

適法性、公平性及び透明性	個人データは、適法、公平かつ透明性のある手段で処理されなければならない。
目的の限定	個人データは、識別された、明確かつ適法な目的のために収集されるものでなければならず、これらと相容れない方法で更なる処理を行ってはならない。
データの限定	個人データは、処理を行う目的の必要性に照らして、適切であり、関連性があり、最小限に限られていなければならない。
正確性	個人データは、正確であり、必要な場合には最新に保たれなければならない。不正確な個人データが確実に、遅滞なく消去又は訂正されるように、あらゆる合理的な手段が講じられなければならない。
保管の限定	個人データは、当該個人データの処理の目的に必要な範囲を超えて、データ主体の識別が可能な状態で保管してはならない。
完全性と機密性	個人データは、当該個人データの適切なセキュリティを確保する方法で取り扱われなければならない。当該方法は、無権限の、又は違法な処理に対する保護及び偶発的な滅失、破壊、又は損壊に対する保護も含むものとし、個人データの適切なセキュリティが確保される形で処理されなければならない。

遵守する原則に対するアカウンタビリティ(第5条第2項)

アカウンタビリティ	管理者は、第1 項について責任を負い、かつ、同項遵守を証明できるようにしなければならないものとする

（参考）【データ取扱いに関する原則の例】
米国における「公正な情報取扱い諸原則」(FIPPs)

- FIPPs(Fair Information Protection Principles：公正な情報取扱い諸原則)とは、1974年プライバシー法(公的部門を対象としたプライバシー保護法制)を貫く8つの原則である。
- 国土安全保障省(DHS)が2008年に、同省における基本的プライバシー方針とその運用原則として、「1974年プライバシー法に基づくFIPPs」を定めている。

	1974 年プライバシー法におけるFIPPs
1	**公開の原則** （Openness Principle）
2	**個人アクセスの原則** （Individual Access Principle）
3	**個人参加の原則** （Individual Participation Principle）
4	**収集制限の原則** （Collection Limitation Principle）
5	**利用制限の原則** （Use Limitation Principle）
6	**開示制限の原則** （Disclosure Limitation Principle）
7	**情報管理の原則** （Information Management Principle）
8	**説明責任の原則** （Accountability Principle）

	DHS におけるFIPPs
1	**透明性** （Transparency）
2	**個人参加** （Individual Participation）
3	**目的明確化** （Purpose Specification）
4	**データ最小化** （Data Minimization）
5	**利用制限** （Use Limitation）
6	**データ正確性と完全性** （Data Quality and Integrity）
7	**セキュリティ** （Security）
8	**説明責任と監査** （Accountability and Auditing）

（参考）【データ取扱いに関する原則の例】
米国消費者プライバシー保護に関する権利章典

- オバマ大統領は、2012年2月に商務省NTIAを通じて、「消費者プライバシー保護に関する報告書」を刊行したが、同報告書では、情報化社会におけるプライバシー保護の在り方の青写真として、「消費者保護のための権利章典」(権利章典)が提示されている。
- 権利章典は、以下の7項目からなり、前述したDHSのFIPPsと共通する部分が多い。

名称		概要
1	個人による統制	消費者は、どの個人情報を企業が収集し、どのような利用をするかについて統制する権利を有する。企業はそのための方法を消費者に提供しなければならない。
2	透明性	消費者はプライバシーと運用の安全性について、容易に理解し、その情報にアクセスできる権利を有する。企業は、プライバシーリスクについて、消費者が容易に理解できるよう、明確にそれらを提示しなければならない。
3	提供目的の尊重	消費者は、企業が個人情報を収集、利用及び開示する場合には、自身がデータを提供した時の目的に沿った方法で行うよう要求する権利を有する。個人情報取得時の目的から逸脱した、企業の情報の利用又は提供は制限される。
4	安全性	消費者は安全で責任ある個人情報の取扱いを受ける権利を有する。
5	アクセスと正確性	費者は、利用しやすいフォーマットによる個人情報へのアクセスと個人情報修正の権利を有し、個人情報が不正確である場合、消費者に及ぶ可能性がある悪影響への適切な対処と情報の精度確保が可能とされなければならない。
6	焦点を当てた収集	消費者は、企業が収集及び保持する個人情報の範囲につき、合理的な制限を設ける権利を有する。企業の個人情報収集は、自身の目的達成のために必要な最小限度に限られ、収集の目的から逸脱しない範囲に限られる。
7	説明責任	消費者は、権利章典の原則の固守を保障する適切な方策を定める企業によって、個人情報が処理される権利を有する。

（参考）【データ取扱いに関する原則の例】
個人データの保護を目的とした主要な諸原則のマッピング

OECD8原則	個人情報保護法(日本)	GDPR(欧州)	DHS FIPPs (米国)	消費者プライバシー保護に関する権利章典(米国)
① 目的明確化の原則	適正な取得(第17条) 取得に際しての利用目的の通知等(第18条)	適法性、公平性及び透明性の原則(第5条1項(a)) 目的の限定の原則(第5条1(b))	目的明確化(Purpose Specification)	提供目的の尊重(Respect for Context)
② 利用制限の原則	利用目的による制限(第16条) データ内容の正確性の確保(第19条)	目的の限定の原則(第5条1項(b)) 正確性の原則(第5条1項(d)) 記録保存の制限の原則(第5条1項(e))	個人参加(Individual Participation) 利用制限(Use limitation)	提供目的の尊重(Respect for Context)
③ 収集制限の原則	利用目的の特定(第15条)	目的の限定の原則(第5条1項(b))	透明性(Transparency) データ最小化(Data Minimization)	焦点を当てた収集(Focused Collection)
④ データ内容の原則	利用目的による制限(第16条) 第三者提供の制限(第23条)	目的の限定の原則(第5条1項(b))	データ正確性と完全性(Data Quality and Integrity)	アクセスと正確性(Access and Accuracy)
⑤ 安全保護の原則	安全管理措置(第20条) 従業者の監督(第21条) 委託先の監督(第22条)	完全性及び機密性の原則(第５条１項(f))	セキュリティ(Security)	安全性(Security)
⑥ 公開の原則	保有個人データに関する事項の公表等(第27条)	適法性、公正性及び透明性の原則(第5条1項(a)) その他 (データ主体の権利行使のための透明性のある情報提供、連絡及び書式)(第12条) (データ主体から個人データが収集される場合において提供される情報) (第13条) (個人データがデータ主体から取得されたものではない場合において提供される情報) (第14条)	透明性(Transparency)	透明性(Transparency)
⑦ 個人参加の原則	開示(第28条) 訂正等(第29条) 利用停止等(第30条) 理由の説明(第31条) 開示等の請求等に応じる手続き(第32条) 手数料(第33条)	適法性、公平性及び透明性の原則(第5条1項(a)) その他 (データ主体の権利行使のための透明性のある情報提供、連絡及び書式) (第12条) (データ主体のアクセス権) (第15条) (訂正の権利) (第16条) (消去の権利) (第17条) (取扱いの制限の権利) (第18条)	個人参加(Individual Participation) データ正確性と完全性(Data Quality and Integrity)	個人による統制(Individual Control) アクセスと正確性(Access and Accuracy)
⑧ 責任の原則	個人情報取扱事業者による苦情の処理(第35条)	アカウンタビリティの原則(第5条2項)	説明責任と監査(Accountability and Auditing)	説明責任(Accountability)

出典： 個人情報保護委員会「個人情報保護法とGDPRの対比表」及び「CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY」を参考に作成