国際データガバナンス検討会
第2回データセキュリティワーキンググループ

事務局説明資料

2024年12月20日　デジタル庁　国際戦略

デジタル庁
Digital Agency

第一回における議論の＜まとめ＞

データセキュリティの議論を進めるにあたっての「３つの投錨点」

① 制度：データセキュリティの根拠となる法益等の明確化
② 技術：データセキュリティを確保する手段
③ 運用：データセキュリティを担う組織の在り方や手順・プロセスを定め、責任の明確化やキャパビル、モニタリングなどの施策を整理

①制度

- 法益におけるリスクの想定（侵害によるリスク、利活用が妨げられることのリスク）については、抽象論ではなくファクトに基づく検討を進める。
- 作業の観点から**以下の３つに分類し、うち「グレーゾーン」についてのリスクの想定整理を優先**する。
  - **黒**：明確にリスクが高く、汎用性が高くないデータ（例：重要インフラに関する情報など）
  - **白**：明確にリスクが低いデータ（例：統計化されたデータ、重要な企業秘密などを含まない産業関連情報など）
  - **グレー**：**リスクがあるものの、特定の用途について非常に高い有用性がある情報など**

②技術

- 技術については、**議論の枠組み（モデルケース）に沿って検討**。

③運用

- 運用については、以下２つの論点が示された。
  - **クラウドの安全性の検証やその責任所在**の検討
  - データセキュリティ関連の技術を活用できるようにするための、**組織論・キャパビル**

第一回における議論を受けた＜今後の方針＞

①制度

以下の３分類のうち、特に**グレーゾーンとして、以下のカテゴリーの情報について整理を優先**。

- **黒**：明確にリスクが高く、汎用性が高くないデータ
- **白**：明確にリスクが低いデータ
- **グレー**：リスクがあるものの、特定の用途について非常に高い有用性がある情報など
  - └ **金融（個人金融情報）、医療（ゲノム情報、生体情報、健康情報）、GPSデータ、IoTデータ（収集源としてコネクテッドカー、工場、家電等）**　⇒詳細次頁

②技術

③運用

- 議論の指針としての**「法令のマッピング作業」を進める。**
- データのライフサイクルを通した現状把握（モデル化）
  - └ **「ライフサイクルのモデル枠組み」を整理する。**

⇒本日の議論

- クラウドの安全性の検証やその責任所在の検討
- データセキュリティ関連の技術を活用できるようにするための組織論・キャパビル

法令マッピングのフレームワーク

<table>
<tr><th>分野</th><th>経済安全保障</th><th>金融</th><th>医療</th><th>GPS</th><th>IoT</th></tr>
<tr><td>対象データ</td><td>■重要インフラに関するデータ
■重要インフラ上で処理されるデータ（金融取引情報、個人情報等）
■重要物資の供給網に関するデータ</td><td>■個人金融情報（口座、支払い履歴、カード情報、信用情報等）</td><td>■ゲノム情報
■生体情報 ※1
■健康情報 ※1

※1 生体情報（顔認証・虹彩・声紋・指紋・歩容データ）および健康情報はIoTとも整理</td><td>■GPSデータ</td><td>■IoTデータ ※2
■生体情報 ※1
■健康情報 ※1

※2 データの収集源として、コネクテッドカー、工場（産業機械）、家電、インフラ、物流ほか（航空、宇宙、HEMS、ウェアラブル等）を想定</td></tr>
<tr><td>①個人情報保護との関係</td><td colspan="5">個人情報保護法における取り扱い</td></tr>
<tr><td rowspan="3">②法令名 ※3

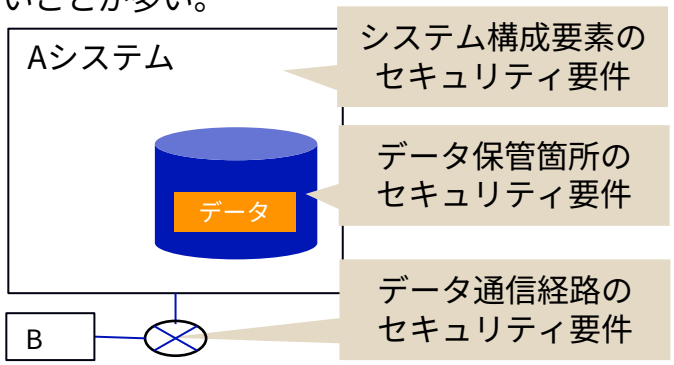
※3 政令/省令/施行規則/ガイドライン等、法令の下部・関連規程を含む</td><td rowspan="3">経済安全保障推進法
外為法</td><td colspan="4">不正競争防止法、著作権法、特許法 等</td></tr>
<tr><td></td><td></td><td colspan="2">電気通信事業法</td></tr>
<tr><td>銀行法
保険業法
金融商品取引法</td><td>次世代医療基盤法
ゲノム医療推進法</td><td>XX</td><td>XX</td></tr>
<tr><td>③保護目的</td><td>XX</td><td>XX</td><td>XX</td><td>XX</td><td>XX</td></tr>
<tr><td>④規律対象者</td><td>XX</td><td>XX</td><td>XX</td><td>XX</td><td>XX</td></tr>
<tr><td>⑤保護内容（技術含む）</td><td>XX</td><td>XX</td><td>XX</td><td>XX</td><td>XX</td></tr>
<tr><td>⑥罰則・救済</td><td>XX</td><td>XX</td><td>XX</td><td>XX</td><td>XX</td></tr>
</table>

システム観点からデータオリエンテッドのセキュリティ要件提示へ

従来、データの保護はデータ処理の主体者に対する要件として提示され、主にシステム観点で実装されてきた。しかし、本来、データの利用主体は単一ではなく、そのライフサイクルによって保護技術も異なるため、特にDFFTではデータ中心の要件とする発想の転換が必要となる。

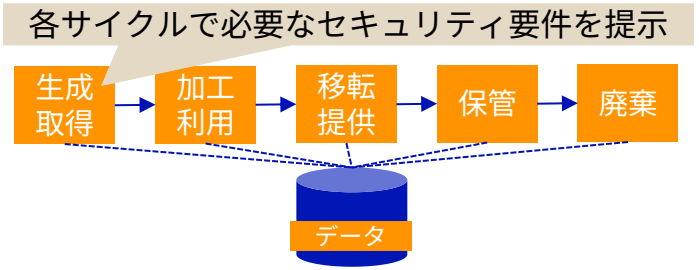
従来のセキュリティ対策

従来、データを保護するための技術的なセキュリティ対策はデータが経由・存在する箇所を中心に考えられ、システム要件として検討されてきた。データの生成・取得プロセスの真正性はシステム構築段階では考慮されないことが多い。



データ中心のセキュリティ対策

ライフサイクルごとにデータの利用主体は異なり、セキュリティ対策が求められる主体も多岐にわたる。データを軸にしたセキュリティ対策の要件を明確にし各主体が要件を実装または実装された仕組みを利用する。



DOA Securityと呼称
(Data Oriented Approach)

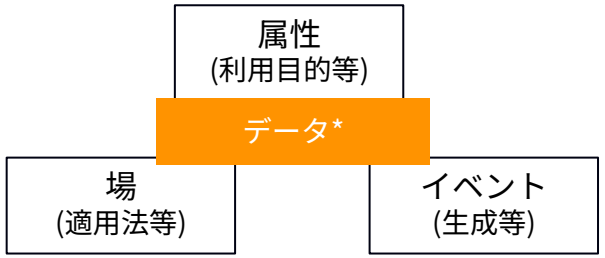
DFFTで考慮すべき技術観点のポイント(例)

- **大量のデータ利用主体、データ処理箇所**
- **各国におけるデータ処理システムの同一化困難**
- **データ信頼性確保、保護の明快な要件提示**

経済産業省

“協調的なデータ利活用に向けたデータマネジメント・フレームワーク”(2022)

データを軸に置き、データのライフサイクルを通じて、その置かれている状態を可視化してリスクを洗い出し、そのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することを可能とするフレームワークとして提示された。



同フレームワークは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目指している。
具体的なリスク分析と対策のマッピングについては、取り扱うデータとユースケースに合わせて個別に検討する。

*経済産業省のデータマネジメントフレームワークでは、データマネジメントを、データが有する性質である「属性」、データに対して特定の規範を共有する範囲である「場」、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」の3つの要素から構成されるモデルとして整理している。

リスク分析によるセキュリティ対策技術の導出イメージ

セキュリティ対策の技術要件を導く手法として従来よりリスク分析に基づいたアプローチが取られてきた。これまでに複数のフレームワークが活用されてきたが、今回、DFFTの文脈に合わせて主要な考慮ポイントにフォーカスした上でデータを軸にした技術要件の提示が必要となる。

技術的対策の導出の流れ(イメージ)

リスク分析対象のモデル化

データ

- 属性(開示範囲、利用目的など)
- 適用される各国法令、組織の規則など

システム

- 業務(アクター, ユースケース等)
- アーキテクチャー図(HW, SW, NW構成, Data Flow Diagram, 外部連携等)
- 仕様・設定情報
- 運用関連情報

イベント

データの生成・取得から廃棄に至るまで、想定されるデータ利活用プロセスにおけるイベントを可視化

検討対象とするデータの定義、ユースケース、データ処理システムの想定がまず必要

フレームワーク適用

脅威	リスク分析
mitre att&ck等	STRIDE / IPA「制御システムのセキュリティリスク分析ガイド」等
脅威インテリジェンス収集が該当	
【要検討】DFFT文脈の脅威は新たに検討が必要	

リスクの識別・評価

サイバーセキュリティ分野	(例)DDoSによる停止
	(例)DDoSによる利用料増大
	(例)ランサムウェアによる停止
	(例)脆弱性による漏洩
	(例)誤設定による漏洩
	(例)認証情報漏洩による不正侵入
	(例)権限昇格による漏洩
【要検討】DFFT分野	**(例)データ統制欠如**
	(例)データ信頼性欠如
	(例)実装機能不備
	(例)監査困難
	(例)個人情報残存

DFFTにおける脅威の洗い出し、リスクの有無、重大度等を評価

データが要求する技術的対策

生成取得	加工利用	移転提供	保管	廃棄

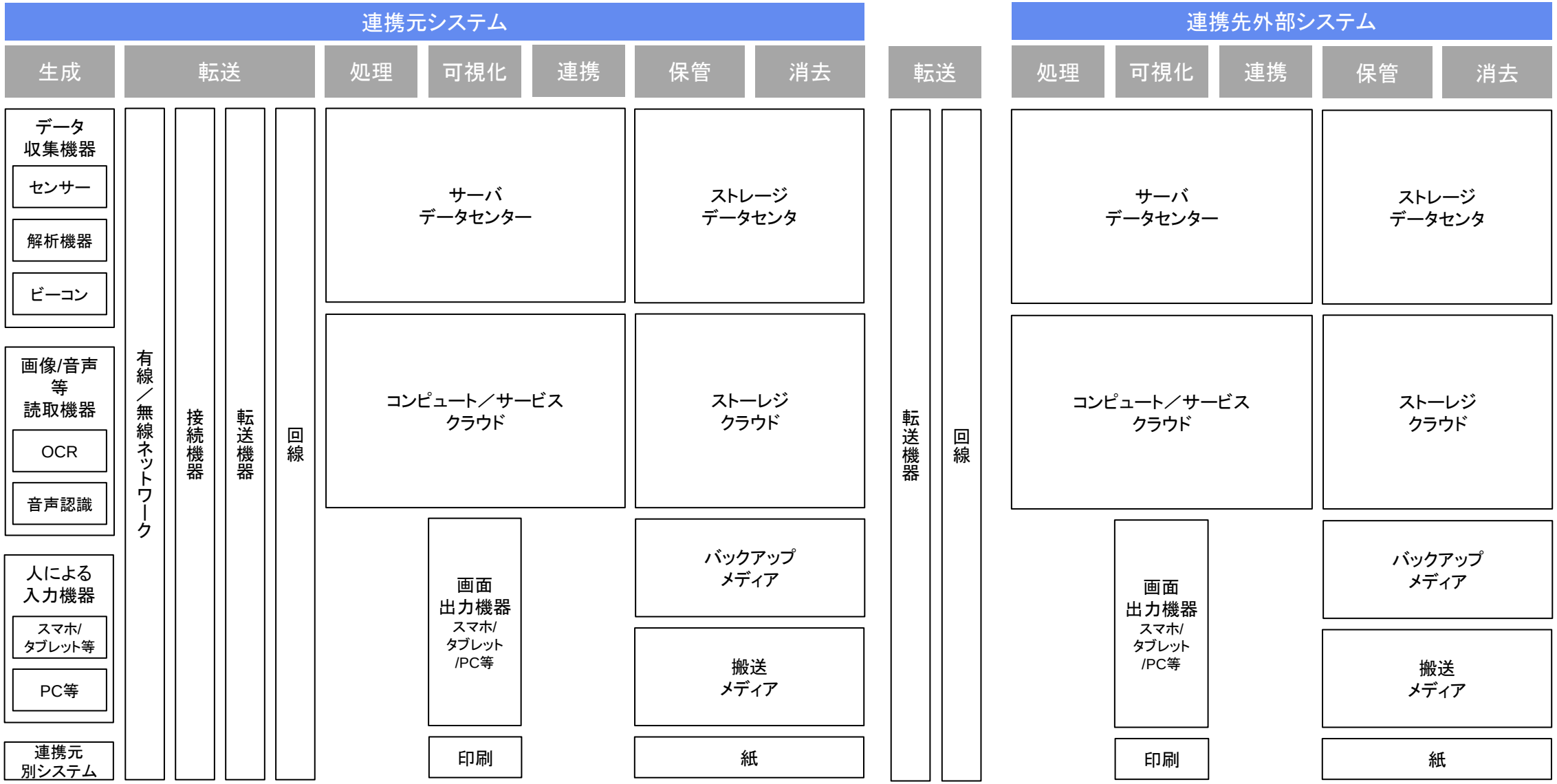
【要検討】
“DOA Security”

DFFTにおいては、各国においてデータの利用主体とデータを取り扱うシステムが多岐に渡る。データのライフサイクルごとに保護内容も異なる。単一のデータ主体とシステム観点ではなく、データを軸にしたセキュリティ対策の要件提示が求められる。

制度・運用

技術的対策の実装を要請する制度、実装内容の安全な運用など

データのライフサイクルごとの要件を検討する際のシステムモデル(例)



デジタル庁
Digital Agency