Vol.2021-IFAT-142 No.10
Vol.2021-DC-120 No.10
2021/3/26

組織が保有する情報を他組織に安全に共有し，複数組織でデータの価値を向上させる「データ価値共創プラットフォーム」

坂本　久[1]　　石田和生[1]　　加藤孝浩[1]　　稲垣嘉信[1]

概要：IoT や DX が叫ばれる現在，それらを引き起こす原動力になるものは「デジタルデータ」であり，それがどのようなものかを認識し，分析したり組み合わせたりして活用することで，社会課題を解決したり，産業活性化を促したりすることが期待できる．現在，企業や大学でも様々なデータを生成し各組織毎に保管しているが，それらデータの活用には安全面や効率面等様々な課題が存在する．
本稿では，企業や大学等各組織が生み出し保管しているデータを，安全に他の組織に共有し効率よく活用するためのプラットフォームである「データ価値共創プラットフォーム」を提案し，その具体的な構成，技術について説明する．．

キーワード：データ利活用，　データ流通，　権限管理，　暗号化，　二次利用，　コンテナ

“Data value Co-creation Platform” which shares organization’s data among other organizations, and enables multiple organizations to increase the value of data

HISASHI SAKAMOTO[†1]　　KAZUO ISHIDA[†1]
TAKAHIRO KATO[†1]　　YOSHINOBU INAGAKI[†1]

1. 背景

IoT（Internet Of Things: モノのインターネット）や DX（Digital Transformation: デジタル・トランスフォーメーション)が叫ばれる現在，それらを引き起こす原動力になるものは「デジタルデータ」である．デジタルデータ（以下，単にデータと表記する）そのものは単なる数値，情報でしかないが，それがどのようなデータかを認識し，そのデータを分析したり他のデータと組み合わせて利用することで，社会の課題を解決したり，産業の活性化を促したりすることができるようになる．

そのため，この数年で，データを利活用するための技術開発やルール整備等が急速に進められている．

近年では，データの利活用について，一企業や大学内に閉じて利活用されるのではなく，複数の組織が連携して価値共創する事例が多く見受けられる．また，我が国のデジタルガバメント閣僚閣議が 2020 年 12 月に発表した「データ戦略タスクフォース第一次とりまとめ」[1]においても，データが最大限の価値を生み出すために必要な「データ利活用の原則」として次の 5 つをあげている．

原則 1：自分で決められる，勝手に使われない（コントローラビリティ・プライバシーの確保）
原則 2：つながる（相互運用性・重複排除・効率性向上）
原則 3：いつでもどこでもすぐに使える（可用性・迅速性・広域性）
原則 4：安心して使える（セキュリティ・真正性・信頼）
原則 5：みんなで創る（共創・新たな価値の創出・プラットフォームの原則）

しかし，現時点で複数の組織が連携してデータを共有し，利活用してデータの価値を最大限に高めていくには，様々な課題が残存おり，前述の原則全てを満たす，データ流通・利活用プラットフォームは整備されていない．

2. データ利活用の課題と解決策

2.1 課題

前述の背景やデータ利活用の原則から鑑み，改めて現在におけるデータ利活用の課題を以下に挙げる．

(1) 課題 1：データ所有者が流通範囲を決定できない

経済産業省がまとめた「AI・データの利用に関する契約ガイドライン」[2]では，”データは無体物であるので，現在の民法等では，所有権や占有権，用益物権，担保物権の対象にならない”と記されている．データの利用については，データの提供者と利用者間で契約を締結し，その契約に従って利用することが必要である．しかし，データ自体は前述の通り無体物であり，そのデータが元々誰によって作られたのか，データそのものを見て識別することはできない．

1 NEC ソリューションイノベータ株式会社
NEC Solution Innovators, ltd.

Vol.2021-IFAT-142 No.10
Vol.2021-DC-120 No.10
2021/3/26

よって，契約で利用可能なデータがどれなのかを特定することは厳密には難しい．また，故意または過失により，データ利用者からデータが漏洩してしまった場合も，データがその利用者から漏れたかどうかもデータそのものを見るだけでは特定できない．これらのリスクが存在するため，データの流通経路や流通範囲はデータの所有者が想定する以上に流通する可能性があり，データ所有者がデータの流通範囲を厳密に決定することが難しい．

(2) 課題 2：データ提供以降，データが保護されない

データ所有者はデータを第三者に利用されない様に暗号化を施してデータ利用者に提供することが望ましいが，データ利用者がそのデータを利用するときは，復号化して使用することになる．使用した結果生成されるデータについての保護はデータ利用者の責任になってしまうため，この時点でデータ所有者の施した保護が途切れる可能性がある．また，前述の課題 1 でも述べた通り，データの利用については契約締結が必要であり，その中にはデータ提供時の取り扱い，例えば商用利用の制限，データを部分的に使用する等の二次利用についての制限等も含まれる場合が多い．画像データや文章データ等著作物として目視できるデータでは，一部の二次利用については確認できる可能性もあるが，そうでないデータについては，新たに生成されたデータが元のデータに基づいているかどうかを判断することが困難である．

(3) 課題 3：どのようなデータがどこに存在しているのかわからない

現在，総務省統計局や公的研究所，自治体等，それぞれがカタログサイトを構築しオープンデータを中心に利用者向けに公開されている．しかし，その公開方法やデータの利用方法はまちまちであり，非オープンデータについては，公開・検索する手法も確立されておらず，どこにどのようなデータが存在し，どのように利用できるかがわからない状態である．また，検索方法も人のインタラクションを必要とするものが多く，例えばデータを分析するプログラムから，直接データを検索し，その結果を元に直接データを参照するような環境も実現されていない．

2.2 課題を解決する技術

筆者らは，これらの課題を解決するために，以下のような技術が必要であると考え，研究開発した。

(1) 課題 1 を解決する技術

アクセス権制御技術：データそのものに所有者権限や利用者権限を付加し，データの所有者と利用可能な者を明確にする．所有者及び利用者は，組織及び所属員の正当性を管理する組織の認証ディレクトリにて証明し，データの所有権限や利用者権限を明確・厳格に管理する．

(2) 課題 2 を解決する技術

二次利用管理技術：一次情報に設定されている権限を二次以降の情報にも引継ぎ，派生した情報についても一次情報生成者の意向・権利を主張する．

セキュアコンテナ技術：権限を設定され暗号化で保護された情報を第三者に漏洩させることなく，安全にプログラム内で使用し，再び保護するためのデータ利用環境である．

(3) 課題 3 を解決する技術

カタログ生成・検索技術：生成された一次・二次情報等に関し，その情報の説明/種別/存在する場所等をカタログとして，広く利用者に向けて公開し，プログラム内から直接カタログ情報を参照して，データを利用可能にする．

3. データ価値共創プラットフォーム

3.1 データ利活用のモデル

ここで，我々が想定する，データ利活用のモデルについて説明する（図 1）．

現状では，一つの組織が情報を生成，収集し，自身が分析して行動を決定したり課題を解決したりするモノリシックな体制ではなく，データの生成や分析等を複数の組織が分担して担う連携型の体制が多くみられている．そのような体制では，少なくとも 3 つの段階が存在し，それぞれがメッシュ状に接続されて，一つまたはそれ以上のデータ生成体制を形成していると考えられる．

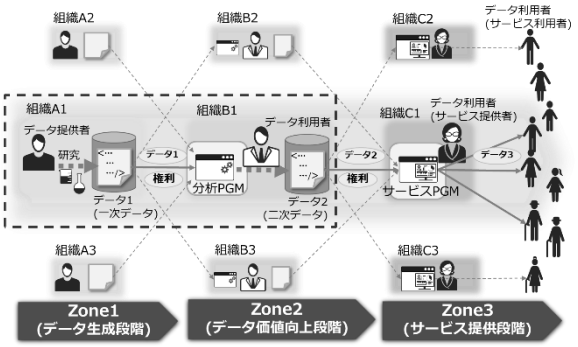

図 1　データ利活用のモデル図

3 つの段階とは，まず，データを生成する「データ生成段階」，そして，生成されたデータを分析・加工してその価値を向上させる「データ価値向上段階」，最後に，価値が上がったデータをサービスとして広く一般利用者に提供する「サービス提供段階」である．

この各段階で，データにかかわるステークホルダーも複数存在し，それぞれのステークホルダーは自分たちの意思

Vol.2021-IFAT-142 No.10
Vol.2021-DC-120 No.10
2021/3/26

でそれぞれに対してデータを流通させる．そのような提供者から利用者へのデータ受け渡しが網羅的に結合し，メッシュネットワークを形成する．

3.2 データ流通の要件

前述のメッシュネットワーク型のデータ流通モデルを実現するため，例えば、図 1 の赤枠で囲ったデータ提供者からデータ利用者にデータを渡す場面にフォーカスすると，以下の処理が必要と考える(図 2).

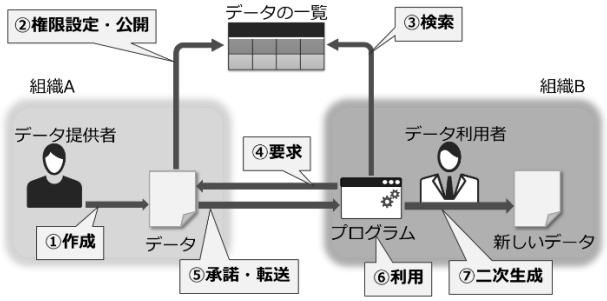

図 2　データ流通に必要な機能要件

① 作成：データ提供者がデータを作成する
② 権限設定･公開：作成したデータの利用者を設定し，登録したデータの種別や存在場所を示す情報をカタログ化し他者が検索可能にする
③ 検索：データ利用者は自分が利用したいデータをカタログから検索する
④ 要求：検索によってデータが発見できて，かつそのデータに自身の利用権限が付加されていない場合は，利用の許諾を要求
⑤ 承諾・転送：データ提供者は，データの利用について利用者から要求があった場合，その利用者に渡して良いかどうかを判断の上、利用権限を付加
⑥ 利用：データ利用者が自身のプログラム内でデータを読み込み利用
⑦ 二次生成：読み込んだデータを活用して，新しいデータを生成

3.3 データ価値共創プラットフォームの構築

筆者らはこれまでに検討してきた，課題を解決する技術，及びデータ流通の要件に基づき，図 3 に示すデータ価値共創プラットフォーム（以下，本プラットフォーム）を構築した．

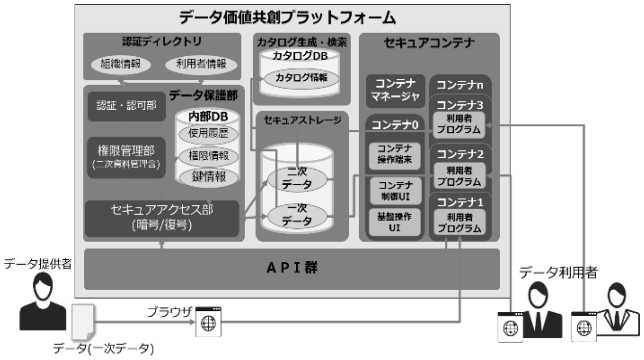

図 3　データ価値共創プラットフォームの構成

ここで，それぞれの構成について説明する．

(1) データ保護部

データに所有権限，利用権限等のアクセス権限を設定し，データを暗号化して保護する．

(2) 認証ディレクトリ

組織が運用する既設のディレクトリを利用して組織，所属人員を認証する．

(3) セキュアストレージ

保護されたデータを共有させるために格納する

(4) カタログ生成・検索部

セキュアストレージに格納したデータから情報を抽出し，データを検索するためのカタログを自動生成する．

(5) セキュアコンテナ

保護データを用いて，データを分析したり加工したりするサービスの実行環境を提供する．

(6) API 群

外部の他基盤や内部の各部に向け，基盤機能利用のためにインターフェースを提供する．

3.4 データ価値共創プラットフォームの動作

本プラットフォームの基本的な動作について，以下に説明する．

(1) データの生成と所有者の定義

本プラットフォームではデータの発生源であるデータソースと呼ぶものが存在する．データソースはデータを入力するためのプログラム，または定期的にデータを送信するセンサ等が相当する．本プラットフォームでは，このデータを誰が所有するか，誰が使用するかを設定することにより，データソースが生み出すデータの所有者とする．プログラムによるデータ入力の場合は，そのプログラムの利用者，具体的に言えばそのプログラムを利用するときにログイン認証等で識別する使用者を入力したデータの所有者として定義する．センサの場合はあらかじめシステム上でセンサとそのセンサの使用者（あるいはセンサを設置、運用している人）を結び付けることにより，センサデータの所有者を定義する．

Vol.2021-IFAT-142 No.10
Vol.2021-DC-120 No.10
2021/3/26

(2) DRM による利用権限の設定とデータの保護

本プラットフォームがデータ入力プログラムによりデータを入力される,またはセンサからデータを受信すると,DRM（Digital Rights Management: デジタル権限管理）でデータを保護する．受信したデータに所有者権限を設定し，データを公開する際には利用権限を設定する．事前にどの組織の誰にデータを公開したいかがこの時点で決まっている場合，本プラットフォームでは，公開したいデータを使いたい利用者について，その利用者が属する組織の認証ディレクトリに，利用者の存在を確認する．その利用者の存在が確認できれば，その利用者に対する利用権限(閲覧権限)を設定する．そして，データをある鍵で暗号化し，その鍵を，設定された所有者と利用者の間でのみやり取りが可能な暗号方式（秘密公開鍵暗号）にて暗号化して保護し，データをセキュアストレージに登録する．

(3) カタログ情報の生成

セキュアストレージに登録され，権限が設定されたデータについては，自動的にカタログ情報が生成される．セキュアストレージに登録された情報は，基本的にカタログとして掲載してもよい公開対象の情報と，暗号化で保護されている情報の二種類が存在し，前者の情報を用いてカタログ情報が生成される．生成されたカタログ情報は，本システム内のカタログ DB に格納され，データ価値共創プラットフォーム間で共有される．データ利用者は，共有されたカタログ情報を検索することで自身が活用したいデータがどこにあるかを示す情報であるコンテントロケーションやデータの種別を獲得することができる．カタログ情報の利用権限とデータの利用権限は別に管理され，データに利用権限が付加されていなくても，カタログ情報を検索してデータの所在を獲得する，といったような設定・運用も可能である．

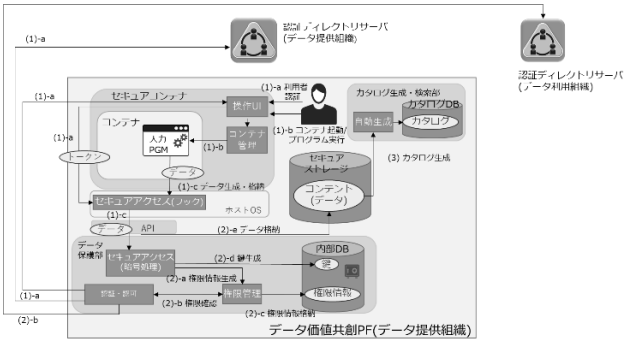

図 4　動作の流れ（データ生成～カタログ生成）

(4) 利用申請と許諾の獲得

カタログ情報により，自身が利用したいデータの所在や所有者が獲得できた場合，データ利用者はそのデータの自身の利用権限が付加されていれば，データを利用することができる．しかし，利用権限が付加されていない場合，データ利用者は，データ所有者にデータの利用を申請する．データ所有者はその申請を許可する場合，その利用者の権限を前述項目３と同じ方法で設定する．

(5) データの利用

データ利用者は，自身が利用可能なデータをプログラムの中で読みだして利用することができる．プログラムは本システム内のセキュアコンテナという特殊なコンテナの中で実行する．このコンテナは，セキュアストレージのデータにアクセスすることができる特別なプログラム実行環境である．また，セキュアコンテナでは，プログラムがセキュアストレージ以外にデータを記録させることはできず，ネットワーク等でコンテナ外にデータを送信することも基本的には制限される．

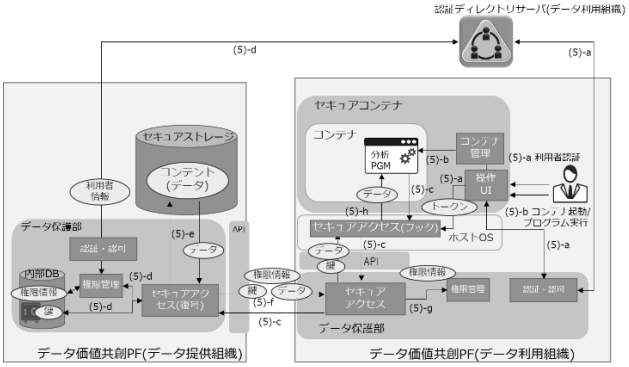

図 5　動作の流れ（データの利用）

(6) 二次生成

セキュアコンテナ内のプログラムは，データ利用者に向けて公開・共有されたデータを用いて，新しいデータを作成し，セキュアストレージ内に記録することができる．そのデータにも新たな所有者権限，すなわちデータ利用者の所有権限や，次のデータ利用者の利用権限を設定され，データの流通が進められていく．

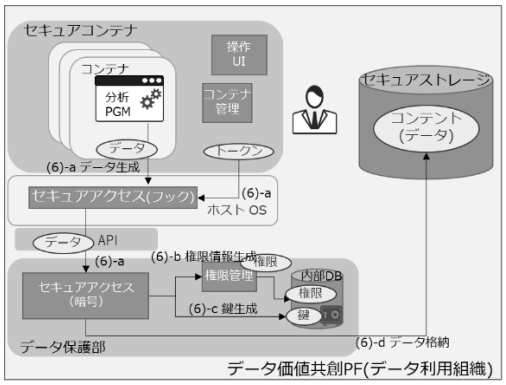

図 6　動作の流れ（二次生成）

4. プラットフォームを構成する要素

4.1 API 群・データ保護部

API 群及びデータ保護部(図 7)はこのプラットフォームの中枢を担う部分で，自組織が有するプラットフォーム内

Vol.2021-IFAT-142 No.10
Vol.2021-DC-120 No.10
2021/3/26

のセキュアコンテナで実行されるプログラムや，他組織のプラットフォーム内で実行されるプログラムから REST API を呼び出して，セキュアストレージ内に格納されている保護されたデータ(コンテント)を読み出す部分である．基本的には以下の機能を所持する．

- コンテント登録
- コンテント参照
- 鍵管理
- コンテント履歴管理
- 権限管理（権限設定，二次利用管理）
- 利用者の認証，及び認可

API 群はこれらの機能を外部から使用できる形でインターフェース化するものであり，データ保護部はアクセス権制御技術により，それらの処理を実装する部分である．コンテント登録・参照・鍵管理・履歴管理，権限管理については，登録されるデータを DRM で保護し，その保護されたデータを正当に読み出すための主要機能である．DRM によるファイルの保護に関して言えば，既存技術として Microsoft Azure Information Protection[3]や Adobe デジタル権限管理[4]等が存在するが，本プラットフォームもそれらと同様の仕組みを用いる．アプリケーションを介して入力・蓄積されるデータや，センサが送信してくるデータについて所有者権限及び利用権限を設定し，データを適当な鍵で暗号化するとともに，その鍵を所有者と利用者の間でのみやり取りが可能な暗号方式(秘密公開鍵暗号)にて暗号化して保護する．前出の既存技術と本プラットフォームとの違いは，複数の組織が有する認証ディレクトリの情報に基づいた権限設定が可能な点である．本プラットフォームでは，組織が導入している認証ディレクトリと連携してデータの所有権限や閲覧権限を設定する．認証ディレクトリは現存する実在証明書拡張型証明書（EV 証明書）等を発行された認証ディレクトリを用いることにより，その組織が公的に認証され，正しく存在している組織であると判断する．その組織に属する人間は，その組織の責任で，その人間が正しく当該組織に属する事を認証ディレクトリの情報で証明する．

また，データ保護部は，内部に認証プロバイダを設置する．本プラットフォームの利用者は，この認証プロバイダに自分の認証，他の利用者の存在確認，データを利用するときの認証，等の問い合わせをする．認証プロバイダは，他組織での認証が必要な場合は他組織の認証ディレクトリに認証処理を転送する．この認証・転送の仕組みには OpenID Connect[5]及び OAuth2．0[6]を活用する．この認証で得られたアクセストークンをデータ利用時に使用する．

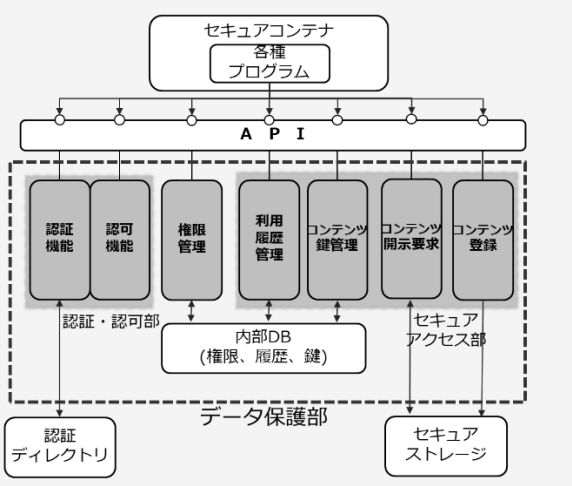

図 7　API 群，データ保護部

4.2 二次利用管理技術

二次利用管理技術は，前述のデータ保護部の一機能部分として存在し，データの二次利用に関する権限設定を司る．データ提供者が所有するデータ（このデータを一次データとする）を，データ利用者が利用し，新たにデータを生成(このデータを二次データとする）するとき，一次データの提供者が二次データ以降の流通先を制限・管理できる技術である．図 8 において，例えば，データ 1 の所有者であるデータ提供者 A は，データ 1 にデータ利用者 D の利用権限を付加し，データ利用者 D にデータ 1 を使用させる．データ利用者 D はデータ 1 を元に新たにデータ 4 を作成するが，このデータ 4 の所有者はデータ利用者 D であり，データ 4 の利用者権限は基本的にはデータ利用者 D の意向で決定される．その際に，データ提供者 A は，自身の提供したデータを元に生成されたデータが，望まない利用者（競合他社等）に渡らない様に，データ 4 の利用者権限設定に，データ 1 に設定された利用者権限を反映させる．また，複数のデータをデータ利用者 D が利用する場合，データ 4 の利用者権限は，利用した全てのデータに設定された利用権限の論理積をとった結果が設定される．

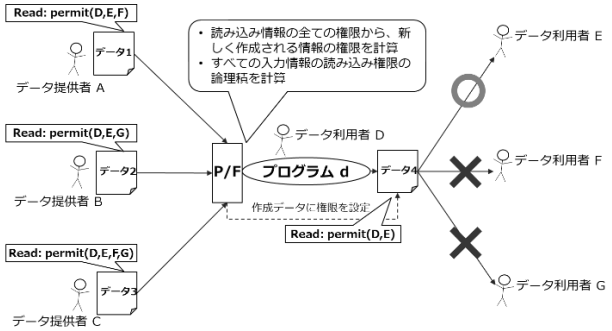

図 8　二次利用管理の概要

Vol.2021-IFAT-142 No.10
Vol.2021-DC-120 No.10
2021/3/26

4.3 セキュアストレージ

セキュアストレージ(図８)は，データ保護部により保護されたデータ（コンテント）を柔軟に格納するストレージである．セキュアストレージは，一般的に利用されているドキュメント型 DB と呼ばれるものを使用する．使用を想定している主なドキュメント型 DB は，一般的なドキュメント型 DB，Amazon S3[7]や MongoDB[8]，Coach DB[9]などである．

格納されたコンテントは，コンテントロケーション（データの URL）により組織外部に公開し他組織からアクセス可能にする．

後述するセキュアコンテナ内で実行されたプログラムで生成したデータはセキュアストレージにしか格納できないので，適切に権限管理され暗号化で保護されたデータのみ生成されることになる．

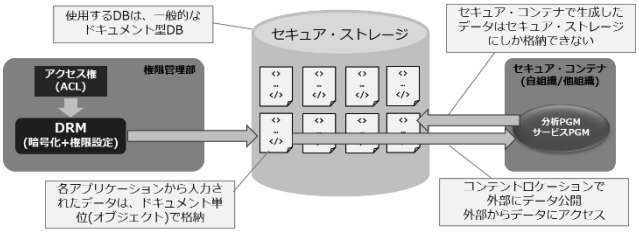

図 9　セキュアストレージ

データ入力プログラムから入力され，セキュアストレージに格納されるデータは一つのドキュメント単位で格納され，それ自体は図 10 に示すような簡単な構造を持つ．この構造は JSON 形式で記述されている．入力されたデータ全体は base64url 変換され，encryptedContent フィールドに格納する．データ本体は元の形式を保ったまま格納されることになり，スキーマレスなデータ管理を実現する．digitalSignature フィールドには，publishRequest，clearTextContent, encryptedContent フィールド内のデータが改ざんされていない事を証明するためのデジタル署名を格納する．

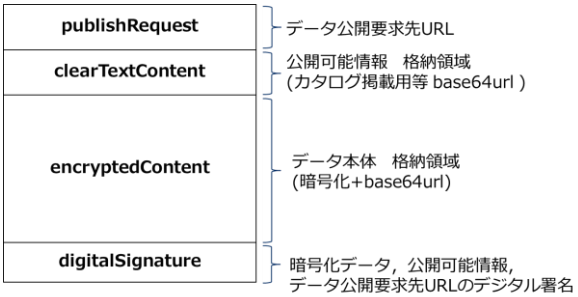

図 10　セキュアストレージ格納ドキュメント形式

4.4 カタログ生成・検索部

カタログ生成・検索部は，セキュアストレージに登録されたデータに関するカタログを自動生成し，組織外からデータを検索可能にする．データがセキュアストレージに格納されたら，データ中の clearTextContent フィールド(図 10 参照)を抜粋して RDF[10]化し，Amazon Neptune[11]や Neo4J[12]等に代表される Graph DB に格納する．この情報が登録されたデータのカタログ情報となり，組織内外のプログラムから SPARQL[13]でクエリ発行することによりデータを検索することができる．検索結果から，データ種別やデータ構造，データの存在場所(コンテントロケーション)を獲得し，プログラム内で直接検索結果を解釈し，利用することが可能となる．

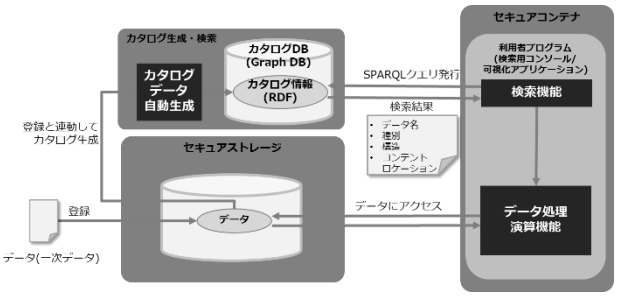

図 11　カタログ生成・検索部

カタログ情報の形式を図 12 に示す．
カタログ情報は，トリプル（主語・述語・目的語）で表現される．トリプルを構成する各要素には以下の通り格納される．

- 主語：データ本体（コンテントロケーション）
- 述語：データの要素名（属性名）
- 目的語：要素の値（属性値）

述語の語彙は Dublin Core[14]から 7 要素（タイトル・内容記述・作成者・公開者・作成日・データ種別・キーワード）を選択し，データの種別を問わず，これを共通項目としている．将来的に，分野ごとの語彙を設定し，領域別項目としてカタログ情報を設定することも検討している．また，準標準として，例えば，緯度経度を伴うデータの場合で，その情報を公開しても問題ない場合は，緯度や経度情報をカタログ情報に追加することも可能である．

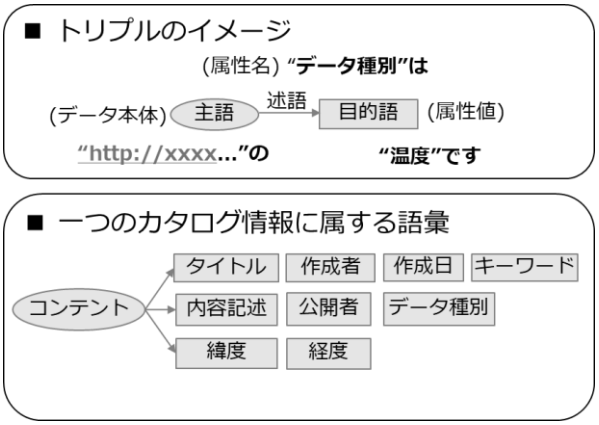

図 12　カタログ情報の構造

4.5 セキュアコンテナ

セキュアコンテナは，暗号化し保護されたデータを，外部からアクセスできない安全な領域で復号化しプログラムで処理することができるプログラム実行環境である．

セキュアコンテナは外部からの不正なログインやネットワークアクセス等は禁止され，他者からはコンテナ内のプログラム処理やデータが覗けない仕組みになっている．

セキュアコンテナ内で実行されるプログラムは，データをセキュアストレージにのみ保存可能で，コンテナ外への通信や他ストレージへの保存はできない．これによりデータの漏洩を防止する．

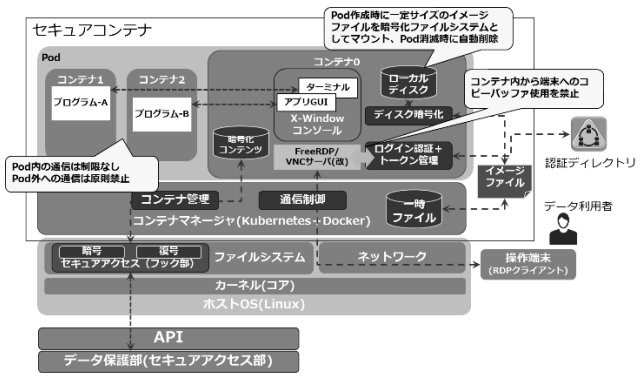

図 13　セキュアコンテナ

セキュアコンテナは，利用者のプログラムを処理するコンテナとコンテナマネージャ，及び，セキュアストレージへのアクセスに介入し，暗号化・復号化を実施するセキュアアクセスフック部から構成される．コンテナマネージャは kubernetes[15]を活用し利用者に対するコンテナ（Pod）の生成や管理を実施する．

コンテナマネージャは一データ利用者に 1 つの Pod を割り当てる．データ利用者はセキュアコンテナのコンソール画面からユーザ認証してログインすることにより，Pod 内に生成される「コンテナ 0」にログインすることができる．コンテナ 0 は，データ利用者が実際にターミナルやブラウザ等のグラフィカルユーザインターフェースを利用するための操作用コンテナである．データ利用者はコンテナ 0 がら，Web サービスとして実行するプログラムや，コマンドラインインターフェースで操作する分析プログラムを実行できる．これらプログラムは事前にコンテナイメージとして作成し，コンテナマネージャからデプロイして Pod 内で別のコンテナ（コンテナ 1，コンテナ 2 等）上で実行する．

プログラムの中では，カタログ検索により獲得した，データのコンテントロケーションを識別子としてデータにアクセスする．このアクセスは，ホスト OS（Operating System）側で動作しているセキュアアクセス部にフックされる．この時，セキュアアクセス部はデータ利用者がセキュアコンテナ使用時にユーザ認証して得られたアクセストークンを利用し，暗号化されているデータにアクセスするため，データが存在するプラットフォーム側にアクセス認可を要求する．認可されればセキュアアクセス部はデータを復号化してデータをアクセス元のプログラムに伝達する．

5. 有効性の評価

本稿執筆時点では，プラットフォーム全体の試作を完了し，順次機能的な評価，プラットフォーム全体としての評価を実施する予定である．

5.1 機能的な評価

プラットフォームを構成する各部に於いて，以下の観点で性能及び利用観点での評価を実施する．

- 権限を設定することによる情報の保護
- 暗号化したデータのアクセス速度
- 二次利用管理の有効性
- 権限情報の容量
- カタログ情報の検索容易性（検索速度，検索結果の網羅度）
- カタログ情報の容量
- カタログ情報のプログラム内での利用
- セキュアコンテナの堅牢性

5.2 プラットフォーム全体としての評価

プラットフォーム全体の有効性を確認するために，図 14 のような構成で実証実験を実施する．

第一段階 : 二つのデータ生成組織により， それぞれデータを生成しプラットフォーム上にデータを登録･公開する「データ登録実験」

第二段階 : 第一段階で共有された情報を活用し， データ利用組織により新たなデータを二次生成し，その情報をさらに共有する「データ共有・利活用実験」

Vol.2021-IFAT-142 No.10
Vol.2021-DC-120 No.10
2021/3/26

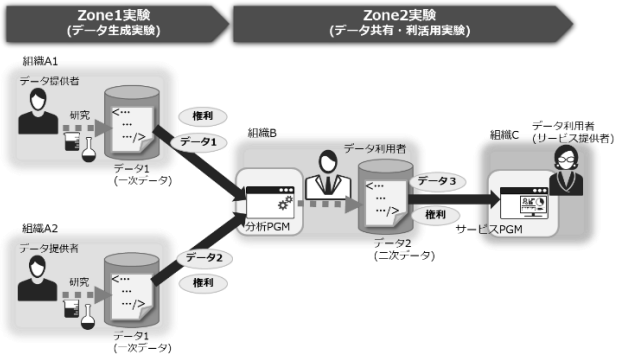

図 14　プラットフォームの有効性確認

それぞれの実験に於いて，データ共有や権限伝搬等の有効性を評価する．

6. 研究成果と今後の展開

6.1 研究成果

データ流通・利活用に関する課題を分析し，その課題を解決するための要素技術を研究開発し，それらを応用したデータ価値共創プラットフォームを設計，試作した．

第一の要素技術である「アクセス権制御技術」によりデータ保護部を実装し，入力されたデータに対して，各組織の認証ディレクトリで認証された所有権,利用権を設定し，DRM で保護する機能を実現した．

第二の要素技術である「二次利用管理技術」により，共有した一次データを元に生成された二次データ以降についても，一次データの提供者の意向を伝搬させ，一次データの提供者が流通経路を制御する事を可能にした．

第三の要素技術である「セキュアコンテナ技術」により，データ利用時に安全に暗号化データを利用することを可能とし，故意または過失による復号データの流出防止を実現した．

第四の要素技術である「カタログ生成・検索技術」により，登録したデータからカタログ情報を自動生成し，その情報を用いて，プログラムからデータを検索し，その結果をプログラム内で直接利用する方法を確立した．

6.2 今後の展開

本稿執筆時点では，機能的な評価，プラットフォーム全体としての評価については実施中または計画中であるため，結果が得られ次第，順次発表する予定である．また実証実験については，具体的に参加組織も決定してきており，順次実施しプラットフォーム全体の有効性を確認する予定である．

今後は引き続き,具体的なユースケースを選定しデータの流通全体に関する有効性を確認し，我が国初のデータ流通プラットフォームとして､さまざまな分野でのデータ流通･利活用に貢献することを目指す．

参考文献

[1] デジタルガバメント閣僚閣議“データ戦略タスクフォース第一次とりまとめ”．
https://www.kantei.go.jp/jp/singi/it2/dgov/dai10/siryou_a.pdf, (参照 2021-01-05).
[2] 経済産業省 “AI・データの利用に関する 契約ガイドライン“.https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20180615001-2.pdf, (参照 2021-02-01)/
[3] Microsoft Azure Information Protection.
https://techcommunity.microsoft.com/t5/microsoft-security-and/azure-information-protection-is-now-generally-available/ba-p/249974,(参照 2021-02-01).
[4] Adobe デジタル権限管理.https://www.adobe.com/jp/marketing/experience-manager-assets/digital-rights-management.html,(参照 2021-02-01).
[5] OpenID Foundation.https://opened.net/connect/, (参照 2021-02-01).
[6] The OAuth 2.0 Authorization Framework.
https://tools.ietf.org/html/rfc6749, https://tools.ietf.org/html/rfc6750, (参照 2021-02-01).
[7] Amazon S3,https://aws,amazon,com/jp/s3/, (参照 2021-02-01).
[8] Mongo DB.https://www.mongodb.com/, (参照 2021-02-01).
[9] Couch DB. https://couchdb.apache.org/,(参照 2021-02-01).
[10] Resource Description Framework (RDF).
https://www.w3.org/RDF/,(参照 2021-02-01).
[11] Amazon Neptune. https://aws.amazon.com/jp/neptune/,(参照 2021-02-01).
[12] Neo4J Graph Platform. https://neo4j.com/,(参照 2021-02-01).
[13] SPARQL Query Language for RDF.
https://www.w3.org/TR/2007/CR-rdf-sparql-query-20070614/,(参照 2021-02-01).
[14]Dublin Core Metadata Initiative. https://dublincore.org/,(参照 2021-02-01).
[15] kubernetes. https://kubernetes.io/ja/,(参照 2020-12-01).