セキュアなデータサービスを支えるデータ管理プラットフォーム

Data Management Platforms to Ensure Security of Data Services in Compliance with Regulations and Guidelines

花谷　嘉一 HANATANI Yoshikazu　　米村　智子 YONEMURA Tomoko　　池田　竜朗 IKEDA Tatsuro

フィジカル空間で得られたデータを利活用して新たな付加価値を創造するデータサービスでは，価値の源泉となるデータを保護する必要がある。特に，データの取り扱いに関しては，国や地域，事業分野などによって異なる法令や規制が存在し，それらを遵守してデータを管理及び利活用する必要がある。

東芝グループは，データサービスにおける適切なデータ保護とコンプライアンス遵守を実現するために，データ管理を担うデータ管理プラットフォームの，セキュリティ要件と参照モデルを定めた。そして，それらセキュリティ要件と参照モデルに基づいて，精密医療向けのデータサービス向けにゲノム情報プラットフォームの機能の一部を試作し，動作を確認した。

Data services are expected to provide new added value by making effective use of a wide variety of data generated in the physical space. Therefore, the protection of such data against security risks in compliance with different regulations and guidelines in Japan and other countries, as well as in diverse service business fields, has become increasingly important.

The Toshiba Group has defined security requirements and a reference architecture for data management platforms in order to provide highly secure data services in compliance with regulations and guidelines. We have prototyped some of the functions of a genome information platform and confirmed that the basic performance of the platform is attained.

1. まえがき

フィジカル空間（実世界）で収集したデータをサイバー空間で分析・加工し，実世界へフィードバックして新たな価値を提供するCPS（サイバーフィジカルシステム）によって，デジタル技術とデータ利活用が進み，産業構造に変革がもたらされている。データサービスは，保有するデータの利用権などをユーザーに与えるデータ提供型，ユーザーに提供したセンサーなどから収集したデータを利活用するデータ創出型，異なる企業などに分散しているデータを積極的に集約して活用するデータ共有型（プラットフォーム型）に分類される[(1)]。

東芝グループは，主にプラットフォーム型のデータサービスの実現を目指している。データサービスにおいては，競争力の源泉となるデータを安全に管理しながら，データを分析・加工・提供する必要がある。特に，個人のプライバシーに関わる情報や企業の秘密情報といった機微な情報に対しては，その利活用を規制する法令やガイドラインが国や地域，事業分野ごとに定められている。そのため，機微な情報を扱うデータサービスでは，法律や，ガイドライン，規格などの規範を遵守するコンプライアンス対応が求められる。

そこで，東芝グループの様々な事業分野において安心・安全なデータサービスを実現するために，データサービスのプラットフォームを，データ管理に関わる共通機能を提供するデータ管理プラットフォームと，データに基づいてサービス固有の付加価値を提供するデータ分析プラットフォームに大別し，それぞれに求められるセキュリティ対策とコンプライアンス対応を支える技術を，研究開発している。

ここでは，データ管理プラットフォームに関して，データサービスを行う上で遵守が求められる国内の法令・ガイドラインへの対応や，データサービスの保護・差異化の観点で定義した11件のセキュリティ要件を示す。更に，11件の要件を満たすデータ管理プラットフォームの参照モデルと，その実践事例について述べる。

2. データサービスに関わる規範

個人に関わる情報全般であるパーソナルデータからは，個人のプライバシーに関わる情報が推測できる場合がある。また，製造装置のセンサーなどにより収集された産業データからは，製品設計情報などの企業の秘密情報が推測できる場合がある。情報に対する個人や企業の権利を保護するために，国や地域ごとに異なる各種法令・ガイドラインや，当事者間の個別契約，国際標準など，データの利活用に対する様々な規範が定められている。データサービスに関わる規

表1. データサービスに関わる規範の例

Examples of lows, guidelines, and standards for data services

対象	規範の例
パーソナルデータ	個人情報保護法，分野別ガイドライン，サービス規約，ISO/IEC 27701など
企業の情報・データ	不正競争防止法，個別契約，ISO/IEC 27001など

範の例を，**表1**に示す。

パーソナルデータに関わる国内の法令としては，個人情報の保護に関する法律（個人情報保護法）がある。個人情報とは，生存する個人の特定が可能な情報であり，パーソナルデータの一部である。個人情報保護法は，個人情報の事業利用についての規範で，その取得・利用・第三者提供を同意の範囲内に制限することや，個人情報の安全管理措置を行う義務などを定めている。特に，診療データや病歴など，不当な差別や，偏見，その他の不利益が生じないように，取り扱いに特に配慮を要するものを要配慮個人情報として定め，それらを取得する際には，個人からの同意をあらかじめ取得する義務を課している。また，パーソナルデータ管理に関する国際的な規範として，ISO/IEC 27701（国際標準化機構／国際電気標準会議規格 27701）などの国際標準も整備されている。更に，産業分野別に定められたガイドラインやサービスごとに定める規約を遵守する必要がある。

企業の情報・データに関わる国内の法令としては，不正競争防止法がある。不正競争防止法では，アクセス制御などで秘密に管理されていて事業に有用な非公知情報である営業秘密などについて，不正な手段での取得・利用などを禁じている。不正競争防止法を遵守して，その保護を受けるためには，適切なセキュリティ対策を施したデータ管理を行う必要がある。また，個別に締結した契約も遵守する必要がある。更に，情報セキュリティ管理についての国際的な規範として，国際標準 ISO/IEC 27001などがある。

個人や企業の権利を尊重した安心・安全なデータサービスを提供するためには，サービスの内容，扱うデータの種類，サービスを提供する国や地域などを考慮して，遵守すべき規範を適切に選定し，それらを遵守するためのセキュリティ対策を施してデータ管理することが必須となる。

3. データ管理プラットフォーム

3.1 基本機能

1章で述べたように，データサービスのプラットフォームは，データ管理プラットフォームとデータ分析プラットフォームから成る。データ管理プラットフォームには，データを安全に“収集”する機能，データを安全に“保存”する機能，利用目的に応じて安心・安全にデータを利活用できるように適切にデータを“加工”する機能，及び利用条件を満たす場合にだけデータ分析プラットフォームにデータを“提供”する機能が必要となる。

3.2 データ管理プラットフォームのセキュリティ要件

3.1節で述べたデータ管理プラットフォームの基本機能について，国内の法令・関連ガイドライン遵守とセキュリティ強化の観点で，11件のセキュリティ要件を定義した。それぞれのセキュリティ要件と3.1節で示した四つの基本機能との対応を，**表2**に示す。「データ管理プラットフォームの機能」の列は，3.3節で提案する参照モデルにおいて，各セキュリティ要件がどの機能により保証されるかを示している。「関係する規範例」の列は，要件に対応する義務・罰則や推奨事項を定めた法令や国際標準の例（2章）を示している。

不正に収集されたデータや改ざんされたデータなど，信頼できないデータを取得すると，コンプライアンス違反による信用失墜やサービスの品質低下などの被害が生じる。そこで，データの取得条件などが満たされているかを確認し，不正なデータの取得を拒否することで確かなデータを取得することを，要件1とした。

データを安全に保存して適切な管理を行わなければ，コンプライアンス違反が生じるだけでなく，信頼できるサービスを提供できない。そこで，データを安全に保存し（要件3），保存したデータに関して法令などで典型的に課される義務を遵守すること（要件4）を要件とした。また，データの収集・保存・加工・提供におけるコンプライアンスの遵守にはデータの利用条件や利用履歴の管理も必要となる（要件5）。更に，コンプライアンスに違反する事象を検知するため，活動の監視・監査が必要である（要件6）。

利用条件を満たさないデータをデータ分析プラットフォームに提供すると，そのデータを利用するデータ分析サービスで損害が生じるおそれがある。そのため，データの利用条件を満たすことをプラットフォームが確認し（要件7），利用条件を満たさないデータの提供を防止する。データの加工に関しても，データ漏洩（ろうえい）の被害などを軽減するために，提供条件や利用目的を考慮して必要な加工を施したデータだけを提供することを要件9とした。

プラットフォームにおいてデータの利用条件を検証できれば，データの収集及び提供に関する既存の規範の義務を履行することができるが，更に第三者により検証が可能な透明性を確保することで，データの信頼性を高める必要があると考え，要件2と要件8を加えた。一方，規範では触れられていないが，実際のサービスでは，利用者のニーズや利用

表2. データ管理プラットフォームのセキュリティ要件

Security requirements of data management platform

要件番号	セキュリティ要件	関連する基本機能	データ管理プラットフォームの機能*	関係する規範例			
				個人情報の保護に関する法律	ISO/IEC 27701	不正競争防止法	ISO/IEC 27001
1	データの取得条件を満たすことをプラットフォームが確認できること	収集	A-1，A-2，C-1	○	○	○	–
2	データの取得条件を満たしていることを第三者が検証できること	収集	A-1，A-2，C-1	–	–	–	–
3	データの漏洩，滅失，毀損を防止すること	保存	A-3	○	○	○	○
4	データの修正・開示・廃棄の要求に応えられること	保存・提供	A-3，A-4	○	○	–	–
5	データの利用条件と利用履歴を管理すること	収集・保存・提供・加工	C-1	○	○	○	○
6	プラットフォーム上の活動の監視・監査を行うこと	収集・保存・提供・加工	C-1	–	○	–	○
7	データの提供条件を満たすことをプラットフォームが確認できること	提供	A-4	○	○	○	○
8	データの提供条件を満たすことを第三者が検証できること	提供	A-4	–	–	–	–
9	提供条件や利用目的に応じてデータを加工し，提供する情報量を制御できること	加工	B-1，B-2	○	○	–	–
10	新しい種類のデータを追加できること	収集・保存・提供・加工	C-1	–	–	–	–
11	データの提供者・利用者の増加に対応できること	収集・保存・提供・加工	A-3，C-1	–	–	–	–

○：該当　–：非該当

＊3.3節の図1で提案する参照モデルにおいて，各セキュリティ要件を保証している機能

者数の増加に柔軟に対応できることが望ましい。そこで，扱うデータ形式をタイムリーに追加してサービスの拡充に対応できるようにすること（要件10），利用者や提供者の増加に対応できるようにすること（要件11），を要件とした。

3.3　セキュリティ要件を満たすデータ管理プラットフォーム

3.2節で定義した要件を満たすデータ管理プラットフォームとデータ分析プラットフォームの構成例を，**図1**に示す。3.1節で述べたように，データ管理プラットフォームには，収集・保存・加工・提供の四つの機能が必須である。図1のデータ管理プラットフォームは，3.2節で定義した11個のセキュリティ要件を満たすために，これらの基本機能に加えて（図1中のA-2）選別などの機能を持ち，A. データ利活用制御，B. データ保護・加工，C. 条件・履歴管理の三つの機能群に整理された機能を利用して，データ源から転送されたデータを管理し，そのデータを必要とするデータ分析プラットフォームに提供する。

特に，C-1のデータ台帳は，データ源と合意したデータの収集元，利用条件，提供先などの収集・提供ポリシー，データの利用目的に応じた加工ポリシー，及び利活用履歴を記録し（要件5），適切なデータ管理を支える重要な機能である。

ここで，データ管理プラットフォームの参照モデルの処理フローについて述べる。まず，データ源から転送されたデータをA-1で収集し，A-2の選別処理に送り，C-1に記録さ

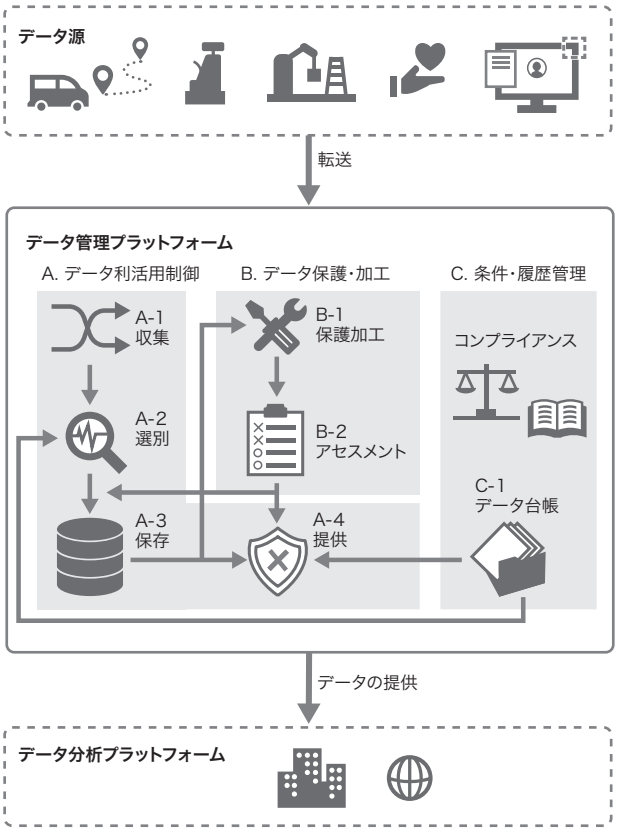

図1. データ管理プラットフォームの参照モデル

データ台帳に記載された利用条件に基づいて，データを収集・加工・保存し，適切なデータ分析プラットフォームだけに提供する。

Reference architecture of data management platform

れた収集ポリシーに基づいてデータ源の認証や利用条件の検証を行う。この際，検証で不合格となったデータを破棄し，取得条件を満たすデータだけを保存する（要件1）。更に，デジタル署名などを用いて，選別が適切に行われたことを第三者が検証可能とする（要件2）。

次に，取得ポリシーの検証で合格したデータだけをA-3に保存する。A-3では，保存したデータへのアクセス制御や改ざん検知を行い，利用者からのリクエストに基づいて適切にデータをB-1の保護加工処理かA-4の提供処理に送ることで，データ漏洩などを防止する（要件3）。

B-1では，C-1に記録された加工ポリシーに基づいて，データの匿名加工・仮名加工やマスキング処理を行い，B-2のアセスメント処理に送る。B-2では，加工後のデータが所定の安全性と有用性の基準を満たすかを検証し，検証で合格したデータをA-3又はA-4に送ることで，提供条件などに応じたデータの加工と情報量の制御を実現する（要件9）。

A-4では，C-1に記録された提供ポリシーなどに基づいて，データに対する要求の妥当性を検証する。要求が検証で合格した場合にだけデータ分析プラットフォームにデータを提供することで，提供条件が満たされる（要件7）。更に，デジタル署名などを用いて，提供前の検証が適切に行われたことを第三者が検証可能とする（要件8）。また，A-4では，データ源からの要求とC-1の収集・提供ポリシーに応じて，データの修正などを行う（要件4）。

また，C-1では，A，B，Cを監視し，その履歴を記録することで，プラットフォームの活動の監視を可能とする（要件6）。そして，A-1で対応可能なデータフォーマットや，A-2で用いる選別ポリシー，A-4で用いる提供ポリシー，B-1で用いる加工ポリシー，B-2で用いる評価ポリシーなどの追加に対応できるようにC-1のデータ台帳を設計することで，新しい種類のデータ追加を可能とする（要件10）。更に，A-3の保存とC-1のデータ台帳を適切に設計しておくことで，ユーザー管理や扱うデータサイズの増加に対応する（要件11）。

4. ゲノム情報プラットフォームの動作確認

4.1 ゲノム情報プラットフォームへの要求

個人のゲノム情報や医療情報を活用した，一人一人の体質や病気に合わせた予防や治療の実現が期待されている。東芝グループは，個人からの同意に基づいて，ゲノムデータ・健康診断データ・医療報酬明細データを収集し，疾病リスク予測サービスなどへのデータ提供を行うためのデータ管理プラットフォーム（ゲノム情報プラットフォーム[2]）を提案した。ゲノム情報などの機微な要配慮個人情報を扱うため，法令・ガイドラインを遵守するだけでなく，データ利活用の透明性を高めて，利用者が安心してデータを提供できる環境を整備しなければならない。

そこで，ブロックチェーンにデータの利用条件と利用履歴を記録することで，図1の機能Aと機能Cに関して高い透明性を実現したプラットフォームを設計・試作し，機能確認を行った。

4.2 ゲノム情報プラットフォーム特有の構成

まず，機能Cにおいて，個人情報保護法で定められた義務を遵守するために，法令で記録などの義務が課されている項目を含むデータの収集・提供の同意，提供履歴のフォーマットを定義した。データ提供者は，データを提供する前に，データの収集・提供同意を定義したフォーマットで同意情報をブロックチェーンに記録する。ゲノム情報プラットフォームの機能Aは，データの収集・提供の前に，ブロックチェーン上に記録されている同意情報を検索し，収集・提供に同意していることを確認できた場合にだけデータを保存・提供し，その履歴を定義されたフォーマットで機能Cのブロックチェーンに記録する。ブロックチェーンのノードを，ゲノム情報プラットフォーム管理者や，データ分析サービス管理者，希望する利用者などの，異なる管理者が運用することで，同意情報などの管理についての権限が分散される。ブロックチェーンにより，記録された同意・提供履歴の不変性を保証し，利用者らが同プラットフォームのコンプライアンス遵守を確認・監視できる仕組みを導入することで，透明性を高めている。

また，図1のBに対応する機能として，オリジナルデータに対して，個人を特定可能な正識別子を全て削除して，個人を特定不可能にした仮名識別子を付与した仮名化データと，仮名識別子と削除した正識別子の対応を記録した仮名対応表を作成して，それらを別権限で管理する機能を開発した。仮名対応表を用いることで，仮名化データから個人を特定できる。通常のサービスでは仮名化データの利用を標準とし，特定のサービスを提供する上でやむを得ない場合にだけ仮名化データと仮名対応表から個人を特定することで，ゲノム情報を取り扱う事業者向けのガイドライン[3]の義務を遵守し，安全性を高めている。

4.3 動作確認

ゲノム情報プラットフォームに格納済みのデータを，所定のアプリケーションに提供するシステムを，クラウドプラットフォーム上で試作した。ブロックチェーンにデータ提供の同意情報が記録されていない限りデータ提供しないことや，仮名化データなどの作成とそれを利用するサービスが実行できることを確認した。一方，ブロックチェーン上にある同意情

報などのデータを検索する速度に，改善が必要であることが分かった。

5. あとがき

データサービスの特性に応じた適切なセキュリティ対策とコンプライアンス対応を確実に行うために，データ管理プラットフォームの要件と参照モデルを定めた。また，精密医療向けデータベースに適用した。個人情報に関しては法令・ガイドラインや国際標準などの規範の整備が進んでいるが，産業データの扱いに関する規範は様々な議論が進められている状況である。また，ここで示したセキュリティ要件には，広くコンセンサスが得られた対策が確立されていないものも存在する。

今後，データサービスについての規範の策定にも関わりながら，安心・安全なデータサービスを支えるセキュリティ技術の研究開発を進め，生活行動や産業活動から生まれるデータに基づいて便益を提供するデータサービスに活用する。

文　献

⑴ 経済産業省．AI・データの利用に関する契約ガイドライン 1.1版．2019, 28p. <https://www.meti.go.jp/press/2019/12/20191209001/20191209001-1.pdf>,（参照 2022-02-05）.

⑵ 花谷嘉一，ほか．“ゲノム情報を適切に利活用するためのデータ流通プラットフォームの開発”．コンピュータセキュリティシンポジウム2021予稿集．オンライン開催，2021-10，情報処理学会．2021，p.825–832.

⑶ 経済産業省．経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン．2021，14p. <https://www.meti.go.jp/press/2020/03/20210323003/20210323003-1.pdf>,（参照 2022-02-05）.

花谷　嘉一　HANATANI Yoshikazu, Ph.D.
研究開発センター サイバーセキュリティ技術センター
セキュリティ基盤研究部　博士（工学）　電子情報通信学会・日本応用数理学会・IACR・ACM 会員
Security Research Dept.

米村　智子　YONEMURA Tomoko
研究開発センター サイバーセキュリティ技術センター
セキュリティ基盤研究部
IACR 会員
Security Research Dept.

池田　竜朗　IKEDA Tatsuro
研究開発センター サイバーセキュリティ技術センター
セキュリティ技術部
Security Technology Dept.