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

花谷 嘉一[1,a)]　米村 智子[1]　小美濃 つかさ[1]　小松 みさき[1]　池田 竜朗[1]　足立 泰則[2]　栗田 英和[2]
山口 泰平[3]

概要： 個人のゲノム情報や医療情報を活用することで，一人ひとり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．ところが，ゲノム情報や医療情報からは非常に機微な情報が推測できるため，法令やデータの属性に対応したガイドラインを順守しながら，安全に収集・保管・利活用しなければならない．また，データを提供する個人が安心してサービスを利用できるよう，高い透明性を持つことが望ましい．本稿では，個人情報保護法を順守しながら，ゲノム情報の事業利用に関するガイドラインで求められるデータの匿名管理を行うと共に，ブロックチェーンを用いた透明性の高い同意・利用履歴管理を行うゲノム情報プラットフォームを提案する．さらに，試作したプラットフォームを用いて行った性能測定の結果を報告する．

キーワード：ゲノム情報，個人情報，プライバシ保護，透明性，ブロックチェーン

Development of a data circulation platform for compliant use of genomic data

Yoshikazu Hanatani[1,a)]　Tomoko Yonemura[1]　Tsukasa Omino[1]　Misaki Komatsu[1]
Tatsuro Ikeda[1]　Yasunori Adachi[2]　Hidekazu Kurita[2]　Taihei Yamaguchi[3]

Abstract: The use of personal genome information and medical information is expected to realize prevention and treatment tailored to each individual's predisposition and illness. However, such information must be collected, stored, and utilized securely while complying with lows and guidelines corresponding to the attributes of the data, since they are sensitive personal information. In addition, the use of information should be highly transparent so that the individuals who provide the sensitive personal data can use the service with confidence. In this paper, we propose a data circulation platform that complies with Act on the Protection of Personal Information, manages sensitive personal data in an anonymized manner required by the guideline for business use of genome data, and uses blockchain to transparently manage consent history and data usage history. We also report results of performance measurement of the prototype platform.

Keywords: Genomic data, Personally identifiable information, Privacy, Transparency, Blockchain

1. はじめに

個人のゲノム情報や医療情報を活用することで，一人ひとり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．ゲノム情報や医療情報からは，個人の体質や病歴等の非常に機微な情報が推測できるため，個人の意思を尊重して安全に収集・保管・利活用する必要がある．そのた

[1] （株）東芝研究開発センターサイバーセキュリティ技術センター
Cyber Security Technology Center, Corporate R & D Center, Toshiba corporation
[2] 東芝デジタルソリューションズ（株）ICT ソリューション事業部
Toshiba Digital Solutions Corporation
[3] （株）東芝技術企画部ライフサイエンス推進室
Life Science Business Office, Corporate Technology Planning Dev., Toshiba corporation
[a)] yoshikazu.hanatani@toshiba.co.jp

め，個人情報を取り扱う事業には，国・地域や事業形態に応じて異なる様々な法令やガイドラインにより義務が課されている．また，法令等を順守するだけではなく，個人が安心して個人情報を提供してサービスを利用できるように，自身のデータの活用状況が確認できる透明性を実現することが望ましい．

本稿では，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，第三者提供を行うゲノム情報プラットフォームを提案する．提案するプラットフォームは，個人情報保護法で課されるデータ利用の同意取得義務やデータの提供・受領の記録義務を確実に果たすために，ブロックチェーンを用いた同意・利用履歴管理サービスを備えている．ブロックチェーンを用いることで，同プラットフォームの管理者等が不正を働いたとしても同意・利用履歴の不正変更等が困難となるだけでなく，ユーザーが自身のデータ利用に関する同意状態やデータの提供・受領といった利用状況が確認可能となり，高い透明性を実現できる．また，同プラットフォームでは，ゲノムデータの事業利用に関するガイドラインで求められるデータの匿名管理をゲノムデータ以外に対しても標準的に行う．さらに，データの分析結果等の本人通知や本人同意に基づく実名データの第三者提供のために，実名と匿名データの対応表を管理する．

2 節において，法令等で課される義務とブロックチェーンの概要を説明し，3 節では医療データに対するブロックチェーン活用に関する既存研究を紹介する．4 節では提案するゲノム情報プラットフォームを示し，5 節にて試作したプラットフォームの安全性や処理性能を評価する．

2. 準備

2.1 用語

ゲノム情報プラットフォームの要件の説明をするために必要となる法律・ガイドライン上の用語を紹介する．個人情報の保護に関する法律（以降，個人情報保護法）[1] および関連ガイドライン [2] に関する用語は下記の通り．

- 個人情報：生存する「個人に関する情報」であって，「当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができるものを含む.）」、又は「個人識別符号が含まれるもの」をいう．
- 個人識別符号：当該情報単体から特定の個人を識別できるものとして個人情報の保護に関する法律施行令（平成 15 年政令第 507 号）に定められた文字，番号，記号その他の符号．一定以上の情報を含むゲノムデータは，個人識別符号の該当する．
- 要配慮個人情報：不当な差別や偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして定められた 11 種の記述等を含む個人情報．病歴，医療従事者により行われた健康診断等の結果，健康診断等の結果に基づき診療若しくは調剤が行われたことは，要配慮個人情報にあたる．
- 個人情報取扱事業者：個人関連情報データベース等を事業の用に供している者のうち，国の機関，地方公共団体，独立行政法人等の保有する個人情報の保護に関する法律で定める独立行政法人等及び地方独立行政法人法で定める地方独立行政法人を除いた者をいう．
- 個人データ：個人情報取扱事業者が管理する「個人情報データベース等」を構成する個人情報をいう．
- 保有個人データ：そして個人情報取扱事業者が，本人又はその代理人から請求される開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止の全てに応じることができる権限を有する個人データをいう．

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（以降，個人遺伝情報ガイドライン）[3] に関する用語は下記の通り．

- 個人遺伝情報：個人情報のうち，個人の遺伝的特徴やそれに基づく体質を示す情報を含み特定の個人を識別することが可能であるものをいう．
- 個人遺伝情報取扱事業者：個人情報取扱事業者のうち，個人遺伝情報を用いた事業を行う事業者をいう．

2.2 個人情報保護法に係る主な義務

個人情報保護法では個人データの取得・利用・第三者提供にあたり，本人が同意した範囲内で実施することや，その記録の保管等が義務付けられている．さらに，個人データを安全に管理する義務や，本人からの個人データの開示・訂正・利用停止等の請求に対応する義務，個人データの漏えい等が生じた際の報告義務等が課されている．本小節では，令和二年改正個人情報保護法において，要配慮個人情報を国内に限定して取り扱う個人情報取扱事業者に課される主な義務を紹介する．なお，法令では義務等が免除される例外が定められているが，本稿では簡単のため省略する．

個人データの取得・利用・第三者提供

(1) 利用目的による制限 (16 条 1 項)：あらかじめ本人の同意を得ないで，特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない．
(2) 適正な取得 (17 条 1 項，2 項)：偽りその他不正の手段により個人情報を取得してはならない．予め本人の同意を得ないで，要配慮個人情報を取得してはならない．
(3) 取得に際しての利用目的の通知等 (18 条 1 項から 3 項)：本人から直接書面（電磁的記録を含む.）に記載された当該本人の個人情報を取得する場合は，あらかじめ，本人に対しその利用目的を明示しなければならない．利用目的を変更した場合は，変更された利用目的を本人に通知し，又は公表しなければならない．
(4) 第三者提供の制限 (23 条 1 項)：予め本人の同意を得ないで，個人データを第三者に提供してはならない．
(5) 第三者提供に係る記録の作成等 (25 条 1 項，2 項)：本人の同意により個人データを第三者に提供したときは，以下の事項に関する記録を作成し，個人情報保護委員会規則で定める期間保存しなければならない．
    - 23 条 1 項の本人の同意を得ている旨
    - 当該受領者の氏名又は名称及び住所並びに，法人にあってはその代表者の氏名（不特定かつ多数の者に対して提供したときは，その旨）

- 当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項
- 当該個人データの項目

(6) 第三者提供を受ける際の確認等 (26 条 1 項から 4 項) : 本人の同意により第三者から個人データの提供を受けるに際しては，以下の事項を確認し，記録を作成し，個人情報保護委員会規則で定める期間保存しなければならない．

- 23 条 1 項の本人の同意を得ている旨
- 当該第三者の氏名又は名称及び住所並びに法人にあっては，その代表者の氏名 （法人でない団体で代表者又は管理人の定めのあるものにあっては，その代表者又は管理人の氏名）
- 当該第三者による当該個人データの取得の経緯
- 当該個人データによって識別される本人の氏名その他の当該本人を特定するに足りる事項
- 当該個人データの項目

個人データの管理

(7) 安全管理措置 (20 条) : 取り扱う個人データの漏えい，滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない．

個人からの請求等への対応

(8) 開示 (28 条 2 項) : 本人から開示請求を受けた時は，遅滞なく，当該保有個人データを開示しなければならない．

(9) 訂正等 (29 条 2 項) : 本人から訂正，追加又は削除の請求を受けた場合は，利用目的の達成に必要な範囲内において，遅滞なく必要な調査を行い，当該保有個人データの内容の訂正等を行わなければならない．

(10) 利用停止等 (30 条 2 項，4 項，6 項) : 本人から利用停止等の請求を受けた場合であって，個人データの不適正な取得・利用、又は、保有個人データを利用する必要がない等の理由があることが判明したときは，当該保有個人データの利用停止等又は第三者への提供の停止を行わなければならない．

公表・報告・通知

(12) 保有個人データに関する事項の公表等 (27 条 1 項から 3 項) : 保有個人データに関し，当該個人情報取り扱い事業者の氏名等，全ての保有個人データの利用目的，及び開示等の請求手続きを本人の知りうる状態に置かなければならない．

(13) 漏えい等の報告等 (22 条の 2) : 取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものが生じたときは，個人情報保護委員会への報告及び本人への通知を行わなければならない．

2.3 個人遺伝情報ガイドラインに係る主な義務

個人遺伝情報ガイドラインでは，「個人遺伝情報」を取り扱う事業者が講じるべき措置が定められている．本小節では，個人遺伝情報ガイドラインにて定められた「個人遺伝情報取扱事業者」の主な義務のうち，個人情報保護法で課された義務よりも厳しいものを記す．

- 個人情報保護法上の「本人に通知」および「本人の同意」は，インフォームド・コンセントで行う．
- 匿名化管理者を設置し，次の管理を行う．
  - 試料等を入手後速やかに，委託又は第三者提供の場合にはその前に，試料等を匿名化する．
  - 匿名化した個人遺伝情報に対して安全管理措置を行う．
  - インフォームド・コンセントの文書，匿名化作業に当たって作成した対応表等の管理及び廃棄を適切に行い，個人遺伝情報が漏えいしないように厳重に管理する．

ここで，求められる「匿名化」とは，個人情報から特定の個人を識別できる情報の全部又は一部を取り除くことにより特定の個人を識別できないようにすることで，特定の個人の個人情報が漏洩することを防止する安全管理措置を意味している．ガイドラインでは，特定の個人を識別できる情報として，「細胞から採取されたデオキシリボ核酸（別名 DNA）を構成する塩基の配列」以外を含まない場合は，匿名化されたものとされる．つまり，「匿名化」により生成される情報は，個人識別符号の混入や再識別等を禁じた匿名加工情報と異なる点に注意が必要である．

2.4 ブロックチェーン

ブロックチェーンは，非中央集権的な分散台帳で，複数のノードで台帳の記載情報の合意形成を行う．台帳の記載情報をブロックチェーンの参加者で互いに監視しあうことで，記載情報の正当性を保証する．

本稿では，東芝デジタルソリューションズにて研究開発中のコンソーシアム型のブロックチェーン [4] を用いて，同意情報等の管理を行う．同ブロックチェーンは，Ben-Or 型の合意形成アルゴリズムを用いることで，ビザンチンフォールト耐性を高速に実現している．また，ブロックの記録閲覧等にユーザ・グループ等の単位でアクセス権限を設定できる．

同ブロックチェーンのユーザー U_i には，BC ユーザー ID $ID_{U_i}^{BC}$ とウォレット $W_{U_i}^{BC}$ が割り当てられている．$W_{U_i}^{BC}$ には，ウォレットを特定するウォレットアドレス $wID_{U_i}^{BC}$，署名鍵 $sk_{U_i}^{BC}$ とそれに対応する検証鍵 $pk_{U_i}^{BC}$ が割り当てられている．同ブロックチェーンのノードは，U_i から $(wID_{U_i}^{BC}$, m, $\sigma = \mathsf{Sign}(sk_{U_i}^{BC}, (wID_{U_i}^{BC}, m)))$ を含むトランザクション要求を受け取ると，$\mathsf{Verif}(pk_{U_i}^{BC}, (wID_{U_i}^{BC}, m), \sigma) = 1$ を検証し，検証が合格したトランザクション要求に関して複数のノード間で合意形成を行いながら，トランザクション要求に対応するスマートコントラクトを複数のノードで多重実行し，その結果をトランザクション ID TxID_j と共にブロックチェーンに記録する．ただし，Sign はデジタル署名の署名関数，Verf は検証関数，$pk_{U_i}^{BC}$ は $sk_{U_i}^{BC}$ に対応する検証鍵，m は任意のメッセージとし，$\mathsf{Verif}(pk^{BC}, m, \mathsf{Sign}(sk^{BC}, m)) = 1$ が成り立つとする．また，ノードは，U_i がデジタル署名した検索クエリを受け取ると，ブロックチェーン上の記録のうち，U_i に開示されているものに限って結果を返す．

3. 関連研究

ブロックチェーンを用いたゲノミクスサービスには，

Nebula Genomics [5] の他，いくつかのサービス [6][7][8][9] が知られている．Nebula Genomics は，ブロックチェーンを用いた同意記録システムを開発しており，ゲノム情報所有者の同意設定と情報へのアクセス要求等をブロックチェーンに記録し、監査を可能とする機能を提供する．医療情報の共有や同意管理システムには、MedRec[10][11] の他，いくつかのシステム [12][13] が知られている．MedRec では，医療情報の所有者がアクセスの可否を決定し，ブロックチェーン上にデータの所有権やアクセス許可についての情報が記録される．

いずれの方式も，日本国内の法令等の規範で求められる同意形式や記録形式となっているかは言及がない．

4. ゲノム情報プラットフォーム

4.1 システム要件

2 節にて示した個人情報保護法および個人遺伝情報ガイドラインの義務に基づき，ゲノム情報プラットフォームの要件を以下の通りに定めた．なお，要件中の条項は，個人情報保護法のものである．

本人同意の管理

要件 1 : (17 条 1 項，2 項，18 条 1 項，2 項) 個人データの取得前までに，本人から個人データを第三者提供（提供先未定）のために取得し，保存する旨の「直接取得の同意」を取得する．

要件 2 : (17 条 1 項，2 項，18 条 1 項，2 項，23 条 1 項) 個人データの第三者提供を行う前までに，本人から個人データの第三者提供（提供先確定）を行う旨と提供先での利用目的のに関する「第三者提供の同意」を取得する．

要件 3（30 条関連）: 本人より「直接取得の同意」または「間接取得の同意」の撤回が申請されたとき，以降は当該個人データの取得・利用を停止する．また，本人より「第三者提供の同意」の撤回が申請されたとき，以降は当該個人データの第三者提供を停止する．

個人データの取得

要件 4 : (17 条 2 項) 本人から個人データを取得する際に，本人より取得したデータ直接取得の同意が有効であることが確認できない場合は，個人データの取得を行わない．

要件 5 : (17 条 2 項，26 条 1 項) 第三者から個人データの提供を受ける際に，提供元の氏名等を取得し，提供者による個人データの取得の経緯の確認と提供者による第三者提供の同意とを確認を行い，取得の経緯が適切であること，もしくは同意が有効であることを確認できない場合は個人データの第三者提供を受けない．

要件 6 : (26 条 1 項，3 項，4 項) 第三者提供を受けた後，2.2 節（6）に挙げた項目を含む受領記録を作成し，安全に保存する．

要件 7 : (20 条，個人遺伝情報ガイドライン) 取得した個人データの保管にあたっては，匿名化を施した状態で保存する．さらに，個人情報の漏えい防止と，データの正確性の確保からなる安全管理措置を行う．

個人データの第三者提供

要件 8 : (16 条 1 項，23 条 1 項) 第三者提供の同意が有効であることを確認できない限り，個人データの第三者提供を行わない．

要件 9 : (25 条 1 項，2 項) 第三者提供を行った後，個人情報保護法で定められた 2.2 節（5）に挙げた項目を含む提供記録を作成し，安全に保存する．

提案するゲノム情報プラットフォームでは，プラットフォームが取得済みのデータを第三者からの要請に応じて提供する想定であるため，データ取得の時点では提供先やその利用目的を確定できない．そこで，データ取得時には 18 条 1 項，2 項にしたがって第三者提供をするという利用目的の同意を取得する要件 1 と，23 条 1 項で求められる提供先を含む第三者提供の同意を取得する要件 2 を定めた．さらに，本人が同意済の内容を撤回する機会があることが望ましいと考えられるため，30 条に関連する機能として，要件 3 を定めた．要件 5 において，取得した提供元の氏名等の検証については，本稿では簡単のため省略した．

なお，簡単のため，個人情報保護法における従業員・委託先の監督，開示請求と訂正等の請求を除く本人からの請求等への対応，通知・公表・報告に関する義務，及び個人遺伝情報保護ガイドラインにおけるインフォームド・コンセントの具体的な実現方法は，本稿の対象外とした．

以上の要件を満たすために，以下に定める「データの安全な匿名化管理」と「透明性」を満たすプラットフォームを提案する．

定義 1. 以下を満たすとき，データ流通プラットフォームはデータの安全な匿名化管理を行っているという．

- 匿名化管理者または実名データを保有しているユーザーを除いたデータ流通システムの全てのユーザーは，仮名データと自身の保有するデータを用いたとしても実名データを復元できない．
- 仮名データまたは仮名化対応表が，保存中に不正に改ざんされた場合，それを検知できる．

定義 2. 以下を満たすとき，データ流通システムは透明性を満たすという．

- データ流通システムの全てのユーザーは，全ての同意および利用履歴を閲覧し，その妥当性を検証できる．
- データ流通システムの一部の管理者およびユーザーが不正を働いても，同意および利用履歴を改ざんできない．

4.2 システム構成

ゲノム情報プラットフォーム PF は，4.1 節に示した要件を満たすために，下記に示す 4 つのサービス群が属するセグメントで分離された構成とした（図 1）．各セグメントは、それぞれ分掌された権限を持つ管理者により管理される．

(1) フロントエンドサービス FES : ユーザーとの直接的なインタラクションを行うための、標準的な Web アプリケーション等を提供するサービス群．

(2) ID 管理サービス IMS : ユーザーが FES にアクセスするためのアカウント情報を管理し，FES に対してユーザー認証を提供するサービス群．ここでのアカウント情報は，認証に必要な最低限の属性情報（ユーザー

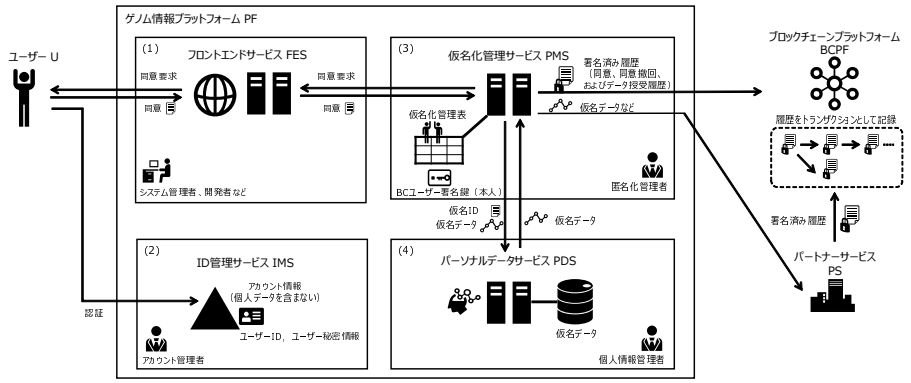

図 1 ゲノム情報プラットフォーム PF のシステム構成

ID とユーザー認証鍵）のみを有するものであり，個人データに類する情報は含まないものとする．また，登録時の本人確認や，ユーザー認証方式などについては，適切な標準仕様等を採用することで十分な安全性を実現できるため，本稿では詳細を割愛する．

(3) 仮名化管理サービス PMS：個人データの仮名化・再識別，ブロックチェーンプラットフォームを利用した同意・利用履歴の管理を行うためのサービス群．PMS の管理者が、ガイドラインで定められた「匿名管理者」に相当する．PMS が持つ仮名化管理表により，アカウント情報および仮名データ，個人データらの関連付けを行う（仮名化・再識別）．また，仮名データを利用したデータ分析を行う PF の内部サービスや，外部のパートナーサービスとのデータ授受をする役割も担う．なお，今回は，ユーザー U_i の同意・同意撤回に署名するための BC ユーザー署名鍵 $sk^{BC}_{U_i}$ については，PMS の鍵管理機構により管理する構成を採用した．

(4) パーソナルデータサービス PDS：PMS により仮名化されたデータ（仮名データ）の保管を行うサービス群．

また、PF と接続する外部サービスとして、次のものを想定している．

(5) ブロックチェーンプラットフォーム BCPF：PF およびパートナーサービスと独立した管理がなされるブロックチェーンプラットフォームを提供する外部サービス．PF および，パートナーサービスからの要求に応じて，個人データの同意情報や第三者提供記録等の利用履歴情報を保存する．

(6) パートナーサービス PS：PF との間で，仮名データや実名データを授受する外部サービス．PS は，PF と同様に，同意情報や利用履歴を BCPF に保存する．

4.3 処理フロー

4.3.1 概要

ユーザー U_i は，事前にサービスへの登録処理を行い，PF に接続するためのユーザー ID $ID^{PF}_{U_i}$，ユーザー認証鍵 $sk^{PF}_{U_i}$ と BCPF を利用するための BC ユーザー ID $ID^{BC}_{U_i}$ とウォレット $W^{BC}_{U_i}$ が安全に割り当てられているとする．$W^{BC}_{U_i}$ には，ウォレットを特定するウォレットアドレス $wID^{BC}_{U_i}$，署名鍵 $sk^{BC}_{U_i}$ とそれに対応する検証鍵 $pk^{BC}_{U_i}$ が割り当てられている．なお，本稿では，各ユーザーに割り当てられた BC ユーザー ID とウォレットを PMS のサブサービスである BC クライアントサービスが管理する構成で試作を行ったが，ユーザー自身がそれらを管理するように構成してもよい．また，BCPF を利用するために，PMS には BC ユーザー ID ID^{BC}_{PMS} とウォレット W^{BC}_{PMS} とそれに対応するウォレットアドレス wID^{BC}_{PMS}，署名鍵 sk^{BC}_{PMS}，検証鍵 pk^{BC}_{PMS} が割り当てられている．PS_i も同様に，BC ユーザー ID $ID^{BC}_{\mathsf{PS}_i}$ とウォレット $W^{BC}_{\mathsf{PS}_i}$ とウォレットアドレス $wID^{BC}_{\mathsf{PS}_i}$，署名鍵 $sk^{BC}_{\mathsf{PS}_i}$，検証鍵 $pk^{BC}_{\mathsf{PS}_i}$ がそれぞれ安全に割り当てられているとする．

本稿で提案する PF は，U_i 本人の同意に基づいて，ゲノムデータについては U_i から直接取得し，健康診断データや診療報酬明細データなどについては健康保険組合から間接取得する．そして，取得したデータを PS_i に第三者提供する．4.3 節では，データ取得の同意・撤回、データ第三者提供の同意・撤回、データ直接取得、データ間接取得、データ第三者提供の処理フローを示す．

4.3.2 データ直接取得／間接取得／第三者提供に関する同意の取得・撤回

データ取得・保存，第三者提供，または同意情報のブロックチェーンへの記録に対する同意を取得・撤回する処理である．PF においてブロックチェーンに記録する同意情報や記録情報は個人情報と考えられるため，ブロックチェーンへのそれらの記録も同意取得の対象とした．同意取得要求には，取得したい同意内容を特定するために必要な情報として，利用を希望するデータ種別・項目を特定する ID 等，個人データの受領者を特定する情報 ID^{BC}_{PMS}，個人データの提供元を特定する情報，利用目的を特定する情報，同意詳細や撤回時の取り扱い等が記載された同意文書が含まれるとする．

Step1: PMS は，FES を介して，ユーザーに対してデータ直接取得，データ間接取得，または第三者提供の同意取得要求を送信する．

Step2: 要求を受信したあるユーザー U_i は，同意取得要求の内容を確認し，その内容に同意する場合は「利用同意」項目と「BC 記録」項目を「同意」とし，「同意詳細」項目に同意要求に含まれる同意文書または同意文書を特定する ID を設定し，表 1 に示す「直接取得の同意」，「間接取得の同意」，または「第三者提供の同意」の記録形式の「同意 ID」項目以外を設定する．

Step3: U_i は，作成した記録形式に対して，$ID_{U_i}^{BC}$ と $W_{U_i}^{BC}$ を用いてトランザクション要求を作成し，BCPF に送信する[*1]．

Step4: BCPF は，受信したトランザクション要求に付された署名の検証に成功した場合，ノード間で合意形成を実行し，新たに TxID_j を付した結果をブロックチェーンに記録する．TxID_j が記録形式の「同意 ID」項目となる．

以降，ブロックに付された BCPF の署名の検証とブロックに記録された記録形式に付された U_i の署名の検証に合格したとき，ブロックの検証に成功したという．

ユーザーが同意を撤回する場合は，ユーザーは撤回を希望する同意要求の記録形式の「利用同意」を拒否とした記録形式を新たに作成し，上述と同様の処理でブロックチェーンに記録する．

4.3.3 個人データの直接取得

PF が，U_i からゲノムデータを取得する処理である．

Step1: PMS は，FES を介して，U_i から $ID_{U_i}^{PF}$ と個人データを受領し，一時的に保存する．

Step2: PMS は，$ID_{U_i}^{PF}$ に対応する $ID_{U_i}^{BC}$ をキーと検索クエリを送信し，BCPF から U_i の「直接取得の同意」が記録された全てのブロックを取得する．一時的に保存した個人データのデータ種別・項目に対応する「直接取得の同意」が記録された最新のブロックの検証に成功し，かつそのブロック中の「利用同意」項目と「BC 記録」項目がが「同意」であるときに限り，Step 3 以降の処理を継続し，それ以外の場合は一時的に保存した個人データを破棄し，以降の処理を中止する．

Step3: PMS は，一時的に保存した個人データから，$ID_{U_i}^{PF}$ とゲノムデータを除く「特定の個人を識別できる全ての情報」を取り除き，$ID_{U_i}^{PF}$ に対応するゲノムデータ専用仮名ユーザー ID $pID_{U_i,g}^{PF}$ を付した仮名データを作成し，PDS に送付する．また，$ID_{U_i}^{PF}$，$pID_{U_i,g}^{PF}$，および取り除いた全ての情報の対応関係を記録した仮名化管理表を作成し，保存する．

Step4: PDS は，受け取った仮名データを保存する．

Step5: PMS は，「直接取得の同意」の「同意 ID」項目の TxID_j を「本人の同意」項目とし，一時的に保存した個人データのデータ種別・項目を用いて「データ種別」項目と「データ項目」項目を設定し，また一時的に保存した個人データのハッシュ値を「データハッシュ値」項目，Step3 で作成した仮名化管理表のハッシュ値を「仮名対応ハッシュ値」項目として，表 2 の「直接取得時の記録」の記録形式を作成する（記録 ID 項目を除く）．そして，作成した記録形式に対して，ID_{PMS}^{BC} と W_{PMS}^{BC} を用いてトランザクション要求を作成し，BCPF に送付する．

Step6: BCPF は，受信したトランザクション要求に付された署名の検証に成功した場合，ノード間で合意形成を実行し，新たに TxID_j を付した結果をブロックチェーンに記録する．TxID_j が「直接取得の記録」記録形式の「記録 ID」項目となる．

Step7: PMS は，一時的に保存した個人データを削除する．

[*1] PMS にウォレット $W_{U_i}^{BC}$ の管理を委託している場合は，FES を介して BC クライアントサービスを用いて，クエリを作成して送付する．

4.3.4 個人データの間接取得

PF が，PS が U_i からの同意に基づいて収集された個人データの第三者提供を受けることで，個人データを取得する．匿名化管理者は，提供元となる PS の名称，住所，代表者の氏名，および PS が U_i からデータを収集する際に取得した同意文書/文書 ID を事前に把握しているとする．

Step1: PMS は，FES を介して，提供元となる PS から U_i の個人データを受領し，$ID_{U_i}^{PF}$ を当該個人データに付して一時的に保存する．

Step2: PMS は，$ID_{U_i}^{PF}$ に対応する $ID_{U_i}^{BC}$ をキーとした検索クエリを送信し，BCPF から U_i の「間接取得の同意」が記録された全てのブロックを取得する．一時的に保存した個人データのデータ種別・項目に対応する「間接取得の同意」が記録された最新のブロックの検証に成功し，かつそのブロック中の利用同意項目と BC 記録項目が「同意」であるときに限り，Step 3 以降の処理を継続し，それ以外の場合は一時的に保存した個人データを破棄し，以降の処理を中止する．

Step3: PMS は，ID_{PS}^{BC} を「提供元 ID」項目とし，PS から事前に取得した同意文書の内容が問題ないことが確認できた場合，「利用同意」項目を同意として，「同意詳細」項目を同意文書/文書 ID とし，表 1 の「取得経緯」の記録形式の同意 ID 項目以外の部分を作成する．そして，作成した記録形式に対して，ID_{PMS}^{BC} と W_{PMS}^{BC} を用いてトランザクション要求を作成し，BCPF に送付する．

Step4: BCPF は，受信したトランザクション要求に付された署名の検証に成功した場合，ノード間で合意形成を実行し，新たに TxID_j を付した結果をブロックチェーンに記録する．TxID_j が「取得経緯」記録形式の記録 ID 項目となる．

Step5: PMS は，一時的に保存した個人データから，$ID_{U_i}^{PF}$ と「特定の個人を識別できる全ての情報」を取り除き，$ID_{U_i}^{PF}$ に対応する仮名 ID $pID_{U_i}^{PF}$ を付した仮名データを作成し，PDS に送付する．また，$ID_{U_i}^{PF}$，$pID_{U_i}^{PF}$，および取り除いた全ての情報の対応関係を記録した仮名化管理表を作成し，保存する．ただし，ゲノムデータとの名寄せを防止するため，$pID_{U_i}^{PF}$ は，ゲノムデータ専用仮名ユーザー ID である $pID_{U_i,g}^{PF}$ と相異なるものが割り振られるとする．

Step6: PDS は，受け取った仮名データを保存する．

Step7: PMS は，「本人の同意」項目に Step2 で検証した「間接取得の同意」の「同意 ID」項目とし，「取得経緯の確認」項目に Step4 でブロックチェーンに記録された「取得経緯の確認」の「同意 ID」項目とし，一時的に保存した個人データのデータ種別・項目を用いて「データ種別」項目と「データ項目」項目を設定し，「データハッシュ値」項目を一時的に保存した個人データのハッシュ値とし，「仮名対応ハッシュ値」項目を Step5 で作成した仮名化管理表のハッシュ値とし，あらかじめ取得した提供者の提供元の名称，住所，代表者の氏名とを用いて「第三者の名称」項目，「第三者の住所」項目，「第三者の代表者」を設定し，表 2 の「間接取得時の記録」の記録形式の「記録 ID」以外の部分を作成する．そして，作成した記録形式に対して，ID_{PMS}^{BC} と W_{PMS}^{BC} を用いてトランザクション要求を作成し，BCPF に送付する．

Step8: BCPF は，受信したトランザクション要求に付

表 1　同意に関するブロックチェーン記録形式

項目	直接取得の同意	間接取得の同意	第三者提供の同意	取得経緯の確認
同意 ID	TxID	TxID	TxID	TxID
署名者 ID	$ID^{BC}_{U_i}$	$ID^{BC}_{U_i}$	$ID^{BC}_{U_i}$	ID^{BC}_{PMS}
年月日	YYYY/MM/DD	YYYY/MM/DD	YYYY/MM/DD	YYYY/MM/DD
本人 ID	$ID^{BC}_{U_i}$	$ID^{BC}_{U_i}$	$ID^{BC}_{U_i}$	
受領者 ID	ID^{BC}_{PMS}	ID^{BC}_{PMS}	$ID^{BC}_{\mathsf{PS}_i}$	
データ種別	種別 ID	種別 ID	種別 ID	種別 ID
データ項目	項目リスト	項目リスト	項目リスト	項目リスト
提供元 ID		$ID^{BC}_{\mathsf{PS}_i}$	ID^{BC}_{PMS}	$ID^{BC}_{\mathsf{PS}_i}$
利用目的 1	第三者提供のための保存	第三者提供のための保存	第三者提供	
利用目的 2			データ利用目的	
利用同意	同意/拒否	同意/拒否	同意/拒否	同意/拒否
BC 記録	同意/拒否	同意/拒否	同意/拒否	
同意詳細	同意文書/文書 ID	同意文書/文書 ID	同意文書/文書 ID	同意文書/文書 ID

された署名の検証に成功した場合，ノード間で合意形成を実行し，新たに TxID_j を付した結果をブロックチェーンに記録する．TxID_j が「間接取得の記録」記録形式の「記録 ID」項目となる．

Step9: PMS は，一時的に保存した個人データを削除する．

4.3.5　第三者提供

PF が，U_i の同意と PS_j の要求に応じて，保存している個人データを，実名データや仮名データに加工して第三者提供する．本小節では，仮名データの第三者提供を行う処理の一例を示す．匿名化管理者は，提供先となる PS_j の名称，住所，代表者の氏名をあらかじめ把握しているとする．

Step1: PMS は，FES を介して，PS_j が提供を希望するデータ種別，データ項目および利用目的を含む提供要求を受信する．

Step2: PMS は，PDS に受信したデータ種別とデータ項目を送信する．

Step3: PDS は，データ種別とデータ項目を含む仮名データを全て検索し，当該仮名データに付されている pID^{PF}_U のリストを PMS に返す．

Step4: PMS は，仮名 ID のリスト中の $pID^{PF}_{U_i}$ ごとに Step5-1 から Step5-3 の処理を実行する．

Step5-1: $pID^{PF}_{U_i}$ と仮名化管理表を用いて $pID^{PF}_{U_i}$ に対応する $ID^{BC}_{U_i}$ を特定し，$ID^{BC}_{U_i}$ をキーとした検索クエリを送信して，BCPF から $ID^{BC}_{U_i}$ の「第三者提供の同意」が記録された全てのブロックを取得する．

Step5-2: PS_j より指定されたデータ種別・項目に対応するものであり，「受領者 ID」項目が $ID^{BC}_{\mathsf{PS}_j}$ と一致し，「利用目的 2」項目が指定された利用目的を包含する「第三者提供の同意」が記録されたブロックを抽出する．抽出したブロックのうち最新のブロックの検証に成功し，かつそのブロック中の「利用同意」項目と「BC 記録」項目が「同意」であるときに限り，Step5-3 を実行し，それ以外の場合は $pID^{PF}_{U_i}$ に対する処理を終了する．

Step5-3: ($pID^{PF}_{U_i}$，Step5-2 で検証した最新ブロックの「同意 ID」項目) を，提供データ ID リストに加える．

Step6: PMS は，提供データ ID リストに記録されている（$pID^{PF}_{U_i}$，同意 ID）の全ての仮名 ID を PDS に送信する．提供データ ID リストに何も記録されていない場合は，PS_j に提供可能なデータが存在しない旨を通知し，処理を終了する．

Step7: PDS は，（$pID^{PF}_{U_i}$，$pID^{PF}_{U_i}$ と組で保存された仮名データ）を記録した仮名データリストを PMS に返す．

Step8: PMS は，Step7 で受信した提供データリスト中の（$pID^{PF}_{U_i}$，仮名データ）ごとに，Step9-1 から 9-3 を実行する．

Step9-1: PS_j 専用仮名 ID $pID^{PS_j}_{U_i}$ を決定し，提供データリストに（$pID^{PS_j}_{U_i}$，仮名データ）を記録する．

Step9-2:（$pID^{PF}_{U_i}$, $pID^{PS_j}_{U_i}$）を仮名化管理表に追加する．

Step9-3: Step5-3 で作成した提供データ ID リストから（$pID^{PF}_{U_i}$，同意 ID_i）を読み出して「本人の同意」項目を同意 ID_i を設定し，「第三者の名称」項目，「第三者の住所」項目，「第三者の代表者」項目に PS_j の名称，住所，代表者の氏名を設定し，提供する仮名データのデータ種別・項目を用いて「データ種別」項目と「データ項目」項目を設定し，「データハッシュ値」項目を提供する仮名データのハッシュ値とし，「仮名対応ハッシュ値」項目を（$pID^{PF}_{U_i}$，$pID^{PS_j}_{U_i}$）のハッシュ値と設定することで，表 2 の「第三者提供時の記録」の記録形式の記録 ID 以外の部分を作成する．そして，作成した記録形式に対して，ID^{BC}_{PMS} と W^{BC}_{PMS} を用いてトランザクション要求を作成し，BCPF に送付する．

Step10: BCPF は，受信したトランザクション要求に付された署名の検証に成功した場合，ノード間で合意形成を実行し，新たに TxID_j を付した結果をブロックチェーンに記録する．TxID_j が「第三者提供の記録」記録形式の「記録 ID」項目となる．

Step11: PMS は，提供データリストを PS に送付し，提供データ ID リスト，仮名データリストおよび提供データリストを削除する．

5.　評価

クラウド環境を利用して，4.2 と 4.3 節で与えた方式を試作し，ダミーデータを用いて動作確認と処理速度の測定を行った．試作において BCPF のノードは，匿名管理者が管理する 1 ノードと PS による管理を想定した 5 ノードで構成した．6 ノードからなる BCPF を構成したため，匿名化管理者等が管理にする 1 ノードが不正を試みたとしても，ブロックチェーン上に記録された同意および利用履歴を改ざんすることはできない．PMS が U_i から管理を委託される $ID^{BC}_{U_i}$ と $W^{BC}_{U_i}$ は，クラウド環境が提供する鍵管理サー

表 2　記録に関するブロックチェーン記録形式

項目	直接取得時の記録	間接取得時の記録	第三者提供時の記録
記録 ID	TxID	TxID	TxID
署名者 ID	ID^{BC}_{PMS}	ID^{BC}_{PMS}	ID^{BC}_{PMS}
年月日	YYYY/MM/DD	YYYY/MM/DD	YYYY/MM/DD
本人の同意	同意 ID	同意 ID	同意 ID
第三者の名称		提供元の名称	提供先の名称
第三者の住所		提供元の住所	提供先の住所
第三者の代表者		提供元の代表者の氏名	提供先の代表者の氏名
取得の経緯		同意 ID(取得経緯)	
データ種別	種別 ID	種別 ID	種別 ID
データ項目	項目リスト	項目リスト	項目リスト
データハッシュ値	取得データハッシュ値	取得データハッシュ値	提供データハッシュ値
仮名対応ハッシュ値	仮名対応ハッシュ値	仮名対応ハッシュ値	仮名対応ハッシュ値

ビスを用いて，匿名化管理者であっても署名鍵 $sk^{BC}_{U_i}$ 等を読み出せない実装を行った．さらに，ウォレット等を通じた $sk^{BC}_{U_i}$ の利用履歴は，匿名化管理者等でも編集ができないクラウド環境のログサービスを利用して蓄積し，監査等で監視する方法を採用した．

4.3.3 節から 4.3.5 節に示すように，PF は，有効な同意がブロックチェーン上で確認できない時には個人データの取得や提供を行わず，データの受領・提供を行ったときにはブロックチェーン上に法令で定められた記録を残す．つまり，デジタル署名の偽造等によるトランザクション要求の成りすましが成功したり，一定数以上のノードが結託することでブロックチェーン上の記録が不正に改ざんされない限り，要件 7 以外の要件を満たす．

PF において，$ID^{PF}_{U_i}$，$ID^{BC}_{U_i}$，$pID^{PF}_{U_i,g}$，$pID^{PF}_{U_i}$，および個人を特定しうる情報の対応関係を記録した仮名化対応表を保持しているのは PMS のみである．PMS の他に実名を特定しうる ID や情報を保持するのは，実名データを元々の保持している U_i と本人の同意に基づいて実名データの提供を受けた PS_i のみである．PF が実名データを提供する場合を除き，仮名データと実名データの対応を推測できる情報は PF から出力されないため，PS_i が結託しても，保有していない実名データを復元できない．また，データの取得・第三者提供時点でのデータと仮名化対応のハッシュ値をブロックチェーンに記録しているため，PF 内でデータの改ざんが起こったとしても，ブロックチェーン上の記録と照合することで改ざんの有無を検知できる．よって，定義 1 を満たすため，要件 7 も満たすといえる．

ゲノム情報プラットフォームの全てのユーザーは，BCPF を利用できるため，全ての同意と利用履歴を閲覧することができる．そして，同意履歴と利用履歴の整合性を検証することで，同意のない不正利用の有無等が確認でき，その妥当性を検証できる．よって，同プラットフォームは定義 2 の透明性を満たすといえる．

さらに，提供するデータに付す仮名 ID を提供先ごとに変更することで，提供先によるデータの名寄せを困難にする対策を施している．他のユーザーがブロックチェーン上の記録を閲覧できることに抵抗を感じるユーザーがいる場合は，ブロックへのアクセス制御を行うことで解決できるが，透明性は低下する．ブロックチェーンへのアクセス制御の導入の検討や PF の安全性証明は，今後の課題である．

試作した PF を用いて処理速度を計測したところ，ブロックチェーンへのトランザクション要求の応答に要した時間は 160ms から 400ms，ブロックチェーンからの検索クエリの応答に要した時間は約 2000ms であった．なお，処理速度測定時のブロックチェーンの長さは数十程度であった．今回の試作ではブロックチェーン上の検索処理に工夫を施していないため，高速化の余地があると考えられる．

参考文献

[1] 個人情報の保護に関する法律（平成十五年法律第五十七号）令和二年法律第四十四号による改正, https://elaws.e-gov.go.jp/document?lawid=415AC0000000057_20220401_502AC0000000044

[2] 個人情報保護委員会: 個人情報の保護に関する法律についてのガイドライン（通則編), https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf

[3] 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, https://www.meti.go.jp/press/2020/03/20210323003/20210323003-1.pdf (2020.03.23).

[4] プライベートブロックチェーン, https://event.samurai-incubate.asia/toshiba-oip2021/pdf/blockchain.pdf, In: TOSHIBA OPEN INNOVATION PROGRAM 2021, (2021).

[5] Nebula Genomics, https://nebula.org/whole-genome-sequencing-dna-test/

[6] LunaDNA, https://www.lunadna.com/

[7] Zenome, https://zenome.io/

[8] EncrypGen, https://encrypgen.com/

[9] DNAtix, https://www.dnatix.com/

[10] MedRec, https://medrec.media.mit.edu/

[11] Azaria A, Ekblaw A, Vieira T, Lippman A, MedRec: Using blockchain for medical data access and permission management. In: Proceedings of the 2nd International Conference on Open and Big Data (OBD). 2016

[12] Embleema, Embleema blockchain network v.2. Embleema WhitePaper, https://icocube.io/uploads/Embleema.pdf, (2018).

[13] Hu-manity.co https://hu-manity.co/my31app/