Vol.2018-CSEC-82 No.8
Vol.2018-SPT-29 No.8
2018/7/25

ブロックチェーンと中央集権型サーバの連携による実用的スマートコントラクトの実現手法

福光 正幸[1,a)]　長谷川 真吾[2,b)]　磯辺 秀司[2,c)]　岩田 直樹[4,d)]　岩崎 淳也[3,e)]　小泉 英介[2,f)]
中田 恒夫[4,g)]　酒井 正夫[2,h)]

概要：中央集権型の売買仲介サービスを利用して秘密情報の取引を行う場合, サービス運営事業者側の問題に起因する情報漏洩のリスクがある. この問題に対し, イーサリアムなどを用いた P2P 型取引であるスマートコントラクトが注目されている. しかし, 秘密情報のスマートコントラクトの実現には課題が多い. なぜなら, イーサリアムなどのスマートコントラクトでは契約内容がブロックチェーンに記載され全公開されるため, 売買する秘密情報自体を契約内容に直接書き込むことができず, 代わりにその秘密情報の特徴を説明するメタ情報のみを記載するのが一般的である. そのため, 秘密情報の販売者に悪意がある場合は, 契約内容に記載するメタ情報を誇張し購入者を錯誤させることで, 代金を不正に取得できる余地がある. さらに, イーサリアムでは, 契約内容の通りに忠実に処理するという特性上, そのような不正に臨機応変に対処することが困難であり, 仮に対処ができた場合でもその実施コストは高額である. そこで, 本稿では, スマートコントラクト処理における代金決済と不正裁定の処理のみを中央集権型サーバに委任する新しい方式を提案する. 提案方式では, サービス運営事業者側に起因する大規模情報漏洩のリスクを回避しつつ, 悪意のあるユーザによる不正を排除した健全かつ実用的な秘密情報のスマートコントラクトの実現が可能である.

A Method for a Practical Smart Contract by using Blockchain and Centralized Server

Masayuki Fukumitsu[1,a)]　Shingo Hasegawa[2,b)]　Shuji Isobe[2,c)]　Naoki Iwata[4,d)]
Jun-ya Iwazaki[3,e)]　Eisuke Koizumi[2,f)]　Tsuneo Nakata[4,g)]　Masao Sakai[2,h)]

1. はじめに

情報通信機器の発達とともに, 個人でも比較的容易に, 映像・音声・位置・心拍数などのいわゆるライフログと呼ばれる多様な個人データを収集・作成できるようになった. 今のところ, これらのデータの多くは作成した本人が自身のために利用する場合がほとんどであるが, ビックデータや AI 研究の発展とともに, 個人が保有するこれらのデータに注目している企業・研究者は増大していると考えられる. このようなデータを幅広く積極的に活用するためには, 個人データを効率的かつ安全に取引できる環境を整えることが重要である.

すでに広く流通している書籍や楽曲などのディジタルデータは, Amazon の Kindle ストア [1] や Apple の iTunes

[1] 北海道情報大学 情報メディア学部
Nishi-Nopporo 59-2 Ebetsu, Hokkaido, 069–8585 Japan
[2] 東北大学 教育情報基盤センター
Kawauchi 41, Aoba-ku, Sendai, Miyagi, 980–8576, Japan
[3] 東北大学 大学院医学系研究科
2-1 Seiryo-machi, Aoba-ku, Sendai, Miyagi, 980–8575, Japan
[4] 株式会社デンソー 先進モビリティシステム開発部
W Bld. 17F, 1-8-5, Konan, Minato-ku, Tokyo, 108–0075, Japan
[a)] fukumitsu@do-johodai.ac.jp
[b)] hasegawa@cite.tohoku.ac.jp
[c)] iso@cite.tohoku.ac.jp
[d)] NAOKI_A_IWATA@denso.co.jp
[e)] iwazaki@med.tohoku.ac.jp
[f)] koizumi@cite.tohoku.ac.jp
[g)] TSUNEO_NAKATA@denso.co.jp
[h)] sakai@cite.tohoku.ac.jp

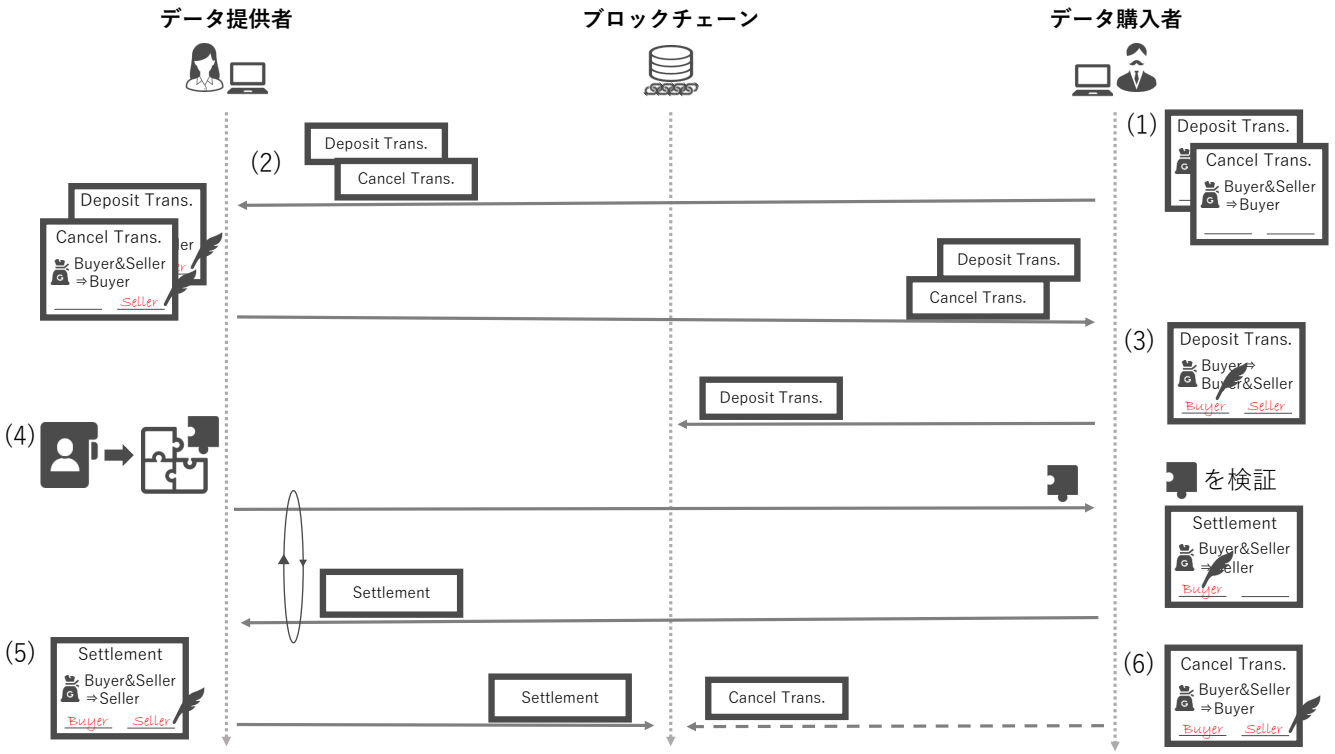

図 1 従来方式による秘密情報のスマートコントラクト

Store[2] などの中央集権型の売買仲介サービスを用いて取引されることがほとんどである．そのため，従来からある中央集権型のオンラインサービスと同様，サービス運営事業者のサーバが不正アクセスされることによる顧客情報の漏洩や改ざん，消失の問題 [3], [4] への対策は避けて通れない．また，サービス運営事業者は商品であるディジタルデータも自社のサーバで保存・管理することになるため，データそのものの漏洩や消失の問題への対策も必要である．

ディジタルコンテンツの売買に伴うこれらの問題を解決するためのアプローチとして，イーサリアム (Ethereum) [5] など，ブロックチェーン技術 [6] を用いた P2P (Peer to Peer) 型取引であるスマートコントラクト (Smart Contract) が注目されている．スマートコントラクトとは，不特定多数のノード群による協調処理により自動実行される契約のことである．スマートコントラクトを利用するメリットとして，その契約内容を実行する中央集権的な主体が不要であることや，契約がブロックチェーンに記載されるため，内容の改ざんが困難になることが挙げられる．例えば，Ujo Music[7] は，スマートコントラクトの仕組みを利用したコンテンツ売買仲介サービスの一つであり，楽曲の提供者と購入者の二者間での楽曲売買契約をブロックチェーンに記述する仕組みを採用している．これにより，仲介マージンの少ない楽曲の販売の仕組みを実現している．

しかし，個人データなど多様かつ機密性の高い秘密情報を取り扱う場合，既存のスマートコントラクトの仕組みをそのまま用いて売買することは困難であると考えられる．というのも，契約内容が書き込まれるブロックチェーンはその内容を全公開することが原則である．そのため，ブロックチェーンに売買する秘密情報自体を記載することはできない．したがって，ブロックチェーンには，その秘密情報のメタ情報のみを記載せざるを得ない．この場合，秘密情報の販売者は，偽または誇張したメタ情報を契約内容に記載することで，購入者を錯誤させることができる．すなわち，販売者が不正に代金を取得する余地が生まれる．また，イーサリアムの場合はその特性上，多様な不正に臨機応変に対処することが困難である．仮に不正に対処しようとした場合，その実施コストが高額になってしまうという，新たな問題が生じる．

そこで本稿では，不正な代金取得およびその対処にかかるコストの両方の問題を根本的に克服する，新しいスマートコントラクトの方式を提案する．その要点は，スマートコントラクト処理における代金決済と不正裁定の処理の部分を，中央集権型サーバに委任することである．これにより，サービス運営事業者に起因する大規模な秘密情報の漏洩リスクを回避しながら，かつ多様な不正への効率的な対処も可能になる．すなわち，本提案方式を利用することで，健全かつ実用的な秘密情報のスマートコントラクトを実現することができる．

以下，2 節では中央集権型サーバを必要としない，従来のスマートコントラクト方式とその問題点を述べる．3 節で新しい方式を提案した後，4 節で従来方式の問題点が，新方式を用いることでどのように解決するか解説する．最後に

5 節でまとめを述べる.

2. 従来方式

本節では，中央集権的な裁定者が存在しない二者間で秘密情報のスマートコントラクトを実施する従来方式について説明する.

具体例として，データ提供者が自身の個人データである秘密情報を 1[ETH] で販売し，データ購入者がそれを購入する事例を考える. このようなスマートコントラクトでは，データ提供者からデータ購入者への秘密情報送付と，データ購入者からデータ提供者への 1[ETH] の送金を同時に実施することは不可能である. そのため，どちらかの処理を先に実施する必要があるが，不正を排除する中央集権的な裁定者が存在しない二者間でのスマートコントラクトでは，後の処理が正しく実施されないリスクがある. 一般的な従来方式では, イーサリアム [5] とマルチ署名技術 [8] を用いることにより，不正リスクの低減を実現する [9]. 以下にその具体的手順を述べる（図 1 参照）.

(1) データ購入者は支払い能力を証明するために，「データ購入者のアドレスから 1[ETH] を，データ提供者とデータ購入者のマルチ署名アドレス（マルチ署名アドレスから別のアドレスに送金する場合はデータ提供者とデータ購入者の二人の署名が必要となる）に預託（送金）する」という**預託取引**を作成する. また，データ購入者は，このスマートコントラクトがキャンセルされるケースを想定して，「預託先マルチ署名アドレスから全額を，データ購入者のアドレスに返金する. ただし，この取引をブロックチェーンに登録できるのは特定日時 (nLockTime) 以降に限る. 」という**返金予約取引**も作成する. なお，この段階では，データ購入者は両取引に自身の署名を行わない.

(2) データ購入者は，作成した**預託取引**と**返金予約取引**をデータ提供者に送付して署名を依頼する. データ提供者は，両取引に自身の秘密鍵で署名してデータ購入者に返送する.

(3) データ購入者は，データ提供者から返送された両取引を受取り，**預託取引**に自身の秘密鍵で署名してブロックチェーンに登録することで，**預託取引**のみを確定させる.

(4) データ提供者は，ブロックチェーン上での**預託取引**の確定を確認後，商品である秘密情報を任意の N 個の部分データに細分化して，データ購入者に最初の 1 個を送付する. データ購入者は，データ提供者から受け取った最初の部分データの内容を検証して問題なければ，「預託先マルチ署名アドレスから，代金 $1/N$[ETH] をデータ提供者のアドレスに送金し，残額 $(N-1)/N$[ETH] をデータ購入者のアドレスに返金する」という**決済取引**を作成し, 自身の秘密鍵で署名して，データ提供者に送付する.

引き続き，データ提供者は $i(\geq 2)$ 番目の部分データをデータ購入者に送付し，データ購入者は受信した部分データの内容を検証後に「預託先マルチ署名アドレスから代金 i/N[ETH] をデータ提供者のアドレスに送金し，残額 $(N-i)/N$ をデータ購入者のアドレスに返金する」という送金内訳を更新した新しい**決済取引**を作成し, 自身の秘密鍵で署名して，データ提供者に送付する. この部分データの送付と**決済取引**の返送の処理は， N 個全て部分データに対して処理を終えるか，または，**返金予約取引**がブロックチェーンに登録可能になる特定日時 nLockTime 直前まで繰り返し実行される. なお，データ購入者は，データ提供者から受信した部分データの内容に問題があると判断した場合，データ提供者に**決済取引**を送付せず，このスマートコントラクトをその段階で途中終了しても良い.

(5) データ提供者は，**返金予約取引**がブロックチェーンに登録可能になる特定日時 nLockTime の前までに，データ購入者から受け取っている最新の**決済取引**に自身の秘密鍵で署名をしてブロックチェーンに登録することで代金受取を確定させる.

(6) データ提供者が**決済取引**を確定させなかった場合，データ購入者は特定日時 nLockTime 以降に**返金取引**に自身の秘密鍵で署名してブロックチェーンに登録することで返金を確定させる.

上記の手順 (4) において，データ提供者が秘密情報を複数の部分データに細分化して一つずつ送付したのは，データ購入者が秘密情報の全体を受け取ったにも関わらず代金を支払う**決済取引**を返送しない不正を防ぐための工夫である. しかし，このような工夫を行ったとしても，悪意のあるデータ購入者は，最初の部分データのみならば代金を支払わずに不正取得することが可能である. また，逆に悪意のあるデータ提供者は，データ購入者に正当だと錯誤させる部分データを作成することで，代金の一部を不正取得できる可能性がある. そして，不正を検知してスマートコントラクトを途中終了できた場合でも，**預託取引**と**返金予約取引**によるブロックチェーンのサイズ肥大化や被害者側でのマイニング手数料損失の問題が残る. さらに，購入者側での部分データの検証の際には，多様かつ狡猾な不正に臨機応変に対応する必要があり，その検証処理の自動化は困難である. したがって，ビックデータ解析や AI アルゴリズム研究に資するほどの大量の秘密情報の購入を従来方式で実施するのは現実的では無い.

3. 提案方式

本節では, 秘密情報のスマートコントラクト処理における代金決済と不正裁定の処理の部分を中央集権型サーバ (中央サーバ) に委任する, 新しい提案方式について説明する.

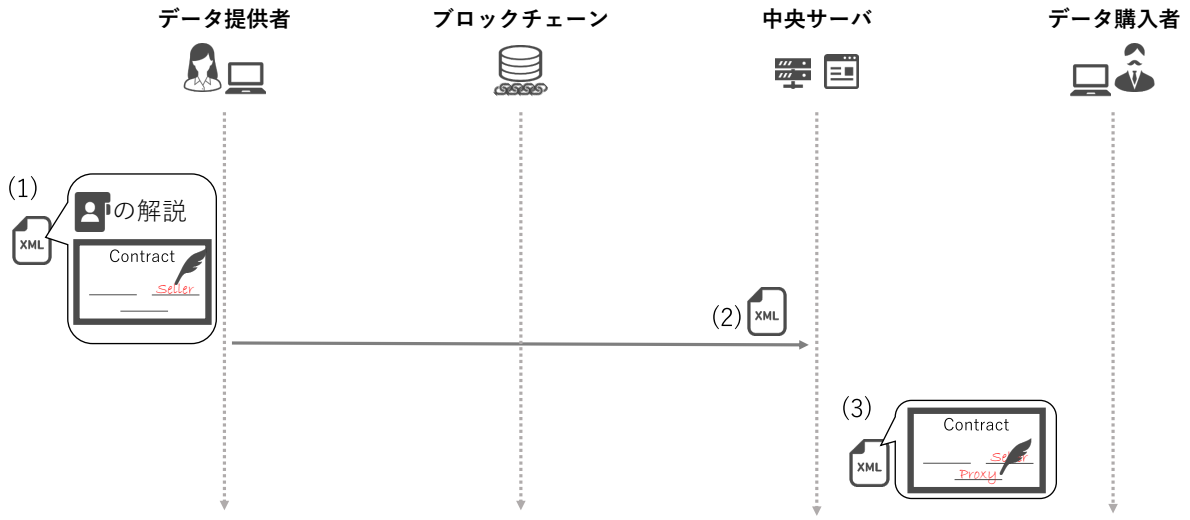

図 2　提案方式のデータ提供者によるデータ登録処理

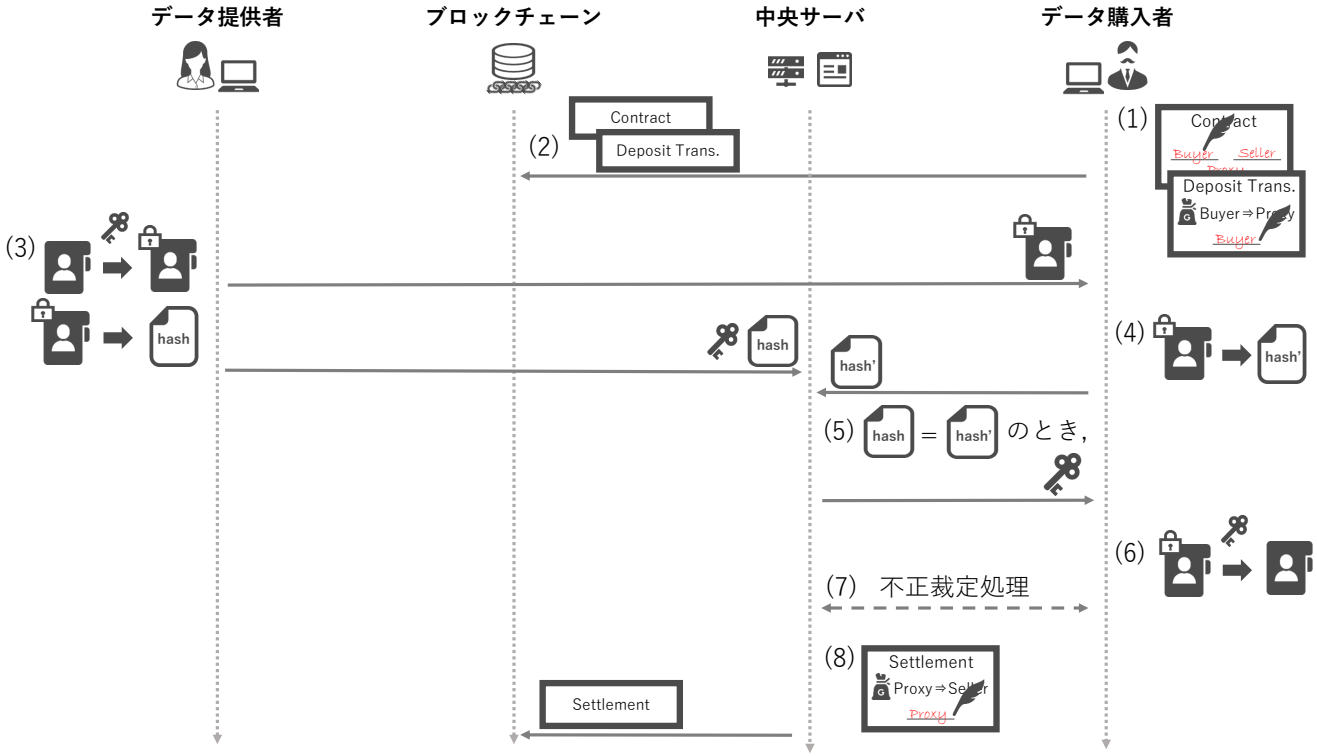

図 3　提案方式のデータ購入処理

提案方式はデータ登録処理とデータ購入処理の 2 つに大別される.

3.1　データ登録処理

提案方式におけるデータ登録処理を示す（図 2 参照）.

(1) データ提供者は, 販売する個人データの解説（メタ情報）を作成する. また, その販売条件などを定めた**契約書**を作成し, 自身の秘密鍵で署名する.

(2) データ提供者は, 解説と**契約書**のペアを, 個人データの販売用カタログとして中央サーバに送付する.

(3) 中央サーバは受信したカタログを検証し, 問題がなければ中央サーバの秘密鍵で**契約書**に署名を行い, カタログを公開する.

3.2　データ購入処理

提案方式におけるデータ購入処理を示す（図 3 参照）.

(1) データ購入者は, 中央サーバが公開しているカタログデータ群から購入するデータを選択し, その**契約書**に自身の秘密鍵で署名する. また, データ購入者は, 「データ購入者のアドレスから中央サーバのアドレスに代金と手数料を預託（送金）する」という**預託取引**を作成して, 自身の秘密鍵で署名する.

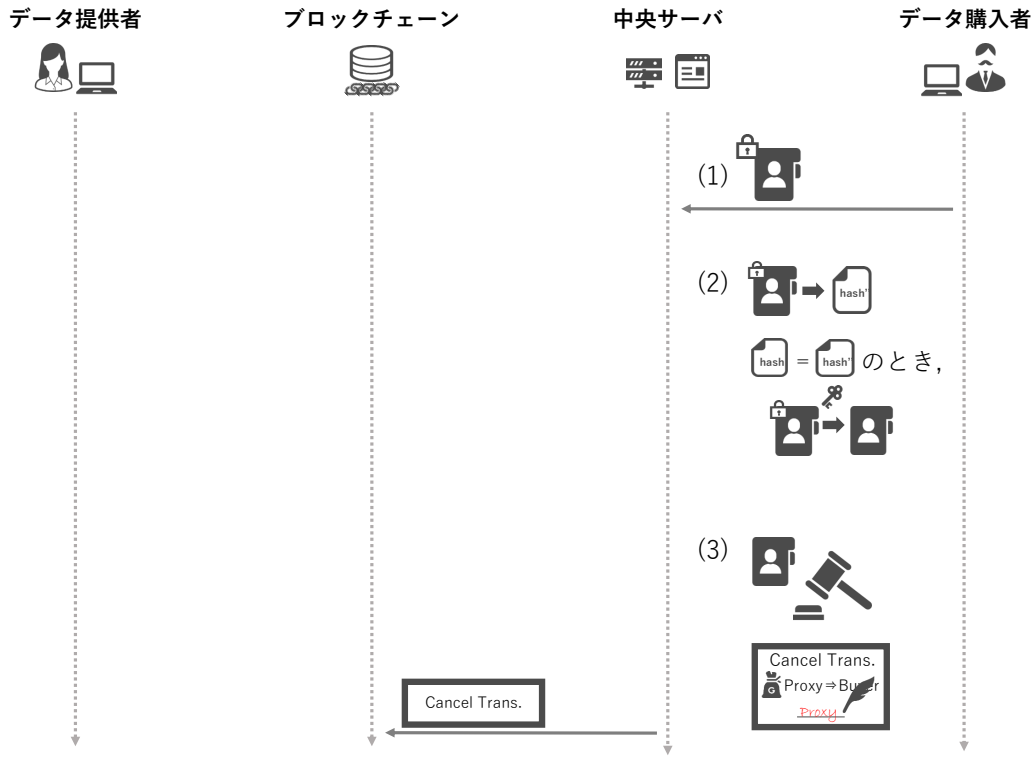

図 4　提案方式の中央サーバによる不正裁定処理

(2) データ購入者は, 署名した**契約書**と**預託取引**をブロックチェーンに登録する. ブロックチェーンに**預託取引**が登録されることで, データ購入者から中央サーバに購入データの代金と手数料が預託される.

(3) データ提供者は, 自身が登録した個人データに関する**契約書**がブロックチェーンに登録されているのを発見した場合, ワンタイムキー（乱数列）を用いて対象データの暗号化を行い, 暗号データを購入者へ送信する. また, そのワンタイムキーと暗号データのハッシュ値を中央サーバに登録する.

(4) データ購入者は, データ提供者から受信した暗号データのハッシュ値を計算し, 中央サーバに送信する. なお, データ提供者から暗号データが届かない場合, データ購入者が中央サーバにその旨を申告し, 中央サーバが預託金（代金と手数料）をデータ購入者に返金（後述の 3.3 節 (3) を参照）して取引を中止する.

(5) 中央サーバは, データ提供者とデータ購入者の双方から受信したハッシュ値が一致した場合, ワンタイムキーをデータ購入者に送付する. なお, データ提供者からワンタイムキーと暗号データのハッシュ値が届かない場合, または, ハッシュ値が一致しない場合, 中央サーバが預託金をデータ購入者に返金（後述の 3.3 節 (3) を参照）して取引を中止する.

(6) データ購入者は, 中央サーバから受信したワンタイムキーで暗号データを復号する.

(7) データ購入者は, 復号データの検証を行い, もし問題があれば中央サーバに不正裁定（後述の 3.3 節を参照）を依頼する.

(8) 契約成立から一定時間以内に, 取引が中止されず, また, データ購入者から依頼された不正裁定において不正と判定されなかった場合, 中央サーバは「中央サーバのアドレスからデータ提供者のアドレスに代金を送金する」という**決済取引**を作成して, 中央サーバの秘密鍵で署名してブロックチェーンに登録する. ブロックチェーンに**決済取引**が登録されることで, 中央サーバからデータ提供者に代金が送金される.

3.3　中央サーバによる不正裁定処理

本節では, 上述した中央サーバによる不正裁定の処理について説明する（図 4 参照）.

(1) データ購入者は,「データ購入処理（3.2 節）」の (6) で得られた復号データの内容に問題があった場合, 暗号データを証拠として添付して中央サーバに不正裁定を依頼する.

(2) 中央サーバは, 証拠として添付された暗号データのハッシュ値を計算し, それが登録されているものと一致した場合, その暗号データを登録されているワンタイムキーで復号する. 一方, ハッシュ値が一致しなかった場合は, 不正とは判定せずに不正裁定処理を終了する.

(3) 中央サーバは, 復号データの内容を検証して不正裁定を行う. そして, 不正（復号データに問題がある）と判断した場合, 中央サーバは「中央サーバのアドレス

からデータ購入者のアドレスに代金と手数料を送金する」という**返金取引**を作成して, 中央サーバの秘密鍵で署名してブロックチェーンに登録する. ブロックチェーンに**返金取引**が登録されることで, 中央サーバからデータ購入者に代金と手数料の全額が返金される.

4. 考察

本節では, 2 節で指摘した従来方式の問題に対する提案方式の有効性と, 中央サーバが不正アクセスの攻撃を受けた場合の情報漏洩リスクについてそれぞれ考察する.

4.1 悪意のあるユーザによる不正な利益取得が可能な問題に対する有効性

従来方式では代金が後払いであるため, 悪意のあるデータ購入者は, 商品である秘密情報を, N 分割したうちの最初の分割データのみならば, 代金を支払わずに不正取得することが可能であった. しかし, 提案方式では事前に中央サーバへの代金の預託が必要なため, そのような不正はできない. また, 提案方式では, 悪意のあるデータ購入者が, 正規の手順により購入データの復号・取得を完了した後に, 購入データの暗号データとハッシュ値が衝突する別データを何らかの方法で作成して, これを中央サーバに証拠として添付して不正裁定を依頼することにより返金を受ける, という不正が想定される. しかし, ハッシュ値の衝突困難性を破ることは実際には困難であり, そのような不正の実施も容易ではない.

また, 従来方式ではデータ購入者側での分割データの不正検証が困難なため, 悪意のあるデータ提供者は, データ購入者に正当だと錯誤させる部分データを作成することで, 代金の一部を不正取得することが可能であった. しかし, 提案方式では, データ購入者は（部分データではなく）完全な状態での購入データに対する不正検証を実施可能であり, また, データ購入者が不正を検知した場合には, 中央サーバに不正裁定を依頼することができる. さらに, 中央サーバは, データ購入者から証拠として添付された暗号データを復号・検証することで, 証拠に基づく不正裁定を実施可能である. そして, 中央サーバが不正と判定した場合には, 預託されていた代金と手数料がデータ購入者に返金され, 悪意のあるデータ提供者には一切の代金も支払われない.

以上のように, 提案方式では, 悪意のあるユーザによる不正な利益取得を困難にすることができる.

4.2 不正な取引が蔓延する問題に対する有効性

従来方式では, 悪意のあるユーザによる不正な利益取得が可能なため, シビル攻撃 [10] によりシステム全体では膨大な数の不正な取引が蔓延する恐れがあった. 仮に不正を検知して取引を途中で中止できた場合でも, 預託取引と返金予約取引の登録によるブロックチェーンのサイズ肥大化や被害者側でのマイニングの手数料損失が発生する問題が残る. また, データ購入者側において部分データに対する不正検証を自動化することが難しいため, 不正な取引が蔓延する従来方式では, ビックデータ解析や AI アルゴリズム研究に資するほどの大量の秘密情報を購入することも困難であった.

一方, 提案方式では, 悪意のあるユーザによる不正な利益取得が困難なため, 不正な取引の実施数自体が大幅に削減されると期待できる. 結果的に, 不正な取引に起因するブロックチェーンのサイズ肥大化を抑制できる. また, 被害者側でのマイニング手数料損失に関しても, 仲介サービスで利益を上げている中央サーバによる信頼維持コストにより補填されることが期待できる. さらに, 提案方式では中央サーバによる不正裁定と返金のしくみにより, 不正な取引によりデータ購入者が損失を被る恐れがないため, データ購入者は大量の秘密情報を安心して購入できる.

4.3 中央サーバが不正アクセスされた場合の情報漏洩リスク

提案方式では, 中央サーバが, スマートコントラクト処理における代金決済と不正裁定に関して中央集権的な存在となる. 本節では, その中央サーバが不正アクセスされた場合の情報漏洩リスクについて考察する.

中央サーバは, 「データ登録処理（3.1 節）」の (2) で取引データである秘密情報の解説と契約書のペアを, また, 「データ購入処理（3.2 節）」の (3) で秘密情報の暗号データのワンタイムキーと暗号データのハッシュ値を, それぞれデータ提供者から受け取り保存する. しかし, 中央サーバが保存しているこれらのデータのみから, 秘密情報そのものを得ることは（秘密情報の暗号データが不足しているため）不可能である.

一方, 「不正裁定処理（3.3 節）」が発生した際には, 中央サーバは, データ提供者から不正の証拠として秘密情報の暗号データを受け取ることができるため, 事前にデータ提供者から受け取っているワンタイムキーを利用して暗号データを復号することで, 秘密情報そのものを得ることができてしまう. しかし, これはデータ購入者が不正裁定を依頼した場合のみに発生する例外的な状況であり, 大部分の正常な取引の際には起こりえない. すなわち, 中央サーバが保持する秘密情報は多くないと考えられる.

以上の理由により, 中央サーバが不正アクセスされた場合でも, 取引データである秘密情報が大規模に漏洩するリスクは低いと考えられる.

5. おわりに

本稿では, 実用的な秘密情報のスマートコントラクトを可能にする新しい方式を提案した. また, 提案方式では, 代金決済と不正裁定の処理のみを中央サーバに委任すること

で, 悪意のあるユーザによる不正な利益取得を根本的に排除可能であること, さらに, 中央サーバによる秘密情報に対するアクセス権を不正裁定処理のための必要最低限に限定することで, 中央サーバ側の問題に起因する大規模な秘密情報の漏洩リスクを回避できることも示した.

提案方式を用いることで, サービス運営事業者によるガバナンスが強化され, 従来は困難であった健全かつ実用的な秘密情報のスマートコントラクトの実施が可能となる.

参考文献

[1] Amazon Inc., Amazon Kindle, https://www.amazon.co.jp/, 最終アクセス: 2018/5/20.
[2] Apple Inc., Apple iTunes, https://www.apple.com/jp/itunes/, 最終アクセス: 2018/5/20.
[3] Dave Lee, Uber concealed huge data breach, BBC News, http://www.bbc.com/news/technology-42075306, 最終アクセス: 2018/5/20.
[4] 朝日新聞社, GMO、顧客情報1万4600件が流出 不正アクセスか, 朝日新聞 DIGITAL, https://www.asahi.com/articles/ASKBZ52P1KBZULFA011.html, 最終アクセス: 2018/5/20.
[5] Ethereum Foundation, Ethereum Blockchain App Platform, https://www.ethereum.org/, 最終アクセス: 2018/5/20.
[6] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, 2008.
[7] Ujo Music, Ujo Empowering Music, https://ujomusic.com/, 最終アクセス: 2018/5/20.
[8] K. Itakura and K. Nakamura, ”A public-key cryptosystem suitable for digital multisignatures”. NEC J.Res.Dev.71 (Oct.1983).
[9] 藤井達人, ビットコイン 次の革新“ライトニングネットワーク”, MUFG, https://innovation.mufg.jp/detail/id=111, 公開日: 2016/11/16.
[10] John R. Douceur, “The Sybil Attack,” In Proc. of the IPTPS02 Workshop, pp. 251-260, http://dl.acm.org/citation.cfm?id=687813, 2002.