様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 １５ 日現在

機関番号：１３７０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2021
課題番号：１８Ｋ０４１３３

研究課題名（和文）データ駆動型サービスのためのプライバシーを考慮したデータ共有に関する研究

研究課題名（英文）Study on Data Sharing for Data-Driven Services

研究代表者
毛利　公美（Mohri, Masami）

岐阜大学・工学部・准教授

研究者番号：５０２８１６９７

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：データ駆動型サービスを支えるクラウドストレージは，ユーザが保存したデータの完全性が保たれているかを確認できる監査機能が求められる．データの提供者や分析者，利用者が関わり合うIoTエコシステムのように様々な主体がデータを取り引きできる環境の構築には認証機能と認可機能も関係する．本研究では，提供者の特別な処理は不要とする第三者による監査と，分散型認証，協調型認可のシステムを設計している．

研究成果の学術的意義や社会的意義
クラウドストレージサービスの信頼性を向上させ，流通するデータの真正性を確保する要素技術の確立は，新しい価値を創造する持続可能なサービスの構築・運用に資すると期待される．

研究成果の概要（英文）：Cloud storage supporting data-driven services requires an audit function to verify the integrity of data stored by users. Authentication and authorization functions are also relevant to the construction of an environment where various entities can trade data, such as in an IoT ecosystem where data providers, analysts, and users interact with each other. This research investigated a third-party auditing system that does not require any additional processing by the user, as well as a distributed authentication system and a cooperative authorization system.

研究分野：情報通信工学

キーワード：クラウド　監査　ディジタル・フォレンジック

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

データ提供者とデータ利用者の間で真正性を持つデータの流通をなし得る技術により，サイバー空間に蓄積されるデータを活用した新しい価値を創造する持続可能なデータ駆動型サービスの構築・運用に資することが期待されている．

２．研究の目的

クラウドストレージシステムはデータ共有を円滑に行うために不可欠なものであり，またデータ駆動型サービスの中核として利用されていく．クラウドシステムは一般に大きくパブリックとプライベートの 2 つに分類される．今日では，ユーザは利用する状況に応じて 2 種類のクラウドシステムを使い分けながら利用する形態が一般的となってきている．いずれの種類のクラウドにおいても，クラウドストレージサービス提供者によるその容量の節約や運用コストの削減のための意図的な操作，あるいは意図しない操作ミスによって，クラウドストレージに保存しているデータが欠損し完全性が損なわれてしまう事態が起こり得る．多くのユーザが利用している大規模なクラウドストレージサービスにおいて，バックアップ技術等をもってしてもデータを復元できないような事故が発生し，データが損なわれる可能性を考慮しておかなければならない．データ駆動型サービスを支えるクラウドストレージを実現するために，ユーザが保存したデータの完全性が保たれているかを確認できるシステムが求められている．データの提供者や分析者，利用者がお互いに関わり合いながら共存共栄を目指す IoT エコシステムのように，様々な主体がオープンにデータを取り引きできる環境の構築に貢献する認証と認可の技術も求められている．

３．研究の方法

信頼性がユーザから見て明らかではないクラウドストレージにクライアントがファイルの保持を委託するような状況を考える．Provable Data Possession（PDP）はストレージに保管されているファイルが，ユーザが保存した元のファイルと同じであるか否かを検証する手法である．本研究ではデータの完全性が保たれていることを確認できる PDP について検討している．PDP の機能があれば，もしもデータ損失があったときにユーザは被害範囲の拡大抑制や被害事実の立証などの行動がとれ，他方のクラウドストレージサービスは無事故の状態で運用を続けていることを対外的に示すことでサービスの信用を得られるなどの効果が期待される．また，データ駆動型サービスに適うデータの提供者と利用者の認証と，データ利用者の属性に応じて提供するデータを指定できる認可の技術を検討している．

４．研究成果

クラウドにデータが存在するかを確かめるには，ユーザがクラウドに保存しているデータをすべて取り出し，ユーザ自身が手元の記録と照合する等で確認するのが単純な方法である．しかし，この方法では保存しているデータが多くなるにつれ検証時間が長くなる．また，多くのデータをクラウドからユーザのストレージに戻してくるときに多くの通信量を必要とする．そこで預けたデータが削除・改ざんされることなく確かにクラウドストレージに存在することを確認する Provable Data Possession（PDP）という概念がある．

PDP は保存しているデータを複数のブロックに分割し，その中からランダムに選んだブロックに対してユーザもしくは第三者の監査者がファイルの完全性検証を行う方法である．確率的にデータの完全性を検証することで，単純な方法よりも少ない計算コストとなる．PDP には，ユーザがサーバとファイルの完全性を検証する private verifiability と，ユーザが第三者である監査者に監査を依頼し監査者とサーバが検証する public verifiability の二種類のモデルが存在する．private verifiability な PDP の一般的な処理は以下のようになる．まずユーザのクライアントは，クラウドストレージに保存したいファイルを複数のファイルブロックに分割し，ファイルの所有検証フェーズで使用するメタデータをファイルブロックに対して生成する．ユーザは，ファイルとファイルブロックに対応したメタデータ全てをクラウドストレージにアップロードする．次に，ファイルの所有検証フェーズでは，ユーザはクラウドストレージにランダムなチャレンジを送る．チャレンジを受け取ったクラウドストレージは，メタデータの中からいくつかをランダムに選択する．そして選んだメタデータとチャレンジからプルーフを求め，ユーザに送る．そしてプルーフを受け取ったユーザはチャレンジとプルーフを用いて，クラウドストレージのファイル所有の有無を判別する．public verifiability な PDP では，ユーザが第三者である監査者に監査を依頼し，クラウドストレージに対してユーザの代わりに監査者が検証する．そして監査処理を行った監査者は監査結果をユーザに伝えるという方法である．本研究では，ユーザ側の計算コストを削減するために public verifiability のモデルに該当する PDP を考えている．先に　　述べたように既存の PDP ではユーザが完全性検証に使用するメタデータを生成し，ユーザまたは第三者である監査者が完全性を検証する．実世界でのクラウドストレージの利用を鑑みると，大半のユーザはファイルのアップロードのみを行う．ユーザ側はファイルに対

して暗号化などの付加的処理を行うことはほとんどなく，クラウド側がファイルの暗号化を行い保存するストレージサービスが多い．本研究では，ユーザはファイルのアップロードの処理のみを行い，既存の監査方式と同様に第三者による監査を可能とするシステムの実現を目指した．すなわち，監査に使用するメタデータ生成をユーザではなくクラウドストレージが行うようにし，ファイルの完全性を第三者である監査者が検証する形となる．

メタデータの生成をクラウドストレージが行えるようになれば，ユーザに特別な変更を求めることがなく監査を行うことができる．本研究では，ユーザはファイルのアップロードのみを実行し，第三者による監査を可能とする透過型 PDP と呼ぶモデルを提案している．透過型 PDP モデルを用いることで，既存のクラウドストレージシステムのユーザアプリケーションを変更することなく監査を行うことが可能になる．さらに，透過型 PDP のシステムモデルの具体的構成法として，離散対数問題に基づく透過型 PDP 方式を与えている．提案方式はクラウドストレージの監査に用いる証拠の偽造防止(Integrity Protection)や，悪意のある監査者がファイルの内容を知れないようにする(Privacy Protection)安全性があることを示している．また各主体の計算量は既存方式と同じか，それより低い計算量で監査を実行できることを確認している．特にユーザの計算量は，クラウドストレージがメタデータを生成することでゼロにしている．

クラウドストレージから監査者にデータの一部が漏洩することなくプライバシーが保護される形のデータ共有ができることと同様に，誰がどのデータを取引したのかの保証がデータの信頼性を確保するには求められる．すなわち，取引主体の本人性の保証はデータ駆動型サービス基盤を支える要素技術である．主体の本人性を保証する方法として，公開鍵基盤（Public Key Infrastructure，PKI）が広く利用されている．公開鍵基盤は，信頼できる第三者機関である認証局が主体と公開鍵の関連を証明書により保証する基盤であり，電子署名による通信相手の確認に利用されている．認証局を絶対的に信頼することが前提なので，認証局は外部不正／内部不正に対抗できるような高度なセキュリティ対策や人材育成など，技術面や運用面での対策が必要となる．しかしながら，認証局へのクラッキングや認証局の不適切な運用により不正な証明書が発行された事例が発生している．公開鍵基盤による主体間の信頼関係の形成に関して，ある主体 A が信頼する認証局が別の主体 B の本人性を保証している場合，主体 A は主体 B の本人性を信頼する．さらに，別の主体 C／主体 D が認証局から本人性の保証を受け，公開鍵基盤に参加することで，主体 A の信頼関係は主体 C／主体 D へと拡がっていく．このように，認証局には多数の主体の信頼点が集約されていく．インターネットのサーバ認証では，主に，主体 A はサービス利用者，主体 B／主体 C／主体 D はサービス提供者であり，サービス利用者はサービス提供者の本人性を信頼してサービスを利用する．認証局を単一信頼点とすることで，サービス提供者はサービス利用者との直接のやり取りなしに信頼関係を構築できる．しかしながら，認証局から不正な証明書が発行された場合，悪意のある主体 X を正規のサービス提供者と見分けることができない．その結果，認証局を基点として形成された全ての主体間の信頼関係が損なわれることとなる．

本研究では，認証局を各サービス提供者に分散させる分散型の認証基盤の構築を目指している．各サービス提供者に分散された信頼点の接続には「相互認証」が利用できる．しかしながら，対向の認証局の評価と相互認証の実施は属人的になっており，各サービス提供者が各々の判断で相互認証するだけでは，システム全体として適切に信頼関係が構築されていることを検証できない．この属人的な作業を自動化するために，スマートコントラクトを用いた相互認証方式を提案している．スマートコントラクトは，分散台帳技術において，分散台帳に格納された情報や入力値に基づいて分散台帳への操作を制御する機能である．各サービス提供者が統一された規則で相互認証を実行できるように，相互認証を行う枠組みをスマートコントラクトで実現している．提案方式により分散型認証基盤に参加する主体は不正を行わないことを前提として，外部の攻撃者による認証局の乗っ取りと偽造に対して安全であることを示している．

取引相手が誰であるかの認証と合わせて，取引相手がどのような属性を持っているかに応じて共有するデータの種類や量などを選択できることが望まれる．データの中には価値の高い情報を含み，流出すれば多大な経済的損失を被るものが存在するからである．データの共有を実現するために，User-Managed Access（UMA）と呼ばれる認可プロトコルに注目する．UMA はオンラインサービスにおけるデータ共有やリソースアクセスの認可処理をサービスユーザが制御できることを目指して策定されたプロトコルである．本研究では UMA の考え方を基本として認可システムを設計している．単純に UMA に従う場合，認可データベースは単一の管理者によって管理されるため，管理者が認可情報を不正に書き換えたとしてもシステム利用者は検証できない．認可データベースを利害が必ずしも一致しない複数の管理者によって管理されれば，ある特定の管理者が認可情報を書き換えたとしても他の管理者によって不正が確認されるという考えのもとに，UMA にブロックチェーンを統合した認可システムを設計している．

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　3件）

| | |
|---|---|
| １．著者名<br>Mazen Alowish, Yoshiaki Shiraishi, Yasuhiro Takano, Masami Mohri, Masakatu Morii | ４．巻<br>8 |
| ２．論文標題<br>Stabilized Clustering Enabled V2V Communication in an NDN-SDVN Environment for Content Retrieval | ５．発行年<br>2020年 |
| ３．雑誌名<br>IEEE Access | ６．最初と最後の頁<br>135138～135151 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/ACCESS.2020.3010881 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Kenta Nomura, Yoshiaki Shiraishi, Masami Mohri, Masakatu Morii | ４．巻<br>8 |
| ２．論文標題<br>Secure Association Rule Mining on Vertically Partitioned Data Using Private-Set Intersection | ５．発行年<br>2020年 |
| ３．雑誌名<br>IEEE Access | ６．最初と最後の頁<br>144458～144467 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/ACCESS.2020.3014330 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Shohei Kakei, Yoshiaki Shiraishi, Masami Mohri, Toru Nakamura, Masayuki Hashimoto, Shoichi Saito | ４．巻<br>8 |
| ２．論文標題<br>Cross-Certification Towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric | ５．発行年<br>2020年 |
| ３．雑誌名<br>IEEE Access | ６．最初と最後の頁<br>135742～135757 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/ACCESS.2020.3011137 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

〔学会発表〕　計24件（うち招待講演　0件／うち国際学会　4件）

| |
|---|
| １．発表者名<br>東 知哉, 白石 善明, 掛井 将平, 毛利 公美, 森井 昌克 |
| ２．発表標題<br>オンライン投票システムの投票者インタフェースのためのWeb API |
| ３．学会等名<br>情報処理学会マルチメディア，分散，協調とモバイル（DICOMO2021）シンポジウム |
| ４．発表年<br>2021年 |

１．発表者名
土井 貴仁，廣友 雅徳，福田 洋治，毛利 公美，白石 善明

２．発表標題
ブロックチェーンを用いたメンタルポーカープロトコルの提案

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム

４．発表年
2021年

１．発表者名
中山 太雅，廣友 雅徳，福田 洋治，毛利 公美，白石 善明

２．発表標題
HQC暗号を応用した秘匿内積計算プロトコル（III）

３．学会等名
電子情報通信学会暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
Shinobu Ogiso, Masami Mohri, Yoshiki Shiraishi

２．発表標題
Transparent Provable Data Possession Scheme for Cloud Storage

３．学会等名
2020 International Symposium on Networks, Computers and Communications (ISNCC)（国際学会）

４．発表年
2020年

１．発表者名
江澤友基，掛井将平，白石善明，瀧田愼，毛利公美，森井昌克

２．発表標題
User-Managed Accessに基づくクロスドメイン認可フレームワーク

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム

４．発表年
2020年

１．発表者名
小木曽仁，毛利公美，白石善明

２．発表標題
クラウドストレージの透過型データ所有証明

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム

４．発表年
2020年

１．発表者名
坂川巧将，廣友雅徳，福田洋治，毛利公美，白石善明

２．発表標題
Raspberry Piを用いたIoTハニーポットの開発

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム

４．発表年
2020年

１．発表者名
中山太雅，廣友雅徳，福田洋治，毛利公美，白石善明

２．発表標題
HQC暗号を応用した秘匿内積計算プロトコル（II）

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム

４．発表年
2020年

１．発表者名
岩原主，毛利公美，白石善明

２．発表標題
Webサイトに認証・認可機能を付加するサービスコンテナ

３．学会等名
情報処理学会第83回全国大会

４．発表年
2021年

１．発表者名
冨田裕涼，毛利公美，白石善明

２．発表標題
事前学習言語モデルによる関連文書検索　～コンピュータセキュリティシンポジウム論文ナビゲーションシステム～

３．学会等名
情報処理学会第83回全国大会

４．発表年
2021年

１．発表者名
Y.Ezawa, M.Takita, Y.Shiraishi, S.Kakei, M.Hirotomo, Y.Fukuta, M.Mohri, M.Morii

２．発表標題
Designing Authentication and Authorization System with Blockchain

３．学会等名
The 14th Asia Joint Conference on Information Security（国際学会）

４．発表年
2019年

１．発表者名
M.Hirotomo, H.Ito, Y.Fukuta, M.Mohri, Y.Shiraishi

２．発表標題
Identification Scheme Based on the Binary Syndrome Decoding Problem Using High-Density Parity-Check Matrices

３．学会等名
The 14th Asia Joint Conference on Information Security（国際学会）

４．発表年
2019年

１．発表者名
T.Tsuchida, M.Hirotomo, H.Ito, M.Takita, Y.Shiraishi, K.Nomura, M.Mohri, Y.Fukuta, M.Morii

２．発表標題
A Signature Scheme Based on the Syndrome Decoding Problem Using LDPC Codes

３．学会等名
The 14th Asia Joint Conference on Information Security（国際学会）

４．発表年
2019年

１．発表者名
池田貴志，廣友雅徳，福田洋治，毛利公美，白石善明

２．発表標題
ブロックチェーンを用いたログ保存システム

３．学会等名
電子情報通信学会技術研究報告（情報通信システムセキュリティ）

４．発表年
2020年

１．発表者名
江澤友基，掛井将平，白石善明，瀧田　愼，毛利公美，森井昌克

２．発表標題
ブロックチェーンを用いたユーザ中心の認可プロトコルの一実装 ～ User-Managed AccessのHyperledger Fabricによる実装 ～

３．学会等名
電子情報通信学会技術研究報告（情報通信システムセキュリティ）

４．発表年
2020年

１．発表者名
久岡　黎，福田洋治，廣友雅徳，毛利公美，白石善明

２．発表標題
大学内におけるセキュリティ違反の意識調査の検討

３．学会等名
情報処理学会第82回全国大会

４．発表年
2020年

１．発表者名
江澤 友基，瀧田 愼，白石 善明，髙野 泰洋，毛利 公美，森井 昌克

２．発表標題
ブロックチェーンを用いた認証システムの検討

３．学会等名
電子情報通信学会技術研究報告（情報通信システムセキュリティ）

４．発表年
2018年

１．発表者名
江澤 友基，瀧田 愼，白石 善明，髙野 泰洋，毛利 公美，森井 昌克

２．発表標題
ブロックチェーンを用いた認証・認可システムの設計と実装

３．学会等名
情報処理学会コンピュータセキュリティシンポジウム

４．発表年
2018年

１．発表者名
江澤 友基，掛井 将平，瀧田 愼，白石 善明，髙野 泰洋，毛利 公美，森井 昌克

２．発表標題
OpenIDで認証情報を発行するブロックチェーンを用いた認証・認可システム

３．学会等名
電子情報通信学会技術研究報告（情報通信システムセキュリティ）

４．発表年
2018年

１．発表者名
土田 敏生，瀧田 愼，白石 善明，毛利 公美，髙野 泰洋，森井 昌克

２．発表標題
ブロックチェーンに格納した認証情報を用いる認証方式

３．学会等名
電子情報通信学会技術研究報告（情報通信システムセキュリティ）

４．発表年
2018年

１．発表者名
小木曽 仁，毛利 公美，白石 善明

２．発表標題
監査者に提出する証拠を選択可能としたクラウドストレージのデータ所有証明

３．学会等名
電子情報通信学会技術研究報告（情報通信システムセキュリティ）

４．発表年
2018年

１．発表者名
掛井 将平，白石 善明，毛利 公美，森井 昌克

２．発表標題
匿名性を考慮したTPMを用いるSSLクライアント認証

３．学会等名
電子情報通信学会技術研究報告（情報通信システムセキュリティ）

４．発表年
2018年

１．発表者名
土田 敏生，瀧田 愼，白石 善明，毛利 公美，髙野 泰洋，森井 昌克

２．発表標題
自己主権型身分証明のためのブロックチェーンを用いた擬似ランダム関数に基づく認証方式

３．学会等名
電子情報通信学会技術研究報告（情報通信システムセキュリティ）

４．発表年
2019年

１．発表者名
江澤 友基，掛井 将平，瀧田 愼，白石 善明，毛利 公美，髙野 泰洋，森井 昌克

２．発表標題
ブロックチェーンを用いた認証・認可システムとデータ流通プラットフォームの一実現法 ～ IoTデバイス向けWebベースクラウドストレージ ～

３．学会等名
電子情報通信学会技術研究報告（情報通信システムセキュリティ）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|
| 研究分担者 | 白石　善明<br>(Shiraishi Yoshiaki)<br>(70351567) | 神戸大学・工学研究科・准教授<br>(14501) | |

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
| --- | --- |