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　 ９ 日現在

機関番号：１４５０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ１１９６３

研究課題名（和文）実世界データの流通のためのアクセス制御に関する研究

研究課題名（英文）Study on Access Control for Real-world Data Exchange

研究代表者
白石　善明（Shiraishi, Yoshiaki）

神戸大学・工学研究科・准教授

研究者番号：７０３５１５６７

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）：異分野連携による価値創出を促進する上で，各ドメインで蓄積されるリソースを共有することは有効である．複数ドメインのリソースを掛け合わせることで，従来では得られなかった新たな知見を獲得することが期待される．組織間でリソースを共有する際には双方が同意することになり，その確認がスムーズに実施できれば異分野連携の促進に貢献できる．本研究ではデータを利活用したい組織同士が自由に取引できるリソース共有エコシステムを実現するための，ブロックチェーンを用いたクロスドメイン認可システムのアーキテクチャを中心に，認証・認可・監査のアクセス制御の要素技術を開発している．

研究成果の学術的意義や社会的意義
ライフスタイル，ヘルスケア，インダストリなどの様々な領域でIoTをベースにしたアプリケーションの利用が加速していく．サービスを提供するスマートデバイスはユーザに関する様々なデータを取得し，リソースサーバに蓄積する．認可機能は各種デバイスがリソースへアクセスする権限を持っているか検証し，アクセスの可否を判断する役割を果たす．データ駆動型サービスの実現を支えるためにますます増加するスマートデバイスを適切にアクセス制御する上で，複雑化するシステムに対応するための高度化の需要に応えるリソース共有エコシステムの構築に資する認可システムを中心とした技術を開発している．

研究成果の概要（英文）：In order to promote value creation through interdisciplinary collaboration, it is effective to share resources accumulated in each domain. By crossing the resources of multiple domains, it is expected that new knowledge that could not be obtained in the past will be acquired. When resources are shared among organizations, both parties must agree to the sharing, and smooth confirmation of this agreement will contribute to the promotion of interdisciplinary collaboration. This research has developed essential technologies for access control such as authentication, authorization, and auditing, focusing on the architecture of a cross-domain authorization system using blockchain to realize a resource sharing ecosystem in which organizations that wish to utilize data can freely trade with each other.

研究分野：情報セキュリティ

キーワード：アクセス制御　認可　認証　監査

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

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サイバーフィジカルシステムのデータ駆動型サービスにおいては，データの提供者と利用者の間で真正性が保証されたデータの流通が必須である．このときデータの目的外利用への懸念を解消することが不可欠である．

２．研究の目的

本研究では安全にデータの取引を行えるようにするデータ流通基盤のアクセス制御に関する開発を行う．所有者とデータ利用者の間，異なるデータ利用者の間でデータ交換を安心して行えるための要素技術を検討している．

３．研究の方法

データ利用者はデータ所有者が直接決められるアクセス制御を実現するリソース管理範囲のドメインを横断した認可の管理を実現する．利用者が設定する認可に関する全ての情報をブロックチェーンに記録することで，認可システムが侵害を受けても設定された認可情報の完全性が維持される特徴を持たせる．

４．研究成果

Internet of Things（IoT）の普及とそれを活用する人や企業は増加の一途をたどっており，膨大な量のデータが生成・蓄積されている．IoT をベースにしたアプリケーションはヘルスケアやライフスタイル，工場などの領域で成功している．サービスを提供するスマートデバイスはこれらの領域でユーザに関する様々なデータを取得し，リソースサーバに蓄積している．認可システムは，リソースサーバに蓄積されるリソースへのスマートデバイスによるアクセスを制御するための仕組みで，スマートデバイスがリソースへアクセスする権限を持っているか検証し，アクセスの可否を判断する役割を果たす．例えば，あるユーザが使用するスマートデバイスが蓄積するリソースに他のユーザがアクセスしようとした場合，認可システムの検証によってそのユーザにはアクセス権限がないと判断されると，そのユーザはそのリソースにアクセスできない．正当な権限を持つユーザにのみリソースへのアクセスを許可するという情報セキュリティの基本的な考え方において，認可システムは不可欠な構成要素である．つまり，データ駆動型サービスの実現を支えるためにますます増加するスマートデバイスを適切にアクセス制御する上で，認可システムはなくてはならない機構であることに変わりはないと同時に複雑化するシステムに対応する高度化が求められる．

新たな価値を創出するために，異なるドメインに所属する組織が連携する動きが活発になっている．異分野連携による価値創出を促進する上で，各ドメインで蓄積されるリソースを共有することは有効である．複数ドメインのリソースを掛け合わせることで，従来では得られなかった新たな知見を獲得することが期待される．組織間でリソースを共有する際には双方の承認が重要になるが，その確認がスムーズに実施できれば異分野連携の促進につながる．

クロスドメイン認可システムは異なるドメイン間でリソースを共有するための仕組みとして注目されている．認可システムは一般的にドメイン毎に独自に構築されるため，ドメインを跨いだアクセスを制御することはできない．クロスドメイン認可システムは，このような異なるドメインに所属するエンティティによるリソースへのアクセスを認可できる．そのため，アナログな手段で実施していた承認にかかるコストを削減できる．

クロスドメイン認可を実現するフレームワークに OAuth がある．OAuth を用いることで，ユーザはクライアントアプリケーションを通して，あるドメインで自身が所有するリソースをドメインの異なる別のサービスでも利用できる．しかし OAuth では，ユーザ自身とは異なる第三者へリソースを共有するケースは考慮されていない．また，リソースを管理するシステム毎に認可の設定が必要であり，リソース管理システムの数に比例して認可の管理にかかるコストが増大する．第三者へのリソース提供を可能とするクロスドメインでの認可を実現するためには，軽量で第三者への権限委任が可能な機構が必要である．第三者へのリソース提供が可能なクロスドメインでの認可を実現できれば，それは新たな価値創出に貢献するであろう．

User-Managed Access は，リソース管理システムがもつ認可の機構を分離・統合することで，リソース管理システムを横断した認可の管理を実現する．また，第三者への認可ができるように考慮されており，データリソースの多様な連携に対応できる．しかし，統合された認可システムは単一の第三者組織によって管理される．認可システムが単一の第三者組織によって運営されると，信頼が単一の組織に集中し，認可処理の透明性が欠如する．したがって，単一信頼点における内部不正やシステムの乗っ取りによって，設定された認可に関する情報が侵害されても，システムの利用者はそれを検知できない．このようなセキュリティ上の脅威に対処するため，いくつかのシナリオを想定したブロックチェーンベースの認可スキームが提案されている．

ブロックチェーンは，信頼された特定の中央機関を介することなくネットワークを運営し，複

数の参加者が同じ内容の台帳を分散して保持できる仕組みである．ノード間で台帳の整合性を維持するための仕組み（=コンセンサス・アルゴリズム）を通して，取引が実行された際にそのトランザクションを台帳に記録してもよいかどうかをブロックチェーンネットワークの参加者が検証し，問題がなければその取引データをブロックチェーンに書き込む．ブロックチェーンでは，検証されたトランザクションがブロックと呼ばれるデータの塊として記録される．各ブロックには取引データと，一つ前に生成されたブロックのハッシュ値があわせて格納される．もし過去に生成されたブロックに含まれるデータの改ざんを試みた場合，改ざんしたブロック以降のハッシュ値も全て計算し直す必要があるため，改ざんは計算量的に困難である．ブロックチェーン上でプログラムを実行できる技術としてスマートコントラクトがある．ブロックチェーン上でスマートコントラクトが実行されると，その結果が改ざん困難な状態で台帳に記録される．

本研究では，認可システムを衆人環視の下に配置することで，単一信頼点の侵害による完全性の崩壊を防止する．また，ブロックチェーンネットワークの参加者は認可処理の検証に参加できるため，処理内容の透明性を確保できる．さらに，認可システムとリソース管理システムが疎に結合していることで，リソース管理システムは認可管理を認可システムに委任でき，複数のリソース管理システムでリソースを所有する組織は認可システムを通して一括でリソースの認可を設定できる．すなわち本研究は，信頼の分散と疎な結合の両方を実現するクロスドメイン認可システムはこれまで提案されていないことに着目している．各組織がデータリソースを所有し，それらを共有することで新たな知見を得ることをモチベーションとして，本研究では，そのようなリソース共有エコシステムを実現するためのクロスドメイン認可システムのアーキテクチャを提案している．具体的には，ブロックチェーンベースのスキームを用いて認可システムへの信頼を分散し，認可フレームワークの UMA のコンセプトに基づいて設計することで第三者への権限委任と，認可システムとリソース管理システムの疎結合を実現する．結果として，提案フレームワークでは，異なるドメインに属する組織間で柔軟にアクセスを制御でき，セキュアなリソース共有を実現する．

本研究の設計原則は以下の通りである．ドメインごとの認可サーバの運用は，リソース所有者が所属するドメインの数に比例して，リソース所有者による認可の管理の負担が増加する．その結果，ドメイン横断的なリソースの利用が阻害されることとなる．そこでまず本研究では，ドメイン横断的な認可の仕組みとして UMA を利用する．UMA は，リソース管理システムがもつ認可の機構を分離・統合することで，リソース管理システムを横断した認可の管理を実現する仕組みである．認可システムが統合されることで，リソース所有者のリソースの管理の負担が軽減される．他方で，統合された認可システムは単一信頼点となるので，認可処理を請け負うドメインの数が増加するほど，UMA での障害が与える影響が大きくなる．リソース所有者の観点からは，この障害はリソースサーバにおける機密性と可用性の侵害を引き起こす．機密性に関しては，認可システムにおいて，内部不正やシステムの乗っ取りによって，設定された認可に関する情報が侵害されてもシステムの利用者はそれを検知できず，侵害されたまま利用してしまうことである．これは，システム内の情報を不正に書き換えることが可能であること，及び認可処理の内容が利用者にとって不透明であることに起因する．そこでこれらの障害に対抗するには，(i)認可システムで管理される認可情報の改ざん耐性，及び(ii)認可システムで実施される認可処理の透明性向上の二点が求められる．次に，可用性に関しては，認可システムのサーバがダウンした場合に，システムの利用者は認可システムによって保護する複数のリソースサーバの認可管理ができなくなることである．これは，単一信頼点として構成される認可サーバが単一障害点になってしまうことに起因する．したがってこの課題を解決するためには，(iii)認可システムにおける単一障害点を排除する必要がある．これら(i)〜(iii)の要件を満たすシステムを構築するために，以下の方針に基づいてシステムを設計する．

方針 1: UMA フレームワークで定義される認可サーバ上の各エンドポイントをスマートコントラクトで構築し，ブロックチェーン上に認可処理及び認可情報を記録する．

方針 2: 認可サーバ，リソースサーバ，及びクライアントの三者間で実施される各処理の内容を，スマートコントラクトを通してトランザクションとして記録する．

方針 1 より，認可情報や認可ポリシーをシステム側で不正に改ざんされることを防ぐ．また，システムを構成するノードの一つがダウンしてもブロックチェーンを構成する他のノードが認可処理を継続して実施できる．よって，(i)及び(iii)の要件を満たす．方針 2 より，ブロックチェーンネットワークに参加するシステム利用者に認可処理内容が可視化され，要件(ii)を満たす．

本研究では以上のようなデータを利活用したい組織同士が自由に取引できるリソース共有エコシステムを実現するための，ブロックチェーンを用いたクロスドメイン認可システムのアーキテクチャを提案し，そのユースケースを示した．ブロックチェーンベースのスキームを用いて認可システムへの信頼を分散し，認可フレームワークの UMA のコンセプトに基づいて設計することで第三者への権限委任と，認可システムとリソース管理システムの疎結合を実現している．実装評価により，リソースサーバやクライアント数に対する処理時間と台帳サイズの増加傾向を調査し，スケーラビリティがあることを確認している．また，既存のブロックチェーンを用いる認可システムとは異なる性質を持つことを確認している．言語命令や外部アクセスによって生じる非決定性に対して注意をすることで運用に問題ないことを確認している．

以上のクロスドメイン認可システムを中心に，認証機能と監査機能の開発を進め，安全にデー

タの取引を行えるデータ流通基盤に対するアクセス制御に関する多面的なアプローチを行った.

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　4件）

１．著者名 Alowish Mazen、Shiraishi Yoshiaki、Mohri Masami、Morii Masakatu	４．巻 14
２．論文標題 Three Layered Architecture for Driver Behavior Analysis and Personalized Assistance with Alert Message Dissemination in 5G Envisioned Fog-IoCV	５．発行年 2021年
３．雑誌名 Future Internet	６．最初と最後の頁 29pages
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/fi14010012	査読の有無 有
オープンアクセス 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 －

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

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

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

〔学会発表〕　計28件（うち招待講演　1件／うち国際学会　6件）

1．発表者名
東 知哉，白石 善明，掛井 将平，毛利 公美，森井 昌克

2．発表標題
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
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
2021年

1．発表者名
熊谷 圭太，掛井 将平，白石 善明，齋藤 彰一

2．発表標題
分散型台帳への秘密鍵の封入による協同運用可能な公開鍵証明書発行基盤の検討

3．学会等名
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
2021年

1．発表者名
Shohei Kakei, Yoshiaki Shiraishi, Shoichi Saito

2．発表標題
Simplifying Dynamic Public Key Certificate Graph for Certification Path Building in Distributed Public Key Infrastructure

3．学会等名
International Conference on Information and Communication Technology Convergence（国際学会）

4．発表年
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
東 知哉，白石 善明，今村 光良，掛井 将平，廣友 雅徳，森井 昌克

２．発表標題
NFT流通プロセスにおける不正検知のための監査システム

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
廣友 雅徳，嘉戸 裕一，白石 善明，今村 光良，森井 昌克

２．発表標題
ブロックチェーンを用いた重複データ排除機能付きマルチクラウドストレージ監査方式

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
野村 健太，高田 雄太，熊谷 裕志，神薗 雅紀，白石 善明

２．発表標題
電子証明書を取り巻く仕組みの分析とその活用

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
熊谷 圭太，掛井 将平，白石 善明，齋藤 彰一

２．発表標題
分散台帳への秘密鍵の封入による協同運用可能な公開鍵証明書発行基盤の実装と評価

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
掛井 将平，今村 光良，白石 善明，廣友 雅徳，齋藤 彰一

２．発表標題
分散台帳技術におけるユーザの同意に基づくアクセス制御フレームワーク

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
Shohei Kakei, Yoshiaki Shiraishi

２．発表標題
Distributed Ledger Technology for Authentication and Authorization: Meta-PKI and Cross-Domain Authorization

３．学会等名
International Conference on Machine Learning & Blockchain Technologies（招待講演）（国際学会）

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
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
西本拓矢，福田洋治，廣友雅徳，白石善明

２．発表標題
IoT機器上で動作するプログラムの改ざん検知で用いるホワイトリストの作成方法の検討

３．学会等名
電子情報通信学会総合大会

４．発表年
2021年

１．発表者名
井上翼，福田洋治，廣友雅徳，白石善明

２．発表標題
準同型暗号を用いた秘匿検索のログ解析への応用

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
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
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

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

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