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　　元 年　　６ 月 １９ 日現在

機関番号：１４５０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１８４

研究課題名（和文）データ流通プラットフォームでのデータ所有者の開示先制御に関する研究

研究課題名（英文）Study on Access Control for Data Sharing

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）　　3,600,000円

研究成果の概要（和文）：交通インフラ，設備管理などの多岐にわたる分野でデバイスからのデータを活用した新しい価値の創造が期待され，機器同士が通信するM2MやIoTへの注目が高まっている．データ所有者による開示先制御が可能なデータ流通プラットフォームをデータを保管する主体の存在するモデルで実現することを目指して，本研究では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全に行う要素技術の開発を行った．

研究成果の学術的意義や社会的意義
交通インフラ，設備管理，エネルギー管理，医療など多岐にわたる分野で，機器同士が通信するM2MやIoTが注目されている．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の創造が期待される中で，データ漏えいやデータ利用者の悪用等の懸念が高まってきている．そのような懸念を緩和・払拭するために，本研究はデータ所有者の意思に応じてデータの開示先が制御をするデータ流通プラットフォームを実現する技術を開発した．

研究成果の概要（英文）：Towards data-driven value creation which is expected in various domains such as transportation infrastructure, facility management, etc., M2M and IoT in which devices communicate with each other are basic technologies. With the aim of realizing a data sharing platform that allows data owners to control the disclosed destination, in this study, the elemental technologies to perform data exchange safely have been researched.

研究分野：情報セキュリティ

キーワード：アクセス制御　認証　認可

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

交通インフラ，設備管理，エネルギー管理，医療など多岐にわたる分野で，機器同士が通信する M2M や IoT への注目が高まっている．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の創造が期待される中で，データ利用者の悪用等の目的外利用への懸念が高まってきている．データ所有者の意思に応じてデータの開示先が制御できれば，悪用等の懸念を緩和，払拭できる可能性がある．データ保管者にデータを預ける際の所有者の懸念事項は，(1)データ保管者の閲覧，(2)第三者によるデータの不正な入手，(3)データの不正な二次利用であり，これらを解消するシステムが求められている．また，データを提供する所有者は，安心してデータを提供できるかどうかについて，技術がいかに優れているかということだけで判断はしていないと考えられる．所有者が安心して使えるデータ共有プラットフォームの構築にあたっては，ポリシー制御が適切に行える技術の開発だけでは不十分である．

２．研究の目的

本研究では，所有者が安心してデータを提供するために，二つの研究項目を設定する．

1. 所有者主導でデータ流通ができる開示先制御方式の開発
2. データ流通プラットフォームに対する心理面の分析

まず，所有者主導で開示先制御が可能なデータ流通プラットフォームを，データを保管する主体の存在するモデルで実現することを目指し，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要素技術の開発を行う．そして，データ流通プラットフォームにデータを提供する所有者の安心感を高めるためにサービス開発者やサービス運用者が留意すべき心理的な点を明らかにする．

３．研究の方法

本研究では，(1)データ保管者はデータの閲覧ができない，(2)開示許可のない者はデータを利用できない，(3)利用許可のないものはデータの二次利用の防止や抑止がなされる，これらの要件を満たすデータ流通方式の設計を行う．具体的には，暗号化クラウドストレージの構成と，認証システムおよび認可システムの構成を検討する．また，データを活用するシステムの利用者の安心感について分析する．

４．研究成果

クラウドストレージのアクセス制御に適した暗号に属性ベース暗号（Attribute-Based Encryption: ABE）があり，暗号化を行うユーザが復号可能な相手を制御できる暗号文ポリシー属性ベース暗号（Ciphertext-Policy Attribute-Based Encryption: CP-ABE）がある．CP-ABE では秘密鍵に関連付けられている属性集合が，暗号文に関連付けられているアクセス構造を満たす場合にのみその秘密鍵によって暗号文を復号することができる．単一の信頼されている機関が秘密鍵を生成する方式だけでなく，複数の機関が発行する属性で ABE を構成する検討がなされている．複数機関が秘密鍵を生成する ABE では信頼できる中央機関（a trusted central authority: CA）とグローバル識別子を用いて構成される方式があるが，CA はすべての暗号文を復号できるため，CA を排除して個々の機関がすべての情報を持たないようにするアプローチがある．単一の機関がすべての情報を管理する場合には，機関が敵からの攻撃にあったときに属性の管理に関わる情報がすべて知られてしまう恐れがあり，管理情報を分散しなければならない．そのようにユーザの秘密鍵を生成する際に，複数の機関が個々の秘密情報を隠したまま秘密鍵を生成できる方式も提案されている．秘密鍵の生成とともに実際の運用では鍵を使えないように失効させることは重要な課題である．属性に有効期限を設けてそれを超過した後に正当なユーザのみに新しい鍵を配布することで鍵を失効させる方式は前方秘匿性を満たさない．前方秘匿性とは一度属性を失効したユーザはそこから先は復号できないことをいう．属性に期限を設けて鍵の失効を行う場合，任意の時刻で特定のユーザを失効させようとしても有効期限に達するまではそのユーザは復号可能となる．したがって即時に失効が可能な方式が望ましい．ユーザが新たに属性を取得したり，属性を失効したりした場合，ユーザ自身が秘密鍵の更新を行う方式は提案されているが，本研究では属性の失効の際に秘密鍵が変化しない特長を持つ CP-ABE 方式を設計した．不正ユーザとストレージが結託する攻撃モデルと属性失効ユーザによる攻撃モデルの両方について，標準モデルのもと Decisional Bilinear Diffie-Hellman（DBDH）仮定において提案方式は選択平文攻撃（Chosen-Plaintext Attack）に識別不可能性（Indistinguishability）を持つという IND-CPA 安全であることを証明し，データの機密性，結託耐性，前方秘匿性を満たすことを示した．

クラウドストレージをはじめとするデータ流通プラットフォームにおいては認証技術と認可技術が必要不可欠である．認証システムと認可システムがサービスに依存せずにユーザ情報や権限情報を共有することができれば，従来のサービスごとに独立した運用に比べて利便性が向上する．ブロックチェーンを認証と認可のデータベースとして利用することを本研究では検討した．ブロックチェーンとは複数のノードに分散された台帳上に情報を記録し，その台帳を各ノードが監視することで情報の改ざんを防ぐ機能を持っている．台帳が公開されているため，情報の透明性が保たれるという特徴もある．データベースに記録された情報が中央集権的に管理されていると履歴を残さずに書き換えることが可能である．ブロックチェーンネットワーク

では公開台帳を互いに監視することで情報の不正な書き換えが困難であり，情報の真正性と透明性が保証される．ブロックチェーンを認証データベースとして利用する考え方に基づいた認証サービスは存在するが，証明者と検証者が密にリンクする形で運用することになり，複数のプロバイダのサービスを連携したデータ活用を目指すならば，証明者・認証基盤・検証者の三者は互いに独立した関係を持つことが望ましいと考えられる．中央集権的な技術である Public Key Infrastructure（PKI）のような認証システムを非中央集権的な技術のブロックチェーンで設計をする取り組みでは，Identity（ID）を認証する主体が存在しない．Web of Trust を認証の起点とするブロックチェーン PKI の提案もあるが，ID を認証する主体は不特定多数の参加者に委ねられている点は信頼性が低い．そこでアカウントを認証するシステムが高信頼に機能するために鍵管理に関与する第三者の存在を考える．本研究では，シングルサインオンのフレームワークと連携するアプローチにより，中央集権的な認証システムにより発行された ID に基づいて認証情報をブロックチェーンに登録することでオープンに利用可能な認証基盤の設計をした．あわせて認可のデータベースも同様にブロックチェーンに登録する認可基盤の設計をした．この認証・認可基盤の実現例として，Web ベースのプロトコルとして実装し，Web ベースクラウドストレージと連携することで概念実証をした．

システムにデータを保管する場合，システムの障害や故障，また利用者の操作ミスによって，情報の紛失や漏えいが起こる恐れがある．従来まで情報セキュリティ技術によって情報システムの安全性を高めることで利用者は安心してシステムを利用できると考えられてきた．これに対して，セキュリティ技術によって与えられる客観的安全性と利用者が感じる安心感にずれが生じることが報告されている．既存研究では，安心感の因子としてセキュリティ技術，信用，ユーザビリティ，知識，経験，プリファレンスを挙げている．また，プライバシー情報を登録する利用者に対して，能力・知識，安全性，ユーザビリティ・プリファレンス，身近な他者，主観的な信用の 4 因子が抽出されている．クラウドサービスの間接利用の不安因子の調査では，オペレーションスキルが低いことに起因する過失，組織における情報システムの利用や運用管理についてのポリシーやガイドライン・教育の不備，クラウドサービスやネットワークの障害，クラウド事業者の知名度や実績・評判の 4 因子が抽出されている．本研究の調査では，システムの利用者が感じる安心感として，安全管理体制，信用，プリファレンス，知識，ユーザビリティ，セキュリティ技術，他者，経験の因子が抽出され，論理的要因と主観的要因に分けられた因子モデルが妥当であることを確認した．

５．主な発表論文等

〔雑誌論文〕（計 7 件）

1. Daiki ITO, Kenta NOMURA, Masaki KAMIZONO, Yoshiaki SHIRAISHI, Yasuhiro TAKANO, Masami MOHRI, Masakatu MORII, Modeling Attack Activity for Integrated Analysis of Threat Information, IEICE Transactions on Information and Systems, Vol.E101-D, pp.2658-2664, 2018.
   DOI: 10.1587/transinf.2017ICP0015
2. Yoshiaki SHIRAISHI, Masanori HIROTOMO, Masami MOHRI, Taisuke YAMAMOTO, Delivering CRL with Low Bit Rate Network Coded Communication for ITS, IEICE Trans. on Information and Systems, Vol.E100-D, No.10, pp.2440-2448, 2017.
   DOI: 10.1587/transinf.2016OFP0009
3. Yoshiaki SHIRAISHI, Kenta NOMURA, Masami MOHRI, Takeru NARUSE, Masakatu MORII, Attribute Revocable Attribute-Based Encryption with Forward Secrecy for Fine-Grained Access Control of Shared Data, IEICE Trans. on Information and Systems, Vol.E100-D, No.10, pp.2432-2439, 2017.
   DOI: 10.1587/transinf.2016OFP0008
4. Kenta NOMURA, Masami MOHRI, Yoshiaki SHIRAISHI, Masakatu MORII, Attribute Revocable Multi-Authority Attribute-Based Encryption with Forward Secrecy for Cloud Storage, IEICE Trans. on Information and Systems, Vol.E100-D, No.10, pp.2420-2431, 2017.
   DOI: 10.1587/transinf.2016OFP0004
5. Kenta NOMURA, Masami MOHRI, Yoshiaki SHIRAISHI, Masakatu MORII, Multi-Group Signature Scheme for Simultaneous Verification by Neighbor Services, IEICE Trans. on Information and Systems, Vol.E100-D, No.8, pp.1770-1779, 2017.
   DOI: 10.1587/transinf.2016ICP0029

〔学会発表〕（計 23 件）

1. 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，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 ～，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），2018 年.
2. 土田 敏生，瀧田 愼，白石 善明，毛利 公美，髙野 泰洋，森井 昌克，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，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），2018 年.

3. 小木曽 仁，毛利 公美，白石 善明，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，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），2018 年.
4. 土田 敏生，瀧田 愼，白石 善明，毛利 公美，髙野 泰洋，森井 昌克，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，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），2018 年.
5. 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，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，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），2018 年.
6. 江澤 友基，瀧田 愼，白石 善明，髙野 泰洋，毛利 公美，森井 昌克，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，情報処理学会コンピュータセキュリティシンポジウム，2018 年.
7. 江澤 友基，瀧田 愼，白石 善明，髙野 泰洋，毛利 公美，森井 昌克，ブロックチェーンを用いた認証システムの検討，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），2018 年.
8. 伊東 春香，廣友 雅徳，福田 洋治，毛利 公美，白石 善明，LDPC 符号を用いたリング署名方式について，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），2018 年.
9. 近藤 秀紀，永井 達也，伊藤 大貴，野村 健太，神薗 雅紀，白石 善明，古本 啓祐，瀧田 愼，髙野 泰洋，毛利 公美，森井 昌克，Structured Threat Information eXpression で記述された情報のモデル化，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），2018 年.
10. 土田 敏生，瀧田 愼，古本 啓祐，白石 善明，髙野 泰洋，毛利 公美，森井 昌克，マルチホップ無線ネットワーク上での分散秘密の配付について，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），2018 年.
11. 稲吉 陽一朗，白石 善明，竹尾 淳，加藤 昇平，矢口 隆明，岩田 彰，HPKI 認証の特長を考慮した在宅医療介護システムにおける患者情報の開示先制御，情報処理学会研究報告（コンピュータセキュリティ），2017 年.
12. 近藤 秀紀，永井 達也，古本 啓祐，伊藤 大貴，野村 健太，神薗 雅紀，白石 善明，髙野 泰洋，毛利 公美，森井 昌克，ダイアモンドモデルに基づく脅威情報分析のためのインタフェースについて，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），2017 年.
13. 土田 敏生，伊東 春香，瀧田 愼，廣友 雅徳，野村 健太，白石 善明，毛利 公美，福田 洋治，森井 昌克，LDPC 符号を用いたシンドローム復号問題に基づく署名方式，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），2017 年.
14. 伊東 春香，廣友 雅徳，福田 洋治，毛利 公美，白石 善明，LDPC 符号を用いたゼロ知識証明型認証方式について(II)，情報処理学会コンピュータセキュリティシンポジウム，2017 年.
15. 稲吉 陽一朗，白石 善明，竹尾 淳，加藤 昇平，矢口 隆明，岩田 彰，HPKI 認証を用いた在宅医療介護連携システムにおける個人情報の開示先制御，電子情報通信学会技術研究報告（ライフインテリジェンスとオフィス情報システム），2017 年.
16. 野村 健太，伊藤 大貴，神薗 雅紀，白石 善明，髙野 泰洋，毛利 公美，星澤 裕二，森井 昌克，脅威情報の統合的分析に向けた攻撃活動のモデル化，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），2017 年.
17. 伊藤 大貴，野村 健太，神薗 雅紀，白石 善明，髙野 泰洋，毛利 公美，星澤 裕二，森井 昌克，脅威情報を関連付けるための攻撃活動の表現，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），2017 年.
18. 野村 健太，毛利 公美，白石 善明，森井 昌克，局所的な同報通信のためのマルチグループ署名方式，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），2017 年.
19. Kenta NOMURA, Masami MOHRI, Yoshiaki SHIRASHI, Masakatu MORII, A Multi-Group Signature Scheme for Local Broadcasting, The 14th Annual IEEE Consumer Communications & Networking Conference, 2017.
20. Daiki ITO, Masami MOHRI, Yoshiaki SHIRAISHI, Masakatu MORII, Virtual Storage and Area Limited Data Delivery over Named Data Networking, The 2nd International Workshop on Future Internet Architecture for Developing Regions, 2017.
21. 福田 洋治，白石 善明，毛利 公美，電子鑑識の動向とネットワークフォレンジック，電気関係学会関西連合大会，招待講演，2016 年.
22. 野村 健太，毛利 公美，白石 善明，森井 昌克，近隣サービスで同時検証するためのマルチグループ署名，情報処理学会コンピュータセキュリティシンポジウム，2016 年.