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 １０ 日現在

機関番号：１１３０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１８１

研究課題名（和文）ＩｏＴ活用：機密性と信頼性を両立するピュアP2P型クラウドストレージ技術の開発

研究課題名（英文）The use of IoT devices: Development of technologies for pure P2P type cloud storage with both confidentiality and reliability

研究代表者
酒井　正夫（SAKAI, MASAO）

東北大学・教育情報基盤センター・准教授

研究者番号：３０３４４７４０

交付決定額（研究期間全体）：（直接経費）　　2,500,000円

研究成果の概要（和文）：本研究では、機密性と信頼性を両立する非中央集権型のピュアP2Pストレージの関連技術を開発した。また、計算機シュミレーションにより、ユーザ自身がパラメータを適切に設計することで、保存データの信頼性を任意に設計できることと、そのリソース使用量が実用可能な水準で収まることを示した。
さらに、当該技術の応用・活用例として、個々の医療機関で蓄積された診断データを患者のプライバシや医療機関の権益を保護しながら安全に医療機関間で相互連携・活用するための関連技術も開発した。

研究成果の学術的意義や社会的意義
本研究において開発したP2Pストレージは、ブロックチェーン技術を採用した非中央集権型構造が特徴である。ブロックチェーンとは、Bitcoinなどの仮想通貨の基幹技術であり、その革新性から仮想通貨（送金システム）以外の様々な応用（いわゆるブロックチェーン２．０）への期待が高まっている。しかし、現状では、それらの実用性は低く、社会的に幅広く普及するほどの成功例はまだ存在しない。その大きな理由の一つは、ブロックチェーン２．０において不可欠な非中央集権型ストレージ技術が未確立であるためである。本研究の成果はその問題克服に資するものであり、今後のブロックチェーン２．０の発展・実用化に役立つと期待される。

研究成果の概要（英文）：In this study, I have developed the methods for pure-type P2P storage with confidentiality and reliability. By using the computational simulations, I have also shown that the reliability and risk levels of stored user data in the storage can be designed arbitrarily, and the network and CPU resource usage can be kept at a practicable level with appropriate parameters which user set.
In addition, as an example of application and utilization of these technologies, the related technologies for mutually and safely utilization of medical data in some medical institutions while protecting the patient's privacy and keeping the medical institution's rights.

研究分野：情報セキュリティ

キーワード：ブロックチェーン　Peer to Peer (P2P)　IoT　クラウド　プライバシ　スマートコントラクト

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

近年，Dropbox などの個人ユーザ向けクラウドストレージサービスが普及し，便利に活用されている．将来的にユーザサービスのクラウド化が促進された場合，個人データの保存先がローカル端末のストレージから､クラウドストレージに完全移行される可能性も十分にあり得る．しかし，クラウドストレージは，現状，必ずしも安全とは言えない．例えば，クラウドストレージに保存したデータは，ターゲット広告配信を目的に，サービス事業者側に解析（覗き見）される恐れがある．また，公的な捜査機関により強制的に保存データが覗かれたり，第三者からの攻撃により保存データが改変・漏洩されたりする恐れもある．実際，2013 年 6 月には、米国諜報機関の元職員エドワード・スノーデン氏が、米国政府が大手インターネットサービス事業者と秘密協定を結びユーザ情報を収集・監視していることを告発しており、そのようなリスクが杞憂でないことを示している．

このようなリスクへの対策として，データを秘密分散法により複数のクラウドストレージに分散保存して守る技術が注目されている．秘密分散法とは，データを複数の部分データ（シェア）に分割し，それらが一定数以上集まることで元データを復元できる（足りない場合は絶対に復元できない）という，情報理論的安全性が証明されている技術である．この技術により秘密を複数のシェアに分割し, 複数の異なるクラウドストレージやユーザ端末に分散保存すれば，一部の保存先が攻撃者に乗っ取られた場合にも，元データを守ることができる．しかし，保存先候補がたかだか少数の主要クラウドストレージサービスとユーザ端末に限定される場合は，攻撃者は対象ユーザの保存先を容易に特定して，その全てを一斉に攻撃することで保存データを奪うことに成功する恐れがある．

このような一斉攻撃に対抗するためには, ピュア P2P 型クラウドストレージ技術が有効ではないかと研究代表者は考える．ここで，ピュア P2P 型クラウドストレージとは，中央集権的な管理サーバを必須とせず，不特定多数のユーザ端末群を P2P ノード（データ保存先）として活用するオンラインストレージのことである．この場合, P2P ノード数が十分に大きい場合には，シェアの保存先候補は少数に限定されず一斉攻撃が実質不可能になり，保存データの機密性を更に向上できる．一方で，ピュア P2P 型クラウドストレージの場合，保存データの信頼性維持が困難という問題がある. 実際, そのような個人向け商用サービスはまだ存在しておらず, 2012 年に MaidSafe 社(http://maidsafe.net/)が個人向け商用サービス「MaidSafe DHT（ユーザ管理用サーバが存在するが，実質的にはピュア P2P 型クラウドストレージとして動作する）」の近日開始を予告して注目されたが，信頼性の問題を理由に開始延期を繰り返し，結局は 2014 年末にサービス中止を決定している.「MaidSafe DHT」の基幹技術である分散ハッシュテーブル（DHT）の技術自体は，大規模分散データベースなどの用途で実用化済みであり深刻な信頼性の問題は起こっていない．したがって，ピュア P2P 型クラウドストレージの実用化が困難な原因はそれを構成する P2P ノード（不特定多数のユーザ端末）の低信頼性にあると推測される．

２．研究の目的

本研究では，情報理論的安全性が証明されている秘密分散法と，実際に破綻することなく利用されていることで安全性の検証がなされている仮想通貨「BitCoin」や匿名通信「Tor」などの P2P 関連技術とを併用し，さらに，IoT デバイスを P2P ノードとして活用することで，機密性と信頼性を両立するピュア P2P 型クラウドストレージ技術を新規開発するのが本研究課題申請時における第一目標であった．また，計算機シミュレーションにより効率的に開発技術の動作検証と有用性評価を行い，さらに，用いた P2P 関連技術が安全であるという仮定のもとで，理論的な考察により開発技術の安全性を数学的に証明することが第二目標であった．さらに，開発技術を活用するクラウドストレージ以外の応用例を検討して、その有用性を示すことが最後目的であった.

３．研究の方法

本研究では、はじめに，秘密分散法に対して P2P 関連技術（BitCoin，Tor，分散ハッシュテーブルなど）を援用して，さらに，今後に普及が予測されている IoT（モノのインターネット）デバイスを P2P ノードとして活用することを前提にして，前述の P2P ノードの低信頼性の問題を克服し, 実用可能レベルのピュア P2P 型クラウドストレージを実現する技術を新規開発する．

その後，計算機シミュレーションを用いた開発技術の動作検証・有用性評価と，理論的考察による開発技術の安全性証明を試み，それらの結果のフィードバックにより，開発技術を段階的に改良し続ける．

最終的には，開発技術を活用するクラウドストレージ以外の応用例を検討して、その有用性を示す．

以下に、主な実施項目とその方法を述べる．

（１）機密性と信頼性を両立するピュア P2P 型クラウドストレージ技術の開発

通信傍受による保存先ノード特定と送受信時の中間者攻撃を不能にする技術を開発する．研究代表者らは，これまでに，秘密分散法を用いて秘密データを複数のクラウドストレージサービスに分散して秘匿保存する技術を開発している．その技術に，ピュア P2P 型ネットワーク技

術と匿名通信技術（Tor など）を援用することで,「分散データの保存先ノード特定」と「送受信時の中間者攻撃」を不可能にする技術を開発する.

（2）クラウドストレージ上に保存したメタ情報の消失・改変を防ぐ技術の開発
BitCoin システムにおけるブロックチェーンの技術を援用する．ブロックチェーンにデータを保存した場合，そのデータの改変や消失を防ぐことが可能であるが，一方でそのデータは公開情報となるため，そこから保存データの機密が漏れる恐れがある．そこで，ブロックチェーンには，P2P ノードに秘匿分散保存したシェアを取り出すための情報（メタ情報）のみを暗号化して保存し，さらに，オフライン解読攻撃のリスクを回避するために，一定時間毎にメタ情報を更新（再保存）し，旧メタ情報を無効化する仕組みの導入も検討する.

（3）サービス利用不能（DoS）攻撃を防ぐ技術の開発
BitCoin システムにおけるプルーフオブワークの技術を援用する．ただし，BitCoin システムの場合, プルーフオブワーク（マイニング）による競争の勝者には経済的利益（新規 BitCoin）が与えられるが，本研究のようなクラウドストレージサービスの場合には，そのような直接的な経済的利益が勝者に与えられない．そのため，BitCoin システムのようには有効に機能しない恐れが有りえる．また，そもそも膨大な維持コスト（電気代など）が必要なプルーフオブワークの技術は, クラウドストレージサービスには割が合わず不適当な可能性もある. そのため, 別の代替技術の利用も並行して検討する.

（4）クラウドストレージ全体の性能をノード間連携により自律的に最適化する技術の開発
本研究では, 中央集権的なサーバを必要としないピュア P2P 型ネットワークを前提としている．そのため, クラウドストレージ全体の性能（保存可能容量や保存データの冗長度など）を, P2P ノードの相互連携により自律的に最適化する仕組みが必要である．この仕組の実現には, 分散ハッシュテーブル(DHT)の技術を援用することを検討している．ただし，一般的な DHT は十分な攻撃耐性を持たず脆弱なため，連携研究者らによる「不正ノード/攻撃の検知と排除, 冗長性の自動評価/回復」の技術を併用する予定である.

（5）計算機シミュレーションによる開発技術の動作検証と有用性評価
開発技術の動作検証と性能評価を計算機シミュレーションにより行う．具体的には，各種パラメータ値と保存データの機密性と信頼性の関係を定量的に評価して, その有用性を検証する. また，その結果のフィードバックにより開発技術の改良を段階的に行う.

（6）開発技術を活用するクラウドストレージ以外の応用例の検討
開発技術のクラウドストレージ以外の応用可能性について検討する．具体的には，ブロックチェーン 2.0 の代表例であるスマートコントラクト分野での応用を目指す.

４．研究成果
（1）機密性と信頼性を両立するピュア P2P 型ストレージ技術の開発
はじめに，秘密分散法にブロックチェーン技術，匿名通信技術（Tor，I2P など）を援用することで，機密性と信頼性を両立するピュア P2P 型ストレージ技術の開発した．当該技術は，中央集権的な管理主体が存在しない非中央集権型であるが，不特定多数のノード群がブロックチェーンを信頼の基点として自律的に動作することで，不正ノードによる中間者攻撃や DoS 攻撃を検知・排除することが可能である．それにより，不正ノードが特定の攻撃対象ユーザのデータ保存先を識別することを困難にして，ユーザの保存データの機密性をより向上させることができる．この成果は，2017 年 3 月開催の AINA2017 をはじめとする複数の国内シンポジウム/国際会議において発表している.

（2）P2P ノード群の相互連携によりクラストレージの信頼性を自動回復する技術の開発
計算機シミュレーションにより（1）で開発したピュア P2P 型ストレージの信頼性の定量的評価を行った．その結果，ストレージのモデルパラメータを適切に設計することで，中央管理サーバに頼ることなく P2P ノード群の自律的な相互作用のみにより，保存データの信頼性を任意の水準に維持できることを示した．一方で，構成 P2P ノード群に短期間で一定以上の大規模消失が生じた場合，たとえ保存データの消失が避けられたとしても，その後の P2P ノード群の自律的な完全復元が困難となり，保存データの信頼性が低い水準のまま維持されてしまう問題も判明した．そこで，従来用いていた秘密分散法に対して再生符号技術を援用するように改良することで，前述の問題を克服することに成功した．新技術では，保存データが消失しない限り，保存データの信頼性を完全に復元することが可能である．この成果は，2017 年 5 月開催の AINA2017 をはじめとする複数の国内シンポジウム/国際会議において発表している.

（3）開発技術を活用するクラウドストレージ以外の応用例の検討
これまでに開発したピュア P2P 型ストレージ技術の応用・活用範囲を広げる方法の検討を行い，不特定多数のノード群による非中央集権的なデータ売買契約（いわゆるスマートコントラ

クト）の安全性と実用性を向上させる方法も新たに開発した．当該手法を用いることで，例えば，個々の医療機関で蓄積された患者の診断データを患者のプライバシや医療機関の権益を保護しながら安全に医療機関間で相互連携・活用することが可能になる．この成果は，2017 年 3 月開催の日本生体医工学会大会において発表している．さらに，３件の特許出願を行っている．

５．主な発表論文等

〔学会発表〕（計５件）

Masayuki Fukumitsu, Shingo Hasegawa, Jun-ya Iwazaki, Masao Sakai, Daiki Takahashi,
A Proposal of a Secure P2P-type Storage Scheme by using the Secret Sharing and the Blockchain,
The 31-st IEEE International Conference on Advanced Information Networking and Applications (AINA-2017), pp. 803--810, (March 27-29, 2017)
DOI 10.1109/AINA.2017.11

岩崎 淳也，酒井 正夫
ブロックチェーン：医療機関間の安全で自律分散的なデータ連携に向けて
第 56 回日本生体医工学会大会，OS-7.3 サイバー医療：最近の技術革新と応用例（第 7 会場）
2017 年 5 月 3-5 日

福光正幸，長谷川真吾，岩崎淳也，酒井正夫
自律分散型 P2P ストレージの定量的信頼性評価
2017 年暗号と情報セキュリティシンポジウム(SCIS2017)，論文集 2D2-5，2017

Masayuki Fukumitsu, Shingo Hasegawa, Shuji Isobe, Jun-ya Iwazaki, Eisuke Koizumi and Masao Sakai,
A Method for Constructing an Autonomous Decentralized P2P Storage with High Confidentiality and Reliability,
The Proceeding of the 4th International Workshop on Information and Communication Security 2017, pp. 439-444, (November 22-24, 2017)
DOI 10.1109/CANDAR.2017.67

福光 正幸, 長谷川 真吾, 磯辺 秀司, 岩田 直樹, 岩崎 淳也, 小泉 英介, 中田 恒夫, 酒井 正夫
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
第 82 回コンピュータセキュリティ研究会 (2018-CSEC-82)，Vol.2018-CSEC-82，No.8，2018/07/25-26

〔産業財産権〕
○出願状況（計３件）

名称：情報処理システム、公開鍵の変更方法、プログラム、および情報処理システムの製造方法
発明者：酒井正夫、岩崎淳也、小泉英介、長谷川真吾、磯邉秀司、福光正幸
出願人：東北大学
特許番号：特願 2018-211811
国内出願日：2018 年 11 月 9 日
国内外の別： 日本

名称：情報処理システム、データ提供方法、および情報処理システムの製造方法
発明者：酒井正夫、岩崎淳也、小泉英介、長谷川真吾、磯邉秀司、福光正幸
出願人：東北大学
特許番号：特願 2018-211813
国内出願日：2018 年 11 月 9 日
国内外の別： 日本

名称：情報処理システム、サービスデータ提供方法、および情報処理システムの製造方法
発明者：酒井正夫、小泉英介、岩崎淳也、久井雅史
出願人：東北大学
特許番号：特願 2019-006705
国内出願日：2019 年 1 月 18 日
国内外の別： 日本