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　５ 年　 ６ 月　 ２ 日現在

機関番号：２４５０６
研究種目：研究活動スタート支援
研究期間：2020～2022
課題番号：２０Ｋ２３３２９

研究課題名（和文）Edge Named Functionアーキテクチャでのプライバシ保護手法の研究

研究課題名（英文）Research on privacy-preserving schemes in Edge-Named Function architecture

研究代表者
栗原　淳（Kurihara, Jun）

兵庫県立大学・情報科学研究科・准教授

研究者番号：１０５７７３９９

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：本研究の目的は、エッジコンピューティングにおいて、計算リソースの保護手法を検討することである。本研究においては、エッジのリソース保護・匿名化について大きく3つの成果を与えた。1) 今まで検討されていなかったエッジノードのリソースの認証・認可手法の分類・検討、2) エッジノードを効率的に利用するためのGeneralized Deduplication手法の検討、3) エッジノードへの匿名性を担保することを目的とした秘匿検索手法の理論検討。また、リソース保護について高度なDNS匿名化手法の初期検討も行うことができた。結果、本研究に関連して、学術論文誌1件、国際会議2件、国内発表5件を実施した。

研究成果の学術的意義や社会的意義
beyond 5Gや6Gを見据え、エッジコンピューティングは低遅延通信を実現するための新たなアーキテクチャとして社会実装が少しずつ進んでいる。計算リソース保護の観点から検討することは、将来の安心・安全なエッジコンピューティングの実現のために必須の事項である。本研究は、その初期検討を開始したという社会的意義を有する。

研究成果の概要（英文）：The aim of this research is to investigate methods for preservation, protection and utilization of computational resources in edge computing environment. In this research, we presented the following three main results: 1) Detailed taxonomy on authentication and authorization of edge resources, 2) application of generalized deduplication for multi-user edge environment, and 3) theoretical analysis of private information retrieval for multi-edge environment. Additionally, we also presented preliminary proposal of anonymized DNS with collusion resistance. Corresponding to these topics, we presented one full-paper on a journal, two papers at international conferences, and four papers at domestic conferences.

研究分野：セキュリティ

キーワード：エッジコンピューティング　リソース保護　ネットワーク　セキュリティ　秘匿検索　匿名化

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

自動運転技術や AR (Augmented Reality) 技術等に求められる「瞬時に処理応答を行う低遅延サービス」を実現する基盤として、ネットワークを介してデータセンタの中央サーバへ接続する「クラウドコンピューティング」に代わり、「エッジコンピューティング」の社会的要望が高まっていた。実際に、5G の次、beyond 5G および 6G においては、エッジコンピューティングはアーキテクチャのコア要素の１つとして検討が始められていた。

エッジコンピューティングでは、中央サーバに加え、ネットワーク中でよりユーザ近傍の箇所へ、計算能力を有する「エッジノード」を配置する。そして、遠方の中央サーバに代わりユーザ近傍のエッジノードが処理・応答することで、低遅延サービスを実現する。一方で、従来のクラウドコンピューティングとは異なり、エッジコンピューティングでは、サービス本体の事業者とは異なる第三者がエッジノードを設置することが想定されている。例えば、モバイル通信基地局をエッジノードとすれば、あるサービスについて、そのサービス事業者に代わり、ネットワーク・通信事業者がその計算処理インフラを請け負うこととなる。このことが、従来のクラウドコンピューティングとは異なる新たなセキュリティ・プライバシ課題を産むことが想定されていた。

２．研究の目的

上記背景を踏まえ、本研究ではエッジコンピューティングについて、そのリソース保護手法、プライバシ保護手法、および効率化手法を検討・評価することを目的とした。それぞれ、詳細な目的は以下の通りである。

(1) リソース保護について : インフラ事業者が提供するエッジコンピューティング基盤において、第三者がサービスを提供することを想定する。これは、従来のクラウドコンピューティングなどとは異なる形態のリソース貸与がなされることを意味する。従って、エッジコンピューティング特有の認証・認可パターンの詳細な分類を行い、それらパターンでの具体的な認証認可手法を検討することを目的とした。

(2) プライバシ保護について: エッジコンピューティングにおける匿名性担保のため「どんな計算結果を所望しているのかエッジノードへ秘密のまま取得するプライバシ保護技術」を検討することを目的とした。特に、秘匿検索技術そのものの性能評価や限界性能の特徴づけを行うことを第一の目的とした。加えて、さらに具体的なトピックとして、エッジコンピューティングのリソース発見に重要な役割を担う Domain Name System (DNS) に着目し、ユーザの ID と DNS クエリとを分離し、そのクエリのプライバシを担保する手法を検討することを第二の目的とした。

(3) 効率化手法について: エッジコンピューティングの利用において、IoT 端末の出力データをエッジノードで受信し、クラウドノードへアップロードすることを考える。このとき、多数の IoT 端末が単一のエッジノードに接続することで課題となりうる、「膨大な通信データ量」について、これを効率的に圧縮する手法を提案することを目的とした。

３．研究の方法

３つの目的に対しての、それぞれの研究アプローチは以下の通りである。

(1) リソース保護について: 本目的に対して、「(ID を有しない匿名の)認可トークンを用いた、計算リソースの利用認可手法」の検討をおこなった。ここでは、OAuth2.0 等、認可トークンを用いた認可技術を前提としている。既存の認可手法を拡張・応用し、複数の AS (Autonomous System) やエッジノード提供 事業者、およびサービス提供者をまたがってトークンをやり取りし、リソース管理する、というシナリオでの検討を行った。

(2) プライバシ保護について: 秘匿検索技術の性能評価・限界性能の特徴づけを行うという第一の目的について、「複数エッジノードに接続したクライアントが、それらにクエリを送ってデータを引き出すことを考える。このとき、いくつかのエッジノードに情報を破壊や盗聴を試みる攻撃者が存在することを仮定する。」というシナリオを仮定した検討を行った。このシナリオにおいて、クライアントがクエリの内容を漏洩させず、さらに所望の情報を正しく取得可能となる理論的な条件の導出を行うことで、秘匿検索技術の性能評価を行った。

また、第二の目的である DNS プライバシの担保については、既存の DNS 匿名化手法よりも強固

なプライバシ保護を担保可能な手法を確立するため、匿名化リレーノードを用いた既存プロトコル（DNSCrypt）を拡張する手法での検討を行った。具体的には、既存手法での脆弱性である結託耐性の欠如を、複数リレーの導入と経路ランダム化により解決する手法を提案し、その性能評価を行った。

(3) 効率化手法について: Generalized Deduplication は、一般的なデータ圧縮手法とは異なり、符号理論を応用しつつストリーミングデータの即時圧縮を可能としている。しかしながら、1-to-1 での圧縮・伸長のみが検討されており、 エッジコンピューティングなどクラウドサーバとの間に別のノードを経由するようなアーキテクチャでの利用は検討されていない。これを踏まえ、エッジノード・クラウドサーバ間でのデータ圧縮効率をより高めるため、Generalized Deduplication をマルチユーザ化し、エッジノードで圧縮データを集約・高効率な再圧縮を施すことができる手法を検討した。

４．研究成果

研究成果についても、目的ごとに分けて記載する。

(1) リソース保護について: エッジノードはネットワークオペレータ等、サービスプロバイダとは異なる事業者が提供しうる。個々のエッジノードの計算リソースは中央サーバに比べ乏しいため、正当なユーザ・サービスのみが計算リソースを利用でき、かつ計算リソースが枯渇しないように、その利用権限を動的に割り当てる必要がある。このためには、計算リソースの所有者が、その実行権限を委譲する「認可」の手法が利用できる。

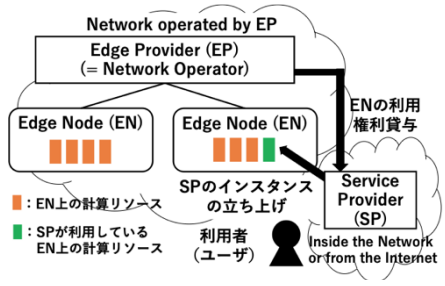

図 1 サービスプロバイダへ権利移譲するパターン

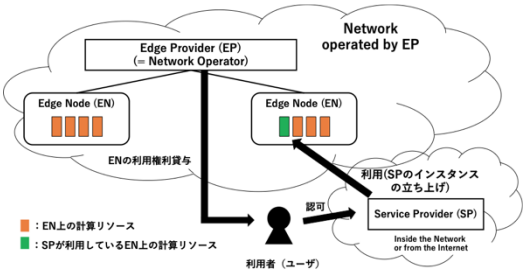

図 2 ユーザへ権利移譲するパターン

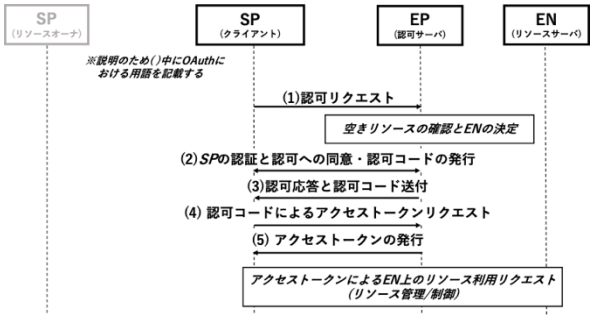

図 3 サービスプロバイダへ権利移譲するパターンにおける OAuth2.0 ベース認可フロー

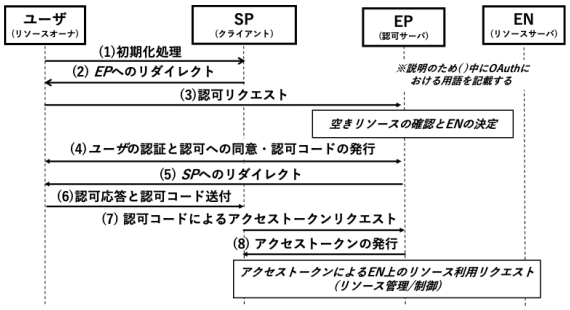

図 4 ユーザへ権利移譲するパターンにおける OAuth2.0 ベース認可フロー

上記を鑑みて、インターネット上の代表的な認可手法である「OAuth2.0」を、エッジコンピューティングでの計算リソースの認可に、どのように適用することができるか、ということに主眼をおいた検討を行った。そして、エッジコンピューティングの参加者（ネットワークオペレータ、ユーザ、サービスプロバイダ）の相互関係性に依存し、大きくパターンが 2 つに分類可能であることを明らかにしている。また、各パターンに応じて適用すべき認可のフローが異なることを明らかにした。本検討で分類したパターンとその認可フローは次の通りである。

- エッジノード の利用権利をサービスプロバイダに移譲したパターン（図 1）:
  → 適用すべき認可フローは図 3 の通り
- エッジノードの利用権利をユーザに移譲したパターン（図 2）:
  → 適用すべき認可フローは図 4 の通り

加えて、モバイルネットワークを考慮した際、（国際） ローミングを考慮しなければならないた

め、これらについても関係性のパターンと、適用すべき認可フローを明らかにした。
本検討成果は、電子情報通信学会の国内研究会、および国際学術会議 AINA2022 にて発表しており、エッジコンピューティングのセキュアな活用のために有用である。今後は、実際の環境での性能評価や各パターンにおいての認可プロトコルフローのさらなる最適化などが検討課題として挙げられる。

(2) プライバシ保護について:
2-a) 秘匿検索手法の限界値究明:
分散符号化されたデータに対する秘匿検索手法(Private Information Retrieval; PIR)において、クエリの内容を秘匿したまま、結託耐性・改竄耐性を保証するための理論限界値を明らかにした。具体的な問題設定と成果は以下の通りである。

- [問題設定] 複数の分散符号化ストレージ (エッジノードを想定) で構成されるデータベースに対して、ユーザが「所望するデータが何であるか」を秘匿したまま、データの取得クエリを発行する。これを、分散符号化ストレージに対する PIR 問題、と呼ぶ。このとき、b 個のエッジノードは保存されるデータの改竄を行い、u 個のエッジノードは意図的に応答を返さないような状況を想定する。これを、b-ビザンチン障害、u-無応答と呼ぶ。このような状況において、ユーザが「所望のデータが何であるかを秘匿したまま、誤りなく完全に取得可能」とするために、許容可能な b,u の最大限界値を明らかにする。
- [主成果] 分散符号化ストレージの符号を C、およびクエリ生成に用いられる符号を D1, D_2 (D_1 の真部分空間) とする。このとき、C と D_1 の符号語同士の Hadamard 積全てで Span される部分空間を $C*D_1$ とする。$C*D_2$ も同様に定義する。このとき、「b-ビザンチン障害、u-無応答の状況の PIR 問題に対し、所望のデータが何であるかを秘匿したまま、誤りなく完全に取得可能」とするための十分条件が以下で表されることを明らかにした。

$$d_{min}(C*D_1/C*D_2) > 2b + u$$

すなわち、商空間 $C*D_1/C*D_2$ における最小コセット距離(ハミング距離)で、記述可能なことを明らかにした。これにより、求める性能を持つ PIR 手法において、符号化データの設計、およびクエリの設計が、よく知られた符号パラメータを用いて可能なことを意味する。
- [付随する成果] 主成果で明らかにしたものは、「どのノードで b-ビザンチン障害、u-無応答を起こすか」を完全にコントロールでき、さらには「どのノードに何のデータが保存されているのかを知っている」という、強力な攻撃者を想定した上での限界値であった。このため、b-ビザンチン障害、u-無応答を起こすノード以外は、保存データについて一切の知識を有さない、より限定的な能力を持つ攻撃者を仮定した際の、b と u の許容限界値の導出を行った。

これらの検討成果は、電子情報通信学会の国内研究会で発表、および国際学術雑誌 IEICE Transactions に掲載されており、PIR の理論限界値の導出や、具体的な PIR の設計に対して寄与している。本結果は、本来であれば国際会議で速報を発表すべきものであったが、コロナ禍のため、検討を終えてから国際学術雑誌へフルペーパを投稿した。

2-b) 匿名化 DNS 手法の開発:
IETF ドラフトに提案されている Oblivious DNS over HTTPS (ODoH)やオープンソースソフトウェア Anonymized DNSCrypt では、ユーザの DNS クエリを受け取り、DNS リゾルバへ転送する匿名化リレー(エッジノードを想定)を用いて DNS 匿名化を実現している。これは、匿名化リレーを挟むことで、リゾルバに対してユーザの IP アドレスが秘匿されることを意味する。しかしながら、匿名化リレーとリゾルバが結託した場合、その匿名性は担保不可能となる。このような結託に対しても、ユーザの匿名性を担保可能な手法を設計した。
図 5 および図 6 にコンセプトを示すように、本手法では、リゾルバとの結託が起きえない「信頼の起点」となるリレーを各ユーザが保持し、その信頼の起点で他ユーザのクエリをミックスすることで匿名性を担保する。信頼の起点は、例えばユーザ専用のリレーである。従来の手法では、信頼の起点を仮定すると、そこを経由するクエリは全てそのユーザのクエリであることが看過されうるが、本手法では他のユーザのクエリとミックス・経路のランダム化を施すことでそれが困難であることを実現している。
本研究課題で行ったのは、コンセプトの設計と、オープンソースソフトウェア開発への着手となる。本成果について、速報として、電子情報通信学会の国内研究会で発表、および ArXiv にてコンセプトペーパーを発行した。このコンセプトをさらに拡張し、次の研究課題として ODoH をベースとした DNS 匿名化手法のオープンソースソフトウェア開発、および実装、サーバ公開、性能評価を進めている。

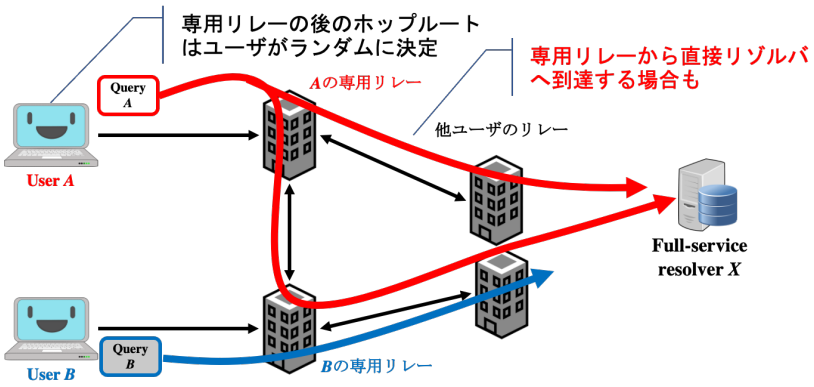

図 5 結託耐性を有する DNS 匿名化のコンセプト 1

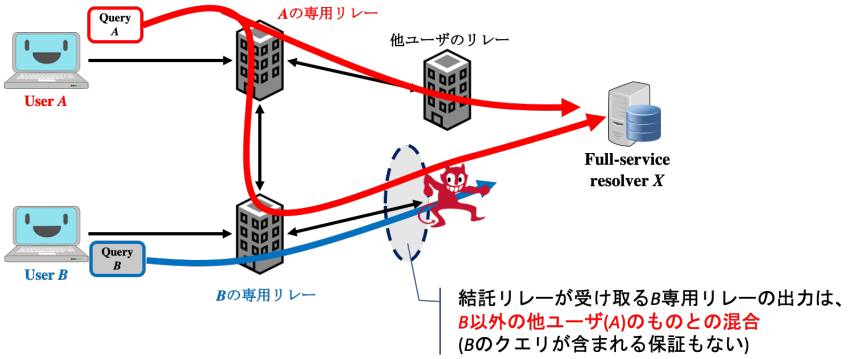

図 6 結託体制を有する DNS 匿名化のコンセプト 2

(3) 効率化手法について:

本検討では、Multi-access Edge Computing (MEC) 環境を想定し、エッジノードを用いた Massive IoT 環境(図 7 を参照) のシナリオを検討した。当該環境におけるデータ圧縮について、軽量かつ IoT センシングデータ等を効率的に圧縮できる、重複削除によるストリームデータ圧縮手法「Generalized Deduplication (GD)」を適用することを検討した。基本的な GD のアルゴリズムは、1 対 1 でのストリーム送受信を前提としている。そのため、エッジノードを経由し、多数の IoT 端末が上位クラウドサーバへデータをアップロードするような環境を考慮した際、IoT 端末～クラウド間でのデータ圧縮を行うことはできても、エッジ～クラウド間のデータ圧縮を行うことはできない。このため、エッジ～クラウド間の帯域を効率的に利用することができない課題がある。そこで、GD の基本手法を拡張し、1 対多(エッジノード対 IoT 端末)の環境でデータをまとめて圧縮統合し、エッジ～クラウド間では 1 つの圧縮ストリームを送受信する「マルチユーザ GD 方式」を提案した。

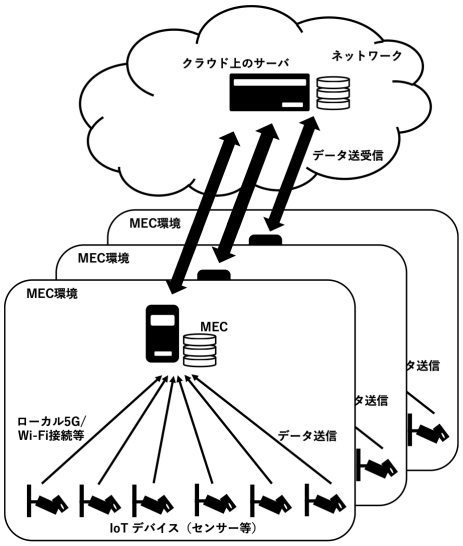

図 7 複数 IoT 端末を収容する中位のエッジノード、および上位クラウドサーバで構成される想定環境

1 対 1 を前提とした GD の基本手法では、ストリームデータ圧縮用の辞書を送信側で作成・更新しつつ、データ圧縮を行う。一方で受信側では、圧縮データを受信しつつ、同様の辞書を復元・共有しながらデータの伸長を行う。そこで本検討では、エッジ～各 IoT 端末間での GD 辞書データを逐次統合し、エッジノードで圧縮データをさらに圧縮・結合するアルゴリズムを提案した。これにより、IoT デバイスからの圧縮ストリームをエッジノードでさらに圧縮されたストリームとして上位クラウドサーバと送受信可能なことを示すことができた。

本成果は、情報処理学会コンピュータセキュリティシンポジウム 2022、および国際会議 AINA2023 にて発表を行った。本成果を用いることで、エッジノード～クラウドサーバ間の帯域の効率的な利用が可能となり、またエッジノードの利用形態のひとつとして利用が見込まれる。今後の研究課題として、具体的な圧縮性能の評価およびより効率的なアルゴリズムへの改良を行なっている。

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　1件）

１．著者名 Watanabe Ryu、Kubota Ayumu、Kurihara Jun	４．巻 655
２．論文標題 Application of Generalized Deduplication Techniques in Edge Computing Environments	５．発行年 2023年
３．雑誌名 Advanced Information Networking and Applications. AINA 2023. Lecture Notes in Networks and Systems	６．最初と最後の頁 585～596
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-28694-0_55	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Watanabe Ryu、Kubota Ayumu、Kurihara Jun	４．巻 449
２．論文標題 Resource Authorization Methods for Edge Computing	５．発行年 2022年
３．雑誌名 Advanced Information Networking and Applications. AINA 2022. Lecture Notes in Networks and Systems	６．最初と最後の頁 167～179
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-99584-3_15	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 KURIHARA Jun、NAKAMURA Toru、WATANABE Ryu	４．巻 E104.A
２．論文標題 Private Information Retrieval from Coded Storage in the Presence of Omniscient and Limited-Knowledge Byzantine Adversaries	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1271～1283
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020DMP0018	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5件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 渡辺龍、窪田歩、栗原淳
２．発表標題 エッジコンピューティング環境へのデータ圧縮手法の適用
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2022
４．発表年 2022年

１．発表者名
栗原 淳、久保 健

２．発表標題
μODNS：結託耐性を考慮した匿名化DNSに関する一考察

３．学会等名
電子情報通信学会ネットワークシステム研究会

４．発表年
2021年

１．発表者名
栗原 淳

２．発表標題
DNSのセキュリティ・プライバシ技術動向

３．学会等名
電子情報通信学会ソサエティ大会

４．発表年
2021年

１．発表者名
Jun Kurihara, Toru Nakamura, Ryu Watanabe

２．発表標題
On the Resistance to Byzantine and Unresponsive Servers in Code-based PIR Schemes

３．学会等名
誤り訂正符号のワークショップ

４．発表年
2020年

１．発表者名
渡辺龍，窪田歩，栗原淳

２．発表標題
エッジコンピューティングにおけるリソース認可のパターンについて

３．学会等名
電子情報通信学会ネットワークシステム研究会

４．発表年
2021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