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　２ 年　 ７ 月　 ６ 日現在

機関番号：１４３０１
研究種目：基盤研究(B)（一般）
研究期間：2014～2019
課題番号：２６２８００３０

研究課題名（和文）フラッシュクラウド耐性のあるオープンなメッセージ型Web情報共有基盤

研究課題名（英文）Open pub/sub messaging platform on the Web addressing flash crowds

研究代表者
岡部　寿男（Okabe, Yasuo）

京都大学・学術情報メディアセンター・教授

研究者番号：２０２０４０１８

交付決定額（研究期間全体）：（直接経費）　　13,000,000円

研究成果の概要（和文）：インターネット本来の自律分散の考え方に基づき，ブログやSNS などのメッセージ型Web サービスを提供する複数の事業者を緩やかに連携させることで，特定の事業者に依存することなくオープンなアーキテクチャによるグローバルなスケールのWeb情報共有基盤を研究開発した．P2P ファイル共有ネットワークを通じてメッセージデータを共有することで，フラッシュクラウドと呼ばれる急激な負荷の増加に対して高い耐性を持つと同時に，認証連携とグループ管理，電子署名・暗号化を用いて，インターネット上に広く流通する情報がセキュリティとプライバシー上の要件を満たすように設計した．

研究成果の学術的意義や社会的意義
現状，大規模広域Web 情報共有サービスは，Google やFacebookに代表される広告による収益を目的とする事業者による寡占が進んでいる．公共サービスでの利用を含み個人情報も扱うこのような情報共有基盤を特定の営利事業者が独占的に担うことについては，セキュリティやプライバシーの点で少なからぬ懸念がある．また，それらの事業者は独自に開発したソフトウェアを用いてサービスを運用しており，内部で用いられているアルゴリズムやプロトコル，ソフトウェアの多くが非公開で，学術の進展に必ずしも寄与していない点も課題であった．本研究により，緩い連携による全世界レベルのオープンなサービスが提供できるようになる．

研究成果の概要（英文）：Based on the inherent autonomous decentralized nature of the Internet, we have developed a new generation of message-based Web services such as blogs and SNS, by loosely coordinating multiple providers of services, independent from a specific provider. Our target is a global-scale web information sharing platform with an open architecture rather than a single one. It is possible to share message data through P2P file sharing networks. It is highly resistant to the rapid increase in load called a flush crowd. At the same time, it has a high level of authentication and group management, digital signatures and encryption to ensure that information that is widely distributed on the Internet is designed to meet security and privacy requirements.

研究分野：インターネットアーキテクチャ

キーワード：ネットワークアーキテクチャ　アクセス制御　Webシステム　コンテンツ管理　仮名性　P2P　インターネット高速化　認証

様　式　Ｃ－１９，Ｆ－１９－１，Ｚ－１９（共通）

１．研究開始当初の背景

インターネットの普及とモバイルネットワーク環境の著しい進展に伴い，電子掲示板，ソーシャルネットワーキングサービス(SNS)，ブログ，マイクロブログ，チャットなど，World Wide Web（以下，Web）に基づく様々なメッセージ型の情報共有技術が，個人レベルのコミュニケーションだけでなく，公共サービスやビジネスでの情報発信にまで広く用いられるようになり，電子メールと並んで不可欠な社会基盤となりつつある．

全国あるいは全世界の利用者を対象とする大規模広域の Web サービスでは，24 時間 365 日の安定した運用が求められるとともに，フラッシュクラウド(flash crowd) と呼ばれる急激な負荷の増加にも対応が必要である．フラッシュクラウドとは，ネットワークや Web サーバが突然大量のトラフィックを受ける現象で，その負荷は平常時の数十倍から数百倍に及ぶ．フラッシュクラウドは，典型的には有名な Web サイトやブログで当該の Web コンテンツが紹介されたことが契機で生じ，その発生も規模も予測が困難であることが少なくない．

これまで，過負荷に対する Web サーバ側の一般的な対策として，リバースプロキシによるキャッシュやロードバランサーによる複数マシンへの振り分け，Content Delivery Networks (CDN) へのキャッシュの分散などが用いられてきた．また，いわゆるクラウドサービスの中でも IaaS (Infrastructure as a Service) と呼ばれるインフラの設備を仮想化しサービスとして提供する手法により，必要に応じて柔軟に設備を増強することで，予測できない負荷の到来に対して比較的迅速に対応することも行われている．しかしこれらはいずれも設備面でのコスト負担が伴うものであり，小規模な Web サイトでは対応が難しい．結果として，メッセージ型の情報共有においては Facebook に代表される大規模な事業者による寡占が進んでいる．

フラッシュクラウドに対して高い耐性を持つ協調型の情報共有基盤の技術として，Peer to Peer (P2P)ファイル共有がある．P2P ファイル共有は，その匿名性を悪用した著作権侵害等により否定的に捉えられることが少なくないが，匿名性は P2P 共有の要件ではなく，Linux のカーネルイメージをはじめ，主要なオープンソースソフトウェアのほか，音楽や映画，商用アプリケーションの配布に，P2P ファイル共有プロトコルの一つである BitTorrent が広く利用されている．近年，P2P ファイル共有を活「用して複数の Web サーバが協調的に連携することで Web サーバのフラッシュクラウドを回避する技術が注目され，盛んに研究されている．

T. Stading らは，HTTP リダイレクトによって協調する Web サーバに負荷を分散する手法を提案している[Peer-to-Peer Systems, 2002]．Backslash と呼ばれるこのシステムでは，コンテンツの提供は Web サーバのみが行い，高負荷時は HTTP リダイレクトによって協調する他の Web サーバへリクエストを分散させる．V. Padmanabhan らは，CoopNet と呼ばれるクライアントも負荷分散に参加するシステムを提案している[Peer-to-Peer Systems, 2002]．K. Yokota らは，リバースプロキシを Web サーバの前に設置し，そこでフラッシュクラウドを検知するとともに，これまでデータを取得したクライアントを記録しておき，フラッシュクラウド時は，この記録しておいたクライアントへリダイレクトする方式を提案している[IEEE ISADS, 2011]．C. Pan らは，フラッシュクラウド下にあるデータへのリクエストを，キャッシュを行うプロキシサーバで構成されるオーバレイネットワークにリダイレクトする方式を提案している[ACM SAC, 2006]．この方式は，フラッシュクラウドが発生した際に，動的にオーバレイネットワークを構築し負荷分散できるため，柔軟にフラッシュクラウドに対処することができる．研究代表者らも，BitTorrent ネットワークを活用し，連携する Web サーバが遊休資源をお互いに融通し合い，需要の高まりに応じてデータの複製が自動的に増加することを利用して柔軟にフラッシュクラウドに対処する手法を提案してきた．

しかし，これらは基本的に静的で比較的大容量のコンテンツを対象としており，リアルタイムにデータが更新されるメッセージ型の動的なコンテンツサービスにはそのままでは適用できない点が課題であった．また，単なるファイル共有の延長であり，セキュリティやプライバシーの保護に関しても不十分であった．

現状，大規模広域 Web 情報共有サービスは，Google や Facebook に代表される広告による収益を目的とする事業者による寡占が進んでいる．公共サービスでの利用を含み個人情報も扱うこのような情報共有基盤を特定の営利事業者が独占的に担うことについては，セキュリティやプライバシーの点で少なからぬ懸念がある．また，それらの事業者は独自に開発したソフトウェアを用いてサービスを運用しており，内部で用いられているアルゴリズムやプロトコル，ソフトウェアの多くが非公開で，学術の進展に必ずしも寄与していない点も課題であった．

２．研究の目的

本研究では，インターネット本来の自律分散の考え方に基づき，このような大規模広域 Web 情報共有基盤を，複数のサービス提供者の緩やかな連携により実現するオープンなサービスモデルの構築を目的とする．具体的には，電子メールサービス，ネットニュースサービス(USENET)，インターネット・リレー・チャットなど，高速な常時接続のネットワークを前提としない古典的なメッセージ型サービスモデルを参考に，Peer to Peer (P2P) ファイル共有ネットワークの技術を中核に据え，クライアント側の高機能化を活用しつつ，動的でスケーラブルなネーミングシステム技術，中央集権的でない認証連携技術を組み合わせる．

一般に，動的なコンテンツを提供する Web サイトはバックエンドにデータベースが存在する構成を取る．それを冗長化して負荷分散するためには，分散データベースにおける同期と一貫性

制御の問題が伴う．この分野における多くの研究が示すように，高速かつ常時接続のネットワークを必ずしも前提としない状況において，この問題を全世界レベルでスケーラブルな形で解決することは困難である．これに対し本研究では，対象をメッセージ型の情報共有サービスに限定し，同期と一貫性制御の制約を緩和することで，この問題を回避して全世界レベルでスケールするサービスの構築を目指す点が特徴的である．

本研究により，一定の信頼度を持つサービス提供者であれば誰もが参入できるような，緩い連携による全世界レベルのオープンなサービスが提供されるようになることで，草創期のインターネットと同様の自律分散かつオープンな情報共有基盤を，今日の社会で要請される高いセキュリティとプライバシーのレベルで実現するとともに，より一般的な Web サービスのスケーラビリティの向上とオープン化に関しての研究につながる点に意義がある．

３．研究の方法

提案するメッセージ型 Web サービスでは，複数の事業者の間で緩やかに連携する Web サーバ群がリアルタイムに情報を交換することで，自律分散型でありながら，全体としてあたかも一つの巨大な事業者が運用しているのと等価に見えるアーキテクチャをとる．そのために，メッセージ型 Web サービスのコンテンツを Web サイトに依存しない識別子で扱えるように定式化し，それらのコンテンツを P2P 型ファイル共有により Web サーバ間で交換させるようにすると同時に，コンテンツが多くの Web サーバ間で共有される状況において生じるセキュリティやプライバシーの問題を，認証連携とグループ管理により解決する．

フラッシュクラウドは，短時間に大量のトラフィックが発生することと，発生の時期や対象となる Web サイトの予測が難しいことが特徴である．本研究では，平時から多くの Web サーバ群が協調しあい，フラッシュクラウドのように一時的に一つのコンテンツにアクセスが集中するようなケースにおいても，ユーザからのアクセスが複数の Web サーバに自動的に分散される相互扶助的仕組みを，広告型を代表とする Web サービス運用のビジネスモデルと整合させる．そのための鍵が，コンテンツを，URL（Uniform Resource Locator）のような Web サイトそのものを含む形の識別子ではなく，URN（Uniform Resource Name）のような Web サイトには依存しない形の識別子で扱うことである．

この考え方に基づき，本研究提案において解決すべき要件は，大別して，動的なものも含めた Web サイトのコンテンツを URN 型の識別子（メッセージ ID）で扱えるようにすること，コンテンツを多くの Web サーバ間で共有させアクセスの負荷を分散させること，コンテンツが多くの Web サーバ間で共有される状況においてセキュリティやプライバシーの問題を解決すること，の 3 点に分類される．各要件について詳細化しそれらを統一的に解決する
アーキテクチャを確立する．

４．研究成果

(1) メッセージのフォーマットと識別子

識別子については，静的なコンテンツであれば，コンテンツのオリジナルが置かれていた Web サイトでの URL と時刻の情報を組み合わせて URN として扱うことで，比較的簡単に扱える．これはこれまで Web サイトのキャッシュサーバにおいて扱われていたのと同様である．しかるに，本研究で考えるフラッシュクラウドは，ブログとそれに対するコメントに代表される，動的なコンテンツであり，URL と時刻の情報だけではうまく扱えない．そこで，本研究では，電子掲示板，SNS，ブログ，マイクロブログ，チャットなどのいわゆるメッセージ型の Web サービス上のコンテンツを，イベント型の比較的サイズの小さなコンテンツと，静的なコンテンツとで区別し，メッセージを体系化して複数のサイトで共有できるようにする．

このような試みは，すでに SNS の代表格である Facebook やマイクロブログの代表格である twitter などのサービスにおいて，異なるサービス間の連携のための API が公開されてることの延長上である．これら既存の連携方式では，API が各サービスの独自定義のものであることに加え，コンテンツそのものは各サービスが保持し他の事業者へ流通させるようにはなっていない点で，フラッシュクラウドの問題の解決にはなっていない．これに対し，本研究提案では，たとえばブログ記事とそれに対するコメント，Facebook における「いいね！」，twitter におけるリツイートなどを，すべてイベントとしてとらえ，それをコンテンツとして流通できるように検討した．その具体的な方法として分散・連合型のミニブログのオープンな標準である OStatus に準拠し，イベント型のメッセージのフォーマットは RFC4287 (The Atom Syndication Format)ならびに RFC4685 (Atom Threading Extensions)に従うこととした．P2P で共有しつつデータの内容をグループ外のメンバーに対して秘匿するメカニズムとして，S/MIME に準じたメッセージの電子署名・暗号化方式と，秘密分散共有ならびに P2P マルチキャストにおける動的鍵配信の仕組みを応用する手法を提案し，詳細化，プロトタイプ実装した．

(2) 負荷分散方式

負荷分散方式を考えたとき，もっとも単純なものは，Web サーバ同士でお互いにすべてのデータの複製を持ち合い，負荷に応じて他の Web サーバへリクエストを分散する方式である．しかし，この方式では，全てのサーバが異なる Web コンテンツを提供しているとすると，サーバ台数に比例する数の Web サイトの複製が発生するため，サーバの台数が増加するに従って複製の

数が膨大になってしまい，全世界レベルではスケールしない．そのため，前述の要件を満たす負荷分散方式を有効なものとするためには，すべてのデータの複製を行うのではなく，CDN (Content Derivery Networking) や CCN (Content Centric Networking)のように負荷が高まっているデータのみ複製を行う仕組みが必要となる．

そこで， P2P 型ファイル共有を活用して複数の Web サーバが協調することで静的コンテンツの Web サービスのフラッシュクラウド耐性の強化を行う手法と，ネットニュースで用いられているバケツリレー型の情報流通とを融合させるアーキテクチャを採ることとした．本手法では，高効率なコンテンツ配信の仕組みとして用いられている P2P ファイル共有ネットワークの性質を活かし，全ての Web サーバが P2P ファイル共有ネットワークに参加し，自身の Web サイトを P2P ファイル共有ネットワーク経由でアクセス可能とすることによって，負荷が高まっているデータのみ効率よく複製を行う仕組みが実現される．

提案手法では，平常時は通常通り自身の Web サーバで処理を行い，負荷の高まりに応じて予め協調関係を結んでおいた他のサーバへ負荷を分散する．また，協調関係にある他のサーバの負荷が高まった場合は，そのサーバに代わって自身の Web サーバでリクエストを処理する．負荷が高まっている協調関係にあるサーバの Web サイトを自身のサーバで提供する際，その Web サイトのデータの取得を，P2P ファイル共有ネットワークから行う．P2P ファイル共有ネットワークは，多くの人がアクセスする人気のあるファイルほど，多くのキャッシュが存在し，ダウンロードに掛かる時間が短くなるという特徴があるため，P2P ファイル共有ネットワークをデータ交換に利用することによって，高負荷の状況において素早く Web サイトのデータを取得し代理で提供を開始することが可能となる．さらに，P2P ファイル共有ネットワークに直接参加可能なクライアントによっても負荷分散が行われるようにする．

P2P ファイル共有ネットワークとしては，初期段階では，広く用いられている BitTorrent のファイル共有の速度と効率，それを用いたシステムのフラッシュクラウド耐性と，OStatus に基づく連合型 SNS の実装である GNU social ならびに Mastdon を評価し，BittTorrent は大容量データの配布においては高効率である一方，メッセージのような比較的サイズの小さなデータを小さい遅延で配送するようには設計されていないことを明らかにした．

さらに，Web サーバの負荷分散アーキテクチャ，ならびにクライアント側での高負荷時のトラフィック優先制御による Web QoE (Quality of Experience)を向上させる技術を開発した．基盤となる高集積マルチテナント環境で動作している Web サーバが高負荷時にもリソース配分が適切に行われ，特定のリクエストが集中してもそれによりリソースが消費されサービスが不能にならないようにするアーキテクチャとして，リクエスト単位で仮想的にハードウェアリソースを分離する Web サーバのリソース制御アーキテクチャを示し,そのようなサーバにおいて HTTP/2 を用いることや IETF で標準化がすすめられている QUIC を用いることの利点，認証などセキュリティ上の課題についても検討を行った．

(3) 認証とグループ管理

P2P ファイル共有ネットワークと，SNS などメッセージ型 Web サービスとの大きな違いは，前者が基本的に公開のコンテンツであるのに対し，後者は必ずしもそうではなく，Facebook の「友達」のような，あらかじめメッセージの作成者が指定し管理するグループのメンバーに対して限定的に公開できるような機能が必須であることである．このような仕組みを単一事業者ではなく複数の事業者間の緩やかな連携によって実現するにあたっては，非公開のメッセージが暗号化されて配信され,復号がエンドユーザのクライアント上で行われることが望まれる.また，なりすましによる偽情報発信を防ぐために，メッセージには作成者の電子署名が付され，流通時ならびにクライアント側での復号時に電子署名が検証されることが望まれる．これが，セキュリティおよびプライバシー上の課題である．

本研究では，メッセージ型 Web サービスの提供者とは独立の，認証基盤の管理者(IdP) ならびにグループのメンバー属性の管理者(mAP) が存在するアーキテクチャを考え，IdP が管理する電子署名鍵，mAP が管理する暗号鍵により，暗号化と署名検証ができるようにした．また合わせてメッセージには有効期限を設定するようにし，期限が過ぎれば対応する鍵を無効化することで，発信した情報が作成者の意図に反してネット上で流通しないようにした．

このような仕組みを複数の事業者間の緩やかな連携により実現するための仕組みとして，Web サービスにおける認証連携のしくみである SAML に倣い，複数の事業者による閾値型認証と秘密分散を組み合わせることで，特定のサーバが単一障害点(single point of failure)となることなく，かつ冗長度を増やすことによるセキュリティ上の懸念を増やすことのない方式を検討した．P2P ファイル共有ネットワークと SNS などメッセージ型 Web サービスとの違いは，前者が書き換えのない静的なコンテンツをすべての参加者に対して共有するのに対し，後者はメッセージの作成者あるいは第三者が管理するグループのメンバーに対して限定的に共有され，またコメントや「いいね！」などメッセージに紐づく動的なアクションがなされることである．そのため P2P で共有しつつデータの内容をグループ外のメンバーに対して秘匿するメカニズムをとして，秘密分散共有ならびに P2P マルチキャストにおける動的鍵配信の仕組みを応用する手法を開発した．またメッセージに対する処理を，内容を秘匿したまま近隣のノードに負荷分散する仕

組みについても提案した.

さらに必要となるユーザ認証についても，ユーザとメッセージとの間に仮名性が必要であることと，認証サーバ(IdP)とユーザの関係が固定的でなく自律分散的である必要があることを前提に加え,ユーザが仮名性を保ちつつ IdP を移動する(migration)ことができる仕組みを提案し，Single Sign-On の実装に用いられている SAML ベースの認証連携のオープンソースプロジェクトである Shibboleth を使用し実装した.

一方，なりすましによる偽情報発信を防ぐための本人確認を，自律分散性と匿名性を両立し，かつ否認不能性を担保するための方式について検討し，Blockchain の技術よる暗号化通貨である Bitcoin にゼロ知識証明を適用して匿名性を高めた Zerocoin の応用やについて検討した.P2P 型で懸念されるノードの不正の問題を，他のノードにより事後に検証したり，他のノードのデータを暗号化したままの状態で操作するような方式について検討し，P2P 型 MMO (Massively Multiplayer Online)ゲームで開発された技術を利用できることを示した.

またメッセージの発信者の仮名性と，違法性があるなど不正なコンテンツの発信者の追跡を両立させるためのアーキテクチャを検討した．具体的には，P2P 型の報発信システムにおいて，発信者の仮名性(pseudonymity)を担保しつつ，テロ予告など，違法な情報発信であると P2P ネットワークに参加する運用者の大多数でコンセンサスが得られる場合には，発信者の追跡が可能(tracable)な仕組みについて，要求要件の明確化とその実装について検討し，電子署名を用いたシステムを設計・実装した．また，それとともに，発信者の認証と実際の情報発信を認証プロキシを介して分離することで，発信者の匿名性を向上させる仕組みも提案し実装した.

５．主な発表論文等

〔雑誌論文〕　計12件（うち査読付論文　9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 Satsuki Nishoka, Yasuo Okabe	４．巻 2
２．論文標題 Centralized Control of Account Migration at Single Sign-On in Shibboleth	５．発行年 2020年
３．雑誌名 Proc. IEEE 44th Annual Computers, Software and Applications Conference	６．最初と最後の頁 1572-1578
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 河野圭太，稗田隆，中村素典	４．巻 21(1)
２．論文標題 ShibbolethとOpenAMの連携による認証レベルを制御可能なシングルサインオン基盤の構築	５．発行年 2018年
３．雑誌名 学術情報処理研究	６．最初と最後の頁 71-81
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.24669/jacn.21.1_71	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 松本亮介，栗林健太郎，岡部寿男	４．巻 59
２．論文標題 リクエスト単位で仮想的にハードウェアリソースを分離するWebサーバのリソース制御アーキテクチャ	５．発行年 2018年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 1016-1025
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 松本亮介，栗林健太郎，岡部寿男	４．巻 J101-B
２．論文標題 Webサーバの高集積マルチテナントアーキテクチャと運用技術	５．発行年 2018年
３．雑誌名 電子情報通信学会論文誌B	６．最初と最後の頁 16-30
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Hiroyuki Sato, Yasuo Okabe, Motonori Nakamura	４．巻 25
２．論文標題 User Identification of Pseudonyms without Identity Information Exposure - A Scenario in Access Federations	５．発行年 2017年
３．雑誌名 Journal of Information Processing	６．最初と最後の頁 788-795
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.25.788	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 Kazuma Matsumoto, Yasuo Okabe	４．巻 2
２．論文標題 A Collusion-resilient Hybrid P2P Framework for Massively Multiplayer Online Games	５．発行年 2017年
３．雑誌名 Proc. IEEE 41th Annual Computer Software and Applications Conference (COMPSAC2017)	６．最初と最後の頁 342-347
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/COMPSAC.2017.10	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 Tomohiro Ito, Daisuke Kotani, Yasuo Okabe	４．巻 2
２．論文標題 A Threshold-based Authentication System Which Provides Attributes Using Secret Sharing	５．発行年 2017年
３．雑誌名 Proc. IEEE 41th Annual Computer Software and Applications Conference (COMPSAC2017)	６．最初と最後の頁 730-735
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/COMPSAC.2017.38	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 松本 亮介・岡部 寿男,	４．巻 55
２．論文標題 mod_mruby：スクリプト言語で高速かつ省メモリに拡張可能なWebサーバの機能拡張支援機構	５．発行年 2014年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 2451-2460
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 辻尾尚樹,岡部寿男	４．巻 114(335)
２．論文標題 自治が可能なP2P型匿名Publish/Subscribeシステム	５．発行年 2014年
３．雑誌名 電子情報通信学会技術報告	６．最初と最後の頁 13-17
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 田島照久，岡部寿男	４．巻 114(335)
２．論文標題 802.11無線LANにおけるバックオフ時間の制御とアクセスポイントのバッファ最適化による低遅延無線の提案	５．発行年 2014年
３．雑誌名 電子情報通信学会技術報告	６．最初と最後の頁 25-27
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 清水 さや子，戸田 勝善，横田 賢史，岡部 寿男	４．巻 8
２．論文標題 統合IDに基づく効率的な権限移譲が可能なグループ管理システム	５．発行年 2018年
３．雑誌名 情報処理学会論文誌コンシューマ・デバイス&システム（CDS）	６．最初と最後の頁 20-31
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 Yu Takabatake, Daisuke Kotani, and Yasuo Okabe	４．巻 116-IA2016
２．論文標題 An anonymous distributed electronic voting system using Zerocoin	５．発行年 2016年
３．雑誌名 IEICE Tech. Rep	６．最初と最後の頁 127-131
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 －

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　5件）

１．発表者名
西岡幸来，岡部寿男

２．発表標題
Shibbolethでのシングルサインオンにおけるアカウント移動の一括制御

３．学会等名
情報処理学会第81回全国大会 7ZA-08

４．発表年
2019年

１．発表者名
岡部寿男

２．発表標題
ユーザの結託による不正に強いハイブリッドP2P型MMOゲームフレームワーク

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(DICOMO2017)シンポジウム

４．発表年
2017年

１．発表者名
Yoshiharu Tsuzaki, Yasuo Okabe

２．発表標題
Reactive Configuration Updating for Intent-Based Networking

３．学会等名
The 31st International Conference on Information Networking (ICOIN2017)（国際学会）

４．発表年
2017年

１．発表者名
Teruhisa Tajima, Yasuo Okabe

２．発表標題
Optimizing Packet Transmission Scheduling for Enhanced Web QoE in Wireless LAN

３．学会等名
The 4th IEEE International Workshop on Consumer Devices and Systems (CDS)（国際学会）

４．発表年
2016年

１．発表者名
伊藤 友浩，小谷 大祐，岡部 寿男

２．発表標題
属性情報を秘密分散した閾値型認証システムの設計

３．学会等名
電子情報通信学会インターネットアーキテクチャ研究会

４．発表年
2016年

１．発表者名
Yu Takabatake, Yasuo Okabe

２．発表標題
An anonymous distributed electronic voting system using Zerocoin

３．学会等名
IEICE Workshop on Internet Architecture and Applications 2016（国際学会）

４．発表年
2016年

１．発表者名
Hiroshi Ueda, Motonori Nakamura

２．発表標題
GakuNinMoodle: Toward Robust E-Learning Services using Moodle in Japan

３．学会等名
20th International Conference KES-2016 (Knowledge-Based and Intelligent Information & Engineering Systems)（国際学会）

４．発表年
2016年

１．発表者名
Naoki Tsujio, Yasuo Okabe

２．発表標題
A Traceable and Psudonymous P2P Information Distribution System

３．学会等名
The 1st IEEE International Workshop on Middleware for Cyber Security, Cloud Computing and Internetworking (MidCCI2015)（国際学会）

４．発表年
2015年

１．発表者名
桑原 貴明，岡部 寿男

２．発表標題
DDoS攻撃を防止するソフトウェアルータについて

３．学会等名
電子情報通信学会2016年総合大会

４．発表年
2016年

１．発表者名
伊藤 友浩，岡部 寿男

２．発表標題
複数のIdPを用いたシングルサインオンの提案と実装

３．学会等名
電子情報通信学会2016年総合大会

４．発表年
2016年

１．発表者名
岡部 寿男，山口 弘純，安本 慶一

２．発表標題
情報流技術とエッジコンピューティング

３．学会等名
電子情報通信学会2016年総合大会

４．発表年
2016年

１．発表者名
辻尾尚樹，岡部寿男

２．発表標題
発信者追跡可能かつ仮名型のP2P情報発信システム

３．学会等名
情報処理学会第77回全国大会

４．発表年
2015年

１．発表者名 田島照久，岡部寿男
２．発表標題 Webブラウジング高速化のためのTCPヘッダに基づく802.11無線通信最適化
３．学会等名 情報処理学会第77回全国大会
４．発表年 2015年

１．発表者名 Naoki Tsujio, Yasuo Okabe
２．発表標題 A Tracable and Pseudonymous P2P Information Distribution System
３．学会等名 MidCCI 2015: 1st IEEE International Workshop on Middleware for Cyber Security, Cloud Computing and Internetworking
４．発表年 2015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
研究分担者	中村　素典 (Nakamura Motonori) (30268156)	京都大学・学術情報メディアセンター・教授 (14301)	
連携研究者	宮崎　修一 (Miyazaki Shuichi) (00303884)	京都大学・学術情報メディアセンター・准教授 (14301)	