# 科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　２１　日現在

機関番号：　１３９０３
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００８５

研究課題名（和文）高い匿名性と安全性を有する家庭向けオーバーレイネットワークシステム

研究課題名（英文）An Overlay Network System with High Level of Anonymity and Security for Home Use

研究代表者
斎藤　彰一（SAITO, Shoichi）

名古屋工業大学・工学（系）研究科（研究院）・准教授

研究者番号：７０３０４１８６

交付決定額（研究期間全体）：（直接経費）　　3,800,000円、（間接経費）　　1,140,000円

研究成果の概要（和文）：本研究において，匿名通信における匿名性の向上と，携帯端末などの性能の低い計算機や家庭や移動端末等のネットワーク環境における匿名通信利用について研究を行った．さらに，新しい通信方式である送信者追跡困難通信を開発した．この新方式は，追跡困難性による利用者個人情報の保護と，匿名性の悪用を防止することが可能である．これらの研究成果は，個人情報を保護するネットワークを備えたネットワークインフラの構築に貢献できると考える．

研究成果の概要（英文）：I made a study on anonymous communication system. The first characteristic of my research is improvement of anonymity. The second is usability of mobile devices which are low computing performance and under a home-network environment. Moreover, I developed a novel privacy enhancement communication system which administrators of Web server cannot pursue users. The proposed communication system can prevent users of web from abusing anonymity, and difficulty of pursuit in the system protect privacy information from leaking. The results of my research can contribute for constructing network infrastructures with preventing privacy information from leaking.

研究分野：　総合領域

科研費の分科・細目：　計算機システム・ネットワーク

キーワード：　ネットワークセキュリティ　プライバシー保護　匿名通信　追跡困難通信　分散ハッシュテーブル　オーバーレイネットワーク

## １．研究開始当初の背景

本研究では,オーバレイネットワークにおける匿名性と安全性を兼ね備え，さらに家庭環境を想定した通信方式を実現する．匿名性とは，通信の送信者計算機と受信者計算機とその経路を第三者が特定できないことを指す．安全性とは検索時における攻撃計算機への誘導，攻撃者の特定機能を指す．さらに．家庭環境を想定とは,xDSL 接続による NAT やファイヤウォール環境での利用と低性能のプロセッサでも十分な性能の通信を可能とすることを指す．

本研究の社会的意義として,内部告発者の保護を目的とした公益通報者保護法が 2006 年 4 月より施行されており，匿名性を持った通信は今後社会的なニーズが大きく増加すると考える．

## ２．研究の目的

本研究では，分散ハッシュテーブルを用いた匿名通信システムの匿名性向上と家庭における計算機環境とネットワーク環境における匿名通信システムの開発を目的とし，次の 4 つの課題を挙げた．

(1) 通信路を決定する際のシステム参加計算機の取得をきっかけとする経路情報漏洩防止
(2) 次接続計算機を DHT で検索する際の経路情報漏洩防止
(3) 中継用計算機が異常離脱した場合の安全な通信路復旧処理
(4) 受信者計算機の送信者計算機に対する匿名性向上

また,「(5) 家庭環境向けの新しい軽量の匿名通信システム」について新たに検討し構築することを目指す．これら(1)から(5)により，匿名通信における匿名性の向上と利用範囲の拡大を実現し，内部告発者の保護を目的とした公益通報者保護法における利用や，匿名カウンセリングなどにおける利用を可能とする．

さらに，新たな通信システムにおいては，悪用に備えて完全な匿名性ではなく，日常利用において有意な利用者特定困難性の実現を目指し，悪用が判明した場合には送信者計算機を特定できることを目指す．

## ３．研究の方法

申請者の従来研究である匿名通信システム Bifrost[参考文献 1] を基盤として，研究および実装を行う．また，分散ハッシュテーブルの課題については，DHT 基盤である OverlayWeaver [参考文献 2] を使用することで，課題となる問題点に集中できる開発体制を採る．さらに，広域実験においては，Planetlab [参考文献 3]を活用することによって，全世界的な規模での分散実験を行う．目的(5)に関しては，複数のインターネットサービスプロバイダ(ISP)と家庭を模した小規模なネットワーク環境を構築し，その中でシステム開発と実験を行った．また，システム開発は申請者の研究室に所属する学生に協力を依頼し，それぞれの課題に取り組んだ．

## ４．研究成果

各課題に対する研究成果について述べる．

(1) ID ベース暗号[参考文献 4]を用いることで，事前の鍵交換を行わずに暗号化のための鍵共有を実現できる．しかし，そのためには通信相手の ID（識別子）を取得しなければならない．匿名通信では，参加ノードを事前に把握は困難であり，また匿名性を低下させる要因でもあるために参加計算機の把握は実施しないことが求められる．そこで，本研究では，計算機を分散ハッシュテーブルに配置するための ID 割り当てに規則を設けることで，通信相手の ID を特別な通信なしに取得可能とした．この規則に従って計算機に ID を割り当てると，各計算機の近傍の ID 割り当て状況を確認するだけで，割り当て済み最大 ID を推測することが可能である．

分散ハッシュテーブルでは，ネットワークを維持するための通信が必要である．この通信は，匿名通信とは無関係であることから，この維持のための通信によって匿名性が低下することはない．本研究では，この維持のための通信を利用して，近傍計算機の配置状況を把握し，その状況と ID 割り当て規則から参加済みの計算機 ID を特定する手法を開発した．これにより，1 つ目の課題を解決した．本研究成果は，業績論文[1]と[2]で発表した．

(2) 分散ハッシュテーブルを用いて通信経路を構築する際に問題となる点として，分散ハッシュテーブルにおける検索が正しく行われているかの確認が難しい点がある．このため，検索結果を改ざんすることによって，悪意ある計算機のみを使用する通信経路を構築することが可能である．この問題については，分散ハッシュテーブルの研究においていくつかの研究があるが，本研究としては匿名性を維持する必要がある点が大きく異なる．

本研究では，参加している計算機が正常な ID を所有して正しくネットワークに接続していることを，匿名性を保持したまま証明する方法を確立した．この方式は，Myrmic[参考文献 5]を基盤とした方式で，匿名性を確保するために計算機がネットワークに参加する時の通信相手の数を最小限とするように改良している．さらに，各計算機が近隣の計算機と ID を確認しあうことにより，各計

算機の存在をお互いに証明しあうことが可能である．これらにより，必要最小限の計算機との通信のみで ID の正当性を確認可能となり，匿名性を低下させずに匿名通信路を構築できる．なお，本方式は分散ハッシュテーブルとして Chord[参考文献 6]を使用している．本研究成果は，業績論文[4],[8],[12]で発表した．

(3) 匿名通信システムの特徴として，複数の中継計算機を経由して送信者計算機から受信者計算機に至る点がある．また，各中継計算機に送信者計算機と受信者計算機を特定されないために，各中継計算機はそれぞれ中継時に暗号処理を行う．このような特徴から，中継計算機が通信途中で離脱した場合，匿名通信路を正しく維持できないという問題がある．本研究では，この問題に対して，各中継計算機の代理となる計算機を利用する方式を開発した．この方式の特徴として，代理計算機の指定には，通信を必要とすることはなく，代理計算機の利用によって匿名性が低下することはない．代理計算機を用いることで，匿名性を低下させずに中継用の暗号鍵を更新し，通信路を修復することが可能である．本研究成果は，業績論文[5],[13],[14]で発表した．

(4) 通信システム一般において，受信者計算機（サーバ）は，送信者計算機（クライアント）にその名前や IP アドレスを公開していることから，匿名で運用することは難しい．本課題は，サーバのクライアントに対する匿名性を向上させることが目的である．本研究では，サーバは，第三者が運用する計算機を接続用計算機として事前に設定して，その接続用計算機を自身の代わりに公開する．クライアントは，この接続用計算機を経由して，サーバに対して接続要求を行う．この際，クライアントは，多重暗号処理を施した通信路開設メッセージをサーバに対して送る．この通信路開設メッセージは，サーバからクライアントへの経路を指定した匿名通信路開設メッセージである．この際，サーバにはクライアントの IP アドレス等を開示する必要はなく，クライアントは自身に向けた開設メッセージを作成するのみであるため，クライアントの匿名性を低下させることはない．接続要求を受けたサーバは，クライアントから送られてきた通信路開設メッセージを用いて，クライアントとの間の匿名通信路を開設する．以上により，クライアントは接続用計算機のみしか知ることはなく，またサーバはクライアントを知ることなしに匿名通信路を開設可能である．本研究成果は，課題(3)の前段階として実施した．

(5) 家庭環境向けの新しい軽量の匿名通信システムにおいては，①NAT やファイアウォールへの対応，②携帯端末などの低性能の計算機に対する対応，③新しい方式の提案の 3 点について研究を実施した．

①家庭用の匿名通信システムとして，NAT やファイアウォール環境下での使用について，分散ハッシュテーブルを用いたネットワークをこのような環境下で構築する方式について開発を行った．NAT やファイアウォール環境下では，インターネット側からファイアウォール内部への通信は遮断されるため，内部から通信を開始する必要がある．このために通常の分散ハッシュテーブルの構築手順ではネットワークを構築することはできない．この点を改良し，NAT やファイアウォール環境下における分散ハッシュテーブルへの参加手順を確立した．本研究は業績論文[11]において発表した．

②匿名通信システムでは，通信に際して多重暗号処理を用いる．また，他の計算機が送信したパケットの中継を行う必要もある．そのため，性能の低い計算機では，これらの負荷によって著しく性能低下することが予想される．この課題に対して，携帯端末などの計算性能やネットワーク性能が低い計算機では，中継計算機としての役割を拒否できる仕組みを構築した．これは，通信路構築時に，送信者計算機に対して中継計算機を引き受けるか否かを通知する機能を付加することで実現した．これにより，計算機の負荷軽減を実現した(業績論文 [10])．次に，中継を拒否するのではなく，中継計算機候補そのものにならない仕組みを開発した．しかし，中継計算機候補にならないことは送信者専用計算機であることを意味するため，送信専用計算機の匿名性が低下する問題がある．つまり，通常の匿名通信では，自身が発した通信と他の計算機が発した通信の両方が混在することにより，自身の通信の特定を困難にしているが，送信専用計算機ではすべての通信は自身が発する通信となるために特定が容易である．これに対するために，送信用 IP アドレスと受信用 IP アドレスを使い分けることで，送信用 IP アドレスが送信専用計算機のものか否かを判断できないようにした．これにより，送信専用計算機が通信していることを中継用計算機に漏洩することがなくなる．本研究は業績論文[9]で発表した．

③匿名通信システムを活用しつつ，犯罪への悪用を防止するために，軽量かつ受信者計算機による送信者計算機の特定が困難な新しい通信システムを構築した．これは，完全な匿名性を実現するのではなく，受信者計算機（一般的には Web サーバ運用者）による，送信者計算機（Web ブラウザの利用者）の特定を困難にする通信方法である．さらに，悪用された場合には受信者計算機の協力のもとで送信者計算機を特定できる通信方式である．この方式は，複数のインターネットサービスプロバイダによって運用される中継サーバによって構成される．送信者計算機による通信は，2 つのインターネットサービス

プロバイダが運用する中継サーバを経由して目的となる受信サーバに到達する．この時，暗号通信を用いることで，経由する 2 つのインターネットサービスプロバイダは，送信者計算機と受信者計算機の双方を同時に知りえない．しかし，通信の時刻と受信者計算機の IP アドレスに基づいて，当該通信を中継した両インターネットサービスプロバイダの協力を得ることで，送信者計算機を特定できる．本研究成果は，業績論文[3],[6],[7]で発表し，さらに多数の暗号通信を処理するための高速な通信基盤に関する研究を進めている．

[参考文献 1] Masaki Kondo, Shoichi Saito, Kiyohisa Ishiguro, Hiroyuki Tanaka, and Hiroshi Matsuo: Bifrost: A Novel Anonymous Communication System with DHT, Second International Workshop on Reliability, Availability, and Security, pp. 324-329 (2009.12).
[参考文献 2] 首藤一幸,田中良夫,関口智嗣, オーバレイ構築ツールキット Overlay Weaver, 情報処理学会論文誌：コンピューティングシステム ,Vol.47,No.SIG12(ACS15),pp.358-367 (2006).
[参考文献 3] PLANETLAB, http://www.planet-lab.org/.
[参考文献 4] Boneh, D. and Franklin, M.: Identity-Based Encryption from the Weil Pairing, SIAM Journal on Computing, Vol. 32, No. 3, pp. 586-615 (2003).
[参考文献 5] Wang, P., Osipkov, I., Hopper, N. and Kim, Y.: Myrmic: Secure and robust dht routing, U. of Minnesota, Tech. Rep (2006).
[参考文献 6] Stoica, I., Morris, R., Karger, D., Kaashoek, F. and Balakrishnan, H.: Chord: A Scalable Peer-To-Peer Lookup Service for Internet Applications, Proc. 2001 ACM SIGCOMM Conference, pp. 149-160 (2001).

５．主な発表論文等
（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 ２件）
[1] 田中寛之，齋藤彰一，松尾啓志，匿名通信におけるディレクトリサーバを用いないノード管理方式，情報処理学会論文誌，査読有，Vol. 53, No. 5, pp. 1558-1569 (2012.5).
[2] Hiroyuki Tanaka, Shoichi Saito, and Hiroshi Matsuo, Node Management without Directory Servers in DHT-based Anonymous Communication Systems using ID-based Encryption, International Journal for Information Security Research, 査読有，Vol. 1, No. 3, pp. 154-163 (2011.9).

〔学会発表〕（計 ３件）
[3] 川澄昇弘，齋藤彰一，松尾啓志，Web ブラウジングにおけるユーザの行動追跡を困難にする軽量な通信方法の提案，2014 年 暗号と情報セキュリティシンポジウム，2014.1.23，鹿児島市.
[4] 中井俊作，野々山正峰，齋藤彰一，松尾啓志，DHT におけるノード検証手法と匿名通信への適用，情報処理学会研究報告 2012-CSEC-60，2013.3.15，東京都足立区.
[5] 八田望，齋藤彰一，松尾啓志，ノード結託による通信路漏洩を防止する匿名路修復方式の提案，コンピュータセキュリティシンポジウム 2012，2012.10.31，松江市.

〔その他〕
○卒業論文
[6] 秦誠一郎，ユーザ認証の有無に応じた IP アドレス選択による追跡困難性向上方式の提案，名古屋工業大学，2014.3.
[7] 川澄昇弘，複数の ISP 連携による利用者 IP アドレス追跡が困難な通信方式の提案，名古屋工業大学，2013.3.
[8] 野々山正峰，DHT の近傍ノード協調型確認手法における Neighborhood Authority の分散方式の提案，名古屋工業大学，2013.3.
[9] 竹下修平，DHT を用いた匿名通信システムにおけるクライアントノードの負荷軽減手法，名古屋工業大学，2013.3.
[10] 廣瀬宗則，多重暗号による匿名通信における携帯端末の負荷軽減手法，名古屋工業大学，2012.3.
[11] 高柳光一，分散ハッシュテーブル Chord の NAT 対応機構の設計と実装，名古屋工業大学，2012.3.
○修士論文
[12] 中井俊作，近隣ノード協調による安全かつ匿名なノード管理手法，名古屋工業大学大学院，2013.3.
[13] 八田望，中継ノードの結託を防止する匿名通信路修復方式，名古屋工業大学大学院，2013.3.
[14] 酒井衛，匿名通信における鍵複製を行わない通信路修復，名古屋工業大学大学院，2012.3.

６．研究組織
(1)研究代表者
齋藤 彰一（SAITO, Shoichi）
名古屋工業大学・大学院工学研究科・准教授
研究者番号：70304186

(2)研究分担者
なし