

第1章 ネットワーク研究部門

1.1 高機能ネットワーク研究分野

1.1.1 スタッフ

職名	氏名	専門分野
教授	岡部 寿男	コンピュータネットワーク
准教授	宮崎 修一	アルゴリズム, 計算量理論
助教	小谷 大祐	コンピュータネットワーク

1.1.2 研究内容紹介

1.1.2.1 岡部 寿男

次世代, 次々世代インターネット技術により, あらゆるものがネットワーク機能を内蔵し, あらゆるところで利用可能となる, ユビキタスネットワーキング環境の実現と利用のための技術の研究を行っている。

IPv6 を用いたインターネットの高信頼化・高機能化 次世代インターネットの基本技術である IPv6 には, ネットワークの端末を識別するアドレス空間が広大 (2^{128}) にある。このアドレス空間を活用した, マルチホーミングによる高信頼化技術, モバイル技術, 端末およびルータの自動設定技術を開発している。応用としては, インターネット家電, インターネット携帯電話, インターネット放送が挙げられる。

マルチメディアストリームデータのリアルタイム伝送 ベストエフォート型サービスであるインターネットで, 映像・音声などのマルチメディアデータを高品質にリアルタイム伝送するため, 資源予約プロトコルによる IP レベルでの品質 (QoS; Quality of Service) の保証や, 誤り訂正符号, パスダイバーシティの活用などをサポートするマルチメディアストリーム配信システムを開発してきている。応用としては, 遠隔講義用高品位映像伝送システム, IP ワイヤレスカメラ・マイクが挙げられる。

インターネット上の諸問題に対するアルゴリズムの設計と解析 インターネットを構築・運用する上で必要な高性能アルゴリズムの開発を行っている。特にルータのバッファ管理問題に対するオンラインアルゴリズム (全ての入力を与えられる前に判断を下すアルゴリズム) の設計と解析において成果をあげている。応用としては, ルータでのバッファ管理, ルーティングアルゴリズムが挙げられる。

インターネット上のコミュニケーションにおけるプライバシー保護と不正防止 インターネット上で見知らぬ相手と通信する際に, 相互に必要な最小限の情報を交換し相手に不正を働かせないことを保証するための, 暗号や電子証明などの技術を利用した安全なプロトコルの開発と, その応用, 実装に関する研究を行っている。応用としては, ロケーションプライバシー, 電子透かし, ネットワークゲーム, Web 認証が挙げられる。

エネルギーの情報化 オンデマンド型電力ネットワークの実現に向けて, 情報通信技術をエネルギー管理へ応用する研究を行っている。インターネット上で使われているルーティングや資源予約などのプロトコルを電力ネットワークに適用させるための検討や, 電力スイッチング技術の開発・実装を行っている。応用としては, 省エネルギーの自動化が挙げられる。

1.1.2.2 宮崎 修一

ネットワーク問題やグラフ問題をはじめとした、離散組合せ問題に対するアルゴリズムの効率についての研究を行っている。最近では、NP 困難問題に対する近似アルゴリズムの近似度解析やオンラインアルゴリズムの競合比解析を主に行っている。

近似アルゴリズム 問題が NP 困難である場合、多項式時間で最適解を求めるアルゴリズムの存在は絶望的である。NP 困難問題に対するアプローチの一つとして、近似アルゴリズムがある。近似アルゴリズムでは、解の最適性をあきらめる代わりに、アルゴリズムの動作時間を多項式時間に限定するというものである。アルゴリズムの良さは、それが求める解と最適解との近さの最悪値（近似度）で評価される。厳密には、アルゴリズム A が r -近似アルゴリズムであるとは、任意の入力に対して A が求める解のコストと最適解のコストの比が r 倍以内であることを言う。近似アルゴリズムの研究は、主に、上限の研究（近似度がより 1 に近いアルゴリズムを開発すること）と下限の研究（ $P \neq NP$ の仮定の下で、近似度をそれより下げることができないことを証明すること）の両面から行われている。

オンラインアルゴリズム 通常の問題は、入力が全て与えられてから計算を行う。オンライン問題では、入力はイベントの列として定義される。イベントが次々と与えられ、アルゴリズムは各イベントを処理していく。ただし、次のイベントが与えられる前に、現在のイベントに対する決定を下さなければならない。オンライン問題を解くアルゴリズムをオンラインアルゴリズムという。オンラインアルゴリズムの良さは、それが求める解と、入力を全て知ってから動作する（オフライン）アルゴリズムの解との近さの最悪値（競合比）で評価される。すなわち、アルゴリズム A が r -競合であるとは、任意の入力に対して A が求める解のコストと最適オフラインアルゴリズムのコストの比が r 倍以内であることを言う。オンラインアルゴリズムの研究も、近似アルゴリズムと同様に、上下限の両面からのアプローチがある。

1.1.2.3 小谷 大祐

大規模で複雑化し、かつ高機能化するコンピュータネットワークをシンプルに保ちつつ、持続的に発展させられる技術について研究を行っている。

Software Defined Networking ネットワークの管理者がソフトウェアによってパケットの転送制御を柔軟に変更できるネットワーク機器を用いて、ネットワークの集中制御や最適化、ネットワークへの迅速な新しい機能の導入や既存の機能の改良等を実現する Software Defined Networking という概念がある。特に、「ネットワークへの迅速な新しい機能の導入や既存の機能の改良」の部分に焦点を当て、この特徴を実現するための機構の開発や、アプリケーションと連携する機構の開発を行っている。

ネットワークセキュリティ ネットワークに接続されたコンピュータやそのコンピュータの中にある情報を外部からの攻撃から保護する技術の開発を行っている。特に、トラフィック分析により攻撃情報を抽出する技術の開発を行っている。

1.1.3 2016 年度の研究活動状況

1.1.3.1 岡部 寿男

インターネットの高信頼化・高機能化 IPv6 の新しいアドレスアーキテクチャの特徴を活かすことで、モビリティとセキュリティの両立や、冗長経路による高信頼化・負荷分散などを実現する研究を行っている。具体的には、小規模なサイトが複数の上流 ISP への接続を持つ IPv6 サイトマルチホーミング環境におけるアドレス割当てと経路制御、および必要な設定の自動化、TCP に代わる汎用の信頼性のあるトランスポート層プロトコルとして開発され、IETF で標準化が進められている SCTP (Stream Control Transport Protocol) におけるマルチホーム対応の改良などの課題に取り組んでいる。

マルチメディアストリームデータのリアルタイム伝送 高品位のマルチメディアストリームデータをインターネット上でリアルタイム伝送するための技術の研究を行っている。具体的には、SCTP を利用してバーストパケットロ

スのある環境で高品位映像を安定して伝送するためのツールを開発している。

インターネットにおけるプライバシー保護と不正防止 インターネット上に安全・安心な社会基盤を構築するためのプライバシー保護と不正防止の技術の研究を行っている。具体的には、無線 LAN ローミングや Web サービスなどにおけるシングルサインオン技術と認証連携技術、TTP (Trusted Third Party) を仮定しない配送内容証明可能な電子メールシステムなどである。

エネルギーの情報化 科学技術振興機構・京都地域研究成果展開事業 (スーパークラスプログラム)「クリーン・低環境負荷社会を実現する高効率エネルギー利用システムの構築」として、家庭、さらにはそれらが複数集まった地域等の面的エリア内で消費される電力に対して、情報通信技術 (ICT) を活用して生活者の利便性を失わず、かつ生活者が意識することなく、確実に消費電力の削減を達成できる技術確立するため、「電力の流れの情報化」及び「供給電力の最適割り当て」に基づく電力管理・制御技術を研究開発している。

1.1.3.2 宮崎 修一

安定マッチング問題における女性戦略可能性判定アルゴリズム 安定マッチング問題の入力では、同数 (n 人) の男女がおり、各人は異性に対する希望リストを持っている。出力として「安定性」という条件を満たすマッチング (n 組の男女ペア) を求める問題である。ここで言う安定性とは、ペアになっていない男女が新たにペアになることにより、双方が現状よりも改善されることが起こりえないということである。安定マッチングを求める Gale-Shapley アルゴリズムを使う場合、男性は嘘の希望リストを出すことにより得をしない (すなわち耐戦略性を持つ) が、女性は得する可能性がある。この際、指定された女性の最適戦略を多項式時間で求められるということは、以前から分かっていた。Gale-Shapley アルゴリズムは男性側に耐戦略性を持っているため、提出された男性の希望リストは真のリストであると考えてよいのに対し、女性は戦略操作が可能のため、女性の希望リストは必ずしも真の希望を反映しているとは限らない。本研究ではこのような背景を考慮して上述の問題を一般化し、女性の戦略可能性を判定する問題が $O(n^4)$ 時間で解けることを示した。本結果は国際会議 SWAT 2016 に採録され発表した。

オンラインフレーム転送量最大化問題における競合比の改良 k 個のバケットからなるフレーム転送量最大化問題 (k -FTM) と呼ばれる、ネットワーク上におけるスイッチのオンラインバッファ管理問題の一問題について考えた。本問題は、大きなフレームが k 個のバケットに分割されてインターネット上で転送され、受信者は k 個全てのバケットを受信できたときに限りフレームを再構成可能という状況をモデル化したものである。Kesselman らは本問題に対して、 $k = 2$ の場合でさえ任意のアルゴリズムの競合比は発散することを示した。そこで、入力に制限を加えた k -FTM (k -OFTM) を考え、任意のバッファの大きさ $B (\geq k)$ に対して、その競合比が高々 $\frac{2kB}{\lfloor B/k \rfloor} + k$ となるアルゴリズムを考案した。また、彼らは $2B \geq k$ かつ k が 2 の冪のとき、任意の決定性アルゴリズムの競合比の下限 $\frac{B}{\lfloor 2B/k \rfloor} = \Omega(k)$ を示した。本研究では、 k -OFTM に対する競合比の上限と下限を改良した。主要な結果として、Kesselman らの上界 $O(k^2)$ を $\frac{5B + \lfloor B/k \rfloor - 4}{\lfloor \lfloor B/k \rfloor / 2 \rfloor} = O(k)$ へ改良し、下界 $\Omega(k)$ に漸近的に一致させた。また、任意の $k \geq 2$ と任意の B に対する、決定性アルゴリズムの競合比の下限 $2k - 1$ と、任意の $k \geq 3$ と任意の B に対する、確率アルゴリズムの初めての非自明な競合比の下限 $k - 1$ を与えた。結果自体は既に得られており、国際会議 ISAAC 2013 にて発表していたが、本年度は論文にまとめ投稿し、査読付き論文誌 Theoretical Computer Science に採録された。

ホームネットワークトポロジー再構成のためのアルゴリズム 家庭内ネットワークの故障箇所特定などに応用するため、ネットワーク機器の通信ポートに蓄積された Mac アドレス情報からネットワークトポロジーを再構成する問題を取り扱った。トポロジー再構築の研究はこれまでも行われていたが、これらはインターネット上のネットワークを対象としており、ホームネットワーク特有のトポロジーには向いていないという欠点があった。本研究では、HTIP (Home Network Topology Identifying Protocol) というホームネットワークのためのプロトコルで蓄積される Mac アドレス情報を前提とし、再構築のアルゴリズムを開発した。また、本研究で開発したアルゴリズム及び上述した既存研究のアルゴリズムを実装し、ランダムに生成された木構造トポロジーに対して実行させ、その計算時間を計測した。その結果、我々の手法は既存手法では特定できなかったトポロジーを扱えるにも関わらず、実行速度は既存手法とはほぼ同程度であることが分かった。本結果は国際会議 CCNC 2017 に採録され発表した。

1.1.3.3 小谷 大祐

IoT 機器向けネットワークプラットフォーム NICT 委託研究「高齢者の活動的・健康的な生活を実現するための欧州との連携によるネットワークプラットフォーム基盤技術の研究開発」として、ロボットや様々なセンサーとクラウドを組み合わせて提供されるサービスを応用としたネットワーク制御技術の研究開発を行っている。この一環として、ロボットやセンサーがやりとりする通信の特性について、様々なロボットやセンサーの通信を調査することを通して、通信の特性をどのように記述し、制御に利用するかについて検討を行った。

トラフィック分析に向けたトラフィックデータの収集 トラフィックの分析技術の開発に向け、分析対象となるトラフィックの収集およびデータを保管するシステムを構築した。トラフィックの収集については、本研究分野で運用している公開サーバ宛てのものと、インターネット上の未使用の IP アドレス（ダークネット）宛てのものの2種類のトラフィックの収集を開始している。また、分析時に生データを扱うことによる事故を防ぐため、一部の機微なデータを削除する処理を行うソフトウェアを開発した。

1.1.4 研究業績

1.1.4.1 学術論文

- Jun Kawahara, Koji M. Kobayashi, and Shuichi Miyazaki, “Better Bounds for Online k -frame Throughput Maximization in Network Switches”, Theoretical Computer Science, Vol. 657, pp. 173-190, January, 2017.

1.1.4.2 国際会議（査読付き）

- Yoshiharu Tsuzaki, Yasuo Okabe, “Reactive Configuration Updating for Intent-Based Networking”, The 31st International Conference on Information Networking (ICOIN2017), Jan. 2017.
- Yoshiyuki Mihara, Shuichi Miyazaki, Yasuo Okabe, Tetsuya Yamaguchi, Okamoto Manabu, “Identifying Link Layer Home Network Topologies Using HTIP”, 14th Annual IEEE Consumer Communications & Networking Conference (CCNC2017), pp. 892-899, Jan. 2017.
- Sushmita Gupta, Kazuo Iwama, Shuichi Miyazaki, “Total Stability in Stable Matching Games”, Proc. the 15th Scandinavian Symposium and Workshops on Algorithm Theory, (SWAT 2016), pp. 23:1-23:12, June 2016.
- Hiroyuki Sato, Yasuo Okabe, Motonori Nakamura, “User Identification of Pseudonyms without Identity Information Exposure in Access Federations”, Proc. IEEE 40th Annual Computer Software and Applications Conference (COMPSAC2016), Vol. 1, pp.487-492, June 2016.
- Yasuo Okabe, Takaaki Komura, Hiroyuki Sato, Kazutsuna Yamaji, Motonori Nakamura, “An Authentication Federation Proxy Which Conceals Attributes and Authorization Policies Each Other”, Second IEEE International Workshop on Middleware for Cyber Security, Cloud Computing and Internetworking (MidCCI2016), in Proc. IEEE 40th Annual Computer Software and Applications Conference (COMPSAC2016), Vol. 2, pp.202-207, June 2016.
- Teruhisa Tajima, Yasuo Okabe, “Optimizing Packet Transmission Scheduling for Enhanced Web QoE in Wireless LAN”, The 4th IEEE International Workshop on Consumer Devices and Systems (CDS), in Proc. IEEE 40th Annual Computer Software and Applications Conference (COMPSAC2016), Vol. 2, pp.312-318, June 2016.

1.1.4.3 その他研究会等

- 小谷大祐, “アジャイル型共創による高齢者補助ロボット用ネットワークプラットフォーム技術の研究開発”, 第11回地域間インタークラウドワークショップ, 2017年3月.
- 岡部寿男, “オンデマンド型電力ネットワークと電力のパケット化”, 科学技術未来戦略ワークショップ「未来エネルギーネットワークと需要科学」, 2017年1月.
- 岡部寿男, “オンデマンド型電力ネットワークと電力のパケット化”, 第一回スマートエネルギーマネジメントシンポジウム～革新的電力マネジメントシステムの構築を目指して～, 2016年12月.
- Antonio Kung, Yasuo Okabe, “ACCRA: Agile CoCreation of Robots for Ageing”, Global Innovation Forum on Active and Healthy Ageing, Dec. 2016.
- 桑原貴明, 小谷大祐, 岡部寿男, “ソフトウェアルータにおける細粒度の帯域制御”, 信学技報, vol.116,

no.292, IA2016-60, pp.23-28, 2016 年 11 月.

- ・伊藤友浩, 小谷大祐, 岡部寿男, “属性情報を秘密分散した閾値型認証システムの設計”, 信学技報, vol.116, no.292, IA2016-57, pp.7-12, 2016 年 11 月.
- ・Yu Takabatake, Daisuke Kotani, Yasuo Okabe, “An anonymous distributed electronic voting system using Zerocoin”, IEICE Tech. Rep., vol.116, no. 282, IA2016-54, pp. 127-131, Nov. 2016.
- ・津崎善晴, 岡部寿男, “Intent-Based Networking におけるリアクティブな設定変更”, 信学技報, vol.116, no.247, IA2016-22, pp.1-6, 2016 年 10 月.
- ・岡部寿男, “京都大学における情報セキュリティ対策のこれまでとこれから”, 静岡大学個人情報保護及び情報セキュリティ対策講演会, 2016 年 10 月.
- ・松本和馬, 岡部寿男, “ユーザの結託による不正を防ぐ P2P 型 MMO ゲームの検討”, 電子情報通信学会 2016 年ソサイエティ大会 B-6-9, 2016 年 9 月.
- ・伊藤友浩, 岡部寿男, “属性情報を秘密分散した閾値型認証システムの検討”, 電子情報通信学会 2016 年ソサイエティ大会 B-16-1, 2016 年 9 月.
- ・岡部寿男, “電力のパケット化”, センサーネットワーク (U2A) 研究会, 2016 年 9 月.
- ・岡部寿男, “京都大学における情報セキュリティ対策”, 平成 28 年度島根大学個人情報保護・情報セキュリティ研修会, 2016 年 9 月.

1.1.5 研究助成金

- ・岡部寿男, 小谷大祐, 情報通信研究機構高度通信・放送研究開発委託研究, 高齢者の活動的・健康的な生活を実現するための欧州との連携によるネットワークプラットフォーム基盤技術の研究開発, アジャイル型共創による高齢者補助ロボット用ネットワークプラットフォーム技術の研究開発, 2016 年度: 4,500 千円, 2017 年度: 10,500 千円, 2018 年度: 10,500 千円, 2019 年度: 6,000 千円, 2016 年度～2019 年度.
- ・岡部寿男, 科学技術振興機構京都地域研究成果展開事業 (スーパークラスタープログラム), クリーン・低環境負荷社会を実現する高効率エネルギー利用システムの構築, 2013 年度: 3,520 千円, 2014 年度: 6,996 千円, 2015 年度: 5,000 千円, 2013 年度～2017 年度.
- ・岡部寿男, 日本学術振興会科学研究費補助金基盤研究 (B) 及び学術研究助成基金助成金, 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, 2014 年度: 2,600 千円, 2015 年度: 17,900 千円, 2016 年度: 2,600 千円, 2017 年度: 2,700 千円, 2018 年度: 2,500 千円, 2014 年度～2018 年度.
- ・宮崎修一, 日本学術振興会科学研究費補助金基盤研究 (C), 安定マッチングを利用した配属アルゴリズムの開発研究, 2016 年度: 1,000 千円, 2017 年度: 900 千円, 2018 年度: 900 千円, 2019 年度: 800 千円), 2016 年度～2019 年度.
- ・小谷大祐, 京都大学若手スタートアップ研究費, 2016 年度: 830 千円.

1.1.6 特許等取得状況

該当なし

1.1.7 博士学位論文

- ・美原義行, ホームネットワーク管理技術と応用サービスに関する研究, 岡部寿男

1.1.8 外国人来訪者

該当なし

1.1.9 業務支援の実績

1.1.9.1 岡部 寿男

全学情報セキュリティ委員会常置委員会委員として、全学の情報セキュリティ対策にかかわっている。また国立情報学研究所学術情報ネットワーク運営・連携本部委員、同セキュリティ作業部会委員として、国立情報学研究所や七大学等と共同で、学術情報ネットワークの構築・運用や大学の情報セキュリティの強化のための検討を行っている。

1.1.9.2 宮崎 修一

広報誌 Info! の編集委員として編集に携わった。

1.1.9.3 小谷 大祐

学術情報ネットワークシステムスイッチー式仕様策定委員会にオブザーバとして仕様の検討に携わっている。

1.1.10 対外活動（学会委員・役員，招待講演，受賞，非常勤講師，集中講義など）

1.1.10.1 学会委員・役員

- ・岡部寿男，電子情報通信学会，通信ソサイエティ執行委員会委員，2015年6月～2017年6月
- ・岡部寿男，電子情報通信学会，大会委員会委員，2015年6月～2017年6月
- ・岡部寿男，電子情報通信学会，通信ソサイエティ研専運営会議副議長，2015年6月～2017年6月
- ・岡部寿男，情報処理学会，論文誌 CDS トランザクション編集委員会編集委員長
- ・宮崎修一，電子情報通信学会，ソサイエティ論文誌編集委員会・査読委員
- ・宮崎修一，電子情報通信学会，情報・システムソサイエティ誌編集委員会・特任幹事，2014年6月～
- ・宮崎修一，情報処理学会関西支部，支部委員，2015年5月～2017年5月
- ・小谷大祐，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専門委員，2016年6月～2018年6月
- ・小谷大祐，情報処理学会，プログラミングシンポジウム委員会情報科学若手の会代表幹事，2016年4月～2017年9月
- ・小谷大祐，AsiaFI 2016 Summer School, CJK Workshop Co-Chair, 2016年6月

1.1.10.2 各種委員・役員

- ・岡部寿男，近畿情報通信協議会幹事，2016年5月～2017年4月
- ・岡部寿男，国立情報学研究所，学術情報ネットワーク運営・連携本部委員，2016年6月～2017年3月
- ・岡部寿男，国立情報学研究所，学術情報ネットワーク運営・連携本部セキュリティ作業部会・委員，2016年6月～2017年3月
- ・岡部寿男，国立情報学研究所，学術情報ネットワーク運営・連携本部高等教育機関における情報セキュリティポリシー推進部会・委員，2016年6月～2017年3月
- ・岡部寿男，国立情報学研究所，学術認証運営委員会委員および同委員会トラスト作業部会，2016年9月～2017年3月
- ・岡部寿男，九州大学大学院システム情報科学府博士後期課程学生アドバイザー委員，2015年7月～2018年3月
- ・岡部寿男，文部科学省，科学技術・学術審議会専門委員，2013年2月～2019年2月
- ・岡部寿男，JPCERT コーディネーションセンター，「平成27年度サイバーセキュリティ経済基盤構築事業（サイバー攻撃等国際連携対応調整事業）」事業評価委員会，2016年9月～2017年3月
- ・岡部寿男，日本学術振興会，学術システム研究センター主任研究員，2016年4月～2017年3月
- ・岡部寿男，公益財団法人国際科学技術財団，2017年（第33回）Japan Prize 審査委員会「エレクトロニクス，情報，通信」分野委員，2016年3月～2017年3月
- ・岡部寿男，公益財団法人国際科学技術財団，公益財団法人国際科学技術財団研究助成選考委員長，2016年12月～2017年4月
- ・岡部寿男，京都府教育委員会，京都府立京都すばる高等学校「スーパー・プロフェッショナル・ハイスクール」

運営指導委員，2016 年 7 月～2017 年 3 月

- ・岡部寿男，サイバー関西プロジェクト幹事

1.1.10.3 受賞

- ・岡部寿男，近畿総合通信局長賞，2016 年 6 月．

1.1.10.4 客員教員・非常勤講師

- ・岡部寿男，京都大学工学部，コンピュータネットワーク，2016 年 4 月～2016 年 9 月
- ・岡部寿男，京都府総合教育センター，平成 28 年度研修講座「校内ネットワーク基礎講座」，2016 年 10 月
- ・宮崎修一，京都大学工学部，グラフ理論，2016 年 10 月～2017 年 3 月

1.1.10.5 集中講義

該当なし

1.1.10.6 招待講演

該当なし

1.1.10.7 地域貢献

- ・宮崎修一，“コンピュータサイエンスの数学 ～アルゴリズム理論，安定結婚問題， $P \neq NP$ 予想～”，京都大学サマースクール 2016，2016 年 8 月 19 日．

1.1.10.8 その他

該当なし