

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, 計量理論
特定研究員 (産官学連携)	坂井 一美	エネルギーの情報化

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 (全ての入力が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出来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。

1.1.3 2014 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。また、大学間連携のための全国共同電子認証基盤構築事業（UPKI）をフィールドとして、開発した技術の応用も検討している。

エネルギーの情報化 NICT の委託研究「情報通信・エネルギー統合技術の研究開発」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を確立するため、「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

与えられたマッチングを安定とする希望リストの存在 安定マッチング問題において、学生の希望リスト及びマッチング M が与えられた際に、 M を安定とするような病院の希望リストが存在するか否かを判定する問題を取り扱った。この問題は、学生が不安定マッチングを提示され騙される危険性を、どこまで排除できるかという背景に基づく。病院の希望リストが任意の場合には必ず解が存在する。従って、病院の希望リストが k 種類しか存在しないという制約を加えた。これは、 k 種類の試験を実施し、そのいずれかの成績を病院が希望リストとして採用することに相当する。本研究では、 $k=1$ の場合には多項式時間で解けることを示した。また、 $k=2$ の場合および $k \geq 3$ で k -頂点彩色問題が NP 完全となる k の範囲において、問題が NP 完全となることを示した。さらに、 $k=2$ の場合に対して数種類の貪欲アルゴリズムを提案し、それらを実装し計算時間や誤り率の観点から計算機実験を行った。研究は概ね昨年度に行っていたが、本年度は追加実験を行い、それをまとめて論文誌に投稿し採録された。

オンライン安定マッチング問題のアドバイス複雑度 オンライン問題の複雑さは、その問題を解くオンラインアルゴリズムの競合比によって評価されるのが主流であるが、最近アドバイス複雑度による新たな解析手法が提案され、盛んに研究されている。これは、オンラインアルゴリズムが最適解を得るために必要とするアドバイスのビット数である。本研究では、オンライン二部マッチング問題と、オンライン安定マッチング問題に対するアドバイス複雑度の一致する上下限「 $\log_2(n!)$ 」を示した。ここで n は、前者の問題では二部グラフの片側の頂点数、後者の問題では男性の数である。

最小直径複数スタイナー木問題 ネットワーク設計において VLAN を構築する問題を、最小直径複数スタイナー木問題として定式化した。一般に、ネットワークのリンクには「遅延」と「容量」が定義できる。また、要求される VLAN には「要求帯域」がある。要求帯域を満たした上で最大遅延を最小化するのが本問題である。形式的には、各枝に「遅延」と「容量」のついたグラフ $G = (V, E)$ が与えられる。1 つの VLAN 要求は V の部分集合 V' と要求帯域の組として与えられ、VLAN の実現とは、 V' の頂点を含む G 上のスタイナー木 T であり、その最大遅延は T の直径で定義される。この問題では入力として複数の VLAN 要求が与えられ、全ての VLAN の実現を求めるものである。ただし、各枝について、その枝を使う VLAN の要求帯域の合計がその枝の容量を超えてはならない。この条件を満たした上で、各 VLAN の実現における最大遅延の総和を最小化するのが問題の目的である。本研究では、実行可能解を求めることすら NP 完全であることを示した。また、本問題に対するアルゴリズムを考案し、それを実装し計算機実験を行った。

1.1.4 研究業績

1.1.4.1 著書

該当なし

1.1.4.2 学術論文

- Hiroyuki Sato, Yasuo Okabe, Takeshi Nishimura, Kazutsuna Yamaji, Motonori Nakamura, "Privacy Enhancing Proxies in a Federation: Agent Approach and Cascade Approach," Journal of Information Processing, Vol. 22, No. 3 pp. 464-471, 2014-7.
- 松本亮介, 岡部寿男, "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," 情報処理学会論文誌, Vol. 55, No. 11, pp. 2451-2460, 2014-11.
- Shuichi Miyazaki, "On the advice complexity of online bipartite matching and online stable marriage," Information Processing Letters, Vol. 114, Issue 12, pp. 714-717, 2014-12.
- Minseon Lee, Shuichi Miyazaki, and Kazuo Iwama, "Finding Witnesses for Stability in the Hospitals/Residents Problem," Journal of Information Processing, Vol. 23, No. 2, pp. 202-209, 2015-2.

1.1.4.3 国際会議（査読付き）

- Masayuki Tsubouchi, Tomotaka Maeda, Yasuo Okabe, "Digital Fingerprinting on Executable File for Tracking Illegal Uploaders," 6th IEEE International Workshop on Computer Forensics in Software Engineering (CFSE2014), (Proc. IEEE

COMPSAC2014 Workshops), pp. 325-330, 2014-7.

- Daisuke Kotani, Yasuo Okabe, “A Packet-In Message Filtering Mechanism for Protection of Control Plane in OpenFlow Networks,” The 10th ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS2014), pp. 29-40, 2014-10.
- Yoshiharu Tsuzaki, Yasuo Okabe, Ray Atarashi, Tatsuya Hayashi, “Development of an Automatic Managing System of Wide-area Distributed Networks with Defined Network Specification,” 1st International Workshop on Management of SDN and NFV Systems (ManSDN/NFV 2014), 2014-11.

1.1.4.4 国内会議（査読付き）

該当なし

1.1.4.5 その他研究会等

- 宮崎修一, “近似アルゴリズムと安定マッチング”, 京都大学経済研究所ミクロ・ゲーム理論研究会, 2014-4.
- 小林浩二, 川原純, 宮崎修一, “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”, 信学技報, Vol. 114, No. 19, COMP2014-6 (電子情報通信学会コンピュータセッション研究会), pp. 37-44, 2014-4.
- 清水さや子, 戸田勝善, 岡部寿男, “統合 ID と属性を用いたグループの体系化”, マルチメディア, 分散, 協調とモバイル (DICOMO2014) シンポジウム, 3G-4, 2014-7.
- 片山健太郎, 菊池正史, 山田聖, 大塚隼人, 岡田耕司, 岡部寿男, 津崎善晴, 新麗, 林達也, “ネットワーク仕様定義による広域分散ネットワークの自動運用管理システムの開発”, 第6回新世代ネットワークシンポジウム, 2014-7.
- 畠山貴行, 宮崎修一, “マジックプロトコルを用いたP2P環境での公正なネットワークブラックジャック”, 平成26年度情報処理学会関西支部支部大会D-01, 2014-9.
- 山崎朋哉, 宮崎修一, “公開鍵暗号を用いたP2P型ネットワーク麻雀将棋”, 平成26年度情報処理学会関西支部支部大会D-02, 2014-9.
- 田島照久, 岡部寿男, “802.11 無線 LAN における複数端末の送信タイミング制御シミュレーション”, 平成26年度情報処理学会関西支部支部大会 E-12, 2014-9.
- 辻尾尚樹, 岡部寿男, “自治が可能なP2P型匿名Publish/Subscribe システム”, 信学技報, Vol. 114, No.335, IA2014-63, 2014-11.
- 田島照久, 岡部寿男, “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”, 信学技報, Vol. 114, No. 335, IA2014-65, 2014-11.
- 津崎善晴, 岡部寿男, 新麗, 林達也, 岡田耕司, 鈴木茂哉, 中村修, “LACCOONS: ネットワーク仕様定義による広域分散ネットワークの自動運用管理システム”, 第36回インターネット技術第163委員会 (ITRC) 研究会 CIS 分科会, 2014-11.
- Andrew Lee, 宮崎修一, 岡部寿男, “複数 VLAN 埋め込みのための貪欲アルゴリズムの評価”, 信学技報, vol. 114, no. 495, IA2014-105, pp. 143-147, 2015-3.
- Andrew Lee, 宮崎修一, 岡部寿男, “複数 VLAN 埋め込みのための最小直径複数スタイナー木問題”, 情報処理学会第77回全国大会, 4W-09, 2015-3.
- 辻尾尚樹, 岡部寿男, “発信者追跡可能かつ仮名型のP2P情報発信システム”, 情報処理学会第77回全国大会, 4X-02, 2015-3.
- 田島照久, 岡部寿男, “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”, 情報処理学会第77回全国大会, 3X-06, 2015-3 (学生奨励賞受賞).

1.1.5 研究助成金

- 岡部寿男, 受託研究 (総務省), ネットワーク仕様定義による広域分散ネットワークの自動運用管理システムの開発, 2,201 千円, 2014 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,

2013 年度～2017 年度.

- ・岡部寿男, 日本学術振興会科学研究補助金基盤研究 (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, 文部科学省科学研究補助金基盤研究 (C), 安定マッチング問題の合理的なモデル化とアルゴリズム開発, 4,000 千円 (2012 年度: 1,100 千円, 2013 年度: 1,000 千円, 2014 年度: 1,000 千円, 2015 年度: 900 千円), 2012 年度～2015 年度.

1.1.6 特許等取得状況

該当なし

1.1.7 博士学位論文

- ・森本尚之, Design and Analysis of Algorithms for Graph Exploration and Resource Allocation Problems and Their Application to Energy Management, 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

情報環境機構副機構長としてサービス全般を統括している. 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, 同認証作業部会主査として, 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・運用や大学電子認証基盤の共通仕様化・連携運用のための検討を行っている.

1.1.9.2 宮崎 修一

本年度は実質的な業務は行っていないが, 業務の情報環境機構への移行に伴い, これまで担当してきた講習会および広報誌に関する引継として, 関係する委員会に出席した.

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, 通信ソサイエティ和文マガジン編集委員, 2011 年 7 月～2015 年 5 月
- ・岡部寿男, 情報処理学会, 論文誌担当理事, 2012 年 6 月～2014 年 6 月
- ・岡部寿男, 情報処理学会, 全国大会実行委員長, 2014 年 4 月～2015 年 3 月
- ・宮崎修一, 電子情報通信学会, コンピューテーション研究会専門委員, 2008 年 5 月～2014 年 5 月
- ・宮崎修一, 電子情報通信学会, 情報・システム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・幹事, 2012 年 6 月～2014 年 6 月, 特任幹事, 2014 年 6 月～
- ・宮崎修一, 電子情報通信学会, 情報・システムソサイエティ運営委員, 2012 年 6 月～2014 年 6 月
- ・宮崎修一, 情報処理学会, 関西支部幹事, 2013 年 6 月～2015 年 6 月
- ・宮崎修一, 情報処理学会, 全国大会実行委員会幹事, 2014 年 4 月～2015 年 3 月
- ・宮崎修一, 3rd International Workshop on Matching Under Preferences (MACTH-UP 2015), Program Committee.

1.1.10.2 各種委員・役員

- ・岡部寿男, ITコンソーシアム京都・委員, 2014年7月～2016年3月
- ・岡部寿男, 京都府ITを活用した業務改革推進評価委員会委員, 2012年6月～2014年6月
- ・岡部寿男, 総務省, 戦略的情報通信研究開発推進制度評価委員, 2013年2月～2014年10月, 2015年2月～2016年10月
- ・岡部寿男, 近畿情報通信協議会・幹事, 2014年5月～2015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, 2014年4月～2015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・連携本部企画作業部会・委員, 2014年4月～2015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・連携本部認証作業部会・委員, 2014年4月～2015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, 2014年4月～2015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～2015年2月
- ・岡部寿男, 日本学術振興会産学協力研究委員会, 2014年4月～2015年3月
- ・岡部寿男, 京都府情報政策有識者会議委員, 2013年3月～2015年3月
- ・岡部寿男, 総務省, 情報通信技術の研究開発の評価に関する会合評価検討会構成員, 2014年1月～2014年12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2月

1.1.10.3 受賞

該当なし

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, 2014年4月～2014年9月
- ・宮崎修一, 京都大学工学部, グラフ理論, 2014年10月～2015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

該当なし

1.1.10.8 その他

該当なし