

地域・産学連携プロジェクト研究
〔研究論文〕

ネットワークの効果的な見える化に向かって
— 構造と利用状況の可視化 —

角田 裕¹⁾, 本間 舜²⁾, 渡邊 佑太²⁾, キニ グレン マンスフィールド³⁾

A study on effective visualization of intranets
— Network structure and usage status of network address space —

Hiroshi TSUNODA ¹⁾, Shun HONMA ²⁾, Yuta WATANABE ²⁾, Glenn Mansfield Keeni ³⁾

Abstract

Computer networks are an essential part of the infrastructure that supports our daily life. Network management is an important but difficult and often neglected task because of the complexity of the network. Security incidents like illegal accesses are increasing by the day. Effective visualization of various aspects of intranets will help network administrators to understand their networks better. In this paper, we describe our efforts towards visualizing the structure of a network and the usage status of network addresses.

1 はじめに

企業におけるネットワークの導入率は、総務省の調査 [1] によれば100～299人規模の企業では80%を上回り、2,000人以上の規模の企業でも90%強という高い水準を示している。さらに、調査に応じた全2,136社の総合的な結果でも70%を超えている。これに加えて、家庭でもスマートフォンやタブレットなどの携帯端末、家電製品の冷蔵庫やゲーム機などが続々とネットワークに参加するようになってきている。結果として、企業や家庭などのあらゆる組織においてイントラネットの拡大や複雑化の進行が予想される。

このような状況の中、ネットワーク管理者にとってはネットワークの構成や利用状況の把握が重要となっている。しかし、ネットワークの構成や利用状況は時間とともに変化する

1) 東北工業大学工学部情報通信工学科

Department of Information and Communication Engineering, Faculty of Engineering, Tohoku Institute of Technology

2) 東北工業大学工学部情報通信工学科 (平成29年3月卒業)

Department of Information and Communication Engineering, Faculty of Engineering, Tohoku Institute of Technology (Graduated in March 2017)

3) 株式会社サイバー・ソリューションズ

Cyber Solutions Inc.

るものであり、その変化に追従して把握し続けていくためには大きなコストを要する。特に専属のネットワーク管理者がいない小規模の組織では大きな課題である。

そこで、本研究ではネットワークの構成や利用状況をわかりやすく見える化するための要素技術の検討と開発を実施した。以下、2ではわかりやすいネットワーク地図の生成に関する検討について説明する。また、3では一覧性を重視したIPアドレスの使用状況可視化システムの検討について説明する。

2 わかりやすいネットワーク地図の生成に関する検討

2.1 ネットワーク地図生成の必要性と課題

本節では、ネットワークの物理構成や論理構成をわかりやすく図の形で見える化するネットワーク地図の生成について検討する。ネットワーク地図が整備されていれば、ネットワーク管理者はそれを参照することで物理的な構成と論理的な構成を把握し、障害やセキュリティインシデントの対応に活用することができる。

ネットワーク地図の生成手段は、手動生成と自動生成の二種類に大別できる。以下に例を交えてそれぞれの利点と欠点について説明する。

手動生成では、管理者が把握している機器の種別や機器間の接続関係に基づいて、専用のツールやMicrosoft PowerPointや同Visio、Adobe Illustratorなどの汎用のドローツールを用いて人間が地図を作成する。レイアウトやデザインの柔軟性を高くできるため、熟練した作成者であれば複雑な構成のネットワークをわかりやすく見える化できるが、作成作業に要する手間と時間コストが掛かるという課題がある。また、ネットワーク構成が変わる度に手動による地図の修正が必要になるため、最新のネットワーク地図を維持するための管理コストが大きい。小規模なネットワークであったり、地図作成に熟練し時間的余裕のある管理者がいたりするような環境でない限り、わかりやすい地図を最新の状態に維持することは難しい。

自動生成では、各機器の設定情報をリモートから収集し、収集結果を比較照合・分析することで構成を把握し、得られた結果を基に地図を作成する。近年ではこのような機能を有するネットワーク機器やソフトウェアが開発・販売されている。各機器のIPアドレスやアクセス情報など入力情報を基に自動で構成を探索して地図が生成されるため、管理者の負担は大幅に低減される。一方で、構成の探索にはベンダ独自の機能やプロトコルを使用するケースも多く、多様なベンダの機器が混在するネットワークへの適応が難しい。また、地図生成時に機器同士の接続関係を放射状に表現した地図しか生成できないなど、地図のレイアウトに制約が大きく、ネットワークの階層構造などを十分に表現できない場合がある。

本研究項目では、インターネット標準のネットワーク管理プロトコルSNMP (Simple Network Management Protocol) [2] を使用して、ネットワークを構成する各機器から情報を収集し、ネットワーク構成を把握する手法について検討した。また、共同で研究にあたった株式会社サイバー・ソリューションズによるネットワーク地図プログラムを改良し、わかりやすいネットワーク地図のあり方を検討した。

2.2 SNMPによるネットワーク機器からの情報と収集結果に基づくネットワーク構造の分析

SNMPは遠隔からネットワーク機器上の情報収集や設定、異常の通知を行うためのアプリケーション層のプロトコルであり、ネットワーク管理ステーション (Network Management Station: NMS) 上のマネージャとネットワーク機器上のエージェント間での通信手順を規定している。マネージャが機器上のエージェントに対して情報や設定変更を要求し、それに対しエージェントは要求された情報の通知や、設定した結果の通知を行う。また発生したエージェントからマネージャに対してイベントの通知を行う仕組みも備えている。

各エージェントは、図1に示すようなMIB (Management Information Base) と呼ばれるツリー構造の管理情報のデータベースを持っている。そして、マネージャからの要求に応じてMIB内の管理情報の参照や書き換えを行う。MIB内の管理情報はその用途毎にモジュール化されており、大きく標準MIBと拡張MIBと呼ばれる2つに分類される。標準MIBは、格納されている情報の内容がインターネット技術の標準化文書RFC (Request For Comments) によって標準として定義されているモジュール群である。拡張MIBは、各ベンダが自身の機器の管理のために独自に定義したモジュール群であり、当該ベンダの機器にのみ実装されているのが通常である。本研究では、マルチベンダ環境のネットワークを対象とした構造分析を行うため、多くの機器に広く実装されている標準MIBを活用する。

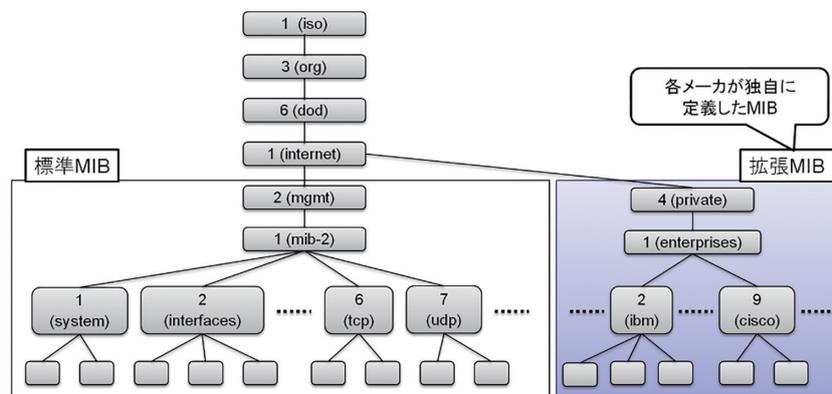


図1 MIBの構造

本研究ではネットワークの構成要素であるスイッチ上から標準MIBであるIF-MIB [3], BRIDGE-MIB [4] の情報を収集しネットワーク構造を分析した。IF-MIBはネットワーク機器のインターフェースに関する管理情報を格納したMIBモジュールであり、BRIDGE-MIBは機器が持つブリッジ機能 (2つのネットワークセグメント間を中継する機能) に関する管理情報を格納したMIBモジュールである。

表1に構造の分析に使用した各MIBの情報項目を示す。構造分析にはスイッチが持つFDB (Forwarding Data Base) の情報を用いる。FDBは、あるMACアドレス (LAN内の機器の識別に使用する物理アドレス) を宛先とするパケットを送出するポートを決定するために使用するデータベースであり、機器同士の接続関係が反映されている。

表1 構造分析に使用した管理情報項目

情報項目名	取得できる情報
IF-MIB::ifPhysAddress	インデックス番号に紐付けられた MAC アドレス
BRIDGE-MIB::dot1dBasePortIfIndex	機器の各ポートに紐付けられたインデックス番号
BRIDGE-MIB::dot1dTpFdbAddress	FDB に登録されている MAC アドレス
BRIDGE-MIB::dot1dTpFdbPort	FDB に登録されている各 MAC アドレスアドレスに紐付けられたポートの番号

2台の機器AとBが相互に接続されている最もシンプルな構造を例として、構造分析の手順を図2に示す。まず、NMSはAからifPhysAddressとdot1dBasePortIf Indexのリストを取得し、各ポートのインデックス番号とMACアドレスの対応関係を把握する。次にBからdot1dTpFdbAddressのリストを取得し、その中にAのいずれかのポートのMACアドレスが存在するか調査する。このとき、存在していなければAとBは接続されておらず、存在していれば接続されていると判断する。AとBが接続されていた場合には、さらにBからdot1dTpFdbPortのリストを取得し、その中からAのMACアドレスに紐付けられているポートを得る。この手順をネットワーク内の各機器に対して繰り返すことで、ある機器が別の機器との接続に使用しているポートが特定できるため構造分析が行える。

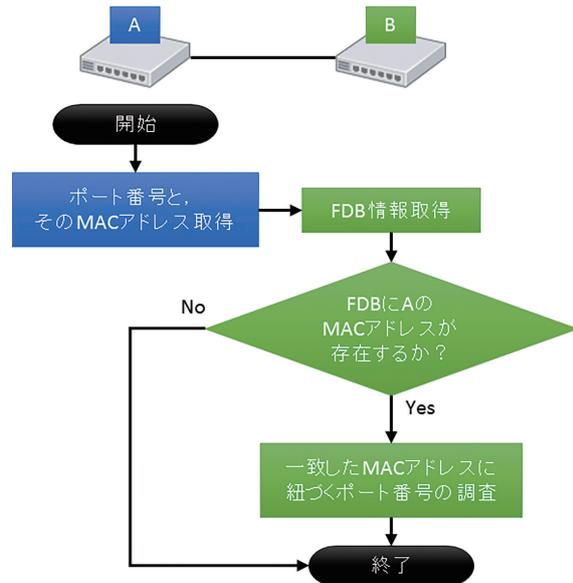
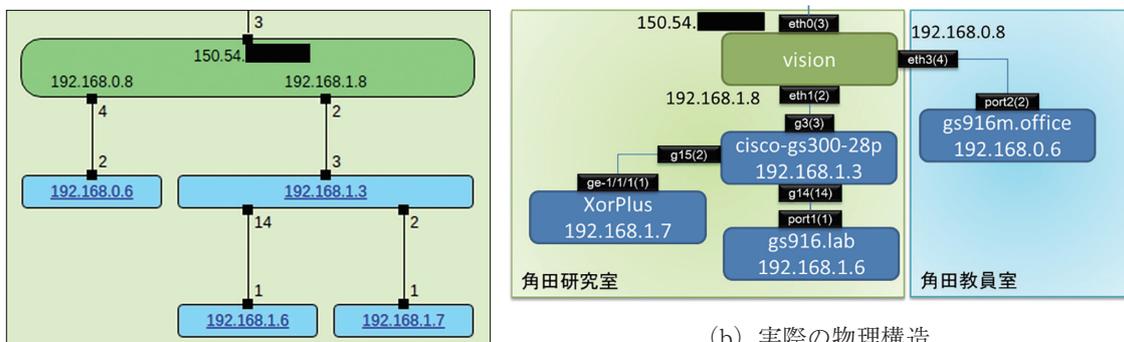


図2 構造分析の手順

本研究では、研究室内ネットワークを対象に前述の手順による構造分析の結果からネットワーク地図を生成し、生成された地図と実際の物理構造と比較して検証した。図3 (a) に生成したネットワーク地図、同 (b) に筆者らが手作業で確認した実際の物理構造を示す。いずれの図でも緑色の四角形がルータを表し、青色の四角形がスイッチを表している。



(a) 生成したネットワーク地図

(b) 実際の物理構造

図3 生成したネットワーク地図と実際の物理構造の比較検証

また四角形上にはその機器が持つ IP アドレスを、機器同士を接続する線はケーブルを表し、線の端点にはケーブルが接続している機器のポート番号を示している。

これらの図からわかるように、生成したネットワーク地図は物理構造を正しく反映しており、前述の手順で正しく構造を把握できていることを確認した。

2.3 わかりやすいネットワーク地図の生成における検討

従来有していた技術により生成したネットワーク地図について検討した結果、以下の問題を解決する必要があるという結論に至った。

- ① 非専門家にとっては、色のみによる機器種別は直感的ではなく判断が難しい。
- ② IP アドレス情報のみでは実機把握が難しい。
- ③ マウスオーバにより表れる詳細情報ウインドウが、マウスを動かすと消えてしまうため情報の閲覧が困難である。

そしてこれらの問題点の解消のため、以下の改良案を提案し実装した。

- ① 機器の違いを視覚的に把握できるようにアイコンと実機画像を追加する。
- ② SNMP によって機器から取得したホスト名を追加して、機器の把握を容易にする。
- ③ 詳細情報ウインドウの表示・非表示をクリックにより切り替え可能にする。

この改良により、非専門家にとってもよりわかりやすいネットワーク地図を生成することができるようになった。なお、本成果は文献 [5] として学会発表を行っている。

3 一覧性を重視した IP アドレスの使用状況可視化システムの検討

3.1 IP アドレス使用状況管理の必要性和課題

計画的な IP アドレスの配布や利用状況の管理は、イントラネットにおけるアドレスの衝突や枯渇を防ぐために重要である。管理を怠ってしまうと、新規接続ホストに割り当てべき IP アドレスの特定に時間がかかったり、使用中のアドレスを他のホストに誤って割り当ててしまったりするなどのトラブルにつながる。また、DHCP (Dynamic Host Configuration Protocol) によってアドレスの動的割り当てを行っている場合でも、アドレスプールの使用状況を把握していないと、気づかぬうちに IP アドレスが枯渇し、新規ユーザが利用できなくなってしまうなどの問題を引き起こす恐れがある。実際にとある企業において、DHCP サーバから IP アドレスを取得しているパソコンがネットワークにつながらなくなったという障害事例が報告されている [6]。この事例では、原因は複数の従業員が私物のスマートフォンを社内の無線 LAN に接続したことによるアドレスプールの枯渇が障害の原因であった。これらの問題を未然に防ぐためには、IP アドレスの使用状況・使用率を把握し、わかりやすく可視化して管理者に提示することが重要である。

すなわち、図 4 に示すように、管理者は管理下のネットワーク

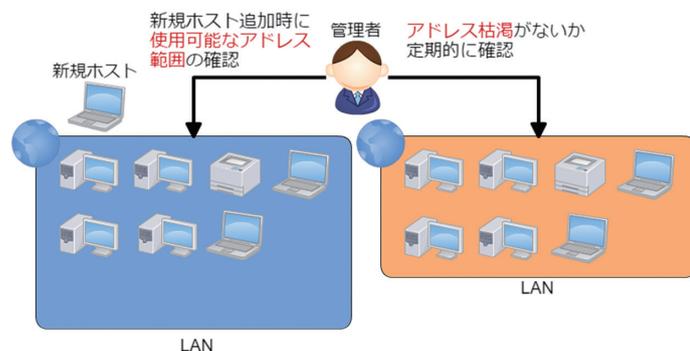


図 4 IP アドレスの利用状況管理の必要性

のIPアドレスの利用状況を常に把握し、新規ホスト追加時に使用可能なIPアドレスをすぐに特定できる状態にしておくことが望ましい。また、管理下のネットワークでIPアドレスの枯渇が迫っていないかを定期的に確認することも求められる。

従来、IPアドレスの利用状況の管理はExcelなどのスプレッドシートに記録し、それを手動で更新することによって行われてきた。しかし、手動管理では更新の手間が大きく更新漏れや入力ミスなどの人為的ミスが発生しやすい。また、表形式であるため視認性が低く、IPアドレスの使用状況・使用率が把握しづらい。そこで、アドレス使用状況の把握やその可視化を支援するIPAM (IP Address Management) [7] ツールも活用されている。しかし、筆者らの調査の結果、既存のIPAMに複数のネットワークにおける使用状況を一覧表示し、俯瞰できるものはなかった。そこで、本研究項目では一覧性を重視したIPアドレスの使用状況可視化システムの開発を進めた。

3.2 一覧性を重視したIPアドレスの使用状況可視化システム

まず、各ネットワークの①IPアドレスの使用割合、②未使用割合、③利用可能なアドレスレンジを一目で把握できるようにするために、図5に示すような帯状のグラフを考案し、IPアドレスの使用状況を可視化することにした。1つの帯状のグラフは、第1～第3オクテットまでが等しい256個 (x.y.z.0 ~ x.y.z.255) のIPアドレス群を表している。グラフを256等分にした左端が0、右端が255に相当する。

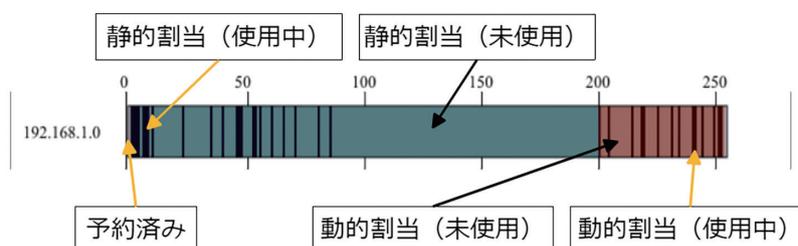


図5 開発したシステムによる1ネットワーク分の利用状況可視化結果

各アドレスは、手動で設定する静的割り当ての範囲、DHCPによる動的割り当ての範囲、予約済みの範囲のいずれかに属するとする。予約済みとは、ネットワークアドレスやブロードキャストアドレスのようなプロトコル上使用が許可されていないものや、管理ポリシー上使用不可とするものを指す。そして、アドレス種別および使用中・未使用の2状態を以下のように色分けして表す。

静的割当の範囲	使用中：濃青	動的割当の範囲	使用中：濃赤	予約済み：白
	未使用：薄青		未使用：薄赤	

この可視化方式の利点は、1つのアドレス群の表示に必要な領域が少ない点である。つまり、複数のネットワークのアドレス利用状況を効率的に表示できる。例えば、図6は6つのネットワークの利用状況を可視化した例である。このように、複数のネットワークの利用状況を一括して管理者に提示することができる。そのため、大規模ネットワークや、

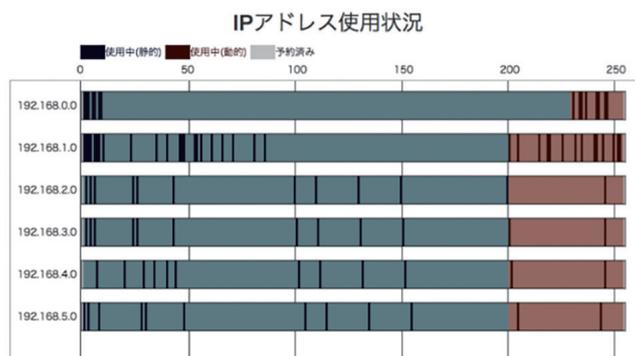


図6 複数のネットワークの利用状況の可視化例

多数の小規模ネットワークを管理する場合に本システムは有効に機能すると考えられる。

また、開発したシステムでは、可視化結果を閲覧端末の解像度に合わせて表示できるようにした。表示方法を変える端末の基準は画面サイズの横幅とし、横幅が1024px以上であればPCサイズで表示、768px以上1023px以下であればタブレットサイズで表示、320px以上767px以下であればスマートフォンサイズで表示するようになっている。タブレット端末やスマートフォンからの閲覧に対しては、端末の解像度に合わせて表示画面が変わるように実装し、実機を用いて正しく動作していることを確認した。閲覧確認を行った端末とブラウザの組み合わせの結果を表2に示す。また、表示結果の例を図7と図8に示す。図7はiPad Air 2からGoogle Chromeで閲覧した場合の表示結果である。図8はiPhone 5から同じくGoogle Chromeで閲覧したときの表示結果である。端末のサイズに応じて表示内容のレイアウトが調整されていることがわかる。なお、本成果は文献[8]として学会発表を行っている。

表2 表示の確認に使用した端末一覧

端末	OS	解像度 (横×縦)	画面 サイズ (インチ)	ブラウザ			
				safari	Google Chrome	Firefox	Edge
iPhone 5	iOS 10.2.1	320 × 568	4	○	○	○	
iPad Air 2	iOS 10.2.1	768 × 1024	9.7	○	○	○	
MacBook Air	OS X El Capitan	1440 × 900	13.3	○	○	○	
HP ProBook	Windows 10 Pro	1366 × 768	13.3		○	○	○
自作 PC	Lubuntu 15.10	1920 × 1080	24		○	○	

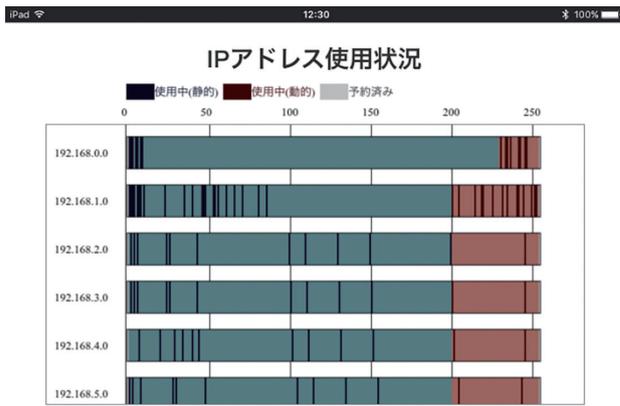


図7 タブレット端末での表示例

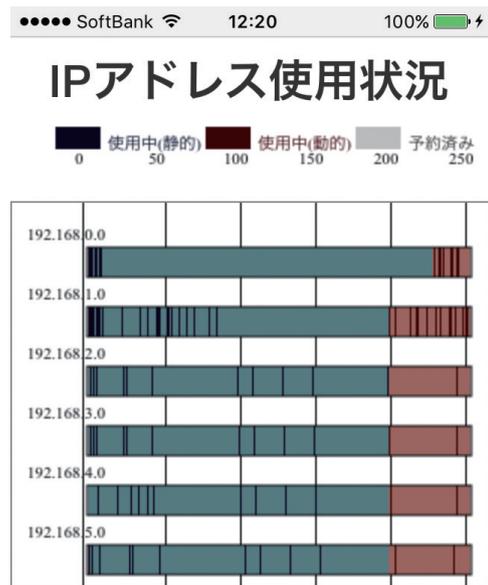


図8 スマートフォンでの表示例

今後はさらにわかりやすく有用な情報を提示するため、主に以下の点から改良を進める。

- ① 表示内容およびレイアウトのシンプル化
- ② 個別のIPアドレスに関する詳細情報の表示機能の追加
- ③ 接続管理情報など追加機能の検討

4 おわりに

本研究プロジェクトでは、各組織においてネットワークをわかりやすく見える化し、ネットワークの構造や現状を効果的に把握するための手段の提供を目的とした。組織における情報セキュリティの取り組みに不可欠な第一歩は、自身のネットワークの構造や現状を正確に把握することである。しかし、ネットワークの利用が広がる中でネットワークは複雑化と大規模化の一途を辿っており、一般のユーザはもちろんネットワーク管理者にとっても構造や現状を把握することは容易ではなくなっている。本研究ではこの現状を克服し、ネットワークをユーザと管理者の双方にとってわかりやすく可視化するために、以下の研究開発項目に取り組み、ネットワークの効果的な見える化を実現するシステムの実用化に資する知見を得ることができた。

- (1) わかりやすいネットワーク地図の生成における基礎検討
- (2) 一覧性を重視したIPアドレスの使用状況可視化システムの開発

謝辞

本研究は、東北工業大学地域連携センターの地域・産学連携プロジェクト研究費の援助により行われたものである。ここに記して謝意を表する。

参考文献

- [1] 総務省, "平成26年通信利用動向調査報告書(企業編)", http://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201400_002.pdf (参照日 2018/01/19)
- [2] D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", RFC3411, December 2002
- [3] K. Mcloghrie, F. Kastenholz, "The Interfaces Group MIB", RFC2863, June 2000
- [4] K. Norseth, E. Bell, "Definitions of Managed Objects for Bridges", RFC4188, September 2005
- [5] 本間 舜, 角田 裕, キニ グレン マンスフィールド, "わかりやすいネットワーク地図の生成に関する検討", 平成29年東北地区若手研究者研究発表会 YS29-P-1-16
- [6] 大森 敏行, "当事者が語る!トラブルからの脱出 IPアドレスが割り当てられない~私物スマホが使い果たす~", 日経NETWORK3月号 第203号 日経BP社 pp.68-73
- [7] Understanding Internet Protocol Address Management (IPAM), <https://www.getfilecloud.com/blog/2013/12/internet-protocol-address-management-ipam-explained/> (参照日 2018/01/19)
- [8] 渡邊 佑太, 角田 裕, キニ グレン マンスフィールド, "一覧性を重視したIPアドレスの使用状況可視化システムの開発", 平成29年東北地区若手研究者研究発表会 YS29-1-3-5