

VLAN情報を含めたネットワークトポロジの表現形式の提案および描画システムの構築

水品 亜久里* 川橋 裕†

1 はじめに

一般的に運用されているネットワークでは、ネットワークの遮断が発生することがある。管理者は、障害が報告された地点から原因となっているネットワーク機器まで、ネットワーク図を用いて調べる必要がある。これは時間がかかり、管理者にとって大きな負担となる。SNMP(Simple Network Management Protocol)の機能の一つである、SNMPトラップを利用することで、ネットワーク機器間の隣接状態の変化を検知でき、この問題を解決することができる。しかし、SNMPトラップはUDP(User Datagram Protocol)の通信であるため、通知を受け取れない可能性がある。そのため、SNMPトラップのみに依存する障害検知では信頼性が高いとはいえない。

そこで、「Link Layer Discovery Protocol と Cisco Discovery Protocol を利用したネットワークトポロジーの探索と描画による障害検知システムの構築」¹⁾という先行研究が行われた。検知可能なネットワーク機器の対象範囲を広げるために、ベンダに依存しない検知が可能なLLDP²⁾を用い、LLDPが未対応の古いネットワーク機器向けにCisco社製品の検知が可能なCDP³⁾を用いた。LLDPとCDPという2つのデータリンク層のプロトコルを併用することで、検知可能なネットワーク機器の対象範囲を広げている。探索で検知したネットワーク機器からネットワークトポロジーを描画するシステムによって、SNMPトラップと比較して、時間ごとにおけるネットワーク機器の隣接情報の変化を比較的容易に確認することを可能にした。

本研究では、VLAN(Virtual Local Area Network)情報を含めたネットワークトポロジーの表現形式の提案を行い、その表現形式に従ってネットワークトポロジーを描画するシステムの構築を目的とする。ネットワーク機器間の隣接情報と設定されているVLANの情報は、レイヤ2のネットワークにおいて重要な要素である。しかし、両者を含めてネットワークトポロジーを描画しようとする

と、複雑化や視認性の悪化といった問題が発生する。そのため、先行研究をはじめとする既存のシステムでは、隣接情報とVLAN情報を併せて描画することが実現できていない。この問題を解決し、より容易かつ正確なレイヤ2のネットワークトポロジーの把握を可能にする方法の一つとして、本システムを提案する。

なお、本論文で頻出する、「ポート」という単語の意味について、LANケーブルなどを接続するために、ネットワーク機器に存在する物理的なポート(差し込み口)のことであると定義する。

2 先行研究

本章では、先行研究である、「Link Layer Discovery Protocol と Cisco Discovery Protocol を利用したネットワークトポロジーの探索と描画による障害検知システムの構築」¹⁾について、その概要を述べ、システムの問題点を提示する。

2.1 概要

先行研究は、SNMPトラップの受動的な検知に依存せず、能動的にネットワークトポロジーを探索して描画するシステムを構築したものである。探索の始点となるネットワーク機器のIPアドレスを与えることで、一定時間ごとにネットワークトポロジーのクロール⁴⁾を行い、ネットワーク機器間の隣接情報をグラフとして表示する。探索において、IEEE802.1ABで指定されているLLDPを利用することによって、各ベンダ間に存在するネットワーク機器の差を軽減し、ベンダが異なってもLLDPの設定がされていれば情報の取得ができる。しかし、ネットワーク機器が古い場合、LLDPに対応していないことがあるため、Cisco社が提供するCDPも利用している。LLDPとCDPを併用して探索することで、より多くの種類のネットワーク機器を対象に、隣接情報の取得を可能にしている。管理者は、時間ごとにおけるネットワーク機器の隣接情報の変化を比較的容易に確認することができる。障害が発生したネットワーク機器の検知を行うことができる。

2.2 問題点

ネットワークトポロジーのクロールにおいて、LLDPとCDPを併用して探索しているため、より多くの種類の

* 和歌山大学大学院 システム工学研究科 川橋研究室

† 和歌山大学 学術情報センター

ネットワーク機器から隣接情報を取得することができている。しかし、レイヤ2のネットワークで重要な要素である VLAN 情報を取得できていない。隣接するネットワーク機器のポートに適用されている VLAN 情報を知ることができれば、より正確なネットワークトポロジの把握が可能になり、障害発生時の影響範囲の推定が容易になると考えられる。

3 関連研究

3.1 FDB を用いたネットワークトポロジの推測

関連研究として、FDB(Forwarding Data Base) を用いてネットワークトポロジを推測し、表示するシステムが存在する⁵⁾⁶⁾⁷⁾。FDB とは、宛先 MAC アドレスと送出ポートと VLAN の組み合わせを管理するデータベースのことである。FDB を用いることで、隣接するネットワーク機器の MAC アドレスとそこに割り当てられた VLAN 情報を取得することができる。これらの FDB によって取得した情報を利用して、ネットワークトポロジの推測を行う。以前までの、対象となる全てのネットワーク機器の接続関係が判明してから、物理的な接続を推測するアルゴリズム⁸⁾ではなく、必ずしも全ての情報を取得する必要がないアルゴリズムに従っている。そのため、推測結果はほぼ安定した結果が得られている。しかしながら、問題点として、FDB から情報を取得しようとしたときにスパンニングツリーが設定されていると、待機状態のネットワーク機器を発見できないという問題点がある。加えて、ネットワークトポロジの推測において取得した VLAN 情報を利用せずに破棄しているため、ネットワークトポロジの表示で VLAN 情報の表示が行われていない。

3.2 HTIP に基づくホームネットワークトポロジの検出システム

関連研究として、「ホームネットワークにおける HTIP に基づくネットワークトポロジ検出システム」がある⁹⁾。情報家電やモバイル端末などが一般家庭に普及し、ホームネットワークのトポロジが複雑化している。ホームネットワークの運営や管理を円滑に行うために、ホームネットワークのトポロジを検出することができる HTIP(Home-network Topology Identifying Protocol) が用いられている。HTIP は、LLDP の機能を利用して各ネットワーク機器から TV や PC などの区分、型番、メーカーコードなどからなる機器情報を取得する。同様に、ネットワーク機器の宛先 MAC アドレスと送出ポートからなる接続構成情報も取得する。これらの情報から Web インタフェース上にホームネットワークのトポロジを描画している。

4 提案手法

本章では、本研究の目的を達成するために用いた手法について述べる。

4.1 ネットワークトポロジのクロール

本研究で利用したネットワークトポロジのクロールのアルゴリズムは、以下に示す内容である。先行研究と同様、始点となるネットワーク機器を指定してクロールを行うアルゴリズムとなっているが、先行研究では取得した LLDP と CDP の情報からポート情報を切り捨ててしまっていた。ポート情報は、LLDP と CDP で取得した隣接情報と 4.3 節で取得する VLAN・トランク情報を結び付けるために必要であるため、本研究では切り捨てずに保存している。

1. 始点となるネットワーク機器から、LLDP か CDP の情報を取得する。
2. 隣接するネットワーク機器のマネジメントアドレスをスタックにプッシュする。
3. スタックに積まれたマネジメントアドレスを 1 つ取得する。マネジメントアドレスを取得できない場合、クロールを終了する。
4. 既に情報を取得したマネジメントアドレスである場合、手順 3 に戻る。
5. 手順 3 で取得したマネジメントアドレスから、LLDP か CDP の情報を取得する。LLDP か CDP の情報を取得できない場合、手順 3 に戻る。
6. 手順 5 で取得した情報からマネジメントアドレスを取得してスタックにプッシュする。その後、手順 3 に戻る。

4.2 収集された情報の整形

前節のアルゴリズムによって取得できた LLDP の情報から、マネジメントアドレスとホスト名の対応データ、あるネットワーク機器の隣接情報をマネジメントアドレスで表した隣接データ、あるネットワーク機器の隣接情報をそのネットワーク機器のマネジメントアドレスとポート番号で表した隣接データを作成する。この3つのデータは、取得できた CDP の情報からも同様の形式で作成される。

ネットワークトポロジのグラフ描画に向けて、取得した LLDP と CDP の情報から作成したデータで、別々になっている同じ種類のデータ同士をそれぞれ 1 つに合成する。その組み合わせを図 1 に示す。

データ合成の際、対応が完全一致した場合のみ重複の削除を行い、部分一致の場合は両者の和集合になるようにして合成する。

4.3 VLAN・トランク情報の取得

前節の整形によって作成された、マネジメントアドレスとホスト名の対応データ内のマネジメントアドレ

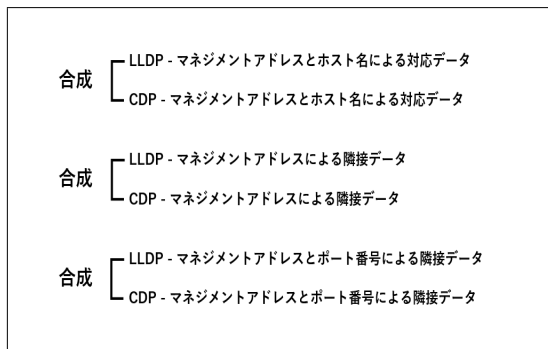


図1 合成するデータの組み合わせ

```
{
  "nodes":[
    {"id":0,"name":"C3560-TEST-A"},
    {"id":1,"name":"C3560-TEST-B"},
    {"id":2,"name":"C3560-TEST-C"}
  ],
  "links":[
    {"source":0,"target":1,"name":"706"},
    {"source":0,"target":2,"name":"806"}
  ]
}
```

図2 正規化されたデータ

表1 4つのネットワーク機器間のVLAN接続内容

区間	VLAN 番号	備考
X と A	100,200	トランク接続
A と B	100	
B と C	100,200	トランク接続
C と A	200	

スを参照し、その管理アドレスを持つネットワーク機器からVLAN情報とトランク情報を取得する。VLAN情報のみの取得では、トランク接続になっているVLANのポート番号がわからず、VLAN情報を含めたトポロジの正確な描画ができないという問題が発生する。そのため、VLAN情報だけでなくトランク情報も含めた、2種類の情報を取得する必要がある。このとき、管理アドレスに対応するホスト名を用いて、そのネットワーク機器のVLAN情報とトランク情報が既に取得済みか確認しているため、同一のネットワーク機器から複数回も情報を取得することはない。

4.4 グラフ描画のための正規化

ネットワークトポロジをグラフ描画するためには、整形された3つのデータとVLAN情報のデータ、トランク情報のデータをポート情報を基に組み合わせ、正規化する必要がある。そのため、以下に示す手順に従って正規化を行う。この手順によって正規化されたデータを図2に示す。

1. 整形された対応データからホスト名を重複なく全て取得し、順にIDを割り振る。
2. 取得したホスト名のネットワーク機器の隣接情報を、整形された2つの隣接データから取得する。
3. ネットワーク機器同士の接続を、手順1で割り振ったIDを利用して、「source(接続元)」と「target(接続先)」で表現する。
4. 隣接データとVLAN情報のデータ間におけるポート番号の対応を調べ、手順3の接続名として、VLAN情報から得たVLAN番号を付ける。
5. 手順4でポート番号の対応が確認できなかった場合はトランク接続と判断し、隣接データとトランク情報のデータを参照して、手順3の接続名を付ける。

4.5 VLAN情報を含めたネットワークトポロジの描画

本節では、レイヤ2のネットワーク図とVLANの関係性の問題について説明したあと、その問題を解決する

ために本研究で用いた、VLAN情報を含めたネットワークトポロジの表現方式について述べる。

4.5.1 レイヤ2ネットワーク図とVLANの関係

X, A, B, Cの合計4台のネットワーク機器からなるネットワークトポロジを考える。それぞれのネットワーク機器は、表1に示すVLANの内容で接続されている。ここで、表1の内容を、ネットワーク機器の隣接情報を重視してネットワークトポロジを描画すると、図3のように表せる。反対に、VLAN情報を重視してネットワークトポロジを描画すると、図4のように表せる。どちらも、表1という同じ情報から描画したものであるにも関わらず、表現の形式に大きな差が生まれている。隣接情報とVLAN情報はレイヤ2のネットワークにおいてどちらも重要な要素であるが、一方を重視してネットワークトポロジを描画すると、他方の情報が読み取りにくくなるといったトレードオフの関係がある。

4.5.2 提案する表現形式

隣接情報とVLAN情報には、一方を重視してネットワークトポロジを描画すると、他方の情報が読み取りにくくなるといったトレードオフの関係がある。この問題を解決するために、以下の項目を満たす、VLAN情報を含めたネットワークトポロジの表現方式を提案する。

- 隣接情報を重視するが、VLAN情報も読み取りやすい。
- ネットワーク機器のホスト名と隣接情報が把握できる。
- ネットワーク機器同士の隣接関係にVLAN番号を付ける。

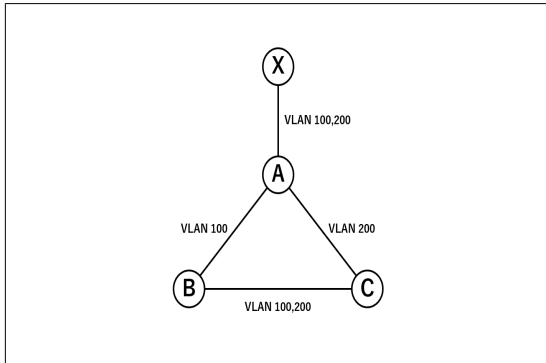


図3 隣接情報を重視したネットワークトポロジ

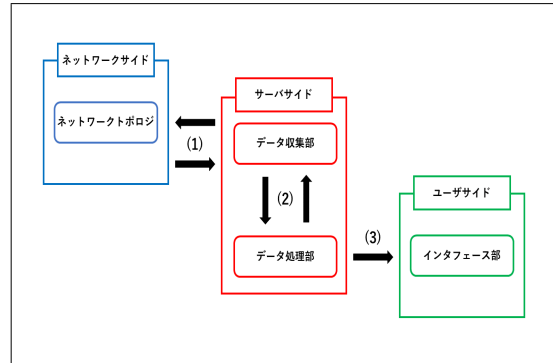


図5 システム構成と処理手順

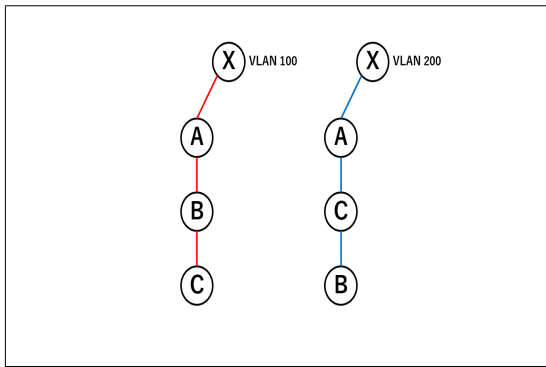


図4 VLAN情報を重視したネットワークトポロジ

- VLANごとに異なる色を用いて描画する。
- トランク接続されているVLANを1つにまとめて描画するのではなく、全て別々にして描画する。

5 提案システム

本章では、必要な動作環境と実装した提案システムの構成について説明する。

5.1 ネットワーク環境

提案システムを実装するために、各ネットワーク機器にLLDPまたはCDPの設定、接続可能なマネジメントアドレスとホスト名の設定がされている必要がある。

5.2 システム構成

提案システムのシステム構成と処理手順を図5に示す。本システムはネットワークサイド、サーバサイド、ユーザサイドの3つから構成されている。

- (1) LLDP・CDP・VLAN・トランク情報の取得
- (2) 収集された情報の伝達
- (3) ネットワークトポロジの描画

図5について、提案システムがネットワークサイドから情報を収集し、VLAN情報を含めたネットワークトポ

ロジの描画をするまでの処理の流れは以上のようになっている。

5.2.1 データ収集部

データ収集部では、指定されたネットワーク機器を始点としてネットワークトポロジのクロールを行う。その後、データ処理部で合成されたマネジメントアドレスとホスト名の対応データを取得し、そのデータ内のマネジメントアドレスを持つネットワーク機器からVLAN情報とトランク情報を取得する。ネットワークトポロジのクロールとVLAN・トランク情報の取得は、同一のネットワーク機器から複数回行われることはなく、cron¹⁰⁾を用いることで定期的に行われる。

5.2.2 データ処理部

データ処理部では、データ収集部で収集されたデータの整形と正規化を行う。ネットワークトポロジのクロールによって得られたLLDPとCDPの情報は別々のデータになっているため、同じ種類のデータ同士を合成し、重複せず不足が起こらないように整形する。そして、ネットワークトポロジのグラフ描画のために、整形された3つのデータとVLAN情報のデータ、トランク情報のデータの合計5つのデータを、ポート情報を基に組み合わせることで正規化する。なお、このとき正規化されたデータはJSON形式で出力される。

5.2.3 インタフェース部

インタフェース部は、JavaScriptによって実装されている。正規化されたデータから、VLAN情報を含めたネットワークトポロジのグラフ描画を行う。グラフ描画は、4章で述べた表現方式に従っている。Webインタフェース上で、始点となるネットワーク機器からのネットワークトポロジを確認できるだけでなく、それぞれの隣接におけるVLAN情報も確認することができる。

6 実験

本章では、本システムの動作を検証するために行った実験の概要とその結果について述べる。

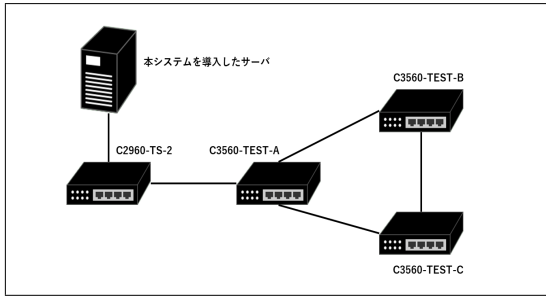


図6 実験用ネットワーク構成

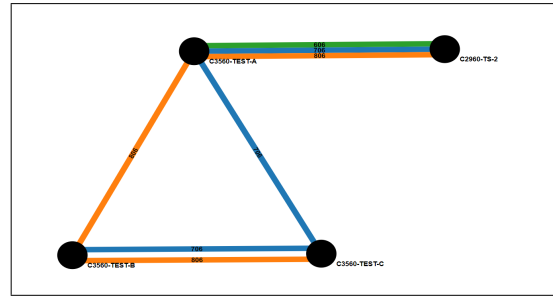


図7 停電前に取得したネットワークポロジ

表2 実験用のネットワーク機器間の VLAN 接続内容

区間	VLAN 番号	備考
C2960-TS-2 と TEST-A	606,706,806	トランク接続
TEST-A と TEST-B	806	
TEST-B と TEST-C	706,806	トランク接続
TEST-C と TEST-A	706	

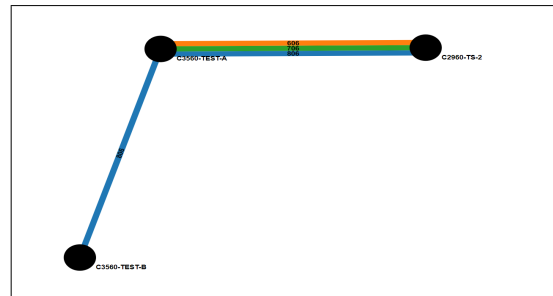


図8 電源復旧後に取得したネットワークポロジ

6.1 実験手法

本実験は、図6と表2に示す、実験用の簡単なネットワークを構築して行った。実験では、停電時を想定して一時的に全てのネットワーク機器の電源を落とした。その際、C3560-TEST-Cとの接続を全て切断し、ネットワークポロジを変化させた。これによって、電源が復旧しても一部のネットワーク機器が通信できない状態にした。その後、本システムでネットワークポロジの変化を検出できるかを検証した。

6.2 実験結果

実験で取得したデータを基に、インタフェース上に描画したネットワークポロジをそれぞれ図7と図8に示す。図7では、ネットワーク機器の電源を落とす前のネットワーク情報を取得して、描画ができていた。それだけでなく、4章で述べた「隣接情報を重視するがVLAN情報も読み取りやすい」、「ネットワーク機器のホスト名と隣接情報が把握できる」などの表現方式に従って描いている。さらに、図8では、C3560-TEST-Cとの接続がない、電源復旧後に変化したネットワークポロジを検出できている。

7 考察

本章では、本研究で実装したシステムの評価と今後の課題について述べる。前章の実験から、本システムの課題として、インタフェース部におけるポート情報の表示問題、ネットワークポロジの変化による同一名のVLANの配色問題、大規模なネットワークにおける動作問題の3つが挙げられる。

7.1 評価

4.5.1項で述べたように、レイヤ2のネットワークにおいて隣接情報とVLAN情報はどちらも重要な要素であるが、一方を重視してネットワークポロジを描画すると、他方の情報が読み取りにくくなるというトレードオフの関係がある。この問題を解決するために、本研究で提案したVLAN情報を含めたネットワークポロジの表現方式は、図7に示した通りである。先行研究と同様に隣接情報を重視したネットワークポロジを基準とし、ネットワーク機器同士の隣接関係に新しくVLAN番号付けとVLANの色分けを行うことで、隣接情報だけでなくVLAN情報も同程度に把握できるようにした。これによって、先行研究のネットワークポロジや図3などの従来の表現方法と比較して、より詳細なネットワークポロジが直感的に理解しやすい描画の実現ができたといえる。

7.2 今後の課題

本システムでは、VLAN情報を含めたネットワークポロジの描画に向けて、隣接情報とVLAN情報という別々のデータを関連付けるためにポート情報を収集しているが、インタフェース部の描画においてポート情報の表示ができていない。2.2節の先行研究の問題点でも述べたように、実際の障害対応では、ネットワーク機器のどのポートに原因があるかといった内容を調べる必要がある。そこで例えば、Webインタフェース上でネットワーク機器のノードをクリックすると、その機器に割り

当てられている VLAN が何番のポートなのかわかるような表示をすることで、管理者が実際に障害対応を行うときの作業量を削減できると考える。

ネットワーク機器の電源を落とす前後の図 7 と図 8 のネットワークトポロジにおいて、同一名の VLAN が別々の色で描画されている。ネットワークトポロジの変化の前後で同一名の VLAN の配色が変わってしまうと、本来は問題なく接続している VLAN の接続がなくなり、本当に接続がなくなった VLAN を問題なく接続していると誤認識する可能性がある。

前章の実験で、本システムは実験用に構築した簡単なネットワークトポロジにおいて、意図した通りに動作することが確認できた。しかし、より大規模なネットワークを想定し、ネットワークを再構築して本システムを動作させたところ、ネットワーク機器間に割り当てられている VLAN の数が一定数を超えると、トポロジ描画のプログラム内容の関係で、その間のトポロジが描画できないという問題を確認した。ネットワーク機器のノードの大きさを一定で描画するという現在の方法から、ネットワーク機器間に割り当てられている VLAN の数に応じて動的にノードの大きさを決定して描画するという方法に変更することで、この問題を解決できると考える。

8 おわりに

本論文では、VLAN 情報を含めたネットワークトポロジの表現方式の提案を行い、その表現方式に従ってネットワークトポロジを描画するシステムについて述べた。ネットワーク機器間の隣接情報と設定されている VLAN の情報は、レイヤ 2 のネットワークにおいて重要な要素である。隣接情報について、2 章と 3 章で説明した先行研究や関連研究でグラフ描画することはできていたが、VLAN 情報と併せて描画することは実現できていなかった。さらに、隣接情報と VLAN 情報の両者を含めて描画しようとする、複雑化や視認性の悪化といった問題が発生した。

そこで、本研究では、「隣接情報を重視するが、VLAN 情報も読み取りやすい」といった 4.5.2 項で述べた表現形式を定め、その表現形式に従ってネットワークトポロジを描画できるように、先行研究のシステムを基にシステムの構築を行った。LLDP と CDP で隣接情報を取得するだけでなく、隣接情報を利用して新たに VLAN 情報も取得し、別々となっているこれらの情報を結び付けるためにポート情報を利用することで、インタフェース部で描画するための準備を整えた。本システムの動作実験において、従来の表現方法と比較して、より詳細なネットワークトポロジが直感的に理解しやすい描画の実現を確認することができた。

しかし、インタフェース部におけるポート情報の表示問題やネットワークトポロジの変化による同一名の

VLAN の配色問題などの改善点が本システムにあることもわかった。今後は、実環境への導入も踏まえ、動作実験と問題点の解決によるシステムの改良を重ね、より大規模かつ複雑なネットワークへの適応と実用的なシステムの構築を目指していきたい。

参考文献

- [1] Link Layer Discovery Protocol と Cisco Discovery Protocol を利用したネットワークトポロジーの探索と描画による障害検知システムの構築：堀内亮汰，和歌山大学システム工学部システム工学科，2019.
- [2] 802.1AB - Station and Media Access Control Connectivity Discovery：
<http://www.ieee802.org/1/pages/802.1ab.html> (January 2023).
- [3] Cisco Discovery Protocol Version 2：
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html> (January 2023).
- [4] クロール/クローリングとは - DIGITOR, IT・Web・マーケティング用語辞典，2019/12/22：
<https://digitor.jp/dictionary/crawl/> (February 2023).
- [5] ループを考慮した Layer2 ネットワーク構成情報の推測アルゴリズムについて：分散システム/インターネット運用技術シンポジウム，2006，論文集 pp.7-12.
- [6] ネットワークトポロジの発見とその表示について：吉田和幸，大分大学総合情報センター，2007
<https://csis.ufinity.jp/wysiwyg/file/download/8/285> (February 2023).
- [7] Layer2 ネットワーク構成情報推測・表示システムのための構成情報の収集～構成情報のベンダ依存性について～：藤田俊輔，吉田和幸，大分大学工学部，情報処理学会，2008.
- [8] Topology Discovery in Heterogeneous IP Networks：Yuri Breitbart, Minos Garofalakis, Ben Jai, Cliff Martin, Rajeev Rastogi, Avi Silberschatz, IEEE/ACM Transaction on Networking Vol.12, 2004.
- [9] ホームネットワークのトポロジ検出と障害検知を実現する HTIP の実装とその活用：岡田崇，Sioutis Marios，牧野義樹，丹康雄，北陸先端科学技術大学院大学，情報処理学会，2018.
- [10] cron - Linux 技術者認定 LinuC, LPI-Japan：
<https://linuc.org/study/knowledge/368/> (February 2023).