情報処理学会論文誌 Vol.59 No.3 1026–1037 (Mar. 2018)

小型コンピュータと画像処理技術を活用したネットワーク機器監視手法の提案と実装

小川 康一[1,2] 吉浦 紀晃[1,2,a)]

受付日 2017年6月26日, 採録日 2017年12月8日

概要：大学では，利用者が自身の裁量で多種多様なネットワーク機器を導入し利用している．利用者が使用するネットワーク機器は，SNMP などの監視プロトコルを利用できない場合が多く，また，利用できたとしても，多種多様なため，大学のネットワーク管理者が利用者のネットワーク環境の状態を把握することは困難である．しかし，利用者が引き起こすネットワーク障害の対応は，大学のネットワーク管理者が，利用者のもとへ出向いて，障害対応しなければならないため，大きな負担となっている．そこで本論文では，ネットワーク管理者の目の代わりとなるカメラを用いてネットワーク機器を撮影し，画像処理技術を活用することによって利用者のネットワーク機器を監視する新しい手法について述べる．この手法では，障害の種類に応じて静止画もしくは動画を選択し利用する．提案手法を小型コンピュータに実装し，評価実験により利用者のネットワーク環境における状態監視に有効であることを示した．

キーワード：ネットワーク障害対応，ネットワーク機器監視，画像処理

Development of Monitoring Equipment for Network Devices by Using Small Computers and Image-processing Technology

Kohichi Ogawa[1,2] Noriaki Yoshiura[1,2,a)]

Received: June 26, 2017, Accepted: December 8, 2017

Abstract: In a university, users can freely use network equipment in the network of the university. Much of the network equipment does not deal with SNMP and even if SNMP is available, the network administrators cannot monitor the network equipment because it is of great variety. The network administrators, however, have to solve the network troubles that are caused by the network equipment in the user environment. To solve the network troubles is a big burden for network administrators. This paper suggests a system which reduces the burden for network administrators by checking a status of the network equipment of users through a web camera in conjunction with a small computer and by automatically determining whether the network equipment is at normal status or abnormal status. The system uses still images or videos that are obtained by the web camera. Whether the system uses still images or videos depends on which kinds of network troubles are focused on.

Keywords: Network Trouble Management, Network Equipment Monitoring, Image Processing

1. はじめに

大学などの教育機関において，情報基盤は教育研究を支える重要な要素の 1 つである．情報基盤の中でも学内ネットワークは，インターネットや学内サーバへの接続に必須であり，教職員や学生が講義や文献検索，研究・実験などに利用している．このため多くの大学では，学内ネットワー

1 埼玉大学情報メディア基盤センター
Information Technology Center, Saitama University, Saitama 338–8570, Japan
2 埼玉大学大学院理工学研究科
Graduate School of Science and Engineering, Saitama University, Saitama 338–8570, Japan
a) yoshiura@fmx.ics.saitama-u.ac.jp

クを整備し，ネットワーク管理組織（以下，情報センタ）を備えている．大学のネットワーク環境は，企業のネットワーク環境と比べて自由度が高い．企業では，ネットワークに接続できる機器は，あらかじめ認められた機器だけであり，厳しく制限されている．一方で，大学では，利用者は各自の用意したネットワーク機器（ルータやイーサネットスイッチなど）を学内ネットワークに各自の判断で接続している．このような環境では，利用者の判断で接続したネットワーク機器により，ネットワーク障害を引き起こすことがある．利用者は IT 技術に精通しているわけではなく，障害を自分自身で解決できない場合が多い．

この障害が利用者のネットワークに影響を及ぼすだけであればよいが，利用者のネットワーク以外，たとえば，学内ネットワーク全体に影響を及ぼす場合，情報センタが障害対応を行う必要が生じる．また，利用者のネットワーク内だけに障害が起きていたとしても，障害解決を利用者自身が行えない場合，大学の情報センタに利用者から障害対応の依頼が来ることとなる．大学の情報基盤の管理運用体制にもよるが，情報センタの関知しないネットワーク機器の障害に，情報センタが対応する必要が生じる．つまり，情報センタでは，利用者が独自の判断で学内ネットワークに接続した機器により生じたネットワーク障害への対応が必要となる．そして，この機器を情報センタのネットワーク管理者（以下，ネットワーク管理者）が障害対応時に初めて見ることになる．

利用者のネットワーク環境における障害は，ネットワークにつながらなくなる場合や，極端にネットワークが遅くなるなどの現象によって発覚する．**図 1** に示すように，この障害の多くは，イーサネットスイッチのループの形成，ネットワーク機器の故障，メタルケーブルの抜け，ネットワーク機器の電源抜けなど，利用者の不注意が原因である．しかし，利用者は障害の原因を特定できないため，情報センタに問い合わせる．ネットワーク管理者が利用者のもとへ出向き，障害対応せざるをえないのが現状である．

このようなネットワーク管理者の負担を軽減するため，我々はネットワークの運用自動化を検討している．その中で，ネットワーク管理者の障害解決の際の振舞いの 1 つである機器の目視による確認の自動化を目指している．そこで本論文では，管理者が管理機能のない機器の異常を調べる方法＝「目視」によって機器が正常か異常かをリアルタイムに判別する方法を提案する．さらに，ネットワーク管理者の目視を代替するカメラを利用した監視装置を開発した．具体的には，カメラでネットワーク機器の LED インジケータ（以下，LED）の静止画もしくは動画を撮影する．そして，検知したい障害の種類に応じて静止画もしくは動画を利用する．監視装置から，監視対象の状態を収集するために移動体通信回線を利用した．さらに，著者がネットワーク管理を行っている埼玉大学（以下，本学）で利用されているメディアコンバータの監視実験，イーサネットスイッチのループの形成検知の実験を通して提案手法の有用性を確認した．

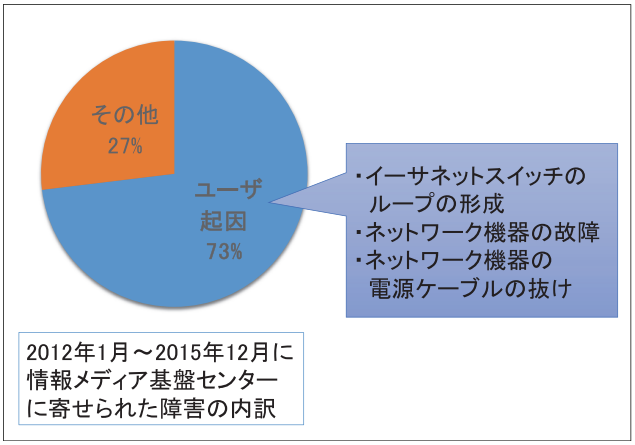

図 1 本学におけるネットワーク障害の原因
Fig. 1 Causes of network troubles in Saitama University.

本論文の構成は次のとおりである．2 章では，本論文の研究背景を述べる．3 章では，本論文で提案する手法を説明する．4 章では，提案手法の実装を説明する．5 章では，実装した監視装置の実際の運用結果を示す．6 章では，考察を行う．7 章では，関連研究を述べる．8 章で本論文をまとめる．

2. 背景

本章では，本論文の背景として利用者環境での障害とその対応の現状について述べる．

2.1 障害対応への人員とコストの不足

大学という教育研究機関の特性上，ネットワークは平日だけでなく休日深夜においても定常的に利用される．しかし，ネットワーク管理者として障害対応や利用者サポートにあたるセンタ職員の勤務時間は定められており，障害対応やサポートを行う時間帯が限られている．障害対応や利用者サポートを外部企業に委託することにより，24 時間・365 日の障害対応やサポートが可能となるが，相当額の委託費用がかかる．国立大学法人の固有の問題であるが，大学の財源が年々減少していくため，情報基盤の運用費用も減少せざるをえない．仮に委託する場合でも，障害対応に要する時間が事象ごとに異なるため，費用の見積りが困難で対応を定型化できず，委託自体が困難である．また，財源の問題とは別に，情報基盤の運用費用を減少させることは非常に重要である．

本学をはじめ，少数のセンタ職員で大学の情報基盤を運用する組織では，利用者のネットワーク環境を手厚く支援するところまで手が行き届かない．一方，企業では，利用する機器が組織全体で統一されており，利用者ごとに環境が異なるということは少ない．このことは，運用コストを

減少させている．大学のように，利用者の判断で，ネットワーク環境が作られている場合，利用者ごとに環境が異なり，障害の内容が多種多様となる．利用者自身はIT技術に精通していないことが多く，利用者自身による障害対応は困難である．そして，利用者自身による障害対応は困難であるからといって，利用者の近辺で発生した障害にセンタ職員が出向いて対応することも困難である．

しかし，利用者がかかえる障害を放置することは，大学のネットワーク全体へ悪影響を及ぼすこともある．たとえば，ネットワーク機器自体が行き先不明なパケットを大量に送出する例 [1] や複合的に障害を発生させる例 [2] が報告されている．これらの障害の原因は，機器の異常やループの形成によるもので，大量のブロードキャストを送出するブロードキャストストームである．ブロードキャストストームを防ぐ機能を持つLayer2スイッチやLayer3スイッチも存在する．しかし，一定量のストームを監視してブロックするだけで障害自体の追跡はできないため，障害の根本原因を発見できない．このようなブロックは，障害の影響を広範囲に伝播することを防ぐだけであり，障害の解決にはならない．また，障害の放置は，ブロックが機能しなくなったときに，さらなる大きな障害をひき起こす原因にもなる．つまり，大学の情報基盤の安定運用のために，利用者のネットワーク環境での障害への対応は必要であり，利用者のネットワーク環境の状況を的確に把握する必要がある．

一方，本論文での提案手法も，ブロードキャストストームを防ぐ機能を持つLayer2スイッチやLayer3スイッチと同様に，障害の根本原因を発見できるとは限らない．しかし，提案手法では，LEDを有するネットワーク機器であれば，直接監視することが可能であり，ループやストームの根本原因となっている端末やケーブルの接続箇所の特定に有効な情報を収集することができる．また，ネットワーク機器に対して特別な機能を必要とせずに，ネットワーク機器の監視を行うことができるという点から，利用者の様々なネットワーク環境の状況を的確に把握可能とする．

2.2 利用者のネットワーク機器の管理機能不足

通常，ネットワーク障害の検知は，管理ツールを用いた監視システムで行われる．監視システムとして，オープンソースソフトウェアではNagios [3] やZabbix [4] が，商用ソフトウェアではJP1 [5] やTivoli [6] などがよく利用されている．監視システムでネットワーク機器を監視する場合，ネットワーク機器が備えた管理機能として，SNMP（Simple Network Management Protocol）[7] といった監視プロトコルを用いて，機器の死活監視やネットワークの状態を確認する方法が用いられる．しかし，利用者が用意するネットワーク機器は，機能が最小限であり，SNMPなどの管理プロトコルや管理機能を備えていない場合が多い．利用する機器は利用者の裁量で決まるため，メーカや機器も多種多様で入れ替えも不定期に行われる．情報センタのネットワーク管理者が初めて目にするネットワーク機器も存在する．このため前述のような監視システムの利用は難しい．仮に，利用者が管理機能を持つネットワーク機器を利用しても，監視対象となるネットワーク機器が多く，管理が立ち行かなくなる．また，利用者が，障害対策機能を持つネットワーク機器を積極的に利用する必要がない．たとえば，ループ検知機能を持つイーサネットスイッチとその機能がないイーサネットスイッチがあれば，利用者は，コスト面から機能がないイーサネットスイッチを選択する．

2.3 継続監視の必要性

利用者が，自身の行動や自身が用意したネットワーク機器が原因で障害が起きた場合，その事実を簡単に認めることは少ない．つまり，障害が起きたときに，その原因を自分自身が関与していないネットワーク機器などにあると考えることが多い．また，1回の障害だけでは，その原因が明らかになることは少なく，利用者に障害の原因が自身の行動や自身が用意したネットワーク機器であると認めさせることは難しい．

障害の原因が分からない場合，障害が発生したネットワーク機器への継続的な監視が必要になる．しかし，ネットワーク管理者が継続して利用者のネットワーク環境を注視することはできない．その結果，障害発生時の時系列変化を確認できず，障害の原因が明らかにならず，障害の解消とはならない．また，慢性的に障害が頻発するような環境では，障害対応が長期間に及ぶ場合もある．このような場合，障害が発生する利用者のもとへ，ネットワーク管理者が何度も通う必要がある．

以上のことから，障害の原因を見つけ出すためには，ネットワーク管理者に負担がかからずに，継続して利用者のネットワーク環境を監視する仕組みが必要である．

3. 提案手法

本章では，利用者のネットワーク機器を継続的に監視するための監視手法について述べる．

3.1 画像処理による監視手法

ネットワーク管理者は障害の状況を把握する際に，問題がありそうなネットワーク機器を目視によって確認している．そこで，継続的な監視方法として，管理者の目の代わりとなるカメラと，その画像を保持，分析するコンピュータを監視装置として用い，ネットワーク機器の状態を自動的に把握する手法を提案する．手法は**図 2** に示すような流れとなる．

ネットワーク機器の障害時のLEDの点灯には，一定である場合と，変化がある場合の2つがある．前者に該当す

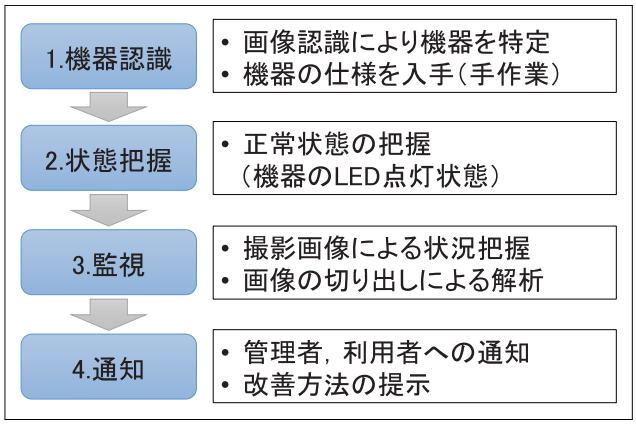

図 2 提案手法の処理手順
Fig. 2 Procedures of proposal method.

図 3 メディアコンバータの正常状態
Fig. 3 Normal state of a media converter.

るのは，たとえば，電源スイッチの ON・OFF，ネットワークケーブルのアクセスインジケータ，通信の状態など，障害がある場合に LED があらかじめ決まった点灯消灯となる場合である．この場合，LED の静止画により障害を検知できる．

後者は，たとえば，イーサネットスイッチのループ形成時の LED の点灯の仕方にあたる．LED は激しく点滅を繰り返す状態になるため，動画を撮影しなければ，障害を検知できない．

3.2 静止画で障害を検知できる場合

本節では提案手法のうち，静止画を用いた障害検知手法を説明する．機器の状態を確認するため，提案手法では，ネットワーク機器の LED の点灯表示の違いを利用する．ネットワーク機器の正常状態と異常状態の判定には 2 つの方法がある．点灯している LED の数のみを用いる方法と，点灯している LED の位置も考慮に入れる方法である．ここでは，本学で利用しているメディアコンバータを例にして説明を行う．本学では，サーバ室と各部屋の間に光ケーブルを敷設し，直接光ファイバケーブルで結ぶ光直収ネットワーク [8] を構築している．その光ファイバケーブルの両端にメディアコンバータを設置している．部屋側のメディアコンバータには，4 つの LED が備わっている．それぞれ，電源 LED，光のリンクアップ LED，メタルケーブルのリンクアップ LED，リンクスピード LED である．**図 3** のようにすべての LED が点灯している状態が正常状態である．

一方で，**図 4** に示すように LED が不完全な状態で点灯する場合がある．これらは，利用者が故意に電源やメタルケーブルもしくは光ファイバケーブルを抜いたことに起因する．提案手法では，これらの LED を画像処理によりオブジェクトとして識別して障害を検知する．

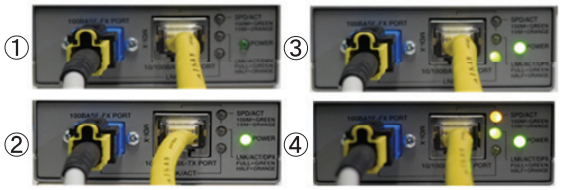

図 4 メディアコンバータの障害時の LED 表示パターン
（①：電源断，②：電源接続のみ，③：光ファイバケーブル接続のみ，④：メタルケーブル接続のみ）
Fig. 4 Display pattern of LED indicators in failure states of media converters.
(① Power supply down, ② No connection optical fiber cable and metal cable, ③ No connection to metal cable, ④ No connection to optical fiber cable).

表 1 メディアコンバータの状態パターン一覧
Table 1 Patterns of status of media converters.

パターン	正常	異常			
		①	②	③	④
電源	○	×	○	○	○
光リンク	○	×	×	○	×
メタルケーブルリンク	○	×	×	×	○
リンクスピード	○	×	×	×	○

メディアコンバータは，LED の点灯状態を把握することで 5 つのパターンに分けることができる（**表 1**）．

メディアコンバータがどのような状態かを把握するために，LED の点灯情報を収集する必要がある．具体的には，LED の点灯位置を把握するために，LED のみを検出する．そのために，撮影した画像に対して二値化処理を行い，LED が白く一連のつながった要素として表示されるようになる．この一連のつながった要素を「ブロブ」（Blob）という．ブロブの把握によって，物体の大きさや姿勢状態の把握が可能である．画像処理では，ブロブの形状を数値化する．また，1 つの画像内に複数のブロブが存在するときは，各ブロブに一意の識別子をつけて個々のブロブを識別するラベリング処理が行われる．このように，LED をブロブとして認識し，個々の LED をラベリング処理によって識別可能であれば，メディアコンバータの状態を把握できる．**図 5** はメディアコンバータの LED 点灯位置を把握するための処理の流れを示したものである．

図 6 にラベリング処理によってメディアコンバータの LED を検出する例を示す．矩形によって LED の範囲が正確にプロットされていることが分かる．しかし，イーサネットスイッチなど，点灯位置が異なるにもかかわらず同じ LED の点灯状態数となる場合が想定される．この場合は，画像認識で取得した位置情報により 2 つの状態の差を認識する．

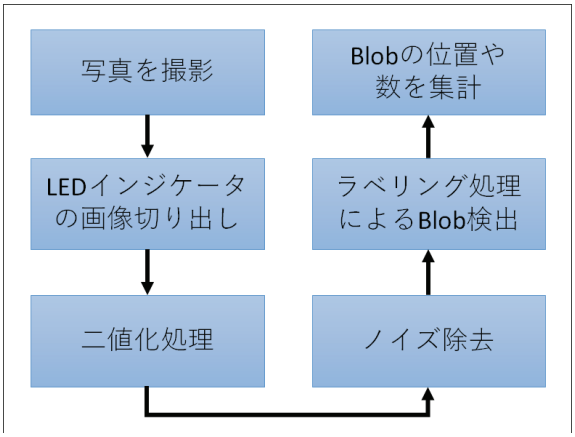

図 5 LED 点灯位置の把握処理
Fig. 5 Procedures of image processing.

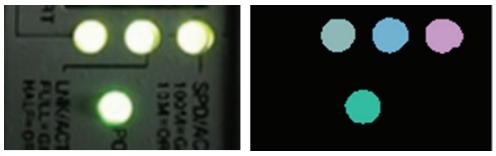

図 6 ラベリング処理による LED 検出の例
（左：元画像，右：LED 検出後の画像）
Fig. 6 Detect LED indicator of a media converter by labeling process.
(Left: Original image, Right: Recognition image).

このメディアコンバータの LED の数の検出については，直接位置情報は利用していない．位置情報は，LED の個数で正常状態か異常状態かをあらかじめパターン分けできない機器の状態の把握，追跡に有効である．

3.3 動画を用いて障害を検知する場合

本節では提案手法のうち，動画を用いた障害検知手法を説明する．利用者のネットワーク環境で多く発生する障害の 1 つにイーサネットスイッチのループの形成がある．この障害の多くは，研究室のレイアウト変更や清掃時，端末に接続していないメタルケーブルをイーサネットスイッチの空きポートに接続することで発生する．ループの形成時にはイーサネットスイッチの LED が激しく点滅を繰り返す．この場合，LED の状態を画像として複数枚連続で取得しても，見かけ上はつねに同じ状態であり，障害を認識できない．前節のメディアコンバータの監視手法や LED の点灯位置の把握手法では対応できない．

そこで，LED の点滅の頻度を把握するために，オプティカルフローにより，LED の点滅動作を動作ベクトルとして抽出し，抽出した傾向を利用して機械学習によって障害を検知する方法をとる．**図 7** は，イーサネットスイッチの LED の点滅状態を撮影し，動画データに対してオプティカルフローを用いてベクトルの状態を描画したものである．

オプティカルフローとは，時間的に連続した画像列を用いて画像の速度場を求め，速度ベクトルによって物体運動の様子を検出する手法である．オプティカルフローの利用の前提条件として，動きによって画像間での対応点の輝度が変わらないことが必要である．本論文では，イーサネットスイッチは移動しないという前提であるため，対応点の輝度は変化せず採用可能である．オプティカルフローの手法としては，勾配法 [9]，Lucas-Kanade 法 [10] がある．

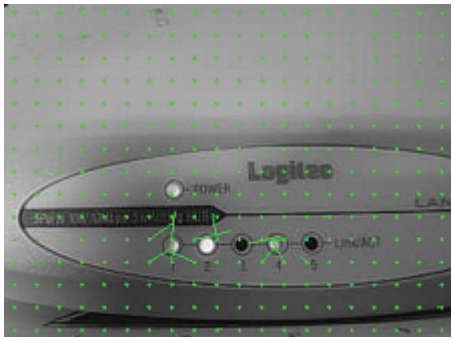

図 7 LED 点滅に対するオプティカルフロー描画の例
Fig. 7 An image of optical flow about LED indicator.

4. 提案手法による監視システムの実装

本章では前章で述べた提案手法に基づき，画像処理を用いた監視システムの実装について述べる．

4.1 監視システム構成

監視システムは，監視装置と監視情報集約サーバ，管理者端末で構成される．システムの構成概要を**図 8** に示す．

以下は，システムの処理の流れと各機器の役割である．

1. 監視装置は，監視装置に接続した USB カメラで LED を撮影し画像を保存する．撮影頻度，撮影間隔，撮影が動画であるか静止画であるかは，監視対象により決定する．
2. 監視装置は，撮影した画像データから画像処理により LED の情報を取得する．この情報は，監視対象により決定する．
3. 監視装置は，手順 2 で得た LED の情報を監視情報集約サーバに送信する．
4. 監視情報集約サーバでは，監視装置から送信された情報をデータベースに蓄積するとともに，送信された情報から監視対象機器の状態を判定し，管理者のブラウザに監視対象機器の最新情報を送信する．

なお，監視対象機器により，監視装置がどのような画像を取得するか，監視情報集約サーバがどのような処理を行うかが異なる．

4.2 通信方式

監視装置と監視情報集約サーバ間，監視情報集約サーバと管理者端末間の通信には，MQTT（Message Queue

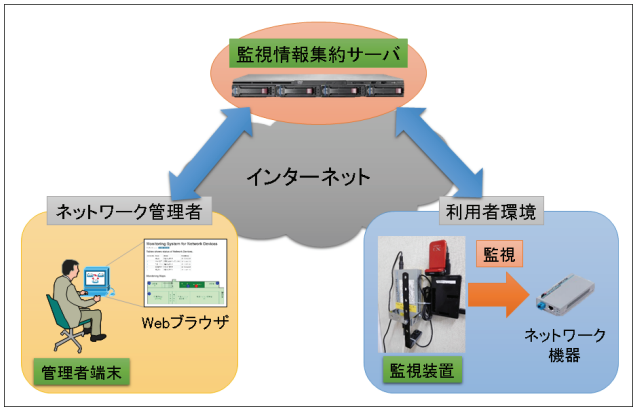

図 8 監視システムの構成概要
Fig. 8 Monitoring system architecture based on our method.

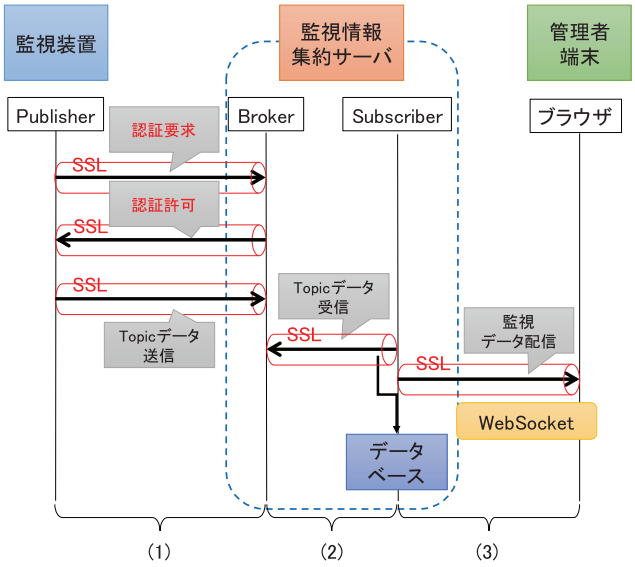

図 9 各機器間の通信フロー
Fig. 9 Communication flows between each equipment.

Telemetry Transport）[11] を利用する．MQTT は IoT 向けのメッセージキュープロトコルである．Publish/Subscribe モデル（出版購読モデル）を採用しており，プロトコルヘッダが小さいという特徴がある．実装には，MQTT の参照実装として広く利用されているオープンソースソフトウェアの Mosquitto [12] を採用する．

MQTT は，データを送出する Publisher，データを受信する Subscriber，Publisher と Subscriber の間をとりもつ中継の役割を担う Broker で構成される．Publisher は事前にデータを必要とする配信先を知る必要がなく，自分の範囲内の Broker にデータを送信するだけでよい．

本システムにおける各機器の通信フローを**図 9** に示す．監視装置は Publisher，監視情報集約サーバは Broker と Subscriber を兼務する．監視情報集約サーバは内部で定期的に Broker よりデータを購読することで監視データを取得する．

監視装置と監視情報集約サーバ間の通信は移動体通信回線を利用する．監視情報集約サーバと管理者端末の通信は学内ネットワークを利用する．監視情報は，WebSocket でリアルタイムに管理者端末に送信する．

図 10 監視装置の設置例
Fig. 10 An example of monitor equipment installation.

MQTT では，データは Topic という単位で定義される．取得したいデータがあれば，Topic を指定して購読する．監視装置の主要プログラムは Python で実装するため，Python の MQTT のパッケージ，Paho-mqtt [13] を利用した．時系列のログを収集して，監視情報を追跡可能にするために MySQL データベースを用意する．監視情報集約サーバの Subscriber は，内部の Broker の Topic を受信するのと同時にデータベースのテーブルへの書き込みを行う．このとき，管理者端末への WebSocket の通信も同時に実施する．WebSocket の実装には Python の Web フレームワークである Tornado [14] を採用する．

MQTT の通信は，セキュリティ面を考慮し SSL により通信を暗号化している．接続時にログイン認証を必須とし，一定のセキュリティを確保している．管理者端末から監視情報集約サーバへのアクセスは，Apache の SSL 通信により暗号化する．ブラウザが読み込んだ HTML ファイルに対して JavaScript を用い，WebSocket により監視情報の更新を Push 配信する．このとき，Tornado の SSL 暗号化により通信のセキュリティを確保する．

4.3 静止画を利用したメディアコンバータの監視装置

メディアコンバータの監視装置では，静止画を利用する．監視装置は，LED を監視するため，Raspberry Pi に USB 接続の Web カメラを取り付け，5 分ごとに撮影し監視を行う．監視装置について**図 10** に設置例を示す．不特定多数の利用者が出入りするオープンスペースでは，ウオルボックスを設置して施錠する．実装には画像ライブラリとして OpenCV [15] を用いる．プログラミング言語は Python 2.7 を用いる．OpenCV のブロブ検出機能を利用してブロブを特定し，LED の点灯状態を取得する．このため，OpenCV のバージョンは，ブロブ検出ライブラリをサポートする 3.1.0 を用いる．障害を想定した場合，監視対

図 11 Web カメラのアタッチメントによる装着例
Fig. 11 An example of attachments of the web camera.

象のネットワークは利用不能となるため，監視装置の通信には移動体通信回線を利用する．監視装置の仕様は以下のとおりである．

- コンピュータ：Raspberry Pi 3
- カメラ：BSWHD06MBK
- データ通信端末：L-02C
- OS：Rasbian Jessie

監視装置では，LED の画像を取得し，二値化などの処理を行い，点灯している LED の個数を求め，その個数を監視情報集約サーバへ送信する．監視情報集約サーバでは，送信された情報を保存するとともに，LED の個数が正常な場合と同じであるかを調べる．

4.4 Web カメラのアタッチメント

ネットワーク機器の LED を的確に監視するためには，LED を監視しやすい位置に取り付ける必要がある．たとえば，本学のメディアコンバータは壁に常設しており，最適な位置に Web カメラを固定可能である．そこで，金具を組み合わせたアタッチメントを設計し，取り付けている（**図 11**）．

監視対象であるメディアコンバータの組み込みネジを利用して，メディアコンバータ自体に金具を直接取り付ける方法を考案した．この方法により，監視を開始する際にメディアコンバータの電源を停止する必要がなく，短時間で装着ができ，既存の利用環境へ与える負荷を最小限に抑えることができる．部屋などに設置され，固定されていないイーサネットスイッチの監視には，ある程度の範囲で移動可能な Web カメラを設置することとした．

4.5 動画を利用したイーサネットスイッチの監視装置

イーサネットスイッチの監視装置では，LED の動画を取得し，オプティカルフローを利用して分析する必要がある．このため，Raspberry Pi では処理能力が不足すると判断される．そこで，次の構成の機器を監視装置として利用する．

- コンピュータ：Intel NUC DN2820FYKH

図 12 イーサネットスイッチ監視システムの設置例
Fig. 12 An example of monitoring system for ethernet switch.

- CPU：Intel Celeron 2.4 GHz Dual Core
- メモリ：4 GB
- 補助記憶装置：SSD 120 GB
- OS：Ubuntu 14.04 LTS
- カメラ：Buffalo BSW20KM11BK

図 12 に監視装置の設置例を示す．基本構成はメディアコンバータの監視装置と同じである．監視対象のイーサネットスイッチの状態を動画で撮影する．データのノイズ除去や動画サイズの縮小などの前処理を行い，特徴量の抽出を行う．実装には，4.3 節のメディアコンバータの監視装置と同様に画像ライブラリとして OpenCV を用いる．OpenCV のバージョンは 2.4.10 である．プログラミング言語は Python 2.7 を用いる．ループ障害を想定した場合，監視対象のネットワークは利用不能となるため，監視装置の通信には移動体通信回線を利用する．

次に，イーサネットスイッチのループの形成検知の仕組みを説明する．監視装置に接続された Web カメラで，監視対象のイーサネットスイッチの状態を動画で撮影する．監視装置は，データのノイズ除去や動画サイズの縮小などの前処理を行い，特徴量の抽出を行う．これらのデータはネットワークを通じて監視情報集約サーバに転送する．監視情報集約サーバでは，あらかじめ正常状態と異常状態を教師あり学習により学習させておく．あらかじめ学習した情報と，監視装置で取得した情報を比較することによって，正常状態か異常状態かを判断させる．

動きの特徴量の抽出については，文献 [16] の手法を用い，「動画のフレームごとの最大ベクトル量（Max0）」を算出し利用する．実装は文献 [17] を参考に実施した．算出にあたっては OpenCV の関数 cvCalcOpticalFlowLK で Lucas-Kanade 法を用い疎な特徴集合に対するオプティカルフローを求める．これにより x 方向の速度ベクトル vx と y 方向の速度ベクトル vy が求まる．次に OpenCV の関数 cvCartToPolar により極座標変換を行い，先に求めた速

度ベクトル vx，vy をもとに特徴量の大きさを算出する．

画像の特徴量から，ループであるかの判定は機械学習を用いて行う．機械学習に用いる実装は，オンライン機械学習フレームワークである Jubatus [18] を用いる．Jubatus を採用した理由は，あらかじめ機械学習のアルゴリズムが備わっており，実装が容易なこと，そしてサーバを分散構築可能なことである．ループという事象の発見には，平常時が継続的に続く中で異常な値が発見される「異常検知」ではなく，一定期間の LED 点滅の傾向を学習し，新たな状態との比較検証を行う必要があると考えた．実装は，Jubatus において標準で利用可能な AROW（Adaptive Regularization of Weight vectors）[19] を用いた．この AROW は機械学習アルゴリズムのうち「分類」にあたる．学習に関する感度設定は 1.0 とした．

機械学習を行った結果は，監視情報集約サーバにおいて利用される．イーサネットスイッチの監視は，監視装置で動画を 30 秒間撮影し，その動画をオプティカルフローにより数値化する．数値化したデータは，監視情報集約サーバへ送信され，監視情報集約サーバで判定を行う．その判定結果に基づいて，管理者へ通知を行う．

4.6 監視情報集約サーバ

監視装置と監視情報集約サーバの通信は，監視対象の機器が利用する学内ネットワークではなく，インターネットを介して行われる．セキュリティの確保は SSL 証明書とユーザ認証により実現する．SSL 証明書は国立情報学研究所が提供する UPKI サービスのサーバ証明書 [20] を利用した．サーバは学内のサーバ室に収容し，固定 IP アドレスを付与した．監視情報集約サーバの仕様は以下のとおりである．

- コンピュータ：HP ProLiant DL320G6
- CPU：Intel Xeon 2.53 GHz Dual Core
- メモリ：8 GB
- 補助記憶装置：HDD 600 GB × 2（RAID1）
- OS：Ubuntu Server 14.04.4

このサーバは，メディアコンバータの監視装置やイーサネットスイッチの監視装置からの情報を受け取り，各装置の状態を判定する．

4.7 管理者端末

管理者端末のユーザインタフェースには，OS やハードウェアを問わず利用可能なブラウザを採用した．ただし，管理者が能動的にブラウザを読み込んで確認する方法は，監視システムにおける通知方法として望ましくない．そこで，即時性を確保するために，監視装置からの情報がリアルタイムに画面上で更新されるよう，WebSocket を採用した．本論文では，情報センタに設置された大きなディスプレイに管理者端末の画面を表示するといった利用方法を想定している．よって監視状況は，情報センタにいる全員が把握することができ，監視対象に異常があったことを把握できる．実際の管理者端末の画面を**図 13** に示す．

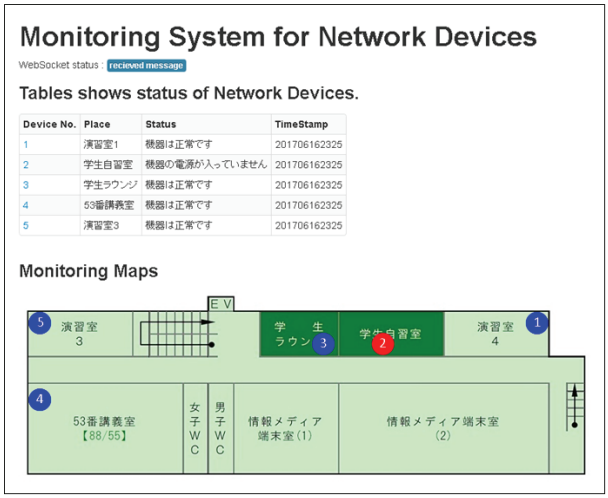

図 13 管理者端末の画面
Fig. 13 User interface of network administrator's terminal.

画面上には実際の監視装置の設置個所の地図を表示し，監視対象の機器が存在する位置を JavaScript の図形ライブラリである Canvas を用いて図示した．異常があるネットワーク機器は赤く点灯させ，管理者に注意喚起する．

5. 監視システムによる実証実験

本章では，前章で述べた監視システムを用い，本学で実運用しているメディアコンバータとイーサネットスイッチを利用した実証実験について述べる．

5.1 メディアコンバータの障害検知の検証結果

メディアコンバータの障害検知の精度を評価するために実験を行った．この実験は，図 13 にもあるように，本学工学部講義棟 2F に設置されている 5 カ所のメディアコンバータに，図 10 の監視装置を取り付け，障害検知の精度を調べた．実験期間は，2017 年 6 月 12 日～2017 年 6 月 16 日の 5 日間である．この期間中，メディアコンバータに異常は発生せず，監視システムは，誤検知，すなわち，メディアコンバータに障害が発生したと判断することがなかった．

一方，障害が発生した場合の監視システムの検知率を確認するために，故意に障害を発生させ，検知率を調べた．具体的には，後述する 5.3 節の実験を利用した．5.3 節の実験では，故意に 4 つのパターンの障害を発生させ，障害検知の通知時間を調べている．5.3 節の実験では，4 つの障害パターンを 75 回，合計 300 回の障害を故意に発生させて，監視システムの検知率を調べた．その結果は，300 回の障害をすべて検知した．本論文での実験結果から，メディアコンバータの障害検知は，偽陽性と偽陰性いずれも

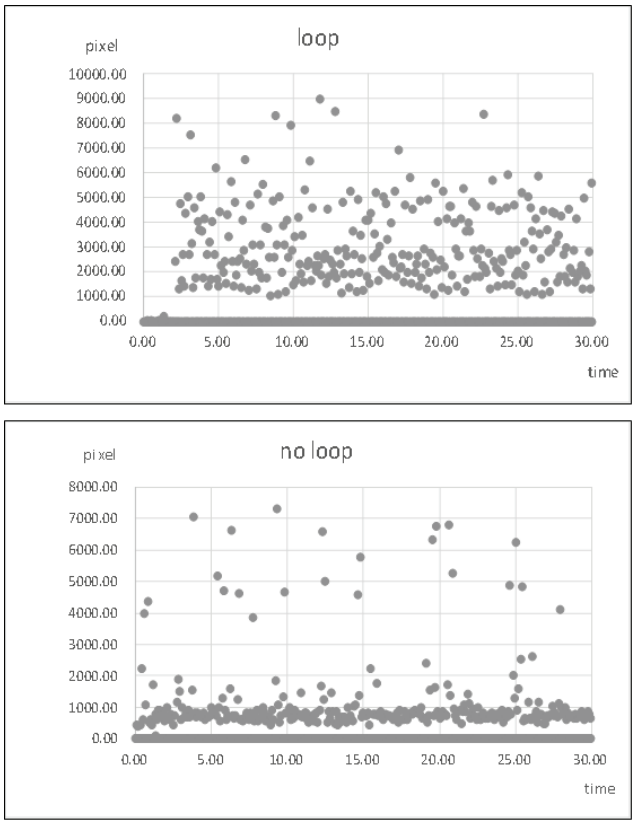

図 14 動きの特徴量抽出例
（上：ループ形成状態，下：正常状態）
Fig. 14 Image feature extraction by optical flow.
(Upper: Loop status, Downer: Normal status).

0%であり，提案手法は実際のメディアコンバータの障害検知に十分利用可能であるといえる．

5.2 イーサネットスイッチのループ形成検知の検証

イーサネットスイッチのループ形成検知の手法を評価するために実験を行った．実験は，ロジテック社製の100BASE-TX 対応，5 ポート（型名：LAN-SW05/P）のイーサネットスイッチを用いた．実験の条件として，暗い室内でイーサネットスイッチのループ形成状態，正常状態をそれぞれ 1 回あたり 30 秒間撮影する．これを 10 回ずつ繰り返し，取得した動画データから動きの特徴量を抽出する．結果の一部を**図 14** に示す．

正常状態の際の特徴量は，小さい値で推移しているのに比べ，ループ形成状態の際の特徴量は中間部に多くの値が集まっていることが分かる．数回の実験においても同様の傾向が現れていることから，機械学習器にこれらの特徴量を投入し学習させる．

ループ形成状態，正常状態の判別用のテスト動画をそれぞれ 1 回あたり 30 秒間で 3 回ずつ，計 6 回分撮影し，機械学習器にかけ判定テストを行った．

Jubatus は，機械学習のフレームワーク内に評価指標が定義されている．Jubatus の Client API [21] によれば，score

表 2 イーサネットスイッチ監視システム判定テスト結果
Table 2 A result of evaluation test of monitoring system.

	1	2	3	4	5	6
正常	1.179227	1.009736	0.876641	0.121993	-0.0238	0.186229
ループ	-0.39924	-0.24146	-0.12336	0.932147	1.075903	0.758367

表 3 実験で使用した SIM カードの仕様一覧
Table 3 Specification lists of 3G/LTE network venders.

MVNO企業名	楽天モバイル	nuromobile	OCNモバイル
SIMの種類	データSIM	データSIM	データSIM
SIM通信速度	最大200Kbps	帯域制限なし	1日110MBまで帯域制限なし以降200Kbps
料金（月額）	525円	0円～1600円（500MBまで0円）	972円
付与IPアドレス	プライベート	プライベート	グローバル

とは，ラベルに対する確からしさの値で，score の値が大きいほど推定されたラベルの信頼性が高いことを意味している．本研究では，正常状態とループ形成状態の 2 つの状態をラベルとして，score を計算する．その結果として，score の高いラベルをイーサネットスイッチの状態と判定する．

この方法に基づいて，テストデータにより実験を行った結果が**表 2** である．1～3 が正常状態，4～6 がループ形成状態である．いずれのテストでも当該の状態に対して score は高い値を示し，正しく判定可能なことを確認した．

5.3 監視システムのリアルタイム性の検証

本実験の目的は，監視システムが実際のネットワーク運用において，十分なリアルタイム性を持つかを確認することである．図 9 において，(3) の監視情報集約サーバと管理者端末間の通信は，本学も含めて，学内ネットワークを利用することが多いと考えられる．この場合，(3) の通信は情報センタの管理下にある．しかし，(1) の監視装置と監視情報集約サーバ間の通信は，移動体通信回線を用いるため，情報センタの管理外であり，通信時間を管理することは難しい．そこで，実験を行い通信時間や通信速度を調べ，監視システムのリアルタイム性を確認する．

この実験では，監視装置と監視情報集約サーバ間の通信に用いる移動体通信回線として 3 種類の回線を準備した．**表 3** に仕様の一覧を示す．このような SIM カードを提供する企業は，仮想移動体通信事業者（Mobile Virtual Network Operator，以下 MVNO）と呼ばれ，回線設備は持たずに他の回線業者の回線を間借りしてサービスを提供する企業を指す [22]．表 3 の企業は，いずれも NTT ドコモの MVNO 提供業者である．

本実験では，メディアコンバータの監視装置を利用した．実験方法は，5.1 節の 5 カ所に設置されたメディアコンバータにそれぞれに，4 つの検証条件の障害を故意に発生させることで実施した．検証条件を下記に示す．

表 4 各実験回数における平均処理時間
（括弧内の番号は図 9 の下部に対応）

Table 4 Processing average time of each test pattern.

実験回数	(1)[s]						(2)[s]	(3)[s]
	処理時間	楽天	処理時間	Nuro	処理時間	OCN		
1	0.025	0.287	0.029	0.314	0.025	0.342	0.250	0.016
2	0.026	0.286	0.029	0.262	0.024	0.352	0.175	0.023
3	0.025	0.265	0.025	0.405	0.026	0.343	0.240	0.015
4	0.027	0.239	0.026	0.318	0.027	0.341	0.321	0.031
5	0.026	0.248	0.026	0.256	0.026	0.329	0.204	0.032
平均	0.026	0.265	0.027	0.311	0.026	0.341	0.238	0.023

■ 検証条件

1. メタルケーブル接続のみ（LED が 3 つ点灯）（図 4 ④に該当）
2. 光ファイバケーブル接続のみ（LED が 2 つ点灯）（図 4 ③に該当）
3. 電源のみ（LED が 1 つ点灯）（図 4 ②に該当）
4. 電源断（全 LED が消灯）（図 4 ①に該当）

検証条件に，正常な状態をあげていない理由は，他の 4 つの検証条件における処理時間との差が見られなかったためである．今回は各検証条件において同一の日時でプログラム内，もしくはログを利用して処理にかかる時間を計測する．連続して 5 回の計測し，平均を算出した．**表 4** に各実験回数における平均処理時間を，**表 5** に検証条件における平均処理時間を示す．

(1) のうち移動体通信回線の使用した通信は，各社ともに 0.3 s 程度の通信でデータをサーバへ送信できることが分かった．これは MQTT のプロトコルヘッダが小さく，少量のデータを細かく転送する通信に向いているためであると考えられる．(2) は主に監視情報集約サーバ内の処理である．平均で 0.23 s 程度処理に要しており，これは受信した監視データをサーバ上で処理するために多少時間がかかっていると推測される．(3) では WebSocket のデータ受信のみの計測で平均して 0.023 s で通信できることが分かった．また，表 5 から，障害の種類が，障害発生から障害通知までの時間に影響を与えないことが分かった．この実験から，5 分ごとに行っている撮影の頻度を，1 秒ごとまで短くし，障害検知をリアルタイムに実行可能であることが分かった．

提案手法を実装した監視システム利用時の監視装置と監視情報集約サーバ間のトラフィック量は，MQTT のデータ形式である Topic として，ブロブのカウント数とタイムスタンプ，LED の画像ファイルなどを合わせて 13 Kbyte となる．1 分ごとに撮影し障害検知を行う場合，1 日で約 18.7 Mbyte, 1 カ月で約 562 Mbyte である．このトラフィック量であれば，表 3 から見ても，移動体通信回線を用いても十分対応可能なトラフィック量であると考えられる．

表 5 各検証条件における平均処理時間
（括弧内の番号は図 9 の下部に対応）

Table 5 Processing average time of verification conditions.

検証条件	(1)[s]						(2)[s]	(3)[s]
	処理時間	楽天	処理時間	Nuro	処理時間	OCN		
1	0.025	0.311	0.029	0.335	0.025	0.354	0.250	0.016
2	0.026	0.255	0.029	0.294	0.024	0.329	0.175	0.023
3	0.025	0.245	0.025	0.265	0.026	0.332	0.240	0.015
4	0.027	0.249	0.026	0.350	0.027	0.349	0.321	0.031
平均	0.026	0.265	0.027	0.311	0.026	0.341	0.247	0.021

イーサネットスイッチのループの形成検知において Topic は，オプティカルフローにおける動きの最大値を示すベクトル情報とタイムスタンプであり，1 分間のトラフィック量は約 10 Kbyte である．メディアコンバータの監視装置よりもトラフィック量は少なく，1 日で約 14.4 Mbyte，1 カ月で約 432 Mbyte であり，メディアコンバータの監視装置同様に移動体通信回線を用いても十分対応可能なトラフィック量であると考えられる．

6. 考察

本章では，提案手法による評価実験をもとに課題に対する考察について述べる．

6.1 提案装置の課題

実験結果から，提案システムでは，ネットワーク機器の異常を検知することが可能である．ただし，現段階では次のような課題がある．

1. カメラのアングルを固定する必要がある．
2. 汎用性が乏しい．

1 については，本論文では，カメラに金具をつけてカメラを固定することでアングルを固定している．この設置の手間を軽減することが今後の課題である．具体的には，簡単に設置できる器具の開発や，カメラのアングルが，金具で固定されていた位置から多少ずれた場合であっても，LED を適確に取得可能な画像処理手法の開発により，この課題を解決したい．

2 については，今後様々な障害検知を提案手法で可能となるように，画像処理手法を蓄積し，画像ライブラリとすることで，汎用性を向上させることを考えている．

本論文の提案手法は，メディアコンバータのような LED の点灯パターンを振り分け可能なネットワーク機器の障害検知，イーサネットスイッチにおいてループが形成された場合の LED の高速点滅によるループの検知に対応できる．しかし，色に対する対応については現状では考慮されていない．つまり，LED の色によって状態が変化するネットワーク機器の障害検知に本提案手法は利用できない．たとえば，機器に不具合があった場合に緑色から赤色に変わる

LED を監視しても不具合を確認できない．また，イーサネットスイッチにおいても，バーストトラフィックで高速点滅する場合がある．現状ではループが形成された場合との違いについて，検証を実施できていない．今後，これらの課題にも取り組んでいく予定である．そして，本論文の提案手法の利用可能範囲を拡大し，汎用性を向上させたいと考えている．

6.2 人手不足に対する解決

提案手法により実装した監視装置を用いることによって，ネットワーク機器が設置された場所にネットワーク管理者が赴かなくても状態を把握可能である．また，移動体通信回線の活用により，ネットワークがない箇所でも監視を維持可能である．メディアコンバータやイーサネットスイッチをはじめ，LED 表示部を持つネットワーク機器は状態変化を把握可能である．

提案手法は，通信が不能になった場合でも監視装置自体の障害か故障であると判断ができる．監視情報集約サーバに蓄積された情報から時系列で順を追って状況変化を把握可能で，監視装置が最後の監視情報を報告するまで，さかのぼってネットワーク機器の状態を追跡可能である．

6.3 利用者ネットワーク環境の把握

提案手法は，SNMP などの監視プロトコルや管理機能がなくても利用者のネットワーク機器の状態を監視可能であることを示した．このことにより，ネットワーク管理者が利用者のもとへ駆けつける前に症状を把握可能である．障害のある部屋へ向かわなくても，利用者に対して電話やメールなどで解決方法をアドバイスすることも可能となる．

メディアコンバータの監視装置の実装では，メディアコンバータの LED の状態を 5 分ごとに静止画で撮影したが，この撮影の頻度が適切かを検討する必要がある．

データベースを活用することにより，長期的な監視が可能となる．監視装置自体が不具合により停止しても，それまでの記録は監視情報集約サーバに蓄積される．このことから，研究室で発生する障害について時系列で障害発生の原因を追跡可能であるといえる．

7. 関連研究

通信の監視の研究では，北口ら [23] は無線 LAN アクセスポイントの状態評価を目的として通信の品質や性能などの指標に基づいて，Raspberry Pi を用いて監視を行う手法を提案している．しかし，当該研究では監視用の有線ネットワークが必要である点など，本論文とは異なる．大垣内ら [24] は，大学ネットワークを構成するエッジスイッチに OpenBlocks を接続してモニタリングする手法を提案しているが，利用者のネットワーク環境自体の監視ではなく，本論文の視点とは異なる．

ネットワークの障害を検知する方法には，ネットワーク機器から収集したログを機械学習やデータマイニングの手法で分析する方法 [25] がある．しかし，ネットワーク機器のログ出力機能や SNMP などの監視プロトコルを備えた機器に限定され，利用者がふだん使う簡易的な機器を網羅できない．一部市販のルータはログを出力する機能を持つが，継続してログを収集するためには別途サーバが必要であり，異常を検知した際には管理者へ通知する監視専用のネットワークが必要となる．また，端末から流れるパケットを分析することにより異常検知を行う方法 [26] や，端末にエージントプログラムを導入して監視する方法があるが，障害の原因が端末にある場合に限られ，この方法ではネットワーク機器に問題があるとは判断できない．

SNMP により監視を行うことで，利用者のバーストトラフィックやブロードキャストストームを検知する研究 [27] もある．しかし，ネットワーク全体への影響を防ぐことに重点が置かれており，利用者が引き起したネットワーク障害自体の解決には利用できない．

以上の点から，本論文のような利用者のネットワーク環境を直接監視し状態を把握するような研究は希少である．本論文は LED を持つ機器であれば監視可能であり，他の研究分野での応用も十分期待できる．

8. おわりに

本論文では，利用者のネットワーク環境に焦点を当て，ネットワーク管理者の行動に着目し，画像処理技術を活用した監視手法を示した．具体的には，カメラで LED の状態を撮影する際，障害の種類に応じて静止画もしくは動画のうち，最適な方を選択して適用することを提案し，実装した．実装には小型コンピュータを用い，監視装置を開発し，監視システムによる実証実験を通して提案手法の有効性を確認した．今後は，実証実験を継続するとともに課題解決を進め，監視装置の情報収集手法について別の解決策も検討していく予定である．

謝辞 本論文の一部は，JSPS 科研費 17H00371 の助成によるものである．

参考文献

[1] インターネット接続解説ブログ KAGEMARU-info（オンライン），入手先 ⟨https://www.akakagemaru.info/port/cannotinternet-hub.html⟩.
[2] 日経ネットワーク：トラブルシューティング「気づき」のヒント，pp.28–43, 日経 BP 社 (June 2012).
[3] Nagios (online), available from ⟨https://www.nagios.org/⟩ (accessed 2017-10-06).
[4] Zabbix (online), available from ⟨http://www.zabbix.com/jp/⟩ (accessed 2017-10-06).
[5] JP1 (online), available from ⟨http://www.hitachi.co.jp/Prod/comp/soft1/jp1/index.html⟩ (accessed 2017-10-06).
[6] Tivoli (online), available from ⟨http://www.ibm.com/

software/tivoli⟩ (accessed 2017-10-06).
[7] Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, The Internet Society (2003).
[8] 小川康一，吉浦紀晃：埼玉大学における光ファイバ直収型ネットワークの運用経験について，情報処理学会研究報告インターネットと運用技術（IOT），2015-IOT-30, pp.1–8 (2015).
[9] Olivier D.F.: *Three-Dimensional Computer Vision, A Geometric Viewpoint*, MIT Press, Cambridge, MA (1993).
[10] Bruce, D.L. and Takeo, K.: An iterative image registration technique with an application to stereo vision, *Proc. 7th international joint conference on Artificial intelligence - Volume 2* (*IJCAI'81*), Vol.2, pp.674–679, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (1981).
[11] MQTT (online), available from ⟨http://mqtt.org/⟩ (accessed 2017-10-06).
[12] Mosquitto (online), available from ⟨https://mosquitto.org/⟩ (accessed 2017-10-06).
[13] Paho-mqtt (online), available from ⟨https://pypi.python.org/pypi/paho-mqtt⟩ (accessed 2017-10-06).
[14] Tornado (online), available from ⟨http://www.tornadoweb.org/en/stable/⟩ (accessed 2017-10-06).
[15] 画像ライブラリ OpenCV，入手先 ⟨http://opencv.org/⟩（参照 2017-10-05）.
[16] Kadir, A.P. and Ajay, D.: A novel pair-wise comparison based analytical framework for automatic measurement of intensity of motion activity of video segments, *IEEE International Conference on Multimedia and Expo* (*ICME 2001*), pp.729–732 (2001).
[17] デジタル映像分析 OpenCV による映像内容の解析，カットシステム (2012).
[18] オンライン機械学習向け分散処理フレームワーク Jubatus（オンライン），入手先 ⟨http://jubat.us/ja/⟩（参照 2017-10-05）.
[19] Koby, C., Alex, K. and Mark, D.: Adaptive regularization of weight vectors, *Machine Learning*, Vol.91, No.2, pp.155–187 (2013).
[20] UPKI 電子証明書発行サービス（オンライン），入手先 ⟨https://certs.nii.ac.jp/⟩（参照 2017-10-05）.
[21] Jubatus References (online), available from ⟨http://jubat.us/ja/api_classifier.html⟩ (accessed 2017-10-06).
[22] MVNO に係る電気通信事業法及び電波法の適用関係に関するガイドラインの改定（プレスリリース），総務省（2017 年 2 月）（オンライン），入手先 ⟨http://www.soumu.go.jp/menu_news/s-news/01kiban03_02000411.html⟩（参照 2017-05-31）.
[23] 北口善明，石原知洋，高嶋健人，田川真樹，田中晋太朗：Raspberry Pi を用いた無線ネットワーク状態評価手法の提案，研究報告インターネットと運用技術（IOT），2014-IOT-25, pp.1–6 (2014).
[24] 大垣内多徳，半田憲嗣，澤田雅子，福井一俊，山下芳範：福井大学学内ネットワークシステムの設計と構築，研究報告インターネットと運用技術（IOT），pp.1–6 (2010).
[25] 木村達明：Syslog 分析による大規模ネットワーク故障診断技術—ネットワーク機器ログデータの活用，電子情報信学会会誌，Vol.98, No.9, pp.823–828 (2015).
[26] 國吉賢吾，森井昌克：端末監視によるホームネットワーク異常検知システム，研究報告ユビキタスコンピューティングシステム（UBI），pp.39–46 (2009).
[27] 村井秀聡，砂田英之，牧 和宏：SNMP を利用したバーストトラフィック検知方式の提案，情報科学技術フォーラム講演論文集，FIT2014, pp.175–178 (2014).

小川 康一 （学生会員）

1974 年生．2014 年産業技術大学院大学産業技術研究科修了．情報システム学修士（専門職）．現在，埼玉大学大学院理工学研究科博士後期課程に在学中．同大学情報メディア基盤センターで全学の情報基盤システムの管理運用業務に従事しながら，研究を実施している．電子情報通信学会，日本ソフトウェア科学会，日本ロボット学会，IEEE，ACM 各会員．

吉浦 紀晃 （正会員）

1968 年生．1991 年東京工業大学工学部情報工学科卒業．1997 年同大学大学院博士課程単位取得退学．博士（学術）．東京工業大学助手，群馬大学助教授を経て，現在，埼玉大学大学院理工学研究科准教授．ソフトウェア検証やネットワーク運用技術の研究に従事．電子情報通信学会，社会情報学会各会員．