

# 回線切断を含むネットワーク防災訓練に関する報告

佐々木 正人†, 豊永 昌彦‡

高知大学総合情報センター†

高知大学自然科学系理学部門‡

sasaki@kochi-u.ac.jp, toyonaga@is.kochi-u.ac.jp

概要：災害等による停電や計算機室温異常などを想定し、これらの障害を人為的に発生させて、監視システムによる検知・通報，担当者による手順通りの対応ができるか訓練を実施した．さらに，上位接続回線を実際に切断し障害箇所の特定や復旧作業が実施できるかについても訓練を実施した．これまでの2回の訓練における本学の問題点や課題，改善点等について報告する．

## 1 はじめに

SINET 高知ノード設置を契機に，2012年4月高知学術情報ネットワーク連絡会を立ち上げ高知県域の学術ネットワークの在り方やその具体的構成等について協議してきた．現在では，連絡会参加の高知大学，高知工科大学，高知県立大学，高知工業高等専門学校，高知学園短期大学が同じ回線業者が提供する冗長構成，マルチホーム，地域IX機能等を利用して学外接続を実現している．さらに，連絡会参加組織を中心にして，災害発生時に迅速に復旧するための技術の研究開発，人為的に障害を発生させてのネットワーク防災訓練などを行うプロジェクト(SCOPE 132309010)が進行中である．本稿では，上記プロジェクトで2回実施されたネットワーク防災訓練における本学の問題点や課題，改善点等について報告する．

## 2 ネットワーク構成と管理運用体制

### 2.1 キャンパス間，学外接続について

本学は5つのキャンパス(朝倉，物部，岡豊，宇佐，小津)に分かれており，総合情報センターのある朝倉地区と他地区を接続し，朝倉地区から学外に接続している．このうち学外接続および朝倉と物部，岡豊地区間は，別ルートで敷設されている光ケーブルにより冗長構成としている．

### 2.2 監視システム

本学では，レンタル機器監視システムと本学独自で開発運用している高知大学版監視システムでシステム全体を常時監視している．異常を検知すると学内メールサーバを経由して保守業者(オペレーションセンターは四国外地域)と学内担当者・管理者に電子メールや携帯メールで通知する．

しかし，学内メールサーバの障害や学外接続でトラブルが発生すると必ずしも通知が届かない．特に夜間・早朝にメール配送されない場合はトラブルの発生に気付くのが大幅に遅れてしまう．

そこで高知大学版監視システムでは，学外監視サーバも設置し，学内ネットワークへの経路や接続性の監視および異常時の通知を行っている．

### 2.3 監視体制

学内担当者(常勤)が勤務している時間帯は，高知大学版監視コンソール画面(図1)を常に表示し，トラブルが発生すると管理者や保守業者と連絡を取りながら対応している．学内担当者勤務後及び土日の総合情報センター開館時間帯(通常21:00閉館)は夜間学生スタッフが監視業務を引き継ぐ．その後の夜間・早朝は無人となりこの間は管理者と保守業者へメールにより通報している．

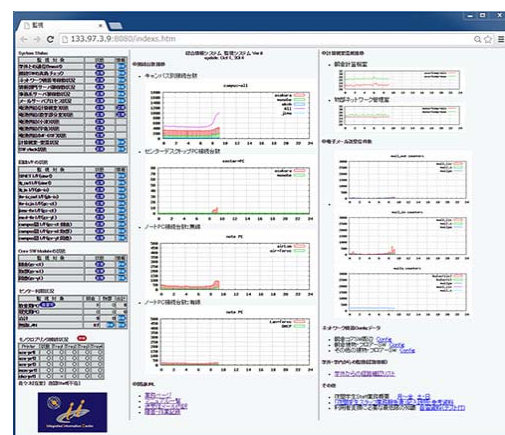


図1 高知大学版監視コンソール(正常時)

### 2.4 監視対象と監視内容

高知大学版監視システムの監視対象は，学内のネットワーク機器(L2/L3-SW, FW, AP等)や主要な計算機システム(仮想化基盤上のDNSサーバ，

メールサーバ、認証サーバ等)である。死活監視、冗長構成の確認、メール配送機能の状態確認等を行っている。また、各キャンパスの主要箇所の停電検知、計算機室の室温監視なども実施し、常に監視コンソールに正常か異常が表示される。また、レンタル機器監視システムの監視対象は学内ネットワーク機器のみで、機器単体の詳細な障害情報の収集と異常時のメール通知を行っている。

## 2.5 異常時通知方法

障害の重要度により、監視コンソールへの表示、電子メール通知、パトランプ点滅・ブザー音、携帯メール通知を組み合わせることで異常を通知する。いずれかの方法で障害発生に気付くと、事前に取り決めている手順にて対応することになっている。

## 3 ネットワーク防災訓練の目的と概要

訓練の目的は、障害を人為的に発生させ、システムや機器等の二重化・冗長化機能が計画通り実現できるか、障害に対してあらかじめ策定している手順通りに担当者に対応できるかを確認し、課題や問題点を洗い出し改善することである。特に、過去検証されなかったような上位回線の切断を人為的に発生させる障害も含めて、より現実的な災害状況を想定している点が特徴である。この他にも、停電発生、計算機室の室温異常、機器のダウン等の訓練も含まれており、これまでに2回の防災訓練を実施している。

- ・ 1回目 2014年1月5日 4:00~9:00
- ・ 2回目 2014年9月22日 21:30~24:00

1回目の訓練では、あらかじめトラブルのシナリオを作成し、順次人為的にトラブルを発生させながら状況把握・対応手順・対応内容を検証した。2回目の訓練では、何時障害が発生するかを関係者に知らせないまま実施し、障害の検知・状況の把握・対応ができるか検証した。

なお、上位回線の切断は回線業者側で操作し、高知学術情報ネットワーク連絡会参加の全組織が同時に訓練を実施した。さらに、各組織で独自の訓練も実施した。

## 4 本学独自の訓練

本学では以下の訓練1, 2, 3を独自に実施した。それらの風景を図2に示す。

### 4.1 訓練1：計算機室で停電発生

停電を監視する ping 応答専用マシンとして旧

DHCPサーバ関係機器を、商用電源に接続して稼働させ、常に死活監視(このマシンがダウンしたら停電と判断)することで停電を検知している。訓練1では、この ping 応答専用マシンの電源が予告なく切断されたときの対応を検証した。

### 4.2 訓練2：計算機室の室温異常

朝倉、物部地区の計算機室には、コア L3-SW, L2-SW, 仮想化基盤やディスク装置が設置されており、複数系統の空調機が稼働している。計算機室内のコア L3-SW の各モジュールの吸気温度情報から室内の温度を監視している。訓練2では、監視温度の閾値を下げた上で実際に空調機を停止させて対応を検証した。

### 4.3 訓練3：ある SW がダウン

監視対象機器への3つの ICMP-request に対して ICMP-reply が2つ以上返ってきたら稼働中とする死活監視を行っている。対象機器は、ネットワーク機器(344台)、無線 AP(355台)、サーバ関係(88台)となっている。訓練3では、実験用として設置した機器の電源を切断して障害を発生させ対応を検証した。



図2 ネットワーク防災訓練風景

### 4.4 訓練1~3の問題点とその改善

訓練1~3で想定したトラブルは、災害時に限らず平時にも発生する事象であり、対応マニュアルの作成、関係者への講習をこれまでも実施していた。そのため今回の訓練でもほぼ計画通りに対応できることが分かった。ただし、1回目の訓練後の反省会で、誰でもが対応できるようにするためには、対応マニュアルに作業手順をさらに詳細に記述すべきとの改善提案があり改定した。2回目は改定後の対応マニュアルを見ながら実施した。結果として、何点か作業に「抜かり」が生じたため対応作業に遅れが生じた。原因は、詳細に記述した対応マニュアルを読みながらの対応で焦りがあり読み飛ばしがあったためと考えられる。以上の結果から事前の教育用マニュアル(詳細説明)と障害発生時に参照する対応マニュアル(作業項目チェックシート付)に分けるように改良した。

## 5 上位接続回線の切断を伴う訓練

1回目の訓練では、冗長構成やマルチホームなどの機能が予定通りに動作するかを確認を含め、あらかじめ人為的に発生させる事象を把握（障害の内容やその発生順序など）した状態で行った。2回目の訓練では、1回目の問題点に対処した上で、何時どのような障害が発生するか分からない状態で行った。

### 5.1 1回目の訓練

この訓練では、学内担当者の勤務時間内に発生し管理者も在室していることを想定して実施した。

#### 5.1.1 冗長構成の確認

冗長構成となっている朝倉と物部、岡豊地区間の光ケーブルの一方を切断（回線業者側で）し、回線業者側のLAGが正常に機能するか検証した。それぞれの地区に設置されている回線業者のSW側での障害であるため、学内SW側では光ケーブル切断の検知はできないものの、LAGが機能し継続してネット利用できることが確認できた。

#### 5.1.2 マルチホームの確認

回線業者の提供するマルチホーム機能（SINETと商用）に関する訓練を実施した。回線業者側の操作で以下の順に人為的に障害を発生させた。なお、（ ）内に想定していた状況を示す（図3）。

- (1) SINET ダウン（商用に切り替わる）
- (2) 商用ダウン（学外との通信断）
- (3) 商用アップ（学外との通信再開）
- (4) SINET アップ（SINETに切り替わる）

学外接続L3-SWではBGPにより経路制御を行っており、上位回線切断によるテストをはじめて行ったが計画通り動作することが確認できた。すなわち、本学の学外監視サーバから見た高知大学への経路や特定機器への到達性から、上記すべての状況変化が把握でき必要な対応ができることが確認できた。特に(2)商用ダウン（学外通信切断）

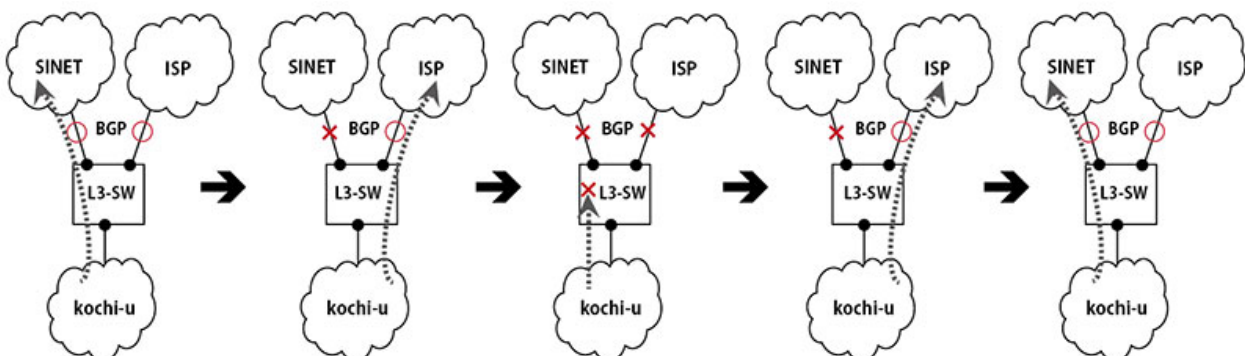


図3 訓練時の学外との接続経路推移

を検知した際、管理者から連絡を受けた学内担当者による回線業者への状況確認の連絡訓練（机上）も行った。なお、学外監視サーバでの高知大学への経路確認は、ICMP requestのTTL値を利用してTime exceeded (ICMP type=11)を返すルータのネットワークアドレスで確認できる（図4）。

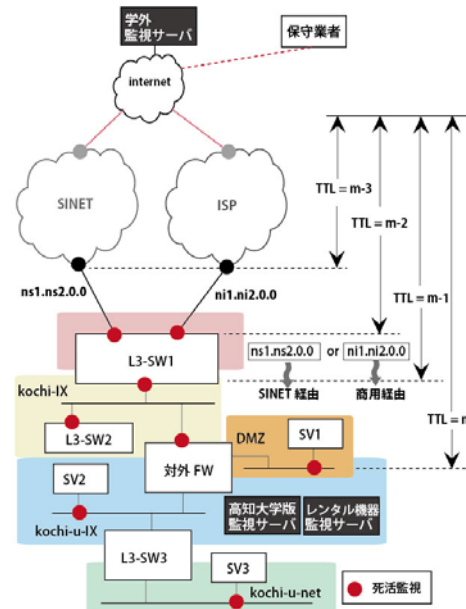


図4 ICMPのTTLを利用した経路確認

### 5.2 1回目の訓練の問題点とその改善

#### 5.2.1 障害通知メール

学外監視サーバからは、(a)高知大学への経路が切り替わった時、(b)学内の特定のポイントと通信できないあるいは復活した時に管理者の携帯にメール通知する仕組みにしている。これらのメール情報は個別に頻繁に届いたため、個別事象は把握できたが、全体状況を把握するためには監視サーバログも参照する必要があった。これを改善するため、(a)、(b)および監視サーバログから全体の状況を整理した結果をメール通知するように改善した。

## 5.2.2 学外との通信状態の表示

学内担当者が参照している監視コンソールには学外との通信状態の表示がなく、学外との通信が途絶えた情報が管理者の携帯にメールとして届くだけであった。

今回の訓練後に、監視コンソールに学外との通信状態を表示するように改良した。

## 5.2.3 障害発生時に必要な情報の準備

今回の訓練で参照したネットワーク構成情報等の資料は業務用 Web ページや業務用パソコン内に保存されており、停電の際に参照できない。緊急連絡先同様今回の訓練で参照した資料を印刷・ラミネート加工し、壁に貼り付けていつでも参照できるように改善した。

## 5.3 2 回目の訓練

2 回目の訓練は、関係者全員が不在となる夜間・早朝を想定して実施した。

### 5.3.1 マルチホームの確認

2 回目の訓練では、結果として以下の順に障害・復旧を回線業者側の操作で実施した。

- (1) SINET ダウン
- (2) 商用へ切り替わる
- (3) SINET アップ

1 回目の訓練後改善した通知メールだけで障害状況が把握できた(図5)。また、監視コンソールに学外との通信状態が表示され、一目で把握できることが確認できた。今後は学外接続にトラブルが発生した場合でも迅速な対応が可能となる。

(IGP reports) 2014/09/22 21:41:04 Transit route: DOWN Last: 10 Now: 00 [X] kochi-IX     [X] FW --- DMZ     [X] L3-SW --- kochi-u-IX     [X] kochi-u-net	(BGP reports) 2014/09/22 21:42:50 Transit route: ISP Last: 00 Now: 01 [o] kochi-IX     [o] FW --- DMZ     [o] L3-SW --- kochi-u-IX     [o] kochi-u-net	(BGP reports) 2014/09/22 22:03:51 Transit route: SINET Last: 01 Now: 10 [o] kochi-IX     [o] FW --- DMZ     [o] L3-SW --- kochi-u-IX     [o] kochi-u-net
---	--	--

図5 学外監視サーバからの通知メール

### 5.3.2 保守業者への緊急通知

学内設置監視サーバが検知したトラブルは保守業者の運用担当者にもメール通知されるが、学外接続が切断されるとその通知は届かないため障害への対応が遅れてしまう。このため2回目の訓練では、学外監視サーバからの障害通知メールを保

守業者の担当者にも送付し、状況把握の訓練に参加してもらった。今後災害が発生した際本学からの連絡前にどのような確認・対応が可能か検討してもらおうこととした。大規模災害が発生した場合、本学側からすぐに連絡できないことが予想されるためである。

## 5.4 2 回目の訓練の問題点とその改善

### 5.4.1 学外監視サーバ

現在は実験運用として、学外監視サーバは学内に設置しているため災害が発生すると機能しない可能性が高い。今後その設置場所について検討する必要がある。

### 5.4.2 学外接続が切断された際の DNS 機能

学外と通信できない場合でも DNS 利用を可能とする DNS サーバの開発が前述の SCOPE プロジェクトにて進められている。今後障害発生時にはこの DNS サーバを利用する予定である。

## 6 おわりに

ネットワーク管理者は、利用者に安定したサービスを提供することが重要なミッションであり、トラブル発生時には迅速な復旧が求められる。このため常にネットワークの状態把握に努め、机上でトラブル時対応手順を策定してきた。一方、今回の上位回線切断などかつて検証されなかった2回のトラブルへの訓練でより多くの問題点がみつき改善できた。安定運用のためにも、このような定期的に訓練を繰り返すことで各種機能の確認や障害時対応を実際に検証・改善することが重要であろう。

## 謝辞

本学ネットワークの保守業者であるコベルコシステムの運用担当者の皆様には、訓練への参加、災害時対応について貴重なコメントを頂きました。研究国際部学術情報課情報係および夜間学生スタッフの皆様には、夜間・早朝の訓練で対応手順等の検証に協力頂きました。この場を借りて感謝の意を表します。2回のネットワーク防災訓練は、SCOPE (132309010)の助成を受けて実施した。

## 参考文献

- [1] 佐々木正人, 斉藤卓也, 石黒克也, 豊永昌彦, 高知大学総合情報システムの監視と利用者動向, 学術情報処理研究, No14, pp-64-71 (2010)