商用クラウド利用時のシステム監視について

佐々木 正人，石黒 克也，佐々 浩司

高知大学学術情報基盤図書館

sasaki@kochi-u.ac.jp, ishiguro@kochi-u.ac.jp, sassa@kochi-u.ac.jp

Monitoring Method for Cloud System

Masato Sasaki, Katsuya Ishiguro, Koji Sassa

Library and Information Technology, Kochi University

概要

本学では，今後予想される地震や津波による災害時でも公式ホームページの公開など最低限のネットワークサービスを継続するため，可能なシステムから順次商用クラウドに移行している．商用クラウド利用時は，それぞれのサーバの監視だけでなく本学との間のネットワークの監視も必要となるが，クラウドサービスで提供されるチェック機能では十分ではない．そのため，商用クラウド利用時に必要な監視機能を検討・開発し，それらの機能を付け加えた運用中の監視システムについて報告する．

1　はじめに

本学では，これまで学内仮想基盤上または専用サーバで学内情報システムを稼働してきたが，可能な学内情報システムから順次商用クラウドへ移行している．次期システム更新時には多くの教育研究用のサーバ等を移行する予定である．さらに，地震や津波による災害時でも本学の公式WWWサーバや最低限のネットワークサービスが継続できるよう，各キャンパスのコアL3-SWより上位を学外（県外等）のDC等に設置する構成も検討中である．また同時に，このような構成においてシステム全体の状況を把握し，障害やトラブル，セキュリティ上のリスクを検知し迅速かつ適切に対処するために必要となるシステム監視機能や体制についても検討中である（図1参照）．

本学で開発した監視システム[1]では，(1)学内ネットワーク，(2)その上で動作する情報システム，(3) 学外接続システムをその監視対象としてきた．しかし，商用クラウドを利用する際は，L2-VPNやL3-VPNなどで接続することになるため，学外との接続監視(IP 到達性や BGP による経路監視)だけでは不十分である．さらに，DC 等で学外接続する場合（学内 LAN とは回線接続）には，接続回線や学内 LAN 側接続機器の障害時に学内LAN側の状況が把握できる機能も必要となる．

現在，商用クラウドで稼働中のシステム監視に必要となる機能を，本学の監視システムに組み込み運用している．ここではその取り組みについて報告する．

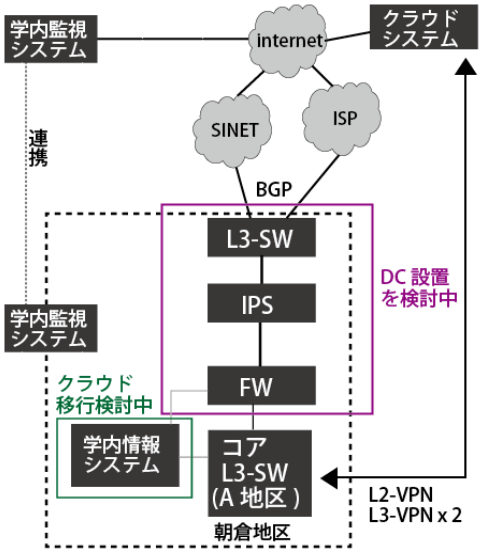

図1 商用クラウドを利用したシステム概要

2　商用クラウドを利用したシステム

2.1 基本方針

商用クラウドを利用する際の基本方針は以下のとおりである．

①クラウド上のシステムは学内専用システムとする(インターネットからのアクセスは認めない)

②暗号化通信できないもの，学内設置サーバとクラウド上のサーバ間でのデータ通信が必要なもの，システム管理操作は VPN ルータ経由で行う．
③クラウドサービス利用料を考慮し，クラウド上のホストは必要な時間帯でのみ稼働させる．またホストの死活監視は稼働時間に応じて実施する．
④アプリケーションの保守については原則業者に依頼する（トラブル時はリモートメンテ）．

なお，現システムでは，認証システムやメールサーバ等ネットワークサービス機能などは学内仮想基盤上で動作している．

2.2 クラウドシステムと接続方式

現在，AWS(Amazon Web Services)上に 2 つの VPC(Virtual Private Cloud)を設定して利用している．VPC#1 で 16 台, VPC#2 で 4 台のサーバが稼動している．すべてプライベートサブネットとして構成し, 本学と VPC#1 間は L2-VPN(SINET)と L3-VPN，VPC#2 間は L3-VPN で接続している．L3-VPN では専用ルータにより接続し，2 つの tunnel で論理的な冗長構成としている．さらに，L2-VPN にトラブルが発生した場合，static route により VPN ルータへ迂回している（図 2）．

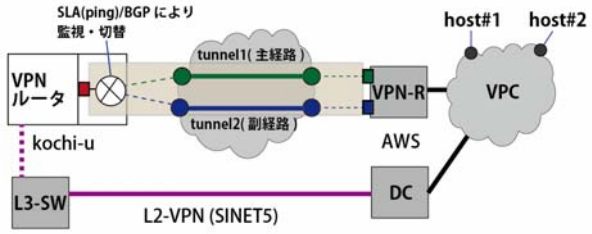

図 2　商用クラウドとの接続

3　商用クラウドとの接続状態の監視

3.1 当初の監視からの教訓

クラウドに移行した当初は，各ホストの死活監視のみを実施した．当初頻繁に VPN ルータの通信トラブルによる通信断が発生したが，死活監視機能による「ホストがダウン」の通知から VPN ルータトラブルの発見が遅れた．このことから，学外との通信状態(IP 到達性，BGP の状態), VPN ルータ間の通信状態の監視機能を追加した．

3.2 L3 監視

本学では SINET5 と ISP から BGP によりマルチホーミングを実現し，通常 SINET5 により通信している．このため，学内から学外へ，学外から学内への IP 到達性のチェックはもちろん，どちらの経路で通信しているか双方向から監視している．BGP 経路は，学外監視サーバから学内 ping マシンに向けて，到達に必要な TTL より小さな TTL で PING を行い TTL exceeded を返すルータのアドレスから経路を判断している．また学内からの経路の状態は，学外接続 L3-SW の IP テーブルから判断している．

3.3 L3-VPN 監視

クラウドの VPC#1，VPC#2 ネットワークへは，VPN ルータで 2 つの tunnel（論理パス）で冗長構成としているため，それぞれの tunnel が通信可能であるかどうか監視している．なお，VPN ルータでは SLA(PING)と BGP により 2 つの tunnel のうち動作側を選択して通信している．

3.4 L2-VPN 監視

クラウドの VPC#1 では，SINET5 L2-VPN でも接続しており，学内利用者用サービスは通常この経路を使用している．VPN ルータでの接続は，主にシステムの保守・管理業務で使用しているが，L2-VPN に障害が発生した場合，static route により自動的に VPN ルータ経由に切り替える．このため，L2-VPN 通信状態をチェックしどちらの経路で接続しているかを監視している．

3.5 VPC#1,#2 上のホストの死活監視

これまでは，サーバを 24 時間 365 日稼働してきたが，従量制のクラウドサービスでは，1 日のサービス時間(表 1)を決めて運用している．このため起動・停止時刻(曜日指定も含む)を考慮した死活監視を実施している．毎日起動・停止を行っているため，正常に起動しているかの監視は欠かせない．

ホスト名	稼動時刻
Host1	毎日 6:10～翌日 3:05
Host2	月～金　8:40～19:00
·····	·····

表 1　商用クラウドとの接続

3.6 通信量推移グラフの表示

監視コンソールには，クラウドシステムとの通信量の推移グラフを表示し，通信状況が常に

確認できるようにしている．また，定時のサーバ間通信やバックアップ処理が実施されているかも確認できる．さらに，学外接続の経路，L2-VPN, L3-VPN の経路も表示している(図 3)．

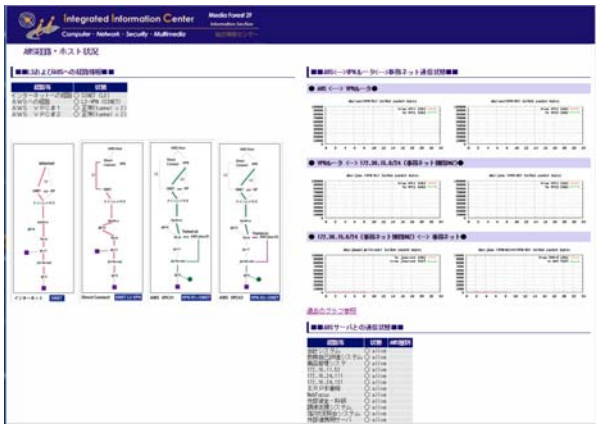

図 3　商用クラウドとの接続状態（監視画面）

4 トラブル検知時の対応

4.1 ネットワーク管理者とクラウド管理者

クラウド上では，現在会計システム等日々の活動に不可欠なシステムが稼働している．安定的にサービスを提供するためには，トラブルを早期に検知し，迅速に対処する必要がある．このため，トラブルを検知した際は，クラウド管理者の携帯にメール通知(図 4．ただし，7:00 から 21:00)し，必要に応じて対応している．

差出人：
件名：[SOC] (Line trouble reports)

===L3/AWS トラブル通知 ====
学内との通信：○ ==> ×
ＢＧＰ経路：SINET ==> 無し
Ｌ２−ＶＰＮ: ○ ==> ×
ＶＰＮ−Ｒ１: ○ ==> ×
ＶＰＮ−Ｒ２: ○ ==> ×

===L3/AWS 現在の状況 ====
to kochi-u ... NG
BGP: none
AWS L2-VPN: unreachable ... NG
AWS VPC#1: unreachable ... NG
AWS VPC#2: unreachable ... NG

差出人：
件名：[SOC] (Line trouble reports)

===L3/AWS トラブル通知 ====
学内との通信：○ ... ○
ＢＧＰ経路：SINET ==> ISP
Ｌ２−ＶＰＮ: × ==> ○
ＶＰＮ−Ｒ１: × ==> ○
ＶＰＮ−Ｒ２: × ==> ○

===L3/AWS 現在の状況 ====
to kochi-u ... OK
BGP: ISP
AWS L2-VPN: VPN-R1 ... OK
AWS VPC#1: 2-tunnel ... OK
AWS VPC#2: 2-tunnel ... OK

図 4　トラブル検知時に送付されるメール例

また，通信は可能であるが L3 経路が ISP に切り替わったり，tunnel の一方が切断された場合など状況が変化する度にネットワーク管理者にメール通知している．ネットワーク管理者は，必要に応じてクラウド管理者に連絡して対処している．

4.2 通知するトラブル

現在クラウドシステムとの接続に利用している 2 台の VPN ルータでは，2 つの tunnel により冗長構成となっており，一方の tunnel がトラブルを起こしても通信断とはならない．このため，携帯への緊急障害通知は通信断時のみとし，一方の tunnel 断の場合は監視コンソールへの表示および電子メールでの通知としている．

4.3 学外接続でのトラブル

学外接続においてトラブルが発生するとクラウド接続のための L3-VPN はもちろん，一般利用者のネットワーク利用にも支障が出る．このため，IP 到達性や BGP 経路の監視，トラブル検知時には緊急通知により迅速な復旧を目指している．もちろん，学外接続にトラブルが発生すると，VPN 接続も不可となり緊急通知を送付するが，その際には直接の原因は学外接続であることを明示し，学外接続に関して調査することを促している．現在は，ネットワーク利用に必要な DNS サーバなどはすべて学内ネットワーク上にあるが，今後クラウドシステムへの移設も考えており，クラウドとの通信状態の監視と迅速なトラブル対応が必要となる．

4.4 トラブル事例から

実際に発生したトラブル事例を紹介する．

[事例 1] DNS サーバの不調により，名前参照ができず通信不可の緊急通知が送付された．この場合，名前参照できないことが直接の原因であったが，通信不可（死活監視）の警告により DNS サーバでの問題発見が遅れた．

[事例 2] 物部地区周辺で落雷があり停電となり，復電前に物部地区全体が停止した．キャンパス間回線のトラブルや，物部地区コア L3-SW の障害などが考えられるが．停電が発生していることを検知していたため，早期に原因が停電であることが特定できた．

[事例 3] BGP ルータに一気に経路情報が流れて来たためパケットロスを起こしたが，死活監視で検

知できない程度のものであったため，このルータでパケットロスを起こしていることが判明するまで時間がかかってしまった．

事例１，３から，トラブルを検知し緊急通知する際は，計算機室の通電状態・室温，DNS サーバの状態や主要機器でのパケットロスの有無なども参照できるように改善している．また，携帯からクラウドシステムの最新情報が参照できるページも作成した（図 5）．

図 5　管理者用携帯 Web ページ

4.5 機能チェックと訓練

必要となる新しい機能を追加する度に，人為的に障害を発生させ，その検知や通知が正常に動作するかなど，個別機能チェックを行っている．本学では，2014 年度から毎年ネットワーク防災訓練[2]を実施している．この訓練では，停電発生や計算機室，温度異常，ネットワーク機器の障害などを人為的に発生させ，異常を検知・通知するかどうか，あらかじめ決められている手順で対応ができるかどうかを実際に行い不具合を改善する．さらに，県内の大学・高専と共同で上位(SINET5 など)接続を実際に切断しての訓練も同時に行っている．今年度は，この訓練に加えクラウドシステムに関する障害訓練を実施した．主な訓練を以下に示す．

なお今回は，人為的に障害を発生させているため，その復旧訓練は実施していない．

(1) VPN ルータの tunnel 切断

2 つの tunnel を順次 shutdown し，両方が shutdown し通信断となると管理者に緊急メール通知が届くことの確認，その通知から状況を判断する訓練を実施した．

(2) 上位 L3 接続の障害

上位 ISP にて SINET 接続切断による BGP 経路切り替わりの訓練では，インターネット接続断に伴う VPN 通信断の通知から原因の特定する訓練を実施した．

(3) L2-VPN の障害

SINET5 回線切断時に，設定どおり VPN ルータに迂回するか確認した．その後 VPN ルータのインタフェースを shutdown し，異常通知の確認，状況判断の訓練を実施した．

なお，今年度の訓練では，ISP 側 BGP 設定の不具合から予想外のトラブルが発生したため，本番さながらの訓練となった．この復旧作業において，外部監視サーバからの DNS 参照チェックや本学への経路監視結果の情報が有益であった．

5 まとめ

これまでの学内で閉じたネットワーク・コンピュータシステムの管理運用から，商用クラウドや外部 DC に機能を移した場合に必要となるシステム監視機能について，商用クラウドに移行したシステムの運用を通じて検討している．分散配置されたシステム全体を管理するためには，一元的な管理が必要となる．今後さらに運用を通じて必要な監視機能を洗い出し，アウトソーシングも含め管理運用体制について検討する．

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)

[2] 佐々木正人，豊永昌彦, 回線切断を含むネットワーク防災訓練に関する報告, 大学 ICT 推進協議会 2014 年度年次大会（宮城県仙台市）, 2014