Vol.2017-IOT-36 No.38
2017/3/4

情報系学科における教育研究用情報システムの運用管理に関する取り組み

田中 大海[1,a)]　城戸 翔大[1,b)]　長田 智和[1,c)]　谷口 祐治[1,d)]

概要：琉球大学工学部情報工学科では，システム管理チームと呼ばれる有志の学生が，教員の指導の下で教育情報システムの設計 · 構築を行い，運用している．現在運用しているシステムは平成 27 年 10 月に初期構築されたものである．本システムは運用開始から 1 年が経過し，システム管理チームはさまざまなトラブル対応や運用の改善を行ってきた．本発表では，本学科における学生による教育情報システムの運用管理に関する取り組みを報告する．

1. はじめに

琉球大学情報工学科で利用されているサービス（Web，DHCP，DNS，VM 貸出サービス，etc.）は，平成 25 年に発足されたシステム管理チームと呼ばれる組織によって構築 · 運営 · 管理が行われている [1]．このチームはシステム管理者を目指す学生が，教員や先輩の指導の下で作業を行うことで，実践的なシステムの運用管理のスキルを習得することを目的としている．現在，本チームが運用管理しているサービスは，平成 27 年 10 月に初期構築 [2] [3] されたもので，運用開始から 1 年が経過した．本発表では，1 年間運用した学科サービスの問題点を改善するための取り組みを報告する．

2. 現行システムの概要

2.1 物理構成

現行システムでは表 1 のスペックの 1U サーバを 4 台，表 2 のスペックの SAN 用ストレージを 2 台，表 3 のスペックの汎用ストレージを 2 台導入している．

CPU	Intel Xeon E5-2699 v3 (2.30GHz / 18 コア)
CPU のユニット数	2
メモリ	768GB (32GB * 24)
実効容量	557GB(279GB*3)

表 1　物理サーバ

HDD	SAS 1.2TB * 24
回転数	15000rpm
RAID	6
実効容量	19.7TB

表 2　SAN 用ストレージ

HDD	SAS 4.0TB * 24
回転数	7200rpm
RAID	6
実効容量	68.5TB

表 3　汎用ストレージ

2.2 仮想化環境

現行システムでは，オープンソースソフトウェアの KVM を採用している．メンテナンス時に VM が止まっている時間を無くすため，稼働中の VM を別ホストに稼働したまま移動するライブマイグレーションが使用できるようにしたい．そのため Filesystem は，複数のノードからのアクセスに対して整合性のある読み書きが可能であり，かつ，iSCSI に対応した RedHat 標準のクラスタファイルシステムである GFS2 を採用した．共有ストレージへのアクセス制御には，RedHat 標準のロック機構である DLM を使用し，クラスタノード間における情報の同期や，死活管理には Pacemaker を使用している．また，そのクラスタ基盤ソフトウェアには Corosync を使用している．図 1 に構成図を示す．

本学科の提供するサービスはこの仮想化環境上で構築されており，KVM Host1 と KVM Host2 上の VM に DNS や RADIUS，LDAP を一つづつ配置することでどちらかのマシンがダウンしてもサービスが停止しないように冗長化している．また他にも Web サーバーやログイン用 Shell サー

[1] 琉球大学
IPSJ, Chiyoda, Tokyo 101–0062, Japan
[a)] tanaka@ns.ie.u-ryukyu.ac.jp
[b)] chinon@ns.ie.u-ryukyu.ac.jp
[c)] nagayan@ie.u-ryukyu.ac.jp
[d)] taniguchi @ cc.u-ryukyu.ac.jp

© 2017 Information Processing Society of Japan

バー，貸出 VM サービスのための VM もこれらの Host 上で稼働している．KVM Host3 は検証用，機材メンテナンス時のライブマイグレーション用，KVM Host4 は授業での実験用に使用している．

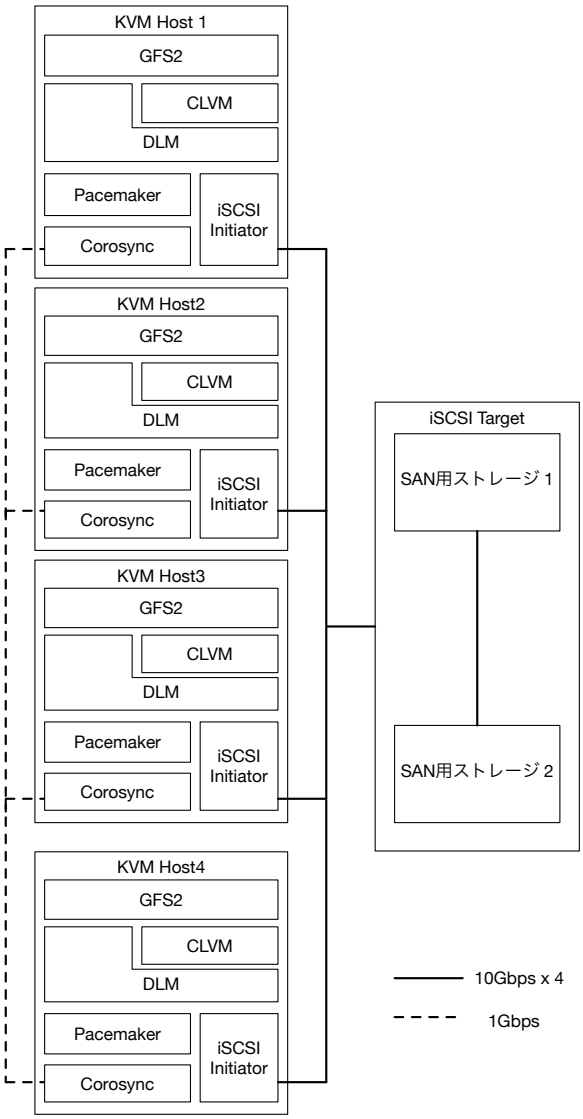

図 1 IP-SAN の構成図

2.3 IP 管理方法

本学科では，現行システムからグローバル IP アドレスとプライベート IP アドレスの使い分けを行っている．以下では使い分けと割り当てまでの手続きについて説明する．

2.3.1 グローバル IP アドレス

グローバル IP アドレスは外部公開が必要なホストにのみ割り当てている．割り当てまでの手順としては，グローバル IP アドレスを割り当てたいホストの管理者から連絡を受けて，本管理チームのメンバーがこのホストにアクセスし，セキュリティ監査を実地している．監査の例を以下に示す．

- 不必要なサービスが稼働していないか?
- アクセス元アドレスの制限やパスワードログインの禁止などのアクセス制限が行われているか
- 不要なユーザは存在しないか
- 必要なポートだけ開放してあるか
- 使用しているアプリケーションや OS の更新を行っているか

これらの監査をクリアしたホストに固定でグローバル IP アドレスを割り当て，外部からの通信ができるように設定を行っている．

2.3.2 プライベート IP アドレス

外部公開する必要のないホストは全てプライベート IP を割り当てている．部外者が学科ネットワークに不正に接続できないようにするために 802.1x 認証を行っており，ネットワーク接続をするためには，LDAP のアカウント登録や MACadress の登録が必要としている．

上記の通り接続認証を行うため，不審な通信を行っているユーザーがいる際に，誰の端末がその通信を行っているかを特定しやすくなっている．

2.4 さくらのクラウドの利用

2.4.1 基幹システム用

基幹システム用に VM を 8 台契約している．この VM は本学科のオンプレミス環境と連携しており，外部バックアップや負荷分散に活用している．また，さくらの専用サーバとストレージサーバとして物理マシンも 1 台契約しており，さくらのデータセンターの内部ネットワークに設置することで NAS や iSCSI としてマウントして利用することもできようになっている．以下の表 4，表 5 にそれぞれのスペックを示す．

CPU	4 コア
メモリ	8GB
HDD	20GB

表 4 基幹 VM

CPU	6 コア*2
メモリ	16
実効容量	22TB(4TB*12)

表 5 ストレージサーバー

2.4.2 学生演習用

学生演習用のリソースとして，CPU100 コア，メモリ 100GB，HDD20GB*100 の契約しており，現在はリソースを分割 100VM を用意して活用している．学生は先進的な技術を学ぶために，IPv6 を利用して本 VM にアクセスし，演習を行う．以下の表 6 に学生演習用 VM のスペックを示す．

© 2017 Information Processing Society of Japan

CPU	1 コア
メモリ	1GB
HDD	20GB

表 6　学生演習用 VM

3. 現行システム運用開始からの取り組み

3.1 さくらのクラウドの運用について

3.1.1 基幹システムの冗長化

琉球大学は沖縄県にあり，台風が接近する機会が多く，その度にサーバ室がある工学部棟は停電している．他にも本大学では電源設備の計画停電などもあり，オンプレミス環境の停止が多々発生する．そこで，停電などの障害発生時でも本学科公式ホームページや授業情報などの告知ページ，学生や教員のブログを利用できるように，以下の作業を行うことでサービスの冗長化を行った．

- DNS のターシャリを設置
- WordPress の冗長化
- LDAP サーバの冗長化

3.1.2 VM 管理の簡略化

現在，さくらのクラウドと本学科が契約している VM は全てシステム管理チームのアカウントで管理されている．学生がさくらのクラウド上の VM を用いて演習を行う際は，本管理チームに申請を行い，アクセストークンとアクセスシークレットトークンも入手し，その情報を用いて管理画面にアクセスを行う図 2.

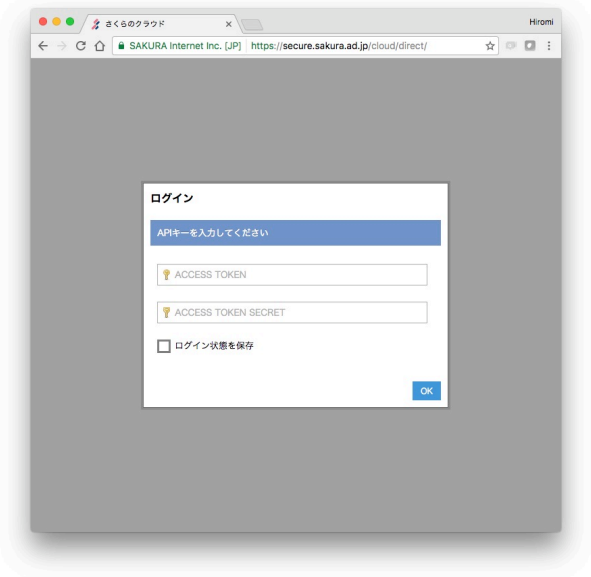

図 2　さくらの VM 管理ページのログイン画面

しかし，1 対のトークンでログインした画面では 1 つの VM の操作しか行えない．よって，複数台の VM を借りて並列処理の実験などを行う学生は，必要な VM の数だけログインして電源を入れなければならない．また，VM 返却時にはさくらのクラウドに連絡を入れ，トークンを再発行してもらわなければならないという問題もある．それら手間を省くために，学科の管理する LDAP のユーザーに貸出する VM のトークンを紐付け，ユーザーは紐付けられた VM のトークンを用いて VM の操作できる Web アプリケーションを，さくらの API を用いて作成した．

3.2 インシデント対応について

以下に，策定したインシデント対策とインシデント発生時の対応方法について記述する．

3.2.1 インシデント対策

2.3.1 節で述べたように，本学科では外部公開が必要なサーバに対し監査を行った上でグローバルアドレスを割り当てている．しかし，グローバルアドレスを割り当てた後の操作は本チームはこれまで関与しておらず，度々グローバルアドレスを持つサーバの脆弱性が報告された．そこで，特定サーバから ssh アクセスし，事前に申請された利用目的や初期構築の時の監査の内容と差異の有無を自動でチェックする仕組みを，Ansible と cron を用いて定期的に対象サーバにアクセスし，監査用スクリプトを実行することで，監査を行う仕組みを策定した．監査する項目を以下に示す．

- 2.3.1 で記述した項目
- 申告した端末とは別端末を接続し利用していないか
- 申請内容と異なるサービスを開始していないか

今回使用する Ansible は，hosts ファイルに記述してあるサーバに対して ssh でアクセスし，コマンドを実行できる構成管理ツールである．コマンドを実行するサーバの OS によって実行するアクションを指定することができるため，監査対象のサーバが増えても hosts ファイルに記述を追加するだけであり，容易に管理ができる．

3.2.2 インシデント発生時の対応

発生したインシデントの種類によってチェック方法は変わると思われるが，どのようなインシデントが発生しても取るであろう対応順序を以下に示す．

(1) 物理的なネットワークから切断．(不可能な場合はスイッチから切断)
(2) 証拠保全のためのホストを回収．(調査や検証が終了するまで返却は不可)
(3) ディスクをコピーする．
(4) 外部ネットワークと干渉しないように専用のネットワーク帯で起動．
(5) 2.3.1 節で述べた項目やアクセス状況，脆弱性を指摘されたファイルを確認する．
(6) 他に問題のあるホストが学科内に存在しないかを確認するために，本学科のグローバル IP をもつ全ホストに対して，5 と同様のチェックを行う．

© 2017 Information Processing Society of Japan

3.3 次期メンバーの技術力向上の取り組み

3.3.1 wiki 構築

現行システムの構築を行った学生は 2016 年度で卒業してしまう．そのため，構築及び運用管理で必要とする知識を引く継ぐために，後輩の育成と作業ログの管理が重要となる．そこで，新しくさくらのクラウド上に wiki を構築した．本チームは Redmine というプロジェクト管理ツールを用いて作業の記録を残していたが，オンプレミス環境で障害が発生したときに参照できないため，今回はクラウド上で wiki を構築することになった．本 wiki では

- 現行システムの構成
- 本チームが提供するサービス
- 障害対応，こんな時どうする Q&A
- 後輩育成用勉強会

について記述してある．

3.3.2 技術者育成プロジェクトへの参加

本チームの次期主要メンバーは，沖縄オープンラボラトリ[*1]にて開催されている, SDN やクラウド技術を修得した人材になることを目的としたプロジェクト[*2]に参加した．SDN やクラウド技術に関わり産業界で活躍しているエンジニアや ICT に関連する学術機関の研究者などの最先端の動向に詳しい人々からの指導を受けながら，サービス開発を行った．以下に本プロジェクトでの活動を示す．

- KVM の操作や VM に対して任意のコマンドを実行できる Web アプリケーションの開発
- 起動するだけで OS のインストールから上記 Web アプリケーションが動く環境を自動で構築する仕組みの開発
- 上記 Web アプリケーションで実行できるコマンドを簡単に組み込むことができる仕組みの開発

4. まとめ

4.1 総括

本研究では，現行システムの運用 · 管理を行い，様々なトラブル対応や運用方法の検討や運用の改善，次期メンバーの技術力向上のための取り組みについて報告した．

4.2 今後の課題

- 日々増える外部からの脅威対策と内部からの不正通信の削減のために，UTM アプライアンス周辺のチューニングを行う．
- オンプレミス環境上で貸出している VM のスペック変更は，本管理チームのメンバーが KVM ホストとなるサーバにアクセスし，VM を操作するコマンドを実行し変更を行っている．3.3.2 節で触れた知識を活かし，現行システムで VM の貸出，電源操作を行っている Web アプリケーションを改良し，管理者はスペックをブラウザ上から変更できるようにし，管理を簡単化したい．
- 3.2.1 節で記述したグローバル IP アドレスを持つホストに対する定期監査を行う仕組みの構築を行う．
- 稼働から 1 年経過したが，今回用いた機材は前回の機材に比べ故障回数が多い．サーバのメモリ故障による突発的なシステムダウンや backup 用の NAS の故障によるデータの消失 · マウント先のシステムのダウンなどのトラブルが発生している．今後，同様の問題が発生する可能性を想定し，対策 · 対応方法を考えてたい．
- 2017 年度から琉球大学の工学部情報工学科は工学科知能情報コースに変更となる．それに伴い必要となる作業をまとめていきたい．

今後はこれらの課題に取り組み，本学科のサービスを更に安定化し，管理の容易性を向上していきたい．

[*1] www.okinawaopenlabs.org
[*2] www.okinawaopenlabs.org/specialist/

参考文献

[1] 金城篤史，城間政司，比嘉哲也，長田智和，玉城史朗，谷口祐治：“情報工学系学科における教育用計算機システムの自主構築に関する取組み”，教育システム情報学会論文誌，Vol.26，No.1，pp.79-88，2009/1
[2] 安里悠矢，城間政司，長田智和，谷口祐治：“琉球大学情報工学科おける教育研究用情報システムの更新に関する研究”，研究報告インターネットと運用技術（IOT），Vol.31，No12，pp.1-6 2015/09.
[3] 城戸翔大，安里悠矢，城間政司，長田智和，谷口祐治：“情報系学科における教育情報システムの構築及び運用管理に関する取り組み”, 研究報告インターネットと運用技術（IOT），Vol.32,No2，pp.1-8，2016/3

© 2017 Information Processing Society of Japan