Vol.2015-IOT-31 No.12
Vol.2015-SPT-15 No.12
2015/9/26

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

安里 悠矢[,a)] 城間 政司[,b)] 長田 智和[,c)] 谷口 祐治[,d)]

概要：琉球大学情報工学科では，教員の指導の下で学生により教育研究用情報システムの運用管理が行われてきた．同学科では 4 年ごとに教育研究用情報システムの更新を行っており，2015 年 9 月に同システムの更新が予定されている．本発表では，現行システムを紹介し，現状の課題点を踏まえて，新情報システムの設計・構築内容について報告する．新システムでは，特にセキュリティの強化やクラウドサービスの利用を積極的に行った．

1. はじめに

琉球大学工学部情報工学科には，約 300 名の学生と 20 人の教職員が所属している．同学科で運用される教育研究用情報システムは，学生及び教職員に日々絶え間なく利用されている．

ここで，同システムの運用管理は，平成 24 年度まで演習科目の 1 テーマとして行われてきた [1]．しかし，システムの高度化に伴い，演習科目の枠組みで行うことが困難となった．このため，平成 25 年度に学生と教職員らの有志による「システム管理チーム」が発足し，以降，同チームによってシステムの運用管理が行われることとなった．同チームは，実践的なシステム運用管理のスキルの修得を目標としている．また，最新の技術の導入とシステムの安定運用の大きく 2 つの役割を担っている．

一方，稼働開始から 4 年半が経過した現行システムでは，ユーザビリティ，信頼性，保守性，セキュリティにおいて多くの問題を抱えている．また，沖縄は台風の影響により停電に見舞われることが多く，システム運用面において課題となっていた．

同学科では，教育研究用情報システムの更新を 4 年ごとに実施しており，2015 年 9 月に同システムの更新が実施される予定である．今回は，上記で挙げた現行システムの問題点を改善するための新システムの設計及び構築内容について報告する．

†1 現在，琉球大学
Presently with ,UNIVERSITY OF THE RYUKYUS
a) yuya@ns.ie.u-ryukyu.ac.jp
b) shiroma@ns.ie.u-ryukyu.ac.jp
c) nagayan@ie.u-ryukyu.ac.jp
d) taniguchi@cc.u-ryukyu.ac.jp

2. 現行の教育情報システムの概要

2.1 ネットワークシステム

全学のネットワークを取りまとめる総合情報処理センターと学科内のメインスイッチ間を 10Gbps × 2 で接続し，各研究室や学生自習室に配置されたフロアスイッチやルームスイッチとメインスイッチ間は 1Gbps × 2 で接続されている（図 1）．また，スイッチ間の伝送経路の二重化を行っている．これにより，一方の伝送経路に障害が発生しても通信を可能にしている．

講義室や学生自習室の入室管理には Edy を利用した非接触型認証装置を導入している．講義室や学生自習室には複数の実験機材が設置されており，学科外のユーザーによる不正利用や持ち出しを阻止するために認証を行っている．

無線 LAN-AP は，情報工学科が利用する建物の各フロアに配備している．無線 LAN を利用するには，同学科が提供する LDAP で管理されたユーザーアカウントを用いて 802.1X 認証を行う．また，ユーザーへの利便性を考慮し，総合情報処理センターで配布しているユーザーアカウントを学科アカウントとして紐付けを行っている．さらに，ユーザーがどの IP アドレスを利用しているかを特定することを容易にするため，ユーザーアカウントとの紐付けも行っている．これにより一つのユーザーアカウントを用いることで全学のネットワークと同学科が提供するネットワークの両方を利用することができる．

ブレードサーバーには仮想化技術を用いたシステムを導入している．ストレージは VM イメージを配置するため，ブレードサーバーとストレージ間を 8Gbps の FC-SAN で構成している．これにより，VM イメージの読み出しにか

Vol.2015-IOT-31 No.12
Vol.2015-SPT-15 No.12
2015/9/26

かるオーバーヘッドを小さくしている．

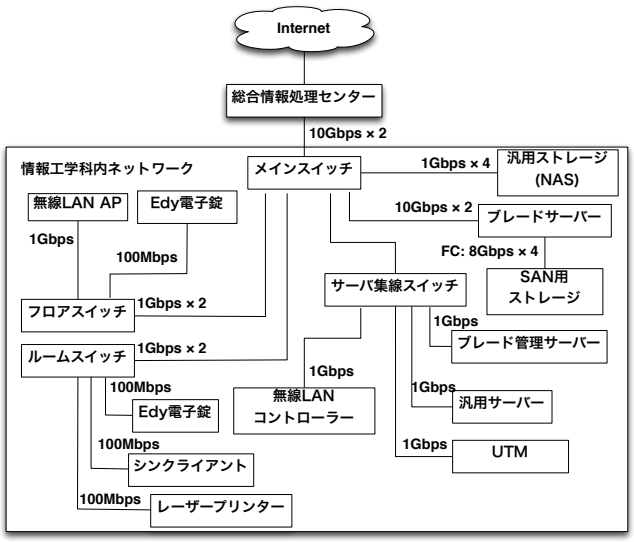

図 1 ネットワークシステム構成図

2.2 シンクライアント

シンクライアントは，ブレードサーバー上で動作している VM を VNC で経由でアクセスして利用する．認証には同学科が提供するユーザーアカウントを用いている．現行のシステムでは，Windows と CentOS の利用が可能である．シンクライアントを利用する利点として，ユーザー自身が端末を所持せずとも，アカウントの認証を行えば，一つの演習環境として利用可能であることが挙げられる．

2.3 仮想化技術を用いたサーバーシステム

2.3.1 物理構成

現行システムのオンプレミス環境は，表 1，2，3 となっている．

表 1 物理サーバー

CPU	Intel Xeon X5650 (2.67GHz / 6 コア) x 2
メモリ	96 GB
台数	16

表 2 SAN 用ストレージ

HDD	SAS 600GB × 45　RAID6 構成
実効容量	25TB
台数	1

表 3 汎用ストレージ

HDD	SAS 1.0TB RAID6 構成
実効容量	13TB
台数	2

2.3.2 ソフトウェア構成

オンプレミス環境には Hypervisor として VMWare ESXi を導入し，FileSystem には VMWare 標準のクラスタファイルシステムである VMFS を用いた．また，VMWare ESXi を導入した複数のサーバーを管理するため VMware vCenter Server を用いた．VMWare を導入する利点として，ホスト間における VM のライブマイグレーションが可能であることが挙げられる，これにより VM の動作を停止せずに別のホストに VM を移行させることで，無停止でメンテナンスを行うことが可能である．

2.3.3 VM 貸し出しサービス

学生の講義演習や研究用途として VM 貸し出しサービスの需要があり，学科独自で提供している Web ベースの VM 管理コンソールを用いて VM の貸し出しサービスを行っている（図 2）．

VM の貸し出しを希望する学生は，システム管理者へメールを送信して VM 使用依頼を行う．システム管理者が申請を受諾し，管理者用コンソールから利用希望者に対して作成権限の付与を行う．その後，利用者は VM 管理コンソールから VM を作成することができる（図 3）．VM 作成と同時に，DHCP による IP アドレスの配布や DNS の自動登録機能も備わっている．

VM 管理コンソールでは，作成した VM の電源を操作，スナップショットやクローンの作成が可能である．VM 貸し出しサービスの需要は年々高まっており，現在約 300VM が稼働している．

図 2 VM 貸し出しサービスの VM 作成ページ

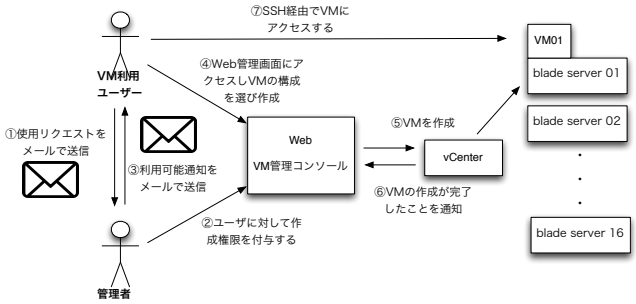

図 3 VM 貸し出しサービスのワークフロー

Vol.2015-IOT-31 No.12
Vol.2015-SPT-15 No.12
2015/9/26

2.4 IP アドレス DNS 管理システム

同学科では，端末やサーバーに IP アドレスを割り当てる場合は，システム管理者への申請が必要である．また，割当てられる IP アドレスは，全て DHCP サーバーによる自動割り当てを行っている．さらに，サーバーを運用するためには，DNS への登録が必要である．そのため，DHCP と DNS の連携システムを作成し，端末やサーバーの MAC アドレスを元に割当てられる IP アドレスと DNS への紐付けを行っている．

3. 現行の教育情報システムへの課題

3.1 ネットワークシステムの課題

現行のネットワークシステムの大きな課題として，許可無く設置された無線 LAN-AP による電波干渉が発生している．具体的には，無線 LAN-AP と物理的に離れた研究室や学生自習室では，通信が途絶してしまうため，学科内のネットワークシステムを利用するユーザーが独自で無線 LAN-AP を設置しているためである．これにより，学科で提供している 2.4GHz 無線 LAN に干渉する問題が発生した．現在，一時的な措置として有線 LAN への利用を促すか，無線 LAN-AP のチャネル変更や出力を調整して運用してもらうなどの協力を呼びかけている．

3.2 VM 貸し出しサービスの課題

VM 貸し出しサービスは，多くの学生や教員に利用されているが，運用時に幾つかの課題が出てきた．VM 貸し出しサービスの需要が増加しすぎたために VM イメージを配置している高速ストレージが容量不足になり，稼働中の VM が全て停止する事例があった．また，VM 作成時に Web コンソールから CPU やメモリなどリソースの構成を選択する必要があるが，ユーザーや利用用途ごとにリソースの制約を設けていなかった．そのため，数名のユーザーが必要以上に多くのリソースを取得してしまい，常にメモリ不足に悩まされていたこともあった． 他にも，VM 作成時に DNS への登録を行うが，Web 側の入力チェックが甘かったため，データベースに不正な文字列が登録されてしまい DNS が停止することがあった． VM へのアクセスには SSH を利用し，事前に作成されたユーザー ID とパスワードを使用する．パスワード認証から公開鍵認証に切り替えるユーザーも多く，公開鍵の設定を誤ってしまうとユーザへの救済措置が無いため，システム管理チームに修正を依頼するしか無かった．

3.3 自然災害に対する課題

沖縄は台風の影響により停電に見舞われることが多く，システム運用面において課題となっていた．学科公式 Web サイトや休講通知を行うための学内で運用する掲示板が閲覧できず不便をかけることがあった．VM 貸し出しサービスにおいても停電時に演習用として利用している VM へアクセスできなくなるため講義を受講する学生に不便をかけた．

3.4 セキュリティの課題

本学科では，ネットワークに接続されている端末やサーバーに全てグローバル IP アドレスを付与していたため，常に学外からの標的にされた．特に SSH へのブルートフォース攻撃が多く，脆弱なパスワードを設定していた VM が標的にされた．また，学科 Web サイトの PHP で作成されたページにおいてクロスサイトスクリプティングによる脆弱性を悪用された．

3.5 監視体制への課題

3.2 で述べたようにストレージの利用率の監視業務が行われておらず，また，DNS や Web サーバーなどのサービスへの監視体制が適切に整備されていなかった．そのため障害が発生してから管理者が気づくまで時間を要し，迅速な復旧が行われなかったことが多かった．

4. 新教育情報システムの概要

現行の教育研究用情報システムの問題点を踏まえ，新システムの設計・構築を行った．

4.1 ネットワークシステム

現行システムで特に改善要求が強かった無線 LAN-AP の改善を行った．3.1 で述べたように無線 LAN-AP と通信できない部屋が存在し，許可無く設置された無線 LAN-AP をユーザー独自に設置している部屋が存在する．この問題に対し，無線 LAN-AP の増設と 802.11ac への対応を行った．電波干渉を避けるため，今後，許可無く設置された無線 LAN-AP は取り締まりを実施する．

4.2 サーバーシステム

4.2.1 物理構成

3.2 で述べたように，VM 貸し出しサービスにおいてユーザや利用用途ごとに制約を設けておらず，メモリ不足に悩まされることがあった．その解決方法の 1 つとして，新システムでは現システムよりもメモリを多く搭載したサーバーを導入し，メモリ不足を対策した（表 4）．

ストレージの容量不足も，より大容量のストレージを導入することで解決した（表 5，表 6）．

表 4 物理サーバー

CPU	Intel Xeon E5-2699 (2.3GHz / 18 コア) x 2
メモリ	768GB (32GB x 24)
台数	4

表 5 高速ストレージ

HDD	SAS 1.2TB x 24 本 RAID6 構成
実効容量	19.7TB
台数	2

表 6 大容量ストレージ

HDD	SAS 4TB x 24 RAID6 構成
実効容量	65.5TB
台数	2

4.2.2 仮想化技術を用いたサーバーシステム

現行システムでは，Hypervisor には有償ライセンスである VMWare を利用していたが，新システムでは，オープンソースソフトウェアであり無償で利用が可能な KVM を採用した．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 を使用した．クラスタノード間における情報の同期や，死活管理として Pacemaker を使用した．また，そのクラスタ基盤ソフトウェアとして corosync を使用した．今回は，クラスタを構成するノード間でボリュームに LVM を使用するため，LVM のクラスタリング拡張機能のセットである CLVM を利用した図 4.

また，現システムで稼働中の VM イメージは ESXi でのみ動作する．そのため，全ての VM イメージを KVM で動作させるためにイメージの変換を行った．さらに，KVM でコンソールログインを行うためには，grub にカーネルオプションを記述する必要がある，そのため，一度変換した VM イメージを Linux 上でマウントしてカーネルオプションの記述をした．

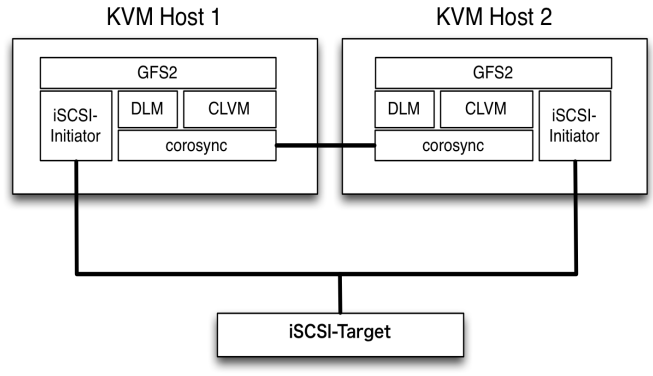

図 4 GFS2 を導入した KVM ホストの構成図

4.3 クラウドサービスの導入

3.3 で述べたように，沖縄は台風の影響により停電に見舞われることが多く，システム運用面において大きな課題となっていた．例えば，DNS が停止すると，メールサービスも停止してしまうそのため，休講通知や教員内連絡が回らない問題があった．そこで，クラウドサービスの導入を行った．クラウドサービスは，Web や DNS を運用するための基幹サービス用クラウドと，主に講義で使用される講義演習用クラウドの 2 つを導入した．

4.3.1 基幹サービス用クラウド

基幹サービス用クラウドの構成は，図 5 の通りである．基幹サービス用クラウドは 8 台で構成されている．内部ネットワーク内にストレージサーバーを配置し，各サーバーに必要な分だけストレージ NFS や iSCSI として切り出し，マウントすることが可能である．

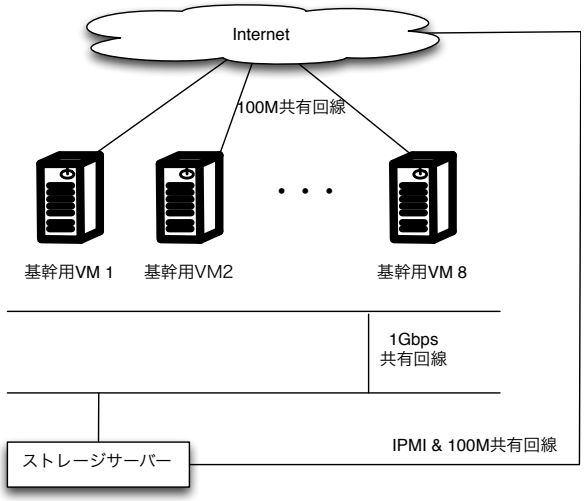

図 5 基幹サーバー用クラウドのネットワーク構成図

4.3.2 オンプレミスとクラウドの連携

本学科では, 基幹サービスとして, DNS や DHCP, LDAP, Web サーバーが動作している．3.3 の解決方法として，オンプレミスで動作する基幹サービスとクラウドサービスの連携を行った．具体的には，DNS のセカンダリをクラウド側に配置し，学科の DNS のレコードを持たせるようにした．

LDAP においても，セカンダリをクラウドサービス上に配置した Web サーバーは，クラウドサービス上にロードバランサと Web のセカンダリを配置し，オンプレミス側の Web サイトが停止した状態でも，閲覧できるように改善した．

4.3.3 講義演習用クラウド

学生の講義演習用に最大 100VM の提供を行っており，リソースの構成は表 7 となっている，一人当たりのリソースは CPU1 コア，メモリ 1GB, ディスク 20GB となっているが，リソースの上限の範囲内でメモリ,CPU などのリソース構成を柔軟に変更することが可能である．ネットワーク

構成は図 6 となっており．VM に割り当てられる IP アドレスは，全て IPv6 アドレスとなっている．

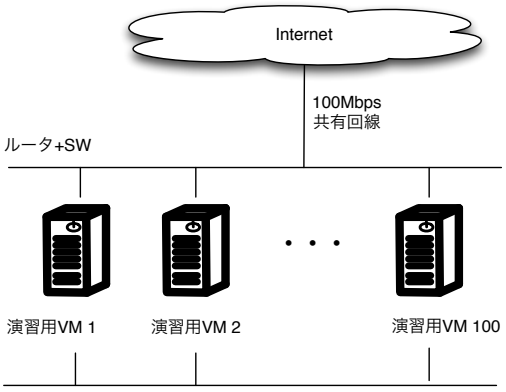

図 6 講義演習用クラウドのネットワーク構成

表 7 講義演習用クラウドのリソース構成

CPU	1 コア
メモリ	1GB
SSD	20GB
台数	最大 100

4.4 VM 管理コンソールの改良

新システムでは，仮想化基盤を VMWare から KVM へ変更したため，VM 管理コンソールも改良を行った．VMWare API から ssh のトンネリングを利用した，libvirt にアクセスに変更した．他にも，現行システムで問題となっていた VM 作成時に行うホスト名の入力チェックの強化やメモリや CPU 等取得に制限をかけた．

4.5 セキュリティ強化への対応

4.5.1 IP アドレスのプライベート化

3.4 で述べたように，本学科のネットワーク構成では，接続されている全ての端末にグローバル IP アドレスを付与していた．そのため，セキュリティ意識の低い管理者が運用するサーバーが標的にされた．そこで，学外から直接の攻撃対象にならないよう，グローバル IP アドレスの付与を必要としない端末や全ての演習用サーバーに対して割当てる IP アドレスをプライベート IP アドレスへと変更した．

4.5.2 セキュリティ監査の実施

グローバル IP アドレスを付与するサーバーには，システム管理チームによるセキュリティ監査を実施した．監査内容は以下の 8 項目である．

- 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など，適切な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
- 通常は使用されない特殊ユーザは，ログオンできないようにしているか
- リモートから管理者ユーザーで直接アクセスできないようにしているか
- ユーザのパスワードは適切に設定されているか
- OS やアプリケーション等を定期的にアップデートする機構が用意されているか
- アプリケーション毎の設定ファイルの記述が適切かどうか

具体的な監査の実施には，同チームが監査対象のサーバーに対してリモートログインを行って実施している．

4.6 監視体制の強化

3.5 で述べたように，システムを監視体制を強化する必要が出てきたため，統合監視システムの Zabbix を導入した（図 7）．監視システムに Zabbix を採用した理由として，非公式コミュニティが活発であり，導入事例も多く，参考となる情報や文献が他の監視システムよりも多かったためである．

Zabbix では，各基幹サーバーやストレージのリソース監視や運用しているサービスの死活監視を行っている．これにより，障害をできるだけ早く検知し，迅速な対応が可能になった．

また，オンプレミス環境だけでなく，クラウド環境の監視も行っている．学生演習用クラウドに関しては，契約の都合上，使用率を一定以下に抑える必要があることから，起動だけを行っている VM を監視し，動作を停止させるようにした．

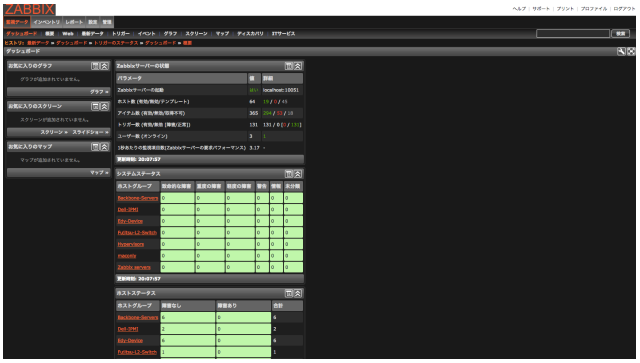

図 7 Zabbix の管理画面

4.7 ハイグレード UTM の導入

セキュリティ対策の 1 つとして，UTM アプライアンスを導入した．UTM アプライアンスを導入する利点は，ネットワーク内への不正侵入を検知し，システム管理チームへの通知と対処を行うことが可能である．また，スパム対策や Web のフィルタリングなども行うことが可能である．

Vol.2015-IOT-31 No.12
Vol.2015-SPT-15 No.12
2015/9/26

5. 総括

本研究では，現教育情報システムの構成と課題を述べ，9月に行われるシステム更新に向け設計と構築を行った．今後の課題として，ユーザーに提供する貸し出し VM において，公開鍵の設定ミスによる救済措置のため VM 管理コンソールに VNC でアクセスするための機構や公開鍵を Web 経由で行うための仕組みを作成する．今回，同チームが提供する VM 管理コンソールには，クラウド環境の VM を操作するための機構が備わっていない．そのため，クラウド環境で稼働している VM を操作するコンソールとオンプレミス環境で動作する VM を操作するための管理コンソールが分離している．今後，1 つのコンパネでオンプレミス環境とクラウド環境の VM を一括で操作できる仕組みを作成したい．

さらに，2015 年 10 月に新システムが本稼働するため，安定したシステム運用とその評価を行いたい．

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.