Vol.2010-IOT-11 No.2
2010/10/15

仮想化環境を用いたサーバ設定演習支援システムの設計と実装

林　　周　斗[†1]　　桝　田　秀　夫[†2]

近年，PC の普及に伴い，大学等のコンピュータリテラシ教育においても，PC の操作方法の指導や，プログラミング言語等の情報処理の基礎指導が行われている．情報処理教育の一環としてサーバの構築を演習科目として実施することにより，ネットワーク技術や，コンピュータの管理を学習させたいといった要望がある．

しかし，サーバ構築演習を受講する演習者はサーバを構築した経験に乏しい場合が多く，構築したサーバが正しく動作しているかどうかを判断することが難しい．演習の規模が大きくなれば，指導者が演習者に個別に対応することは難しく，演習を進める上でも問題となる．演習者が自身の構築したサーバの動作を自主的に，自身のペースで確認できることが望ましい．

そこで，本稿では仮想化環境を用いて複数のサーバを構築し，さらに，演習者が自身が構築したサーバに対して動作確認を行い，その結果が確認できるシステムの設計と実装を行った．

Design and Implementation of a Training Course Environment of Unix server setup with Virtualization Technology

Shuto Hayashi[†1] and Hideo Masuda[†2]

Recently, many people use PC and there are many basic guidance of the information technology. Many university students study with PC operation, computer literacy, and programing language. Teachers wont to give them instructions network technology and computer system management by training of Unix server setup. But, there are students they don't have experience of Unix server setup. They can't judge constructed server works correctly. In propotion as the scale of training course increase, it will become difficult for teachers to guide student individually and it will become a hindrance of training. Students should be able to judge constructed servers by them work correctly or not correctly. I state about support system with virtualization environment that setup many server instances and test behavior of constructed servers by students.

1. はじめに

近年，一般家庭においても PC が普及し，多くの人々が日常的にコンピュータを扱うようになってきている．それに伴い，大学等のコンピュータリテラシ教育では，PC の操作方法を指導する段階から，コンピュータのより高度な活用，プログラミング言語等の情報処理の基礎を指導する段階へと移行しつつある．情報処理教育の一環として OS の設定やサーバの構築を演習科目として行うことにより，ネットワーク技術や，コンピュータの管理をより深く学習させることが可能となる．OS の設定やサーバの構築を演習として行う場合，演習者がコンピュータの管理者権限を持つ必要があるため，演習に用いるシステムのセキュリティの確保や外部ネットワークへの影響を考慮する必要がある．

大学等の設備環境においてサーバ構築演習を実施する場合には，専用の設備を導入するコストが大きいため，他の演習等で利用されている PC 演習室等の共同設備を利用して，サーバ構築演習として適切な演習環境を用意することが考えられ，実際に演習を実施した例も報告されている．[1)2)] しかし，演習者はサーバの構築等の経験が少ない場合が多く，自身が構築したサーバの設定内容の正誤を正確に判断することが難しい．そのため，自身の進捗状況を自分のペースで確認できないことが問題となる．文献 1)，2) では演習者が変更したファイルを参照可能にして，演習者が行った設定を追跡できるようにしているが，演習規模が大きくなり，多数の演習者が演習を行うような環境においては，演習者によって構築されたサーバを 1 台 1 台個別に検査することは，指導者としても負担が大きく，演習者の状況にあわせて演習を進める上でも望ましくない．

このことから，サーバ構築演習中に演習者の任意のタイミングで構築したサーバに対して動作確認を行い，その結果から設定内容の正誤を演習者に通知できるシステムを提供することにより，演習をよりスムーズに進めることが可能であると考えられる．

本稿では，仮想化環境を用いて複数のサーバを構築し，演習者が構築したサーバに対して動作確認を行い，その結果を通知するようなシステムの設計と実装を行う．サーバ設定を確認する手法について検討を行い，仮想計算機技術と VPN を利用する方法を提案する．これらを利用することで設定されたサーバがやりとりするパケットの収集を容易にし，パ

†1 京都工芸繊維大学大学院 工芸科学研究科
Graduate School of Science and Technology, Kyoto Institute of Technology
†2 京都工芸繊維大学 情報科学センター
Center for Information Science,, Kyoto Institute of Technology

© 2010 Information Processing Society of Japan

ケットのやりとりから構築されたサーバの設定状態を判断し通知を行うことで進捗状況を判断可能にする．また，DNS サーバを設定する演習を対象とし，様々な運用形態における DNS サーバの動作を検証し，動作確認の方法を検討，支援システムの実装を行う．

2. サーバ設定演習と動作確認手法

本章では，本稿が想定するサーバ設定演習について述べる．

2.1 既存のサーバ設定演習について

演習者が設定する対象のサーバを本稿では**演習者サーバ**と呼ぶ．Unix 系 OS のもとでサーバを設定し動作させる場合には，演習者が演習者サーバに対して管理者権限を行使できる必要がある．そのため，既存の研究においては，USB メモリや外付けの HDD などの取り外しが容易なデバイスを利用する方法やネットワークブートなどを利用する方法，仮想化環境を用いて専用の環境を用意する方法[3] などが用いられている．演習者が設定するサーバは 1 つであるとは限らず，複数台の演習者サーバ群を扱える．

2.2 想定するサーバ設定演習

本稿ではサーバ設定演習は，既存の手法と同様に，PC 演習室などの設備を利用してプログラミング演習のように，多数の演習者が参加する演習授業を想定している．数十人の演習者に対して数人の指導者，TA が対応するといった状況が考えられる．教授者達が各演習者へ個別に対応した場合でも負担軽減のための動作確認システムがあれば，演習をスムーズに進行できると考えられる．また，課題や自習時間などの演習時間外にも対応できる必要がある．

2.3 動作確認手法

演習者サーバの動作を確認する場合，以下のような手法をとることで動作確認が可能であると考えられる．

手法 1　指導者が演習者サーバにログインして確認する

演習者サーバにログインして，設定ファイルやプロセスの状態を確認する方法である．設定したサーバの様々な状態を得ることができる．また，演習者サーバ上でプロセスやファイルの状態を監視するプロセスを実行させ ておくことでも動作確認ができると考えられる．しかし，演習者サーバの管理者権限は演習者が保持しているため，外部からログインしたり，監視のためのプロセスを保護することは難しい．

手法 2　設定ファイルを解析する

演習者が編集した設定ファイルを提出させ，そのファイルを解析することで設定内容が間違っているかどうかを確認できる．しかし，実際に演習者サーバのプロセスがどのように動作しているかは判断できず，そのファイルをサーバのプロセスが使用しているかどうかも判断できない．

手法 3　演習者サーバを利用してその応答を得る

実際にクライアントとして演習者サーバを利用し，その応答を得ることで演習者サーバがどのような設定であるかを確認する．サーバの状態を確認する手法として一般的に使われる方法であるが，演習で指定された動作が実現できているかをサーバの応答からどの程度調べることが可能であるかを検討する必要がある．

手法 1 では演習者が管理者権限を持つため，動作確認が正しく行えない可能性がある．手法 2 では課題としてファイルを提出させて採点を行うような場合には有効であるが，実際に動作させた状態を確認することができないため，演習中の確認作業としては不適当である．手法 3 は基本的にはサーバを動作させておくだけで良いため，比較的容易に実現可能であると考えられるため，本稿ではこの手法 3 を選択した．実際にサーバからの応答で確認できる事項については以降で検討する．

3. 動作確認サービスの検討

サーバが何らかのサービスをクライアントに提供する際には，そのサーバとクライアント間でのみ通信することもあるが，サーバが単独で動作せず，外部のサーバと連携することでサービスを提供することが多い．演習内容によっても異なるが，多くの場合，演習者サーバも他のサーバと通信を行うと考えられる．演習において演習者サーバが通信する他のサーバは演習を実施する側で適切に用意する必要がある．これらのサーバ群を本稿では**演習環境サーバ群**と呼ぶ．動作確認の際には，演習者サーバが正しく動作していることを確かめるために，演習者サーバ群と演習環境サーバ群との間でどのような通信を行っているかを監視できる必要がある．

通信を監視するためには演習環境サーバ群にパケット監視用サーバを加え，演習内容に関わるパケットを監視用サーバが監視可能にすればよい．しかし，サーバ構築演習は PC 演習室など通常は他の目的にも用いられる設備を利用することを想定しているので使用する PC やネットワーク機器に対してパケットのミラーリングなど特別な設定を施すことは望ましくない．そこで仮想計算機と仮想ネットワークを組み合わせて利用することを検討した．演習者サーバ群にも仮想計算機を用いることで，PC 演習室などの通常では Windows などが利用される PC 上で管理者権限を演習者に付与した複数の Unix 系 OS を使用することが

© 2010 Information Processing Society of Japan

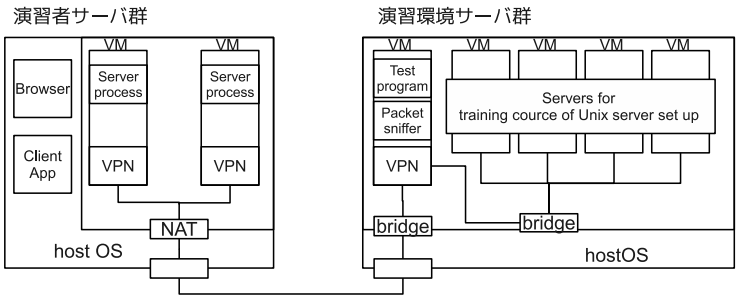

図 1 動作確認可能なサーバ設定演習システム
Fig. 1 Server setup training system

できる．また，演習環境サーバ群にも仮想計算機を用いることで演習環境の導入や運用のコストを低くすることが期待できる．さらにこれらを VPN で接続することにより．演習者サーバ群と演習環境サーバ群との間の通信を監視可能となる．動作確認のためのシステム概略を**図 1** に示す．仮想ネットワークを用いることで自宅学習などにも応用可能であると考えられる．

4. 実例：DNS サーバ設定演習

サーバ設定演習として，DNS サーバの設定を行う演習について検討を行った．DNS サーバは運用形態によって様々な設定を行うことができる．DNS サーバを設定する演習を実施する際にはそれぞれの運用形態を実際に設定し，動作させることが想定される．DNS サーバの実装の一つである BIND[4] ではおおまかに区別すると 4 つの形態として DNS サーバを設定することができる．

4.1 DNS サーバの運用形態

- キャッシュサーバ
  キャッシュサーバは DNS クライアントから名前解決を依頼され，検索を行い，ドメイン名の解決を図る．検索の際ははルートネームサーバから順にドメインツリーを辿り，目的のプライマリサーバから応答を得る．また，検索を行った結果を一定の期間保持することで外部サーバへの問い合わせを減らし，クライアントの問い合わせに素早く応答する．
- フォワードサーバ
  フォワードサーバは DNS クライアントから受け取った名前解決要求をキャッシュサーバへそのまま回送する．そしてキャッシュサーバから受け取った回答をクライアントへ送る．また，フォワードサーバ自身もキャッシュサーバと同様に結果を一定の期間保持する．
- プライマリサーバ
  プライマリサーバは自分が権限を持つドメインにおけるゾーン情報を保持する．ゾーン情報には IP アドレスとドメイン名の対応表などが含まれており，これを使ってキャッシュサーバやクライアントからの反復的な問い合わせに対して応答する．
- セカンダリサーバ
  セカンダリサーバはプライマリサーバと同じ情報を保持し，問い合わせに対しても同様に応答する．しかしセカンダリサーバ自身がゾーン情報をローカルに保持するのではなくプライマリサーバからのゾーン転送により，ゾーン情報を得る．

DNS サーバ設定演習では，それぞれの運用形態を実際に設定して演習を行うものとする．動作確認はそれぞれの運用形態にあわせて行える必要がある．

4.2 DNS パケットの監視

DNS サーバはクライアントに応答する際に，他の DNS サーバと通信することが多いため，正しく動作確認を行うためにはクライアントとして DNS サーバの応答を得るのみでは不十分である．演習者 DNS サーバが通信する他の DNS サーバ群を演習環境 DNS サーバ群として用意することでパケットを監視可能にできる．キャッシュサーバは名前解決の際にドメインツリーを辿るのでドメインツリーを構成するためのフェイクのルートネームサーバとプライマリサーバが，フォワードサーバは問い合わせを回送するキャッシュサーバがそれぞれ必要である．また，プライマリサーバとセカンダリサーバもドメインツリーを辿って到達できることが望ましいので，ドメインツリーを構成するサーバ群を用意するべきである．

© 2010 Information Processing Society of Japan

4.3 DNS サーバの動作確認

4.3.1 キャッシュサーバの動作確認

キャッシュサーバとして以下の項目を確認する必要がある．

- クライアントからの解決要求について正しく応答するか
- 名前解決の結果を正しくキャッシュするか

キャッシュサーバの応答の内容のみでは，その応答がは新たに演習環境サーバ群に問い合わせをして得たものであるか，以前の結果をキャッシュしたものであるかの区別がつけられないため，正しくキャッシュするかどうかを確かめる方法が必要となる．よって以下のような確認手順をとる．

(1) キャッシュサーバに対して問い合わせを行う
(2) 名前解決できているかを確認する
(3) キャッシュサーバの回答が既にキャッシュされたものではなく，演習環境サーバ群に問い合わせたものであることを確認する
(4) もう一度同じ問い合わせを行ってキャッシュされていることを確認する

キャッシュサーバからの応答が新たに問い合わせたものであるか，キャッシュしていたものであるかは，キャッシュサーバが応答を返すまでにどのような通信をしていたかを監視することで確かめることができる．キャッシュサーバに問い合わせる際には，既にキャッシュされていないようなドメイン名を選ぶようにする必要がある．

4.3.2 フォワードサーバの動作確認

フォワードサーバとして以下の項目を確認する必要がある．

- クライアントからの解決要求について正しく解決するか
- 正しいキャッシュサーバに対して解決要求を回送しているか

正しいキャッシュサーバとは演習環境サーバ群に用意したキャッシュサーバである．フォワードサーバの応答は演習環境キャッシュサーバに同じ問い合わせを行ったときの応答とほぼ同じである． 例外としてはフォワードサーバもキャッシュを持つことが可能であるためレコード内の TTL が異なる場合がある．動作確認には以下のような方法をとる．

(1) フォワードサーバに対して問い合わせを行う
(2) 名前解決できているかを確認する
(3) 正しいキャッシュサーバに回送しているかを確認する

キャッシュサーバの動作確認と同様にフォワードサーバ自身のキャッシュを考慮して，問い合わせの際にキャッシュされていないドメイン名を選ぶ必要がある．

4.3.3 プライマリサーバの動作確認

プライマリサーバとして以下の項目を確認する必要がある．

- あるゾーンに対して正しく権限を持っているか
- 権限を持つゾーンに対する反復的な問い合わせのみに応答するか
- 権限を持つゾーンの情報を正しく保持しているか

プライマリサーバとして，ゾーン情報を正しく保持しているかを確認する必要がある．また，プライマリサーバは再帰的な問い合わせや権限を持たないゾーンに対してはルートサーバへのヒントを返す．ルートサーバには演習環境サーバ群に用意したフェイクのルートサーバである．動作確認には以下の方法をとる．

(1) 権限を保持しているゾーンについて SOA レコードを問い合わせる
(2) SOA レコードが適切かどうかを確認する
(3) 正引き，逆引きの反復的な問い合わせを行い，結果を確認する
(4) 反復的な問い合わせや，権限を持たないゾーンについて問い合わせる
(5) 応答に含まれるルートサーバへのヒントが適切であるかを確認する

4.3.4 セカンダリサーバの動作確認

セカンダリサーバとして以下の項目を確認する必要がある．

- プライマリサーバと同じ確認項目
- プライマリサーバから正しくゾーン転送をしているか

セカンダリサーバはプライマリサーバと同じ情報を保持するのでプライマリサーバと同じ確認項目が必要となる．また，プライマリサーバからのゾーン転送を行っていることを確かめる必要がある．確認は以下のような方法をとる．

(1) プライマリサーバと同じ動作確認を行う
(2) プライマリサーバへの問い合わせ結果と比較を行う

5. 実　　装

仮想化技術を用いた DNS サーバ設定演習が可能なシステムの実装について述べる．システムの全体図を**図 2** に示す．

5.1 演習環境サーバ群

演習環境サーバに用いたコンピュータを**表 1** に示す．仮想計算機として Xen 3.0.3[7] の完全仮想化を用いた．Domain0，DomainU にはそれぞれ 1Gbyte のメモリを与え，DomainU

© 2010 Information Processing Society of Japan

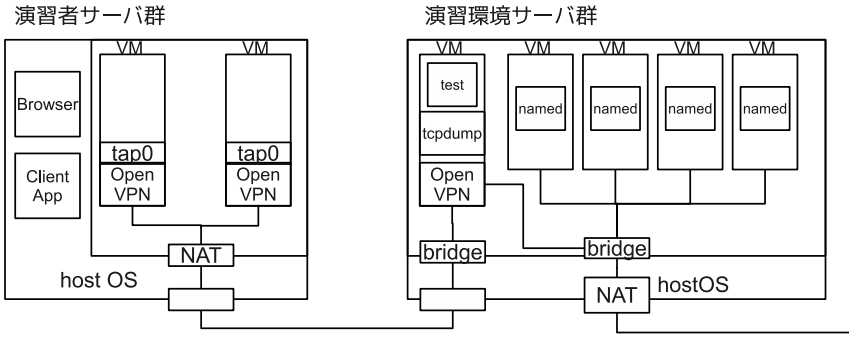

図 2 仮想化技術を用いた DNS サーバ設定演習が可能なシステム
Fig. 2 DNS server setup training system with virtualization technology

は 5 台を作成し，必要に応じて 2 台増やす余地を残した．

5.1.1 演習環境 DNS サーバ群

演習環境 DNS サーバ群として BIND 9.3.6 をインストールした DomainU4 台を使用した．1 台はキャッシュサーバとして動作するように設定を行い，残り 3 台はそれぞれフェイクのルートサーバ 1 台，TLD(Top Level Domain)2 台となるように設定し，ドメインツリーを構築した．

表 1 PC スペック表
Table 1 Spec of PCs

	OS	CPU	Memory	NIC
演習環境サーバ群	CentOS 5.5(x86_64)	AMD Athlon 64 3500+	8Gbyte	1000Base-T
演習者サーバ	CentOS 5.5(i386)	AMD Athlon 64 3500+	4Gbyte	1000Base-T

5.1.2 パケット監視サーバ兼動作確認サーバ

サーバ群がやりとりする DNS パケットを収集し，保存する機能と，演習者サーバに問い合わせを行い，その応答と保存したパケットの記録から演習者サーバの動作確認を行う機能を持ったサーバである．DNS パケットを保存するために tcpdump[5] を用いた．DNS は UDP の 53 番ポートを利用するので 1Mbyte ずつファイルに連番をつけてパケットを保存するには以下のようなコマンドを実行する．

- # tcpdump -i eth0 -C 1M -w pcaplog udp port 53

また，動作確認機能については C 言語を使って実装を行った．コード規模はコメントも含めて約 2000 行であった．

5.2 演習者サーバ群

演習者サーバ群に用いたコンピュータを表 1 に示す．仮想計算機として Xen 3.0.3 の完全仮想化を用いた．DomainU を 2 台作成し，512Mbytes のメモリを与えた．Xen のネットワークには NAT を選択した．DomainU それぞれに BIND 9.3.6 をインストールし，それらに対して設定することで演習を行うものとした．

5.3 仮想ネットワーク

仮想ネットワークとして OpenVPN[6] を用いた．バージョンはサーバ，クライアントともに 2.0.9 を使用した．

5.3.1 OpenVPN サーバ

演習者サーバ群と演習環境サーバ群を仮想ネットワークで接続するために，パケット監視サーバとして設定した演習環境サーバ群の DomainU に OpenVPN をインストールしサーバとして動作させた．OpenVPN はブリッジモードで動作することにより，クライアントとなる演習者サーバが同じイーサネットのサブネット内にいるかのように，論理的に双方を接続させることができる．

5.3.2 OpenVPN クライアント

演習者のコンピュータの DomainU のそれぞれ OpenVPN をインストールした．演習者サーバは VPN クライアントとして VPN サーバにアクセスする．演習者サーバがそれぞれ OpenVPN による仮想ネットワークに参加することにより，演習者サーバ同士の通信でも OpenVPN サーバを経由することになり，パケットを収集可能となる．また，演習者のコンピュータでは Domain0 と DomainU 間のネットワークに NAT を選択しているため，DomainU 側でプライベートな IP アドレスを使用する．この方法はにより，演習者サーバ群側で用いる仮想計算機技術は Xen 以外も使用することが可能であり，Windows がインス

© 2010 Information Processing Society of Japan

トールされた PC からその上で VMware や VirtualBox などの仮想計算機技術でも学習することが可能である．

6. まとめと今後の課題

本稿では，サーバを設定する演習において，演習者が設定したサーバの動作確認を可能として演習をスムーズに進めるための支援システムとして仮想計算機技術と VPN を利用して演習者サーバかやりとりするパケットを収集し，動作確認を行うシステムの検討を行った．また，DNS サーバを設定する演習を想定し，様々な DNS サーバの運用形態における動作確認手法を検討し，動作確認が可能となるシステムの実装を行った．

今後の課題としては，本稿のシステムをどの程度の規模のサーバ設定演習に利用できるのかを動作確認プログラムや，パケット監視サーバなどの演習環境サーバ群の負荷を測定し明らかにしていく必要がある．また，実際に演習を実施し，演習者にシステムを利用してもらうことにより，支援システムの効果について評価を行うことも挙げられる．

参 考 文 献

1) 桝田 秀夫, 中西　通雄, 安留　誠吾: 「PC 演習室を使用した持ち込みブートサーバによる OS 設定演習事例」2007 年 PC カンファレンス, pp.447-450, August 02-04, 2007.
2) 桝田 秀夫, 中西　通雄, 安留　誠吾, 齊藤 明紀: 「サーバ設定演習が可能なディスクレス計算機環境の検討」情報処理学会 DSM 研究会, 2006-DSM-43, pp.1-6, September 15, 2006.
3) 中川泰宏, 浮貝雅裕, 三井田惇郎：「仮想計算機演習室を利用したネットワークの基本知識の学習支援に関する研究」教育システム情報学会第 31 回全国大会, pp.363-364, Aug 23-25, 2006.
4) Cricket Liu，Paul Albitz：DNS&BIND, 第 5 版, オライリージャパン，2008.
5) tcpdump http://www.tcpdump.org/
6) OpenVPN http://openvpn.org/
7) Xen http://www.xen.org/

© 2010 Information Processing Society of Japan