

コンピュータ実習室のサーバの構築

システム科学技術学部　電子情報システム学科
2年　佐々木　渚

指導教員　システム科学技術学部　情報工学科
助教　橋浦　康一郎

1　はじめに

現在、生活で使用する物の IoT 化が進み、様々なサービスが登場している。また、サービス上では、個人情報や機密情報を取り扱うことも多く、その情報を守るためにもセキュリティについての知識が必要である。これらの背景を受け、サーバを構築することでセキュリティについての知識と関心を高め、日々の生活で個人情報を守るための対策を考えられるようになるために、本学のコンピュータ実習室のサーバの構築を自主研究にした。コンピュータ実習室のサーバは、電子情報システム学科および情報工学科の学生が利用する端末を管理・運用するためのサーバである。

本自主研究の目的は堅牢なコンピュータ実習室のサーバを構築することで、その重要性は、サーバを作成することで、サーバの動作や役割について学び、近年求められているシステムを攻撃から守るすべを学び、それを広めることで、周囲の人のセキュリティに関する知識や関心を高めることである。

2　サーバの概要

サーバとはネットワーク上で他のコンピュータやソフト、すなわちサーバの利用者（クライアント）にサービスを提供するコンピュータのことである。サーバはクライアントの要求を受け、それに答えるかたちでサービスを提供している。例えば、図1のサーバの処理の流れの図で赤い矢印がクライアントのサーバに対する要求を表していて、青い矢印がサーバのサービスを表している。代表的なサーバとして Web サーバがあり、Web サーバの場合は、図1の赤い矢印はクライアントがサイトの情報を要求したことを表し、青い矢印はサーバが要求されたサイトのデータをクライアントへ送っていることを表す。

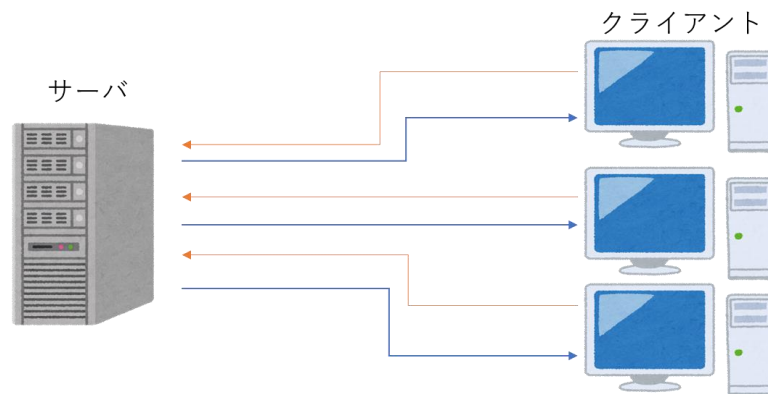


図1 サーバの処理の流れ

3 各サーバの構成

コンピュータ演習室のサーバは3つのサーバから構築されており、それぞれを認証サーバ、Webサーバ、ファイルサーバと呼ぶ。認証サーバではLDAP (Lightweight Directory Access Protocol) により利用者の情報を管理している。Webサーバではイントラネット (Web ページ) への端末からの接続の管理とDNS (Domain Name System) の管理を行っている。ファイルサーバではNFS (Network File System) により端末利用者によって作成されたファイルを一元管理している。

3.1 認証サーバ

認証サーバは、LDAP により端末利用者の情報を管理しており、ファイヤーウォールにより、認証サーバへのアクセスに使うポートを制限している。LDAP は端末利用者のユーザ名、グループ名、パスワード等を保管するソフトウェアである。作成したサーバではLDAP の情報は端末のログイン時の認証に利用される。LDAP の情報の具体例は、学籍番号が B19B036の生徒であればLDAP にはログインユーザ名が B19B036、個人の名前が sasaki nagisa、ホームディレクトリのパスが/home/student/b19B036等の情報が登録されている。

3.2 Webサーバ

Webサーバは、Apache により、学科イントラや各教員の個人ページを管理している。Apache はWebサーバを構築するためのソフトウェアである。DHCP (Dynamic Host Configuration Protocol) により各端末に固定のIPアドレスの割り当てを行っている。そして、DNSによりイントラへ数通りのドメイン名からアクセスできるようにしている。DNS はドメイン名とIPアドレスを対応させる仕組みのことである。そして、プログラミング演習などの講義で課題を提出するためにSubversionによりファイルを共

有できるようにしている。Subversion とはバージョン管理システムで、特定の相手やグループとファイルを編集の履歴を残しながらやり取りが出来るようにするソフトウェアである。また、Webサーバへはファイヤーウォールにより学内からしかアクセスできないようにしている。

3.3 ファイルサーバ

ファイルサーバでは NFS を利用しているため、どの端末からでも同一のファイルを決められた権限の下で操作することができる。NFS とは一つの機器に保存されているデータを複数の端末で操作可能にするソフトウェアである。また、HDD (Hard Disk Drive) の構成として RAID5 (Redundant Arrays of Inexpensive Disks Five) を導入しているため、データが失われにくい。RAID5は各ハードディスクを複数のブロックに区切り、そのブロック1つに対して、その他の全てのブロックのパリティを計算し、その結果をブロックとしてハードディスクに保存しておく仕組みのことである。図2は RAID5の構成を表していて、4つの HDD がブロック (A1, A2, A3, B1~4のパリティなど) に区切られて、A1のブロックのパリティは A1以外のパリティのブロックを含めないブロック (A2~4, B1~4, C1~4, D1~4) のパリティを計算し、その値を別の HDD に保存することで、HDD 1 のデータが消えたとしても他の HDD4に保存されている A1~4のパリティから消えたデータを元に戻すことができる。

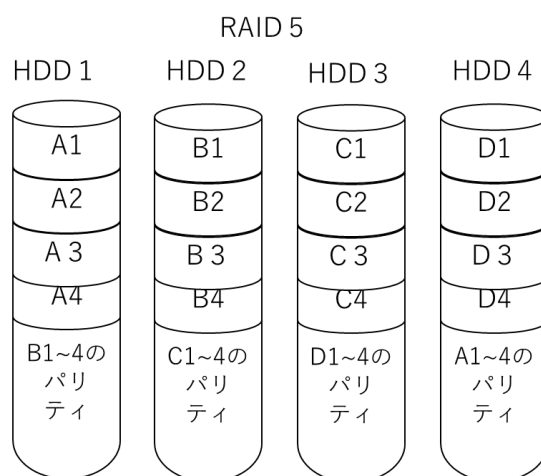


図2 RAID 5 の構成

保存したデータは clamav というセキュリティソフトによって、常時ウイルスチェックを行っている。そして、データのバックアップは月に一回行われている。ファイルサーバには、ファイヤーウォールにより学内からしかアクセスできないようにしている。

4 各サーバの動作例

ユーザがログインしてファイルを操作するまでを図3を用いて説明する。端末に電源

が入ると、DHCP により端末に IP アドレスが割り当てられる (①) .次に NFS により /home ディレクトリが端末にマウントされる (②) .ユーザはパソコンに LDAP に登録されている学籍番号とパスワードを入力する (③) . 入力すると LDAP が登録内容と照らし合わせ、評価を返す (④) . ログインに成功すると各自のホームディレクトリ (学籍番号が B19B036であれば/home/student/b19B036) を読み込み, 設定ファイル等に従って動作する.

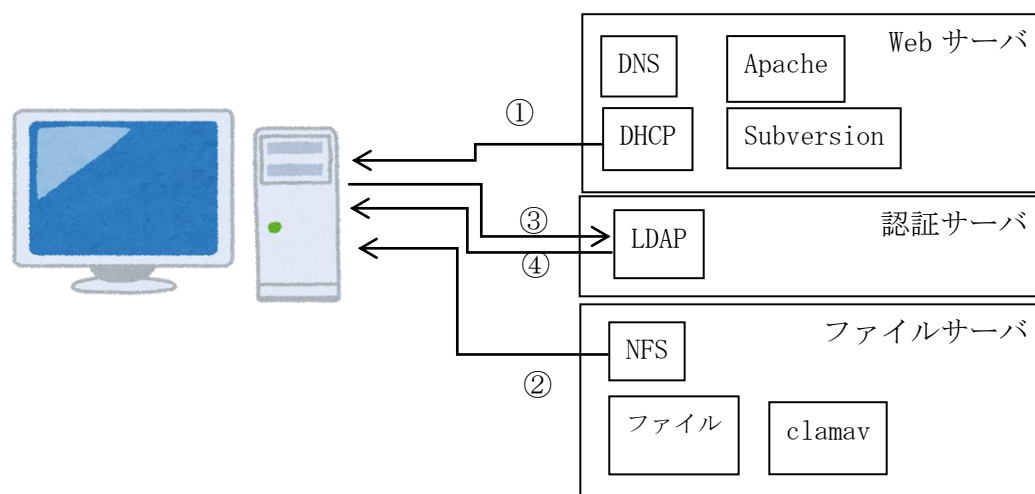


図3 各サーバの動作例

5 まとめ

本自主研究で作成したサーバは, データの保存形式を RAID 5 にしていることや clamav による常時ウイルスチェックを行っていること, サービスを行っているハードウェアが管理者しか入れないサーバールームにあることから堅牢なサーバを構築することができたといえる. 本自主研究を通してサーバの仕組みや構築の仕方や運用方法を学ぶことができた. この経験を活かし周囲のセキュリティに関する知識や関心を高めていきたい.

参考文献

- [1] きはし まさひろ, "イラスト図解式 この一冊で全部わかるサーバーの基本", SB クリエティブ (2016)
- [2] デージーネット, "入門 LDAP/OpenLDAP ディレクトリサービス導入・運用ガイド第三版", 秀和システム (2017)
- [3] C. Michael Pilato, Ben Collins-Sussman, Brian W. Fitzpatrick, "実用 Subversion 第二版", オライリージャパン (2009)
- [4] 高橋基信, "改訂新版サーバ構築の実例がわかる Samba[実践]入門", 技術評論社 (2016)