

3-13 学内LAN運用管理講習会

本講習会は、私立大学におけるネットワークの運用・管理に携わる教職員のネットワーク運用管理技術の修得を目的に、テーマごとにテキスト等による講習と情報機器を使用した技術指導を行うものである。平成14年度は、参加者の技術水準や関心事項に対応できるよう、難易度、テーマにより設定の10クラスの中から4クラスを選択する”アラカルト”形式にて実施した。講習会の企画・運営・実施は、ネットワーク研究委員会学内LAN運用管理小委員会が担当した。

(1) 開催要項の決定と実施準備

- ① 参加者のスキル、講習会への要望等が多種多岐にわたっており、従来の固定3コースでは一人々のニーズに即した適切な講習困難になっているため、受講者が希望するクラスを選択できるアラカルト形式で実施することにした。
- ② 一般的なクラス選択例として、初級者・中級者・上級者の3例を想定し、各レベルの間を補完する形でクラスの設定を行うこととした。
- ③ 初級者向けクラスでは、学内LAN運用管理経験が2年未満の教職員を対象とし、ネットワーク運用の基本的な概念と仕組みについて、演示及び実習により技術を修得することにした。
- ④ 中級者を対象としたUNIX管理業務クラスでは、参加者の技術水準が幅広いため、UNIXの利用経験のない者を対象とした、同テーマの基礎編クラスを設けることとした。
- ⑤ 上級者を対象としたIP基礎実習、不正侵入対策実習クラスは参加者がノートPCの持参を義務付けた。実習環境の構築が平易となるよう、事前に委員会が作成したLinuxシステムのイメージファイルをWindowsPCに取り込み、参加者所有PCの環境に変更を加えないよう工夫することとした。

平成14年度学内LAN運用管理講習会開催要項

1. 講習会の目的

本講習会は、受講目的・経験に応じて講習テーマを設け、私立大学におけるネットワークの導入と運用管理に携わる教職員の養成を目的とします。

2. 受講資格

会員大学・短期大学の教職員の方で、学内のネットワークの導入と運用管理業務に携わる方

3. 講習概要

(会場イ)

【第1限～第4限：A1, A2, B1, B2クラス】

対象者：学内LAN運用管理2年未満で、ネットワーク運用管理手法全般に関する基本的な技術の習得を目指す方。

ねらい：ネットワークに関する基礎的な仕組みを講義や簡単なデモンストレーションを通じて理解し、学内LAN管理業務に携わるための前提となる基本的な知識の習得を目指す。

※A1, A2クラスおよびB1, B2クラスはそれぞれ異なる講習内容ですが、関連した内容であり、連続して進行しますので、特に初級レベルの方は一貫して受講することを推奨します。

<各講習内容>

第1限：A1クラス LAN, インターネットの仕組み

講習内容：LAN（イーサネット）における通信の原理、LANの構成、インターネットの仕組み

第2限：A2クラス LAN, インターネットの仕組み

講習内容：IPプロトコル、ルーティング、DNSの仕組み

第3限：B1クラス ネットワークサービス

講習内容：ネットワークサービス、クライアント・サーバモデル、WWWの仕組み

第4限：B2クラス ネットワークサービス

<講習内容>Proxy, e-mailの仕組み

(会場ロ)

【第1限：C'クラス UNIXホストのセキュリティ管理基礎編】

【第2限：C'クラス（どちらも同じ内容です）】

対象者：ネットワーク運用管理に関する基礎的な知識があるものの、UNIXに関する知識はなく、今後UNIXホスト管理業務に携わる予定のある方。

ねらい：UNIXシステムの基礎を学ぶことで、セキュリティ管理で必要なことを理解し、UNIXホストの管理者として必要な基礎知識の習得を目指す。

<講習内容>

1. ファイルシステムのセキュリティ、2. プロセス、3. アカウントシステム

【第3限：D'クラス UNIXネットワーク管理基礎編】

【第4限：D'クラス（どちらも同じ内容です）】

対象者：ネットワーク運用管理に関する基礎的な知識があるものの、UNIXに関する知識はなく、今後UNIXシステムによるネットワークサーバ運用に携わる予定のある方。

ねらい：UNIXシステムでのネットワークサービスについて基礎的な事項を学習し、ネットワークサービスを運用するUNIXシステムのセキュリティ管理で必要なことを理解する。

<講習内容>

1. プロセスの管理 2. ネットワークサービス 3. システムの監視

(会場ハ)

【第1限：Cクラス UNIXホストのセキュリティ管理】

【第2限：Cクラス（どちらも同じ内容です）】

対象者：UNIXの基礎知識を有する方で、UNIXによるサーバシステム管理の基本的な知識および技術の習得を目指す方。

ねらい：学外ネットワークからの攻撃や学内情報コンセントを使用した不正使用からコンピュータを守るため、セキュリティ対策について自己防御に必要な技術の習得を目指す。

<講習内容>

1. セキュリティホールとセキュリティパッチ
(1)OSのセキュリティホール (2)セキュリティパッチの入手法と当て方
2. サービスごとのアクセス制限
(1)Wrapping概要 (2)TCP Wrapperについて

【第3限：Dクラス UNIXネットワーク管理】

【第4限：Dクラス（どちらも同じ内容です）】

対象者：UNIXによるLAN運用管理の基本的な知識及び技術の習得を目指す方（UNIXの基礎知識を有する方）

ねらい：サン・マイクロシステムズがSolarisシステム運用管理に関して、一定水準の技能及び知識を有していることを認定する全世界共通の資格制度であるSCSA（Sun Certified System Administrator）の出題問題を参考にしながら現場でのUNIXネットワーク運用管理技術の一部を習得する。

<講習内容>

1. ネットワークの設定 2. ネットワーク（モニタコマンド等）
3. ネーム・サービス

(会場ニ)

【第1限：Eクラス IP基礎実習ほか】

対象者：IPv4のことは一応知っているが、より詳しいことを理解したい、また今後IPv6の実験をしたいと思っているネットワーク管理者。UNIX

のコマンド操作ができること、root作業経験が少しはあること、viなどのテキストエディタは問題なく使用できること。

ねらい： IPv4による古典的なLAN構築における基礎的な事項を実習を通じて体得する。IPv6について基礎的な事項を理解し、体験利用することでどのようなものを理解する。

<講習内容>

1. インターネットプロトコルの復習
2. DNSの役割 — クライアントにおけるDNSサーバの指定実習
3. 経路制御（会場内ネットワーク構築実習）
4. IPv6概説 — 解説とノートPCのIPv6機能の設定と確認

【第3限：Fクラス ファイアウォール・ゲートウェイ、IDS（ネットワーク型侵入検知システム）の運用管理】

対象者：ネットワークセキュリティのことは一応知っているが、実際にセキュリティ対策機器操作の経験が浅いが、IDSやファイアウォール・ゲートウェイの導入を検討しているのでその動作原理をきちんと理解したいネットワーク管理者。管理のためのUNIX基本操作ができること、テキストエディタが使えること、プログラムのコンパイル経験があること。

ねらい：オープンソースのファイアウォール・ゲートウェイ、およびネットワーク型侵入検出システムを実際に使用し、その機能を理解する。

<講習内容>

1. FWGW（ファイアウォール・ゲートウェイ）
各自のノートPCルータを用いた実習
2. IDS（ネットワーク型侵入検出システム）
オープンソースNIDS(snort)の設定と運用
※ EおよびFクラスではノートPCの持込が必須となっています。指定のWebページにて必要な機材を確認のうえ、持参可能な場合のみお申込下さい。

【共通プログラム】

各コース共通のプログラムです。

<1日目>

◇最近の学外接続サービス事例紹介

◇ネットワークセキュリティポリシーの考え方

<2日目>

◇学内LAN管理委託業務の事例紹介 ◇質疑応答

4. 日程：平成14年8月6日（火）、7日（水）

5. 会場：東洋大学白山キャンパス
6. 募集定員：会場イA1, A2, B1, B2クラス：各90名
 会場ロC', D'クラス：各80名
 会場ハC, Dクラス：各60名
 会場ニE, Fクラス：各40名

※会場の都合により、応募者多数の場合には参加人数を調整することがあります。

(2) 開催結果と次年度開催計画の検討

参加者は122大学、9短期大学から計230名であった。その内、初級クラス約100名、中級クラス約80名、上級クラス約45名であった。開催結果の詳細は、(資料編【資料13.学内LAN運用管理講習会関係資料】)を参照されたい。本年度は、試行的にアラカルト形式を取り入れたが、希望通りのクラスを受講できなかった参加者があった。また、実習時間の割り当てが十分でなく、消化不良が生じたクラスがあった。テーマごとに講習を受ける要望が大きいことから、講習内容を見直し、受講クラスを増やすよう企画している。

クラスDコース

5. Network File System(16)

■クライアント側の設定(続き)

リモート資源だけをアンマウントするには次のようにします。

```
# umount /usr/man
# umount unixev01:/usr/man
# umountall
# umountall -F nfa
```

利用されているサービスを探る

- TCP/UDPのポートとサービス
 - プロトコルポート:TCP/IPにおけるサービスの終点として使われる
 - 既知ポート番号:標準化されたサービスに割り付けられたプロトコルポート番号(SMTP:25,HTTP:80等)
 - See: <http://www.iana.org/numbers.html>
- ポートスキャンによるサービスの探索
 - 網羅的に既知ポート番号によるアクセスを試す事で、サービスされているものを探索する

その他のパスワード技術

- チャレンジレスポンス方式の認証方法例

④ 認証サーバは保存してあるユーザパスワードと送信したチャレンジコードによりレスポンスコードを生成

```

  graph LR
    User[ユーザ] -- "パスワード  
チャレンジコード" --> Server[サーバ]
    Server -- "ID通知  
チャレンジコード" --> User
    User -- "レスポンスコード" --> Server
  
```

社団法人 独立大学機構教育協会