情報システム工学実験第３K

不要サービスの停止

グループ４

２．不要サービスの停止

- 実験の目的
  - 不要なサービスを停止して、負荷を軽減させる。また、サービスを利用しての不正アクセス、不正行為等を防ぐ（セキュリティの向上を図る）。
- 実験の内容
  - Windows NTおよびVine Linuxで標準で動作している不要なサービスを停止する。

用語の説明 (1)

- 規定のサービス
  - Windows NTは、起動すると自動的にシステムが動作するように設定されている。これを「サービス」と言う。
  - 通常のアプリケーションとは異なり、設定の変更はコントロールパネルから行える。
- Schedule
  - Windowsの規定サービスの一種。
  - atコマンドを用いて、コマンドやプログラムが指定した日時に実行されるように設定できる。
  - 今回は「不要サービス」とする。

用語の説明 (2)

- run level
  - Linuxの起動方法を指定する。
  - ランレベルは０～６まであり、変更することによって動作を変えることができる。そのため起動されるプログラムも変わる。
  - 各サービスのランレベル設定状況は「/etc/inittab」に記載されている。
- inetdまたはxinetd
  - inetdとは、プロトコルの着信を監視し、それぞれのプロトコルのを処理するサーバプログラムを起動するシステム。いわゆる、各種サーバを管理するサーバ。
  - xinetdはinetdの機能拡張版である。IPアドレス制限、時間帯制限などのTCI Wrapperがカバーしていたものも設定できるようになった。

run levelの説明 (1)

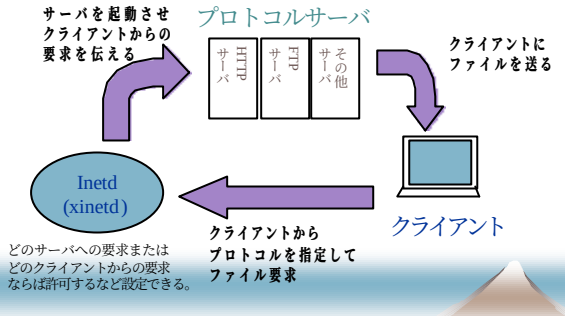
- run levelの意味
  - **ランレベル０**：シャットダウン（システムの停止）
  - **ランレベル１**：シングルユーザモード（rootのみ）
  - **ランレベル２**：ネットワークなしのマルチユーザモード
  - **ランレベル３**：通常のマルチユーザモード（テキストログイン）
  - **ランレベル４**：未使用
  - **ランレベル５**：X11
  - **ランレベル６**：システムの再起動
- 現在各グループのVine Linuxはコンソール画面でログイン（テキストログイン）しているので、ランレベルは３となる。

run levelの説明 (2)

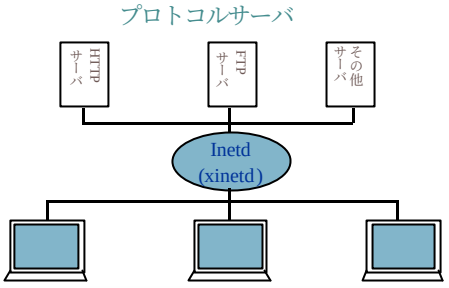
- chkconfigコマンド（後ほど詳しく説明）を用いてどのサービスを、どの起動方法の時に立ち上げるかどうかを設定することができる。
- 例
  - httpdサービスについて。chkconfigコマンドを用いてhttpdサービスの設定状況を調べた。

    `httpd 0:off 1:off 2:off 3:on 4:on 5:on 6:off`
  - 先頭がサービス名、番号がランレベル、ONが起動、OFFが停止。
  - つまり、「通常のマルチユーザモード」と「グラフィカルログインによるマルチユーザモード」の場合でログインしたら、httpdサービスが起動する。

Inted(xinetd)の説明



inetdの木構造



実際の使われ方

- セキュリティ向上
- リソース節約

Windows NTの作業手順 (1)

- Windowsサービスの調査からパネル表示手順まで
  - ← コントロールパネルを開く。
  - ↑ 「サービス」のアイコンをダブルクリック。サービス一覧表が表示。
- サービスの停止方法
  - ← 表示されたサービスの一覧から停止したいサービスを選択する。
  - ↑ 停止ボタンをクリック。（※この時、停止するサービスに別のサービスが従属している場合は警告メッセージが表示される）
  - → そのサービスを停止して良いか、ダイアログが表示されるので「はい」を選択する。
- サービスの起動条件の変更
  - ← 起動条件を変更したいサービスを選択してダブルクリック。
  - ↑ 出てきた画面の上半分にあるスタートアップの種類から選択。

Windows NTの作業手順 (2)

- パネルの説明
  - **サービス：**サービスの名称
  - **状態：**サービスの状態
    - 開始
    - 一時停止
    - 停止（空白で表示）
  - **スタートアップ：**サービスのスタートアップの種類
    - 自動（システム起動のたびにサービス開始）
    - 手動（ユーザor所属サービスが開始）
    - 無効（サービスを開始できない）

Windows NTの規定のサービス

- Alerter
- ClipBook server
- Computer Browser
- Directory Replicator
- Eventlog
- Messenger
- Net Login
- Net work DDE
- Network DDE DSDM
- NT LM Security Support Provider
- Remote Procedure Call(RPC) Locator
- RPC Service
- schedule
- Server
- spooler
- UPS
- Workstation

以上計１７種類のサービスがある。

- Schedule以外のサービスで不要と思ったサービスは各グループで停止作業を行う。

Vine Linuxの作業手順 (1)

- chkconfigコマンドについて
  - /etc/rc.d内の各ディレクトリにシンボリックリンクを作成したり、削除したりすることが簡単にできる。
  - run levelの設定状態表示や変更を行うことができる。
  - 詳しい説明の表示は以下のコマンドを入力する。
    - man chkconfig
  - コマンド一覧表は以下のコマンドを入力する。
    - chkconfig --help
  - 現在動かせるサービスサーバ名の表示とrun levelの表示。
    - chkconfig --list

Vine Linuxの作業手順 (2)

- chkconfigコマンドを利用したサービス設定
  - chkconfigコマンドを用いてrun levelを設定し、不要なサービスを停止（OFF）する。
  - 停止するサービスは各グループで考えること。
  - 例えば
    - 外部からの不正侵入を防ぐため、telnetのポートを塞ぐ
    - 使用しないメールデーモンを停止する

など。

Vine Linuxの作業手順 (3)

- inetd.conf (xinetd.conf) の見直し
  - inetdまたはxinetdはinetd.conf(xinetd.conf)に記述されていることを参照してサービスを行っている。
  - inetd.conf (xinetd.conf) を読み返し、設定の内容を理解する。
  - 必要があれば、サーバへの接続許可やクライアントの接続要求を許可するなどのサービス設定変更を行う。

以上を持ちまして
グループ４の発表を終わります。