佐賀大学の端末用LANと Opengate

渡辺義明、江藤博文、大谷誠、
渡辺健次、只木進一

「jus大規模教育用情報環境運用技術シンポジウム2005」 9月21-22日(鳥取環境大学)

「オープン」なキャンパスネットワーク

- 要求
  - ロビーや教室など自由に出入りできる場所
  - 自由に利用できる公開端末や演習端末の設置
  - NotePCを接続可能な情報コンセントの設置
    （開発当初は無線LANなし、公開端末設置相次ぐ）
- 実現
  - 従来型LANの外に、端末用LANを設置
  - 利用者認証システムOpengateを開発

ネットワーク利用者認証

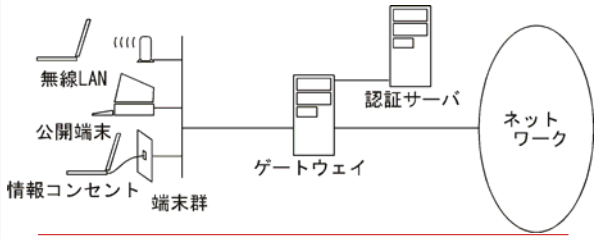
- 必要性
  - 不正侵入・妨害行為、権利侵害行為など頻発
- 機能
  - 利用者の制限
  - 利用者・利用場所・時間の記録・特定
- 要求
  - できるだけ容易に利用
  - できるだけ容易に管理
  - できるだけ多様な環境に適用
    - 公開端末、情報コンセント、（無線LAN）
    - Windows、MacOS,Linux,…

開発経緯

- 1999年8月　Opengateのスクラッチ版稼動
- 2000年6月　情報処理センター内で試験運用
- 2000年9月　学部設置の演習室で試験運用
- 2001年1月　附属図書館で実運用開始
- 2001年4月　全キャンパスに端末用LAN配備、大規模運用開始
- 2001年12月　情報処理学会論文誌掲載
  利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発、渡辺義明、渡辺健次、江藤博文、只木進一、情報処理学会論文誌、Vol42、No.12、pp.2802-2809(2001)
- 2005年4月　情報処理学会論文誌掲載
  利用者移動端末に対応した大規模ネットワークのOpengateによる構築と運用 、只木進一、江藤博文、渡辺健次、渡辺義明、情報処理学会論文誌、Vol.46,No.4,pp.922-929(2005)
- 2005年5月　Version1.0公開、SourceForge登録

ネットワーク利用認証システム Opengate

- ゲートウェイ上のファイアウォールをCGIで制御



動作原理：ファイアウォールルールの追加・削除

```
……
10000 allow ip from 192.168.0.11 to any
10000 allow ip from any to 192.168.0.11
……
60000 fwd localhost tcp from any to any http
65535 deny ip from any to any
```

192.168.0.11への入出力は通過

192.168.0.11からの認証通過時に追加 利用終了時に削除

ここまで不一致のWebアクセスはローカルへ転送

ここまで不一致のパケットは拒否

この順にチェック

利用終了の検知は

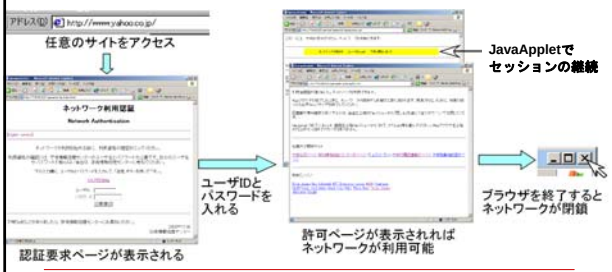
- TCPコネクションの有無では判断不可
- 物理的検知は公開端末に適用不可
- 端末ソフト導入は持参端末に適用難

⇩

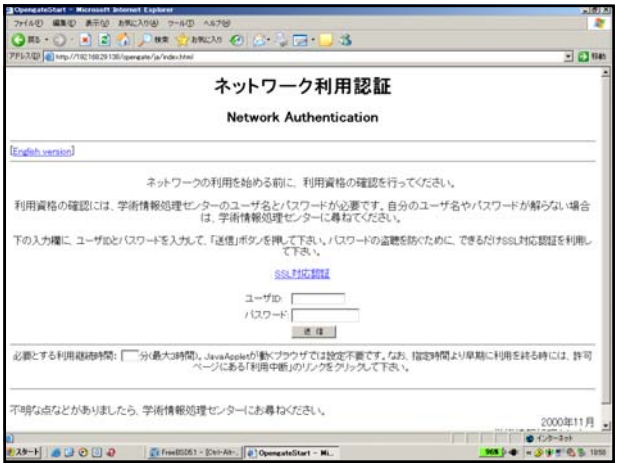
- 認証時にJavaAppletを送り込み、それとコネクションを張る方法を採用
  - JavaAppletなしのときも他のチェックで対応

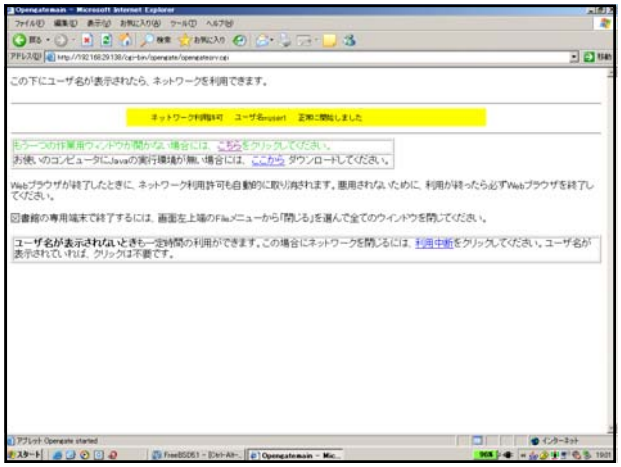
7

利用手順

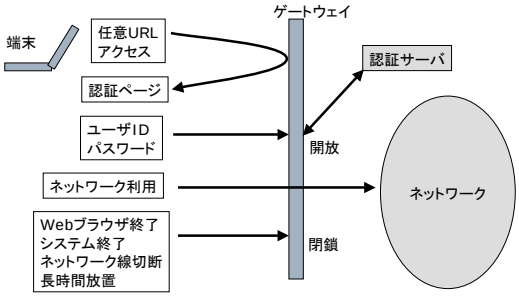


8



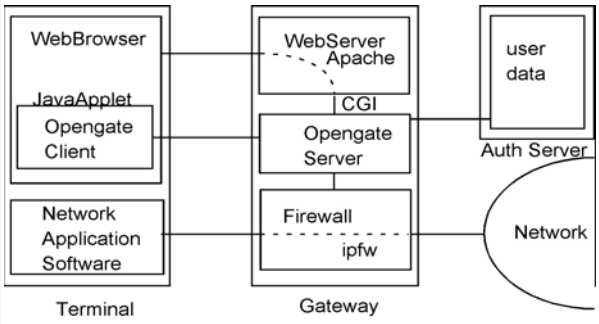


動作概要

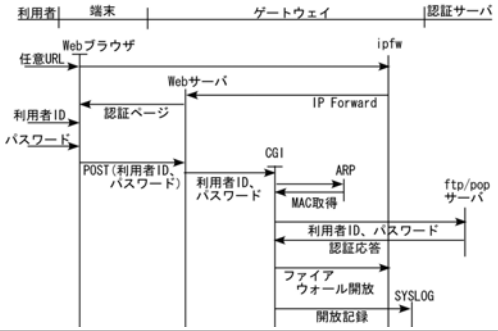


12

ソフトウェア構成

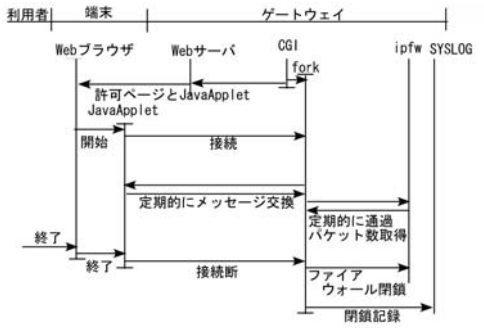


処理フロー



14

処理フロー続き



15

Opengateシステムの構成要素

- クライアント
  - 利用者が利用する端末。JavaAppletが稼動の時はTCPコネクションで利用終了を監視
- ゲートウェイ
  - 通信の制御。CGIプログラムopengatesrv.cgiが認証を行いファイアウォールipfwを開放・閉鎖。CGI制御のWebサーバも稼動
- 認証サーバ
  - 利用者情報の保持と認証応答
- 利用記録サーバ
  - 利用開始時と利用終了時に、日時・ユーザ名・IPアドレス等をsyslog経由で受け取り

16

クライアントマシン

- Webブラウザが稼動すること。JavaApplet稼動を推奨
- ゲートウェイとクライアントの間にアドレス変換機器が無いこと
- TCP/IPによる接続、無線&有線LAN可
- 個人持参PC&固定設置端末可、PDA可
- Windows,MacOS,Linux,FreeBSD, …

17

ネットワーク開放

- ユーザID,パスワードが認証通過すると開放
- 標準では、その端末アドレスへの出入りパケットを全て通過
- ファイアウォールに、優先ルールを設定すれば、特定通信を無条件停止・許可も可能
- ファイアウォール制御のPerlスクリプトを扱えば、条件制御も可能

18

ネットワーク閉鎖

- JavaAppletが有効な場合
  - Webブラウザを終了した（通常終了）
  - JavaAppletの定期交信が失敗した（線切断に対応）
  - 一定時間、クライアントが通信を行わなかった（端末放置に対応）
- JavaAppletが有効でない場合
  - 開放後、利用者が指定した時間が過ぎた
  - 一定時間、クライアントが通信を行わなかった（端末放置に対応）
  - ARPコマンドに対して異なるMACアドレスが返された（端末入替）
  - 閉鎖指示のリンクを利用者がクリックした

19

ゲートウェイマシン

- OS
  - FreeBSD4.0以降
- ハードウェア
  - 上記が稼動可能なもの、Ether NIC　2枚以上
- 必須ソフトウェア
  - Apache、ipfw
- 任意選択ソフトウェア
  - natd、DHCP、SSL、perl

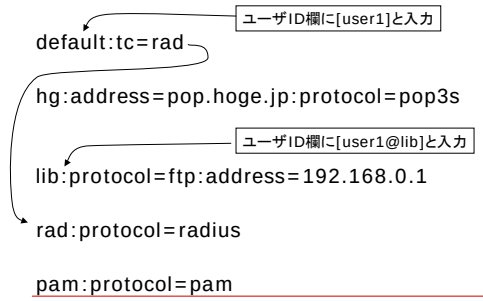
20

認証サーバ

- 対応プロトコル
  - POP3、POP3S、FTP、RADIUS、PAM経由
- 設定
  - 設定ファイルに、連携する認証サーバの詳細を設定
- サーバの選択
  - 利用者IDのみ入力[user]では、標準サーバへ認証要求
  - サーバIDを付加[user@serv]すると、サーバID[serv]のサーバへ、[user]の認証要求。

21

認証サーバ設定例



22

インストール

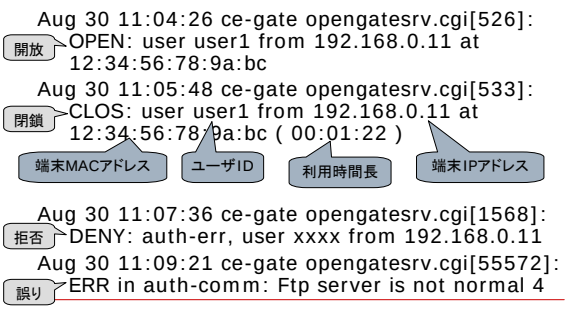
- ファイアウォールipfw付きのカーネルを作成
- 各種ソフトのインストールと動作確認
  - Apache、ipfw 、natd、DHCP、SSL、perl、、
- ファイアウォールを設定し手動で開放・閉鎖確認
- Apacheを設定しページの転送・表示確認

- opengatesvr.cgiのインストールと設定
- 認証サーバとの連携チェック

- ドキュメント・チェックプログラム等用意

23

Syslog出力



24

psコマンドによる現接続状況表示

```
ps -x | grep opengate

525  ??  I      0:00.24 opengatesrv.cgi:
   10000,user1,192.168.0.11

533  ??  I      0:00.01 opengatesrv.cgi:
   10002,user2,192.168.0.15
```

ファイアウォール ルール番号　ユーザID　端末IPアドレス

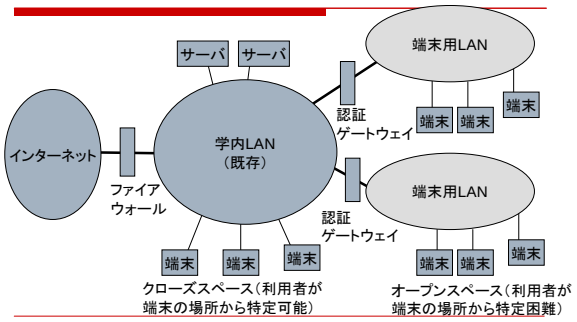
25

特長

- 利用が容易
  - 任意URLへのアクセスで認証要求ページ
  - ブラウザを閉じるとネットワーク閉鎖
  - 端末ソフトのインストール等が不要
- 管理が容易
  - ゲートウェイのみ管理（UNIX管理の知識は必要）
  - 既存認証サーバ利用可(POP,POPS,FTP,RADIUS,PAM)
  - 既存ネットワーク環境に導入容易
- 多様な環境に適用
  - 無線/有線、公開設置/持参端末、Windows/Mac/Linux、、
  - Java稼動のWebブラウザのみ要求、Javaなしでも利用可能
    （一定時間経過、利用者の操作、MACアドレス変化、無パケット等で閉鎖）

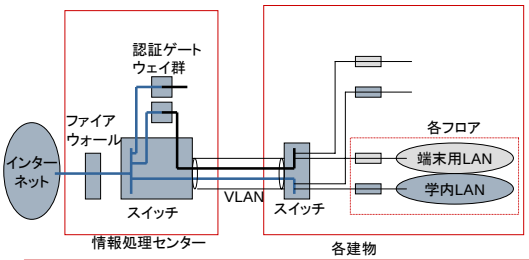
26

端末用LAN



27

実際の配線



28

端末用LAN規模

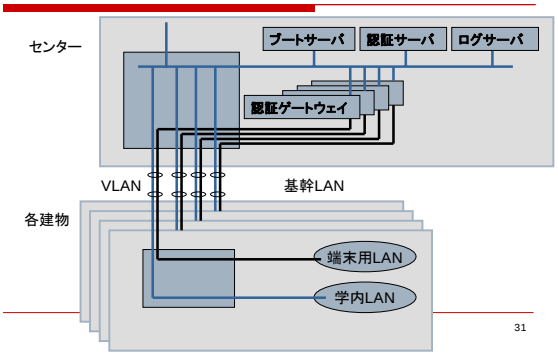
- ほぼ建物ごとに1台の認証ゲートウェイ（22台）
- 公開設置端末（約110台）
  - 図書館、各学部設置演習室、就職相談室など、既存端末を取込み
- 情報コンセント（約730口）
  - ほぼ全教室（各2口）、図書館、学生居室等に設置
- 無線LAN(約87箇所）
  - ほとんどの教室から利用可能な位置、図書館等に設置
- 利用登録者（約10000人）

29

認証ゲートウェイ群

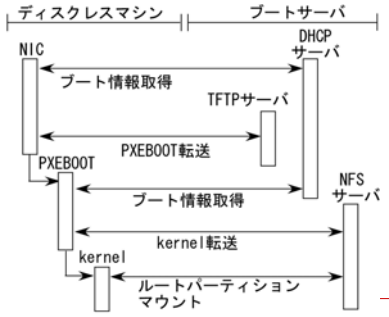
30

サーバ構成



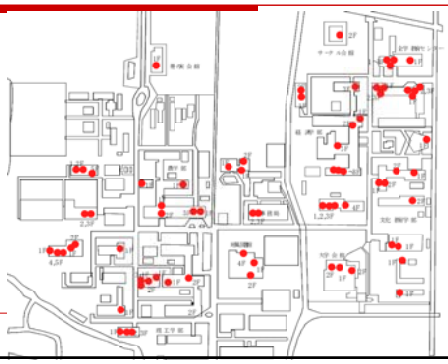
31

ディスクレスブート



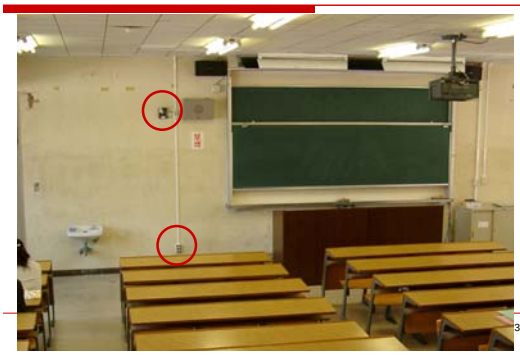
32

無線LAN配置



33

講義室



34

廊下

35

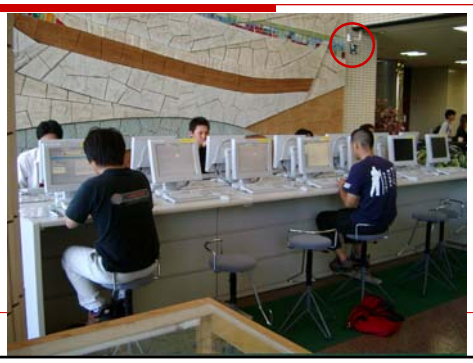
大学会館

36

附属図書館

37

附属図書館



38

附属図書館

39

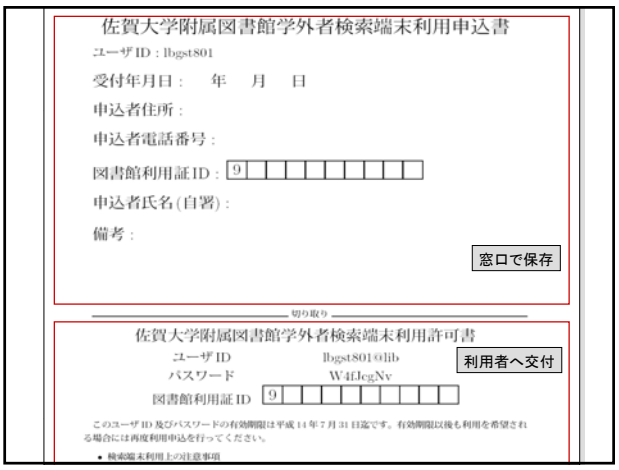
就職相談室

40

運用

- 学内利用者
  - センターの利用者IDとパスワードで利用
  - 接続申請不要でどこでも自由に
  - 情報リテラシー教育以外に特別な利用指導なし
- 学外利用者
  - 図書館学外利用者、学会参加者、一時滞在者等
  - 窓口で申請すると期限付き利用者IDとパスワード
  - 一時利用認証サーバで、ネット利用権のみ付与

41



佐賀大学附属図書館学外者検索端末利用申込書

ユーザID：lbgst801

受付年月日：　年　月　日

申込者住所：

申込者電話番号：

図書館利用証ID：9

申込者氏名(自署)：

備考：

窓口で保存

切り取り

佐賀大学附属図書館学外者検索端末利用許可書

ユーザID　lbgst801@lib

パスワード　W4fJcgNv

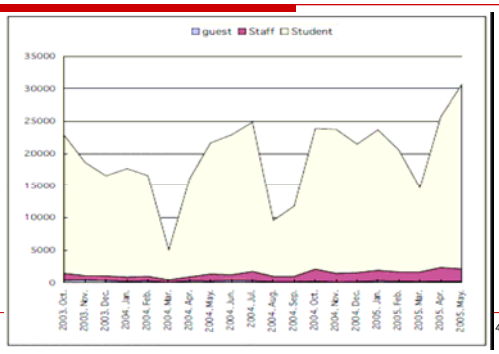
図書館利用証ID　9

利用者へ交付

このユーザID及びパスワードの有効期限は平成14年7月31日迄です。有効期限以後も利用を希望される場合には再度利用申込を行ってください。

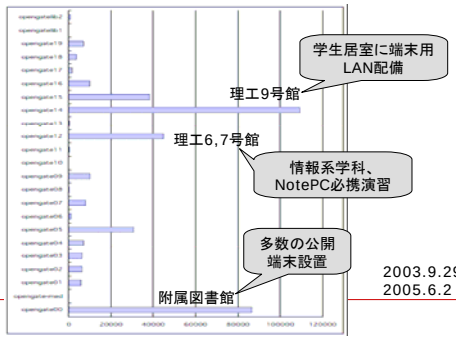
・検索端末利用上の注意事項

利用者数の推移



43

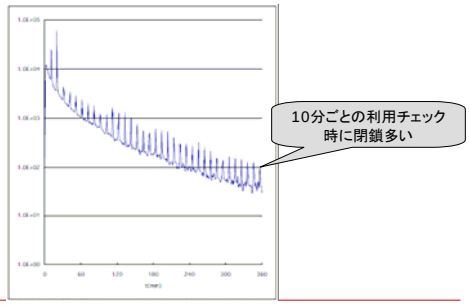
ゲートウェイごとの利用者数



2003.9.29-2005.6.2

44

利用継続時間分布



45

利用状況・パフォーマンス

- 利用状況
  - 公開端末、学生居室配備、ノートPC利用学科が利用多
  - 2004年前半：のべ14万回接続、実利用者数6,000名
    （学生・職員数の合計、約10,000名に対して）
  - 一時利用者サービスも好評
    (図書館外部利用者、学会利用者、一時滞在者)
- パフォーマンス
  - ゲートウェイ機：PentiumIII 1GHz、512MBメモリ、HDD無し
  - 100人規模のNotePC利用演習実施
  - 40Mb帯域3時間のDVTSビデオ中継実施
  - ウイルスの大量パケット送信で、NAT処理あふれによる停止
    （MSBlaster感染1端末でNAT処理がCPUの20%、ping拒否設定で対応）

46

運用上の諸工夫

- 遠隔施設のつなぎこみも端末用LANへ
  - 学生等の自由利用希望、ファイアウォール設定で職員PCのみ自動通過、他は認証
- ウイルス対応
  - ファイアウォール設定でウイルス利用ポートを閉鎖
- ゲートウェイマシンのトラブル
  - 他のマシンに配線入れ替えで即時肩代わり
- 一時的なネットワーク利用制限の強化や撤廃
  - ファイアウォール設定で実施
- 端末用LANの増設、一時的設置
  - スイッチへの差込位置変更で、学内LANと端末用LANを切替
- ネットワーク不審利用の調査
  - 認証ゲートウェイにおける監視、ログ利用

47

経験した障害の原因

- クライアントPC：大多数
  - LAN設定の不備（自宅でのネット接続設定がそのままなど）
  - ネットワークカードのハード故障
  - Javaが無効（この場合、使えるが一定時間で閉鎖）
- ネットワーク機器
  - アンテナ、スイッチのハード故障
- サーバ機：極めて少
  - DHCPサーバの停止
  - ウイルス大量パケットによるNAT処理あふれ
  - ハード故障

48

コスト

- 金銭的コスト
  - 通常のPC機を必要区画分
  - ネットワーク配線、無線LAN配備
    - 基幹LAN整備の一環として整備
- 人的コスト
  - 導入：FreeBSDの平均的インストール＋ファイアウォール、Webサーバ、DHCP、CGI等
  - 運用：トラブル無ければ全く手間無し
    - サーバ停止：サーバ電源ON/OFFでリブート、直らなければ他のサーバへつなぎ代えて、後でゆっくり調査
    - 不正発見：各種ログ調査、ネットワーク監視など
    - OS等のセキュリティホール：クリティカルな場合はシステム再構築
  - 認証サーバの利用者管理は手間、共通システムを利用要

49

関連したシステム開発

- 公開端末にキーロガーが仕掛けられる
  - Opengateと連携したシステム起動時認証の開発
- Webでの認証は面倒
  - Javaによる認証クライアントの開発
- IPv6の普及
  - IPv4とIPv6の両方を一度の認証で開放したい
  - Ipv6対応Opengateの開発
- 開発環境の見直し
  - JavaServletを利用したOpengateの試作

50

オープンソース

- GNU Public License で公開

  http://www.cc.saga-u.ac.jp/opengate

  http://sourceforge.net/
  projects/opengateproject

51

公開サイト

52

他の認証ネットワーク構築方法

- VLANを切り替え⇒対応機器分散配置
- VPNの利用⇒クライアント制限、パフォーマンス
- 登録MACアドレスのみ開放⇒管理手間
- SSH接続維持の間のみ開放⇒利用方法難
- HTTP REFRESHで定期チェック⇒閉鎖遅延
- IEEE802.1X⇒クライアント制限
- その他各種アプライアンス⇒価格、柔軟性

53

関連システムのリンクサイト

- オープンアクセスフロア(仮称)運用実験 – 名大
  http://www.cc.hit-u.ac.jp/
  monban/ref.html
- PortalSoftware – Personal Telco
  http://wiki.personaltelco.net/
  index.cgi/PortalSoftware

54

大規模導入の留意点

- 管理容易性： 既存認証方式に対応できるか。ネットワーク機器や端末の個別管理が必要か。利用に際して講習や端末へのソフト導入・設定が必要か。システムの維持管理は容易か。障害対応は容易か。
- 利用容易性： 利用者にとって直感的な利用形態か。即時利用可能か。一時利用者は容易に受け入れ可能か。
- 端末互換性： OS (Windows, MacOS, Linux等）や設置形態（モバイル・固定設置等）、接続形態（有線・無線等）にどこまで対応可能か。
- システム互換性： 既存のシステム・ネットワークへの追加導入は容易か。逐次的拡張は可能か。関連システムやネットワークの構成は柔軟に変更可能か。汎用的なハード・ソフトを利用か。将来の技術進歩に耐えうるか。
- 柔軟性： ネットワークの一部開放・閉鎖等、柔軟な制御が可能か。
- セキュリティ： 利用者の怠惰で穴が発生しないか。盗聴への対応は可能か。
- 低廉性： 特殊・高価な機器を使用するか。機器の大量導入が必要か。
- 継続性： 技術進歩の中、サービスを継続して維持できるか。より良いシステムが出たときに移行は容易か。

55