# 利用者用ネットワークと統合認証

只木進一
佐賀大学学術情報処理センター

©S. Tadaki Computer and Network Center, Saga University

## 本日の論点

- 利用者用ネットワーク
  - どこでもネットワーク
  - 利用者が持ち込むノート型PC
  - 認証と記録
  - Opengate
  - 大規模運用:ディスクレスサーバ
- 統合認証
  - 利用者用ネットワークの認証基盤
  - 全学規模の認証
  - 情報システムに共通な情報の一元化

©S. Tadaki Computer and Network Center, Saga University

## 新しいタイプの情報基盤の必要性

- 教員が携帯する端末
  - 講義でネットワークを使いたい
  - 会議でネットワークを使いたい
- 学生が携帯する端末
  - 講義でネットワークを使いたい
  - 図書館でネットワークを使いたい
- 来学者が携帯する端末
  - 携帯した端末でネットワークを使いたい
- 空港、駅、ホテルのインターネット接続サービス
- 端末用ネットワークという新しいネットワーク

©S. Tadaki Computer and Network Center, Saga University

## 普通のネットワーク

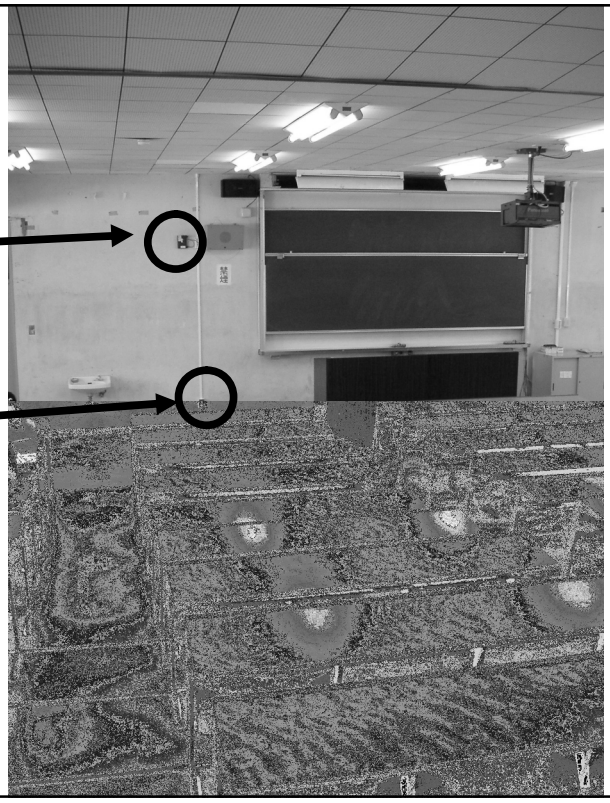
- 部局ごとのサブネット
  - 端末に固定IPアドレス
  - 端末と利用者を紐付け
  - 接続申込
- 一旦接続すると、放置状態
  - アドレスをもらったら勝ち?
- 携帯型端末に対応できない
- 学生・来訪者
  - 部局の判断でヤミで接続
- ウィルスやP2Pの蔓延

©S. Tadaki Computer and Network Center, Saga University

# 利用者用ネットワークの要件

- 簡単に使える
  - 移動型情報端末が有線/無線で接続できる
  - 特別な申請をしない
  - 特別な操作をしない :簡単な操作
  - 特別な機器を求めない :利用者
  - 広範な利用者に対応できる
- 大規模に運用できる
  - 特別な機器を使わない
  - 利用者管理ができる
  - 利用記録が残る
- オープンスタンダードに対応しなきゃ

©S. Tadaki Computer and Network Center, Saga University




電源が無い(^^;

## よくある利用者(ゲスト)用ネットワーク

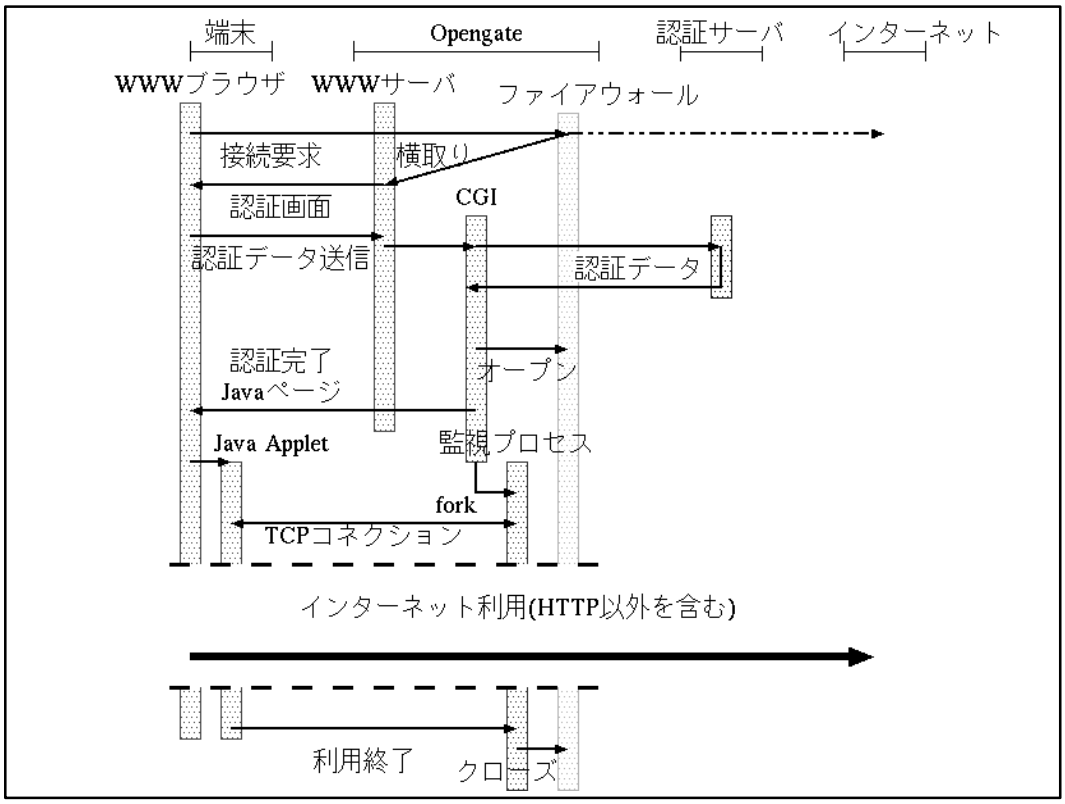
- 面倒な接続手順
  - 特定のWebにアクセスする
  - 特定のキーを取得する
- 特定のポートしか通せない
  - 80番しか通らない :メールは読めない
  - アクセス先のポリシーと合わない
  - かえって、トンネルを掘られてしまう危険性
- 特定のOSやブラウザしか対応できない
- 外部の人間には使わせない(^^;

©S. Tadaki Computer and Network Center, Saga University

## Opengate

- Web ブラウザ起動を契機に認証を行う
  - 特別な操作は無い
  - 特別なソフトウェアが不要
- 認証後にfirewallを開く
- Web ブラウザにappletを落す
  - TCPセッションを開き、利用をモニタ
  - 利用を記録する
- ブラウザ停止でfirewallを閉じる
  - 空きっ放しポートの不正利用を防ぐ

©S. Tadaki Computer and Network Center, Saga University




# Opengateの特徴

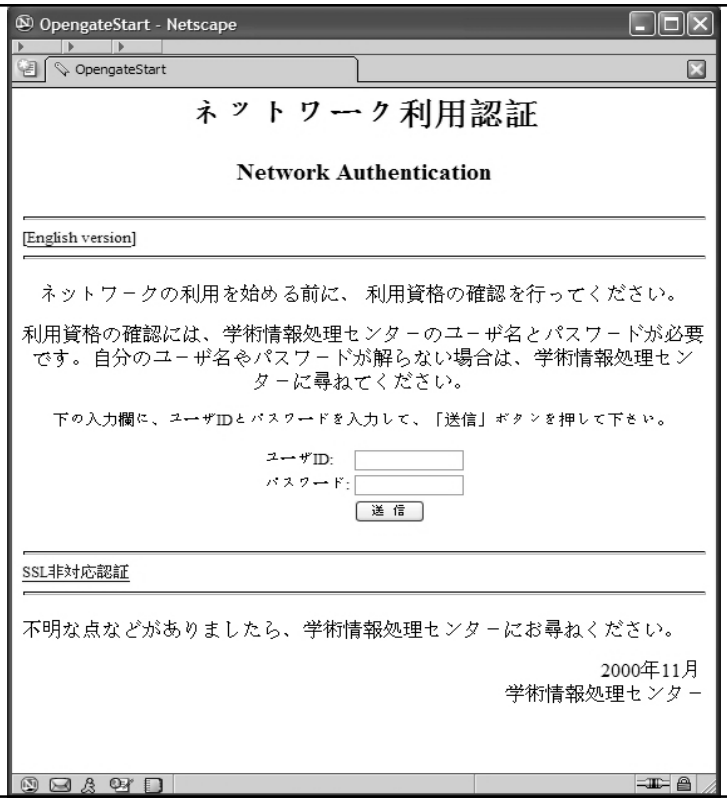
- Web ブラウザとjreだけしか求めない
- クライアントのOSを縛らない
- 特殊なネットワーク機器を求めない
  - GatewayはFreeBSD
- 外部認証サーバを使う
  - 既存の認証を使える
  - 特別な利用登録が不要
- 利用終了時に直ちにfirewallを閉じる

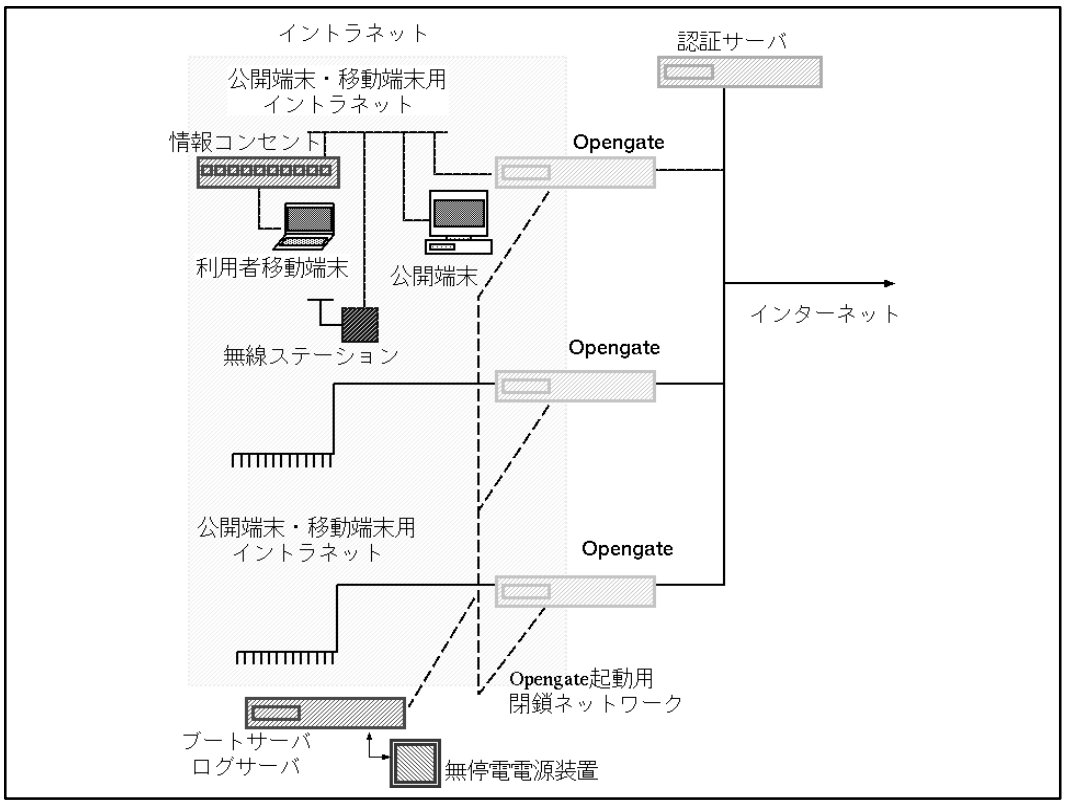
©S. Tadaki Computer and Network Center, Saga University

# Opengate構成要素

- OS :FreeBSD
- ファイアウォール :ipfw
- Web Server :Apache
- CGI :C プログラム
- Java Applet
- NAT
- DHCP

©S. Tadaki Computer and Network Center, Saga University




イントラネット
認証サーバ
公開端末・移動端末用
イントラネット
情報コンセント
Opengate
利用者移動端末
公開端末
インターネット
無線ステーション
Opengate
公開端末・移動端末用
イントラネット
Opengate
Opengate起動用
閉鎖ネットワーク
ブートサーバ
ログサーバ
無停電電源装置

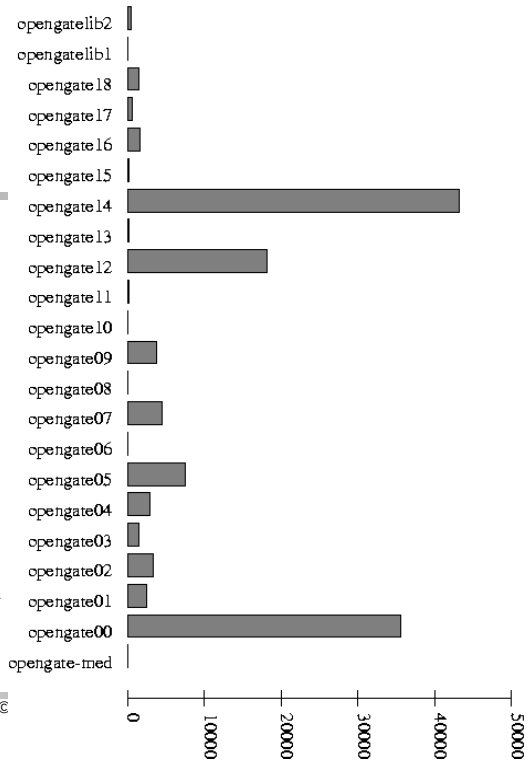
# 設置概要

- 概ね建物ごとにOpengateを設置 :20台程度
- ひとつのネットワークをあまり大規模にしない
  - 携帯型PCは十分に管理されていない
  - ウィルス活動を小規模に抑える
  - コトが起こったときに、人と場所を特定する
- Opengateの障害時に他のOpengateに切替える

©S. Tadaki Computer and Network Center, Saga University

# 利用状況

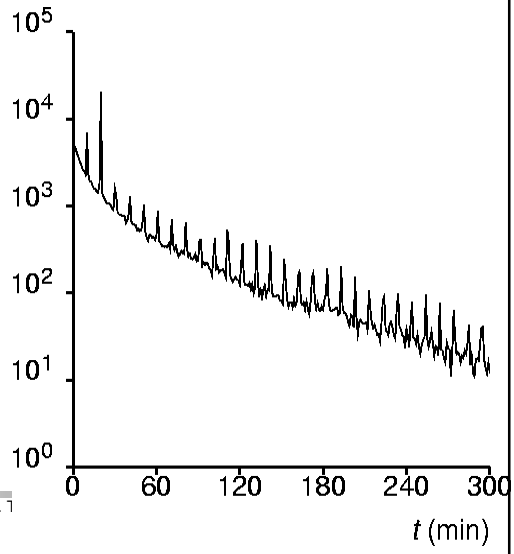
- 2003/9/29から2004/6/8
- 利用累計時間
- Opengate14:化学系
  - 学生の個人PC
- Opengate12:情報系
  - 全学生が携行
  - プログラミング演習
- Opengate00:図書館
- 全構成員の半数以上が利用




©

# 利用状況

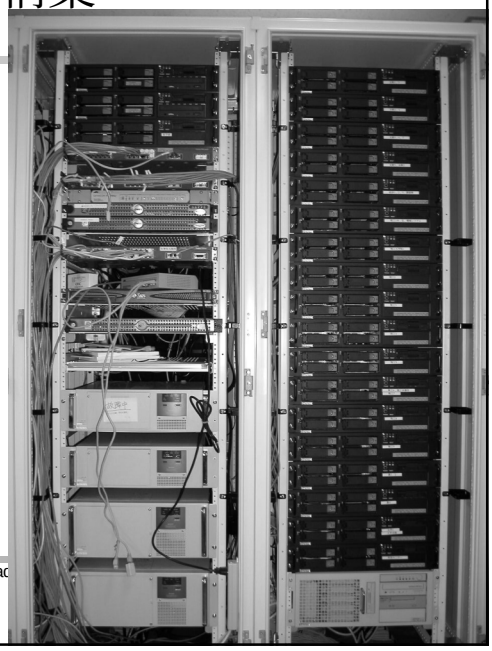
- 利用時間分布
- 指数分布
- 非常に長時間の利用者も居る :繋っ放し
- 放置端末の強制切断によるピーク




©S. T

# ディスクレスサーバの構築

- 多数のOpengateはIPアドレスなど少数の設定を除いて同じ
- FreeBSDのディスクレス機能を活用
- 起動サーバに設定DB
  - 設定ファイル自動生成
- 障害時の入れ換え、増強が容易



©S. Tac

## 検疫的成果

- ファイアウォールのログのチェック
  - ウィルス活動の早期発見
  - P2P的挙動の早期発見
  - 認証ログから持ち主を特定し対処
- 認証を持たない公開端末の認証
  - OpengateLogin

©S. Tadaki Computer and Network Center, Saga University

## 追加的機能

- 多言語対応
- 暗号通信
- 利用者による切断時間設定
- IPv4/IPv6同時対応

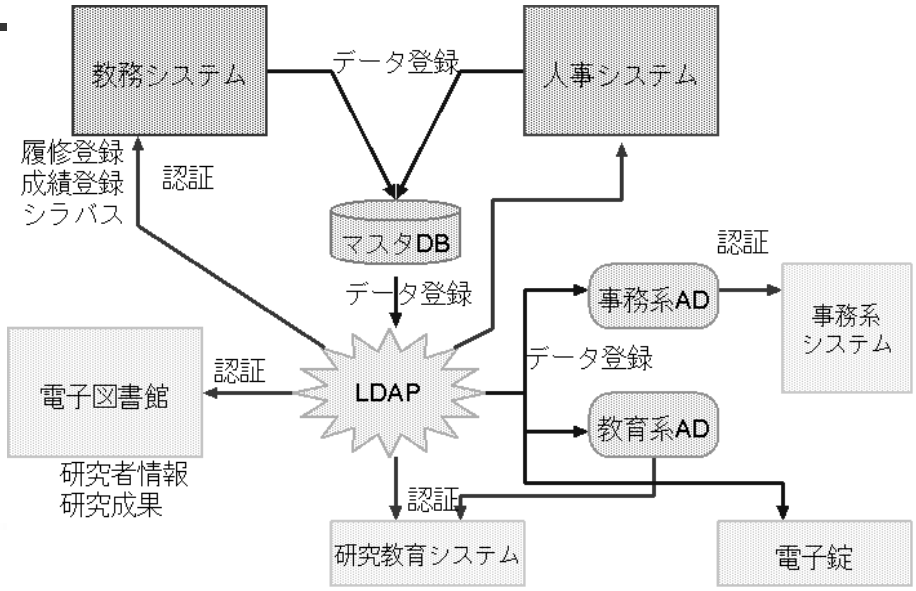
©S. Tadaki Computer and Network Center, Saga University

## 統合認証とは何か

- 全学に共通認証を提供する
- 全構成員のデータベース
- 教育研究用システムへの認証提供
- 電子図書館・図書館業務システムへの利用者情報提供
- 各種Webシステムへの利用者情報提供
- 教務システムへの利用者情報提供：構築中
- 電子錠システムへの利用者情報提供：計画中

©S. Tadaki Computer and Network Center, Saga University

## 統合認証システムの構成



# 統合認証システムの主要構成

| サーバ | 構成 | 主たる機能 |
|---|---|---|
| 認証DB | Sun Fire V20z / Solaris 10 / PortgreSQL | 全利用者(非活性を含む)のユーザ名、氏名、所属などを保持 |
| LDAP主サーバ | Sun Fire V20z / Solaris 10 / Openldap | 全利用者(非活性を除く)のユーザ名、氏名、所属などを保持 |
| LDAP副サーバ (5台) | Sun Fire V20z / Solaris 10 / Openldap | 全利用者(非活性を除く)のユーザ名、氏名、所属などを保持 |
| Active Directory サーバ (5台) | Xeon 3.2GHz / Windows 2003 Server | LDAPから情報取得 / Windows クライアント認証 |
| 認証管理サーバ | Sun Fire V20z / Solaris 10 / Apache | パスワード変更 / 利用者管理作業 |

2006年3月稼働予定システムの構成

©S. Tadaki Computer and Network Center, Saga University

# 統合認証と利用者用ネットワーク

- 全学生 ･全教職員のデータベース
  - LDAPとADを使った端末/サーバ認証
  - IMAPSを使って、CGI/PHPなどから認証
- Opengateは多様な認証プロトコルに対応
- 統合認証システムを使った認証
  - 特別な利用登録は不要
- Opengateは認証サーバを複数指定可能
  - 外来者用認証サーバ
  - 外来者用IDが常に準備されている

©S. Tadaki Computer and Network Center, Saga University

# 統合認証の課題

- コンピュータシステムの構築は容易
  - 必要とするデータの洗いだし
- データ登録体制が問題
  - 人事、教務、教育研究の連携が必要
  - それぞれの作業手順の差
- 必要なことはわかりきっているが

©S. Tadaki Computer and Network Center, Saga University