社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－ＱＡＩ－21（３）
2006／10／23

[招待講演] キャンパス共通認証・認可システムが拓く高度な研究・教育のための情報通信基盤

飯田 勝吉†

†東京工業大学 学術国際情報センター

〒152-8550 東京都目黒区大岡山 2-12-1-E2-9

E-mail: †iida@gsic.titech.ac.jp

あらまし 東京工業大学（以下東工大）では、先進的な研究、教育環境を実現するための情報通信基盤（Information Communication and Technology: ICT） infrasturcture を整備している。その大きな３つの柱は、共通コンピューティング資源としてのスパコン・グリッド TSUBAME、ネットワークアクセス環境としてのキャンパス無線 LAN、そして、キャンパス共通認証・認可システムがある。本稿では東工大の情報通信基盤の３つの柱を紹介し、その後キャンパス共通認証・認可システムを紹介する。キャンパス共通認証・認可システムは、キャンパス共通個人情報ディレクトリシステム（LDAP サーバ）、ウェブシングルサインオンシステム等から構成されるもので、東工大の在籍者に特別な手続きを強いることなく、東工大に在籍するだけで利用可能となる情報システムのアカウント（IC カード）を提供する。当該システムの特徴は、利便性、セキュリティ、管理性などを考慮にいれて設計されたことであり、2006 年４月から運用を開始した。当該システムの設計理念や各種課題を克服するためのシステム設計等について説明する。

キーワード 認証、認可、IC カード、PKI、LDAP、ウェブシングルサインオン、キャプティブポータル認証

Campus-wide authentication and authorization system: Construction of ICT infrastructure toward advanced research and educational environment

Katsuyoshi IIDA†

† Global Scientific Information and Computing Center, Tokyo Institute of Technology,

2-12-1-E2-9, O-okayama, Meguro-ku, Tokyo, 152-8550 Japan.

E-mail: †iida@gsic.titech.ac.jp

Abstract Tokyo Institute of Technology (Tokyo-Tech) is now expanding its own Information and Communication Technology (ICT) infrastructure to achieve advanced research and educational environment. It includes three major components; SuperComputing Grid called TSUBAME for providing shared computing resources, campus-wide wireless LAN for providing ubiquitous network access entire campus, and campus-wide authentication and authorization (CWAA) system. In this paper, we first outline three major computes then go into the detail of CWAA. The campus-wide authentication and authorization system, which consists of the campus-wide member directory (LDAP server) and web single-signon servers, provides ICT accounts using smartcards, to Tokyo-Tech members without special paperwork. The CWAA system, which startetd in operation from April 2006, was designed to take into account various aspects such as ease-of-use, security and management-ability. We explain its design concept as well as technical difficulties we attacked.

Keyword Authentication, authorization, smartcard, PKI, LDAP, web single-signon, captive-portal authentication..

キャンパス共通認証・認可システムが拓く高度な研究・教育のための情報通信基盤

東京工業大学
学術国際情報センター
飯田勝吉(いいだかつよし)
iida@gsic.titech.ac.jp

キャンパスICT環境の発展(1)

- これまでのキャンパスICT環境
  - アプリケーション
    - 電子メール:学内限定、POP
    - ウェブアクセス、ウェブサーバ設置
  - 実現方法
    - 各部局、各研究室で個別に実現
  - ネットワーク
    - 研究室、事務室の固定端末、アドホックな無線LAN

キャンパスICT環境の発展(2)

- 今後登場が期待されるアプリケーション
  - オンラインウェブアプリケーション
    - 教務用システム:履修申告、成績確認
    - 研究用システム:共有計算資源、研究業績管理
    - 共通アプリケーション:人事給与管理、ウェブメール、オフィスソフト、などなど

キャンパスICT環境の発展(3)

- 集中化とサービスのバーチャルホスティング
  - 個別導入の弊害
    - コストの増加、利便性・セキュリティレベルの低下
  - 少なくとも学内の各システムの連携が必要
  - ICTサービスホスティング環境を構築
    - サービスホスティング環境上にサービスを設置

本日の講演概要

- 東京工業大学の情報通信基盤
- キャンパス共通認証・認可システム

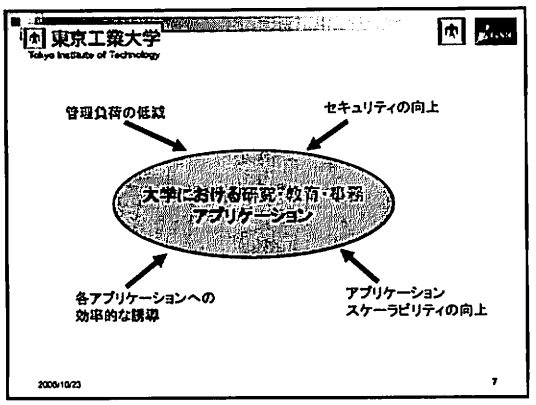
東京工業大学 Tokyo Institute of Technology

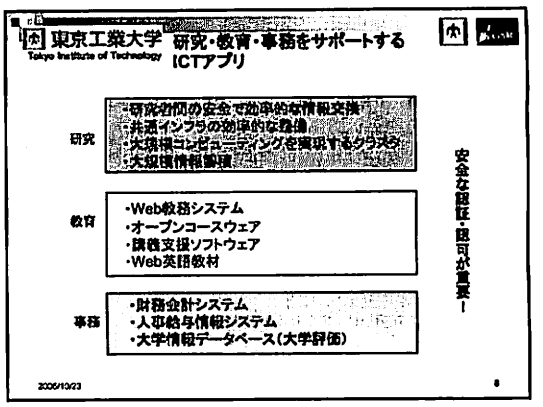
現在の国立大学の置かれた環境

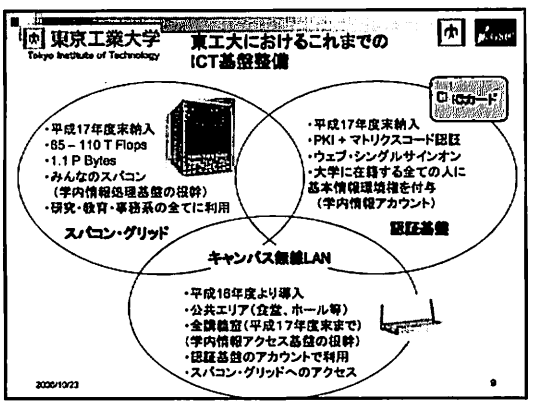
- 激しい競争
  - 少子化による学生確保の困難さ増大
  - COE等競争的研究資金の拡大
- 効率的な経営
  - 効率化係数による法人運営費の削減
- 大学評価の拡大
  - 機関別認証評価
  - 民間の各種評価

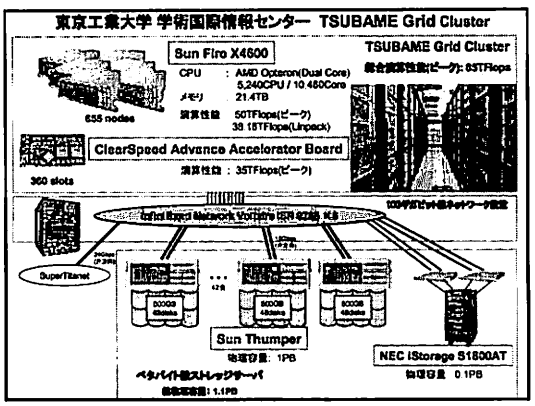
⇩

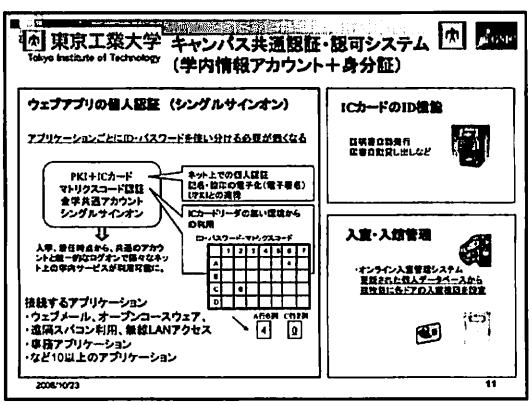
安全で効率的なICTアプリケーションの導入促進が有効

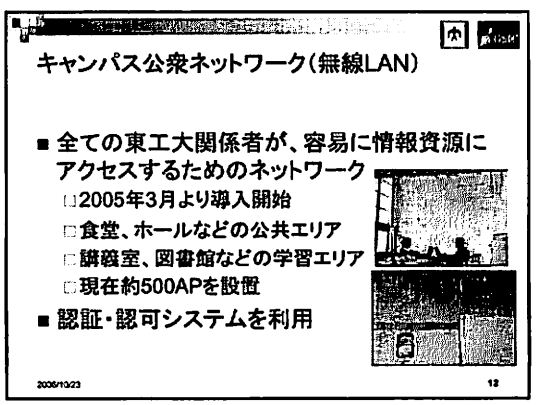

東京工業大学
Tokyo Institute of Technology
管理負荷の低減
セキュリティの向上
大学における研究・教育・事務
アプリケーション
各アプリケーションへの
効率的な展開
アプリケーション
スケーラビリティの向上
2005/10/23
7


東京工業大学
Tokyo Institute of Technology
研究・教育・事務をサポートする
ICTアプリ
研究
・研究者間の安全で効率的な情報交換
・共通インフラの効率的な整備
・大規模コンピューティングを実現するクラスタ
・大規模情報蓄積
教育
・Web教務システム
・オープンコースウェア
・講義支援ソフトウェア
・Web英語教材
事務
・財務会計システム
・人事給与情報システム
・大学情報データベース(大学評価)
安全な認証・認可が重要！
2005/10/23
8


東京工業大学
Tokyo Institute of Technology
東工大におけるこれまでの
ICT基盤整備
ICカード
・平成17年度末納入
・85－110 T Flops
・1.1 P Bytes
・みんなのスパコン
(学内情報処理基盤の役幹)
・研究・教育・事務系の全てに利用
スパコン・グリッド
・平成17年度末納入
・PKI＋マトリクスコード認証
・ウェブ・シングルサインオン
・大学に在籍する全ての人に
基本情報環境権を付与
(学内情報アカウント)
認証基盤
キャンパス無線LAN
・平成18年度より導入
・公共エリア(食堂、ホール等)
・全講義室(平成17年度末まで)
(学内情報アクセス基盤の役幹)
・認証基盤のアカウントで利用
・スパコン・グリッドへのアクセス
2005/10/23
9

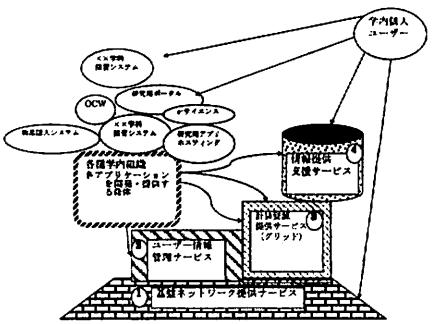

東京工業大学 学術国際情報センター TSUBAME Grid Cluster
TSUBAME Grid Cluster
Sun Fire X4600
CPU : AMD Opteron(Dual Core)
5,240CPU / 10,480Core
メモリ 21.4TB
655 nodes
ClearSpeed Advance Accelerator Board
360 slots
SuperTitanet
Sun Thumper
NEC iStorage S1800AT


東京工業大学
Tokyo Institute of Technology
キャンパス共通認証・認可システム
(学内情報アカウント＋身分証)
ウェブアプリの個人認証 (シングルサインオン)
アプリケーションごとにID・パスワードを使い分ける必要が無くなる
PKI＋ICカード
マトリクスコード認証
全学共通アカウント
シングルサインオン
ICカードのID機能
入室・入館管理
接続するアプリケーション
・ウェブメール、オープンコースウェア、
・遠隔スパコン利用、無線LANアクセス
・事務アプリケーション
・など10以上のアプリケーション
2005/10/23
11


キャンパス公衆ネットワーク(無線LAN)
■ 全ての東工大関係者が、容易に情報資源にアクセスするためのネットワーク
□2005年3月より導入開始
□食堂、ホールなどの公共エリア
□講義室、図書館などの学習エリア
□現在約500APを設置
■ 認証・認可システムを利用
2005/10/23
12

キャンパス公衆ネットワーク(無線LAN)設計方針

- 安全、安心であること
  - 学生のアカウントの貸し借りに歯止めをかけたい
  - ワーム等の外部への攻撃を防ぎたい
- 利便性が高いこと
  - 特別な書類手続き、アカウント発行手続きが必要ないこと
  - 電波受信環境に入れば、特別なコンサルティングなく誰でも利用可能であること
- スケーラブルであること
  - AP数およびアクセスエリアの拡大が容易であること
- 管理運用が容易であること
  - 限られた技術職員で集中管理が可能であること



認証システムが必要な背景(1)

- ICTセキュリティリスクの上昇
  - ウィルス、ワーム、ボットの発生
  - 著作権侵害
  - 迷惑メール、フィッシングメールの中継
  - *個人情報・重要情報の流出*
- うちの大学でおきたらどうしよう!

認証システムが必要な背景(2)
政府機関の情報セキュリティ対策のための統一基準

- http://www.nisc.go.jp/active/general/kijun01.html
- 4.1.1 主体認証機能
- (1) 主体認証機能の導入
- 【基本遵守事項】
- (a) 情報システムセキュリティ責任者は、すべての情報システムについて、主体認証を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、主体認証を行う必要性があると判断すること。
- (b) 情報システムセキュリティ責任者は、主体認証を行う必要があると認めた情報システムにおいて、識別及び主体認証を行う機能を設けること。
- ・・・

キャンパス共通認証認可システム設計指針

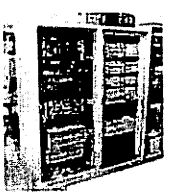
- 情報資源アクセスアカウント
  - 東工大在籍者全員に情報資源アクセスアカウントを配布
- 高い利便性とセキュリティ
  - ×学内便でアカウント・パスワード配布
    →システムごとに異なるアカウント ⇨ Webシングルサインオン
  - ×複数人でアカウント・パスワード共有
  - ×httpのベーシック認証
  - ID・パスワード認証よりも高いセキュリティレベルを提供
- 高い管理性
  - 限られたスタッフで大きなシステムをいかに管理するか

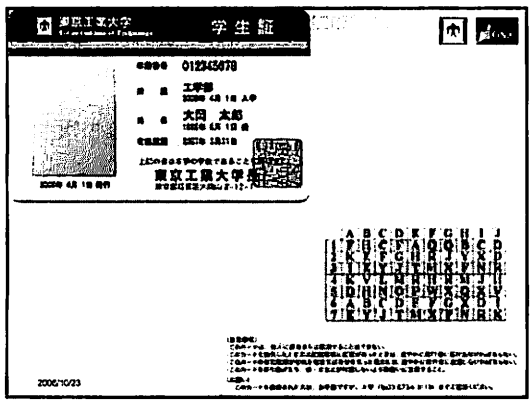
⇩

①認可権限分散管理システムの導入
②身分証発行部署、情報システム管理部署の分離
③認証局のアウトソース運用

東京工業大学
キャンパス共通認証認可システム

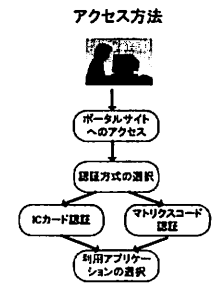
- 2006年3月導入
- ICカード身分証
- 個人情報ディレクトリシステム
  - LDAPサーバ
- Webシングルサインオンシステム
  - 認可権限分散管理システム
- 東工大ポータルシステム
- 全学共通メールシステム
- VPNサーバ





キャンパス共通認証認可システム 2種類の認証方法

- ICカード認証
  - カードリーダに挿入
  - PINコードで認証
  - PKI技術を利用
- マトリクスコード認証
  - ID/パスワード認証
  - マトリクスコード認証



2008/10/23 20

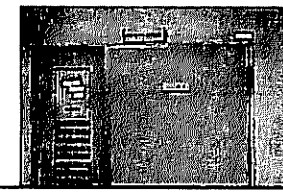
キャンパス共通認証認可システム 認可権限分散管理

- 認証 *Authentication*
  - サービス提供時に利用者の主体が正等であることを確認すること
- 認可 Authorization
  - 認証された利用者に対して、定められた権限にもとづきサービス提供の可否を判断すること
- 認証だけでは何もできない！＝認可権限の設定が必要
  - 誰がどうやって設定する？
- 認可権限分散管理
  - 5階層までの階層構造により、センターとしては、権限を付与する権限だけを設定し、大学全体の運用性を高める

2008/10/23 21

キャンパス共通認証認可システム 運用体制

- システム管理
  - 学術情報部 情報基盤課 認証認可システム係
- ICカード発行=アカウント登録=RAオペレータ
  - 人事課、教務課
- 認証局運用
  - 外部アウトソース



2008/10/23

キャンパス共通認証認可システム アプリケーション

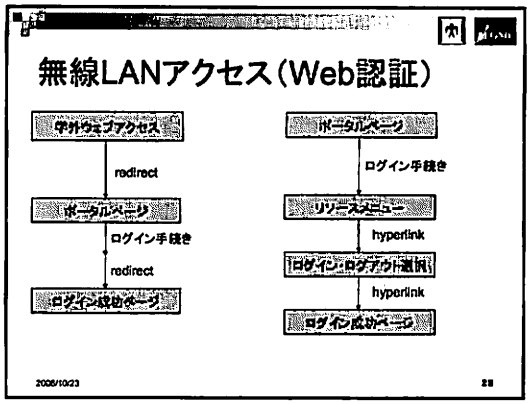
- 現在運用中のもの
  - キャンパス共通メールシステム
    - 全員に配布 (@m.titech.ac.jp)
    - Webメール/POP/IMAP環境
    - ウィルス、迷惑メールフィルタ
  - 遠隔ネットワークアクセス
    - SSL-VPN
  - 無線LANネットワークアクセス
  - Open Course Ware
  - 教育支援システム
  - 物品等請求システム
  - ウェブストレージシステム
- 今後導入を検討しているもの
  - TSUBAMEログイン
  - Web教務システム
  - 図書館システム
  - 英語教育システム
  - 研究者情報システム
  - 大学情報データベース
  - など

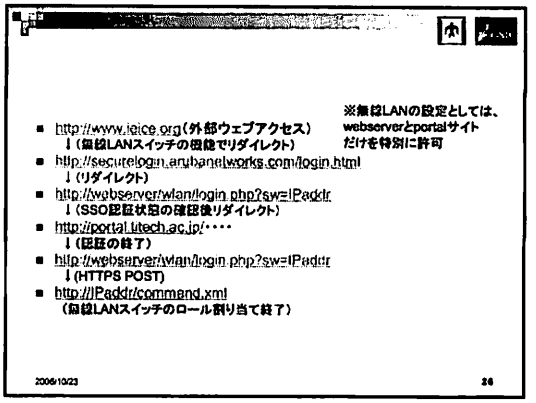
2008/10/23 23

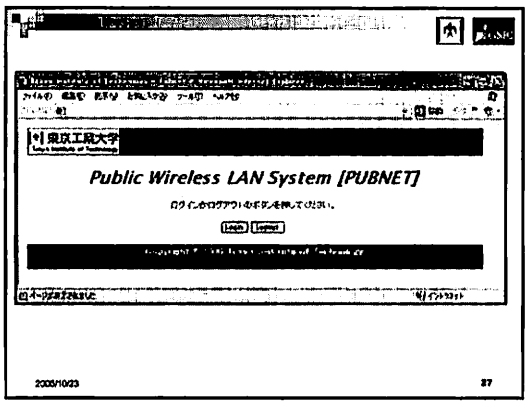
キャンパス公衆ネットワーク(無線LAN) 認証方法

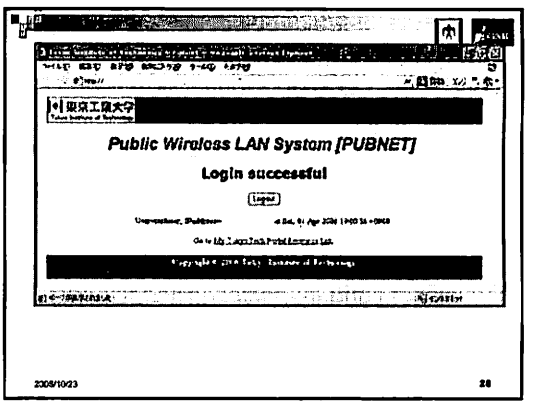
- キャンパス共通認証認可システムを利用
  - 入学、任用時に配られたICカードに付属するアカウントを利用＝事前のアカウント発行手続きがいらない
  - システムごとの個別アカウント管理が必要ない
  - 高度なセキュリティを提供可能
- Web認証
  - 無線LAN接続後、ウェブブラウザを起動する

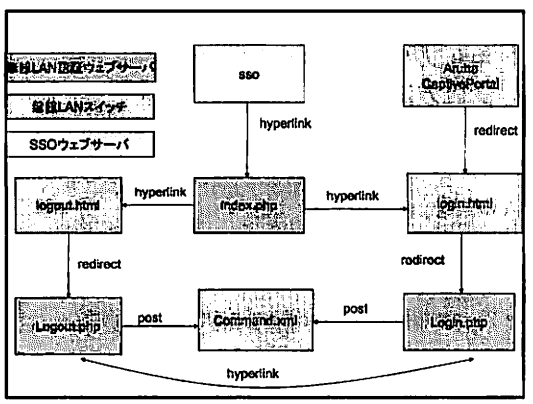
2008/10/23 24

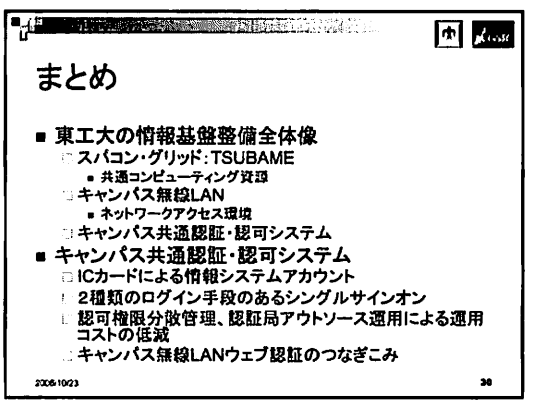

無線LANアクセス(Web認証)
学外ウェブアクセス
redirect
ポータルページ
ログイン手続き
redirect
ログイン成功ページ
ポータルページ
ログイン手続き
リソースメニュー
hyperlink
ログイン・ログアウト選択
hyperlink
ログイン成功ページ
2006/10/23
28


※無線LANの設定としては、webserverとportalサイトだけを特別に許可
http://www.teice.org(外部ウェブアクセス)
↓(無線LANスイッチの機能でリダイレクト)
http://securelogin.arubanetworks.com/login.html
↓(リダイレクト)
http://webserver/wlan/login.php?sw=IPaddr
↓(SSO認証状態の確認後リダイレクト)
http://portal.itech.ac.jp/・・・・
↓(認証の終了)
http://webserver/wlan/login.php?sw=IPaddr
↓(HTTPS POST)
http:///IPaddr/command.xml
(無線LANスイッチのロール割り当て終了)
2006/10/23
26


東京工科大学
Public Wireless LAN System [PUBNET]
Login
Logout
2006/10/23
27


東京工科大学
Public Wireless LAN System [PUBNET]
Login successful
Logout
2006/10/23
28


無線LAN認証ウェブサーバ
無線LANスイッチ
SSOウェブサーバ
SSO
Aruba CaptivePortal
hyperlink
redirect
logout.html
hyperlink
index.php
hyperlink
login.html
redirect
redirect
Logout.php
post
Command.xml
post
Login.php
hyperlink


まとめ
東工大の情報基盤整備全体像
スパコン・グリッド:TSUBAME
共通コンピューティング資源
キャンパス無線LAN
ネットワークアクセス環境
キャンパス共通認証・認可システム
キャンパス共通認証・認可システム
ICカードによる情報システムアカウント
2種類のログイン手段のあるシングルサインオン
認可権限分散管理、認証局アウトソース運用による運用コストの低減
キャンパス無線LANウェブ認証のつなぎこみ
2006/10/23
30