




データベースと運用の連携

ユーザ管理、機器管理、課金、
その他情報の統合利用



東京大学生産技術研究所

福島 瞳



本日の内容概略

- 東京大学生産技術研究所について
- 課金システムとデータベース概略(歴史的部分も含め)
- グループ(研究室等)の扱い
- ネットワーク管理原則と体制
- データベース内の管理関係テーブルの概要
- ユーザ申請、機器申請の実際と手順
- 課金とその処理について
- データベースを利用したユーザ用ツール
- データベースを利用した管理用ツール

東京大学生産技術研究所(生研)の紹介

- 場 所:** 駒場リサーチキャンパス(駒場II)
教養キャンパスの西、元宇宙研、現在は生研のほか先端研等がある。
- 生研本館:** 巨大な一続き ブロックごとに B棟 - F棟(東と西)
最高8階 高低でこぼこ。(A棟は建設中)
- その他:** 試作工場、食堂・会議室棟、図書棟、22号館、45号館、56号館、千葉実験所
- 人 員:** 全体で 1300人以上。
教員、職員、非常勤職員、任期付教職員、
大学院生、研究員、研究生、研究実習生、その他
- 研究室体制:** 教授、助教授、講師が研究室主宰者。100人以上。
5つの部門とセンター: 研究内容は生研全体として流動的。
部屋の移動、人員の所属も変更がありうる。

ネットワークなどの管理体制 生研の特殊性

- ・ **学部学生がいない** --- 研究室に属さない学生がいない。
教育用環境(PC教室など)は必要ない -- 個々の要求に対応。
- ・ **ユーザ管理、機器管理等、課金請求** --- グループごとに
研究室、センター(国際災害軽減センター、計算科学連携センターなど)
事務部の各係や試作工場等の組織
現在 研究部系: 115 その他: 30 計 145
- ・ **ネットワーク管理者**
グループに最低ひとり、トラブルや問い合わせ窓口になる担当者を登録。
- ・ **電子計算機室スタッフ:** 助手、技術職員計5名 +

課金、データベース利用

-- 歴史をたどる その1

- ・ 生研電子計算機室は 40年以上前から
工学用計算環境提供から所内ネットワーク管理へ
- ・ 大型汎用機時代：
ユーザごとのCPU、ディスク、プリント課金。
汎用機固有の課金システムで課金処理。
研究室単位に集計して請求。
- ・ ネットワーク接続開始：1989年頃から。
その後ホスト管理が必要になり、Access にデータを入れはじめる。

課金、データベース利用

-- 歴史をたどる その2

- ・ 課金管理の移行：
 - 更新で汎用機利用終了。
 - サービスはネットワークと UNIXへ。
 - 1996 HP-UX SYBASE 課金用データベース利用本格化。
 - 1999 Solaris SYBASE に移行、2000年問題のため。
- ・ 課金体系変更：
 - CPU、ディスクの従量課金主体から、
 - 研究室、ユーザ基本料金、ネットワーク接続課金主体に。
 - 2000 Solaris SYBASE 課金体系変更反映。
 - 2003 BSD/OS PostgreSQL に移行。現在に至る。
- ・ 課金原則：昔から変わっていない。
 - 課金請求は研究室単位、課金年度は 1月から 12月
 - 課金で電子計算機室予算をまかなう。
 - (各種保守費、機器やソフトウェアの購入、消耗品購入など)

現在のデータベースと関連システム概要

- ・ 種々管理、課金などをデータベースで。拡張構想を具体化。
データベース構築と移行、各種プログラム作成を更新時の仕様にした。
2003年3月 レンタル更新:ハードウェアとプログラムの納入。
- ・ PostgreSQL でネットワーク利用可能に。
様々なホストからアクセス可能 -- ライセンス数考慮の必要がない。
- ・ 操作コマンド等の構築は Ruby プログラム。
データ変更等は Access 画面、Common SQL Environment (Free)で。
- ・ ユーザ / 機器 -- 登録・更新・削除システム
作業用テーブル構成と管理用の Access 画面
画面確認、修正ののち、コマンド入力で各サーバと連携、DB操作。
- ・ 課金システム -- 単価と計算式、複雑な計算に対処。
結果をDBテーブルに格納後、整形してテキストファイルに出力。
- ・ その他 -- 電子計算機室作成のさまざまなツール

ネットワーク概要

物理的構成

建物、階ごとにネットワークスイッチを配置、
支線ネットワークスイッチ(別棟を含め、70台)から
各室内に配線し、情報コンセントから利用。

サブネット

一般サブネット(建物単位:24)、研究室サブネット(25)。
柔軟なサブネット構成(離れた部屋も同一サブネットに構成可能)

運用

DHCPサーバ運用 --- MAC アドレスで管理。
無線LAN 認証つき --- VLAN 指定のためにユーザごとの登録必要。

生研内利用のルール

- ・ グループ： 研究室、研究グループ、係、その他
研究系は「利用料金」とリンク
- ・ ユーザ利用： 研究室主宰教員、または係長等の許可が必要。
メールのみユーザと メール・ワークステーション利用
PPP利用。
- ・ 機器利用： ユーザと同様の許可が必要。
会議室は登録無し機器も可能、セキュリティ強化。

これらに合致するよう、データベースや登録の仕組みを考慮。

管理用テーブル抜粋

ユーザ
ユーザ名
status
UID
本名
グループ名
身分
TEL
VLAN
日付

グループ
グループ名
status
GID
課金コード
部
正式名
chief
日付
課金情報

接続機器
ホスト名
(IP)
MAC
グループ名
室
DHCPか
VLAN
日付

管理者情報
グループ名
Email
TEL
氏名

サブネット情報
VLAN
サブネット名
アドレス (cidr)
研究室VLANか

VLAN情報
VLAN
グループ名

パッチ情報
スイッチ
スロット
ポート
VLAN
情報コンセント番号
室

室利用情報
室
グループ名

登録申請ページ

ユーザ申請用と ホスト登録用それぞれのWWWページがある。
1998年より、このWWWページが利用されている。

- ・ユーザ名、ホスト名重複チェック(多重の場合、再入力を求められる)
日付時刻で、申し込みに IDがつく。
- ・メール発信: 「教員や係長」および電子計算機室に。
Subject: User Registration, ID
または Network Registration, ID
- ・教員等が許可メール返信: 電子計算機室に配送。
「印鑑」の代りとしての機能。
- ・ログに記録。IDで検索可能。

■ ユーザ新規登録申請 ■

所属	1部	
研究室/係		研究室/係
氏名	漢字	<input type="text"/> ◆空白は入れないでください
	ローマ字	<input type="text"/>
利用申請者身分	大学院生	◆正確な身分を選択する(注)
希望ユーザ名 (3~8文字)	<input type="text"/>	◆英字から始まる半角英数字のみ
内線番号	<input type="text"/>	
部屋番号	<input type="text"/>	
利用目的	<input type="text"/>	
利用形態	<input checked="" type="radio"/> メールのみの利用 <input type="radio"/> ワークステーションとメールの利用	
PPP接続	<input type="radio"/> 利用する <input checked="" type="radio"/> 利用しない	
担当 教員/係長	氏名	<input type="text"/>
	e-mail	<input type="text" value="xxxx.u-tokyo.ac.jp"/>

http://www.cc.iis.u-tokyo.ac.jp - IIS-CC Network Registration form - Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H) リンク >>

■ ネットワーク機器接続 ■

接続地区	駒場	地区
所属	1部	
研究室/係		
担当 教員/係長	氏名	
	e-mail	xxxx.u-tokyo.ac.jp
連絡先	氏名	身分等 教授
	e-mail	xxxx.u-tokyo.ac.jp
	内線番号	
設置場所	部屋番号	(例 Ce-201)
	内線番号	
接続機器	OS名	バージョン、型番等
	利用形態	<input checked="" type="radio"/> クライアント機能のみ <input type="radio"/> サーバ機能も含む
	接続形態	<input checked="" type="radio"/> 有線LAN <input type="radio"/> 無線LAN
	DHCP接続(*)	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
	機器名	
	ホスト名	半角英数と`-`15文字以内(`.`と`.`は使用禁止)
	MACアドレス	(例 08:00:20:76:63:ae) 「MACアドレスの調べ方」
	備考	接続希望日など

申請する 書きなおす

インターネット

メールの例

To: yyy@xxxx.u-tokyo.ac.jp
Subject: USER Registration #20041001162006
From: [xyz-staff @ xxxx.u-tokyo.ac.jp](mailto:xyz-staff@xxxx.u-tokyo.ac.jp)
Date: Fri, 1 Oct 2004 16:20:06

井内工作様

以下の内容で「ユーザ新規登録申請」が提出されています。

許可の場合はその旨記載の上、[xyz-staff @xxxx.u-tokyo.ac.jp](mailto:xyz-staff@xxxx.u-tokyo.ac.jp)宛にメールを出してください。

申請日時: 2004/10/01(金) 16:20:06
所属: 9部
研究室(係): 井内
職名等: 大学院生
氏名(漢字): 海河たくみ
氏名(ローマ字): Takumi Umikawa
ログイン名: umikawa
担当教員/係長(氏名): 井内工作
担当教員/係長(email): yyy @ xxxx.u-tokyo.ac.jp
内線番号: 59253
部屋番号: Ew-222
利用目的: 研究のため
利用形態: ワークステーションとメールの利用
PPP接続: 利用しない

管理用登録・削除・変更関連ツールと操作

登録時

- ・ 入力用コマンドにIDをつけて実行 専用登録用テーブルに入力される。
グループ名は、許可者のメールアドレスから検索して設定。
- ・ 必要ならAccess 画面で変更。
- ・ 登録用コマンド実行で、各サーバに必要な登録が一気に実行される。

削除時

- ・ Access 上でキー(ユーザ名、ホスト名など)を入力すると
削除用テーブルに反映され、削除用コマンドで(各サーバ分も)削除される。

変更時

- ・ キーをパラメータに入力コマンドで変更用テーブルに取り込む。
- ・ Access で必要事項を変更し、変更用コマンドを実行する。

ユーザ登録の場合

- ・ コマンドにより、以下が実行される。
 - 1) NIS サーバの パスワードファイルに登録。
 - 2) Active Directory (Windows2000 サーバ) へのユーザ登録。
 - 3) LDAP サーバへのユーザ登録 (メールサーバ用)
 - 4) 無線用RADIUSサーバ(ACS)へのユーザ登録。
(データファイルコピーの上、実行)
 - 5) 必要に応じ、ダイヤルアップ用 RADIUSサーバへのユーザ登録。
 - 6) データベースのユーザマスターテーブルへの登録。
 - ・ 登録通知書プリントアウト(LaTeX出力、仮パスワードつき)
- 窓開き封筒で研究室ポストに届ける。ほぼ1日。

機器登録の場合

- ・ コマンドにより、以下が実行される。
 - 1) DHCPサーバへの機器情報登録
 - 2) 無線機器の場合、無線用 RADIUSサーバ(ACS)への機器情報登録
 - 3) データベースのマシンマスターテーブルへの登録
 - ・ 固定IP を与える場合は、1) をせずにDNS サーバへの登録を実行する。
(これは手作業)
 - ・ 申請者に Email で登録完了を連絡。
固定IP接続の場合は、アドレスとパラメータ(サブネット情報など)も送付。
- ほとんど時間がかからないため、ユーザに好評。

課金用データ収集方法

すべてデータは利用量テーブルに流し込む。

- CPU 利用量 ---- 計算用としている Solaris 機器対象。
daily account からデータ収集。
- ディスク利用量 ---- ホームディレクトリで du -s コマンド 1日1回実行。
- メール領域 ---- メールサーバ mirapoint でのディスク利用量。
ログファイルをメールでデータベースサーバに送付、
データベースサーバ上でコマンドに流し込む形で処理。
- プリント枚数 ---- ユーザが伝票記入。室員が Access 画面で手入力。
両面カラープリンタ、ポスタープリンタ。件数は多くない。
- ダイアルアップ ---- ダイアルアップサーバアクセスログから自動抽出。
- フリーダイアル ---- NTT からの詳細ログ (フロッピー) とアクセスログを付き合わせ、
料金額をユーザごとに集計するプログラムを利用。

課金関連テーブルと計算方法

利用量
日付
ホスト名
タイプ
ユーザ名
利用量

単価表
タイプ
最小量
単価
切片

課金タイプ表
タイプ
項目名
集計項目

利用量を x としたとき、単価は a 切片 b

$$y = ax + b$$

また他の課金計算も、同様にこの式で可能。

課金計算

月はじめに前月分について計算実行。

データベース情報により、自動計算される。

$y = ax + b$ が基本。

計算方法いろいろ：

CPU: 月合計時間数に対して計算。

ディスク: 日ごとに課金額計算、月単位で集計。

教授、助教授加算: グループ情報のchief 身分により計算。

サブネット: $2500 \times 2^{**} (27 - \text{ネットマスク})$

情報コンセント数: 利用室の情報コンセント数を集計。

複数研究室で同一室を利用の場合は均等割り。

研究室分課金テーブル、個人分課金テーブルに項目ごとに格納。

請求用帳票作成

帳票は、各課金テーブルから要素を抜き出し、作成。

- 1) 研究室合計の帳票
- 2) 研究室ごと合計、コードつき帳票 事務方に回す。
- 3) 研究室ごと個人利用料金データ内訳帳票

テキストファイルとしてファイルサーバに保存。
プリント出力も保存。

テキストとした理由：簡単に表示・検索できる。
必要に応じ、部分抜き出しも簡単。

関連: ユーザ用もろもろツール その1

ツール類: 室員が必要に応じ作成し、数が増えた。
Ruby プログラムが主体。

- ・ ユーザ登録関係、機器登録関係申請ページ CGI (前述)
- ・ 機器情報閲覧 兼 変更・廃止申請ページ CGI

アクセスしている IP を元に、
または (DHCPサーバに問い合わせ) MACアドレス から
DB 検索 グループ グループ所属機器リスト表示
(表形式で表示される)

部屋、MACアドレスなどの項目の変更を行い、
申請者情報など入力の上 submit すると「変更申請」ができる。
(メール発信等一連の流れとなる。)

関連：ユーザ用もろもろツール その2

- ・ 研究室課金情報閲覧ページ

ユーザ認証： NIS にアクセス。

データベース：ユーザ身分チェック。何らかの職員である必要。

データベース：ユーザ所属研究室分の課金を月ごとに表示。

- ・ 研究室ユーザ情報参照ページ

ユーザ認証： NIS にアクセス。

データベース：所属研究室の登録全ユーザリスト等閲覧。

(在籍者の制限確認、転出ユーザチェック)

関連：管理用もろもろツール その1

WWWからの通知ツール

a) ホストトラブルの場合（例：ウィルス感染）

トラブルホスト のリストを入れ、通知文入力。
(IP, FQDN, MACアドレス、ホスト名どれでも、また混在も可。)
DHCP サーバのログ等から、問題機器を特定できる。
ホスト名から研究室を検索、管理者に研究室ごとのリストつきで送付。
リスト：ホスト名、MACアドレス / IPアドレス、室、機種、OS

b) ユーザの利用に問題のある場合(例：パスワードが安易)

問題ユーザ のリストを入れ、通知文入力。
ユーザそれぞれに通知メール送付。
管理者にも、研究室内問題ユーザー一覧と別途管理者向け通知を送付できる。

関連：管理用もろもろツールその1（続き）

通知ツールにより、以下のようなメールが管理者に送付される。

To: dareka@xxxx.u-tokyo.ac.jp
Subject: 調査対策のお願い
From: xyz-staff@xxxx.u-tokyo.ac.jp

9部 井内研究室の計算機管理担当者様

貴研究室の以下のマシンで、ウイルスと思われる異常なトラフィックを検出しました。

調査の上、コンピュータウイルスが原因の場合はそのウイルス名称もお知らせください。

ホスト名 (IP/MACアドレス)	OS	機種
-------------------	----	----

dokka	(00:80:45:2b:c8:91)	WindowsXP	IBM-ThinkPad
-------	---------------------	-----------	--------------

電子計算機室 xyz-staff@xxxx.u-tokyo.ac.jp

関連: 管理用もろもろツール その2

室員用各種コマンド

(よくある検索を迅速に行うために作成し、利用している。)
UNIX系ホストで実行可能な Ruby プログラム。

- ・ **ホスト情報表示**
ホスト名から または MACアドレスから
研究室名、室、VLAN、MAC アドレス、IP などを表示。
- ・ **ユーザ情報表示**
ユーザ名から 所属研究室、身分、電話番号など表示。
- ・ 研究室機器情報一覧コマンド
- ・ 研究室ユーザ情報一覧コマンド
- ・ スイッチポートと情報コンセント対応一覧表示: less 等で検索。

管理利用の例：緊急時の利用

- 1) 問題のある機器について、IPアドレスでの連絡が寄せられる。
- 2) 機器検索で所属研究室、MACアドレスがわかる。
- 3) 接続ポート発見用コマンドを利用する。

しくみ：

- a) DNSで固定IPか、DHCPかを知る。
DHCPの場合、DHCPサーバのログからホスト特定。
 - b) MACアドレスやIPからネットワークスイッチをたどる。
トラブルポートがわかる。
- 4) DB から設置室、対応情報コンセント番号がわかる。
 - 5) 利用研究室から管理者が順に DB から参照される。

(続く)

管理利用の例：緊急時の利用(続き)

6) 問題解決。

特定した機器情報を元に研究室に連絡する。
(管理者情報検索:連絡先取得)

必要なら部屋を訪問する。
トラブル回避や機器停止が不可能な場合、LANケーブルを抜く。

部屋にも入れない場合には、LANスイッチのポートを disable にする。

データベースを利用した管理 – まとめ

管理したいデータ(ユーザ、グループ、機器、ネットワーク情報等)でデータベースを構築し、利用している。

- 各種サーバ登録と連携。
- 一般ユーザ用に登録や参照のWWWページを用意。
- 研究室との連携迅速化。
- 課金システムとしても重要。
- 日々のアップデート(登録、更新)がかなめ。