# セキュリティ保持のための学生向け演習室利用状況提供システム

本田 修啓

福島大学総合情報処理センター

nhonda@fukushima-u.ac.jp

**概要**：福島大学総合情報処理センターでは,実習講義および自習のためのパーソナルコンピュータ端末の運用管理を行っている.管理者向け利用状況表示および統計システムに加え,今回,学生が自分自身の利用状況を安全に確認できるシステムを試作し運用を開始したので,その概要を紹介する

## 1. はじめに

本学総合情報処理センターは平成 23 年 2 月に演習用端末システムの設備更新を行った.クライアントシステム概要を表 1 に示す.Windows7 端末,Macintosh 端末ともネットブートシステムである.前システムで構築運用していた「多種 OS 対応端末利用監視システム」についても見直しを行い,平成 24 年度より新システムとして運用を開始した.新システムは従来の管理者向け情報発信システムに加え,ユーザである学生向け情報発信システムを新たに追加した 2 系統構成となっている.学生向け情報発信システムでは,端末利用履歴,パスワードツール利用履歴閲覧の他,個人情報を含まない端末利用情報,ファイルサーバ利用状況を提供している.

セキュリティ保持には,管理担当者の努力だけでなく,適切なパスワード管理をはじめとする学生の協力が必須である.1 個の利用アカウントへの不権限アクセスから大きなインシデントにつながる可能性もある.利用履歴を随時確認することにより,学生自身が身に覚えのない不権限アクセスを監視することでセキュリティの向上を期待している.

表 1 クライアントシステム

| クライアント端末 | 台数 | OS | 仕様 |
|---|---|---|---|
| Windows7端末 | 309 | Windows7 | iSCSIネットブートシンクライアント |
| Macintosh端末 | 58 | MacOS X | Mac X serve ネットブート |
| Linux演習サーバ | 5 | RedHat ES5 | 負荷分散構成最大200ユーザ対応 |

## 2. 利用記録の取得と記録

### 2.1. システム構成

構築した情報収集システムの構成を図 1 に示す.

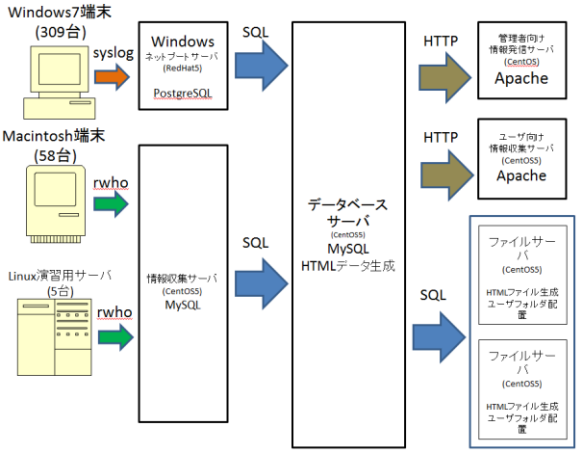



図 1 システム構成図

MySQL で構築したデータベースサーバに利用履歴が蓄積保存される.蓄積情報はデータベースサーバ自身が定期的に処理を行い,HTML ファイルを生成している.この HTML ファイルは定期的に管理者向けあるいはユーザ向け情報発信サーバに転送され,そこから発信が行われる.管理者向けサーバでは,管理者端末のアクセスのみ許可している.セキュリティ面に配慮しデータベースサーバと情報発信サーバを分離し,また管理者向け情報発信と学生ユーザ向け情報発信を別サーバとしている.

### 2.2. Windows7 端末の利用情報

Windows7 ネットブートシステムでは,各端末はユーザ利用開始,利用終了等のイベントを syslog としてネットブートサーバに送信する.この情報を受けたネットブートサーバは内部データベースにそれを記録する.データベースサーバは,ネットブートサーバから定期的に利用中端末情報を SQL で読み出し,利用履歴記録として自身のデータベースに登録する.ネットブートサーバのイベントには,起動開始およびログオン可能状

態となった時刻情報も含むので,性能評価機能として有用な起動所用時間情報もあわせて記録している.

## 2.3. Macintosh 端末の利用情報

Macintosh 端末利用情報は,各端末で rwhod を有効にすることで,周期的に broadcast されるログイン利用者情報をデータベースサーバで処理し,端末名,利用開始時刻,利用終了時刻をデータベースに記録する方法で得ている.rwhod は MacOS X 標準添付のものを使用している.

## 2.4. 演習用 Linux サーバ利用履歴

演習用 Linux サーバは 5 台負荷分散構成である.Windows あるいは Macintosh 端末から VNC クライアント,もしくは SSH ターミナルを使用して利用する.VNC,SSH とも負荷分散装置経由の利用となり,ユーザからは 1 台のサーバのように見えている.

利用情報は Macintosh 端末と同様データベースサーバが各演習用サーバの rwhod による利用者情報の周期的な broadcast を収集している.これに加えアクセスクライアント情報取得のため TCP セッション情報を SMNP で読み出し,port 番号から,利用手段である VNC 接続あるいは ssh 接続を判別している.rwhod は負荷分散構成に対応し broadcast させるホスト名および間隔を変更する修正を行ったものを使用している.

## 2. 5. 認証管理情報の取得と記録

### 2.5.1. システム構成

Windows7 端末,Macintosh 端末,演習用 Linux サーバ,電子メールでは同一ユーザアカウントとパスワードで認証が行われる.これらはそれぞれ Active Directory, LDAP, GoogleApps 認証の異なる認証システムを使用する.これらのアカウントの統合管理するため,Unicorn ID Manager を採用し,同一 ID およびパスワードで認証が行われるようにしている.ユーザおよび管理者は Web ブラウザ経由,アカウント登録/削除(管理者),パスワード変更,リマインダ利用(ユーザ)を行う.これらの処理イベントは認証管理サーバのログに記録される(図 2).

定期的にログファイルをスキャンし,記録内容を認証管理サーバデータベースに登録するプログラムを実行させ,イベントをデータベースに登録している.

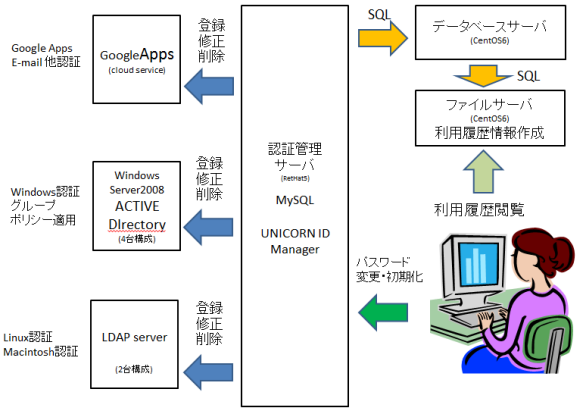



図 2 認証管理情報収集システム構成

### 2.5.2. 記録情報

認証管理サーバデータベースでは以下のイベントを記録している.

(1) イベント発生日時
(2) 実行者(管理者/ユーザ)
(3) 対象ユーザ ID
(4) イベント内容(パスワード変更等)
(5) コメント(エラー原因等)

主なイベントは以下の通りである.

(1) ユーザ登録(管理者)
(2) ユーザ削除(管理者)
(3) パスワード管理者変更
(4) パスワード変更(ユーザ)
(5) パスワード再発行ユーザ
(6) パスワード再発行用「秘密の質問」登録

## 2.6. ファイルサーバ利用状況取得と記録

ユーザの端末利用の際に必要となるユーザ領域は2台のファイルサーバから,NFS および CIFS で各端末がリモートマウントする方法で提供している.

表 2 ファイルサーバ提供領域

| 端末 | 提供方法 | 容量 | 用途他 |
|---|---|---|---|
| Windows7 | CIFS | 2GB | ファイル保存(ユーザプロファイル含む) |
| Linux | NFS | 2GB | ホームディレクトリ |
| Macintosh | NFS | 2GB | ホームディレクトリ |

システム構成を図 3 に示す.ユーザの領域使用量は,ファイルサーバ(OS は CentOS)で repquota を実行,その出力を処理しデータベースサーバのデータベースに SQL で登録する処理を深夜に

cron で行っている.

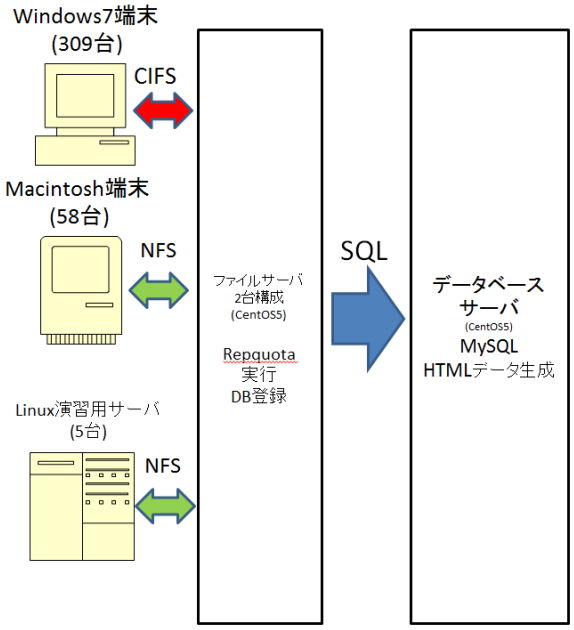



図 3　ファイルサーバ状況取得

## 3.　ユーザ向け情報生成と表示

### 3.1.　個人情報表示システム構成

取得した情報を利用し,ユーザに対し自身の以下の履歴等の提示については,個人情報を含むことから,本人だけが安全に閲覧可能であり,第三者は閲覧不可能でなければならない.

本システムでは,図 4 に示すようにファイルサーバの Windows7 用ユーザ領域に対応ユーザ利用状況をまとめた html ファイルを書き出させ,ユーザはブラウザで ローカルファイルを表示させる方法を採用している.

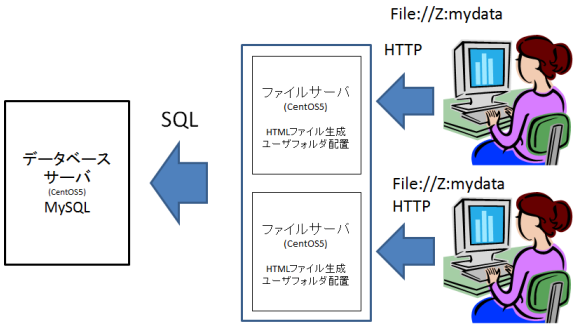


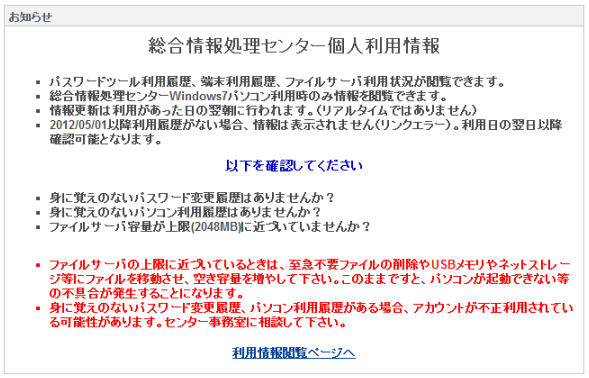

図 4　個人利用情報の生成と閲覧

ファイルサーバのユーザ領域は,該当ユーザのみアクセス制限が実施されている.従って第三者が閲覧することはファイルサーバのアクセス制限機能で禁止される.

また作成する html 情報には,ユーザ ID 等を含ませないよう配慮し.この情報が流出した場合でも個人特定が行えないようにした.

### 3.2.　ユーザ利用方法と表示例

ユーザが Windows7 端末にログオンしブラウザを起動すると,総合情報処理センター演習室ポータルページが強制的に表示される.ポータルページにリンクを設定し,クリックすることで以下のようなページが表示される.


お知らせ

総合情報処理センター個人利用情報

- パスワードツール利用履歴、端末利用履歴、ファイルサーバ利用状況が閲覧できます。
- 総合情報処理センターWindows7パソコン利用時のみ情報を閲覧できます。
- 情報更新は利用があった日の翌朝に行われます。(リアルタイムではありません)
- 2012/05/01以降利用履歴がない場合、情報は表示されません(リンクエラー)。利用日の翌日以降確認可能となります。

以下を確認してください

- 身に覚えのないパスワード変更履歴はありませんか？
- 身に覚えのないパソコン利用履歴はありませんか？
- ファイルサーバ容量が上限(2048MB)に近づいていませんか？

- ファイルサーバの上限に近づいているときは、至急不要ファイルの削除やUSBメモリやネットストレージ等にファイルを移動させ、空き容量を増やして下さい。このままですと、パソコンが起動できない等の不具合が発生することになります。
- 身に覚えのないパスワード変更履歴、パソコン利用履歴がある場合、アカウントが不正利用されている可能性があります。センター事務室に相談して下さい。

利用情報閲覧ページへ

図 5 個人利用情報閲覧入り口ページ

このページでは本システムの目的および確認ポイントおよび異常を感じた場合の対応方法を指示している.このページで”利用情報閲覧ページへ”のリンクをクリックすることで,表示が行われる.


総合情報処理センター個人利用履歴

2012-08-23 01:00:00 現在

| | | | |
|---|---|---|---|
| パスワード最終変更 | 2011-05-17 10:58:08 | 秘密の質問登録／変更 | 2011-05-18 11:12:32 |
| Windows最終ログオン | 2012-08-12 16:35:28 | Windowsファイル | 2048MB中 629 MB 使用 |
| Macintosh最終ログイン | 2012-06-12 10:19:00 | Macintoshファイル | 2048MB中 30 MB 使用 |
| Linux最終ログイン | 2012-07-19 10:00:05 | Linuxファイル | 2048MB中 6 MB 使用 |

パスワード更新履歴

2011-05-18 11:12:32 秘密の質問登録
2011-05-17 10:58:08 パスワード変更

Windows利用履歴

ref6004 2012-08-12 16:35:02 2012-08-12 16:42:43
ref6007 2012-07-31 09:13:09 2012-07-31 09:16:39
wu18022 2012-07-30 15:41:06 2012-07-30 15:51:06
ref6003 2012-07-26 10:13:33 2012-07-26 10:18:02
ref6007 2012-07-25 14:47:32 2012-07-25 14:57:29
wu18013 2012-07-23 16:26:31 2012-07-23 18:47:36
ipc1038 2012-06-25 16:19:05 2012-06-25 17:35:45
wu18019 2012-06-22 13:34:10 2012-06-22 17:51:53
wu18016 2012-06-20 16:26:24 2012-06-20 17:46:30
wu18011 2012-06-19 15:04:55 2012-06-19 15:58:22
wu18011 2012-06-19 09:53:16 2012-06-19 10:02:12
ref6006 2012-06-18 16:29:55 2012-06-18 17:34:28
ref6006 2012-06-15 10:08:47 2012-06-15 10:11:27
ipc1102 2012-06-01 13:55:16 2012-06-01 15:11:45
ref6001 2012-06-01 09:45:33 2012-06-01 10:09:21
ipc1036 2012-05-31 16:26:50 2012-05-31 17:37:21
ref6007 2012-05-22 10:02:00 2012-05-22 10:13:13
wu18025 2012-05-18 13:28:39 2012-05-18 16:07:51
wu18020 2012-05-15 14:41:31 2012-05-15 16:01:37
ref6002 2012-05-11 15:38:56 2012-05-11 15:47:02
ref6006 2012-05-09 18:17:44 2012-05-09 20:41:31

Macintosh利用履歴

ipc3030 2012-06-12 10:19:00 2012-06-12 10:37:01

Linux利用履歴

venus3 2012-07-19 10:00:05 2012-07-19 10:19:48

2012 (c)福島大学総合情報処理センター

図 6 個人利用履歴情報の表示例

### 3.3. 制限事項

表示データの生成はファイルサーバで深夜に行われる.したがって,利用実績はリアルタイムに反映されず,翌日以降に反映される.

また処理対象を前日に端末の利用履歴あるいはパスワード修正履歴が存在するユーザに限定し処理負荷を軽減している.

## 4. ユーザ向け端末利用状況生成と表示

### 4.1. 演習室利用状況閲覧システム

データベースサーバに蓄積される演習室端末利用統計情報を学生実習用情報発信サーバ経由で IP アドレスによるアクセス制限を設定せずに提供している.学生ユーザは演習室端末だけでなくスマートフォンや携帯電話のブラウザを利用して随時閲覧が行える.閲覧が行えるのは以下の通りである.

(1) リアルタイム端末利用状況
(2) 当日を含む過去の日毎端末利用記録
(3) 当月を含む月毎端末利用記録

これらについては,以下の URL および右 QR コードでスマートフォンあるいは携帯電話ブラウザ参照することができる.

http://www.ad.ipc.fukushima-u.ac.jp/mrtg

### 4.2. リアルタイム端末利用状況

リアルタイム端末利用情報表示例を図 7 に示す.演習室毎に端末数,電源 ON である端末数,ログオン中の端末数,利用端末一覧を表示している.時間毎の利用者数の推移および演習室全体のネットワーク流量グラフも併せて表示している.

また利用端末一覧では,起動に要した時間およびネットワーク接続速度を併せて表示している.

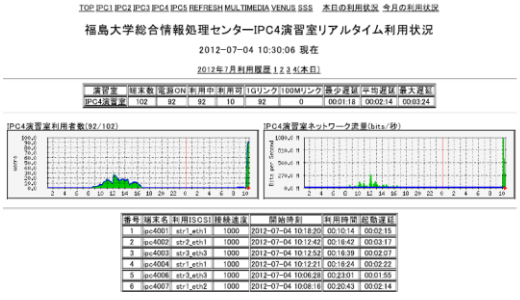



図 7 リアルタイム端末利用状況表示例

### 4.3. 日毎端末利用記録

端末利用状況を日単位でまとめた情報表示例を図 8 に示す.


図 8 日毎の端末利用状況表示例

### 4.4. 月毎端末利用記録

月ごとにまとめた情報表示例を図 9 に示す.

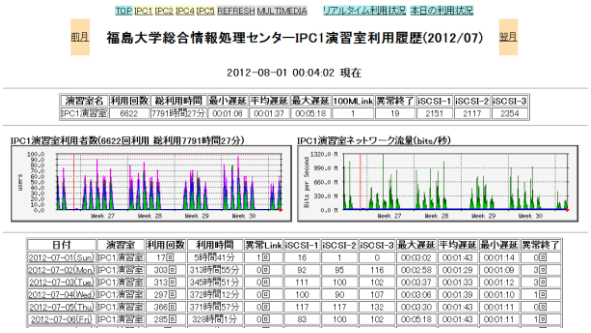



図 9 月毎端末利用状況表示例

### 4.5. セキュリティ関係

ユーザアカウント名は個人情報であるので表示に含めていない.データベースサーバが直接情報発信するのではなく,html ファイルを情報発信サーバに転送し,そこで発信するようにすることで,情報流出リスクを低減させている.

## 5. 管理者向け端末利用状況生成と表示

### 5.1. 管理者向け情報閲覧システム

データベースサーバに蓄積される情報から,ユーザアカウント情報を含む演習室端末利用状況を管理者向けに生成し,発信するシステムをユーザ向けシステムとは独立させて構築している.ユーザ向け情報発信とは別サーバで行っており,総合情報処理センター担当者端末のみ閲覧が可能なように IP アドレスアクセス制限を行っている.

以下の情報閲覧が行える.

(1) リアルタイム端末利用状況
(2) 当日を含む過去の日毎端末利用記録
(3) 当月を含む月毎端末利用記録

利用ユーザアカウント情報,所属学類毎の統計情報が表示に含まれる.

## 5.2. リアルタイム端末利用状況

リアルタイム端末利用情報表示例を図 10 に示す. 利用ユーザ ID, 端末記番, 利用ネットブート iSCSI, 接続速度, 起動遅延, 利用開始時刻, 利用時間が表示される他, 別フレームで演習室毎の利用者数, iSCSI ストレージ接続数が表示させている.

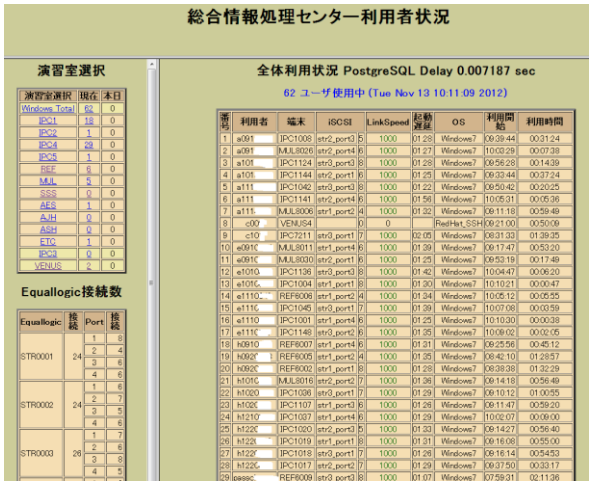



図 10 リアルタイム端末利用状況(管理者向け)

## 5.3. 日毎端末利用記録

全体の端末利用状況を日単位でまとめた情報表示例を図 11 に, 演習室毎の情報表示例を図 12 に示す. 全体情報では, ユーザの所属学類毎の利用者数が表示される.


図 11 日毎全体利用状況(管理者向け)


図 12 日毎演習室利用状況 (管理者向け)

## 5.4. 月毎端末利用記録

管理者向け月毎端末利用情報表示例を図 13 に示す.


図 13 月別端末利用情報表示(管理者向け)

## 6. 効果とまとめ

管理者向けに構築されることが多い端末管理情報表示システムに学生ユーザ向け機能を追加し構築した.アカウント不正利用の発見には,管理者側の努力だけでなく,学生ユーザ自身の日常的な不権限アクセス監視が必要である.本システムは利用履歴を利用者本人に提供する機能を有しており,本センターシステム全体のセキュリティ向上を期待しており,評価するためのデータ集積と解析を行っている.

また,起動所用時間情報や接続リンクアップ速度情報,ストレージ利用情報は新システム導入後の初期不良原因特定および対策に有効であった.

現在,安定した端末利用サービス提供が実現できており,セキュリティインシデントも発生していない.日常運用管理に尽力していただいている本センタースタッフおよび利用者である学生および教職員の協力に深く感謝する.

## 7. 参考文献


[1] 本田 : 多種 OS 対応端末利用監視システムの構築,平成 19 年度情報処理教育研究集会講演論文集

[2] 本田 : 学生アカウント状況記録閲覧システム, 平成 20 年度情報処理研究集会講演論文集

[3] 本田 : 仮想サーバとクラウドサービスを活用した演習室クライアントシステム構築の一例, 学術情報処理研究,No15 2011

[4] 本田 : iSCSI 型ネットブートシステム起動性能評価システム,学術情報処理研究,No16 2012

[5] オープンソース・ソリューション・テクノロジ株式会社 Unicorn ID Manager ページ http://www.osstech.co.jp/product/unicorn