プラクティス連携による学内統合認証基盤の構築
Construction of Practice-Oriented Authentication Infrastructure

小野悟 †, 黒木謙信 †, 谷重喜 †

Satoru Ono†, Kenshin Kuroki†, Shigeki Tani†

takumi@hama-med.ac.jp, k-kuroki@hama-med.ac.jp, tani@hama-med.ac.jp

浜松医科大学情報基盤センター †
Information Technology Center, Hamamatsu University School of Medicine†

概要

浜松医科大学では平成 24 年度に情報部門の組織再編成を行い，部門間の網羅的な連携を可能とする情報基盤センターを設立した．これに伴い，部門毎に管理運営されていた各種情報システムを統合すると同時にこれら情報システムを支える統合認証基盤を構築するに至った．本稿では，この統合認証基盤と各種情報システムの連携状況について説明し，実際に運用を行った結果の効用を考察する．さらに，それらの考察を踏まえ今後の課題について述べる．

キーワード

認証基盤, センター運営, IC カード, 電子メール, クラウド

1　はじめに

浜松医科大学では，平成 5 年度に全学的なキャンパス情報システムの導入を行い，これらの管理運営のため，約 2 年後の平成 7 年度に情報処理センターを設置した．キャンパス情報システムはキャンパス全域を網羅した有線ネットワークに加え，インターネットに接続するための各種ノード装置や，電子メールシステムおよび Web サイトシステムなどを主要構成物として運用が行われていた．一方，キャンパス情報システムが提供するインフラの一部を活用する形で，会計事務，人事事務などの業務用アプリケーションから構成される事務用電子計算機システムと図書館業務システムが並行して運用されていた．これらの管理運用母体は事務局であり，運用管理を担う専任のセクションとして平成 12 年度に情報企画室が設置された．

2 つの組織は必要に応じて連絡や協力体制を取りながら運用を行なっていたが，運用母体と予算管理が異なるため，各自が運用するシステム間連携は希薄であり，インフラとアプリケーションが分断されるという深刻な問題を抱えていた．このような問題点を解決すべく，2 つのドラスティックな改革を実施した．1 つ目は賃貸借契約を行なっている各システムの統合である．具体的には，平成 19 年度に事務用電子計算機システムと図書館業務システムを統合し，5 年後の平成 24 年度には事務用電子計算機システムとキャンパス情報システムを統合した．2 つ目は組織の再編成である．学内の主要な情報部門である教育研究系の情報処理センターと事務系の情報企画室を実務的に連携可能とするためには，部門間の横断的な調整が必要であり，困難を極めたが，約 2 年の歳月を費やしついにこれが実現した．この調整のために情報・広報担当副学長，研究・社会貢献担当副学長，事務局長および情報処理センター長ならびに技術部長の各面々が幾度と無くネゴシエーションを行い，基盤センター設立に関する協議を繰り返した経緯がある．組織の名は情報基盤センターに改め，従前は医療情報システム部門と兼任だったセンター長を専任として新規に雇用し，学内の各部門から網羅的に関係者を招集した．平成 25 年 5 月現在，情報基盤センターの構成員は 14 名である．なお，情報基盤センターの構成員にはすべて兼任発令を行い，運営に関する諸事項を整備するために，

情報基盤センター運営内規を策定した．

本稿では，教育研究系の情報システムと事務系の業務用アプリケーションを融合したキャンパス情報システムを支える統合認証基盤システムの全容について解説する．全学的な認証基盤の構築については，各大学で様々な取り組みが行われているが [1][2][3][4]，本学では特に業務指向でプラクティカルな実装を目標とした．第一章では，人事事務システムからの情報を源泉とする統合認証基盤システムについて説明する．第二章では，統合認証基盤システムの全景について述べ，続く第三章では，連携する応用アプリケーションについて説明する．第四章では統合認証基盤システムに関連する各種システムについて述べる．第五章と第六章ではシステムの稼働状況に関する説明と評価を行い，最後に第七章でまとめと今後の課題について述べる．

2　統合認証基盤システム

医学部の人事異動は煩雑多岐であり，且つ頻繁である．本学は医学部単科大学のため，その傾向が顕著である．そのような事情から人事異動情報はその発生源である人事事務システムから取得した．これらの情報は事務局内部で幾重ものチェックを経た信頼性の高い情報であり，電子的に連携を行うことで転記ミスなどの誤謬が飛躍的に低減可能である．また，学生情報については，同様の理由から学務情報システムから連携している．各システムから取得可能な教職員および学生の基本プロファイル情報には，職員証（学生証）の作成時などに必要となる顔写真や，アカウントのパスワードなどのメタデータが付加されつつ，統合認証アカウントデータベースに格納される．データベースを保有するアカウント管理システムとして，ソリトン社の ID Admin[5] を採用した．ID Admin は Microsoft 社の Active Directory や，OpenLDAP などの主要なディレクトリ管理システムと連携が可能であり，連携時に任意のクエリを発行することができる他，連携先のシステムが必要とする各種フォーマットに対応した任意のファイル形式を作成することができる．すなわち本認証基盤システムは，アカウントデータベースである ID Admin と，認証のインタフェースシステムである統合認証 Active Directory および事務局認証 Active Directory の 3 つの要素から構成されている．主要な連携システムを含むシステムの全容を図 1 に示す．連携先の各種システムについては，次節以降で説明する．

統合認証 Active Directory には，カレントで在職中あるいは在学中の教職員および学生のアカウント情報がすべて格納されている．ID Admin と本ディレクトリはネイティブに連携されるため，外部ファイルなどの媒体を介する必要がない．ID Admin に職員や学生の異動情報が格納される都度，ディレクトリ情報が更新される仕組みになっている．異動情報は採用時（入学時）であれば，職員証（学生証）の発給と同時に入力されるため，ほぼリアルタイムに更新される．アカウント情報が職員である場合，次のプロパティを保有する．

- 氏名
- アカウント名（個人番号）
- 生年月日
- 性別
- 所属名称
- 属性
- IDm コード
- パスワード
- 発行回数

学生の場合にはこれに加えて学科情報が保存される．なお，本学は医学部単科大学であるため，学部情報は必要としない．属性は学生と教職員の区分に利用される．IDm コードとは，職員証（学生証）として採用する FeliCa タイプの IC カードに付番されたユニークな番号のことをいう．パスワードには英数字をランダムに配置した 12 桁の文字列が初期値として登録されるが，Web アプリケーションを通じて利用者が任意のものに変更可能である．発行回数には職員証（学生証）の発行回数が格納され，初期値は 1 である．これらのプロパティの利用方法については次節以降で後述する．

さらに本ディレクトリは，無線 LAN システムの 802.1x Radius サーバおよび学務情報システムの認証サーバ，さらに証明書自動発行機の認証サーバとして機能する．また，後述する電子メールシステムとアカウント同期を常時行なっている．事務局ではシンクライアントシステムを採用しており，各種利用権限の設定に必要となるアカウント情報のプロパティが多岐に亘るため，統合認証 AD とは別に事務局認証 AD の設置をした．

事務局認証 Active Directory には，所属情報が事務局属性であるアカウント情報がすべて格納されている．統合認証 AD と同様に ID Admin とはネイティブに連携する．事務局職員には 1 人 1 台ずつ端末装置が配布されており，装置起動時の認証には職員証が利用されている．これらの端末装置はネットワークブート型のシンクライアントシステムであるため，補助記憶のリソースはすべてファイルサーバに依存している．各種リソースに対する利用権限はその職員が所属する部署に相関するため，割り当てるべきリソースを自動的に構成するように設定した．このように端末装置内部に情報を保有しないので，事務局で毎年必ず実施される職員の所属異動の際にも，サーバ内部に仮想的に保管されたプロファイル情報を用い，事務局内に設置された任意の端末装置において，任意のタイミングで職員が構成した環境を即座

に展開することが可能である．セキュリティ面では，職員証の盗難・紛失時を考慮し，認証因子としてパスワードの同時入力を必要とした．その他，事務局に設置される複写機の利用時においては，消費枚数の把握や適切な利用制度を担保するため，職員証を利用した認証によって正当な利用者の判別を行なっている．

図- 1: 統合認証基盤システムの全容

3　連携システム

現在，統合認証基盤システムから直接データ連携するシステムは次のとおりである．

- 入退出管理システム
- 職員証（学生証）発行システム
- 電子メールシステム

3.1　入退出管理システム

本学では平成 18 年度から病院再整備計画が進行しており，これを機に病棟および外来棟への入館ならびに棟内の重要区域などへ入退出するため，IC カードを用いた電子錠による入退出管理システムを導入した．これ以前にも一部の附属施設では独自の入退出管理システムを導入していたが，同時期に認証キーとして利用する IC カードをすべて FeliCa に統一し，必要な箇所はカードリーダの更改を行った．しかし，学内に複数稼働するそれぞれの入退出システムが必要とするアカウント情報を一元的に管理する必要があり，統合認証基盤システムから各システムへの連携を行うこととした．特に附属病院においては，重要区域への入退出情報が職責や配属部署によって異なるため，これらの入退出権限をパターン化し，連携時に自動的に入退出権限を付与することを可能とした．従前は夫々の入退出管理システム毎に認証デバイスである IC カードの発給を行なっていたが，これを統合することによって，発給業務の一元化と発給対象者の厳格化が実現した．入退出に必要なデバイスは，職員証（学生証）を活用しているが，紛失・盗難時の悪用などを考慮し，認証キーにはカード固有情報である IDm コードを利用している．

職員証（学生証）の IC カード化を実施するため，平成 23 年度に実施した職員証の更新時期に合わせて，全職員および全学生について既存カードの更改を実施した．この際，一部の職員は，既に入退出に必要な IC カードを発給済みであったため，これらの職員には職員証券面のみを印字した PVC カードを発給することとし，既に発給済みの IC カードと PVC カードを同時に封入可能なカードケース（図 2）を利用することで発給コストを大幅に削減した．

全学共通の入退出管理システムを利用するのは原則として建物への出入り口と建物内部の重要管理区域であるが，区域外であっても部局等の要望に応じて IC カードインタフェースを有する鍵収容箱を設置し，職員証による鍵管理を可能とした．この鍵収容箱は利用者の本人照合を職員証で行い，管理者が許可した鍵のみを取り出し・返却することが可能である．さらに鍵の利用ジャーナルが管理用コンピュータに逐次記録可能なため，入退出管理システムと同等の安全性が確保できる．

なお，本学で稼働する入退出管理システムのネットワークには Ethernet を利用している．このネットワークインフラはキャンパスネットワークと同種でありながら，物理的に分離して設置をした．コストや利便性の面からは不利であるが，ネットワークを流通する情報のセキュリティレベルや利用目的が全く異なるためであり，利用者および建物管理の安全性を優先した結果である．

図- 2: PVC カードと IC カードの同封

3.2　職員証（学生証）発行システム

職員証と学生証は施設への入退出キーとしても利用可能であるため，採用（入学）時直後から必ず携帯しなけらばならない．したがって，統合認証基盤システム

に格納される各種アカウント情報の登録トリガは職員証（学生証）の作成時となる．人事事務システムから作成される所定のフォーマットの異動情報ファイルを用いて，カードの作成を実施する．認証基盤システムとしてのアカウント管理上，人事システムから捕捉しなければならないイベントはアカウントの「追加・変更・削除」の 3 点である．しかし，これらのイベントをすべて連携した場合，問題が生じる．一例として，非常勤職員の「限り退職」と称する発令行為は，実際には退職しないが，書類上の手続きの関係で退職発令がされるのが慣例である．このような発令は人事システム上で連携データに含まれないようなアルゴリズムを構築した．このように事務的には必要なイベントでも，情報システム管理上では不要なイベントが種々存在するため（例えば，育児休業や休職など），これらのイベントをフィルタリングすることが肝要である．また，大学院生はリサーチアシスタントやティーチングアシスタントなど職員として雇用発令する場合がある．この場合，同一人物に対して複数のアカウントを発給するが，プライマリとするべきアカウントを捕捉するためには，人事・学務の両システムから発生する異動情報をヒストリカルに連動させる必要がある．現在は目視による確認で対応しているが，システマティクな対応が望まれる部分であり，鋭意アプリケーションを開発中である．

FeliCa の IC チップには 2KB のユーザエリアが実装されている．同エリアを用いて 6 つのエリア区分を行った．それぞれのエリアを用いて入退出管理，PC セキュリティ，キャッシュレスシステム，個人認証サービスなどを利用可能としている．また，共通エリアとして本学が独自に設計したフォーマットを区分した．同エリアには次の情報が格納されており，サードパーティ製のアプリケーションから読み取りが可能である．

- 個人番号（学籍番号）
- 漢字氏名
- ローマ字氏名
- 発行回数
- 性別
- 生年月日
- 開始年月日
- 終了年月日
- 予備

発行回数は 3.1 節で述べた統合認証 AD のアカウント情報が保有する発行回数プロパティと同期が取られており，認証因子として活用される．カード単体で認証を行う一因子認証方式では，カードの盗難や拾得などによって第三者が不正に入手したカードを悪用するリスクがあるためである．つまり，カード内部の認証コードに加え，発行回数を同時に照合するようにし，不正入手したカードは利用できないようにしている．終了年月日には職員証の有効期限満了日（開始年月日を問わず 2016 年 3 月 31 日で固定）が格納される．本学では職員証の有効期限を 5 年間として設定しており，更新後旧カードは論理的に利用できなくなる．予備エリアは 64Byte が利用可能である．

職員証（学生証）の作成時に利用者を視覚的に識別することを可能とする顔写真を撮影する．このデータは職員証（学生証）への印刷に利用されるだけでなく，人事事務システムおよび学務情報システムへとフィードバックされ，職員および学生のプロファイル情報として活用されている．発行回数や開始終了年月日など人事事務システムから取得できないアイテムについては，この段階でデータがマージされ，統合認証基盤システムへインポートされていく．なお，職員証（学生証）の発行業務はデータの準備から実際の印刷・発行に至るまですべて学内で行なっている．特に学生証の発行に関しては，合格者の最終確定が例年 3 月末日であり，カードの配布までの期日が数日しかなく，外部業者への委託が困難なためである．

3.3 電子メールシステム

本学では，キャンパス情報システムの更新を機に，従来はオンプレミスで運用されていた電子メールシステムをクラウド化すると同時に Microsoft 社が提供する Office365(o365)[6] に完全移行を行った．Microsoft を含め，Google や Yahoo!など大手のプロバイダはアカデミックエディションと称して，これらのサービスを高等教育機関に無償で供与している．o365 ではアカデミックエディションが最上位版であるエンタープライズ版とほぼ同等の機能が利用できる．オンプレミスで同等の機能を有するシステムを構築した場合，相応のコスト負担を余儀なくされることに加え，管理運用のために専門的知識を有する技術者が必要となる．本学は医学部の単科大学であるため，情報分野の専門家は希少であり，その育成も困難であることや，大規模な震災時における情報伝達手段の担保，さらにはシステム内部の情報保護などの観点から電子メールシステムの外部移管を選択した．選択にあたり，Office365 のほか，Google Mail，Yahoo! Mail，有償のプロバイダメールシステムについて比較を行った．結果，o365 と Google Mail の両者は機能面において殆ど差異がないことがわかった．しかし，2012 年 3 月 1 日に Google が表明したプライバシーポリシーの内容に鑑み，利用者の情報保護の観点から o365 を採用することとした．外部移管にあたっては学内のコンセンサスを得る必要があり，これを実現すべく全職員に対してパブリックコメントの募集を行った．多くの利用者は既存システムのメールスプール領域の

狭隘さに不満を感じており，移行に対しては概ね肯定的であったが，一部の利用者は秘匿性の高い情報を外部移管することに対して抵抗を感じていたため，そのような利用者のために学内で数回説明会を開催した．また，電子メールシステムの移行にあたっては，最大の関門が利用者のパスワードの取り扱いであった．Unix ベースの OS で運用されていた旧システムのアカウントのパスワードは/etc/passwd などにハッシュ化されて保存されており，同一のハッシュアルゴリズムを利用している OS であればバイナリレベルで移行は可能であるものの，今回は全く異なる環境への移行であるため，この方法が利用できない．このため，Web ベースのパスワード変更プログラムを新規に開発し，このプログラムを通じて入力されたパスワードは，既存 Unix システムと統合認証 Active DIrectory および o365 の 3 つのパスワードを同時に更新できるようにした．その後，すべての利用者に対して本プログラムを用いて期日までにパスワードの変更を行って欲しい旨の通知を発布することで旧システムから新システムへのパスワードの移行を実施した．

o365 と Active Directory は同一のベンダが提供する製品であるため，両者の親和性は高い．電子メールシステムとディレクトリサーバの連携に関しては，文献 [7] などでその有効性が古くから提言されている．統合認証 AD に格納されたアカウント情報のすべてのプロパティが o365 に同期可能である．これらのプロパティを利用して，o365 では動的配布グループという機能が利用できる．この機能は，アカウント情報のプロパティに対するクエリを設定し，その応答結果を電子メールの送信グループとして活用するものである．例えば，教職員全体にメールを送信したいというニーズは高いが，採用や離職に対するメンテナンスが常時必要であり運用コストが大きい．しかし，動的配布グループ機能を活用し，「教職員」というプロパティを有するグループを作成するだけで，これが実現可能である．現在本学では，教職員全体，学生全体，さらに学生においては各学科別の動的配布グループを作成し，活用している．今後，ニーズに合わせた様々な配布グループを作成する予定である．

リプレイス以前は，職員の電子メールは申請制としており，利用者が希望する任意の文字列がメールアドレスとして供与していた．このような運用の場合，メールアドレスを保有する職員とそうでない職員が混在してしまうこと，関係者が任意の職員のアドレスを知る術がないなどの問題があるため，リプレイス後は採用された職員すべてにメールアドレスをもれなく発給することとし，アドレスのフォーマットは”職員番号@hama-med.ac.jp”をデフォルトとした．このアドレスは利用者が申し出ることで任意の文字列に変更可能であるが，o365 では，学内全体を網羅した共通アドレス帳が利用可能であり，氏名や所属などから任意の利用者のアドレスが検索できるため，前述の問題は生じない．電子メール機能の他，スケジュール管理機能や，施設予約管理機能が無償で利用可能である．これらの機能は iPhone などの携帯デバイスと簡単に同期が取れるため，利便性が高い．

o365 のインタフェースは送受信メソッドともにすべて SSL による暗号化が必須である．しかし，従前運用されていたオンプレミスのシステムでは，POP，SMTP ともに SSL には非対応であった．このため，o365 へネイティブに接続するためには，ユーザ側のメールソフトウェアの設定変更が必要となる．学生も含めて 3 千人近い利用者が漏れなくこの設定変更を期限内に行うことは困難であることと，移行時のトラブルを軽減する目的で，SSL ゲートウェイサーバを学内に設置した．このサーバの FQDN は従前のオンプレミス時に利用されていたメールサーバのものと同一とし，基本的には利用者側の設定変更を行うことなく新メールシステムに移行できるようなシステム構成とした．ただし，これらは移行時の暫定的構成であり，徐々に o365 ネイティブ環境への移行を促す方針である．

4　その他の関連システム

統合認証基盤システムとは直接連携しないが，アカウントの認証を通じて以下の 3 つのサブシステムが稼働している．

- 無線ネットワークシステム
- 学務情報システム
- 証明書自動発行機

以降，それぞれのサブシステムについて説明する．

4.1　無線ネットワークシステム

リプレイス以前には一部の区域で無線ネットワークを提供していたが，今回の更新で約 300 台の無線基地局を設置し，キャンパス全域で利用可能な無線ネットワークを整備した．無線ネットワークシステムの選定にあたっては，次の 3 点に留意した．

1. AP への一斉アクセス時に電波リソースが均等に配分されること．
2. 集中管理可能な無線ネットワークシステムであること．
3. シングルチャネルに対応していること．

1 点目は，電子会議や授業で利用する場合を想定している．会議資料や授業の教材などを電子的に閲覧した際，参加者ほぼ全員が同時に資料を開くことが可能なことが望ましい．会議や授業の進行上，時間がかかった端末を閲覧状態になるまで待つことは効率が悪いためで

ある．2 点目は，従来の無線ネットワークではアクセスポイント毎に設定が必要なため，管理運用コストがアクセスポイントの増加に比例して大きくなることを抑制するためである．チャネル制御や，SSID，アクセスキーなどの設定が集中管理できることは数百台のアクセスポイントを効率よく運用する上では必須の機能である．最後の 3 点目については，セル設計の容易さと既設機器へのチャネル干渉を考慮した結果である．シングルチャネル技術を用いることで，無線ネットワークでは避けて通れないカバレッジホールの軽減に加え，セル設計が極めて容易になる等のメリットが生じる．また，学内には既に各研究室などに個別に設置された無線基地局が運用されており，これらの機器への電波干渉を回避しなければならない．シングルチャネルを利用することで，電波リソースの消費を最小限に抑え，既設の無線機器への干渉を最小限にとどめることができる．このような要求要件を満たすものとして，本学では MERU Networks 社の無線ネットワークシステム [8] を採用した．基地局装置の設置例を図 3 に示す．無線ネットワークの利用には統合認証 AD と連携し，Captive Portal によって認証を行なっている．認証アカウントは電子メールシステムと共通である．

図- 3: 無線ネットワーク基地局の設置例

4.2 学務情報システム

学務情報システムは業務用アプリケーションであり，機能面の詳細については本稿の主旨を逸脱するため割愛する．本学では，学務情報のシステム化が遅れており，キャンパス情報システムの更新に合わせて，商用パッケージ型学務情報システムを調達することとした．学務情報システムでは，学生の個人情報を取り扱うため，アカウントの使い回しや貸借などを防止する必要がある．これを心理的に抑制するために，学務情報システムの認証サーバを統合認証 AD とし，無線ネットワークシステムと同様，電子メールシステムのアカウントと共通のものを利用することとしている．

4.3 証明書自動発行機

多くの大学では証明書発行機のサービス対象は学生のみであるが，本学では教職員もサービスを享受可能としている．現在，職員が出力可能な帳票は在職証明書と源泉徴収票の原本証明書の二種類であるが，今後充実させていく予定である．装置の外観を図 4 に示す．

証明書発行機の利用は職員証（学生証）のみの一因子認証方式であるが，前述したとおり認証時にカード内部に記録されている発行回数フラグを参照するため，不正入手したカードの利用はできない．利用者アカウントの認証は統合認証 AD を参照する．

図- 4: 証明書自動発行機の外観

5 運用状況

システムの稼働開始から約半年が経過し，導入過渡期特有の利用者からの各種問合せや，ソフトウェアエラーなどは収束した．しかし，一方で多くのシステムがネットワークを通じて統合認証システムに依存するようになり，ネットワークインフラの重要性が増大している．このため，これを機にキャンパスネットワーク内に整備された各種ノード装置をリアルタイムに監視可能なネットワーク監視装置を導入した．本装置は主に snmp をトラップすることによって障害や輻輳およびこれらの予兆などを検知するものであるが，ノード装置の物理的な設置場所を容易に特定するべく，建物の平面図面にノー

ド装置をプロットしていることが大きな特徴である．また，監視装置が出力する各種情報を基盤センターの執務室内に設置した大型モニタに常時投影しており，ネットワークインフラに対するインシデントをいち早く把握可能とした．

また，運用面については，アカウントのパスワードの取り扱いをより厳格化した．統合化以前の各システムのパスワード忘失については，電話連絡によって事案を受け付け，その都度再発行を行なっていたが，統合化後は本人認証のために所定様式を用いた再発行依頼に基づき，本人宛の親展通知文書を発給することとした．これらの運用変更は，業務レベルでは煩雑となるものの，利用者のパスワードの取り扱いに対する意識レベルの向上が期待できると考える．

6　導入後の評価

今回のリプレイスでは，電子メールシステムの抜本的更改を行ったため，導入直後は電子メールに関する多くのトラブルが発生したが，約一週間で鎮静化した．トラブルの内容としては，メーラの送受信プロトコルの実装が標準的仕様と微妙に異なるために SSL ゲートウェイサーバが応答できないというケースが最も多く，このようなケースでは個別に設定の変更を行い，o365 に直接接続するよう対応した．認証系に関する大きなトラブルはなかったが，パスワードをメーラに記憶させていて，これを忘失したユーザが多く，そのような利用者に関しては，逐次パスワードを再発行することで対処した．また，フリーソフトのメーラを利用するユーザも多く，この場合メーカのサポートが得られないため，送受信プロトコルの詳細仕様の把握にはそれらの通信ログから解析するしかなく，この作業は難解を極めた．各種障害対応を通じて，近年の電子メールシステム環境は，送受信プロトコルの SSL 対応や，smtp 認証の多様化等，設定方法が多岐に亘るため，情報システムに関する基本的知識を持たない利用者が正確な設定を自ら施すのはかなり敷居が高くなっていることを感じた．一部のメーラは電子メールアカウントのドメイン情報から，電子メールの送受信に必要な情報を自動設定するものがあるが，ネットワークの環境によってはそれらが機能しない場合もあった．電子メールシステムの障害対応は学内外を問わないため，解決が長期に及ぶ場合がある．図 5 にシステム導入直後からの障害発生件数の時系列な推移を示す．

電子メール以外の障害では，事務局のシンクライアントシステムに関するものが 9 割以上を占めている．リプレスに起因する障害が完全に収束したと判断されるまで約二ヶ月間を有したが，その間に発生した障害総件数は 182 件であった．

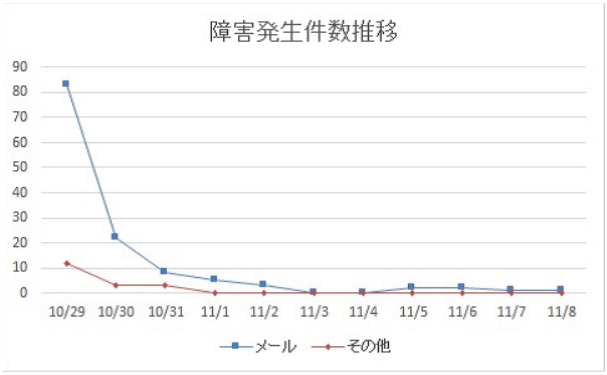

図- 5: システム導入後の障害発生件数推移

情報システムの故障率は，一般に 3 つの段階を経て変化をするバスタブ曲線で表記される．本グラフ曲線は初期故障期（10/29〜11/2）と偶発故障期（11/3〜）を示しているといえ，したがって今後の故障率は一定であり，これを求める信頼度関数は次式による．ここで平均故障率 λ は偶発故障期区間から算出し，0.1 とした．ただし，障害症例数には人為的エラーが含まれていることに留意されたい．

$$R(t) = e^{-\lambda t} \tag{1}$$

(1) 式より，信頼度 $R(t)$ は 0.904 が算出される．JUAS（Japan Users Association of Infomation Systems）が実施した企業 IT 動向調査 2011[9] によれば，日本の基幹系情報システムの信頼度は 99%を超えており，世界的に見ても高水準である．本システムの稼働率は同指標を用いた場合平均以下ではあるが，信頼性を上げるためには相応の構築・運用費用が必要であり，過剰な信頼度の追求は，費用対効果の観点からも好ましくない．著者らはシステムの評価指標として，信頼性や可用性だけでなく，ユーザビリティやオペラビリティが重要な要素であると考える．これらの評価には多くの時間と信頼性のあるサーベイが必要である．現時点における運用的評価としては，採用者および離職者に対するアカウント処理がシステマティクに行われることで従前は技術職員が逐次コマンドを投入していた作業が大幅に簡略化・平準化され，その結果，作業内容の本質が変革し，業務の継続性が担保されたことである．また，一元化されたアカウント中に，電子メールシステムや証明書自動発行機を含めることにより，アカウントの使い回しや賃借などの行為が心理的に抑止されていると推察できる．何故なら学務情報システムのカスタマイズとして，秘書による教員の代行入力機能が強く要望されたからである．

7　まとめと今後の課題

本稿では，教育研究系の情報システムと事務系の情報システムを融合したキャンパス情報システムを支える統合認証基盤システムの全容について述べた．黎明期の情報システムは一部の好事家が利用するニッチなガジェットであったが，今や教育研究は言うに及ばず，各種業務用途等広範囲に利活用が進んでいる．大学という組織の中で情報システムが有効に機能するためには，学内を横断的に網羅した実践的なデータ連携が必要であり，今回はこれを目標とした．人事発令と完全に連携した各種アカウント管理は信頼性が高く，安定した認証基盤を構築することができた．所謂口コミでアカウントを取得していた従前の運用が改善できた意義は大きい．しかし，一方で人事的発令行為が伴わない構成員が少なからず存在するため，例えば一部の研究員や，臨床協力医などの取り扱いをシステム化することは今後の課題である．

今後はこれらの認証基盤を活用し，各種学術情報リソース（電子ジャーナルや文献データベース）への相互認証連携を実現することを計画している．具体的には，国立情報学研究所が運営する学術認証フェデレーションへの参画である．現在，Elsevier，Springer，Thomson Reuters，IEEE など主要なサービスプロバイダが参画しており，その利用価値は大きい．相互認証連携の実現後は，安全な認証基盤を用いた VPN を通じて学外からの学術リソースへのアクセスも早期に実現したい．また，国際無線 LAN ローミング基盤である eduroam への参加も検討している．eduroam は多くの国が加盟するキャンパス無線ネットワークの国際的なデファクトスタンダードとも言われており，自局が発行するアカウント情報で訪問先の無線インフラが利用可能な優れた技術である．利用者の利便性をまず第一に考え，今後の取組を進めていきたいと考える．

参考文献

[1] 江原康生: 大阪大学における新全学 IT 基盤システムの構築と運用, 電子情報通信学会論文誌 J95-D(5), pp. 1172–1182 (2012-05-01).

[2] 宮本貴朗，小島篤博，青木茂樹，西本隆，金森剛志，山本貴史，上田博文: 大阪府立大学における認証基盤の構築, 電気学会研究会資料.IS，情報システム研究会 2008(23), pp. 31–36 (2008-09-11).

[3] 奥村勝，本山聡，三河邦夫: 福岡大学における統合認証システムの構築と運用について, 情報処理学会研究報告.DSM，[分散システム/インターネット運用技術]2006(38), pp. 7–12 (2006-03-29).

[4] 伊東栄典: 九州大学全学共通認証基盤と全学共通 ID「SSO-KID」の紹介, 九州大学情報統括本部 IT マガジン 1(2)，pp. 42–48 (2007-07).

[5] https://www.soliton.co.jp/products/management/idadmin/index.html

[6] http://www.microsoft.com/ja-jp/office/365/default.aspx

[7] 廣澤敏夫, 吉澤康文, 伊藤勉: 電子メールシステムのメールアドレス・ビュアによるディレクトリサーバ連携と移行方式, Vol. 42, 情報処理学会論文誌 No. 12, pp. 2847–2859 (Dec 2001).

[8] http://www.merunetworks.co.jp/

[9] http://www.juas.or.jp/servey/it11/it11_summary.pdf