紹　　介

midPoint 始めました

永 井 孝 幸*
nagai@kit.ac.jp

1. はじめに

2022 年に導入した第 11 世代情報基盤計算機システム（System11）では、システム利用者の原簿管理を行うシステムにオープンソースソフトウェア（以下 OSS）の midPoint を採用しました。midPoint は Evolveum 社が開発した「ID ガバナンス（ID 統制）」を実現するソフトウェアです。midPoint を使って利用者情報（氏名、パスワード、システム利用資格等）を集中管理し、LDAP や ActiveDirectory 等の認証基盤と連携させることで利用者の種類に応じたきめ細かいサービスを提供することができます。

本稿では midPoint 導入の背景と midPoint の使い方について紹介します。

2. 利用者原簿と認証基盤

俗に「コンピュータ、ソフトが無ければただの箱」と言われますが、情報システムもデータが無ければ使えません。本学の情報基盤計算機システムでは人事システム・学務システムのデータと連係してアカウントを発行し、どのシステムでも同じアカウントで利用できるように認証基盤に情報を登録しています［1］。システム毎にバラバラにアカウントを登録するやり方は手間がかかるだけで無く、使われない古いアカウントが放置されて不正アクセスの温床になる等、セキュリティ上の問題も引き起こします。このような問題が起きないようにするのが利用者原簿管理システムの役割です。

利用者原簿管理システムは人事システム・学務システムに登録された情報を自動的に取り込み、原簿上のユーザ情報（氏名、所属、職種、離籍日など）を元にアカウントを生成して認証基盤に登録します［2］。これに加えて、利用者自身でパスワード変更や利用サービスを指定できるようにする「利用者ポータル」の機能や、利用者原簿を閲覧・修正するための管理者機能も提供しています［3］。

利用者原簿管理システムは大量の個人情報を取り扱うため高いセキュリティが求められる［4］［5］だけでなく、ユーザ情報からアカウント情報（アカウント名に加え、パスワード・メールアドレス・ホームディレクトリ・利用資格など各システムの利用に必要な属性を加えたもの）を生成するための設定が複雑なため、導入するのは一筋縄ではいきません。これは「提供したいサービス内容と要求されるセキュリティ水準」という「人の言葉」をソフトウェアの設定という「コンピュータ用の言語」に解釈しなおす必要があるためです。

今回導入した midPoint はこれらの要求を満たす数少ないソフトウェアの一つです。

2.1　midPoint とは

midPoint（https://evolveum.com/midpoint/）は Evolveum 社（本社スロバキア）が開発した「ID ガバナンス（ID 統制）」を実現するソフトウェアです。従来からある ID 管理システムのように利用者原簿に登録された情報を外部システム（LDAP, ActiveDirectory, Database, CSV ファイルなど）に配信するだけではありません。事前に定義したルールに基づいて各アカウントにシステム利用資格を割り当てたり、Web 画面を通じてサービス利用資格を要求・承認したりする「ガバナンス」機能が整っていることが特徴です。

日本ではあまり知られていないソフトウェアですがその歴史は長く、2011 年の 5 月に最初のバージョン 1.7 がリリースされてから毎年数

＊情報工学・人間科学系 准教授 /
情報科学センター副センター長

回のバージョンアップを繰り返し、本稿執筆時点（2023年9月）の最新版がバージョン4.7.1です。

midPointはForgeRock社により開発されていたOSSのID管理ソフトOpenIDMが非OSS化されたことを受け、元開発者らが独立して新たにOSSとして開発したという経緯があります［9］。企業が主体となって開発するOSSでは「コアとなる基本機能だけを公開し、実環境での利用に不可欠な機能（LDAP連携やクラスタリング機能など）を別途有償で販売する」というビジネスモデルをとることもあるのですが、Evolveum社はその方針はとらずmidPointの全ての機能がOSSとして公開されています。

3. System10からの宿題

利用者原簿管理システムの入れ替えは影響範囲が大きいため、「動いているプログラムは触るな」というエンジニアの感覚からすると、できるだけ長く同じシステムを使いたいところです。そうは言っても情報基盤計算機システムは定期的（4年､5年間隔）に更新することになっていますので、システム更新をどう乗り切るかが大きな課題になります。

今回のSystem11の調達をどうするかあれこれ考えをめぐらしていたある日のこと、現行システム（System10）の業者から「次期システムの入札には参加しない予定」との情報が寄せられます。これは2010年に導入したSystem8以来、10年以上にわたって作り込まれてきた業者独自部分を手放すことを意味します。前向きに捉えれば古いシステムを刷新するよい機会ですが、移行先のシステムがあるかどうかが問題です。この業者独自部分は業務上の勘所をよく押さえてあり、

- アカウント（CISアカウント、KITパーソナルID）発行管理
- 利用者原簿管理
- 利用者ポータル（パスワード変更、利用サービス指定、確認テスト連携）
- 認証基盤連携（アカウント情報配信）

という、いずれも無くなれば全システム・全利用者に影響が出る機能を提供していました。

実は、この部分については2017年にSystem10の仕様検討を行った時点で「そのまま置き換えられるような代替製品は存在しない」というのが私の結論でした（System10についてはSystem9と同じ業者が落札したため、幸いこの業者独自部分はそのまま引き継がれました）。

「現行システムの機能をもれなく次期システムの仕様書に盛り込めば、他の業者がぴったりなシステムを持ってきてくれる」かというと、話はそれほど簡単ではありません。あまりに詳細な要件を仕様に盛り込むと、「業者が提案できる製品が存在しない」ということになり入札自体が不調（不成立）に終わってしまいます。かといって仕様に漏れがあると、本学の実情に合わない、使い物にならないシステムが導入される恐れが出てきます。

となると、どういう既存の製品やOSSの組み合わせなら現実的に業者の提案が可能になるか、System10と同等の仕組みを再現できるか、System11の仕様を決める前に自分の中で答えを持っておく必要があります。

3.1 小規模組織に足りないもの

System9からSystem10への切替で痛感したことは、「我々の組織（情報科学センター）では短期間で全部のシステム更新をやるのは無理がある」ということでした。利用者にできるだけ影響が出ないように旧システムから新システムに切り替えるため、System10では2018年の2月末稼働に向けて2018年に入ってから一斉に各システムの更新と動作テストを行いました。業者の方は大手SI業者だけあってシステム切替の山場では人員を増員して膨大な作業をさばいていきます。一方、大学側の我々は2月といえば学期末対応・学生指導に追われる時期です。業者側で全ての作業を滞りなく終えられればよいのですが、実際にはシステムが思ったように動かない部分の対処に共同であたることになります。一つ一つの不具合は数時間程度で解決するものであっても、それが一斉にやってくると対処しきれません。

「マネジメント力」―これが我々小規模組織の弱みであり、大手業者の強みとなる部分です。刻々とシステムの切替が一斉に進む中､「ど

のシステムで不具合が発生し、どの不具合が作業中の一時的な不具合で、どの不具合が本当の不具合で、どの不具合が対応中で、どの不具合が手つかずで、どの不具合をどう直すか、どの作業の順番を変更するか、次にどの作業を実施するのが効率的か」等、全体の状況を把握し作業指示を出すことに専念するマネージャーがいるかどうかでシステム切替の成否が決まります。小規模組織の我々には専属のマネージャーを置く余裕はなく、非常に苦しい状況になります。System11 では利用者原簿管理システムの更新が避けられないとすると、このマネージメントの問題が更に深刻になります。

3.2 小規模組織としての戦略

リソース（人、モノ、金、時間、情報）が足りなければどうするか。手持ちのリソースを有効に活用するのはもちろんですが、外部のリソースを活用することができればリソース不足を補うことができるはずです。そのための方策が標準技術とオープンソースソフトウェア（OSS）の活用です（内部のリソースを増やせるともっとよいのですが、単純にはできないのでその話は横に置いておきましょう）。

インターネットはその生い立ち（当時の大手通信事業者に対するアンチテーゼ）から技術を独占することをせず、積極的に標準技術として公開し、世界中の誰もがインターネットの普及と発展に参加できるようにすることで成功を収めました。そのおかげでインターネットの標準技術であれば様々な手段で入手することができ、学会などのつながりを通じて専門家の助言を得ることもできます。標準技術を用いて作った情報システムであれば、同じ技術に基づく他の製品に置き換えることも検討しやすくなります。

これはどういうことかというと、企業独自の技術で作られたシステムの場合は詳細が非公開なため、「技術的にできる / できない」という根本の部分の判断について業者側の説明を信じるしかありません。一方で標準技術については我々と業者の間に情報の非対称性がありませんので、対等の立場に立てます。技術的な問題や実現可能性の検討については実際の業者が決まるよりも前から考えることができ、時間を味方につけることもできます。本学の情報システムについて言うと、ネットワーク部分については標準技術を積極的に採用する方針で整備を続けてきました。そのため過去に整備した設備が無駄にならず、システム更新を繰り返しながらノウハウを蓄積することが出来ています。

同じように本学で継続的に発展しているシステムに Moodle があります。Moodle は全世界で利用されているオープンソースの学習管理システム（LMS）で、本学では 2008 年にパイロットシステムとして導入された後［7］、バージョンアップを繰り返しながら着実に利用者を増やしてきました。LMS にはこれまでに作られた教材や課題、提出物など、大勢の活動の成果が蓄積されています。それだけでなく、LMS のどの機能をどう使えば教育上効果的か、というノウハウも暗黙知として蓄えられています。もしシステム更新によって全く別の LMS になりこれらの成果が使えなくなったとすると、使い方を覚え直したり、教材を作り直したりと大きな損失になります。「同じことを別のシステムでもできるようにする」という現状維持のためだけに貴重なリソースを投入するのは避けたいところです。

OSS は特定企業の製品ではないため、入札仕様書に具体的なソフトウェアを指定することができます（政府調達の入札仕様書には例外的なケースを除き、特定企業の製品を指定することができません）。また様々な業者が取り扱っていますので、ある業者が取り扱いをやめても他の業者から調達することができます。長期的に知的資産（暗黙知も含めた知識やコンテンツ）を蓄積していく情報システムには、入札結果によってある年に突然無くなってしまうかもしれない特定企業の製品よりも、OSS のほうが適していると考えられます。

以上のような考えをもとに立てた作戦はこうです：

1. OSS を使った技術検証環境を先に立ち上げ、System11 への移行に必要な技術的な課題を事前に洗い出しておく
2. 知的資産が蓄積されるシステムでは継続性を重視し、OSS での構築を視野に入れる

導入業者が使える時間は落札からシステム稼働まで半年程度しかありませんが、こちらは次のシステム更新まで年単位の猶予がありますので、標準技術とOSSの組み合わせで時間を味方につけることができれば何とかなるだろうという発想です。

OSSを使えばうまくいくような話ばかり書いていますが、もちろん話はそんなに単純ではありません。OSSは特定企業の製品ではないがゆえに、「何のためにどう使うか」「どう組み合わせるか」を自分で考える必要があります。整ったマニュアルもありません。企業の製品であれば製品の利用場面は前もって想定され、仕様があり、システムを動かすのに必要なハードウェア・ソフトウェアの組み合わせや導入手順も用意されています。この考える部分がまさに「デザイン」で、「誰かに決めてもらいたい」のにOSSを使うと失敗しやすくなります。本来はOSSの導入を支援する業者と組むのが良いのですが、今回は自力で行いました。

4. midPoint導入までの道筋

System11では利用者原簿管理システムとしてmidPointを導入することになりましたが、準備も含めるとかなりの時間をかけています。midPointというソフトウェアの存在を知ってからSystem11での実運用に至るまでに、私の中では実に4年以上の時間が過ぎました。OSSを自力で実運用の水準まで持って行こうとするとどういう感じになるか書いてみたいと思います。

4.1 情報収集期間（2018）

System10への切替を直前に控えた2018年のある日、統合認証基盤で利用しているソフトウェア（Shibboleth, Grouper）の最新情報を見ようとInCommon Trusted Access PlatformのWebサイト（https://incommon.org/trusted-access/）を眺めているとmidPointというソフトウェアが取り上げられているのに気がつきました。

早速midPointの解説書［8］を読みあさり、このソフトウェアがあれば利用者原簿管理システムがどうやら作れそうだということが分かりました。試しに少し使ってみると、EU圏で開発されているので英語の操作画面はもちろん整っているのですが日本語への翻訳が不十分でした。そこでmidPointの翻訳プロジェクト（https://explore.transifex.com/evolveum/midpoint/）に参加し、少しですが日本語翻訳を行っていました。この時に精力的に日本語翻訳を行っているグループに遭遇し、その翻訳の質と量からどこかの企業が組織的に活動に取り組んでいることが想像されました。日本国内でmidPointを使っているという具体的な話はほとんど見つからなかったのですが、「どうやらこのソフトウェアは本物らしい」という感触を掴みます。

4.2 技術検証期間（2021 ～ 2022.7）

2019年からは足踏み状態だったのですが、2021年に入り次期システム（System11）のための基礎検討としてmidPointの情報収集を再開しました。midPointの仕組みや主要な機能については開発元の書籍に書かれており全体像は掴めたのですが、実利用するための具体的な設定をどのように行うかはよく分からない状態でした。

通常、利用者原簿管理システムのように複雑な業務システムを導入する場合は導入支援を行う業者なり専門家が間に入るので、システム導入の段取りや設定情報はインターネット上の公開資料としてはなかなか出てきません。特に利用ライセンスが無料のOSSの場合はそこが飯の種になるので仕方の無い話ではあります。

System11の利用者原簿管理システムが何になるかは入札をしてみるまで決まりませんが、midPointと連携することも念頭に置きながらSystem11の仕様書を作成しました。2022年1月の入札の結果、System11の導入業者は新規の業者となり、これまでの業者が提供していた利用者原簿管理システムが廃止となることが確定します。また、System11の利用者原簿管理システムは本学側で構築・運用する範囲となり、midPointを用いた完全内製システムとして利用者原簿管理システムを構築することが確定します。System11の認証基盤（LDAP, ActiveDirectory）をmidPointと連携させるための設定も本学側の担当です。

開発元の Wiki（https://docs.evolveum.com/）に書かれている技術情報を読み漁り、midPoint のバージョン 4.3 を元に本学の利用者原簿管理システムとして使うための技術検証を進めていきました。OSS の場合は「動く」といっても「どのバージョンで」「どの機能の組み合わせで」動くのかは実際にやってみるまで分かりません。

ソフトウェアの出荷を見合わせなければならないような致命的な不具合のことを show stopper（ショーストッパー）と言いますが、技術検証の過程でこの show stopper に遭遇してしまいました。System10 の利用者の情報を midPoint に登録できるか検証していたところ、一部の利用者の氏名を登録しようとするとエラーになり登録できないことが分かりました。これは利用者原簿管理システムとしては致命的です。

「隼」という文字を処理するところでエラーが出たのですが、この手の CJK（Chinese-Japan-Korea）文字の処理に起因するエラーは EU 圏ではそもそも発生しません。漢字文化圏でしか起きない問題なので、案の定、インターネット上に公開されている情報にも類似の不具合は報告されていませんでした。エラーが出た文字の文字コード（UTF-16BE 表現だと D8 67 DD 4B）を調べると「サロゲートペア」として表現されるケースに該当し、midPoint の実装ではサロゲートペアを正しく処理できていませんでした。

OSS の良いところは原因が分かれば自分で修正できるところです。サロゲートペアを正しく処理するようにソースコードを修正し、無事に動くようになりました（midPoint を導入している国内の他の組織がこの問題にどのように対処しているかは気になるところです）。

4.3　実運用開始（2022.8 ～）

導入業者が初期設定をした System11 の Linux サーバに本番環境の midPoint を導入し、いよいよ実運用を開始します。技術検証環境に構築した midPoint を本番環境に移植する必要があるのですが、インフラ構築自動化ツールの ansible とコンテナ仮想化技術（podman）を駆使することで作業期間を大幅に短縮します。

さてテスト用アカウントを midPoint に登録して実際に System11 の Windows/Linux 端末を使おうとするとうまくいきません。業者の作業に何か間違いがあるのか、本学側の作業に間違いがあるのか、端末自体が新しくなっているうえに利用者原簿管理システムも認証基盤も新しくなっているので、ソフトウェア自体の不具合の可能性も捨てきれません。9 月下旬の後学期開始に間に合うよう連日の確認作業が続きます。

一般ユーザの目からは後学期の開始時点で System11 への切替が終わったように見えたと思いますが、実はこの時点では利用者原簿管理システムの midPoint への切替は完了していませんでした。アカウント発行と利用者ポータルの部分については System10 の利用者原簿管理システムを継続利用し、System10 の利用者原簿を midPoint に中継するという方式で System11 の認証基盤を動かしていました。

新システムが技術的には動作していても、それを人の方が受け入れるのには時間がかかります。情報科学センターが提供するサービスの使い方については年度初めに習うようになっていますので、夏休み明けに突然利用者ポータルの使い方が大きく変わると一般ユーザが混乱することが予想されました。アカウント発行についても同様で、年度途中に新しい仕組みに切り替えるのは現場の不安が大きいということで新システムへの切替は見送りになりました。

System10 の利用者原簿管理システムを切り離し、利用者ポータル・アカウント発行部分についても System11 に完全に切り替え終わったのは 2023 年の 3 月のことです。

5.　midPoint の使い方

midPoint にはユーザが自分自身の情報を閲覧・更新できる「利用者ポータル」の機能が用意されています。ここでは一般利用者の目から見た midPoint の使い方について紹介したいと思います。

5.1　ダッシュボード画面

midPoint にログインすると最初に表示されるのがこのダッシュボード画面です（図 1）。この画面からシステムに登録されている自分の

情報を確認したり、パスワード変更や利用サービス指定を行うことが出来ます。

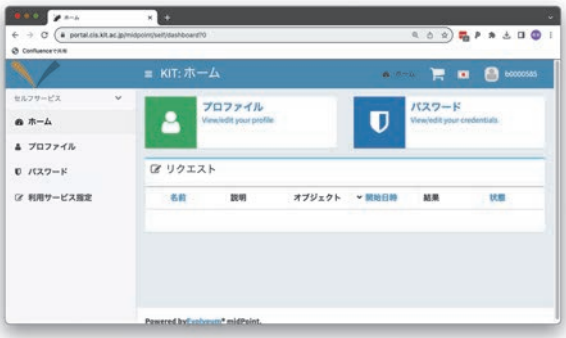

図 1 midPoint のダッシュボード画面

また、画面上部にある言語セレクタで表示言語を切り替えることも出来ます（図 2）。

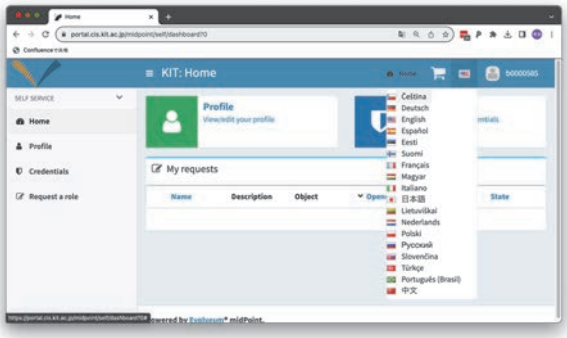

図 2　表示言語を英語にした状態の画面

英語の画面とよく見比べると分かるのですが、英語の画面で「Credentials」「Request a role」となっている部分が日本語の画面では「パスワード」「利用サービス指定」となっています。元々の日本語訳では「クレデンシャル」「ロール要求」となっていたのですが、本学での利用に合わせてカスタマイズしたものです。

5.2　プロファイル画面

プロファイル画面ではシステムに登録されている自分の情報を閲覧することが出来ます（図 3）。System10 ではシステムに登録されている自分の詳細情報を閲覧する仕組みがなかったのですが、midPoint のプロファイル画面では詳細な情報を表示することが出来ます。System11 では GDPR の考え方を取り入れ、情報セキュリティ上問題になる情報を除き、自分自身に関する情報はできるだけ閲覧できるように設定しました。

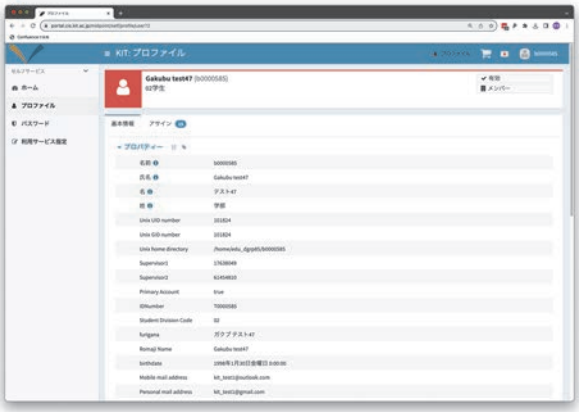

図 3　プロファイル画面で登録情報を閲覧

プロファイル画面では単に情報を閲覧するだけでなく、編集権限を持つ属性についてはユーザ自身で更新することができます（図 4）。この仕組みを使い、通常のログインに使用するパスワードだけでなく、SSH 認証に使う公開鍵やサービス固有のパスワードもこの画面から設定できるようにしています（本稿執筆時点では試行段階）。

図 4　追加認証情報入力用のフォーム

System10 でも利用者原簿上は SSH 公開鍵やクライアント証明書を登録するための項目を用意していたのですが、利用者自身で設定するための操作画面が無いために利用までの敷居が高く、一部ユーザの利用にとどまっていました。midPoint では利用者属性の項目に応じた入力フォームが自動生成されるので、ユーザ自身でこういった追加認証用の情報を設定することも可能になりました。

5.3　Moodle 確認テスト連携

情報科学センターが提供する一部のサービスについては Moodle に用意されている「情報リテラシーガイダンス」コースの確認テストに合

格してからでないと利用できないようにしています。これはSystem8を導入した際に、確認テストの合否状況をMoodleのデータベースから利用者原簿管理システムに取り込む処理を本学独自の機能として実装してもらうことで実現していました［6］。今回、同様の仕組みをmidPointの基本機能とMoodleのバッジ発行機能を組み合わせることで実現しました。

利用したいサービスは「利用サービス指定」の画面からオンラインショッピングストアの要領で指定することが出来ます。ただし、CISアカウントが発行された初期状態では、一部のサービスだけが表示されています（図5）。

図5　初期状態では一部サービスのみ表示

残りのサービスを使うには、Moodle上に用意された「情報リテラシーガイダンス」コース（図6）の内容を理解し、確認テストに合格する必要があります（図7）。

確認テストに合格するとMoodle上で「情報リテラシーガイダンス合格証」（図8）が発行され、この合格情報がmidPointに取り込まれると残りのサービスが利用サービス指定画面で表示されるようになります（図9）。System11

図6 「情報リテラシーガイダンス」コース

ではこの仕組みをMoodleとmidPointの標準機能だけを用いて実現しました。確認テストに合格してからmidPointに反映されるまで数分程度待つ必要がありますが、2023年度前期を通じて特に大きな不具合も無く安定して動作しています。

図7　確認テスト合格画面

図8　情報リテラシーガイダンス合格証

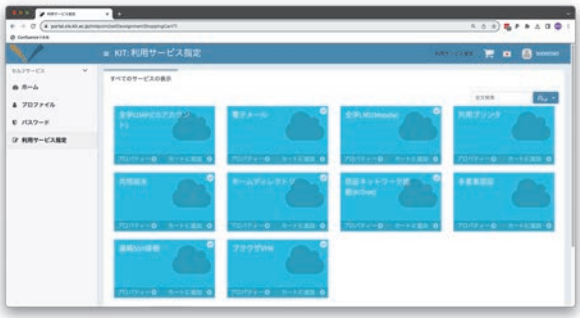

図9　利用可能サービス（確認テスト合格後）

6. 終わりに

本稿ではSystem11の利用者原簿管理システムとして採用したmidPointについて、導入の背景と使い方を紹介しました。今回のシステム更新ではOSSと標準技術を組み合わせることで利用者原簿管理システムを内製することに成功しましたが、内製することは手段であって目的ではありません。

効果的な情報システムを実現するには「与え

られた制約の中で何をどう組み合わせるか」というデザインが重要であり、技術的な解決手段だけでなく、自分たちが何を必要としているかを深く理解している必要があります。利用者原簿管理システムとしてはIDaaS（Identity as a Service）と呼ばれる商用のクラウドサービスも登場してきており、将来的には今回のシステム更新で得られた知見を元に外部サービスを取り入れることも考えられます。

7. 参考文献

[1] 永井 孝幸，山岡 裕美，桝田 秀夫：”京都工芸繊維大学における利用者原簿管理基盤の強化と連携サービスの構築”，第25回CLE研究発表会 情報処理学会研究報告 Vol.2018-CLE-25 No.9（2018-06）

[2] 桝田 秀夫：”情報基盤計算機システムSystem10について”，京都工芸繊維大学情報科学センター広報，No.37，pp.3-6，2019

[3] Hideo Masuda, Kazuyoshi Murata, Yu Shibuya, Koichiro Wakasugi, and Yasuaki Kuroe: “KIT’s campus computer system by virtual machine technology and integrated identity service”, In Proceedings of the 38th annual ACM SIGUCCS fall conference, pp. 251–256, 2010.

[4] 独立行政法人等の保有する個人情報の保護に関する法律，https://elaws.e-gov.go.jp/document?lawid=415AC0000000059_20220401_503AC0000000037

[5] 政府機関の情報セキュリティ対策のための統一基準，内閣サイバーセキュリティセンター，https://www.nisc.go.jp/policy/group/general/kijun.html

[6] Hideo Masuda, Kazuyoshi Murata, Yuki Shirakawa, Yu Shibuya, and Yasuaki Kuroe: “Moodle integration of an automated account enabling system and a user status collection system”, In Proceedings of the 39th annual ACM SIGUCCS conference on User services, pp. 207–210, 2011

[7] 桝田秀夫，村田和義，渋谷雄：“低コストな高可用性と学務システム連携を考慮したMoodleシステムの構築”，情報処理学会研究報告，2008-IOT-1, pp.65-69（2008）

[8] Practical Identity Management with MidPoint https://docs.evolveum.com/book/

[9] From OpenIDM to Success https://evolveum.com/from-openidm-to-success/