Office365 を利用した統合認証プラットフォーム構築とその運用

Constructing and operation of an integrated authentication platform using Office 365

鈴木　歩*，野口　俊樹**，水野　信也*
Susumu SUZUKI, Toshiki NOGUCHI and Shinya MIZUNO

Abstract : Currently, academic institutions such as universities are becoming increasingly aware of the use of in-campus data, and a wide range of initiatives such as IR (Institutional Research) has started. However, there are many systems used by students and staff within the university, and these data often have independent structures. Also, there are many cases where ID and password for each system are used. Integration of data is indispensable when using in-campus data, but since authentication is performed on a system-by-system basis, it is difficult to integrate data. Authentication is linked to all elements and is an important role. Although it is required to strengthen the authentication infrastructure, introduction does not proceed in many cases due to cost and the current situation covering operation. In this research, we will build an authentication platform required for future universities with the scheme of Office 365. Office 365 is currently widely deployed in educational institutions such as universities and it is thought that it will be a wide platform in educational institutions. By using this Office 365, many universities can use the same authentication platform, which can improve security and reduce costs. We expect that the authentication model in this research will be an indicator of the certification base in the same scale educational institution.

1．はじめに

現在，大学等の学術機関では学内データの利活用に対する意識が強くなり，IR(Institutional Research)[1][2]のように幅広い取り組みが始まっている．しかしながら学内には学生，教職員が利用するシステムが多数存在し，それらのデータは独立した構造となっている場合が多い．またそれぞれのシステム毎の ID 及びパスワードが使用されている場合も多く存在する．学内データを利用する場合にデータの統合が不可欠だが，認証をシステム毎に実施しているため，データの統合が困難である．図 1 は大学における情報基盤の環境として必要とされる要素である．その中でも認証はすべての要素と結びつき，重要な役割となっている．認証基盤を強固にすることが求められているが，費用の面や運用面で足らない機能をカバーしている現状から導入が進まない場合も多い．

本研究では今後の大学で必要とされる認証基盤を Office365 のスキーム[3]で構築を行う．Office365 は現在大学などの多くの教育機関が導入している．今後も拡大が期待され，教育機関では幅広いプラットフォームになると考えられる．この Office365 を利用することで多くの大学が同じ認証プラットフォームを利用でき，セキュリティを向上させると共にコスト削減も期待出来る．本研究での認証プラットフォームは同規模の教育機関での認証基盤の指標となると期待する．

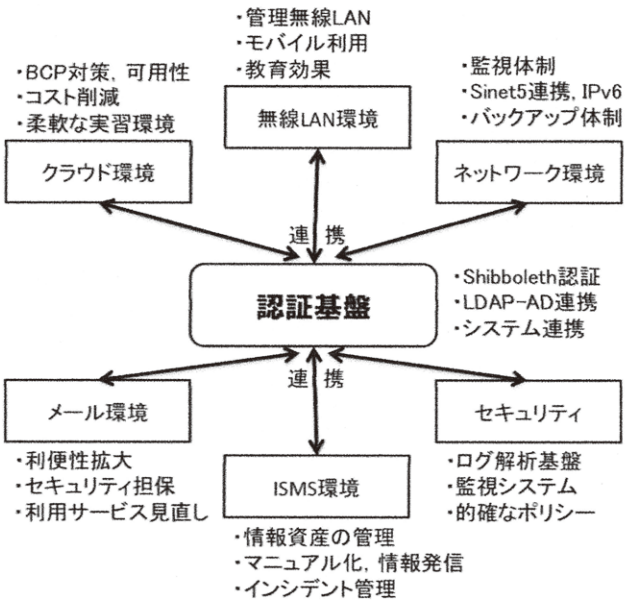

図 1 大学における情報基盤環境

Office365 の ID 体系は Azure Active Directory[4](以下 Azure AD)で管理されている．Azure AD の認証方式に対応しているサービスはまだ限られており，オンプレミスの AD との連携が現状必要とされている．今回の認証プラットフォームはそのような現状を踏まえ構築を実施している．

2017 年 5 月 8 日受理
*　総合情報学部　コンピュータシステム学科
**　株式会社 CAI メディア

2．Office365 を利用した認証プラットフォーム

2.1 Office365 の利用

Office365 は多くの教育機関で活用されている．また Office 製品も幅広く利用されており，教育機関にとっては必須のソフトウェアである．特に大学では研究室単位で Office 製品のライセンス購入がされており，ライセンス管理は担当教員に任せられている場合が多い．また古い Office 製品を使い続けているとセキュリティ面で心配がある．マイクロソフトから提供されている教育機関向け総合契約ＯＶＳ－ＥＳ(Open Value Subscription-Education Solutions)[5]は下記のメリットがあり，教育機関での運用に対して有効であると考えられる．

1. ソフトウェア管理が簡単（コンプライアンス対策）
   人数カウント方式のため，ライセンスの管理が容易
   最小限のコストでのアプリケーション不正利用の防止．管理には Azure AD を利用
2. 教育機関における情報基盤の強化
   全教職員で契約するとトータルコストも大幅削減
3. 常に最新バージョンを利用可能
   必要に応じて旧バージョンへのダウングレードも可能
4. 有事係争の場合 Office 365 は日本国内の法律が適用
   契約の準拠法が日本国内，管轄裁判所も国内
   Google Apps は米国の法律が適用
5. 長期的な利用
   Office 365 の卒業生用 Exchange Online の無償ライセンス．OneDrive(1TB)の利用，メールストレージ(50GB)

2.2 学校法人静岡理工科大学での取り組み

学校法人静岡理工科大学は大学に加え専門学校 6 校，日本語学校 2 校，中学・高校がそれぞれ 2 校となる学校法人である．平成 28 年度に静岡理工科大学が OVS-ES の利用を開始した．平成 29 年度には学校法人全体で OVS-ES の契約をする予定である．専門学校では利用したい Office 製品の種類が異なることから，ベース契約は学校法人全体で締結し，各校で必要なオプション契約を結ぶことにしている．これにより契約全体の明確化，及びソフトウェア管理の心配を無くし，さらに今まで各校でそれぞれ決めていたメールアドレスを Office365 で統一する．教職員は学校間での異動があり，その度にメールアドレスを変更していたが，これにより異動に関係なく常に同じメールアドレスを利用可能となった．静岡理工科大学で平成 28 年度にダウンロードされた Office の内訳は表 1 のようになっている．平成 28 年度の Office インストール本数は 334 本となっており，Office 製品の標準的な価格を，972 円（税込）ユーザー/月×12 = 11,664 円とすると，今回のインストール本数では 3,895,776 円となり，平成 28 年度に OVS-ES 契約で支払った費用が約 163 万円(税込)であることから，十分なコストメリットが出たことがわかる．また学校法人全体で利用する Office365 の ID を SIST-ID と名付け，この SIST-ID を今後の統合認証で利用する ID としていく．

表 1 平成 28 年度 Office インストール内訳

Office インストール数	334	
OS 別インストール数		
Windows	316	95%
Mac	18	5%
学科別インストール数		
機械工学科	67	20%
電気電子工学科	56	17%
物質生命科学科	6	2%
コンピュータシステム学科	68	20%
人間情報デザイン学科	38	11%
情報センター	81	24%
その他	18	5%
Office 種類別		
Office2016 64bit 版 (Windows)	242	72%
Office2016 32bit 版 (Windows)	58	17%
Office2013 32bit/64bit (Windows)	16	5%
Office2016 (Mac)	18	5%

2.3 統合認証環境の現状

近年，セキュリティインシデントが多発し多くのトラブルが報告されている[6][7][8]．これらの多くは使用しているサービスで同じパスワードを利用し，一つのパスワードが漏洩すると他のサービスまで不正アクセスされてしまった．またパスワードは変更すべきでないとの報告もある[9]．標的型メールのトラブルも非常に増えている[10]．このような脅威から組織を守るためには，強固な統合認証基盤が欠かせない．またクラウドコンピューティング環境が広く使われるようになった現在，多要素認証も普及を始めている．このような環境を踏まえ，Office365 を利用する形態では図 2 のように Azure AD とオンプレミスの AD を連携し，学内の認証を連携するようなプラットフォームが基盤となると考える．

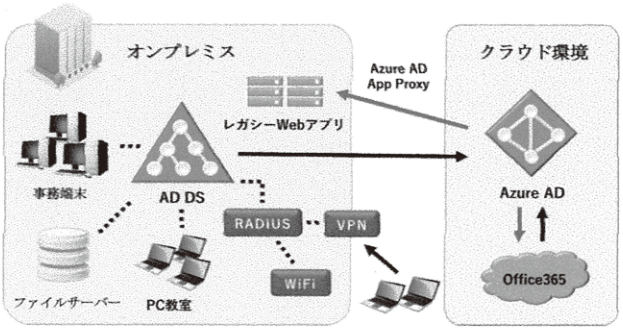

図 2 Azure AD とオンプレミス AD との連携

3. 統合認証プラットフォームとその応用

3.1 統合認証プラットフォームの概要

本研究で構築する統合認証プラットフォームは図 3 のようになる. Office365 において ID 管理で利用する Azure Active Directory と学内に設置する Active Directory のパスワードを同期する. これにはパスワード変更システムから Azure Active Directory のパスワード変更をした後, 学内の Active Directory のパスワード変更を行う. 利用者はパスワード変更についてはこのシステムを利用する.

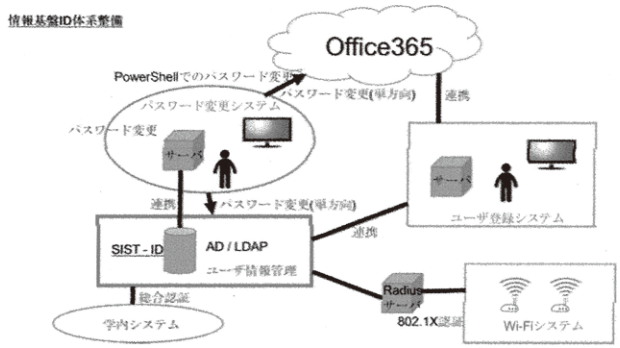

図 3 SIST-ID を利用した統合認証

利用者の利便性を考慮し利用者は図 4 のように 2 段階の入力確認をとる. まず現在の ID とパスワードを入力し認証が得られた後, 新しいパスワードを入力して変更処理がなされる.

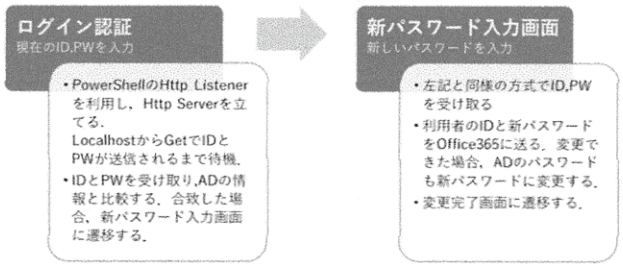

図 4 利用者のパスワード変更の流れ

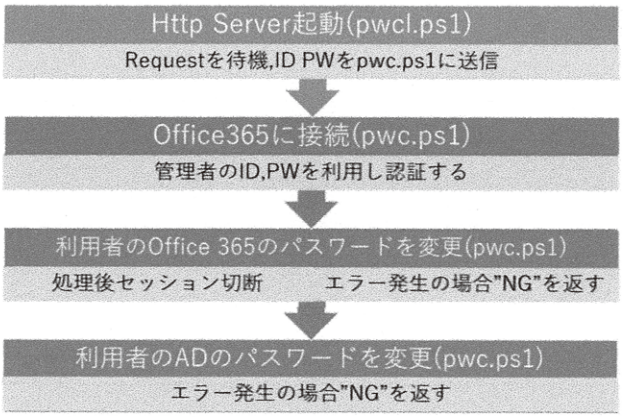

図 5 パスワード変更システムの基本フロー

サーバ環境は WindowsServer2012R2 上に IIS, Active Directory サーバを学内に構築する. また Office365 との通信は PowerShell を介して行う. Office365 に対してパスワード変更を行うには権限付きのアカウントが必要となる. このパスワード変更システムの基本フローは図 5 のようになる. PowerShellScript は 2 ファイルで構成され, pwcl.ps1 はリクエスト受付を, pwc.ps1 は Office365 の認証及びパスワード変更を行っている.

また Microsoft Office 365 PowerShell[11]で利用した関数は表 2 のようになっている.

表 2 Office365 PowerShell 利用関数一覧

関数名	内容
System.Management.Automation.PSCredential	資格情報の作成(管理者の ID, PW を入力)
New-PSSession	セッションを作成 (引数:接続先, 資格情報, 認証方式)
Import-PSSession	コマンドをインポートする
Connect-MsolService	Office365 に接続(引数:資格情報)
Set-MsolUserPassword	パスワードを変更(引数:利用者 ID, 新 PW)
Remove-PSSession	セッションを切断
Set-ADAccountPassword	AD のパスワードを変更(引数:利用者 ID, 新 PW)
Write-Output	コマンドラインに出力

3.2 統合認証プラットフォームの応用

本研究で提案した統合認証プラットフォームを利用することでデータの統合が可能となる. 例えば学内に設置した 11 個の無線 LAN アクセスポイントのログに対して, データ集約が可能となる. 表 3 はある認証者の WiFi ログを利用して移動先を推定したものである. このログから朝登校した時, 学生ホールに 60 分ほど滞在し, その後ラウンジに少し立ち寄った後, 食堂に移動している. その後夕方再び食堂に来た後, 研究室に向かっている. RSSI はアクセスポイントが得られた電波強度平均である. 数値が高い方がアクセスポイントの近くにいたと推定される. また表 4 はログからアクセスポイント間の推移確率を求めたものである.

表 3 WiFi ログから移動先の推定

TO	FROM	滞在時間(分)	RSSI	日時
学生ホール	NULL	60.8	31	2016/12/15 9:15
Lounge	学生ホール	2.2	25	2016/12/15 11:34
食堂東	Lounge	15.9	34	2016/12/15 12:22
研究室	食堂東	23.4	31	2016/12/15 19:42

表 4 各アクセスポイント間の推移確率

From＼To	教育棟101	教育棟505	English Room	図書館 GroupWork	図書館北	図書館西	Lounge	研究室	食堂東	食堂西	学生ホール
教育棟101	0	0	0	0	0.25	0.25	0	0	0	0	0.5
教育棟505	0	0	0	0.11	0	0.33	0.11	0	0	0.33	0.11
English Room	0	0	0	0.4	0	0	0	0.2	0	0.2	0.2
図書館 GroupWork	0.04	0.18	0.14	0	0.07	0.04	0.04	0.07	0.11	0.22	0.07
図書館北	0	0.33	0.17	0	0	0.33	0	0	0	0.17	0
図書館西	0	0.29	0.06	0.12	0.12	0	0.12	0	0.23	0	0.06
Lounge	0	0.2	0	0	0.2	0	0	0	0.2	0.4	0
研究室	0	0	0.12	0	0	0.12	0	0	0.37	0.25	0.12
食堂東	0	0.01	0.07	0.10	0	0	0.03	0.06	0	0.64	0.07
食堂西	0	0.02	0.08	0.04	0	0.10	0.04	0.04	0.59	0	0.06
学生ホール	0.17	0.08	0.08	0.25	0.08	0	0	0	0.25	0.08	0

4. さいごに

本研究では今後教育機関で幅広く利用されることが期待される Office365 の ID 体系を利用し，学内のシステムと連携し統合認証を行うことが可能なプラットフォームを提案した．本統合認証プラットフォームを利用することで，学内で統合認証が可能となり，今後必要となるセキュリティや IR などでデータの統合を図り，活用することが可能となる．

謝辞

本研究は静岡理工科大学平成 28 年度　研究プロジェクト (A) 研究代表者：水野信也「統一管理下 WiFi ネットワークの実現と統合認証環境の構築および教育 IR との連携」の研究成果の一部をまとめたものである．

参考文献

1） 大桑良彰. "宮崎医科大学における入試の追跡調査-入試成績と学内成績の関係." 医学教育 31.3 (2000): 181-193.

2） 姉川恭子. "大学の学習・生活環境と退学率の要因分析." 経済論究 149 (2014): 1-16.

3） 教育 ICT - 教育機関向けソリューション，https://www.microsoft.com/ja-jp/education/default.aspx，(2017/03)

4） Azure Active Directory，https://azure.microsoft.com/ja-jp/services/active-directory/，(2017/03)

5） 教育機関向けライセンスプログラム，https://www.microsoft.com/ja-jp/education/license/ovses/default.aspx，(2017/03)

6） 高校生１万人の情報流出，東京新聞，http://www.tokyo-np.co.jp/article/national/list/201606/CK2016062702000241.html (2016/6/27)

7） ＪＴＢ個人情報７９３万件流出か？，YOMIURI ONLINE，http://www.yomiuri.co.jp/science/goshinjyutsu/20160615-OYT8T50004.html (2016/6/15)

8） LinkedIn の 2012 年の情報流出，ITmedia エンタープライズ，http://www.itmedia.co.jp/enterprise/articles/1605/19/news067.html (2016/5/19)

9） Paul A. Grassi, et al., Digital Identity Guidelines Authentication and Lifecycle Management, DRAFT NIST Special Publication 800-63B.

１０） サイバー情報共有イニシアティブ（J-CSIP） 運用状況，J-CSIP, (2016/4/28).

１１） Microsoft Office 365 PowerShell ガイド，https://www.microsoft.com/ja-jp/download/details.aspx?id=42673 (2017/03)