大阪大学における全学認証基盤への多要素認証システムの導入と課題

村尾　靖子 [1], 原口　直大 [1], 山本　浩二 [1], 猪俣　敦夫 [2]

1)　大阪大学 情報推進部
2)　大阪大学 サイバーメディアセンター
auth-admin @ml.office.osaka-u.ac.jp

Implementation and Issues of Multi-Factor Authentication to Campus-wide Authentication Platform in Osaka University

Yasuko Murao [1], Naohiro Haraguchi [1], Kouji Yamamoto [1], Atsuo Inomata [2]

1)　Department of Information and Communications Technology Service, Osaka University
2)　Cybermedia Center, Osaka University

概要

大阪大学では学内の様々な情報システムに，シングルサインオンによる認証連携を可能とする全学 IT 認証基盤システムを運用している．本システムで発行する ID とパスワードでの認証により学内に複数ある情報システムを利用できるが，一方で ID とパスワードが漏洩すれば不正アクセス被害を受ける可能性が生じる．不正アクセスのリスク低減を図るため，2020 年 2 月から多要素認証機能の試行を開始し，学内の全利用者への適用を進めている．本稿では本システムの利用状況について紹介し，多要素認証の導入までの経緯と導入後の動向について報告する．

1　はじめに

全学 IT 認証基盤システム（以下,「本システム」という.）は学内で運用されている様々な情報システムが統合的かつ安全に機能するためのシステムで，2006 年 10 月に運用を開始した[1]．本システムでは，本学の教職員や学生が学内の情報システムにシングルサインオン（Single Sign-on: SSO）認証にてログインをする際に使用するアカウントである大阪大学個人 ID（以下,「個人 ID」という.）の発行や，メールや無線 LAN サービスの認証に個人 ID を用いるために学内の認証連携サーバとの情報連携サービスを提供している．

2010 年のシステム更改では，システムリソース不足の改善や新たなデータ連携機能の実装による利用者の利便性の向上を図った．また，本システムとは異なるアカウントを認証に用いていた事務基幹系システムとの SSO 認証を新たに開始し，事務職員が業務を行う際に利用する複数の情報システムを 1 つの個人 ID とパスワードで利用可能となる環境を構築した．

システム更改により重要なデータへアカウントとパスワードのみでアクセス可能となり利便性が向上した反面，アカウントとパスワードの漏洩による不正アクセスの危険性を高める弊害があった．昨今，特に情報セキュリティの重要性が問われていることから，本学として不正アクセスのリスク低減策を講ずる必要があった[2].

本稿では，本システムでの個人 ID の利用状況について紹介し，情報セキュリティ対策と本人確認の方法として有効とされる多要素認証の導入までの経緯および導入後の動向について報告する．

2　個人 ID について

2.1 個人 ID の発行対象者と情報源

本学は 11 学部，16 研究科を擁する総合大学であり，学生 23,333 名，教職員（非常勤職員等を含む）10,616 名の計 33,949 名が本学の構成員となる[3]．本システムでは本学の構成員全てに対して個人 ID を発行している．

個人 ID に紐づく利用者の情報は，学生については学生の情報（学生の学籍情報，履修情報，成績情報など）を管理する学務情報システムから，教職員については教職員の個人情報や人事情報を取り扱う人事給与システムと連携し登録される．また，学内で教育・研究活動を行う招へい教員や共同研究員，事務業務に携わる派遣職員など，本学に直接雇用されていない者に対しても，部局の事

務部からの申請を経て個人 ID を発行している．

本システムにある情報は，学務情報システム，人事給与システム，および部局事務部からの申請データを情報源として登録している．個人 ID の発行対象者の分類と情報源について表 1 に示す．

表 1 個人 ID の発行対象者の分類および情報源

分類	情報源
学生（学部学生，大学院生，研究生等）	学務情報システム
教職員（教員，研究員，職員）	人事給与システム
個人 ID 発行申請による利用者	各部局からの申請データ

2.2 個人 ID の保有する属性情報

本システムには個人 ID に紐づいた利用者情報（以下「属性情報」という．）が保存されている．主な属性情報として，氏名，生年月日，メールアドレス，性別，所属，職名，身分などがある．

属性情報および在籍者情報について最新の状態を保つため，情報源となる学務情報システムから月 1 回，人事給与システムから月 2 回の頻度で在籍者のデータを受け取り，個人 ID の登録を担当する職員が確認を実施し，誤りがないものについて登録・更新処理を行っている．

2.3 個人 ID を使用した SSO 認証により利用可能となる情報システム

本システムでは 54 の情報システムに対して SSO の認証連携を行っている（2020 年 9 月現在）．認証連携を行っている代表的な情報システムについて，表 2 に示す．

表 2 認証連携中の代表的な情報システム

情報システム名
マイハンダイ
学務情報システム
大阪大学 CLE
勤務管理システム
出張旅費システム
財務会計システム
就職支援システム
包括契約ソフトウェア提供システム
図書館 Web サービス

表 2 の情報システムは，本学の情報ポータルや事務関連業務で使用するシステムである．

アクセス可能な利用者の限定や，属性情報に応じた権限の設定を行うため，SSO 認証時に情報システムが必要とする属性情報の取得が可能となる認証連携を許可している．

2.4 個人 ID とパスワードの SSO 認証の問題

利用者にとって利便性が向上した反面，個人 ID とパスワードの漏洩による悪意のある第三者からの不正アクセスも容易となる可能性が高まる結果となった．

不正アクセスの可能性を低減するために，英字大文字，英字小文字，数字，記号を組み合わせた難読のパスワードの設定や，情報セキュリティ研修（e-learning）によるパスワード管理の重要性の周知を行ってきた．また，教員本人がシステムに入力する必要がある業務を，秘書に対して入力代行権限を付与することにより，秘書が代行者として入力が可能となる入力代行設定機能を実装し，個人 ID とパスワードの委譲等を防止する対策を行った．

SSO 認証を適用した本学の情報システムは，学生の成績情報や個人情報等の機密性の高い情報を保有するシステムがある一方，施設予約情報等の利用者間で情報共有を行うためのシステムがあるなど，システム内に保有する情報の機密性は多様な状況にある．全ての情報システムが同じ SSO 認証で利用されているため，ID とパスワードの管理方法やリスクに対する意識は利用者により様々である．

アカウントとパスワードの使い回しをしている本学の管理下にない外部サービス等での情報漏洩や，フィッシングサイトによる情報詐取を起因とする不正アクセスへの対策は現在までの周知では不十分であり，不正アクセスを試みられた際に防ぐ仕組みを検討する必要があった．また，本学では 2017 年に発生した学内の情報システムへの不正アクセス事案を受け，より強固な情報セキュリティ対策が求められていた．

3 多要素認証の導入

本システムが抱える個人 ID とパスワード漏洩による不正アクセスの脅威への対策のため，個人 ID とパスワードによる 1 種類の認証から，認証手段として分類される 3 つの要素（知識情報，所有物，生体情報）のうち，2 つの要素を用いた多要素認証を導入することとした．

3.1 導入についての検討

2018 年 4 月から多要素認証の導入について検討を開始した．一方で，本システムから個人 ID とパスワード情報を連携している事務職員用のメールは 2018 年 9 月から，学生用のメールは 2019 年 3 月から多要素認証を導入した．

メールへの多要素認証導入時の周知において，多要素認証の有効性についての説明を行っていたが，本システムへの導入にあたっては，適用される情報システム数と利用者の範囲が拡大すること，今までの個人 ID とパスワードによる認証と異なる設定や入力が必要となることから，利用者が混乱なく環境に適用しやすい多要素認証方式について検討を重ねた．

多要素認証方式の候補として，スマートフォンアプリを利用したワンタイムパスワード（One Time Password: OTP），PIN コード，秘密の質問と答え，登録メールアドレスへの OTP 送信，およびクライアント証明書の利用等が挙げられた．

候補とした多要素認証方式は，以下の条件を考慮し選定した．

- 多くの利用者（37,000 人以上）の利用が想定された運用が可能であること
- 単一要素ではなく複数要素とすること
- 現在認証連携している全ての情報システムで利用可能な多要素認証方式であること
- 固有業務により複数の職員が PC を共有する環境でも支障が出ないこと

検討の結果，多くの利用者が日常的に使用し，操作に慣れているスマートフォンでアプリケーションを利用する方法に決定した．

利用者の利便性を著しく損なわないようにすること，また，共有の PC は学内での利用が主となることから，学内のネットワークからのアクセスは多要素認証を適用せず，従来の SSO のみの認証とすることとした．

しかしながら，本方式の採用にあたり個人が所有するスマートフォンを利用することとなるため，大学の業務に個人所有物の使用を強制することに対する反発や，スマートフォンを所有しない利用者からの苦情等の懸念があった．利用者からの理解を得るため，多要素認証の導入を，大学全体の情報セキュリティ対策水準の底上げとする方針として定め，多要素認証は本人確認のために有効な手段である旨の説明を十分に行っていくこととした．また，利用者向けマニュアルと FAQ ページを用意し，必要な情報を得るための環境を整備した．そのほか，スマートフォンやタブレット端末以外を用いて認証をするための手順も併せて整備し，多様な利用者環境へ対応した．

多要素認証の適用は利用者の混乱を避けるため，適用までに十分な期間を設け周知を行い，全ての利用者へ一斉に適用することとした．

加えて，スマートフォンや OTP の操作に慣れていない利用者がいることも考慮し，多要素認証の適用から 90 日間は OTP を入力することなく情報システムにログインできる事前登録期間を設け，利用者による多要素認証の登録が完了した後から OTP を必須とする仕組みとした．

なお，多要素認証の登録をせず情報システムにログインを行った場合，情報システムの画面に遷移する前に多要素認証の事前登録期間と説明の画面を表示し，登録を促す仕組みとしている．

3.2 多要素認証の画面イメージ

多要素認証を適用すると，利用者は多要素認証の初期登録画面に遷移することができる．登録は事前にスマートフォンへの認証アプリのインストールを行い，初期登録画面に表示される秘密鍵の QR コードを認証アプリで読み取って行う．

多要素認証の登録を完了すると，次回の SSO のログインから個人 ID とパスワードの入力の次に認証コードを入力する画面が表示される．

画面のイメージは図 1 のとおりである．

3.3 多要素認証導入のスケジュール

多要素認証機能の開発は 2019 年度に行い，2020 年 2 月から試行運用を始め，順次適用範囲を拡大していく方針とした．具体的なスケジュールは表 3 のとおりである．

試行運用については本学における情報の事務部門である情報推進部の全職員と，全学の情報サービスの整備や推進を担うサイバーメディアセンターの教職員に協力を依頼し，多要素認証の利用に関する意見を集約し明らかになった課題を基に改修を行った．

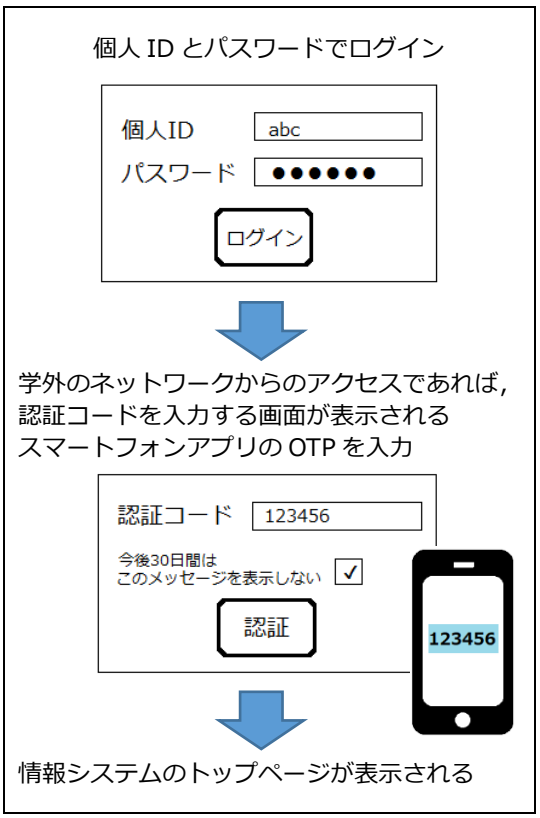

図 1 多要素認証の画面イメージ

表 3 多要素認証導入スケジュール

年月	適用対象
2020 年 2 月	全学 IT 認証基盤システム担当の教職員に適用（試行運用開始）
2020 年 4 月	情報推進部およびサイバーメディアセンターの教職員に適用（試行運用開始）
2020 年 8 月	全教職員に適用
2020 年 11 月	全学生に適用予定

3.4 導入後の状況

全教職員への多要素認証導入後，5 週間後までの登録者数の推移を，教員（教員，研究員等），職員，非常勤講師等（非常勤講師，招へい教員等）に分類して確認すると表 4 から表 6 までの結果が得られた．

表 4 教員における多要素認証登録数の推移

	登録済	未登録	前週からの登録増加数
1 週間後	2363	1975	2363
2 週間後	2648	1690	285
3 週間後	2804	1542	156
4 週間後	2892	1454	88
5 週間後	3159	1250	267

表 5 職員における多要素認証登録数の推移

	登録済	未登録	前週からの登録増加数
1 週間後	2454	3422	2454
2 週間後	2788	3088	334
3 週間後	2968	2917	180
4 週間後	3069	2816	101
5 週間後	3191	2759	122

表 6 非常勤講師等における多要素認証登録数の推移

	登録済	未登録	前週からの登録増加数
1 週間後	569	2508	569
2 週間後	716	2384	147
3 週間後	836	2308	120
4 週間後	928	2220	92
5 週間後	1023	2189	95

多要素認証導入開始から 1 週目が最も登録者数が多く，2 週目以降の登録数は減少傾向にあった．5 週目については，教員，職員，および非常勤講師等の全ての登録者数が前週よりも増加する結果となった．1 週目以降の登録数推移が減少傾向にあることは，事前登録期間は未登録の状態でも情報システムへのログインが可能となるため，登録をせずに利用し続けていることによるものと予想される．一方，5 週目については，翌週から 10 月に入り授業開始となる時期であったことから，情報システムへのアクセスが必要となった利用者が多要素認証登録を必要であると認識し登録を完了させたため，登録数が大きく増加したものと思われる．

未登録の状態で事前登録期間を超過すると，学外のネットワークから情報システムへのログイン

は不可となるため，多要素認証の登録を行っていない利用者には，事前登録期間中に登録を完了させるよう改めて案内や広報の実施が必要である．また，非常勤講師等については未登録数が著しく多いことから，情報の周知方法についても工夫が求められている．

全教職員への多要素認証を適用してから約 1 ヶ月の期間に，利用者からは想定された質問のほか，自身での登録後のログイン時に何を認証コードに入れたらいいかわからない，登録後に認証アプリをアンインストールしてしまった，という問い合わせもあった．今後さらに利用者向けマニュアルを充実させ，多要素認証の案内と周知に努める必要があると考える．

4 おわりに

本稿では，全学 IT 認証基盤システムの利用状況と，多要素認証導入の経緯と導入後の状況について紹介した．本稿を事例の一つとして参考いただき，全国の大学をはじめとする教育機関における多要素認証導入手法や課題，取られた工夫などの情報を交換し，よりセキュアな情報システム環境構築の一助となると幸いである．

謝辞

本稿の執筆にあたり，大阪大学情報セキュリティ本部，情報推進本部，サイバーメディアセンター，情報推進部の皆様にご指導とご助言をいただきましたことに心より感謝申し上げます．

参考文献

[1] 秋山豊和, 他, 大阪大学における全学 IT 認証基盤の構築, Vol.49, No.3,pp.1249-1264, 情報処理学会論文誌, 2008.
[2] 独立行政法人情報処理推進機構「不正ログイン対策特集ページ」（https://www.ipa.go.jp/security/anshin/account_security.html）
[3] 大阪大学プロフィール（https://www.osaka-u.ac.jp/ja/guide/about/profile/profile2020), p. 4-4，2020.