複数種の多要素認証必須化に伴う運用とその支援

尾崎 拓郎 [1)]，松井 聴治 [2)]，佐藤 隆士 [1)]

1) 大阪教育大学 理数情報教育系・情報基盤センター

2) 大阪教育大学 学術部学術情報課情報企画室

{ozaki[1)], kmatsui[2)], sato[1)]}@cc.osaka-kyoiku.ac.jp

Practice and Support for Mandatory Multi-Factor Authentication of Multiple Services

Takuro OZAKI[1)], Kikuji MATSUI[2)], Takashi SATO[1)]

1) Center for Information Communication and Technology, Osaka Kyoiku University

2) Information Planning Office, Osaka Kyoiku University

概要

大阪教育大学では，2021 年 2 月に情報基盤システムのリプレースを実施し，利用者の認証の強化を図った．これまでに本学が提供していたサービスに加えて新たに提供を開始した複数のクラウドサービスに対しても認証強化を図るべく，複数のサービスに対して多要素認証の必須化を利用者に求めるようにした．本稿では，大阪教育大学における複数のサービスそれぞれに対して多要素認証必須化を導入した経緯とその実施・支援体制及びそれらをを実施した結果と課題について報告を行う．

1 はじめに

大阪教育大学（以下，本学と記す）では，2021 年 2 月に情報基盤システムのリプレースを実施し，複数のサービスに対して認証基盤の体制を一新した．

それ以前からも，本学で稼働している複数のサービスに対して利用者情報管理システムから適切に情報を連携し，同一 ID でのサービス利用が可能となるように設計していたものの，シングルサインオンの導入が部分的にしかできておらず，適切な認証連携ができているとは言えない状況であった．

また，高等教育機関を狙うフィッシングメールが急激に増加している背景もあり，本学の資産を守る観点からも多要素認証の導入は急務であった．

そのような背景を踏まえ，本稿では 2021 年 2 月に実施した情報基盤システムのリプレースとそれに関連する多要素認証をサービス利用者に対して必須化にした事例の報告を行う．

2 本学における情報基盤システムリプレース

2.1 本学におけるクラウドサービス利用の兆し

本学では，2017 年 2 月稼働の全学の情報基盤システム運用時からクラウドサービスの活用検討を始めていた．他大学が全学メール等をはじめとするサービスをクラウドサービスに切り替えている中，本学においてもクラウドサービスの活用検討はしたものの，本格的な導入には至らなかった．

一方で 2017 年度の学部新入生より実施を開始したノートパソコン必携や 2020 年度に実施した Office 365（現 Microsoft 365）の Office アプリケーションの包括契約に伴い，クラウドサービス活用の土台が徐々に築き上げられるようになった．もともと，ノートパソコン必携事業を実施するにあたり，クラウドサービスの全面的な活用については視野に含まれておらず，Office アプリケーションやウイルス対策ソフトウェアの展開を利用者にどのように実施していくのかといった課題が挙げられていた [1]．

その課題を受けて，Office アプリケーションのサブスクリプションを学生利用者に全面的に提供するべく，Office 365（現 Microsoft 365）の Office アプリケーションの包括契約を結ぶに至った．

Office 365 を利用者に提供開始した 2020 年 3 月時点では，下記のような状況であった．

- アカウント名（Office 365 上におけるメールアドレス）については，本学のマイクロソフトに関連するサービスであることがわかるように，サブド

メインをマイクロソフトサービス用に変更したアカウントを提供

- サービス提供開始当初，パスワードは全学の情報基盤システムで利用しているものから独立したものを付与
- 主たるサービス提供目的は Office アプリケーション（デスクトップアプリケーション）インストール環境の提供

先に述べた Office 365 については，2020 年 2 月頃から猛威をふるい始めた COVID-19 の世界的な拡大もあって大学が提供するサービスの遠隔利用が検討された．そのため，本学における情報基盤システムのネットワークトラフィック負荷分散を目的として，Office 365 についてはクラウドストレージサービス（OneDrive）やコミュニケーションサービス（Teams）の利用検討を教職員のテレワーク環境整備や学生とのコミュニケーション確保のために急遽検討することとなった．

結果として，2020 年度は OneDrive については教職員，学生ともに利用可能とし，Teams については教職員に限って利用可能とした．このとき，サブドメインが通常利用しているメールアドレスと異なることや，パスワードが全学の情報基盤システムで利用しているものから独立して運用されているため，利用者への周知不足もあり，利用者からの問い合わせが増加する結果となった．

これと並行して，本学では 2021 年 2 月に全学の情報基盤システムのリプレースを行い，それに合わせて組織利用のクラウドサービス利用が拡張されるようになった．システムリプレースの概要を次節にて述べる．

2.2 情報基盤システムリプレースの概要

2021 年 2 月に実施した全学の情報基盤システムのリプレースでは，基幹サーバーのデータセンター移設やのネットワーク回線の増強を行い，2017 年度より実施していたパソコン必携事業や本学附属学校における GIGA スクール構想にも対応可能な情報基盤として整備を行ってきた．

また利用者に提供するサービスの観点からは，これまで複数のサービスに対して認証連携を行ってきていたが，シングルサインオンを導入していなかったため，サービスへのログインはサービスごとに行う不便さを利用者に強いていた．今回のリプレースに伴ってシングルサインオンを導入し，利用者に対してシームレスな認証環境を提供することができるようになった．具体的な連携先サービスの例を表 1 に示す．

表 1　リプレースに伴う統合認証システムを活用したサービスの例 (2021.2〜)

	専任教員	非常勤講師	事務職員	学生
教務システム (2022.4〜)	✓	✓	✓	✓
学習管理システム	✓	✓	✓	✓
業務利用メール	✓	-	✓	-
グループウェア	✓	-	✓	-

また，これまでオンプレミスの基幹サーバーで稼働・提供していたサービスの一部をクラウド環境に移管する形でクラウドサービスの導入を行った．

2020 年 3 月から導入を行っていた Microsoft 365 Education 及び，このリプレースを期に新たに導入した Google Workspace について，それぞれ認証連携を行い，利用者に対してシームレスな利用が可能なように整備を行った．

それぞれのクラウドサービスについて利用者に対して提供しているサービスについて表 2 及び表 3 に示す．

表 2　リプレースに伴うクラウドサービスの導入内容（Microsoft 365 Education）

	専任教員	非常勤講師	事務職員	学生
Office アプリ*1	✓	✓	✓	✓
OneDrive 利用	✓	✓	✓	✓
Teams 利用	✓	✓	✓	-

表 3　リプレースに伴うクラウドサービスの導入内容（Google Workspace）

	専任教員	非常勤講師	事務職員	学生
教育利用メール (Gmail)	✓	✓	✓	✓
GoogleDrive 利用	✓	✓	✓	✓
各 Google アプリ利用	✓	✓	✓	✓

このリプレースにより，オンプレミスで運用していたサービスから利用者数が多いサービス，とりわけ学生用メールサービスをクラウドに運用することができるようになった．また，多くの学内システムについてもシングルサインオンによる認証連携を行うことができるようになり，シームレスなサービスへのアクセスを実現できるようになった．

2.2.1 システムリプレースに伴う Microsoft 365 Education の認証連携

本学における Microsoft 365 Education の利用は表 2 に示したとおりである．2.1 節で述べたとおり，もともとは Office アプリケーションの活用を主眼に

していたが，コロナ禍の影響を受けて，OneDrive や Microsoft Teams といったクラウドサービスの積極的な活用を検討することとなった．2020 年 3 月にサービスを開始していたが，2021 年 2 月のシステムリプレースに伴い，認証系を利用者管理システムと連携することとし，Azure AD Connect を利用したユーザーデータベースの同期を行うようにした．

2.2.2 システムリプレースに伴う Google Workspace の導入と認証連携

本学における Google Workspace の利用は表 3 に示したとおりである．もともと，教育利用メールと呼ばれるサービスを提供しており，教職員・学生ともに利用可能なメールサービスをクラウドサービスに移行させることを目的として実施したものである．

2021 年 2 月のシステムリプレースに伴い，教育利用メールを全面的に Google Workspace の Gmail に移行し，Google Workspace に付随するサービスに関しても基本的には利用可能とした．

なお，利用者管理システムから LDAP の情報を Google Cloud Directory Sync (GCDS) を用いてユーザーデータベースの同期を行うようにした．

2.3 統合認証システムにおける多要素認証

表 1 で示したとおり，これまで本学で利用してきた複数のサービスに対しては統合認証システムを経由してシングルサインオンを実現するようにした（図 1）．

この認証連携に関連して，高等教育機関を狙うフィッシングメールが急激に増加していることにも関連して，より安全な認証環境が求められている状況であった．本学においても情報セキュリティポリシーを策定する中で，Web メールやグループウェア等にアクセスするために認証箇所については高度で安全な認証環境の構築が急務であった．そこで，このリプレースではそれぞれの認証箇所にて多要素認証の設定が実施できるように基盤構築を行った．

図 2 にその概要を示す．今回導入した統合認証システムによる多要素認証の要求は，学外のネットワークからアクセスした場合には必須とし，学内のネットワークからアクセスした場合には利用者が任意に設定できるようにした．なお，学内のネットワークからアクセスする際の多要素認証要求の初期値は「多要素認証を要求しない」設定となっている．

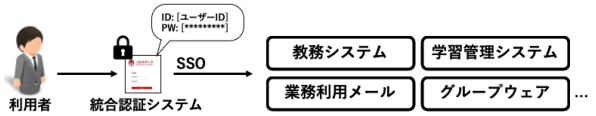

図 1　統合認証システムを活用したシングルサインオンの例

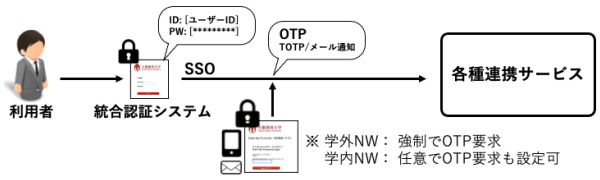

図 2　統合認証システムにおける多要素認証の実施

また，多要素認証のワンタイムパスワード認証としては TOTP アプリ利用もしくはメール通知のいずれかを選択できるようにした．ただし，多要素認証利用方法の初期値は未定義の状態であったため，利用者に対しては利用者自身で統合認証システムの設定を行い，ワンタイムパスワード認証が実施できるようにしなければ実質的に学外から関連の連携サービスが利用できない状態となっていた．

2.3.1 教職員への案内と対応

2021 年 2 月のシステムリプレース段階においては，教職員の業務利用メールへの利用に対してコロナ禍であることも重なり，多大なる支障となることが懸念された．そのため，教職員に対してはシステムリプレースにあわせて多要素認証設定の依頼文書並びに簡易マニュアルを配布した．

事前にシステムリプレースに関しては周知をしていたものの，具体的な作業依頼にまで落とし込むには検討を要する事項が多く，結果として教職員利用者に対してはごく僅かな設定可能期間しか確保することができず，電話等による利用者対応の増加に繋がる結果となった．

2.3.2 学生への案内と対応

2021 年 2 月のシステムリプレース段階においては，教職員の業務利用メールへの利用に対してコロナ禍であることも重なり，多大なる支障となることが懸念された．そのため，教職員に対してはシステムリプレースにあわせて多要素認証設定の依頼文書並びに簡易マニュアルを配布した．

事前にシステムリプレースに関しては周知をしていたものの，具体的な作業依頼にまで落とし込むには検討を要する事項が多く，結果として教職員利用者に対してはごく僅かな設定可能期間しか確保することができず，電話等による利用者対応の増加に繋がる結果となった．

2.4 Microsoft 365 Education における多要素認証設定の導入

2021 年 2 月のシステムリプレース直後，Microsoft 365 Education のサービスにおいては利用者が任意に多要素認証の設定をできるようにしていたものの，設

定は利用者に委ねる形をとった．これはシステムリプレース直後における利用者の混乱を避けるためであることと，利用者への案内を行うまでには検証が不十分であったことが挙げられる．

その後，必須化の案内と設定は 2021 年度中に実施した．

2.4.1 リプレース直後の教職員への案内と対応

教職員においては，コロナ禍となり始めた 2020 年 3 月から Microsoft Teams や OneDrive といったクラウドサービスの利用を案内し，テレワークで利用可能なリソースとして頻繁に利用していた．

Microsoft 365 Education の多要素認証については，システム管理者側で強制化した場合であっても利用者がサービスログオン直後に多要素の設定を促すようになっており，その設定が完了しない限りはログオンできない仕組みである[*2] ．

そのような背景もあり，ユーザーサポートへの負荷は他のサービスに比べて低いと判断し，2021 年 10 月冒頭に多要素認証必須化の案内を行い，同年 11 月に必須化を実施した．

2.4.2 リプレース直後の学生への案内と対応

学生においては，デスクトップの Office アプリケーションの利用を主として想定していた．OneDrive の活用についてはコロナ禍の影響もあり，情報基礎の全学必修科目 [1] で案内したほか，学習管理システムにおけるクラウドサービスの活用 Tips にも掲載していた．

Office アプリケーションのインストール権限は，学生利用者にとって権利として有しているものの，様々な理由でその権利を利用していない利用者も一定数存在している．そのため，利用の案内は行っているものの，学生利用者が必ず利用しているサービスとは言えない状況であった．

そのような背景もあり，Microsoft 365 Education のサービスを利用するにあたり，多要素認証必須化の案内や作業を行う上での重要度は教職員利用者に比べて低いものであった．また，2.4.1 項で述べたとおり，多要素認証の設定を強制にしたとしてもその設定が完了しない限りは，その設定が完了するまでログオンできない仕組みであったため，教職員利用者と同様のスケジュール・案内方法を取ることにし，2021 年 10 月冒頭に多要素認証必須化の案内を行った後，同年 11 月に必須化を実施した．

2.5 Google Workspace における Google 2 段階認証プロセスの導入

2021 年 2 月のシステムリプレース直後，Google Workspace のサービスにおいては利用者が任意に Google 2 段階認証の設定をできるようにしていたものの，設定は利用者に委ねる形をとった．これは，Google 2 段階認証の利用を必須化した場合の案内フローが確立できてなかったことや，とくに学生利用者に関して基幹のメールサービスが利用できないことが懸念されたこともあり，リプレース実施直後は利用者の混乱を回避するためである．

その後，必須化の案内と設定は 2021 年度中に実施した．

2.5.1 リプレース直後の教職員への案内と対応

教職員においては，業務利用メールを別に運用しているため，リプレース実施後まもなくは，Google サービスそのものの需要は高くはなかった．そのような中で Google 2 段階認証プロセスの必須化を案内・実施することとで他のサービスへの対応依頼も含めると利用者への混乱を招くことが予想された．そのため，リプレース直後の Google 2 段階認証プロセスの必須化は見送ることとなった．

2.5.2 リプレース直後の学生への案内と対応

学生においては，教育利用メールと称して学生用のメールアドレスの運用をオンプレミスの環境から Gmail に切り替えた．学生に対する大学からの連絡は基本的にこのメールアドレスに送付されるため，このアクセスパスが絶たれてしまうと，学生との連絡がつかなくなってしまう可能性が考えられた．コロナ禍であり，学生の入構が制限されていたり，大学に来訪することが困難な事情を持った者もいたりするような背景もあり，Google 2 段階認証プロセスの必須化の案内及び作業については慎重に行う必要があった．そのため，リプレース直後の Google 2 段階認証プロセスの必須化は見送ることとなった．

3 多要素認証必須化作業実施

本章では，これまでに説明した各サービスに対する多要素認証必須化作業の実施と，その実施に伴うサービス影響について述べる．

[*2] Microsoft の説明ページによれば，「ユーザーが認証方法にまだ登録されていない場合は、先進認証 (Web ブラウザーなど) を使用して次回サインインするときに登録するように求められます。 [有効] 状態で登録が完了したユーザーは、 [強制] 状態に自動的に移動されます。」との記述がある． https://learn.microsoft.com/ja-jp/azure/active-directory/authentication/howto-mfa-userstates

3.1 統合認証システムにおける多要素認証必須化の実施とその影響

3.1.1 既存利用者に対する対応

システムリプレース時に情報基盤システムを利用している利用者に関する主だった対応は 2.3 節で述べたとおりである．

2021 年度の新学期授業開始に向けて，学習管理システムを統合認証システム経由で利用する必要が発生したため，多要素認証の設定が未完了の場合，自宅等の学外ネットワークから学習管理システムにアクセスする術を失うことになる（図 2）．専任教職員に対しては，2.3.1 節で述べたとおり，依頼文書や簡易マニュアルでの対応を中心に行い，多要素認証の設定を促した．

一方で非常勤講師については，年度初めの授業初日まで大学キャンパスに来訪しない可能性やそもそも授業期間中に来訪することができない可能性が懸念された．そのため，非常勤講師に対して必要に応じて希望のあったメールアドレスを多要素認証のワンタイムパスワード送付先に指定する臨時の手続きを実施できるように体制を整えた．この手続きの実施には統合認証システムを管理している LDAP で管理されたデータベースを直接編集する方法を取っている．

2021 年度の授業開始前後においては，学習管理システムに多要素認証の設定を未実施であったために自宅等からアクセスできない利用者に対して専用の申請フォームを設置し，2021 年 3 月から 4 月にかけての申請数は，学生・教職員あわせて 364 件にものぼった．その後，後期授業が開始される 2021 年 10 月 1 日前後を境に申請数の増加が確認されたものの，2022 年度以降の申請は僅かながらにあるだけで，ほぼ収束している状態である．

3.1.2 新規利用者に対する対応

システムリプレースに合わせた統合認証システムの多要素認証設定対応は，初期状態が未設定であるがゆえに利用者にその設定を強制してしまうこと，また，学内ネットワークからのアクセスの場合は多要素認証の設定をせずとも認証できてしまうことから，利用者視点でアカウントのセットアップを行うときにこの多要素認証設定を行わずとも利用そのものができてしまうことにあった．

そこで，2022 年度の新規利用者に対しては，多要素認証の初期設定値を教育利用メールである大教 Gmail のメールアドレスに設定することを基本とした．表 3 のとおり，大教 Gmail は利用者管理システムに登録されているほぼすべての構成員が利用可能である．このことを利用し，多要素認証に利用するワンタイムパスワードの送付先を設定した上で新規アカウント作成し，新規利用者にアカウントを配布した．

なお，一部で大教 Gmail を利用できないロールが存在するため，そのアカウントに対しては当該利用者に事務局からワンタイムパスワード送付先をヒアリングし，システム管理者が直接の設定を行う方法をとっている．

3.2 Microsoft 365 Education における多要素認証必須化の実施とその影響

3.2.1 既存利用者に対する対応

Microsoft 365 Education の多要素認証必須化に関する主な経緯は 2.4 節で述べたとおりである．

システム管理者側で多要素認証を利用者に強制化した場合であっても，その利用者がサービスログオンした直後に多要素の設定を促すようになっており，設定が完了しない限りはログオンできない仕組みである．そのため，2021 年 10 月に必須化の案内を行い，同年 11 月に必須化を実施した．

3.2.2 新規利用者に対する対応

新規利用者への対応については，利用者のロールによって細かなニーズが異なるものの，ユーザーアカウント利用時にセットアップを行う案内をした．アカウント配布後，約 1 ヶ月程度を目安に多要素認証を必須としない状態とし，その間に多要素認証の登録作業を行ってもらう流れである．特に，新入生については対応人数が膨大になることから，セットアップマニュアルを作成・配布することとで対応を行った．

3.3 Google Workspace における多要素認証必須化の実施とその影響

3.3.1 既存利用者に対する対応

Google Workspace の Google 2 段階認証プロセス必須化に関する主な経緯は 2.5 節で述べたとおりである．

専任教職員や非常勤講師，学生といったそれぞれのロールによって，Google 環境の重要度が異なることと，必須化作業を行う段階において，る Google 2 段階認証プロセスが未設定である利用者については管理者側で特別な対応を実施する必要があったため，利用者への案内と必須化の実施は慎重に行われた．

専任教職員に対しては，コロナ禍における学生へのコミュニケーションパスやクラウドサービスを活用した資料共有の利便性確保を行うべく，事務局を主として会議利用を想定した活用を模索することとなった．結果として，学内の会議資料を Google ドライブ

で取り扱うことを事務局で取り決め，教職員に対してGoogle ドライブの活用が円滑に進むように準備・案内を行った．

2021 年度中に，ほぼすべての専任教職員が参加する会議が控えていたため，その会議の参加にあわせてGoogle 2 段階認証プロセスの必須化を実施した．具体的には 2021 年 9 月末に当該会議が実施されるスケジュールであったため，約 1 ヶ月前の 2021 年 8 月末にアナウンスを行い，当該会議の実施直前に Google 2 段階認証プロセスの必須化を実施した．

また，Google 2 段階認証プロセスの必須化を実施するにあたり，学生や非常勤講師に対しては，連絡先の生命線となるメールサービスへのアクセスパスを断つことのないように繰り返しアナウンスを行った．この案内は 2021 年 10 月から案内を開始し，必須化作業を実施するまでに 5 回程度の周知・再通知を行い，設定実施を促した．最終的に 2022 年 1 月に必須化を実施した．

なお，未設定の学生利用者はある程度の数が認められることが予想されたため，設定猶予を申請に基づいて自動的に実施できる支援ツールを開発し，利用者の設定支援にあたった [2]．

結果として，周知・案内を受け取れていない利用者がわずかに残るものの，9 割以上の既存利用者に対しては Google 2 段階認証プロセス必須化の実施を完了させることができた．

3.3.2 新規利用者に対する対応

新規利用者への対応については，利用者のロールによってニーズが異なるものの，ユーザーアカウント利用時にセットアップを行う案内をした．アカウント配布後，約 1 ヶ月程度を目安に多要素認証を必須としない状態とし，その間に多要素認証の登録作業を行ってもらう流れである．特に，新入生については，連絡の生命線となるメールアドレスの利用に関わることから，セットアップマニュアルを作成・配布するとともに，時間確保可能な部署においてはセットアップガイダンスの時間を設け，メールアカウントのセットアップ作業と同時に Google 2 段階認証プロセスの設定を行ってもらうべく，セットアップ支援対応を行った．

4 多要素認証必須化後における利用者へのフォローアップ

本章では，各サービスの多要素認証必須化後に生じた事象とそのフォローアップについて述べる．

4.1 統合認証システムにおける多要素認証必須化に関するフォローアップ

統合認証システムにおける多要素認証の設定についてはシステムリプレース時に設定マニュアルを準備し，案内を行ったため，当時作成したマニュアルをベースに本稿執筆時点においても利用者に対しての案内や説明を行うことができている．また，既存利用者の中でも多要素認証未設定利用者を一部残すのみとなり，新規登録利用者については初期値を設定してアカウントを配布するため，大きな混乱には至っていない．

ただし，統合認証システムの設定の中で「学内ネットワークであっても多要素認証を必須とする」設定がオプションで存在し，利用者自身がその設定内容を理解していないままに設定を施す利用者が若干名存在しており，たびたび「鍵の閉じ込め」トラブルが発生している．利用者からの問い合わせがあった際に，管理者側でその「鍵の閉じ込め」設定を個別に対応する措置を取っている．

4.2 Microsoft 365 Education における多要素認証必須化に関するフォローアップ

Microsoft 365 Education における多要素認証の設定については，2021 年 10 月に既存利用者に多要素認証設定の案内を行うべく設定マニュアルの作成を行った．認証に設定可能な要素としては Microsoft が提供している標準の方法である「認証アプリ」，「電話番号 (SMS・音声)」及び「セキュリティキー」があり，利用者が個別に選択できるようにしている．殆どの利用者は認証アプリや電話番号を利用しているが，携帯電話を所有していない利用者に対して，PC にプラグインを導入することでスマートフォンの認証アプリのように PC のみで認証を完結できる方法や希望者に対してセキュリティキーを貸与することで運用を柔軟に行っている．

4.3 Google Workspace における多要素認証必須化に関するフォローアップ

Google Workspace の Google 2 段階認証プロセスの設定については，2021 年 8 月に既存利用者の中でも専任教職員から順次設定の案内を行うべく設定マニュアルの作成を行った．認証に設定可能な要素としては統合認証システムの多要素認証設定時に案内している「認証アプリ」に加えて，「Google アプリ」や，「電話番号 (SMS・音声)」，「セキュリティキー」をあり，利用者が個別に選択できるようにしている．Google 2 段階認証プロセスについては，Microsoft 365 Education の多要素認証と同様に殆どの利用者は認証アプリや電

話番号を利用しているが，携帯電話を所有していない利用者に対して，PC にプラグインを導入することでスマートフォンの認証アプリのように PC のみで認証を完結できる方法や希望者に対してセキュリティキーを貸与することで運用を柔軟に行っている．

4.4 利用者からの問い合わせ

システムリプレース直後の対応や 2021 年度中に実施した各種サービスにおける多要素認証の必須化対応を終え，システムリプレース直後の既存利用者への概ねの対応は完了した．また，2022 年度の新規利用者が入り交じる運用となって半年以上が経過し，現行の情報基盤システムにおいては安定した運用時期に差し掛かった．

2022 年度の各サービスにおける認証設定に関する問い合わせ件数を表 4 に示す[*3]．

表 4　各サービスにおける認証設定に関する問い合わせ件数（2022 年度）（件）

	統合認証	M365	GWS
4 月	24	28	40
5 月	12	4	13
6 月	5	5	0
7 月	9	7	0
8 月	7	2	3
9 月	16	6	8

年度はじめについてはアカウントのセットアップ作業等で利用案内を行うことから，相対的に対応件数が多い傾向にある．また，長期休みである 9 月についても「携帯電話の機種変更や破損にともなう多要素の紛失」を理由に，多要素認証に関連する問い合わせが授業期間中に比べると増加する傾向にあった．これは，9 月の中旬に後期授業の履修登録を実施する影響で，多くの学生利用者が学外からの統合認証システムのアクセスを必要とするが，多要素の移行作業を適切に行えていなかったためであると推察される．また，本学において同時期には教育実習を実施しており，上記と同様の理由でアクセスできないかつ早急なアクセスを求められる対応に迫られた．

これらの対応はいずれも大学の行事にあわせて需要が変動する事項であり，これまで各部署で独立して運用していたサービスを認証基盤についてすべて片寄せしたことで大学の情報基盤を担う部署に問い合わせが多く来ることが自明である結果と言える．そのため，今後認証基盤に関わるサービスを利用者に必ず利用させるようなプロセスが発生する場合，利用者に対しての事前周知や情報基盤を担う部署である情報基盤センターへの事前の相談等，大学運営側の密な連絡を行うことが課題であると考えられる．

[*3] 情報基盤センターや ICT 教育支援ルームにおける，参照可能な対応記録から抽出した．

5 おわりに

本稿では，本学における複数のサービスのそれぞれに対して，多要素認証を必須化し，利用者への案内や実際の実施，それに係る支援とその状況について報告した．現行の情報基盤システムの運用も 2 年目に差し掛かり，1 年目に多くの利用者対応を要した多要素認証設定に関しても，利用者問い合わせ件数の結果から，ある程度落ち着いた運用フェーズに入ったと言える．

一方で，認証部分を情報基盤センターが一手に担っていることもあり，例えば履修登録といった短期間かつ大規模な情報基盤システムの利用が観測されると，利用者対応に時間を要することとなる．サービスを提供する側それぞれの立場で情報基盤システムを活用していることを土台に，サービス利用者へのより適切な案内や支援ができるように，情報連携を密にしていくことが今後の課題として挙げられる．

参考文献

[1] 尾崎拓郎，佐藤隆士，片桐昌直：学習管理システムを利用した全学情報関係共通必修科目「ICT 基礎 a」の実践，大学 ICT 推進協議会 2017 年度年次大会，WA2-6，2017.

[2] 山本望実，坂本伸行，松井聰治，尾崎拓郎，佐藤隆士：多要素認証未設定者に対する利用資格変更自動対応システムの提案，情報処理学会研究報告，インターネットと運用技術，Vol.2022-IOT-56，No.24，pp.1-3，2022.