Vol.2022-IOT-58 No.12
2022/7/12

旧教職員向け電子メールシステムにおける多要素認証の導入

根本 貴弘[1,a)]　三島 和宏[1,b)]　石橋 みゆき[1,c)]　長島 和平[1,d)]　青山 茂義[1,e)]

概要：東京農工大学では，近年の高度化するサイバー攻撃から学内情報資産を守るために，2021 年より全学的な多要素認証の導入に取り組んでいる．2022 年 5 月には，Microsoft365 のクラウドメールサービスを利用した「旧教職員向け電子メールシステム」の全アカウントに対する多要素認証の有効化を完了した．本システムでは，Microsoft が提供する多要素認証機能を使用しており，利用者が事前に各自で多要素認証の設定を行えるように，多要素認証設定マニュアルの作成や多要素認証設定講習会の実施，学内の会議体での説明や教職員向けのポータルサイト等で周知をしてきた．本稿では，「旧教職員向け電子メールシステム」における多要素認証導入における取り組みとして，導入に向けたこれら周知活動に加え，問い合わせ状況可視化ツールを用いた総合情報メディアセンターへの問い合わせ状況と多要素認証の設定状況についてまとめ，報告をする．

キーワード：大学情報システム, 情報セキュリティ, 多要素認証, 利用者支援，教職員研修

Deployment of multi-factor authentication to the old faculty e-mail system

1. はじめに

近年のサイバー攻撃の高度化に伴い，インターネット上の脅威から利用者を守るための仕組みとして，ID/パスワードによる認証に加えて追加の認証を行う多要素認証の利用が推奨されている．東京農工大学（以下，本学）では，サイバー攻撃から学内情報資産を守るために，2021 年より全学的な多要素認証（二要素認証）の導入に取り組んでいる．現在対象としているシステムは，2021 年に導入した統合認証システムと旧教職員向け電子メールシステムである．統合認証システムは，学内の各種教育研究用システムに対しシングルサインオン機能等を提供する認証基盤で，2022 年 8 月に全ユーザアカウントの多要素認証機能を有効化することを目指し，段階的に多要素認証の有効化を実施している．一方で，旧教職員向け電子メールシステムは，2015 年までに着任した教職員に対し発行を行なってきた電子メールアカウントで，本メールアカウントを主要なメールアドレスとして業務で使用している利用者も多いことから 2016 年以降も運用を継続しており，こちらも段階的に多要素認証の有効化を行い，2022 年 5 月に全ユーザアカウントの多要素認証機能の有効化を完了した．

情報システムログイン時の多要素認証機能を有効化することで，利用者は多要素認証を設定するまで対象の情報システムが利用できなくなることから，多要素認証の導入は業務への影響が大きい．そのため多要素認証は，特に円滑な導入が求められるシステムである．

本学では，多要素認証機能を有効化する期日を設け，各利用者が事前に対象システムの多要素認証の設定を自身で行なってもらう方針で導入を行なってきた．この場合，円滑な導入を行うためには，事前の周知活動による事前の設定者数を増やすことと，期日後の問い合わせ件数を減らすことが重要であると考える．あらかじめ多要素認証の設定をしてもらうことで，多要素認証機能有効化当日もその影響を受けず，業務を継続できることが期待できる．また，期日後の問い合わせ件数が，問い合わせ対応者が 1 日の業務時間内に回答可能な件数を超える場合，問い合わせ者はその日対象システムを利用できない状況になることが想定

[1] 東京農工大学
Tokyo University of Agriculture and Technology
[a)] nemo@go.tuat.ac.jp
[b)] three@cc.tuat.ac.jp
[c)] saji@cc.tuat.ac.jp
[d)] nagashima@go.tuat.ac.jp
[e)] aoyama@go.tuat.ac.jp

される．そのため，期日前までにどの程度利用者が設定を完了しているかを把握しておく必要がある．

本稿では，旧教職員向け電子メールシステムにおける多要素認証導入における取り組みとして，導入に向けたこれら周知活動に加え，問い合わせ状況可視化ツールを用いた本センターへの問い合わせ状況と多要素認証の設定状況についてまとめ，報告をする．

2. 旧教職員向け電子メールシステムの多要素認証

2.1 旧教職員向け電子メールシステム概要

本学では，Microsoft365 のクラウドメールサービスを利用し，旧教職員向け電子メールシステムを提供している．2015 年までに着任した教職員に対しアカウント発行を行なってきたが，2016 年以降は，Google workspace 及び Microsoft365 のクラウドメールサービスのクラウドメールサービスを利用する全学電子メールシステムの導入に伴い，新規アカウントの発行は停止した．一方で，旧教職員向け電子メールシステムのメールアカウントを業務上の主要なメールアドレスとして継続利用する利用者が多いことから 2016 年以降も運用を継続している．なお，利用者は，常勤教職員の他に，非常勤教職員と名誉教授がいる．

多要素認証の導入のための取り組みをはじめた，2021 年 7 月の旧教職員向け電子メールシステムのアカウント数は 1,280 件であった．また，その利用者別の内訳は**表 1** に示す通りである．

表 1 旧教職員向け電子メールシステムの利用者別アカウント数

利用者	アカウント数
常勤教職員	1085
非常勤教職員	78
名誉教授	117

2.2 旧教職員向け電子メールシステムの多要素認証

旧教職員向け電子メールシステムでは，統合認証システムの仕様上の制約による導入コストの増大や統合認証システム導入当時 Microsoft365 の Web アプリケーションがマルチアカウントの切替機能を有していなかったことにより，2016 年以降提供を開始した全学電子メールシステムとの併用による利便性向上が期待できないこと等の複合的な理由から，統合認証システムは利用せず，Microsoft が提供する多要素認証機能を利用することとした．Microsoft が提供している追加の認証要素は**図 1** に示す通り，認証アプリを用いた認証と電話を用いた認証である．

認証アプリを用いた認証方法には以下の 2 通りがある．

- 通知方式
- TOTP(Time-based One Time Password) 方式

通知方式は，Microsoft の「Authenticator」アプリをインストールしているスマートフォンに対して，サインイン通知が届くので，その通知に対して，承認を選択することで認証を行う方法である．この方式は，インターネット接続環境があれば利用可能であることや他の認証方式で認証失敗による一時的な利用制限がかかっても利用可能であること等の特徴がある．なお本学では，スマートフォンを所有する利用者に対しては本認証方式を推奨している．

図 1 Microsoft が提供する追加の認証要素

TOTP 方式は，ソフトウェアトークン（Google や Microsoft の「Authenticator」アプリ等）で OTP(One Time Password) を表示し，その数字を認証画面に入力することで認証を行う方法である．この方式は，インターネット接続環境がなくても利用可能であることや Microsoft の「Authenticator」アプリ以外でも使用可能である等の特徴がある．なお，スマートフォンやパソコンの複数の認証アプリの設定支援を行うことは困難であったことから，本方式については，パソコンで認証アプリを使用する方法として，Twilio の「Authy」アプリを用いた設定方法のみを紹介している．

また，電話を用いた認証方法には以下の 2 通りがある．

- SMS(Short Message Service) 方式
- 通話方式

SMS 方式は，登録した SMS を受信できる携帯電話番号に対して OTP を記載したショートメッセージが送信されるので，その数字を認証画面に入力することで認証を行う方法である．この方式は，認証アプリのインストールが不要であることや通信圏外では利用不可であること，海外での SMS 使用については契約している電話会社に確認が必要等の特徴がある．

通話方式は，登録した電話番号に対して OTP を告げる電話が発信されるので，そこで告げられた数字を認証画面に入力して認証することで認証を行う方法である．この方式は，SMS 方式同様に，認証アプリのインストールが不要であることや通信圏外では利用不可であること等の特徴に加え，固定電話の電話番号を登録する場合，固定電話が設置された場所でしか使用できないという特徴がある．

また，認証に使用する機器毎に利用可能な認証方式を整理したものを**表 2** に示す．各認証方式に対してその認証方式が利用可能な機器は「○」，利用不可能な機器は「×」を記している．なお，表中のスマホはスマートフォンを意味する．また，設定によってはパソコンで SMS を受信する方法もあるが，通常，SMS はスマートフォンや携帯電話等で受信するものであるため，表中では「×」としている．

表 2 機器毎に利用可能な認証方式

	スマホ	パソコン	携帯電話	固定電話
通知方式	○	×	×	×
TOTP 方式	○	○	×	×
SMS 方式	○	×	○	×
通話方式	○	×	○	○

なお本学では，認証に使用する機器の故障や紛失，アプリの削除等により，旧教職員向け電子メールシステムが使用できなくなる機会を減らすために，複数の認証方式の設定を推奨している．

3. 多要素認証導入に向けた取り組み

本学の多要素認証の導入は，全アカウントを対象とする多要素認証機能の有効化日を 2022 年 1 月 5 日に設定し，それまでに利用者が各自で対象システムの多要素認証の設定を自身で行なってもらう方針で導入を行なってきた．本センターでは，2.2 節でも述べたように，スマートフォンで認証アプリを使用したい利用者には Microsoft の「Authenticator」アプリを使用した通知方式を，パソコンで認証アプリを使用したい利用者には Twilio の「Authy」アプリを使用した TOTP 方式を紹介するとともに，電話を用いる認証を含む複数の認証方式の設定を推奨している．

有効化実施日当日を迎えても利用者が，旧教職員向け電子メールシステムを利用できるようにするため，また，有効化後の問い合わせ件数を減らすためには，事前に多要素認証の設定を終えていることが重要であることから，本センターでは多要素認証に関して**表 3** に示す周知活動を行なってきた．

本学では，2021 年 7 月の両学部教授会での多要素認証導入に向けた説明を行なった後，専用サイトを用意し，多要素認証に関するマニュアルや FAQ，スケジュール，講習会資料の公開等の情報発信を行なってきた．なお，マニュアルについては利用者からの問い合わせを受けてわかりにくい部分については適宜改版を行なってきた．また，利用者に対して能動的にお知らせ発信を行うために，教職員ポータルや旧教職員向け電子メールシステムの全アカウント宛のメーリングリスト（ML）でのお知らせ発信も行なってきた．本学の教職員ポータルでは，お知らせをポータルサイトに掲示すると，そのお知らせ内容が本学の教職員のメールアドレス宛に届く仕組みとなっている．なお，お知らせ発信に教職員ポータルの他にメーリングリストを利用した理由は，名誉教授が教職員ポータルを閲覧できないため，別途，名誉教授を含む旧教職員向け電子メールシステムの全アカウントを宛先とするメーリングリストを用意した．

表 3 周知活動のタイムライン

日付	媒体	周知内要
2021/7/14	農学部教授会	多要素認証導入の説明
2021/7/14	工学部教授会	多要素認証導入の説明
2021/7/30	専用サイト	専用サイトの公開
2021/7/30	教職員ポータル	専用サイト公開の案内
2021/9/17	教職員ポータル	説明会開催の案内
2021/9/24	説明会	概要と実施時期の紹介
2021/9/24	教職員ポータル	説明会資料公開の案内
2021/11/12	教職員ポータル	有効化実施日及び講習会の案内
2021/11/17	専用サイト	設定マニュアルの公開
2021/11/29	教職員ポータル	有効化実施日及び講習会の案内
2021/11/30	ML	有効化実施日及び講習会の案内
2021/12/2	講習会	設定方法の紹介
2021/12/3	教職員ポータル	講習会資料公開の案内
2021/12/24	教職員ポータル	有効化実施日変更の案内
2021/12/24	ML	有効化実施日変更の案内
2022/3/11	教職員ポータル	有効化実施日及び講習会の案内
2022/3/11	ML	有効化実施日及び講習会の案内
2022/3/22	講習会	設定方法の紹介
2022/3/24	講習会	方法の紹介
2022/4/26	教職員ポータル	有効化実施日の案内
2022/4/26	ML	有効化実施日の案内

しかし，2021 年 12 月 24 日時点での，設定済みアカウント数が 1280 件中 637 件と全体の半数未満であったことから，このまま多要素認証機能を有効化した際に，有効化実施日当日，残りの 643 件のアカウント所有者から一斉に問い合わせが生じた場合，当日中の問い合わせ対応は困難であると判断し，有効化実施日を延期することとし，そのお知らせ発信を行なった．

また，延期後の有効化実施日のお知らせは 2022 年 3 月に行った．なお，延期後の有効化実施日は，名誉教授を 2022 年 4 月 13 日，その他の教職員を 2022 年 5 月 11 日とし，それまでに各自が業務影響の少ない時期を見て設定するよう設定の依頼を行なった．また，名誉教授とその他の教職員で実施日を分けた理由は，実施日後の問い合わせ件数を分散させるためである．

4. 設定済アカウント数と問い合わせ件数の集計方法

多要素認証の円滑な導入を実現するためには，現在の設定済アカウント数と 1 日に対応可能な問い合わせ件数を把握しておくことが重要であるため，今回の多要素認証の導入では，以降の方法により，設定済アカウント数の集計と問い合わせ件数の集計を行なった．

4.1 設定済アカウント数の集計

多要素認証設定済アカウント数は，Microsoft の PowerShell を利用し，アカウント名とそのアカウントが設定している多要素認証の認証方式を csv ファイルに出力し，多要素認証の認証方式に値が入っているアカウントを設定済みアカウント，値が空のアカウントを未設定アカウントとみなして集計を行なった．また，出力された csv ファイルのアカウント名と本センターで管理している旧教職員向け電子メールシステムのアカウント管理表を照合し，設定済み利用者の職種や所属等も把握できるようにした．なお，集計は 2021 年 11 月 22 日より開始し，集計時期は不定期であるが，概ね周知活動実施日や有効化実施予定日の後前後の時期に実施を行なった．

4.2 メールでの問い合わせ件数の集計

本センターでは，問い合わせ受付用メールに Google グループを利用している．メールに関する問い合わせについては，未回答を防止する目的で問い合わせメールに対する回答の有無を Google スプレッドシート上に出力する仕組みを 2020 年頃より Google Apps Script（GAS）を用いて実装していた．この仕組みでは，問い合わせ内容の傾向を捉えるため，あらかじめ設定したキーワードがメールの件名や本文に含まれているかを出力する機能があり，今回の多要素認証の導入においては，旧教職員向け電子メールシステムに関する問い合わせを区別するためのキーワードとして，旧教職員向け電子メールシステムのドメイン名や学内での略称等をキーワードに設定し，それらを含むメールの件数を集計した．

4.3 窓口及び電話での問い合わせ件数の集計

本センターへの問い合わせは，メールでの受付を原則としつつ，窓口及び電話での問い合わせも受け付けている．しかし，メールでの問い合わせ状況については 4.2 節の通り，可視化可能であるが，窓口及び電話での問い合わせについては可視化が行われてこなかった．そのため，窓口及び電話で受け付けた問い合わせ内容が本センター関係者間で共有できず，過去の回答例が利用できないという問題があった．そこで，2021 年 9 月頃より問い合わせ内容を共有する目的で，**図 2** に示す窓口及び電話での問い合わせ内容を可視化するツールを用意した．このツールは，Google フォームを利用した簡易的なものであり，フォームに回答をすると，その結果が Google スプレッドシートに記録されるとととともに本センター関係者全員にその回答内容がメールで通知される仕組みとなっている．本ツールでは主に以下の情報が記録されており，今回の多要素認証の導入においては，旧教職員向け電子メールシステムと多要素認証に関するカテゴリが選択されているものを対象に集計を行なった．

- 問い合わせ日時
- 問い合わせ媒体
- カテゴリ
- 問い合わせ者の属性
- 問い合わせ者の所属キャンパス
- 回答に要した時間
- 問い合わせ内要
- 回答内要

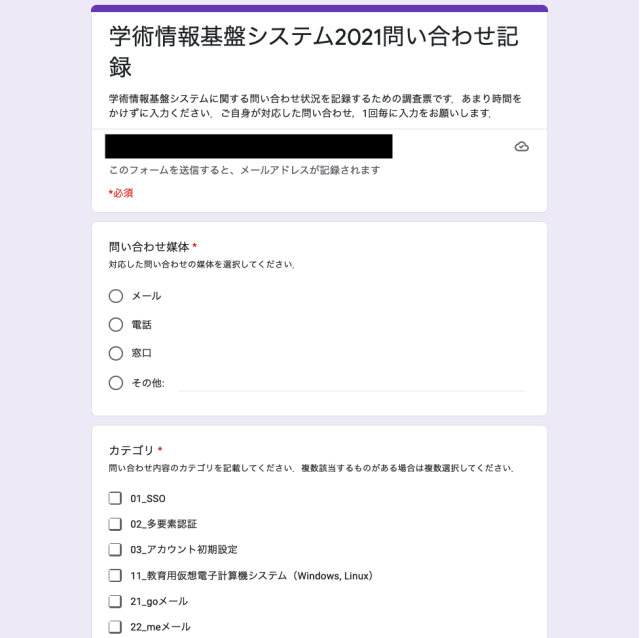

図 2 Microsoft が提供する追加の認証要素

5. 設定状況と問い合わせ状況

本節では，4 節で述べた方法により集計した設定状況と問い合わせ状況の結果とそれらに対する考察について述べる．

5.1 設定状況

多要素認証の設定状況として，**表 4** に設定状況の総数と利用者別内訳を，**図 3** に表 4 の値をグラフ化した設定者数の推移を示す．表 4 中の，総数は設定済アカウントの総数，常勤は常勤教職員，非常勤は非常勤教職員を意味し，総数，常勤，非常勤，名誉教授の各列における数値は設定済アカウント数を意味する．

2021 年 11 月 17 日に設定マニュアルを公開してから徐々に設定者が出はじめ，12 月 2 日の講習会実施後の 12 月 6 日の設定済アカウント数が 153 件となり，12 月 24 日には設定済アカウント数が 637 件まで増加した．しかし，同日有効化実施日の変更の案内を発出してから延期後の有効化実施日の案内を行なった 2022 年 3 月 11 日後の 3 月 22 日までに設定されたアカウント数は 126 件と緩やかになり，その後 5 月 11 日の有効化実施日までに設定済アカウント

数が 164 件増加している．なお，5 月 16 日から 5 月 23 日にかけて設定済アカウント数が減っている理由は，不要になったアカウントの削除を行なったためである．

表 4　設定状況の総数と利用者別内訳

日付	総数	常勤	非常勤	名誉教授
2021/11/22	11	8	2	1
2021/11/29	23	16	6	1
2021/12/6	153	138	9	6
2021/12/11	292	261	22	9
2021/12/16	360	314	32	14
2021/12/21	590	524	44	22
2021/12/24	637	567	45	25
2022/1/24	722	643	46	33
2022/3/22	763	674	49	40
2022/3/24	766	675	49	42
2022/4/12	785	689	50	46
2022/4/13	800	690	51	59
2022/4/25	822	691	53	78
2022/5/11	927	787	60	80
2022/5/12	951	810	61	80
2022/5/16	958	816	62	80
2022/5/23	956	816	60	80

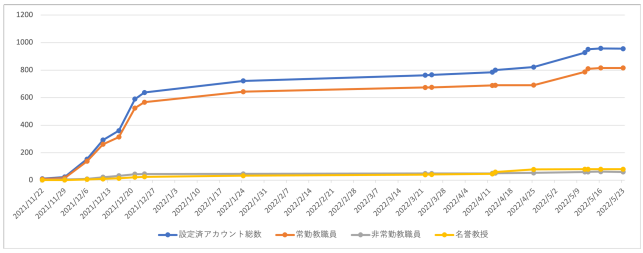

図 3　設定者数の推移

この結果から，期日の直前に設定者数が増加する傾向があることが考察できる．また，5 月 11 日の有効化実施日の前後に集計した，4 月 25 日と 5 月 16 日の設定済アカウント数の差から，概ね有効化実施後に設定を行なったアカウント数は 136 件以内であることがわかる．一方で，アカウント総数である 1,280 件と 4 月 25 日の設定済アカウント数の差が 458 件であることから，使用されていないアカウントが存在することがわかった．そのため，多要素認証の導入に際しては，事前に未使用アカウントの棚卸しをしておくことで，期日の延期等をより適切に判断できることがわかった．

5.2　問い合わせ状況

旧教職員向け電子メールシステムの多要素認証に関する問い合わせ件数を日毎に集計したグラフを**図 4** に示す．図 4 では，受け付けた問い合わせの総数とその内訳として，窓口，電話，メールでの問い合わせ件数を示す．また，同期間中に受け付けた問い合わせ件数とその内訳を日毎に集計した**図 5** に示す．

多要素認証に関する問い合わせは，有効化実施日当日とその直前の 1 ヶ月程度の期間に増加する傾向がわかった．また，全体的な問い合わせはメールによる問い合わせが多い一方で多要素認証に関しては，窓口での問い合わせが多いこともわかった．また，1 日の問い合わせ件数は最大で 80 件程度であり，多要素認証の有効化実施日近くで 60 件程度となった．また，実際の設定数に対して問い合わせ件数が少ないことから，多くのユーザは事前にマニュアルを読んで自身で設定を行えていることがわかった．

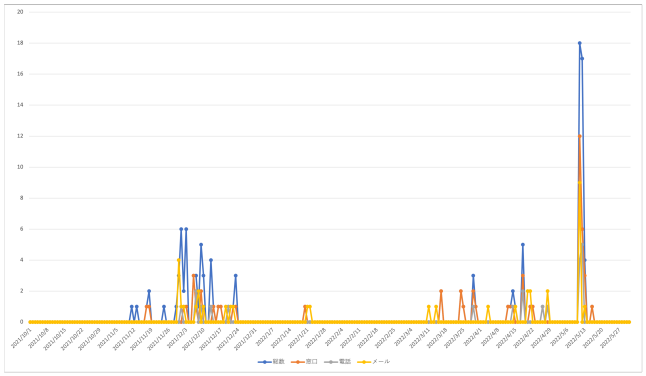

図 4　多要素認証に関する問い合わせ件数の推移

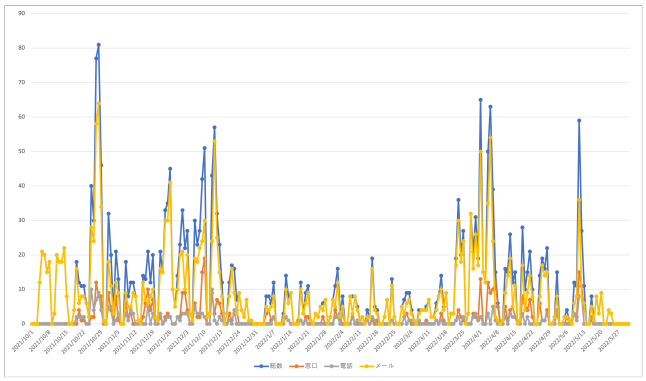

図 5　全問い合わせ件数の推移

6.　おわりに

本稿では，旧教職員向け電子メールシステムにおける多要素認証導入における取り組みとして，導入に向けたこれら周知活動に加え，問い合わせ状況可視化ツールを用いた本センターへの問い合わせ状況と多要素認証の設定状況についてまとめ，報告をした．その結果，設定済アカウント数も問い合わせ件数も期日の 1 ヶ月程度まえから増加する傾向がわかった．また，実際に設定したアカウント数が総数よりも少なかったことから，事前に未使用アカウントの棚卸しを行なっておくことが重要であることがわかった．