岐阜大学統合認証およびMicrosoft365への多要素認証導入について

田中宏和[1]・田中昌二[1]・渡邉美穂[1]・上田康信[1]

1.岐阜大学　管理部 情報連携課

近年，標的型メール攻撃や偽Webページ等による本学システム利用者のアカウント情報の窃取，また利用者自身による不適切なパスワード管理といった原因により，岐阜大学の情報システム（主にメールシステム）が不正に利用される事案が増加してきている．本学でも，情報セキュリティ強化が求められている状況を鑑み，今年度統合認証およびMicrosoft365について多要素認証を導入することとなった．本稿では，岐阜大学における多要素認証導入の状況を報告する．

Key Words： *多要素認証，統合認証，Microsoft365*

１．はじめに

近年，コンピュータシステムの利用促進に伴い，それを狙ったセキュリティインシデントが多発するようになっている．どの組織においても，その対策は年々重要度を増しており，非常に大きな労力を払っていることも周知になってきている．

本学システムにおいても，アカウント情報の不適切な取り扱い（外部サービスとのアカウント情報使いまわし，パスワードが容易に推測できる状態で使い続けている）や，学外での情報管理上の問題行為（ホテル等での共用PCやFree WiFi，無料充電スポット等の安易な利用），フィッシングメール等によりアカウント情報を窃取され，システムを不正利用される事案が後を絶たない状況が続いていた．

大学としても情報セキュリティ強化の要請を受けており，その必要性は認識されていた．

２．多要素認証の導入に向けて

情報セキュリティ強化に関し，CSIRT 活動として教育・研修と情報セキュリティインシデント発生時の対応は継続的に行っているものの，構成員各員の努力だけでなくシステム的な対応を行うことでインシデント発生の可能性を抑える必要があった． その方法として，本学では統合認証とMicrosoft365利用認証において，多要素認証を導入することとした．

(1) 情報セキュリティ強化に関する対応の検討

情報セキュリティ強化に関するシステム的な対応を行うにあたり，どの程度の予算措置が可能か，投入できる人的資源等を検討した．その結果，多要素認証の導入が適当であるという結論に達した．

多要素認証の導入に向けた準備として，テスト環境を準備し変更点や問題点を洗い出しつつ，利用者向けマニュアル整備を行うこととした．（2019年11月本格着手）また導入時期の目標としては2020年前期からとされた．

2020年に入って新型コロナウィルス感染症が流行し，その対応が優先されたことで，準備作業への支

障や導入時の混乱がコロナ対応の混乱と重なることが危惧されるようになった．このため，多要素認証については導入時期を延期し，2020 年後期とすることになった．

（a）統合認証での多要素認証の検討

本学統合認証（Single Sign On）には，もともと多要素認証を想定した機能があったので，基本的にそれを利用することとした．多要素認証の方法としては，システムに登録したスマホアプリの認証コードを利用する方法，あるいは登録したメール宛にワンタイムパスワードを送信する方法のどちらかを利用する内容となっている．両方設定してもよいが，認証時にどちらか選択して認証を行う方式となっている．

使用するスマホアプリ（Authenticator）は，統合認証を提供している SECIOSS 社のものと Microsoft 社のものを比較検討し，Microsoft365 の多要素認証への利用も考慮し，Microsoft 社のものを採用することにした．

Fig. 1　多要素認証導入前のログイン画面
（多要素認証導入後も第一要素として残る）

Fig. 2 多要素認証導入後の画面（第二要素選択）

Fig. 3　多要素認証導入後の画面（第二要素入力）

Fig. 4　多要素設定画面（QR コード）

（b）Microsoft365 での多要素認証の検討

Microsoft365 については，Microsoft 社が提供している多要素認証の機能を利用することで検討を進めた．

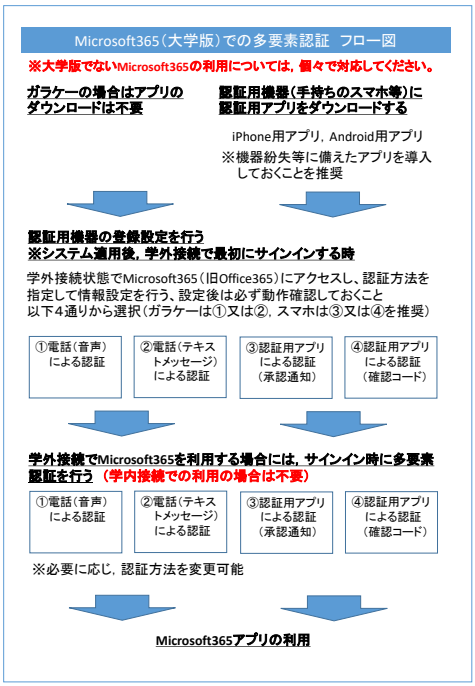

Fig. 5　Microsoft365 多要素認証のフロー図

多要素認証の方法としては，大きく電話番号を使う方法とスマホアプリを使う方法があり，それぞれ２通りのパターンの全４パターンの方法がある．

具体的には 1．音声電話がかかってきて特定の操作を行う，2．電話番号の SMS に認証コードが送信される，3．スマホアプリで承認要求が通知される，4．スマホアプリの認証コードを入力する，の 4 パターンである．

下図は,Authenticator アプリの参考画面である．上２つは統合認証用アカウント（個人用と事務用），一番下が Microsoft365 用であり，必要に応じて使い分けて多要素認証を行う．

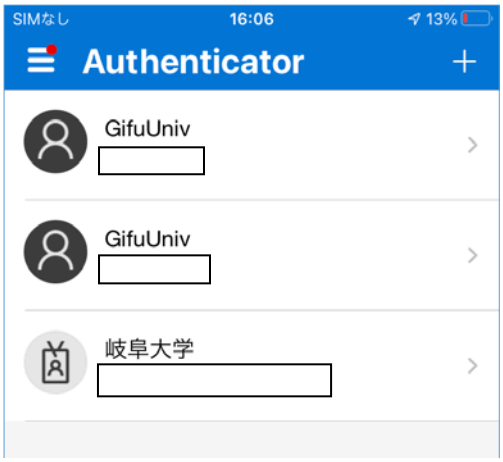

Fig. 6　Microsoft Authenticator 参考画面

（2）準備の進捗状況

2019 年 11 月から準備してきた統合認証における多要素認証は，3 月時点で公開準備の段階まで進行していたが，コロナ禍により 4 月適用を断念することとなった．3 月から 5 月の約 3 ヶ月間に Microsoft365 側の多要素認証の動作検証およびマニュアル作成などの準備を進め，統合認証と Microsoft365 の多要素認証を 10 月に同時適用することを新たな目標とした．なお，10 月 1 日では履修登録への影響が大きいとの意見もあったことから，適用期日は 10 月 19 日とされた．

また留学生向けの英語マニュアルの整備，設定動画作成，学外者向けメール認証代行手順整備といったことを行い，混乱が最小限となるよう準備した．

（3）多要素認証導入とその後の対応状況

2020 年 9 月 18 日に全学に対して多要素認証導入のアナウンスを行い，利用者による多要素認証の登録が本格化した．登録作業を進める中で，若干の不具合や利用者の混乱などがあったものの大きな障害なく 10 月 19 日を超えることができた．

対応状況のすべてが把握できているわけではないが，把握できている範囲で下記に記す．

（a）対面での直接対応

名誉教授と学生を中心に，導入前に 17 名，導入後に 18 名，多要素認証設定について対面での直接サポートを行った．11 月以降は，統合認証の多要素については学外者や未登録者のメールサポートに移行していき，直接対応は Microsoft365 の多要素設定対応，およびスマホの機種変更等に伴う再設定対応が中心となっている．12 月には，概ね日に 1～2 件程度の水準まで対応数は減少してきている．

（b）メールや電話での対応

特に 10 月はメール対応も非常に多く，正確には把握できていない．記録に残っている件数から，9 月に 31 名，10 月に 88 名（うち多要素認証適用前が 80 名，適用後が 8 名），11 月が 9 名，12 月以降が 3 名の対応を行った．なお 10 月 19 日以降，統合認証については主に学外者向けにメール認証の代理設定を開始し，119 名の対応を行った．（1/31 まで）

（c）不具合とその対応

設定開始当初，第二要素のワンタイムパスワードが保存可能な状態となっており，パスワードを PC 等に記憶させて利用している利用者から，設定後に第一要素部分でパスワードの入力ミスによりロックが発生する事例が多く報告された．原因を調べたところ，第一要素側のパスワードが，保存されたワンタイムパスワードに置き換わっているためと分かった．そのため，第二要素のワンタイムパスワードを保存しないよう，入力画面を修正した．

（d）今後発生が予想される対応予定

多要素認証については，今後発生しうる事柄とし

て新入生対応が予想されている．非常に多人数の対応が短期間に集中するため，可能な限りの自動化対応を検討している．現状では入学手続き書類に各自判別可能なQRコード等を記載し，そこからメール認証の代理設定に似た手順での登録を想定した準備を進めている．

また非常勤講師等については，人事登録を早めることにより，学期開始前に多要素認証を終わらせ，学期開始すぐの授業にも対応できるよう，各部局に働きかけをしている．

(e) 多要素認証導入による効果

多要素認証導入前は，アカウント情報の窃取事案やメールシステムの不正利用が年数回程度の頻度で発生していた．多要素認証導入後，アカウント情報の窃取やメールシステムの不正利用といった事案は全く発生していない．導入後それほど経過してはいない段階ではあるが，１つの効果として目に見えるものではないかと考えるところである．

(4) 今後の多要素認証の展開について

今回のセキュリティ強化として多要素認証対応したのは，統合認証ログイン画面とMicrosoft365サインインについてだけであり，本学システム利用における認証経路は他にも存在している．またほとんど利用者のいなくなった過去の方法で多要素認証に適さない認証経路などもあるため，不要な認証経路の廃止や多要素認証等の強化セキュリティ適用範囲を拡大してさらなるセキュリティ強化を図り，システムへの不正侵入や不正利用の予防に努めていくことが重要である．

３．まとめ

本稿では，本学におけるセキュリティ強化策として継続的なCSIRT活動と統合認証及びMicrosoft365利用における多要素認証導入について紹介した．情報セキュリティインシデントというものは，どれだけシステム的な防御を行ったとしても，ちょっとした不注意や操作ミスなどにより，ある日突然に誰にでも起こりうることである．本稿で紹介したようなシステム的な防御は，特にハード的な対応は普段利用者側からは意識されにくい部分ではあるが非常に有効に働いていると考えている．今回の多要素認証導入は，利用者の手間は増加するが十分セキュリティ意識を想起させるものであり，セキュリティ意識向上で期待するところは大である．

ソフト的な対応も併せて行っており，教育・研修以外にも，平素から構成員に対して情報セキュリティに関する情報発信を行っているが，過多な情報発信や注意喚起は構成員のストレスになったり，情報を聞き流されてしまったりすることがあるため，これら対応の匙加減が難しいところである．

しかしながら，本学における情報セキュリティインシデントは構成員自身の不注意によるところもあるため，更なる教育・研修の充実化および研修受講の向上を図るとともに，利便性を確保しながらも，情報サービス利用時における多要素認証や不正ログインの検知機能を採用するなど，よりセキュリティ性の高い環境を構築することが必要と思われる．

謝辞

本報告を作成するにあたり，岐阜大学情報セキュリティ最高責任者（CISO） 松原正也教授，情報連携推進本部 村上茂之教授，情報連携課長 佐藤俊介氏をはじめ，多くの方々からご協力とご助言をいただきました．ここに感謝申し上げます．