

東京農工大学における多要素認証導入と運用報告

根本 貴弘¹⁾, 長島 和平¹⁾, 佐藤 亮介¹⁾

1) 東京農工大学 総合情報メディアセンター

nemo@go.tuat.ac.jp

Implementation and Operation of Multi-Factor Authentication at Tokyo University of Agriculture and Technology

Takahiro Nemoto¹⁾, Kazuhei Nagashima¹⁾, Ryosuke Sato¹⁾

1) Information Media Center, Tokyo University of Agriculture and Technology.

概要

東京農工大学（以降、本学）は、2021 年度に学術情報基盤システムの更新を行い、その一環として認証基盤の整備を行い、全学的な多要素認証導入を段階的に行なってきた。認証環境の変化は利用者及びサービス提供部門への負担が大きいことから、本学では、IDaaS を用いた認証基盤の統合とそれに対する多要素認証導入を行うことで、認証セキュリティの強化を目指した。また多要素認証導入では、少人数で全学ユーザのサポートを支援する必要があることから、セルフサポートを支援ことに注力した導入準備を進めた。また、導入後の問い合わせ件数及び内容について調査を行い、多要素認証の導入が運用業務にどの程度影響があったのか評価する。そして、多要素認証の導入によって認証セキュリティの強化が実現できたのか導入後のアカウント不正利用に関するインシデント件数及び認証時の接続元 IP アドレスの調査を通じて考察する。本稿では、2021 年度から取り組んだ全学的な多要素認証導入とそれによる運用業務への影響として問い合わせ状況や導入後の情報セキュリティインシデントについてまとめ、報告を行う。

1 はじめに

近年の情報システムの多様化に伴い、大学においても学外のクラウドサービスの利用が増加している。本学では、2016 年度教育系計算機システム（現：学術情報基盤システム）の更新から、クラウドサービスを含む複数情報システムの利用を念頭に置いた、アカウントの統合管理や情報サービスの利用管理を一元的に行うための申請管理システムを構築し [1]、以降、プライベートクラウドサービスやパブリッククラウドサービスの利用を積極的に行なってきた。

一方で、サイバー攻撃の高度化に伴い、アカウント不正利用に伴う、情報漏洩、改ざん、他組織への攻撃の踏み台化等の脅威が続いている [2]。本学においても、クラウドメールサービスにおけるアカウント不正利用 [3] をきっかけに、全学的な認証セキュリティ強化が急務となった。

本稿では、認証セキュリティ強化として 2021 年度から取り組んだ、IDaaS による認証基盤の統合と多要素認証の必須化の効果と運用業務への影響について報告する。

2 IDaaS を用いた多要素認証の導入

2.1 認証セキュリティ強化に向けた課題

本学では、システム面での認証強化を検討することと並行し、暫定措置として教職員を対象としたパスワードの変更を依頼を全学の周知用メールを用いて実施し、多くのユーザに対応してもらった。しかし、同じ ID とパスワードを外部サービスで使いまわしていた場合、外部サービスのサイバー攻撃被害によりログインに必要な情報が漏洩するリスクがあること、加えて、依頼ベースでは全ユーザのパスワード変更の実現が困難であったことから、パスワード管理に関する教育と注意喚起のみでのセキュリティ確保には限界があると判断した。また、漏洩した際の情報の重要度は個人レベルであるが、その影響が組織レベルに発展するリスクがあることや、ユーザ数が多いため他のリスクと比較して起こりやすいこと等から、改めて本学では各種情報システムにおけるシステム面での認証強化が課題であった。

一方、システム面での認証セキュリティの強化を行う場合、外部サービス利用の拡大に伴う、個々のサー

また、新規ユーザについての支援は、新人職員については、総数が多くないことから通常窓口での対応を行うこととし、新入生については、臨時窓口を授業開始日までに3日開室することで、臨時窓口の運用開始を始めた2022年度以降、授業開始日までに毎年99%以上の新入生が多要素認証を含むアカウント初期設定を完了している[8]。なお、2024年度における新入生

の多要素認証の設定状況も図 4 の通り、99 %以上の学生が設定済みであった。

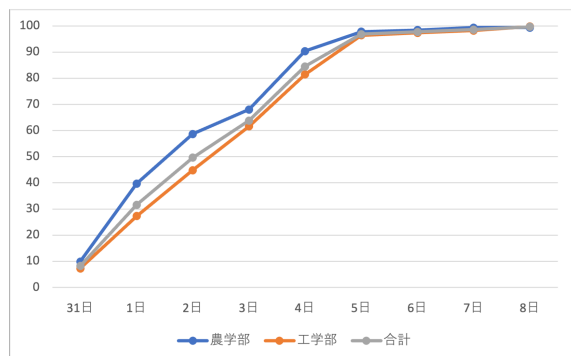


図 4 2024 年度開始時の多要素認証の新規設定者数の推移

なお、Extic で利用可能な多要素認証には、登録されたメールアドレスに送信されるワンタイムパスワード (MOTP) を利用するメール認証、及び、認証アプリに表示されるワンタイムパスワード (TOTP) を利用するアプリ認証があり、本学では、スマートフォンを持たないユーザでも利用可能なメール認証による多要素認証を必須化し、アプリ認証については任意で利用可能としている。メール認証の登録は、アカウント初期設定時に申請管理システムから登録するメールアドレスの登録を行う。この際、登録していたメールアドレスが使用できなくなった際に、メール認証機能を使わずに多要素認証用メールアドレスの設定を変更するために使用するコード番号 (MOTP アドレス変更コード) も併せて登録する。この MOTP アドレス変更コードにより、ユーザが登録していたメールアドレスが使用できなくなった場合にも、ユーザは、窓口にお問い合わせすることなく、専用サイトからユーザは自身で MOTP 用メールアドレスを変更することが可能となっている。Extic の多要素認証機能を用いた、サービス利用時の認証手順は、図 5 に示す通りである。

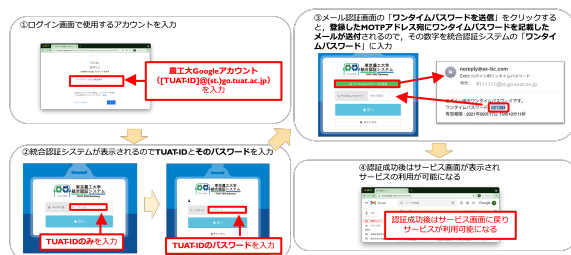


図 5 サービス利用時のメール認証手順例

3 多要素認証導入後の問い合わせとインシデント

3.1 多要素認証導入後の問い合わせ

本センターでは、ユーザからあった問い合わせ記録として、問い合わせ内容の他に、内容に応じたカテゴリ、問い合わせ媒体、対応時間等を問い合わせ対応者が記録している。本節では、2021 年 10 月 13 日から 2024 年 10 月 21 日までに記録された情報を元に、多要素認証の導入が問い合わせ業務にどの程度影響があったかを確認するために、毎月毎の問い合わせ件数の総数と多要素認証に関する問い合わせ件数について調査を行なった。図 6、図 7、図 8、図 9 に毎月毎の問い合わせ件数の総数と多要素認証に関する問い合わせ件数を示す。

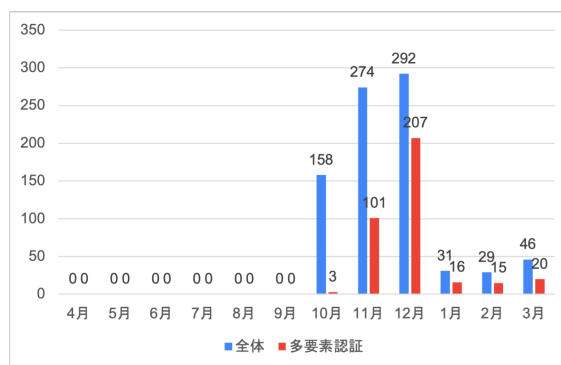


図 6 2021 年度の問い合わせ件数

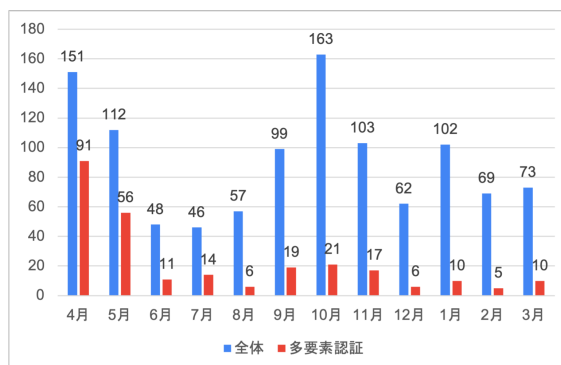


図 7 2022 年度の問い合わせ件数

多要素認証必須化前の 2021 年の 11 月および 12 月、IDaaS とは別に多要素認証の必須化を行なった旧教職員向けメールシステムの多要素認証必須化前の 2022 年の 5 月 [7]、新入生の入学及び新任職員の着任がある 4 月は問い合わせ件数が高い傾向にあるが、それ以外の月においては 1 営業日あたり、1 件以下であった。

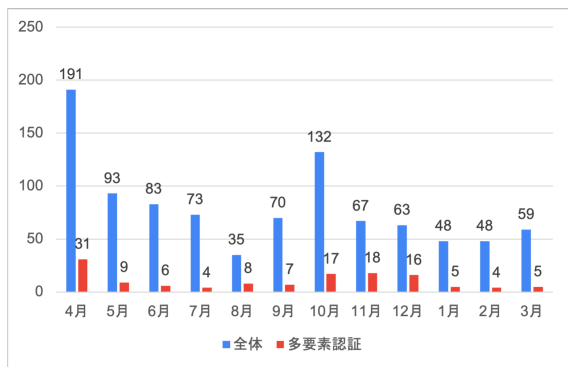


図 8 2023 年度の問い合わせ件数

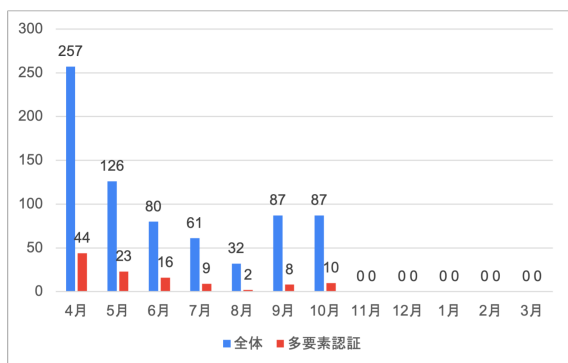


図 9 2024 年度の問い合わせ件数

なお、多要素認証に関する問い合わせには、アカウントの初期設定方法やパスワードの再設定等の多要素認証導入前から存在した問い合わせと重複する内容もあることから、多要素認証導入による実際の問い合わせ件数への影響は、本調査により得た値よりも小さくなると考えられる。

また、主な問い合わせ内容は、以下の通りであり、問い合わせの約 75 %は 15 分以内に対応が問い合わせであった。なお、一般的なパスワード忘れに関する問い合わせは、多要素認証と関係なく、単に設定した PW を忘れに関する問い合わせであるが、多要素認証と関係したパスワード忘れについては、Web ブラウザで自動生成したパスワードを、MOTP アドレス設定時に登録するワンタイムパスワードで上書き保存してしまったという多要素認証導入に伴い、発生した問い合わせもあった。

- アカウント初期設定手順
- パスワード忘れ
- 登録した MOTP アドレスにメールが届かない

3.2 多要素認証導入後のインシデント

多要素認証導入が本学の認証セキュリティ強化に有効であったか確認するために多要素認証必須化後の IDaaS と連携するシステムのアカウント不正利用に関する問い合わせ件数を集計したところ 0 件だった。

しかし、ユーザが不正利用に気づかずに問い合わせを行っていない可能性があることから、本調査では日本国外からの国や地域からのアクセスがないか確認するために、IDaaS の認証ログに記録される接続元 IP アドレスを元に、IPinfo 社の IP Whois API[9] を用いて多要素認証に成功している日本国外の IP アドレス件数についても調査を行なっている。本稿では具体的な具体的な接続元の国や地域及び認証件数の報告は控えるが、本稿執筆時に確認できた、IP アドレスについては、1 日における認証では、いずれの認証も 1 つの IP アドレスから 1 つのアカウントに対する認証をおこなっており、そのアカウントの出現回数は 1 日あたり 1 回から 2 回程度と、学内の IP アドレスから認証に成功しているユーザの認証ログと同様の傾向が伺えることから、日本国外からのアクセスにおいても、国外にいる本学の構成員によるアクセスであることが考察され、多要素認証の導入が本学の認証セキュリティ強化に有効であったこと考察できる。

4 まとめ

本稿では、東京農工大学における多要素認証導入と運用報告として、IDaaS を用いた多要素認証の導入の課題と取り組み、そして導入後の運用業務への影響評価として、多要素認証導入後の問い合わせとインシデントについて報告した。本学では、クラウドサービスの利用を積極的に行なっていることから、複数のクラウドサービスの認証セキュリティ強化を行うために IDaaS による認証基盤の統合を図り、IDaaS の多要素認証機能を利用することで、ユーザ及びサービス提供者の負担を軽減しながら多要素認証の導入を行なった。また、円滑に導入を行うために、本学ではセルフサポートを支援による潜在的な問い合わせ者数の削減と利用者の設定状況を確認しながら、導入計画の見直しを行い大きな混乱なく多要素認証の必須化を実現した。また、多要素認証導入後の問い合わせ件数も、本センターの 1 日の対応可能件数の範囲内であったことに加え、アカウント不正利用によるインシデント件数も 0 件であったことから、多要素認証の導入は概ね成功していることが確認できた。今後は、現在観測されている国外からの多要素認証に成功している IP ア

ドレスは利用者が意図した認証であるかを調査することで、より、今回導入した多要素認証が認証セキュリティの強化に寄与しているかを確認する予定である。

参考文献

- [1] 櫻田, 三島, 石橋, 萩原、運用管理システム「Salut」の概要、研究報告インターネットと運用技術、2016-IOT-35、9、1-6、2016.
- [2] 独立行政法人情報処理推進機構、情報セキュリティ 10 大脅威 2024、<https://www.ipa.go.jp/security/10threats/10threats2024.html>、2024.
- [3] 国立大学法人東京農工大学、個人情報の漏洩及びフィッシングメールの送信について、https://www.tuat.ac.jp/NEWS/info/20200205_01.html、2020.
- [4] EXGEN NETWORKS、Extic、<https://www.exgen.co.jp/extic/>、2024.
- [5] 三島, 根本, 青山、統合認証基盤としての IDaaS 導入と初期運用、研究報告インターネットと運用技術、2022-IOT-58、10、1-6、2022.
- [6] Takahiro Nemoto, Kazuhiro Mishima, Shigeyoshi Aoyama、Implementation and Initial Operation of IDaaS as Integrated Authentication Infrastructure in TUAT、Proceedings of the 2023 ACM SIGUCCS Annual Conference March 2023、SIGUCCS '23、5、48–52、2023.
- [7] 根本, 三島, 石橋, 長島, 青山、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、研究報告インターネットと運用技術、2022-IOT-58、12、1-5、2022.
- [8] 根本, 三島, 長島, 青山、多要素認証必須化による新年度業務への影響評価、大学 ICT 推進協議会、2023 年度次大会 論文集、12、306-312、2023.
- [9] IPinfo、IP Whois API、<https://ipinfo.io/products/whois-api>、2024.