全学セキュリティ教育のクラウド認証基盤での実現

玉造 潤史 [1)], 杉山 洋子 [2)], 今田 哲也 [2)], 田川 善教 [2)], 松岡 喜美代 [2)]

1) 東京大学情報システム本部
2) 東京大学情報システム部情報環境課

tamatsukuri.junji@mail.u-tokyo.ac.jp
jouhou-security.adm@gs.mail.u-tokyo.ac.jp

University Security Education on Cloud Authentication platform

Junji Tamatsukuri [1)], Yoko Sugiyama [2)], Tetsuya Imada[2)]
Yoshinori Tagawa[2)], Kimiyo Matsuoka [2)]

1) Division for Information and Communication Systems, the University of Tokyo.
2) Information Systems Department, Information Environment Group, the University of Tokyo.

概要

東京大学では情報システムを利用する全構成員に対して毎年必須の情報セキュリティ教育を実施している。全構成員に対して研修やテストを実施するには専用の研修用プラットフォームが必要であったり、大規模な受講管理が必要であったりと困難点が多い。特に本学では、情報セキュリティ教育の未受講者に対してサービス利用を停止するという措置を実施しており、効率的な運営のためには情報セキュリティ教育の受講とサービス運用を連携させて実施する方法が不可欠であった。しかし、認証基盤としてクラウドサービス Microsoft AzureAD(Entra ID)を利用しているため、ローコード実装により大学が契約する包括ライセンスの範疇でこれらの要件を満たす機能を実現できることが分かった。そして 2023 年度から予算をかけずにアカウント全利用者に対して情報セキュリティ教育を実施できるようになった。本稿ではその実施方法と成果について示す。

1 はじめに

東京大学では全学の情報システム利用者を対象に適切な情報システム利用と安全性確保を目的として「情報セキュリティ教育」という研修を実施している。大学の学生・教職員からなる全構成員に対して情報システムを統合的に利用することができる 「UTokyo Account」を発行しており、その運用規程ですべてのアカウント利用者がセキュリティ研修を受講することが定められている。すなわち、本学の「情報セキュリティ教育」は全学的なアカウント「UTokyo Account」に紐づいて管理されている構成員に対して、情報システム利用によって生じる可能性のある情報セキュリティインシデント事案を未然に防ぐことを目的に、セキュリティに関する現状と対応策を確認するために行う研修となっている。

「情報セキュリティ教育」の実施方法として、これまでもアカウント利用と研修の受講状態が対応付く、すなわち、「情報セキュリティ教育」を受講しなければアカウントが利用できない形での研修実施が求められてきた。アカウント利用者が必ず受講しなければならないということを「システムが利用できないこと」で認識できれば、受講が必須であることを認識でき、システム利用におけるセキュリティに対する認識の必要性を理解することができるであろうという考え方に基づいた方針である。

このような方針は非常にシンプルである一方、実現方法を考えた場合、アカウントを管理する認証基盤と密に連携した研修機能が必要となり、受講と受講後のアカウント制御を実現するためにある程度のシステム開発工数が必要となる。しかし、このような特定の研修活動のために専

用のシステムを用意するコストは相対的に非常に高くなる。そのため、2022 年度までの情報セキュリティ教育では研修機能については授業管理システムである 「ITC-LMS」を利用し、「UTokyo Account」本体と直接連携はせず実施管理を行なってきた。サービスの停止措置にはそれぞれのサービス担当に受講情報を提供し運用的な対応（手動でアカウント停止を実施）することで対応してきた。そうすることで、アカウントでのサービス利用と研修受講の関係を作り、利用者に提供し実施してきた。

この方法は既存システムの活用により特別なコストを必要とせず実施できた。一方、サービス運用担当者の負担と、なによりアカウント利用者の受講負担（未受講の場合の停止ペナルティは１ヶ月単位であった）など運営上の問題があった。

2020 年からのコロナ禍対応で大学全体のデジタル化と連携するサービスの利用が進み「UTokyo Account」の重要性が改めて高まった。合わせて認証基盤や導入した情報サービスへの理解も深まり、情報システムの活用が進んだ。特に、学内で実施されているコンプライアンス研修等で導入済みの包括ライセンスにより利用できる Microsoft Forms を用いて実施されるものが散見されるようになった。Microsoft Forms はアンケートなどを実施するクラウドサービスであるが、工夫すると研修など回答者の理解を確認するようなコンテンツを作ることができる。そうした工夫を学内利用者が多数行なった結果 Microsoft Forms を利用する研修が学内で違和感ないものとなってきた。結果として、これまで我々が認証基盤の改修や受講方法を必要だと考えていた研修の受講とアカウント利用の関連付けが既存のライセンス契約により利用できるソフトウェアの既存機能の活用だけで概ね実現できるのではないかと考えるに至った。

既に大学における情報セキュリティ教育の実施は一般的であり、学生においては実施が当たり前の状況である。[2][3] しかし、現状において大規模な大学機関において全構成員に対してセキュリティ教育が困難な事業であることに変わりはない。

これらの状況を踏まえ、本稿では東京大学で行われている「情報セキュリティ教育」研修をコストのかかる特別なシステム改修を行わず実現した方法とその結果を示す。

なお、「情報セキュリティ教育」の成果の本質はセキュリティ事案の抑止と利用者のセキュリティへの認識の確保である。これらの源泉は情報理工学研究科情報セキュリティ教育センターと協力して作り上げたコンテンツである。その内容、教育成果も重要な観点であるがこれらについては別の機会での報告とさせていただきたい。

以下、本稿ではこれまでの取り組みについて紹介した後、実装方法と教育の実施方法を示し、実施結果についてまとめる。

2　これまでの取り組み

本学では学内でのセキュリティインシデントの増加を受け、2017 年度から情報セキュリティ教育を開始することとした。開始に向け当初より学内で授業管理に提供されている「ITC-LMS」を想定し、研修受講のためのプラットフォームとして利用できるよう情報基盤センターに協力を依頼した。元来、ITC―LMS では授業を実施に必要な教職員と学生がどちらも利用できるようアカウントが設定されており、情報セキュリティ教育の対象者である UTokyo Account の全利用者がサインインすることができた。ITC-LMS にはクラスという概念があり、受講者をそのクラスに割り当てることで教育を実施できた。クラス人数の上限が 5000 人だったため、受講者を所属する（管理する）部局ごとに割り当てることとし、全体で約 20 クラスほどのクラスを作成して実施してきた。

例として 2021 年度は、学生は 5 月から 6 月に

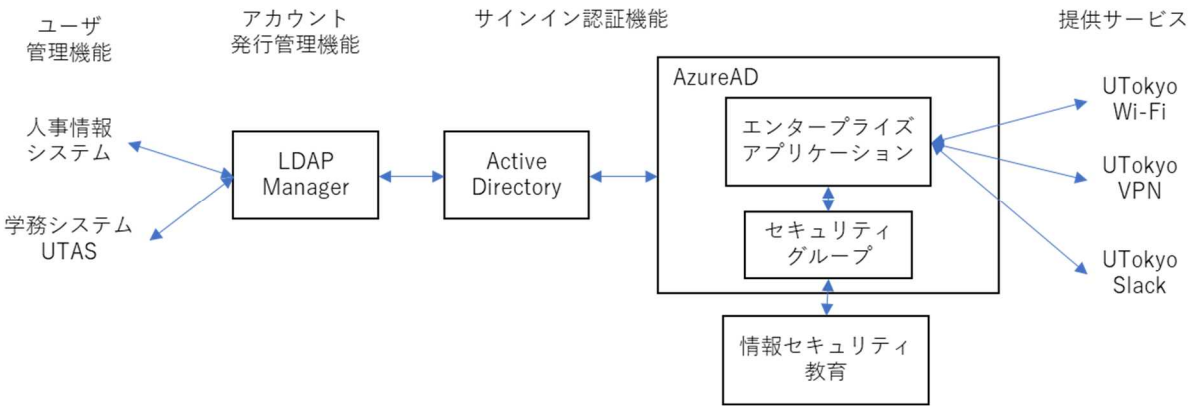

図 1　認証基盤の構成

実施し、教職員は 7 月から 8 月に実施し、10 月から半年間未受講者のサービスアカウントを停止するという形で運営された。

当初より情報セキュリティ教育を受講しないと利用を停止するサービスが設定されており、2022 年度においては学内 Wi-Fi である UTokyo Wi-Fi および VPN サービスである UTokyo VPN である。停止するサービス側では、未受講者のアカウントのサインイン禁止設定を追加することで利用不能とし、追加で受講した利用者の情報は毎月禁止設定を解除するという形で運用実装した。

適時改善を行いながら実施してきたが、いくつかの問題点があった。

1. 実施時期を定める必要があり、年度途中からの対象者（秋入学や中途雇用者、休学者、休職者）への実施が難しかった。
2. 利用を停止するサービスの運用負担が大きく連携頻度を上げることが難しかった。

そしてなによりも、本来セキュリティ教育はアカウント利用開始時に行われるべきものであるが、本方式ではアカウントの利用開始後の受講となるため、実質的な効果が薄いと思われた。そのため、持続的なセキュリティ教育活動として定着させることはできたが実施方法の検討を続ける必要が依然としてあった。

3 新たな情報セキュリティ教育の実装

これらの問題点への対応として考えたのが 2023 年度の情報セキュリティ教育の実施方法である。ここではその実装について説明する。

本学の認証基盤は利用者情報を集め、管理する人事システムと学務システムから連携されたアカウント情報を管理する LDAP Manager と認証自体を行う Active Directory および AzureAD(EntraID)の連携で構成されたハイブリッドな認証基盤である[1]（図 1）。アカウントの発行と情報セキュリティ教育の受講状態を連携することを考えると直接的には LDAP Manager への機能改修が必須となる。本学が 2021 年に行なった多要素認証機能の導入では、多要素認証の制御は LDAP Manager の機能改修で実装した。しかし、多要素認証を必須とするサービスの制御の大部分は AzureAD が持つ条件付きアクセス機能への設定を管理者が自ら行った。この経験から LDAP Manager と連携する機能はアカウントの発行管理と密に結合した機能として実現できるが、サービスの利用制御とだけ連携することができればよい機能であれば、AzureAD の機能を管理者が用いることだけで十分実現できることが運用上の知見として分かった。

さらに、在宅勤務の定着で研修活動も多くがオンラインとなり学内の DX 活動も盛んとなった。

そして前述した通り、いくつかの研修活動が Microsoft Forms を工夫して利用して行われ始めた。それらの多くは Microsoft Forms の機能を活用した研修コンテンツで非常に精緻なものであった。同様の活用ができれば情報セキュリティ教育を実施するのに十分な研修クオリティを実現できるものであると考えられた。そして、採点およびアカウント制御については Microsoft PowerAutomate（内部で、AzureAD にアクセスするコネクタを利用）を用いることで、Microsoft Forms で作った情報セキュリティ教育コンテンツとその受講状況を判定し合格者を AzureAD に登録し、サービス管理に連携して実装することとした。AzureAD 内部では、情報セキュリティ教育合格者をメンバーとするセキュリティグループを年度ごとに作成している。そのセキュリティグループを制御するアプリケーション（本学では UTokyo Wi-Fi, UTokyo VPN, UTokyo Slack）のユーザとして登録する。こうすることで、毎年必須の研修に対して対応することができるようにした。

この方法は、全学契約の包括ライセンスで利用できる Microsoft365 の機能だけで UTokyo Account の全利用者が研修を受講でき、利用するに提供するサービスと研修の受講状態を連携できる。結果として、全学研修をアカウントと連携させながらシステム改修における費用を全く生じさせなかった。

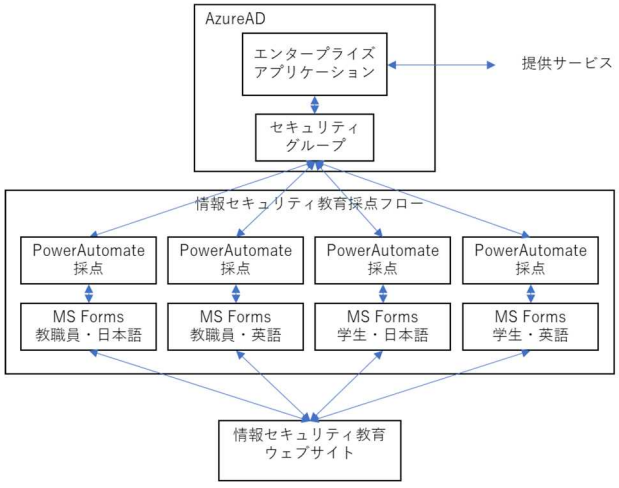

図 2　情報セキュリティ教育実施機能

図 2 に設定した連携のイメージを示す。実際の設定方法は PowerAutomate が利用できるものである管理者であれば、誰でも設定可能な平易なものである。

セキュリティ教育の実施管理を担当する情報環境課において、Microsoft Forms で研修コンテンツを作成した。ここで工夫したのは、利用者に受講結果が少しでも分かりやすいように「クイズ機能」を利用したことである。クイズ機能では受講後に正解を採点して示すことができる。しかし、クイズ機能には、多言語に対応していないという機能的な不備もあり、情報セキュリティ教育では対象者である教職員と学生にそれぞれ異なる研修内容を実施することしている。そのため、実施言語として日本語および英語を設定したことで、フロントエンドとなる Microsoft Forms は計 4 個作成することとなった。作成した Forms の画面を図 3 に示す。

受講者が Microsoft Forms で回答を送出すると PowerAutomate が受け取り、採点を実施し、身分を判断した上で AzureAD にあるセキュリティグループに追加する。

受講者は、MS Forms の最後の画面で採点結果を確認できるが、加えて合格者のセキュリティグループだけにアクセス権を付与した Sharepoint サイトを作成し合格判定サイトとして提供した。

図 3 情報セキュリティ教育の画面

利用停止措置は直接認証連携しているサービス

では、利用権が合格者グループそのものに付与されるので、サービス側ですることはない。UTokyo Wi-Fi では、アカウントコントロールのため、認証アプライアンスを利用して Wi-Fi 用のアカウントを発行している。そのため、利用停止措置を行う際には合格者ではないアカウントを削除する必要がある。また、Slack のようにクライアントが一定期間認証状態を保持してしまうサービスにおいてもサインアウトを強制し、再認証を求めるようにする必要がある。さらに、これまでは ITC-LMS に受講者の登録をあらかじめ行う必要があった。しかし、この方法では、認証基盤と直接連携しており、Microsoft Forms にアクセス可能な利用者、すなわち、すべての UTokyo Account 利用者を自動的に受講対象者とすることができる。結果として、これまで受講対象とできていなかった、受講開始後に在籍開始となった利用者や復帰した利用者すべてに受講を必須とすることができた。

現在、新たに本学に在籍する構成員は UTokyo Account を受け取った後、情報セキュリティ教育を受講しないと Wi-Fi, VPN などのサービスは利用できない。こうして全構成員必須の講習として情報セキュリティ教育を実現した。

これらの機能実装については、2022 年度中に簡単な検証を行い、実現性を確認したのち、2023 年度に入って実施準備をし、全体としては概ね 3 ヶ月で実施準備を行なった。

4 情報セキュリティ教育実施結果

このようにして準備した情報セキュリティ教育は 2023 年 7 月 5 日から 8 月 7 日までの約 1 ヶ月を受講期間として実施した。8 月 8 日に受講者データの検証を行い、8 月 9 日より各システムにおける利用停止措置を実施した。

システム	対象者数	停止者数	受講率
全体	55627	-	65.1%
UTokyo Wi-Fi	37783	8978	76.2%
UTokyo Slack	13844	4340	68.7%

表 1 情報セキュリティ教育の受講者数とサービス停止数

情報セキュリティ教育の未受講または不合格によりサービスでアカウント削除または停止となった UTokyo Account 利用者は表 1 のとおりである。受講期間中での受講率は概ね 65%であり相応する未受講者のサービスの利用停止措置を実施した。明確に利用者数が分かる UTokyo Wi-Fi でのアカウント発行数は 9 月中に研修開始前と同様の 40000 人を超えており、その人数が情報セキュリティ教育を受講済みであることが分かる。

情報セキュリティ教育の実施開始前に、2 回学内に周知を行い、実施結果を集計して、定期的に各部局ごとの受講率を Sharepoint サイトに掲載した。これらによって受講促進を行った。

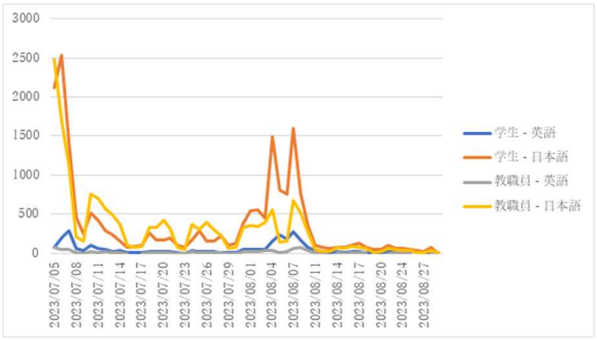

図 4 情報セキュリティ教育の受講状況

情報セキュリティ教育の受講状況を示したグラフが図 4 である。7 月 5 日の開始直後に多くの受講者が受講し、その後週ごとに同じような受講状況を繰り返していることがわかる。これは、学内で定期的にアナウンス等が繰り返されているためである。学生向けにはアカウント停止に

より教育を受ける機会を失うことにつながることから学務システムUTASで全学生へのメール通知を教育開始時と終了前とに実施した。そのため、受講期限である8月7日前に駆け込みでの受講が大きくあった。受講期限である8月9日以降にサービス停止により未受講に気づいた利用者の受講が若干あり、その後は1日あたり数名から 10 名程度の未受講者の受講が続いている状況にある。

受講期限以降に利用を開始するユーザに対しては、新規構成員向けにutelecon サイト上で提供している「大学生活に必要な情報システムの準備について（新入生向け）」と「東京大学の情報システムの準備について（教員向け）」の開始手順においてアカウントの新規利用時の設定手順に、情報セキュリティ教育の受講を織り込んでいる。その手順に従い、おそらく後期授業が始まる前に若干の増加が見込まれるが新規利用者も受講すればすぐに各サービスを利用できるので、速やかに受講いただけるものと考える。

5 実施評価

情報セキュリティ教育を認証基盤と連携して実施した結果についてまとめる。

情報サービス利用者全員が受講するしくみとなっているため制御対象である UTokyo Wi-Fi, UTokyo VPN, UTokyo Slack を利用するネットワークセキュリティへの認識が必要な者の受講率は100%である。

一方で情報システム利用者へのサポートへの負担は大きくなっている。具体的にはutelecon サイトで提供しているユーザサポート窓口[5] には情報セキュリティ教育の受講を知らず、Wi-Fiが利用できない、VPN が利用できないといった状況で問い合わせをしてくる利用者が受講期限以降、ずっと来続けている。

これには、いくつか理由があると考えられる。まず、一つには、大学情報システムの利用意識が低い所属関係、具体的には附属病院の医療職員、共同研究などでの関係者、名誉教授などの構成員に対しては、大学本部からの周知や各部局での周知が届きづらく、UTokyo Account を利用しながらも情報セキュリティ教育の実施情報自体も届かない、あるいは届いても認識できていないという状況がある。これはサービス利用時になんらかの表示を行うような対応ができればよいが、今回のように定型化されたクラウドサービスを活用した方法では困難であり、せっかくの有益性を失わせてしまうことになる。

また、もう一つの理由として、情報リテラシー全般において言えることであるが、情報セキュリティの常識的な内容を問うような平易な研修では、その平易さのためか用意されているコンテンツや指示の全てを読むことをせず、正しく理解できないために受講を完了できないといった状況を生じる者が多くでてしまうことである。これらの問題については、技術的な対応での改善よりも、情報セキュリティ教育の実施自体を定着させ、毎年確実に実施することが情報システム利用において必須であるという認識を作ることが有効であるように思われる。

現行の方法として利用している Microsoft Forms の機能は未だ完成しておらず、今回の研修準備中にも少なからぬ改善が図られている。そのため、今回の研修受講においてはクラウドサービス特有のカスタマイズできない機能上の穴については、ドキュメント等で説明を補い受講しやすくなるような対応を行なっている。しかし、それらを読むことなく、うまく受講できず、機能改善（特に、Microsoft Forms の終了画面での結果表示があまりうまくできていないことに起因する意見）を求める声は大きい。当然、機能的に改善すべきものは要望していくことを考えている。しかし、クラウドサービスの活用によって、特別な費用を一切生じることなく全構成員に対して提供できており、そのための制約であることがユーザに理解されることがDX というものの一部であると思われる。今後

の実施において考慮していきたい。

5 まとめ

本稿では、本学で実施した情報セキュリティ教育の認証基盤との連携による費用をかけない効率的な実現方法について紹介した。今回紹介した方式での情報セキュリティ教育はまだ始めたばかりで多くの改善点があると思われる。受講結果（特に不合格であった場合）を受講者に的確に提示することは必要な機能であると思われる。認証基盤への機能追加による改善ではせっかくのローコスト手法での効果がうすくなってしまうので、クラウドサービスを活用した DX 的な対応方法を考えていきたいと考える。

先にも述べたが、デジタル化によって全学的な認証基盤である UTokyo Account と連携した機能を活用したオンラインでの研修が増加している状況にある。我々が情報セキュリティ教育を実施した後にも全学構成員を対象としたコンプライアンス研修や調査が 3 種類も実施された。当然のことながら受講者からはこれらの研修受講状況を分かりやすく提示することが求められ始めている。

そういった大学全体の研修活動への対応としても、本件で活用したようなクラウドサービス機能は有効であるため、さらにクラウド認証基盤を活用して受講管理ができるような方向での対応を検討中である。

大学のような学生、共同研究者など多くの構成員がコラボレーションするインフラとして情報システムは必須であり、コロナ禍によってさらに拡大したオンライン化によってさらに不可欠なものとなった。そうしたことで情報システムを利用するもののセキュリティ教育の重要性もまた高くなっている。その重要性を鑑みて今後も工夫と改善を続けていきたい。

謝辞

情報セキュリティ教育の実施に当たっては情報システム部、情報システム本部の諸氏には多くの協力を頂きました。特にサービス停止措置では情報システム本部野口昌志氏、竹内朗氏には対応いただきました。また、適切な受講に向けてユーザサポートでの多大な協力をしていただいているサポート窓口のコモンサポーターの皆さんには敬意を表します。

参考文献

[1] 中村　誠、東京大学における認証基盤の取り組み、NII 学術情報基盤オープンフォーラム 2023、https://www.nii.ac.jp/openforum/2023/day2_auth1.html

[2] 符　儒徳, 情報セキュリティ教育の現状と大学の課題, 開智国際大学紀要 第 19 号（2020）
https://doi.org/10.24581/kaichi.19.0_121

[3] 中西　貴裕, 川村　暁, 尾中　夏美, 松岡　洋子, 岩手大学における留学生向け情報セキュリティ教育と他組織との教材の共有, AXIES 2019, SF1-3

[4] 竹内　朗, 玉造　潤史, 学生・教職員の協働によるワンストップの ICT サポート窓口運営の実践, AXIES2022, 13PM2C-5.pdf