

多要素認証システムの機能移行事例に基づく クラウドサービス仕様変更による不具合発生リスク抑制の考察

大野 真伯¹⁾, 竹原 一駿¹⁾, 後藤田 中¹⁾, 亀井 仁志¹⁾

1) 香川大学 情報メディアセンター

ono.masanori@kagawa-u.ac.jp

A Study of Failure Risk Reduction by Changes of Cloud Service Specifications based on MFA Function Replacement

Masanao Ono¹⁾, Ichitoshi Takehara¹⁾, Naka Gotoda¹⁾, Hitoshi Kamei¹⁾

1) Kagawa University, Information Technology and Media Center

概要

香川大学では、2021年度よりクラウドサービスを活用した多要素認証システムの全学導入を進めている。2023年度には、本学構成員の導入割合が9割を超えた。本稿は、クラウドベンダーによるサービスの更新に伴う多要素認証システムの機能移行時に発生したトラブルの詳細を報告し、得られた知見からクラウドサービス仕様変更による不具合発生リスク抑制について考察する。

1 はじめに

香川大学情報メディアセンター（以下、センター）は、2021年度から多要素認証システムとしてMicrosoft社のクラウドサービスである「Microsoft Entra 多要素認証」（以下、ME-MFA）を導入している。同社は、2023年の11月から12月にかけて、ME-MFAに「Microsoft マネージド条件付きアクセスポリシー」機能（以下、「条件付きアクセスポリシー」）を導入し、従来機能である「ユーザーごとのMFA」を非推奨とした[1]。

センターは、Microsoft社の方針変更にあわせて、2024年3月に「条件付きアクセスポリシー」へ機能を移行し、従来運用において問題となっていたユーザーアカウント新規登録時のME-MFA初期値有効化を図る事とした。しかし、機能仕様に差があり、特定条件下において機能移行が困難となった。本稿は、機能移行時に発生したトラブルについて報告し、得られた知見から、クラウドサービス仕様変更による不具合発生リスク抑制について考察する。

2 多要素認証システム

センターで導入している多要素認証システムの環境について述べる。

2.1 導入経緯

多要素認証システムとは、サインインプロセスの保護が目的である。一般に、IDとパスワードによる単一認証によるアクセスに加えて、スマートフォン認証や指紋認証といった異なる2つ以上の認証方法を組み合わせる本人確認を行う仕組みを提供する。センターは、本学の構成員に向けて導入しているMS365のユーザーアカウントに対し、多要素認証システムを導入した。

本学は、Microsoft社とEES包括ライセンス契約(Enrollment for Education Solutions)を結んでおり、サブスクリプションにME-MFAが含まれる。多要素認証システムの導入にあたり、追加費用無しに利用でき、MS365と容易にシステム連携可能な、高い費用対効果を望めるME-MFAを選定した。ME-MFAの認証方法では、第三者の成りすましに直ぐに気付け、移動先での承認が容易なスマートフォンでの運用を前提とし、専用の認証用アプリであるMicrosoft Authenticatorの使用を推奨した。

2.2 段階的導入と導入目標達成率

センターでは、本学の構成員およそ1万人に対し、2027年度までの多要素認証システム導入率95%を目標とした(図1)。

多要素認証システムの導入は、段階を踏むように、職員530名を対象としてスモールスタートした。その後、学生、教員へと対象範囲を広げた。

対象/年度	2021	2022	2023	2024	2025	2026	2027
職員	530	253	783				
学生		1,410	6,290				
教員			1,961				
その他							
合計	530	1,663	9,034				
目標達成率	-	17%	38%	58%	78%	95%	95%
導入達成率	4.4%	18.4%	91.5%				

※多要素認証導入目標対象者数(2023年3月時点): 9,872
 ※セキュリティ強化のため、2023年度に計画を見直し、
 前倒しでの学生・教職員全ての登録を目標とした。

図1 多要素認証システム導入計画概要

その結果、2023年度には90%を超える導入率を達成した。この結果から、目標を達成できる見込みである。

3 「条件付きアクセスポリシー」導入

「条件付きアクセスポリシー」を導入する上で検討した内容と成果を述べる。

3.1 従来の運用における問題

「条件付きアクセスポリシー」を導入する前の運用(以下、従来運用)では、ユーザーアカウントごとにME-MFAを有効、無効とする機能である「ユーザーごとのMFA」を用いていた(図2)。有効とは、MS365に初回サインインする際にME-MFAの設定を強制的にユーザーに求める設定を指す。無効とは、ME-MFAから設定及び認証を求められない設定を指し、本学運用における初期値となる。

従来運用において、この操作は専任のシステム担当者が都度手動で行っていた。そのため、中途採用など、イレギュラーなユーザーアカウントの新規登録時にME-MFAを有効とする操作の漏れが



図2 「ユーザーごとのMFA」画面

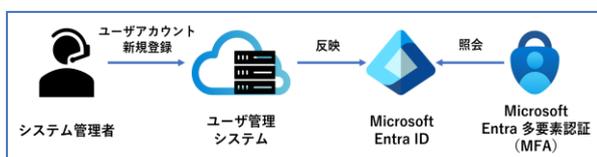


図3 ユーザーアカウント登録環境

発生する原因となっていた。この操作の漏れが発生しないこと、また漏れが発生してもセキュリティが保たれることを目的とし、ME-MFAの初期値を有効とする改善要望が挙げられていた。

一方で、本学のユーザーアカウントの登録が、ME-MFAが照会するMicrosoft Entra IDではなく、別のユーザー管理システムからであり、ME-MFAの初期値を有効とするためには、このユーザー管理システムのデータ連携に関わる修正を要した(図3)。

3.2 機能移行による対応と課題

Microsoft社は「Secure Future Initiative」の一環として、2023年11月に「条件付きアクセスポリシー」を発表し、サービス利用のテナントに対し、積極的な導入を促した[2]。「条件付きアクセスポリシー」は、Microsoft Entra IDの機能であり、ME-MFAのテナント一括制御が可能となる(図4)(図5)。従来運用で用いていたユーザーアカウント単位にME-MFAを設定する「ユーザーごとのMFA」は非推奨となった[1]。

3.1節に述べた問題改善のために、センターは

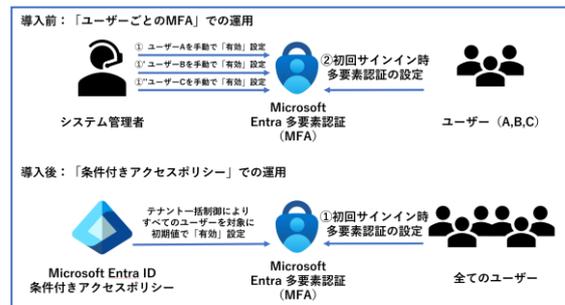


図4 「条件付きアクセスポリシー」の導入前と導入後の運用



図5 「条件付きアクセスポリシー」画面

「条件付きアクセスポリシー」を導入した。これにより、初期値設定が Microsoft Entra ID 側で制御可能となり、ユーザー管理システムの修正を行わずに対応できる。

今回、「条件付きアクセスポリシー」の導入初期の運用において、「アプリパスワード」が消失するというトラブルが発生した。従って、ME-MFA の機能移行において、本トラブルの解決が課題となる。

4 「アプリパスワード」の消失

「条件付きアクセスポリシー」の導入で発生したトラブルと対策について述べる。

4.1 「アプリパスワード」の利用

ME-MFA の仕様として、一部の古い非ブラウザアプリにおいて、認証プロセスの一時停止や中断が発生する。このような非ブラウザアプリに対し、安全な方法で動作させる ME-MFA の認証方法として「アプリパスワード」がある[3]。「アプリパスワード」は、「条件付きアクセスポリシー」には無い「ユーザーごとの MFA」特有の認証方法である。

「アプリパスワード」を使用できる状態で「条件付きアクセスポリシー」を適用した場合のみ、「アプリパスワード」を継続使用できる条件がある。一方、「ユーザーごとの MFA」を途中で無効とした場合、「アプリパスワード」は消失し、認証

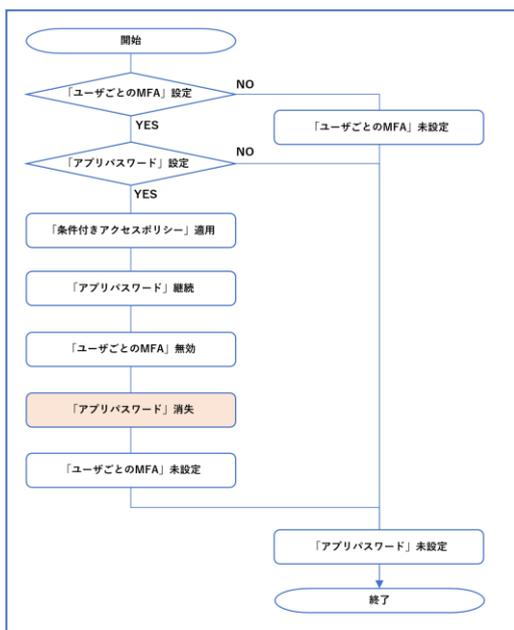


図6 「アプリパスワード」消失フロー

方法として使用できなくなる。この仕様を事前の調査と検証で確認できず、「アプリパスワード」が消失する。上記のフローを図6に示す。

4.2 トラブルの詳細

およそ1カ月の事前評価期間を経て、2024年3月に「条件付きアクセスポリシー」の運用を開始した。4月に、繁忙期となる新入生及び入職者対応を控えていたことから、問い合わせ業務の負荷軽減を目的に、既存ユーザーアカウントの「ユーザーごとの MFA」を無効とした。今回実施の機能移行では、評価期間中のトラブル対策として切り戻し用に「ユーザーごとの MFA」の設定を残していた。スマートフォン故障時の対応を例に、ME-MFA を無効とする場合は、「条件付きアクセスポリシー」から除外する操作となる。しかし、切り戻しの設定が残る間は、「条件付きアクセスポリシー」の除外操作により回帰する「ユーザーごとの MFA」を無効とする追加の操作が必要となっていた(図7)。

この無効の操作直後から、センターの問い合わせ窓口でメールの受信が出来なくなったという連絡が入った。問い合わせ窓口からのエスカレーションを受け調査した結果、認証エラーによるものであり、使用のメールソフトが古い非ブラウザアプリに限られていたことから「アプリパスワード」に絡む内容と推察された。結果として「ユーザーごとの MFA」を無効としたことが原因であり、「アプリパスワード」が認証方法から消失していたことが判明した(図8)。



図7 スマートフォン故障時の対応



図8 「アプリパスワード」消失の挙動

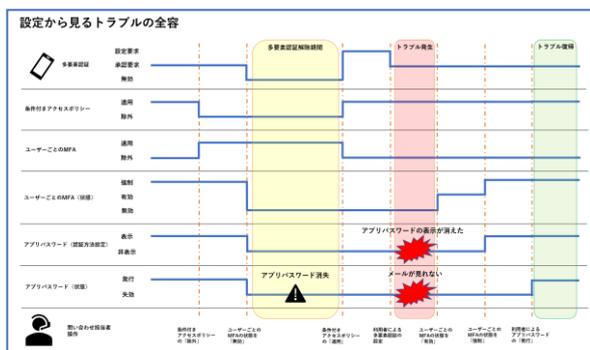


図9 設定から見るトラブルの全容

Microsoft 社の問い合わせ窓口にて「アプリパスワード」の復帰方法等を問い合わせたが、公開情報や事例は無く、困難であるとの連絡を受けた。

4.3 トラブルの対応

「アプリパスワード」は、一部の非ブラウザアプリにおいて、ME-MFA の認証プロセスを安全な方法で動作させる仕組みとして機能提供されている。しかし、センターは、そのようなアプリの利用を推奨しておらず、本学が推奨とする OWA (Outlook on the Web) への移行契機と捉え、問い合わせのあったユーザーに対し、OWA へ移行するよう協力を要請した。ただし、ユーザーによる移行が難しいと判断したものについては「ユーザーごとの MFA」を有効に戻し、「アプリパスワード」の再登録を依頼した (図 9)。

センターでは、2020 年から 2022 年にかけて、全学メールを Microsoft Exchange に移行させていた。さらに、非ブラウザアプリを提供していたベンダー各社が、「アプリパスワード」を必要としない認証プロトコル「OAuth 2.0」の適用を進めており、メールソフトの更新によって解決することもあった。対応の結果、「アプリパスワード」の再登録を要したのは 2 名のみであった。

4.4 考察

サービス品質の向上のために、クラウドサービスは頻りにアップデートされる。その内容、規模により、サービスの仕様が変更されることがある。また、クラウドサービスの情報は、Web サイトなどで多数公開されており、適宜アップデートされる。

今回は、多要素認証システムの機能移行に関する仕様変更の公開情報に追従できず問題が発生した。従って、仕様変更の有無を確認する情報収集体制の構築が必要と考えられる。

さらに、互換性を維持するために、クラウドサ

ービスは変更前の機能を停止しないことがある。

今回は、変更前の一部の機能が引き継がれたため、公開された仕様変更情報だけでは、機能引継ぎの仕様に追従できなかった。この問題を避けるには、仕様変更前のテストによる実際の変更仕様の洗い出しが必要である。

クラウドを用いた情報システムの管理者は、クラウドサービスの機能追加や仕様変更に対しては総務省からも示される通り[4]、定期的ではなく特別に注意してチェック及び対応を行うように努め、仕様変更によるシステムの不具合が発生するリスクを抑えるように備えておくことが求められる。

5 まとめ

本稿は、クラウドサービス仕様変更によるトラブル事例を挙げ、不具合発生リスクを抑えるために、システム管理者に求められることを考察した。

今回、多要素認証システム ME-MFA の機能移行時に発生したトラブルから、クラウドサービスの情報は常に更新されていくことを示した。クラウドを用いた情報システムの管理者は、仕様変更による不具合発生リスクを抑えるために、仕様情報の収集に努めるなど、日々研鑽が必要である。

参考文献

- [1] Japan Azure Identity Support Blog, Microsoft マネージド条件付きアクセス ポリシー, <https://jpazureid.github.io/blog/azure-active-directory/microsoft-managed-conditional-access-policies/>, (2024.10.1 参照)
- [2] Japan Azure Identity Support Blog, 今すぐご対応を: Microsoft マネージド条件付きアクセス ポリシーを有効化またはカスタマイズする, <https://jpazureid.github.io/blog/azure-active-directory/microsoft-managed-conditional-access-policies/>, (2024.10.1 参照)
- [3] Microsoft Learn, レガシ アプリケーションでアプリ パスワードを使用して Microsoft Entra 多要素認証を適用する, <https://learn.microsoft.com/ja-jp/entra/identity/authentication/howto-mfa-app-passwords>, (2024.10.1 参照)
- [4] 総務省, クラウドサービス利用・提供における適切な設定のためのガイドライン (2022.10), p.53, https://www.soumu.go.jp/main_content/000843318.pdf, (2024.10.21 参照)