Vol.2019-CSEC-85 No.5
Vol.2019-IOT-45 No.5
2019/5/23

個人情報保護と情報セキュリティを考慮した Office 365 Educationの環境構築方法

嶋吉 隆夫[1,a)]　笠原 義晃[1]　藤村 直美[1]

概要：教育機関向けに Microsoft はクラウドアプリケーションスイートの Office 365 Education を提供しており，その基本機能を含んだ Office 365 A1 プランは無償で利用できる．しかし，A1 プランを用いた標準的な Office 365 の構成ではパスワードスプレー攻撃への十分な対策が難しいという問題点がある．また，Office 365 の既定の設定では，個人情報，管理情報を含む組織の全ユーザ情報を一般ユーザが入手可能であり，アカウント不正利用の場合に個人情報漏洩の危険性がある．そこで本稿では，まず，パスワード攻撃への対策を有料プランを用いず安価に実現する手法として，認証フェデレーションを用いたシステム構成を提案し，Office 365 へのサインインに用いる ID を他者に開示する必要がないようにすることでパスワード攻撃への耐性を向上するのに加えて，静的な条件に応じた多要素認証の要求を実現可能にする．次いで，個人情報の漏洩を防止するために必要な Office 365 の設定方法を提案する．この設定では Office 365 の主要な機能や一部サービスの利用に制限が生じるが，個人情報保護の観点から利便性を犠牲にしてでも提案設定を行うことを推奨する．

A System Configuration of Office 365 Education Considering Personal Information Protection and Information Security

1. はじめに

教育機関向けに Microsoft が提供するクラウドアプリケーションスイートとして Office 365 Education がある．Office 365 Education には，Office 365 A1, A3, A5 の 3 プランがあり，A1 は教育機関に対して無償で提供されている．A3, A5 は有償である．A1 は Office 365 の基本機能を含んでおり，それには，ブラウザアプリ版の Office である Office Online，メールサービスの Exchange Online，オンラインストレージサービスの OneDrive for Business，組織内ウェブサイト基盤およびドキュメント共有基盤の SharePoint Online，チャットや音声会話，会議などの機能を持つコラボレーションツールの Teams といったオンラインサービスが含まれる．Office 365 A1 は教育機関であれば無料で利用できることから，多くの大学等で導入が進んでいる．なお，Office 365 A3, A5 は，上記機能に加えて，組織管理のための機能，情報セキュリティに関する機能などを含む．

Office 365 Education は，申し込みを行うだけで，特別にシステムを構築することなく，また，設定を何も行わずとも利用を開始できるようになっている．しかしながら，無料プランである Office 365 A1 を標準的な構成で用いることは，情報セキュリティの観点で，アカウント不正利用への対策が不十分であるという問題がある．有料の Office 365 A5 に含まれる情報セキュリティ機能を適切に設定して活用すればアカウント不正利用への対策が可能だが，多くの教育機関において Office 365 A5 は高額であり導入には財政上の困難がある．また，Office 365 を規定の設定で利用することは，個人情報漏洩の危険性をはらんでいる．

そこで本稿では，アカウント不正利用に対する情報セキュリティの確保を無料の Office 365 A1 を用いて安価に実現するシステム構成，および，個人情報漏洩の危険性を軽減する Office 365 の設定を提案する．まず，2 章で，Office 365 の標準的なシステム構成，および，既定の設定に存在する危険性について述べる．次いで，3 章で，アカウント不正利用への対策を安価に実現するシステム構成，および，個人情報漏洩を防ぐ設定方法を提案する．なお，本稿の内

[1] 九州大学情報基盤研究開発センター
Research Institute for Information Technology, Kyushu University
[a)] simayosi@cc.kyushu-u.ac.jp

容は，2019 年 4 月時点で Microsoft がインターネット上で一般に公開している情報だけをもとに筆者らが確認した結果であり，未公開の脆弱性や非公開機能を用いた内容などは含まれていない．

2. Office 365 標準構成における危険性

2.1 Office 365 におけるユーザ情報の格納

Office 365 では，申し込み組織ごとにテナントと呼ばれる管理単位が作成され，このテナントにユーザなどを登録して Office 365 を利用する．テナントには DNS ドメイン名を紐付ける．Office 365 のユーザアカウントは User Principal Name (UPN) を用いて識別される．UPN は RFC 822[1] に定められるメールアドレス形式を持ち，そのドメイン部分はテナントに紐付けられた複数ドメイン名から選択する．Office 365 へのサインインには，標準的に UPN とそのパスワードが用いられる．この UPN は，OneDrive for Business 上でのファイル共有や Teams でのメッセージ送信などで相手先を指定する際に利用される．また，Exchange Online を使用する場合は自動的にユーザの有効なメールアドレスとして用いられることから，一般的にはユーザのメールアドレスを UPN として用いる．

Office 365 のユーザアカウントは Azure Active Directory (Azure AD) を用いて管理される．1 個の Office 365 テナントに対して 1 個の Azure AD ディレクトリが自動的に構成され，Office 365 で使用されるユーザの個人情報や管理情報などは基本的に Azure AD に格納される．標準構成ではユーザのパスワードも Azure AD に保存され，Azure AD を用いてユーザ認証が行われる．また，テナント外部のユーザと情報共有や情報交換するときに，場合によっては外部ユーザをゲストユーザとしてテナントに登録する必要があるが，テナントに登録されたゲストユーザの情報も Azure AD に格納される．

大学等において Office 365 で用いる情報，すなわち，Azure AD に登録する情報は，一般的に学内の認証基盤や学務情報システムなどといった他のシステムと共用または連携することが一般的である．Office 365 のユーザ情報を組織内の別システムと連携する場合には，オンプレミスに構築した Active Directory（以下，オンプレ AD と呼ぶ）と Azure AD とを，Microsoft が提供するツールである Azure AD Connect を使って同期する構成が一般的に用いられる．この AD 同期により，オンプレ AD へのユーザの新規作成，削除，および，ユーザ情報の変更が，自動的に Azure AD に反映される．

2.2 アカウント不正利用の危険性

前述の通り，ユーザの UPN は標準的に Office 365 へのサインイン ID に用いられるが，UPN は情報交換や情報共有を行う場合に相手に教える必要があり，また，一般的に UPN にはユーザのメールアドレスが用いられることから，UPN は意図して公開されうるものである．攻撃者が何らかの方法で Office 365 ユーザの UPN を入手すると，Office 365 へのサインインパスワードに対するブルートフォース攻撃を試みることができる．特に近年は，多数のサーバの多数の ID に対して各 ID については低頻度にパスワード攻撃を行うパスワードスプレー攻撃が増加していると報告されている [2]．

ブルートフォース攻撃，パスワードスプレー攻撃への対策の一つとして，多要素認証 (MFA) の利用が推奨されている [2]．Office 365 へのサインインも MFA に対応しており，第 2 認証の手段としてモバイルアプリ Microsoft Authenticator を用いた承認，携帯電話のショートメッセージサービス (SMS) を用いた認証コードの送信，ハードウェアトークン，電話番号への発信が利用できる．Microsoft もパスワードスプレー攻撃への対策として MFA の利用を推奨している [3]．ただし，危険性に応じて MFA を要求するためには有料の Azure AD Premium P2 のライセンスがユーザ数分必要であり，また，あらかじめ定義した静的な条件に応じて MFA を要求するためにも有料の Azure AD Premium P1 のライセンスがユーザ数分必要である．無料の Office 365 A1 プランでは，管理者がユーザ別に MFA を有効化，無効化する必要があり，MFA を有効化したユーザのサインインには MFA が常時要求される．しかし，大学等の教職員には，モバイルアプリが利用可能なデバイスを持たず，SMS を受信できない，もしくは，SMS 受信に個人負担が発生する者が存在し，全ての教職員に対して常時 MFA を強制することは非常に困難である．

2.3 個人情報漏洩の危険性

Office 365 は，利便性を向上させるために，一般ユーザが他のユーザの情報を入手できる様々な機能を持っている．しかし，フィッシングや前述のパスワードスプレー攻撃などといった何らかの手段により攻撃者がアカウントの不正利用に成功した場合，Office 365 テナントに登録されている全てのユーザの個人情報が漏洩する危険性がある．既定の設定では，Office 365 テナントのいずれのユーザも全ユーザの個人情報を閲覧できる．つまり，攻撃者が Office 365 テナントのアカウント 1 個の不正利用に成功すれば，テナント内の全ユーザの個人情報を取得できる．それゆえ，Office 365 アカウントの不正利用が 1 件でも生じれば，個人情報が流出した可能性が否定できない．個人情報漏洩そのものも問題であるが，流出した個人情報が別のサイバー攻撃に利用される危険性も高い．また，攻撃者が UPN の一覧を入手できれば，別のパスワードスプレー攻撃に活用できる．

Exchange Online はグローバルアドレス一覧 (GAL) というアドレス帳を自動的に作成する [4]．GAL には既定で，

ユーザを含む Office 365 テナント内のメールが有効な受信者オブジェクトがすべて登録され，各オブジェクトについて Azure AD に格納されている姓名や所属，電話番号などの個人情報が登録される．UPN は必ず Exchange Online で有効なメールアドレスであるから，GAL は全ユーザの UPN を含んでいる．また，既定では GAL はテナントの全てのユーザが閲覧できる．つまり，既定の設定では，Office 365 テナントのいずれのユーザも全ユーザの個人情報を閲覧できる．さらに，Windows デスクトップアプリ版の Outlook を用いれば，Outlook の個人アドレス帳に GAL の登録情報全件を容易にコピーでき，個人アドレス帳はファイルへとエクスポートできる [5]．この方法により，GAL に登録されている全ての個人情報をファイルに出力できる．このことから，不正アクセスに成功した者は GAL からテナント内の全ユーザの UPN および個人情報の一覧を容易に取得できる．さらには，GAL の全件コピーを禁止する設定や検出する手段は現時点では存在しない．

Office 365 に含まれる各種サービスは利用上の利便性のために様々な形でユーザを検索する機能を持っている．SharePoint Online や OneDrive for Business において，既定の設定では，ファイルの共有相手を指定するダイアログボックスが補完検索する機能を持つ．例えば，1 文字 a と入力すると，UPN や氏名などが a から始まるユーザの一覧がリスト表示される．また，UPN や氏名だけでなく所属なども閲覧できる．他のサービスの多くも同様の機能を持っている．また，Yammer は標準機能としてテナントの全 Yammer 利用者を一覧表示する機能を持つ．これらの機能を利用すれば，不正アクセスに成功した者は機械的に全ユーザの UPN や個人情報を入手可能である．

前述の通り，Office 365 のユーザ情報は Azure AD に格納される．この Azure AD にアクセスする API が Microsoft により提供されており，MSOnline PowerShell モジュール [6] と AzureAD PowerShell モジュール [7]，および，REST 形式の Microsoft Graph API[8] が公開されている．既定の設定では，これらの API により一般ユーザであっても Azure AD に登録されているユーザ情報を取得できる．ここで取得できる情報には，姓・名，所属，別名アドレスを含むメールアドレス，電話番号などの個人情報だけでなく，アカウント作成日時，最終パスワード変更日時，ユーザに割り当てられているライセンス情報，さらには，ObjectId, ImmutableId, LiveId などの内部識別番号など，一般ユーザが知るべきではないと考えられる管理情報も含まれる．PowerShell を用いれば，単一のコマンドを Microsoft が公開する仕様 [9], [10] に従って実行するだけで，ゲストユーザを含んだ Azure AD に登録されている全ユーザの情報を取得できる．

3. 提案する構成・設定

3.1 サインイン認証構成

前章で述べたサインインパスワード攻撃についての危険性は，Office 365 A5 プランを利用して適切に設定すれば対策できる．しかし，多くの大学等では A5 プランは高額であり，導入には困難がある．そこで，Office 365 の有料プランを用いず安価に危険性を回避するためのシステム構成を提案する．

3.1.1 サインイン ID と UPN の分離

Office 365 へのサインインにおける認証の既定設定は，Azure AD に格納された UPN とパスワードを用いるクラウド認証であるが，外部の認証機構を用いるフェデレーション認証と呼ばれる構成 [11] とすることも可能である．このフェデレーション認証構成を活用し，Office 365 へのサインイン ID と UPN とを分離することで，パスワードスプレー攻撃などへの対策とする方法を提案する．

フェデレーション認証を構成するときは，Office 365 テナントに登録された DNS ドメインの中からフェデレーション認証を用いるドメインを設定する．フェデレーション認証には，Active Directory Federation Service (AD FS)，または，Security Assertion Markup Language (SAML)[12] を利用できるが，本稿では Microsoft によって標準的にサポートされる AD FS を用いた構成を採用する．オンプレミスで AD FS サーバを稼働させ，Azure AD と同期するオンプレ AD を AD FS サーバに参照させることで，Office 365 サインインの認証に Azure AD ではなくオンプレ AD を使用できる．

オンプレ AD と Azure AD とを同期する Azure AD Connect の既定の設定では，オンプレ AD の各ユーザオブジェクトの UPN 属性がそのまま Azure AD の UPN 属性へと同期される．しかし，Azure AD の UPN 属性へと同期される属性としてオンプレ AD の UPN 以外の属性を指定する代替 ID と呼ばれる設定を行うことで，オンプレ AD の UPN と Azure AD の UPN とを別の値に設定できる [13]．ただし，Azure AD Connect で代替 ID を選択すると，自動的に AD FS サーバに対して代替ログイン ID が構成され [14]，オンプレ AD の UPN に加えて代替 ID に選択した属性で AD FS でのサインインが可能になる．そこで，AD FS の代替ログイン ID 構成を以下の PowerShell コマンドレットにより手動で解除する必要がある．

```
Set-AdfsClaimsProviderTrust ‘
 -TargetIdentifier "AD AUTHORITY" ‘
 -AlternateLoginID $NULL -LookupForests $NULL
```

そして，Office 365 の UPN，および，オンプレ AD の UPN に用いるドメイン名に対して Office 365 テナントでフェデレーション認証を設定する．この方法により，Office 365

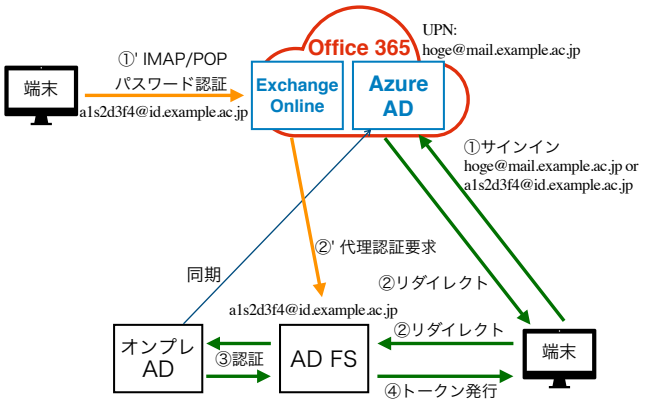

図 1 提案手法におけるサインインの流れ

へのサインインにはオンプレ AD の UPN を用いるようになり，Office 365 の UPN を用いてサインインできなくなる．このとき，オンプレ AD の UPN は他者に開示する必要はない．そこで，オンプレ AD の UPN は，無作為に選択された英数字などを設定し，管理者を除いて本人だけが知る秘密情報として扱う．これによって，パスワードだけでなく，Office 365 へのサインインに用いる ID についても基本的に本人だけが知ることとなり，Office 365 の UPN を用いたサインイン試行の攻撃を無効化できる．

本構成におけるサインインの流れを以下に説明する（図 1）．なお，図では例として，Office 365 の UPN に hoge@mail.example.ac.jp を，オンプレ AD の UPN に a1s2d3f4@id.example.ac.jp を用いている．サインインしていない状態で Office 365 にアクセスすると，まず Microsoft による Office 365 サインイン画面が表示される (1)．このとき，ドメイン部分にフェデレーション認証を設定したドメイン名を持つ任意のメールアドレス形式の文字列を入力すると，オンプレミスで稼働する AD FS のサインイン画面へとリダイレクトされる (2)．AD FS のサインイン画面での入力情報によりオンプレ AD で認証が行われ (3)，認証が成功すると AD FS から Office 365 へとトークンが発行されて (4) サインインが完了する．このとき，認証情報はユーザの端末と AD FS との間で通信される．ただし，Exchange Online に対する IMAP や POP による接続でパスワード認証を用いるときは，クライアントは Exchange Online のサーバに認証情報を送信し (1')，送られた認証情報を用いて Exchange Online が代理で AD FS に対して認証を要求する (2')．

Azure AD Connect での代替 ID 構成における既定の設定では，オンプレ AD の UPN は Azure AD の onPremisesUserPrincipalName 属性へと同期される [15]．つまり，Azure AD には Office 365 の UPN とサインイン ID の組が登録されることになり，望ましくない．Azure AD Connect ではフィルタ処理を設定することで，オンプレ AD から Azure AD へと同期される属性の一部を除外できる [16]．そこで，onPremisesUserPrincipalName 属性に対してフィルタを設定する．他にも Office 365 のサービスで必要としない属性についてはフィルタ処理を設定することが望ましい．

3.1.2 条件付き多要素認証の実現

前節で述べた構成では，比較的入手しやすい UPN を用いた Office 365 へのサインインが不可能であり，本人だけが知るサインイン ID を用いることから，パスワード攻撃への耐性が向上する．しかし，フィッシングなどの攻撃によってユーザが実際に利用するサインイン ID とパスワードが漏洩する可能性は否定できない．そういった事態への対策として依然として多要素認証 (MFA) の利用は有効である．

Office 365 へのサインインに AD FS を使ったフェデレーション認証を用いる場合，AD FS の機能により条件付きの MFA が実現できる [17]．それには，AD FS サーバにおいて，Office 365 への証明書利用者信頼 (relying party trust) に対して，要求規則 (claim rule) を設定する．要求規則によって，AD FS で MFA を実施したことを意味するトークンを実際の MFA なしで発行することで，Azure AD 側の MFA を迂回できる．これを用いて，例えば，接続元 IP アドレスが学内ネットワークであるサインイン要求に対しては MFA を不要とするなどといった条件付きの MFA が実現できる．

3.1.3 他の構成との比較

Office 365 へのサインイン認証として選択できる方法として，フェデレーション認証の他にパススルー認証 [18] がある．パススルー認証は，オンプレミス環境にインストールされたパススルー認証エージェントを介して Azure AD から送られた認証要求をオンプレ AD で検証する．パススルー認証でも代替 ID を利用できる．パススルー認証は，提案手法で用いるフェデレーション認証と比べて，AD FS サーバが不要であり，そのための設置，運用コストが掛からない利点がある．しかし，パススルー認証を用いる構成において，提案手法と同じ条件付きの MFA を実現するためには，有料の Azure AD P1 ライセンスがユーザ数必要である．このことから，総合的には提案手法の方が安価である．なお，パススルー認証では認証要求が必ず Azure AD を経由することから，同一 IP から別テナントに対するパスワードスプレー攻撃が検知できる可能性が考えられるが，無料プランの機能だけでその情報が活用されるかは不明である．

標準で用いられるクラウド認証では，サインイン ID は必ず Office 365 の UPN であり，条件付き MFA には Azure AD P1 ライセンスを要することから，提案手法に対する利点はほとんどないと考えられる．

3.2 個人情報保護のための設定

3.2.1 Azure AD

2.3 節で述べたとおり，Azure AD の既定の設定では，PowerShell を用いることで一般ユーザが全ユーザの登録情報を取得でき，非常に危険である．現時点では，有料プランや付加サービスを利用しても，PowerShell を用いた Azure AD へのアクセスに制限を課すことはできない．

一般ユーザが Azure AD のユーザ情報にアクセスすることを防ぐためには，以下の PowerShell コマンドレットを用いて Azure AD を設定する必要がある [19].

```
Set-MsolCompanySettings ‘
 -UsersPermissionToReadOtherUsersEnabled $False
```

しかし，この設定を行うと Office 365 の一部機能の利用に制限が生じる．具体例の一つとして，標準設定では Office 365 グループの所有者は一般ユーザであってもグループメンバーの追加が可能だが，上記設定を行った状態ではグループメンバーの追加ができない．他に，一般ユーザーの Teams 利用では，同じチームに所属しているなどして既に Teams 内で表示されているアカウントを除き，UPN を直接指定しても他のユーザへのメッセージ送信や音声通話，会議などの機能が使えず，実質的に Teams が利用できない状態となる．

このように，上記の設定には Office 365 利用上の不都合が多いが，この設定を行わない状態では全ユーザ情報が漏洩する危険性があり，管理情報も含むことから漏洩の影響が非常に高いことから，情報セキュリティと個人情報保護の観点では上記設定は必須だと言える．

3.2.2 グローバルアドレス一覧

Exchange Online では 2.3 節で述べたとおり，既定の設定では全ユーザの個人情報が登録されているグローバルアドレス一覧 (GAL) をあらゆるユーザーが閲覧でき，さらには容易にファイルに出力できる．

ユーザによる GAL の閲覧を制限する方法として，アドレス帳ポリシー (ABP) 機能を用いた GAL 分割がある [20]. ABP 機能を用いれば，全受信者オブジェクトが登録されたデフォルト GAL の一部だけを閲覧できる GAL を複数作成でき，各ユーザに対して参照させる GAL を割り当てられる．これにより，不正アクセスなどにより漏洩する個人情報の範囲が限定される．なお，各ユーザの既定の GAL は必ずデフォルト GAL であり，Exchange Online でアカウントが有効になった後でなければ ABP による GAL の設定ができないことに注意が必要である．

別の方法として，各受信者オブジェクトをデフォルト GAL から除外する設定が可能である．オンプレ AD と Azure AD とを同期している構成では，オンプレ AD におけるユーザオブジェクトの msExchHideFromAddressLists 属性に False を設定すれば，そのユーザは Office 365 テナントのデフォルト GAL に掲載されない．それ以外の受信者オブジェクトについては，個々の受信者オブジェクトに対してその有効化後に手動で GAL から除外する設定を行う必要がある．

大学等の教育機関では，学生は一般企業における顧客に相当する側面を持ち，一般企業の従業員に相当する教職員よりも個人情報に求められる機密性が高い．そこで，学生アカウントについてはデフォルト GAL に掲載しない方法が推奨される．教職員については，利便性を考慮して GAL 分割を利用する構成も考えられるが，その場合でも漏洩範囲を限定するために適切に GAL 分割を設定する必要がある．

3.2.3 各サービスへの制限

Office 365 に含まれる各サービスの多くは，2.3 節で述べたとおりユーザを検索する機能を持っている．しかし，この機能を悪用すれば全ユーザの情報を収集できることから，何らかの制限が必要である．

SharePoint Online の既定設定ではユーザの検索が可能だが，これを制限する方法が 2 種類ある [21]．一方は，検索範囲を前節で述べた ABP により割り当てられる GAL の範囲に制限する方法であり，以下の PowerShell コマンドレットの実行で設定できる．

```
Set-SPOTenant ‘
 -UseFindPeopleInPeoplePicker $True
```

もう一方は，検索機能を無効化してユーザ指定を UPN 完全一致だけに限定する方法であり，以下の PowerShell コマンドレットの実行で設定できる．

```
Set-SPOTenant ‘
 -SearchResolveExactEmailOrUPN $True
```

なお，前者の設定の場合にも，GAL 範囲外のユーザを UPN 完全一致で指定できる．OneDrive for Business と Delve はユーザ検索に SharePoint Online の機能を用いており，これらの設定が有効である．個人情報の漏洩を防ぐために，いずれかの設定を行う必要がある．

Yammer はテナントの全 Yammer 利用者を一覧表示する標準機能を持ち，それを無効化することはできない．また，Stream などのサービスは，ユーザ検索機能を無効化できない．個人情報保護の観点からは，これらのサービス自体を無効化するべきである．

4. おわりに

本稿では最初に，Microsoft が教育機関向けに提供する Office 365 Education について，無料の Office 365 A1 プランを標準構成で用いる場合にはパスワードスプレー攻撃などによりアカウントが不正利用される危険性が存在すること，また，Office 365 を既定の設定で利用する場合には個人情報が漏洩する危険性が存在することを報告した．そこでまず，アカウント不正利用への情報セキュリティ対策を Office 365 の有料プランを用いず安価に実現するシステム

構成を提案した．提案構成では，Office 365 へのサインインに用いる ID として，情報共有，情報交換に用いる UPN とは別の，基本的に本人しか知らない ID を用いることで，不正なサインインの危険性を低減するとともに，接続元 IP アドレスなどを条件として多要素認証を要求することが可能である．次いで，個人情報漏洩の危険性を軽減するために推奨される Office 365 テナントの設定方法を述べた．

アカウント不正利用への対策については，Microsoft から有料ではあるが手段が提供されている．一方，個人情報漏洩の危険性については，有料プランや付加サービスを用いるだけでは対策できない．それゆえ，個人情報保護の観点から，本稿で提案する設定方法を用いることが強く推奨される．しかしながら，その設定を適用すると，Office 365 の主要な機能の利用に制限が生じ，一部サービスは実質的に利用できない．また，一部のサービスは個人情報保護の対策を施せないことから利用が推奨できない．Office 365 に含まれるこれらの問題点について，Microsoft による対応が望まれる．

参考文献

[1] Crocker, D. H.: Standard for the Format of ARPA Internet Text Messages, RFC 822, IETF (1982).
[2] : Brute Force Attacks Conducted by Cyber Actors, Alert TA18-086A, US-CERT (2018).
[3] Simons, A.: Azure AD and ADFS best practices: Defending against password spray attacks, Microsoft (online), available from ⟨https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/⟩ (accessed 2019-04-16).
[4] : Address lists in Exchange Online, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/exchange/address-books/address-lists/address-lists⟩ (accessed 2019-04-16).
[5] : Export contacts from Outlook, Microsoft (online), available from ⟨https://support.office.com/en-us/article/10f09abd-643c-4495-bb80-543714eca73f⟩ (accessed 2019-04-16).
[6] : MSOnline, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/powershell/module/msonline/⟩ (accessed 2019-04-16).
[7] : AzureAD, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/powershell/module/AzureAD/⟩ (accessed 2019-04-16).
[8] : Microsoft Graph, Microsoft (online), available from ⟨https://developer.microsoft.com/en-us/graph⟩ (accessed 2019-04-16).
[9] : Get-MsolUser, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoluser⟩ (accessed 2019-04-16).
[10] : Get-AzureADUser, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/powershell/module/azuread/get-azureaduser⟩ (accessed 2019-04-16).
[11] : What is federation with Azure AD?, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed⟩ (accessed 2019-04-16).
[12] Cantor, S., Kemp, J., Philpott, R. and Maler, E.: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard (2005).
[13] : Azure AD UserPrincipalName population, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-userprincipalname⟩ (accessed 2019-04-16).
[14] : Configuring Alternate Login ID, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configuring-alternate-login-id⟩ (accessed 2019-04-16).
[15] : Azure AD Connect sync: Attributes synchronized to Azure Active Directory, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-sync-attributes-synchronized⟩ (accessed 2019-04-16).
[16] : Azure AD Connect sync: Configure filtering, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering⟩ (accessed 2019-04-16).
[17] Ozkir, B.: Office 365 customers who have ADFS installed can do simple filtered MFA using ADFS claim rules, Microsoft (online), available from ⟨https://blogs.technet.microsoft.com/bulentozkir/2016/05/01/office-365-customers-who-have-adfs-installed-can-do-simple-filtered-mfa-using-adfs-claim-rules/⟩ (accessed 2019-04-16).
[18] : User sign-in with Azure Active Directory Pass-through Authentication, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta⟩ (accessed 2019-04-16).
[19] : Set-MsolCompanySettings, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/powershell/module/msonline/set-msolcompanysettings⟩ (accessed 2019-04-16).
[20] : Address book policies in Exchange Online, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/exchange/address-books/address-book-policies/address-book-policies⟩ (accessed 2019-04-16).
[21] : Set-SPOTenant, Microsoft (online), available from ⟨https://docs.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant⟩ (accessed 2019-04-16).