Office 365 のフィッシング対策強化のための PowerShell による設定事例

葛西 真寿 [1),2)], 小倉 広実 [2)], 須藤 勝弘 [2)], 竹内 淑怜 [2)]

1) 弘前大学 大学院理工学研究科

2) 弘前大学情報連携統括本部 情報基盤センター

cnc-director@hirosaki-u.ac.jp

Setting anti-phishing measures in Office 365 by PowerShell

KASAI Masumi[1),2)], OGURA Hiromi[2)], SUTO Katsuhiro[2)], TAKEUCHI Sumire[2)]

1) Graduate School of Science and Technology, Hirosaki Univ.

2) Information Technology Center, Information Management Headquarters, Hirosaki Univ.

概要

弘前大学では，2015 年の情報基盤システムの更新時に Office 365 Education（契約当時は E1, 現在の A1 にあたる無料ライセンス）へ全面移行し，全ての職員及び学生がこのパブリッククラウドメールを活用してきた。しかし昨年，Office 365 team を騙るフィッシングメールによって利用者のパスワードが詐取され，なりすましログインによる不正転送設定によって本学に送信されたメールが学外へ不正転送されるというインシデント発生を受け，フィッシング対策強化のための各種設定を行うこととなった。本稿では，Office 365 Education A1 において，本学がこれまで行ってきたセキュリティ対策やフィッシング対策強化のための PowerShell による設定事例を報告する。

1 はじめに

弘前大学では，2015 年に更新した情報基盤システム HIROINS 2015 において，それまで運用してきた学内メールサーバとオンプレミス型 Web メールソフトウェアによるサービスから，Microsoft 社が提供する教育機関向けクラウドサービスである Office 365 Education（契約当時は E1, 現在の A1 にあたる無料ライセンス）に全面移行し，全ての職員及び学生がシングルテナント・単一メールドメイン （@hirosaki-u.ac.jp) で，このパブリッククラウドサービスを活用してきた。

しかし，2018 年 6 月，Office 365 team を騙るフィッシングメールによって利用者のパスワードが詐取され，なりすましログインによる不正転送設定によって本学に送信されたメールが学外へ不正転送されるというインシデント発生を受け，フィッシング対策強化のための各種設定を行うこととなった。

ここでは，Office 365 Education A1 のままで，本学がこれまで行ってきたセキュリティ対策やフィッシング対策強化のための PowerShell による設定事例を報告する。この機会に，AXIES 会員間で情報の共有と交換を行うことができれば，さらなるセキュリティの強化に繋がると期待される。

2 2018 年 6 月インシデントの概要

2018 年 6 月に発生したフィッシングメールによるインシデントの概要は以下の通りである。

1. メール不達を知らせる，Office 365 team を騙った英文メールが学内 242 名に配信された。
2. フィッシングメール本文のリンクをクリックした利用者が，Office 365 の詐欺サイトに誘導されてパスワードを入力してしまい，パスワードが詐取された。
3. 詐取した ID とパスワードで，本人になりすましてログインされ，学内 12 名の利用者のアカウントに不正転送先への自動転送が設定された。
4. 不正転送設定後，当該利用者に送信されたメールが，本人が気づかないうちに学外へ不正転送されて，結果として情報が漏洩した。

3 発見後の緊急措置

不正転送の発見後，ただちに不正転送設定されていた 12 名の転送設定を削除し，さらにフィッシングメールを受信した 242 名については，メール本文のリンクをクリックしたかどうかに関わらず全員のパスワードの変更を行った。

このような応急対策の後，セキュリティ強化に向けた対策の検討と実施を行うこととなったが，これまであまり事例報告されていない，本学特有の対応策もあるかと思うので，以下にまとめておく。

4　Microsoft 社への対策問い合わせと回答

本人になりすまして不正ログインした形跡をログからたどると，国外（カントリーコードはナイジェリア等）の IP アドレスからアクセスされていることがわかったため，まず Microsoft 社に，たとえパスワードを詐取されても国外から不正にアクセスされないような対策も含めて，フィッシング対策強化に向けた提案について問い合わせを行ったところ，Microsoft 社からの当初の回答は，有料プラン Microsoft 365 A5 の包括契約，という 1 択であった。これは，本学の職員数では，年間 4 千万円以上のライセンス料となる。では，これだけ払えば，他の対策，例えば多要素認証の設定は不要かと問い合わせると，それはそれ，多要素認証は必要との回答である。であれば，本学ではまず，Office 365 Education A1 という無料ライセンスのまま，多要素認証の必須化を含めたセキュリティ強化対策を行うこととなった。

5　当面の対策：学外への自動転送を全面的に禁止

学外への自動転送設定が，利用者本人による正規の設定なのか，なりすましによる不正設定なのか判断できない以上，学外への自動転送を学生・職員問わず全面的に禁止することとした。

2018 年 6 月 15 日に決定し，3 日後の 6 月 18 日 15:00 より禁止措置を開始。この時刻を過ぎても自動転送設定が残っている場合は，センターで強制削除した。

ただし，例外措置として，学内の別メールアドレスへの転送，またスマートフォン以外の携帯電話のみを使用している学生への配慮として，学生については Office 365 から国内 3 大キャリアのキャリアメール（@docomo.ne.jp, @ezweb.ne.jp, @softbank.ne.jp）への転送は認めることとしている。そのため，Office 365 の管理者設定からテナント全体で一律に転送を禁止する設定は入れずに，担当技術職員が管理者として転送設定を発見次第，削除してきた。

Office 365 では，利用者が自動転送設定を行なった場合に管理者に図 1. のような通知があり，この通知を受けてその都度，転送設定削除等の必要な対応を行なってきた。

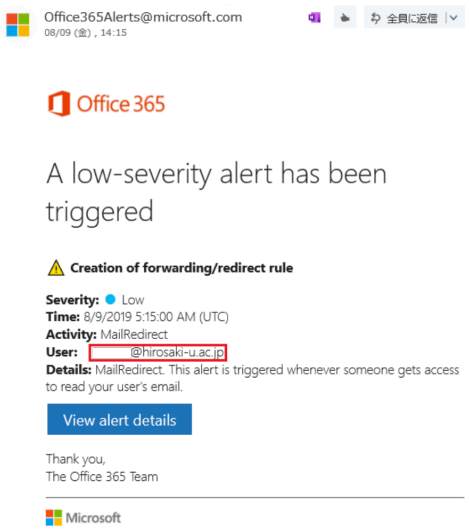

図 1. 利用者が転送設定を行なった際に管理者に送信されるアラートメール

PowerShell で利用者 (user) の転送設定を確認する例は以下の通りである。（実際には 1 行。）

```
PS C:¥> Get-Mailbox -Identity
  user@hirosaki-u.ac.jp | Select-Object
  Name,ForwardingSmtpAddress
```

また，転送設定を無効にする（削除する）例は以下の通り。

```
PS C:¥> Set-Mailbox -Identity
     user@hirosaki-u.ac.jp
     -ForwardingSmtpAddress $null
```

ちなみに，学外への自動転送については，本学が定める電子メール利用ガイドラインにも「原則として要保護情報を含む電子メールを，本学が整備した電子メールシステム以外の情報システムへ自動転送しないこと。」という記載がある。そこで，多要素認証の必須化により，なりすましによる不正な転送設定が実質上不可能になった現在も，学外への自動転送は禁止している。

6　その後 2018 年度に実施した対策

6.1　全職員のパスワード変更

当該フィッシングメールの受信者には，メール本文のリンクをクリックしたかどうか・フィッシングサイトに誘導されてパスワードを入力したかどうかに関わ

らず全員のパスワードの変更を実施済みであるが，あらためて全職員に対して期限を定めてパスワード変更を義務化した。期限までにパスワードを変更しなかった利用者に対しては，メール使用を不可とする対応をとった。

6.2 全職員に対する多要素認証の義務化

さらに，Office 365 の多要素認証の設定を全教職員に対して義務化し，2018 年 11 月 26 日の全学情報統括責任者（CIO, CISO 兼務）依頼文書により対応を開始した。（我々の知る限り，少なくとも国立大学法人において多要素認証の設定を全教職員に対して義務化したのは本学が最初ではないかと思う。）

多要素認証未設定者には罰則を課すことをせずに，定期的に設定依頼をメールや電話等で根気強く行った結果，2018 年度末時点で多要素認証設定率は 94%，2019 年度 8 月の本稿執筆時点では多要素認証設定率は 98.3% である。

ちなみに，休職者やメール未使用者を除いた実質多要素認証設定率は 99.5% である。

6.3 Office 365 の有料防御オプションの導入

また, Office 365 の有料のフィッシング防御オプションについても，検討の上，導入を行なった。Office 365 Education A1（無料ライセンス）でも，迷惑メールフィルタが機能するが，この迷惑メールフィルタだけでは高度なフィッシングメールに対しては無力である。有料のオプションとして，Microsoft 社の Advanced Threat Protection (ATP)　や，Trend Micro 社の Cloud App Security (CAS) 等の製品を比較検討し，2019 年 1 月より CAS を導入して現在に至っている。API 連携により，危険度の高いフィッシングメールは利用者の手をわずらわせずに自動的に隔離し利用者には見えないようにする点や，年度途中からの数ヶ月間の契約にも柔軟に対応したことが CAS の選定理由である。

7 今年度実施のフィッシング対策強化のための設定

本学では引き続き，Office 365 Education A1（無料ライセンス）のままで，フィッシング対策強化に向けて Office 365 の設定の見直しを行ってきている。Office 365 の管理者として設定を強化した項目は以下の通りである。

7.1 Office 365 自動転送の制限に関する設定

2018 年 6 月インシデントが，詐取されたパスワードによって本人になりすまして Office 365 にログインされ，自動転送設定を入れられたことによって発生したことを踏まえ，本学全構成員に対して自動転送設定を禁止したことは前述したが，全構成員に自動転送禁止の通知後も，ポツリポツリと自動転送設定を行う利用者が現れる。

前述したように，Office 365 の管理者には転送設定が行われる度に通知があり，その都度，管理者が手動で転送設定の削除を行なってきたが，以下のように PowerShell で設定することにより，たとえ利用者が個人的に転送設定をしても，転送が実際には行われないようにするようにした。この設定により，自動転送設定はもちろん，受信トレイルールで設定した転送ルールも無効になる。

原則，自動転送禁止。

```
PS C:¥> Set-RemoteDomain
       -Identity Default
       -AutoForwardEnabled $false
```

学内ユーザへの転送許可。

```
PS C:¥> New-RemoteDomain
  -Name Hirosaki_University
  -DomainName hirosaki-u.ac.jp
```

ドコモへの転送許可。

```
PS C:¥> New-RemoteDomain
  -Name DOCOMO -DomainName docomo.ne.jp
```

ソフトバンクへの転送許可。

```
PS C:¥> New-RemoteDomain -Name
     SOFTBANK -DomainName softbank.ne.jp
```

7.2 Office 365 の管理者ログインの制限

万が一，Office 365 の管理者の ID やパスワードが詐取されたとしても，管理者のログインを学内からのみ可能とするように制限することで，大事に至らないようにできる。PowerShell で以下のように設定する。

```
PS C:¥> New-ClientAccessRule
    -Name "Restrict EAC Access"
    -Action DenyAccess
    -AnyOfProtocols ExchangeAdminCenter
    -ExceptAnyOfClientIPAddressesOrRanges
     133.60.0.0/16  -Enabled $True
```

7.3 Office 365 に関する PowerShell 実行の制限

本学で発生した 2018 年 6 月インシデントでは，詐取されたパスワードを利用して犯人が逐一 Web ブラウザで手動ログインし，転送設定を行ったとは考えにくい。おそらく ID とパスワードのリストを用意し，PowerShell で自動設定を行ったのではないかと推測される。そうであれば，国外から自由に PowerShell を実行されないように制限することは有効であると考える。そこで，PowerShell の実行を学内からのみに制限することとした。設定は以下の通りである。

```
PS C:¥> New-ClientAccessRule
  -Name "Restrict PowerShell Access"
  -Action DenyAccess
  -AnyOfProtocols RemotePowerShell
  -ExceptAnyOfClientIPAddressesOrRanges
   133.60.0.0/16  -Enabled $True
```

ここで，CAS の挙動に問題が発生したので付記しておく。PowerShell の実行を学内 IP アドレスからのみに制限するというクライアント・アクセス・ルールを設定した後，CAS が正常に機能しなくなった。

Trend Micro 社サポートといろいろやりとりをした結果，このクライアント・アクセス・ルールの設定が原因であることがようやくわかった。おそらく，API 連携によって CAS がフィッシングメールの検知や隔離を行う際，Trend Micro 社が保有する IP アドレスから何らかの PowerShell スクリプトが実行されるのだが，それが，設定したクライアント・アクセス・ルールによってブロックされ，正常な動作ができなくなったのではないかと推測される。

この点については，CAS が使う IP アドレスの範囲をクライアント・アクセス・ルールに追記することで，PowerShell の実行が可能になると思われるが，Trend Micro 社では CAS という商品の運用に関してクライアント・アクセス・ルールの設定を想定していないらしく，当初の公式回答は，CAS を使うならクライアント・アクセス・ルールは設定するな，というものであった。これは本学が目指すフィッシング対策の強化を根幹から揺らがす回答であった。

そこで，CAS を実行するユーザを新たに登録し，このユーザについては，PowerShell を実行する IP アドレスの制限をつけない，というようにクライアント・アクセス・ルールを修正して運用を行なっている。

8 おわりに

本稿で紹介した Office 365 のクライアント・アクセス・ルールの設定は，Microsoft 社の Office 365 サポートから直接情報を得たものではない。ネット上でこのような情報を公開している有志の個人 Web サイトからの情報が非常に役立った。以下のサイトの作者の方々には深く感謝したい。

参考文献

[1] 追加費用なしでアクセス制御を実現できる，Exchange Online 条件付きアクセス - 今日も元気に IT 屋さん
https://prius.hateblo.jp/entry/2017/12/07/235723

[2] Office365 コミュニティ
https://www.facebook.com/groups/Office365Com.jp/

[3] 渡辺元気 他，Office 365 管理者のための逆引き PowerShell ハンドブック，日経 BP 社，2018 年.