事務職員を対象とするファイル暗号化の導入

齋藤　彰一 [1], 松尾　啓志 [2]

1) 名古屋工業大学　サイバーセキュリティセンター
2) 名古屋工業大学 情報基盤センター

shoichi@nitech.ac.jp

Introduction of File Encryption System for Office Staff

SAITO Shoichi [1], MATSUO Hiroshi [2]

1) Cybersecurity Center, Nagoya Institute of Technology
2) Information Technology Center, Nagoya Institute of Technology

概要

名古屋工業大学では 2022 年 8 月 1 日より、マイクロソフト社のファイル暗号化機能 Azure Information Protection を、全事務職員を対象としてデフォルト適用の運用を開始した。本論文では、ファイル暗号化機能の全事務職員を対象とした導入までの経過と、導入時の課題について述べる。

1　はじめに

名古屋工業大学では、情報漏洩対策の一環として、2022 年 8 月 1 日より、全事務職員の Office 365 利用に対して Azure Information Protection（AIP）をデフォルトで適用する運用を開始した。AIP は、マイクロソフト社の包括ライセンスで使用できるアクセス権制御やファイル暗号化を含む情報保護機能である。本学では、A5 ライセンスを契約し、AIP を含む各種機能を利用している。

AIP の情報保護機能では、マイクロソフトアカウントを有するユーザに対して、ファイルのアクセス権を制御することができる。このアクセス権は、管理者があらかじめ設定したラベルによって設定することを基本とする。このラベルによる保護では、アクセス権やファイル暗号化の他にヘッダやフッターの設定等の表示に関する設定もできる。また、カスタム設定として、AD に登録されたグループやユーザを指定して、事前設定のラベルとは別の独自の設定も可能である。これらは、Office 365 であればアドインなしで利用可能であり、Office 2022 等の場合はアドインをインストールすることでラベルを利用できる（注 : 2022 年 10 月時点でアドインの利用は勧められていない[1]）。なお、ファイル所有者が不在となったファイルにアクセスするために AIP 用のスーパーユーザを指定することができる。

AIP では、グループ（ユーザ）に対してポリシーを適用することができる。そのポリシーの一つに、既定ラベルをファイルに自動で適用する項目がある。ポリシーでこの項目を指定されたユーザが Office アプリ（Web を含む）を使用してラベルが適用されていないファイルを開いた場合、そのファイルにポリシーで設定された規定ラベルが自動で適用される。以下、これをデフォルト適用という。本学ではこのポリシーを全職員に対して適用した。

本論文では、2 章で、本学の AIP の設定の概要について述べる。3 章で AIP の導入から全職員に適用するに至った経緯について述べる。4 章では、デフォルト適用時に発生した問題点について述べ、5 章で今後の課題について述べる。6 章でまとめる。

2　AIP 設定

本学において運用している AIP の設定について述べる。本学における AIP 利用の目的は学外への情報漏洩対策である。そのために、ラベル定義の基本的な考えとして、学外へのファイル流出時に情報が漏洩しないことを第一としている。また、デフォルト適用の対象はファイルである。メールにも適用することができるが、論文執筆時点では対象にしていない。

表 1：ラベルの基本形

ラベル		暗号化
機密性 1	公開可	なし
機密性 2	教職員	あり
	教職員＋学外関係者	なし
機密性 3	特定の教職員	あり
	特定の教職員＋学外関係者	なし

2.1 ラベルの概要

表 1 に本学のラベルの基本形を示す。機密性 1 は公開用であり、アクセス権の制限や暗号化は適用していない。機密性 2 は全教職員で共有できるファイルに適用する。アクセス権は共同所有者とし、暗号化の範囲は職員及び教員である。共同所有者とすることで、ファイルを共有したアクセス権を有する教職員は、アクセス権を変更や解除することができる。これは、AIP 利用の目的が学外にファイルが流出した場合でも情報漏洩が発生させないためであることから、学内の情報流通を阻害しないために教職員の設定変更を可能としている。また、外部業者等の学外関係者と共有するファイルに対して暗号化を行うには、学外関係者の協力（マイクロソフトアカウントの登録等）が必要であるため、学外関係者と共有するファイルについてはアクセス権と暗号化を適用しない設定としている。

機密性 3 は特定の教職員のみアクセスできるファイルに適用する。特定の教職員をラベルによって事前に設定することはできないため、ファイル作成者がカスタム設定によって利用者およびアクセス権を設定する。ただし、設定しない場合に備えて初期状態では機密性 2 と同じアクセス権と暗号化設定を行っている。

利用者が 1 クリックで様々な設定ができるようにするために、表 1 のラベルを基本形として「編集の可否」と「ヘッダ表記（機密性表記）の有無」のバリエーションを選択できるラベルを用意した。デフォルトラベルは「機密性 2（編集可・ヘッダなし）」を指定しており、職員が変更しない限り暗号化が適用される。

表 2：ラベルの利用割合

機能	割合
機密性 1／2／3	34%／62%／ 4%
ヘッダあり／なし	25%／75%
学外関係者ラベル	3%

2.2 ラベルの利用割合

実際のラベルの利用割合を表 2 に示す。最も利用割合の高いラベルはデフォルトラベルの「機密性 2（編集可・ヘッダなし）」であった。多くの職員がラベルを変更せずに使用していると思われる。機密性 3 として特定の教職員を指定する割合は約 4%であり、少数であることが分かった。ヘッダの有無は、なしが 75%を占めている。デフォルトラベルがヘッダなしであることが主因と考えるが、ヘッダを付けることができない形式の決まったファイルも多いと考えられる。また、学外関係者を指定したファイルは約 3%程度である。学外送付にあたって暗号化を解除するために機密性 1 を誤用している可能性も考えられる。

2.3 カスタム設定

機密性 3 のファイルでは、ファイル作成者がアクセスできる権限やユーザを指定する。このユーザ指定には、できるだけ個人指定ではなく Azure AD グループによる指定を行うことを推奨している。例えば、課内で共有するファイルに AIP を設定する場合、ファイル作成時の所属職員を指定すると、後日の配置換えによって所属職員が変更された場合にも旧所属職員にアクセス権が残存する。この問題は、配置換えに連動したグループに対してアクセス権を設定することで解決できる。本学では統一データベースと呼ぶ認証の基本データベース[2]を有してお

り、事務局課室の Azure AD を含むユーザ情報は配置換えの日に更新される運用を行っている。これを活用し、AIP のアクセス権には Azure AD のグループを使用することでアクセス権の残存や設定もれが発生しない運用を実現している。

3　導入に至る経緯

本学におけるファイル暗号化機能の利用は、2018 年 3 月に開始した。しかし、AD-RMS によるシステムであったことや PDF を利用できるアプリが限られていたことなどから普及するに至らなかった。2019 年 5 月より AIP に移行して利用を開始した[3]。しかし、学内で利用していたシンクラ上での動作が安定せずに、やはり広く普及させるには至らなかった（原因は、シンクラシステムと OS のバージョン不一致)。その後、学内システムの環境を整えることにより、AIP を安定して利用することが可能となった。AIP 利用環境が整った後、学内に掲示を行ったが、利用者数は伸びることはなく、一部の教職員のみが使用する状況であった。

サイバーセキュリティセンターでは、2020 年 3 月より事務局の課室を対象とした個別セキュリティ訓練を実施している。本訓練では、各課室が扱う情報やファイルのやり取りの特徴に応じて、保護すべき情報や保護のポイント等を指摘している。この訓練において、AIP の利用の説明や利点について説明を行った。さらに、事務局内への周知や学内会議資料への AIP 適用を通じて、AIP の認知は広がったと考える。

名古屋工業大学では、2022 年 7 月から新型コロナウイルス対応の勤務体系から通常に戻すことが決まり、サイバーセキュリティセンターでは同年 5 月より在宅勤務におけるセキュリティ既定等の見直しを行った。この見直しの一環で、事務局内の情報漏洩対策を合わせて行うこととなり、AIP 適用の全職員へのデフォルト適用が決まった。

実施に向けて、6 月から事務局内で情報関係を所掌する学術情報課、7 月から人事課を対象に先行実施し、全職員を対象にした場合に発生する問題の事前評価を実施した。合わせて、事務局内の連絡会議を通じて周知した。この期間中に発生した問題点については 4 章で述べる。大きな問題は発生することなく、8 月 1 日に全職員に対して AIP をデフォルトで使用するポリシーを適用し、本論文を執筆している 10 月時点において継続している。

4　デフォルト適用時の問題点

本章では、デフォルト適用に際して発生した問題点について述べる。

4.1 Office 365

本学の事務職員の多くは、シンクライアントシステムにより業務を行っている。デフォルト適用前には、Office はバージョン 2021 を使用していた。この環境では、ファイルの共同編集ができない問題が発生し、これを解決するために共同編集を有効とする設定を行った[4]。しかし、これにより AIP アドインの動作が不安定となった。調査の結果、AIP アドインがすでに「保守のみ」となっており、Office 365 を使用する旨のアナウンスが行われていた。このため、シンクライアントの Office を Office 365 へ移行し、アドインを無効化することで解決した。

4.2 マクロによる保存

AIP を適用したファイルによるマクロ利用について、本学職員より報告があった問題について述べる。マクロにファイル保存が含まれる場合に、そのファイルに AIP をデフォルト適用できずにエラーとなっている。問題のファイルは他機関の指定ファイルであり保護されているために解析はできておらず、詳細は不明である。マクロで保存するためには、AIP のデフォルト適用の影響を受けないようにする必要がある。現状の対応策として、このマクロを含んだファイルを使用する場合に限り、Office アプリから一時的にサインアウトすることで保存する運用を行っている。

5　今後の課題

本章では、AIP の全学的な活用に向けての課題について述べる。

5.1 格付けの徹底

本学の AIP 設定では、機密性 1 を適用すると暗号化されないファイルを作成できる。学外へのファイル送付や一般公開のファイルが必要であることから、暗号化を適用しない手段は必要である。しかし、ラベル設定を誤ることによる情報漏洩の危険性を否定できない。今後、誤ったラベル設定に対して修正を依頼するとともに、情報格付けによるラベル設定を適切に行うようにさらに周知する必要がある。

5.2 メールへの適用

AIP 設定では、ファイルへのデフォルト適用に加えてメールへのデフォルト適用も設定できる。しかし、本学ではメールに対する適用は行っていない。これは、ファイルよりも学外とのやり取りも多いことから復号できない相手に暗号化ファイルを送った場合の対応に時間がかかること。また、Outlook 以外のメーラーやメーリングリストでの復号ができないため、学内においてもコストの増加が心配されるためである。今後、対応の検討が必要である。

5.3 教員対応

本学では、全職員に対して AIP をデフォルトで適用したが、教員へのデフォルト適用については実施していない。教員も AIP の利用は可能であり、利用している教員も多い。すでに、学内会議の多くでは、機密性の高い情報を扱う場合には AIP が設定されたファイルが配布されており、教員も AIP 付きファイルを閲覧する機会は多い。しかし、以下の理由により論文執筆時点でデフォルト適用を実施予定はない。

- 利用環境がシンクライアントで大半が統一されている事務職員に対して、教員の PC 環境は様々であり、その設定も教員自身によることが多い。PC 環境の準備について時間が必要である。
- 学生や学外とのやり取りも多く、AIP にラベルを自ら設定することに対する理解を浸透させる必要がある。

現在、教員に対する普及活動として、会議のファイル以外でも、事務職員から教員に送る機密性の高い情報を含むファイル（個人情報、人事、入試、成績等）については AIP を設定して送るように事務局に依頼し実施している。今後、教員に対する AIP 普及活動を継続して行い、教員に対するデフォルト適用を実現させたい。

6 おわりに

本論文では、本学における事務職員への AIP のデフォルト適用について述べた。AIP に関する情報は Web でも少なく、難しい面があることは否定できない。しかし、情報流出対策におけるファイル暗号化は有効であり、復号のためのパスワードを事前共有する必要がない本機構を活用することで大学の情報セキュリティの向上に大きく寄与できる。本論文執筆時点でデフォルト適用開始から 2 か月程度経過しているが、大きな問題なく運用できており、今後も運用を継続する計画である。さらに、教員やメール対応等の課題についても対策の検討を進め、さらに安全な情報管理体制を構築する。

参考文献

[1] Announcing AIP unified labeling client maintenance mode and sunset of mobile viewer、https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-aip-unified-labeling-client-maintenance-mode-and/ba-p/3043613（2022 年 10 月 11 日アクセス）.

[2] 齋藤彰一、打矢隆弘、松井俊浩、大曽根康裕、松尾啓志、名工大統一データベース：学内情報共有・認証基盤データベースの構築と運用、大学 ICT 推進協議会 2011 年度年次大会、2011.

[3] 齋藤彰一、松尾啓志、名古屋工業大学における 2018・2019 年度の情報セキュリティ対策、大学 ICT 推進協議会 2019 年度年次大会、SF2-2、2019.

[4] 機密度ラベルを使用して暗号化されたファイルの共同編集を有効にする、https://learn.microsoft.com/ja-jp/microsoft-365/compliance/sensitivity-labels-coauthoring （2022 年 10 月 11 日アクセス）.