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

齋藤 彰一 [1)], 松尾 啓志 [1)]

1) 名古屋工業大学

shoichi@nitech.ac.jp

Security Measures at Nagoya Institute of Technology in 2018-2019

SAITO Shoichi [1)], MATSUO Hiroshi [1)]

1) Nagoya Institute of Technology

概要

名古屋工業大学において 2018 年度と 2019 年度に実施した情報セキュリティ対策について述べる。この 2 年間に、Endpoint Detection and Response(EDR)、多要素認証(MFA)、ファイル暗号化の運用を開始した。本稿では、これら 3 つのサービスについて導入と運用状況と課題を示す。

1 はじめに

名古屋工業大学では、情報セキュリティ対策を目的として 2017 年 3 月に学内 CSIRT としてサイバーセキュリティセンターを設置した。セキュリティ向上策を実施するために、本学が契約しているマイクロソフト社の教育機関向け包括ライセンスを調査し、追加費用が不要で対策効果が高いと判断できる 3 種類の対策について 2018 年度より導入を行った。導入した対策は、端末における異常検知(EDR)、利用者認証、情報漏洩対策の 3 点である。これら対策は、情報セキュリティ対策に不可欠であり、これらの対策を向上させることで本学のセキュリティレベルの向上が大きく期待できる。

異常検知としては、Endpoint Detection and Response(EDR)である Microsoft Defender Advanced Threat Protection(MDATP)[1]を導入した。MDATP により、従来よりも正確な異常検知の実現と、異常発生時の正確な状況把握を実現できる。次に、利用者認証の安全性向上として、多要素認証[2]を本学でも導入する。さらに、個人情報や研究情報の漏洩対策として、ファイル暗号化を進めるための Azure Information Protection(AIP)[3]を導入した。AIP により、学外への情報漏洩防止を低コストで実現する。また、クラウドストレージを活用するための基本的な情報保護機構としても利用できる。

本稿では、2 章で MDATP の概要と利用状況について述べる。3 章では多要素認証として MS MFA の概要と導入について述べる。4 章では、AIP を利用した情報保護対策の概要と、本学での運用計画について述べ、5 章でまとめる。

2 マルウェア対策

本章では、本学で導入した Microsoft Defender Advanced Threat Protection(MDATP)[1]の概要と本学での利用状況について述べる。

2.1 Microsoft Defender ATP の概要

MDATP は、Windows 10 に組み込まれたセンサーから動作シグナルを収集して、クラウドにおいて各種脅威情報に基づいて分析を行うシステムである。異常検知時には、自動での駆除（ウイルス対策機能）や管理者への通報はもとより、複数台の検知を関連付けた分析なども可能である。また、各端末の OS の状況やアプリのインストール状況の収集や、遠隔でのスキャン実施等が可能である。

2.2 MDATP の利用状況

本学では、2018 年 12 月に MDATP を導入した。導入当初は情報基盤センターが管理する、事務用シンクライアント（約 250 台）に導入、その後に教育用端末（約 500 台）にも導入した。また、研究室設置端末については希望者のみとして運用を開始した。毎月 1 日付の導入端末数を**表 1** に示す。なお、2019 年 3 月には教授会と職員向けにセキュリティ講習会を開催し、システムの導入についての説明と共に研究室端末への導入依頼を行った。本論文執筆時の 2019 年 9 月時点で約 1400 台の端末に導入されている。端末管理システムに登録された Windows は約 5400 台であることから、導入

率は約 28%であり、まだ普及が不十分であると言える。今後も各教員に導入の依頼を行う。

表 1 MDATP 導入端末数の推移

年	月	Active 端末数
2019	2	862
	3	891
	4	1,030
	5	1,070
	6	1,110
	7	1,370
	8	1,520
	9	1,410

2.3 検知状況

MDATP の検知は 4 レベル（Informational, Low, Middle, High）に分類される。この内、Middle と High に分類された検知は月に 0～2 件程度であり、ほぼすべてが研究室端末であった。これら High, Middle レベルの検知の多くが、バックアップファイル等の昔のファイルをスキャンした結果、新たにマルウェアや PUA(Potentially Unwanted Application)と検出されたファイルが複数検出されたためであった。

一方、Informational と Low の低レベルによる検知の多くは PUA であり、Adware が多い。MDATP 導入直後に、それ以前にインストールされていた PUA が検出される場合が多い。低レベルの検知においても、研究室端末での検知が大部分を占め、教育用端末での検知数は全体の約 12%程度、事務用シンクラについては約 5%である。なお、4 月以降については事務用シンクラの検知数は 2 件のみとなっており、利用者が注意して利用しているためと思われる。

2.4 検知時の対応

問題が検出された場合には、MDATP から指定されたメールアドレスにメール通知が送られる。サイバーセキュリティセンタースタッフがこのメールを受信し、状況調査を行う。状況調査においては、感染ファイルの駆除状況、保存デバイス（ローカルストレージか、USB やネットストレージかの別）、マルウェアの活動状況などについて Web ポータルで確認を行う。その確認結果に基づいて、追加対応の要不要を決める。

開始当初から 7 月までは、駆除の成否に関わらず、すべての通知に対して Defender によるフルスキャンの実施を端末管理者に依頼した。しかし、追加で検出されることはほぼないことが分かったため、8 月以降については以下の場合を除いて追加依頼は実施しないようにした。例外的に追加対応を依頼する場合は次のとおりである。

- Middle レベルと High レベルの場合
- マルウェアや PUA が駆除されるまでに動いた場合
- 駆除に失敗した場合
- USB ドライブやネットストレージ内のファイルが検出された場合

MDATP の Web ポータルでは、駆除されるまでに問題のファイルが動作したか否かを確認できる。駆除完了までに動作した場合には、他のファイル等への影響を判断できないため追加のフルスキャンを依頼する。また、USB 等に保存されたファイルが検知された場合には、当該 USB ドライブやネットストレージでファイルを共有している他方の端末が感染している可能性があるため、共有先の端末のスキャンを依頼している。Middle や High レベルの検知の場合は、詳細な調査と共に、端末管理者への連絡と聞き取り調査を実施している。なお、9 月時点において、問題となるような感染は検知していない。

2.5 MDATP で得られる情報の活用

MDATP では、インストールされている OS やアプリのバージョンや、当該バージョンに関連した脆弱性を確認できる。確認方法には、Web ポータルと API が利用できる。ただし、API での情報取得は、Web ポータルよりも提供時期が遅くなっている。

本学では、OS のバージョン情報やパッチ適用状況をこの機能を利用して取得し、古いバージョンや脆弱性があるバージョンの利用者へ、更新を実施するように促すメールを送っている。具体的には、8 月に Windows 10 の 1803 以前の利用者に対して 1903 への更新の依頼や、CVE-2019-0708(Win7 等の RDP 脆弱性)のパッチを適用していない利用者に対してパッチ適用の依頼を実施した。今後は、アプリケーションのバージョンが API で取得できる機能の提供を待ち、アプリケーションの最新版への更新依頼を実施する計画である。

2.6 MDATP 活用の課題

情報活用面では、MDATP を利用すると低レベルの感染状況の把握は容易になる。さらに、MDATP で取得できる各種情報（プロセス実行状況、レジスタ操作やネットワーク通信開始、ファイル生成やリネームなど）を活用してより詳細な状況調査も可能である。しかし、当然ではあるが、レジスタの利用状況などには Windows 管理の知識、また通信先に関するセキュリティ情報との関係調査能力などが必要である。

一方、管理運用面では、MDATP の利用は AD で管理している端末群にはグループポリシーで一括登録が可能である。また、Microsoft Intune や SCCM も利用できる。しかし、研究室端末など教員が管理している端末については個別に設定する必要がある。設定に際して、各教員の協力を得ることが普及のための大きな課題となる。本学においては、教授会での説明会、センターWeb ページや学内掲示板での案内を実施しているが普及率は20%台にとどまっており、さらなる普及が課題である。

3 多要素認証

最近多数発生しているパスワードへの攻撃の対策として多要素認証の導入が広く行われている。本学においても、2019 年 2 月よりマイクロソフト社製の Multi-Factor Authentication(MFA)システム[2]を運用している。MFA の対象サービスは、Office 365、VPN と学内ポータルである。

3.1 MFA 認証の概要

本学で利用可能な MFA 認証は、Microsoft 社の Authenticator アプリを利用したスマホ認証と電話認証の 2 つである。SMS 認証も可能であるが、国際 SMS の利用申請と国際 SMS の通信料金が必要であるため、SMS 方式は利用しないようにマニュアルなどで案内している。なお、本学では 2017 年より IC カードによる認証基盤を導入しており、シンクライアントや教育用端末へのログインは、IC カードによる多要素認証である。ポータルへのログインは、従来からの IC カードによる多要素認証と今回導入した MFA 認証との併用であり、ログイン用のリンクを別々に用意することで、どちらの認証方式も利用可能なシステムを構築した。

3.2 MFA 認証の運用

本学の MFA はオンプレミス環境に構築した。ポータルでの利用方法としては、すでに導入済みの SSO 基盤である OpenAM に認証システムとして MFA を追加した。これにより、OpenAM は、従来からの LDAP 認証と新たな MFA 認証の両方の認証が成功した場合のみに認証成功と判定する。また、VPN の認証では、MFA サーバを Radius サーバとして運用する方式を利用している。これらの方式の利点は、認証方式の追加として実現していることで利用者側システムへの変更がないことである。このため、導入が容易と考える。しかし、利用者側の変更を行えないことから、MFA 認証実行途中にスマホや電話の確認待ち状態であることを利用者に示すことができないことが問題である。特に VPN 利用時には、VPN への接続失敗か認証失敗かの区別が利用者には判断できず、利便性を下げている。

MFA 認証におけるセキュリティ面以外では、ポータルを Mac で利用できるようになったことが利点としてあげられる。従来のポータルでは IC カード認証が必須であったが、IC カード認証が Windows に限られていたため Mac ユーザには不便であった。MFA を利用することで Mac での利用が可能となり好評である。

3.3 MFA 認証の課題

MFA に関する課題として、スマートフォンを持たない利用者への対応がある。現時点では、ポータルの認証には、IC カードによる認証も併用している。また、シンクライアント端末については、情報基盤センターが一括管理しており MDATP の運用やアプリのインストールが適切に運用されていることから、ポータルと Office 365 利用時に MFA 認証を省略する運用としている。これらにより、学内からの学内情報システムへの利用には不都合は生じないように配慮している。

また、メールにおける imap や pop 等の Web 以外のプロトコルへの対応についても対応方法や代替案の検討が必要である。

4 情報漏洩対策

メールの誤送信やノートパソコンの紛失などの個人情報や研究情報の漏洩を防止するための仕組みとして、ファイル暗号化の Azure Information

Protection(AIP)[3]システムを導入した。

4.1 AIP の概要

AIP の主な機能としては、Azure AD に登録されたユーザにアクセス権を付与したファイルの暗号化である。暗号化はユーザや AD グループを組み合わせて設定可能である。管理者は、ラベルと呼ばれる暗号化の設定をあらかじめ行う。ラベルは、アクセス権を与える利用者と AD グループの設定、ファイルヘッダやフッターの設定を行う。さらに、管理者はポリシーを定義して、利用者毎や AD グループ毎に利用できるラベルを指定することができる。利用者は、ラベル単位で暗号化を行うか、カスタム設定として任意の利用者を組み合わせて暗号化を行うかの指定を Office のバーで簡単に設定することができる（**図 1** 参照）。

ファイルの所有者は、暗号化したファイルを誰が開封したか、また権限がない利用者が開封しようとしたかを確認できる機能もある。

なお、ファイル所有者が退職した場合等で復号できなくなった場合は、AIP の管理者権限によりファイルのアクセス権を変更できる。

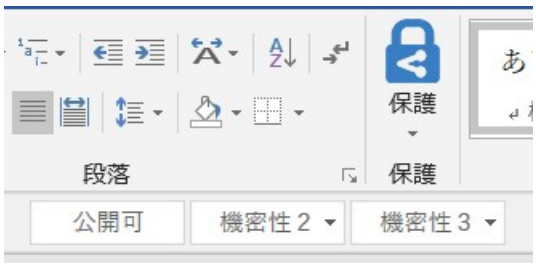

図 1 Office アプリの AIP ラベル選択肢とカスタム設定（保護）

4.2 AIP の導入

最初の導入は 2018 年 3 月であり、AD-RMS を利用したシステムであった。しかし、対象 OS が Windows のみであったことと、PDF ファイルのサポートのために有料の Foxit Reader のプラグイン導入が必要であったために広く利用されることはなかった。

2019 年 5 月に AD-RMS から AIP に移行した。これは、AIP には以下の利点があり、AD-RMS での問題点を解決できると考えたためである。

- MacOS, Android, iOS での利用が可能
- Office アプリのインタフェースの改良
- PDF 対応が進んだ
  - ➢AIP Viewer で閲覧とアクセス制限が可能
  - ➢Adobe Reader の無料プラグインが利用可能

さらに、学内の文書格付との連携において次にあげる機能も有効であると判断した。

- アクセス権設定と同時に Office ファイルやメールのヘッダやフッターへの格付け情報の出力（「機密性２」等の文書格付情報の出力）
- Office ファイル作成時に標準の文書格付を設定可能
- 保護されたファイルの開封状況の確認

AIP に移行後に、学内で導入試験を実施し、2019 年 7 月より本学総務課を主体として推進体制を構築し、事務局において 9 月から試行、10 月から本格運用を開始する。

4.3 AIP の運用

まず、本格運用前であるため、本稿での状況は 2019 年 9 月の準備時点での内容であることをお断りする。

本節では、本学におけるラベル定義の概要について述べる。本学のラベル定義は、文書格付規定に基づき、「公開可」、「機密性２」、「機密性３」の 3 種類とした。ファイルを作成する教職員が図 1 に示したインタフェースを利用して文書格付を行う。これら文書格付情報は、各ファイルとメールのヘッダ部に出力される。一方、アクセス権の設定は、「制限なし」、「教職員」、「カスタム設定」の 3 種類である。各ラベルへの対応は、「公開可」が「制限なし」、「機密性２」と「機密性３」が「教職員」である。「カスタム設定」は機密性２と３において利用者の判断で設定する。

さらに、各事務課や各委員会内のファイルで利用するために各課や各委員会用のラベルも設定可能である。また、これらのラベルを各課・委員会に属する教職員のみが利用できるよう設定した。

本格運用前であるため、まだすべての問題点を検討しきれていないと思われる。例えば、カスタム設定において厳しくアクセス権を設定することができるが、ファイル作成者の想定よりもファイル利用者が多い場合（会議への代理出席等）に設定追加などの作業増加が考えられる。基本的には、AIP によるアクセス制限は学外への流出対策とし

て学内構成員へのアクセス権は緩めとし、利用の効率と情報漏洩対策のバランスを取ることが必要と考える。

5 おわりに

本学において 2018 年度からの 2 年間で導入したセキュリティ対策システムについてその概要と本学での運用状況について述べた。これらシステムはマイクロソフト社の教育機関向け包括ライセンスを活用したものであり、当初より A5 ライセンスを契約していた本学の場合は追加必要が発生していないことは大きなメリットであった。

今後は、MDATP の利用推進がある。MacOS 版もプレビューとして提供されているため、利用可能になった時点で利用する予定である。また、AIP の職員への浸透と教員への普及を務め、情報漏洩対策や研究データ保護に活用する計画である。

参考文献

[1] Microsoft Defender Advanced Threat Protection, https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection (2019/9/19 アクセス).

[2] How it works: Azure Multi-Factor Authentication, https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/concept-mfa-howitworks (2019/9/19 アクセス).

[3] What is Azure Information Protection?, https://docs.microsoft.com/ja-jp/azure/information-protection/what-is-information-protection (2019/9/19 アクセス).