三重大学教育学部研究紀要　第 70 巻　自然科学（2019）　7－14 頁

怪しいメールを確認するためのセキュリティ対策

山　守　一　徳*

A Security Method to Check Suspicious E-mail

Kazunori YAMAMORI

要　旨

Windows 端末上で、自分に届いたメールを開く時に、ウィルスが含まれているのでないかと心配になるような場面がよく起きる。その時に、被害が最小で確認することができるようにするための方策を提案する。「ネットワーク分離」と呼ばれる、総務省が推奨する方式が一部自治体では導入されているが、構築費用が莫大となり、大学での導入は難しい。提案する策は、マイクロソフトの Windows Defender Application Guard ソフトと Web メールを利用する方法である。Windows Defender Application Guard ソフトは、端末内に別 OS が存在しているかのように動作し、ウィルス等で被害を受けても端末の基本 OS と切り離されているため、被害最小で済むものである。見た目は、Windows Edge の Web ブラウザを開いているように見える。その特別の Web ブラウザで Web メールを開くことで、怪しいメールを確認することができる。

１．はじめに

「ネットワーク分離」と呼ばれる方式は、インターネットに繋がる Web ブラウザとインターネットに繋がらない Web ブラウザが、自分の端末内に存在し、組織内部の仕事をしている時は、インターネットに繋がらない Web ブラウザで仕事をすることで、怪しいサイトへアクセスすることを防ぐ。インターネットに繋がらない内部ネットワークと、インターネットに繋がる外部ネットワークが切り離されて存在している状態であり、外部から届くメールは、無害化処理を施されてから、内部ネットワーク内で見ることができるようになる。この方法は、無害化させるためのソフトや外部ネットワークから内部ネットワークへファイル転送するためのソフト等を購入する必要があり、導入費用が高くなるのが欠点である。提案する策は、無料の Windows Defender Application Guard ソフト（以後、Application Guard と略記）を外部ネットワークに相当させるように使う方法である。

Application Guard を立ち上げて、自分宛のメールを Web メールソフトを使って中身確認する。メールの中身を見ることができ、迷惑メールならば削除する。必要メールならば、通常のメールクライアントソフトでメールを読み直すことができる。

２．Application Guard

Application Guard は、Windows10 Enterprise Edition または Professional Edition の OS に付属し、Hyper-V の仮想化技術を利用して Windows Edge をより安全に稼働させようとするものである。マルウェアに侵

＊三重大学教育学部情報教育講座

入されたとしても仮想環境内で留まり、物理環境には実害が及ばないようにするものである。Hyper-V が稼働できるハードウェアが必要であり、BIOS の設定画面で CPU 設定の中の Intel Virtualization Technology 機能を「有効」に設定しないと動かない。できればEnterprise Editionで動かした方が、Application Guard で使える機能が多くなり、クリップボード共有や印刷機能を制御する「エンタープライズモード」で動かすことができる。Windows10 Enterprise Edition Version1803 の「エンタープライズモード」では、Application Guard の Windows Edge でダウンロードしたファイルをベース OS 側から取り出すことができるようにもなる。

図１　「アプリと機能」の画面

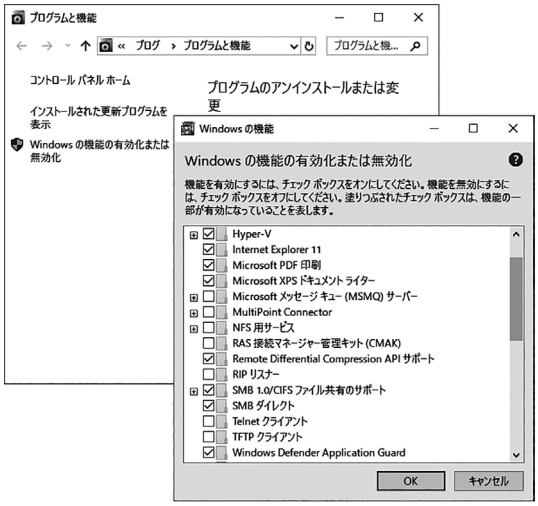

図２　「プログラムと機能」の画面

2.1　インストール方法

左下の Windows 旗マークを右クリックし、「アプリと機能」を選択する。開くウィンドウ（図 1 参照）の中の「プログラムと機能」を選択する。

「プログラムと機能」のウィンドウ（図 2 参照）の中の「Windows の機能の有効化または無効化」を選択し、開くウィンドウの中の「Hyper-V」と「Windows Defender Application Guard」にチェックを入れる。チェックを入れられない状態になっている時は、端末立ち上げ時に Del キーを押すと表示される BIOS の設定画面で CPU 設定の中の Intel Virtualization Technology 機能が「有効」に設定されていることと、Windows10 の Edition や Version を確かめる。ハードウェアが古くてプロセッサーに必要な仮想化機能がない場合には、Hyper-V プラットフォームにチェックが入らない。

図３　ローカルグループポリシーエディタの画面

左下の Windows 旗マークを右クリックし、「ファイル名を指定して実行」を選択し、gpedit.msc を実行し、ローカルグループポリシーエディタ（図 3 参照）を起動する。その中のコンピュータの構成、管理用テンプレート、Windows コンポーネント、Windows Defender Application Guard を順にクリックし、設定項目のリストを表示させる。「Windows Defender Application Guard をエンタープライズモードでオンにします」を有効に設定する。さらに「Windows Defender Application Guard のクリップボード設定を構成します」を有効にし、「クリップボードの操作をブロックする（既定）」をクリックし「分離セッションからホストへのクリップボード操作を

有効にする」を選択し、その下の「クリップボードの内容のオプション」を 3 に設定する。その他、印刷設定なども有効に設定する。

English(United States)の言語パックが Application Guard 起動時に必要になるため、左下の Windows 旗マークを左クリックし、歯車の絵の「設定」を選び、「設定の検索」の入力欄（図 4 参照）に“言語”と入力し、現れてくる「地域と言語の設定」メニューを選ぶ。「地域と言語」のウィンドウ（図 5 参照）の中の「言語を追加する」を選択し、English（United States）を選んで「次へ」ボタンを押し、「自分の Windows の表示言語として設定する」のチェックをはずして「インストール」ボタンを押す。

図４　設定の画面

図５　地域と言語の画面

2.2　起動方法

インストールが完了すれば、Windows Edge の右上の設定メニューの中に「新しい Application Guard ウィンドウ」のメニューが現れるので、それを選択すれば、Application Guard が起動する。Windows Edge の上に赤い線が入った形で表示される（図 6 参照）。Windows10 Professional Edition ではスタンドアローンモードで Application Guard を立ち上げることができる。左下の Windows 旗マークを右クリックし、「ファイル名を指定して実行」を選択し、regedit を実行し、¥HKEY_LOCAL_MACHINE¥software¥Microsoft¥Hvsi に行き、右側枠内で右クリックし、新規の中から DWORD（32 ビット）値（D）を選択し、名称を IsHvsiStandaloneMode、その値を 1 に設定すると、Windows　Edge の右上の設定メニューの中に「新しい Application Guard ウィンドウ」のメニューが現れる。

図６ Application Guard の画面

３．Web メールでメール確認

Application Guard の Windows Edge を使って自分に届いたメールを確認することで、マルウェア付きメールであった場合でも被害最小に抑えることができる。教育学部のメールサーバは、SquirrelMail が稼働しているので、https://minerva.edu.mie-u.ac.jp/webmail/の URL を Windows Edge に入力すれば良い。SqurrelMail が稼働していない場合は、Google の Gmail または Outlook.com メールを使って受信メールサーバを追加設定すれば、教育学部のメールサーバに届いたメールを読むことができる。お薦めは、SquirrelMail の利用であり、Gmail や Outlook.com メールを使うとクラウド先でメール中身が読まれてしまうことが起きる。特に Gmail の場合、Google が 2017 年 6 月 23 日に「Gmail」で実施していた各ユーザーのメールの中身スキャンを終了するという方針を発表したが、終了したという報告は挙がっていない。その点では、Outlook.com の方が安全である。

3.1 Outlook.com の設定の仕方

https://outlook.live.com/mail/ にアクセスし、Microsoft の無料アカウントでサインインした後、「設定」ボタンを押し、「メール」、「メールを同期」を選択する。表示される画面（図 7 参照）の中の「その他のメールアカウント」を選択する。既に使い込んでいる場合は、https://outlook.live.com/owa/ にリダイレクトされ、「設定」ボタンを押し、「接続されているアカウント」「その他のメールアカウント」を選択する。

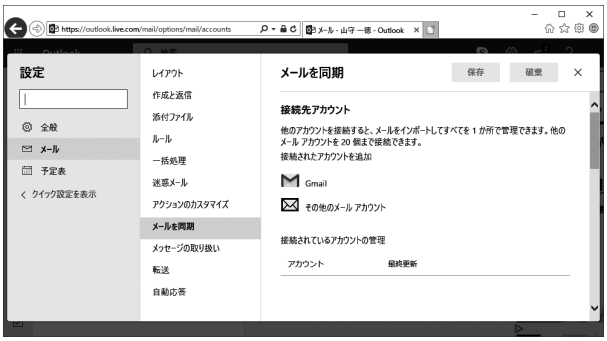

図 7「メールを同期」の画面

メールアドレスを入力する欄（図 8 参照）に、教育学部から支給されているメールアドレス、パスワードを入力する欄に、教育学部のメールサーバにログインする時のパスワードを入れる。「インポートされたメール用の新しいフォルダを 1 つ作成し、、、」にチェックを入れ、「アカウント設定を手動で構成する（POP、IMAP、または送信専用アカウント）」にチェックを入れて、「OK」ボタンを押す。表示される画面（図 9 参照）の中のユーザー名の欄は、教育学部から支給されているメールアドレスの@より左の文字列を入れる。「IMAP/SMTP 接続の設定」か「POP/SMTP 接続の設定」を選ぶ。IMAP はメールサーバにメールが残り、POP はメールが残らないのが基本的な違いであるが、「サーバーにメッセージのコピーを残す」にチェックを入れれば POP でも読み込んだ後メールが残る。POP の場合、ポート番号 995 に設定する。認証の欄を「Basic」、暗号化の欄を「SSL」とする。「Outlook.com のサーバーを使用してメールを送信する」を選択すれば、学外からメール発信ができる。

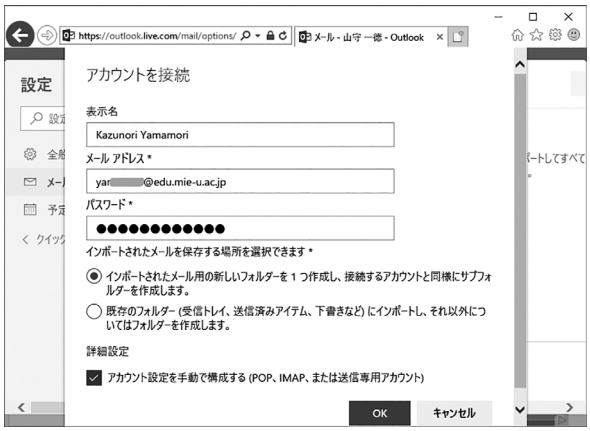

図 8　「アカウントを接続」の画面

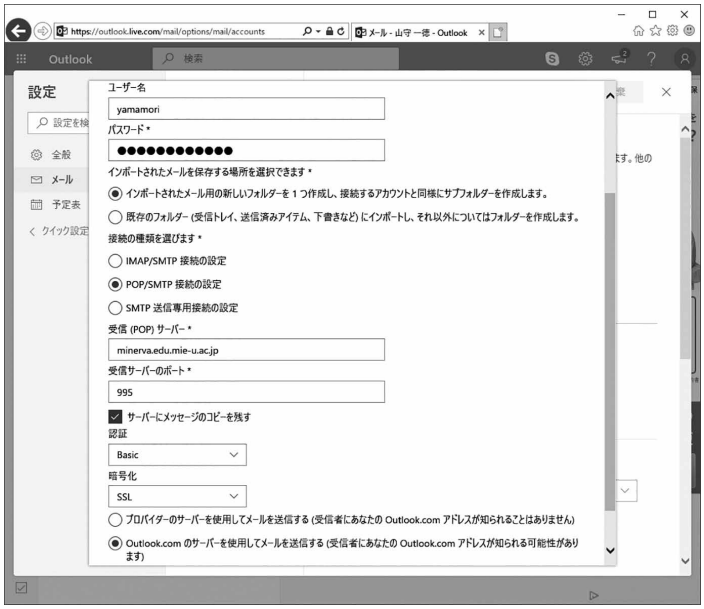

図 9　詳細設定の画面

図 7 が図 10 のように変わり、「接続されているアカウントの管理」の中に教育学部から支給されているメールアドレスが表示されていれば、追加成功。「既定の差出人アドレスを設定する」の欄は、教育学部から支給されているメールアドレスにした方が、発信した時に、From:の欄がそのアドレスとなって相手側が受け取ることができる。　以後、https://outlook.live.com/owa/で学内でも学外でも教育学部のメールサーバに届いたメールを読み（図 11 参照）、返信もできる。

3.2 Gmail の設定の仕方

https://mail.google.com/ にアクセスし、Google の無料アカウントでログインした後、「設定」ボタンを押し、「設定」を選択する。「アカウントとインポート」のタグを選択し、表示される画面（図 12 参照）の中の「他のアカウントでメールを確認」の右にある「メールアカウントを追加する」をクリックする。

現れてくるウィンドウのメールアドレスの欄に、教育学部から支給されているメールアドレスを入力し、「次へ」ボタンを押す。「他のアカウントからメールを読み込む（POP3）」にチェックを入れたまま「次へ」ボタンを押す。

現れてくるウィンドウ（図 13 参照）の「メールの取得にセキュリティで保護された接続（SSL）を使用する。」にチェックを入れ、「受信したメッセージにラベルを付ける：」にチェックを入れ短めの文字列（例えば、edu:)と入力し、POP サーバーの欄は minerva.edu.mie-u.ac.jp、ポート番号は 995、ユーザー名の欄は、教育学部から支給されているメールアドレスの@より左の文字列、パスワードを入力する欄に、教育学部のメールサーバにログインする時のパスワードを入れる。メール確認用に用いるので「取得したメッセージのコピーをサーバーに残す。」にチェックを入れる。「アカウント追加」ボタンを押すと、「これで、このアカウントからメールを取得できるようになる。

さらに yamamori@edu.mie-u.ac.jp からメールの送信もできるようにしますか？」と聞いてくるので、「はい」で答える。From:に使うメールアドレスを追加することになり、図 14 の「エイリアスとして扱います」にチェックを入れて、「次のステップ」を押すと、SMTP サーバーを指定する画面（図 15 参照）になる。ここで、SMTP サーバーの欄は、学外からでも使えるように、smtp.gmail.com を入力し、ポート番号 587 にする。ユーザー名の欄は、Google のアカウント名を入れ、パスワードは Google アカウントのパスワードを入れる。「TLS を使用したセキュリティで保護された接続（推奨)」にチェックを入れて、「アカウントを追加」のボタンを押す。メールアドレスの確認の画面（図 16 参

図 10　追加成功後の画面

図 11　届いたメール一覧の画面

図 12　「アカウントとインポート」の画面

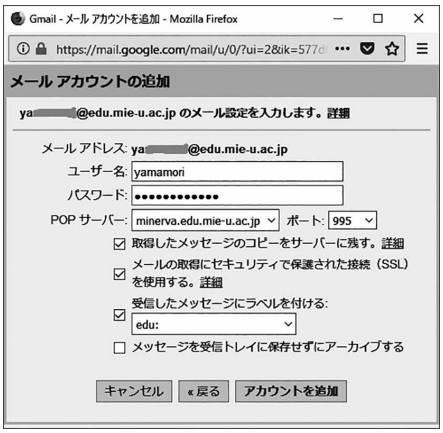

図 13　メールアカウントの追加の画面

照）が出るため、メールアドレスに送られてくる確認コードを入力する。

設定が完了した状態での、「アカウントとインポート」の画面（図17参照）は、名前：の欄の右側に、Google の無料アカウントのメールアドレスと教育学部から支給されているメールアドレスが表示され、その下の「デフォルトの返信モードを選択：」の欄では、「メールを受信したアドレスから返信する」にチェックを打った方が使いやすい。「他のアカウントでメールを確認」の欄の右側には、教育学部から支給されているメールアドレスが表示される。

図 14　アドレス追加の画面

以後、https://mail.google.com/で学内でも学外でも教育学部のメールサーバに届いたメールを読み、返信もできる。

図 15　SMTP サーバーの設定画面

４．怪しいメール確認の仕方

開くのが怪しいメールは、Application Guard の中の Windows Edge を使って、SquirrelMail か、Outlook.com メールか Gmail の URL にアクセスし、メール一覧の中から怪しいメールを開いてみる。メールの発信元メールアドレスや名前、メール本文の記述内容や、本文中に書かれている URL 等が注意するところであり、さらには、メールのヘッダーの詳細を見ると発信元のメールサーバが見えるので、そのサーバーのドメイン名も確認すると良い。co.jp でなかったり、ac.jp でない、見慣れないドメイン名は要注意である。

図 16　確認の画面

添付ファイルがあった場合は、すぐに開かずに、https://www.virustotal.com/ja/ の VirusTotal でチェックすると良いが、最新のウィルスであった場合は、VirusTotal の検出能力向上が間に合ってないため、1 週間とか待ってからチェックした方が良い。ただし、VirusTotal のサイトにチェックしたファイルの中身は見られていることに注意する。添付ファイルは、拡張子をまず確認すべきであり、そのためにも WindowsOS のエクスプローラーでファイルの拡張子が表示されない初期設定になっているのを表示する設定に変更しておいた方が良い。Windows10 の場合は、エクスプローラーの「表示」タブの中の「ファイル名拡張子」にチェックを入れておく。Windows7 の場合は、エクスプ

図 17　設定完了後の画面

ローラーの「整理」―「フォルダと検索のオプション」―「表示」タブの中の「登録されている拡張子は表示しない」のチェックを外しておく。拡張子を非表示にしていると、”abc.pdf　　.exe”というような exe の危険なファイルの場合でも気付かず、pdf ファイルと見せ掛ける手口にひっかかってしまうからである。

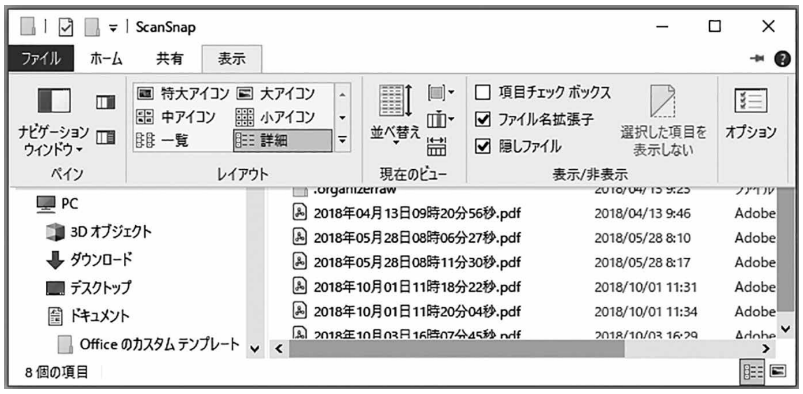

図１８　「ファイル名拡張子」のチェックを入れた画面

メールの本文の中の URL をクリックした時に、被害に遭う可能性が高いが、Application Guard は、仮想環境内だけに被害を留めてくれるため、物理環境側に実害が及ばないはずである。

Application Guard の当初の欠点は、日本語キーボードに未対応な点であった。その時には特殊文字の入力する時に苦労した。!#$%<>?は、英語キーボードとキー位置が同じなので、まだ助かるが、それ以外の特殊文字はキー位置が異なり見つけるのが大変であったが、その点は改善された。また、WindowsUpdate で起動しなくなることも置き、KB4343909　をアンインストールし KB4340917 をインストールし KB4343909 をインストールすることで復活したことがあった。

５．まとめ

Application Guard の利用は、メールを確認する時だけでなく、ネットサーフィンする時にも有効であり、日頃からインターネットサイトにアクセスする時には、Application Guard の Windows Edge でアクセスするようにした方が安全である。

Web メールの利用は、学外から教育学部から支給されているメールアドレスに届いたメールを読む時に活用できるが、お薦めの順番は、SquirrelMail ＞ Outlook.com ＞ Gmail である。後者ほど、メールの中身がクラウド会社に読まれてしまっているためである。他人に読まれて困る物を送る場合は、暗号化したファイルを添付して送る必要がある。ただし、パスワードは直後に送らないのが良い。直後のメールにパスワードが付いていることを利用するクラッキング装置が存在するからである。日頃から自分の端末内のファイルも盗まれて困る物は暗号化した状態で保存しておくことが望ましい。その習慣が身に付いていれば、USB メモリに入れる場合でも、暗号化した状態でファイルを入れることになるので、USB メモリを紛失した場合でも安全である。

ウィルス対策ソフトがパソコンにインストールされているから守られているというのは幻想である。Windows10 では、Windows Defender というウィルス対策ソフトが付随しており、その能力も高まって、良い評判が上がってきているが、無防備よりましで完璧に守り切れないと考えた方が良い。

標的型メール攻撃やパスワードクラッキング攻撃などに晒されている現状では、個々人の意識が高くないと防御が難しい。そのための手法を紹介した次第である。

参考文献

1）Windows Defender Application Guard の概要：https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-application-guard/wd-app-guard-overview（2018.10 現在）
2）山市良のえぬなんとかわーるど：https://yamanxworld.blogspot.com/2018/04/ windows-10-18031713373-wdag.html（2018.10 現在）
3）マルウェア感染の調査方法：http://www.terilogy.com/solution/apt/004a.html（2018.10 現在）