

マルウェアと詐欺を防ぐ Windows10 メッセージ対応マニュアルの開発

松澤 英之

宮崎大学 情報基盤センター

matuzawa@cc.miyazaki-u.ac.jp

Development of Manual for Windows10 Warning Message to Prevent Malwares and Internet Scams

Hideyuki Matsuzawa

Information Technology Center, University of Miyazaki

概要

最近マルウェアのダウンロード・実行、詐欺サイトへの誘導を行うメッセージが表示されることが多い。本研究ではマルウェアのダウンロード・実行、詐欺サイトへの誘導を防ぐことに特化した Windows10 向けメッセージ対応マニュアルを開発しその効果を測定した。

1 はじめに

パソコンはユーザに対して様々なメッセージを表示するが、一般ユーザがメッセージを読み、適切に対応することは非常に難しい。

宮崎大学のパソコン相談には偽メッセージに騙されてウィルスダウンロードしたり、偽サイトの誘導に従って偽サイトに掲載されている連絡先に電話してしまい相談に訪れる学生が年 1、2 人いる。また Windows10 でのライセンス管理強化に伴い OS・ソフトウェアのライセンス認証を求める警告を長期間放置して、セキュリティアップデートが適応できなかつたり、ソフトウェアがインストールできなくなつたり正常に動かなくなり相談窓口を訪れる学生が後を絶たない。相談に訪れた学生に話を聞くと警告メッセージが出ていることに気が付いたが対応を取らなかつた学生がほとんどである。

警告インタフェースに対する研究は Sankarapandian[1]ら、Sunshine[2]らや藤原ら[3]によって行なわれている。これらの研究からユーザが警告メッセージを見ない事がわかっている。そこで Sunshine らや藤原らは警告メッセージが読まれるように警告インタフェースの改良を行っている。Sunshine らの研究でユーザは警告メッセージを読んでいるが理解していないのではないかと示唆している。今までの研究では主に警告インタフェースの改良することによってユーザに対して警告メ

ッセージを読ませる研究がなされている。

では警告メッセージとはどのようなものなのか？警告メッセージが表示する内容は非常に多岐にわたり、警告メッセージの内容を理解するためにはパソコンのハードウェア、OS を含むソフトウェア、ネットワーク、サービスプロトコル、サービス内容等非常に多くの事を網羅して理解する必要がある。警告メッセージの内容を理解する事はパソコンが得意ではない一般ユーザに対しては要求が高すぎるのではないかと私は考える。学生からのパソコン相談などで聞いた話、学生が偽メッセージ、偽サイトに誘導される事例がある事および Sunshine らの研究から学生は警告メッセージの内容が理解できないので一度見た警告メッセージと同じように見える警告メッセージは再度見ないのではないかと考えられる。そこで、本研究では従来の研究の様に警告メッセージを読ませることに重きを置くのではなく、警告メッセージを画像として認識し見ることでセキュリティインシデントに遭遇しないことを目指す。具体的にはマルウェアのダウンロード・実行、詐欺サイトへの誘導などセキュリティ的に問題となる偽メッセージの発見とマルウェアのダウンロード・実行、詐欺サイトへの誘導を防ぐことができる警告メッセージの利用方法を学習するメッセージ対応マニュアルを開発する。またメッセージ対応マニュアルを学習することでどの程度警告メッセージを読むようになるか測定するために、アンケートを行う。

2 メッセージ対応マニュアル

本研究のメッセージ対応マニュアルはパソコンの習熟度がそれほど高くない一般ユーザを対象にする。一般ユーザが簡単に読めるような内容を目指すので、掲載される警告メッセージの例は Windows10 でデフォルト状態で表示される一部の警告メッセージとマルウェアのダウンロード・実行或いは偽サイトへ誘導する偽警告メッセージのみとする。また本マニュアルはマルウェアのダウンロード・実行或いは偽サイトへ誘導を防ぐことだけを目指している。警告メッセージが表示する内容に対する解説は本マニュアルの目的ではないのでインシデントを防ぐ操作ができる警告メッセージ以外の警告メッセージの内容については言及しない。

本マニュアルで取り上げる Windows10 デフォルトでの警告メッセージはパソコン起動時、ログイン画面が表示される前に表示される場合のあるブルー画面、Windows Defender SmartScreen が表示する警告メッセージ、ユーザアクセス制御が表示する警告メッセージ、Windows10 標準ブラウザ Edgeが表示する警告メッセージである。また宮崎大学向けとして宮崎大学で提供しているウイルス対策ソフト ESET ENDPOINT ANTIVIRUS の警告メッセージのうちマルウェアの除去および有害サイトをフィルタした時の警告メッセージを例示した。それ以外に IPA の安心相談窓口だより[4]で例示されている詐欺に誘導する Web 画面を例示した。

警告メッセージはパソコン操作の途中で選択、確認を促すメッセージと操作結果が正常、異常である事を表示するメッセージに分類できる。選択、確認を促すメッセージは選択、確認する際にマルウェアのダウンロード・実行或いは偽サイトへ誘導を防ぐことができる。マルウェア等ではないソフトウェアと OS が操作結果を表示するメッセージは基本的にマルウェアのダウンロード・実行或いは偽サイトへ誘導しない安全なメッセージであると考えられる。本マニュアルで明示する警告メッセージで選択、確認を促すメッセージは Windows Defender SmartScreen とユーザアクセス制御、操作結果を表示するメッセージはブルー画面、Edge と ESET ENDPOINT ANTIVIRUS である。

ブルー画面はパソコン起動時に表示される。このブルー画面が表示される理由(インシデントを

含む)にかかわらずブルー画面の内容によってさらにインシデントを誘発する可能性がないものとして安全である警告メッセージとした。同じ理由で Edge の場合も Edge 実行後に示される Edge 自らが警告メッセージは安全な警告メッセージであるとした。この警告メッセージは Edge 自身が表示するメッセージでサーバから送られ Edge が表示するいわゆるサーバサイドの警告メッセージの事ではない。一方 ESET ENDPOINT ANTIVIRUS の警告メッセージはマルウェアの除去と安全でないサイトをブロックした際に表示される画面を表示しているため、安全が確保されている状態に表示されている警告メッセージであるとした。Windows Defender SmartScreen の警告メッセージは Windows10 Windows Defender SmartScreen ドキュメント[5]に書かれているように"フィッシング詐欺対策およびマルウェア対策のサポート"機能がある。ユーザが起動したソフトウェアの名前と作成者或いは表示する Web サイトの URL を表示する。自分の起動したソフトウェア名、作成者名或いは閲覧する Web サイトの URL 名を覚えておけば実際にマルウェアのダウンロード・実行および詐欺への誘導を防ぐ可能性がある。またユーザアクセス制御の警告メッセージも Windows Defender SmartScreen と同様にアプリ名と発行者元名を表示する。そのため Windows Defender SmartScreen、ユーザアクセス制御および偽警告メッセージでマルウェアのダウンロード・実行および詐欺に誘導される可能性があるとした。

3 実験

開発したメッセージ対応マニュアルが警告メッセージを読むことに効果があるか測定するためにアンケートと警告メッセージ画面を示して安全性の有無を確認するテストを実施する。対象実験は 2019 年度後期私が担当する講義を受講する学生に対して定期的に複数回行う。初回はテストとアンケート、マニュアル表示と再度最初とテストを行う。以後マニュアル表示、テストとアンケートを行う。複数回マニュアルに対する学習を行なって習得が進むか、学習によってどのようにユーザの意識が変化するか、またどの程度の回数マニュアルを閲覧することで学習効果が出てくるかを確かめる。結果と考察は発表で行う。

参考文献

- [1] Sankarpandian, K., Little, T. and Edwards, W.K., TALC: using desktop graffiti to fight software vulnerability, Proc. ACM CHI 2008 Conference on Human Factors in Computing Systems, pp.1055–1064, 2008.
- [2] Sunshine, J., Egelman, S., Almuhiemedi, H., Atri, N. and Cranor, L.F., Crying wolf: An empirical study of SSL warning effectiveness, 18th USENIX Security Symposium, 2009.
- [3] 藤原康宏、村山優子、コンピュータ利用時の不快感を利用した警告インタフェースの提案、情報処理学会論文誌、Vol. 52、No. 1、pp77-89、2011.
- [4] 独立行政法人情報処理推進機構 安心相談窓口だより、
<https://www.ipa.go.jp/security/anshin/mgdayori20180718.html>
- [5] Windows10 Windows Defender SmartScreen ドキュメント、
<https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-smart-screen/windows-defender-smart-screen-overview>