2017 年 7 月 13 日

Office 365 の迷惑メール対策について

総合情報センター

1. はじめに

迷惑メールは、システム改ざんの危険なものから広告等のある人には有益であるが、多数の人には無意味なものまで多種多様です。総合情報センターではシステム改ざんの危険な添付ファイルは事前に可能な限り削除し、後者のような判断の難しいメールは利用者の判断で設定を変更していただく運用となります。本資料を参考にご確認をお願いいたします。

2. Office 365 のメールセキュリティ対策

Office 365 での迷惑メール対策として、「迷惑メールフォルダーに自動隔離する」ことで運用を開始しましたが、多くのメールが自動隔離の対象になることが危惧されるとともに、この状況をメールソフト（POP 受信）の利用者が確認することが難しいため、現在「迷惑メールフォルダーに移動しない」設定に既定値を変更しました。今後は、「迷惑メールを自動的にフィルター処理する」設定は、利用者の判断で変更する運用なりました。

Office 365 のメールセキュリティは、複数の対策（Office 365 ブラックリストチェック、添付ファイルの種別ブロック、ウイルス／マルウェアチェック等）が講じられており一定のレベルの対策となっております。しかし、巧妙な迷惑メールをシステムとして一定のルールで処置するには問題があり、また利用者の環境（迷惑メールの多い、少ない）によっても異なります。また、迷惑メールフォルダーを PC のメーラーソフト（Outlook, Thunderbird など）で確認することができず、Office 365 にサインインをして確認する必要があります。

また、メール本文には、各種情報提供サイトを紹介（誘導）する URL(Uniform Resource Locator: Web サイトへのリンク)が記入されてことが多くなり、これをクリックすることによりアクセスしたサイトが有害なサイトの場合、知らぬ間に好ましくプログラムを仕込まれる危険性が生じます。このため、Office 365 のセキュリィの一つとして、この URL が検査（完璧ではない）する設定（URL Safe-Link）が既定値では有効となっています。この設定についても利用者の希望で除外することを可能とする運用とします。

迷惑メール等の運用に関する 2 つの事項について、利用者の判断の設定に委ねる運用とすることとなりました。

	対策	備考
Office365 システム既定値	A) 送信ドメインのブラックリストチェック	・NDR の送信
	B) 添付ファイルの種別ブロック(exe 等)	・添付ファイルの削除を行い、その旨をメール通知
	C) 添付ファイルのウイルス／マルウェア検査	・添付ファイルの削除を行い、その旨をメール通知
	D) URL Safe-Link 検査	・除外したい場合はセンターへ届出
利用者の設定	E) 迷惑メール：「迷惑フォルダー」への移動	・システム既定値は「移動しない」

NDR: Non-Delivery Receipt/配信不能メール

3. 「迷惑メールを自動的にフィルター処理する」と変更した場合

以下のような設定値で、迷惑メールと判断されたメールが、[受信トレイ]フォルダーではなく[迷惑メール]フォルダーに自動的に配信されます。[迷惑メール]フォルダーは、PCのメールソフトの受信対象とはなりません。

なお、[迷惑メール]フォルダーに配信されたことの通知メールはありませんので、定期的に確認し、必要であればリリース処理、また不要なメールは削除してください。

<u>迷惑メール処理のポリシー</u>

A) 「迷惑メール」、「高確度迷惑メール」、「フィッシング詐欺メール」、「バルクメール」: → メッセージを[迷惑メール]フォルダーに移動する

B) 一括しきい値： 9（1～9）「1」は殆どのバルクメールをスパムと判断、「9」は逆に殆どのバルクメールをスパムと判断しない。

以下の設定は、各利用者個別の設定となります。

■ リリース処理と「信頼できる差出人と宛先リスト」の登録

登録した送信者またはドメインからのメールは[迷惑メール]フォルダーに移動しません。

なお、[迷惑メール]フォルダーのメール確認において、迷惑メールでないメールを「このメッセージはスパムではありません。」をクリックするとその送信者のメールアドレスがこのリストに追加登録されます。また、対象のメールが[迷惑メール]フォルダーから[受信トレイ]フォルダーに移動されます。

■ 「受信拒否リスト」の設定

設定した送信者またはドメインからのメールは無条件で[迷惑メール]フォルダーに移動されます。

なお、[受信トレイ]フォルダーで「購読を解除できます」という表示あるメールについて、この部分をクリックすると対象アドレスが「受信拒否リスト」に登録され、対象メールは[削除済み]アイテムフォルダに移動されます。

[参考]

- 迷惑メールとは

  迷惑メールメッセージは"スパム"メッセージで、サービスによってフィルター処理される未承諾(かつ通常は不要な)電子メールメッセージです。既定で、サービスは、送信元の IP アドレスの評価に基づいてスパムメッセージを拒否します。ただし、そのメッセージが IP 検査を通過しても、コンテンツフィルターでスパムに分類された場合は、宛先になっている受信者の迷惑メールフォルダーに送信されます。

- バルクメールとは

  グレーメールとも呼ばれるバルクメールは、分類がより困難な電子メールメッセージのことです。迷惑メールは「常にある脅威」であるのに対して、バルクメールは、通常、繰り返し送られてくるわけではない広告メッセージまたはマーケティングメッセージで構成されます。バルクメールは一部のユーザーによって要求されたものであり、事実、彼らは意図的にそれらのメッセージの受信を申し込んでいるのに対して、それ以外のユーザーはその種のメッセージをスパムと見なしています。たとえば、一部のユーザーは Contoso Corporation からの広告メールまたは次回のサイバーセキュリティに関するカンファレンスの招待状を受信したいと思っているのに対して、その他のユーザーはそのような電子メールをスパムと見なしている場合です。

- バックスキャターとは

  バックスキャターメッセージは、通常、スパムを受信した結果としてメールサーバーから送信される自動バウンスメッセージです。Exchange Online Protection(EOP)はスパムフィルタリングサービスのため、存在しない受信者やその他の疑わしい宛先への電子メールメッセージがこのサービスによって拒否されます。これが発生すると、EOP が配信不能レポート(NDR)メッセージを生成して、「送信者」に配信します。スパム送信者はメッセージ内で偽造したまたは無効な"差出人"アドレスを使用することが多いため、NDR が送信される送信者アドレスが原因でバックスキャターメッセージになる場合があります。この場合は、EOP ネットワークに関連付けられた送信サーバーがバックスキャターDNS 禁止リスト(DNSBL)に掲載される可能性があります。バックスキャターDNSBL はバックスキャターメッセージを送信する IP アドレスのリストです。スパム送信者のリストではないため、掲載されたサーバーがバックスキャターDNSBL から削除されることはありません。

4. 添付ファイルの種別ブロック、ウイルス／マルウェア（サンドボックスでの挙動検査）対策とメール本文中の URL の Safe Link 検査

(ア) 種別ブロック

ブロック対象のファイル識別子（.exe 等）を持つ添付ファイルは削除され、送受信者に削除した旨のメッセージが本文あるいは添付ファイルで通知されます。

添付ファイルに送信が禁止されたファイルが検出されましたので、すべての添付ファイルを削除しました。ファイル宅配便での送信をお願いいたします。

削除された添付ファイル名

(イ) ウイルス／マルウェア（サンドボックスでの挙動検査）対策

既知のウイルスと判断された添付ファイル、仮想環境で実行し挙動が怪しい添付ファイル（マルウェア）を削除し、本文にその旨のメッセージ追加し、受信トレイに配信します。なお、暗号化された添付ファイルは、検査の対象外です。

Virus/Malware was deleted save attachments in one or more attachments included with these mail message.
Action: All attachments have been removed.

(ウ) URL の Safe Link 検査

メールの添付ファイル以外のウイルス／マルウェアの侵入経路には、Web サイトの閲覧時に送送り込まれる場合があります。この対策として、記述されたサイトが「悪意のあるサイト等」のブラックリストに登録されているかの検査を行う仕組みです。ただし、*.chubu.ac.jp を送信者とするメールおよび一部の*.chubu.ac.jp サイトは、対象外とします。

安易に URL をクリックし、対象サイトが表示された時点でマルウェアをダウンロードする危険性を緩和するもので、本来の URL が検査用情報に置き分かります。この点がメールの確認には慣れないとデメリットです。また、置きかえられた URL 内に受信者のメールアドレスを容易に推測できる情報が追加されます。再々転送時に受信者のメールアドレスが通知される。

URL をクリックした後、対象の Web サイトが有害と分類されたものであれば、注意のポップアップ画面が表示されます。以後の処理は利用者の判断に委ねられ、「この Web ページを閉じます」あるいは「この Web ページに進みます（お勧めできません）」の選択となります。

[例] 6：Amazon ギフト券 5000 円が当たる「Windows10」に関する読者調査

https://apac01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.keyman.or.jp%2Fpd%2F10032217%2F%3Fml%3Dd20170622&data=02%7C01%7Ct???isc.chubu.ac.jp%7Ce31fdh6s3e5674777ebe708d4b8f153ef%7Cb758546664gt7NrRXZEbYP3gKSkfoshj5cGrjAI8NAIJlSL7IBk%3D&reserved=0

置き換えられる前の標記

http://www.keyman.or.jp/pd/10032217/

・実際の受信メールの例（詐欺 Web サイト）

URL の置き換え表示は、メールのメッセージ形式（テキスト／HTML 形式）およびメールソフトの表示設定等によっても異なります。

右図は上から、OWA Outlook、Thunderbird のプレーンテキスト表示形式、Thunderbird のオリジナル HTML 表示形式の表示例です。

なお、URL の検査で有害サイトとして分類された場合は、右のような注意画面が表示されます。

以上