第 15-19-343 号
2015 年 12 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「ウイルス感染を目的としたばらまき型メールに引き続き警戒を」
～新たな攻撃の兆候を察知するための情報提供受付専用メールアドレスを新設～

2015 年 10 月の 8 日、27 日、30 日の各日において、実在する組織からの注文連絡等を装った添付ファイル付きメールが不特定多数の宛先に届くという事象が確認されました。IPA にも多くの相談が寄せられ、相談の内容や情報提供からウイルス感染を目的としたばらまき型メールであると判断し、注意喚起[*1]を行っています。

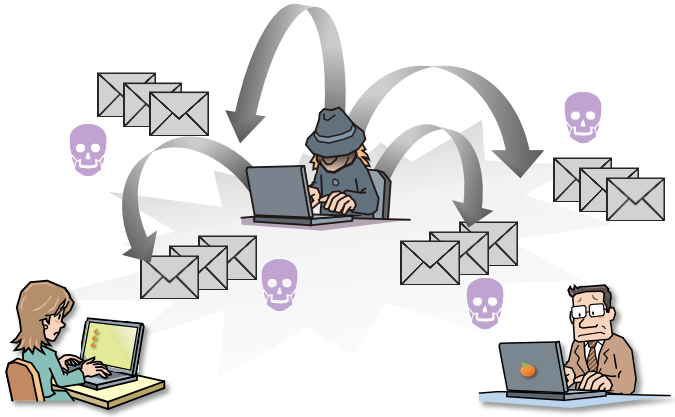

図 1：ウイルス感染を目的としたばらまき型メールが大量に送信される被害が発生

このメールは実在する組織を装い、本文に不自然な言い回しがないなど、その**内容に不審な箇所を見い出しにくい点や添付ファイル（ウイルス）がセキュリティソフトで検知できない点等、標的型攻撃の手口と似ています**[*2]。実際、相談者が受信したメールには複数のパターンがありましたが、いずれも「添付ファイルを開いてしまった」という相談が寄せられています。このことから、特に不審をいだかずに添付ファイルを開いてしまう巧妙なタイトル、文面のメールであることが伺えます。

11 月以降、IPA では同様の被害を確認していませんが、今後もウイルス感染を目的とした巧妙な内容のメールがばらまかれる可能性は十分にあります。今月の呼びかけでは、このばらまき型メールについて、IPA が確認した手口と今後注意すべき点および対策について紹介します。

（1） ばらまき型メールの特徴

相談および情報提供の内容を IPA で確認したところ、ばらまき型メールには次のような特徴がありました。

*1 【注意喚起】特定の組織からの注文連絡等を装ったばらまき型メールに注意
https://www.ipa.go.jp/security/topics/alert271009.html
*2 IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」
https://www.ipa.go.jp/security/technicalwatch/20150109.html

① メールの内容（件名や本文）

実在の組織を騙ったり、FAX や複合機の自動送信を装った内容のメールでした。特に組織を騙ったメールの場合、日本語に不自然な表現もなく、一見では、不審をいだきにくい内容となっていました。

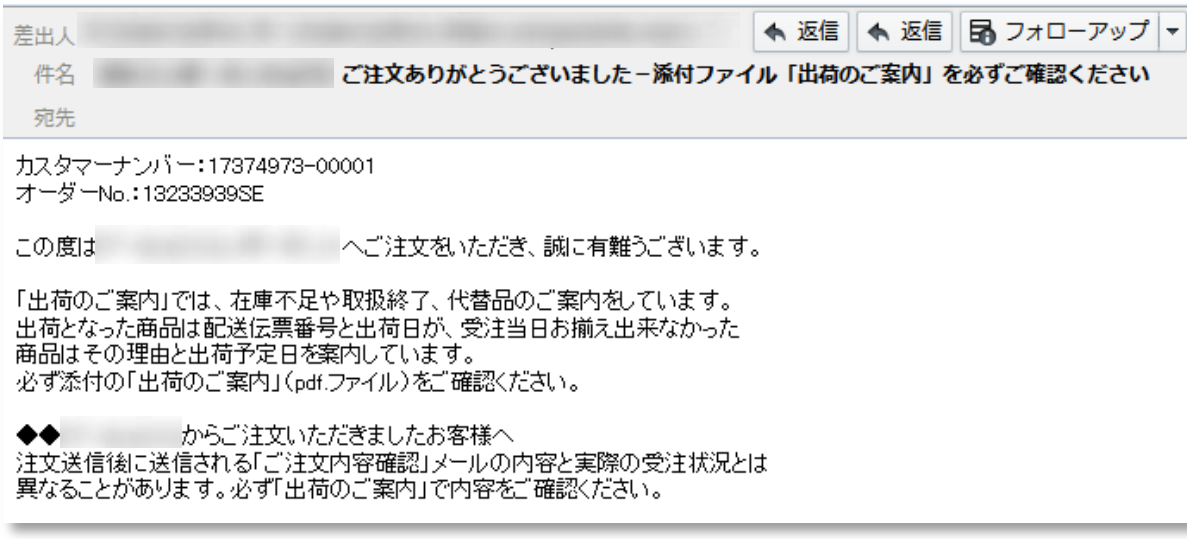

図２：実際に送信されたばらまき型メールの例

② 添付ファイル

別のウイルスをインターネットからダウンロードし、実行（感染）させるマクロ[*3]が仕掛けられた Word ファイルが添付されていました。この Word ファイルを開き、さらにマクロを有効にする（図３の「コンテンツの有効化」をクリックする）とウイルスに感染してしまいます。

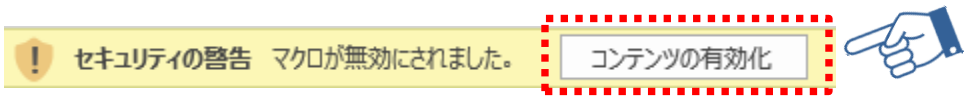

図３：マクロが組み込まれたファイルを開いた際のセキュリティ警告

また、インターネットからダウンロードされる際のファイル名（通信ログに記録される情報）と、ダウンロード完了後に端末に保存されるファイル名が異なるという特徴もありました。

（２） ばらまき型メールの今後の動向

下記はこれまでに IPA で確認しているばらまき型メールを、送信日、件名、添付ファイル名の情報で分類したものです。

*3 マクロ：あらかじめ必要となる操作手順を設定しておき、作業の効率化・自動化が図れる機能。

■10/8 に送信されたメール

No.	件名	添付ファイル名
1	【●●●●（実在の組織名）より】ご注文ありがとうございましたー添付ファイル「出荷のご案内」を必ずご確認ください	1312061102_13233939SE.doc
2	Message from "RNP0026738E40D2"	20151007112034511.doc

■10/27 に送信されたメール

No.	件名	添付ファイル名
3	タンケンー請求書(小)の件です。	10280.doc
4	請求書	2610-099189.doc
5	ファックス受信完了: Fax Received	2F4A8C1B-9DB6-4749-AA9C-9ED67A419132-574-IF.doc

■10/30 に送信されたメール

No.	件名	添付ファイル名
6	●●（実在の組織名）様宛請求書をお送りします	2015-10-29-002903.doc
7(*4)	タンケンー請求書(小)の件です。	102911.doc

これまでに確認しているのは、上記のように Word ファイルが添付されたメールです。しかし、ウイルス感染させるためのマクロを実行させることが出来るファイルであれば、必ずしも Word ファイルである必要はありません。実際、内容は英文であるものの、ウイルス感染させるためのマクロが仕掛けられた Excel ファイルが添付された、ばらまき型と推測されるメールも IPA で確認しています。

なお、IPA に寄せられた相談では、上記のうち 1 つのメールのみを受信していたケースや 2～3 通の複数のメールを受信していたケースを確認しています。また、PDF ファイルに偽装した実行形式のファイル（PDF のアイコンで表示される exe ファイル）が格納された zip ファイルが添付されていたという別の相談もありました。

一連の関係性や詳細は不明ですが、今後も同様の手口のメールがばらまかれる可能性があり、注意が必要です。ウイルス感染被害に遭わないためにも、次に述べる対策を確認、実施してください。

（3） ばらまき型メールによってウイルス感染しないための対策

ウイルス感染を目的としたメールへの対策としては、従来通り、**不用意に添付ファイルを開かない、リンクをクリックしない等といった手段が有効**です。さらに、今回のばらまき型メールの手口から考えると、下記のような対策も必要です。

- **マクロが自動で有効になるような設定は行わない。**
- **安全性が不明なファイルではマクロを有効にするための「コンテンツの有効化」を絶対クリックしない。**

*4 No.3 と件名は同一ですが、添付ファイルが異なります。

また、今回のばらまき型メールに関する相談の多くは組織から寄せられたものでした。組織においては、ウイルス感染による組織運営への被害を回避するため、下記のような対策が有効です。

・ウイルス感染の影響がない環境（万が一、ウイルスに感染しても組織運営への支障を最小限に留められる端末等）で添付ファイルを開く。
・必要に応じて、添付ファイル（メール）の送信者に対して送信有無を確認する。

なお、結果的に開いてしまったメールの添付ファイルが不審であったことに気付いた場合は、次のような対応を推奨します。

1. 当該端末をネットワークから切り離す（LAN ケーブル抜線や無線 LAN 機能の無効化）
2. セキュリティソフトでウイルススキャンを実施する
3. 必要に応じて、スキャン結果や開いてしまったファイルの情報、セキュリティソフトの定義ファイルの情報等をまとめてセキュリティベンダに相談する
4. 通信ログを確認（監視）する
5. ウイルス感染が確認できた場合は当該端末の初期化または保全を検討する[*5]

（4） 情報提供受付専用メールアドレスの新設

今回のばらまき型メールのような新たな手口による攻撃の出現に備え、その兆候を察知する目的として、この度、情報提供受付専用メールアドレスを新設しました。[*6]

【情報提供受付専用メールアドレス】
teikyou@virus.ipa.go.jp

受信したメールやアクセスしたサイトにおいて、不審な内容を確認できた場合には、上記のメールアドレスに情報提供をお願いします。なお、本メールアドレスは情報提供受付専用となりますので、ウイルスや不正アクセスによる被害が疑われ、相談の必要がある場合にはこれまでと同様に情報セキュリティ安心相談窓口[*7]までご連絡ください。

■お問い合わせ先
情報セキュリティ安心相談窓口
Tel: 03-5978-7509　Fax: 03-5978-7518
E-mail: anshin@ipa.go.jp
技術本部セキュリティセンター 加賀谷／野澤

*5 セキュリティソフトによる駆除ができた場合でも、感染端末に未知のウイルスが残されている可能性がゼロとは言えないため、安全な利用のためには初期化が推奨されます。また、ウイルス解析のためには感染したままの状態で保全することが望ましい場合もあります。
*6 情報提供受付について
https://www.ipa.go.jp/security/teikyou/index.html
*7 情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/index.html