【参考資料】

DDE(※)を悪用した攻撃手口に関する注意点

2018年1月26日

IPA 独立行政法人**情報処理推進機構**
技術本部 **セキュリティセンター**

※ Dynamic Data Exchange の略。

はじめに

2017年10月頃から、Microsoft OfficeのDDE（Dynamic Data Exchange）という機能を悪用した手口の攻撃が観測されています。
本資料は、「DDE」を悪用した攻撃手口について紹介し、注意点を説明するものです。（この攻撃手口は、従来より多く観測されているマクロ機能の悪用とは異なるものです）

本資料では、次の2つの攻撃手口の事例を紹介します。

- 事例１：罠が仕込まれたWord文書ファイルのパターン
- 事例２：罠が仕込まれたOutlookメールのパターン

本資料をもとに、攻撃の手口について知っていただくとともに、不審なメールや、不審な添付ファイルに対して警戒いただくようお願いいたします。

概要

DDE（Dynamic Data Exchange）とは

- DDEは、Windows環境において、複数のソフトウェア間で通信を行う技術です。

DDEを悪用した攻撃の状況

- DDEを悪用した攻撃について、2017年10月に攻撃手口の情報が公開されました。10月19日にはランサムウェアの感染を意図した攻撃に使われ（※1）、さらに、日本国内の標的型攻撃にも使われた形跡が確認されています。
- Microsoft社も、2017年11月9日付で本件に関する注意と緩和策を提示するセキュリティ情報を公開しています（※2）。
  - なお、2018年1月9日、Microsoft WordとExcelについて、更新プログラムの適用（Windows Update）により、本攻撃手口で悪用されているDDEの機能が無効化される（※3）ようになり、本攻撃手口が動作しなくなったことを確認しています。

※1: Necurs Botnet malspam pushes Locky using DDE attack（SANS ISC）
https://isc.sans.edu/forums/diary/Necurs+Botnet+malspam+pushes+Locky+using+DDE+attack/22946/
※2：マイクロソフトセキュリティアドバイザリ 4053440（マイクロソフト）
https://technet.microsoft.com/ja-jp/library/security/4053440.aspx
※3：ADV170021 | Microsoft Officeの多層防御機能の更新プログラム（マイクロソフト）
https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/ADV170021

本資料で紹介する事例の特徴

- 現時点で確認している、「DDEを悪用した攻撃の手口」による攻撃には次のような特徴があります。

特徴

① メールに添付されたWord文書ファイルを開いたり、Outlookでメールを開くと、『リンクされたデータで文書を更新する』旨の**警告ウインドウ**が表示される。

② 上記①の警告ウインドウで「はい」を選択すると、『遠隔データへのアクセスができないため、アプリケーションを起動する』旨の**警告ウインドウ**が表示される。

⇒ ②の警告ウインドウで「はい」を選択してしまうと、**ウイルスに感染させられてしまう。**

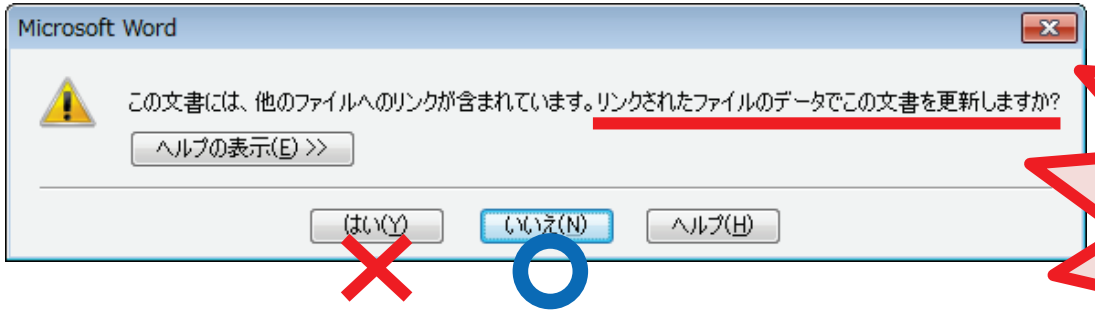
次のページに、実際の警告ウインドウを示します。

※本資料では、Microsoft Office 2016 の画面で説明しています。
バージョンにより、表示される警告画面等は異なる場合があります。

対応方法

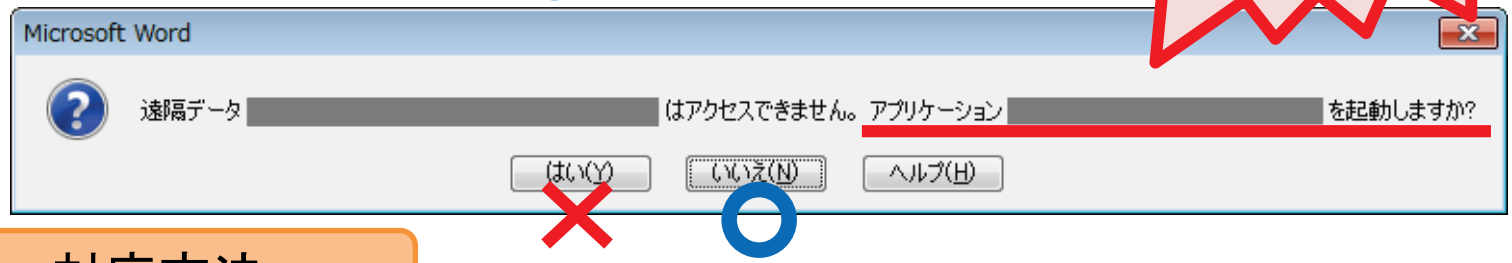
- DDEを悪用した攻撃にはいくつかのパターンがありますが、次の警告ウインドウが表示された場合で、閲覧中のメールやファイルが安全なものであると確証がない限り、「いいえ」を選択してください。

①



危険！
「はい」はクリックしない！

②



対応方法

上記の特徴にあてはまる、身に覚えのないメールを受信した場合、操作を中断し、**システム管理部門等へ連絡**してください。
（警告ウインドウで「いいえ」を選択した場合は、ウイルスに感染しません）

次のページからは、実際の悪意のある攻撃を例にして説明します。

事例1－(1)

- メール等で送られた、罠が仕込まれたWord文書ファイルを開いた場合

① Word文書ファイルを開くと、警告ウインドウが表示されます。
→**「いいえ」をクリックすることで攻撃を回避できます。**

［次ページへ続く］

事例1－(2)

- 前ページの警告ウインドウで「はい」を選択してしまった場合

② アプリケーションの起動を確認する警告ウインドウが表示されますが、ここで「はい」をクリックすると、ウイルスがダウンロードされ、感染させられてしまいます。
→ **「はい」はクリックしないでください。**

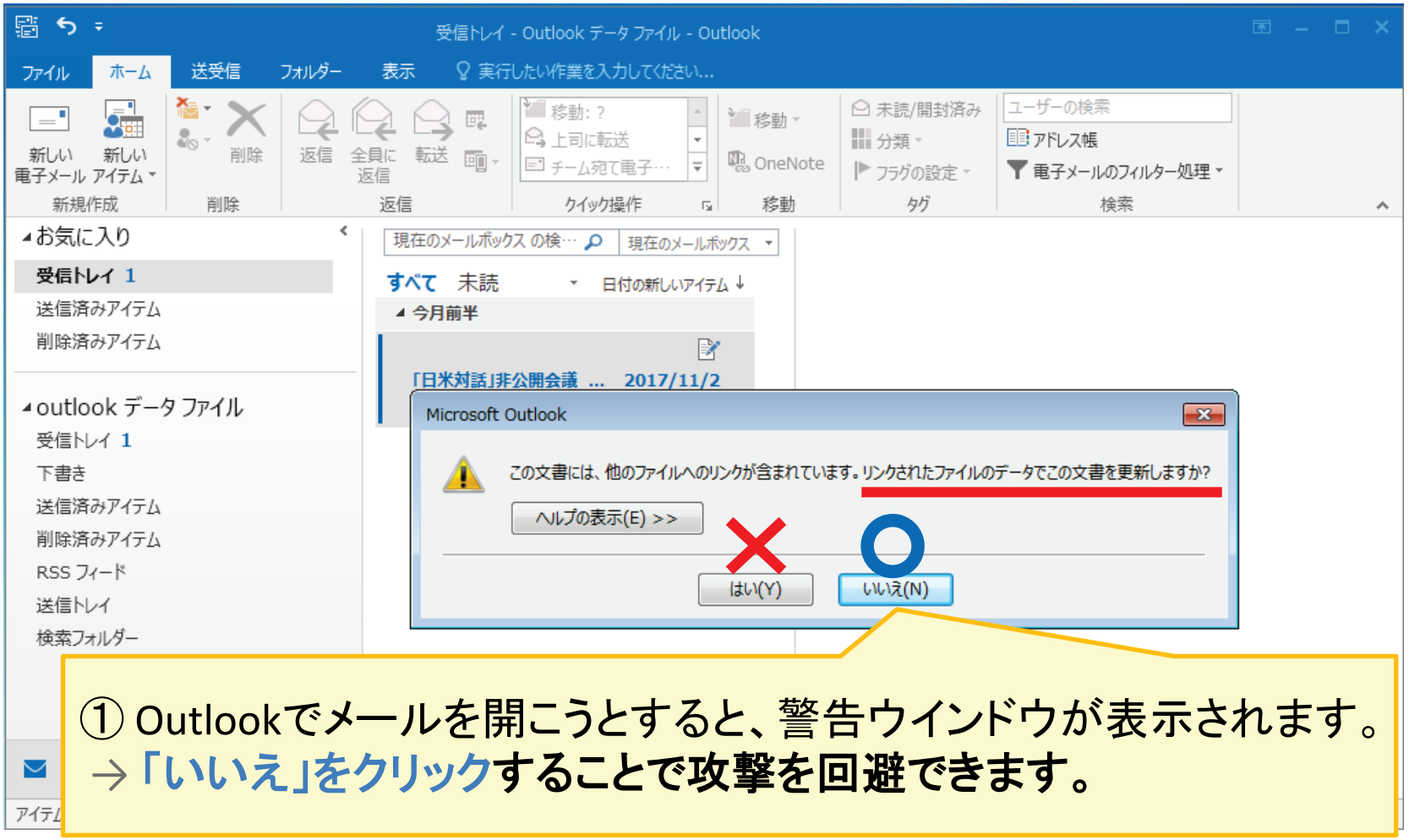
［次ページへ続く］

事例1－(3)

- メールに添付されている状態から、添付ファイルを開いた場合

事例2－（1）

- 罠が仕込まれたメールをOutlookで開いた場合

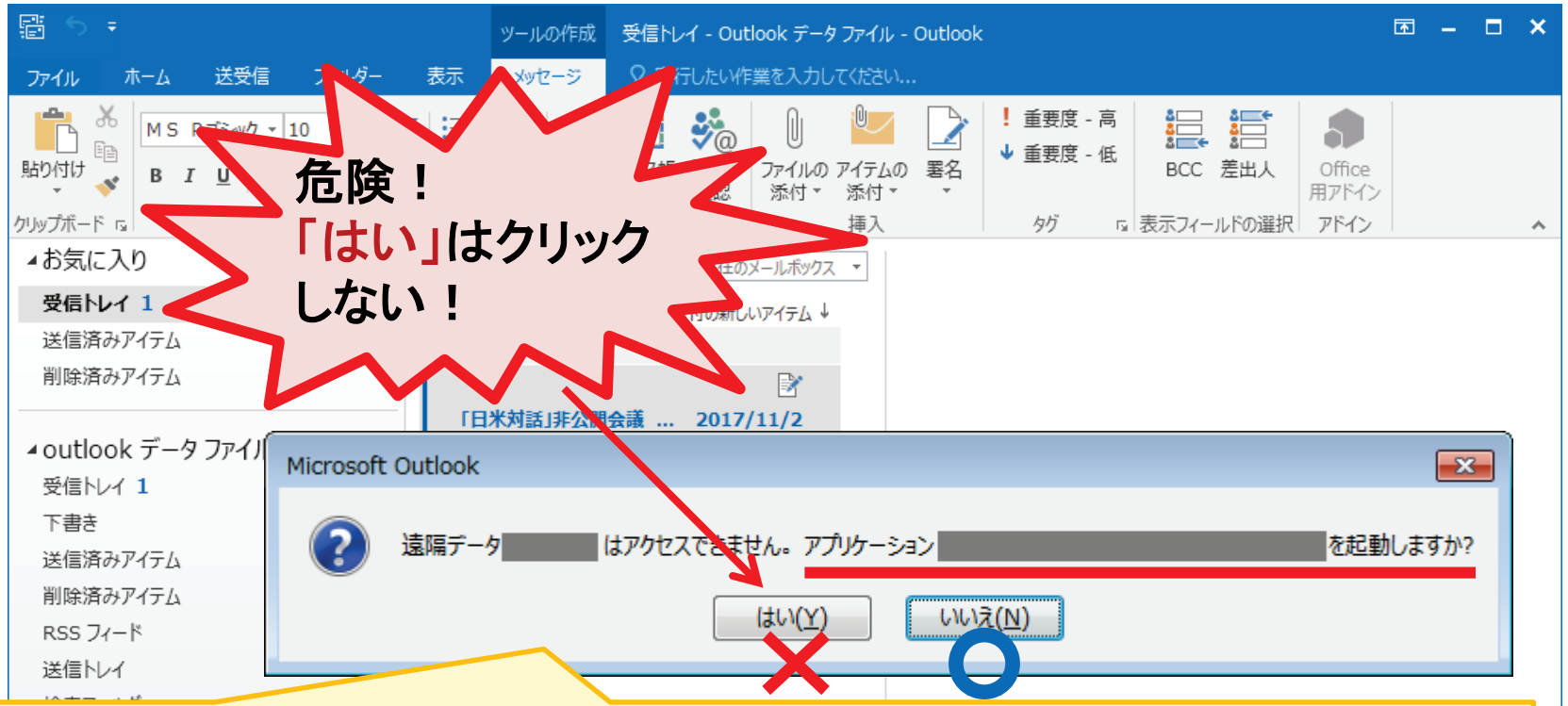


① Outlookでメールを開こうとすると、警告ウインドウが表示されます。
→「いいえ」をクリックすることで攻撃を回避できます。

［次ページへ続く］

事例2－（2）

- 前ページの警告ウインドウで「はい」を選択してしまった場合



② アプリケーションの起動を確認する警告ウインドウが表示されますが、ここで「はい」をクリックすると、ウイルスがダウンロードされ、感染させられてしまいます。
→ **「はい」はクリックしないでください。**

おわりに

本資料で説明した警告ウインドウが表示された場合は、安易に「はい」をクリックしないでください。また、身に覚えのないメールや添付ファイルを開いてしまった場合は、**すぐにシステム管理部門等へ連絡**してください。

本資料で説明したタイプの攻撃のほかにも、Microsoft Officeの機能を悪用したウイルスが存在します。

これらのウイルスに感染しないよう、次のような基本的なウイルス対策を行ってください。

- ✓ **不審なメールの添付ファイルは開かない。**
- ✓ **OSやアプリケーション、セキュリティソフトを常に最新の状態にする。**
- ✓ **信頼できないメールに添付されたWord文書やExcelファイルを開いた際にマクロに関する警告が表示された場合、「マクロを有効にする」、「コンテンツの有効化」というボタンはクリックしない。**
- ✓ **メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、警告の意味が分からない場合は操作を中断する。**