【参考資料】

OneNote形式のファイルを悪用した攻撃の手口と対策

2023年5月

IPA 独立行政法人情報処理推進機構
セキュリティセンター

はじめに

Microsoft OneNote形式のファイル(拡張子 .one)を悪用し、悪意のあるファイルを実行させることで、ウイルスに感染させる攻撃を公開情報より確認しました。
本資料では、本攻撃の手口と対策について説明します。

【参考情報】

● Microsoft OneNote とは

Microsoft社が提供するデジタルノートアプリです。OneNoteでは、作成したノートへの文字入力のほかに、画像やファイルを添付すること等が可能です。ノートを拡張子「.one」のファイルとして保存することができ、次のようなアイコンです。

※ 本資料では、Office 2021の画面を用いて説明しています。
バージョンにより、表示されるアイコン等は異なる場合があります。

本資料をもとに、本攻撃の手口と対策を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。

攻撃手口

OneNote形式のファイルを悪用した攻撃の手口

1. 攻撃者は、OneNote形式のファイル（※1）を添付したメールを受信者に送り付けます。
2. メール本文に、添付ファイルの開封を促す内容(※2)を書くことで、受信者に添付ファイルをOneNoteで開かせます。
3. 表示されるノートに、ボタンや文書ファイルのアイコン(※3)をクリックするように促す指示を書くことで、受信者にノートの特定の位置をダブルクリックさせます。
4. ノートに埋め込んだ悪意のあるファイルが実行(※4)され、受信者のコンピュータをウイルスに感染させます。

(※1) ファイル名は、請求書や配達通知、注文書等に関係するものを確認しています。
OneNote形式のファイルを格納したZIP形式のファイルが添付されている場合もあります。
(※2) 添付ファイルの開封を促す内容が、書かれていない場合もあります。
(※3) 本物のボタンや文書ファイルではなく、ボタンや文書ファイルに模した画像です。
(※4) 悪意のあるファイルの実行前に、OneNoteのセキュリティ警告が表示されます。

観測状況

OneNote形式のファイルを悪用した攻撃の観測状況

- 2023年1月、本手口を用いた攻撃メールを初観測しました(事例①)。
- 2023年3月、本手口を用いたEmotetへの感染を企図する攻撃メールを観測しました(事例②)。
  観測した複数のメールでは、**件名・本文が日本語で書かれたメールを確認**しています。

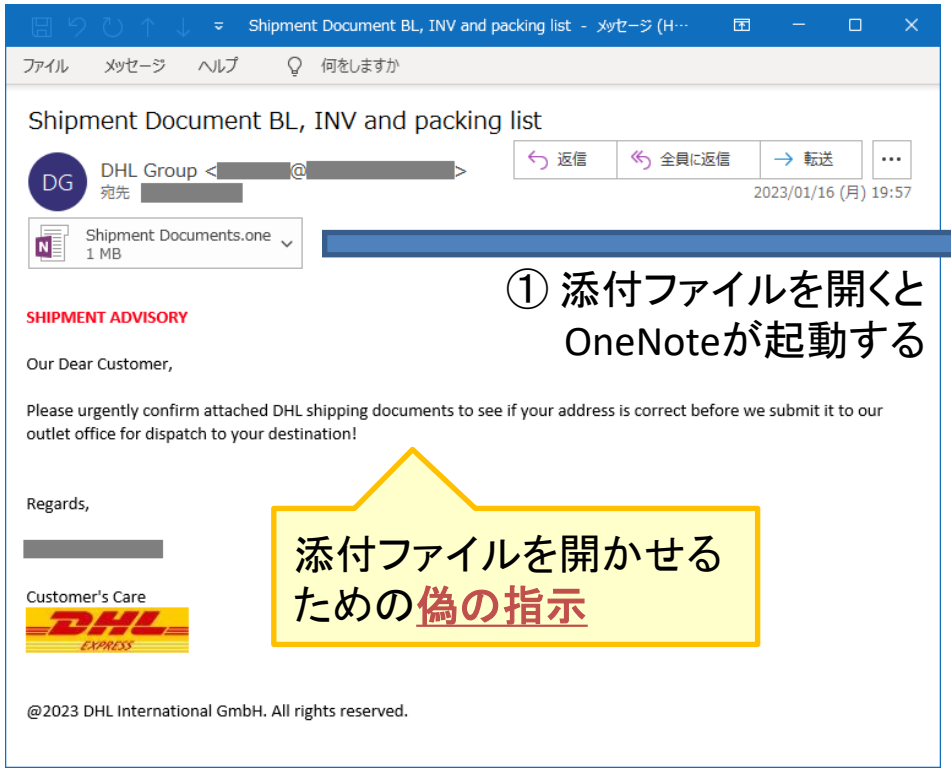
注意点

本手口は、**Emotetに限らず他の攻撃でも悪用されている**との情報があります。引き続き、**さまざまな攻撃で悪用される可能性があるため注意が必要です**。
また、本手口は**「保護ビュー」での閲覧を行ったとしても防ぐことはできません**。表示される**警告画面をよく読み、不用意にOKボタンをクリックしない**よう注意してください。

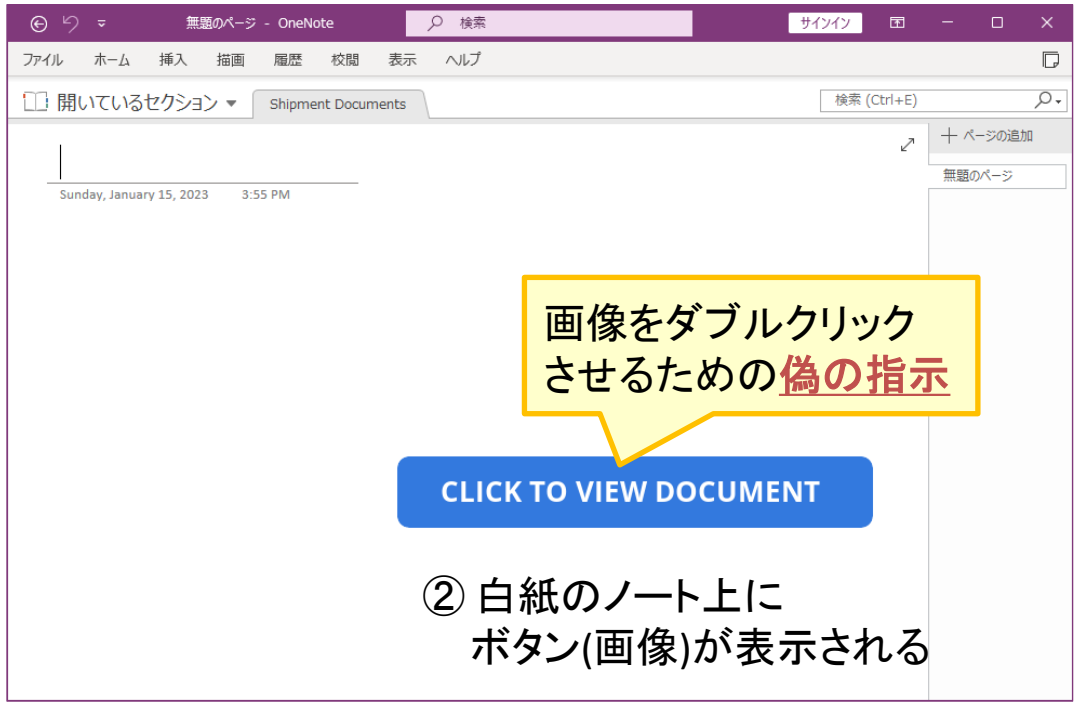
次のページからは、事例①②を含む攻撃の事例を4つ紹介します。

事例①

本事例は、2023年1月に観測した攻撃メールです。メールに添付されたOneNote形式のファイルを開くと、白紙のノート上に、「CLICK TO VIEW DOCUMENT」と書かれたボタンに模した画像が表示されます。



① 添付ファイルを開くとOneNoteが起動する



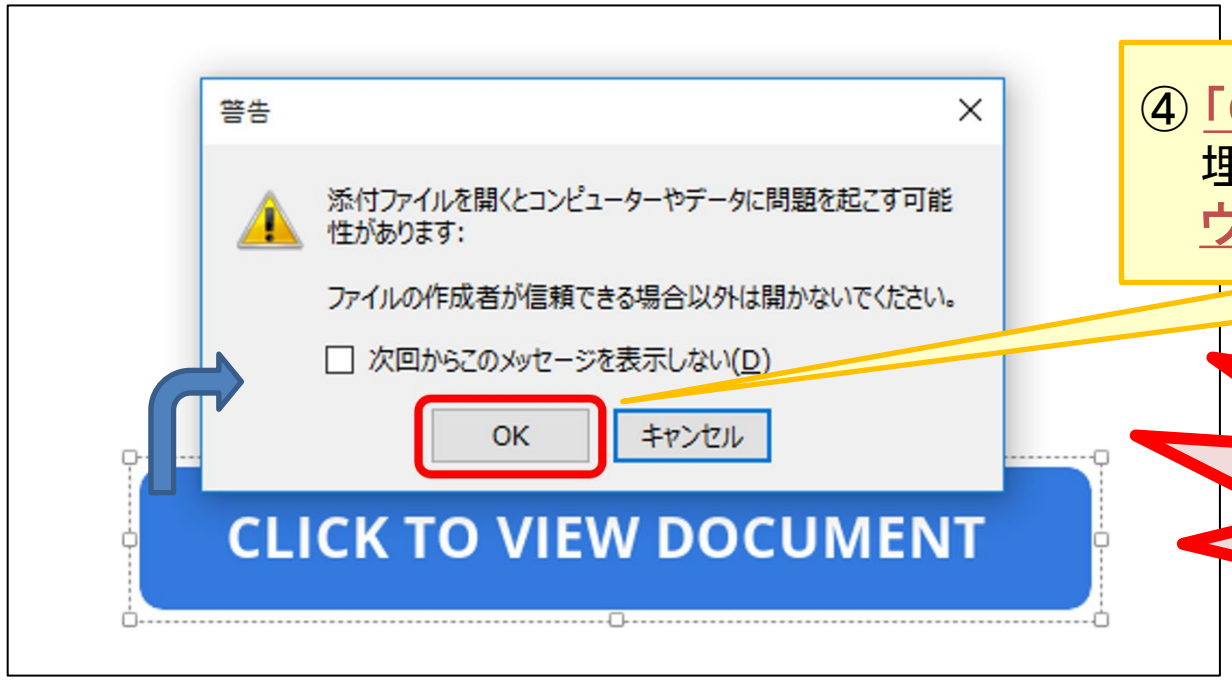
② 白紙のノート上にボタン(画像)が表示される

[次ページへ続く]

事例①

ノート上の「CLICK TO VIEW DOCUMENT」と書かれた画像をダブルクリックすると、OneNoteのセキュリティ警告が表示されます。表示された警告画面で「OK」ボタンをクリックすると、ウイルスに感染してしまいます。

③「CLICK TO VIEW DOCUMENT」と書かれた
画像をダブルクリックすると警告が表示される

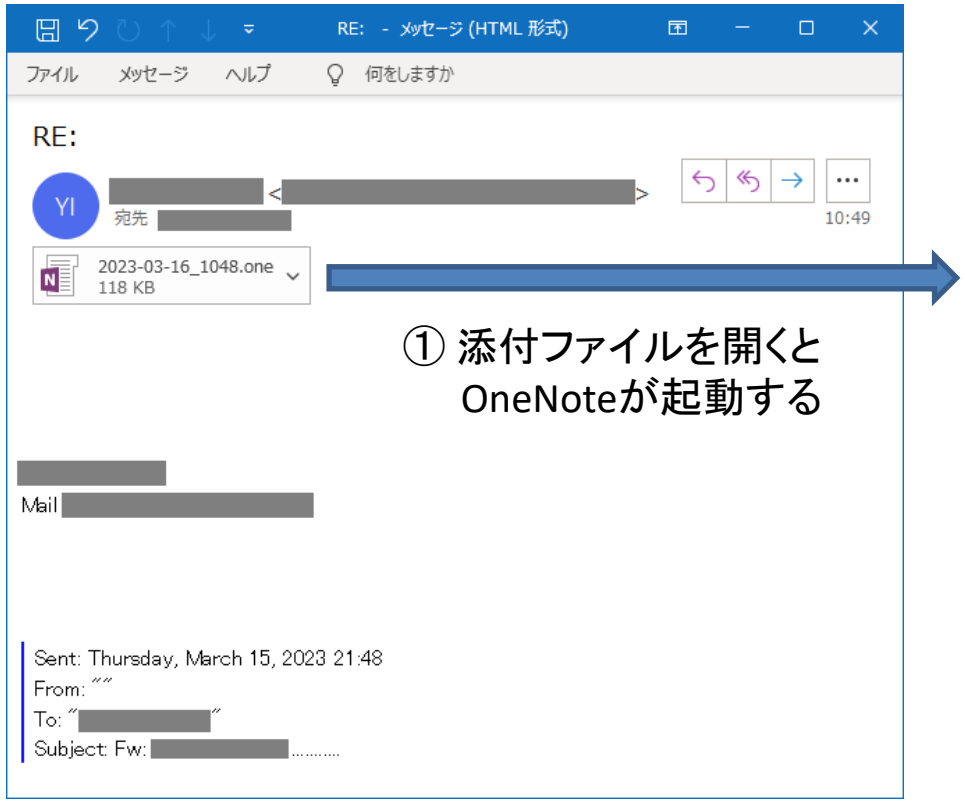


④「OK」ボタンをクリックしてしまうと、ノートに埋め込まれた悪意のあるファイルが実行され、ウイルスに感染してしまう。

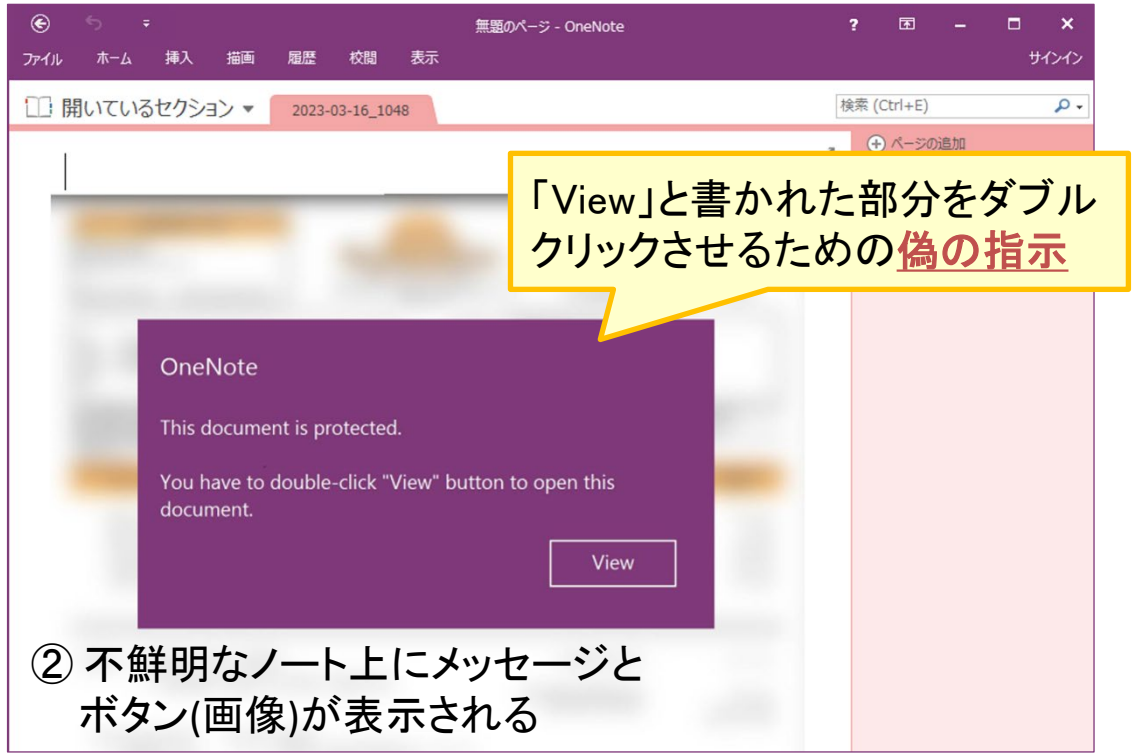
「OK」ボタンはクリックしない！

事例②

本事例は、2023年3月に観測した、Emotetへの感染を企図する攻撃メールです。メールの添付ファイルを開くと、不鮮明に表示されたノート上に、ノートの内容を閲覧するために「View」ボタンをダブルクリックするように促すメッセージと、「View」ボタンに模した画像が表示されます。



① 添付ファイルを開くと
OneNoteが起動する



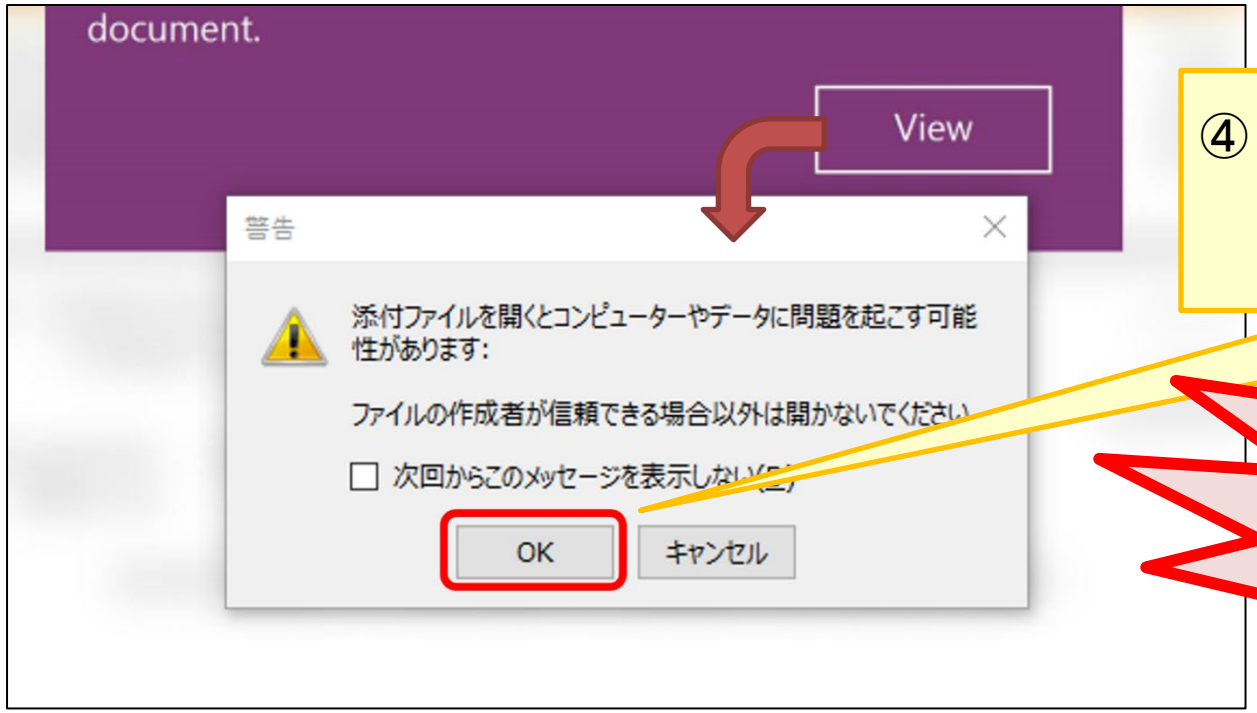
② 不鮮明なノート上にメッセージと
ボタン(画像)が表示される

[次ページへ続く]

事例②

ノート上の「View」と書かれた部分をダブルクリックすると、OneNoteのセキュリティ警告が表示されます。表示された警告画面で「OK」ボタンをクリックすると、Emotetに感染してしまいます。

③「View」と書かれた部分を
ダブルクリックすると警告が表示される

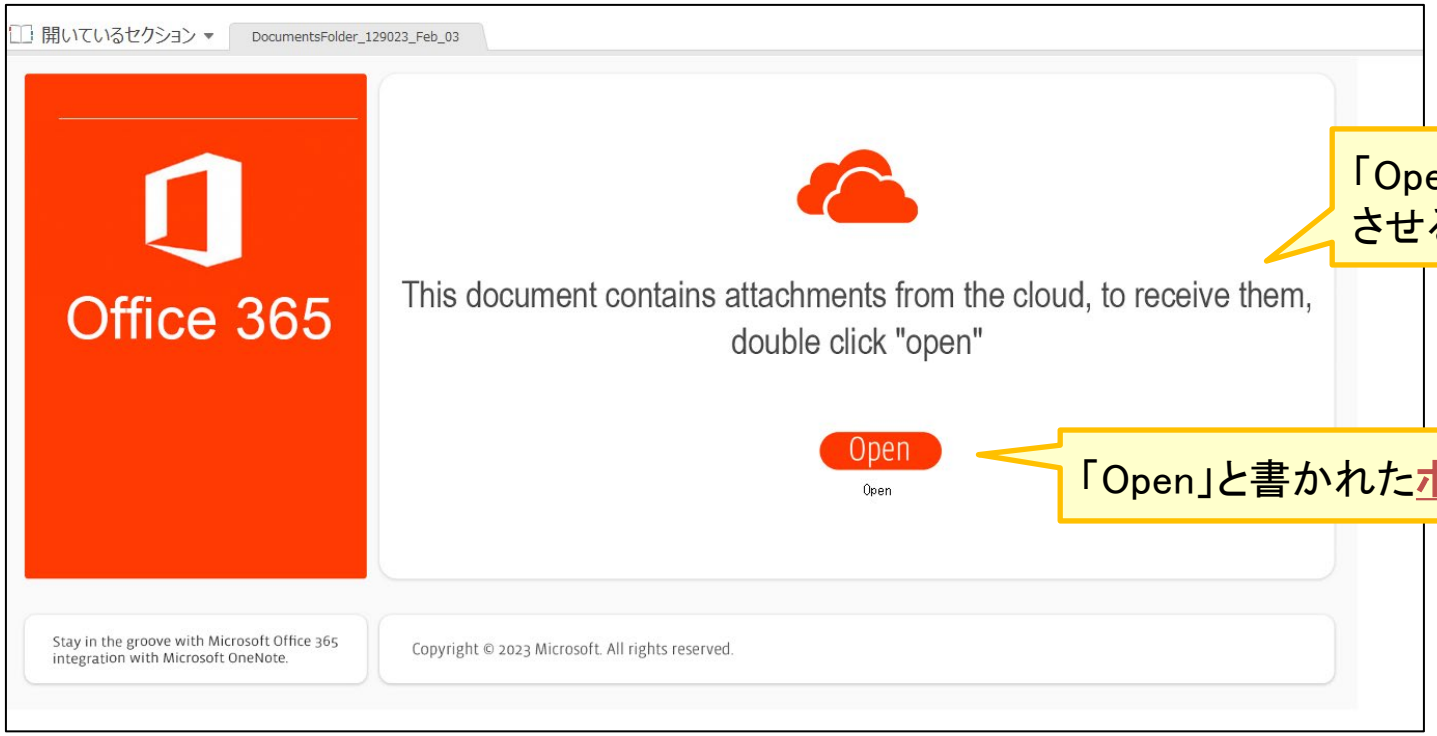


④ 「OK」ボタンをクリックしてしまうと、ノートに埋め込まれた悪意のあるファイルが実行されEmotetに感染してしまう。

「OK」ボタンはクリックしない！

事例③

メールに添付されたOneNote形式のファイルを開くと、クラウドサービス上のファイルを開くために「Open」ボタンをダブルクリックするように促すメッセージと、「Open」と書かれたボタンに模した画像が表示されます(※)。



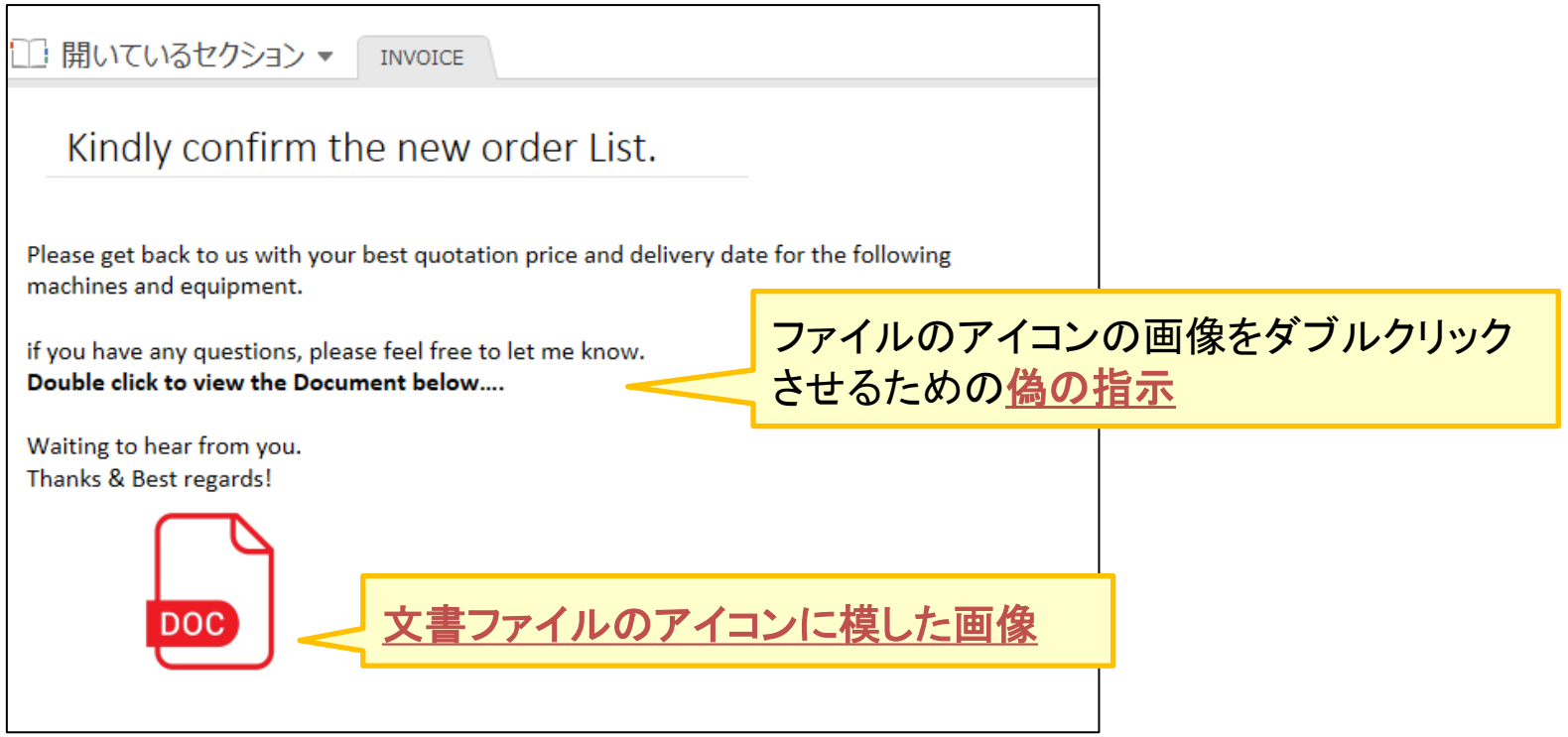
「Open」と書かれた画像をダブルクリックさせるための**偽の指示**

「Open」と書かれた**ボタンに模した画像**

(※)「Open」と書かれた画像をダブルクリックした後の動作は、事例①と同一です。
表示される**警告画面のOKボタンはクリックしない**でください。

事例④

メールに添付されたOneNote形式のファイルを開くと、ノートに添付している文書ファイルを開くために、ファイルのアイコンをダブルクリックするように促すメッセージと、文書ファイルのアイコンに模した画像が表示されます(※)。



(※) ファイルのアイコンの画像をダブルクリックした後の動作は、事例①と同一です。
表示される警告画面のOKボタンはクリックしないでください。

特徴

悪用されるOneNote形式のファイルの特徴

本手口で悪用される「OneNote形式のファイル」には、次のような特徴があります。

特徴

- ✓ ノートの内容が、**見えない状態(白紙、不鮮明)**になっている。
- ✓ ノートに、「CLICK TO VIEW DOCUMENT」、「View」、「Open」等の**ボタンが表示**されている。
- ✓ ノートに、**文書ファイルのアイコンが表示**されている。
- ✓ ノートの内容や添付されている文書ファイル、クラウドサービス上のファイルを閲覧するために、**ボタンやファイルのアイコンをクリックするように促す指示**が書かれている。

上記の特徴のうち、いずれかにあてはまるような不審な「OneNote形式のファイル」を受信した場合、ノートに書かれた**指示通り操作しないよう注意する**とともに、**システム管理部門等へ連絡するなど、所定のルールに沿った対応**をしてください。

対策

OneNote形式のファイルを悪用した攻撃への対策

本攻撃による被害を回避するために、次のような対策が有効です。

対策

- ✓ 身に覚えのないOneNote形式のファイルは**開かない**。
- ✓ 身に覚えのないOneNote形式のファイルのノートに**書かれた指示には従わない**。
- ✓ OneNote形式のファイルの閲覧中に、セキュリティ警告が表示された際、**警告文をよく確認し、安全であると判断できない場合は「OK」ボタンをクリックしない**。

おわりに

万が一、身に覚えのないOneNote形式のファイルを開いてしまった場合や、ノートに書かれた指示通り操作してしまった場合は、**すぐにシステム管理部門等へ連絡**してください。

また、本資料で説明した「OneNote形式のファイル」のほかにも、Word形式やExcel形式のファイル等の機能を悪用し、ウイルスに感染させようとする攻撃が存在します。これらの攻撃によって、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徹底してください。

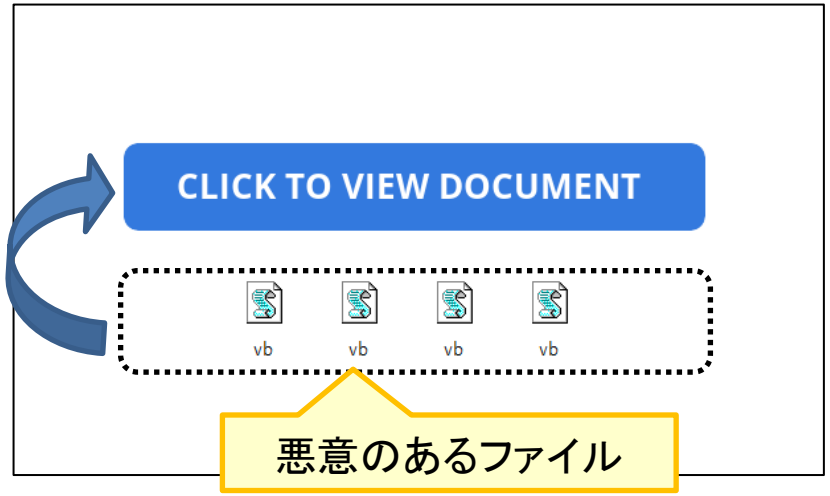
基本的なウイルス対策

- ✓ 身に覚えのないメールの**URLリンクはクリックしない**。
- ✓ 身に覚えのないメールの**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**常に最新の状態にしておく**。
- ✓ セキュリティ警告が表示された際は、**警告文をよく確認し、安全であると判断できない場合は操作を中断する**。
- ✓ 身に覚えのないWord形式やExcel形式の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」ボタンや「コンテンツの有効化」ボタンはクリックしない**。

補足情報

事例①②で紹介した「CLICK TO VIEW DOCUMENT」ボタンや「View」ボタンに模した画像の背面には、悪意のあるファイル(※1)が隠されています(※2)。この画像部分をダブルクリックすることで、悪意のあるファイルが実行される仕組みになっています。

◆事例①



◆事例②

(※1) vbs、swf、hta、cmd、bat形式のファイルを確認しています。
(※2) 事例③④も同様に、ボタンやアイコンに模した画像の背面に、悪意のあるファイルが隠されています。