【参考資料】

文書ファイルを悪用したフィッシング詐欺の手口に関する注意点

2017年10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**

はじめに（1）

フィッシング詐欺（フィッシング攻撃）とは

- フィッシング詐欺とは、インターネットバンキング、ショッピングサイト等の利用者の アカウント情報（ID、パスワード等）や、クレジットカードの情報等を騙し取る攻撃です。

- 典型的な手口としては、攻撃者が本物のウェブサイトと似た偽のウェブサイト（フィッシングサイト）を構築し、利用者に本物と錯誤させ、IDやパスワードを入力させます。偽のウェブサイトへ利用者を誘導するために、それらしい偽のメール（フィッシングメール）が送られることがあります（例えば、「今すぐログインして口座情報を確認してください」といったメッセージと共に、偽サイトへのリンクが書かれている、等）。

はじめに（2）

フィッシング詐欺への対策

- フィッシング詐欺への対策は、このような攻撃があるということを知り、騙されないよう注意し、IDやパスワード等を偽の画面で入力しないことです。

- 具体的には、「IDやパスワードの入力が求められた画面が本物であるか、URL等を確認する」「ウェブサイトを開く場合、メールに書かれたリンクからではなく、ブックマーク等、信頼できる方法で開く」といった対策が有効です。

より詳しくは、「フィッシング対策協議会」のウェブサイトも参照してください。
https://www.antiphishing.jp/

攻撃の手口

攻撃手口の変化

- フィッシングサイトへの誘導手口として、これまでは偽メールの本文中にURLリンクが書かれている手口が多かったのですが、最近、メールに添付されたPDFなどの文書ファイルからフィッシングサイトに誘導する手口が確認されています。

- 本資料で紹介する事例は、文書ファイルを共有するクラウドサービスと連携しているかのようなPDFファイルを装い、IDやパスワードを詐取するという手口です。

目的の変化

攻撃者の目的の変化

- オンラインバンキング等の直接金銭に関わる情報だけではなく、企業で利用するクラウドサービスのアカウント情報も狙われるようになってきており、注意が必要です。

- 具体的には、Office 365 や Google Apps のアカウント情報が狙われている事例を確認しています。これらのアカウント情報が攻撃者に奪われると、組織内の情報（メールやクラウド上に保存したファイル等）が窃取されたり、奪われたメールアカウントを使って別の人へ攻撃が行われることがあります。これは、深刻な標的型サイバー攻撃の準備段階として行われる可能性もあります。

自らのアカウント情報が盗用された場合の被害の大きさを今一度認識し、IDやパスワードの入力時は、慎重に確認することを心掛けてください。

本資料の目的

ウイルスに感染させるための罠（脆弱性の悪用等）が仕掛けられた悪意のあるPDFファイルは、これまでにも事例がありました。

しかし、昨今、ウイルスへの感染とは異なり、フィッシングサイトへ誘導させることを目的としてPDFファイルを使う手口が出てきています。

本資料は、その攻撃手口について紹介し、注意点を説明するものです。

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、添付された不審な文書ファイルに対して警戒いただくようお願いいたします。

※本資料では、Adobe Reader XI 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。

本資料で紹介する事例の要点

特徴

- メールに添付されたPDFファイルを開くと、何らかの理由をつけて、文書内をクリックするように指示する旨の文面が書かれている。
- 文書内をクリックすると、ウェブブラウザでフィッシングサイトが開く。
  ※ 環境により、その前に警告ウインドウが表示される。
- フィッシングサイトでは、メールアドレス、ID、パスワードなどを入力するよう求めてくる。ここで入力した内容は、悪意のある者に送られてしまう。

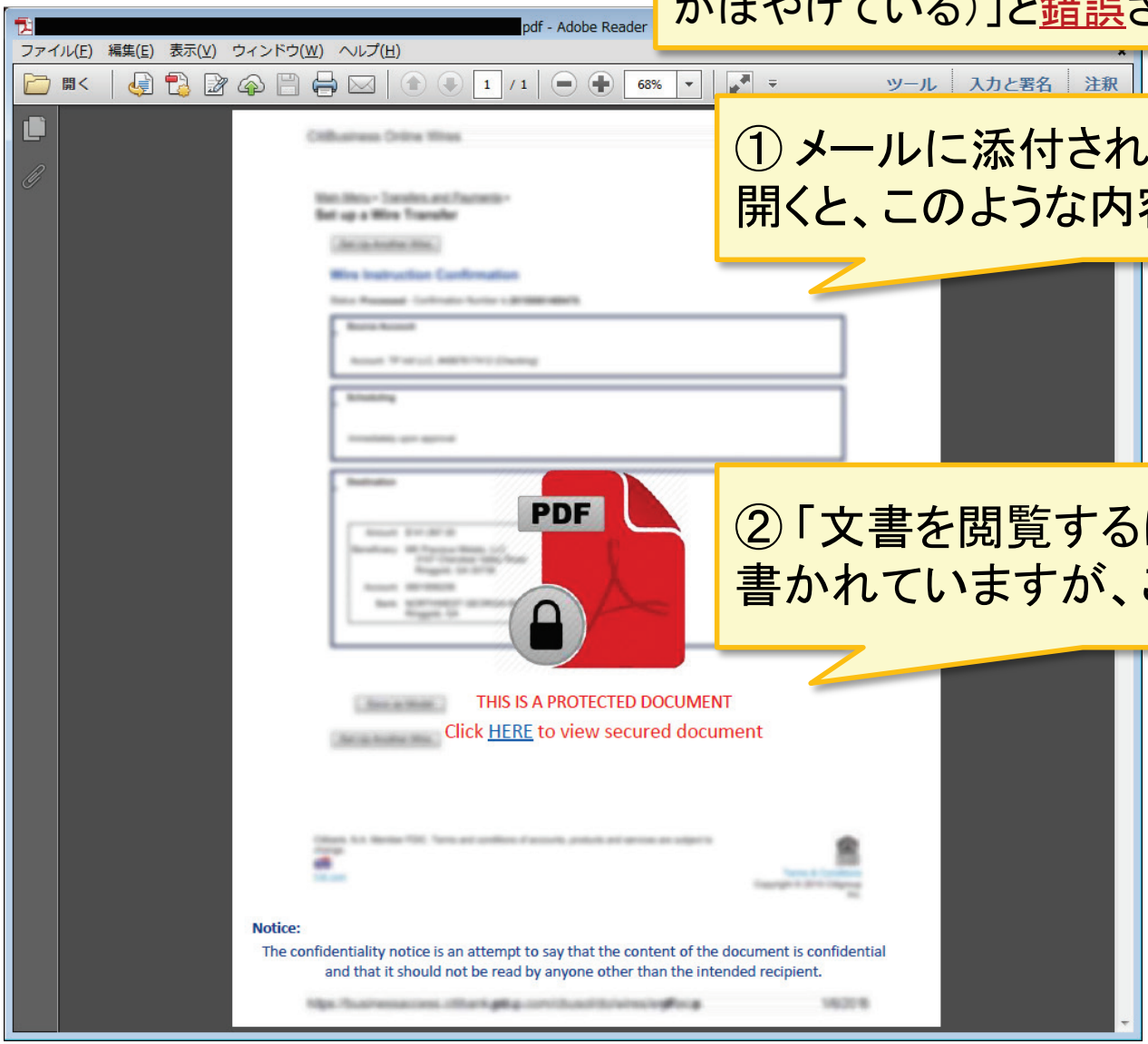
対応方法

- 身に覚えのない添付ファイルを開かないよう注意するとともに、ここで説明する特徴が見られた場合、**システム管理部門等へ連絡**してください。
  （本事例のタイプの文書ファイルを開いただけでは、被害は発生しません）
- 身に覚えのないログイン画面等で、IDやパスワードを入力しないでください。

次のページからは、公開情報から得られた実際のPDFファイルを例にして説明します。

事例（1）-1

この事例では、受信者に「文書の内容がセキュリティで保護されていて、表示できていない（画面がぼやけている）」と錯誤させようとしています。



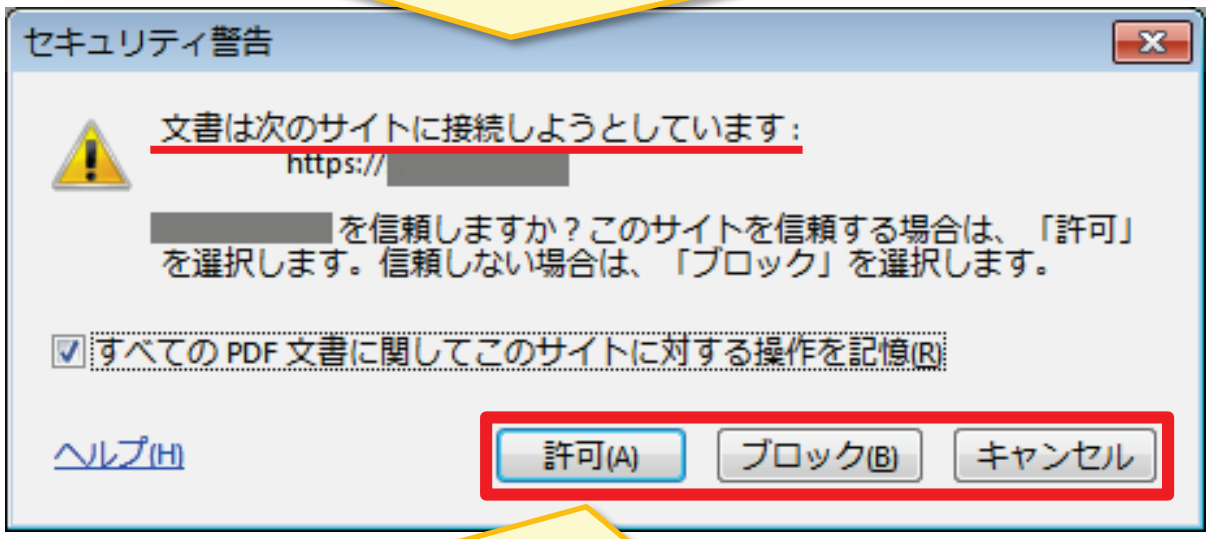
① メールに添付されているPDFファイルを開くと、このような内容が表示されます。

②「文書を閲覧するにはここをクリック」と書かれていますが、これは罠です。

[次ページへ続く]

事例（1）-2

③ 書かれた指示通りにクリックすると、PDF内に設定されたURLリンクを開くため、警告ウインドウが開きます。
（指示された箇所以外をクリックしても表示される場合があります）



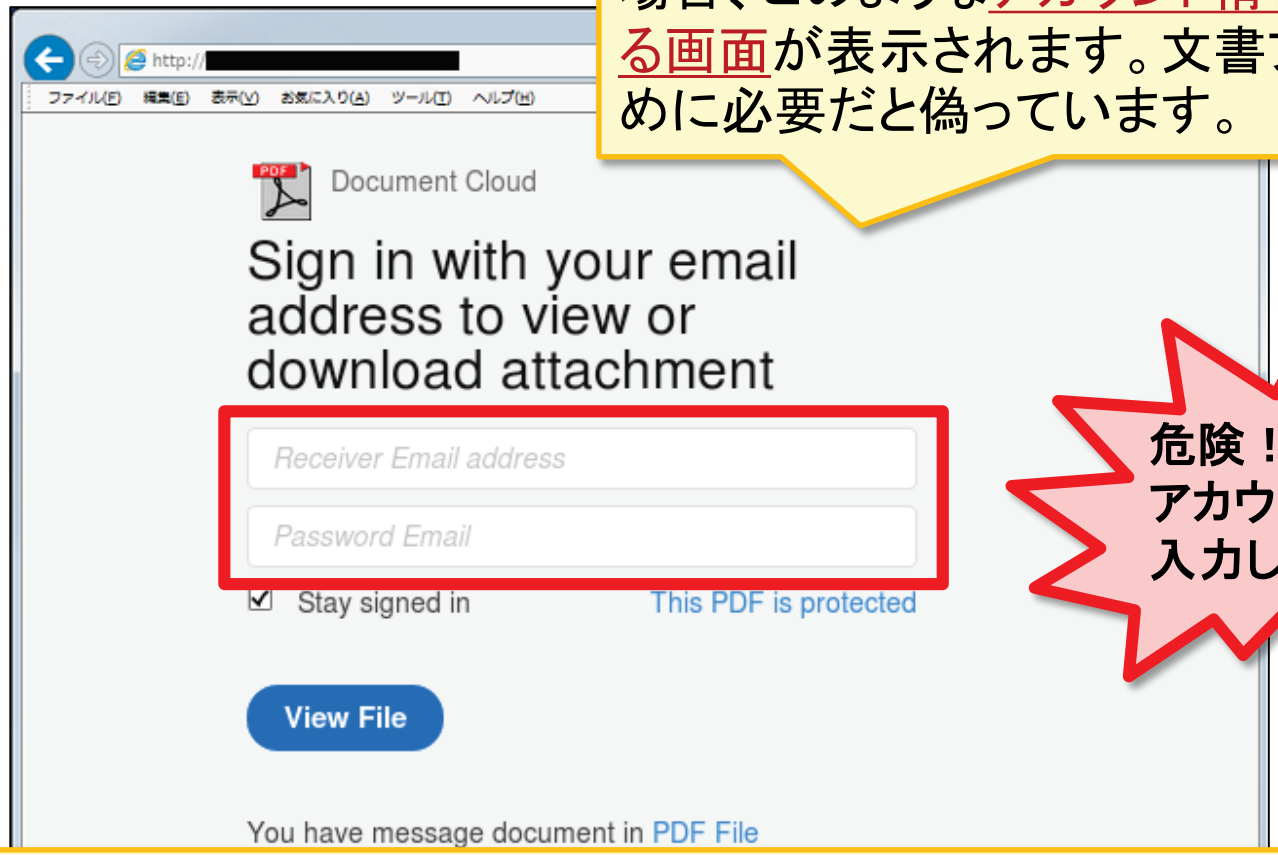
Adobe Reader が表示している本警告ウインドウは、URLリンクを含む正規のPDFファイルのリンクをクリックしても同じように表示されます。

④ ここで「許可」ボタンをクリックすると、フィッシングサイトが開きます。
→ 身に覚えのないURLが開かれようとしている場合は、「ブロック」または「キャンセル」をクリックしてください。

［ 次ページへ続く ］

事例（1）-3

⑤ フィッシングサイトがブラウザで開かれた場合、このようなアカウント情報の入力を求める画面が表示されます。文書ファイルを開くために必要だと偽っています。



危険！！
アカウント情報は
入力しない！

⑥ ここでメールアドレスやパスワードを入力してしまうと、その情報が窃取されてしまいます。不用意に情報を入力せず、システム管理部門等へ連絡してください（入力してしまった場合は、速やかにパスワードを変更してください）。

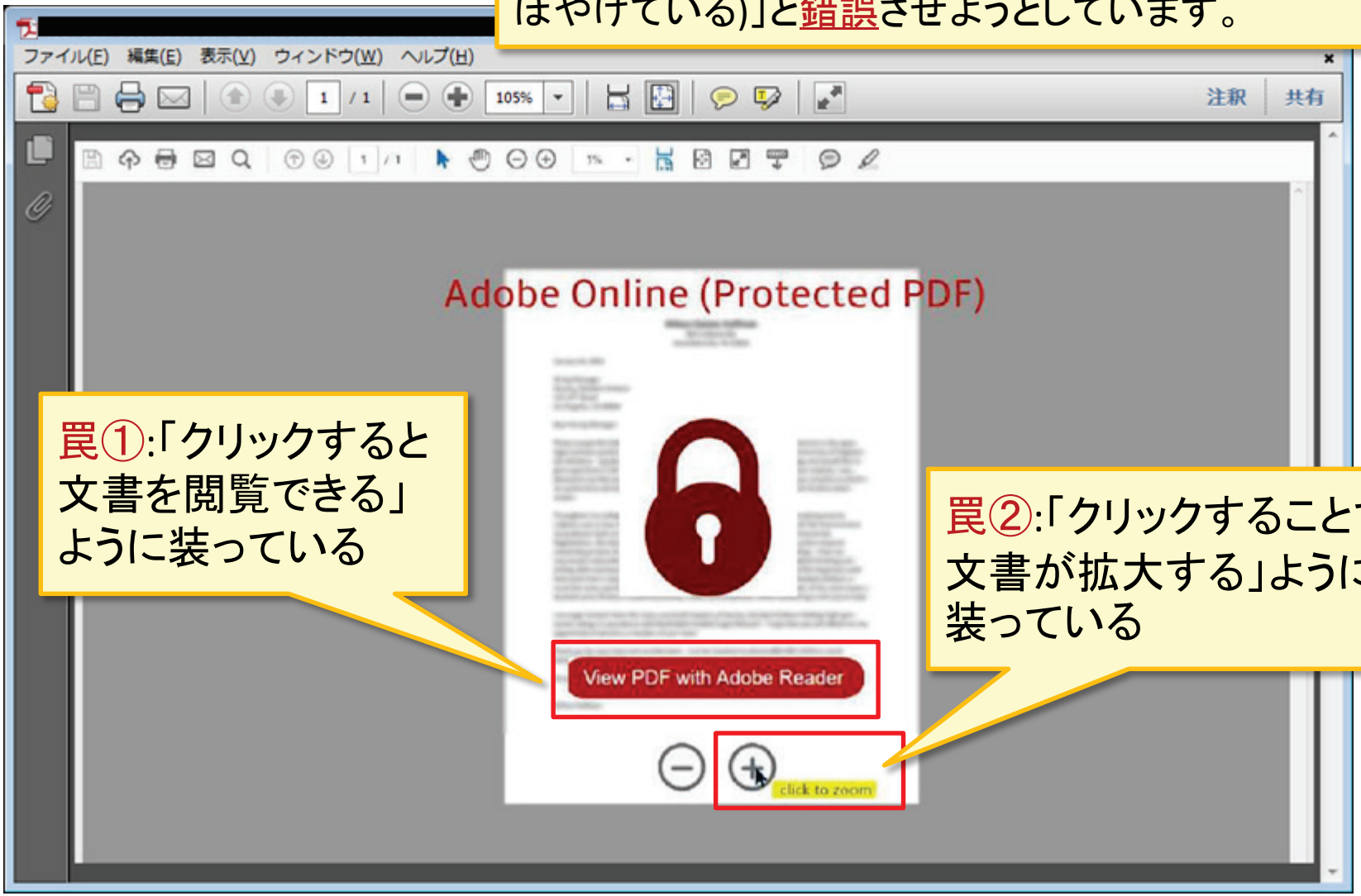
事例（2）～（4）

他の同種事例

- 次ページ以降では、攻撃者が、メール受信者にPDFの画面をクリックさせ、アカウント情報を入力させるために、どのような騙しの手口を用いてくるのかを中心に紹介します。
- 次ページ以降で紹介するPDFファイルも、攻撃者によって仕掛けられた罠をクリックしてしまった後の動作は、基本的に事例（1）と同様です。

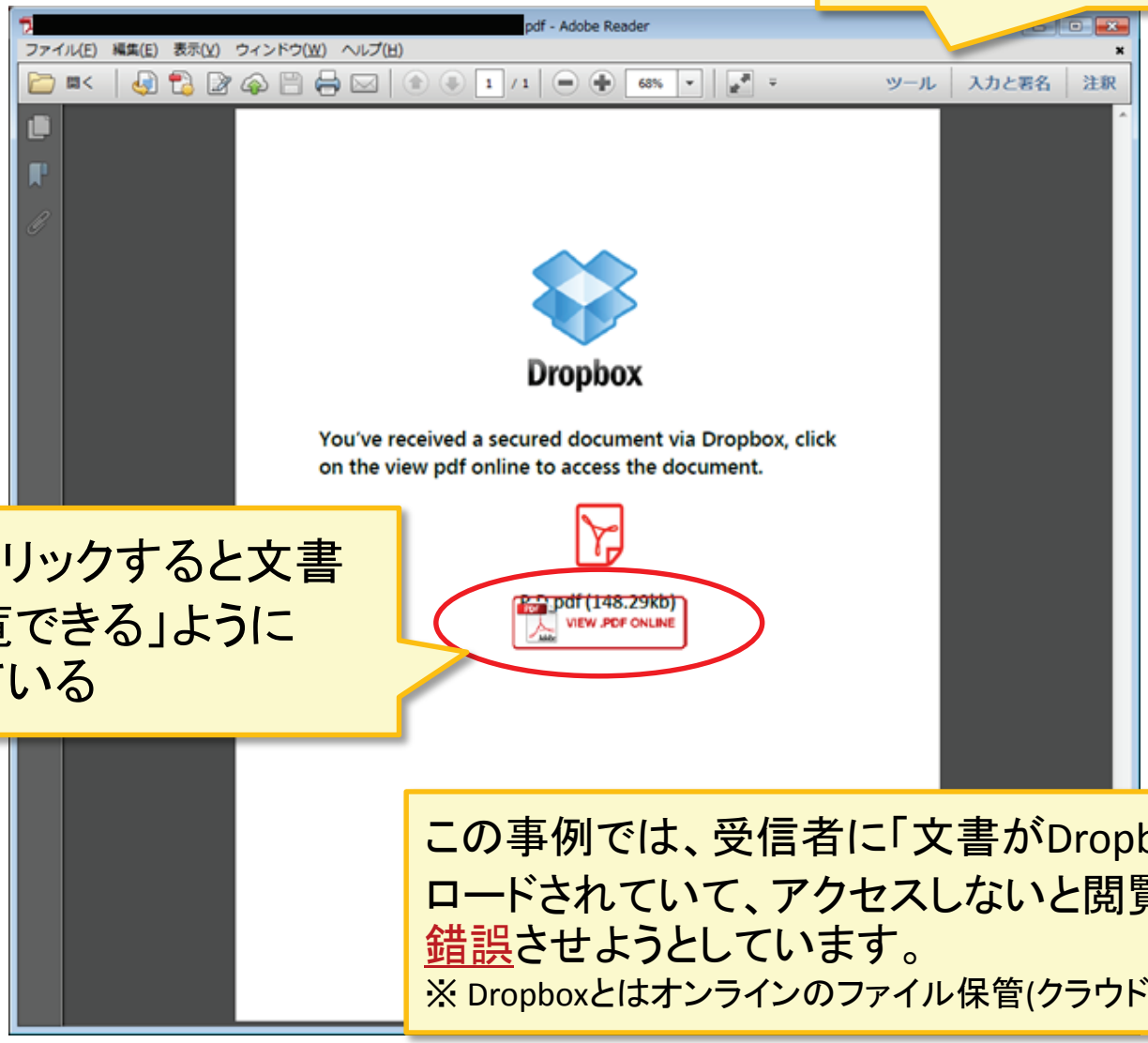
事例（2）

この事例でも、受信者に「文書の内容がセキュリティで保護されていて、表示できていない(画面が小さく、ぼやけている)」と錯誤させようとしています。



事例（3）

PDFファイルを開いた画面



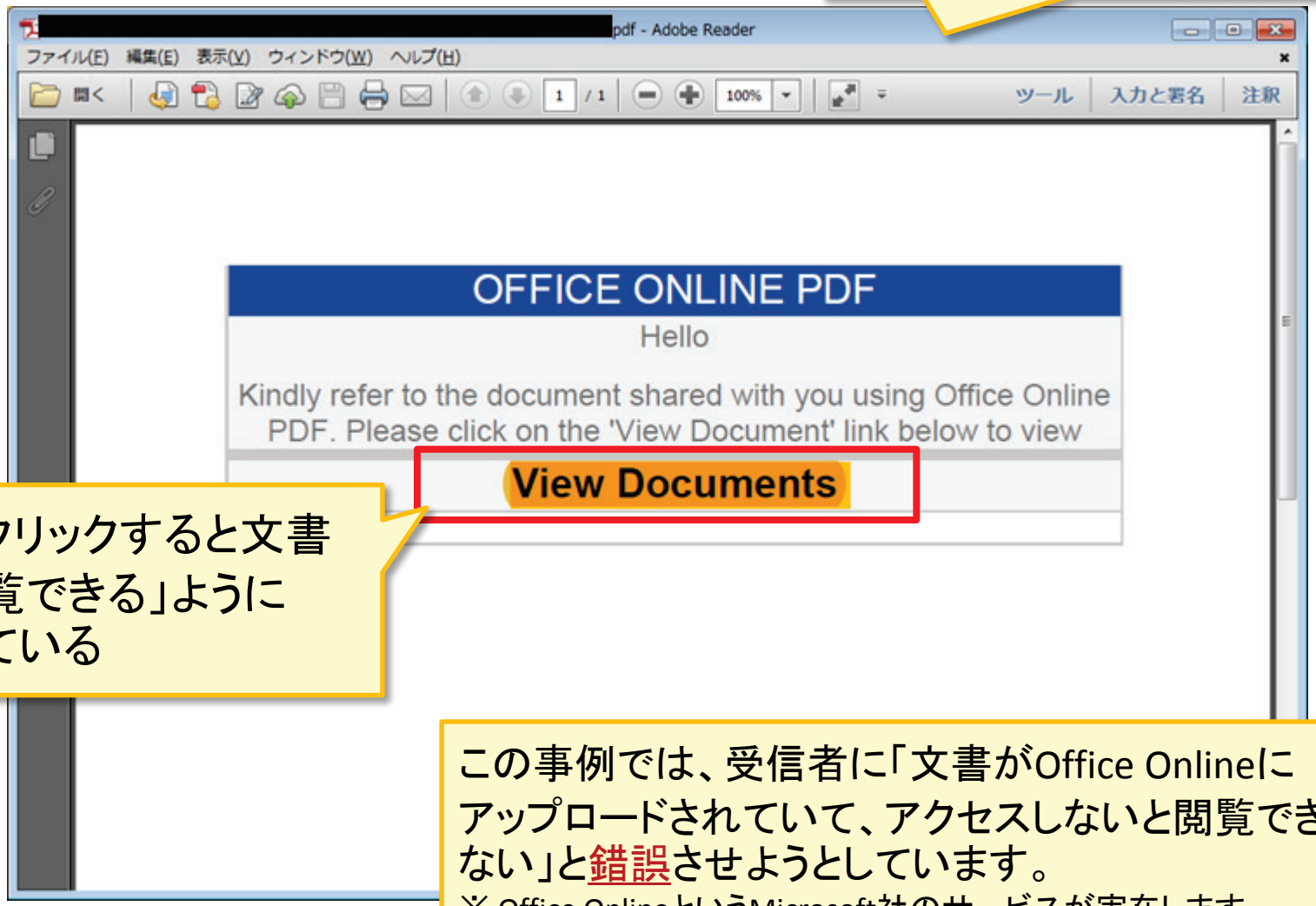
罠:「クリックすると文書を閲覧できる」ように装っている

この事例では、受信者に「文書がDropboxにアップロードされていて、アクセスしないと閲覧できない」と錯誤させようとしています。

※ Dropboxとはオンラインのファイル保管(クラウド)サービスです。

事例（4）

PDFファイルを開いた画面



罠:「クリックすると文書を閲覧できる」ように装っている

この事例では、受信者に「文書がOffice Onlineにアップロードされていて、アクセスしないと閲覧できない」と錯誤させようとしています。

※ Office OnlineというMicrosoft社のサービスが実在します。

おわりに

フィッシング詐欺は、本資料で説明した手口のほかにも様々なバリエーションが存在しますが、共通点は「利用者を騙して自らIDやパスワードを入力させる」という手口です。

フィッシング詐欺による被害を防ぐため、次のような基本的な対策を行ってください。

- ✓ 不審なメールに書かれたURLリンクを不用意に開かない。
- ✓ 不審なメールの添付ファイルは開かない。
- ✓ IDやパスワードを入力する画面（ログイン画面等）が表示された場合、それが正常な動作なのか、正規のウェブサイトであるのかという確認ができない場合は、入力を控える。