CyberCrime Control Project

平成27年第4号

広島県警察本部
サイバー犯罪対策課
082－228－0110

～ 実在する企業を騙った ウイルス付き メールに注意 ～

■ 最近の標的型メールの特徴

実在する企業名を騙って請求書やFAX受信通知などを装ったメールが送信され，添付されたファイル等を開くとウイルスに感染します。

これらのウイルスに感染すると，ネットバンクから不正にお金を盗み出されたり，社内の重要な情報を盗み取られる被害に遭うことも多くあります。

～ メールの一例 ～

(件名)【●●●(某電子部品販売会社)より】ご注文ありがとうございました-添付ファイル「出荷のご案内」を必ずご案内ください
※ メール本文中において「●●●(某電子部品販売会社)」を騙ったもの

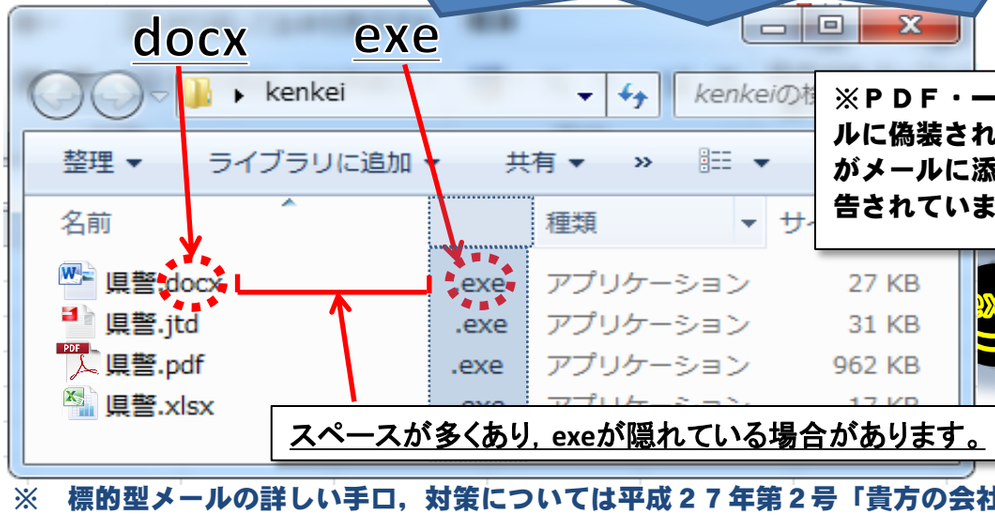
(件名) ●●●-請求書(小)の件です。-添付ファイル
※ メール本文中において「●●●印刷（某大手印刷会社）」を騙ったもの

(件名)Messafe from "●●●P0026738E40D2"
※ メール本文中において「●●●製複合機（大手企業）」を騙ったもの

(件名)ファックス受信完了：FAX Received
※メール本文中において，ファックスの受信完了通知を装ったもの

(件名)【請求書】●●●システム利用料の送付
※メール本文中において，「ホテル●●●(大手ホテル)」を騙ったもの

一見，文書ファイルに見えますが，本当は実行ファイル!!
つまり"偽装"している!!



※ＰＤＦ・一太郎・ワード等の文書ファイルに偽装された，実行形式ファイル（exe等）がメールに添付されているケースが多く報告されています。

※ 標的型メールの詳しい手口，対策については平成２７年第２号「貴方の会社が標的に！？」をご参照下さい。