

令和2年12月1日

サイバーセキュリティ関連情報（12月号）

鳥取県警察本部サイバー犯罪対策課

○ マルウェア「IcedID（アイストアイディー）」に注意！

トレンドマイクロ社は、マルウェア「IcedID（アイストアイディー）」による感染報告が相次いでおり、国内の広範囲に拡散が見られるとして注意喚起をしています。

「IcedID」は、パスワード付きzipファイルが添付されたメールの本文中に記載された解凍用パスワードによってファイルを解凍し、文書ファイルの「コンテンツの有効化」ボタンをクリックすることで感染します。

メールの本文は日本語で書かれており、件名が「Re:」と返信型になっているなど、昨年からの被害が継続しているマルウェア「EMOTET（エモテット）」に類似しています。**パスワード付きzipファイルは、ウイルス対策ソフトで検知されないことから注意が必要となります。**

マルウェア感染の被害に遭わないためには、メールと添付ファイルの正当性を判断して、不審なものは開かないよう注意しましょう。



※ メールに添付された圧縮ファイルを解凍してもコンテンツの有効化をしないで下さい

参考：トレンドマイクロ セキュリティブログ <https://blog.trendmicro.co.jp/archives/26656>

○ パスワード付きzipファイル、内閣府と内閣官房で廃止へ！

平井卓也デジタル改革担当相は11月24日の会見で、メールでパスワード付きzipファイルを送り、パスワードを別送する方法について、11月26日から内閣府、内閣官房で廃止すると発表しました。今後、外部へのファイル送信には、外部ストレージサービスを活用し、他省庁の状況についても実態調査を進めるとしています。

平井卓也大臣は、この方法について「セキュリティ対策や受け取り側の利便性の観点から適切ではない」として廃止する意義を改めて説明し、「このような取り組みは政府内だけでなく、民間にも影響のある問題」と指摘し、「民間企業の対応も注視しつつ、今後どのようなセキュリティ向上策をとっていくのが望ましいか、民間の知恵をアイデアボックスに送って頂きたい」と政府の意見募集サイト「デジタル改革アイデアボックス」への投稿を呼びかけています。

パスワード付きZipファイルに関しては、手間がかかる一方でセキュリティ対策としての効果を疑問視する声があるほか、セキュリティ製品によるウイルス検知を回避され、上記「IcedID（アイストアイディー）」のようなマルウェアの拡散にも悪用されるケースがあるなど、アメリカ政府ではセキュリティ対策としてパスワード付きzipファイルが添付されたメールをブロックすることを奨励しています。

また、プライバシーマーク制度を運営する日本情報経済社会推進協会（JIPDEC）でも、11月18日付「メール添付のファイル送信について」において、同方法によるファイルの送信は、『プライバシーマーク制度では個人情報情報の漏えいを防げないこと等から従来から奨励していない』旨明言しているほか、情報処理推進機構（IPA）でも、『添付ファイルを暗号化したメールの復号のためのパスワード等は、別の通信手段を利用して相手に伝えることが重要』としています。

パスワード付きzipファイルにおける今後のセキュリティ情勢について、ぜひ注視しておきましょう。



参考：内閣府デジタル改革アイデアボックス <https://ideabox.cio.go.jp/>

