Ksisnetだより

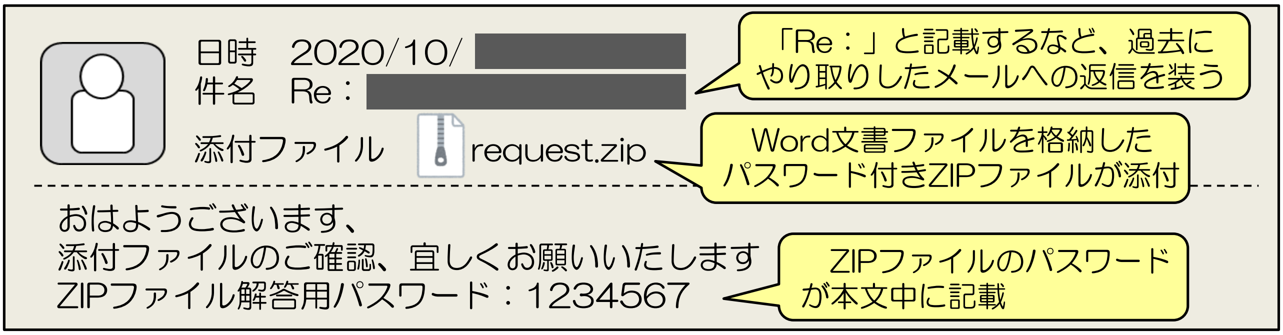
発行:Ksisnet事務局
令和2年11月19日
Vol.87

マルウェア「IcedID」にご注意ください！

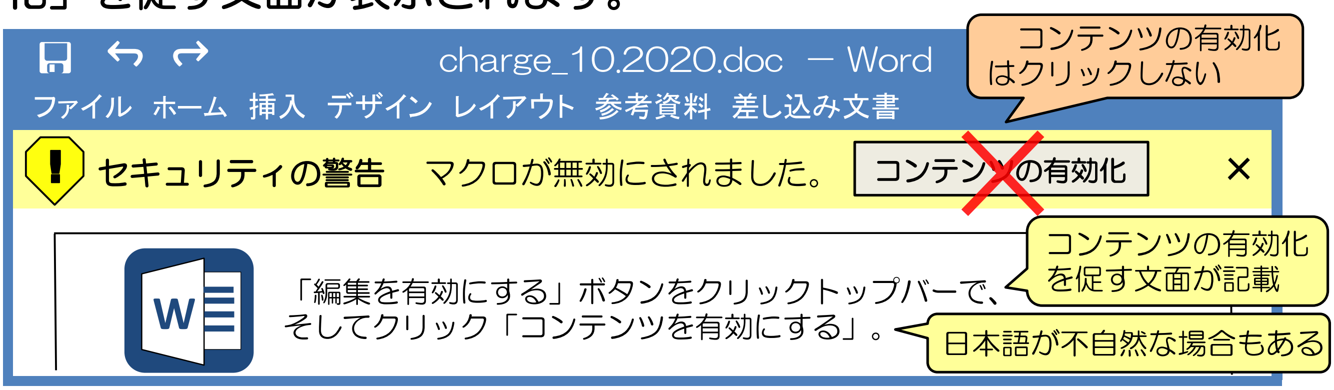
マルウェア「IcedID」に感染すると、「メールやブラウザなどの認証情報を窃取される」「別のマルウェアがダウンロードされる」「自組織から他の組織へ攻撃メールが送信される」などの被害が発生するおそれがあります。

【感染・拡散手法】

● Word文書ファイルを格納したZIPファイルを添付した攻撃メールが送られます。



● ZIPファイルに格納されたWord文書を開くと「コンテンツの有効化」を促す文面が表示されます。



● 「コンテンツの有効化」をクリックするとWord文書内の不正なマクロが実行され、IcedIDに感染します。

「コンテンツの有効化」はクリックしないようにご注意下さい。

被害防止のポイント

○ 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。
○ 過去のやり取りに返信する形のメールであっても、ZIPファイル形式やWord文書形式の添付ファイルには十分注意し、不自然な点があれば開かない。
○ 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に連絡する。

参考　トレンドマイクロ