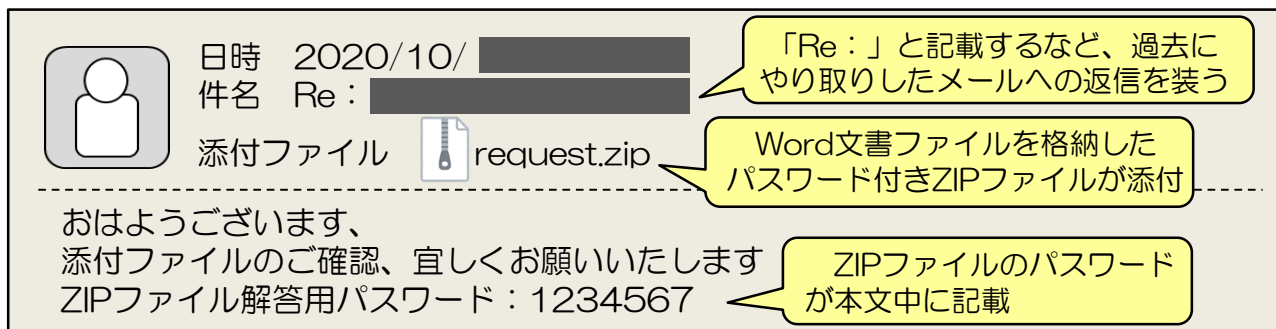



マルウェア「IcedID」にご注意ください！

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。



日時 2020/10/ [redacted]
件名 Re: [redacted]
添付ファイル  request.zip

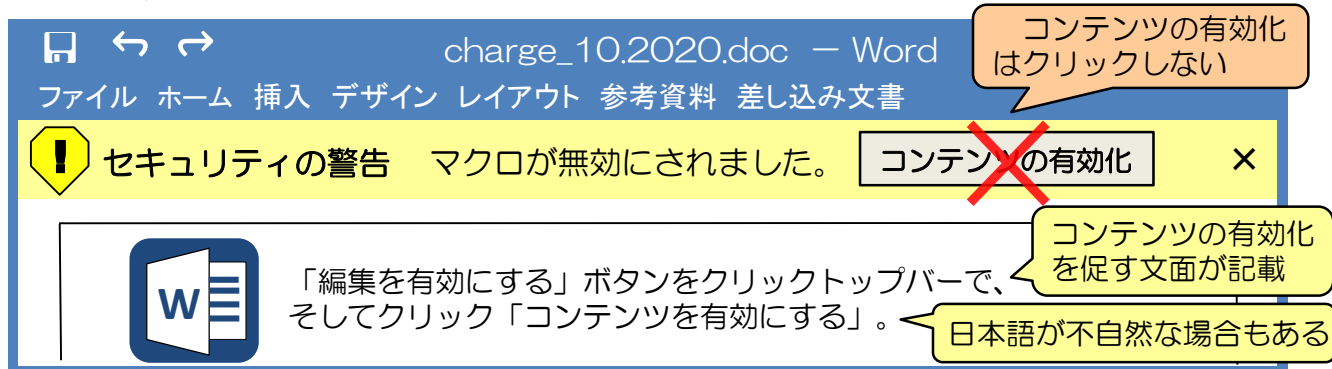
おはようございます、
添付ファイルのご確認、宜しくお願いいたします
ZIPファイル解答用パスワード：1234567

「Re:」と記載するなど、過去にやり取りしたメールへの返信を装う

Word文書ファイルを格納したパスワード付きZIPファイルが添付

ZIPファイルのパスワードが本文中に記載

- 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。



charge_10.2020.doc — Word
ファイル ホーム 挿入 デザイン レイアウト 参考資料 差し込み文書

セキュリティの警告 マクロが無効にされました。

「編集を有効にする」ボタンをクリックトップバーで、そしてクリック「コンテンツを有効にする」。

コンテンツの有効化はクリックしない

コンテンツの有効化を促す文面が記載

日本語が不自然な場合もある

- 「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ください。

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。