Cyber Security news

CS通信

NIIGATA PREFECTURE CYBER THREATS COUNCIL FOR
新潟県サイバー脅威対策協議会
～サイバー空間の脅威に対する新潟県産学官民合同対策プロジェクト推進協議会～

No. 6 （R 1.12. 6 発行）

新潟県警察本部、新潟県内の警察署に寄せられた相談情報、新潟県サイバー脅威対策協議会に寄せられた情報等を元に、トピックスを選定して皆様に情報提供、注意喚起を行っております。

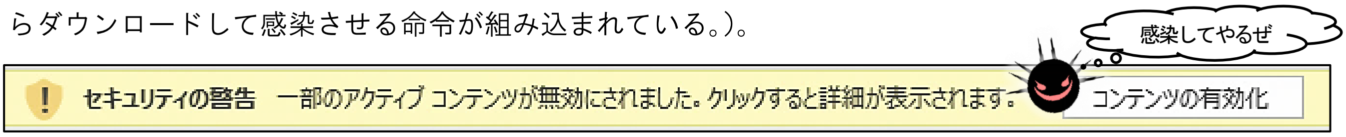
■ メールに添付されたMicrosoft Office文書ファイルによるマルウェア感染に注意！

■ 一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）によると、2019年10月後半より、マルウェア「Emotet」の感染に関する相談を多数受けており、特に実在の組織や人物になりすましたメールに添付された悪性な Word 文書ファイルによる感染被害が多数報告されているとのことです。

◆

■ 感染経路について

メールの添付ファイル（Word 形式）を開いて、悪意のあるマクロ（プログラム）の実行を許可（コンテンツを有効化する）してしまうと、マルウェアに感染させられてしまいます（マクロにはEmotetを外部からダウンロードして感染させる命令が組み込まれている。）。



! セキュリティの警告　一部のアクティブ コンテンツが無効にされました。クリックすると詳細が表示されます。

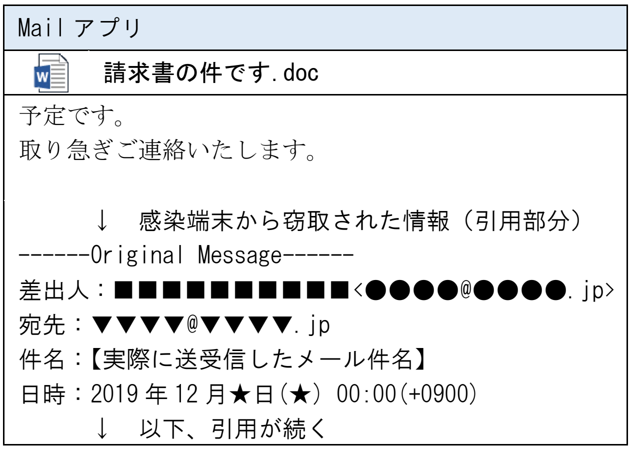
※ マクロの実行を許可するかどうかの警告画面（設定によっては警告なしに Emotet がダウンロードされる場合があります。）

◆

■ 影響について

Emotet に感染してしまうと、端末やブラウザに保存されたパスワード等の認証情報が窃取され、ネットワーク内の端末に感染を広げるほか、メールアカウントとパスワード、メール本文やアドレス帳の情報が窃取された後、窃取されたメールアカウントや本文などが悪用されて、取引先や顧客に対してEmotet の感染を広げるメール（なりすましメール）が配信されてしまうおそれがあります。

※ Emotet の感染に繋がる添付ファイル付きのメール（一例）


Mail アプリ
請求書の件です.doc
予定です。
取り急ぎご連絡いたします。

↓　感染端末から窃取された情報（引用部分）
-------Original Message-------
差出人：■■■■■■■■■■<●●●●@●●●●.jp>
宛先：▼▼▼▼@▼▼▼▼▼.jp
件名：【実際に送受信したメール件名】
日時：2019年12月★日（★） 00:00(+0900)
↓　以下、引用が続く

◆

■ 「なりすましメール」に注意

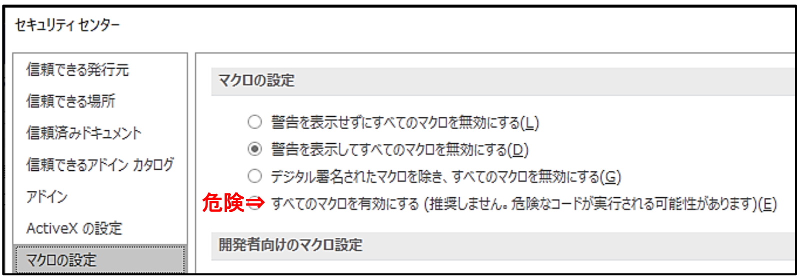
Emotet の感染に繋がるメールには、組織間でやりとりされた実際のメール内容を引用し、取引先相手からの返信メールであるかのように装うものがあります。

◆

■ 対策について

Microsoft Office の「セキュリティセンター」からマクロの設定を確認し、マクロが自動実行されないようにしましょう。

また、メールの相手をよく確認して、不審なものは開かないようにしましょう。



マクロの設定
○ 警告を表示せずにすべてのマクロを無効にする(L)
● 警告を表示してすべてのマクロを無効にする(D)
○ デジタル署名されたマクロを除き、すべてのマクロを無効にする(G)
危険⇒ ○ すべてのマクロを有効にする（推奨しません。危険なコードが実行される可能性があります）(E)
開発者向けのマクロ設定

▼編集・発行：サイバー空間の脅威に対する新潟県産学官民合同対策プロジェクト推進協議会（新潟県サイバー脅威対策協議会）
事務局（URL：http://www.cyber.niigata.jp/）
〒950-8553 新潟県新潟市中央区新光町4番地1（新潟県警察本部サイバー犯罪対策課内）
TEL: 025-285-0110　FAX: 025-281-0165　MAIL: project@cyber.niigata.jp
サイバー脅威対策協議会　検索

※　会員の皆様からの情報も受け付けております。詳しくは、協議会事務局までお問い合わせください。