埼玉サイバーセキュリティ推進会議（事務局：埼玉県警察本部生活安全部サイバー犯罪対策課）
R4.3.2
S.C.S.C.通信
第77号

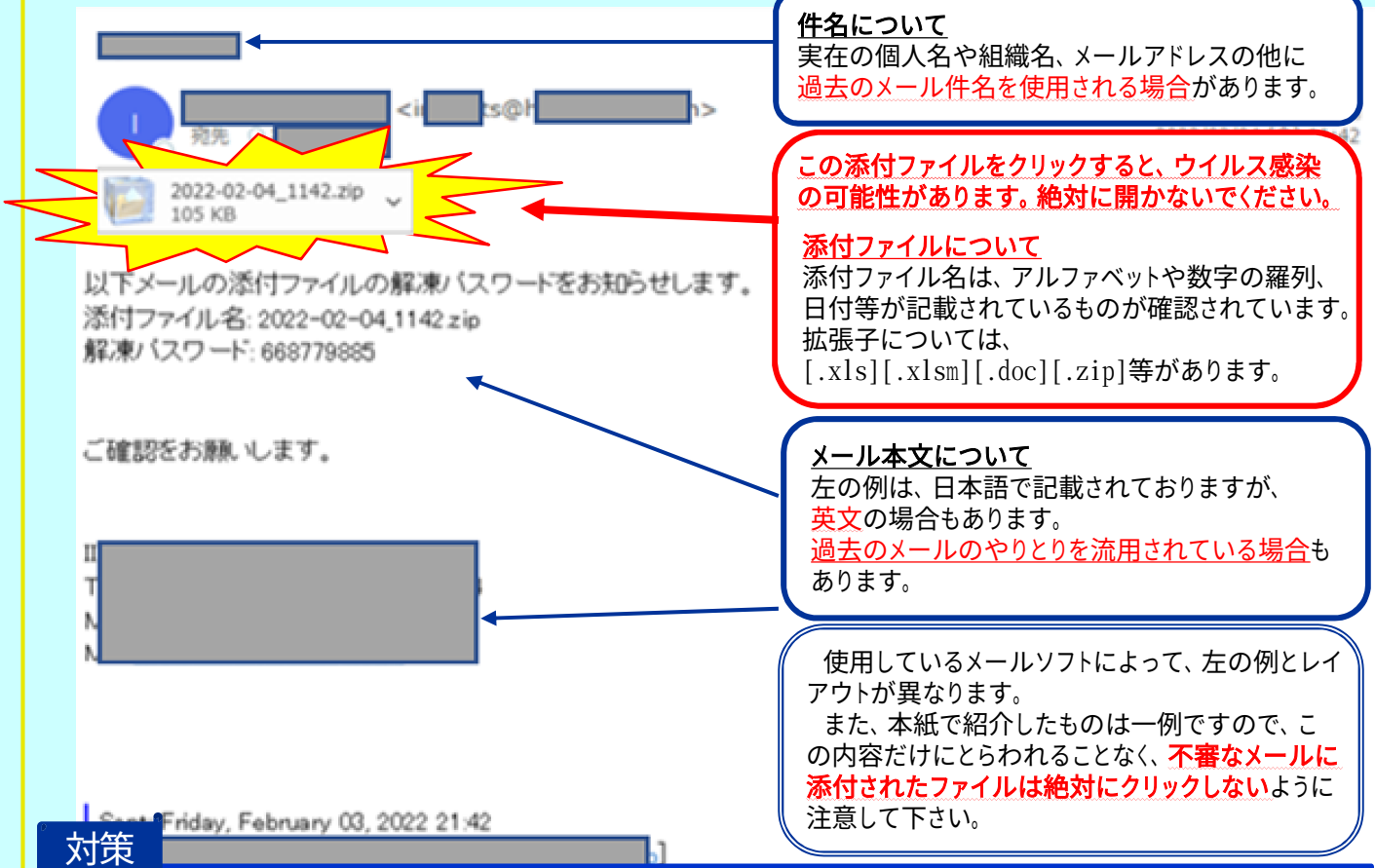
メール添付型マルウェア「Emotet（エモテット）」が急速に拡大中！！

埼玉県内でも、**Emotet（エモテット）に関する相談が急増**しています。Emotetは、メールに添付された文書ファイルや圧縮ファイル等を開くことで感染します。感染すると、重要情報の盗み取りやランサムウェア等の被害に遭うおそれがあるだけでなく、取引先等に感染を拡散してしまうおそれもあります。

関係者からのメールであっても油断せず、安易に**添付ファイルを開かないでください**。

Ｅｍｏｔｅｔの受信例と対策

Emotetの受信例



件名について
実在の個人名や組織名、メールアドレスの他に過去のメール件名を使用される場合があります。

この添付ファイルをクリックすると、ウイルス感染の可能性があります。絶対に開かないでください。

添付ファイルについて
添付ファイル名は、アルファベットや数字の羅列、日付等が記載されているものが確認されています。
拡張子については、
[.xls][.xlsm][.doc][.zip]等があります。

メール本文について
左の例は、日本語で記載されておりますが、英文の場合もあります。
過去のメールのやりとりを流用されている場合もあります。

使用しているメールソフトによって、左の例とレイアウトが異なります。
また、本紙で紹介したものは一例ですので、この内容だけにとらわれることなく、**不審なメールに添付されたファイルは絶対にクリックしない**ように注意して下さい。

対策

○ 感染しないために注意すること

・メールに添付されたファイルを安易に開かないこと
・身に覚えの無いExcel、Word等のofficeファイルの**「マクロの実行」を許可しない**こと
・Microsoft Office ソフトの**「マクロの自動実行」の設定を「無効」にする**こと

○ 自社を騙る不審なメールが確認された場合の対処

・ 直ちに**不正プログラム感染の有無を調査**し、専門事業者に相談･手配をする
⇒ セキュリティソフトのほか、Emotet感染有無確認ツール「**EmoCheck**」の利用も有効です。
詳細は、JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」
（https://www.jpcert.or.jp/at/2022/at220006.html）を参照してください。
・ 直接の電話連絡やウェブサイトへの掲載等を通じ、普段メールをやり取りする相手先を中心に、自社を騙るメールが蔓延していることの注意喚起を実施する
・ 感染した場合は、警察への通報をお願いします！