行政機関や医療機関を騙る不審メールが配信されておりますが、この度、弊社社員を騙った不審メールを社内でも受信されている事実を確認いたしました。
不審なメールには ZIP ファイルが添付されており、中のファイルを開きますと、マルウェア「Emotet（エモテット)」感染や不正アクセス等の恐れがございます。
6 月 13 日現在、弊社では全社員の端末感染チェックを行い、クリーンな状態であることを確認しておりますが、弊社とお取引のあるお客様から、弊社社員を装った不審メールがあったとご連絡がありました。
弊社社員の名前を利用した不審なメールを受信された方は添付されているファイル、並びに本文内のリンク URL などを開きますとマルウェアに感染する恐れがありますので、
絶対に開かないでください。
不審なメールには下記のような特徴があります。

- 弊社社員名、法人名などが署名、又は送信元となっている
- 不審な zip ファイルが添付されている
- 送信元のメールアドレスが全く知らない人となっている

メール例

以下メールの添付ファイルの解凍パスワードをお知らせします。
添付ファイル名：2022-06-13_1234.zip
解凍パスワード：AUIHW
鳳凰会グループ ○○ ○○
Tel:044-○○○-○○○○　Fax：044-○○○-○○○○
Mail:○○○○

重ねてのお願いとなりますが、上記のような**不審なメールを受信されたお客様がおられましたら絶対に開かないでください。**
Emotet に関しましては独立行政法人 情報処理推進機構 (IPA)から注意喚起が報告されており、警視庁から Emotet 感染確認ツールの実行手順が公開されておりますので合わせてご確認お願いいたします。