2022 年 3 月 4 日
株式会社 船場　PR 部

弊社社員を装った不審なメールの送信について

このたび、弊社社員を装った不審なメールを外部の複数の方が受信されていることを確認いたしました。悪意を持った外部システムより弊社社員を装い、断続的に送信されている状況です。

これらの不審なメールにはZIPファイルが添付されている、あるいは本文内にリンクが記載されております。現状、弊社としましては、セキュリティ対策機関JPCERTにて国内での感染被害の注意喚起がされているマルウェアEmotet（エモテット）による可能性が高いものと判断しております。中のZIPファイルやリンクにアクセスすると、Emotetに感染し、不正アクセス等の恐れがありますので、不審なメールは開封せずに削除し、ファイルを開いたりリンクをクリックしたりしないようにお願いいたします。

なお、現時点において弊社内の感染は確認されておらず、弊社社員（退職者を含む）のメールアドレス情報を保有されている外部の方が感染されたことが原因と推測しております。

上述のJPCERTでの注意喚起において、マルウェアEmotetの概要、感染経路、対策、対応などについて記されていますので、こちらも併せてご参照ください。

https://www.jpcert.or.jp/at/2022/at220006.html

実際に送信されている不審なメールの特徴と例は次の通りです。

[不審なメールの特徴]

❶ 弊社社員名が記載されているが、メールの送信アドレスと無関係

❷ Subject（件名）や本文で添付ファイルの開封やリンクのクリックを促す内容

❸ 電話番号も社員のものではない

メール例：
From：弊社社員名＜xxx@xxx.com＞ ←「.com」は弊社社員のメールアドレスではありません。
To：受信者名
Subject：RE: ←開封やリンクのクリックを促す内容もございます。
本文：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: 2022-03-02_2048.zip
解凍パスワード: 3271
ご確認をお願いします。

弊社社員名
Tel 044-XXX-XXXX　Fax 044-XXX-XXXX ←「044」から始まる番号は弊社の電話番号ではありません。
Mobile 090-XXX-XXXX
Mail xxx.xxx@semba1008.co.jp

以上

SEMBA