【重要】不審メール発生に関するお詫びのお知らせ

お取引先各位

2020 年 9 月 2 日 15 時頃、弊社社内のパソコンがウイルスに感染している可能性があることが判明いたしました。

当該パソコンに保存されていた過去のメール送受信履歴が流出し、これに含まれるメールアドレスに対して、弊社社員を名乗っている、または弊社社員メールアドレス ***@acesystem.co.jp より不審なメールが送付されている状況です。

弊社のお客様、またお取引先をはじめとする関係者の皆様には、多大なご迷惑をおかけしておりますことを深くお詫び申し上げます。
現在わかっている範囲ですが、アドレスと過去の送受信のメッセージが流出された疑いがございます。

緊急対策としまして、感染経路等の調査及び処置につきましては、専門家のアドバイスのもと現在ほぼ調査完了し、緊急対策を講じたところです。
当該メールを受信された場合には添付ファイルや、メール文中のリンクを絶対に開かれることのないよう、ご留意の程お願いいたします。
尚、万が一誤って添付ファイルを開いたり、URL にアクセスされたりした場合には、至急パソコンをインターネットから離してください。

※社内緊急対策
・メールサーバー調査対応実施（実施済み）9/3 済
・社内にて専門家を交えたセキュリティインシデント対策実施及び強化（実施済み）9/4 済
・社外向けお客様への対応・通知（順次実施中）9/ 2 より実施中
※社内恒久対策
・社員のセキュリティ意識向上教育の徹底及び運用方法のルール化（計画中）

今後は対策・監視を更に強化し、安全な運営に万全を期してまいりますので、ご理解くださいますよう何卒よろしくお願いいたします。

■確認されている不審メールの例
現在、確認されている弊社を装ったメールは以下のとおりですが、類似した他のパターンも発信されている可能性がありますので、十分ご注意ください。

■メールの件名

例：【○○様××生産ラインの件】、【○○提出書類のご確認】、【Re:現地調査の件】など。

今までやり取りしたことのある実在の件名を引用されています。

よって件名だけでは、正規メールか偽物メールか判別が難しい。

■メール内容

例１．添付ファイルが付いている場合はまず疑って下さい。△△.zip、○○.doc　など。

例２.「協力会社各位」　・・・本文・・・　　この「協力会社各位」が付いている

例３.添付メールに「パスワード」が記載されている。(正規メールであれば別便で送られる)

例４．添付ファイル名がランダムな英数字となっている。

※件名は、様々な実在する内容なので判別が難しいが、上記の内容のように不審な箇所が見受けられます。

但し、あくまで一例に過ぎない為、自己判断にて対処をよろしくお願いいたします。

この度は、多大なご迷惑をおかけしておりますことを深くお詫び申し上げます。

エースシステム株式会社

本　　社：〒594-1157　大阪府和泉市あゆみ野３－１－３

TEL：0725-54-3958

東京支店：〒103-0025　東京都文京区本郷４丁目２－４　勉精堂ビル

TEL：03-3868-3983