令和４年３月３日

(一社)神奈川県警備業協会
会　員　各　位

(一社) 神奈川県警備業協会
会　長　　畠　山　　操

ウイルスメールへの注意喚起について

謹　啓

時下ますますご清栄のこととお慶び申し上げます。

平素、協会運営につきまして格別のご高配を賜り厚く御礼申し上げます。

さて、この度、会員に対する、当協会を発信元とする不自然なメールの送付事案が発生しました。

つきましては、業務ご多忙のところ誠に恐縮に存じますが、別紙資料「サイバー攻撃についてのお知らせ」を参考にされ、不自然なメールを受信した場合などは、安易に添付ファイル（Zip ファイル、ワード、エクセルなど）や URL を開いたりしないで、発信元に確認するなどの注意をお願いいたします。

なお、本件に関する詳細な内容については独立行政法人情報処理推進機構（IPA）の『「Emotet」と呼ばれるウイルスへの感染を狙うメールについて』をご覧ください。

謹白

○　独立行政法人情報処理推進機構（IPA）
「Emotet」と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html#L13

別紙

資料

「サイバー攻撃についてのお知らせ」

1　不審メールに要注意

エテモットに感染すると

○　知らぬ間にネットワーク内データが盗まれる

➡不正ログイン、ダークネットに流出、販売

○　取引先にウイルス付きメールがばらまかれる

➡取引先がウイルスに感染する

○　ネットワークに自由に侵入される

➡恒常的な情報流出と他への攻撃の踏み台にされる

○　ネットワーク内のデータが勝手に暗号化されて使用できなくなる

➡複合するため金銭を要求される（ランサムウェア）

2　今現在、エモテットに感染していないかのチェック

専用チェックプログラム「EmoCheck」で会社内ネットワーク全PCのチェックをする。

➡感染していた場合は、PCのリセット・初期化、流出情報の確認

3　不審なメールを受信した時

メールの発信元に電話で知らせる。

発信源をブロックしないと再度ウイルスメールが送られることもある。

4　不審なメールを送ってしまった時（取引先から連絡を受けたら）

すぐにネットワークをインターネットから遮断して上記2のチェックをする。

5　ウイルス感染、拡大防止策

おかしなメールは開かない。

ZIPファイルを開かない。（パスワード付きもあり）エクセル・ワードの「コンテンツ有効化」「マクロの有効化」のボタンを押さない。

不審メールの発信元に連絡する。

協会職員名（実名）

会員警備会社名（実名）

㈱会員警備保障

神警協アンザイ（nisemono@usouso.or.jp）

宛先：㈱会員警備保障　←　会員警備会社名（実名）

2022.03.03kansen.zip　←　ZIP ファイルは
絶対に開かないでください。

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。
（過去、実際に使用された題名の場合もあります。）

添付ファイル名: 2022.03.03kansen.zip
解凍パスワード: 426219693

会員警備会社名（実名又は不明な会社名）

Tel 044-872-1820 Fax 044-028-2461
Mobile 090-2915-2891
Mail mukai@kss-yokohama.co.jp

←　不明な連絡先。
絶対に連絡しないでくださ