２０２２年２月８日

お取引様 各位

北海道エアポート株式会社

弊社社員からと思われるウィルス付きメールへのご注意のお願い

本日、弊社に Emotet ウィルス付きと思われるメールが届き、一部の社員が誤って添付ファイルを開封したことにより同ウィルスに感染し、弊社社員を偽装したウィルス付きメールが多数の方々に送信される事態が発生致しました。

当該 Emotet ウィルスは、パソコン内の情報を窃取する悪意のあるプログラムを自動ダウンロードし、**過去のメールや様々な情報を外部サーバへ送信、悪用される凶悪なウィルスです。**

また、**過去のメールからお取引様のメールアドレスが窃取され、お取引様宛にウィルス付きメールが届く恐れがございます。**ご迷惑をお掛けし誠に申し訳ございませんが、ご注意いただきますようお願い申し上げます。

弊社内に送信されたメールを参考として下記に記載致しますので、添付ファイルは絶対に開かないようご注意をお願い致します。

記

１. サンプルメール

・下図のように、弊社社員から送信されたように偽装されております。
・送信元アドレスが、弊社と全く異なるドメインとなっております。

From: 社員名 <XXXXXXX@jpclothins.com>
注）送信者のアドレスが弊社と全く無関係です
注）左記以外にも複数確認されております
Sent: Tuesday, February 8, 2022 5:24 PM
To: 受信者名＜XXXXXX.XXXXXX@hokkaido-airports.co.jp＞
Subject: Fwd:【SMS 関連】Safety Information の発行について
注）件名が受信者（お取引様）の例も確認されております

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：2022-02-08_1723.zip
解凍パスワード：UAJHIJMEAX
注）左記以外にも複数確認されております

社員名
Tel XXX-XXX-XXXX Fax XXX-XXX-XXXX
Mobile XXX-XXXX-XXXX
Mail 社員名@hokkaido-airports.co.jp
www.hokkaido-airports.co.jp

２. お問合せ先

北海道エアポート株式会社　企画部 情報企画課（cyber@hokkaido-airports.co.jp）

以　上