≪体制整備の豆知識 Part7≫　　2023.1.23

ふうたのワンポイントレッスン

Ｖｏｌ７　代理店監査におけるプロ代理店の体制（態勢）整備課題（７）

～サイバー犯罪の認識と対応策～

体制整備の豆知識の Part7、7 回目は「サイバー犯罪の認識と対応策」についてお届けします。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

～最近のサイバー犯罪に対する認識と対応策～

警視庁サイバーセキュリティー対策本部の警部補による説明内容をぜひ参考に知っていただきたいのでポイントをお伝えします。

《サプライチェーン攻撃とその対策！》

自社のみならず、関係する取引先（保険会社や取引先など）や繋がりのあるビジネスパートナー等を含めた先にある中小企業を攻撃し、大企業侵入の足掛かりとする攻撃です。

当然、セキュリティー対策が不十分な場合は、被害を受けた取引先業から賠償請求や取引停止などになることがあります。

▼対策:中小企業自身でもできる自衛手段を講じること。セキュリティーソフトは情報資産を守る投資と考えるべきです。

※機械的安全管理措置として、ネットワークへの侵入を監視・防御する「IPS」や端末の挙動監視する「EDR」など。

《メールを悪用した犯罪とその対策！》

悪意のあるメールを送りつけ、感染（ランサムウェア・マルウエア等）させて不正アクセスにより侵入した PC を遠隔操作して情報収集する犯罪が急増しています。

次の（１）～（３）の対策を行う必要があります。

（１）「二段階認証または二要素認証」に加え、「強固な認証設定」を設定する。

※「二段階認証（例）」

ID/パスワードの認証後に登録済のメールアドレスに通知されるワンタイムパスワードを入力する方式など。

※強固な認証の設定（例）

ランダムパスワードによる設定。「英大文字・英小文字・数字・記号から 4 種混ぜ合わせて 10 桁以上（名前、誕生日や簡単な英単語等は不可）」

有料のメールサーバー専門業者とメールサーバーの利用契約のうえ、独自ドメイン（固有管理・有料）を取得し、その専門業者が実施しているセキュリティ対策（アクセス制限等）の設定で、利用・保管する代理店メールのセキュリティー強化をまずは図ってください。

（注意）フリーメールは、業者がメールの内容を機械的に読み取り、ユーザーに見せる広告を選ぶ材料にする等、業者の業務上の情報に利活用されてしまうリスクや、問題発生時にフリーメール業者から調査に協力してもらえない等のリスクがあります。

（２）不明や不必要なメールは開かずに削除する。

▼ウイルスを仕込んだメールの見極め方と対応策

①メール添付ファイルの拡張子を「表示する」設定でパソコンを使用する。

→設定のファイル名拡張子に✓を入れる。

②種類欄に「アプリケーション」とある添付ファイルは絶対に開かない。

→右クリックでファイルの種類を確認。またプログラムファイルではないかプロパティを確認

「不用意に開いたら危ない添付ファイルの種類」

次の拡張子は開かない→.exe/.docm/.xlsm/.wiz/.iqy

③受信したメールで少しでも「おかしい」と感じたら、マクロ付きのファイルを開く前に送信者に確認する。

（３）本文内にある URL の真偽の確認→URL にカーソルを当て、画面下部に実際の URL を表示させ確認する。または右クリックでプロパティのアドレス（URL）を確認する。

作成 ： 日本代協アドバイザー 日本創倫株式会社 代表取締役（CEO） 山本 秀樹
配信 ： 日本代協事務局