標的型攻撃メールに対する注意の徹底について

現在、官公庁や公的機関等に対する深刻なサイバー攻撃と個人情報の漏えい等の問題が相次いで発生していることから、各都道府県中央会における情報取扱い規程及び個人情報保護規程等を確認・順守のうえ、個人情報の保護について万全を期することが求められています。

特に、問題が深刻になっている標的型攻撃メールについては以下の対策等をご確認いただき対処ください。

（１）組織として行う対策例

①ＩＰＡ（情報処理推進機構）等が提供する最新情報を役職員に周知徹底する。

②情報システム担当者またはＩＴ関連事業者等と連携し、情報ネットワークのセキュリティ状況を把握する。

③各種パスワードの複雑化、ファイルの暗号化、アクセス可能領域の細分化、文書機密レベルの設定等を行う。

④不正アクセス等の認知方法と緊急対応手順を確認し、被害発生時に報告を行う連絡先を確認する。【必須連絡先例：システム管理（事業）者、都道府県、全国中央会】

（２）個人で行う対策例

①メールが着信したら、送信者名とアドレスの関連性、添付ファイルの拡張子を確認し、判然としない場合は、開封せずに送信者または信頼できる第三者に確認をとる。

②不審な添付ファイルを開封してしまったら、ネットワーク接続を解除し、システム管理（事業）者に知らせる。

《参考資料》

■「標的型攻撃メールの例と見分け方」

https://www.ipa.go.jp/files/000043331.pdf

（リンク先はＩＰＡですので安心です。Hot-Biz にも掲出しています。）

■ＩＰＡ情報セキュリティ安心相談窓口「よくある相談と回答(FAQ)」

https://www.ipa.go.jp/security/anshin/

（リンク先はＩＰＡですので安心です。）

《事例》

■国内大手航空会社における顧客個人情報の漏洩事件（2014 年 9 月）

『標的型攻撃で最大 74 万件漏洩。社内 PC からのサイバー攻撃への対策が不十分で、情報漏洩に気付くまでに 2 カ月を要した。』

→漏洩検出は困難。侵入され、不正アクセスされることを前提とした対策が重要。