

◆標的型攻撃メール等への対策の徹底のお願い



報道でも取り上げられていますように、この度、日本年金機構において標的型攻撃メールによりパソコン等がウイルス感染し、個人情報が出ました。また、この他にも、企業・組織の機密情報が窃盗されるケースが増えております。

つきましては、下記の事項について改めてご留意いただきますようお願いいたします。

1. 疑わしいメールの削除の徹底

ウイルス付きメールの場合、件名が記載されていない、送信者とメールの内容があわない、不必要に添付ファイルを開かせようとするなど何らかの異常な兆候があります。

送信元や内容が不明なメール、なりすましメール（類似するメールアドレス）が送信されて来ますので、注意してください。また、上記内容のメールは、決して開封することなく確実に削除してください。特に、添付ファイルの開封やメール本文にあるURLのクリックは、絶対に行わないよう徹底してください。

2. セキュリティ対策のないUSBメモリ等の使用禁止

ウイルスの感染経路として、メールの他にもUSBメモリ（外部記憶装置）等にウイルスを仕込むという手法があります。リスクを低減させるために原則として、セキュリティ対策がなされていないUSBは使用しないでください。

3. 業務用データの持ち出し・自宅の個人用パソコンでの作業の禁止

最近のサイバー攻撃は、特定企業の従業員を直接のターゲットにするものが増えており、従業員の自宅のパソコンのメールアドレスも対象にされています。

4. 個人情報の管理の徹底と確認

個人情報の取扱いについては、貴社の個人情報保護規定に基づき、適正な管理を徹底してください。

個人情報などを含む機密性の高いデータについては、ファイル自体にパスワードを施す、アクセス制限をかけたフォルダ等に収納しているかを改めて確認し、徹底してください。

5. パソコン等のウイルス感染等が発生した場合の対処方法の確認

万が一、パソコン等のウイルス感染等が発生した場合の対処について、改めて社内ルールを確認してください。

また、情報セキュリティの強化について、独立行政法人情報処理推進機構（IPA）のホームページ（<http://www.ipa.go.jp/security/index.html>）をご参照ください。

情報セキュリティについてご不明な点、ご質問等がございましたら当所へご連絡ください。