

## 標的型攻撃メールに対しては三位一体の対策を

標的型攻撃メールに起因した情報流出事案が後を絶ちません  
主な要因として次のことが考えられます



- ・リテラシ(情報や知識の活用能力)不足
- ・不十分な運用管理体制・対応策の検討
- ・不十分なシステム対策

### ■標的型攻撃メールに備え、次の対策を「三位一体」で推進しましょう

#### ①リテラシの向上 ②適切な運用管理 ③セキュアなシステムの構築

### ■ポイント

#### 1 受信時のメール取扱方法の再確認と報告の習慣化【リテラシ向上・運用管理】

- ・メールの見分け方などの定期的な教養による警戒心の維持向上
- ・標的型攻撃メール訓練ではクリック率を測るだけでなく、担当部門への報告など取るべき行動の習慣化を促進
- ・取引先を装うメール対策に向け、受信メールの真正性を保証する仕組み(DKIM<sup>※</sup>、SPF<sup>※</sup>)の導入検討

※DKIM、SPF：いずれもメールが確かにその組織から送信されたことを証明する技術のこと

#### 2 被害を回避、低減するためのシステム上の見直し【システム構築・運用管理】

- ・重要情報を保有するデータベースに外部から容易にアクセスできないような保護対策(アクセス制限など)
- ・不審な添付ファイルの安全性を確認する環境整備(ネットワークから切り離れたPCで確認など)

#### 3 インシデント発生に備えた体制整備と訓練の実施【運用管理】

- ・会社等組織内の連絡体制の整備・外部関係者連絡先のリスト化(迷わず初動対応できるよう準備)
- ・発生時における問題の切り分けや対応手順書の整備(問題を早く検知するための整備)
- ・有事の対応に関する社内調整フローの確立(サービス停止など適切に対応するための体制構築)

参考：独立行政法人情報処理推進機構(IPA)ホームページ H28.6.23掲載 注意喚起情報「攻撃の早期検知と的確な初動による深刻な被害からの回復を」  
(詳しくは<https://www.ipa.go.jp/security/ciadr/vul/20160623-ta.html>をご覧ください)

Ksisnetでは、情報漏えいに繋がる「標的型攻撃メール」への危機意識を高めていただくため、初回無料の「**標的型攻撃メール訓練サービス**(Ksisnetホームページ参照)」を提供しています。

また、適切な情報セキュリティ対策を支援する「**IT相談窓口**(下記参照)」を設けていますので、ぜひご活用ください。

ホームページアドレス：<https://www.ksisnet.kyoto/> 【Ksisnet(ケースネット)で検索】

京都中小企業情報セキュリティ支援ネットワーク(Ksisnet)

IT相談窓口(公益財団法人京都産業21 お客様相談室)

相談内容：情報セキュリティ対策、情報漏えい・流出事案等  
※毎週月曜日～金曜日の9:00～17:00(祝日を除く)

TEL 075-315-8660 メールアドレス [okyaku@ki21.jp](mailto:okyaku@ki21.jp)

公益財団法人京都産業21 お客様相談室(〒600-8813 京都市下京区中堂寺南町134 京都府産業支援センター内)

お困りの  
ときは!!