

静岡県警察からのお知らせ

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、SPF※)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)

「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」

<https://www.ipa.go.jp/security/ciadr/vul/20160623-ta.html>

お問い合わせ先

静岡県警察本部生活安全部サイバー犯罪対策課 企画指導係

TEL:(代表)054-271-0110 (内線)711-3496