平成２７年６月発行

Kagawa Cyber Security Information

香川県情報セキュリティ連絡ネットワーク通信 Vol.3

標的型メール攻撃にご注意！

標的型メールとは、組織の機密情報を狙って、特定企業や個人を対象に送り付けられるメールのことです。

典型的な例として、取引先企業の社員や行政機関の職員など信頼性の高い人物を装い、メール本文や件名を業務に関連した内容にしてメール受信者を騙すという手法になります。

メール受信者が偽装に気づかずに不正プログラム（ウイルス）を仕込んだ添付ファイルやリンク（URL）をクリックしてしまうと、ウイルス感染し、パソコン内の情報が漏えいする可能性があるだけでなく、パソコンが接続された組織のネットワーク全体がセキュリティ上危険な状態になる可能性があります。

■標的型メールの着眼点■

1、知らない人からのメールだが、メールの本文の URL や添付ファイルを開かざるを得ない内容
　例）取材申込、講演依頼、問い合わせ、クレーム、アンケート調査
2、心当たりのないメールだが、興味がそそられる内容
　例）議事録、講演原稿、VIP 訪問に関する情報
3、これまで届いたことがない公的機関からのお知らせ
　例）インフルエンザ等の感染流行情報、災害情報
4、フリーメールアドレスから送信されている
5、ファイルが添付されている
6、ショートカットファイル（lnk など）が添付されている
7、何度かメールでやり取りをして信用させた後、添付ファイルを送信してくる

※　詳細は、独立行政法人情報処理推進機構（IPA）がウェブで公開している「標的型攻撃メールの例と見分け方」をご参考にしてください。（http://www.ipa.go.jp/security/technicalwatch/20150109.html）

添付ファイルは、拡張子やアイコンを偽装することが可能です。
心当たりのないファイルが添付されたメールを受信した場合は、必ず差出人に確認しましょう。
自分で判断できない場合は、システム管理者等のセキュリティ専門家に相談しましょう。
自分勝手な判断が、企業・組織に大きな問題を引き起こす可能性があります。

気を付けよう　危険な情報　不審なアプリ

第 10 回 IPA 情報セキュリティ標語コンクール受賞作品

香川県警察本部生活環境課
サイバー犯罪対策室
TEL：087－833－0110