サイバーセキュリティだより

発行 ： 愛媛県警察本部生活安全部生活環境課サイバー犯罪対策室

平成29年
11月8日
Vol.14

フィッシングメール等にご注意！！

フィッシングメール

不特定多数の相手に対し、プロバイダや銀行などを詐称した電子メールを送りつけ、個人情報の入力を促す内容が記載されたポップアップウィンドや偽のホームページを表示させ、個人情報を入力させるといった方法で、相手のアカウント情報（ユーザーＩＤ、パスワード）やクレジットカード番号などの重要な個人情報を盗み出すメール。

標的型メール

標的とした特定の組織に対し、取引先等の関係先を詐称して、重要書類に見せかけたウイルスが添付されたメールを送りつけ、端末にウイルスを感染させるといった方法で、そのウイルスの機能により、機密情報やアカウント情報（ユーザーＩＤ、パスワード）などの重要情報を盗み出すメール。

フィッシングメールの例

メール本文

システムのテストによりますとあなたのアカウントのパスワードは簡単すぎて、安全問題**からございます**。すぐに**パスワードを改ざん**してアカウントをログインするための**二級必要パスワード**として、個人の生年月日を設置して下さい。

こんにちは、このメールは自動送信されています。以下のURLをクリック**しろ。**

http://www.〇〇〇△△.com

差出人アドレス
△△△@〇〇〇△△.com

日本語が不自然

標的となる組織の関係先などを詐称する

実在する組織のホームページのURLに偽装しており、クリックすると別のサイトに転送される

差出人のアドレスを実在するアドレスに偽装している

標的型メールの例

メール本文

株式会社〇〇〇の鈴木です。いつもお世話になっております。

先週発表された貴社の新製品「□□」について、導入を検討しております。

今週または来週、打ち合わせの場を設けていただきたいと存じますが、まずはいくつかの質問を送らせていただきます。回答いただきたく、お願い申し上げます。（**http://www.〇〇〇.com**）

添付ファイル
問い合わせ内容.zip

差出人アドレス
△△△@〇〇〇△△.com

圧縮ファイルが添付されていたり、URLが記載されており、クリックするとウイルスがダウンロードされる

- 〇 メールの差出人アドレスは偽装できるため、実在するメールアドレスであっても安易に信用せず、直接電話などで相手に確認する。
- 〇 相手サイトにアクセスする場合には、メール本文内のURLはクリックせず、Webブラウザから直接公式サイトにアクセスする。
- 〇 添付ファイルを安易に開かない。
- 〇 ウイルス対策ソフトを導入し、常に最新の状態にしておく。
- 〇 OSを常に最新の状態にしておく。

相談窓口 愛媛県警察本部生活安全部生活環境課
サイバー犯罪対策室 TEL 089-934-0110