詐欺メールにご注意を！（ソースネクストサポート通信より抜粋）

令和５年７月　足立秀一

メールやSMSによる詐欺でよく使われる、危険な文言について紹介します。

１．こんな言葉が、危ない

メールの件名やSMSのメッセージで**「重要なお知らせ」「緊急のご連絡」**
などと書かれていると、多くの人が「何だろう」と思いアクセスしがちです。
しかし、それこそが犯罪者の狙いであり、フィッシング詐欺の第１段階です。
ここでアクセスしなければ、被害に遭うことはありません。

２．次の２つの条件が揃えば、詐欺の可能性は高いと思われます。

□　危険のキーワードが使われている
□　心当たりがない

心当たりがなくても、気になってしようがない時は
検索したり、正規サイトで詐欺の情報がないかをチェックしましょう。
うっかりアクセスしてしまった時も、先に進まずに安全を確かめましょう。
アカウント情報やクレジットカード番号の入力や登録を求められたら、怪しいと肝に銘じておくことが大切です。

３．被害に遭わないためにはこんな行動習慣を身に着けましょう！

最も安全なのは、日頃から次のような行動習慣をつくることです。

イ．あらかじめ正規サイトをブックマークしておく。
ロ．メール上やSNSメッセージのリンクからはアクセスしない。
ハ．どうしても気になる時は、検索で詐欺の情報を確認する。
　　ブックマークからアクセスして正規サイトの情報を調べる。
ニ．ウイルス対策アプリを導入する。
　　フィッシングメールを警告したり、フィッシングサイトへのアクセスをブロックしたりと多重的な安全策が取れます。

４．詐欺・危険なトロイの木馬

【悪事の内容】

1）　webページ上に「PCの問題がある」などの警告が表示される。
2）　クリックするとマイクロソフト社のサポートへ電話を促すページが表示される。
　　（表示されている電話番号は犯罪者のもの）

3） 電話を掛けると PC の問題解決のために　遠隔操作ソフトのインストールを勧められたり、クレジットカード情報などの個人情報を聞かれたりする。
サポートページは偽物で、結果として不正な操作で情報を盗まれたり、聞き出した情報を悪用され金銭的な被害に遭ったりします。

（対策）

・心当たりのない表示が出たらブラウザを閉じる。
・ウイルス対策ソフトの導入。

５．Android(スマホ、タブレット)で検出されるトロイの木馬

【悪事の内容】

1）正規アプリだと思ってアプリをインストールする。
アプリの例：ゲーム、VPN、ビデオ、NetFlix、広告なし YouTube/TikTok　等。

2. インストール完了時にエラー画面が表示され、アプリのインストールは失敗に終わる。
インストールの失敗は、インストールしなかったと思わせるための偽装で、実はウイルスに感染し、結果としてネット検索中などに頻繁に広告が出るようになる。

（対策）

・正規サイト以外からアプリをインストールしない。
・ウイルス対策アプリの導入。

以　上