



— 標的型メールの被害に遭わないために —

特定のターゲットに絞ってサイバー攻撃を仕掛けることを「**標的型攻撃**」といいます。その中でも電子メールを利用したものを「**標的型メール**」と呼びます。電子メールは、様々なサイバー攻撃に利用され、手口も非常に巧妙になってきています。被害に遭わないように確認する習慣をつけましょう！



IPAが公表している「情報セキュリティ10大脅威2021」の組織編で
第2位 「標的型攻撃による機密情報の窃取」
になっています。

(参照) IPA <https://www.ipa.go.jp/security/vuln/10threats2021.html>

標的型メールには、**悪意のあるファイル**が添付されたり**URLリンク**が記載されています。

添付ファイルを開いたり、本文のURLリンクにアクセスしてしまうと、以下のような被害に遭う恐れがあります。



特徴

- 【件名】以下のような**メールを開かざるを得ない**ような内容が記載されていることが多い
 - ・製品、サービスや契約に関する問い合わせやクレーム
 - ・至急対応依頼
 - ・公的機関からのお知らせ
 - ・アンケート調査
- 【メールアドレス】
 - ・フリーメールアドレス
 - ・差出人のメールアドレスと本文の署名に記載されたメールアドレスが異なる
- 【本文】
 - ・不自然な日本語が使われている
 - ・記載のURLが実際のURLと異なる
 - ・署名に記載された組織名や電話番号等が実在しない
- 【添付ファイル】
 - ・実行形式ファイルやショートカットファイル（拡張子が.exeや.lnk等）
 - ・アイコンや拡張子を偽装（実行ファイル形式を文書ファイル等に偽装）

対策

- ・OSや各種ソフトウェアを更新して、最新の状態にする
- ・セキュリティ対策ソフトウェアを導入する
- ・送信元が判然としないところからのメールは安易に開かない
- ・本文に記載されているURLリンクをよく確認をする