



# 標的型攻撃メールに注意！

## 標的型攻撃メールとは？

標的型攻撃メールとは、特定の組織（官公庁や企業）だけに送られるメールで、その目的は、個人情報等を窃取することです。

標的型攻撃メールは、

- 新聞社や出版社からの取材申込のメール
- 就職活動に関する問い合わせのメール
- 製品に関する問い合わせのメール
- セキュリティに係る注意喚起のメール
- 製品の注文メール・海外からの注文を装ったメール

など、受信者がメールを開くよう巧妙に作られています。

### 【標的型攻撃メールの例】

	日時	2015/06/11 (木) 14:32
	差出人	Sec-marumarusoft@example.com
	タイトル	〇〇ソフトの脆弱性の修正について (MM15-XXX)
	宛先	cyber-police@saga.police.go.jp
<p>日本〇〇ソフト株式会社の〇〇ソフトにリモートからコードが実行される脆弱性が発見されました。 この脆弱性を悪用した攻撃が確認されたとの情報があるため、添付文書の手順に従って、MM15-XXX を至急適用してください。 詳細は、日本〇〇ソフト株式会社から提供される情報を参照して下さい。 <a href="http://tech.marumarusoft.com/ja-jp/security/mm15-xxx">http://tech.marumarusoft.com/ja-jp/security/mm15-xxx</a></p>		
添付ファイル	脆弱性 (MM15-XXX) の修正方法.zip (106KB)	

フリーメールアドレスが使用されている！

ZIP (圧縮) ファイルが添付されているため、慎重な対応が必要！

## 標的型攻撃メールの対策

- 不審なメール等を受信した場合は、電話等で送信元に直接確認する。
- インターネットに接続されたパソコン等に個人情報を保存しない。
- 個人情報にはパスワードを設定する。
- 万が一、添付ファイルを開いた場合は、ネットワークから切り離す。