

# HUMAN FACTOR

## 2017

不正なメールはコードではなく、人の弱点を利用します。

サイバー犯罪者は様々な手口でユーザーを騙し、不正なメールやソーシャルメディアの投稿を開かせようとします。2016年に顕著だった傾向をまとめました。



### ビジネスメール詐欺 (BEC) 攻撃が急増

2015年に1%だったBECのメッセージ量は2016年の終わりには**42%**に増加しています。



### ソーシャルメディアを利用したフィッシング詐欺

2016年はソーシャルメディアアカウントによるフィッシング詐欺が**150%**増加しました。



### 曜日によってマルウェアの種類が異なる

ランサムウェアは火曜日から木曜日の間に出現する傾向があります。



### 時は金なり

不正なURLのクリックの**87%**は最初の24時間以内に行われています。



約50%は1時間以内



25%は10分以内

### 攻撃のピークは日中

仕事が始まってから**4~5時間後**がクリックのピーク。ちょうど昼休みが危ない時間帯です。



### 偽のモバイルアプリ

不正なアプリは、**ブランドを装い、紛らわしい名前**を使ってユーザーにマルウェアをダウンロードさせようとします。



### スマートフォンの増加でリスクも増大

不正なURLのクリックの**42%**はモバイルデバイスで発生しています。**昨年の20%から**倍増しています。



レポートの完全版をダウンロード

[proofpoint.com/jp/resources/human-factor-report-2017-form](http://proofpoint.com/jp/resources/human-factor-report-2017-form)