# 標的型攻撃メール訓練(※)の目的と活用
# ～効果を上げる方法～

| | | |
|---|---|---|
| 訓練の目的<br>期待する効果 | Step1. | 社員が攻撃メールの罠に引っ掛からなくする |
| | Step2. | 組織の感染可能性の芽を早期に摘む |
| | Step3. | 引っ掛かった社員を早期に発見し、初動対応をとる |
| | Step4. | 組織として、被害を低減、最終甚大被害を回避する |

| | |
|---|---|
| Step1. | ① メールを怪しい（タイトル、送信者/アドレス etc.）と判断したら開封しない。<br>② 開封して、怪しければ（業務や組織を騙っている、心当りのない組織から etc.）、添付ファイルや記載リンクをクリックせず、破棄する。 |
| Step2. | ③ 開封して、怪しければ（業務や組織を騙っている、心当りのない組織から etc.）、添付ファイルや記載リンクをクリックせず、システム管理部門に報告する。システム管理部門は、分析をして、組織内へ注意喚起し、報告を呼びかける。 |
| Step3. | ④ 誤って添付ファイルや記載リンクをクリックした際、表示内容が業務外であったり、適切な表示がなかったり、動作に違和感を覚えたら、即座にシステム管理部門に報告し、指示を仰ぐ。<br>⑤ システム管理部門は、当該端末の緊急措置（ネットからの隔離等）、攻撃メールの着信を 組織内へ注意喚起、報告の呼び掛け、同一攻撃メールの着信の有無と処理状況をログ（アーカイブ）等で確認する。 |
| Step4. | ⑥ 当該端末のネットワークからの切り離し、ウイルスの駆除、可能であればウイルスの分析で得られた情報による組織内汚染状況の検査などを実施し、さらにその分析で得られた今後の攻撃を回避するための情報を、ネットワークサーバ等に設定する。 |

標的型サイバー攻撃における対策は多くの場合 Step1.までを行い、開封率やクリック率をユーザーのセキュリティ意識向上の判断材料等に活用されるに留まっている。しかし、組織にとっては、一人でも引っ掛かる人がいれば、結果的に侵入を許してしまうことになる。そのため、Step2.では感度の高い人の「気付き」を活用し、組織内で共有することにより被害を回避する方法を推奨している。また、Step3、Step4 は、罠にかかっても感染後に組織としてできるだけ早く対策がとれるよう、訓練を実施することで被害回避能力の大幅向上が期待できる対策である。

※標的型攻撃メール訓練

自組織の IT システムユーザーに対して教育のため偽の標的型攻撃メールを送信し、各ユーザーがメールの不審な点に気付いて開封を回避できるか、添付ファイルを開封したり本文に記載された URL をクリックするなどの危険な行動を回避できるかを、模擬的に訓練することで、標的型攻撃メールへの耐性の向上を図る。