攻撃メールへのリスクレベルを評価把握！
ユーザ端末のマルウェア感染確率を大幅に低減！

GSX
GLOBAL SECURITY EXPERTS

標的型メール訓練サービス

標的型攻撃メールに対する、技術的な対策の限界

標的型攻撃における最も典型的な攻撃手法は、**"マルウェアを含む添付ファイル"**や、**"マルウェアに感染させるためのURLリンク"を記載したメール**をユーザ(一般社員)に送りつける、標的型攻撃メールによる攻撃と言えます。

誤ってこの攻撃メールを開いた場合、「ウィルス対策ソフトでは検知できない」あるいは「PCやデータが破壊されるなどの症状が現れない」等の理由から、マルウェアに感染した事実自体に気が付かないまま、結果的に重要情報を盗み出される危険性があります。

この様な標的型攻撃メールに対して、技術的な対策を実施しても100%の防御は難しく限界があるのが実情です。

この様な背景から【標的型メール訓練】による ユーザへの教育啓蒙が、有効な対策手段のひとつとして、一般企業や行政機関で積極的に取り組まれています。

標的型メール訓練とは

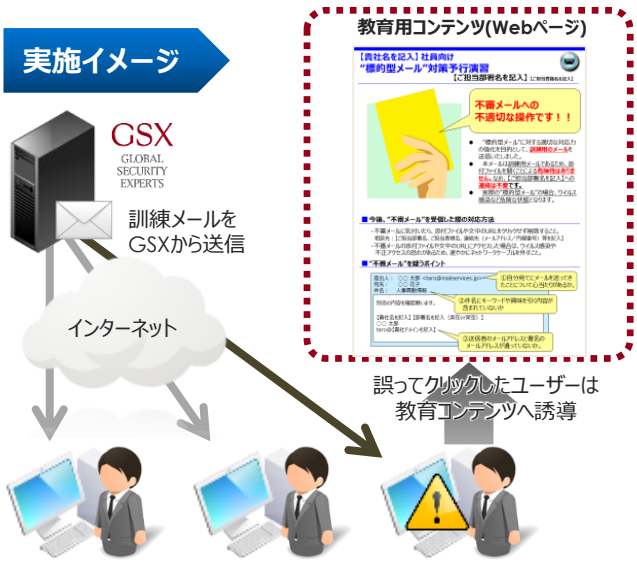
標的型攻撃を模擬した【訓練メール】をユーザに送信し、標的型攻撃メールへの対応を教育訓練するサービスです。

クリック状況をユーザ毎にログ取得、結果をクリック率で報告

誤ってクリックしたユーザには、教育コンテンツを閲覧表示

添付ファイル方式では訓練メールの添付ファイル、URLリンク方式では訓練メール本文中のURLリンクをクリックしたユーザについて、教育コンテンツ表示・ログ取得します。

実施イメージ



標的型メール訓練を実施するメリット・効果

調査・評価目的でのメリット

① 攻撃メールへのリスクレベルを評価把握！

実際に、どの程度のユーザが攻撃メールを開封してしまうか、現状のリスクレベルを調査把握する事が可能です。より踏み込んだ技術的な対策などの導入をご検討される場合、この結果を参考にすることが可能です。

教育・啓蒙目的でのメリット

② ユーザ端末のマルウェア感染率を大幅低減！

ユーザが攻撃メールを誤って開封してしまう確率が半分になれば、ユーザ端末のマルウェア感染リスクも半分になります。過去の実績では、継続的にあるいは複数回メール訓練を実施した場合、そのクリック率は半分~三分の一まで低減しています。

教育・啓蒙目的でのメリット

③ 感染時の初動対応を徹底し、被害を最小化

ユーザーが攻撃メールを誤って開封してしまった場合でも、適切な初動対応ができれば被害を最小化することが可能です。教育コンテンツに、"LANケーブルを抜いてヘルプデスクへの報告"するルール等を記載することで、適切な初動対応についても教育訓練が可能です。

GSX標的型メール訓練サービスの特長

GSX独自開発システムによる、柔軟なカスタマイズ対応

初めての訓練でも、手間を掛けずに、効果の高い訓練を実現するサポートコンテンツ

訓練サービス自体への万全のセキュリティ対策

標的型攻撃対策のエキスパートによる訓練全般のサポート・アドバイザリー

サポートコンテンツ(一部)

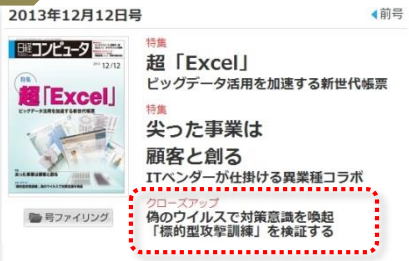
実施前の事前教育
訓練後の事後教育

予告通知メールサンプル
終了通知メールサンプル
ヘルプデスクマニュアルサンプル

サービス提供実績 (一部抜粋)

業種業態	規模	備考
金融機関A	1,000名	実際のマルウェア感染時のユーザ対応の訓練・評価のため実施
製造業B	110,000名	実施後、グループ会社各社へ波及。継続的に訓練を実施中
製造業C	5,000名	グループ会社120社で同時実施
製造業D	500名	防衛関連部門および役職者に対して実施
サービス業E	2,000名	全社員に対しセキュリティ強化月間の中で実施
通信業F	500名	全社実施前、事業部門を選択してパイロット的に実施
官公庁G	1,000名	情報セキュリティ監査業務の一部として実施

新聞・雑誌掲載実績



導入事例

- 電源開発株式会社様 東証一部上場 グループ 7,000人規模
- ポケットカード株式会社様 東証一部上場 全社 450人規模
- 学校法人北里研究所様 研究所内 2,500人規模
- 丸文株式会社様 東証一部上場 グループ 1,400人規模

FAQ

Q1 発注から訓練実施までにどの程度の期間が必要ですか？

最短2週間ほどで実施が可能です。お客様内での社内体制のご準備や事前教育などを実施されるにあたり、ご発注頂いてから3～4週間程で訓練を実施されるのが一般的です。

Q2 標的型メール訓練を受けた対象者の反響が気になるのですが？

多くの対象ユーザの方からは、「座学やeラーニング等による教育研修と比べ、訓練として実感体感できる事から、分かりやすい。」との反響を頂いております。

Q3 訓練を開始する前に、事前に対象者に向け教育コンテンツを配布して事前教育を実施してから訓練開始したいのですが？

事前教育用の教育コンテンツ資料をご提供しています。自社のルールに沿った内容に変更のうえ活用頂くことも可能です。

Q4 訓練メールをクリックしてしまった際の教育コンテンツを表示させず、クリックしたログだけを取得することは可能ですが？

対応可能です。教育コンテンツは白紙もしくは任意のコンテンツを表示させ、ログだけを取得することができます。

Q5 他社サービスで何度かメール訓練を実施済みですが、もっとレベルの高いメール訓練を実施してみたいのですが？

訓練メールの文面などもさることながら、弊社メール訓練サービスでは、よりレベルの高い訓練をご希望のお客様に向けた訓練システムの機能もご用意しております。（詳細は別途お問合せ下さい）

Q6 送信する訓練メールの内容や教育コンテンツ内容は変更可能ですか？

双方とも数種類の雛形サンプルをご提供しております。また、内容は自由にカスタマイズが可能です。更に、標的型攻撃対策のエキスパートがアドバイザリーとしてご相談に応じております。

Q7 訓練メールを添付ファイル方式で実施する場合、MicrosoftOffice等のソフトウェアバージョンに依存しませんか？また受信するメーラーへの依存はありませんか？

双方とも数種類の雛形サンプルをご提供しております。また、内容は自由にカスタマイズが可能です。更に、標的型攻撃対策のエキスパートがアドバイザリーとしてご相談に応じております。

Q8 訓練メールは一斉に対象ユーザに送信されるのですか？メールサーバの負荷が心配です。また一日にどの位の対象者に送信可能ですか？

対象ユーザにはタイムラグを持って順次送信しますので、メールサーバへの負荷は特にありません。(このタイムラグについても調整可能)本システムは、一日の営業時間帯に約5,000件の対象ユーザへの送信実績があります。

本カタログは、2017年7月時点における内容になります。