情報システム監査株式会社

標的型メール攻撃訓練のご案内

標的型メール攻撃訓練とは

標的型メール攻撃とは組織の情報の盗難を目的として、実在の企業名や官公庁名をかたって特定の組織や人物に送られるメールを用いた攻撃手法のことです。メールの添付ファイルを開いたり、本文中のURLをクリックするとウイルスに感染する仕掛けが施されており、ウイルスに感染したことに気付けないまま日々を過ごすと、重要情報が盗まれる危険性があります。

このような標的型メールに対して、「ウイルス対策ソフトでは検知できない」、「パソコンやデータが破壊される等の症状が現れない」等の理由から、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。

こういった背景から、訓練による従業員への教育啓発が有効な対策手段のひとつとして一般企業や行政機関において積極的に取り組まれています。また、組織で整備した対応ルールの妥当性・適切性の確認等もできるため、組織全体のセキュリティレベルの向上にもなります。

2015 年において社会的影響が大きかったセキュリティ上の脅威（組織）において、標的型攻撃が1位に挙げられています

この攻撃手法の脅威が顕在化し、組織内部の情報漏えいが社会問題化しています。

順位	タイトル
1	**標的型攻撃による情報流出**
2	内部不正による情報漏えいとそれに伴う業務停止
3	ウェブサービスからの個人情報の窃取
4	サービス妨害攻撃によるサービスの停止
5	ウェブサイトの改ざん
6	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加
7	ランサムウェアを使った詐欺・恐喝
8	インターネットバンキングやクレジットカード情報の不正利用
9	ウェブサービスへの不正ログイン
10	過失による情報漏えい

出典：「情報セキュリティ10大脅威 2016」 独立行政法人情報処理推進機構（IPA）

標的型メール攻撃訓練 サービス

本サービスでは標的型メール攻撃に対する知識の習得や対応力の向上を目指します。

＜目標＞

1. 標的型メールの開封、未開封に関わらず、適切な行動を取る → 標的型メール攻撃訓練により実施
2. 訓練の結果に応じて、行動の適切性を参加者自身で確認する → 集合研修により実施

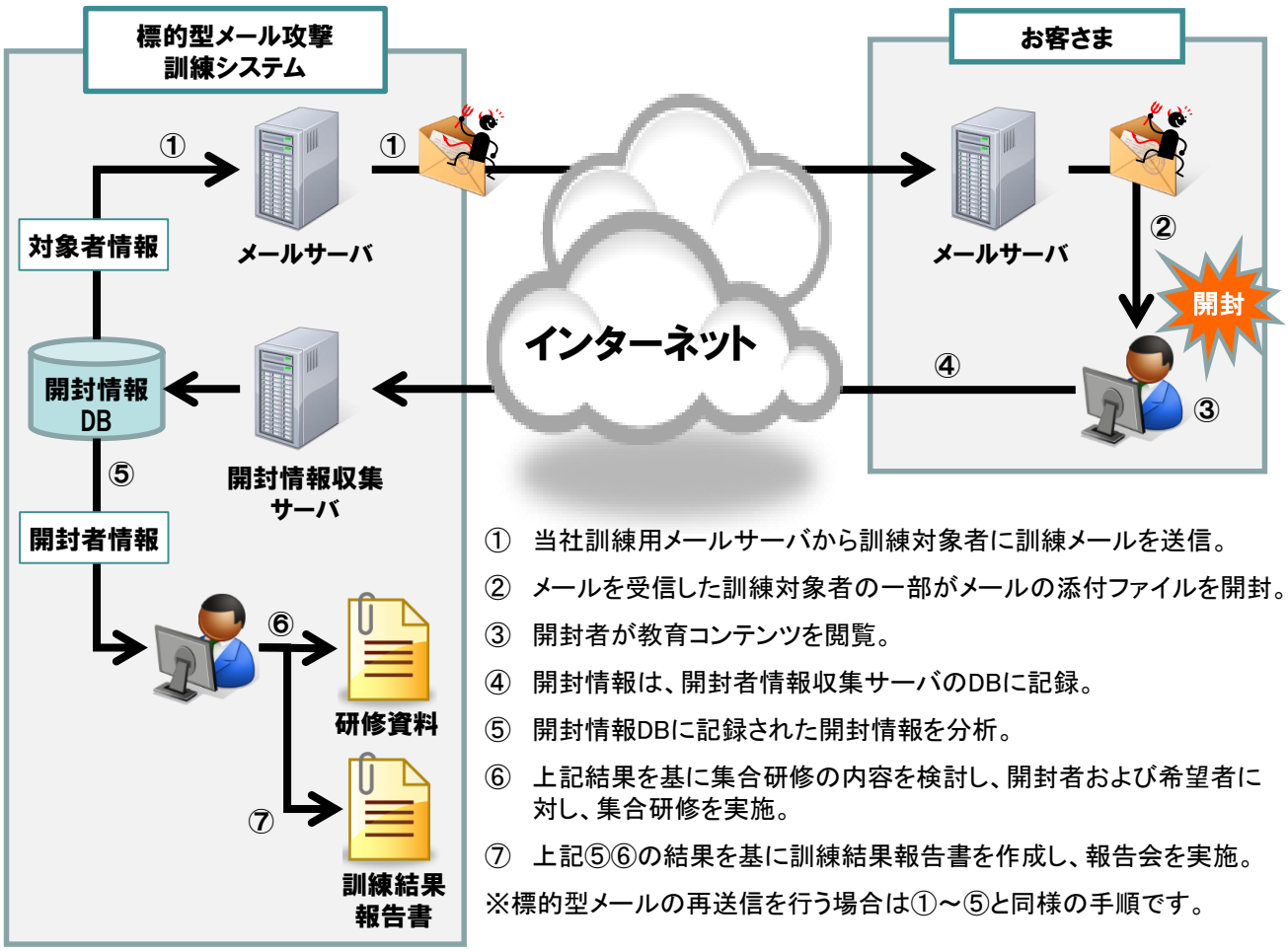
サービスの詳細は次ページをご覧ください

■ 標的型メール攻撃訓練 サービスの流れ

擬似的な標的型メールを送信し、標的型攻撃の脅威を体験していただきます。

送信したメールを開封した場合は、教育用コンテンツを表示して標的型メールの危険性についての周知を行い、開封情報を取得します。開封情報により開封率を集計、分析し、その情報を基に対応力等について訓練結果報告書で報告いたします。

なお、訓練メールや教育コンテンツの内容はご希望に応じて変更することが可能です。



① 当社訓練用メールサーバから訓練対象者に訓練メールを送信。

② メールを受信した訓練対象者の一部がメールの添付ファイルを開封。

③ 開封者が教育コンテンツを閲覧。

④ 開封情報は、開封者情報収集サーバのDBに記録。

⑤ 開封情報DBに記録された開封情報を分析。

⑥ 上記結果を基に集合研修の内容を検討し、開封者および希望者に対し、集合研修を実施。

⑦ 上記⑤⑥の結果を基に訓練結果報告書を作成し、報告会を実施。

※標的型メールの再送信を行う場合は①～⑤と同様の手順です。

■ 実績

中央省庁、地方公共団体、民間企業　　※数十名～数万名まで幅広い訓練実績があります

■ 価格

送信する対象数や回数、訓練後の対策（教育・アンケート）等の有無をお聞きした上で、お見積りいたします。

情報システム監査株式会社　営業部 CS営業課

●当社ホームページ　http://www.isanet.co.jp　　●E-Mail：isasales@isanet.co.jp

東京本社　TEL：03-5783-8680　東京都港区港南2-12-27　イケダヤ品川ビル8階
大阪本社　TEL：06-6395-7665　大阪市淀川区宮原4-4-50　南都ビル9階
名古屋営業所　TEL：052-566-1238　名古屋市中村区名駅南1-23-14　ISE名古屋ビル8階