標的型メール訓練サービス

～実践型セキュリティ教育サービス～

増え続ける標的型メール攻撃
組織としての対策をしていますか？

～ 一人のメール開封で多数の情報流出のリスクがあります ～

標的型攻撃メールは、近年ますます巧妙化、複雑化し、被害が増加しています。
標的型攻撃メールは、従来のウイルス対策ソフトで検知しにくく、完全に防ぐことは不可能です。一人でも標的型攻撃メールを開封してしまった場合、ウイルス（マルウェア）に感染し、情報が漏えいしてしまいます。
一人ひとりのセキュリティ意識の向上によって、標的型攻撃メールを開封するリスクの低減につながります。

サービス概要

本サービスは、模擬的な標的型メール（不審メール）を実際に受信し、開封結果を報告書にまとめ、訓練実施後のセキュリティ対策につながるサービスとなります。実際に標的型メールを受信した場合を想定しており、マルウェア感染のリスク低減と組織における対処への理解を促進します。

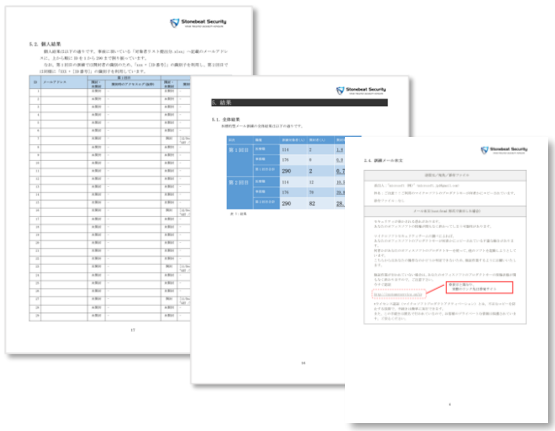
実施項目

- 対象（スコープ）選定
- メールコンテンツ選定
- 対応の準備・確認
- 担当部署責任者と実施調整
- 標的型メール（不審メール）の送信
- 実施結果のご報告
- 事後対策の実施フローご確認

サービス内容

サービス名	標的型メール訓練サービス	
実施対象	全ての組織にご提供中	
実施方法	疑似的な標的型メール（不審メール）の送信、開封率を調査・分析・報告	
サービス内容	対象（スコープ）選定	全従業員、全正社員、特定の部署、特定の対象者など実施対象者を選定します。
	メールコンテンツ選定	対象者にあわせて、メールコンテンツを選定します。また、メールのテーマ、差出人のメールアドレス、メールの本文、添付ファイルを作成します。
	対応の準備・確認	不審メールを受信した場合の対応フロー（ユーザからの問い合わせ窓口、連絡体制、対応手順など）の有無の確認、対応フローの事前周知、問い合わせ窓口との調整・準備を行います。
	担当部署責任者と実施調整	対象部署の責任者・担当者へ実施説明を行い、実施日程や実施回数を調整します。
	疑似的な標的型メールの送信	対象者へ模擬的な標的型メールを送信します。添付ファイルまたはWebリンクをクリックした対象者には、啓発コンテンツが表示されます。
	実施結果のご報告	訓練結果や不審メールの添付ファイルまたはWebリンクをクリックした対象者をご報告し、結果に応じた必要対策をご提案します。
	事後対策の実施フローご確認	標的型メールの脅威、対策、セキュリティ脅威動向などについて、セキュリティ研修を実施します。（オプションサービス）
実施期間	約１~3ヵ月程度（実施規模によって期間が変わります）	
成果物	報告書 （訓練結果の総評、統計情報、開封率、結果に応じた必要対策類など）	
価格	メール送付数や実施時期などをご確認の上、お問い合わせください	

-報告書サンプル-



■お問い合わせ
ストーンビートセキュリティ株式会社
TEL：050-6877-5988
E-mail：sales@stonebeat.co.jp

Stonebeat Security
Your Trusted Security Advisor
www.stonebeat.co.jp