令和元年７月４日

「令和元年度　標的型攻撃メール訓練業務」の公募について

独立行政法人　中小企業基盤整備機構
情報システム基盤センター長　橋本　大哉

１．目的

年々増加、巧妙化する標的型攻撃メールによる個人情報等の機密性の高い情報の漏えいリスクを最小化するためには、技術的な対策以外に、標的型攻撃メールに記載されたＵＲＬのクリックの防止やＣＳＩＲＴへの報告等に関する各ユーザのリテラシーを向上させることが重要である。感染拡大の防止及び感染後の速やかな対策の必要性の認識を高めるため、訓練の実施を行う必要があるものと考えている。

本業務においては、標的型攻撃を模擬した訓練メールを訓練対象者へ送信し、メールに記載されたＵＲＬのクリック、添付ファイル開封などの行為を体験させることにより、標的型攻撃に関する理解を深め、メールを開く際の注意、ＣＳＩＲＴへの迅速な報告の必要性など、情報セキュリティに対する職員等のリテラシーの強化を目的とする。

併せて、受講者の学習効果が期待できるよう、セキュリティ研修等（e ラーニング、アンケートなど）のツールを活用した一連の研修を実施する。

２．業務の内容

本業務の実施内容は以下の通りである。

（１） 標的型攻撃メール訓練

- 中小機構メールアドレスを有する者に対しておこなう。
- 訓練対象アドレス数は約1,900件とし、最大でも2,000件とする。
- 訓練実施（訓練メール送信～クリック状況の集計等）のために必要な環境を準備し、正常に動作するのに適した設定調整等を行うこと。
- 環境の準備にあたっては、以下を要件とする。
  ① サーバの設置場所は日本国内とする。
  ② 訓練メールの差出元メールアドレス、差出人表記は任意に設定できるものとする。
  ③ 一時間に1,000件程度のメールが送信できる性能を有すること。
  ④ 訓練メールに記載されたＵＲＬをクリックまたは添付ファイルを開封した者を確認、集計するための仕組みを用意すること。
  ⑤ メールサーバやメール送信端末等が不正アクセスされないよう、かつウイルスに感染しないよう適切なセキュリティ対策を施すこと。
- 中小機構にて利用しているセキュリティ機器、メールフィルタ等の設定状況について確認し、訓練メールが迷惑メールやマルウェア等と認識されないよう訓練実施に必要な対策をとること。
  またセキュリティ機器、メールフィルタ等の調整が必要となる場合には、調整に必要となる情報を提示すること。
- 中小機構側にて設定変更等の作業が必要な場合について、中小機構への適切な情報提供および中小機構からの問い合わせへの対応を行うこと。
- 訓練実施のために必要なデータ登録（訓練対象者の所属部門、メールアドレス等）を行うこと。中小機構から提示する基データを訓練実施環境登録に必要なフォーマットに変換するデータ加工作業を含むものとする。
- 本調達業務実施のために必要な一連の動作について各種テストを実施し、問題がないことを確認すること。
- 確認結果については、中小機構へ報告を行い、了承を得ること。

・訓練実施に向けてシステムが正常に動作しない場合は、原因の切り分けを行い、受注者の責任および負担において正常に動作させること。
・テストに必要となる資材、機器、物品、消耗品、什器等は受注者の負担において準備すること。
・訓練実施のために必要なコンテンツ（標的型攻撃を模した訓練メール、訓練対象者がクリックした際に遷移する画面等）を準備し、中小機構と協議の上で内容を確定し、訓練実施環境へ装備する。
① 訓練メールは、あらかじめ受注者が準備し、中小機構との打合せにより内容（標題、発信元、本文、添付ファイル等）のカスタマイズを行うこと。
② 訓練メールは、情報セキュリティや標的型攻撃に関する最新の知見・動向等を反映した内容とすること。
③ 各訓練対象者のメールアドレスへ、訓練メールに記載されたＵＲＬのクリックまたは添付ファイルの開封により表示する内容の２種類の訓練メールを作成すること。添付ファイルはMicrosoft Word、Excel、PowerPoint、PDFのいずれかの形式とする。
④ 同一の訓練期間において、訓練者を複数のグループに分け、それぞれ異なる内容の訓練メールの送信を行えること。
⑤ 合計2回の訓練メール送信を行うが、訓練メールの内容（件名、差出人、本文等）は同一とせず二通り以上作成すること。
⑥ 訓練対象者から不審なメールと容易には判断できないタイトル・送信元・内容等とすること。
⑦ 訓練対象者がＵＲＬのクリック等をした際に遷移する画面は、訓練メールであることを通知するとともにセキュリティ意識の向上を促し、かつ初動対応を促す内容とする。
⑧ 訓練対象者がＵＲＬのクリック等をした際に遷移する画面は、あらかじめ受注者が準備し、中小機構との打合せにより内容のカスタマイズを行うこと。
・訓練実施計画および訓練用コンテンツの内容に基づき、訓練メールを訓練対象者へ送信し、訓練を実施すること。
① 訓練対象者のメールアドレス宛てに、訓練メールを2回に分けて送信する。
② 訓練メールに記載されたＵＲＬをクリックまたは添付ファイルを開封した場合は、啓発画面（標的型攻撃メール訓練であることの表示・標的型攻撃メールに関する啓発内容・ＣＳＩＲＴへの報告の指示等）へ遷移する。
③ ＵＲＬをクリックまたは添付ファイルを開封したクリック者について結果を集計する。
④ 1回目の訓練実施後、一定期間経過後（１月程度を想定）に２回目の訓練を実施することとし、1回目と2回目の結果を比較する。
・訓練の実施にあたっては、中小機構のシステム環境への負荷を考慮し、影響のない実施方法とすること。事前に中小機構と打合せを行い、調整した上で実施すること。
・訓練中は中小機構情報システム基盤センター担当者からの問い合わせに対し、窓口等を設け、受注者自らが速やかに適切な対応をすること。
訓練対象者の訓練実施情報を記録、集計する。ＵＲＬをクリックまたは添付ファイルを開封したクリック者について、日時、部署別、職制別に人数・率等を集計すること。
① クリック者について、以下を把握できること。
- ＵＲＬをクリックした者
- 添付ファイルを開封した者
- 上記の両方を行った者

② 添付ファイルを開封したメールについて、以下を把握できること。把握できないケースがある場合は具体的に内容を提案書へ記載すること。

- 中小機構メールからクリックした者

③ ＵＲＬリンクをクリックしたメールについて、以下を把握できること。把握できないケースがある場合は具体的に内容を提案書へ記載すること。

- 中小機構メールからクリックした者

・訓練結果の集計・分析結果を、中小機構へ報告すること。
・訓練メール送信1回目及び2回目の各結果速報（電子ファイル）も別途報告すること。
・クリック者数やクリック率の分析は、日時、部署別、職制別、訓練メールの内容（上記①）別を含む観点から行うこと。
・集計期間は2週間以内を想定している。
・集計・分析結果は、グラフや表等にとりまとめ、分かりやすい表記とすること。
・中小機構が今後必要な情報セキュリティ強化の対策を検討することができるよう情報セキュリティ対策に係る課題及び対応案を中小機構へ報告すること。

（２） 教育の支援

・標的型攻撃を含む情報システム利用に関するセキュリティ意識の向上を目的としたeラーニングによる教育の支援を提案し、中小機構の了承を得た上で実施すること。
・訓練メールにあるURLまたは添付ファイルをクリックした者及び職員等に対しておこなう。
・実施時期は、各訓練メールの送信後とし、一定の受講期間（１月以上を想定）を設けること。
・eラーニングシステムについては、管理画面等で受講結果（受講状況）を把握できるものを提供すること。
・教育の内容は、訓練メールにあるURLまたは添付ファイルをクリックした者及び職員等が、情報システム利用に関する脅威を自身の身の回りに存在するものとして認識を持ち、脅威への対策の必要性やルール順守の重要性に関する意識付けができるような内容である必要がある。
・本調達で受注者が中小機構へ提供する教育用コンテンツ（資料等）については、中小機構が本調達による業務終了後も教育用資料として機構内部で利活用することを前提とし、これを承諾すること。
・eラーニングによる教育の受講結果（受講者数等）を集計し、報告すること。

＜参考＞

- 中小機構では、LMS（Learning Management System）を活用したEラーニングを実施している。

〔主な仕様〕

１）利用環境

・パソコン、スマートフォン、タブレット端末による利用が可能なマルチデバイスに対応していること。
・Windows7以降、ios、Androidによる利用が可能であること。
・InternetExplorer11.0以降、Safari、Chromeによる利用が可能であること。

２）利用時間

・利用可能時間帯は原則24時間365日とすること。

３）利用ユーザ数。

・５０ユーザが同時にシステムを利用できること。

４）システム基本要件

①システム設置場所

・e-ラーニングシステムを提供するサーバは、日本国内に設置していること（バックアップを含む）。
・クラウド環境を設置しているデータセンター施設は、日本データセンター協会の定め

るデータセンターファシリティスタンダードのティア２相当以上のサービスレベルであること。

・クラウド環境を設置しているデータセンター施設におけるセキュリティは以下を充足していること

- TLS(2048bit)による通信の暗号化
- サーバ証明書の発行
- ファイヤーウォールの設置

・伝送データは全て暗号化されていること。

②アクセス制限

・ユーザＩＤとパスワードでアクセス制限を実施できること。
中小機構では、地方拠点と本部（虎ノ門３７森ビル）を接続するテレビ会議システムの仕組みを導入している。

（３） アンケートの実施

・（２）のｅラーニングの受講者に対してアンケートを実施する。

・アンケートの内容は、標的型攻撃に関する訓練対象者の理解度や情報セキュリティ意識を把握できるものとする。
ＵＲＬのクリック者に対する項目だけでなく、クリックしていない者への訓練メールだと気づいた点など記述形式の項目も想定している。

・アンケート実施結果について記録し、職制別に集計・分析し、報告すること。

・集計期間は２週間以内を想定している。

・集計・分析結果は、グラフや表等にとりまとめ、分かりやすい表記とすること。

３．業務の実施期間

本業務の実施期間は契約日から令和２年１月３１日までとする。

４．請負先選定の方法

総合評価方式により、企画および価格の合計点により選考を実施し、最も点数が高い１者を選定する。

（１）公募参加者から「企画書等」の提出を受ける。

（２）本業務の請負先選定に関して設置される「企画評価委員会」が、公募参加者からのプレゼンテーションにより、企画の評価を行う。

（３）企画評価にあわせて「入札書」の提出を受け、価格評価を行う。

（４）企画評価と価格評価の合計点により、最も点数が高い１者を請負先として選定する。

５．請負先選定日程

（１） HP への入札公告	令和元年７月　４日（木）
（２） 入札説明会	令和元年７月２２日（月）
（３） 質問書提出期限	令和元年７月２６日（金）
（４） 質問書回答	令和元年８月　１日（木）
（５） 企画提案書および入札書等提出期限	令和元年８月１９日（月）
（６） 企画評価委員会（プレゼンテーション）	令和元年８月２２日（木）
（７） 開札	令和元年８月２７日（火）
（８） 契約締結【予定】	令和元年８月３０日（金）

６．参加資格

（１）中小企業基盤整備機構契約事務取扱要領（要領 16 第 29 号）（以下「要領」という。）第２条および第３条の規程に該当する者でないこと。※要領については、当機構HP を参照のこと。

https://www.smrj.go.jp/org/info/bid/contract/index.html

（２）中小機構の反社会的勢力対応規程（規程 22 第 37 号）第２条に規定する反社会的勢力に該当する者ではないこと。
https://www.smrj.go.jp/org/policy/index.html

（３）中小企業基盤整備機構平成 29・30・31 年度競争参加資格審査において、「役務の提供等（３３０３ 調査・研究）」、「役務の提供等（３３０４ 情報処理）」、「役務の提供等（３３０６ ソフトウェア開発）」のいずれかに登録された者で、「A」または「B」区分に登録されている者であること。また、全省庁統一資格において当該資格を有する同業区分の「A」～「C」いずれかの等級に格付けされた者は、その資格をもってこの競争に参加できるものとする。
なお、新たに競争参加資格を登録する者は、令和元年８月５日（月）１７時（必着）までに中小企業基盤整備機構　財務部調達・管理課に必要な書類を添えて競争参加資格の申請を行うこと。
※申請方法、申請書類等は、当機構の「平成 29・30・31 年度競争参加資格審査申請書提出要領（物品製造等）」に基づき作成すること。なお、要領、申請方法、申請書類等については、当機構 HP を参照のこと。
https://www.smrj.go.jp/org/info/bid/qualification/index.html

（４）政府機関及び独立行政法人、地方公共団体における入札への参加制限や指名停止等の処分を受けていないこと。

（５）ISO27001（ISMS）または ISO9001（QMS）の認証を取得していること。

（６）現在、機構の専門家として業務委託契約を締結している者、または専門家が役員等に所属する法人に該当する者ではないこと。

（７）令和元年７月２２日（月）に実施する説明会に参加していること。

７．入札説明会　実施日時等

「令和元年度　標的型攻撃メール訓練業務」についての説明会を下記のとおり実施する。

開催日時：令和元年７月２２日（月）１０：００～

開催場所：独立行政法人中小企業基盤整備機構本部　２階　２A 会議室

※　参加人数の確認のため、説明会に参加する者は下記連絡先までメールにて社名、担当者名、担当者連絡先および参加人数を記載し、７月１９日（金）１０：００までに送信のうえ、必ず電話にて連絡することとする。連絡のない者の参加は認めない。

※　参加人数多数の場合は、１社あたりの人数を制限する場合がある。

（連絡先）この件についての問合せは下記宛にメールまたは電話にて行うこと。

〒105-8453　東京都港区虎ノ門 3-5-1 虎ノ門 37 森ﾋﾞﾙ
中小機構 情報システム基盤センター情報システム課　担当：大塚、東條、清水
ＴＥＬ：03-5470-1513
E-mail：ohtsuka-k@smrj.go.jp、tojo-k1966@smrj.go.jp、shimizu-n@smrj.go.jp

以上