1-1.ウイルスメール攻撃対応訓練の改善について

令和２年12月1日

商工会議所会員等、ユーザ協会非会員の更なる利用促進に向けて改善をかけることとする。

1.改善のポイント

(1)「セキュリティセミナー(録画)＋ウイルスメール攻撃対応訓練」のセット開催
　⇒ **なんのために訓練が必要か理解できる、情報セキュリティについて動画で学習ができる**
(2)訓練に関わる稼働削減の仕組み、各種ツールの提供(商工会議所向け、支部向け)
　⇒ **訓練参加企業の社員、セキュリティ責任部門等の理解促進が図れる、稼働削減ができる**
　⇒ **商工会議所、支部の負担軽減ができる**

2.セミナー内容について

(1)常時録画コンテンツセミナー(約20分)を開催
　※一般社員、経営者向け(notセキュリティ責任者向け)
(2)四半期にzoomでライブセミナー(約60分)を開催
　①専門家を講師とした最新動向も織り交ぜたセミナー　※クラウドソリューション部の粕淵講師等を予定
　②参加枠overの方はYouTubeライブで視聴
(3)将来的には、5分～30分程度のやや専門的なミニセミナーを提供する
　①ウイルスメールの見破り方、テレワークにおけるセキュリティ　等
　②専門家によるセキュリティ責任者向けセミナー

3.提供予定時期

2020年12月中旬以降

4. 費用

今年度は近畿負担済(来年度以降MAツールの利用料120万円/年が発生)　※ウイルスメール攻撃対応訓練費用含む

【追加検討事項】･･･当面は見送り、月毎にメール文を変更し対応

送信するメールを2～3分岐する･･･提供時期は少し先でも可。
　①怪しいメールと気づかせるメール(普通は開封しない)　⇒　メールを見破る力をつける
　②怪しいメールと気づきにくいメール(開封する可能性がある))　⇒　トラブル発生時の対応力をつける

＜課題＞

　①フォーム上で新たなカスタムフィールドを設定し選択肢を設ける必要がある
　②名簿作成ツール変更の必要がある
　③提供時期によっては、シナリオキャンパスを停止し、補正シナリオ対応等が必要。

1-2.ウイルスメール攻撃対応訓練の改善について

本施策を通して、非会員情報を収集し会員拡大を目指す。

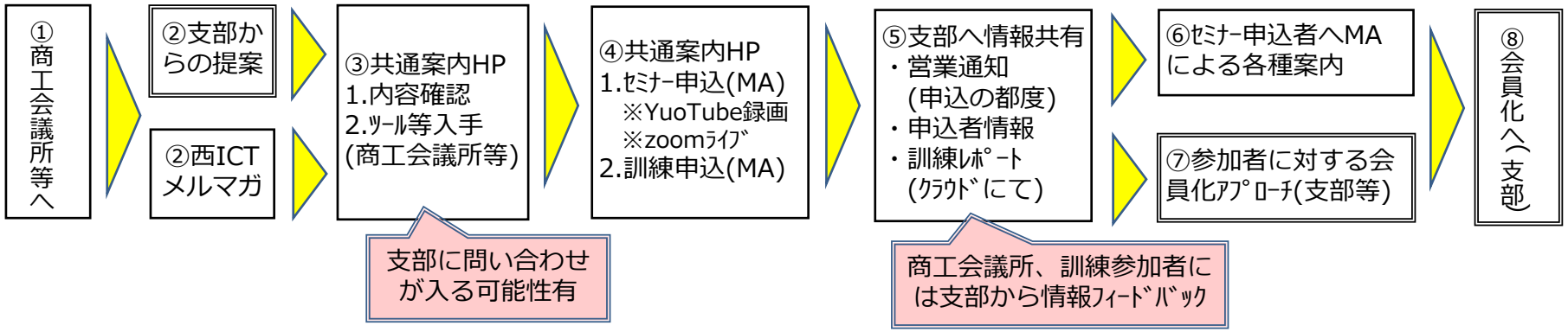
3.運用方法

(1)支部負担を考慮し、全支部共通案内サイトを利用し運用する(支部サイトには本部訓練等の混乱を回避するため記載しない)。
(2)商工会議所への提案等に活用する「施策紹介資料」、「共催施策案内チラシ」、「HP記載例」を別途用意する。
(3)西ICTとして実施する商工会議所職員向けメルマガでも定期的に案内する。
(4)参加者情報、訓練レポートのフィードバックは支部から商工会議所等に実施する。

4.全国共通案内サイト記載内容(案) 「★」は新規作成物

(1)セミナー申込URL
※四半期毎開催するライブセミナーのURLは定期的にメンテするor過去のURLを利用？
(2)訓練申込URL
(3)訓練参加者向け事前案内メール例★
①定期的に訓練を行います。
②不信なメール受信時の対応ルール
(3)セキュリティ責任者向け簡易マニュアル★
①定期的開催の意義、実施方法について
②訓練参加者へのヒアリング、測定内容。
③運用上の注意事項(訓練の1週間後等に訓練参加者に訓練であった旨のメールを組織としても送信する　等)

5.全体の流れ ※□は支部等実施事項



1-3.ウイルスメール攻撃対応訓練の改善（準備事項）

1.セミナー資料
ウイルスメール攻撃対応訓練のパートの修正・・・現在作成中のセキュリティ勉強会資料にて修正済

2.支部・商工会議所提供資料・・・過去の資料を探して修正、支部が商工会議所に連携提案する資料は映像化する？
(1)訓練の流れ、必要性がわかるppt資料　作成済
(2)商工会議所の役割がわかるppt資料　作成済
(3)商工会議所等がHPに記載する文例　作成済
(4)訓練メール文例　**未修整（MAから抽出、責任者向け、訓練参加者向けの2つ作成（word））**

3.訓練参加企業提供資料（PDF化）・・・新規作成
(1)経営者・セキュリティ責任者向け　作成済
　①上記「2-(1)」
　②事前に社員に案内すべき内容を記載したppt資料
　　例　定期的訓練します、怪しいと思った時・メールを開いた時の対応について　　作成済
(2)訓練参加者向け
　上記「3－(1)②」

4.MAツール関係
(1)申込受付フォーム
　①セミナー受講**・・・新規作成要**（専用フォーム、カスタムフィールドは新たに設定しない）
　②訓練体験・・・既存のフォームを利用
(2)メール文
　セミナー受講申込受付・自動返信メール（注意事項、参加用URLも記載する）**・・・新規作成要**

5.HP関係
(1)訓練&セミナー申込ページ**・・・新規作成要**
　（訓練概要、注意事項等記載、申込用のフォームのURLを記載する、申し込むとセミナー参加URLを配信する）
(2)HP掲載コンテンツ
　上記「3」で作成した資料を掲載する
　レポートに「開封時間」、「適切な動作」、「備考欄」を追加する

6.セミナー(資料)
資料作成後、YouTube（限定公開）で録画・提供

【商工会議所・連携団体のみなさまへ】本施策における実施事項

商工会議所様、各団体様における実施事項は以下のとおりです。少ない稼働で会員様、地域のセキュリティ意識の向上を図ることができます。

1.なぜ会員、地域に対するセミナー・訓練が必要か
（1）Microsoft社のWindows7、office2010のサポート切れに伴う情報セキュリティ事故の拡大が予想される
（2）テレワークの拡大により情報セキュリティに関する社員の意識が希薄になっている

2.今回の施策のポイント
（1）ほとんど手間をかけずに会員等のセキュリティに関する意識向上を図ることができる
（2）ユーザ協会HPにて最新のメニューを定期的に更新します。
（3）常時受け付けているのでHP記載情報の修正が不要（修正が発生した場合、支部経由でご案内します）

3.商工会議所様に実施いただく事項
(1)会員等へのご案内
①商工会議所様HPでの案内
②商工会議所様HPのバナー等での案内・・・更新する稼働がかからない
③メルマガ等での案内
(2)参加者からの一次問合せ対応
セミナー。訓練の詳細はユーザ協会各支部（もしくは地域事業推進部）からご説明致します。
(3)訓練参加企業リスト受領
訓練に参加した企業名等ユーザ協会からフィードバックします。
※申込時に所属商工会議所名等の記載のない方はフィードバックできません。

4.参加条件
誰でも可、ただし1事業所1回限り。

5.参加費
無料

6.提供時期
24時間・365日
※サービスのメンテナンス等で受付を停止することもあります。

原則、ユーザ協会から参加企業に郵送等しますが、商工会議所様からフィードバックいただくことも可能です。

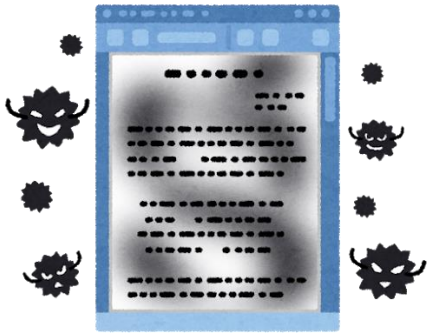
★HPに記載等PR → ★問合せ対応（一次） → 申込受付・名簿作成 → セミナーの開催 → メール訓練実施 → 学習コンテンツの提供 → 訓練レポートの作成 → 訓練レポートのフィードバック

※「★」は商工会議所様等必須実施事項。

【ご提案】セミナー・訓練参加希望の経営者のみなさまへ

ユーザ協会が主催する情報セキュリティセミナーのポイントは以下のとおりです。セミナー。メール訓練の組み合わせで社員の皆さんの情報セキュリティに対する意識づけができます。

1.サンドイッチ形式のセキュリティ学習
①セミナーによる学習　＋　②メール訓練　＋　③学習コンテンツによる再確認



2.訓練のポイント
(1)訓練前にセミナーを受講することで情報セキュリティ対策の動機づけができる
　※セミナーは何回でも無料で受講可能です。
(2)事前体験ができる
「ウイルスメール訓練ワンショット体験」をすることで、
　①訓練のイメージを事前に確認いただけます。
　②訓練が有効か事前に把握できる
　※セキュリティ機器の設定がある程度把握できます（セキュリティ機器がメールをブロックしているか　等）
(3)セキュリティ対応力の測定ができる
　メール送信時間、開封時間等が把握できるので
(4)訓練実施から訓練結果のフィードバックが早い
　最短約2週間でフィードバック可能。訓練の間隔がある内に訓練参加者への動機づけが可能です。
(5)社内動機づけのための資料も提供しています
　社員、情報セキュリティ責任部門の方等に訓練の必要性、訓練のポイント等説明するための資料もご提供します。

3.申込方法
ユーザ協会の専用のサイトから申込みください。

【注意事項】
1.メール訓練は1事業所1回限りのご利用とさせていただきます。
　※毎年利用したい方はユーザ協会入会、訓練サービス事業者の利用等検討願います。
2.メール訓練は最大10名までの参加とさせていただきます。
3.ご入力いただいた情報はユーザ協会、共催組織、講師等セミナー協力組織からの各種連絡、情報提供に使うことがあります。これらについては申込者ご本人に同意いただいたものとして取り扱わせていただきます。
4.セキュリティ機器、パソコン、ソフトウェアの設定によっては、メール開封情報が正しく取得できない場合があります。

【ご提案】情報セキュリティ責任者、経営者のみなさまへ

ユーザ協会が主催する情報セキュリティセミナーのポイントは以下のとおりです。セミナー。メール訓練の組み合わせで社員の皆さんの情報セキュリティに対する意識づけができます。また、以下に記載の事前の準備をしていただくことで更に効果をあげることができます。

1.サンドイッチ形式のセキュリティ学習
①セミナーによる学習　＋　②メール訓練　＋　③学習コンテンツによる再確認

2.訓練のポイント
「セミナー・訓練参加希望の経営者のみなさんへ」に記載のとおり

3.訓練にあたっての準備事項（お薦め）
（1）自社の情報セキュリティルールの明確化＆社内掲示板等への記載
　⇒　不審なメールを受信した時の対応ルールの明確化
（2）「ワンショット体験」によるセキュリティ環境の確認、必要に応じて臨時のセキュリティ機器の環境設定を実施する
　⇒　メール開封確認等測定できるようにする。
（3）訓練の目的・訓練における測定事項の整理
　⇒　訓練の目的　「怪しいメールは開封しないための訓練」、「怪しいメールを受信した場合の対応力を養う訓練」
　⇒　測定事項　「メール開封の有無」、「メール開封から報告までに要した時間」
（4）測定事項を管理するためのチェックシート
　⇒　ユーザ協会の訓練レポートをご参考ください
（5）訓練体験者部門の上長との意識あわせ
　⇒　訓練をする予定であること
（6）訓練結果レポートに基づく社員指導、社内研修の追加実施

訓練の１週間後に訓練体験者宛に訓練を実施した旨を案内するメールを送付することをお薦めします。

★セミナー・研修に関する注意事項等確認 → ★セミナー申込 → ★セミナー参加ＵＲＬの社内周知 → セミナー受講 → ★★メール訓練準備 → ★メール訓練申込 → メール訓練体験 → 学習コンテンツ → 訓練結果レポート受領 → ★社員指導・社内研修

※実践囲みは必須事項、「★」は情報セキュリティ責任者に実施いただくことをお薦めする事項

【ご案内】セキュリティセミナー、メール訓練に参加される方へ

情報セキュリティトラブルの原因は「人的要因」によることがほとんどです。
定期的に研修、訓練を受けることで上記トラブルを削減するとともに、トラブル発生時の対応力を上げることで万が一の被害拡大を防ぐことができます。是非積極的に参加願います。

1.今回のセミナー・訓練の目的
(1)セミナー(指定した期間内に受講願います) ⇒ **情報セキュリティの基本を理解する！**
(2)訓練(随時・対象者未定) ⇒ **怪しいメールを受信した時の対応力の向上！**

2.今回のセミナー＋訓練について
サンドイッチ形式のセキュリティ学習
①セミナーによる学習 ＋ ②メール訓練 ＋ ③学習コンテンツによる再確認

3.今回のセミナー・訓練の概要
(1)セミナーによる学習(約20分)
①24時間視聴可能なセミナーです。
②情報セキュリティの必要性、標的型攻撃メールの被害・対策等理解してください。
(2)メール訓練に参加(実施時期・対象者は未定)
①必要により社内ルールに沿った対応をしてください。
(3)学習コンテンツによるフォロー学習(訓練参加者が対象)
(4)訓練結果レポートによる社内研修等の実施(各社によって対応は異なります)
※研修等は社内で実施願います。

★社内情報セキュリティルール等確認 → ★セミナー受講 → メール訓練準備 → メール訓練申込 → ★メール訓練体験 → ★学習コンテンツ → 訓練結果レポート → ★社員指導・社内研修

※実践囲みは必須項目。「★」は参加者に実施いただく事項

【ご案内】怪しいメールを受け取った時の対応について

怪しいメールを受け取った場合にとるべき一般的な行動は以下のとおりです。会社によって対応すべきルールが異なりますので事前にご確認願います。

1.社内ルールの理解
心当たりのないメール等、怪しいメールは安易に開封しないよう常日頃から意識しましょう。

2.怪しいメールの見極め方の理解
(1)セキュリティソフトが「警告」を発した場合
(2)その他セキュリティ責任者から提供される資料等で事前に理解願います(次ページに参考例を記載します)。

3.怪しいメールへの対応
(1)未開封
怪しいメールを「受信」した旨を上長、セキュリティ責任者等に共有する
⇒ 社内の他の人の感染を回避するため開封しなくても情報共有を早期にすることは重要です。
(2)開封した場合
①自分の端末を社内ネットワークから切り離す
LANケーブルを抜く
Wi-Fiからログアウトするor Wi-Fiルーターの電源を落とす
②怪しいメールを「開封」した旨を上長、セキュリティ責任者等に共有する
③メールに記載のURLをクリックした場合、添付ファイルを開いた場合はその旨、その時のパソコンの状況等も共有する
④上長・セキュリティ責任者の指示に従う
＜NG事項＞
指示があるまでパソコンの初期化はしないこと。原因の究明、適切な対処ができなくなります。

★社内ルールの理解 → ★セミナー等による学習 → 怪しいメールを受信 → ★適切な対応 → ★上長等への報告 → ★セキュリティ責任者からの指示

【ご案内】怪しいメールの見極め方

怪しいメールの見極め方は以下のとおりです。非常に巧妙なメールもあり怪しいなと感じたら送信元に送信の有無を電話で確認することをお薦めします（「なりすまし」メールの場合もありメール確認は危険です）。

1.怪しいと疑うべきメール

（1）ヘッダー・宛先等

①身に覚えのない内容
「〇〇を購入いただいた方への特典です」
②知らない企業・人からのメール
「1円で最新のスマートフォンが入手できます」・・・私の妻が引っ掛かりそうになりました。
③無料で発行されるメールアカウント（gmail　等）からのメール

（2）タイトル・本文

①宛先、差出人名が記載されていない
②文字化け（日本語ではない文字を含む）・漢字の誤変換が多い
③日本語の表現に違和感がある
④連絡先（TEL、mail）が記載されていない

（3）添付ファイル・URL

①添付ファイルの形式が実行ファイル（exe．等）
②わざわざ「添付ファイルを確認してください」、「URLからアクセス願います」という行動を求める

2.システムが警告した怪しいメール

ウイルス対策ソフト、メーラー、Windows等感染リスクのあるマクロを含んだ添付ファイルが届いた場合等、アラームメッセージを出すものがあります。
その場合は、セキュリティ責任者に対応方法を確認することをお薦めします。

3.怪しいと思ったメールへの対応

怪しいと思いつつも、業務に関係しそうなメールであれば送信者に電話で送信の有無を確認することをお薦めします。

【注意事項】

1つのメールアドレスを複数名で利用する場合は、特に注意が必要です。
誰か1人が感染してしまえば・・・
また、メールの確認漏れ・対応漏れという観点からもメールアドレスは1人1人が持つことをお薦めします。