



自社内製での標的型メール訓練実施を実現する 標的型攻撃メール対応訓練実施キットのご案内

御社でも業者に頼らずに標的型メール訓練が実施できます！



1

標的型攻撃メール対応訓練実施キットとは？

標的型攻撃メール対応訓練実施キットは、自社内製での標的型メール訓練実施を実現する、訓練実施担当者のためのDIY（Do it yourself）ツールセットです。

訓練用の標的型メールを作成・送信するためのツールや、従業員教育用のコンテンツ等、自社内製で標的型メール訓練を実施する際に必要となるものが揃っていますので、業者に標的型メール訓練の実施を委託した場合と同等、または、それ以上のレベルの訓練を、業者に委託した場合よりも低コストで実現することができます。

訓練実施にかかるコストを大幅に削減できるというメリットが評価され、大手企業様を中心に、既に様々な企業様にご利用を頂いております。

キットでは無料の評価版をご提供しています



キットの詳細案内

ask@kunrenkit.jp でもお問合せをお受けしております。

標的型メール訓練と言えば、標的型攻撃メール対応訓練実施キット

ask@kunrenkit.jp

標的型メール訓練をするなら、標的型攻撃メール対応訓練実施キットがお役に立ちます。訓練実施に際して、何でもお問い合わせ下さい。

キットのご購入に関するご案内はこちら

Top | キットの詳細 | 商品ラインナップ | お問い合わせフォーム | キットを無料でお試し | 訓練実施の教科書 | コラム | サイトマップ

標的型メール訓練は内製で実施できるということ、知っていますか？

実際に現場で訓練を実施している「中の人」が、コストも手間もかけずに標的型攻撃メール訓練を実施できないだろうか？そう考えて作ったもの、それが、

標的型攻撃メール 対応訓練実施キット

なんです。

コストパフォーマンスの良い標的型攻撃メール訓練をご検討なら、是非キットを検討候補にお加えください。

【標的型メール訓練は自社内製での実施が正解】 本当に成果の上がる訓練は自らの手で実施することから

紹介動画

コンセプト

キットの特徴

キットの構成

他社訓練サービスとの違い

標的型メール訓練やらないや！でも、予算とクオリティの両立に悩んだら・・・そんなあなたに、お奨めの解決方法をお教えします！



標的型メール訓練やらないや！でも、予算とクオリティの両立に悩んだら・・・そんなあなたに、お奨めの解決方法をお教えします！

標的型メール訓練を実施するよう、会社から指示された。それも、なる早で。

しかし、今期の予算は限られているし、予算の追加も期待薄。費用はかけずに、しかし、クオリティは下げずに。そんな理想を叶えるサービスはありませんか？

はい。そんなあなたの理想を叶えるのが「標的型攻撃メール対応訓練実施キット」です！

「標的型攻撃メール対応訓練実施キット」は、プロの訓練実施代行業者にも活用頂いている、標的型メール訓練実施のためのツールセット。まずは動画をご覧ください。

WebサイトURL : <https://kit.happyexcelproject.com/> または <https://kunrenkit.jp>

2 標的型攻撃メール対応訓練実施キットの特徴

1. 自社内製で標的型メール訓練を実施するために必要な物が揃っており、**外注不要**で訓練を実施することができます。
2. 訓練実施にまつわる作業を省力化することに特化したツールが揃っており、**手間がかからず**に訓練を実施することができます。
3. 標的型メールの様々な手口を再現することができるので、工夫次第で**色々なパターン**の訓練を実施することができます。
4. 手持ちのパソコンを使って訓練が実施できるので、訓練実施のために**新たな機材の購入は不要**で、**すぐに**訓練が実施できます。
5. 訓練メール本文の文例が**100種類**（日本語版81種、英語版19種）付属していますので、文例を参考に訓練の内容を考えることができます。
6. キットのサポートの一環として、様々な組織の標的型メール訓練実施に立ち会った経験を持つ**専門家のアドバイス**を受けられます。

3

標的型攻撃メール対応訓練実施キットがご提供するもの

標的型攻撃メール対応訓練実施キットには、自社内製での訓練を実施するために必要となる、以下のもの、及びサービスを、キット一式としてご提供します。

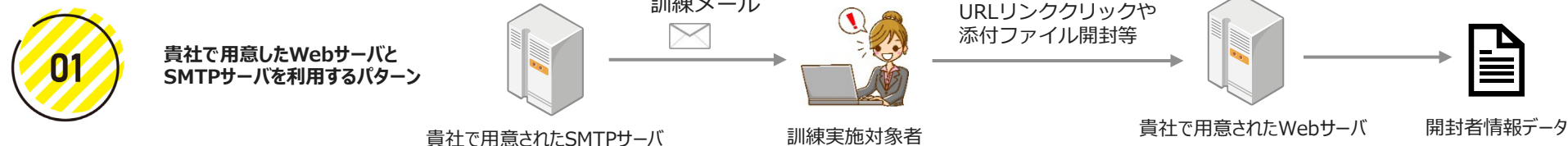
1. 標的型メール訓練を実施するための訓練メール一括送信ツール
2. 訓練メールに添付する様々な模擬マルウェアファイルを作成するためのツール
3. 訓練用のメール本文の文例（テンプレート）
4. 訓練の実施手引書と、訓練実施計画書の雛形
5. 編集が可能な、訓練対象者向けの教育用コンテンツ
6. 誰が模擬のマルウェアファイルを開封したかを集計するためのツール
7. フィッシング詐欺対応訓練にも対応した、Webサーバに設置するためのプログラムとWebコンテンツデータ
8. 訓練メールを送信するサービス及び、開封者情報を集計するWebサービス
9. 訓練実施後のアンケート実施を可能にするアンケートページサービス
10. 理解度確認テストを含むトレーニングコンテンツの提供

既に出来上がっているものを基に、自社で自由にカスタマイズして訓練を実施する事ができますので、初めて訓練を実施されるような組織であっても、業者に委託するのと全く遜色のない、もしくは、それ以上の訓練を、自社内製で実施することができます。

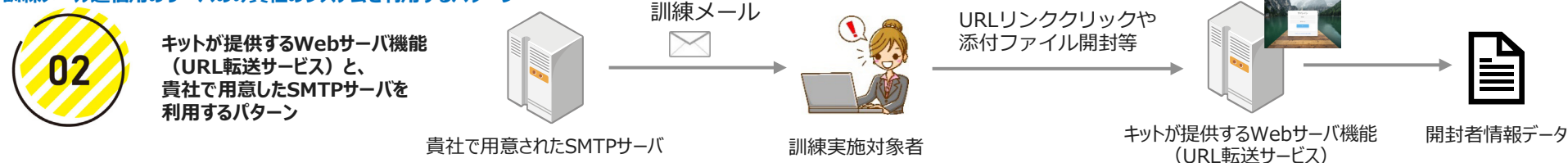
4 キットを活用した標的型メール訓練の実施構成

キットでは、キットが提供するサーバを用いて自社ではサーバを用意することなしに訓練を実施する、また、貴社で用意されたサーバを用いて貴社内に閉じた形で訓練を実施いただくなど、貴社の要望に応じた形で訓練を実施いただけます。自社では設備を持ち合わせていない企業様はもちろん、自社で持っている設備を活用したい、また、メールアドレスなどの情報を業者に開示することなく訓練を実施したいといった様々なニーズにお応えすることができます。

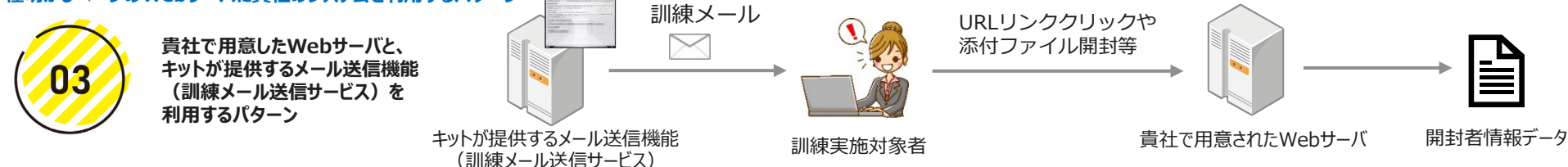
貴社ネットワーク内に完全に閉じた形で実施するパターン



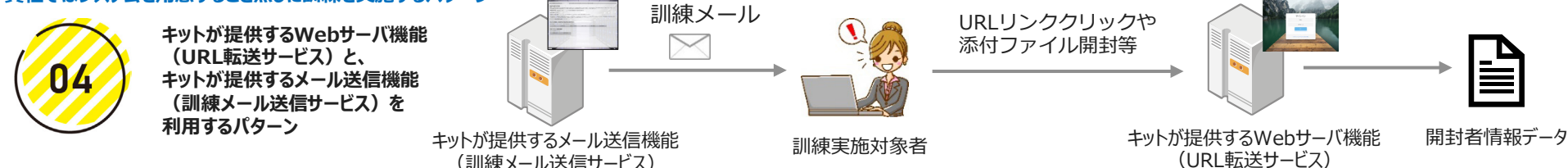
訓練メール送信用のサーバのみ貴社のシステムを利用するパターン



種明かしページのWebサーバに貴社のシステムを利用するパターン



貴社ではシステムを用意すること無しに訓練を実施するパターン



5

訓練メールの作成・送信と、誰が訓練メール本文中のURLリンクをクリックしたか（又は添付ファイルを開いたか）？の集計は、キットに付属のツールを用いて手軽に行うことができます。

6 キットで作成できる模擬マルウェアファイル

キットでは訓練メールに添付する模擬のマルウェアファイルとして、様々な添付ファイルを作成することができます。予め用意されたテンプレートを選択して模擬マルウェアファイルを作成する事ができるだけでなく、担当者様側でご用意頂いたファイル（普段の業務で使用しているドキュメントや、自作のマクロを使ったファイルなど）を用いて添付ファイルを作成することも可能です。

訓練メール作成支援作成ツールで作成できるファイルの例

標的型攻撃メール対応訓練実施キット 訓練メール作成支援ツール 評価版 Ver.2021.11.02.01

このツールは、標的型メール訓練で使用する訓練メールの作成を支援するツールです。本ツールを使用することにより、訓練メールをeml形式ファイルで出力する、また、訓練メール送信サービスにアップロードするZipファイルを作成することができます。

訓練メールの生成と同時に添付ファイルを作成する場合は、本タブの設定を行うと共に、訓練メール本文の編集において、添付ファイル有無に「有り」を選択してください。なお、既に作成済みのファイルを訓練メールに添付する場合は、送信先リストデータの添付ファイル欄に、添付するファイルのパスを記載してください。

☐ 生成したファイルをZipファイルにする → Zipファイルのパスワード

生成する添付ファイルの種類

- ☒ Wordファイル パターン4-A:Emotet-日本語版 ☐ 拡張子を.docにする
- ☐ Excelファイル パターン1-A:白紙(.xlsx版) ☐ 拡張子を.xlsにする
- ☐ その他 HTMLファイル(ログインページ)(.html)

添付ファイルの出力先フォルダ ☐ 出力先にあるファイルを削除した上でファイルを生成する

添付ファイル生成の元とするファイルのパス

生成するファイル名(拡張子より前の部分を指定して下さい)
例:総務からのお知らせ

生成するファイルに埋め込むリンク

- ☐ URLリンク1 ☐ URLリンク5
- ☐ URLリンク2 ☐ URLリンク6
- ☐ URLリンク3 ☐ URLリンク7
- ☐ URLリンク4 ☐ URLリンク8

添付ファイル生成の対象とする本文パターン

- ☐ 本文パターン1 ☐ 本文パターン5
- ☐ 本文パターン2 ☐ 本文パターン6
- ☐ 本文パターン3 ☐ 本文パターン7
- ☐ 本文パターン4

プレビュー

これは標的型攻撃メールの訓練です！

あなたが今行った行為（メールに添付されているファイルを宛先に開いてしまうという行為）は、あなたが持っているパソコンや、コンピュータウイルスに感染させてしまうかもしれない危険な行為です。これは訓練ですので何もありませんが、もし、これが訓練でなかった場合は、深刻な問題が発生する可能性が十分あることを、この機会に知って下さい。

標的型攻撃メールの怖さを知っていますか？

標的型攻撃メールは、特定の企業を狙って、顧客情報や重要な技術情報などを盗み取る、社内システムに侵入して業務を麻痺させるようにしてしまおうと、会社に重大な被害をもたらすものです。

あなたが今開いたこのファイルが添付されていたメールは、この「標的型攻撃メール」による攻撃の手口の一例を使った訓練用のメールです。

これは訓練なので本物ではありませんが、もしこれが本当の標的型攻撃メールであった場合は、あなたのパソコンやコンピュータウイルスに感染し、社内に重大な被害をもたらすきっかけになっていってしまうかもしれません。

標的型攻撃のターゲットになるのは、なにも政府や軍事関連の組織ばかりではありません。当社もその標的とされる可能性は十分あります。

あなたの元に、いつ、本物の標的型攻撃メールが送られてきても不思議ではありません。今回の訓練をきっかけに、標的型攻撃メールについて理解し、うっかり被害に遭ってしまわないように、受け取ったメールが標的型攻撃メールでないかどうか、常に注意を怠らないようにして下さい。

【注意しましょう！】

会社に被害をもたらすことを目的としたコンピュータウイルスが添付された、悪意を持ったメール（標的型攻撃メール）が、いつ届くかは知られてきても不思議ではありません。

次ページ以降に記載されている「気づきポイント」をよく読んで、標的型攻撃メールにうっかり引っかかってしまわないように、くれぐれも注意して下さい。

標的型攻撃メールのパターン

「標的型攻撃メール」には主に以下の3つのパターンがあります。

- ① 悪意のあるプログラム（コンピュータウイルス）をメールに添付し、メールの受信時に添付ファイルを開くように誘導するもの。
- ② 悪意のあるプログラムを実行する仕組みに、Webブラウザなどの脆弱性を利用し、悪意のあるプログラムに感染させるためのWebサイトに誘導しようとするもの。
- ③ 有名なソフトウェアの名前を振り、セキュリティ対策のためのアップデートなどを装って、見かけ上、有名なソフトウェアに付け加えた悪意のあるプログラムをインストールさせようとするもの。

悪意のあるプログラムを実行し込ませようとする手口は異なりますが、メールの受信者に対して、悪意のあるプログラムを実行し込ませようとする手口をやらせようとする点においては、いずれも同じです。

このための手口として用いられる方法は主に以下の2つ、また、これらの方法を巧みに組み合わせるものがあります。

- ④ 怪しい人物から送られたものではないと信じ込ませる。
- ⑤ 添付ファイルを開きたい、又、Webサイトにアクセスしたいと誘われる。

前者は、怪しい人物や偽装者、顧客など、メールを送られてくることが自然と信じられないような相手を使い、文面も自然な内容を使う形が多く見られます。

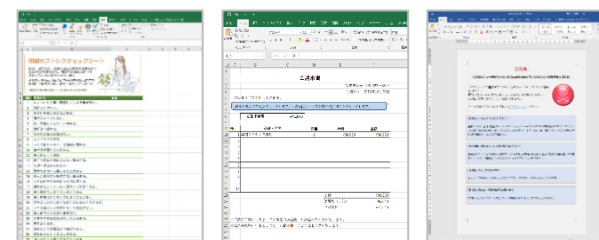
代理を装って記事を送付するような形式や、システム管理者を装って特定のWebサイトに誘導するような形式はこのパターンと言えます。

そして後者は、人の心理の隙をついて、そうしなくてはならないような形式です。例えば、「http://xxx.xxx <怪しい品名>について危険が予測されていますが、開かれている事は本番でしようか?」などといったメールが届いたらどうでしょうか?

「怪しいかも?」という思いがよぎったとしても、「自社製品に対する批判だ」と受け取れたら、つい、アクセスしてしまうのではないのでしょうか?

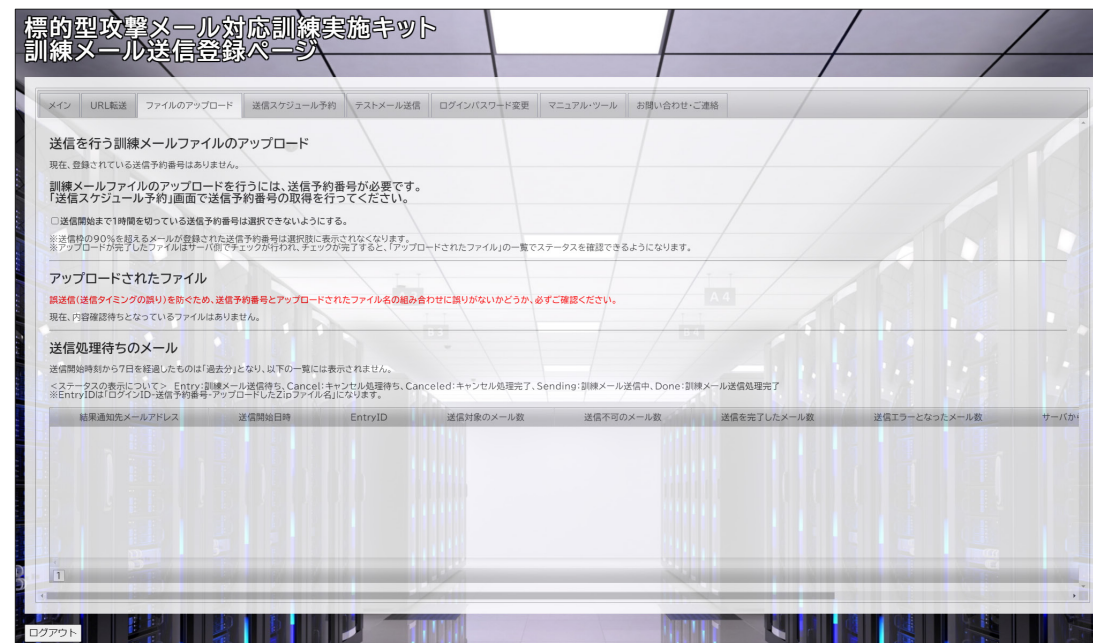
このように、心理の隙を突くなどの方法は「ソーシャルエンジニアリング」と呼ばれ、その内容は非常に多岐にわたります。攻撃の手法も日々進化しています。

あの手口の手でメールの読み手を騙し、結局に被害を被るのか?これが攻撃者の最も心算なのです。あなたは、どのような攻撃者の心理をかわすことができるのでしょうか?



7 スケジュール送信可能な訓練メール送信サービス

キットが提供する「訓練メール送信サービス」では、訓練メール送信日時を指定して訓練メールを送信することができますので、訓練メール送信時にパソコンの前に張り付いて作業を行う必要はありません。訓練メールを送信するために、わざわざ休日や早朝に出社するといったことなしに、訓練を実施することができます。



「訓練メール送信サービス」では、

- SPF (Sender Policy Framework)
- DKIM (Domain Keys Identified Mail)
- DMARC (Domain-based Message Authentication Reporting and Conformance)

に対応した、訓練メール送信用のメールアドレスをご提供しています。また、訓練メールの送信間隔を指定してメールを送信することもできますので、メールを受信するサーバ側にて同一のメールサーバからのメール受信数に制限が設定されている場合でも、制限を超えない範囲で訓練メールを送信することができます。

8

訓練実施後に行うアンケートページサービス

後述する「スタンダード版」及び「グループ企業用」ライセンスをご契約の場合は、任意の設問でのアンケート実施を可能とするアンケートページサービスをご利用いただけます。

アンケートへのご協力をお願いします

本ページは、○月×日に実施した標的型攻撃メール訓練について、アンケートへのご協力をお願いしますものです。
以下の設問への回答についてご協力をお願いいたします。

設問1 訓練メールが届いた際、不審なメールが届いたことを上長等に報告されましたか？

☐ 報告した
☐ 報告していない

設問2 訓練メール内に記載されたURLをクリックしましたか？

☐ クリックした
☐ クリックしていない

設問3 今回の訓練メールについて、不審なメールであるとすぐにわかりましたか？

☐ 全くわからなかった
☐ 不審かも？とは思ったがわからなかった
☐ すぐにはわからなかったが、よく見たら不審だと気づいた
☐ すぐに不審なメールだとわかった
☐ 事前に不審なメールだと聞いていた

設問4 今回の訓練に関してお気づきの点などありましたら、コメントをお願いします。

回答する

アンケートページのデザインや
設問の内容はオリジナルのものが
お使いいただけます。

開封者情報集計ツール スタンダード版 Ver.2024.03.20.01

本ツールは、標的型攻撃メール対応訓練実施キットを用いて実施した標的型メール訓練で得られた開封者情報のデータを集計するためのツールです。
キットが提供する「URL転送サービス」を利用して開封者情報を取得している場合は、アクセス元のIPアドレスに関する情報も出力されます。

メイン 開封者情報データ アンケートデータ マスタデータ アクセス元IPアドレスの一覧 除外IPアドレス

アンケート回答データのパス F:\Testデータ\Enq-Apt\KIT-4c35246863ac20d0cb55838e.zip

アンケートデータのインポート アンケートデータのエクスポート

登録日時	転送URL	突合キー情報	アクセス元IPアドレス	UserAgent情報	q1	q2	ans3	q3	ans4
2024/03/17 22:54:43	4c35246863ac20d0cb55838e	EnMark.005		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36	報告した	クリックしていない	訓練担当者にお気...		
2024/03/17 22:55:06	4c35246863ac20d0cb55838e	EnMark.005		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36	報告していない	クリックした	これはテストです。		
2024/04/03 18:11:25	4c35246863ac20d0cb55838e	Enmark.001		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36	報告した	クリックしていない		不審かも？とは思	台湾の台北

アンケートページサービスで収集した回答データは、訓練メール送信サービスのWeb画面からダウンロードを行うことができます。

このデータをキットに付属の「開封者情報集計ツール」に取り込んでいただくことで、回答データとマスタ情報を突合し、XMLデータとしてエクスポートすることができます。

AnswerData.xml

開封者情報集計ツール スタンダード版 Ver.2024.03.20.01

このデータをキットに付属の「開封者情報集計ツール」に取り込んでいただくことで、回答データとマスタ情報を突合し、XMLデータとしてエクスポートすることができます。

登録日時	転送URL	突合キー情報	アクセス元IPアドレス	UserAgent情報	q1	q2	ans3	q3	ans4
2024/03/17 22:54	4c35246863ac20d0cb55838e	EnMark.005	103.x.x.212	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36	報告した	クリックしていない	訓練担当者にお気...		
2024/03/17 22:55	4c35246863ac20d0cb55838e	EnMark.005	103.x.x.212	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36	報告していない	クリックした	これはテストです。		
2024/04/03 18:11	4c35246863ac20d0cb55838e	Enmark.001	103.x.x.212	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36	報告した	クリックしていない		不審かも？とは思	台湾の台北

XMLデータとしてエクスポートされたデータはExcelに読み込むことで、集計やグラフを作成するなどのとりまとめ作業を行っていただけます。

訓練メールに記載されていたURLリンクを何故クリックしたのか？など、訓練メールを受信した際に取った行動について尋ねるアンケートを実施したい場合は、Microsoft Formsなど、無料で利用できるアンケートASPサービスを利用する方法もありますが、この場合、アンケートの回答者と訓練メールを開いた人（URLリンクをクリックしたり、添付ファイルを開いたりした人）を結びつけるには、氏名やメールアドレスなど、個人を特定するための設問をアンケート内に設ける必要があります。

キットが提供するアンケートページサービスを利用すると、特定のキー情報を用いて、訓練メールを開いた人とアンケートの回答者を結びつけることが可能になります。

9

理解度確認テストを含むトレーニングコンテンツの提供

キットでは、理解度確認テストを含むトレーニングコンテンツも提供しています。（2024年6月時点では5種類）
トレーニングコンテンツは毎月1つ以上、順次追加されますので、実施する訓練に合わせてお使いいただくことができます。

※評価版、ベーシック版のライセンスではお使いいただけるトレーニングコンテンツに制限があります。

【トレーニングコンテンツを活用した種明かしページの例】

標的型攻撃メールの怖さを知っていますか？

標的型攻撃メールは、特定の企業を狙って顧客情報や重要な社内情報などを盗み取る、また、社内システムに侵入して業務を継続できないようにしてしまうなど、会社に重大被害をもたらすものです。

あなたが今、開いたメールは、この「**標的型攻撃メール**」による攻撃の手口の一例を模した訓練用のメールです。

今回は訓練なので本物ではありませんが、もし、これが本当の標的型攻撃メールであった場合は、あなたのパソコンがコンピュータウイルスに感染し、社内に莫大な被害をもたらすきっかけとなってしまうかもしれません。標的型攻撃のターゲットになるのは、なにも政府や軍事関連の組織ばかりではありません。当社もその標的とされる可能性は十分あります。「**うちの会社には関係ない話**」ではないのです。

あなたの元に、いつ、本物の標的型攻撃メールが送られてきたとしても不思議ではありません。上記の研修コンテンツを元に、標的型攻撃メールについて知っていただき、うっかり被害に遭ってしまつてはならないよう、常に注意を怠らないようにして下さい。

本訓練についてのお問い合わせ先
〇〇部 標的型メール訓練実施担当
田中 一郎
Tel. 03-1234-5678 メール: tanaka@hoge.co.jp

キットが提供するトレーニングコンテンツ（解説や確認テストなど）

キットの機能を活用したフィッシング詐欺型の訓練のデモページを以下のURLで公開しています。
<https://o365network.com/729b7ed8f51ecf29618e59ea/Demo0001>

貴社で作成されたコンテンツ

これは標的型攻撃メール訓練です！

あなたは、企業を狙った「標的型攻撃メール」というものがあることを知っていますか？
フィッシング詐欺メールやウイルス送付メールなど、いわゆる標的型攻撃メールの類が送られてくるのは、個人や中小企業ばかりではありません。
大企業に狙われることも、国や自治体などにも狙われることがあります。
標的型攻撃メールは、あなたの会社や個人に被害をもたらすだけでなく、あなたの大切な顧客情報や社内情報なども盗み取られる可能性があります。
フィッシング詐欺メールに誘導されたり、ウイルスやマルウェアに感染したり、大切な顧客情報や社内情報などが盗み取られるなど、被害は想像以上に深刻です。
あなたが今、開いたメールは、この「**標的型攻撃メール**」による攻撃の手口の一例を模した訓練用のメールです。
今回は訓練なので本物ではありませんが、もし、これが本当の標的型攻撃メールであった場合は、あなたのパソコンがコンピュータウイルスに感染し、社内に莫大な被害をもたらすきっかけとなってしまうかもしれません。標的型攻撃のターゲットになるのは、なにも政府や軍事関連の組織ばかりではありません。当社もその標的とされる可能性は十分あります。「**うちの会社には関係ない話**」ではないのです。
あなたが今、開いたメールは、この「**標的型攻撃メール**」による攻撃の手口の一例を模した訓練用のメールです。
今回は訓練なので本物ではありませんが、もし、これが本当の標的型攻撃メールであった場合は、あなたのパソコンがコンピュータウイルスに感染し、社内に莫大な被害をもたらすきっかけとなってしまうかもしれません。標的型攻撃のターゲットになるのは、なにも政府や軍事関連の組織ばかりではありません。当社もその標的とされる可能性は十分あります。「**うちの会社には関係ない話**」ではないのです。

今回は訓練ですが、あなたがクリックしたURLやボタンが、もし、犯罪者が仕掛けた本物の罠であつたとしたら？ということを考えてみてください。

あなたの元に、いつ、本物の標的型攻撃メールが送られてきたとしても不思議ではありません。上記の研修コンテンツを元に、標的型攻撃メールについて知っていただき、うっかり被害に遭ってしまつてはならないよう、常に注意を怠らないようにして下さい。

もし、情報セキュリティ事故が発生したら何が起きるか？

日々業務を行う中で、もし、情報セキュリティに関する事故(情報漏洩、業務システムへの不正侵入・乗っ取り、データの改ざん・破壊、不正送金など)が発生したら、どのようなことが起きるか、あなたは想像できますか？

物理的損害 ウィルスによって業務システムやデータが破壊されてしまえば、個人・組織に与える被害は想像以上に深刻です。

金銭的損害 情報漏洩によって発生する賠償、復旧にかかる費用の支出、業務システムが停止してしまうことで発生する売上上の損失などが、多額の金銭的損害が発生します。

信用の失墜 セキュリティ事故が発生してしまうような企業との取引は不安定である。安心してデータを提供しないという状況になり、将来的な信用を失ってしまう可能性があります。

資産の喪失 金銭的、物理的な資産の喪失のみならず、優秀な人材が会社を辞職してしまう、社員の士気が低下してしまう、大事な取引先が離れてしまうなど、様々な資産を失ってしまう可能性があります。

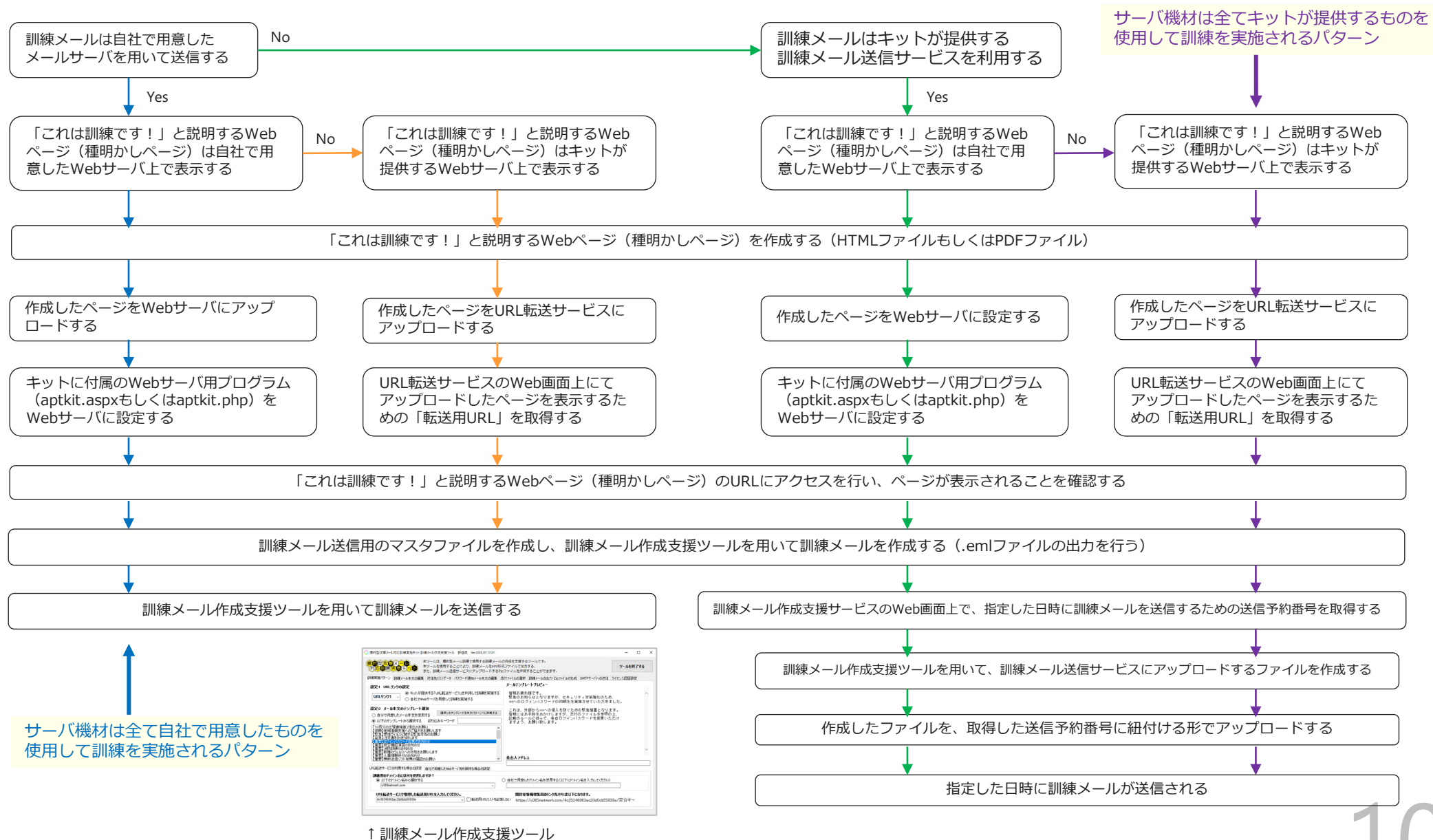
その他の損失 その他にも、場合によっては刑事罰を科せられ、監禁被害が発生する、新しい人材の採用に影響が出てしまうなど、想像し難い被害が発生するものもあります。

フィッシング詐欺とは？

「フィッシング(phishing)詐欺」とは、假り偽物を「fishing」のように、言葉巧みに偽のサイトに誘導して、様々な情報を盗み取ろうとするネット詐欺の手段です。
「fishing」の英文字の「f」を「ph」に変えて「phishing」という綴り、この詐欺の手口を表す用語として使われるようになりました。
「f」を「ph」に変えたのは、手口が巧妙で盗み取られることを「phishing」から「phishing」に変えたという説や、盗み取りを「phishing」から「phishing」に変えたという説など、諸説あります。

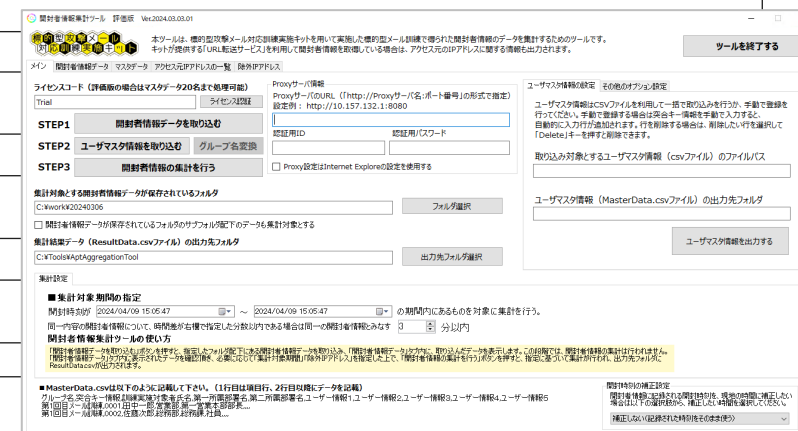
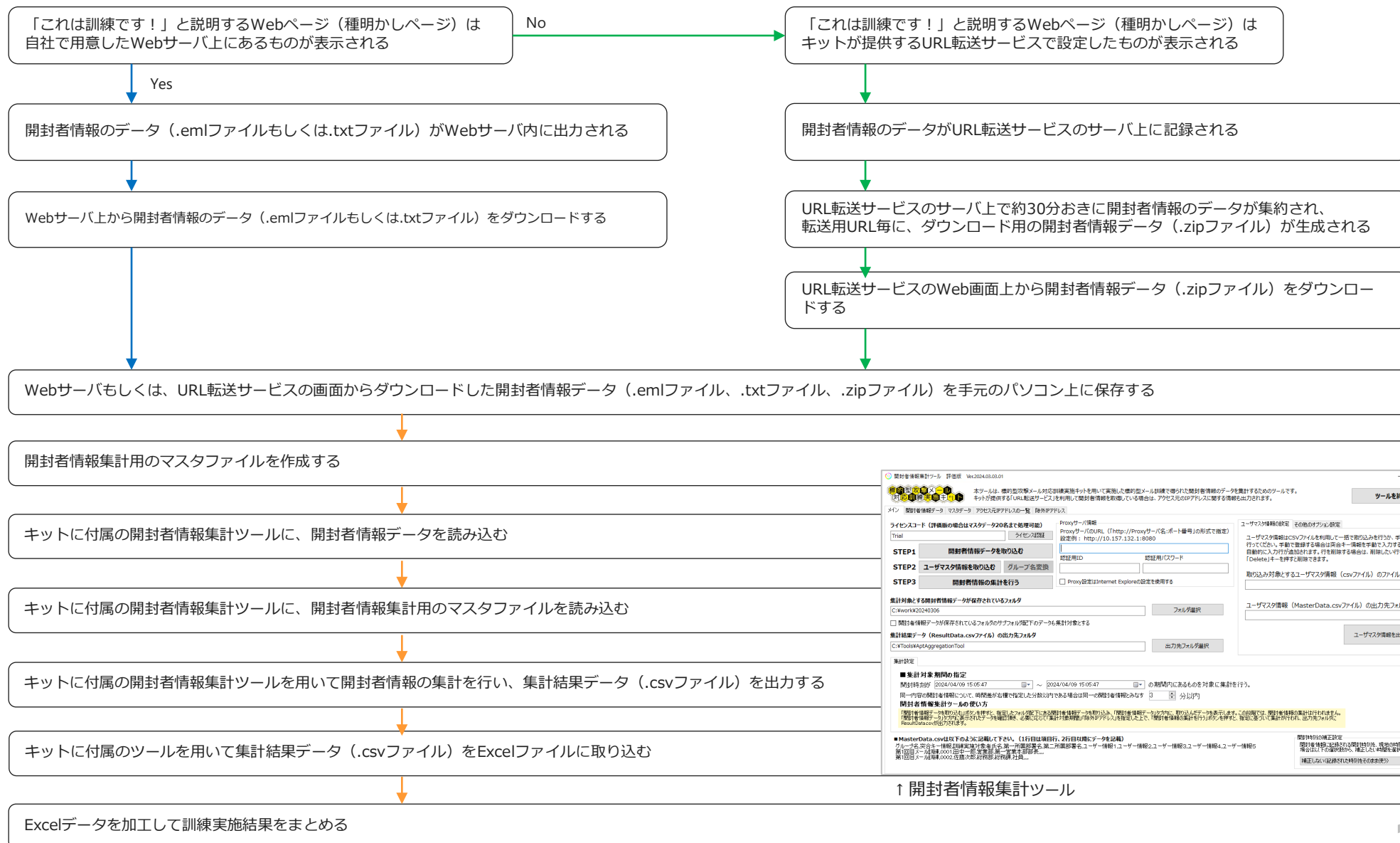
10

キットを活用して訓練を実施される場合の作業の流れ（訓練メール送信まで）



11

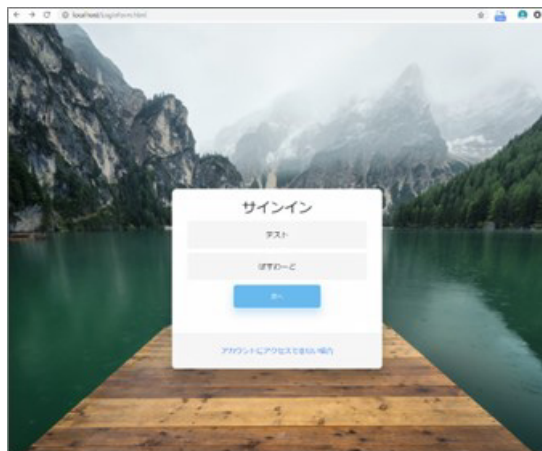
キットを活用して訓練を実施される場合の作業の流れ（開封者情報集計まで）



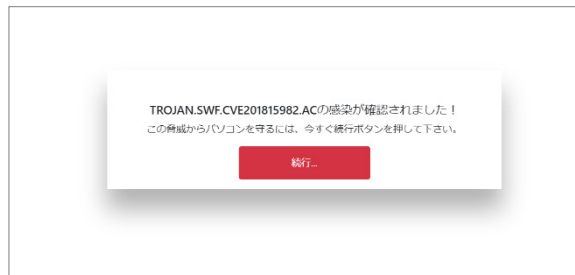
12 フィッシング詐欺対応訓練に対応したコンテンツ

キットでは、標準で3パターンのフィッシング詐欺対応訓練用のコンテンツデータをご用意しており、ご自身でカスタマイズしたものを使用する事も可能です。

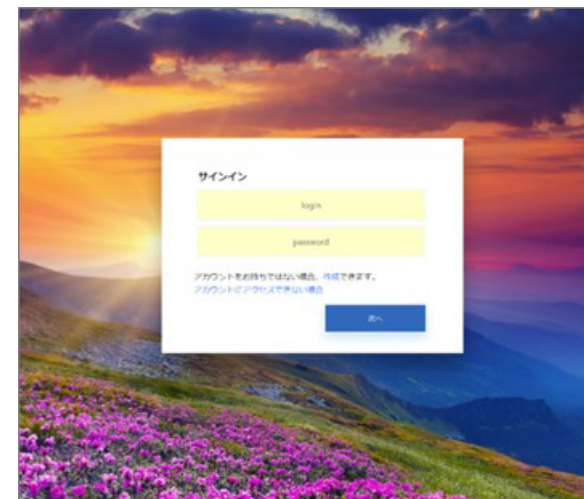
パターン① 動きのあるログインフォーム



パターン② ウィルス感染通知



パターン③ Office365風のログインフォーム



【フィッシング詐欺対応訓練の流れ】

フィッシング詐欺対応訓練では、訓練メール本文中のURLリンクをクリックしたかどうか？また、ログインフォームページで「次へ」ボタンを押したかどうか？が開封者情報として記録されます。

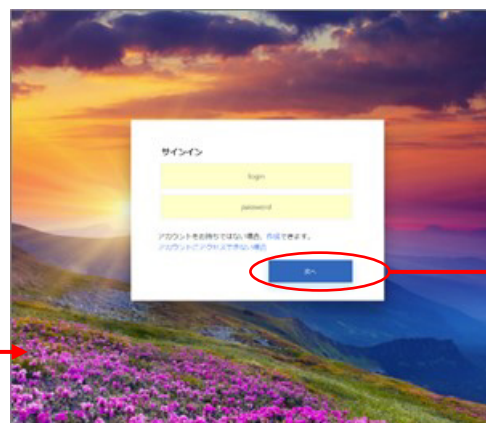
各位

昨夜、弊社メールシステムへの不正アクセスがあり、ログインIDとパスワードが漏洩した可能性があることがシステム担当者より通知されました。

各位におかれましては、不正ログインの発生防止のため、現在のログインパスワードの変更対処を至急実施頂きたく、対応をお願い致します。

つきましては、以下よりパスワード変更をお願い致します。

<http://mailsys.hoge.co.jp/aptkit.aspx?usr=0003>



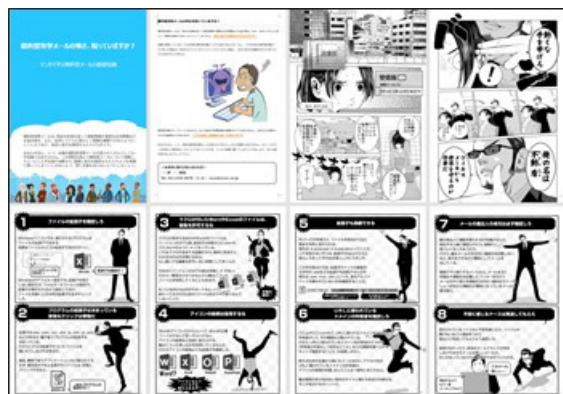
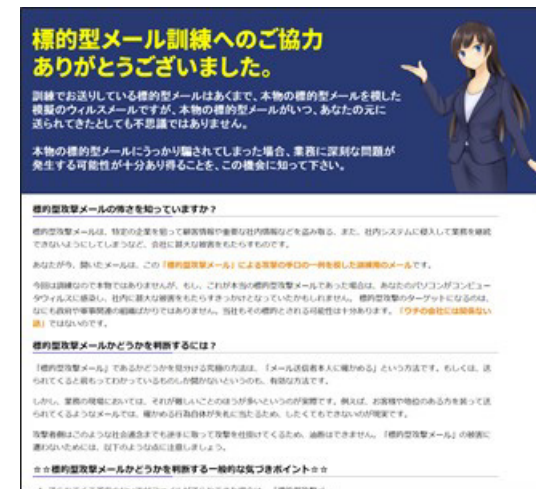
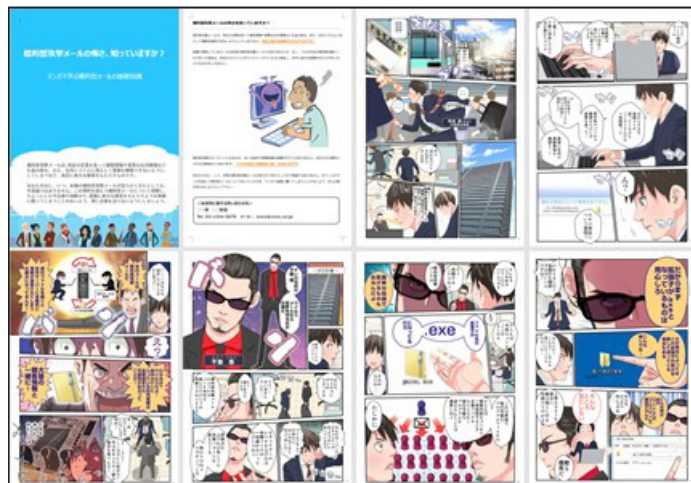
リンクをクリックするとログインフォームが表示される。



さらにログインを実行すると教育用コンテンツが表示される。

13 キットに付属する教育用ドキュメント

キットには、従業員の皆様に「標的型メールとは何か？」また、被害に遭わないために、「どのような点に気を付けるべきか？」といったことを学んでいただくための従業員教育用コンテンツ（資料）が3種類、標準で付属しています。



文字ばかりのコンテンツでは、関心を持って読んでもらうことがなかなか難しいため、キットではプロの漫画家によるマンガを活用し、興味を持って学んでいただけるよう工夫しています。なお、コンテンツについては、随時新しいものを追加して参ります。

また、資料はWord文書形式及び、HTMLデータ形式でご提供しますので、そのままお使い頂けるだけでなく、担当者様にて自由に編集してお使い頂くこともできるようになっています。

14 マンガ動画形式の従業員教育用コンテンツもご提供しています

弊社では、無料でお使い頂けるセキュリティ教育コンテンツとして、マンガ動画を楽しみながらセキュリティを学ぶことができるYouTubeチャンネル「情弱返上？悪玉ちゃん！」を開設しております。標的型メールやフィッシング詐欺など、インターネットに潜む様々なリスクや対策方法について学ぶことができる動画コンテンツとなっております。貴社の従業員研修用の動画として無料でお使い頂けますので、キットと併せてご活用頂ければ幸いです。

【マンガ動画】情弱返上？悪玉ちゃん！
情弱返上？悪玉ちゃん！公式サイト

https://www.youtube.com/channel/UCjUvK_6dXYorrfYJQP6q1g
<https://akudamachan.com/>



第1話



第2話



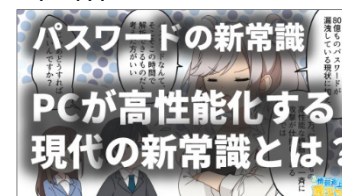
第3話



第4話



第5話



第6話



15 標的型攻撃メール対応訓練実施キットのライセンス体系

キットのライセンス体系は、1ユーザー毎のライセンスではなく、**1社毎の年間ライセンス制**となり、1社単独での訓練実施を対象とした「単一企業用ライセンス」、グループ会社も交えた訓練実施を可能とする「グループ企業用ライセンス」をご用意しています。

・単一企業用キット・ベーシック版 99,000円/年(消費税込み) 2年目以降 66,000円/年(消費税込み)

他社を交えず、1社単独で訓練を実施される場合は、こちらをご選択ください。標的型メール訓練を初めて実施される企業様や、高度な訓練は実施できなくても良いので、とにかくリーズナブルに訓練を実施したいとお考えの企業様には、こちらがお奨めです。

・単一企業用キット・スタンダード版 198,000円/年(消費税込み) 2年目以降 140,800円/年(消費税込み)

ベーシック版では、「模擬のマルウェアファイルのカスタマイズができない」「1回の訓練で対象とすることができる訓練対象者の数が1,000名まで」という制限がありますが、スタンダード版の場合は、これらの制限なしに訓練を実施することができます。1,000名以上の従業員を対象とした訓練を実施される場合、また、自社オリジナルの添付ファイルを訓練で使用したい場合は、こちらをご選択ください。

・グループ企業用Sキット 220,000円/年(消費税込み) 2年目以降 220,000円/年(消費税込み)

グループ企業用Sは、連結従業員数が2,000名以下となるグループ会社様であれば、グループ会社全て（親会社・子会社・孫会社・関係会社）を対象に、実施回数や対象者数の制限なしに、訓練を実施することができるライセンスとなります。単一企業用のライセンスでは自社内での訓練実施に限られますが、グループ企業用のライセンスの場合は、スタンダード版で提供される機能が利用できるのに加えて、自社及びグループ会社に対して訓練を実施することが可能なライセンスとなります。

・グループ企業用Aキット 330,000円/年(消費税込み) 2年目以降 330,000円/年(消費税込み)

グループ企業用Aは、連結従業員数が2,000名を超えるグループ企業様について、親会社・子会社・関係会社を対象に、実施回数や対象者数の制限なしに、訓練を実施することができるライセンスとなります。但し、グループ企業用Aの場合は、孫会社に対する訓練の実施は対象外となりますので、孫会社まで含めての訓練実施を希望される場合は、グループ企業用Bのライセンスをご検討下さい。

・グループ企業用Bキット 396,000円/年(消費税込み) 2年目以降 396,000円/年(消費税込み)

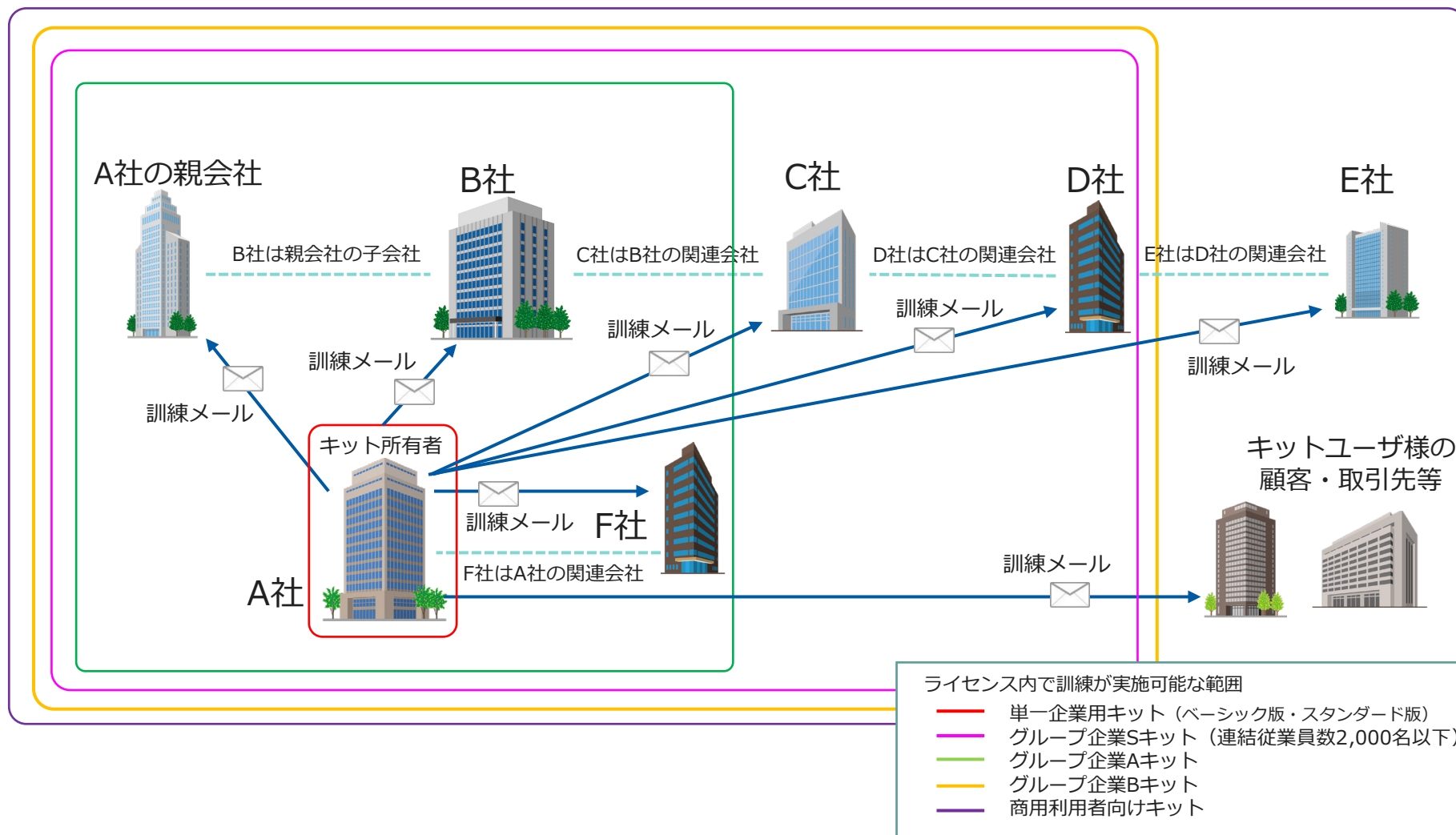
グループ企業用Aと、グループ企業用Bの違いは、グループ企業用Aが、自社・親会社・子会社・関係会社を対象とした訓練が実施できるのに対し、グループ企業用Bは、グループ企業用Aでカバーされる範囲に加えて、親会社・子会社・関係会社の子会社・関係会社も交えて、訓練が実施できる点となります。孫会社も含めて訓練を実施することを希望される場合は、こちらをご選択ください。

標的型攻撃メール対応訓練実施キットのライセンスの考え方につきましては、以下の図のようになります。



17 標的型攻撃メール対応訓練実施キットのライセンス体系②

一例として、グループ企業において、親会社のシステム運用子会社が訓練を実施するような場合、キットのライセンスの考え方につきましては、以下の図のようになります。



18 さらに、次のようなご支援プランもご用意しています

キットを使えば、標的型メール訓練を内製で実施できそうなことはわかったけれど、自社には技術がわかる者もいないし、自分にはなんだか難しそうで使いこなせそうにないかも・・・。

そのように仰る担当者の方も少なくありません。実際のところ、そんなことはないのですが、一見、難しそうなお内容を見て、キットを使ってみることに躊躇してしまったり、また、普段から忙しいために、キットを使ってみたいと思っても、そのための時間がなかなか取りづらい。そんなご担当者様のために、以下のご支援プランもご用意しています。

キット導入支援プラン (<https://kit.happyexcelproject.com/installsvc/>)

キットの設定や使い方に精通した担当者が御社にお伺いし、キットを使ってすぐに標的型メール訓練が実施できるよう、必要な設定を行うプランです。

実際のところ、担当者様が躊躇してしまうのは、キットを使って訓練が実施できるようになるまでに必要な設定について、キットに付属の資料を読んで内容を理解し、実際に設定を行う。という作業の部分です。実際にやってみたらたいしたことなかった。というようなことであっても、それがわからないうちは、どうしても面倒なことのよう思えて、なかなか手がつかない。ということはあるがちです。

これがハードルとなって、なかなか訓練実施に踏み出せない。という担当者様のために、訓練がすぐにでも実施できる状態にまで、キットに精通した技術者が担当者様に代わって設定を行います。担当者様がやるべきことは、訓練メールの本文を考える、訓練メールに添付するファイルを作成する、訓練メールの送付先のアドレスリストを用意する、など、技術者でなくてもできることだけ。

普段から忙しくて、なかなか時間が取れないような担当者様でも、本支援プランを利用すれば、すぐにでも標的型メール訓練を実施頂くことが可能です。

詳細は <https://kit.happyexcelproject.com/installsvc/> をご参照ください。

訓練実施支援プラン (<https://kit.happyexcelproject.com/engineer-plus/>)

自社内製で訓練を実施したい。と思っではいるのだけれど、年中忙しくて自分でやるのはなかなか厳しい。でも、業者に委託したのでは予算が合わない。

そんな担当者様のために、訓練実施に必要な設備の用意や、訓練メールの送信など、ご自身でやるのはなかなか厳しい。という部分について、キットに精通した技術者が、貴社に代わって代行をさせて頂く支援プランです。

業者に全てお願いするのではなく、キットを使って自社内製で訓練を実施するという形を取りながらも、ご自身では手が回らない部分についてのみ、作業の実施を弊社に委託頂くプランなので、業者に訓練実施を委託するよりもリーズナブルな価格で訓練が実施できます。

詳細は <https://kit.happyexcelproject.com/engineer-plus/> をご参照ください。

19 キットに関する詳細、お問い合わせは

キットに関する詳細情報、また、お問い合わせにつきましては、以下のサイトをご参照下さい。

キットに関するお問い合わせページ
キットの試用版お申込みページ
無料でご利用頂けるマンガ動画の公式サイト

<https://kit.happyexcelproject.com/askandorder/>
<https://kit.happyexcelproject.com/monitor/>
<https://akudamachan.com/>

<https://kit.happyexcelproject.com/>



キットの詳細案内

ask@kunrenkit.jp でお問合せをお受けしております。

標的型メール訓練と云えば、標的型攻撃メール対応訓練実施キットが
お役に立ちます。訓練実施に際すること、何でもお問い合わせ下さい。

[キットのご購入に関するご案内はこちら](#)

Top | **キットの詳細** | 商品ラインアップ | お問い合わせフォーム | キットを無料でお試し | 訓練実施の無料講座 | コラム | サイトマップ

標的型メール訓練は内製で実施できるということ、知っていますか？

実際に現場で訓練を実施している「中の人」が、コストも手間もかけずに標的型攻撃メール訓練を実施できないだろうか？そう考えて作ったもの、それが、

標的型攻撃メール 対応訓練実施キット

なんです。

コストパフォーマンスの良い標的型攻撃メール訓練をご検討なら、是非キットを検討候補にお加えください。

【標的型メール訓練は自社内製での実施が正解】 本当に成果上がる訓練は自らの手で実施することから

紹介動画

コンセプト

キットの特徴

キットの構成

他社訓練サービスとの違い

標的型メール訓練やらなきゃ！でも、予算とクオリティの両立に悩んだら・・・そんなあなたに、お役めの解決方法をお教えします！



標的型メール訓練をするよう、会社から指示された。それも、なるほど。

しかし、今期の予算は限られているし、予算の追加も期待薄。費用はかけずに、しかし、クオリティは下げずに、そんな理想を叶えるサービスはありませんか？

はい、そんなあなたの理想を叶えるのが「標的型攻撃メール対応訓練実施キット」です！

「標的型攻撃メール対応訓練実施キット」は、プロの訓練実施代行業者にも活用されている、標的型メール訓練実施のためのツールセット。まずは動画をご覧ください。

<https://kunrenkit.jp/>



コストをかせずに標的型メール訓練を実施したいなら、幅広い業種・業界で利用されている当キットの利用を是非、他社と比較して検討してみてください。

Top | **キットの特長** | 商品ラインアップ | キット評価版の申し込み | キットに関するお問合せ

標的型メール訓練は内製で実施できるということ、知っていますか？

実際に現場で訓練を実施している「中の人」が、コストも手間もかけずに標的型攻撃メール訓練を実施できないだろうか？そう考えて作ったもの、それが、

標的型攻撃メール 対応訓練実施キット

なんです。

コストパフォーマンスの良い標的型攻撃メール訓練をご検討なら、是非キットを検討候補にお加えください。

キットで実施できる訓練

1. URLリンククリック型の訓練
2. 添付ファイル型の訓練
3. フィッシング詐欺対応訓練
4. ファイルダウンロード型の訓練

以上を組み合わせた訓練

キットが提供するもの

- ① 訓練メールを作成するための支援ツール
- ② 統計情報を集計するためのツール
- ③ 訓練メールを送信するためのシステム
- ④ 通知カレンダーを表示するWebサイト機能
- ⑤ 従業員トレーニングのためのコンテンツ
- ⑥ 訓練実施後のアンケートを実施する機能
- ⑦ その他、内製で標的型攻撃訓練を実施するために必要なツールやドキュメント

無料で使える評価版でまずはお試しを！

約1ヶ月間、キットを無料でお試しいただける評価版をご提供しています。

訓練の外注を検討されているのでしたら、コスト削減に繋がる内製での訓練実施ができないう、キットを使って試してみてください！

[⇒キット評価版お申し込みフォームへ](#)

本資料を御覧頂きまして ありがとうございました

サイバーセキュリティ対策は今や経営課題、
もはや“やらない”という選択肢はありません。
貴社はこの課題に社を挙げて取り組むことができますか？
サイバーセキュリティに関する関心や知識、肝心の社員が
持ち合わせていなければ取り組みのしようがありません。
社員全員を対象に体験型の「標的型メール訓練」を実施する
ことは、社員の関心と意識向上に役立ちます。

訓練実施に関するご相談、お気軽にお寄せください。

ask@kunrenkit.jp