標的型攻撃メール対応訓練サービスのご案内

株式会社ブロードバンドセキュリティ

Ver.16

はじめに

平素は格別のご高配を賜り、厚く御礼申し上げます。

ご提案の機会を賜り誠にありがとうございます。

さて、国内外で、特定の組織をターゲットとした「標的型攻撃」が相次ぎ、大きな問題となっております。
攻撃を許すことで受ける被害は内部にとどまらず、外部への攻撃拠点となってしまうこともあるため、情報セキュリティの確保は社会的責任として合理的な取り組みが求められております。

本資料では、総合セキュリティ対策企業として「情報セキュリティに関する多角的な問題の洗出し」、「課題解決のコンサルティングやソリューションをご提供・ご支援」してまいりました弊社より「標的型攻撃メール対応訓練サービス」をご提案させて頂きます。

お客様のさらなる情報セキュリティ向上にお役にたてるよう尽力する所存でございますので、御用命賜りますよう宜しくお願い申し上げます。

株式会社ブロードバンドセキュリティ

本サービス実施の目的

目　的

情報セキュリティにおける脅威の理解と適切な対処の促進

　情報セキュリティ教育の一環として、標的型攻撃を想定した不審メールの対処に関する職員・従業員への訓練を実施します。

　既知のウイルス対策やメールフィルタリングを潜り抜ける標的型攻撃メールに対してメール受信者である従業員の適切な判断が被害防止の最初の砦となります。

　訓練を通じて、実際の脅威に近い形で体験していただくことでメールを用いた攻撃に対する危機意識とセキュリティ意識が向上し、適切な対処に関する理解促進が期待されます。

標的型攻撃の脅威の理解

インシデントに関する迅速な報告

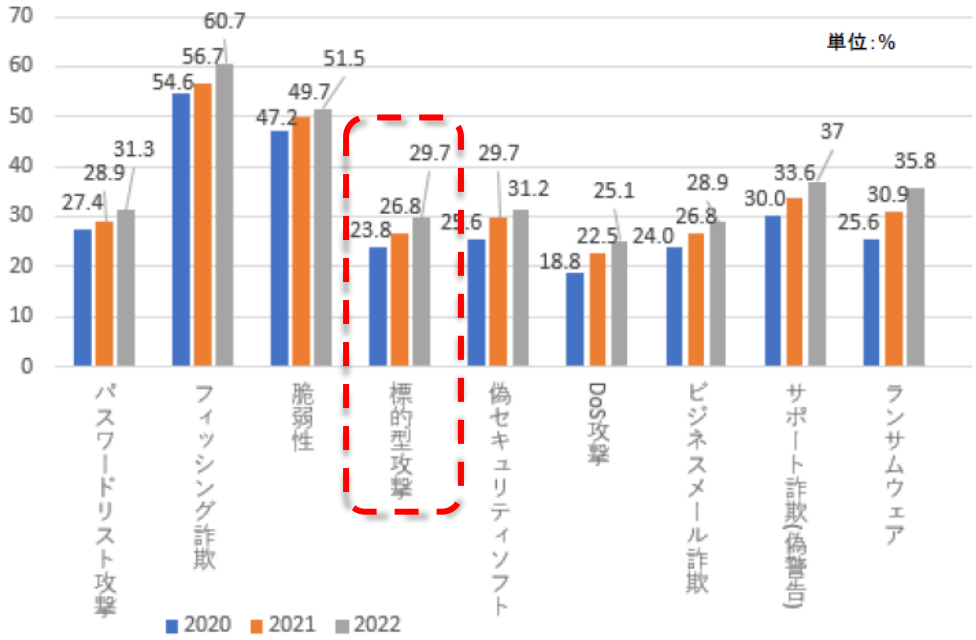
標的型攻撃の増加と認知度のギャップ

■メールによる標的型攻撃は、それを受けているのに気づかず放置され、内部のパソコン・サーバから情報を長期間にわたって奪取されるため、危険度の高い攻撃といえます。

■無数の亜種がある標的型攻撃のウイルスは、対策ソフトで検知できる可能性が低いのが実態です。

■また、標的型攻撃は2006年5月から情報処理推進機構によって報告されていますが、認知率は29.7%（右グラフ参照）に過ぎません。

脅威名の認知度（Q.2）パソコン利用者経年比較



※「知っている」「ある程度知っている」の合計値。

出典：情報セキュリティの倫理と脅威に対する 意識調査（IPA、2023年2月より）
P18「3-2-2. 脅威名の認知度（ Q.2 ）パソコン利用者 経年比較」より抜粋

標的型攻撃がどういったものか実体験を通じて一人ひとりのセキュリティ知識を深めることが、情報漏洩の入り口対策として必要といえます。

標的型攻撃の種類

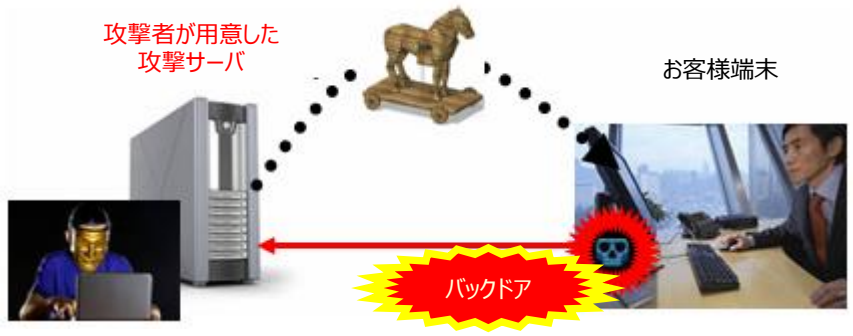
標的型攻撃は、大きく分けて以下の4タイプがあります。
そのうちメール添付型・不正サイト誘導型に代表されるメールによる標的型攻撃は
受信者一人ひとりのセキュリティ意識がなければその被害に合う可能性が高いといえます。

標的型攻撃メールによる情報漏えいの流れ

① 標的型攻撃メールの添付ファイルを実行することで、端末がウイルスに感染

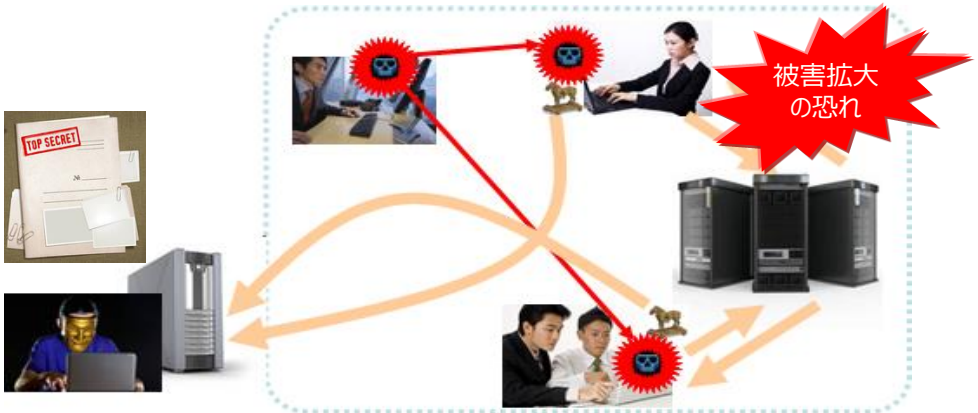
② 感染した端末がウィルス「トロイの木馬等」をダウンロード
（不正操作環境が構築される）

感染しても気づかない場合が多い



③ 感染した端末が攻撃者に情報を送信

④ 感染が長期間検出されないことで被害拡大

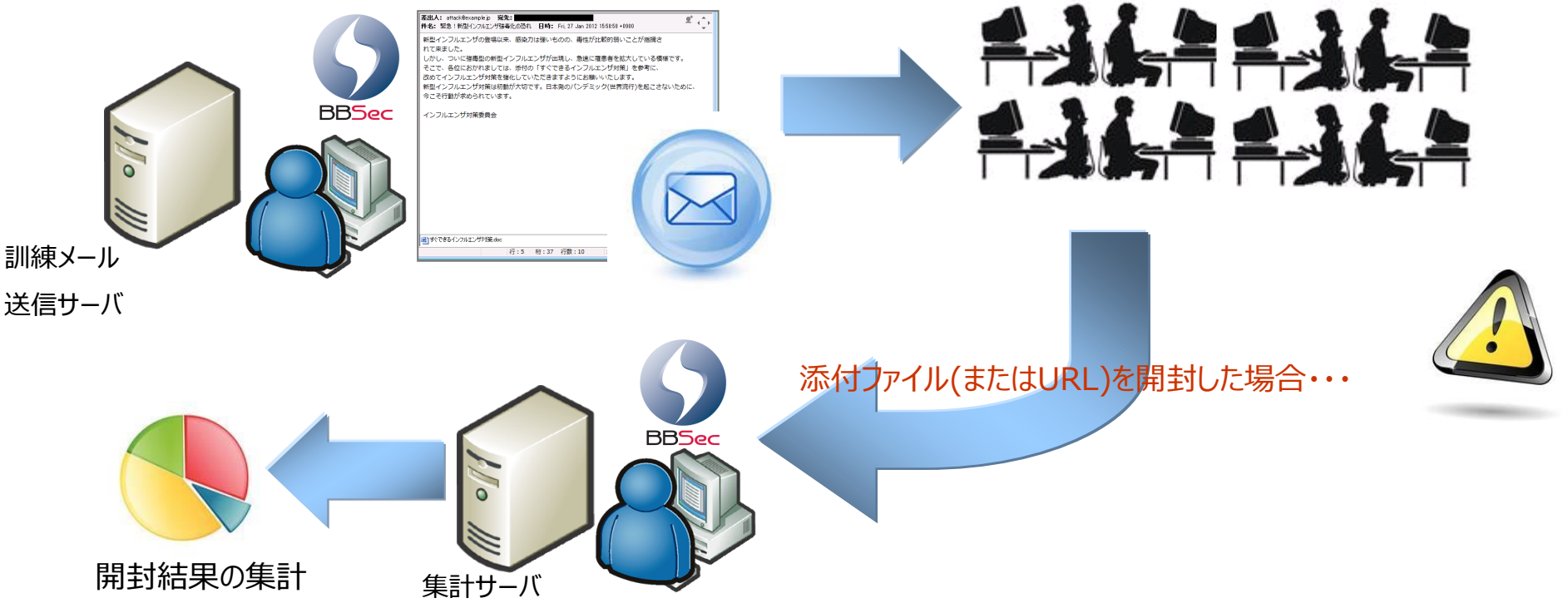


標的型攻撃メール対応訓練の概要イメージ

弊社から擬似標的型攻撃メールを配信します。

添付型：擬似標的型攻撃メールにファイルが添付

URL型：本文中にURLが記載



添付ファイル開封（URLアクセス)による

Webビーコンのアクセスログを取得します。

標的型攻撃メール対応訓練のご提供概要

標的型攻撃手法

ファイル添付型、URL型のご選択が可能です。（添付ファイル形式はMS　Wordなど）

訓練メール配信回数

同一の対象者に1ケ月間の中で2回の訓練メールを配信し、1回目と2回目の効果を図ります。

訓練の流れ（一般的な流れ）

①事前教育メール（お客様にて配信）第1回訓練メール送信の1週間から1ケ月前に配信を推奨しております。

②テストメール配信　（BBSec配信）　お客様ご担当者のみにテストメールをお送りします。

③第1回訓練メール（BBSec配信）配信時間は、10時と13時を推奨しております。

④種明かしメール（お客様にて配信）訓練メールの配信後、翌営業日（または翌々営業日）を目途に配信頂きます。

※開封者の不安や問合せに配慮して、休日をまたがないことを推奨します。

※配信後に内部の混乱を招いた場合は、種明かしメールの前倒しを推奨します。

⑤第2回訓練メール（BBSec配信）　第1回訓練メールの1週間後を目途に配信を行います。

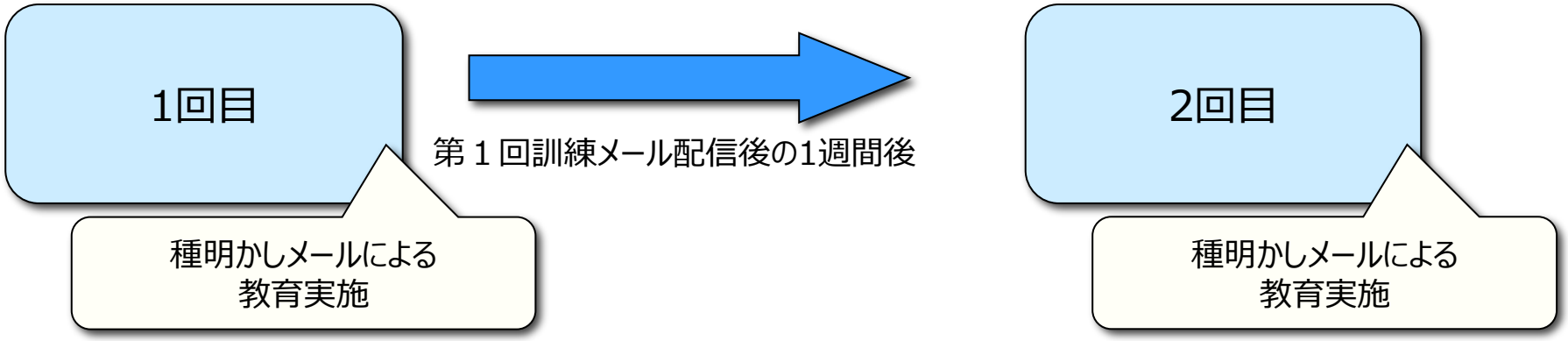
⑥種明かしメール（お客様にて配信）訓練メールの配信後、翌営業日（または翌々営業日）を目途に配信頂きます。（④と同様の配慮を推奨）

⑦報告書のご提出（BBSec集計、作成）

※報告書を内部に開示し、セキュリティ向上に活用されることを推奨します。

※結果は統計的に利用し、開封者名を公開しないことを推奨します。（開封者が傷ついたりしていることへの配慮）

標的型攻撃メール対応訓練のメール配信回数



2回の擬似攻撃メール配信でセキュリティ意識向上の効果を計る
本サービスの標準構成です。

標的型攻撃メール対応訓練の具体的な流れ①

2週間～約１ケ月程度～　　約１ケ月間程度

実施前準備

訓練メール文や教育資料サンプル等をご提供します。

事前教育
メール配信
（お客様にて
実施頂きます）

訓練対象者に、標的型攻撃に関する事前教育（メール）を推奨します。

訓練対象者からの訓練への反発（ハレーション）をやわらげる効果があります。

お客様にて配信頂きますが、サンプルをご提供します。

第1回訓練
メール配信

弊社メールシステムから、訓練対象者に擬似攻撃メールを配信します。

種明かしメール
メール配信①
（お客様にて
実施頂きます）

訓練対象者に擬似攻撃メールの種明かし及び標的型攻撃メールへの理解度を高める内容のメールをお送り頂きます。

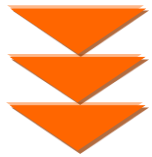
サンプルをご提供します。

第2回訓練
メール配信

再度、擬似攻撃メールを訓練対象者に配信します。

種明かしメール
メール配信②
（お客様にて
実施頂きます）

第1回同様、擬似攻撃メールの種明かし及び標的型攻撃メールへの理解度を高める内容のメールをお送り頂きます。



全社に結果を開示

情報セキュリティリテラシーの向上を目的に結果の開示を行うことを推奨します。
尚、個人名やメールアドレスは公開しないことを推奨します。

結果集計/報告書作成
ご報告

訓練結果を集計、報告書を作成し報告致します。

お客様にて実施頂く事項

弊社実施事項

標的型攻撃メール対応訓練の具体的な流れ②

大項目	項目	担当	内容
ご提案からご発注	本サービスのご案内	BBSec	本サービス内容と留意事項についてご説明します。
	コンテンツサンプル提供	BBSec	ご発注後に以下の資料をご提供致します。 1.メールサンプルコンテンツ　2.教育コンテンツサンプル　3.登録情報申込書　4.メール配信技術仕様書
訓練実施準備	役割のご決定と関係者(協力者）への説明とご承認	お客様	・お客様ご担当者を確定下さい。 ・経営者及び訓練対象の部門長には本企画内容をご説明下さい。 ・情報システム部門のメール担当者、セキュリティ担当者には本企画内容をご説明下さい。
	システム確認。 ①MUAは受信アドレスを表示しているかの確認 ②３秒間隔配信による流量制限抵触の有無などを確認 ③WebビーコンのHTTPアクセスの可否について確認　等	お客様	情報システム部門のメール担当者やネットワーク担当者にご確認下さい。 ※詳細は、「メール配信技術仕様書」をご確認下さい。
	全配信コンテンツのご検討とご決定	お客様	お客様にて配信する内容、弊社から配信する内容、配信希望日等をご決定下さい。
	ホワイトリストへの登録	お客様	配信する訓練メールのメールアドレスまたはIPアドレスをホワイトリストに登録して下さい。
	登録情報申込書及び訓練対象者アドレスのご提出	お客様	配信日希望日、配信メール内容、訓練対象者メールアドレスを申込書にあわせてご提供頂きます。
	テストメールによる配信テスト	BBSec	以下を目的としてお客様ご担当者向けに本番と同じ内容にて配信テストを実施します。 ・スパム判定無しの確認・ファイル開封のカウント確認
	事前教育メール配信 （お客様にて実施頂きます）	お客様	訓練対象者に、標的型攻撃に関する事前教育（メール）を推奨します。 訓練対象者からの訓練への反発（ハレーション）をやわらげる効果があります。 メールのサンプルは弊社からご提供致します。
訓練実施期間	第1回訓練メール配信	BBSec	弊社メールシステムから訓練対象者に配信します。擬似攻撃メールには、開封判定するためのWebビーコンが埋め込まれています。
	種明かしメールメール配信① （お客様にて実施頂きます）	お客様	訓練対象者に擬似攻撃メールの種明かし及び標的型攻撃メールについて理解度を高める内容のメールをお送り頂きます。
	第2回訓練メール配信	BBSec	第1回と同様。
	種明かしメールメール配信② （お客様にて実施頂きます）	お客様	第1回と同様。
	報告書作成	BBSec	集計、結果報告書を作成します。
	お客様にご報告	BBSec	報告書を納品します。
	結果を内部に開示	お客様	結果を内部に開示することで更なるセキュリティ向上意識の向上を図って頂くことを推奨します。

御提供資料等について

■システム確認を行う上での技術仕様書について

技術的な配信仕様をまとめた「メール配信技術仕様書」をご用意しております。
システム確認を行う上での配信形式やホワイトリストへの登録IPアドレス、Webビーコン集計サーバのURLなどが記載されております。ご検討頂ける場合、別途ご提出させて頂きます。

■訓練サンプルコンテンツ等について

以下、訓練で必要となるコンテンツのサンプルを用意しております。

Ⅰ.標的型攻撃メール対応訓練サービスメールサンプルコンテンツ
①事前教育メールサンプル
②種明かしメールサンプル
③訓練で使用する擬似攻撃メールサンプル　130種類以上

Ⅱ.教育コンテンツサンプル

Ⅲ.訓練メール　添付ファイル

Ⅳ.登録情報申込書

事前教育メールについて

各位

情報セキュリティ対策委員会
責任者：○○××

「標的型メール攻撃についての注意喚起」の件

お疲れ様です。
近年、特定の組織・職員を狙う
「不審なメールによる攻撃（標的型攻撃）」が
増加する傾向にあります。
攻撃メールは、ウイルス対策ソフトウェアやスパムフィルタ等を迂回して、あなたのメールボックスまで届きます。

偽メールに騙されて、添付ファイルなどを実行してしまうと、ウイルス感染や情報漏えいの被害につながります。被害を避けるためには、各自が不審なメールに対する警戒心を日頃から高めておくことが大切です。

・・・省略・・・

■事前教育メール例

お客様でご配信いただく事前教育メールのサンプルになります。

本メールに教育コンテンツを添付し注意喚起と理解を促進する方法もございます。

■事前教育メール配信の意味

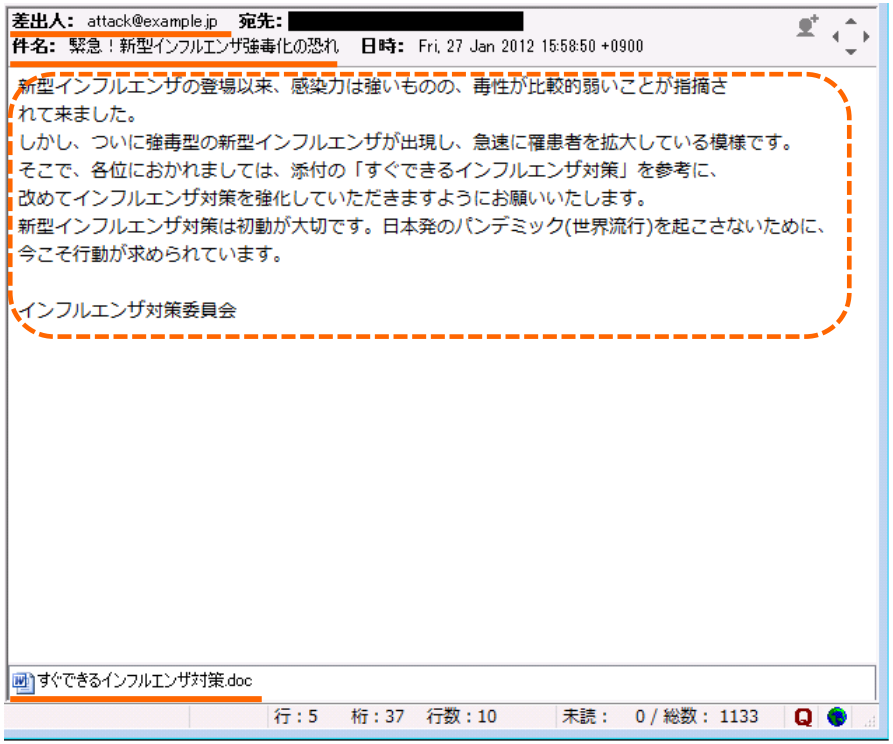
過去、抜き打ちで訓練メールを配信したために対象者が感情を害し、訓練を継続できない事例がありました。
事前にこうした攻撃の脅威を周知、喚起して従業員が訓練の主旨を理解頂くためにも事前教育メール配信を推奨します。
事前教育によって、次の効果が期待できます。

1. 訓練対象者の反発(逆効果）をやわらげること。
2. 事前教育メールと訓練体験を結びつけることで対象者に標的型メール攻撃の脅威をより深く体感していただき不審なメールへの対応方法を学んでいただくこと。

※お客様の情報セキュリティ教育においてこうした注意喚起を行っている場合があるかと存じますが、再認識の観点から訓練前の事前教育メール配信をご検討下さい。

訓練で使用する擬似攻撃メールについて

＜擬似攻撃メールイメージ＞



■擬似攻撃メールについて

メールサンプルは、130種類以上を用意しております。

変更可能部分

① 差出人（送信元）メールアドレスのローカルパート
② 件名
③ 本文の一部修正
④ 添付ファイル名

※詳細については文面作成時に協議とさせていただきます。

(ご注意事項)

メール内に実在または類似の企業名、商品名などの記載は弊社訓練ポリシーにより
ご遠慮いただいております。

文字化けを防ぐため、機種依存文字は使用しないようお願いします。
記号(①②③・・・)、№㏍㍉℡㊤㊥㊦㊧㊨㈱㈲㍾㍽㍼㍻、ローマ数(Ⅰ Ⅱ Ⅲ・・・)等

訓練メール　添付ファイル内容について

〔本件に関するお問合せ先〕
部門:○○○部　○○○課　○○○○○
TEL:○○○○○○○

①

本件は、情報セキュリティ訓練です。

ご注意！ このような怪しいメールの添付ファイルを不用意に開封すると
貴方を狙うウイルス等に感染する恐れがあります

本添付ファイルを開けたメールは、当社のセキュリティ訓練のために不審メールを模したもので、本文・件名に記載された内容は架空のものです。今回の訓練は、今後このような標的型メール攻撃による脅威への予防活動として実施しました。
訓練として実施のため、各位に事前説明を行わずに送付しており、ご説明が事後になりましたこと事情ご理解いただきご容赦ください。また、本添付ファイルには危険性はありません。ウイルスとしての機能はありません。添付ファイルを開いた際に訓練用ウェブサイトに添付ファイルのオープン状況の取得を行なっています。今回の結果を集計し今後のセキュリティ改善に活かす予定です。
最近の情勢では、本物の標的型メール攻撃がいつあってもおかしくないと言われています。また、昨今の悪意ある標的型攻撃は、日々高度な技法で情報搾取を狙っておりシステム防御が困難な場合もあります。世間全般に非常に難しい問題となっております。社員一人ひとりがセキュリティ意識を高めることで情報漏えいを守れることも少なくありません。是非、皆様におかれましても継続的に注意していただきますようご宜しくお願い申し上げます。

○不審なメールと添付ファイルがもたらす脅威（標的型攻撃）:
近年、特定の組織・職員を狙う「不審なメールによる攻撃(標的型攻撃)」が増加する傾向にあります。
標的型攻撃の偽メールは、従来のウイルス対策ソフトウェアやスパムフィルタ等を迂回して、あなたのメールボックスまで直接届きます。もっともらしい偽メールの文面・件名に騙されて、添付ファイルを実行してしまうと、ウイルス等への感染や情報漏えいの被害につながります。被害を避けるためには、各員が不審なメールに対する警戒心を日頃から高めておくことが大切です。

○対処の方法:
怪しげなメールが届いた場合には、標的型攻撃を受けている可能性を疑ってください。
騙される前に普段とどこか異なる点や違和感に気づくことができるかもしれません。
怪しげなメールについた添付ファイルの実行や保存は避けてください。
また、怪しげなメールが届いた場合は、上長や情報セキュリティ担当者に報告してください。

②

○不審なメールの特徴　以下にご注意頂きたい例を挙げさせて頂きます。
- 差出人の名前やアドレスが、見慣れないものである。
- 組織内の知人なのに、外部のメールアドレスから届いている。
- 添付ファイルを開くよう不自然に誘導している。
- 緊急などと急がせて、メールの内容を吟味させないとしている。
- 差出人の署名や名乗りが怪しい・曖昧である。
- 差出人の名前や組織名として、架空のものを名乗っている。

■添付ファイルについて

左記のMicrosoft Word形式を標準としております。

① （本件に関するお問合せ先）

お客様内の問合せ先となります。

部門名、ご担当者名を申込書に記載下さい。

② 対処の方法

文言は参考として記載してありますがお客様の実態に合わせて変更が可能です。

「上長や情報セキュリティ担当者に報告してください。」

※上記②は、事前教育メール、種明かしメール、教育コンテンツに同様の記載がございます。②を変更される場合は、これらも修正することにご留意下さい。

「白紙を表示」、「404Not Found風」なども対応可能です。

種明しメールについて（訓練メール配信後）

各位

情報セキュリティ対策委員会
責任者：○○××

標的型攻撃メールの訓練の実施について(報告)

お疲れ様です。
日頃、情報セキュリティ対策にご協力を頂きまして、誠にありがとうございます。

今回、標的型攻撃に対する情報セキュリティ教育訓練として、「擬似攻撃メール訓練」を実施いたしました。
件名：○○○　配信日時：○○○

これは、擬似的な標的型攻撃を体験していただくことで本当の攻撃に対する訓練とするものです。
今回の訓練でうまく対応できなかったとしても、実害もありませんし、マイナスの評価をするわけでもありません。今後の対応の参考にしていただければ十分です。

標的型攻撃とはどのようなものか、またどのような対応をする必要があるかは、○月○日に注意喚起した通りです。

･･･省略･･･

■種明かしメール例

お客様にて配信いただく種明かしメールのサンプルになります。
教育コンテンツを添付する方法や社内のグループウエアに教育コンテンツを掲載し注意喚起と理解を促進する方法もございます。
開封結果の集計締めタイミング把握のために、種明かしメールには、BCCに以下のアドレスを入れて下さい。
customer_service@bbsec.co.jp

■第２回訓練メールの種明かしについて

訓練終了となる２回目の種明では「今回で今年の訓練は終了です。但し、標的型攻撃には引き続きご注意下さい」と通知するお客様もございます。これは業務への支障を考慮し対象者の訓練メールに対する嫌悪感を和らげる効果もあります。

教育コンテンツについて(オプション)

■教育コンテンツのご利用方法

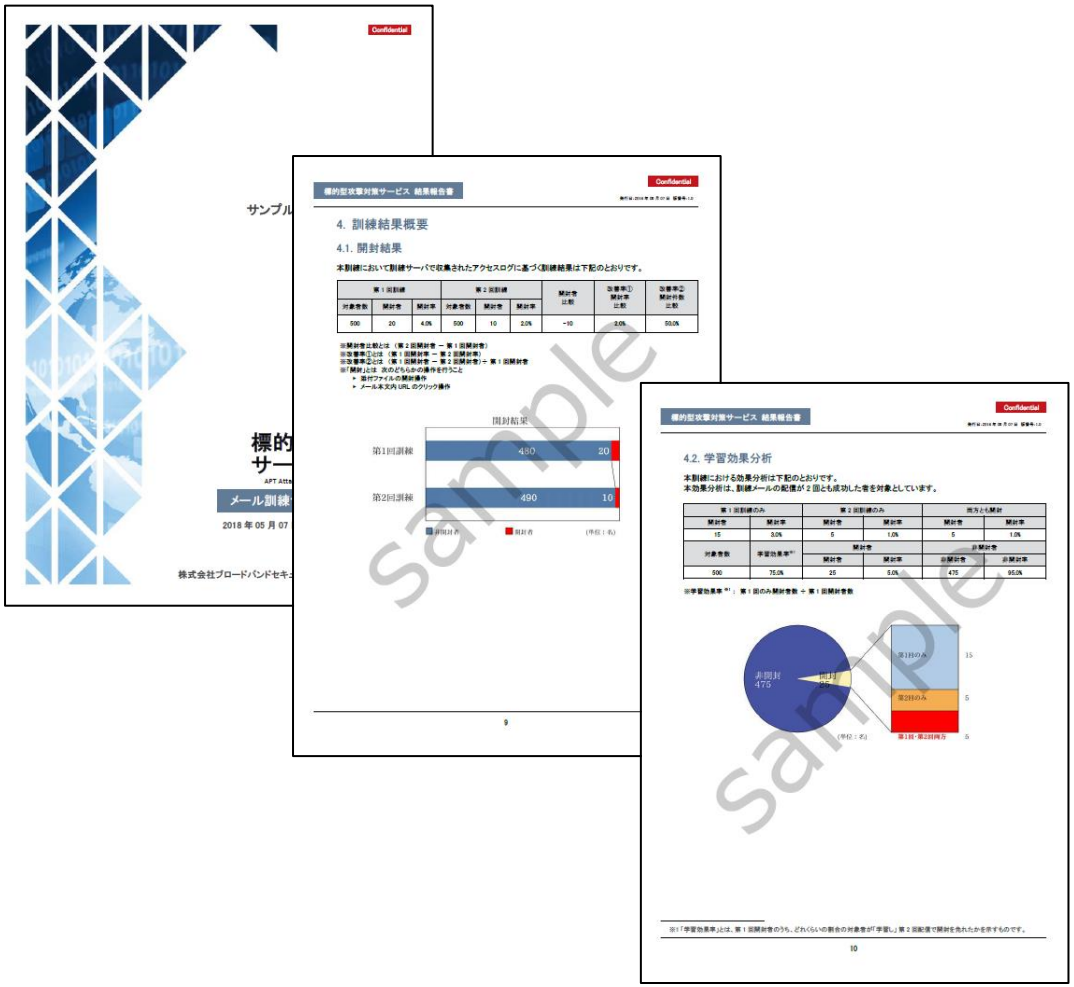
標的型メール攻撃に関する教育資料を有償にてご用意しております。

お客様の事前教育メール、種明しメールに添付してご利用頂くことが可能です。

本資料を編集いただき、お客様のセキュリティ教育資料としてグループウェアへの掲載等の活用も可能です。

※転売等は禁じております。ご承知おき下さい。

報告書イメージ



■報告書の内容

訓練実施内容、第１回、第2回開封者集計と、２回の結果の比較になります。

経営層へのご報告や内部展開によりセキュリティ意識の向上にお役立てください。

■報告書の納品について

原則.pdfによるデータでの納品となります。

■報告書以外のご提供資料

①配信結果一覧

対象者メールアドレスごとの配信した時間、配信結果

②開封者一覧

開封者メールアドレスと配信した時間、開封した時間

上記データと属性データ（職種別、入社年数別等）を照合して分析に活用されるお客様もいらっしゃいます。

※訓練の目的はセキュリティ意識向上であり、懲罰を行うためのものではありません。開封者個人名の公表は控えることを推奨します。

訓練実施における推奨事項①

（１）訓練の目的をご認識いただくこと

開封者への懲罰等が目的ではないことをご認識下さい。難易度の高い標的型攻撃メールは、誰でも開封してしまう可能性があり、開封者を懲罰対象にすることは推奨しません。 攻撃の可能性があるということを訓練対象者に認識していただきセキュリティ意識の向上が目的とすることを推奨します。

（２）事前に訓練実施を周知しておくべき対象者

訓練実施前に関係者にこの訓練実施（実施日等詳細）をお伝えする必要があります。
管理職の方、各ラインの部門長、情報システム部担当者、メール管理者等があげられます。訓練対象者及びシステム部門の上長の承諾を得ておくことが重要です。情報システム部担当者、メール管理者が訓練を知らないで実施した場合、スパムとして全社に通知されインシデント扱いとなる可能性があるためです。

（３）役割の決定

事前教育や種明かしはお客様に実施頂きます。このご担当者(事務局)を決定しておく必要があります。情報セキュリティ責任者名で通知する組織が多く、これらのメールには問合せ先も明記し、問合せのフォローも必要になります。

（４）訓練対象者からの問合せについて

可能な限り個別説明を行い、他の訓練対象者のために、周囲に訓練を明かさないように依頼する必要があります。また、こうした標的型攻撃メールに対してシステム側で対策を取って欲しいという依頼もありえます。「セキュリティ対策は随時実施しているが、日々進化する攻撃に対して完全に防御が出来ない場合もある。インシデント防止には皆様の協力が必要です。」などの回答案を持っておくことを推奨します。

訓練実施における推奨事項②

（５）訓練のポイント「気づき」

訓練のポイントは、対象者の不審メールの「気づき」になります。
対象者の学習レベルにもよりますが、初期訓練の場合、高度な訓練は望ましくありません。極端に難しくすると、対象者の警戒心や判断力に関する現在の状況を知ることができないだけではなく「自分には対処不能」という印象を与えてしまい、訓練による意識向上の効果が期待できないからです。
そのため、何を「気づき」のポイントにさせるかが重要になります。
「気づき」のポイントとして、見知らぬメール、メールアドレスに対して不信感を持たせ気づかせることがあります。
そのため、初回は以下の事項などを考慮頂ければと存じます。
・一読して違和感を覚えるやや怪しげな文面を作成する。
・署名欄の内容を不審を抱かせるものにする。

（６）第1回訓練メールの配信のタイミング

1. 事前教育から1週間以上経過していること。
2. お客様によって異なりますが、週明けの月曜日は業務多忙となりがちなことから火曜日や水曜日を推奨します。
   また、休日に訓練メールを開封し、問合せ窓口がないことによる混乱を発生させないために週後半の配信も推奨しておりません。
3. 配信開始は、10:00または13:00からのご選択になります。これは業務が一段落するタイミングや、その日のうちにある程度訓練メールに接することができるタイミングを考慮したものとなります。

（７）教育資料のご活用　事前教育メール、種明かしメールへの添付資料

事前教育メール、種明かしメールに添付資料として教育コンテンツを添付することは可能です。お客様にてご判断下さい。

訓練実施における推奨事項③

（８）種明かしメールのタイミング

はじめて訓練を実施する場合、混乱の程度が推測出来ません。
混乱がひどい場合には種明かしメールを予定よりも早く出して頂いても構いません。
配信から種明かしまでを長くとっても全員がメールを閲覧できるとは限りません。また、種明かしまでは問合せ担当者の負担が増えます。
訓練により業務に悪影響が出ないように種明かしを実施することを推奨します。
基本的には、訓練メール配信後、種明かしメールまでを1日を目安としております。
種明かしのタイミングが開封結果の集計締めタイミングとなりますので、実施した日時をお教え下さい。
尚、種明かしメールには、BCCで次のアドレスを入れて下さい。customer_service@bbsec.co.jp

また、第1回訓練と第2回訓練において訓練効果を測定するためには、同一の訓練期間を推奨しております。
つまり、第1回訓練の種明かしを訓練翌日とする場合、第2回訓練の種明かしも翌日にするということです。

（９）インシデント対応力の強化と問合せ記録

擬似攻撃メールを開封しないように、メールを吟味する習慣づけも大切ですが、怪しいメールと気づいた場合にお客様内のルールに則ったインシデント対応として、セキュリティ担当者に連絡をする習慣をつけていただくことも重要です。
また、問合せは出来得る限り記録することを推奨します。セキュリティ担当者または、上長にあがってきた情報を、いつ、どこから、報告があがってきたかまとめているお客様もあります。この問合せ内容を記録しておくと、内部レポートを作成し、経営あるいは内部に開示する際のキーポイントとなります。
こうした攻撃に対して敏感に反応したことをきちんと褒めることもセキュリティ意識向上の重要な要素と言えます。

（１０）標的型攻撃訓練の頻度

実施頻度は慎重に検討し、狼少年効果を生んでしまうことを避けるべきです。半年に１回、年1回程度を推奨します。

訓練実施におけるご留意事項①

（１）配信するアドレスのスパム登録について

訓練メール配信中にスパム登録が行われてしまうと訓練メールがスパムとして処理される可能性があります。
留意すべき事項としては・・・
①訓練に用いるメールアドレスは事前に情報システム部門にお伝え頂きホワイトリストに追加いただくこと。
②訓練対象者からスパム登録機関へのスパム申請を実施しないこと。スパム申請が行われた場合でも訓練の中止は行いません。
スパム判定がされた場合、対象者に訓練メールが届かない可能性があることを予めご承知おき下さい。これらの対応については
お客様内での運用ルール次第となりますので、スパムの個人申請を許容していないか等について予め確認をお願いします。

（2）配信リスト対象外　メーリングリスト

配信対象にはメーリングリストを含めないようお願いします。メーリングリストの開封者を特定することはできません。また、メーリングリストへの配信トラブル(ループ、過負荷等)を防止することもその理由です。

（3）メールソフトウェア動作環境

現在リリースされているWindowsOS＋メールソフトには原則対応可能。
※本番配信前のテストメールで最終的な提供可否を確認致します。

（4）対象外メールソフトウェア

Lotus Notesはお客様での個別設定により動作が安定しないためURL型訓練を推奨します。（添付ファイル型は非推奨）
Microsoft Exchange ServerのWebメールは対象外となります。（セキュリティ保護により添付ファイルが削除されるため）

（5）WordファイルによるWebビーコンの動作確認環境

現在リリースされているWindowsOS＋wordには原則対応可能。
※本番配信前のテストメールで最終的な提供可否を確認致します。

（6）差出人のメールアドレス表示について

気づきのポイントである「差出人のメールアドレス」が表示されるかメールソフトの設定ご確認下さい。

訓練実施におけるご留意事項②

（7）訓練メールの削除について
訓練メールは、訓練終了後に削除をお願いします。種明かしメールにはその旨を記載しております。理由としては、訓練終了後にも弊社サーバに不要なログが記録されることになるためとなります。
（8）配信未達の場合について
訓練メールが配信未達となる場合があります。例えば、対象者のメールボックスがあふれている、個人のスパム設定で受信しないようにしている、お客様ネットワークのご都合等で受信できないなど。これらの未達に関する調査は免責事項とさせて頂きます。配送結果はご提出致しますが、再配信は致しません。尚、第 1 回訓練メールで未達となったものは第 2 回訓練メールでは配信対象から除外します。
（9）訓練メール配信希望日について①
配信希望日がご希望に添えない場合がございます。その場合、別途日程調整をさせていただきます。
（10）訓練メール配信希望日について②
配信希望日は、原則、弊社営業日をご記入下さい。また、訓練メールから種明かしメールまでは休日をまたがないことを推奨します。
（11）テストメールの確認結果
確認結果によっては本番配信スケジュールが再調整となります。予めご承知おき下さい。
（12）種明かしメールついて
種明かしを予定日時より早く実施された場合、必ずご連絡をお願い致します。
（13）Webビーコンが受信できないケースについて
Microsoft製品のセキュリティ機能「保護されたビュー」により添付ファイル開封時のWebビーコン受信ができない場合がございます。 その際には代替案を提示致します。

標的型攻撃メール訓練サービス
サービスプラン

標的型攻撃メール訓練サービス　プラン

項目	プラン	スタンダード	プレミアム（カスタマイズ例）*3
訓練メール内容	メール文面	当社作成サンプル (日本語・英語）から選択	その他の言語対応（中国語など）が可能
	メール文面変更	カスタマイズ可能	宛名の差し込み等の希望に応じたカスタマイズが可能
	メールのタイプ	弊社指定のURL型または添付型 （Word、JS、EXEより選択）での実施	お客様独自のURL型または添付型での実施が可能 (EXEについては添付ファイルのアイコンの変更が可能)
訓練メール配信	配信日	弊社指定配信日時より選択	お客様希望による日程調整が可能
	配信対象数	メールアドレス数 1,000件以内	配信対象数の上限なし*4
	配信回数	2回（配信間隔は1ヶ月以内）	お客様希望による配信間隔の調整が可能
	配信枠数	2枠（配信回数 2回分）*2	スタンダード同様
	配信速報の送付	枠単位での送付	複数枠の集計が可能
訓練報告	報告書提出	開封結果・学習効果（2回の配信の比較）を報告	開封結果・学習効果（2回の配信の比較）を報告
	報告・相談会	なし	管理者向けの報告会・対策の相談会を実施
	実施後アンケート	なし	訓練実施後にアンケート*5 を実施し、報告書に追加可能

*1 文面につき、弊社ガイドラインに従っていることが条件
*2 オプションにより枠を買い増し、グループ別の分割配信が可能
*3 スタンダードをベースとして、追加サービスの選択が可能
*4 2,000件以上は複数枠による分割配信が必要、8,000件以上の場合には別途プロジェクト・マネージメント費用が必要（別途見積）
*5 有償オプションとしての提供

標的型攻撃メール訓練サービス　費用

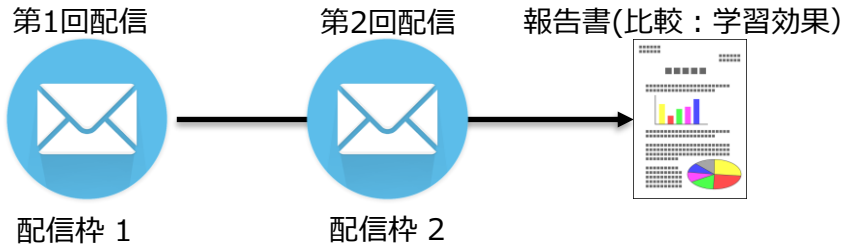
項目 ＼ プラン	スタンダード	プレミアム
メール訓練サービス 基本料金 *1	¥300,000	¥400,000
共通オプション料金		
- 配信枠数追加 (分割配信)	¥150,000/配信枠	¥150,000/配信枠
プレミアム・オプション料金（カスタマイズ）		
- 訓練メール内容 カスタマイズ	-	¥150,000 *3
- 訓練メール配信　個別対応	- *2	¥150,000 *4
- 訓練報告 カスタマイズ	-	¥150,000
プレミアム・オプション料金（追加）		
- 事後アンケート実施・報告書反映	-	¥150,000 *5
- プロジェクト・マネージメント	-	別途見積

プラン ＼ 価格	価格	備考
自己学習 資料提供	¥100,000	学習資料（ドキュメントとしての提供）
オンサイト・セキュリティ講習会	別途見積	セキュリティ・プロフェッショナルによる90分の講習会 習熟度テストの提供

*1 Office 365向け特別配信技術料を含みます
*2 スタンダードを選択の場合には配信日の変更はできませんが、お客様都合によりやむを得ず変更が必要になってしまった場合には追加料金を申し受ける場合がございます
*3 翻訳作業が必要な場合には、別途見積となります
*4 3ヶ月を越える配信間隔が必要な場合には別途見積となります
*5 事後アンケートは8,000人以下を対象に行うアンケート1回当たりの価格であり、これを越える場合には別途見積となります

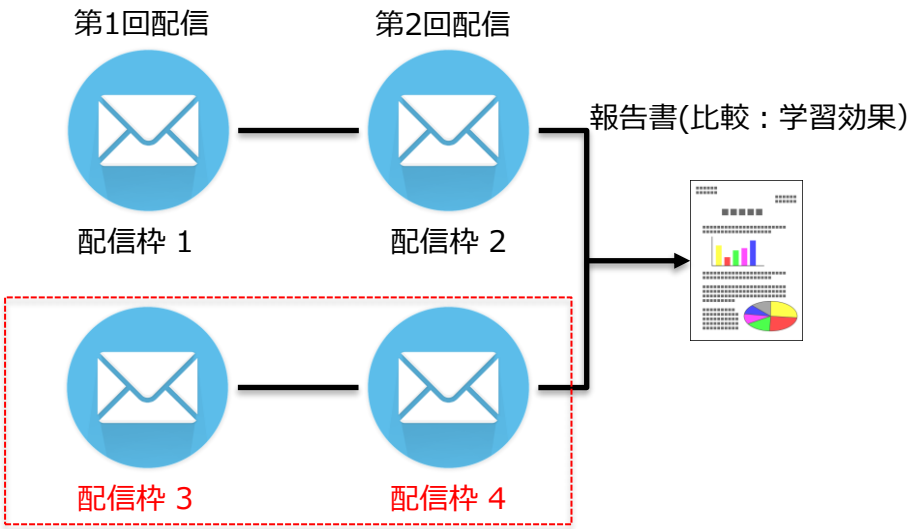
標的型攻撃メール訓練サービス　配信枠の考え方

スタンダード(配信枠 2) :標準仕様



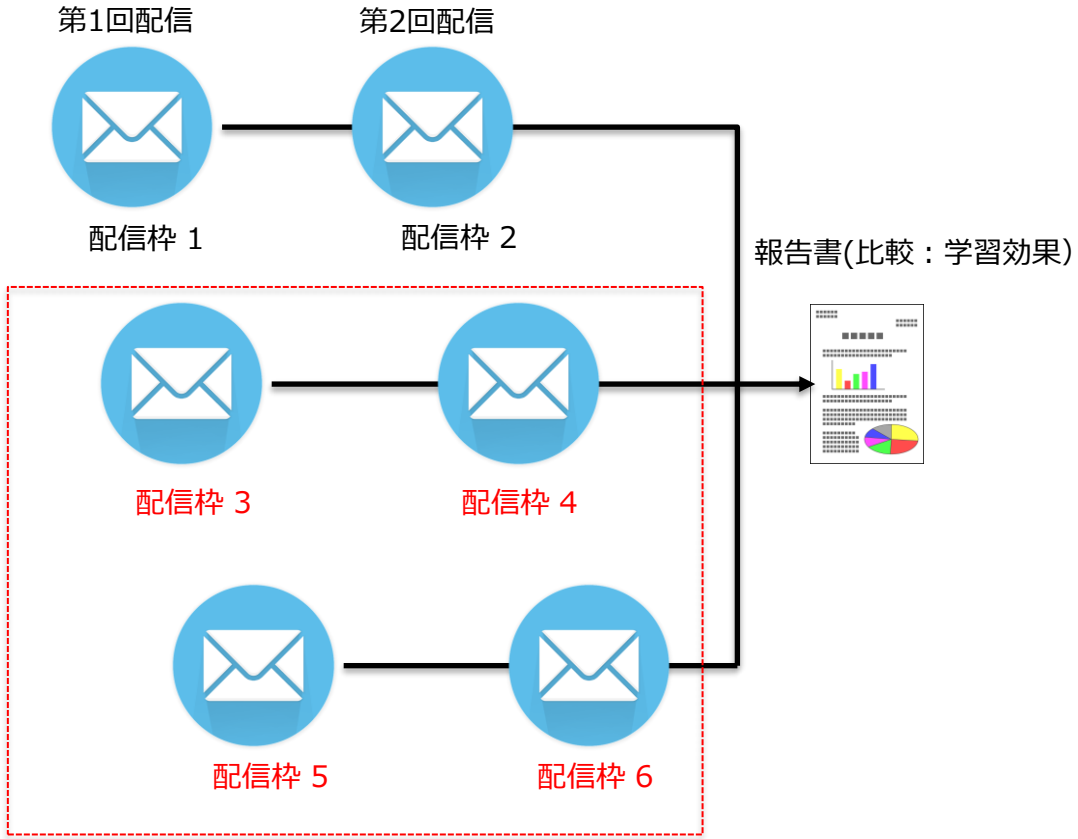
【分割配信例】：■配信枠別に異なる文面、タイプで配信

スタンダード(配信枠 2) + 配信枠 2 追加（分割配信）



【分割配信例】：■配信枠別に異なる日時で配信

スタンダード(配信枠 2) + 配信枠 4 追加（分割配信）



会社概要

会社概要

■会社名　株式会社ブロードバンドセキュリティ

■本社所在地　東京都新宿区西新宿8-5-1　野村不動産西新宿共同ビル4F
TEL：03-5338-7430

■事業内容　当社は、企業における情報漏洩の予防や防止、セキュリティ機器の24時間365日体制での遠隔監視、未知のマルウェア検知によるネットワーク遮断等により、情報漏洩リスクから企業を守る事を目的としたセキュリティサービスを主要な事業としております。

詳細は弊社webサイトをご覧下さい。

https://www.bbsec.co.jp/

公的認証取得

組織

 ICMS-SR0328 / JIS Q 27001	 10470048	
ISO/IEC 27001:2013=JIS Q 27001:2014	プライバシーマーク	Qualified Security Assessor (QSA)

技術者・コンサルタント保有資格

- Qualified Security Assessor (QSA)
- Associate Qualified Security Assessor (AQSA)
- 3-D Secure Assessor(3DS)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Network Forensic Analyst (GNFA)
- 情報処理安全確保支援士/情報セキュリティスペシャリスト
- 公認情報セキュリティ監査人 (CAIS-Auditor)
- Certified Ethical Hacker (CEH)

その他多数