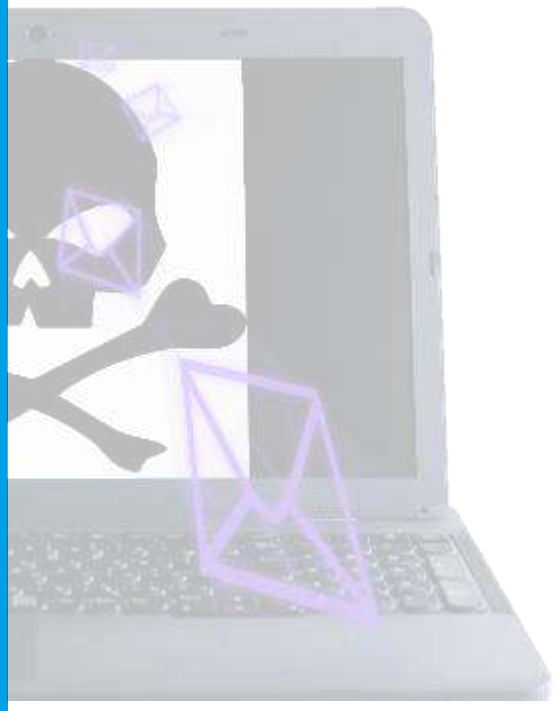
増大する
標的型攻撃
メールの脅威

～今日から始める
社内対策～



アクモス 株式会社

[- INDEX -]

はじめに

増大する標的型攻撃メールの脅威
その実態と対策は？

アクモス 株式会社

はじめに

増大する標的型攻撃メールの脅威
その実態と対策は？

近年、**特定の組織や人をターゲットとした標的型攻撃メールの被害が増えています。**
企業の種類や大小を問わず被害を受けており、情報漏えいや金銭被害を受けていても、時間が経過してから発覚するケースも少なくありません。

メールは多くの企業で利用される汎用的なツールです。その分**「誰でも・いつでも」被害者になりえる**ため、常日頃からの対策が欠かせません。

「企業向けのセキュリティ対策が知りたい」

「従業員へのセキュリティ教育を強化したい」

とお考えの皆様。標的型攻撃メールに対する訓練から、組織全体のセキュリティ対策を見直しませんか？

悪意のあるメールに対する耐性向上を図り、**企業の資産を守りましょう。**本資料では、標的型攻撃メール対策の効果や訓練方法を解説していきます。

第１章

標的型攻撃メールの実態とは？

アクモス 株式会社

第１章　標的型攻撃メールの実態とは？

標的型攻撃メールとは？

“標的型攻撃メール”とは、**特定の組織や個人に対して攻撃を意図した、悪意のあるメール**を指します。興味・関心をひく巧妙な内容のメールを送信し、メールに添付されたファイルやURLを受信者がクリックするよう促し、マルウェアのインストールやアカウント情報の窃取などを行います。

また、経営層や取引先などを装い、入金や口座変更等の金銭的被害をもたらす**「ビジネスメール詐欺」**や、不特定多数をターゲットとしてフィッシングメールを送信する**「ばらまき型攻撃メール」**も、広義の標的型攻撃メールと捉えることができます。

第１章　標的型攻撃メールの実態とは？

標的型攻撃メールの内容

攻撃に使われるメールの内容として、以下のようなものがあります。

- **不特定多数の方の興味を誘う偽メール**
  ※財産、健康、性的な内容、身近な人間関係など
- **有名企業やサービスを騙った偽メール**
  ※ECサイト、Webサービス、宅配業者など
- **事前に入手した企業の詳細情報を元に、人間関係や組織関係を偽装したメール**
  ※HPに掲載された情報、事前に漏えいしたメール、ソーシャルハックで取得した情報等

いずれも巧妙な内容で、“最初の目的”である**「悪意のあるURLにアクセス」「悪意のある添付ファイルを実行」**に開封者を誘導します。

また、初回のメールでは攻撃を行わず、関係者になりすまして複数回メールのやり取りを行い、信用を得た後に攻撃メールを送信して騙す例もあります。

偽装メールの内容や攻撃手段は日々進化しており、**セキュリティシステムでの防御、社内での注意喚起のみでは被害の防止が困難**です。

第１章　標的型攻撃メールの実態とは？

「訓練が重要」な3つの理由

攻撃の起点は「攻撃用URLをクリックしてしまう・攻撃用ファイルを実行してしまう」ことです。システム的な対策によってこの確率を減らす事はできますが、最終的には**ひとりひとりが判断するしかありません。**

攻撃メールの脅威から組織を守るためには、災害に対して避難訓練を行うように、攻撃メールに対する訓練を行うという事前対策が効果的です。

すぐにでも対策を始めるべき理由として、次の3つが挙げられます。

1. **増大するメール攻撃の脅威度**
2. **だれでもターゲットになりうる危険性**
3. **実際に発生している甚大な被害**

詳しくは次のページから見ていきましょう。

第１章　標的型攻撃メールの実態とは？

1. 増大するメール攻撃の脅威度

2019年8月に公表された、IPA（情報処理推進機構）の「情報セキュリティ10大脅威 2019」によると、組織にとっての脅威１位は**「標的型攻撃による被害」**であり、これは4年連続での1位です。また２位の「ビジネスメール詐欺による被害」、３位の「ランサムウェアによる被害」も**攻撃メールによるもの**です。

近年では大手企業や官公庁などへの攻撃の起点・踏み台として利用するため、比較的セキュリティ対策が薄い取引先の中小企業を対象とした攻撃（サプライチェーン攻撃）も増加しており、その手段として標的型攻撃メールが用いられるケースもあります。

「情報セキュリティ10大脅威 2019」※組織編から一部抜粋

順位	昨年	
1	1	標的型攻撃による被害（※4年連続の1位）
2	3↑	ビジネスメール詐欺による被害
3	2↓	ランサムウェアによる被害
4	圏外↑	サプライチェーンの弱点を悪用した攻撃の高まり
5	8↑	内部不正による情報漏洩
6	9↑	サービス妨害攻撃によるサービスの停止

出典：https://www.ipa.go.jp/security/vuln/10threats2019.html

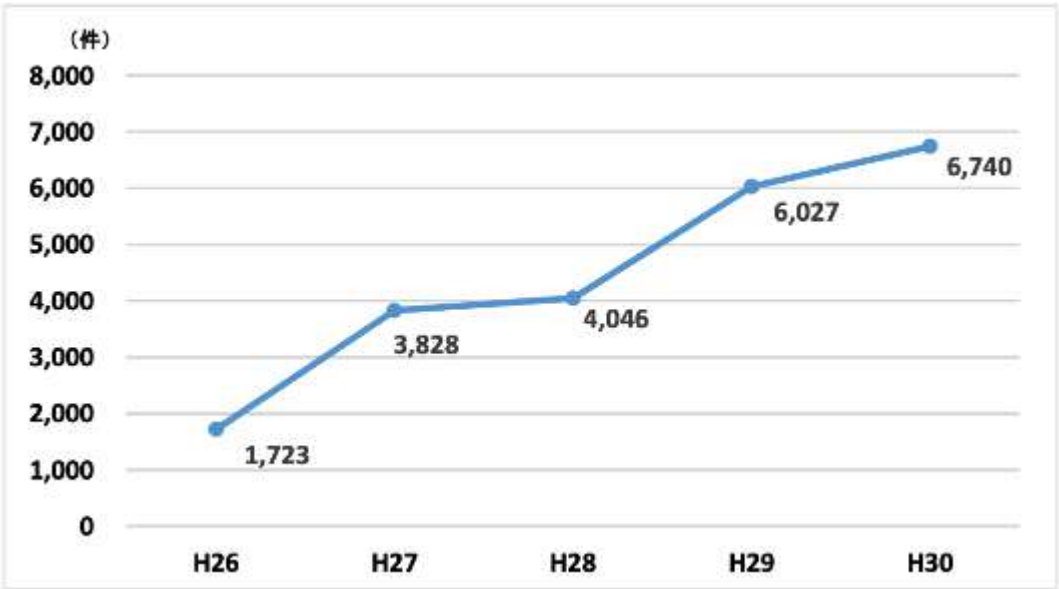
2. だれでもターゲットになりうる危険性

特定の企業に対して、情報を盗むことを目的に計画を実行する**標的型攻撃メールは、ここ4年で3.5倍**にも増えています。

また、より広範囲のターゲットに悪意あるメールを送信するばらまき型攻撃が、標的型攻撃メールの90%を占めています。

組織内の部署や個々人によって、情報への関与度、IT知識、セキュリティ意識にバラつきがありますが、重要な情報に関与していない方でも、攻撃を受けたPCを起点にその他のPCやサーバにまで感染が拡大し、攻撃が組織内に広がる恐れがあります。機密情報の管理者など**特定の人物だけでなく、組織全体でセキュリティ意識を強化していくことが重要**です。

【標的型メール攻撃の件数の推移】



（警察庁/広報資料）
出典：https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf

3. 実際に発生している甚大な被害

標的型攻撃メールによる被害は、数、被害額とも増加しています。2019年11～12月頃にはNTT西日本グループや関西電力、首都大学東京、軽金属製品協会など様々な企業・団体が「Emotet」と呼ばれるマルウェアに感染したことが大きなニュースとなりました。

参考：「Emotet」と呼ばれるウイルスへの感染を狙うメールについて（IPA）
https://www.ipa.go.jp/security/announce/20191202.html

＜標的型攻撃メール訓練の被害事例＞

実例1：東京理科大学 殿（2019年2月）
▶約**4,000件**の個人情報が流出

- フィッシングサイトへの誘導を行うメールが教職員、学生へ送信され、ID／PWが窃取
- 不正ログインにより登録されていたメールアドレスを含む個人情報約4,000件が漏洩

実例2：コインチェック株式会社 殿（2018年1月）
▶**580億円**相当の仮想通貨が流出

- 外部から複数の社員宛てに攻撃メールが届き、業務PCがマルウェアに感染
- 感染したPCから社内ネットワークに侵入し、管理サーバの秘密鍵を用いて不正送金したと想定されている

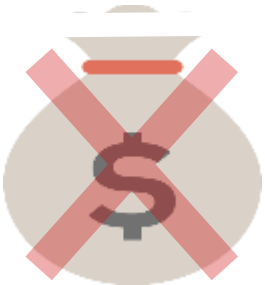
実例3：日本航空株式会社 殿（2017年12月）
▶「振込詐欺」で**約3億8千万円**の被害

- 2017年、取引のある金融会社の担当者を装った詐欺メールを受信
- 支払口座が変更になったと伝える内容で、本物に酷似した請求書も添付されていた

標的型攻撃メールの被害に合うと、**世間からの信頼低下のみならず、多大な損失が発生するケース**もあります。

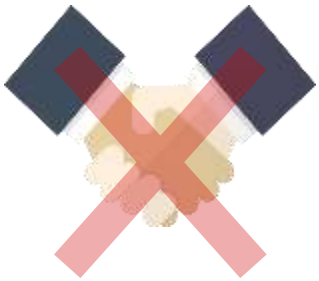
攻撃の被害

標的型攻撃メールによる攻撃を受けると、以下のような被害が発生する可能性があります。



1.金銭被害※

2.対応に要する時間の損失



3.社会的信頼の失墜

また、攻撃に成功してもすぐには被害を発生させず、数ヶ月～数年に渡って対象組織のネットワークに潜伏し、徐々に情報を奪ったり、他への攻撃の踏み台にするなどの執拗な攻撃を行う例もあります。

これらの損失を防ぐためには、注意喚起とあわせて、**実践型の訓練を通じて従業員一人ひとりのセキュリティ意識を高めること**が重要です。

※　偽の入金、データの身代金、障害対応・事故調査対応・原状回復にかかる費用、ビジネス機会の損失、損害賠償など

第２章

標的型攻撃メールの手法と対策

アクモス 株式会社

なぜ攻撃メールを送れる？

そもそも、なぜメールが危険な攻撃に利用されてしまうのでしょうか？

「メール」は規格が古い

メール送信に使われる「SMTP」というプロトコル（データ通信のルール）は1982年に制定された古い規格※です。自由度が高い反面、**攻撃者は簡単に他の利用者や組織を偽装できます。**

※リリース後何度かアップデートが行われ、偽装抑止のためのセキュリティ対策改訂などが行われていますが、インターネット全体で見ると対策は遅れています。

「メール」は広く浸透している

メールアドレスは公私問わず多くの方がお持ちです。つまり攻撃者から見ると**対象の数が多く、簡単にコンタクトを取れる「魅力的な攻撃手段」**なのです。

「メール」は多くの情報を送れる

電子ファイルの添付や、HTMLメールによるURLリンク表示などが可能なため、**攻撃者がマルウェアを添付したり、フィッシングサイトへの誘導**が可能です。

「メール」は簡単・安い

メールは簡単に大人数に向けて送信できます。また配信にかかる総合的なコストは他の手段と比べて格安です。
金銭目的の攻撃者にとって、**低コストで楽に攻撃できるメールは「魅力的」**なのです。

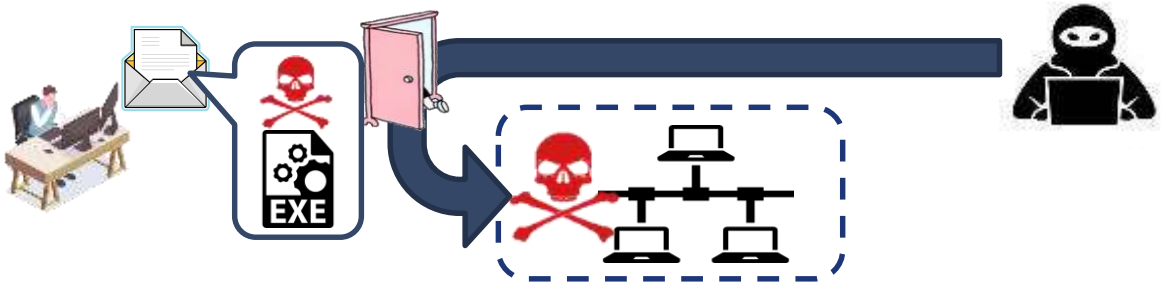
メールによる攻撃の手法

関係者偽装による金銭操作

偽装サイトによる個人情報窃取

ランサムウェアによる重要ファイルのロック

バックドアによる組織ネットワークへの侵入



攻撃を防ぐためには？

標的型攻撃メールなど、インターネットを経由する攻撃に対する防御として、大まかに３つの対策ポイントがあります。

1.入口対策

攻撃メールを「送信させない」「受信しない」ことで防御する手段です。

メール送信元の偽装を防ぐために「メールの送信者が正しいこと」を証明する仕組み＝「**送信ドメイン認証**」が策定されています。いくつか手段があり、防御できる範囲も若干異なりますが、高度な対応を求める場合、送信側・受信側双方の対応を揃える必要があるため、インターネット全体で見た浸透度は高くありません。

受信側で広く行われている入り口対策が、アンチスパムに代表される「**迷惑メールフィルタ機能**」の導入です。一定の効果はありますが、フィルタをすり抜ける攻撃メールもあり、また逆に本来受信するべきメールを誤ってブロックしてしまうなどの弊害もあります。

2.エンドポイント対策

攻撃メールを受信した後の、**クライアント（端末）側での対策のこと**です。

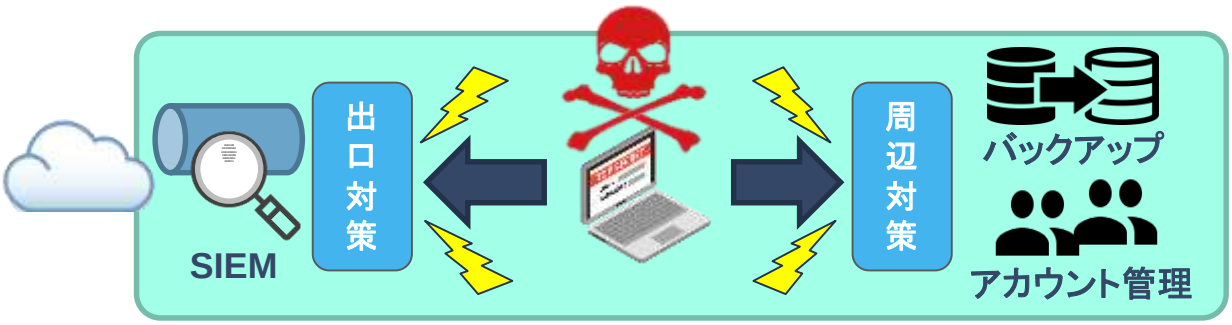
OS・ソフトウェアの環境は「常に最新の状態を保つ」事が最低条件です。攻撃者はOS・ソフトウェアの既知の脆弱性を利用して想定外の挙動を誘発し、マルウェアのインストール等を試みます。

代表的な対策は**アンチウィルスによる防御**です。メールを受信したタイミングで添付ファイルのウィルスチェックや本文のチェック行い、危険なメールであれば警告を出すなどの対応を行います。また一般的にフィッシングサイト対策のURLフィルタ機能を備えています。

これらは標準的な手法ですが、**マルウェアの巧妙化や、新しい攻撃手段への対応が完全ではないことなどから、「入っていれば安心」とは言えなくなっています。**

3.周辺/出口対策

攻撃を受けてしまった場合を想定した対策であり、**被害を最小限に抑えるための対策**です。



データのバックアップは大切です。ランサムウェア等で重要ファイルが使用できなくなっても、適切なバックアップがあれば被害は最小限で済みます。

また、攻撃者は侵入した端末にしかけたバックドアを介してネットワーク上の重要なサーバへ侵入を試みます。その際にサーバのセキュリティが脆弱ですと簡単に侵入を許します。各PCやサーバはそれぞれ異なるアカウントを設定し、強度の高いパスワード、各アカウントの権限を必要最小限にすることが重要です。また、虹彩認証（生体認証）や物理キーなどの多要素認証も有効です。

出口対策として、機器や通信の状況を集中監視する「**SIEM**」(Security Information and Event Management)を導入することで攻撃者の通信やデータ漏えい、不審な挙動の発見が期待できます。

全ての攻撃を防ぐことは不可能

先述の通り、攻撃を防ぐ手段は複数あり、それぞれ防ぐことのできる攻撃の種類・範囲は異なります。しかし、残念ながら**全ての攻撃を防ぐことの出来る防御手段は存在しません**。どうしても、防御をすり抜ける攻撃が一定数出てきてしまいます。

システムによる防御は非常に重要ですが、**システムだけに頼り切るのではなく、私たち一人ひとりが攻撃の被害を受けないため注意をすることが重要**です。

- 「**教育訓練**」は、技術対策と並ぶ重要なセキュリティ対策
- 入口対策－エンドポイント－出口対策の中心に「**人の対策**」

第３章

メール訓練の目的と効果

第３章　訓練の目的と効果

攻撃の脅威に「気づき」を得るチャンス

以前の攻撃メールは「日本語が不自然」などの不審さが目立ち、偽装内容もわかりやすいとされてきました。しかし、近年では翻訳機能の進歩やターゲットの絞り込み等により自然さと現実性が急激に進歩しており、一見しただけでの判断は相当困難です。悪意のある添付ファイルもPDFやExcel、Word、圧縮ファイルなど多様化しています。

十分な知識と注意力をもった方でも、多忙な時期などで注意力が散漫になれば警戒が薄れる傾向にあります。

「うちは大丈夫」ということはありません。注意喚起や研修とあわせて、継続的な訓練で全従業員のセキュリティ意識を高め、情報漏えいや詐欺に対するリスクヘッジを図りましょう。

標的型攻撃メールの脅威を訓練を通して体感することで、**いかに危険が身近なものかという「気づき」を得る**と共に、**実際の攻撃メールを受け取った際の対応力を鍛える**ことができます。

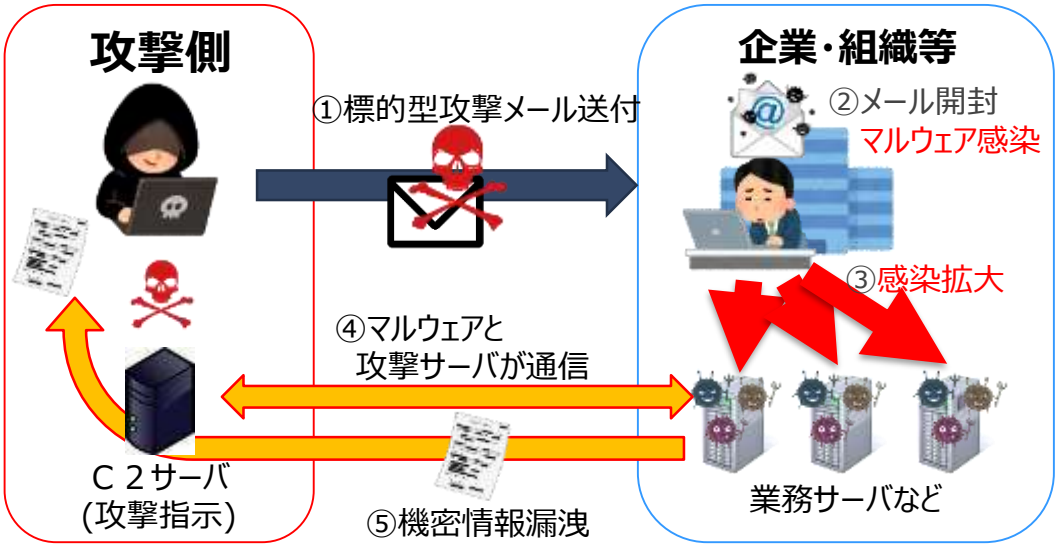
第３章　訓練の目的と効果

メール訓練の目的

標的型攻撃メールの訓練では、擬似的な攻撃メールを受信した従業員が不審な点に気づき、適切なインシデント対応を行えるか確認できます。同時に、標的型攻撃メールに対しての意識調査や教育も実施すると共に、結果情報を集計して自社の傾向を把握することができます。

メール訓練の効果

まずは、**従業員が悪意あるメールだと気づく力をつけること**が重要です。怪しいメールが届いても、URLにアクセスしたり、添付ファイルを実行することがなければ攻撃をかわすことができます。また、もし気づかずに悪意のある誘導にひっかかった場合でも、組織全体に被害が拡散しないよう、組織毎のセキュリティポリシーに則った適切な対処方法を取れることが重要です。



標的型攻撃メールによる情報漏えいの発生イメージ

第３章　訓練の目的と効果

訓練の目標設定

標的型攻撃メールの被害を最小化するためには**早期検知と的確な初動対応**が重要となります。しかし、いきなり全てを完璧にこなそうとしてもなかなか難しいものです。

訓練を行う際には、小さな目標からステップアップしていくことを意識して目標設定をしていきましょう。

Step.1：社員が攻撃メールの罠に掛かり難くする

①メールを怪しいと判断したら開封しない。
②開封して、怪しければ破棄する。

Step.2：組織感染の芽を早期に摘む

③怪しい添付ファイルや記載リンクをクリックせず、システム管理部門に報告する。システム管理部門は、組織内へ注意喚起し、報告を呼びかける。

Step.3：引っ掛かった社員を早期に発見し、初動対応をとる

④添付ファイルや記載リンクをクリックして問題があった際に、即座にシステム管理部門に報告。
⑤システム管理部門は、緊急措置、組織内へ注意喚起、報告の呼び掛け、状況を確認。

Step.4 ：組織として被害を低減、最終甚大被害を回避する

⑥当該端末のネットワークからの切り離し、ウイルスの駆除、組織内汚染状況の検査などを実施。その分析で得られた今後の攻撃を回避するための情報を、ネットワークサーバ等に設定する。

※参考：「IPA 注意喚起：攻撃の早期検知と的確な初動による深刻な被害からの回避を」
別紙「標的型攻撃メール訓練目的と活用～効果を上げる方法～」

訓練の実施方法

メール訓練の実施には大まかに３パターンの方法があります

① セキュリティコンサル会社に訓練の実施を委託する

② 自社内のシステムを活用して訓練を内製する

③ 訓練用のツールを利用する

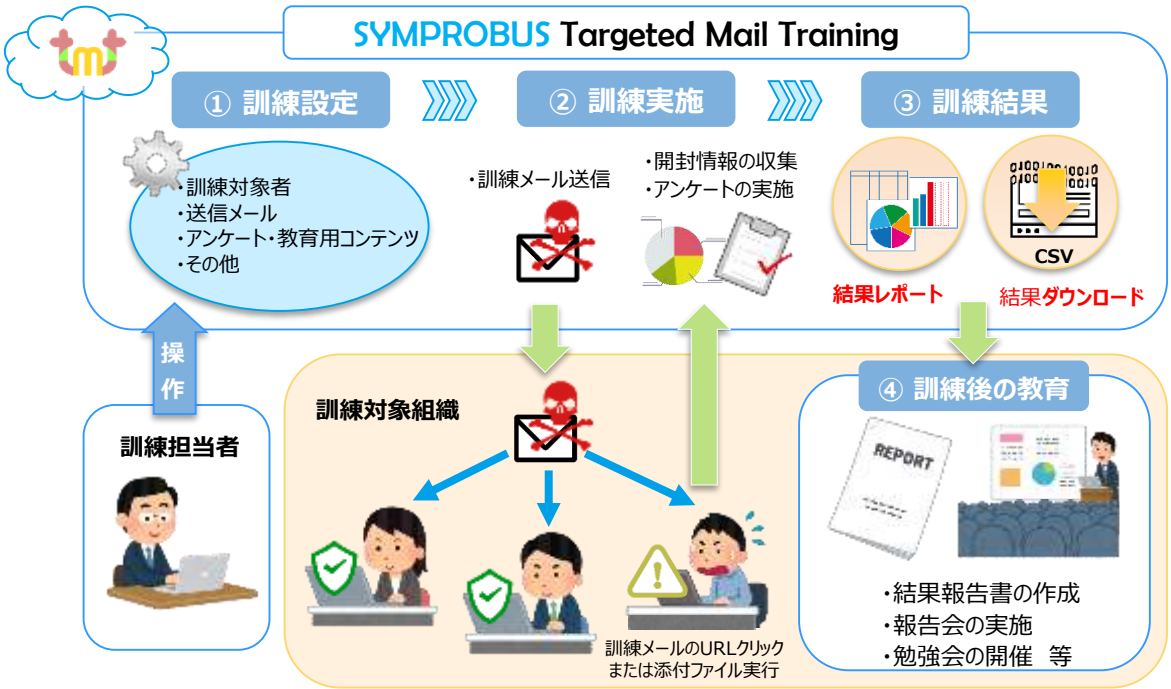
どの方法が最も適しているかは各法人様により異なりますが、それぞれ、以下のようなメリット、デメリットがあります。

	メリット	デメリット
①訓練委託型	• 専門の業者に全てお任せで訓練が可能	• 費用が高額（概ね数十～数百万円程度）
②内製型	• 費用がかからない • 任意のタイミングで自由に訓練可能	• 訓練の準備、実施に一定程度の専門知識が必要であり、時間と人手がかかる
③ツール利用	• 費用が①と比較して安価（概ね数万～数十万円程度） • 任意のタイミングで自由に訓練可能 • 専門知識がなくとも簡易に訓練が可能	• 訓練の準備、実施を自分たちで実施する必要がある

第３章　訓練の目的と効果

訓練はだれでも簡単に実施できる

アクモスでは、安価・簡易に訓練の実施が可能なクラウドサービスをご用意しております。設定は全てWebブラウザ上から行え、特別な知識なども必要ありません。



※サービスは複数あり、プランによって訓練イメージが異なります。上記は短期間に訓練をシンプルに実行できるTMT（Targeted Mail Training）を一例としたイメージ画像です。

1. 「いつ・だれに・どのようなメールを送るか」訓練内容の設定を行います。
2. 設定した内容をもとに、各訓練対象者に疑似標的型攻撃メールが送信されます。
3. 訓練の結果が自動集計され、開封率などの情報を確認します。

まずはアクモスの標的型攻撃メール訓練を無料で体験してみませんか？

アクモスでは、サービス内容をご納得のうえ導入いただけるように、**2ヶ月間無料で標的型攻撃メール訓練を体験できる「Freeプラン」**をご用意しています。実際のサービス体験で、訓練の大切さを実感いただけます。

Freeプランのご利用後も、ご継続いただけるよう、各プラン低コストの安心価格でご用意しております。ご興味がございましたら、お気軽にお問い合わせくださいませ。

Freeプランのお申込みはこちら！！
URL：https://tmt.cloudmenu.jp/freeplan

お問合せ先

アクモス株式会社　ネットワーク営業部

アクモスHP：https://www.acmos.co.jp/

製品サイト：https://tmt.cloudmenu.jp/

E-mail：network_sales@acmos.jp　TEL:03-5217-3155