

---

～ サービス業向け ～

# 標的型メール訓練サービスのご紹介

2019年2月版

株式会社 日立ソリューションズ・クリエイト

---

<はじめに>  
標的型メール攻撃による被害の事例

## 標的型メール攻撃とは

【 添付ファイルやリンク先をクリックさせて、ウイルス感染等を引き起こす攻撃 】

標的型攻撃と呼ばれるサイバー攻撃における、最も典型的な攻撃手法です。重要な情報を盗み出す手段として、標的のクライアントPCをマルウェアに感染させることを目的として、あらゆる騙しのテクニックを用いた攻撃メールを送信し攻撃してきます。攻撃メールに含まれる、リンク先URLあるいは添付ファイルを開封するとマルウェアに感染します。

## よくある誤解

⚠️ ウイルス対策ソフトを導入しているから大丈夫!?

この攻撃では、ゼロデイ攻撃というアプリケーションの未知の脆弱性を利用するケースや各種OSやソフトウェアの**パッチ未適用**といったスキを狙う攻撃であり、**ウイルス対策ソフトでは完全に防ぎきれません。**

⚠️ 感染してもすぐに気づく!?

目的の多くは、マルウェアに感染させてデータを破壊することではなく、組織内に深く潜行し、重要なデータを外部に持ち出すこと等です。多くの場合、**初期症状が表れず攻撃されても気づきません。**



### 事例

**業種：サービス業（旅行代理店）**

**被害：793万件の個人情報の流出**

**原因：標的型攻撃メールと気づかず、メールに添付されていた航空券のeチケットに偽装したファイルを開封したため、PCがウイルスに感染。**

**サーバへ感染が拡大し、情報が外部に流出した。**

### 本事例における標的型攻撃メールの特徴

**(1)明らかに被害にあった会社を狙っている**

- ・実際に業務に使用する、件名「航空券控え 添付のご連絡」、添付ファイル名「E-TKT控え」が使用されている。

**(2)手口が巧妙であり、気づきにくい**

- ・標的型メールの送信元は実際の取引先のアドレスで、本文に署名がある。

---

## 教育対策の重要性について

### 技術対策

標的型攻撃対策において、  
右記に代表される技術的対策は  
必須事項といえます。

しかしながら、技術的な対策には、  
必ず限界があるのが事実です。



最終的に、端末を扱うのも情報資産を扱うのも、従業員であり、ひとりの人間です。  
**「一人ひとりが、その端末を、情報資産を、セキュリティ意識をもって扱えるかどうか。」**  
技術的対策に依存しない、最後のセキュリティ対策が教育といえます。

### 教育対策の必要性

一人ひとりのセキュリティ意識を向上させることができる

- ① 感染リスク自体の低減 「マルウェアを開封実行させない」 = 開封率の低減
- ② 感染被害の極小化 「マルウェアを開封してもすぐに報告させる」 = 適切な初動対応の徹底

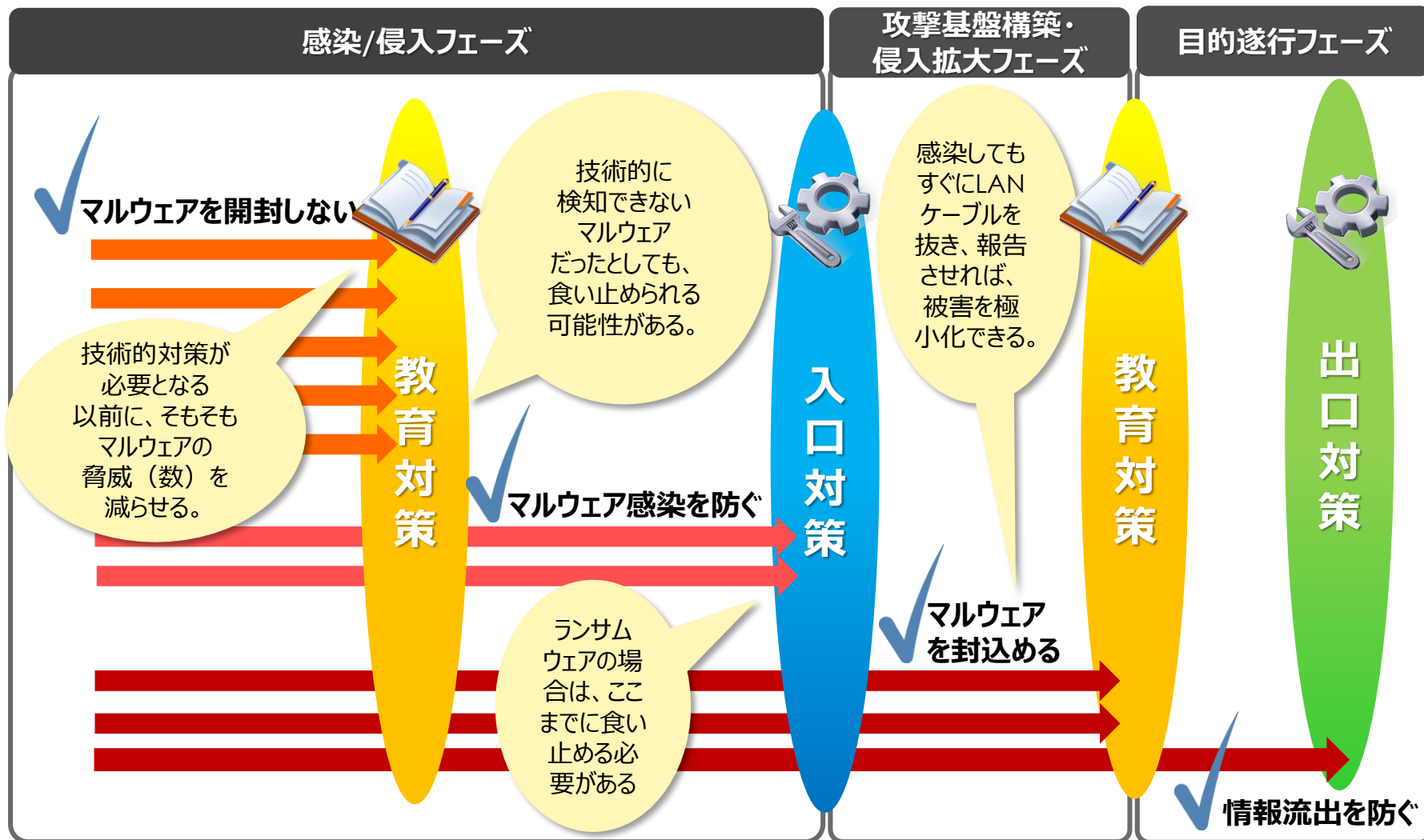
開封状況から、攻撃メールへの  
耐性を把握することも可能です。



## 2-2. 標的型メール攻撃への多層防御の概念

サイバーキルチェーンに基づく各フェーズでの対策による、多層防御が最も有効といえます。

※サイバーキルチェーンとは、標的型攻撃における攻撃者の一連の行動を軍事行動になぞらえて示したもので、2009年に米国の航空機、宇宙船の開発製造会社「ロッキードマーチン」で提唱されたもの（出典元：ZDNet Japan）



## 経済産業省/サイバーセキュリティ経営ガイドライン Ver 2.0での推奨事項

【指示5 サイバーセキュリティリスクに対応するための仕組みの構築】という項目における対策方法として下記の記載があります。

### 指示5 サイバーセキュリティリスクに対応するための仕組みの構築

サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる。

#### 【対策例】

- 従業員に対する教育を行い、適切な対応が行えるよう日頃から備える。
  - －従業員に対して、防御の基本となるソフトウェア更新の徹底、マルウェア対策ソフトの導入などによるマルウェア感染リスクの低減策等を実施させる。さらに定期的な対応状況の確認等を行う。
  - －従業員が不審なメールを受信した場合、当該情報を報告させるとともに全従業員に対して類似のメールを開かないよう注意喚起を行う。

※サイバーセキュリティ経営ガイドラインVer2.0より

#### 適切な初動対応の徹底

開封者によるシステム部門への開封報告まで実施することまでが、ガイドラインのなかで求められています。







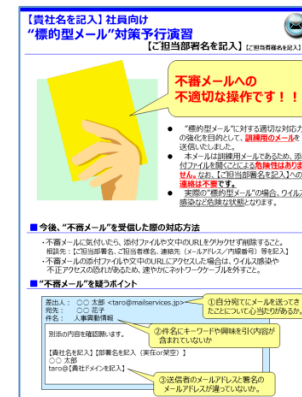
## サービス概要と実績

標的型攻撃メールを模擬した、【訓練メール】を対象者に送信します。従業員に対して、攻撃メールへの意識向上ならびに初動対応について、教育訓練することができます。

実際には無害の"訓練メール"をGSX(※)が対象者に送信します。訓練メールに含まれる、URLリンクあるいは添付ファイルを開封した対象者には、コンテンツが表示されるとともに、開封した日時等のアクセスログがGSX訓練サーバ側に取得されます。最後に訓練結果を集計し、ログデータ一式とともに報告します。



開封時にコンテンツを表示し、適切な教育研修を実施します。



\*白紙や任意のコンテンツ表示も可能


個人毎のアクセスログを取得し、報告します。



※標的型メール訓練サービスは、グローバルセキュリティエキスパート株式会社（本書ではGSXと略します）のサービスです。

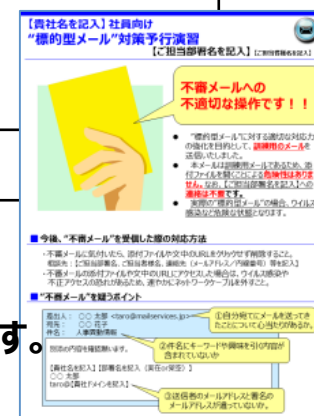
## 3-2. 訓練メールのサンプル

自由に内容をカスタマイズ可能です。(テンプレートも多数ご提供しています。)

項目名	内容
送信元メールアドレス	Abcsys-tanaka@xxxxxxxx.jp
件名	【秘】前回議事録の送付
本文	<p>平素大変お世話になっております、ABCシステム田中です。</p> <p>前回お打ち合わせの際の議事録について、添付ファイルにて送付させていただきます。</p> <p>お打ち合わせの際の内容通り、一般リリース前の情報が記載されておりますので、お取扱いにはご留意を御願い申し上げます。</p> <p>-----</p> <p>ABCシステム 田中</p>
添付ファイル名 	議事録_ABCsys_0110.docx



この添付ファイルを開くと、  
開封時コンテンツが表示され、  
同時にアクセスログが取得されます。



1

**GSX独自開発  
システムによる、  
柔軟なカスタマイズ対応**



システムは全てGSX  
内で独自に開発して  
います。訓練メールの  
本文、送信元、開封  
時コンテンツ、さらには  
訓練メールの送信間  
隔などについても、柔  
軟にカスタマイズする  
ことが可能です。

2

**訓練サービス自体への  
効果的なセキュリティ対策**



お客様メールアドレス  
情報の取扱や、訓練  
メールの第三者への  
転送対策、訓練用  
サーバへの不正アクセ  
ス対策など、万全のセ  
キュリティ対策を実施  
したうえで当該サービ  
スを提供しています。

3

**初めての訓練でも、  
手間を掛けずに、  
効果の高い訓練を実現  
するサポートコンテンツ**



初めてのお客様でも、  
他社での豊富な実施  
実績をご紹介できま  
す。また、訓練メール  
テンプレート・社内通  
知メールテンプレート・  
ヘルプデスクの対応マ  
ニュアル等についても  
準備しています。

4

**継続的な訓練では、  
開封時の初動対応訓練  
が可能(オプション)**



継続的に訓練を実施  
されるお客様には、開  
封時の初動対応まで  
を訓練できる、分散  
型送信や開封時通  
知メールなどのオプショ  
ンを準備しています。

## 実施実績 抜粋

業種業態	規模	備考
製造業A	110,000名	実施後、グループ会社各社へも展開。継続的に訓練を実施中。
製造業B	5,000名	グループ会社120社で同時実施。
サービス業C	2,000名	全社員に対してセキュリティ強化月間の中で実施。
官公庁D	1,000名	情報セキュリティ監査業務の一部として実施。
金融機関E	1,000名	実際のマルウェア感染時のユーザー対応の訓練・評価のため実施。
システム開発F	1,000名	全社員に対し、セキュリティ対策としてのリテラシー向上を目的に実施。
製造業G	800名	同業他社の実施を知り、必要性を認識し、全社で実施。
通信業H	500名	全社実施前、事業部門を選択してパイロット的に実施。
製造業I	500名	防衛関連部門および役職者に対して実施。


**【2017年度実績】**  
**対象:約400社、約111万アドレス**  
**(累計約333万アドレス)**

## 導入事例



## 新聞・雑誌掲載実績

- 2013年12月12日号 『日経コンピュータ』  
**特集**  
 超「Excel」ビックデータ活用を加速する新世代帳票  
**特集**  
 尖った事業は顧客と創るITベンダーが掛ける異業種コラボ  
**クローズアップ**  
 偽のウイルスで対策意識を喚起「標的型攻撃訓練」を検証する
- 2014年8月20日 『日本経済新聞』  
 「何気なく開封…感染」



## 標準サービスパックおよびご提供フロー

# 4-1.標準サービスパック

下記の3項目を選択頂くことで、サービスパック費用が決まります。



## 標準サービスパック3種

STEP1

### プレミアム

<実施内容>

訓練メール送信+WEBアンケート実施

<成果物>

ログデータ&報告書(アンケート分析含む)

### スタンダード

<実施内容>

訓練メール送信

<成果物>

ログデータ&報告書

### エクスプレス

<実施内容>

訓練メール送信

<成果物>

ログデータ



## 訓練メール送信回数(訓練回数)

STEP2

### 1回訓練パック

1回訓練実施

### 2回訓練パック

2回訓練実施 ※1回め終了から2週間以内を前提



## 対象メールアドレス数

STEP3

500アドレス未満一式

500-1,000アドレス一式

1,001-2,000アドレス一式

以降1,000アドレス毎一式

※アドレスレンジ毎での一括費用となります。(アドレス単位ではありません。)

### 標準サービスパックに含まれるもの

#### メール訓練全般のサポート

1回の打ち合わせ(以降は電話・メールにより対応) ※都内近郊を除き別途旅費交通費

#### 訓練メールの送信&カスタマイズ

訓練メール種類は、1回の訓練につき最大3パターンを作成可能です。  
(2回訓練パックの場合、3パターン×2回=最大6パターン)  
※テンプレートご提供のうえ、お客様にて訓練メール内容を作成いただきます。

訓練メールの送信は、5,000アドレス以下については、1営業日(平日営業時間内)に一括で順次送信します。(一斉送信ではありません。)  
※送信日の分割(追加)については、別途費用を頂戴します。

#### 開封時コンテンツの表示&カスタマイズ

開封時コンテンツは、1回の訓練につき1パターンのみを作成可能です。  
※テンプレートご提供のうえ、コンテンツを作成いただきます。

#### 各種サポートコンテンツの提供

各種テンプレートを提供可能です。

#### 教育資料の提供

メール訓練の事前事後等に活用いただける教育資料(PPTデータ)を提供します。

### その他、前提条件

- お申込み並びにご契約にあたっては、サービス利用規約への同意が必要となります。
- 子会社を含めた訓練の実施など対象のメールアドレスが異なる場合、最大4ドメインまでを標準サービス費用内にて実施可能です。
- メールサーバや各種セキュリティ機器が訓練メールを誤検知しブロックしないよう、ホワイトリスト登録等の設定変更が必要です。
- 事前テスト完了後の内容変更およびスケジュール変更は原則として対応しません。
- 開封ログの集計分析については、弊社メール訓練システムで取得したもののみを対象とします。  
(お客様で取得される、ネットワーク機器等で取得したログは対象としません。)

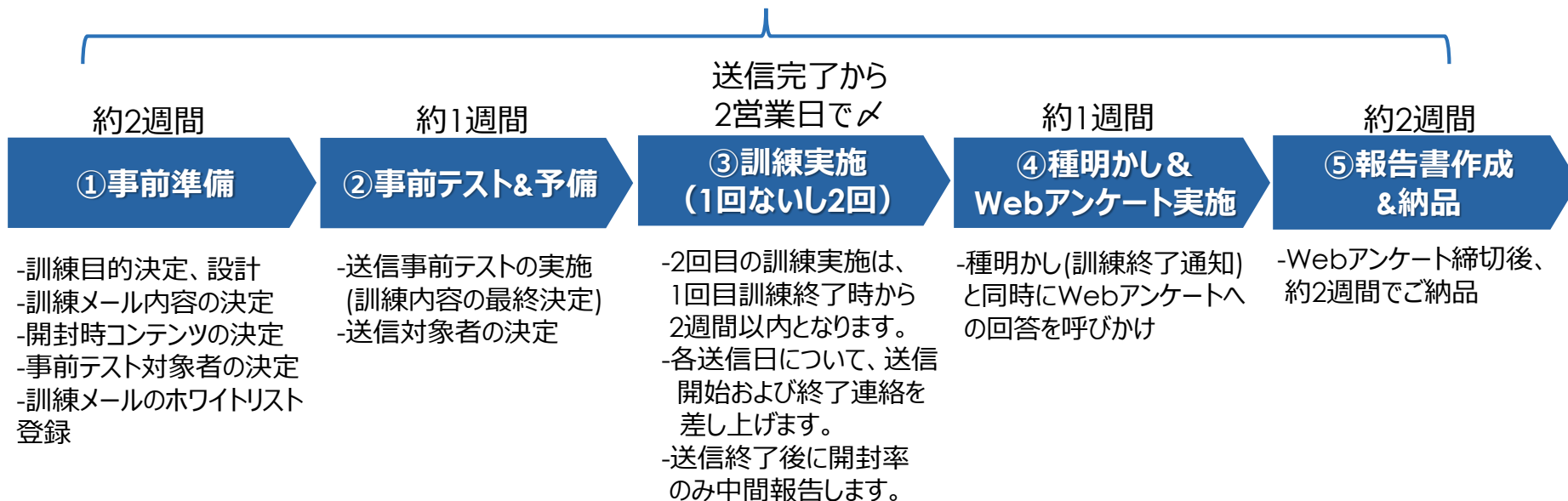


## 4-3.ご提供フロー/プレミアムパックの場合

### プレミアムパック の場合

プレミアムパック以外では③訓練実施を送信完了後=④種明かしから、約2週間にて報告書納品となります。

契約から約3ヶ月での納品となります。(調整により、短期間での対応も可能)



各段階にてGSXコンサルタントが、アドバイザーおよびサポートします。  
(事前準備段階で1回お打合わせを実施させていただき、その後は適宜メール・お電話にてサポートします。)



---

## サービス詳細仕様

## 自由に内容をカスタマイズ可能です。(テンプレートも多数提供しています。)

※標準パックのなかで、訓練メールの種類は、1回の訓練につき最大3パターンを作成可能です。(2回訓練パックの場合、3パターン×2回=最大6パターン) 各訓練メールについて、下記項目をカスタマイズ可能です。

※テンプレート提供のうえ、お客様にて訓練メール内容を作成いただきます。

項目名	内容
送信元メールアドレス	<p>下記2種類のドメインが選択可能です。</p> <ul style="list-style-type: none"> <li>- GSX訓練専用ドメイン 【mail-system-manager.net】【global-quality-management.net】【national-university.net】【office-all.net】【safegovernment.net】【tokyo-central-bank.net】【anshin-service.net】【cat-site.net】【shinagawa-logi-co.jp】【sunrightwest.com】【techsupport-co.jp】【fsa-go.jp】</li> <li>- フリーメール・ドメインの偽装 yahooもしくはgmail</li> </ul>
件名&本文	<p>&lt;件名&gt;自由にカスタマイズ可能です。</p> <p>&lt;宛名&gt;対象者毎に個別に設定が可能です。対象者の社名、部署、お名前を個別に記載することができます。</p> <p>&lt;本文&gt;自由にカスタマイズ可能です。(サンプルを次頁に記載しております。)</p>
実施方式 (開封と見なすキー)	<p>下記2種類が選択可能です。</p> <ul style="list-style-type: none"> <li>- URLリンク方式 (GSX訓練専用ドメイン) <ul style="list-style-type: none"> <li>・リンクをクリック (開封) すると、教育コンテンツWEBサイトにアクセスします。</li> <li>・使用URL <code>http://*.mail-system-manager.net/*</code> (GSX訓練専用ドメインから選択可能)</li> </ul> </li> <li>- 添付ファイル方式 <ul style="list-style-type: none"> <li>・.docx形式 (開封すると、ワード内に教育コンテンツが自動ダウンロード表示されます。)</li> <li>・.pdf形式 (開封すると、ブラウザ内に教育コンテンツが自動ダウンロード表示されます。)</li> <li>・.exe形式 (開封すると、ブラウザに教育コンテンツが表示されます。)</li> <li>・.lnk (ショートカット) 形式 (開封すると、教育コンテンツWEBサイトにアクセスします。)</li> </ul> </li> </ul> <p>※それぞれ、ZIP化 (パスワード有or無) が可能。パスワードは、訓練メール本文に同時に記載。</p> <p>#原則として、教育コンテンツは、お客様のグローバル IPアドレス以外からのアクセスを制限して実施します。 (添付ファイル方式の場合、開封しても白紙表示もしくは任意のコンテンツを表示します。)</p> <p>訓練メールが外部に転送された場合でもそのコンテンツ内容が第三者に知られない仕様になっています。</p>

## 5-2. 訓練メール仕様: サンプル

訓練メール内容については、豊富なテンプレートを準備しておりますが、内容のカスタマイズ等は自由に実施可能です。

※以下は、テンプレートの一部抜粋です。

	内容	送信元アドレス	件名	本文	URL/添付ファイル
業務連絡系	議事録の送付	田中 <a href="mailto:tanaka@office-all.net">tanaka@office-all.net</a>	【至急】 ご確認のお願い	参加者各位 議事録を添付しますので、ご確認下さい。パスワードは1234です。	議事録.zip →議事録.docx (解凍後)
	休暇案内	人事部・佐藤 <a href="mailto:jinji_satou@gmail.com">jinji_satou@gmail.com</a>	【重要】 夏季休暇に関する連絡	社員各位 今年度の夏季休暇を取得するにあたり、注意事項をご確認下さい。	注意事項： <a href="http://w2.mailservices.jp/a.php?...">http://w2.mailservices.jp/a.php?...</a>
注意喚起系	情報セキュリティ	情報セキュリティ室 <a href="mailto:security@cat-site.net">security@cat-site.net</a>	【至急】 アップデートのお願い	社内標準のソフトウェアに脆弱性が発見されましたので、添付のファイルを実行して下さい。	update.exe
	最近の話題	政府広報 <a href="mailto:tokyo2020@yahoo.co.jp">tokyo2020@yahoo.co.jp</a>	東京オリンピック開催に伴う要請	開催に伴い国際オリンピック協会より以下の要請が出されておりますので、ご確認ください。	国際オリンピック協会からの要請： <a href="http://w3.mailservices.jp/a.php?...">http://w3.mailservices.jp/a.php?...</a>
セールス系	自社製品のお問合せ	顧客・鈴木様 <a href="mailto:suzuki@sunrightwest.com">suzuki@sunrightwest.com</a>	貴社製品に関するお問合せ	〇〇部 ××様 貴社製品の検討にあたり、質問を添付しますので、ご確認ください。	質問事項.pdf
	セミナー開催案内	取引先・XXソフト <a href="mailto:xx-soft@yahoo.co.jp">xx-soft@yahoo.co.jp</a>	新製品のご紹介セミナーについて	〇〇様、いつもお世話になっております。新製品のセミナーを開催しますので、是非ご参加下さい。	セミナー開催のご案内： <a href="http://xxsoft.com/a.php?...">http://xxsoft.com/a.php?...</a>

訓練の目的・お客様の業態に応じ様々な内容を選択いただけます。  
全く新しい内容をカスタマイズして作ることもできます。

差出人は自由に設定できます。メールアドレスは当社指定及びGmailもしくはYahooのアドレスを使用できます。

本文内に訓練対象者の名前や部署名を挿入して、より関心を惹きつけることができます。

添付ファイルはdocx, pdf, exe, ショートカット(lnk)形式が使用できます。(ZIP圧縮&パスワード設定も可)URLリンクのドメイン名は弊社メール訓練専用ドメインが利用可能。

自由に内容をカスタマイズ可能です。(テンプレートもご提供しています。)

※標準パックのなかで、1回の訓練につき1パターンのみ作成可能です。

※テンプレート提供のうえ、お客様にて訓練メール内容を作成いただけます。(PPTデータとなります。)

## 教育コンテンツへの記載内容例

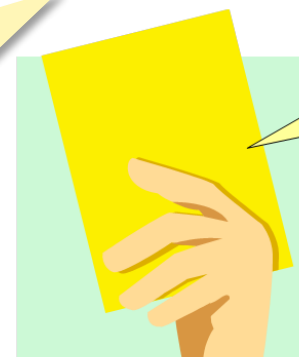
- ✓ 訓練であり、実際には無害である旨の明記
- ✓ 開封した方への業務指示  
(LANケーブルを抜き、システム部門へ報告する等)
- ✓ 本訓練メールを怪しいと見分ける為のポイント
- ✓ 社内の教育コンテンツの保管場所など

継続的な訓練の結果、開封率を一定レベルより低減した後は、  
初動対応訓練を含めたメール訓練実施を推奨します。

(これにあわせた、開封時コンテンツのアレンジ、オプションの活用  
を提案します。\*P30以降に記載)

【貴社名を記入】社員向け  
“標的型メール”対策予行演習

【ご担当部署名を記入】 【ご担当者様名を記入】



不審メールへの  
不適切な操作です！！

- “標的型メール”に対する適切な対応力の強化を目的として、**訓練用のメール**を送信いたしました。
- 本メールは訓練用メールであるため、添付ファイルを開くことによる**危険性はありませ**ん。なお、【ご担当部署名を記入】への**連絡は不要**です。
- 実際の“標的型メール”の場合、ウイルス感染など危険な状態となります。

### ■ 今後、“不審メール”を受信した際の対応方法

- ・不審メールに気付いたら、添付ファイルや文中のURLをクリックせず削除すること。  
相談先：【ご担当部署名、ご担当者様名、連絡先（メールアドレス/内線番号）等】を記入
- ・不審メールの添付ファイルや文中のURLにアクセスした場合は、ウイルス感染や不正アクセスの恐れがあるため、速やかにネットワークケーブルを外すこと。

### ■ “不審メール”を疑うポイント

差出人： ○○ 太郎 <taro@mailservices.jp>

宛先： ○○ 花子

件名： 人事異動情報

①自分宛てにメールを送ってきたことについて心当たりがあるか。

別添の内容を確認願います。

②件名にキーワードや興味を引く内容が含まれていないか

【貴社名を記入】【部署名を記入（実在or架空）】

○○ 太郎

taro@【貴社ドメインを記入】

③送信者のメールアドレスと署名のメールアドレスが違っていないか。

初動対応を徹底させるため、開封時コンテンツに、適切な対応を取る指示を記載します。

## 実施するうえでのポイント

### ヘルプデスクへのインシデント報告までの訓練を前提

実際のマルウェア感染時と同様に、インシデント報告をさせることを主眼とした訓練となります。

初動対応を徹底させることが、感染被害の極小化につながります。

## 留意点

- コンテンツの指示に従い、開封した一般ユーザからの開封報告があります。これに対応できるだけのヘルプデスクのリソースが訓練実施時に必要となります。

⇒ リソースに懸念がある場合、継続的な訓練を経て、開封率を一定レベル以下まで低減した後、初動対応に重点を置いた訓練にシフトすることを推奨します。

### XXXXXXXX株式会社 社員向け “標的型メール”対策訓練

【情報システム部】【担当者：碓、綾波】

不審なメールへの不適切な操作です！！



- “標的型メール”に対する適切な対応力の強化を目的として、訓練用のメールを送信いたしました。
- 今回を含め、社内ルールに準拠した行動を実施願います。(LAN抜線および情報システム部への即時報告が必要です)
- なお、本メールは訓練用メールであるため、添付ファイルやURLをクリックすることによる危険性はありません。

## ランサムウェアを模倣した開封コンテンツにもアレンジが可能です。

**記載例**  
**金銭要求画面を表示(訓練である旨は非記載)**

### 実施するうえでのポイント

#### ヘルプデスクへのインシデント報告までの訓練を前提

実際のランサムウェア感染時を体感して頂き、インシデント報告をさせることを主眼とした訓練となります。

### 留意点

- 一般ユーザから問合せ(インシデント報告)が殺到する可能性があります。(セキュリティ意識のうえで正しい反応です。)
- 実際に暗号化はされません。
- マルウェアの場合は、ランサムウェアの様に感染しても目に見える表示・被害が無いことも、あわせて教育説明の必要があります。

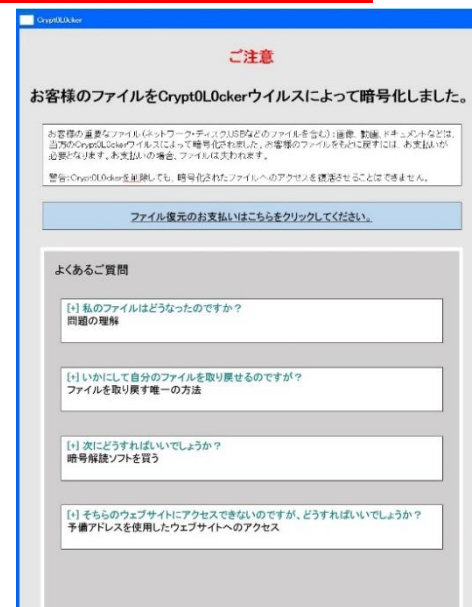
### 警告!

あなたのファイルの一部は暗号化されました。  
ファイルを元に戻すための、秘密鍵(ファイルを復元化するために必要)を手に入れるには5万円を支払う必要があります。

ファイルを使えるようにするためには、ウイルス対策ソフトや専門家の対応も役に立ちません。必ず期限までお支払いください。

期限までにお支払いが確認できない場合には、暗号化されるファイルが増加し、お支払いいただく金額も増額します。

支払い方法・期限については24時間以内に連絡いたします。



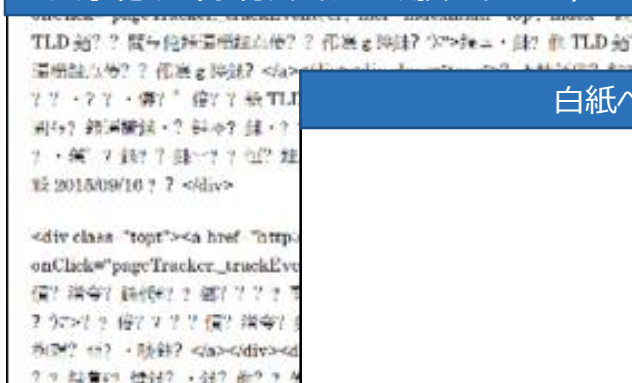
個人の見破る力や社内ルールの定着度を測る開封時コンテンツにすることも可能です。

## 実施するうえでのポイント

### ヘルプデスクへのインシデント報告までの訓練を前提

あえて開封時コンテンツは訓練とは明示せず、「不信感」を表現するもの(文字化けや白紙ページ)とすることで、個人の不審メールに対する見破る力や、社内ルールの定着度を測ることを目的とした訓練となります。

文字化け (添付ファイルの破損をイメージ)



白紙ページ



## 留意点

- コンテンツの指示に従い、開封した一般ユーザからの開封報告があります。これに対応できるだけのヘルプデスクのリソースが訓練実施時に必要となります。
- ⇒ リソースに懸念がある場合、継続的な訓練を経て、開封率を一定レベル以下まで低減した後、初動対応に重点を置いた訓練にシフトすることを推奨します。



本文中URLのクリックの遷移先を、社内イントラや外部サイトにすることが可能です。

## 実施するうえでのポイント

### 不審メールへの耐性を正確に確認

開封時コンテンツを表示せず、正規のWebサイトが表示されるため、メール訓練と気づきにくくなります。

HTML形式のメール本文を使い、見た目のURLを偽装することも可能です。

項目	内容
件名	【重要】新種ウイルスへの対応について
本文	各位  極めて深刻な新種のウイルスが多数確認されています。感染した場合、PCおよびファイルサーバ内の全ての情報が漏えいする可能性があります。緊急対応が必要になりますので、URLをご確認ください。  ▼ウイルス情報▼ <a href="https://www.ipa.go.jp/security/vuln/">https://www.ipa.go.jp/security/vuln/</a>

訓練システム



開封記録

クリック後に遷移

## 留意点

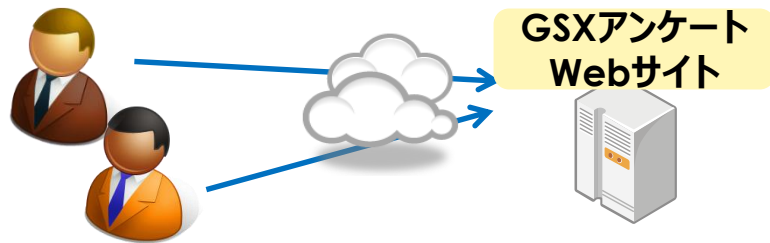
- URLリンク形式のみ実施可能です。
- ブラウザのリダイレクト機能が有効か確認が必要です。
- クリック後のサイトは自由に設定可能です。



# 5-4. Webアンケート仕様(プレミアムのみ)

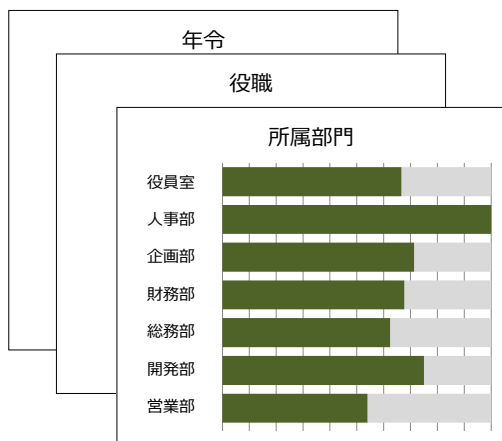
## 開封者だけでなく、全対象者にアンケートを実施します

開封者だけでなく全対象者様に向けWebアンケートを実施します。開封/非開封の理由、攻撃メール受信時/開封時の対応方法について浸透状況を把握できるため、標的型攻撃メールに対する今後の課題を整理できます。

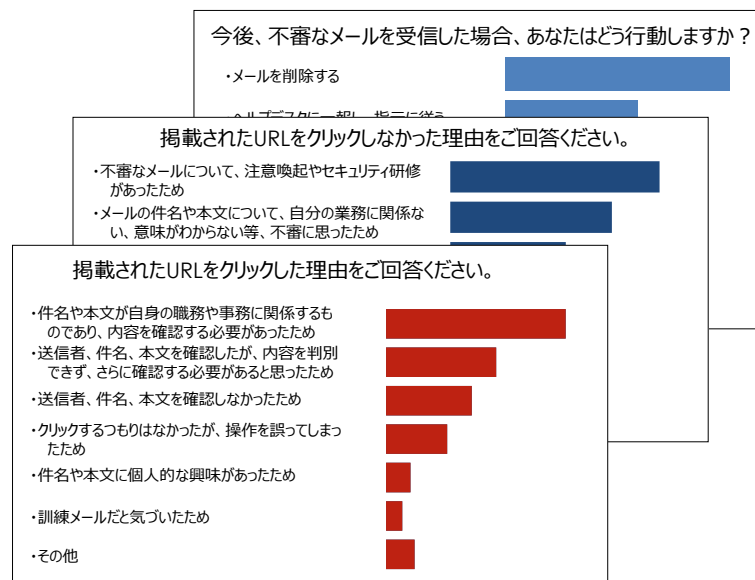
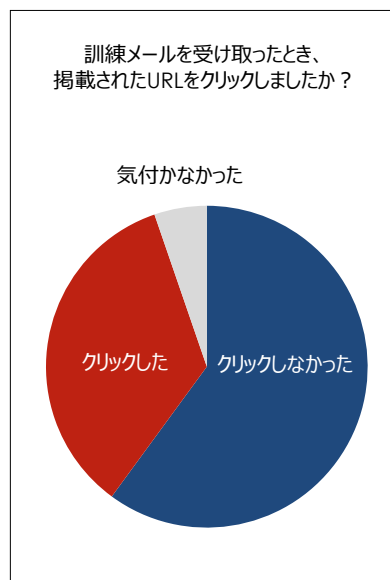


- ※標準パックの中で1種類が作成可能です。
- ※設問項目は、選択式・所定12項目となります。(回答者属性のカスタマイズを除き、設問変更には別途費用を頂戴します。)
- ※その他、ご意見等をお聞きする自由回答項目のON/OFFが可能です。(自由回答は報告書において分析非実施となります)
- ※アンケート対象者の個人特定は行わず、属性だけを任意にお聞きして集計を実施します。

【回答者属性】



【回答結果】

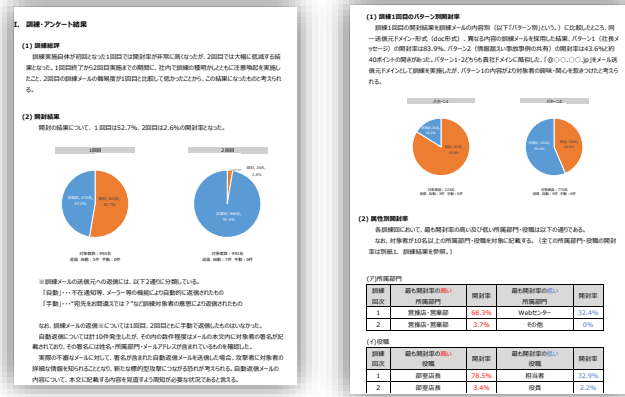


# 5-5.報告書イメージ(1)

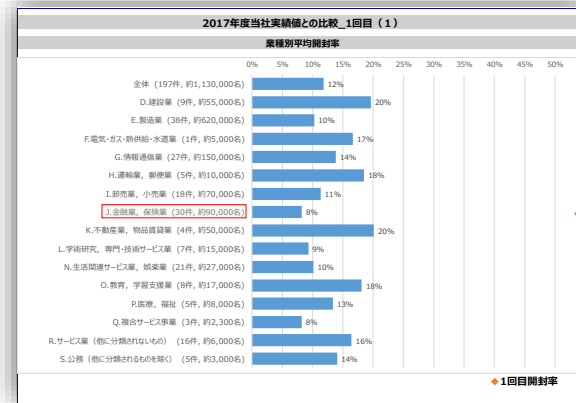
報告書には全体の集計結果等を取りまとめて記載します。またエクセルデータにて、対象者毎のアクセスログデータをご納品させていただきます。また、ご要望に応じて、同業種同業態との開封率の比較データなども報告書に記載可能です。

## 報告書イメージ 開封結果

### 開封結果 (全体開封率)

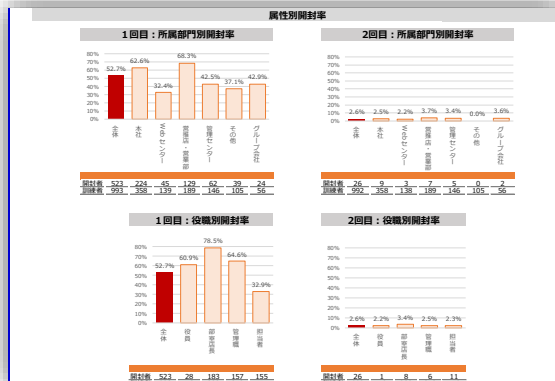


### 他社実績による開封データ比較

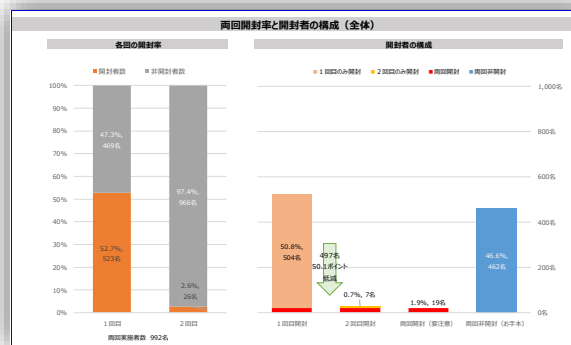


## 報告書イメージ 開封率

### 所属別、役職別開封率



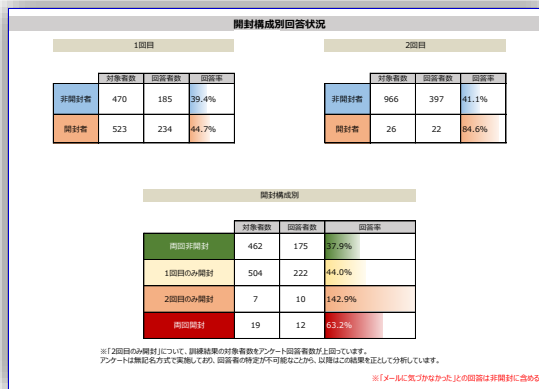
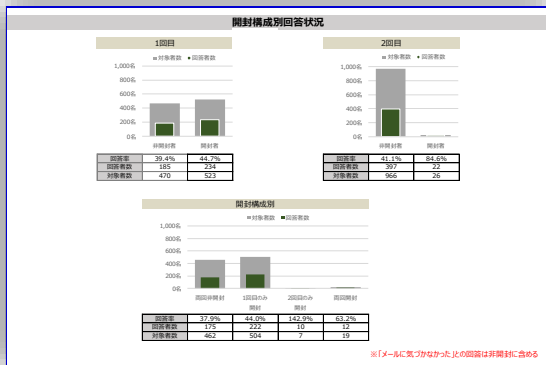
### 開封低減 変化要因分析



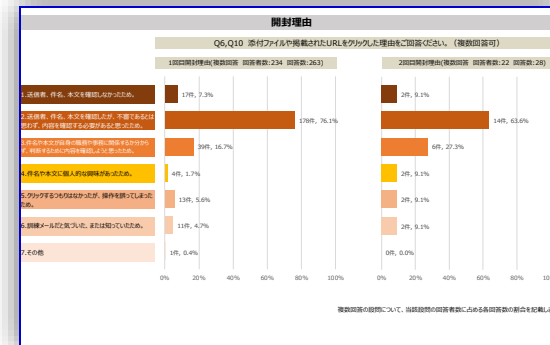
部門	開封者数	1回目開封率		2回目開封率	
		開封率	開封件数	開封率	開封件数
営業	922	67.3%	620	2.6%	24
開発	250	49.9%	125	97.4%	225
総務	138	53.7%	74	0.0%	0
人事	189	62.6%	118	2.5%	5
企画	144	68.3%	99	2.2%	3
品質	103	37.1%	38	0.0%	0
サポート	193	42.9%	83	3.6%	2

## 報告書イメージ アンケート結果

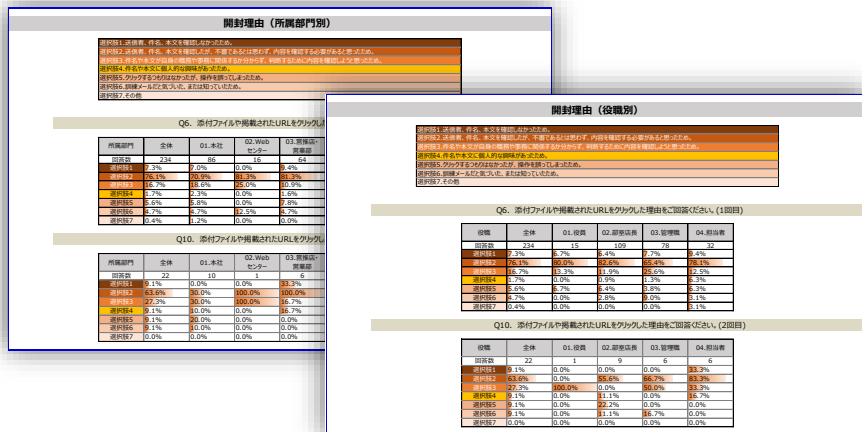
### 回答者の開封状況



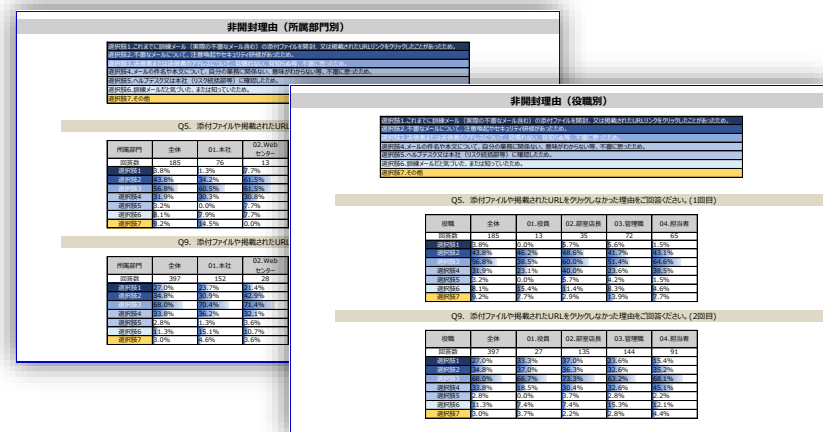
### 訓練メール開封理由



### 開封理由/部門別/役職別



### 非開封理由/部門別/役職別



---

## サービス詳細仕様 – サポートコンテンツ

## 訓練の事前通知をする際に

訓練を事前通知する際のメールテンプレートを提供可能です。

《標題》  
標的型攻撃メール訓練の実施について

《本文》  
各位

## 事前通知メール テンプレート

以下の通り、標的型攻撃メール対応訓練を実施します。

1. 目的

- 「業務遂行上、メール開封は必要である」ことを前提に、当社が保有し、次のことを目指し、体験型学習と意識の確認・向上の場とし
- 訓練対象者が不審なメールをできるだけ開封しないこと。
  - 訓練対象者が不審なメールを開封した場合、組織が影響を極小に抑えること。

2. 実施期間

平成25年XX月XX日 (X) からXX月XX 日 (X) の間

## 事前通知の実施状況

事前通知の有無について、過去のお客様実績では下記3パターンに大別されます。それぞれ一長一短がありますが、お客様の社内状況などを材料にご判断されるケースがほとんどです。

### 対象者への事前通知を実施されるケース

1 **注意喚起**  
(不審メールが急増している旨などの注意喚起のみ)

2 **事前通知**  
(訓練実施の旨、実施期間などの具体的な通知)

3 **抜き打ちで実施されるケース (対象者への事前通知をしないケース)**

“教育資料”の活用が可能(次頁)

70%程度

“事前通知メール”のテンプレート活用が可能

30%程度

事前通知をするのであれば、初動対応のルールまでも事前に説明するとベター。

# 6-2. サポートコンテンツ(2)

## 訓練の事前教育や事後教育をする際に

訓練の事前教育あるいは事後教育用に活用いただける資料を提供します。ユーザー向けに平易な言葉で記載しています。PPT形式データで提供しますので、社内ルールや初動対応ルールを追記して活用いただくことが可能です。

## 教育資料

### 不審なメールの取扱方法について

#### 1 標的型メールとは？ ～標的型攻撃（サイバー攻撃）の発端～

標的型攻撃と呼ばれる、特定の組織から個人情報を取得し、機密情報の漏洩を目的とするサイバー攻撃の発端です。

この攻撃は標的型メールと呼ばれる、添付ファイルやURLやマルウェアを含むメール、メール本文に不正なURLを含むメールを送りつけて、組織内のPCをマルウェアで感染させる攻撃です。

標的型攻撃の発端として、標的型メールが送られてくる。不審なメールで送られてくる添付ファイルやURLをクリックしないことが重要なポイントです。実際に送られてくるメールでメール送信者が不審な場合は、送付先または送信元のドメイン名を確認してください。

- 【標的型メールの例】
- ・ 迷惑メールの迷惑文を読んだ、メール送信人
  - ・ メール送信者名が不明なメールが届いたら、メール本文
  - ・ 添付ファイルのファイル名やURLを確認し、疑わしいファイルの宛先は異なるファイル
  - ・ URLをクリックして、ファイルを開かないこと。不正なファイルは実行しないこと。

本資料では、標的型メールが発せられる不審なメールを見つけたポイントで、不審なメールの取扱方法を記載しています。

資料が読めるようにするために、図表、写真、イラスト、動画の挿入を行っています。

資料が読めるようにするために、図表、写真、イラスト、動画の挿入を行っています。

#### 6 不審なメールの見分ける

本資料は、迷惑メールの個人情報を取得し、機密情報の漏洩を目的とするサイバー攻撃の発端です。メール本文に不正なURLを含むメールを送りつけて、組織内のPCをマルウェアで感染させる攻撃です。

この攻撃は標的型メールと呼ばれる、添付ファイルやURLやマルウェアを含むメール、メール本文に不正なURLを含むメールを送りつけて、組織内のPCをマルウェアで感染させる攻撃です。

標的型攻撃の発端として、標的型メールが送られてくる。不審なメールで送られてくる添付ファイルやURLをクリックしないことが重要なポイントです。

特にメールアドレスのドメイン名を確認することは、ポイントです。

#### 6 不審なメールの見分ける (続き)

メールの送信人から不審なメールがあることを見分けるためには、以下のようなポイントを確認してください。

- 送信元: 送信元が不明なメールが届いたら、メール本文
- 送信元: 送信元が不明なメールが届いたら、メール本文
- 送信元: 送信元が不明なメールが届いたら、メール本文
- 送信元: 送信元が不明なメールが届いたら、メール本文
- 送信元: 送信元が不明なメールが届いたら、メール本文
- 送信元: 送信元が不明なメールが届いたら、メール本文

メールの添付ファイルやURLから不審なメールがあることを見分けるには、以下のポイントを確認してください。

- 添付ファイルの拡張子が、自分が開けない形式や実行ファイル(実行可能ファイル)である
- あるいはURL(ドメイン名)が、目撃していないURLやメール本文と異なるURL(社内メールの場合はドメイン名のURL)になっている、実際のリンク先と異なっている

- 件名や本文に「緊急」「重要」と記載されている、メールの本文を参照した上で、添付ファイルやURLをクリックしないこと。
- 件名や本文に「緊急」「重要」と記載されている、メールの本文を参照した上で、添付ファイルやURLをクリックしないこと。

#### 2 不審なメールの添付ファイルやURLをクリックする？

標的型メールが送られてくる。不審なメールで送られてくる添付ファイルやURLをクリックしないことが重要なポイントです。

PCがウイルスやマルウェアに感染して、PCが遠隔操作されてしまい、新たなウイルス感染、組織内のウイルス感染、機密情報の流出などの危険性、組織のITシステムの破壊、といった大きな被害が発生する。組織全体のセキュリティ上、危険な行為であると認識してください。

日本の中央官庁や政府関係機関、社会インフラ関連企業を狙ったサイバー攻撃、TV番組などへの不正アクセス、個人情報などへの不正アクセスなど、近年では標的型攻撃によるものが数多く報道されています。

近年の標的型メールによるサイバー攻撃事例		
2014年5月 日本経済新聞社への不正アクセス	日本経済新聞社への不正アクセス	日本経済新聞社への不正アクセス
2015年6月 日本年金機構への不正アクセス	日本年金機構への不正アクセス	日本年金機構への不正アクセス
2016年3月 ITRグループへの不正アクセス	ITRグループへの不正アクセス	ITRグループへの不正アクセス

また悪意では組織内のPC内のデータを悪用しない、それを見逃さないことが重要です。

資料が読めるようにするために、図表、写真、イラスト、動画の挿入を行っています。

#### 3 ウイルス対策ソフトを導入しているから大丈夫？

ウイルス対策ソフトは有用ですが、ウイルス対策ソフトは万能ではありません。標的型攻撃は、標的型メールの添付ファイルやURLをクリックして、組織内のPCをマルウェアで感染させる攻撃です。

また、同一メールアドレスから送られてくる、添付ファイルやURLやマルウェアを含むメール、メール本文に不正なURLを含むメールを送りつけて、組織内のPCをマルウェアで感染させる攻撃です。

この攻撃は標的型メールと呼ばれる、添付ファイルやURLやマルウェアを含むメール、メール本文に不正なURLを含むメールを送りつけて、組織内のPCをマルウェアで感染させる攻撃です。

#### 4 誰が狙われてメールを送りつけられる？

- ・ 攻撃対象の組織内の全ての方が狙われています。
- ・ 標的型攻撃は、標的型メールを送りつけて、組織内のPCをマルウェアで感染させる攻撃です。
- ・ 攻撃対象の組織内だけでなく、関係組織や取引先も狙われています。

標的型攻撃は、標的型メールを送りつけて、組織内のPCをマルウェアで感染させる攻撃です。

資料が読めるようにするために、図表、写真、イラスト、動画の挿入を行っています。

#### 5 実際どんなメールが送られてくる？

標的型攻撃の発端として、標的型メールが送られてくる。不審なメールで送られてくる添付ファイルやURLをクリックしないことが重要なポイントです。

この攻撃は標的型メールと呼ばれる、添付ファイルやURLやマルウェアを含むメール、メール本文に不正なURLを含むメールを送りつけて、組織内のPCをマルウェアで感染させる攻撃です。

また悪意では組織内のPC内のデータを悪用しない、それを見逃さないことが重要です。

この攻撃は標的型メールと呼ばれる、添付ファイルやURLやマルウェアを含むメール、メール本文に不正なURLを含むメールを送りつけて、組織内のPCをマルウェアで感染させる攻撃です。

#### 10 ランサムウェア (身代金ウイルス) の注意

ランサムウェアは、金銭を要求する身代金型不正プログラムです。次のような特徴があります。

- ・ パソコン内のファイルが暗号化されて開けられなくなり、画面がロックされて使用不能になる。
- ・ 画面ロックや暗号化の解除と引き換えに「身代金」を要求される。

ランサムウェアは、金銭を要求する身代金型不正プログラムです。次のような特徴があります。

- ・ 画面ロックや暗号化の解除と引き換えに「身代金」を要求される。
- ・ 画面ロックや暗号化の解除と引き換えに「身代金」を要求される。

ランサムウェアは、金銭を要求する身代金型不正プログラムです。次のような特徴があります。

- ・ 画面ロックや暗号化の解除と引き換えに「身代金」を要求される。
- ・ 画面ロックや暗号化の解除と引き換えに「身代金」を要求される。

## 訓練メールの内容を検討する際に

訓練メール内容を検討する際に、メールの内容別・難易度別に分類された、多数のサンプルを参考にすることが可能です。(サンプルをそのまま利用しても、あるいは部分カスタマイズでも自由に活用できます。)

### 1. ① 議事録・資料等の確認依頼 (1)

項目名	内容
分類	A. 組織内外の区別がつかない内容
送信者名 <メールアドレス>	田中 <tanaka123@yehoo.jp>
件名	【ご確認お願いします】先日の打合せ議事録について
本文	各位 いつもお世話になっております。 先日のお打合せの際の議事録を添付にてお送り致します。 恐れ入りますが、内容をご確認の上、次回お打合せ候補日のご返信をお願い致します。 ファイルのパスワードは 2018xx です。 田中
メール形式	添付ファイルEXE (ファイル名: 議事録.zip → 議事録.pdf.exe ※パスワード付きZIP、ア
見破るポイント	<ul style="list-style-type: none"> <li>これまで受信したことがない、自分の業務とは関係のないメールアドレスから来ている。</li> <li>内容に心当たりがない。</li> <li>署名が不十分である。</li> <li>添付ファイルのアイコンがPDFにもかかわらず、拡張子がEXEである。</li> </ul>

### 1. ② システム・セキュリティに関する対応依頼 (1)

項目名	内容
分類	B. 内部連絡を装う依頼など
送信者名 <メールアドレス>	情報システム部 <system123@safesites.jp>
件名	【重要】ユーザID・パスワードの確認について (事務連絡)
本文	〇〇様 システム機能障害のため、ログイン設定の一部に急遽変更を加えました。 つきましては、システムアクセスに問題ないことを確認するため、 添付ファイルの記載した手順に従い、ユーザID及びパスワードを至急ご確認ください。 情報システム部
メール形式	添付ファイルDOC (ファイル名: 確認手順書.doc)
見破るポイント	<ul style="list-style-type: none"> <li>これまで受信したことがない、自分の業務とは関係のないメールアドレスから来ている。</li> <li>「情報システム部」という組織が存在しない。</li> <li>署名が不十分である。</li> <li>こうした通知がメールで送られてくることはない。</li> </ul>

### 1. ③ 経営層インタビュー

項目名	内容
分類	B. 内部連絡を装う依頼など
送信者名 <メールアドレス>	広報部 <kouhou123@cas-go.jp>
件名	【広報】社長インタビュー掲載のお知らせ
本文	各位 お疲れさまです。 社長のインタビューが雑誌に掲載されましたのでお知らせします。 添付ファイルよりご確認ください。 [インタビュー.pdf]
見破るポイント	<ul style="list-style-type: none"> <li>署名がない。</li> <li>添付ファイルがショートカット形式である。</li> </ul>

## メール本文サンプル集

## 終了通知をする際に

訓練の終了を通知する際のメールテンプレートを提供可能です。

《(標頭)》  
標的型攻撃メール訓練の終了について

《(本文)》  
各位、

## 終了通知メール テンプレート

次のとおり、標的型メール攻撃の訓練を実施しました。

・実施内容  
送信日時 平成25年MM月DD日 (X) HH:MM ~ HH:MM  
件名 <訓練メールの件名>  
送信者名 <訓練メールの送信者名>  
メール開封期間 平成YY年MM月DD日 (X) からDD日 (X)



---

<オプション>  
分散送信&開封通知による、初動対応訓練

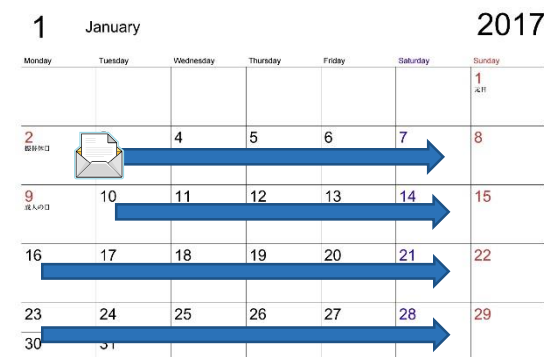
# 7-1. 分散送信 (有償オプション)

「分散送信」とは、訓練メールの送信を少数ずつ分散して行うためのオプションです。  
開封通知オプションと組み合わせて実施することで、最も効果的な初動対応訓練が実施できます。

送信開始日を含む最大20営業日での分割送信が可能です。  
(ただし、送信開始から1ヶ月間での全数送信完了を前提とします。)

## <前提条件>

- 事前テスト完了後のスケジュール変更および内容変更は原則対応しません。
- 各送信日での開始連絡および終了連絡は実施しません。
- 中間報告は、期間途中1回および全数送信完了時の2回のみとします。
- 2回訓練パック利用時については、1回目送信完了時と最終納品時での2回分割にて請求とさせていただきます。



## 開封通知オプションと組み合わせの効果

・分割することで1日あたりの開封者数を抑えられます。



・開封通知により、初動対応にもとづいた報告対応ができていない開封者を逐次フォローできます。

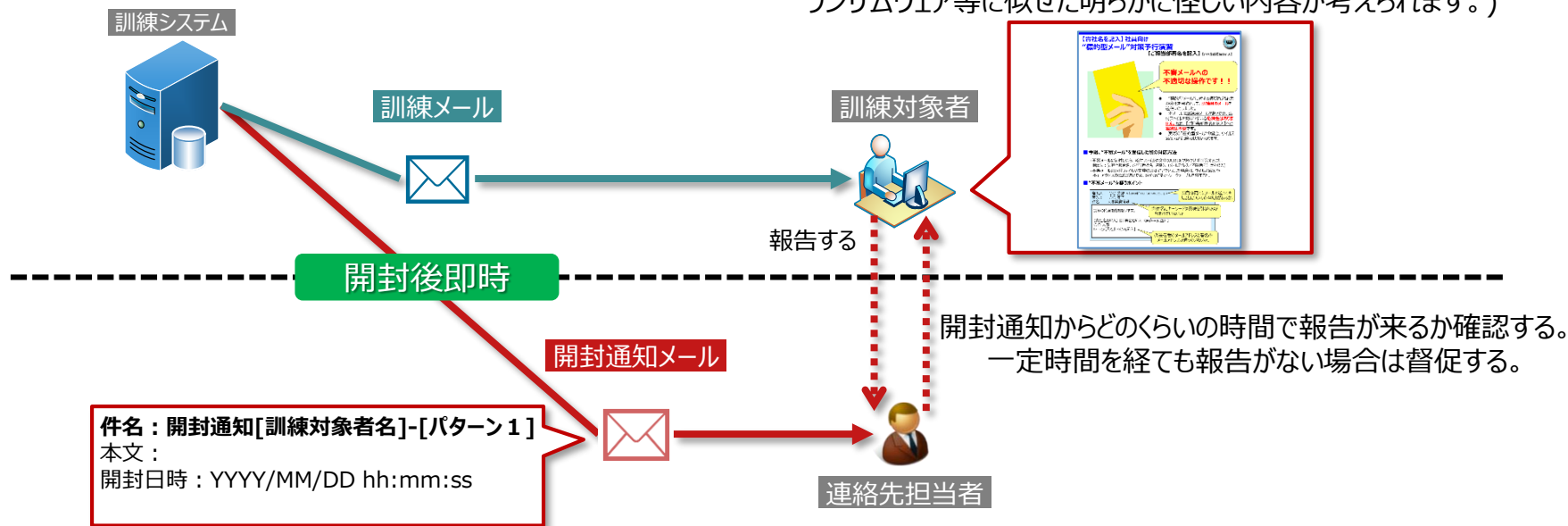
初動対応を重視した  
訓練を実現可能

## 7-2. 開封通知 (有償オプション)

「開封通知」とは「誰が、いつ、何を開封したか」を通知するメールです。開封後即時、所定の連絡先の担当者へ送付します。(自動送信にて送信します)

### 【開封通知機能の利用例】

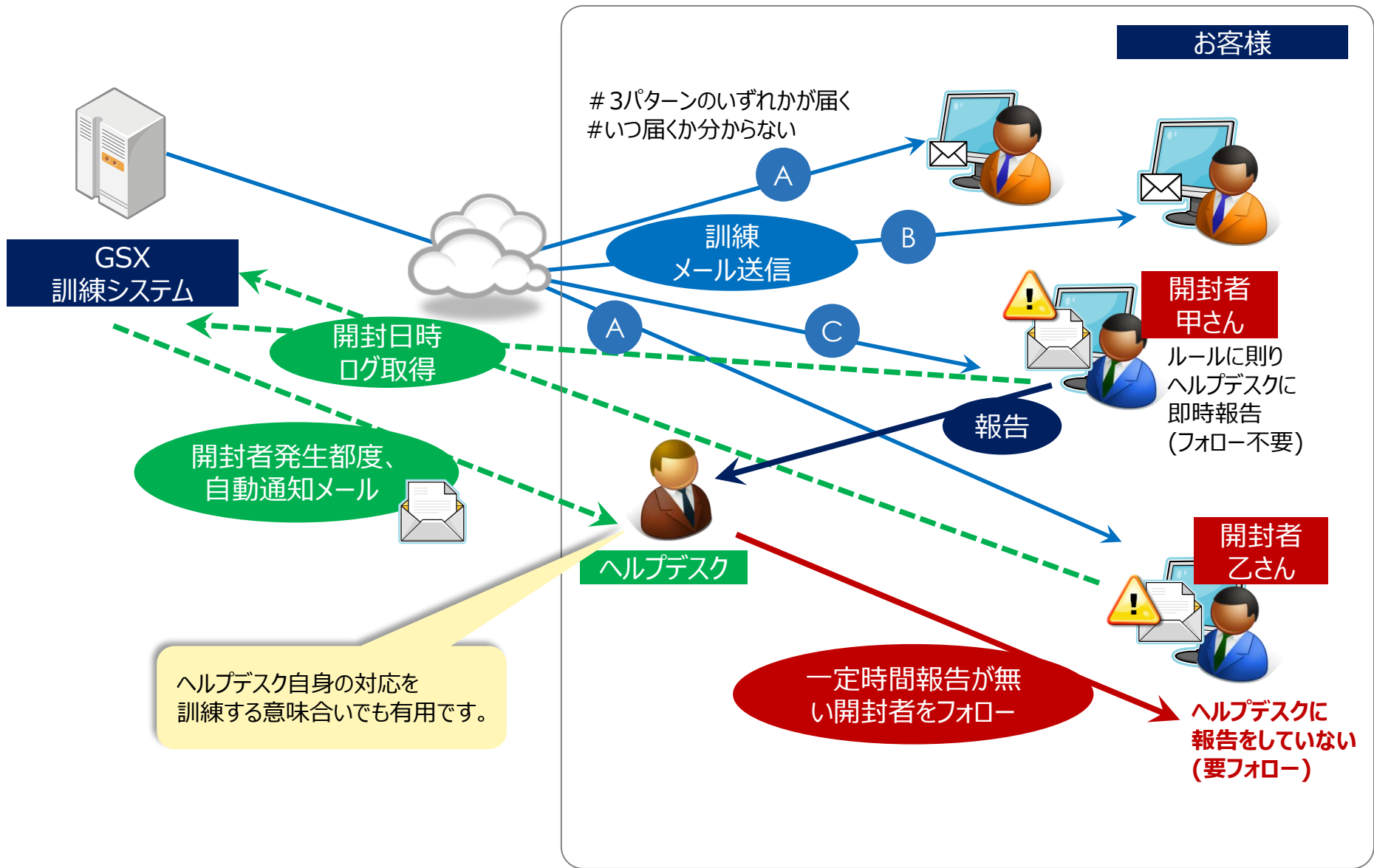
コンテンツ内容は、任意となります。(即時の初動対応を指示する内容や、ランサムウェア等に似せた明らかに怪しい内容が考えられます。)



### 開封通知機能を利用する目的と注意点

- 訓練対象者が、開封時には対応ルールに従い、所定の連絡先へできるだけ速やかに報告すること（初動対応）を徹底させます。連絡先担当者は、訓練対象者が開封からどれくらいの時間で報告してくるか（速やかに初動対応しているか）を確認します。
- 次の状況下での利用は推奨しません。
  - 不審なメールの開封時における対応ルールが浸透していない、あるいはルールや体制が未整備である。
  - 対象者の訓練経験が少なく、高い開封率が予想される。(連絡先担当者への問合せが殺到し、通常業務に支障をきたすおそれ)

# 7-3. 訓練イメージ: 分散送信&開封通知の活用例



# 株式会社 日立ソリューションズ・クリエイト

電話でのお問い合わせ

**0120-954-536**

受付時間 10:00~17:30 月曜日~金曜日（祝日、弊社休業日を除く）

メールでのお問い合わせ

**[hsc-contact@mlc.hitachi-solutions.com](mailto:hsc-contact@mlc.hitachi-solutions.com)**

※ご相談、ご依頼いただいた内容は、回答等のため、当社の関連会社（日立ソリューションズグループ会社）及び株式会社日立製作所に提供（共同利用含む）することがあります。取り扱いには充分注意し、お客様の許可なく他の目的に使用することはありません。



## 表示に関する注意事項

### ■他社商品名、商標などの引用に関する表示

- 標的型メール訓練サービスは、グローバルセキュリティエキスパート株式会社のサービスです。

### ■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2019年2月現在のものです。

サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。