

挑みつづける、変わらぬ意志で。



# 「標的型攻撃」メール訓練 実施結果

2023年11月24日

東京商工会議所 中小企業のデジタルシフト・DX推進委員会

# 1.実施目的

## 実施経緯

現在、企業や民間団体、官公庁等、特定の組織を狙う「標的型攻撃」による被害が頻発しています。企業におけるデジタル化・DXの進展に伴い、企業を取り巻くサイバーリスクも増大しており、ひとたびサイバー被害が発生すれば経営に致命的なダメージを与える可能性があります。

東京商工会議所では、中小企業・小規模事業者における情報セキュリティ意識の現状について広く周知すること、また、企業の経営者や担当者の意識向上と対策強化を促すことを目的に「標的型攻撃」メール訓練を実施しました。

※2019年度に初めて実施、以後毎年実施

## 「標的型攻撃メール」とは？

特定の組織やユーザー層にターゲットを絞り、悪意のあるファイルの添付やサイトへ誘導するためのURLリンクを貼り付けたメールを送信し、電子端末をマルウェアに感染させようとする攻撃のこと。最終的に業務上取り扱っている重要情報や個人情報等が盗まれ、経済的な損失はもちろん、顧客や取引先等からの信頼も大きく損なう可能性があり、企業にとって警戒すべきサイバー攻撃です。

独立行政法人情報処理推進機構（IPA）が公表した「情報セキュリティ10大脅威 2023」でも上位に挙げられます。

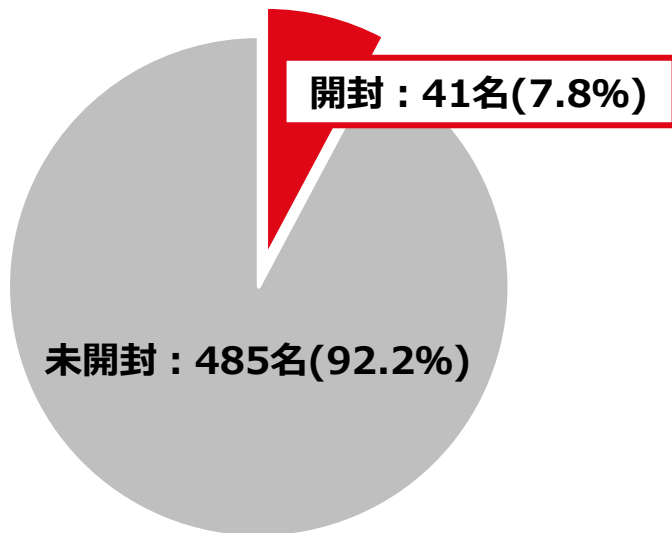
- 1位：ランサムウェアによる被害
- 2位：サプライチェーンの弱点を悪用した攻撃
- **3位：標的型攻撃による機密情報の窃取**

出所：情報セキュリティ10大脅威2023  
<https://www.ipa.go.jp/security/10threats/10threats2023.html>

## 2. 訓練内容 – 総括 –

- 2023年9月25日（月）から9月29日（金）の期間において、訓練対象者のメールアドレスに「標的型攻撃メール（訓練用）」を送信。
- 9月29日（金）までの期間に訓練対象者がメール本文内のURLをクリックした場合に「開封」としてカウントされ、画面上に警告メッセージを表示。

実施人数：526名



### 【対 象】

- 東京商工会議所会員企業（従業員300名以下）の経営者・従業員（公募）
- 申込社数：65社（昨年度：103社）
- 申込人数：526名（昨年度：811名）
- 1社あたり最大10名が参加

### 【実施スケジュール】

- メール送信日：2023年9月25日（月）12:00
- 開封確認期間：2023年9月29日（金）11:59まで

### 【訓練結果】

- **開封率：7.8%**

〈参考：過年度開封率〉  
2019年度 25.4%、2020年度 24.0%、2021年度 15.3%、2022年度 12.2%

## 2. 訓練内容 – 訓練メール本文 –

### 訓練メールの内容：偽の研修案内

#### 件名

Strengths Finder 2.0  
アクセスコードのお知らせ



#### 送信者名

Strengths Finder Customer Support

#### 送信ドメイン

strengths-finder@gallup-couese.biz

#### 本文

Strengths Finder 2.0 アクセスコードのお知らせ External  

Strengths Finder Customer Support <strengths-finder@gallup-course.biz>  
to me  Oct 29, 2021, 2:29 PM (6 days ago)   

様

この度は、弊社法人研修プランにお申込みいただきありがとうございます。  
Strengths Finder 2.0®の受験アクセスコードを、以下の通り発行いたしましたのでお知らせいたします。

下記サイトからアクセスコードをご入力いただくと、アカウントが作成されますので、案内に従って  
テストをご受験ください。

[受験案内ページ](#)  
アクセスコード：S%n7653Xt

※コードの有効期限は72時間となります。  
期限を過ぎますとアクセスができなくなるためご注意ください。

どうぞよろしくお願いたします。

---

◇このメールは送信専用アドレスから配信しています。返信しても回答できません。  
◇お問い合わせは、上記リンク先の問合せフォームからお願いいたします。  
Copyright © 2023 Gallup, Inc. All rights reserved.

---

## 2. 訓練内容 – 開封率 従業員数別 –

### 本年度

従業員数	対象者数	開封数	開封率
<u>0-5名</u>	20	1	<b>5.0%</b>
<u>6-20名</u>	126	15	<b>11.9%</b>
<u>21-50名</u>	210	14	<b>6.7%</b>
<u>51名以上</u>	170	11	<b>6.5%</b>
<b>全体</b>	526	41	<b>7.8%</b>

### (参考) 22年度

対象者数	開封数	開封率
81	9	11.1%
161	10	6.2%
308	38	12.3%
261	42	16.1%
811	99	12.2%

### 21年度

対象者数	開封数	開封率
28	2	7.1%
191	24	12.6%
208	35	16.8%
265	45	17.0%
692	106	15.3%

## 2. 訓練内容 – 開封率 業種別 –

### 本年度

業種	対象者数	開封数	開封率
製造業	92	4	<b>4.3%</b>
建設業	38	2	<b>5.3%</b>
卸売業	101	3	<b>3.0%</b>
小売業	22	0	<b>0%</b>
不動産業	21	1	<b>4.8%</b>
運輸業	10	2	<b>20.0%</b>
情報通信業	95	11	<b>11.6%</b>
宿泊・飲食業	0	0	–
その他	147	18	<b>12.2%</b>
全体	526	41	<b>7.8%</b>

### (参考) 22年度

対象者数	開封数	開封率
170	19	11.2%
50	5	10.0%
127	14	11.0%
46	3	6.5%
50	10	20.0%
10	0	0.0%
131	17	13.0%
0	0	–
227	31	13.7%
811	99	12.2%

### 21年度

対象者数	開封数	開封率
182	30	16.5%
56	6	10.7%
85	20	23.5%
60	7	11.7%
35	3	8.6%
10	1	10.0%
99	25	25.3%
0	0	–
165	14	8.5%
692	106	15.3%

## 2.訓練内容 – 開封率 役職別 –

本年度				(参考)	22年度			21年度		
役職	対象者数	開封数	開封率		対象者数	開封数	開封率	対象者数	開封数	開封率
経営者、 経営幹部	19	1	<b>5.3%</b>		45	1	2.2%	47	5	10.6%
肩書あり (経営者・ 経営幹部以外)	140	6	<b>4.3%</b>		243	36	14.8%	207	34	16.4%
肩書なし	367	34	<b>9.3%</b>		523	62	11.9%	438	67	15.3%
全体	526	41	<b>7.8%</b>		811	99	12.2%	692	106	15.3%

※訓練対象者のうち、役職・肩書・氏名いずれかの記載があった人数を集計。

## 2.訓練内容 – 開封者あて警告メッセージ –



こちらは「標的型攻撃メール訓練」です



本件は、本物のハッカーによる攻撃ではなく、東京商工会議所で実施している標的型攻撃メール訓練です。  
リンクをクリックしてしまった方は、下記からアンケートへのご回答、及びフィッシング対策を学んでください。

アンケートへの回答

フィッシング対策を学ぶ

(AironWorks株式会社：本訓練業務委託企業)

開封者へのフォローアップとして、フィッシング対策（標的型攻撃メールを見分けるポイント等）を学ぶ教育コンテンツを配信



### 3.東商の支援体制

#### 「東商サイバーセキュリティコンソーシアム」(2021年7月30日に発足)

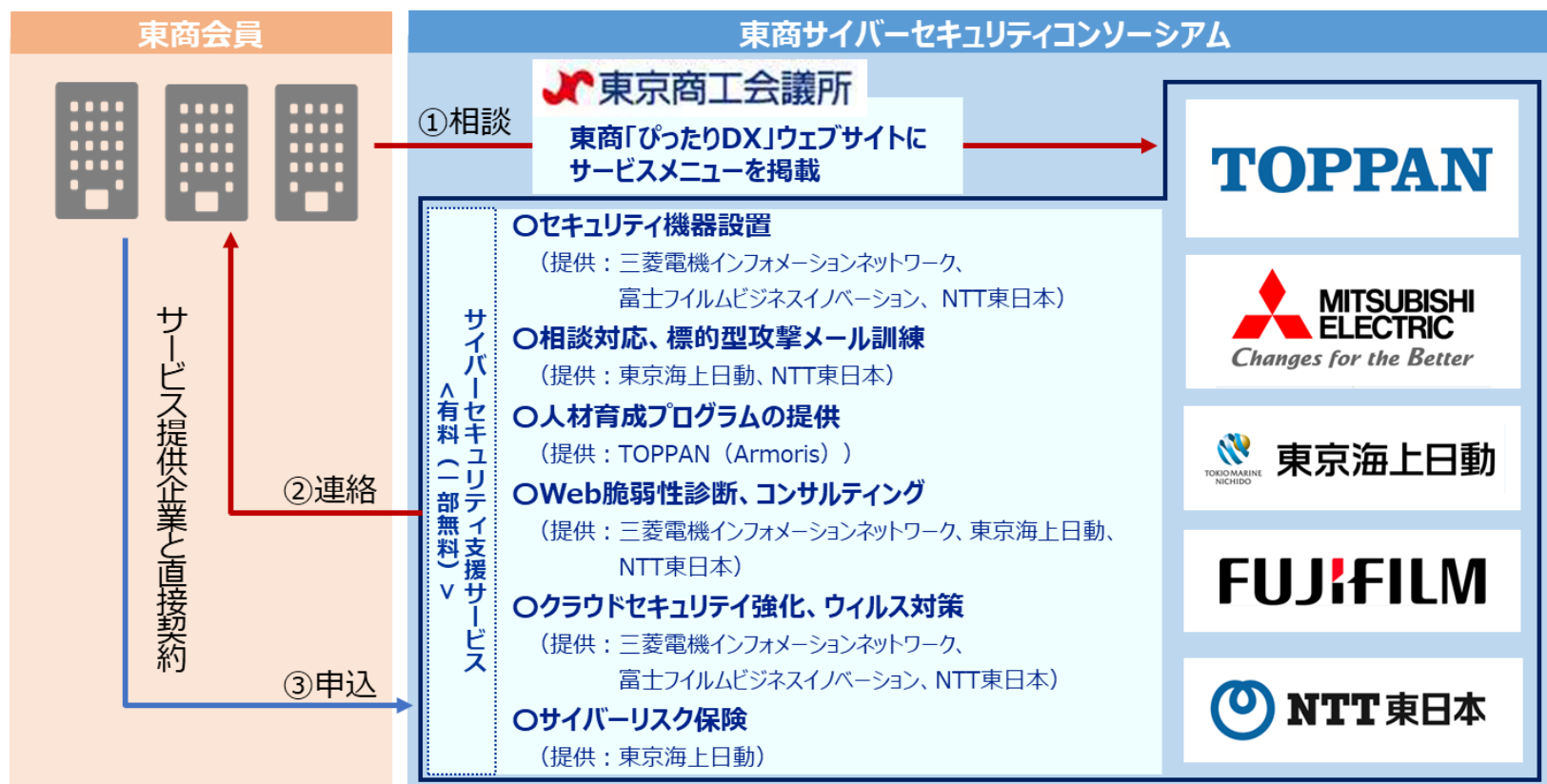
東商会員のサイバーセキュリティ対策を総合的に支援することを目的に、東商「ぴったりDX」ウェブサイトを通じて、中小企業向けサイバーセキュリティ支援サービスを提供しています。

#### ■ 参画企業

TOPPAN、三菱電機、東京海上日動火災保険、富士フィルムビジネスイノベーション、東日本電信電話

#### ■ 参照ウェブサイトURL

<https://www.tokyo-cci.or.jp/digital-support/security/>



## 3.東商の支援体制

### 【オンラインセミナー実施のご案内】

#### 中小企業・小規模事業者必見！最新のサイバー脅威と対策 ～「標的型攻撃」メール訓練結果から読み解く～

##### ■ 概 要

デジタル化・DXの進展に伴い、企業を狙ったサイバー攻撃のリスクが年々増加。中小企業・小規模事業者を狙った事例も少なくありません。さらに、ChatGPTに代表される生成AIの進展により企業の生産性向上や業務効率化、イノベーション促進が期待される一方、サイバー攻撃の高度化など新たなリスクも生じており、サイバーセキュリティ対策においては常に新しい知識を身に付け、対策を講じることが重要です。本セミナーでは、今回の標的型攻撃メール訓練の結果を踏まえたうえで今後どのような脅威が考えられるのか、最近のトレンドを交えて解説します。

- (内容)
- ・最新のサイバー脅威について
  - ・「標的型攻撃」メール訓練（2023年度）実施結果を踏まえた考察
  - ・一般的な標的型攻撃メール対策
  - ・質疑応答

- 講 師 AironWorks株式会社 担当者
- 配信期間 12月15日（金）～2024年1月26日（金）
- 形 式 オンライン（YouTube動画配信）
- 詳細・申込ページURL

[https://myevent.tokyo-cci.or.jp/detail.php?event\\_kanri\\_id=203119](https://myevent.tokyo-cci.or.jp/detail.php?event_kanri_id=203119)



▲詳細はこちら

## 4.参考

### 東京中小企業サイバーセキュリティ支援ネットワーク(Tcyss)

#### ■ 相談窓口

警視庁、東京都、東京商工会議所などの中小企業支援機関、ならびに、サイバーセキュリティ対策機関等が連携し、中小企業のサイバーセキュリティ対策の強化と支援、情報共有を目的とする「東京中小企業サイバーセキュリティ支援ネットワーク（Tokyo **Cyber Security Support** network for small and medium enterprises・通称Tcyss）の相談窓口では、情報セキュリティ対策の強化や情報流出事案等に関する相談を受け付けています。

#### ■ 関連ページURL

<https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/shoko/cyber/>

### IPA（独立行政法人情報処理推進機構）

#### ■ 「標的型攻撃」対策

特定の組織や人を狙って行われる「標的型攻撃」は、近年大きな脅威となっています。ソーシャルエンジニアリング手法を駆使した標的型攻撃メールや、セキュリティソフト等による検知を回避し侵入の痕跡を巧妙に隠蔽しながら活動するマルウェアなど、手口や技術も年々高度化しています。

IPAでは、「標的型攻撃」による被害拡大防止のため、各種情報、企業・組織向けの相談窓口や対応支援、情報共有の仕組みの提供など、様々な取組みを行っています。

#### ■ 関連ページURL

<https://www.ipa.go.jp/security/index.html>

挑みつづける、変わらぬ意志で。

