

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

2025年10月22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

実施目的

<目的>

近年、企業や官公庁等、特定の組織を狙う「標的型攻撃」による被害が多発している。デジタル化・DXが進展する中、企業を取り巻くサイバーリスクも増大しており、ひとたび被害が発生すれば、企業経営に致命的なダメージを与える可能性がある。

当所では、企業のサイバーセキュリティ対策支援の一環として、中小企業・小規模事業者の経営者や従業員の意識向上と対策強化を促すことを目的に2019年度より毎年「標的型攻撃メール」訓練を実施しており、本年度も引き続き実施したものの。

<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、知り合いや取引先を装い、ウイルスが仕込まれた添付ファイルや悪意のあるサイトに誘導するためのURLリンクを貼り付けたメールを送信し、パソコンやスマートフォンなどをマルウェアに感染させようとするサイバー攻撃。業務上取り扱っている重要情報や個人情報等が盗まれ、経済的損失・業務復旧への対応など事業継続に多大な影響を及ぼすおそれがある。さらに、サプライチェーンを構成する関連企業への攻撃の踏み台とされれば、顧客や取引先等からの信頼を大きく損なう可能性があり、中小企業が狙われるケースも増加している。

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2025」でも上位に挙げられている。

■ 情報セキュリティ10大脅威2025

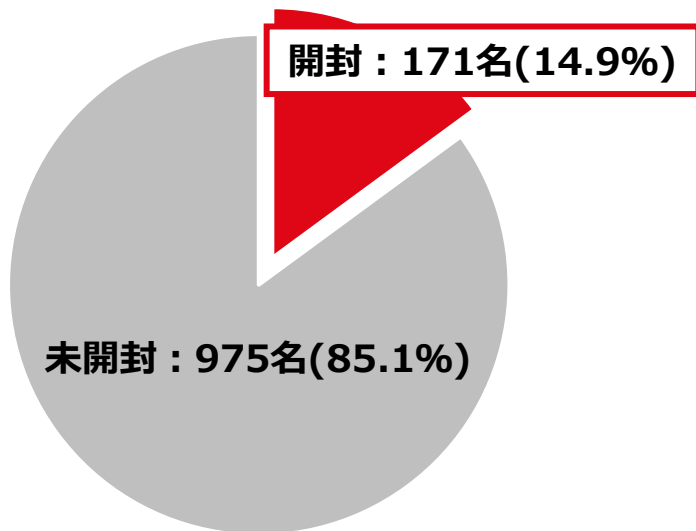
- 1位：ランサム攻撃による被害
- 2位：サプライチェーンや委託先を狙った攻撃
- 3位：システムの脆弱性を突いた攻撃
- 4位：内部不正による情報漏えい等

■ 5位：機密情報等を狙った標的型攻撃

訓練内容・結果

- 2025年9月2日～5日の期間において、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5日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」としてカウントし、画面上に警告メッセージを表示。

実施人数：1,146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：84社（昨年度：81社）
- 申込人数：1,146名（昨年度：920名）
- 1社あたり最大20名が参加

【実施スケジュール】

- メール送信日：2025年9月2日（火）11:00
- 開封確認期間：2025年9月5日（金）23:59まで

【訓練結果】

- **開封率：14.9%**

〈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%
2023年度 7.8%、2024年度 6.1%

訓練メールの内容：予定していないオンラインミーティングへの参加案内

件名

Teamsミーティングに招待されました

送信者名

Teams by Microsoft

送信アドレス

noreply@waveai.net

本文

{{employee.full_name}}様

Teamsミーティングに招待されました。

Teamsアカウントにログインいただくか、ミーティングのD、アクセスコードほか参加情報は以下のリンクからご確認いただけます。

参加情報を確認する：

{{attack_url}}

ミーティングID：
2519 957 3782

パスワード：
上記リンク先からミーティングパスワードを取得してください。

このメールは、ミーティング設定時に自動で送信されるメールです。
お心当たりがない場合は、お手数ではございますが、メールの破棄をお願いいたします。

© 2025 Microsoft and/or its affiliates. All rights reserved.

訓練内容・結果

アンケート結果（URLクリック者を対象に実施。n=29）

リンクや添付ファイルを開いてしまった理由として、最も当てはまるものを選んでください。

普段から、メールの内容に関わらずリンクや添付ファイルを開くことが多い	3.4%
差出人の名前を見て信頼してしまった	13.8%
メールの内容が具体的・自然で本物だと思った	31.0%
内容が緊急に感じられ、冷静な判断ができなかった	3.4%
怪しいと思ったが、開いてみないと判断できないと思った	31.0%
怪しいと思ったが、確認方法や対処法がわからなかった	-
その他	17.2%

不審なメールを見分けるポイント

- 不審な文体・表現がないか
- 差出人の名前とメールアドレス（ドメイン）が一致しているか
- リンク（URL）のドメインは正規のものか
- 表示されているURLと遷移先が合っているか ※リンクにカーソルを合わせ、遷移先のURLを確認
- 添付ファイルの種類や拡張子を確認する ※むやみに開封しない
- メールの署名を正規のものとの照合する

※実務上目にする頻度の高い内容であるほど、明確な心当たりのない場合には要注意！

訓練参加実績 (企業)	対象者数	開封数	開封率
昨年参加 ※1	628	88	14.0%
昨年非参加	518	83	16.0%

※1：2024年度の当所訓練事業へ参加した企業

訓練参加実績 (個人)	対象者数	開封数	開封率
昨年参加 ※2	256	31	12.1%
昨年非参加	890	140	15.8%

※2：2024年度の当所訓練事業の訓練対象者

属性別開封率

本年度

従業員数	対象者数	開封数	開封率
0-5名	76	6	7.9%
6-20名	194	27	13.9%
21-50名	446	79	17.7%
51名以上	430	59	13.7%
全体	1,146	171	14.9%

(参考) 24年度

対象者数	開封数	開封率
49	6	12.2%
124	8	6.5%
470	28	6.0%
277	14	5.1%
920	56	6.1%

23年度

対象者数	開封数	開封率
20	1	5.0%
126	15	11.9%
210	14	6.7%
170	11	6.5%
526	41	7.8%

属性別開封率

本年度

業種	対象者数	開封数	開封率
製造業	166	15	9.0%
建設業	95	31	32.6%
卸売業	187	34	18.2%
小売業	10	1	10.0%
不動産業	68	9	13.2%
運輸業	0	0	-
情報通信業	176	19	10.8%
その他	444	62	14.0%
全体	1,146	171	14.9%

(参考) 24年度

対象者数	開封数	開封率
202	13	6.4%
63	2	3.2%
163	5	3.1%
0	0	-
77	5	6.5%
0	0	-
116	8	6.9%
299	23	7.7%
920	56	6.1%

23年度

対象者数	開封数	開封率
92	4	4.3%
38	2	5.3%
101	3	3.0%
22	0	0%
21	1	4.8%
10	2	20.0%
95	11	11.6%
147	18	12.2%
526	41	7.8%

属性別開封率

本年度

(参考) 24年度

23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	114	17	14.9%	90	6	6.7%	19	1	5.3%
肩書あり (経営者・ 経営幹部以外)	484	76	15.7%	585	36	6.2%	140	6	4.3%
肩書なし	548	78	14.2%	245	14	5.7%	367	34	9.3%
全体	1,146	171	14.9%	920	56	6.1%	526	41	7.8%

※訓練対象者のうち、役職・肩書いずれかの記載があった人数を集計

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、重要なセキュリティ情報の発信や企業・組織向けの相談窓口・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。

