お知らせ

2025.02.21
毎年2月1日～3月18日は【サイバーセキュリティ月間】です。
期間中には、セキュリティ対策に関する『中小企業向けセミナー』が開催されます。

2024.12.02
【年末年始休業のお知らせ】
誠に勝手ながら、下記の期間は運営事務局の年末年始休業とさせていただきます。
■年末年始休業期間
2024年12月30日（月）～2025年1月3日（金）の5日間

「サイバーセキュリティ対策の極意」
中小企業向けサイバーセキュリティ対策の極意を
こちらで詳しく紹介しています。
ポータルサイトへ

中小企業サイバーセキュリティ啓発事業について

参加することのメリット！

- セミナーへの参加を通じて、経営課題としてのセキュリティ対策へ取り組む意識が高められる
- 標的型攻撃メールの模擬訓練を実施し、人的なセキュリティ対策を強化できる
- ネットワーク調査および構成図作成により、セキュリティリスクを可視化できる

中小企業サイバーセキュリティ啓発事業とは

近年のサイバー攻撃は、ますます巧妙化されています。機密データや個人情報の盗難、標的型攻撃メールやウイルスを、従来通りの技術的な対策だけで100%検知・防御することは難しいため、包括的なアプローチが求められます。本事業では、「サイバー攻撃対応演習セミナー」「標的型攻撃メール訓練」「ネットワーク調査・構成図作成」を実施することで、社内全体のセキュリティ意識醸成を促し、セキュリティ対策の実践を後押しします。

啓発効果と各サービスの連携イメージ

サイバー攻撃対応演習セミナー

「サイバー攻撃対応演習セミナー」への参加により、経営層にセキュリティ対策を「経営課題」として認識していただき、意識啓発と対策費用の予算化を促します。

標的型攻撃メール訓練

「標的型攻撃メール訓練」を実施することで、従業員のセキュリティ意識が醸成され、社内全体を包括的にサイバー攻撃の脅威から守ります。

ネットワーク調査・構成図作成

「ネットワーク調査・構成図作成」によりセキュリティ担当者に対しセキュリティ機器での対策方法を助言することで、現状改善やリスク対策が可能となります。

募集概要

「サイバー攻撃対応演習セミナー」「標的型攻撃メール訓練」「ネットワーク調査・構成図作成」は
ご好評につき、
申込数が上限に達したため募集を締め切りました。

申込期間	2024年6月～9月頃
支援対象	東京都内に主たる事業所を有する中小企業
受講対象	本事業における取組に意欲的に参加できる経営層、従業員、セキュリティ担当者等
支援期間	2024年7月～11月頃

参加費用　　無料

募集要項[PDF:781KB]　›

中小企業サイバーセキュリティ啓発事業説明会のご案内

本事業の特徴や支援の概要について詳しくご案内するほか、サイバーセキュリティ対策強化の意識向上につながるセミナーをあわせた説明会を開催します。ぜひご参加ください。

説明会は終了いたしました。

開催日程

1回目

~~6月18日(火)14:00~15:00(現地相談会 15:00~)~~

2回目

~~6月21日(金)16:00~17:00(現地相談会 17:00~)~~

3回目

~~6月26日(水)10:30~11:30(現地相談会 11:30~)~~

開催方式

ハイブリット開催
- 現地(東京都渋谷区渋谷2-12-4 ネクストサイト渋谷ビル2階)※先着25名
- オンライン(Microsoft Teams)

プログラム

第一部

『「サイバーリスク=ビジネスリスク」事業継続と成長に必要なサイバーセキュリティ対策とは?』
トレンドマイクロ株式会社　ジェネラルビジネス本部
シニアマネージャー　坂本 健太郎

第二部

『中小企業向け情報セキュリティ対策の基本』

独立行政法人情報処理推進機構（IPA）
セキュリティセンター　普及啓発・振興部　普及啓発グループ
田島 凛（6月18日、6月26日）
セキュリティセンター　普及啓発・振興部　普及啓発グループ
小山 祐平（6月21日）

第三部

『中小企業サイバーセキュリティ啓発事業について』
東日本電信電話株式会社　東京事業部　ビジネスイノベーション部
課長　堀 琢也

参加費用

無料

参加から実施までの流れ

事業説明会参加フォームより申し込み

説明会への参加を希望される場合は、お客様にてお申し込みください。
※下記ボタンより可能です。
※説明会への参加は、事業参加の必須条件ではございません。

説明会参加

指定日時の中から選択した説明会にご参加ください。事業内容の説明や質疑応答などを行います。

参加申込フォームより申し込み

支援内容をご確認いただき、お客様にて事業参加をお申し込みください。

①サイバー攻撃対応演習セミナー

「講義・演習・座談会」の3つのステップを1回のセミナーで行います。10日程のうち、いずれか1つの日程にご参加ください。

②標的型攻撃メール訓練

標的型攻撃メールの疑似訓練を2回行います。その後、開封率の結果を基にフィードバックコンサルティングを行い、今後の対策方法等のアドバイスを実施します。

③ネットワーク調査・構成図作成

通信トラブルの原因となる機器の配線・接続・設置状況や、LANケーブルの保護状況など通信機器の周辺環境も含めた調査を実施します。その後、フィードバックコンサルティングとしてアドバイス等を実施します。

支援内容について

啓発事業全体の流れ

まずは「自社セキュリティ診断」によってセキュリティ対策の現状を把握し、各サービス内で必要な対策を各社ごとにフィードバックします。

事業申込時に「自社セキュリティ診断」を実施

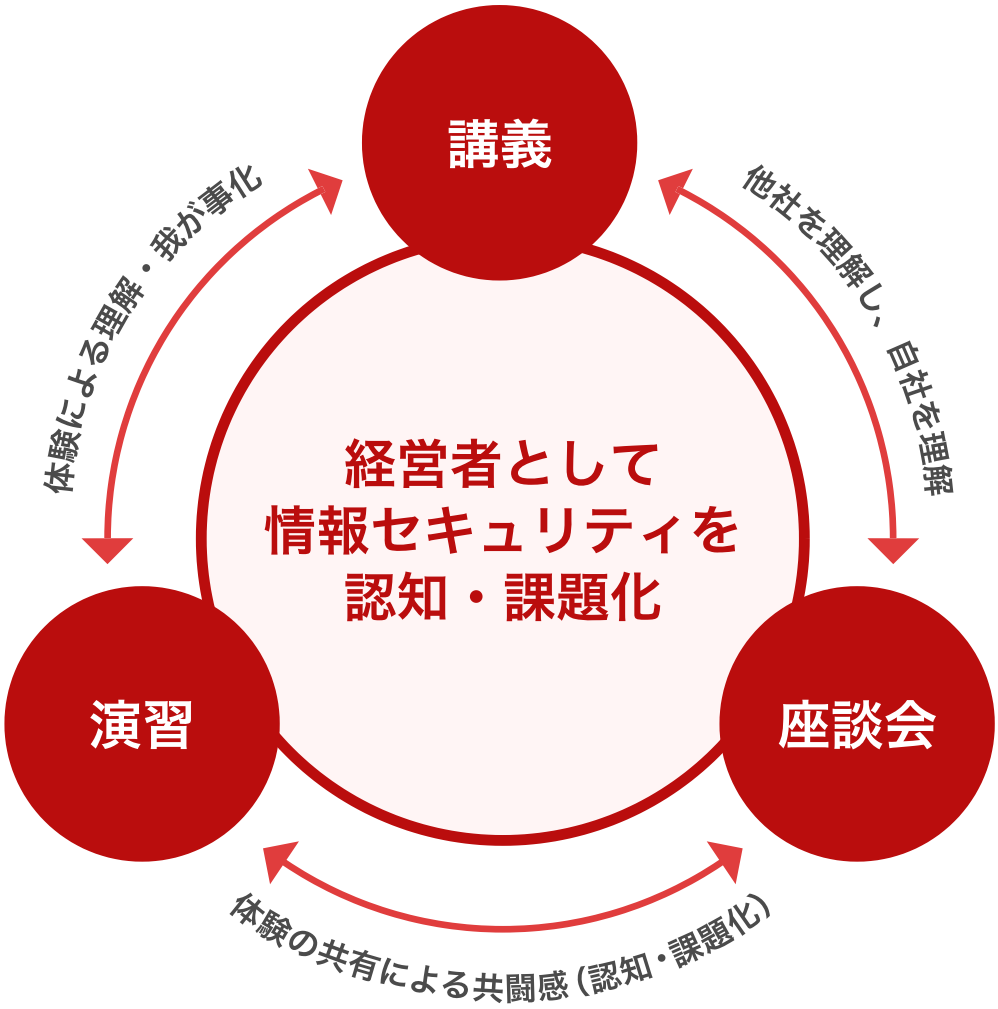
各種支援を実施するうえで、事業申込企業のサイバーセキュリティ対策の現状を把握する必要があるため、事業申込時に全社を対象とした「自社セキュリティ診断」（IPA「5分でできる！情報セキュリティ自社診断」）を行います。結果をもとに、セミナー講師または標的型攻撃メール訓練・ネットワーク調査の専門家からフィードバックします。

サイバー攻撃対応演習セミナー

1回のセミナーで「講義・演習・座談会」の3つのステップを行います。計10回実施予定です。

※10日程のうち、いずれか1つの日程にご参加ください。

※月に約2回開催予定となります。申込フォームにて参加日程を選択してください。



セミナーにより得られる効果

講義（自社診断評価含む）

一般的なセキュリティ知識と対策方法を学べる・理解できる

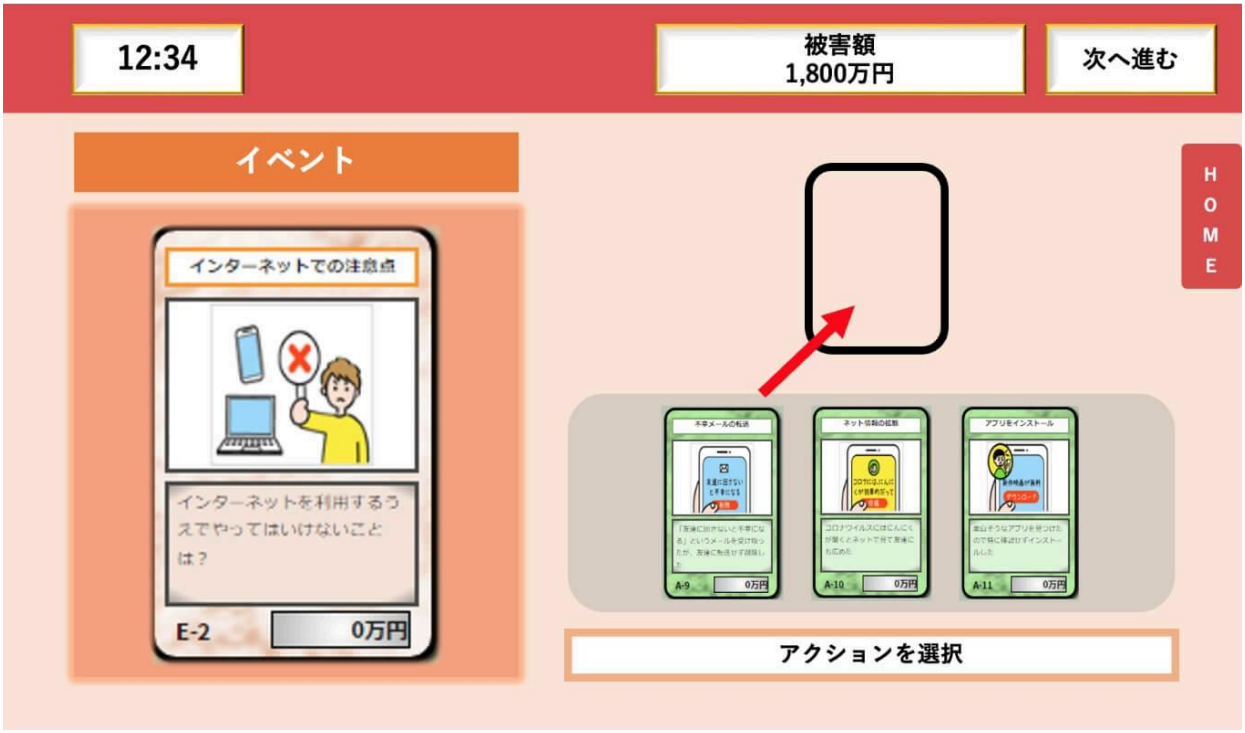
演習（体験型個人ワーク）

サイバー攻撃に対して適切な判断ができるか、自身の現状を把握できる

座談会（グループワーク）

他社状況把握と自社理解をし、今後取り組むべき事項を発見できる

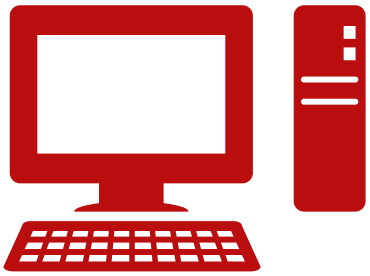
演習で活用するアプリケーション



※演習の画面イメージです

標的型攻撃メール訓練

技術的な対策

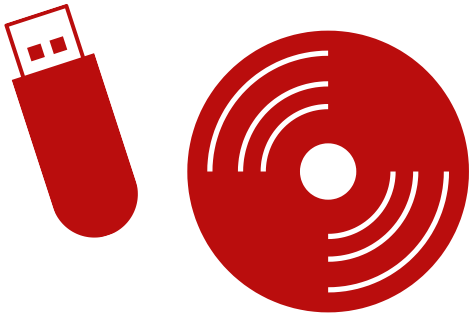


ウイルス対策

暗号化ソフト

UTM

人的な対策



データ持出管理

標的型攻撃メール訓練

昨今の巧妙化するサイバー攻撃を防ぐためには、従来通りのウイルス対策ソフト等による技術的対策に加えて、社員へのセキュリティ教育や標的型攻撃メール訓練等の人的対策が必要となります。また、人的対策は技術的な対策と異なり、繰り返しかつ継続的に意識啓発を行うことが求められます。訓練前後のコンサルティングでは訓練自体のコーディネートだけでなく、1回目の訓練後に実施するお客様社内での周知方法に関するサポートや、今後の具体的なお客様社内の対応ルール等の検討に関するアドバイスも実施します。

メール訓練後のコンサルティングにより得られる効果

不審なメールを見極める力

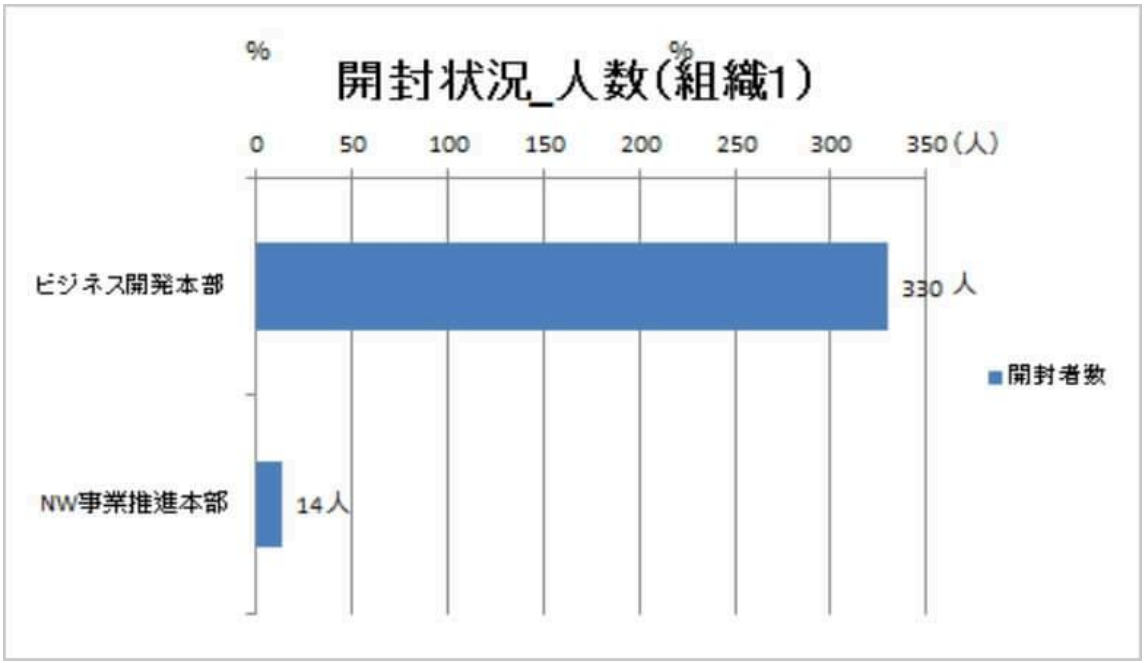
社内エスカレーション体制の構築

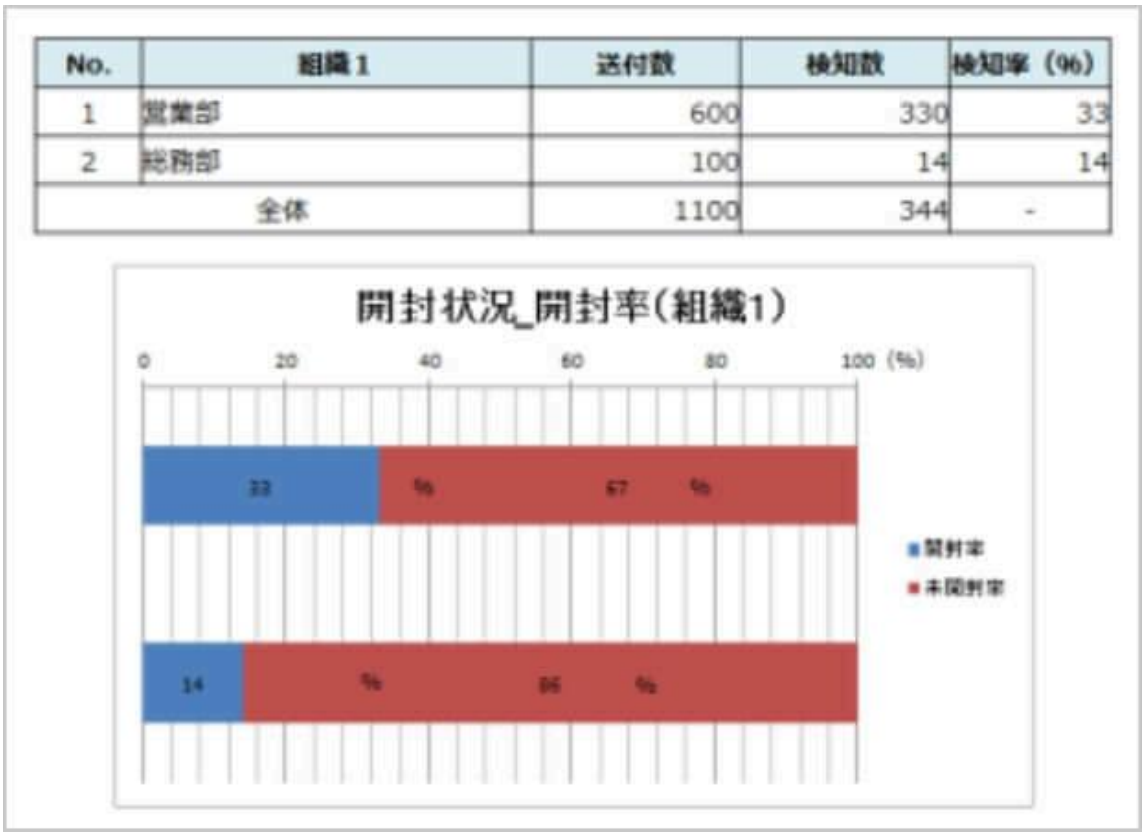
従業員のセキュリティ意識の向上

メール訓練の結果をレポートとして提供

訓練実施後に、全体の開封状況（開封時間や開封率など）に関する情報だけでなく、組織別・部署別・役職別の開封状況など、より詳細な内容まで網羅したレポートを提供します。訓練結果は、一覧化・グラフ化して視覚的に分かりやすく作成します。

【レポートイメージ】





No.	組織1	送付数	検知数	検知率（%）
1	営業部	600	330	33
2	総務部	100	14	14
全体		1100	344	-

※こちらはイメージです

ネットワーク調査・構成図作成

多角的にセキュリティ状況を把握するために、調査時には「機器調査」に加え、ネットワーク機器の利用環境も調査します。また、通信トラブルの原因となる機器の配線・接続・設置状態の確認のための「物理環境調査」もあわせて実施します。

機器調査

- 機器種別（ルーター/スイッチ/HUB 等）
- メーカー・品番・シリアルNo.

物理環境調査

- LANケーブルの保護状況（モール等）
- 消火設備（スプリンクラー等）周辺のPC/SV

作成物

●接続構成図　●平面図　●機器一覧　●物理環境調査レポート
●自社セキュリティ診断レポート

専門家にて構成図・平面図を作成します。接続経路や設置位置が明確化され、トラブル対応時や工事・点検時に役立ちます。また、平面図は「セキュリティ関連規定」作成時に活用できます。

調査後にフィードバックコンサルティングを実施

技術的対策と物理環境的対策の両面で指導・助言を実施いたします。

技術的対策

「接続構成図」「機器一覧」
「自社セキュリティ診断レポート」の結果

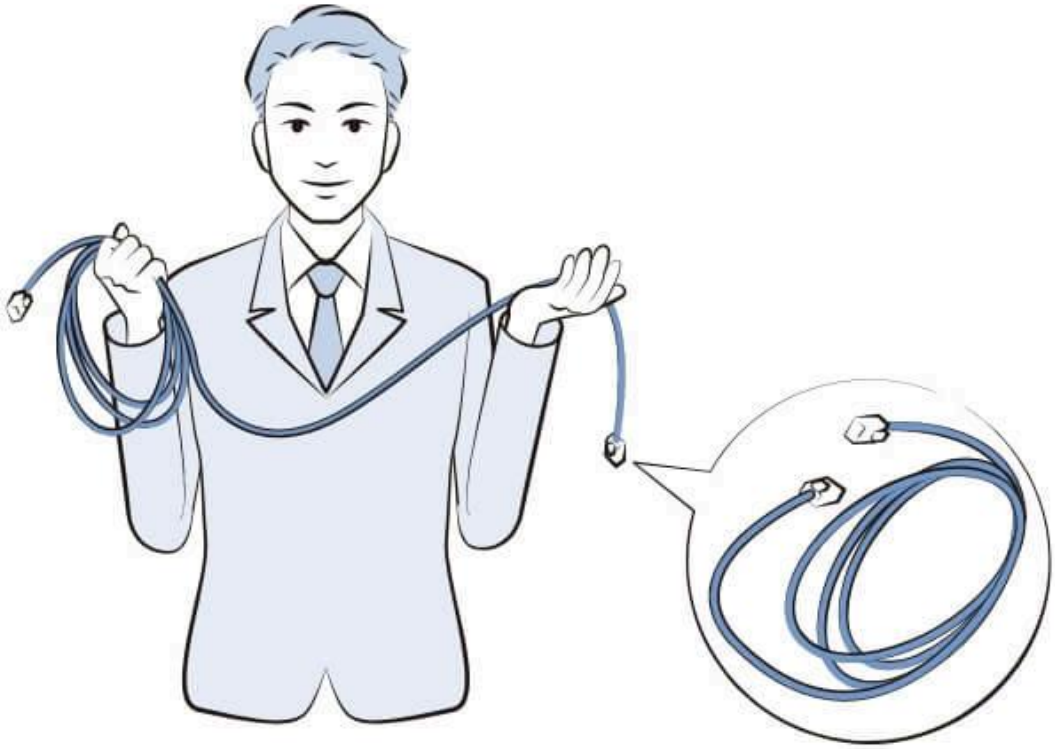
↓

セキュリティ機器・ソフト等の対策検討

物理環境的対策

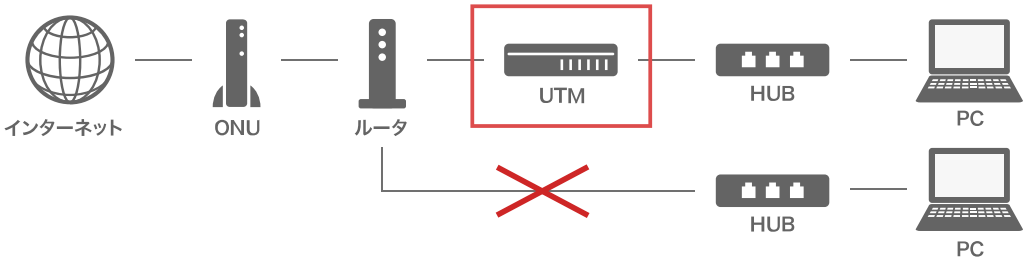
「物理環境調査レポート」の結果

LANケーブルへのタグ取付等の対策検討



【参考】

現在の構成ではセキュリティ対策装置（=UTM）を経由せずにインターネットを利用しているため、一部のPCが脆弱です。設置位置の変更が必要です。



ネットワーク調査により得られる効果

セキュリティ対策状況の可視化

自社のネットワーク環境の把握・セキュリティリスクの可視化が可能

トラブル時の迅速な原因究明
ネットワーク環境内の故障や通信障害等へのスムーズな対応が可能

通信環境の把握
通信トラブルの原因となる機器の劣化やケーブルの保護状況など現状把握が可能

参加企業の声

令和6年度中小企業サイバーセキュリティ啓発事業にご参加の企業様に、3つの質問にご回答いただきました。

参加した支援　サイバー攻撃対応演習セミナー

学術研究・専門・技術サービス業
従業員数:6～20名

Q　Qサイバー攻撃対応演習セミナーを通じて、セキュリティへの意識や考え方に変化はありましたか。

A　A今回のセミナーを通じて、セキュリティ意識が大きく向上したと実感しています。これまでセキュリティを意識する機会がそれほど多くなかったため、セミナーはとても良い機会となりました。講義では過去の被害事例をもとにサイバー攻撃への理解が深まり、演習では実際の脅威を体感することで、対策の重要性を改めて認識することができました。今後は社

内全体のセキュリティ意識向上に努めるとともに、具体的な対策の強化を進めたいと考えています。

Q　Qサイバー攻撃対応演習セミナーを通じて、セキュリティ対策への強化に繋がったことがあれば教えてください。

A　A第二部の演習は想像以上に実践的な内容で、セキュリティ対策への意識向上につながる非常に有益な機会となりました。この経験をもとに、新たなセキュリティ対策として、社内での情報共有の仕組みやドキュメントの保管体制を強化する計画を進めています。これにより、より安全な業務運営を実現し、サイバー攻撃などのセキュリティリスクを最小限に抑えることを目指しています。

Q　Qサイバー攻撃対応演習セミナーを通じて、得たことや学びを教えてください。

A　A座談会では、他社との比較を通じて自社が業務委託を受ける際のセキュリティ対応において一定の水準を満たしていることを確認できました。一方で、社内での情報共有の方法やドキュメントの保管体制に関しては、改善の余地がある点を認識しました。他社の取り組みを知ることで、自社のセキュリティ状況を客観的に把握し、多くの学びを得る機会となりました。セミナーで得た知見を社内で共有し、全社的なセキュリティ意識のさらなる向上を目指します。

金融・保険業
従業員数:6～20名

Q　Qサイバー攻撃対応演習セミナーを通じて、セキュリティへの意識や考え方に変化はありましたか。

A　A今回のサイバー攻撃対応演習セミナーを通じて、セキュリティ意識が大幅に向上しました。特に、他業種の参加者と交流をすることで、普段とは異なる視点からセキュリティを考えることができました。さらに、講義内容や具体的な事例をもとに、サイバー攻撃の脅威を実感

し、セキュリティに対する理解を一層深めることができました。こうした学びを今後の業務に生かし、社内全体のセキュリティ強化に取り組んでいきます。

Q **Qサイバー攻撃対応演習セミナーを通じて、セキュリティ対策への強化に繋がったことがあれば教えてください。**

A Aサイバー攻撃対応演習セミナーを通じて、セキュリティ対策への強化に繋がったことがあれば教えてください。自社のセキュリティ対策を改めて見直すきっかけとなりました。特に、パスワード管理の徹底やメール送信方法の見直しなど、具体的な対策の必要性を強く認識しました。また、サイバー攻撃への対処の難しさを実感し、インシデント発生時における迅速な対応の重要性についても考えさせられる機会となりました。今後は、セキュリティシステム全般を見直し、運用効率と対策強度のバランスを考慮しながら改善を進めます。

Q **Qサイバー攻撃対応演習セミナーを通じて、得たことや学びを教えてください。**

A Aサイバー攻撃対応演習セミナーを通じて、得たことや学びを教えてください。他業界のセキュリティ状況を知る良い機会となりました。講師の解説や他社との座談会を通じて、異なる業種の考え方や注目ポイントを学び、新しい視点を得ることができました。異なる視点からの学びが得られるため、全体的なセキュリティ意識の向上に繋がったと思います。他の業種の方とセキュリティ対策について話すことは滅多になく、とても貴重な経験でした。次回の開催があれば、ぜひ他社にもおすすめしたいです。

参加した支援　標的型攻撃メール訓練

学術研究・専門・技術サービス業
従業員数:101～300名

Q **Q標的型攻撃メール訓練を通じて、セキュリティへの意識や考え方に変化はありましたか。**

A Aサイバー攻撃対応演習セミナーを通じて、セキュリティ対策への強化に繋がったことがあれば教えてください。業種柄、ITに長けている社員が多く、取引先も個人情報保護やセキュリティには厳しいため、訓練前からそれなりにセキュリティ意識は高かったと思います。しかし、結果を見ると4

割の社員が標的型攻撃メール訓練に引っかかっていました。訓練に参加したことで、組織全体のセキュリティ意識は非常に向上しました。以前から標的型攻撃メール訓練をやる価値があるかどうか疑問でしたが、効果を実感し訓練を毎年実施することを検討しています。

Q　Q標的型攻撃メール訓練を受けたことで、セキュリティ対策への強化に繋がったことがあれば教えてください。

A　A標的型攻撃メール訓練の後、セキュリティ対策強化に向けてまずは全社員向けに社内の定例会で訓練結果と他社で起きた事故の事例について共有しました。また、エスカレーション体制を整えるために、コンサルティングの際にアドバイスいただいた内容を踏まえて、全社員が理解しやすくシンプルなルールの策定をします。さらに、標的型攻撃メール訓練の定期的な実施およびUTM・EDRなどの導入を検討しています。

Q　Q標的型攻撃メール訓練を通じて、得たことや学びを教えてください。

A　Aこれまでもセキュリティリスクについて理解はしていましたが、実際に対策まで踏み出せずにいました。しかし、今回の訓練を受けることでセキュリティリスクを自分事として捉えられるようになり、実際に対策に着手するきっかけを得ることができたため、非常に有意義でした。この支援は特にセキュリティ体制が整っていない中小企業へ紹介したい内容です。東京都の施策で費用が発生しないことも大きな魅力で、セキュリティ対策に踏み出せない企業の後押しになると思います。

情報通信業
従業員数:21~50名

Q　Q標的型攻撃メール訓練を通じて、セキュリティへの意識や考え方に変化はありましたか。

A　A社員全体のメールに対する警戒意識が大幅に向上しました。訓練中に不審なメールを見つけた社員がすぐに周囲に伝達し、送信者への確認や全体への注意喚起を迅速に実施した対応が非常に効果的でした。このおかげで、組織内での被害を未然に防ぐ重要性を再認識することができました。一方で、管理者への報告に時間がかかるなどの課題も明らかになり

ました。今後は発見時の対応手順を改善し、より迅速にエスカレーションできる体制を整えていく予定です。

Q　**Q標的型攻撃メール訓練を受けたことで、セキュリティ対策への強化に繋がったことがあれば教えてください。**

A　A発見者が適切に対応する一方で、不審なメールを無視してしまう社員もおり、社員間でセキュリティ意識に差が見られることが課題として浮き彫りになりました。この問題を解決するために、今後は専門の社内システム特任チームを新たに設置する予定です。さらに、UTMやEDRといった技術的な対策に加え、情報セキュリティ研修や標的型攻撃メールを活用した訓練など、人的対策も強化して、社内のセキュリティ対策全体を一層充実させる方針です。

Q　**Q標的型攻撃メール訓練を通じて、得たことや学びを教えてください。**

A　A発見時の初動対応が、被害拡大の抑止において極めて重要であるという認識を社内で共有することができました。訓練後、報告や周知の手順を再構築する必要性を強く感じ、具体的にはエスカレーション先の明確化や、不審なメールへの対応マニュアルの調整が必要だと考えています。この経験を踏まえ、定期的なセキュリティ訓練や教育を行い、組織全体のセキュリティレベル向上に努めたいと思います。

参加した支援　ネットワーク調査・構成図作成

建築業
従業員数:1～5名

Q　**Qネットワーク調査・構成図作成を通じて、セキュリティへの意識や考え方に変化はありましたか。**

A　Aセキュリティ意識の大幅な向上を実感する機会となりました。日常業務では見過ごされがちな部分を、専門家による訪問調査を通じて細かな脆弱性を発見できたことは、非常に有益でした。特に、ネットワーク機器ごとの役割に対する理解が深まり、改めてセキュリティの重要性を認識しました。この取り組みをきっかけに、全社的なセキュリティ意識の向上が図られ、従業員全体のリテラシー向上にも繋がったと感じています。

Q　**Qネットワーク調査・構成図作成を受けたことで、セキュリティ対策への強化に繋がったことがあれば教えてください。**

A　A今回の調査と、体系的かつ詳細な構成図をいただいたことで、物理的リスクへの対策強化を図るとともに、エンドポイントセキュリティソフトの導入を実施しました。また、電源供給方法の見直しを行い、漏電リスクが指摘されていた箇所も改善しました。今後は、UTMやEDRの導入、WPA3対応のWi-Fi機器の活用など、最新のセキュリティ対策を積極的に取り入れ、第三者の侵入防止およびログ管理の徹底に取り組みます。

Q　**Qネットワーク調査・構成図作成を通じて、得たことや学びを教えてください。**

A　Aネットワーク調査・構成図作成を通じて得られた知識と対策によって業務の効率化とセキュリティの強化ができました。今回配布された専門家のレポートを社内に共有したところ、セキュリティに関心のない従業員からも理解が深まったとの声があがりました。物理環境の改善やUTMの導入の重要性を理解することができ非常に有意義でした。今後も更なるセキュリティ強化と業務改善を図りたいと考えています。

卸売・小売業
従業員数:301名～

Q　**Qネットワーク調査・構成図作成を通じて、セキュリティへの意識や考え方に変化はありましたか。**

A　A社内にある機器構成を把握することで、ネットワーク構成全体の理解度が向上しました。これにより、自社ネットワークの脆弱性や改善ポイントを意識するきっかけとなり、セキュリ

ティ意識も高まりました。支援を受けた直後から、自分たちで他店舗を回ってネットワーク機器や接続構成を確認するようになり、今後は定期的にネットワークをチェックする習慣を身につけたいと考えています。

Q **Qネットワーク調査・構成図作成を受けたことで、セキュリティ対策への強化に繋がったことがあれば教えてください。**

A **A**現在のところ、ウィルス対策ソフト以外のセキュリティ対策には取り組めていませんでした。しかし、本支援での専門家とのコンサルティングを通じて、社内の機器構成やネットワークを正確に把握することで、将来的な機器故障やトラブルにも迅速な対応ができる体制の構築ができました。また、ネットワーク機器の更改時期を把握することで、適切な予算計画を立て、安定した運用を実現できるようにしたいと考えています。

Q **Qネットワーク調査・構成図作成を通じて、得たことや学びを教えてください。**

A **A**本支援に参加することで、セキュリティ意識の向上が図れたことは非常に有意義だったと感じています。特に、日常的に使用しているネットワークの構成や脆弱性を把握できたことで、セキュリティ対策の必要性を再認識できました。さらに、潜在的なリスクの洗い出しができたことにより社内体制全体を改善するきっかけとなりました。得られた成果や知識は、同じような課題を抱える知り合いの企業にもぜひ共有したいと感じています。

お問い合わせ

東京都「中小企業サイバーセキュリティ啓発事業」運営事務局

TEL：0800-800-5513（電話受付時間・事務局営業時間 ：平日 9:00～17:00）

メール：cs-keihatsu-info-ml@east.ntt.co.jp

主催：東京都 ※本事業は東京都より委託を受け、東日本電信電話株式会社が運営しています。

東京都 TOKYO METROPOLITAN GOVERNMENT

東京都産業労働局