訓練だけで終わらせない！

”本気“の不正メール訓練サービス

Mail Fort Insight

一般社団法人
中小企業をサイバー攻撃から守る会

従業員の１クリックで

会社の未来が吹き飛ぶ可能性があるとしたら

そのリスク、放置できますか？

サイバーインシデントの実態

情報セキュリティ10大脅威 2025（独立行政法人 情報処理推進機構）

apsc.jp

順位	「組織」向け脅威	10大脅威での取り扱い
1	**ランサムウェアによる攻撃**	**10年連続10回目**
2	**サプライチェーンや委託先を狙った攻撃**	**7年連続7回目**
3	システムの脆弱性をついた攻撃	5年連続8回目
4	内部不正による情報漏えい等	10年連続10回目
5	**機密情報を狙った標的型攻撃**	**10年連続10回目**
6	リモートワーク等の環境や仕組みを狙った攻撃	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	5年ぶり6回目
9	ビジネスメール詐欺	8年連続8回目
１０	不注意による情報漏洩	7年連続8回目

メールを起点とした
サイバー攻撃

不審なメールに対する
一人一人の危機意識の醸成は
企業防衛の観点からも
非常に重要な経営課題の一つ
と言えます！

重大なサイバーインシデントのトリガーは「人」

apsc.jp

Twitter（現 X）
・**社員がソーシャルエンジニアリング攻撃を受け、社内管理ツールにアクセス**させた
・バラクオバマ、イーロンマスク、ビルゲイツなど著名人のアカウントが乗っ取られ、ビットコイン詐欺が行われた。

三菱電機
・**社員がメール添付ファイルを不用意に開封**し、マルウェアに感染
・社内の複数システムに不正に侵入され、軍事、電力などの機密情報が漏えい

日本年金機構
・**職員が不審な添付ファイル付きメールを開封**し、マルウェアに感染
・年金受給者の氏名・基礎年金番号などが漏えい、社会批判が高まり、職員の処分や組織改革に発展

Google、Facebook
・GoogleとFacebookの担当者が**詐欺メールに騙され、合計1億ドルを送金**し続けていた
・世界中で報道され、内部チェック体制の甘さが露呈、社会的信用を失った

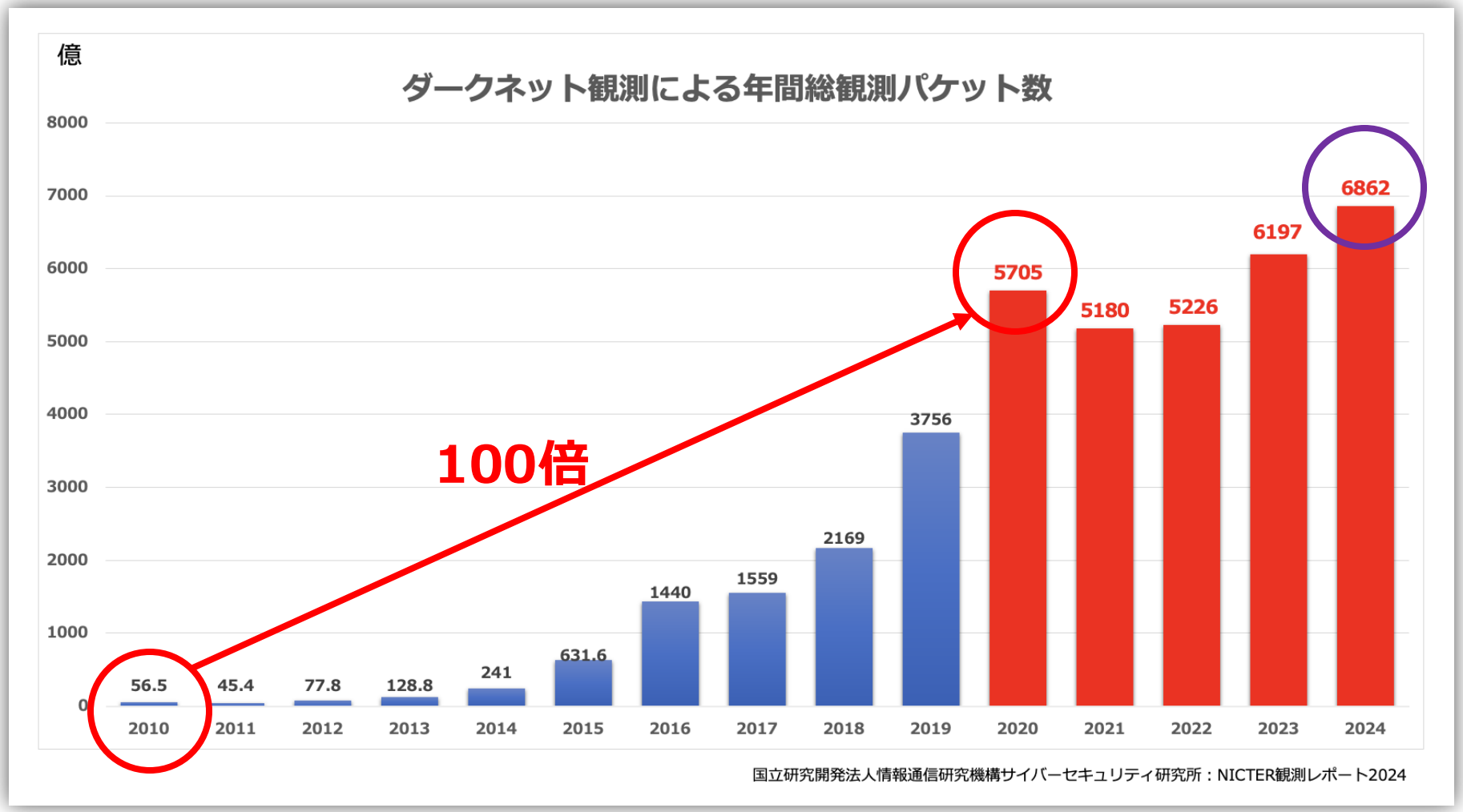
Uber
・**人事担当が騙されクラウドに不正アクセス**され、5700万人の顧客とドライバー情報が流出
・ハッカーに10万ドルを支払って隠蔽しようとしたことが問題視され、多額の罰金を支払うこととなった

重大インシデントの90%以上で、トリガーは「人」だと言われています。

セキュリティが強固な有名企業でも「人」が原因で大きな問題に発展しています

増え続ける日本に対するサイバー攻撃

apsc.jp



国立研究開発法人情報通信研究機構サイバーセキュリティ研究所：NICTER観測レポート2024

添付ファイル付きの１MBのメール

↓

約667パケット

6862億パケット

↓

10億２千800万通の

添付ファイル付きメール

に相当する量

apsc.jp

ランサムウェアとは？

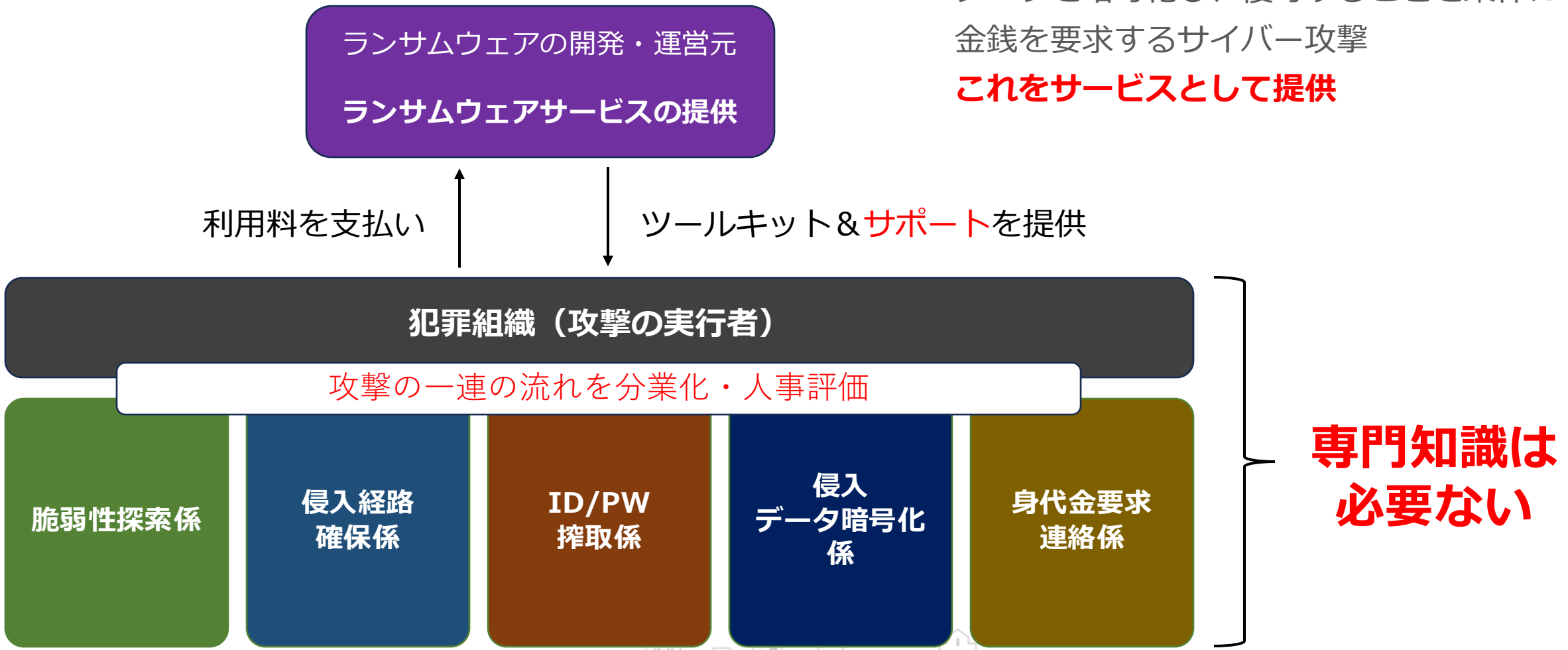
データを暗号化して開けない状態にし、
複合を条件に金銭を要求する不正プログラム

金銭を要求されて支払ってしまった企業団体の割合

46%

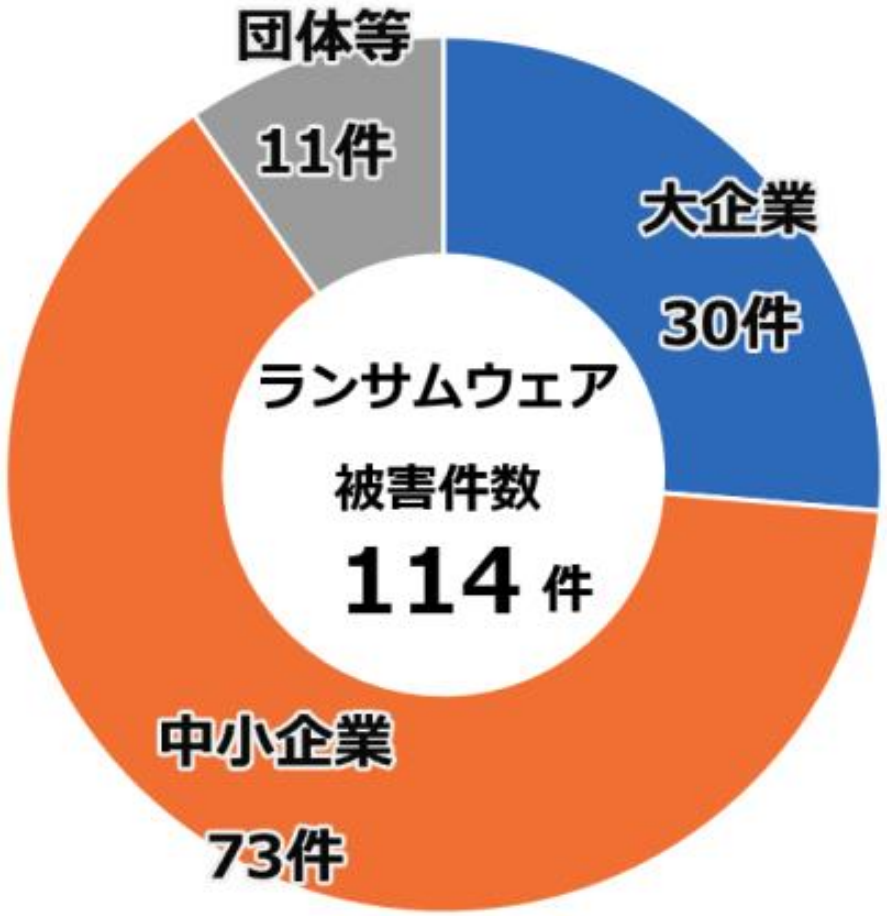
Raas：Ransomware as a Service

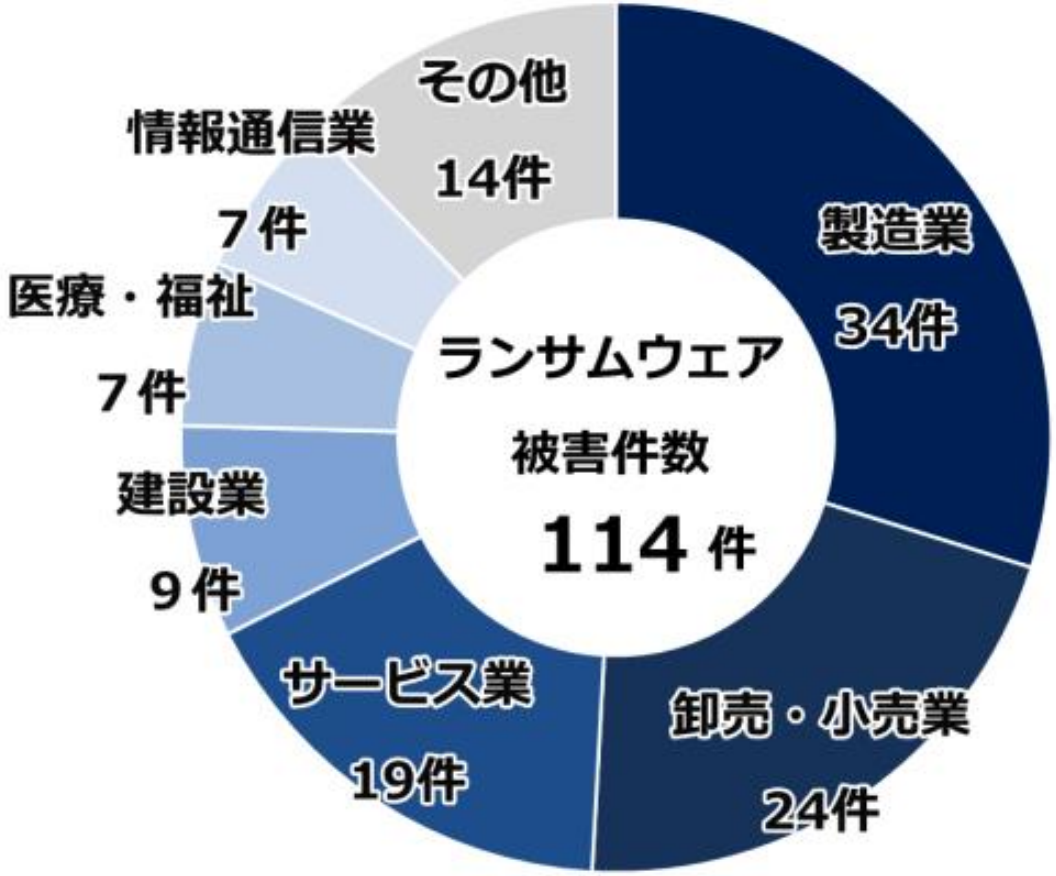
＜ランサムウェア攻撃＞
データを暗号化し、復号することを条件に
金銭を要求するサイバー攻撃
これをサービスとして提供



ダークWebで取引される、ランサムウェアツール

ランサムウェア　～　規模別／業種別報告件数

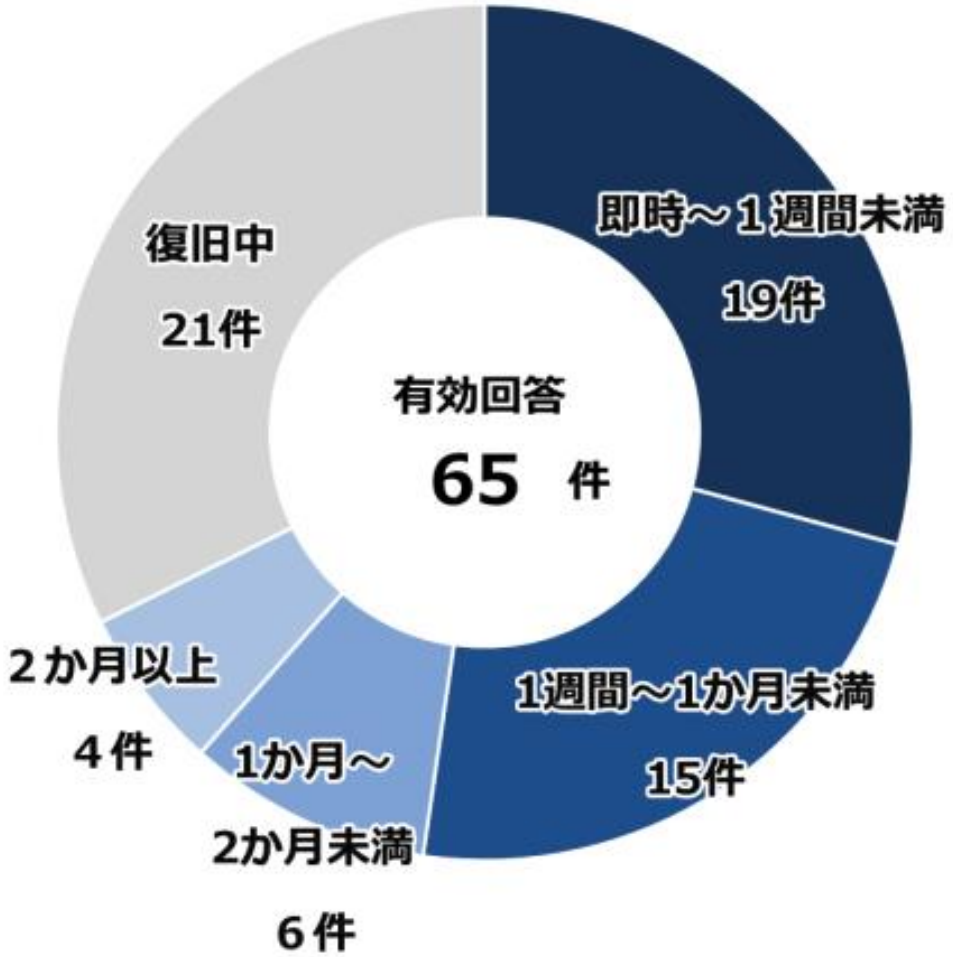




令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）より

ランサムウェア被害　～　復旧に要した期間／調査費用の総額

apsc.jp



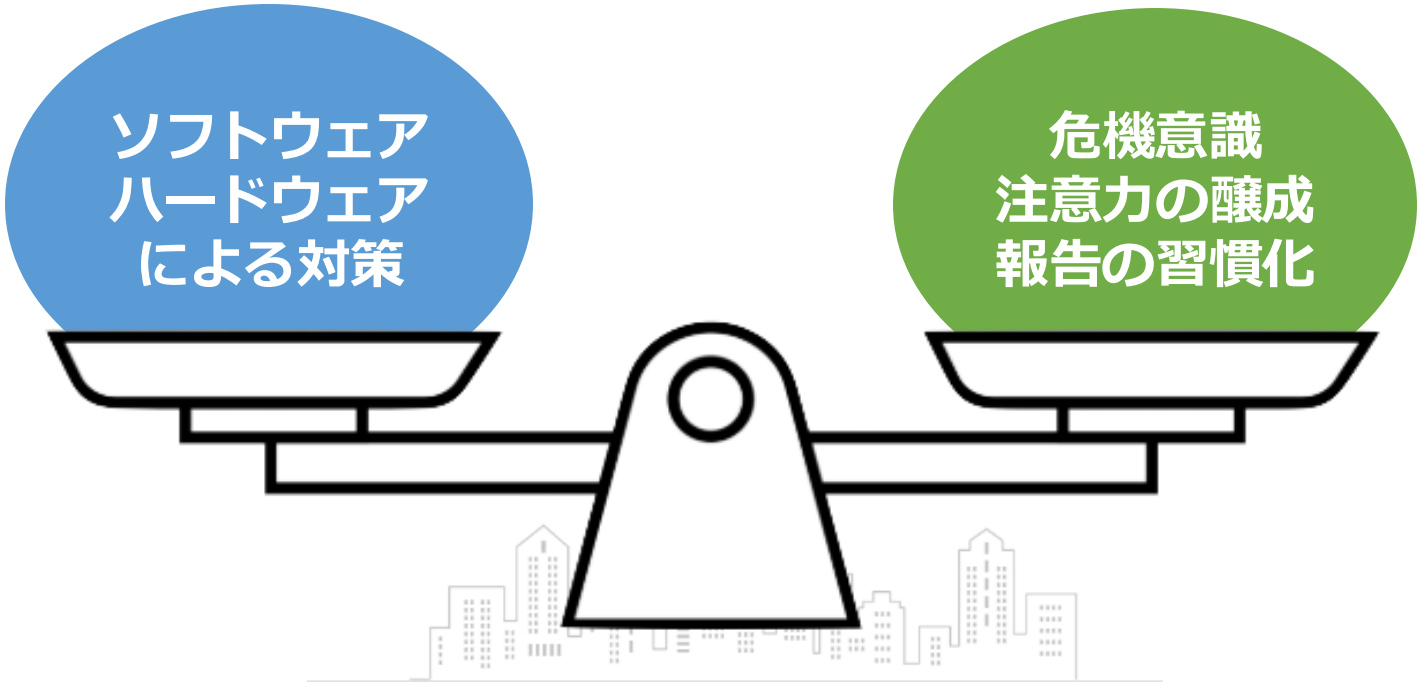
令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）より

どれだけお金をかけて対策をしても、使う「人」の

「ついうっかり」や「不注意」で、

「知らなかった」「気づかなかった」

では済まされない、重大なサイバーインシデントに発展します！



不正メール訓練サービス
「Mail Fort Insight」

apsc.jp

従業員の１クリックで
会社の未来が吹き飛ぶ可能性があるとしたら
そのリスク、放置できますか？

そんなリスクをより低くさえるためのお手伝い

それが、改善コンサルティング付き不正メール訓練サービス

「Mail Fort Insight」です！

apsc.jp

～ 全社的なサイバーリスク耐性の底上げ ～

- 不審なメールの開封率を下げる
- セキュリティ意識の向上
- 開封後の初動を確認
- インシデント通報習慣の定着
- 不正メールに対するアンテナ強化

従業員の危機意識が高まれば、あなたの会社を不正メールから守る「砦」となるでしょう！

Mail Fort Insight の概要

apsc.jp

①「擬似不正メール」を一斉配信

②訓練後、対象者にアンケート

③結果を元に改善コンサルティング

状況に応じて「情報セキュリティ研修」の追加も可能

「Mail Fort Insight」の特徴１

apsc.jp

訓練だけで終わらせない！　改善に導く“本気”の訓練「Mail Fort Insight」

多くのサービスは
ここまでで終わり

**実はこちらの方が
とても重要**

- 訓練メールの実施
- 訓練結果レポート
- 事後アンケートの実施
- アンケート結果分析
- 改善コンサルティング
- 情報セキュリティ研修（※）

**「Mail Fort Insight」は
これらをワンパッケージで
ご提供いたします！**

※ 情報セキュリティ研修はオプションです。
講師は、警視庁、愛知県警察、京都府警察などとコラボした
セミナーの登壇経験のあるプロフェッショナルです！

「Mail Fort Insight」の特徴２

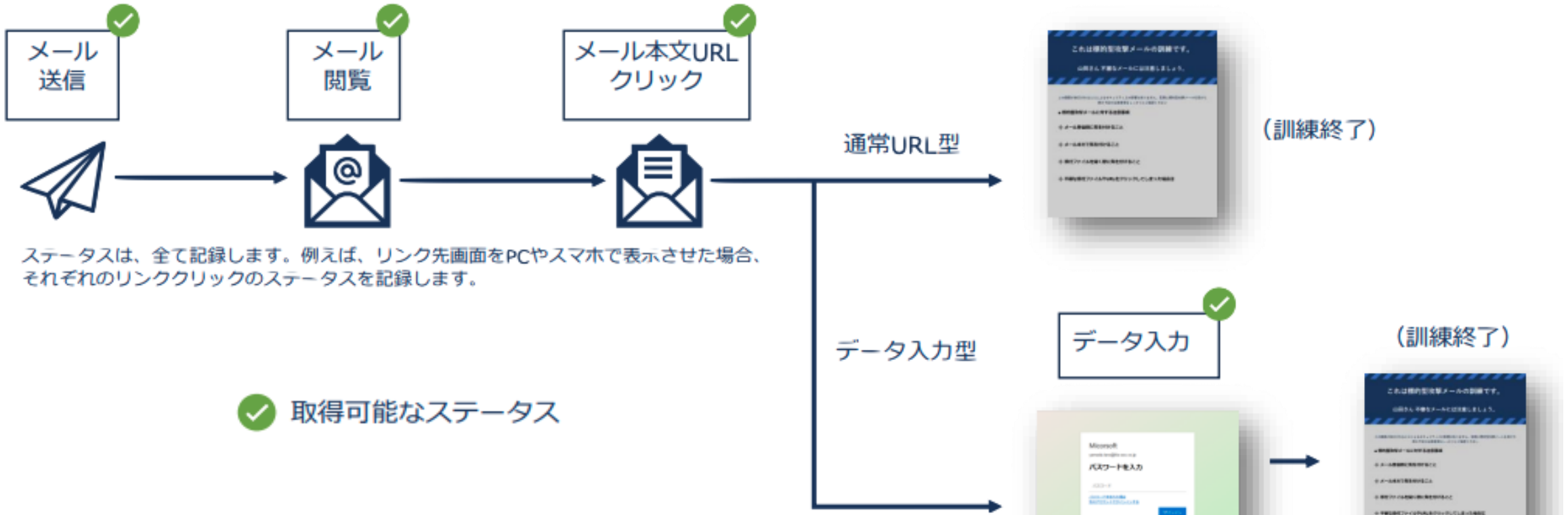
apsc.jp

メール送信数	予めご契約いただいた件数、上限なし
メールの種類	クリック型 添付ファイル型 ハイブリッド型 QRコード型
メールテンプレート	２００種類以上ご用意
トライアル	10通の無料トライアルあり
レポート提出	メール開封、リンククリック、添付ファイル開封などの数、割合、人の特定
事後アンケート	詳細は別ページをご参照ください
改善コンサルティング	詳細は別ページをご参照ください

「Mail Fort Insight」リンククリック型

apsc.jp

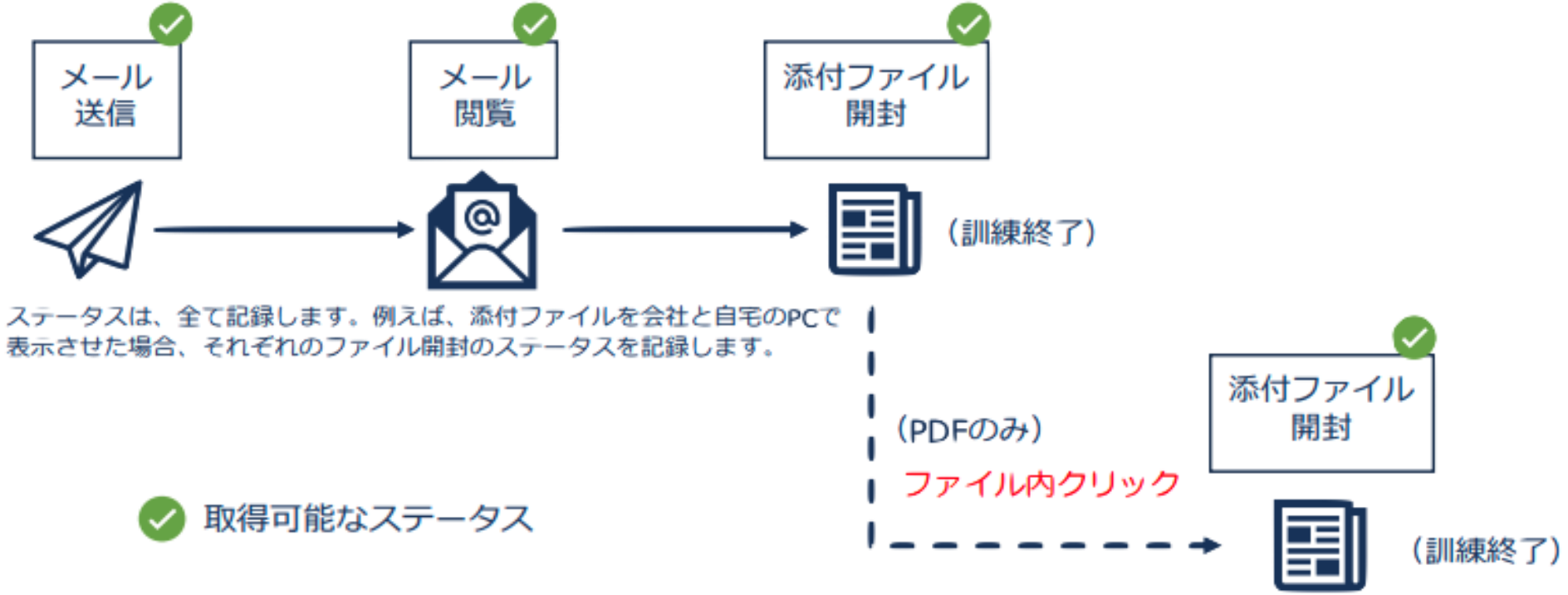
偽サイトへ誘導し、個人情報やID /パスワードを窃取することを目的とした攻撃



「Mail Fort Insight」添付ファイル型

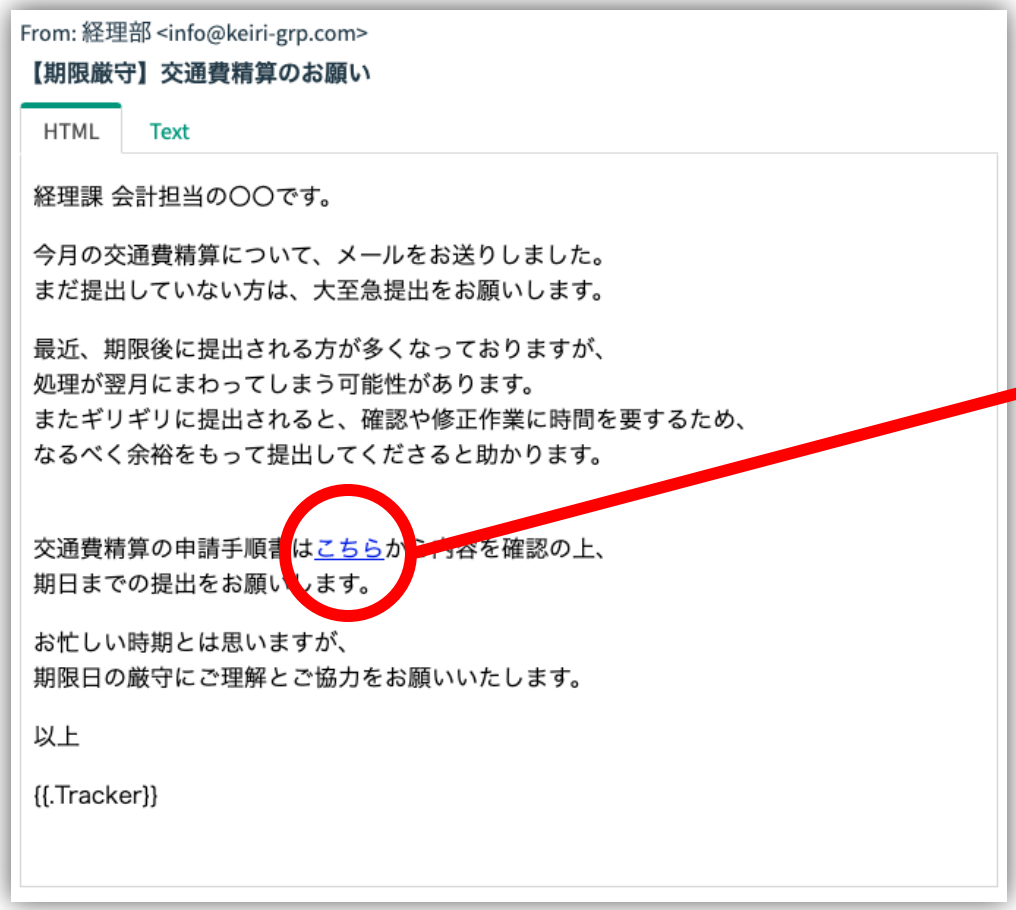
apsc.jp

ウィルスを仕込んだ添付ファイルを送信し、直接ウィルス感染させることを目的とした攻撃

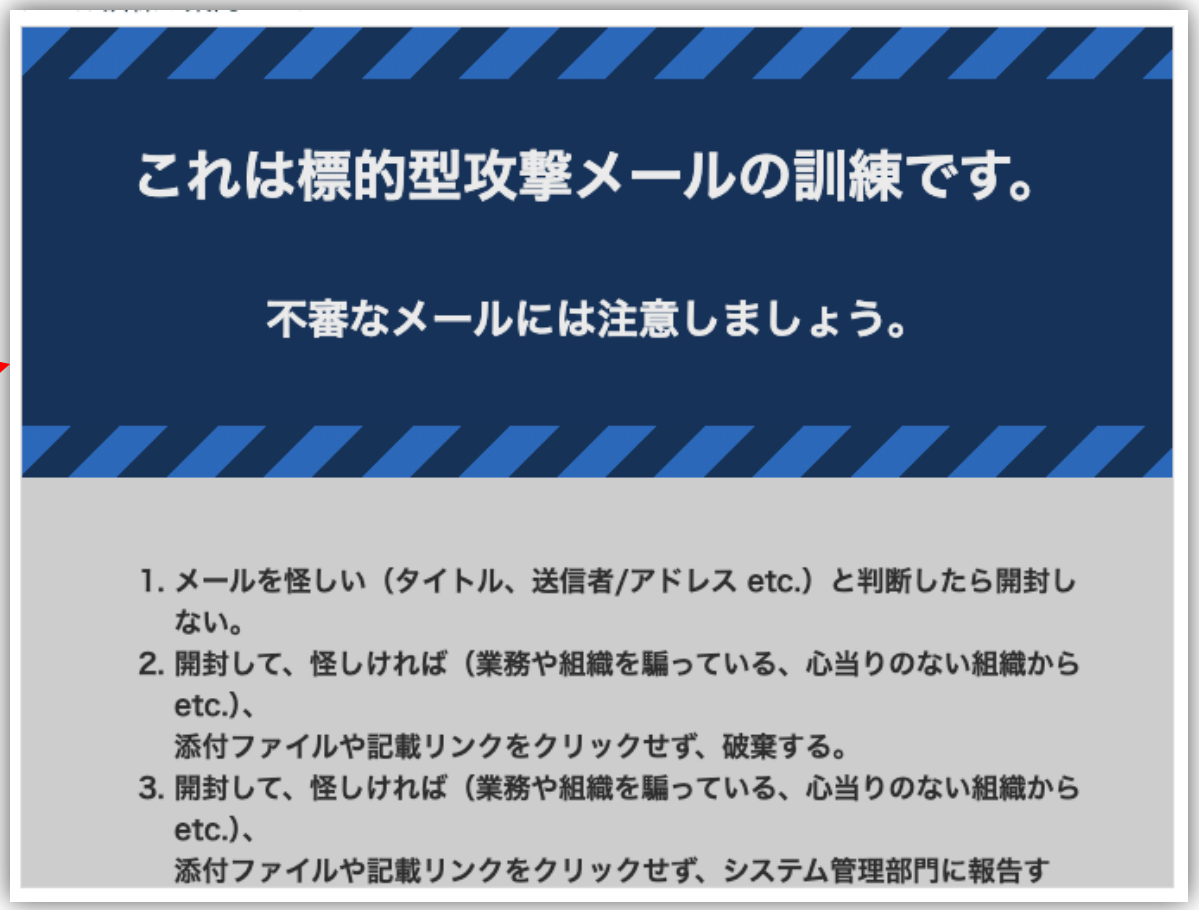


「Mail Fort Insight」訓練メールの例１

apsc.jp



内容の編集可能



内容の編集可能・リンク先URL変更可能

「Mail Fort Insight」訓練メールの例２

apsc.jp

●●健康保険組合 被保険者の皆様へ

2024年12月2日より、健康保険証の新規発行は中止し、
マイナ保険証を基本とする仕組みに移行しました。

医療機関・薬局に行かれる際は、ぜひマイナ保険証をご利用ください。

！医療機関・薬局の受付で使用するカードリーダーの不具合などにより
マイナ保険証での受付が上手くいかなかった場合に10割負担になるのでは、
と不安を感じている方がいらっしゃいますが、他の手段で資格確認を行うため、
医療費が10割負担になることはありません。！

■マイナ保険証移行手順
マイナンバーカードの保険証利用について（被保険者証利用について）

厚生労働省

[トラッカー]

内容の編集可能

！コンピュータでウイルスが確認されました！

16%

08:27

表示時間内にセキュリティソフトをインストールして、不正プログラムの無害化を行えば、被害を最小限に抑えられます

！私のコンピュータに何が起こったのですか?

ファイルの使用停止、あるいは外部へ流出している記録があります。放置すると被害が大きくなる可能性があります。

！ファイルを回復できますか?

セキュリティソフトのインストールにより元の状態に回復させることができます。

できるだけ早くインストールして不正プログラムを停止してください。

インストール

内容の編集可能

⚠これは標的型攻撃メールの訓練です⚠

不審なメールには注意しましょう。

実際に標的型攻撃メールを受けた際の下記の注意事項をしっかりとご確認ください。

■ 標的型攻撃メールに対する注意事項

1. メール受信時に気を付けること

送信者アドレスが通常と違うアドレスもしくは 似せたアドレスでないことを確認してください
例：Microsoft社からのメールなのにgmail等関連性がないメールアドレス、Micorsoftなどスペルが違う似せたメールアドレス

2. メール本文に気を付けること

通常のメールに精密に似せた内容のメールが多くなってきています。本文に不審な点がないかを確認してください
例：日本語に違和感がある場合や、むやみにログインを要求してくる

3.ログイン先で気を付けること

メールに記載されたURLをクリックすると、精密に似せた偽ログインサイトの場合があります。ログインする場合は検索エンジンでサービスを検索して検索エンジン経由のサイトからログインすると安心です
例：ログイン画面がいつもと違う、ロゴマークの画質が荒いなど

4.不審な添付ファイルやURLをクリックしてしまった場合は

⚠不審なURLをクリックした。不審なサイトでID,パスワードを入力してしまった。不審な添付ファイルをクリックした、添付ファイルのマクロを有効化した場合は速やかにIT部門に連絡してください

内容の編集可能
リンク先URL変更可能

「Mail Fort Insight」訓練メールの例３

apsc.jp

社員各位

お疲れ様です。情報システム部の〇〇です。

情報システム部より「大至急」のご連絡です。

本日午前中に社内のPCが数台感染しているとの報告を受け
現在復旧作業中です。

そこで、被害を最小限に抑えるため、現在使用中のPCについて以下の
対応をお願いします。
＊＊＊社員全員の方々が対象です。＊＊＊

■ウィルスチェックを行う
感染していないかどうかを確認するためです。
（不在の方のPCや部門で共用しているPCについてもご協力願います）

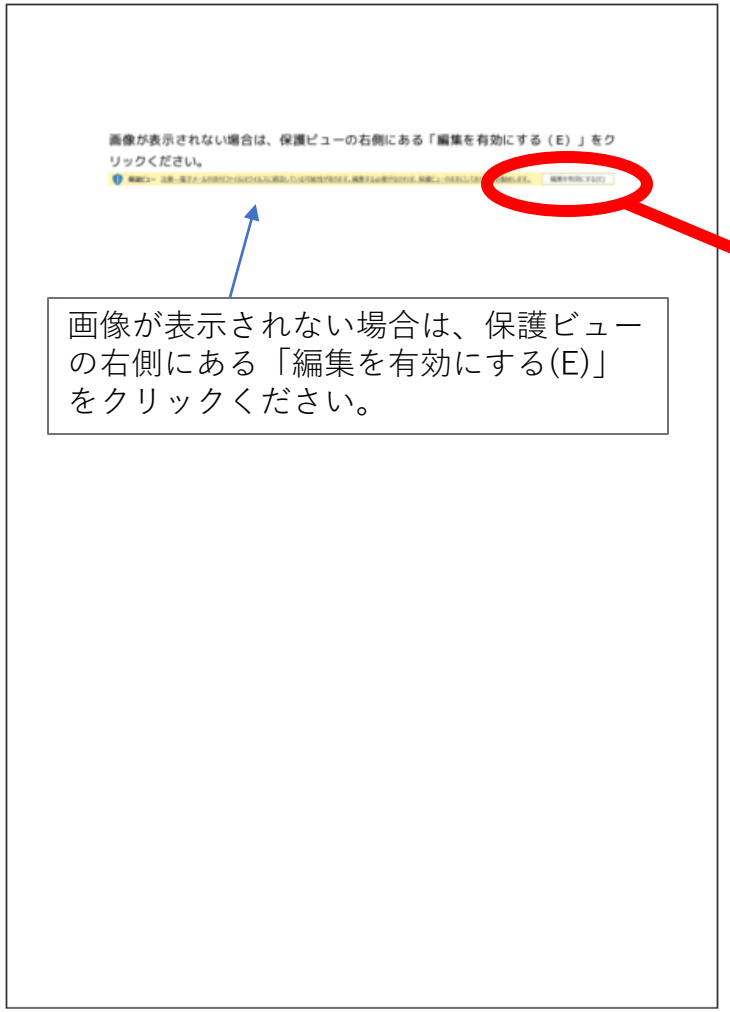
チェック方法は添付ファイルを参考にして下さい。
↓
PCのウイルスチェック手順.docx

チェック後、感染していなければここで終了ですが、
感染していた場合は、情報システムまで報告をお願いします。

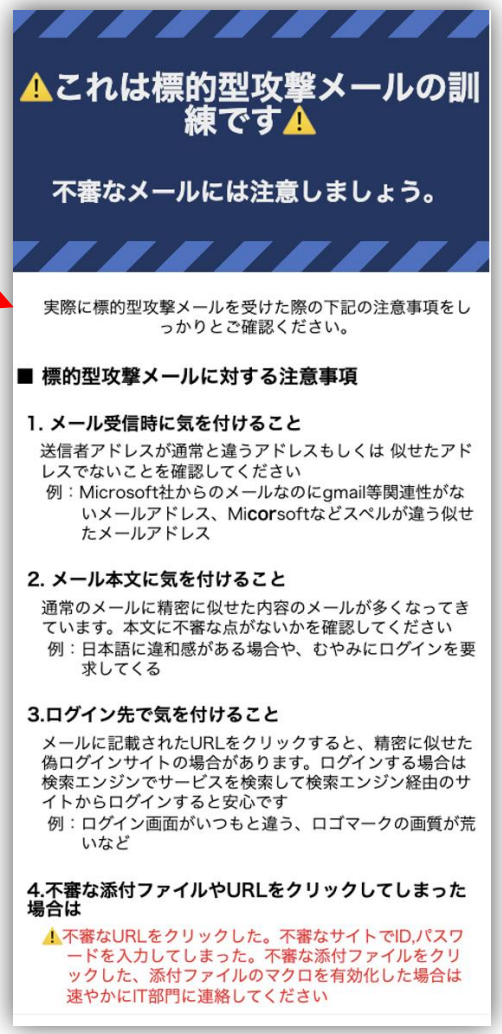
以上

[トラッカー]

内容の編集可能



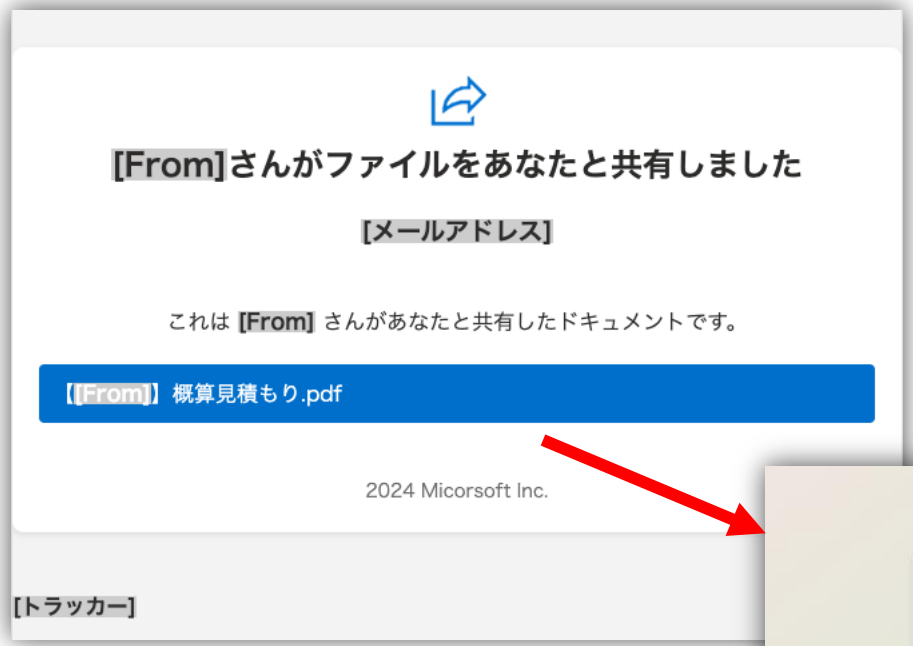
オリジナルファイルへ変更可能



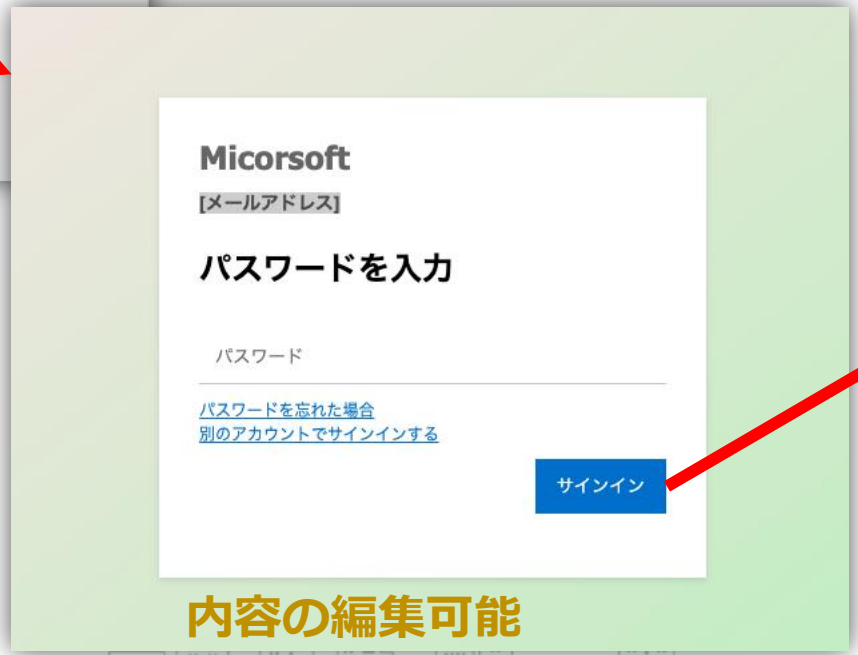
内容の編集可能
リンク先URL変更可能

「Mail Fort Insight」訓練メールの例４

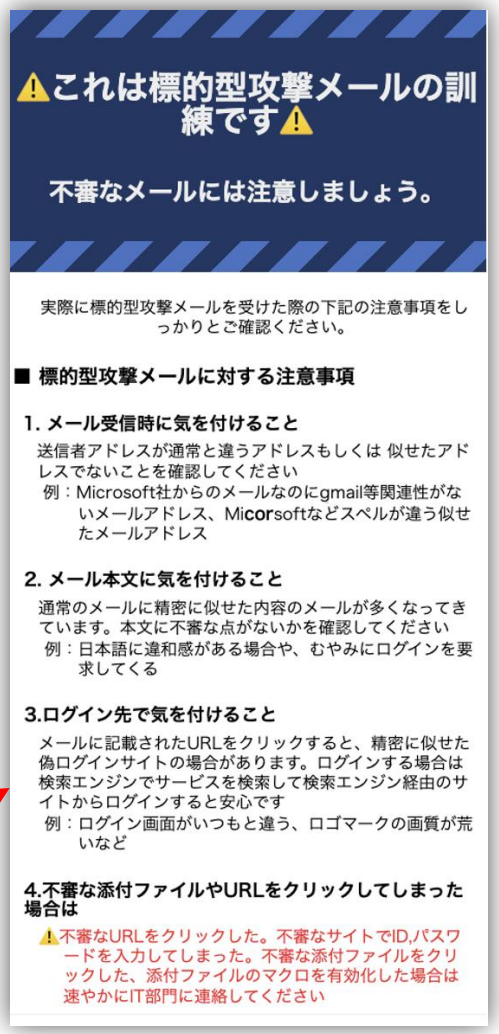
apsc.jp



内容の編集可能



内容の編集可能



内容の編集可能
リンク先URL変更可能

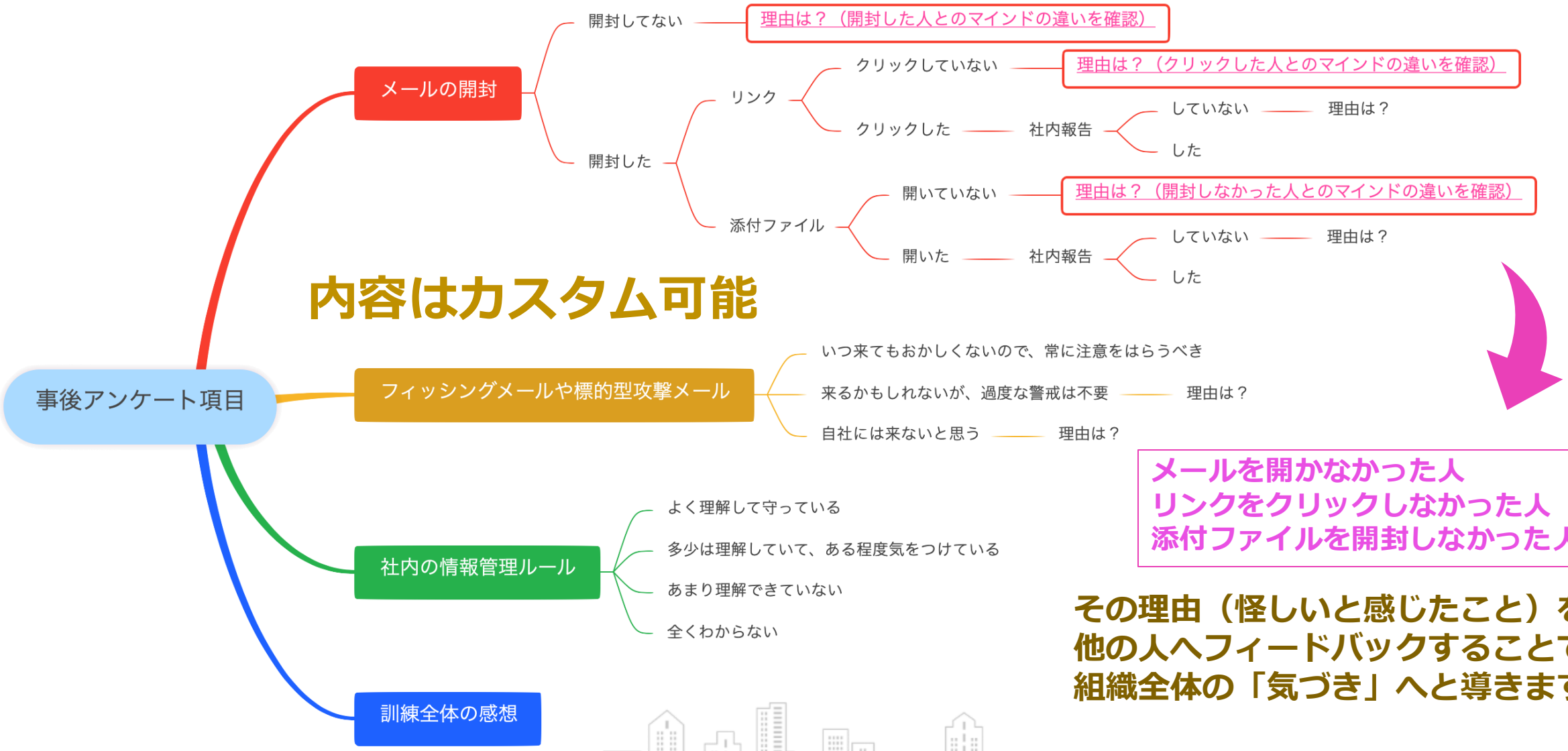
「Mail Fort Insight」実施の流れ

apsc.jp

1	**お打ち合わせ**	お客様／弊社	本サービスのご提案、実施時期等のお打ち合わせを行います。
2	**お申し込み**	お客様	お申込書をご提出いただきます。
3	**対象者選定**	お客様	対象者の氏名、所属部署、メールアドレスを抽出して頂きます。
4	**テストメール送信**	弊社	受信テストです（M365、Googleworkspaceなどは、一部設定が必要です）
5	**訓練メール配信**	弊社	予定の配信日時に一斉に送信します。訓練期間は3～5日間で設定します。
6	**結果レポート提出**	弊社	訓練結果のレポートをご覧いただきます。
7	**対象者へ事後アンケート**	お客様／弊社	訓練対象者に事後のアンケートを実施します。
8	**アンケート結果集計**	弊社	回答の内容を集計、分析いたします。
9	**改善コンサルティング**	お客様／弊社	メール訓練およびアンケートにより顕在化した課題について、改善策や今後の社員教育についてのコンサルティングやご提案をさせて頂きます。ご案内した内容を実施するかどうかは、お客様のご判断となります。

「Mail Fort Insight」アンケートについて

apsc.jp



内容はカスタム可能

メールを開かなかった人
リンクをクリックしなかった人
添付ファイルを開封しなかった人

その理由（怪しいと感じたこと）を
他の人へフィードバックすることで、
組織全体の「気づき」へと導きます

改善コンサルティング

apsc.jp

1、メール訓練およびアンケート結果から、インシデント発生危険度を数値で評価

メール開封率・リンククリック率・添付ファイル開封率を総合評価（下記は評価例）

80点以上・・・危険度MAX 今すぐ追加の対策を

10点以下・・・非常に優秀、リスクはかなり限定的だが、注意は必要

2、改善すべき点や、今後検討すべき施策などについてコンサルティング

- 社内ルールや規程の見直しは必要か？
- 追加の研修は必要か？
- 定期的なメール訓練を実施すべきか？
- インシデント発生シナリオの作成は必要か？
- 現状のサイバーセキュリティ対策は必要十分か？
- その他

ご提供価格（税別）

apsc.jp

メール送信数	Mail Fort Insight基本料金	送信単価
10通以下	100,000円	ー
11～50通	130,000円	350円
51通以上	130,000円＋260円×（送信数−50）	350円

50通の場合・・・130,000円＋350円×50通＝**147,500円（1通あたり 2,950円）**
100通の場合・・・130,000円＋260円×(100-50)+350円×100通＝**178,000円（1通あたり 1,780円）**
300通の場合・・・130,000円＋260円×(300-50)+350円×300通＝**300,000円（1通あたり 1,000円）**
500通の場合・・・130,000円＋260円×(500-50)+350円×500通＝**422,000円（1通あたり 844円）**

事後アンケート＋改善コンサルティング付きでこの価格！

業界最安値です！ （当社しらべ）

apsc.jp

1ヶ月に1社限定！

下記3つの条件全てに当てはまる法人様へ　10通無料トライアル！

- ✓ 弊社サービスを初めてご利用
- ✓ 30名以上の訓練メール送信先がある
- ✓ トライアル終了後、弊社サービスのご提案の機会をいただける

さらに・・・トライアル終了後、

「Mail Fort Insight + 情報セキュリティ研修」セット申込で **10%OFF**

情報セキュリティ研修（オプション）

apsc.jp

「Mail Fort Insight」訓練メール実施
→ 従業員の意識の高まり
→ 組織としての課題が明確に

情報セキュリティ研修の実施

サイバーリスク耐性の底上げには、非常に効果的です

- 日本におけるサイバー攻撃の現状
- 自社が保有する情報資産とは？
- ランサムウェア被害の実態
- 同業他社のインシデント例
- グループディスカッション
- サイバー攻撃の最新動向
- 明日から無料でできる日常対策

・90分間のオンライン研修
・内容は、お客様の課題に合わせてカスタム
・参加型で飽きない研修スタイル
・メール訓練の振り返り、気づきの共有
・研修は全て録画、貴社の資産として二次利用可能

150,000円～（税別）

「Mail Fort Insight」のお問い合わせは下記まで

一般社団法人 中小企業をサイバー攻撃から守る会

Association to Protect SMEs from Cyberattacks

office@apsc.jp