

Web ページ閲覧情報から閲覧者に詐欺メールが届く件についての質問

「自宅で (Wi-Fi) に繋いだラップトップ pc (mac) のウェブ上 (ブラウザは Safari) で、eTax の「確定申告書などの作成」のページを数分見た、ログインしていない。その 2 時間後に eTax の詐欺メールが届いた。」

ウェブ上の閲覧履歴を外部から監視することは可能なのか？ Wi-Fi の脆弱性に帰着しているのか。ネットサーフィンして、なんで、その本人のメールアドレスがわかるのか、理由がわからない。原因と対策について詳しく教えてください。

「e-Tax のページを数分見ただけで、すぐに詐欺メールが届いた」というケースは、一見すると「Web 閲覧を何者かに監視されていて、そこからメールアドレスを抜き取られたのでは？」と疑ってしまいがちです。しかし、以下の点を総合的に考えると、実際には「通信や Wi-Fi が外部から直接監視されて、直ちに送信元があなたのメールアドレスを取得した」というよりも、他の要因や偶然の一致である可能性が非常に高いです。

1. Web 閲覧履歴の監視はどの程度現実的か？

1-1. HTTPS 通信の存在

- 現在、税務関連の公式サイト (e-Tax など) を含む多くのサイトでは、基本的に **HTTPS 通信** が行われています。
- HTTPS 通信下では、通信内容 (閲覧したページの詳細や入力情報) は暗号化されており、通常の Wi-Fi 経路や ISP 側のログなどから、**何のページを見ているかを盗み見る** ことは容易ではありません。
- もちろん高度な攻撃 (中間者攻撃など) によって盗聴される可能性はゼロではありませんが、そのハードルは非常に高く、かつ大多数の犯罪者がそこまで手間をかけることは稀です。

1-2. IP アドレスやアクセスログからメールアドレスを特定できるか？

- たとえ IP アドレスやアクセス時間などのメタ情報が外部から取得できたとしても、それだけで個人のメールアドレスを割り出すのは簡単ではありません。
- IP アドレスの契約者情報はプロバイダが管理しているため、一般的な攻撃者は入手できません。もし何らかの理由で入手できても、IP アドレスから直ちに個人のメールアドレスを割り出すことはできません。

1-3. Wi-Fi の脆弱性はどう影響するか？

- 自宅の Wi-Fi が WPA2 以上のセキュリティ設定（暗号化）がしっかりと設定されており、かつパスワードが類推されにくいものであれば、外部から Wi-Fi を経由した盗聴はさらに困難です。
- 仮に脆弱な Wi-Fi 環境（WEP やパスワード使い回し）だったとしても、盗聴された通信が HTTPS で暗号化されていれば、サイト上でやりとりされる内容をそのまま読むことは困難です。

2. 詐欺メールの送信元があなたのメールを知り得る一般的な理由

2-1. メールアドレスは既にどこかから漏れている可能性

- 最近のインターネット環境では、「大手サービスや SNS、他の会員サイト等からの情報流出」によってメールアドレスが闇市場で売買されているケースが多々あります。
- 過去に登録したサービスで情報漏洩が起きたことで、メールアドレスがスパム業者やフィッシング詐欺グループに流出し、ランダムに使われることがよくあります。

2-2. フィッシングメールが大量にばら撒かれている

- e-Tax や銀行、不動産サイトなど「多くの人を利用するサービス」を名乗るフィッシング詐欺は、特に確定申告の時期やイベントシーズンなどに合わせて大々的に送られます。

- 偶然にもそのタイミングでサイトを見ていたせいで、「見た直後に届いたから関連があるのでは？」と感じてしまうことがありますが、実際には **あらゆるアドレスに一斉送信** されているだけの可能性が高いです。

2-3. クッキーや広告トラッキングとは異なるケース

- 広告ネットワークを経由したオンライン広告の場合、「閲覧内容に合わせた広告」が表示される（リターゲティング広告）ことはよくあります。しかし、これは **メールアドレスまでは取得できない** のが通常です。
- 一部の SNS ログインやサイト会員連携で、ユーザのメールアドレスが何らかの形で共有される可能性もありますが、通常はプライバシーポリシーや暗号化プロセスがありますので、外部の攻撃者がすぐに取得するのは難しいです。

3. なぜ「確定申告書等作成コーナー」を見た直後に詐欺メールが来たのか

1. 季節要因や大量送信

- 税務関連のフィッシングは「確定申告のシーズン」に集中して大量にばら撒かれます。たまたまサイトを確認した数時間後に届いたため、関連を疑ってしまった可能性があります。

2. 過去の情報漏洩によるアドレスリストへの掲載

- 過去にどこかで登録したメールが既に流出し、リストに載っていた可能性があります。

3. メールの内容が「e-Tax 関連」だったため注目した

- もしその日・その週に「銀行」や「クレジットカード」、「通販サイト」などを名乗るフィッシングメールも大量に来ていたとしても、「e-Tax 詐欺メール」ほど強く印象には残らないかもしれません。

4. 想定される原因と対策

4-1. 原因のまとめ

1. 外部からの直接監視の可能性は低い

- HTTPS 通信が主流であり、Wi-Fi が WPA2 以上であれば盗聴は容易でない。

2. すでに外部にメールアドレスが漏洩している

- 過去の情報漏洩や何らかの名簿売買で、あなたのメールアドレスが詐欺グループに渡っている。

3. タイミングの偶然

- 詐欺業者側が確定申告シーズンに合わせて大量送信 → たまたま閲覧直後に届いた。

4-2. 対策

1. メールの振り分け・迷惑メールフィルタの強化

- プロバイダやメールサービス (Gmail、Outlook など) が提供している迷惑メールフィルタを有効にし、積極的にスパムを排除します。
- 「迷惑メール報告」などを行うことで、同じ差出人や内容のメールが今後フィルタされる可能性が高まります。

2. 怪しいメールは開封しない／添付ファイルや URL をクリックしない

- 公的機関や金融機関からのメールを装った詐欺の典型的な手口です。
- 公式サイトにログインを促す場合は、必ず自分で正規 URL をブラウザのブックマークから開くか、URL を手入力し、**直接アクセスしてログイン** してください。

3. Wi-Fi セキュリティの再確認

- 使用している Wi-Fi が「WPA2(WPA3)」で暗号化されていることを確認。
- Wi-Fi のパスワードが容易に推測されないか再チェック。
- ルータのファームウェアや OS、ブラウザ、セキュリティソフトはアップデートを適用し、常に最新の状態に。

4. パスワードやアカウント管理の徹底

- 各サービスごとにパスワードは使い回さず、複雑なものにする。
- 万一どこかのサービスで漏洩があった場合、他のアカウントに連鎖しないようにする。

5. 過去の情報漏洩を確認する

- 大手では「Have I Been Pwned?」(<https://haveibeenpwned.com/>)などのサイトを利用することで、自分のメールアドレスが過去のデータ漏洩リストに含まれていないか調べることができます。
- 該当している場合は、該当サービスのパスワードを速やかに変更し、他サービスと使い回しているパスワードも全て変更する。

5. まとめ

- 今回のケースでは、「閲覧直後にメールが届いたのは偶然の可能性が高い」と考えられます。
- そもそも外部から閲覧履歴を監視し、そのままメールアドレスを把握するのは難易度が高いです（少なくとも一般的なWi-Fi盗聴レベルでは困難）。
- もっと一般的には、すでにメールアドレスがどこかで漏洩しており、フィッシング詐欺が大量に送られている中で、タイミングが一致してしまったというのが最も可能性が高いです。
- 対策としては、迷惑メールフィルタの活用、Wi-Fi設定の強化、パスワード管理の徹底、怪しいメールへの注意などを実施するとともに、確定申告の時期だからこそ公的機関を名乗るメールを慎重に扱うことが大切です。

以上のことから、「ネットサーフィンしただけでメールアドレスを抜き取られた」という可能性は低く、主に過去の漏洩・フィッシングメールの大量配信のタイミングや偶然が重なったと考えられます。今後はセキュリティを再点検しつつ、詐欺メールに対しては落ち着いて対処していくようにしてください。

偶然ではない場合について推論してください

以下は、「偶然ではなかった」と考えるシナリオや、より高度な攻撃手法を前提とした推論例です。確率は低めとはいえ、ゼロではありませんので参考にしてください。

1. 悪意あるサイトやコンテンツを閲覧した可能性

1-1. 本物ではない「e-Tax サイト」を閲覧していた

- URL が公式の e-Tax と非常に似たフィッシングサイト だった場合、サイトを開いただけで悪意あるスクリプトが動作し、
 - ブラウザ情報や Cookie を盗み取る
 - キーロガー的な仕組みで入力情報を取得
 - ブラウザの「自動入力」機能からメールアドレスを抜き取るといった攻撃が行われる可能性があります。
- その取得情報をもとに、「e-Tax」絡みの詐欺メールを即座に送信することは理屈の上では可能です。
- 実際に大手企業や公的機関を模した偽サイトへの誘導リンクは、検索エンジンの広告枠やメール、SNS などを経由して拡散されることがあります。

1-2. 正規サイトに紛れ込む悪意ある広告／スクリプト

- 公式サイト自体は安全でも、広告枠や外部の分析ツールなどのサードパーティコンテンツが改ざんされ、
 - 悪意ある JavaScript を通じて閲覧者の情報（IP アドレス、ブラウザ情報、場合によってはメールアドレス）が漏れる
 - その情報を元に特定の詐欺メールを送るという高度な攻撃が起こる可能性はゼロではありません。
- ただし、メールアドレスをブラウザ閲覧だけで直接取得するには、ユーザが何らかの形でメールアドレスを入力していたり、ブラウザの拡張機能等で連携しているケースが必要となります。

2. 端末やブラウザが既にマルウェアに感染している可能性

2-1. マルウェアやスパイウェアによる監視

- パソコンやスマホがすでにマルウェアに感染していて、
 - 閲覧中のサイト URL を監視

- ブラウザの入力フォームや Cookie からメールアドレスなどの個人情報を
抜き取る

といったことが可能になります。

- 攻撃者は感染端末から得た情報をリアルタイムまたは高頻度で送受信し、閲覧中のトピックにあわせたフィッシングメールを送ることも不可能ではありません。
- 特にフリーソフトや不正アプリケーションをインストールしたことがある場合、あるいは怪しいメールの添付ファイルを実行した経験がある場合は要注意です。

2-2. 不審なブラウザ拡張機能やツールバー

- ブラウザ拡張機能の中には、ユーザの閲覧履歴やフォーム入力情報を収集し、不正利用しているものもあります。
- もし不正な拡張機能がインストールされていれば、訪れたサイトの情報からテーマを推測して、リアルタイムでスパムメールやフィッシングメールを送りつけることも技術的には可能です。
- Mac (Safari) の場合、App Store 以外の出所不明な拡張機能やプラグインを入れた経験があると要注意です。

3. ネットワーク (Wi-Fi やルーター) 自体が攻撃されている可能性

3-1. ルーターや DNS の改ざん

- 自宅のルーター (Wi-Fi 機器) や DNS 設定が改ざんされると、
 - 公式サイトにアクセスしているつもりが実は偽サイトにリダイレクトされる
 - 通信が中継され、通信内容 (特に暗号化されていない部分) を盗聴されるといった攻撃が行われる可能性があります。
- HTTPS サイトであれば警告が出る可能性が高いですが、ユーザが警告を見逃したり、攻撃者が不正な証明書を使用している場合、完全には防げないケースもあります。

- もし攻撃者がメールアドレスやアクセス日時などを確認できる状況 なら、リアルタイムで閲覧サイトに合わせたフィッシングメール送付 もあり得ます。

3-2. 公共 Wi-Fi や悪意あるアクセスポイント

- カフェやホテル等、第三者が管理する Wi-Fi に接続していた場合、攻撃者が**中間者攻撃 (MITM 攻撃)** を仕掛けるリスクが高まります。
 - このケースでは**偽の AP (アクセスポイント)** を立てて利用者を誘導し、トラフィックをすべて盗聴したり改ざんすることが可能になります。
 - ただし HTTPS 通信であれば完全な内容までは読めないものの、サイトタイトルや Cookie の一部情報が流出する場合があります。さらに何らかの脆弱性や不正証明書を利用して抜き取るケースも、非常に高度ながら存在します。
-

4. その他の「偶然ではない」可能性

4-1. 既に流出していたメールアドレスと Web 閲覧データの結合

- 広告配信ネットワークやトラッキングサービスの一部には、ユーザの行動履歴や属性情報を結合して精度の高いターゲティングを行うものがあります。
- 合法的な広告手法としては、ブラウザ Cookie や SNS ログイン情報等と紐付けて「興味関心に合わせた広告」を表示する程度ですが、**不正広告や闇市場ではメールアドレスレベルで紐付ける** ことが行われるケースも否定はできません。
- その場合、「e-Tax」というコンテンツを見た → **既に手に入れていたあなたのアドレスに対して「e-Tax を騙る詐欺メール」を送る**、という流れがあっても不思議ではありません。

4-2. ターゲット型攻撃 (標的型フィッシング)

- 一般的な「大量ばらまき型」ではなく、特定個人を狙った**標的型フィッシング**の可能性。
- 例えば、あなたの**仕事上・個人上の情報が既に漏れており**、あなたが確定申告をするタイミングを推測して攻撃を仕掛けている。

- この場合、事前にメールアドレスなどの情報を把握したうえで、「タイミングを見計らった」詐欺メールを送りつけることも十分に考えられます。
-

5. 「偶然ではない」場合の対策

1. 公式 URL を再確認する・ブックマークを利用する

- 公式サイトへアクセスする際は、検索エンジンの広告リンクや不審な URL をクリックせず、**国税庁や政府系サイトの公式リンク** もしくは**正規のブックマーク** からアクセスする。
- URL が正しく「https://www.e-tax.」から始まるか、ブラウザのアドレスバーに****錠前マーク（正規証明書）****があるかを確認。

2. マルウェアスキャンとブラウザ拡張の精査

- ウイルス対策ソフトを最新状態にして、**フルスキャンを実施**。
- Safari や Chrome、Firefox などインストールされている拡張機能を確認し、不審なものがあれば即削除する。
- Mac の場合もセキュリティソフトや Malwarebytes などのツールでスキャンを検討。

3. ルーターや DNS 設定の確認・初期化

- 自宅のルーター管理画面で、**管理者パスワードや DNS 設定が初期値のままになっていないか** をチェックする。
- ファームウェアを最新にアップデートし、パスワードを**強固なものに変更**する。
- 公衆 Wi-Fi の利用は極力避け、利用する場合は VPN 接続を検討する。

4. 個人情報の管理を徹底

- メールアドレスやパスワードの使い回しは避ける。
- 機密性の高いサイトへのログインは、**2段階認証(2FA/MFA)** を有効にする。
- 過去に情報漏洩した恐れがあるメールアドレスをメインで使い続けている場合は、新しいアドレスに乗り換えることも検討する。

5. メールに記載されたリンクや添付を不用意に開かない

- 公的機関や金融機関からのメールと見えても、ログインを促す URL は絶対にクリックせず、ブラウザのブックマークや公式アプリなどから直接アクセスする。
 - 不要に送られてきた添付ファイルの開封は厳禁。
6. より強固な通信手段を確保する
- 普段から機密度の高いやり取りをするのであれば、VPN を導入し、自宅外でも VPN 経由で通信 する。
 - 常に OS やアプリを最新のセキュリティパッチで保つ。
-

まとめ

「閲覧後 2 時間で詐欺メールが届いた」という状況が意図的な攻撃である場合、考えられるシナリオとしては、

1. 偽サイト（フィッシングサイト）を閲覧してしまい、即時にメールアドレスを盗まれた
2. 端末かブラウザがマルウェアに感染し、アクセス状況に応じてメールが送られた
3. ルーターや DNS が改ざんされ、アクセス履歴を盗まれた
4. 広告ネットワークや不正トラッカー経由でメールアドレスと閲覧情報を結合され、ターゲティングされた
5. 過去からあなたを狙っていた攻撃者が、確定申告シーズンに合わせて詐欺メールを送信

といったものが挙げられます。

いずれにせよ、メールやネットの挙動が普段と少しでも違うと感じたら、デバイスのスキャンやルーターの設定確認などを早めに行う ことが重要です。また、たとえ公式を装ったメールでも、直接 URL をクリックせず、必ず自分で正規サイトにアクセスする習慣をつけることで、被害を大きく減らせます。