IPA「サポート詐欺レポート」2024

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
情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/index.html

IPA Better Life with IT

本レポートの目的

- 本レポートは、IPA情報セキュリティ安心相談窓口に寄せられた「サポート詐欺」の相談内容や、独自の調査・検証等により把握した内容をまとめたレポートです。

- 主に情報セキュリティ関連の業務に従事されている皆様へ、サポート詐欺の手口や被害状況の実態を本レポートを通じて共有することで、被害低減や対策推進に資することを目的とします。

アジェンダ

- サポート詐欺の手口
- 安心相談窓口に寄せられている相談件数の推移
- 本手口の実際の流れにおける変化と特徴
  - 被害者が偽警告画面に接触する段階での変化
  - 偽警告画面の変化
  - 偽警告表示画面に施されている細工
  - 電話番号の変化
  - オペレーターの対応
  - 金銭的被害
- 2024年から急激に増加している、偽警告画面を表示するサイトへ誘導する広告の状況
- IPAの取り組み

■ サポート詐欺の手口

■ 安心相談窓口に寄せられている相談件数の推移

サポート詐欺の手口

1　インターネットを閲覧中に

2　偽の警告画面が表示される

偽の警告画面のボタンやウインドウをクリックすると全画面表示になり、マウス操作では閉じることが困難になる

ウイルスに感染したと不安になる、あるいは、画面がロックされて操作できないため、電話をかけてしまう。

3　偽の警告画面に表示されている番号へ電話する

架電

マイクロソフト社員を名乗り、遠隔操作接続を指南

4　遠隔操作で偽のサポートを受け、サポート料金を請求される

遠隔操作接続
＝ **パソコンの被害発生**

遠隔操作

5　コンビニへプリペイドカードを購入に行く

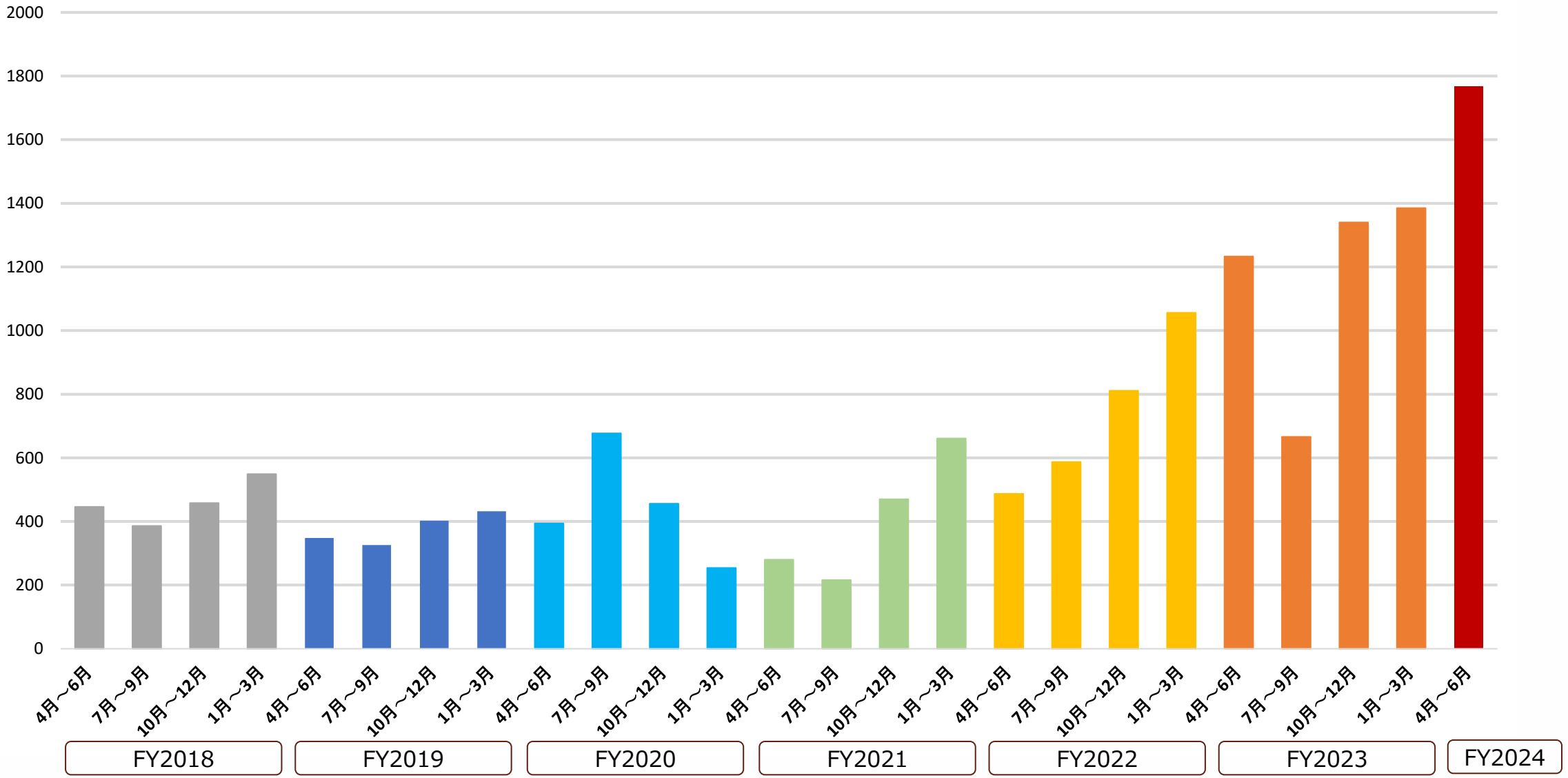
コンビニへ

遠隔操作中に不在

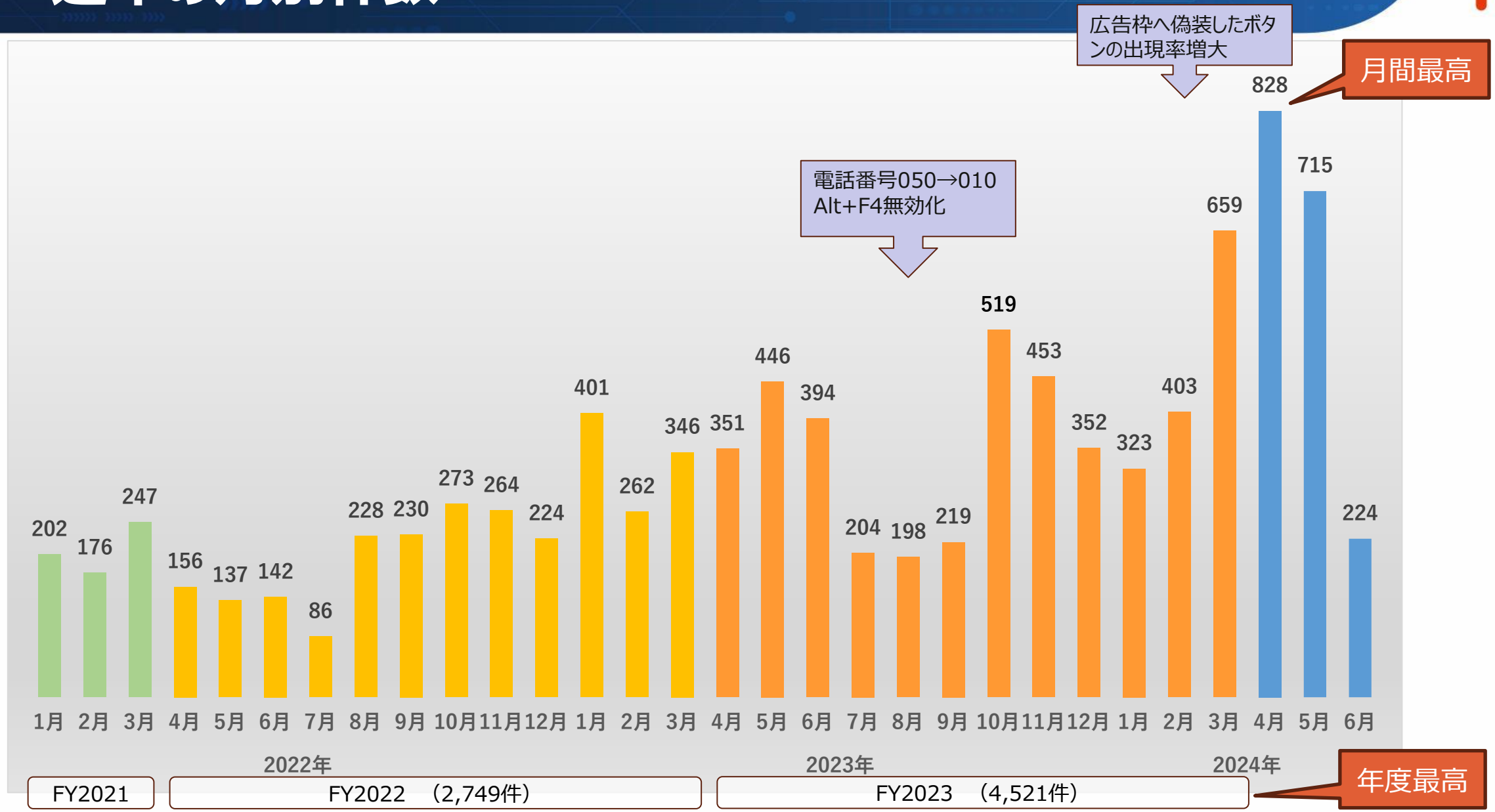
6　プリペイドカードの番号を伝える
＝ **金銭被害発生**

番号が違う、エラーが出ている等の理由で、後日返金があるという根拠のない説明をして、もう一度購入してくるように言われ、これを繰り返す

サポート詐欺の相談件数推移



近年の月別件数


広告枠へ偽装したボタンの出現率増大
月間最高
電話番号050→010
Alt+F4無効化
202
176
247
156
137
142
86
228
230
273
264
224
401
262
346
351
446
394
204
198
219
519
453
352
323
403
659
828
715
224
1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月 4月 5月 6月 7月 8月 9月 10月 11月 12月 1月 2月 3月 4月 5月 6月
2022年
2023年
2024年
FY2021
FY2022 （2,749件）
FY2023 （4,521件）
年度最高

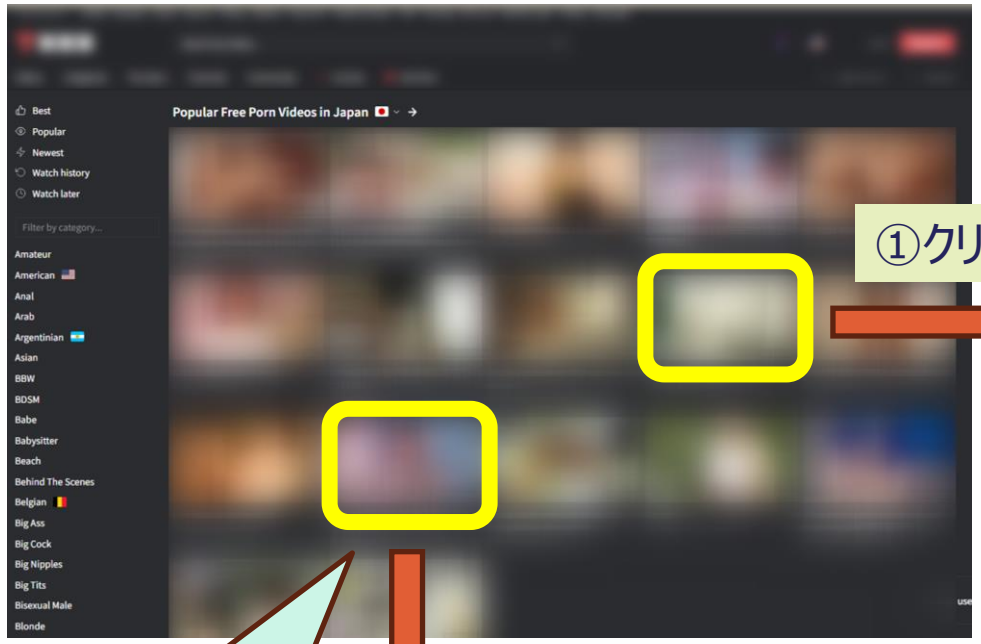
■本手口の実際の流れにおける変化と特徴
（2023.7頃以降）

被害者が偽警告に接触する段階での変化

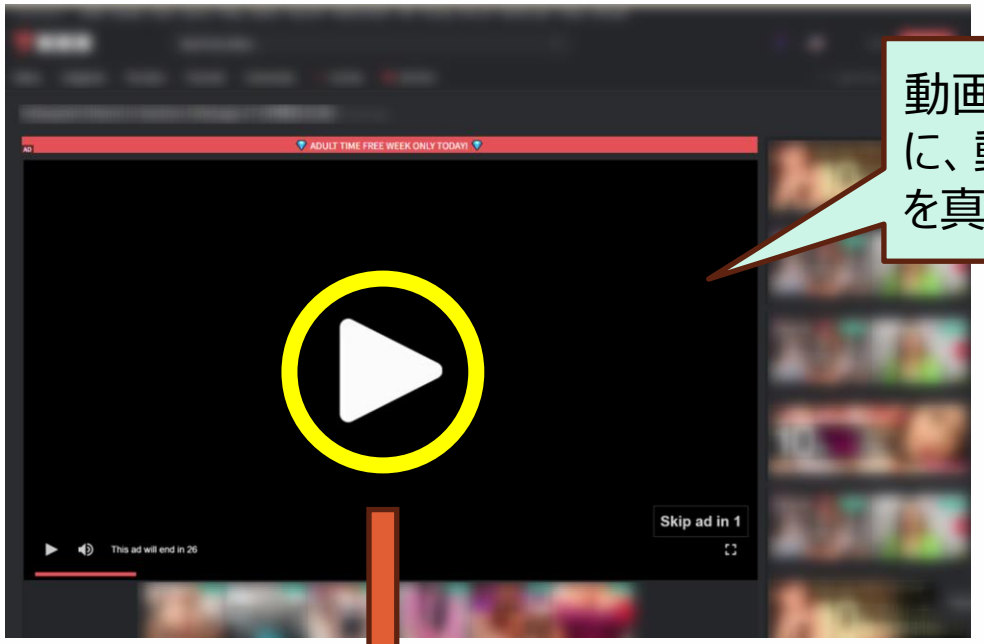
・過去：アダルトサイトなどが主流で、動画のサムネイル画像から偽警告サイトへリンク
・2023.07～：サイトの広告枠に、時世の話題や興味を惹くキーワードなどから偽警告サイトへリンク
・2023.12～、2024.02～：サイトの構成要素のようなボタンに偽装した画像が広告に出る。2月末から激増
・2024.04～：検索サービスの検索結果に、実在するブランドそっくりの広告が出る

被害者が偽警告に接触する機会のいろいろ 1/7

アダルトサイトや動画配信サイトでの偽警告への誘導



①クリック



動画表示エリア全体に、動画再生ボタンを真似た広告画像

②クリック

動画コンテンツのサムネイル画像のように見える広告

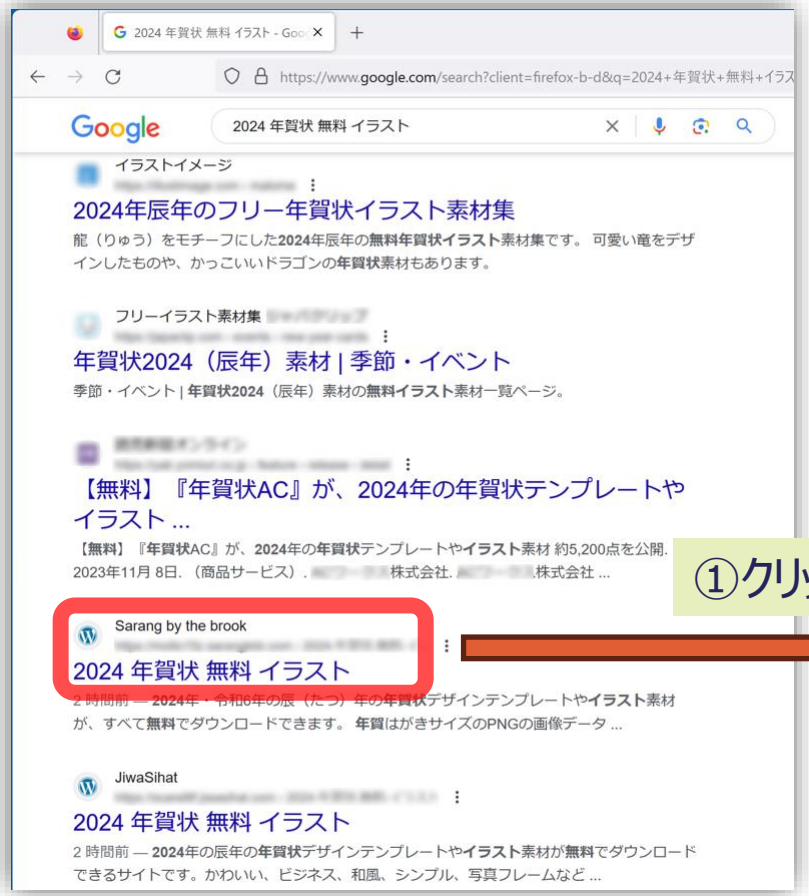
広告とは判別できずクリックして偽警告へ

ディスプレイ広告枠

被害者が偽警告に接触する機会のいろいろ 2/7

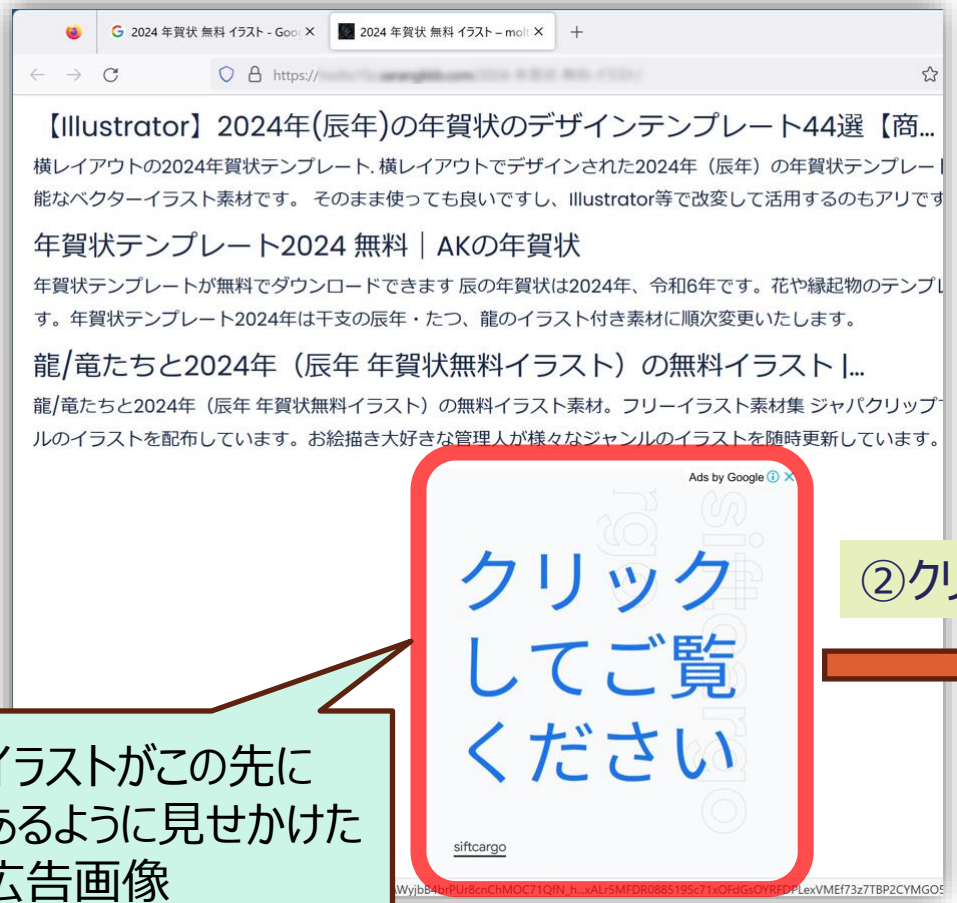
話題性ある検索から罠ページへ誘導するパターン

「2024年賀状　無料　イラスト」と検索



①クリック

移動したページには無料イラストの実物がない



イラストがこの先にあるように見せかけた広告画像

②クリック

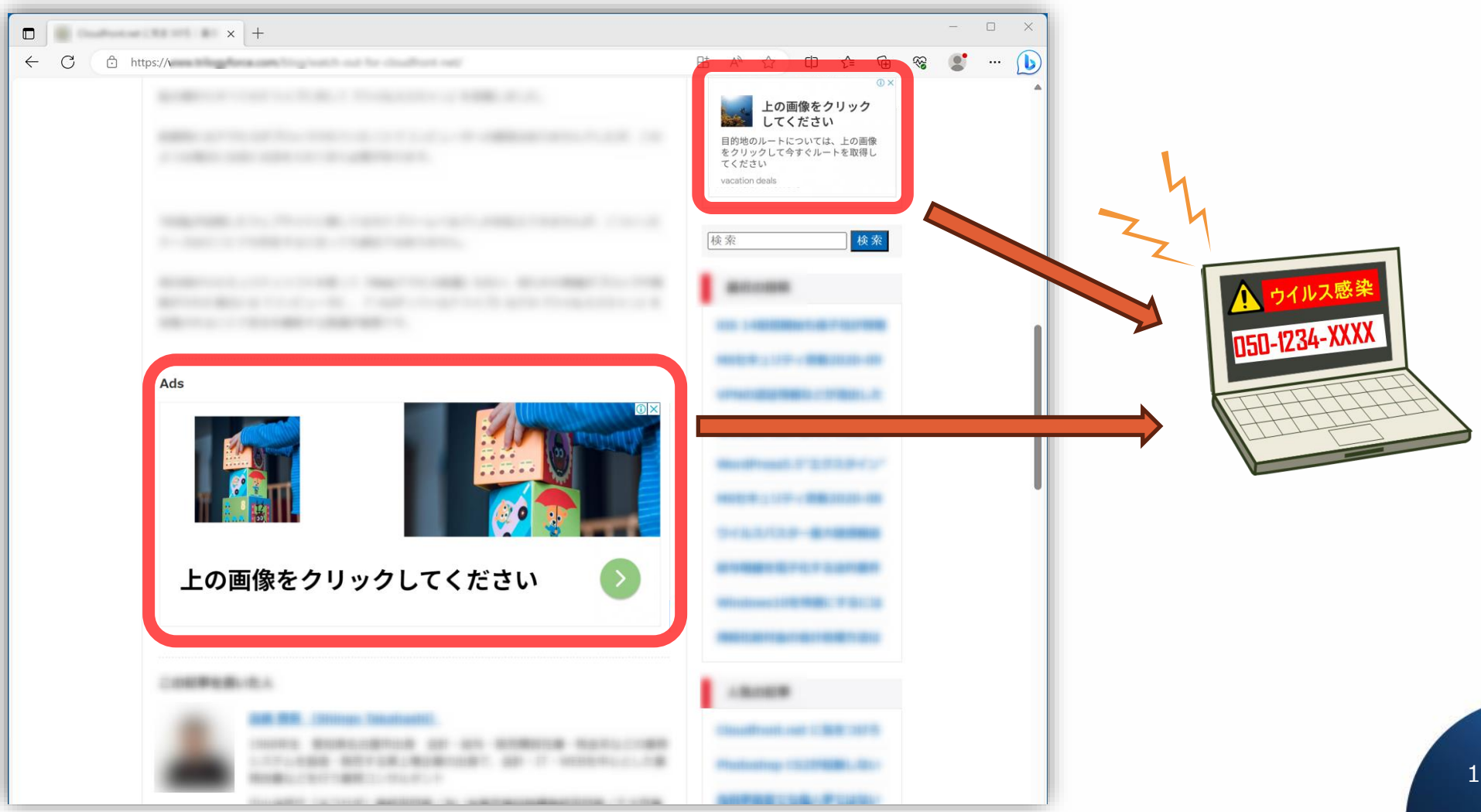
（参考）
2023.10～12
図例のとおり、年賀状のイラストを検索中に遭遇した相談が相次ぐ

2024.1
能登半島地震被災状況を検索すると、同様の罠があることを確認した

本手口は、罠ページを作成後にSEO施策で検索結果の上位に出現させることが可能

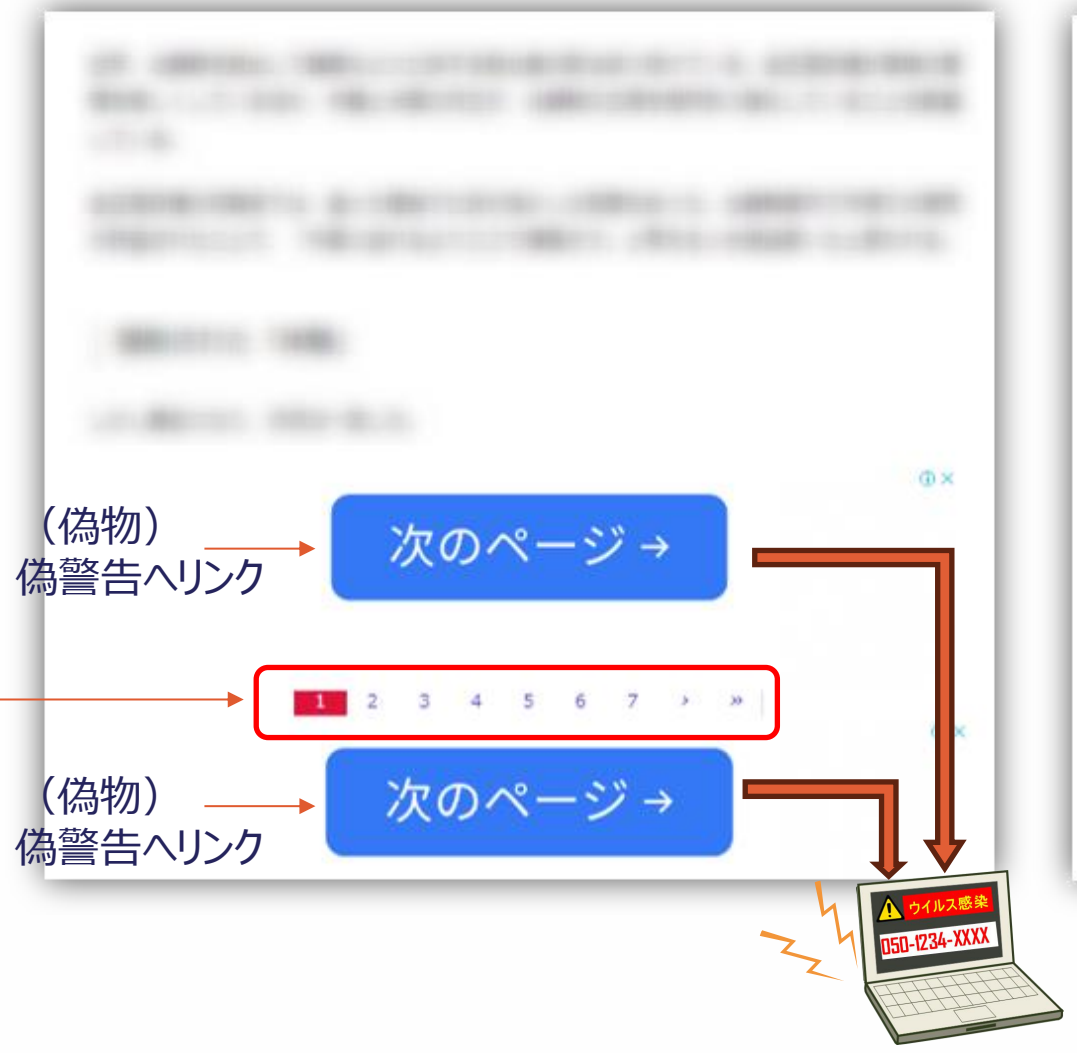
被害者が偽警告に接触する機会のいろいろ 3/7

一般のウェブページの広告枠（広告スペース・アフェリエイト）に
時世の話題や興味を惹くキーワードを画像化して表示

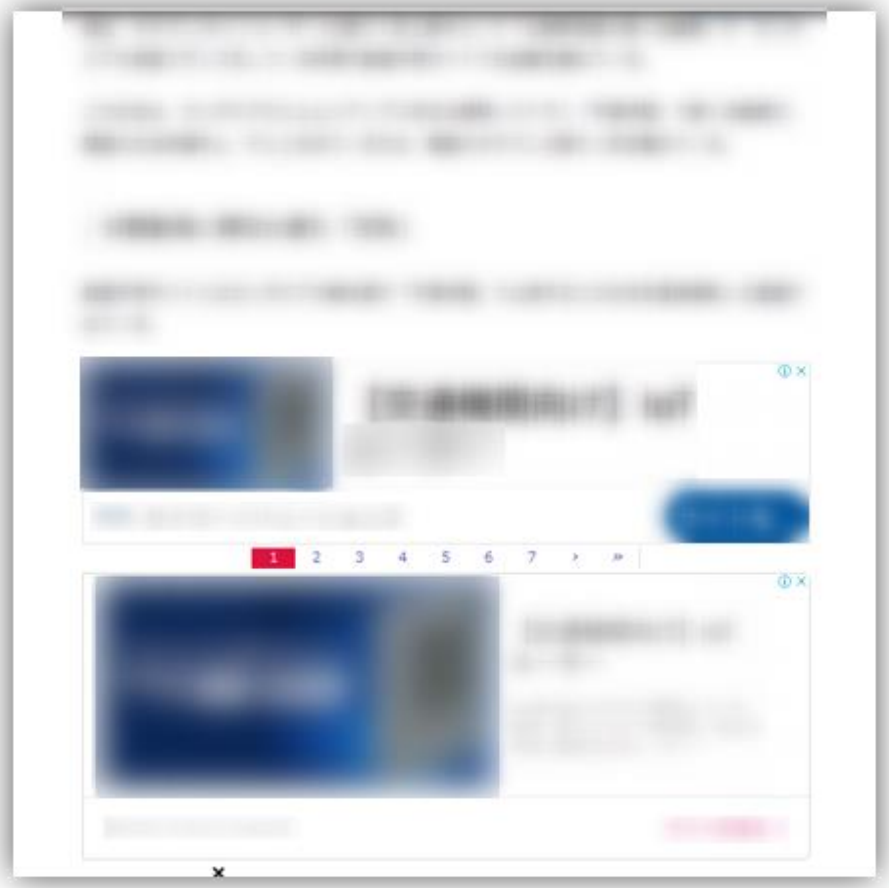


被害者が偽警告に接触する機会のいろいろ 4/7

前ページと同じく広告枠に出現するもの。ウェブページの次のページや次のコンテンツへ進むボタンのように見せかけた画像



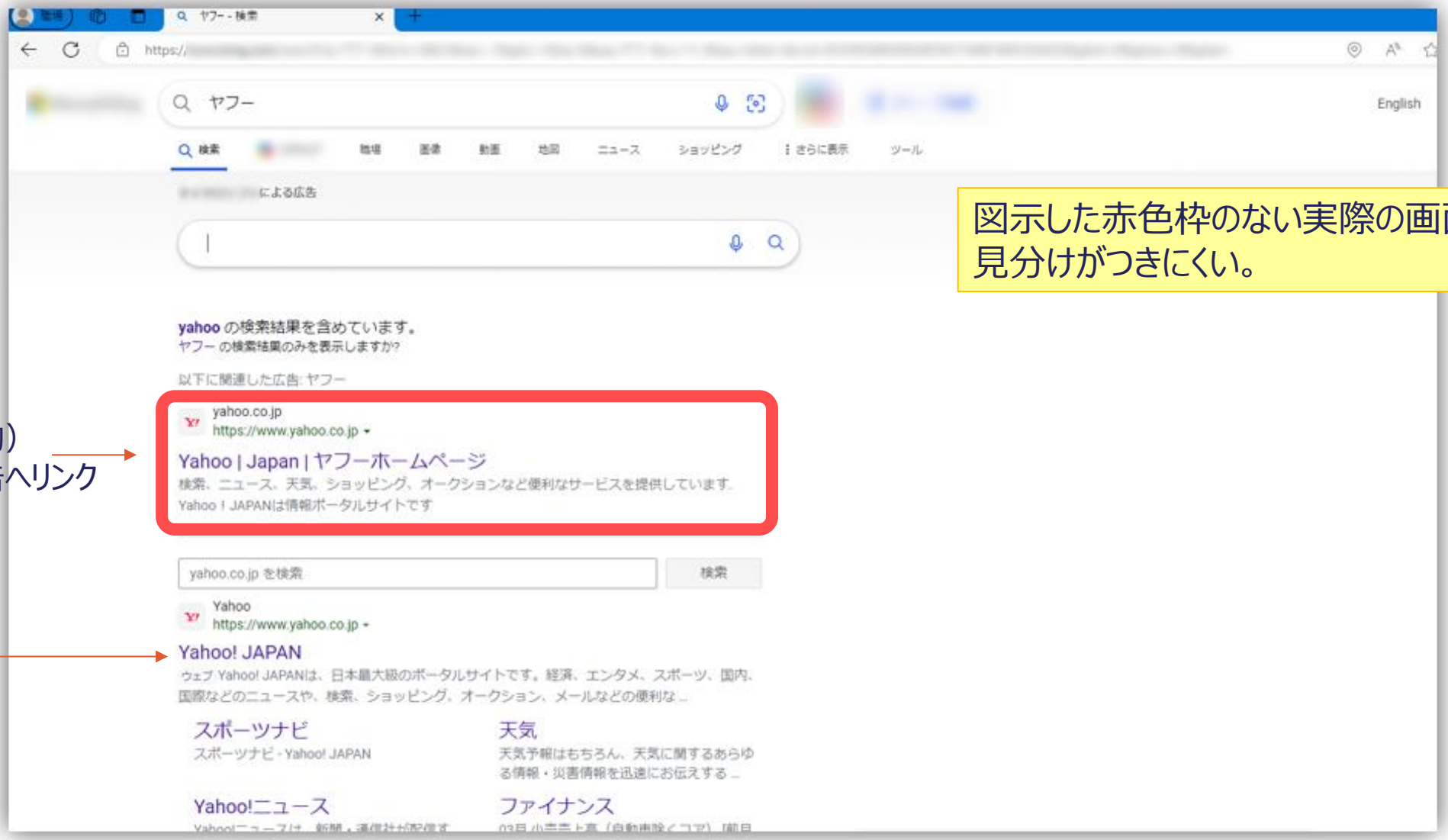
（参考）
同ウェブページで一般的な広告の表示例



被害者が偽警告に接触する機会のいろいろ 5/7

検索結果に広告として出てくる偽リンク 【検索連動型広告】

※リスティング広告とも呼ばれる



（偽物）
偽警告へリンク

（本物）
Yahoo!のホームページ
へ移動する

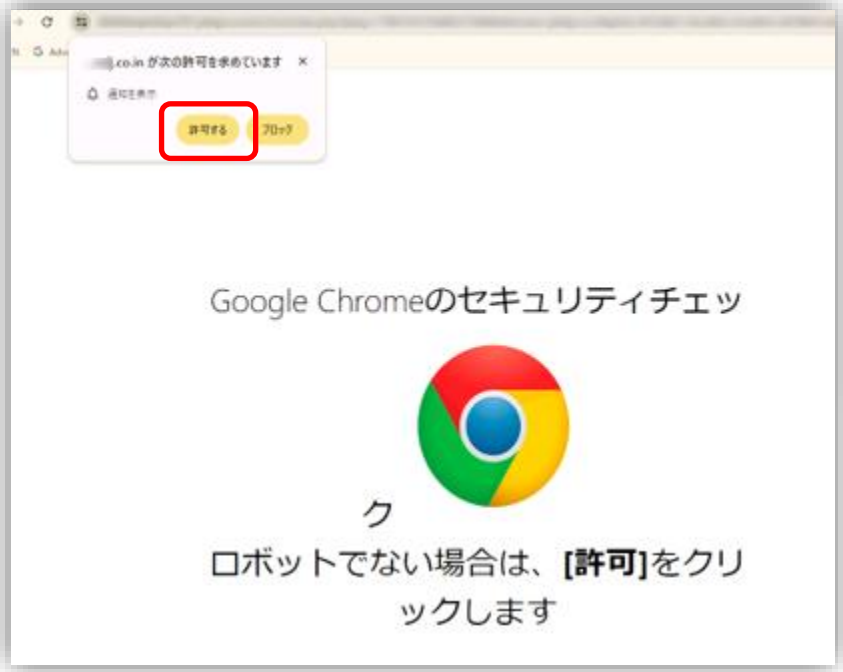
図示した赤色枠のない実際の画面では、
見分けがつきにくい。

被害者が偽警告に接触する機会のいろいろ 6/7

ブラウザの通知機能を悪用し、定期的（数分おき）に通知領域に嘘のメッセージを出し、
それをクリックすると偽警告サイトへ移動する

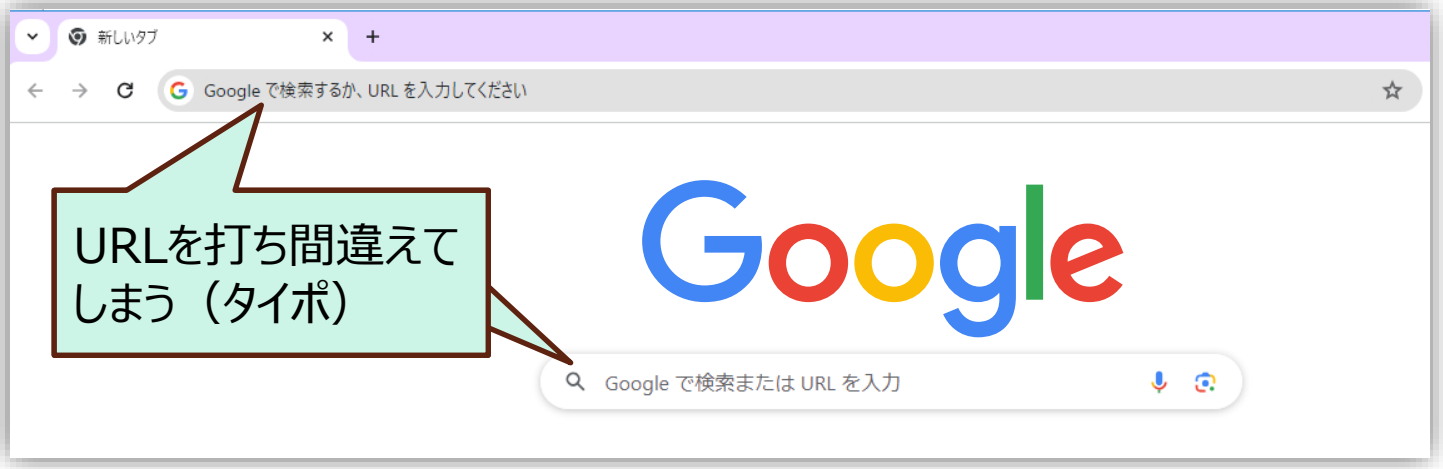
ブラウザに通知が登録されてしまう罠

CAPTCHA認証のように見せかける等で、スクリプト（ページ内のプログラム）を実行させるためのボタンを押させる。スクリプトが実行されると意図しない通知が登録されてしまう



被害者が偽警告に接触する機会のいろいろ 7/7

URLの打ち間違い（タイポスクワッティング）を待ち構えて偽警告サイトへ移動する

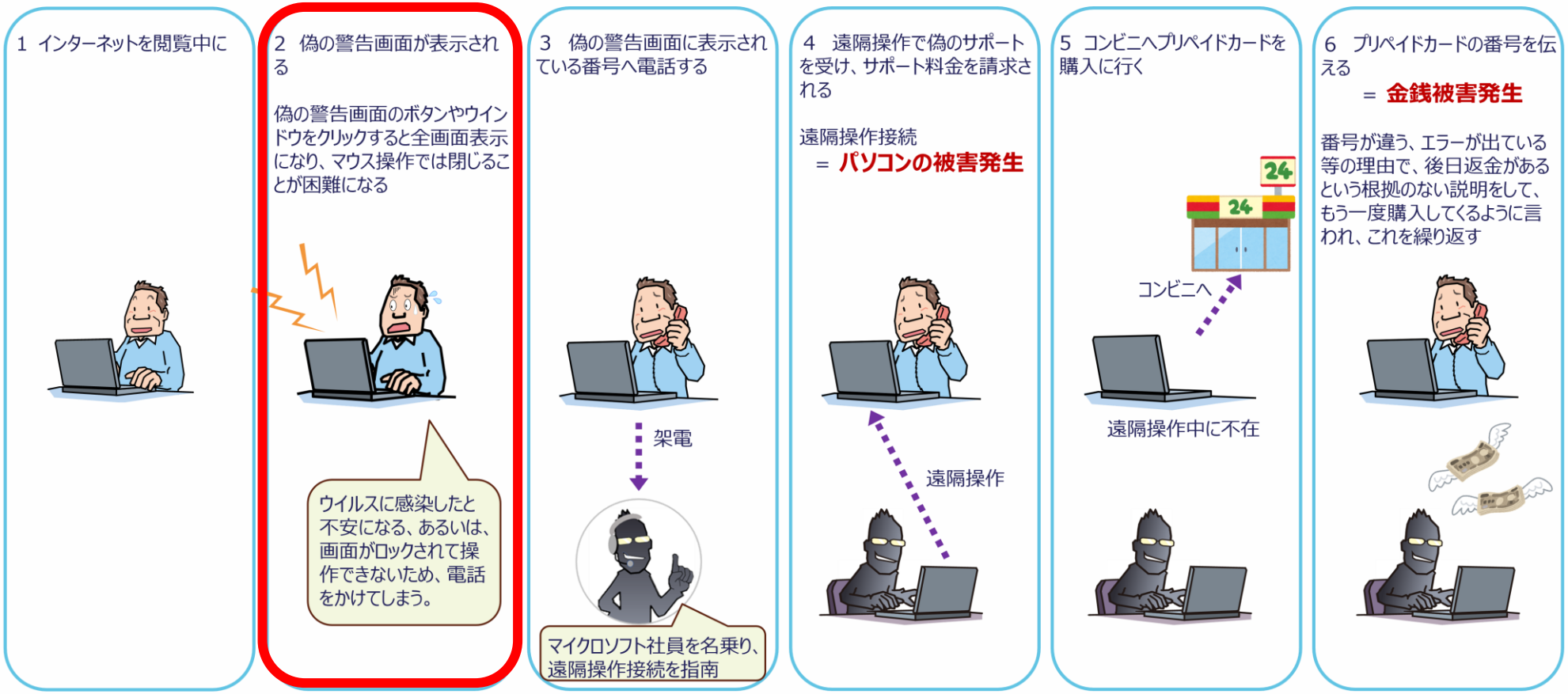


・キー入力で打鍵を間違えそうなドメインをあらかじめ取得・登録し、リダイレクトサイトを立ち上げて待機している
・アクセスすると、さまざまな詐欺サイトや偽サイトへリダイレクトされ、偽警告サイトへリダイレクトされる場合もある

確認したドメイン（例）	本物のドメイン	偽警告を含むさまざまな偽サイトへリダイレクトされたドメイン
	gmail.com	gmai.com

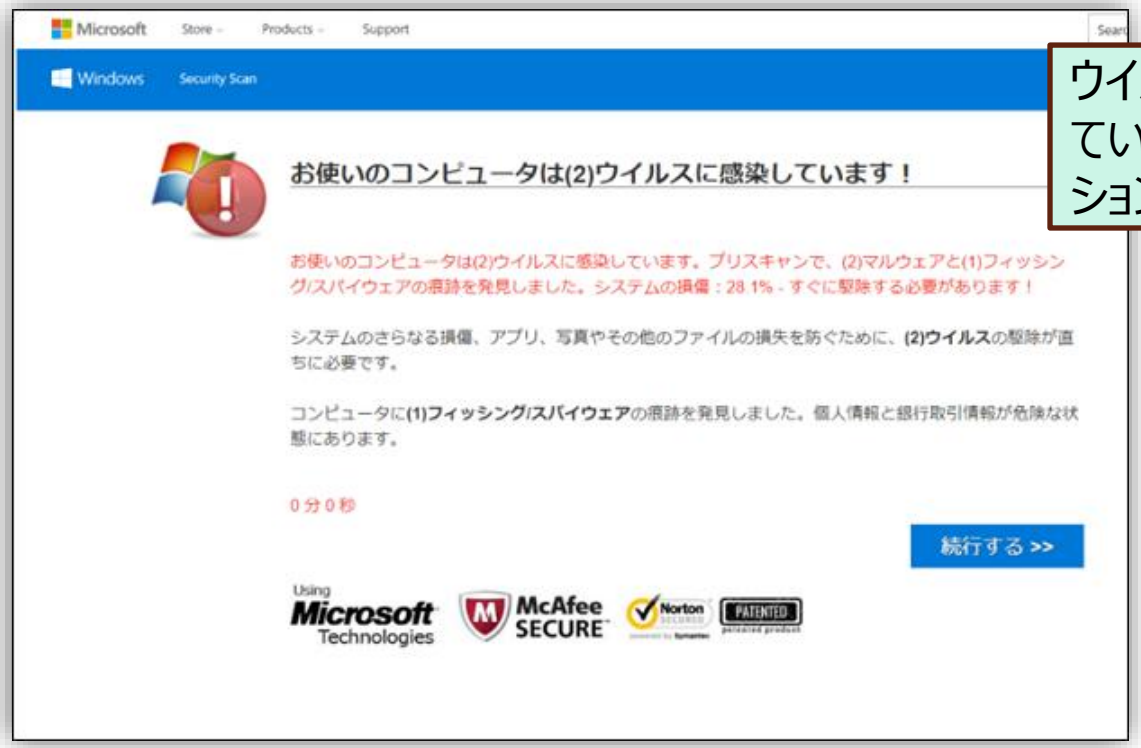
偽警告画面の変化

・偽警告画面について、2023年～2024年にかけ徐々に変化していることを確認（2023年までは詳細な検証記録がないため省略）
・画面の構成、視覚的効果
・画面の閉じ方
・表示される電話番号（『電話番号の変化』の章で説明）

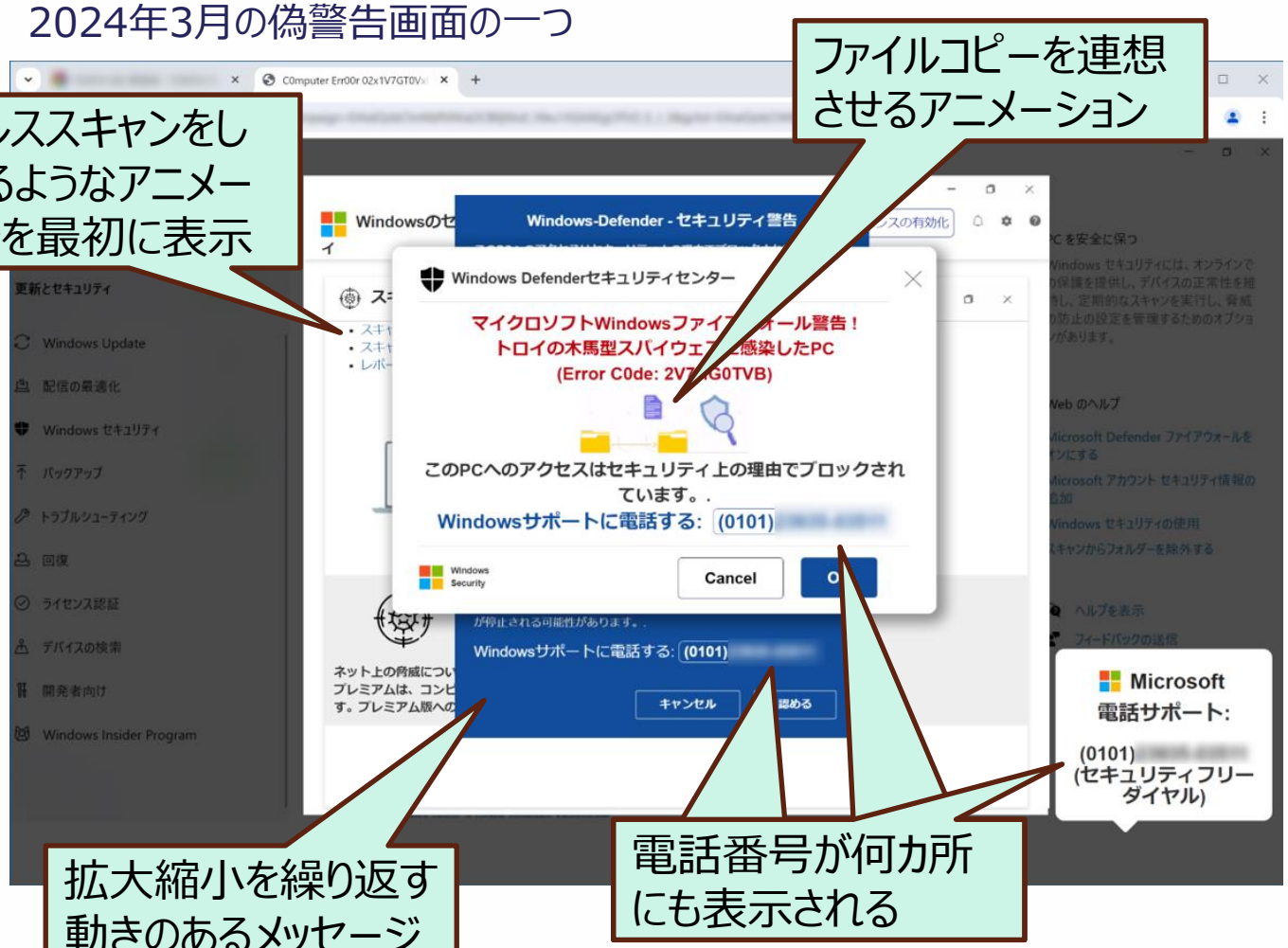


画面構成、視覚効果の変化

2018年ごろの偽警告画面



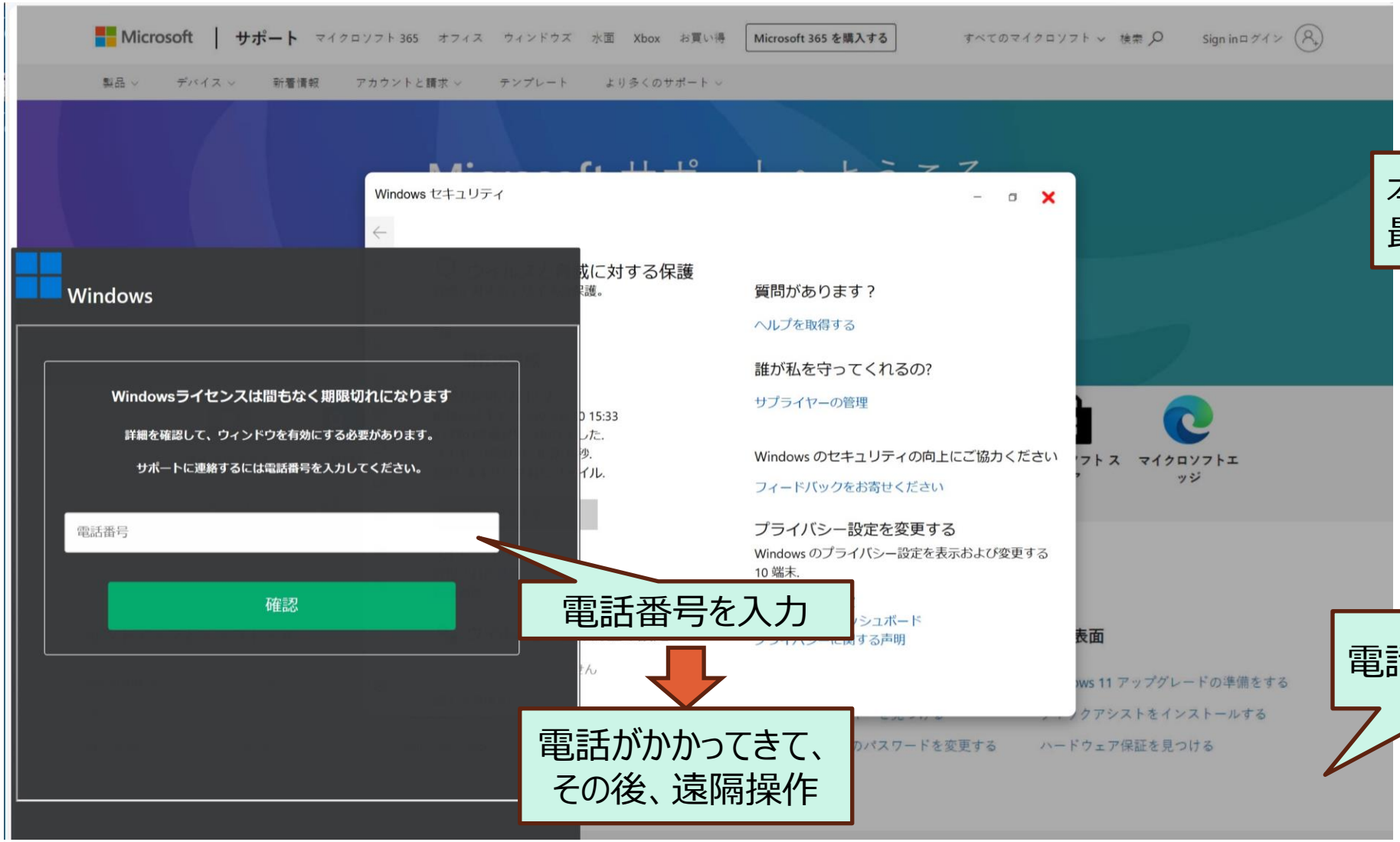
2024年3月の偽警告画面の一つ



・マイクロソフトWindowsを騙り、ロゴを使っている点は不変
・最近の偽警告画面は、画面全体に表示（ブラウザの全画面表示）される。複数のダイアログが重なるようの表示される。数秒かけて徐々に表示されてくる

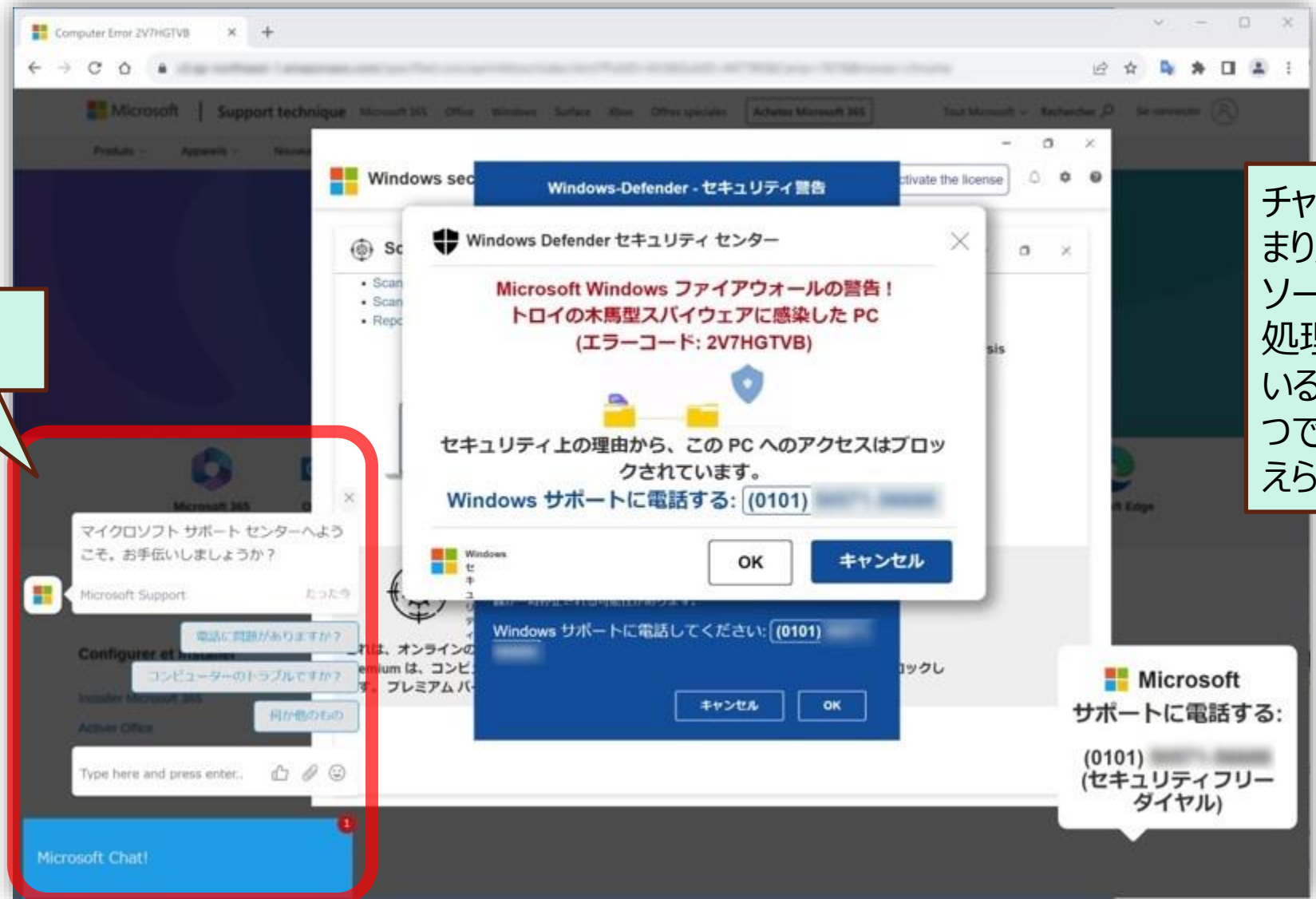
2023年にみられた画面の変化

2023年8月頃 ダイアログに電話番号を入力させ送信させる手口（数件の相談があった）



2023年にみられた画面の変化

2023年9月頃　チャットが出る（数件の相談があった）

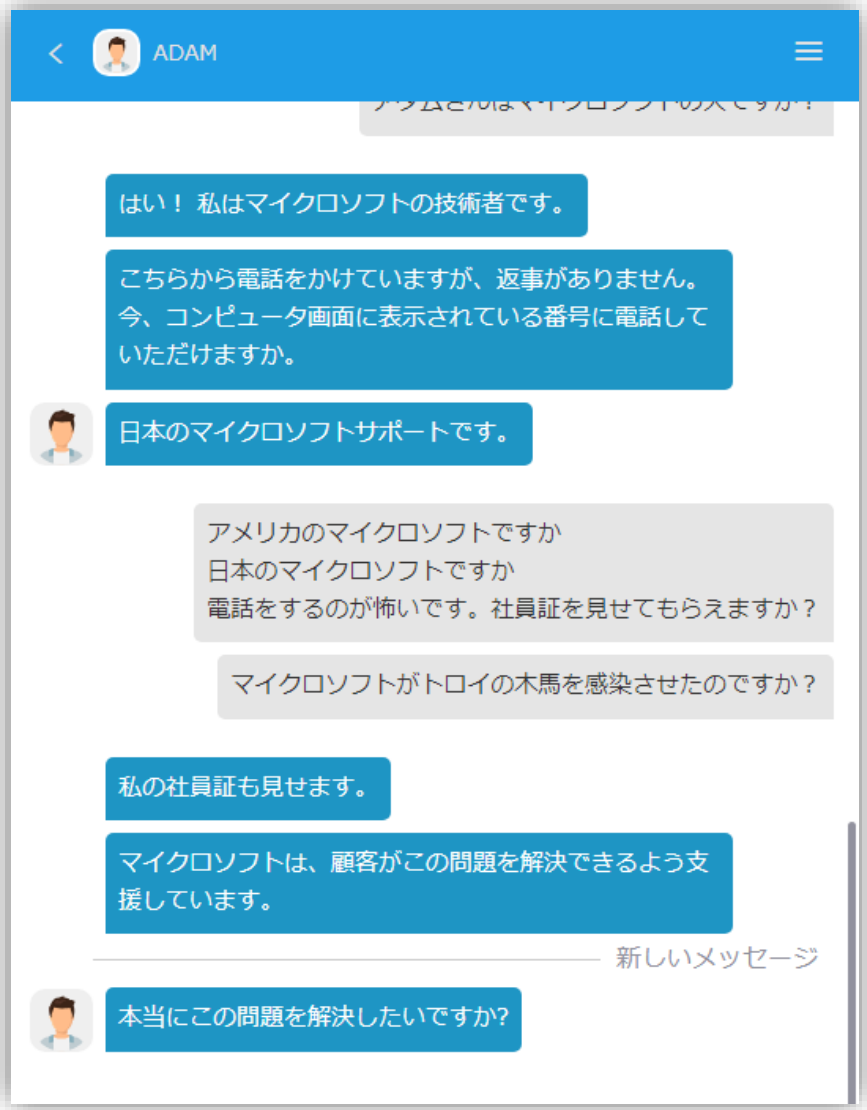


チャット画面

チャット画面は、最近はあまり見かけなくなったが、ソースコード内にはチャット処理のスクリプトが残っているのを確認しており、いつでも再開できるものと考えられる

チャットは有人対応だった

偽警告画面のチャットを検証
- チャットオペレータは、アダムと名乗る
- 放置していても、しつこく語りかけてくる
- 正確な日本語
- こちらの電話番号を聞きたがる



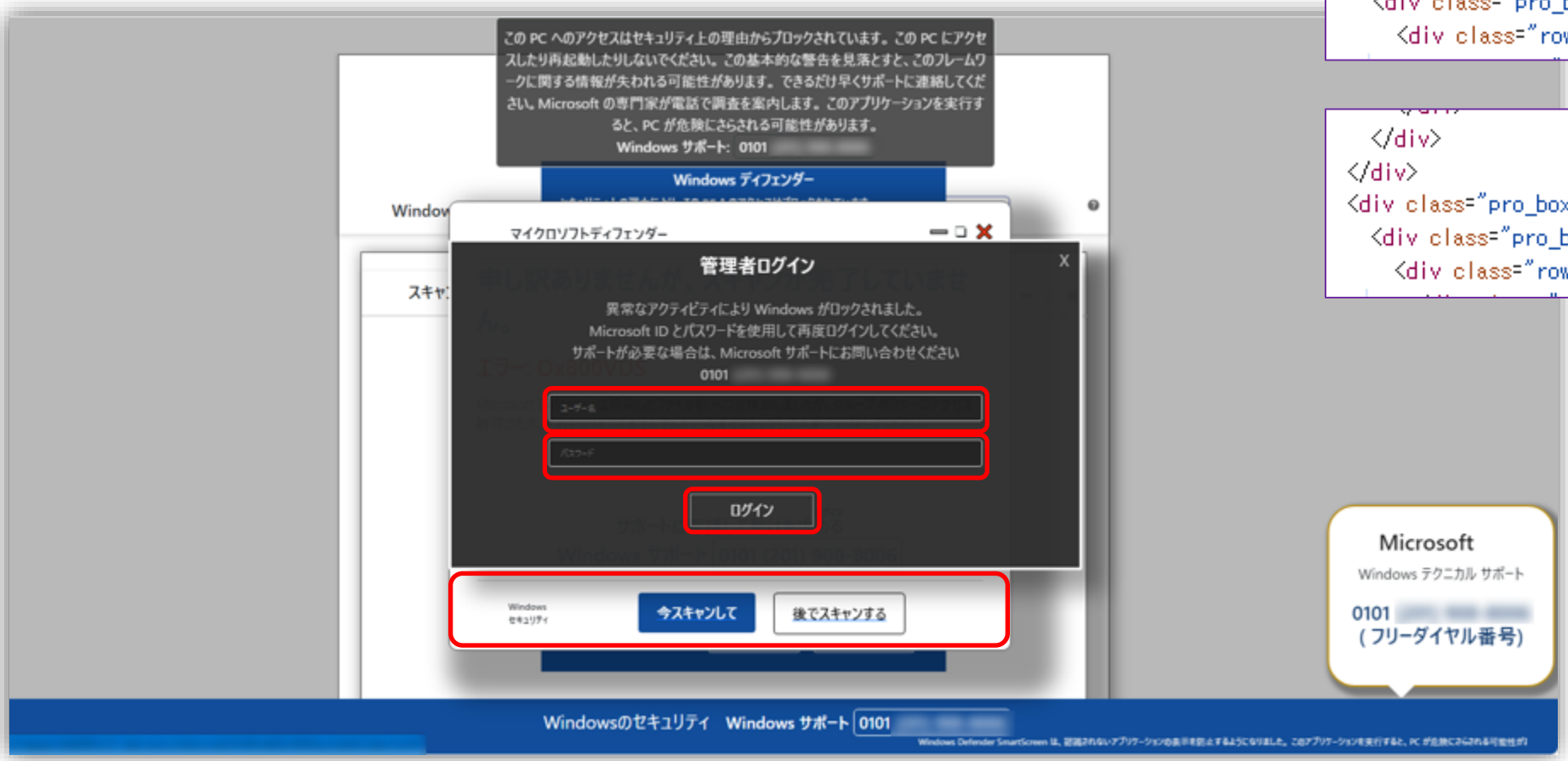
2023年にみられた画面の変化

2023年4月 一時期、警官風のイラストが表示された
（2024年にも一時期表示された）

2023年末頃から、ログイン画面が出る。入力しようとしてマウスクリックすると偽警告画面が全画面表示となる
ボックス内への入力はできない

偽警告表示画面に施されている細工

マウスカーソルを非表示にする（2023年から確認）
・ブラウザの表示領域全体でマウスが表示されない細工が施されている
・下記赤枠部分では、マウスが表示される




```
</div>
</a>
<div class="pro_box" style="cursor: none; display: default;">
  <div class="pro_box_header">
    <div class="row">
```

マウスカーソルを非表示にする

```
  </div>
</div>
<div class="pro_box2" style="cursor: default; display: none;">
  <div class="pro_box_header">
    <div class="row">
```

マウスカーソルを表示にする

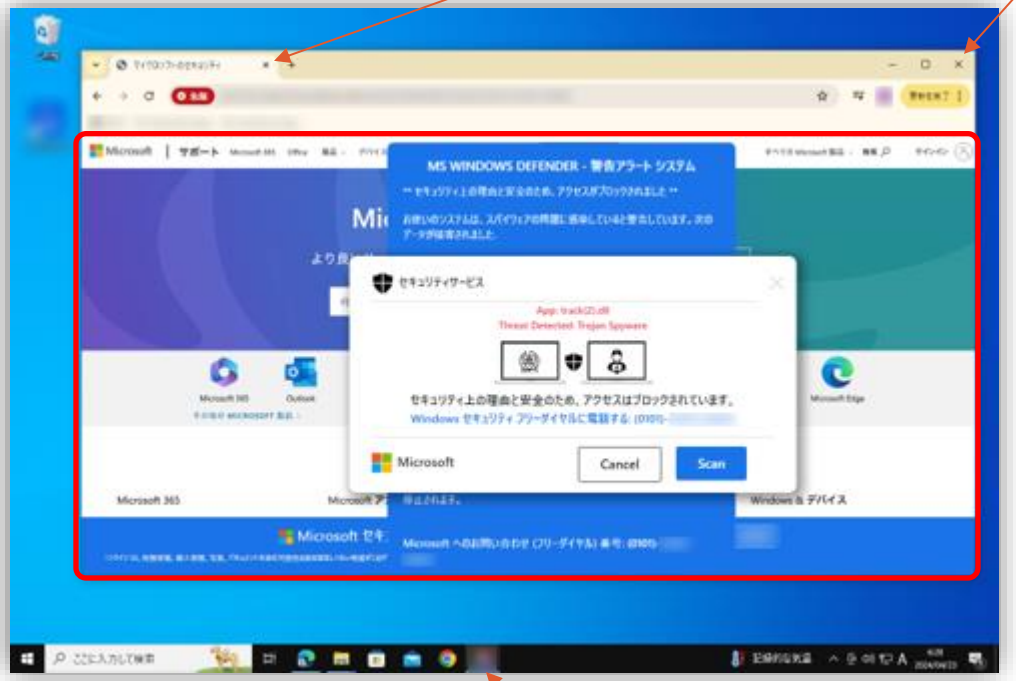
偽警告表示画面に施されている細工

表示領域をマウスクリックすると、全画面表示になり、警報音が鳴る

可変サイズウィンドウ

タブを閉じるボタン

ブラウザを閉じるボタン



タスクバーから閉じることも可能

赤枠内のどこをクリックしても、全画面表示になる。

タブがない

閉じるボタンがない

全画面表示

タスクバーがない

・前項で説明したとおり、警告画面表示内のほとんどのエリアでマウスが表示されず、閉じることが困難なため、一般のユーザは操作ができなくなったと思い込んでしまう

・全画面表示は、TopMost属性（最前面に表示）のため、他のウィンドウが全て偽警告表示の裏側に隠れ偽警告以外が表示されない

・警報音はタスクバーでの音量調整ができなくなる

偽警告表示画面に施されている細工

ブラウザの全画面表示状態を抜け出すキー操作 2023年3月頃まで

対象	キー操作	操作	全画面表示からの脱出操作
OS	**Ctrl + Alt + Del**	セキュア・アテンション画面の表示	タスクマネージャからブラウザのタスクを終了、または再起動等
OS	**Ctrl + Shift + ESC**	タスクマネージャの起動	タスクマネージャからブラウザのタスクを終了
OS	**Win + X**	トラブルシューティングツールのメニュー表示	タスクマネージャからブラウザのタスクを終了、または再起動等
OS	**Win + R**	ファイル名を指定して実行	シャットダウンコマンド（再起動）の実行
OS	**Win**	Windowsメニューの表示	電源メニューから再起動
デスクトップ	**Win + M** **Win + D**	全てのウィンドウを最小化する デスクトップを表示する	タスクバーからブラウザを終了
ブラウザ	**Alt + F4**	ウィンドウを閉じる	ブラウザを閉じる
ブラウザ	**Win + ↓**	可変サイズウィンドウに戻す	ブラウザの閉じるボタン、またはタブの閉じるボタンで終了
ブラウザ	**ESC長押し**	可変サイズウィンドウに戻す	ブラウザの閉じるボタン、またはタブの閉じるボタンで終了

ブラウザの F11 キーによる、全画面表示 ↔ 可変サイズウインドウ の切り替えは、スクリプト（プログラム）で全画面表示にした偽警告表示では使えない

2023年3月頃まで
- 偽警告画面が表示されたという相談においては、Alt+F4の操作を案内していた
- Alt+F4で閉じれないときは、タスクマネージャを起動してブラウザのタスクを終了する案内をしていた。（ときどき、このタイプの偽警告があった）

偽警告表示画面に施されている細工

ブラウザの全画面表示状態を抜け出すキー操作 2023年9月頃から

対象	キー操作	操作	全画面表示からの脱出操作
OS	**Ctrl + Alt + Del**	セキュア・アテンション画面の表示	タスクマネージャからブラウザのタスクを終了、または再起動等
OS	**Ctrl + Shift + ESC**	タスクマネージャの起動	タスクマネージャからブラウザのタスクを終了
OS	**Win + X**	トラブルシューティングツールのメニュー表示	タスクマネージャからブラウザのタスクを終了、または再起動等
OS	**Win + R**	ファイル名を指定して実行	シャットダウンコマンド（再起動）の実行
OS	**Win**	Windowsメニューの表示	電源メニューから再起動
デスクトップ	**Win + M** **Win + D**	全てのウィンドウを最小化する デスクトップを表示する	タスクバーからブラウザを終了
ブラウザ	**Alt + F4**	ウィンドウを閉じる	ブラウザを閉じる
ブラウザ	**Win + ↓**	可変サイズウィンドウに戻す	ブラウザの閉じるボタン、またはタブの閉じるボタンで終了
ブラウザ	**ESC長押し**	可変サイズウィンドウに戻す	ブラウザの閉じるボタン、またはタブの閉じるボタンで終了

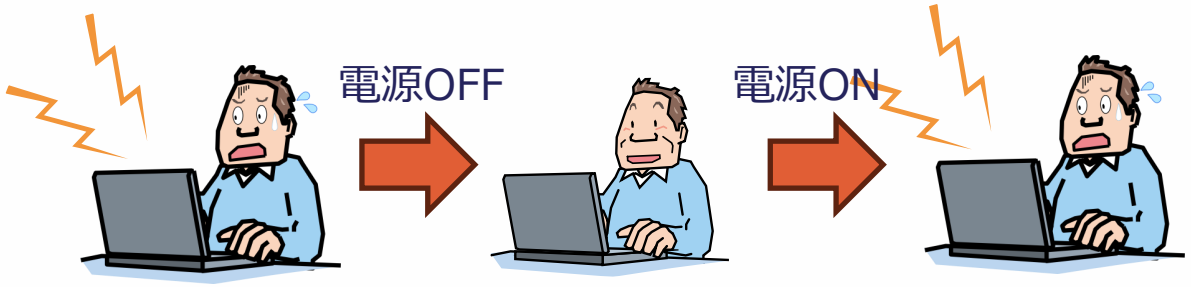
ブラウザの F11 キーによる、全画面表示 ↔ 可変サイズウインドウ の切り替えは、偽警告表示では使えない

- 2023年4月頃～8月頃：Alt+F4が効かなくなるケースが徐々に増加してきた
- 2023年9月頃以降：Ctrl+Alt+Del と ESC長押し 以外が全く効かなくなった

ESC長押しが効かないケース

■全画面表示のブラウザでESC長押しが効かないケース

相談の内容（一例）：「操作できなくなったので、電源を切って、入れなおしたが、まだ警告が出ている」



・被害者は電源ボタンを押して電源を切ったつもりだが、ノートパソコンはスリープ状態で電源が切れている
・電源を入れなおした時には、スリープ直前の状態に復旧するため、偽警告画面表示は継続する
・また、スリープから復帰した際には、ブラウザがフォーカスを持っておらず、ESCキー長押しが効かない

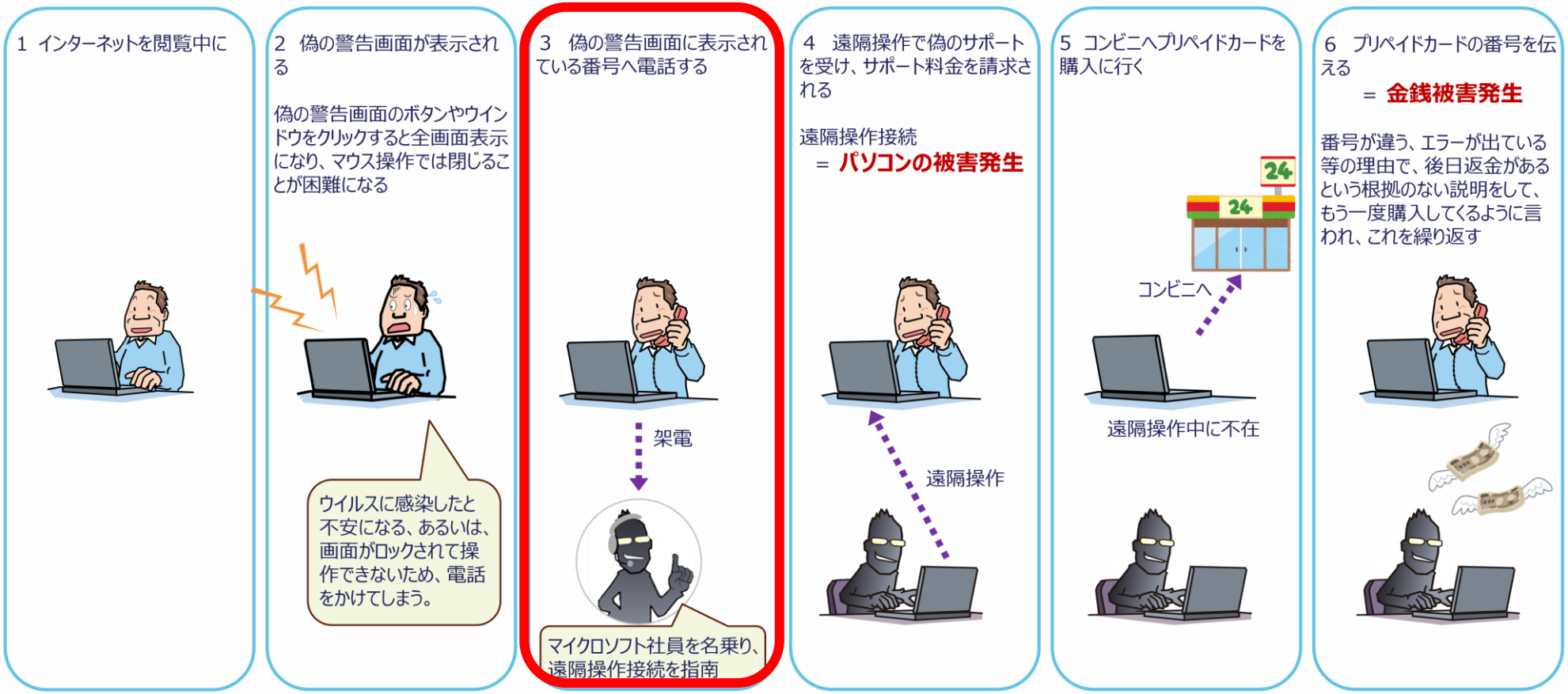
ESCキー長押しはブラウザが受け取る必要があり、ブラウザがフォーカスを持っていない場合はブラウザに伝わらない

■対処

1. マウスをクリックしてもらう（この際、マウスポインターが表示されていないが、**一度クリックすることでブラウザがフォーカスを得る**）
2. その後、ESCキー長押し

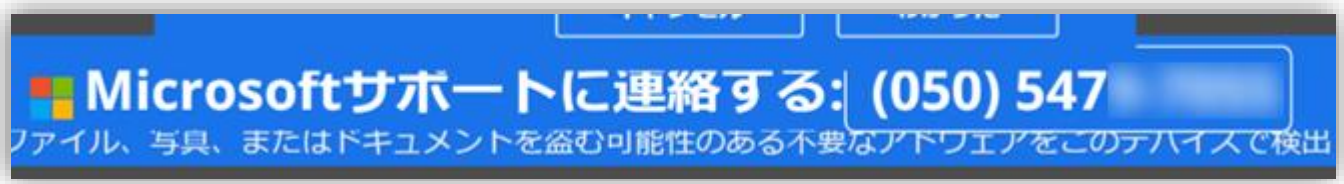
電話番号の変化

これまでに確認している電話番号は、050で始まるIP電話、010で始まる国際通話、080で始まる国内携帯電話がある



2023年からの電話番号の変化

・050（IP電話）だった番号が、010（国際通話）に変わってきている
・完全には切り替わっていないが、現在は010がほとんどで、たまに050が出る



2023年から出始めた

・0101（010-1） はアメリカへの国際通話
・加入者番号は、一定（固定）ではなく、複数の番号を確認しており、不規則に変わる
・アメリカへの発信になるが、他国へ転送されている可能性がある（後述）

特殊詐欺対策として050番号の本人確認義務化

【特殊詐欺対策】

本日、犯罪対策閣僚会議が開催されまして、3月の会議で、SNS上で実行犯を募集する手口の強盗や特殊詐欺事案に対し「緊急対策プラン」が策定されました。本日は、その進捗状況について議論を行ったところでございます。

私からは、総務省において、特に悪用の多い「050アプリ電話」について、契約時の本人確認を義務化する制度改正に向け準備を進めていること、悪質事業者が保有する「在庫電話番号」を一括して利用制限するため、スキーム改正に向けた準備を進めていること、偽変造された本人確認書類による不正契約の防止のため、マイナンバーカードの活用に取り組んでいることなどを報告いたしました。

総理からは、犯行ツール対策として、携帯電話など電話が犯罪に悪用されることのないよう、対策を加速するようご指示がございました。これを踏まえて総務省における取組を加速し、準備をしている施策を速やかに実行に移してまいりたいと考えております。

総務省：総務大臣閣議後記者会見の概要 令和5年6月16日　より抜粋
https://www.soumu.go.jp/menu_news/kaiken/01koho01_02001247.html

2023年からの電話番号の変化

2024.4.22　国内の携帯電話080の番号が出た

電話をかけたところ、通常とは異なる呼び出し音でサポート詐欺に繋がった
手口には乗らず終話したところ、折り返し、非通知の着信があった

電話をかけた場合の特徴

■184（発信者番号非通知）でかけた場合
下記のようにいろんなケースがある
・接続もされず、呼び出し音も鳴らない
・呼び出し音のあと、すぐに切れる
・オペレータとつながる

■184をつけず、発信者番号を通知してかけた場合
・通話前に切断した場合（ワンギリ等）、折り返しかかってくる
・通話中に切れた場合も、折り返しかかってくる

■折り返しかかってくる番号
・大半が番号非通知の表示
・番号表示されているものも確認しているが、全て海外

■折り返しかかってきた番号（調査中に実例2件）
+82 2-22▲▲-▲▲▲▲（韓国）
+65 62■■-■■■■（インドネシア）
この2件とも、010-1（アメリカ）にかけた直後であるため、かけた電話はアメリカから国外へ転送されている可能性が考えられる

発信者番号が安心相談窓口に偽装された事例

■相談内容から事例判明
・5/29サポート詐欺に遭った。詐欺と気付き電話を切り、パソコンを強制終了
・その直後に2回着信したが、詐欺の電話と確信したので出なかった。番号は03-5978-7509が表示されていた
（その後、消費生活センターなどに相談や確認したところ、IPAの電話番号だと言われた）

■以下の情報を得ることができた
・着信履歴から電話をかけたら呼び出し音が鳴ったが、すぐに切った

→ 相談者が電話をかけた時間帯の安心相談窓口（03-5978-7509）は音声による自動応答のため、
呼び出し音が鳴ることはない

■別の手口による詐欺で、5/20に類似相談あり
・3月頃に電話で少し会話をして詐欺に遭いかけた。それ以降、不思議なことが起こる
・在宅中に、家の固定電話（番号）から携帯に着信した。固定電話は目の前にあり、誰も使っていない
・5/13頃に、知らない番号の0359787509から着信記録が数件残っている

→ 安心相談窓口の発着信履歴を確認したが、相談者の番号（固定、携帯）への履歴はなかった

6月11日追加

発信者番号が偽装された事例

■相談者から着信履歴のスクリーンショットを提供いただいた

（左図：履歴の時系列は下から上へ）

相談者の対応

4段目：被害者が偽マイクロソフトへ架電
怪しいと感じて34分後に電話を切る

3段目：直後に着信。被害者は電話に出た
偽サポートの声だったので聞こえないフリをして切った

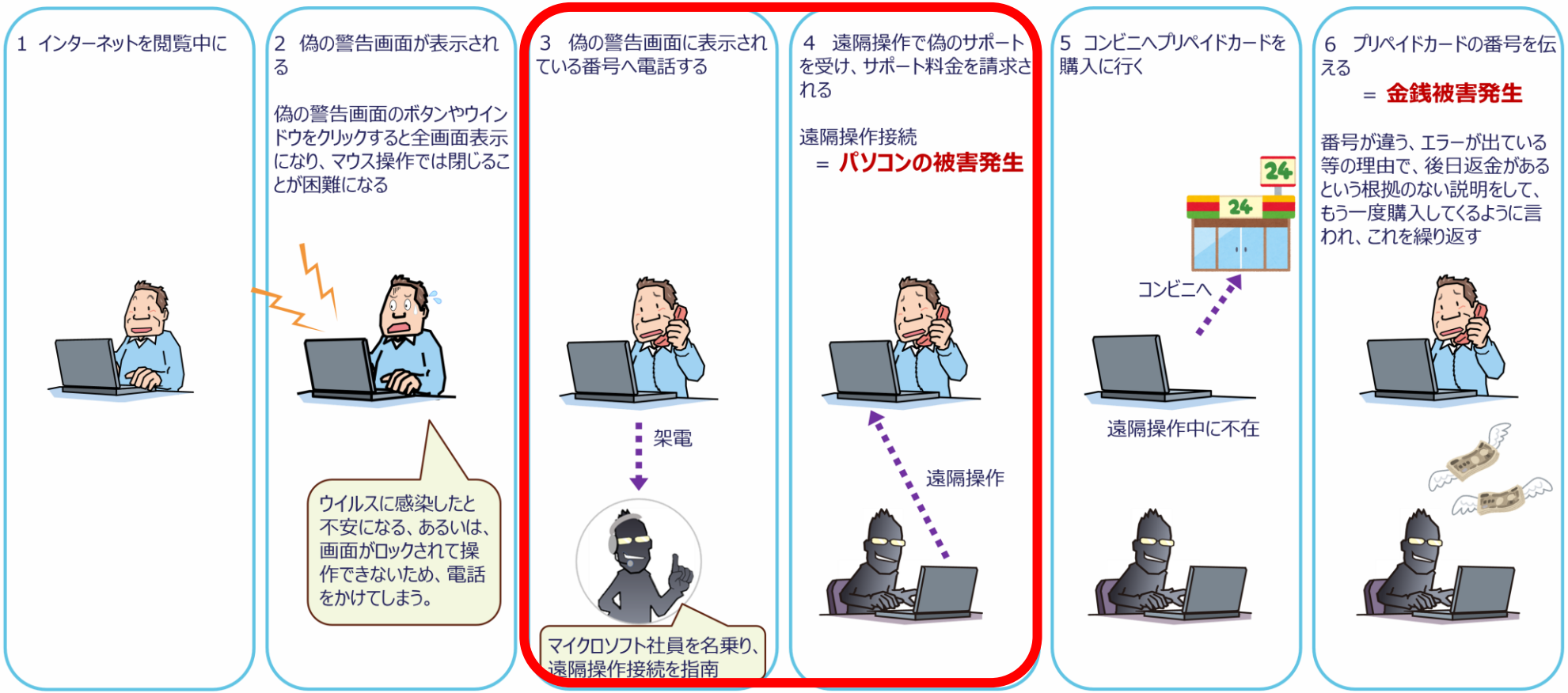
表示されている電話番号は都内に実在する番号
（ホームページで公開されている企業の電話番号）

1段目：その後、被害者は通信事業者のサポート（0077■■■■）へ架電し、サポートに本事案の相談をした

2段目：通信事業者のサポートとの電話中にも同番号から2回着信している

オペレーターの対応

・電話をかけると、片言の日本語を喋るオペレーターが電話対応する
・何人かのオペレーターと実際に会話をしたが、オペレータの対応が統一されている部分と、まちまちな部分がある



オペレーターの対応

■トークスクリプト

・何度かかけてみて、同じトーク部分がある
・被害者からの相談時に聞く状況とも一致する

マイクロソフトです。お客様どうしましたか？

「再起動したら直った」と回答

ハッカーが侵入したのでトロイの木馬が残っています。
マイクロソフトからパソコンの点検をして
ウイルスの駆除を行います。

「結構です」と回答したところ、「マイクロソフトのOSです。私はマイクロソフトの技術者です。点検をしないといけません」と遠隔操作の必要性を言ってきた。

パソコンの画面になんて書いてありますか？
何をしているときにその画面が出ましたか？そのメッセージを見るのは初めてですか？
ハッカーがパソコンに侵入したためブロックされました。
しかし大丈夫です。マイクロソフトからウイルスの除去を行います。

会社のパソコンですか？自宅のパソコンですか？

「会社のパソコン」と回答

会社の口座に不正にアクセスされています。
残金を移しますので会社の口座の情報が必要です。

Win+Ctrl+Qを押して、クイックアシストを起動させる事例を確認した。

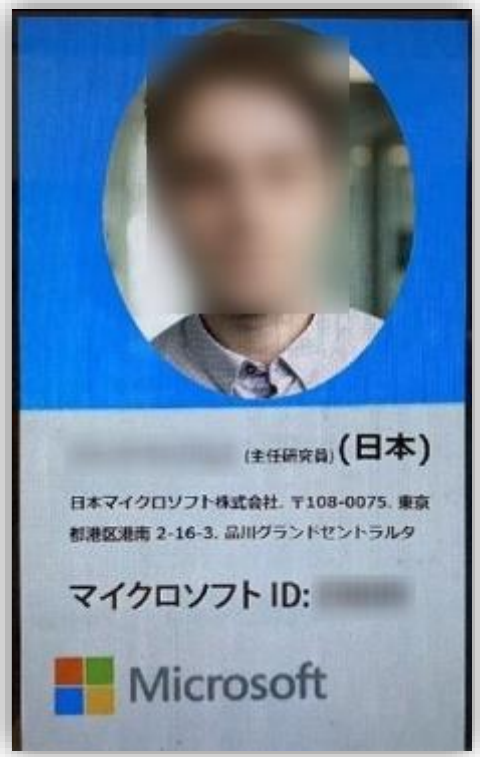
お客様、キーボードの一番下の一番左のキーを見てください。
なんて書いてありますか？
その隣は？その隣にウインドウズのロゴマークのキーがありますか？
ウインドウズのロゴマークのキーとRを同時に押します。どうなりましたか？

・こののち、「ファイル名を指定して実行」では、遠隔操作ソフトのダウンロードや、
遠隔操作サービスサイトなどのURLを入力を指南する

オペレータによる偽社員証の提示

■偽オペレーターが提示する偽社員証

・これらの社員証のような画像はネット上でも検索することができ、単に流用していると考えられる



・遠隔操作開始直後、社員証を画面上に表示し、ウソの身分を説明する
・遠隔操作ソフトのファイル転送機能により、被害者のデスクトップ上へ画像ファイルをコピーし、それを開く
・システムの復元後も、デスクトップ上に画像ファイルが残り、サムネイル表示され、まだ遠隔操作が続いていると誤解する被害者も多数いる

（上記写真は、相談者のデスクトップ上に残っていたファイルや、画面をスマホで撮影されたものを情報提供していただいたもの）

オペレータによる嘘の説明（遠隔操作併用）

■ウイルスに感染していると思い込ませるための嘘の展示と説明

・イベントビューアで「警告」や「エラー」を見せてハッカーの仕業と説明

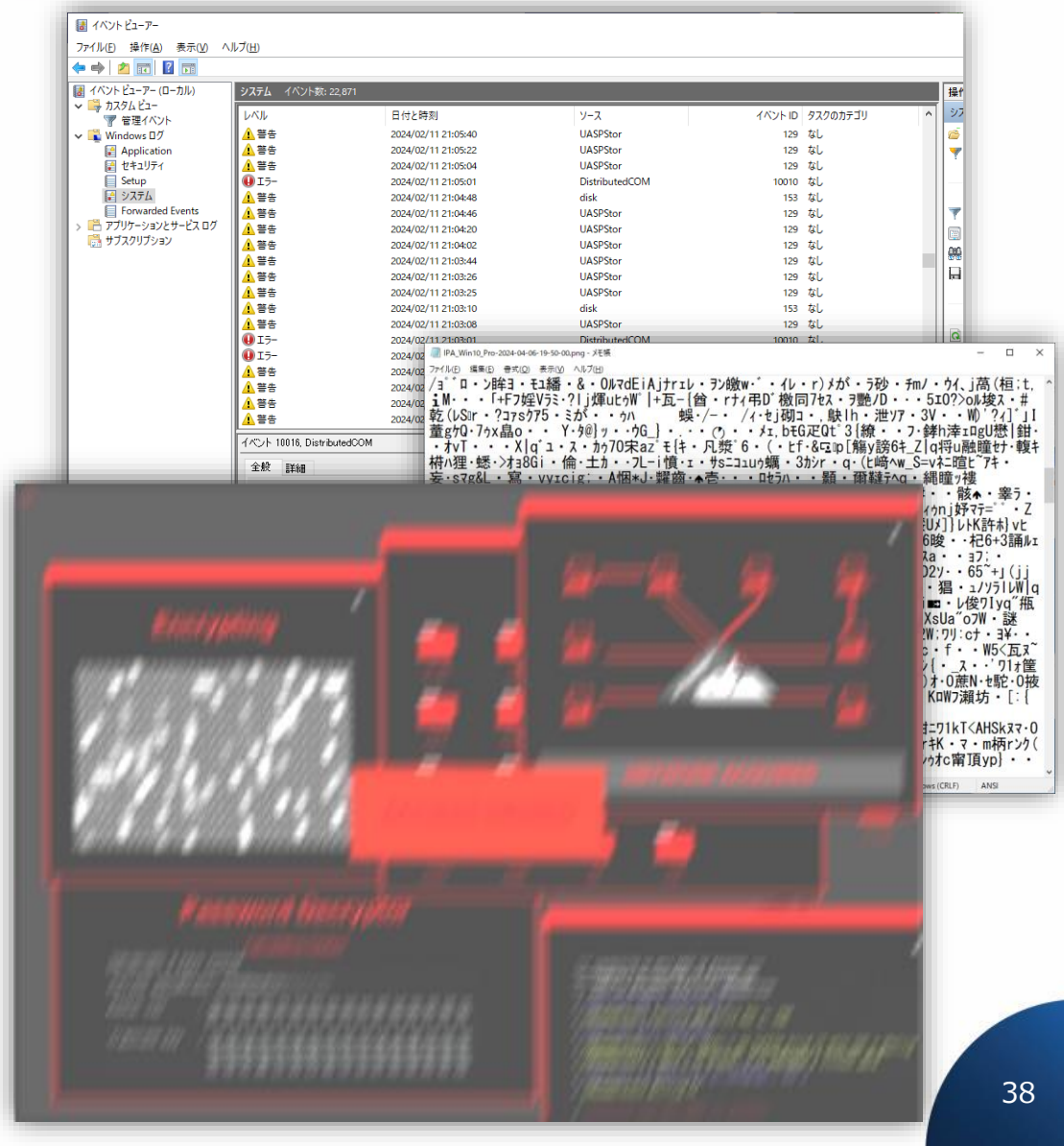
・バイナリファイルをメモ帳で開き、ハッカーによって改ざんされたと説明

■　ハッキングツールの画面を模倣したサイトを開き、嘘の説明

・相談者が信じ込んでしまうことを相談内容から確認している

■パソコンから情報が漏えいしていると嘘の説明

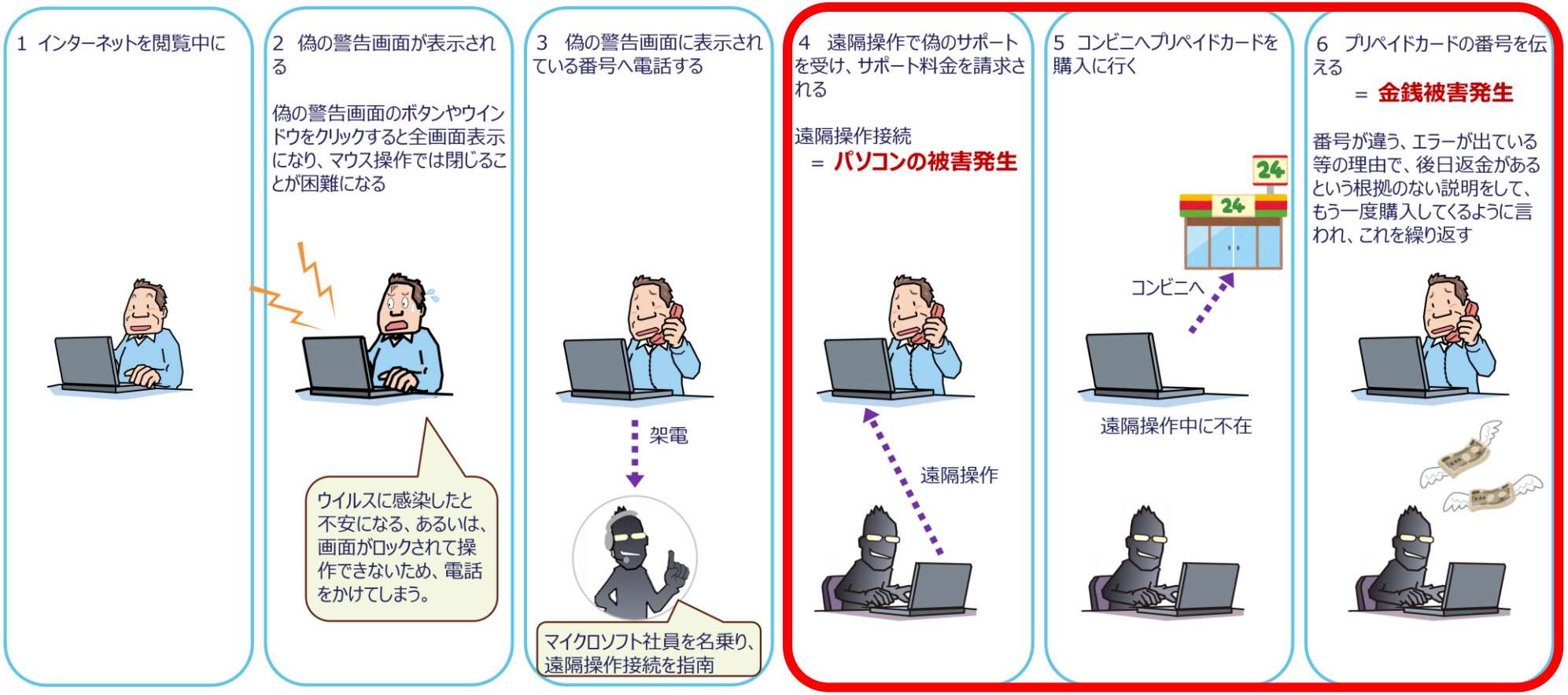
・パソコンのカメラアプリを開き、被害者や室内が画面に映るのを悪用し、世界中にプライベートが流出していると嘘の説明



オペレーターの対応

遠隔操作で偽のサポートを演じ、被害者にウイルス対処を思い込ませたのちに、料金の支払いへ話が移行する

大半の被害者は、この時点で詐欺を疑うなどして、金銭支払いを行わないケースが増えている



金銭支払いに応じさせるため、遠隔操作で設定変更する

■データを元に戻すために金銭を支払わせる

・デスクトップのアイコンを非表示に設定

・デスクトップのアイコンを全て削除された（ゴミ箱）

■ウイルスが残っていると思わせ金銭を支払わせる

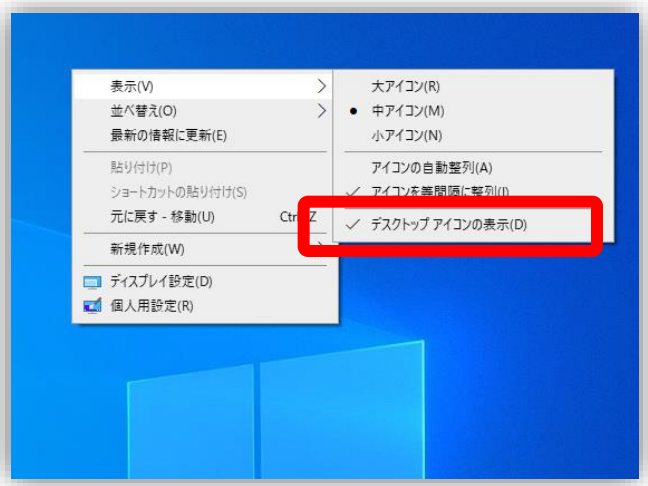
・背景を変更された（黒や赤の原色）

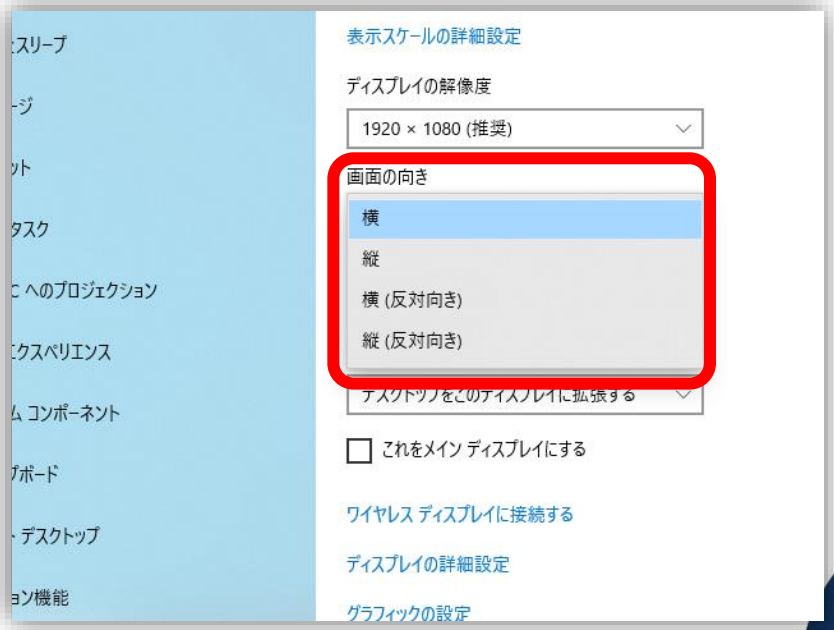
■パソコンが使えるようにするため金銭を支払わせる

・画面の向きを変えられた

・スタートアップに「Windowsシャットダウンとコメント」を登録された
（サインインするとすぐにシャットダウンする）

・金銭を取得できなかった場合の、犯罪者側にとって保険的な措置であると考えられる
・これらの設定変更によってパソコンが元通り使えないために、再び偽サポートへ電話した相談者も確認している





金銭的被害（未遂含む）

■遠隔操作中にAmazonで5万円のギフト券を購入され、ギフトコードを送信された（被害者は気付かず）

・本被害は2024年2月頃から確認されるようになった

・なお、サポート料金としてAmazonのギフト券購入を指示された例もある

■サポート料金としてコンビニでプリペイドカード型電子マネーを購入し、プリペイドカード番号を伝えた

■プリペイドカード番号が違っていると言われ、再度プリペイドカードを購入した

■サポート料金としてネットバンキングで送金した

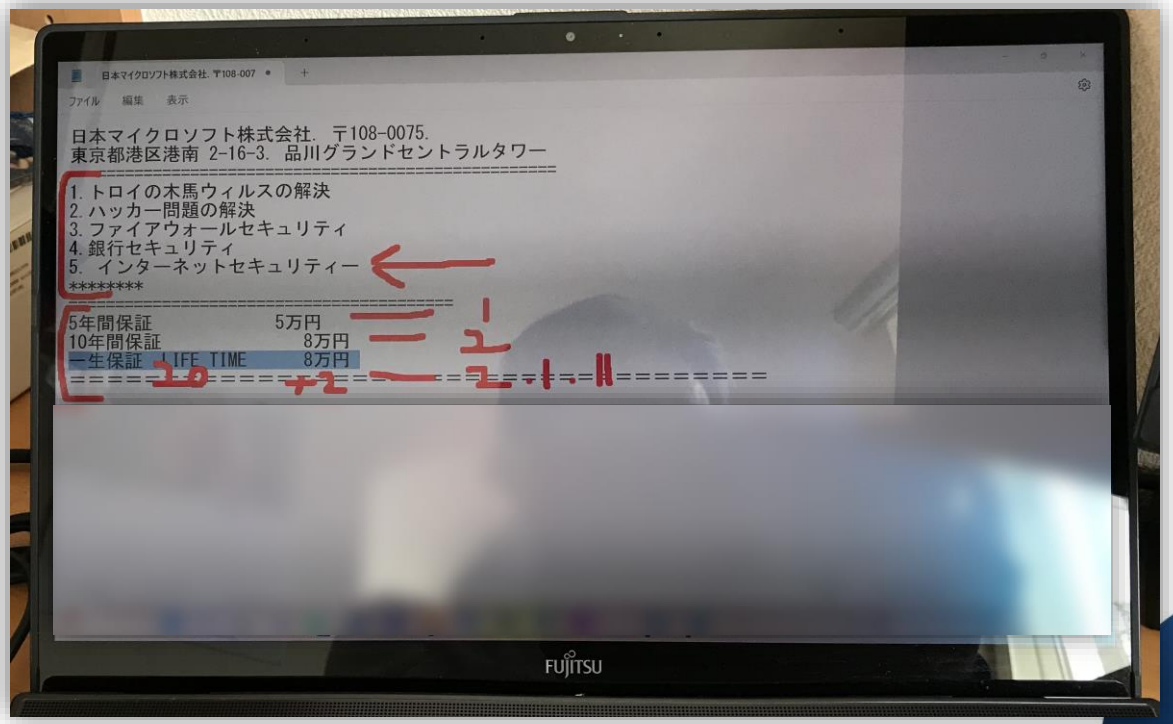
■ネットバンキングで送金する際に、遠隔操作で送金金額を変更され多額の不正送金をされた

■ハッカーから預金を守るため、一次的に安全な口座に残高を移すように指示された（未遂）

■国際通話料金

・キャリアや契約プランで異なるが、アメリカへの国際通話は1分間当たり約70～80円

・偽の警告画面ではフリーダイヤルと嘘が書いてある



■ 2024年から急激に増加している、
偽警告画面を表示するサイトへ誘導する広告の状況

「開く」「次へ」などのリンクボタンに偽装した広告の出現

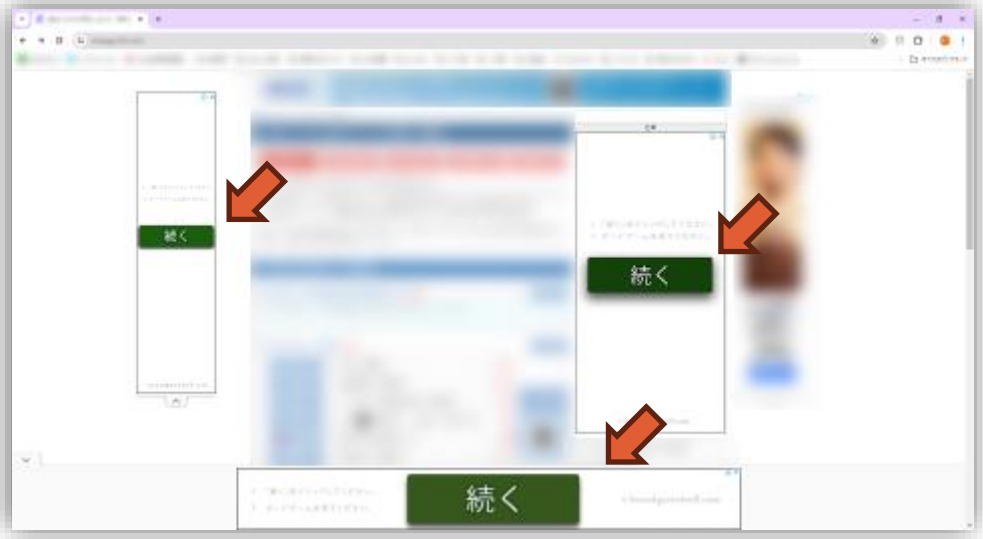
ディスプレイ広告枠

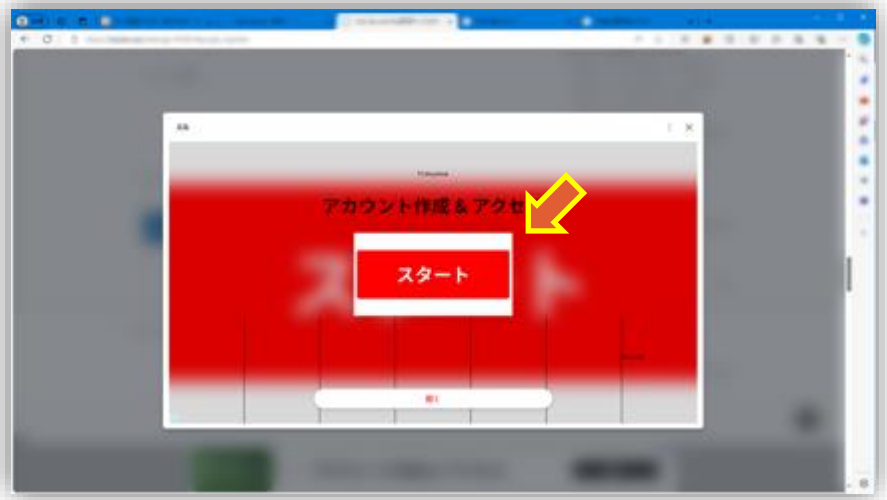
サポート詐欺の被害を伝えるニュースや記事のページにも、サポート詐欺へ誘導する広告が出現

「開く」「次へ」などのリンクボタンに偽装した広告の出現

ディスプレイ広告枠

左）一つのページに複数のボタン風の広告
　　画面をスクロールする間、絶えず画面内のどこかにボタンが出現する配置となっている
中）コンテンツを取り囲むように配置されたボタン風の広告
右）ウェブページにオーバーレイ表示される広告。右上の×をクリックすると消えるが、出現してから数秒間はクリックできなくなっている。（※例示している広告は偽警告ではなくオンラインアクティベーション・フィッシングサイトへ誘導される）





検索サイトの検索連動型広告枠に出てくる偽リンク

相談者の声
インターネットの検索からリンクをクリックしたら、Defenderのセキュリティ警告が出て、表示された電話番号に電話をして、オペレータの指示に従った

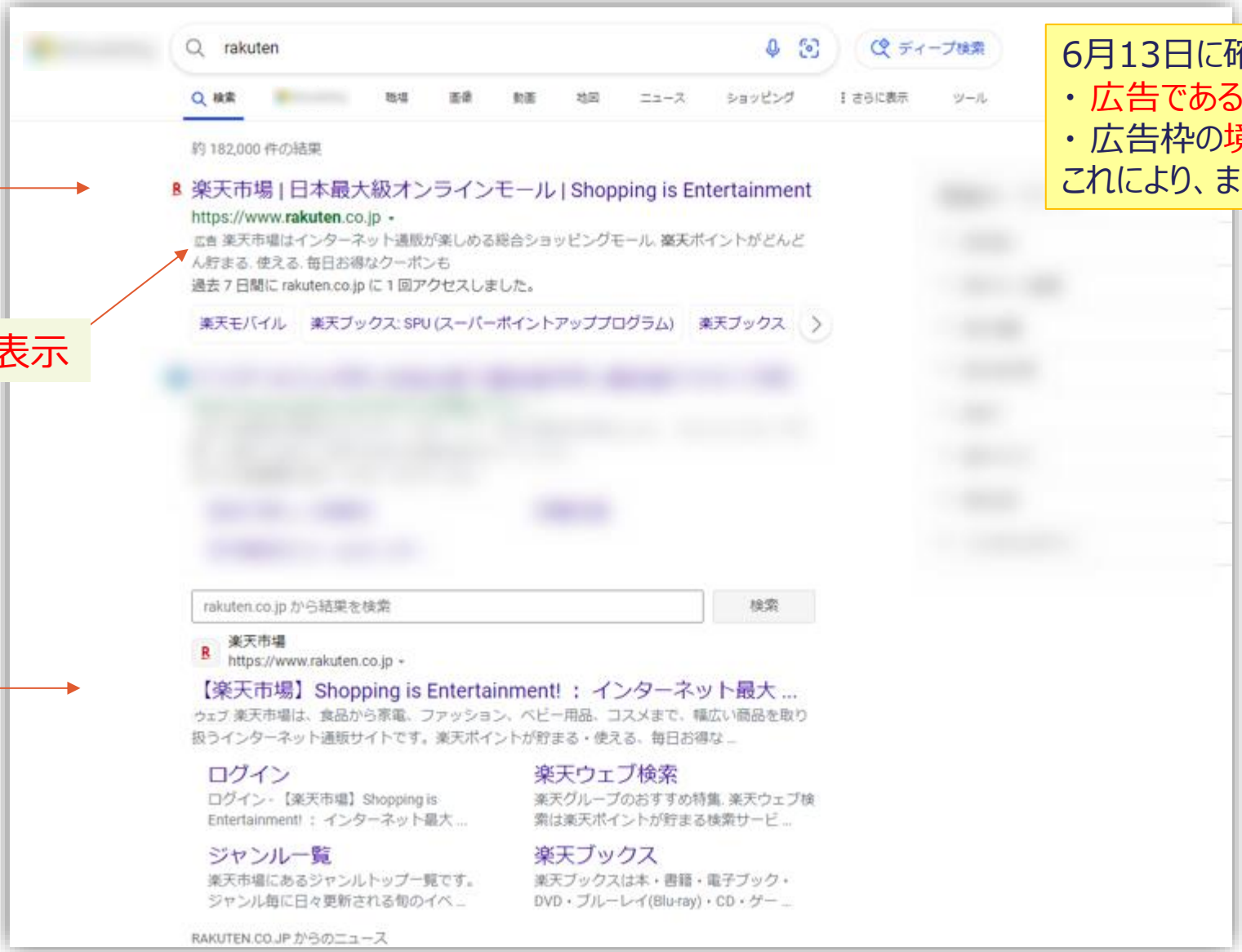
6月13日追加

検索サイトの検索連動型広告枠に出てくる偽リンク

偽警告へリンク

広告であることの表示

楽天へリンク

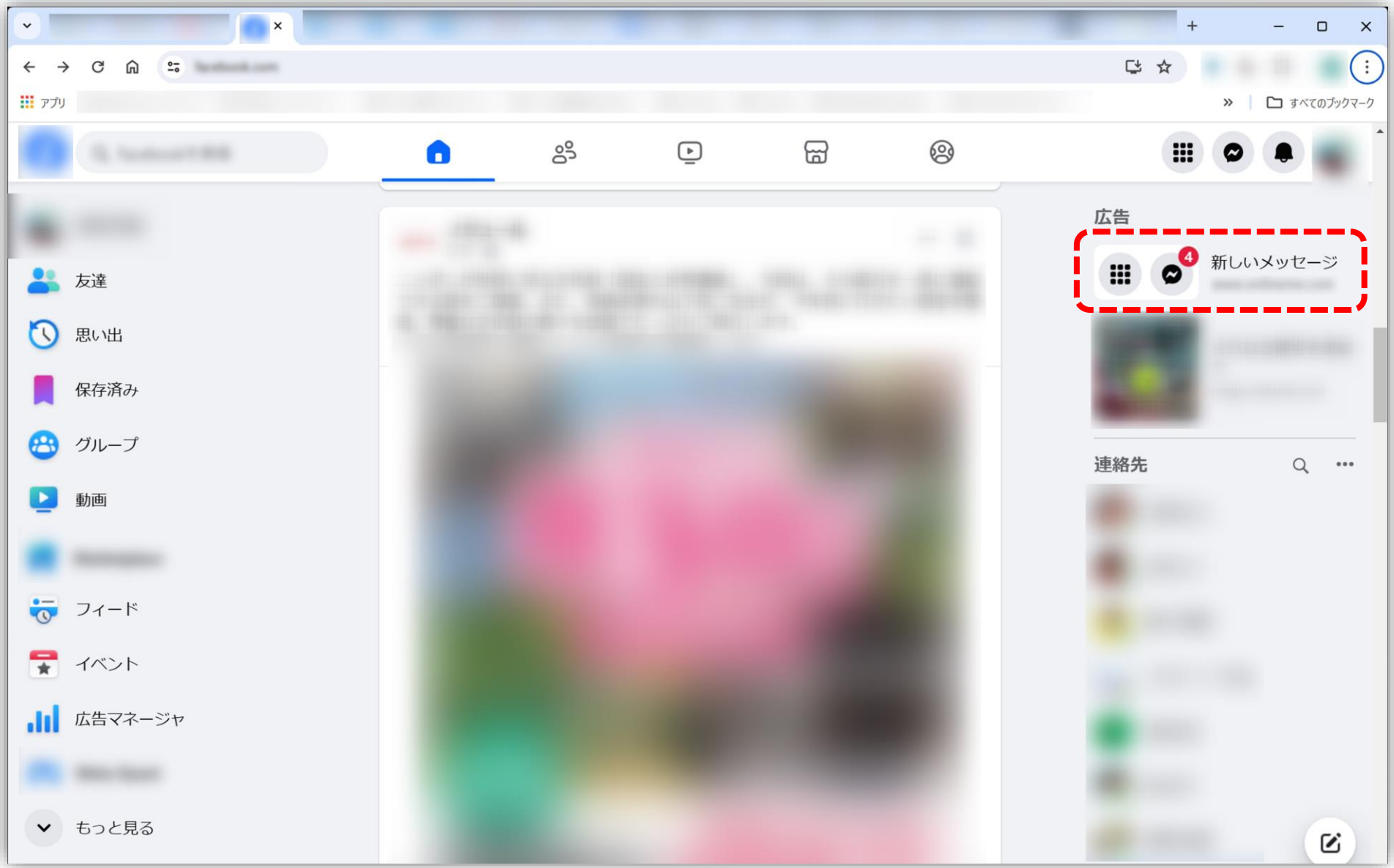


6月13日に確認された検索結果には
- 広告である表示が小さく見えにくい
- 広告枠の境界線がない

これにより、ますます**見極めることは困難に**

6月13日追加

SNSにメッセンジャー通知を偽装した広告



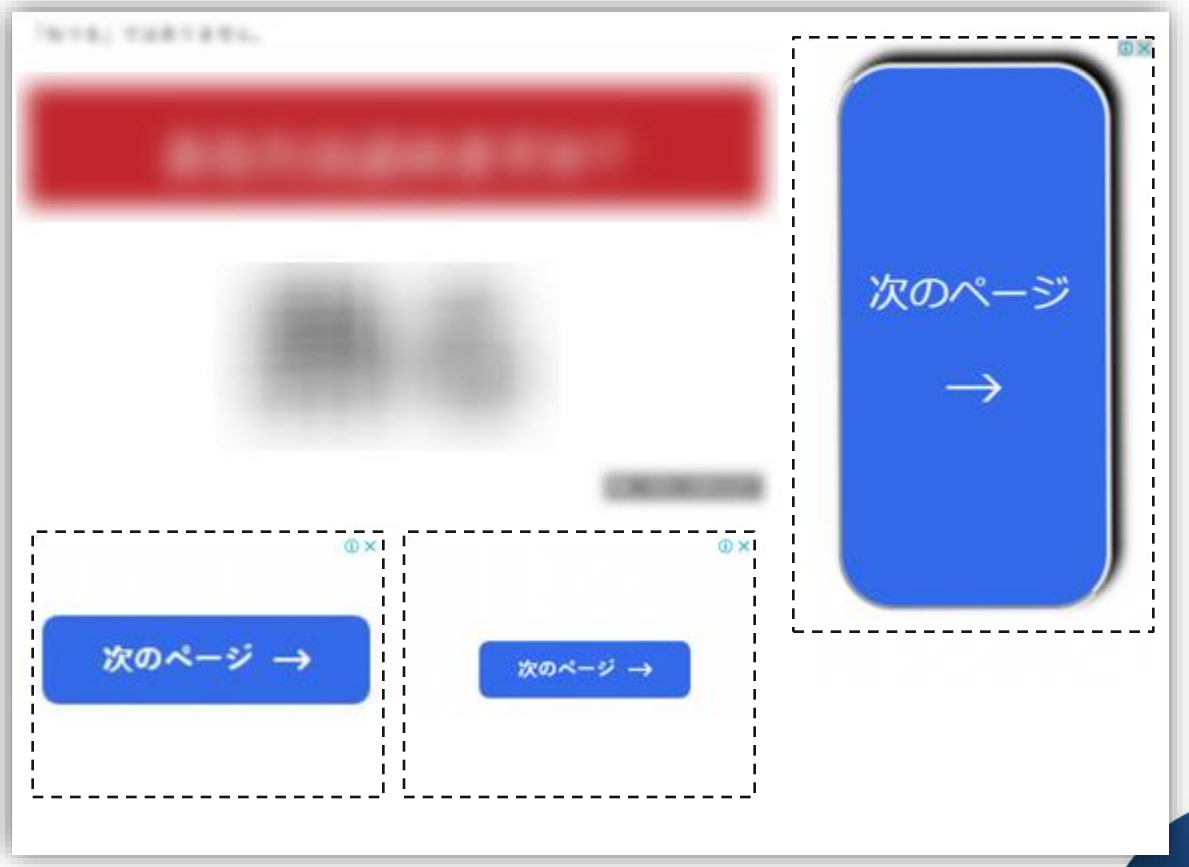
6月10日に相談者からの画像情報提供

・メッセンジャーの通知を装ったイメージを表示し、クリックすると偽警告画面が表示される

・その後、他の利用者からも情報が寄せられている

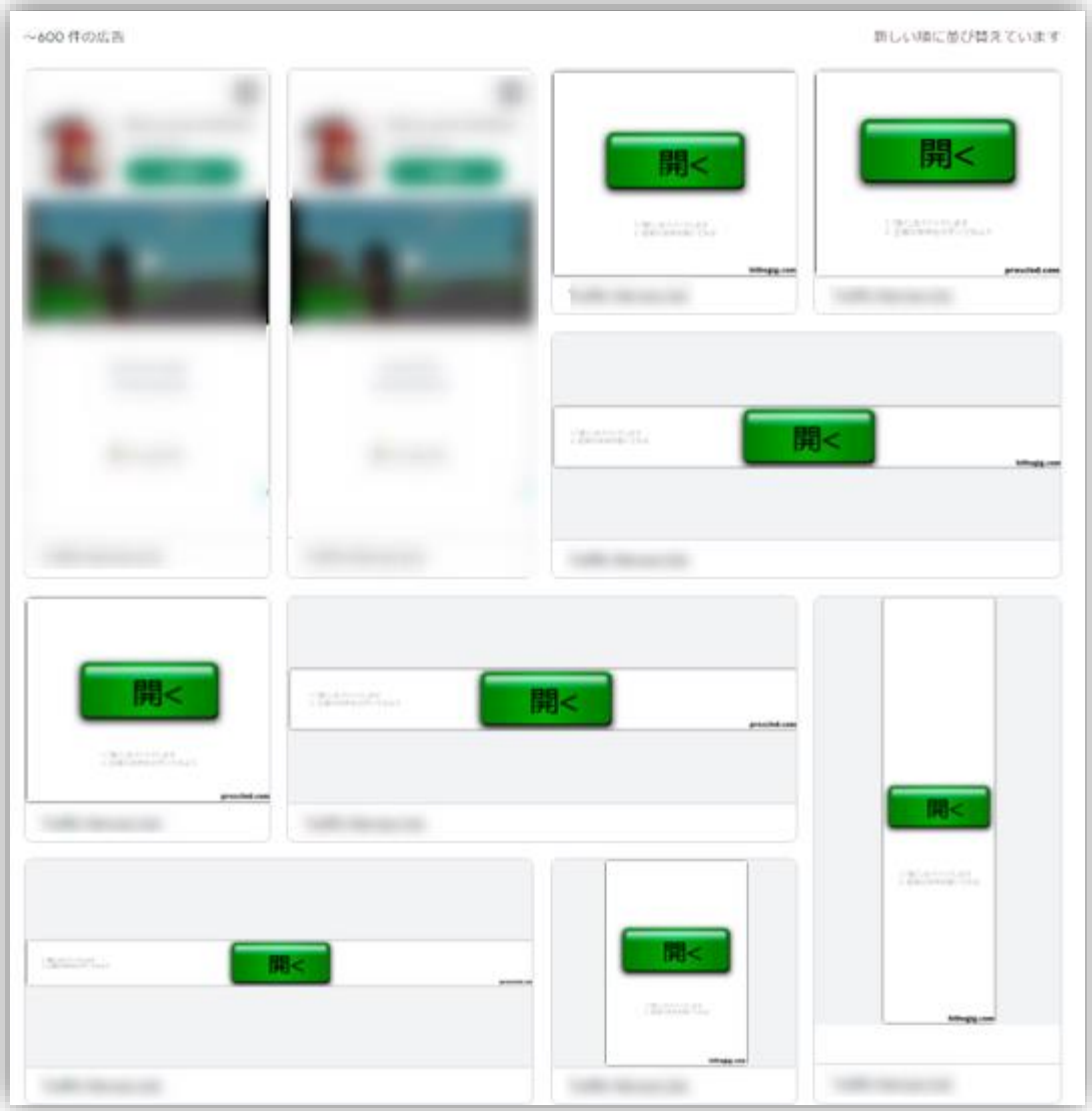
広告枠の判断

- 広告枠の右上（左下）には ⓘ ✕ の小さなボタンアイコンがある。左が情報ボタン、右が広告を閉じるボタン
- 広告枠の広告画像は矩形型であり、この右上のボタンアイコンが目安になる（右図）
- ボタンに似せた広告画像は、背景色の余白を多めに取ることで右上のアイコンから離れて見え、広告と判断しにくくなっている



広告主の登録している他の広告画像

様々な広告枠のサイズに合わせたような、偽画像（ボタン）が確認できる（画像にボタンの周囲の余白も確認できる）



アクセス元によってリダイレクト先が振り分けられる例（偽警告サイトのURLがこまめに変わる）

確認した多くのサイトやサーバ遷移から一例を簡略して紹介

■IPAからインターネットアクセス ⇒ ファーストフードチェーンのホームページへ

■プライベート環境からインターネットアクセス ⇒ 偽警告表示サイトへ

・アクセス元によって振り分けられる ⇒ 例：広告審査で偽警告が出ない。レジデンシャルIPを狙う

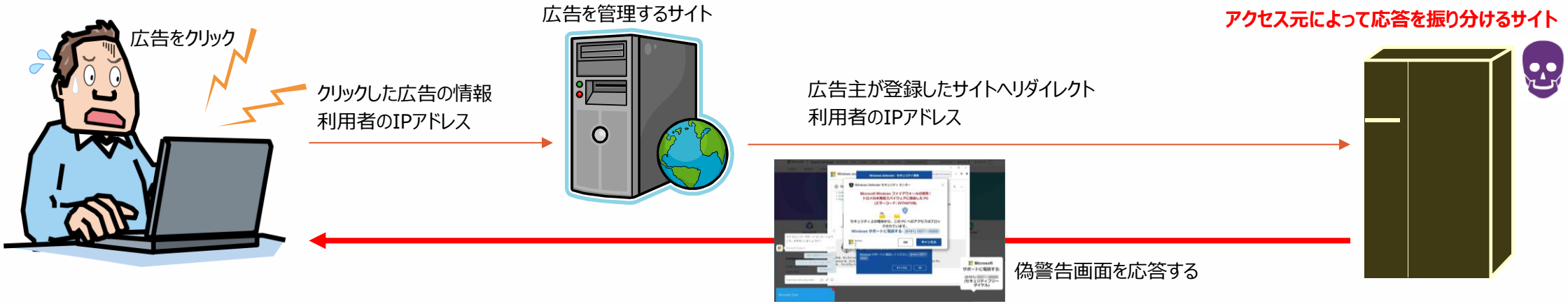
・偽警告表示サイトのURLが数分で変更される。 ⇒ リダイレクトによるアクセスの強要（URLをブックマークしても次回はアクセスできず）

振り分けされずに偽警告サイトへ到達する例（偽警告サイトのURLが変わらない）

確認した多くのサイトやサーバ遷移から一例を簡略して紹介

■IPAからインターネットアクセス ⇒ ファーストフードチェーンのホームページへ

■プライベート環境からインターネットアクセス ⇒ 偽警告表示サイトへ

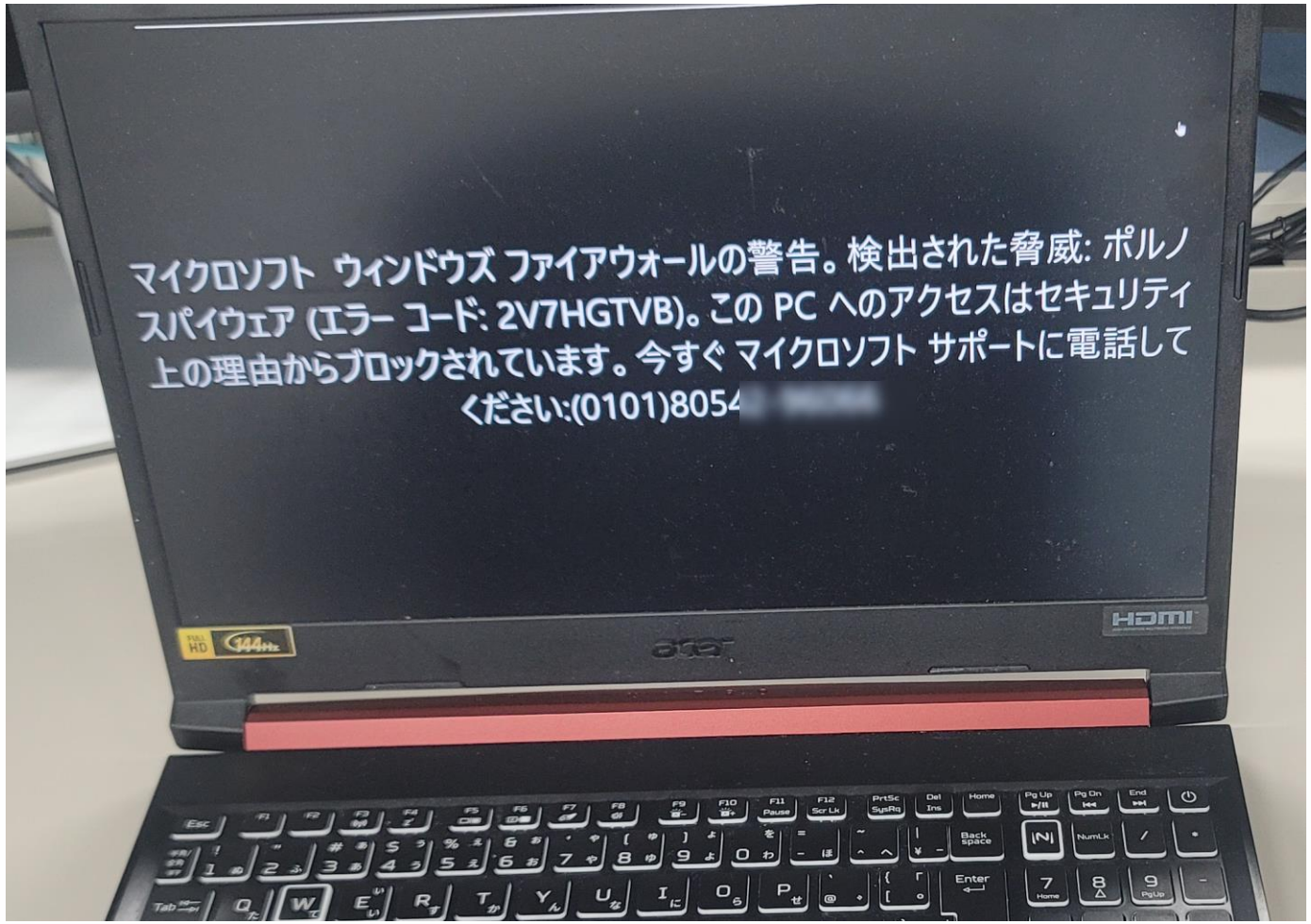


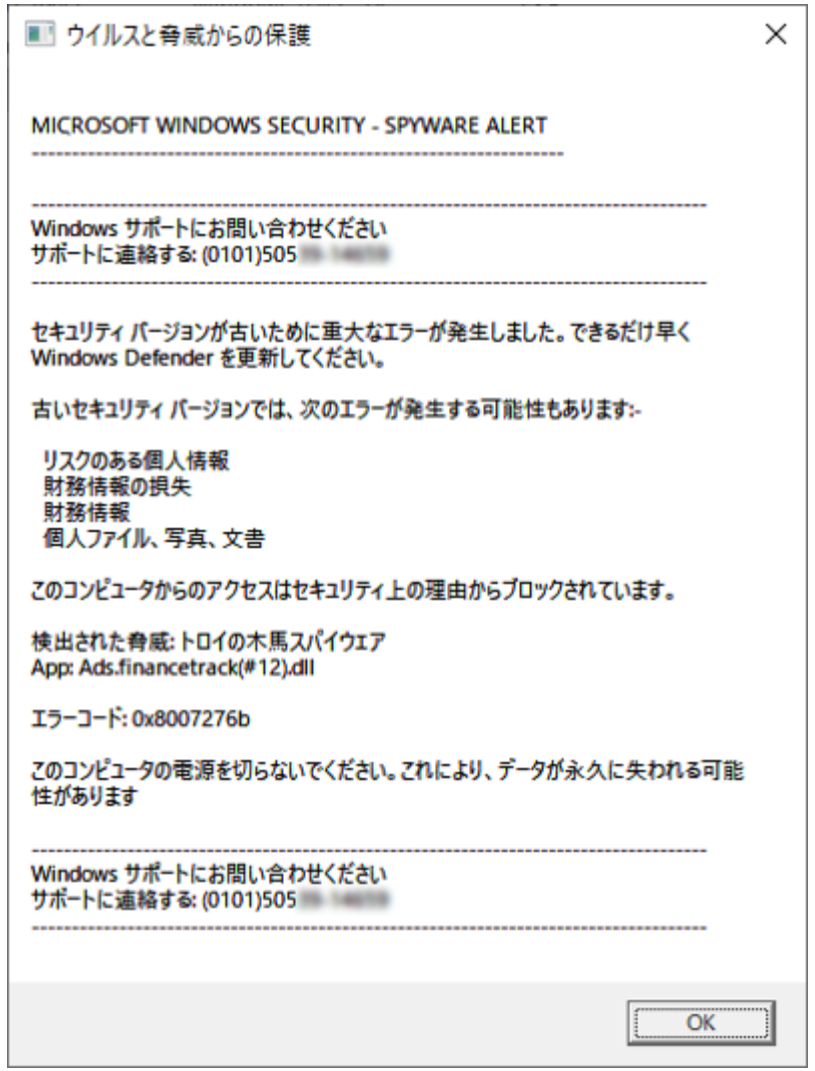
・広告リンクで移行したサイトで、応答するページが振り分けられる（説明のため詳細を一部省略）
・偽警告表示サイトのURLは長時間有効で、URLで直接アクセスしても同じ結果になる

6月24日追加

新たな偽警告画面の手口か？（確認中）

■全画面にテキストだけで表示される偽警告（左）と、ダイアログ表示される偽警告（右）





最新情報　7月22日更新
新たな偽警告画面の手口か？（確認中）

■確認できている事象
- 黒い警告画面（前ページ左側）が突然表示され、パソコンの操作ができなくなる
- ネットワークを切断してしばらくすると、黒い警告画面は消えて、パソコン操作ができるようになる
- 黒い警告画面が消えたあとに次の事象を伴う場合がある
    - ・デスクトップやデスクトップ上のアイコンが表示されず、白い警告画面（前ページ右側）が表示されている
    - ・白い警告画面（ダイアログ表示）は、OKや閉じるボタンを押してもすぐに再表示される。再起動しても表示される
- 黒い警告画面が出ている間に、リモートオペレーションをされていることを確認している

■確認できている原因
- インターネットからダウンロードされた不審なファイルを実行するとRMM（Remote Monitoring and Management）がインストールされる
- 管理者権限がなくてもインストールされ、インストール後は即時実行される。また、インストール中の操作によってサービス登録される
- サービス登録されてしまうと、強制終了しても、再起動後にRMMは起動し常駐する
- 黒い警告画面はRMMの相手側の操作により、表示されたり表示されなかったりする
- 白い警告画面の症状は、スタートアップに不正に登録された.batファイルと.vbsファイルによる

■現時点での最良の対処
- 黒い警告画面が表示されたら、すぐにネットワークを切断する（LANケーブルを抜く、Wi-Fiアクセスポイントの電源を切る等）
- 白い警告画面が表示されていたら、タスクマネージャで”Microsoft Windows Based Script Host”を終了する
- タスクバーやデスクトップが表示されていない場合は、タスクマネージャの「新しいタスクを実行」で”explorer”を実行する
- デスクトップアイコンが表示されていない場合は、デスクトップ上でマウスを右クリックし「表示」→「デスクトップアイコンの表示」と操作する
- パソコンが操作できるようになったら、重要なファイルや情報を取り出し、パソコンを初期化（再インストール）する

※本警告画面と、既存サポート詐欺手口との関連性は不明

■ IPAの取り組み

サポート詐欺体験サイトの作成・公開中

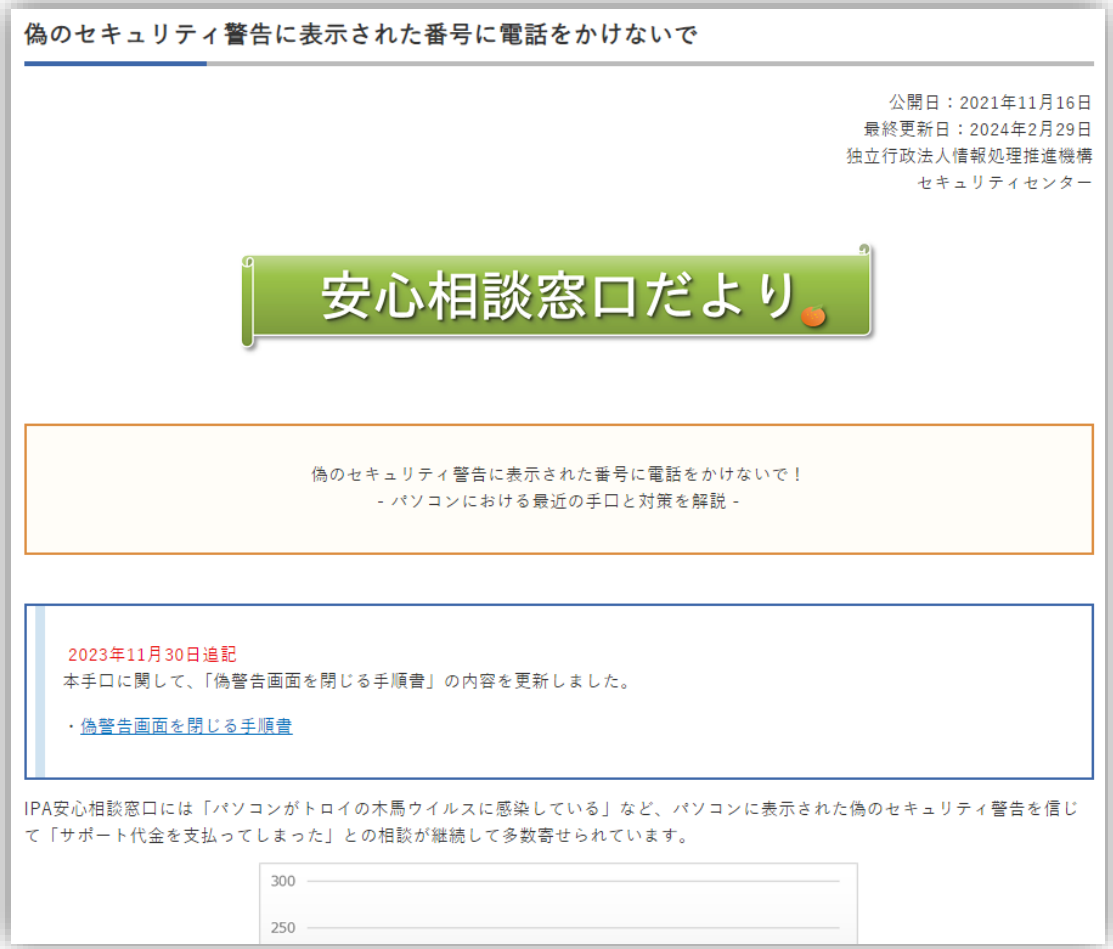
https://www.ipa.go.jp/security/anshin/measures/fa-experience.html

ふなっしーも体験

NHK：NEWS WEB
https://www3.nhk.or.jp/lnews/chiba/20240205/1080022653.html

安心相談窓口だよりによる注意喚起（個人向け・組織向け）

■個人（一般利用者）向け



偽のセキュリティ警告に表示された番号に電話をかけないで

公開日：2021年11月16日
最終更新日：2024年2月29日
独立行政法人情報処理推進機構
セキュリティセンター

安心相談窓口だより

偽のセキュリティ警告に表示された番号に電話をかけないで！
- パソコンにおける最近の手口と対策を解説 -

2023年11月30日追記
本手口に関して、「偽警告画面を閉じる手順書」の内容を更新しました。
・偽警告画面を閉じる手順書

IPA安心相談窓口には「パソコンがトロイの木馬ウイルスに感染している」など、パソコンに表示された偽のセキュリティ警告を信じて「サポート代金を支払ってしまった」との相談が継続して多数寄せられています。

300
250

https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211116.html

■組織向け

会社や組織のパソコンにセキュリティ警告が出たら、管理者に連絡！

公開日：2023年7月11日
独立行政法人情報処理推進機構
セキュリティセンター

安心相談窓口だより

会社や組織のパソコンにセキュリティ警告が出たら、管理者に連絡！
- セキュリティ警告が出た際の対応ルールを改めて徹底しましょう -

IPA情報セキュリティ安心相談窓口における、パソコンのブラウザ画面に表示される「偽セキュリティ警告（別名：サポート詐欺）」の手口（図1）に関する相談件数が継続して増加しています。月間相談件数が、2023年5月は過去最高の446件となりました（図2）。また、最近では、組織や企業においてもサポート詐欺の被害にあったという報道を目にするケースがあります。数は少ないですが当相談窓口にも組織や企業からも当該被害に関する相談が寄せられています。

企業・組織ではテレワークで社員や職員が自宅で業務用パソコンを使って仕事をする機会が増え、「偽セキュリティ警告（サポート詐欺）」の手口に遭遇した際に、同僚、上司、システム管理者が近くにいないため、自分で解決しようとして被害が発生していることも要因のひとつと思われます。

組織や企業にて、表示された電話番号に電話をかけて、相手にパソコンを遠隔操作されると、パソコン内に機密情報や個人情報が保管されていた場合に、情報漏えい事故としての対応が必要になるかの判断や調査を迫られます。その結果、情報漏えい事故として対外的に発表を行うケースが発生しています。

これまで当窓口において「偽セキュリティ警告（サポート詐欺）」については一般ユーザー向けに様々な注意喚起を実施してきましたが、今回は組織や企業向けに同手口に関する注意点を説明いたします。

https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20230711.html

機を失せずSNSによる注意喚起（X・Facebook）

■X（旧Twitter）

X: @IPA_anshin https://x.com/IPA_anshin

■Facebook

Facebook: ipa.anshin https://www.facebook.com/ipa.anshin

まとめ

- 相談件数は今後も同水準で続くと思われる
- 被害者をだますための手口も変化し続けると考えられる
- インターネット利用時に表示される広告など、一般の方が広く目にする場所から偽警告に誘導されることが、主な被害要因と考えられる。
- 各機関が連携して一般向けの啓発活動を行っていくほか、不正な広告等、誘導経路そのものを減らしていくための取組みが重要である。