

2025 年 6 月 14 日

発表者：坂本和弘



一緒にセキュリティ意識を高め、



インターネットを安全に使いましょう！



目次

1. 情報セキュリティの重要性	3
a. 情報セキュリティとは？.....	3
2. サポート詐欺とは？	5
a. 詐欺の定義と基本的な仕組み.....	5
b. なぜ被害が拡大しているのか？.....	5
c. 過去の被害事例（簡単な統計データ）.....	5
3. サポート詐欺の手口	6
a. 偽の警告ポップアップ.....	6
b. 偽サポートサイトや電話による誘導.....	6
c. 遠隔操作ソフトを使った詐欺.....	6
d. 金銭や個人情報に要求する手法.....	6
4. サポート詐欺を防ぐ方法	7
a. 怪しい警告メッセージを無視する.....	7
b. 公式サイトで情報確認.....	7
c. セキュリティソフトの活用.....	7
d. 不審な電話やメッセージに反応しない.....	7
e. 個人情報を安易に提供しない.....	7
5. サポート詐欺に遭ってしまった場合	8
a. すぐに公式サポートに相談.....	8
b. クレジットカード会社へ連絡（不正請求の対応）.....	8
c. 証拠を保存し、警察や消費者庁へ報告.....	8
d. 金銭のやり取りがあった場合の 決済記録.....	8
e. パスワード変更やセキュリティ対策強化.....	8
6. 情報セキュリティの意識向上	10
a. 企業や個人で取り組むべきセキュリティ対策.....	10
b. セキュリティ教育の重要性（従業員研修や個人学習）.....	10
c. 定期的なセキュリティチェックの推奨.....	10
7. まとめ	11
a. 「詐欺に遭わないための3つのポイント」.....	11
i. 1 怪しい警告やメッセージに惑わされない	11
ii. 2 個人情報を慎重に管理する	11
iii. 3 冷静に対応し、疑わしい場合は相談する	11
b. 注意喚起のメッセージ.....	11
*参考までに！①・②（巻末）	

1. 情報セキュリティの重要性

a. 情報セキュリティとは？

情報セキュリティとは、情報資産の「**機密性**」「**完全性**」「**可用性**」を確保するための取り組みを指します。つまり、次の3つのポイントを満たす状態を維持することが目的です。

- ① 情報の不正な閲覧や漏えいを防ぐ (**機密性**)
(限られた人だけが情報にアクセスできるように制限をかける)
- ② ウィルス等の不正な改ざんなどから情報を保護し正確に保つ (**完全性**)
- ③ 必要な時に情報にアクセスできる (**可用性**)
(システムが継続して稼働できる)

情報セキュリティの3要素 (CIA)

- ① **機密性**¹ (Confidentiality)
- ② **完全性**² (Integrity)
- ③ **可用性**³ (Availability)

* 情報セキュリティの対象には、デジタルデータだけでなく紙の文書など非デジタルの情報も含まれます。

なぜ個人・企業にとって重要なのか？

情報は、個人にとっても企業にとっても貴重な資産です。例えば**個人情報**が流出すると**詐欺やなりすましの被害を受ける可能性**があり、**多額の金銭被害**に繋がる可能性もあります。企業の場合、機密情報の漏洩は経済的損失やブランド価値の低下を招き、信頼を失うことにつながります。

セキュリティリスクの種類 (サポート詐欺、フィッシング、マルウェアなど)

¹ パスワードの設定

² セキュリティソフトの設定

³ 代替機の手配やデータのバックアップ

サポート詐欺

偽の技術サポートを装い、ユーザーを騙して金銭を要求したり、不正アクセスを試みたりする詐欺のことです。「あなたの PC に問題があります」と偽の警告を表示し、サポート費用を請求するケースが一般的です。

フィッシング

本物そっくりのメールや Web サイトを使い、個人情報やログイン情報を盗み取る攻撃手法です。銀行やオンラインサービスを装って偽のログインページに誘導し、ユーザーが情報を入力してしまうケースがよくあります。

マルウェア

悪意のあるソフトウェアで、デバイスに感染するとデータを盗まれたり、システムを破壊されたりする可能性があります。代表的なものに、ウイルス、ワーム、トロイの木馬、ランサムウェアなどがあります。

* IPA に寄せられている相談件数推移（IPA 資料参照）



2. サポート詐欺とは？

a. 詐欺の定義と基本的な仕組み

サポート詐欺とは、偽の技術サポートを装い、ユーザーを騙して金銭を要求したり、不正アクセスを試みたりする詐欺のことです。典型的な手口としては、インターネット閲覧中に「あなたの PC に問題があります」と偽の警告画面を表示し、ユーザーを不安にさせて電話をかけさせるものがあります。その後、詐欺師が遠隔操作を提案し、サポート料金を請求するケースが一般的です。

b. なぜ被害が拡大しているのか？

近年、サポート詐欺の被害が急増しています。その理由として、以下の要因が挙げられます。

巧妙化する手口 – 偽の警告画面がより本物らしくなり、ユーザーが騙されやすくなっています。

広告を悪用した誘導 – 偽の警告画面へ誘導する広告が増加し、一般のウェブサイトにも表示されるケースが報告されています。

検索結果の悪用 – 検索サービスの広告枠に偽のサポートサイトが表示されることがあり、ユーザーが誤ってアクセスしてしまうことがあります

c. 過去の被害事例（簡単な統計データ）

2023 年のサポート詐欺を含む架空料金請求詐欺の認知件数は **5,198 件** で、前年比 **1.8 倍** に増加しています。

被害額は **140.4 億円** に達し、前年比 **1.4 倍** に増加しています。

2023 年に IPA⁴ の「情報セキュリティ安心相談窓口」に寄せられた相談のうち、サポート詐欺に関するものは **4,145 件** で、全体の **38%** を占めています。

参考 URL: [茨城県 “サポート詐欺” 相次ぐ 警察が相談や対応を呼びかけ](#)

参考 URL: [「PC 感染、修理費は電子マネーで」と言われ…詐欺被害 355 万円](#)

参考 URL: [携帯電話サポートセンター名乗る電話きっかけの詐欺事件か](#)

⁴ 参考 URL: [IPA 独立行政法人 情報処理推進機構](#)

3. サポート詐欺の手口

参考 URL: [【手口検証動画】偽のセキュリティ警告画面](#)

参考 URL: [サポート詐欺の手口・対処方法に関する動画／茨城県警察](#)

a. 偽の警告ポップアップ

ユーザーがインターネットを閲覧している際に、突然「ウイルスに感染しました」「PC に深刻な問題があります」などの偽の警告が表示されることがあります。これらのポップアップは、不安を煽ってユーザーに電話をかけさせる目的で作られています。

b. 偽サポートサイトや電話による誘導

偽の警告ポップアップに記載された電話番号に連絡すると、詐欺師が本物のサポートスタッフのように対応します。また、検索エンジンの広告枠や偽のサポートページを使って、ユーザーを騙すこともあります。これらのサイトは公式のものに似せて作られているため、見分けるのが難しくなっています。

c. 遠隔操作ソフトを使った詐欺

詐欺師は「問題を解決するために遠隔操作が必要」と偽り、リモートアクセスツール（例えば、TeamViewer や AnyDesk など）のインストールを促します。一度インストールすると、詐欺師はユーザーの PC を自由に操作できるようになり、個人情報の盗難やシステムの改ざんが行われる可能性があります。

d. 金銭や個人情報を要求する手法

遠隔操作後、「修理費用」「サブスクリプション料」「ウイルス除去費」などの名目で金銭を要求します。支払い方法として、クレジットカード情報やギフトカード購入を求めるケースがよくあります。また、個人情報を抜き取られ、さらなる詐欺やなりすまし被害につながることもあります。

4. サポート詐欺を防ぐ方法

a. 怪しい警告メッセージを無視する

偽の警告ポップアップはユーザーの不安を煽るために作られています。これらに反応しないことが重要です。突然「ウイルスに感染しました」などの警告が表示されても、閉じるか無視し、表示された電話番号には連絡しないようにしましょう。

b. 公式サイトで情報確認

システムやソフトウェアに問題があるかどうかを確認する際は、必ず公式のサポートサイトを利用しましょう。企業の公式ページには正規のサポート窓口が記載されているため、そこから正しい情報を得ることができます。

c. セキュリティソフトの活用

信頼できるセキュリティソフトを導入することで、怪しいサイトや詐欺ポップアップをブロックできます。また、定期的なアップデートを行うことで、最新の詐欺手口から身を守ることが可能になります。

d. 不審な電話やメッセージに反応しない

知らない番号からの電話や、不審なメール・メッセージには注意しましょう。「技術サポート」や「セキュリティアラート」などの内容でも、本当に正規のサービスかどうかを確認することが大切です。

e. 個人情報を安易に提供しない

詐欺師は、クレジットカード番号や銀行口座情報を盗むために巧妙な手口を使います。オンライン上では、自分の個人情報を慎重に管理し、不審な要求には応じないようにしましょう。

5. サポート詐欺に遭ってしまった場合

参考 URL : [JPA 偽警告注意動画](#)

参考 URL : [偽のセキュリティ警告画面の閉じ方体験サイト](#)
(IPA 資料参照)

a. すぐに公式サポートに相談

詐欺の可能性があると感じたら、まずは PC やスマートフォンの公式サポート窓口 に相談しましょう。特に、Microsoft や Apple、Google などの正規サポートに問い合わせることで、正しい情報を得ることができます。

b. クレジットカード会社へ連絡（不正請求の対応）

詐欺師に支払いをしてしまった場合、クレジットカード会社に連絡し不正請求の取り消しを依頼しましょう。状況によっては、返金対応を受けられる場合があります。また今後の被害を防ぐ為にカードの再発行を検討するのも有効です。

c. 証拠を保存し、警察や消費者庁へ報告

被害を受けた際は、以下の証拠を保存しておくことが重要です。

- ① 詐欺の警告画面やメッセージの スクリーンショット
- ② 詐欺サイトの URL : XXXXX
- ③ 詐欺師との メールやチャットの履歴

d. 金銭のやり取りがあった場合の 決済記録

上記（c.）の情報を 警察（サイバー犯罪対策課）や消費者庁に報告し、被害を拡大させないようにしましょう。

e. パスワード変更やセキュリティ対策強化

遠隔操作を許可してしまった場合や、個人情報を入力してしまった場合は、

以下の対策を行きましょう。

- ① **すべての重要なパスワードを変更**（特に、銀行・メール・SNS アカウント）
参考 URL: [パスワード解析時間 15 文字以上を推奨](#)
- ② **段階認証の有効化**（認証アプリの導入など）* オーセンティケーター⁵
- ③ **信頼できるセキュリティソフトを使って PC をスキャン**
- ④ **OS やソフトウェアの最新アップデートを適用**

i. ⁵ 認証器（au・thén・ti・cà・tor） グーグルやマイクロソフトで提供

6. 情報セキュリティの意識向上

a. 企業や個人で取り組むべきセキュリティ対策

- ① **強固なパスワード管理**: 長く複雑なパスワードを設定し、使い回しを避ける。
- ② **二要素認証（多要素認証）の導入**: ログイン時に追加の認証手段を設定し、不正アクセスを防ぐ。
- ③ **定期的なソフトウェア更新**: OS やアプリを最新の状態に保ち、脆弱性を修正する。**(ウィンドウズアップデートの更新)**
- ④ **アクセス制御の強化**: 企業内の重要情報には、権限を持つ人のみがアクセスできるようにする。
- ⑤ **データの暗号化**: 機密情報は暗号化し、盗まれても悪用できないようにする。

b. セキュリティ教育の重要性（個人学習）

個人学習

インターネットを安全に利用するために、**基本的なセキュリティ知識を身につけること**が大切です。例えば、**怪しいリンクやメールに注意する**、**SNS での情報公開を制限する**などの対策があります。

c. 定期的なセキュリティチェックの推奨

セキュリティ診断ツールの利用: 企業や個人向けのセキュリティ診断ツールを活用し、システムの安全性を定期的に確認しましょう。

Windows には、セキュリティ診断や脆弱性チェックを行うための便利なツールがいくつかあります。ツールを活用することで、システムの安全性を確認し、セキュリティ対策を強化できます。

Windows セキュリティ (Windows Defender)

Windows に標準搭載されているセキュリティツールで、ウイルスやマルウェアのスキャン、ファイアウォール管理、リアルタイム保護を提供します。

7. まとめ

a. 「詐欺に遭わないための3つのポイント」

i. ① 怪しい警告やメッセージに惑わされない

突然の「ウイルス感染警告」や「緊急対応を求めるメール」は詐欺の可能性が高いです。

表示された電話番号には絶対に連絡せず、公式サイトで情報を確認しましょう。

ii. ② 個人情報を慎重に管理する

クレジットカード情報やパスワードを安易に入力しない。

不審なリンクや添付ファイルを開かないように注意する。

信頼できるセキュリティソフトを導入し、最新の状態に保つ。

iii. ③ 冷静に対応し、疑わしい場合は相談する

もし詐欺に遭ってしまったら、速やかにクレジットカード会社や公式サポートに相談する。

証拠を保存し、警察や消費者庁へ報告することで、被害の拡大を防ぐ。

強固なパスワードで管理し、二要素認証を活用する。

b. 注意喚起のメッセージ

「サポート詐欺は誰にでも起こり得る脅威です。不安を煽る警告画面や不審な電話には冷静に対応し、決して個人情報を提供しないでください。怪しいと感じたら、公式の情報を確認し、適切な対策を講じましょう！」

「詐欺の被害を防ぐために、日頃からセキュリティ意識を高めることが大切です。こうした情報を共有して、一緒に安全な環境を作っていきましょう！」

(* IPA 資料参照)

- 相談件数は今後も同水準で続くと思われます。
- 被害者をだますための手口も変化し続けると予想されます。
- 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ます。
- 各機関が連携して一般向けの啓発活動を行っていく他、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す。

参考までに！①

「二要素認証」と「二段階認証」の違い？

「二要素認証」と「二段階認証」は似ていますが、異なる概念です。

二要素認証（多要素認証）

認証の際に、異なる **2つの要素**（知識要素・所有要素・生体要素）を組み合わせる方法です。例えばパスワード（知識要素）とスマホのSMS認証（所有要素）を組み合わせることで、より強固なセキュリティを確保します。

二要素認証の要素とは

	具体例
知識要素	パスワード  PINコード 指でなぞるパターン認証  秘密の質問 
所有要素	スマホのSMS認証とアプリ認証  ICカード  トークン  鍵  印鑑  身分証  クレジットカード 
生体要素	顔認証  指紋  虹彩  声紋  静脈  位置情報 

二段階認証

認証を **2回のステップ** に分けて行う方法です。例えば、最初にパスワードを入力し、次に秘密の質問に答える場合、どちらも「知識要素」なので、二要素認証ではなく二段階認証になります。

つまり、**二要素認証は異なる要素を組み合わせることが必須**ですが、**二段階認証は同じ要素を2回使う場合もある**という違いがあります。どちらもセキュリティ強化に役立ちますが、**二要素認証の方がより安全性が高い**とされています。

参考までに！②

レベルアップ勉強会資料

「情報セキュリティ」と「サイバーセキュリティ」の違い？

両者は似ているようで実は微妙に異なる概念です。

参考 URL: [情報セキュリティとサイバーセキュリティの違いを分かりやすく解説](#)