ウ　作品テーマ例

## 作品テーマ例

【ＳＮＳ型投資・ロマンス詐欺】

ＳＮＳ型投資詐欺は、著名人の名前・写真を無断で使用した嘘の投資内容や、「必ず儲かる投資方法を教えます」などのメッセージを送ることで投資を持ちかけます。

ロマンス詐欺は、ＳＮＳやマッチングアプリを通じて知り合った者に恋愛感情や親近感を抱かせ、結婚のための資金調達などと投資を勧めます。

その後、どちらもトークアプリに誘導し、投資に関するメッセージのやりとりを重ねて被害者を信用させ、投資名目で金銭等を騙し取る手口です。

（被害の例）

・ＳＮＳ上で著名人が投資を勧める広告を見つけてアクセスしたところ、著名人を名乗る者のＳＮＳアカウントに誘導され、「必ず儲かるグループ」を勧められグループチャットに加入した。

その後、グループチャット内で勧められた投資の運用サイトに登録し、指定の銀行口座に振り込むと運用利益が上昇。出金を試みるも「保証金」「税金」などの理由をつけて出金させてもらえず詐欺に遭った。

・ＳＮＳで知り合った異性に恋愛感情を抱くようになったところ、相手から「２人の将来のために投資でお金を貯めよう」と勧められた。相手に勧められるがまま投資専用アプリをインストールし、指定された銀行口座にお金を振り込むと相手と連絡がとれなくなった。

（特徴）

・著名人が投資の広告に悪用される

・マッチングアプリで知り合い、直接会ったことのない人から「会いたいから旅費を送ってほしい」「結婚するのにお金が必要」などと金銭を要求される

・ＳＮＳやマッチングアプリで知り合った人から投資の話を持ち掛けられ、投資に関するグループチャットに誘導される

・投資サイトや投資アプリを登録し、入金すると利益が出たように見せかける

・出金しようとすると「出金するには税金がかかる」などの理由で、さらに送金を求められる

（対策）

・実際に会ったことがない人から「投資」の話をされたら詐欺を疑う

・「必ず儲かる」「確実に利益が出る」「あなたにだけ教える」という儲け話は詐欺

・勧められた投資アプリが正規の物かインターネットで確認する

・振込先の口座が個人名義、振込先が振り込みのたびに変わるなど不審な口座へは振り込まない

【フィッシング】

フィッシングとは、実在の企業・団体をかたりメールやＳＭＳを送り、正規のＷｅｂページに酷似した偽サイトへ誘導し、ＩＤやパスワード等のアカウント情報、クレジットカード番号、暗証番号等の重要な情報を入力させて盗み取る犯罪行為です。

（被害の例）

・インターネットバンキングに不正アクセスされて、勝手に送金される

・クレジットカードで身に覚えのない決済をされる

・電子決済サービスにログインされて、電子マネーで買い物をされる

・偽のアプリをインストールしてしまい、スマートフォンから勝手に知らない人にＳＭＳが送られる

（対策）

・「緊急」「至急」等、何らかの行動を急かす文章であっても、メールに記載されたリンクを開かない

・偽物のサイトを開いても、すぐに閉じる

・公式Ｗｅｂサイトを事前にブックマークしたり、企業が提供する公式アプリをインストールしておき、そこから確認する習慣を作っておく

・アカウント情報（ＩＤ、パスワード）やクレジットカード情報等の重要な情報、住所や氏名等の個人情報を入力しない
・ウイルス対策ソフトやブラウザには、偽サイトへのアクセスを遮断する機能があるため、常に最新の状態を保っておく

【サポート詐欺対策】

インターネットを閲覧中に、突然、ウイルス感染したかのような嘘の画面を表示するなどして不安をあおり、画面に記載されたサポート窓口に電話をかけさせ、遠隔操作ソフトをダウンロードやインストールさせたり、サポートの名目で金銭を騙し取ろうとしたりするものです。

（被害の例）
・警告画面に表示された連絡先に電話したら、ウイルスの除去費用を請求された
・サポート料として、次々と料金を請求されるので、コンビニで電子マネーを購入し支払ってしまった
・パソコン内に保存していたネットバンキングのアプリから送金するよう指示をされ、送金画面になったところで送金金額を勝手に操作され高額な金銭を振り込んでしまった

（特徴）
・偽の警告画面に実在する企業のロゴ等が使われている場合がある
・警告音を鳴らしたり、警告メッセージを音声で流したり、偽のセキュリティ警告画面を閉じられないようにして不安を煽る
・偽のサポート窓口に電話をかけると、遠隔操作ソフトをダウンロード・インストールするよう誘導されたり、有料のサポート契約を勧められたりする
・支払いはクレジットカード決済や各種ギフトカード、コンビニ決済や電子マネー等が使われる
・ネットバンキングで送金するよう誘導された際、秘匿事項である旨を告げられ席を外すように告げられる

（対策）
・偽のセキュリティ警告が表示されたら、ブラウザを終了する
・ブラウザを終了できない場合は、強制的に終了する
・（Windows の場合：「Ctrl」＋「Alt」＋「Delete」を同時に押してタスクマネージャを起動し、利用中のブラウザを選択、右クリックして「タスクの終了」を選択する）
・偽のセキュリティ警告画面に表示されている電話番号に電話しない
・電話先の相手の指示に従って、アプリやソフトウェア等をインストールしない
・アプリやソフトウェアをインストールした場合は、ネットワークから切断してウイルスチェックを行い、ダウンロードしたものを削除、インストールしたものをアンインストールし、可能であれば初期化を行い、各種パスワードを変更する
・ネットバンキングを起動するよう指示されたら詐欺を疑う、安易にＩＤやパスワードを教えない

【ＩＤ・パスワードの適切な管理】

ＩＤ：個人を識別するための符号
パスワード：本人であることを示す認証情報

正しいパスワードを入力した人が本人であると認められるのは、「パスワードは本人しか知らない」という原則があるからです。パスワードが漏えいしてしまうと、悪意のあるユーザーがパスワードを盗用し、その本人になりすまして不正アクセスを行います。

（対策）
・名前や誕生日、事典掲載の単語等、他人が推測できるパスワードは設定しない
・アルファベット、数字、記号、大文字・小文字を混ぜ、できるだけ長くする
・パスワードの使いまわしはしない
・パスワードは絶対に人に教えない
・二段階、多要素認証を活用する（指紋等の生体認証やワンタイムパスワード等）
・パスワードは適切に保管・管理する（ＩＤとパスワードは別々にメモする。不特定多数の人が使用する端末

にはブラウザにパスワードを記憶させない等)

【偽情報・誤情報対策】

1　偽情報

意図的に作成・流布される虚偽の情報のことをいいます。

誰かを騙したり、誤解させたり、混乱させたりする目的で、意図的に虚偽の内容が作られ、広められるという特徴があります。

2　誤情報

意図的でなく、誤解や勘違いによって拡散した間違い情報のことを指します。

この場合、必ずしも悪意があるとは限りません。

(過去の例)

・令和６年１月１日に発生した能登半島地震の際、埼玉県内に居住する男性がＳＮＳ上に「倒壊した建物に親族が挟まれて重篤な容態に陥っている」等といった偽情報の書き込みをした。

・平成 28 年４月 16 日に発生した熊本地震の際、神奈川県内に居住する男性がＳＮＳ上に「ライオンが放たれた」という書き込みとともに写真を投稿した。

※上記投稿をした男性らはいずれも偽計業務妨害罪で逮捕されました。

(対策)

・信頼できる情報源（公的機関、報道機関、専門家など）からの情報かを確認する

・複数の情報源を比較する

・古い情報や更新されていない情報は現在の状況と異なる可能性があるため、常に最新の情報を確認する

・偽情報サイトには悪意ある広告やポップアップを利用してサポート詐欺に誘導するものもあるため、セキュリティ対策サービスを活用する