別添２

作品テーマ例

１　インターネット上の誹謗中傷防止

⑴　インターネット上の誹謗中傷とは

インターネット上に個人の名前や写真を勝手に掲載され、誹謗中傷する書き込みをされてしまうもの。

⑵　被害の例

ア　友達から教えられ、SNSに自分の個人情報が掲載されていることが分かった。

心配になり、他のサイトも確認したところ、掲示板サイトに、誹謗中傷する書き込みとともに自分の名前や写真が掲載されていることが分かった。

イ　知らない人からメールが来るようになり、送信されたメールに「掲示板サイト○○を見て連絡した」と書かれていたので、その掲示板を見てみると、そこには卑猥な文章とともに自分の名前やメールアドレス等が掲載されていた。

⑶　被害に遭わないために

ア　ホームページや掲示板、SNS等で安易に自分や家族等の個人情報を掲載しない。

１つのサイトでは特定されなくても、複数のサイトの情報を集めて特定される可能性があります。

イ　インターネット上で知り合った人に、安易に名前や連絡先を教えたり、顔が分かる画像を送らない。

ウ　自分の個人情報をある程度公開しなければならないときは、電話番号や詳細な住所等が本当に必要なのか、十分に考える。

エ　他人の個人情報を本人の許諾なく掲載することは、厳に慎む。

⑷　被害に遭った場合は

ア　掲載された内容の記録

自分自身を誹謗中傷する内容がインターネット上に掲載されていることを把握した場合には、プロバイダや掲示板サイト管理者等への削除依頼や関係機関への相談、警察への通報・相談の際に必要となりますので、掲載されたサイトやSNSのページを印字やスクリーンショット、当該サイトの名称、URL、書き込み者、書き込み日時、内容等を記録してください。

イ　警察への通報・相談

相手方の処罰を望む場合は、最寄りの警察署に相談してください。

ウ　関係機関への相談

インターネット上の誹謗中傷に対しては、官民の相談機関等が対応しています。下記の関係機関等への相談も検討してください。

（ｱ）　違法・有害情報相談センター（総務省委託事業）

インターネット上の書き込みにより、名誉毀損やプライバシー侵害等の被害にあわれた場合、インターネットに関する専門知識を有する相談員が、相談者自身で行う削除対応方法等をアドバイスします。

https://www.ihaho.jp

(ｲ)　人権相談（法務省）

インターネット上の投稿による人権侵害など、人権に関する相談を受け付ける窓口です。

相談者自身が行う削除依頼の方法について助言を行うほか、法務局が事案に応じてプロバイダ等に対する削除依頼を行います。

https://www.moj.go.jp/JINKEN/index_soudan.html

(ｳ)　誹謗中傷ホットライン（一般社団法人セーファーインターネット協会）

インターネット上の誹謗中傷について連絡を受け付け、国内外のプロバイダ等に利用規約に沿った削除等の対応を促す通知を行います。（相談対応は行っていません。）

https://www.saferinternet.or.jp/bullying

2　犯罪実行者募集活動（闇バイト）防止

⑴　犯罪実行者募集活動とは

いわゆる「闇バイト」など犯罪実行者を募集するものです。

SNSやインターネット上の掲示板等で、仕事の内容を明らかにせず著しく高額な報酬の支払いを示唆するなどして犯罪の実行者を募集する投稿が掲載されています。

簡単に高収入を得られるなら、と応募してしまうと、強盗や詐欺といった犯罪に加担することとなり、逮捕されてしまいます。

一度加担してしまうと「やめたい」と思っても応募したときに登録した自分自身、家族等の個人情報を基に「家に行く」「周囲の人に危害を加える」と脅され、逮捕されるまで抜け出せません。

犯罪グループは雇った人間を都合よく利用した後、「捨て駒」として切り捨て、待ち受けているのは、重い刑罰です。

⑵　犯罪実行者募集活動（闇バイト）例

ア　SNSに投稿された闇バイトの募集に応募したところ、お年寄りが居住する家に行き、キャッシュカードを受け取り、ATMでお金を引き出すよう指示され、指示に従い受け取ったキャッシュカードでお金を引き出していたところ、駆けつけた警察官に逮捕された。

イ　闇バイトに申し込んだところ、自分名義の口座を作り、キャッシュカードを指示された住所に送付した。

すると、報酬は支払われたが、その後警察官が自宅に来て逮捕された。

ウ　闇バイトに申し込んだところ、一定時間経過するとメッセージのやり取りが自動的に消えるアプリで身分確認として運転免許証の写真を送るよう指示された。

その後、仕事の内容が強盗であると知らされ、断ろうとしたが「家に行く」「家族に危害を加える」などと言われ、仕方なく強盗に加担してしまった。

エ　そのほかにも、令和５年７月に警察庁生活安全局人身安全・少年課から「犯罪実行者募集の実態～少年を「使い捨て」にする「闇バイト」の現実～」という資料が公表されていますので、参考としてください。

「犯罪実行者募集の実態～少年を「使い捨て」にする「闇バイト」の現実～」

https://www.npa.go.jp/bureau/safetylife/yamibaito/yamibaitojirei.pdf

⑶　犯罪実行者募集活動（闇バイト）の特徴

犯罪実行者募集活動（闇バイト）は、「高額バイト」「即日入金」「書類を受け取るだけ」等と、一見好条件に見える求人情報を装っています。

また、募集情報に「受け子」「出し子」「闇バイト」等の隠語が使用されていたり、匿名性の高いアプリケーションでの連絡が求められたりします。

⑷　被害に遭わないために

世の中にはそんな上手い話はありません。

甘い言葉に騙されることなく、怪しいかもしれない、と迷ったら、一人で判断せずに家族等周囲の人や警察に相談しましょう。

3　フィッシング被害防止

⑴　フィッシングとは

フィッシングとは、実在する企業や団体等の組織をかたり、偽のメールやSMSで偽サイトに誘導し、アカウントID、暗証番号、クレジットカード番号、インターネットバンキングの口座番号、暗証番号等の個人情報を入力させ、情報を盗んだり、マルウェアに感染させたりする手口です。

情報を盗まれると、アカウントを乗っ取られてお金を不正に送金されて盗まれたり、インターネット通信販売サイトで勝手に買い物をされたりします。

また、マルウェア感染してしまうと、パソコンやスマートフォンに保存されている連絡先の情報が盗まれたり、自分の端末がフィッシングメールやSMSの発信源となってしまうこともあります。

⑵　被害の例

ア　ネット口座を開設している銀行から「重要なお知らせ」という件名のメールが届いたので、記載されたURLにアクセスし、口座番号、暗証番号等を入力した。

その後、知らない口座に対して、身に覚えのない多額の送金をされていることが分かった。

イ　クレジットカード会社から「クレジットカード情報の確認」という件名のSMSが届いたので、記載されたURLにアクセスし、カード情報を入力したところ、後日、クレジットカードの支払い明細に身に覚えのない支払いがあった。

ウ　大手通販サイトから「アカウントで不正なログインが確認されたため、アカウントをロックしました。解除するには下記のURLから手続きしてください。」というSMSが届き、慌ててURLに接続し、当該大手通販サイトのIDとパスワードを入力したところ、アカウントに不正アクセスされ、高額商品を大量に購入された。

⑶　被害防止対策

ア　電子メールやSMSに記載されているリンクはクリックしない

電子メールに記載されたリンクは偽装可能なほか、正規サイトに類似したドメイン名を伏したフィッシングサイトも多く存在することから、見た目で真偽を判断することは非常に困難です。

電子メールやSMS内のリンクは安易にクリックせず、あらかじめ「お気に入り」や「ブックマーク」に登録した公式サイト、公式アプリを活用して、正しいサイトに接続するようにしてください。

イ　パソコンやスマートフォンを安全に保つ

OSやアプリ、ソフトウェアの脆弱性や不具合を悪用し、広告などからフィッシ

ングサイトに誘導される場合があるので、OSやアプリ、ソフトウェアのアップデートを行い、パソコンやスマートフォンを安全な状態に保って下さい。

ウ　携帯電話会社などが提供するセキュリティ設定を活用する

携帯電話会社などが提供する迷惑メッセージブロック機能などを活用し、フィッシングメールや不審なSMSが届きづらい設定にする。

エ　IDやパスワードの使いまわしはしない

複数のサイトで同じIDやパスワードを使いまわしていると、一つでもID、パスワードが流出した場合、全てのサービスにおいてアカウントが乗っ取られてしまいます。

IDやパスワードはサイトやサービス毎違うものを設定しましょう。

4　偽サイト・詐欺サイト被害防止

⑴　偽サイト・詐欺サイトとは、インターネットショッピング等に掛かる詐欺を目的としたウェブサイトを構築し、商品の注文、代金の振込を受けた上で、商品を発送しない又は偽物の商品を発送するなどの手口をいいます。

⑵　偽サイト・詐欺サイトの特徴

ア　品薄等の表示で商品の購入を急がせる

「品薄」「本日限り」等と表示することで消費者心理につけ込み、商品購入を急がせます。

イ　割引が過大である

通常では考えにくい販売価格の大幅な値引きを強調し、消費者心理につけ込み、商品購入をあおります。

ウ　代金支払い方法が限定的である

銀行口座等への前払いのみ、クレジットカードのみ、代金引換のみなど、代金支払い方法が限定されていることがあります。

クレジットカードの場合、カードを不正利用される場合もあります。

エ　会社概要に実在しない住所が記載されている

ウェブサイトに記載されている販売業者の住所が、虚偽であったり、無関係の住所の場合があります。

⑶　被害に遭わないために

ショッピングサイト等を利用する際は、購入手続前に次に掲げる点を確認し、手続き中に支払い方法等が明示された方法と異なり銀行振込のみになるなど不審点を感じたら、すぐさま手続きを停止してください。

ア　URLの「https://～」やドメイン（.jp.com等）が見慣れない（.shop.xyz等）もので違和感はないか

イ　商品が極端に安くないか、割引率が極端に大きくないか

ウ　「本日限り」等と記載されるなど、購入を急がせていないか

エ　会社概要の内容についてインターネット検索を行い、企業名の盗用や虚偽の内容等が記載されていないか

オ　日本語が不自然でないか

カ　SAGICHECKの活用

一般財団法人日本サイバー犯罪対策センター（JC3）では、収集した偽ショッピ

ングサイト情報を、インターネット利用者がウェブサイトの信ぴょう性を確認出来るサービス「SAGICHECK」(https://sagicheck.jp) へ提供しています。

この「SAGICHECK」を利用することで、ウェブサイトの危険性の有無について確認することができます。

詳しくはJC3ウェブサイトをご覧下さい。

JC3ウェブサイト (https://www.jc3.or.jp/news/2023/20230301-488.html)

5　その他サイバー事案、セキュリティに関するもの

上記１から４に示した題材のほか、下記サイバー事案、セキュリティに関するもの。

⑴　SNS型投資詐欺・ロマンス詐欺

ア　SNS型投資詐欺とは

SNS型投資詐欺とは、SNS等で直接対面することなく、連絡を取り合い信頼関係を深めて信用させ、嘘の投資話等の儲け話を持ちかけて金銭を騙し取る詐欺。

イ　SNS型ロマンス詐欺とは

SNS型ロマンス詐欺とは、SNS等で直接対面することなく、連絡を取り合い信頼関係を深めて信用させ、恋人や結婚相手になったかのように振る舞い、恋愛感情や親近感を抱かせて金銭等を騙し取る詐欺。

※　警察庁が公表している「SNSを悪用した投資・ロマンス詐欺の被害発生状況等について」等を参考としてください。

https://www.soumu.go.jp/main_content/000942561.pdf/

⑵　サポート詐欺対策

ア　サポート詐欺とは

サポート詐欺とは、パソコンでインターネットを閲覧中に、突然、ウィルスに感染したかのような嘘の画面を表示させたり、警告音を発生させるなどして、ユーザーの不安をあおり、画面に記載されたサポート窓口に電話をかけさせ、サポートの名目で金銭をだまし取ったり、遠隔操作ソフトをインストールさせたりするものです。

イ　対策

(ｱ)　相手に絶対電話をしない

偽の警告画面には、サポート窓口の電話番号が書かれていますが、ここには絶対に電話をしないでください。

(ｲ)　偽の画面を閉じる

偽の警告画面は閉じるボタンが無く、消せない場合があります。

そのような場合は以下の方法を試してください。

・「Esc」キーを長押しして、ブラウザの「×」をクリックする。

・「Ctrl」＋「Alt」＋「Delete」を同時に押し、タスクマネージャを起動させ、利用しているブラウザを選択して右クリックし、「タスクの終了」を選択する。

※　警察庁、長野県警察公式ホームページ等に掲載されている資料等を参考としてください。

警察庁　https://www.npa.go.jp/bureau/cyber/countermeasures/support-fraud.html

長野県警察　https://www.pref.nagano.lg.jp/police/anshin/cyber/supportsagitaisaku.html

⑶　IDやパスワードの適切な保管管理

他人に自分のユーザアカウントを不正利用されないようにするには、適切なパスワードの設定と管理が大切です。

適切なパスワードの設定・管理には、以下の３つの要素があります。

ア　安全なパスワードの設定

安全なパスワードとは、他人に推測されにくく、ルールなどで割り出しにくいものを言います。

無関係な（文章にならない）複数の英単語をつなげたり、その間に数字列を挟んだりしたものであれば、推測されにくく、覚えやすいパスワードになります。

イ　パスワードの管理方法

パスワードを設定しても、他人に漏れてしまえば意味がありません。

パスワードは「他人に教えない」「電子メールでやり取りしない」「他人の目に触れる場所にメモしない」等と言った対策が必要です。

ウ　パスワードを複数のサービスで使い回さない

パスワードはできる限り、複数のサービスで使い回さないようにしましょう。

パスワードを使い回していると、あるサービスから流出したアカウント情報を使って、他のサービスのアカウントへ不正アクセスされてしまいます。

詳しくは、総務省ホームページ「安心してインターネットを使うために」の「インターネットの安全な歩き方」のページにある「IDとパスワード」を参考にしてください。

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_privacy_01-2.html/

⑷　インターネットの適正利用

インターネットを利用するためには正しい知識を身につけ、ネット上のルールとマナーを守る必要があります。

詳しくは、総務省ホームページ「上手にネットと付き合おう！安心・安全なインターネット利用ガイド」を参考としてください。

https://www.soumu.go.jp/use_the_internet_wisely/