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

(1)　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。

(2)　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。

(3)　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つのサイトの情報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。

(4)　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

(1)　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。

(2)　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

(3)　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。

(4)　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

(1)　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、マルウェアに感染してしまうと、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。

(2)　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。

(3)　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うおそれがあります。

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。