特別企画・特集

特別企画

身近な脅威

特別企画では、あなたにも降りかかり得る「身近な脅威」について様々なケースを取り上げる。

「先週、SNSを通じて知り合った人から誘われたセミナーに参加したけど、あれはもしかして･･･」、「今まで何気なく使っていたいつものカフェの無料Wi-Fiはもしかして･･･」、「最近知り合ってすぐ仲良くなったあの人はもしかして･･･」

「身近な脅威」を知ることが、トラブルに巻き込まれないための第一歩となる。

1　注意すべき団体が「あの手、この手」で勧誘活動を実施 ～団体名や本来の目的を巧妙に秘匿した誘いに注意～

過激派やオウム真理教、特異な主張を掲げる集団などは、団体名や本来の主義主張を巧妙に秘匿するなどして、街中などで接触を図り、個人情報の入手、人間関係の構築、入会への説得といった流れで勧誘を進めている。

近年は、SNSサービス等の普及に伴い、インターネット上における接触を勧誘の入口にするなど、その手法は多様化・巧妙化している。無用のトラブルを避けるため、これら団体の勧誘手法等や実際にトラブルに遭ってしまった際の相談先などについて理解しておくことが重要である。

街中やキャンパスで･･･

- 同好会やサークル活動への参加呼びかけ
- 署名やアンケートへの協力依頼
- 社会的課題･自己啓発関係イベントの紹介

など様々な名目で接触して、個人情報の入手を試み、その後、人間関係の構築を図りつつ、徐々に独自の主義･主張を植え付けていくことで、関係を断ち切りにくい状況において入会を迫る事例を確認。

〈イメージ(当庁作成)〉

◀「ボランティア、社会貢献」サークルを装う例も

◀「SDGs、就活･起業、ダイバーシティ」など若者の関心の高いテーマを掲げたセミナーを装い、「自己実現に資する」と誘う例も

SNSなどでは･･･

- オンラインセミナーを装うなど団体名を秘匿したアカウントを使用
- 若者の興味を引く演出･表現を使用した動画･画像等の発信

などを行い、「いいね」など好反応を示した者に個別に連絡を試みる事例を確認。

また、最近では、いわゆる「マッチングアプリ」を利用した勧誘事例も確認されており、これら団体が用いるツールも多様化。

〈YouTube 中核派の「前進チャンネル」(youtube.com/@user-gf3lg5bo4q)〉

◀中核派は、過激な表現等で「若者受け」を企図

「過激派」による若い世代の取り込みについて知りたい方は、P.73へ

「オウム真理教」が起こした重大事件や勧誘手法について知りたい方は、P.15 特集1「オウム真理教とは」、P.70 COLUMN①「ターゲットは若者!」

事　例

※以下の事例は、実際の事例を基に当庁作成

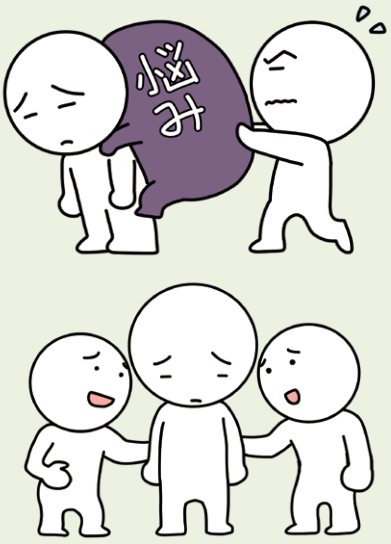
1

20歳代女性は、異文化に関心があり、SNSを通じて知り合った女性から、オンラインセミナーへの参加を促された。参加当初は、日常会話や文化を紹介する内容であったが、**4～5回目以降からは、宗教の話や、「世の中を支配するのは悪魔」などと不安をあおる言辞を繰り返し語られた。**女性は、違和感を覚えたが、講師から毎回参加するよう強く求められ、断れず継続的に参加せざるをえなかった。

〈イメージ（当庁作成）〉

2

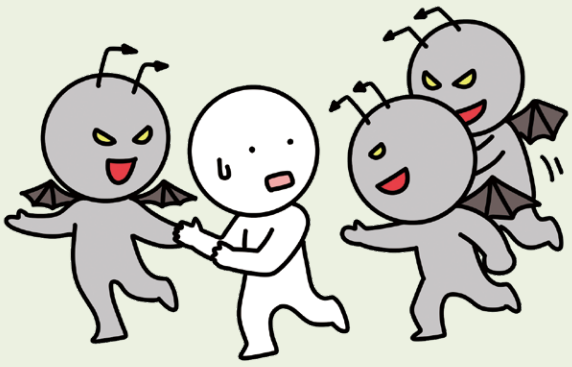
30歳代男性は、「戦争」に関する写真展を訪れた際、女性スタッフから連絡先の交換を求められた。後日、女性から「会って話がしたい」と連絡があり、面談して、仕事上の悩みや社会に対する不満などについて会話した。男性は、**「悩みを聞いてくれる」と女性を信用していた**ところ、数回の面談後に、「世の中を変えるために、集会であなたの悩みや不満を発言してほしい」などと、**過激派が主催する集会への参加と発言を求められた。**



「悩み相談」、「寄り添い」で人間関係構築を企図

3

20歳代女性は、同じ占い好きの女性AとSNSで仲良くなり、数回会った後に、Aの勧めで占いサークルに入会した。サークルは、実は宗教系団体であり、数か月後には教義の学習と**新たな信者の勧誘を求められた。**女性は、勧誘への加担に嫌気がさし、Aに脱会する意思を伝えたところ、Aのほか信者数人から「やめたら災いがふりかかる」、「個人情報をネットに晒す」などと**集団による脅しまがいの説得を長時間にわたり受けた。**


集団で囲み脱会することが困難な状況に追い込む例も

トラブルに巻き込まれないために‥

❶ 連絡先(SNSアカウント、メールアドレス、電話番号等)の提供・交換を求められたとしても、安易に応じない

❷ 自身が主体的に参加する場合でも、誘われた場所や状況、参加するサークルやイベント名、主催者等に関する情報は、冷静に検索する

❸ 少しでも違和感を覚えたら、早期に家族や友人など身近な人物や、弁護士等に相談する

❹ 意に反する要求に対しては、明確に拒否、又は無視する

ことなどがトラブル防止に有効である。

SNSでのささいな発信も勧誘の材料に‥

トラブルに実際に遭ってしまったら‥

日本司法支援センター（法テラス）では、一連の「旧統一教会」問題を契機に、霊感商法等によりトラブルに遭った際の相談窓口として、「霊感商法等対応ダイヤル」を設置している。

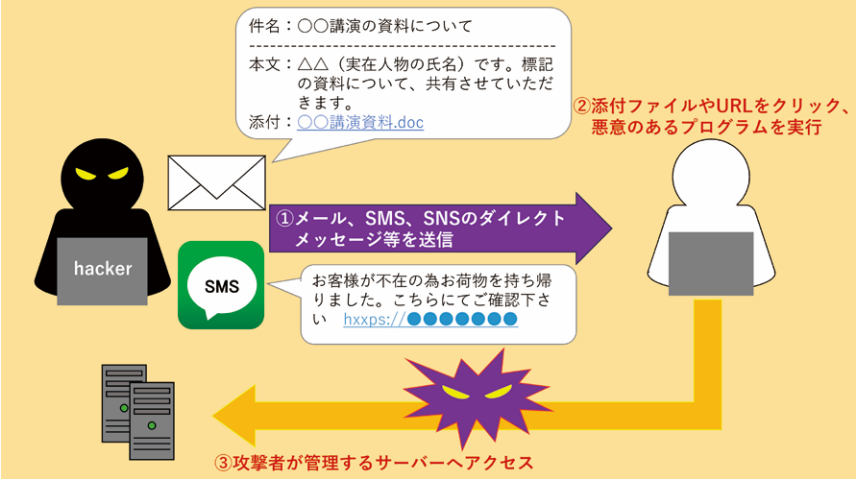
同窓口は、「旧統一教会」問題や霊感商法に関する金銭トラブル、心の悩み、家族の悩み、児童虐待、修学など、様々な相談を受け付け、内容に応じて適切な機関へつなげる取組を行っている。

法テラス 霊感商法等対応ダイヤル
0120-005931
（受付時間）9：30～17：00（平日）

2　身近に迫るサイバー攻撃の脅威

人間の心の隙を突いたサイバー攻撃

サイバー空間における悪意ある攻撃者は、フィッシング攻撃等において、ターゲットの心理・行動の隙を突き、不正アクセス等を図ろうとしている。

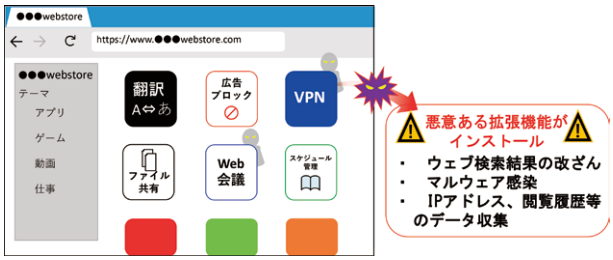


フィッシング攻撃のイメージ

無料サービスを悪用するサイバー攻撃

ウェブブラウザの機能を追加するための拡張機能の多くは、インターネット上で無料で入手できる反面、ブラウザを経由する全通信データへのアクセス権を有するものもあり、様々なサイバー脅威主体に悪用され得る。北朝鮮のサイバー脅威主体も、マルウェアを感染させてパスワード等を窃取する目的で、拡張機能を使用しているとされる。

また、無料コンテンツの広告を装ってサイト利用者にクリックさせ、悪意のある拡張機能をインストールさせる手法も報告されている。利用者においては、意図せずして、こうした悪意のあるサービスを利用している可能性があるため、無料サービスには特に注意が必要である。



ウェブストアに潜む脅威

インターネット上の広告に潜む脅威

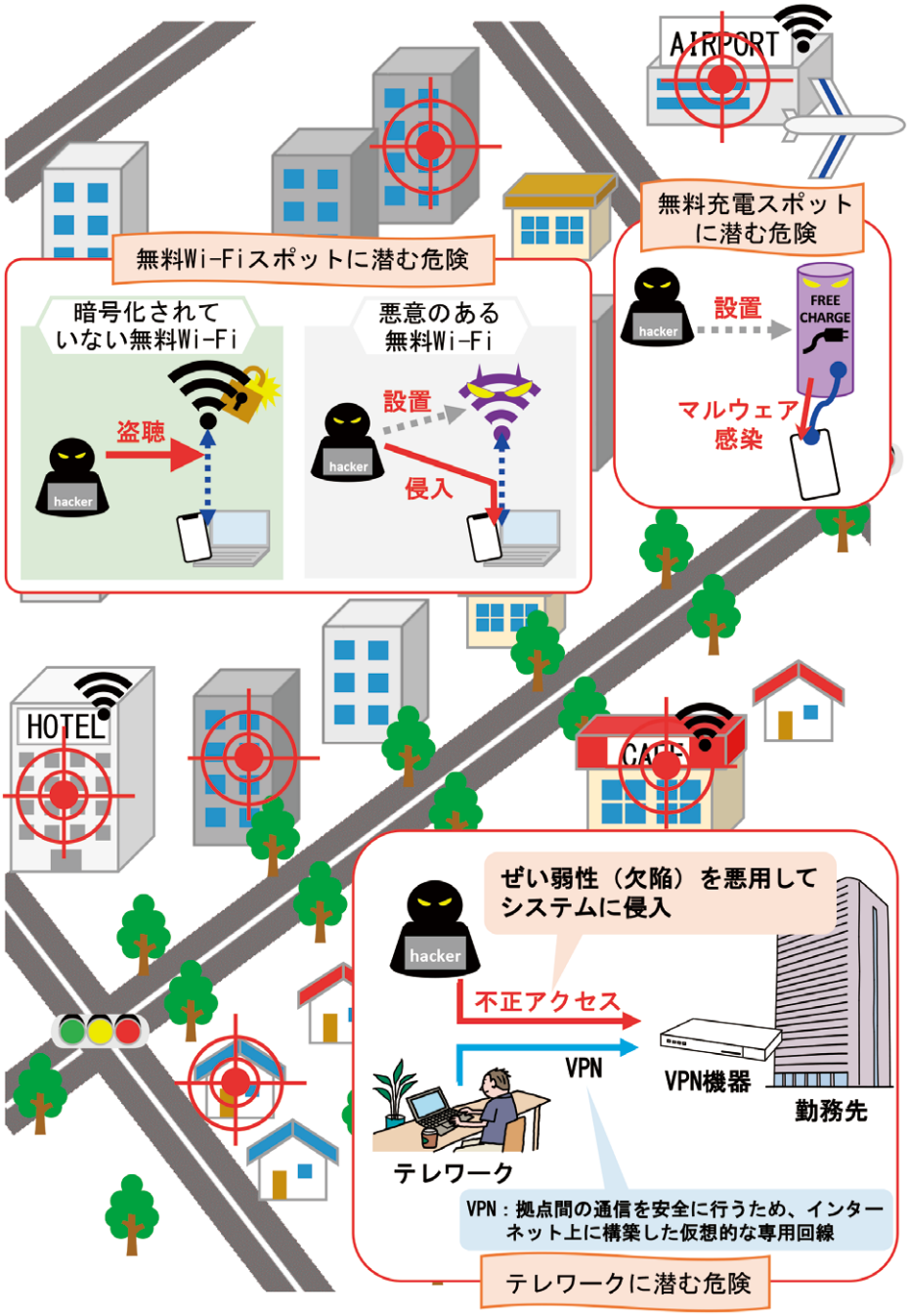
街中に潜む脅威

無料サービスを悪用したサイバー攻撃だけでなく、街中にあふれる無料のWi-Fiスポットにも注意が必要である。令和元年（2019年）12月、米国連邦捜査局（FBI）は、認証情報の窃取やマルウェア感染を引き起こす可能性があるとして、旅行中に空港やホテル等の無料Wi-Fiスポットに自動接続しないよう注意喚起を行った。また、令和5年（2023年）4月には、米国連邦通信委員会（FCC）が、公共の場所に設置されている、携帯電話やタブ

レット端末用の無料充電スポットには、マルウェア感染等を企図した悪意あるものも紛れているとして、注意を促した。

テレワーク等に潜む脅威

コロナ禍以降、テレワークの普及といった働き方の変化も相まって、インターネット通信の安全性を確保するため、VPN機器等のセキュリティ機器を利用する機会が増えている。一方で、認証情報等の窃取が可能となるVPN機器のぜい弱性を狙ったサイバー攻撃が複数確認されており、米国等の政府当局は、令和4年（2022年）に日常的に悪用されたぜい弱性の一つとして、VPN機器のぜい弱性を挙げ、適時適切に修正プログラムが適用されていなかったことが原因であると指摘した（8月）。



街中に潜む脅威

サイバー攻撃のリスク軽減のための自己対策

様々なサイバー脅威主体が活動し、その手口も巧妙化していることから、我々の身近に潜むサイバー攻撃の脅威リスクを軽減するためには、個人の情報セキュリティリテラシーの向上も必要である。これについて、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）は、各個人ができるサイバーセキュリティ対策として、次の4点を示している。

① 多要素認証（所持情報、生体情報、知識情報等の組合せで本人認証を行う方法）

- 所持情報：電話やSMS、アプリ等によるワンタイムパスワード認証
- 生体情報：静脈認証、指紋認証など
- 知識情報：パスワードなど

② 複雑かつ使い回しではないパスワードの設定

③ PC、携帯電話、タブレットのOS及びアプリの最新版への更新

④ クリックする前に一呼吸
（成功するサイバー攻撃の90%以上は、フィッシングメールから始まる）

米国サイバーセキュリティ・インフラセキュリティ庁（CISA）発表
「サイバーセキュリティのためにできる4つのこと」（令和4年〈2022年〉）に基づき当庁作成

3　SNS等で拡散する偽情報の脅威

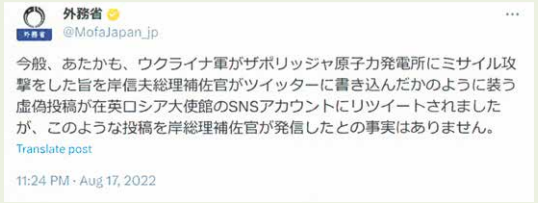
ソーシャルメディアの一種であるSNSは、誰もが情報を容易に発信することができ、短期間に広く拡散させることができる。そのため、勘違いや誤解で拡散された「誤情報」や、受信者を欺くことを意図した「偽情報」の拡散が社会問題となっている。また、「偽情報」に関しては、近年、我が国の外交関係を捉えて世論を混乱させることを目的に発信されているとみられる投稿が散見されており、注意が必要である。

「園田康博内閣府政務官（当時）が、平成23年（2011年）10月、東京電力福島第一原子力発電所の低濃度汚染水を浄化した水を飲んで安全性をアピールしたが、後年、消息不明となった。同人は、多発性骨髄腫を患い療養のためにパラオ共和国に滞在していたところ、令和2年（2020年）8月に死亡。その旨をパラオ保健局が発表した」などという動画の偽情報が中国のSNSを中心に多数拡散。園田元政務官は、9月、我が国メディアの取材に応じ、同偽情報の内容を改めて否定

記者会見に臨む園田内閣府政務官（当時、写真提供：時事）

ウクライナ偽情報対策センターウェブサイト（https://cpd.gov.ua/result/kampaniya-z-dyskredytacziyi-ukrayinsko-yaponskyh-vidnosyn/）

「話題を変えよう！美味しい寿司について話そう！」との文言と共に寿司職人がウクライナ人とみられる女性の口を塞ぐイラストが掲載された、我が国企業の広告であるかのように偽装した画像が、ロシアメディアなどにより紹介され、SNSにおいても拡散。ウクライナ偽情報対策センターは、令和4年（2022年）8月、同画像を日・ウクライナ関係を毀損する「偽情報」と指摘



外務省公式X（旧Twitter）（https://twitter.com/MofaJapan_jp）

岸信夫総理大臣補佐官（当時）が、ウクライナ軍によるザポリッジャ原子力発電所に対するミサイル攻撃を批判した旨をSNSに投稿したかのように装う虚偽投稿画像がTwitter（現X）上に投稿され、在英ロシア大使館などのアカウントが当該投稿を引用するなどして拡散（令和4年〈2022年〉）

なお、岸補佐官（当時）は投稿を否定しており、我が国外務省は、在英ロシア大使館に申入れを行った旨Twitter（現X）に投稿（同大使館は、その後、上記の当該投稿を削除）

以上のような疑わしい情報を見聞きした際には、うのみにせず、オリジナルの情報（一次情報）の確認はもちろんのこと、他の情報（特に新聞や雑誌などのネット以外の情報）と比較してみることが必要である。

4　隣の客は外国情報機関員！？

絶世の美男美女が、世界を救う極秘情報を、時にスマートに、時に派手な銃撃戦によって入手する。“スパイ”と聞くとそのような姿を思い浮かべるかもしれないが、実際の外国情報機関員は目立つことを嫌う。“ホンモノ”は、日々、一般人として立ち振る舞い、その正体や活動が他人に知られないように細心の注意を払って活動している。

外交官や民間人に成りすました外国情報機関員は、我が国にもいると言われている。古くは「20世紀最大のスパイ」と呼ばれる旧ソ連の情報機関員、リヒャルト・ゾルゲ、近年では、外交官として来日し、都内の繁華街（路上）で声を掛けたことをきっかけとして我が国大手通信企業社員に近づき、営業秘密を入手していたロシアの情報機関員など、幾つものケースが確認されている。

外国情報機関員は、特殊な訓練を受けており、例えば、「エリシテーション」（elicitation）と呼ばれる会話術を使い、標的に警戒されることなく情報を引き出している。米国連邦捜査局（FBI）は、「エリシテーション」を“（相手に気付かせないように）慎重に情報を収集する手法”として、“多くの情報機関員が訓練を受けている”と警告している。「これぐらいなら話しても大丈夫」と思った話が相手にとっては貴重な情報になることもあり得る。

外国情報機関員による情報収集パターン例

左：リヒャルト・ゾルゲ（写真提供：共同通信社）、右：出国するロシアの情報機関員とみられる男（写真提供：時事）

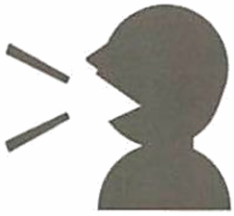
偶然の出会いから始まり、趣味や興味が重なって意気投合をしたその人は、実はあなたがアクセスできる大切な情報を狙っている外国情報機関員かもしれない。

偽りの知見
例）専門家から聞いた話ですが・・・

秘密の餌
例）ここだけの話なんですが・・・

擦り寄り
例）キーパーソンのあなたに教えてもらいたいのですが・・・

誘導尋問
例）今の御担当は経理ですよね？



情報収集されていることに気付かず、ついつい、喋りすぎてしまい・・・・

エリシテーションのテクニックの一例

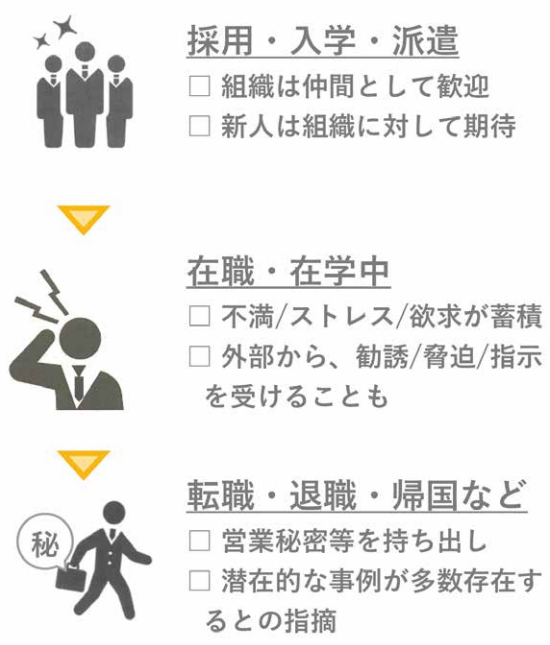
5　仲間を“脅威”にしないためにも

商品の原価データをコピーして転職先への手土産にする。上司への腹いせに重要情報を削除する。私的な利益のために研究成果を持ち出す。これらは、我が国の企業や研究機関、公的機関で実際に発生した「内部脅威」事案である。

「内部脅威」とは、欧米で「インサイダースレット」（Insider Threat）と呼ばれるリスクであり、組織の社員・職員らが、その権限や知見を悪用して当該組織に損害を与えることを指す。

米国で行われた調査結果によると、多くの「内部脅威」事案で、同僚や家族などの身近な人々が、不正行為の兆候に事前に気付けていたということである。しかし、個々人がその兆候に気付いたとしても、それを組織内で共有しなければリスクが潜在化してしまい、気付いたときにはもう遅い、ということにもなり得る。

「内部脅威」は、社員・職員が持つ本来の性格に、ストレスや職場環境など様々な要因が組み合わさって醸成され、何らかのきっかけにより顕在化し、最悪の場合、組織に甚大な被害をもたらす。企業や大学等は、何が「内部脅威」となり、それにどう対処するかのルールを事前に策定しておいたり、同僚の言動から兆候を察知した場合の連絡窓口を周知したりしておくことが重要である。



「内部脅威」が生まれるまで

「内部脅威」の兆候と考えられる言動と、それを把握し得る者の一例