情報社会の現状と情報モラル

㈱ラック サイバー・グリッド・ジャパン
七條 麻衣子 氏

■ はじめに

今日の講演会の内容は、まずデータを踏まえた情報社会の現状、そしてインターネットにおける人権侵害のうち、セキュリティインシデント、セキュリティの事故における人権侵害、情報発信、ソーシャルメディア等の中で起きる問題、そして最後に、組織としてこの人権侵害を防ぐためにどうしていけばいいか、この流れでまとめていく。

■ 主な情報通信機器の保有状況の推移

総務省が発表している令和 5 年版情報通信白書の「通信利用動向調査」のグラフは、日本の世帯においてどれくらいインターネットがつながるか、情報通信機器が普及しているかを示している。平成 22 年に初めて登場したスマートフォンの保有率は、令和 5 年末には 90%になった。推移の表の一番上にある「モバイル端末全体」のグラフを見ると、携帯電話・スマートフォンを含めた普及状況は 97.4%で、その内 90%がスマートフォンである。パソコンは 70%を切っている。私は大学で 20 年近く講師をしているが、昔は大学に入ると、ノートパソコンを買ってもらう学生が非常に多かった。それがここ数年は、レポートの作成もスマホでこなし、パソコンを持つ学生が減ってきた。ただコロナ禍においては、オンライン教育が徹底されたため、Zoom で講義を聞きながら資料を閲覧する必要があり、2021 年には、またパソコンの利用率が一時増えたが、今はまたこのグラフと同じように少しずつ減ってきている。また、固定電話の所持率もかなり急激に下がっている。私の自宅でも固定電話はなく、家族全員がスマホである。そして、スマートウォッチなど身に着ける通信端末、いわゆるウェアラブル端末が 1 割程度になってきた。このように、今、さまざまな通信端末・通信機器が普及している。

■ 年齢階層別インターネット端末の利用状況

一方で、6 歳から 80 歳以上までを対象とした年齢階層別インターネット端末の利用状況の調査結果をみると、2 年ほど前から、80 代でもパソコンよりスマートフォンを使う割合が多くなってきた。ただ、使いたい用途によって使用するインターネット端末が違っている側面もある。

■ 若年層のネット活用

５ページ目のグラフは、こども家庭庁が、2 歳から 17 歳までの若年層を対象に、機器の専用率（スマートフォン）を調査したものである。

小学校の中学年から高学年に入ると、防犯のため、また塾の送り迎えに必要ということで、以前から子供に携帯端末を持たせる保護者は多かったが、特に最近は、10 歳時点で、65%の子供が専用のスマホを使っている。保護者にどうして子供専用のスマホを持たせるのかと聞くと、「家族みんなでスマホにした方が料金が安くなる」という理由が挙がっている。たしかに携帯会社のキャンペーンを見ていると、「5 歳以上の方のスマホデビューで家族みんながお得になる」というプランも出てきている。

若年層のスマートフォン以外に、ゲーム機やテレビも含め、若年層がどのようなサービスをインターネット上で使っているか。項目にある「動画を見る」は、数年前からほぼどの世代でも 100%である。また、「勉強をする」も小学校 1 年生ぐらいから結構な割合を占め、「撮影や記録をする」「写真を撮る」「動画を撮影する」も割合が高く、かなり小さい頃からインターネットを使い始めていることがわかる。

子供たちにとってインターネットは今や特別な世界ではない。インターネットは日常生活に必須の道具となっている。去年、大分市内の中学生に「友達や家族と連絡を取るときには何を使うか」というアンケートを採ったところ、3 年生は、友達や家族ともに LINE を使ってやり取りをしていると答えたが、1 年生は、家族は LINE だが、友達には LINE を教えず、Instagram の DM を使うという回答だった。若年層において、LINE は非常に近しい人たちとのやり取りに使うツールとなっている。Instagram は画像や動画の投稿用ではなく、むしろメッセージアプリとして使われ始めている。

小中学生の特に男子は、テレビ画面でオンラインゲームをしながら、チャットをするのが当たり前になってきている。Discord アプリで画面共有や音声チャットをしている。Discord は、特にゲームをする世代にとって重要なツールになってきている。

今の若年層において「共有」は非常に重要なキーワードである。2 年前にサービスが終了した Zenly というフランス生まれの位置情報共有アプリも非常に人気があった。昨年度、私の地元の県が調査した結果では、高校生の 35%が友達と位置情報を共有するアプリを使っていると答えている。アプリを使って、今、誰といるか、自分が何をやっているかを共有するのである。例えば、自分の部屋でテスト勉強をしていたら、その状態で友達とビデオ通話で 3 時間も 4 時間もつなぎっぱなしにするのが数年前から当たり前の文化になっている。仲が良くても趣味が違う相手もいる。普段仲が良い友達に対してはリア友専用アカウント

（リア垢）を作る。「垢」はアカウントという意味である。リア垢には、クラスや自分の出身校などを明記する。テスト期間は勉強垢を使用し、趣味でつながりたいときは二次垢やサブ垢を作って、用途に合わせてコミュニケーションする相手を切り替えている。

小さな子供たちでも動画を撮影・加工して誰かに送ることが簡単にできるようになった。YouTube の影響も非常に大きいが、今は「ライバー」（配信をしながら収入を得ている人たち）と呼ばれる方々も子供たちにとって憧れの職業である。生命保険会社等の将来なりたいものランキングでも、配信をしながら収入を得る職業が子供たちの憧れとなっている。

■ 高齢者のネット活用

一方で、60 代・70 代の方がどのような端末を使ってネットを活用しているか。NTT ドコモが毎年発行している「モバイル社会白書」によると、パソコンよりもスマートフォンが多くなっている。インターネットで何をしているかというと、60 代は 100%に近い割合で検索に使っている。ただ、高齢者の中には、Google でも Yahoo でも何かキーワードを検索して、上部に出てくるものが広告であることを知らない方が非常に多い。パソコンで検索すると、画面のほとんどが広告で埋め尽くされることもある。高齢者は、それに気づかず検索結果としてアクセスしてしまう。そこに不審な広告が紛れ込んでいることもある。日常的に何か検索しようとして怪しい広告から詐欺へと誘導されてしまう危険がある。

高齢者もスマホは便利だから使いこなしたい。でもわからないことがある場合、誰に聞きたいか。女性は、特に家族に聞きたいと思っている方が非常に多い。男性は購入店で聞くか自分で検索するという方が多い。

身内の話をするが、私の母は 70 代である。5 年ほど前にスマートフォンを初めて持った。それまでパソコンもインターネットも使ったことがなかったので、私と同じ機種を母に持ってもらい、わからないことがあったら私に全部聞くことにして、アプリの設定などは私が管理することにした。ところが、最近非常に困ったことが起きた。母は一人で買い物に行くとき、私が入れておいたポイントカードのアプリを使っているのだが、先日お店でそのアプリを使おうとしたら、ドラッグストアの店員から「これはもう古いので使えません」と言われたそうである。「なら、いいです」と母は断ったそうだが、店員は親切そうに母のスマホを使って何か設定を始めてしまった。母は何をされているかよくわからなかったが、相手がスマホを操作しながら下の名前と誕生日を聞いてきたので、母は答えたそうである。自宅に帰り、「新しいアプリを入れてくれたんだよ」と話していたので、私はびっくりして慌てて母のスマートフォンを見た。母のスマホは iPhone で、アプリを入れるときには Apple ID とパスワードを入れる設定にしていたが、なんと Apple ID のパスワードがリセットされて

いた。リセットをするためには、新しい手続きのメールが来るようになっているが、その店員は、メールの中身も見て、全て設定し直していた。結果的に、母は、新しいパスワードが何に設定されたのか知らないという状況になっていた。店員がお客様のスマホを使ってはいけないと指導している企業が多いとは思うが、お節介で設定してしまう店員もいる。しかし、これは非常に危ないことである。高齢者は自分のパスワードがますますわからなくなり、自分で管理ができなくなってしまう。そういうことが実は巷でじわじわ広がっているのではないかと危惧している。

一方で、80 代の親戚はインターネットに自信がある。新しいスマートフォンやパソコンをよく買う。わからないことがあったら検索するのだが、この 1 年間で 5 回、偽サポート詐欺の被害に遭いそうになった。普段見ているサイトで、突然、偽の警告が出てきて、「ここに電話してください」という画面が出てきたとのことだった。夜だったが、「これはまずい」と私に電話をかけてくれたので、そこで詐欺を止めることができた。このように、夜、自宅にいるときにパソコンを使っていて、偽の警告が出てくることがあり、どうしていいかわからずに詐欺の相手に電話をかけてしまう方が結構いるのではないだろうか。

■ 高齢者の状況

高齢者がこれからスマートフォンやタブレットに移行していく際、一緒に住んでいる家族がいればすぐに聞けるかもしれないし、外出先なら誰かに聞くこともできるかもしれない。ただ、購入店で聞こうとなっても、今は予約制でかなり待たないと教えてもらえない。しかも個別のアプリや自分が登録したサービスの説明はしてもらえない。「多分これは詐欺なのではないか」と思っても、どうしていいかわからなくなって偽サポート詐欺相手に電話をかけてしまう。

全ての年代に当てはまることだが、何か困ったときに相談することを恥ずかしいと思う方はかなり多い。そういう人にとって「サポートします」と申し出てくれる人は、ときには神様のように見えてしまう。悪質業者がそういった心の不安に付け込んできている。今、特に高齢者に対するサポート系の悪質な詐欺が本当にたくさん出ている。

■ ソーシャルメディアについて

ソーシャルメディア（SNS）は、広く公開され、誰かとつながれる場所である。設定で非公開にすることもできるが、基本的には全世界に公開されている。その代表格が旧 Twitter の X、Instagram、Facebook、TikTok である。

ソーシャルメディアでは、人と人とがつながる。自分が友達になっていない人でも検索す

れば見つけることもできるし、サービスを使っていない人でも外部から検索をして投稿を見ることが可能である。つまり人間関係が視覚化される特徴がある。そして簡単な操作で誰かの投稿を全世界に拡散することも可能である。

最近ソーシャルメディアの活用シーンが大きく広がってきた。企業においてもリクルート用、広報用など、いくつものソーシャルメディアのアカウントを使い分けており、就職活動中の学生にとっても、ソーシャルメディアのアカウントが非常に重要なツールとなっている。最近では、飲食店で注文する際、QR コードを読み取って注文するというお店が増えている。お店によって、スマホを QR コードにかざすと、いきなり LINE の友達登録の画面が出てくることもあり、以前私も驚いた経験がある。このように一時的ではなく友達登録が前提のお店も出てきている。

ソーシャルメディアの利用率は、ほぼ全ての世代において少しずつ増えてきている。13 頁のグラフを見ると、65 歳以上でも、60%の人が何らかのソーシャルメディアを使っている。ドコモのデータを見ると、日本においては年代によってどのサービスを使うかがかなり違っている。10 代では、TikTok が高く、42.3%である。70 代においては LINE が一番多く、その次が Facebook である。

私が非常勤講師をしている大学では、毎年 1 年生全員に「あなたがアカウントを持っている（登録している）コミュニケーションサービスはどれですか」というアンケートを実施している。どこの大学でも LINE はほぼ 100%利用している。3 年ほど前から、旧 Twitter の利用率が徐々に低くなり、その代わりに Instagram が 92.6%と非常に高い割合になってきた。この大学は芸術系のコースがあるので Pixiv というイラストを描いて共有するサービスの利用率が高い。そして、去年のデータにはなかった、フランス発の BeReal の利用者が急増している。BeReal は特に高校生や大学生にとても人気のある写真共有サービスである。特徴は、アプリから 1 日 1 回ランダムな時間に通知が届き、加工する暇もなく、2 分以内に今の自分の状況と自分の顔写真をインカメラとアウトカメラで撮影して全世界で共有するというものである。いわゆる「盛れない SNS」と言われている。最近では、位置情報共有アプリ Zenly の代わりに whoo というサービスが人気となっている。ゲームの中でよく使われる Discord は、大学生の利用率が割と高い。

■ 自分の個人情報やプライベートな情報の公開に対する考え

IPA 情報処理推進機構が 2 年に 1 回、情報セキュリティの倫理に対する意識調査をしている。ソーシャルメディア等でプライベートな情報を公開することに対してどう考えるか。自分の身の回りのこと、家族のことをどれくらいの範囲の人までだったら見せてもいいと

考えるか。どの年代においても、「公開範囲を限定しているので問題はない」という意見が多いかと思いきや、10 代・20 代において、他の年代よりも特に多い意見が「家族や友人しか見に来ないので大丈夫」「これまでに問題が起きたことはないから大丈夫」という意見だった。「非公開にしなくても、自分の動向をわざわざ見に来る人はいない」と若年層は考えている。だが、ソーシャルメディアは誰でも検索することができるので、その考え方は危険である。

■ 誰もが情報の発信源に

世界的に見ると、今、数十億人の人たちが何らかの情報発信サービスやソーシャルメディアを使っている。となると、真偽不明の情報もたくさん出てくる。日本では、不確かなニュースや情報のことをまとめて「フェイクニュース」と呼ぶことが多いが、世界では、「ミスインフォメーション」と呼ぶ。 特に日本では、災害が発生したときなどに「誰かのために」と、不確かな情報が拡散されることがよくある。

2 年前、静岡県で水害が起きた。旧 Twitter には、「ドローンで撮影された静岡県の水害、マジで悲惨すぎる」という投稿とともに、濁流が街を飲み込む様子の写真が 3 枚掲載されていた。この投稿を見た多くの人が「大変そうだな」と思って拡散した。ところがこれは AI で作られたフェイク画像だった。それに気づいた人たちが投稿者を批判したが、投稿者はそれに対し、「ざまあ」と返信した。「なぜそんなことをしたのか」という問いに対して、彼は「騙される方が悪いから注意喚起のつもりで投稿した」と答えていた。私は決して騙される方が悪いとは思わない。もちろん騙す方が悪い。問題とすべき点は、誰でも無料でフェイク画像が作れるようになったことである。そのことに本当に危機感を持つべきだと思った。そのほかにも、誰かが喋っているように加工したもの、口元だけを改竄したようなものを「ディープフェイク」というが、無料のアプリで、誰でも簡単に作ることができる。こういったフェイク画像をどうやって見分けるか。見分けることも AI でできるのかもしれないが、非常に難しくなってきた。

悪意があって作られた偽の情報を「ディスインフォメーション」と呼ぶ。ロシアによるウクライナ侵攻以降、このディスインフォメーションが特に多く、メディアでも語られるようになった。

ソーシャルメディアを使っていくと、慣れてきた頃に、情報の偏りが起きてくる。例えば、私が何か自分の意見を投稿すると、「いいね」ばかりついてくる。その結果、自分と同じ考えの人が周りに多いと思い込む。それが「エコチェンバー」である。自分がシャボン玉の中にいることに気づかずに過ごしてしまう。世界はそんなものだと思いがちになってしまう。

特に日本でも災害が起きたときには不確かな情報が出回る。2016 年に熊本・大分で地震が起こったときは、大分の警察署が外国人専用の避難場所だと SNS で投稿された。実際に多くの外国人が詰めかけたが、それは虚偽の情報だった。ほかにも、行方不明や「落し物を見つけた」など、「誰かのために」「助けてあげたい」という投稿も拡散されやすい。私自身の身近な例だが、とある高校生が家族と喧嘩をして家出をした。その高校生は友達の家にいてすぐに自宅に戻ったのだが、いなくなったことを知った周りの友達が彼女のプリクラを使い、「この子がいなくなりました」と一斉に投稿し、あっという間に拡散された。ところが「もう大丈夫」という投稿は全く拡散されなかった。何年経っても、未だにネット上では、探している情報だけが独り歩きを続けている。投稿者は情報を出すときに、後処理のことまで思い至っていなかった。行方不明の人を探している投稿の中には、悪意ある投稿もある。今後、もし人を探しているという情報を目にしたら、すでに届け出があるかどうか、警察署の連絡先が書かれてあるかを目安にしてほしい。

誰かを告発するためや「こんな人がいる」と晒す目的で拡散されたケースもある。例えば、お店で何か食べ物を買ったら、そこに異物が入っていたとする。本来は、まずその買ったお店に連絡するものだと思うが、人によって、異物混入の事実をまず投稿して、みんなに知らせようとする人たちがいる。まず関係者に知らせるべきだという啓発も必要ではないかと思う。

自分の講義で、学生に落とし物を拾ったらどうするか聞いてみると、半分の学生は「まず投稿する」と答えた。その方が早く本人に届くからということなのだが、そもそも落とし物を拾ったときにどうすればいいか、適切な行動を知らない学生が多い。現在、落とし物は、最終的に警察に届けば、警察庁の公式サイトで全国の落とし物が検索できる仕組みを整えているが、広く知られていない。

■ 令和 6 年能登半島地震での事例

今年 1 月 1 日に能登半島で大きな地震があった。私は、地震が発生した直後からソーシャルメディアを見ていたが、数時間も経たないうちに偽情報が多く出てきた。SNS 上では、日本人ではない、海外の方が投稿したと思われる情報もたくさん広まっていた。このことは、去年、旧 Twitter で始まった「クリエイター広告収益分配プログラム」が影響している。多くの人が自分の発信を目にするとそれに伴い広告収入が入るプログラムである。閲覧者数（インプレッション）を稼ぎたい海外の人が日本で話題になっている投稿に殺到してしまった。この状況は今現在もずっと続いている。東日本大震災以降、日本では、災害のときに、ソーシャルメディアを広く使おうという機運が高まっていたが、今ではもう使い物にはな

らなくなってしまった。

17 頁に掲載している右端の投稿の画像は、実在する車のナンバーを写真に撮り、「空き巣かもしれない」という投稿をしたものである。その投稿を多くの人が拡散したが、実際は救助に駆けつけた親戚の車両や、他県から災害対応ですぐに乗り込んだ通信設備会社の車両だった。間違った情報が投稿されると、こういった方々が地域で活動しにくくなってしまう。それが災害のたびに起きてしまう。このディスインフォメーションに関連して、今週、能登半島地震の被災者を装って虚偽の文章を 10 数件投稿した男性が偽計業務妨害で逮捕された。

このように警察は業務妨害で逮捕し、事件化するように動いているが、誰が投稿したかを特定するのは、海外のサービスである旧 Twitter が相手ではなかなか手続きが難しいという現状もある。

■ ファクトチェック／情報のトリアージ

情報発信における情報の見分け方を「ファクトチェック」という。自分が目にした情報、出所はどこなのか、自分が発信することでかえって誰かの迷惑になっていないか、ノイズになっていないかを確認する。そして、情報の真偽に迷ったときは何もしないのが得策である。これを「情報のトリアージ」という。自分の中で情報の順位付けをすることは、社会人だけではなく情報発信ができる道具を手に入れた全ての世代の人たちにとって必要である。今、どうやって情報の順位付けを行なっていくかの訓練が求められている。

もし、ネット上のニュースを見ていて「この話は本当か」と気になったら、ファクトチェックの普及・推進活動を行っている非営利団体「ファクトチェックイニシアティブ」と「日本ファクトチェックセンター」のウェブサイトなどもぜひ参考にしてほしい。

■ 情報社会の現状

コロナ禍により、なるべく人と人とが接しないようにする気運が高まった影響で、ネットショッピングやスマホの決済を使う人も増えてきた。そして人と会えないからこそ、ソーシャルメディアが有効に活用できたという側面もあった。一方で、悪意ある人のほうがこういったサービスを悪用しているという現状もある。金融機関では以前から様々な対策を取られているが、利用者のリテラシーはなかなか向上していない。その結果、残念ながらフィッシング被害が急増しており、インターネットバンキングの不正送金も激増している。昨今では、偽サポートや偽広告がきっかけで詐欺に巻き込まれるケースが多い。特に広告を悪用した SNS 上のなりすまし詐欺の被害額が非常に多い。企業や組織、サービスを提供する側が

どんなに対策を取っても、社会全体で利用する側のリテラシーやセキュリティに関する知識を底上げしていかなければ撲滅は難しい。セキュリティは、自分一人がわかっていればよいというものではない。攻撃者はお客さん、家族、高齢者、子供たちなど、弱い人を狙ってくるので、みんなで見守っていく必要がある。

■ インターネットにおける人権侵害

識別情報の摘示

インターネットにおける人権侵害は、法務省のグラフを見ると、なかなか減ることもなく、令和 4 年から令和 5 年に至っては少し増えてしまっている。その中で、「識別情報の摘示」がじわじわ増えている。これは特定の地域に住む方々を差別する投稿がなされているということだが、ソーシャルメディア上でも最近結構見るようになった。特定の地域を撮影しながら配信または投稿し、「あくまで観光しているだけ」と投稿者たちはうそぶいている。

情報漏洩

インターネットにおける人権侵害には、まず情報漏えいがある。これは不正アクセスやウイルス感染などによって起きる。自分の個人情報を抜き取られ、被害に遭ってしまうこともある。

悪意ある投稿・肖像権

悪意ある投稿によって、プライバシーや名誉をひどく傷つけられてしまうことがある。私が相談を受ける中でも非常に多かった。仲の良い友達が無断で自分を撮影して投稿しても消してと言えずに自分の肖像権が侵害されてしまうこともある。

ストーカー行為

インターネット上のストーカー行為については、誰かが投稿したアイドルの顔写真の瞳に映った風景から、本人が生活している場所やよく利用しているところを読み取り、待ち伏せをして暴行を加えたという事件が実際に起きている。

情報アクセシビリティ

情報アクセシビリティは知る権利に関わってくる。例えば、色の見え方、カラーアクセシビリティに問題がある人や視覚障害者の方々など、全ての立場の方々にも等しく情報が届いているか、知る権利がちゃんと守られているか、人権侵害を考える上では重要である。

■ 情報セキュリティ 10 大脅威　2024

IPA 情報処理推進機構では、毎年、私達が生活や仕事をする上でどのような情報セキュリティの脅威があるか、個人と組織、それぞれ 10 項目を発表している。企業だけではなく、個人をターゲットとした情報やお金が狙われていることがわかる。

■ セキュリティインシデントにおける人権侵害

情報漏えいについては、ここ数年、ランサムウェア攻撃により情報を盗み取られる事件が続いている。病院や大きなデパートが被害に遭い、数ヶ月間、診察や営業ができなくなる状況が起きている。また、データや書類を紛失し、それが誰かに悪用されるといったことも情報漏えいにつながる。そのほか、ソーシャルエンジニアリングによる情報窃取も起きている。ソーシャルエンジニアリングは、私達の行動や心理的な隙を突いてターゲットの情報を盗み取っていくものである。

不正アクセス・不正ログインによっても情報が盗み取られる。インターネットバンキングの不正送金は、フィッシングやウイルス感染、ソーシャルエンジニアリングなどがきっかけで行われる。

■ 情報漏えい

2023 年に東京商工リサーチが出した調査結果を見ると、個人情報の漏えい等事故を公表した上場企業ならびにその子会社において、事故の件数は、175 件だった。これはあくまでも正直に公開したところに限るので、もしかしたら氷山の一角かもしれないが、漏えいした個人情報は 4,090 万件ほどだった。その原因は、半分近くが「ウイルス感染・不正アクセス」である。以前は、個人のうっかりミスや誤送信によって情報が漏えいすることが最も多かったが、ここ数年は、ウイルス感染・不正アクセスによる情報漏えいの 1 件あたりの規模が大きい。実はこの個人情報の漏えい件数は、前年の 7 倍になっている。

■ 最近の漏えい事故

福岡県

ここ数年で起きた特に深刻な漏えい事故は、2021 年のコロナ禍真っ最中に福岡県で起きた事例である。福岡県では、外部の医療従事者の方とコロナ対策に関する情報共有を行うため、クラウドサービスを利用していた。そのクラウドサービスにアクセスするためには、URL を関係者にメールで送信する必要があった。ところが、そのメールを無関係な第三者

に誤送信してしまった。そのメールに気づいた第三者が県に注意をし、設定を変更したものの、実際のところ個別のアクセスは可能となっていた。そのあと、第三者が報道機関に通知し、本件がニュースになった。当時、コロナに感染した方の住所・氏名だけではなく、過去の病歴までも第三者に公開されてしまっていた。こうした事態は、福岡だけでなく他の自治体でも発生した。中には、公式サイトにコロナ陽性者の詳細な情報が載ってしまった自治体もあった。

精神科医療センター

今年の 5 月には、岡山の精神科医療センターで、ランサムウェアによる不正アクセス被害があった。詳しく調べたところ、実はダークウェブ上に流出した情報が公開されていることがわかった。件数としては患者 4 万人分で、その中には患者の住所・氏名・生年月日だけではなく、治療方針や病棟会議の議事録等も含まれていた。使用機器の脆弱性を関係機関から指摘されていたにもかかわらず、対策が棚上げ状態になっていたことが原因だった。その結果、不正アクセスを受け、情報が外部に公開される事態に至った。精神科の通院情報は、本当にセンシティブなものである。被害者の方は今もとても不安な状況で過ごされていることかと思う。

大阪の小学校

大阪の小学校でも事例がある。先生が職員室のパソコンで学級通信を作ろうと思い、インターネット上からイラストをダウンロードしていた。すると、突然パソコンが停止して「ウイルスに感染しています。修復するにはここに電話をかけてください。」と出てきたので、その先生は電話をかけてしまった。相手の指示どおりに操作をしていたところ、途中で校長先生が電話を代わり、校長先生はおかしいと気づき電話を切った。その後、パソコンを再起動してみると、デスクトップに保存していた生徒の個人情報等が入ったファイルがなくなっていたことが判明した。本来、偽サポート詐欺の対策を知っていればよかったのだが、そもそもデスクトップに個人情報が載ったデータを置くことがルール違反であった。万が一事故が起きた場合に備え、人に見られてはいけない情報にはパスワードをかけるなどの対策をして、管理をしっかり行う必要がある。たまたま学校という公的な機関で発生したことからニュースになったが、報道されていなくても、偽サポート詐欺により、遠隔操作でパソコンの中身を見られたかもしれないという事例はあちこちで発生している。

北海道の中学校

先月、北海道の中学校で先生が体育館のステージに書類を置き忘れたという事故が発生した。そこには、生徒の成績や交友関係、保護者の情報、その生徒に対する配慮事項等が含まれた文言があった。体育館に置き忘れたのを知った生徒たちが、書類の写真を撮って、生徒間で共有をした。さらに、それだけではなく、誰かが撮った写真を SNS に投稿したのか、最終的には暴露系インフルエンサーと呼ばれる人がネット上に公開した。名簿の写真も投稿されていて、部分的に黒塗りされてはいたが、具体的な学校名とともに事故の概略が発信され、拡散される事態となった。そもそも置き忘れたことが最大の問題ではあるが、見てはいけないものをたまたま見てしまったときに撮影してしまう人たちがいることに対して、どうすればいいかも含めて、我々教員も今後注意をしていかなければいけないと思っている。

■ 情報漏えいによる深刻な被害

先月、特殊詐欺の容疑者が逮捕され、詐欺電話のマニュアルが押収されたニュースがあった。その中には、認知症患者の情報リストが含まれていたことが報道された。愛知県警では、特殊詐欺に遭った後に亡くなられた方々のデータを公開している。データを見ると、亡くなってしまった理由として、「親族に責められたから」「申し訳ないと思ったから」という回答が多い。あくまで被害者なのに、周りに責められ、申し訳ないと思って自死をされてしまった方が実際これだけいることに、私は非常にショックを受けた。お金を失ってしまうということは、私達が生きるうえでこんなにも深刻な被害を及ぼすのである。アルバイト感覚で特殊詐欺に手を染める人たちの軽い思いと、この深刻な被害のバランスが全く取れていない。警察や金融機関の皆さまが本当に努力して様々な啓発をしているが、私達利用者のリテラシーがまだまだ追いつかず、自分たちが狙われていることにピンと来ていない。被害者になってしまう方を減らすため、地域、あるいは日本全体で、私達のような啓発する立場の人たちがもっともっと頑張っていかなければいけないと強く感じた次第である。

■ 情報発信による問題

本人は匿名だと思っていても、職務上知り得た情報や特定の業種の人しか使わない言葉で投稿していると、ある程度、例えば「金融機関にお勤めの人かな」と察しがつく。プロフィールを詳しく書いていないつもりでも、地震が起きたときや近くでサイレンが鳴ったとき、突然ゲリラ豪雨になったときに、そのことを投稿すると、わりと個人が特定できてしまうことが多い。

内容によっては労働問題に発展したケースもある。例えば、とある方が病気で休職されて

いて、たまたま上司のソーシャルメディアを見てみると、実名を挙げて「○○さんが休んでいるから仕事がたまって大変だ」「○○さんの代わりに雇用した××さんはすごく働いてくれるからありがたい」といったことを日々投稿していることを知り、ショックを受け、ますます復職しにくくなった、という相談があった。私は労働問題と判断し、労働局に仲介した。その結果、上司によるパワーハラスメントと認定され、労働局が仲裁に入るまでに発展した。世の中には、誰かから見聞きした情報を悪意なく投稿する人もいる。「いま電車乗っているけど＊＊の社員がめっちゃ愚痴ってる。」「友達が○○支店に異動になったけど、△△から 1 時間ぐらいしか離れてない。」といった具合に、ご本人は投稿していないことでも、周りの人が本当に何気なく、ただ近くの友達に知らせる感覚で全世界に公開することがある。

6 月には、研修中の大学生が病院で患者の電子カルテをパソコンの画面上で撮影し、それを友達しか見ないはずの SNS に投稿したというニュースがあった。その投稿を見た友達の中に、「これは良くないな」と思った方がいたのか、通報があって発覚した。私も医療系の大学で非常勤講師をしているが、医療現場において、倫理上、こういうことをしてはいけないと繰り返し厳しく教育されているのだが、業務や実習に慣れてくると、仲間内で情報共有してしまう人が出てくる。その他、プロフィールに金融機関とは一切書いていなくても、投稿内容から様々な想像がつく。例えば、投稿内容にお客さんのことが書かれていると、投稿を見た人から「私のことではないか」と思われかねない。

誹謗中傷

誹謗中傷というのは、いわゆる悪口である。俗に悪口と呼ばれるものは侮辱罪と判断される。一方で名誉毀損というのは、たとえそれが事実であっても、本人が知られたくないことを広く公開することで成立する場合がある。以前、プロレスラーの方が番組出演を通して誹謗中傷を受けて自死された事件では、加害者は罰金 1 万円以下だったが 2 年前に 30 万円以下に引き上げられた。時効も 1 年から 3 年まで延長された。

ある事例では、動画投稿者は、自分が直接相手を傷つけたのではなく投稿されていた情報を集めて動画を作っただけだと主張したが、名誉毀損で書類送検された。

不適切な行為の投稿

去年、愛知で起こった事件がある。10 代の少年少女らが「何か買ってあげるから」とホームレスの人をコンビニに呼び出した。そして、そのコンビニで買い物をする様子を撮影し、さらに会計するときになって、お金を払わずに逃げた。そしてその様子をずっと配信していた。もちろんこれは相手をひどく傷つける行為であり名誉毀損にもなると思うが、実際は、

本来の目的とは違うことでコンビニに入ったということから、建造物侵入容疑で書類送検された。本人たちは、「受けると思った」「バズりたかった」と供述したとのことだった。

5月には、岡山で同僚の社員の飲み物に自らの体液を繰り返し入れ、盗撮をしていた人が書類送検された。もちろん、その行為自体が言語道断だが、それを本人が SNS に投稿し、その投稿を見つけた第三者が犯人探しを始めて、一気に話題になってしまった。その後、犯人は書類送検されたが、事件の被害者の人権が考えられていなかった。特定した人たちは正義感からやっていたとしても、自分が被害を受けた当事者だと知られたくないと考える被害者も多い。この事例では、勤め先だけでなく、どこの支店までわかってしまった。ソーシャルメディアでは、被害者が置いてきぼりの正義感の暴走が時々起こってしまう。

暴露系インフルエンサー／世直し系・私人逮捕系配信者

「内部告発を募集します」「こういう不正があるらしいので今調査中です」といって情報を集める人がいる。世直しをするためにとうそぶいて、「この人が犯人だと思われます」「この会社に勤めていると思われます」と配信する。行き過ぎた行為で、全く違う人を犯人扱いして逮捕された事例もある。世直し系や私人逮捕系の配信をどう思うか、授業の中で学生に聞いてみると、約3分の1の学生が「エンターテイメント」「必要悪として仕方ない」と答えた。その数が少なくなかったことに、ショックを受けた。警察が逮捕しないのだったら、他の人が懲らしめるのもありだと考える人たちがいるが、私達に誰かを裁く権利はなく、被害者の人権が置いていかれてしまう。安易に誰かを告発しようとすることは人権侵害につながりかねない。

肖像権

相談の中でも非常に多いのが、肖像権の問題である。私達は写真や動画を公開されない権利を持っている。しかし、仲が良い相手だからこそ、撮影されることや投稿されることに対して嫌と言えない。私達の周りには、DV の被害やストーカー行為等いろいろな理由から、「この街に住んでいる」「この企業に所属している」と言えない人たちが一定数暮らしている。知り合いであっても、その写真を撮影して何に使うか、一言言ってあげる配慮が必要である。

去年、性的姿態撮影等処罰法が新設され、これまで条例等でしか対応できなかった隠し撮りが厳罰化されるようになった。

リベンジポルノ

リベンジポルノは、過去にやり取りしたプライベートな画像や動画を公開され、ばらまかれるという行為で、深刻な人権侵害につながる。リベンジポルノを行なった相手を名誉毀損で逮捕することはできるが、実際起きた後では救うことが非常に難しい。

警察庁が最近出したデータによると、リベンジポルノの被害者は 10 代 20 代が 70%を占める。加害者になる相手はほとんどが元々身近な相手だった。学校現場では、リベンジポルノや児童ポルノなど、性的な被害・加害に対しての教育が後回しになっており、なかなか生々しくて話せないと言われる先生が多い。でもこれだけの被害が起きており、特に若年層の被害が大きく、社会人であれば逮捕されると会社名まで表に出る。そして被害者は、業務もままならないほどに傷つく。社会に出ると、性的姿態撮影等処罰法など新しい法律を知る機会がなかなかないので、ぜひ社員教育の一環に入れてほしい。プライベートであっても誰かの裸の画像を記録に残さないこと、隠し取りは法に触れるということなどを、一年に一度は周知してほしい。被害を受けてからではなかなか助けられず、一生苦しむことになる。被害者にも加害者にもなってはいけない。どんなに信頼できる相手であっても、記録に残してはいけない。自分も撮影しないし、人に撮影をお願いしてもいけない。繰り返すが、社員教育の中でもこういった内容をぜひ入れていただきたい。

■ 投稿による被害を受けたら

新しくできた性的姿態撮影等処罰法について、非常にわかりやすくまとめた文書を法務省が公開している。また、弁護士が法教育の出前講座をしている地域もあるので、法律について詳しく知りたい場合、都道府県の弁護士会等にぜひ問い合わせるとよい。

情報発信による投稿の被害を受けるとパニックになってしまう方が多くいるので、総務省または警察庁の相談窓口に公開されているチラシを組織全体に周知してほしい。このチラシでは、ケースごと被害者の窓口が分かれている。そのほか、各ソーシャルメディア事業者が用意している通報システムを利用するとよい。私もよく旧 Twitter 等で通報する。早ければ 1 時間以内に「ルール違反が見つかったのでアカウントを凍結した」という返事が返ってくる。

インターネット上での人権侵害における開示請求等を定めるプロバイダ責任制限法は、2022 年に改正され、発信者を特定する裁判が 2 回から 1 回になるなど手続きが簡略化された。だが、被害者の削除に対しての権限は依然として弱い。それに対し、1 年以内に施行される情報流通プラットフォーム対処法では、削除依頼の窓口を設けることや対応方法が明確化され、わかりやすくなったので、かなり助けになると考えている。これまでは削除依頼を出そうにも、問い合わせの窓口にたどり着いても英語のみのページになってしまったり、

そのまま海外サイトにつながる等、そこから先に進まないというケースが非常に多かった。この情プラ法では、日本の社会・文化に詳しく、かつ日本語がわかる担当者を窓口に置くことが義務付けられているので、被害者の救済に対して早く動けるようになるものと期待している。なりすまし広告、偽広告の被害に対しても、なりすまされた有名人がすぐに削除申請を出し、スムーズに対処できるようになると考えている。この 1 年以内に総務省もガイドラインを作ると言っているが、表現の自由とのバランスや、対象とするサービス事業者の範囲など、もっともっと内容を詰め込んだ法律になっていくことを期待している。

■ 違法・有害情報の通報

児童ポルノの掲載など、違法有害情報については、インターネットホットラインセンターという窓口がある。全国でサイバー防犯ボランティアとして、今、数百人の方々が活動しており、私もその指導にあたっている。子供たちを危険にさらすような有害情報があれば、IHC に通報するとそこで精査されて、都道府県警に連絡が行く。海外のプロバイダ等であれば、海外の関連機関を通して対処を行う。誰かを危険にさらすようなソーシャルメディアの投稿やウェブサイトを見つけたら、皆さまご自身でも通報できるので、ぜひ活動をしてみてほしい。通報窓口は、猥褻なものなのか児童ポルノなのか等、対応する法律でカテゴリーが分かれており、緊急を要するものは 110 番になるが、どのジャンルになるかわからない場合は「その他」でよい。

■ こんなこと、ありませんか？

ソーシャルメディア上、匿名であっても本人を特定することができることがある。自分の投稿が誰かに影響を与えていないか、投稿者自身がよく注意してほしい。その場に実はいたということを言えない人もいるかもしれない。飲み会や懇親会で「今日は誰々といます」という写真を投稿するときは、仲が良い方であっても事前に許可を取ってほしい。

最近はもう情報発信していないけれどアカウントだけはまだ生きているという人もいるだろう。一度登録したアカウントは、アプリを消しただけではネット上の投稿は消えず、検索したら永遠に出てきてしまう。もう使わないのであれば、時間が経って ID とパスワードを忘れてしまう前に、アカウントの退会手続きをすることがお勧めである。アカウントを削除してソーシャルメディアから退会手続きをするときは、プロフィールの写真を消し、プロフィールに書いてあることを真っ白にしてからアカウントを削除したほうがよい。サービスによっては、いつ戻ってきてもいいように一度登録したプロフィールを退会後もそのままにしておくところがあるからである。

■ その情報、相手は公開していますか？

例えば、A さんという方が「今日は家族でお花見です」と家族でお弁当を食べているところを投稿したとする。この方は匿名で、自分の住んでいる場所をオープンにしていない。だが、コメント欄を見ると「〇〇さんのご家族初めて見ました！」「〇〇ちゃん大きくなったね！」と本人以外の人が実名を公開してしまっていることがある。親しい仲でも相手の情報公開に関するポリシーを尊重し、相手が過去にどこまで明らかにしているのかを確認してから投稿してほしい。

■ 情報収集について

「ソーシャルエンジニアリング」とは、私達の行動や心理的な隙につけ込んで、個人情報を収集する手口である。ハイテクではなくアナログな手段も使われる。皆さんもご承知のとおり、金融機関の ATM では、ショルダーハッキングを防ぐ取り組みがなされている。攻撃者は攻撃するために私達の関心を引き、お金をかけてでも情報を収集し、ターゲット近づいていく。攻撃者は様々な手口を研究しているので、社員の皆さまにもこういったことがあるということを共有してほしい。

■ アカウントの管理を厳重に

皆さまが情報通信端末を手にしたら、まずその端末自体を安全に保つと同時に、サービスのアカウントの管理をぜひ厳重にしてほしい。昨今、パスワードリスト型攻撃が非常に多く発生している。面倒でも絶対にパスワードは使い回さず、多要素認証を設定する。多要素認証とは、知識（パスワード）と所有（スマホや端末）と生体（指紋）などの複数要素を組み合わせた認証方法である。

■ 情報発信の注意点

情報発信においては、インターネットという場である以上、秘密の場所はない。とあるソーシャルメディアでは、非公開リストが公開されるバグが発生したこともあった。限定公開、非公開は、必ずしも完全ではないと考えていた方が無難である。

言葉や写真は、想像以上に、他人によって異なる捉え方をされるものである。情報は常に発信した後に独り歩きをしてしまう。言葉を選ぶというのは、非常に難しいことである。その難しいツールをうまく使いこなすために、特に体調が悪いときやお酒を飲んだときにアクセスをしないことを私はお勧めしている。自分が弱っているときに事故は起きてしまう。

弱っていることを自覚しなければならない。弱っているときにソーシャルメディアが助けてくれることもあるかもしれないが、自分から発信することはやめておく。言葉遣いが強くなって誰かを傷つけてしまうかもしれないことを意識してほしい。

■ 組織における対応

組織で研修するときは、最近の実例を用いて具体的に話すのが効果的である。世代間で、または経験の差から、情報の取り扱いに関するギャップが非常に大きくなっている。「そんなこと言わなくても当たり前」は、もう通用しない。皆さんが当たり前に思っていることも、丁寧に教えていかなければいけない。若年層と高齢者では文化が違う。プライバシーに関する考え方もかなり変わっている。それを超えるためには、世代を超えてどういう意識を持っているか共有しないと、なかなかここの溝は埋まらない。

「情報モラル」という言葉は、元々学校教育で生まれた言葉である。学習指導要領の中に「情報モラル教育」が登場してもう 20 年近くになる。元々は、この情報モラルの中に「セキュリティ」という分野も入っていた。モラルは人によってかなり違う。何を規範とするかは、世代によってもかなり違う。リテラシー、活用ということと職業倫理、あるいは法律に基づいて、丁寧に教えていかないと、なかなか事故は防げない。モラルは国によっても全然違う。多国籍社会になった今こそ法教育をもとに、日本では何を禁止されているか、何が裁判で侮辱とされているか、人権侵害とされているか、実例を用いて全ての人に話をすることが必要である。

情報発信する道具においても、どのような安全対策がとれているか、会社としてどのようなサイバーセキュリティ対策をしているのか、皆さまに共有してほしい。プライベートであっても社会人として、人権に配慮して情報発信することの重要性を、事例をもとに紹介してほしい。

どんなに気をつけていても事故は起きる。万が一事故が起きたときに、どのように対処すべきなのか。例えば相談窓口があるのか、会社としてどの部署が受け付けるのか、社員の皆さまにも明確にわかるようにしておきたい。

■ 相談窓口

セキュリティの相談窓口については、IPA の安心相談という窓口がある。警察にも相談窓口があり、職場でいきなりサポート詐欺の画面が出てきたときなど Web 上でも対応方法を確認することができる。お金や契約に関する不正な請求があれば、消費生活センターにつながる全国共通のホットライン 188（イヤヤ）も利用できる。違法有害情報の削除依頼を受け

付けている機関もある。何も起きてないときにこそ、こうした情報を把握しておいてほしい。

【質疑応答】

質問者：情報流通プラットフォーム対処法が施行される 1 年以内にガイドラインが出るとのことだが、内容は細かいものになりそうか、大体の今のイメージでも構わないので教えてほしい。

七條氏：総務省が消費者委員会の会議資料を 7 月 8 日に公開したが、そこに情報流通プラットフォーム対処法は 1 年以内に国として取り組むことが明記されている。
省令の整備については、まずプラットフォームの事業者を指定する際、各事業者に対して利用者数・発信者数等の提出が求められるが、その中で、通知までの具体的な期間など、総務省が個別に指示を出すための省令を整備し、手本となるようなガイドラインを策定する予定である。いつぐらいかはわからないが、「速やかに」と書いてあるので、ワーキンググループの検討委員によってガイドラインが 1 年以内に作られるだろうと理解している。
「国民を詐欺から守るための総合対策」で検索すれば、この PDF 資料が閲覧できる。

以上