

匿流犯罪と市民安全の心技体



2025.1.18 円卓会議配布資料

警察政策学会

市民生活と地域の安全創造研究部会

(注) 表紙のイラスト画の作成経緯と意味

「匿流」についての関心や注意を高めるためには、新春でもあり市民に馴染みの落語家にお話のきっかけをお願いするのが良いのではと入船亭扇治氏にご相談したところご快諾をいただき。その際、氏が大のネコ好きであることを知り、チラシにネコを登場させたいとデザイナーの櫻田秀美氏をお願いし、ネコの手を「千手観音」にたとえ官民協働の安全活力力量の増大を図っていきたいという願いを込めて。

はじめに

匿名・流動型犯罪グループによる 令和 5 年（2023 年）1 月の東京都狛江市の強盗殺人事件は、その凶暴性・また、人（ひと）間違い故に社会を震撼させた。特に「闇バイト」の「脳ところ」を支配下の起き、2024（令和 6）年 8 月以降、短期間・多数連続発生・凶悪強盗事件で、「匿流」（トクリュウ）の名を全国民が知るところとなった。

このグループ（犯罪主体）は、SNS や求人サイト等 を利用して募集された実行犯らで、緩やかに 結び付いたメンバー同士が役割を細分化させ、その都度、メンバーを入れ替えながら多様な資金獲得活動を行うという特性が見られ、特殊詐欺・投資詐欺・ロマンス詐欺事件の他、各種犯罪を敢行しており、今や、市民社会安全・安心を脅かす最大の脅威となっており、2023（令和 5）年 7 月、警察庁が「匿名性の高い SNS を通じて募集する闇バイトなど緩やかな結びつきで離合集散を繰り返す集団」と定義し、政府をあげてその取締や被害予防に各種対策を取っている。

彼らは、海外拠点で活動を活発化させるとともに、獲得した資金を Web・サイバー空間で「暗号資産」（資金洗浄：マネーロンダリング）とし更なる違法活動や新たな資金獲得事業活動を展開していると思われる。

新型組織犯罪の被害の未然防止のためにも資金源を差配する金主を含む匿名・流動型犯罪グループ全体の実態解明が急がれる。

当部会では、匿名・流動型犯罪グループを、市民安全・安心を脅かす最大の脅威と位置づけ、被害予防の観点から円卓会議や研修会を行っているところである。

本資料は、令和 6 年度部会活動において実施した「最近の犯罪情勢と市民安全の心技体」と題する有識者の講演記録等を資料化したものである。一般啓発資料としても活用していただければ幸いである。

市民生活と地域の安全創造研究部会

部会長 石 附 弘

目 次

I 円卓会議【匿・流】型犯罪から市民社会を守る 講演録（2025 年 1 月）

第 1 部 新春落語 「匿流小話と新年の笑い」 入船亭 扇治…………… 1

第 2 部 「匿名・流動型犯罪グループの実態と対策」

1 「匿名・流動型犯罪グループが敢行する詐欺や強盗から身を守るポイント」
石 井 啓 介…………… 4

2 「サイバー空間の脅威の情勢と JC3 の主な活動～産官学の連携の現場から」
櫻 澤 健 一…………… 11

第 3 部 市民安全の心技体

1 「子どもの SNS 利用の現状～大人が知っておきたいこと、できることは～」
大 久 保 貴 世…………… 18

2 「高齢者がネット取引でだまされないために」
木 村 嘉 子…………… 25

3 指定発言
世界の闇バイト事情、犯罪組織のメタモルフォーゼ（metamorphose）
浦 中 千 佳 央…………… 30

II 研究ノートから

SNS を含む Web・サイバー空間の犯罪社会現象について
～詐欺蔓延社会の構造と人の脳（若干の考察）～

石 附 弘…………… 34

円卓会議 【匿・流】型犯罪から市民社会を守る

闇バイト連続強盗殺人事件などサイバー空間の脅威と市民安全

講演録（於 日比谷図書文化館 2025 年 1 月 18 日）



1) 講師 入船亭 扇治氏（いりふねてい せんじ）

肩書 一般社団法人落語協会所属真打

演目 「匿流小断と新年の笑い」 1962 年岐阜県美濃市出身 1981 年上智大学文学部新聞学科卒、2001 年真打昇進

受賞歴 第 53 回国立演芸場花形演芸会銀賞、NHK 新人演芸大賞入選、林家彦六賞
カルチャーセンター NHK 学園の文化講座で『落語に学ぶユーモア』について講義。



2) 講師 石井啓介氏（いしい けいすけ）

肩書 警察庁長官官房参事官（匿名・流動型犯罪グループ対策担当）兼組織犯罪対策第二課長

演題 「匿名・流動型犯罪グループが敢行する詐欺や強盗から身を守るポイント」

2001 年警察庁入庁。暴力団対策課課長補佐、在中華人民共和国日本国大使館一等書記官、刑事企画課理事官などを経て、2022 年警視庁第一方面本部長兼警務部参事官、2023 年警察庁刑事指導室長、2024 年 4 月警察庁長官官房参事官（匿名・流動型犯罪グループ対策担当）、同年 10 月組織犯罪対策第二課長を兼務。



3) 講師 櫻澤健一氏（さくらざわ けんいち）

肩書 一般財団法人日本サイバー犯罪対策センター（JC3）業務執行理事

演題 「サイバー空間の脅威の現状と JC3 の主な活動」

1988 年に警察庁入庁。富山県警察本部長、内閣情報調査室審議官、警察庁総括審議官等を経て、2022 年 8 月警備局長で退官。2023 年 1 月から現職。同センターは米国 NCFTA 等との国際連携も図りながら、サイバー対策分野における民官学連携を進めている。2024 年 4 月から静岡大学情報学部客員教授。



4) 講師 大久保貴世氏（おおくぼたかよ）

肩書 一般財団法人インターネット協会 研究員

演題 「子どもの SNS 利用の現状～大人が知っておきたいこと、できることは～」

SNS の利用方法やフィルタリングの設定マニュアル「その時の場面集」の作成、インターネットのルール＆マナー検定の実施、自治体の相談窓口相談員などを担当。トラブルの事前予防策や対処法を周知するため、学校講演や教育ビデオ等も出演。



5) 講師 木村嘉子氏（きむらよしこ）

肩書 消費生活コンサルタント

演題 高齢者がネット取引で騙されないために

平成 4 年（1992 年）より消費生活相談員として消費生活センターに勤務。電気通信事業分野の消費者トラブルに取り組みながら、消費者教育・啓発を実施。関係省庁や業界団体との意見交換もかさね、トラブル削減に努める。



6) プロモータ 石附 弘（いしづきひろし）

肩書 日本市民安全学会会長、警察政策学会、市民生活と地域の安全創造研究部会長。警察庁暴力団対策第一課長（初代）、長崎県警察本部長、WHO 推奨セーフコミュニティ厚木市専門委員などの経験から、事件事故の被害予防安全について調査研究や啓発活動に邁進中。

第1部 新春落語「匿・流小噺と新春の笑い」

「トクリュウ落語」を手がけ見えてきたこと

一般社団法人落語協会所属真打 入船亭 扇治

「落語を通じて、匿名流動型犯罪について語ってもらいたい」。日本市民安全学会の石附会長から私の出身大学大先輩を通じてそうお話をいただいた時、正直初めは戸惑いました。

一介の弱小噺家である私も、トクリュウが「離合集散を繰り返し主犯が特定しづらい、ネット社会の新しい形態の犯罪集団である」という程度の認識はあります。でもそれを笑いの芸能・落語とどう結びつけたらいいのか…。ちょっと悩むところもございましたが素人が生半可な知識を妙にこねくり回すのではなく、学会関係者皆様の新年の集いでの一席・専門家の方々の講演に先立つ前座役のお賑やかしとして気軽にやらせてもらえばいいんだと腹をくくり、トクリュウを題材とした短い創作落語の構想を練り始めました。

10分弱にまとめる予定なので、一席の中にトクリュウについてのあれもこれも詰め込むわけにはいきません。ここは一般人が知らず知らずのうちに犯罪に加担してしまうきっかけの一つとして社会問題になっている「闇バイト」を中心ネタとして、噺を紡いでみます。

最初は「お喋りが得意な方にピッタリの好案件！」のフレーズに乗せられた呑気な噺家が、特殊詐欺ターゲットとの直接連絡役「かけ子」を引き受けてまき起こるひと騒動…。というストーリーを考えついたのですが、実際に組み立てていくと思ったほど話がうまく転がってくれません。ここは無理に内容を落語の方に寄せるのではなく、闇バイトに一番はまりやすい若い世代を主人公として方向転換。地方から上京しまだまだ都会に慣れていない純朴な苦学生「橋本」、その同期の友人で面倒見のいい自宅通学生「井上」。仲のいい男子学生二人の掛け合いで、物語は進んでいきます。

～創作落語『勇者よ、トクリュウに立ち向かえ！』あらすじ～

大学のキャンパス内で友人の橋本がスマホ画面眺めてニコニコしているのを見かけた井上、なにが嬉しいんだと訊ねると、学費生活費を稼ぐため日々アルバイトに精出している橋本にとってこれ以上ない好条件の仕事が見つかったとのこと。

その内容は「お年寄りのお宅へ伺って荷物預かって、それを都内の指定された場所へ運ぶだけで1件につき手取りで1万円もらえる」という、いかにも怪しげなもの。匿名流動型犯罪の片棒を担がされることになる闇バイトだから応募するのはよせと親身に教える井上、でも世間知らずでトクリュウなんて初耳の橋本は「とりあえず申し込みだけして、危なそうだったらすぐ辞めればいいんだし」と危機感ゼロ。

主犯格に個人情報握られてなかなか抜け出せず深みにはまっていくのがこの手の募集の怖いところだと井上に説かれた橋本、初めてトクリュウの恐ろしさに気づきすんでのところ闇バイトの

畏を回避することができた。ガタガタ震えながら「俺みたいな世間知らずで気の弱い流されやすい人間は、いつまた匿名流動型犯罪に巻き込まれないとも限らない。それが怖くってしょうがない」訴える橋本に、井上は優しく語りかける。「正しい情報知識の剣を持てば、お前もトクリュウ（竜）というドラゴンの牙を抜く、立派な勇者だ」

～了～

お後がよろしいようで…。

なにぶん本邦初公開の創作なので、まだまだ完成にはほど遠いのですが、作中出てくる「ホワイトで楽で高収入！」を謳って闇バイト募集をかける会社の名が「ピースフルハッピーナイスワーク」だとか「うま過ぎる話と裕の着物には必ず裏がある」と井上の祖母が言ってるなんてクスグリには聴衆のうち何人かの方がクスクス笑ってくださり、地口の落ちも「ふ～ん、なるほど」と手を叩いていただけたので、お客様に助けられてのまずは成功の部類ということにさせていたしましょう。

これからはさらにストーリーをブラッシュアップ・発展させ、笑いを通じて一人でも多くの方が匿名流動型犯罪について考えていただくための一助となる。今回ひねり出した物語がそんな一席に育ってくれたら、漸家冥利に尽きるというものです。

この漸を作り実際に人前で喋る過程を通じて、名称と漠然としたイメージしか頭になかったトクリュウというものの具体的な怖さ＝「人間が生まれ持った欲望を利用する、サイバー空間の深部に隠れた犯罪者」について私なりに理解が深まったのは大きな収穫でした。

人は誰しもよほどの徳を積んだ聖人でない限り、「楽して得したい、少ない労力でより大きな利益を得たい」という気持ちを心の奥底に秘めているもの。「自分はマンモス狩りにはあんまり貢献してないんだけど、洞窟に帰ったら一番大きい肉が欲しいなあ」と願った太古の人類の頃から変わっていない人間の性。そこに付け込む犯罪は昔も今も枚挙に暇がありません。オレオレ・ロマンス・投資系など特殊詐欺はその典型ですが、過去の犯罪集団にないトクリュウ独自の恐ろしさは、「我々は被害者だけでなく加害者にもなる危険性がある」点。

『勇者よ、トクリュウに立ち向かえ！』の登場人物・橋本もいくら世間知らずとは言っても闇バイトがどういうものかくらいは知っていますから、ちょっと前のように SNS 経由での募集だったらいくらなんでも怪しいと思ったはず。大手有名企業の運営する求人サイトに堂々と案件が掲載されていたから、疑おうとせず引っかかりそうになったわけです。

ことほど左様に、トクリュウの手口は進化・多様化が進んでいる。そして匿名性の高い通信アプリや海外サーバー・プロキシを利用することで自身はあたかも『ドラえもん』や『ハリー・ポッター』の透明マントをまとったかのように姿を表には表さない。一番行為が危険で犯罪が破綻・発覚するきっかけになりやすい実行犯を従来のように裏社会で調達するのではなくごくごく普通の一般人を騙して仲間に引き入れ、失敗したら手先はトカゲの尻尾と切り捨てられ主犯はの

うのうと逃げ延びまた新たな犯罪集団を形成する。不定形のアメーバによくたとえられるトクリュウは確かにこれまで私たちが遭遇したことの無い、

気づかないうちに社会のあちこちに触手を伸ばしている得体の知れない魑魅魍魎。

便利な反面諸刃の剣であるネット社会を悪用したトクリュウは確かに強敵ですが、拙作でも井上に語らせたように私たち一人ひとりがそれぞれ匿名流動型犯罪のことをちゃんと認識理解し「正しく恐れる」ことを心がければ自分たちの身はしっかり守れるはず。私も今回日本市民安全学会新年の集いに参加させていただいたことをきっかけに、トクリュウだけでなく「現代型犯罪に一般人はどう対処すべきか」について日々考え続けていきたいと思っています。

知識こそトクリュウ倒す矛と盾

第2部 匿名・流動型犯罪グループの実態と対策 その1

匿名・流動型犯罪グループが敢行する詐欺や強盗から身を守るポイント

石井 啓介

警察庁長官官房参事官（匿名・流動型犯罪グループ対策担当）

警察庁長官官房参事官（匿名・流動型犯罪グループ対策担当）は昨年４月に新設されたポストでして、昨今問題になっている匿名・流動型犯罪グループ対策の警察庁内の司令塔という役割であり、現在、私が務めさせていただいています。本日は「匿名・流動型犯罪から市民社会を守る」というお題でお話をさせていただきます。

匿・流型犯罪というものは非常に危機的な状況にございまして、警察は一生懸命頑張っておりますけれども、なかなか警察の力のみでは及ばない点もあります。そんな中で、社会全体で市民を守っていかなければならない、そういったことが重要だと思っております、本日の説明が皆さんの御理解を深める参考になればと思っております。

【匿名・流動型犯罪グループとは】

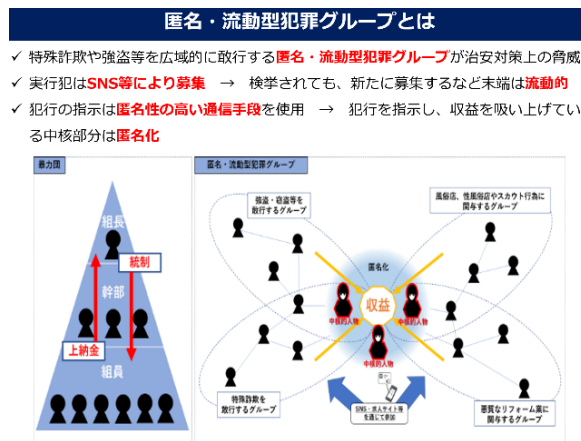
最初に、**匿・流グループ**とはということでございます。**匿・流グループ**の特徴について、暴力団との違い、又は同じようなところを、少しコントラストをつけながら御説明できればと思います。

暴力団というのは、日本における治安に対する最大の課題であります。最近、その勢力そのものは構成員の数等、減少傾向にあるということで、これも平成一桁の時代から暴力団対策法の制定、暴力団排除運動そういった取組の中で、社会全体で暴力団の力を弱める、衰退させることができているということです。

暴力団は、組長、親分は、擬制血縁関係という形で、子分、組員とピラミッド型の上下関係がはっきりとした組織であり、暴力団は「〇〇組だ」と名乗って、その威力を使って資金獲得をしていることが一つの特徴であります。また、組織実体もある程度把握しやすい組織かと思います。

では、匿・流はということですが、中核部分、いろいろな悪さ、悪くみをしているやつらが、自分は捕まるリスクを避けるために、SNS を使って、捕まるかもしれない、悪いことを実際にやる実行犯は、いわゆる「闇バイト」などで募集をする。そういった形で実行犯を調達し、そいつらにいろいろと悪さをさせて得たお金を吸い上げて自ら使うということで、中核部分が非常に匿名化されているのが特徴です。

これが昨今、SNS を中心としたサイバー世界の一つの特性かもしれませんが、特に本人



確認がなされていない「シグナル」とか「テレグラム」といったスマートフォンの通信アプリを使って連絡を取り合っているものですから、例えば犯人を捕まえて「お前、誰の指示を受けてやっているんだ」と聞きますと、例えば、「『〇〇』というシグナルのアカウントのやつに指示されました」などと言われたと。そいつは誰なんだということを突き止めるのが難しく、本当に悪いことをたくらんでいたり実際にお金を吸い上げているやつというのが匿名化されているのが実態です。

また、その下で悪いことをする実行犯、強盗に入らされたり、受け子、出し子といった、実際に被害者のお宅に行ってお金を受け取ったりするような、そういった実行役は SNS などでも募集されていて、捕まったらまた募集すればいいやということで、どんどん流動的になっているという特徴があります。

さらには、犯罪をやるに当たって、いろいろな役割分担がされているということです。例えばマネーロンダリングという、違法に得たお金を口座間でどんどん移動させるときに使うため、他人の口座等の必要な道具を調達する人間とか、携帯電話を他人に契約させて集める。そういう道具を調達する人間とか、詐欺とかのだましのシナリオを作る人間とか、いろいろな役割があります。

そういうやつらがネットワークし、違法なビジネスモデルみたいなものを作り上げて、今回の犯行はこいつと手を組んでやろうとか、今度、詐欺をやろうと思っているけれども、人が足りないから誰か調達してという、リクルーター役みたいな人間が、俺が SNS で募集するよとか、そういう形で、違法なことをビジネスのように相手をとっかえひっかえしながらやっている、そんな実態があります。

【いわゆる「闇バイト」等による実行犯の募集】

次に、いわゆる「闇バイト」についてですが、今、SNS などでも犯罪の実行者の募集が行われており、X（旧ツイッター）が非常に多く使われておりまして、ここは随分と削除などの対策を進めて、少し数は減っているかなと思いますけれども、今、Instagram とか Facebook や、通常の求人など、いろいろなところの求人情報で真つ当な求人を装って、応募してきた人間から個人情報を吸い取る。本人確認に必要であるとか、さらには、「お前の実家の住所を教えろ」とか、恋人がいるという「恋人の連絡先も教えろ」となって、本当に引くに引けなくするというようなところがあります。

闇バイトは、本当に真つ当なアルバイトでお金が欲しくて応募したのに、犯行を強要されてしまうという事案もあるわけです。東南アジア諸国の警察当局などと話していますと、人身取引詐欺と言われるような用語が、実は東南アジアでは認識されている実態があります。その国の地域の人たちも、誘拐というか、人身取引のような形で犯行に加担をさせられ、拠点に閉じ込められて、その中でいろいろな人に電話をしたり、騙しのテキストメッセージを送らされたりという形で、犯罪に組み込まれているという実態があります。こういった形で、捕まる可能性があるような実行犯は、SNS 等で調達しているというのが、匿・流の一つの大きな特徴だろうと思います。

【匿名・流動型犯罪グループに対する戦略的な取締りの推進】

警察の対策についてですが、警察庁では匿名・流対策ということで、昨年中いろいろと施策を打ち出しております。匿名・流は、日本国内はもとより、SNS、サイバーの世界は国境がありませんので、海外からも犯罪が可能という状況であります。このように広域的に活動しているので、個々の都道府県警察の取組、個々の部門、個々の所属では、実態解明や取り締まりはままならないということで、警察の総力をどう結集させるのかが課題となっています。

警察庁では、匿名・流が主にやっていると思われる資金獲得の手段を重点取組対象事犯として指定し、各都道府県警察での取組み結果を吸い上げて、警察庁でもしっかり横串を刺して解明し、それを各都道府県警察にフィードバックすると。また、得られた情報を基に、どういう体制で、どことどこが手を組めば匿名・流に対抗できるのか、総力を結集させるための取組を進める。そのための司令塔ということで警察庁では私が担当し、各都道府県警察でも横串を刺す司令塔を指定しています。

このように、警察が部門間の縦割りになっているところをいかに排除し、また匿名・流にとって都道府県の県境は関係ないものですから、県境の縦割りを排して、戦えるようにしようというのが、警察の匿名・流の取組の主な柱となっております。

【匿名・流動型犯罪グループの主な資金獲得活動と被害から身を守るポイント】

次に、匿名・流の主な資金獲得活動ということで3つ御紹介をしたいと思います。一つは特殊詐欺、あとは一昨年から急増しているSNS型投資・ロマンス詐欺、あとは昨年の8月以降、首都圏を中心に発生している強盗事件の関係です。

【特殊詐欺】

最初は特殊詐欺の関係です。令和5年の被害総額は440～450億というところでしたけれども、令和6年11月末の数字が581億、手元の速報値ですが12月末の数字は700億を上回るなど、過去最悪の被害となっており、特に昨年10月、11月、12月と、後半にかけて急増しているという状況です。

一番多いのは警察官がたりの手口です。「警察だ」と言われると、皆様、な

かなか話したことがないということで緊張されるのだと思います。緊張した中で、「あなたに犯罪の容疑がかかっている」、「自分の身の潔白を証明したければ、あなたの口座のお金を一旦移し替える必要がある」などと言われ、その指示に従って自分の口座にあるお金を振り込んでしまう。普通に聞けば、そんなことあるわけじゃないかというようなことが、「警察だ」という

最近の特殊詐欺の手口

- 警察官を名乗って電話がかかってきて、「あなたの口座が犯罪に利用されている」などと言って、被害者に犯罪の嫌疑がかかっていると欺罔
- SNSに誘導され、偽の逮捕状を示されたり、偽の制服を着た警察官がビデオ通話に登場
- 身の潔白を証明するために必要などと言われ、被疑者の指定口座に送金



者に言われ、しかも制服様のものを着た人間がビデオコールの中で出てきて、警察手帳様のものを示し、偽造した逮捕状の画像を LINE など送ってきて、あたかも相手方に逮捕状が本当に出しており、本当に自分が逮捕されるかもしれないと信じ込ませるような手口です。

皆さん、オレオレ詐欺というと「母さん、俺だよ俺、助けてよ」というのが昔は主流だったのですけれども、現在はいろいろな人物が登場してきます。弁護士役とか、警察、検察などの役所系も多く、このような手口が昨年急増したということで、注意を呼びかけています。

【特殊詐欺から身を守るポイント】

身を守るポイントについて御説明したいと思います。やはり犯人と話をしてしまうと、だまされてしまう方が多いということです。皆さんも「自分は大丈夫だろう」と思っていたらと思うのですけれども、実際にだまされた方も「自分は大丈夫だ」と思っていた方が非常に多いという状況です。電話をかけている犯人は、闇バイトなどで雇われているので、それこそ嘘家でも何でも人間が電話で「〇〇警察ですけど」と言っているのですけれども、これを何度も何度も繰り返しやっていると、こなれてきて、巧妙なシナリオとともに、騙しのプロになっていきます。1日何百件と電話していますので、トレーニングも相当積んでいます。

それに対して、警察官と話したことがない、犯罪の関係では素人とも言える一般の方が電話を受けてしまうと、どんなに用心していてもだまされてしまうのが実情でございまして、であれば、騙されないような心構えも大変重要でありますけれども、そもそもきっかけを無くせないかということで推進しているのが、国際電話サービスの休止の奨励であります。最近の情勢として、御自宅の固定電話に対して、国際電話番号からかかってくるのが非常に多いというのが実情です。国際電話番号というと、皆さんは「海外からかけているのか」と思われるかもしれませんが、実はスマホのアプリケーションを使って、例えば、アメリカとかの電話番号を取得して、その電話番号を使って電話をすとか、ショートメッセージのやり取りが、ほぼ無料でできたりします。このような実態を踏まえますと、国際電話をブロックするというのは非常に有効ではないかと思います。

今、NTT の契約は基本、付帯契約という形で、デフォルトで国際電話のやり取りができるサービスが入っていますけれども、使わないという方に対して、国際電話を一旦やめませんかというキャンペーンをやっています。さらに NTT さんや総務省さんとも話をし、原則は使えないようにし、必要な人が申し込むという形にすれば、より詐欺の被害は防げるのではないかと。そういったことについても御検討いただけないかという話も、併せてしております。

もちろん国際電話以外でも、皆様の携帯電話に、例えば、佐川急便やヤマトを騙って不在通知の連絡と称するショートメッセージが来て、URL をクリックすると犯罪被害に遭ってしまうようなことがあるなど、ショートメッセージ、電子メールといったものも悪用されていますし、SNS のダイレクトメッセージなども使われているので、こういうものに総合的に対策を取っていかねばならないと考え、取り組んでいるところです。

次は、やはり一個人だとだまされてしまうので、何かあったら相談をしてくださいということ

です。皆様の家族のネットワーク、家族の絆が大事だということで、我々は普段からお声がけをさせていただいているのですけれども、そんな対策を無効化しようというのがインターネットバンキングを悪用した手口です。これは皆さん、普通に使っていられちゃう方も多いと思うのですけれども、被疑者側は、被害者が銀行とかに行くと銀行の人に心配をされて、「これ、詐欺じゃないですか」と声がけをされるものですから、銀行に行かなくてもいいように、「インターネットバンキングの利用を開始して、自宅でそのまま振り込んでください」ということをやってきます。

この手口の悪い点は、インターネットバンキングの送金限度額というのが、ATM 利用よりも非常に高い。何百万とか、時には 1,000 万円台のものもあります。これを利用することで、自分の持っている資産を全額自分で振り込んでしまうという被害もあるのが問題です。警察などを騙る者から「インターネットバンキング」と言われたら、何で作らなきゃいけないんだと。最近、急増している手口ということで、キーワード的に是非覚えておいていただければと思います。

【SNS 型投資・ロマンス詐欺】

次は、SNS 型投資・ロマンス詐欺です。これは一昨年から急増しています。一昨年の 1 月からずっと右肩上がりが増加し、昨年 4 月をピークにちょっと下がっている感じなのですが、残念ながら 12 月に反転をし、急増しているという状況です。

被害額は特殊詐欺を優に超えておりまして、昨年中は 11 月までの数字で 1,141 億円ということで、投資・ロマンス詐欺と特殊詐欺を合わせて、11 月末の数字は 1,700 億円ですけれども、12 月末までいけばほぼ 2,000 億になります。これは警察に届け出があったものだけですので、相談に留まったものや、相談されていないものも含めると、さらに多額の被害が実際には出ているという状況だと思っています。これらが匿・流の資金源になっている。匿・流の中には海外のグループ、例えば東南アジアで捕まっているのは中華系の犯罪組織みたいなものもありまして、日本からお金をだまし取って、暗号資産とかに変えて自分の収益にしているというものも、実態としてあるという状況です。

手口についての御紹介でございますけれども、投資詐欺とは何かというと、よくあるものとして SNS 等に「必ず儲かるよ」とか、すごい札束を背景に「俺みたいになりたいか」みたいな広告が掲載されているのを見たことがある人もいると思いますけれども、はっきり言って詐欺ですよ。また、著名な方々を騙って自分が必勝法を教えますみたいなものもありました。こういった広告系は半分減りつつあるのですけれども、最近は SNS のダイレクトメッセージで、いろいろな方に「高収入、高額アルバイトに興味ありませんか」又は「投資に興味がある方はぜひこちらへ」という形で、個別にアクセスをしにくるものも非常に多い状況です。

犯行のほとんどは「LINE に登録して」と言って誘導し、LINE のやり取りの中で投資を指南すると称して、実在しないようなアプリをダウンロードさせて、仮想通貨や、現物の株などへ投資をさせると称してお金を振り込ませるというものです。振り込ませたお金があたかも偽のアプリ上ではすごく儲かっているように見えるため、更にお金を振り込んでしまう。その後、お金を引

き出そうとしたら引き出せないというのが、一つの典型的なパターンです。

投資詐欺は、InstagramとかLINEとかFacebookというのが昨年中は多かったのですが、ここに来て TikTok も増加している状況にあります。国民に広く使われている SNS が悪用されており、こういうところに広告を出したり、そのユーザーに対して個別にダイレクトメッセージを送るという形で、詐欺に引きずり込んでいるのが実情です。

【SNS 型投資・ロマンス詐欺から身を守るポイント】

どうやって気をつければいいのかということですが、一つは知らない人からのダイレクトメッセージとか友達登録申請というのは、用心すべきということです。ついこの間作られたばかりのアカウントからのメッセージであれば、注意するかもしれませんが、中には 1 年、2 年と育てている偽のアカウントを使っている例もあります。いずれにせよ、最近作ったアカウントで、友達の数もあまり多くないアカウントからのメッセージは

SNS型投資・ロマンス詐欺の被害から身を守るポイント①

3 知らない人からのDM、SNSの友人登録申請は要注意！

- 直接DMを送付したり、友人登録の申請をする手口が多発
- 知り合いではない人からのメッセージ、申請は詐欺の可能性あり

4 投資する際には登録事業者か確認！

- 株等のほか、海外金融商品や暗号資産への投資を勧誘する手口が多発
- 金融商品取引業の登録等を受けているか確認を

5 安全対策を講じているマッチングアプリか確認！

- 本人確認やその記録等を保有していない例も多く、相手方の特定困難

6 「必ず儲かる」は嘘！

- 少額の利益を払い戻した上で、多額の投資を促す例も

要注意です。また、SNS では自分の趣味とか活動を皆さん発信されているので、それを見て、「あなたと同じ趣味を持っています」などと言って、親近感を覚えさせる巧妙さがあるかと思います。自分の発信した情報を利用して近づいてくる、そういったところは要注意かなと思います。

この他にも、投資先についてはよく確認する必要がある点、マッチングアプリが最近よく使われている点も要注意です。マッチングアプリを利用して結婚とか、交際相手を探したいという方に対して、そういう真剣な気持ちをないがしろにするような卑劣な手口です。しっかりした安全対策がとられ、本人確認もされているようなマッチングアプリを利用してもらうことが大事かと思います。最後に、「必ず儲かります」は裏があるということで、詐欺ということを、よくよく覚えておいていただければと思います。

【強盗】

次は、強盗の関係です。これは昨年末の状況ですが、皆さん、非常に不安を覚えていらっしゃると思います。連続して強盗事件が一都三県を中心に発生してしまっていて、警察は実行犯を中心にたくさん捕まえているのですが、その首謀者の検挙に至っていないというのが実情でございます。政府全体で取り組んでおり、特に闇バイトの募集に関して、総理からの「そういうことはやってはいけない」という呼びかけをはじめ、警察への相談を呼びかけています。個人情報握られて引くに引けなくなった人も警察に相談してくださいということでお願いをしているのが、緊急でやっている対策でございます。

【強盗から身を守るポイント】

身を守るポイントとして、犯人グループは強盗の前に事前に下見をしていたりします。一つの例で、悪質リフォームをやっているグループが、実は裏では強盗とかをやっているグループとくっついているのではないかとという見立てもあります。「リフォームをしますよ、屋根が壊れているので上がらせてください」ということで家に上がり込み、やりとりの中でお家の状況、家族構成、資産状況がある程度分かったりするものですから、「ここはいけるな」といったリストみたいなものが裏で出回っているのではないかと危惧しています。ですので、そもそも悪質リフォームに引っかからないというのが必要ですし、そういった訪問販売的なものや、様々な勧誘電話に対して自分たちの情報を出さないということがすごく大事です。自分の個人情報をしっかり管理して守るのが重要だと思います。

さらには、「不審者、不審車両を発見したら警察へ」ということで、地域の絆がすごく大事です。地域防犯力が高いところには、なかなか近づきにくい。防犯カメラが地域全体に設置されているとか、死角が少ないとか、地域で「こんにちは」という声かけがされているところは犯罪が起きにくいというのは、一般的にあると思います。そういう地域の絆がすごく大事なかなと思っています。

社会全体で被害に遭わないように守る、犯行に加担させないように守るということが大事だと思います。さらには犯罪が発生してしまうメカニズムそのものに対して、どのように社会全体でアプローチして、我が国が犯罪に強い社会にしていけるか。そのために警察も一生懸命頑張りますけれども、様々な皆様のお力添えをいただきながら頑張っていきたいと思っています。

お時間の関係で詳細な説明は割愛いたしますが、強盗への防犯対策を若干記載しておりますので、参考にいただければと思います。キーポイントは「時間を稼ぐ」ということと「周りに知らせる」ということです。警察や政府も様々な SNS で情報を発信しておりますので、ぜひこういった情報を皆様のみならず、関係の方々にも共有していただければと思います。

御清聴ありがとうございました。

各種対策の詳細

- 警察庁の施策の詳細については、各種 SNS でも配信しています。
- 詳細をご確認いただき、ご家族やお知り合いの方にも共有いただければ幸いです。

警察庁公式 X
(旧Twitter)



警察庁特殊詐欺予防
LINE



政府広報オンライン
「住まいの防犯対策」



「サイバー空間の脅威の現状と JC3 の主な活動」

櫻澤 健一

一般財団法人日本サイバー犯罪対策センター（JC3）業務執行理事

1 はじめに

冒頭の入船亭扇治さんのお話をお聞きして、もう私が話す必要はないのではないかと思います。短い時間で豊富な内容のお話しができるのは嘶家さんならではで、ポイントをしっかり突いていますね。私にはとてもできないので、資料を使ってサイバー犯罪対策のお話をいたします。

サイバーと言うと「分からないからいいや」と言う人が多いのですが、皆さんは立派なサイバー専門家だと思います。なぜなら、今や子供から大人までスマホを使っているスマホは、私が大学でロボット工学等を勉強していた頃の大型コンピューターに近い能力を持っており、それを皆さんはポケットに入れて十分に使いこなしているからです。でもセキュリティはというと別ですね。

かつては専門家だけが扱っていたコンピュータ、サイバーの世界では、それなりの能力を持つ専門家だからこそセキュリティ面の心配なく動いていたのですが、サイバーの世界が私たちの生活や仕事等の非常に近いところに迫ってただけに、今や誰もがサイバー世界のトラブルに巻き込まれてしまう時代になってしまいました。より生活に近いところ、あるいは子供たちにとってのサイバーにおける注意事項についてのお話は後ほど別の方からありますので、私はここでサイバー世界の裏側で何が起きているのかということ、皆さんにお伝えします。

私は、昭和 63 年に警察に入りました。経済職の国家公務員試験を受けていたので経済官庁を回っていましたが、ふらっと立ち寄った警察庁で、ある先輩が「日本は十分豊かになった。これからは安全だとか命といった経済的な価値だけでは測れないものが日本人にとっての一番の価値になる。今の日本では水と安全はただと言われているけれども、そんな時代はもう大国にはない。だったら日本の国民がこれから求めていくであろう安全を提供する側にならないか。一生をかける仕事だぞ」と言われて警察庁に入りました。それ以降、犯罪捜査や国際テロ対策を中心に、安全にかかわる様々な仕事をしてきましたが、サイバーの専門家ではありません。ただ、この 35 年間というのはリアルな世界の脅威が徐々にサイバーの世界に移ってきたという時代でした。テロ対策分野でも、昔のように洞窟の中でオサマ・ビン・ラディンが説教をするなんてことはなく、インターネットで不況をしています。テロの方法もインターネットで教

JC3の組織概要

法人名

✓ 一般財団法人日本サイバー犯罪対策センター
(英語名: Japan Cybercrime Control Center) ※2014年11月13日に業務開始

創設の背景

✓ サイバー空間の脅威が深刻化する中、個別具体的な脅威に対して、事後的に防護措置を講ずる受け身の対応
→サイバー空間全体を俯瞰し、産学官(警察)それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有し、サイバー空間の脅威を特定、軽減及び無効化するための活動に貢献する。
警察庁の有識者会議等を経て、「世界一安全な日本」創造戦略(平成25年12月閣議決定)でも言及

～米国のモデル～NCFTA=National Cyber-Forensics & Training Alliance

米国ではサイバー空間における脅威への対処を目的とした非営利法人としてNCFTAを創設。2002年以降、FBIをはじめとする法執行機関、大学等の学術機関及び200以上の民間企業との連携組織として活動しており、迅速な情報収集、50人以上のアナリストによる情報分析、情報に基づく迅速な捜査等を遂行するためのトレーニングを提供している。



© 2017 JC3 All Rights Reserved.

JC3 JAPAN CYBERCRIME CONTROL CENTER

スライド 1

え、手製爆弾ではなく、マルウェアを相手に送りつけて、相手の能力を止めるのです。ウクライナに対するロシアの戦争の3分の1はサイバー戦です。戦争でさえもサイバーの世界に入っているのです。

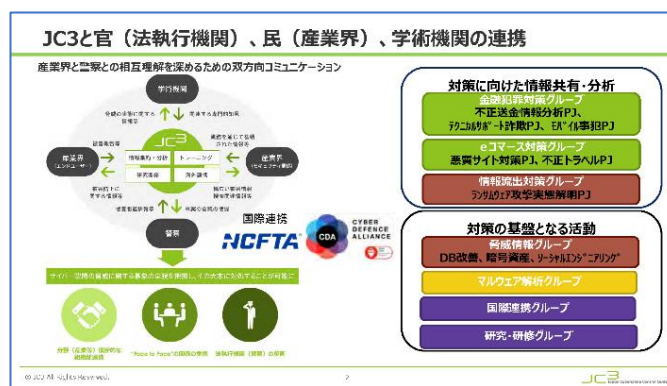
日本サイバー犯罪対策センター（JC3、Japan Cybercrime Control Center）は、スライド1、スライド2

にあるように、官と民と学の人たちが集まって、サイバー空間で起きている犯罪をどうやって知り、犯罪を食い止め、無効化するかについて常に相談できる場所として機能しています。

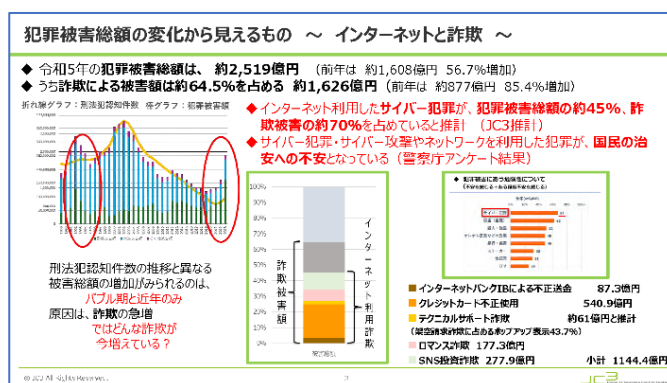
ちょうど10年です。JC3がモデルとした米国のNCFTA（National Cyber-Forensics & Training Alliance）は既に20年以上活動を行っており、その活動に倣って歴史を刻んできました。会員企業は既に110を超えています。会員企業の担当者の方々は、日々サイバー犯罪と戦っている勇者たちです。本日はこうした方々で行っている、金融やeコマース、テクニカルサポート詐欺、ランサムウェア攻撃等をめぐる勉強会の中で報告されているサイバー空間の実態を皆様にお伝えできればと思います。また、サイバー犯罪は国境を超える犯罪ですので、海外の団体とも情報交換していることもあり、その中で知っていた情報もお伝えいたします。

2 サイバー犯罪の実態

さて、まずは現在の犯罪情勢の中で、サイバー犯罪がどのような位置づけになるかについてお伝えします。スライド3の左側の折れ線グラフは、警察が犯罪、治安状況を表すのに示す刑法犯認知件数ですが、2002年をピークにどんどん減ってきて、昨年は73万7,679件とかなり少なくなりました。一方で、この数年急激に増加している棒グラフは、財産犯の被害総額で、認知件数が増えていないのに被害額が増えているのは、1件当たりの被害額が相当増えているためです。かつては刑法犯の件数、被害額とも7割以上が窃盗犯でしたが、令和5年の被害額の3分の2は詐欺です（3月に令和6年の犯罪統計が発表され、4分の3が詐欺による被害であることが明らかとなった）。真ん中の棒グラフは、その詳細ですが、インターネットを利用した詐欺が、詐欺の6割以上、全体の半分近くを占めていることが分かります。犯罪の中で詐欺が私たちの財産を狙う一番怖い存在になっているのです。



スライド2



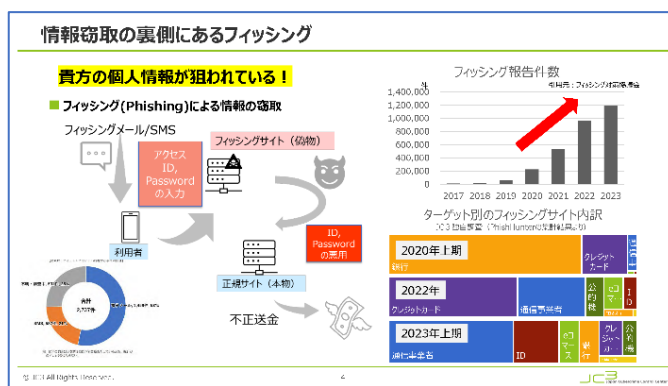
スライド3

まずフィッシングについて説明します。フィッシングは、スライド4にあるように、犯人側が作成した偽サイトにメールやSNSで誘導し、個人情報、特に銀行やクレジットカード、アカウント情報等を入力させて奪います。これらの情報を悪用し、インターネットバンキングのサイトやアプリを利用し、被害者の口座にある預貯金を自分たちが用意した銀行口座に送金してしまうのです。その被害額はスライド5で示したように、2024年には87億円を超えました。また、盗んだクレジットカード情報を悪用し、ECサイトで被害者になりすまして買い物をし、年間500億円以上の被害が出ています。

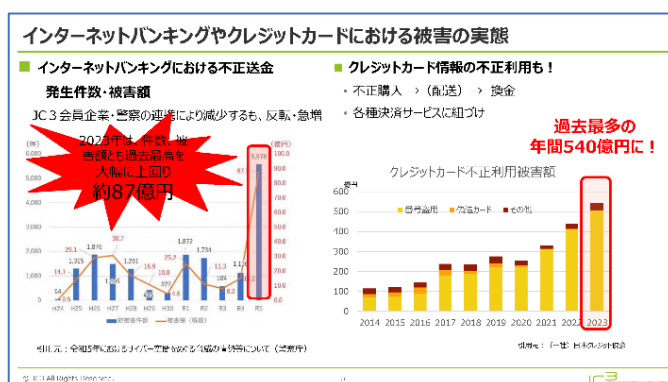
具体的なサイトを見てみましょう。かつてはフィッシングサイトの作りも荒かったのですが、警察からは「不審なサイトには入力しないように」との注意喚起をしていましたが、スライド6に示したように、今はいずれも本物そっくりで、これらのサイトを示された段階で不審を抱く人はほぼいないでしょう。銀行、証券、クレジットカード、支払い代行、消費者金融といった金融関係サイトがとて

多く、Amazon等のeコマースサイト、鉄道チケットサイト、宿泊仲介サイト等のほか、NHKや農協、ETCといった身近で皆さんが契約しているような機関のサイトや最近はやりのサブスクリプションの動画サイトもあります。いずれもクレジットカードでの支払いを前提としているサービスなので、クレジットカード情報を求められても自然なこととして入力してしまうものですが、そこに誘導するメールやメッセージには、「一時的な利用制限がかかっている」、「支払いが滞っているので間もなくサービスを停止する」、「セキュリティ保護のため本人確認が必要」、「(本人が記憶にない) ××万円以上の利用が行われたので、不正使用でないかについて確認したい」というような脅しともいえる文言が書かれているために、IDやパスワード、クレジットカード情報等を入力させられてしまうのです。

銀行サイトでの送金やクレジットカード決済を求める際には、多要素認証等により本人確認を



スライド4



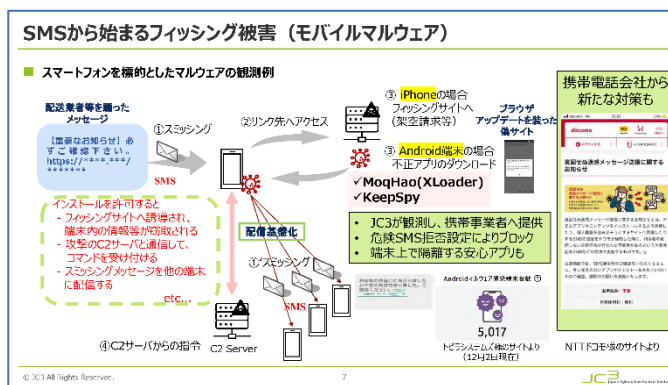
スライド5



スライド6

やっていますが、例えばワンタイムパスワードもリアルタイムフィッシングという手口では簡単にすり抜けられてしまいます。犯罪者は、銀行が顧客に示す可能性のある 30 以上もの画面をあらかじめ用意し、被害者の入力をリアルタイムに観測することで、銀行が電話メッセージで送ったワンタイムパスワードも、その入力を求める画面を被害者に示し、入力させてしまうのです。生年月日、秘密の質問、母親の旧姓、メール認証等、どのようなことをやっても対応できるように、犯罪者は準備しています。

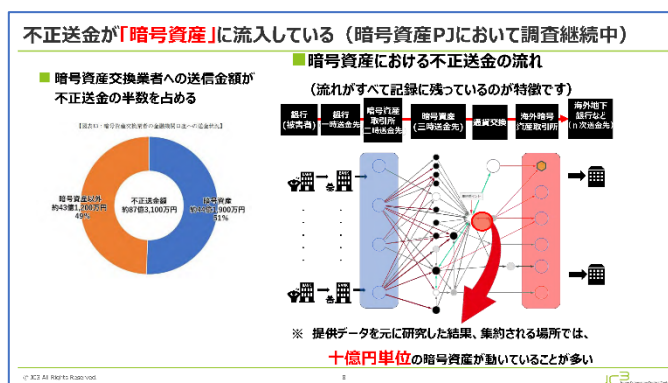
最近最も多い手口は、スライド7にあるような SMS によるメッセージを使ったスミッシングです。「重要なお知らせ。〇〇銀行」、「ご不在のため、お荷物を持ち帰りました」というようなものですが、ボタンは小さく、見にくいこともあって、簡単に押してしまう可能性が高く、フィッシングサイトに連れていかれる人が相当数います。フィッシングサイトに連れていかれるだけでなく、Android 端末の場合はそこで Keepsy とか Moqhao/XLoader という不正アプリをダウンロードしてしまうことがあります。感染した携帯電話は、犯罪者が持つ



スライド 7

サーバと通信を始め、犯罪者の指令で約 200 件の電話番号に向けてメッセージを発信してしまうのです。この手口は悪質で、バックグラウンド、つまり画面には見えないところで受信や発信が行われ、履歴も表示されないような形になっており、月額使用料が急増してはじめて気づく人も多いようです。JC3 ではこの通信を観測し、携帯電話事業者と連携して、これらのメッセージを止めています。この措置は通信の秘密にもかかわるものかもしれませんが、明らかな犯罪のための通信を止めるということで実現にこぎつけました。なお、昨年 12 月では約 5,000 の携帯電話が感染していたようです。

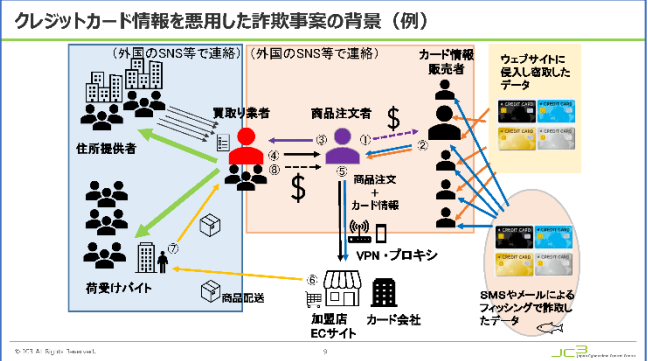
スライド8にあるように、不正に取得された資産のうち半分ぐらいは暗号資産に換金されて海外に送金され、本人確認等も十分にされていないところで現金化されているようです。どの地域から攻撃が仕掛けられているのかはわかりませんが、例えば中国語で書かれたテレグラムのオープンチャットには、日本の銀行口座やクレジットカードを販売するコミュニティが形成されており、何とフィッシングのやり方を教えるサイト、フィッシングサイトを作ってくれるサイトまであるのです。



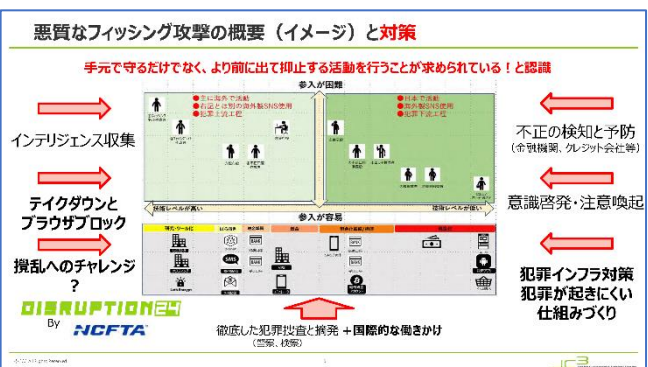
スライド 8

スライド9でクレジットカードの不正使用も組織的に行われており、悪質なフィッシング攻撃の概要をスライド10でまとめました。今後、不正の検知や注意喚起等で守るだけでは、こうした攻撃を防ぐことはできないと考えており、犯人側に電話をして彼らの手口を明らかにしたり、犯人側が作っているフィッシングサイトをテイクダウンする、という積極的な防御を行っていく必要があると考えます。

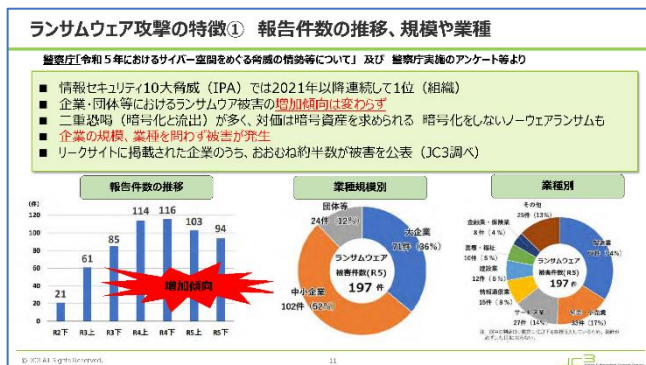
ランサムウェア攻撃（スライド11）、テクニカルサポート詐欺（突然PCの画面が大きなブザー音を出しながらフリーズし、サポートセンターに電話するように促すことから始まる詐欺、スライド12、13）等についても注意が必要です。JC3のサイトには注意喚起とともに、犯人側の偽のサポートセンターに電話をかけるとどんなことが起きるのかを動画で載せています（スライド14）。参考にしてください。



スライド9



スライド10



スライド11

テクニカルサポート詐欺 ～ 誰もが巻き込まれる恐れのある犯罪 ～

パソコンを使っている途中に、突然こんな画面とともに警告メッセージが大音量で流れたら、あなたは？ あわてて○○○○○○サポートに電話しますか？

多くが IP 電話 050-????-???? ですが、海外の電話番号 0101-???????? も

海外でも頻発しており、国際的な協力体制が急務！

- 「サポート詐欺」という犯罪があることを伝えてほしい。
- サポート詐欺に限らずパソコンを使って困ったことが起きたら、親しい身の回りの人や警察に相談し、絶対に画面の電話番号に電話しないことと伝えてほしい。
- コンビニなどで高額な電子マネーを買おうとしている人が居たら、声をかけてあげてほしい。

※ 参考文献 サイバークリッドジャーナルVol.15 特集1 突然の警告!? サポート詐欺の謎に迫る！
https://www.lac.co.jp/lacwatch/pdf/20230302_cgjournal_vol15.pdf

スライド12

テクニカルサポート詐欺の遭遇経路（誰でも感染する可能性がある）

様々なオンライン広告をクリックすることで遭遇

ルートプランナー

＜サポート詐欺サイトの消し方＞

- 全画面表示を解除するためにESCキーを押す。長押しも有効
- Ctrl+Del+Altキーを押し、「タスクマネージャー」を起動させてください。
- サポート詐欺サイトが表示されているブラウザ（Edge, Firefox, Chromeなど）を選び、「タスクの終了」をクリックすればブラウザが終了します。
- どうしてもならないときは、電源を切る

スライド13

電話をかけるとうなるかを知って、決して「電話をかけない」ことを広げましょう。

<https://www.jc3.or.jp/threats/examples/article-570.html>

サイバー警察局便り

サポート詐欺被害の発生！脅迫に抵抗し、絶対に画面の電話番号に電話しないことと伝えてほしい。

「サポート詐欺」という犯罪があることを伝えてほしい。

サポート詐欺に限らずパソコンを使って困ったことが起きたら、親しい身の回りの人や警察に相談し、絶対に画面の電話番号に電話しないことと伝えてほしい。

コンビニなどで高額な電子マネーを買おうとしている人が居たら、声をかけてあげてほしい。

※ 参考文献 サイバークリッドジャーナルVol.15 特集1 突然の警告!? サポート詐欺の謎に迫る！
https://www.lac.co.jp/lacwatch/pdf/20230302_cgjournal_vol15.pdf

スライド14

3 サイバー犯罪対策における課題（スライド 15～18）

最後に、サイバー犯罪への対策として最も重要なことは、いざというときに役に立つ仲間を日頃からつくりましょうということです。サイバーの知識を高めることも重要ですが、セキュリティをよく知っている企業、携帯電話事業者、そして警察も仲間にするすることで、相談や情報交換をすることで対策をするということが、サイバーの脅威に対抗するには必要だと思います。

私ども JC3 としては、これからも皆様に様々な事例や資料を提供していきたいと思えます。日本よりも先にいろいろ起きる海外の情報も必要ですね。もちろん、JC3 のサイトを除いていただければ様々な情報を入手できるように準備していますので、皆さん、ご利用いただければと思います。

今後の課題① 先進技術の社会実装と安全安心の両立

- ✓ サイバー分野における新たな先進技術の社会実装には、大きな利益とともに一定のリスクが存在している。⇐ 予想されるリスクに対して必要十分な規制が実施されるためには、より詳細な実態に関する情報が政府に集約される必要あり

■例えば、、、生成AIによって犯罪も変わる？

ChatGPTが犯罪行為の手助けをしていることをEuropolが警告！

(2023.4.20公表)

「ChatGPTの公開からわずか数週間後には具体的な犯罪行為が確認されています」 犯罪に活用！

「ChatGPTは、犯罪の準備プロセスを加速させ、侵入方法やテロ活動、サイバー犯罪、児童虐待等、広範囲な犯罪について学ぶことができます」 犯罪の手法や新しいツールを教える！

「技術的知識が乏しい潜在的な犯罪者にとっては非常に貴重なリソースで、同時に、より高度な犯罪者は、洗練されたサイバー犯罪の手法をさらに洗練させ、自動化することができます」 手法を高度化！

「会話型チャットボットと非構造的リアルタイムディープフェイクなどの合成メディアを生成できるシステムを組み合わせたAIシステムが、今後の犯罪手法となる可能性があります」 AIが巧妙に人をだます！



スライド 15

今後の課題② 公共空間におけるサイバー犯罪の予防には何が必要か

- ✓ 子供からお年寄りまで、知識や技術がある人もない人も、都会の人も田舎の人も、生活もビジネスも、もはやサイバーの世界と関係なしにはられない。
⇐ 今後さらに拡大するサイバーの世界の中で安全安心を確保するには、個人のリテラシーの向上も大切なが、権限・能力があり信頼される組織が対応することが大切

◆情報とリソースを持った民間組織の役割

◆幅広い情報把握権限・能力と国際連携が可能な行政機関、法執行機関の役割

自衛隊を含めた中央官庁、警察、セキュリティ事業者、システム提供事業者、通信事業者、自治体、

勤務先、学校、等が期待に応える能力を備え、積極的に行動することが必要

◆誰にどのような権限を持たせるべきか

【国家安全保障戦略より】

・サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用

・政府機関等のシステムの導入から廃棄までのライフサイクルを通じた防衛の強化、

政府内外の人材の育成・活用促進等

・能動的サイバー防御の導入に期待

スライド 16

今後の課題③ サイバー犯罪対策における官民学連携の意義

- ✓ 攻撃者、犯罪者は、互いの専門性を共有し、合法、違法様々な手段、方法を講じている。

⇐ 現実の脅威に対抗することは、一企業、一組織単独では困難

◆情報とリソースの共有が重要

業界を超えて、官民学の隔いを越えて

攻撃の主体、動向、対象、手法、犯罪インフラ等のリアルな実態を把握

◆＜企業＞と＜法執行機関＞等との連携の「場」の提供（JC3）

＜定期的＋随時＞の情報共有等の場の設定

→ 業界を超えた関係者間の相互理解の醸成

育成へ立ち向かう目的意識を共有する関係者による信頼関係、同志的関係の構築

関係者が活用できるデータ、情報の収集、整理

◆攻撃者のエコシステムへの対抗

社会全体での、攻撃しづらい環境・システムの構築

スライド 17

【最後に】今後の課題 企業に何が求められるのか

- ◆自社（従業員）が標的となる可能性についての意識啓発が、経営層を含め、企業内の各層で十分に行われ、必要な対策が取られることが前提。

- ◆被害が蔓延しやすいサイバー犯罪や攻撃（サイバー犯罪や国家支援型のサイバー攻撃への対処）については、より多くの情報に接する民間企業（被害企業を含む。）側からの情報提供・政府への協力が、悪悪ある攻撃への対抗手段とする上で必須。
⇐ 営業庁Webサイトに、都道府県警察の通報・相談窓口を統一化

- ◆企業側が政府へ情報提供や被害の公表を行う上での、法的リスクやレputationリスクを下げるための産業界全体での取組が必要。

- ◆広義のサイバー領域において、企業本体及びそのビジネスを守るために必要な「積極的な投資」を求めたい。



スライド 18

質疑応答

○中村 日興技科の中村と申します。ただいまの JC3 のお話を聞いている中で、官、いわゆる警察とか自衛隊とかの組織がそれぞれサイバー世界に対応するための組織を持っていると思うのですが、そういうところと JC3 さんの関わり合いはどうなっているのか、お伺いできる範囲でお願いしたいのですが。

○櫻澤 ありがとうございます。JC3 は一般財団法人ですが、都道府県警察や警察庁から十数名のサイバー捜査官を派遣いただいていますので、皆さんがサイバー犯罪のことについて何か相談したいときに、常に答えられるメンバーがいます。一方で、防衛省・自衛隊とは組織的なお付き

合いはありませんが、私自身が長く安全保障分野でも仕事をしてきましたので、何かあればそういう方々にもご相談しています。

JC3 のグループやプロジェクトのミーティングには、会員企業のほか全国の警察の方々にも出ていただいております、気軽に「おいおい」と声をかけられるような近い関係で仕事をしています。

○河井 下妻市役所の河井と申します。先ほどの櫻澤さんのお話で、ネット犯罪の中で、特に私などは「IDとパスワードを入れてください」とよくメールとかが来るので、それは危ないなと思って入れないのですけれども、アプリの更新などで、アプリを開いたりすると時々IDとパスワードを入れてくれと。これは今のところ信用して入れているのですけれども、こういうのが駄目な場合もあるのでしょうか。

○櫻澤 極めて危ないです。アプリの更新についての連絡が来たときにも、そのメールに書かれているリンクから行くのは絶対にやめてください。必ず、正規のアプリやサイトからアクセスしてください。メール等のリンクからですと、多くは偽サイトに入ってしまう。犯人側は常に被害者を騙して、罠を仕掛けているのです。

○樋口 弁護士をしております樋口といいます。JC3 のほうにも質問しようと思ったのですけれども、この犯罪グループは国際化も進んでいるし、日本国内においても犯罪グループがいろいろな連携を取っていると承知しております。そういう中で対抗措置として、裁判も含めてですけれども、最近、短期任用公務員という形で民間との交流等もされているやに報道で承知しております。

私が反社、犯罪グループであれば、潜入捜査の逆で、潜入をさせると。つい最近は、裁判官の身分を持った人が、お金を前に目がくらんで、接触情報等を使ってインサイダー取引等で検挙されるとか、そういうのがありますよね。そういったことについて、国として、あるいはいろいろな団体として、防衛措置はどのように取られているのかが一番関心がありますので、よろしくお願いします。以上です。

○櫻澤 私ども JC3 にも様々な企業が会員になりたいとの申し出をいただいておりますが、その際には、過去にその企業や取締役等がどのようなものであったのかについて、それなりにオープンソースの調査をします。私どもは参加する各企業と「情報を外に漏らさない」という秘密保持契約を必ず結びますが、そもそもその前提となる信用性があるかどうかをチェックするようにしています。犯罪者は常にこちら側の行動を綿密に調査し、その隙間を狙っていますので、こちら側もきちんとした対抗策を取る必要があります。

私もかつて公務員でしたので、公務部門が法令に基いて様々な努力をされていると承知しています。特定秘密保護法をはじめ、公務における保全法制もこの数年で相当強化されました。海外からまだ弱いと指摘されることもありますので、さらに強化していただきたいと期待しています。

第3部 市民安全の心・技・体 その1

子どもの SNS 利用の現状 ～大人が知っておきたいこと、できることとは～

大久保 貴世
一般財団法人インターネット協会研究員

内容

1. 6つの盲点
2. 大人の皆さまへ期待すること
3. クイズで覚える「インターネットルール&マナー検定」
4. 大人も子どもも知っておきたい「その時の場面集」



はじめて SNS を使う時

その SNS、子どもに使わせて大丈夫でしょうか？

利用できる年齢なのか。投稿する方法だけでなく、削除する方法もわかっているのか。

アカウントの管理はできているか。質問やトラブルの問い合わせ方法を知っているか。など。

はじめて使う時こそ、面倒くさがらずに知ってほしい、**6つの「盲点」**についてお話しします。

盲点1 アカウント情報を記録しておく

1つ目、典型的な相談を紹介します。

14歳女子中学生。

X を友達限定ではじめ、プロフィールに自撮り写真をあげた。写真は加工して女子力を上げた奇跡の一枚。“いいね”が15件もついた。しかし、「別人なのでは？」とか「性格の方を磨いたら？」というコメントもある。写真を消そうとログアウトしたら、再度ログインができなくなった。登録時のメールアドレスとパスワードは忘れています。写真が消えないままだと辛いです。

この相談でわかることは何か。

『SNS 登録時のパスワード情報は、メモしておくこと』です。

スマホでログイン状態のままずっと使っていると、再度ログインを求められた際に、「あれ？パスワードって何だっけ」となります。アカウント名、メールアドレス、パスワードの3つは、記憶に頼らずにノート等にメモしておくといよいでしょう。

そして、相談者はログアウトすれば削除できる、と勘違いをしています。自分の SNS を操作するためには、ログイン状態にしないなりません。

参考として、登録時のメールアドレスについて、携帯電話を機種変更する場合も想定すると、携帯電話会社のメールアドレスではなく、「フリーメールアドレス」の利用をおすすめします。

一方、他にもわかることは何か。

『SNSに載せたものは、見られている』ということ、です。

友達限定であっても、プロフィールやプロフィール写真は公開の状態です。プロフィールに学校名や好きなタレントを書いたりする利用者を見かけますが、この部分は公開情報なのです。

さらに、わかってほしいことがあります。

『悪口を言う人がいけないのであって、悪口を言われる人は悪くはない』ということ、です。

相談者は自分の好きな写真だからこそプロフィール写真にしました。自信をもって毅然とした態度でいればよいのではと思います。何年か経って過去の思い出写真と思える日まで、時間が解決してくれるものと考えてほしいです。

盲点2 削除方法を知っておく

2つ目、こちらも典型的な事例を紹介します。

11歳男子小学生。

同級生の顔がはっきり分かる動画をYouTubeにアップした。動画のタイトルに、中傷する言葉をつけている。学校も把握しており、同級生には謝罪をしたが、削除する方法がわからない。

この相談でわかることは何か。

『SNSにあげた情報の削除方法を、あらかじめ知っておくこと』です。

SNSそれぞれ方法に違いがあります。

YouTubeの場合は、以下の図のように、YouTube Studio ページからステップを踏むことで、削除できます。方法を知るだけでなく、削除の練習をして実際に削除できたかどうかまで確認しておく、なお良いでしょう。間違って投稿したり、公開設定を間違ったりするなど、うっかりミスをした際に、方法を知っていれば冷静に対応することができます。

ところで、相談者は11歳。YouTubeの利用規約の年齢に関する要件に、こう書かれています。

「本サービスを利用するには、13歳以上である必要があります。

投稿に責任の持てる年齢に達するまでは使ってほしくないという目的です。

動画の内容はいじめの動画なので、不適切な投稿として利用規約違反となる可能性もあります。YouTubeを運営するGoogle社へ通報することにより、不適切動画として削除す



図：YouTube動画を削除するステップ

ると判断された場合は、削除されることとなりますが、どのくらいの日数がかかるのかはわかりません。公開されている間に、その動画は多くの人に見られる状態になってしまいます。自分で投稿した動画は自分で削除できますので、早く削除するようにしましょう。

動画を削除すれば、同級生に謝罪の言葉だけでなく、対処した誠意も伝えることができます。利用可能な年齢になって使い始めた時は、誰に見られても良い、みんなが楽しめるような動画を投稿するようにしましょう。もちろん個人が特定できる情報には注意することを忘れずにしてください。

盲点3 写真の撮影場所の位置情報がある

3つめの相談事例。

女子中学生。

ネットで知り合った人とメールアドレスを交換して写真を送った。すると、住所が特定できたから、住所や電話番号をネットにさらすと言われた。すごく怖い。自分の居場所をわかっているような言い方をされた。

この相談でわかることは何か。

『落とし穴は写真にあること』です。

スマートフォンで撮影した写真は、緯度経度情報から撮影場所が特定されてしまうことがあります。購入時のカメラの位置情報の初期設定は「オン」になっています。この設定を「オフ」にしておけば位置情報はつきません。もし、自宅で撮影した写真をインターネットに不用意に公開すると、緯度経度情報からおおよその自宅が特定されてしまうこともあります。

なお、多くの SNS (LINE、X 等) では、位置情報付きの写真を投稿した場合でも、投稿した時点で、写真の位置情報を削除してくれる設定にしてくれている場合があります。ですが、全ての SNS ではありませんし、iPhone の AirDrop のような端末同士のやりとりや、メールでやりとりする場合には、位置情報は削除されません。

盲点4 SNS から離れて様子を見る

4つ目は、最近よくある相談から。

LINE グループで、どうでもいいこと、悪口や自慢話にうんざりしている。

既読無視をすると、何でも何も言わないの？と言われて、疲れてしまった。

グループから外されたり、逆にグループから外れることを禁止されたり、困っている。

この相談でわかることは何か。

『SNS から離れてみること』です。

LINE などの SNS の中でのことでも、問題は人間関係だったり学校生活でのことです。普段の学校での支障が何もないのであれば、グループの人たちと一時的に距離をおいて、このまま様子を見るというのが1つの方法です。

もし、明らかに誰かを傷つけているとしたら、それはいじめにつながるかもしれませんので、学校の先生やスクールカウンセラーへ相談することをおすすめします。

非公開のグループ内であっても、悪口が一度グループの外へ公開されれば、より広範囲に拡散

し、より多くの人が被害者にも加害者にもなってしまいう可能性があります。 相手を思いやりみんなルールを守って、会話を楽しむための場所として活用してください。

盲点 5 性的な画像を送れと言われるのは犯罪です

5つ目は、このところ増えている相談から。

女子高校生。

SNS で知り合った人に性的な画像が欲しいと言われ、送ってしまった。顔も映っている。その後、動画が欲しいと言われたが嫌だったので断った。すると、前に送った写真を拡散すると脅してきて、本当に拡散されてしまったかもしれない。実際にその画像がインターネット上に載せられているところは見えない。

この相談でわかることは何か。

『犯罪だということを、いち早く知ること』です。

18 歳未満の児童の性的な画像は「児童ポルノ」にあたり、性的な画像や映像を送信することは、「児童ポルノ禁止法」に違反します。また、相手の行為についてはその写真を性的好奇心で保持していることも法律違反になります。

さらに、「刑法及び刑事訴訟法の一部を改正する法律」に、裸の写真を送るよう要求する行為の禁止が新設、2023 年 7 月 13 日施行されました。

16 歳未満の者に対する面会要求等の罪（新設）

性交等をする姿、性的な部位を露出した姿などの写真や動画を撮影して送るよう要求すること

「1 年以下の懲役又は 50 万円以下の罰金」

（※）相手が 13 歳以上 16 歳未満の子どもであるときは、行為者が 5 歳以上年長である場合

出典:法務省 https://www.moj.go.jp/keiji1/keiji12_00200.html

このことから、今できることとして、**自宅を管轄する警察へ相談することをすすめます。**

警察への相談の際には、まず、把握している状況を時系列で思い出せる限りのことをメモとして書き出し、その証拠となるもの（相手の SNS アカウント等）が残っているのであれば、消さずにスクリーンショット等も使って保存して伝えるようにとアドバイスします。

一方、もしも、インターネット上などに掲載されているのを見つけたら、適切な対応を考えることになりますので、その時には再度相談してほしいとお話しします。

盲点 6 SNS の問い合わせ方法を知ること

最後の 6 つ目は、根本的な話です。

『ほとんどの SNS には問い合わせのための電話窓口がないこと』です。

問い合わせフォーム、ヘルプページ、Q&A コミュニティで自己解決する方法しかありません。自分ではどうにも出来ない場合には、インターネットに詳しい知人を探して、スマホの実機を見せて対処方法を教えてもらうのが、てっとり早い方法です。

また、SNS を運営する会社の本社がアメリカ等の外国であることが多く、英語で書かれているページがありますので、英語の先生を頼るか、ネットの翻訳ページを利用すると良いでしょう。

SNS の利用規約の一番下には、「準拠法」という項目があり、例えばアメリカの各州、シンガポール等、どの国や州の法律に準拠するかが書かれていますので、ここまで見てほしいことです。

使い始めのうちに「盲点」を知っておくと安心だし、SNS を活用するための自信につながるものと思います。

大人の皆さまへ期待すること

子どもが、ネットに詳しいのは当然です。

わからないアプリは、以下のように子どもに教えてもらいましょう。優越感で話はじめるでしよう。



子どもとの対話、5つの質問

1. 友だちはインターネットで何をしているの？
2. あなたの最近のいちばんおもしろいサイトやアプリは？
3. あなたのお気に入りのサイトを見せてくれる？
4. ネットいじめのことは知っている？いじめにあったり、目撃したりしたことはある？
5. ネットでおかしなもの、悲しい気持ちになるもの、怖いものや嫌な気分になるものを見たことがある？

出典：ノートン「家族のためのインターネットセキュリティガイド」より

子どもと会話する時の、○と×

× いつまでスマホ触っているの？

○ とても楽しそう、やめられない気持ちはわかる。

○ あなたの健康が心配。睡眠をとらなきゃね。

○ あなたは、どういうルールだったら守れるの？

○ 守れなかった場合、どうしようか？

○ ルールを守ったら、見直しをしましょうね。

決めたルールは、貼っておくと良い。

参考ページ

インターネットの基本知識、具体的知識

インターネットのトラブルの原因は、インターネットのルールとマナーを無視した使い方をしていたり、それぞれのSNSの仕組み（メッセージの公開/非公開、注意事項、削除方法など）をよく知らないまま、とりあえず使ってしまうことにあります。知ってほしい参考知識を紹介します。

（１）基本知識

インターネット協会「インターネットルール＆マナー検定」

<https://rm.iajapan.org/>

「自分の身は自分で守る」「相手のことを思いやる」「声や表情は伝わらない」「セキュリティ」「関連法規」など、安心して利用するために、身につけることの知識習得を確かめるために、クイズ形式で覚えてもらう検定です。

受検方法はウェブで、毎日24時間実施。受験料は無料。何度でも受検ができます。

合格証、スコア認定証(大人版)を希望者に有料で発行。

インターネット利用アドバイザー試験の受験もできます。

インターネットルール＆マナー検定

<https://rm.iajapan.org/>

インターネット上のルールやマナーの知識をテストし、正解および解説を見ることにより知識のレベルアップを行えるようにする検定です。受験料は**無料**。

ビジネス版 50問  就活を控えた学生や企業のインターネット利用者向けです。	こどもばん 30問  生徒（中学生・高校生）、保護者、教員向けです。	こどもばん 30問  児童（小学4年・6年生）向け「ふりがな」付きです。	大人版 100問  大人一歩/インターネット利用アドバイザーをめざす人向けです。
---	--	---	---

（２）具体的知識

インターネット協会「インターネットを利用する際に知っておきたい『その時の場面集』

<https://www.iajapan.org/bamen/>

幅広い年齢層に利用されている主要なSNSについて、それぞれの利用方法や注意方法、トラブルに遭った際の問い合わせ方法、有害情報を見つけた場合の連絡方法、パスワードを忘れた場合など、必要と思われる場面を集めて具体的に説明したマニュアルです。

スマートフォン基本設定編、フィルタリング編もあります。

知っておきたい『その時の場面集』

<https://www.iajapan.org/bamen/>

1.SNS編 Instagram TikTok LINE X(Twitter) Facebook YouTube Google Ameba GREE Mobage ニコニコ動画	2.スマートフォン 基本設定編 Android iPhone 3.フィルタリング編 スマートフォン、タブレット、 パソコン、ゲーム機、 音楽プレイヤー、 ルーター
--	--

★例：Instagram 編 「16. 他人の投稿を削除したい時」より

その時の場面集 Instagram 編

16 ・他人の投稿を削除したい時

ルールや利用規約に違反する投稿に対して、違反報告をすることができます。

何らかの理由で他人の投稿を削除したい場合は、その投稿者本人と面識がある場合は、まずは直接その本人にその理由と共に削除の依頼をしてみましょう。面識のない人にダイレクトメッセージなどで直接連絡を取ることもできますが、場合によっては別のトラブルにつながる恐れもありますので、未成年者は保護者に相談してからにするなど、慎重に対応しましょう。

もし、その投稿内容が Instagram のガイドラインに明らかに反している場合（自分になりすましている、自分の個人情報を勝手に掲載している、嫌がらせ・誹謗中傷を受けている、など）は Web サイトの問い合わせフォーム、もしくは相手の投稿を閲覧する画面から Instagram へ報告が可能です。ガイドラインに反していることが認められれば、何らかの対応を行ってもらえる可能性があります。



報告画面

コミュニティガイドラインへの違反を報告
<https://help.instagram.com/contact/383679321740945>

★例：YouTube 編 「18. 不適切なコンテンツを見たくない時」より

その時の場面集 YouTube 編

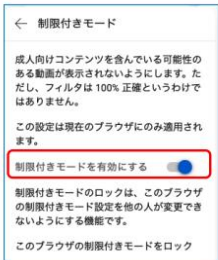
18 ・不適切なコンテンツを見たくない時

制限付きモードを利用して、未成年者に相応しくないコンテンツを除外しましょう。

制限付きモードとは、YouTube のオプション設定です。成人向けコンテンツを含む可能性のある動画が表示されないようにします。ただし、フィルタは 100% 正確というわけではありません。

動画のタイトル、説明、コミュニティガイドラインによる審査、年齢制限などのさまざまな情報を基に、成人向けの可能性があるコンテンツを特定し除外しています。

なお、制限付きモードはブラウザまたはデバイスごとに適用されるため、使用する各ブラウザで有効にしておく必要があります。自分が見たくない、また自分のデバイスを使用する他の人に見せたくない動画が表示されることを防ぎます。



制限付きモードを、オンまたはオフにする

1. アカウントにログインします。
2. 右上にあるプロフィール写真 をクリックします。
3. 画面の中の【制限付きモード】をクリックします。
 (モバイルの場合は、[設定] から[全般]をタップします)
4. 【制限付きモードを有効にする】をクリックしてオンとオフを切り替えます。

YouTube で制限付きモードをオンまたはオフにする
<https://support.google.com/youtube/answer/174084>

以上、今日のお話が参考になりましたら、嬉しいです。

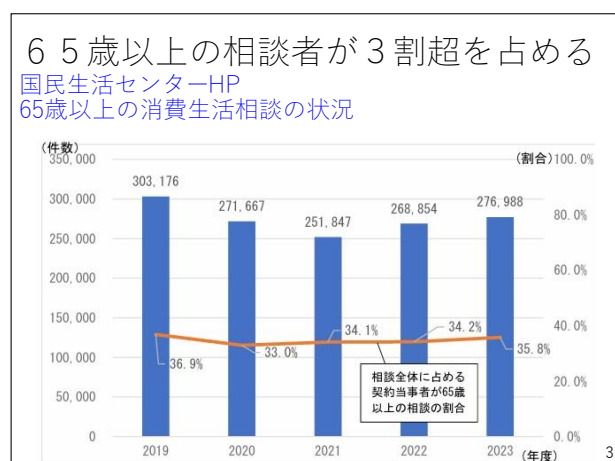
第3部 市民安全の心・技・体 その2

高齢者がネット取引で騙されないために

木村 嘉子

消費生活コンサルタント

全国の消費生活センターの相談をまとめている国民生活センターの報告によりますと、全国の消費生活センターの年間相談件数は約 90 万件で、65 歳以上の相談者が 3 割を超えています。高齢者の割合はどんどん増えていくと思われます。



トラブルのトップはインターネット通販です。2 番目の定期購入もインターネット通販です。

私は長年、消費生活センターで相談員をしています。昔は「消防署のほうから来ました」と言ってお火器を売るといふ相談がありましたが、今考えてみると本物の消火器を売っていますし、ちょっと高いぐらいで、かわいいものだったと思います。今は多くの相談が詐欺で、毎日相談を受けていると後ろに匿・流

の人たちが浮かんできます。

私は本日、5 つの事例と対策を御紹介します。これらの事例は汎用性のないようにしております。

トップは、「商品が届かないサイト」

インターネット通販で、長年欲しかったレコードを見つけて購入しました。ところが、クレジットカード番号を入れても決済ができず、販売会社に連絡したところ、「口座振込となります」といふメールがあり、指定された個人口座に振込をしました。「入金確認いたしました。発送準備に入ります」とメールが届いたのですが、商品が届きませんでした。メールをしても返信はありません。サイトに記載された電話番号に電話したところ、全く違う会社でした。振り込め詐欺ですので、まず返金は不可能です。

クリスマスプレゼントで子供にゲーム機を買おうと思ったところ、メーカーでは売切れだったゲーム機が〇〇サイトで売っていました。ちょっと高い程度のため購入したが届きませんでした、などの悲しいご相談がたくさん入ります。公式サイトに売っていないものを売っていたら疑っていただきたいと思います。

「お金は返ってこないのですか」と皆さんおっしゃるのですが、事実上被害回復は困難です。「振り込め詐欺救済法」といふ法律で、振り込んだ口座にお金が残っていた場合は、預金保険機

構というホームページに公告がされて、期限内に金融機関に申し出ること、全額ではないですが被害者で案分することができますが、出し子が送金確認の時点でお金を下ろしていますので、口座は空っぽです。

サイトで何かを買おうと思ったときには、事前に事業者の住所と電話番号の確認をすることが大切です。地図アプリで販売会社の場所を確認したり、事前に非通知「184」という番号をつけると、自分の電話番号を相手に知らせずに電話をすることができますので、電話をしてみることも一法と思います。

私は NACS という消費者団体に所属しており、「危ないサイトにご注意」という疑似体験サイトをつくりましたので、QR コードをお示ししておきました。どういう点に注意したら騙されないのか、ご自身のスマホやタブレット、パソコンなどで試してみると面白いので、後で試していただければと思います。

疑似体験サイトの紹介（安心して疑似体験可能）



8

2 番目は「詐欺的な定期購入」

お試しと思って商品を買ったら翌月も届いたというトラブルです。Instagramで「お試し 500 円」「サンプル」「縛りなし」という広告を見て化粧品を買って、コンビニでお支払いをしました。ところが、10 日後に同じものが今度は 2 本届いて、1 万 5,000 円を請求されました。

「私はお試ししか頼んでいません」と電話をしましたが、「解約する場合は次回配達の前までに申し出る必要があります」と言われます。よく見ると小さな字でそのように書いてありました。7 日前までに申し出る場合、1 回目が届いた直後に申し出ないと、2 回目が自動的に届くことになります。

また「500 円」という文字は大きく書いてあるのですが、500 円で申し込むと、すぐ個人情報を入れる画面になります。ひどい場合には、単発の A コースを申し込んだはずなのに、「今なら〇〇でお得」というボタンを押すと長期間の B コースに変わっていることがあります。

スマホで「500 円」の表記と比べてこんなに小さい字で、「定期コースについて」と書いてあります。分からないように仕組んでありますので要注意というか、やめてほしいと思います。

「特定商取引法」の改正法が 2022 年に施行され、例えば最終確認画面にあれや、これや、それを書け、書いてなかったら取消しもできる、と厳しくなったのですが、結局、最終確認画面に小さな字で書いてあったとしても、よく読めないのが、読み飛ばしてボタン

②詐欺的な定期購入 国民生活センターHPより



10

を押してしまうと B コースを契約してしまいます。ダークパターンといいますけど、これらに巧妙にだまされてしまうために、トラブルは減っていません。

最終確認画面に、コースを確認することや、スクリーンショットで画面を保存しておくことは必要ですが、申し込む前にやめるとのことしか、今のところないと思っています。

3 番目は「サポート詐欺」

先ほど櫻澤様に「ビービービー」と鳴る画面を見せていただきましたが、まさにこのご相談です。人知れず支払っている方がたくさんいらっしゃると思います。

昔は「ちょっとエッチな画面」にアクセスして代金を請求されましたが、今は普通にインターネットを閲覧していて、いきなり「ビービービー」と警告音が鳴ります。電話をすると、日本語がたどたどしい人が出て、サポートセンターなどで使う遠隔操作ソフトを入れさせられます。双方で同じ画面を見ながら、ウイルスを除去しているふりをし、「ウイルス除去のサポート費用が必要だ」「コンビニでプリペイドカードを買って支払え」と言ってきます。

「トロイの木馬に感染しています」と表示されますが、ウイルス感染はしていません。しかし、パソコンをそのままにしてコンビニにプリペイドカードを買いに行ってしまうと、詐欺にパソコンの中を見られてしまう可能性はあります。また、ネットバンキングで支払うと、暗証番号や口座番号などを見られてしまう可能性があり、非常に危険です。「ビービービー」と鳴っても、絶対連絡はしてはいけません。私の家でもこの間、その「ビービービー」が鳴りました。「Ctrl+Alt+Del」を押しても消えなかったのが、強制終了して、再起動すると元にもどりました。後で IPA（情報処理推進機構）という、ウイルス 110 番などをやっている団体をご紹介します。

4 番目は「投資詐欺」

石井様のお話にもありましたが、すごく多くて、被害金額が高額なため、非常に心を痛めております。

インスタグラムに旅行の写真を載せていたところ、外国人の異性と称する人から、「素敵な写真ですね」とダイレクトメッセージが届きました。LINE で友達登録し、やり取りをしているうちに、暗号資産での投資というものに誘われて、暗号資産を扱う（偽）投資アプリに登録しました。試しに言われた口座に 10 万円振り込んでみると、2 日ぐらいで 13 万円ぐらいが振り込まれたので、「本当にもうかるんだな」と思ってしまい、何度かに分けて 150 万円を振り込みました。偽の投資アプリ上では 300 万円ぐらいになり、そろそろ下ろそうと思うと、「関税が 30 万かかる」

「口座が凍結されているから凍結解除費、手数料が必要だ」と言われて、何度かに分けて 150 万円振り込みました。それでも換金できなかったため、詐欺だと気づいたというトラブルです。

インスタグラムや LINE でやり取りをしているので、相手の名前も住所も分からないところが問題です。格好いい写真は嘘です。

暗号資産に関するトラブルについては、金融庁、消費者庁、警察庁が共同でポスターを出しています。SNS での勧誘で最初は安心させますが、グラフもアプリも嘘。暗号資産というのは、金融庁の登録を受けた暗号資産交換業者しか取り扱えません。

詐欺業者とは連絡が取れず、暗号資産がどこにいつているかは分かるのですが、それが誰かが分からないので、まず返金は困難です。

手口：

- ・ SNSでの勧誘が多い。
- ・ 最初は安心させるがグラフもアプリも皆嘘。
- ・ 暗号資産は金融庁の登録を受けた暗号資産交換業者しか取り扱えない。
- ・ 詐欺業者とは連絡が取れず返金は困難。

金融庁・消費者庁・警察庁のポスターより

5 番目は「架空請求」

スマホに+800 や+1 など+から始まる着信があったというご相談です。石井様のお話で、国際電話でなくても発番できるということが分かって、今日とてもいいお話を聞いたと思いました。+から始まる着信があり「料金未払いです。覚えのない人は連絡ください」とアナウンスが流れ、アナウンスに従い、9 番や 5 番などを押すとオペレーターにつながります。「住所、氏名と生年月日を教えてください」などと言われて、答えると「お調べします」と言われて、「あなたは昨年登録したアプリ代金が幾ら未納なので、コンビニでサーバー型プリペイドカードを買って 30 万円を払ってください」などと言われます。これを防ぐためには、国際電話を常にご利用している方は別ですが、国際電話不取扱受付センターに連絡して、国際電話が使えないようにしておくといよいと思います。

「A 社サーバー型プリペイドカード」は Amazon ギフト券です。「コインで削ってください」というところをコインで削ると番号が出てくるので、その番号を相手に教えてしまうことによって、相手にプリペイドカードの代金が渡ってしまいます。

支払ってしまうと、原則お金は戻らないのですが、「今振り込んだ」が「相手がまだ使っていない」場合、プリペイドカード会社がロックしてくれるケースもあります。Amazon ギフト券、楽天ポイントカード、Apple、Google、ビットキャッシュとかのサポートセンターの連絡先を案内しておきました。情報を知っているのと知らないのでは大違いだと思います。

次に、偽佐川、偽ヤマトですね。架空請求（偽宅配便 SMS）。スマホに「お荷物のお届けに上がりましたが不在のため持ち帰りました。配送物は下記より御確認ください」と SMS が届きました（よく見ると sagiwa です）。URL にアクセスしたところ、ウイルスに感染して不特定多数に同じ SMS を送り始めてしまいました、送付を止めたいがどうしたらよいでしょうか、というトラブルです。これはアンドロイドのスマホで起こります。その場合、スマホを機内モード（通信通話ができないよう）にして、アプリにアイコンが出ていたら、削除します。最終的にはスマホを初期化することになりますが、初期化でデータが亡くなってしまうことを防ぐためには、常にバックアップを取っておく必要があると思います。様々なサイトのパスワード変更もしたほうが良い

と思います。

iPhone では、フィッシングといって、たとえば Amazon から「アカウントを更新できません」「クレジットカードが期限切れになっているか住所変更などで情報更新できませんよ。ログインして情報を更新してください」というメールなどが届いて、ID、パスワード、クレジットカードを入力したら偽 Amazon だったというご相談もあります。

これは IPA（独立行政法人情報処理推進機構）のホームページですが、Amazon とあり、メールアドレスも Amazon ですが、偽 Amazon です。添付ファイルを開かないことや、メールに記載の

⑥ー3 架空請求（フィッシング）

IPA（独立行政法人 情報処理推進機構）HPより
フィッシングメールと対策

(Amazon.com) 重要なお知らせ

Amazon顧客サービス<info@amazon.co.jp>
宛先 tarou@example.ne.jp

見かけ上の送信元表示名
※偽装されている

見かけ上の送信元メールアドレス
※偽装されている

対策

- ・添付ファイルを開かない
- ・メールに記載のURLからウェブサイトアクセスしない
- ・メールに記載の電話番号に電話をしない
- ・返信しない

23

URL や電話番号に連絡しないことに尽きます。

アクセスした場合は、使いまわしているパスワードをすべて変更してください。その他クレジットカード会社に連絡をします。カード番号の変更や請求保留をしてくれるところもあります。しかし、URL を安易にタップしない、「アプリ内課金を許可しない」などの設定をしておくといいと思います。

まとめ

まとめは、「通信販売はクーリング・オフはできない」「住所や連絡先を確認」「画面保存しておく」「安易にURLをタップしない」「儲かる話を人に教えるわけではない」です。

私は「NO、GO、TELL」という言葉を必ず言っていますが、これは性被害の防止をしているプログラムです。NOは「断る」。GOは行くのではなく「立ち去る」。TELLのは「信頼できる人に相談する」という意味です。怪しい誘いに近づかない。うまい話などない。安易に個人情報を教えない。はっきり断る勇気を持つ。最後に1人で悩まず、すぐ信頼できる人に相談していただきたいと思っています。

188 という番号にかけると、自分の居住の消費生活センターにつながる仕組みです。あとは警察の#9110。地元の警察署に相談するよう案内しています。

世界の闇バイト事情、犯罪組織のメタモルフォーゼ (metamorphose)
(ZOOM で京都から参加)

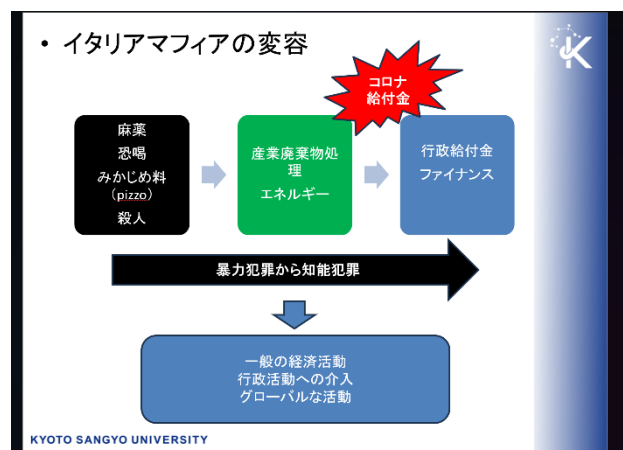
浦中 千佳央
京都産業大学法学部教授

京都産業大学の浦中です。京都から失礼いたします。石附会長のほうから、闇バイトというのは日本だけのものなのかという質問を受けて、実は世界のどこにでもあるのですよというお話をします。アメリカやその他の地域のことは分からないので、主にイタリアとフランスの状況についてお話しします。

「匿・流」のお話が出ていたのですけれども、日本であれば暴力団、あるいは海外、特にイタリアであればマフィアとか、そういう伝統的な犯罪組織というのは、今まで疑似家族制で、親分・子分や義理兄弟を利用して、疑似家族制で組織を運営したり、あるいは地縁に基づいたり、主に中国系だと思いますけれどもやっていました。これらマフィアの活動内容ですが、恐喝や麻薬や人身売買、殺人とか暴力的なことをしていました。

しかし、これが企業型犯罪に変化しています。要はそのような疑似家族制やその他、面倒くさい伝統的なものではなくて、もう会社型に組織運用をしてしまっ、構成員はフラットな関係で犯罪組織を運営します。その対象が、麻薬や人身売買というよりは環境問題、今、廃棄物の処理やエネルギー関連、あるいはファイナンス、先ほどからあるようにお金に関する暗号資産の運用や、ファイナンス系の企業型の犯罪組織になりました。

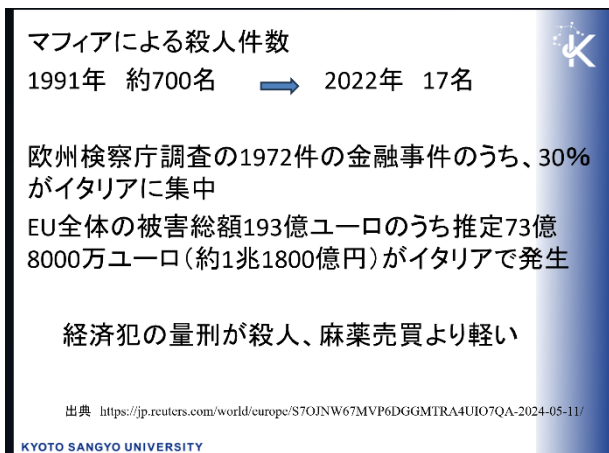
どうしてそのようなことが始まったのかというと、やはり国際化や、自由化、匿名化、こういうものが非常に技術革新や政治的な緊張の緩和、特に冷戦以降、そのような人と金とサービスの流れというもの自由化されたというのが背景にあるのではないかと思います。



それでは、イタリアのマフィアの変容ということで、これは昨年のロイターの記事からの内容になります。昔からイタリアマフィアは、麻薬や恐喝やみかじめ料の徴取、殺人をやっていました。しかし、今では、それではちょっと割に合わないということで、産業廃棄物の処理やエネルギー関連に介入している。さらにコロナ禍では国から給付金をいただける。それだったら行政給付金やそういうものを搾取しようと方向転換しました。金融分野で高利貸しや合法的な資産運用

を活動の柱にしようという風になりました。要は暴力犯罪から知能犯罪に転換しているということです。日本でも民事介入暴力というものがあつたと思いますが、一般の経済活動に進出してきている。そして、行政活動へ介入して、グローバルな活動をしています。

そのロイターの記事によると、マフィアによる殺人件数が、今から 30 年前は 700 名ほど殺されていましたが、2022 年には 17 名になっています。その代わり、金融犯罪のほとんどがイタリアに集中していて、イタリアのマフィアがかなり経済でいろいろなことをやっている。要は、どうしたのかと言ったら、経済犯の量刑が殺人や麻薬売買よりも軽い。殺人や麻薬売買ではいきなり懲役何十年、無期刑ということになるわけです。それだったら経済犯で、給付金の搾取や詐欺をやったほうが、すぐに出てこれ、割に合うという判断があつたのです。



もう一つ大きいのが、犯罪組織の巨大化です。先ほどからサイバー犯罪のお話をしていますが、犯罪組織集団は、IT 技術に非常に長けていて、詐欺文章の作成を全部 AI にさせたり、盗んだものを全部暗号通貨にしたりしています。

そして、麻薬ですが、今までコカインやヘロインといったような麻薬は、広大な土地で栽培するため、土地が必要でしたが、今は化学物質により合成するため、面積の小さい工場で生産でき、土地から解き放されるので、どこでも手狭な空間で麻薬が作れる。それと、多様化した多国籍ですね。先ほどの櫻澤先生のご発表でありました、コールセンターに電話したら、たどたどしい日本語で応答される音声を聞きました。要は非常に多様化した多国籍な人間が絡んできている。そうして巨大化した組織が、犯罪を捜査する機関に汚職という形で介入してきます。あるいは恐喝や暴力ということで、警察官や刑務官を自分たちの意思に従わせるということをやっているわけです。

現に、去年フランスでは、麻薬売買グループのメンバーが刑務所から護送されている途中に襲われて刑務官が 2 人殺害されました。これも護送の計画がだだ漏れだったわけです。現在彼は逃走中です。それと衝撃的な事件、これは日本の「闇バイト」に該当するのでしょうかけれども、去年、14 歳の闇バイトに誘われた少年が、15 歳の少年を殺害したということが発生しました。この 15 歳の殺された少年は人違いだったのです。対立する麻薬売買の人物ではなかったということだったのですが、要は 900 万円で人を殺す闇バイトに応募してしまったということです。

では、その 14 歳の少年がなぜヒットマン、闇バイトに手を出したのかといたら、かなり家庭環境がかわいそうで、両親も 2 人とも麻薬売買で刑務所に入っています。このため、いわゆる施設で育ち、そこで虐待を受けたりして、9 歳のときに警察の御厄介になり、ちょっと様子がお

かしいので血液検査をしたらコカインの反応が出ている。学童なので、その後もいろいろな施設から入ったり出たりということです。このように早い段階で司法や福祉のお世話になっていたのですけれども、諸制度の機能不全で、彼も麻薬に行きつき、結局 14 歳にして、900 万円で人を殺めるものになってしまった。

彼はヒットマンになったのですが、フランスの場合、彼が移民系の子供かどうかというのは記事ではわからなかったのですが、もう 1 つはイスラム系のテロリストになるという可能性もあったわけです。つまり、そういう家庭環境や麻薬売買や、教育環境が非常に悪い子で、そういったところにイスラムの過激思想を持ったリクルーターがやってきて「見てみろ、イスラムの人間たちが虐げられている。イスラエルやアメリカというのはとんでもないことをやっているんだ」と洗脳して、テロリストに仕上げるということで、ヨーロッパがおかれている状況が非常に深刻だということになるわけです。

では、日本の場合はどうなのかという場合、特に闇バイトというものが非常に深刻なのですが、先ほどお話しした 14 歳の少年のように、日本人の彼ら（彼女ら）も多分虐待を受けていたり、いろいろな家庭環境が複雑なのでしょうけれども、フランスの少年までは壮絶生い立ちではない。それと、日本の場合、「匿・流」や「半グレ」にしろ、特に若い女性を「商品」としてターゲットにしている。歌舞伎町や大阪のキタホテル街で、今、いわゆる「立ちんぼ」が出現している。要は、ホストクラブに入れ込んで、それで借金をこさえて身を売ってしまうというのです。これは「この女の人たちが悪いんですよ」という意見がインターネット上では非常に多いのですが、「彼女たちの自己責任に帰するということで、本当にそれでいいのですか」ということを考えたいと思います。彼女たちのような弱い人間（恋愛感情を利用して多額の借金を作らせるように仕向けるビジネスモデル）をどんどん見つけて、要は人身売買のようなビジネスのシステムを確立し、（風俗店に斡旋する、売春の上りをはねるなど）、「人の生き血をすすっている人たち」がたくさん存在し、それは今まで、民事だとか、自己責任とかで、すごく放置されてきました。本当にそれでいいのかと。

また、日本で外国系の方の犯罪者が少し増えてきており、特に実習生の問題ですね、これは人権の観念の欠如があると思います。要は、若い女性や外国人にせよ、そういう弱い立場の人たちが追い込まれて、それを搾取するシステム（管理売春、奴隷労働など）が確立されているのであれば、やはりそれは組織犯罪として対処する必要があるのではないかと思います。自己責任論ではなく、人間の尊厳とか人権を守るための活動が必要です。

それと、もう 1 つは、先ほど来のお話を聞いていると教育が大事だということですね。子供たちは学校で教育されますけれども、そこから飛び出してしまった子供たちにどこが教育をしているのかという課題があります。様々な問題があるのですが、もう 1 つは、私たちのような昭和生まれの人たちですよ。この人たちは、もう人生の半分以上を過ぎたぐらいからスマホやインターネットを使っているわけです。誰からも安全対策やネットリテラシーなどを教えてもらっていない

わけなのです。だから、日本市民安全学会のような、本当に最新のいろいろなお話を聞けるという機会をぜひ昭和生まれの人たちにやっていただくと、犯罪組織やネットにおける犯罪対策になるのではないかなと思いました。

いずれにせよ、日本だけではなく、世界が犯罪の自由化というか、犯罪の国際化や、お金の暗号化、匿名化ということで、要は私たち自身が、日本にいるから大丈夫だと思っていっても、実は既に外国からつながっているから気をつけましょうというお話でした。

Ⅱ 研究ノート

SNS を含む Web・サイバー空間の犯罪社会現象について

詐欺蔓延社会の構造とヒトの脳（若干の考察）

石 附 弘

警察政策学会 市民生活と地域の安全創造研究部会会長

第 1 新たなサイバー空間の特徴

第 2 「詐欺師」とは何者か？

第 3 匿流型犯罪闇バイト・特殊詐欺犯罪の悪質性の核心はどこにあるのか？

第 1 新たな Web・サイバー空間の特徴

- 1 SNS に代表される Web・サイバー空間の新技术が、遠くは地球の裏側の問題・世界の主要国の国家戦略から近くは地域や市民生活まで、時空を超えた一体的包摂社会を作り出し、市民安全・安心にこれまで経験したことのない「光と影」を作り出している。

（注 1）用語の使い方 出典 <https://openai.com/ja-JP/chatgpt/overview/>

◎ Web（ウェブ）：インターネット上の情報を閲覧・検索・共有するための「世界的な情報空間」で、ウェブサイト、ブログ、SNS、オンラインショップなどが含まれる。主にユーザーがブラウザを通じてアクセスする「情報の見える部分」。

◎ サイバー（Cyber）：コンピュータやネットワークを基盤とした「仮想的な空間や技術的な世界全体」（サイバースペース（cyberspace））で、インターネットだけでなく、通信ネットワーク、組み込みシステム、センサー、さらには電磁波を用いた技術全般が含まれる。Web を含む、より広範な「デジタル社会全体」を指す。

- 2 特に、「認知戦争」（注 2）は、時空を超えた一体的包摂社会を作り出す Web・サイバー空間にあっては、この空間が「騙し社会への誘引空間」となり、犯罪の新たな温床となっている。

（注 2）「認知戦争（Cognitive Warfare）」という言葉は、近年、情報戦や心理戦の一環として注目されている概念で、人々の思考・判断・認識そのものを戦場にする戦い方。物理的な武力を使う戦争ではなく人間の心や考え方に影響を与えることで、目的を達成しようとする戦略。

一般市民の「認識」「判断」「意思決定」に影響を与えることで、フェイクニュースの拡散、ソーシャルメディアでの情報操作、サイバー攻撃、ディープフェイクや AI 生成コンテンツの使用、教育・文化的浸透による価値観の変化の誘導等がある。

中国（戦わずして勝つ（孫子の兵法）の元祖中国は、認知領域が新たな戦闘空間となりつつあるとして、認知領域を「感知」「理解」「信念」「価値観」といった意識が構成するバーチャルな空間での戦いが重要だとして、例えば、尖閣列島は中国領との心理戦を展開して

いる)。また、米国、NATO においても国防・軍事・安全保障機関において「認知空間」を新たな戦場として定義しており、従来のサイバー戦を超える脅威となっている。

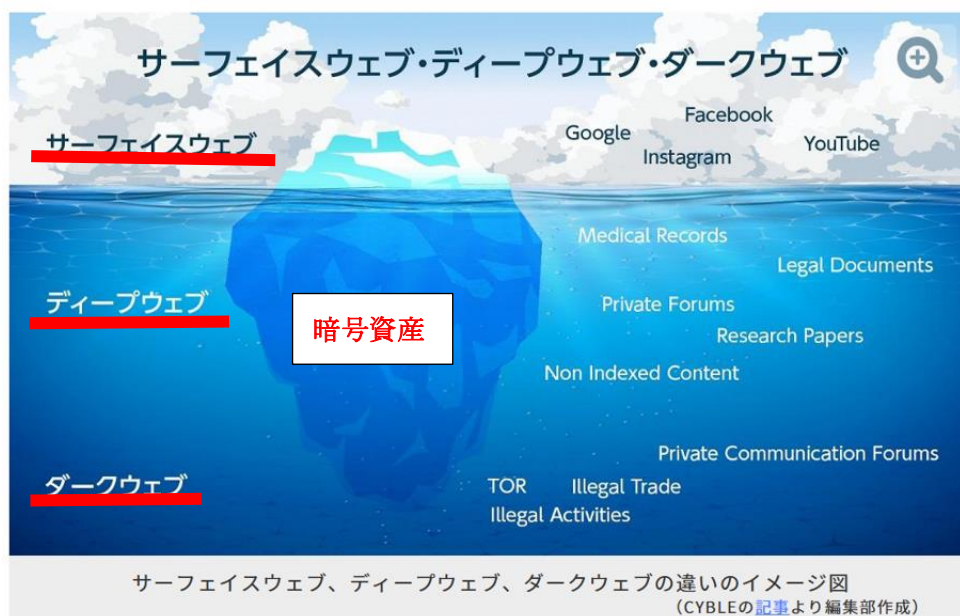
【なぜ危険なのか？】

本人が気づかないうちに影響を受けてしまう。「何が本当か」がわからなくなる（情報の洪水・操作）。民主主義や社会の信頼基盤が崩壊するリスク。

3 詐欺罪の欺罔とは、「騙し」によって相手の『脳とところ』を支配することであり、被害者は、自分が騙されたと知るまでは相手を信じる時間差犯罪である。換言すれば、認知戦争の「一般市民の『認識』『判断』『意思決定』に影響を与え、支配・操作・混乱させる」ことにほかならない。

4 3層構造のWeb・サイバー空間と市民安全

(1) Web 空間は、①表層のサーフェイスウェブ)、水面下の②ディープウェイブ、③ダークウェイブの3つの空間を有しているといわれている。



(2) 市民安全の第一条件

日常生活で私達が生活の1部としてアクセスしているWeb空間は、空間全体の表層Web（サーフェイスウェブ）部分で、この表層Web（サーフェイスウェブ）空間の安全・安心の確保（信頼性・安定性・秩序系の構築）をどう推進していくが喫緊の課題となっている。

(3) 市民安全の第二条件

問題は、海面下の②ディープウェイブ、③ダークウェイブ空間である。反社会勢力の暗躍の場となっており、犯罪収益を洗浄（マネロン）して蓄財する場所（秘匿の蓄財：暗号資産）として悪用されている。悪用の実態解明と国際的な取締が課題となっている。

Web・サイバー空間とは天空の問題ではなく、今や、「生活基盤を支える土台の問題」であり、「無限定条件の下での自律的な最適適応」が求められている。

＊農耕時代の市民生活の土台は土地であった。工業化時代時代の土台は自動車が、そして現代は、サイバー空間の土台の上に市民生活の生活が構築されている。

5 サイバー空間は、何故、詐欺を含む「騙し世界」の温床になったのか？

(1) サイバー空間の有する4つの特性

4つの長所（光） ①時間的・地理的・無限定性、②被害の不特定多数性、③無痕跡性、④匿名性が、4つの短所（影：脆弱性）をつくり、詐欺の「欺罔」という行為を、何時でも、誰でも、何処でも容易に行える環境を作り出した。

（サイバー空間の構造が、詐欺犯罪の誘発環境を作り出している。

サイバー犯罪者がいち早くDXを推進 **サイバー空間犯罪（秩序化未整備）**
高い専門知識や技術を持つ犯罪者たちが相互に連携し、犯罪の分業化、サプライチェーン化が急速に進んだ。
今や、世界中の脆弱なサーバ、漏えいしたアカウントなどの情報は、ダークウェブを介して犯罪者間で共有・売買され、そうした脆弱性を利用する攻撃ツールも専門業者が素早く提供してくれる時代になった。犯罪被害のリスクは急激に大きくなっている。

(2) 古典的詐欺犯罪と現代の詐欺犯罪の構造変化

㉞ 古典的詐欺犯罪の構造＝対称関係

㉞ 現代の詐欺犯罪の構造＝非対称関係

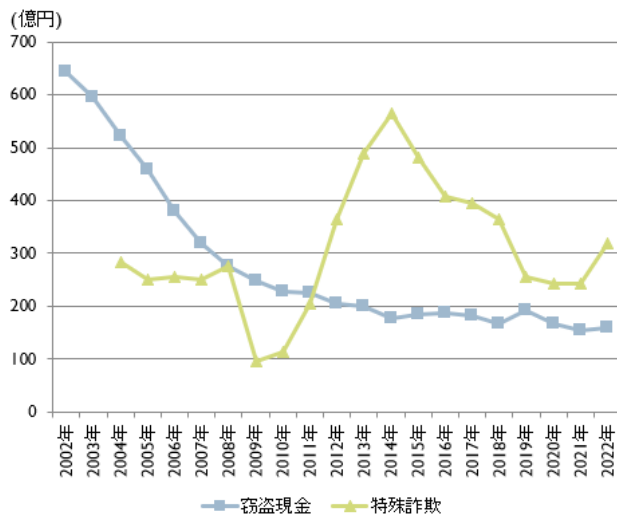


犯罪加害者（㉞）と被害者（㉞）は、
「対称関係」（リアル、対面、接
触、実名・・・目や顔の表情、声な
ど人は5感・6感を使って真偽の
ほどを総合判断できた

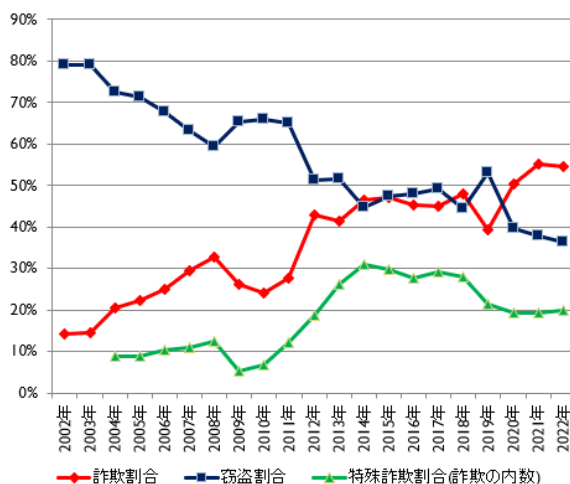


6 時空を越えたサイバー空間が犯罪の新天地になり、市民生活の安全・安心が「騙し」のリスクに曝されている。その象徴的現象が、2012年の窃盗と詐欺の犯罪被害額序列入れ替わり現象である。表は、法務省犯罪白書（令和6年版（2025年1月発行）等をもとに濱田宏彰氏作成。

▶ 現金の被害額としてみると
▶ 2012年に窃盗と特殊詐欺は逆転



財産盗に占める詐欺の割合の増加



被害金額の割合:

窃盗
2002年 79.1% → 2022年 36.4%
詐欺
2002年 14.3% → 2022年 54.5%

特殊詐欺
2004年 8.7% → 2022年 19.8%

※財産犯: 強盗、恐喝、窃盗、詐欺、横領及び占有離脱物横領

(法務省、犯罪白書、2019など)

©2018 SECOM CO., LTD

7 世界規模の「だまし」研究が始まった！（人類の「能」の歴史転換期？）

● 霊長類は、進化するほど脳の大脳新皮質の比率が高くなる。複雑な社会的環境への適応が脳の進化を促進

◎ 「戦術的だまし」(隠ぺい、はぐらかし、装う、社会的道具の利用など) = 仲間の裏をかく行動がみられる

2011.9「だまし」に関する5日間連続公開講座より

(1) 脳の進化：「騙し」と「見破り」の共進化現象

人類の脳新皮質の進化により「騙し」と「見破り」の共進化現象（進化的軍拡競争）が起きている。

(2) 即ち、「だまし能力と、だましを見破る能力」の両者は、対立し相互に作用しあう共進化の関係にある。

(3) ヒトの社会的知性は、他者への共感や共同体生活を維持していくために協力・共同性がある。これからの進化心理学の中心課題は、「裏切り者検知」に鋭敏なところ、協力行動の進化である。

（東京大学総合文化研究科認知行動科学専攻 長谷川寿一教授 東京大学：2011.9「だまし」に関する講座）

なお、2015年8月には、「嘘や欺瞞行動」に関する国際学会が、英ケンブリッジ大学で2015.8開催。世界の科学者が、だましの人間社会行動に関心を寄せているという。

8 国家安全保障分野でも、前述の通り「認知戦争」（相手国世論の分裂戦略等）が国際的な主戦場の1つになった（NATO 公式文書、米国報告書、中国）。また、国内政治においても、「認知戦争」の負の側面が際立ってきた。（注）

（注）認知戦争とトランプ

トランプ政権下で話題になったのが「オルタナティブ・ファクト（Alternative Facts）」という概念。これは事実に対して都合のいい別の解釈や事実を提示する手法で、従来の政治家と違ってメディアを通さず直接 SNS（主に Twitter）で支持者に語りかけ、情報洪水でメディアの批判を封じ込む政治手法。

ここでは、「何が正しいか（知性主義）」ではなく、「何がより強く人々の心情に訴えられるかが最大関心事になる」（2016年のアメリカ大統領選挙で、トランプは典型的な「反知性主義的」リーダーとして浮上、感情や経験、直感を優先する政治を行っている）。

第2 「詐欺師」とは何者か？

1 詐欺の鉄則 15 条（久保博 「詐欺師のすべて」 文春文庫 2002）

これによれば、最近の詐欺師の鉄則は、あまり変わっていないことに気づく。と同時に、認知戦争の戦術にも相通ずるところがあることに留意する必要がある。

詐欺の鉄則 15 箇条 詐欺師のすべて 久保博著 2002 年

- 第1条 自分は詐欺師ではないとの信念を抱け
- 第2条 演技力を磨け
- 第3条 権威を利用せよ
- 第4条 人の弱みをにぎって活用せよ
- 第5条 無価値のものを価値あるように見せかけよ
- 第6条 真実を核にして嘘を構築せよ
- 第7条 最初はまともな話で相手を安心させよ
- 第8条 騙すなら徹底して騙せ
- 第9条 前科のない者を表に立てよ
- 第10条 必要なら契約書をつくって安心させよ
- 第11条 相手をあわてさせ、冷静さを失わせよ
- 第12条 あらゆる手段を使って時間を稼げ
- 第13条 引き際を心得よ
- 第14条 強い返済要求には応じよ
- 第15条 騙し取ったら金は隠しとおすか使い切れ

2 何故、詐欺師になったのか（古典例）？ オレオレ詐欺師は、顔も見えない。邪道だ！

刑務所内の受刑者（常習犯）の生の声を取材したものであり参考になる。

これをみると、刑務所出所後も、手軽に詐欺社会に戻ることができるようである。

4の「オレオレ詐欺は邪道だ！」が面白い。「自分の話術できちんと説明し消火器を販売、相手も納得して20万円稼いでいる。」と。ある種、プロの詐欺師としての個人芸への誇りや職人気質のようなものすら感じられる。

今昔物語1：詐欺師世界も世代交代・詐欺師根性変わらない 昔 （外山ひとみ著 ニッポンの刑務所 講談社現代新書）

1 自称 悪徳商法(詐欺師)の元祖の述懐

前科10数犯、人生の半分30年を刑務所遍歴(刑務所エリート)の60代男

2 何故、詐欺師になったのか？

- ・20代半ば訪問販売の仕事、直ぐにトップの成績
- ・巧みな話術で手取り早く稼ごうと独立し、詐欺師に。点検作業と嘘をつき高齢者宅に消火器などを高く売りつけ成功

3 被害者は高齢者、人を騙すことに抵抗はないのか？

- ・簡単に儲かるし普通の仕事なんか考えられない。出所して2~3時あれば、段取りして運転手と事務員を雇い、すぐに詐欺ができる
- ・罪悪感はない

4 オレオレ詐欺は邪道だ！

- ・自分の話術できちんと説明し消火器を販売、相手も納得して20万円稼いでいる。
- ・オレオレ詐欺師は、顔も見えないし邪道だ！

5 足を洗う気はないのか？

- ・もう先がないから反省しても意味がない、開き直るほかない

油断禁物：われわれの敵は、「プロ」の詐欺師集団

下のスライドは、現代の組織的詐欺集団の指示役とバイト感覚の受け子との関係であるが、闇バイトの凶悪事件以前の、オレオレ詐欺の受け子の供述報道の一例である。

今昔物語 2：詐欺師世界も世代交代・詐欺師根性変わらない
 今 (各種報道から)

「受け子」の供述から「犯罪教育」の実態が明らかに！

- 暴走族ではダメ。社会人を演じないといけない。茶髪を黒く染め、ホテルに備え付けの整髪料を髪になでつけた
- スーツは、詐欺グループの『衣装担当』からレンタル料1万円の有料で貸し出された。使い慣れない敬語を覚え、セリフも練習した。」
 (犯罪版 社会人教育)
- それから貸与された携帯電話が鳴り、指示に従って受取場所に移動
- 被害者から現金を受け取ると、すぐに現金回収役に取り上げられ、そこで任務は終了。
- 受け子の行動を監視していた管理役から帰りの交通費を渡された

3 Web・サイバー空間の出現は、「詐欺」や「社会環境としての騙し」世界を一変させた。

- (1) Web・サイバー空間（携帯・スマホ、IT・AI・DXなどの新技術がもたらした新たな生活空間）の誕生（環境変化）は、詐欺師の活動空間を拡大させ、さらに新技術を悪用して、詐欺犯罪組織の会社化、分業化、専門化、海外拠点化、犯罪インフラの整備などを促進させた。
- (2) 特に、収益効率性と捕まり難さ（安全性）から、機に聡い暴力団の資金獲得の場が、詐欺世界に拡大した。
- (3) 時空を越えたサイバー空間の出現は、第2のWeb空間の有する4つの特性の短所（影：脆弱性）が、騙し（周辺行為を含む）という行為を、何時でも、誰でも、何処でも容易に行える環境を作り出し、無責任あるいは有害な情報拡散につながるなど悪しき社会風潮が増幅している。
- (4) このように、「騙し」の大衆化・蔓延化・肥大化という社会病理現象は、既存の社会安全システム全体の信頼性・安定性を損ね、市民生活の安全・安心の新たな脅威となっている。

第3 匿流型犯罪闇バイト・特殊詐欺犯罪の「悪質性の核心」はどこにあるのか？

～「命（自由意志）」と「財産」は、どちらの「法的価値」が高いのか？

1 匿流型犯罪闇バイト「加害者」と特殊詐欺「被害者」の共通点

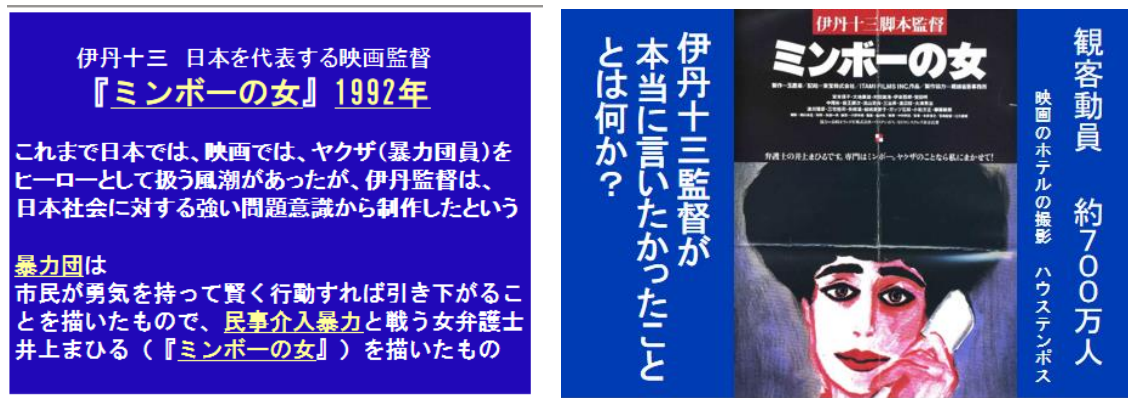
いずれも携帯電話で「指示役からの『指示』」に従って行動していることである。



加害者も被害者も、その起因は「見えない相手」からの詐欺心理学的アプローチによって犯罪者に「脳とこころ」を支配されたことに始まる。即ち、詐欺犯によって自己の自由意志（命の源泉である自己決定能力という法益）が剥奪されたことを意味する。

特殊詐欺は、詐欺という財産犯罪で処罰されるが、「財産」より上位価値のある「自由意志（命の源泉である自己決定能力という法益）が剥奪される」という重大な法益侵害の違法性については、あまり考慮されてこなかったように思う。

2 伊丹十三監督が「ミンボーの女」で、国民に一番伝えかったことは何か？



この映画は、暴力団対策法（公布 1991 年 5 月 15 日、施行 1992 年 3 月 1 日）の制定と軌を一にして上映されたもので、「暴力団の本質」をズバリ描いた名作であり、観客動員約 700 万人と言われている。当時、筆者は警察庁暴力団対策 1 課長であったが、この映画が国民の暴力団に対する意識を変えた契機の 1 つとなり法執行の円滑化にも資したものと考えている。

ところで、伊丹監督がこの映画を通じ国民に伝えたかった「暴力団の本質」とは何だったのか？

監督は、主役のミンボーの女（女性弁護士井上まひる）に、暴力団の反社会的・人間として許し難い行為、その悪質性（核心）を「人々を『恐怖で支配』し、人々に『嘘の人生』を強いている」と言わせている。

近年の犯罪手口では『詐欺と恐怖で支配』に置き換えなければならない。いずれにせよ、「『人の自由意志』の他者支配が、悪質性の核心と考えるべきではないか。

この考え方によれば、匿流グループ犯罪の特殊詐欺の場合、これを「単なる財産犯」（詐欺罪）とみるべきではなく、「人の脳とこころ」の支配を通じて「継続的に資金獲得を目的」とした「人間支配犯罪（人格権侵害犯罪）」と言えるのではないかと。

3 匿流型犯罪グループの「悪質性」や「犯罪被害の重大性」は、昔の暴力団より高いといえるのではないかと。

（1）被害者の守られるべき重大法益の侵害と長期継続的な被害規模の大きさ

被害額の規模、詐欺被害者の絶対数、犯罪インフラ・共生者による健全な社会的安全システムの機能障害市民生活の安全・安心の侵害、加えて末端若者闇バイトの対する心身のダメージ

(被害者の側面)

(2) 犯罪グループ・犯罪形態からみる社会的危険性

大規模、分業化、専門化、会社化、国際化、特に「金主（不良収益の最終領得者）」の悪質性（推測であるが、使途先は、犯罪事業の拡大、半合法事業へ進出、合法企業の乗っ取り、合法企業への転身等か？）

第4 私の身近に迫った「匿流」の魔の手

誰でも何処でも、詐欺の魔の手が！ 私事にわたるが実例なので紹介する。

1 我が家の前の生活道路に、スマホ片手の不審者が調査活動

昨年 10 月、闇バイトと思われる自転車に乗った若い男が、スマホ片手で我が家の前の生活道路一突き当りと知らず入ってくる者もいるが、この若者は3回も行き来しており、反社会的調査活動を思われる。（防犯カメラに映像が記録されており、近隣への注意喚起と地元警察への通報を行った。

2 スプーフィング詐欺電の恐怖

(1) 警察の公的番号から「あなた名義の口座が不正に開設されている」とウソをつきお金をだまし取るスプーフィング詐欺電であるが、この 5 月 18 日、当方の携帯ワンタッチダイヤルに娘から電話（10:14）があり、何の疑いもなく2回架電する（10:27、10:32）したが応答がなく、家内の携帯で娘に連絡した所、当方には電話を架けていないことが判明した。

(2) そこで着信電話の番号 080-××××-××××) を調べ娘に確認すると、娘のものではないことがわかり、ワンタッチダイヤル（娘名義）を乗っ取り、娘になりすまして電話を架けるという極めて悪質な手口の詐欺電と判明した。

匿流型犯罪グループから市民社会を守る術については、円卓会議の中で、詳細な説明がされているが、詐欺の魔の手が、誰にでも何処でも忍び寄って来るということを、知っておくことが、我が身の「脳とこころ」を守る事始めであることを記して筆を擱く。

警察政策学会資料 第 141 号

匿流犯罪と市民安全の心技体

令和 7（2025）年 7 月

編集 警察政策学会
市民生活と地域の安全創造研究部会
発行 警察政策学会

〒 102-0093
東京都千代田区平河町 1-5-5 後藤ビル 2 階
電話 (03) 3230-2918・(03-3230-7520)
FAX (03) 3230-7007