

日本のマネロン対策、次の一手

【連載】第2回

変化するマネロンリスク



KPMG/あずさ監査法人
金融アドバイザー事業部
エグゼクティブ・アドバイザー
尾崎 寛

海外拠点から 日本へ犯行指示も

マネー・ロンダリングやその前提犯罪を行う組織や犯行拠点は多様化しており、犯行の手法・形態もさまざまに変化している。

警察庁の「令和4年版犯罪収益移転危険度調査書」によると、特殊詐欺の犯行グループは、首謀者を中心に詐欺金の引き出し役や犯行ツールの調達役など役割を分担し、組織的に詐欺を行っている。詐欺金の振込先には、架空口座や他人名義の口座が利用されるなど、資金の出所や真の所有者を分からなくするマネ

ロンが行われている。

犯行グループは、犯行拠点として賃貸マンション・オフィス、民泊、ホテル、車両などを利用しており、外国の拠点を利用している事例もある(注1)。最近の報道によれば、全国で相次ぐ強盗事件に関して、フィリピンから日本国内の実行役に指示を出していた「ルフィ」と名乗る人物が、フィリピンに拠点を置く特殊詐欺グループ幹部だったとされる。被害者から詐取した資金をATMから出金する「出し子」らにも、フィリピンから指示を出していたという。

このような犯罪を行う、わが国の代表的な組織は暴力団であ

る。暴力団は、集団的または常習的に犯罪を行っており、暴力団対策法の規定で指定暴力団として25団体が指定されている(2022年10月1日現在)。

このほか近年、暴力団のような明確な組織構造を有しない「半グレ」といわれる準暴力団等も、特殊詐欺等の違法な資金獲得活動を活性化させており、違法に得た資金の一部を暴力団に上納する実態もある(注2)。

わが国におけるマネロン等における主体は、暴力団、特殊詐欺グループ、外国人犯罪者グループであり(注3)、これらは密接に関係し、連携しながら、金融犯罪・マネロン等を敢行して

いる可能性がある。

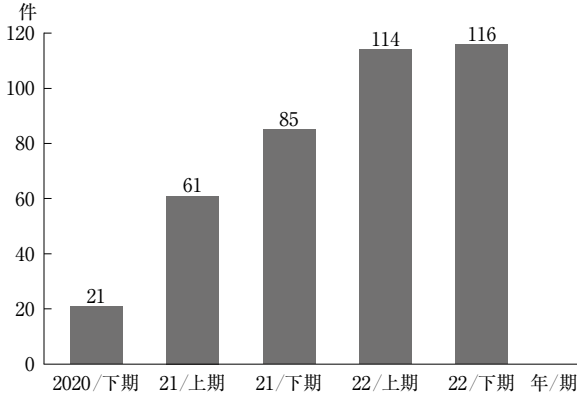
ランサムウェアによる被害も拡大

犯行の手法も変化している。

新型コロナウイルス感染症拡大等により、インターネット利用時間やEC(オンライン通販)におけるクレジットカード決済が増加し、フィッシング詐欺の被害も増大している可能性(注4)がある。また、スマートフォン

の普及によるインターネットサービス利用機会の拡大を悪用する犯罪が拡大している可能性(注5)もあり、それぞれ注意が必要だ。
「ランサムウェア」による被害も、国内外を問わず市民生活にまで重大な影響を及ぼしている(注6)。ランサムウェアとは、「Ransom」(身代金)と「Software」(ソフトウェア)を組み合わせた造語である。犯罪者が不正プログラムをメール送信などによって企業・組織等のパソコンなどに感染させ、保存されていたデータを暗号化して使用できない状態にした上で、そのデータを元の状態に戻す対価

〔図表〕 企業・団体等におけるランサムウェア被害の報告件数推移



(出所) 警察庁広報資料

(金銭や暗号資産)を要求することを指す。

国際社会においては「ランサムウェアの発達と急増は、金融機関が現在直面している課題のなかで最も重大なものの一つである」とみなされている(注7)。日本国内のランサムウェアによる感染被害は、22年に報告件数が230件となるなど、サイバー空間における脅威が続いている(図表)。これらの被害の中には、中国、ロシア、北朝鮮と

いった国家を背景に持つサイバー攻撃集団によるサイバー攻撃も含まれている(注8)。

犯罪者は新技術や脆弱性を活用

また、「収納代行スキーム」におけるリスクも見られる。ある事業者は、第三者から代理受領権を取得した上で、当該第三者から事業者の銀行口座に入金させ、その資金を、海外に所在する別の事業者に対してまとめ

て送金している。この際、銀行は、顧客宛てに入金をする者や最終的に資金を受領する者の実態を直接把握できない。暗号資産交換業者が銀行に開設している銀行口座を受け皿として、不正送金を行う事例も確認されている(注9)。

このように、技術革新等はさまざまな面で国民生活の利便性を向上させている一方で、犯罪者等が

先端技術や新たなサービス等を悪用することにもつながっている。金融犯罪の脅威は、サイバー空間をはじめさまざまな領域において拡大しており、新たな手法・形態によるマネロン事案等が発生している可能性がある。

金融機関もリスクの変化を捉え、特定・評価し、技術も活用しながら、リスクへの対応を高度化させる必要がある。

(本稿の意見に関する部分は筆者の個人的見解である)

(注) 1 国家公安委員会「令和4年犯罪収益移転危険度調査書」13ページ。
2 同44ページ、本文および脚注。
3 同12ページ、1項。
4 警察庁「令和4年版警察白書」第1節技術革新に伴う現代社会における脅威、第1項先端技術等の悪用により深刻化する現代社会における脅威と対策。
5 警察庁「令和4年版警察白書」第1節技術革新に伴う現代社会における脅威、第1項先端技術等の悪用により深刻化する現代社会における脅威と対策。

6 警察庁広報資料(23年3月16日)「令和4年におけるサイバー空間をめぐる脅威の情勢等について」。
7 22年10月21日、G7サイバー・エキスパート・グループ(Cyber Expert Group)が作成し、G7議長国ドイツが公表した「金融セクターのランサムウェアに対するレジリエンスに関するG7の基礎的要素」1項。
8 警察庁「令和4年版警察白書」第1節技術革新に伴う現代社会における脅威、第1項先端技術等の悪用により深刻化する現代社会における脅威と対策、①深刻化するサイバー空間における脅威、(ウ)国家を背景に持つサイバー攻撃集団によるサイバー攻撃。
9 国家公安委員会「令和4年犯罪収益移転危険度調査書」69ページ「所管行政庁が新たに把握した脅威・脆弱性等」。