

# 特殊詐欺対策通信

## 特殊詐欺発生状況 ▶ 令和5年1月～8月の状況

8月中	件数	金額	1～8月	件数	金額
R5年	17	約1,370万円	R5年	122	約2億8,080万円
R4年	9	約4,460万円	R4年	107	約2億3,040万円
増減	+8	約-3,090万円	増減	+15	約+5,040万円

※金額欄は端数を四捨五入しており、金額の増減と一致しない場合があります。

## 手口ピックアップ! 還付金詐欺や架空料金請求詐欺を認知!!

8月中は、市役所職員を名乗る者の電話から始まる**還付金詐欺**やパソコンのウイルス感染名目の**架空料金請求詐欺**を認知しました。

～ 手口の一例 ～

還付金詐欺

被害者の自宅の固定電話に、市役所健康保険課の職員を名乗る犯人から「5年間に渡って支払った保険料の過払い金が〇万〇千円あります。」などと電話が掛かってきます。続いて、金融機関職員を名乗る犯人から「ATMに行ってください。到着したら手続きを教えるので〇50-XXXX-XXXXに電話をして下さい。」などと電話が掛かってきます。被害者が、ATMに赴き、教えられた電話番号に電話を掛けると、金融機関職員を名乗る犯人からATMの操作方法を指示され、指示に従ってATMを操作すると、いつの間にか、被害者が犯人の口座に振込みをさせられ金銭をだまし取られます。

架空料金請求詐欺

被害者が自宅でパソコンでインターネットを利用していると、突然、画面に「トロイの木馬、セキュリティ上の理由によりブロックされています。」などのメッセージと「連絡先〇50-XXXX-XXXX」という電話番号が表示されます。被害者が、表示された電話番号に電話を掛けると、外国人名を名乗る犯人から「あなたのパソコンはウイルスに感染しています。ウイルスの除去をしますので、遠隔操作ソフトをダウンロードして下さい。」などと言われ、被害者が遠隔操作ソフトをダウンロードすると、被害者のパソコンが犯人から操作可能な状態となります。そして、犯人から「ウイルス除去代金として電子マネーカードを購入し、電子マネーカードのカードIDと購入したレシートをパソコンのカメラにかざして、パソコンのメモ帳ソフトにカードIDを入力して下さい。」などと指示され、購入した電子マネーをだまし取られます。

## トピックス

8月中、津山信用金庫本店では、キャッシュカードの振込制限によりATMでの振り込みができなかった来店客が窓口に来店したことから、職員が話を聞いたところ、来店客がATMでの振り込みにこだわることなどから詐欺と見破り、警察に通報するなどして架空料金請求詐欺被害を未然に防止できました。JA大佐支店では、来店客が携帯電話を使用してATMを操作していたことから、操作を中止させ、電話を代わるなどして架空料金請求詐欺被害を未然に防止することができました。また、セブンイレブン倉敷児島柳田店、ファミリーマート西大寺中店、ローソン岡山万成西町店等では、電子マネーカードを購入しようとした来店客に店員が声を掛けたことにより、架空料金請求詐欺被害を未然に防止することができました。

このほかにも、コンビニエンスストア等で合計35件の特殊詐欺被害を未然に防止することができました。

## ココに「技あり」!

来店客がATMの振り込みにこだわることなどを不審に感じて警察に通報したことや携帯電話を利用してATMを操作していることを不審に感じて電話を代わるなどして被害を未然防止した好事例です。