SNS型投資・ロマンス詐欺被害の流れ

資料6

	犯罪グループ	被害者	取組と課題
			緑：R6.6総合対策・R6.12緊急対策 黄：課題
犯行準備	●犯罪者同士は秘匿性の高い通信アプリを利用して通信 ●SNSを用いて実行犯の募集 ●拠点が海外にも所在		「犯行に加担させない」ための対策 ● 「闇バイト」の募集情報の実効的な削除等のための取組を推進 「犯罪者を逃がさない」ための対策 ● 本人確認の強化や日本法人窓口の設置等を要請 ● 本人確認の徹底 ● 犯罪者間の通信内容等の解明 ● 外国当局・国際機関との連携
着手	●SNSやマッチングアプリのアカウントや他人名義口座等の犯行ツールを調達		「犯罪者のツールを奪う」ための対策 ● 携帯電話の不正利用防止対策等の強化
欺罔	●著名人や投資家等を騙り必ず儲かるなどの偽広告をSNSに掲載 ●SNSやマッチングアプリ上で、ダイレクトメッセージを送信 →SNSやマッチングアプリの本人確認はSMS認証やE-mail認証 →海外の電話番号やWeb E-mailアドレスからの利用者特定が困難	【接触ツール】 ●投資詐欺は、SNSが72.1% ※入口はバナー等広告からダイレクトメッセージへ変化 ※悪用されるＳＮＳも変化 ●ロマンス詐欺ではマッチングアプリが35.0%	「被害に遭わせない」ための対策 ● SNS事業者における広告掲載時の審査を強化 ● LINE公式アカウントについてSMS認証による本人確認を導入 ● LINEにおける友だち追加する際のポップアップ表示（注意喚起） ● SNSやマッチングアプリのアカウント開設時の本人確認の強化
	●LINEに誘導 ●時間をかけて信用させ、信頼関係を構築した上で投資等に誘導 →登録時のSMS認証に利用される携帯番号やIPアドレスは海外のものが多数	●被疑者を信用し、長期間にわたるやりとりを繰り返す傾向 →被害に遭ったことを認知するまでの期間が長期化し、通信履歴等の必要な情報が削除	「犯罪者を逃さない」ための対策 ● LINEにおける照会対応体制の拡充 ●ガイドラインの改定や通信履歴の保存の義務付けを含め検討 ● 海外事業者の日本人窓口の設置の働き掛けなど情報提供の迅速化のための環境整備に向けた更なる働きかけ等の推進
金銭等の交付	●犯罪者同士は秘匿性の高い通信アプリを利用して通信 ●譲渡口座や実態のない法人の口座を悪用 ●ネットバンキングを用い口座間を繰り返し送金、暗号資産に交換 →警察認知時には既に被害回復困難、金融機関の協力が不可欠	●被害件数に占める割合は振込（81.5%） ※うち59.2%がネットバンキングを利用 ※暗号資産(15.0%)、電子マネー(2.2%) →ネットバンキングの利用限度額は非対面で変更可能であり、また、複数回にわたる振込により被害高額化	「犯罪者のツールを奪う」ための対策 ● 預貯金口座の不正利用等防止に向けたモニタリング等対策や警察との連携の強化等を要請 ●被害金を確実に捕捉し、その回復を図るため預金取扱金融機関と暗号資産交換業者における情報連携の推進 「犯罪者を逃さない」ための対策 ● 金融機関への照会・回答の迅速化に向けた協議を推進 ●犯罪収益を剥奪し、効果的なマネロン対策を講じるための新たな捜査手法の導入等 ●外国当局との協力関係の強化が課題

特殊詐欺被害の流れ

犯罪グループ	被害者	取組と課題

緑：R6.6総合対策・R6.12緊急対策 黄：課題

犯行準備

●犯罪者同士は秘匿性の高い通信アプリを利用して通信

●SNSを用いて実行犯の募集

●拠点が海外にも所在

●他人名義口座、国際電話番号、名簿等の犯行ツールを調達
→国際電話番号は容易に取得可能

「犯行に加担させない」ための対策
- 「闇バイト」の募集情報の実効的な削除等のための取組を推進

「犯罪者を逃がさない」ための対策
- 本人確認の強化や日本法人窓口の設置等を要請

- 本人確認の徹底
- 犯罪者間の通信内容等の解明
- 外国当局・国際機関との連携

「犯罪者のツールを奪う」ための対策
- 個人情報保護法等違反での立件等の闇名簿対策を推進

着手

●各種名簿掲載の電話番号に対し、オートコール利用による大量に発信
●国際電話番号を用いた架電が増加

「被害に遭わせない」ための対策
- 国際電話不取扱等の犯人からの電話を直接受けないための対策を推進

- 国際電話を悪用した詐欺電話への対策として、契約者全体に国際電話利用休止について周知が必要
- 携帯電話への迷惑電話・迷惑メール・迷惑SMSに対する被害防止機能の向上
- 詐欺に誘引するダイレクトメッセージ等に対する取組の推進

欺罔

●警察官等を騙ったオレオレ詐欺では、LINEに誘導し、偽の警察手帳や逮捕状等を提示して欺罔
→世の中の話題に応じて、騙しの文言を随時変化

【欺罔手段に用いられたツール】
●電話（79.1%）
※　うち約７割が固定電話へ携帯電話への割合も増加
●SMS・電子メール等（9.7%）
●ポップアップ表示（8.9%）

「被害に遭わせない」ための対策
- ターゲティング広告やアドトラックの活用等多様な媒体を活用した情報発信を実施

●犯罪者同士は秘匿性の高い通信アプリを利用して通信

- 海外事業者の日本人窓口の設置の働き掛けなど情報提供の迅速化のための環境整備に向けた更なる働きかけ等の推進

●騙しの口実や手口が巧妙化
※　特殊詐欺のことを知っていても騙されてしまう実態

●最新の手口等について、更に効果的な情報発信が必要

金銭等の交付

【交付形態】(被害件数の割合)
●振込（52.6%）
※　高額振込被害（500万円以上）の60.6%がネットバンキングを利用
→ネットバンキングの利用限度額は非対面で変更可能であり被害高額化
●手交（26.9%）
●電子マネー(10.9%)

「犯罪者のツールを奪う」ための対策
- 預貯金口座の不正利用等防止に向けたモニタリング等対策や警察との連携の強化等を要請

●被害金を確実に捕捉し、その回復を図るため預金取扱金融機関と暗号資産交換業者における情報連携の推進

●譲渡口座や実態のない法人の口座を悪用
●ネットバンキングを用い口座間を繰り返し送金、暗号資産に交換
→警察認知時には既に被害回復困難、金融機関の協力が不可欠

●現金等は運搬役を用いてマネロン
→防犯カメラの増設も不可欠

「犯罪者を逃さない」ための対策
- 金融機関への照会・回答の迅速化に向けた協議を推進
- 防犯カメラの増設

●犯罪収益を剥奪し、効果的なマネロン対策を講じるための新たな捜査手の導入等
●外国当局との協力関係の強化が課題

ＩＤ・パスワード等の窃取による被害の流れ

犯罪グループ	被害者	取組と課題

緑：R6.6総合対策・R6.12緊急対策　黄：課題

犯行準備

ＩＤパスワード クレカ情報 不正入手

●実在する企業等のHPを模した
フィッシングサイトを構築

「被害に遭わせない」ための対策
●フィッシングサイトの閉鎖促進

「被害に遭わせない」ための対策
●フィッシングサイトに係るＵＲＬ情報の提供
●先制的なフィッシングサイト対策（フィッシングサイトの特性を踏まえた対策の高度化）の実施
●生成ＡＩ等を活用したフィッシングサイト判定の高度化・効率化を実施

【不正送金におけるフィッシングサイト等に誘導する手口の内訳】
電子メール　58.2%
SMS　14.0%
（※他は不明）

●実在する企業等を装った
メール／ＳＭＳの作成・送信

「被害に遭わせない」ための対策
●ＳＭＳの不適正利用対策の推進

フィッシングメール/SMSの受信
リンクからのアクセス・入力

●ID/パスワードの窃取

「被害に遭わせない」ための対策
●送信ドメイン認証技術（DMARC等）への対応促進

●クレジットカード情報番号の窃取

●ECサイトの脆弱性を悪用し、
クレジットカード番号等を窃取

「被害に遭わせない」ための対策
●パスキーの普及促進

脆弱性のあるＥＣサイトにおける情報窃取対策の必要性

ＩＤパスワード クレカ情報 不正利用

●正規サイト・アプリに不正ログインし、犯罪者自身が管理する口座等へ不正送金

「被害に遭わせない」ための対策
●ＥＣ加盟店等との情報連携の強化

「被害に遭わせない」ための対策
●クレジットカード不正利用情報提供の効率化

●不正入手したクレジットカード番号等をECサイト等で不正利用

「被害に遭わせない」ための対策
●コード決済に関する被害防止対策の実施

暗号資産交換業者における送金後のモニタリング強化の必要性

●不正プログラムに感染したIoT機器等を不正利用し、不正アクセス元のＩＰを一般家庭のＩＰに偽装

不正送金等を行う際の踏み台として、一般家庭のＩＰが悪用され、アクセスの検知・捜査上の支障が存在

「犯罪者のツールを奪う」ための対策
●暗号資産交換業者への不正送金に係る対策の実施

資金洗浄・現金化

●譲渡口座や実態のない法人の口座を悪用
●ネットバンキングを用い口座間を繰り返し送金、暗号資産に交換
→警察認知時には既に被害回復困難、金融機関の協力が不可欠

【不正送金被害の送金先口座】
暗号資産交換業者：約32.1億
その他　　：約54.8億

ペイメントサービス等のアカウント作成や不正送金時のアクセスに利用されるデータ通信専用SIMは、契約時の本人確認の義務付けなし