AI ビデオ通話分析が明らかにする「ニセ警察詐欺」の心理操作構造

～巧妙化する特殊詐欺へのリアルタイム防御システムの提言～

ライフデザイン研究部 主席研究員/テクノロジーリサーチャー 柏村 祐

1.深刻化するニセ警察・検察詐欺

法執行機関職員を装い金銭を詐取する「ニセ警察・検察詐欺」は、手口の巧妙化が著しく、深刻な社会問題として対策が急務である。本レポートは、この喫緊の課題に対し、AI によるビデオ通話分析という最先端の技術で犯行手口の実態を鋭くえぐり出し、被害の防止に向けた実効性のある戦略的対策を提言することで、社会の安全確保に貢献することを目的とする。

警察庁統計（令和 7 年 3 月末）によれば、警察官等を騙る詐欺被害額は特殊詐欺全体の 6 割強（171.7 億円）に達し、なお増加傾向にある。警察庁の注意喚起（注 1）等が示すように、犯人は「口座が犯罪に利用された」「携帯電話の不正契約により情報流出」等の虚偽情報を用いて、被害者の不安を煽る。その上で「資産保護」「口座調査による潔白証明」といった巧妙な口実で金銭を要求する手口が横行している。特に、「逮捕の可能性」「全財産喪失」といった脅迫的言辞や、偽造された身分証・逮捕状の提示は、被害者の判断能力を麻痺させる悪質性の高いものである。手口は劇場型や SNS 誘導など常に進化し、複雑化・高度化の一途を辿っている。

2.AI ビデオ通話分析によるニセ検察官の手口の構造的解明

本節では、ニセ検察官を名乗る人物と被害者との実際のビデオ通話記録（図表 1）を AI が解析した結果にもとづき、その手口を構造的に解明し、犯人が用いる心理操作のメカニズムを明らかにする。この分析は、詐欺の「ブラックボックス」を可視化する試みである。

図表１　犯人からのビデオ通話

資料：警察庁（https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/241218/02.html）より

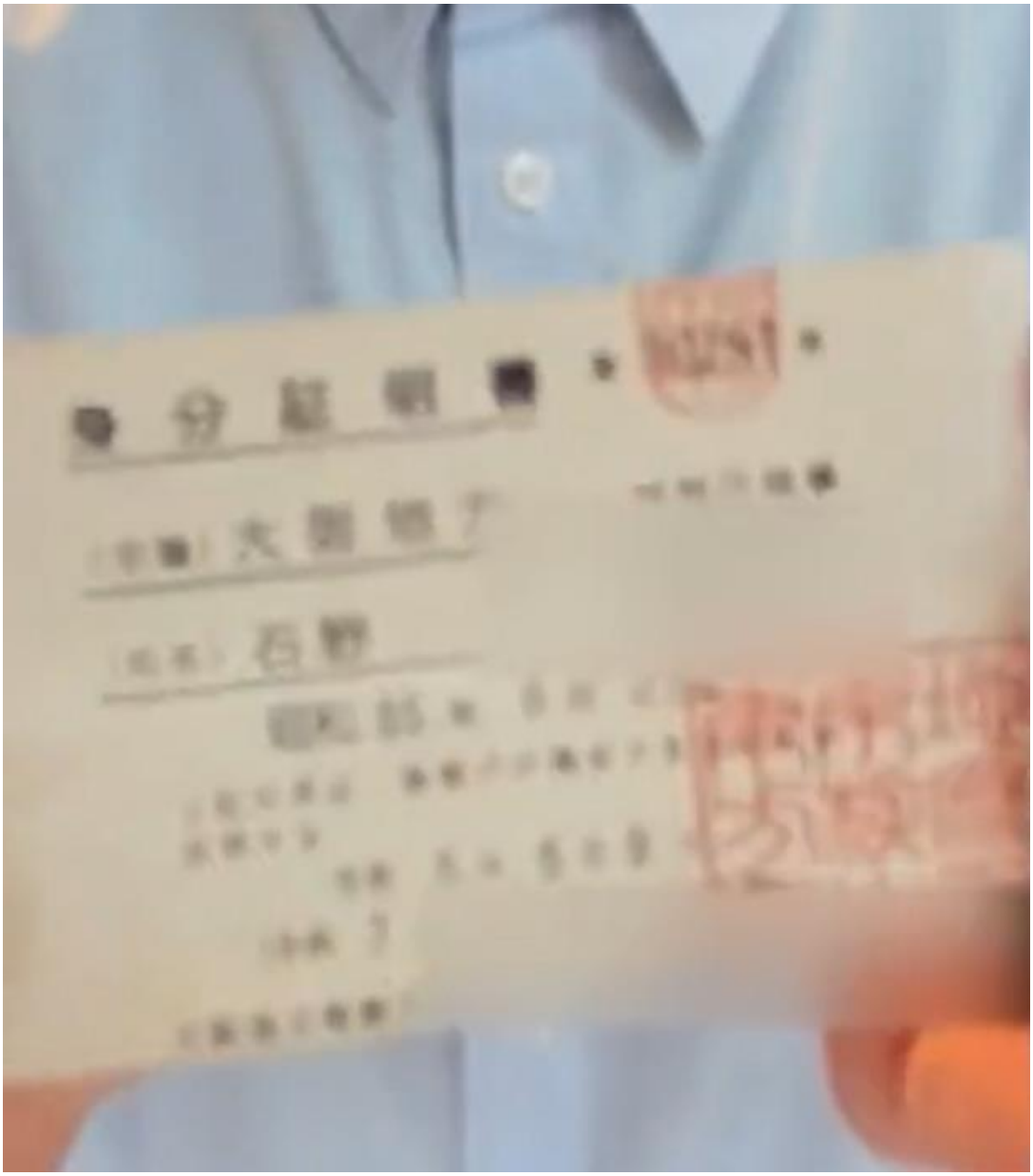
1)初期段階：権威の構築と心理的布石

通話の冒頭で、詐欺師は被害者の本人確認の後、「大阪地検特捜部検事イシノ」と名乗った上で、被害者に対し自身の身分証明として「カード」による身分証明を一方的に通告した。AI はこの時点で最初の危険信号を特定する。正規の検察官がこのような形で身分証明を要求することは通常想定されず、「大阪地検特捜部」という公的な組織名を騙ることで、事態の深刻さと権威を演出し、被害者を心理的に支配下に置こうとする明確な意図が読み取れる。この段階の核心は、偽の権威を迅速に確立し、被害者を自身のシナリオに引き込むことにある。

2)中核手口：偽造身分証による視覚的詐術と判断力の麻痺

次に、詐欺師は偽造された「身分証明書」（氏名、所属、生年月日、公印を模した印影、有効期限を模した日付記載）を提示する（図表 2）。同時に、「ピントが合っていなければ見えにくいでしょう」などと、あたかも映像の問題であるかのように装って声をかけ、被害者を急かし、詳細な確認を妨げる。AI はこの行為を、「被害者の認知プロセスに介入し、偽造物に対する批判的思考を抑制させる高度な心理操作」と分析する。身分証は偽造の蓋然性が極めて高く、詐欺師は一瞬または不鮮明な状態で見せることで被害者からの検証を回避する。これは偽の権威を視覚的に補強し、被害者の判断力をさらに麻痺させる巧妙な戦術である。

図表 2　犯人が提示する偽の身分証明書



資料：図表 1 に同じ

3)信頼醸成と支配の深化：安心感による操作と次段階への誘導

身分証提示後、詐欺師は不明点がないか尋ね、手続きの正当性を装い被害者の警戒心を一時的に緩和させる。これは威圧と懐柔を巧みに使い分けるソーシャルエンジニアリングの典型であり、被害者の心理的抵抗を無力化する。これまでの本人確認と身分証明の一連のプロセスによって築かれた偽りの信頼関係は、次の金銭や個人情報を要求するための決定的な布石として機能する。

4)最終段階への移行：「かけ直し」戦略による完全な孤立化と心理的掌握

通話終盤、詐欺師は一度通話を切り、再度かけ直すと告げる。AIはこの「かけ直し」を最大の危険信号とし、詐欺成功の鍵を握る古典的かつ効果的な戦術と断定する。その戦略的意図は、①被害者を外部の助言や情報から完全に遮断し、心理的に孤立させる、②犯行フェーズへスムーズに移行する、③追跡や証拠保全を困難にする、④「重要な捜査の継続」を匂わせ、被害者の期待感と切迫感を最大限に高め、指示に従わざるを得ない状況を作り出すことにある。この戦略により、被害者は完全に詐欺師の支配下に置かれ、詐欺の核心部分へと誘導される。

AIは、このビデオ通話について、なりすまし詐欺の初期段階における犯人の行動計画と心理操作技術を鮮明に示しているとする。「偽造身分証の提示」と「かけ直し」は、被害者を欺き、支配するための計算され尽くした手口であり、次の電話で展開されるであろう虚偽の告発や金銭・情報要求の成功率を高めるものである。

3.既存啓発の限界と新たな防衛パラダイムの必要性

警察庁等が啓発している、詐欺の見破るポイントの周知や相談窓口（#9110等）の充実は、基礎的な防衛ラインとして重要である。公務員が電話のみで捜査内容を詳述したり、一般的なSNSで公式に連絡を取ったり、身分証画像を安易に送付したり、予告なくビデオ通話をかけたりすることは通常あり得ない。

しかし、AI分析が示すように、詐欺師は巧妙な心理操作と視覚的詐術を駆使し、被害者の認知バイアスを巧みに利用する。このような高度化した脅威に対し、知識ベースの既存啓発だけでは限界があり、被害者のリアルタイムの判断を支援する新たな防衛パラダイムの構築が急務である（図表3）。

図表 3　ニセ警察・検察詐欺：犯行の進行と被害者の心理的な落とし穴

資料：筆者作成

4.AIリアルタイム詐欺アラート機能の実装戦略

既存啓発の高度化に加え、より能動的かつ技術的な防衛策として、情報端末への「AI詐欺アラート機能」の標準搭載または高度セキュリティアプリとしての実装・普及を最重要戦略として提言する。この機能は、詐欺の疑いがあるコミュニケーションをリアルタイムで検知・警告するものである。

1)AI 詐欺アラート機能の核心技術と実装イメージ

本機能は、最先端 AI 技術を駆使した多層的な検知・警告システムを想定するものである。

第一は、ビデオ通話のリアルタイム・マルチモーダル解析である。AI が映像（身分証の微細な偽造痕跡、背景の矛盾等）、音声（声紋分析による不審者特定、脅迫・誘導キーワードの高度な意味理解、会話構造分析による「かけ直し」等の詐欺特有パターンの検出）を統合的に常時監視・分析する。そのうえで危険度をスコアリングし、閾値を超えた場合、「緊急警告：検察官を名乗る人物とのビデオ通話は、AI 分析により詐欺の可能性 9X%と判定。提示された身分証は偽造の疑い濃厚。金銭・個人情報の要求には絶対に応じないでください！」等の具体的かつ強い警告を画面にオーバーレイ表示する。

第二は、音声通話・テキストメッセージの高度コンテキスト分析である。表層的なキーワードだけでなく、文脈、感情、会話の意図を AI が深層学習モデルで解析し、詐欺特有のコミュニケーションパターンを早期に検知し警告する。

第三は、動的脅威インテリジェンス連携による発信者リスク評価である。「+」で始まる国際電話、詐欺に多用される番号帯、ダークウェブで取引される不正取得アカウント情報等を、国内外の脅威インテリジェンス・プラットフォームとリアルタイムで照合し、プロアクティブにリスクを警告する。

これらの機能により、まずは利用者自身では詐欺と判別が困難な状況下でも、AI が客観的に危険を評価し、被害が顕在化する前に利用者が適切な対処を取ることを可能にする。

2)利用者中心のインターフェースと迅速なエスカレーション支援

警告は単なる通知に留まらず、「通話を即時ブロック/切断」「会話記録の自動保全（証拠化支援）」「信頼できる連絡先への緊急通知」「#9110 等の専門機関へのワンタッチ通報（状況サマリー自動生成）」といった、利用者の次の行動を直感的かつ確実に支援するインターフェースを備える。これにより利用者が詐欺の脅威に直面した際に、パニックに陥ることなく、冷静かつ確実な対応を迅速に実行できるため、被害の拡大を最小限に抑えるとともに、証拠保全や捜査協力への道筋を確保し、二次被害の防止にも貢献するが期待される。

3)期待される効果と社会実装への道筋

本機能の社会実装は、個々の被害防止に留まらず、詐欺犯行のROI（投資対効果）を著しく低下させ、犯罪抑止にも繋がる戦略的意義をもつ。また、検知された詐欺試行データは、匿名化・統計処理の上でさらなるAIモデルの強化や、捜査機関による犯行グループの特定・検挙に貢献し得る。実現には、通信事業者、端末メーカー、OS開発企業、セキュリティ企業、そして政府・警察機関による強力なリーダーシップと連携体制の構築が不可欠である（図表 4）。

図表 4　AI 詐欺アラートシステムの戦略的価値とエコシステム

資料：筆者作成

5.安全なデジタル社会実現に向けた官民一体の戦略的行動

ニセ警察・検察詐欺は、高度な心理操作と技術を駆使する現代社会特有の脅威であ

る。AIによるビデオ通話分析は、その手口の巧妙さと危険性を客観的に明らかにした。

この脅威に対抗するためには、既存の啓発活動の質的向上に加え、本稿で提言した「AIリアルタイム詐欺アラート機能」のような革新的技術を社会インフラとして実装することが不可欠である。これは単なる技術導入に留まらず、社会全体の防犯リテラシーとレジリエンスを向上させる戦略的投資と位置づけるべきである。

政府は、本機能の開発・普及を国家戦略として推進し、必要な法制度整備や研究開発支援、国際連携を主導するべきである。同時に、企業は社会的責任として本技術の導入に積極的に取り組み、利用者の安全確保に貢献することが求められる。

この官民一体となった戦略的行動を通じてこそ、巧妙化する詐欺の脅威から国民を守り、真に安全で安心なデジタル社会を実現することができる。本レポートが、その実現に向けた一石となることを期待する。

【注釈】

1）警察庁ウェブサイト「ニセ警察詐欺に注意！ #ニセ警察詐欺」
https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/241218/02.html