トクリュウ対策としての「遠隔解析」

警察庁有識者検討会資料の読み解きと、民間企業・金融機関への影響

弁護士法人三宅法律事務所
弁護士　渡邉雅之

出典・参考：警察庁 有識者検討会資料掲載ページ　https://www.npa.go.jp/bureau/soumu/kentoukai/shiryou.html

2026年9月

最初に用語をそろえる：本資料では「トクリュウ」と略す

匿名・流動型犯罪グループ ＝ トクリュウ

- 実行犯募集・犯行指示が、秘匿性の高い通信アプリで非対面・匿名に行われる
- 実行犯は入れ替わるが、指示役・標的リスト・資金移転ルートは残り続ける
- この構造が「捕まえても次の被害が止まらない」問題を生む

出所：警察庁・有識者検討会 提言骨子、資料3・9・10

この制度を一言でいうと

「犯人を捕まえる」だけではなく、
「次の被害者を見つけて止める」制度

遠隔解析は、捜査技術の話に見えるが、政策の中心は「被害防止」への転換である。

事後処罰

起きた犯罪を立件する

►

事前阻止

標的・犯行計画を把握し被害を防ぐ

出所：提言骨子「犯罪者グループの端末から通信内容等を迅速に把握し、被害防止に活用」

全体構成：50枚以内に凝縮した読み方

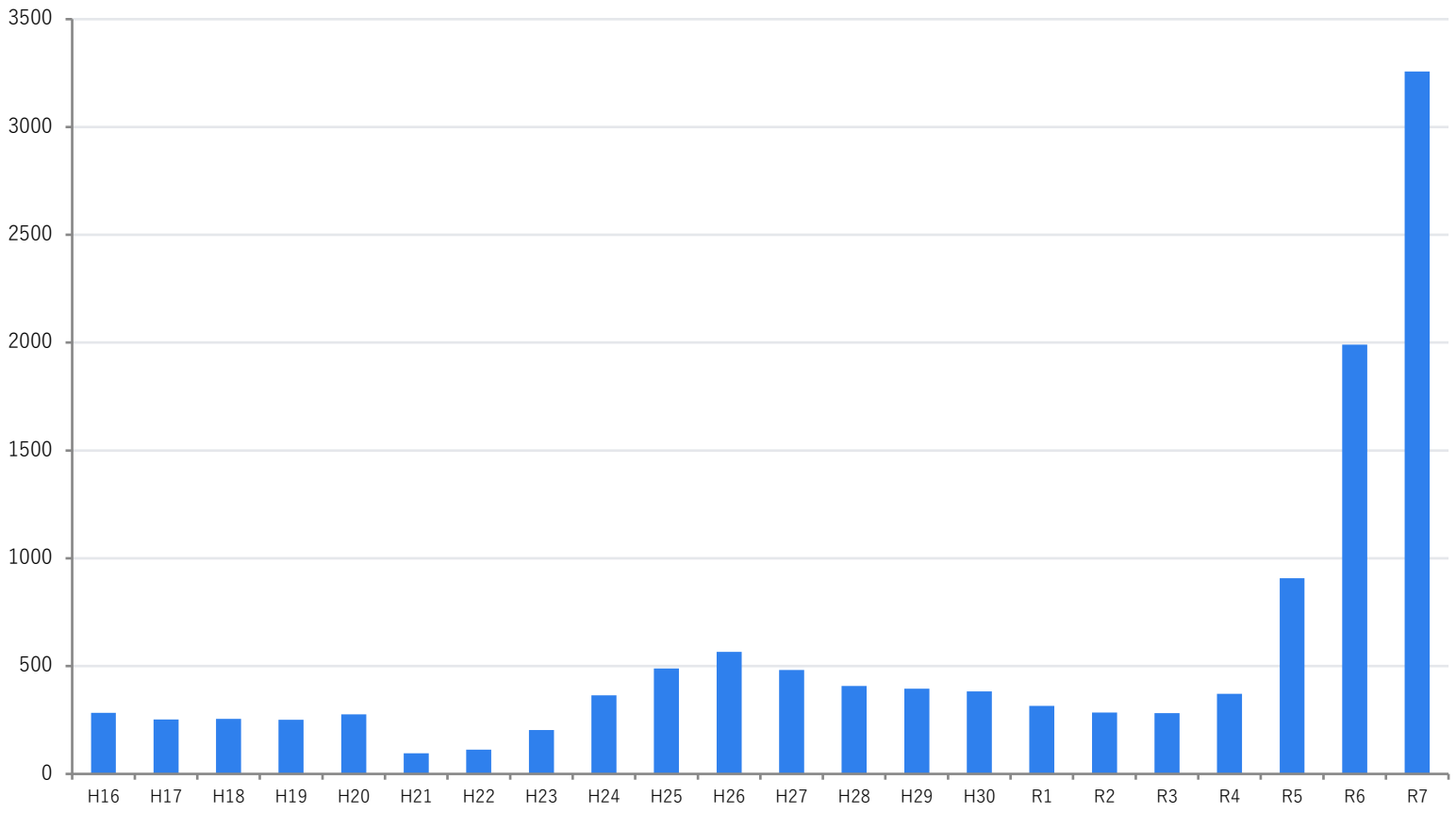
1	**数字で見るトクリュウ**	被害規模・凶悪化・スマホ化
2	**なぜ従来手法では限界か**	E2E暗号化・端末押収の時間差
3	**遠隔解析とは何か**	行政手続・非継続取得・被害防止
4	**要件・手続・歯止め**	司法審査・消去・通知・監督
5	**海外制度との比較**	英独などとの位置づけ
6	**民間企業・金融機関への影響**	情報管理と水際対応

01

数字で見るトクリュウ

特殊詐欺の急増、強盗への拡大、スマートフォン・闇名簿の実態を押さえる。

特殊詐欺被害額は、令和5年以降に急角度で跳ね上がった



3,257億円

令和7年中：過去最多

約8.8倍

令和4年371億円から令和7年まで

3年連続急増

R5 908 → R6 1,991 → R7 3,257

出所：警察庁資料3・10（特殊詐欺の被害状況）

令和8年上半期だけで、さらに前年同期を上回る

約1,816億円

令和8年上半期の特殊詐欺被害額

約10億円/日

1日当たりの被害額に換算

約12億円

9回にわたり詐取された個別事案も発生

示唆

- 被害は「件数」だけでなく、金額・継続性・巧妙性で深刻化している
- 単発の注意喚起ではなく、被害進行中の人を早く見つける必要がある
- 企業・金融機関の窓口対応にも「今日止める」時間感覚が求められる

出所：警察庁資料10 p.1

特殊詐欺は「長く・深く」被害者を追い込む

問題は、金額だけではない。
長期間の欺罔により、財産面・精神面の打撃が蓄積する。

- 9回にわたり総額約12億円をだまし取られる事案が発生
- 被害者は「だまされた」だけでなく、生活基盤・家族関係・自己責任感まで傷つく
- 制度目的は「検挙」だけではなく、悲惨な被害者を生まないことに置かれている

出所：警察庁資料10 p.1、提言骨子

トクリュウは、強盗・強盗殺人にも広がっている

18件

令和6年、南関東1都3県で連続発生した強盗事件

1名死亡・12件負傷

18件のうち死亡・負傷を伴った事案

55名／延べ85名

令和8年2月までの検挙状況

「詐欺対策」ではなく、生命・身体を守る治安対策へ

- 令和8年5月には、栃木県で高校生等を実行役とする強盗殺人事件も発生
- 指示役・上位指示役は秘匿性の高い通信アプリを使用
- スマートフォン上の犯行計画を、事前に把握できるかが被害防止の鍵になる

出所：警察庁資料10 p.1

犯行ツールはスマートフォンに集約されている

84台

特殊詐欺の連絡拠点で差し押さえられた連絡用スマートフォンの例

12台

投資詐欺事件のリクルーター1名が所持していたスマートフォンの例

闇名簿

氏名・住所・所得・保有銀行口座・家族構成などが記録されていた例

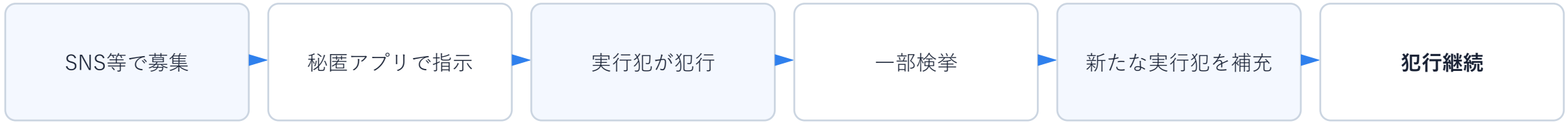
スマホの中身は、単なる会話ログではなく「標的リスト」「犯行計画」「資金移転先」である。

- E2E暗号化により通信経路・事業者側では内容が分からない
- しかし端末側には、復号後のメッセージや保存ファイルが残り得る
- この「端末に残る情報」を被害防止に使えるかが遠隔解析の発想

出所：警察庁資料10 p.3-4、資料3 p.7

トクリュウの構造：実行犯は入れ替わる、指示は残る

- 実行犯は「捨て駒」化し、検挙しても上位指示役や次の標的に届きにくい
- 固定組織ではなく、犯罪ごとに人員が流動的に組み替わる
- 「一件ずつ立件」では、同種犯行の反復・拡散を止めきれない



出所：警察庁資料3・8・10

被害防止は「時間との競争」になっている

約7か月

ホテル型「架け場」事案：検挙までに要した期間

約5か月

車両型「架け場」事案：検挙までに要した期間

捕まえるまでの間に、標的となった人々をどう守るか

- 警察庁資料は、検挙までの間に標的への被害防止措置をとることができなかったと整理
- 遠隔解析は、この「空白時間」を縮めるための制度として位置づけられる

出所：警察庁資料10 p.3

02

なぜ従来手法では限界か

通信事業者への照会、通信傍受、端末押収のどこに限界があるのかを整理する。

現行手法には、それぞれ「時間」と「技術」の壁がある

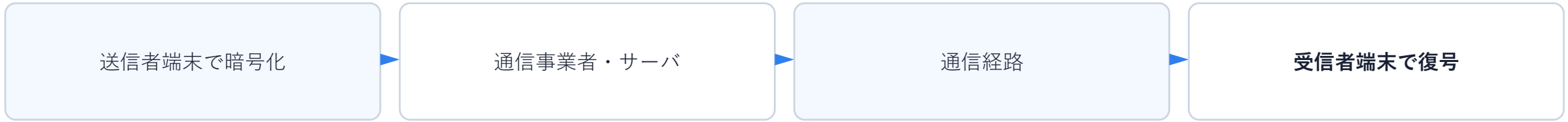
手法	何を取るか	トクリュウでの限界
電磁的記録提供命令	事業者が保管・管理する情報	E2E暗号化では事業者も内容を持たない
通信傍受	通信経路上の内容	経路上では暗号文のため中身が読めない
端末押収・解析	端末内の保存情報	押収まで時間、ロック・自動消去で被害防止に間に合わない

事業者を巻き込めば解決、という発想が通用しにくい

出所：警察庁資料3・10、提言骨子

E2E暗号化：通信経路上では「読めない」

通信事業者側でも、通信経路上でも、内容は暗号文の状態。



- E2E暗号化は一般利用者の安全に重要な技術である
- 一方で、トクリュウはその保護を犯罪の秘匿にも利用する
- 「通信を見る」のではなく「端末に保存された情報を見る」発想に移る

出所：警察庁資料3 p.4、資料10 p.4

E2E通信アプリの具体例：アプリ名だけでなく「仕様・設定」を見る

E2E暗号化は、利用者の通信を守る重要技術。問題は、匿名性・自動消去・多端末利用等と組み合わさり、犯行計画や標的情報の把握を難しくする点に

分類	代表例	実務上の見方
原則E2E型	**Signal / WhatsApp**	メッセージ・通話の本文を、事業者側で読みにくい。通信事業者への照会だけでは本文把握に限界が出る。
OS・標準機能型	**iMessage / FaceTime**	端末間通信がE2Eとなる場面がある。バックアップ・端末保存・削除設定など周辺仕様も確認が必要。
日本で身近な例	**LINE（Letter Sealing）**	対応範囲のメッセージは端末側で暗号化される。一般利用者にも広く浸透している点が実務上重要。
モード限定型	**Telegram（Secret Chats）**	通常チャットとSecret Chatで仕様が異なる。自動消去・匿名性・端末保存の組合せが捜査上の難所になる。
RCS等	**Google Messages 等**	利用者・端末・OS・キャリア・設定によりE2Eの有無が変わる。ロック表示等、実際の通信状態を確認する

ポイント：アプリ名で一括りにせず、「本文が事業者側で読めるか」「端末に何が残るか」「自動消去・匿名アカウントの有無」を見る。

出所：警察庁資料3 p.6、資料5 p.4、各社公表情報（Signal / WhatsApp / Apple / LINE / Telegram 等）

端末には、被害防止に直結する情報が残り得る

端末に保存され得る情報	被害防止上の意味
電話帳・発着信履歴	被害者・共犯者・連絡先の把握
アプリの友達リスト・送受信履歴	指示役・実行役・標的のつながりを把握
写真・文書・表計算ファイル	闇名簿、住所、自宅写真、集合場所等の把握

一方で、保存されていない通話音声などは対象にならない可能性がある。

出所：警察庁資料3 p.7

「秘匿性」と「匿名性」は分けて考える

秘匿性

やり取りの内容が把握できない

匿名性

やり取りを行う個人を特定できない

犯行内容を知ることと、実行者を知ることの両方が必要

出所：警察庁資料5 p.4

03

遠隔解析とは何か

行政手続として、保存データを一回の機会に取得し、被害防止につなげる制度。

遠隔解析の定義：端末から情報を把握し、被害防止に使う

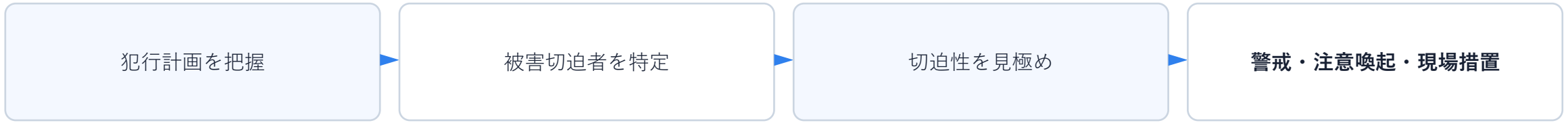
犯罪者グループの端末から、犯罪に悪用される通信アプリの通信内容等を迅速に把握し、被害防止に活用する手法

- 狙いは、被害が切迫している人を特定すること
- 通信傍受のように今後の通信を継続的に聞き続ける制度ではない
- 制度の詳細な技術的手法は、対抗措置防止のため情報保全が求められる

出所：提言骨子、警察庁資料9

目的は「被疑者の特定」より前に、「被害切迫者」を見つけること

- 犯人を直ちに特定・検挙できない段階でも、標的が分かれば被害防止は可能
- 強盗なら警ら・警戒、詐欺なら注意喚起・金融機関との水際対応などが想定される
- ここから民間企業・金融機関への接点が生まれる



出所：警察庁資料10 p.4、資料9 p.6

制度は「2階建て」で理解すると分かりやすい

1階：情報取得

遠隔解析により、端末内の被害防止情報を取得する

2階：被害防止

得た情報を使い、注意喚起・警戒・水際対応につなげる

民間が接する可能性が高いのは、主に2階の「被害防止」局面である。

出所：提言骨子「技術的措置」と「被害発生・拡大防止措置」を併せて整備

制度設計の軸：行政手続 × 非継続的取得

	保存されたデータを一回取得	流れる通信を継続取得
行政手続	遠隔解析（本案） 被害防止・危険防止が目的	外外通信目的送信措置など
刑事手続	差押え・電磁的記録提供命令・検証	通信傍受

「ずっと監視する制度ではない」ことが、制度正当化の重要な柱。

出所：警察庁資料3 p.8、提言骨子

なぜ刑事手続ではなく行政手続か

- 刑事手続は、基本的には起きた犯罪の真相解明・刑罰法令の適用を目的とする
- トクリュウでは、犯罪が成立する前・予備未遂にも達しない段階で介入すべき場面がある
- そこで「犯罪の予防・阻止」を目的とする行政調査権限として構成する考え方が採られている
- 根拠法としては、警察官職務執行法への規定が想定されている

問い：処罰のための資料収集ではなく、被害防止のための情報取得として設計できるか。

出所：提言骨子、警察庁資料8・9

遠隔解析に求められる3つの機能

密行性

犯人グループに察知されず実施

所在不明でも可

端末の場所が不明でも、端末が特定されていれば取得可能

被害防止情報

標的・日時・手口等を取得できる

「気づかれず」「端末に届き」「間に合わせる」ための制度

出所：提言骨子 p.3

取得対象は、被害防止に必要な情報に限られる

類型	想定される情報	意味
被害者特定情報	氏名、住所、自宅写真、電話番号	誰を守るべきかを特定する
犯行計画情報	日時、場所、手口、実行役人数、凶器	切迫性と現場対応を決める
詐欺関連情報	架電先リスト、欺罔方法、振込先	注意喚起・送金阻止・口座対策につなげる
強盗関連情報	役割分担、集合場所、標的住所	警戒・警ら・現場阻止につなげる

端末内の全情報を見る制度ではなく、被害防止目的で範囲を特定する制度。

出所：提言骨子 p.5、警察庁資料9 p.5

04

要件・手続・歯止め

強い権限をどう限定し、どう検証するか。制度の読みどころはここにある。

入口要件：6つのゲートを越えなければ実施できない

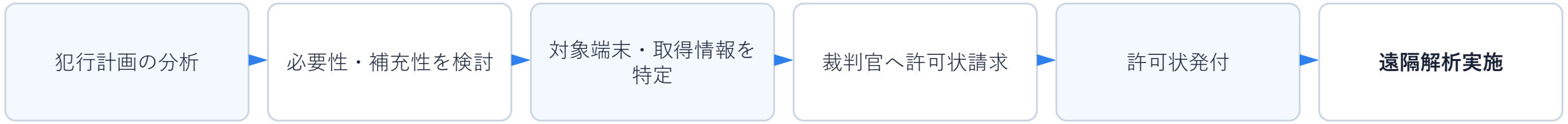
- 重大犯罪による被害であること
- 被害の発生・拡大について具体的なおそれがあること
- 犯人が使用すると合理的に認められる端末であること
- 取得情報が被害防止に必要な範囲に限られること
- 被害発生・拡大が差し迫っていること
- 他の方法では速やかな情報収集が困難であること

「便利だから使う」ではなく、「使わなければ間に合わない」場面に限定する。

出所：提言骨子 p.4-5

事前手続：裁判官の許可状が必要

- 対象端末は電話番号・IPアドレス等の何らかの方法で特定
- 取得する電磁的記録の範囲も、被害防止に必要な情報として特定
- 密行的措置であるからこそ、事前に司法審査を置く



出所：警察庁資料9 p.4、提言骨子 p.5-6

「継続的監視」ではないという限定が重要

対象は「権限行使時点で端末に記録されている電磁的記録のみ」

- 今後発生する通信を継続的に捕捉する通信傍受型とは異なる
- 保存データに対する非継続的措置として整理することで、制度の射程を限定
- 再実施の必要があれば、その都度要件・手続を満たす必要がある

出所：提言骨子 p.4、警察庁資料5 p.2

「必要な処分」とプレイン・ビュー問題

- 目的情報を探すためには、端末内データの確認・選別が必要になる
- 技術上、警察官側端末へ一時送信して確認する場面も想定される
- しかし、探索中に偶然見えた別情報を何でも使える制度にはできない
- 日本法では米国型の「プレイン・ビュー法理」は一般的制度として採られていない

鍵は、「探すために見る」ことと、「目的外に取得・利用する」ことを分けること。

出所：提言骨子 p.6、警察庁資料5 p.3

適正性を支える5つの歯止め

歯止め	内容
事前司法審査	全件について裁判官の許可状を取得
実施者の限定	専門的知識・能力を持つ警察官を警察庁長官が指名
不要情報の消去	許可範囲外の情報は消去し、他の警察官にも提供しない
事後通知	支障がない限り対象端末の使用者に通知し、救済の道を開く
公安委員会監督	全件報告・確認、必要に応じ是正措置

権限単体ではなく、歯止めとのパッケージで評価する。

出所：警察庁資料9 p.8、提言骨子 p.7-8

行政調査として構成しながら、実質は端末差押えに近い

ここが制度評価の一番おもしろいところ：目的は「被害防止」だが、手段は通信内容・端末内情報に強く踏み込む。

行政調査としての顔

- 目的は被疑者の処罰ではなく、被害切迫者への防止措置
- 犯罪成立前・予備未遂前でも、標的が分かれば保護が必要
- 根拠法は警察官職務執行法への新設が想定

強制処分に近い顔

- 本人に事前通知せず、端末内の通信内容等を確認
- スマートフォンは生活情報の集積体
- 骨子も「物理的な差押えと同程度」と位置づける

正当化のパッケージ

- 保存データの一回取得に限定
- 対象端末・取得情報を特定
- 裁判官の許可状
- 不要情報の消去・事後通知・公安委員会監督

問い

「差押えと同程度の強制処分」といいながら、差押え水準の要件で足りるのか。
この緊張関係を、目的限定・司法審査・事後統制でどこまで受け止められるかが争点。

出所：提言骨子 p.6-7（憲法31条・35条との関係、物理的差押えと同程度の強制処分との整理）

目的外利用との境界：入口目的と出口利用を混同しない

- 入口：遠隔解析は、犯罪被害の防止目的でのみ行使できる。捜査目的での行使は許されない
- 出口：被害防止目的で適法に取得した情報は、必要な刑事手続を経れば刑事手続で利用し得る
- 統制：目的、対象端末、取得範囲、分析担当への提供、刑事手続への移行経路を記録する
- リスク：「被害防止」を名目にした証拠収集に見えれば、制度全体の信頼性を損なう
- 実務上の鍵は、行使時の目的限定と、取得後の利用管理を別々に設計すること

出所：提言骨子 p.9（遠隔解析により得られた情報の活用の在り方）

今後の争点：制度設計よりも「運用」が問われる

- 差押え水準の要件で足りるか、通信傍受に近い厳格性が必要か
- 電話番号・IPアドレス等による端末特定で、憲法35条の特定性を満たすか
- 事後通知の例外が広くなりすぎないか
- 行政手続による通信の秘密の制限を、どこまで許容できるか
- 刑事手続への利用を、目的外行使に変質させない統制をどう置くか

制度成立後は、実施件数・対象犯罪・通知実績・監督実効性が検証ポイントになる。

05

海外制度との比較

類似制度は各国にあるが、目的・要件・審査・通知・監督の組合せは国ごとに異なる。

海外にも、端末から直接情報を取得する類似制度がある

国	根拠法令	主な性格
米国	連邦刑事訴訟規則	一定犯罪の捜査のための刑事手続
英国	調査権限法 第5部	重大犯罪等の予防を含む行政的制度
ドイツ	刑訴法／州警察法	刑事手続型と危険防止型が併存
フランス	刑事訴訟法	一定犯罪の捜査のための刑事手続
豪州	監視機器法	一定犯罪の捜査のための刑事手続

「外国にもある」ではなく、どの歯止めと組み合わせるかが重要。

出所：警察庁資料4 p.2

英国・ドイツ比較：共通するのは必要性・比例性・補充性

観点	英国	ドイツ（連邦・州）
目的	国家安全保障・重大犯罪対策	刑事訴追／公共安全・危険防止
必要性	必要性がある場合	他の方法では見込みがない又は著しく困難
比例性	比例原則あり	比例原則あり
補充性	他の手段では目的達成できない場合	他の方法では著しく困難な場合
事前審査	司法的機能を有する委員	裁判所

出所：警察庁資料4 p.3-5

日本案の位置づけ：危険防止型だが、司法審査を厚く置く

- 目的面では、犯罪予防・被害防止を重視する危険防止型
- 手続面では、行政手続であっても裁判官による事前審査を置く
- 実施後は事後通知と公安委員会監督を組み合わせる方向
- 行政の迅速性と、強制処分に近い慎重さを両立させようとする設計

制度比較の結論：日本案は「行政目的 × 司法統制」のハイブリッド。

出所：警察庁資料4・9、提言骨子

06

民間企業・金融機関への影響

遠隔解析の直接の名宛人ではない。しかし、被害防止の出口で民間実務と接続する。

民間企業は直接の実施主体ではない。しかし無関係ではない

遠隔解析を行う主体は警察。
民間企業に端末解析義務を課す制度ではない。

- ただし、被害防止措置の場面で、企業の顧客情報・連絡先・取引情報が関係する可能性がある
- 顧客名簿が犯罪者の標的リストになるリスクは、個人情報保護と犯罪被害防止の両方の問題
- 警察・行政からの緊急照会や協力要請に備え、窓口・判断権限・記録を整備する必要がある

出所：提言骨子「従来の事業者を巻き込む制度設計は十分に機能しにくい」

企業の顧客情報は、犯罪者から見ると「標的リスト」になり得る

- 高齢顧客、富裕層、相続・退職金、貸金庫、高額商品購入履歴、住所・家族構成
- 闇名簿では、所得・保有銀行口座・利用端末・会話状況まで記録されていた例がある
- 情報漏えいは、迷惑メールや詐欺電話だけでなく、強盗の標的選定に結びつき得る
- 情報管理は、コンプライアンスだけでなく顧客の生命・身体・財産を守る施策になる

問い：自社が持つ情報のうち、犯罪者が最も欲しがるものは何か。

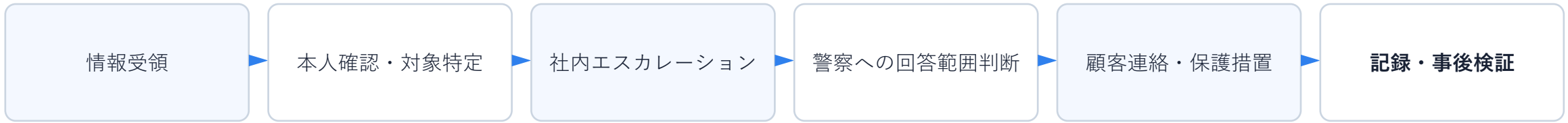
出所：警察庁資料10 p.3-4

民間企業の点検ポイント：外部攻撃だけでなく内部者・委託先も見る

観点	点検項目
アクセス権限	顧客情報・高リスク情報への閲覧権限を最小化しているか
異常閲覧	大量照会、深夜閲覧、退職予定者の閲覧を検知できるか
委託先	派遣・委託先の権限、再委託、ログ取得、返却・削除を管理しているか
緊急対応	警察から顧客保護の連絡が来た場合の窓口・判断者が決まっているか
記録	情報提供・拒否・顧客連絡の判断過程を残せるか

ケース：警察から「貴社顧客が標的」と連絡が来たら

- 誰が受けるか：営業拠点・コールセンター・法務・コンプラの窓口を一本化する
- 何を確認するか：顧客情報・連絡先・最近の取引や接点をどこまで確認するか
- 何を残すか：警察情報の内容、回答範囲、本人連絡、判断者、時刻を記録する



金融機関での意味：お金が動く直前が、最後の水際になる

遠隔解析は警察制度。
金融機関の焦点は「情報が来た後に何をするか」。

- 高齢顧客の高額出金・振込を、どのような根拠と手順で止めるか
- 加害側口座について、モニタリング強化・取引制限・凍結をどう判断するか
- 営業店任せにせず、本部・AML部門・法務・事務・システムを含めた業務フローが必要
- 「止めた理由」だけでなく「止めなかった理由」も説明できる記録が必要

金融機関の時系列対応：警察情報を実務に落とす

- 情報受領が「調査開始のトリガー」になる
- 共有情報だけで機械的に凍結するのではなく、自行情報と照合して判断する
- 同姓同名・法人名寄せ・関連口座の誤検知対応が重要
- 緊急時に回るよう、平時から権限者・様式・期限を決めておく

口座対策本体も動いている：2027年4月に向けた情報共有枠組み

- 犯収法施行規則改正により、犯罪・犯罪収益移転に利用又はそのおそれがある口座情報の提供・受領情報の整理分析等が努力義務化
- 監督指針でも、情報共有枠組みへの参加、情報提供、受領情報を用いたリスク低減策が明記
- 施行・適用は2027年4月1日

遠隔解析とは別制度だが、「外部情報を受けて、被害・犯罪を止める」流れは共通する。

出所：金融庁2026年6月26日公表資料、CAML公表資料

2027年4月までに作るべき「Who does what when」

問い	決めるべきこと
Who	受付者、一次判断者、凍結権限者、法務・AML・営業店の責任分界
What	名寄せ、取引確認、追加照会、モニタリング、制限・凍結、解除判断
When	日次受領、即時アラート、営業店連絡、当日判断、事後レビューの期限
Evidence	受領情報、照合結果、判断理由、顧客説明、警察対応、解除理由の記録

最も危ないのは、情報は来たが、誰も「自分の仕事」として動かない状態。

実務の難問：凍結する判断と、しない判断の両方を設計する

制度対応は「情報を受け取る」だけでは終わらない。最も難しいのは、短時間でリスク判断を行い、その判断を後から説明できる形にすること。

難問	実務で起きる場面	事前に決めること
共有情報だけで凍結できるか	警察・共同機構・他行情報はあるが、自行での裏付けは限定的	名寄せ確度、追加調査、凍結・制限・監視の判断基準
凍結しない場合の責任をどう見るか	情報は来たが、誤認リスクや顧客影響を踏まえ措置を見送る	判断権者、見送り理由、再検知条件、経営・本部報告ライン
誤認・解除・顧客説明をどうするか	同姓同名、法人名寄せ、親族・関連口座で誤検知が生じる	解除基準、本人説明、苦情対応、記録保存、免責条項の点検

講演での問い：口座を止めた理由だけでなく、「止めなかった理由」を監査・当局・顧客に説明できるか。

出所：不正利用口座情報共有制度・金融機関実務への示唆（講師整理）

まとめ：遠隔解析を、制度論と組織実務の両面から読む

- トクリュウ対策の核心は、事後処罰から事前阻止への転換である
- 統計は、被害額・凶悪化・スマホ化・闇名簿化の全てで危機水準を示している
- 遠隔解析の制度評価では、行政調査としての目的と、端末差押えに近い強制性との緊張関係が重要になる
- 取得情報は、入口では被害防止目的に限定し、出口では刑事手続利用との境界管理が問われる
- 民間企業は、顧客情報を「犯罪者が欲しがる情報」として再評価すべきである
- 金融機関は、凍結する判断・しない判断・解除する判断の全てを説明できる業務フローを作る必要がある

最後の問い：今夜、警察から「御社のお客様が標的」と連絡が来たら、誰が何を判断し、何分後に動けるか。

参考URL｜警察庁「匿名・流動型犯罪グループによる犯罪被害対策のための技術的措置に関する有識者検討会」資料掲載ページ
https://www.npa.go.jp/bureau/soumu/kentoukai/shiryou.html