2026年9月・最終提言

トクリュウ対策の新段階
「遠隔解析」は何を変えるのか

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提言を読む

被害防止 × 通信の秘密 × 司法審査 × ガバナンス

YouTubeウェビナー｜あたらしい法律情報
弁護士法人三宅法律事務所　弁護士 渡邉雅之

まず、この数字から

令和7年 特殊詐欺被害

3,257億円

過去最悪。

令和8年上半期

1,816億円

前年同期をさらに上回る。

1日あたり

約10億円

被害が進行。

「被害後に犯人を追う」だけでは、被害の速度に追いつかない。

9回にわたり総額約12億円をだまし取られた事例も。

出典：提言1頁

9月24日、最終提言まで到達

8/10	8/26	9/2	9/9	9/24
論点提示	海外制度	骨子	取りまとめ議論	最終提言

「制度を作るべきか」から、対象・要件・司法審査・情報消去・通知・監督をどう組み合わせるかへ。

出典：提言 参考資料2

今日の地図：遠隔解析を6つの問いで読む

WHY

なぜ必要？
時間差／E2E暗号化

WHAT

何をする？
保存データを遠隔取得

WHO

誰が対象？
重大犯罪の犯人端末

WHEN

いつ使える？
蓋然性・緊急性・補充性

HOW

どう手続？
裁判官の事前許可

CHECK

誰が監督？
事後通知＋公安委員会

出典：提言・概要を基に作成

従来手法が詰まる3つの壁

壁1 | 物理捜査の時間差

犯行拠点を転々とする例では検挙まで約5〜7か月。その間、標的への直接的な被害防止が難しい。

壁2 | E2E暗号化

通信事業者のサーバや通信経路上では暗号文。事業者の協力があっても内容解明が困難。

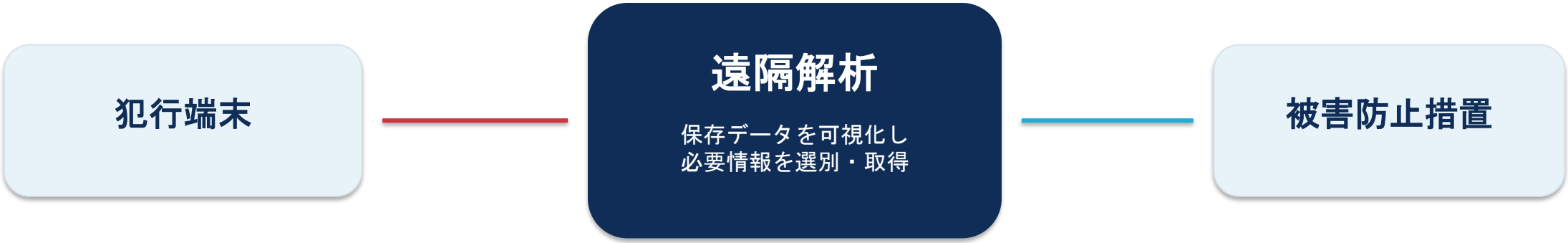
壁3 | 端末押収の限界

押収まで時間を要し、画面ロックや自動消去もある。迅速な被害防止に間に合いにくい。

だから「端末を押収する前」に、切迫する被害情報へ到達する仕組みが必要になる。

出典：提言 3〜5頁

遠隔解析とは何か



生成されるデータを継続監視する制度ではなく、権限行使時点で端末に記録されているデータを対象とする「非継続的措置」。

出典：提言 8〜9頁

刑事捜査ではなく「被害防止の行政調査」

刑事手続

目的：犯人の訴追・処罰
中心：成立した犯罪の証拠収集
限界：犯罪成立前の被害防止には手段が限られる

遠隔解析＝行政手続

目的：切迫する重大犯罪の予防・阻止
対象：被害防止に必要な情報
法制：警察官職務執行法への規定を想定

「行政調査だから軽い」ではない。強制性が高いため、司法審査を組み込む。

出典：提言8頁

対象・情報・タイミングを絞る

対象者

重大犯罪の犯人が使用すると合理的に認められる端末。無関係な第三者端末への拡張を排除。

対象端末

指示役と実行役、犯人と被害者の連絡に用いられ、被害防止情報が保存されている蓋然性が高い端末。

対象情報

被害切迫者の氏名・住所・自宅写真、犯行日時、実行役人数、凶器など。

出典：提言9〜10頁

遠隔解析の「4つのゲート」

1	**具体的なおそれ**	重大犯罪の被害発生・拡大が具体的に懸念される。
2	**犯人端末への限定**	対象者・対象端末を合理的に特定する。
3	**緊急性**	重大犯罪の被害が差し迫り、緊急の職務執行が必要。
4	**補充性**	他の方法では速やかに必要情報を収集できない。

出典：提言9〜10頁

司法審査：全件、事前に裁判官へ

① 警察

必要性・端末・取得情報を特定

② 裁判官

要件・特定性を事前審査

③ 許可状

電話番号・IP等で端末を特定

④ 実施

許可範囲で情報を選別・取得

憲法35条の「特定性」を意識し、対象端末と取得する電磁的記録の範囲を事前に絞り込む。

出典：提言11頁

実施時に何ができるのか

アクセス

犯行グループが使用する端末に、察知されない形でアクセス。

確認・選別

端末内データを可視化し、被害防止に必要な情報を探す。

複写・取得

許可状の範囲で必要情報を取得。技術上必要なら一時的送信も想定。

許可対象外の情報は「見つけたら使う」のではなく、原則として消去する。

出典：提言11頁・概要4頁

他の犯罪データを偶然見つけたら？

例：別犯罪の証拠を発見

遠隔解析中に、許可対象とは別の犯罪への関与を示すデータを発見した場合でも、それだけを理由に直ちに証拠保全することは許されないとの整理。

なぜ？

日本には米国のプレイン・ビュー法理に相当する一般的な無令状緊急差押え規定がない。別の法的根拠・手続が必要。

強い権限だからこそ、「目的外利用をしない」ことが制度の信頼性を支える。

出典：提言 16頁

憲法上の核心：通信の秘密とプライバシー

憲法13条

端末内の私的情報・プライバシーへの制約。目的と手段の比例性が必要。

憲法21条2項

秘匿性の高い通信アプリの内容は「通信の秘密」に関わる。

憲法31条・35条

適正手続・令状主義の要請。行政手続でも強制性が高いため事前司法審査を採用。

提言の発想：実体要件＋手続規律＋ガバナンスをセットにして、人権制約を必要最小限にする。

出典：提言7・11〜12頁

GPS判決との違いは「継続性」

GPS捜査

車両等にGPS端末を取り付け、継続的に位置情報を把握。最高裁は立法措置を求めた。

今回の遠隔解析

保存データを一の機会に取得する非継続的措置として構成。事後通知等の適正性担保措置を法定する方向。

ただし「非継続」と言っても、必要限度を超えて長時間接続し続ける運用は許されない。

出典：提言17頁

適正性担保：5層のガードレール

①	**厳格な要件＋司法審査**	高度な蓋然性、緊急性・補充性、犯人端末への限定。
②	**担当官の限定**	専門知識・能力を持ち、警察庁長官が指名した警察官。
③	**情報の消去**	許可対象外情報は全て消去し、他の警察官にも提供しない。
④	**事後通知**	被害防止に支障がある場合等を除き、対象端末使用者へ通知。
⑤	**公安委員会**	全件を事後確認し、必要に応じ是正措置。

出典：提言13〜14頁・概要7頁

遠隔解析担当官と被害防止担当を分ける

遠隔解析担当官

- 高度な専門知識
- 警察庁長官が指名
- 許可範囲の情報だけを取得

必要な
情報だけ

分析・被害防止担当

- 必要情報を受領
- 被害切迫性を分析
- 現場警察へ指揮・警戒

権限分離は、内部統制としても重要。『取れる人』と『使う人』を分ける。

出典：提言 13頁

事後通知：密行性と権利救済をどう両立するか

原則

対象端末の使用者に、権利保護に必要な事項を遅滞なく通知。
違法な処分があった場合の救済ルートを確保する。

例外

通知により被害防止に支障が生じる場合、通知先が不明な場合等は例外。支障がなくなれば速やかに通知。

「秘密に実施する権限」だからこそ、事後的な可視化が重要になる。

出典：提言13・17頁

公安委員会が全件を事後確認

全件報告

遠隔解析を実施した警察官は、所属の公安委員会に悉皆的に報告。

確認・是正

必要があれば、公安委員会が具体的な是正措置をとれる仕組み。

専門性・透明性

外部専門家の補助、個人情報保護委員会との連携、実施状況の公表も論点。

提言は「監督機関を置けば終わり」ではなく、監督能力と透明性まで問題にしている。

出典：提言 14・17〜18頁

取得情報は刑事手続でも使えるのか

権限行使の目的

遠隔解析そのものを犯罪捜査目的で行使することは不可。あくまで犯罪被害防止が目的。

取得後の利用

適正に取得した情報は、刑事訴訟法等の必要な手続を経て刑事手続で利用することは許容され得る。

「目的外の権限行使」は禁止。しかし「適法に得た情報の二次利用」は別問題として整理。

出典：提言14頁

技術的手法：脆弱性利用まで射程に

技術上の現実

強固な暗号化があると、通信事業者でもメッセージ閲覧は事実上困難。

提言の議論

端末の脆弱性を突く、端末利用者を欺罔する手段を用いざるを得ない場面も想定。

安全との緊張

被害防止のために国民の安全を逆に脅かさないよう、運用統制と情報保全が必要。

具体的手法は秘匿性が高い一方、取得情報が『本当に対象端末由来か』を事後検証できる仕組みも必要。

出典：提言17頁

国外にある端末はどうする？

制度設計

端末が海外に所在する場合も対象となり得る制度を検討。ただし執行管轄権・主権侵害の問題が生じる。

運用の基本

関係国との協力関係の下で権限を執行し、相手国の同意を得ることが基本との意見。

トクリュウが国境を越える以上、遠隔解析も国際捜査協力・国際法の問題になる。

出典：提言19頁

海外制度も参照：英国・ドイツ

英国

調査権限法（Investigatory Powers Act）など、端末への技術的干渉を含む制度が参考対象。

ドイツ

刑事訴訟法やバイエルン州警察法の制度が検討会で紹介。予防警察法制との比較も重要。

日本案の特徴は、被害防止の行政権限として警察官職務執行法に置く方向を明確にした点。

出典：提言 7頁 注1

提言の制度を1枚で見る

① 情報分析

重大犯罪の高度な蓋然性
緊急性・補充性

② 司法審査

対象端末・取得情報を特定
裁判官が許可

③ 遠隔解析

保存データを確認
必要情報のみ取得

④ 被害防止

被害切迫者を特定
警戒・警ら・防犯指導

横断ガードレール：担当官限定｜対象外情報消去｜事後通知｜公安委員会の全件監督

出典：提言概要2〜7頁を基に再構成

企業実務への示唆①：通信・プラットフォーム

本人確認・端末

SIM・番号・アカウントの不正取得、名義貸し、異常な大量登録を検知・停止。

闇バイト・広告

募集投稿、詐欺広告、匿名連絡アプリ誘導を複合シグナルで監視。

ログ・照会対応

警察照会に対応できるログ保全、社内窓口、法的根拠の確認を整備。

遠隔解析が導入されても、民間の『犯罪インフラを使いにくくする』役割はむしろ重要になる。

出典：提言を踏まえた実務上の整理

企業実務への示唆②：金融・決済

Detect

高額・反復・新規宛先・第三者指示など、被害の赤信号を拾う。

Stop

送金保留、追加確認、冷却時間、上席承認など『止める権限』を現場へ。

Connect

警察、被害者、他金融機関との迅速な連携。犯罪収益移転と被害拡大を同時に止める。

被害切迫情報を警察が得られる世界では、金融機関側の即応速度も一層重要になる。

出典：提言を踏まえた実務上の整理

企業実務への示唆③：プライバシー・ガバナンス

目的限定

『安全のため』を万能な理由にしない。目的と利用場面を明確化。

最小化・権限分離

必要なデータだけを扱い、取得者・分析者・意思決定者の権限を分ける。

監査可能性

ログ、削除、事後レビュー、外部チェックで『なぜこの処理をしたか』を説明可能に。

遠隔解析の制度設計は、企業の高リスクデータ利用・AIガバナンスにもそのまま応用できる。

出典：提言を踏まえた実務上の整理

今後の立法で注目する5点

1. 対象犯罪の具体的範囲
2. 『高度な蓋然性』『緊急性』の条文化
3. 許可状の特定性・再度実施の扱い
4. 事後通知・実施状況公表の例外
5. 公安委員会の専門性と外部チェック

出典：提言 19〜20頁を基に整理

経営・法務向けチェックリスト

- [ ] 自社サービスが犯罪インフラのどこで悪用され得るかを整理したか
- [ ] 不審な端末・アカウント・送金・募集投稿の赤信号を定義したか
- [ ] 現場が一時停止・上席エスカレーションできる権限を持つか
- [ ] 警察照会・緊急連携の窓口と証跡保存ルールがあるか
- [ ] 個人情報・通信情報の目的限定、最小化、アクセス権限を定めたか
- [ ] 重大事案を経営・取締役会へ上げるガバナンスがあるか

出典：提言を踏まえた実務上の整理

まとめ：『被害成立前の遮断』へ

トクリュウ対策は、
「被害後の摘発」だけから「被害成立前の遮断」へ。

遠隔解析

犯行端末から切迫する被害情報を取得

司法審査

強い権限を事前に裁判官がチェック

ガバナンス

消去・通知・公安委員会監督で適正性を担保

核心は「警察が端末を見ること」ではなく、「次の被害者を救うこと」。

出典：有識者検討会「提言」（令和8年9月）