

2026年10月16日 閣議決定・国会提出

遠隔解析法案

警察はスマホの「何を」見るのか？

警察官職務執行法改正案(新8条・新9条)を条文で読む

弁護士法人三宅法律事務所 弁護士 渡邊 雅之

出典:警察庁「国会提出法案」(第222回国会・令和8年10月16日提出)<https://www.npa.go.jp/laws/kokkai/index.html>

今日の問い

明日から、警察は あなたのスマホを見られる？

答え：普通の人々のスマホは対象外。3つの限定がある

① 誰の端末か

犯人が連絡に使ったと認める
合理的な理由のある端末だけ

② 何を取るか

次の被害者の氏名・住所、犯行
の日時など

③ どんな手続か

実施前に必ず裁判官の許可。
例外なし

今日の結論は3つ

① 目的は「捜査」ではなく「次の被害者を守る」

「犯罪捜査のために認められたものと解してはならない」と明記(9条11項)

② 強い権限を「5つの歯止め」で縛る

裁判官の事前許可・範囲外データの消去・事後通知・公安委員会の確認・捜査転用の否定(9条3項～11項)

③ 残る課題は「透明性と運用」

実施状況の公表や国会への報告の規定は置かれていない

被害は「過去最悪」を更新し続けている

財産犯の被害(2025年)

4,983億円

6年連続で増加。2002年の
3,758億円を超えた

特殊詐欺の被害(令和7年)

3,257億円

過去最悪

特殊詐欺(令和8年上半期)

**約1,816億
円**

1日あたり約10億円のペース

実行役は「捨て駒」。捕まえても、指示役と「次の標的」にはたどり着けない

2026年5月、栃木県上三川町で60代の女性が犠牲になる強盗殺人事件。警察庁長官は「まさに異常事態」(10月13日)

今の捜査手段が詰まる「3つの壁」

① 暗号化の壁

エンドツーエンド暗号化のアプリは、通信経路でも事業者のサーバでも暗号文。通信傍受をしても読めない

② 時間の壁

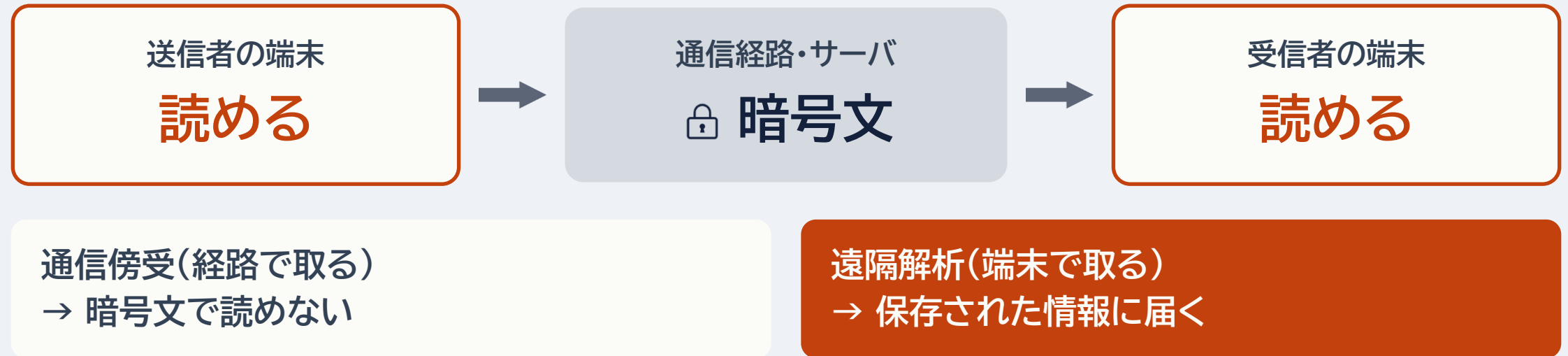
拠点を転々とするグループでは、検挙まで約5～7か月かかった例も。その間、標的を守れない

③ 押収の壁

押収まで時間がかかり、画面ロックや自動消去も。被害防止に間に合わない

だから「端末を押収する前に」被害の情報に届く仕組みが要る

暗号は「端末の中」では解かれている



法案は「2本柱」でできている

新8条

被害を防ぐ措置＝
警察官の「義務」

重大犯罪の被害が迫る人を、直ちに守らなければならない



情報を提供
(9条7項)

新9条

被害防止電子計算機調査
(いわゆる遠隔解析)

8条の義務を果たすための「情報を集める手段」

その他:今の8条は10条へ繰り下げ／3条・5条は表記の現代化(「すみやかに」→「速やかに」、「虞」→「おそれ」)／6条の2(能動的サイバー防御)の定義を9条でも使えるよう調整

仕組みを1枚で: 7つのステップ

①

現場の警察官が資料を
調査官へ

9条2項

②

調査官が重大犯罪の発
生・着手を確認

9条2項

③

裁判官が許可状を出す

9条3項・4項

④

犯人の端末に接続し、複
写・取得

9条2項

⑤

許可範囲の情報だけ現
場へ

9条7項

⑥

現場で警戒・指揮

8条

⑦

詐欺電話・強盗を阻止

8条

ポイント

「取る人」と「使う人」を
条文で分けている

5条との違いと、8条の位置づけ

現行5条

犯罪が「正に行われようとする」とき
警告と、急を要する場合の制止
＝目の前の犯罪

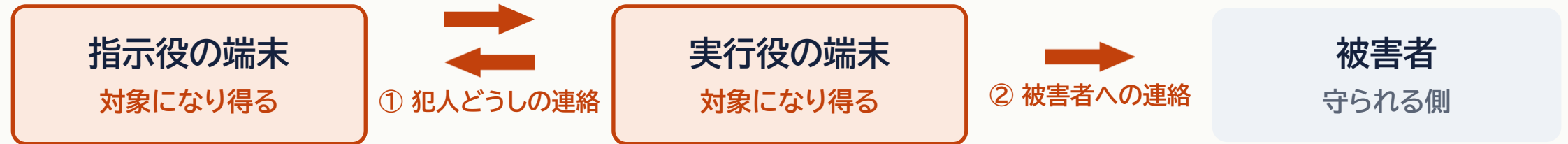


新8条

犯罪が既に行われた・着手された段階から
次の被害者を特定して守る
＝トクリュウの「次の標的」

- ・8条の各号は、9条の発動条件にそのまま引用される(9条2項2号)→ 8条が遠隔解析の「入口」
- ・8条が例示するのは「方法の指導」。新たな強制権限ではない。強い権限は9条にまとめられている

対象は「犯人が連絡に使った端末」



- ・「連絡に用いたと認める合理的な理由」が必要。回線につながる「電子計算機」で、PCも入り得る(9条2項)
- ・実施できるのは、警察庁長官が指名した調査官だけ(9条1項)。現場の警察官は接続せず受け取るだけ(9条7項)
- ・通知の相手は所有者ではなく「使用者」。名義貸し・他人名義の端末も想定(9条8項)

取れるもの・取れないもの

☑ 取れる

- ・被害切迫者の氏名・住所
- ・犯行が行われる日時
- ・その他、被害防止措置に必要な事項(9条2項)
- ・そのための接続・複写・取得と「必要な処分」(同項後段)

⚠ 取れない

- ・これからの通信のリアルタイム傍受(対象は端末に「記録された」データ)
- ・許可状の範囲を超える取得(9条4項)
- ・範囲外データの利用・提供(9条6項)

端末の中身を「丸ごと」見る制度ではない

3つのゲートを全部通らないと使えない

前提:現場の警察官からの資料で、重大犯罪の発生・着手を確認していること

① 組織性(1号)

数人の共謀で行われた・着手された
と合理的に認められる

→ 単独犯は対象外

② 緊急性(2号)

8条1号・2号に当たり、被害を防ぐ
緊急の必要がある

→ 8条が入口

③ 補充性(3号)

他の方法では、必要な情報をすぐ集めるのが「著しく」困難

→ 最後の手段

「便利だから使う」ではなく「使わないと間に合わない」ときだけ

裁判官の許可:申請から許可状まで

申請書に書く4項目(9条3項)

- ① 実施できる場合に当たる理由
- ② 対象の端末と、その理由
- ③ 取得するデータの範囲
- ④ 行為の具体的内容と手順

許 可 状 (9 条 4 項)

- ・対象の端末
- ・取得するデータの範囲
- ・許可の有効期間
- ・発付の年月日・裁判所名
- ・裁判官の記名押印

- ・許可するのは、警察本部等の所在地を管轄する地方裁判所か簡易裁判所の裁判官
- ・必ず「あらかじめ」。緊急時に事後承認で済ませる例外はない
- ・技術的な「手順」まで審査し、端末だけでなくデータの範囲も特定させる(憲法35条の特定性)

強盗の「次の標的」を守る

- 1 指示役Xの下で、実行役Aらが住宅強盗。Aが逮捕される
- 2 Aのスマホのやり取りは自動消去。ただしXの連絡先につながる番号は判明
- 3 Xが近く「次の家」を狙うと判断できる具体的な事実がある(8条2号)
- 4 調査官が許可状を得て、Xの端末から次の標的の住所・日時を取得(9条2項～4項)
- 5 現場の警察官が住人に注意を呼びかけ、周辺を重点警戒(8条)

事後、端末の使用者に通知。ただし被害防止の妨げになるおそれがあれば、なくなってから(9条8項ただし書)

見すぎたら？「渡さない・消す」

渡さない

範囲外のデータ・情報は、現場の警察官を含め誰にも提供禁止

9条6項前段

消す

調査が終わったら、国家公安委員会規則に従い直ちに全部消去

9条6項後段

範囲内だけ

許可の範囲内で取得したデータだけを現場へ提供

9条7項

+ 実施にあたり、関係者の正当な業務をみだりに妨げてはならない(9条5項)

「探すために見る」と「目的外に取って使う」を切り分ける

事後通知：秘密に実施するからこそ

原則：遅滞なく使用者へ通知する6項目

① 端末を特定する事項

② 罪名

③ 許可状の発付日

④ 実施した日

⑤ 取得データを特定する事項

⑥ 消去した日

例外

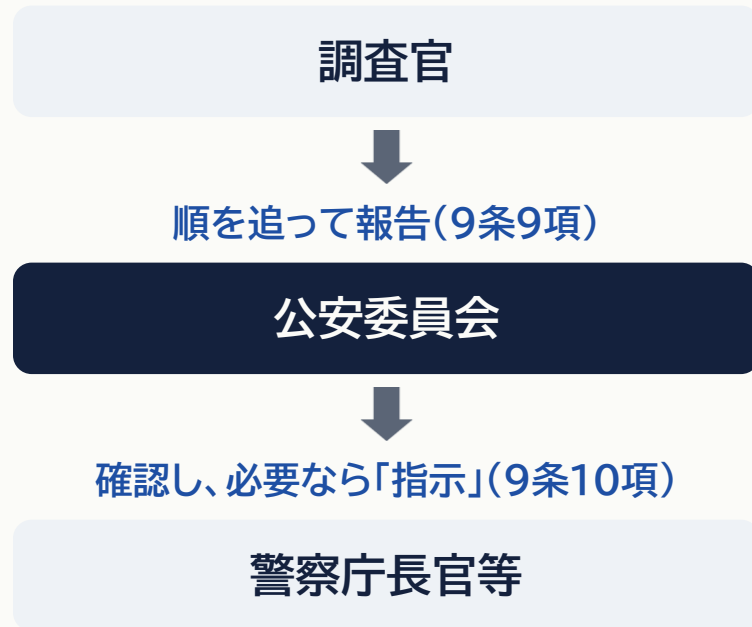
使用者の所在が分からないなど、通知が難しい場合

先送り

被害防止の妨げになるおそれ → おそれがなくなった後、速やかに

通知があって初めて、違法な実施を争う手がかかりができる

公安委員会のチェックと「捜査ではない」条項



9条11項

「被害防止電子計算機調査等の権限は、犯罪捜査のために認められたものと解してはならない」

国税通則法74条の8など、行政調査で使われる定番の条項と同じ形。捜査目的で権限を使うことを禁じる

憲法から見ると、どこが論点か

13条(プライバシー)

スマホは生活情報の集積。目的と手段のつり合いが問われる

21条2項(通信の秘密)

秘匿性の高いアプリのやり取りの中身にまで及ぶ

35条(令状主義)

行政手続でも保障が及び得る(川崎民商事件・最大判昭和47年11月22日)→ 裁判官の事前許可を採用

GPS判決(最大判平成29年3月15日)

GPS捜査は令状を要する強制処分で、立法的措置が望ましいとした → 法律で要件と手続を定めるルート

争点:「差押えと同程度」とされる強い権限を、この要件で受け止められるか

通信傍受・能動的サイバー防御と比べる

観点	通信傍受	能動的サイバー防御(6条の2)	遠隔解析(新9条)
性格・対象	刑事手続。これからの通信	行政手続。サイバー攻撃に使われる機器	行政手続。端末に保存されたデータ
事前チェック	地方裁判所の裁判官の令状(通信傍受法4条1項)	監理委員会の承認。緊急時の例外あり(4項)	裁判官の許可(地裁か簡裁)。例外なし(3項)
事後チェック	国会へ報告(同法36条)	監理委員会が「勧告」(10項)	公安委員会が「指示」(10項)。国会報告・公表の規定なし
自衛官への準用	—	あり(自衛隊法91条の3など)	なし(附則2項)＝警察だけの権限

よくある誤解Q&A

Q1 普通の人のスマホも？

原則No。犯人が連絡に使った端末に限る(9条2項)

Q2 メッセージは全部読まれる？

No。許可状で特定した、被害防止の情報の範囲だけ(9条2項・4項)

Q3 通話を盗聴される？

No。対象は端末に記録されたデータ。リアルタイム傍受ではない

Q4 別の犯罪の証拠は使われる？

範囲外は誰にも渡さず、直ちに消去(9条6項)

Q5 取った情報で逮捕できる？

捜査目的の行使は否定(9条11項)。刑事手続での利用は条文に規定なし

Q6 調べられたら知られる？

原則、事後に通知。ただし例外と先送りあり(9条8項)

前回の「5つの宿題」、法案の答え

論点	法案の答え	残った点
① 対象犯罪	罪名の列挙なし。抽象的な定義＋共謀の要件(8条・9条2項1号)	「財産に重大な損害」の線引き
② 蓋然性・緊急性	合理的判断・具体的事実・緊急の必要・補充性を明記(8条・9条2項)	運用での具体化
③ 許可状の特定性	端末・範囲・手順・有効期間を記載(9条3項・4項)	再実施の扱いは明文なし
④ 通知・公表	事後通知を明文化(9条8項)	公表・国会報告の規定なし
⑤ 公安委員会	報告・確認・指示(9条9項・10項)	外部専門家の関与なし

ほかに注目:簡易裁判所でも許可可(通信傍受は地裁)／「必要な処分」の中身(脆弱性の利用? 秘匿と事後検証の両立)／通知の例外・先送りの運用と争い方

警察の情報を実務に落とす7ステップ

①

警察から情報を受け取る

②

顧客・口座を特定(名寄せ)

③

取引履歴・予定を確認

④

営業店・顧客へ連絡

⑤

振込・出金の保留、監視の強化

⑥

制限・凍結を判断

⑦

記録を残し、事後に検証

注意

機械的に止めず、自行情報と照合。同姓同名の誤認に注意

今日のまとめ

① 遠隔解析＝「次の被害者」の情報を取る権限

犯人が連絡に使った端末から、被害を防ぐ情報だけを取る行政上の権限(8条・9条)

② 強い権限を「5つの歯止め」でパッケージ化

事前許可(3項・4項)・消去(6項)・通知(8項)・公安委員会(9項・10項)・捜査転用の否定(11項)

③ 残る論点は「透明性と運用」

国会審議と国家公安委員会規則に注目。民間は「出口」での即応体制を

最後に、ひとつだけ問いを

今夜、警察から
「御社のお客様が標的です」と
連絡が来たら——
誰が、何分で動けますか？

チャンネル登録をお願いします | あたらしい法律情報

弁護士 渡邊 雅之