

法務・コンプライアンスニュース 令和8年 10 月 16 日号

警察はスマホの「何を」見るのか？

遠隔解析法案(警察官職務執行法改正案)の解説

— 令和8年 10 月 16 日閣議決定・第 222 回国会提出の法律案を、条文で読む —

平素より大変お世話になっております。

本日(令和8年 10 月 16 日)、匿名・流動型犯罪グループ(以下「トクリュウ」といいます。)による特殊詐欺や強盗の被害を防ぐため、スマートフォン等の端末にアクセスして情報を取得する「遠隔解析」を導入する、警察官職務執行法の一部を改正する法律案(以下「**本法案**」といいます。)が閣議決定され、第 222 回国会(臨時)に提出されました¹。報道では「警察がスマホの通信内容を把握する」と伝えられており²、「自分のスマホも見られるのか」という不安の声も聞かれます。

結論を先にいえば、本法案が定める遠隔解析は、**犯人が連絡に使った端末から、次の被害者を守るために必要な情報だけを、裁判官の事前の許可を得て**取得する制度であり、一般の方の端末を自由に見られるようにするものではありません。他方で、強い権限であることは確かで、実施状況の公表や国会への報告の規定が置かれていないなど、運用面の課題も残されています。

本号では、法律案の条文・要綱・新旧対照条文・概要を読み、①制度の仕組み、②歯止めの内容、③他の制度との違い、④国会審議の注目点、⑤企業・金融機関の実務への示唆を、できるだけ平易に整理しました。9月に公表された警察庁有識者検討会の提言³の内容との対応関係にも触れています。本号が、今後の国会審議の理解と、社内での準備の一助となれば幸いです。

令和8年 10 月 16 日

弁護士法人三宅法律事務所

* 本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。

弁護士法人三宅法律事務所

弁護士 渡邊雅之(執筆者)

TEL 03-5288-1021 FAX 03-5288-1025

Email: m-watanabe@miyake.gr.jp

¹ 警察庁「国会提出法案」(警察官職務執行法の一部を改正する法律案:要綱、案文・理由、新旧対照表、参照条文、参考資料。第 222 回国会(臨時)、令和8年 10 月 16 日提出)(<https://www.npa.go.jp/laws/kokkai/index.html>)。以下、条文・要綱・概要の記載は同資料による。

² 日本経済新聞「トクリュウのスマホ遠隔解析、被害 5000 億円の抑止なるか 法案閣議決定」(令和8年 10 月 16 日)。

³ 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・提言(令和8年9月)(<https://www.npa.go.jp/bureau/soumu/kentoukai/shiryoku.html>)。

警察官職務執行法改正案(遠隔解析)の解説

— 令和8年 10 月 16 日閣議決定・第 222 回国会提出の法律案を、条文で読む —

【目次】

- 1 まず結論——本法案のポイント3つ
- 2 背景——なぜ今、遠隔解析なのか
- 3 法案の全体像——「2本柱」と条文の構成
- 4 新8条——被害切迫者を守る「義務」
- 5 新9条——誰の端末から、何を、どんな条件で取れるのか
- 6 歯止めの仕組み——許可・消去・通知・監督
- 7 他の制度との比較——通信傍受・能動的サイバー防御
- 8 提言から法案へ——決まったこと・残ったこと・国会審議の注目点
- 9 実務への示唆——今から着手すべき事項

1 まず結論——本法案のポイント3つ

- 目的は「捜査」ではなく「次の被害者を守る」こと——遠隔解析の権限は「犯罪捜査のために認められたものと解してはならない」と明記されています(新9条 11 項)。
- 対象は「犯人が連絡に使った端末」で、取れるのは「被害防止に必要な情報」だけ——被害を受けるおそれのある人の氏名・住所、犯行の日時などに限られます(新9条2項)。
- 強い権限を、5つの歯止めで縛る——裁判官の事前許可、許可範囲外のデータの提供禁止・消去、使用者への事後通知、公安委員会による確認・指示、捜査目的での行使の否定です(新9条3項～11 項)。

一方で、通信傍受法のような国会への報告(同法第 36 条⁴)に当たる規定は、本法案にはありません。この点を含め、制度の「透明性」と「運用」が今後の焦点になります。

(1) よくある疑問への答え

疑問	答え(根拠条文)
普通の人のスマホも見られる？	原則として対象外です。犯人が犯人間の連絡や被害者への連絡に用いたと認める合理的な理由のある端末に限られます(新9条2項)。
メッセージを全部読まれる？	読まれません。取得できるのは、許可状で特定された「被害防止措置用情報」に係る電磁的記録の範囲だけです(新9条2項・4項)。
通話を盗聴される？	盗聴(リアルタイムの傍受)ではありません。対象は、端末に記録されたデータです(新9条2項)。
関係ないデータを見たら？	範囲外のデータは、現場の警察官を含む誰にも提供してはならず、調査の終了後に直ちに全部消去されます(新9条6項)。
取った情報で逮捕できる？	捜査目的での権限行使は否定されています(新9条 11 項)。取得した情報を後に刑事手続で使えるかは、条文には書かれていません(後記 8(2))。
調べられたことは知らされる？	原則として事後に通知されますが、例外と先送りがあります(新9条8項)。

2 背景——なぜ今、遠隔解析なのか

(1) 被害の深刻化

日本経済新聞によれば、詐欺・窃盗・強盗といった財産犯の令和7年の被害額は 4,983 億円で、6年連続で増加し、

⁴ 犯罪捜査のための通信傍受に関する法律第 36 条に基づく国会報告(法務省ウェブサイト https://www.moj.go.jp/keiji1/keiji11_00015.html)。

刑法犯の認知件数が戦後最多だった平成 14 年(3,758 億円)を超えました⁵。特殊詐欺の被害額は令和7年が 3,257 億円と過去最悪で、令和8年上半期だけで約 1,816 億円に上ります⁶。警察庁長官は 10 月 13 日、全国の捜査幹部を集めた会議で「まさに異常事態」と述べたと報じられています。令和8年5月には栃木県上三川町で強盗殺人事件も起きています。

(2) トクリュウの構造と、今の捜査手段の「3つの壁」

トクリュウでは、SNS で募集した実行役が秘匿性の高い通信アプリで指示を受けて犯行に及び、実行役が検挙されても、指示役や次の標的にはたどり着けないという構造が指摘されています。警察庁は、従来の手段が次の3つの壁に直面しているとしています⁷。

壁	内容
①暗号化の壁	エンドツーエンド暗号化のアプリでは、通信経路上も事業者のサーバ上も暗号文のため、通信傍受をしても内容が読めない。
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か月を要した例があり、その間、標的への被害防止措置がとれない。
③押収の壁	端末の押収・解析には時間がかかり、画面ロックや自動消去もあるため、被害防止に間に合わない。

ここで着目されたのが、「暗号は端末の中では解かれている」という点です。送信者・受信者の端末の画面では、メッセージは通常どおり読めます。通信経路で情報を取る通信傍受とは異なり、**端末に保存された情報**に届く手段が遠隔解析です。

3 法案の全体像——「2本柱」と条文の構成

本法案は、警察官職務執行法(以下「警職法」といいます。)に、次の2つの条文を新設します(現行の第8条は第 10 条に繰り下げ)。

条文	名称	内容
新8条	被害切迫者に対する被害を防止するための措置	重大犯罪の被害が迫る人を守るための措置を、警察官の 義務 として定める。
新9条	被害防止電子計算機調査(いわゆる遠隔解析)	新8条の措置に必要な情報を得るため、犯人の端末に回線経由で接続し、データを複写・取得する。

政府の概要資料は、新9条を「新8条の措置の実施に当たる警察官に必要な情報を提供し、職務上の義務を的確に果たすことができるようにするため」の措置と位置づけています。つまり、**主役は「被害を防ぐ」新8条で、新9条はそれを支える情報収集の手段**という構造です。

このほか、第3条・第5条は表記の現代化(「すみやかに」→「速やかに」、「虞」→「おそれ」など)にとどまり、第6条の2(能動的サイバー防御)は、新9条との関係で定義規定等が調整されます。施行は、公布の日から6か月を超えない範囲内で政令で定める日です(附則第1項)。

(1) 登場人物をそろえる

条文の用語	意味
重大犯罪	人の生命・身体に危険を及ぼし、又は財産に重大な損害を及ぼすおそれのある犯罪(新8条)

⁵ 前掲注 2。

⁶ 前掲注 3。

⁷ 前掲注 3。

条文の用語	意味
被害切迫者	重大犯罪による被害を受ける者(新8条)。「次の被害者」にあたる
被害防止措置実施警察官	新8条の措置を実際に行う現場の警察官(新9条2項)
被害防止電子計算機調査官	遠隔解析を実施する警察官。警察庁長官が指名する(新9条1項)
被害防止措置用情報	被害切迫者の氏名・住所、犯行の日時など、被害防止措置をとるために必要な情報(新9条2項)

現場の警察官と調査官が分けられている点は重要です。データを「取る人」と「使う人」を条文上で分けており、現場の警察官は自ら端末に接続できず、調査官から許可範囲内の情報の提供を受けるだけです(新9条7項)。企業でいう職務分掌・内部統制と同じ発想といえます。

4 新8条——被害切迫者を守る「義務」

新8条は、次の要件がそろったとき、警察官が直ちに、被害を防ぐ方法の指導その他の必要な措置を「とらなければならない」と定めます。「とることができる」ではなく義務の形である点に特徴があります。

- **要件1** 重大犯罪であること
- **要件2** その犯罪が行われ、又は実行に着手されたことを認めたこと(何も起きていない段階では使えません)
- **要件3** 次の1号又は2号のいずれかに当たること
- **要件4** 被害を受ける者(被害切迫者)が特定されていること

号	場面	例(説明のための仮想例)
1号	合理的に判断して、既に行われた重大犯罪による被害が 拡大 し、又は着手された重大犯罪による被害が 発生 すると認められるとき(今の被害)	特殊詐欺でだまされている最中の高齢者が、追加で振り込もうとしている。
2号	犯罪を行い、又は着手した者による 同種の重大犯罪 で被害が発生することとなると判断すべき 具体的な事実 が認められるとき(次の被害)	強盗を実行した組織の指示役が、別の家を次の標的にしている。

現行第5条は、犯罪が「正に行われようとする」のを認めたときの警告・制止(目の前の犯罪)を定めています。これに対し新8条は、**既に行われ、又は着手された犯罪を出発点に、まだ姿の見えない次の被害者を特定して守るところまで**警察の職務を広げるものです。特に2号は、トクリュウの「次の標的」を想定した規定といえます。ただし「抽象的な危険」では足りず、「具体的な事実」が必要とされている点に注意が必要です。

また、新8条1号・2号は、そのまま新9条の発動条件として引用されます(新9条2項2号)。**新8条が遠隔解析の「入口」**になっている点も、条文の組み立て上の重要なポイントです。

5 新9条——誰の端末から、何を、どんな条件で取れるのか

(1) 誰が実施するのか

実施できるのは、警察庁長官が指名した「被害防止電子計算機調査官」だけです。警察庁又は都道府県警察の警察官のうち、処置を適正にとるために必要な知識及び能力があると認められる者が指名されます(新9条1項)。

(2) どの端末が対象か

対象は、重大犯罪の犯人が**犯人間の相互連絡又は被害切迫者への連絡**に用いたと認める**合理的な理由のある電**

子計算機（電気通信回線に接続しているものに限る。）です（新9条2項）。指示役と実行役の連絡端末、犯人が被害者に詐欺の電話をかけた端末などが想定されます。なお、条文上の用語は「電子計算機」であり、スマートフォンに限らずパソコンも含まれます。事後通知の相手は所有者ではなく「使用者」とされており（新9条8項）、名義貸しや他人名義の端末を前提とした書き方といえます。

(3) 何が取れるのか（取れないのか）

取得できるのは、端末に**記録された電磁的記録**のうち、被害防止措置用情報（被害切迫者の氏名・住所、犯行の日時その他被害防止措置をとるために必要な事項）に係るものです。そのための接続・複写・取得と、「必要な処分」をすることができます（新9条2項）。これからの通信をリアルタイムで捉える制度ではなく、端末の中身を丸ごと見る制度でもありません。

(4) いつ使えるのか——3つのゲート

新9条2項は、現場の警察官から提供された資料により重大犯罪の発生・着手を認めた場合において、次の**3つのすべて**に当たるときに限り、遠隔解析を認めています。

ゲート	条文	内容
①組織性	2項1号	犯罪の態様等から合理的に判断して、 数人の共謀 により行われ、又は実行に着手されたと認められること（単独犯は対象外）
②緊急性	2項2号	新8条1号又は2号に当たり、被害の拡大・発生を防止するため 緊急の必要 があること
③補充性	2項3号	他の方法によっては被害防止措置用情報を速やかに収集することが 著しく困難 であること

(5) 裁判官の事前許可

調査官は、実施の前に「あらかじめ」、次の4項目を明らかにした書面と疎明資料を提出して、裁判官の許可を得なければなりません（新9条3項）。

- ①実施できる場合に当たると認める理由
- ②対象となる電子計算機と、それを対象とする理由
- ③複写・取得する電磁的記録（対象電磁的記録）の範囲
- ④調査のために行う行為の**具体的内容及び手順**

許可をするのは、調査官が所属する警察庁又は都道府県警察本部の所在地を管轄する**地方裁判所又は簡易裁判所**の裁判官です。裁判官は、申請が2項に照らして適切であると認めるときに許可状を発付し、許可状には、対象の電子計算機、対象電磁的記録の範囲、許可の有効期間、発付の年月日、裁判所名を記載します（新9条4項）。注目すべきは、①**技術的な「手順」まで裁判官が審査する点**、②**端末だけでなくデータの範囲まで特定させる点**（憲法35条の特定性を意識した作り）、③**緊急時に事後承認で足りるとする例外が置かれていない点**です。

6 歯止めの仕組み——許可・消去・通知・監督

歯止め	条文	内容
①事前の司法審査	新9条3項・4項	全件について、あらかじめ裁判官の許可状を得る。
②提供禁止・消去	新9条6項・7項	許可範囲外の電磁的記録・情報は、現場の警察官その他の者に提供してはならず、調査終了後、国家公安委員会規則に従い 直ちに全部消去 する。現場に渡せるのは範囲内のデータだけ。

歯止め	条文	内容
③事後通知	新9条8項	原則として遅滞なく、使用者に6項目(端末を特定する事項、罪名、許可状の発付日、実施日、取得した電磁的記録を特定する事項、消去した場合はその日)を通知する。使用者の所在が不明など通知が困難な場合は除く。通知により被害防止措置が妨げられるおそれがあるときは、そのおそれがなくなった後速やかに通知する。
④公安委員会の監督	新9条9項・10項	調査官の処置は、順を経て所属の公安委員会に報告する。公安委員会は、適切に行われたかを確認し、必要があれば警察庁長官等に対し必要な措置をとるべきことを指示する。
⑤捜査目的の否定	新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。

このうち、②は「探すために見る」と「目的外に取って使う」ことを切り分ける規定です。端末の中から被害者の情報を探す過程で関係のないデータが目に入ることは避けられないため、条文は、見えてしまうことを前提に、その後の取扱いを厳しく定めています。⑤は、国税通則法第74条の8などの行政調査権限で用いられる定番の規定と同じ形であり、行政上の権限を捜査に流用させないための「入口の鍵」といえます。

なお、消去・提供・通知の具体的な方法は国家公安委員会規則に委ねられています(新9条6項～8項)。歯止めが実際に機能するかどうかは、この規則の内容と運用にかかっています。

(1) 憲法上の論点

遠隔解析は、憲法13条(プライバシー)、同21条2項(通信の秘密)、同35条(令状主義)に関わります。最高裁は、刑事手続でなくても35条の保障が及び得ることを示しており(最大判昭和47年11月22日刑集26巻9号554頁(川崎民商事件))、GPS捜査については令状を要する強制処分であり、立法的措置が望ましいとしました(最大判平成29年3月15日刑集71巻3号13頁)⁸。本法案が、行政上の権限でありながら裁判官の事前許可を置き、要件と手続を法律で定めた背景には、こうした判例の流れがあると考えられます。最大の争点は、有識者検討会でも物理的な差押えと同程度の強制処分とされた強い権限を、この要件と歯止めで受け止められるかです。

7 他の制度との比較——通信傍受・能動的サイバー防御

観点	通信傍受	能動的サイバー防御(警職法6条の2)	遠隔解析(新9条)
性格	刑事手続(捜査)	行政手続(サイバー危害の防止)	行政手続(重大犯罪の被害防止)
対象	これからの通信	サイバー攻撃に用いられる電子計算機等	端末に記録されたデータ
事前チェック	地方裁判所の裁判官の令状(通信傍受法第4条第1項)	サイバー通信情報監理委員会の承認。承認を得ないとまがない特段の事由があれば例外あり(6条の2第4項)	裁判官の許可。例外なし(新9条3項)
事後チェック	国会への報告(同法第36条)	監理委員会が「勧告」(6条の2第10項)	公安委員会が「指示」(新9条10項)。報告・公表の規定なし
裁判官	地方裁判所	—	地方裁判所又は簡易裁判所
自衛官への準用	—	あり(自衛隊法第91条の3等)	なし(附則第2項により、自衛隊法第89条第1項・第92条第2項の準用から除外)

新8条・9条が自衛隊法の準用の対象から外されている点は、見落とされがちですが、遠隔解析が**警察だけの権限**で

⁸ 最大判昭和47年11月22日刑集26巻9号554頁、最大判平成29年3月15日刑集71巻3号13頁。

あることを示しています。

8 提言から法案へ——決まったこと・残ったこと・国会審議の注目点

(1) 有識者検討会の「宿題」への答え合わせ

9月の最終提言⁹を受けて、今後の立法で注目すべき5点が指摘されていました。法案の条文は、次のように答えています。

論点	法案の答え	残った点
①対象犯罪	罪名は列挙せず、抽象的な定義(新8条)と共謀の要件(新9条2項1号)で絞る。	「財産に重大な損害」の線引き
②蓋然性・緊急性	「合理的に判断」「具体的な事実」「緊急の必要」「著しく困難」を条文化(新8条、新9条2項)。	運用での具体化
③許可状の特定性・再実施	端末・範囲・手順・有効期間を記載(新9条3項・4項)。	再実施の扱いは明文なし
④事後通知・公表	事後通知を明文化(新9条8項)。	実施状況の公表・国会報告の規定なし
⑤公安委員会の専門性	報告・確認・指示の仕組みを規定(新9条9項・10項)。	外部専門家の関与は条文上なし

(2) 国会審議で注目したい5点

- 「財産に重大な損害」の線——特殊詐欺は、どの金額・どの段階から対象となるのか。
- 簡易裁判所の裁判官による許可——通信傍受は地方裁判所の裁判官に限られる(通信傍受法第4条第1項)のに対し、より広い裁判所に許可権限を認める理由は何か。
- 「必要な処分」の中身——端末の脆弱性を利用するのか。手法の秘匿と事後の検証可能性をどう両立させるのか。
- 通知の例外・先送りの運用——違法な実施があった場合に、どのように争えるのか。取得した情報の刑事手続での利用(提言は、必要な手続を経れば利用し得るとするが、条文には規定がない。)をどう整理するのか。
- 透明性——実施件数の公表や国会報告の仕組みを設けるのか(通信傍受法第36条との比較)。

9 実務への示唆——今から着手すべき事項

本法案は警察を名宛人とする制度であり、民間企業に端末解析の義務や協力義務を課すものではありません。しかし、遠隔解析により警察が被害切迫者の情報を早く得られるようになれば、新8条の措置の場面で、**警察から企業・金融機関への連絡や協力要請が増える**ことが予想されます。また、情報が早く届くほど、受け取った民間側の**即応速度**が問われます。

部門	着手すべき事項
金融機関(営業店・AML・法務)	警察からの連絡の受付窓口を一本化し、名寄せ・取引予定の確認を当日中に行える体制を整える。振込・出金を保留する権限と上席へのエスカレーション、「止めた理由」と「止めなかった理由」の記録、同姓同名等の誤認への対応を定める。2027年4月に適用が予定される不正利用口座情報の共有の枠組みと一体の業務フローとして設計する。
小売・サービス・一般企業	警察から「顧客が狙われている」との連絡を受けた場合の窓口・判断者・顧客連絡の手順を決め、記録を残す。
通信・プラットフォーム	警察からの照会への対応窓口、ログの保全、法的根拠の確認手順を整備する。

⁹ 前掲注3。

部門	着手すべき事項
情報管理・個人情報保護	顧客名簿・資産・住所・家族構成等は、犯罪者から見れば「標的リスト」となり得る。内部者・委託先の持ち出し、大量照会、深夜閲覧、退職予定者のアクセスを検知できるか点検し、安全管理措置（個人情報保護法第 23 条）を、顧客の生命・身体・財産を守る施策として見直す。
経営・取締役会	重大な被害切迫情報を経営層に上げる報告ライン、休日・夜間の意思決定体制を確認する。

「今夜、警察から『御社のお客様が標的ですよ』と連絡が来たら、誰が、何分で動けるか」——この問いに即答できるかどうか、準備の出発点です。

なお、本ニュースレターは一般的な情報提供を目的とするものであり、個別の事案への対応については別途ご相談ください。本法案は国会審議中であり、内容が修正される可能性があります。

以上