

令和7年6月12日

サイバー空間における事後追跡上の 障害に関する実態調査

警察庁刑事局捜査支援分析管理官

○ 調査概要

サイバー空間における事後追跡上の障害について実態を把握するため、令和6年中に都道府県警察が捜査した事件について調査を実施。

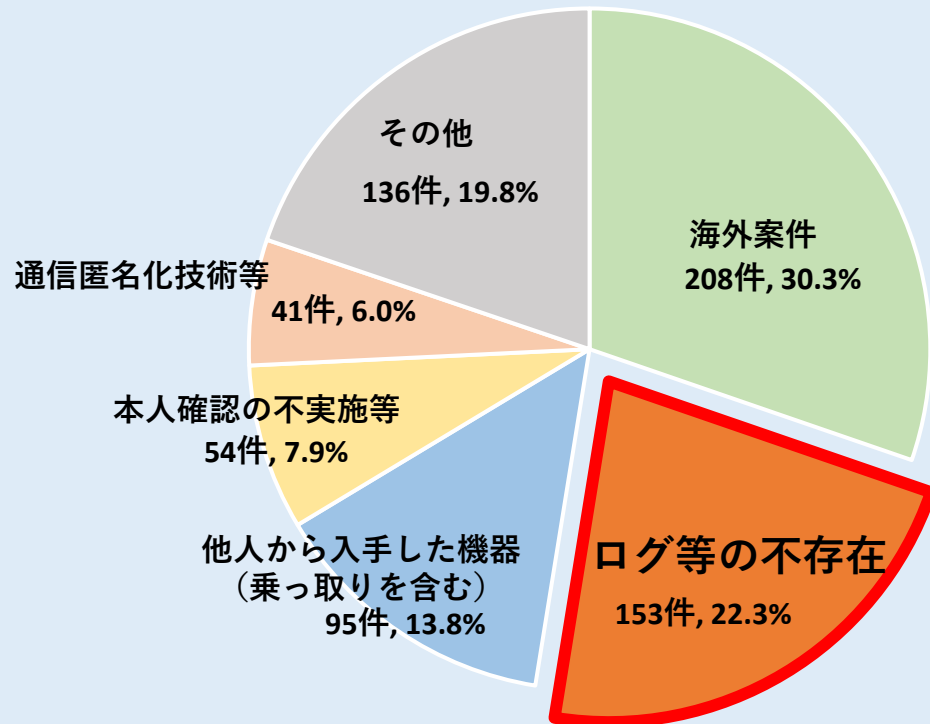
○ 集計対象

実行行為のほか、実行犯の募集、被疑者間の連絡等にインターネットが用いられた被疑事件のうち、未検挙であるもの。

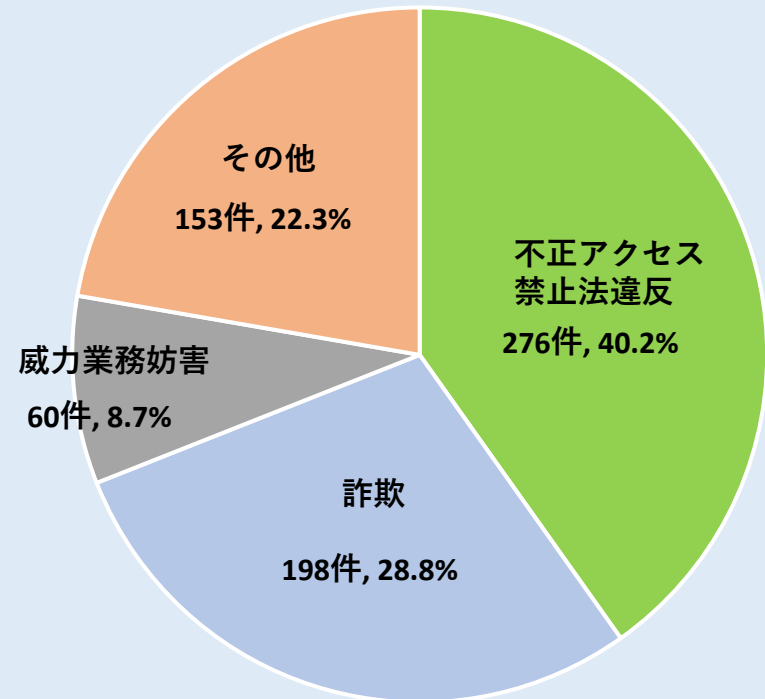
サイバー空間における事後追跡上の障害に関する実態調査概要

- 635事件について、**687件（※）の事後追跡上の障害が存在**。 ※ 1事件当たり複数回答あり。
- 障害の種別でみると、海外案件（208件、30.3%）が最多。次いで**ログ等の不存在（153件、22.3%）**。
- 事後追跡上の障害があった事件の罪種では、不正アクセス禁止法違反（276件、40.2%）が最多。次いで詐欺（198件、28.8%）。

事後追跡上の障害の件数（687件）



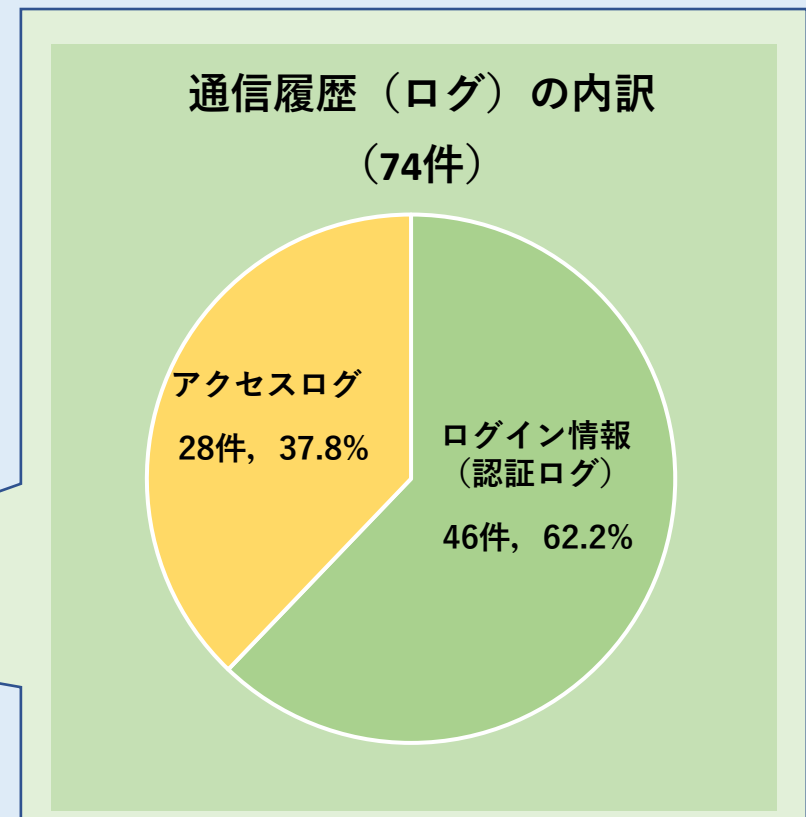
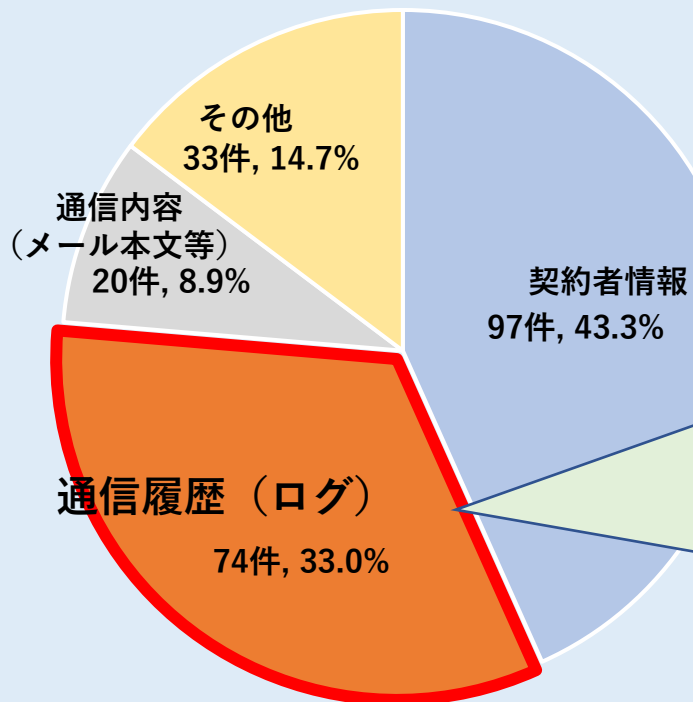
罪種（687件）



不存在であった情報の種別等

- ログ等の不存在（※）による障害に関して、不存在であった情報の件数は224件。
※ 照会、保全要請、差押えの時点で通信履歴（ログ）、契約者情報等について、保有期間を超過又は保存していないもの
- 不存在であった情報の種別でみると、契約者情報（97件、43.3%）が最多。次いで、通信履歴（ログ）（74件、33.0%）。
- 不存在であった通信履歴（ログ）の内訳では、ログイン情報（認証ログ）（46件、62.2%）が最多。次いで、アクセスログ（28件、37.8%）。

不存在であった情報の種別（224件）

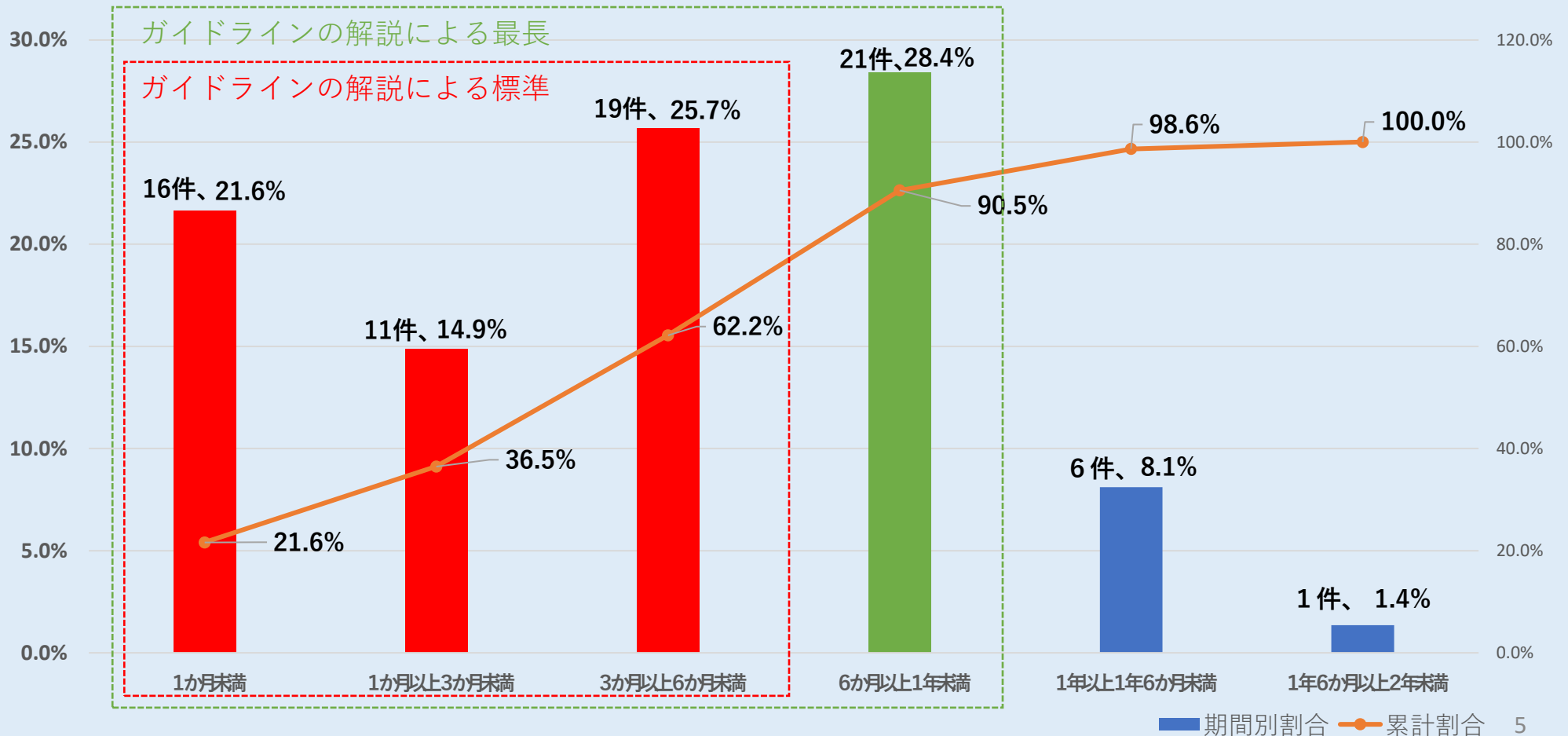


事件発生から照会等までの期間

- 通信履歴（ログ）の不存在による障害は74件。
- 事件発生から照会等（※）までの期間は、1年6か月未満が73件（98.6%）。

※ 照会、保全要請、差押え

事件発生から照会等までの期間の内訳



考察

今回の調査結果から、実効性のあるルール（※）の下で、通信履歴（ログ）が1年6か月保存されていれば、ログの不存在を原因とした捜査上の障害を概ね解消できると思料。

※ 電気通信事業における個人情報保護に関するガイドラインでは、通信の秘密への配慮から、業務遂行上必要な場合に限って通信履歴を記録することを認め、その場合、一般に6か月程度の保存は認められ、より長期の保存をする業務上の必要性がある場合には、1年程度保存することも許容されるとの解説がなされている。