FBIの調査・捜査手法

2025年4月23日

茂田インテリジェンス研究室
https://shigetatadayoshi.com/

目　次

１－１　問　題　意　識

■　米FBI・National Security Branchによる摘発件数

出典：『警察政策』26巻（2024年）（宇生航）「Justice News」

年平均　約30件（2016～23年前半）

対象事件：先端技術窃取、不正輸出、Counter-Intelligence

（テロ事案などは含まない。）

■　韓国：産業技術の対外流出摘発件数

出典：『治安フォーラム』2025年1月号（流出対策研究会）

年平均　約20件（2019～23年）

対象事件：産業技術の対外流出のみ

■　我が国の摘発件数は、？？？

日本は標的ではない？　or摘発出来ていないだけ？

1-2　FBI：法執行且インテリジェンス

＜機能＞

◇ ヒューミント（人的諜報）
human intelligence

◇ シギント（信号諜報）
signals intelligence

◇ イミント（画像諜報）
imagery intelligence

◇ マシント（計測・特徴諜報）
measurement and signature intelligence

◇ セキュリティ・サービス

（スパイ対策、テロ対策、国家転覆阻止、
大量破壊兵器拡散防止WMD）

＜主な組織＞

◆ CIA（中央諜報庁）
Central Intelligence Agency

◆ NSA（国家安全保障庁）
National Security Agency

◆ NGA（国家地理空間諜報庁）
National Geospatial-Intelligence Agency

◆ DIA（国防諜報庁）
Defense Intelligence Agency

◆ FBI（連邦捜査局）
National Security Branch
（*national security service*と指定）
＋ 国内ヒューミント所管

1-3　FBIの摘発事例に見る特徴

■　調査手法・捜査手法

- ○　通信傍受（広義）
- ○　クレジットカード使用履歴（使用店舗を含む）
- ○　傍受機器の秘密設置（事務所や住宅など）
- ○　秘密捜索・押収
- ○　囮捜査
- ○　公開情報：各種SNS情報（Facebook、Tick-Tock他）
- ○　街頭カメラ、交通カメラ、商店・企業の各種防犯カメラ

NSAの支援有

■　罰条

- ○　虚偽供述罪
- ○　外国代理人登録義務違反罪
- ○　共謀罪

■　司法制度の運用

- ○　厳罰主義（且つ併合罪規定無し）　⇔　我が国/寛刑主義
- ○　司法取引
- ○　令状非開示手続

1−4　FBIの調査・捜査権限の構造

＜行政調査＞	＜司法捜査＞
■　1978年対外諜報監視法FISA	
○Title1 電子的監視（通信傍受） （住居侵入の上の監視装置の設置を含む）	○　通信傍受法
○Title3 物理的捜索（秘密の捜索差押等）	○　刑事手続法の捜索差押
○Title4 発着信記録装置（ペン・トラップ）	○　ペン・トラップ法
○Title7 米国外の者を対象とする米国内収集 （FISA702条）「プリズム」	
○Title5 企業記録の提出（NSLs） （NSLs＝国家安全保障書簡）	
■　保管通信法（合衆国法典18篇2709条）（NSLs）	○　保管通信法（18篇2703条）

◆大統領権限で実施していたものを、後にFISAで法制化
◆FISA収集情報の刑事訴追使用は可
◆FISAの「対外諜報情報の収集」:「the目的」から「重要な目的」
◆1994年「法執行のための通信支援法」

目　次

2-1　江蘇省国安庁第6局①

■　江蘇省国家安全庁第6局

◆　第6局　処長：査栄、副処長：徐延軍、科長：柴萌

◆　2010年代の同局の経済スパイの重要目標
　　国産ジェット旅客機の開発支援（技術情報の収集）

◆　取組態勢

○　シギント（インターネット経由）
　　柴萌指揮～APT26（タービン・パンダ）劉春亮以下6人以上

○　シギント（インサイダー工作）
　　徐延軍支援～仏企業の中国支社社員、田曦、顧根

○　ヒューミント～徐延軍担当
　　南京航空航天大学の協力を得て、大学を場として活動
　　LinkedInで情報価値のある海外研究者を探して招聘
　　副学部長・陳鋒の協力～学術交流や講演を名目
　　工作～旅費・謝礼、飲食接待、親族関係
　　他に・　講演プレゼンでの質問攻め　・　ホテル作業

2-1　江蘇省国安庁第6局②

■　協力者工作の事例（対アーサー・ガウ）

○　アーサー・ガウ（Honeywell社のエンジニア）

○　2003年頃　南京航空航天大学の依頼で訪問講演（数回）
「大学関係者」査栄と知遇。母親を揚子江上流遊覧で歓待
Honeywell社の航空機プロジェクトの情報要求、関係中断

○　2014年　査栄からメールを受け、連絡復活
○　2016年　ガウが友人訪問のため北京訪問
査栄、徐延軍が空港に出迎え、夕食接待と交通費3000ﾄﾞﾙ
○　2017年　訪中。ホテルで徐延軍と技術者数人に講義
Honeywell社の航空機の補助動力装置
浙江省西湖に1泊2日の観光旅行。講演料・旅費6200ﾄﾞﾙ

○　2018年秋　訪中帰国を計画中、FBIが逮捕
○　2021年5月　輸出規制品の無許可輸出で有罪答弁
2021年秋　徐延軍の裁判で証人出廷。　「司法取引」
2022年　保護観察と罰金。

参考

■　協力者工作の事例（対アーサー・ガウ）

＜浙江省西湖＞　　ガウ

（出典：米司法省）

2-1　江蘇省国安庁第6局③

■　囮捜査（デビッド・チェン、囮作戦に同意）

○　デビッド・チェン　ハルピン工業大学卒、米国留学、博士号
　　GEアビエーション社でジェット・エンジンの研究員

○　2017年3月　LinkedIn経由、南京航空航天大学の講演依頼
　　5月　親族の結婚式などのため、訪中
　　6月　大学で講演。（GE社の承認を受けず）
　　徐延軍、「江蘇省国際科技発展協会」副秘書長
　　夕食接待と講演謝礼・旅費3500ドル

○　6月末　FBI担当官、GE社「内部脅威」特別班に連絡

○　11月　突然、チェンの呼出し面接（インタビュー）
　　GE社セキュリティ担当、続いてFBI担当官
　　＜訪中目的と行動について＞

○　FBI担当官、チェンに南京訪問の証拠を突き付ける
　　虚偽供述罪（18U.S.C.§1001(a)）の成立
　　防諜作戦に参加すれば、起訴しない

2-1　江蘇省国安庁第6局④

■ 囮捜査（徐延軍の誘出しと身柄拘束）

○ 2017年12月　チェン、翌年2月春節での親族訪問を通知
　　情報提供への積極姿勢を示す
○ 2018年1月　徐延軍から具体的な情報要求が始まる
　　チェン、それらしい情報提供開始（GE社協力）
○ 　2月　チェン、重要なフランス出張で、春節帰国中止を通知
○ 　2月　徐延軍、欧州での会合を提案
○ 　4月　ベルギーで身柄拘束

○ 2018年10月　米国移送：
　　経済スパイ、企業秘密窃盗などで起訴
○ 2021年11月　陪審裁判で有罪評決
○ 2022年11月　拘禁刑20年の宣告
○ 2024年　8月　控訴棄却。一審判決確定
○ 2024年11月　囚人交換で釈放、帰国

（出典：米司法省）

2-1　江蘇省国安庁第6局⑤

■ 徐延軍の愚かな規律違反（の筈）

○　iPhone使用

○　Gメール（jastxyj@gmail.comとjastquhui@gmail.com）

○　iCloud（iPhoneのデータをバックアップ）

身分証明書、給料明細、健康保険証、休暇届など各種の資料写真。
iPhoneのカレンダーを日記帳代わり（日々の業務や私生活での出来事、
上司との査栄との関係、考えたこと、感じたこと）。
工作対象の他の航空産業社員との通信記録

遅くとも2017年11月以降は、FBIによる通信傍受対象【推定】

■　FBIは如何にして、南京訪問を探知したのか？

【推定】

（警察政策学会資料第137号、『警察公論』2025年1月号参照）

2-2　海帰創業･経済スパイ①

■　事案の概要

○　鄭シャオチン（1963頃生れ）

○　西安市西北工業大学卒。MIT大学院で研究。米国で就職。
　　2008～18年　GE社でタービンのエンジニアとして勤務。

○　2016年4月　中国在住の張ジャオシーと中国に会社を設立。
　　（タービン部品の開発製造）

○　2016年2月　GE社に対して会社設立について虚偽説明

○　2016～18年　GE社の企業秘密を持出し、中国に送信。

○　2017年末　鄭の業務用コンピュータで暗号化ファイルを発見

○　2018年7月　鄭が暗号化ﾌｧｲﾙ40件のﾃﾞｽｸﾄｯﾌﾟ転送を探知

○　2018年8月　逮捕。　　2019年4月起訴。

○　2022年3月　陪審裁判で経済ｽﾊﾟｲ、企業秘密窃盗、4罪有罪

○　2023年1月　拘禁刑2年、保護観察1年、罰金7500ドル宣告

2-2　海帰創業・経済スパイ②

■ FBIの把握情報（起訴状に基づく）

◆　2016年1月～2018年7月　鄭と張の間の通信

①　メッセージアプリの暗号化通信　40日分以上

暗号化通信（テクスト、音声）の内容を、起訴状に記載

内容：事業展開（工場設計、技術図面他）の打合せ中心

②　技術データ（暗号化ファイル）のメール送信の解明。

鄭の業務用コンピュータ　⇒デスクトップに送信

デスクトップ⇒（ステガノグラフィ）⇒Hotmailアカウントに送信

鄭のHotmailアカウント　⇒共犯者・張のQQアカウント

◆　中国当局者との関係の判明（例）　メッセージアプリ通信から判明

○　遼寧省【推定】の党書記、省長等幹部の工場視察。補助金。

○　瀋陽発動機研究所、中国航空発動機有限公司との遣取り

○　瀋陽航空航天大学との「戦略的協力合意」締結

2-2　海帰創業・経済スパイ③

■ 注目点

- ○　GEパワー社のセキュリティ措置
- ○　GEパワー社（セキュリティ部署）とFBIとの協力関係
- ○　FBIの情報収集力
  - ・　鄭と張の間の暗号化メッセージの解読
    2016年に遡っての入手解読
  - ・　鄭のHotmailアカウントのデータ入手
  - ・　ステガノグラフィの解読
  - ・　メールに添付した暗号化ファイルの解読

（『警察公論』2025年3月号、2月初旬発売、参照）

2-3　韓国系元CIA分析官①

米国帰化人利用の韓国国情院の対米影響力工作

■　事案の概要

○　スー・ミ・テリー（1970頃、韓国ソウル生れ）
　　米国留学、フレッチャー・スクールで博士号取得

○　2001～2010年　CIA、国家安全保障会議等で
　　韓国、東アジア専門家として勤務

○　2010～2015年　「外交問題評議会」「コロンビア大学」勤務
　　国情院NY駐在員からの情報を基に、講演や論文投稿

○　2015年～　「CSIS」「ウィルソンセンター」等で勤務
　　大使館勤務の国情院代表の意向に沿った活動を展開

○　謝礼：高級ブランド品、高級レストランの会食、資金提供

○　2023年6月　FBIによるインタビュー。同時に捜索差押。

○　2024年7月　外国代理人登録義務違反で起訴

2-3　韓国系元CIA分析官②

■　FBIの把握情報（起訴状等に基づく）

＜韓国政府の代理人としての活動＞

○　言論活動の例
- 『フォーリン・アフェアーズ』2023年1月号に論文投稿の経緯
  国情院代表依頼、韓国政府の立場に立った核政策提言
- 2023年　依頼を受けてシンポジウム開催の経緯
- 議会証言（2016，2017，2022）

○　政府非公開情報の提供の例
- 2022年　国務長官とのオフレコ会合の記録提供の状況
  外交ナンバー自動車内、国情院代表による撮影写真
- 2023年　駐日米大使との会合内容の提供

○　米国政府幹部との仲介の例
- 2019年　国情院長官と政府高官との親密会合の設定の経緯
- 2022年　議会スタッフを集めたパーティ開催（国情院職員同席）

＜謝礼提供の状況＞

2-3　韓国系元CIA分析官③

■　情報の入手方法【推定】

○　テリーの国情院代表などの間の通信の傍受

Eメール

電話通話　　FISAによる通常の通信傍受

暗号化通信アプリ（推定Signal）テキストメッセージや音声通話

FBI：遅くとも2010年代半ば以降、傍受解読

【推定】テリーの携帯端末をハッキングしていた可能性大

○　国情院代表が撮影した写真を入手　　How？

＜謝礼関係＞

○　各種高級ブランド品の購入状況　3店（証拠写真付き）

○　高級レストランでの会食　多数（写真付、時に会話記録付）

クレジットカードの使用履歴（国情院代表、テリーなど）

店舗カメラ、街頭カメラなど各種のカメラ

秘匿設置したマイク、カメラ；　携帯端末のマイクON

○　資金提供～金融情報

（警察政策学会資料137号、『治安フォーラム』2025年1月号参照）

2-4　元米陸軍諜報部隊員①

■　事案の概要

○　ジョセフ・シュミット（1994頃生れ）
○　2015年1月～20年1月　陸軍・第109軍事諜報大隊勤務。
　　除隊時、軍曹でヒューミント分隊長
　・　ヒューミントの各種訓練コース受講。中国語学習。
　・　台湾有事では、中国兵捕虜の尋問などの戦術諜報担当
　・　セキュリティ・クリアランスはTS/SCI（最高レベル）

○　2020年2～7月　提供予定文書（国防情報）各種を作成。
○　2月　　イスタンブールで中国領事館に接触を図る。
○　3月上旬　北京で国家安全部周辺を徘徊。
○　3～7月　香港で中国国営企業2社に対してメールを送信。
　　国防情報の提供を申し出る。

○　その後の動静は不明。香港滞在を継続と見られる。
○　2023年10月6日　帰国時にサンフランシスコ空港で逮捕。

2-4　元米陸軍諜報部隊員②

■　FBIの把握情報（起訴状、宣誓供述書を基に）

＜国防情報の不正保有＞以下の文書を作成、iCloudに保管

- ○　2月26日 文書「中国政府に提供する重要情報」（22頁）
- ○　3月 9日　文書「ヒューミントAIT」（4頁）
- ○　3月16日 文書「高級秘密」（23頁）
- ○　5月12日 PPT「軍事諜報源作戦と訊問技術」（28頁）
- ○　5月20日 手書きスケッチ「Mat V Computers」

＜国防情報の提供未遂＞

- ○　2月24日　在イスタンブール中国領事館にGメール送信
  経歴を明かして面会を要望
- ○　3月20日　IT企業・航天信息股份有限公司にGメール送信
  米軍の極秘レベル・ネットワーク侵入への協力を申し出
- ○　7月21日　某国営企業に（別アカウント）Gメール送信
  米国インテリジェンス技術の情報提供を申し出

2-4　元米陸軍諜報部隊員③

■　情報の入手方法

FBI：グーグル検索、グーグルマップ検索、
Gメール、Outlookメール、Yahooメール、iCloud 等を把握

【プリズム】　FISA702条収集

○　IT企業の米国内データセンターから、
必要なデータを随時、検索取得

○　FBIとCIAとNSA三者の共同事業

○　2007年に開始。2013年時点の協力企業9社、増加中。

○　取得データ

【コンテンツ情報】 メール（Gメール、Outlookメール、Yahooメール）、
チャット、ボイスメッセージ、送信ファイル、
写真、ビデオ、保管データ（iCloud、OneDrive）等

【メタデータ】メールアドレス、電話番号、通信時刻、位置等

【端緒情報】 全くの推測

（元）インテリジェンス職員の懸念国渡航検索システム？？

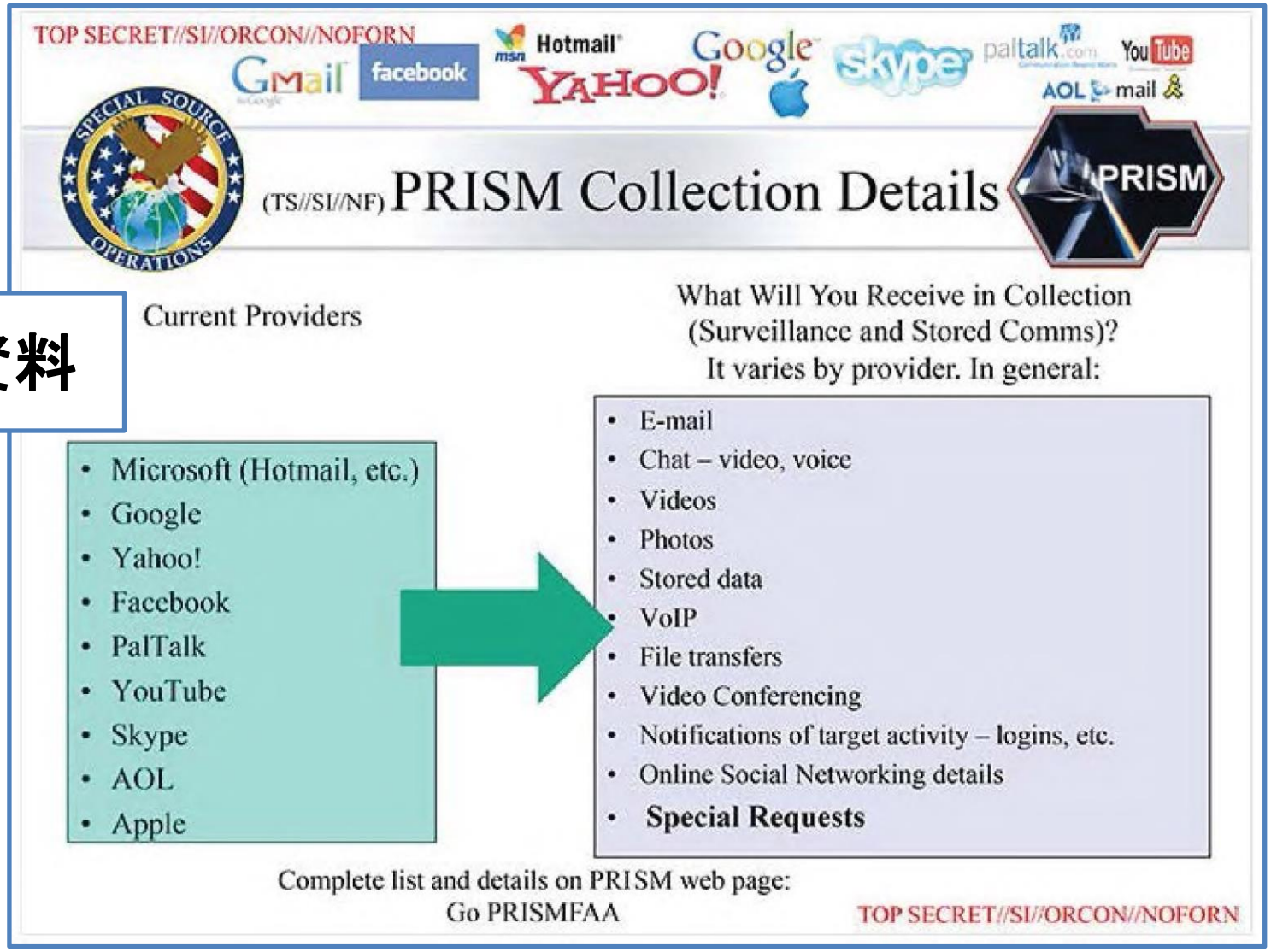
（『治安フォーラム』2024年5月号、『ウェブサイト』2023．11．27トピック参照）

（参考）「プリズム」計画

漏洩されたパワーポイント資料

National Security Agency, Public domain, via Wikimedia Commons

漏洩資料



2-5　9.11型自爆テロの阻止①

■　事案の概要

○　チョロ・アブディ・アブドラー（1990生、ケニア人）

○　2016年頃から、過激思想の傾斜
　　アル・シャバーブのキャンプに参加。戦闘訓練を受ける
　2016年 旅客機自爆テロの計画に参加、指示を受ける

○　フィリピンのパイロット学校で飛行訓練（2017～2018年）
○　並行して、旅客機乗取り自爆テロ準備の調査活動
（2018～2019年）

○　2019年 7月　フィリピン当局が身柄拘束
○　2020年12月　米国に身柄移送（同時に起訴）
○　2024年11月　陪審裁判で有罪評決
　　航空機ハイジャックの共謀など6罪
　　科刑宣告は本年3月の予定（終身刑か相当の長期刑）

2-5　9.11型自爆テロの阻止②

■　FBIの把握情報（起訴状等に基づくと）

○　2016年　旅客機自爆テロの計画参加と指示受け

○　2016年12月からのパイロット学校への入学手続

○　パイロット訓練の進捗状況（学校の過程終了）

○　起訴状記載の調査活動

- 2018年10月6日　9.11事件に関するジハード主義者の
  ウェブサイトを閲覧
- 同12月　旅客機のセキュリティ措置、
  コックピットへの侵入方法などをインターネット検索
- 19年1月　米国某都市の最高層ビルをインターネット調査
  【推定】NYCのOne World Trade Center
- 同1月2月　旅客機乗取りと米国査証の入手方法を
  インターネットで調査

○　アル・シャバーブ担当者への報告通信（暗号メッセージ）

2-5　9.11型自爆テロの阻止③

■　端緒情報と捜査情報の入手方法の推定

ヒューミントの可能性は低い。
NSAが探知して、FBIに通報。FBIの追加調査・捜査

【NSAの構築したX-Keyscoreシステム】の能力

○　特定の過激ウェブサイトを頻繁に閲覧する者を検出抽出
○　特定の単語によってウェブ検索をする者を検出抽出
○　グーグルマップやグーグルアースの検索状況から、
テロ準備の調査活動を行っている者を検索抽出。
○　例えば、ソマリアの特定地域と頻繁に暗号通信をする者を
抽出検索。

こうして、
テロリスト容疑者を探知　⇒　同人のネットワーク活動を監視

（『警察公論』2025年6月号、『ウェブサイト』2024．11．20トピック参照）

（参考） X-Keyscore

世界150ヵ所
サーバー700以上

漏洩資料

漏洩資料・2008年2月25日付

National Security Agency, Public domain, via Wikimedia Commons

目　次

3-1　補足/通信傍受

＜通信傍受（広義）＞

○　通信内容
- データセンター収集
- 回線傍受
- 端末傍受（ハッキング）

音声通話、メール、
テキストメッセージ、音声ファイル
iCloudなどクラウド・データ　等

○　通信当事者の把握

○　ウェブ検索履歴　（google検索、google map検索、他）

○　位置情報　（スマートフォン、スマートウォッチ、車両等）

Emergency disclosure requests
Stingray傍受システム
NSLs
Geofence warrant

Phone：　Google, Facebookなどapp企業
Smartwatch: app企業
自動車telematics system
トヨタT-Connect、日産Nissan Connect
Honda Connect、スズキｺﾈｸﾄ、ダイハツｺﾈｸﾄ
GM OnStar、Chrysler Uconnect、Ford SYNC

○　ウェブカメラ、マイク使用

＜クレジットカード使用履歴（使用店舗を含む）＞

Emergency disclosure requests
NSLs

3-2 位置情報の利用 ①

位置情報の氾濫 ～ 通信塔、GPS、Wi-Fi、Bluetooth

（例）・ 携帯電話会社の通信塔cell tower情報

・ グーグル(特にAndroid端末) (location history、web & app activity)

Sensorvault 位置情報データベース 2009-2024

・ Meta(Facebook、Instagram、WhatsApp、Messenger)

・ Amazon ・ アップル(iOS)

・ 地図交通、気候、フィットネス、地元ニュース他のアプリ

■ FBI、2010年代初、無令状・通信塔情報 ⇒“tower-dump” warrant

■ Geofence warrant(ジオフェンス令状)2016年頃～

特定区域で特定時間帯に所在した全端末のデータ取得

対象犯罪 ＊強盗＊殺人・傷害＊放火＊誘拐

連邦刑事手続規則Rule41(捜索差押) ; 保存通信法

① 特定区域・特定時間帯の全端末の位置情報

② 関連性の高い端末についての区域外の位置情報

③ 更に関連性の高い端末契約者の個人特定情報

Google1社：2018年982件、2019年8396件、2020年1万1554件

3-2　位置情報の利用 ②

■　IP-geolocation service

米国20社以上。
高精度：　MaxMind社のGeoIP2
　　Digital Element社のNetAcuity
某社のセミナー
日本「らっこ社」

■　Phone location data industry

- ○　2019.1Vice.com. 米、賞金稼ぎは位置情報を購入
  情報源：T-Mobile、AT＆T、Sprint
- ○　2019.12 NYT連載。各種アプリから位置情報収集
- ○　2022.6.13 EFF org. 位置情報産業の実態

日本にも上陸

（参考）NSAの位置情報DB：FASCIA

漏洩情報

2013年スノーデン漏洩情報
＜携帯電話の位置情報追跡システム＞

FASCIA（位置情報のデータベース）

- 世界中の携帯の位置情報を毎日50億件収集
  内、数億件以上を保存
- 位置情報：携帯電話特定の為の位置情報（DNR）
  ネットサービスの為の位置情報（DNI）
- 10以上の収集方法
  （1例）「Stormbrew」 ～ ベライゾン
  通信会社の回線接続点27ヵ所から収集

＜利用例＞
- ○ 行動監視 ：スパイ容疑者、テロ容疑者の行動監視
- ○ 不審者の割出 ：通信保全活動の自動検出
- ○ Co-Traveler分析 ：同伴者、仲間の探知
- ○ Fast-Follower分析 ：海外エージェントの追跡者探知

3-3　Hacking/NIT令状

- 当初、テロ対策でFISA権限　2000年前から？

■連邦捜査手続規則Rule 41（捜索差押）の一般条項

- サイバー犯罪、児童ポルノ対策、薬物取引他
- Tor、Signal、VPNs等、匿名化通信・暗号化通信の増加

◆ ダークウェブ（Tor）の児童ポルノサイト　⇦　NIT令状

- Torpedo作戦(2012)～PedoBoard、PedoBook、PB2
- Pacifier作戦(2015)～Playpen（ベビーサークル）

FBI、運営者逮捕。サイトを管理して「水飲み場」攻撃。
2週間、サイト来訪者に対してNITコード注入
IPアドレス、MACアドレス他、端末特定情報を収集
米国内、逮捕348人以上、起訴51人以上、救出55人以上
米国外、逮捕548人以上、救出296人以上

■ NIT warrants / remote access searchの規定と活用

- Rule41（b）項（6）号（遠隔アクセス捜索）2016年12月施行

（A）匿名化犯罪者　（B）多数のボットネット

- 2023年12月Volt TyphoonのKV Botnetマルウェアの除去
- 2024年秋　Twill TyphoonのPlug Xマルウェアの除去

3-4　キーワード令状

■ Keyword search warrant

○　特定キーワードで特定期間に検索した者の
IPアドレス他の端末・個人特定情報

○　対象企業：グーグル、マイクロソフト、ヤフー等の検索機能

○　2017年頃から？　年数件？
令状は殆ど開示されていないので、全体像は不明だが
（例）

- 2017年ミネソタ州、小切手詐取事件
～被害者の名前を検索
- 2018年テキサス州、連続爆破事件
～爆破場所、爆弾製造に係わる用語を検索
- 2019年ウィスコンシン州、女子誘拐事件
～女子の名前や住所などを検索
- 2020年コロラド州、放火殺人事件～被害者の住所を検索

○　国家安全保障調査手法の一般犯罪捜査への波及

目　次

4-1　治安の将来

＜客観条件＞

■　「善良な犯罪者」前提の刑事司法の限界

（例、任意捜査の原則、取調重視、寛刑主義）

併せて ＜外国からの脅威を前提としない行政制度＞

But,　悪質な犯罪者・犯罪企業集団（例：トクリュウ）

外国からの脅威（経済スパイ、サイバー攻撃、影響力作戦）

■　少子高齢化・人口減少

⇒　警察官増員ではなく、減員？？！！

■　働き方改革　働かせ放題⇒実質勤務時間の削減の必要

＜対策は？＞　■　生産性の向上

＜調査効率・捜査効率、刑事司法全体の有効性・効率性＞

各分野：　調査手法・捜査手法、罰則規定、寛刑主義

4-2　努力の方向性＜結論＞

- ◆　都道府県警察の現場
- ◆　警察庁は？
- ◆　法曹関係者？

■　当面の努力

「仮装身分捜査」だけ？

「GPS捜査令状」？　「Telematics検証令状」？

■　近未来への努力

≪大前提≫

主権者たる国民の判断

判断の前提＝世界標準と我が国の現状の知識

参考資料

◆ ウェブで読める主な参考資料（無料）

茂田インテリジェンス研究室ウェブサイト　⇒著作へ

https://shigetatadayoshi.com/

- 「米国の治安と警察活動」　警察政策学会資料96号（2017年）
- 「オサマ・ビンラディンを追え（上）（下）テロ対策におけるシギントの役割」　季刊現代警察（2018年）
- 「米国における行政傍受の法体系と解釈運用」　学会資料94号（2017年）
- 「米国国家安全保障庁の実態研究」　警察政策学会資料82号（2015年）
- 「サイバーセキュリティとシギント機関　～NSA他UKUSA諸機関の取組」情報セキュリティ総合科学2019年
- 「テロ対策に見る我が国の課題～欧米諸国との対比において」113号2020年
- 「江蘇省国家安全庁第6局による経済スパイ」他　学会資料137号（2024年）

◆ ウェブサイト 「トピックス」

◆ 定期刊行物

- 『警察公論』（「インテリジェンスこぼれ話」連載
- 『治安フォーラム』、『軍事研究』など