
ODYSEC
貼身的眼睛
近距離監控
CLOSE-RANGE SURVEILLANCE – DETECTION AND RESPONSE

貼身的眼睛

近距離監控的偵測與應對

Odysec 技術白皮書 WP-001 ｜ **版本** 1.0 ｜ **發布日** 2026-08-30 **領域**：網路 × 實體（Cyber × Physical）

目錄

關於本白皮書

近距離監控可經由四條技術上完全不同的途徑達成，而被監控者不會事先知道自己遇到的是哪一類——他只知道「對方總是知道」。**四條途徑必須放在同一張表上比較，讀者才知道自己剛才那次陰性檢查究竟排除了什麼。** 本白皮書即以此為軸，並補上同類指引普遍缺少的一章：**當受檢裝置本身不可信時，網路側能看見什麼**。

本白皮書的性質分為兩部分，其可支持的推論強度不同：

- **第 2 章至第 5 章、第 7 章至第 8 章**屬於**綜整與方法論**：整理已發表的學術量測、標準文件與平台公開資料，並在其上建立可自行執行的偵測程序。
- **能支持**：監控可經由哪些途徑達成、現行防護在原理層面存在哪些結構性缺口、各層檢查分別涵蓋哪一條途徑、以及陰性結果的意義。
- **不能支持**：任何關於「某平台或某產品目前如何反應」的當下事實。凡引用他人量測之處，均標明其量測者、受測對象與時點——**那是該研究在該時點的觀察，不是現況的保證**。
- **第 6 章**屬於**本團隊自有之實測**：在可重現的受控環境中量測「加密流量下，週期性回報的可偵測性」。該章的數據、實驗環境與分析腳本隨本白皮書公開，任何人皆可複驗。

兩者不得混用。第 6 章量測的是**行為模式**（週期性回報），不是任何真實監控產品；第 2 至 5 章的缺口分析則是原理層面的推論，不是對特定廠商的評價。

摘要

近距離監控——由伴侶、前任、家人或熟人所進行的持續掌握——的技術門檻已經降到消費級。加害者不需要任何技術能力，只需要一次實體接觸的機會，或一組他早已知道的密碼。

本白皮書的四個主要發現：

1. **一次陰性檢查，至多只排除四條途徑中的一條。** 監控可經由四條途徑達成：實體追蹤器、帳號層、裝置層、設定層。四者的偵測位置**完全不同**，其中三條在手機掃描下永遠是陰性。一份乾淨的掃描報告換來的安全感，多數時候是查錯了位置的產物。
2. **現行防護的失效不是實作品質問題，而是前提假設問題。** 自動警示假設「被監控者持有相容手機」、掃描引擎假設「惡意程式與正當程式可由行為區分」、安全通知假設「收件人就是被保護的人」。在親密關係監控這個最主要的濫用情境中，這三個假設同時不成立——加害者同住、共用帳單、且經常就是那支手機的購買者。
3. **偵測行為本身有風險，因此順序不能顛倒。** 若手機已被監控，則在該手機上進行的每一次查證與求助都可能即時呈現在加害者面前。方法論必須從「改用一部乾淨裝置」開始，而不是從掃描開始。同理，發現監控後立即移除，等同於向對方宣告已經察覺——而那正是危險程度最高的時刻。
4. **裝置不可信時，網路側仍是獨立的觀測點——但它的極限可以量出來。** 本團隊在受控環境中，對九種回報週期與抖動的組合各觀測三十個視窗（第 6 章）。**結論的形狀是：時序判準會被抖動擊垮，流量方向判準不會——但方向判準在本實驗中的零誤判，是背景流量設計的產物，不足以支持它在真實網路可用。** 具體數值與其限制見該章。

行動建議：若您懷疑自身被監控，請勿在可疑的手機上搜尋求助資訊；請改用他人或公用裝置。發現任何監控跡象後，切勿立即移除或丟棄——請先評估人身風險，再完成證據保全。

---

1. 問題陳述

1.1 一個威脅，四條途徑

被監控者感受到的是單一現象：**對方總是知道**。知道他去了哪裡、和誰見面、說了什麼、什麼時候離開家。

但這個現象背後有四條技術上完全不同的途徑：

途徑	加害者需要什麼	洩漏什麼
A　實體追蹤器	一次把裝置放入物品或車輛的機會	位置
B　帳號層	知道雲端帳號的密碼	位置、照片、備份、通訊錄，視平台亦可能包含訊息
C　裝置層	一次拿到解鎖狀態手機的機會	幾乎全部——含訊息內容、通話、畫面
D　設定層與周邊	一次代為「幫你設定」的機會	依設定而定，且**更換手機通常無效**

這四條途徑共用同一個威脅模型（第 2 章），卻需要四種不同的檢查位置。**這正是本白皮書把四條途徑放在一起處理的理由**：若只針對其中一條檢查，讀者很容易在完成後得到「已經查過了」的結論，而實際上另外幾條途徑連碰都沒碰到。

1.2 台灣的具體情境

《跟蹤騷擾防制法》於 2022 年施行，其規範的行為態樣包含以電子通訊、網際網路或其他設備對特定人持續監視、追蹤或掌握行蹤；《刑法》妨害電腦使用罪章與妨害秘密罪章對無故入侵他人電腦設備、無故竊錄他人非公開活動亦設有處罰。

法律工具存在。缺的是另一端：**法律規定了什麼行為違法，卻沒有教人如何發現違法正在發生。** 被害者面對的實務問題是：

- 我懷疑遭到監控，但應如何證明？
- 手機沒有跳出任何警示、防毒掃描也沒有異常，是否即代表安全？
- 我發現了可疑的裝置或程式，直接移除是否即可？

第三個問題的直覺答案是錯的，而且錯得可能危及人身安全（見 7.1 節）。

1.3 本白皮書要回答的問題

1. 監控是如何發生的（統一威脅模型與四條技術途徑）
2. 現行防護為何在這個情境下失效（結構性缺口，而非實作瑕疵）
3. 如何自行偵測（分層方法論、各層的涵蓋範圍、以及陰性結果的意義）
4. 裝置不可信時還能怎麼觀測（網路側量測，含本團隊實測結果）
5. 發現後如何處置（人身安全、證據保全、法律途徑、清理順序）

2. 統一威脅模型

2.1 攻擊者分型

類型	動機	特徵
親密關係加害者	控制、監視行蹤與人際往來	**最大宗**：具備長期實體接觸機會，且經常知道或能取得解鎖密碼
分手／離婚糾紛當事人	蒐證、持續掌控	關係存續期間建立的存取往往在分手後仍然有效
家庭內監控	以關心為名的控制	使用親子監護工具監控成年或近成年家庭成員
職場監控逾越	管理之名的越界	公司裝置或行動裝置管理權限被用於工作範圍外
竊盜前置勘查	掌握屋主作息	目標是物品而非人，追蹤器多置於車輛

本白皮書主要針對前兩類，因為它們同時具備**最高的存取機會**與**最嚴重的人身後果**。

2.2 能力假設：技術能力為零

這是本威脅模型最需要強調的一點：**攻擊者的技術能力假設為零**。

不需要撰寫程式、不需要越獄或改機、不需要理解藍牙協定或作業系統。他需要的只是下列**任一**項：

- 一次把追蹤器放入對方物品或車輛的機會；
- 一次拿到解鎖狀態手機的機會，或知道解鎖密碼；
- 知道雲端帳號的密碼，或能通過其密碼重設流程；
- 曾經以「幫你把手機設定好」之名義經手過裝置。

在親密關係中，這幾項幾乎是日常。**知道伴侶的解鎖密碼在多數關係中被視為信任的表現——威脅模型必須承認這個社會現實**，而不是假設密碼保密。

正因為門檻如此之低，這類威脅的普遍程度遠高於需要技術能力的攻擊手法。防禦思考不能假設對手技術高明——恰恰相反，要假設對手完全不懂技術，卻擁有充足的接觸機會。

2.3 被害者處境

- **不知情期間長**：在收到警示或主動察覺之前，監控可能已持續數週至數月。
- **知識不對稱**：加害者知道自己放了什麼、設定了什麼；被害者連該找什麼都不清楚。
- **查證管道本身被監控**：最自然的反應是「用手機搜尋因應方式」——而那支手機可能正是被監控的裝置。
- **無從區分同意與脅迫**：在控制型關係中，「自願」交出密碼、「自願」安裝定位 App 可能是在壓力下發生的。技術機制看到的是一次合法授權，看不到授權背後的脅迫。
- **多點同時失守**：加害者可能同時掌握手機、雲端帳號、電子信箱與車輛服務。任何單點的清理都可能立即被其他失守點察覺並復原。

2.4 一條貫穿全篇的原則

上述處境收斂成一條原則，它決定了本白皮書所有程序的順序：

> **不能假設受檢裝置是可信的工具。** 在追蹤器情境中手機通常還能當工具用；在其餘三條途徑中，那支手機本身就是調查對象。凡是在受檢裝置上做的檢查，其結果無論陰陽都不可信，而且檢查行為本身可能被看見。

---

3. 四條監控途徑

3.1 途徑 A：實體追蹤器

低價藍牙追蹤器原本是為了尋找遺失物品而設計，但它們的三項特性——單價低廉、電池以年為單位、依附全球群眾外包網路而無須自備連線——使其同時成為理想的跟蹤工具。

追蹤器本身不知道自己在哪裡。 它沒有 GPS，也沒有行動網路，只做一件事：持續以低功耗藍牙廣播一段識別訊號。定位發生在別人的裝置上：

1. 追蹤器廣播識別訊號；
2. 任何一支經過的、屬於同一生態系的手機接收到訊號；
3. 該手機用自己的 GPS 判斷「我在這裡，而我聽到了這個識別訊號」；
4. 這筆資訊經加密後上傳至廠商伺服器；
5. 追蹤器的擁有者查詢時，取得解密後的位置。

代為回報的路人手機**無從得知自己回報了什麼**，位置資訊以端對端加密方式僅有擁有者能解讀。對一般使用者的隱私而言，這是良好的設計。

輪替識別碼的雙面性：為避免追蹤器變成長期可追蹤的固定標記，各生態系的裝置會定期輪替其廣播的識別碼。這保護了一般使用者——路人無法靠持續觀察某個固定識別碼來記錄您的行蹤。但對**正在被追蹤的人**，同一項設計造成困難：您無法靠「這個識別碼一直跟著我」來判定，因為識別碼會變；通用型藍牙掃描工具看到的是一串不斷變動的匿名裝置，難以與環境中大量其他藍牙裝置區分。

這是一個經典的隱私設計權衡：保護多數人不被追蹤的機制，讓少數正在被追蹤的人更難自救。 理解這一點，才能理解為何自助偵測不能只靠通用掃描 App。

各生態系的網路密度差異極大，而**網路密度直接決定定位精度與更新頻率**：在裝置密度高的都會區，追蹤的即時性遠高於裝置稀疏的區域。

3.2 途徑 B：帳號層（無須在裝置上安裝任何東西）

只要知道雲端帳號的密碼，加害者即可從自己的裝置登入，取得該帳號同步的一切：定位、照片、備份內容、通訊錄、行事曆，視平台而定亦可能包含訊息。

這條途徑有三個對加害者極為有利的特性：

- **裝置掃描永遠陰性**：手機上沒有任何額外程式；

- **持續有效**：只要密碼不變、登入工作階段不被登出，存取就持續存在；
- **來源難以察覺**：多數人不會定期檢查帳號的登入裝置清單。

此外，平台內建的**位置共享**與**家人共享**功能，若在關係存續期間開啟而在關係惡化後未關閉，效果等同於一條被遺忘的監控通道。

3.3 途徑 C：裝置層（需要一次實體接觸）

即在手機上安裝監控程式。兩大平台的樣貌不同：

- **Android**：允許自商店以外來源安裝應用程式。監控程式安裝後，典型作法是請求**無障礙服務**與**裝置管理員**等高權限——這些機制原為輔助功能與企業管理設計，被反向用於讀取畫面內容、攔截通知與防止移除。安裝後多會隱藏圖示或偽裝為系統元件。
- **iOS**：未經越獄的裝置難以側載具持續性的監控程式，因此 iOS 情境的監控多改走途徑 B 或 D。經越獄的裝置則與 Android 的暴露程度相當，而越獄本身通常會留下可辨識的痕跡：出現非官方商店的安裝介面、系統更新持續失敗、或裝置行為與同型號他機明顯不同。

裝置層的程式可分為兩類，其法律與偵測處境截然不同：

類別	取得方式	偵測處境
雙用途程式	官方商店合法上架，名義為親子監護、裝置防盜、員工管理	**主流**：程式本身合法，掃描引擎無正當理由標記
專用監控套件	側載安裝，明示或暗示用於監看伴侶	較易被安全產品標記，但安裝後會主動隱藏

本白皮書刻意不列出任何監控產品的名稱、來源與安裝方式。 該類資訊對加害者的助益遠大於對被害者：被害者需要的是「如何在自己的裝置上發現異常」，而非「市面上有哪些產品」。此一取捨依循本團隊《研究倫理準則》中關於攻擊性細節的處理原則。

3.4 途徑 D：設定層與周邊裝置

第三條途徑既不是密碼外洩，也不是安裝程式，而是**利用裝置本身的正當設定機制**。它最容易被忽略，因為每一項設定單獨看都是合理功能：

- **管理描述檔與工作設定檔**：原為企業管理裝置而設計，一旦被安裝，可及於流量導向、應用程式派送與部分使用紀錄。以「幫你把手機設定好」為名義完成安裝，在關係中並不突兀。
- **訊息與通話的轉發規則**：於電子郵件設定自動轉寄、於電信服務設定通話轉接、或將簡訊同步至另一部裝置。此類設定一旦建立，**即使更換手機也持續有效**。
- **已配對的周邊裝置**：手錶、車載系統、耳機、平板。配對關係常在關係惡化後仍然存在，而車載系統尤其值得注意——它同時掌握位置歷程與通訊錄。
- **桌面端與瀏覽器的同步**：手機訊息同步至共用電腦、瀏覽器帳號同步書籤與密碼，皆可能形成一條不經過手機的旁路。
- **平台內建的共享功能**：位置共享、家人群組、相簿共享。這些功能設計時的假設是雙方持續同意，但**沒有任何機制會在關係改變時提醒您重新確認**。

3.5 四條途徑的全景比較

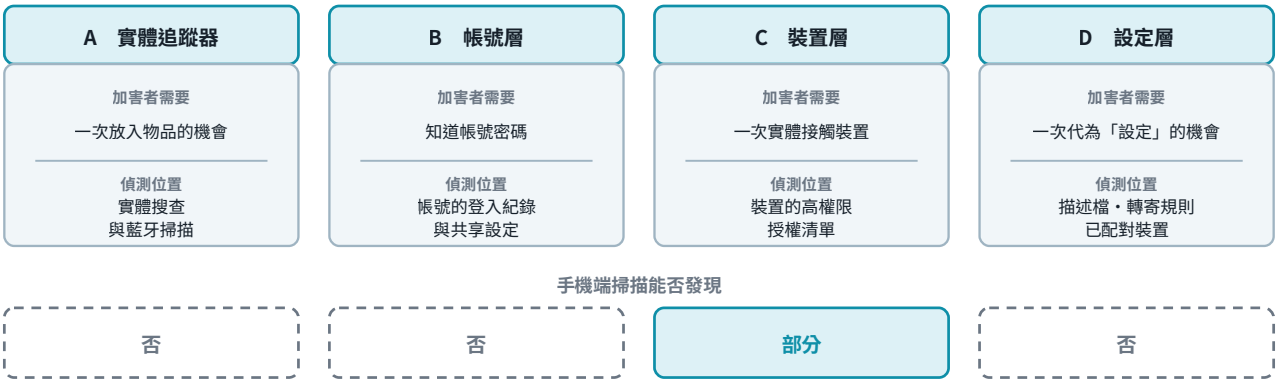

圖 1：四條監控途徑與各自的偵測位置。四條中有三條，手機掃描在原理上看不到。

這張表是本白皮書最該被記住的一頁。四者的關鍵差異不在技術複雜度，而在**應該去哪裡查**：

	A 實體追蹤器	B 帳號層	C 裝置層	D 設定層
需要實體接觸	是（一次）	否	是（一次）	多數需要
手機掃描能否發現	**否**	**否**	部分可	**否**
系統會否主動警示	部分（視生態系）	部分（登入通知）	少見	**否**
偵測位置	實體搜查與藍牙掃描	帳號的登入與共享設定	裝置的高權限清單	裝置設定與外部服務規則
洩漏範圍	位置	位置、備份、相簿、通訊錄	幾乎全部	依設定而定
移除方式	取出裝置（先保全證據）	撤銷工作階段並更換憑證	移除程式並撤銷高權限	逐項檢視並刪除設定
更換手機是否有效	否（追蹤器在物品上）	**否**（帳號未處理則跟著移轉）	是	**否**（多數規則在裝置之外）

最後一列是實務上最常見的誤解：**換一支新手機並不會解除四條途徑中的三條**。若僅更換裝置而未處理帳號，新裝置在登入的當下即再度暴露。

第二列則解釋了為什麼「我掃過了」不能作為結論：**四條途徑中有三條，手機掃描在原理上就看不到。**

---

4. 現行防護的結構性缺口

結論先行：**現行機制對「典型情境下的典型使用者」有效，但近距離監控的加害者不是典型情境。**

4.1 現行機制沿三條線發展

1. **不明追蹤器的自動警示**：偵測到一個不屬於您、且長時間與您同行的追蹤器時發出通知。跨平台的偵測標準（DULT）由主要廠商共同於 IETF 推動。多數追蹤器在與擁有者分離一段時間後亦會主動發出聲響。
2. **程式來源管制與權限可見化**：官方商店的上架審查、對非商店來源安裝的限制、高風險權限改為明示授權、以及權限使用紀錄的回顧介面。
3. **帳號活動通知**：新裝置登入時寄送通知、提供已登入裝置的清單。

這三條線對「陌生人植入惡意程式」的威脅模型是有效的。問題在於，本白皮書的威脅模型並非陌生人。

> **關於具體數值的處理方式**：警示的觸發條件、延遲時間與涵蓋範圍會隨作業系統版本、地區與廠商政策而變動。本白皮書的處理方式不是略去數值，而是**只引用有公開量測支持的數值，並一律附上量測者、受測對象與時點**。理由是：略去數值會讓讀者無從估計風險的量級——「會延遲」與「延遲八小時」對一份安全計畫的意義完全不同；而未標時點的數值則會被當成現況。兩者都有害，標註時點的數值是其中較小的害。**若您需要的是當下的行為，唯一可靠的來源是您自己的裝置。**

4.2 五類結構性缺口

以下五項不是實作瑕疵，而是機制前提與濫用情境之間的落差。它們無法靠調整參數解決。

缺口一：前提假設把最需要保護的人排除在外

自動警示的成立需要三個前提同時滿足：被監控者**持有智慧型手機**、**藍牙開啟**、**系統版本支援該功能**。不符合者實質上不受保護：使用功能型手機的長者、未持有手機的兒童、基於省電或隱私習慣關閉藍牙者、以及使用舊版系統而未更新的人。

這幾個族群與跟蹤騷擾的高風險族群有相當程度的重疊。

同一類問題在裝置層以另一種形式出現：若手機是由加害者購買、設定或「幫忙處理過」的，其信任鏈自始即不完整。目前沒有任何機制能讓使用者事後確認「這支手機在交到我手上之前被做過什麼」。

缺口二：偵測的涵蓋範圍由攻擊者選擇

跨平台標準的存在不等於全面涵蓋。DULT 已於 IETF 成立工作組並產出威脅模型與配件協定的草案，但標準文件描述的是應然，實際偵測能力取決於各廠商在各自平台上的實作範圍與更新推送情形。

從攻擊者的角度，這意味著一個不需要任何技術知識的規避策略：**選擇被害者手機生態以外的追蹤器**。學術界對此缺口的回應之一是跨生態的第三方偵測工具（Heinrich 等人於 2022 年發表的 AirGuard 即為一例，以逆向工程還原 iOS 的追蹤保護邏輯，使 Android 使用者也能偵測 Apple 生態的追蹤器）。**這類工具的存在本身即是缺口的證據**——若原廠涵蓋已足，就不需要它。

更根本的一層是：偵測依賴裝置遵守標準所規定的行為，而**遵不遵守由裝置自己決定**。市面上存在移除發聲元件的改裝品，也存在不參與任何標準的自製裝置；Shafqat 等人於 2023 年更展示了一種可持續回報位置、同時規避被害端警示的克隆追蹤器。**防護機制的有效性建立在攻擊者的配合之上，這在威脅模型上是不成立的假設。**

缺口三：合法授權與脅迫授權在技術上無從區分

一款監護程式的功能清單，與一款監控程式幾乎完全相同。差別不在程式做了什麼，而在**裝置持有者是否知情且自願**——這是程式碼之外的事實，掃描引擎在原理上無從判斷。廠商若一律標記，將誤傷正當使用；若一律不標記，則放行了跟蹤情境中的主力工具。

這不是邊緣情形。Chatterjee 等人於 2018 年對此生態的首次系統性量測即發現，**可用於親密關係監控的應用程式中，絕大多數是具有正當用途的雙用途程式，而非公然的間諜軟體**；Roundy 等人於 2020 年進一步指出，被用於人際攻擊的程式種類遠不止監控一類。換言之，掃描引擎面對的不是少數難以歸類的例外，而是這個問題的主要形態。

系統看到的是一次合法的授權：畫面出現、使用者按下同意。系統看不到的是按下同意時，另一個人正站在旁邊。**在控制型關係中，「自願」是一個技術層無法驗證的概念。**

同一個困境在追蹤器上的對應物是「同行判定的兩難」：判定過於寬鬆會產生大量誤報（與家人同車、在公共運輸上與陌生人長時間同行），使用者很快學會忽略警示；判定過於嚴格則漏報，**尤其在被害者與加害者共處同一空間時——而親密關係暴力恰恰經常是這種情境。當雙方同住或共用車輛，「異常同行」這個訊號本身就失去了鑑別力。**

缺口四：告警的收件人可能就是加害者

若手機的門號、帳單或家庭群組由加害者掌握，則安全通知、登入提醒與訂閱明細會送到加害者手上。更根本的情況是：裝置本身即為加害者所購買與設定。**此時所有以「通知使用者」為設計前提的防護，其保護對象都反轉了。**

缺口五：防護設計假設「發現即應移除」

現行的安全提示幾乎一律建議立即移除可疑程式或裝置。在陌生人威脅模型下這是正確的；在近距離監控情境下，突然中斷的資料回報等同於向加害者宣告「對方已經察覺」，可能直接觸發報復。

偵測與移除之間，需要一個現行機制完全沒有提供的中介步驟：安全評估與證據保全。 本白皮書第 7 章即為此步驟。

4.3 缺口與途徑的對應

缺口	A 追蹤器	B 帳號層	C 裝置層	D 設定層
一　前提假設排除人群	●	○	●	○
二　涵蓋範圍由攻擊者選擇	●	○	●	●
三　授權脈絡不可見	●	●	●	●
四　告警收件人反轉	●	●	●	●
五　假設發現即應移除	●	●	●	●

●＝直接適用　○＝部分適用

缺口三、四、五橫跨全部四條途徑，因為它們的根源不在技術，而在**威脅模型假設了錯誤的攻擊者**。

5. 分層偵測方法論

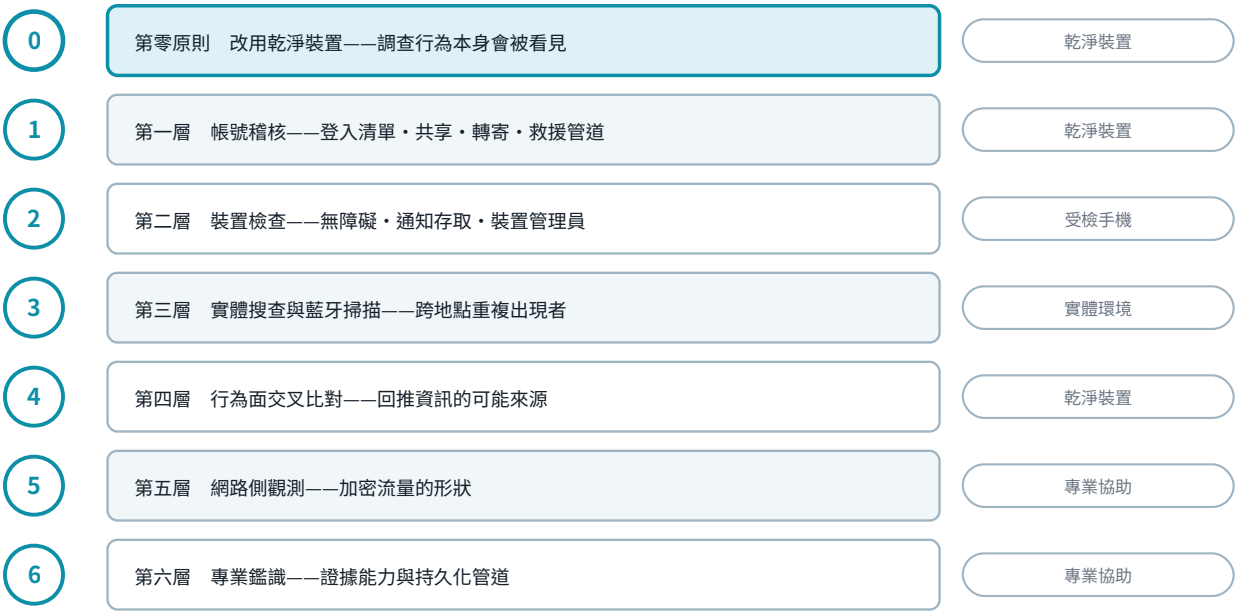

圖 2：六層偵測方法論。第零原則不是準備工作，而是其餘各層可信與否的前提。

第零原則：先取得一部乾淨裝置

這是唯一不可跳過的步驟。

若監控存在，則您在受檢裝置上的每一次搜尋、每一則求助訊息、每一通電話，都可能即時呈現在加害者面前——**包含您正在閱讀本白皮書這件事**。

因此：

- 使用他人的裝置、公用電腦，或一部與您所有既有帳號皆無關聯的裝置；
- 在該乾淨裝置上，**請勿登入**任何您原有的帳號（登入即可能觸發登入通知，反而暴露）；
- 若必須在原手機上維持日常行為以避免引起懷疑，請保持其使用樣態與過去一致。

判別原理：什麼算是發現，什麼不算

沒有明確的判定準則，檢查就只是「看一看」——看完之後既無法確認，也無法排除。

層	陽性判定（達到即應進入第 7 章）	涵蓋之途徑	於何處進行
一　帳號稽核	清單中出現**任何一項您無法指認來源**的裝置、共享對象、轉寄規則或授權	B，及 D 的服務端部分	乾淨裝置
二　裝置檢查	高權限清單中出現您不認得的項目	C，及 D 的裝置端部分	受檢手機（風險最高）
三　實體搜查與藍牙掃描	尋獲不屬於自己的電子裝置；或**同一標的在三個以上不同地點、間隔一段時間後重複出現**	A	實體環境
四　行為面交叉比對	對方掌握的資訊，其可能來源已收斂至特定途徑	四條皆可，但只能指向不能確認	乾淨裝置
五　網路側觀測	於網路邊界觀察到上行明顯大於下行的持續連線（週期性可作佐證，但單獨不可靠——見第 6 章）	B、C，部分 D	需要專業協助
六　專業鑑識	由鑑識人員判定	全部	專業協助

第一層與第二層的判準是同一句話：**「您無法指認來源」即為陽性**，而不是「看起來可疑」。這個區別很重要——監控程式會偽裝成系統元件，共享關係會顯示為合理的名稱；若判準是「看起來可疑」，偽裝成功的項目就會被自己排除掉。**能不能說出這一項是何時、由誰、為何建立的，才是可靠的判準。**

第三層的判準值得特別說明：**單次掃描看到未知藍牙裝置沒有任何意義**——都市環境中隨時有數十個裝置在廣播。有意義的訊號是**同一標的跨地點重複出現**，因為唯有如此才能排除「那是別人的裝置，只是剛好在附近」。這也正是識別碼輪替削弱通用掃描工具的原因（見 3.1 節）。

第四層的判定則本質不同：它只能**縮小範圍**，不能確認。它的價值在於當技術檢查全為陰性時，它往往是唯一還能推進的方法。

陰性結果的三種來源

這是本方法論最重要的一段。當您做完檢查而沒有發現任何東西，可能的原因有三種，而**它們對後續行動的意涵完全不同**：

1. **真陰性**：確實沒有監控。
2. **查錯位置**：確實有監控，但不在您檢查的那一層。**在本主題中這是主要情形而非例外**——四條途徑中有三條在裝置掃描下永遠是陰性（見 3.5 節）。一份乾淨的手機掃描報告，完全不排除帳號層與設定層的監控。
3. **檢查本身失效**：檢查根本沒有真的執行到。例如藍牙被關閉而掃描其實未運作、定位權限未授予而警示機制從未啟用、在受檢手機上進行了本該於乾淨裝置進行的稽核、或只檢視了應用程式清單而未檢視高權限授權清單。

第三種最危險，因為它與真陰性**在外觀上完全一樣**：兩者都是「什麼都沒找到」。因此在採信任何陰性結果之前，必須先確認檢查本身處於可運作狀態——附錄 A 的準備清單即為此用途。**它不是準備工作，而是陰性結果能否被採信的前提。**

> 這條原則來自本團隊的量測經驗：WP-003 的研究中曾三次遇到儀器已經壞掉、輸出卻與真實的陰性結果一模一樣的情況，若未察覺就會把「沒有洩漏」當成結論。第 6 章的量測因此把陽性對照列為每次執行的前置條件。**先驗證工具處於可量測狀態，再看結果**——這條原則對自助偵測同樣成立。

第一層：帳號稽核（於乾淨裝置進行，風險最低）

帳號層是最普遍也最常被略過的一層。請逐項檢視：

- **已登入的裝置清單**：是否有您不認得的裝置或地點？請留意名稱貌似合理但實際上並非您所有的項目。
- **位置共享與家人群組**：目前有誰能看到您的位置？共享是何時開啟的？
- **郵件的自動轉寄與過濾規則**：是否存在您未曾建立的轉寄規則？此為最常見且最持久的旁路之一。
- **帳號的救援管道**：救援電子郵件與救援電話號碼是否仍為對方所有？**若救援管道未清理，更換密碼的效果可能在數分鐘內被撤銷。**
- **雙因素驗證的設定**：第二因素是否綁定在對方能取得的裝置或號碼上？
- **應用程式專用密碼與已授權的第三方應用**：是否存在您不記得授權過的項目？
- **備份設定**：備份的目的地帳號是否確實為您本人所有？

第二層：裝置檢查（於受檢手機操作，風險最高）

請先閱讀 7.1 節再進行本層。 本層的所有操作都可能被監控程式記錄。

裝置層監控為求持續運作，必須取得少數幾類高權限，因此檢查的重點不是「找出可疑的圖示」，而是**逐一檢視這幾份權限清單，確認每一個項目您都認得**：

- **無障礙服務的授權清單**：此為讀取畫面內容與模擬操作的關鍵權限，正當用途的程式數量極少。
- **通知存取的授權清單**：取得此權限即可讀取所有應用程式的通知內容，包含訊息預覽。
- **裝置管理員或裝置擁有者權限**：取得此權限的程式無法以一般方式移除。
- **管理描述檔與工作設定檔**：您未曾任職的公司或您不認得的組織名稱，皆屬異常。
- **非官方來源安裝的授權**：哪些應用程式被允許安裝其他應用程式？
- **電池與行動數據的用量排行**：持續於背景回傳資料的程式，會在這兩份清單上留下痕跡，即使其圖示已隱藏。
- **已配對的藍牙裝置與已知的無線網路**：是否有不屬於您的項目？

若在上述任一清單中發現不認得的項目，請**記錄其完整名稱後停止操作**，直接進入第 7 章。

第三層：實體搜查與藍牙掃描（針對途徑 A）

主動掃描（約十分鐘）：使用各生態系官方 App 的手動掃描功能，或以開源工具進行通用低功耗藍牙掃描。掃描時**遠離自己的其他裝置**，並在移動中於不同地點重複掃描至少三次——真正跟隨您的裝置會在不同地點重複出現。

實體搜查（一至數小時，不需任何工具）：當掃描無所獲但懷疑仍然存在，實體搜查往往是最有效的方式。**應按固定順序進行，勿憑直覺隨意翻找。**

- **車輛**（最常見的放置處）——車外：前後保險桿內側、輪拱、車底樑架、牌照框後方、拖車勾附近；車內：座椅下方與椅縫、備胎槽、後車廂側邊置物槽、雜物箱深處、車頂內襯邊緣。檢查所有磁吸可附著的金屬平面——磁吸盒是常見的搭配配件。
- **隨身物品**：背包與提包的夾層與底部襯墊下方、外套內襯與口袋縫線異常處、皮夾夾層、行李箱襯裡與輪座、以及常帶物品中重量或厚度異常者。
- **住家與贈禮**：對方贈送的玩偶、擺飾、電子配件；兒童的書包與玩具（在監護權爭議情境中應特別檢查）。此處也可能涉及錄音錄影裝置，處理方式不同，建議轉由專業協助。

搜查時的安全提醒：若加害者可能觀察到您正在搜查（例如同住），搜查行為本身可能升高風險。此情況下應先與專業協助者討論時機。

第四層：行為面交叉比對（於乾淨裝置進行，最容易被低估）

技術檢查為陰性時，本層往往是唯一能夠推進的方法。作法是把「對方知道的事」逐一列出，並回推**該項資訊的可能來源**：

- 對方知道的是**位置**，或是**對話內容**？前者可能來自途徑 A 或 B，後者則指向途徑 C 或通知存取。
- 對方知道的是**已寄出的訊息**，或**尚未寄出的草稿**？後者的來源範圍極窄。
- 對方掌握的資訊是**即時**，或**延遲數小時**？後者較符合定期同步或備份的模式。
- 對方是否知道**只出現在特定一部裝置**上的事？此可直接縮小範圍至該裝置。

請以書面記錄每一次事件的日期、對方所知的具體內容，以及您當時所在之處——此份紀錄同時也是 7.2 節的證據基礎。

第五層：網路側觀測（需要專業協助）

前四層都在受檢裝置或其帳號之內進行；當這些檢查全為陰性、而 2.4 節的原則又提醒我們受檢裝置本身不可信時，**唯一還沒被污染的觀測位置是網路邊界**。

監控程式必須把資料送出去，而送出去的流量會經過某一台路由器。內容雖然加密，**流量的形狀不會被加密**：什麼時候送、送多少、送去哪裡、上行與下行的比例，全部可見。

這些線索的份量並不相等。本團隊的實測顯示，**承擔鑑別力的是「上行明顯大於下行」，不是「回報很規律」**——後者可被零成本的抖動規避，且會把良性的心跳流量一併誤判。第 6 章即為該量測，含其適用界線。

這一層需要設備與專業判讀，不屬於自助範圍。

第六層：專業鑑識（何時應停止自行處理）

出現下列任一情形時，請停止自行檢查並尋求專業協助：

- 找到裝置，但無法判斷其種類或是否具備錄音錄影能力；
- 已在裝置上發現高權限的不明程式，且涉及人身安全的立即風險；
- 監控疑似來自具技術能力的加害者，或涉及工作用裝置與企業管理權限；
- 案件可能進入司法程序，需要具備證據能力的鑑識報告；

- 已多次清理但監控狀態反覆恢復——此通常代表尚有未被發現的持久化管道。

自行操作與鑑識取證之間存在難以兼顧之處：任何清理動作都會破壞現場。**若法律途徑對您而言重要，保存優先於清除。**

---

6. 網路側觀測：加密流量中的週期性回報

6.1 為什麼需要一個裝置之外的觀測點

第 5 章的前四層有一個共同的弱點：它們都在受檢裝置或其帳號之內進行，而那正是可能已被控制的地方。第五層把觀測位置移到裝置之外。

其立論基礎是一個結構性事實：**監控要有價值，資料就必須離開裝置。** 加密可以保護內容，但無法隱藏「有東西定期被送出去」這件事。因此問題變成：在只看得到流量中繼資料的位置上，週期性回報究竟有多容易被認出來？

這個問題有實務意義，因為它決定了一項服務能不能做：若判準只在理想條件下有效，宣稱能以網路側偵測監控就是在販售安全感。因此本團隊實測了它的極限。

6.2 實驗環境

量測於 **BCN-349** 進行——一個以 EVE-NG 建置的四節點受控環境，位址全部採 RFC 5737 文件用範圍，完整的拓撲、佈建腳本、原始數據與分析程式隨本白皮書公開（見附錄 D）。

節點	角色
PHONE	受監控端。同時產生週期性回報流與背景的正常應用流量
GW	**觀測點**（家用路由器角色）。全程擷取流量
C2	監控服務端。以 TLS 接收上傳並回覆短 ack
WEB	良性服務端。供背景流量使用

受測對象是「週期性回報」這個行為模式，不是任何真實監控產品。 本實驗不涉及任何監控軟體樣本，也不對任何產品作評價。

6.3 判準與量測方法

全部判準只使用 GW 上可見的流量中繼資料計算，**不解密任何內容**：

判準	定義	直覺
T　時序判準	相鄰上行事件間隔的變異係數 `CV < 0.15`	人的操作不規律，程式的回報規律
A　方向判準	`上行位元組 ÷ 下行位元組 > 3`	一般使用是下載為主，外傳是上傳為主
T∧A　合併判準	兩者同時成立	—

變因：三種回報週期（2／5／15 秒）× 三種抖動比例（0%／20%／50%），共九組組態。抖動的定義為實際間隔落在週期的正負該比例內均勻隨機。九組於同一觀測視窗內併行，各自使用不同的目的埠以便分流；背景良性流量同時運作，作為偽陽性的分母。**每組組態觀測三十個視窗**；未達三十者不報告該格的統計量，僅報告原始觀察。

> 兩個門檻（`CV < 0.15` 與比值 > 3）是事前選定的固定值。門檻的選擇會左右結論，其代價見 6.5 節——**方向判準的門檻在本實驗中並未受到考驗**。

儀器驗證：每次執行前確認擷取確實看得到全部受測流、且受監控端沒有繞過觀測點的旁路；並以「零抖動」組作為陽性對照——該組若未被時序判準穩定命中，即代表擷取或分析失效，該次執行作廢而非記為陰性。此項直接對應第 5 章〈陰性結果的三種來源〉的第三種。

6.4 結果

三十個觀測視窗**全部通過儀器驗證**：每次執行前後都確認九條受測流齊備（30/30）、零抖動組（陽性對照）確實被時序判準命中（30/30），且抵達監控服務端的 315 條連線全部來自觀測點的對外位址、無一條繞過（315/315）。無效視窗 0 個，下列統計均以三十個視窗為基礎。

偵測（每格 30 個視窗）

週期	抖動	每視窗事件數	CV 中位數（IQR）	T	A	T∧A
2 秒	0%	150	0.0010（0.0002–0.0011）	30/30	30/30	30/30
2 秒	20%	151	0.1158（0.1132–0.1181）	30/30	30/30	30/30
2 秒	50%	150	0.2904（0.2797–0.2977）	**0/30**	30/30	0/30
5 秒	0%	60	0.0002（0.0002–0.0005）	30/30	30/30	30/30
5 秒	20%	60	0.1167（0.1116–0.1205）	30/30	30/30	30/30
5 秒	50%	61	0.2892（0.2772–0.3030）	**0/30**	30/30	0/30
15 秒	0%	20	0.0002（0.0001–0.0002）	30/30	30/30	30/30
15 秒	20%	20	0.1127（0.1064–0.1179）	30/30	30/30	30/30
15 秒	50%	21	0.2926（0.2641–0.3131）	**1/30**	30/30	1/30

> 15 秒／50% 那一格的單次命中發生於第 25 個視窗，該次僅觀測到 17 個事件、CV 為 0.1455，剛好落在門檻之下。**那是 CV 估計的抽樣波動，不是「長週期較易被偵測」**——同一個機制也可能造成一次虛假的漏失。這一點在離散度上看得最清楚：事件數最少的 15 秒／50% 組，其 CV 橫跨 0.1455–0.3652；事件數最多的 2 秒／50% 組只橫跨 0.2692–0.3200。**樣本數影響的是估計的穩定度，不是判準的中心趨勢**——三個週期的 CV 中位數幾乎相同（0.290／0.289／0.293），因為 CV 是無因次量。n＝1，此處只報原始觀察，不主張任何比率。

偽陽性（三十個視窗共 577 條良性流；每視窗中位數 19 條，範圍 15–23）

良性流別	流數	T 誤判	A 誤判	T∧A 誤判
頁面載入流	487	16（3.3%）	0	0
同步流	30	2（6.7%）	0	0
keepalive 流	60	**60（100%）**	0	0
合計	577	78（13.5%）	**0**	**0**

每個視窗中被誤判的良性流數：T 的中位數為 2（範圍 2–4），A 與 T∧A 皆為 0。

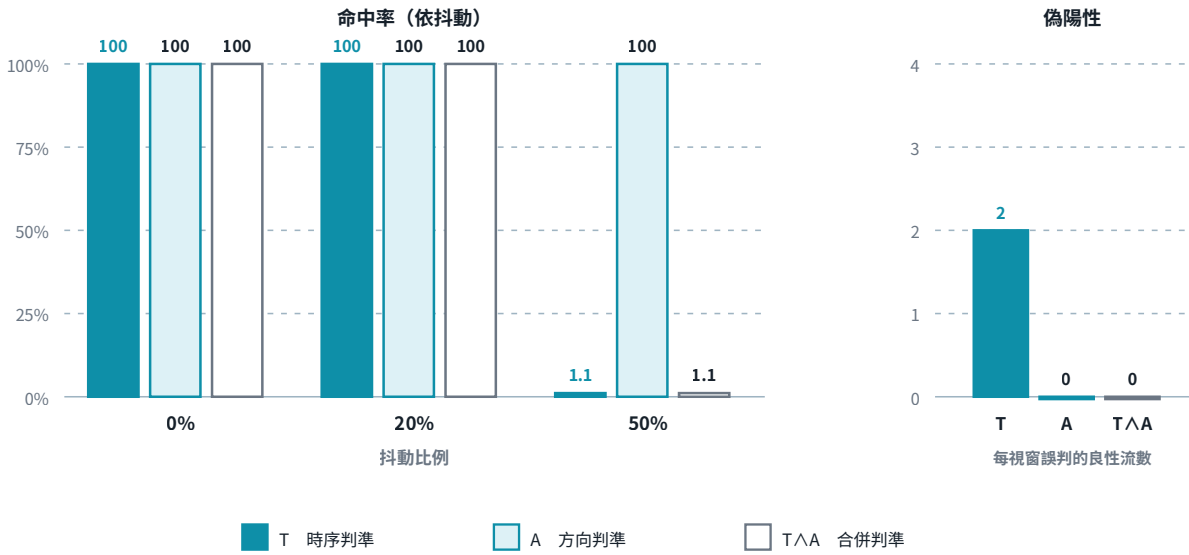

圖 3：BCN-349 實測。左：命中率，每根長條彙整三個週期共 90 個觀測視窗（完整 3×3 結果見 6.4 節的表）——抖動超過臨界值後時序判準失效，方向判準不受影響。右：每視窗被誤判的良性流數中位數（每視窗共約 19 條良性流）——時序判準對良性 keepalive 穩定誤判，這是它不能單獨使用的原因。

三項發現

1. **方向判準在本環境中完全可靠，時序判準不是。** A 在 270 次觀測（九組 × 三十視窗）中全部命中，且對 577 條良性流零誤判；T 則在抖動 50% 時幾乎全部漏失。
2. **時序判準的失效點可以事先算出來，因此可以被零成本規避。** 均勻抖動下，間隔的變異係數為 `CV = j / √3`，與週期長短無關。判準門檻 0.15 因而對應一個抖動臨界值 `j* ≈ 26%`。實測與理論的吻合在千分之三以內：抖動 20% 時實測中位數 0.1158 對理論 0.1155，抖動 50% 時 0.2904 對 0.2887。**要躲過時序判準不需要任何技巧——把抖動設在四分之一以上即可，而抖動的實作成本是零。**
3. **時序判準對良性的週期流量穩定誤判。** 兩條 keepalive 流在全部三十個視窗中都被 T 判為陽性，60/60，100%。這不是偶爾的誤判而是必然：keepalive 的定義就是規律地送出一個小封包。它與外傳的差別不在時序，而在方向。

由此收斂出的論點

在本環境中，**合併判準 T∧A 並不優於方向判準 A 單獨使用**：A 已經是零誤判，加上 T 只會讓它在高抖動時漏掉本來抓得到的目標。時序判準的價值僅限於「對手不知道有人在看時序」的情況——而那正是第 4 章缺口二所指出、不該被當成前提的假設：**防護機制的有效性不能建立在攻擊者的配合之上。**

6.5 這組數據支持與不支持什麼

支持：

- 在只看得到流量中繼資料的位置上，可以把具週期性與上行不對稱特徵的連線，與本實驗所建立的背景流量區分開來。
- 兩個判準對抖動的敏感度顯著不同，且時序判準的失效點與理論預測一致（見發現 2），因此該失效點可外推至本實驗未測試的抖動比例。
- **時序判準單獨使用不成立**：它既可被零成本規避，又對常見的良性週期流量穩定誤判。

不支持：

- **不支持「方向判準在真實網路中也是零誤判」。** 這是本章最重要的一項限制。全部良性流的上下行比最大值為 1.44，而全部受測回報流的最小值為 9.85——兩者之間是一段數倍寬的空白帶。**這意味著門檻設在 3 並未受到任何考驗**：本實驗無法區分「門檻選得好」與「背景流量太容易」。原因是**背景流量不含上行為主的良性流量**——雲端備份、相簿同步、對外視訊、檔案上傳，正是最會挑戰 A 的一類。A 的零誤判是這個背景模型的產物，不是 A 的性質。要主張 A 在真實網路可用，必須另以包含備份與同步流量的環境重測。**本白皮書不作此主張。**
- **不支持「網路側偵測可取代裝置檢查」。** 網路側看不到監控的內容，也無法指認是哪一支程式；它只能指出「有一條連線具備外傳特徵」。
- **不支持**任何關於真實監控產品回報行為的推論。本實驗的受測對象是受控的回報行為，真實產品的週期、抖動與傳輸方式未經量測。
- **不支持**把本章結果外推到加密流量以外的判讀，或外推到本實驗未涵蓋的網路條件。

量測代理的說明：本實驗以 2／5／15 秒為週期的代理，而真實監控軟體的回報週期多為分鐘至小時級。此代理之所以仍有意義，是因為時序判準的行為取決於**抖動與週期的比例**以及**觀測到的樣本數**，而非週期的絕對長度——發現 2 的理論關係即與週期無關，而三個週期的實測結果也確實一致。但它**不能**用來推論「真實情境下需要觀測多久才會累積到足夠的事件數」——那取決於絕對週期，必須另行量測。

---

7. 發現監控後之處置

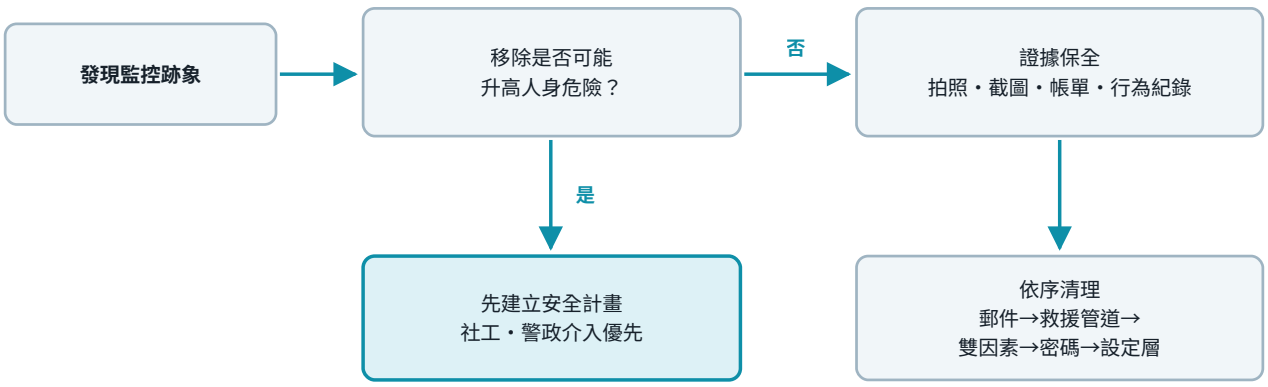

圖 4：發現監控後的處置流程。移除永遠不是第一步。

多數技術指南止於偵測。但對被監控者而言，**找到東西的那一刻才是真正的難題開始**。

7.1 第一優先：人身安全

移除監控是一個會被對方立即察覺的動作。 追蹤器一旦被移除或遮蔽，位置回報就會停止或凍結在原地；程式一旦被刪除、帳號一旦被登出，資料回報隨即中斷。這些對加害者而言都是明確的信號，代表被害者已經察覺並開始行動。

在親密關係暴力的研究中，**被害者採取抵抗或準備離開的階段，正是危險程度最高的階段。**

因此，在處置之前請先確認：

- 您是否已有可執行的安全計畫（安全的去處、可聯繫的人、必要的證件與財物）？
- 移除之後，若對方立即到場或聯繫，您將如何應對？
- 是否有專業的社工或警政管道已經介入？

若答案為否，合理的選擇是暫時維持現狀，先建立支援，再處理技術層面。 監控令人難以忍受，但技術上的清理無法保障人身安全，順序不可顛倒。

若您正處於立即危險，請撥打 110；若需要保護服務與諮詢，請撥打 113。

7.2 證據保全

在移除之前完成下列紀錄。所有紀錄請儲存於**受檢裝置之外**：

若為實體追蹤器：

1. **先在原始位置拍照**，含環境全景與特寫，讓照片能顯示裝置藏放的位置關係；
2. 記錄發現的日期時間與確切位置（車輛哪個部位、包包哪一夾層）；
3. 記錄外觀、序號與可見的識別碼；若手機能讀取到裝置資訊，一併截圖；
4. **請勿重置裝置、請勿拆解、請勿取出電池**——重置會清除與擁有者帳號的關聯，那正是指向加害者的關鍵連結；
5. 若需暫時中斷其功能而不破壞裝置，可裝入不透光的容器或包裝。

若為手機或帳號上的監控：

1. 對可疑程式或設定的畫面截圖，含其完整名稱與授權狀態；
2. 帳號登入紀錄的截圖，含裝置名稱、時間與地點；
3. **訂閱與帳單紀錄**——商用監控服務需要付費，金流是最有力的證據之一；
4. 第四層所建立的行為對照紀錄（日期、對方所知內容、您的實際行蹤）；
5. 若可能，請他人以另一部裝置**拍攝您操作受檢裝置的過程**，以佐證截圖並非事後製作。

共同原則：請勿刪除、請勿重置、請勿更換手機，直到證據保全完成為止。

> **最常見的錯誤**：發現後因驚嚇或憤怒而立刻丟棄裝置或刪除程式。這使得唯一能將行為連結到特定人的物證消失，後續舉證會變得極為困難。**重置是最徹底的清除，也是最徹底的證據銷毀。**

7.3 台灣的法律途徑

- **《跟蹤騷擾防制法》**：其規範的行為態樣包含以電子通訊、網際網路或其他設備對特定人持續進行監視、追蹤或掌握行蹤。被害者得向警察機關報案，經調查後得對加害人核發書面告誡；書面告誡後二年內再犯者，得聲請保護令。
- **《刑法》妨害電腦使用罪章**：無故入侵他人電腦或其相關設備、無故取得或變更他人電磁紀錄，以及製作專供犯本章之罪的程式，均設有處罰規定。
- **《刑法》妨害秘密罪章**：無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位，設有處罰規定。
- **《個人資料保護法》**：非法蒐集、處理或利用個人資料並足生損害於他人者，設有相關責任。
- **《家庭暴力防治法》**：若雙方具有家庭成員或親密關係伴侶關係，得聲請保護令，其款項包含禁止對被害人為騷擾、跟蹤等行為。

報案時建議前往**婦幼警察隊**，或於報案時明確說明涉及跟蹤騷擾與家庭暴力，以便由熟悉此類案件的單位承辦。攜帶 7.2 節所保全的證據，並保留原始裝置。**個案的法律評價應由律師判斷**，本白皮書不構成法律意見。

情境	管道
人身安全立即危險	110
家庭暴力、性侵害、兒少保護	113 保護專線
跟蹤騷擾案件報案	各地警察局婦幼警察隊
法律諮詢	各地律師公會、法律扶助基金會

7.4 重建乾淨環境的順序

順序錯誤是清理失敗最常見的原因。**若在帳號救援管道仍為對方掌握的情況下更換密碼，新密碼可能於數分鐘內被重設。**

1. **於乾淨裝置上，先處理電子郵件帳號**：它是所有其他帳號的救援出口，必須最先奪回。
2. **清理救援管道**：移除不屬於您的救援電子郵件與電話號碼。
3. **重設雙因素驗證**：改綁至僅您本人持有的裝置，並重新產生備用碼。
4. **更換密碼並撤銷所有工作階段**：撤銷登入是關鍵動作——僅更換密碼，既有的登入狀態在部分服務上仍可能持續有效。
5. **依序處理其他帳號**：雲端、社群、金融、電信服務。
6. **清理設定層**：轉寄規則、通話轉接、位置共享、家人群組、已配對裝置、管理描述檔。
7. **最後才處理受檢裝置本身**：於證據保全完成後回復原廠設定，並且**切勿自舊備份還原**——舊備份可能含有監控設定。請以手動方式重新設定。
8. **檢視所有其他裝置**：平板、電腦、車載系統、智慧家庭裝置。

完成後，請於數週內重新執行第一層帳號稽核。**監控狀態的復發，通常代表清單上仍有一項未被發現的管道。**

8. 給廠商與政策制定者的建議

對追蹤器與行動平台廠商：

1. **偵測能力不應以生態系為界**：加害者選擇裝置時完全不受生態系限制，跨平台偵測的涵蓋範圍應盡快趨於完整。
2. **正視「共處空間」的漏報情境**：現行以異常同行為核心的判定邏輯，在最主要的濫用情境中鑑別力最低。此處需要的可能不是更靈敏的參數，而是不同的判定思路。
3. **為不持有智慧型手機者提供路徑**：例如低成本的獨立偵測裝置，或可由第三方（社工、警察單位）代為執行的檢測工具。
4. **將帳號層納入安全檢查的單一入口**：目前使用者必須橫跨多個設定畫面才能完成一次完整稽核。單一入口應涵蓋已登入裝置、位置共享、轉寄規則、救援管道與第三方授權，並可一鍵撤銷。
5. **共享關係應設有效期與定期再確認**：位置共享與家人群組不應永久有效而無任何回顧提示。
6. **雙用途程式的常駐揭露**：具備持續回報位置或內容能力的程式，無論其上架分類為何，皆應在被監控裝置上維持不可關閉的常駐指示。**監護的正當用途不因被監護者知情而受損。**
7. **重新設計「發現後」的引導**：警示與安全提示不應一律建議立即移除，應提供「這可能是親密關係監控」的分支，引導至證據保全與求助資源。
8. **通知的收件人應可獨立設定**：安全通知不應僅送往帳單持有人或家庭群組管理者。
9. **裝置交付狀態的可驗證性**：應提供機制，使使用者能確認一部裝置自原廠或自上次重置以來，被安裝了哪些管理描述檔與高權限程式。

對政策制定者與實務單位：

1. **技術偵測能力應納入保護服務體系**：目前被害者需要自行跨越技術門檻，建議在婦幼警察隊與家暴防治中心層級建立基本的檢測能力與轉介機制。
2. **證據保全指引應公開且易取得**：7.2 節的內容應該是每一位受理員警都能當場告知被害者的標準說明。
3. **第一線受理人員需要數位監控的基本識讀能力**，被害者取證的協助管道亦應納入數位證據的處理。

9. 研究限制與後續工作

9.1 外部效度界線

第 2 章至第 5 章結論的性質是「機制在原理層面存在這些缺口」，而不是「某平台或某產品目前的表現如何」。

- 本白皮書**沒有**測試任何追蹤器產品、任何手機的偵測功能，也沒有測試任何平台的防護，**不應**被引用為對任何產品或平台的評價或比較。
- 引用的他人量測結果，其適用範圍僅止於該研究所述的受測對象、版本與時點。廠商的行為會改變，而且已知會改變。
- 第 3 章的途徑分類與第 4 章的缺口分析建立在公開文件所描述的機制之上。若某廠商的實際實作與其文件描述不符，該部分推論即不適用於該廠商。

- **第 5 章的方法論未經有效性驗證**：本團隊尚未量測各層檢查的偵測率與偽陰性率，也尚未驗證 7.4 節的清理順序是否確實能中斷監控。它們是依機制原理設計的合理程序，不是已知有效的程序。
- 第 6 章的限制見 6.5 節，其結論不得外推至該章實驗未涵蓋的條件。
- 本白皮書不點名特定產品，亦不記載監控程式的取得與安裝方式，此為刻意的取捨（見 3.3 節）。代價是讀者無法自行複核該部分敘述；本團隊認為相較於降低對加害者的助益，此代價可以接受。
- 法律敘述以台灣現行法規為範圍，且不構成法律意見。

9.2 預先登記的實驗設計（v2.0）

以下設計於實測開始之前公開，目的是讓外界能在看到結果之前檢驗設計本身。**先公開設計再產生數據，事後就無法藉由調整判準來遷就結果。**

共同設定

- **受測對象**：三大生態的追蹤器各一，搭配兩大平台的測試裝置各一；監控途徑則於本團隊自有之測試裝置上分別建立。所有裝置於每次執行前回復原廠設定。
- **對照組設計**：每個情境只建立一條途徑——若同時建立兩條，偵測到的結果即無從歸因於哪一條。並以未受監控之同型裝置為對照。
- **重複次數**：追蹤器情境每種組合每個情境 20 次；途徑 B 至 D 每種組合 10 次。未達次數者不報告該格的統計量，僅報告原始觀察。
- **儀器驗證**：每次執行前以已知存在的監控驗證該層檢查確實能看到它（陽性對照）。**陽性對照未通過即中止該次執行**，不併入統計。
- **統計呈現**：時間類數值一律報告中位數與四分位距而非平均值（分布右偏，平均值會被離群值拉走）。
- **公開範圍**：全部原始紀錄與分析腳本隨 v2.0 發布，格式比照本白皮書附錄 D。**監控樣本本身不對外散布。**

實驗矩陣

編號	情境	受測變因	主要量測項
E1	跨生態偵測矩陣	追蹤器生態 × 手機平台	是否曾出現警示；首次警示的延遲
E2	警示延遲分布	時段（日間／夜間）	分離至警示的時間分布
E3	共處空間	擁有端是否與被害端持續同處	警示是否觸發；與 E2 同條件下的差異
E4	各層偵測率	監控途徑 × 檢查層	該層是否發現該途徑；偽陰性率
E5	清理完整性	清理順序（依 7.4 節／隨意順序）	清理後監控是否確實中斷；數週後是否復發
E6	換機是否有效	是否同時處理帳號	新裝置登入後監控是否恢復

每個情境只改一件事。

預先聲明的可證偽條件

若下列任一情形出現，對應主張即應視為被推翻，v2.0 將明確記載該結果：

- E1 中所有生態 × 平台組合皆於相近時間內觸發警示 → **缺口二**不成立。
- E3 的警示觸發情形與 E2 無顯著差異 → **缺口三**中關於共處空間的推論不成立。

- E4 中裝置層檢查能穩定發現途徑 B 或 D 的監控 → 3.5 節的比較表需修正。
- E5 中隨意順序與 7.4 節順序的清理成效無差異 → 該節「順序很重要」之主張不成立。
- E6 中僅更換裝置即可解除監控 → 3.5 節末段之主張有誤。

倫理與法律前提：依本團隊《研究倫理準則》第 4.1 節，所有實驗的受測對象僅限研究人員本人，或經書面知情同意的自願者。不對任何未同意者進行測試，不使用任何真實被害者的裝置或資料，追蹤器全程置於研究人員自有之物品上。

9.3 我們希望收到的回饋

- 實務工作者（社工、員警、律師）對第 7 章流程可行性的意見；
- 對第 4 章缺口分析的補充或反證；
- 各層檢查是否有本白皮書未涵蓋的持久化管道；
- 第零原則對於缺乏第二部裝置的被害者是否過於嚴苛；
- 台灣本地的案例樣態（**請勿提供可識別當事人的資訊**）。

意見請寄 `contact@odysec.org`；涉及敏感內容請以 PGP 加密寄至 `security@odysec.org`。

附錄 A：偵測檢查表

> 可單獨列印使用。

開始之前 - ☐ 評估：處置是否可能升高加害者的危險行為？若是，先聯繫 113 或警方 - ☐ 已取得一部與自身帳號無關聯的乾淨裝置 - ☐ 未在該乾淨裝置上登入既有帳號 - ☐ 未於受檢手機上搜尋求助資訊

準備：確認檢查本身有效

> 本段不是準備工作，而是**陰性結果能否被採信的前提**。任一項未通過，則「沒有發現」只代表檢查機制從未啟用（見第 5 章〈陰性結果的三種來源〉）。

- ☐ 藍牙已開啟
- ☐ 定位權限已授予
- ☐ 作業系統為最新版本
- ☐ 追蹤警示通知未被關閉
- ☐ 已安裝對應另一生態系的偵測 App

第一層：帳號稽核（乾淨裝置） - ☐ 已登入裝置清單逐項確認 - ☐ 位置共享與家人群組逐項確認 - ☐ 郵件自動轉寄與過濾規則逐項確認 - ☐ 救援電子郵件與救援電話號碼確認為本人所有 - ☐ 雙因素驗證綁定於本人持有之裝置 - ☐ 第三方應用程式授權逐項確認 - ☐ 備份目的地帳號確認為本人所有

第二層：裝置檢查（受檢手機，風險最高） - ☐ 無障礙服務授權清單 - ☐ 通知存取授權清單 - ☐ 裝置管理員或裝置擁有者權限 - ☐ 管理描述檔與工作設定檔 - ☐ 允許安裝其他應用程式的來源清單 - ☐ 電池與行動數據用量排行 - ☐ 已配對藍牙裝置與已知無線網路

第三層：實體搜查與藍牙掃描 - ☐ 遠離自己的其他藍牙裝置後執行官方 App 的手動掃描 - ☐ 於**不同地點**重複掃描至少三次，記錄重複出現的未知裝置 - ☐ 車外：保險桿內側、輪拱、車底、牌照框後方 - ☐ 車內：座椅下方與椅縫、備胎槽、後車廂側槽、雜物箱、車頂內襯邊緣 - ☐ 背包提包：夾層、底部襯墊下方 - ☐ 衣物：外套內襯、縫線異常處 - ☐ 皮夾、行李箱襯裡與輪座 - ☐ 對方贈送的物品 - ☐ 兒童的書包與玩具

第四層：行為面交叉比對（乾淨裝置） - ☐ 已列出對方所知之具體事項 - ☐ 已區分位置類與內容類資訊 - ☐ 已判斷資訊為即時或延遲 - ☐ 已記錄日期、內容與自身行蹤

若發現任何監控跡象 - ☐ **請勿立即移除、請勿重置、請勿丟棄** - ☐ 已評估移除是否會升高人身危險 - ☐ 追蹤器：已於原始位置拍照（全景＋特寫）、記錄時間地點與識別碼 - ☐ 手機與帳號：已完成截圖與登入紀錄之保全（存於受檢裝置之外） - ☐ 已保存訂閱與帳單紀錄 - ☐ 已記錄自己的行蹤時間軸 - ☐ 已攜帶證據至婦幼警察隊報案 - ☐ 清理依「郵件→救援管道→雙因素→密碼與工作階段→其他帳號→設定層→裝置」之順序進行 - ☐ 未自舊備份還原 - ☐ 已於數週後重新執行第一層稽核

附錄 B：名詞對照

中文	English	日本語
藍牙追蹤器	Bluetooth tracker	Bluetooth トラッカー
群眾外包定位網路	crowd-sourced location network	クラウドソース型位置ネットワーク
意外追蹤警示	unwanted tracking alert	不要な追跡の通知
輪替識別碼	rotating identifier	ローテーション識別子
跟蹤軟體	stalkerware	ストーカーウェア
雙用途程式	dual-use application	デュアルユース・アプリ
帳號層監控	account-level surveillance	アカウント層の監視
無障礙服務	accessibility service	ユーザー補助サービス
通知存取	notification access	通知へのアクセス
裝置管理員	device administrator	デバイス管理者
管理描述檔	configuration profile	構成プロファイル
工作設定檔	work profile	仕事用プロファイル
工作階段	session	セッション
救援管道	account recovery options	アカウント回復手段
雙因素驗證	two-factor authentication	二要素認証
乾淨裝置	clean device	クリーンな端末
證據保全	evidence preservation	証拠保全
持久化	persistence	永続化
判定準則	decision criterion	判定基準
偽陰性	false negative	偽陰性
變異係數	coefficient of variation	変動係数
流量中繼資料	traffic metadata	トラフィックのメタデータ
外部效度	external validity	外的妥当性
預先登記	pre-registration	事前登録

附錄 C：參考文獻

本白皮書技術主張的依據全部列於此。**凡引用他人量測結果之處，請連同其受測對象與量測時點一併引用。**

學術研究

1. Heinrich, A., Stute, M., Kornhuber, T., & Hollick, M. (2021). Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System. Proceedings on Privacy Enhancing Technologies, 2021(3), 227–245. https://petsymposium.org/popets/2021/popets-2021-0045.pdf — 群眾外包定位網路的機制分析，為 3.1 節技術背景之依據。

2. Heinrich, A., Bittner, N., & Hollick, M. (2022). AirGuard — Protecting Android Users from Stalking Attacks by Apple Find My Devices. ACM WiSec 2022（最佳論文獎）. https://arxiv.org/abs/2202.11813 — 跨生態偵測工具之設計與實地使用觀察，為缺口二之依據。

3. Shafqat, N., Gerzon, N., Van Nortwick, M., Sun, V., Mislove, A., & Ranganathan, A. (2023). Track You: A Deep Dive into Safety Alerts for Apple AirTags. Proceedings on Privacy Enhancing Technologies, 2023(4), 132–148. https://petsymposium.org/popets/2023/popets-2023-0102.pdf — 警示延遲的實測（含日間逾八小時之觀察）與克隆追蹤器規避警示之展示，為 4.1 節與缺口二之依據。**該量測針對特定產品，執行於 2023 年，之後的系統版本行為可能不同。**

4. Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., & Ristenpart, T. (2018). The Spyware Used in Intimate Partner Violence. IEEE Symposium on Security and Privacy 2018, 441–458. https://www.ieee-security.org/TC/SP2018/ — 對親密關係監控軟體生態的首次系統性量測，指出雙用途程式為此生態之主體。為摘要與缺口三之依據。

5. Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. ACM CHI 2018（最佳論文獎）. https://dl.acm.org/doi/10.1145/3173574.3174241 — 八十九名參與者的質性研究，為第 2 章「攻擊者技術能力為零、但存取機會充足」之依據。

6. Roundy, K. A., Mendelberg, P. B., Dell, N., McCoy, D., Nissani, D., Ristenpart, T., & Tamersoy, A. (2020). The Many Kinds of Creepware Used for Interpersonal Attacks. IEEE Symposium on Security and Privacy 2020. https://acartamersoy.github.io/papers/roundy_sp20.pdf — 指出人際攻擊所用程式的種類遠不止監控一類，為缺口三之補充依據。

7. Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N., & Ristenpart, T. (2019). Clinical Computer Security for Victims of Intimate Partner Violence. USENIX Security Symposium 2019. https://www.usenix.org/conference/usenixsecurity19/presentation/havron — 由專業人員協助被害者進行技術檢查的實務模型，為第五、六層與第 8 章政策建議之依據。

8. Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., & Dell, N. (2019). "Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. Proceedings of the ACM on Human-Computer Interaction, CSCW 2019. https://dl.acm.org/doi/10.1145/3359304 — 實際介入案例的分析，為 7.1 節「移除即被察覺」之風險評估依據。

標準文件

1. IETF Detecting Unwanted Location Trackers（DULT）工作組。DULT Threat Model, draft-ietf-dult-threat-model；Detecting Unwanted Location Trackers Accessory Protocol, draft-ietf-dult-accessory-protocol. https://datatracker.ietf.org/wg/dult/about/ — 第 4 章所稱「跨平台偵測標準」即指此二份草案。**草案狀態會變動，引用時請以當下版本為準。**

組織資料

1. Coalition Against Stalkerware。跟蹤軟體之定義、實務指引與參與組織資料。https://stopstalkerware.org/
2. IPV Tech Research（Cornell Tech 等機構之聯合研究計畫）。親密關係暴力與技術濫用之文獻與資源。https://www.ipvtechresearch.org/

廠商與平台文件

1. 各追蹤器廠商與兩大行動平台之官方支援文件與隱私說明。因其版本更迭頻繁且與地區設定相關，本白皮書不固定特定版本；**具體行為請以您使用當下的官方文件與您自己的裝置為準**。

法規

1. 中華民國《跟蹤騷擾防制法》、《刑法》妨害電腦使用罪章與妨害秘密罪章、《個人資料保護法》、《家庭暴力防治法》。

本團隊報告

1. Odysec（2026）。《隧道之外：VPN 保護邊界的量測方法與實測結果》。Odysec 研究報告 WP-003。— 量測紀律與「先驗證儀器再看結果」原則之來源。

附錄 D：實驗環境與數據

第 6 章的實驗環境 **BCN-349**、佈建腳本、原始紀錄與分析程式隨本白皮書公開，可自研究發表頁下載。

環境僅使用可自由取得的 Debian 13，**刻意不使用任何不可合法散布的授權映像**，因此讀者可完整重建。位址採 RFC 5737 文件用範圍，金鑰與憑證為 lab 專用固定值——**它們已公開，任何情況下都不得用於真實用途。**

修訂紀錄

版本	日期	變更
1.0	2026-08-30	初版。

引用格式：Odysec（2026）。《貼身的眼睛：近距離監控的偵測與應對》。Odysec 技術白皮書 WP-001，版本 1.0。

免責聲明：本白皮書為技術研究與教育用途，不構成法律意見。個案的法律評價請諮詢執業律師。若您正處於人身安全的立即危險，請撥打 110；保護服務與諮詢專線為 113。