すぐそばの目
近距離の監視

CLOSE-RANGE SURVEILLANCE – DETECTION AND RESPONSE

すぐそばの目

近距離監視の検出と対応

Odysec 技術白書 WP-001 ｜ **バージョン** 1.0 ｜ **発行日** 2026-08-30 **領域**：サイバー × フィジカル（Cyber × Physical）

> 本書は中国語原本の参考訳です。中国語版を正式版とします。

目次

本白書について

近距離監視は、技術的にまったく異なる四つの経路で成立しえます。そして監視される側は、自分が遭遇しているのがどの類型なのかを事前に知ることはできません。分かるのは「相手が必ず知っている」ということだけです。**四つの経路は同じ一枚の表の上で比較されなければなりません。そうしてはじめて読者は、いま行った陰性の点検が何を除外したのかを知ることができます。** 本白書はその表を軸に据え、さらに同種の指針に欠けがちな一章を補います：**点検の対象である端末そのものが信頼できないとき、ネットワーク側からは何が見えるのか**。

本白書の性質は二つの部分に分かれ、それぞれが支持しうる推論の強さは異なります：

- **第 2 章から第 5 章、および第 7 章から第 8 章**は**総合分析と方法論**です：既発表の学術的測定、標準文書、プラットフォームの公開資料を整理し、その上に自ら実行できる検出手順を構築しています。
- **支持できること**：監視がどの経路で成立しうるか、現行の保護に原理レベルでどのような構造的欠落があるか、各層の点検がどの経路をカバーするか、そして陰性結果が何を意味するか。
- **支持できないこと**：「あるプラットフォームや製品が現在どう反応するか」という現時点の事実。他者の測定を引用する箇所にはすべて、測定者・対象・時点を明記しています——**それはその研究がその時点で観察した内容であり、現状の保証ではありません**。
- **第 6 章**は**当チーム自身による実測**です：再現可能な統制環境において、「暗号化された通信のもとで、周期的な送信がどれだけ検出可能か」を測定しました。同章のデータ、実験環境、分析スクリプトは本白書とともに公開し、誰でも追検証できます。

両者を混同してはなりません。第 6 章が測定したのは**行動のパターン**（周期的な送信）であって、実在の監視製品ではありません。第 2 章から第 5 章の欠落分析は原理レベルの推論であり、特定の事業者への評価ではありません。

要旨

近距離の監視——パートナー、元パートナー、家族、知人による継続的な把握——の技術的敷居は、すでに消費者水準まで下がりました。加害者に技術力は一切必要ありません。必要なのは一度の物理的接触の機会か、すでに知っている一組のパスワードだけです。

本白書の四つの主要な知見：

1. **一度の陰性の点検が排除できるのは、四つの経路のうち多くとも一つだけです。** 監視は四つの経路で成立しえます：物理的トラッカー、アカウント層、端末層、設定層。四者の検出すべき場所は**まったく異なり**、うち三つは端末のスキャンでは常に陰性です。きれいなスキャン結果が与える安心は、多くの場合、確認する場所を誤ったことの産物です。
2. **現行の保護の失敗は、実装の品質の問題ではなく前提の問題です。** 自動警告は「監視される側が対応端末を所持している」ことを、スキャンエンジンは「悪意あるソフトウェアと正当なソフトウェアは挙動で区別できる」ことを、セキュリティ通知は「受け手が守られるべき本人である」ことを前提としま

す。親密な関係における監視という最大の悪用場面では、この三つの前提が同時に崩れます——加害者は同居し、請求を共有し、しばしばその端末を購入した本人だからです。

3. **検出という行為そのものに危険が伴うため、順序を入れ替えてはなりません。** 端末がすでに監視されているならば、その端末上で行う一回一回の確認と支援の求めが、加害者の目の前にそのまま現れうるのです。方法論はスキャンからではなく、「クリーンな端末に移る」ことから始めなければなりません。同様に、監視を発見して直ちに除去することは、気づいたと相手に宣言することに等しく——そしてそれは危険度が最も高い瞬間です。
4. **端末が信頼できないとき、ネットワーク側はなお独立した観測点です——ただしその限界は測定できます。** 当チームは統制環境において、九つの送信周期とジッターの組み合わせについて、それぞれ 30 の観測ウィンドウを取得しました（第 6 章）。**結論の形は、時系列判定はジッターに打ち負かされ、方向判定は打ち負かされない、というものです——ただし本実験における方向判定の誤検出ゼロは背景通信の設計の産物であり、それが実際のネットワークで使えることを支持するには足りません。** 具体的な数値とその限界は同章をご覧ください。

推奨される行動：監視されている疑いがある場合、その疑わしい端末で支援情報を検索しないでください。他者の端末または公共の端末をご利用ください。監視の兆候を見つけても、直ちに除去したり廃棄したりしないでください——まず身体的なリスクを評価し、そのうえで証拠保全を完了してください。

---

1. 問題の所在

1.1 一つの脅威、四つの経路

監視される側が感じ取るのは単一の現象です：**相手が必ず知っている**。どこへ行ったか、誰と会ったか、何を話したか、いつ家を出たかを。

しかしこの現象の背後には、技術的にまったく異なる四つの経路があります：

経路	加害者に必要なもの	漏れるもの
A　物理的トラッカー	持ち物や車両に機器を入れる一度の機会	位置
B　アカウント層	クラウドアカウントのパスワードの知識	位置、写真、バックアップ、連絡先。プラットフォームによってはメッセージも
C　端末層	ロックが解除された端末に一度触れる機会	ほぼすべて——メッセージの内容、通話、画面を含む
D　設定層と周辺機器	「設定してあげる」と一度引き受ける機会	設定次第。かつ**端末を買い替えても通常は無効**

この四つの経路は同一の脅威モデル（第 2 章）を共有しますが、検出すべき場所は四つとも異なります。**本白書が四つの経路をまとめて扱うのは、まさにこのためです**：一つだけを点検すると、読者はその時点で

「もう調べた」という結論に至りやすく、実際には他の経路にまったく手が触れていないということが起こります。

1.2 台湾における具体的状況

「ストーキング・ハラスメント防止法」は 2022 年に施行され、規制される行為態様には、電子的通信・インターネットその他の設備により特定の人を継続的に監視し、追跡し、または所在を把握する行為が含まれます。また「刑法」の電脳使用妨害罪の章および秘密妨害罪の章は、正当な理由なく他人のコンピュータ設備に侵入する行為、正当な理由なく他人の非公開の活動を録取する行為について罰則を定めています。

法的手段は存在します。欠けているのはその反対側です：**法律はどの行為が違法かを定めていますが、その違法行為が起きていることに気づく方法は誰も教えてくれません。**被害者が直面する実務上の問いは次のようなものです：

- 監視されている疑いがあるが、どのように証明すればよいのか。
- スマートフォンに警告が出ず、アンチウイルスのスキャンにも異常がない。それは安全という意味なのか。
- 不審な機器やソフトウェアを見つけた。そのまま除去すればよいのか。

三つめの問いに対する直観的な答えは誤りであり、しかもその誤りは身体の安全を危うくしうるものです（7.1 節参照）。

1.3 本白書が答える問い

1. 監視はどのように成立するのか（統合脅威モデルと四つの技術的経路）
2. 現行の保護がこの場面でなぜ機能しないのか（実装の瑕疵ではなく構造的な欠落）
3. どのように自己検出するのか（階層的方法論、各層のカバー範囲、そして陰性結果の意味）
4. 端末が信頼できないとき、なお何を観測しうるのか（ネットワーク側の測定と当チームの実測結果）
5. 発見後どう対応するのか（身体的安全、証拠保全、法的手段、解除の順序）

---

2. 統合脅威モデル

2.1 加害者の類型

類型	動機	特徴
親密な関係の加害者	支配、行動と人間関係の監視	**最多**：長期にわたる物理的接触の機会があり、ロック解除コードを知っているか入手できることが多い
別離・離婚の当事者	材料の収集、支配の継続	関係の存続中に確立されたアクセスが、別離後も有効なまま残ることが多い
家庭内の監視	気遣いの名を借りた支配	保護者向け監視ツールを成人または成人に近い家族に対して使用
職場における逸脱	管理の名を借りた越境	会社端末やモバイル端末管理の権限が業務範囲外に用いられる
窃盗の事前偵察	住人の生活パターンの把握	標的は人ではなく物。トラッカーは主に車両に設置

本白書が主に対象とするのは前の二つの類型です。**アクセスの機会が最も多く**、かつ**身体的な帰結が最も重大**だからです。

2.2 能力の前提：技術力はゼロ

本脅威モデルで最も強調すべき点：**加害者の技術的能力はゼロと仮定します。**

プログラミングも、ジェイルブレイクや改造も、Bluetooth プロトコルや OS の理解も不要です。必要なのは以下の**いずれか一つ**だけです：

- 相手の持ち物や車両にトラッカーを忍ばせる一度の機会；
- ロックが解除された端末に一度触れる機会、またはロック解除コードの知識；
- クラウドアカウントのパスワード、またはそのパスワード再設定手続きを通過できること；
- 「端末を設定してあげる」という名目で一度端末を預かった経験。

親密な関係において、これらはいずれも日常の一部です。**パートナーのロック解除コードを知っていることは、多くの関係で信頼の表れとみなされます。脅威モデルはこの社会的現実を認めなければならず**、コードが秘匿されていると仮定すべきではありません。

敷居がこれほど低いからこそ、この種の脅威は技術力を要する攻撃よりはるかに広く存在します。防御の思考は「高度な敵」を想定してはなりません——正しい想定は、「技術は何も分からないが、接触の機会は十分にある敵」です。

2.3 被害者の置かれた状況

- **無自覚期間が長い**：警告や自覚に至るまで、監視は数週間から数か月続いている可能性があります。

- **知識の非対称**：加害者は何を仕掛け、何を設定したかを知っていますが、被害者は何を探せばよいかすら分かりません。
- **確認の経路自体が監視下にあること**：最も自然な反応は「手元の端末で対応方法を検索する」ことですが、その端末こそが監視されている端末かもしれません。
- **同意と強制を区別できないこと**：支配的な関係においては、「自発的に」パスワードを渡すことも、「自発的に」位置情報アプリを入れることも、圧力の下で起こりえます。技術的機構が見るのは一度の正当な権限付与であり、その背後にある強制は見えません。
- **複数の地点が同時に失われうること**：加害者が端末・クラウドアカウント・メール・車両サービスを同時に掌握している場合があります。単一の地点だけを片付けても、他の地点から直ちに気づかれ、元に戻されうるのです。

2.4 全編を貫く一つの原則

以上の状況は一つの原則へ収斂し、それが本白書のすべての手順の順序を決めます：

> **点検の対象である端末を、信頼できる道具と仮定してはなりません。** トラッカーの場合、スマートフォンは通常なお道具として使えます。しかし残る三つの経路では、その端末自体が調査の対象です。対象の端末上で行った点検は、陰性であれ陽性であれ信用できず、しかも点検という行為そのものが見られている可能性があります。

---

3. 監視の四経路

3.1 経路 A：物理的トラッカー

安価な Bluetooth トラッカーは本来、遺失物発見のために設計されました。しかしその三つの特性——極めて低い価格、年単位のバッテリー、自前の通信を必要としないグローバルなクラウドソース・ネットワークへの依存——は、同時に理想的なストーキングの道具にもなります。

トラッカー自身は自分がどこにいるかを知りません。GPS も携帯回線もなく、行うことはただ一つ、Bluetooth Low Energy で識別信号を発信し続けることです。位置の特定は他人の端末の上で起こります：

1. トラッカーが識別信号を発信する；
2. 同じエコシステムに属する通りすがりのスマートフォンがそれを受信する；
3. その端末が自身の GPS で「自分はここにいて、この識別信号を聞いた」と判断する；
4. この情報が暗号化されてベンダーのサーバーへ送られる；
5. トラッカーの所有者が照会し、復号された位置を得る。

中継した通行人の端末は、自分が何を中継したかを知り得ません。位置情報はエンドツーエンドで暗号化され、所有者だけが読めます。一般利用者のプライバシーにとって、これは良い設計です。

ローテーション識別子の両義性：トラッカーが長期的に追跡可能な固定標識となることを防ぐため、各エコシステムの機器は発信する識別子を定期的にローテーションします。これは一般利用者を守ります——第三

者が固定の識別子を観察し続けてあなたの行動を記録することはできません。しかし**現に追跡されている人**にとって、同じ設計が困難を生みます：識別子が変わるため「この識別子がずっとついてくる」という判定ができず、汎用の Bluetooth スキャナーに映るのは絶えず変化する匿名機器の列であり、環境中の大量の Bluetooth 機器と区別しにくいのです。

これは古典的なプライバシー設計のトレードオフです：多数を追跡から守る仕組みが、現に追跡されている少数の自救をより難しくします。この点を理解して初めて、自己検出が汎用スキャンアプリだけに頼れない理由が分かります。

ネットワーク密度はエコシステム間で大きく異なり、**密度が測位精度と更新頻度を直接決定します**。機器が密集する都市部では、追跡のリアルタイム性は機器の少ない地域よりはるかに高くなります。

3.2 経路 B：アカウント層（端末には何もインストールしない）

クラウドアカウントのパスワードさえ知っていれば、加害者は自分の端末からサインインし、そのアカウントが同期するすべてを取得できます。位置情報、写真、バックアップの内容、連絡先、予定、そしてプラットフォームによってはメッセージも含まれます。

この経路には、加害者にとって極めて有利な三つの性質があります：

- **端末のスキャンは常に陰性**：端末上に余分なソフトウェアが存在しません；
- **持続すること**：パスワードが変わらず、サインインのセッションが破棄されない限り、アクセスは継続します；
- **出所に気づきにくいこと**：アカウントのサインイン済み端末一覧を定期的に確認する人はほとんどいません。

さらに、プラットフォーム標準の**位置情報共有**や**ファミリー共有**は、関係の存続中に有効化され、関係の悪化後も解除されないままであれば、忘れられた監視経路として機能します。

3.3 経路 C：端末層（一度の物理的接触を要する）

すなわち端末上に監視ソフトウェアをインストールする方法です。二つのプラットフォームで様相が異なります：

- **Android**：ストア以外の提供元からのインストールが可能です。インストール後、監視ソフトウェアは典型的に**ユーザー補助サービス**や**デバイス管理者**などの高権限を要求します。これらは本来、補助機能や企業管理のために設計された機構ですが、画面内容の読み取り・通知の傍受・削除の防止に逆用されます。インストール後はアイコンを隠すか、システム構成要素を装うことが一般的です。
- **iOS**：脱獄していない端末に持続的な監視ソフトウェアをサイドロードすることは困難であり、そのため iOS における監視は経路 B または D を通ることが多くなります。脱獄した端末の露出度は Android と同等ですが、脱獄自体が識別可能な痕跡を残すのが通常です。非公式ストアの画面が現れる、システム更新が繰り返し失敗する、同一機種の他端末と挙動が明らかに異なる、といった形です。

端末層のソフトウェアは、法的にも検出上も状況が大きく異なる二種類に分かれます：

種別	入手方法	検出上の位置づけ
デュアルユース・アプリ	公式ストアに保護者向け監視・盗難対策・従業員管理として合法的に公開	**主流**：ソフトウェア自体が合法であり、スキャンエンジンに検知する正当な根拠がない
専用監視スイート	サイドロード。パートナーの監視を明示的または暗示的に目的とする	セキュリティ製品に検知されやすいが、インストール後は自ら隠蔽する

本白書は、監視製品の名称・入手先・インストール方法を意図的に一切記載しません。この種の情報は被害者よりも加害者に大きく資するからです。被害者に必要なのは「自分の端末でどう異常を見つけるか」であって、「市場にどの製品があるか」ではありません。この判断は、当チーム『研究倫理綱領』における攻撃的詳細の取扱い原則に従うものです。

3.4 経路 D：設定層と周辺機器

第三の経路は、パスワードの漏洩でもソフトウェアのインストールでもなく、**端末が本来備える正当な設定機構の利用**です。個々の設定はいずれも合理的な機能であるため、最も見落とされやすい経路です：

- **構成プロファイルと仕事用プロファイル**：本来は企業の端末管理のために設計された機構ですが、いったんインストールされると通信の誘導・アプリの配信・一部の利用記録にまで及びます。「端末を設定してあげる」という名目でのインストールは、関係の中では不自然に映りません。
- **メッセージと通話の転送設定**：メールの自動転送、通信事業者側の通話転送、SMS の別端末への同期。これらは一度設定されると、**端末を買い替えても有効なまま残ります。**
- **ペアリング済みの周辺機器**：時計、車載システム、イヤホン、タブレット。ペアリング関係は関係の悪化後も残ることが多く、とりわけ車載システムは位置情報の履歴と連絡先を同時に保持するため注意を要します。
- **パソコンとブラウザの同期**：端末のメッセージが共用パソコンに同期される、ブラウザのアカウントがブックマークやパスワードを同期する。いずれも端末を経由しない迂回路となりえます。
- **標準搭載の共有機能**：位置情報共有、ファミリーグループ、共有アルバム。これらは双方の同意が継続することを前提に設計されていますが、**関係が変化したときに再確認を促す仕組みは存在しません。**

3.5 四経路の全景比較

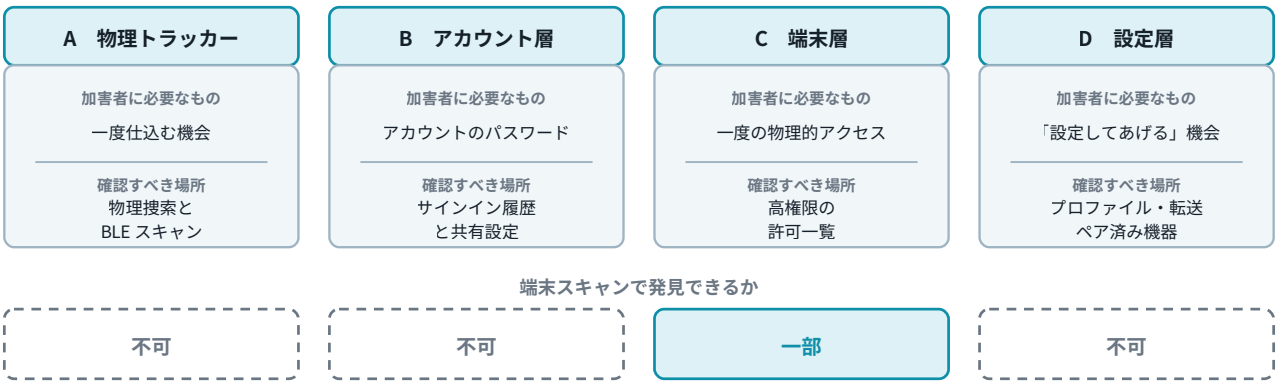

図 1：監視の四経路と、それぞれの検出位置。四つのうち三つは、端末スキャンでは原理的に見えません。

この表は、本白書で最も記憶されるべき一頁です。四者の決定的な違いは技術的な複雑さではなく、**どこを確認すべきか**にあります：

	A　物理的トラッカー	B　アカウント層	C　端末層	D　設定層
物理的接触の要否	必要（一度）	不要	必要（一度）	多くの場合必要
端末スキャンで発見できるか	**不可**	**不可**	一部可能	**不可**
システムが自ら警告するか	一部（エコシステム次第）	一部（サインイン通知）	まれ	**なし**
検出すべき場所	物理的捜索とBluetooth スキャン	アカウントのサインイン記録と共有設定	端末の高権限の一覧	端末設定と外部サービスの規則
漏れる範囲	位置	位置、バックアップ、写真、連絡先	ほぼすべて	設定次第
解除の方法	機器を取り出す（先に証拠保全）	セッションを破棄し認証情報を変更	ソフトウェアを削除し高権限を取り消し	設定を一つずつ確認し削除
端末の買い替えは有効か	無効（トラッカーは物品の側にある）	**無効**（アカウントを放置すれば一緒に移行）	有効	**無効**（規則の多くは端末の外にある）

最後の行は実務上最も多い誤解です：**新しい端末に買い替えても、四つの経路のうち三つは解除されません。**端末だけを替えてアカウントを放置すれば、新しい端末はサインインした瞬間に再び露出します。

上から二番目の行は、「スキャンした」を結論にできない理由を説明しています：**四つの経路のうち三つは、端末スキャンでは原理的に見えません。**

---

4. 現行の保護の構造的欠落

結論を先に：**現行の機構は「典型的状況の典型的利用者」には有効ですが、近距離監視の加害者は典型的状況ではありません。**

4.1 現行の機構は三つの線に沿って発展してきた

1. **不明なトラッカーの自動警告**：自分の所有ではなく、かつ長時間同行しているトラッカーを検出したときに通知します。クロスプラットフォームの検出標準（DULT）が主要ベンダーの共同により IETF で推進されています。多くのトラッカーは、所有者から一定時間離れると自ら音を発します。
2. **ソフトウェアの提供元の管理と権限の可視化**：公式ストアの審査、ストア外からのインストールに対する制限、高リスク権限の明示的な許可制、および権限の使用履歴を振り返る画面。

3. **アカウントの活動通知**：新しい端末からのサインイン時の通知、およびサインイン済み端末の一覧の提供。

この三つは「見知らぬ他人がマルウェアを仕込む」という脅威モデルに対しては有効です。問題は、本白書の脅威モデルが見知らぬ他人ではないことにあります。

> **具体的数値の扱い方について**：警告の発動条件、遅延、カバー範囲は、OS バージョン・地域・ベンダー方針により変動します。本白書の方針は数値を省くことではなく、**公開測定に裏づけられた数値のみを引用し、測定者・対象・時点を必ず併記する**ことです。理由はこうです——数値を省くと読者はリスクの桁を見積もれなくなります。「遅延がある」と「遅延は八時間」では安全計画上の意味がまったく違います。一方、時点を欠いた数値は現状として読まれてしまいます。どちらも有害であり、時点を明記した数値のほうが害は小さいと判断しました。**現在の挙動が必要なら、唯一信頼できる情報源はご自身の端末です。**

4.2 五つの構造的欠落

以下の五つは実装の瑕疵ではなく、機構の前提と悪用の場面との落差です。パラメータの調整では解決できません。

欠落一：前提が、最も保護を必要とする人々を締め出している

自動警告の成立には三つの前提が同時に満たされる必要があります：監視される側が**スマートフォンを所持**し、**Bluetooth が有効**で、**OS バージョンが機能に対応**していること。前提から外れる人々は実質的に保護を受けません：フィーチャーフォンを使う高齢者、スマートフォンを持たない子ども、省電力やプライバシーの習慣で Bluetooth を切る人、旧バージョンのままの利用者。

これらの集団は、ストーキング被害の高リスク層と相当程度重なります。

同種の問題は端末層でも別の形で現れます。端末を加害者が購入し、設定し、あるいは「処理してくれた」ものであれば、その信頼の連鎖は当初から不完全です。「この端末は自分の手に渡る前に何をされたのか」を事後に確認できる仕組みは、現在存在しません。

欠落二：検出のカバー範囲を攻撃者が選べる

クロスプラットフォーム標準の存在は完全なカバーを意味しません。DULT は IETF にワーキンググループが設置され、脅威モデルとアクセサリ・プロトコルの草案が出ていますが、標準文書が述べるのはあるべき姿であり、実際の検出能力は各ベンダーが各プラットフォームで何を実装し配信したかに依存します。

攻撃者の視点では、これは技術知識をまったく必要としない回避策を意味します：**被害者のスマートフォンと異なるエコシステムのトラッカーを選ぶ**こと。この欠落に対する学術側の応答のひとつが、エコシステム横断の第三者検出ツールです（Heinrich らが 2022 年に発表した AirGuard がその例で、iOS の追跡保護ロジックをリバースエンジニアリングし、Android 利用者が Apple エコシステムのトラッカーを検出できるようにしました）。**この種のツールの存在自体が欠落の証拠です**——純正のカバーで足りているなら、必要にならないからです。

さらに根本的な層があります。検出は機器が標準の定める挙動に従うことに依存しており、**従うかどうかは機器の側が決める**という点です。市場にはスピーカーを除去した改造品が流通し、いかなる標準にも参加しない自作機器も存在します。Shafqat らは 2023 年、位置を報告し続けながら被害者側の警告を回避するクローン・トラッカーを実証しました。**防護機構の有効性が攻撃者の協力の上に成り立っているのであれば、それは脅威モデルとして成立しません。**

欠落三：正当な権限付与と強制された権限付与は、技術的に区別できない

保護者向け監視アプリの機能一覧は、監視アプリのそれとほぼ完全に一致します。違いはソフトウェアが何をするかではなく、**端末の所持者が知っており、かつ自発的であるか**にあります。これはコードの外側にある事実であり、スキャンエンジンが原理的に判断しえないものです。事業者が一律に検知すれば正当な利用を巻き添えにし、一律に検知しなければストーキングの場面における主力の道具を素通しにすることになります。

これは周縁的な事例ではありません。Chatterjee らが 2018 年に行ったこの生態系への初の体系的測定は、**親密な関係における監視に利用しうるアプリのうち、大多数が正当な用途を持つデュアルユース・アプリであり、あからさまなスパイウェアではない**ことを示しました。Roundy らは 2020 年、対人攻撃に用いられるソフトウェアが監視の一類型にとどまらないことをさらに明らかにしています。つまりスキャンエンジンが直面しているのは、分類の難しい少数の例外ではなく、この問題の主要な形態そのものです。

システムが見るのは一度の正当な権限付与です。画面が表示され、利用者が同意を押しました。システムに見えないのは、同意を押したその時に、もう一人がすぐ横に立っていたことです。**支配的な関係において「自発的」は、技術層が検証しえない概念です。**

同じ困難がトラッカーの側では「同行判定のジレンマ」として現れます。判定が緩ければ大量の誤報が生じ（家族との同乗、公共交通での長時間の同行）、利用者はすぐに警告を無視することを学びます。判定が厳しければ見逃しが生じ、**とりわけ被害者と加害者が同じ空間を共有する場面で顕著です――そして親密な関係における暴力は、まさにこの形態が通常なのです。双方が同居し、あるいは車を共有しているとき、「異常な同行」という信号自体が識別力を失います。**

欠落四：警告の受け手が加害者でありうる

端末の電話番号・請求・ファミリーグループを加害者が掌握している場合、セキュリティ通知もサインイン警告も課金明細も加害者の手に届きます。さらに根本的には、端末そのものを加害者が購入し設定した場合があります。**その時点で、「利用者に通知する」ことを設計の前提とするあらゆる保護は、守る対象が反転します。**

欠落五：保護の設計が「発見すれば除去すべき」を前提としている

現行の安全に関する案内は、ほぼ例外なく不審なソフトウェアや機器の即時除去を勧めます。見知らぬ他人という脅威モデルの下ではそれが正解ですが、近距離監視の場面では、突然途絶えたデータ送信は「相手が気づいた」と加害者に宣言することに等しく、報復を直接引き起こしかねません。

検出と除去の間には、現行の機構がまったく提供していない中間の段階が必要です。すなわち安全性の評価と証拠保全です。本白書の第 7 章がその段階にあたります。

4.3 欠落と経路の対応

欠落	A トラッカー	B アカウント層	C 端末層	D 設定層
一　前提が人々を締め出す	●	○	●	○
二　カバー範囲を攻撃者が選ぶ	●	○	●	●
三　権限付与の文脈が不可視	●	●	●	●
四　警告の受け手が反転する	●	●	●	●
五　発見すれば除去すべきという前提	●	●	●	●

●＝直接該当　○＝部分的に該当

欠落三・四・五は四つの経路すべてにまたがります。その根源が技術ではなく、**脅威モデルが誤った攻撃者を想定していること**にあるからです。

---

5. 階層的な検出の方法論

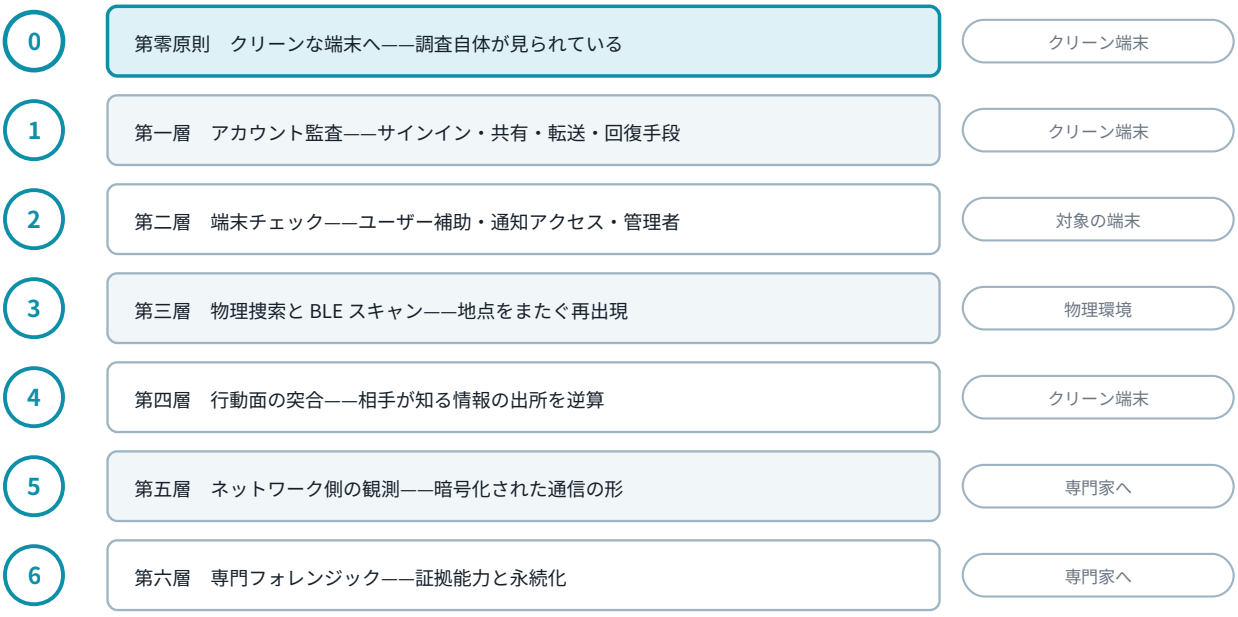

図 2：六層の検出手法。第零原則は準備ではなく、他のすべての層が信頼できるかどうかの前提です。

第零原則：まずクリーンな端末を確保する

これが唯一省略できない段階です。

監視が存在するならば、対象の端末上で行う一回一回の検索、助けを求める一通一通のメッセージ、一本一本の通話が、加害者の目の前にそのまま現れている可能性があります――**あなたが本白書を読んでいるという事実を含めてです。**

したがって：

- 他者の端末、公共のパソコン、または既存のアカウントと一切結びつかない端末を用いてください；
- そのクリーンな端末上で、既存のアカウントに**サインインしないでください**（サインイン自体が通知を発生させ、かえって露見しうるためです）；
- 疑いを招かないために元の端末での日常的な利用を続ける必要がある場合は、その利用の様態を従来どおりに保ってください。

判定原理：何をもって発見とし、何をそうしないか

判定基準がなければ、点検は「見てみる」だけになり、終わっても確認も除外もできません。

層	陽性判定（該当すれば第 7 章へ）	カバーする経路	実施場所
一　アカウント監査	一覧の中に**由来を説明できない項目**——端末・共有相手・転送ルール・権限付与——が一つでもある	B、および D のサービス側部分	クリーンな端末
二　端末点検	高権限の一覧に見覚えのない項目がある	C、および D の端末側部分	対象の端末（危険度は最高）
三　物理的捜索と Bluetooth スキャン	自分のものではない電子機器を発見する；または**同一の対象が三か所以上の異なる場所で、時間を空けて再出現する**	A	物理的な環境
四　行動面の突き合わせ	相手が把握している情報の出所が特定の経路に絞り込めた	四経路すべて。ただし指し示すだけで確定はできない	クリーンな端末
五　ネットワーク側の観測	ネットワークの境界で、上りが下りを明らかに上回る継続的な接続を観測した（周期性は傍証にはなるが、単独では信頼できない——第 6 章参照）	B、C、および D の一部	専門的な支援が必要
六　専門的フォレンジック	鑑識担当者が判定	すべて	専門的な支援

第一層と第二層の判定基準は同じ一文です：**「由来を説明できない」ことが陽性**であり、「怪しく見える」ことではありません。この区別は重要です——監視ソフトウェアはシステム構成要素を装い、共有関係はもっともらしい名称で表示されます。判定基準が「怪しく見える」であれば、うまく偽装できた項目は読者自身の手で除外されてしまいます。**その項目がいつ、誰によって、何のために作られたかを言えるかどうかが、信頼できる判定基準です。**

第三層の判定基準はとくに説明を要します。**一度のスキャンで未知の Bluetooth 機器が見えること自体には何の意味もありません**——都市環境では常時数十の機器が発信しています。意味を持つ信号は**同一の対象が場所をまたいで繰り返し現れること**です。それによってはじめて「他人の機器がたまたま近くにあっただけ」を排除できます。識別子のローテーションが汎用スキャンツールを弱めるのも、まさにこの点です（3.1 節参照）。

第四層の判定は性質が異なります。**範囲を狭めること**はできますが、確定はできません。その価値は、技術的な点検がすべて陰性であったときに、なお前進しうる唯一の方法であることが多い点にあります。

陰性結果の三つの由来

これは本方法論で最も重要な一節です。点検を終えて何も見つからなかったとき、理由は三つ考えられ、**それぞれ次の行動への含意がまったく異なります**：

1. **真の陰性**：実際に監視が存在しない。
2. **見る場所が違う**：監視は存在するが、点検した層にはない。**本主題においてこれは例外ではなく主要な場合です**——四つの経路のうち三つは端末スキャンの下では常に陰性です（3.5 節参照）。きれいなスキャン結果は、アカウント層と設定層の監視を少しも排除しません。
3. **点検自体が機能していない**：点検が実際には実行されていない。Bluetooth が切られていてスキャンが動いていなかった、位置情報の権限が未付与で警告機構が一度も有効になっていなかった、クリーンな端末で行うべき監査を対象の端末で行った、アプリ一覧だけを見て高権限の付与一覧を見ていなかった、など。

三つめが最も危険です。**外見上は真の陰性とまったく同じ**——どちらも「何も見つからなかった」だからです。したがって、いかなる陰性結果を信用する前にも、まず点検そのものが動作可能な状態にあることを確認してください。付録 A の準備のリストはそのためのものです。**これは準備作業ではなく、陰性結果を信用してよいかどうかの前提条件です。**

> この原則は当チームの測定経験から得たものです。WP-003 の研究では、計器がすでに壊れているにもかかわらず出力が真の陰性とまったく見分けがつかない状況に三度遭遇しました。気づかなければ「漏洩なし」が結論になっていたはずです。第 6 章の測定はそのため、陽性対照を各実行の前提条件としています。**結果を見る前に、道具が測定可能な状態にあることを検証する**——この原則は自助検出にも同じく当てはまります。

第一層：アカウント監査（クリーンな端末で実施、危険度は最低）

アカウント層は最も一般的でありながら、最も見落とされやすい層です。以下を一つずつ確認してください：

- **サインイン済みの端末一覧**：見覚えのない端末や場所はありませんか。名称は妥当に見えても実際にはご自身のものではない項目にご注意ください。
- **位置情報共有とファミリーグループ**：現在、誰があなたの位置を見られる状態にありますか。その共有はいつ有効化されたものですか。
- **メールの自動転送とフィルタ規則**：ご自身が作成した覚えのない転送規則はありませんか。これは最も多く、かつ最も持続する迂回路の一つです。
- **アカウントの回復手段**：回復用のメールアドレスと電話番号は、いまだ相手のものではありませんか。**回復手段を整理しないままでは、パスワードを変更してもその効果が数分で取り消されうるのです。**
- **二要素認証の設定**：第二の要素は、相手が入手できる端末や番号に結びついていませんか。
- **アプリ用パスワードと認可済みの第三者アプリ**：認可した覚えのない項目はありませんか。

- **バックアップの設定**：バックアップ先のアカウントは、確かにご自身のものですか。

第二層：端末チェック（対象の端末で操作、危険度は最高）

本層を実施する前に 7.1 節をお読みください。本層のあらゆる操作は監視ソフトウェアに記録されうるものです。

端末層の監視は動作を継続するために、ごく限られた種類の高権限を取得しなければなりません。したがって確認の要点は「不審なアイコンを探す」ことではなく、**これらの権限一覧を一つずつ確認し、すべての項目に見覚えがあることを確かめる**ことにあります：

- **ユーザー補助サービスの許可一覧**：画面内容の読み取りと操作の模倣を可能にする鍵となる権限であり、正当な用途のソフトウェアは極めて少数です。
- **通知へのアクセスの許可一覧**：この権限を得れば、メッセージのプレビューを含むすべてのアプリの通知内容を読み取れます。
- **デバイス管理者またはデバイスオーナーの権限**：この権限を持つソフトウェアは通常の方法では削除できません。
- **構成プロファイルと仕事用プロファイル**：勤務したことのない企業名や、見覚えのない組織名はいずれも異常です。
- **非公式の提供元からのインストール許可**：どのアプリが他のアプリのインストールを許可されていますか。
- **電池とモバイルデータの使用量ランキング**：背景で継続的にデータを送信するソフトウェアは、アイコンを隠していてもこの二つの一覧に痕跡を残します。
- **ペアリング済みの Bluetooth 機器と保存済みの無線ネットワーク**：ご自身のものでない項目はありませんか。

上記のいずれかの一覧に見覚えのない項目を見つけた場合は、**その完全な名称を記録したうえで操作を中止し**、第 7 章へお進みください。

第三層：物理的捜索と Bluetooth スキャン（経路 A に対応）

能動的スキャン（十分程度）：各エコシステムの公式アプリの手動スキャン機能、またはオープンソースのツールによる汎用の Bluetooth Low Energy スキャンを用います。スキャンは**自分の他の機器から離れて**行い、移動しながら異なる場所で最低三回繰り返してください——本当についてくる機器は、異なる場所で繰り返し現れます。

物理的捜索（一〜数時間、道具不要）：スキャンで見つからなくても疑いが残る場合、物理的捜索がしばしば最も有効です。**直感で手当たり次第に探すのではなく、決まった順序で進めてください。**

- **車両**（最も一般的な設置場所）——外部：前後バンパーの内側、ホイールアーチ、車体下部フレーム、ナンバープレート枠の裏、牽引フック付近；内部：座席の下と隙間、スペアタイヤ収納部、トランク側面ポケット、グローブボックスの奥、天井内張りの縁。磁石が付く金属面をすべて確認してください——磁気ケースはよく使われる付属品です。
- **携行品**：バッグの仕切りと底面パッドの下、コートの裏地や不自然な縫い目、財布の仕切り、スーツケースの内張りとキャスター部、そして常に持ち歩く物のうち重さや厚みが不自然なもの。

- **住居と贈り物**：相手から贈られたぬいぐるみ、置物、電子アクセサリー；子どものランドセルと玩具（親権係争中は特に確認を）。この領域では録音・録画機器が関わる可能性もあり、取り扱いが異なります。専門家への相談を推奨します。

捜索時の安全上の注意：捜索する姿を加害者に見られる可能性がある場合（同居など）、捜索自体がリスクを高め得ます。その場合はまず専門支援者とタイミングを相談してください。

第四層：行動面の突合（クリーンな端末で実施、最も過小評価されやすい）

技術的な確認が陰性であるとき、本層が唯一前進しうる方法となることが少なくありません。方法は、「相手が知っている事柄」を一つずつ列挙し、**その情報の出所として何がありうるか**を逆算することです：

- 相手が知っているのは**位置**ですか、それとも**会話の内容**ですか。前者は経路 A または B からでありえ、後者は経路 C または通知へのアクセスを示唆します。
- 相手が知っているのは**送信済みのメッセージ**ですか、それとも**未送信の下書き**ですか。後者の出所の範囲は極めて限られます。
- 相手が把握している情報は**即時**ですか、**数時間の遅れ**を伴いますか。後者は定期的な同期やバックアップの様態に符合します。
- 相手は**特定の一台の端末にのみ現れた**事柄を知っていますか。これにより範囲を当該端末へ直接絞り込めます。

個々の出来事の日付、相手が知っていた具体的な内容、そのときのご自身の所在を書面で記録してください。この記録は 7.2 節の証拠の基礎ともなります。

第五層：ネットワーク側の観測（専門的な支援が必要）

前の四層はいずれも対象の端末またはそのアカウントの内側で行われます。これらの点検がすべて陰性であり、しかも 2.4 節の原則が対象の端末そのものは信頼できないと告げているとき、**まだ汚染されていない唯一の観測位置はネットワークの境界です**。

監視ソフトウェアはデータを外へ送り出さなければならず、送り出された通信はどこかのルーターを通過します。内容は暗号化されていても、**通信の形は暗号化されません**：いつ送るか、どれだけ送るか、どこへ送るか、上りと下りの比率——これらはすべて見えます。

これらの手がかりの重みは等しくありません。当チームの実測は、**識別力を担うのは「上りが下りを明らかに上回ること」であって「送信が規則的であること」ではない**ことを示しました——後者はゼロコストのジッターで回避でき、しかも良性のハートビート通信までまとめて誤検出するからです。第 6 章がその測定であり、適用の境界も併せて示します。

この層には機材と専門的な判読が必要であり、自助の範囲には属しません。

第六層：専門フォレンジック（自力での対応を中止すべき時点）

次のいずれかに該当する場合は、自力での確認を中止し、専門的な支援を求めてください：

- 機器を見つけたが、種類や録音録画機能の有無が判別できない；
- 端末上に高権限を持つ不明なソフトウェアをすでに発見しており、かつ身体的安全に差し迫った危険が及ぶ；

- 監視が技術的能力を有する加害者によるものと疑われる、または業務用端末と企業管理権限が関わる；
- 事件が司法手続に進む可能性があり、証拠能力のある鑑識報告が必要である；
- 複数回にわたり解除したにもかかわらず監視状態が繰り返し復活する——これは通常、未発見の永続化経路が残っていることを意味します。

自力での操作と鑑識のための取得は両立が困難です。いかなる解除作業も現場を破壊するからです。**法的手段があなたにとって重要であるならば、保全は除去に優先します。**

---

6. ネットワーク側の観測：暗号化された通信の中の周期的な送信

6.1 なぜ端末の外に観測点が必要なのか

第 5 章の第一層から第四層には共通の弱点があります。いずれも対象の端末またはそのアカウントの内側で行われ、そこはまさにすでに掌握されているかもしれない場所だからです。第五層は観測の位置を端末の外へ移します。

その立脚点は一つの構造的事実です：**監視に価値があるためには、データは端末から出ていかなければなりません。**暗号化は内容を守れますが、「何かが定期的に送り出されている」ことそのものを隠すことはできません。したがって問いはこうなります——通信のメタデータしか見えない位置から、周期的な送信はどれだけ容易に見分けられるのか。

この問いには実務上の意味があります。あるサービスが成立するかどうかを決めるからです。判定基準が理想的な条件でしか有効でないのなら、ネットワーク側で監視を検出できると称することは安心を売っているにすぎません。そこで当チームはその限界を実測しました。

6.2 実験環境

測定は **BCN-349** で行いました。EVE-NG で構築した四ノードの統制環境であり、アドレスはすべて RFC 5737 の文書用範囲を用いています。トポロジ、構築スクリプト、生の記録、分析プログラムはすべて本白書とともに公開します（付録 D 参照）。

ノード	役割
PHONE	監視される側。周期的な送信と、背景となる通常のアプリ通信を同時に生成
GW	**観測点**（家庭用ルーターの役割）。全期間にわたり通信を取得
C2	監視のサーバー側。TLS でアップロードを受け、短い ack を返す
WEB	良性のサーバー側。背景通信の相手

測定の対象は「周期的な送信」という行動のパターンであり、実在の監視製品ではありません。本実験は監視ソフトウェアの検体を一切扱わず、いかなる製品の評価も行いません。

6.3 判定基準と測定方法

判定基準はすべて GW 上で見える通信のメタデータのみから計算し、**内容は一切復号しません**：

判定基準	定義	直観
T　時系列判定	隣接する上り事象の間隔の変動係数が `CV < 0.15`	人の操作は不規則だが、プログラムの送信は規則的
A　方向判定	`上りバイト数 ÷ 下りバイト数 > 3`	通常の利用はダウンロードが主体、外部への持ち出しはアップロードが主体
T∧A　併用判定	両者が同時に成立	—

変数：三種類の送信周期（2／5／15 秒）× 三種類のジッター比率（0%／20%／50%）、計九つの構成。ジッターは、実際の間隔が周期に対してプラスマイナス当該比率の範囲内で一様乱数となることと定義します。九つの構成は同一の観測ウィンドウの中で並行して動作させ、分離のためそれぞれ異なる宛先ポートを用いました。背景の良性通信も同時に動作させ、偽陽性の分母としました。**構成ごとに 30 の観測ウィンドウを取得します**。30 に満たないセルについては統計量を報告せず、生の観察のみを報告します。

> 二つの閾値（`CV < 0.15` と比 > 3）は事前に選定した固定値です。閾値の選び方は結論を左右します。その代償は 6.5 節をご覧ください——**方向判定の閾値は、本実験では試されていません**。

計器の検証：各実行の前に、取得がすべての対象の通信を確かに捉えていること、および監視される側に観測点を迂回する経路がないことを確認します。あわせて「ジッターなし」の構成を陽性対照とします——同構成が時系列判定に安定して該当しない場合、それは取得または分析が失敗していることを意味するため、その実行は陰性として記録するのではなく無効とします。これは第 5 章〈陰性結果の三つの由来〉の三つめに直接対応します。

6.4 結果

30 の観測ウィンドウは**すべて計器の検証を通過しました**：各実行の前後に、測定対象の九つのフローが揃っていること（30/30）、ジッターなしの構成（陽性対照）が時系列判定に確かに該当すること（30/30）、および監視サーバー側へ到達した 315 の接続がすべて観測点の対外アドレス由来であり、迂回したものが一つもないこと（315/315）を確認しました。無効なウィンドウは 0 個であり、以下の統計はいずれも 30 のウィンドウに基づきます。

検出（各セル 30 ウィンドウ）

周期	ジッター	ウィンドウあたり事象数	CV 中央値（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% のセルにおける単発の該当は、第 25 ウィンドウで発生しました。その回に観測された事象は 17 個のみで、CV は 0.1455、ちょうど閾値を下回るところでした。**それは CV 推定の標本変動であって、「周期が長いほど検出されやすい」ということではありません**——同じ機構は、一度の見かけ上の取りこぼしも同様に生みうるからです。この点は散らばりに最もよく現れています：事象数が最も少ない 15 秒／50% の組の CV は 0.1455–0.3652 にわたるのに対し、事象数が最も多い 2 秒／50% の組は 0.2692–0.3200 にとどまります。**標本数が左右するのは推定の安定度であって、判定基準の中心傾向ではありません**——三つの周期の CV 中央値はほぼ同じ（0.290／0.289／0.293）です。CV が無次元量だからです。n＝1 であり、ここでは生の観察のみを報告し、いかなる比率も主張しません。

誤検出（30 のウィンドウで合計 577 の良性フロー。ウィンドウあたり中央値 19、範囲 15–23）

良性フローの種別	フロー数	T 誤検出	A 誤検出	T∧A 誤検出
ページ読み込みフロー	487	16（3.3%）	0	0
同期フロー	30	2（6.7%）	0	0
keepalive フロー	60	**60（100%）**	0	0
合計	577	78（13.5%）	**0**	**0**

各ウィンドウで誤検出された良性フローの数は、T の中央値が 2（範囲 2–4）、A と T∧A はいずれも 0 でした。

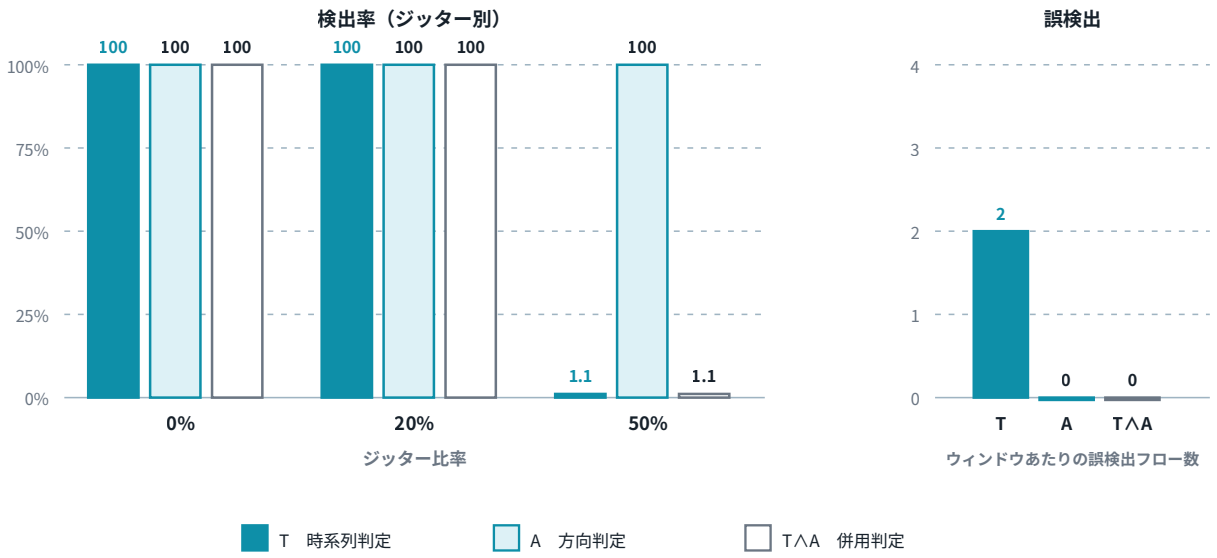

図 3：BCN-349 実測。左：検出率。各バーは三つの送信周期をまとめた 90 の観測ウィンドウです（3×3 の完全な結果は 6.4 節の表）——ジッターが臨界値を超えると時系列判定は失効し、方向判定は影響を受けません。右：ウィンドウごとに誤検出された良性フロー数の中央値（各ウィンドウの良性フローは約 19 本）——時系列判定は良性の keepalive を安定して誤検出します。単独で使えない理由がこれです。

三つの発見

1. **本環境において方向判定は完全に信頼でき、時系列判定はそうではありません。** A は 270 回の観測（九つの構成 × 30 ウィンドウ）ですべて該当し、かつ 577 の良性フローに対して誤検出はゼロでした。一方 T は、ジッターが 50% のときほぼすべてを取りこぼしました。
2. **時系列判定が失効する点は事前に計算でき、したがってゼロコストで回避できます。** 一様なジッターの下では、間隔の変動係数は `CV = j / √3` となり、周期の長短によりません。判定の閾値 0.15 はしたがって、ジッターの臨界値 `j* ≈ 26%` に対応します。実測と理論の一致は千分の三以内です：ジッター 20% では実測中央値 0.1158 に対し理論値 0.1155、ジッター 50% では 0.2904 に対し 0.2887。**時系列判定を逃れるのに技巧は要りません——ジッターを四分の一以上に設定するだけであり、その実装コストはゼロです。**
3. **時系列判定は良性の周期的な通信を安定して誤検出します。** 二つの keepalive フローは、30 のウィンドウすべてで T により陽性と判定されました。60/60、100% です。これは時折の誤検出ではなく必然です。keepalive の定義そのものが、小さなパケットを規則的に送り出すことだからです。外部への持ち出しとの違いは時系列にはなく、方向にあります。

ここから収斂する論点

本環境において、**併用判定 T∧A は方向判定 A の単独使用に優りません**：A はすでに誤検出ゼロであり、T を加えれば、高いジッターのときに本来捕捉できる対象を取りこぼすだけです。時系列判定の価値は「相手が、時系列を見られていると知らない」場合に限られます——そしてそれこそ、第 4 章の欠落二が指摘した、前提としてはならない仮定です：**防護機構の有効性を攻撃者の協力の上に置くことはできません。**

6.5 このデータが支持すること、しないこと

支持すること：

- 通信のメタデータしか見えない位置から、周期性と上りの非対称性という特徴を持つ接続を、本実験が構築した背景の通信と区別できること。
- 二つの判定基準のジッターに対する感度が著しく異なり、かつ時系列判定の失効点が理論の予測と一致すること（発見 2 参照）。したがってその失効点は、本実験が試していないジッター比率へも外挿できます。
- **時系列判定は単独では成立しないこと**：ゼロコストで回避でき、しかもよくある良性の周期的な通信を安定して誤検出するためです。

支持しないこと：

- **「方向判定は実際のネットワークでも誤検出ゼロである」ことは支持しません。**これは本章で最も重要な限界です。すべての良性フローの上り下り比の最大値は 1.44、すべての測定対象の送信フローの最小値は 9.85——両者の間には、数倍の幅を持つ空白帯があります。**これは、閾値を 3 に置いたことが何ら試されていないことを意味します**：本実験は「閾値の選び方が良かった」のか「背景の通信が易しすぎた」のかを区別できません。理由は**背景の通信に、上りが主体の良性通信が含まれていない**ことです——クラウドバックアップ、写真の同期、外部への映像通話、ファイルのアップロードこそ、A を最も試す種類の通信です。A の誤検出ゼロは、この背景モデルの産物であって、A の性質ではありません。A が実際のネットワークで使えると主張するには、バックアップと同期の通信を含む環境で改めて測定しなければなりません。**本白書はその主張をしません。**
- **「ネットワーク側の検出が端末の点検を代替しうる」ことは支持しません。**ネットワーク側からは監視の内容は見えず、どのソフトウェアかを指し示すこともできません。示せるのは「外部への持ち出しの特徴を持つ接続が一つある」ことだけです。
- 実在の監視製品の送信挙動に関するいかなる推論も**支持しません**。本実験の測定対象は統制された送信の挙動であり、実在の製品の周期・ジッター・送信方式は測定していません。
- 本章の結果を暗号化通信以外の判読へ外挿すること、また本実験が扱っていないネットワーク条件へ外挿することも**支持しません**。

測定上の代理についての説明：本実験は 2／5／15 秒を周期の代理として用いていますが、実在の監視ソフトウェアの送信周期は分単位から時間単位であることが多いものです。それでもこの代理に意味があるのは、時系列判定の挙動が**ジッターと周期の比**および**観測された標本数**によって決まり、周期の絶対的な長さによらないからです——発見 2 の理論的な関係は周期に依存せず、三つの周期の実測結果も実際に一致しました。ただしこの代理から「実際の場面で十分な事象数が積み上がるまで、どれだけ観測すればよいか」を推論することは**できません**。それは絶対的な周期に依存するため、別途測定する必要があります。

---

7. 監視発見後の対応

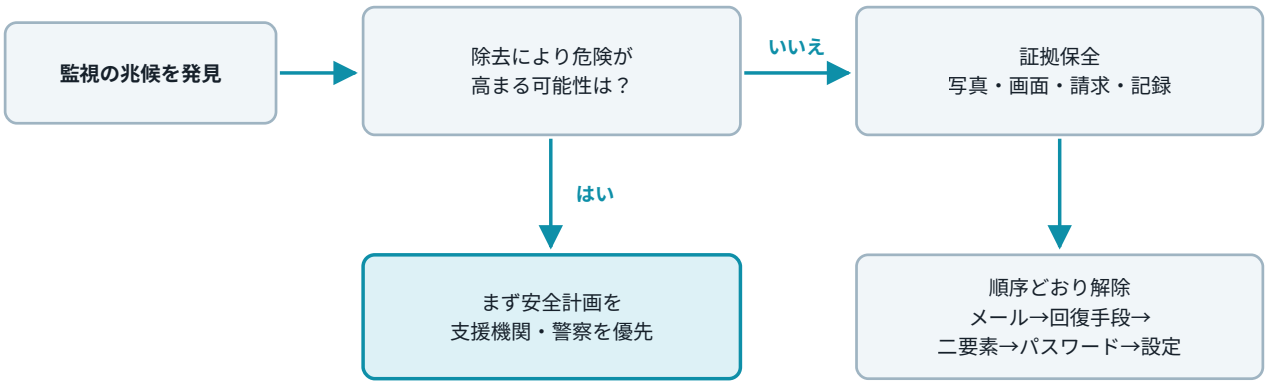

図 4：監視発見後の対応フロー。除去は決して最初の一歩ではありません。

多くの技術ガイドは検出で終わります。しかし監視される側にとって、**何かを見つけた瞬間こそが本当の難題の始まり**です。

7.1 第一の優先事項：身体的安全

監視の除去は、相手が直ちに気づく行為です。トラッカーは、いったん取り外されるか遮蔽されれば、位置の報告が止まるか、その場で凍結します。ソフトウェアが削除され、アカウントからサインアウトされれば、データの送信はただちに途絶えます。これらはいずれも加害者にとって、被害者が気づき行動を始めたという明確な信号です。

親密な関係における暴力の研究において、**被害者が抵抗し、あるいは離れる準備を始める段階こそ、危険度が最も高い段階**とされています。

したがって、対応の前に次を確認してください：

- 実行可能な安全計画はありますか（安全な行き先、連絡できる人、必要な身分証明書と金銭）。
- 除去の後、相手が直ちに現れたり連絡してきたりした場合、どのように対応しますか。
- 専門の社会福祉士や警察の窓口はすでに関与していますか。

答えが否である場合、合理的な選択は現状を当面維持し、まず支援を確立してから技術面に対処することです。監視は耐えがたいものですが、技術的な解除は身体的安全を保障しません。順序を逆にしてはなりません。

差し迫った危険がある場合は 110 番へ、保護サービスと相談が必要な場合は 113 番へご連絡ください（いずれも台湾）。

7.2 証拠保全

除去の前に以下の記録を完了してください。すべての記録は**対象の端末以外**に保存してください：

物理的トラッカーの場合：

1. **まず元の位置で撮影する**：全景と接写を含め、機器が隠されていた位置関係が分かる写真を残す；

2. 発見の日時と正確な位置（車のどの部位、バッグのどの仕切り）を記録する；
3. 外観、シリアル番号、見える識別子を記録する。スマートフォンで読み取れる情報があれば画面キャプチャも；
4. **初期化しない、分解しない、電池を抜かない**——初期化は所有者アカウントとの紐付けを消します。それこそが加害者を指し示す鍵となる接続です；
5. 機能を壊さず一時的に遮断する必要があれば、不透明な容器や包装に入れる。

スマートフォンやアカウント上の監視の場合：

1. 不審なソフトウェアや設定の画面キャプチャ（完全な名称と権限の状態を含むもの）；
2. アカウントのサインイン記録の画面キャプチャ（端末名・日時・場所を含むもの）；
3. **サブスクリプションと請求の記録**——商用の監視サービスは有料であり、金銭の流れは最も有力な証拠の一つです；
4. 第四層で作成した行動面の対照記録（日付、相手が知っていた内容、実際のご自身の所在）；
5. 可能であれば、別の端末で**ご自身が対象端末を操作する過程を撮影**してもらい、画面キャプチャが事後に作成されたものでないことを裏づけてください。

共通の原則：証拠保全が完了するまで、削除せず、初期化せず、端末を買い替えないでください。

> **最も多い誤り**：発見のショックや怒りから、その場で機器を捨てたりソフトウェアを削除したりすること。行為を特定の人物に結びつける唯一の物証が消え、その後の立証は極めて困難になります。**初期化は最も徹底した除去であると同時に、最も徹底した証拠の消去です。**

7.3 台湾における法的手段

- **「ストーキング・ハラスメント防止法」**：規制される行為態様には、電子的通信・インターネットその他の設備により特定の人を継続的に監視し、追跡し、または所在を把握する行為が含まれます。被害者は警察機関へ申告でき、調査を経て加害者に書面による戒告が発せられ、その後二年以内の再犯については保護令の申立てが可能となります。
- **「刑法」電脳使用妨害罪の章**：正当な理由なく他人のコンピュータまたはその関連設備に侵入する行為、正当な理由なく他人の電磁的記録を取得または変更する行為、およびこれらの罪を犯すための専用のプログラムを作成する行為について、いずれも罰則が定められています。
- **「刑法」秘密妨害罪の章**：正当な理由なく録音・撮影・録画または電磁的記録により他人の非公開の活動・言論・談話または身体のプライバシーに属する部位を録取する行為について、罰則が定められています。
- **「個人資料保護法」**：個人データを不法に収集・処理・利用し、他人に損害を生じさせるに足りる場合、相応の責任が定められています。
- **「家庭暴力防治法」**：双方が家族構成員または親密な関係のパートナーに当たる場合、保護令の申立てが可能であり、その内容には被害者への嫌がらせや追跡の禁止が含まれます。

申告の際は**婦幼警察隊**へ赴くか、ストーキングおよび家庭内暴力に関わる旨を明確に伝え、この種の案件に習熟した部署が担当するようにすることをお勧めします。7.2 節で保全した証拠を持参し、元の機器は保持

してください。**個別事案の法的評価は弁護士の判断に委ねるべきであり**、本白書は法的意見を構成しません。

状況	窓口
身の危険が差し迫っている	110
家庭内暴力・性暴力・児童保護	113 保護ホットライン
ストーキング事件の申告	各地警察の婦幼警察隊
法律相談	各地弁護士会、法律扶助基金会

7.4 クリーンな環境を再構築する順序

順序の誤りは、解除が失敗する最も多い原因です。**アカウントの回復手段が相手の掌握下にあるまま、パスワードだけを変更した場合、新しいパスワードは数分のうちに再設定されうるのです。**

1. **クリーンな端末で、まずメールアカウントに対処する**：他のすべてのアカウントの回復の出口であり、最初に取り戻さなければなりません。
2. **回復手段を整理する**：ご自身のものでない回復用メールアドレスと電話番号を削除します。
3. **二要素認証を再設定する**：ご本人のみが所持する端末に結びつけ直し、バックアップコードを再生成します。
4. **パスワードを変更し、すべてのセッションを破棄する**：セッションの破棄が鍵となる操作です。パスワードの変更のみでは、既存のサインイン状態が一部のサービスで有効なまま残りうるためです。
5. **他のアカウントを順に処理する**：クラウド、ソーシャル、金融、通信事業者。
6. **設定層を整理する**：転送規則、通話転送、位置情報共有、ファミリーグループ、ペアリング済み機器、構成プロファイル。
7. **最後に対象の端末そのものに対処する**：証拠保全の完了後、端末を工場出荷時の設定に戻し、そのうえで**古いバックアップから復元しないでください**——古いバックアップには監視のための設定が含まれている可能性があります。手作業で設定し直してください。
8. **その他すべての端末を確認する**：タブレット、パソコン、車載システム、スマートホーム機器。

完了後、数週間のうちに第一層のアカウント監査を再度実施してください。**監視状態の再発は通常、一覧のうち未発見の経路が一つ残っていることを意味します。**

---

8. ベンダーと政策立案者への提言

トラッカーおよびモバイルプラットフォームの事業者へ：

1. **検出能力をエコシステムの境界で止めない**：加害者の機器選択にエコシステムの制約はまったくありません。クロスプラットフォーム検出のカバー範囲は速やかに完全化されるべきです。

2. **「空間共有」での見逃しに正面から向き合う**：「異常な同行」を核とする現行の判定ロジックは、最大の悪用場面において最も識別力を欠きます。必要なのはより敏感なパラメータではなく、異なる判定の発想かもしれません。
3. **スマートフォンを持たない人への経路を用意する**：例えば低コストの独立型検出器や、第三者（ソーシャルワーカー、警察部署）が代行できる検査ツール。
4. **アカウント層を単一のセーフティチェック入口に統合する**：現状では、一度の完全な監査のために利用者が複数の設定画面を横断しなければなりません。単一の入口がサインイン済み端末・位置情報共有・転送規則・回復手段・第三者への認可を網羅し、一括で取り消せるべきです。
5. **共有関係に有効期限と定期的な再確認を設ける**：位置情報共有とファミリーグループが、何の見直しの促しもないまま永続的に有効であるべきではありません。
6. **デュアルユース・アプリの常時開示**：位置情報や内容を継続的に送信しうるソフトウェアは、ストア上の分類を問わず、監視される端末上に解除不能な常時のインジケータを維持すべきです。**監督の正当な用途は、監督される側が知っていることによって損なわれません。**
7. **「発見後」の導線を設計し直す**：警告や安全に関する案内が一律に即時の除去を勧めるべきではありません。「これは親密な関係における監視である可能性がある」という分岐を設け、証拠保全と支援資源へ導くべきです。
8. **通知の受け手を独立して設定可能とする**：セキュリティ通知が請求先の名義人やファミリーグループの管理者にのみ届くべきではありません。
9. **端末の引き渡し状態を検証可能とする**：工場出荷時または前回の初期化以降、どの構成プロファイルと高権限ソフトウェアがインストールされたかを利用者が確認できる仕組みを提供すべきです。

政策立案者と実務機関へ：

1. **技術的検出能力を保護サービス体系に組み込む**：現状、被害者は技術の敷居を独力で越えなければなりません。婦幼警察隊と家庭内暴力防止センターのレベルに、基本的な検査能力と紹介の仕組みを設けるべきです。
2. **証拠保全の指針を公開し入手しやすくする**：7.2 節の内容は、受理するすべての警察官がその場で被害者に伝えられる標準的説明であるべきです。
3. **第一線の受理担当者にはデジタル監視に関する基礎的な素養が必要です。**また被害者の証拠収集を支援する窓口も、デジタル証拠の取扱いを含むべきです。

---

9. 研究の限界と今後の課題

9.1 外的妥当性の境界

第 2 章から第 5 章の結論の性質は「機構の原理レベルにこれらの欠落が存在する」であって、「あるプラットフォームや製品が現在どう振る舞うか」ではありません。

- 本白書はいかなるトラッカー製品も、いかなる端末の検出機能も、いかなるプラットフォームの保護も**テストしていません**。特定の製品やプラットフォームの評価・比較として引用**してはなりません**。

- 引用した他者の測定結果が当てはまる範囲は、その研究が述べる対象・バージョン・時点に限られます。事業者の挙動は変化しますし、実際に変化することが分かっています。
- 第 3 章の経路の分類と第 4 章の欠落分析は、公開文書が記述する機構の上に立っています。ある事業者の実装が自社の文書の記述と異なる場合、その部分の推論はその事業者には当てはまりません。
- **第 5 章の方法論は有効性の検証を受けていません**：各層の点検の検出率も偽陰性率もまだ測定しておらず、7.4 節の解除順序が実際に監視を途絶させるかも未検証です。機構の原理から設計した合理的な手順ではありますが、有効だと分かっている手順ではありません。
- 第 6 章の限界は 6.5 節をご覧ください。その結論を、同章の実験が扱っていない条件へ外挿してはなりません。
- 本白書は特定の製品名を挙げず、監視ソフトウェアの入手方法やインストール方法も記載していません。これは意図的な判断です（3.3 節参照）。その代償として読者はその部分の記述を自ら追検証できませんが、加害者にとっての有用性を下げることと引き換えに、受け入れうる代償だと当チームは判断しました。
- 法に関する記述は台湾の現行法を範囲とし、法的意見を構成するものではありません。

9.2 事前登録された実験設計（v2.0）

以下の設計は実測の開始前に公開します。結果を見る前に設計そのものを外部が検証できるようにするためです。**設計をデータより先に公開すれば、事後に判定基準を結果へ合わせることはできません。**

共通設定

- **対象**：三大エコシステムのトラッカー各一つと、二大プラットフォームのテスト端末各一台。監視の経路は当チームが所有するテスト端末上にそれぞれ構築します。すべての端末は各実行の前に工場出荷時の設定へ戻します。
- **対照群の設計**：一つのシナリオで構築する経路は一つだけです——二つを同時に構築すれば、検出できてもどちらに帰属するか分かりません。あわせて、監視されていない同型の端末を対照とします。
- **反復回数**：トラッカーのシナリオは組み合わせごと・シナリオごとに 20 回。経路 B から D は組み合わせごとに 10 回。回数に満たないセルについては統計量を報告せず、生の観察のみを報告します。
- **計器の検証**：各実行の前に、存在が既知の監視を用いて、その層の点検が実際にそれを見つけられることを確認します（陽性対照）。**陽性対照が通らなければその実行を中止し**、統計には算入しません。
- **統計の示し方**：時間に関する数値は平均値ではなく中央値と四分位範囲で報告します（分布が右に歪み、平均値は外れ値に引かれるため）。
- **公開範囲**：生の記録と分析スクリプトはすべて v2.0 とともに、本白書の付録 D と同じ形式で公開します。**監視のサンプル自体は外部に配布しません。**

実験マトリクス

番号	シナリオ	検証する変数	主な測定項目
E1	エコシステム横断の検出マトリクス	トラッカーのエコシステム × 端末基盤	警告が出たか否か；初回警告までの遅延
E2	警告遅延の分布	時間帯（日中／夜間）	分離から警告までの時間分布
E3	空間の共有	所有者側が被害者側と同所に留まるか	警告が発動するか；同条件下での E2 との差
E4	層ごとの検出率	監視の経路 × 点検の層	その層がその経路を発見できるか；偽陰性率
E5	解除の完全性	解除の順序（7.4 節に従う／任意の順序）	解除後に監視が確かに途絶するか；数週間後に再発するか
E6	端末の交換は有効か	アカウントを同時に処理するか否か	新端末のサインイン後に監視が復活するか

各シナリオで変えるのは一つだけです。

事前に宣言する反証条件

次のいずれかが生じた場合、対応する主張は反証されたものとみなし、v2.0 にその結果を明記します：

- E1 ですべてのエコシステム × 基盤の組み合わせが近い時間内に警告を発動する → **欠落二**は成立しない。
- E3 の警告の発動状況が E2 と有意に変わらない → **欠落三**のうち空間共有に関する推論は成立しない。
- E4 で端末層の点検が経路 B または D の監視を安定して発見する → 3.5 節の比較表の修正が必要。
- E5 で任意の順序と 7.4 節の順序で解除の成果に差がない → 同節の「順序が重要である」との主張は成立しない。
- E6 で端末の交換だけで監視が解除される → 3.5 節末尾の主張は誤り。

倫理的・法的前提：当チーム『研究倫理綱領』4.1 節に基づき、すべての実験の被験者は研究者本人、または書面によるインフォームド・コンセントを得た志願者に限ります。同意のない者へのテストは行わず、実在の被害者の端末やデータも使用しません。トラッカーは全期間を通じて研究者自身の所持品に取り付けます。

9.3 お寄せいただきたいご意見

- 実務家（ソーシャルワーカー、警察官、弁護士）による第 7 章の流れの実行可能性についての意見；
- 第 4 章の欠落分析への補足または反証；
- 各層の点検に、本白書が扱っていない永続化経路はあるか；
- 第零原則は、二台目の端末を持たない被害者にとって過度に厳しいものではないか；
- 台湾国内の事例の傾向（**当事者を特定できる情報は含めないでください**）。

ご意見は `contact@odysec.org` へ。機微な内容は PGP で暗号化のうえ `security@odysec.org` へお送りください。

付録 A：検出チェックリスト

> 単独で印刷して使用できます。

始める前に - ☐ 判断：対応が加害者の危険な行動を招く可能性はないか。あるなら先に 113 か警察へ - ☐ 自身のアカウントと無関係のクリーンな端末を確保した - ☐ そのクリーンな端末で既存のアカウントにサインインしていない - ☐ 対象の端末で支援情報を検索していない

準備：点検そのものが有効であることの確認

> この項目は準備作業ではなく、**陰性結果を信用してよいかどうかの前提条件**です。いずれかが未達なら、「何も見つからなかった」は点検の機構が一度も有効になっていなかったことを意味するだけです（第 5 章〈陰性結果の三つの由来〉参照）。

- ☐ Bluetooth が有効
- ☐ 位置情報の権限を付与済み
- ☐ OS が最新
- ☐ 追跡警告の通知が無効化されていない
- ☐ 他エコシステムの検出アプリを導入済み

第一層：アカウント監査（クリーンな端末） - ☐ サインイン済み端末の一覧を一つずつ確認した - ☐ 位置情報共有とファミリーグループを一つずつ確認した - ☐ メールの自動転送とフィルタ規則を一つずつ確認した - ☐ 回復用メールアドレスと電話番号が本人のものであることを確認した - ☐ 二要素認証が本人の所持する端末に結びついている - ☐ 第三者アプリへの認可を一つずつ確認した - ☐ バックアップ先のアカウントが本人のものである

第二層：端末チェック（対象の端末、危険度は最高） - ☐ ユーザー補助サービスの許可一覧 - ☐ 通知へのアクセスの許可一覧 - ☐ デバイス管理者またはデバイスオーナーの権限 - ☐ 構成プロファイルと仕事用プロファイル - ☐ 他のアプリのインストールを許可された提供元の一覧 - ☐ 電池とモバイルデータの使用量ランキング - ☐ ペアリング済みの Bluetooth 機器と保存済みの無線ネットワーク

第三層：物理的捜索と Bluetooth スキャン - ☐ 自分の他の Bluetooth 機器から離れて公式アプリの手動スキャンを実行した - ☐ **異なる場所**で最低三回繰り返し、繰り返し現れる未知の機器を記録した - ☐ 車外：バンパー内側、ホイールアーチ、車体下部、ナンバープレート枠の裏 - ☐ 車内：座席の下と隙間、スペアタイヤ収納部、トランク側面、グローブボックス、天井内張りの縁 - ☐ バッグ類：仕切り、底面パッドの下 - ☐ 衣類：コートの裏地、不自然な縫い目 - ☐ 財布、スーツケースの内張りとキャスター - ☐ 相手から贈られた物 - ☐ 子どものランドセルと玩具

第四層：行動面の突合（クリーンな端末） - ☐ 相手が知っている具体的な事柄を列挙した - ☐ 位置に関する情報と内容に関する情報を区別した - ☐ 情報が即時か遅延を伴うかを判断した - ☐ 日付・内容・自身の所在を記録した

監視の兆候を見つけた場合 - ☐ **直ちに除去せず、初期化せず、廃棄しない** - ☐ 除去により身体的危険が高まらないかを評価した - ☐ トラッカー：元の位置で撮影した（全景＋接写）。日時・場所・識別子を記録した - ☐ スマートフォンとアカウント：画面キャプチャとサインイン記録を保全した（対象の端末以外に保存） - ☐ サブスクリプションと請求の記録を保存した - ☐ 自身の行動タイムラインを記録した - ☐ 証拠を持参して婦幼警察隊へ申告した - ☐ 解除は「メール→回復手段→二要素認証→パスワードとセッション→他のアカウント→設定層→端末」の順序で行った - ☐ 古いバックアップから復元していない - ☐ 数週間後に第一層の監査を再実施した

付録 B：用語対照

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

付録 C：参考文献

本白書の技術的主張の根拠はすべてここに列挙します。**他者の測定結果を引用する際は、その対象と時点も併せて引用してください。**

学術研究

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 — クラウドソース型位置ネットワークの機構分析。3.1 節の技術的背景の根拠。
2. Heinrich, A., Bittner, N., & Hollick, M. (2022). AirGuard — Protecting Android Users from Stalking Attacks by Apple Find My Devices. ACM WiSec 2022（最優秀論文賞）. https://arxiv.org/abs/2202.11813 — エコシステム横断の検出ツールの設計と実地での利用観察。欠落二の根拠。
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 — 警告遅延の実測（日中に八時間を超える観察を含む）と、警告を回避するクローン・トラッカーの実証。4.1 節および欠落二の根拠。**この測定は特定の製品を対象に 2023 年に実施されたもので、以降の OS バージョンでは挙動が異なる可能性があります。**
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/ — 親密な関係における監視ソフトウェアの生態系への初の体系的測定。デュアルユース・アプリがその主体であることを示す。要旨および欠落三の根拠。
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（最優秀論文賞）. https://dl.acm.org/doi/10.1145/3173574.3174241 — 89 名の参加者による質的研究。第 2 章の「攻撃者の技術能力はゼロ、ただしアクセスの機会は豊富」との仮定の根拠。
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 — 対人攻撃に用いられるソフトウェアが監視の一類型にとどまらないことを示す。欠落三の補足的根拠。
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 — 専門家が被害者の技術的点検を支援する実務モデル。第五層・第六層および第 8 章の政策提言の根拠。
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 — 実際の介入事例の分析。7.1 節「除去は即座に気づかれる」という危険性評価の根拠。

標準文書

1. IETF Detecting Unwanted Location Trackers（DULT）ワーキンググループ。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 章にいう「クロスプラットフォーム検出標準」はこの二つの草案を指します。**草案の状態は変動します。引用時は最新版をご確認ください。**

団体資料

1. Coalition Against Stalkerware。ストーカーウェアの定義、実務指針、参加団体の資料。https://stopstalkerware.org/
2. IPV Tech Research（Cornell Tech などによる共同研究プログラム）。親密な関係における暴力と技術の濫用に関する文献と資源。https://www.ipvtechresearch.org/

ベンダーとプラットフォームの文書

1. 各トラッカーベンダーおよび二大モバイルプラットフォームの公式サポート文書とプライバシーに関する説明。改訂が頻繁で地域設定にも依存するため、本白書は特定バージョンを固定しません。**具体的な挙動は、ご覧になる時点の公式文書とご自身の端末を基準としてください。**

法令

1. 台湾の「ストーキング・ハラスメント防止法」、刑法のコンピュータ使用妨害の罪および秘密侵害の罪の章、「個人資料保護法」、「家庭暴力防治法」。

当チームの報告

1. Odysec（2026）『トンネルの外側：VPN の保護境界の測定手法と実測結果』Odysec 研究報告 WP-003。 — 測定の規律と「結果を見る前に計器を検証する」原則の出所。

付録 D：実験環境とデータ

第 6 章の実験環境 **BCN-349**、構築スクリプト、生の記録、分析プログラムは本白書とともに公開し、研究発表ページからダウンロードできます。

環境は自由に入手できる Debian 13 のみを用い、**合法的に配布できないライセンスのイメージは意図的に一切使用していません。**したがって読者は環境を完全に再構築できます。アドレスは RFC 5737 の文書用範囲を用い、鍵と証明書はラボ専用の固定値です——**それらはすでに公開されており、いかなる場合も実運用に用いてはなりません。**

改訂履歴

バージョン	日付	変更内容
1.0	2026-08-30	初版。

引用形式：Odysec（2026）『すぐそばの目：近距離監視の検出と対応』Odysec 技術白書 WP-001、バージョン 1.0。

免責事項：本白書は技術研究および教育を目的とするものであり、法的意見を構成しません。個別の案件に関する法的評価は弁護士にご相談ください。身体の安全に差し迫った危険がある場合は 110 番へ、保護サービスと相談が必要な場合は 113 番へご連絡ください（いずれも台湾）。