ODYSEC

無音の同伴者
Bluetooth トラッカー悪用

BLUETOOTH TRACKER ABUSE – DETECTION AND RESPONSE

無音の同伴者

Bluetooth トラッカー悪用の検出と対応

Odysec 研究報告 WP-001 ｜ **バージョン** 1.0 ｜ **発行日** 2026-08-22 **研究ライン**：融合領域（Cyber × Physical） **DOI**：10.5281/zenodo.22065463

> 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

本報告の性質について

本報告は**総合分析および方法論の研究**です。技術的記述はすべてベンダーの公開文書、公開の標準草案、既発表の学術研究に基づいており、本バージョンにおいて独自の実測データは主張していません。具体的な挙動（警告の発動までの時間など）に関わる箇所では、OS のバージョンや地域設定によって変動することを明記しています。読者はご自身の端末の現在の挙動を基準としてください。

第 8 章に、計画中の対照実験の設計を記載しています。実測結果は v2.0 として公開予定です。

要旨

安価な Bluetooth トラッカーは遺失物発見のために設計されましたが、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。技術的知識は一切不要で、必要なのは一度の物理的接触の機会だけです。

本報告の三つの主要な発見：

1. **保護機構は「追跡される側がスマートフォンを所持し、Bluetooth を有効にしている」ことを前提に設計されている：**この前提から外れる人々——高齢者、子ども、フィーチャーフォン利用者、習慣的に Bluetooth を切る人——は、現在、実質的にいかなる自動保護も受けていません。これは実装の欠陥ではなく、機構の構造的な境界です。
2. **エコシステム横断の検出が最大の欠落である：**各社の警告は自社ネットワークが中心です。クロスプラットフォーム標準は前進していますが、カバー範囲は各社の実装の進み具合に依存します。加害者は被害者のスマートフォンと異なるエコシステムの機器を選ぶだけで、発見を大幅に遅らせることができます。
3. **技術的検出と法的救済のあいだに断絶がある：**多くの技術ガイドは「トラッカーを見つける」ところで終わります。しかし被害者の本当の困難はその後——証拠の保全、身の安全と証拠のどちらを優先するかの判断、誰に助けを求めるか——にあります。第 6 章はまさにこの区間を扱います。

行動指針：追跡が疑われる場合、まず身の安全を確保してから検出を行うこと。機器を発見したら、すぐに捨てたり初期化したりしないこと——それが唯一の証拠です。

1. 問題の所在

1.1 なぜ今なのか

Bluetooth トラッカーは何年も前から市場に流通しており、技術自体は新しくありません。リスクの様相を変えたのは**クラウドソース型位置ネットワークの規模**です。あるエコシステムの端末が都市環境の至る所に

存在する密度に達したとき、GPS も携帯回線も持たない低コストのタグが、ほぼリアルタイムの位置報告能力を獲得します。

これによりストーキングの敷居は、「技術力と継続的な労力」から「一度の接触の機会と数百円」にまで下がりました。

1.2 台湾の状況

台湾では「ストーカー行為等防止法（跟蹤騷擾防制法）」が 2022 年に施行され、法的手段は存在します。しかし公開資料を検討した結果、**中国語圏には技術面での自己検出の指針がほぼ空白である**と当チームは判断しました。被害者が直面する実務上の問いは次のとおりです。

- 追跡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ていないが、それは安全という意味なのか？
- 不審な機器を発見したが、次に何をすべきか？

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。この落差こそ、技術研究者が埋められる部分です。

1.3 本報告が答える問い

1. 追跡はどのように行われるのか（脅威モデルと技術的原理）
2. 自力での検出方法（層別の方法論と各層の限界）
3. 発見後の対応（証拠保全、身の安全、法的経路）

---

2. 脅威モデル

2.1 攻撃者の類型

類型	動機	特徴
親密な関係にある加害者	支配、行動の監視	**最多：**長期の物理的接触機会を持ち、被害者の生活習慣と持ち物を熟知
別離・離婚係争の当事者	証拠収集、嫌がらせ	関係終了とともに接触機会は減るが残存し得る（共有財産、子の受け渡し）
商業・職場のストーキング	競合情報、従業員監視	接触機会は特定の場に限定
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

本報告は第一の類型に焦点を当てます。**最大の接触機会**と**最も重大な身体的帰結**を併せ持つためです。

2.2 能力の想定

本脅威モデルで最も強調すべき点：**攻撃者の技術力はゼロと想定します。**

プログラミングも、ジェイルブレイクも、Bluetooth プロトコルの理解も不要です。攻撃者に必要なのは：

- 相手の持ち物や車両に機器を忍ばせる一度の機会；
- 自分名義のスマートフォンとアカウント。

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、物理的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、追跡は数週間続いている可能性があります。
- **知識の非対称**：加害者は何をどこに仕掛け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。
- **支援経路の断絶**：警察は具体的な証拠を必要とし、証拠の取得には技術的知識が必要で、技術支援の窓口と保護サービスの体系はうまく接続されていません。
- **被害者の機器自体がすでに掌握されている可能性**：親密な関係の文脈では、被害者のスマートフォン、クラウドアカウント、車両も加害者の支配下にあり得ます。「スマートフォンは安全」という前提に立つ検出手法は、最も必要とされる場面で成立しない恐れがあります。

---

3. 技術的背景：クラウドソース型位置ネットワークの仕組み

3.1 基本的な流れ

トラッカー自身は**自分がどこにいるかを知りません**。GPS も携帯回線もありません。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。

図 1：クラウドソース型位置ネットワークの仕組み

この設計の巧妙さは、**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ない**点にあります。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。

3.2 ローテーション識別子の両義性

トラッカー自体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。

この設計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**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」という単純な判定ができない；
- 汎用の BLE 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；
- 有効な検出には各エコシステムのローテーション規則の理解が必要——これこそ、公式の検出機能が汎用ツールに対して持つ優位です。

これは古典的なプライバシー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。

3.3 三大エコシステム

エコシステム	ネットワークの源	検出支援の概要
Apple Find My	iPhone・iPad など Apple 機器	iOS 内蔵の不要追跡警告；Android 向け検出アプリも提供
Samsung SmartThings Find	Galaxy 系機器	Samsung エコシステム内蔵の検出
Tile	Tile アプリ利用者	アプリ内の手動スキャン機能

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**。Apple 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。

4. 現行の保護機構とその欠落

本報告の中核となる分析です。結論を先に：**現行機構は「典型的状況の典型的利用者」には有効ですが、ストーキングの加害はしばしば典型的状況ではありません。**

4.1 現行機構の基本ロジック

自動警告の判定ロジックは概ね「**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ら通知する」というものです。クロスプラットフォームの検出標準（DULT——Detecting Unwanted Location Trackers）が主要ベンダーの共同で推進されており、異なるエコシステムの機器も検出可能にすることを目指しています。

加えて、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**。これはスマートフォンに依存しない第二の警告層です。

> **バージョン差異への注意**：警告の発動条件、遅延、対象機器の範囲は、OS バージョン・地域・ベンダー方針により変動します。本報告は意図的に具体的な分数を記載しません——その種の数字は公開後すぐに陳腐化し、古い数字に基づく安全判断は数字がないより危険だからです。

4.2 欠落の分析

欠落一：機構の前提が一部の人々を排除している

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：追跡される側が**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。

特筆すべきは、**これらの集団がストーキング被害の高リスク層と相当程度重なる**ことです。

欠落二：エコシステム横断の検出は各社の実装進度に依存する

標準の存在は完全なカバーを意味しません。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、これは極めて単純な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。技術知識は不要で、相手がどの端末を使っているかを知っていれば足ります。

欠落三：非標準・改造機器

スピーカーを除去・無効化した改造品が流通しており、主流標準に参加しない小規模メーカー品や自作タグも存在します。前者は音響警告を無効化し、後者は検出機構の対象から完全に外れる可能性があります。

欠落四：同行判定のジレンマ

警告機構は「このトラッカーが異常に長く同行しているか」を判定しなければなりません。この判定には本質的なジレンマがあります：

- 判定が緩い → 大量の誤報（家族との同乗、公共交通での長時間の同行）が発生し、利用者は警告を無視することを学ぶ；
- 判定が厳しい → 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——親密な関係における暴力はまさにこの形態が通常です。

加害者と被害者が同居し、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：これは原理上の限界であり、パラメータ調整で解決できる問題ではありません。

欠落五：トラッカー以外の代替手段

本報告は市販の Bluetooth トラッカーに焦点を当てますが、ストーキングはアカウント共有の位置情報機能、車両メーカーのコネクテッドサービス、スマートフォンに仕込まれたストーカーウェアを通じても行われ得ます。トラッカー検出が陰性でも被害者の状況が依然として加害者に把握されている場合、調査対象をこれらの経路に広げるべきです。これらは別の報告で扱います。

---

5. 自己検出の方法論

低コスト・低リスクの層から始める四層構成です。**どの層にも検出できないものがあり、陰性の結果は安全を意味しません。**

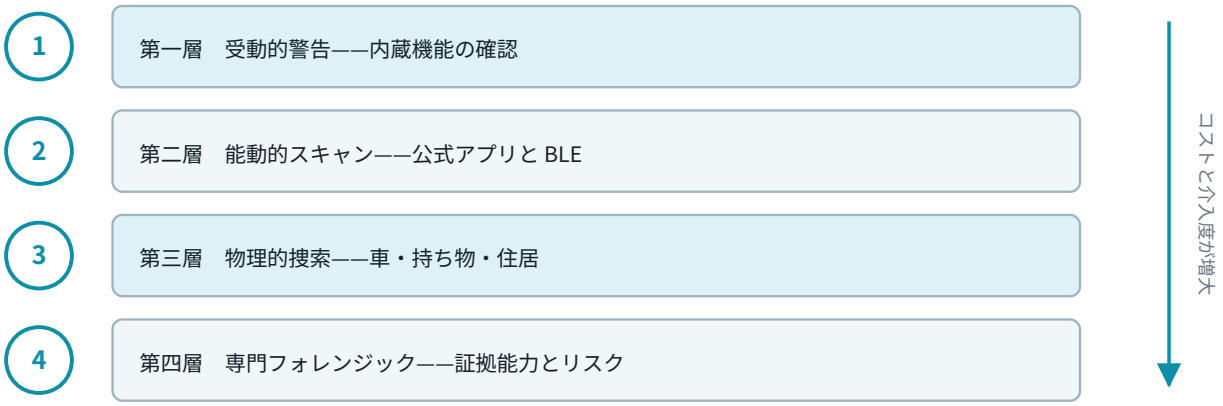

図 2：四層の自己検出手法

第一層：受動的警告（設定のみ）

実施事項：スマートフォンの追跡検出機能が動作可能な状態にあることを確認する。

- Bluetooth と位置情報の権限を有効に（検出には両方が必要）；
- OS を最新に保つ；

- 関連通知が無効化・ミュートされていないことを確認；
- Android 利用者で周囲が Apple 機器中心の環境（またはその逆）なら、他エコシステムの公式検出アプリの導入を検討。

限界：標準に参加する機器しか検出できず、遅延は不可避です。**警告が来ないことは、追跡されていないことを意味しません。**

第二層：能動的スキャン（十分程度）

実施事項：公式アプリの手動スキャン機能、または汎用 BLE スキャンツールを使う。

- 各エコシステムの公式アプリの多くは「周辺の未知のトラッカーを能動的に探す」機能を提供しており、受動的警告を待つより速い；
- 学術界にはオープンソースの検出ツールもあります（例：ドイツ・ダルムシュタット工科大学の研究チームが発表した AirGuard）。検出ロジックが公開されており検証可能です；
- スキャンは**自分の他の機器から離れて**行い、移動しながら繰り返すこと——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。

判読の要点：一度のスキャンで多数の未知の Bluetooth 機器が見えるのは正常です（イヤホン、バンド、車載機、近隣の機器）。意味のある信号は、**同一機器が複数の異なる場所で繰り返し現れる**ことです。

限界：発信を止めた機器や非標準の機器は映りません。汎用ツールは識別子ローテーションのため同一機器の追跡が困難です。

第三層：物理的捜索（一〜数時間、道具不要）

前二層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。**直感ではなく、決まった順序で探すこと。**

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——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、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；- 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：- 相手から贈られた物——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：専門フォレンジック（自力対応を止めるべきとき）

次の場合は自力での対処をやめ、専門家の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；

- スマートフォン自体にストーカーウェアが仕込まれている疑いがある；
- 事件が司法手続きに進む可能性があり、証拠能力のある鑑識報告が必要；
- 身の安全に差し迫った危険がある。

---

6. 発見後の対応

多くの技術ガイドは第 5 章で終わります。しかし被害者にとって、**機器を見つけた瞬間こそが本当の難題の始まり**です。

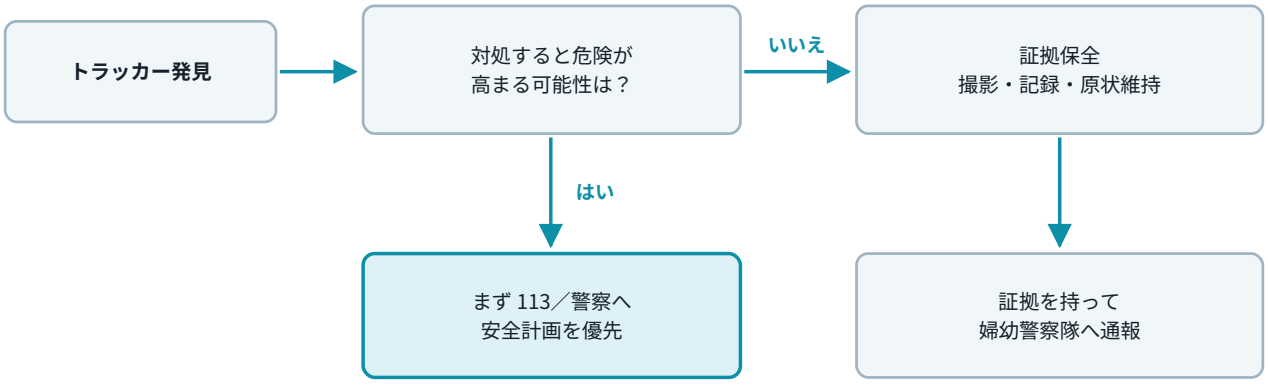

図 3：機器発見後の対応フロー

6.1 最優先：身の安全

機器に手を触れる前に、一つの判断をしてください：**機器が沈黙したことに加害者が気づき、行動をエスカレートさせる可能性はないか？**

トラッカーが除去・遮蔽・停止されると、位置報告は止まるか、その場で凍結します。加害者にとって、それは明確な信号です。

エスカレートの可能性があると判断した場合：

- **機器をすぐに処置しない**；
- まず 113 保護ホットラインまたは警察に連絡し、安全計画を相談する；
- 安全の手配が整ってから、助言に従って対処する。

証拠は重要です。しかし身の安全は証拠に優先します。

6.2 証拠保全

機器への対処が直ちにリスクを高めないと確認できたら、次の順序で進めます：

1. **その場で撮影**：**元の位置**のまま、全景と接写を撮り、隠されていた位置関係が分かる写真を残す；
2. **日時と場所の記録**：発見の日時、正確な位置（車のどの部位、バッグのどの仕切り）；

3. **機器情報の記録**：外観、シリアル番号、見える識別子。スマートフォンで読み取れる情報があればスクリーンショットも；
4. **原状のまま保存**：**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**；
6. **自分の行動タイムラインを記録する**：機器が記録していた可能性のある期間と照合でき、侵害の範囲と期間の立証に役立ちます。

> **最も多い誤り**：発見のショックや怒りからその場で捨てる・壊すこと。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。

6.3 台湾における法的経路

通報：警察に通報します。ストーキングと家庭内暴力を扱う専門部署は各地警察の**婦幼警察隊**です。6.2 節で保全した証拠を持参してください。

ストーカー行為等防止法：反復・継続するストーキング行為を規制し、被害者は警察に調査を求め、裁判所に**保護命令**を申し立てることができます。トラッカーで行動を把握する行為は、同法が規制しようとする行為態様に含まれます。

その他の関連規定：事案によっては、刑法の秘密妨害罪の章（第 315-1 条は道具・設備による非公開活動の覗き見・盗聴・盗撮を規定）、個人資料保護法、機器が車両や住居に設置された場合のその他の規定が関わり得ます。**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**、本報告は法的助言ではありません。

相談窓口（台湾国内）：

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通報	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

6.4 その後のデジタル・クリーンアップ

物理的なトラッカーの発見は終わりではありません。加害者に物理的接触の機会があった以上、併せて確認すべきものがあります：

- スマートフォンと PC に本人が入れていないアプリや構成プロファイルがないか；
- クラウドアカウントの端末一覧、位置情報共有設定、ファミリー共有のメンバー；
- 車両メーカーのコネクテッドサービスのアカウント紐付け；
- パスワードと二要素認証のリセット（端末自体の安全が確認できてから行う）。

順序が重要です：掌握された端末上でパスワードを変えることは、新しいパスワードを相手に直接手渡すことと同じです。クリーンアップは、安全が確認された一台の端末から始めてください。

---

7. ベンダーと政策立案者への提言

ベンダーへ：

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、最大の悪用場面である親密な関係の暴力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. **警告に次のステップを含める：**現在の警告の多くは「未知のトラッカーを検出」で終わります。「初期化しないこと、証拠の残し方、相談先」を併せて示せば、被害者の状況は大きく改善します。

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：**本報告 6.2 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。

---

8. 研究の限界と今後の作業

8.1 本バージョンの限界

- 本報告は**総合分析と方法論の研究**であり、独自の実測データを含みません；
- 各社機構の具体的挙動（発動条件、遅延）はバージョンにより変動するため、本報告は意図的に原理のレベルで記述しています；
- ストーカーウェアと車両コネクテッドサービスの悪用は対象外とし、別途扱います。

8.2 計画中の実測（v2.0）

同業者の検証と再現を可能にするため、実験設計をここに公開します：

実験	目的
三大エコシステム × 二つのスマートフォン基盤の検出マトリクス	エコシステム横断検出の実際の落差を定量化
警告遅延の測定	所有者との分離から被害者側警告までの時間分布
空間共有シナリオ	同居・同乗の状況での見逃し率の検証
Bluetooth オフ・省電力モードのシナリオ	非典型的な利用習慣を持つ人の露出度を定量化
汎用 BLE スキャンツールの判読難度	非公式ツールの一般利用者にとっての実用性評価

倫理的・法的前提：当チームの研究倫理綱領 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いません。

8.3 お寄せいただきたいフィードバック

- 実務家（ソーシャルワーカー、警察官、弁護士）による第 6 章の実行可能性への意見；
- 第 4 章の欠落分析への補足または反証；
- 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：機器への対処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

第一層：受動的保護の確認 - ☐ 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

第二層：能動的スキャン - ☐ 自分の他の Bluetooth 機器から離れる - ☐ 公式アプリの手動スキャンを実行 - ☐ **異なる場所**で最低三回繰り返す - ☐ 繰り返し現れる未知の機器を記録

第三層：物理的捜索 - ☐ 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 - ☐ 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

機器を見つけたら - ☐ まず元の位置で撮影（全景＋接写） - ☐ 日時と正確な位置を記録 - ☐ 外観・シリアル・識別子を記録 - ☐ **初期化しない・分解しない・電池を抜かない** - ☐ 自分の行動タイムラインを記録 - ☐ 証拠を持って婦幼警察隊へ通報 - ☐ スマートフォン、クラウド、車両サービスを確認

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
跟蹤騷擾	stalking	ストーキング
跟蹤軟體	stalkerware	ストーカーウェア
證據保全	evidence preservation	証拠保全

付録 C：資料の出所

本報告は次の種類の公開資料に基づいています：各トラッカーベンダーの公式サポート文書とプライバシー説明、クロスプラットフォーム検出標準（DULT）の公開草案、Bluetooth トラッカーのプライバシーと検出に関する既発表の学術研究（ダルムシュタット工科大学の研究チームの成果とそのオープンソースツール AirGuard を含む）、および台湾のストーカー行為等防止法・刑法・個人資料保護法の条文。

各社機構の具体的な挙動については、各ベンダーの最新の公式文書をご参照ください。

引用形式：Odysec（2026）。『無音の同伴者：Bluetooth トラッカー悪用の検出と対応』。Odysec 研究報告 WP-001、バージョン 1.0。

免責事項：本報告は技術研究と教育を目的とし、法的助言を構成しません。個別事案は弁護士にご相談ください。身の危険が差し迫っている場合は（台湾では）110 へ。