ポケットの中の密告者
ストーカーウェア

STALKERWARE – DETECTION AND RESPONSE

ポケットの中の密告者

スマートフォンのストーカーウェア検出と対応

Odysec 研究報告 WP-002 ｜ **バージョン** 1.0 ｜ **発行日** 2026-08-23 **研究ライン**：融合領域（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プラットフォーム事業者の公開文書、ストーカーウェア対策連合（Coalition Against Stalkerware）などの団体が公開する資料、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（ある保護機能の発動条件など）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。

本報告は WP-001『無音の同伴者』の姉妹編です。前者が物品に取り付けられる物理的トラッカーを扱ったのに対し、本編はスマートフォン自体に寄生する監視を扱います。後者が取得しうる情報は位置情報にとどまりません。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

ストーカーウェアとは、端末の所持者が知らないまま、あるいは同意しないまま、その位置情報・メッセージ・通話その他の私的な情報を継続的に送信するソフトウェアまたはサービスを指します。Bluetooth トラッカーと比べ、その侵害範囲ははるかに広範です。トラッカーが知るのはあなたがどこにいるかだけですが、ストーカーウェアは誰に何を話したかまで知ります。

本報告の三つの主要な知見：

1. **最も一般的な監視経路は、そもそも何もインストールを必要としない可能性があります**：クラウドアカウントのパスワードさえ入手できれば、加害者はバックアップ・同期・端末を探す機能を通じて位置情報・写真・メッセージを継続的に把握できます。この「アカウント層の監視」は端末上にスキャン可能な痕跡を一切残しません。**端末のスキャン結果が陰性であっても、監視されていないことの証明にはなりません。**
2. **アンチウイルス的な発想では権限の濫用を捉えられません**：主要プラットフォームの保護は「悪意あるソフトウェアを阻止する」という考え方に立ちますが、ストーキングの場面における監視の多くは、正規に公開されている保護者向け監視・盗難対策・標準搭載の共有機能を逆用して達成されます。ソフトウェア自体は合法であり、問題はインストールと権限付与を取り巻く強制的な文脈にあります。これはスキャンエンジンが原理的に判断しえない領域です。
3. **確認する行為そのものに危険が伴います**：トラッカーの場合と根本的に異なります。すでに端末が監視されているならば、**その端末上で行うあらゆる確認・検索・支援の求めが、相手に見られている可能性があります**。したがって本報告の方法論は、手元の端末をスキャンさせることからではなく、「第零原則：クリーンな端末に移る」から始まります。

推奨される行動：端末が監視されている疑いがある場合、その端末で支援情報を検索したり支援者に連絡したりしないでください。他者の端末または公共の端末をご利用ください。監視ソフトウェアを発見しても直ちに削除しないでください。まず証拠保全を完了し、削除により加害者が気づいて危険が高まらないかを評価してください。

1. 問題の所在

1.1 なぜ今か

WP-001 の欠落分析では、トラッカーの検出結果が陰性であるにもかかわらず被害者の行動や私的情報が把握され続ける場合、調査範囲をスマートフォン上のストーカーウェアとアカウント層の監視へ広げるべきであると指摘しました。本編はその予告に応えるものです。

ストーカーウェアは新しい存在ではありませんが、二つの変化がリスクの様相を変えました：

- **スマートフォンが個人生活の完全な鏡像となったこと**：位置情報・会話・写真・予定・健康データ・金銭のやり取りが一台に集約されています。端末を掌握することは、その人の生活を一望する視野を掌握することに等しくなりました。
- **監視の入手障壁が消費者水準まで下がったこと**：サブスクリプション型の商用監視サービスであれ、プラットフォーム標準の共有・監督機能であれ、その操作画面は技術的背景を持たない一般の人向けに設計されています。

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」が規制する行為態様には、電子的通信の方法により特定の人の所在や活動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を規制しています。法的手段は存在しますが、WP-001 と同じ落差が再び現れます。**中国語圏には、自己検出から対応までを網羅した指針が存在しません。**被害者が直面する実務上の問いは次のようなものです：

- 相手は私がどこへ行き誰と話したかを常に知っているのに、異常が何も見つかりません。何から着手すべきでしょうか。
- スマートフォンにアンチウイルスを入れてスキャンしても異常なしでした。これで安全といえるでしょうか。
- 監視ソフトウェアを見つけました。そのまま削除すればよいのでしょうか。

1.3 本報告が答える問い

1. 監視はどのように成立するのか（脅威モデルと三つの技術的経路）
2. どのように自己検出するのか（階層的手法、各層の限界、そしてなぜ当該端末上で行えないのか）
3. 発見後の対応（証拠保全・身体的安全・法的手段・クリーンな環境の再構築）

2. 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カウントへのアクセスが、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 MDM 権限が業務範囲外の監視に用いられる

本報告が主に対象とするのは第一と第二の類型です。**接触の機会が最も多く**、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

WP-001 と同様、**加害者の技術的能力はゼロと仮定します**。加害者はプログラムを書く必要も、OS を理解する必要もありません。必要なのは以下の**いずれか一つ**だけです：

- 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、この三つ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。

2.3 被害者の置かれた状況

- **情報の全面的な喪失**：位置情報のみが漏れるトラッカーと異なり、端末の監視はメッセージの内容・通話・写真・閲覧履歴にまで及びます。
- **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対象です。
- **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。
- **端末とアカウント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（一つのパスワードを変えるだけなど）、他の地点から直ちに気づかれ、元に戻されうるのです。

3. 技術的背景：監視の三経路

この経路分類の理解が本報告の方法論の基礎です。**三つの経路は検出すべき場所がまったく異なる**からです。端末を調べるべきものもあれば、アカウントを調べるべきものもあり、場所を誤れば偽りの安心を得ることになります。

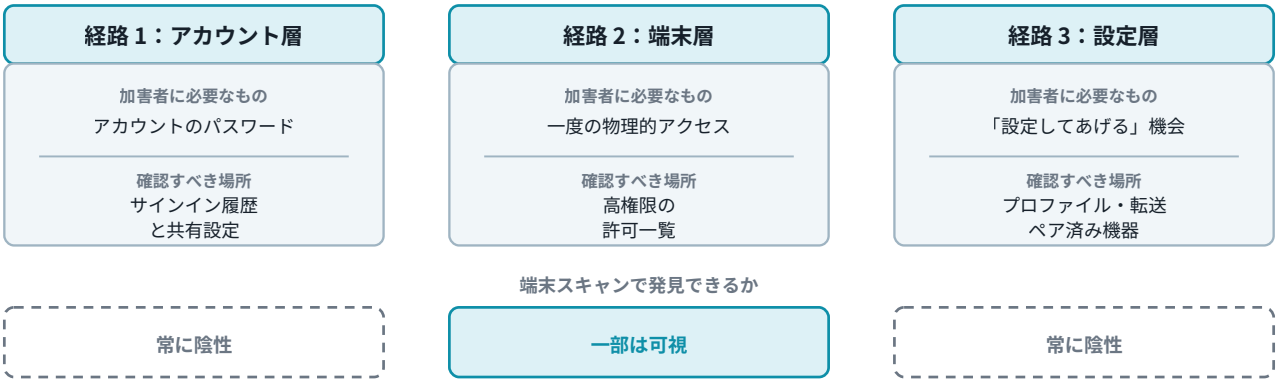

図 1：監視の三経路と、それぞれの検出位置

3.1 経路一：アカウント層の監視（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（端末を探す機能）、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。

3.2 経路二：端末層の監視（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**（accessibility service）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一（アカウント層）または経路三（設定層）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。

端末層の監視ソフトウェアは、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

本報告は、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、当団体『研究倫理準則』における攻撃的詳細の取扱い原則に従うものです。

3.3 経路三：設定層と周辺機器（ソフトウェアではないため、ソフトウェアとして扱われない）

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。**

3.4 三経路の比較

三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：

	経路 1：アカウント層	経路 2：端末層	経路 3：設定層
物理的接触の要否	不要	必要	多くの場合必要
端末スキャンで発見できるか	**不可**	一部可能	**不可**
検出すべき場所	アカウントのサインイン記録と共有設定	端末の高権限の付与一覧	端末設定と外部サービスの規則
解除の方法	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**（アカウントとともに移行）	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。**端末を買い替えても、アカウント層と設定層の監視は解除されません。**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。

---

4. 現行の保護機構とその欠落

4.1 現行機構の基本的な考え方

二大プラットフォームの保護は、おおむね三つの線に沿って発展してきました：

1. **ソフトウェアの提供元の管理**：公式ストアの審査、およびストア外からのインストールに対する警告と制限。
2. **権限の可視化**：高リスクの権限を明示的な許可制とし、機微なセンサーの使用中はインジケータを表示すること。近年は権限の使用履歴を振り返る画面も追加されました。
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、本報告の脅威モデルが見知らぬ他人ではないことにあります。

4.2 欠落の分析

欠落一：アカウント層の監視は、いかなるスキャンの視野にも入らない

セキュリティ製品がスキャンするのは端末上のファイルとソフトウェアです。加害者が正しいパスワードで自分の端末からサインインしている場合、端末側には不審な対象が一切存在しません。**これはスキャンエンジンの性能不足ではなく、確認する場所を誤っているのです。**被害者にとっての帰結は最も危険な部類のものです。陰性のスキャン結果と引き換えに、安全であるという誤った結論を得てしまいます。

欠落二：デュアルユース・アプリの判定困難

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。

欠落三：権限付与の強制的文脈は技術的に不可視である

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。**

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「発見すれば削除すべき」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の即時削除を勧めます。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、親密な関係における暴力の場面では、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。**検出と削除の間には、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。**

欠落六：関係の中にある端末の信頼の連鎖

相手が購入し、設定し、あるいは「処理してくれた」端末は、その信頼の連鎖が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。中古端末と贈られた端末は、この意味において同一の問題です。

---

5. 自己検出の方法論

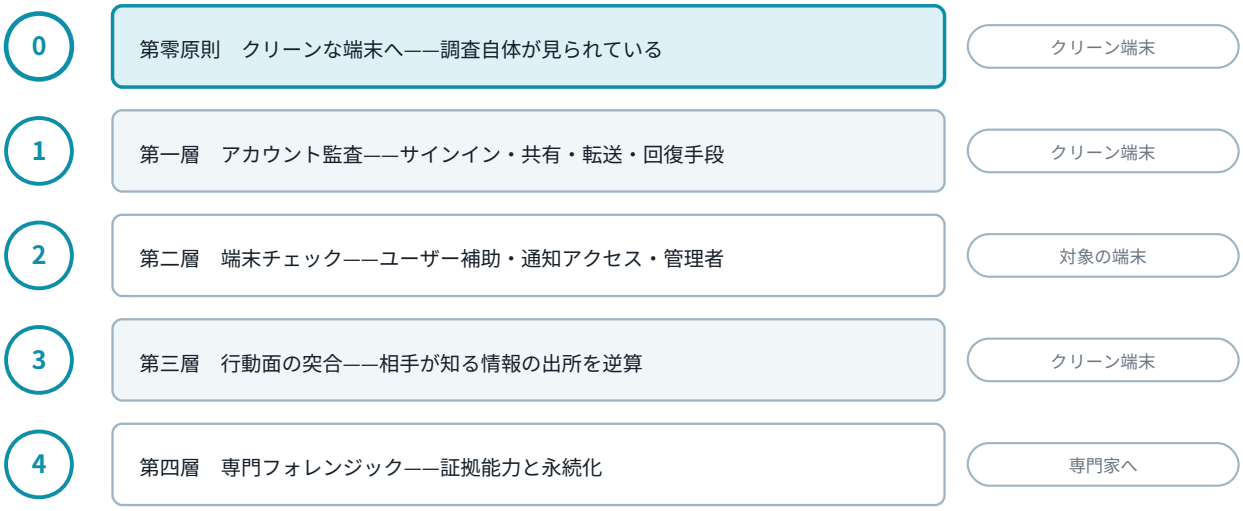

図 2：検出手法——第零原則と四層のチェック

第零原則：まずクリーンな端末を確保する

これが WP-001 との最大の相違であり、唯一省略できない段階です。

トラッカーの場合、被害者の端末は通常は信頼できる道具です。しかしストーカーウェアの場合、その端末こそが調査の対象です。監視が存在するならば、そ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。**あなたが本報告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。

以下の四層のうち、第一層と第三層はクリーンな端末で行い、第二層は対象の端末で操作する必要があるため、最も危険度の高い層となります。

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第 6.1 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 6 章へお進みください。

第三層：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。前者は経路一またはトラッカーからでありえ、後者は端末層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。

実務上、この一覧は何の道具も用いずに調査範囲を単一の経路まで絞り込めることが少なくありません。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。この記録は第 6.2 節の証拠の基礎ともなります。

第四層：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：

- 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場合；
- 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場合、または業務用端末と企業管理権限が関わる場合；
- 必要としているのが監視の解除にとどまらず、**法的手続に用いうる証拠**である場合；
- 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場合。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. 監視発見後の対応

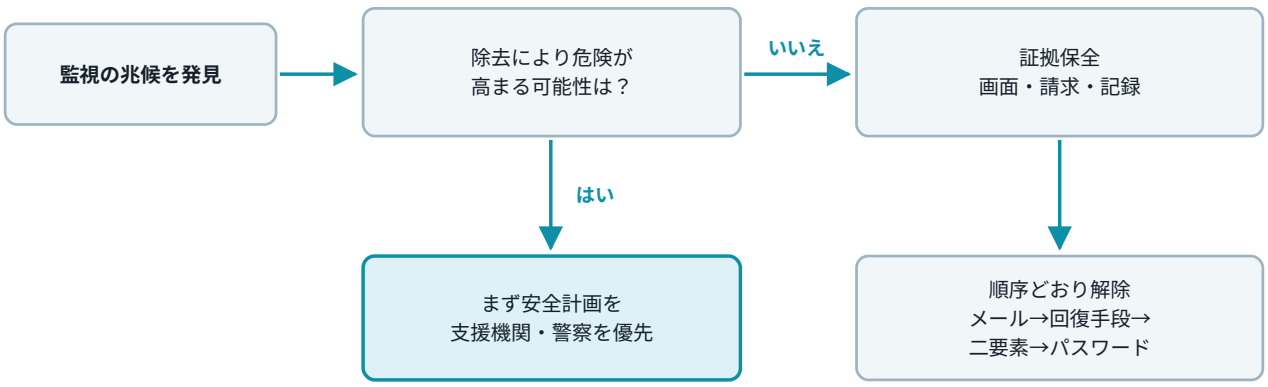

図 3：監視発見後の対応フロー

6.1 第一の優先事項：身体的安全

ストーカーウェアの場合とトラッカーの場合とで、この点の差が最も決定的です。**除去は、相手が直ちに気づく行為です。**

データ送信の途絶、ソフトウェアの消失、アカウントからのサインアウト。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、除去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）。

6.2 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：

- 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）；
- 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）；
- 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；
- 第三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）；
- 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。

証拠保全が完了するまで、**不審なソフトウェアを削除せず、端末を初期化せず、端末を買い替えないでください**。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。

6.3 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。第 6.2 節で保全した証拠を持参し、元の端末は保持してください。

6.4 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。**次の順序で進めることをお勧めします：

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。**

---

7. 事業者と政策立案者への提言

1. **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こと**：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。
2. **共有関係に有効期限と定期的な再確認を設けること**：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。定期的な再確認により、忘れられた共有は自然に失効します。

3. **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。
4. **「発見後」の導線を設計し直すこと**：安全に関する案内が一律に即時の削除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、削除ボタンへ直行させるのではなく、証拠保全と支援資源へ導くべきです。
5. **通知の受け手を独立して設定可能とすること**：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。
6. **端末の引き渡し状態を検証可能とすること**：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。
7. **政策面**：ストーキングおよび家庭内暴力の案件を受理する第一線の担当者には、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。

---

8. 研究の限界と今後の課題

8.1 本バージョンの限界

- 本バージョンは総合分析および方法論の研究であり、**当団体独自の実測データを含みません。**
- プラットフォームの具体的な挙動は OS のバージョンや地域設定によって変動するため、本報告は速やかに古くなる具体的な数値やバージョン番号の記載を意図的に避けています。
- 本報告は特定の事業者の製品名を挙げず、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（第 3.2 節参照）。
- 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。

8.2 計画中の実測（v2.0）

各層の検出手法が実際にどの程度有効であるかを、対照実験により測定する計画です。設計の要点は次のとおりです：

- **被験端末**：当団体が所有する試験用端末。二大プラットフォームの複数バージョンを対象とします。
- **対照群の設計**：経路一・経路二・経路三のそれぞれにより監視状態を構築し、監視されていない端末を対照とします。
- **測定項目**：各層の検出率と偽陰性率、プラットフォームのセキュリティ通知が実際に発動するか、および解除手順の完全性の検証（解除後に監視が確かに途絶するか）。
- **倫理上の制限**：**被験者は当団体の構成員本人、または書面による同意を得た参加者に限ります。**同意していない第三者は一切関与させず、実在の被害者の端末やデータは使用しません。実験に用いる監視のサンプルは外部に配布しません。

本設計は当団体『研究倫理準則』に従い、実験の開始前に公開することで、外部からの検証を可能にしています。

8.3 お寄せいただきたいご意見

- 本報告の方法論は実務上、実行可能でしょうか。とりわけ第零原則は、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でしょうか。
- 第一線の社会福祉・警察・法律の実務家の方々から、第 6 章の対応順序についてどのような修正のご意見がありますか。
- 各層の確認に、本報告が扱っていない永続化経路はありますか。
- 翻訳版の用語は現地の実務に適合しているでしょうか。

ご意見は security@odysec.org へお寄せください（機微な内容は PGP で暗号化してください）。

付録 A：検出チェックリスト

第零原則 - ☐ 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

第一層：アカウント監査 - ☐ 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 - ☐ 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：行動面の突合 - ☐ 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

監視を発見した場合 - ☐ **直ちに削除せず、端末を初期化しない** - ☐ 除去により身体的危険が高まらないかを評価した - ☐ 画面キャプチャとアカウント記録を保全した（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 - ☐ 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
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

付録 C：情報源

本報告は次の種類の公開資料に基づいて執筆されています。二大モバイルプラットフォーム事業者の公式サポート文書とプライバシーに関する説明、ストーカーウェア対策連合（Coalition Against Stalkerware）およびその参加団体が公開する資料と実務指針、親密な関係における監視とストーカーウェアに関する既発表の学術研究、ならびに台湾の「ストーキング・ハラスメント防止法」「刑法」「個人資料保護法」「家庭暴力防治法」の条文です。

プラットフォームの機構の具体的な挙動については、各事業者の公式文書の現行版を基準としてください。本報告と WP-001『無音の同伴者』は姉妹編であり、脅威モデルと方法論の構成は一貫しています。

引用形式：Odysec（2026）『ポケットの中の密告者：スマートフォンのストーカーウェア検出と対応』Odysec 研究報告 WP-002、バージョン 1.0。

免責事項：本報告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）。