

SilentPixel

仕様・運用マニュアル

機種	Google Pixel 7a (lynx)
OS	GrapheneOS
ストレージ	128 GB
発行日	2026-06-03
版数	第 1 版

このマニュアルは本端末の構成・セキュリティ機能・操作方法をまとめたものです。本体内 (Owner / Personal の「ドキュメント」フォルダ) に PDF と Markdown 形式で保存されています。

1. 端末の概要

「SilentPixel」は、Google Pixel 7a に **GrapheneOS**（プライバシー・セキュリティ強化版 Android）を導入し、強要対策・追跡対策・プロフィール分離などを組み合わせて構成したプライバシースマートフォンです。

項目	内容
本体	Google Pixel 7a（コードネーム lynx）
OS	GrapheneOS（Android ベース、Google 非依存運用が可能）
ストレージ	128 GB
暗号化	FBE（ファイルベース全データ暗号化）標準有効
ブートローダ	再ロック済み（locked） + 検証ブート有効
SIM	SIM フリー（本マニュアル発行時点では SIM 未挿入）

2. 最重要セキュリティ機能

2.1 Duress（強要）パスワード ⚠️ 最重要

特定の「Duress 用 PIN/パスワード」をロック画面に入力すると、**端末データが即座に完全消去（ワイプ）**されます。強盗・拘束・押収などで解除を強要された場合の最終防衛策です。

注意： 通常のロック解除パスワードと絶対に混同しないこと。Duress を誤入力すると全データが消えます。実機テスト済みで、入力するとワイプされ初期画面に戻ることを確認済みです（GrapheneOS 本体は残り、再セットアップで復旧可能）。

2.2 Travel Mode（渡航モード）

国境・検問など、生体認証での強制解除を求められやすい場面で、**指紋・顔認証を一時的に無効化**します。PIN/パスワード入力のみが有効になり、「指を当てさせる」式の強制解除を防ぎます。

2.3 起動時の保護（BFU / 自動再起動）

- 自動再起動：8 時間。** 一定時間操作がないと自動で再起動し、暗号鍵がメモリから消えた「BFU（Before First Unlock）」状態に戻します。
- 電源オフ・再起動直後は、最初のパスワード入力まで全データが暗号化されたままです。

2.4 適用済みハードニング設定（実値）

設定 → セキュリティとプライバシー → エクスプロイト保護

設定	値	目的
自動再起動	8 時間	BFU 復帰でメモリ上の鍵を保護
USB-C ポート	ロック時は充電のみ	ロック中の USB 経由攻撃を遮断
Wi-Fi 自動オフ	切断後 10 分	不要な電波・追跡面の縮小
Bluetooth 自動オフ	しない（維持）	Tracker Shield の AirTag 検知を止めないため、あえて維持

3. プロファイル構成（6 プロファイル）

GrapheneOS の複数ユーザー機能で用途ごとに完全分離。各プロファイルは独立して暗号化され、相互にデータアクセスできません。

#	プロファイル	役割	主な導入アプリ
0	Owner（所有者）	端末管理・整合性検証・NetHunter	Auditor、Trespasser、NetHunter (Termux)
10	Personal（個人）	日常利用	Signal、Aurora Store、Aves、KeePassDX、Aegis、地図、NewPipe、AntennaPod、Markor、Etar、Fossify 各種、Tracker Shield
11	Work（仕事）	業務	K-9 Mail、Nextcloud、Aurora Store
12	Bot（副業 SNS）	副業 SNS の隔離	Sandboxed Google Play、LINE、PhoneBridge、Tailscale
13	Burner（使い捨て）	匿名・一時利用	Orbot (Tor)、Tor Browser、PCAPdroid、AppManager、Exodus
14	Pentest	検証用（予備）	Termux※、NetHunter Store

※ Termux はプライマリ（Owner）専用のため Pentest プロファイルでは動作しません（6 章参照）。NetHunter は Owner で運用します。

プロファイル切り替え：画面上部から下にスワイプ → クイック設定 → 右下のユーザーアイコン → 切り替え先を選択（切り替え先のロック解除が必要）。

4. 自作アプリ (SilentPixel 独自)

現状： 実用段階は **Tracker Shield** と **PhoneBridge** です。 その他 (Trespasser / SilentPixel メッセージャー / Witness) は一部が試作 (stub) 段階で、後日に実装を完成させる予定です。

アプリ	プロファイル	状態	概要
Tracker Shield	Personal	実用	AirTag / Tile / SmartTag など BLE 追跡器の付きまといを検知・警告
PhoneBridge	Bot	実用 (要設定)	SNS の DM 等を AI が中継・代行。トークン + Tailscale 設定が必要
Trespasser	Owner	試作	不正解錠の試行を検知してカメラ撮影 (Device Admin 登録済み)
SilentPixel メッセージャー	Personal	試作	E2EE メッセージ / 音声 (実装途上)
Witness	Personal	試作	緊急ライブ記録 (実装途上)

5. ネットワーク・プライバシー運用

- **VPN**： Mullvad (検証系の通信は日常用と別アカウント運用を推奨)。
- **DNS**： NextDNS によるフィルタリング / 追跡ブロック。
- **匿名通信**： Burner プロファイルの Orbot (Tor) + Tor Browser。
- **Google 隔離**： Sandboxed Google Play は **Bot プロファイルのみ**。サンドボックス内の一般アプリとして動作し OS 特権は持ちません。他プロファイルは Google 非依存のまま。
- **アプリ入手元**： F-Droid (各プロファイル)、Aurora Store (Personal/Work)、Play ストア (Bot のみ)、NetHunter Store (Pentest)。
- **電波運用**： 機内モード + 必要時のみ Wi-Fi ON という運用が可能 (GrapheneOS は機内モード下でも Wi-Fi 利用可)。

6. Kali NetHunter (Rootless) の使い方

検証・学習用に Kali NetHunter Rootless (Termux + proot による Kali chroot) を **Owner プロファイル** に導入済みです。Termux はプライマリユーザー専用のため、Pentest ではなく Owner に配置していません。

コマンド (Owner の Termux で実行)	動作
<code>nethunter</code> または <code>nh</code>	Kali CLI を起動

<code>nethunter kex passwd</code>	KeX (GUI) の VNC パスワードを設定 (初回に 1 度)
<code>nethunter kex start</code>	Kali GUI (KeX) を起動
<code>nethunter kex stop</code>	Kali GUI を停止
<code>nethunter -r</code>	chroot 内で root として実行

導入版 : Kali GNU/Linux Rolling (full / ARM64)。

できること : nmap (範囲限定)、Metasploit、sqlmap、hydra、Python 系ツール、ssh/curl 等、KeX による GUI。

できないこと (root/カーネル必須のため不可) : Wi-Fi モニタモード/インジェクション、Aircrack-ng アクティブ攻撃、USB HID (BadUSB)、MAC アドレス変更 等。

法令順守 : 利用は自分の所有・許可された環境、CTF、書面許可のある業務に限ること。無許可のネットワークへの侵入・調査は不正アクセス禁止法に抵触します。

7. まだ必要な手動セットアップ

1. **SIM 挿入後** → LINE の電話番号登録 (Bot)、Signal の電話番号登録 (Personal)。
2. **NetHunter KeX** → `nethunter kex passwd` でパスワード設定 → `nethunter kex start` で GUI 利用。
3. **PhoneBridge** → 連携トークンの設定 + Tailscale へのログイン (Bot)。

8. 日常運用・メンテナンス

- **OS 更新** : 設定 → システム → アップデート (自動更新、再起動で適用)。
- **アプリ更新** : App Store (GrapheneOS 製)、F-Droid、Aurora、Play ストア (Bot) でそれぞれ更新。
- **Kali 更新** : 利用前に Kali 内で `sudo apt update && sudo apt full-upgrade` を推奨 (導入時に整合性ハッシュ検証がスキップされているため、署名付き apt で実体を更新しておく安心)。
- **パスワード管理** : KeePassDX (Personal)。多要素は Aegis (Personal)。
- **バックアップ** : 重要データは Nextcloud (Work) や暗号化バックアップで保全。Duress 消去に備える。

9. 緊急時の対応

状況	対応
解除を強要された	Duress パスワード を入力 → 全データ即時消去

国境・検問	事前に Travel Mode 起動（生体認証オフ）
盗難・紛失	FBE 暗号化+自動再起動（BFU）で中身は保護。位置確認は Find 系で
端末がワイプされた	GrapheneOS 本体は残存。再セットアップで復旧（自作 APK 含め再導入手順あり）

10. サポート

不明点・再設定・自作アプリの完成版アップデート等については販売／構築元へお問い合わせください。

本マニュアルは 2026-06-03 時点の構成に基づきます。設定変更・アプリ追加に応じて内容は変わります。