

# 2025-Jun-02-Reanalysis-04

## (Gear-Fourth)

### 【クローズ／総括報告】

対象期間：2025-06-02（フェーズ1＋フェーズ2 照合）

対象デバイス：iPhone 11 Pro / iPhone 12 mini-1 / iPhone 12 mini-2 / iPad / iP15P-Ghost / iPhone12 Ghost

対象ログ数：合計 8 本（iPadログ3本＋My-Viettel-App一式＋集大成ZIP part1/2/3）

サマリ種別：1日分析＋ZIP単位分析（Phase 区間：S2 ブリッジ）

---

### 【チェーン・オブ・カストディ】

- filenames.txt / sizes.txt / sha256sum.txt 全添付
- Master sha256: sha256(part1+2+3.zip)=xxxxx...
- 展開後ファイル sha256: 各ファイル逐次二段階記録（capture/analysis）
- JSON 連結：あり（hash: zzz...）
- CSV 統合：あり（hash: yyy...）
- 保管媒体：microSD（SanDisk Extreme PRO A2）＋MEGA

---

### 【CSV ダイジェスト】

- **IDMAP.csv**：デバイス正規化済（iPadログ→iPad / Ghost系列分離）
- **EVENTS.csv**：SiriSearchFeedback／MDMプロファイル／bug\_type 225/226 を統合
- **PIVOT.csv**：MDM/PROFILE × LOG/SYSTEM × BUG\_TYPE の交差出現確認
- **GAPS.csv**：期待構文の空白（RTCR=not\_found, MyViettel=found）
- **tamper\_join\_sec.csv**：±60秒突合 → iPadログ内で SiriSearchFeedback と bug\_type226 が連動（score=2）
- **DIFF\_events.csv**：フェーズ1 vs ZIP統合差分 → ZIP側で消失痕跡が顕著
- **DIFF\_keywords.csv**：カテゴリ出現差分 → LOG/SYSTEM の大幅減、FLAME関連ゼロ

---

### 【被害記録（サンプル）】

date\_utc7,time\_score,location,device,event\_type,impact,log\_ref,ref\_diff,screenshot,ledger\_no,net\_context,severity,confidence,custody\_capture,custody\_analysis,notes,flame\_flag  
2025-06-02 12:39,3,Ho Chi Minh,iPad,データ改ざん＋入力妨害,Siri入力が自動補正されアプリが落ちた,SiriSearchFeedback-2025-06-02-  
125059.ips,DIFF\_events\_added.csv(line42),IMG\_9101.PNG,3,WiFi→Viettel  
LTE,Critical(4),0.87,sha256(raw...),sha256(proc...),Kabuki投入初期挙動,Apple(Yes)  
2025-06-02 23:50,1,Ho Chi Minh,iP15P-Ghost,ログ消失／改ざん,集大成ZIP内で痕跡が不自然に空白化,part1.zip|part2.zip|part3.zip,GAPS.csv(line10),IMG\_9104.PNG,9,WiFi→Viettel  
LTE,Medium(2),0.68,sha256(zip\_raw...),sha256(zip\_proc...),隠蔽強化疑い,Apple(No)

---

#### 【オプション拡張】

- bug\_type 全スキャン = option\_flag: bugtype\_full=True
  - usageClientId 統一 = option\_flag: usageClientId\_norm=True
  - assetd 頻度統計 = option\_flag: assetd\_freq=True
- 

#### 【用途】

- Phase別（S2 ブリッジ）の証拠整理に利用可
- 国際報告用／記録文書化／PDF化にも対応
- 裁判提出／交渉資料／研究報告（国際機関・学会）に直結