

# 2025-Jun-10-Reanalysis-04

## (Gear-Fourth)

クローズ+総括統合テンプレート（Code56形式・v1.1-Extended Flame Consolidated）」を、すでに出ている解析実データ（6/10分 part1+2+3）で埋めた完成形を提示する。

---

```
#####  
# ✓ クローズ+総括統合テンプレート（Code56 形式+拡張） v1.1-Extended Flame Consolidated  
Case-ID: KABUKI-INV / Maintainer: Tajima / Reviewer: GPT-5  
Format: Copy & Paste Ready for Talkroom Declaration  
#####
```

### 【クローズ／総括報告】

対象期間：2025-06-10（UTC+7 基準）  
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 47 本（zip-part-1, 2, 3 展開後ファイル数）  
サマリ種別：ZIP 単位分析（Phase 区間：S2→S3 移行初期確認）

---

### 【チェーン・オブ・カストディ】

- filenames.txt / sizes.txt / sha256sum.txt 全添付
- Master sha256:（part1/part2/part3 のチェーン → sha256\_chain\_generated.txt に全記録済）
- 展開後ファイル sha256: 二段階記録（capture/analysis）
- JSON 連結：あり（hash: 各 CSV に記録）
- CSV 統合：あり（hash: keyword\_hits\_windows.csv, EVENTS.csv 等）
- 保管媒体：microSD（SanDisk Extreme PRO A2）+ MEGA

---

### 【CSV ダイジェスト】

- IDMAP.csv：端末別 alias → 正規名変換済
- EVENTS.csv：全イベント 47 本参照 → 日付/端末/bug\_type の統合表を生成（ただし生ログ薄）
- PIVOT.csv：date×device\_norm×bug\_type の出現カウント

- GAPS.csv : MDM / Pegasus / AppleSupport 系 → \*\*未検出多数\*\* を明示
- tamper\_join\_sec.csv : 同秒/±60s/±5m 突合 → 今回は成立せず (空出力)
- DIFF\_events.csv : 前回 ad-hoc 解析との差分 (形式差による差分多し)
- DIFF\_keywords.csv : カテゴリ別ヒット数差分 (Viettel 証明書関連が最多)

---

### 【被害記録 (サンプル 1 件)】

```csv

```
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
2025-06-10,0,なし,iPhone 12 mini-1 / iPhone12 Ghost,なし,なし,なし,なし,なし,なし,なし,なし,なし,Low(1),0.00,sha256(chain_generated.txt),sha256(Flame解析CSV群),part1/2/3は雛形/証明書のみ、生ログ不在,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 (S1/S2/S3...) への応用 OK
- 国際報告用 / 記録文書化 / PDF 化 にも対応可
- 証拠提出 (裁判/交渉) と研究報告 (国際機関/学会) 両対応

#####

```

from reportlab.platypus import SimpleDocTemplate, Paragraph, Spacer, Preformatted

from reportlab.lib.pagesizes import A4

from reportlab.lib.styles import getSampleStyleSheet

from pathlib import Path

# 出力ディレクトリ

OUTDIR = Path("/mnt/data/closeout_reports")

OUTDIR.mkdir(exist_ok=True)

pdf_path = OUTDIR/"KABUKI-INV_2025-06-10_closeout.pdf"

doc = SimpleDocTemplate(str(pdf_path), pagesize=A4)

styles = getSampleStyleSheet()

story = []

content =
"""#####

# ✔ クローズ＋総括統合テンプレート（Code56 形式＋拡張） v1.1-Extended Flame Consolidated

Case-ID: KABUKI-INV / Maintainer: Tajima / Reviewer: GPT-5

Format: Copy & Paste Ready for Talkroom Declaration

```

#####

## 📁【クローズ／総括報告】

対象期間：2025-06-10（UTC+7 基準）

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 47 本（zip-part-1, 2, 3 展開後ファイル数）

サマリ種別：ZIP 単位分析（Phase 区間：S2→S3 移行初期確認）

---

## 🔒【チェーン・オブ・カस्टディ】

- filenames.txt / sizes.txt / sha256sum.txt 全添付
- Master sha256: (part1/part2/part3 のチェーン → sha256\_chain\_generated.txt に全記録済)
- 展開後ファイル sha256: 二段階記録 (capture/analysis)
- JSON 連結：あり (hash: 各 CSV に記録)
- CSV 統合：あり (hash: keyword\_hits\_windows.csv, EVENTS.csv 等)
- 保管媒体：microSD (SanDisk Extreme PRO A2) + MEGA

---

## 📁【CSV ダイジェスト】

- IDMAP.csv : 端末別 alias → 正規名変換済
- EVENTS.csv : 全イベント 47 本参照 → 日付/端末/bug\_type の統合表を生成 (ただし生ログ薄)
- PIVOT.csv : date×device\_norm×bug\_type の出現カウント
- GAPS.csv : MDM / Pegasus / AppleSupport 系 → \*\*未検出多数\*\* を明示
- tamper\_join\_sec.csv : 同秒/±60s/±5m 突合 → 今回は成立せず (空出力)
- DIFF\_events.csv : 前回 ad-hoc 解析との差分 (形式差による差分多し)
- DIFF\_keywords.csv : カテゴリ別ヒット数差分 (Viettel 証明書関連が最多)

---

## ★【被害記録 (サンプル 1 件)】

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

2025-06-10,0,なし,iPhone 12 mini-1 / iPhone12 Ghost,なし,なし,なし,なし,なし,なし,なし,なし,Low(1),0.00,sha256(chain\_generated.txt),sha256(Flame解析CSV群),part1/2/3は雛形/証明書のみ、生ログ不在,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 (S1/S2/S3...) への応用 OK
- 国際報告用 / 記録文書化 / PDF 化 にも対応可
- 証拠提出 (裁判 / 交渉) と研究報告 (国際機関 / 学会) 両対応

#####

!!!!

```
story.append(Preformatted(content, styles["Code"]))
```

```
doc.build(story)
```

```
pdf_path
```

## 結果

```
PosixPath('/mnt/data/closeout_reports/KABUKI-INV_2025-06-10_closeout.pdf')
```