

新潟県糸魚川市役所 御中

教育用端末調査業務 報告書

2026 年 5 月 29 日

NEC セキュリティ株式会社

目次

1. 実施概要	3
1.1. はじめに.....	3
1.2. 調査目的.....	3
1.3. 調査実施期間.....	3
1.4. 調査対象.....	3
1.5. 調査担当者.....	3
1.6. 調査に使用したソフト.....	3
1.7. 本報告書の取扱いについて.....	4
2. 保全	5
2.1. 保全方法.....	5
2.2. 保全結果.....	5
3. 調査結果	7
3.1. 調査結果概要.....	7
3.2. 調査結果詳細.....	8
3.2.1. 初期化状況の確認	8
3.2.2. Wi-Fi 接続履歴の確認	9
3.2.3. 記録された位置情報について	10
3.2.4. Web 履歴について	11
3.2.5. 画像ファイルについて	12
巻末資料・保全で行った操作	13

1. 実施概要

1.1. はじめに

本報告書は、新潟県糸魚川市役所様（以降「貴庁」という。）向けに実施した、フォレンジック調査の結果を記述したものです。

1.2. 調査目的

本調査では、[REDACTED] 中学校で発生した人間関係トラブルに伴い、「1.4. 調査対象」に記載した調査対象端末の紛失期間（令和 4 年 12 月～令和 5 年 3 月）において、外部への情報書き込みなどの操作が行われた履歴等、使用状況を調査することを目的としました。

1.3. 調査実施期間

本調査の実施期間は以下の通りです。

2026 年 5 月 12 日～2026 年 5 月 21 日

1.4. 調査対象

本調査では、以下の機器・データを調査対象としています。

① iPad01

- デバイス名 : ito-[REDACTED]
- OS: iOS 16.3.1
- ディスク容量 : 32GB

② iPad02

- デバイス名 : ito-[REDACTED]
- OS: iOS 16.3.1
- ディスク容量 : 32GB

1.5. 調査担当者

[REDACTED] (NEC セキュリティ株式会社)

[REDACTED] (NEC セキュリティ株式会社)

[REDACTED] (NEC セキュリティ株式会社)

[REDACTED] (NEC セキュリティ株式会社)

1.6. 調査に使用したソフト

解析ツール

- Cellebrite Inseyets Physical Analyzer バージョン : 10.9.0.3029
- Magnet AXIOM バージョン : v9.9.0.46675

1.7. 本報告書の取扱いについて

本報告書の取扱いについては、以下の点にご注意ください。

- 本報告書には、貴庁の情報セキュリティ事象についての重要な記述が含まれていますので、取扱いには十分注意してください。
- 本報告書には、調査で判明した貴庁利用のスマートフォンに関する詳細や個人情報の記述が含まれておりますので、取り扱いには十分注意してください。
- 本報告書に記された調査結果は、発見された痕跡、ログからの事実および、そこからの推測を記述したものであり、実際の行動がその通りとは限りません。
- 本報告書の著作権は弊社が所有しており、本報告書の複製、改変、開示及び、翻訳を禁止します。システム管理者や経営者への報告、関係会社への報告、セキュリティ対策の実施のために使用する場合に限り、複製することを許諾いたします。それ以外の目的に使用する場合は弊社にお問い合わせください。

2. 保全

本調査では、調査を行うにあたり調査対象の複製データを作成する保全を行いました。保全方法および結果は以下の通りです。

保全実施日時

- 2026/5/12 09:56~2026/5/12 14:23

保全実施場所

- 新潟県糸魚川市 糸魚川市立 中学校

保全使用機器

- 保全用 PC : DELL Latitude 3400
- 保全用ソフトウェア : Cellebrite Inseyets UFED 10.9.0.284
- 保全用ディスク : Western Digital WD Blue SA510 4TB

保全対応者

- (NEC セキュリティ株式会社)
- (NEC セキュリティ株式会社)
- (NEC セキュリティ株式会社)

2.1. 保全方法

iPad01 及び iPad02 は以下の手順で保全作業を実施しました。

1. 保全対象の確認
2. 保全対象の起動及びシリアル番号を確認
3. 保全用 PC 上で保全用ソフトウェアを起動し、同 PC と保全対象を接続
4. 保全用ソフトウェアを使用して、保全対象のデータを保全用ディスクに抽出
5. 正常に保全が完了したことを確認

保全で行った操作に関しては、巻末資料として記載しました。

なお、iPad はセキュリティ向上の目的でパスコードが設定されていることが多いですが、本件の保全対象の 2 台の iPad は、保全実施時において、パスコードは設定されていない状態となっていました。

2.2. 保全結果

iPad01 の保全結果は以下の通りです。

- メーカー : Apple
- モデル : iPad 第 8 世代 (Wi-Fi)
- モデル番号 : J171aAP
- 製造番号 : H9HF2TKXQ1GD
- デバイス名 : ito-
- OS : iOS 16.3.1
- 容量 : 32GB
- 保全データ : 15.88 GB

- ディスクイメージ形式 : zip
- SHA256 形式のハッシュ値
 - ✧ Source ハッシュ値 :
AE2D04C57EF17837EC2217CCAB11A87565F8A08B36638231EAD60FAD0F0621DB
 - ✧ Verify ハッシュ値 :
AE2D04C57EF17837EC2217CCAB11A87565F8A08B36638231EAD60FAD0F0621DB

iPad02 の保全結果は以下の通りです。

- メーカー : Apple
- モデル : iPad 第 8 世代 (Wi-Fi)
- モデル番号 : J171aAP
- 製造番号 : H97F3C5LQ1GD
- デバイス名 : ito-XXXXXXXXXX
- OS : iOS 16.3.1
- 容量 : 32GB
- 保全データ : 17.66 GB
 - ディスクイメージ形式 : zip
 - SHA256 形式のハッシュ値
 - ✧ Source ハッシュ値 :
F6EB1BF9D96CFD128F65EFB22221789CD484D32E2A9DF6A2DB61BAE9129AB2A8
 - ✧ Verify ハッシュ値 :
F6EB1BF9D96CFD128F65EFB22221789CD484D32E2A9DF6A2DB61BAE9129AB2A8

以下のことを確認し、保全が正常に完了したことを確認しました。

- 作成した複製データのハッシュ値¹ (Source ハッシュ値) が、確認用のハッシュ値 (Verify²ハッシュ値) と一致している
- 作成ディスクイメージに破損などが無い

上記の結果より、原本 (調査対象のデータ) と複製データの内容が同一であることを確認した上で、調査を実施しました。

なお、本保全では、調査対象 iPad から可能な限りのデータ抽出を行いましたが、iOS の特性上、ディスクの未使用領域も含めた iPad データ全体の抽出には至りませんでした。これにより、ディスク未使用領域から削除されたデータの復元を行うことは出来ませんでした。

¹ ハッシュ値：特殊な手順によって計算される不可逆の値。1 文字でもデータが異なる場合は、まったく違う値が生成されるため、データが改ざんされていないことを証明するためによく用いられる。

² Verify：データの正確性等を検証すること。今回の場合、保全対象や抽出したデータ自体を Source ハッシュ値、解析する際のデータを Verify ハッシュ値と定義し、この両者の値が同一であることをもって、解析対象の同一性や真正性を担保している。

3. 調査結果

3.1. 調査結果概要

調査を行った結果、iPad01 及び iPad02 共に、データの初期化が行われている痕跡が確認されました。初期化が行われたと思われる日時は以下の表 1 に記載のとおりです。

表 1 初期化の実施日時

調査対象	日時
iPad01	2023/3/17 09:22:32 付近
iPad02	2023/3/16 11:04:07 付近

なお、初期化処理が行われた日時付近に記録された位置情報を参考にと iPad01 及び iPad02 共に、以下の位置情報が記録されていました。

表 2 初期化処理時付近に記録された位置情報

調査対象	データ記録日時	記録された座標	
		緯度	経度
iPad01	2023/3/17 09:31:31	37.038994290324304	137.86284845269319
iPad02	2023/3/16 11:32:33	37.038992108411264	137.86279296875

上表記載の座標情報を確認すると、いずれの座標も糸魚川市役所と確認できました。そのため、初期化処理が糸魚川市役所付近で行われた可能性が高いと推測されます。

その他、ユーザーの使用痕跡を確認するため、Web 履歴や画像ファイル等の調査を行いました。ユーザーが明示的に検索したと思われる履歴や撮影及び編集した画像ファイルなどは発見されませんでした。

以上のことから、本事案に関係があると推測される痕跡は、iPad01 及び iPad02 共に初期化処理によって残存していないものと推測されます。

3.2. 調査結果詳細

保全終了後、調査を開始するために調査対象データを確認したところ、データが初期化されている状況が確認できました。初期化が行われたと思われる日時は以下のとおりです。

- iPad01：2023/3/17 09:22:32 付近
- iPad02：2023/3/16 11:04:07 付近

なお、初期化が行われた日時の調査については、各 iPad 内の「.bootstrapped」ファイルの作成時刻を参照しております。

本ファイルは、iPad において初期化が実施された際に作成されるサイズ 0 バイトのファイルであり、当該ファイルの作成日時を参照することで、初期化が行われた時間帯を確認することが可能です。

各 iPad の「.bootstrapped」の日時情報については、次の図 1 及び図 2 のとおりです。

FileDump / EXTRACTION_FFS.zip / root / private / var / root					
↑ 名前	サイズ (バイト)	作成日	更新日	アクセス日	
Library	69041024	2023/03/17 9:22:32(UTC+9)	2023/03/17 9:26:12(UTC+9)	2023/03/17 9:22:32(UTC+9)	
.aks_allowlist	1	2023/03/17 9:23:25(UTC+9)	2023/03/17 9:23:25(UTC+9)	2023/03/17 9:23:25(UTC+9)	
.aks_migrate	1	2023/03/17 9:24:46(UTC+9)	2023/03/17 9:24:46(UTC+9)	2023/03/17 9:24:46(UTC+9)	
.bootstrapped	0	2023/03/17 9:22:32(UTC+9)	2023/03/17 9:22:32(UTC+9)	2023/03/17 9:22:32(UTC+9)	
.mkb_seshat_health	98	2023/03/17 10:59:27(UTC+9)	2026/05/12 11:16:39(UTC+9)	2023/03/17 10:59:27(UTC+9)	

図 1 iPad01 の初期化状況（「.bootstrapped」の作成日時）

↑ 名前	サイズ (バイト)	作成日	更新日	アクセス日	
Library	78214727	2023/03/16 11:04:07(UTC+9)	2023/03/16 11:19:04(UTC+9)	2023/03/16 11:04:07(UTC+9)	
.aks_allowlist	1	2023/03/16 11:05:03(UTC+9)	2023/03/16 11:05:03(UTC+9)	2023/03/16 11:05:03(UTC+9)	
.aks_migrate	1	2023/03/16 11:06:25(UTC+9)	2023/03/16 11:06:25(UTC+9)	2023/03/16 11:06:25(UTC+9)	
.bootstrapped	0	2023/03/16 11:04:07(UTC+9)	2023/03/16 11:04:07(UTC+9)	2023/03/16 11:04:07(UTC+9)	
.mkb_seshat_health	100	2023/03/16 12:26:21(UTC+9)	2026/05/12 11:59:34(UTC+9)	2023/03/16 12:26:21(UTC+9)	

図 2 iPad02 の初期化状況（「.bootstrapped」の作成日時）

3.2.1. 初期化状況の確認

保全時に、調査対象の状態について、以下が確認できました。

- ① 端末の初期化が行われているようだが、デバイス名が初期名称から変更されている。
- ② 同一仕様の端末で初期化を実施したと考えられるにも関わらず、ディスク使用サイズが異なる。

この点について、確認をおこなったところ、本端末には Meraki MDM といわれる管理アプリケーションがインストールされていることが判明しました。

本管理アプリケーションの処理が端末の初期セットアップ後に行われている痕跡が確認できたことから、その処理により、iPad01 及び iPad02 のデバイス名が変更された可能性が存在します。

また、iPad01 において、管理アプリケーションの処理が未完了となっている痕跡が存在しました。

そのため、iPad01 はアプリケーションのインストール等一部処理が終了していないなどの理由により、iPad02 よりも少ないデータ量となっている可能性が考えられます。

3.2.2. Wi-Fi 接続履歴の確認

iPad01 及び iPad02 共に複数の Wi-Fi 接続履歴が確認できました。

それぞれの接続履歴については、図 3 及び図 4 のとおりです。

↓ 前回接続時	前回自動接続時	タイムスタンプ	終了時刻	BSSID	SSID	位置
2023/03/17 9:26:12(UTC+9)	2024/10/10 16:39:20(UTC+9)	2023/03/17 9:26:12(UTC+9)			216_Itoigawa_Student	
	2024/09/27 11:57:34(UTC+9)			18:ec:e7:2e:a5:20	216_Itoigawa_Student	■■■■■■■■■■
	2024/10/10 16:39:20(UTC+9)			18:ec:e7:2e:a5:30	216_Itoigawa_Student	■■■■■■■■■■

図 3 iPad01 の Wi-Fi 接続履歴

↓ 前回接続時	前回自動接続時	タイムスタンプ	終了時刻	BSSID	SSID	位置
2023/03/16 11:19:22(UTC+9)	2024/10/08 15:28:07(UTC+9)	2023/03/16 11:19:22(UTC+9)			216_Itoigawa_Student	
		2024/10/08 15:28:11(UTC+9)	2026/05/12 10:28:53(UTC...		216_Itoigawa_Student	
		2024/09/27 10:38:34(UTC+9)	2024/09/27 12:06:28(UTC...		216_Itoigawa_Student	
		2024/09/09 17:59:05(UTC+9)	2024/09/09 18:09:19(UTC...		216_Itoigawa_Student	
		2024/09/07 11:32:37(UTC+9)	2024/09/07 19:32:46(UTC...		216_Itoigawa_Student	
		2024/09/06 12:06:10(UTC+9)	2024/09/06 13:51:13(UTC...		216_Itoigawa_Student	
			2024/09/03 11:41:16(UTC...		216_Itoigawa_Student	
					216_Itoigawa_Student	
	2024/09/09 18:06:39(UTC+9)			18:ec:e7:2e:cf:e0	216_Itoigawa_Student	■■■■■■■■■■
	2024/09/27 12:00:56(UTC+9)			18:ec:e7:2e:a5:20	216_Itoigawa_Student	■■■■■■■■■■
	2024/10/08 15:28:07(UTC+9)			18:ec:e7:2e:a5:30	216_Itoigawa_Student	■■■■■■■■■■

図 4 iPad02 の Wi-Fi 接続履歴

確認された Wi-Fi 接続履歴はすべて、SSID「216_Itoigawa_Student」のものでした。

また、一部接続履歴には座標情報が記録されており、記録されていた座標はすべて■■■■■■■■■■中学校付近となっていました。

調査対象内の Wi-Fi 接続履歴にて、最も古い履歴を調査したところ、それぞれ以下のものとなりました。

- iPad01 の最古の Wi-Fi 接続日時：2023/3/17 9:26:12
- iPad02 の最古の Wi-Fi 接続日時：2023/3/16 11:19:22

3.2.3. 記録された位置情報について

iPad01 及び iPad02 共に、初期化が実施されたと思われる日時以降の位置情報のみが記録されていました。

それぞれに記録されていた位置情報の詳細については表 3 及び表 4 のとおりです。

なお、表 3 及び表 4 に記載の場所については、端末内に記録されている緯度・経度の情報を元に、確認調査をした結果を記載しております。

表 3 iPad01 に記録されていた位置情報

場所	日付
糸魚川市役所付近	・ 2023/03/17
■■■■中学校付近	・ 2023/03/17 ・ 2023/03/28 ・ 2024/09/03 ・ 2024/09/06 ～ 2024/09/07 ・ 2024/09/27

表 4 iPad02 に記録されていた位置情報

場所	日付
糸魚川市役所付近	・ 2023/03/16 ～ 2023/03/17
糸魚川警察署付近	・ 2023/05/01
■■■■中学校付近	・ 2023/04/17 ・ 2023/04/19 ～ 2023/04/20 ・ 2023/04/24 ・ 2023/05/01 ・ 2024/09/03 ・ 2024/09/06 ～ 2024/09/07 ・ 2024/09/27 ～ 2024/10/08

なお、本位置情報については、座標の誤差や iPad の位置情報記録間隔の理由から、その時に必ず記載の場所に当該 iPad が存在したということを証明するものではありません。

また、表 3 及び表 4 については日付のみを記載しております。各 iPad に記載された詳細な位置情報については、「別紙 1_iPad01 の位置情報」及び「別紙 2_iPad02 の位置情報」をご参照ください。

なお、iPad の初期化処理が行われた日時付近に記録された位置情報を参考にと iPad01 及び iPad02 共に、以下の位置情報が記録されていました。

表 2 初期化実施時付近に記録された位置情報

調査対象	データ記録日時	記録された座標	
		緯度	経度
iPad01	2023/3/17 09:31:31	37.038994290324304	137.86284845269319
iPad02	2023/3/16 11:32:33	37.038992108411264	137.86279296875

上表記載の座標情報を確認すると、いずれの座標も糸魚川市役所と確認できました。そのため、初期化処理が糸魚川市役所付近で行われた可能性が高いと推測されます。

3.2.4. Web 履歴について

iPad01 及び iPad02 共に、Safari (iPad の標準ブラウザアプリ) と Google Chrome の 2 種類がインストールされていることを確認しました。

Safari 及び Google Chrome のログを調査しましたが、iPad02 においては、ユーザーが明示的に行ったとみられる検索履歴、Web 閲覧履歴及びブックマークなどの情報は残存しておりませんでした。

iPad01 については、Safari 及び Google Chrome 共に少量の閲覧履歴が残存しておりましたが、どちらも 2024 年 9 月の履歴となっていました。

表 5 iPad01 における Safari の閲覧履歴

アクセス日時	Web ページのタイトル	URL
2024/09/06 12:18:52	iCloud	https[:]//www[.]icloud[.]com/ ³
2024/09/06 12:19:21	iCloud	https[:]//www[.]icloud[.]com/

表 6 iPad01 における Google Chrome の閲覧履歴

アクセス日時	Web ページのタイトル	URL
2024/09/03 11:37:11	Education Fundamentals - Google for Education	https[:]//edu[.]google[.]com/products/gsuite-for-education/
2024/09/03 11:37:11	Education Fundamentals - Google for Education	https[:]//edu[.]google[.]com/workspace-for-education/editions/education-fundamentals/
2024/09/03 11:37:23	Education Fundamentals - Google for Education	https[:]//edu[.]google[.]com/workspace-for-education/editions/education-fundamentals/
2024/09/06 12:23:35	Education Fundamentals - Google for Education	https[:]//edu[.]google[.]com/workspace-for-education/editions/education-fundamentals/

なお、iPad01 の Safari 閲覧履歴にて、iCloud へのアクセス履歴が存在しますが、iPad01 及び iPad02 共に、iCloud を使用するために必要となる Apple アカウントへのログイン痕跡は確認されず、iCloud の使用に関しても履歴は確認されませんでした。

³ 本報告書に記載の URL に関しては、誤接続防止のために、URL 内記載の「:」及び「.」部分を括弧 ([]) で囲んでおります。

3.2.5. 画像ファイルについて

調査対象内に、ユーザーの操作によって作成された画像などが存在するか、確認を行いました。

iPad では、画像ファイルは主に以下の場所に保存されます。

- ① DCIM：ユーザーがカメラ等で写真を撮影した際に保存される領域
- ② PhotoData：端末内の画像ファイルの管理データやサムネイル画像等が記録される。

表 7 iPad01 の画像ファイルの保全結果

フォルダパス	フォルダ内の使用サイズ	フォルダ内のファイル数
mobile/Media/DCIM	0B	0
mobile/Media/PhotoData	4.85MB	72

表 8 iPad02 の画像ファイルの保全結果

フォルダパス	フォルダ内の使用サイズ	フォルダ内のファイル数
mobile/Media/DCIM	0B	0
mobile/Media/PhotoData	4.69MB	68

確認の結果、iPad01 及び iPad02 共に、確認された画像ファイルは PhotoData フォルダ内にあるシステムが作成したと考えられるもののみであり、ユーザーの操作によって撮影、保存及び編集が行われたと考えられる画像ファイルの痕跡は、確認されませんでした。

巻末資料・保全で行った操作

本件の保全は、以下の操作により実施しました。

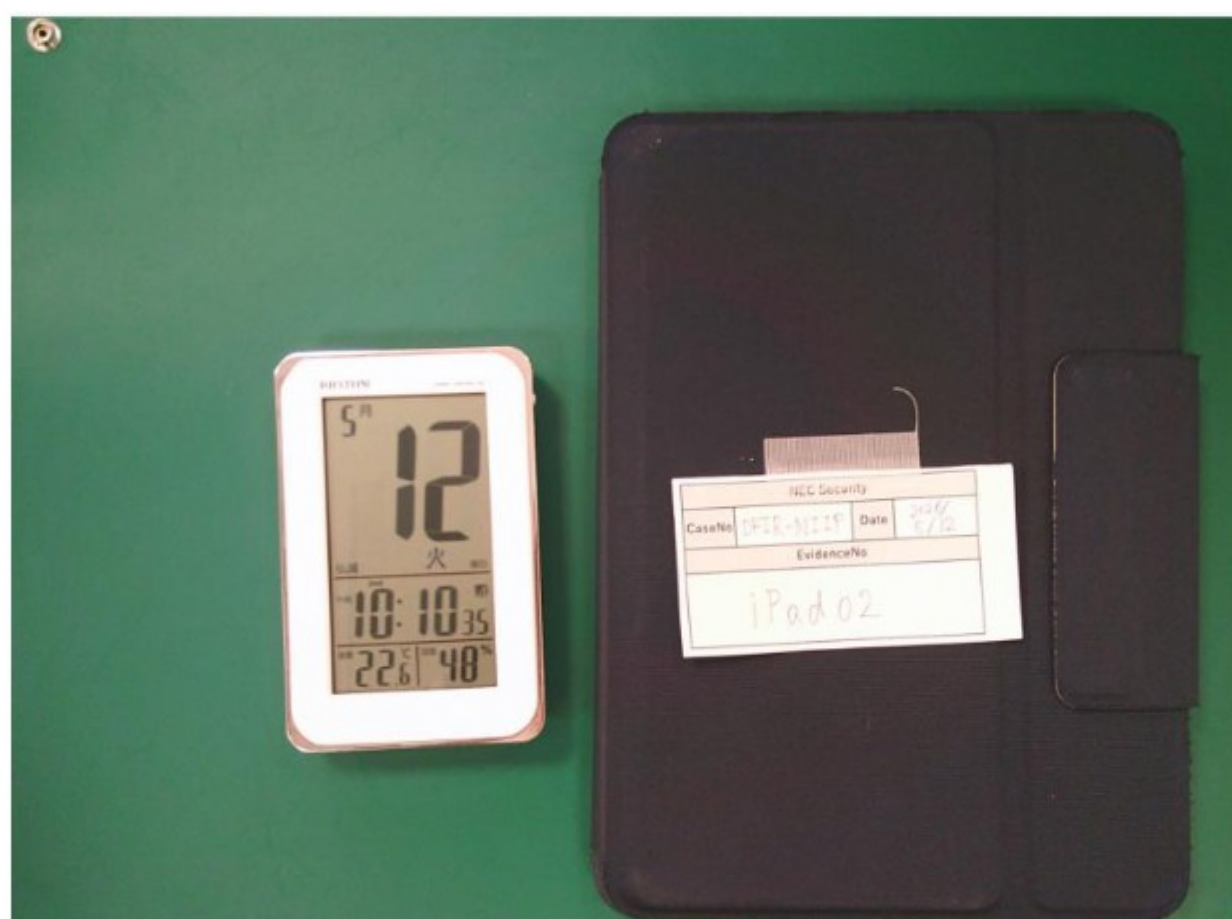
① 保全対象確認 (2026/05/12 09:56:48 実施)



② 保全対象 iPad01 の確認 (2026/05/12 10:03:05 実施)



③ 保全対象 iPad02 の確認 (2026/05/12 10:10:35 実施)



④ 保全対象 iPad01 の起動及びシリアル番号の確認 (2026/05/12 10:29:11 実施)

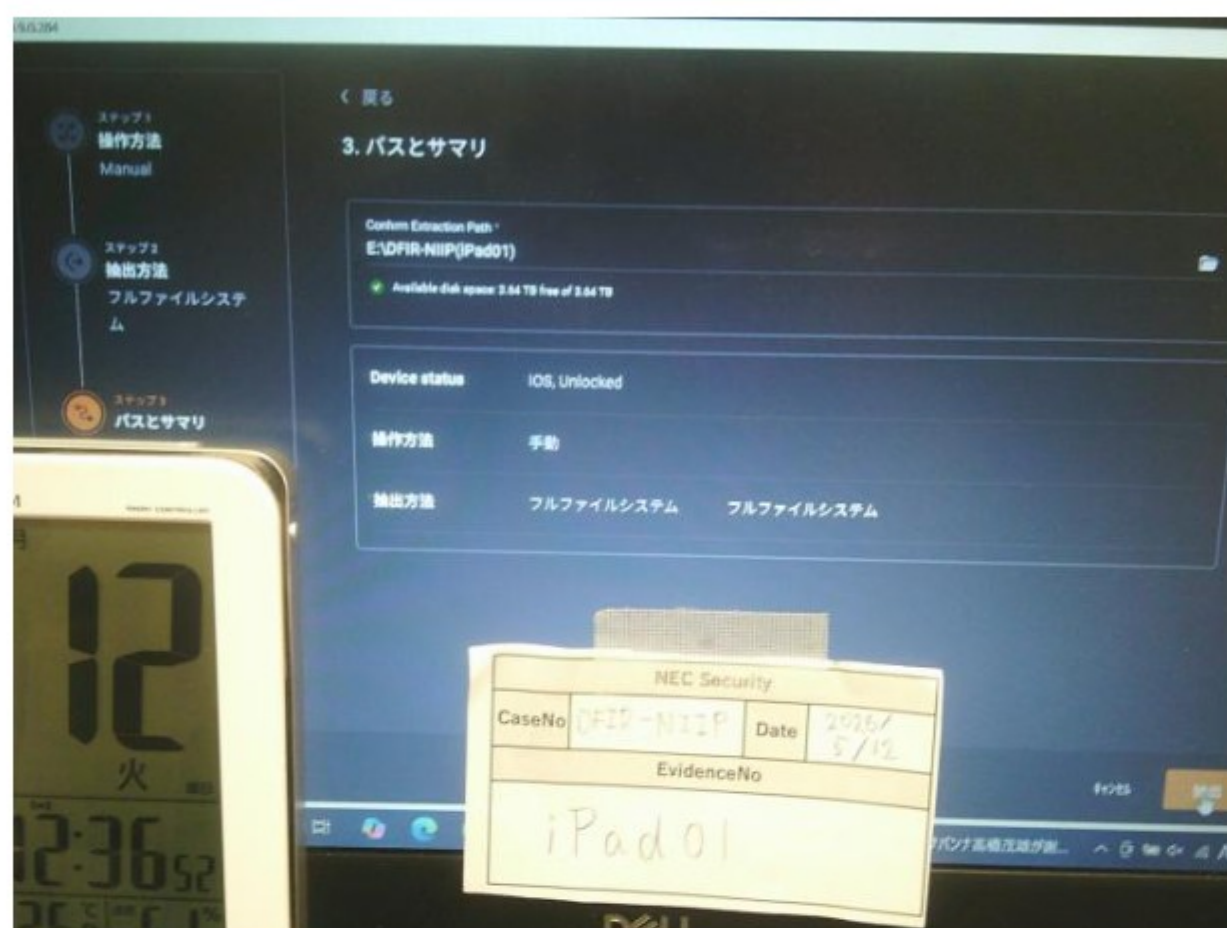
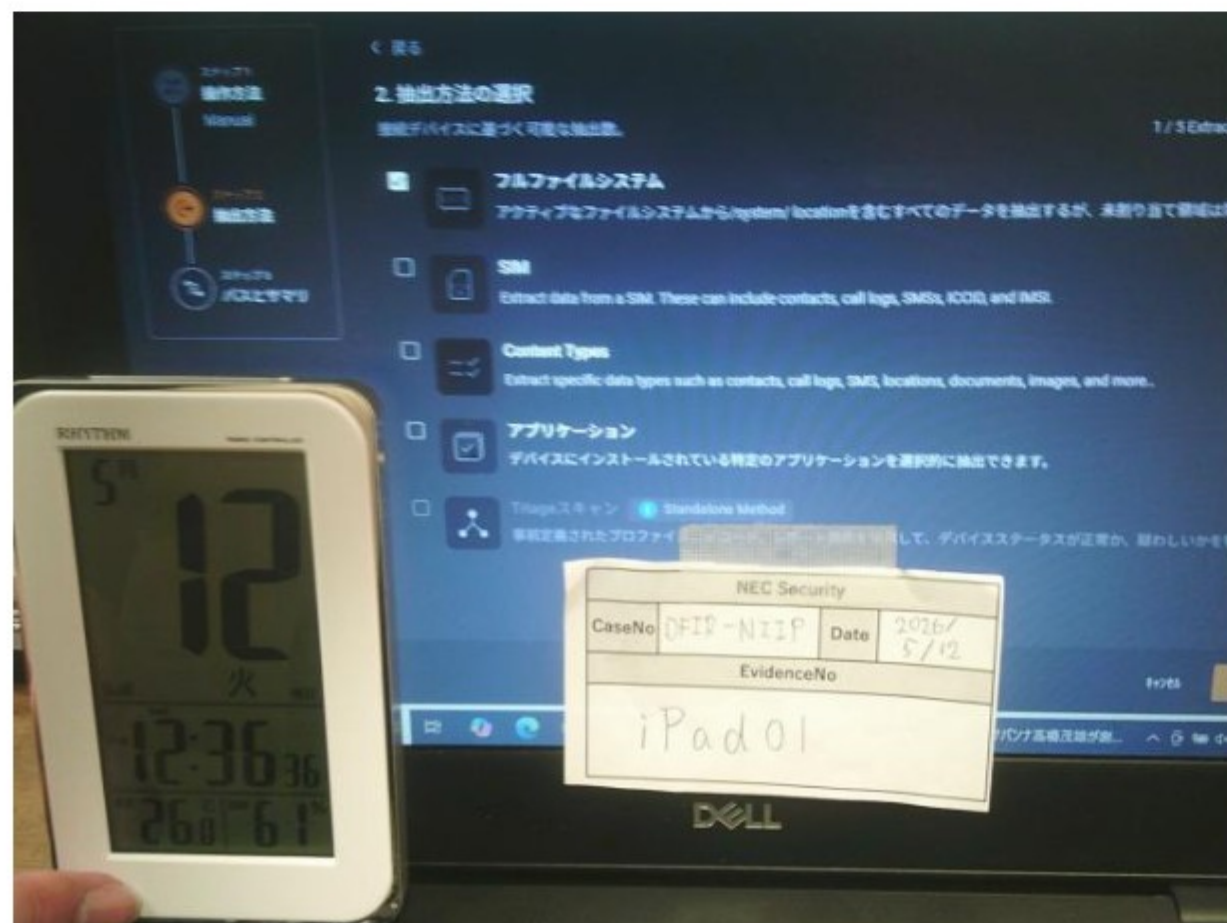


⑤ 保全対象 iPad02 の起動及びシリアル番号の確認 (2026/05/12 10:31:41 実施)



⑥ 保全対象 iPad01 のデータ抽出作業開始 (2026/05/12 12:34:54 ~ 13:06:40 実施)



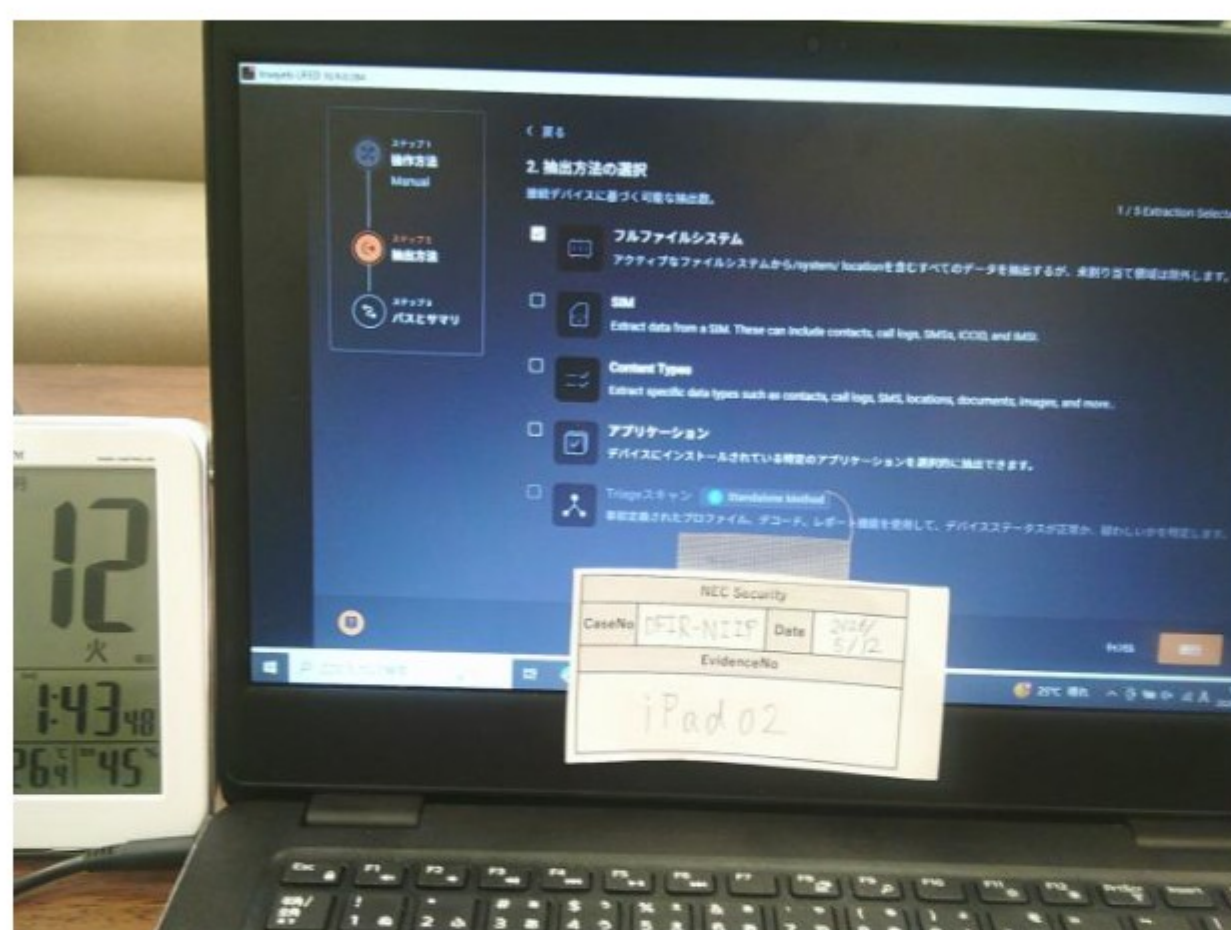
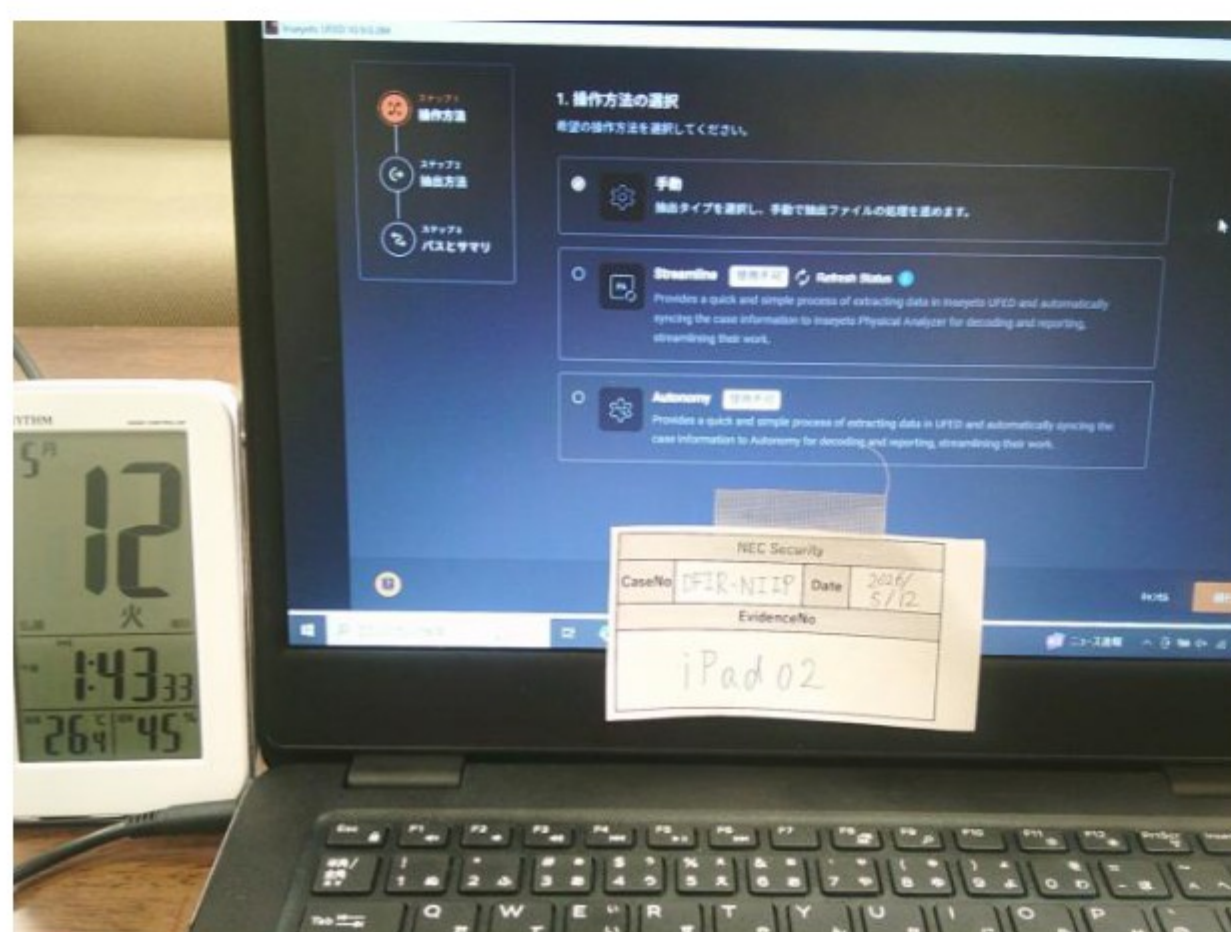


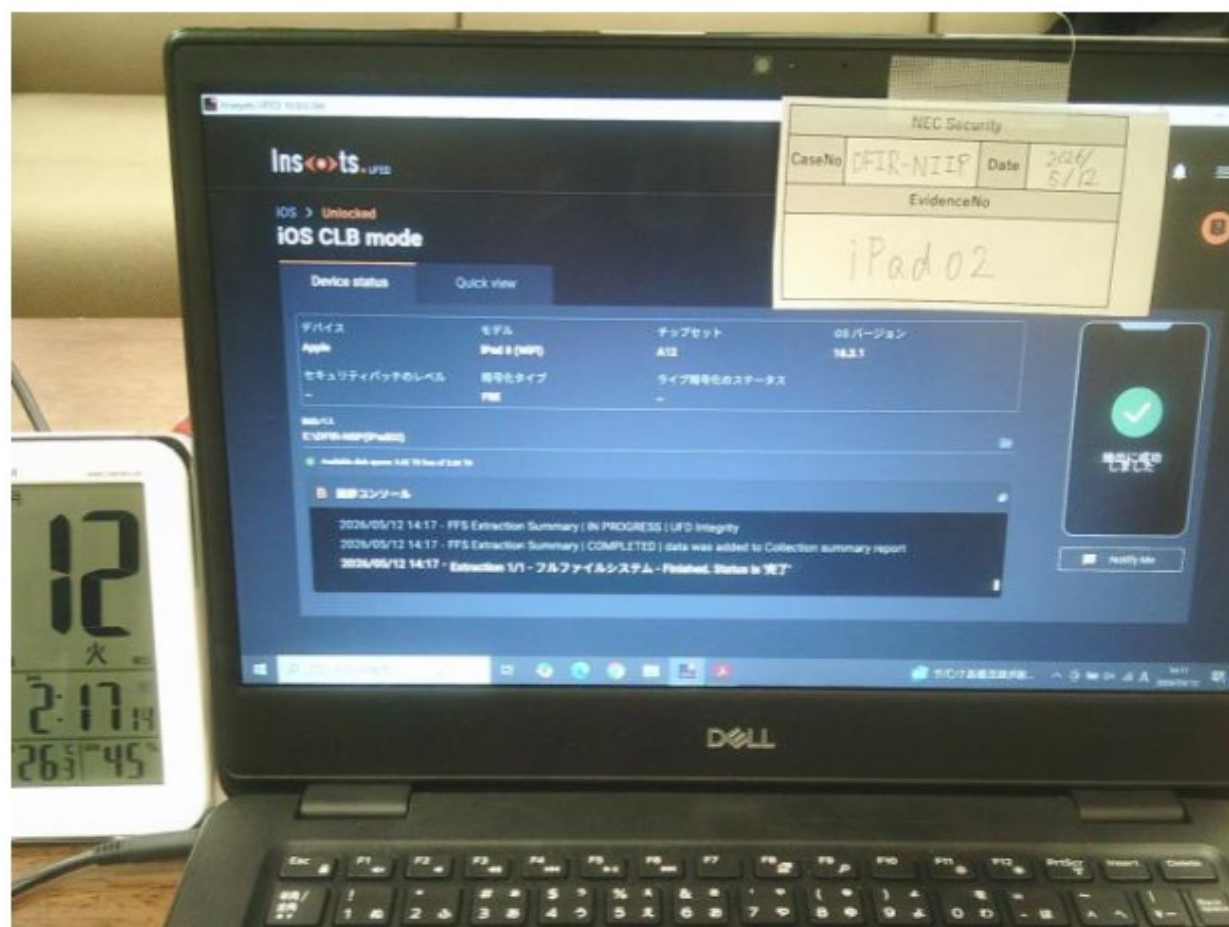
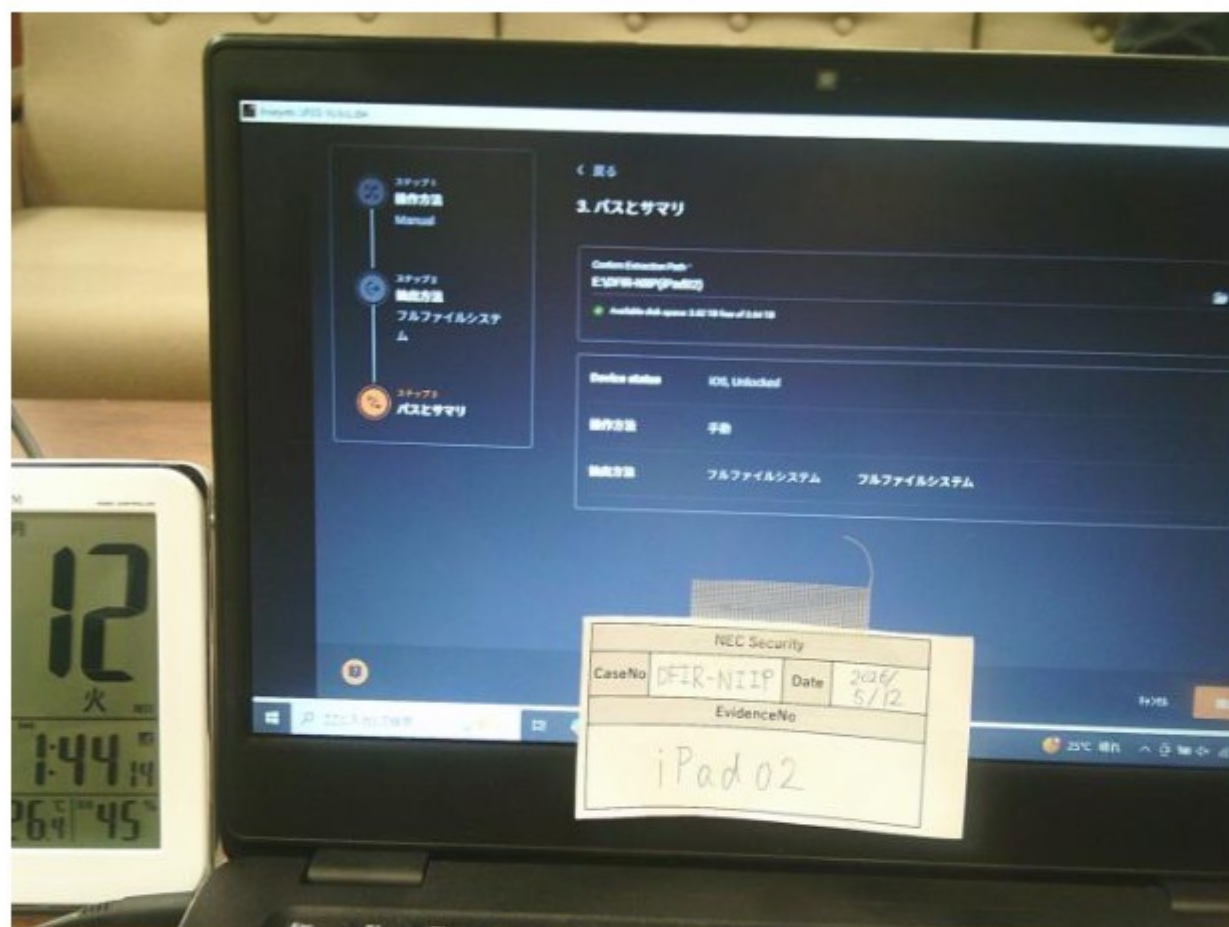


⑦ 保全対象 iPad01 の保全終了 (2026/05/12 13:21:21 実施)



⑧ 保全対象 iPad02 のデータ抽出作業開始 (2026/05/12 13:42:30 ~ 14:17:11 実施)





⑨ 保全対象 iPad02 の保全終了（2026/05/12 14:23:01 実施）



以上