

# デバイス所有者の行動履歴を知りたい

Ver. 1.0



**OXYGEN  
FORENSICS**

## 目次

1	デバイス所有者の行動履歴を知りたい.....	1
1.1	主に利用する機能.....	1

## 1 デバイス所有者の行動履歴を知りたい

解析の説明に使用しているデータの詳細は、当サポートページに掲載の資料「解析を始める前に…」の「1.1 解析に使用しているデータについて」をご覧ください。またこちらの資料はそのデータを元に解析したもので、お客様の環境とは異なります。必要に応じて読みかえていただきますようお願い申し上げます。

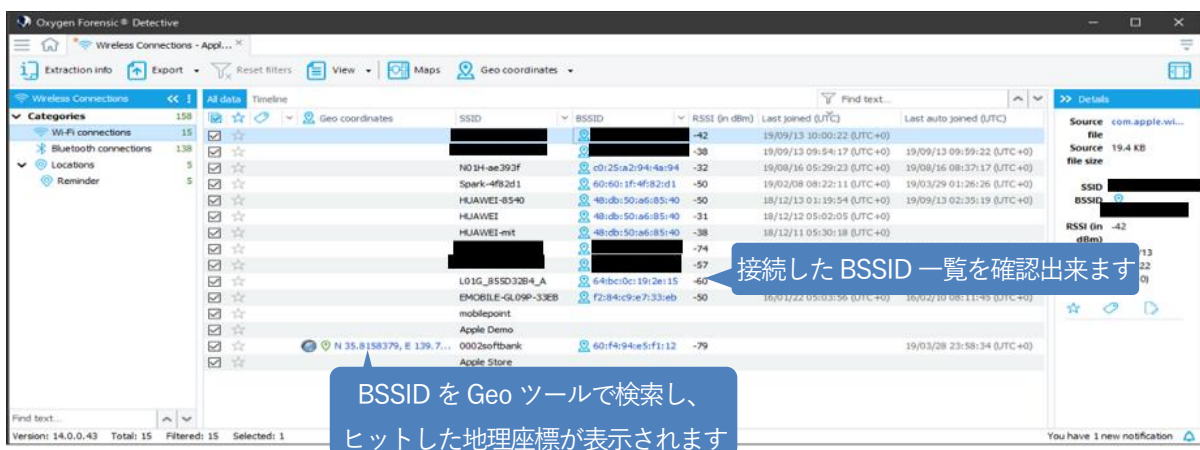
### 1.1 主に利用する機能

デバイス所有者の行動履歴を知りたい時に主に使用する機能は「Wireless Connections」、「Timeline」、「地図系アプリ」、「ヘルスケア系アプリ」、「Calendar」や「OS Artifacts」等です。

#### ➤ Wireless Connections

Wi-Fi 接続や Bluetooth 接続などの接続履歴を知りたい場合は、「Wireless Connections」から確認することができます。

#### ➤ Wireless Connections の解析画面

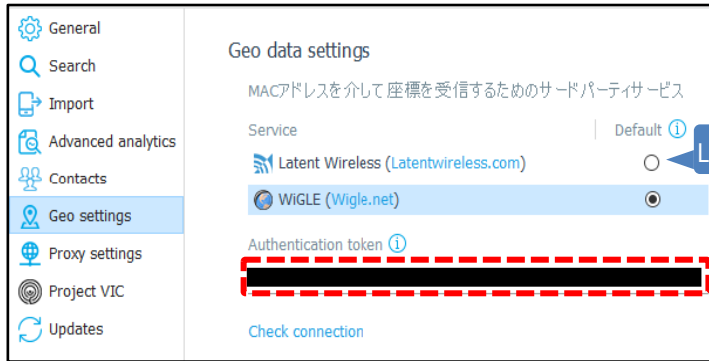


#### 📌 BSSID とは (出典 : <https://e-words.jp/w/BSSID.html>)

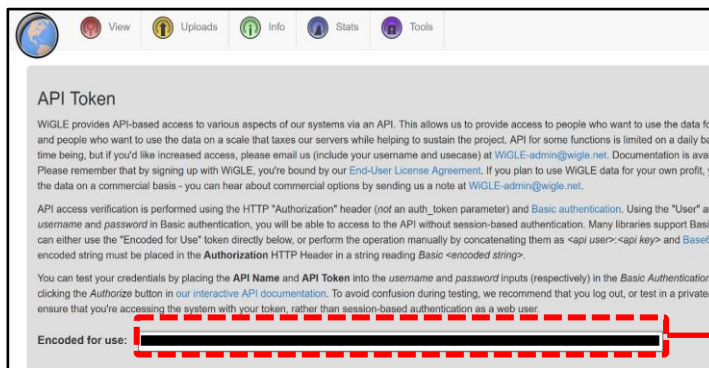
無線 LAN(Wi-Fi)における無線アクセスポイント (AP) および無線ネットワークの識別子の一つで、48 ビットの値。通常はアクセスポイントの MAC アドレスをそのまま用いる。

➤ Detective に WiGLE を設定する

外部サービスである WiGLE を使用することによって、Wi-Fi の接続情報(BSSID)から位置情報を解析することも可能です。Detective の Options メニュー > Geo Settings から設定可能です。



Latent Wireless は日本では使用不可



WiGLEを使用する場合は、Web サイトから会員登録を行ったあと、Authentication key を発行し、Oxygen の Geo data settings に登録する必要があります。

WiGLE の Web サイト

### WiGLE

世界中のさまざまなワイヤレスホットスポットに関する利用者が提供した情報を収集し公開するサービス

### Latent Wireless

Wi-Fi 情報から位置情報を探す海外の法執行機関向けのサービス（日本国内では使用不可）

➤ Timeline

デバイス内のアクティビティが時系列で表示される。

時系列でアクティビティ量の変化を表示

Timeline 解析の対象となった、デバイス内のアプリ一覧

➤ 地図アプリ(Google Map)の解析画面

地理座標とタイムスタンプが確認出来ます。  
地理座標をクリックすると Maps が起動します。

➤ 地図 (Maps) の起動パターン①

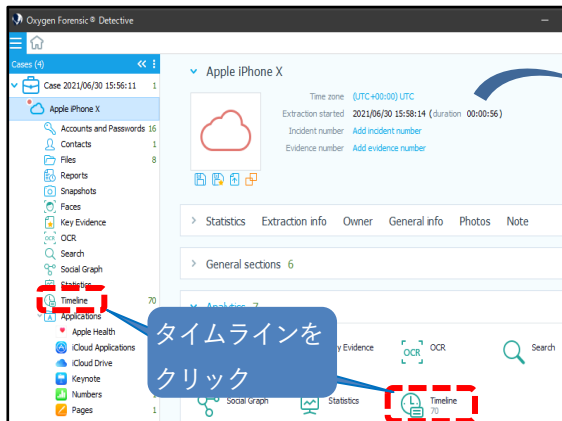
画面右上のボタンをクリックして「menu」を開き、更に「Maps」をクリックします



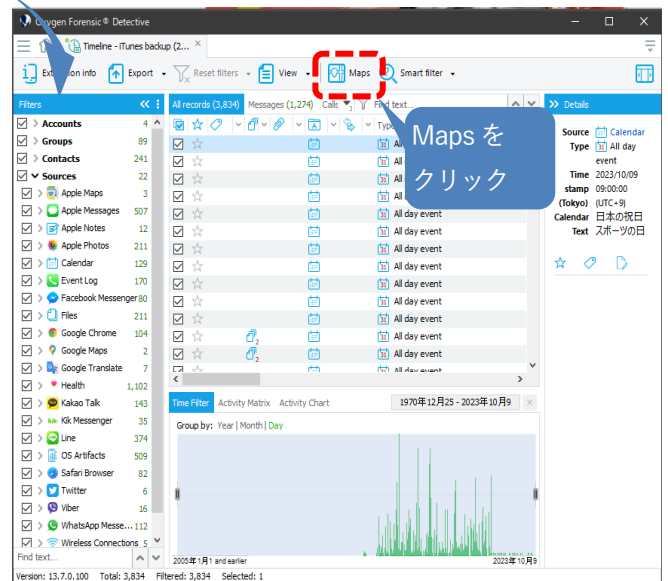
➤ 地図 (Maps) の起動パターン②

タイムライン解析ツール上から「Maps」を選択して起動する。

タイムラインのデータは、位置情報が含まれていた場合、「Maps」機能を使う事で位置情報を地図表示で確認できます。



タイムライン



➤ Places タブ

調査対象が長時間いる場所 (Places) を表示します (例、オフィス、空港、家等)

Places.kml (13 points)

Coordinates	Time stamp
N 35.679345, E 139.773564	26 Aug 2019 08:21:02 UTC+9
N 35.679155, E 139.773533	25 Aug 2019 12:11:02 UTC+9
N 35.679355, E 139.773562	25 Aug 2019 11:11:02 UTC+9
N 35.679745, E 139.773512	25 Aug 2019 11:11:02 UTC+9
N 35.679645, E 139.773513	25 Aug 2019 11:11:02 UTC+9
N 35.679245, E 139.773553	25 Aug 2019 11:11:02 UTC+9
N 35.679845, E 139.773513	25 Aug 2019 11:11:02 UTC+9
N 35.681170, E 139.774430	23 Aug 2019 12:15:02 UTC+9
N 35.682576, E 139.775586	23 Aug 2019 12:09:02 UTC+9
N 35.681932, E 139.772895	23 Aug 2019 12:07:02 UTC+9
N 35.680744, E 139.771583	23 Aug 2019 12:05:02 UTC+9
N 35.679845, E 139.773513	25 Feb 2019 11:11:02 UTC+9
N 35.679845, E 139.773513	25 Feb 2019 11:09:02 UTC+9

① 距離 (m)

●隣接するポイントの「最短の距離 (m)」を入力する  
 入力する距離を長くすれば、より多くのポイントが抽出対象になるが、精度は粗くなる

② 時間 (分)

●「最小の時間 (分)」を入力する  
 ここで指定した分以上の期間がない場合、そのポイントは抽出されない。(同じ場所に長くいないとカウントされない)

Places は、円で表示される

タイムラインがグラフで表示される

- 縦軸 Point 数等
- 横軸 時間軸

Places タブを選択

Places が複数ある場合、ここで切り替えられる

Places のクリア (再表示可能)

➤ Route タブ

調査対象が移動した経路を表示します

Route は、線で表示される

Route タブを選択

タイムラインがグラフで表示される  
・縦軸 Point 数等  
・横軸 時間軸

Route が複数ある場合、ここで切り替えられる

Route のクリア (再表示可能)

Coordinates	Time stamp	Details
N 35.632070, E 139.882407	25 Aug 2019 19:05:52 UTC+9	route
N 35.632940, E 139.882392	25 Aug 2019 12:35:41 UTC+9	route
N 35.633934, E 139.878408	25 Aug 2019 12:28:08 UTC+9	route
N 35.632416, E 139.877796	25 Aug 2019 12:21:11 UTC+9	route
N 35.630908, E 139.880961	25 Aug 2019 12:15:12 UTC+9	route
N 35.632668, E 139.882764	25 Aug 2019 12:09:32 UTC+9	route
N 35.633751, E 139.882270	25 Aug 2019 12:07:01 UTC+9	route

①距離 (m)

●時間的に隣接するポイント間の「最大の距離 (m)」を入力する

②時間 (分)

●隣接するポイント間の「時間 (分)」を入力する



➤ Common locations 機能

2人以上の調査対象が、同じ時間、同じ場所にいたかどうか調べ表示します

Common locations は、円で表示される

Common Location タブを選択  
※2つ以上のデバイスが読み込まれていない場合、このタブは表示されない

タイムラインがグラフで表示される  
・縦軸 Point 数等  
・横軸 時間軸

Common locations が複数ある場合、ここで切り替えられる

PDF 出力(Common locations1 つにつき1ページ)

① 距離 (m)  
●ポイント間の最大の距離をメートルで入力する。

② 時間 (分)  
●ポイント間の最大の時間間隔を分で入力する

➤ ヘルスケア系アプリ

健康やフィットネスに関するデータ：身長、体重、活動量や活動時間などが確認できる

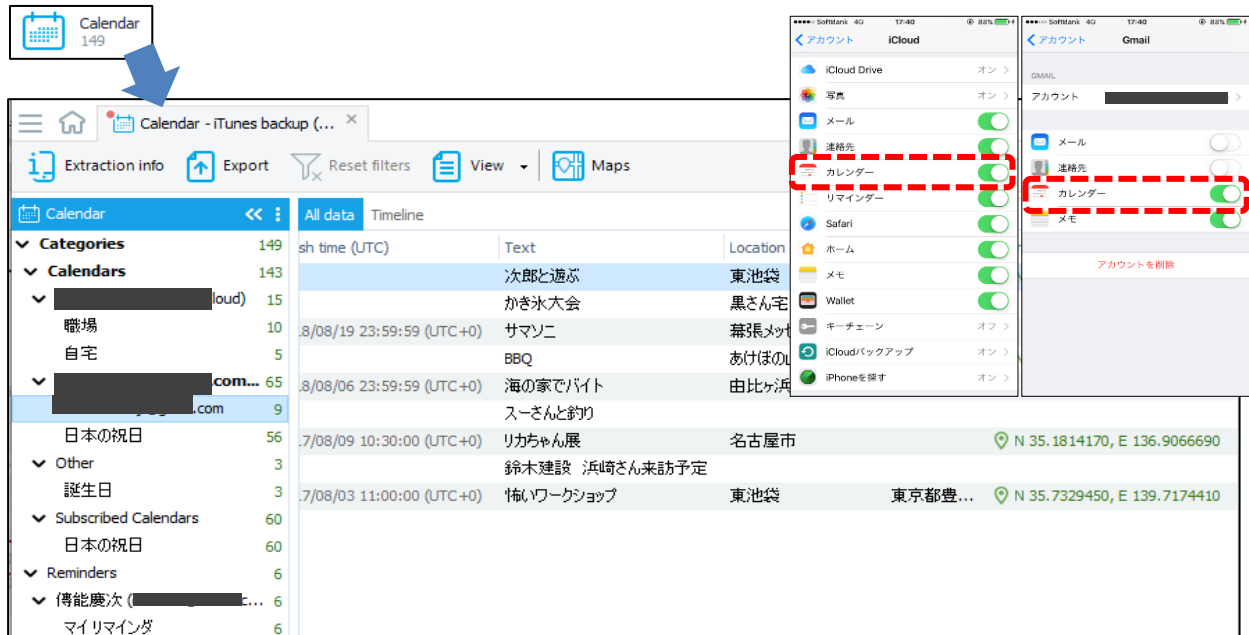
➤ 例：Apple Health の解析画面

歩数や移動距離などから、  
活動量や活動時間が確認出来る

Category	Item	Value	Start time stamp (UTC)	End time stamp (UTC)	Time s...	Created (UTC)	Description	Original value	Source	Was user entered	Source device
Steps	Steps	8	16/04/08 09:13:33 (UTC+0)	16/04/08 09:16:40 (UTC+0)		16/04/08 09:43:44 (UTC+0)			iPhone0,0 (9.3.1)		iPhone0,0 (9.3.1)
	Steps	13	16/05/09 04:49:52 (UTC+0)	16/05/09 04:50:10 (UTC+0)		16/05/09 04:58:39 (UTC+0)			iPhone0,0 (9.3.1)		iPhone0,0 (9.3.1)
	Steps	430	16/05/18 11:30:44 (UTC+0)	16/05/18 11:35:45 (UTC+0)		16/05/18 12:35:15 (UTC+0)			iPhone0,0 (9.3.1)		iPhone0,0 (9.3.1)

## ➤ Calendar

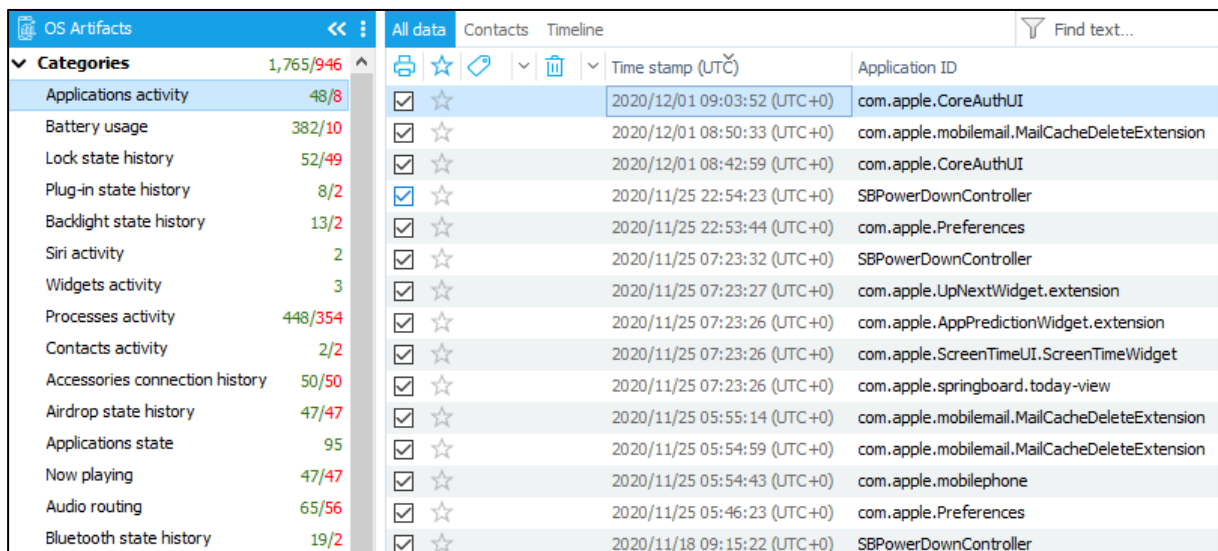
カレンダーを一覧に表示。メールアプリ等を同期している場合は、同期データも表示される。その他、ユーザが登録した予定や位置情報を確認できる。



## ➤ OS Artifact

プロセスアクティビティとコンタクトアクティビティを確認出来る。

物理抽出データの場合は、加えて、アプリケーションアクティビティ、バッテリー使用量、ロック状態履歴、Siriのアクティビティなども確認可能となる。



### 改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2023年3月8日	初版発行