CyberDefense

デバイス所有者の行動履歴を知りたい

Ver. 1.0

目次

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すので、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。

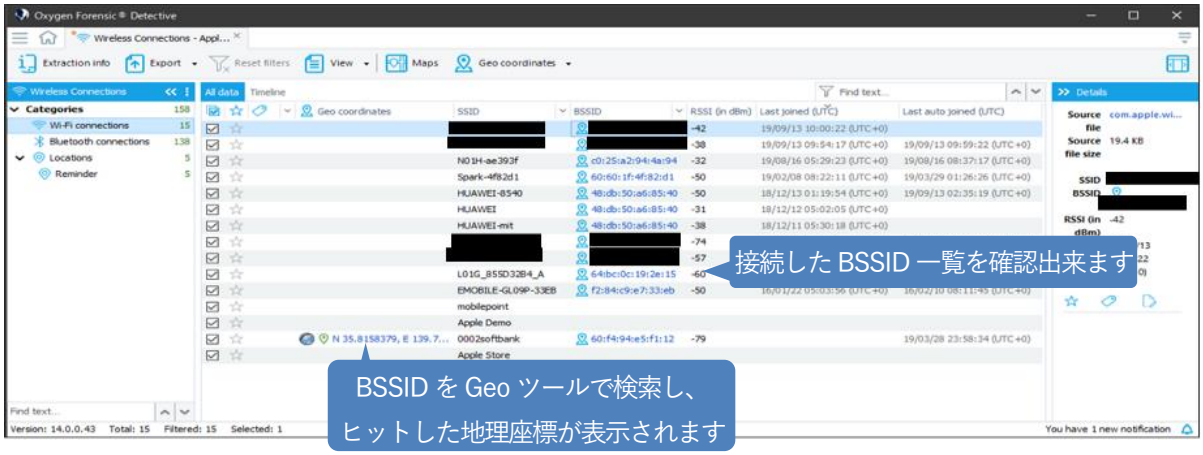
1.1　主に利用する機能

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。

WiGLE の Web サイト

☛ WiGLE

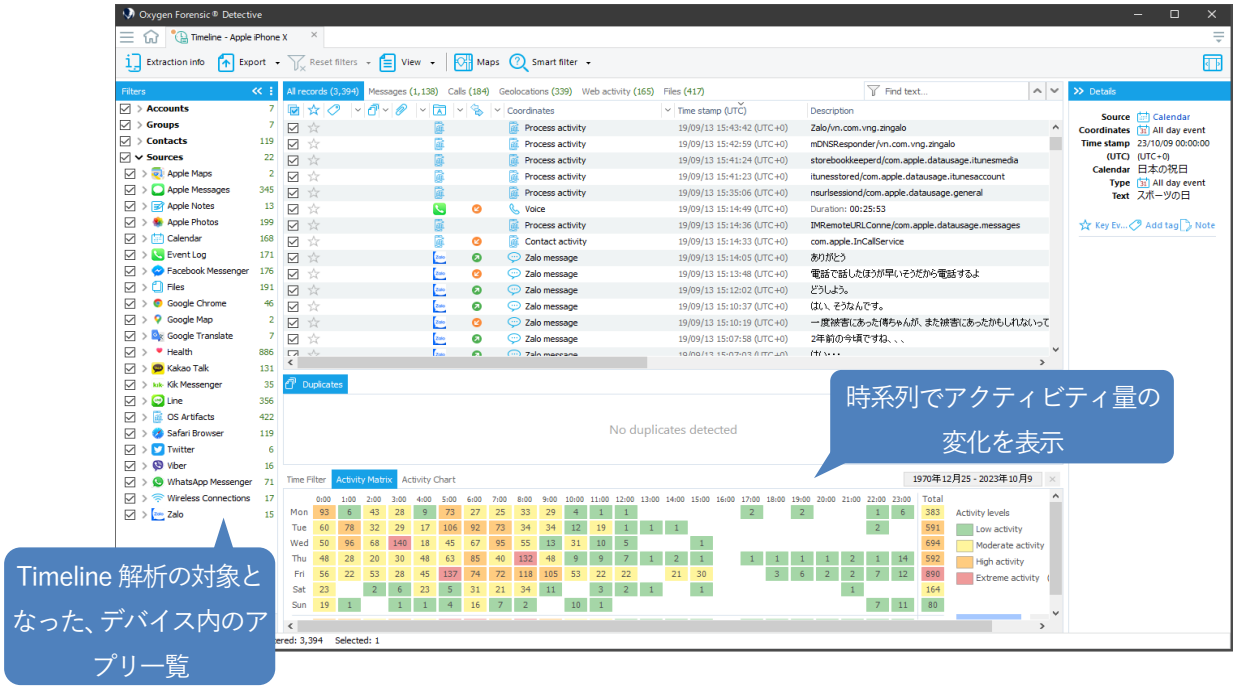
世界中のさまざまなワイヤレスホットスポットに関する利用者が提供した情報を収集し公開するサービス

☛ Latent Wireless

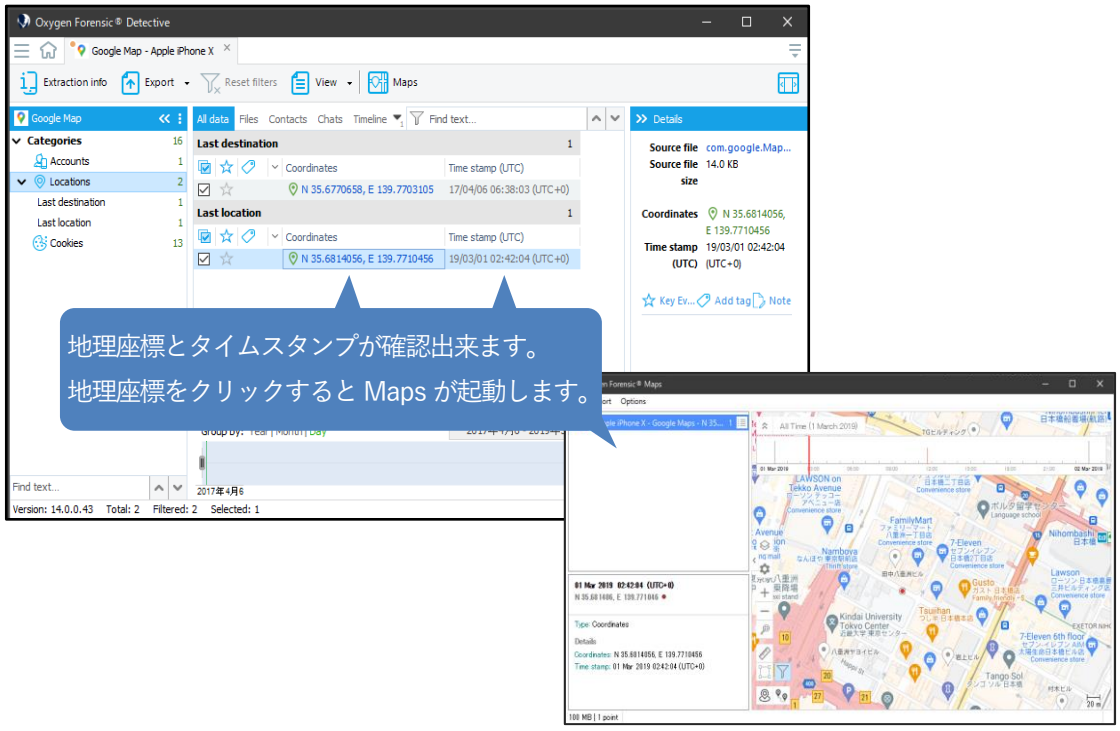
Wi-Fi 情報から位置情報を探す海外の法執行機関向けのサービス（日本国内では使用不可）

➢ Timeline

デバイス内のアクティビティが時系列で表示される。

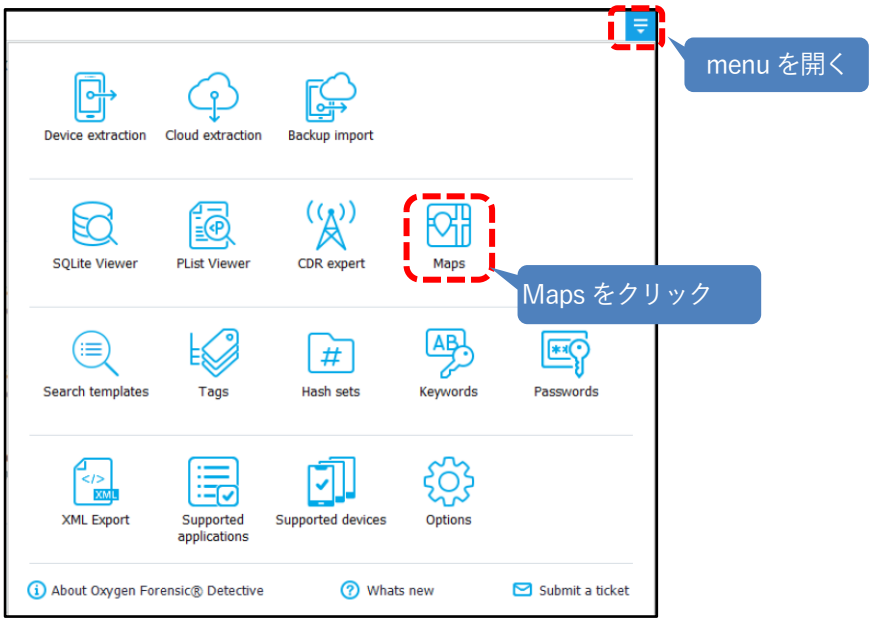


➢ 地図アプリ(Google Map)の解析画面



➢ 地図（Maps）の起動パターン①

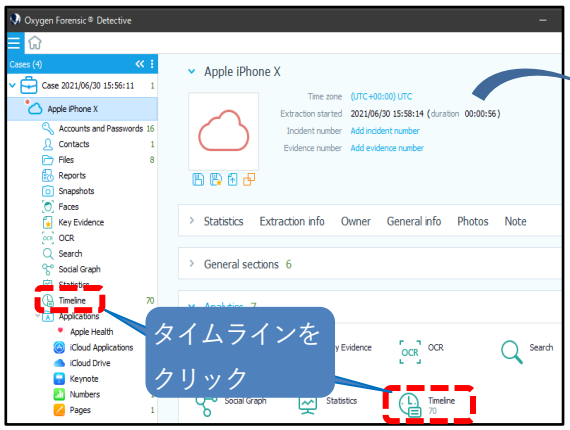
画面右上のボタンをクリックして「menu」を開き、更に「Maps」をクリックします



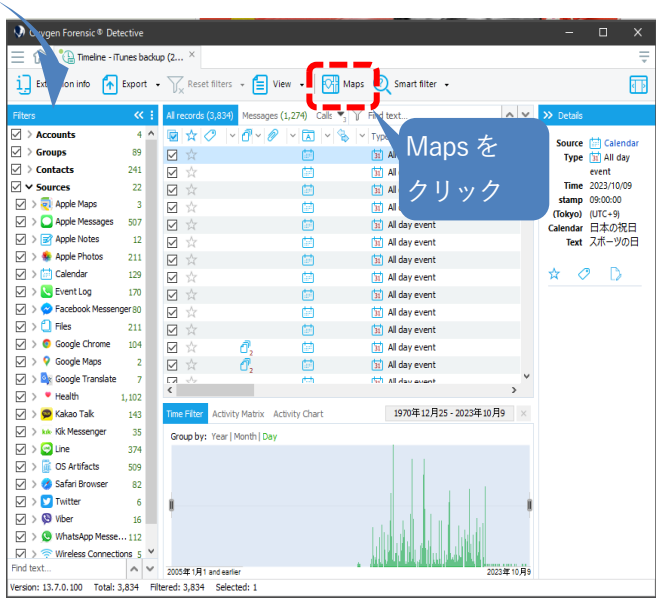
➢ 地図（Maps）の起動パターン②

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）

①距離（m）

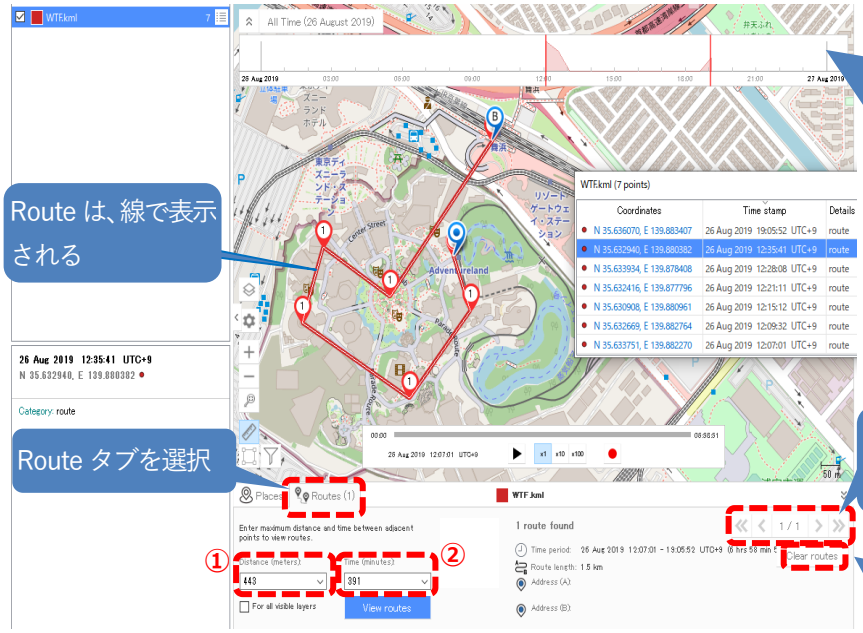
●隣接するポイントの「最短の距離（m）」を入力する
入力する距離を長くすれば、より多くのポイントが抽出対象になるが、精度は粗くなる

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）

➢ Route タブ

調査対象が移動した経路を表示します



①距離（m）

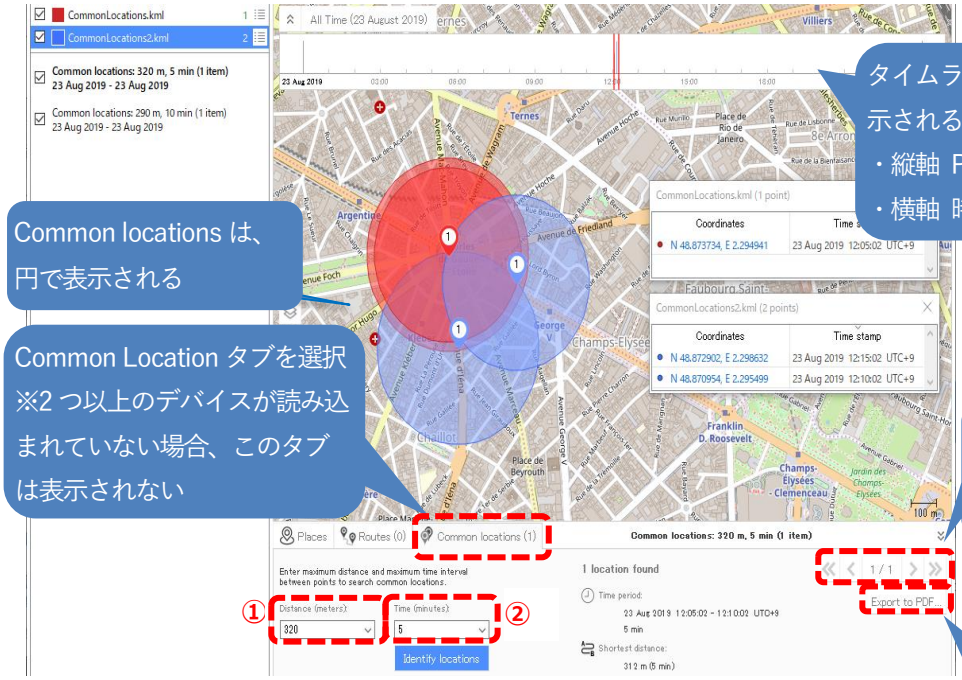
●時間的に隣接するポイント間の「最大の距離（m）」を入力する

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



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 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

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。

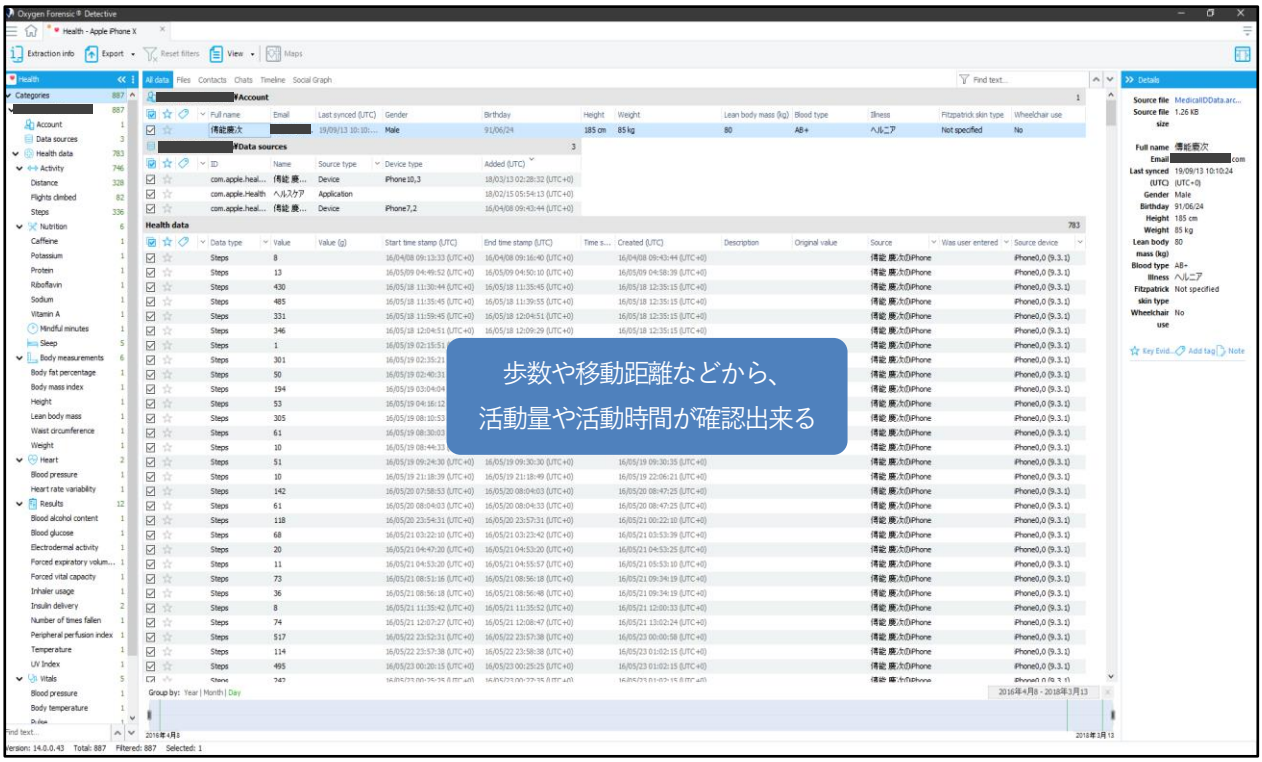
②時間（分）

●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

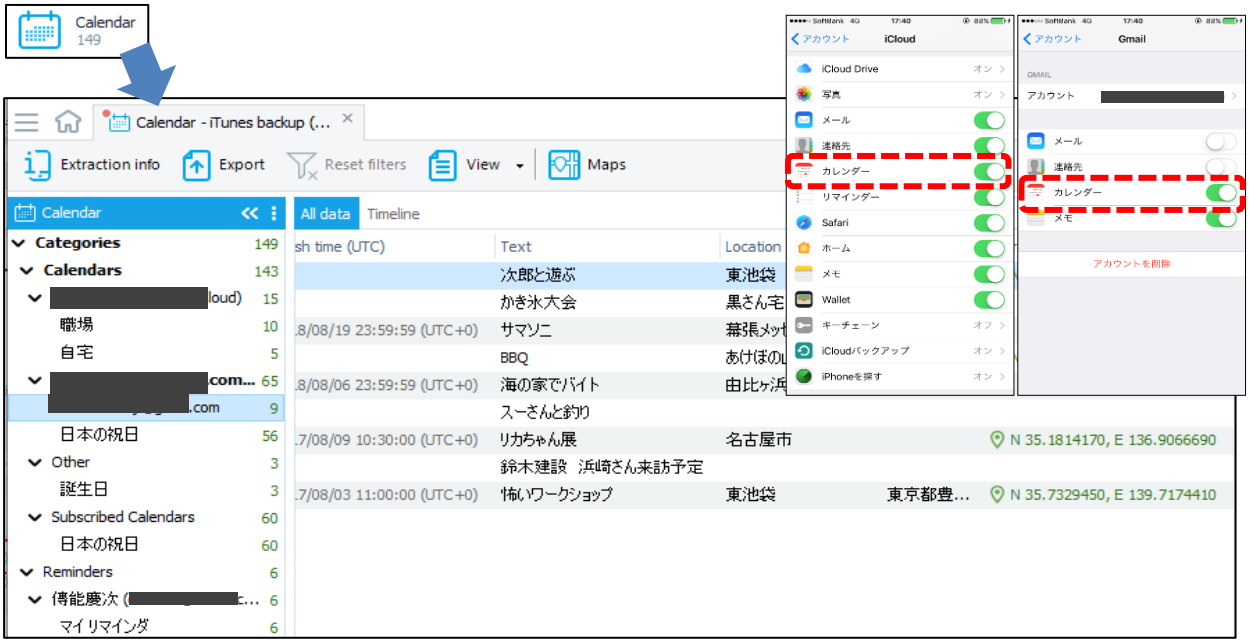
  健康やフィットネスに関するデータ：身長、体重、活動量や活動時間などが確認できる

  - 例：Apple Health の解析画面



➢ Calendar

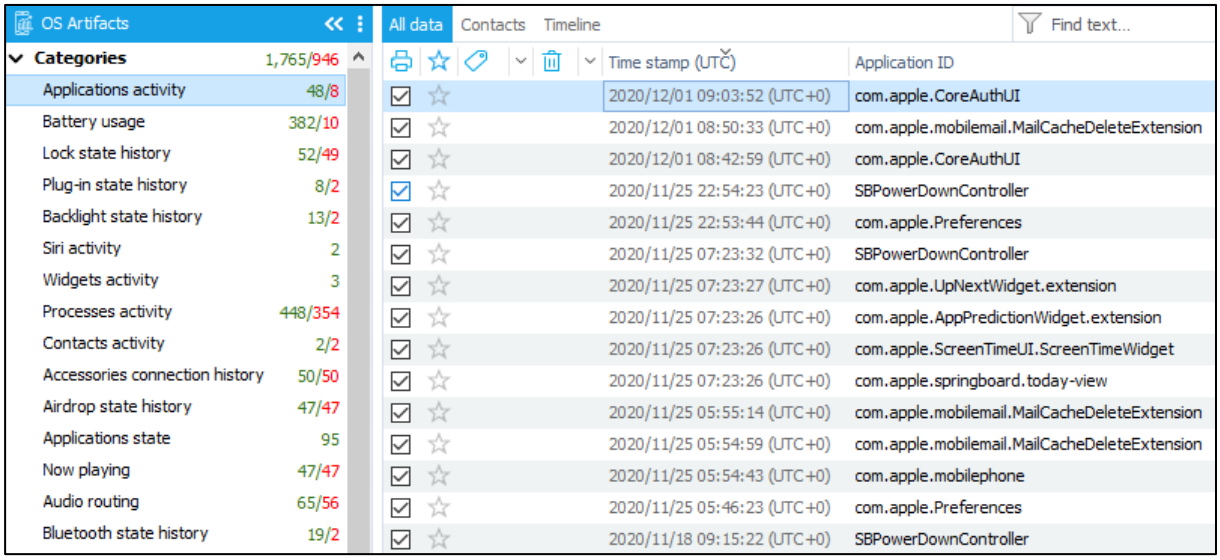
カレンダーを一覧に表示。メールアプリ等を同期している場合は、同期データも表示される。その他、ユーザが登録した予定や位置情報を確認できる。



➢ 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