

Cloud Extractor を用いた 抽出方法

Ver. 1.0



**OXYGEN
FORENSICS**

目次

1	イントロダクション.....	1
1.1	Cloud Extractor を用いた抽出.....	1
2	Cloud 抽出するための条件や認証方法の種類.....	1
2.1	共通した前提条件.....	1
2.2	パターン別.....	1
2.2.1	電話番号 or ユーザ名とパスワード or トークン等.....	1
2.2.2	二段階認証(2FA).....	2
2.2.3	JB 済デバイスが必要な場合.....	3
2.2.4	その他.....	4
3	JB 済デバイスからのクラウドデータ抽出ガイド.....	4
3.1	前提条件.....	4
3.2	OxyAgent を JB 済デバイスにインストールする.....	4
3.3	クラウドサービスからデータを抽出する.....	6
3.4	デバイスから OxyAgent をアンインストールする.....	7

1 インTRODクシヨN

1.1 Cloud Extractor を用いた抽出

Oxygen Forensic Cloud Extractor を用いて抽出できるクラウドサービスは複数あり、現在も増え続けています。そのため、どのクラウドサービスを選択するかによって、抽出するための条件や認証方法がそれぞれ異なります。現時点(2021年6月3日リリース)では、大きく分けて4つのパターンに分類できます。

- 電話番号 or ユーザ名とパスワード or トークン等
- 二段階認証(2FA)
- JB 済+OxyAgent インストールの上、同じネットワークに載せる
- その他 (上記以外のパターン)

2 Cloud 抽出するための条件や認証方法の種類

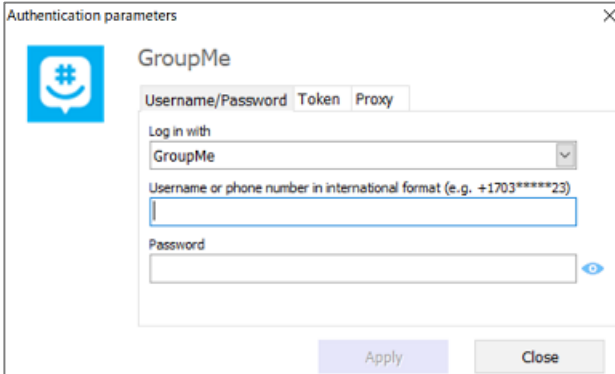
2.1 共通した前提条件

クラウドサービスからデータ抽出を行う場合、クレデンシャル情報が必要です。

2.2 パターン別

2.2.1 電話番号 or ユーザ名とパスワード or トークン等

ユーザ名または電話番号とパスワードを入力して認証する方法です。



Authentication parameters

GroupMe

Username/Password Token Proxy

Log in with
GroupMe

Username or phone number in international format (e.g. +1703****23)

Password

Apply Close

上記図は、例として「GroupMe」の認証要求画面を掲載していますが、他にも以下のサービスが同様の方法でログイン可能です。

GroupMe / Ring / Airbnb / Amazon Shopping / BlaBlaCar / Booking.com / Box / DJI Cloud / Dropbox / Evernote / Facebook / Firefox Brower / Firefox Lockwise / Fitbit / Google Android Cloud Data / Google Bookmarks / Google Calendars / Google Chrome / Google Contacts / Google Drive / Google Fit / Google Home / Google Keep / Google Location History / Google Mail / Google My Activity / Google Photos / Google Tasks / iCloud iTunes Store / Instagram / JioCloud / LINE / Line Google Backup / Line Keep / LinkedIn / Mail(IMAP) / Mi Cloud Data / My Parrot Cloud / OKCupid / OneDrive / Outlook Calendar / Outlook Mail / Outlook People / QQ Mail / Skype / SkyPixel / Slack / Swarm(Foursquare) / Telegram / Telegram Passport / Tinder / Twitter / Uber / Viber Google Backup / VIPole / VKnotokte / WhatsApp Google Backup / Wickr Me / Windows Phone Cloud Data / Zoom

2.2.2 二段階認証(2FA)

- ① ユーザ名または電話番号とパスワードを入力します
- ② ①を入力後、以下の様な画面が表示され、2FAの方法を選択します



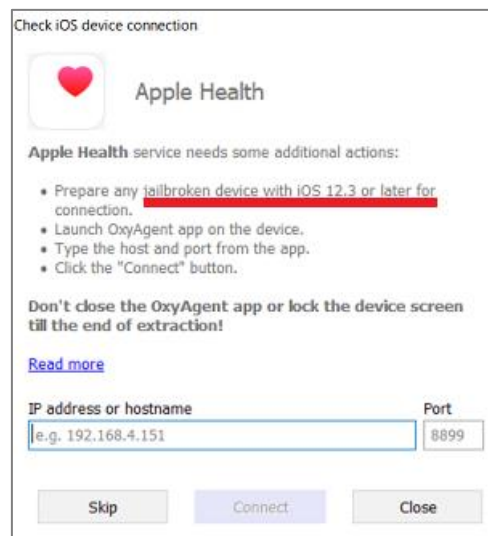
上記図は、例として「WhatsApp Cloud」の2FA 要求画面を掲載していますが、2FA の選択肢はサービスによって異なります。他にも以下のサービスが2FA でログイン可能です。

WhatsApp Cloud (SMS か Phone call) / Amazon Alexa(capture 入力) / Amazon Photos(capture 入力) / Discord(capture 選択) / JioChat(SMS)/ Samsung Cloud Backup(SMS か Backup code か Trusted device) / Samsung Cloud Data(SMS か Backup code か Trusted device) / Samsung Health(SMS か Backup code か Trusted device) / TamTam(SMS) / TikTok(capture パズルのピースをはめる) / Yandex Taxi(SMS)

2.2.3 JB 済デバイスが必要な場合

- ① ユーザ名または電話番号とパスワードを入力します
- ② 入力後、以下の様な画面が表示されます。赤線部分「jailbroken device with iOS12.3 or later」と明記されているので、このサービスからデータ抽出を行う場合はJB 済のデバイスが必要になります。

※ 手順については「3. JB 済デバイスからのクラウドデータ抽出ガイド」をご覧ください



上記図は、例として「Apple Health」への接続画面を掲載していますが、他にも以下のサービスが同様にJB 済デバイスを必要とします。

Apple Health / Apple Maps / iCloud Applications / iCloud Calendars / iCloud Call History / iCloud Contacts
/ iCloud Drive / iCloud Keychain / iCloud Notes / iCloud Photo Stream / iCloud Photos / iCloud Safari
Bookmarks / iCloud Safari History / Viber iCloud Backup / WhatsApp iCloud Backup

2.2.4 その他

以下は上記に当てはまらないサービスであり、より複雑な認証方法が必要となる場合もあり、個々のサービスによって方法はさまざまとなります。例として、2デバイスが必要な場合や、Torの使用が必要な場合などがあります。

Huawei Cloud Backup / iCloud Backup(2デバイス必要) / IMO / SecMail(Torを使用する必要あり) / Viber
Cloud / WhatsApp QR

3 JB済デバイスからのクラウドデータ抽出ガイド

3.1 前提条件

- ・ JB済のデバイスを用意
- ・ OpenSSH 利用可
- ・ iCloud アカウントとパスワードを用意

JBを行う方法は様々あるので、checkra1n (for Mac)や chimera 等のフリーツールを使用して事前にデバイスのJBを行ってください。

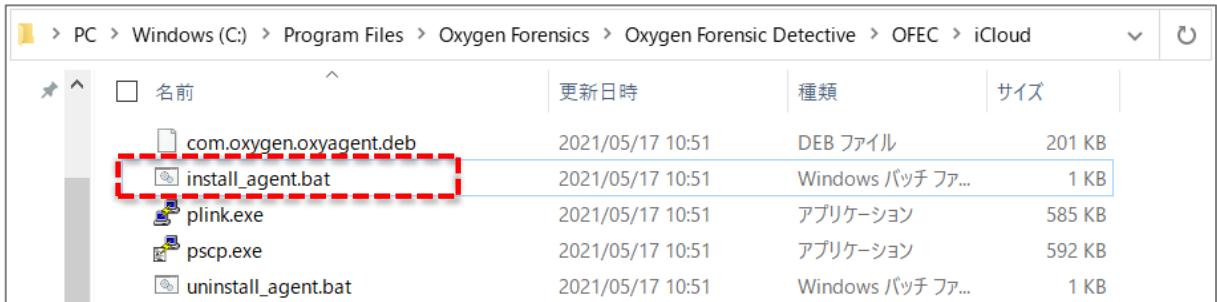
3.2 OxyAgent を JB済デバイスにインストールする

- ① Oxygen Forensic Detective がインストールされている PC とデバイスを同じネットワークに接続する
- ② デバイス側の IP アドレスをメモする

- ③ 「install_agent.bat」をダブルクリックする

インストールプログラムが配置されている場所：

C:\Program Files\Oxygen Forensics\Oxygen Forensic Detective\OFEC\iCloud



- ④ コマンドプロンプトが起動したら、②でメモしたデバイスのIPアドレスを入力します。

この時、パスワードを要求されますが、デフォルトの場合はスキップ（Enterキーを押下）してください

```
C:\WINDOWS\system32\cmd.exe
Please, type the IP address of the iPhone: 192.168.4.209
SSH password (leave blank to use default):
```

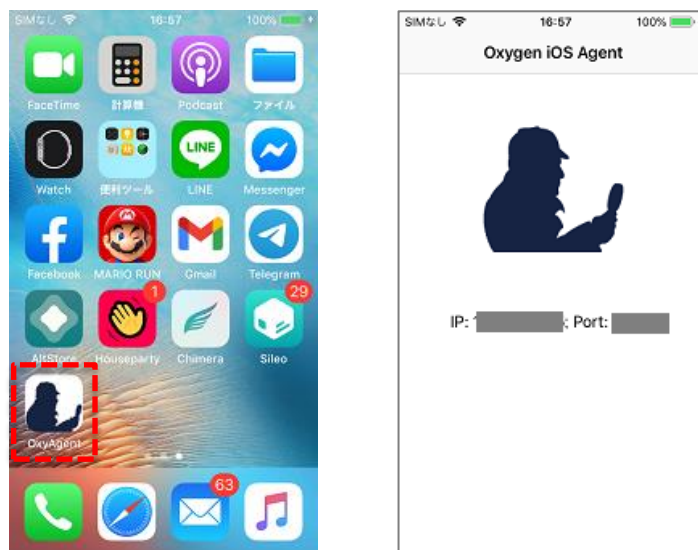
OxyAgent のインストールが完了するまでしばらくお待ちください。

```
C:\WINDOWS\system32\cmd.exe
Please, type the IP address of the iPhone: 192.168.4.209
SSH password (leave blank to use default):
com.oxygen.oxyagent.deb | 193 kB | 193.7 kB/s | ETA: 00:00:00 | 100%
Selecting previously unselected package com.oxygen.oxyagent.
(Reading database ... 1082 files and directories currently installed.)
Preparing to unpack com.oxygen.oxyagent.deb ...
Unpacking com.oxygen.oxyagent (0.0.1-41+debug) ...
Setting up com.oxygen.oxyagent (0.0.1-41+debug) ...
Processing triggers for org.coolstar.sileo (1.1.5) ...

Updating device cache...
Press any key to continue . . .
```

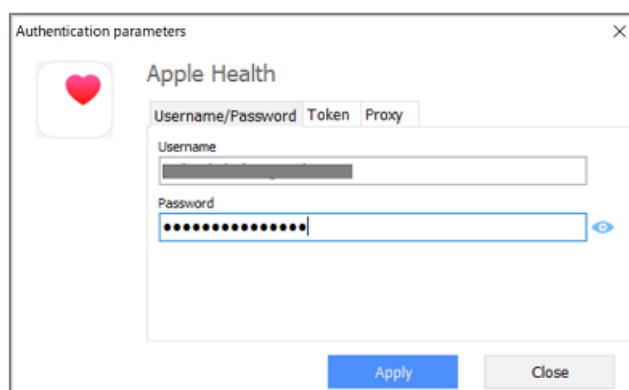
- ⑤ デバイスにインストールしたOxyAgentを起動します。

⚠ OxyAgent 起動中はデバイス画面が常にオンになっている必要があります。




3.3 クラウドサービスからデータを抽出する

- ① ユーザ名とパスワードを入力します



- ② デバイス側の OxyAgent に表示されている IP アドレスとポート番号を記入します

Check iOS device connection



Apple Health

Apple Health service needs some additional actions:

- Prepare any jailbroken device with iOS 12.3 or later for connection.
- Launch OxyAgent app on the device.
- Type the host and port from the app.
- Click the "Connect" button.

Don't close the OxyAgent app or lock the device screen till the end of extraction!

[Read more](#)

IP address or hostname Port

Skip
Connect
Close

接続が完了すると、緑の文字が表示されます。

[Read more](#)

IP address or hostname Port

Skip
Connect
Close

✓

The connection was established successfully! This window will be closed in 3...

3.4 デバイスから OxyAgent をアンインストールする

- ① 「uninstall_agent.bat」をダブルクリックし、IPアドレスを入力し、OxyAgentのアンインストールが完了するまで待つ。

改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2021年6月25日	初版発行