|  |
| --- |
|  |
| **操作チュートリアル**  **端末管理** |
|  |

|  |
| --- |
| 第2版  2020/10/29 |

目次

[1. 概要 1](#_Toc54869012)

[2. アクセス可能端末設定 2](#_Toc54869013)

[2.1. システム全体のアクセス可能端末設定 2](#_Toc54869014)

[2.2. プライマリグループのアクセス可能端末設定(Enterprise Editionのみ) 5](#_Toc54869015)

[2.3. ユーザーのアクセス可能端末設定 9](#_Toc54869016)

[3. 端末管理 13](#_Toc54869017)

[3.1. 端末管理一覧 13](#_Toc54869018)

[3.2. エクスポート 14](#_Toc54869019)

[3.3. アクティベート 15](#_Toc54869020)

[3.3.1. アクティベートの停止 15](#_Toc54869021)

[3.3.2. アクティベートの再開 16](#_Toc54869022)

[3.3.3. アクティベートの削除 17](#_Toc54869023)

[3.4. リモート消去 19](#_Toc54869024)

[3.4.1. リモート消去指示 19](#_Toc54869025)

[3.4.2. リモート消去指示の取消 22](#_Toc54869026)

# 概要

Proselfの端末管理機能を利用すると、ProselfのWindowsアプリ/iOSアプリ/Androidアプリ(※)を使用してProselfにアクセスした端末を管理することができます。また、管理対象となった端末に対しては、停止/再開/削除といったアクティベート機能のほかリモート消去機能を利用することができます。

本資料では管理者ユーザーによる端末管理機能の使用方法について記載しております。

* ProselfのWindowsアプリ/iOSアプリ/Androidアプリとは以下を指します。なお、本チュートリアルでは以降「クライアントアプリ」と呼称します。
* Windowsアプリ

「Proself Client」及び、「同期ツール」を指します。

* iOSアプリ

iPhone/iPad向けのアプリ「Proself Client for iOS」を指します。

* Androidアプリ

Android向けのアプリ「Proself Client for Android」を指します。

# アクセス可能端末設定

本設定を行うことで、ユーザーがクライアントアプリでProselfへのログインが成功するとアクティベートが行われ、クライアントアプリに設定された端末IDがProselfに登録されます。登録された端末IDについては端末管理機能より管理することができます。

※端末管理機能の詳細については「[3.端末管理](#_端末管理)」を参照してください。

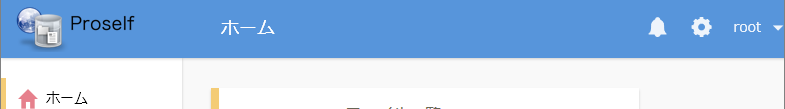
また、本設定によりクライアントアプリ経由でアクセスできる端末の数を絞ることができます。登録された端末IDが指定した台数を超える場合は、新たな端末からクライアントアプリ経由でProselfにログインすることができなくなります。

アクセス可能端末の設定は、システム全体、プライマリグループ(Enterprise Editionのみ)、ユーザーに対して行うことができ、優先度はユーザー > プライマリグループ > システム全体の順で判定されます。

## システム全体のアクセス可能端末設定

システム全体のアクセス可能端末を設定することが可能です。ユーザーやプライマリグループ個別に設定を行っていない限り、本節での設定内容が全てのユーザーに対して適用されます。

ログイン後のホーム画面右上にある歯車のアイコンをクリックし、管理画面に移動します。



**ホーム画面**

管理画面の左メニューよりシステム設定 - セキュリティ - アクセス制限の設定の順に画面を移動して、クライアントアクセス制限設定の「設定」をクリックします。



**管理画面**



**システム設定**



**システム設定 - セキュリティ**



**システム設定 - セキュリティ - アクセス制限の設定**

クライアントアクセス制限設定画面上で、端末管理を行うクライアント種別と端末認証にチェックを入れ、端末認証を行う台数を指定します。



**クライアントアクセス制限設定**

上の画面例の場合、Proselfで端末認証され端末管理対象となるアプリはWindowsアプリ(Proself Clientが1台)、iOSアプリが2台、Androidアプリが3台となります。

* 1ユーザーあたりの台数となります。

「設定」ボタンをクリックすることで設定内容が反映されます。

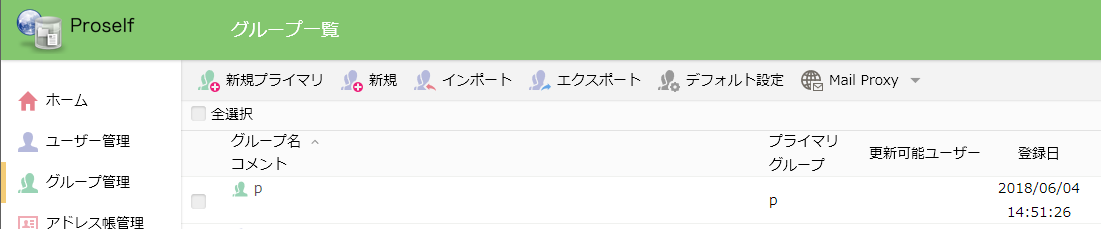
## プライマリグループのアクセス可能端末設定(Enterprise Editionのみ)

プライマリグループに所属するユーザー共通のアクセス可能端末を設定することが可能です。

なお、ここでの設定内容は「[2.1.システム全体のアクセス可能端末設定](#_システム全体のアクセス可能端末設定)」よりも優先されます。

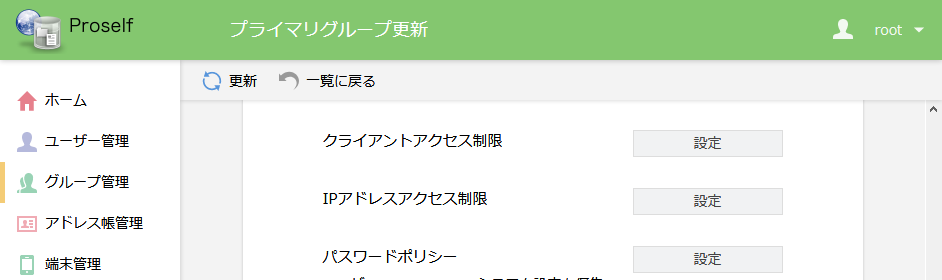
本節では例として作成済みのプライマリグループに対して設定する手順を記載しております。

管理画面の左メニューより「グループ管理」へ移動し、プライマリグループ名をクリックします。



**グループ一覧**

「クライアントアクセス制限」の「設定」をクリックします。



**プライマリグループ更新画面**

クライアントアクセス制限設定画面を表示すると、各項目がグレーアウトされております。



**クライアントアクセス制限設定**

「クライアント種別許可を設定」および「端末認証を設定」のチェックをONにするとクライアント種別や端末認証が設定可能な状態になりますので、端末管理を行うクライアント種別と端末認証にチェックを入れ、端末認証を行う台数を指定します。



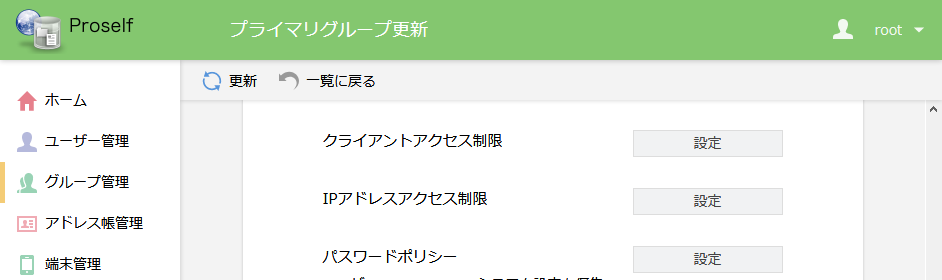
**クライアントアクセス制限設定**

上の画面例の場合、Proselfで端末認証され端末管理対象となるアプリはiOSアプリが1台、Androidアプリが1台となります。

* 1ユーザーあたりの台数となります。

設定後は画面上部の「戻る」をクリックします。

戻った画面で上部の「更新」ボタンをクリックすることで設定内容が反映されます。



**プライマリグループ更新画面**

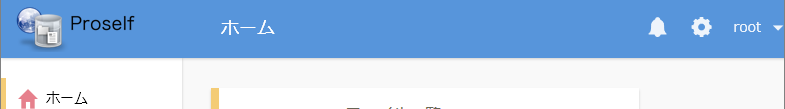
## ユーザーのアクセス可能端末設定

ユーザー個別にアクセス可能端末を設定することが可能です。

なお、ここでの設定内容は「[2.1.システム全体のアクセス可能端末設定](#_システム全体のアクセス可能端末設定)」「[2.2.プライマリグループのアクセス可能端末設定(Enterprise Editionのみ)](#_ユーザーのアクセス可能端末設定)」よりも優先されます。

本節では例として作成済みのユーザーに対して設定する手順を記載しております。

ログイン後のホーム画面右上にある歯車のアイコンをクリックし、管理画面に移動します。



**ホーム画面**

管理画面の左メニューより「ユーザー管理」へ移動し、ユーザー名をクリックします。



**ユーザー一覧**

「クライアントアクセス制限」の「設定」をクリックします。



**ユーザー更新画面**

クライアントアクセス制限設定画面を表示すると、各項目がグレーアウトされております。



**クライアントアクセス制限設定**

「クライアント種別許可を設定」および「端末認証を設定」のチェックをONにするとクライアント種別や端末認証が設定可能な状態になりますので、端末管理を行うクライアント種別と端末認証にチェックを入れ、端末認証を行う台数を指定します。



**クライアントアクセス制限設定**

上の画面例の場合、Proselfで端末認証され端末管理対象となるアプリはWindowsアプリ(Proself Clientおよび同期ツール)が3台となります。

* 1ユーザーあたりの台数となります。

設定後は画面上部の「戻る」をクリックします。

戻った画面で上部の「更新」ボタンをクリックすることで設定内容が反映されます。



**ユーザー更新画面**

# 端末管理

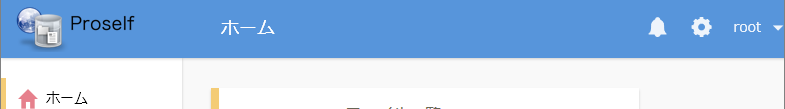
クライアントアプリ経由でProselfにアクセスする端末を管理することができます。

本機能を利用するには、「[2.1.システム全体のアクセス可能端末設定](#_システム全体のアクセス可能端末設定)」「[2.2.プライマリグループのアクセス可能端末設定(Enterprise Editionのみ)](#_ユーザーのアクセス可能端末設定)」「[2.3.ユーザーのアクセス可能端末設定](#_ユーザーのアクセス可能端末設定_1)」で、クライアント種別(Windowsアプリ、iOSアプリ、Androidアプリ)の端末認証にチェックを入れ、台数を設定する必要があります。

## 端末管理一覧

アクティベートされた端末の一覧が表示されます。本画面上より対象端末のアクティベート停止、再開、リモート消去処理を行うことができます。

ログイン後のホーム画面右上にある歯車のアイコンをクリックし、管理画面に移動します。



**ホーム画面**

管理画面の左メニューより「端末管理」をクリックします。



**管理画面**

端末管理一覧画面が表示されます。



**端末管理一覧**

## エクスポート

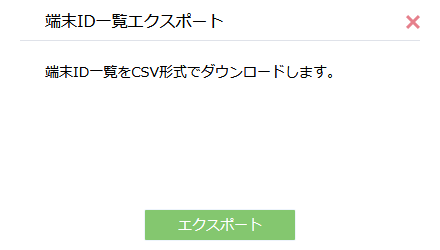
登録されている端末の一覧をCSV形式でエクスポートすることができます。

上部メニューの「エクスポート」をクリックします。



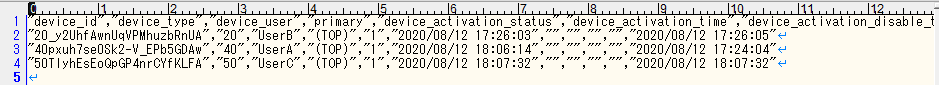
**端末管理一覧**

ダイアログが表示されますので「エクスポート」をクリックします。



**エクスポート確認ダイアログ**

エクスポートしたファイルがダウンロードされます。ファイルをテキストエディタ等で開くと端末の一覧情報を確認することができます。



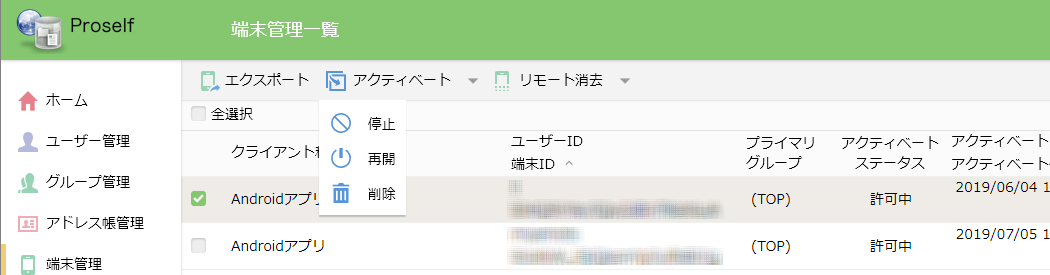
## アクティベート

端末に対してアクティベートの停止、再開、削除を行うことができます。詳細については以降に記載しております。

### アクティベートの停止

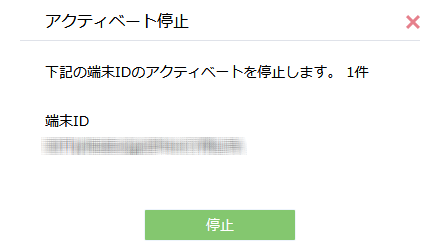
選択した端末のアクティベートを停止することができます。停止された端末からはクライアントアプリ経由でProselfにログインすることができなくなります。

アクティベートを停止したい端末にチェックを入れると「アクティベート」メニューが表示されます。このメニュー内より「停止」をクリックします。



**端末管理一覧**

アクティベート停止確認ダイアログが表示されますので、「停止」をクリックします。処理を取り消す場合は右上の「×」をクリックします。



**アクティベート停止確認ダイアログ**

停止された端末については端末管理一覧上のアクティベートステータス列に「停止中」と表示され、アクティベート停止日時列に停止された日時が表示されます。



**端末管理一覧**

### アクティベートの再開

「[3.3.1.アクティベートの停止](#_アクティベートの停止)」で停止された端末を再開することができます。

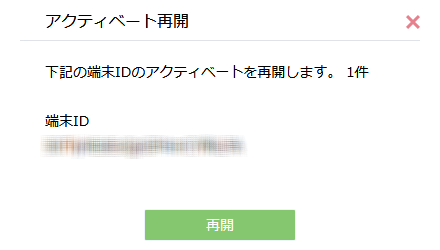
再開すると対象端末上のクライアントアプリからのProselfへのログインが再び可能となります。

アクティベートステータスが「停止中」の端末にチェックを入れると「アクティベート」メニューが表示されます。このメニュー内より「再開」をクリックします。



**端末管理一覧**

アクティベート再開確認ダイアログが表示されますので、「再開」をクリックします。処理を取り消す場合は右上の「×」をクリックします。



**アクティベート再開確認ダイアログ**

再開された端末については端末管理一覧上のアクティベートステータス列に「許可中」と表示され、アクティベート日時列に再開された日時が表示されます。

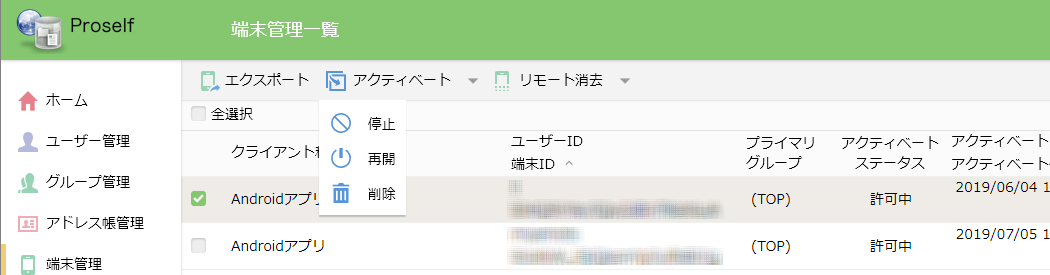


**端末管理一覧**

### アクティベートの削除

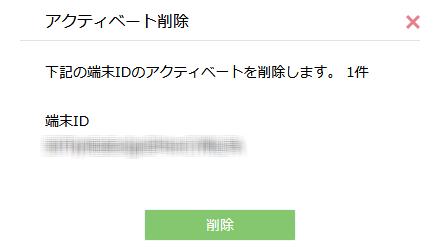
端末管理一覧に登録された端末を削除して管理対象から外します。

アクティベートを削除したい端末にチェックを入れると「アクティベート」メニューが表示されます。このメニュー内より「削除」をクリックします。



**端末管理一覧**

アクティベート削除確認ダイアログが表示されますので、「削除」をクリックします。処理を取り消す場合は右上の「×」をクリックします。



**アクティベート削除確認ダイアログ**

該当の端末が端末管理一覧上から消えていることが確認できます。



**端末管理一覧**

## リモート消去

端末に対してリモート消去指示や消去指示の取消を行うことができます。詳細については以降に記載しております。

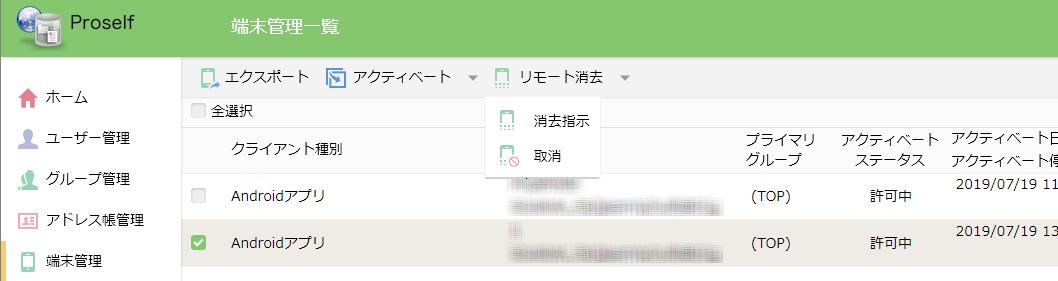
### リモート消去指示

端末にインストールされているクライアントアプリに対し、登録されている接続先と端末に保存されたファイルの消去指示を行います。

クライアントアプリをインストールしている端末を紛失した場合などにご利用ください。

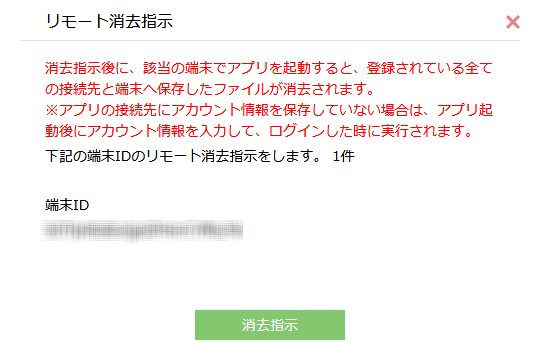
* クライアント種別が「iOSアプリ」「Androidアプリ」の端末に対してのみリモート消去指示を行うことができます。

リモート消去指示を行う端末にチェックを入れると「リモート消去」メニューが表示されます。このメニュー内より「消去指示」をクリックします。



**端末管理一覧**

リモート消去指示削除確認ダイアログが表示されますので、「消去指示」をクリックします。処理を取り消す場合は右上の「×」をクリックします。



**リモート消去指示確認ダイアログ**

リモート消去指示された端末については、端末管理一覧上のリモート消去ステータス列に「指示中」と表示されます。また、リモート消去指示日時列には指示を実行した日時が表示されます。

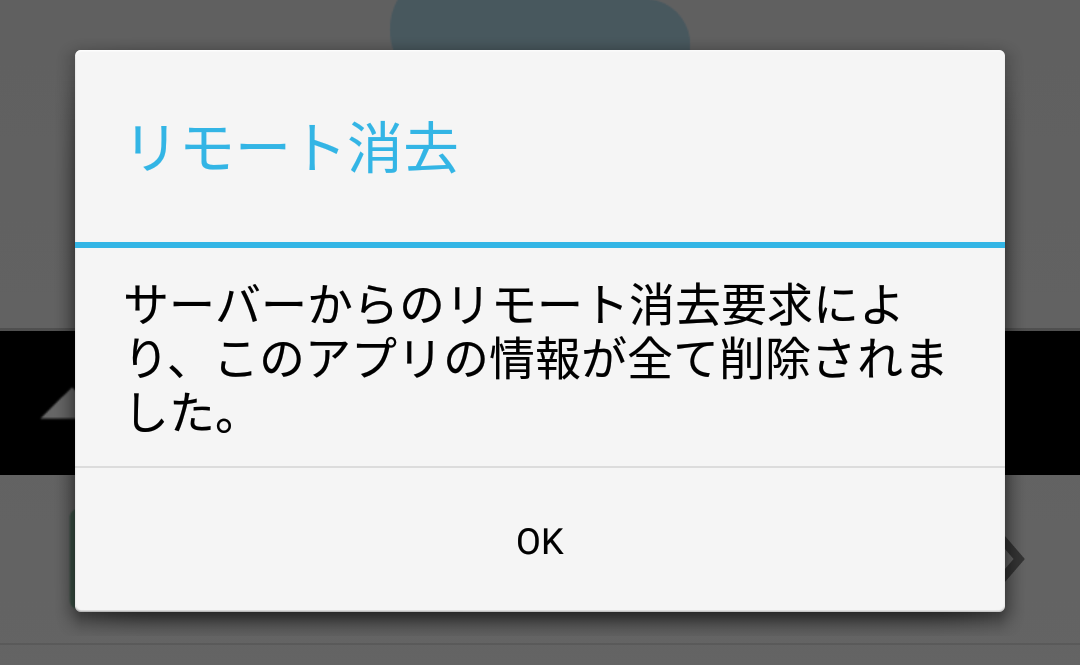


**端末管理一覧**

リモート消去指示を受けた端末のクライアントアプリを起動すると、リモートで消去された旨のメッセージが表示されます。なお、リモート消去実施時はiOSアプリ/Androidアプリで削除対象が異なります。

**Androidアプリの場合**

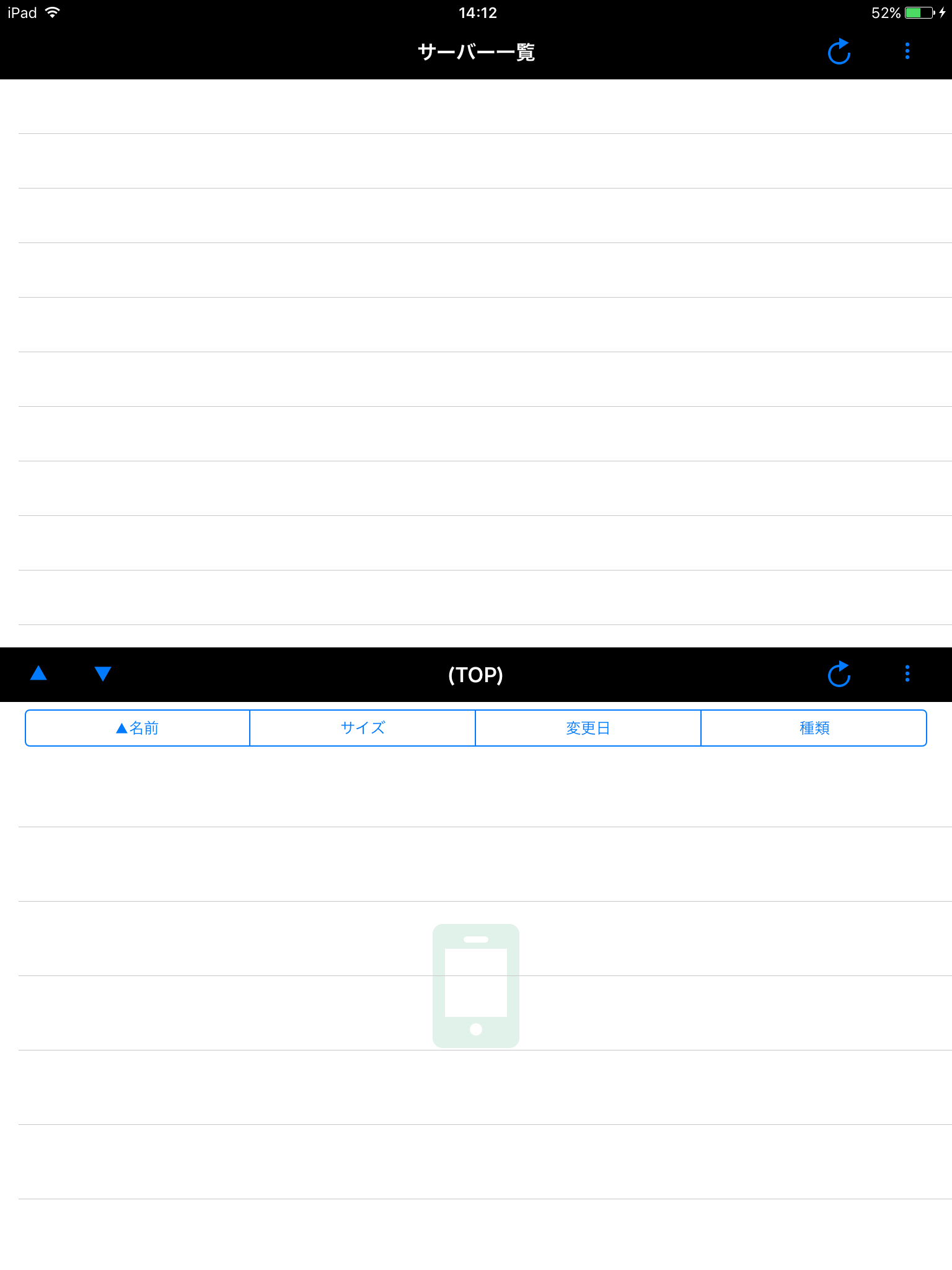
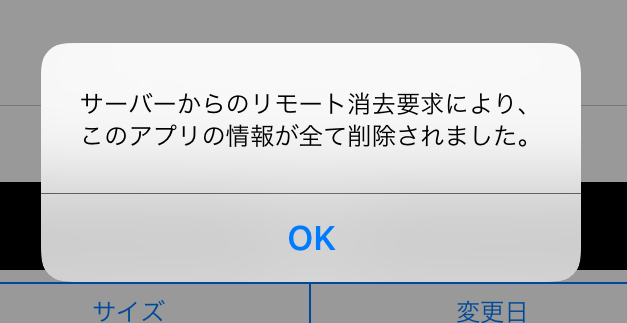
アプリ内に登録されている全ての接続先情報とローカル側「アプリのフォルダ」以下に保存された全てのファイルやフォルダが消去されます。



**リモート消去実施後(Androidアプリ)**

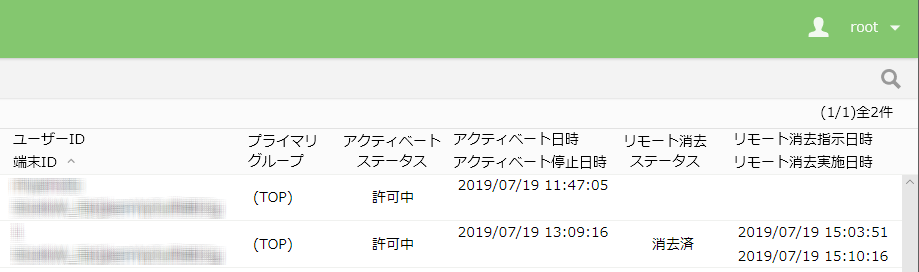
**iOSアプリの場合**

アプリ内に登録されている全ての接続先情報とローカル側(TOP)以下に保存された全てのファイルやフォルダが消去されます。



**リモート消去実施後(iOSアプリ)**

指示後にリモート消去が実施された端末については、リモート消去ステータス列に「消去済」と表示され、リモート消去実施日時列にリモート消去が実施された日時が表示されます。



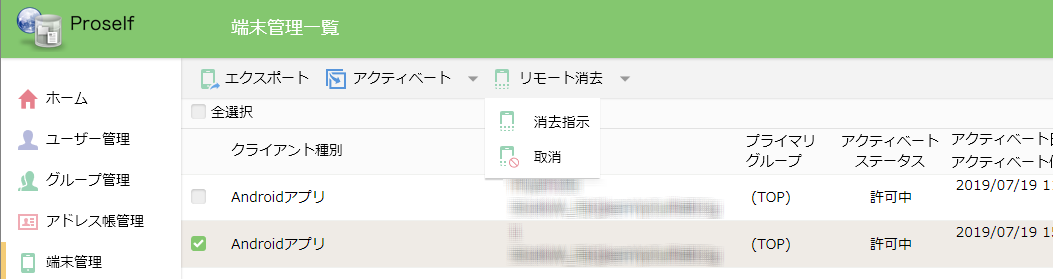
**端末管理一覧**

### リモート消去指示の取消

「[3.4.1.リモート消去指示](#_リモート消去指示)」によりリモート消去指示中となっている端末のリモート消去指示を取り消すことができます。

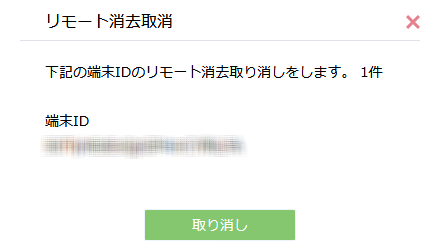
消去指示後に対象端末でクライアントアプリを起動するとリモート消去が実施されますので、本処理は端末上からのクライアントアプリ起動前であれば有効です。

リモート消去指示の取消を行う端末にチェックを入れると「リモート消去」メニューが表示されます。このメニュー内より「取消」をクリックします。



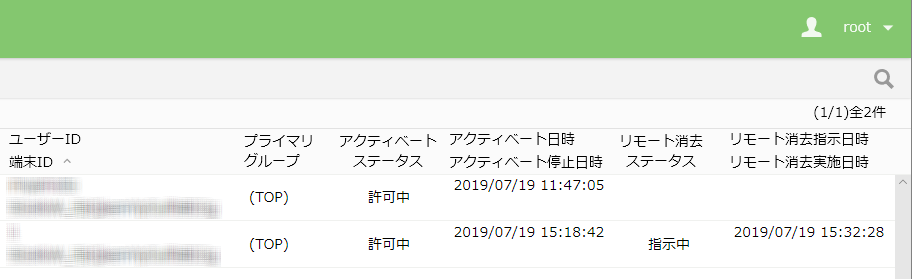
**端末管理一覧**

リモート消去取消確認ダイアログが表示されますので、「取り消し」をクリックします。処理を取り消す場合は右上の「×」をクリックします。

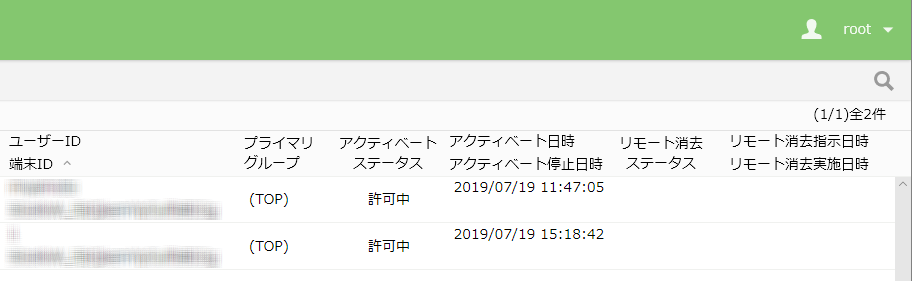


**リモート消去取消確認ダイアログ**

リモート消去取消が実施された端末については、リモート消去ステータス列の「指示中」が非表示となります。また、リモート消去指示日時列の日時が非表示となり、リモート消去指示を実施する前の状態となります。



**端末管理一覧(リモート消去取消実行前)**



**端末管理一覧(リモート消去取消実行後)**