RemoNavi シェアサービス版

ユーザーズマニュアル

1.0 版　2024/08/01

【目次】

1. RemoNavi シェアサービス版のご利用に当たって 3
2. RemoNavi SaaS の利用手順 5
2.1. 利用シーン 5
2.2. 利用登録 6
2.3. ログイン・ログアウト 7
2.4. パスワード変更 8
2.5. OTP リセット 8
2.6. API Token 発行・削除 9
2.7. トップページ 9
2.8. リモート接続 10
2.8.1. リモート接続の利用 10
2.8.2. リモート接続ログ 17
2.9. アクセスログ 19
2.10. サービスプランの変更 21
2.11. 利用停止 22

1. RemoNavi シェアサービス版のご利用に当たって

RemoNavi のサービス形態は SaaS です。 クラウド上に配備される RemoNavi SaaS は認証、暗号化通信、ACL 制御を有したゲートウェイ的な役割を果たし、プライベート・ネットワークなど非公開のリソースへの通信接続を提供します。

RemoNavi SaaS には企業様が利用するエンタープライズ版。 個人小企業様が利用するシェアサービス版の 2 種類がありますが、基本的なリモート接続機能は同一です。 シェアサービスの提供単位は 1 アカウントのため、ACL 機能をお客様には提供しておりませんが、内部的には ACL 機構によって、お客様別のサービス提供を実現しています。
本マニュアルの対象は、シェアサービス版です。

以下は本サービズの第一機能であるリモート接続の通信イメージです。
「どこからでも、どこへでも」、「VPN とは異なる新しいリモート接続」、「SaaS で実現するリモート接続のインフラ」とはこの機能を指し、特出すべきは TCP | UDP 通信の提供です。 異なるネットワーク間を VPN 機器なしに FW を越えて接続します。

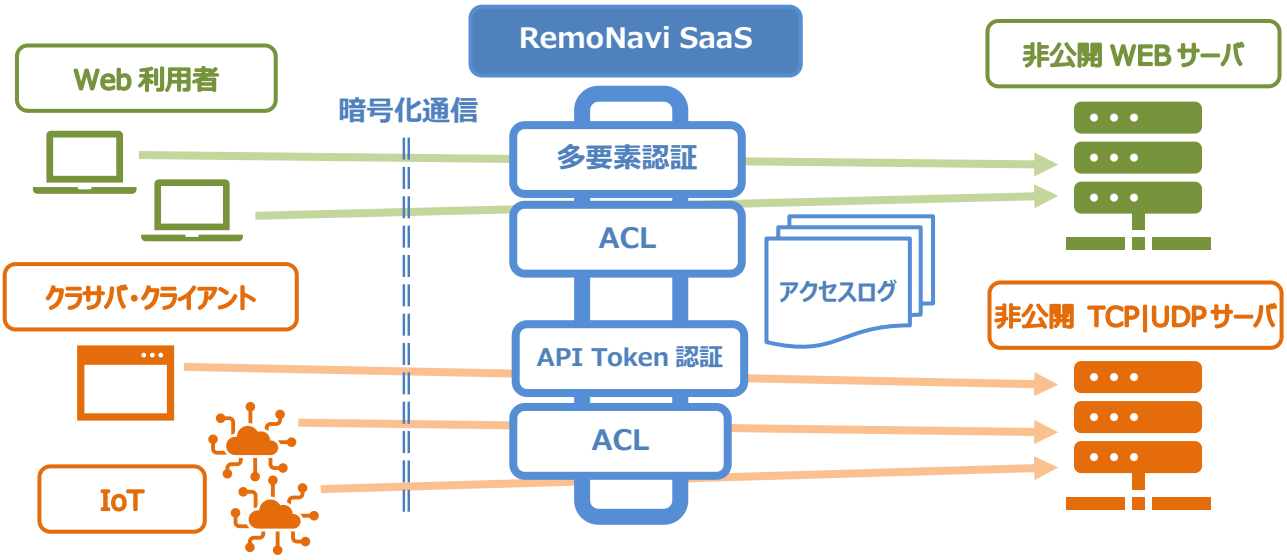

図 1 RemoNavi 通信イメージ

RemoNavi エンタープライズ版では大別して 3 つの機能が提供され、シェアサービス版はこの中の 1 つ「リモート接続機能」だけとなります。

表 1 サービスの大機能分類

	機能名	対象 *1	機能概要
1	リモート接続	E,S	Peer to Peer、2 点間のセキュアな通信接続を提供します。 ① 認証（OTP 認証	API Token） ② 暗号化通信 ③ ACL 適用（シェアサービスは利用者様分離にのみ利用で機能非公開） ④ 全通信のアクセスログ保存 接続対象は以下。 ① TCP, UDP

			② HTTP, HTTPS (リバースプロキシ適用)
2	セキュリティ施策	E	以下、情報瀬セキュリティ運用に必要な重要 2 機能とそれらの運用に必要な規定書類が提供されます ① セキュリティ・インシデントの発生から解決までのフロー管理、 ② セキュリティ検査 ③ 情報セキュリティ運用を規定する「情報セキュリティ規定書、情報セキュリティ対策基準」 の雛形提供
3	企業ユーティリティ	E	以下、セキュリティ運営に役立つユーティリティ機能が提供されます ① アカウント管理 （利用権限設定含む） ② アクセスログ管理 ③ タスク管理機能 ④ 全社通知機能 ⑤ 個人メモ機能 ⑥ チャット機能 以下の機能は完成された機能ではなく、今後拡張、成熟させていくもので安価ないしは無料で提供 ⑦ ビデオチャット機能（オープンソース Janus 利用 client をリモナビで実装） ⑧ データ分析 （名寄せ、回帰分析） ⑨ 動画・画像一時補完機能（機器等、保全業務時の記録媒体などに拡張予定。 後、保全リポート作成などと組み合わせたカスタマイズも想定）

*1) [E] エンタープライズ版、[S]シェアサービス版

【ネットワーク環境】

- お客様環境のファイアウォールにてポート開放の必要はありません。
- 接続する側、される側はいずれもインターネット上に配備される RemoNavi SaaS に接続できる必要があります。

【カスタマイズ案件】

RemoNavi シェアサービス版をお客様にて運用するなどの構成も可能であればご提供いたします。

カスタマイズ案件については、気軽にご相談ください。

2. RemoNavi SaaS の利用手順

2.1. 利用シーン

RemoNavi エンタープライズ版が導入された直後からのすべき操作の一覧を以下に示し、以降それらの操作説明をしていきます。 利用に至っては、まずは本節をご参照ください。

表 2 利用シーンの一覧

	利用シーン	運用フェーズ	作業概要
1	利用登録	契約登録	詳細は **2.2 節**参照
2	ログイン・ログアウト	日常運用	詳細は **2.3 節**参照
3	パスワード変更	日常運用	詳細は **2.4 節**参照
4	OTP リセット	日常運用	詳細は **2.5 節**参照
5	API Token 発行・削除	日常運用	詳細は **2.6 節**参照
6	トップページ	日常運用	詳細は **2.7 節**参照
7	リモート接続 (リモート接続ログ含む)	日常運用	リモート接続の利用 詳細は **2.8.1 節**参照 リモート接続ログ 詳細は **2.8.2 節**参照
8	アクセスログ	日常運用	詳細は **2.9 節**参照
9	サービスプランの変更	契約変更	詳細は **2.10 節**参照
10	利用停止	契約変更	詳細は **2.11 節**参照

2.2. 利用登録

利用登録は、以下の URL から実施します。

https://remonavi.com/?pos=subscription

シェアサービス用のサーバー一覧から、登録したいサーバを選択して「登録」をしてください。

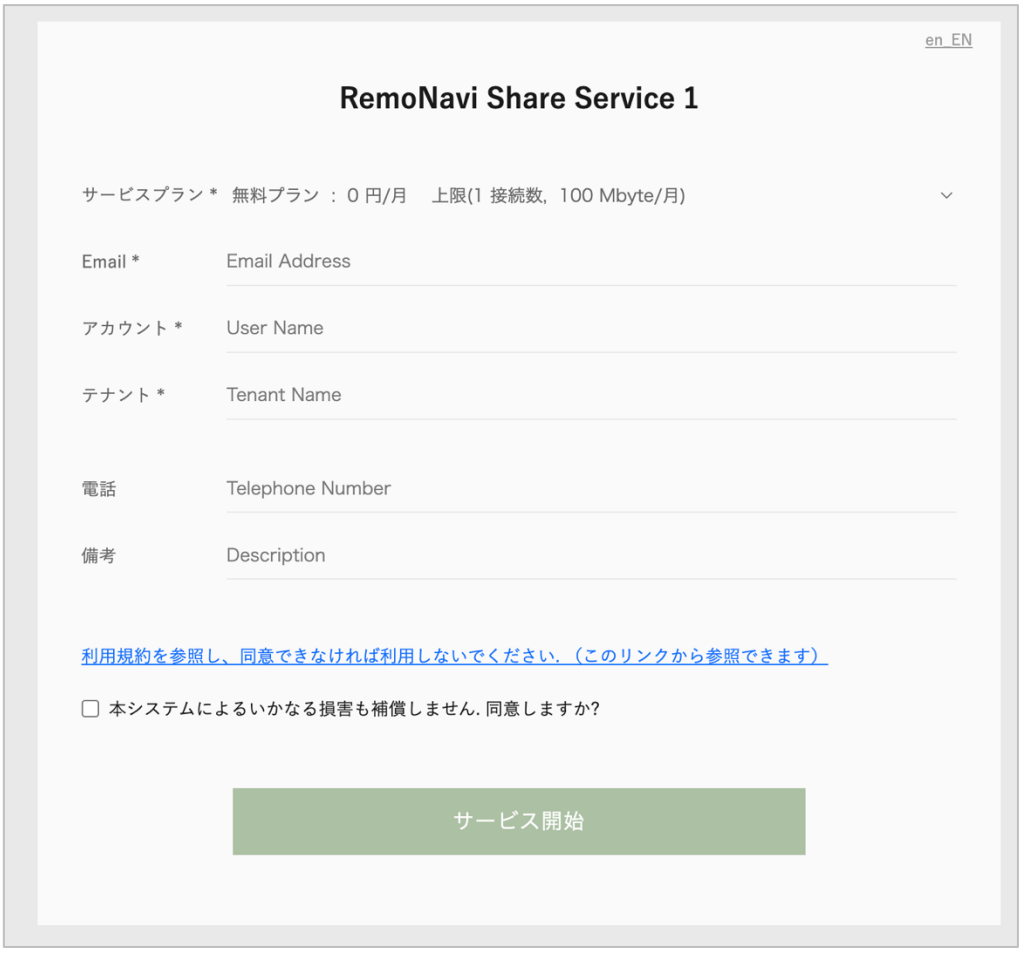

図 2 シェアサービス登録画面

登録すると、登録した Email アドレスに「アクセス URL」「ユーザ」「パスワード」が送信されますので、30 分以内にログインしてください。 時間超過すると、アカウントは削除されます。

また、利用不能な Email アドレスを利用すると、登録通知メールが届きませんので、有効なメールアドレスをお使いください。

登録時は無料アカウントになります。 100Mbyte/月の通信量制限があります。

また、無料アカウントは、30 日以上利用がないと、自動的に削除されます。

2.3. ログイン・ログアウト

RemoNavi SaaS のログインは、ワンタイムパスワード（OTP）による２段階認証です。

① 初期ログイン手順

- 利用者の「Email，パスワード」を入力します。 [A-1]
- GoogleAuthenticator アプリにて QR コードを読み込むと、６桁の数値が定期更新され表示されます。
- 表示されている６桁の数値を入力すればログイン完了です。 [A-2]

② GoogleAuthenticator アプリ登録後の通常ログイン手順

- 利用者の「Email，パスワード」を入力します。 [B-1]
- 表示されている６桁の数値を入力すればログイン完了です。 [B-2]

③ ログアウト手順

- ログイン後は全ての画面のトップメニュー右端のログイン Email のドロップダウンメニューからログアウトできます。

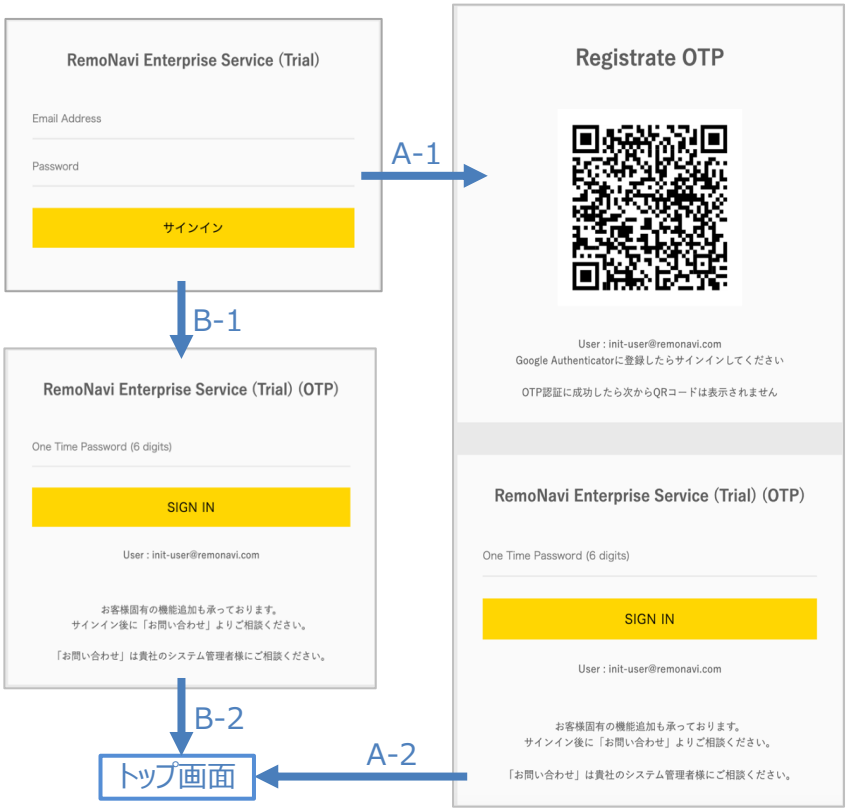

図 3 ログイン画面

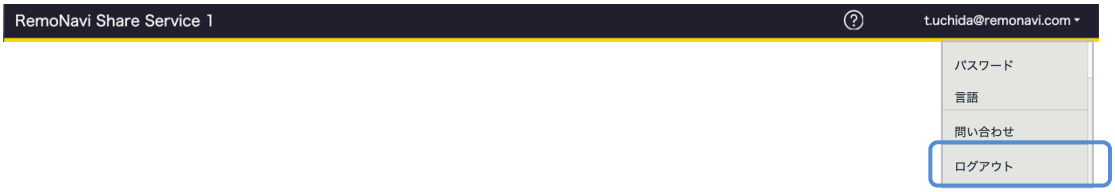

図 4 ログアウト画面

2.4. パスワード変更

利用者は自らパスワードを変更することができます。 パスワードは 「英数字と記号(._-@#!*)」の利用が可能です。

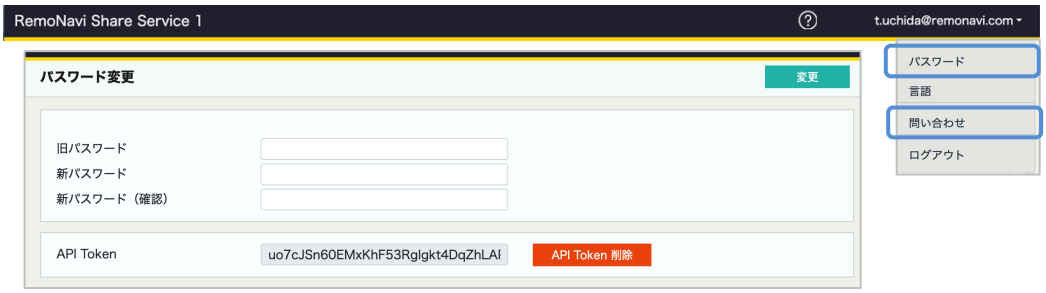

図 5 パスワード変更画面

もしパスワードを忘れてしまった場合は、「お問い合わせ」よりご連絡ください。

2.5. OTP リセット

モバイルフォンの買替えなどで GoogleAuthenticator アプリを再インストールする場合、端末にインストールしたアプリで OTP の再登録が必要になります。 利用者に新たな登録の QR コードを提供するために提供される機能です。

OTP リセットは、サイドメニュー「アカウント/アカウント」から、「アカウント一覧画面」 を表示し、アカウント行をダブルクリックないしは、E-Mail 列のリンクをクリックして 「アカウント情報画面」から操作します。

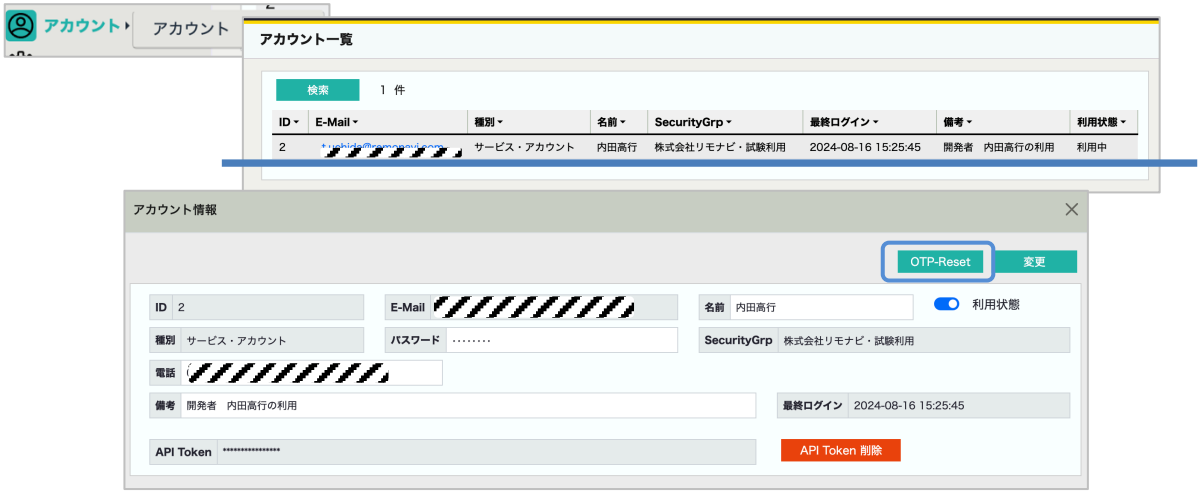

図 6 アカウント情報画面

「OTP Reset」ボタンを押下するとリセットされます。 リセットすると、次回ログイン時に QR コードが出力され新たな登録が要求されます。これまでの GoogleAuthenticator の設定は利用できなくなります。

次項目の API Token の発行・削除もこの画面でできますが、発行値の参照がこではできないため、次項の操作で実施してください。

2.6. API Token 発行・削除

「パスワード変更画面」より「API Token 発行 | 削除」をします。 再発行する場合は、削除の後に再度発行してください。

発行済みの場合、英数字で構成される 32 桁の文字列が表示され、操作ボタンには「API Token 削除」が表示されます。

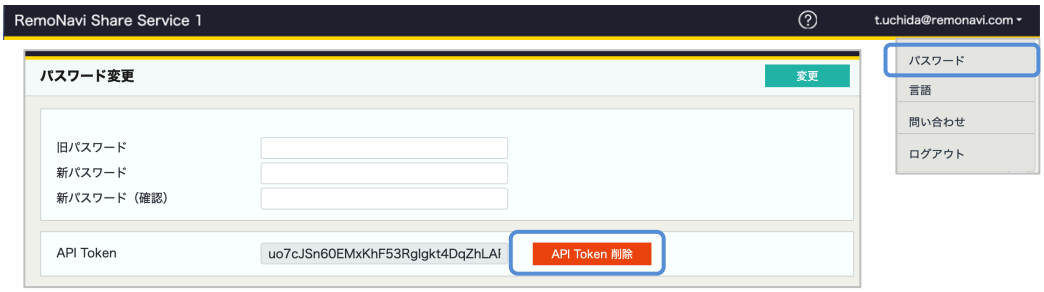

図 7 パスワード変更画面 API Token 発行・削除設定

2.7. トップページ

ログインすると最初に表示されるページです。

ここに表示されるのは、 リモート接続で http, https 接続の設定がアイコン表示されます。 このアイコンをクリックすると、リモートに WEB アクセスします。 ただし Receiver 経由の場合、Receiver が稼働していないと接続エラーになります。この画面には状態反映されないので、注意してください。

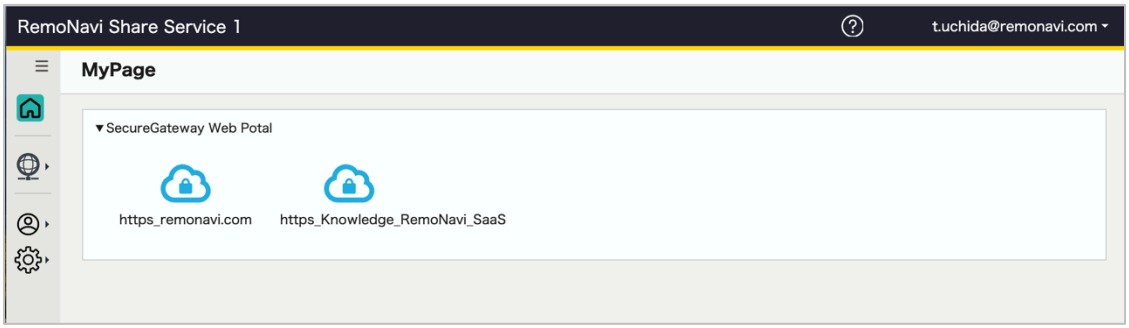

図 8 トップ画面

2.8. リモート接続

2.8.1. リモート接続の利用

リモート通信は利用プロトコルや、接続環境によって利用するものが異なるため、全網羅的に利用について説明します。

1) リモート通信の種類の選択

RemoNavi が提供するリモート接続には以下の 4 種類の接続があります。 まずは実現するリモート接続がどれにあたるのかを確認してください。

接続ケースによっては利用者環境に Sender アプリ、接続先サーバ等に Receiver アプリのインストールが必要になります。

表 3 リモート接続の種類

	接続構成	通信種別	接続種別	Sender	Recver
1	プライベートネットワークの「SSH, データベース、クラサバ・サーバ」などへの接続	TCP｜UDP	Recver 経由	○	○
2	ローカル環境の WEB サーバへの接続（ブラウザ・アクセス）	WEB	Recver 経由	—	○
3	パブリックネットワークの「SSH, データベース、クラサバ・サーバ」などへの接続。 RemoNavi サーバから直に	TCP (*1)	直接接続	○	—
4	パブリックネットワークの WEB サーバへの接続（ブラウザ・アクセス）		直接接続	—	—

(*1) RemoNavi クラウドサーバは FW 設定をしており、外部公開 IP ポートは固定されているため、RemoNavi から UDP 送信はできても、戻り通信が FW で遮断されてしまうため、利用できません。

2) Sender と Receiver の配備について

Sender は、利用者の API Token を設定して RemoNavi SaaS に接続します。

- Sender を使った通信は、SaaS 側のリモート接続ログに記録されます。
- Sender 側でもクライアント IP アドレスを含む通信ログが保存されます。
- Sender の配備は、利用端末が収容されるネットワークに 1 台ないしは複数台設置することが可能です。設置数に制限はありません。

Receiver は、利用者の API Token を設定して RemoNavi SaaS に接続します。

- Receiver の配備は、接続先サーバ、システムが収容されるネットワークに 1 台ないしは複数台設置することが可能です。設置数に」制限はありません。
  - ・ Receiver から接続先システムへ TCP|UDP|SSH 接続するため、接続先はアドレス解決できるホスト名が指定されないといけません。
  - ・ localhost ホスト名も利用可能ですが、それについては注意が必要です。それについては次項「Sender と Receiver の提供形態」を参照ください。

3) Sender と Receiver の提供形態

Sender と Receiver は、①Windows アプリ (msi インストーラー提供)、②Docker (docker イメージの gzip) の 2 種類で提供されます。

注意）Docker 提供の場合、特に Receiver においてネットワーク的に注意すべきことがあります。 それが localhost です。いうまでもありませんが Docker はホスト上で動作するコンテナで localhost というホスト名は、ホストマシンではなく、docker コンテナ自身にアドレス解決します。 そのため localhost は接続先ホスト名としては原則利用しないことを推奨します。

運用上のヒント）
接続するホスト名は、Receiver をインストールしたホスト・マシンでアドレス解決できる必要があります。この簡単な方法は、ホスト・マシンの hosts ファイルで定義してしまうことです。

4） リモート利用の設定（SaaS での SecureGateway の登録）

SecureGateway(リモート接続) の操作は、サイドメニュー「SecureGatewat/Gateway 設定」から、「SecureGateway 一覧・画面」を表示して操作します。

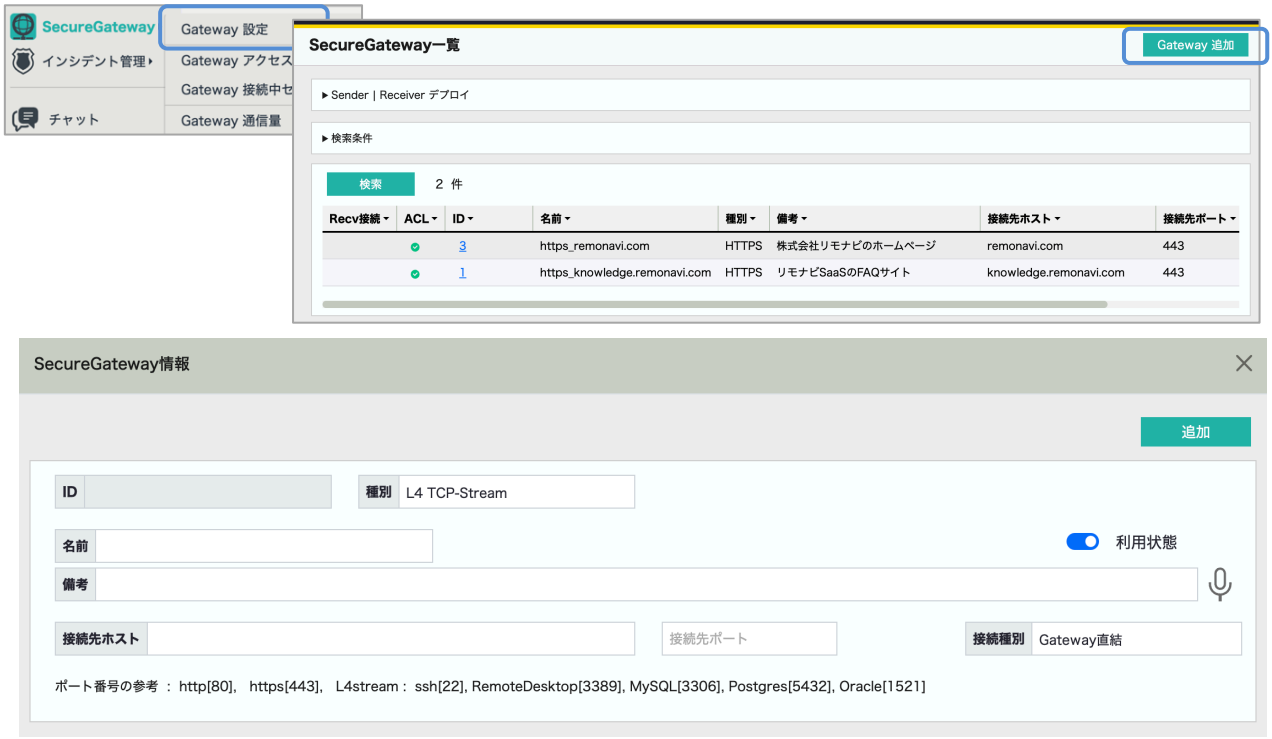

図 9 SecureGateway(リモート接続)一覧・画面 と SecureGateway 登録画面

SecureGateway の設定項目は、実際のネットワーク情報を設定する必要があるため、設定項目の詳細を説明します。

【入力項目】

	入力項目	説明
1	種別	リモート通信の種類。 ・ L4 TCP-Stream (TCP/IP) ・ L4 UDP-Stream (UDP/IP) ・ L6 SSL-Stream (SSL) [*1] ・ HTTP （WEB リバースプロキシ対象） ・ HTTPS （WEB リバースプロキシ対象）

2	名前	一意の名称です。 重複は許容されません。
3	利用状態	当該 Gateway の利用可否。
4	備考	当該 Gateway の説明文。
5	接続ホスト [*2]	接続先のホスト（ドメイン名 | IP アドレス） ・ Receiver 経由の場合、Receiver インストールホストで、 ・ 直接接続の場合、RemoNavi SaaS ホストで、アドレス解決できるホスト名である必要があります。 Receiver が docker である場合、前節の注意事項の通りです。
6	接続ポート [*2]	接続先の IP ポート番号
7	接続種別	RemoNavi SaaS からの接続種別で、以下の 2 種類から選択します。 ・ 直接接続 ・ Receiver 経由

[*1] SSL の利用は接続先サーバで、TLS ホスト名のチェックが厳密である場合にのみ利用し、通常は L4 TCP-Stream を利用してください。 SSL-Stream は、以下のように、ネットワーク間毎に SSL コネクションがそれぞれ個別に確立されます。

利用者 Clent —(ssl-conn#1)— **Sender** —(ssl-conn#2)— **RemoNavi SaaS** —
—(ssl-conn#3)— **Receiver** —(ssl-conn#4 接続先ホスト名)— **接続先ホスト**

[*2] 編みかけ部が「実際のネットワーク情報」です。

【登録結果】

登録が完了すると、一覧画面に反映されます。

5) 具体的な利用設定例（Sender、Receiver 利用の TCP 通信）

設定操作手順は以下の通りです。

① SaaS での SecureGateway の登録
② Sender のインストール
③ Sender の利用設定
④ Receiver のインストール
⑤ Receiver の利用設定
⑥ TCP/IP 通信をする

6) 具体的な利用設定例（Receiver 利用の WEB 通信）

設定操作手順は以下の通りです。

① SaaS での SecureGateway の登録
② Receiver のインストール
③ Receiver の利用設定
④ WEB ブラウザ通信をする（RemoNavi SaaS の MyPage 画面から）

7) Sender | Receiver のインストール

SecureGateway 一覧画面の「Sender | Receiver デプロイ」アコーディオン表示を開けると、ダウンロードすることができます。

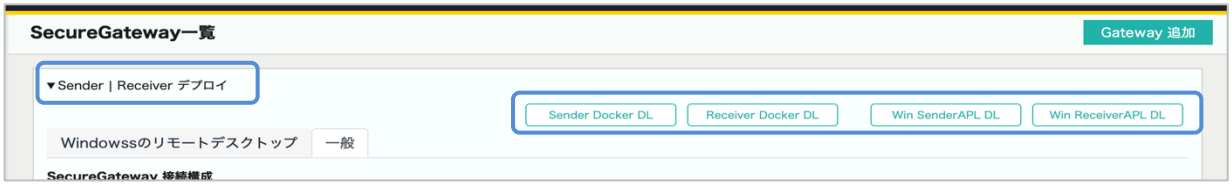

図 10 SecureGateway(リモート接続)一覧画面から Sender|Receiver ダウンロード

◆Win アプリの インストール方法

Sender, Receiver の Windows アプリは、 msi ファイルでの提供で、GlobalSign の EV コードサイニング証明書による署名をしていますが、一部のブラウザや AV ソフトでは 「不正ソフトウェア」の誤検知をすることがあります。 もし誤検知されたとしても、構わずダウンロードしてください。 msi ファイルのプロパティ表示：デジタル署名 から、EV コードサイニング証明書によって署名されていることを確認できます。

- msi ファイルをダブルクリックすると、Windows 標準のアプリケーション・インストーラーによってインストールされます
- インストールが完了すると、デスクトップに「RemoNavi Sender」「RemoNavi Receiver」のショートカットが作成されます。
- 1 ホストには Sender, Receiver はそれぞれ 1 つずつのみしかインストールできません。Sender|Receiver の共存は可能です。

◆Dodkcer の インストール方法

Docker は tar.gz ファイルでの提供です。

こちらも一部のブラウザや AV ソフトでは 「不正ソフトウェア」の誤検知をすることがあります。 もし誤検知されたとしても、構わずダウンロードしてください。

ダウンロードしたら、インストール方法は「SecureGateway 一覧画面の「Sender | Receiver デプロイ 一般タブ」の記載の通りです。 Docker の場合、公開する IP ポートを利用者様にて決定する必要があります。

【Sender Docker での特記事項（Receiver にはこの制約はありません）】

Sender は 接続先の TCP|UDP 受け口になり変わって、TCP|UDP 待受けをします。 この待受 IP ポート番号は、Sender の利用設定の際に指定して登録します。 一方で、Docker ホストマシンに対してどの IP ポートを公開するかを起動時のパラメータで指定します。 つまり公開した IP ポートしか利用できないのです。

TCP/IP 利用のみ：利用ポート 9100-9200 利用の場合

```
docker run -d -p 9100-9200:9100-9200/tcp …
```

TCP/IP, UDP/IP 両方利用： TCP 利用ポート 9100-9150、 UDP 利用ポート 9151-9200 利用の場合

```
docker run -d -p 9100-9150:9100-9150/tcp -p 9151-9200:9151-9200/udp …
```

これはプログラム的な制約ではなく、Docker の制約です。

こうした制約が面倒な場合は、Windows アプリを利用することも検討してみてください。

近年はマルウェアの巧妙化により、AV ソフトなどの誤検知も多くなっています。
ダウンロードに不具合がございます場合、Sender | Receiver の Win アプリ、Docker ファイルを直接お渡しいたしますので、必要に応じてご要望ください。

8) Sender の利用設定

【共通・利用手順】

Windows アプリ、Docker 共に以下の手順で利用します。

① RemoNavi SaaS との接続設定

Server Domain 名 ： 利用している RemoNavi SaaS のドメイン名
API Token ： アカウントの API Token (このアカウントで許可された接続のみ利用になります)
Local Domain ： Sender のホスト名（アドレス解決できるホスト名）

正常に接続できたら、利用可能な SecureGateway 一覧を画面に表示することができるようになります。Receiver 経由のリモート接続では、Receiver の稼働状態を 「稼働🟢」、「未稼働🔴」で表示します。

② リモート接続（SecureGateway の利用設定）

- 利用するリモート接続（SecureGateway）行に Sender「受け入れ IP ポート」を入力します。
- 同一行の「管理対象」にチェックを入れます。

これで完了です。利用設定には数秒かかります。
利用を終了する場合は、このチェックを外すだけです。（これにも数秒かかります。）

【Windows アプリ】

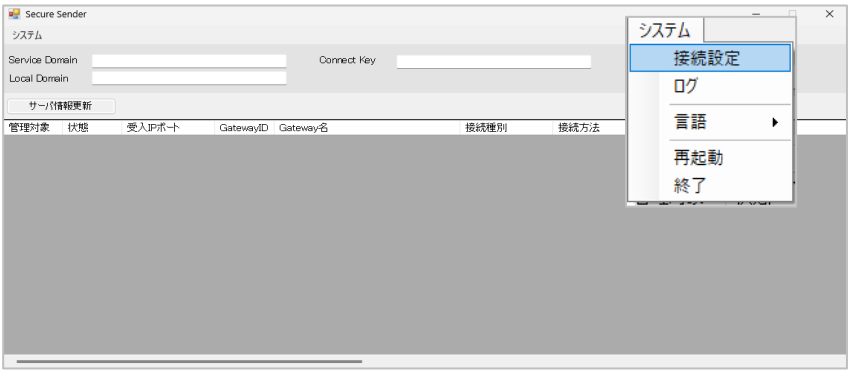

図 11 Windows Sender 管理画面（接続設定）

接続設定が完了したら、ブラウザの再表示をすると、利用可能な SecureGateway（リモート接続）一覧が表示されます。 利用設定は、この一覧から「共通・利用手順」の通り実施します。

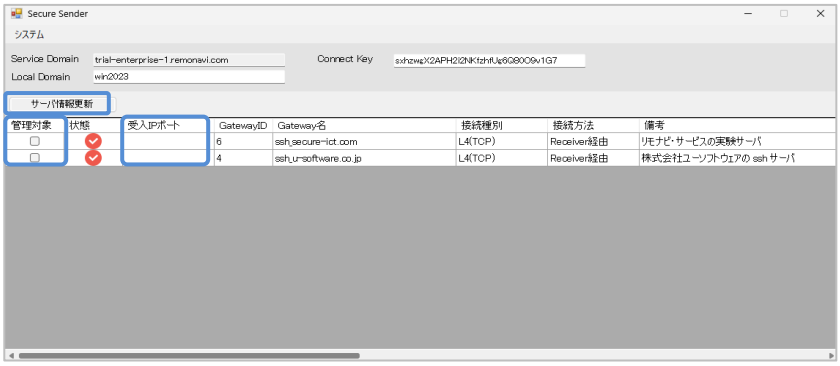

図 12 Windows Sender 管理画面（利用設定）

【Docker】

Docker では IP 80 番ポートで Web サーバを立ち上げています。このポートのホストマシンの紐付けを 9070 として、以下に初期設定、利用設定について説明していきます。

図 13 Sender Docker 管理画面 (接続設定)

接続設定が完了したら、ブラウザの再表示をすると、利用可能な SecureGateway（リモート接続）一覧が表示されます。 利用設定は、この一覧から「共通・利用手順」の通り実施します。

図 14 Sender Docker 管理画面 (利用設定)

9) Receiver の利用設定

【共通・利用手順】

Windows アプリ、Docker 共に以下の手順で利用します。

① RemoNavi SaaS との接続設定

Server Domain 名 ： 利用している RemoNavi SaaS のドメイン名

API Token ： アカウントの API Token (このアカウントで許可された接続のみ利用になります)

正常に接続できたら、利用可能な Receiver 経由の SecureGateway 一覧を表示することができるようになります。

② リモート接続（SecureGateway の利用設定）

- 同一行の「管理対象」にチェックを入れます。

  これで完了です。利用設定には数秒かかります。

  利用を終了する場合は、このチェックを外すだけです。（これにも数秒かかります。）

Receiver が稼働状態になると、RemoNavi SaaS や Sender の Receiver 接続状態（「稼働🟢」、「未稼働🔴」）が反映されます。 SaaS や Sender ともに自動反映ではなく、画面を再表示する必要があります。

【Windows アプリ】

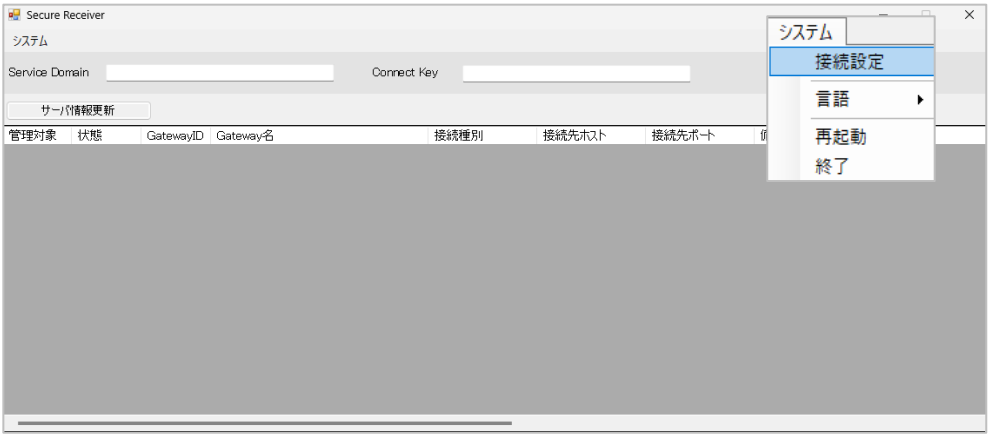

図 15 Windows Receiver 管理画面（接続設定）

接続設定が完了したら、ブラウザの再表示をすると、利用可能な SecureGateway（リモート接続）一覧が表示されます。 利用設定は、この一覧から「共通・利用手順」の通り実施します。

図 16 Windows Receiver 管理画面（利用設定）

【Docker】

Docker では IP 80 番ポートで Web サーバを立ち上げています。このポートのホストマシンの紐付けを 9080 として、以下に初期設定、利用設定について説明していきます。

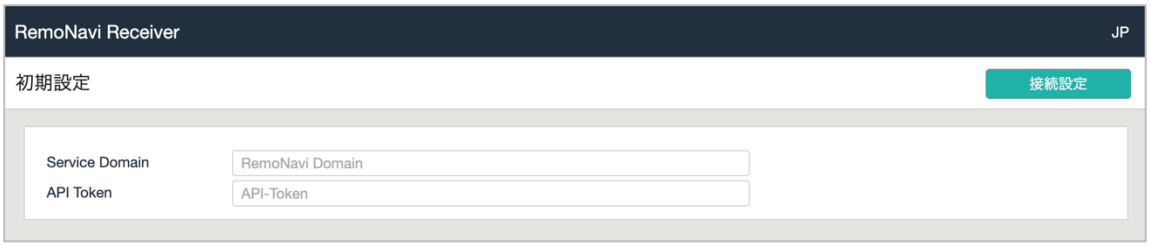

図 17 Receiver Docker 管理画面（接続設定）

接続設定が完了したら、ブラウザの再表示をすると、利用可能な SecureGateway（リモート接続）一覧が表示されます。 利用設定は、この一覧から実施します。

図 18 Receiver Docker 管理画面 (利用設定)

2.8.2. リモート接続ログ

リモート接続ログは RemoNavi SaaS で通信した全てのログ関連の管理画面です。

リモート接続ログの操作は、サイドメニュー「SecureGateway/Gateway アクセスログ」から、「SecureGateway Access Log 画面」を表示して操作します。

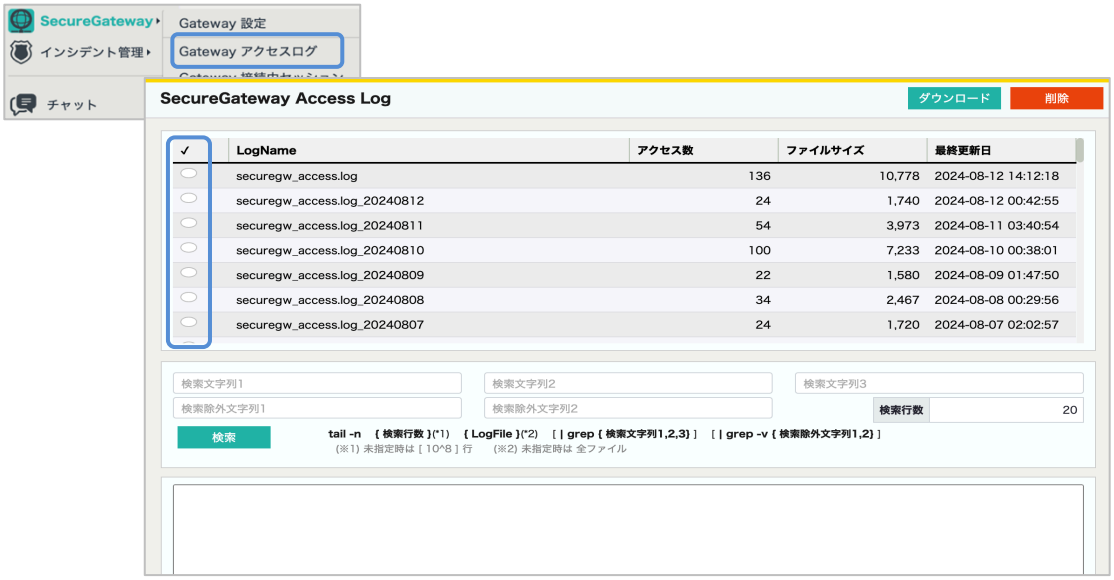

図 19 SecureGateway Access Log 画面

SecureGateway Access Log 画面の構成は以下です。

① アクセスログファイル一覧

- ログファイルの一覧を新しいもの順に全て表示します。
- 参照、ダウンロード(DL)、削除 をする際には、このファイル一覧の「✓」列を選択して、操作します。

② アクセスログ参照の検索フィルタ

検索は、Linux OS の tail コマンドを、以下のように実行します。

```
tail -n {検索行数} { LogFile } [ | grep { 検索文字列 1,2,3} ] [ | grep -v { 検索除外文字列 1,2} ]
```

- 検索文字列、検索除外文字列　に空白文字を入力することはできません。
- 検索行数は、全行検索したい場合には対象ファイルのアクセス数より大きな数値を指定してください。（最大は 100,000,000）
- アクセスログを選択せずに検索する場合は、ファイル一覧の「✓」をせずに検索します。
  - この場合、検索文字列の入力が必須です。
  - 検索結果は最大 50,000 行しか表示されません。
  - この操作によるサーバ負荷は考慮されません。十分に注意して実施してください。

③　アクセスログの参照エリア

検索したアクセスログを表示します。 ログフォーマットについては、ヘルプ画面を参照してください。

図 20　ヘルプ画面（Gateway アクセスログ）

【SecureGateway アクセスログの操作】

	操作種別	操作内容
1	検索	検索条件を入力して、「検索」ボタンを押下して検索します。
2	ダウンロード	アクセスログファイル一覧から対象ファイルに「✓」をつけて、画面上部の「ダウンロード」ボタンを押下します。

2.9. アクセスログ

アクセスログは RemoNavi SaaS で操作した全てのログ情報の参照などの管理画面です。

アクセスログの操作は、サイドメニュー「システム/アクセスログ」から、「アクセスログ画面」を表示して操作します。

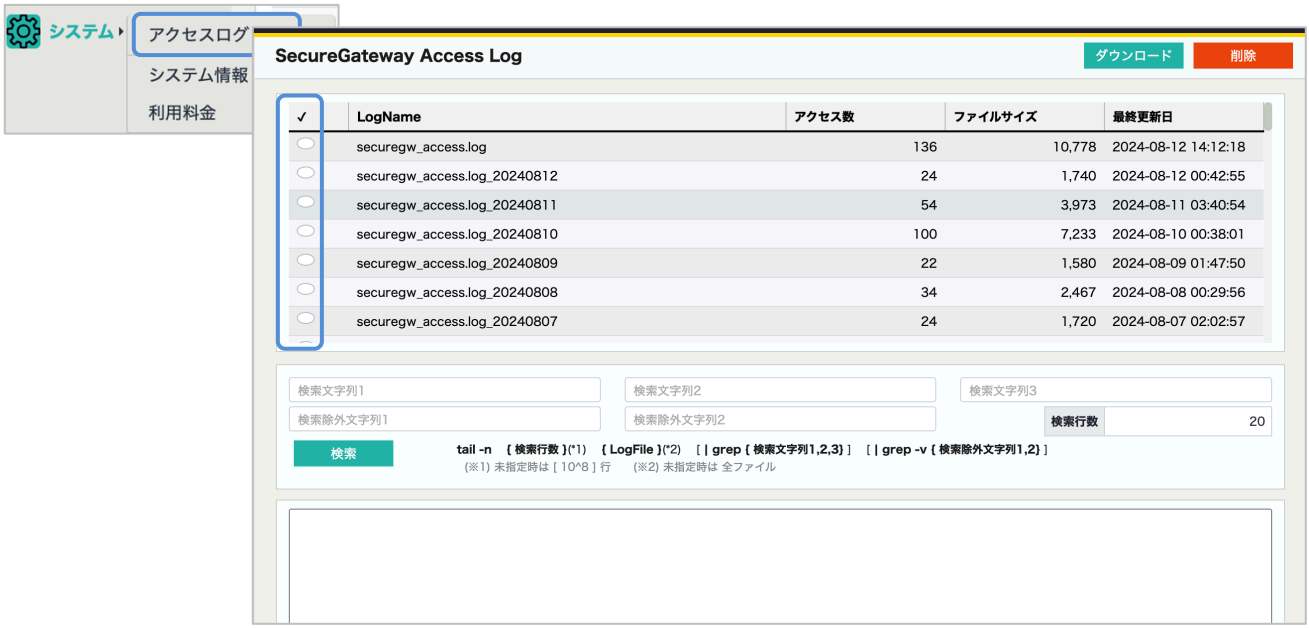

図 21 アクセスログ画面

アクセスログ画面の構成は以下です。

① アクセスログファイル一覧

- ログファイルの一覧を新しいもの順に全て表示します。
- 参照、ダウンロード(DL)、削除 をする際には、このファイル一覧の「✓」列を選択して、操作します。

② アクセスログ参照の検索フィルタ

検索は、Linux OS の tail コマンドを、以下のように実行します。

tail -n {検索行数} { LogFile } [| grep { 検索文字列 1,2,3}] [| grep -v { 検索除外文字列 1,2}]

- 検索文字列、検索除外文字列 に空白文字を入力することはできません。
- 検索行数は、全行検索したい場合には対象ファイルのアクセス数より大きな数値を指定してください。 (最大は `100,000,000`)
- アクセスログを選択せずに検索する場合は、ファイル一覧の「✓」をせずに検索します。
  - この場合、検索文字列の入力が必須です。
  - 検索結果は最大 50,000 行しか表示されません。
  - この操作によるサーバ負荷は考慮されません。十分に注意して実施してください。

③ アクセスログの参照エリア

検索したアクセスログを表示します。 ログフォーマットについては、ヘルプ画面を参照してください。

図 22 ヘルプ画面（アクセスログ）

【アクセスログの操作】

	操作種別	操作内容
1	検索	検索条件を入力して、「検索」ボタンを押下して検索します。
2	ダウンロード	アクセスログファイル一覧から対象ファイルに「✓」をつけて、画面上部の「ダウンロード」ボタンを押下します。

2.10. サービスプランの変更

利用停止は、サイドメニュー「システム／システム情報」で「システム情報画面」を表示し、「契約情報」から「契約情報画面」を表示して操作します。

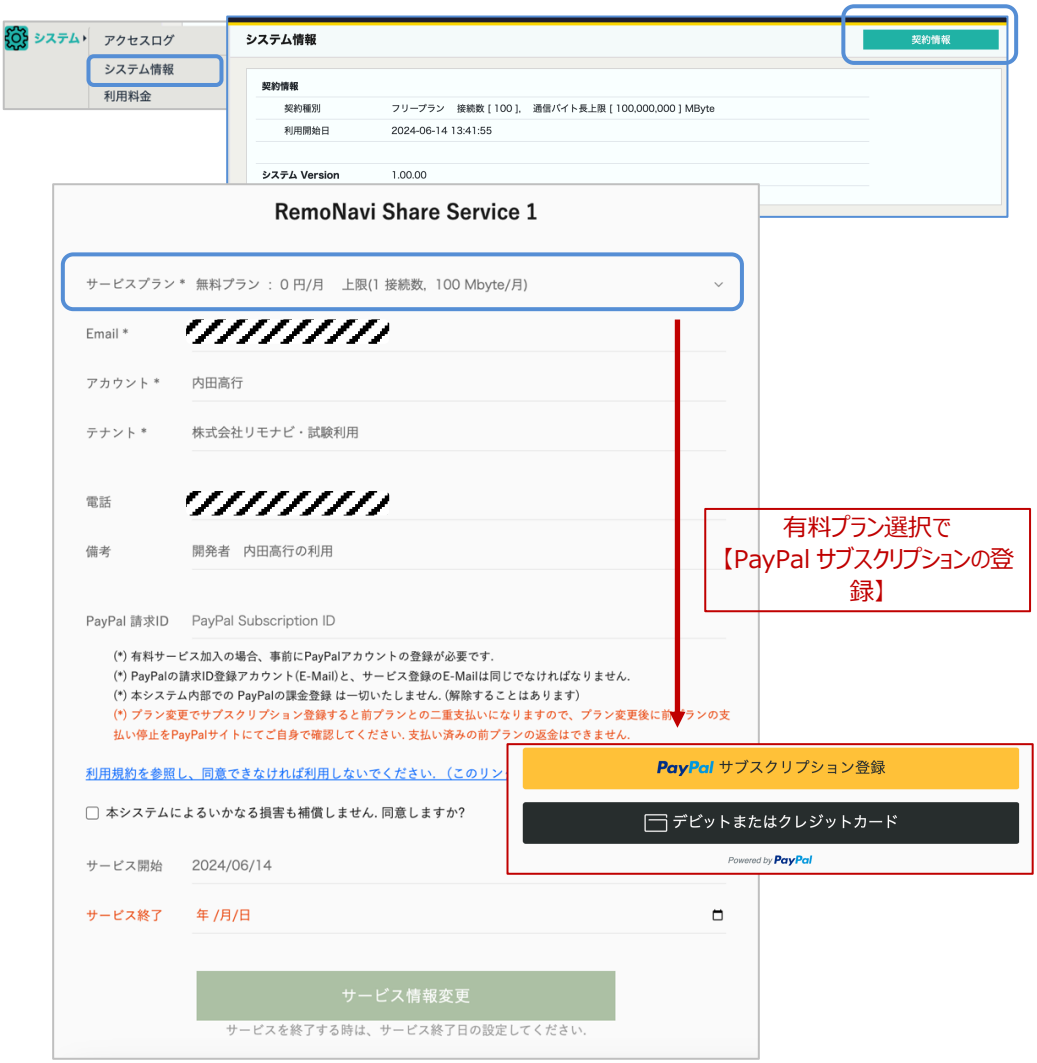

図 23 契約情報･画面

【重要】

本システムは、PayPal のサブスクリプションを利用しております。PayPal のサブスクリプションは変更･登録した時点で支払いが発生します。 そのため、前プランの利用中にプラン変更すると、その時点から新プランの適用となり、前プランの当月利用期間が残っていてもその分の返金はありません。

本システムは PayPal のサブスクリプションを利用していますが、お客様と PayPal のご契約に関しては関与しておりません。このことから、お客様がプラン変更する場合は、以下の手順を取ってください。

① プラン変更前に前プランの停止をしてください。

- 本システムの PayPal のサブスクリプションは月単位で、契約日から翌月の前日までといった形態になります。そのため、停止がその日を 1 日でも超えてしまうと 1 ヶ月分の支払いをすることになりますので、停止日は PayPal の契約状況をご自分で確認してください。

② 本システムでプラン変更すると、当画面から PayPal 管理画面にジャンプしますので、そこで新プランの適用をしてください。

本システムでは毎日、PayPal の支払い状況を確認し、未支払いの利用者は強制的にフリープランに変更しています。この時、リモート接続の設定も「利用停止」にします。 フリープランは、リモート接続は１つのみ利用可能ですので、有料プランで複数ご利用のお客様の場合、それらのうちの１つのみしか利用できなくことに注意してください。

2.11. 利用停止

利用停止は、サイドメニュー「システム／システム情報」で「システム情報画面」を表示し、「契約情報」から「契約情報画面」を表示して操作します。

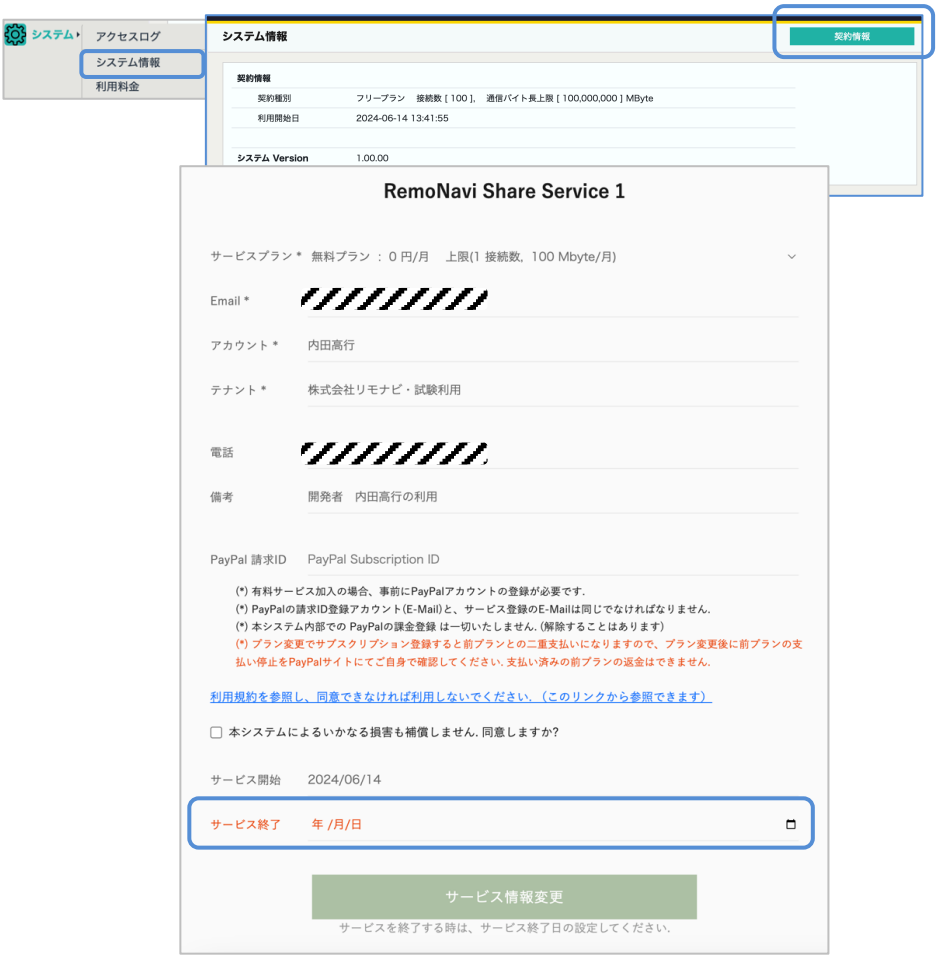

図 24 契約情報･画面

「サービス終了日」を入力して「サービス情報変更」を確定すれば、指定日にサービスは終了します。

有料サービスをご利用の場合などを考慮して管理情報は数ヶ月間保持されたのちに削除されます。 そのため同一 Email アドレスでの再登録はできませんのでご注意ください。

有料サービスの場合、支払った料金の返済は一切致しません。 そのため PayPal サブスクリプションの支払い日については十分に考慮してください。 本システムは PayPal のサブスクリプションを利用していますが、お客様と PayPal のご契約に関しては関与しておりません。