RemoNavi エンタープライズ版

ユーザーズマニュアル

1.02 版　2025/6/10

【目次】

1. RemoNavi エンタープライズ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. 共通操作 ★ 7
2.2.1. ログイン・ログアウト 7
2.2.2. パスワード変更 8
2.2.3. OTP リセット 8
2.2.4. API Token 発行・削除 8
2.3.「管理者」の操作 ★★★ 9
2.3.1. 運用開始設定 9
2.3.1.1. 組織情報の生成・変更 9
2.3.1.2. セキュリティグループの生成 11
2.3.1.3. アカウント生成 13
2.3.2. アカウント変更・削除（パスワード,OTP リセット含む） 15
2.3.3. 権限の付与 16
2.3.3.1. セキュリティ・グループの設定変更 16
2.3.3.2. セキュリティグループの複製 17
2.3.4. アクセスログ 18
2.3.5. リモート接続ログ 20
2.3.6. シングルサインオン 22
2.4.「セキュリティ管理者」の操作 23
2.4.1. セキュリティ規定 23
2.4.2. セキュリティ検査 23
2.4.3. セキュリティインシデントの発生対応 27
2.5.「利用者」の操作 31
2.5.1. トップページ 31
2.5.2. リモート接続の利用 ★★★ 32
2.5.3. タスク管理の利用 42
2.5.4. チャットの利用 46
2.5.5. 個人メモの利用 50
2.5.6. 全体通知の利用 51
2.5.7. セキュリティ検査の実施（利用者） 53
2.5.8. ビデオチャットの利用 55
2.5.9. データ分析の利用 58
2.5.9.1. データセット 58
2.5.9.2. 原因分析セット 60
2.5.9.3. 名寄せセット 65
2.5.9.4. 分析ジョブ 68
2.5.10. ImageBox の利用 69

管理者であれ、利用者であれ、まずはここを参照してください！

2.1 利用シーン

リモート通信をする場合、以下を参照してください！

2.5.2 リモート接続の利用

1. RemoNavi エンタープライズ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、エンタープライズ版です。

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。

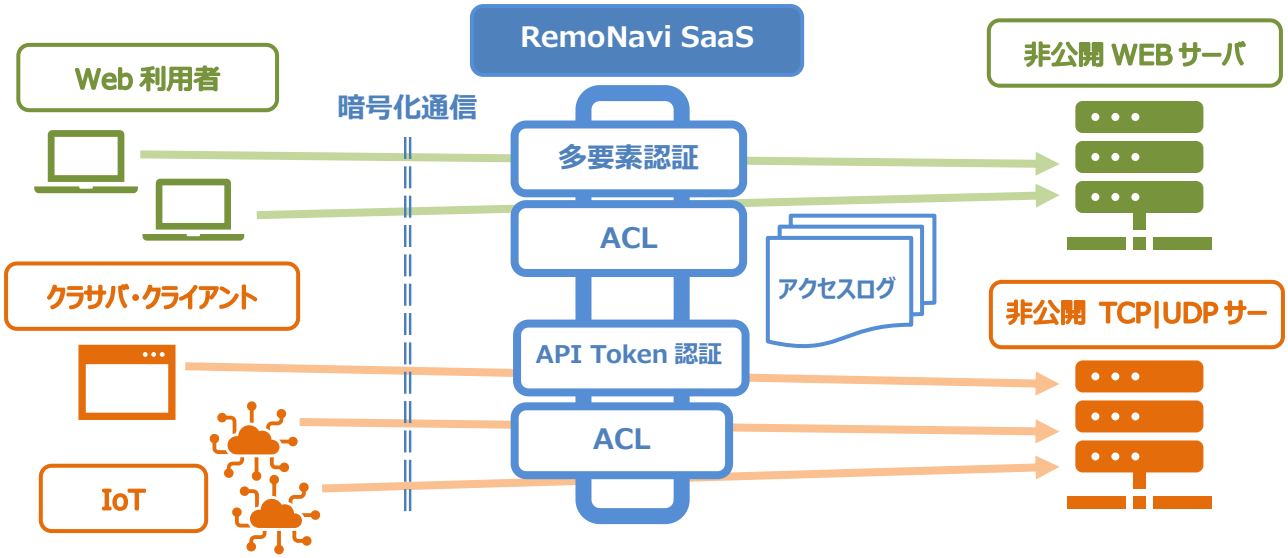


図 1 RemoNavi 通信イメージ

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 エンタープライズ版は SaaS 提供ですが、お客様の要望に応じて、お客様プライベートネット内への配備にも対応いたします。 ただし リモート接続は RemoNavi を介しで実現されるため、利用環境における、接続する側、される側が RemoNavi を認識できるドメイン名等の解決が必要です。

また、RemoNavi はセキュリティ製品でもあるため、 https でのみ動作します。プライベートネット内へ配備する場合、プライベート SSL 証明書を利用しての配備となります。

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（共通操作）

	利用シーン	運用フェーズ	作業概要
1	ログイン・ログアウト	日常運用	詳細は **2.2.1 節**参照
2	パスワード変更	日常運用	詳細は **2.2.2 節**参照
3	OTP リセット	日常運用	詳細は **2.2.3 節**参照
4	API Token 発行・削除	日常運用	詳細は **2.2.4 節**参照

表 3 利用シーンの一覧（システム管理者）

	利用シーン	運用フェーズ	作業概要
1	運用開始設定	初期設定	① 組織の作成 ② セキュリティグループ作成 ③ アカウント作成 詳細は **2.3.1 節**参照
2	アカウント変更・削除	日常運用	利用者情報の変更・削除 ① 利用者の退職等による削除 ② 利用者の OTP、パスワードリッセット ③ 利用者の部署移動 詳細は **2.3.2 節**参照
3	権限の付与	日常運用	部門ごとに付与した権限をベースに、個人やグループへの個別設定方法 ① セキュリティグループの詳細設定 ・リモート接続（SecureGateway 設定の ACL） 詳細は **2.3.3 節**参照
4	アクセスログ	日常運用	RemoNavi SaaS の操作ログの参照と保存と定期監視について 詳細は **2.3.4 節**参照
5	リモート接続ログ	日常運用	RemoNavi リモート接続通信ログの参照と保存と定期監視について 詳細は **2.3.5 節**参照
6	シングルサインオン	構成更新	シングルサイオンの SP としての設定について 詳細は **2.3.6 節**参照

表 4 利用シーンの一覧（セキュリティ管理者）

	利用シーン	運用フェーズ	作業概要
1	セキュリティ規定	初期設定 日常運用	① セキュリティ規定書、セキュリティ対策基準の設定 ② セキュリティインシデント発生時の対処動作確認 詳細は **2.4.1 節**参照
2	セキュリティ検査	日常運用	① セキュリティ定期試験のスケジュール作成 ② セキュリティ検査（試験）の作成・運用 詳細は **2.4.2 節**参照
3	セキュリティインシデントの発生対応	日常運用	利用者がセキュリティインシデントを発生させた場合の管理者としての対応 詳細は **2.4.3 節**参照

表 5 利用シーンの一覧（利用者）

	利用シーン	運用フェーズ	作業概要
1	トップページ	日常運用	利用機能で今すべき項目を抽出して表示します 詳細は **2.5.1 節**参照
2	リモート接続の利用	日常運用	リモート接続の利用方法について 詳細は **2.5.2 節**参照
3	タスク管理の利用	日常運用	タスク管理機能の利用方法 詳細は **2.5.3 節**参照
4	チャットの利用	日常運用	チャット機能の利用方法 詳細は **2.5.4 節**参照
5	個人メモの利用	日常運用	個人メモの利用方法 詳細は **2.5.5 節**参照
6	全体通知の利用	日常運用	全体通知の表示方法 詳細は **2.5.6 節**参照
7	セキュリティ検査の実施	日常運用	セキュリティ検査による試験の回答と合格承認の獲得 詳細は **2.5.7 節**参照
8	セキュリティインシデントの発生対応	日常運用	セキュリティインシデントを発生させた場合の対応は、セキュリティ管理者の利用シーンにまとめて記載
9	ビデオチャットの利用	日常運用	ビデオチャット機能の利用方法 詳細は **2.5.8 節**参照
10	データ分析の利用	日常運用	名寄せ、回帰分析の利用方法 詳細は **2.5.9 節**参照
11	ImageBox の利用	日常運用	画像、動画の保存利用方法 詳細は **2.5.10 節**参照

2.2. 共通操作 ★

2.2.1. 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。

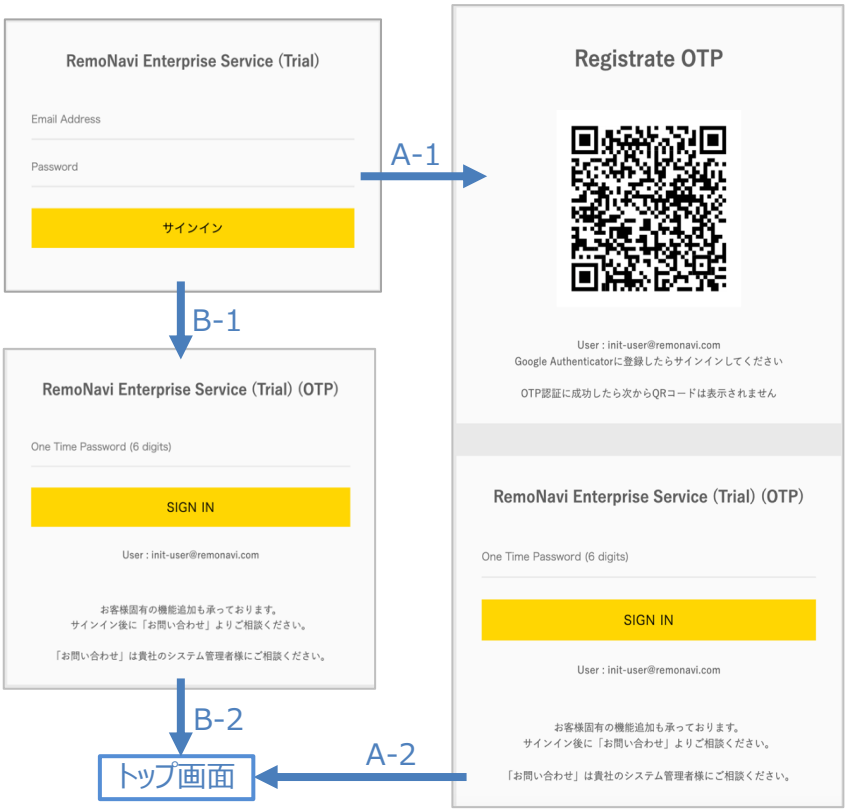


図 2 ログイン画面

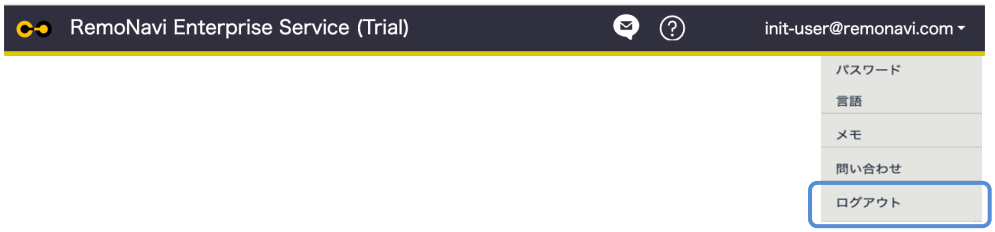


図 3 ログアウト画面

2.2.2. 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。

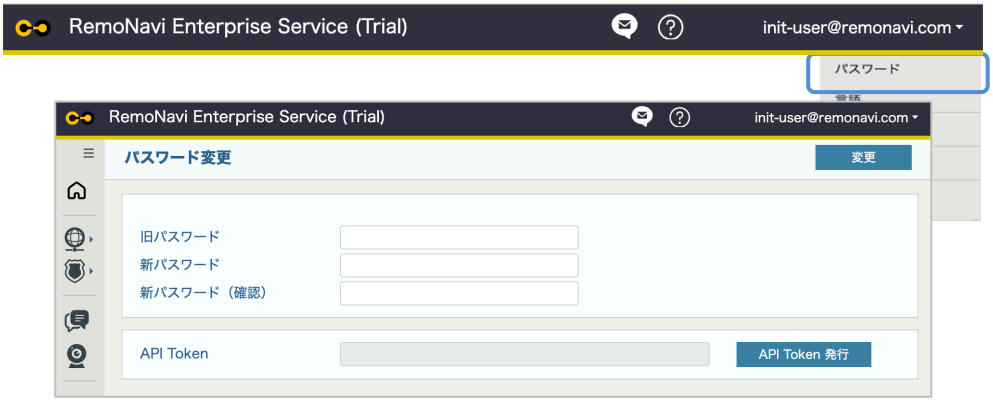


図 4 パスワード変更画面

もしパスワードを忘れてしまった場合は、システム管理者に依頼してパスワード設定してもらった後にログインして、本画面にてパスワードを再設定してください。

2.2.3. 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。

エンタープライズ版では、利用者自らが OTP リセットはできないよう設計されています。
リセットが必要な場合は、システム管理者に依頼して OTP リセットを依頼してください。

2.2.4. API Token 発行･削除

2.2.2 パスワード変更 の「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 48 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。

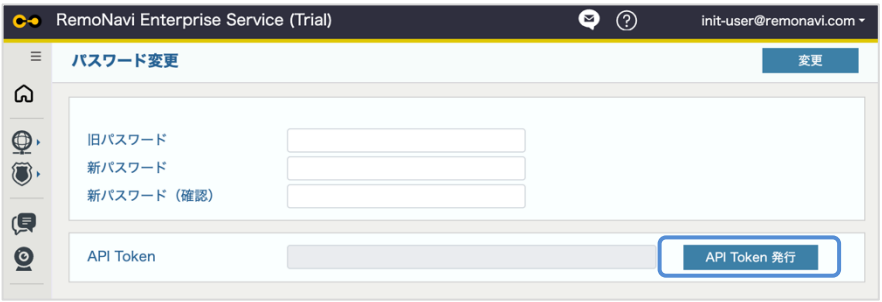


図 5 パスワード変更画面 （API Token）

2.3. 「管理者」の操作 ★★★

2.3.1. 運用開始設定

エンタープライズ版の初期状態には以下の情報が設定されています。

- 初期ユーザーアカウント
- セキュリティグループ２つ（フルアクセス利用可能、フルアクセス利用不能）
- セキュリティ検査：幾つかの試験サンプル
- タスク管理：幾つかの管理グループ（進捗管理、メンバ週報管理、IT システム管理）

システム管理者は以下の作業をする必要があります。

① システム管理者の作成
- 初期アカウントとは別に、実際のシステム管理者の Email アドレスでアカウントを作成、初期アカウントは削除することを推奨します。 この SaaS では設定した Email アドレスにメール送信することもあるためです。

② 組織情報の作成（省略可能） 参照（2.3.1.1 組織情報の生成）

③ セキュリティグループの生成 参照（2.3.1.2 セキュリティグループの生成）

④ アカウント生成 参照（2.3.1.3 アカウント生成）
- アカウントは、画面から１人ずつ作成する以外に、CSV ファイルによる一括作成もできます。

2.3.1.1. 組織情報の生成･変更

組織は３段階の構成をサポートしています。 名称を「部」、「課」、「グループ」としていますが、必要に応じて読み替えて利用してください。作成方法は、上位から作成し、下位を登録していきます。

1） 組織の生成

組織の生成は、サイドメニュー「アカウント/組織」から、「組織･画面」を表示して操作します。

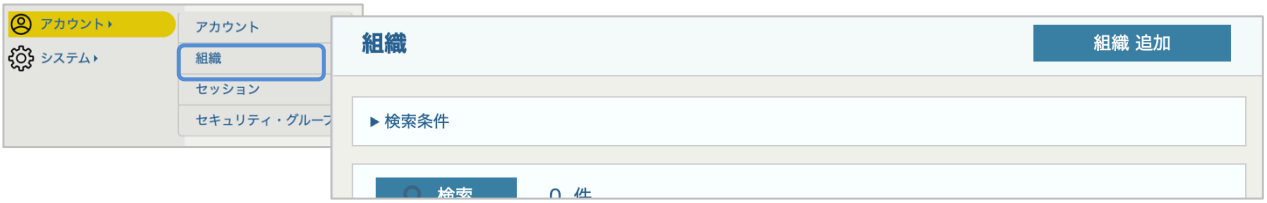


図 6 組織･画面（サイドメニュ：アカウント/組織）

図 7 組織追加･画面（組織追加）

「組織の登録」は「部」、「課」、「グループ」によらず、上記画面にて登録します。

① 部の作成は、入力項目「部」に作成したい名称を入力して、「部・追加」を押下します。

② 部の中の「課」を作成する場合、「部」の入力エリアでマウスをクリックすると、すでに作成した「部」の選択リストが表示され、選択することで入力できます。 選択せずに文字入力することも可能です。 続いて、「課」に作成したい名称を入力して、「課・追加」 を押下します。

同じ要領で、「グループ」も作成することができます。

2) 組織の変更

組織の生成は、サイドメニュー「アカウント/組織」から、「組織・画面」を表示して操作します。

図 8 組織・画面（組織作成後）

組織を作成すると、上記のように表示されます。

組織名称の部分一致で検索することが可能です。 変更はこの組織一覧の当該行をダブルクリックして、変更画面を表示し、変更する名称を入力して「変更」を押下します。

図 9 組織変更・画面

2.3.1.2. セキュリティグループの生成

セキュリティグループは、利用者の「操作権限」と「利用可能なリモート接続（SecureGateway)」を設定できます。以下に操作権限の一覧と説明をします。

表 6 セキュリティ・グループの機能権限一覧

機能	操作権限	対象操作
セキュリティ・グループ	参照（*）	操作、利用権限の参照
	設定（*）	操作、利用権限の設定
アカウント	参照（*）	アカウント、部署の参照
	設定（*）	アカウント、部署の設定
セッション	参照（*）	ログイン中のセッションの参照
通知	参照	全体通知の参照
	設定（*）	全体通知の設定
アクセスログ	参照（*）	操作履歴ログの参照
	設定（*）	操作履歴ログのダウンロード、削除
システム情報	参照（*）	システムの各種情報
シングルサインオン	参照（*）	シングルサインオン SP 機能の設定情報の参照
	設定（*）	シングルサインオン SP 機能の設定
SecureGateway	通信	SecureGateway によるリモート通信
	参照	SecureGateway の参照
	設定	SecureGateway の登録・変更・削除 この権限に加え、リモート接続の利用権限がないと変更、削除はできません。
	管理者操作（*）	以下の機能の全て(参照含む) - SecureGateway AccessLog - SecureGateway Session 一覧 - SecureGateway 通信量
インシデント管理	参照	セキュリティ・インシデント機能、セキュリティ検査機能の参照
	設定	セキュリティ・インシデントの対処フローの利用 セキュリティ検査の回答
	管理者操作	セキュリティ・インシデントの対処フローの承認・責任者 セキュリティ検査の試験問題の作成・公開・集計
タスク管理	参照	タスクの参照。 タスクはグループ毎に利用者設定があり、自身が所属しているグループのみ参照可能です。
	設定	タスクの登録、削除、変更、投稿。
チャット	参照	チャットの参照。 チャットはグループ毎に利用者設定があり、自身が所属しているグループのみ参照可能です。
	設定	チャットの登録、削除、変更、投稿。
ビデオチャット	参照	ビデオチャットの参照
	設定	ビデオチャットの登録・削除
Image Box	参照	動画、画像ボックスの参照
	設定	動画、画像ボックスの投稿、削除
MyPage	参照・設定	トップ画面の参照で、この設定は利用者なら必ず設定すべきです。 トップ画面の設定権限項目はありません。ユーザカスタマイズ用の予約です。

（*）管理者のみに権限設定することを強く推奨します。

生成は、サイドメニュー「アカウント/セキュリティ・グループ」から、「セキュリティ・グループ一覧・画面」を表示して操作します。

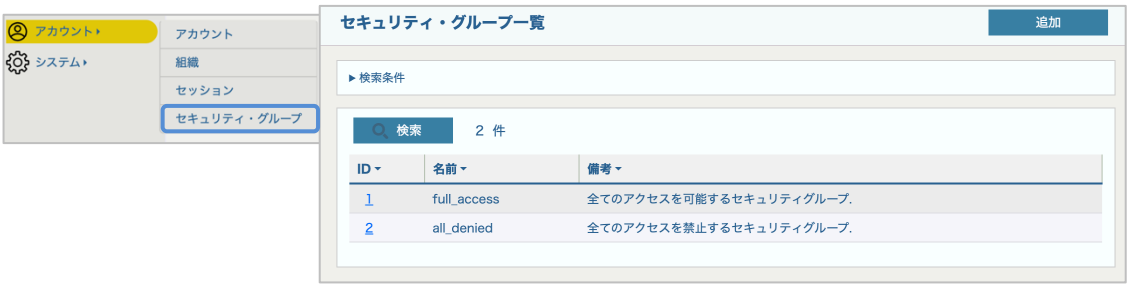


図 10 セキュリティグループ一覧・画面（サイドメニュ：アカウント/セキュリティ・グループ）

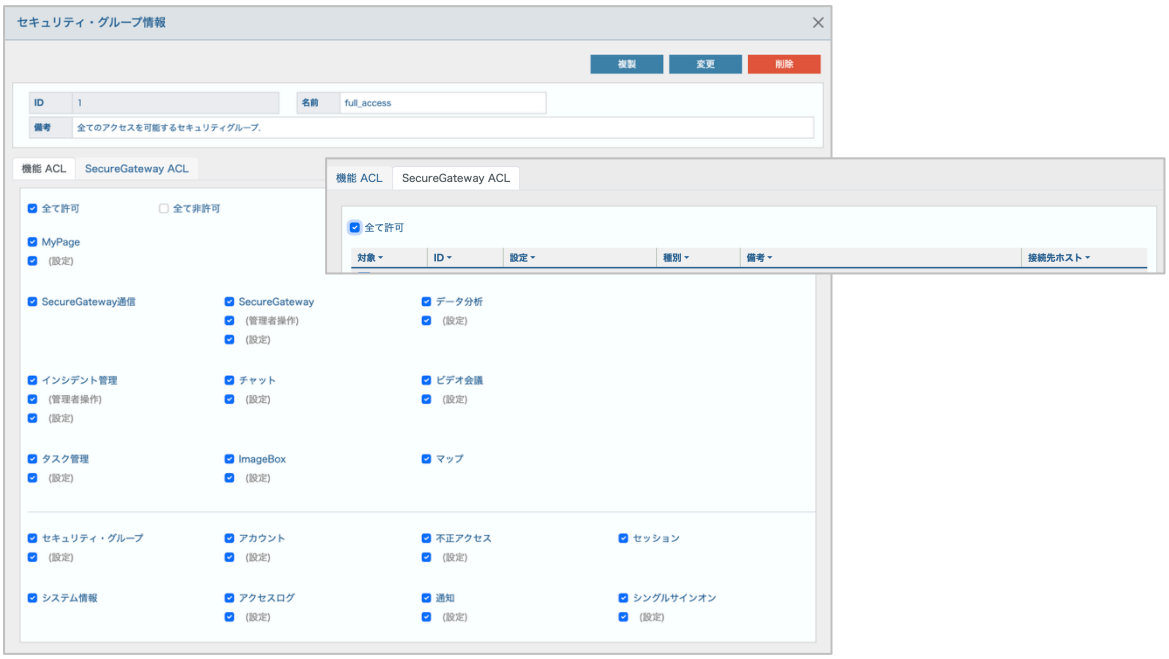


図 11 セキュリティ・グループ追加・画面（一覧画面からモーダル表示）

一覧画面の「追加」から、「セキュリティ・グループ追加」画面がモーダル表示されます。

名前と備考の入力に加え、2 種類に大別される、「利用可能な画面操作」と「リモート接続(SecureGateway)の利用」を設定します。

- 名前 ： 重複した名前で生成することはできません。
- 利用可能な画面操作
  「利用可能な機能」と当該機能の「参照のみ」、「参照・設定利用」の利用範囲を設定することが可能です。
  - 「利用可能な機能」の利用範囲を全て未設定にすると、その機能は利用できなくなります。 この場合、画面のメニューも一切表示されなくなります。
  - 利用可能な機能は、お客様とのご契約によって提供する機能のみが表示されます。
- リモート接続(SecureGateway)設定
  リモート接続の登録がある場合「SecureGatewayACL タブ」には全ての登録一覧が表示され、その中から利用可能なものを選択します。 リモート接続の設定は安全のために生成時は「未設定」にしておくことを推奨します。

変更・削除については、2.3.3 権限の付与 にて別途説明します。

【注意事項】
このセキュリティ・グループ機能も、利用可能機能の一つです。もし全てのアカウントに、この権限のないセキュリティグループを割り当ててしまった場合、誰も権限設定をできなくなってしまいます。
この場合、SaaS 運用会社によって管理データを直接編集する以外に方法がないため、十分注意して設定してください。

【運用のヒント】
セキュリティグループには「複製」機能があります。 運用においては、担当者と責任者のように若干の権限の違いをつけると思いますが、それらは運用開始設定後に「複製」を使って各部門長と相談しながら詳細設定することができます。
また、セキュリリティ・グループの権限はこのシステムで最も重要なものです。基本は情シスのみで管理し、運用中の各部門の依頼を受けて情シスが設定することをお勧めします。

2.3.1.3. アカウント生成

アカウントの作成方法は 2 種類あります。
運用開始時は、CSV ファイルによる一括作成が効率的で、入社、退職対応などでは画面から 1 人ずつ対応します。
アカウントの操作は、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」を表示して操作します。

図 12 アカウント一覧・画面（サイドメニュ：アカウント/アカウント）

1） 画面から 1 人ずつ作成

一覧画面の「アカウント追加」から、「アカウント追加」画面がモーダルを表示して操作します。

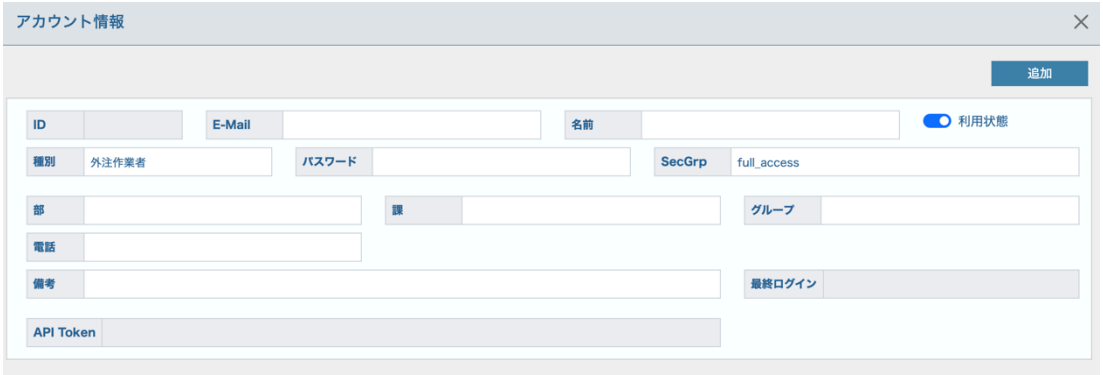


図 13 アカウント追加・画面（一覧画面からモーダル表示）

「部署、電話、備考」は設定省略可能です。
「種別」は、「システムア管理者」のみ削除できない特別な制約がありますが、それ以外はただの識別でしかありません。

SecurityGrp(セキュリティグループ) と 部署は、マウスをクリックすると選択リストが表示されますので、選択入力してください。

図 14 アカウント追加の完了時に表示される一覧画面

追加に成功すると追加の確認画面を経て、上記のように「アカウント一覧画面に「E-Mail を検索条件」とした一覧表示をします。 アカウント全体を再表示する場合は、「検索条件クリア」で条件削除をしたのちに、「検索」してください。

当該アカウントを表示する場合は、当該行をダブルクリックするか、E-Mail 列のリンクをクリックしてください。
アカウント情報画面がモーダル表示されます。

2) CSV ファイルによる一括作成

一覧画面の「CSV 一括追加」を押下すると「ブラウザ標準の CSV ファイル選択ダイアログ」表示されます。作成した CSV ファイルを選択してください。
CSV ファイルフォーマットが以下です。

種別, E-Mail, 名前, 電話, パスワード, SecurityGrpID, 部 ID, 課 ID, グループ ID, 備考, 状態

- UTF-8、カンマ区切り
- 種別　[1]システム管理者、[2]業務責任者、[3]業務担当者、[4]外注作業者
- xx ID　セキュリティグループ、部署、は画面に表示される ID 数値を指定してください
- 状態　[1]利用可能 , [0]利用不可

追加に成功すると、アカウント一覧画面が再表示されます。1 人作成とは異なり、検索条件は設定されませんので、必要に応じて検索してください。
登録はアトミック操作です。1 人でも登録に失敗したら登録されません。

【注意事項】
作成したアカウントが、他の機能で利用された場合、当該アカウントの削除は可能ですが、内部的には削除フラグを設定するだけでデータとして残しています。 これは削除アカウントが作成したリソースを表示することや、セキュリティ・インシデント、検査の記録などに紐づいているからです。
そのため、**一度もログインしていない利用者だけは「アカウント削除」はデータが完全に削除されますが、それ以外は削除フラグの設定で削除され、同一 E-Mail アドレスで再生成することはできなくなります。**
こうした問題を回避するためには、「利用状態」を利用停止にする運用をお勧めします。

2.3.2. アカウント変更・削除（パスワード,OTP リセット含む）

アカウントの操作は、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」を表示して実施します。

次に一覧表示されたアカウント行のダブルクリックないしは、E-Mail 列のクリックをして、アカウント情報モーダル画面を表示して操作します。

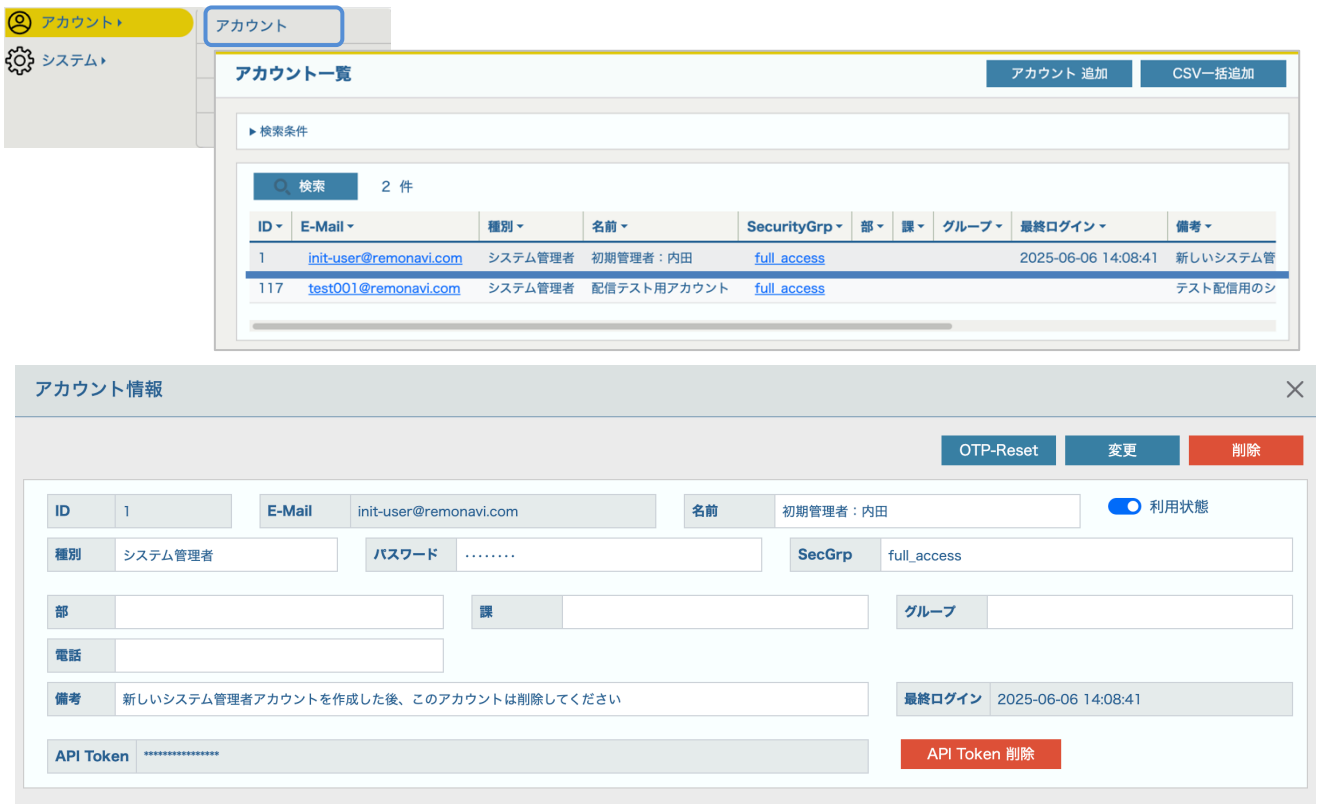


図 15 アカウント情報・画面（一覧画面からモーダル表示）

1） OTP リセット

アカウント情報・画面 の「OTP-Reset」を押下することでリセットできます。

エンタープライズ版では、OTP リセットはこの画面からのみ操作可能です。 これはアカウント乗っ取り対策として、利用者によってリセットすることはできないようにしているためです。リセットは管理者による操作としてください。

2） アカウント情報「変更」

変更内容を入力して「変更」ボタンを押下することで実施します。

- 「アカウントの利用停止」はこの操作で実施します。
- 利用者がパスワードを忘れてしまった場合、ここでパスワード 情報を入力して、「変更」することができます。
- E-Mail 情報は重複設定が不能です。
- API Token の発行・削除はここからの操作でも可能です。

3） アカウント情報「削除」

「削除」ボタンを押下することで実施します。 アカウント情報の削除に大きな制約があります。

一度作成したアカウントで、一度でもログインしたアカウントは削除することは可能ですが、再生成することはできない点で、これは「2.3.1.3 アカウント生成」の注意事項で記載した通りです。

【注意事項】
種別が「システム管理者」のアカウントは削除できません。 削除する場合は、種別を変更したのちに削除してください。

2.3.3. 権限の付与

2.3.3.1. セキュリティ・グループの設定変更

アカウントの操作は、サイドメニュー「アカウント/セキュリティ・グループ」から、「セキュリティ・グループ一覧・画面」を表示して実施します。 次に一覧表示されたセキュリティ・グループ行のダブルクリックないしは、ID 列のクリックをして、セキュリティ・グループ情報モーダル画面を表示して操作します。

図 16 セキュリティ・グループ一覧・画面（一覧画面からモーダル表示）

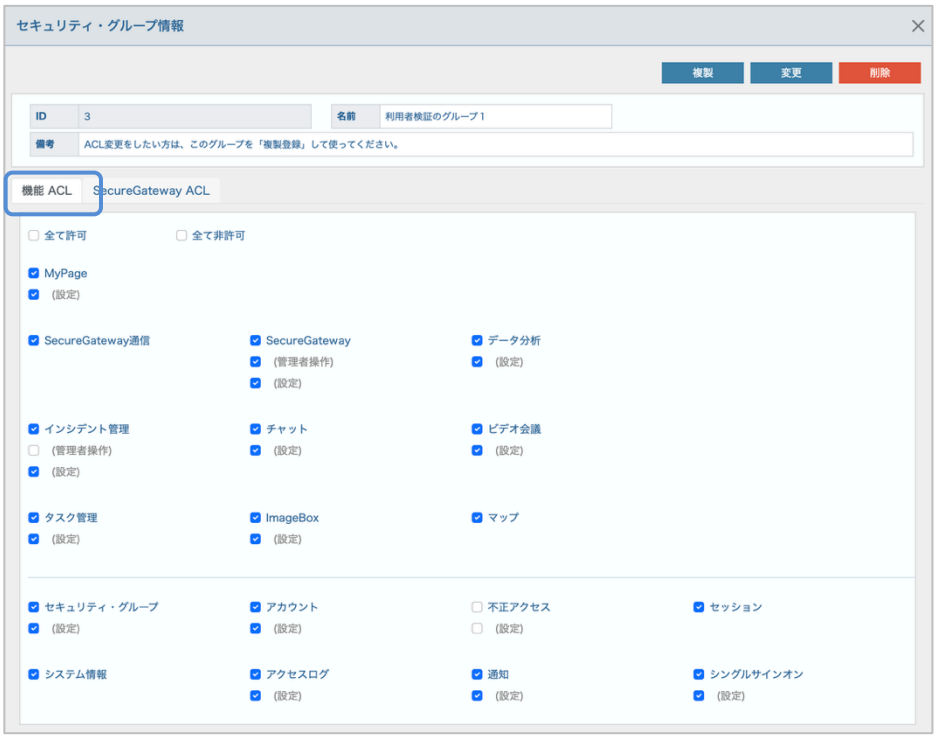


図 17 セキュリティ・グループ情報・画面（機能 ACL 設定タブ）

図 18 セキュリティ・グループ情報・画面（一覧画面からモーダル表示）

セキュリティ・グループ情報は、2.3.1.2 セキュリティグループの生成 の通り、「利用可能な機能」と「利用可能な SecureGateway(リモート接続)」の２種類の設定があります。

情報変更では、名前、備考に加え、これらの情報の変更設定をして「変更」ボタンを押下することで実施します。

名前を変更する際には、変更する名前のセキュリティ・グループがすでに存在する場合は変更できません。

【重要項目】
利用者が「リモート接続(SecureGateway)」を登録しても、セキュリティ・グループで「全て許可」になっていなければ、登録利用者はそのリモート接続を利用することはできません。 利用可能にするには、管理者によってこのセキュリティ・グループで許可設定をしなければなりません。 この仕様により管理者による利用管理を実現しています。

2.3.3.2. セキュリティグループの複製

セキュリティグループは複製ができます。 複製は、変更操作の手順で、「セキュリティ・グループ情報・画面」を表示し、「複製」ボタンを押下することで実現します。

複製の際には、以下の情報を変更入力して、実施する必要があります。

- 名前 ： 重複しない名前を指定する必要があります。
- 備考 ： 変更は必須ではありませんが、複製したことがわかる説明を入力しておくことを推奨します。

2.3.4. 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。

重要）アクセスログは一般利用者に解放すべきではありません。 システムではログの自動削除は一切していませんが、手動で削除することができるからです。 参照権限についても、管理者以外に解放すべきではありません。 不正操作者に不正操作の記録があること周知することには、なんらメリットがないからです。

図 19 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 20 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。 本操作は、即時確認のためのものです。 アクセスログは定期的にダウンロードし、ダウンロードしたファイルは削除することを推奨しております。
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。
3	削除	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「削除」ボタンを押下します。

検索時のヒント）

検索文字列にはヘルプにある「アクション名」や、利用者の「E-Mail」を入力するとことで効率よく検索できます。

2.3.5. 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。

重要）リモート接続ログ（SecureGateway AccessLog）は一般利用者に解放すべきではありません。 システムではログの自動削除は一切していませんが、手動で削除することができるからです。 参照権限についても、管理者以外に解放すべきはありません。 不正操作者に不正操作の記録があること周知することには、なんらメリットがないからです。
リモート接続ログ（SecureGateway AccessLog）の権限は、セキュリティ・グループにて 「SecureGateway 管理者操作」にて設定可能です。

図 21 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 22 ヘルプ画面（Gateway アクセスログ）

テナント ID は、シェアサービス時の識別に利用されるもので、エンタープライズ版では以下のように設定されます。

[-] 接続開始ログ（まだ利用者が確定していない通信の開始ログ｜異常通信ログ）

[0] 接続完了ログ（利用者が確定している通信の終了ログ）

【SecureGateway アクセスログの特記事項】

SecureGateway 接続は暗号化と通信に先立って API Token による認証シーケンスをしています。そのため接続時は利用者が不明です。 そのため以下のように接続時と通信完了時にそれぞれログ出力をすることで、現状やそれらの不正アクセス解析をすることができるようになっています。

- TCP/IP 接続してきて、SSL 接続確立が異常

-,24/08/12 14:12:18,-,start,282,87.236.176.6,-,-,-,0,0,-
-,24/08/12 14:12:18,24/08/12 14:12:18,err,282,87.236.176.6,-,-,-,0,0,ssl-handshake-error

- ssh 接続してきて、認証シーケンスが異常

-,24/08/12 23:50:25,-,start,283,35.203.210.22,-,-,-,0,0,-
-,24/08/12 23:50:25,24/08/12 23:50:25,err,283,35.203.210.22,-,-,-,0,0,illegal-client

- 正常な通信ログ

-,24/08/12 13:11:05,-,start,239,-,-,-,-,0,0,-
0,24/08/12 13:11:05,24/08/12 13:11:05,ok,239,122.26.1.23,remonavi,remonavi.com:443,test@remonavi.com,77482,1633,-

通信にはシーケンシャルに番号が振られます。 上記の異常は実際によくあるもので、欧米の監視サイトなどが定期的に、TCP 接続状況、SSH 接続状況などの情報作成をしています。 これらのログから、専用サーバで運用しているエンタープライズ版では発 IP アドレス制限を SaaS 運営社に依頼するなどして、通信を制限することも可能です。

【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。 本操作は、即時確認のためのものです。 アクセスログは定期的にダウンロードし、ダウンロードしたファイルは削除することを推奨しております。
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。
3	削除	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「削除」ボタンを押下します。

2.3.6. シングルサインオン

シングルサインオンの SP 機能を提供します。

シングルサインオンの SP 機能では、ログイン時に登録した IDP の認証を経て、この RemoNavi SaaS にログインすることになります。 このシステムのログイン画面は経由しません。

認証は IDP にて実施されますが、このシステムでのアカウント登録は必須です。そのため、シングルサイオンを採用する場合でも、このシステムのアカウント管理は必要であることを忘れないでください。

図 23 シングルサインオン IDP 設定画面

空欄は IDP 運用会社から提供されるものを設定してください。また IDP 運用会社からは SP 情報の提示を求められますので、上記 EntityID, URL を提供してください。

IDP との通信で利用される SAML メッセージは IDP 運用者毎に若干の差異があり、うまく接続できない可能性もあります。その場合、当該メッセージを共有いただければ、対応いたしますので、ご要望ください。

2.4. 「セキュリティ管理者」の操作

セキュリティ運用におけるセキュリティ管理者は、本システムはセキュリティ・グループの権限設定で実現されます。具体的には 表 6 セキュリティ・グループの機能権限一覧 の通り、「インシデント管理/管理者操作」 権限が設定された社員となります。

セキュリティ管理者に許可された権限は、「インシデント発生時の対処フローの承認者」と「セキュリティ検査（試験）の実施」です。

2.4.1. セキュリティ規定

情報セキュリティ対策では、以下の２つを定めることが必須とされています。

① 情報セキュリティ規定書

② 情報セキュリティ対策基準

エンタープライズ版では情報セキュリティ対策の実運用を考慮した形で、これらの書類が作成され、サンプルとして提供しています。 もし、これらの規定がまだ策定されていない、あるいはすでにある場合は、以下をそのまま利用するか、「置き換え」によって自分等で策定したものをアップしておくことをお勧めします。

なぜなら、社員のほとんどがこうした書類に一度も目を通したことがない、その理由がファイルの存在をしらないからです。

図 24 セキュリティ規定・画面

2.4.2. セキュリティ検査

情報セキュリティには３つの脅威があります。

「物理的脅威」、「技術的脅威」、「人的脅威」

いかなる技術的、物理的施策も、完全なセキュリティ対策とは言えません。それはそれらを駆使するのが人だからです。

RemoNavi SaaS この「人的脅威」にアタッチすべく、セキュリティ検査機能を具備しています。 セキュリティ検査の具体的な機能は、定期的なセキュリティ試験の実施と集計です。

ただ試験をするのではなく、試験に合格するまで試験完了状態にしない、などの工夫が組み込まれています。 また試験は独自に作成することが可能なため、利用社様の状況の即した試験の実施も可能となっています。

セキュリティ検査の管理者操作は、サイドメニュー「インシデント管理/セキュリティ検査（管理）」から、「セキュリティ検査・一覧」を表示して操作します。

図 25 セキュリティ検査一覧・画面

1） 検査情報の作成

一覧画面の「追加」ボタン を押下すると、検査情報の登録画面が表示されます。

セキュリティ検査では、以下の試験が可能です。

① アンケート形式

② 試験形式（合格不問）

③ 試験形式（合格必須）

設問数は 最大 20 まで。

設問の回答形式は、以下の２種類が可能です。

① 単一選択

② 複数選択

検査の実施は、生成後の「情報変更」にて、「回答期限」と「状態：検索中」にすると、全社員に検査内容が公開されます。 公開されると、トップ（MyPage 画面）の「未完了セキュリティ検査」覧に表示されます。

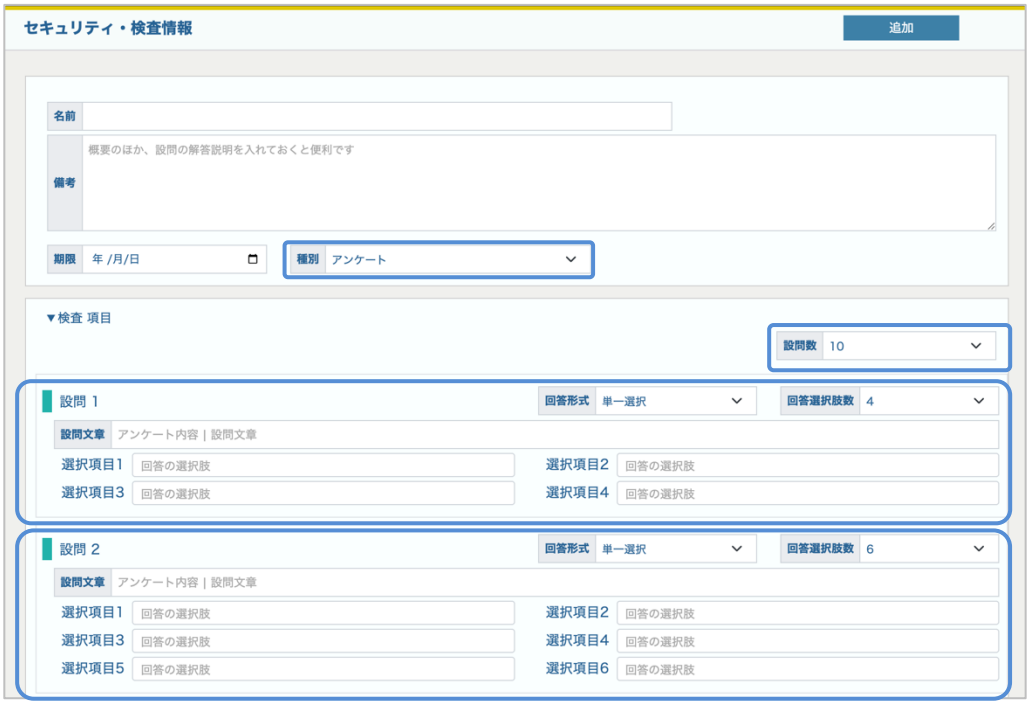


図 26 セキュリティ検査 [登録]・画面（アンケート作成）

図 27 セキュリティ検査 [登録]・画面 (試験作成)

2) 検査情報の変更と検査実施

作成した検索項目は、一覧画面の当該行のダブルクリックないしは、ID 列のリンクをクリックして、セキュリティ検査情報画面を表示して操作します。

図 28 セキュリティ検査一覧からのセキュリティ検査情報画面の表示

- 検査情報画面から、「編集」ボタンを押下すると編集モードとなり、編集可能な項目が入力可能となります。
  - 変更内容を入力して「変更保存」ボタンを押下することで実施します。
  - 検査の実施は、生成後の「情報変更」にて、「回答期限」と「状態：検索中」にすると、全社員に検査内容が公開されます。公開されると、トップ（MyPage 画面）の「未完了セキュリティ検査」覧に表示されます。

3） 検査情報の複製

セキュリティ・グループ機能と同様に「複製」があります。

一度実施した試験は、利用者が回答しているので、再度同じ試験をする場合は、この「複製」を使って検査情報を作成、「検査名」、「回答期限」などを編集して、再実行します。

複製の際には、以下の情報を変更入力して、実施する必要があります。

- 名前　：　重複しない名前を指定する必要があります。
- 備考　：　変更は必須ではありませんが、複製したことがわかる説明を入力しておくことを推奨します。

4） 検査結果の確認

編集同様、セキュリティ検査情報画面を表示して以下の項目を確認します。

検査 結果　：　アコーディオン表示になっています。

回答者、未回答者の一覧や件数を確認することが可能です。

もし、未回答者があまりに多い場合などは、全社員通知機能（参照 2.5.6 全体通知の利用）などで回答を促すなどの対応が必要です。少数の場合でも、未回答者一覧を全社員通知機能にするのも運用の一つです。

2.4.3. セキュリティインシデントの発生対応

どこからがセキュリティ・インシデントで、そうでないか、にはその企業での規定が必要なので、そこに言及はしません。
ここでは、セキュリティ・インデントとされる事象の発生があった場合にどのようにフロー管理するかについて説明します。
本システムでの操作には ①から⑥ までの番号を振ります。

表 7 セキュリティ・インシデント発生から完了までの対処フロー

事象	インシデント発生者	セキュリティ管理者
インシデント発生	AV ソフトによるウィルス検知なら Wifi 切断 後に被害状況を確認するため、自身で削除等はしない ①利用可能な PC からインシデント発生登録 セキュリティ管理者にインシデント発生が自動でメール送信されます ※自動でメール送信されますが、規定された管理者に電話連絡することが望ましい	→インシデント発生通知の受信 ①で登録されたインシデント内容の確認 ※被害拡大防止措置がなされていれば規定された手順の作業。 ※個人情報流出の恐れがある場合は即時対応
インシデント解析	セキュリティ管理者などの解析結果などを踏まえ、 ②インシデントの対処等を、インシデント項目に追記 ・関係先への連絡	②インシデントの対処等を、インシデント項目に追記 ・関係先への連絡 ・必要に応じた実施内容
対処	対処完了	
インシデント対処承認	②インシデントの対処等を、インシデント項目に追記 - 再発防止策 の記載 ③インシデント「完了承認申請」を要求 セキュリティ管理者にインシデント発生が自動でメール送信されます →インシデント完了承認 ⑥インシデント「完了承認受領」で完了 差し戻しの場合は②の再発防止の記載から再度実施	→インシデント完了承認要求の受信 ③の再発防止策を確認 ④再発防止の指摘事項を追記 再発防止に問題があれば ⑤インシデント「完了承認却下」で差し戻し インシデント発生者に自動でメール送信されます 再発防止に問題がなければ ⑤インシデント「完了承認却下」で差し戻し インシデント発生者に自動でメール送信されます

注意）「申請、承認、却下」 をする前に、それぞれ必要な情報を入力・変更してください。

セキュリティ・インシデントの操作は、サイドメニュー「インシデント管理/インシデント一覧」から、「セキュリティ・インシデント一覧」を表示して操作します。

図 29 セキュリティ・インシデント一覧・画面

1） インシデント発生時の報告 （インシデント発生者）

一覧画面の「追加」から必要情報を入力して登録します。

登録すると、セキュリティ管理者全員に、インシデント通知メールが送信されます。

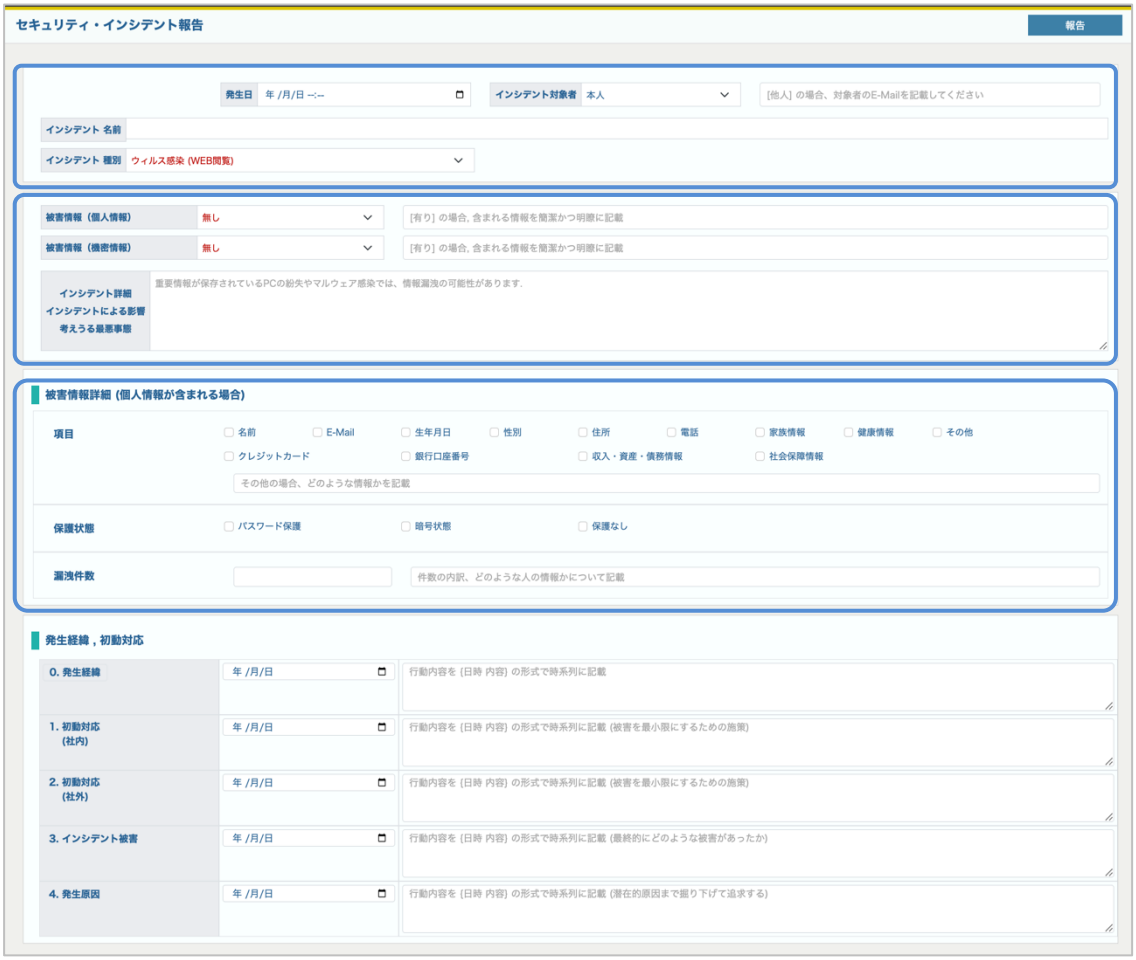


図 30 セキュリティ・インシデント登録画面

入力項目は、画面の内容に従って入力してください。

上記の囲み部分は、個人情報や機密情報の漏洩の可能性に言及する項目です。 漏洩があったか、なかったかは端末や社内通信状況の調査をしないと不明なので、当該端末にインシデントが発生し、感染があった前提で記載します。

2） インシデント報告後の、詳細情報の追記 （インシデント発生者、セキュリティ管理者）

報告後は、インシデント発生者、セキュリティ管理者がコミュニケーションをとって、状況詳細を追記していきます。

記載したら「変更」で保存します。

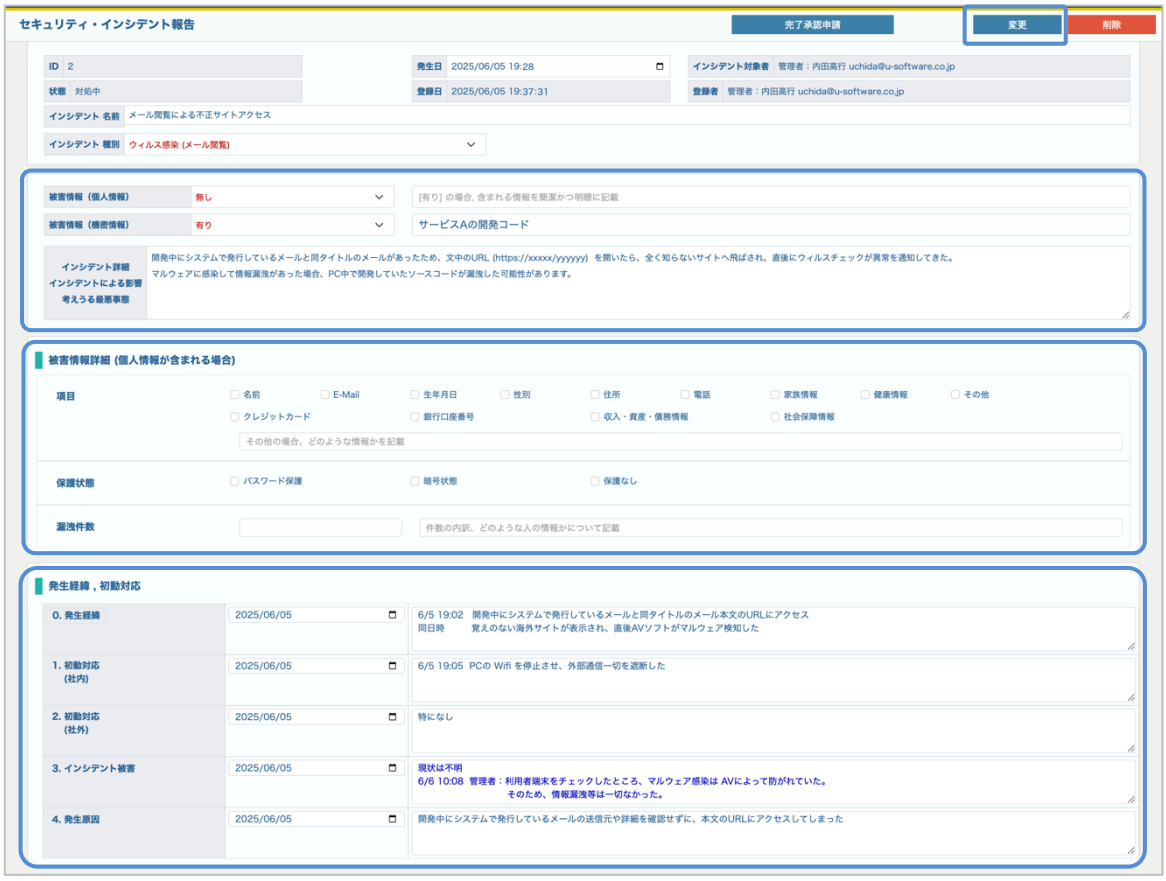


図 31 セキュリティ・インシデント情報（変更）画面

3） インシデント報告後の、詳細情報の追記（インシデント発生者）

インシデント対処が完了したら、インシデント発生者は、以下を記載して、インシデント情報の「変更」を完了させた後、「完了承認の申請」を管理者に要請します。申請すると、セキュリティ管理者にメール通知されます。

- 対処内容と関係者への報告
- 再発防止策
- 承認者

図 32 セキュリティ・インシデントの完了承認申請

4） インシデント完了承認申請の承認｜差し戻し（セキュリティ管理者）

セキュリティ管理者は、インシデント発生者の「再発防止策」を吟味し、その評価を記載して、インシデント情報の変更を完了させます。

そして、再発防止策に問題がなければ「完了承認」、問題があれば「完了承認却下」をします。

承認、却下いずれの場合でも、インシデント発生者にメール通知されます。

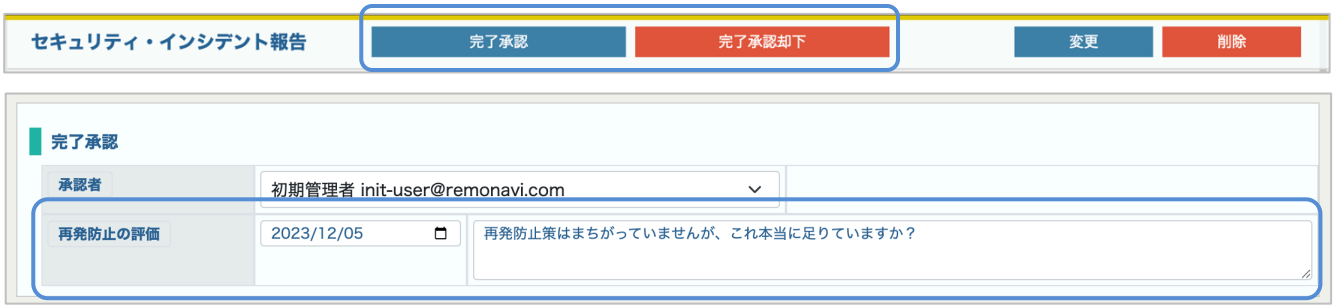


図 33 セキュリティ・インシデントの完了承認

却下の場合、インシデント発生者は指摘内容を反映した「再発防止策等」を記載して、再度「完了承認申請」をします。

5） インシデント完了承認の受領（インシデント発生者）

セキュリティ管理者の承認を受けたインシデント発生者は「受領」します。

これで一連のインシデントの管理フローが完了します。

図 34 セキュリティ・インシデントの完了承認の受領

2.5. 「利用者」の操作

2.5.1. トップページ

トップページは、セキュリティグループで利用可能な機能に限定して、利用者が今すべきことが抽出表示されます。
具体的には、以下が表示されます。

1) リモート接続（SecureGateway）の WEB 接続
   ✓ アイコンをクリックすると、リモート接続先の WEB ページを別タブで表示します。
2) セキュリティ・インシデント
   ① 自身が発生させたセキュリティ・インシデントの対処未完了なリスト
   ② 情報セキュリティ管理者（インシデント・フロー処理の承認者）の場合は、対処フロー中の承認要求リスト
   ✓ 当該行をダブルクリックか、ID 列のリンクをクリックすると、当該ページにジャンプします。
3) セキュリティ検査
   ① 回答しなければならないセキュリティ試験のリスト
   ✓ 当該行をダブルクリックか、ID 列のリンクをクリックすると、当該ページにジャンプします。
4) 担当タスク管理
   自身が担当している完了していないタスクのリスト
   ✓ 当該行をダブルクリックか、ID 列のリンクをクリックすると、当該ページにジャンプします。

図 35 トップ画面

2.5.2. 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 8 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 の配備方法の選択

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

- API Token 保持者に権限付与された「リモート接続設定」のみ利用可能です。
- Sender を使った通信は、設定した API Token 保持者の利用として SaaS 側の通信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 の配備方法について】

- 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
  - 利用者は設置された Sender に向けて送信するだけです。

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

- API Token 保持者に権限付与された「リモート接続設定」のみ利用可能です。

【Receiver の配備方法について】

- 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
  - 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。

以下の構成では、{利用者 A は 接続先 a1, a2} {利用者 B は接続先 b1, b2} への権限付与されるものとします。このケースで「Sender をネットワーク上に代表配置」すると、利用者 A が利用者 B の Sender を利用できます。こうした構成を許容するかの考慮は必要です。

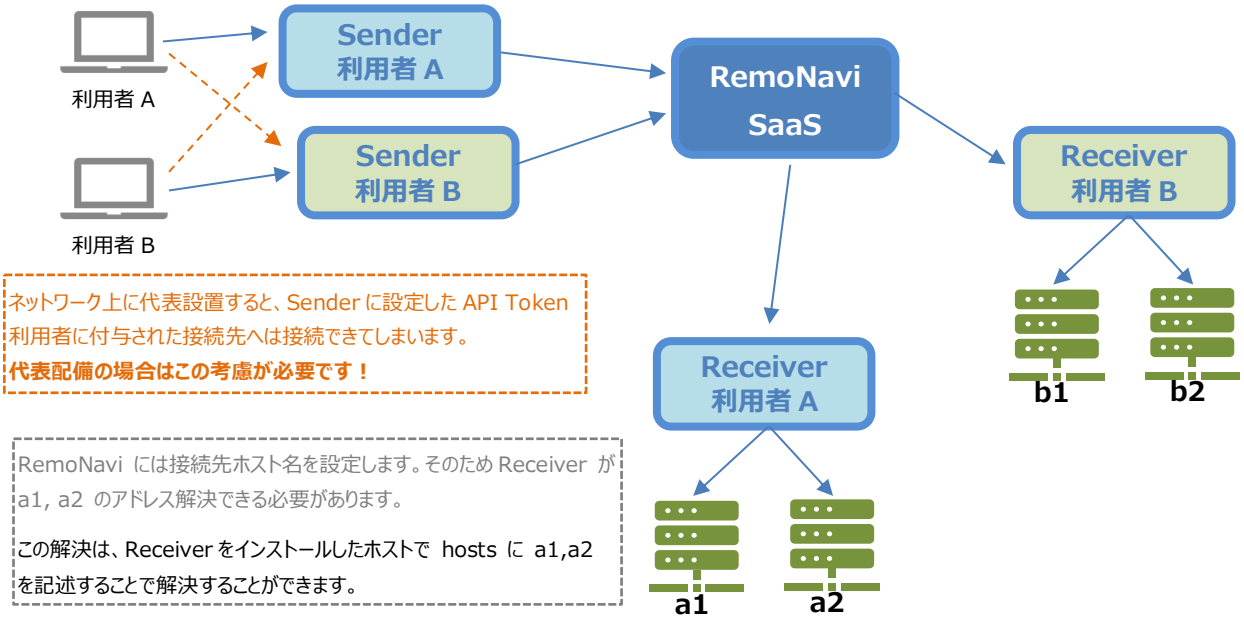


図 36 Sender|Receiver の配置イメージ

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。 表示される SecureGateway 一覧・画面には、以下の情報のみ表示されます。

① セキュリティ・グループで許可された SecureGateway (リモート接続)
② 自身が登録した SecureGateway (リモート接続)

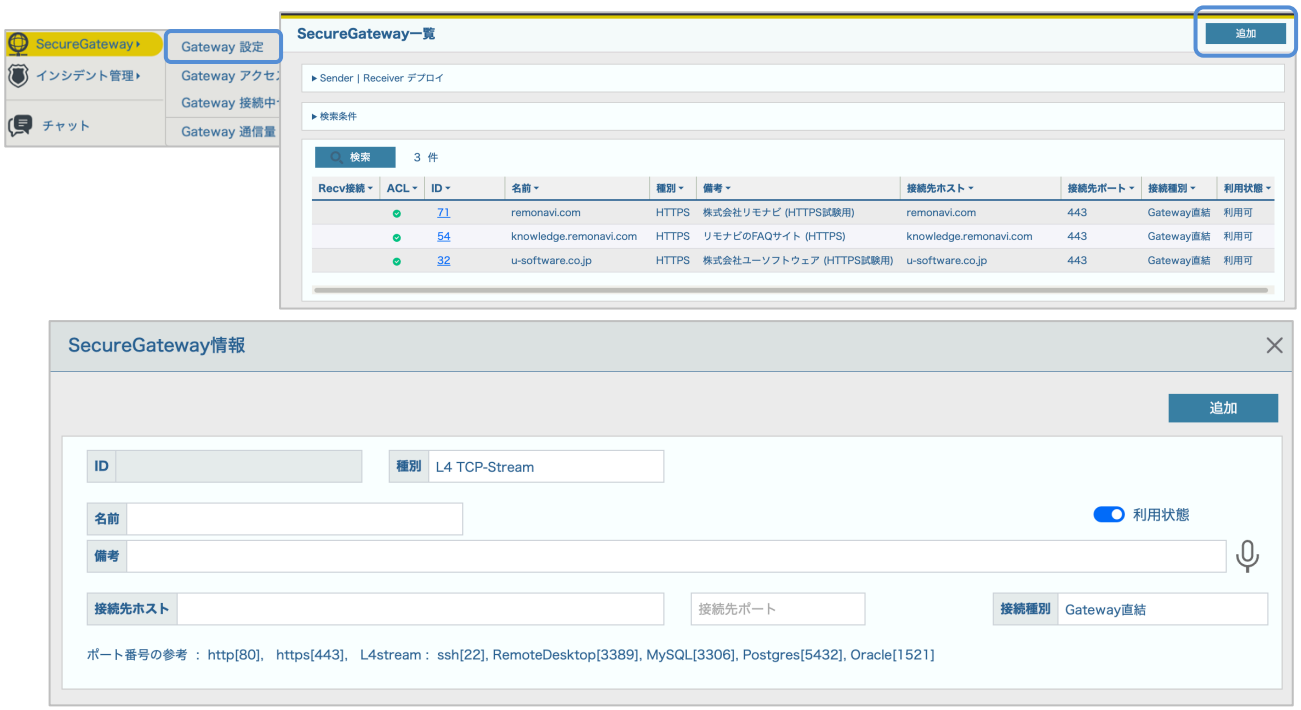


図 37 SecureGateway(リモート接続)一覧･画面 と SecureGateway 登録画面

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。

エンタープライズ版は、リモート接続の利用は管理者の許可なしにはできないようにしています。

そのため、利用者が SecureGateway(リモート接続)を登録しても、利用者のセキュリティ・グループが「全て許可」である以外は管理者によって当該 SecureGateway の利用を許可されない限り利用することはできません。

SecureGateway 一覧には、セキュリティ・グループで許可されたものと、自身が登録したもの、が一覧表示されます。

自身が登録したもので、セキュリティ・グループで許可されていないものが、ACL 列の 🔴 表示されます。

図 38 登録した SecureGateway(リモート接続)で許可されていない場合の ACL 表示

5) リモート利用の設定（SaaS での SecureGateway の 利用制限の設定）

SecureGateway(リモート接続) は、利用時間帯と Sender|Receiver からの接続 IP アドレス制限を設定することができます。

図 39 SecureGateway(リモート接続)の情報変更画面 （利用制限設定欄）

【入力項目】

	入力項目	説明
1	Sender｜WebAccess Src IP 制限	Sender 利用時の Receiver の Src IP アドレスのの、許可、非許可の IP アドレスをプレフィックスで指定します。 許可、非許可は許可が優先されます。 例) 192.168.84.0/24, 172.16.0.0/28 本設定は Gateway からの WEB アクセスにも適用されます。
2	Receiver Src IP 制限	Receiver 利用時の Receiver の Src IP アドレスのの、許可、非許可の IP アドレスをプレフィックスで指定します。 許可、非許可は許可が優先されます。 例) 192.168.84.0/24, 172.16.0.0/28
3	利用時間帯制限	利用可能な時間帯を 15 分単位 に指定します。 時刻文字列をクリックすると、1 時間単位の 利用 ON/OFF 設定ができます。

6) 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 （前節 4)RemoNavi エンタープライズ版のご利用に当たって）参照
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

7) 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 （前節 4)RemoNavi エンタープライズ版のご利用に当たって）参照
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)

8) 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。

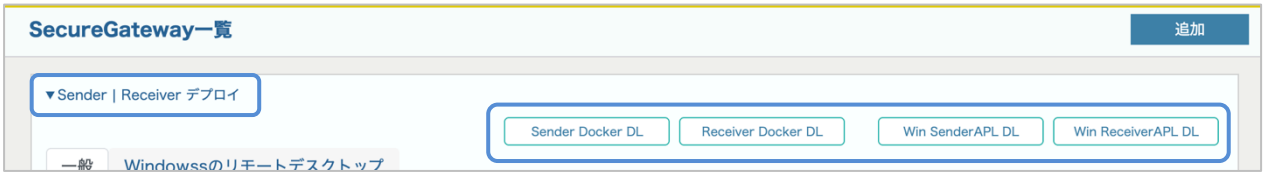


図 40 SecureGateway(リモート接続)一覧画面から Sender|Receiver ダウンロード

◆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。

9） 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）
Proxy Addr | Port	：	Proxy 経由の場合の Proxy 接続情報

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。

L7 通信による RemoNavi SaaS からの HTTPS による情報取得は Proxy 経由に対応しますが、L4 Stream は HTTP/HTTPS 通信ではないため、Proxy を通過させることができません。 もし Stream 通信を Proxy 通過させる必要がある場合には、カスタマイズ対応いたしますのでご相談ください。

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】

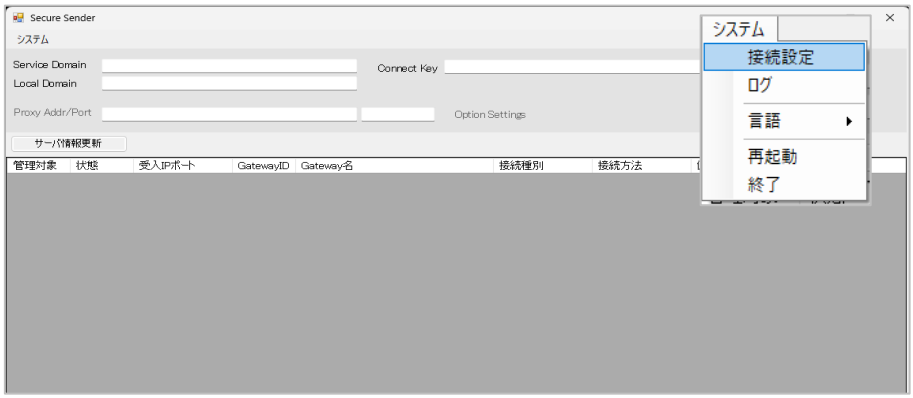


図 41 Windows Sender 管理画面（接続設定）

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。

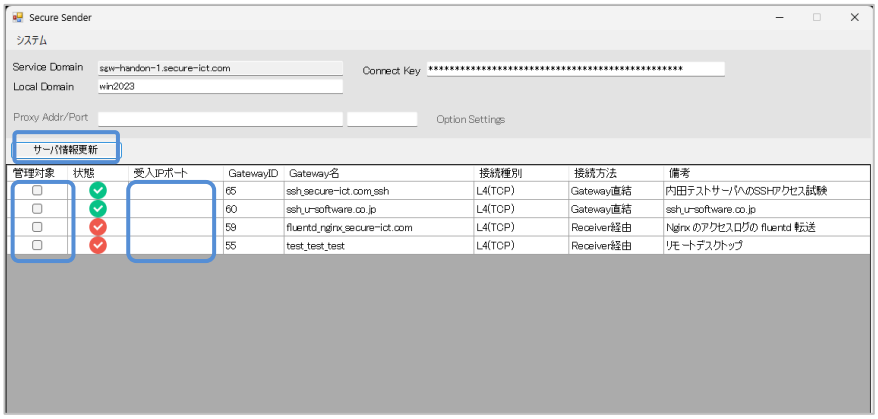


図 42 Windows Sender 管理画面（利用設定）

【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。

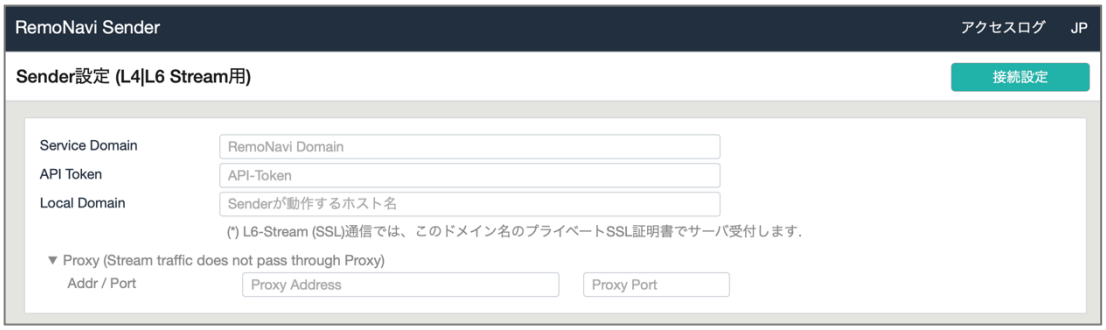


図 43 Sender Docker 管理画面（接続設定）

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 44 Sender Docker 管理画面（利用設定）

10) 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)
Proxy Addr | Port ： Proxy 経由の場合の Proxy 接続情報

正常に接続できたら、利用可能な Receiver 経由の SecureGateway 一覧を表示できるようになります。
L7 通信による RemoNavi SaaS からの HTTPS による情報取得は Proxy 経由に対応しますが、L4 Stream は HTTP/HTTPS 通信ではないため、Proxy を通過させることができません。 もし Stream 通信を Proxy 通過させる必要がある場合には、カスタマイズ対応いたしますのでご相談ください。

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】

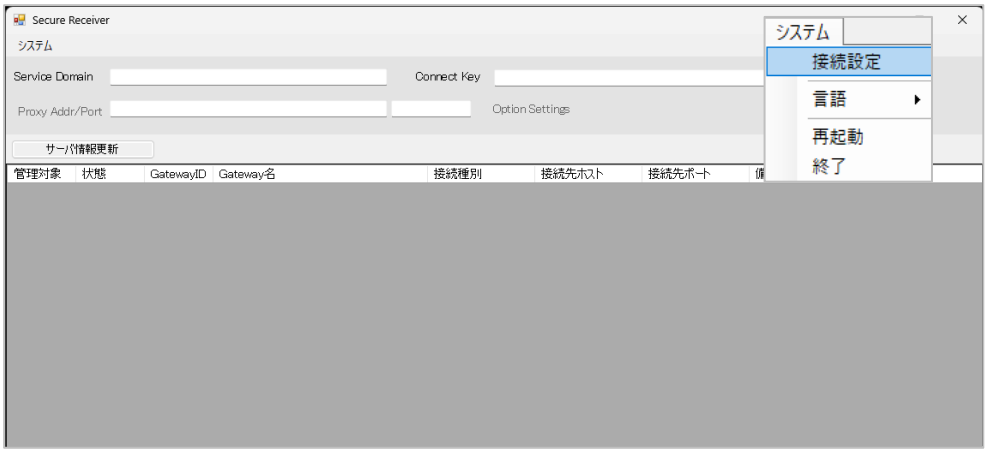


図 45 Windows Receiver 管理画面（接続設定）

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。

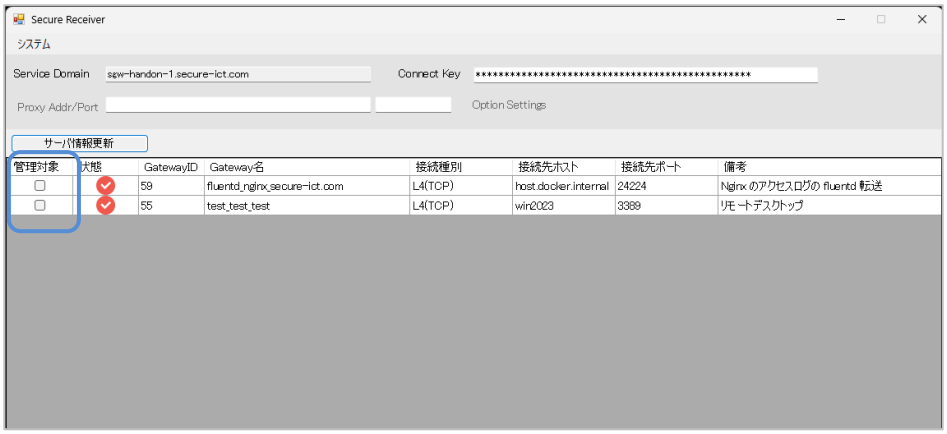


図 46 Windows Receiver 管理画面（利用設定）

【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 47 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 48 Receiver Docker 管理画面（利用設定）

2.5.3. タスク管理の利用

タスク管理 の操作は、サイドメニュー「タスク管理」から、「タスク一覧・画面」を表示して操作します。
タスクグループにはメンバ設定があり、自身がメンバに含まれているグループのみ一覧表示されます。

図 49 タスクグループ一覧・画面

1) タスク・グループの登録

タスクグループの追加は一覧画面の「追加」から実施します。
グループ名、説明、種別、管理者、メンバ を入力します。 どの情報の登録後に編集可能です。

図 50 タスクグループ登録・画面

「管理者、メンバ選択」は「検索文字」を入力して Enter すると、絞りこまれたアカウントの一覧が表示されますので、そこから選択して入力してください。 検索文字列は アカウントの名前と ID が適用されます。

メンバ選択で決定したアカウントは、左のメンバ一覧に追加されます。
追加されたメンバを削除する場合は、メンバ一覧の当該行をダブルクリックしてください。

2) タスク・グループの設定・変更

タスクを生成したら、まず設定すべきは Kanban 定義です。

Kanban 定義の「タスクボード」を追加します。

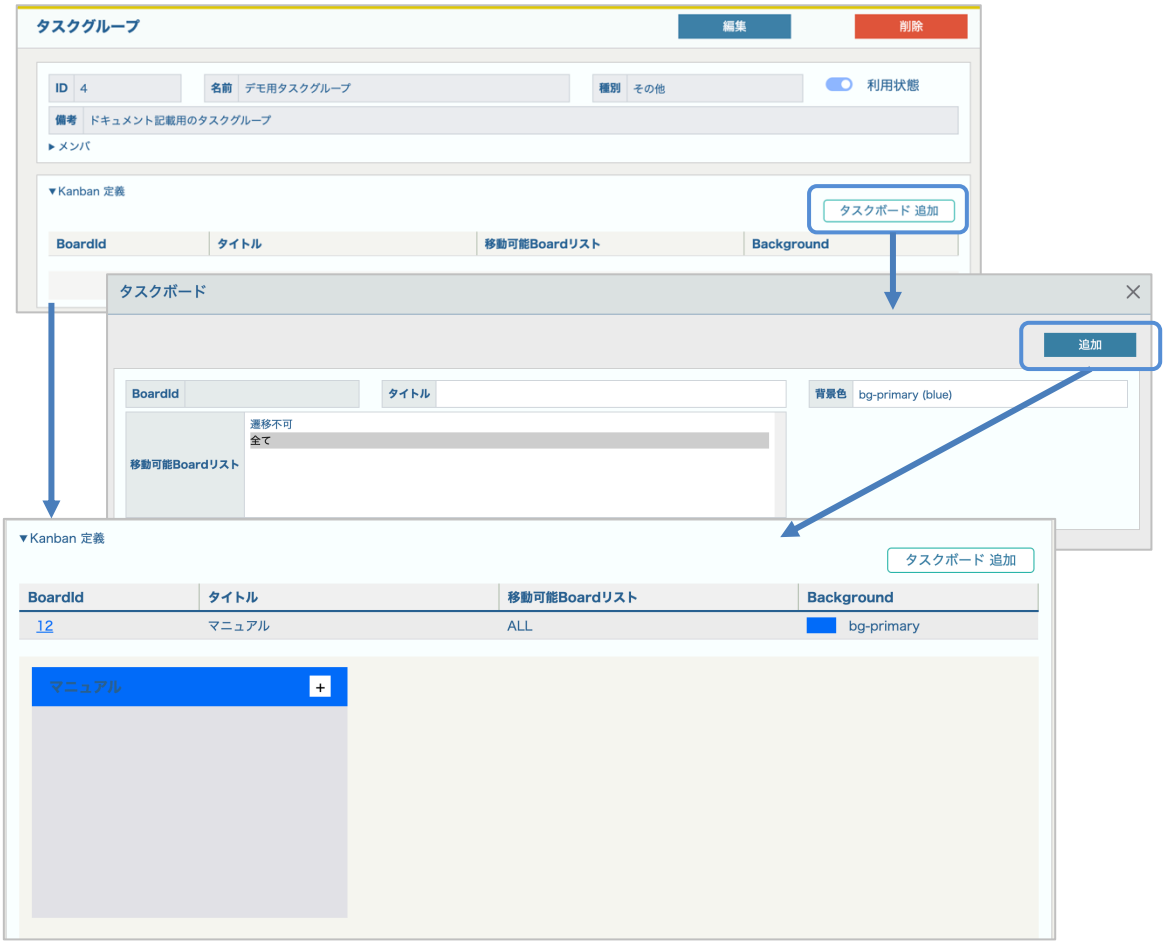


図 51 タスクグループ・タスクボードの追加

- 進捗管理などでは、「状態」を タスクボードにして管理することができます。
- 業務管理などでは、「作業分類」をタスクボードにして管理することができます。
- 変わったところでは、サンプル情報として提供している「サブシステム管理」で、契約 SaaS などの各種情報共有に利用するなども、この機能の利用方法です。

「タスク」は「タスクボード」の中に登録し、状態に応じてタスボードを移動させることで、残タスクを管理することができます。

「移動可能 Board リスト」はこのタスクボードの移動先を制限するものです。 設定はいつでも変更できるため、利用者が誤った遷移をしないガイドライン程度のものと考えてください。

状態遷移例） [検討中] → [作業中] → [処理済] [ベンディング]

注意点としては、タスクボードの表示順は利用者のブラウザ上ではドラッグ・ドロップで変更することが可能ですが、初期位置は登録順から変更できないことです。 これは今後の改善項目の一つです。

3) タスクの登録

タスクの登録は、分類されるタスクボードの［＋］から実施します。

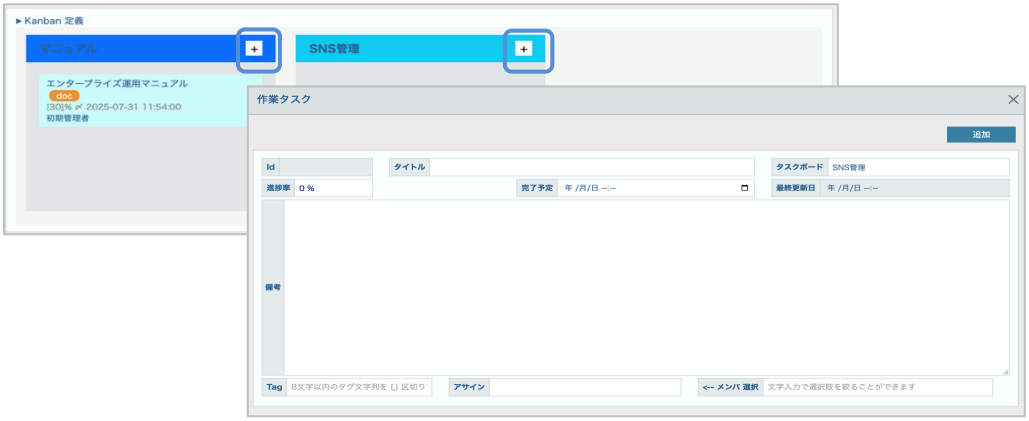


図 52 タスクの登録

【入力項目】

	入力項目	説明
1	タイトル	タスクのタイトル。
2	進捗率	0-100%で、5%刻みの選択形式。進捗率によってタスクの背景色が変わります。 ［0%］白 、［5-95%］薄青 、［100%］薄緑 ,［100%以外期限切れ］薄赤
3	完了予定	完了予定日時。
4	備考	タスクの内容や、実際の作業内容など。
5	Tag	一覧表示時に表示されるタグ。 8 文字以内の利用が識別容易なキーワードを自由入力。
6	アサイン	担当者。 メンバ選択で担当者をアカウントから選択。選択要領は、タスク作成時のメンバ設定と同様。

登録するとタスクは、タスクボードの先頭に表示されます。 タスクは更新が新しいものほど上に表示されます。

4) タスクの情報変更

タスクの情報変更は、タスクボードに表示されるタスクをクリックして表示される「タスク情報画面」から実施します。

変更すると最終更新時刻が更新され、タスクボードの先頭に表示されます。

図 53 タスクの情報変更

【タスクボードの移動】

タスクを別のタスクボードに移動させるには 2 種類の方法があります。

- Kanban 上で対象タスクをドラッグして、移動先ボード上にドロップする
- タスクが下の方法の表示や、画面上にボードが全て表示されていない場合などは、タスクの情報変更画面から以下の操作で実施します。
  - ・「タスクボード」で移動先を選択して、「ホード移動」
  - ・「タスクボード」で移動先を選択して、「変更」 この場合は他の入力内容も反映されます

2.5.4. チャットの利用

チャット管理 の操作は、サイドメニュー「チャット」 から、「チャット・チャネル一覧・画面」 を表示して操作します。
チャット・チャネルにはメンバ設定があり、自身がメンバに含まれているチャネルのみ一覧表示されます。

図 54 チャット・チャネル覧・画面

1) チャット・チャネルの登録

チャット・チャネルの追加は一覧画面の「追加」から実施します。
チャネル名、説明、管理者、メンバ を入力します。 どの情報の登録後に編集可能です。

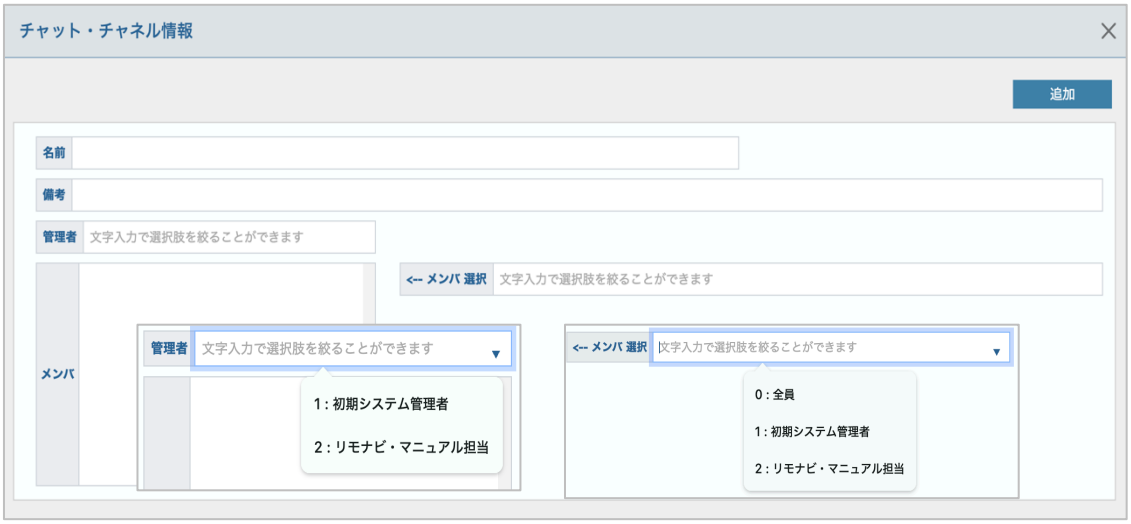


図 55 チャット・チャネルの登録

「管理者、メンバ選択」は「検索文字」を入力して Enter すると、絞りこまれたアカウントの一覧が表示されますので、そこから選択して入力してください。 検索文字列は アカウントの名前と ID が適用されます。

メンバ選択で決定したアカウントは、左のメンバ一覧に追加されます。
追加されたメンバを削除する場合は、メンバ一覧の当該行をダブルクリックしてください。

2) チャットの投稿・変更

チャット・チャネルは、一覧画面の当該行のダブルクリックないしは、ID 列のリンクのクリックで表示して操作します。

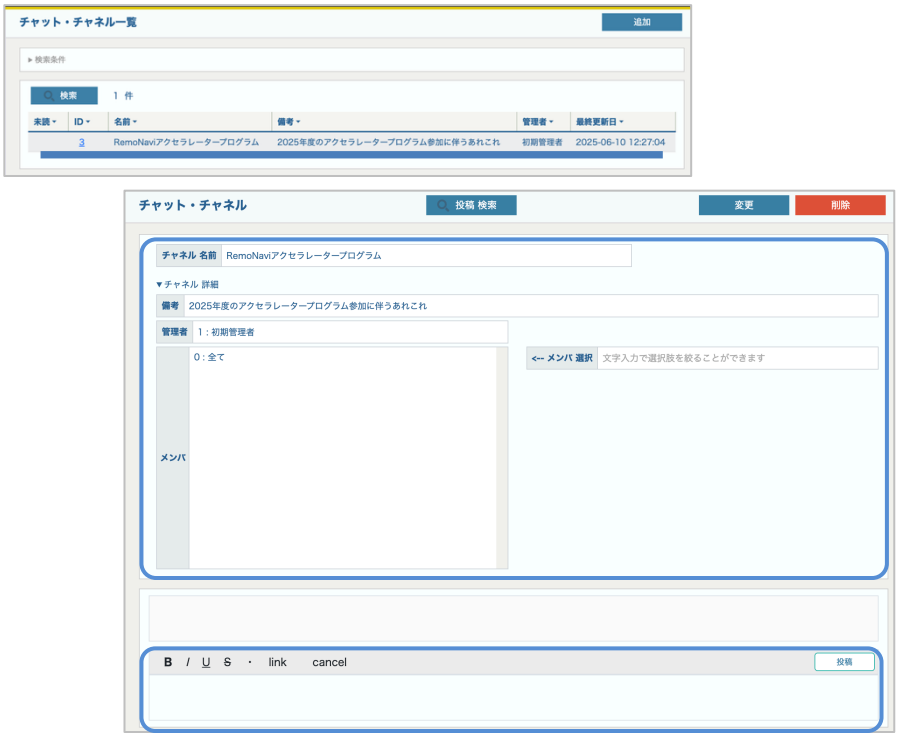


図 56 チャット・チャネル画面

画面丈夫がチャット・チャネルの管理情報で、これらは変更情報を入力して、「変更」ボタンを押下します。
画面を開いた状態では、「チャネル詳細」のアコーディオンは閉じています。

【チャネルの投稿】

投稿は、画面下部の投稿欄へ入力したら、右上の白抜きボタン「投稿」を押下します。
すると、投稿情報が画面に反映されます。 画面への投稿情報の反映は、WebSocket によるリアルタイム反映なので、別の人の投稿も自動的に反映されます。

入力文章の装飾は当該文章を選択して編集ボタンを押下することで実現します。

[B] 太字 [I] 斜体字 [U] 下線 [S] 取り消し線 [cancel] 装飾取り消し

ただし、装飾は２重にできてしまい、そうした場合、装飾のキャンセルができなくなることがあります。そうなった場合は、当該文章を削除し、再入力することで対応してください。

図 57 投稿の表示

【投稿の再編集】

自分が投稿したものだけ、下図枠囲みの「再編集」「削除」アイコンが表示されます。

「再編集」アイコンを押下すると、以下のように投稿情報が「再編集モード」に切替わりますので、編集後に「変更」ボタンで確定することができます。

図 58 投稿の再編集

【投稿へのリプライ】

「リプライ」アイコンを押下すると、以下のようにリプライ投稿が参照できるようになり、リプライ投稿欄が表示されます。

ここに投稿と同じ要領で入力し、「スレッド投稿」ボタンを押下するとリプライ投稿することができます。

図 59 投稿へのリプライ投稿

投稿が完了すると、返信欄に追加されます。 返信の再編集も投稿同様、「再編集」アイコンを押下すると、再編集モードになりますので、同じ要領で変更することができます。

【投稿へのリアクション】

右上の「顔マーク」を押下して、リアクション用の絵文字を選択すると、投稿の下に表示されます。

図 60 投稿へのリアクション操作

リアクションの削除は、投稿の下に表示された絵文字をクリックすると、解除されます。

【制限事項】

- チャットへのファイル投稿はできません。
- メンバへのメンション機能はありません。

いずれも今後の機能追加候補でありますが、RemoNavi SaaS エンタープライズ版は、「リモート接続」と「セキュリティ運用支援としてインシデント管理と検査」を主に提供しています。 チャットなどその他の機能はそれらを支援するツール機能にすぎないため、それら機能への追加の優先度は高くありません。

2.5.5. 個人メモの利用

メモ の操作は、トップメニューのドロップダウンメニュー「メモ」から、「メモ一覧・画面」を表示して操作します。

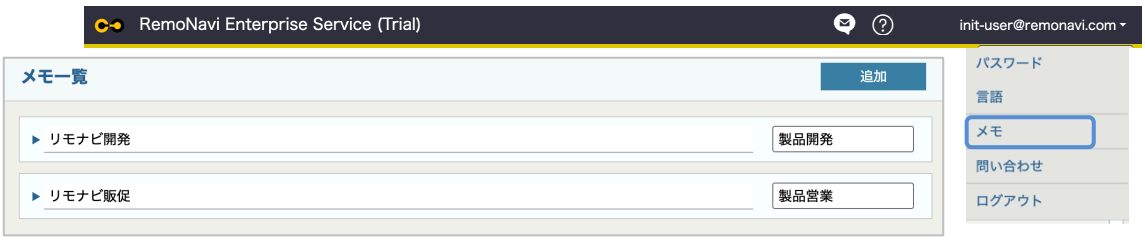


図 61 メモ一覧・画面

1) メモの追加

メモは「メモ一覧」の「追加」をすると、追加されメモ一覧に「アコーディオン表示」でタイトルのみ表示されます。
追加されたメモは先頭に表示されます。 メモは最大２０個まで追加可能です。

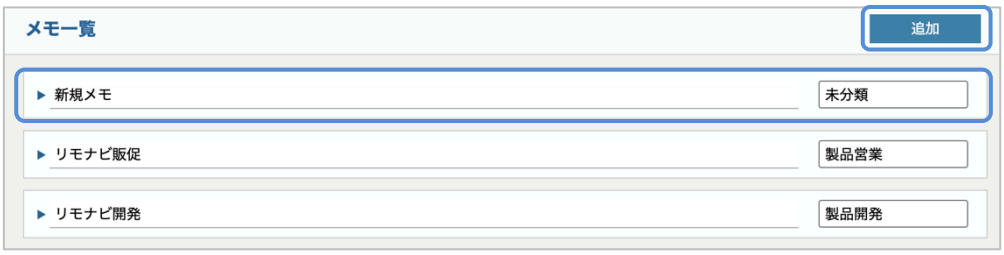


図 62 追加後のメモ一覧・画面

追加では、メモが追加されるだけです。 メモ内容の編集は、次項の編集・保存を参照してください

2) メモの編集・保存

メモ・タイトルがアコーディオン表示になっているので、それを開くと、メモの入力ができます。
分類とメモを編集して、左下部の「保存」でセーブします。

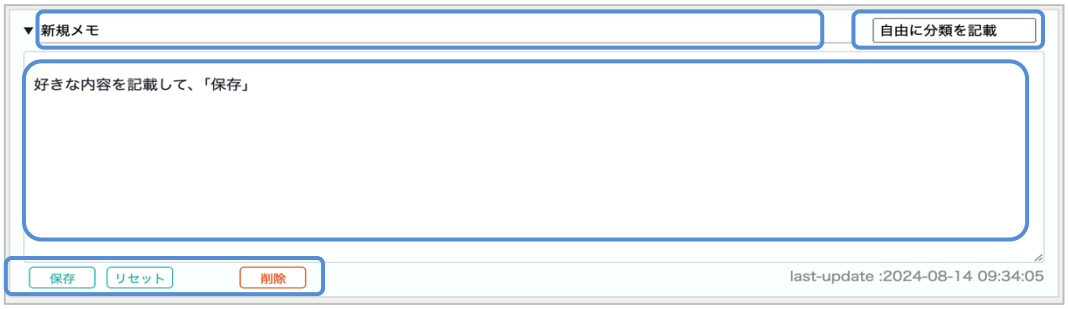


図 63 メモの編集（メモのアコーディオンを開いた状態）

2.5.6. 全体通知の利用

全体通知 の操作は、トップメニュー「お手紙マーク」から、「通知一覧・画面」を表示して操作します。

図 64 通知一覧・画面

- 未読通知があると、「枠囲みのアイコン」がゆっくり点滅します。
- 通知の発行権限がない利用者は、「追加」ボタンが表示されません。

1) 全体通知の追加

全体通知は、追加が完了した時点で利用者全員に反映されます。

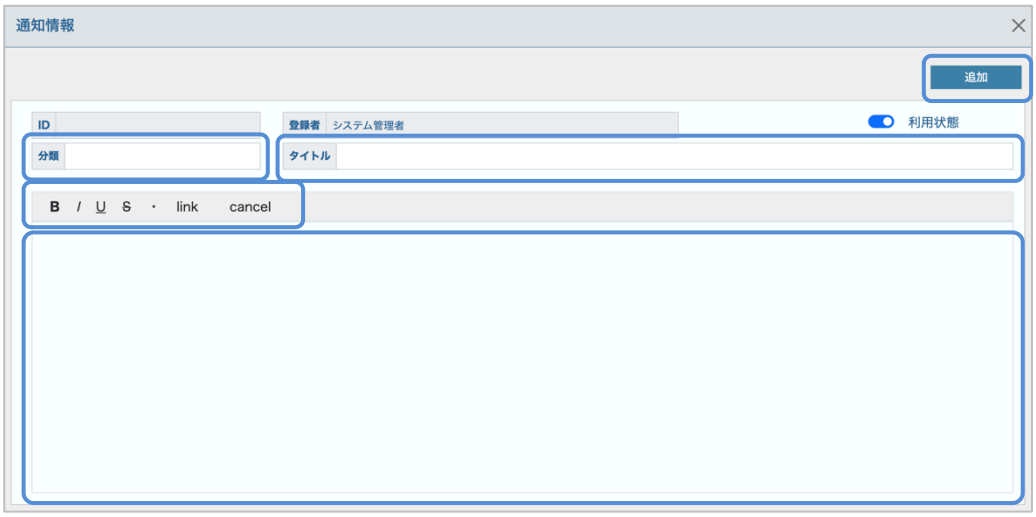


図 65 通知の追加・画面

入力情報は、項目タイトル通りで特に説明の必要はないと思いますが、一点「分類」は、利用者がどのような通知なのかを直感的に理解できる単語を利用することを推奨します。 例えば「一般通知」「セキュリティ通知」などです。

装飾は当該文章を選択して編集ボタンを押下することで実現します。

[B] 太字 [I] 斜体字 [U] 下線 [S] 取り消し線 [cancel] 装飾取り消し

ただし、装飾は 2 重にできてしまい、そうした場合、装飾のキャンセルができなくなることがあります。そうなった場合は、当該文章を削除し、再入力することで対応してください。

2） 全体通知の参照、情報変更・削除

通知の参照は、一覧の当該行をダブルクリックないしは、ID 列のリンクをクリックすると表示することができます。

- 通知の発行権限がない利用者は、「編集、削除」ボタンは表示されません。

図 66 通知情報・画面

編集は、「編集」ボタンを押下すると、以下の「編集モード」モード画面となって記事を編集することができます。

編集した記事の保存は「変更」で実現します。 また、記事を未公開にする場合、「利用状態」を「無」にすることで実現可能です。

図 67 通知情報の編集モード・画面

文字装飾は「登録」と同様です。

2.5.7. セキュリティ検査の実施（利用者）

利用者が回答する必要があるセキュリティ検査は「MyPage」の「未完了セキュリティ検査」に表示されます。
回答する場合は当該行をダブルクリックして、検査（回答用）画面を表示して、操作してください。

図 68 MyPage の実施すべきセキュリティ検査一覧

検査（回答用）には、回答すべき問題と選択項目の回答が表示されます。
単一選択は○型、複数選択は□型で表示されますので、全ての設問の回答を選択し、右上段の「回答」をしてください。

図 69 セキュリティ検査（回答）画面

合格必須の検査の場合、以下のように、どの設問の回答に誤りがあるか表示されます。

設問を再考した後、再回答して合格してください。

図 70 合格必須の検査の場合の不合格画面

2.5.8. ビデオチャットの利用

ビデオチャット機能は、完成された機能ではなく、今後機能精度の向上や拡張をしていくものです。 （オンプレは未対応）

なぜ試験的にでも導入したかですが、RemoNavi SaaS エンタープライズ版は、「リモート接続」と「セキュリティ運用支援」を主に提供しています。 その中の「セキュリティ運用支援」において、コミュニケーション面から必要なこともあるであろうことから本機能を試験導入しています。

本機能は以下のオープンソースを利用して実現しています。

Janus [GPLv3] https://janus.conf.meetecho.com

サーバ機能は、オープンソースを Docker 配備し、クライアント機能のみ RemoNavi 独自のインプリメントをしています。

1) ビデオ･ミーティングの一覧表示

ビデオチャット の操作は、サイドメニュー「ビデオ会議」から、「ビデオ･ミーティング一覧画面」を表示して操作します。

画面は月毎に表示されます。

図 71 ビデオ･ミーティングの一覧画面

2) ビデオ･ミーティングの予約

予約は、一覧画面の「追加」から実施します。

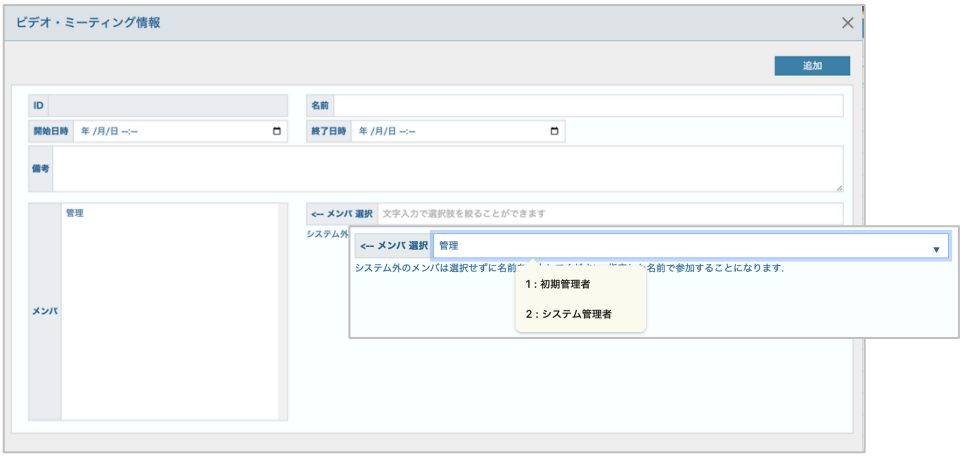


図 72 ビデオ･ミーティングの予約登録･画面

「メンバ選択」は「検索文字」を入力して Enter すると、絞りこまれたアカウントの一覧が表示されますので、そこから選択して入力してください。 検索文字列は アカウントの名前と ID が適用されます。

メンバ選択で決定したアカウントは、左のメンバ一覧に追加されます。 また、追加されたメンバを削除する場合は、メンバ一覧の当該行をダブルクリックしてください。

RemoNavi SaaS に登録のない利用者をミーティングに参加させる場合には、「メンバ選択」に参加者の名前を入力・Enter することで追加できます。

登録が完了したミーティング情報は、以下の情報が付加されて表示されます。

ゲスト招待者には、下記の「枠囲み URL」と「メンバに登録した名前」を送付してください。 URL にアクセスすると「招待名」の入力を求められます。

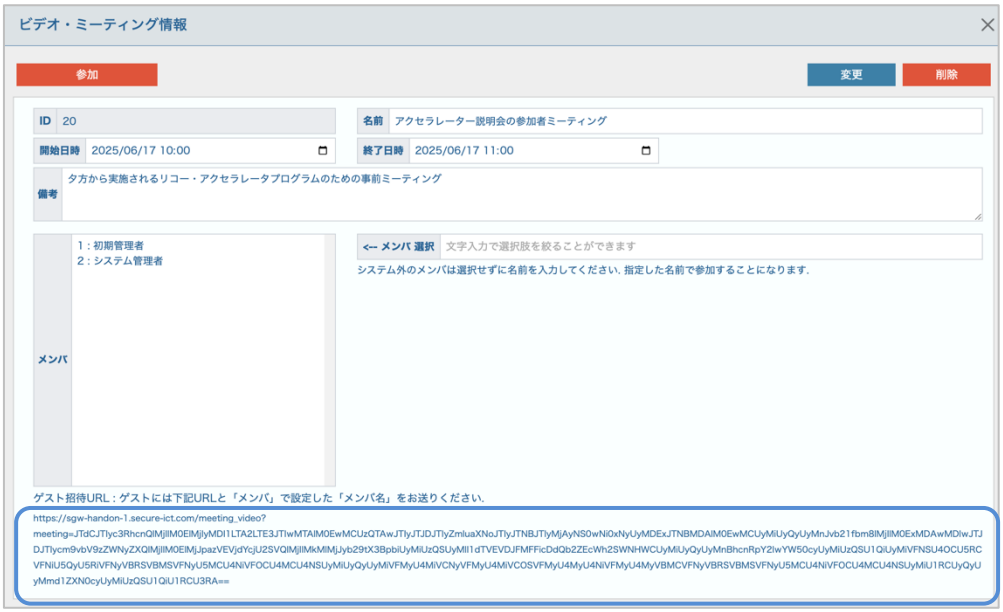


図 73 ビデオ・ミーティングの登録情報

ミーティング情報の変更は、変更内容を入力して「変更」するだけです。

制限事項）

- ミーティングは終了時刻になっても自動終了しません。 開始・終了時刻は、ミーティング参加時のチェックにのみ使用しています。
- ミーティング・メンバは「ミーティング画面」を開いた時のメンバとなります。ミーティング中に追加してもすでに開いたミーティング画面では許容されません。 ただし、メンバ追加の変更はできますので、その後「ミーティング画面」を開き直せば、追加したメンバも許容されます。

3） ビデオ・ミーティングの開始

ビデオ・ミーティングは、ミーティング期間の前後 20 分間に限って開始することができます。

ミーティングの開始は、方法は以下の 2 種類です。

- SaaS アカウント： 一覧画面をクリックして開いた「ビデオ・ミーティング情報」画面の「参加」から
- 招待アカウント： 招待 URL へアクセスし、「登録した招待者の名前」を入力

制限事項）

- ミーティングで「画面共有」する場合は、Chrome ブラウザのみの対応です。
- ミーティングの録画機能はサポートしていません。もし録画が必要な場合、OS 標準機能にて録画してください。
  - Windows は標準機能で録画可能です。ミーティング画面を開いた状態で、「Windows」+「G」で ゲームバーを起動することで録画を実現できます。
  - MAC は標準機能で録画可能です。「shift」+「command」+「5」で録画を実現できます。

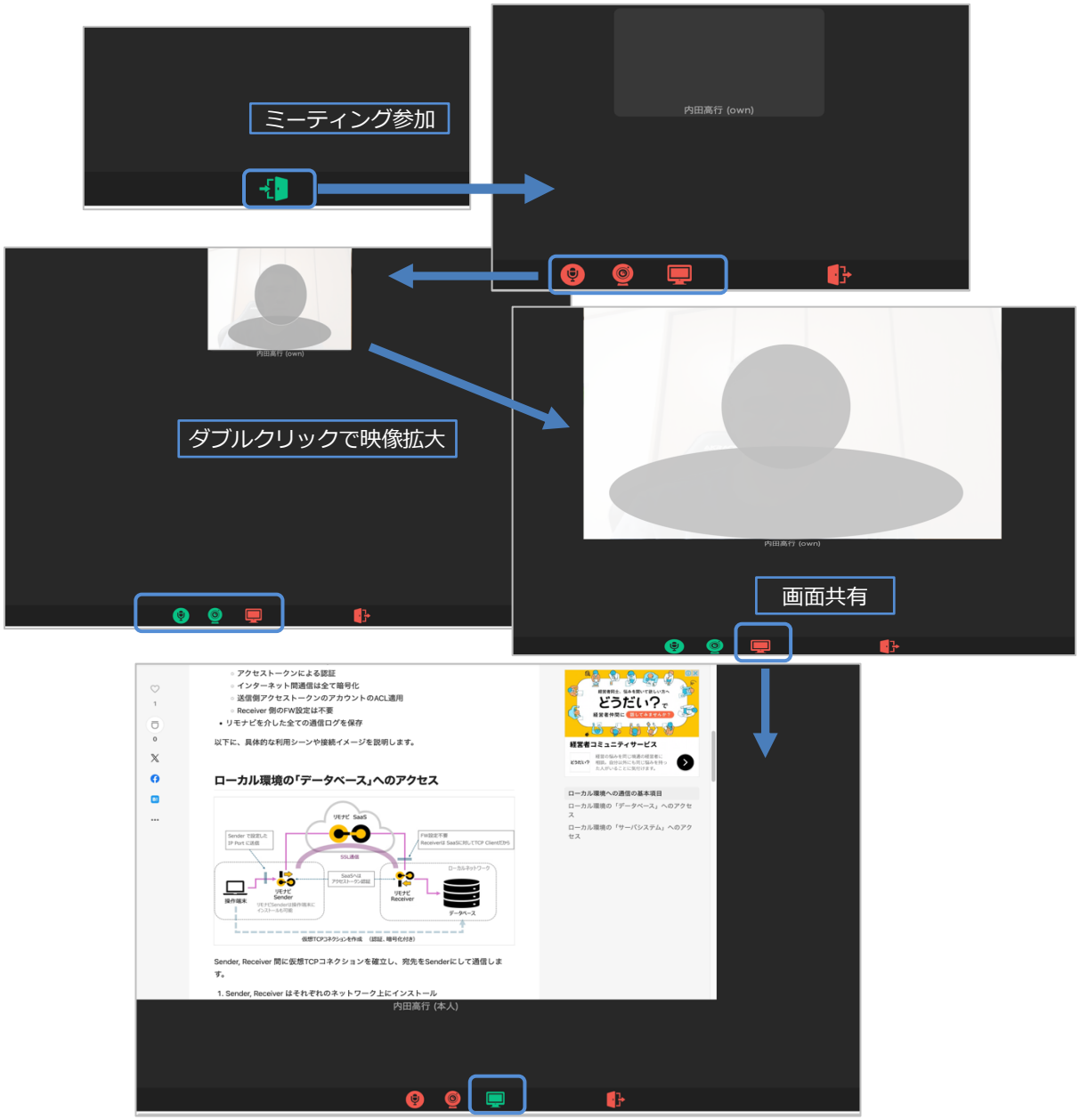


図 74 ビデオ・ミーティング画面

2.5.9. データ分析の利用

データ分析機能は、完成された機能ではなく、今後機能精度の向上や拡張をしていくものです。

なぜ試験的にでも導入されたかについてですが、理由は以下です。

- RemoNavi SaaS による通信でデータ収集
- 収集したデータを分析に利用

RemoNavi SaaS は SaaS で実現するリモート接続のあたらしいインフラですが、それらを使ったソリューションへ、を将来的に目指しているからです。その一つにデータ分析を実装した次第です。

このシステムが提供するデータ分析は 2 つ。それら分析をするためのデータセット、の系 3 機能から構成されます。

2.5.9.1. データセット

分析のためのデータ定義で、現在は以下のみのサポートとなっております。

表 9 分析データセット一覧

	大分類	中分類	説明
1	アップロード・ファイル	CSV	解析のための CSV 形式のデータファイル。 1 行目タイトル行、カンマ区切り、UTF-8
2		Parquet	解析のための Paquet 形式のデータファイル。
3	データベース	MySQL | MariaDB	MySQL データベース。 Host, IP ポート番号、ユーザ、パスワード、データベース名 を指定
4		Postgres	Postgres データベース。 Host、IP ポート番号、ユーザ、パスワード、データベース名 を指定

データベースは接続先を指定します。分析に使うデータのテーブル指定は、各分析セットにて指定します。

データセットについては要望に応じて随時拡張いたします。

1) データセットの一覧参照

データセットの操作は、サイドメニュー「データ分析／データセット」から、「データセット一覧画面」を表示して操作します。

図 75 データセット一覧・画面

2) データセット情報の参照・変更

一覧の当該行をダブルクリップあるいは、ID 列のリンクをクリックすると情報画面が表示されます。

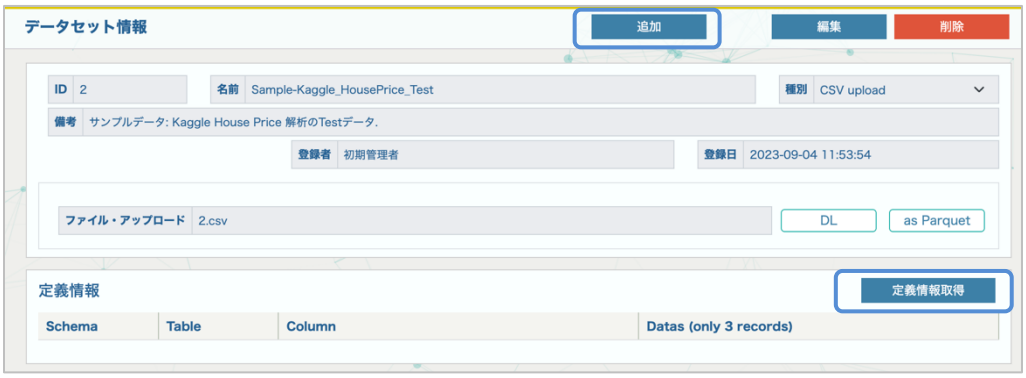


図 76 データセット情報・画面

【追加】

データセットが CSV アップロード、Parquet アップロードの場合には、追加設定をすることが可能です。

「追加」ボタンを押下すると、ファイル選択画面が表示され、指定ファイルを追加することができます。 また、この追加は API Token を使った非画面アクセスでも実現することができます。 日々の集計業務など、プログラマブルに追加が必要な場合に対応したものです。 詳細は、ヘルプ画面に操作 URL 等が掲載されていますので、そちらを参照してください。

【データ参照】

定義情報を参照すると、以下の行が出力され、アコーディオンをあけると、定義情報が表示されます。

Datas 列の「データ参照」をあけると、最初の 3 行だけサンプルデータが表示されます。

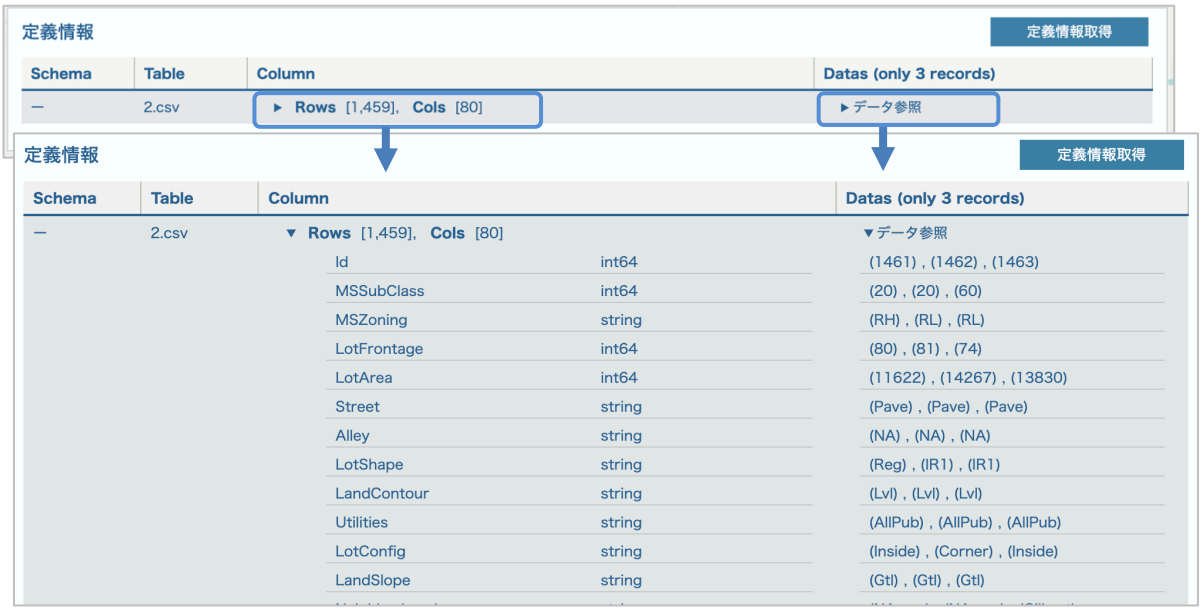


図 77 データセット情報のデータ参照

データ解析において、データの参照は軽微なものではなく様々な角度から参照、検索がなされるものですが、ここでは定義を若干のサンプル表示のみです。

データサイエンティストが利用するデータ参照はここでは提供していません。 必要に応じて、各種分析セットの機能でそれらは機能追加、改善していきます。

2.5.9.2. 原因分析セット

データセットの情報を使って以下の分析セットを作成します。

- 「トレーニングデータ」と「プレディクト対象データ（結果予測をする場合）」のセットを決定し、
- データカラムから、説明変数と結果変数の決定する。
  - ・ カラムごとに未設定データの補完方法の決定（最繁,平均,中央, 0 など）
  - ・ 文字データの数値化（OneHot | Oridinal）

【分析内容】

原因分析では、以下の分析がなされ、結果ファイルに出力されます。

① トレーニング・データの分布グラフ

② トレーニング・データの結果変数と説明変数の分散分析(ANOVA)

・ 結果変数に対して全ての説明変数(標準化)の分散分析をして、p 値順に説明変数を出力します。

③ Ridge 回帰分析（sklearn - linear_model.Ridge 利用)

・ GridSearch {"alpha":[0.001,0.1,1,10,20,50,100,1000],"tol":[0.01,0.02,0.03,0.04,0.05,0.1,0.15]}

・ 解析結果 Score, 説明変数の Coefficient

④ Lasso 回帰分析(sklearn - linear_model.Lasso 利用)

・ GridSearch {"alpha":[0.001,0.1,1,10,20,50,100,1000],"tol":[0.1,0.15,0.2]}

・ 解析結果 Score, 説明変数の Coefficient

現状は Predict を主目的とした回帰分析としているためこのような実装となっています。 これらについては、ご要望に応じて、解析内容の追加・改善をしてまいります。

【分析結果】

分析内容の結果を Excel ファイルに出力します。

1st Sheet ： 分散分析(ANOVA)、回帰分析結果(score, coefficient)

2nd Sheet ： 説明変数の分布図

3rd Sheet ：Predict 結果

【その他】

原因分析は、サンプルで Kaggle House Price 問題の価格予測ができるよう「データセット」と「原因分析セット」が設定されていますので、それを使って実際に分析し、結果を参照ください。

サンプル設定してあるものでの解析は、 1000 位/4000 人 程度、正解率８～９割です。

1） 回帰分析セットの一覧参照

回帰分析セットの操作は、サイドメニュー「データ分析／原因分析セット」から、「回帰分析セット一覧画面」を表示して操作します。

図 78 回帰分析セット一覧・画面

2) 回帰分析セットの登録

一覧画面の「追加」から登録画面を表示し、トレーニングデータとプレディクトデータの設定をします。変数の詳細設定は登録後の詳細編集で行います。

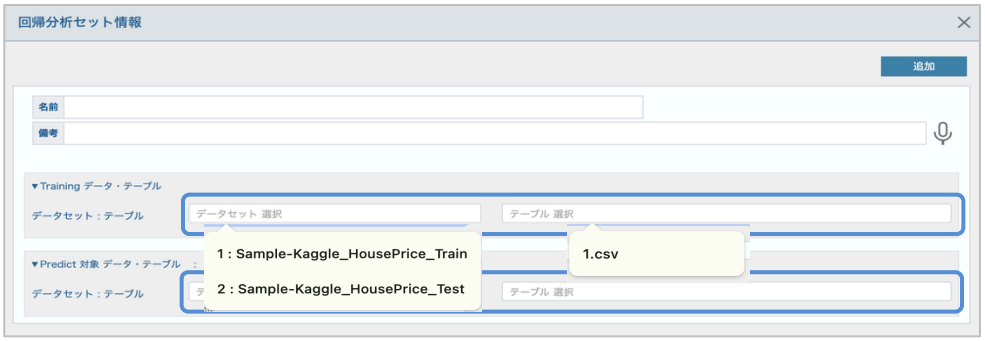


図 79 回帰分析セット登録モーダル・画面

「データセット」でマウスクリックすると一覧が表示されます。文字入力をすると部分一致で検索されたデータセット一覧が表示されますので、そこから選択します。 データセットが確定すると、「テーブル」でマウスそのデータセット内のテーブル一覧が表示されます。同様に検索した一覧を表示できますので、そこから選択して確定させます。

3) 回帰分析セットの設定変更と分析ジョブの実行

回帰分析セット一覧画面から当該行をダブルクリックあるいは、ID 列のリンクをクリックすると、回帰分析セット画面が表示されます。この画面から変更、分析ジョブの実行をします。

図 80 回帰分析セット・画面

「編集」ボタンを押下すると、「編集モード」になり、そこで各変数について設定していきます。

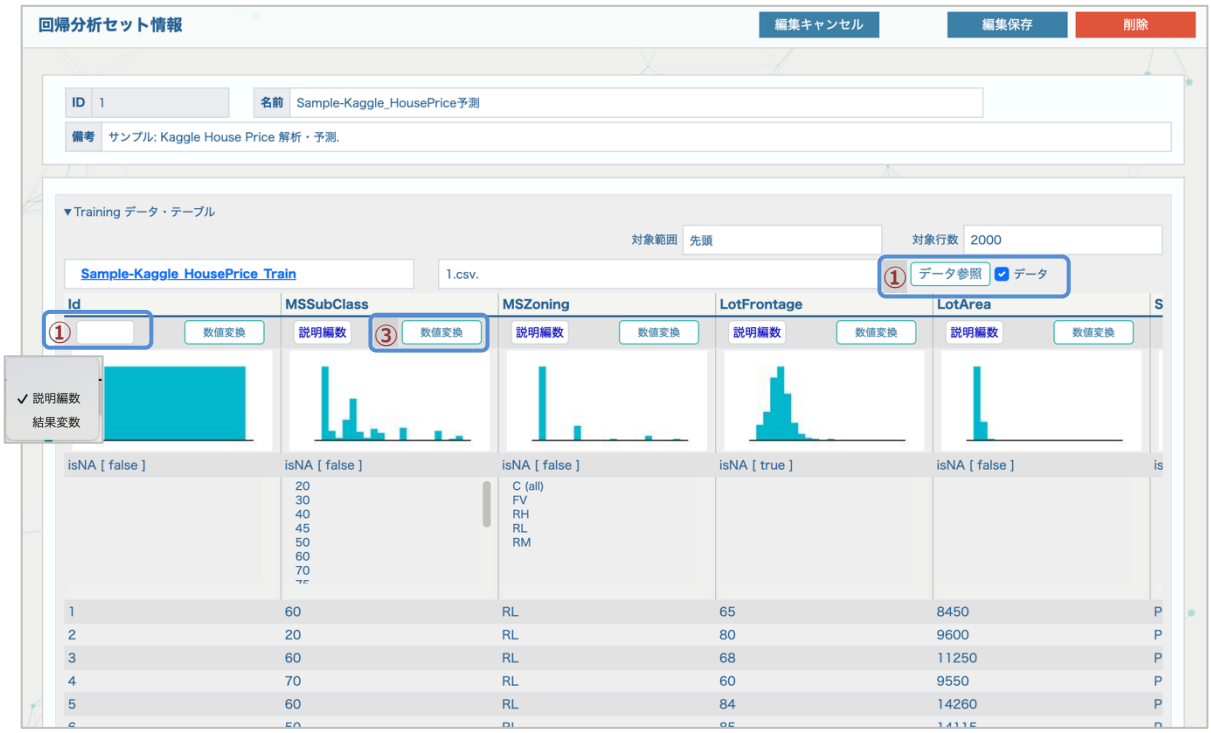


図 81 回帰分析セット・画面 （編集モード・変数設定）

設定すべき項目は以下です。

- 説明変数と結果変数の選択
- 説明変数の「数値化変換」と「欠損値補完」
- 結果変数の「数値化変換」

これらをするための操作を図の①～③の順に説明していきます。

① データを参照します。「データ」チェックを付与すると、100 個までですが情報が表示されます。グラフと設定内容はデータチェックをしなくても表示されます。

② どの変数が 「説明変数」、「結果変数は(1 つだけ)」なのかを設定していきます。 未利用にすることもできます。

③ 変数の「数値化変換」と「欠損値補完」をします。
まずは数値変換についてです。

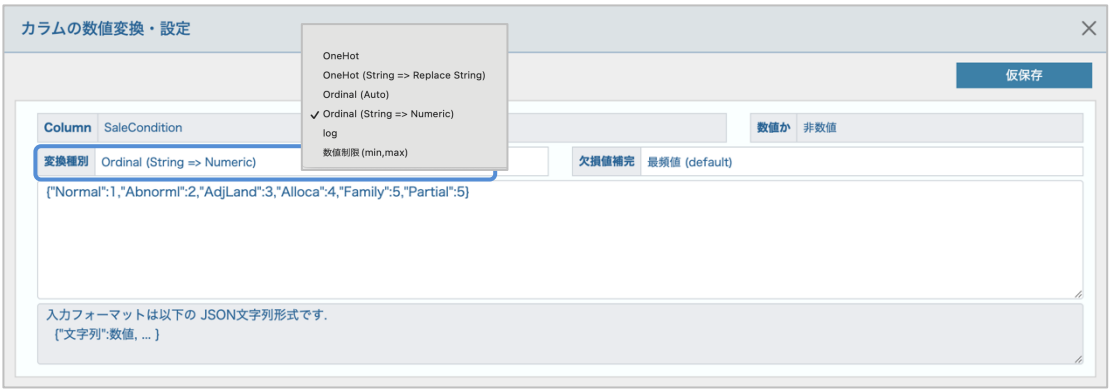


図 82 回帰分析セット・画面 （編集モード・変数設定：数値変換）

数値変換と提供しているのは以下です。

表 10 数値変換の種類と説明

	種別	説明
1	OneHot	１つの変数を OneHot 変換します。 設定値が A,B,C の３種類の場合、変数_A, 変数_B, 変数_C のように展開して A なら 変数_A を 1、それ外を 0 にします。 説明変数が極端に増えてしまうので、利用には注意が必要です。 入力値：不要
2	OneHot (String => Replace String)	誤字等に対応した OneHot です。 設定値は３種類のはずなのに A, B,C, a だった場合の [a] を [A]に補正して OneHot 変換します。 入力値：{"文字列":"変換文字列", ... , "文字列":"変換文字列"}
3	Ordinal (Auto)	出現する文字列を GroupBy して１から番号を振っていきます。付与される番号は順不同です。 入力値：不要
4	Ordinal (String => Numeric)	誤字、変換数値に意味を持たせるための Ordinal です。 振られる番号を操作したい場合や、OneHot 同様誤字の吸収です。 入力値：{"文字列":数値, ... , "文字列":数値}
5	log	Log に変換します。 回帰分析は結果変数が正規分布していることが望ましく、裾野が広い分布傾向にあるデータなどは、Log して正規分布に近づけることができます。 結果変数を Log した場合でも、Predict 結果は逆変換をかけて元に戻した値が出力されます。 入力値：不要
	数値制限 (min, max)	数値制限を超える行は利用されなくなります。 明らかなエラーデータなどの排除外を目的としています。 入力値： {"min":最小値 , "max":最大値} (*) min, max を片方だけ指定可能.

(*) 指定は全て JSON 形式です。 画面下部に JSON フォーマットが表示されますので、それを参考に入力してください。

(*) Predict をする場合、OneHot、Ordinal は Train データと Predict データ 共通の 変換がされる必要があります。どちらもデータ要素の出現が同じなら、OneHot や Ordinal(Auto) が使えますが、そうでない場合は、面倒ですが OneHot (String => Replace String)、Ordinal (String => Numeric) で両データを包含した設定が必要になります。

続いて欠損値補完についてです。

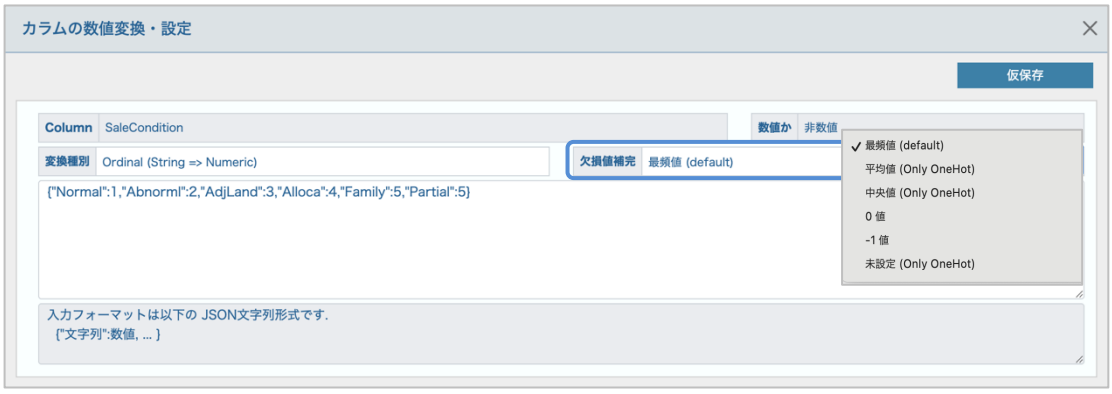


図 83 回帰分析セット･画面 （編集モード･変数設定：欠損値補完）

表 11 欠損値補完の種類と説明

	種別	説明
1	最頻値 default	最も多く使われている値。
2	平均値	平均値。 Ordinal では平均値に相当する数値がいなこともあるので利用不可
3	中央値	中央値。 Ordinal では平均値に相当する数値がいなこともあるので利用不可
4	0 値	0
5	-1 値	－1
6	未設定	OneHot の場合は展開されるため、未設定の場合もで全ての変数が 0 になるだけ

(*) 欠損値補完によって解析精度が大きく変わることは周知の通りで、他の変数による色分けをしたのちの色ごとの最頻値設定などは比較的一般です。 ですが、本システムではそこまでの機構を備えておりません。それらについては、今後の課題として、精度の向上に努めてまいりたいと考えております。

「ジョブ実行」で原因分析処理を分析ジョブに登録します。

分析ジョブは即時ではなく、バックグラウンドで登録順に実行していきます。同時実行数は 1 つです。 詳細は、2.5.9.4 分析ジョブを参照のこと。

4) 回帰分析セットの分析結果

分析ジョブの結果概要（データ分析／分析ジョブ／分析ジョブ情報）には以下の情報が出力されます。

結果ファイルは本項、処理説明の「分析結果」を参照ください。

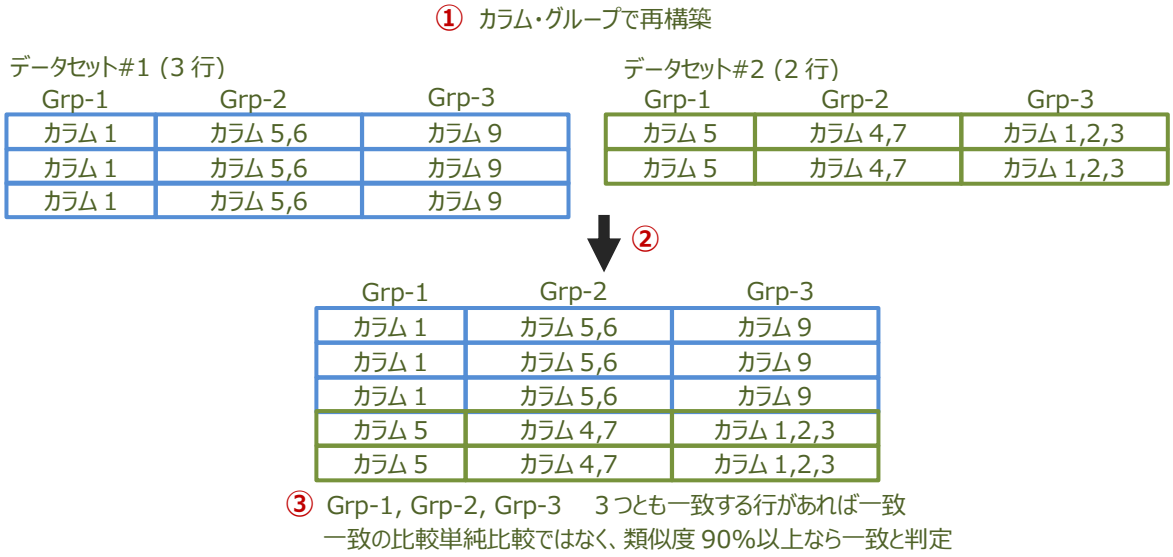
2.5.9.3. 名寄せセット

データセットの情報を使って以下の名寄せセットを作成します。

ここでいう「名寄せ」は対象データから、表記の揺らぎ等を考慮して、同一と思われるデータの一覧を構築することです。 完全一致せず、疑わしいと思われる行については、それら結果ファイルに出力します。

- 名寄せの対象カラムは、複数で一つのカラムとすることができます。
  複数カラムを連結して一つのデータとします。最大３カラムまで連結可能です。
- 名寄せ対象のカラム・グループは最大３つまで指定可能です。
  対象カラムを複数指定する場合、指定するすべてのカラム・グループが一致とみなされた行だけを一致とします。
- 名寄せの対象データセットは最大４つまで指定可能です。

【名寄せの処理イメージ】



① データセット毎に指定されたカラムグループで、データを再構成します。
- カラムグループを３使う場合は、指定するすべてのデータセットで同一の Grp-1,2,3 を指定する必要があります。
- データセットは１つのみの指定も可能です。その場合、データセット内の同一行探しになります。

② 同じカラム構成となったすべてのデータセットを連結して一つのデータセットを作成します。
- 指定したデータセット順に連結します。名寄せ結果はこの連結テーブルに「一致有無、一致行」が付与されて出力されるので、若番優先等があるばあいは、優先度の高いデータセットを先に指定してください。

③ 同一行を解析します。
- 同一行とは、 Grp1,2,3 すべてが一致する行が他にあるかです。
- 一致とは、完全一致の他、内部比較アルゴリズムによる類似度 90%以上の場合を指します。

【名寄せの結果】

結果は「CSV ファイル」で出力されます。 出力フォーマットは以下です。

```
通番 ,{一致有無}, 一致する行の通番 , カラムグループ１[ , カラムグループ２[ , カラムグループ３] ]
```

一致有無： [有] exist [無] 空白　　一致行は、双方の行が一致となります。

1） 名寄せセットの一覧参照

名寄せの操作は、サイドメニュー「データ分析／名寄せセット」から、「名寄せセット一覧画面」を表示して操作します。

図 84 名寄せセット一覧・画面

2) 名寄せセットの登録

名寄せ一覧画面から「追加」を押下すると登録モーダル画面が表示されます。

データセット、カラムグループについては先の説明に従って設定してください。 ここで重要なことは、データセットとカラムグループの設定については情報変更できない点です。 もし変更が必要な場合、新たな名寄せセットを作成する必要があります。

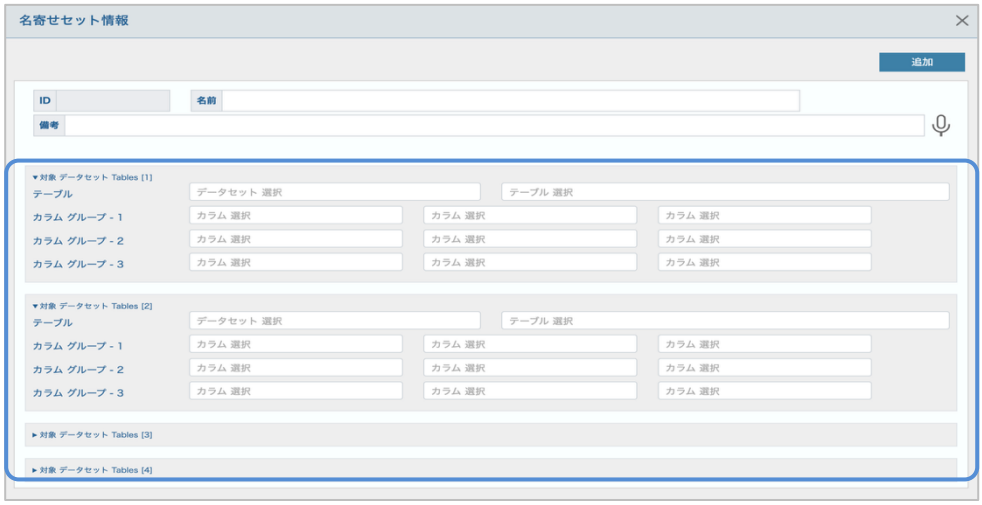


図 85 名寄せセットの登録モーダル・画面

3) 名寄せセットの詳細情報参照・変更と分析ジョブの実行

名寄せセットの詳細情報(モーダル画面)を表示して、各種操作を実施します。

図 86 名寄せセット情報のモーダル・画面

「ジョブ実行」で名寄せ処理を分析ジョブに登録します。

分析ジョブは即時ではなく、バックグラウンドで登録順に実行していきます。同時実行数は１つです。 詳細は、2.5.9.4 分析ジョブを参照のこと。

4） 名寄せセットの分析結果

分析ジョブの結果概要（データ分析／分析ジョブ／分析ジョブ情報）には以下の情報が出力されます。

結果ファイルは本項、処理説明の「名寄せの結果」を参照ください。

(*1) が名寄せセットで指定したデータの全行で、(*2)が 一致を検知した行です。

以下は国税局(神奈川県の法人)データを使った解析です。 法人は地域が違えば同じ商号で存在することができるため、「法人名＋住所」で名寄せすると、重複が大幅に減少することがわかります。 ただし、国税局の法人情報では住所変更があった場合、前住所と新住所で２行ありますので、必ずしも同一商号の存在をこれでチェックできるわけではありません。

「法人名のみ」の名寄せ

```
Start RecoredLinkage JobId[5]
Load Dataset : 国税局の神奈川県の法人一覧 (csv_upload)      [OK]
Start RecoredLinkage
    source-data row length : 354940      (*1)
    linkage-data row length : 92716      (*2)
Finish RecoredLinkage

結果ファイルの先頭 2 カラム(linkage, linkage_indeies)に linkage があった場合の情報が付与されます。
linkage がある場合は、linkage カラムに[exist]、linkage_indeies カラムに同一と思われるレコード番号が設定されます.
```

「法人名と住所」の名寄せ

```
Start RecoredLinkage JobId[6]
Load Dataset : 国税局の神奈川県の法人一覧 (csv_upload)      [OK]
Start RecoredLinkage
source-data row length : 354940      (*1)
linkage-data row length : 669        (*2)
Finish RecoredLinkage

結果ファイルの先頭 2 カラム(linkage, linkage_indeies)に linkage があった場合の情報が付与されます。
linkage がある場合は、linkage カラムに[exist]、linkage_indeies カラムに同一と思われるレコード番号が設定されます.
```

2.5.9.4. 分析ジョブ

前述の通り、回帰分析や名寄せは、それぞれ「原因分析セット」、「名寄せセット」にて使用するデータセットや解析対象データの設定をするのみです。 解析セットから実際の分析処理が「ジョブ実行」がなされると、分析処理キューに繋がれ、登録順にバックグランドで実行されることになります。分析処理は同時に一つしか実行されません。

分析ジョブはそれら分析処理をリスト管理し、状態を「未実施[空白]、実施中[実行アイコン]、実施完了・成功[🟢]・失敗[🔴]」を表示しています。 この一覧にあるものは、すべて分析処理が実行される、されたものです。 未実施の場合も、これから実施されものです。

1) 分析ジョブの一覧参照

分析ジョブの参照は、サイドメニュー「データ分析／分析ジョブ」から、「分析ジョブ一覧画面」を表示して操作します。

図 87 分析ジョブ一覧・画面

2) 分析ジョブ情報の参照

分析結果等は分析ジョブ情報から取得します。 分析ジョブ情報は、一覧画面の当該行のダブルクリックあるいは、ID 列のリンクをクリックすることで表示できます。

分析結果は、「原因分析」、「名寄せ」の解析毎に個別に説明していますので、そちらを参照してください。

図 88 分析ジョブ情報・画面

2.5.10. ImageBox の利用

ImageBox 機能は、完成された機能ではなく、今後機能精度の向上や拡張をしていくものです。

なぜ試験的にでも導入されたかですが、RemoNavi SaaS エンタープライズ版は、「リモート接続」と「セキュリティ運用支援」を主に提供しています。 その中の「セキュリティ運用支援」において、画像や動画によって共有すべきものなどもあるだろう、とのことから本機能を試験導入しています。

3) 画像・動画の一覧参照

ImageBox の操作は、サイドメニュー「ImageBox」から、「Image Box 画面」を表示して操作します。

一覧には画像から自動作成されたサムネールが投稿順に表示されます。

図 89 ImageBox 一覧・画面

投稿画像等には、それぞれコメントを付与することが可能で、それらは各画像の上、「編集」から画像の詳細表示画面から実施します。 その他、ダウンロード、削除も可能です。

図 90 Image の詳細画面

4） 画像・動画の投稿

あらかじめ撮影した画像、動画の投稿をします。

画像は、アップロードされたファイルをそのまま保存するのではなく、長編が 1280px 以上の場合には、1280px に縮小された保存されることに注意してください。 これは目的が、画像そのものの保存ではないからです。

動画は MP4 形式を原則としますが、そうでない場合、変換が可能であれば RemoNavi SaaS サーバにて MP4 変換します。ただし、動画変換はサーバの CPU を著しく消費するため、できる限り MP4 での投稿を推奨します。

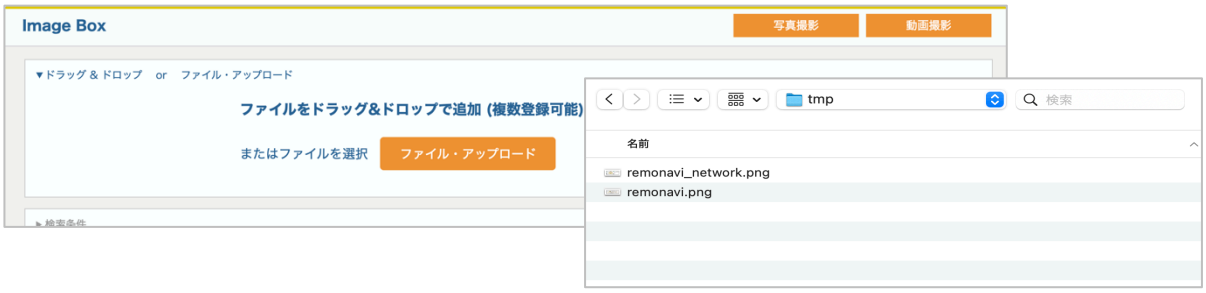


図 91 画像・動画ファイルのアップロード

アップロードは、ImageBox 一覧画面の上部「ドラッグ＆ドロップ or ファイルアップロード」のアコーディオン表示を開いて行います。ファイルの選択は、当該エリアにドラッグ＆ドロップするか、「ファイルアップロード」のファイル選択で行います。

同時アップロードファイル数　　５ファイル
１ファイルのサイズ上限　　1Gbyte （動画が考慮して）

１ファイルのサイズ上限は 1Gbyte と大きくしていますが、サーバのディスク容量、ネットワーク帯域には限りがあり、そのようなアップロード負荷は確実にリモート接続等に影響を与えます。 また、この投稿による RemoNavi SaaS サーバのディスクフルなどのチェックはしておりません。 十分なモラルを持って利用してください。
サーバのディスク使用量などは、サイドメニュー「システム/システム情報」から参照可能です。 使用デイスク容量が **20G** を超えないように運用してください。

5） リアルタイム撮影による投稿

遠隔環境などでの詳細状況説明のためにカメラ機能を具備した端末からのブラウザ操作だけで、状況の画像や動画を共有するために、提供しています。 ある意味、余裕のない状況下での緊急避難的な機能と考えてください。

リアルタイム撮影による投稿は、一覧画面の上部メニュー「写真撮影」、「動画撮影」から実施します。

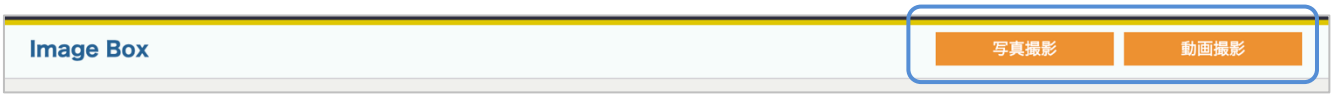


図 92 リアルタイム撮影による投稿

写真撮影、動画撮影は、それぞれ以下の画面が表示されます。

撮影完了後、「備考」にコメントを入力してアップロードします。

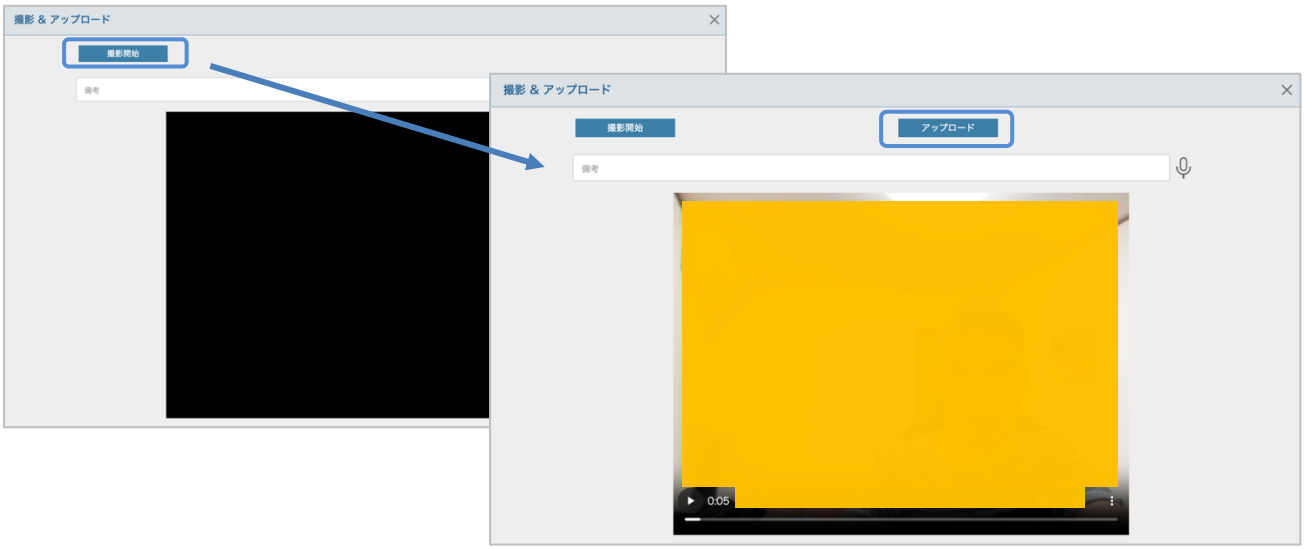


図 93 リアルタイム撮影のモーダル画面

このカメラの向きは、外側カメラ利用にしており、タブレットやスマートフォンなどは、対象物を撮影することを前提としております。PC の場合はマシンの設定あるいはブラウザの設定に依存します。