GENESYS CLOUD 専用 管理ツール

GC ProBox

導入マニュアル

ダウンロード・インストールから、Genesys Cloud との接続設定まで

対象バージョン：GC ProBox Version 2（2.4.0）
発行：2026 年 11 月
株式会社ソリディア

目次

1. はじめに

1.1 準備するもの

2. ダウンロードとインストール

2.1 インストーラーのダウンロード
2.2 インストール
2.3 アップデート

3. 接続のしくみと Genesys Cloud 側の準備

3.1 接続のしくみ
3.2 2 つの作り方
3.3 A の準備：本人ログイン用の OAuth クライアント
3.4 B：役割と OAuth クライアントを手で作る
3.5 アクセス区分の考え方
3.6 複数の PC・複数の利用者で使う場合
3.7 （任意）ライブ監視

4. GC ProBox の設定

4.1 ライセンス認証
4.2 A：OAuth セットアップで管理者用を作る
4.3 A：利用者用を作って渡す（Standard 以上）
4.4 SV の PC：設定ファイルを読み込む
4.5 B：OAuth クライアントを登録する
4.6 接続の確認と、権限を変えたとき
4.7 （任意）ライブ監視の設定
4.8 使い始める

5. 動作環境と通信要件

5.1 動作環境
5.2 通信要件（接続先）
5.3 データの保存と送信

6. 困ったとき

お問い合わせ

1. はじめに

本書は、GC ProBox をお使いいただくまでの準備と設定の手順をまとめたものです。次の 4 つのステップで進めます。

ステップ	作業	作業する場所	本書
1	インストーラーをダウンロードし、PC にインストールする	お使いの PC	2 章
2	接続のしくみを知り、作り方（A か B）を選んで準備する	Genesys Cloud（管理画面）	3 章
3	ライセンスキーを入力し、役割と OAuth クライアントを作って登録する（A は GC ProBox の画面で作れます）	GC ProBox	4 章
4	接続を確認し、使い始める	GC ProBox	4 章

1.1 準備するもの

準備するもの	内容
ライセンスキー	ご購入後にメールでお送りするライセンスキーの一覧です。ご利用者 1 名につき 1 つのキーを使います。
PC	Windows 10 または Windows 11（64bit）の PC。1 つのライセンスキーで PC 2 台まで使えます（5.1 節）。
Genesys Cloud の管理者アカウント	役割と OAuth クライアントを作成できるアカウントが必要です。管理者の役割（admin）か、次の 7 つの権限を持つアカウントで作業してください。Authorization > Role > View / Add / Edit、Oauth > Client > View / Add / Edit、Authorization > Grant > Add
通信の確認	PC から Genesys Cloud と、GC ProBox のライセンス認証サーバーなどへ接続できることを、事前にネットワーク管理者の方と確認してください（5.2 節）。

ポイント

作業時間の目安は、PC 1 台あたり約 15 分です。

Genesys Cloud 側の準備（3 章）と、役割と OAuth クライアントの作成は、最初の 1 回だけです。2 台目以降の PC では、作ったクライアントを登録する（または設定ファイルを読み込む）だけで済みます。

2. ダウンロードとインストール

2.1 インストーラーのダウンロード

1. ブラウザで次のページを開きます。

   https://d1fn5mh4spwkno.cloudfront.net/wizard/download.html?environment=mypurecloud.jp&langTag=ja

2. 最新バージョンの確認が終わるまで待ち、ダウンロードボタンからインストーラー（GC ProBox Setup 〈バージョン〉.exe）を保存します。

2.2 インストール

1. 保存したインストーラーをダブルクリックして実行します。
2. 「Windows によって PC が保護されました」と表示された場合は、**詳細情報** をクリックし、**実行** を押します（下の注意を参照）。
3. インストールの種類（このユーザーだけ／すべてのユーザー）とインストール先を選び、画面の案内に沿って進めます。インストール先は変更できます。
4. インストールが終わると、デスクトップとスタートメニューに「GC ProBox」が作られます。そのまま起動して、4 章へ進んでください。

注意：「Windows によって PC が保護されました」について

GC ProBox のインストーラーには、現在コード署名が付いていないため、Windows の SmartScreen がこの画面を表示することがあります。

ダウンロード元が上記の URL であることを確認のうえ、実行してください。社内の規定でインストールが制限されている場合は、情報システム部門の方にご相談ください。

2.3 アップデート

GC ProBox は、起動中に新しいバージョンを自動で確認します。新しいバージョンがあるとダウンロードが始まり、終わると再起動の確認が表示されます。再起動すると新しいバージョンに切り替わります。

3. 接続のしくみと Genesys Cloud 側の準備

3.1 接続のしくみ

GC ProBox は、Genesys Cloud の「OAuth クライアント」を使って接続します。OAuth クライアントは、GC ProBox が Genesys Cloud に入るための**入館証**のようなものです。入館証には番号と暗証番号があり、それぞれ**クライアント ID** と**クライアントシークレット**にあたります。

入館証で何ができるかは、OAuth クライアントに付ける次の 2 つで決まります。

付けるもの	決まること	例
役割	できること（権限のまとまり）	キューを見る、ユーザーのスキルを変える
アクセス区分	見える範囲	すべての区分、東京拠点の区分だけ

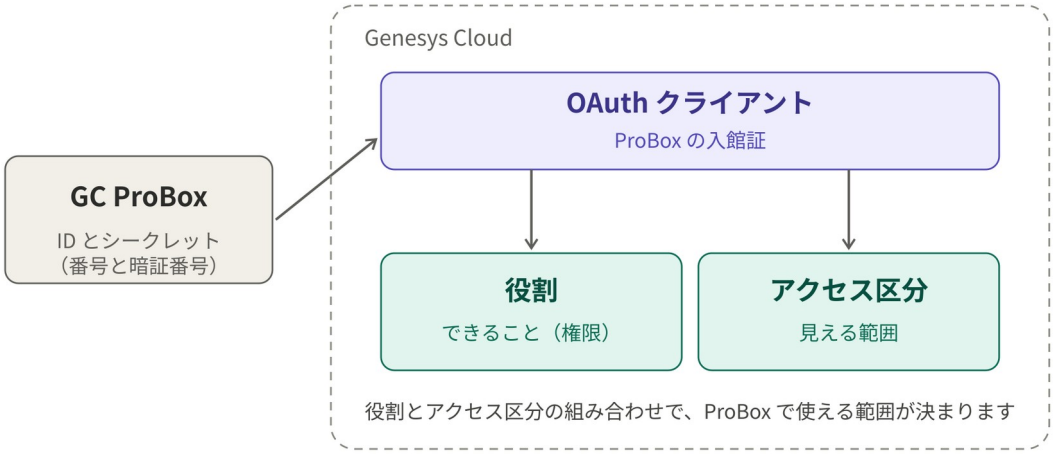

図 3-1　GC ProBox・OAuth クライアント・役割・アクセス区分の関係

入館証は、使う人に合わせて 2 種類を使い分けます。

	管理者用	利用者用
使う人	管理者	SV など、管理者以外の人
できること	GC ProBox の全機能	選んだ機能だけ
見える範囲	すべての区分	選んだ区分だけ（すべての区分も選べます）
渡し方	管理者どうしで共有し、シークレットは各社の方法で保管する	パスワード付きの設定ファイルで渡す

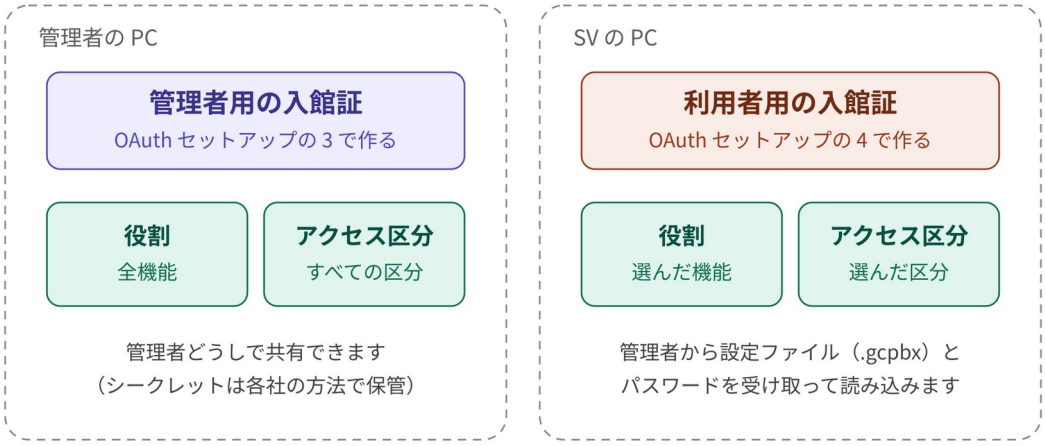

図 3-2　管理者用と利用者用

注意：管理者用の OAuth クライアント

管理者用の OAuth クライアントは、GC ProBox の全機能を使える強い入館証です。管理者の PC だけで使い、SV の PC には利用者用を渡してください。

3.2 2 つの作り方

役割と OAuth クライアントは、次のどちらかの方法で作ります。**A をおすすめします。**

	A. OAuth セットアップで作る（おすすめ）	B. Genesys Cloud の画面で手で作る
作る場所	GC ProBox の API 設定「OAuth セットアップ」	Genesys Cloud の管理画面
権限の選び方	GC ProBox が、エディションに合わせて必要な権限をまとめて入れる	表 3-1〜3-3 を見て 1 つずつ付ける
利用者用（SV 用）	使わせる機能とアクセス区分を選んで作れる（Standard 以上）。設定ファイルで渡せる	役割とクライアントをそれぞれ手で作り、ID とシークレットを渡す
事前の準備	本人ログイン用の OAuth クライアントを 1 つ作る（3.3 節）	なし
向いている場合	ほとんどの場合	会社の決まりで、OAuth クライアントを Genesys Cloud の画面でしか作れない場合など

- A は、Lite を含むすべてのエディションで使えます。利用者用を作るのは Standard 以上です。
- A はメイン組織だけで使えます（サブ組織では B で作ります）。
- A を選んだ場合は 3.3 節のあと 4.1〜4.4 節へ、B を選んだ場合は 3.4 節のあと 4.1 節・4.5 節へ進んでください。

3.3 A の準備：本人ログイン用の OAuth クライアント

OAuth セットアップは、作業する人が**ご本人の Genesys Cloud アカウントでログインして**行います。そのためのクライアントを、最初に 1 つだけ Genesys Cloud で作ります。このクライアントは、ライブ監視（Operation Map・Transcription Visualizer）の本人ログインにも使います。

1. **管理** ＞ **統合** ＞ **OAuth** を開き、**クライアントを追加** を押します。
2. 次のとおり入力して保存します。

項目	入力する内容
アプリ名	例：GC ProBox 本人ログイン
付与タイプ	コード認証（Code Authorization）
認可されたリダイレクト URI	http://localhost/gcprobox-oauth
スコープ	users:readonly、authorization:readonly、notifications、conversations、analytics:readonly、speech-and-text-analytics:readonly、authorization、oauth 8 つすべてが必要です。

3. 表示されたクライアント ID を控えます（4.2 節で入力します。シークレットは使いません）。

ポイント

・スコープの 8 つのうち、authorization と oauth は役割とクライアントを作るために、残りの 6 つはライブ監視に使います。

・作業する人の役割には、1.1 節の 7 つの権限が必要です。足りないときは、OAuth セットアップの確認（4.2 節の手順 2）で ✗ が付いて止まります。

3.4 B：役割と OAuth クライアントを手で作る

B を選んだ場合は、Genesys Cloud の管理画面で、役割を作り、その役割を割り当てた OAuth クライアント（付与タイプ：クライアントの資格情報）を作成します。

3.4.1 役割を作成する

1. Genesys Cloud に管理者でログインし、**管理** ＞ **ユーザー** ＞ **役割/権限** を開きます。
2. **役割を追加** を押し、名前を入力します（例：GC ProBox 接続用）。
3. **権限** タブで、3.4.2 節の表の権限を付与します。検索欄に「Routing > Queue > 」のように入力すると、目的の権限を絞り込めます。
4. **保存** を押します。

3.4.2 役割に付与する権限

ご契約のエディションに合わせて、次の表の権限を付与してください。表記は Genesys Cloud の権限画面と同じ「ドメイン > エンティティ > アクション」です。

OAuth セットアップ（A）で作る管理者用の役割には、この表の権限がまとめて入っています（Lite・Standard 用 39 個、Professional 用 75 個）。

ポイント

・付与しなかった権限に関係する機能は、GC ProBox で使えないか、メニューが表示されないだけです。アプリ全体が動かなくなることはありません。

・権限はあとから追加できます。追加したあとは、GC ProBox の API Setting で「トークン再取得」を押してください（4.6 節）。

・「（任意）」の権限は、その機能を使う場合だけ付与してください。

表 3-1　すべてのエディションで必要な権限（接続と表示）

権限	用途
Oauth > Client > View	接続時に、この OAuth クライアントに割り当てたアクセス区分を確認します
Authorization > Division > View	アクセス区分の名前の表示と、区分による絞り込み
Authorization > Role > View	役割の一覧（Data Explorer の「役割」タブなど）
Authorization > License > View	役割ごとのライセンスの表示（任意）
Directory > User > View	ユーザーの一覧と詳細
Directory > Group > View	グループの一覧とメンバー
Groups > Work Team > View	チームによる絞り込み（任意）
Routing > Queue > View	キューとキューメンバーの一覧
Routing > Skill > View	スキルの一覧（アクセス区分付きのスキルも表示するために必要）
Routing > Skill Group > View	スキルグループの一覧とメンバー
Routing > Wrap-up Code > View	ラップアップコードの一覧
Presence > Presence Definition > View	在席状態の名前の表示
Analytics > Conversation Aggregate > View	着信・応答・放棄などの集計
Analytics > Conversation Detail > View	インタラクションの検索
Analytics > User Aggregate > View	ユーザー別の実績
Analytics > User Detail > View	ログイン人数・ステータスの推移
Analytics > Queue Observation > View	キューのリアルタイムの状況（待ち呼・対応中）
Architect > Flow > View	IVR・フローの一覧
Routing > Call Route > View	DID に割り当てた IVR の表示（任意）
Routing > Schedule Group > View	DID の詳細に出るスケジュールグループ（任意）
Scripter > Script > View	スクリプトの一覧
Telephony > Plugin > All	DID・電話・トランク・サイトの情報

表 3-2　Standard 以上で追加する権限（Power Tools・リアルタイム表示など）

権限	用途
Directory > User Profile > Edit	Power Tools の「ユーザー設定の変更」「ユーザープロファイル編集」

権限	用途
Directory > User > Edit	プロファイル項目の保存
Routing > Skill > Assign	ユーザーへのスキルの付与・変更・解除（まとめて入れ替えを含む）
Routing > Queue Member > Manage	キューメンバーの追加・削除、キュー参加（オン／オフ）の切り替え
Routing > Queue > Edit	「キュー設定の変更」と、キューへのラップアップコードの割り当て
Routing > Wrap-up Code > Add / Edit / Delete	ラップアップコードの登録・変更・削除
Presence > User Presence > Edit	ユーザーの在席状態の変更
Analytics > Agent State > View	Operation Map で、対応中の会話を特定する
Analytics > Data Export Static Link > View	DataExplorer の「固定リンク」で、Genesys Cloud の固定リンクからレポートを取得する（任意）
Conversation > Communication > View	会話の詳細の取得
Audits > Audit > View	共有フォルダのデータの更新確認（任意）
Recording > Recording > View	インタラクションの文字起こしの表示（任意）
Speech And Text Analytics > Data > View	同上（任意）
Conversation > Summary > View	インタラクションの要約の表示（任意）
Outbound > Campaign > View	インタラクションに出るキャンペーン名の表示（任意）

表 3-3　Professional で追加する権限

機能	権限	用途
ユーザー管理	**Directory > User > Add**	ユーザーの作成・招待
	Directory > User > Set Password	ユーザー作成時の招待の送信（ログイン方式「招待する」を使う場合）（任意・SSO 運用時は必須）
	Directory > Organization > Admin	作成時のパスワードポリシーの取得（パスワード自動生成を使う場合）（任意）
	Authorization > Grant > View / Add / Delete	役割の保有状況の確認・一括割り当て・一括解除
	Routing > Queue > Add	キューの CSV インポート（新規作成）
	Routing > Predictor > View	キュー(Pro) で、ルーティング方法「プレディクティブ」を正しく表示する（任意）
	Routing > Skill > Manage	スキルの一括作成・一括削除
	Audits > Audit > View	スキルの最終更新日時の表示（任意）
	Authorization > Audit > View	スキルの最終更新日時の表示（任意）
ルーティング	**Routing > Call Route > View / Add / Edit**	コールルーティング（IVR）の表示・作成・変更
	Routing > Schedule > View / Add / Edit	スケジュールの表示・作成・変更

機能	権限	用途
	Routing > Schedule Group > View / Add / Edit	スケジュールグループの表示・作成・変更
	Routing > Emergency Group > View / Edit	緊急グループの表示・切り替え
	Architect > Dependency Tracking > View	緊急グループの参照先の表示（任意）
	Architect > User Prompt > View	プロンプトの一覧と試聴、コールフローデザイナー（β）での音声の選択
	Architect > System Prompt > View	保留音（システムプロンプト）の表示
	Architect > Flow > Add / Edit / Publish	コールフローデザイナー（β）でフローを作成・公開
	Architect > UI > View	同上（Architect の表示）
	Architect > Job > Create / View	同上（フローのアップロード）
テレフォニー	**Telephony > Plugin > All**	Edge・トランク・サイト・DID・電話の表示と変更
インタラクション管理	**Recording > Recording > View**	録音の検索と取得（すべての録音機能に必要）
	Recording > Recording Segment > View	録音ダウンロード
	Recording > Recording > Download	録音ダウンロード
	Recording > Recording Job > Add / View / Edit / Delete	録音削除のジョブの作成・実行・取り消しと、ジョブ管理
	Recording > Recording > Edit Retention	録音の削除予定日の変更（録音削除）
	Speech And Text Analytics > Data > View	トランスクリプトの取得
	Speech And Text Analytics > aiSummary > View	要約の取得（任意）

録音・インタラクション管理とユーザー作成についての補足

・Recording > Recording > View がないと、Professional の「インタラクション管理」の 4 つのタブ（録音ダウンロード・録音削除・トランスクリプト DL・ジョブ管理）がすべて表示されません。

・View はあるが、各タブに必要な権限が足りない場合は、操作したときにエラーが表示されます。表 3-3 の権限をご確認ください。

・録音の再生（Power Tools ＞ 録音再生）は、PC 内の録音ファイルを再生する機能のため、Genesys Cloud の権限は不要です（Standard 以上）。

・Directory > User > Set Password がないと、ログイン方式「招待する」でユーザーを作成したとき、作成はされますが招待の送信に失敗し、エラーが表示されます。SSO で運用する場合は付与してください。

・Routing > Predictor > View がないと、キュー(Pro) のルーティング方法は推測で表示するため、「プレディクティブ」を正しく表示できないことがあります。

3.4.3 OAuth クライアントを作成する

1. 管理 ＞ **統合** ＞ **OAuth** を開き、**クライアントを追加** を押します。

2. 次のとおり入力します。

項目	入力する内容
アプリ名	わかりやすい名前（例：GC ProBox_山田）
説明	任意（例：GC ProBox 接続用）
トークンの有効期間	86400 秒（既定値のままで構いません）
付与タイプ	クライアントの資格情報（Client Credentials）

3. **役割** タブで、3.4.1 節で作成した役割を割り当てます。あわせて、その役割を適用する**アクセス区分**を選びます（3.5 節）。
4. **保存** を押します。表示された**クライアント ID** と **クライアントシークレット** を控えます。

> **注意：クライアントシークレットの扱い**
> クライアントシークレットはパスワードと同じ扱いです。メールやチャットに貼り付けず、安全な方法で共有してください。
> 漏えいのおそれがある場合は、シークレットを再発行し、GC ProBox の設定を更新してください（6 章）。

3.5 アクセス区分の考え方

GC ProBox に表示される範囲と、変更できる範囲は、OAuth クライアントの役割に割り当てたアクセス区分で決まります（3.1 節）。

- 組織全体を管理する管理者は、「すべての区分」の入館証（管理者用）を使います。
- 拠点や委託先ごとに見せる範囲を分けたい場合は、その区分だけを選んだ利用者用を、利用者のグループごとに作ります（A：4.3 節）。B の場合は、その区分だけを割り当てた OAuth クライアントを手で作ります。

> **注意：役割は作業する人にも付きます**
> Genesys Cloud の決まりで、OAuth クライアントに付ける役割は、作業する人のアカウントにも同じアクセス区分で付いている必要があります。A では GC ProBox が自動で付けます（付けた役割は外しません）。

3.6 複数の PC・複数の利用者で使う場合

使う人	おすすめの方法
管理者が複数いる	管理者用の OAuth クライアントを共有します。2 人目以降は、OAuth セットアップの「今ある管理者用クライアントを使う」を選び、保管しているシークレットを入れます（4.2 節）
SV など管理者以外の人	利用者用を作り、設定ファイルとパスワードを渡します（4.3 節・4.4 節）

1 つの OAuth クライアントを使う人数は、**20 人まで**を目安にしてください。理由は次のとおりです。

理由	内容
API の利用枠	Genesys Cloud の API には、OAuth クライアントごとの利用上限があります。クライアントを分けると、ほかの人の操作の影響を受けません。
操作の記録	GC ProBox からの変更は、Genesys Cloud の監査ログに「クライアント」として記録されます。クライアントを分けると、誰の操作かを区別できます。

誰がどの PC でどのクライアントを使っているかを記録しておくと、シークレットを再発行するときに困りません（Professional では「IT と統合」›「OAuth クライアント」のメモに書けます）。

3.7 （任意）ライブ監視

Operation Map から通話のモニター・コーチ・割り込みを行う場合と、Transcription Visualizer で通話の文字起こしを表示する場合（AI の会話の監視、Operation Map からの文字起こしの表示を含む）だけ、SV ご本人の Genesys Cloud アカウントでログインします。どちらも使わない場合は、この節は不要です。

- ログインには、3.3 節の本人ログイン用クライアントを使います。B で作った場合や、まだ作っていない場合は、3.3 節のとおり作ってください（ライブ監視だけで使う場合も、スコープは 3.3 節の 8 つをおすすめします）。
- 監視を行う SV ご本人のユーザーに、次の権限を含む役割を割り当ててください。

権限	用途
Conversation > Call > Monitor	通話のモニター
Conversation > Call > Coach	通話のコーチ
Conversation > Call > Barge	通話への割り込み
Conversation > Message > Monitor	チャット・メッセージのモニター
Conversation > Call > Add	担当者への内線発信
Conversation > Transcription > View	Transcription Visualizer での文字起こしの表示
Analytics > Conversation Detail > View	Transcription Visualizer の集計（通話の検索）
Speech and Text Analytics > Data > View	Transcription Visualizer の集計（通話後の文字起こしの取得）

Conversation > Transcription > View は、Genesys Cloud 側ではアクセス区分で範囲を限定できない権限です。GC ProBox の Transcription Visualizer では、この権限を含む役割を SV ご本人に割り当てたアクセス区分のキューの通話だけを表示します。役割は、その SV が文字起こしを見てよい範囲のアクセス区分に割り当ててください。

ポイント：Transcription Visualizer を使う場合

Transcription Visualizer は、Genesys Cloud 側で通話の文字起こし（Agent Copilot・音声の文字起こし）が有効になっていることが前提です。

スコープや役割の権限を追加・変更したあとは、Transcription Visualizer で本人でログインし直してください。AI の会話の監視では、Transcription Visualizer で監視するボットフローを選びます。

画面の操作は「GC ProBox Transcription Visualizer 操作マニュアル」をご覧ください。

4. GC ProBox の設定

4.1 ライセンス認証

1. GC ProBox を起動します。初回は「GC_ProBox ライセンス認証」の画面が表示されます。
2. メールでお送りしたライセンスキーを 1 つ入力し、**認証する** を押します。
3. 認証が終わると、API 設定の画面（「初回セットアップ」の案内つき）に切り替わります。

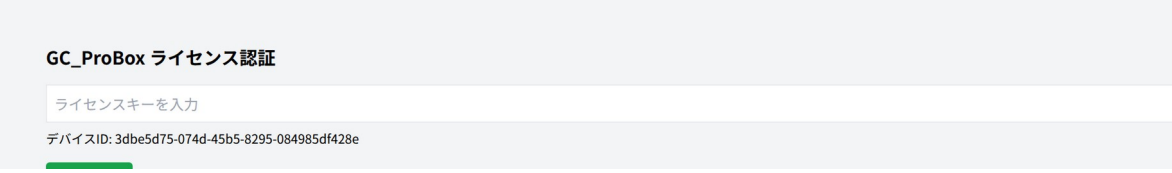

図 4-1　ライセンス認証の画面（デバイス ID は PC ごとに異なります）

ポイント

・1 つのライセンスキーは、1 名のご利用者が PC 2 台まで使えます。3 台目の PC では認証できません。
・PC を入れ替える場合は、ソリディアまでご連絡ください。

A の場合は 4.2 節、B の場合は 4.5 節へ進みます。

4.2 A：OAuth セットアップで管理者用を作る

API 設定の「OAuth セットアップ」タブで行います。画面は「1」〜「4」の順に並んでいます。

1. 「1. 本人ログイン用の OAuth クライアント」に、3.3 節で控えたクライアント ID を入れて **保存** を押します。
2. 「2. ログインして準備を確かめる」で **確かめる** を押し、ご本人の Genesys Cloud アカウントでログインします。組織・スコープ・あなたの役割の権限が確かめられます（この時点では何も作りません）。✕ が出たら、画面の案内のとおり直してから、もう一度 **確かめる** を押します。
3. 「3. 管理者用の役割とクライアント」で、表示されたボタンを押します。この PC の状態によって、次のどれかになります。

この PC の状態	動き
初めて（組織に管理者用のクライアントが無い）	役割と OAuth クライアントを作り、この PC の API 接続設定にそのまま登録します
組織に管理者用のクライアントがある（2 台目以降・2 人目以降の管理者）	「今ある管理者用クライアントを使う（おすすめ）」を選び、保管しているシークレットを入れて登録します。人ごとに分けたいときは「別に作る」を選びます
この PC にもう接続用のクライアントがある（B で作ったものなど）	クライアントは作らず、役割を作ってそのクライアントに足します

4. 作った直後に、**クライアントシークレットが黄色の枠に一度だけ表示されます**。パスワード管理ツールなど、決まった場所に保管してから **保存したので閉じる** を押します。

注意：シークレットの扱い

・Genesys Cloud では、シークレットは作ったときにしか確かめられません。画面を離れると二度と表示できません。

・メールやチャットに貼り付けないでください。

・作った役割は、作業したあなたのアカウントにも付きます（Genesys Cloud の決まり。3.5 節）。

ポイント

管理者用の役割の権限は、Lite・Standard 用が 39 個、Professional 用が 75 個です（3.4.2 節の表と同じ内容）。2 回目以降に押すと、役割の権限を最新にするだけです。

4.3 A：利用者用を作って渡す（Standard 以上）

SV など管理者以外の人には、使わせる機能とアクセス区分を絞った利用者用を作って渡します。

1. 「4. 利用者用の役割とクライアント」で、「作るもの」を「新しく作る」にし、役割の名前を入れます（既定は「GC ProBox 利用者用」。クライアントにも同じ名前が付きます）。
2. 使わせる機能を選びます。閲覧だけの機能（稼働状況サマリー・KPI Navi・Operation Map と Transcription Visualizer の表示・DataExplorer の会話の中身を含まないタブなど）は、選ばなくても入ります。

選べる機能	使えるようになるもの
会話の中身	DataExplorer の要約・テキスト化・会話テキスト
現場での操作	キュー中トグル、マルチキュービューのキュー参加、Operation Map のステータス変更
テレフォニー	DataExplorer の DID、管理者ビューのトランク、Power Tools の電話管理（Professional ではテレフォニーのカテゴリも）
Power Tools の各メニュー	ユーザー設定の変更・ユーザープロファイル編集・キュー設定の変更・ラップアップコード
Professional のカテゴリ（Professional のときだけ）	ユーザー管理・ルーティング・インタラクション管理

3. 画面の右の「この役割で使えるメニュー」で、使えるようになるメニューを確かめます。Genesys の権限は一部が重なっているため、選んでいない機能が使えるようになることがあります（黄色の枠に「選んでいないのに使えるもの」と出ます）。
4. アクセス区分で「すべての区分」か「区分を選ぶ」を選びます。
5. **役割とクライアントを作る** を押します。
6. 黄色の枠にシークレットが一度だけ表示されたら、**設定ファイルとして書き出す（パスワード付き）** を押し、パスワード（12 文字以上で、英字と数字を含む）を 2 回入れて書き出します。

注意：設定ファイルの渡し方

・パスワードは、ファイルとは別の方法（口頭など）で伝えてください。ファイルとパスワードを同じメールで送らないでください。

・設定ファイルは共有フォルダには置かず、手で渡してください。

ポイント

・利用者用は何個でも作れます（例：SV 用と、閲覧だけの用）。

・あとから機能や区分を変えるときは、「作るもの」で作った利用者用を選び直します。クライアントと設定ファイルはそのままで、配り直しは要りません（SV の PC には、次にトークンを取り直したときに反映されます）。

・「管理者」を選ぶと、管理者用と同じ権限を全部付けます。区分を絞った管理者を作りたいときに使えます。

4.4 SV の PC：設定ファイルを読み込む

SV の PC では、OAuth セットアップは使いません。

1. 4.1 節のとおりライセンス認証をします。
2. API 設定の画面で **設定ファイルを読み込む** を押し、管理者から受け取ったファイル（.gcpbx）を選んで、パスワードを入れます。
3. 読み込むと接続設定が終わります（クライアント ID・シークレット・リージョンが入ります）。

出た文	確かめること
パスワードが違います	パスワードを入れ直す
ファイルの組織が、このライセンスの組織と違います	管理者に、どの組織のファイルか確かめる
ファイルが壊れています	管理者にファイルを書き出し直してもらう

4.5 B：OAuth クライアントを登録する

1. **API ホスト** で、お使いの Genesys Cloud のリージョンを選びます。

リージョン	選ぶ項目	API のアドレス
東京	APNE1 (Japan)	api.mypurecloud.jp
大阪	APNE3 (Japan)	api.apne3.pure.cloud

2. **クライアント ID** と **クライアントシークレット** に、3.4.3 節で控えた値を入力します。
3. **保存** を押します。接続が確認されると、接続ステータスが「接続済み」になり、このライセンスがお使いの Genesys Cloud 組織に紐付きます（「組織バインド済み」と表示されます）。

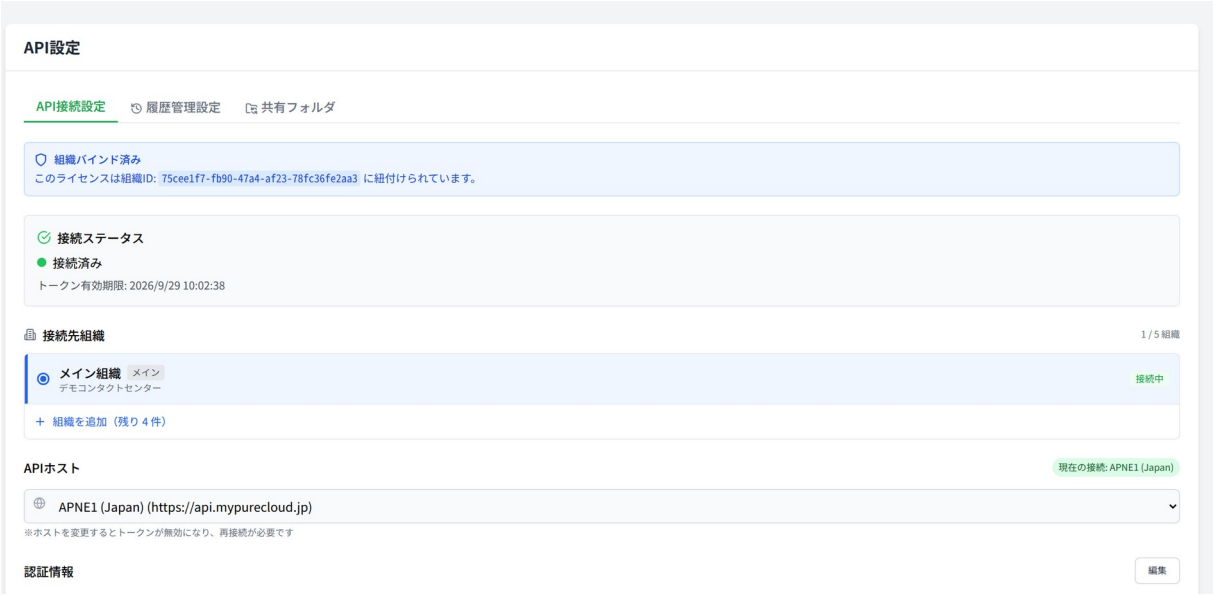

図 4-2　API 設定の画面（接続済みの例。画面の値は架空のものです）

注意：組織の紐付けについて

・最初に保存した組織に、ライセンスが紐付きます。2 台目の PC でも、同じ組織の OAuth クライアントを登録してください。

・別の組織の OAuth クライアントを登録すると「このライセンスは別の組織…」と表示され、保存できません。組織を変更する場合は、ソリディアまでご連絡ください。

4.6 接続の確認と、権限を変えたとき

ボタン	使う場面
接続テスト	Genesys Cloud に接続できるかを確認します。
トークン再取得	役割の権限を追加・変更したあとに押します。新しい権限が GC ProBox に反映されます。
クリア	登録した OAuth クライアントの情報を消します。

4.7 （任意）ライブ監視の設定

3.7 節のライブ監視を使う場合だけ設定します。

1. API 設定の画面の「ライブ監視ログイン」で、**ライブ監視用クライアント ID** に 3.3 節のクライアント ID を入力し、**クライアント ID を保存** を押します。
2. **本人でログイン** を押し、表示された Genesys Cloud のログイン画面で、SV ご本人のアカウントでログインします。



図 4-3　ライブ監視ログインの設定

ログインの有効期間は約 24 時間です。翌日以降は、Operation Map または Transcription Visualizer を開いたときに再ログインを求められます。

4.8 使い始める

保存が終わると、GC ProBox が Genesys Cloud からユーザー・キュー・役割などのデータを取得します。組織の規模によって、数十秒から数分かかります。取得が終わると、各メニューが使えるようになります。

Standard 以上では、API 設定の「履歴管理設定」「共有フォルダ」タブで、データの履歴保存や、チームでのデータ共有を設定できます（任意）。

5. 動作環境と通信要件

5.1 動作環境

項目	内容
OS	Windows 10 / Windows 11（64bit）
ネットワーク	インターネットに接続できること（5.2 節の接続先へ HTTPS で通信できること）
Genesys Cloud	東京（APNE1）または大阪（APNE3）リージョンの組織
利用できる台数	1 ライセンスあたり 1 名・PC 2 台まで

5.2 通信要件（接続先）

Genesys Cloud への通信（ブラウザで Genesys Cloud を使うときと同じ接続先）に加えて、GC ProBox は次の接続先と通信します。社内のネットワークで通信先を制限している場合は、これらへの接続を許可してください。

接続先	用途	必要な場面
l7jgmnk35d.execute-api.ap-northeast-1.amazonaws.com	ライセンス認証と、同時利用の確認（起動中は定期的に通信します）	常に
gc-probox-releases.s3.ap-northeast-1.amazonaws.com	アップデートの確認とダウンロード	起動中（定期的に確認）
d1fn5mh4spwkno.cloudfront.net	インストーラーのダウンロード	インストール時

通信はすべて TCP 443 番ポート（HTTPS）で、PC から外へ向かう通信のみです。外部から PC への着信は使いません。

ポイント：ライセンス認証の通信について

・起動時にライセンスを確認し、起動中は同時利用の確認のため 30 秒ごとに通信します。

・ライセンス認証サーバーと約 2 分以上通信できないと、「サーバーに接続できません」と表示されて操作できなくなります。通信が戻ったら「再試行」で再開できます。

注意：プロキシサーバーについて

現在の GC ProBox は、プロキシサーバーを経由した接続に対応していません。インターネットへの接続にプロキシが必須の環境では、接続できない場合があります。導入前にソリディアまでご相談ください。

5.3 データの保存と送信

- OAuth クライアントの情報、取得したデータ（キャッシュ）は、お使いの PC のユーザーフォルダ内に保存されます。取得したデータは暗号化して保存します。
- Transcription Visualizer は、会話の本文を保存しません。ワード検知と AI の会話の判定の記録（本文なし）だけを、お使いの PC に保存します。記録は保持期間（7 日〜90 日）を過ぎると自動で削除します。

- ライセンス認証のために、ライセンスキー・デバイス ID・Genesys Cloud の組織 ID・OAuth クライアント ID をライセンスサーバーへ送信します。クライアントシークレットや、Genesys Cloud から取得したデータは送信しません。
- ダウンロードした録音は、既定では暗号化して保存します（Professional）。

6. 困ったとき

こんなとき	確認すること
インストール時に「Windows によって PC が保護されました」と表示される	2.2 節の注意を参照し、「詳細情報」→「実行」で進めてください。
ライセンス認証でエラーになる	ライセンスキーの入力ミスがないか確認してください。3 台目の PC では認証できません（4.1 節）。
保存すると「このライセンスは別の組織…」と表示される	最初に紐付けた組織と別の組織の OAuth クライアントを登録しています（4.5 節）。
接続テストに失敗する	API ホスト（リージョン）、クライアント ID・シークレット、付与タイプが「クライアントの資格情報」になっているかを確認してください。社内ネットワークでは、5.2 節の接続先への通信が許可されているかも確認してください。
メニューやタブが表示されない／操作でエラーになる	役割の権限が足りない可能性があります。A の場合は利用者用の機能を選び直し（4.3 節）、B の場合は 3.4.2 節の権限を追加し、「トークン再取得」を押してください。
アクセス区分のついたスキルが表示されない	Routing > Skill > View を付与してください。
「サーバーに接続できません」と表示されて操作できない	ライセンス認証サーバーとの通信が切れています。ネットワークを確認し、「再試行」を押してください（5.2 節）。
画面の更新が遅い、「レート制限」と表示される	複数の人で 1 つの OAuth クライアントを共有している場合は、個別のクライアントへの切り替えをご検討ください（3.6 節）。
OAuth セットアップの「確かめる」で ✕ が出て止まる	× の権限・スコープを足してから、もう一度 確かめる を押してください（3.3 節）。管理者でない方は、管理者から設定ファイルを受け取り、「設定ファイルを読み込む」で読み込んでください（4.4 節）。
OAuth セットアップのタブが出ない／使えない	ライセンス認証が終わっているか、メイン組織に接続しているかを確かめてください（サブ組織では使えません）。
クライアントシークレットをなくした・漏えいのおそれがある	シークレットを再発行し、使っている PC で入れ直してください。Professional は「IT と統合」›「OAuth クライアント」で再発行できます（新しいシークレットは一度だけ表示。利用者用は設定ファイルも書き出せます）。Lite・Standard は Genesys Cloud の 管理 ＞ 統合 ＞ OAuth で再発行します。
使わなくなった OAuth クライアントを消したい	Professional は「IT と統合」›「OAuth クライアント」で削除できます（この PC が使っているものは削除できません。役割は残ります）。Lite・Standard は Genesys Cloud の画面で削除します。

お問い合わせ

解決しない場合は、GC ProBox の画面右上の「FAQ」からチャットでご質問いただくか、次のフォームからお問い合わせください。

https://form.run/@solidiagcprobox2025

製品サイト：https://gcprobox.solidia.biz

Genesys および Genesys Cloud は、Genesys Cloud Services, Inc. の商標または登録商標です。本書の画面は架空のデモデータです。