

リモートサポート&管理

PC・サーバー・Mac・タブレット・スマートフォン・組み込み端末
Windows・macOS・Android・iOS・CE

WiseMo ゲストモジュール
例えば、お使いの Windows PC で



Internet



Premises based

WiseMo ホストモジュール
お使いの Mac コンピューターで



WiseMo は、PC やサーバー、Mac コンピューター、スマートフォン、タブレット端末、その他の携帯型／無人端末間など、コンピューターと端末間の遠隔操作を可能にするソフトウェアを開発しています。WiseMo のソフトウェアを使用すれば、業務効率を大幅に向上させる強力な遠隔操作・管理機能を利用でき、時間とコストの節約が可能です。

ゲストモジュール&ホストモジュール

WiseMo のゲストモジュールは、遠隔操作を行いたい他のコンピューターや端末にアクセスするためのコンピューターまたは端末上で動作します。

WiseMo のホストモジュールは、認証されたユーザーがゲストモジュールを使用して安全に遠隔アクセスできるよう、コンピューターや端末上で動作します。

クラウド接続&オンプレミス接続：

ゲストモジュールとホストモジュール間の接続は、インターネット経由で WiseMo の myCloud 接続機能を利用するか、お客様が管理する LAN/WAN ネットワーク上で TCP/IP 通信を直接行う方法で確立されます。

クラウド接続の場合（WiseMo myCloud）お使いのコンピューターまたは端末は、固定回線、Wi-Fi、またはモバイル通信事業者のネットワーク（3G、4G、5G）などを通じてインターネットを利用する必要があります。これにより、ゲストコンピューターとホストコンピューターの両方にインターネット接続があれば、場所を問わず任意のコンピューターや端末にアクセスすることが可能になります。

ゲストコンピューターとホストコンピューター間で TCP/IP を直接使用することで（例えば Wi-Fi、LAN、または WAN などの自社ネットワークを利用）、インターネットトラフィックを回避できるほか、モバイル通信事業者からのデータ料金が発生する可能性もなくなります。

macOS を搭載したコンピューター向けの WiseMo ホストプログラム

macOS 10.9 以降を搭載したコンピューター用のホストモジュールで、ホストコンピューターを簡単・迅速・安全に遠隔操作できるように準備します。このホストモジュールは、WiseMo ゲストモジュールを実行するコンピューターや端末からの遠隔操作を可能にします。

注意：ホストモジュールを実行するコンピューター/端末をリモート制御するには、WiseMo ゲストモジュールを使用します。ゲストモジュールの設定方法については、当該モジュールのチュートリアルを参照してください。利用可能なドキュメントはこちらから確認できます：<https://its.tos.co.jp/support/download/wisemo/>



WiseMo は、PC やサーバー、Mac、スマートフォン、タブレット、その他の携帯型／無人端末間で使用する、クラウドベースおよびオンプレミスペースの遠隔操作ソフトウェアを開発しています。当社のクロスプラットフォームソリューションは、商業・産業用途のリモートサポートおよび管理（RSM）市場を対象としています。

詳細については <https://its.tos.co.jp/products/wisemo/> をご覧ください。

1. Mac ホストのインストール

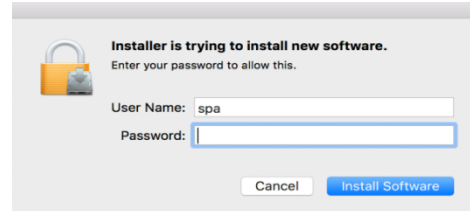
WiseMo ゲストモジュールを実行する認証済みユーザーがリモート制御できるよう、Mac ホストアプリをインストールします。

Mac ホストアプリは、macOS 10.9 から 26 (Tahoe) までのバージョンで動作し、おそらくそれ以降のバージョンでも動作します。

インストールファイルである.pkg ファイルは、myCloud ドメイン（事前にライセンス認証と設定が完了している場合）から提供される場合もあれば、別のソースから提供される場合もあります。この場合、初期ライセンス認証やアクセスセキュリティなどの設定は、ホストアプリを初めて起動した後に別途指定する必要があります。詳細については、以下のセクション 1.1 および 1.2 を参照してください。

インストールファイルを実行すると、インストールウィザードが表示され、ライセンス条項に同意するよう求められます。

macOS からは、プログラムのインストールを許可するようプロンプトが表示されます。また、インストールプログラムがコンピューターを管理するための権限を求める場合もあります。すべての機能を正常に動作させるには、この権限を付与する必要があります。



最新の macOS バージョンでは、初回起動時にリモートコントロールに必要な権限について確認が行われます。詳細については、以下のセクション 1.4 をご参照ください。

1.1 myCloud からのインストールファイル

任意のブラウザーで myCloud ドメインにログインし、「デバイスの管理」>「デプロイメント」ページの右コラムから、macOS ホスト用のデプロイメントリンクを選択してください。

注意：myCloud のデフォルトデプロイメントリンクは、例えば電子メールなどで対象の Mac コンピューターに送信することも可能です。

このような標準の myCloud デプロイメントリンクを使用してダウンロードする場合、ホストは事前にライセンス認証され、myCloud 接続（インターネット経由）と TCP/IP 接続（LAN/WAN 直接接続）の両方に事前設定されます。インストール完了後、ホストは自動的に起動します。

myCloud ドメインで myCloud デバイスアクセス制御（mDAC）が有効になっている場合（myCloud トライアルに登録した際のデフォルト設定です）、デプロイされるホストは mDAC を使用するよう設定されます。mDAC の初期設定では、特定の myCloud ドメインで認証されたゲストユーザーが、そのドメイン内で mDAC で保護されたホストにフルアクセス権を持ってオンライン接続できます。myCloud ドメインの mDAC を有効化/無効化するには、「デバイスアクセス制御」>「ドメインセキュリティ」を選択してください。

ドメインが mDAC に対応していない場合、デプロイされるホストは Mac のシステムセキュリティ管理方式を採用します。この場合、Mac コンピューターに組み込まれた管理者ユーザーと一般ユーザーは、各自の Mac ユーザーアカウントを通じて完全なアクセス権限を持ちます。

デフォルト設定は、ホストのユーザーインターフェースから直接変更するか、構成ウィザードを実行することで簡単に変更できます。また、カスタマイズした設定ファイルを myCloud にアップロードすることで、デプロイ前にデフォルト設定を変更することも可能です。

重要な点として、ホストを mDAC 対応に設定する場合、myCloud ドメインで mDAC を有効にしておく必要があります。そうしないと、ゲストユーザーは mDAC 対応ホストを認識できず、接続することもできません。ホストのセキュリティ方式（システムセキュリティ管理またはその他のアクセス方法）は、myCloud ドメインのセキュリティ設定とは独立して設定可能です。

myCloud ライセンス管理と設定にはインストール時にコンピューターがインターネットに接続可能であることおよび https プロトコルのサポートが必須です。古いコンピューターで http しかサポートしていない場合は、myCloud ドメインへの認証を行うために特別な設定が必要です。詳細は第 4.3.3 節を参照してください。

1.2 myCloud 以外のソースからのインストールファイル

永続ライセンスの納品メールに記載されるダウンロードリンクや、無料試用版のリクエスト後に送付されるリンクからホストをインストールすることができます。

プログラムはこちらからもダウンロード可能です：（バージョン v.20.0）



インストールが完了すると、構成ウィザードが起動します。以下のセクション 1.3 を参照してください。本プログラムのライセンス取得方法としては、myCloud ドメインへのサインアップ、またはライセンスキーの指定のいずれかを選択できます。ライセンスキーは購入することも可能ですし、無料試用をお申し込みの際に提供されるトライアルキーを使用することもできます。

1.3 構成ウィザードについて

構成ウィザードでは、一般的に利用される各種設定項目を順番に案内します。設定完了後は、ホスト画面からウィザードを起動することも可能です。具体的には、ツールバーの「ウィザード」ボタンをクリックすることで起動できます。

以下にウィザードの各ページについて簡潔に説明します。表示されるページは、ウィザード内でのこれまでの選択内容やホストの全体的な状態によって異なります。

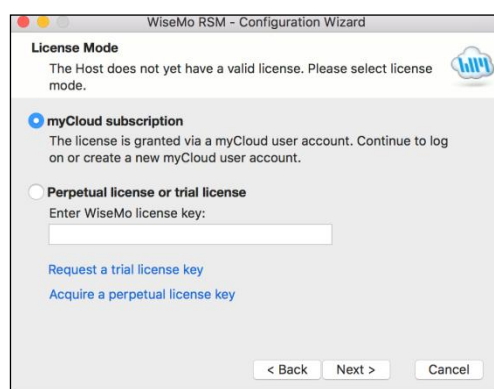
a. ライセンスモードの選択

ホストがまだライセンス認証されていない場合、ウィザードでは使用するライセンスの種類を選択するよう求められます。

1. myCloud ドメインを介したライセンス認証

myCloud ドメインを所有している場合、myCloud ドメインにログオンすることでプログラムのライセンス認証が可能です。myCloud サブスクリプションを選択し、「次へ」をクリックしてください。

次に、myCloud のユーザーアカウント資格情報（通常はメールアドレスとパスワード）を入力します。アカウントが 2 段階認証（2FA）で保護されている場合は、検証コードの入力が求められます。



2. ライセンスキーによるライセンス認証

プログラムのライセンス認証には、ライセンスキー（試用版キーまたは購入した永久ライセンスキー）を入力します。ライセンスキー入力欄にキーを貼り付け、「次へ」をクリックしてください。

ライセンスキー方式を使用することで、インターネット接続が利用できない環境でもプログラムを使用できるようになります。このライセンスキー方式では、myCloud を接続手段として利用することが可能です - インターネットアクセスがあり、myCloud ドメインにサブスクリプション契約している場合に限りです。

b. 一般設定オプション

ホストのデフォルト設定を変更することができます。これらの設定は、プログラムのユーザーインターフェースからも後から変更可能です。本ドキュメントの後半で、各種設定オプションの詳細について説明します。

c. ゲストアクセス認証方式

認証方法を設定してください。デフォルトの方法は（myCloud が導入されていない場合）「共有パスワード」方式で、ここでパスワードを定義します。複数のユーザーがホストにアクセスする必要がある場合は、「システムセキュリティ管理」オプションまたは「ユーザー名とパスワード」オプションを選択することで、パスワードの共有を回避することをお勧めします。ユーザー資格情報の集中管理や、認証されたユーザーがどのコンピューターで何を行えるかを一元的に制御したい場合は、myCloud デバイスアクセス制御の利用をご検討ください。

d. 二要素認証

エンドポイントの認証保護を強化するため、二要素認証（2FA）を設定できます。これにより、通常の資格情報に加えて追加の認証要素として検証コードが必要となり、アクセスが可能になる前にこのコードの入力が求められます。

e. ゲストアクセス権限

セキュリティロールは、認証済みのゲストユーザーが実行できる操作を定義します。以下の 3 種類の WiseMo 定義ロールが用意されています。後からセキュリティロールを変更したり、まったく新しいセキュリティロールを定義することも可能です。WiseMo で定義されたセキュリティロールを変更した場合、ウィザード画面に警告が表示されます。

f. ゲストユーザーの定義

選択した認証方式でゲストユーザーの定義が必要な場合、ウィザードがその手順を提示します。

g. myCloud の設定

ライセンス方式が永久ライセンスの場合、ウィザードはホストを **myCloud** 接続用に設定するオプションを提示します。後から再度ウィザードを実行することでこの設定を行うことも可能です。

h. 通信プロファイル

ウィザードを使用すると、通信プロファイルの有効化/無効化が可能になります。通常、これらの設定を変更する必要はありません。

i. 設定の完了

「完了」ボタンをクリックすると設定が完了します。ウィザードを使用してライセンスを取得した場合、画面に「ライセンスが正常に適用されました」というメッセージが表示されます。設定ファイル **host.xml** とライセンスファイル **host.lic** が保存/更新されます。これらのファイルの保存場所については第 5 節を参照してください。

ウィザードを途中で終了した場合、プログラムが正常に動作するためのライセンスが無効になり、デフォルト設定の変更が反映されない可能性があります。再度ウィザードを実行するには、ホストコンピューターからウィザードを起動してください。ウィザードボタンを選択してください。

電源オプションで「電源に接続されている場合でもコンピューターをスリープ/休止状態にすることを許可する」と設定されている場合、警告画面が表示されることがあります。このような状況では、ネットワークアクセスが制限されているためリモートコントロールが不可能になる場合があります。

1.4 macOS で必要な権限について

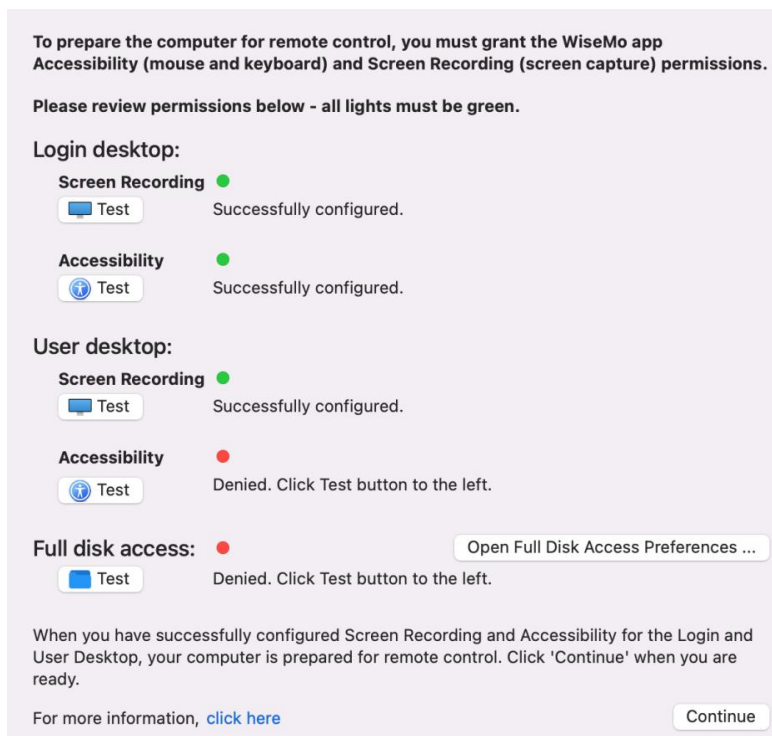
Apple は macOS 10.14 および 10.14 以降のバージョン向けに新しいセキュリティメカニズムを導入しました。

このセキュリティメカニズムでは、リモートコントロールアプリケーション、およびそれに伴う **WiseMo Mac** ホストアプリに対して特別なアクセス許可が必要です。これらの権限を付与することで、ログオン前・ログオン後の両方でコンピューターを監視およびリモート操作できるようになり、**WiseMo** のファイルマネージャー機能をフルに活用できるようになります。

必要な権限にはユーザーデスクトップのリモート操作とログオン画面のリモート操作の両方が含まれます（画面録画権限によりリモートで画面を表示でき、アクセシビリティ権限によりリモートでキーボードとマウスを操作できるようになります）。

また、**WiseMo** ファイル転送機能を使用する際に、通常は制限されているディスク領域にアクセスするためにも権限が必要になる場合があります。

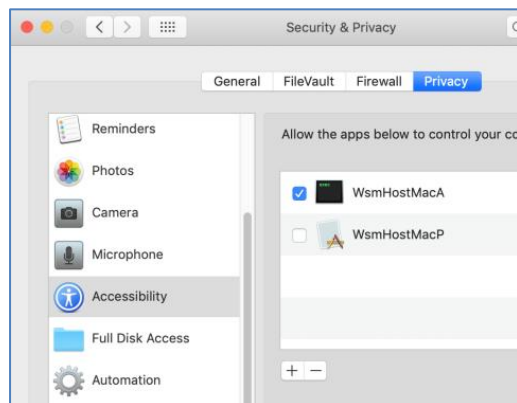
Mac ホストを初めて起動すると、必要な権限についてのプロンプトが表示されます。**WiseMo** によるガイダンスダイアログが表示されますので、指示に従ってください。



各機能が正常に動作するようにするため、アクティブなテストボタンのいずれかをクリックして緑色のチェックマークを取得してください。完全な設定が完了するまで続けてください。

赤いライトが点灯している項目のテストボタンをクリックすると、「許可しない」または「システム環境設定を開く」を選択するよう求められます。必ず「システム環境設定を開く」を選択してください。

この操作により Mac コンピューターのセキュリティ&プライバシー画面が表示されます：



ここで、各適切なアプリケーションについて、チェックボックスまたはスイッチを使用して必要な WiseMo アプリケーションのアクセス許可を有効にすることができます。

アクセス許可が必要な WiseMo アプリケーションは最大 4 つあります：WiseMo ホストマネージャー、WsmHostMacA、WsmHostMacP、および WsmHostMacD です。これらのアプリケーションの詳細については、付録 A を参照してください。

以下のすべてのアプリに許可を与えてください：

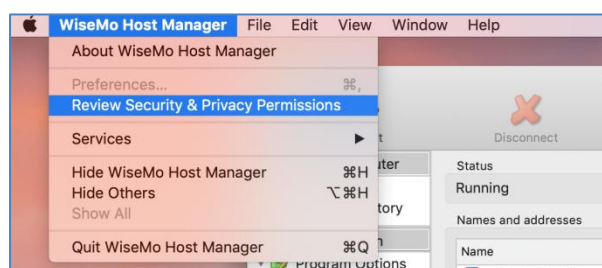
セキュリティとプライバシー >：

- 画面録画機能（リモート画面表示）
- フルディスクアクセス（WiseMo ファイルマネージャーへのアクセス）

各テストボタンをクリックした後に「セキュリティとプライバシー」項目に移動しない場合は、システム環境設定を開き、セキュリティとプライバシーに移動して適切な項目を選択してください。その後、ロックアイコンをクリックして変更を許可しチェックマークを付けたりオンにしたりできます（WiseMo 関連ファイルの表示を有効にします）。

各テストボタンをクリックした後も緑色のランプが表示されない場合は、[こちら](#)をクリックして詳細情報をご確認ください。

セキュリティとプライバシーのアクセス権限を後で確認するには、「WiseMo ホストマネージャー」を開き、ホストメニューから「セキュリティとプライバシーのアクセス権限を確認」を選択してください：



1.5 リモートコントロール準備完了

インストールと設定が完了すると、ホストは稼働状態となり、ゲストユーザーが接続できるようになります。

準備状況を確認するには、ステータスバーなどからホストマネージャープログラムを起動してください。ホストアイコン（クラウドのアイコン）をクリックし、ポップアップメニューから「表示」を選択します。



ホストマネージャーウィンドウの左側ペインにある「プログラム状況」オプションを選択します。右側ペインの「ステータス」セクションに「実行中」と表示されていることを確認してください。

「名前とアドレス」セクションに有効な IP アドレスが表示されていることを確認してください。このセクションにはホスト ID と場合によってはユーザー名も表示されます。これらは重要な識別情報であり、ゲストユーザーがホストにアクセスしたり識別したりする際に使用します。

「初期化済み通信プロファイル」セクションを確認することで、ホストが myCloud ドメインとオンライン接続されているかどうかを確認できます。myCloud 経由での通信設定が行われている場合に限りです。

「端末」欄に myCloud と表示され、詳細欄にはご自身のドメイン名が記載されているプロファイルが確認できるはずです。

Initialized communication profiles		
Profile	Device	Details
 myCloud	myCloud	Wisemo Demo Internal
 TCP/IP (TCP)	TCP/IP (TCP)	1970/1970
 TCP/IP (UDP)	TCP/IP (UDP)	1970/1970

このセクションでは、ホストが UDP または TCP プロトコルで接続可能かどうか、およびそれぞれのポート番号（「送信ポート」/「受信ポート」として表示）も確認できます。

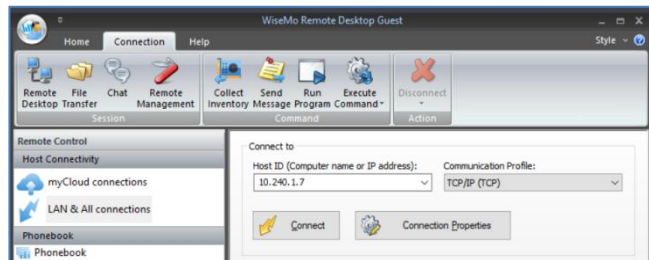
また、「バージョン情報」セクションを確認して、プログラムが正しくライセンス認証されているかを確認することをお勧めします。

2. リモートコントロールの使用例

WiseMo のゲストモジュールを使用することで、Mac コンピューター（WiseMo ホストモジュールがインストールされ動作している状態）を遠隔操作することが可能です。

WiseMo の適切なゲストモジュールを使用することで、さまざまなプラットフォームから Mac を遠隔操作できます。具体的には、別の Mac コンピューターから、Android 端末（スマートフォン/タブレット）、iOS 端末（iPhone/iPad）、そして Windows PC からの操作が可能です。

ブラウザから接続を開始する場合、適切なゲストモジュールのインストールを求められることがあります。インストール済みの状態であれば、接続を開始することができます。最も機能豊富なゲストモジュールは、Windows リモートデスクトップ用ゲストモジュールで、Windows PC にインストールして使用します。



本章では、Windows リモートデスクトップ用ゲストモジュールを使用したリモートコントロールのいくつかの使用例をご紹介します。myCloud（インターネット通信）経由と、お客様が管理されているネットワーク上の TCP/IP を直接利用したリモートコントロール（例えば LAN など）の両方の方法について解説します。iPad や Android 端末からインターネット経由でリモートコントロールを行う例もご紹介します。

これらのゲストタイプの詳細な使用方法については、各モジュールに関連するドキュメントを以下のサイトでご確認いただけます：<https://its.tos.co.jp/support/download/wisemo/>

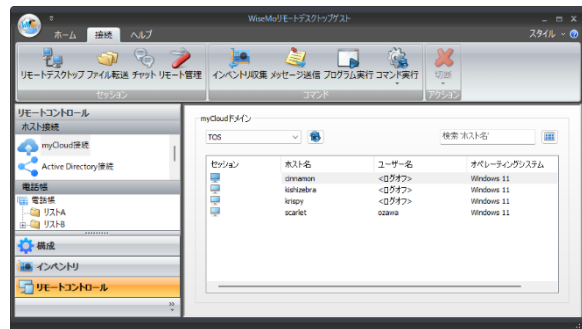
2.1 インターネット経由のリモートコントロール（WiseMo myCloud を使用）

この手順例では、myCloud ドメインを既に設定しており、この myCloud ドメインに接続された少なくとも 1 つの Mac ホストモジュールがデプロイされていることを前提としています。

myCloud は WiseMo が提供するクラウドベースのサービスで、PC、サーバー、Mac、スマートフォン、タブレットなどのコンピューターや端末間のリモートコントロール接続を容易にします。また、事前に設定済みでライセンス認証済みのホストモジュールやゲストモジュールを簡単に展開できるよう、ダウンロードリンクや SMS 展開リンクなどの展開オプションも提供しています。まだ myCloud ドメインをお持ちでない場合は、こちらで無料トライアルにお申し込みください：

<https://its.tos.co.jp/products/wisemo/trial/>

1. PC 上で Windows リモートデスクトップゲストモジュールを起動してください。ゲストモジュールは、myCloud ドメインの「デバイスの管理」>「展開」タブから入手できます。
2. 左側のメニューから「myCloud 接続」を選択し、myCloud ドメインにログオンしてください。これにより、オンライン状態のホストコンピューターの一覧が表示されます。
3. ホストコンピューターをダブルクリックするか、右クリックして「リモートデスクトップ」オプションを選択してください。また、ホストコンピューターを選択した後、ツールバーの「接続」タブにある「リモートデスクトップ」ボタンを使用することもできます。
4. プログラムがリモートコンピューターに接続し、別のリモートデスクトップ制御ウィンドウを開きます。このウィンドウには、リモートホストコンピューターまたは端末のデスクトップが表示されます。ウィンドウを選択して、実際にその前で操作しているかのようにリモートホストコンピューターを遠隔操作できます。
5. リモートコントロールセッションは、ウィンドウを閉じるか、切断ボタンを押すことで終了できます。



2.2 LAN/WAN 環境における TCP/IP を使用したリモートコントロール

自社の TCP/IP ネットワーク上にあるコンピューターや端末を遠隔操作する最も一般的で迅速な方法は、リモートコンピューターの IP アドレスまたは DNS 名を指定し、接続することです。

1. PC 上で Windows リモートデスクトップゲストモジュールを起動します。

2. 左側のメニューから「LAN とすべての接続」を選択してください。

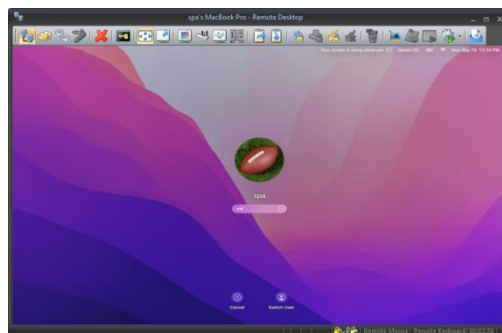
3. ホスト名欄に、リモートコンピューターの IP アドレスまたは DNS 名を入力します。

4. 「接続」ボタンを押します。



(または接続タブにあるリモートデスクトップボタンをクリックします)

5. プログラムがリモートホストコンピューターに接続します。Windows ゲストコンピューター上では、別のリモートデスクトップ制御ウィンドウが開き、リモートホストコンピューターまたは端末のデスクトップが表示されます。ウィンドウを選択して、リモートコンピューターの制御を開始します。マウスとキーボードの入力は、リモートコンピューターまたは端末上で実行されます。



このボタンを押すことで、広々としたウィンドウ内で完全なリモートデスクトップを簡単に表示できます。

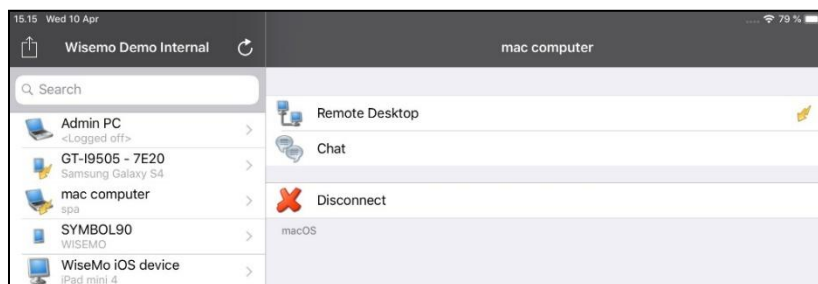
2.3 iOS または Android からのインターネット経由のリモートコントロール

タブレットやスマートフォンを使用することで、どこからでも Mac コンピューターにアクセスできます。Wi-Fi 接続でもモバイルデータ通信でも、WiseMo は高速で安定したリモートコントロール接続を Mac コンピューターに提供します。

この例では、myCloud ドメインを設定済みであり、この myCloud ドメインに接続された少なくとも 1 つの Mac ホストモジュールが導入されていることを前提としています。

1. 端末に iOS ゲストモジュールまたは Android ゲストモジュールをインストールしてください。

2. myCloud ドメインにサインインしてオンライン状態のコンピューターと端末の一覧を表示します。



3. 一覧からホストコンピューターを選択し、「リモートデスクトップ」をクリックすると、端末上に Mac のデスクトップ画面が表示されます。

4. iOS ゲストモジュールまたは Android ゲストモジュールの操作方法については、以下のガイドを参照してください：
<https://its.tos.co.jp/support/download/wisemo/>



3. ホストの機能

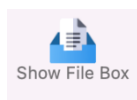
WiseMo ホストモジュールは、Mac コンピューターを準備し、WiseMo ゲストモジュールを実行するユーザーによる遠隔操作を可能にします。ホストモジュールは多くの機能を提供し、お客様の利便性と価値を大幅に向上させます。これは、無人コンピューターのサポートが必要な場合でも、ユーザーが直接コンピューターにアクセスしている場合でも同じです。ホストコンピューターの前にいるかのように遠隔操作を行うことも、ヘルプを必要とするユーザーに対して遠隔サポートや支援を提供することも可能です。また、ファイルやディレクトリを中断することなく双方向に転送する必要がある場合にも便利です。例えば、ファイルやディレクトリを中断することなくユーザーのデスクトップ上で作業しているコンピューターを操作することができます。あるいは、どこからでも接続して単にログアウトやコンピューターのシャットダウンを行うこともできます。

使用するゲストモジュールによるサポートと、適用されているセキュリティ設定によって許可されている場合、ホストはリモートデスクトップ制御（表示と操作）、リモートクリップボード転送、プライバシー保護のためのホスト画面の非表示、バックグラウンドファイル転送、ファイルボックス、ハードウェア/ソフトウェアインベントリ収集、チャットなどの機能を提供します。さらに、複数のゲストが同時に同じホストに接続することも可能です。

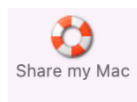


Mac ホストは多くの機能をサポートしており、以下は Windows ゲストユーザーが Mac ホストコンピューターに接続した際に利用できる機能の一例です。

マルチモニター環境のコンピューターのリモート制御にも対応しています。Windows および iOS ゲストモードでは、接続前に「接続プロパティ > ディスプレイ設定」を通じて表示する特定のモニターを指定することが可能です。デフォルトでは、すべてのタイプのゲストはメインモニターを表示します。また、画面の特定領域をリモート制御することも可能です。



ファイルボックス機能を使用すると、ユーザーはファイルをドラッグ&ドロップするだけで、そのファイルが直接相手側のファイルボックスに送信されます。これにより、ゲストユーザーとホストユーザー間でのファイル交換を迅速かつ簡単に行うことができます。



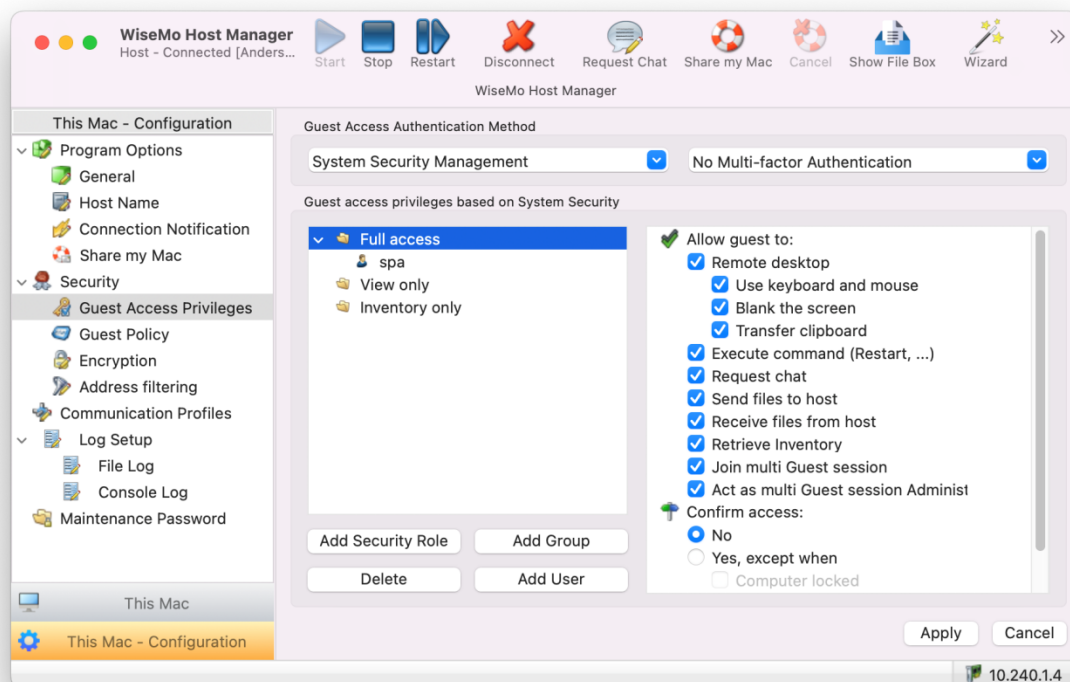
ホストコンピューターで利用できるもう一つの機能として「Mac を共有」機能があります。この機能を有効にすると、簡単な支援の提供やデモンストレーションなどのために、コンピューターへの一時的なアクセスを他者に招待できます。「Mac を共有」機能により、WiseMo ゲストモジュールをインストールした任意のユーザーに渡せるリンクが作成されます。

「Mac ホスト」プログラムは多言語対応しており、利用可能な場合は Mac コンピューターに設定されている言語を自動的に使用します。設定されていない場合は、デフォルトで英語が使用されます。

4. ホストシステムの構成

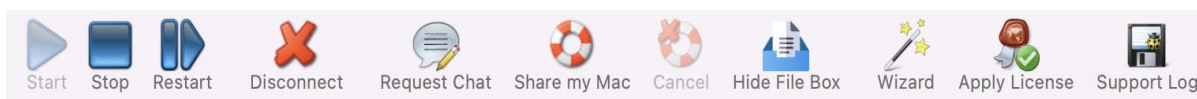
ホストモジュールは、ホストデーモンとユーザーインターフェースを提供する「ホストマネージャー」プログラムで構成されています。ホストデーモンはホストマネージャーが実行されていない状態でも動作可能ですが、チャット機能や「アクセスの確認」画面など、ユーザーインターフェースを必要とする一部の機能は利用できません。

ホストマネージャーのユーザーインターフェースは、上部にボタンを配置したツールバーと、左側のナビゲーションバーで構成されています。ナビゲーションバーでは各メニュー項目の詳細が表示され、右側のパネルに詳細な情報が表示されます。



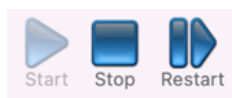
ナビゲーションバーに表示されるメニューは、選択するメニューカテゴリによって異なります。メニューカテゴリはナビゲーションバーの下部で選択します。通常、「この Mac」「この Mac - 設定」の 2 つのカテゴリが利用可能です。

4.1 ツールバーについて



ツールバー上の各ボタンにはツールチップが表示され、カーソルをボタンの上に重ねるだけで説明を確認できます。ツールバーをカスタマイズするには、右クリックしてください。

「再起動」ボタンを使用すると、ホストとの通信をワンクリックで停止・再開できます。特に、リモートで設定変更を行った後に再起動が必要な場合に便利です。



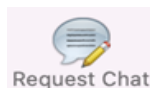
「停止」ボタンを使用すると、ホストの通信機能を一時停止できます。ホストが現在通信を行っていない場合は、「開始」ボタンを使用して通信を再開してください。「開始」ボタンをクリックするとホスト通信が初期化され、ゲストユーザーからの通話を受信できる状態になります。

注意：「この Mac - 構成」>「プログラムオプション」>「一般」のデフォルト設定では、コンピューターの再起動またはログオフ後に自動的に通信が開始されます。これは常にコンピューターがリモートコントロール可能な状態を保つためです。この動作を希望されない場合は、ホスト側のプログラムオプションを変更してください。

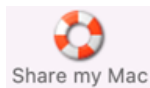


ゲストユーザーとの接続を切断します。

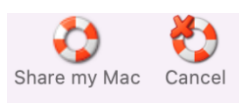
複数のゲストユーザーが同時に接続している場合、すべての接続が切断されます。



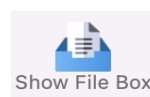
ゲストユーザーに接続されている場合、ホストマネージャーからゲストユーザーとのチャットセッションを開始することが可能です。



「Macを共有」ボタンを使用すると、Macホストユーザーは第三者が一時的にコンピューターにアクセスできるようにするための招待リンクを作成できます。この機能を使用するには、ホストが myCloud ドメインにログオンしており、この機能が有効になっている必要があります。このボタンをクリックすると、「Macを共有」ウィンドウが表示され、ここから招待リンクの有効期間、セキュリティ設定、および実際のリンクの作成が可能です。リンクを作成したら、第三者にメールで送信するなどして共有してください。第三者は、任意のインストール済み WiseMo ゲスト端末（例えば Android、iOS、Mac および Windows）からリンクを実行できます。**ヒント:**ホストの設定メニューから、この機能の有効/無効を切り替えたり、許可する接続数や、リンクが有効期限切れになった後に実行するアクションを設定したりできます。



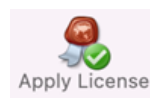
有効な共有リンクは、「キャンセル」ボタンを使用するか、「Macを共有」ボタンを介してキャンセルできます。このボタンをクリックすると「Macを共有」ウィンドウが表示され、これはリンク作成時に使用したものと同一ウィンドウです。この画面では、招待の残り時間も確認できます。



このボタンを押すとファイルボックスが開きます。ファイルボックスは、ゲストユーザーとホストユーザー間でファイルをやり取りする際に使用します。ファイルをボックス内にドラッグ & ドロップすると、そのファイルが送信され、反対側のファイルボックスに表示されます。



ウィザードボタンを押すと構成ウィザードが起動します。例えば、ホストが接続すべき myCloud ドメインを変更する場合などに使用します。また、セキュリティ設定など、さまざまなホストの構成設定を案内します。上記のセクション 1.3 もご参照ください。



「ライセンス適用」ボタンを使用すると、WiseMo ライセンスキーを入力できます - ウィザードを実行する必要はありません。



サポートログは、ゲストとホスト間のより詳細な通信内容を WsmHost Mac.log ファイルに記録します。これはトラブルシューティングに使用されます。問題を報告する必要がある場合、WiseMo サポートチームからこのサポートログの作成を依頼され、当社に送付していただく場合があります。

ホストの詳細情報は、Mac コンピューターの上部ステータスバーに表示される WiseMo ホストアイコンからアクセスできます。



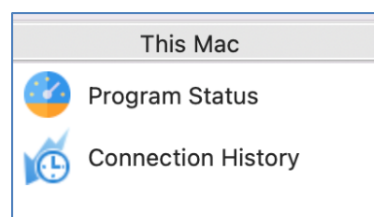
詳細情報ウィンドウでは、バージョン情報、ライセンス情報、著作権表示など、ホストプログラムに関する詳細情報を確認できます。

WiseMo ゲストから Mac コンピューターに接続できない場合、こちらで Mac ホストモジュールが有効にライセンス認証されているか確認できます。試用版のライセンス期限が切れていないか、ご確認ください。

4.2 ホスト情報

ナビゲーションバー（左側パネル下部）では、「この Mac」を選択することで、2つのメニュー項目（プログラム状況と接続履歴）が表示されます。

項目を選択すると、その詳細が右側パネルに表示されます。



4.2.1 プログラム状況

「プログラム状況」を選択すると、右側パネルに表示される情報を確認できます。ホストデーモンの状態は「ステータス」セクションに表示されます。

「名前とアドレス」セクションには、ホスト ID、ユーザー名（該当する場合）、および IP アドレス（複数可）が表示されます。

「初期化済み通信プロファイル」セクションでは、初期化された通信プロファイルが表示されます。「myCloud」プロファイルの場合、「詳細」列にはホストがログオンしているドメイン名が表示されます。

ゲストユーザーからの通話を受信するためには、ホストにライセンスが付与されている必要があります（「バージョン情報」ボックスを確認してください）。また、「実行中」の状態であること、少なくとも 1 つの通信プロファイルが初期化されていること、有効な IP アドレスが設定されていることが必要です。ゲストユーザーは、初期化された通信プロファイルのいずれかを使用してホストに接続します。

「アクティブなゲスト接続」セクションでは、どのゲストユーザーがホストに接続されているか、セッションの種類（小さなアイコンで表示）、ゲストユーザー名、および使用されている暗号化レベルを確認できます。

Status

Connected

Names and addresses

Name	Type
 spa's MacBook Pro	Host ID
 spa	User Name
 10.240.1.4	IP address

Initialized communication profiles

Profile	Device	Details
 TCP/IP (UDP)	TCP/IP (UDP)	1970/1970
 TCP/IP (TCP)	TCP/IP (TCP)	1970/1970

Active guest connections

Sessions	Login Name	Encryption Mode
	SPA	Very High

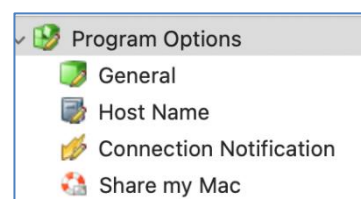
4.2.2 接続履歴

ホスト起動後から現在までに接続／切断されたゲストユーザーの一覧です。より詳細なログ記録が必要な場合は、後述する高度なロギング機能をご利用ください。

4.3 ホスト設定

ナビゲーションバー（左側パネル下部）では、「この Mac - 設定」を選択することで、複数のメニュー項目が表示されます。

メニュー項目を選択すると、詳細設定が右側パネルに表示されます。設定を変更した場合は、必ず「適用」ボタンを押してください。一部の変更内容は、効果を反映させるためにホストの再起動が必要になる場合があります。



4.3.1 プログラムオプション

このセクションでは、ホストプログラムの各種設定オプションを提供しており、以下に説明する 4 つのメニュー項目で構成されています。

全般

Startup
☒ Listen for incoming connections at Host startup
Stop if no activity for 0 s. (0 = do not stop)
User interface
☒ Start user interface as minimized
☒ Show status bar icon
☒ Show icon in Dock
☐ Stealth mode (hide user interface)
Connection
☒ Send Keep Alive messages
☒ Allow multiple Guest connections

起動:

この設定を有効にすると、ホストが起動した際にホストデーモンが通信を初期化します（通常はコンピューターの起動時¹⁾）。有効にしない場合は、ホストマネージャーの「起動」ボタンを手動で押す必要があります。また、ホストを一定時間操作がない場合に自動的に停止させる設定（ゲストユーザーが接続されていない状態）を定義することも可能です。

ユーザーインターフェース:

ホストマネージャーの表示方法（最小化時またはステルスモード時）や、ホストアイコンの表示位置・方法を定義する設定です。

接続:

各種接続設定を制御します。「キープアライブメッセージを送信」

¹ macOS のセキュリティ設定により（ディスクが暗号化されていない必要があります）、WiseMo デーモンが起動し、リモートコントロールが利用可能になる前に、ユーザーが一度ログオンする必要がある場合があります。その後は、ユーザーは問題なくリモートでログオフ・ログオンを繰り返すことができます。

を有効にすると、ゲストモジュールが突然利用不能になった場合にホスト側で検知できるようになります。ホストは複数のゲストから同時にアクセス可能ですが、「複数のゲスト接続を許可する」設定が無効にされている場合は例外です。

ホスト名

ゲストユーザーがホストにアクセスしたり選択したりする際に利用可能な ID をカスタマイズするための設定です。

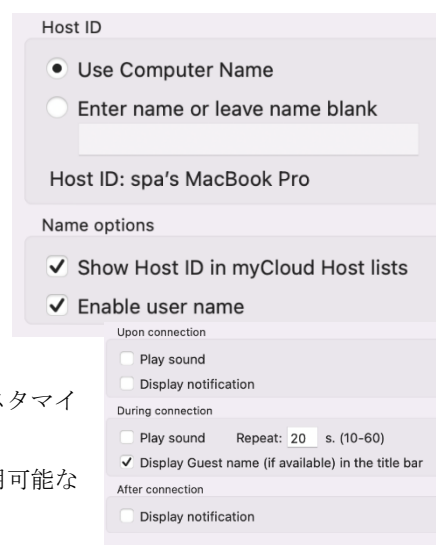
通常は **Mac** コンピューターの名前をホスト ID として使用します。代わりに、ご自身で設定したホスト ID（任意の名前）を指定することも可能です。

また、「名前を入力」フィールドを使用することで、ホストに **CSV** 形式のファイルからホスト ID を読み取らせることができます。ファイルから名前を取得する方法は、以下の構文に従って指定してください。

%CSV:[区切り文字]:[検索キー]:[値列]:[ファイル名]%

「myCloud ホスト一覧にホスト ID を表示」のチェックボックスがオフの場合、ホストは **myCloud** のホスト一覧に表示されません。この一覧は、ホストが同じ **myCloud** ドメインにログオンしているゲストユーザーに表示されます。このチェックボックスをオフにすると、ゲストユーザーは **myCloud** 経由でホストに接続するためにホスト ID を入力する必要があります。

ユーザー名表示を有効にすると、ログオンしている **Mac** ユーザーの名前が **myCloud** のホスト一覧にも表示されるようになります。



The image shows the 'Host ID' settings panel. It has two main sections: 'Host ID' and 'Name options'. In the 'Host ID' section, 'Use Computer Name' is selected with a radio button, and 'Enter name or leave name blank' is unselected. Below this, the 'Host ID' is displayed as 'spa's MacBook Pro'. In the 'Name options' section, 'Show Host ID in myCloud Host lists' and 'Enable user name' are both checked with checkboxes. Below these are two sections for notifications: 'Upon connection' and 'During connection'. 'Upon connection' has 'Play sound' and 'Display notification' both unchecked. 'During connection' has 'Play sound' unchecked, 'Repeat: 20 s. (10-60)' set, and 'Display Guest name (if available) in the title bar' checked. There is also an 'After connection' section with 'Display notification' unchecked.

接続通知

ユーザーが接続時、接続中、および接続後に通知を受ける方法をカスタマイズするための複数のオプションが用意されています。

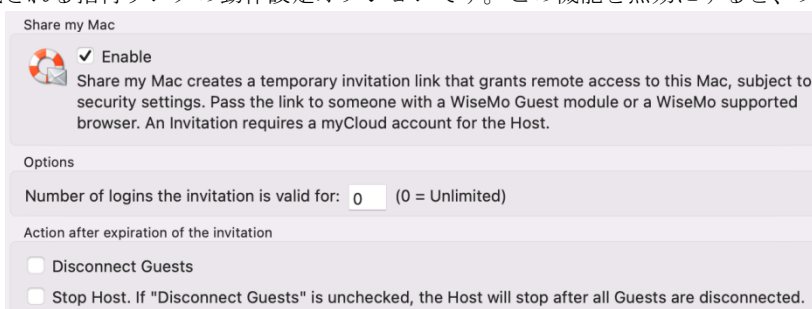
これには音声通知と視覚的表示が含まれます。デフォルトでは、利用可能な場合はゲストユーザー名がタイトルバーに表示されます。

Mac を共有

「Mac を共有」機能によって作成される招待リンクの動作設定オプションです。この機能が無効にすると、ツールバーの「Mac を共有」ボタンも使用できなくなります。

オプションには、リンク経由で許可される接続数や、招待リンクの有効期限が切れた後の処理方法などが含まれます。

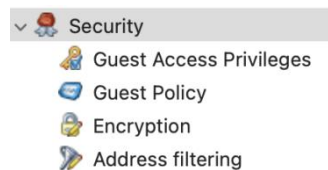
「招待リンクの有効期限切れ後のアクション」を設定することで、ゲストユーザーがリンクの有効期限が切れた際に自動的に切断されるようにすることができます。



The image shows the 'Share my Mac' settings panel. It has a title 'Share my Mac' and a status 'Enable' with a checkmark. Below this is a description: 'Share my Mac creates a temporary invitation link that grants remote access to this Mac, subject to security settings. Pass the link to someone with a WiseMo Guest module or a WiseMo supported browser. An Invitation requires a myCloud account for the Host.' There is an 'Options' section with 'Number of logins the invitation is valid for: 0 (0 = Unlimited)'. Below this is 'Action after expiration of the invitation' with two options: 'Disconnect Guests' (unchecked) and 'Stop Host. If "Disconnect Guests" is unchecked, the Host will stop after all Guests are disconnected.' (checked).

また、リンクの有効期限が切れた際に自動的に「ホストを停止」（新たな接続を受け付けないように）することも可能です。これにより、ホストが再度通信を開始するまで、いかなるゲストからも接続ができなくなります。（注意：この設定は、コンピューターの再起動後などにホストデーモンが自動的に起動した際に、新たな接続を自動的に受け付けるようにする起動時設定を上書きするものではありません。）

4.3.2 セキュリティ



このセクションではホストのセキュリティ設定を管理します。以下の 4 項目で構成されています。

各項目について以下に説明します。

ゲストアクセス権限

認証方法を制御し、認証済みのゲストユーザーが実行できる操作を設定します。エンドポイントへのアクセスをさらに保護するため、二要素認証を適用することが可能です。

権限

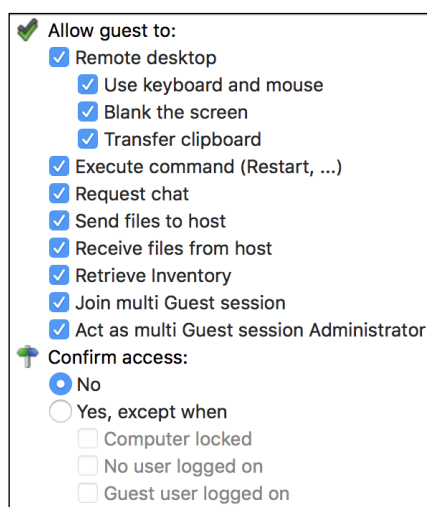
権限は、認証済みのゲストユーザーが実行することが許可されている操作内容を定義します。権限は、ゲストユーザーが割り当てられたセキュリティロールを通じて設定されます。

認証済みのゲストユーザーが実行できる操作には、許可される場合と許可されない場合があります。デフォルトでは、**WiseMo** は以下の 3 つの異なるセキュリティロールを設定しています。独自のセキュリティロールを定義することも、**WiseMo** が定義したロールを変更することも可能です。

例えば、ファイルの送信または受信を許可するかどうかを定義したり、ゲストユーザーの操作を画面表示のみに限定し、キーボードやマウスの制御は許可しないように制限したりできます。図には利用可能な設定オプションが表示されています。

「アクセスの確認」機能を使用すると、通常であれば認証済みのユーザーであっても、ホストコンピューター側で別の人物が明示的にアクセスを許可するまでアクセスを許可しないようにすることができます（この機能は、監視下に置かれたホストコンピューターがある場合にのみ使用してください）。

注意：4 種類ある認証方法のうち、3 種類についてはホスト側で権限が定義されます。認証方法 **myCloud デバイスアクセス制御 (mDAC)** の場合のみ、アクセス可能なユーザーとその権限は中央で一元管理され、ホスト側では定義されません。



認証方法

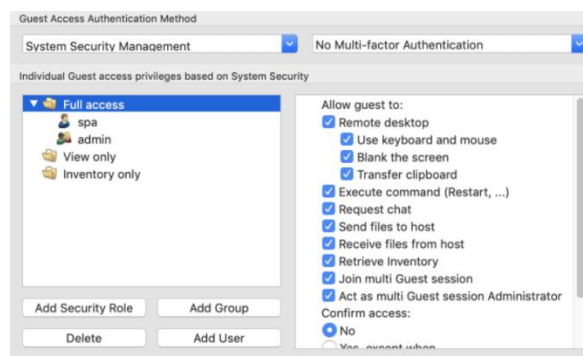
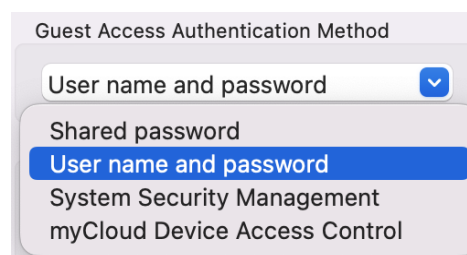
利用可能な認証方法は以下の 4 種類です：

a. 共有パスワード方式：単一のパスワードでアクセスを保護し、デフォルトのセキュリティロールを使用して権限を定義します。

b. ユーザー名とパスワード方式：ゲストユーザーにはそれぞれ個別のユーザー名とパスワードが割り当てられます。各ゲストユーザーには、特定のセキュリティロールが割り当てられ、このユーザーの権限を管理します。

c. システムセキュリティ管理：macOS システムのセキュリティ機能を利用して、ゲストユーザーの認証を行います。ローカルコンピューター用にユーザーとグループを追加できます。各ユーザーまたはグループには、それぞれの権限を規定するセキュリティロールが割り当てられます。

なお、ユーザーはグループメンバーシップを通じて間接的に複数のセキュリティロールに割り当てられる場合があることにご注意ください。最終的に適用される権限は、ユーザーが直接割り当てられたロールと、グループメンバーシップを通じて間接的に割り当てられたす



すべてのロールの権限が合算されたものです。ただし、「アクセス確認」が有効になっていないロールにユーザーが直接または間接的に割り当てられている場合、「アクセス確認」は有効になりません。

d. myCloud デバイスアクセス制御：ゲストユーザーの認証および個別のアクセス権限は、接続が確立される **myCloud** ドメインによって一元管理されます。直接的な **TCP/IP** 接続の場合、認証は指定された **myCloud** ドメインを通じて処理されます。

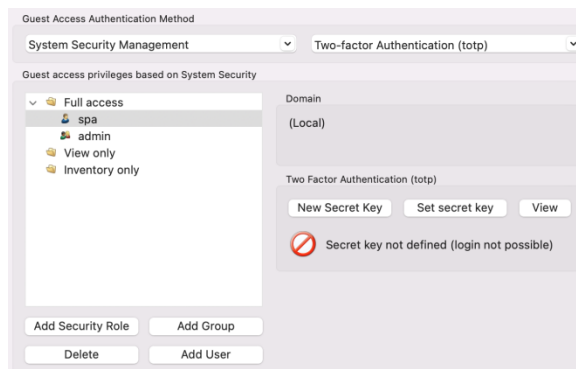
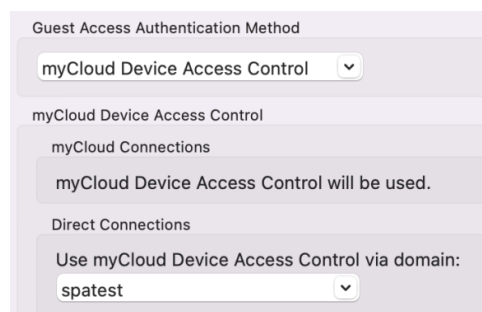
二要素認証 (2FA)

エンドポイントへのアクセスを **2FA** で保護することは、非常に強力なセキュリティ設定です。通常、**ATM** や自宅のパソコンなど、限られた人数のみがアクセスすべき極めて機密性の高いコンピュータへのアクセス保護に使用されます。

2FA によるエンドポイント保護は、共有パスワード方式、ユーザー名/パスワード方式、およびシステムセキュリティ管理の認証方式で利用可能です。「**myCloud** デバイスアクセス制御」認証方式においては、**2FA** による保護が設定され、**myCloud** によって管理されます。

2FA による保護は認証方式レベルで定義されており、アクセスを試みるすべてのゲストユーザーは、常に変化する検証コードを入力する必要があります—このコードが提供できない場合、アクセスは許可されません。通常、この検証コードはスマートフォン（第二要素）で生成されます。例えば **Google Authenticator** や **Microsoft Authenticator** アプリを使用して生成します。

ゲストユーザーを定義した認証方式の場合、ゲストユーザーごとに個別の秘密鍵を設定することが可能です／推奨されます（非常にセキュリティレベルが高い設定です）。**2FA** の設定に関する詳細については、こちらの [ドキュメント](#) をご参照ください（開発元のドキュメントになります）。



ゲストポリシー

このセクションでは、ゲストユーザーが切断した際にどのような処理を行うかを設定します。例えば、自動的にコンピュータのログオフを実行するかどうかなどを指定できます。

また、許可するパスワード試行回数の上限や、上限に達した場合の処理方法もここで設定可能です。

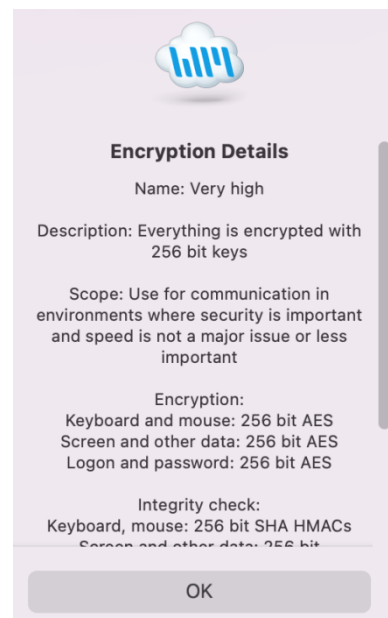
さらに、一定期間操作のないゲスト接続を自動的に切断することも可能です。ホスト側では、ゲストからのデータ受信が指定期間内でない場合、自動的に切断が行われます。

暗号化

ホスト側では、データストリームが改ざんされていないことを保証するため、複数の暗号化レベルとデータ完全性機能を提供しています。設定オプションは「なし」から「非常に高い」までの範囲で選択可能です。

最終的にどの暗号化設定が使用可能かは、ホスト側の設定によって決定されます。ゲストユーザーは自身の好みをリクエストできますが、ホスト側の設定で許可されている場合に限り、その設定が適用されます。許可されていない場合は、ホスト側で許可されている暗号化レベルが使用されます。デフォルトでは、ホストは「非常に高い」と「高い」レベルの暗号化を許可しています。「クラシック」レベルは、一部の特殊なモジュールとの互換性が必要な場合にのみ有効です。

各種の暗号化方式については、該当する項目を選択して「詳細を表示」ボタンを押すことで説明を確認できます。右側の画像は、「非常に高い」設定の説明を表示したものです。



強力な暗号化方式を使用すると、CPU 負荷が増加する可能性があります。特にインターネットなど、ご自身で管理していないネットワークに接続する場合は、必ず何らかの暗号化方式を使用する必要があります。ご自身で管理しているネットワーク上で運用する場合、よりセキュリティレベルの低い暗号化方式を選択することが適切な場合もあります。現在の **WiseMo** ゲストモジュールでは、デフォルトで「非常に高い」レベルの暗号化を使用するよう設定されています。

アドレスフィルタリング

ゲストユーザーが LAN (TCP または UDP) 経由でホストに接続できる IP アドレスを制限することができます。許可するゲスト用 IP アドレスまたは IP アドレス範囲を指定してください。これは、許可されたゲストユーザーが静的 IP アドレスまたは IP アドレス範囲を使用している場合に有効な対策です。リストに記載されていない IP アドレスからのゲストユーザーは、接続プロセスの早い段階でアクセスを拒否されます。この機能を有効にしている場合、**myCloud** 経由で接続するには、コネクションサーバーの IP アドレスを許可する必要があります。これらのアドレスは、ホスト名 **csall.wisemo.net** から確認できます。詳細については、[ファイアウォール設定ガイド](#)を参照し、**WiseMo** コネクションサーバーに関する情報を確認してください。**myCloud** 経由の接続については、ゲスト用 IP アドレスのフィルタリングは行われません。

4.3.3 通信プロファイル



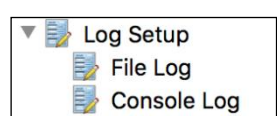
本プログラムは TCP、UDP、HTTP、および **myCloud** 接続による通信をサポートしています。ユーザーインターフェースから、定義済みプロファイルの有効/無効の切り替えや、通信プロファイルの編集・削除・追加が可能です。

TCP/IP プロファイルについては、ホストがデフォルトで使用する送信/受信ポート番号を変更できます。TCP と UDP は 1970 番ポートを、HTTP は 80 番ポートを使用します。

myCloud プロファイルの場合、**myCloud** 接続アカウントを手動で設定できるほか、**myCloud** サービス URL を変更することも可能です。例えば、ホストコンピューターやファイアウォールが HTTPS 通信を許可していない場合などに対応できます。

一般的に、**myCloud** 接続の設定にはウィザードの使用が推奨されます。このウィザードでは **myCloud** ユーザーアカウントの資格情報（メールアドレス+パスワード）を利用するためです。

4.3.4 ログの設定

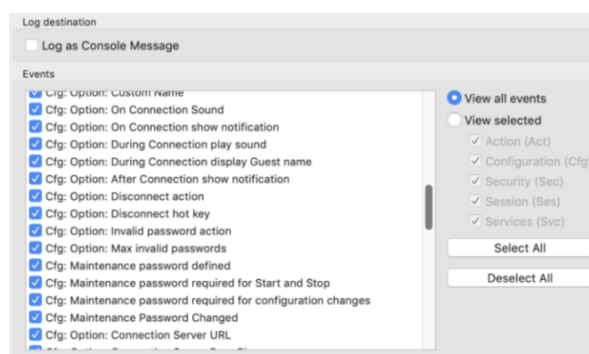


ホストは、ホストに関連するイベントアクティビティの詳細なログ記録機能を提供します。これには、構成設定の変更、特定のアクション、セキュリティ関連イベント、およびセッションイベントが含まれます。

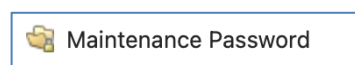
ログ記録はファイルへの出力と、コンソールログへの記録が可能で、ローカル環境または別のコンピューター/サーバーに保存することができます。

ファイルへのログ記録はデフォルトで以下の場所に保存されます：

/etc/WsmHost/wsmhostevent.log

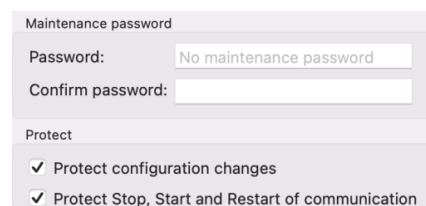


4.3.5 メンテナンス用パスワード



メンテナンス用パスワード機能を不正アクセスから保護するために、許可されていないユーザーが設定変更を行えないように設定することができます。

また、ホストの制御ボタン（開始/停止/再起動）の不正使用を防止する機能も備えています。



5. Mac ホストモジュールの更新または削除

ホストアプリケーションの新しいバージョンまたはサービスリリースは、既存のインストールの上にインストールできます。既存のインストールを更新する場合、デフォルトでは設定ファイル（Host.xml）が保存されます。この設定ファイルは「/etc/WsmHost」フォルダー内に配置されています。

デフォルトの設定で開始したい場合は、インストール前に Host.xml ファイルを削除することができます。

例外：myCloud 展開リンク（例えばメールなどで送信される場合）を使用してインストールする場合、ホストは常にこの特定のドメインに対して有効化されます。さらに、展開リンクにカスタマイズされた設定ファイルが追加されている場合、この設定ファイルが常に使用され、コンピューター上の既存の設定ファイルを上書きします。これにより、myCloud 展開リンクを利用した設定の展開が可能になります。

Mac コンピューターから WiseMo ホストアプリケーションを削除するには、「/Applications/WiseMo RSM」フォルダー内にある WiseMo ホストアンインストールパッケージ（WiseMo Host Uninstall.pkg）を起動してください。

ホストアプリケーションのアンインストールでは、app（アプリ）が特定の一時ファイルや設定ファイルを削除しない場合があります。例えば、「/etc」ディレクトリ内の「Wsmhost」フォルダーにある設定ファイルやライセンスファイルなどが該当します。

アンインストール完了後は、手動で「/etc」ディレクトリ内の「Wsmhost」フォルダーを削除することで、ホストアプリケーションの再インストール前にシステムをクリーンな状態にすることができます。

6. ホストアプリケーションのライセンス情報

バージョン 20 のホストアプリケーションは、複数のライセンス方式に対応しています。

myCloud ライセンス（サブスクリプション）

このライセンス方式は、ホストモジュールを myCloud ドメインへのサインインを通じてライセンス認証したい場合に使用します。これにより、サブスクリプションベースの myCloud ライセンスが消費されます。この方式では、インターネット経由で、あるいは TCP/IP 接続を介して直接ホストにアクセスすることが可能です。また、mDAC を中央アクセスセキュリティとして使用することもできます。myCloud 接続だけでなく、TCP/IP を介した直接接続にも適用可能です。コンピューター／端末は、インターネット経由で myCloud と通信する必要があります。

永続ライセンスキーを myCloud ライセンス習得済みのホストに適用すると、そのライセンス方式は永続ライセンスに自動的に切り替わります（詳細は後述）。

永続ライセンス（一括払い方式）

この方式では、ホストに永続ライセンスキーを適用する必要があります。ゲストユーザーは TCP/IP 接続を介してホストにアクセスできます。TCP/IP 接続のみでホストに直接アクセスする必要がある場合、またはインターネットの利用可能性に依存したくない場合には、永続ライセンス方式を選択してください。

永続ライセンスを取得したホストは、myCloud 接続機能も利用したい場合、myCloud ドメインにサインインすることができます。これにより、コンピューターへのアクセスが可能となるほか、myCloud デバイスアクセス制御機能によってコンピューターへのアクセスを保護することができます。永続ライセンスを取得したホストを myCloud ドメインにサインインさせる場合、myCloud ライセンスを 1 つ消費します。

試用版ライセンス

もしホストに試用版ライセンスキーを設定した場合、ホストは永続ライセンスを取得した場合と同様の動作を行います。使用期間は限定されます（試用版ライセンスキーの発行をご希望の場合は[こちら](#)からお申し込みいただけます）。

myCloud ライセンスを使用したホストの動作テストを行うには、myCloud ライセンス対応のホストインストールファイルを以下のページからダウンロードし、インストールしてください：myCloud トライアルドメインの「デバイスの管理」>「デプロイメント」ページにて。既に試用版ライセンスキーでインストール済みのホストがある場合（試用版ライセンスキーを設定済みの場合）、ホストのユーザーインターフェースまたはホストマネージャーから、ウィザードを実行することで myCloud ライセンスを使用するように設定できます。

インストール前に「/etc/WsmHost」フォルダー内の「host.lic」ファイルを特定して削除した場合、ライセンスの入力が求められます。

7. 用語解説

コンピューター – ゲストモジュールまたはホストモジュールがサポートするオペレーティングシステムを実行している、あらゆる種類のサーバー、ワークステーション、デスクトップ PC、ノート PC を指します。

端末 – スマートフォン、タブレット、セットトップボックス、スキャナー、またはその他の携帯型もしくは非常設の端末で、ゲストモジュールまたはホストモジュールがサポートするオペレーティングシステムを実行しているものを指します。文脈によっては、この用語にはコンピューターも含まれる場合があります。

ゲスト – コンピューターや端末（例：PC、iPad、iPhone、Android 端末、または対応ブラウザから実行される）にインストールされるモジュールです。ゲストモジュールを使用することで、ユーザーはホストモジュールが動作している別の端末やコンピューターを遠隔操作できます。

ホスト – ゲストモジュールから遠隔操作される対象のコンピューターまたは端末にインストールされるモジュールです。具体的には、PC、Mac、スマートフォン、タブレット、セットトップボックス、またはその他の対応オペレーティングシステムを実行する端末が該当します。

ホスト構成マネージャー – ホストマネージャーとも呼ばれます。WiseMo ホストアプリケーションの設定に使用するツールです。このツールはコンピューターにインストールされ、ホストデーモンと通信を行います。

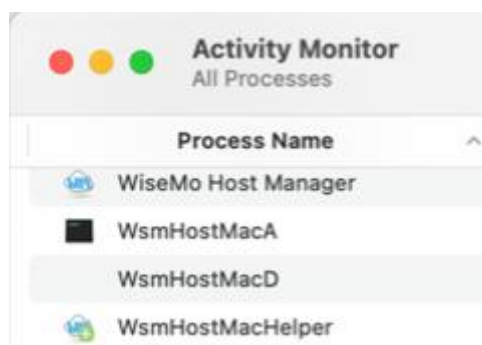
スキン – Windows 環境においてゲストモジュールが端末を遠隔操作する際に使用するグラフィカルユーザーインターフェースです。通常、操作対象の実際の端末とほぼ完全に一致するグラフィック表示となっています。スキン上のボタンは「生きている」状態で、実際のボタンと同じ操作を模倣します。つまり、スキン上のボタンのいずれかをクリックすると、実際の端末上で同じ操作が実行されるのです。

通信プロファイル – ゲストモジュールとホストモジュール間の通信に使用されるプロトコル設定です。主な通信方式としては、TCP/IP 方式と myCloud 方式の 2 種類があります。ゲストモジュールからホストモジュールに接続する前に、使用する通信プロファイルをゲスト側で指定する必要があります。

myCloud – 通信プロファイルの一つです。myCloud 通信はインターネットベースのプロトコルで、ファイアウォールやプロキシ、NAT 設定されたネットワークを介した接続を可能にします。WiseMo の myCloud サブスクリプションサービスの一部として提供されており、コンピューターや端末間のリモートコントロール接続を容易にします。

付録 A

WiseMo の macOS ホストコンポーネントは、それぞれ異なる役割を担う複数のモジュールで構成されています。



主要なモジュールは以下の通りです：

- **WiseMo ホストマネージャー**。ホストのユーザーインターフェースです。ホストのステータス表示、設定、および機能制御を担当します。ログオンユーザーごとに 1 つのインスタンスが起動します。
- **ホストヘルパー (WsmHostMacHelper)**。ユーザーコンテキストで動作する非表示のヘルパーモジュールです。ログオンユーザーごとに 1 つのインスタンスが起動します。
- **ホストデーモン (WsmHostMacD)**。これは通信処理、暗号化、プログラムロジック、認証などを担当する主要なホストモジュールです。
- **ホストユーザーエージェント (WsmHostMacA)**。このユーザーエージェントは、デスクトップ画面のキャプチャなど、ユーザーコンテキストで実行する必要があるタスクを担当します。ログオンユーザーごとに 1 つのインスタンスが起動します。
- **プリログオンエージェント (WsmHostMacP)**。ログオン画面のコンテキストで動作するエージェントです。ログオン画面のコンテキストで実行する必要があるタスク、例えばログオンデスクトップ画面のキャプチャなどを担当します。

ホストマネージャーは通常のアプリケーションと同様に起動/停止できます。その他のモジュールは LaunchDaemon/LaunchAgent としてインストールされており、ターミナルウィンドウから `launchctl` コマンドを使用して管理する必要があります。

デーモンの起動/停止

ターミナルコマンドを起動します。デーモンを起動するには、以下のコマンドを入力してください：

```
sudo launchctl load /Library/LaunchDaemons/com.wisemo.wsmhostmacd.plist
```

デーモンを停止するには、以下のコマンドを入力してください：

```
sudo launchctl unload /Library/LaunchDaemons/com.wisemo.wsmhostmacd.plist
```

どちらのコマンドも管理者パスワードの入力を求められます。

ユーザーエージェントの起動/停止

ターミナルコマンドを起動します。エージェントを起動するには、以下のコマンドを入力してください：

```
launchctl load /Library/LaunchAgents/com.wisemo.wsmhostmaca.plist
```

エージェントを停止するには、以下のコマンドを入力してください：

```
launchctl unload /Library/LaunchAgents/com.wisemo.wsmhostmaca.plist
```

プリログオンエージェントの起動/停止

ターミナルを起動してください。プリログオンエージェントを起動するには、以下のコマンドを入力します：

```
launchctl load /Library/LaunchAgents/com.wisemo.wsmhostmacp.plist
```

プリログオンエージェントを停止するには、以下のコマンドを入力します：

```
launchctl unload /Library/LaunchAgents/com.wisemo.wsmhostmacp.plist
```

注意：このシステムはログオンウィンドウ上でのみこのプロセスを開始します。ユーザーがログオンしている間は実行されないようにしてください。

ホストヘルパーモジュールの起動および停止

ターミナルを起動してください。ホストヘルパーモジュールを起動するには、以下のコマンドを入力します：

```
launchctl load /Library/LaunchAgents/com.wisemo.wsmhostmachelper.plist
```

ホストヘルパーモジュールを停止するには、以下のコマンドを入力します：

```
launchctl unload /Library/LaunchAgents/com.wisemo.wsmhostmachelper.plist
```