

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



WiseMo ホストモジュール

お使いの PC またはサーバーで



Internet

Premises based

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／遠隔操作機器間のリモートコントロールを実現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リモートコントロール機能と管理機能を利用可能です。これにより、時間とコストの両方を節約できます。

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、他のコンピューターや端末にリモートアクセスして制御を行う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リモートアクセスできるように、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の接続は、WiseMo の myCloud 接続機能を介してインターネット経由で確立するか、お客様が管理する LAN/WAN ネットワーク上で TCP/IP 通信を直接使用して行うことができます。

クラウド接続を利用する場合（WiseMo myCloud）、お客様のコンピューターまたは端末はインターネットを利用できる環境である必要があります（固定回線、Wi-Fi、または携帯電話事業者のネットワーク（3G、4G、5G）など）。これにより、ゲストモジュール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介した場合）、インターネットトラフィックを回避できるだけでなく、携帯電話事業者からのデータ料金も発生しません。

Windows 搭載 PC およびサーバー用の WiseMo ホストプログラム

本ガイドでは、Windows ホストプログラム（Windows PC およびサーバー用のホストモジュール）のインストール方法、設定方法、使用方法、およびアンインストール方法について詳しく解説しています。このホストモジュールは、簡単に迅速かつ安全なリモートコントロールを可能にし、WiseMo ゲストモジュールを搭載したコンピューターや端末からの操作を実現します。

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. Windows ホストプログラムのインストール

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、Windows ホストアプリケーションをインストールしてください。

Windows ホストアプリは Windows 11、10、8.x、7、Vista、および XP および Windows Server 2003 以降のバージョンをサポートしています。

インストールファイル（拡張子 .msi のファイル）は、myCloud ドメインから提供される場合（事前ライセンス取得済みかつ事前設定済み）、または別のソースから提供される場合があります。この場合、初期ライセンスと設定（アクセスセキュリティなど）は、インストール時に指定する必要があります。具体的な手順については、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にてライセンス条項に同意した後、デフォルトのインストールディレクトリを変更できるようになります。

Windows 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を表示します。プログラムをインストールするには、**コンピューター上で管理者権限が必要です。**

WiseMo スマートカードドライバと、場合によってはモニタードライバ（一部の OS バージョンで画面を非表示にする機能に必要なドライバ）のインストールを求められることがあります。



1.1 myCloud からのインストールファイル

任意のブラウザで myCloud ドメインにログインし、「デバイスの管理」>「展開」ページ右側の一覧にある「Windows Host」を選択してください。

注意：myCloud 展開リンクを、例えば電子メールなどで対象の PC やサーバーに転送することも可能です。

このような標準の myCloud 展開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 を使用するように設定されます。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/無効にするには、「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。

もしドメインが mDAC に対応していない場合、デプロイされるホストは Windows セキュリティ管理を使用するように設定されます。この場合、すべてのローカルユーザーおよび Windows ドメインユーザーは、各自の Windows ユーザーアカウントを通じて完全なアクセス権限を取得します。

デフォルト設定はデプロイ後、ホストのユーザーインターフェースから直接変更できます。例えば構成ウィザードを実行することで（詳細は後述のセクション 1.3 を参照）設定を変更可能です。さらにカスタマイズした設定ファイルを myCloud にアップロードしてデフォルト設定を変更することも可能です（デプロイ前の設定変更）。

ホストで mDAC を使用するよう設定する場合は、必ず myCloud ドメイン側でも mDAC を有効化してください。有効化していないと、ホストに接続できなくなります。なお、ホストは myCloud ドメインのセキュリティ設定にかかわらず、Windows セキュリティ管理機能（またはその他のアクセス方式）を使用することができます。

myCloud のライセンス管理と設定を行うには、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り、かつ https プロトコルに対応している必要があります。もし古いコンピューターで http プロトコルしかサポートしていない場合は、myCloud ドメインへのサインインのために特別な設定が必要です。詳細はセクション 4.3.3 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

永続ライセンスの購入後、または無料トライアル申し込み後に届くメールに記載されたダウンロードリンクから、ホストをインストールできます。

プログラムは弊社ホームページからもダウンロード可能です：

<https://its.tos.co.jp/product-update-modules/wisemo/>

インストール完了後、構成ウィザードが自動的に起動します。以下のセクション 1.3 を参照してください。ライセンスキーの入力が必要になります。ライセンスキーを購入するか、無料トライアルを申し込んだ際に提供されるトライアルキーを使用することができます。

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設定オプションを順番に案内します。設定完了後は、ホストのホームタブから直接ウィザードを起動することが可能です。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と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未取得の場合、ウィザードでは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登録

myCloud ドメインをご利用の場合、このドメインにログインすることでプログラムのライセンスを取得できます。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。

その後、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、検証コードの入力が求められます。

2. ライセンスキーを介したライセンス登録

ライセンスキー（試用版キーまたは購入済みの永久ライセンスキー）を入力することでプログラムのライセンスを取得できます。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環境がない環境でもプログラムを利用できます。この方式では、myCloud を接続手段として使用することも可能です - インターネットアクセスがあり、myCloud ドメインに登録している場合。

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。詳細は本ドキュメントの後半で説明します。

c. ゲストアクセス認証方式

認証方式を設定してください。デフォルト設定（myCloud が導入されていない場合）は「共有パスワード」方式です。この方式では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、「Windows 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できます。ユーザー資格情報の集中管理や、各ユーザーが特定のコンピューターで実行できる操作を管理したい場合は、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

二要素認証（2FA）を導入することで、エンドポイントの認証セキュリティを強化できます。これにより、通常の資格情報に加えて、アクセス前に追加の検証コード（第二要素）が必要となるため、セキュリティの層がさらに厚くなります。

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範囲を定義します。WiseMo では 4 つの定義済みセキュリティ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が変更された場合、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、ウィザードがその設定を行うオプションを提示します。

g. myCloud 対応の設定

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。これは後から行うことも可能で、例えば再度ウィザードを実行することで設定できます。

h. 通信プロファイル

ウィザードでは通信プロファイルの変更が可能です。これは高度な設定項目であり、通常は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」ボタンを押すと設定が完了します。ウィザード経由でライセンスを取得した場合、「ライセンスは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」は保存／更新されます。これらのファイルの保存場所については、セクション 5 を参照してください。



もしウィザードを途中で終了した場合、プログラムが実行可能な状態にライセンスされていない可能性があり、デフォルト設定の変更も反映されません。ホストから再度ウィザードを実行してください。「ホーム」タブを選択し、「ウィザード」ボタンを押してください。

また、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状態または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、リモートコントロールが不可能になる場合があります（ネットワークアクセスが制限されている場合など）。

1.4 リモートコントロール準備完了

ホストプログラムをインストールして設定が完了すると、ホスト側で待機状態となり、ゲストユーザーが接続できるようになります。

接続状態を確認するには、ホストアイコン（クラウドアイコン）にマウスカーソルを合わせ、ステータスが「実行中」と表示されていることを確認してください。ホストアイコンは **Windows** システムトレイから確認できます。ホストマネージャーを開き、左側のペインにある「プログラム状況」オプションを選択してください。右側のペインの「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ます。また、タイトルバーに「実行中」と表示されていることも確認してください。

「名前とアドレス」セクションに正しい **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 **Windows** ユーザー名も表示されます。これらはゲストユーザーがホストを特定したり識別したりする際に重要な識別情報となります。

「通信プロファイルの初期化」セクションを確認し、ホストが **myCloud** ドメインとオンライン接続されていることを確認してください。**myCloud** 経由での通信設定が完了している場合、**myCloud** というプロファイルがデバイス列に表示され、詳細列にはドメイン名が表示されているはずです。このセクションでは、ホストが直接 **UDP** または **TCP** プロトコルでアクセス可能かどうか（送信ポート/受信ポートとして表示）も確認できます。

通信プロファイルの初期化

プロファイル	デバイス	詳細
TCP/IP (TCP)	TCP/IP (TCP)	1970/1970
myCloud	myCloud	mydomain
TCP/IP (UDP)	TCP/IP (UDP)	1970/1970

「ヘルプ」タブの「バージョン情報」からも、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できます。

2. リモートコントロールの使用例

WiseMo ゲストモジュールを使用して、WiseMo ホストモジュールがインストールされ動作している PC またはサーバーにアクセスし、リモートコントロールすることができます。

適用可能な WiseMo 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 Windows PC やサーバーをリモートコントロールすることが可能です。具体的には、別の Windows PC から、Android 端末（スマートフォン/タブレット）、iOS 端末（iPhone/ iPad）、および Mac コンピューターからリモートコントロールを行うことができます。

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。インストールが完了すると、接続を実行できるようになります。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ゲストで、Windows PC にインストールして使用します。

この章では、Windows リモートデスクトップ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（インターネット接続）経由、およびユーザーが管理するネットワーク上で TCP/IP を直接利用したリモートコントロールの方法です（例えば社内 LAN など）。また、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場合の具体例もご紹介します。

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）

この例では、myCloud ドメインを保有しており、少なくとも 1 つの Windows ホストモジュールを myCloud ドメインに接続して導入していることを前提としています。

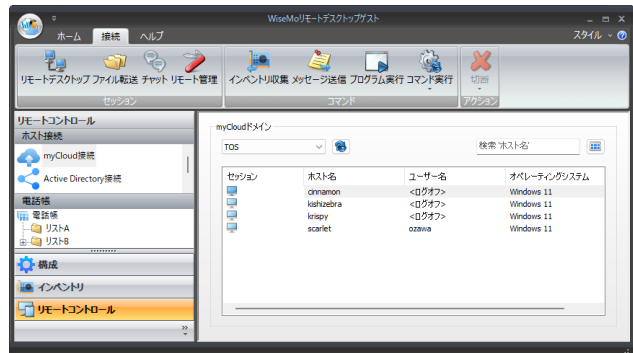
WiseMo が提供する myCloud は、PC、サーバー、Mac、スマートフォン、タブレットなどのコンピューターや端末間で、簡単にリモートコントロール接続を可能にするクラウドベースのサービスです。また、事前に設定済みでライセンス認証済みのホストモジュールやゲストモジュールを簡単に展開できるよう、ダウンロードリンクや SMS 展開リンクなどの導入オプションも提供しています。まだ myCloud ドメインをお持ちでない場合は、こちらから無料トライアルにお申し込みいただけます：

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

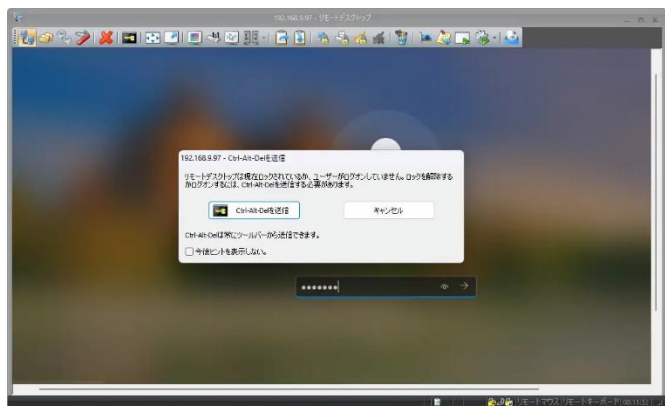
1. お使いの PC で WiseMo ゲストモジュールを起動してください。
2. 左側のメニューから「myCloud 接続」を選択し、myCloud ドメインにログインしてください。オンライン状態のホストコンピューターの一覧が表示されます。
3. ダブルクリックでホストを選択するか、右クリックしてリモートデスクトップオプションを選択します。また、ホストを選択してツールバーの接続タブにあるリモートデスクトップボタンを使用することもできます。
4. ホストに接続し、リモートデスクトップウィンドウを開きます。このウィンドウにはホストのデスクトップが表示されます。



リモート接続先の PC またはサーバー上で Ctrl+Alt+Del キー操作を簡単に実行できるボタンが表示されます。例えば、サインイン画面を表示させる場合などに便利です。



5. リモート操作セッションは、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。

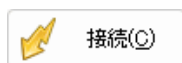


2.2 LAN/WAN 環境でのリモート操作（TCP/IP を使用）

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制御する最も一般的で迅速な方法は、リモート対象のコンピューターの IP アドレスまたはコンピューター名を指定し、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 ID 欄に IP アドレスまたはコンピューター名を入力します。
4. 「接続」ボタンを押します。

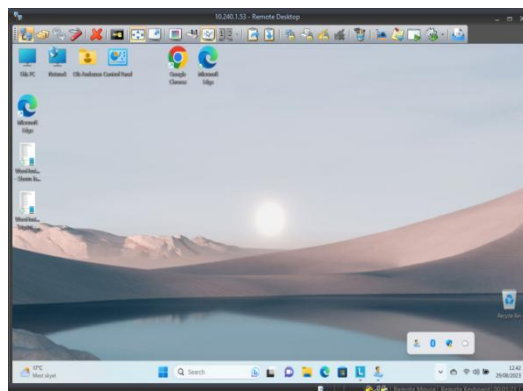


(または接続タブのリモートデスクトップボタンをクリックします)

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、別ウィンドウでリモートホストコンピューターのデスクトップが表示されます。このウィンドウを選択し、リモートホストコンピューターの操作を開始します。マウスとキーボードの操作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。



このボタンをクリックすると、大きなウィンドウ内でリモートデスクトップ全体を簡単に切り替えることができます。

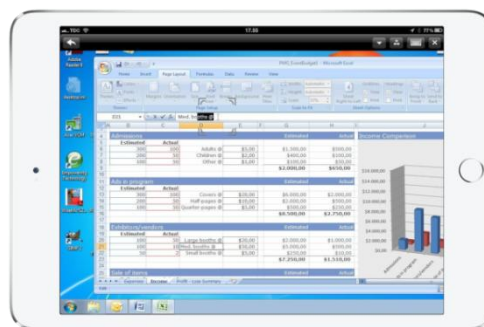
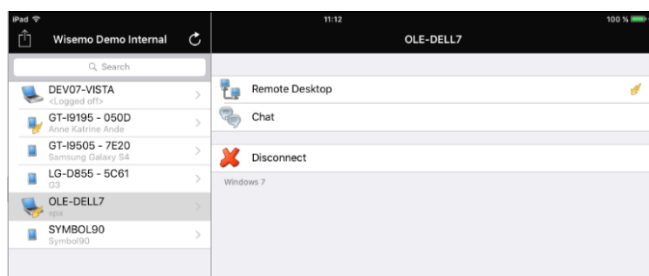


2.3 インターネット経由で iOS または Android からリモート操作

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 PC やサーバ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 Windows PC やサーバーへの高速で安定したリモートコントロール接続を提供します。

この例では、myCloud ドメインを保有しており、少なくとも 1 つの Windows ホストモジュールが myCloud ドメインに接続されていることを前提としています。

1. iOS 用ゲストモジュールまたは Android 用ゲストモジュールをお使いの端末にダウンロードしてください。
2. myCloud ドメインにサインインし、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します。するとお使いの端末に Windows PC のデスクトップが表示されます。ここからリモート操作を開始できます。端末からリモートコントロールを開始してください。



3. ホストの機能

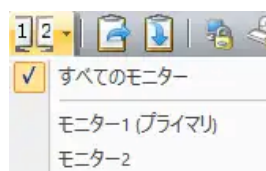
WiseMo ホストモジュールは、Windows PC または Windows Server を、WiseMo ゲストモジュールを実行しているユーザーによるリモート操作が可能になるように設定します。WiseMo ホストモジュールは、ユーザーの利便性と価値を大幅に向上させる多彩な機能と価値を提供します。これは、無人環境をサポートする場合でも、ユーザーが直接コンピューターにアクセスしている場合でも同じです。あたかもコンピューターの前に座っているかのようにリモート操作を行うことも、リモートサポートや支援を必要とするユーザーに提供することも可能です。さらに、サービスやプロセスの終了・開始など、コンピューター上でのシステム管理タスクをリモートで実行することもできます。例えば、ファイルやディレクトリを双方向に転送する必要がある場合や、コンピューターで作業しているユーザーの作業を中断することなくデスクトップ上でこれを行うことができます。あるいは、どこからでも接続してコンピューターのログオフやシャットダウンを行うことも可能です。

使用するゲストモジュールのサポート対象であり、適用されているセキュリティ設定で許可されている場合、ホストは以下の機能を提供します：リモートデスクトップ制御（表示および操作）、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機能、バックグラウンドでのファイル転送、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、チャット機能、プログラムのリモート実行、ゲストからのメッセージ受信など。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。



Windows ホストは多くの機能をサポートしており、ここでは Windows ホストコンピューターに接続した Windows ゲストユーザーが利用可能な各種ボタンの例を示します。

接続済みの状態で利用可能な機能の一つがデスクトップマーカーツールです。ゲストユーザーはホスト側のデスクトップ上でこのツールを起動できます。このツールには以下の機能が含まれています：フリーハンド描画、透過マーカー、矢印、テキスト、楕円、長方形の描画機能、「付箋」機能、およびマウスの動きに合わせて追従する画面拡大機能とスポットライト機能です。デスクトップマーカーは、トラブルシューティング中のユーザーを支援する際や、デスクトップ上に「メモを残す」場合などに、デスクトップ上の特定領域をマークするのに便利です。



もう一つの機能は、マルチモニター環境のコンピューターを遠隔操作できる機能です。ゲスト側から接続前に、表示する特定のモニターを選択することも、すべてのモニターを同時に表示することも可能です。Windows ベースのゲストモジュールでは、接続中でも異なるモニター間を切り替えることができます。デフォルトでは拡張デスクトップが表示されます。また、画面の特定部分だけを遠隔操作することも可能です。

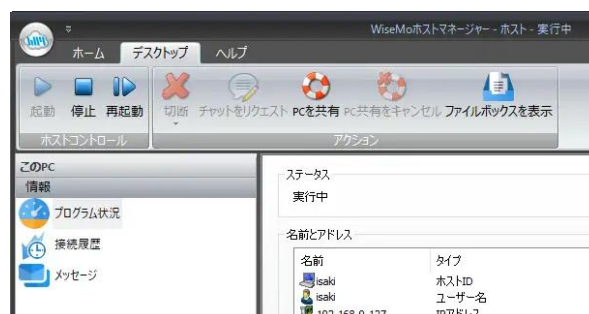


ファイルボックス機能では、ゲストユーザー／ホストユーザーがファイルをファイルボックスにドラッグするだけで、そのファイルが反対側のファイルボックスに送信されます。これは簡単にファイルを素早く交換できる便利な方法です。

ホストモジュールはスマートカードリーダーのリダイレクト機能もサポートしています。この機能により、ゲスト側のスマートカードリーダーを物理的にホストコンピューターに接続されているかのように使用できます。例えば、ホスト側で Windows が認証のためにスマートカードの挿入を要求する場合、通常は物理的に不可能ですが、WiseMo リモートコントロール機能を使えば、ゲスト側のスマートカードリーダーにスマートカードを挿入するだけで済みます。ホスト側でスマートカードリーダーを選択するように求められた場合は、「WiseMo A/S バーチャルスマートカードリーダー」を選択してください。



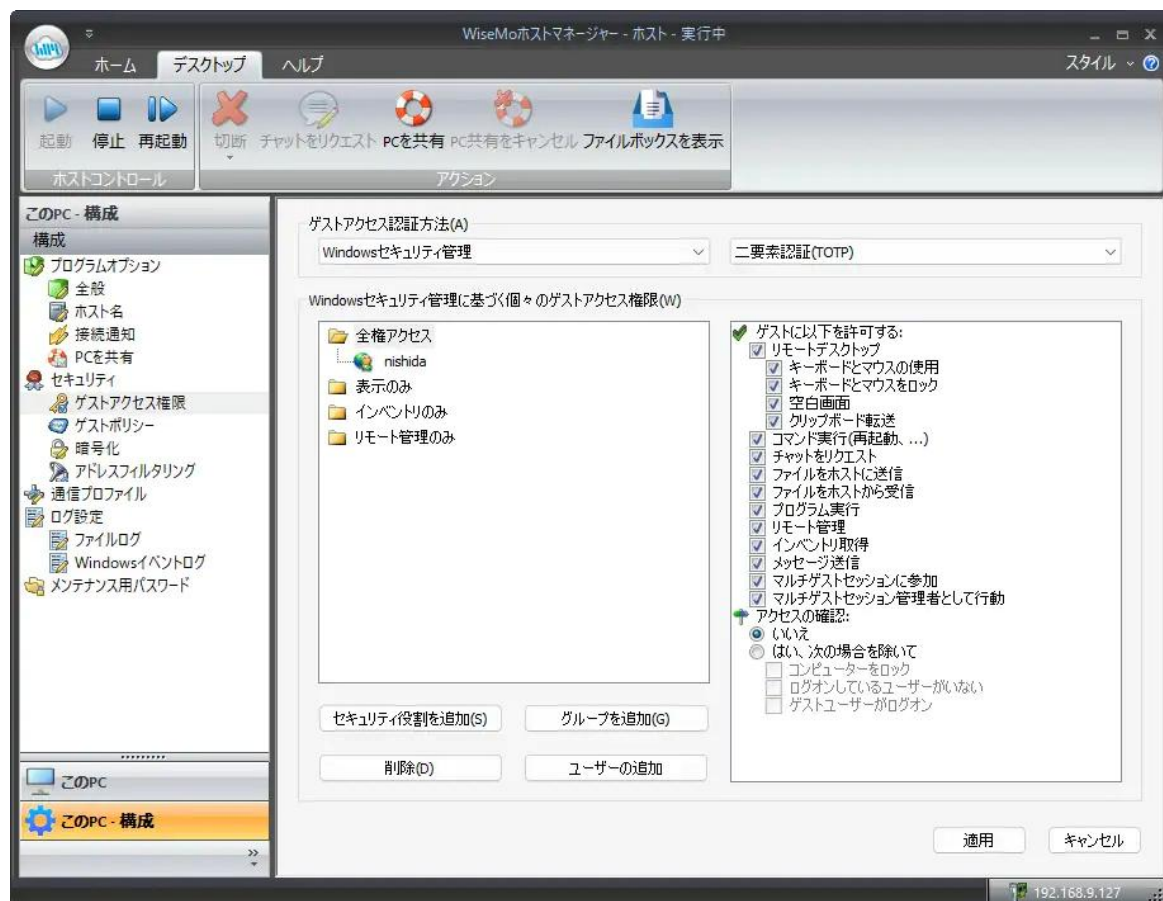
ホストコンピューターを使用するユーザー向けのもう一つの機能として「PC を共有」機能があります。この機能を有効にするとホストコンピューターを一時的に誰かにアクセス許可することができ、例えば迅速なサポートを提供したり、特定の操作をデモンストレーションしたりする場合に便利です。「PC を共有」機能を使用すると、共有リンクを作成でき、このリンクを WiseMo ゲストモジュールをインストールした任意の端末に送信できます。



4. ホストシステム構成

ホストモジュールは、**Windows** サービス（通信処理などを担当）とホストマネージャープログラム（ユーザーインターフェースを提供するプログラム）で構成されています。ホストサービスはホストマネージャーが起動してなくても動作可能ですが、チャット機能や接続を許可画面など、ユーザーインターフェースを必要とする一部の機能は使用できません。システム管理者として、他の **Windows** サービスと同様にホストサービスの有効/無効を設定することができます。

ホストマネージャーのユーザーインターフェースは、上部にリボンツールバーを配置し、左側にナビゲーションバー、右側に各メニュー項目の詳細を表示する構成となっています。



ナビゲーションバーに表示されるメニューは、選択した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 PC」と「この PC - 構成」の2つのカテゴリが利用可能です。

ただし、ホストマネージャーは、**WiseMo** の **Android** ホストまたは **Windows Mobile/CE** ホスト上で動作する端末向けのホスト設定管理ツールとしても機能します。これにより、これらの端末の XML ベースの設定ファイルをより簡単に変更することが可能になります。



システムメニューから既存の **host.xml** ファイルを開くか、完全に新しいデフォルトの設定ファイルを作成することができます。各設定はナビゲーションペインの下部にメニューカテゴリとして表示されます。いずれかを選択して変更してください（例えば、パスワードのみではなくユーザー名/パスワード認証でアクセスを保護するなど）。変更した設定ファイルは保存可能で、「デバイス」カテゴリを閉じることでカテゴリメニューから削除することもできます。

Android 端末や **Windows Mobile/CE** 端末を **USB** ケーブルで **PC** に接続すると、各端末がメニューカテゴリとして表示されます（**PC** が端末上の **host.xml** ファイルを検出して開くことができる場合）。



4.1 リボンツールバー

リボンツールバーは 3 つのタブ（ホーム、デスクトップ、ヘルプ）で構成されています。通常、ホストユーザーインターフェースを操作するには、主に「デスクトップ」タブを使用します。リボンツールバーに表示される各ボタンの説明は、ツールチップで確認できます。説明を確認したい場合は、対象のボタンの上にカーソルを合わせてください。

4.1.1 デスクトップタブ

「デスクトップ」タブでは、制御やタスク実行のための各種ボタンをご利用いただけます：

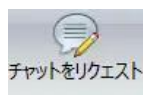


「再起動」ボタンを使用すると、ホストとの通信をワンクリックで停止・開始できます。特に、リモート操作で設定変更を行った後に再起動が必要な場合に便利です。「停止」ボタンを使用するとホストの通信機能を一時停止できます。ホストの通信を開始していない場合は、「開始」ボタンを使用して通信を開始してください。「開始」ボタンはホスト通信を初期化し、ゲストユーザーからの呼び出しを受信できる状態にします。注：「構成」>「プログラムオプション」で設定されているデフォルト値では、コンピューターの再起動後に自動的に通信が開始されます。これは常にリモートコントロールに対応できる状態を維持するためです。この動作を希望されない場合は、「プログラムオプション」の設定を変更してください。



ゲストユーザーとのセッションを切断します。

複数のゲストユーザーが同時にホストコンピューターに接続されている場合、すべての接続が切断されます。ドロップダウン矢印を使用して、特定のゲストユーザーとのセッションのみを終了することができます。



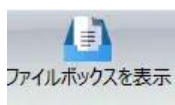
ゲストユーザーに接続している場合、ホストマネージャーからゲストユーザーとのチャットセッションを開始することが可能です。



「PC を共有」ボタンを使用すると、Windows ホストユーザーは第三者に一時的にコンピューターへのアクセスを許可するための招待リンクを作成することが可能になります。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いる必要があり、かつこの機能が有効化されている必要があります。このボタンをクリックすると、「PC 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になります。リンクを作成したら、それを第三者に送信してください（例えばメールで送信します）。第三者は、インストール済みの任意の WiseMo ゲスト（Android、iOS、Mac、Windows など）からこの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、許可する接続数を設定したり、リンクの有効期限が切れた後に実行するアクションを構成したりすることができます。



有効なリンクは、「PC 共有をキャンセル」ボタンを使用するか、「共有招待を表示」ボタンから「PC を共有」ウィンドウを表示することでキャンセルできます。この画面では、リンク作成時に使用した「PC を共有」ウィンドウが表示され、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にドラッグすると、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。

4.1.2 ホームタブ

「ホーム」タブでは、プログラム全体の設定オプションを管理できます。

インポート、開く、保存

ホストの設定は XML ファイルに保存されています。現在有効になっている設定を置き換えるために新しい設定をインポートしたり、設定を開いたり変更を加えたりすることができます。また、設定をバックアップとして保存したり、カスタマイズした設定ファイルをホスト展開リンクに添付したい場合（myCloud ドメイン内のホスト展開リンクに添付したい場合）myCloud に添付することも可能です。Windows ホスト用の host.xml ファイルは、以下のフォルダに配置されています：

`%ProgramData%\WiseMo\WiseMo RSM\Remote Desktop Host`



ウィザード

ホスト環境をある **myCloud** ドメインから別のドメインへ変更する場合、構成ウィザードをご利用ください。セキュリティ設定など、さまざまなホスト構成オプションについてもガイドします。上記のセクション **1.3** もご参照ください。プログラムがライセンス未取得の場合も、このウィザードを通じてライセンス手続きを行うことができます。

言語

使用可能な言語から選択してください。「自動」を選択すると、**PC** に設定されている言語が使用されます（設定可能な場合）。設定が利用できない場合は、デフォルトで英語が使用されます。

4.1.3 ヘルプタブ

ヘルプタブには、オンラインサポートやその他のリソースにアクセスするためのボタンが用意されています。また、ホストプログラム自体を操作するためのボタンも配置されています。



サポート

このボタンをクリックすると、**WiseMo** のサポートページにアクセスできます。このページでは、不具合の報告や観察事項の提出が可能です。

ナレッジベース

接続することで、**WiseMo** が提供する製品モジュールの使用方法に関するよくある質問集を閲覧できます。

登録

接続することで、**WiseMo** のオンライン登録システムを利用し、当社製品のユーザーとして登録できます。

ライセンスを適用

以下の操作が可能になります：使用するライセンスを **myCloud** または **WiseMo** ライセンスキー経由で指定できます。

サポートログ

WsmHostWin.log ファイルを低レベルの通信内容とともに保存します - ゲスト環境とホスト環境間の通信記録で、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と送付を求められることがあります。

バージョン情報

バージョン情報画面では、プログラムに関する詳細情報を確認できます。バージョン番号、ライセンス情報、著作権表示などが含まれます。

WiseMo ゲスト環境から **Windows** コンピューターに接続できない場合、ここで **Windows** ホストモジュールのライセンスが有効かどうかを確認できます。トライアルライセンスの有効期限が切れている可能性があります。



4.2 ホスト情報

ナビゲーションバー（左側のパネル下部）から、「この PC」を選択できます。これにより 3 つのメニュー項目で構成される詳細情報が表示されます。

項目を選択すると、その詳細情報が右側の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」を選択し、右側のパネルに表示される情報を確認してください。ホストサービスの状態は「ステータス」セクションに表示されます。

「名前とアドレス」セクションでは、ホスト ID、ユーザー名（設定されている場合）、および IP アドレスが表示されます。「通信プロファイルの初期化」セクションでは、初期化されている通信プロファイルの一覧が表示されます。

「**myCloud**」プロファイルの場合、「詳細」列にはホストがログイ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接続を受け付ける準備を整えるには、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）。「実行中」の状態であり、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必要があります。ゲストユーザーは、初期化済みの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が表示されます。

4.2.2 接続履歴

ホスト起動以降に接続／切断されたゲストユーザーの一覧と、日付／時刻スタンプが表示されます。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。

4.2.3 メッセージ

「メッセージ」を選択すると、ゲストユーザーから受信したメッセージの一覧が表示されます。

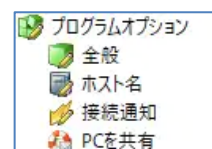
4.3 ホスト構成

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

項目を選択すると、詳細内容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。一部の変更内容を有効にするには、ホストを再起動する必要があります。

4.3.1 プログラムオプション

このセクションには、ホストプログラムの設定オプションが含まれており、以下の 4 つの項目で構成されています。



全般

起動

☒ ホスト起動時に着信接続を待機
活動がなければ停止 秒(0 = 停止しない)

ユーザーインターフェース

☒ ユーザーインターフェースを最小化した状態で起動
☒ トレイアイコンを表示
☒ 最小化時にユーザーインターフェースを隠す
☐ ステルスモード(ユーザーインターフェース非表示)

接続

☒ キーブライブメッセージを送信
☒ 複数同時のゲストセッションを許可

起動: この項目にチェックを入れると、ホストサービスがロードされた際に自動的に通信が初期化されます。チェックを入れない場合、ホストマネージャーで手動で「起動」ボタンを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（ゲストユーザーが接続されていない場合）に自動的に停止するように設定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有無、および表示する場合の表示方法や位置を設定する項目です。

接続: 各種接続関連の設定を制御します。「キーブライブメッセージを送信」機能により、ホスト側はゲストモジュールが突然利用不能になった場合にそれを検知できます。ホストは複数のゲストから同時にアクセス可能ですが、「複数同時のゲストセッションを許可」設定が無効になっている場合は

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項目です。

ホストID

☒ Windowsコンピューター名を使用
☐ 名前、環境変数を入力するか、名前を空白のままにする

ホストID: ISAKI

名前のオプション

☒ myCloudのホストリストにホストデバイスを表示する
☒ Windowsユーザー名を有効

通常は **Windows** コンピューターのコンピューター名をホスト ID として使用します。

別の方法として、独自のホスト ID を入力することも可能ですし、環境変数を使用することもできます。

また、名前入力欄を通じてホストにファイルからホスト ID を読み取らせることも可能です。以下の構文に従って、ファイルから名前を取得する方法を指定してください。

%CSV:[区切り文字]:[検索キー]:[値列]:[ファイル名]%

「Windows ユーザー名を有効」をチェックすると、ログイン中の Windows ユーザー名が、myCloud のホスト一覧に表示されます。ただし、ホストが myCloud ドメインに接続されている場合に限りです。

「ホスト ID を表示」を myCloud ホスト一覧に表示しないように設定した場合、ホストは myCloud ドメインにログインしているゲストユーザーには表示されません。この一覧は、myCloud ドメインに接続しているホストにも表示されます（ホストも myCloud ドメインにログインしている場合）。このチェックを外した場合、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。myCloud との連携に関するヒント：ホストはホスト ID を Windows フォルダ内の WiseMo.ini ファイルに記録します。

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、ホストアイコンがアニメーション表示されます（ゲストが接続中であることを示すために点滅します）。

PC を共有

「PC を共有」機能で作成した招待リンクの動作設定オプションです。この機能を無効化すると「PC を共有」ボタンが使用不可になります。

設定項目には、リンクから許可する接続数や、アクセスを容易にするためタスクトレイに共有アイコンを追加するかどうかなどが含まれます。招待リンクの有効期限切れ後のアクション設定では、リンクが失効するとゲストユーザーが自動的に切断されるように設定できます。

また、リンクの有効期限切れと同時にホストを自動的に停止する（つまり新たな接続を受け付けられない）ように設定することも可能です。これにより、ホストの通信が再開されるまで、いかなるゲストユーザーからも接続ができなくなります。（注意：この設定は、ホストサービスが再起動された場合などに自動的に接続を受け付ける「起動」設定を上書きするものではありません。例えばコンピューターの再起動後など。）

PCを共有

☒ 有効

PCの共有は、セキュリティ設定に従って、このPCへのリモートアクセスを許可する一時的な招待リンクを作成します。このリンクをWiseMoゲストアプリまたはWiseMoサポートブラウザを使用しているユーザーに渡します。招待には、ホスト用のmyCloudアカウントが必要です。

オプション

招待が有効なログイン数:
0 (0 = 無制限)

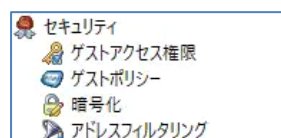
☐ トレイに共有アイコンを追加

招待の有効期限後のアクション

☐ ゲストを切断

☐ ホストを停止します。[ゲストを切断]がチェックされていない場合、すべてのゲストが切断された後にホストが停止します。

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。4つの項目で構成されており、それぞれの設定内容は以下の通りです。

ゲストアクセス権限

認証方法と、認証済みゲストユーザーが実行できる操作を制御します。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も可能です。

権限

権限は、認証済みゲストユーザーが実行できる操作を定義します。これらの権限は、ゲストユーザーに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。ゲストユーザーは、直接または間接的に複数のセキュリティロールに割り当てることが可能です。

認証済みゲストユーザーが実行できる操作には、様々な種類があります。デフォルトでは、WiseMo が 4 種類のセキュリティロールを初期設定しています。独自のセキュリティロールを定義するか、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・受信を許可するか否か、あるいは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、といった設定が可能です。図には利用可能な設定オプションが表示されています。

ゲストに以下を許可する:

- ☒ リモートデスクトップ
- ☒ キーボードとマウスの使用
- ☒ キーボードとマウスをロック
- ☒ 空白画面
- ☒ クリップボード転送
- ☒ コマンド実行(再起動、...)
- ☒ チャットをリクエスト
- ☒ ファイルをホストに送信
- ☒ ファイルをホストから受信
- ☒ プログラム実行
- ☒ リモート管理
- ☒ イベントリクエスト
- ☒ メッセージ送信
- ☒ マルチゲストセッションに参加
- ☒ マルチゲストセッション管理者として行動

アクセスの確認:

- ☒ いいえ
- ☒ はい、次の場合を除いて
 - ☐ コンピューターをロック
 - ☐ ログインしているユーザーがいない
 - ☐ ゲストユーザーがログイン

「アクセスの確認」機能を使用することで、通常の認証を通過したユーザーであっても、ホストコンピューター側でさらに許可を与えた人物が確認するまでアクセスを許可しないようにできます（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）。

ご注意ください：4つの認証方法のうち3つの方法については、ホスト側で権限が定義されています。認証方法 **myCloud デバイスアクセス制御（mDAC）** の場合、アクセス可能なユーザーとその権限はホスト側ではなく中央で一元管理されます。

認証方法

利用可能な認証方法は以下の4種類です：

- 共有パスワード**：アクセスは単一のパスワードで保護され、デフォルトのセキュリティロールが権限定義に使用されます。
- ユーザー名とパスワード**：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。各ゲストユーザーは特定のセキュリティロールに紐付けられ、そのユーザーの権限を管理します。
- Windows セキュリティ管理**：Windows のセキュリティ機能（ローカル環境および Active Directory）を利用し、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の Windows ユーザーおよびグループ、および Windows ドメイン用のユーザー／グループを追加できます。各ゲストユーザーまたはグループは特定のセキュリティロールに紐付けられ、権限を管理します。

注意：ゲストユーザーは、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ります（例：すべての Windows ユーザーは「ユーザー」グループのメンバーです）。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、Windows グループのメンバーシップを通じて間接的に追加されたすべてのロールの権限が合算されたものです。ただし、「アクセスの確認」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、「アクセスの確認」は有効になりません。

- 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、接続を確立する 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、認証処理は指定された myCloud ドメインを通じて行われます。

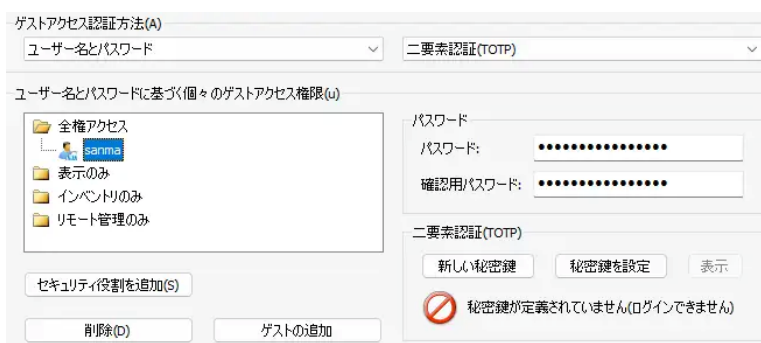
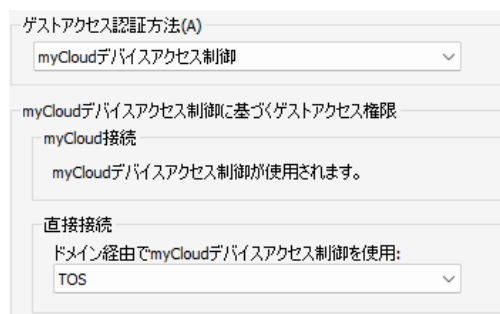
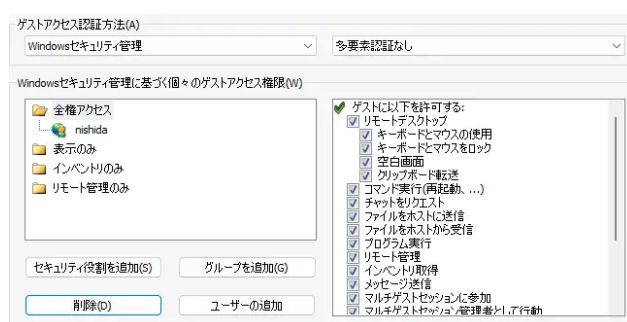
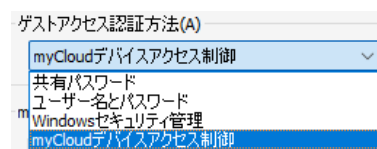
二要素認証（2FA）

2FA によるエンドポイントへのアクセス保護は、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システムの保護に使用されます。

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 Windows セキュリティ管理方式の認証方法に対して利用可能です。特に myCloud デバイスアクセス制御方式においては、2FA による保護が myCloud によって設定・管理されます。

2FA 保護は認証方式レベルで定義され、設定されている場合、アクセスを試みるゲストユーザーは、常に変化する認証コードの入力またはアクセス手段の提供が必須となります。この認証コードは通常、スマートデバイス上で生成されます（第二要素として）。例えば、Google Authenticator や Microsoft Authenticator アプリを使用してスマートフォン上で生成します。

ゲストユーザーを定義した認証モードにおいては、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。この設定により、さらにセキュリティレベルが高くなります。二要素認証の設定手順については、[こちらのドキュメント](#)をご参照ください。（英語のド



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された後に実行すべき動作を制御します。例えば、**Windows** の自動ログオフを自動的に実行するなどの設定が可能です。また、ゲストユーザーを切断するためのホットキーの定義や、許可するパスワード試行回数の上限設定、上限に達した場合の対応方法などもここで制御できます。

暗号化

ホストシステムでは、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」まで用意されていますが、デフォルトで有効になっているのは「高い」と「非常に高い」の 2 段階のみです。

最終的にどの暗号化設定を適用するかは、ホスト側の設定によって決定されます。ゲストユーザーが特定の設定を要求した場合、ホスト側の設定で許可されていれば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自動的に使用されます。なお、クラシックレベルは、古い特殊モジュールとの互換性確保の場合にのみ適用されます。最新のモジュールとは互換性がありません。



各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」ボタンをクリックすることで説明を確認できます。左側の図は、「非常に高い」設定の場合の説明例です。

強力な暗号化を使用する場合、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外部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選択してください。自社管理ネットワーク上で運用する場合、セキュリティレベルをやや下げた暗号化方式を選択することも検討に値します。**WiseMo** ゲストモジュール (v.17 以降) 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。これは範囲指定の形式で設定することも可能です。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、この対策は特に有効です。リストに登録されていない 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。この機能は慎重に **myCloud** 接続環境と併用する必要があります。すべての **myCloud** 接続サーバー (ルーティングポイント) を追加登録しなければならないためです。

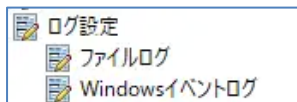
4.3.3 通信プロファイル

本プログラムが使用する通信プロファイルを詳細に設定できます。このプログラムは TCP/UDP、HTTP 通信、および **myCloud** 接続による通信をサポートしています。

TCP/IP プロファイルの場合 (TCP、UDP、HTTP)、ホストが使用する送信/受信ポート番号をデフォルト値 (例: 1970/1970) から変更することが可能です。

myCloud プロファイルについては、接続アカウントを手動で定義できます。例えば、ホストコンピューターやファイアウォールが HTTPS 呼び出しを許可していない場合などに有効です。一般的に、**myCloud** 接続の設定にはウィザードを使用することをお勧めします。この方法では **myCloud** のユーザーアカウント資格情報 (メールアドレスとパスワード) を利用するためです。

4.3.4 ログ設定

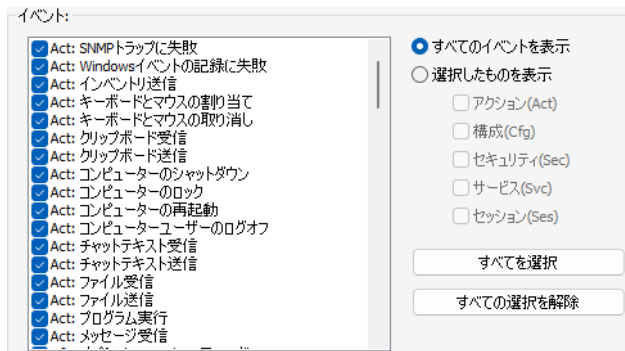


ログ記録はファイルへの出力と Windows イベントログへの記録が可能で、ローカル環境または別のコンピューター/サーバーへの記録を選択できます。

ホストシステムでは、ホストに関連するイベント活動の詳細なログ記録機能を備えています。これには、設定変更、特定の操作、セキュリティ関連イベント、およびセッションイベントなどが含まれます。

4.3.5 メンテナンス用パスワード

設定変更やホストの制御ボタン（起動/停止/再起動）の不正使用を防止するため、メンテナンス用のパスワードを設定することができます。



5. Windows 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、既存のバージョンの上にインストールすることが可能です。

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情報が保持されます。これらの設定は通常、以下の場所に保存されている **Host.xml** ファイルに格納されています：

C:\ProgramData\WiseMo\WiseMo RSM\Remote Desktop Host

Windows XP 環境では、**WiseMo** フォルダは通常以下の場所に配置されています（フォルダが非表示になっている場合があります）：

C:\Documents and Settings\All Users\Application Data\

インストール前に **Host.xml** ファイルを削除することも可能です。デフォルトの設定で開始したい場合にご利用ください。

例外： **myCloud** 展開リンク経由でインストールする場合（例えばメールなどで配布される場合）、ホストは常にこの特定のドメイン用に有効化されます。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、そ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は上書きされます。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。

ライセンスファイル **Host.lic** は、**WiseMo** フォルダ内の **Program Files / Program Files (x86)** ディレクトリに保存されています。このファイルを削除すると、プログラムが起動できなくなり、ライセンス情報の入力を求められる場合があります。

Windows PC またはサーバーから **WiseMo** ホストアプリケーションを削除する手順は、他の Windows プログラムを削除する場合と同様です。具体的には、コントロールパネルの「プログラムと機能」オプションから実行できます（具体的な用語は **Windows** のバージョンによって異なります）。

ホストプログラムをアンインストールしても、特定の一時ファイル、ライセンスファイル、および設定ファイルは削除されません。

ホストマネージャーはモバイルホストモジュールと共有されています。そのため、ホストをアンインストールしても、コンピューターにモバイルホストのインストールファイルが残っている場合、ホストマネージャー部分が削除されない可能性があります。ホストマネージャーは、最後にホストマネージャーを使用しているモジュールがアンインストールされた時点で完全に削除されます。

6. ホストプログラムのライセンス情報

ホストプログラム（バージョン 20）は、さまざまな方法でライセンス認証が可能です。

myCloud ライセンス（サブスクリプション方式）

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経由でライセンス認証したい場合に使用します。この場合、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または TCP/IP 接続経由で直接ホストにアクセスできます。また、mDAC を使用して myCloud 接続の集中アクセスセキュリティを設定することもでき、myCloud 接続だけでなく直接的な TCP/IP 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 ライセンス済みのホストに適用すると、そのライセンス方式は myCloud 永続ライセンス方式に移行されます（詳細は以下を参照）。

永続ライセンス（一括払い方式）

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。この場合、ゲストユーザーは TCP/IP 接続を使用してホストにアクセスできます。インターネットの利用可能性に依存せず、直接 TCP/IP 経由でホストにアクセスする必要がある場合のみ、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 接続機能の利用や、コンピューターへのアクセス保護、myCloud デバイスアクセス制御によるアクセス管理を行うために、myCloud ドメインにサインインすることも可能です。永続ライセンスを取得したホストを myCloud ドメインに登録することで、myCloud ライセンスが消費されます。

クローズドユーザーグループオプション（大規模導入向け）は、ホストへのアクセスをさらに保護するための機能です。クローズドユーザーグループライセンスキーを使用するとゲストユーザーのアクセスを制限でき、該当するライセンスキーでライセンス認証されていない限り、ゲストユーザーはアクセスできません。ただし、対応するクローズドユーザーグループライセンスキーでライセンス認証されている場合は例外です。

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提供した場合、ホストは永続的にライセンスされているかのように動作しますが、その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](#) からお申し込みください）。

myCloud ライセンスを使用してホストをテストするには、myCloud トライアルドメイン内の「デバイスの管理」>「展開」ページからホストのインストールファイルをダウンロードし、インストールしてください。既にホストがインストールされている場合は、「ヘルプ」タブ > 「ライセンスを適用」から設定を行うことで myCloud ライセンスを使用できるようになります。インストール前に host.lic ファイルを見つけて削除した場合、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する、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、スキャナーなど、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する、あらゆる手持ち型または非常時接続型端末を指します。文脈によっては、「端末」という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）にインストールされるモジュールで、iPad、iPhone、Android 端末、または対応ブラウザから動作します。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することが可能になります。

ホスト – 遠隔操作の対象となるコンピューターや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など、対応オペレーティングシステムを搭載したあらゆる種類の端末が該当します。

ホスト構成マネージャー – ホストマネージャーまたはモバイル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を行うためのツールです。Windows デスクトップコンピューターにインストールされ、端末が USB 接続されている場合にはホストサービスや端末と通信を行います。

スキン – グラフィカルユーザーインターフェース ゲストモジュールが Windows 環境で使用 するリモート制御用インターフェースです。通常、 リモート制御対象の実機とほぼ同一のグラフィカル表示を再現します。スキンのボタンは"生きている"ように動作し、実際のボタン操作を模倣します：いずれかのボタンをクリックすると、実機の該当ボタンを直接押した場合と同じ操作が実行されます。

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関するプロトコル設定です。主な通信方式として以下の 2 種類があります：TCP/IP と myCloud。ゲストからホストへ接続する前に、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種です。myCloud 通信はインターネットベースのプロトコルであり、ファイアウォールやプロキシ、NAT（Network Address Translation）対応ネットワークを介した接続を可能にします。これは WiseMo 社の myCloud サブスクリプションベース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遠隔制御接続を容易にします。