

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
お使いの端末で



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、認証済みユーザーがゲストモジュールを使用して安全に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、WiseMoが提供する以下のいずれかの方法で確立されます：
myCloudソリューション（インターネット経由）、またはLAN/WANネットワークを直接介した接続（TCP/IPプロトコルを使用）
直接接続のいずれかです。

クラウド接続（WiseMo myCloud）を利用する場合、お使いのコンピューターまたは端末はインターネットに接続できる必要があります。具体的には、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）経由での接続が可能です。これにより、場所を問わず、任意のコンピューターや端末にアクセスできるようになります。ただし、ゲストコンピューターとホストコンピューター/端末の両方でインターネット環境が整っていることが条件となります。

LAN（Wi-Fi/有線）またはWAN経由でTCP/IPを使用したオンプレミス接続を行う場合、インターネット通信に伴うデータ使用量やモバイル通信事業者からの追加料金が発生する可能性があります。また、ファイアウォールの設定を適切に管理し、ゲストモジュールからホストモジュールへの通信を可能にする必要があります。

Android 用ホストアプリは、Android 搭載端末向けに設計されたホストモジュールです。

このガイドでは、Android ホストアプリケーション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説明します。これは当社の Android 端末向けホストモジュールです。ホストモジュールを使用することで、簡単に迅速かつ安全なコンピューターや WiseMo ゲストモジュールを搭載した端末からの遠隔操作が可能になります。

注意：ホストモジュールが動作しているコンピューター/端末を遠隔操作するには、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ベ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. インストールと初回起動

本プログラムは対象端末にインストールされるため、**WiseMo** ゲストモジュールが動作しているコンピューターや端末から当該端末を遠隔操作することが可能です。

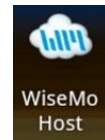
WiseMo Android ホストモジュールのダウンロードおよびインストール方法には、**Google Play** などのアプリストア経由や、ダウンロードリンク（**WiseMo** 提供）からの方法など、複数の選択肢があります。

すべてのインストール方法に共通する目的は、プログラムファイルを端末にインストールすることです。一部のインストール方法では、ライセンスファイルや設定ファイルも提供されます。これらのファイルが既に存在する場合、初回起動時にユーザーへの入力要求は表示されません。

ホストアプリのインストール時／初回起動時には、完全なリモートコントロール機能を許可するために必要な手順がいくつかあります。具体的な手順は **Android** のバージョンと **WiseMo** が端末メーカーとどのように連携しているかによって異なります。これらの手順には、プログラムに特定の **Android** リソースへのアクセス権限を付与することが含まれます。場合によっては、**WiseMo** のアドオンコンポーネントをダウンロード・インストールしたり、さまざまなユーザープロンプトを受け入れたりすることが必要になることもあります。

一般的に、アプリが要求する内容（アクセス許可の付与や追加モジュールのダウンロードなど）に同意すれば、リモートコントロールの準備は整います。これらの要求に同意しない場合、画面のリモート表示やキー入力・タッチ操作の送信が行えなくなる可能性があります。

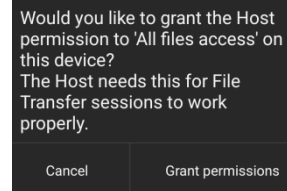
通常、ホストアプリはインストール後に自動的に起動します。起動しない場合は、端末上で **WiseMo** ホストアプリのアイコンを探し、手動で起動してください。



1.1 アプリストアからのインストール方法

ホストアプリは、**Samsung Galaxy Store** や **Google Play** など、さまざまなアプリストアからダウンロード可能です。このホストアプリには 内蔵の 試用版ライセンスが付属しており、後で永続ライセンスにアップグレードすることもできます。また、ホストを **WiseMo myCloud** に登録すればクラウドベースのライセンス管理と接続が可能になります。詳細は **myCloud** について後ほどご説明します。

- [Google Play](#) などのアプリストアでホストアプリを探してください。Samsung 端末の場合は、[Galaxy Store](#) でもホストアプリを見つけることができます。
- 「インストール」をクリックしてアプリをダウンロードし、端末にインストールします。「開く」ボタンをクリックするとホストが起動します。
- 初回起動時には、特定のファイルへのアクセス許可など、いくつかの権限を求められる場合があります。要求されるすべての権限は必須ではありませんが、完全な機能を利用するためには必要となります。
- 構成ウィザードが表示されます。ここでセキュリティ設定を定義し、**WiseMo myCloud** へのアクセス設定を行います。詳細はセクション 1.6 を参照してください。
- 最後に、リモートビューおよびコントロールの準備に必要な要件が表示される場合があります。詳細はセクション 1.5 を参照してください。



ホストアプリは、**myCloud** ドメインにサインインしている場合、LAN/WAN 経由で TCP 通信を行う準備が整います。また、インターネット経由での通信も可能になります。

1.2 WiseMo myCloud 展開用リンクを使用してインストール

ホストアプリは、**myCloud** ドメインから APK 形式のインストールファイルとしてダウンロードできます。この方法を使用するには、端末側で非 App Store アプリのインストールを許可する設定が必要です。ホストのインストールはあらかじめ設定済みで、**myCloud** ドメインへの参加が可能となっており、**myCloud** ライセンスが付与されています。インターネット経由で **myCloud** を介して、または LAN/WAN 上で TCP 通信を使用してホストに接続できます。このインストール方法は、事前に作成して **myCloud** ドメインにアップロードしておいたカスタマイズ設定ファイルを含むインストールファイルが必要な場合にも便利です。

- 端末のブラウザーから [myCloud](#) ドメイン（試用版または有料版）にログインします。次に「デバイスの管理」>「展開」に移動し、**Mobile Host** のダウンロードリンクを選択してください。ダウンロードリンクは、例えば電子メールや SMS（テキストメッセージ）で対象端末に送信することも可能です。
- ダウンロードページから、**Android** ホストインストーラーをダウンロードを選択してください。これによりファイルが端末に直接ダウンロードされます。別の方法として、APK インストールファイルをコンピューターにダウンロードしてから端末に転送することも可能です。

注意：myCloud ダウンロードページから Google Play または Samsung Galaxy を選択した場合、ホストアプリのインストールは、事前に myCloud ドメイン用に設定された状態では提供されません。myCloud ライセンスも適用されず、アップロードしたカスタマイズ設定ファイルも含まれません。代わりに、動作は上記 1.1 の説明通りとなります。

- c. ダウンロードしたインストールファイルを実行します。この操作には、端末がインターネットに接続している必要があります。
- d. 初回起動時には、特定のファイルへのアクセス許可など、各種権限の承認を求められる場合があります。すべての要求される権限は必須ではありませんが、完全な機能を利用するためには必要となります。
- e. 最後に、リモートビューおよびコントロールの準備に必要な要件が表示される場合があります。詳細はセクション 1.5 を参照してください。

1.3 スリーワンシステムズから APK ファイルを入手

APK インストールファイルをご希望の方は、スリーワンシステムズまでお問い合わせください。この方法は、アプリストアからのインストールを希望しない場合、または WiseMo myCloud を使用しない場合に適しています。

注意：端末はアプリストア以外のアプリのインストールを許可している必要があります。別の方法として、ホストは MDM ツールを使用して展開することも可能です。

- a. ダウンロードページから、**APK リンク**を選択してファイルをダウンロードしてください。

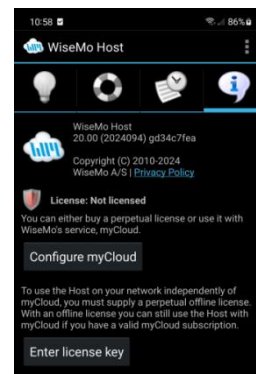
注意：ダウンロードページからは Google Play または Samsung Galaxy を選択することも可能です。これにより、指定したストアに遷移します。動作については上記 1.1 の説明を参照してください。

こちらから APK ファイル直接ダウンロードすることもできます：www.wisemo.com/d/a

- b. 端末上で APK ファイルを実行し、ホストアプリケーションをインストールしてください。
- c. 初回起動時には、特定のファイルへのアクセス権限など、各種権限の許可を求められる場合があります。要求されるすべての権限は必須ではありませんが、完全な機能を利用するためには必要となります。
- d. 構成ウィザードが表示されます。ここでセキュリティ設定を定義し、オプションとして WiseMo myCloud へのアクセス設定を行うことが可能です。詳細はセクション 1.6 を参照してください。
なお、インストール前に事前に設定済みの host.xml 設定ファイルをホストアプリの構成フォルダーに配置¹することで、ウィザードを省略することが可能です。
- e. myCloud へのアクセス設定を行わない場合、情報画面が表示され、ホストはライセンスが未取得のため起動しません。「**ライセンスキーを入力**」を選択し、試用版キーまたは購入した永続ライセンスキーのいずれかを入力してください。

なお、この手順を省略するには適切な host.lic ライセンスファイルをホストアプリの構成フォルダーにインストール前に配置してください。

- f. 最後に、リモートビューおよびコントロールの準備に必要な設定を求められる場合があります。詳細はセクション 1.5 を参照してください。



1.4 MDM ソリューション経由または Android 管理構成を使用してインストール

大規模な展開の場合、MDM ソリューションを使用できます。このソリューションは、設定ファイル、ライセンスファイル、およびアプリケーション本体の展開を処理し、場合によってはアドオンモジュールのインストールも行います。Android ホストアプリは Android 管理構成（多くの場合 MDM ソリューションでサポートされています）によるインストール/設定にも対応しています。詳細については別添のドキュメント [こちら](#) を参照してください（開発元のドキュメントになります）。

1.5 リモートビューとコントロールの準備

WiseMo ホストアプリでは、端末の製造元や場合によっては Android のバージョンに応じて、画面キャプチャと入力操作のシミュレーションに異なる技術を採用しています。具体的には：

¹ 構成フォルダー：[SDCard]/Android/data/com.wisemo.host.v10/files/WsmHost/

- **WiseMo** が開発・提供するメーカー専用のアドオンコンポーネントを使用しますが、このコンポーネントは端末製造元によって署名されています。
- **WiseMo** が提供する汎用的なユニバーサルアドオンを使用し、**Android** のアクセシビリティサービスを活用します。
- 端末製造元が提供する **API** を使用します。
- **Android** に標準搭載されている画面キャプチャ機能を利用します。
- 上記の方法を組み合わせた手法
- ルート化済み端末を使用する場合

ホストアプリでは、最適な操作方法を提案します。セットアップ時に各種権限の許可要求やダウンロード推奨メッセージを受け入れると、通常、端末を遠隔から表示・操作できるようになります。ただし、端末が最新バージョンの **Android** を実行している場合に限りです。

各操作方法にはそれぞれ異なるセットアップ手順が必要です。以下に一般的な例をいくつか示します。詳細については [こちら](#) をご覧ください。

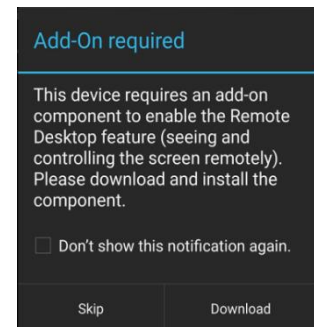
アドオンコンポーネント方式

アドオンコンポーネントには、メーカー固有のアドオンと **WiseMo** 汎用アドオンの 2 つの基本的なバージョンがあります。

ホストは初めて起動する際にアドオンコンポーネントのダウンロードを推奨します。

一部のアドオンは **Google Play** から入手可能です。この場合、**Google Play** の該当アドオンページに誘導され、直接インストールできます。その他のアドオンは **WiseMo** からのみ入手可能です。ホストアプリは **WiseMo** のページに誘導し、そこで推奨されるアドオンが一覧表示されます。推奨されるアドオンをダウンロードしてインストールしてください。

重要な点として、インストールするアドオンは 1 つだけにし、適切なものを選択してください。必ず推奨されるアドオンをご利用ください。アドオンコンポーネントは、ホストアプリのメニュー「設定」「プログラムオプション」から後でインストールすることも可能です。「ホストリモートコントロールアドオンをインストール」をクリックしてください。

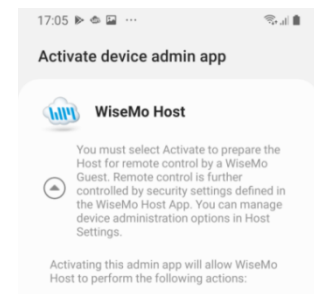


メーカー認証済みのアドオンが利用できない場合、汎用ユニバーサルアドオンの使用が推奨されます。リモート画面の表示と操作は通常、**Android 8** 以降でサポートされています。画面キャプチャ機能は、**Android** の標準画面キャプチャ機能と **WiseMo** ユニバーサルアドオンの組み合わせで利用可能です。ユニバーサルアドオンは、**Android** のアクセシビリティサービスを利用して入力をシミュレートします。タッチ入力は完全にサポートされていますが、キーボード入力の注入は部分的にしかサポートされていません（アプリやテキスト入力制御の仕様により異なります）。ゲストアプリからの操作となります。それ以外の場合、**Android** のオンスクリーンキーボードはリモートで開かれて使用することが可能です。

大規模な端末展開の場合、アドオンコンポーネントは **WiseMo** からリクエストし、ホスト本体をインストールする前の別工程としてインストールできます。例えば、**Android** 端末向けの **MDM** ソリューションを使用して展開する場合などに有効です。

Samsung KNOX 方式

Samsung 製端末にホストをインストールする際、ホストはデフォルトで **Samsung** の **Knox** 機能を利用し、リモート表示とリモート入力制御を提供します。ホストは「端末管理者」権限を要求しますので、これを承認する必要があります。右側の操作画面例を参照してください。「有効化」をクリックし、**Samsung Knox** ライセンス画面に移動して利用規約に同意することで、完全なリモートデスクトップ制御が有効になります。



Zebra 方式

Android 5.0 以降を搭載した **Zebra** 端末はリモート表示が可能です。完全なリモート制御を行うには追加の設定が必要です。この設定では、キーボード操作やタッチイベントのエミュレーションも可能になります。設定

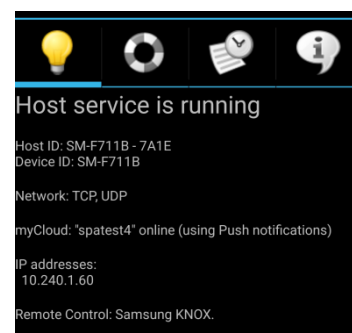
は端末上で Zebra Stage Now を介して、あるいは MDM ソリューションを通じて行うことができます。必要な設定手順については、以下のガイドで詳細に説明しています（開発元のドキュメントになります）。

https://download.wisemo.com/download/WiseMo_remote_control_of_Zebra_scanner_devices.pdf

適用されている認証方式の確認

ホストアプリには、端末に設定されている認証方式が表示されます。ステータスビューをご確認ください。この例では、**Samsung Knox** 方式が使用されています。

端末上でこのステータスを確認してください。リモートで端末を表示または制御できない場合は必ず確認が必要です。



1.6 構成ウィザード

インストール後にホストが未設定の場合（例えば myCloud、Android 管理構成、構成フォルダーにコピーした設定ファイルやライセンスファイルなどを介して設定されていない場合）、構成ウィザードが表示されます。

ゲストアクセス用の認証方式と関連設定を選択し、myCloud ドメインへのアクセスを設定することが可能です。

まず、端末にアクセスするリモートゲストユーザーの認証方法を選択してください。「共有パスワード」方式と「myCloud デバイスアクセス制御」方式のいずれかを選択します。

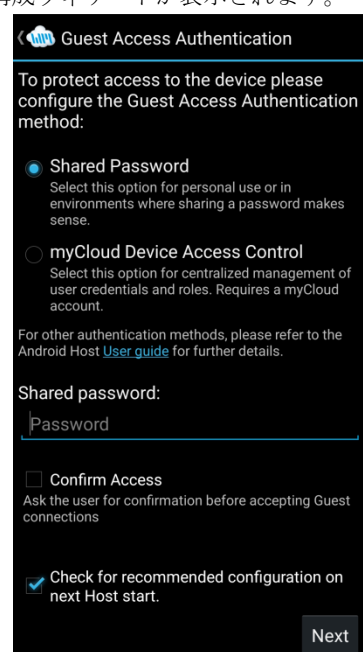
共有パスワード方式

「共有パスワード」方式を選択した場合、リモートゲストユーザーがアクセスするために入力しなければならないパスワードを設定できます。

「アクセスの確認」機能を有効にすることも可能です。この機能は、端末上で遠隔操作を行うユーザーがアクセス許可を求めるプロンプトを表示します。WiseMo ゲストモジュールが端末にアクセスする前に、この確認が行われます。ホスト端末が無人で使用されている場合、「アクセスの確認」機能は無効にしておくことをお勧めします。

遠隔操作を行うゲストユーザーが共有パスワードオプションを使用してアクセスを許可された場合、デフォルトのアクセス権限ではすべての利用可能な機能を使用できるようになります。

アクセス権限を制限したり、単一のパスワードではなく個別のユーザー名やパスワードを定義することも可能です。詳細はセクション 5.4 を参照してください。



myCloud デバイスアクセス制御

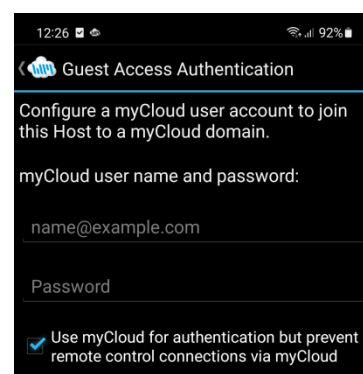
myCloud デバイスアクセス制御 (mDAC) は、WiseMo が提供する認証とアクセス権限の集中管理ソリューションです。mDAC が選択されている場合、ウィザードは認証とアクセス権限を管理する myCloud ドメインにホストを登録するための資格情報の入力を求めます。

ウィザードで「次へ」をクリックすると、myCloud ドメインにホストを登録するための資格情報を入力する画面が表示されます。mDAC を使用するには、myCloud へのアクセス設定が事前に行われている必要があります。

ホストは mDAC による TCP/IP 接続のみの認証設定が可能であり、リモート制御は TCP/IP (LAN/WAN 経由) でのみ可能です。認証は myCloud へのアクセスを通じて行われます。この方式では、ホストに永続ライセンス（初期段階ではトライアルライセンスでも可）が必要となり、さらに myCloud ライセンスも消費されます。

ウィザードの完了後、ホストがライセンスを取得している場合、端末の電源投入時に自動的に起動するように設定されます。また、起動後は通信のための初期化処理が自動的に実行されるため、定義されたセキュリティ設定に従い、WiseMo ゲストアプリからのリモート接続に対応できる状態になります。

注意：初回起動時、ホストに構成ウィザードが表示されない場合があります。例えば、mDAC が有効化された myCloud ドメインから展開リンクを使用してホストを展開した場合などです。この場合、ホストは既にセキュ



リティ設定が定義されており、どの **myCloud** ドメインにサインインすべきかを把握しています。同様に、これらの設定が既に定義された設定ファイルが別途存在する場合も同様です。

構成ウィザードは、「ホストアプリのメニュー」>「設定」>「ゲストアクセスセキュリティ」から手動で実行できます。

Android ホストモジュールは多くの構成オプションをサポートしています。ユーザーインターフェース自体ではこれらの設定の一部しか操作できませんが、詳細は以下セクション **2.2** を参照してください。利用可能なすべての構成オプションにアクセスするには、**Windows** ベースのホストマネージャーを使用して設定ファイル **host.xml** をカスタマイズします（設定の詳細については、セクション **5** のホストマネージャーを使用した設定に関する記述を参照してください）。

1.7 リモート制御可能状態

インストール後または初回起動後、**WiseMo** ホストモジュールはリモート制御可能な状態になっているはずです。

WiseMo ホストのロゴは、**Android** 端末の通知バーに表示されます。ホストサービスが初期化されると、このロゴが表示されます。

通知バーを展開し、ホストアイコンを選択して、ホストアプリに素早くアクセスしてください（または「アプリ」からホストを選択します）。

ライセンス状態が正常であることを確認してください

「情報」画面を選択し、ホストのライセンス状態が正常であることを確認します。緑色の盾のアイコンが表示されれば、ライセンスが有効であることを示しています。

ライセンスが未取得の場合は、ライセンスを設定する必要があります（トライアル版または購入版のいずれかを選択してください）。また、ホストを **myCloud** ドメインに登録することでライセンスを付与することも可能です。

ホストのステータスが正常であることを確認してください

ステータス画面を選択し、以下の表示内容を確認してください。「ホストサービスが実行中」と表示されており、以下の **2** つの項目のうち少なくとも **1** つが表示されていることが必要です：

- 「ネットワーク：UDP、TCP」と表示されている場合、ホストが **LAN/WAN** 上で **TCP/IP** 経由で直接アクセス可能な状態に設定されていることを示します。また、表示されている **IP** アドレスが有効であることも確認してください。
- 「**myCloud**：<ドメイン名> オンライン」と表示されます。セキュリティ設定に応じて、**myCloud/LAN/WAN** 経由での接続が可能です。ステータスが「オンライン」と表示されず、「**myCloud** デバイスアクセス制御」のみが表示されている場合、この **myCloud** ドメインを介して **LAN/WAN** 接続の認証が設定されていますが、**myCloud** 経由の接続はできません。

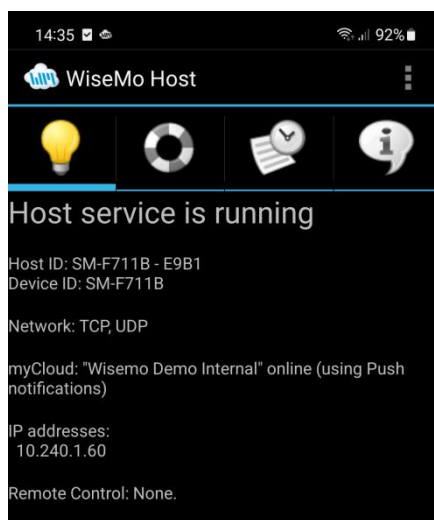
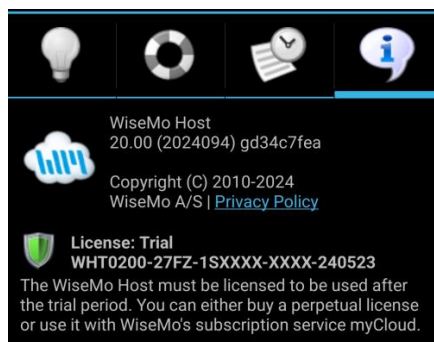
ステータスが「実行中」と表示されていない場合は、ホストメニューを選択し、「開始」または「再起動」をクリックしてください。

また、「リモートコントロール：」の項目が「なし」またはリモートコントロールが完全に有効になっていないことを示す他の表示になっていないことを確認してください。この項目には、ホストが設定されているモードが表示されるはずです。上記のセクション **1.5** を参照してください。

ホストのアドレス / ゲストモジュールからホストを識別する方法

ステータス画面に表示される **IP** アドレスとホスト **ID** に注意してください。これらは、通信方法に応じてゲストユーザーがホストを指定または識別する際に使用する重要な **ID** です。必要に応じてホスト **ID** を変更することもできます（**2.2.2** を参照）。

「端末 **ID**」（スクリーンショット上の **SM-F711B**）は、ゲストモジュールがスキンファイル（端末の画像）を **WiseMo** のスキンサーバー、またはローカルのゲストコンピューターもしくはローカルサーバーからダウン

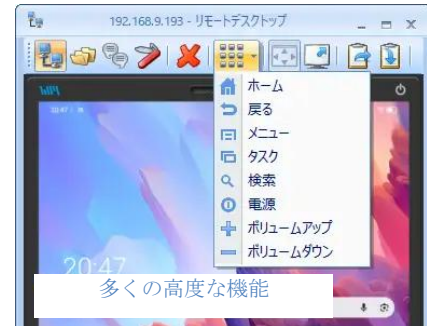


ロードする際に使用します。例えば、ゲストコンピューターにインターネット接続がない場合などに、スキンファイルをここに配置しておくことができます。

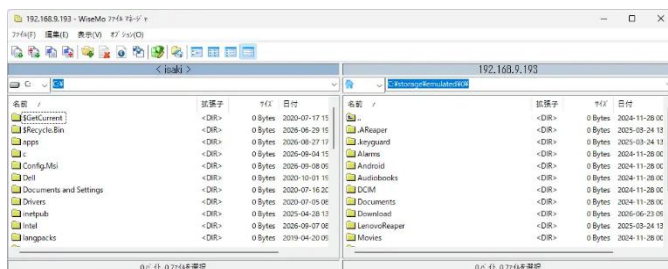
上記の設定がすべて完了していれば、ホスト側のリモートコントロール準備が整いました。以下のセクション 2 では、ホストの機能とそのユーザーインターフェースについて詳しく説明します。端末への接続方法については、ブラウザまたは **WiseMo** ゲストアプリからの接続方法について記載したセクション 3 を参照してください。

ホストは、リモートアクセス用に **WiseMo** ゲストアプリを実行しているユーザー向けに **Android** 端末を準備します。さらに、この機能は利便性と価値を大幅に向上させる数多くの機能を提供します。これらの機能は、端末を目の前に操作しているかのように遠隔操作を行う場合にも、問題を抱えたユーザーに対して遠隔サポートや支援を提供する場合にも、**Android** 端末とゲスト PC 間のファイルやディレクトリの転送を行う場合にも活用できます。

WiseMo Android ホストは、無人環境とユーザーが立ち会う環境の両方での使用を想定して開発されています。無人環境においては、遠隔アクセスが必要になった際に即座に応答できる状態にしておくことが重要です。ユーザーが立ち会っている場合には、セキュリティ上の理由やバッテリー・リソースの節約のため、遠隔アクセスを行う直前にプログラムを起動させたい場合があるでしょう。無人環境においても、**WiseMo** はバッテリーやリソースを消費することなく端末にアクセスできる独自の機能を提供しています（自動起動機能など）。



使用するゲストモジュールに応じて、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（画面表示と操作、端末のほとんどのボタン操作を含む）、リモートクリップボード転送、ファイル転送、ハードウェア/ソフトウェアインベントリ収集、チャット、アプリのリモート実行、ゲストユーザーからのメッセージ受信など。さらに複数のゲストユーザーが同時に同じ端末に接続することも可能です。



2.1 ホストユーザーインターフェース

ホストユーザーインターフェースは4つの画面（タブ）とメニューで構成されています。

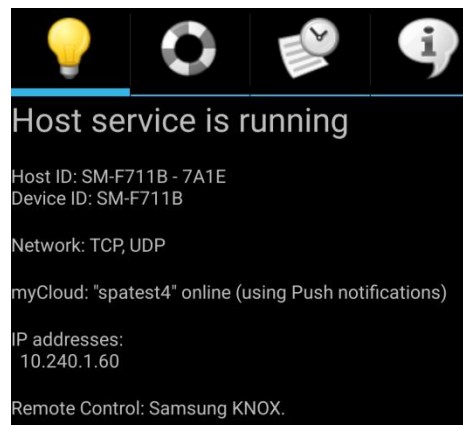
2.1.1 ステータス画面



この画面ではホスト ID と検出された IP アドレスが表示され、ゲストユーザーが接続時に対象端末を特定するために使用できます。より一般的な端末 ID も表示されます。

この画面では通信関連の情報と、myCloud 通信用に準備された状態が表示されます。

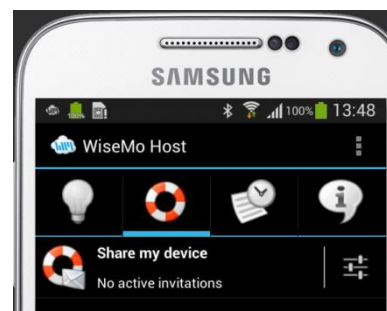
最後に、ステータス画面では、画面キャプチャと入力の送信に使用されている方法（タッチ操作、キーボード、マウスなど）も表示されます。



2.1.2 端末画面の共有



「端末を共有」をクリックすると、招待リンクの有効期間、セキュリティ設定、およびアクティブなリンクの実際の作成または無効化を設定できます。「端末を共有」ボタンの右側にある設定ボタンを押すと、ホストユーザーは許可する接続数と、リンクの有効期限が切れた後の動作を定義できます。



作成後、このリンクを第三者に転送してください（例えばメールで送信します）。第三者は、対応ブラウザーから、またはインストール済みの **WiseMo** ゲストアプリケーション（Android、iOS、Mac、Windows など）からリンクを実行できます。

注意：デスクトップ上に端末共有アイコンを配置することで、ユーザーがリンクを簡単に作成できるようになります。このオプションの設定方法については、セクション 2.2.1 を参照してください。

2.1.3 履歴画面

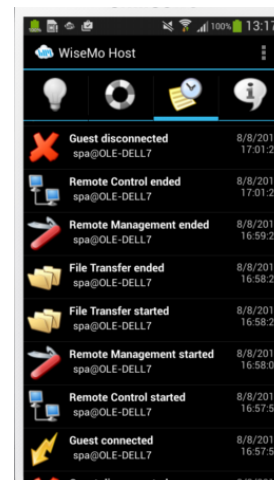
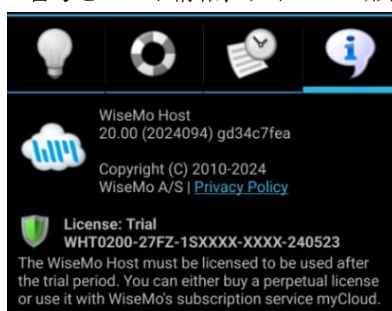


履歴画面には、ホストアプリケーションが起動してから接続／切断されたゲストの一覧が、日付と時刻とともに表示されます。また、主要なセッションタイプ、リモートデスクトップ制御、ファイル転送、チャット、リモート管理などの機能も表示されます。追加メニューオプションの履歴をクリアを選択すると、履歴リストが空になります。より詳細なログをファイルに記録する場合は、利用可能な詳細なロギング機能を使用してください（詳細はセクション 2.2.6 ログ設定を参照してください）。

2.1.4 情報画面



情報画面では、ホストのバージョン番号とビルド情報、ライセンス形態（サブスクリプション、永続ライセンス、または試用版）、著作権情報が表示されます。また、ライセンスの取得や設定を簡単に行うことができ、例えばホストを **myCloud** ドメインに登録したり、試用版または永続ライセンスキーを適用したりすることができます。端末に接続できない場合は、この画面を確認してください。試用版キーの有効期限が切れている可能性があります。



2.1.5 メニュー

設定： ホスト自体から設定可能な各種設定項目へのアクセスを提供します。詳細については、第 2.2 節の詳細な説明を参照してください。

チャットの表示： ゲストユーザーはホストユーザーとチャットを行うことができます。通知が表示されるか、またはメニューオプションの「チャットを表示」を選択すると、ホストユーザーはチャットダイアログ画面に移動します。ホストユーザーはチャットセッションを終了し、ダイアログの履歴を消去することで、ゲストユーザーとホスト間のアプリ起動時からのチャット履歴を削除することができます。

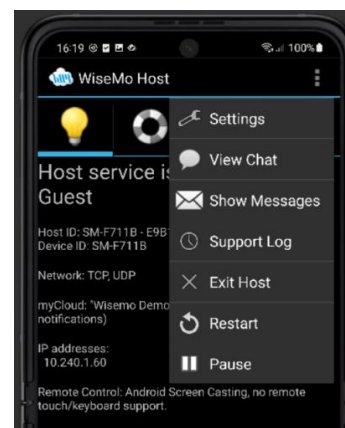
メッセージ表示： ホストアプリ起動後にゲストから送信された一方向メッセージを表示します。すべてのメッセージを消去するには、サブメニューの「メッセージをクリア」を使用するか、ホストアプリを終了してください。

サポートログ： トラブルシューティング用のログファイルを作成します。**WiseMo** に問題を報告する際に添付すると便利です。このファイルは `[SDCard]/Android/data/com.wisemo.host.v10/files/WsmHost/` フォルダーに、**wsmHostAndroid.log** という名前で作成されます。

アンインストール： このオプションは古い **Samsung** 端末でのみ利用可能です。ホストアプリをアンインストールするためのクイックアクセスオプションです。通常、古い端末では **Android** アプリを削除する際に必要な「端末管理者の有効化」設定を無効にします。

ホストアプリを終了： ホストアプリを閉じます。「プログラムオプション」で「自動起動」機能が有効になっている場合、その機能は引き続き有効です。

再起動： 通信を再起動します。通常、新しい設定を適用した後に使用します。

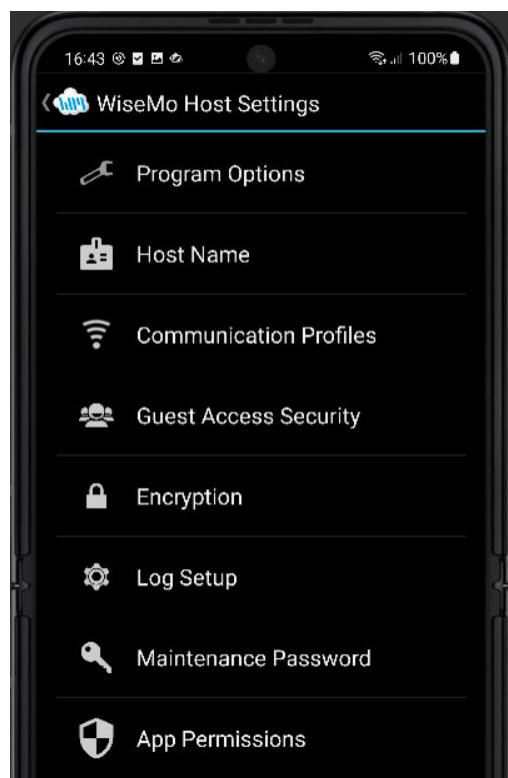


起動/一時停止/切断：ホストの状態に応じて、通信の開始/一時停止、またはゲストユーザーとの接続切断を行うことができます。

2.2 設定

ホストの設定項目の多くは、ホストのユーザーインターフェースから直接管理できます。セキュリティロール（アクセス権限）や個別のパスワードを含むユーザー資格情報の定義など、追加の設定項目については、ホストマネージャーモジュールを使用します（本文書の後半で説明するセクション5「ホストマネージャー」をご参照ください）。

ホストメニューから「設定」を選択すると、ユーザーインターフェース経由で利用可能な構成オプションが表示されます：



2.2.1 プログラムオプション

自動起動機能：ホストアプリが実行されていない状態でも端末に接続できます。また、バッテリーやその他のリソースの節約にも役立ちます。この機能は、**myCloud** を使用している場合に利用可能で、ホストを起動することができます。

起動時の読み込み：端末を起動すると、ホストアプリが自動的に読み込みされます。

起動時の開始：ホストサービスが通信を初期化し、実行状態に移行します。認証済みのゲストユーザーからの操作を受け付ける準備が整います。

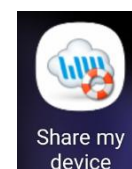
端末管理の有効化：**Samsung** 製品特有の設定です。**WiseMo** リモートコントロールアドオンがインストールされていない場合は必ず有効にしてください。

画面密度最適化：高解像度ディスプレイを搭載した端末でパフォーマンスを向上させるために利用可能です。リモートセッション中にオン/オフの切り替えが可能です。

リモートコントロール機能のアドオン：リモートコントロール用アドオンモジュールがインストールされているかどうか、または必要なアドオンのインストール方法を通知します。この項目は、端末に対応するアドオンコンポーネントが存在する場合にのみ表示されます。

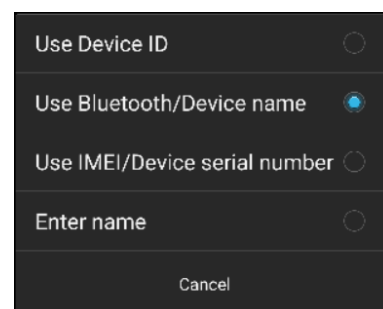
プライベート設定を使用：ライセンスおよび設定ファイルはプライベートに保存され、ホストマネージャーや他のファイルマネージャーからはアクセスできません。一部の端末/組み込みシステム（例えばセットトップボックスなど）では、プライベート設定の使用が必要となる場合があります。

「端末を共有」アイコン：デスクトップ上に一時的な招待リンクを作成する追加アイコンの表示/非表示を切り替えます。詳細はセクション 2.1.2 「端末を共有する画面」 もご参照ください。

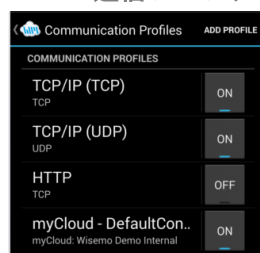


2.2.2 ホスト名

ホスト ID のソースを選択してください。デフォルトでは、ホストは端末 ID にランダムな番号を付加したものを使用します。別の方法として、**Bluetooth**/端末名または **IMEI**/端末シリアル番号を使用することも可能です（使用している **Android** バージョンでこれらが利用可能な場合）。固有の名前を必ず使用してください。そうすることで、アクセスしたい端末を正しく識別できるようになります。



2.2.3 通信プロファイル



各種接続方式の通信設定を定義します。主に上級者向けの機能です。プロファイルをクリックして編集してください。プロファイルの有効/無効を切り替えるには、「オン」/「オフ」ボタンをクリックしてください。**myCloud** 経由のリモートアクセスのみを必要とする場合は、他の接続方式を無効にしてください。また、新しいプロファイルを追加したり、既存のプロファイルを削除したりすることもできます。

TCP/IP プロファイルの場合、例えばポート設定などを構成できます。

myCloud プロファイルを使用する場合、myCloud ドメインへのログインや別ドメインへの切り替えが必要になることがあります。myCloud プロファイルをクリックし、「ドメイン設定」を選択して、対象ドメインの myCloud ユーザー資格情報を入力した後、「myCloud ドメインにホストを追加」ボタンをクリックしてください。また、myCloud プロファイルがインターネット経由で接続する際にプッシュ通知を使用するかポーリングを使用するかを設定することも可能です。接続時間を短縮できるプッシュ通知の使用が推奨設定となっています。

2.2.4 ゲストアクセスのセキュリティ設定

ホストシステムには、誰が何を実行できるかを管理する高度な認証・認可機能が搭載されています。

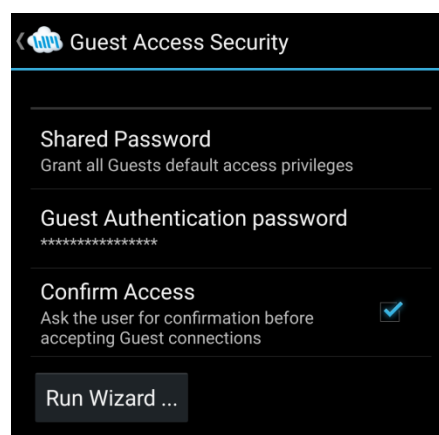
ユーザーインターフェースでは、端末へのアクセスを保護するための 2 つの選択肢が用意されています：「共有パスワード」または「myCloud デバイスアクセス制御（mDAC）」です。選択した方法をクリックすることで、別の方法に変更することができます。

共有パスワード

共有パスワード方式では、パスワードによる端末アクセス保護に加え、オプションとして確認済みのアクセスを要求することができます。

ゲスト認証用パスワード：パスワードを入力して端末にアクセスするか、パスワード保護なしで端末を使用します。パスワード保護が有効になっている場合、ゲストユーザーはアクセス許可前に正しいパスワードを入力するよう求められます。

アクセスの確認：この機能は、ゲストユーザーがアクセスを取得する前にホストユーザーに許可を求めるものです（確認済みアクセス）。ユーザーが端末の近くに存在している場合の強力なセキュリティ機能ですが、無人の端末へのアクセスには使用しないでください。



共有パスワード方式では、パスワードがデフォルトのアクセス権限ルールとして使用され、ゲストモジュールでサポートされているすべての機能の使用が許可されます。デフォルトのアクセス権限ルールを変更することで、権限を制限することが可能です。この設定はホストマネージャーから行います。詳細は 5.4.1 を参照してください。ここでは、二要素認証を使用してアクセスを保護することもできます。この場合、ユーザーはアクセスを取得する前に常に変化するパスコードを入力する必要があり、パスワードに加えてこの操作が求められます。

「ウィザードを実行」をクリックすると、上記 1.6 で説明した構成ウィザードが表示されます。

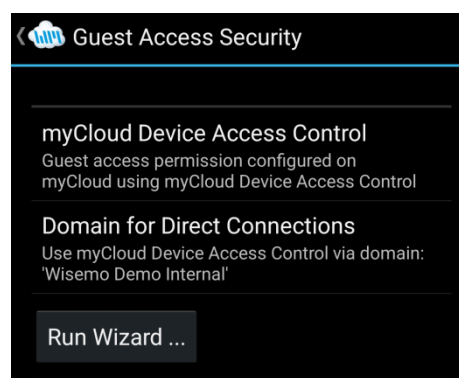
ユーザーID/パスワードによるアクセス制限を実施し、ユーザーごとに異なるアクセス権限を設定したい場合は、ホストマネージャープログラムを使用してください（セクション 5.4.1 を参照）。

myCloud デバイスアクセス制御（mDAC）

mDac 方式は、各端末に対するユーザーの操作権限を一元管理する手法です。ユーザー定義（誰）、アクセス権限定義（何を操作できるか）、およびユーザーがアクセス可能な端末の指定を、myCloud ドメイン内で集中管理します。

mDAC を LAN/WAN（TCP/IP）経由の認証のみに限定して設定することも可能です。これにより、myCloud（インターネット）経由でのアクセスを禁止することができます。

「ウィザードを実行」ボタンをクリックすると、上記 1.6 で説明した構成ウィザードが表示されます。



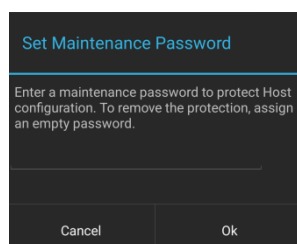
2.2.5 暗号化

ホストシステムは最上位レベルの暗号化機能とデータ傍受・改ざん防止対策を提供し、データストリームの保護を行います。ホストの設定によって最終的に適用される保護レベルが決定されます。ホストの設定で複数の保護レベルが許可されている場合、ゲストユーザーは暗号化なしを含む任意の暗号化レベルを選択できます。特にインターネット経由での操作時には、データストリームがどのコンピューターを通過するか分からないため、暗号化の使用が強く推奨されます。

2.2.6 ログ設定

イベントのログ記録を有効にし、ログファイルの保存先を指定できます。記録するイベントをカスタマイズするには、ホストマネージャープログラムを使用してください（セクション 5.6 参照）。

2.2.7 メンテナンス用パスワード

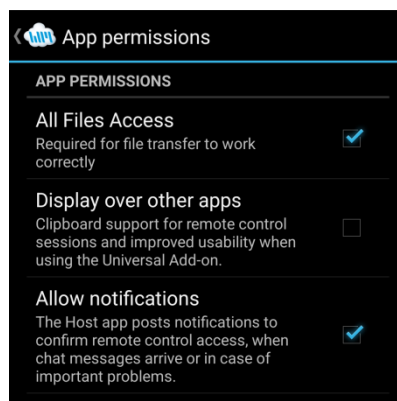


ユーザーインターフェースを介したホストアプリケーションの設定変更を防止するため、メンテナンス用パスワードで設定を保護することができます。**Wisemo**ホストの設定にアクセスするには、ユーザーはこのメンテナンス用パスワードを知り、入力する必要があります。

2.2.8 アプリの権限

この画面では、各種 **Android** 権限が有効化されます。特定の機能を動作させるために、権限を選択／解除する必要があります。

権限を選択／解除すると、その権限の有効 **Android** 設定画面に移動します。



されているかどうかが表示は、必要な権限が設定され

化／無効化を行うための

3. 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 Android 端末にアクセスし、リモート操作を行うことができます。

さまざまなプラットフォームから対応する WiseMo ゲストモジュールを使用することで、端末のリモート操作が可能です。具体的には、Android 端末（スマートフォン/タブレット）、iOS 端末（iPhone/iPad）、Mac コンピューター、および Windows コンピューターから操作できます。最も機能豊富なゲストモジュールは、Windows PC にインストールする Windows リモートデスクトップゲストモジュールです。

また、Android、iOS、Mac、または Windows の任意のブラウザからリモート操作を開始することも可能です。ブラウザは、リモート操作セッションを確立するために、インストール済みのゲストモジュールを利用します。

本章では、Windows リモートデスクトップゲストモジュールを経由した myCloud（インターネット通信）によるリモート操作と、TCP/IP を直接利用したリモート操作の両方の使用例をご紹介します。

このモジュールやその他のゲストタイプの使用法に関する詳細情報については、各モジュールに関連するドキュメントをこちらでご確認ください：<https://its.tos.co.jp/support/download/wisemo/>

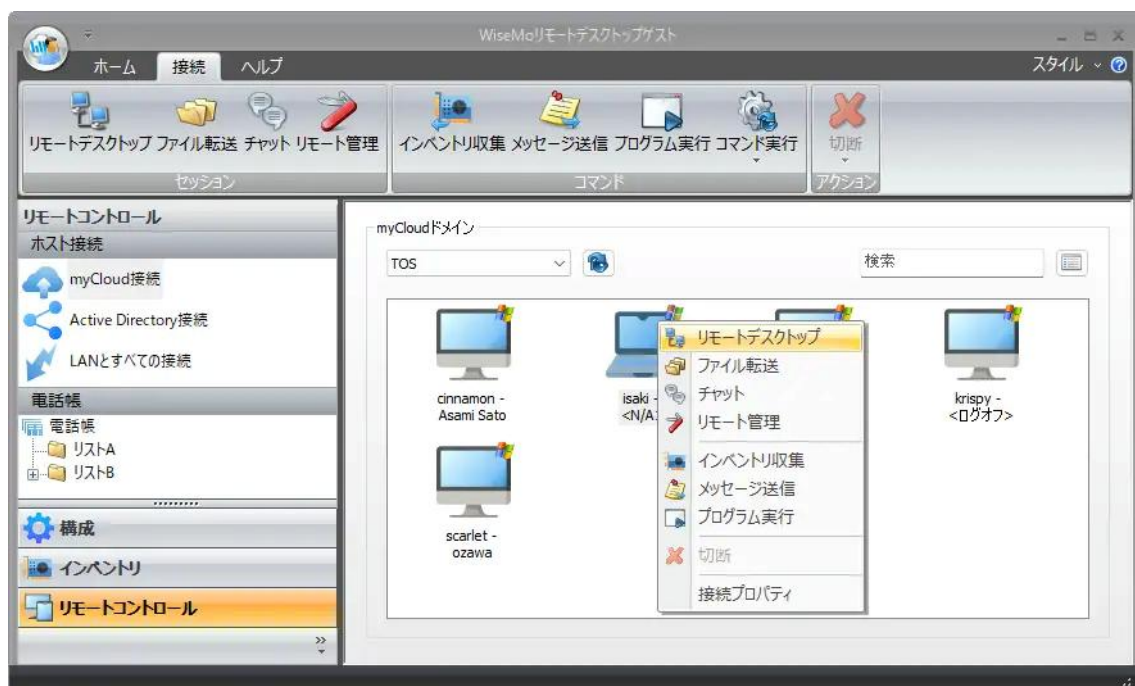
3.1 インターネット経由のリモートコントロール（WiseMo myCloud を使用）

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 Android ホストモジュールが展開されていることを前提としています。

myCloud（WiseMo 提供）は、コンピューターや端末間（PC、サーバー、Mac、スマートフォン、タブレット、その他の携帯型／無人端末など）でのリモートコントロール接続を容易にするクラウドベースのサービスです。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。myCloud では集中管理型のセキュリティ管理が可能で、各端末に対して誰が何を実行できるかを細かく設定できます。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[こちら](#)のページから直接ダウンロードするか、myCloud ドメイン内の「デバイス管理」>「展開」ページから入手できます。
2. 左側のメニューから「myCloud 接続」を選択し、myCloud ドメインにログインしてください。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と、リモートデスクトップセッションが開始されます（デフォルト設定）。別の方法として、ホストコンピューターを選択した後、「接続」タブで希望する機能のボタン（リモートデスクトップ、ファイル転送、チャット、リモート管理、メッセージ送信、インベントリ収集、プログラム実行またはコマンド実行）をクリックすることもできます。また、ホストコンピューターを右クリックしてメニューから選択することも可能です。
4. リモートデスクトップセッションを開始すると、プログラムがリモート端末に接続し、PC のデスクトップ上に独立したリモートデスクトップ制御ウィンドウが表示されます。

初めて端末に接続する場合、ゲストが端末のスキン画像をダウンロードするため、数秒かかります（スキンについての詳細は本ドキュメントの後半で説明します）。

ウィンドウには端末のライブボタンとライブ画面が表示されます。上部にはメニューが、下部には接続状態に関する情報が表示されます。ウィンドウを選択してリモート制御を開始すれば、まるで端末の前に座っているかのようにリモートホスト端末を操作できます。端末 - あたかも目の前にいるかのように

ヒント:ウィンドウを表示せずに端末を表示することも可能です（「透明なウィンドウとして表示」を使用）。接続前に接続プロパティ設定でこの設定を定義できます。透明なウィンドウを使用する場合、端末のスキン部分にマウスカーソルを合わせて右クリックすると、メニューオプションにアクセスできます。3.2 のスクリーンショットを参照してください。

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。



3.2 LAN / WAN 上でのリモートコントロール

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 アドレスまたはコンピューター名を指定し、その後接続することです。

1. お使いの PC 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. 左側のペインにあるメニューから「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 アドレスを入力してください。ホストの IP アドレスは、**Android** 端末上でホストモジュールを開くことで確認できます。IP アドレスはホストのステータス画面に表示されています。

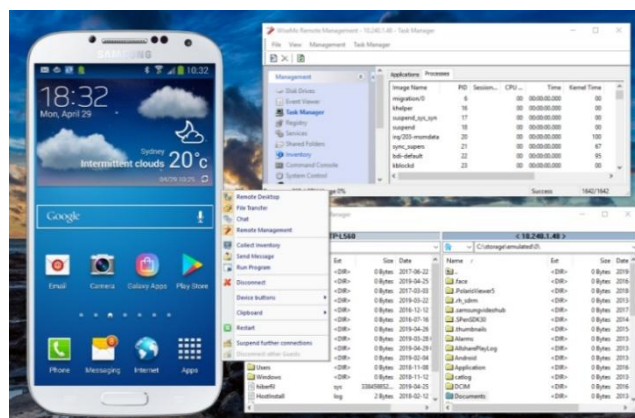


4. 「接続」ボタンをクリックしてください。



（または「接続」タブの「リモートデスクトップ」）

5. 端末に初めて接続する場合、PC にリモートコントロール画面が表示されるまでに数秒かかります。これは、ゲストが端末の画像（「スキン」と呼ばれるもので、本ドキュメントの後半で詳しく説明します）をダウンロードしているためです。
6. 同時に、ファイルマネージャーやリモート管理コンソールなどの他の機能も起動できます。



端末をリモート操作できます。リモート端末にキー入力を送信したり、リモート端末の画面の変化を確認したり、ファイル転送、ハードウェア/ソフトウェアインベントリ、チャット、リモートクリップボードなど、さまざまなその他の機能を利用できます。

上記の例のように透過スキンを使用している場合、スキン上で右クリックするとメニューオプションにアクセスできます。

4. スキン

デフォルトでは、Windows PC 上では、Android 端末のデスクトップが端末の画像内に表示されます。この端末の画像は「スキン」と呼ばれます。

スキン上に表示される端末ボタン（一部例外あり）は「リアルタイム」で動作し、あたかも端末本体で直接ボタンを押したかのように、端末を操作するために使用できます。

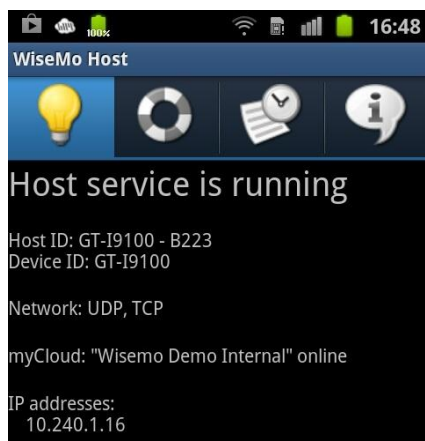
WiseMo の製品は、物理的な距離を感じさせない体験を提供することで、遠隔操作の課題を解決するように設計されています。WiseMo の先進的なスキン技術を活用することで、この「その場にいるような感覚」を大幅に向上させることができます。マウスを直接スキン上で操作できるほか、ゲスト用キーボードを使用してホスト端末上でキー入力を行うことも可能です。

スキン機能は、ホストについては「接続プロパティ」で、また全体的には「構成」で管理され、いずれも Windows ゲストモジュール内にあります。



デフォルトでは、スキンはウィンドウ内に表示されます。このウィンドウ下部にはメニューオプションとステータス情報が表示されます。なお、メニューバーは分離可能で、表示可能な範囲を超える追加オプションが含まれている場合があります。

ウィンドウを表示せずに端末を表示することも可能です（透明なウィンドウを使用）。接続前に「接続プロパティ」設定でこの設定を行います。透明なウィンドウを使用する場合は、マウスカーソルを端末のスキン部分自体に合わせて右クリックすると、メニューオプションにアクセスできます。



特定の端末用のスキンは、自動的に「端末 ID」に基づいて選択されます。

特定の端末の「端末 ID」は、ホストアプリのステータス画面で確認できます。

WiseMo では多数の端末用スキンを作成していますが、一部の端末にはスキンが用意されていない場合があります。もし特定のスキンがスキンリポジトリに存在しない場合、デフォルトのスキンが使用されます。

システム設定により、スキンを使用せずに端末の「デスクトップ」をそのまま表示することも可能です。

特定のスキンのサポートをご希望の場合は、ぜひご連絡ください。詳細は sales@its.co.jp までメールでお問い合わせください。この際、ホストアプリのステータス画面で確認できる端末 ID を必ず記載してください。

5. ホストマネージャー（設定編集用）

設定項目は **host.xml** ファイルに保存されており、以下の場所にあります：

/storage/emulated/0/Android/data/com.wisemo.host.v10/files/WsmHost/

多くの設定項目はホストアプリから直接変更できますが、利用可能な構成オプションが多数あるため、**WiseMo** では **Windows PC** から簡単にホスト設定を変更できる「ホストマネージャー」プログラムを開発しました。

「ホストマネージャー」は[こちら](#)からダウンロードし、**Windows PC** にインストールしてください。すでに **Windows** 用ホストアプリがインストールされている場合でも、**Android** ホストの設定用にホストマネージャーとして使用できます。インストールが完了すると、ホストマネージャーは **Windows** のスタートメニュー内の **WiseMo RSM** フォルダーに表示されます。ホストマネージャーを起動してください。

5.1 ホスト設定ファイル（host.xml）へのアクセス方法

USB ケーブルで端末を **PC** に接続してください。端末側で **PC** からのファイルアクセスが許可されていることを確認してください（「**USB** の使用目的：ファイル転送」）。この確認を行うには、**Windows** のファイルエクスプローラーを開き、端末に接続して端末上のファイルシステムにアクセスできることを確認してください。

端末が検出された場合、ホストマネージャーの左側パネル下部に表示されるリストから端末を選択してください（ホストマネージャー内）。プログラムは、可能であればその端末上に既に存在するホスト設定ファイルを取得します。取得できない場合、「開く」を選択してください（ホームタブで、ホスト.xml ファイルをその保存場所から開くことができます）。

「保存」ボタンを使用して変更した設定ファイルを端末に戻すことができますが、これは後の **Android** バージョンでは不可能な場合があります。その場合は、**Windows PC** 上にファイルを保存し、**Windows** のファイルエクスプローラーを使用してファイルを端末にコピーしてください。

Android バージョン 12 以降では、ホストマネージャーが直接端末上の設定ファイルにアクセスできないケースが多くなっています。

代わりに、**Windows** エクスプローラーを使用して、端末上の **host.xml** ファイルを **Windows** コンピューター上の任意のフォルダーにコピーしてください。ホストマネージャーでこのファイルをファイルとして開きます（ホームリボンタブから

「開く」を選択）。設定を変更した後は、再度ファイルを保存し（ホームリボンタブから「保存」を選択）、**Windows** エクスプローラーを介して **host.xml** ファイルを端末上の元のフォルダーにコピーし直してください。新しい設定を適用するには、端末のホストメニューから「再起動」を選択することを忘れないでください。

ホストマネージャーが端末上の設定にアクセスできない場合には

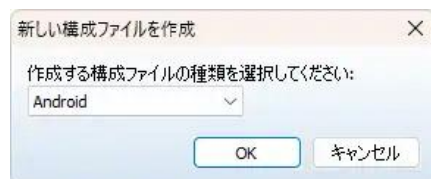
 適切な検出方法が端末検出用に有効になっていることを確認してください。これはホストマネージャーのホームタブから行います。



ホームタブの「リフレッシュ」ボタンを試してみてください。

「**Android ADB**」方式を使用するには、端末上で「**USB デバッグ**」を有効化する必要があります。そのためには、端末上で **Android** の設定を開き、「ビルド番号」を探してください。「ビルド番号」の項目に移動したら、5～6 回素早くタップします。次に「開発者オプション」を探し、「**USB デバッグ**」を有効にします。

まったく新しい構成ファイルを作成することも可能です。ホストマネージャーの「システム」メニューから「新規作成」を選択し、続いて「**Android**」を選んでください。



設定変更を行った後（ウィザードを使用する場合など）構成ファイルを保存し、**Windows** エクスプローラーを使用してホスト.xml ファイルを端末の構成フォルダーにコピーした後、端末上のホストアプリメニューで「再起動」を選択してください。

「デバイスを閉じる」を選択することで、ホストマネージャーインターフェースからファイルを削除できます。



システムメニュー

5.2 構成ウィザード

ホストマネージャーには構成ウィザードが用意されています。ホームタブからこのウィザードを選択してください。端末を PC に接続すると自動的に読み込まれる場合もあります。このウィザードは、起動設定や認証・認可オプションなど、さまざまな設定を行う際に役立ちます。

特定の **myCloud** ドメインにホストを接続するための設定を行う場合も、このウィザードをご利用ください。例えば、ホストが **myCloud** ドメインからの展開によって事前に設定されていない場合や、後で別のドメインに接続するように再設定したい場合などに便利です。

「次へ」ボタンを画面が **myCloud** の設定画面に表示されるまで押し続けてください。その後、「はい」を選択して **Enter** キーを押します。

次に、**myCloud** の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、および **myCloud** ユーザーアカウントが二要素認証保護されている場合は検証コード）を入力します。ウィザードが完了するまで「次へ」ボタンを押し続けてください。新しい設定を端末に保存することをお忘れなく（モバイルタブから、または **host.xml** ファイルを **Windows** コンピューターに保存して端末に転送することで行えます）。端末のホストメニューから「再起動」を選択して、新しい設定を適用してください。

ウィザードを使用して好みの設定を構成する代わりに、ホストマネージャーの設定パネルに直接アクセスして必要な具体的な変更を加えることができます。



5.3 プログラムオプション

このセクションでは、プログラムの一般的なプログラム設定を定義することができます。

変更を行った際には、必ず適用ボタンをクリックし、その後設定ファイルを端末に保存し、ホストモジュールを再起動してください。

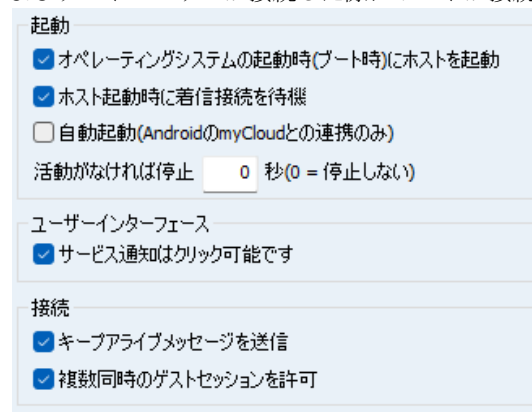


5.3.1 一般設定

起動：ホストが端末の起動時に自動的に起動するかどうか、およびゲストユーザーが接続した際にホストが接続を受け付ける準備が整っている必要があるかどうかを設定します。ホストが起動した後にこの設定が適用されます。両方の設定は無人運用の場合必ずチェックしてください。チェックを入れない場合、ホストの「開始」ボタンを手動で押す必要があります。また、ホストを自動的に停止させる設定も可能です。具体的には、一定時間（ゲストユーザーが接続していない状態）経過後に自動的に停止するように設定できます。ゲストユーザーが接続している間はホストは停止しませんが、接続が切断された直後に停止します（設定時間が経過した場合）。

ユーザーインターフェース：ホストアプリが実行されている間、**Android** の通知領域に表示されます。「サービス通知がクリック可能」機能は、ホストの通知をタップした際にホストアプリを起動するかどうかを制御します。この機能は、キオスクモードなど、ユーザーがホストアプリケーションを表示または操作できないようにしたい場合に特に便利です。

接続：様々な接続設定を管理できます。「キーブアラライブメッセージを送信」機能により、ホスト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、「複数の同時ゲストセッションを許可」設定が無効に設定されている場合は例外です。



5.3.2 ホスト名

ゲストユーザーがホスト端末を識別し接続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。

デフォルトでは、ホスト **ID** は端末 **ID** にランダムな番号を付加することで一意性を確保しています。

ホスト **ID** は、好みの任意の一意な **ID** に変更することが可能です。

また、ホスト ID として IMEI（IMEI が利用できない場合は端末のシリアル番号）を使用することも設定できます。あるいは、Bluetooth 名（Bluetooth 名が利用できない場合は端末 ID）を使用するように設定することも可能です。

以下の手順で「名前を入力」フィールドから、ホスト ID として使用する独自の値を自由に設定できます。「名前を入力」を選択し、使用したい名前を指定してください。

「ホスト名を入力」フィールドを使用することで、ホストにファイルからホスト ID を読み取らせることもできます。名前をファイルから

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」 %

「区切り文字」：列の区切り文字です。タブ文字の場合は'\t'、コロンの場合は'\:'、またはその他の表示可能な文字を指定できます。

「検索キー」：列0（最初の列）内で検索するテキスト文字列です。先頭のスペースは無視されます。

「値列」：値を読み込むべき列番号です。列は区切り文字で区切られています。値の前後にあるスペースは無視されます。

「ファイル名」：ANSIまたはASCIIテキストファイルです。ファイル名には完全なパスを指定できます。パスが指定されていない場合、ファイルはホスト実行ファイルと同じフォルダー内に配置されている必要があります。

「公開ホスト ID」のチェックボックスをオンにすると、このホストが myCloud のホスト一覧に表示されます。この一覧は、myCloud ドメインにログインしているゲストユーザーに表示されます。この設定をオフにした場合、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 を手動で入力する必要があります。

サードパーティ統合に関するヒント：API が利用可能です（実際のホスト ID を取得するための API については、セクション 8 の 8b を参照してください）。

5.3.3 デバイスを共有

「デバイスを共有」機能によって作成される招待リンクの動作に関する構成オプションです。

オプションには、リンクから許可される接続数の指定や、招待リンクの有効期限が切れた後に実行するアクションの定義などが含まれます（例えば、ゲストがリンクの有効期限切れと同時に接続を切断するように設定する場合など）。

また、リンクの有効期限が切れた際に自動的にホストをシャットダウンする（つまり受信接続を受け付けられない状態にする）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、いかなるゲストからも接続が不可能になります。（注意：これは、ホストを起動した際に自動的に受信接続を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。例えば、端末の再起動後にホストを起動した場合など）

5.4 セキュリティ

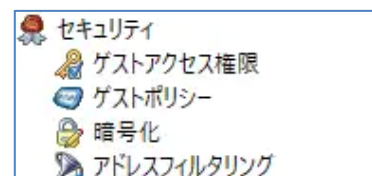
このセクションではホストのセキュリティ設定を管理します。以下の 4 つの項目で構成されており、それぞれの詳細は以下の通りです。

5.4.1 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内容を定義します。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。

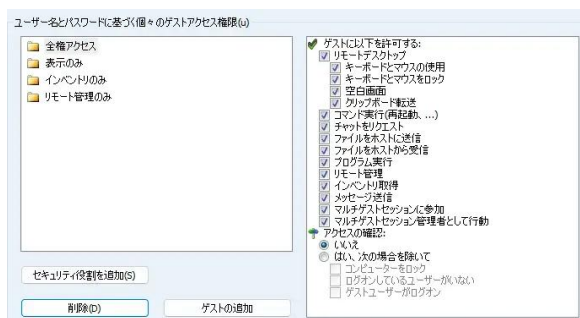
アクセス権限

認証済みゲストユーザーが実行できる操作内容は、ゲストユーザーに割り当てられたセキュリティロールによって制御されます。認証済みゲストユーザーが実行できる操作には、許可される場合と制限される場合がある様々なアクションが存在します。



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。**WiseMo** が定義したロールをカスタマイズするか、独自のセキュリティロールを定義することができます。

例えば、ファイルの送信・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する（キーボード/マウスによるタッチ入力の送信を許可しない）といった設定が可能です。図には利用可能な権限の一覧が表示されています。

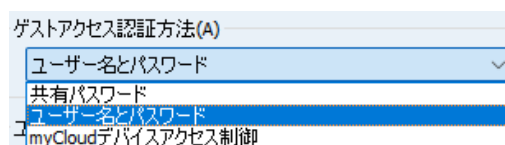


「アクセスの確認」機能を使用することで、通常認証済みのユーザーであっても、ホスト側の端末側でアクセス許可が与えられるまではアクセスできないようにすることができます（この機能は、有人監視下にあるホスト端末の場合にのみ使用してください）。

認証方法

利用可能な認証方法は以下の 3 種類です：

a. 共有パスワード：単一のパスワードでアクセスを保護します。左画面の「デフォルトユーザー」を選択してパスワードを設定し、「デフォルトセキュリティロール」を選択して権限（「アクセスの確認」機能を含む）を設定します。



b. 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。各ゲストユーザーには、この人物のセキュリティロール（権限設定を規定する役割）が設定されます。

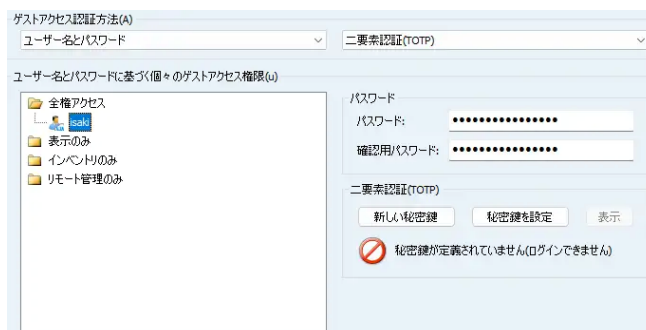
c. myCloud デバイスアクセス制御：myCloud を通じて、誰が（ゲストユーザー）、どのコンピューターや端末（ホスト）に対して、どのような（アクセス権限）操作を行えるかを一元管理および制御します。この方法を採用することで、ユーザーの入退が頻繁な環境においても、多数の端末のセキュリティ管理が容易になります。

二要素認証 (2FA)

二要素認証 (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 やその他の特定のコンピューター（アクセス権限を持つユーザーが 1 人または少数に限られるシステム）の保護に使用されます。

エンドポイントの 2FA 保護設定は、認証方式レベルで定義されます。これは、共有パスワード方式またはユーザー名とパスワード認証方式のいずれにも適用可能です。mDAC を使用する場合、2FA は myCloud ユーザーアカウントに対して中央集権的に定義されます。

アクセスを試みるゲストユーザーは、常に変化する検証コードを入力するか、アクセスが許可されない状態となります。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、例えば



Google Authenticator や Microsoft Authenticator アプリを使用して取得します。

ゲストユーザーを個別に定義した認証モードの場合、ゲストユーザーごとに独立した秘密鍵を設定することが可能です（非常にセキュリティレベルが高い設定です）。二要素認証 (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）。

5.4.2 ゲストポリシー

このセクションでは、許可されるパスワード試行回数の上限と、上限に達した場合の処理方法を設定できます。

パスワード	
無効なパスワードの最大試行回数:	3 (0 = 無制限)
最大試行回数を超えた場合のアクション:	切断
切断	3分間ログイン試行を禁止
切断後のアクション:	なし
非アクティブ時のタイムアウト	
ゲストからのアクティビティがない場合に切断:	0 分. (0 = タイムアウトなし)

5.4.3 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完全性機能を提供しています。構成オプションは「なし」から「非常に高い」まで選択可能です。

ホスト側の設定が最終的にどの暗号化方法が使用可能かを決定します。ゲストユーザーは自身の好みをリクエストでき、ホスト側の設定で許可されている場合、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、ホスト側では「高い」と「非常に高い」が許可されています。クラシックレベルは、特定の特殊モジュールとの互換性が必要な場合にのみ関係します。

各種類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。左側の画像は、「非常に高い」設定の説明を表示した例です。

ご自身が管理していないネットワーク（例：インターネット）に接続する場合は、常に強力な暗号化方式を使用する必要があります。**WiseMo** ゲストモジュール（**v.17** 以降）では、デフォルトで最高レベルの暗号化方式を採用しています。



5.4.4 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**を制限することが可能です。

これは範囲指定の形式で設定することもできます。許可されたゲストユーザーが静的 IP アドレスを使用している場合、あるいは特定の IP アドレス範囲から接続している場合に有効な対策です。myCloud 接続機能と併用しないでください。

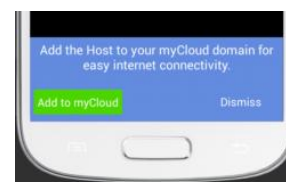
5.5 通信プロファイル

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。本プログラムは TCP/UDP 通信、HTTP 通信、および myCloud 接続機能をサポートしています。

TCP/IP プロファイルについては、例えばホストが使用する送信/受信ポート番号を変更することが可能です（デフォルトの送信/受信ポート番号：1970/1970）。

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ます。また、例えばホスト端末や企業のファイアウォールが HTTP 通信を許可していない場合、HTTPS に変更することも可能です。

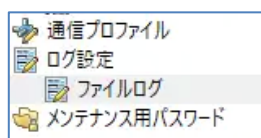
一般的に、myCloud 接続の設定にはウィザードの使用が推奨されます。この方式では、myCloud ユーザーアカウントの資格情報（メールアドレス+パスワード）を使用して、ホストを myCloud ドメインに認証します。



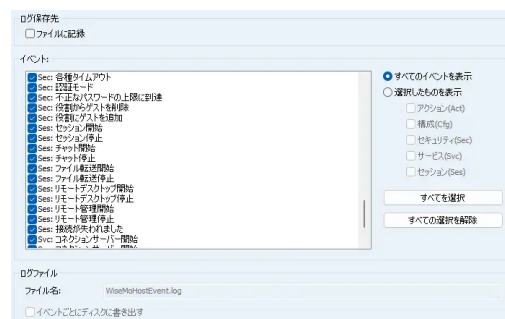
または、ホストアプリのインストール後に利用可能なオプション（myCloud 設定用）を使用できます。端末がまだ myCloud を使用できるように設定されていない場合に有効です。

5.6 ログ設定

ホストはホストに関連する活動およびホストへのアクセスに関する詳細なログ記録機能を提供します。



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が含まれます。ログ記録は端末上のローカルファイルに保存されます。



5.7 メンテナンス用パスワード

ユーザーインターフェースを介したホストアプリの設定変更を防止するため、設定をメンテナンス用パスワードで保護することができます。ユーザーが **WiseMo** ホスト設定にアクセスするには、このメンテナンス用パスワードを知って入力する必要があります。

6. Android ホストモジュールの更新または削除について

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可能です。

これにより、以下の場所にある既存の設定が保持されます：

`/storage/emulated/0/Android/data/com.wisemo.host.v10/files/WsmHost/`

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。

注意：myCloud 展開リンク（例えば SMS やメールなどで送信される場合）を介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使用され、端末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。

Android 端末から **WiseMo** ホストアプリケーションを削除する手順は、他のアプリを削除する場合と同様です。例えば「設定」→「アプリ」「アプリ一覧」からホストアプリを選択し、「アンインストール」をタップします。ホスト用のアドオンモジュールがインストールされている場合も、同じ手順に従ってください。ホストアプリのアンインストールでは、設定ファイルとライセンスファイルも削除されますのでご注意ください。

ヒント：アンインストールボタンがグレイアウトしている場合（特に古いバージョンの **Android** を搭載した **Samsung** 端末で発生する可能性があります）は、ホストアプリを起動し、メニューから「アンインストール」を選択してください。

ホストマネージャーの削除

Windows PC からホストマネージャーを削除するには、**Windows** のコントロールパネルにある「プログラムの追加と削除」/「プログラムと機能」を使用するか、インストール済みの **MSI** パッケージに含まれる「削除」機能を利用できます。

7. ホストプログラムのライセンス情報

バージョン 20 のホストプログラムは、以下の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)

このライセンスを使用するには、ホストモジュールを **myCloud** ドメインにログインさせる必要があります。そのため、コンピューター/端末はインターネット経由で通信可能な状態である必要があります。認証済みゲストユーザーはデフォルトで **myCloud** 接続機能を利用でき、さらにホストへの直接的な **TCP/IP** 接続も可能です。

インターネット経由でホストにアクセスする必要がある場合、またはゲストとホスト間の直接的な **TCP/IP** 接続に対してサブスクリプション型の課金モデルをご希望の場合には、**myCloud** ライセンスをご利用ください。

永続ライセンスキーを **myCloud** ライセンス対象のホストに適用すると、そのライセンス形態は永続ライセンスに切り替わります（詳細は以下をご覧ください）。

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。ゲストユーザーは **TCP/IP** 接続を利用してホストにアクセスできます。

TCP/IP 経由で直接ホストに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、永続ライセンスのご利用をお勧めします。

永続ライセンスを取得したホストは、**myCloud** ドメインにサインインすることで **myCloud** 接続機能を利用できます。この場合、**myCloud** ライセンスが消費されます。

試用版ライセンス

ホストが **Google Play** などの正規アプリストアからダウンロードされた場合、あるいは試用版ライセンスキーを提供した場合、ホストは永続ライセンスを取得した場合と同様に動作しますが、利用期間は限定されます（試用版ライセンスキーの発行は [こちら](#) から申請可能です）。

アプリストアからダウンロードしたホストが **myCloud** ドメインにサインインすると、ライセンス方式が **myCloud** ライセンス方式に切り替わります。

試用版ライセンスキーを入力した後、**myCloud** ライセンス方式に切り替えたい場合は、ホストを一度アンインストールしてから再インストールしてください。情報画面から「**myCloud** を設定」を選択するか、すでに **myCloud** ドメインにサインインしている場合は「**myCloud** ライセンスを使用」ボタンを押してください。

8. 上級ユーザー向け

本プログラムには、ゲストモジュール/サードパーティーアプリケーションから対象端末にアクセスする際の利便性向上や、大規模な展開を容易にするためのさまざまなオプション設定が含まれています。このような問題については、WiseMo までお気軽にお問い合わせください。例えば support@wisemo.com までメールでご連絡いただけます。

8a. ゲストコンピューターから端末にアクセスする

ステータス画面で表示される IP アドレスと固有のホスト ID は、ゲストユーザーがホストを識別し、使用する通信方法に応じてホストにアクセスするために使用できる重要な識別情報です。

デフォルトでは、ホスト ID は端末 ID に一意性を確保するためのランダムな番号を追加した形式となっています。

ホスト ID は、任意の一意な ID に変更することが可能です（ホストアプリのユーザーインターフェースから、または Windows PC 上のホストマネージャーを使用して設定できます）。ここでは、IMEI 番号（IMEI が利用できない場合は端末のシリアル番号）を使用するようにホスト ID を設定することもできます。また、Bluetooth 名（Bluetooth 名が利用できない場合は端末 ID）を使用するように設定することも可能です。

以下の表に、通信プロファイルの種類に応じて使用可能な ID の種類を示します。

ゲスト端末から Quick Connect 経由で、電話帳から、または myCloud リストからホストにアクセスする場合

Communication profile	IDs for Host addressing	Default value	Comment
TCP direct	IP address		
UDP direct	IP address		
UDP direct	Host ID	Device ID + number	Define your own Host ID, via Host Conf. Mng.
myCloud direct	Host ID	Device ID + number	Define your own Host ID, via Host Conf. Mng.
myCloud, from list	Host ID	Device ID + number	Define your own Host ID, via Host Conf. Mng.
myCloud, from list	User name	Bluetooth name	If no Bluetooth name, the Device ID will be shown



注記： Bluetooth 名は通常、端末の設定メニューから変更できます。

8b. サードパーティーAPI

サードパーティ製 Android アプリケーション（MDM ソリューションなど）で使用するための API が用意されており、サードパーティーアプリケーションがホストに問い合わせを行ったり、設定を変更したり、コマンドを発行したりしてホストを停止・起動・再起動することが可能です。この API は Android AIDL ベースのサービスとして実装されています。この API に関する詳細情報については、support@tos.co.jp までお問い合わせください。

8c. 高度な設定

高度なホストのインストールと設定に関する詳細な説明については、この[ガイド](#)を参照してください。

特定の動作を制御するための「オプション」フラグを定義することが可能です。これらの「オプション」フラグは、フラグ名と同じ名前の空のファイルを作成し、それをホスト構成フォルダー/WsmHost に配置することで設定します。オプションフラグは大文字小文字を区別し、ファイル名は小文字で指定する必要があります。

opt.no-device-admin	Samsung 製端末において、端末管理者権限に関するユーザー入力要求を抑制します。
opt.no-rcbridge-ui	ホスト追加モジュールのインストール時に発生するユーザー入力要求を抑制します。

8d. 導入方法

ライセンスと設定を適用した端末を準備し、ホストの起動時に可能な限り少ないユーザーインターフェース操作で起動させたい場合、この手法をご検討ください。

- 以下のフォルダーを作成してください：
/storage/emulated/0/Android/data/com.wisemo.host.v10/files/WsmHost/
- ライセンスファイル（host.lic）をこのフォルダー内に配置します。

3. 設定ファイル (host.xml) をこのフォルダー内に配置します。
4. ホストアプリケーションを起動すると、ライセンスと設定を自動的に検出するため、ユーザーによる入力是不要です。

高度なホストインストールについては、この[ガイド](#)もご参照ください（開発元のドキュメントになります）。

8e. Microsoft Intune および Google Android の管理設定

Intune および Android 管理構成でホストを使用する方法についての詳細情報は、[こちら](#)をご覧ください（開発元のドキュメントになります）。

9. 用語集

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サーバー、ワークステーション、デスクトップ、またはラップトップを指します。

端末 – 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または非操作型端末を指します。

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）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あらゆる種類の端末が該当します。

ホストマネージャー – 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。Windows デスクトップコンピューターにインストールされ、ホストの設定情報が格納された host.xml ファイルを作成・編集することができます。また、通信機能を備えており、端末が PC に USB 接続されている場合、端末上の host.xml ファイルとの通信が可能です。

スキン – 端末のリモート制御用グラフィカルユーザーインターフェースです。通常、実際にリモート制御する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仕組みです。

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するプロトコル設定です。主な通信方式は 2 種類あります：TCP/IP 方式と myCloud 方式です。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、ファイアウォールやプロキシ、NAT (Network Address Translation) 環境を通過可能なインターネットベースのプロトコルです。WiseMo myCloud の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リモートコントロール接続を容易にします。