

WiseMo ファイアウォール構成ガイド

目次

概要	2
WiseMo myCloud 概要	2
WiseMo myCloud 接続のためのファイアウォール設定	3
接続プロトコル	3
コネクションマネージャー	3
コネクションサーバー	4
スキンサーバー	4
ポート 80、443、および 1970 のアウトバウンド（送信）接続の許可	4
必要なポートの最適化	4
特定の IP アドレスに対するポート 80、443、および 1970 のアウトバウンド（送信）接続の許可	5
コネクションマネージャー	6
コネクションサーバー	6
スキンサーバー	6
IP アドレス	6
ファイアウォール設定に関する追加情報	7
LAN 接続のためのファイアウォール設定	8
ゲストおよびホストアプリケーションへのインバウンドトラフィックの許可	8
特定ポートの開放	9
ゲストアプリケーションからのアウトバウンド接続の許可	9
モバイルデバイスのリモートコントロールにおける「スキン」の利用	9
myCloud サブスクリプションによるライセンス認証の利用	10
myCloud デバイスアクセス制御（Device Access Control）サービスの利用	10
外部ファイアウォールの通過（VPN 環境など）	10

概要

WiseMo リモートコントロールは、LAN 内でのローカル接続だけでなく、WiseMo myCloud を利用したインターネット経由の接続にも対応しています。

本ドキュメントでは、LAN 接続におけるファイアウォールの設定（「LAN 接続のためのファイアウォール設定」の項を参照）、および myCloud を使用したインターネット経由の接続における設定について説明します。

WiseMo myCloud 概要

WiseMo ゲストおよびホストアプリケーションは、myCloud を介してインターネット上でリモートコントロール接続を確立・ルーティングするために、WiseMo myCloud インフラストラクチャへのアクセスを必要とします。

WiseMo myCloud は、特別なファイアウォール設定を必要とせず、簡単に接続できるよう設計されています。WiseMo のゲストおよびホストはアウトバウンド（送信）接続のみを行うため、通常、ファイアウォールによってブロックされることはありません。

ただし、企業ネットワークなどセキュリティポリシーが厳格な環境では、未承認のアウトバウンド通信がすべてブロックされる場合があります。そのようなケースでは、WiseMo myCloud への接続を許可するようにファイアウォールを設定する必要があります。

myCloud のインフラストラクチャは、インターネット上にある 2 つの主要なサーバーコンポーネントで構成されています。

1. コネクションマネージャー

認証処理を行い、ゲストとホストの接続ごとに最適なコネクションサーバーを割り当てます。

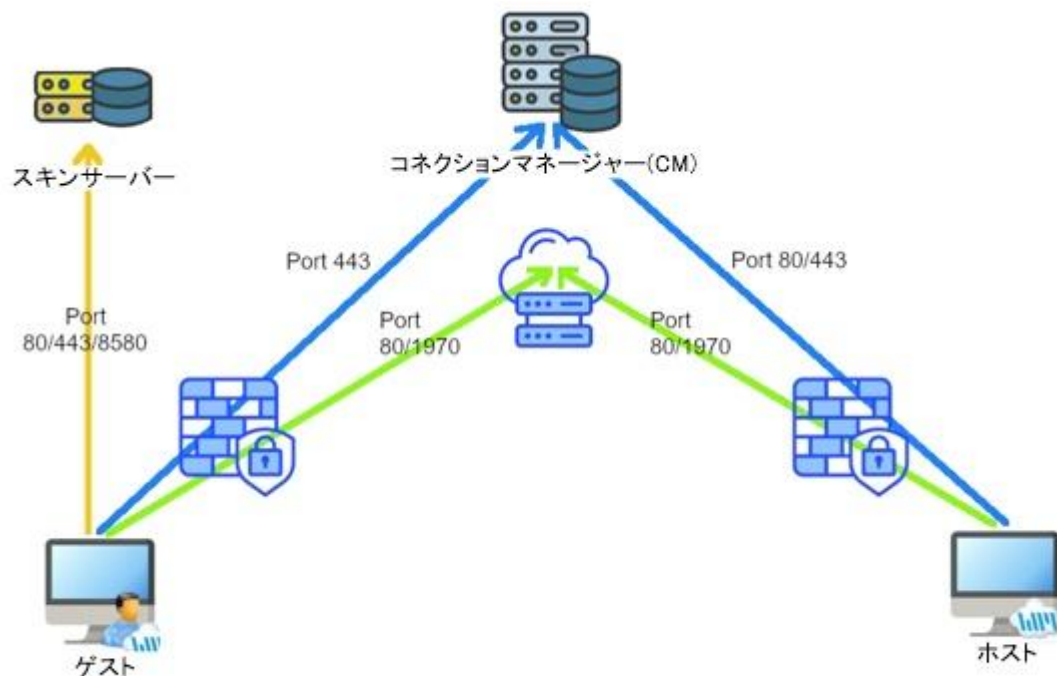
2. コネクションサーバー

認証された接続のみが確立されるよう保証しつつ、エンドツーエンドの暗号化接続を仲介します。これらのサーバーは、効率的なルーティングを実現するために世界各地に分散配置されています。

また、補助サーバーとしてスキンサーバーが存在します。

3. スキンサーバー

モバイルデバイスのリモートコントロール時に使用されるデバイス画像のリポジトリです。遠隔操作する側の画面上に、実際のホストデバイスの外観イメージを重ねて表示するために使用されます。



WiseMo myCloud 接続のためのファイアウォール設定

ファイアウォールの設定が必要な場合、次のステップとして、WiseMo 用のポートを特定の IP アドレスに対して設定する必要があるか、あるいはアウトバウンド（送信）ポート全般を許可するだけで十分かを確認します。

接続プロトコル

WiseMo サーバーへのすべての接続の基盤となるプロトコルは TCP です。

コネクションマネージャー

コネクションマネージャーへの接続は、設定、モジュール、および実行するタスクに応じて、HTTP または HTTPS が使用されます。

- ゲスト：常に HTTPS を使用します。
- ホスト：myCloud への常時接続確認（プレゼンス・ポーリング）には HTTP を使用し、セキュリティ関連のタスクには HTTPS を使用します。なお、ホストの設定を常に HTTPS を使用するように変更することも可能です（詳細は後述します）。

コネクションサーバー

コネクションサーバーへの接続には TCP が使用されますが、必要に応じて通信が HTTP 内にカプセル化される場合があります。送信される実際のデータは、デフォルトで AES 暗号化によるエンドツーエンドの暗号化が施されています。

スキンサーバー

スキンサーバーへの接続には、HTTP プロトコルの拡張機能である WebDAV（Web Distributed Authoring and Versioning）が使用されます。

ポート 80、443、および 1970 のアウトバウンド（送信）接続の許可

ファイアウォールの最も簡単な設定は、すべてのアプリ、または WiseMo ゲストアプリとホストアプリに対して、ポート 80、443、および 1970 でのアウトバウンド接続を全般的に許可することです。

Windows の場合、各アプリのデフォルトのフルパスとファイル名は以下の通りです。

- ゲストアプリ: C:\Program Files (x86)\WiseMo\WiseMo RSM\Remote Desktop Guest\WsmGuest.exe
- ホストアプリ: C:\Program Files (x86)\WiseMo\WiseMo RSM\Remote Desktop Host\WsmHostSvc.exe

必要なポートの最適化

ゲスト¹で必要となるのは、ポート 443 と 1970 へのアクセスのみです。Windows ゲストにおけるスキンリポジトリの設定は、デフォルトでポート 80²を使用するように構成されています場合がありますが、ゲストアプリの「構成」>「セッション」>「スキン」からポート 443 へ変更することが可能です。

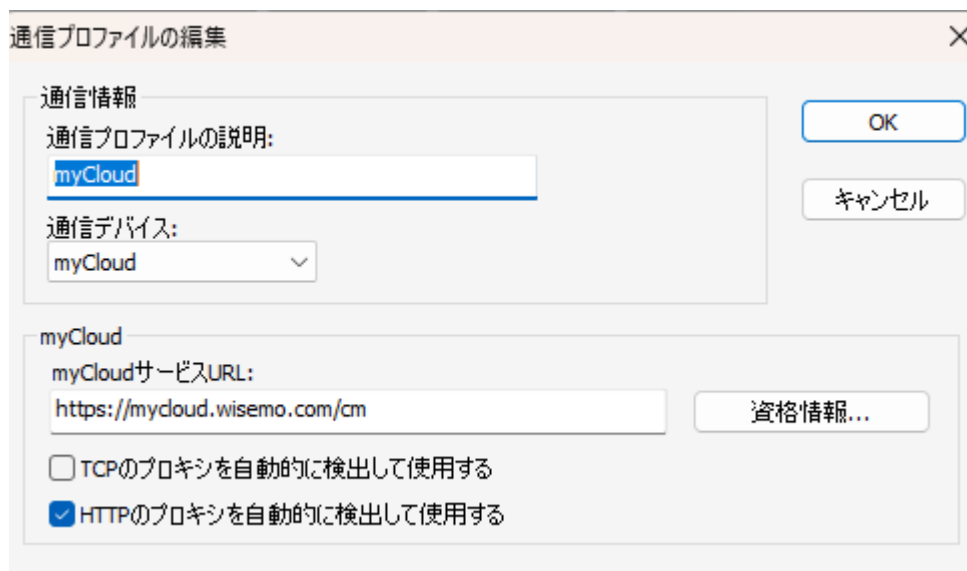


¹ ゲストバージョン 20 以降（すべてのビルド）。

² ゲストバージョン 20 ビルド 2025016 以降では、デフォルトでポート 443 を使用します。

Windows の場合、ホストがポート 80 の代わりに HTTPS（ポート 443）を使用するように設定を変更できます。

設定は「構成」>「通信プロファイル」>「myCloud」から行えます。画面内の「myCloud サービス URL」³の項目にある「http」を「https」に書き換えてください。



また、「myCloud サービス URL」に以下を指定することで、コネクションサーバーとの接続と同じポート 1970 を使用することも可能です。

`http://mycloud.wisemo.com:1970/cm`

これらの変更は、Windows 以外の OS でも、設定ファイルである **Host.xml** を直接編集することで同様に行うことができます。

特定の IP アドレスに対するポート 80、443、および 1970 のアウトバウンド（送信）接続の許可

この項目は WiseMo myCloud サービスが使用している IP アドレスを特定する必要がある場合の、より高度なファイアウォール設定を行うケースとなります。

³ ホストバージョン 20 ビルド 2025185 以降でサポートされます。

コネクションマネージャー

コネクションマネージャーは複数のロードバランサーの背後に配置されているため、ポート 80 および 443 に対して、すべてのロードバランサーの IP アドレスを追加する必要があります。なお、HTTPS への切り替えなどゲストおよびホストのポート番号に関する前述の注意点は、ここでも同様に適用されます。

具体的な IP アドレスについては、後述の「IP アドレス」の項を参照してください。

コネクションサーバー

コネクションサーバーは、ゲストおよびホストモジュールからの地理的な近さに加え、その地域内にある各コネクションサーバーの負荷状況に基づいて、接続ごとに動的に割り当てられます。そのため、接続のたびにコネクションサーバーの IP アドレスが異なる場合があります。

なお、コネクションサーバーを介した最初の接続試行はポート 1970 で行われ、それが失敗した場合にポート 80 での接続が試みられます。

接続がポート 80 (HTTP) のみに制限されている環境では、設定に合わせて myCloud を適切に構成することをお勧めします。

myCloud にアクセスして、以下のメニューから変更できます。

「設定」>「接続」>「優先接続プロトコル」

優先接続プロトコル

ネットワークからのアウトバウンドTCP接続が何らかの理由で制限されている場合、優先接続プロトコルとしてHTTPを設定すると、ドメイン内のホストへの接続を確立するために必要な時間を改善できます。

優先接続プロトコル:

WiseMo コネクションサーバーの IP アドレスのプールについては、後述の「IP アドレス」の項を参照してください。

スキンサーバー

スキンサーバーはデフォルトでポート 443 を使用しますが、ポート 80 およびポート 8580 経由でもアクセス可能です。

IP アドレス

WiseMo myCloud サービスが使用する IP アドレスは安定していますが、特にコネクションサーバーに関しては、時折追加されたり、稀に削除されたりすることがあります。

新しいコネクションサーバーが追加された場合、リモートコントロールの接続先としてその新しいサーバーが割り当てられる可能性があるため、その IP アドレスを許可リストへ追加する必要があります。追加されていない場合、ファイアウォールによって接続が拒否される可能性があります。

現在使用されている **WiseMo myCloud** の IP アドレス、およびそれらの保証された有効期間は、以下の通り **DNS ルックアップ** を実行することで取得できます。

サーバー	プロトコル	ポート	DNS ルックアップ名	有効日数
コネクションマネージャー	TCP	80 or 443	mycloudall.wisemo.com	30
コネクションサーバー	TCP	80 or 1970	csall.wisemo.com	7
スキンサーバー	TCP	80, 443 or 8580	skinsall.wisemo.com	30

具体例として、すべてのコネクションサーバーにて使用されている IP アドレスを調べるには、各 OS で以下のコマンドを実行します。

Windows の場合： コマンドプロンプトを開き、以下のコマンドを入力します。

```
nslookup csall.wisemo.com
```

Linux、**macOS**、**Android**、またはその他の **UNIX** 系 OS の場合： ターミナルウィンドウを開き、以下のコマンドを入力します。

```
host csall.wisemo.com
```

コマンドの実行によって返された IP アドレスの一覧は、コマンドを実行してから少なくとも 7 日間は有効です。可能であれば、この **DNS ルックアップ** を自動的に行うファイアウォール機能の利用を推奨します。自動化できない場合は、**30** 日ごと（コネクションサーバーのリストについては **7** 日ごと）に手動でルックアップを再実行し、ファイアウォールを再設定する必要があります。

なお、上記のコマンドを実行すると、リストの取得に使用した **DNS** サーバーの IP アドレスが表示されることもありますが、それらはリストの一部ではありません。

ファイアウォール設定に関する追加情報

WiseMo 製品が使用する可能性のあるポート（ポート **80**、**443**、**1970** など）へのアクセスをブロックまたは制限する場合は、ファイアウォールの設定で送信（アウトバウンド）パケットを警告なしに破棄（**Drop**）するのではなく、明示的に拒否（**Reject**）するように設定してください。

これにより、**WiseMo** 製品やネットワーク内のその他のプログラムは、ユーザーにエラーを通知したり適切な代替動作を行ったりすることで、ポリシーによる制限をより効率的に処理でき

るようになります。受信パケットを何も通知せずにドロップすることは、悪意のある攻撃者や外部からのポートスキャンを阻止するのに有効ですが、送信パケットを何も通知せずにドロップすることは、内部のコンピューターやユーザーのパフォーマンスを著しく低下させます。

ネットワーク内の **Web** ブラウザに対して検査システム専用の **CA** 証明書を信頼させる必要がある「**HTTPS** 検査」システムを使用している場合は、**WiseMo** ホストプログラムを実行しているマシンを含め、内部マシンのシステム **CA** 信頼ストアにその **CA** 証明書が導入されていることを確認してください。**Windows** マシンの場合は、グループポリシーの「ユーザー」の構成ではなく、「コンピューター」の構成を使用してください。同様に、スタンドアロンの **Windows** マシンの場合は、「信頼されたルート証明機関」の「ローカル コンピューター」証明書ストアに証明書をインポートします。信頼の設定をユーザーごとの設定にしか適用しない場合、**WiseMo** ホストのようにユーザーのログイン状態とは無関係に動作するシステム全体のサービスには対応できません。

LAN 接続のためのファイアウォール設定

LAN（ローカルエリアネットワーク）環境では、ゲストは **IP** アドレスまたは **DNS** 名を使用してホストに接続します。この接続には、**TCP**、**UDP**、または **HTTP**（**TCP** の派生）を使用できます。

TCP 接続の場合

ゲストからホストに対してアウトバウンド（送信）接続を開始し、ホスト側でインバウンド（受信）接続を受け取ります。ローカルファイアウォール（アプリケーションと同じコンピューターやデバイス上にあるファイアウォール）がアウトバウンドトラフィックをブロックすることはめったにないため、ほとんどの場合、ホストのファイアウォールでインバウンド **TCP** 接続を許可するだけで設定は完了します。

UDP 接続の場合

UDP はセッションベースではないため、動作が異なります。**UDP** は持続的な接続を確立することなく、個別のデータグラムを送信します。ファイアウォールは、最近送信されたデータグラムのアドレスと一致する場合に受信 **UDP** データグラムを許可することがありますが、この動作が保証されているわけではありません。通信を開始するのは常にゲスト側ですが、実際には、ホストとゲストの両方のファイアウォールで受信 **UDP** トラフィックを許可する設定が必要になることが多くあります。

ゲストおよびホストアプリケーションへのインバウンドトラフィックの許可

Windows 版のゲストアプリおよびホストアプリのインストール中、セットアッププログラムは **Windows** の機能を自動的に使用してローカルファイアウォールを調整します。ゲストアプリのインストールでは、ゲストアプリに対するすべての **UDP** ポートの受信トラフィックが許可されます。一方、ホストアプリのインストールでは、ホストアプリに対するすべての **UDP** ポートお

よび TCP ポートの受信トラフィックが許可されます（2 つのルールとして追加されます）。
Windows を使用していない場合は、ファイアウォールで同様の設定を手動で行う必要がある場合があります。

特定ポートの開放

デフォルトでは、ゲストアプリケーションはポート 1970（TCP または UDP）を使用してホストへの LAN 接続を確立します。このポートへのインバウンドトラフィック（受信トラフィック）のみを許可することで、セキュリティを強化できます。

なお、ゲストおよびホストは他のポートを使用するように設定することも可能です。その場合は、設定に合わせてファイアウォールも変更する必要があります。たとえば、ホスト上で HTTP 通信プロファイルを有効にする場合、ファイアウォールでポート 80 へのインバウンドトラフィックを許可してください。

ゲストアプリケーションからのアウトバウンド接続の許可

セキュリティポリシーが厳しい環境では、ゲストアプリケーションの送信トラフィックを明示的に設定しなければならない場合があります。デフォルトでは、UDP と TCP の両方でポート 1970 のアウトバウンド接続を許可する必要があります。通信が UDP または TCP のいずれか一方に限定されている場合は、ファイアウォールは使用するプロトコルのみの許可で十分です。

ゲストとホストがデフォルト以外のポートを使用するように設定されている場合、ゲストのファイアウォールはそれらの特定のポートでのアウトバウンド接続を許可する必要があります。たとえば、デフォルト設定の代わりに HTTP プロトコルを使用する場合は、ゲストのファイアウォールでポート 80 のアウトバウンド接続を許可する必要があります。

モバイルデバイスのリモートコントロールにおける「スキン」の利用

スキンサーバーは、実機のホストデバイスの画像内にリモートコントロール画面を表示するために、モバイルデバイスのリモートコントロールで使用するデバイス画像のリポジトリです。

スキンサーバーはデフォルトでポート 443 を使用しますが、ポート 80 および 8580 経由でもアクセス可能です。スキンサーバーへのアクセスについては、前述の「WiseMo myCloud 接続のためのファイアウォール設定」該当段落を参照してください。

myCloud サブスクリプションによるライセンス認証の利用

myCloud サブスクリプション経由で WiseMo ゲストおよびホストのライセンスを取得する場合、myCloud を使用するときと同様に、ゲストおよびホストからコネクションマネージャーへアクセスできる必要があります。その場合は、「WiseMo myCloud 接続のためのファイアウォール設定」にあるコネクションマネージャーの設定に関する該当段落を参照してください。

myCloud デバイスアクセス制御（Device Access Control）サービスの利用

WiseMo ホストを集中管理型の myCloud デバイスアクセス制御サービスを利用するように構成する場合、ゲストおよびホストは、通常の myCloud 接続時と同様にコネクションマネージャーへのアクセスが必要となります。

この機能を使用する場合は、前述の「WiseMo myCloud 接続のためのファイアウォール設定」内にあるコネクションマネージャーの構成に関するセクションを参照してください。

外部ファイアウォールの通過（VPN 環境など）

VPN 環境など、接続が外部ファイアウォールを通過する場合があります。その場合は、ポート 1970 を直接解放するか、または各ファイアウォールの背後にあるホストのポート 1970 に対して、任意のポート番号からファイアウォールのポート転送を設定する必要があります。別のポートを使用するように設定している場合（デフォルト以外の HTTP 通信プロトコルを使用してポート 80 を利用している場合など）も同様です。