フィルタリングとクライアントポリシーガイド

19.3

Parallels International GmbH
Vordergasse 59
8200 Schaffhausen
スイス
Tel: + 41 52 672 20 30
www.parallels.com/jp

目次

はじめに

本ガイドの目的

本ガイドは、Parallels® Remote Application Server (以降 RAS) の評価を目的に、初めて環境を構築されようとしているお客様や、販売店のエンジニア様に、シンプルなシステム構成で構築を完了し、RAS のリモート アクセスをお試しいただき体験いただくことを目的としております。

RAS 管理者ガイド (日本語) を、弊社 Web サイトに公開しておりますが、公開資料を補足する内容となっております。ぜひ、RAS 製品のシンプルで、かつ操作性の良いリモート アクセスを評価いただければ幸いです。

RAS 管理者ガイドを含むマニュアルの公開ページ
https://www.parallels.com/jp/products/ras/resources/

注意事項

- 本ガイドで紹介した仮想ネットワークおよび仮想サーバー等の導入に関しては自己責任での利用をお願いいたします。
- 本ガイドで示す環境構築および運用手順の実行に関しては、所属する組織等のセキュリティポリシーに必ず従ってください。
- 本ガイドに記載されている画面例、URL 等はガイド記載時のものとなるため、画面仕様が実際の画面とは異なることがありますのでご注意ください。
- 本ガイドに記載されている内容は、改善のため予告なしに変更される場合があります。あらかじめご了承下さい。
- 評価の際は、是非、インストール メディアのバージョンを含め、本ガイドの最新バージョンをご使用されることを推奨いたします。

適用範囲

本ガイドは、以下バージョンを対象としています。

- RAS Ver. 19.3

表記規則

本ガイド内の表記は、以下の規則に沿って行われています。

- RAS の画面に表示されるメニュー名/タブ名/プロパティ項目名/値/ボタン名は、[ ] で囲んで表記しています。
- 可変の値は < > で囲んで表記しています。

概要

本ガイドでは、RAS を使用してフィルタリングとクライアント ポリシーを構成する方法について説明します。

RAS では、フィルタリングとクライアント ポリシーを利用して、公開済みのリソースに対するユーザーの操作を一元管理することができます。また、特定のパラメータを満たしたユーザーだけがリソースにアクセスできるようにすることで、セキュリティを強化します。

この章の内容

フィルタリング

フィルタリング (制限) 機能を利用することで、公開済みのリソースに対するユーザーの接続可否を制御できます。フィルタリングの条件は、ユーザーおよびユーザー グループによる利用許可の定義以外に、複数の条件を組み合わせることも可能です。

一般的には、ユーザーやユーザー グループを条件にアクセスを定義することがほとんどですが、運用の要件に応じて、よりセキュリティを高めたい場合や、接続を制限させたい場合などに、RAS Connection Broker サーバー側で、Parallels RAS Client を参照し、アクセス条件を識別させて、接続を制御できます。

例えば、デバイスの OS 種別、デバイスの MAC アドレスなどを識別し、リモート接続を制御することができますので、指定の PC デバイスを特定するなどが可能です。

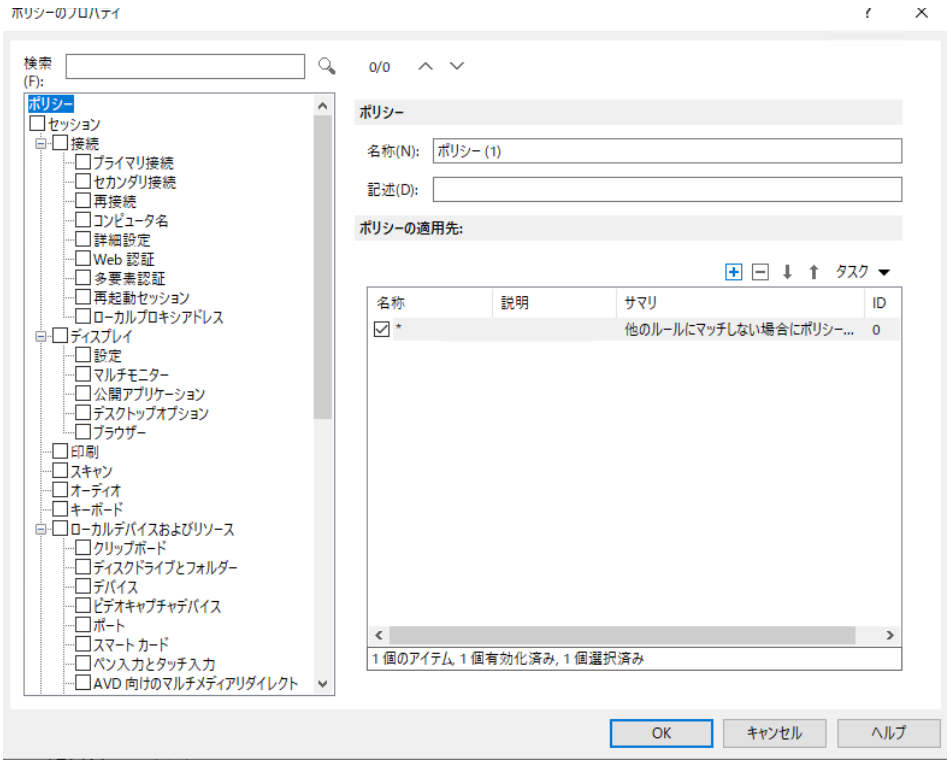
フィルタリング条件の詳細な情報は、管理者ガイド「フィルタールールの使用」をご参照ください。

クライアント ポリシー

RAS では、機密データへの安全なアクセスを確保するために、様々なクライアント ポリシーを設定することができます。クライアント ポリシー機能を利用すると、Parallels Client でユーザーが利用できる接続オプションを RAS Console 上で集中的に管理することができます。

代表的な利用形態として、機密データの外部漏洩や不正プログラムの内部侵入を防止する目的で、クライアント マシンの内蔵ディスクや、外部記憶装置などの認識を無効化する事例があります。

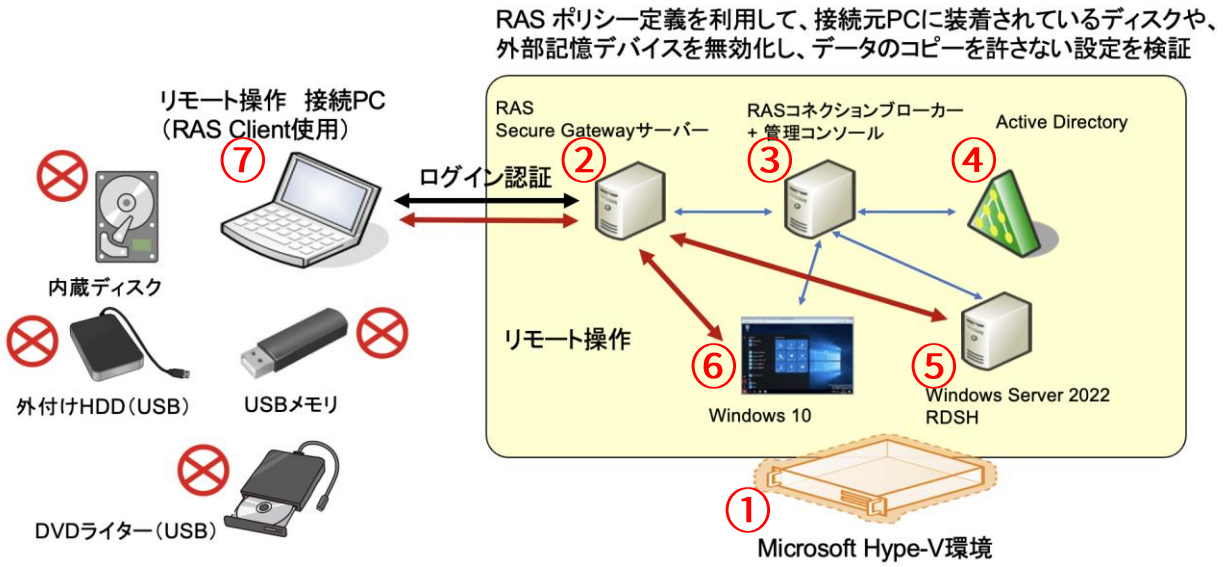
クライアント ポリシーの詳細な情報は、管理者ガイド「クライアント ポリシー」をご参照ください。



検証環境の構成

本ガイドであつかう検証環境について説明します。検証環境を構成するコンポーネントのうち、サーバー側のコンポーネント (②～⑥) につきましては 1 台の物理マシン (①) 上に構築します。クライアント側のコンポーネント (⑦) は、Windows OS の物理マシンを使用します。

物理サーバーとして構成した Hyper-V 上に、管理サーバーおよび VM を構築した場合の構成イメージを以下に示します。



構成イメージにおける各コンポーネントの概要を以下に示します。

項番	マシン	役割	OS
1	Hyper-V	仮想基盤 (ハイパーバイザー) ベースのプロバイダー。	Windows Server 2022
2	RAS Secure Gateway	RAS 環境へのログオン入り口。	Windows Server 2022
3	RAS Connection Broker 兼 RAS Console	RAS 環境への接続誘導、設定の保持。	Windows Server 2022
4	Active Directory	ユーザー認証。マシン登録。	Windows Server 2022
5	RDSH 用マシン	RDSH 環境を提供するための仮想マシン。	Windows Server 2022
6	VDI 用マシン	VDI 環境を提供するための仮想マシン。	Windows 10
7	クライアント マシン	ユーザーが Parallels Client を使用し、VDI にリモート接続するための物理マシン。	Windows 10*1

*1:本ガイドでは、Windows マシンを使用していますが、任意の OS を利用可能です。詳細は管理者ガイド「ソフトウェア要件」をご参照ください。

構築手順

この章では、公開リソースのフィルタリングの設定とクライアントポリシーの設定する手順を紹介します。

この章の内容

公開リソースのフィルタリング

RAS では、ユーザーへリモート アクセスを許可する [公開] 定義を設定する際に、様々なフィルタリング (制限) を設定することができます。

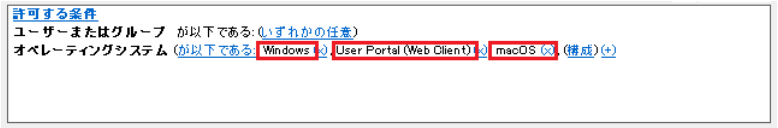
フィルタリング ルールを使用すると、特定の公開済みのリソースにどのユーザーがアクセスできるかを制御できます。各ルールは、ユーザー接続に対するマッチングに使用される 1 つまたは複数の条件で構成されています。各条件は、マッチング可能な 1 つまたは複数の特定のオブジェクトで構成されています。

注意点

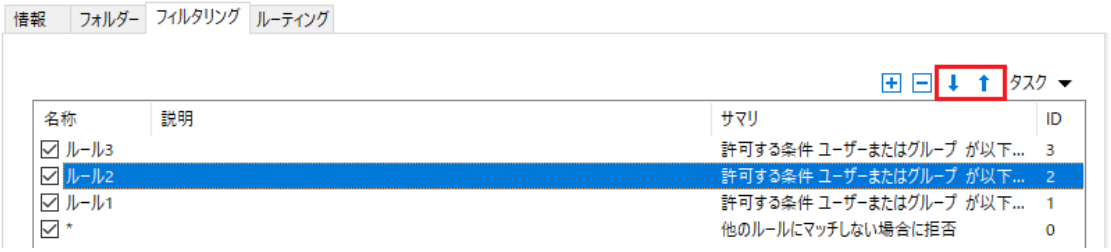
ルールについて、以下の項目に注意してください。

- **条件は AND 演算子で連結される**:例えば、あるルールに、「特定のユーザーに一致」と「特定のクライアント デバイスのオペレーティング システムに一致」という条件が含まれる場合、ユーザーの接続が条件の両方に一致する場合に、ルールが適用されます。

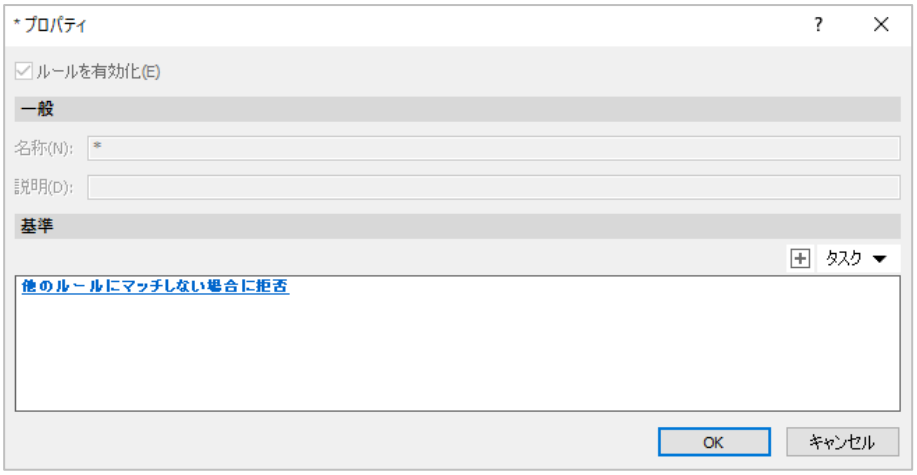
- **オブジェクトは OR 演算子で接続される** : 例えば、あるルールに、「クライアント デバイスのオペレーティング システム」に一致という条件のみを作成した場合、いずれかのオペレーティング システムがクライアント接続に一致すれば、ルールが適用されます。



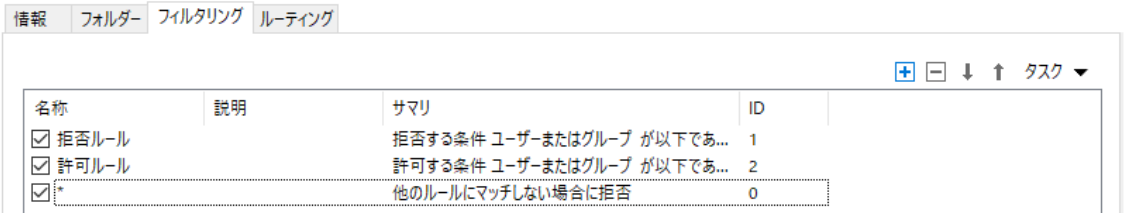
- **ルールの優先順位は昇順**：ルールは、上から順にユーザー接続と比較されます。ユーザー接続に一致する最初のルールが適用されます。優先順位を変更する際は、[↑ (上矢印)] または [↓ (下矢印)]ボタンをクリックして、リスト内のルールを移動します。



- **いずれのルールにも一致しない場合には、既定値のルールが使用される**：既定値のルールは、[他のルールに一致しない場合に許可] または [他のルールに一致しない場合に拒否] のいずれかに設定できますが、条件を利用することはできません。



- **“拒否” は “許可” よりも優先順位が高い**：“拒否” は “許可” よりも優先順位が高いため、リスト上で “許可” ルールよりも上位に配置する必要があります。



フィルタリング ルールの追加

新たにルールを追加する手順は以下の通りです。

1 RAS Consol の左ペインから [公開] を選択し、[公開済みのリソース] ツリーの下にある公開リソースまたはフォルダをクリックします。

2 [フィルタリング] タブを選択し、[+] ボタン (または [タスク] > [追加]) をクリックします。

3 [新しいルールのプロパティ] ウィンドウが表示されます。[名称] 枠にルール名を入力します。

4 [+] ボタン (または [タスク])をクリックし、ルールの条件を選択します。

以下の条件を選択することができます。

名称	説明
ユーザーまたはグループ	ユーザー、グループ、またはコンピューターの SID。
Gateway	ユーザーが接続する RAS Secure Gateway。
テーマ	Parallels Web Client 用の定義済みテーマ。
クライアントデバイス名	クライアント デバイスの名前。
クライアント デバイスのオペレーティング システム	クライアント デバイスのオペレーティング システム (OS)。 **注**: OS 種別は、詳細なバージョンは指定できません。例えば、Windows の場合、Windows 7、Windows 10、Windows 11 などの識別はできません。他の OS も同様です。
IP アドレス	クライアント デバイスの IP アドレス。
ハードウェア	クライアント デバイスのハードウェア ID (MAC アドレス)。

5 以下のコントロールを利用できます。

名称	説明
許可 / 拒否	ユーザー接続がすべての条件に一致した場合に、リソースへのアクセスが許可されるか、リソースへのアクセスが拒否されるか指定することができます。
が以下でない / が以下である	ユーザー接続が条件に一致した場合に、リソースをアクセス可能にするかどうかを指定します。
(×)	オブジェクトの削除。
(構成)	オブジェクトのリストを編集。
(+)	新しい条件の追加。

クライアント ポリシーの構成

RAS のクライアント ポリシー機能を利用することで、ユーザーの操作を制限することができます。

クライアント ポリシーの追加

クライアント ポリシーを追加する手順は以下の通りです。

1 RAS Console を起動し、[ポリシー] に遷移します。[ポリシー] タブで [+] ボタン (または [タスク] > [追加]) をクリックします。

2 「ポリシーのプロパティ」ウィンドウが表示されます。追加するポリシーの [名前] を入力します。

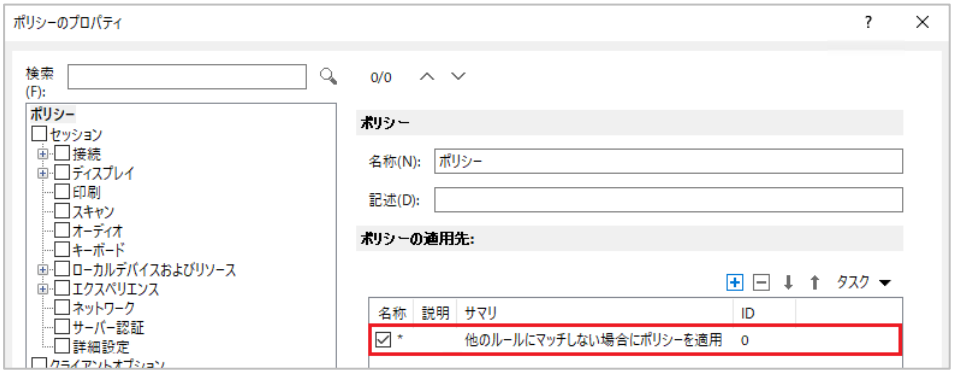
名称	説明
名前*	新しいポリシーの名前
記述	任意の説明

3 [ポリシーの適用先] セクションで、ポリシーの適用範囲を定義するフィルタリング ルールを設定できます。

フィルタリング ルールを追加しない場合 (既定値) は、既定のルール [*] が [他のルールにマッチしない場合にポリシーを適用] であることを確認します。

フィルタリング ルールを追加する場合は、「クライアント ポリシーのフィルタリングルールの追加 (p. 14) 」をご参照ください。

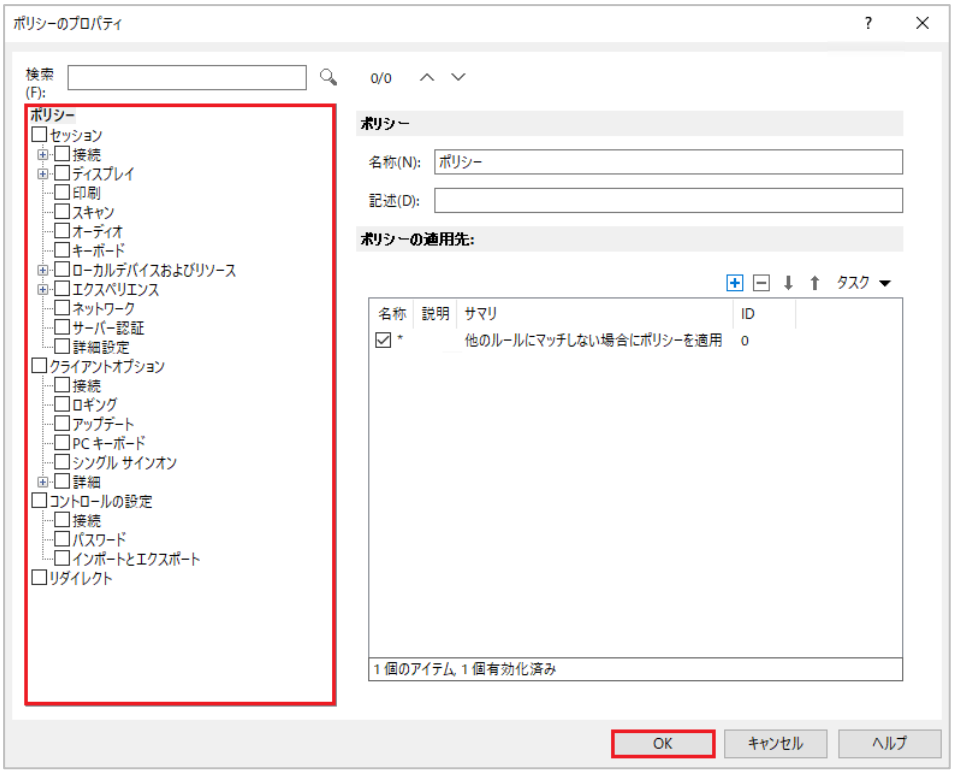
注 : 既定値では、すべてのユーザーに対して定義されたポリシーが適用されます。



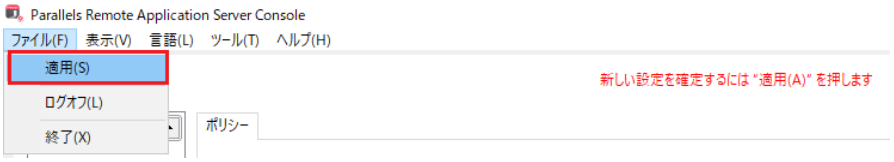
4 左ペインに含まれるナビゲーション ツリーを使用して、構成するオプションを選択できます。

注 : 既定値では、多くのカテゴリーがチェック済みであることに注意してください。不要な項目は、チェックを外して無効化してください。

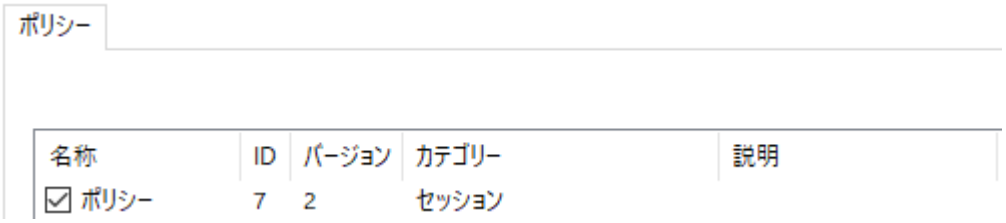
オプションの設定後、[OK] をクリックし、ウィンドウを閉じます。



5 RAS Console 上部メニューから [ファイル] > [適用] の順にクリックし、設定を保存します。



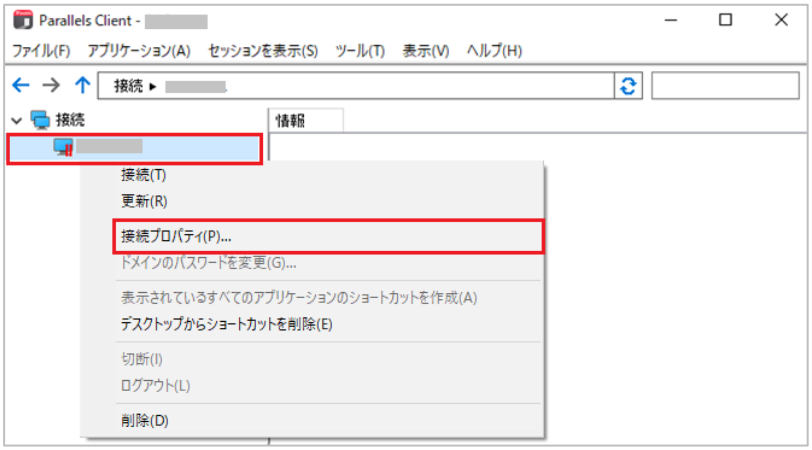
6 ポリシーが適用されていることを確認します。ポリシーの [ID] と[バージョン] を確認してください。



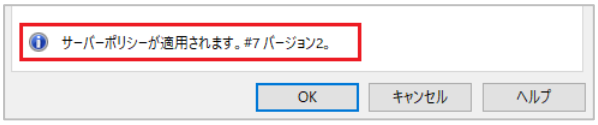
7 以降の操作はクライアント マシンにて実施します。Parallels Client を起動し、ログオンします。

注 : ポリシーは、次回のユーザー ログイン時に適用されます。強制的に適用する場合は、 [ファイル] > [終了] を選択して Parallels Client を終了し、再起動してください。

8 Parallels Client のメインウィンドウが表示されます。左ペインの <接続先> を右クリックし、[接続プロパティ] をクリックします。



9 [接続プロパティ] ウィンドウが表示されます。RAS Console 上で確認したポリシーのポリシーの [ID] と [バージョン] が Parallels Client で表示されるポリシー情報と一致していることを確認します。



クライアント ポリシーのフィルタリングルールの追加

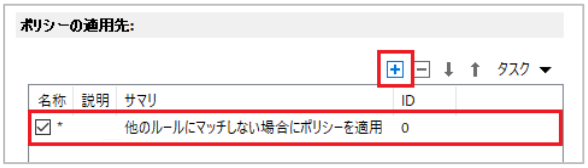
既定値では、フィルタリングルールが存在しないため、RAS に接続している全てのユーザーに対してクライアント ポリシーが適用されます。クライアント ポリシーの適用範囲を定義する場合は、フィルタリング ルールを追加します。

フィルタリング ルールを追加する手順は以下の通りです。

1 「ポリシーのプロパティ」ウィンドウを表示します。

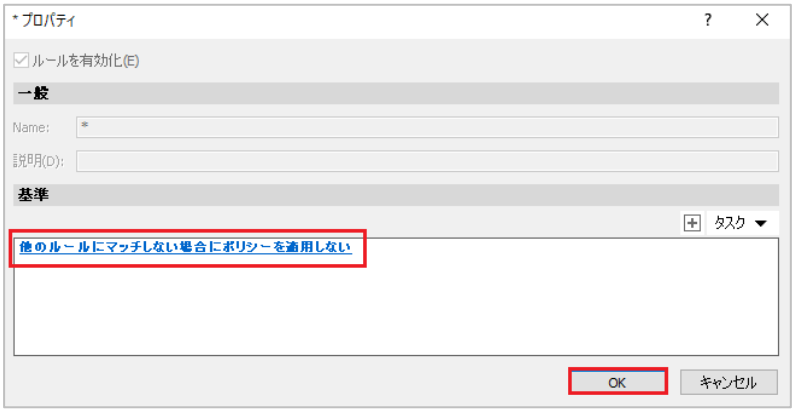
2 [ポリシーの適用先] 枠で、[＋] ボタン (または [タスク] > [追加]) をクリックします。

3 「新しいルールのプロパティ」ウィンドウが表示されます。要件に応じたフィルタリング ルールを追加してください。フィルタリング ルールの追加方法は、「フィルタリング ルールの追加 (p. 9)」をご参照ください。



4 「*」ルールをダブルクリックします。

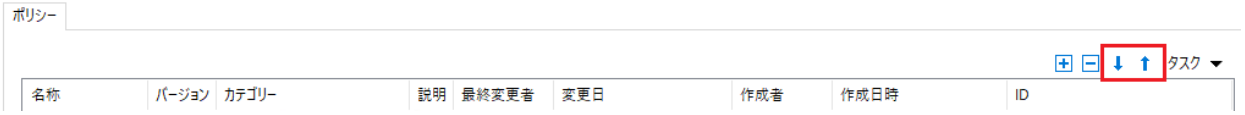
5 「*プロパティ」ウィンドウが表示されます。[他のルールにマッチしない場合にポリシーを適用] をクリックし、[他のルールにマッチしない場合にポリシーを適用しない] に変更します。[OK] をクリックします。



ポリシーの優先順位

クライアント ポリシーは、リストの上から順に適用され、クライアントごとに 1 つのポリシーのみが適用されます。同じクライアントに対して、適用可能なポリシーが複数ある場合、ポリシーのリストで上位にあるポリシーのみが適用されます。

優先順位を変更する際は、[↑ (上矢印)] または [↓ (下矢印)]ボタンをクリックして、リスト内のポリシーを移動します。



設定例

この章の内容

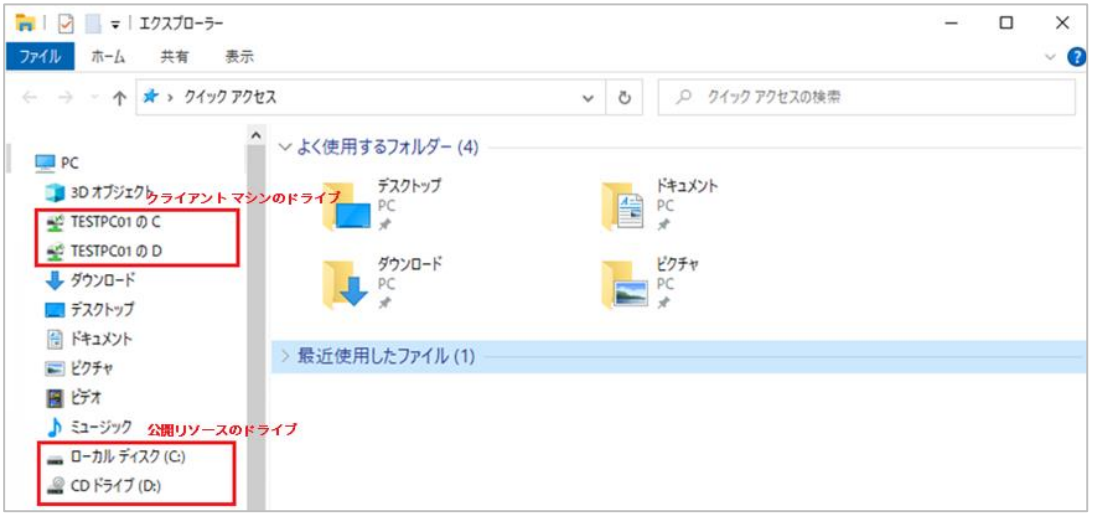
クライアント ポリシーの設定例

RAS のクライアント ポリシー機能を使用した、クライアント マシンに対する記憶デバイスの利用を制限する方法をご紹介します。本節に記載の設定例を利用して、ドライブやクリップボードのリダイレクト、クライアント マシンの周辺機器の制御が実現できます。

クライアント ポリシーを追加する方法につきましては、「クライアント ポリシーの追加 (p. 11) 」をご参照ください。

ドライブのマッピング制御

ポリシー設定を利用せず既定値のまま、公開リソースへ接続すると、クライアント マシンのドライブと、公開リソースのドライブが表示されます。いずれのドライブも、マシン間の境目を感じることなくアクセスすることが可能です。



セキュリティの観点から、仮想デスクトップを利用する場合には、クライアント マシンと仮想デスクトップ間で、データ コンテンツのコピーを制限することを推奨いたします。特に、Windows RDSH 環境を使用する際には、システム安定稼働のため、サーバーのドライブに格納されているデータに、ユーザーがアクセスをすることがないように運用する必要があります。

ログオン ユーザーが作成したデータ コンテンツは、ファイル サーバー (共有フォルダ) や、ログイン個人用フォルダのリダイレクト機能を利用して、一元管理するとよいでしょう。

クライアント マシンのドライブのマッピング制御

クライアント ポリシー設定を利用することで、クライアント マシンのドライブのマッピング (認識) を制限できます。

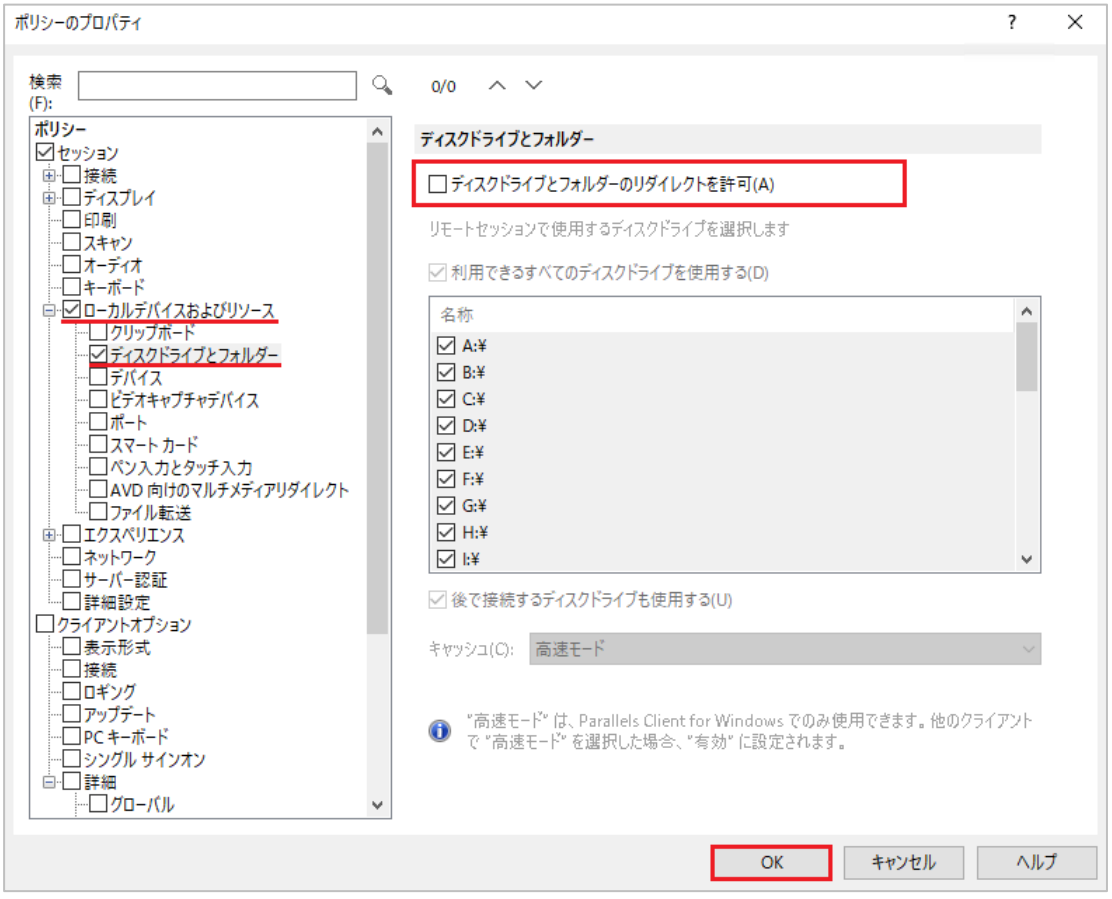
> 注 : このオプションは、Parallels Client for Windows のみに適用されます。

クライアント マシンのドライブを非表示にする手順は以下の通りです。

1 「ポリシーのプロパティ」ウィンドウを表示します。

2 左ペインにて、[ローカルデバイスおよびリソース] > [ディスク ドライブとフォルダー] にチェックを入れます。

3 [ディスク ドライブとフォルダー] セクションの [ディスクドライブとフォルダーのリダイレクトを許可] のチェックを外し、[OK] をクリックします。



公開リソースのドライブのマッピング制御

グループ ポリシーを利用することで、公開リソースのドライブのマッピング (認識) を制限できます。

公開リソースのドライブを非表示にする手順は以下の通りです。

1 Active Directory サーバーにて、[グループポリシーの管理] を起動します。

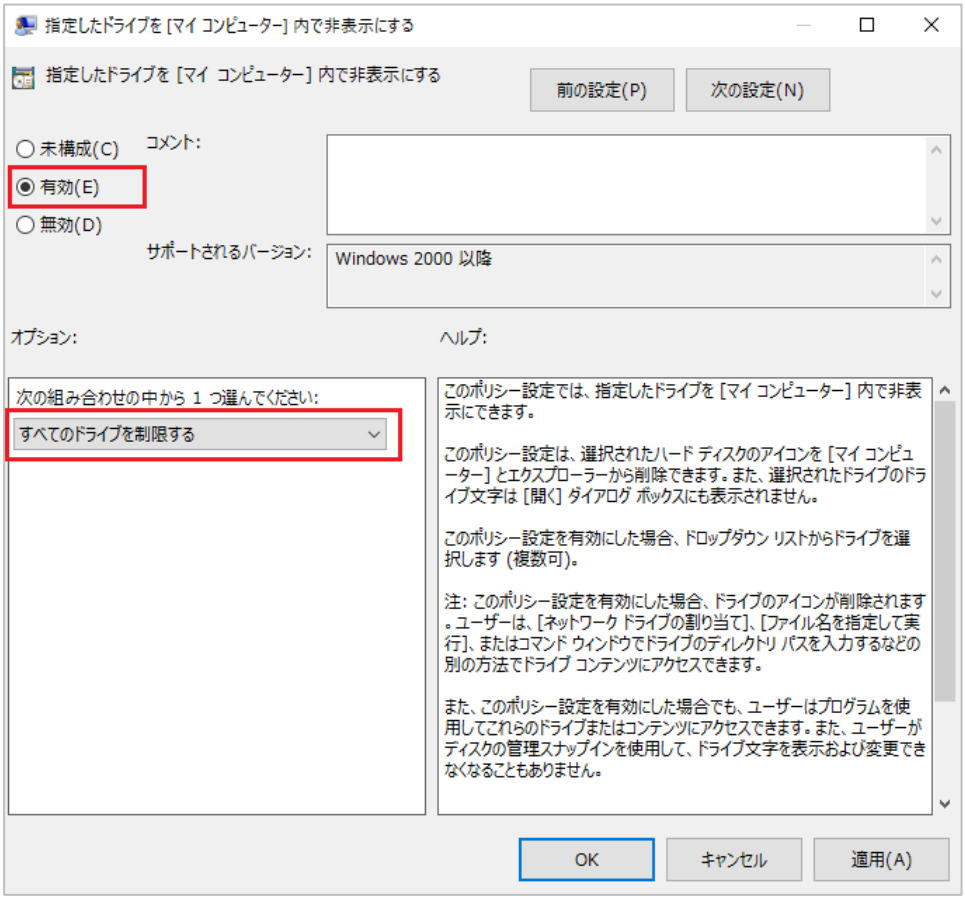
2 「グループポリシーの管理」ウィンドウが表示されます。ポリシーを右クリックし、[編集] を選択します。

3 「グループポリシー管理エディター」ウィンドウが表示されます。[ユーザーの構成] > [ポリシー] > [管理用テンプレート] > [Windows コンポーネント] > [エクスプローラー] の順に遷移します。

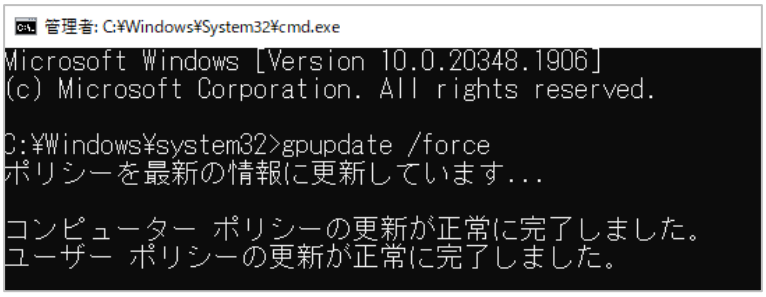
4 [指定したドライブを [マイ コンピューター] 内で非表示にする] をダブルクリックします。

5 [有効] を選択し、[オプション] セクションで、制限するドライブを選択します。 [OK] をクリックして、ウィンドウを閉じます。

注 : この設定を有効にした場合、ドライブのアイコンが非表示となります。ただし、ユーザーは、[ネットワーク ドライブの割り当て]、[ファイル名を指定して実行]、またはコマンドでのドライブのディレクトリパス入力などの方法でドライブにアクセスできます。



6 グループ ポリシーを適用するため、コマンド プロンプトから、[gpupdate /force] コマンドを実行します。



クリップボードの利用制限

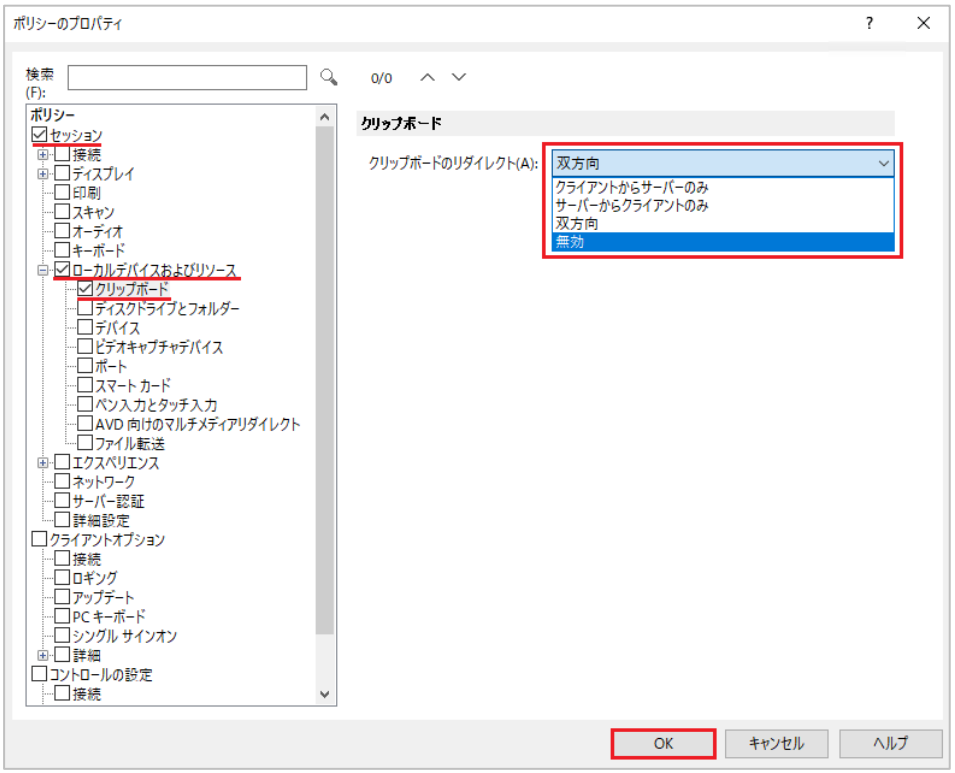
クリップボードの共有 (リダイレクト) 機能を利用すると、リモート間でのデータのコピー＆ペーストだけでなく、ファイル転送を容易に行えます。意図しないデータ漏洩を防止するために、不要な場合はクリップボードの共有を制御することを推奨します。

クリップボードの共有 (リダイレクト) を無効化する手順は以下の通りです。

1 「ポリシーのプロパティ」ウィンドウを表示します。

2 左ペインにて、[ローカルデバイスおよびリソース] > [クリップボード] にチェックを入れます。

3 [クリップボード リダイレクト]で [無効] を設定し、[OK] をクリックします。



周辺機器の利用制限

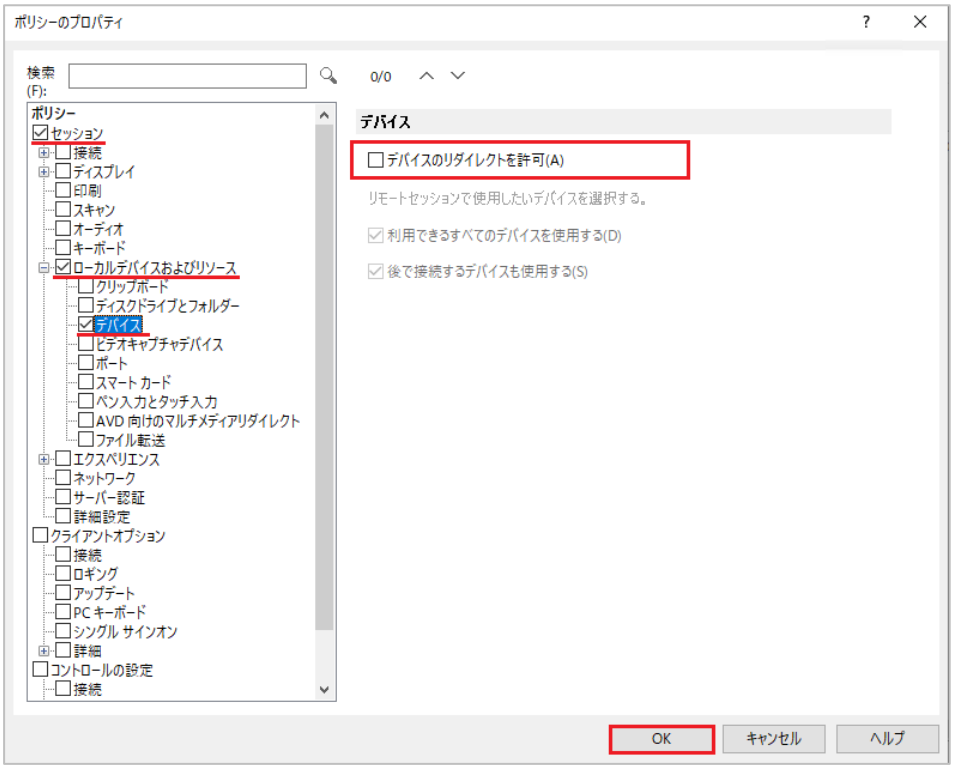
デバイスを介したウィルス感染やデータの持ち出しによる情報漏洩を防ぐために、外付けの記憶デバイスなど周辺機器の使用を制御することを推奨します。

クライアント マシンに接続された周辺機器の利用を無効化する手順は以下の通りです。

1 「ポリシーのプロパティ」ウィンドウを表示します。

2 左ペインにて、[ローカルデバイスおよびリソース] > [デバイス] にチェックを入れます。

3 [デバイスのリダイレクトを許可] のチェックを外します。



ポリシー ルールの条件の組み合わせ

クライアント ポリシーを適用するルールを複数の条件で構成した場合の動作について説明します。

既定値では、すべての構成済みのユーザーとグループとコンピューターにクライアント ポリシーが適用されます。オプションで、ポリシーを適用するタイミングを定義するルールを指定できます。この機能を使用すると、同じユーザーやコンピューターに対して複数のポリシーを作成し、ユーザーがどの場所のどのデバイスから接続しているかに応じてポリシーを適用することが可能になります。各ルールは、ユーザー接続に対するマッチングに使用される 1 つまたは複数の条件で構成されています。各条件は、マッチング可能な 1 つまたは複数の特定のオブジェクトで構成されています。

クライアント ポリシーのルールを構成する手順は以下の通りです。

1 「ポリシーのプロパティ」ウィンドウを表示します。

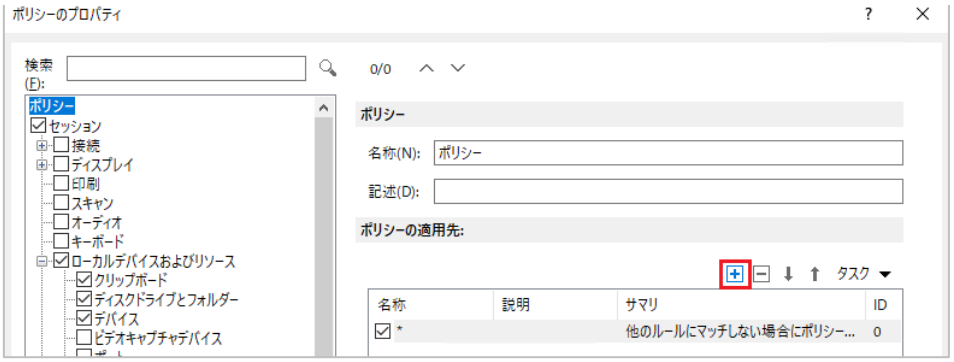
2 以下のオプションを有効化します。

> 注：詳細な設定方法は各節の内容をご確認ください。

- ドライブのマッピング制御
- クリップボードの利用制限
- 周辺機器の利用制限

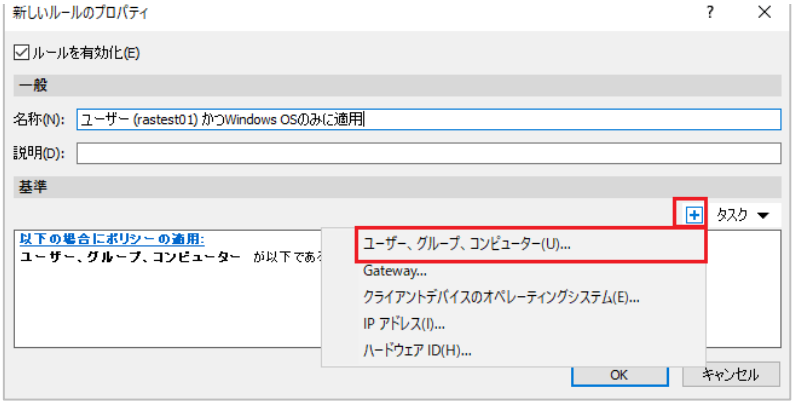
3 「特定のドメイン ユーザー」かつ「特定のマシン」に対してポリシーを適用させるため、クライアントポリシーのルールを追加します。

[ポリシーの適用先] 枠で、[＋] ボタン (または [タスク] > [追加]) をクリックします。

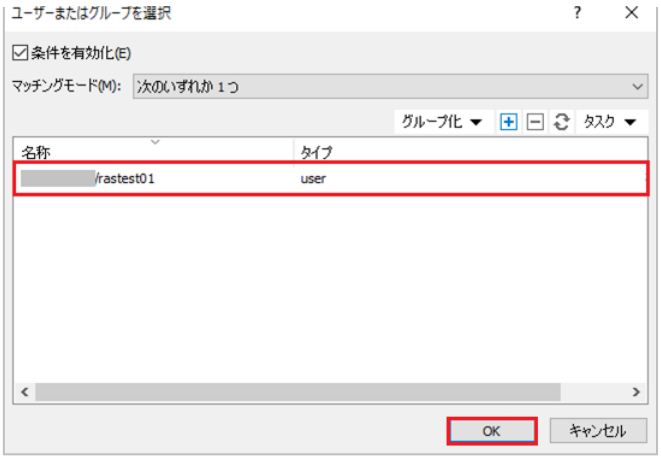


4 「新しいルールのプロパティ」ウィンドウが表示されます。

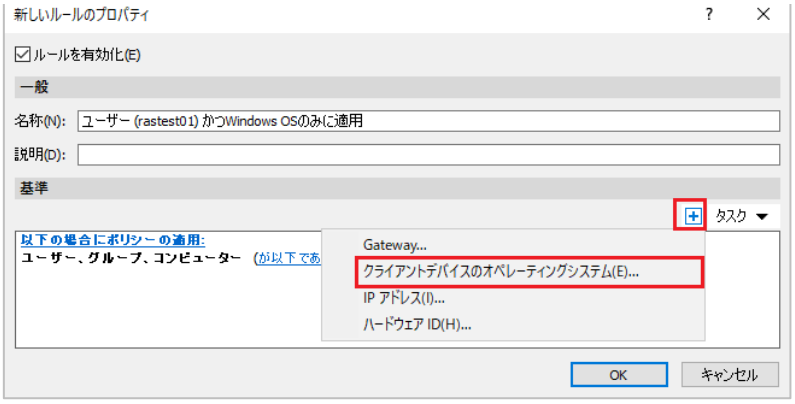
1 つ目の条件を追加します。[基準] 枠で、[＋] ボタン (または [タスク]) をクリックし、[ユーザー、グループ、コンピューター] を選択します。



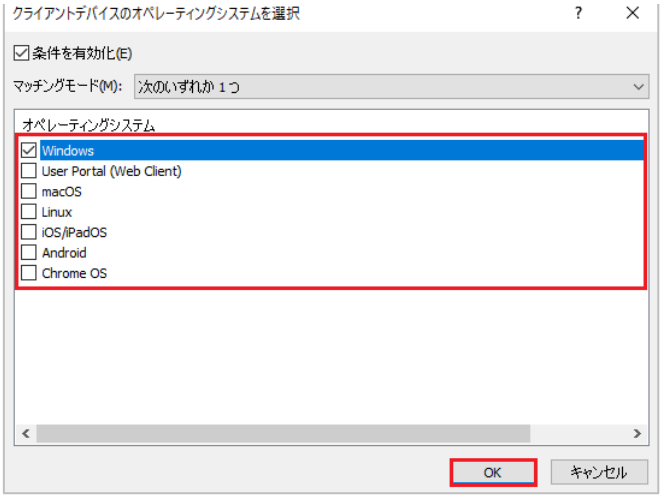
5 「ユーザーまたはグループを選択」ウィンドウが表示されます。[+] ボタン (または [タスク] > [追加]) をクリックし、<対象のユーザー> を選択します。[OK] をクリックします。



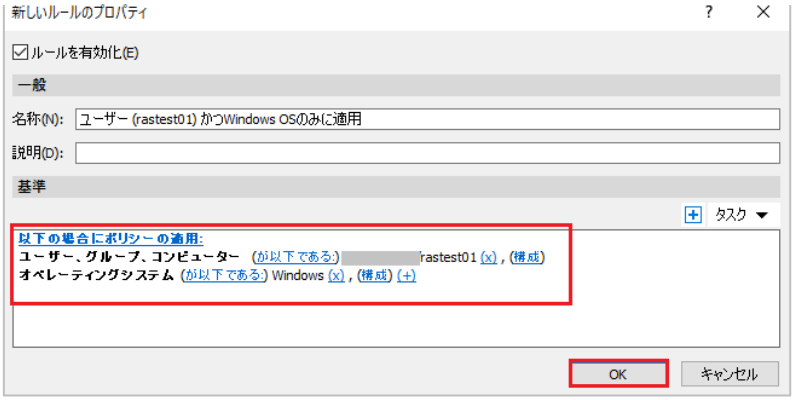
6 2 つ目の条件を追加します。[基準] 枠で、[+] ボタン (または [タスク]) をクリックし、[クライアント デバイスのオペレーティング システム] を選択します。



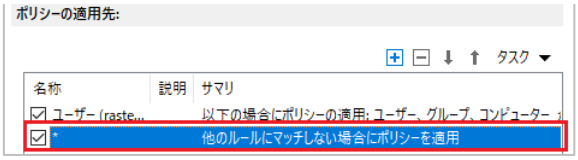
7 「クライアント デバイスのオペレーティング システムを選択」ウィンドウが表示されます。<対象の OS> を選択し、[OK] をクリックします。



8 ルールの [名称] を入力します。2 つの条件が設定されていることを確認し、[OK] をクリックします。

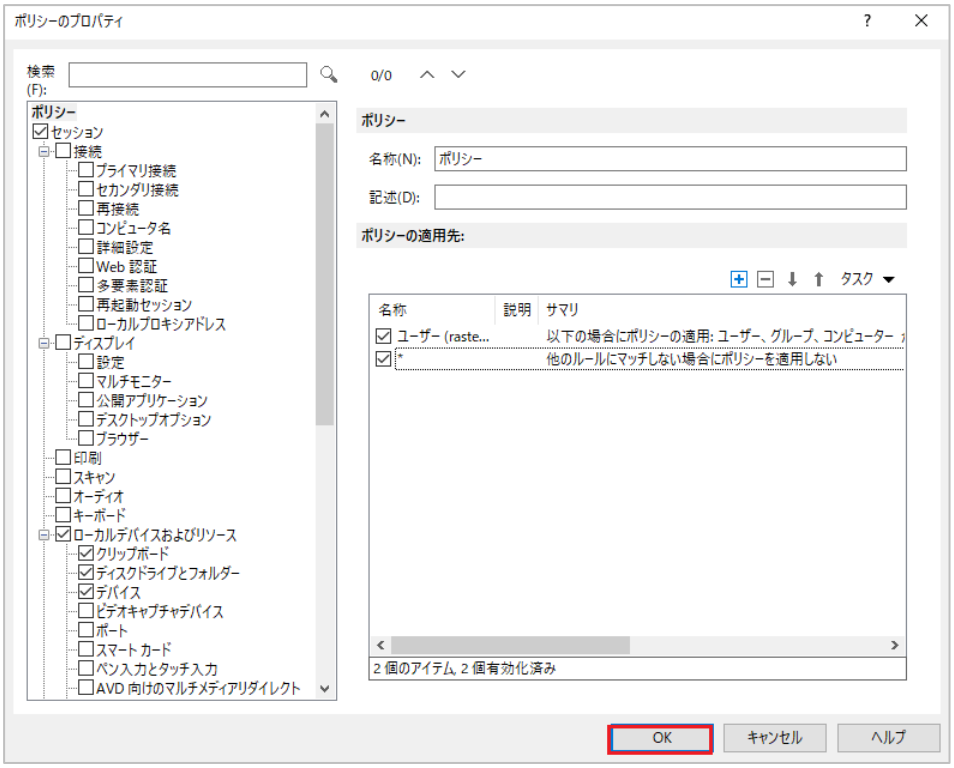


9 続けて、既定値の [*] ルールをダブルクリックします。

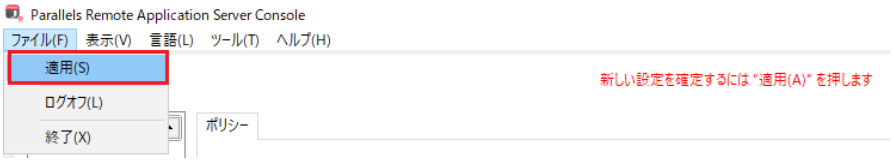


10 「*プロパティ」ウィンドウが表示されます。[他のルールにマッチしない場合にポリシーを適用] をクリックし、[他のルールにマッチしない場合にポリシーを適用しない] に変更します。[OK] をクリックします。

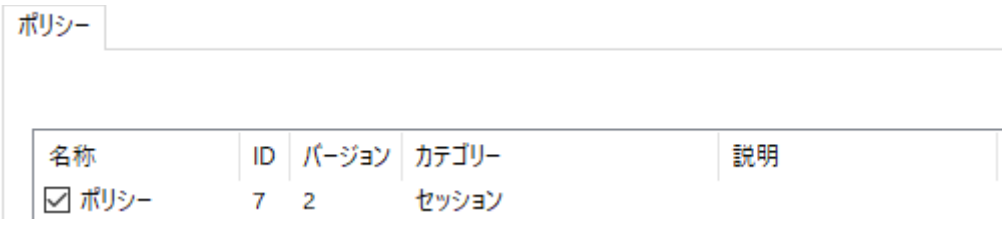
11 [OK] をクリックし、ウィンドウを閉じます。



10 RAS Console 上部メニューから [ファイル] > [適用] の順にクリックし、設定を保存します。



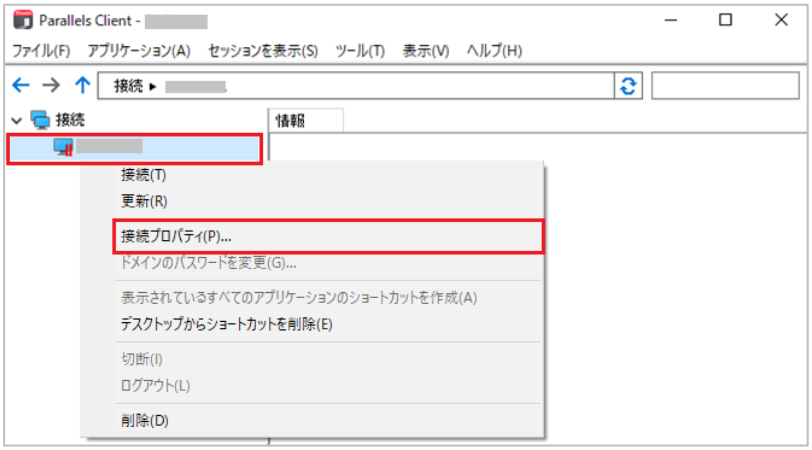
11 ポリシーが適用されていることを確認します。ポリシーの [ID] と[バージョン] を確認してください。



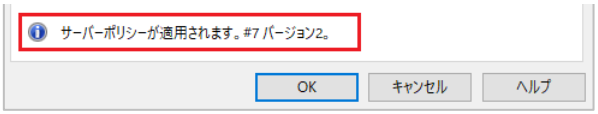
12 以降の操作はクライアント マシンにて実施します。Parallels Client を起動し、<対象のユーザー> 且つ <対象の OS> にてログオンします。

> 注 : ポリシーは、次回のユーザー ログイン時に適用されます。強制的に適用する場合は、 [ファイル] > [終了] を選択して Parallels Client を終了し、再起動してください。

13 Parallels Client のメインウィンドウが表示されます。左ペインの <接続先> を右クリックし、[接続プロパティ] をクリックします。



14 [接続プロパティ] ウィンドウが表示されます。RAS Console 上で確認したポリシーのポリシーの [ID] と [バージョン] が Parallels Client で表示されるポリシー情報と一致していることを確認します。



続けて、追加したポリシーの機能制限が有効であることを確認します。クライアント マシンのローカル ディスクが参照不可であること、クリップボードが使用不可であること、外付けの記憶デバイスなど周辺機器の使用が制限されていることを確認してください。

12 確認が完了しましたら、[ログアウト] します。

13 <対象のユーザー> 以外のユーザー且つ <対象の OS>にて、再度ログオンします。

14 前述のポリシーが適用されていないことを確認してください。