本書について

本書では、複数の Windows 機に対して ksocket からの WinRM 接続の受け入れ設定を一括で 行うための手順について記載いたします。

前提

本書の手順では、Active Directory のグループポリシー機能を使用します。そのため、下記の条件を満たす必要があります。

- Active Directory ドメインコントローラーが構成済みであること
- 設定対象の Windows 機が全てドメインコントローラーにて管理可能であること

また、本書は Active Directory 上での操作を経験済みの方を対象に内容記載いたします。各ア プリケーションの詳細操作については割愛する部分もございますので、ご了承ください。

本書で使用する名称について

本書では設定を行う上で使用する各種オブジェクトの名称として、下記を使用します。

ksocket からアクセスするために作成するドメ	ksocket
インユーザーアカウント名	
設定対象の Windows 機を所属させるセキュ	ksocket-machine
リティグループ名	
ksocket からの接続受け入れ設定を管理する	ksocket
グループポリシーオブジェクト名	

既存のユーザーアカウント・セキュリティグループを使用する場合や、運用上の都合で別の命名を 行う際は上記を適宜読み替えるようお願いいたします。

設定の流れ

本書では下記の流れにて設定を行います。

- 1. ドメインユーザー、セキュリティグループおよびグループポリシーオブジェクトの作成
- 2. セキュリティグループへのグループポリシー適用
- 3. ドメインユーザーに対する各コンピューターのローカルグループ割り当て

次ページ以降に、各手順の詳細を記載いたします。

ドメインユーザーの作成

ドメインユーザーを作成するには下記の手順を実施します。

- ① 「Active Directory ユーザーとコンピューター」を起動する
- ② 左ツリーメニューよりユーザーを作成する組織単位(OU)を選択する
- ③ 右リスト内の何もない部分を右クリックし、「新規作成」→「ユーザー」を選択する
- ④ 「姓」「ユーザーログオン名」に「ksocket」と入力し、「次へ」をクリックする
- ⑤「パスワード」に任意のパスワードを入力する
 (このパスワードは後に ksocket のクレデンシャル設定に使用します)
- ⑥ 「ユーザーは次回ログオン時にパスワード変更が必要」のチェックを外す
- ⑦ 「パスワードを無制限にする」のチェックを入れ、「次へ」をクリックする
- ⑧ 「完了」をクリックする

組織単位「Users」へユーザー作成を行った例を下記へ記載します。

		Active Director
ファイル(F) 操作(A) 表示(V) へ	Jレプ(H)	
🗢 🔿 🖄 📅 🤞 🗶 🖫) @ 🚘 🛛 🖬 🗏 📚 🛍 🍸 🚨 🍇	
 Active Directory ユーザーとコンと ○ 保存されたクエリ ● ○ ○ ○		
	& ksocket	ユーザー

セキュリティグループの作成

セキュリティグループを作成するには下記の手順を実施します。

- ① 「Active Directory ユーザーとコンピューター」を起動する
- ② 左ツリーメニューよりユーザーを作成する組織単位(OU)を選択する
- ③ 右リスト内の何もない部分を右クリックし、「新規作成」→「グループ」を選択する
- ④ 「グループ名」に「ksocket-machine」と入力する
- ⑤ 「グループのスコープ」を「ドメインローカル」に変更する
- ⑥ 「OK」をクリックする

組織単位「Users」へグループ作成を行った例を下記に記載します。

	Active Directory ユー					
ファイル(F) 操作(A) 表示(V) ヘルプ(H)						
🗢 🔿 📶 📋 🖾 🍳 📾 🦉 💆	<u></u>					
 Active Directory ユーザーとコンと 保存されたクエリ ● ●<th></th>						
& ksocket-machine	セキュリティ グループ - ドメイン ローカル					
28. 28.						

セキュリティグループへのメンバー追加

セキュリティグループを作成したら、下記の手順にて設定対象の全てのコンピューターをメンバー として追加します。

- ① 「Active Directory ユーザーとコンピューター」より「ksocket-machine」グループを右クリック する
- ② 「プロパティ」を選択し、「メンバー」タブを開く
- ③ 「追加」をクリックする
- ④ 対象のコンピューター名を入力し、「名前の確認」より対象コンピューターを選択する。
 この操作を対象コンピューター全てに対して繰り返す
- ⑤ 「OK」をクリックする
- ⑥ 「適用」をクリックする

実際に設定を行った例を下記に記載します。

ksocket-machineのプロパティ ? x
全般 メンバー 所属するグループ 管理者
所属するメンバー(M):
名前 Active Directory ドメイン サービス フォルダー
WINSRV2008R2SP1
追加(D) 削除(R)
OK キャンセル 適用(A)

グループポリシーオブジェクトの作成

グループポリシーオブジェクトを作成するには、下記の手順を実施します。

- ① 「管理ツール」より「グループ ポリシーの管理」を起動する
- ② 左ツリーメニューより設定対象のドメインを右クリックする
- ③ 「このドメインに GPO を作成し、このコンテナーにリンクする」をクリックする
- ④ 「名前」に「ksocket」を入力し、「OK」をクリックする

実際に追加した例を下記に記載します。

2 ファイル(F) 操作(A) 表示(V) ウィンド	ゔ)(W) へルプ(H)
 マーブボリシーの管理 ▲ フォレスト: ▲ 高 ドメイン ▲ 高 ドメイン ▲ 高 ● 回 ○ クルーブボリシー オブジェクト ● 回 ● 回 ○ クリーブボリシー のモデル/作成 	の グルーブ ボリシー オブジェクト 内容 委任 ② Default Domain Controllers Policy ③ Default Domain Policy ④ ksocket

グループポリシーオブジェクトの編集(WinRM の設定)

作成したグループポリシーオブジェクトに対し、具体的な設定を加えます。

- 「グループ ポリシーの管理」の左ツリーメニューより 設定対象ドメイン内の「グループ ポリシー オブジェクト」を選択する
- ② 「ksocket」を右クリックし、「編集」を選択する
- ③ 左ツリーメニューより、「コンピューターの構成」→「ポリシー」→「管理用テンプレート」→
 「Windows コンポーネント」→「Windows リモート管理(WinRM)」→「WinRM サービス」を選択する
- ④ 「WinRM によるリモートサーバー管理を許可する」を右クリックし、「編集」を選択する
- ⑤ ラジオボタンより「有効」を選択する
- ⑥ 「オプション」内の「IPv4 フィルター」「IPv6 フィルター」双方に「*」を入力し、「OK」をクリックす る

ここまでの設定を行った例を下記に示します。

<u>.</u>	グループ ポリシー管理エディター				
ファイル(F) 操作(A) 表示(V) ヘルプ(H) ◆ ◆ 2 □ □ マ					
 Windows リモートシエル Windows リモート管理 (WinRM) WinRM ウチイアント WinRM ウチーどス Windows ログオンのオプション Windows ログオンのオプション Windows 信頼会分析 Work Folders Work Folders 	 ▲ WinRM サービス 項目を違択すると説明が表示されます。 ● WinRM によるリモート サーバー管理を許可する ● 使キャジ運を許可する ● ごでedSSP 認証を許可する E 暗号化されていないトラフィックを許可する E チャネル バインディングトークン強化機能レベルを指定する 	500 有効 未構成 未構成 未構成			

引き続き、次ページの手順を行います。

- ⑦ 左ツリーメニューより「コンピューターの構成」→「基本設定」→「コントロール パネルの設定」→「サービス」を選択する
- ⑧ 右の表内(この時点では項目なし)を右クリックし、「新規作成」→「サービス」を選択する
- ⑨ 「スタートアップ」を「自動」に変更する
- 11 「サービス名」の右にある「…」をクリックする
- ① 「Windows Remote Management」を選び、「選択」をクリックする
- ① 「サービス操作」を「サービスを開始する」に変更し、「OK」をクリックする

設定を行った例を下記に記載します。



グループポリシーオブジェクトの編集(ファイアウォールの設定)

ksocket からの接続をブロックしないよう、ファイアウォールの設定を加えます。

- 「グループ ポリシーの管理」の左ツリーメニューより
 設定対象ドメイン内の「グループ ポリシー オブジェクト」を選択する
- ② 「ksocket」を右クリックし、「編集」を選択する
- ③ 左ツリーメニューより、「コンピューターの構成」→「ポリシー」→「管理用テンプレート」→
 「ネットワーク」→「ネットワーク接続」→「Windows ファイアウォール」→
 「ドメイン プロファイル」を選択する
- ④ 「Windows ファイアウォール: ICMP の例外を許可する」を右クリックし、「編集」を選択する
- ⑤ ラジオボタンより「有効」を選択する
- ⑥ 「オプション」内の「着信エコー要求を許可する」にチェックを入れ、「OK」をクリックする
- ⑦ 「Windows ファイアウォール:着信リモート管理の例外を許可する」を右クリックし、 「編集」を選択する
- ⑧ ラジオボタンより「有効」を選択する
- ③「オプション」の「要請されない着信メッセージを許可する IP アドレス」に「*」を入力し、「OK」をクリックする

設定を行った例を下記に記載します。

	グループ ポリシー管理	エディター	_ 0
ファイル(F) 操作(A) 表示(V) ヘルプ(H) ◆ ● ② □ ● ② □ ● ③ □ ▼			
■ BrainLadie ■ DirectAccess クライアント エクスペリエンスの) ■ DNS クライアント ■ LAN Manager サーバー ■ Link-Layer Topology Discovery ▶ ■ Microsoft ピア ツー ピア ネットワーク サービス ▶ ■ QoS パケット スケジューラ ■ SNMP ■ SSL 構成設定 ▶ ■ TCPIP 設定	ドメイン プロファイル 項目を選択すると説明が表示されます。	設定 注 Windows ファイアウォール: ローカル プログラムの例外を許可する 注 Windows ファイアウォール: 著信プログラムの例外を注意する 注 Windows ファイアウォール: すべてのネットワーク接続の保護 ご Windows ファイアウォール: 例外を許可しない ひいかめの ファイアウォール: 例外を許可しない ご Windows ファイアウォール: ICMP の例外を許可する ご Windows ファイアウォール: ICMP の例外を許可する	状態 未未未構成 未未未 未構成 有効 未構成
 Windows Connect Now Windows 接続マネージャー WLAN サービス WWAN サービス オフライン ファイル ネットワーク プロパイダー オットワーク接続 Windows ファイアウオール ドメイン プロファイル デメイン プロファイル 		 E) Windows ファイアウォール: 通知を禁止する E) Windows ファイアウォール: ローカル ポートの例外を許可する E) Windows ファイアウォール: 老信サートを聞めを完善する E) Windows ファイアウォール: 老信リモート管理の例外を許可する E) Windows ファイアウォール: 宅信レモト アスト・ブの例りを許… E) Windows ファイアウォール: マルキャストまたはプロートキャスト要… E) Windows ファイアウォール: 老信 UPnP フレームワークの例外を… 	未構成 未 其基成 有効 未構成 未構成 未構成

引き続き、次ページの手順を実施します。

- ① 左ツリーメニューより、「コンピューターの構成」→「ポリシー」→「Windows の設定」→ 「セキュリティの設定」→「セキュリティが強化された Windows ファイアウォール」→「セ キュリティが強化された Windows ファイアウォール」→「受信の規則」を選択する
- ① ビューを右クリックし、「新しい規則」を選択する
- ⑦ ラジオボタンにて「事前定義」を選択し、セレクトボックスより「Windows リモート管理」を選択 する
- ③ 「次へ」をクリックする
- ④ 2 つの規則が表示されるので、「プロファイル」が「パブリック」になっている規則のチェックを 外す
- ① 「次へ」→「完了」をクリックする
- 16 作成された規則を右クリックし、「プロパティ」を選択する
- ① 「詳細設定」タブを開き、「プロファイル」内の「プライベート」のチェックを外す
- 18 「OK」をクリックする

設定を行った例を下記に記載します。

_		_						_
	<u>I</u>		グループ ポリシー管理エディ	9-				_
	ファイル(F) 操作(A) 表示(V) ヘルプ(H)							
	(=							
	👰 コンピューターの構成 🛛 🗠	f	有別	ヴループ	עריינטל	市初	15 /F	優
	⊿ 🛅 ポリシー	II	Windows リモート管理 (HTTP 受信)	Windows リモート管理	ドメイン	はい	許可	LU
	▶ 🛗 ソフトウェアの設定	Ц						
	▲ 🦳 Windows の設定							
	▶ 1 名前解決ポリシー							
	スカリプト (スタートアップ/シャットダウン)							
	4 単 セキュリティの設定							
	▶ 🖪 ファイル システム							
	▶ iii ワイヤード (有線) ネットワーク (IEEE 802.3) ボ							
	▲ 2キュリティが強化された Windows ファイアウォー							
	▲ ● セキュリティが強化された Windows ファイアウ							
	🗱 受信の規則							
	🕵 送信の規則							
	🌆 接続セキュリティの規則							
	ネットワーク リフト マネージャー ポリシー							

グループポリシーオブジェクトの編集(ネットワークポリシーの設定) ネットワークポリシーの設定を加えます。

- 「グループ ポリシーの管理」の左ツリーメニューより 設定対象ドメイン内の「グループ ポリシー オブジェクト」を選択する
- ② 「ksocket」を右クリックし、「編集」を選択する
- ③ 左ツリーメニューより、「コンピューターの構成」→「ポリシー」→「Windows の設定」→ 「セキュリティの設定」→「ネットワーク リスト マネージャー ポリシー」を選択する
- ④ 「識別されていないネットワーク」を右クリックし、「プロパティ」を選択する
- ⑤ 「場所の種類」を「プライベート」に変更し、「OK」をクリックする

実際に設定を行った例を下記に記載します。

9	ガルーゴ ヂルミ、 佐田テゴ ル	
ファイル(F) 操作(A) 表示(V) ヘルプ(H)	識別されていないネットワークのプロパティ	x
アイル(F) 操作(A) 表示(V) ヘルプ(H) マーンビューターの構成 の	ネットワーク名 ネットワークの場所 ネットワークの場所 ネットワークの場所により、コンピューターが接続されているネットワークの運動が識別され、 その場所に適したファイアウォール設定が自動的に使用されます。 第 識別されてい ネットワークの すすべてのネッ 場所の種類 ・ 主構成(N) ・ ブライペート(R) ・ フィーサーのアクセス許可 ・ 未構成(O) ・ ユーザーは場所を変更できるい(S)	
▶ 27トウェアの制限のポリシー ~	OK キャンセル 適用(A)	

セキュリティグループへのグループポリシー適用

作成したグループポリシーを、下記の手順でセキュリティグループへ適用します。

- ① 「管理ツール」より「グループ ポリシーの管理」を起動する
- ② 左ツリーメニューより対象ドメイン内の「グループ ポリシー オブジェクト」→「ksocket」を選 択する
- ③ 「セキュリティ フィルター処理」下部の「追加」をクリックする
- ④「選択するオブジェクト名を選択してください」ボックス内に「ksocket-machine」と入力し、「名前の確認」をクリックする。複数の候補が出た場合は「ksocket-machine」グループを選択する
- ⑤ 「OK」をクリックする

実際に設定を行った例を下記に記載します。

	10. e a 7 /10.	グルーフ
📓 J71ル(F) 操作(A) 衣示(V) J72F9(V ◆ ➡ 🔷 📶 🖸 👔 🖬	v) ∕\µ/(H)	
な グループポリシーの管理 ▲ フォレスト: ▲ 論 ■ Default Domain Policy ■ ksocket ■ RDP	ksocket スコープ 詳細 設定 メスロープ 詳細 設定 委示するリンクの場所(L): 次のサイト、ドメイン、および OU がこの GPO にリンクされご 場所	ています(T): 調 リンクの有効化
 ▶ ▶ ■ ♪ ● ●<td><u>ب</u></td><td>いえばい</td>	<u>ب</u>	いえばい
	セキュリティ フィルター処理 この GPO での設定は、次のグループ、ユーザーおよびコン 名前 ▲ Authonticated Licerc & ksocket-machine (■ ¥ksocket-machine)	ビューターにのみ適用されます(5

ドメインユーザーに対する各コンピューターのローカルグループ割り当て

最後に、ドメインユーザーを各コンピューターのローカルグループへ割り当てます。

- ① 「管理ツール」より「グループ ポリシーの管理」を起動する
- ② 左ツリーメニューより設定対象ドメイン内の「グループ ポリシー オブジェクト」を選択する
- ③ 「ksocket」を右クリックし、「編集」を選択する
- ④ 左ツリーメニューより「基本設定」→「コントロールパネルの設定」→「ローカル ユーザー
 とグループ」を選択する
- ⑤ ビュー内を右クリックし、「新規作成」→「ローカルグループ」を選択する
- ⑥ 「グループ名」プルダウンより「Administrators(ビルトイン)」を選択する
- ⑦ 「メンバー」下部の「追加」をクリックする
- ⑧ 「名前」の右にある「…」をクリックする
- ⑨ 「選択するオブジェクト名を入力してください」に「ksocket」と入力する
- ① 「名前の確認」をクリックする。複数の選択肢が提示された場合は「ksocket」ユーザーを選択 する
- ①「OK」をクリックして「ユーザー、コンピューターまたはグループの選択」ダイアログを閉じる
- ① 「OK」をクリックして「ローカル グループ メンバー」ダイアログを閉じる
- ③ 「メンバー」に選択したユーザーが追加されたことを確認し、「OK」をクリックする

実際に設定した例を下記に記載します。



以上にて全ての設定手順は完了となります。

適宜、「ksocket」ユーザーを使用するよう ksocket のクレデンシャル設定を行ってください。