

弊社商品を動作させるための WindowsXP SP2 の設定方法

この手順書では、WindowsXP ServicePack2（以下 SP2）環境において、弊社製品『GaiaMX』『Gaia21』『Gaia』『Charites21』『Q-1(LAN 版)』を動作させるための設定方法についてご説明いたします。

弊社では、SP2 に対応した商品の改良も行っており、SP2 対応版の商品ではこの手順書の作業を行わなくても商品を使用することができます。

（GaiaMX、Gaia21 のお客様であれば、SP2 リリース後に「Gaia チャンネル」より最新プログラムをダウンロードしていただきますと、自動で設定が行われます。）

また、後述する設定作業を自動で行うツールプログラムをご用意しており、弊社 WEB サイトよりダウンロード可能になります。（ご希望のお客様には CD でのご提供も行います。）

上記方法により、SP2 環境にて弊社製品が動作している場合には、この手順書にある作業は必要ありません。

SP2 にて追加／変更された機能のうち、

- ・ **ファイアウォールが標準で有効になった件**
- ・ **DCOM のセキュリティが強化され、標準でリモートからのアクセスができなくなった件**

の 2 つにより、

サーバーに SP2 をインストールした時の標準設定では、C/S 版(LAN 版)商品において、クライアント機からサーバー機へアクセスすることができません。

また、スタンドアロン版におきましても、データベースエンジンと弊社プログラムの通信においてファイアウォールから警告メッセージが表示されます。

そのため、上記 2 点について、設定の変更が必要です。

1. ファイアウォールの設定

SP2 ではファイアウォール機能が強化され、標準で有効になりました。そのため、外部からコンピュータへの通信が、特定のものを除き全て遮断されます。サーバー機においては、クライアント機からの必要な通信も全て遮断されてしまうため、設定変更により通信を許可する必要があります。

変更には 2 通りの方法があります。

1 つ目は、ファイアウォールを無効にする方法です。

ただしセキュリティの観点からはお勧めできません。他の手段にて、コンピュータのセキュリティを確保した上で行うべき方法です。

2 つ目は、ファイアウォールを有効にした上で、弊社プログラムの接続を許可するように設定する方法です。

詳細については後述します。

2. DCOM の設定

DCOM はネットワークを通じてプログラムが通信を行うための技術ですが、SP2 ではネットワークを介した DCOM の利用は標準設定では許可されていません。

そのため、リモートからのアクセス・起動を許可する作業が必要になります。

全てのユーザーに許可する方法と、指定ユーザーのみに許可する方法があります。

詳細については後述します。

SP2 を適用するコンピュータによって、必要な対策が異なります。

『GaiaMX』

サーバー機	ファイアウォールの設定、DCOM の設定、両方が必要です。 設定を行わない場合、クライアントが接続できず、商品が動作しません。
クライアント機	動作に支障はありませんが、ファイアウォールの警告メッセージが表示されます。 詳細は P.8 を参照してください。 GaiaMX の利用者が Windows の管理者権限を持つ場合には、その場で警告を解除することができますが、そうでない場合には、あらかじめファイアウォールの設定が必要です。(P.3～7) DCOM の設定は必要ありません。

『Gaia21』『Charites21』

サーバー機	ファイアウォールの設定、DCOM の設定、両方が必要です。 設定を行わない場合、クライアントが接続できず、商品が動作しません。
クライアント機	動作に支障はありませんが、ファイアウォールの警告メッセージが表示されます。 詳細は P.8 を参照してください。
スタンドアロン	Gaia21、Charites21 の利用者が Windows の管理者権限を持つ場合には、その場で警告を解除することができますが、そうでない場合には、あらかじめファイアウォールの設定が必要です。(P.3～7) DCOM の設定は必要ありません。

『Gaia』

サーバー機	Gaia のサーバーは WindowsXP 非対応のため、今回の設定からも対象外です。
クライアント機	動作に支障はありませんが、ファイアウォールの警告メッセージが表示されます。 詳細は P.8 を参照してください。
スタンドアロン	Gaia の利用者が Windows の管理者権限を持つ場合には、その場で警告を解除することができますが、そうでない場合には、あらかじめファイアウォールの設定が必要です。(P.3～7) DCOM の設定は必要ありません。

『Q-1』

サーバー機にて、ファイアウォールの設定が必要です。

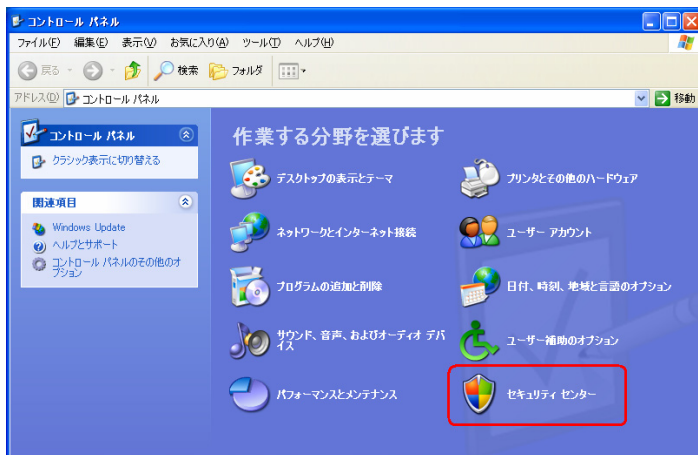
注意!!

以下の設定を行う場合には、Administrator 権限を持つユーザーで WindowsXP にログインする必要があります。

1. ファイアウォールの設定



Windows のスタートボタンを押し、メニューから「コントロールパネル」を選択します。



コントロールパネル画面の下部に、SP2 で新しく追加された「セキュリティセンター」のメニューがあります。

これを選択します。



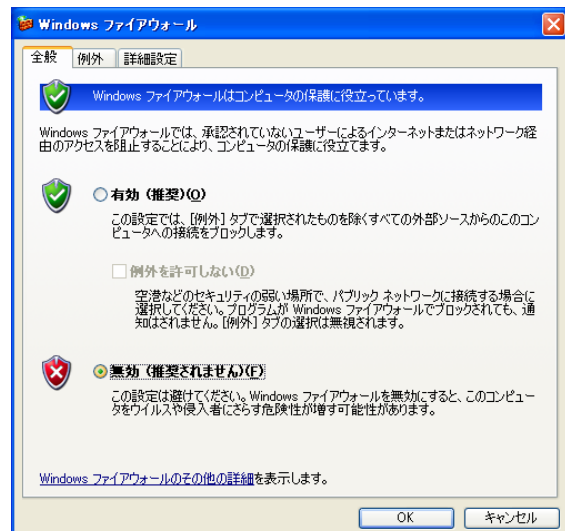
セキュリティセンター画面下部に、「セキュリティの設定の管理」の項目があります。

その中の、「Windows ファイアウォール」を選択します。

ファイアウォールを無効にする場合

ファイアウォール機能を無効に設定すると、SP2 導入以前と同様にすべてのアクセスを通過させることができます。

しかし、セキュリティレベルについても以前と同様となり、ファイアウォールによって遮断されるべき不正アクセスを通してしまうこととなります。



そのため、ファイアウォール機能を無効にすることはお勧めできません。別の手段でコンピュータの安全性が確保されている場合にのみ、標準のファイアウォール機能を無効にしてよいかもしれません。

それ以外の場合は、次項の「ファイアウォールを有効にする場合」の設定をお願いします。

他の方法で安全性が確保されているため、標準のファイアウォールを無効にするには、左図ファイアウォール画面にて、

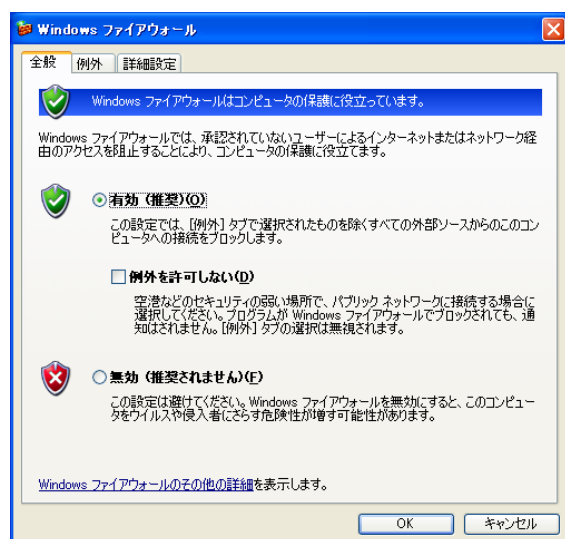
「無効 (推奨されません)」のボタンにチェックをつけて「OK」を押してください。

また、ファイアウォールを無効にした場合には、セキュリティセンターにて警告が表示されるようになります。警告を解除するには、セキュリティセンターのファイアウォールの項目にある、「推奨される対策案」ボタンを押し、「自分でファイアウォール対策を行い、管理します」にチェックを入れる必要があります。

ファイアウォールを有効にする場合

ファイアウォールを有効にした場合、外部からコンピュータへのアクセスを遮断できます。

この状態では、例えば弊社製品 GaiaMX、Gaia21、Charites21 などのサーバーがインストールされているパソコンにアクセスしようとした場合でも、ファイアウォールによって遮断されてしまい、サーバーのデータ等にアクセスすることができません。



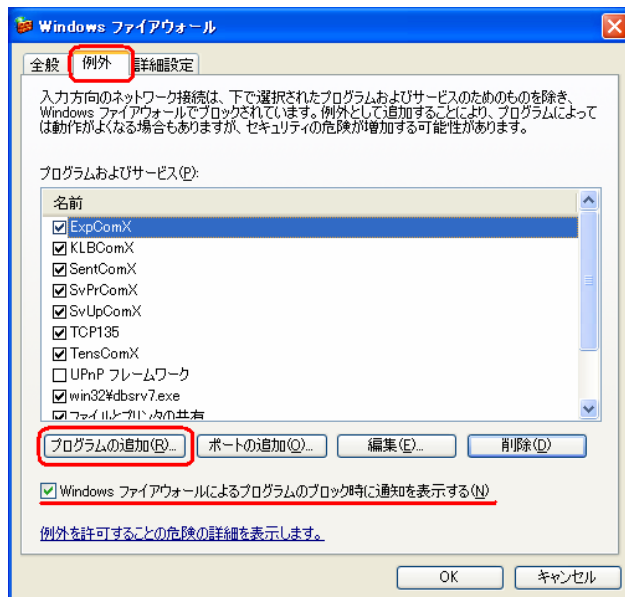
ファイアウォールが有効の状態、不正なアクセスを遮断しながら、特定のプログラムには通信を許可する設定が可能です。

以下、その方法について説明します。

Windows ファイアウォールの画面にて、「有効 (推奨)」

のボタンが選択されていることを確認してください。

また、「例外を許可しない」のチェックが外れていることを確認してください。

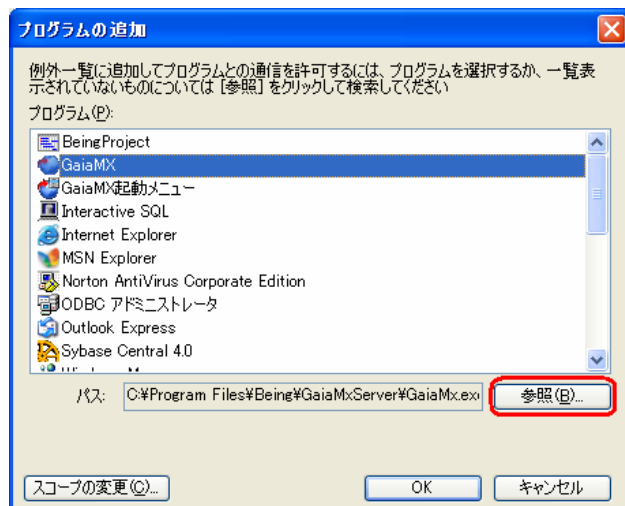


「例外」タブをクリックします。

左図のような画面が表示されます。
この画面で接続を許可するプログラム等の設定を行います。

「Windows ファイアウォールによるプログラムのブロック時に通知を表示する」
にチェックがついていることを確認してください。

「プログラムの追加」ボタンを押し、
接続を許可するプログラムを選択します。



プログラムの追加画面が開きます。

「参照」ボタンを押し、プログラムを追加して
いきます。
追加するプログラムは商品によって異なります。
次ページに一覧を記します。

プログラムの追加は、必要なプログラムを全
て登録するまで繰り返します。

追加プログラム一覧

GaiaMX、Gaia21、Gaia、Charites21

2通りの設定方法があります。

1. 最低限必要なプログラムのみ登録し、残りは実行時に適宜追加していく方法
2. あらかじめ全ての対象プログラムを例外に登録する方法

サーバーでは、下記表の「最小設定」を例外に登録する必要があります。(必須)

クライアント、スタンドアロン版、サーバー版(GaiaMX の場合)は、あらかじめ設定を行わなくとも、実行時にファイアウォールより表示される通知画面にて適宜例外登録を行うことができます。

ただし、その場合製品利用時に、Windows の Administrator(管理者)権限があるユーザーで Windows にログインしている必要があります。管理者権限がない場合には、その方法は使えませんので、あらかじめ全ての対象プログラムを登録する必要があります。

通知画面については、P.8「※弊社製品をご使用中に、Windows ファイアウォールから警告メッセージが表示される場合」を参照してください。

※インストール先のドライブ名、フォルダ名はお客様の環境に合わせて変更してください。

下記表では、標準設定のままインストールした場合を想定しています。

GaiaMX

最小設定		
サーバー	C:\Program Files\Being\GaiaMxServer\	ExpComX.exe
		SentComX.exe
		SvPrComX.exe
		SvUpComX.exe
		TensComX.exe
	C:\Program Files\Being\KojiLibMx\	KLBComX.exe
		SvPrComX.exe
	C:\Program Files\Sybase\SQL Anywhere 7\win32\	dbsrv7.exe
全て登録の場合		
サーバー	C:\Program Files\Being\GaiaMxServer\	.exe ファイル全て
	C:\Program Files\Being\KojiLibMx\	.exe ファイル全て
	C:\Program Files\Sybase\SQL Anywhere 7\win32\	dbsrv7.exe dbeng7.exe
クライアント	C:\Program Files\Being\GaiaMxClient\	.exe ファイル全て
	C:\Program Files\Sybase\SQL Anywhere 7\win32\	dbeng7.exe

Gaia21

最小設定		
サーバー	C:\Program Files\Being\Gaia21\	ExpCom. exe
		SentCom. exe
		SvProCom. exe
		SvUpCom. exe
		TensoCom. exe
	C:\Program Files\Being\KojiLib21\	KLBCom. exe
全て登録の場合	C:\Program Files\Being\Gaia21\	SvProCom. exe
	C:\Program Files\Sybase\SQL Anywhere 7\win32\	dbsrv7. exe
サーバー	C:\Program Files\Being\Gaia21\	. exe ファイル全て
	C:\Program Files\Sybase\SQL Anywhere 7\win32\	dbsrv7. exe dbeng7. exe
クライアント/ スタンドアロン	C:\Program Files\Being\Gaia21\	. exe ファイル全て
	C:\Program Files\Sybase\SQL Anywhere 7\win32\	dbeng7. exe

Gaia

最小設定		
サーバー	WindowsXP 非対応のため、対象外	
全て登録の場合		
クライアント/ スタンドアロン	C:\Program Files\GaiaSystem\GaiaWin\	. exe ファイル全て
	C:\sqlany50\win32\	dbeng50. exe

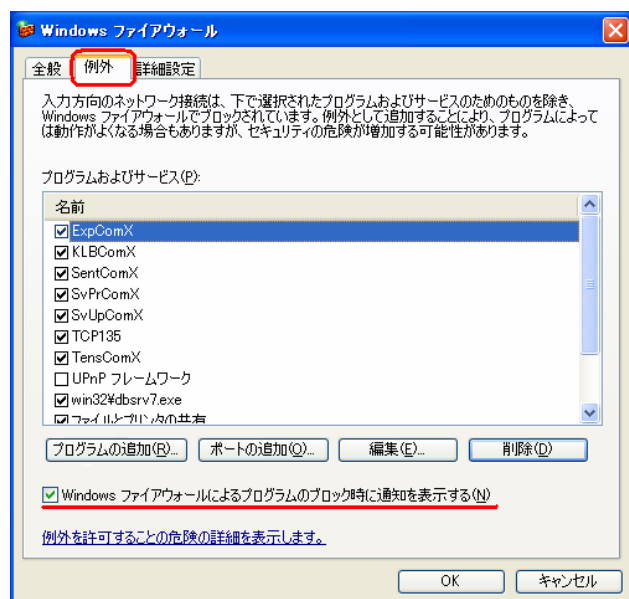
Charites21

最小設定		
サーバー	C:\Program Files\Being\ChKojiLib\	ChKLBCom. exe
	C:\Program Files\Sybase\SQL Anywhere 7\win32\	dbsrv7. exe
全て登録の場合		
サーバー	最小設定と同じ	. exe ファイル全て
	C:\Program Files\Sybase\SQL Anywhere 7\win32\	dbsrv7. exe dbeng7. exe
クライアント	C:\Program Files\Being\Charites21\	. exe ファイル全て
	C:\Program Files\Sybase\SQL Anywhere 7\win32\	dbeng7. exe

Q-1

「例外」画面に標準で用意されている、「ファイルとプリンタの共有」にチェックをつけてください。

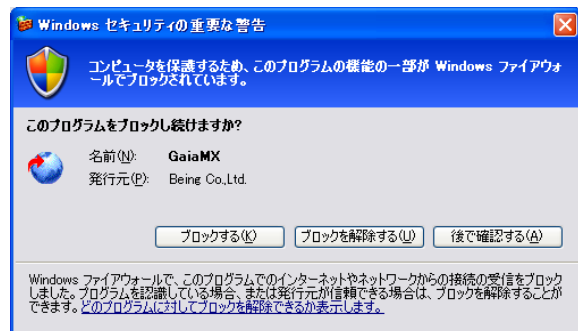
※弊社製品をご使用中に、Windows ファイアウォールから警告メッセージが表示される場合



ファイアウォール設定画面の「例外」タブにおいて、「Windows ファイアウォールによるプログラムのブロック時に通知を表示する」にチェックをつけておくと、ファイアウォールがアクセスをブロックした際に通知画面が表示され、引き続きそのアクセスをブロックするか、解除するか指定を行うことができます。

当社商品以外のソフトウェアご使用時においても、あらかじめプログラム登録を行わなくても、この機能によって、アクセスが発生した時点で例外登録を行うことができます。

弊社製品をご利用中に、次のような警告画面が表示される場合があります。



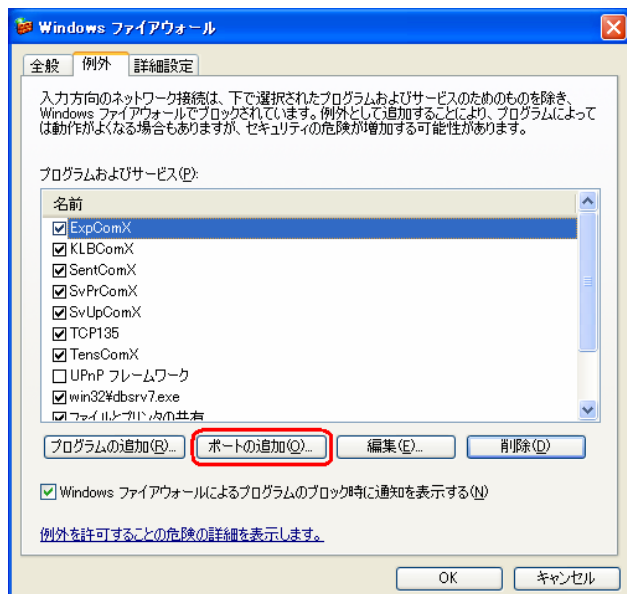
画面には警告とありますが、深刻な問題ではありません。

Windows ファイアウォールにて、コンピュータの通信がブロックされているため、通信を利用するプログラムが動作する場合に、この警告が表示されます。

プログラムの名前と発行元をご確認の上、問題ないプログラムであれば、「**ブロックを解除する**」ボタンを押していただくと、ファイアウォールの設定に追加され、次回から警告メッセージは表示されなくなります。

ただし、「**ブロックを解除する**」ボタンを押すためには、Windows の Administrator 権限(管理者権限)が必要です。

権限がないユーザーで Windows にログオンしている場合、この画面では解除できませんので、あらかじめファイアウォールの例外登録が必要になります。

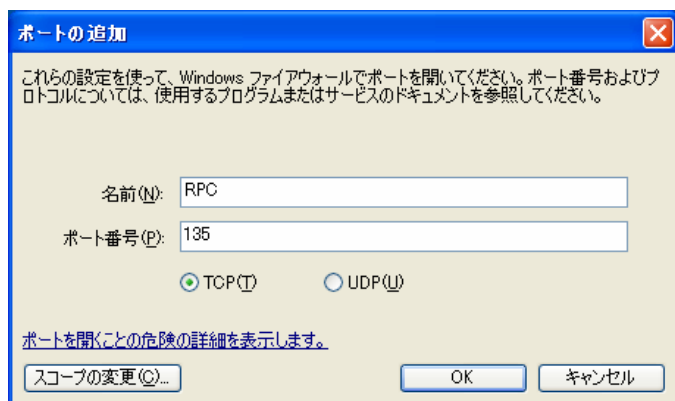


次に、「ポートの追加」を行います。

Windows ファイアウォールの画面から、「**ポートの追加**」ボタンを押してください。

※ポートとは？

パソコンがネットワークを通じてデータのやり取りをする際に、データを区別するために利用される番号です。通信の種類ごとに番号が振られており、たとえば ホームページへのアクセスは 80 番、電子メールの送信は 25 番、受信は 110 番などと決められています。



ポートの追加画面にて、名前とポート番号を入力します。

名前は区別がつく任意の名前で構いませんが、例として「RPC」

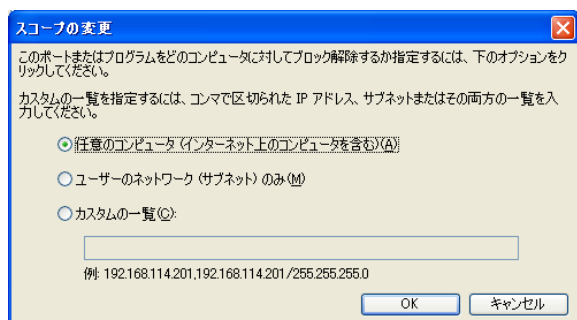
ポート番号は **135**

TCP/UDP の選択は、**TCP** にチェックがついていることを確認してください。

入力が終わりましたら、「**OK**」を押してください。

ポートの追加画面が閉じられ、例外の一覧に先ほど入力した名前が追加されています。

※ よりセキュリティを高めるために



「ポートの追加」画面において、「**スコープの変更**」ボタンを押すことで、特定のコンピュータのみ接続を許可することができます。

標準では「任意のコンピュータ」になっています。「**ユーザのネットワーク**」を選択すると、同一 LAN 内のみからの接続を許可します。

「**カスタムの一覧**」を選択し、IP アドレス、サブネットを入力することで、コンピュータを個別に

指定したり、特定の範囲の IP アドレスを持つコンピュータに制限したりすることができます。お客様のネットワークの IP アドレスが不明な場合は、ネットワーク管理者に相談してみてください。

以上でファイアウォールの設定は終了です。

2. DCOM の設定

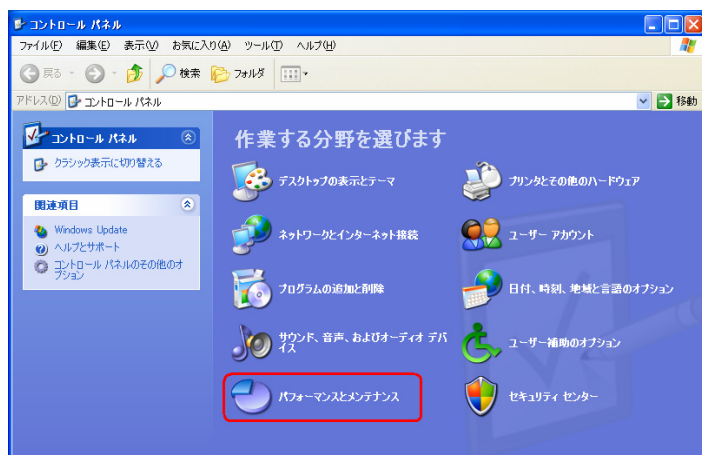
WindowsXP SP2 では、DCOM のセキュリティが強化され、リモートからのアクセスに制限をかけることができるようになりました。

DCOM とは、クライアント/サーバー型のプログラムにおいて、クライアントからサーバーのプログラムを起動・アクセスするための技術です。

SP2 では、標準でリモートからの DCOM へのアクセスができなくなっています。

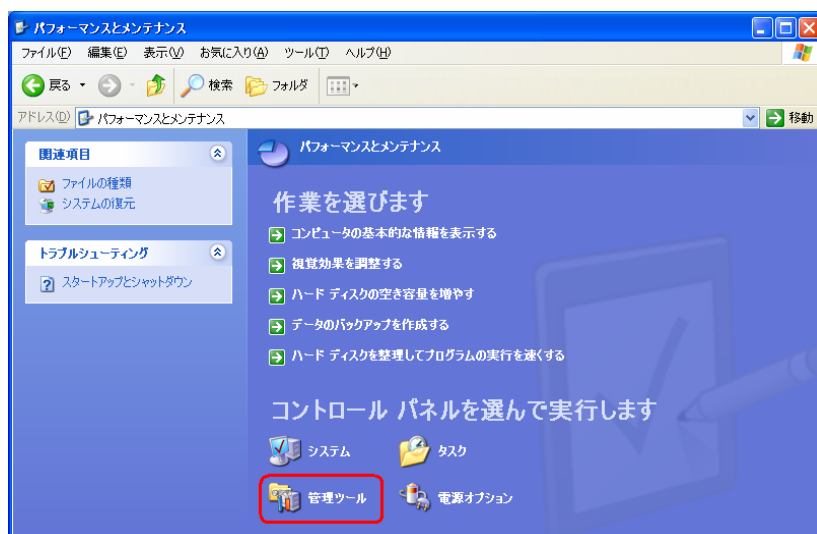


Windows のスタートボタンを押し、メニューから「コントロールパネル」を選択します。

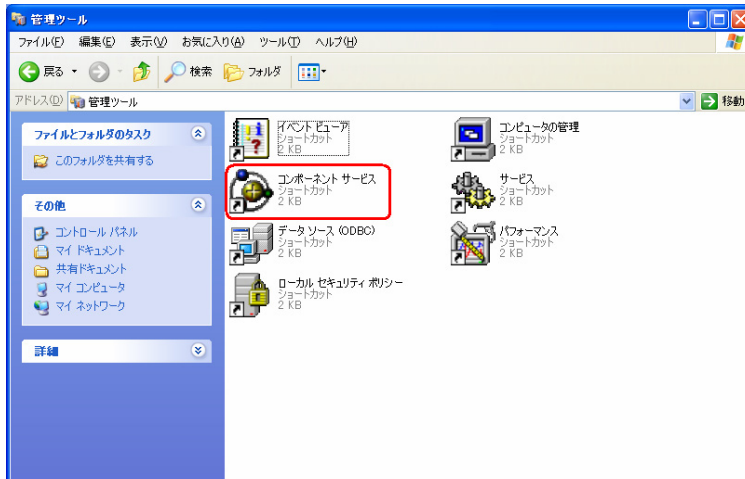


コントロールパネル画面の下の方に、「パフォーマンスとメンテナンス」のメニューがあります。

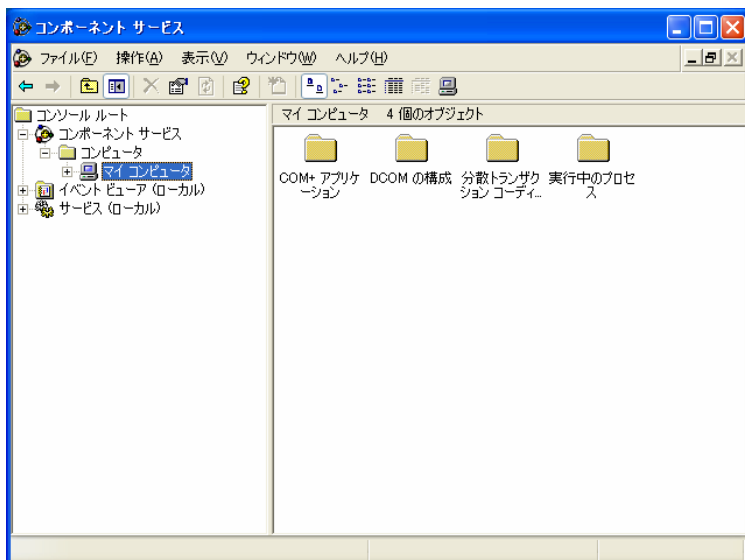
これを選択します。



画面下部のアイコンから、「管理ツール」を選択します。



管理ツール画面より、「コンポーネントサービス」を選択します。

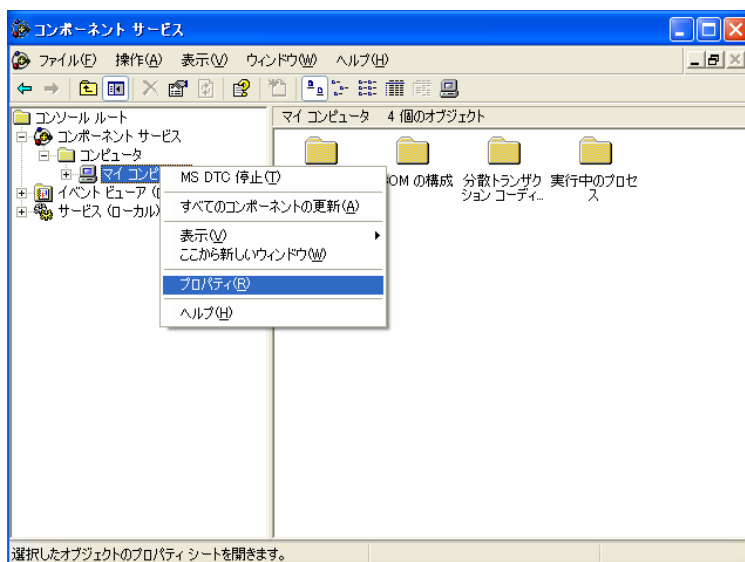


コンポーネントサービスの画面にて、画面左のツリーより、

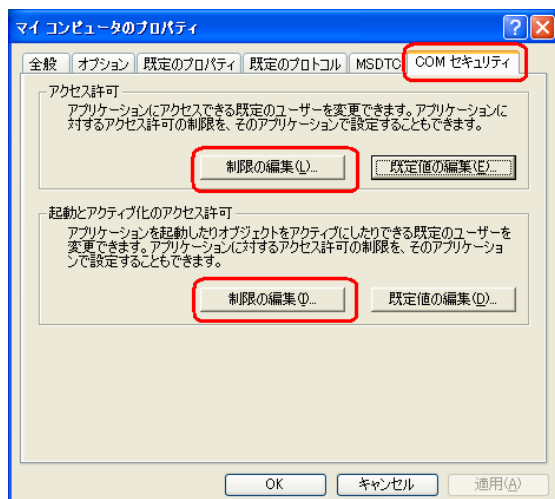
コンソールルート
↓
コンポーネントサービス
↓
コンピュータ
↓
マイコンピュータ

と選択します。

※ 選択中に、ファイアウォールの警告メッセージが表示される場合がありますが、「ブロックを解除する」ボタンを押し、選択を続けてください。

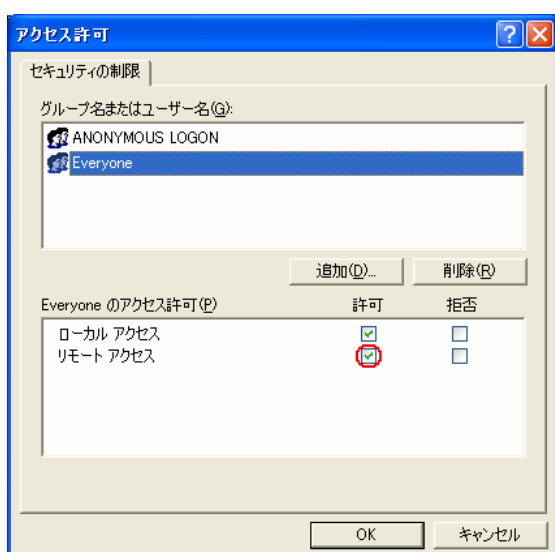


マイコンピュータを右クリックし、表示されたメニューから「プロパティ」を選択します。



マイコンピュータのプロパティ画面にて、一番右の「COM セキュリティ」タブを選択します。

左図のような設定画面が開きますので、「アクセス許可」の「制限の編集」「起動とアクティブ化のアクセス許可」の「制限の編集」を行います。



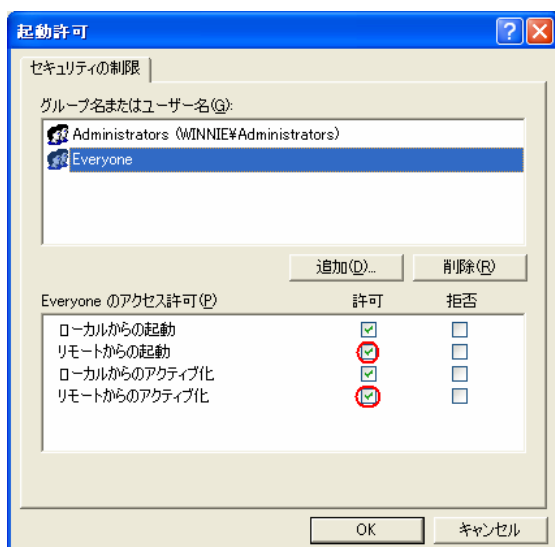
「アクセス許可」の「制限の編集」ボタンを押すと、左図のような設定画面が表示されます。

グループ名またはユーザー名に表示されている「Everyone」を選択し、

画面下部に表示される「Everyone のアクセス許可」にて、

「リモートアクセス」の許可にチェックがついていることを確認してください。

(標準で許可されているはずです。)



「起動とアクティブ化のアクセス許可」の「制限の編集」ボタンを押すと、左図のような設定画面が表示されます。

グループ名またはユーザー名に表示されている「Everyone」を選択し、

画面下部に表示される「Everyone のアクセス許可」にて、

「リモートからの起動」「リモートからのアクティブ化」の許可にチェックをつけてください。

(ローカルからの起動とアクティブ化は標準で許可されているはずです。)

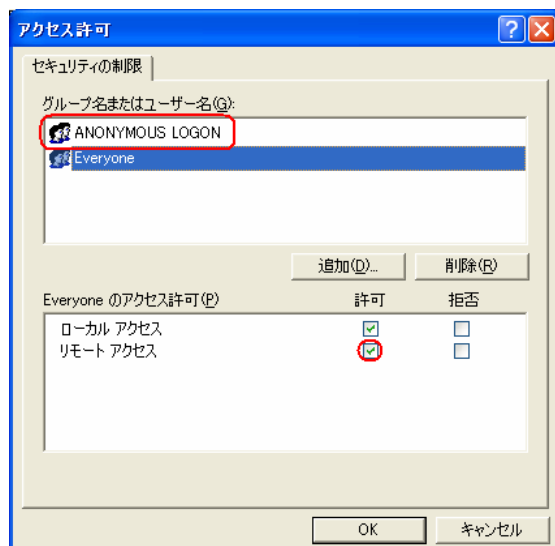
※1 上記設定でアクセスできない場合

サーバーにて Guest アカウントが有効で、クライアントが Guest 権限にてアクセスしている場合、上記設定ではアクセスできない場合があります。その場合には、

1つめの、「アクセス許可」の「制限の編集」の画面にて、

「追加」ボタンを押し、「ANONYMOUS LOGON」を追加してください。

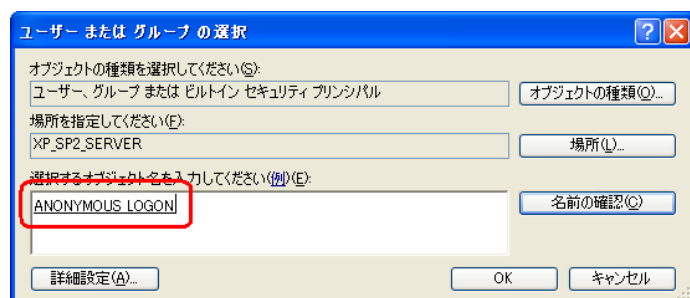
その上で、「ANONYMOUS LOGON」にリモートアクセスを許可してください。



「アクセス許可」画面にて、「ANONYMOUS LOGON」が

表示されている場合は、リモートアクセスを許可してください。

表示されていない場合は、「追加」ボタンを押します。



「選択するオブジェクト名を入力してください」の入力域に、「ANONYMOUS LOGON」（半角）と入力し、OK してください。

成功すると、「アクセス許可」画面に ANONYMOUS LOGON が表示されますので、リモートアクセスを許可してください。

※「名前が見つかりません」という画面が表示される場合は、入力文字が間違っている可能性がありますので、入力した文字をご確認ください。

※2 Everyone、ANONYMOUS LOGON を使用せず、ユーザーを限定する場合

セキュリティの観点から、限定したユーザーにのみリモートからのアクセスを許可する場合、

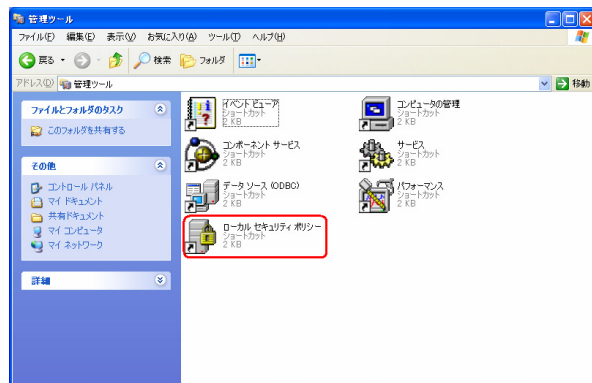
1. 弊社商品のサーバーが稼動するサーバーに、ログインするユーザーを登録してください。（コントロールパネルの、「ユーザーアカウント」メニューより行います。）
ユーザーが複数ある場合には、グループを作成し、登録したユーザーをグループにまとめておくと便利です。
2. 「アクセス許可」「起動とアクティブ化のアクセス許可」の設定画面にて、Everyone、もしくは ANONYMOUS LOGON のリモートからの起動・アクセスのチェックをはずし、登録したユーザー／グループにチェックをつけてください。
これで、匿名ユーザーではなく、指定ユーザーのみ、アクセスを許可することができます。

※3 P.10~13のDCOMの設定を行ってもアクセスできない場合

ケース1:

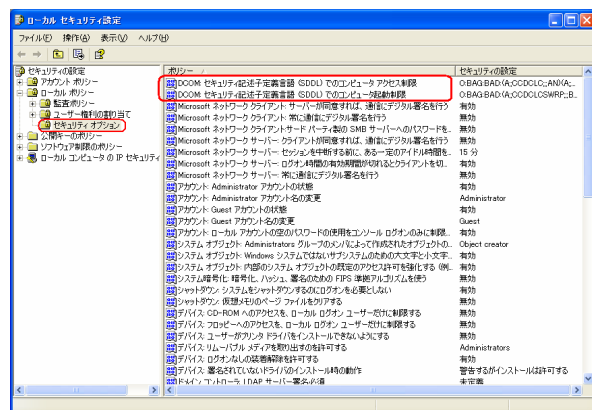
ローカルセキュリティポリシーにて、別途DCOMのセキュリティが設定されている可能性があります。

ローカルセキュリティポリシーの設定は、上記にて説明したCOMセキュリティ設定に優先して採用されます。こちらでセキュリティの設定がされていると、上記操作にて設定してもうまく動作しない可能性があります。



コントロールパネルの「パフォーマンスとメンテナンス」より、「管理ツール」画面を開きます。

「管理ツール」画面から、「ローカルセキュリティポリシー」を選択します。



左のツリーより、

セキュリティの設定

↓

ローカルポリシー

↓

セキュリティオプション

を選択します。

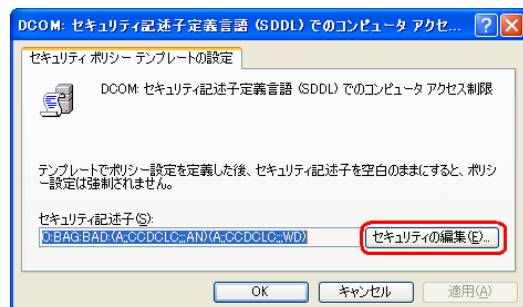
右画面の上位2行、

DCOM:セキュリティ記述子定義言語(SDDL)でのコンピュータアクセス制限

DCOM:セキュリティ記述子定義言語(SDDL)でのコンピュータ起動制限

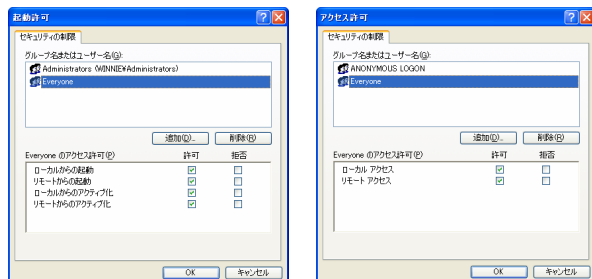
にて、セキュリティの設定を行います。

行をダブルクリックすると、セキュリティ記述子の入力画面が開きます。



この画面にて、「セキュリティの編集」ボタンを押すと、アクセス許可を設定する画面が表示されます。

前述の作業と同様に、リモートからの起動・アクセス許可を設定してください。



設定画面にて、
Everyone もしくは特定ユーザー／グループ
にリモート起動・アクセスを許可してください。

設定の詳細は、P.12～13 を参照してください。

上記作業を、

DCOM:セキュリティ記述子定義言語 (SDDL) でのコンピュータアクセス制限

DCOM:セキュリティ記述子定義言語 (SDDL) でのコンピュータ起動制限

の 2 行分を行います。

ケース 2 :

グループポリシーが設定されている可能性があります。

グループポリシーは、ドメインに参加する全てのコンピュータに影響します。

ケース 1 のローカルセキュリティポリシーを設定した場合でも、お客様のネットワークがグループポリシーによって運用されている場合、グループポリシーの方が優先され、設定が上書きされます。

可能であれば、ネットワーク管理者に連絡し、グループポリシーのセキュリティオプションが変更可能であるか、確認してください。

設定の方法は、P. 14 を参考にしてください。

本文書の内容につきまして、ご不明な点がございましたら弊社サポートセンターもしくは最寄の営業所までご連絡ください。

サポートセンター

〒514-0009

三重県津市羽所町 700 番地 アスト津 10F

TEL : (059) 227-2932 受付時間 : 9 : 00 ~ 18 : 00 (土日祝祭日を除く)

FAX : (059) 224-8407

E-mail : support@beingcorp.co.jp

<http://www.beingcorp.co.jp/support/xpsp2/>

本文書の内容は、2004 年 8 月 16 日時点での情報を元に作成しています。

WindowsXP SP2 の画面、仕様は、RC2 (評価版) を使用しています。

今後の Microsoft 社からのリリース内容によって、本文書の内容が変更になる場合があります。あらかじめご承知ください。