



OPC を Windows XP SP2 で利用するための
DCOM 設定について

日本 OPC 協議会
技術部会

1 はじめに

Windows XPのService Pack 2(SP2)は、より強固なセキュリティ環境を確立し、コンピュータをウイルスやワームなどの悪意ある攻撃から守るために役立つ機能を提供します。SP2では、いくつかのセキュリティ機能強化と最新のセキュリティ更新プログラムを含んでいますが、主に下記の4つの機能強化が行われています。

1. ネットワークからWindows XPを守るための機能強化
 - a) RPCとDCOMのセキュリティ機能強化
 - b) Windowsファイアウォールの機能強化
2. メモリー保護の機能強化
3. 電子メールの安全性強化
4. Internet Explorerのセキュリティ機能強化

OPCをリモート接続で使用しているOPCクライアントとOPCサーバは、ネットワークでの通信にDCOMを利用しているため、SP2による機能変更の影響を受けます。SP2をインストールした直後のデフォルト設定では、DCOMを利用したOPCのリモート接続は動作しない状態です。本ホワイトペーパーでは、Windows XP SP2でDCOMによるOPCのリモート接続を使用するための方法について説明します。

SP2ではいくつかのセキュリティ対応機能が強化されていますが、DCOMを利用したOPCの動作に直接影響を与えるのは次の二つの機能変更です。一つ目は、DCOMに新しい設定が追加された点です。もう一つは、Windows XPが持っているソフトウェアファイアウォールの機能が大幅に強化され、デフォルトで機能が有効になっていることです。

OPCのコールバック機能は、OPCクライアントがDCOMを利用するサーバに、OPCサーバがDCOMを利用するクライアントに変わることを意味しますので、本ホワイトペーパーで説明する方法はOPCサーバとOPCクライアントのどちらに対しても適用する必要があります。

補足: OPCをスタンドアロンで利用している場合(DCOMではなく、COMを利用するローカル接続の場合)は、本書に記述されている方法を適用しなくても、SP2のインストール直後のデフォルト設定でOPCの機能は正常に動作します。

2 Windows Firewallについて

Windows ファイアウォールは、ファイアウォールの外側からユーザの許可なくコンピュータにアクセスしようとする相手からコンピュータを保護します。インターネットやネットワーク経由で、第三者がコンピュータに接続しようとする要求(以降"未承諾要求"とします)がコンピュータに送信

されると、Windows ファイアウォールが接続をブロック (阻止) します。このファイアウォールでは、「例外」を設定することで、未承諾要求を受信可能にすることができます。

例外の設定は、「アプリケーションレベルでの設定」と「ポートとプロトコルレベルでの設定」をすることができます。「アプリケーションレベルでの設定」では未承諾要求の受信を可能にするアプリケーションを指定することができ、「ポートとプロトコルレベルでの設定」ではTCPかUDPのどちらかのプロトコルとポート番号を指定して通信を許可することができます。OPCサーバ/クライアントでDCOMを利用できるようにするには、両方のレベルで例外の設定をする必要があります。

補足: OPC対応製品を開発する場合に、ファイアウォール設定の自動化プログラムを記述するために、マイクロソフトはWindows Firewall APIを公開しています。

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ics/ics/inetfwauthorizedapplication.asp>

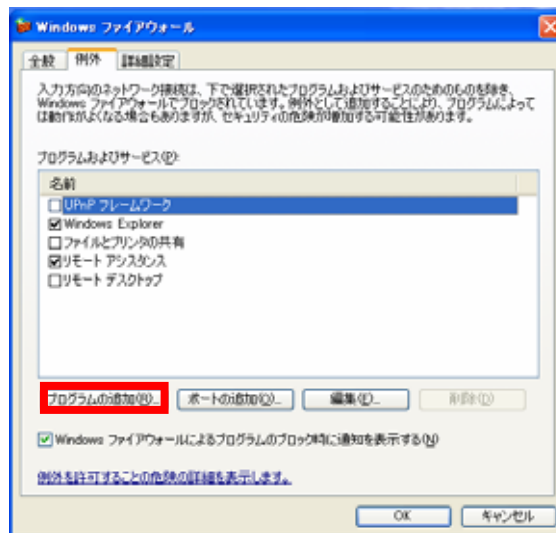
2.1 Windows Firewallの設定

1. Windowsファイアウォールは、デフォルトで「有効」に設定されています。マイクロソフトと日本OPC協議会は、PCを最も安全に保つため、この設定を「有効」にすることを推奨します。ファイアウォールの設定による通信障害かを検証するためなどの場合には、一時的に無効にすることはあるかもしれません。

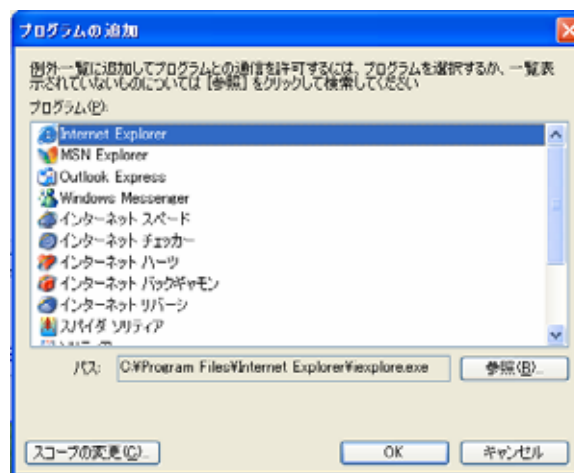
補足: 社内ネットワークのファイアウォールでPCが十分に保護されている場合には、Windows ファイアウォールの設定を無効にする場合も考えられます。ファイアウォールの設定を無効にする場合には、以下に記述する設定を行わなくてもOPCを利用することができます。



2. Windows Firewallが有効になっている場合は、以下の設定を行う必要があります。
 - (1) “コントロールパネル”から“Windows ファイアウォール”を選択し、“例外”タブを選択します。



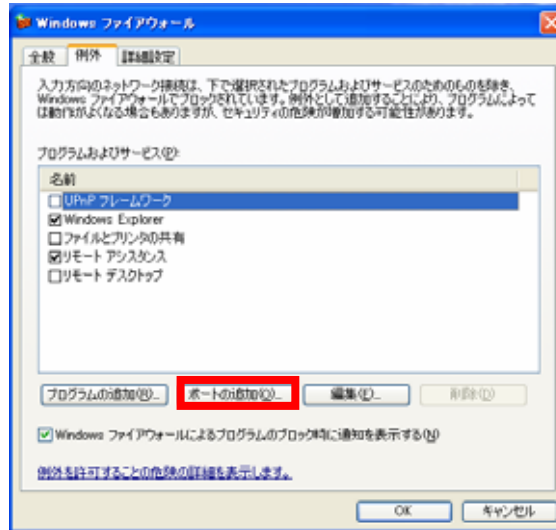
- (2) “例外”タブの“プログラムの追加”をクリックし、例外リストにすべてのOPCクライアント、OPCサーバ、および、Windows¥System32にあるMicrosoft Management Console (mmc.exe)とOPCEnum.exeを追加します。



「プログラムの追加」で、アプリケーションがリストに表示されない場合には、“参照”ボタンを押してアプリケーションを指定してください。

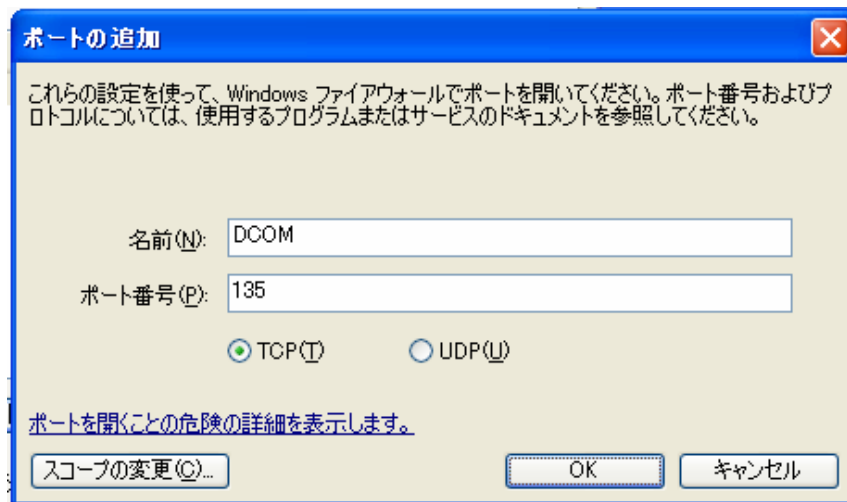
補足：例外リストに追加できるのは、拡張子がexeのファイルのみです。インプロセス(DLLやOCX)のOPCクライアントやOPCサーバを指定する場合には、これら呼び出しているexeファイルのアプリケーションを例外リストに追加します。

- (3) 次に、TCPの135番ポートを追加します。“Windows ファイアウォール”の“例外”タブで“ポートの追加”を選択します。



“ポートの追加”ダイアログで、以下のポートを追加します。

- ・ 名前: DCOM
- ・ ポート番号: 135
- ・ “TCP”のボタンを選択



3 DCOMの機能強化

SP2では、DCOMのセキュリティが強化されています。OPCを利用する場合には、強化された機能の中で次の二点を考慮する必要があります。一つは、コンピュータレベルの制限が追加されたことです。もう一つは、より細かいレベルでのCOMアクセス許可が可能になったことです。

一つ目の、コンピュータレベルの制限について簡単に説明をします。SP2では、コンピュータ上のCOMサーバの呼び出し、アクティブ化、起動毎にコンピュータレベルのアクセス制御リストに対するアクセスチェックが追加されました。これにより、管理者がコンピュータに登録されている全てのCOMアプリケーションのセキュリティ設定をより適切に把握できるようになります。つまり、コンピュータ上のCOMサーバへのアクセスに対して最低限の承認制約が設定されます。このコンピュータレベルのアクセス制御リストには、起動とアクティブ化を処理するための「起動アクセス許可」リストと、呼び出しを処理する「アクセス許可」リストの二つがあります。「起動アクセス許可」は、ネットワーク経由もしくはローカルのどちらの場合についても、COMサーバの起動を許可するユーザを指定します。「アクセス許可」では、起動後のCOMサーバにアクセスを許可するユーザを指定します。この変更により、既定ですべてのユーザにリモート呼び出しのアクセス許可を与えて動作しているCOMサーバの場合、デフォルト設定を変更する必要があります。

補足: Anonymous Logon グループは、Everyone グループのメンバではありません。アカウント名、パスワード、またはドメインを使用せずにネットワークを介してコンピュータとそのリソースにアクセスするすべてのユーザは、Anonymous Logon グループにビルトインされたセキュリティグループのメンバです。Windows の以前のバージョンでは、Anonymous Logon セキュリティグループのメンバには Everyone グループのメンバシップがあったため、多くのリソースにアクセスできました。Windows 2000 システムを Windows XP Professional にアップグレードすると、匿名ユーザは、Everyone グループ (および Anonymous Logon グループとして明示されていないグループ) のアクセス許可エントリを持つリソースを、アップグレード後は利用できなくなります。匿名アクセスが必要な既存のアプリケーションをサポートするためには、匿名アクセスを許可する必要があります。Anonymous logon グループへのアクセスを許可する場合は、Anonymous Logon セキュリティグループとそのアクセス許可を明示的に追加する必要があります。(Windowsのヘルプの「既定のセキュリティ設定の違い」より抜粋)

二つ目のより細かいレベルのアクセス許可とは、COMアクセス許可ポリシーを“距離”の概念を基に柔軟に制御できるようになります。SP2で定義されている距離には、「ローカル」と「リモート」の2種類があります。ローカルは、LRPC プロトコル経由で着信する COM メッセージと定義され、リモートは、TCP などのリモート RPC プロトコル経由で着信する COM メッセージと定義されます。この制御の導入は、RPC 呼び出しがリモート ソースから送られてきたものであることを認識し、その結果、許可するアクセス許可をより限定する (あるいは完全になくす) ことで、ネットワークベースの攻撃リスクを軽減することを狙っているものです。また、SP2では、呼

び出しとアクティブ化のアクセス許可が分離されるように変更され、アクティブ化のアクセス許可が起動アクセス許可のアクセス制御リストに移行されました。これにより、非認証呼び出しアクセスでコールバックをサポートするCOMサーバのサポートを実現しながら、アクティブ化の権利を制約する事で最初のオブジェクト参照を取得できるユーザを制限できます。起動アクセス許可では、「ローカル起動」「リモート起動」「ローカルアクティブ化」「リモートアクティブ化」の4種類があります。

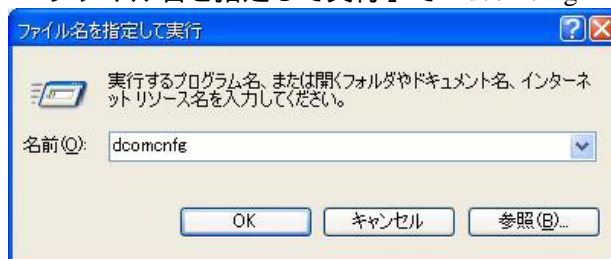
SP2で設定されてデフォルトの制限設定では、ネットワーク経由でOPCを利用することはできません。利用するためには、ユーザあるいはグループに対して、ローカルアクセス許可かリモートアクセス許可(あるいは両方)を設定する必要があります。

3.1 DCOM設定

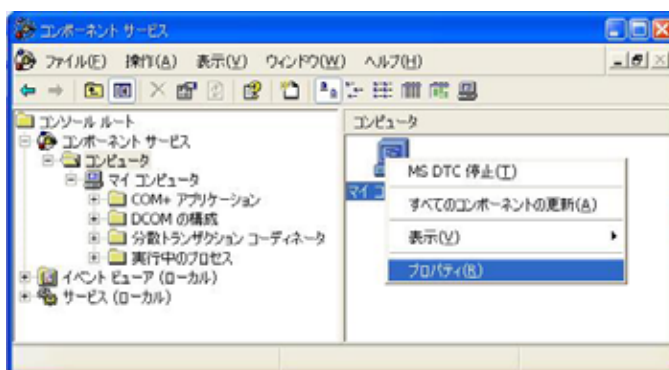
以下のようにDCOMの設定を行う必要があります。

- (1) DCOMCNFG.EXEを起動します。

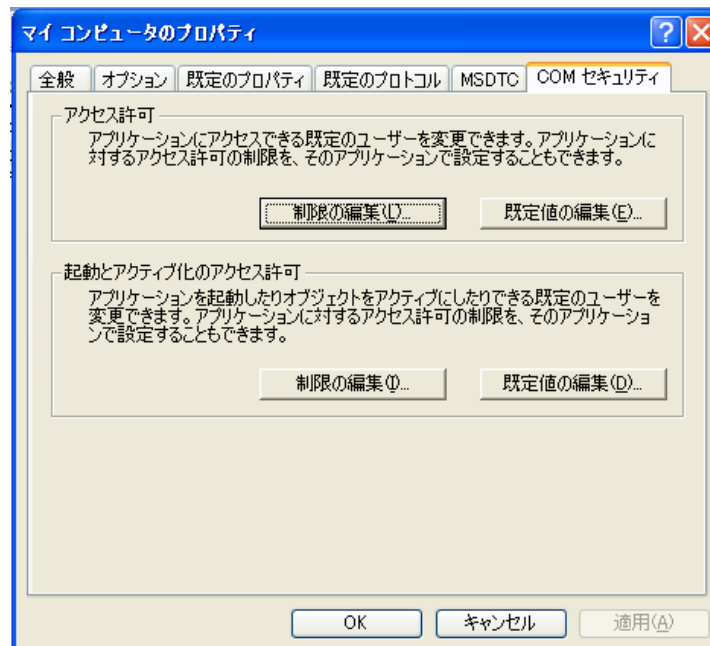
「スタート」 「ファイル名を指定して実行」で “ dcomcnfg ” を起動



- (2) “コンソール ルート”下の“コンポーネント サービス”をクリックします。
- (3) “コンポーネント サービス” 下の“コンピュータ”をクリックします。
- (4) “マイ コンピュータ”上で右クリックし、“プロパティ”を選択します。

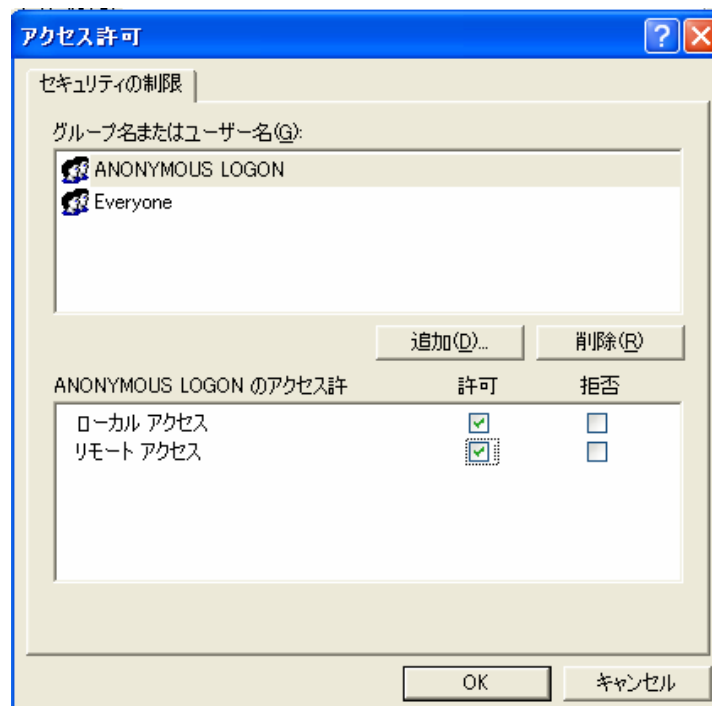


- (5) “COM セキュリティ”タブを選択します。

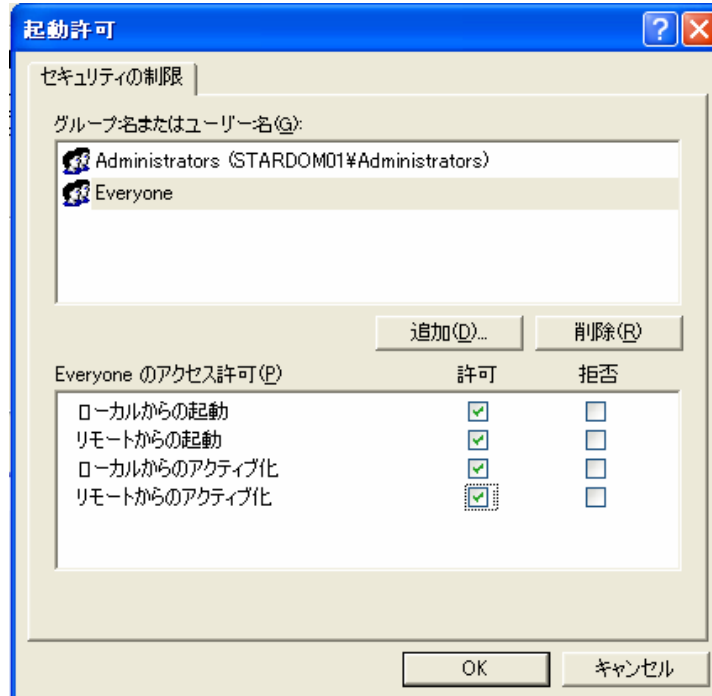


- (6) “アクセス許可”の“制限の編集”をクリックし、“ANONYMOUS LOGON”ユーザに対して、“リモートアクセス”を許可するように設定します。

補足:この設定は、OPCEnumを使用し、匿名アクセスを許可するように“認証レベル”を“なし”に設定しているOPCサーバやOPCクライアントに必要です。ただし、OPCEnumを使用していない場合は、設定の必要はありません。

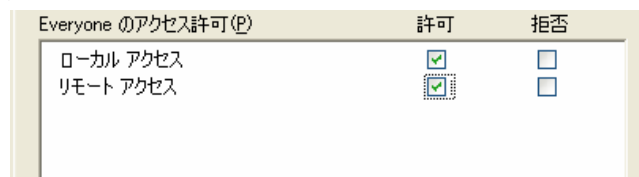


- (7) “起動とアクティブ化のアクセス許可”の“制限の編集”をクリックし、“Everyone”ユーザに対して、“リモートからの起動”および“リモートからのアクティブ化”を許可するように設定します。

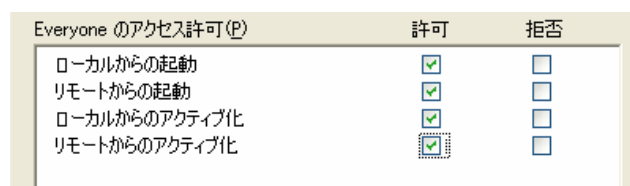


補足: 「Everyone」は全ての認証ユーザを含むので、より小さなユーザグループに許可を設定するのが望ましいです。例えば、「OPC Users」というグループを作成してOPCサーバとOPCクライアントを利用するユーザを登録し、「Everyone」の代わりに「OPC Users」に同様の設定を行います。

- (8) “アクセス許可”の“既定値の編集”をクリックし、OPCの通信に関する各ユーザ(グループ)に対して、ローカルおよびリモートのアクセスを許可するように設定します。



- (9) “起動とアクティブ化のアクセス許可”の“既定値の編集”をクリックし、OPCの通信に関する各ユーザ(グループ)に対して、ローカルおよびリモートのアクセスを許可するように設定します。



本ホワイトペーパーに関する注意

本ホワイトペーパーは、日本 OPC 協議会技術部会で調査を行った最善の方法ですが、日本 OPC 協議会と日本 OPC 協議会技術部会は、本ホワイトペーパーの利用者に対して、記述内容の保証や個々のサポートは行いません。

参考資料

1. TechNet “ Windows XP Service Pack 2 セキュリティ強化機能搭載 IT プロフェッショナルのためのリソース ”
<http://www.microsoft.com/japan/technet/prodtechnol/winxppro/maintain/winxpsp2.mspx>
2. Windows XP Service Pack 2: 開発者向け情報
<http://www.microsoft.com/japan/msdn/windows/windowsxp/securityinxpsp2.asp>
3. Windows XP Service Pack 2 - 開発者向けセキュリティ情報
<http://www.microsoft.com/japan/msdn/security/productinfo/xpsp2>
4. Microsoft Windows XP Service Pack 2 での機能の変更点
<http://www.microsoft.com/japan/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx>
5. オンラインセミナー「Windows XP SP2 の機能紹介」
<http://www.microsoft.com/japan/seminar/windowsxp/sp2/default.mspx>
6. Windows XP Service Pack 2 (SP2) セルフ サポート
<http://support.microsoft.com/WindowsXPSP2>
7. Windows XP Service Pack 2 - Security Information for Developers
<http://msdn.microsoft.com/security/productinfo/XPSP2/default.aspx>
8. Changes to Functionality in Microsoft Windows XP Service Pack 2
<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx>