## LAN 対応版 導入時の注意点

Windows Server 2003 R2 の画面イメージが用意できなかったため、Windows 7 での注意点を参考にしてください。

Oサーバー管理機能を、Windows 7 にインストールした場合、サーバー管理機能の共有フォルダの設定を 行う必要があります。

- ・サーバー管理機能の共有フォルダを手動設定します。
- 手順1)[スタート]メニューの[コンピュータ]をクリックします。
- 手順2) [C:¥Program Files¥ SSS\_Server]フォルダを右クリックしてメニューを表示して、[プロパティ]をクリックします。

(64 ビット版OSの場合は[C:¥Program Files (x86)¥SSS\_Server]フォルダ)



手順3)[共有]タブをクリックします。

」SSS_Serverのプロ	<b>パティ</b> ×
全航 共有 アキュ	リティ 以前のバージョン カスタマイズ
	SSS_Server
種類	ファイル フォルダー
場所:	C:¥Program Files
サイズ:	471 MB (494,390,414 /ኝረጉ)
ディスク上のサイズ:	471 MB (494,432,256 /ናረ ኑ)
内容:	ファイル数: 36、フォルダー数: 7
作成日時:	2011年4月29日、11:34:54
属性: ■	読み取り専用 (フォルダー内のファイルのみXE) 隠しファイル(H) 詳細設定(D)
[	OK         キャンセル         適用(A)

手順4)『詳細な共有』をクリックします。

🖡 SSS_Serverのプロパティ 🛛 💌
全般 共有 セキュリティ 以前のバージョン カスタマイズ
ネットワークのファイルとフォルダーの共有
SSS_Server 共有
ネットワーク パス( <u>N</u> ): ¥¥YSPC101¥SSS_Server
共有( <u>S</u> )
詳細な共有 カスタムのアクセス許可を設定したり、複数の共有を作成したり、その他の詳 細な共有のオブションを設定したりできます。
OK キャンセル 適用(A)

手順5)『このフォルダーを共有する』をチェックします。 「共有名]は『SSS\_Server』と設定して、『アクセス許可』をクリックします。

詳細な共有		×
マレのフォルダーを共有する(S)		
設定		
共有名(日):		
SSS_Server		•
<b>追加(<u>A</u>)</b> 肖耶余( <u>R</u> )		
同時に共有できるユーザー数(L):	20	\$
アクセス許可(P) キャッシュ(C)		
 OK キャンセル		用

手順6)アクセスを許可するユーザーをフルコントロールにします。 ※ ユーザー名が不明な場合は、『追加』ボタンをクリックレて Fu

※ ユーザー名が不明な場合は、	<u>『追加』ボタンをクリック</u>	して、Everyone	を追加して下さい。
💫 HWSvr のアクセス許可			

クルーノ名またはユーサー名(g): 続 Everyone	
	<u> </u>
Everyone のアクセス計可( <u>P)</u> フルコントロール 変更 読み取り	許可 指否
アクセス制御とアクセス許可の詳細を表	<u>示します。</u>

手順7)すべての画面をOKで終了すれば、共有設定は終了です。

・サーバー管理機能フォルダのセキュリティを手動設定します。

手順1) [スタート]メニューの[コンピュータ]をクリックします。

手順 2) [C:¥Program Files¥SSS\_Server]フォルダを右クリックしてメニューを表示して、[プロパ ティ]をクリックします。

(64 ビット版OSの場合は[C:¥Program Files (x86)¥SSS\_Server]フォルダ)

> 🅌 Microsoft.NET	SSS_Server.exe.manifest	
🛚 🍑 MSBuild	SSSDataCnv.exe	
Reference Assemblies	U SSSPOS.ldf	
SSS Server	SSSPOS.mdf	
SESWin	展開(A)	
2 33 a	新しいウィンドウで開く(F)	
Þ 📠 Sun	An other test to character	
퉬 Uninstall Information	共有(H) ▶	
🛯 🎍 Windows Defender	以前のバージョンの復元(V)	
🛛 🛺 Windows Journal	ライブラリに追加(I) ・	
🛛 🏭 Windows Mail	送る(N) ト	
Nindows Modia Dlavor	+TID B1D (T)	1
NetSetup.exe 更新日時:	4/29 9:19	9
アプリケーション サイズ:	$\Box E^{-(C)}$	
	削除(D)	
	名前の変更(M)	
	新規作成(X) ▶	
	プロパティ(R)	
amix		

手順3) [セキュリティ]タブをクリックします。

] SSS_Serverのプロパティ				
全般共有したキュ	リティー以前のバージョン カスタマイズ			
	SSS_Server			
種类頁:	ファイル フォルダー			
場所:	C:¥Program Files			
サイズ:	473 MB (496,690,192 /강イト)			
ディスク上のサイズ:	473 MB (496,734,208 / ٢イト)			
内容:	ファイル数: 36、フォルダー数: 6			
作成日時:	2011年9月23日、13:06:05	_		
属性: 画)	読み取り専用 (フォルダー内のファイルのみ)(B) 隠しファイル(出)			
	OK         キャンセル         適用(	(A)		

## 手順4)『編集』をクリックします。



手順5)アクセスを許可するユーザーをフルコントロールにします。

※ ユーザー名が不明な場合は、『追加』ボタンをクリックして、Everyone を追加して下さい。

🝌 SSS_Server のアクセス許可		×	
セキュリティ			
オブジェクト名: C¥Program Files¥	SSS_Server		
グループ名またはユーザー名(G):			
& Administrators (YSPC101¥Admin	nistrators)	*	
Stressone & Stressone			
& Users (YSPC101¥Users)		=	
& TrustedInstaller		-	
<		•	
	追加(D) i	削除(R)	
Everyone のアクセス許可(P)	許可	拒否	
די ארב ארכ		· ·	
変更			
読み取りと実行			
フォルダーの内容の一覧表示 🔽 🗌			
読み取り 🔽 📼 👻			
アクセス制御とアクセス許可の詳細を表示します。			
ОК	キャンセル	適用(A)	

手順6)すべての画面をOKで終了すれば、セキュリティ設定は終了です。

Oサーバー管理機能を、Windows 7 にインストールした場合、ファイアウォール機能により、クライアントから SSS for Windows (データベース SQLServer)に接続できるように設定する必要があります。

■設定方法

Oファイアウォールの設定にて、SQLServer の通信を許可します。

通信を許可するには、以下のポートとプログラムの受信及び送信を許可する必要があります
① TCP ポート: 1433

- ② UDPポート: 1434

③ プログラム : C:¥Program Files¥Microsoft SQL Server

¥MSSQL10.YSSSDB08¥MSSQL¥Binn¥sqlservr.exe

64 ビット版OSの場合

C:¥Program Files (x86)¥Microsoft SQL Server ¥MSSQL10.YSSSDB08¥MSSQL¥Binn¥sqlservr.exe

以下に、①の受信規則を追加する方法を示しますので、①~③について、受信および送信規則の両方を 追加してください

手順1)[スタート]メニューの[コントロールパネル]から[システムとセキュリティ]をクリックします。



手順2) [Windows ファイアウォール]をクリックします。



手順3) [詳細設定]をクリックします。



手順4) [受信規則]を右クリックして、[新しい規則]をクリックします。



## 手順5) [ポート]を選択して、次へ進みます。

🔐 新規の受信の規則ウイザー	- ř				
規則の種類	規則の種類				
作成するファイアウォールの規則の	種類を選択してください。				
ステップ	ビハ45×雨ハ4月日は大/たま1 キマカック				
● 規則の種類	この場合が100%が11名したりからならりいい				
<ul> <li>フロトコルおよびホート</li> <li>操作</li> </ul>					
● プロファイル					
● 名前	● ホートロー TGP または UDP ポートの接続を制御する規則です。				
	◎ 事前定義(E):				
	BranchCache - コンテンツ取得 (HTTP を使用)				
	Windows エクスペリエンスのために接続を制御する規則です。				
	◎ <b>カスタム(C)</b> カスタムの規則です。				
	規則の種類の詳細を表示します				
	< 戻る(B) (次へ(N) > キャンセル				

手順6) [TCP(T)]を選択、[特定のローカルポート]に1433を入力して、次へ進みます。

②の UDP を追加する場合は、ポート番号は 1434 となります。

🔐 新規の受信の規則ウイザー	۳	×
プロトコルおよびポート		
この規則を適用するプロトコルとポ	ートを指定してください。	
ステップ:		
● 規則の種類	TCP と UDP のどちらにこの規則を適用しますか?	
● プロトコルおよびポート		
◎ 操作	© UDP(U)	
● プロファイル		
◎ 名前	すべてのローカル ボートと特定のローカル ボートのどちらを対象にこの規則を適用するかを選択し てください。	
	🔿 ታላፒውፅ	
•	● 特定のローカル ポート(S): 1488	
	フロトコルとボートの詳細を表示します。	
	< 戻る(B) / 次へ(N) > ) キャンセル	,

手順7) [接続を許可する]を選択して、次へ進みます。

🔐 新規の受信の規則ウイザード 🛛 🗾				
操作				
規則で指定された条件を接続が満	<b>誌</b> をす場合に、実行される操作を指定します。			
7				
<ul> <li>         ・ 規則の種類         ・     </li> </ul>	接続が指定の条件に一致した場合に、どの操作を実行しますか?			
<ul> <li>プロトコルおよびボート</li> </ul>				
◎ 操作	● 接続を許可するIAI fr-su-を使用して保護された接続と保護されていない接続の両方を含みます。			
● プロファイル	◎ ヤをっリティで保護されている場合のみ接続を許可する((*)			
● 名前	IPsecを使用して認証された接続のみを含みます。接続は、IPsecプロパティ内の設定と接続 わたっしティ相則ノード内の規則を使用して、わたっしティ保護されます。			
	カスタマイズ( <u>Z</u> )			
	◎ 接続をブロックする(K)			
	操作の詳細を表示します			
	〈 同ろ( R) 、 ケヘ( N) 〉 また、 セル			

手順8)	すハ	ヾてチェック	を入れた状態で、	次へ進みます。
------	----	--------	----------	---------

🔐 新規の受信の規則ウイザ	– ۲
<b>プロファイル</b> この規則が適用されるプロファイ。	レを指定してください。
ステッナ:         規則の種類         プロトコルおよびボート         操作         プロファイル         名前	この規則はいつ適用しますか?
	< 戻る(B) 次へ(M) > キャンセル

手順9) 規則に名前をつけて、次へ進みます。 名前は任意です。例) SQLServer TCP 1433 など

- ※現の啓信の規則ウノザード		
この規則の名前と説明を指定してくたさい。		
ステップ		
● 規則の種類		
● ブロトコルおよびポート		
● 操作		
<ul> <li>プロファイル</li> </ul>	名前(N):	
● 名前	SQLServer TCP 1433	
	説明 (オプション)(D):	
	〈戻る(B) 完了(F) キャンセンション (F) キャンセンション (F) キャンセンション (F) キャンセンション (F)	216

以上で①の受信規則が追加されました。

同様の処理で、①~③について、受信及び送信規則を追加してください。

※ セキュリティソフトがファイアウォール機能を持っている場合は、クライアントから SSS for Windows で接続しようとすると、サーバー側で『接続を許可しますか?』などとメッセージが 表示される場合があります。その時は『常に許可をする』設定にする事でクライアントからの接 続が可能になります。

また、セキュリティソフトが自動的にブロックしている場合もありますので、その時は、セキュ リティソフトの設定にて、①~③のブロックを解除してください。