

# 賃貸名人の通信をファイアウォールに許可させる (ウィルスバスター)

**《**Microsoft SQL Server 2005**》** 

以下の手順は、賃貸名人(Microsoft SQL Server 2005)の通信が『トレンドマイクロ ウ ィルスバスター』のファイアウォール機能にブロックされ、クライアント(子機)からの 接続に障害が発生した場合にご利用いただきます。

〔目次〕	
■ 『ウィルスバスター2010 の設定』	2
■ 『ウィルスバスター2011 クラウド』の設定	14

(クリックすると該当のページにジャンプします)

#### ■ 『ウィルスバスター2010の設定』

※以下の手順は、サーバ(親機)にてウィルスバスター2010のファイアウォール機能が「有効」に設定されている運用環境を対象としています。

※以下の手順は、Microsoft SQL Server 2005 (2007 年 4 月 リリース以降の賃貸名人に同梱)をご利用の場合の設定です。

### (1) ポート番号の確認 ※サーバ(親機)で作業します

1. スタートメニューより [すべてのプログラム]  $\rightarrow$  [Microsoft SQL Server 2005]  $\rightarrow$  [構成ツール]  $\rightarrow$  [SQL Server 構成マネージャ] をクリックします。



※以下のメッセージが表示された場合は、[続行] ボタンをクリックします。

ユーザー アカウント制御
💎 続行するにはあなたの許可が必要です
あなたが開始した操作である場合は、続行してください。
Microsoft 管理コンソール Microsoft Windows
✓ 詳細( <u>D</u> ) 続行(C) キャンセル
ユーザー アカウント制御は、あなたの許可なくコンピュータに変更が適用 されるのを防ぎます。

2. 「SQL Server 構成マネージャ」が起動しますので、左ウィンドウにて[SQL Server 2005 ネットワークの構成]→[DANGONET のプロトコル]と展開し、右ウィンドウにて[TCP/IP] を右クリックし、[プロパティ] をクリックします。

🙀 SQL Server Configuration Manager			
ファイル(F) 操作(A) 表示(V) ヘルプ(H) (中 🔿 🖄 🗐 🗟 🛛			
<ul> <li>SQL Server 構成マネージャ (ローカル)</li> <li>SQL Server 2005 のサービス</li> <li>▲ <u>9</u>. SQL Server 2005 ネットワークの構成</li> <li>■ DANGONET のプロトコル</li> <li>▶ <u>9</u>. SQL Native Client の構成</li> </ul>	プロトコル名 す 共有メモリ す 名前付きパイプ す TCP/IP す VIA	<ul> <li>状態</li> <li>有効</li> <li>有効</li> <li>無効</li> </ul>	有効化(E) 無効化(I) プロパティ(R) ヘルプ(H)
選択した項目のプロパティ ダイアログ ボックスを	開きます。		

3. **[TCP/IP**のプロパティ] ウィンドウで、**[IP** アドレス] タブを選択し、「**TCP** 動的ポ ート」項目に表示されているポート番号を確認します(以下の例では「<u>**49879**</u>」がポート番 号です)。

プロ	אבאנ 🛛 אבאנ			
	IP アドレス	fe80::5efe:192.168.1.185%12	^	
	TCP ポート			
	TCP 動的ポート	0		
	アクティブ	(はい		
	有効	いいえ		
	IP6			
	IP アドレス	fe80::ffff:fffe%8		
	TCP ポート			
	TCP 動的ポート	0		
	アクティブ	はい		
	有効	いいえ	-	
	IPAII		-	
	TCP ポート			
	TCP 動的ポート	49879	-	
TCP 動的ポート 動的ポートが無効な場合は空白。動的ポートを使用するには、0 に設定します。				

以上でポート番号の確認は完了です。

## (2) ウィルスバスター2010の設定 ※サーバ(親機)で作業します



1. タスクトレイのアイコンを右クリックし、[メイン画面を起動]をクリックします。

2. メインウィンドウで、[パーソナルファイアウォール] を選択し、右ウィンドウにて [設 定] をクリックします

	スノ(スタ=2010	■ ×
マイコンピュータ	ホームネットワーク管理	? ヘルプとお問い合わせ先
<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	▲ パーソナルファイアウォール( ネットワークからの不正アクセン 現在のプロファイル: 社内ネッ セキュリティレベル:中	と) √有効 スや攻撃からコンピュータを保護します。 トワーク
()) パーソナル ファイアウォール	マネットワーク接続状況 (緊急ロ	ック)(N) 正常 (接続されています)
図 有害サイト/ 迷惑メール対策		
🔅 契約更新その他		
その他のッー	ıı	

3. [パーソナルファイアウォール]ウィンドウで、[詳細設定]ボタンをクリックします。

パーソナルファイアウォール		x
<ul> <li>パーソナルファイアウォー コンピュータ外部からの 報は「プロファイル」とし</li> </ul>	ー <b>ルを有効にする(A)</b> 不正侵入や、コンピュータ内部から して保存されます。	のデータ流出などを防止します。設定情
現在のプロファイル: <u>胤</u>	社内ネットワーク	
	初期設定に	戻す( <u>D</u> ) ブロファイルの変更( <u>P</u> )
セキュリティレベル		
高中 中 低 最小限	<ul> <li>ネットワークウイルスの攻撃を</li> <li>受信: 例外設定されていない場合は</li> <li>送信: 例外設定されていない場合は</li> <li>※信頼するプログラムのリスト( 場合は、送受信とも警告を表示し 告を表示)</li> </ul>	ンブロック 常に警告を表示 に警告を表示 こ安全なプログラムとして登録されている っない (情報がない場合は、送受信とも警
		詳細設定( <u>S</u> )
<ul> <li>ネットワーク接続環境</li> <li>ネットワーク投続環境</li> </ul>	党の変更を自動的に認識する( <u>W</u> ) 出システムを有効にする( <u>E</u> )	
②この画面の説明(出)		<u>O</u> K キャンセル( <u>C</u> )

4. [プロファイルの詳細設定] ウィンドウで、[例外ルール (プロトコル)] タブを選択し、 [追加] ボタンをクリックします。

プロファ	マイルの詳細設定					×
	トワーク情報 例外ルール	プログラム	) 例外ルール C	7akaw) 🕇	ロキシ	
パーン ェアガ この機	パーソナルファイアウォールは、アクティブなすべてのネットワークプロトコルを監視し、スパイウ ェアが使用している疑いのあるプロトコルを拒否することで、コンピュータとの通信を制御します。 この機能をカスタマイズするには、次のリストを使用します。					
追加	(A) 編集(E) 削除(	<u>R)</u>				
状況	説明	方向	処理	IPアドレスの	カ プロトコル	<u> </u>
	メール送信 <mark>(</mark> SMTP)	送信	許可	IPv4/v6	TCP	=
	メール受信 (POP3)	送信	許可	IPv4/v6	TCP	
	Webサービス (HTTP)	送信	許可	IPv4/v6	TCP	
	Secure Webサービス (	送信	許可	IPv4/v6	TCP	~
	ファイル転送プロトコ	送信	許可	IPv4/v6	TCP	
	Telnet	送信	許可	IPv4/v6	TCP	
	SSH	送信	許可	IPv4/v6	TCP	~
	DNS	送信	許可	IPv4/v6	TCP/UDP	
	Network News Transfe.	…送信	許可	IPv4/v6	TCP	
	AOL接続 (送信)	送信	許可	IPv4/v6	TCP	-
٠ 📃					۱.	
: : : : : : : : : : : : : : : : : : :	<ul> <li>⑦ この画面の説明(H)</li> <li>①K</li> <li>キャンセル(C)</li> </ul>					

5. [例外ルールの追加または編集] ウィンドウが表示されます。

例外ルール (パー	ソナルファイアウォールネット	ワーク) の追加また	たは編集 ×
説明( <u>D</u> ):	新規例外ルール (プロトコル)		
方向:	◎ 受信(I) 💿 送信(G)		
処理:	◎ 許可(L) ◎ 拒否(K)	◎ 警告(W)	
プロトコル( <u>P</u> ):	TCP 🔹		
ポート:	<ul> <li>● すべてのポート(<u>S</u>)</li> <li>● 指定のポート(<u>E</u>)</li> </ul>		例:10, 15, 20-30
タイプ( <u>Y</u> ):	すべてのIPアドレス <ul> <li>● IPv4およびIPv6</li> <li>● IPv4</li> <li>● IPv6</li> </ul>	•	
(?) この画面の!!	税 <sup>8</sup> 月( <u>H</u> )		<u>Q</u> K キャンセル( <u>C</u> )

6. [例外ルールの追加または編集] ウィンドウで、「送信」用の設定を行います。変更点は 以下の通りです。

説明 :「SQL Server (DANGONET) 送信」に変更

方向 :「**送信**」を選択

ポート:「指定のポート」を選択し、(1)で確認したポート番号を入力(この例では「49879」)

例外ルール (パー	ソナルファイアウォールネットワーク)の追加または編集 X
説明( <u>D</u> ):	SQL Server (DANGONET) 送信
方向:	○ 受信(I)  ● 送信(G)
処理:	● 許可(L) ○ 拒否(K) ○ 警告(W)
プロトコル( <u>P</u> ):	TCP -
ポート:	<ul> <li>● すべてのポート(<u>S</u>)</li> <li>● 指定のポート(<u>E</u>)</li> <li>49879</li> <li>例:10, 15, 20-30</li> </ul>
タイプ( <u>Y</u> ):	<ul> <li>すべてのIPアドレス ▼</li> <li>◎ IPv4およびIPv6</li> <li>◎ IPv4</li> <li>◎ IPv6</li> </ul>
? この画面の説	8月(H) <u>OK</u> キャンセル(C)

変更が完了しましたら、[OK] ボタンをクリックします。

7. [プロファイルの詳細設定] ウィンドウに「送信」用の設定が反映されたことを確認し、 再び[追加] ボタンをクリックします。

プロファ	イルの詳細設定				x	
রিভা	・ワーク情報 例外ルール (プログラム	↓ 例外ルー	и∉анаи)	プロキシ		
パーソ エアが この機	パーソナルファイアウォールは、アクティブなすべてのネットワークプロトコルを監視し、スパイウ ェアが使用している疑いのあるプロトコルを拒否することで、コンピュータとの通信を制御します。 この機能をカスタマイズするには、次のリストを使用します。					
状況	説明	方向	処理	IPアドレスの	D 🔺	
	SQL Server (DANGONET) 送信	送信	許可	IPv4/v6		
	メール送信 (SMTP)	送信	許可	IPv4/v6		
	メール受信 (POP3)	送信	許可	IPv4/v6	-	
	Webサービス (HTTP)	送信	許可	IPv4/v6		
	Secure Webサービス (HTTPS)	送信	許可	IPv4/v6	-	
	ファイル転送プロトコル (FTP)	送信	許可	IPv4/v6	-	
	Telnet	送信	許可	IPv4/v6	-	
	SSH	送信	許可	IPv4/v6		
	DNS	送信	許可	IPv4/v6	-	
	Network News Transfer Protocol (N	L 送信	許可	IPv4/v6	· •	
•	III				4	
<u>ැ</u> _ උ	<ol> <li>この画面の説明(H)</li> <li>QK</li> <li>キャンセル(C)</li> </ol>					

8 [例外ルールの追加または編集] ウィンドウで、「受信」用の設定を行います。

説明 :「SQL Server (DANGONET) 受信」に変更

方向 :「**受信**」を選択

ポート:「指定のポート」を選択し、(1)で確認したポート番号を入力(この例では「49879」)

例外ルール (パー	ソナルファイアウォールネットワーク) の追加または編集	x
説明( <u>D</u> ):	SQL Server (DANGONET) 受信	
方向:	<ul> <li>● 受信(I)</li> <li>● 送信(G)</li> </ul>	
処理:	<ul> <li>● 許可(L)</li> <li>● 拒否(K)</li> <li>● 警告(W)</li> </ul>	
プロトコル( <u>P</u> ):	TCP -	
ポート:	◎ すべてのポート( <u>S)</u>	
	⑧ 指定のポート(E) 49879 例:10, 15, 20-30	
タイプ( <u>Y</u> ):	すべてのIPアドレス ▼	
	<ul> <li>IPv4およびIPv6</li> </ul>	
	◎ IPv4	
	◎ IPv6	
② この画面の診	旭明( <u>H</u> ) <u>Q</u> K キャンセル(	<u>C</u> )

変更が完了しましたら、[OK] ボタンをクリックします。

9. [プロファイルの詳細設定] ウィンドウに「受信」用の設定が反映されたことを確認し、 [OK] ボタンをクリックします。

プロファ	イルの詳細設定				x	
নিলা	・ワーク情報 例外ルール (プログラム	↓ 例外ルー	ル(プロトコル)	プロキシ		
パーソ: ェアが この機能	パーソナルファイアウォールは、アクティブなすべてのネットワークプロトコルを監視し、スパイウ ェアが使用している疑いのあるプロトコルを拒否することで、コンピュータとの通信を制御します。 この機能をカスタマイズするには、次のリストを使用します。 追加(A) 編集(E) 削除(R)					
状況	説明	方向	処理	₽アドレスの	. 🔺	
	SQL Server (DANGONET) 受信	受信	許可	IPv4/v6		
	SQL Server (DANGONET) 送信	送信	許可	IPv4/v6		
	メール送信 (SMTP)	送信	許可	IPv4/v6	•	
	メール受信 (POP3)	送信	許可	IPv4/v6	· · · · ·	
	Webサービス (HTTP)	送信	許可	IPv4/v6		
	Secure Webサービス (HTTPS)	送信	許可	IPv4/v6		
	ファイル転送プロトコル (FTP)	送信	許可	IPv4/v6	· · · · · · · · · · · · · · · · · · ·	
	Telnet	送信	許可	IPv4/v6		
	SSH	送信	許可	IPv4/v6		
	DNS	送信	許可	IPv4/v6	· •	
•					•	
ಾ ವರು	画面の説明(日)			<u>0</u> K	キャンセル( <u>C</u> )	

10. [パーソナルファイアウォール] ウィンドウで、[OK] ボタンをクリックします。

パーソナルファイアウォール	×		
<ul> <li>パーソナルファイアウォール</li> <li>コンピュータ外部からの不正報は「プロファイル」として</li> </ul>	<b>を有効にする(A)</b> 侵入や、コンピュータ内部からのデータ流出などを防止します。設定情 保存されます。		
現在のプロファイル: <u>凧</u> 社	タネットワーク		
	初期設定に戻す(D) ブロファイルの変更(P)		
セキュリティレベル			
□ 高 - 中 - - 低 - 最小限 <sup>2</sup> -	<ul> <li>ネットワークウイルスの攻撃をブロック</li> <li>受信: 例外設定されていない場合は常に警告を表示</li> <li>送信: 例外設定されていない場合は常に警告を表示</li> <li>※信頼するプログラムのリストに安全なプログラムとして登録されている 場合は、送受信とも警告を表示しない (情報がない場合は、送受信とも警告を表示)</li> </ul>		
	書¥細語定( <u>S</u> )		
<ul> <li>ネットワーク接続環境の変更を自動的に認識する(W)</li> <li>ネットワーク攻撃検出システムを有効にする(E)</li> </ul>			
②この画面の説明(出)			

以上でウィルスバスター2010の設定は完了です。

# (3) SQL クライアント設定ユーティリティ (cliconfg)の設定

## ※<u>クライアント (子機)</u>で作業します

1. [Windows] ( )キー+ [R] キーで、[ファイル名を指定して実行] ウィンドウが表示されます。

□ ファイル名を指定して実行
<ul> <li>実行するプログラム名、または開くフォルダーやドキュメント名、インターネットリソース名を入力してください。</li> <li>名前(Q):</li> </ul>
OK キャンセル 参照( <u>B</u> )

2. [ファイル名を指定して実行] ウィンドウで、「名前」項目に「**cliconfg**」と入力し、[OK] ボタンをクリックします

□ ファイル名を指定して実行
<ul> <li>実行するプログラム名、または開くフォルダーやドキュメント名、インターネットリソース名を入力してください。</li> <li>名前(<u>0</u>): cliconfg</li> </ul>
OK キャンセル 参照( <u>B</u> )

 SQL クライアント設定ユーティリティ」が起動しますので、[別名] タブを選択し、 [追加] ボタンをクリックします。

▲ SQL クライアント設定ユーティリティ	×
全般 別名 DB-Library オブション   ネットワーク ライブラリ	
サーバー別名の設定(N)	
サーバー別名 ネットワークラ… 接続パラメーター	
	追加( <u>D</u> )
	削除( <u>R</u> )
	編集( <u>E</u> )
OK キャンセル 適用	(A)(A)

4. [ネットワーク ライブラリ設定の追加] ウィンドウが表示されます。

🕼 ネットワーク ライブラリ設定の追加	1	×
サーバー別名(A):		
<ul> <li>ネットワーク ライブラリ</li> <li>○ 名前付きパイプ(P)</li> <li>○ TOP/IP(T)</li> <li>○ マルチブロトコル(M)</li> <li>○ NWLink IPX/SPX(X)</li> <li>○ AppleTalk(K)</li> <li>○ Banyan VINES(Y)</li> </ul>	接続パラメーター サーバー名(S): パイプ名(E):	  ¥¥¥pipe¥sql¥query
○ その他(②)		OK キャンセル ヘルプ

5. [ネットワーク ライブラリ設定の追加] ウィンドウで、ご運用の環境に合わせて設定を 行います。変更点は以下の通りです。

ネットワーク ライブラリ:「**TCP/IP**」に変更

サーバー別名 : 「[サーバーのコンピュータ名]¥dangonet」(例:server¥dangonet)
 あるいは
 「[サーバーの IP アドレス]¥dangonet」(例:192.168.0.2¥dangonet)
 を入力

接続パラメーター:「サーバー名」項目は「サーバー別名」と同一であることを確認 「ポートを動的に決定する」チェックを外す

「ポート番号」項目に(1)で確認したポート番号を入力(例:「49879」)

📢 ネットワーク ライブラリ設定の追加		X
■「「「「」」「「「」」「「」」「」」「」」「」「」」「」」「」」「」」「」」「	server¥dangonet	
<ul> <li>ネットワーク ライブラリ</li> <li>         ◆ 急討はまい(イブ(P)     </li> <li>         で TCP/IP(T)     </li> <li>         の TCP/IP(T)     </li> <li>         で TCP/IP(T)     </li> <li>         の TCP/IP(T)     </li> <li>         で TCP/IP(T)     </li> <li>         の TCP/IP(T)&lt;</li></ul>	- 接続パラメーター サーバー名(S): □ ポートを動的に決定する( <u>D</u> ) ポート番号( <u>R</u> ):	server¥dangonet
	ОК	キャンセル ヘルプ

変更が完了しましたら、[OK] ボタンをクリックします。

6. [SQL クライアント設定ユーティリティ]ウィンドウに設定が反映されたことを確認し、 [OK] ボタンをクリックします。

🔺 SQL クライアント設定ユーティリティ	×
全般 別名 DB-Library オプション ネットワーク ライブラリ	
サーバー別名の設定( <u>N</u> )	
サーバー別名 ネットワーク ラ 接続 バラメーター	
	ietn(D)
	肖/除( <u>R</u> )
	編集(E)
	 ۷   میلیخ

以上で SQL クライアント設定ユーティリティの設定は完了です。クライアントからの接続 をご確認ください。

#### ■ 『ウィルスバスター2011 クラウド』の設定

『ウィルスバスター2011 クラウド』は、独自のファイアウォール機能を持たず、Windows に付属する『Windows ファイアウォール』を用います。

従いまして、賃貸名人の通信障害が発生した場合、『ウィルスバスター2011 クラウド』で はなく、『Windows ファイアウォール』を設定する必要があります。

『Windows ファイアウォール』の設定手順に関しては FAQ: 18001 をご参照ください。