

JU-FUDE TOT

サーバー接続時の ウィルスセキュリティソフト設定手順書



<u>(詳細)編</u>

1 ESET Smart Securityの設定

1. ESET Smart Securityを起動し、左側のリストから[設定]を選択し、標準モードの場合は 「詳細モード」に切り替えます。

ESET Smart Security		
ESET Smart Se	ecurity 4	
 保護の状態 コンピュータの検査 アップデート 設定 ヘルプとサポート 	設定 ユーザー名とパスワードを入力 ③ ホットワークコンピュータの 保護モードを変更す ③ 一時的に ウイルス・スパイウェア対策 を無効は ③ 一時的にパーソナル ファイアウォールを無効は	る ① こする ① こする ④ 可能にします。
	詳細モードへ切り替え	詳細モードへ切り替え
表示: 標準モード 変更…		we protect your digital worlds

2. [パーソナルファイアウォール]をクリックします。

ESET Smart Security					
ESET Smart Se	ב-ש-אלי-אלי ב-ש-אלי-אליביבים ב-שי-אליבים	-ス(<u>U</u>) ▼	設定⑸▼	Ÿ-ル □ ▼	∧,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
✓ 保護の状態 ○ コンピュータの検査	🔆 設定				
 アップデート 設定 ウイルス・スパイウェア対 パーソナルファイアウォー 迷惑メール対策機能 ジール 	ウイルス・スパイウェア対策 保護 リアルタイムファイルシステム保護 電子メールクライアント保護 Webアクセス保護 パーソナルファイアウォール ベットリーク畑にフィルタリング 迷惑メール対策機能 電子メールクライアント保護	 ✓ 有效 ✓ 有效 ✓ 有效 ✓ 有效 			
	アップデートするためのユーザー名とパスワードをみ プロキシサーバを設定する 設定をインポートおよびエクスポートする 詳細設定のツリー全体を表示する	、力する…			
表示: 詳細モード 変更…			we prote	ct your digital w	orlds (eset

3. [パーソナルファイアウォールの詳細設定]をクリックします。



4. [フィルタリングモード]で「例外付きの自動モード」を選択して「OK」をクリックします。

ESET Smart Security	? ×
設定	eser
 電子メールクライアント アクション POP3、POP3S Webアクセス(保護 HTTP、HTTPS コンピュータの検査 防除外 プロトコルフィルタリング パーンナルファイアウォール 学習モード ルールとゾーン IDSと詳細オプション アグリケーション(に対する変更の検 システム統合 接続表示 迷惑メール対策機能 電子メールクライアント(保護 アップテート ツール ログファイル 隔離 スケジューラ 警告と通知 	パーソナルファイアウォール フィルタリングモード(E) 例外付きの自動モード(ユーザー定義ルール) ・ **** *******************************

5. [ルールとゾーンの設定]をクリックします。

ESET Smart Security	
ESET Smart Se	ユーザーインタフェース山・設定国・ツールロ・ヘルプ山・ ecurity 4
 マップデート アップデート 設定 ウイルス・スパイウェア対… パーソナルファイアウォ… 送惑メール対策機能 ジール 	ネットワーク通信フィルタリング ③ ✓ 有効 ◎ すべてのネットワーク通信を遮断する:ネットワーク接続をしない ④ ◎ フィルタリングをしない:すべての通信を許可する ④ 例外付きの自動フィルタリングモード ③ ✓ 有効 ◎ 対話型フィルタリングモードへ切り替え ルールとゾーンの設定… → ケーレーン - クの保護モードの変更… ④
ペルプとサポート 表示:詳細モード 変更	パーソナルファイアウォールの詳細設定… we protect your digital worlds (ESE)

6. [詳細表示(すべてのルールを表示)に切り替え]をクリックします。

ノーンとルールの設定				
ルール ゾーン				
ルールでは、ネットワーク通信をファイアウォールでどのように処 信を許可するか遮断するかを設定できます。 ループの詳細	理するかを定義します。特 こついては、ここをクリックして	注定のアプリケーション、リ 【ください。	モートコンピュータ、および	特定のポートについて、通
詳細表示(すべてのルールを表示)に切り替え				
次のプロ:	ファイルで使用するルールを	表示する:	্রন্থ	•
アプリケーション/ルール	信頼ゾーン <mark>(</mark> 内)	信頼ゾーン(外)	インターネット <mark>(</mark> 内)	インターネット(外)
■・アプリケーションが割り当てられていない場合のルー	ル目固有	三固有	目間有	■固有 ▲
Windows サービスのホスト フロセス Windows Logon User Interface Host	三回月	三回月	三 回 月 三 固 有	三回月 三固有
■ ■サービスとコントローラー アプリケーション	■固有	■固有	■固有	■固有
E Indexe ログオン アプリケーション	三固有	三固有	三固有	三固有
新規(N) 編集(<u>E</u>) 削除(Del)(<u>D</u>)				
			😚 OK(O) 🛛 🕹 🕈 ヤ.	ンセル(C) 🔋 🚱 適用(A)

7. [新規]をクリックします。

ע–	ンとバ	レールの設定								
\mathcal{V}	·-ル	ゾーン								
	ルール 信を許	では、ネットワー - 可するか渡断	ーク通信を さるかを副	ファイアウォー 設定できます	-ルでどのように処理す 。 ルールの詳細につい	おかを定義しま いては、「こをクリ	す。特定のアプ ックLinください。	リケーション、リモ	ートコンピュータ、および 特定の	ポートについて、通
	<u>アプリク</u>	<u>アーションツリー</u>	。 表示に切	<u>い</u> 起ここの。 り <u>替え</u>	0 // /////////////////////////////////		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
					次のプロファイ	ルで使用するル	ールを表示する	:	ৰশব	-
	名前		アク	プロト	アドレス	ローカルボ	リモートポート	アプリケーション	,	ว้อวราน 📩
	v	すべての 	1	тср	すべて	すべて	すべて	すべて		=
		すべての	1	тср	すべて	すべて	すべて	すべて		
		開始され	+	тср	すべて	すべて	すべて	すべて		
	1	ローカル	+	тср	IP: 127.0.0.1	すべて	すべて	すべて		
	1	בטציד 	14	тср	IP: 127.0.0.1	すべて	すべて	Windows	サービスのホスト プロセス	
	v	בטלב	1	UDP	IPサブネット 22	すべて	すべて	Windows	サービスのホスト プロセス	
	v	בטלב	14	тср	IP: 127.0.0.1	すべて	すべて	Windows	Logon User Interface H	
	1	仮想ネッ	+	тср	ローカルアドレス;	すべて	すべて	すべて		
	v	DHCPを	14	UDP	すべて	67 - 68	67 - 68	Windows	サービスのホスト プロセス	
	V	DHCP东	45	LIDP	すべて	67 - 68	67 - 68	■1 サービスと1	<u> 1) トローラー アプリケーション</u>	*
l	•	/	/							P
	新	·規(<u>N</u>)	編集(E)	训除(Del)(<u>D</u>)					
C										

8. 次の項目を入力します。

- 1 [名前]ボックスに、「SQL Browser」と入力します。
- 2 [方向]オプションの選択を、「内向き」に設定します。
- 3 [アクション] ボックスを、「許可」
- ④ [プロトコル]ボックスを、「UDP」に設定します。
- [プロファイル]ボックス「すべて」になっていることを確認
- 6 [ローカル]タブで「ポートの追加」から番号「1434」を入力して、[OK]をクリックします。

ルールの編集:	ルールの編集:
一般 ローカル リモート	一般 ローカル リモート
ルールの概要 名前(U): 1 SQL Browser 方向(D): 2 内向き アクション(A) 3 許可 フロトコル: (E 4 UDP フロファ 5 すべて 7 フロトコルの選択(S) フロファ 5 すべて 7 フロ・ 追加アクション ログに記録(L) ユーザー(こ通知する(U)	□-カルボート
ー般: 方向:内向き アクション:許可 プロトコル:UDP プロファイル	ー般: 方向:両方 アクション:許可 プロトコル: UDP プロファイル:すべて
リモート側: すべて	リモート側: すべて
ローカル側: ポート: Ms-SQL-m (1434)	ローカル側: ポート: Ms-SQL-m (1434)
アプリケーション: すべて	アプリケーション: すべて 6
OK(O) [OK(2) (**>\text{vision}

サーバー接続時のESET Smart Securityの設定手順書(ESET Smart Securityの設定)

- 9. 再度、「新規」ボタンより次の項目を入力します。
 - 1 [名前]ボックスに、「SQL Server Express」と入力します。
 - 2 [方向]オプションの選択を、「内向き」に設定します。
 - 3 [アクション] ボックスを、「許可」
 - ④ [プロトコル]ボックスを、「TCP」に設定します。
 - 5 [プロファイル]ボックス「すべて」になっていることを確認
 - ⑥ [ローカル]タブで「ポートの追加」から番号「1435」を入力して、[OK]をクリックします。

ルールの編集:	ルールの編集:
一般 ローカル リモート	-般 ローカル リモート
ルールの概要 名前(N): 1 30L Server Express 方向(D): 2 内向き ・ アクション(A): 3 許可 ・ ブロトコル (P 4 TCP 7ロトコルの選択(S) ブロファ・5 すべて ・ ブロト 追加アクション ログに記録(L) 2 - ザー(ご通知する(U)	□-カルボート ポートの違加(A)… ポートの選択 アプリケーション 番号(B): 1435 説明: (C) キャンセル(C)
ー般: 方向:内向き アクション:許可 プロトコル:TCP プロファイル	一般: 方向: 内向き アクション: 許可 プロトコル: TCP プロファイル: すべて
リモート側: すべて	リモート側: すべて
ローカル側: ボート: 1435	ローカル側: ポート: 1435
アプリケーション: すべて	アプリケーション: すべて 6
OK(0)	<u> </u>

10. 再度、「新規」ボタンより次の項目を入力します。

- 1 [名前]ボックスに、「BTXAMTS」と入力します。
- 2 [方向]オプションの選択を、「内向き」に設定します。
- 3 [アクション] ボックスを、「許可」
- ④ [プロトコル]ボックスを、「TCP」に設定します。
- 5 [プロファイル]ボックス「すべて」になっていることを確認
- ⑥ [ローカル]タブで「ポートの追加」から番号「8103」を入力して、[OK]をクリックします。

新規ルール:	新規ルール:
一般 ローカル リモート	一般 ローカル リモート
ルールの概要 名前(<u>い</u>): 1 BTXAMTS 方向(<u>D</u>): 2 内向き ・ アクション(<u>4</u> 3 詳可 ・ フロトコルの選択(S) フロス 5 すべて ・ フロ	□-カルポート ポートの道加(A) ポートの選択 アプリケーション 番号(B): 8103 説明: OK(O) キャンセル(C)
一般: 方向:内向き アクション:許可 プロトコル:TCP プロファイ, リモート側:すべて ローカル側:すべて	 一般: 方向:内向き アクション:許可 プロトコル: TCP プロファイル:すべて リモート側:すべて ローカル側:ポート: 8103 アプリケーション:すべて
OK(<u>O</u>)	ОК(O) * *>±лиС)

11. プロテクトがSNS-LANのときのみ行ってください

再度、「新規」ボタンより次の項目を入力します。

- 1 [名前]ボックスに、「SNS-LAN」と入力します。
- 2 [方向]オプションの選択を、「内向き」に設定します。
- ⑧ [アクション] ボックスを、「許可」
- 4 [プロトコル]ボックスを、「UDP」に設定します。
- [プロファイル]ボックス「すべて」になっていることを確認

6 [ローカル]タブで「ポートの追加」から番号「5093」を入力して、[OK]をクリックします。

ルールの編集:	ルールの編集:
 一般 □-カル リモート ルールの概要 名前(<u>D</u>): 2 内向き ▼ アクション(A) 3 許可 ▼ プロトコル・(E 4 UDP プロトコルの選択(S)_ プロファ 5 すべて ▼ 追加アクション ログに記録(<u>L</u>) ユーザー(ご通知する(<u>U</u>) 	一般 ローカル リモート ローカルボート ボートの追加(A) ボートの選択 2 アブリケーション 名前(1): 名前(1): <<<ボートの選択 >> 番号(1): 5093 説明: 〇K(0) キャンセル(C)
 一般: 方向:内向き アクション:許可 プロトコル: UDP プロフ リモート側:すべて ローカル側:ボート: 5093 アプリケーション:すべて OK(0) 	 一般: 方向: 内向き アクション: 許可 プロトコル: UDP プロファイル: すべて リモート側: すべて ローカル側: ポート: 5093 アプリケーション: すべて OK(0) キャンセル(<u>C</u>)

12. 1 [SQL Browser]、「SQL Server」、「BTXAMTS」、にチェックが付いていることを確認してください。 チェックがついていない場合はチェックを付けてください。

2 確認できたら、[OK]をクリックします。

・ンとルー	ールの設定								
/-// Y	バーン								
ルールで	は、ネットワー	り通信を	ファイアウォ	ールでどのように処	理するかを定義しま	す。特定のアプ	リケーション、リモ	ニートコンピュータ、および 特定	のポートについて、通
信を許可	「するか遮断」	するかを読	と定できます	。 ルールの詳細は	こついては、 <u>ここ</u> をクリ	ックしてくだざい。			
<u> </u>	ージョンツリーオ	を示してい	<u>) 替え</u>	<u>አ</u> ምጋር በር	ァイルで使用するル	ールを表示する		ৰ্নাত	•
5 34			-0-1						-0 (.)
名胢		Y0	705	7562	ローカルボ	リモートボート	アプリケーション	,	70771/
✓ 1	信頼ゾー	+	UDP	信頼ゾーン	3540	すべて	Windows	サービスのホスト プロセス	
V	外向きの	1	UDP	すべて	すべて	3702	すべて		
V [内向きの	+	UDP	すべて	3702	すべて	すべて		
V (ekrn検証	1	тср	すべて	すべて	DNS (53)	ESET Ser	rvice	
V	リモート管	1	TCP	すべて	すべて	2222	ESET Ser	rvice	
V _	TEANING	*	TCD	オペア	±∧"7	DNS (53)	C ESET GU	I	
V 5	SQL Bro	₽	UDP	すべて	Ms-SQL	すべて	すべて		
V 3	SQL Ser	₽	TCP	すべて	1435	すべて	すべて		-
V 6	BTXAMTS	₽	ТСР	すべて	8103	すべて	すべて		=
•									
新規	1(<u>N</u>)	編集(<u>E)</u> [i	削除(Del)(<u>D</u>)					
								() OK(U) キャンセル	(C) 🔋 () () () () () () () () () () () () ()

13. 画面右上の[×]をクリックして、設定を終了します。

ESET Smart Se	curity 4	97 ± −ス(<u>U</u>) •	設定(S) ▼ ツール	
 保護の状態 コンピュータの検査 	🔆 設定			
 アップデート 設定 ウイルス・スパイウェア対… パーソナルファイアウォー… 迷惑メール対策機能 ジール 	ウイルス・スパイウェア対策 保護 リアルタイムファイルシステム保護 電子メールクライアント保護 Webアクセス保護 パーソナル ファイアウォール ネットワーク通信フィルタリング 迷惑メール対策機能 電子メールクライアント保護	 ✓ 有効 ✓ 有効 ✓ 有効 ✓ 有効 		
ペルプとサポート	アップデートするためのユーザー名とパスワー プロキシサーバを設定する 設定をインポートおよびエクスポートする 詳細設定のツリー全体を表示する	ドを入力する…		

14. クライアントインストールされているPCの現場管理を起動し、サーバー現場が起動すれば完了です。