## Norton Internet Security 設定方法について(参考)

以下に Norton Internet Security 2003 の設定方法を説明します。

Norton Internet Security 2003 を起動後、ファイアウォールを選択して画面右下の「設定」を選択します。

🏐 Norton Internet Security 📃 🗔 🗙			
🥃 セキュリティモニタ 🕜 🤤 通信	言の速断( <u>A</u> ) <mark>(愛)LiveUpdate</mark>	🛃 オフ%ョン@	() ^µ7°( <u>H</u> ) →
Norton Internet Security	システムの状態: 問	題ありません 🥝	)
状態と設定( <u>S</u> ) 🚽	🧭 セキュリティ	オン	ファイアウォール
警告レベル(⊻)	🧭 ファイアウォール	オン	ファイアウォールはコンピュ ータを確認のないアクセ
統計①	❷ 侵入検知	オン	人がら1条渡します。
更新サービス( <u>B</u> )			
	🧭 プライバシー制御	オン	
	🔥 広告ブロック	オフ	
		オン	<u>無効にする</u>
			設定
Symantec. Norton Internet Security <sup>™ 2003</sup>			

画面右上の「拡張」を選択し、「一般ルール」を選択します。

🏐 Norton Internet Security 🛛 🔀
ファイアウォール プログラム制御 ホームネットワーク 拡張
拡張ファイアウォール
ファイアウォールで特定の種類のインターネットトラフィックをどう扱うかを設定します。 ほとんどのユーザーはこれらの設定を変更する必要はありません。
ファイアウォールはルールのセットを使ってコンピュータの保護のしかたを制御します。ファイアウォー ルは発着信するすべてのデータをこれらのルールと自動的に比較してその情報を遮断または許 可します。
→般ルールはネットワークの基本的な機能性を定義してコンピュータをインターネットの既知の危険性から保護します。これらのルールはすべてのインターネットプログラムに適用されます。 →般ルール(g)
トロイの木馬ルールは不適切なアクセスを許可にする悪質なアプリケーションからコンピュータを保 護します。
トロイの木馬ルール(工).
OK

画面下の「追加」を選択します。

🏐 一般ルール 💌
一般ルール
説明の表示
このルールは、どのようにファイアウォールが送受信する接続を扱うかを判断します。リストの上位 にまテキれているルールがその下のルールトロを頂先します
✓ 記叩
■ デフォルトインバウンド ICMP ■ デマ,方向:インバウンド,コンピュータ:任意,通信:特定,プロトコル:ICMP ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
✓ 場 デフォルトアウトバウンド ICMP 許可,方向:アウトバウンド,コンピュータ:任意,通信:任意,プロトコル:ICMP
✓ ● デフォルトインバウンド DNS 許可,方向:インパウンド,コンピュータ:任意,通信:特定,プロトコル:UDP
✓ 男→男 デフォルトアウトバウンド DNS 許可,方向:アウトバウンド,コンピュータ:任意,通信:特定,プロトコル:TCPとUDP
▲ 追加 修正 削除 上に移動 下に移動
OK キャンセル

「許可」を選択し、「次へ」を選択します。

	🥞 ルールの追加
	ルールの追加
	説明の表示
	新しい接続を許可、遮断、あるいは監視しますか?
<	◎ 許可: このルールに一致する接続を許可します。
	○ 追断: このルールに一致する接続を遮断します。
	○ 監視: このルールに一致する接続をログに記録します。これを見ればこのルールを使った回数を監 視できます。
	< 戻る (次へ ) キャンセル

「他のコンピュータに対する接続」を選択し、「次へ」を選択します。

🔮 ルールの追加
ルールの追加
説明の表示
どの種類の接続を許可しますか?
他のコンピュータに対する接続 インターネットを使うアプリケーションのほとんどが確立する接続の種類です。アウトバウンド接続と もいいます。
○ 他のコンピュータからの接続 Web サーバーまたは FTP サーバーなどのサーバーアプリケーションでよく使う接続の種類です。インバウンド接続ともいいます。
○ 他のコンピュータに対する接続と他のコンピュータからの接続 両方の接続の種類 (インバウンドとアウトバウンド)を利用するアプリケーションもあります。
〈 戻る 〈 次へ 〉 キャンセル

許可するコンピュータを設定します。必要に応じて設定を行って下さい。この例では「任 意のコンピュータ」選択しています。「次へ」を選択して下さい。

🌍 ルールの追加					×
				JU-	ルの追加
-			NY Z	<u>a</u> ~/	説明の表示
[ <b>60</b> ]. <b>1</b> . <b>1</b>	. / . + = + -	+ 40 0		1 3	
とのコンピュータまたはつ	ゴトを計 可しま !	9 7.D ?		12	
● 任意のコンピュータ	>		- A.		
○ 下のリストにあるコンビ	ュータとサイトのみ				
					111/
追加	削除				
[アダプタ]をクリックすると	特定のネットワーク	アダプタに対する対	通信を限定できま は日本のユネオ	ます。この操作	が必要な
0141761-862714	エのネットワークア	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	い病音ののです。	)	
アダプタ					
-					
			z Vro	× ×	العليدين
				- +	ヤノセル

許可するプロトコルと、通信の種類またはポートを設定します。プロトコルは「TCP」、 通信の種類またはポートは、「下のリストにある通信の種類またはポートのみ」を選 択します。その後、「追加」を選択して下さい。

🌗ルールの追加	×
	ルールの追加
	説明の表示
どのブロトコルを <mark>許可</mark> し	ょますか?
© TCP	
O UDP	
O TOP と UDP	
CICMP	
どの種類の通信または	はボートを許可しますか?
○すべての種類の	通信(すべてのポート、ローカルとリモート)
🔍 下のリストにある	通信の種類またはポートのみ
	<b>V</b>
追加	前除
	< 戻る 次へ > キャンセル

フィルタを行う通信の週類ポートを指定します。フィルタは「リストにある既知のポート」 選択し、場所は「リモート」を選択します。通信の種類は、「ポート:389、名前:ldap」 を選択します。その後、「OK」を選択して下さい。

🌍 ポートを指	定	×
		ポートを指定
		説明の表示
フィルタ:		場所:
<b>○</b> リフ	いたにある既知のポート	
〇個	別に指定するポート	© IJE−ト
<u>о</u> ж.		
		ARZ
<u>  - / ポート</u>	名前	
🗆 <sup>194</sup>	irc	aka , Internet Relay Chat Protocol 🔎
□ <sup>213</sup>	ipx	aka , IPX over IP
<b>№</b> <sup>389</sup>	ldap	aka , Lightweight Directory Access 💻 Protocol
	https · ·	aka MCom 🗨
	ОК	キャンセル

「リモート Idap (ポート 389)」が追加されたことを確認し、「次へ」を選択します。

🌍 ルールの追加		×
	JL	ールの追加
		説明の表示
どのブロトコルを許可し	」ますか?	
⊙ TOP		
O UDP		
O TOP と UDP		
⊂ IC MP		
どの種類の通信または	はポートを許可しますか?	
○すべての種類の	通信(すべてのポート、ローカルとリモート)	
◎ 下のリストにある	)通信の種類またはポートのみ	1
リモート Idap け	Ҟ−ト 389)	
追加	削除	
	〈 戻る ( 次へ 〉)	キャンセル

設定したルールに一致した場合の通知方法を設定します。任意に設定して下さい。設定 後「次へ」を選択して下さい。

🌍 ルールの追加
ルールの追加
説明の表示
接続がこのルールに一致するときに通知するオブションを選択できます。
接続がルールに一致したら:
1 回じたイベントが起きた後でログのみに記録する
□ セキュリティチェカメッセージで通知する
く 戻る ( 次へ > キャンセル

設定したルールに名前をつけます。任意の名前を設定して下さい。以下の例では「LDAP」 という名前で設定しています。設定後「次へ」を選択して下さい。

🌍 ルールの追加	×
	ルールの追加
	説明の表示
<b>このルールにどんな名</b> 前 この説明はこのルールを調 LDAP	<b>京をつけますか?</b> 散別できるようにルールの概略リストに表示されます。
	< 戻る (次へ >) キャンセル

設定した内容が表示されます。内容を確認して「終了」を選択します。

🌍 ルールの追加	×
	ルールの追加
インターネット通信を	可するために次のルールを作成しました。対象は このコンピュータ:
説明: LDAP	
処理:許可	
方向: アウトバウンド	
」)21-% 任息 通信: 特定	
プロトコル: TCP	
	< 戻る 🧹 終了 🔵 キャンセル

設定したルール(LDAP)の内容が表示されていることを確認して、「OK」を選択して下さい。

●●一般ルール	×
一般ルール 説明の表示	
このルールは、このようにファイアウォールが足文信争る後後を扱うがを判断しよう。ラストの工业 に表示されているルールがその下のルールよりも優先します。	
✓   記印月	
■ EPMAPの デフォルト達断 連時,方向:インバウンド,コンピュータ:任意,通信:特定,プロトコル:TCPとUDP,追 跡中:ログエントリを作成します	
☑ ■●● UPNP ボート 5000 達断ルール 連騎,方向: イン/アウト,コンピュータ:任意,通信:特定,プロトコル: TCP	
☑ ■ UPNP ボート 1900 達断ルール 連続,方向: インバウンド,コンピュータ:任意,通信:特定,プロトコル: UDP	
✓ 場→ LDAP 許可,方向:アウトバウンド,コンピュータ:任意,通信:特定,プロトコル:TCP	
追加 修正 削除 上に移動 下に移動	
OK キャンセル	

以上で設定は終了です。