

# アプリケーション・コントロール 設定手順書



ウォッチガード・テクノロジー・ジャパン株式会社 2014 年 8 月 Rev-01

## 目次

はじめに	3
Application Control アクセス制御設定	4
アプリケーション単体のアクセス制御	4
カテゴリ毎のアクセス制御	8
Application Control のポリシーへの適用	9
Application Control を有効にしたポリシーのスケジュール	10
おわりに	12

- 2012 年 3 月 初版
- 2014 年 8 月 第二版

## はじめに

この度はウォッチガード製品を選定していただきありがとうございます。

本書は、WatchGuard XTM が持つ強力な機能の一つである、アプリケーション・コントロールの設定方法を 解説するものです。

本手順書は、Fireware XTM OS v11.5.1 をベースとしたものです。

#### Application Control アクセス制御設定

Application Control は先ず、アプリケーション(Web、P2P、IM など)毎に許可・禁止設定をするための定義 が必要となります(デフォルトは全て許可)。

定義が完了したら、各ポリシーに対して Application Control の有効/無効設定して頂きます。

尚、アプリケーションによって制御項目が異なるのでご注意ください。

アプリケーション単体のアクセス制御

- 1. Policy Manager の[セキュリティサービス] ⇒ [Application Control] 画面を開きます。
- 2. 一覧にあるデフォルト(Global)を選択して画面右側にある"編集"で修正画面を開きます。

-	R Application Control アクション	/		×
	アクション ポリシー			
	7021-21		41121-	
	Global		805-	
				複製…
				·····································
L				
L				
L				
L				
L				
L				
L				
L				
L				
L				
L				
	署名バージョン4.170 サーバー	- の更新		
			<u>о</u> к = +ャンセル	<u>^107</u>

3. Application Control でサポートしているアプリケーション一覧が表示されます。

アクセス制御したいアプリケーションを探す方法としては、下記の3種類があります。

- スクロールダウンして探す
- カテゴリを選択して、カテゴリ内から探す
- 検索機能を使って検索する

Application Control	アクション(事前定義済)		X
名前: Global			
● すべてのアプリケ~ ● 構成済みアプリケ~	-ションを表示 -ションのみを表示 カテゴ	J: বিশ্ব	▼ (検索:
カテゴリ	アプリケーション	動作	アクション
Business	Altiris	Access	<u>^</u>
Business	AMS	Access	
Business	Apache Synapse	Access	
Business	Avamar	Access	
Business	Avaya	Access	
Business	BackupExec	Access	
Business	Backweb	Access	
Business	Big Brother	Access	
Business	Bugzilla	Authority	
Business	BZFlag	Access	
Business	CAJO	Access	
Business	Cisco HSRP	Access	
Business	Citrix	Access	
Business	CodeMeter	Access	
Business	concur	Authority	
Business	Convoq	Access	
Business	Corba	Access	
Business	CPanel	Authority, Access	
Business	Cups	Access	
Business	Cvsup	Access	
Rusiness	Dame\//are	Communicate	
カテゴリ別で選択 アプリケーションが一番	次しない場合: 接続を許可	•	アクションをクリアする <b>編集</b>
			<u>OK</u> キャンセル ヘルブ

4. 例として、"YouTube"を制御したい場合、検索機能を使って"Youtube"にて検索すると一覧に表示されま す。一覧に表示された"Youtube"をダブルクリックまたは画面右下にある"編集"を選択することで詳細な 制御項目画面が表示されます。

🔣 Application Control アクショ	ン(事前定義済)				
名前· Global					
	ait 47.				
● すべてのアプリケーションを: ● ■ □===================================	表示				
◎ 構成済みアフリケーションの	みを表示 カテゴリ: ◙	147	▼ 換索: youtube		
カテゴリ	アプリケーション	動作	アクション		
Streaming Media	Youtube	Authority, Access			
カテゴリ別で選択			アクションをクリアする 編集		
アプリケーションが一致しない場	合: 接続を許可	•			
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,					
		<u> </u>			

5. "Youtube"(例)は、2つの制御項目があります。"Access"(アクセス)と"Authority"(認証)の2項目があります。

全体をブロックしたい場合は下記の画面通りにしてください。



"Authority"(認証)のみ禁止にしたい場合は、下記の画面通りにして下さい。

下記の通りにすることで、閲覧が可能になるが"Youtube"への動画投稿が禁止となります

(理由:YouTube はログイン認証をしないと動画投稿が出来ないため)。



※制御項目はアプリケーションによる異なるのでご注意ください。

個別アプリケーション毎の制御ではなく、カテゴリ毎に大きい枠での制御も可能です。

#### カテゴリ別で選択 ボタンをクリックします。

村: Global				
月:				
)すべてのアプリケーションを表示				
構成済みアプリケーションのみを表示	カテゴリ: すべて	▼ 検索:		
テゴリ アプリケー	-ション 動作	アクション		
siness Altiris	Access		<u> </u>	
siness Apache Sy	ynapse Access			
siness Avamar	Access			
siness Avaya siness BackupExe	ec Access			
siness Backweb	Access			
siness Big Brothe siness Bugzilla	r Access Authority			
siness BZFlag	Access			
siness CAJO	Access			
siness Citrix	Access			
siness CodeMeter	Access			
isiness Convoq	Access			
siness Corba	Access			
siness CPanel siness Cups	Authority, Ac Access	ccess		
Cvsup	Access		-	
siness DameWare カテゴリ別で達起	Communicate	・ アクションをクリアする 編集		
		4117		
フリケーションが一致しない場合: 接筆	☆を許可 ▼			
\		<u>O</u> K <u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>		
カテゴリ別で選択				
カテゴリ別で選択 アプリケーション別のアクミ	ッョンはカテゴリのアク	ションに優先されます。		
カテゴリ別で選択 マ <b>ブリケーション別のアク</b> 5 「 Business	<b>ションはカテゴリのアク</b> 切断 →	ションに優先されます。 同 Bypass Proxies and Tunnels	切断	
カテゴリ別で選択 アブリケーション別のアクS 回 Business	<b>&gt;ョンはカテゴリのアク</b> 切断 <del>▼</del>	ションに優先されます。	切断	
カテゴリ別で選択 ア <b>ブリケーション別のアク</b> S Business Database	ジョンはカテゴリのアク 切断 <del>-</del> 切断 <del>-</del>	ションに優先されます。 Bypass Proxies and Tunnels     File Transfer		
カテゴリ別で選択 アブリケーション別のアクS Business Database Games	ジョンはカテゴリのアク 切断 ← 切断 ←	ションに優先されます。	切断 切断 切断	
カテゴリ別で選択 ア <b>ブリケーション別のアク</b> S Business Database Games	ジョンはカテゴリのアク 切断 ← 切断 ← 切断 ←	ションに優先されます。	<ul> <li>切助斤</li> <li>切助斤</li> <li>切助斤</li> </ul>	
カテゴリ別で選択 ア <b>ブリケーション別のアク</b> S Business Database Games Mail and Collaboration	> ョンはカテゴリのアク 切断 - 切断 - 切断 - 切断 -	ションに優先されます。	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 ア <b>ブリケーション別のアク</b> S Business Database Games Mail and Collaboration	ジョンはカテゴリのアク 切断 - 切断 - 切断 - 切断 -	ションに優先されます。 Bypass Proxies and Tunnels     File Transfer     Instant messaging     Mobile	切断 切断 切断 切断	
カテゴリ別で選択 ア <b>ブリケーション別のアク</b> S Business Database Games Mail and Collaboration	ジョンはカテゴリのアク 切断 ▼ 切断 ▼ 切断 ▼ 切断 ▼	ションに優先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 アブリケーション別のアクS Business Database Games Mail and Collaboration Network Management	ションはカテゴリのアク 切断 の断 の断 マ 切断 マ 切断	ションに優先されます。 ② Bypass Proxies and Tunnels ③ File Transfer ③ Instant messaging ③ Mobile ③ Network Protocols	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 ア <b>ブリケーション別のアク</b> S Business Database Games Mail and Collaboration Network Management	ションはカテゴリのアク 切断 の断 の断 の断 の断 ー	ションに優先されます。 Bypass Proxies and Tunnels     File Transfer     Instant messaging     Mobile     Network Protocols	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 アブリケーション別のアクS Business Database Games Mail and Collaboration Network Management	ションはカテゴリのアク         切断         切断         切断         切断         切断         切断         切断	ションに優先されます。 <ul> <li>Bypass Proxies and Tunnels</li> <li>File Transfer</li> <li>Instant messaging</li> <li>Mobile</li> <li>Network Protocols</li> <li>Private Protocol</li> </ul>	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 アブリケーション別のアクS Business Database Games Mail and Collaboration Network Management V P2P	ションはカテゴリのアク         切断         切断         切断         切断         切断         切断         切断         切断	ションに優先されます。 <ul> <li>Bypass Proxies and Tunnels</li> <li>File Transfer</li> <li>Instant messaging</li> <li>Mobile</li> <li>Network Protocols</li> <li>Private Protocol</li> </ul>	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 マブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management	ションはカテゴリのアク 切断  - 切断  - 切断  - 切断  - 切断  - 切断  - 切断 - 切断 - 切断 - 切断 - 切断 - 切断 - 切断 - 切断 - 切断 - 切断 - 切断 - 切断 - 切断 - 切断 - の の - の - の - の - の - の - の - の - の - の - の - の - の - の - の - の - -	ションに優先されます。 ② Bypass Proxies and Tunnels ③ File Transfer ③ Instant messaging ③ Mobile ③ Network Protocols ③ Private Protocol	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 マブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management ジ P2P Remote Access Termina	ションはカテゴリのアク         切断         調可	ションに優先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 マブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management ジ P2P Remote Access Termina	ジョンはカテゴリのアク         切断         調許可	ションに優先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 アブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management ジ P2P Remote Access Termina	ションはカテゴリのアク         切断         ブ町         切断	ションに優先されます。 <ul> <li>Bypass Proxies and Tunnels</li> <li>File Transfer</li> <li>Instant messaging</li> <li>Mobile</li> <li>Network Protocols</li> <li>Private Protocol</li> <li>Security Update</li> <li>Stock Market</li> </ul>	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 マブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management ジ P2P Remote Access Termina	ションはカテゴリのアク         切断         卸断         卸断	ションに優先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update Stock Market	<ul> <li>切断</li> </ul>	
カテゴリ別で選択 マブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management ジ P2P Remote Access Termina	ションはカテゴリのアク         切断	ションに優先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update Stock Market	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 P ブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management V P2P Remote Access Termina Social Network Streaming Media	ジョンはカテゴリのアク         切断	ションに優先されます。 <ul> <li>Bypass Proxies and Tunnels</li> <li>File Transfer</li> <li>Instant messaging</li> <li>Mobile</li> <li>Network Protocols</li> <li>Private Protocol</li> <li>Security Update</li> <li>Stock Market</li> <li>Voice over IP</li> </ul>	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 マブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management ジ P2P Remote Access Termina Social Network Streaming Media	ジョンはカテゴリのアク         切断	ションに優先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update Stock Market Voice over IP	<ul> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> <li>切断</li> </ul>	
カテゴリ別で選択 P ブリケーション別のアクS Business Database Games Mail and Collaboration Network Management V P2P Remote Access Termina Social Network Streaming Media	ションはカテゴリのアク         切断         ・         切断	ションに破先されます。 <ul> <li>Bypass Proxies and Tunnels</li> <li>File Transfer</li> <li>Instant messaging</li> <li>Mobile</li> <li>Network Protocols</li> <li>Private Protocol</li> <li>Security Update</li> <li>Stock Market</li> <li>Voice over IP</li> <li>Web IM</li> </ul>	<ul> <li>切断</li> </ul>	
カテゴリ別で選択 アブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management ジ P2P Remote Access Termina Social Network Streaming Media Web / Web 2.0	ジョンはカテゴリのアク         切断	ションに 破先 されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update Stock Market Voice over IP Web IM	<ul> <li>切断</li> </ul>	
カテゴリ別で選択 マブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management ジ P2P Remote Access Termina Social Network Streaming Media Web / Web 2.0	ションはカテゴリのアク         切断	ションに破先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update Stock Market Voice over IP Web IM	切断	
カテゴリ別で選択 P ブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management V P2P Remote Access Termina Social Network Streaming Media Web / Web 2.0	ジョンはカテゴリのアク         切断	ションに破先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update Stock Market Voice over IP Web IM	七刀趾斤	
カテゴリ別で選択 P ブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management V P2P Remote Access Termina Social Network Streaming Media Web / Web 2.0	ジョンはカテゴリのアク         切断	ションに優先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update Stock Market Voice over IP Web IM	<ul> <li>切断</li> </ul>	
カテゴリ別で選択 P ブリケーション別のアクラ Business Database Games Mail and Collaboration Network Management P2P Remote Access Termina Social Network Streaming Media Web / Web 2.0	ジョンはカテゴリのアク         切断	ションに破先されます。 Bypass Proxies and Tunnels File Transfer Instant messaging Mobile Network Protocols Private Protocol Security Update Stock Market Voice over IP Web IM	<ul> <li>切断</li> </ul>	

制御したいカテゴリにチェックを入れて、"切断"を指定することにより該当するカテゴリ内に含まれるアプリ ケーションを全てアクセス禁止にすることが可能です。

ただし、細かい制御はできません。カテゴリによる制御は許可か禁止のみとなります。細かい制御に関して はアプリケーション毎に設定して頂く必要があります。 Application Control のポリシーへの適用

最終的に各ポリシーに対して Application Control を有効にしなければアクセス制御はされません。当手順書では、"Outgoing"ルール(ポリシー)に対して Application Control を有効にする方法をお知らせします。

1. Policy Manager 上に登録されている"Outgoing"ルールのプロパティを開いてください。

<b>駅</b> 編集 ポリシーのプロパティ	×
名前: Outgoing	☑ 有効
ポリシー プロパティ 詳細	
TCP-UDP 接続を	
FTOP RSTの送信 WARE	· · · · · · · · · · · · · · · · · · ·
Any-Trusted	
	<b>追加</b> 編集 削除
Any-External	
アウトバンド非 IPSec トラフィックのルーティング方法の選択:	₩ 30 • • • • • • • • • • • • • • • • •
■ ポリシー ペースのルーティングの使用 External □ フェールオーバー 構成	•
▼ Application Control を有効にします: ○ このポリシーの IPS を有効にします プロキシ アクション: □ 「Control を有効にします □ Global □ For Promotion Group ■ For Sales and Technical Gro ■ ●	
(	<u>OK</u> キャンセル ヘルブ

Application Control で作成したルールをプルダウンメニューで選択します。ここで指定したルールがファイア ウォールポリシーに対して適用されます。

※ 送信元を限定することにより、送信元別(部署/PC単位)に Application Control のルールを分けて適 用することが可能です。 Application Control を有効にしたポリシーのスケジュール

スケジュールはポリシーのオプション機能です。ポリシーに対してスケジュール設定をすることで、 Application Control が有効となっているポリシーを時間帯によって有効/無効にすることが可能です。

1. Policy Manager で Application Control が有効となっているポリシーをダブルクリックしてプロパティ画面 を開きます。[詳細]タブを開いてください。

同画面に"スケジュール"の設定項目欄があり標準では"Always On(常に有効)"になっています。スケジュール設定をしたい場合には編集ボタンをクリックして下さい。

🧗 編集 ポリシーのプロパティ	<b>X</b>
名前: TCP-UDP	☑ 有効
ポリシー プロパテー 詳細	
スケジュール: Always On 🕞 💽 💽	
トラフィック管理: (釈定 (制限なし) 🔹 📷 🍉	
·接続速度 (bps)	
制限なし	▼
🥅 容量を超えたらアラームで知らせる	通知
iCMP エラー処理	
グローバル設定の使用 ▼ ICMPの設定	
NAT QoS 固定接統	
両方のルールでトラフィックが制限される場合は 1-1 NAT が優先されます。	
☑ 1-1 NAT (ネットワーク NAT 設定の使用)	
☑ 動的 NAT	
◎ ネットワーク NAT 設定の使用	
◎ このプロキシのすべてのトラフィック	
ソース ℙの設定	
	<u>OK</u> キャンセル ヘルプ

 Application Control を有効にしたポリシーの有効時間を選択します。最小で15分単位、最大で1時間 単位で指定が可能です。



### おわりに

アプリケーション設定手順書をご活用いただき、ありがとうございます。

このガイドを通して、ウォッチガード製品により、アプリケーションの社内利用の制御がいかに容易か、実感していただけたと思います。

WatchGuard XTM が御社のセキュリティにお役に立てれば幸いです。