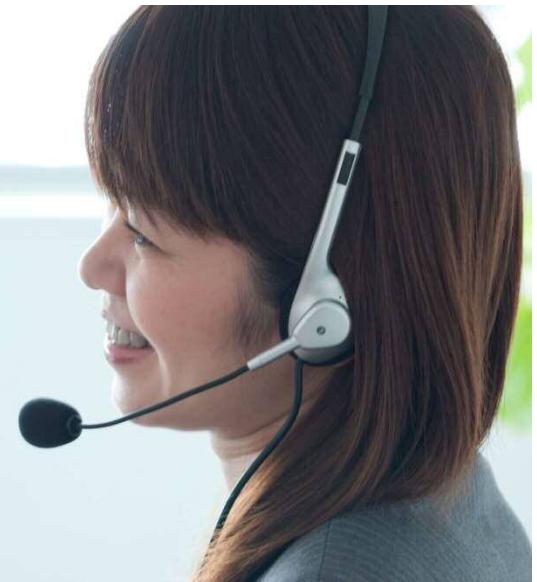




アプリケーションコントロール例外設定マニュアル

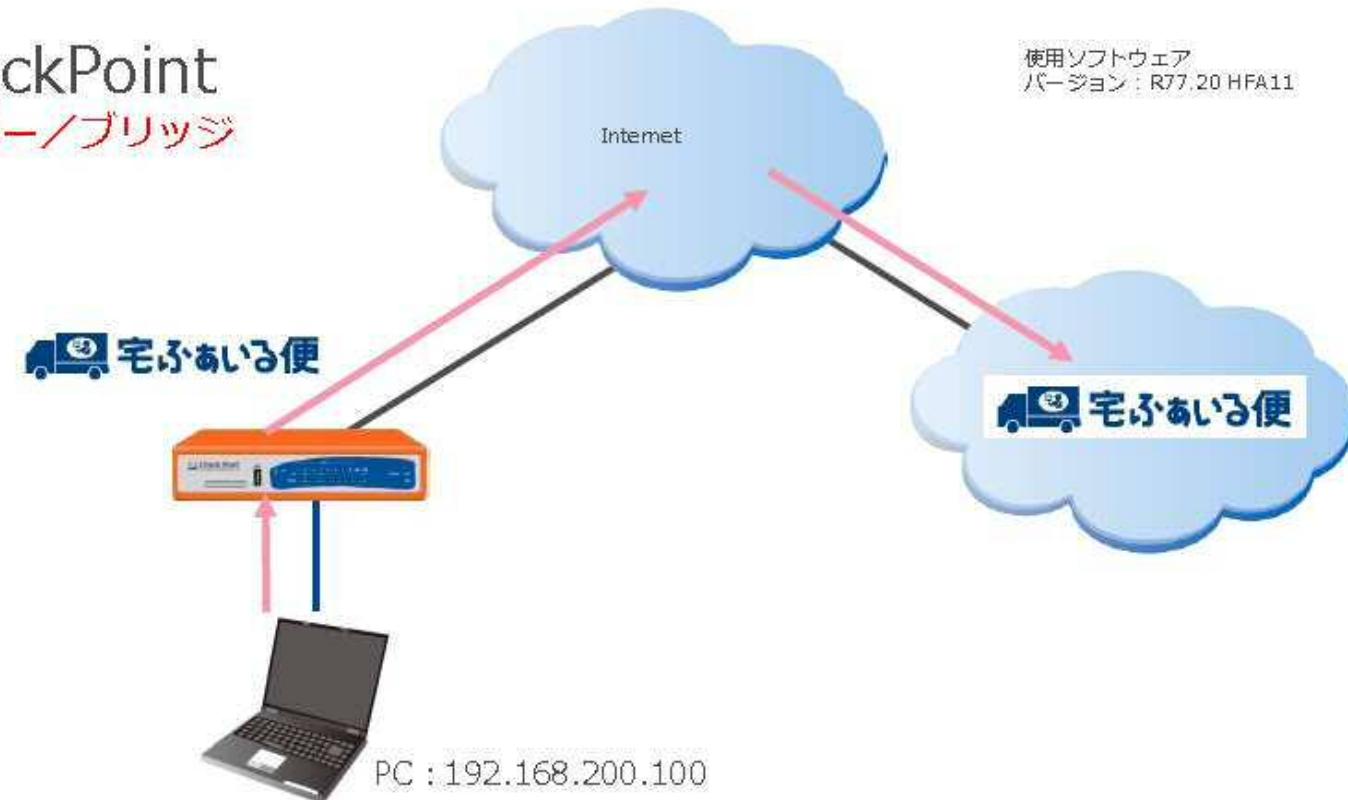
Checkpoint 600/700シリーズ



## 設定例ネットワーク構成図

CheckPoint  
ルーター／ブリッジ

使用ソフトウェア  
バージョン：R77.20 HFA11



- 本書はファイル共有サービス（今回の例では宅ファイル便）の利用時に、CheckPointのファイル共有アプリケーションのブロック機能によってブロックされている場合に、解除の操作を行うための手順書です。

## 2 : CheckPointアプライアンスへのアクセス

- ・ ブラウザを起動してURL欄にデフォルトIPを入力します。  
<https://アプライアンスIP:4434>
- ・ 【詳細設定】をクリック ⇒ 「\*\*\*.\*\*\*.\*.\* (アプライアンスのIP) にアクセスする（安全ではありません）」の文言をクリックします。  
※推奨ブラウザ : Google Chrome , Mozilla FireFox



## 2 : セキュリティログの確認

- 「ログ&モニタリング」タブ ⇒ 【セキュリティログ】

“Block”を確認すると、“filesend.to”を“Application Control”でブロックしたことがわかります。  
ログをダブルクリックするブロックされたアプリケーションなどの情報が確認できます。

The screenshot shows a log viewer interface with two main sections: a table of logs on the left and a detailed log view on the right.

**Table of Logs:**

Time	Blade	Interface	Action	Source	Destination	Service	Rule	Description
Today 19:30:29	■ Firewall	WAN	Block	192.168.200.100	224.0.0.352	UDP/5355	Default policy/incomm...	Blocked on rule Default policy/incoming[internal]
Today 19:30:29	■ Firewall	WAN	Block	192.168.200.100	224.0.0.352	UDP/5355	Default policy/incomm...	Blocked on rule Default policy/incoming[internal]
Today 19:30:29	■ Firewall	WAN	Block	192.168.200.100	224.0.0.252	UDP/5355	Default policy/incomm...	Blocked on rule Default policy/incoming[internal]
Today 19:30:04	■ Application Control	WAN	Block	192.168.203.100	119.145.226.212	HTTPS	1 (Outgoing)	filesend.to was blocked
Today 19:29:07	■ Firewall	WAN	Block	192.168.200.100	224.0.0.151	UDP/5355	Default policy/incomm...	Blocked on rule Default policy/incoming[internal]
Today 19:29:47	■ Firewall	WAN	Block					
Today 19:29:47	■ Firewall	WAN	Block					
Today 19:29:47	■ Firewall	WAN	Block					
Today 19:29:47	■ Firewall	WAN	Block					
Today 19:29:47	■ Firewall	WAN	Block					
Today 19:29:47	■ Firewall	WAN	Block					
Today 19:29:47	■ Firewall	WAN	Block					
Today 19:29:47	■ Firewall	WAN	Block					
Today 19:29:47	■ Application Control	WAN	Block					
Today 19:29:47	■ Application Control	WAN	Block					
Today 19:29:04	■ Firewall	WAN	Block					
Today 19:28:03	■ Application Control	WAN	Block					
Today 19:28:37	■ Firewall	WAN	Block					
Today 19:28:15	■ URL Filtering	WAN	Block					
Today 19:28:15	■ URL Filtering	WAN	Block					
Today 19:27:59	■ URL Filtering	WAN	Block					
Today 19:27:45	■ Application Control	WAN	Block					
Today 19:27:25	■ Firewall	WAN	Block					

**Detailed Log View (Right Panel):**

**ログ詳細** (Dropbox was blocked [REDACTED])

ログ情報	その他
発生元: [REDACTED]	登録時間: 05/04/2016 19:17:35
時刻: 05/04/2016 19:17:35	プライマリカテゴリ: File Storage and Sharing
ブレード: Application Control	説明: Dropbox was blocked
製品バージョン: Network	プロキシソースIP: [REDACTED]
タイプ: Alert	Suppressed-Logs: 4

**操作**

アクション	状況
Dropbox was blocked [REDACTED]	Block
ルール: 2 (Outgoing)	Block

**トラフィック**

ソース	宛先	サービス	送信(パケット)	受信(パケット)	合計パケット数	インターフェースの方向	インターフェース	プロトコル	端末ポート	ソースポート	サービス名
	108.160.172.206	TCP/443	1148	368	1516	出	outbound	HTTP	443	61787	HTTP

**詳細**

ア�플리케ーション名	説明
File Storage and Sharing	Dropbox is an application that allows the user to store and share files. Supported from: R75.
Autostart/Sysv Resident, High Bandwidth, Transmits Information, Encrypts Information, Share Address, Show Files, High Risk, File Storage and Sharing, Cloud Services	Dropbox is an application that allows the user to store and share files. Supported from: R75.
File Storage and Sharing	Dropbox is an application that allows the user to store and share files. Supported from: R75.

### 3：アクセスポリシーの作成①

- 「アクセスポリシー」タブ ⇒ ファイアウォールの【ポリシー】 ⇒ 「インターネットへの外部アクセス」の【新規】

The screenshot shows the Check Point 600 Appliance management interface. The top navigation bar includes links for Home, Devices, Access Policy, Firewall Policies, VPN, User & Objects, Logs & Monitoring, and Help/Support. The current view is under the Access Policy tab, specifically the 'Internet-to-External Access' section. A red box highlights the 'Policy' link in the left sidebar. Another red box highlights the 'New' button in the 'Internet-to-External Access' section. The main pane displays two automatically generated rules:

No.	ソース	宛先	サービス	アクション	ログ
1	Any	Internet	Undesired app...	TCP/UDP ブロック	なし
2	Any	Internet	Any	許可	なし

Below this, there is a section for '着信、内部および VPN トрафик' (Incoming, Internal, and VPN Traffic) with one rule listed:

No.	ソース	宛先	サービス	アクション	ログ
1	cp7f2bd262	Any	Any	許可	なし

## 4：アクセスポリシーの作成②

- アプリケーションの【ANY】をクリック ⇒ 「絞込み」を【すべて】に変更 ⇒ 該当のアプリケーションを検索してクリック
- アクションの【ブロック】をクリック ⇒ 【許可】 ⇒ 【適用】

ルールの追加: インターネットへの外部アクセス

任意のサービスにおける任意のアプリケーションの任意のソースからインターネットへのトラフィックはログとしてログ記録

ソース	宛先	アプリケーション	サービス	アクション	ログ
Any	Internet	FileSend	Any	ブロック	ログ

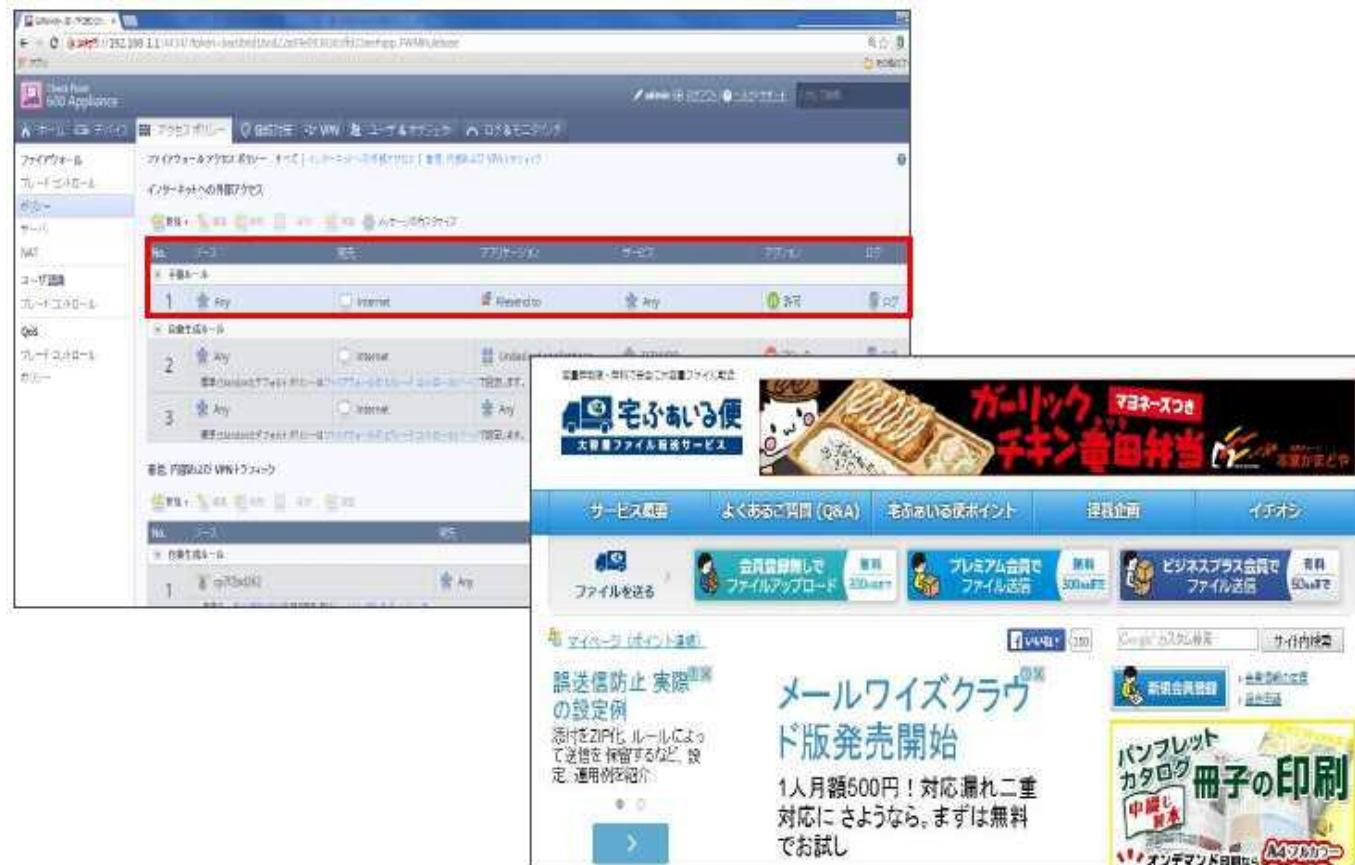
ルールの追加: インターネットへの外部アクセス

任意のサービスにおける FileSend.to の任意のソースからインターネットへのトラフィックは許可してログ記録

ソース	宛先	アプリケーション	サービス	アクション	ログ
Any	Internet	FileSend.to	Any	許可	ログ

## 5：設定の完了とWeb確認

- “手動ルール”に新しくアクセスポリシーが追加されたことを確認できれば設定は完了です。
- ブラウザを開いて、宅ファイル便のページが表示されることを確認してください。



## 6：アクセスポリシーの作成時の補足

- ・ アプリケーション名ではなく、サイトのURLで許可を追加したい場合も同様にルールを作成します
- ・ アプリケーションの【ANY】をクリック ⇒ 一覧右下の【新規】 ⇒ 【URL】  
「新しいURL」に【許可するアドレスを入力】 ⇒ 【適用】

**補足**：URLの入力はワイルドカード (\*) を使うことで、より広い範囲で指定できます。  
「http://www.post.japanpost.jp/zipcode/index.html」を例にとると、「\*japanpost.jp/\*」と入力ができます。

