



# McAfee Web Gateway 7.x

## Best Practices: External List の利用について

TM

Support & Service 統括本部  
Contents Security Support  
Jul 26, 2016

# 概要

本書では、McAfee Web Gateway(以下MWG)のExternal List機能を使った外部リストの参照について解説します。

本記事作成時の最新リリースバージョンは以下の通りです。

Main Release: 7.5.2.8

# 本書について

本書では MWG が標準で参照している URL フィルタリングデータベース (GTI/Trusted Source) 以外の、外部サービスによって提供されるリスト (Ransomware ボットネットや C&C サーバーのリスト) を参照して、クライアントが危険性のあるサイトへ接続することを防ぐ手順を解説しています。

解説の中でご案内する外部サービスについては弊社が提供するサービスではございませんので、これに関するお問い合わせにはお答えできません。ご了承下さい。

# External Listについて

アプライアンスのルールで使用できるデータをWebサーバーなどの外部ソースから取得する機能です。

文字列、IPアドレス、数値などさまざまなデータ型を利用できます。

外部リストは一定期間内部キャッシュ(メモリ内)に保存されますが、ディスクには保存されません。メモリ上にキャッシュデータを保存しますので、その分メモリを消費します。

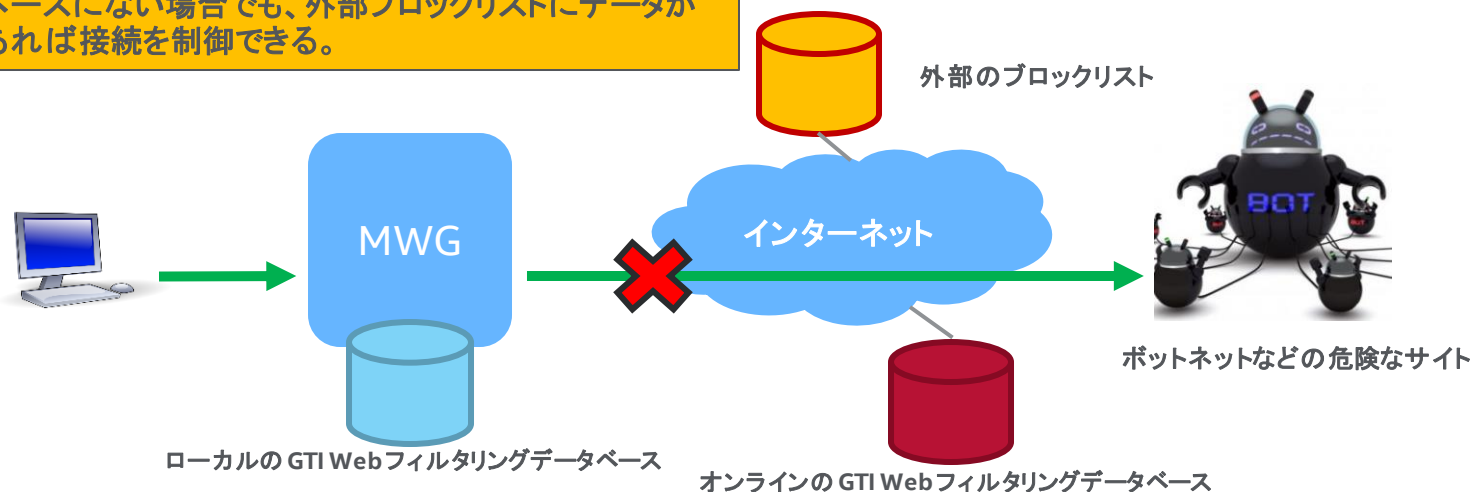
リストデータは初めてルールで利用されるときに参照、取得されます。

External List の活用例としては、頻繁に変更が予想される、外部ソースに保存された多数のデータを参照する必要があり、Central Management 構成で複数のアプライアンスに対して同様に変更を適用する場合です。

# External Listで外部ブロックリストを参照するメリット

MWGが参照する標準のWebフィルタリングデータベースには非常に多数の危険なサイトのURL、IPアドレスが保存されています。しかしこのデータベースにすべての危険なサイトの情報を必ず保存しているとは限らないため、外部ブロックリストを参照することで、標準のフィルタリングデータベースに含まれない危険なサイトへの接続をチェックします。

危険なサイトのデータがGTI Webフィルタリングデータベースにない場合でも、外部ブロックリストにデータがあれば接続を制御できる。



MWG は 通常 GTI Web フィルタリングデータベースを参照する。  
ローカルのデータベースとオンラインのデータベースで更新情報の差はあっても、大元の情報は同じ。

# 設定手順

## 1. External Listの登録

例ではabude.chに公開されているRansomware tracker のリストを参照するように設定します。今回は最低限必要な設定のみ解説します。

Ransomware tracker blocklists

<https://ransomwaretracker.abuse.ch/blocklist/>

以下、三つのリストを追加します。

Domain Blocklist: [http://ransomwaretracker.abuse.ch/downloads/RC\\_DOMBL.txt](http://ransomwaretracker.abuse.ch/downloads/RC_DOMBL.txt)

URL Blocklist: [http://ransomwaretracker.abuse.ch/downloads/RW\\_URLBL.txt](http://ransomwaretracker.abuse.ch/downloads/RW_URLBL.txt)

IP Blocklist: [http://ransomwaretracker.abuse.ch/RW\\_IPBL.txt](http://ransomwaretracker.abuse.ch/RW_IPBL.txt)

## 2. External Listに合致した場合のルールを追加

1で設定したExternal Listを参照し、クライアントの要求したIPアドレス、URL、ホスト名がリストに合致した場合にアクセスを拒否するルールを追加します。

# 設定手順

## 1. External Listの登録

The screenshot displays the McAfee Web Gateway configuration interface. The top navigation bar includes 'Dashboard', 'Policy', 'Configuration', 'Accounts', and 'Troubleshooting'. The main content area is divided into a left sidebar and a right main panel. The sidebar shows a tree view of settings, with 'External Lists' expanded and 'Ransomware tracker ip blocklist' selected. The main panel shows the configuration for the selected list, including 'Data source type' (set to 'Web Servi...'), 'Common Parameters' (Operation timeout: 5 seconds, Simple expiration selected), 'Data conversion settings' (Data type: Plain Te...), and 'Web Service Specific Parameters' (Web service's URL: http://ransomwaretracker.abuse.ch/downloads/RW\_IPBL.txt).

データソースの種別をWeb Serviceに設定します

リストを取得するURLを設定します

残りの二つのリストも同様に追加します。

# 設定手順

## 1. External Listの登録(External List の取得制限)

External Listには取得制限があります。リストのエントリー数またはデータサイズが制限値を超えるとエラーとなりますので、サイズの大きなリストを取得する際には External Lists を追加する際 Advanced Parameters にある以下の項目を変更します。

### Advanced Parameters

Skip "bad" entries during data conversion

Maximum number of entries to fetch (1 - 100000)

10000

Maximum size of data fetch in Kb (1 - 100000)

1000





# 設定手順

## 2. ルールを追加(ルール解説)

追加したルールの詳細は以下の通りです。

**URL.Host is in list ExtLists.StringList(“”, “”, “”) <Ransomware tracker domain blacklist>**

ExtLists.StringListは、文字列型の外部参照リストで、()内のパラメーターはリスト内で参照すべきデータを識別するための条件となる値です。

このルールは、URL.Host(クライアントの要求したURLのホスト名)が、外部参照リスト<Ransomware tracker blacklist>に含まれている場合に一致します。

**URL.DestinationIP is in list ExtLists.Iplist(“”, “”, “”) <Ransomware tracker ip blacklist>**

評価対象がURLをDNS検索して見つかった宛先IPアドレスである、参照するリストが<Ransomware tracker ip blacklist>であること以外は、先のルールと変わりません。

# 設定手順

## 2. ルールを追加(ルール解説 - 続き)

### **URL.SmartMatch (ExtLists.StringList(“”, “”, “”)<Ransomware tracker URL blacklist>) equals true**

このルールは少し特殊です。URL.SmartMatch はパラメーターとして渡されている外部参照リスト<Ransomware tracker URL blacklist>で文字列として指定されている1つ以上の部分を要求されたURLを比較し、マッチするものがあればtrueを返します。

URL.Smartmatchプロパティを利用すると、URLに含まれるホスト名や完全なURL、URLパスの一部などを含むより複雑なリスト検索を行うことができます。

製品ガイドのプロパティリストに詳しい合致条件が記載されていますので、ご参照ください。

※**URL is in list ExtLists.StringList(“”, “”, “”)<Ransomware tracker URL blacklist>** というルールに変更することで、先の二つのルールと同じように評価を行います。例ではURL.SmartMatch のご紹介のため、あえて設定方法を変更していますが、同じように評価したい場合は、こちらをご利用ください。

# 設定手順

## 3. Error Handlerルールを追加

参照先のリストが存在しない場合、MWGは Error ID: 25006 としてそれを検知します。既定ではインターネットへのアクセスがブロックされてしまうため、これを避けるために Error Handler に、このIDを検知した際、ルールセットを迂回するためのルールを設定します。

Server: mwg7429 | Server Time: 2016-07-26 13:49 JST | UI Version 7.5.2.8.0 (21496) | User: admin | Role: Super Administrator

McAfee Web Gateway

Dashboard Policy Configuration Accounts Troubleshooting

Rule Sets Lists Settings Templates

Add Edit... Enable Enable in Cloud Criteria: Always

Rules in 'Block on All Errors':

Add Rule... Edit... Delete... Move up Move down Copy Paste Show details

Enabled	Name/Criteria	Action
<input checked="" type="checkbox"/>	<b>Ignore no such resource from ext Lists</b> Error.ID equals 25006	Stop Rule Set
<input checked="" type="checkbox"/>	<b>Ignore Mail Bomb Warning</b> Error.ID equals 10063	Stop Rule Set
<input checked="" type="checkbox"/>	<b>Always Block</b> Always	Block<Internal Error>

Rule Criteria: Error.ID equals 25006  
Action: Stop Rule Set

