MRB、MRB-cloudのフィルタ設定例

株式会社テクノル
IS推進部

はじめに

最近、Emotetが猛威を振るっております。
MRB、MRB-cloudを導入頂いているお客様で、
Emotet感染後の通信をチェックする設定になっていないお客様もいます。

次スライド以降で推奨設定①、②をご紹介します。
※全ての通信先を完全に判定できる事をお約束するものではありません。

推奨設定	メリット	デメリット
① 簡易設定	・PCにMRB、MRB-cloudの証明書をインストールする必要がないため、簡単に設定できる。 ・Emotet感染後の通信をチェックする。	・推奨設定②に比べて、セキュリティレベルが低い。 ・httpsサイトブロック時にブロック画面が表示できない。
② 詳細設定	・Emotet感染後の通信をチェックする。推奨設定①に比べてチェックするレベルが高い。	・PCにMRB、MRB-cloudの証明書をインストールする手間がかかる。 ・推奨設定①に比べてセキュリティレベルが高いので、業務利用するサイト、サーバをブロックする可能性がある。（アクセスするためにはホワイトリスト登録が必要）

MRB、MRB-cloudの設定例：推奨①

【想定するお客様】
・危ないサイトには行きたくないが、ブログ等のレンタルサーバを閲覧する頻度が多いお客様

【防御範囲】
・HTTP（URLフィルタリング、IPフィルタリング）
・TCP/IPによるすべての通信（IPフィルタリング、振る舞い）

【設定例】

フィルタ名	強度	機能	設定効果
URLフィルタリング	中	URLのカテゴリを選択された強度でブロックする＋URLの脅威スコアによりブロックする。	最低限の危険なカテゴリはアクセスさせず、 脅威スコア39点以下のURL（httpサイトのみ）をブロックする。
IPフィルタリング	低	ブラウジングの際に、接続先のIPアドレスに危険が潜んでいる場合にアクセスをブロックする。	脅威を含む可能性があるサイトへはアクセスさせない。 脅威スコア5点以下のIPをブロックする。
IP判定方式	スコアと脅威	IPアドレスの”スコア”、”脅威”、”スコアと脅威”によりブロックする。	IPの脅威を含むカテゴリとスコアをチェックする。
振る舞い検知	低	ブラウジング以外のアウトバウンド通信の際に、接続先のIPアドレスに危険が潜んでいる場合にアクセスをブロックする。	C＆Cサーバーへの通信をブロックする。 **IPのスコアにもよりますが、Emotet感染後のメール送信等を防止する。**
HTTPS通信	OFF	HTTPS通信の際に、接続先に危険が潜んでいる場合にアクセスをブロックする。 OFFの場合、IPがブロックされた際に、ブロック画面は表示されない。	httpsサイトアクセス時にブロックしても、ブロック画面は表示されない。

MRB、MRB-cloudの設定例：推奨②

【想定するお客様】
・UTMの機能を十分に活用したいお客様
・危ないサイトには行きたくないお客様
・HTTPSのwebサイトもフィルタリングしたいお客様

【防御範囲】
・HTTP、HTTPS（URLフィルタリング、IPフィルタリング）
・TCP/IPによるすべての通信（IPフィルタリング、振る舞い）

【設定例】

フィルタ名	強度	機能	設定効果
URLフィルタリング	中	URLのカテゴリを選択された強度でブロックする＋URLの脅威スコアによりブロックする。	最低限の危険なカテゴリはアクセスさせず、 脅威スコア39点以下のURLをブロックする。
IPフィルタリング	中	ブラウジングの際に、接続先のIPアドレスに危険が潜んでいる場合にアクセスをブロックする。	脅威を含む可能性があるサイトへはアクセスさせない。 脅威スコア10点以下のIPをブロックする。
IP判定方式	スコアと脅威	IPアドレスの”スコア”、”脅威”、”スコアと脅威”によりブロックする。	IPの脅威を含むカテゴリとスコアをチェックする。
振る舞い検知	中	ブラウジング以外のアウトバウンド通信の際に、接続先のIPアドレスに危険が潜んでいる場合にアクセスをブロックする。	C＆Cサーバーへの通信をブロックする。 **IPのスコアにもよりますが、Emotet感染後のメール送信等を防止する。**
HTTPS通信	ON	HTTPS通信の際に、接続先に危険が潜んでいる場合にアクセスをブロックする。 OFFの場合、IPがブロックされた際に、ブロック画面は表示されない。	HTTPSフィルタリング機能を使用するためには**MRB、MRB-cloudの証明書を各端末にインポートする必要**がある。

HTTPS通信：ON時の注意点

HTTPS通信をONにするとMRB、MRB-cloudの証明書を利用してアクセスします。
そのため、クライアント証明書を利用してアクセスするサイトには、MRB、MRB-cloudの証明書でアクセスすると相手側で接続を拒否します。
回避するために、サイトの接続方式に応じて、HTTPS通信の対象外IP、対象外URLの登録をお願いします。

サイトの例：銀行のオンラインバンキング、Web会議（Zoom、Cisco Webex）等

HTTPS通信：OFFの時

クライアント証明書（鍵）でアクセス

HTTPS通信：ONの時

MRBの証明書（鍵）でアクセス

Webサイト側で知らない証明書で通信が来ているので、
アクセスを拒否しています。そのため対象外登録する必要があります。

IPフィルタリング「中」、振る舞い検知「中」時の注意点

昨今サイバー攻撃が猛威を振るっており、クラウドサービスのIPスコアが低く判定されブロックすることがあります。
ログを確認してブロック先のURLまたはIPアドレスをホワイトリスト登録すれば、利用しているクラウドサービスを利用することができます。

ブロック元のIPアドレス

ブロック先のURLまたはIPアドレス

ログ表示

セキィリティログ - URLフィルタリングログ

```
2021/03/05 09:11:30 U001 100 172.30.30.41->202.230.200.207 GROUP_BLACKLIST www.technol.co.jp
2021/03/05 09:11:37 U001 100 172.30.30.41->202.230.200.207 GROUP_BLACKLIST www.technol.co.jp/favicon.ico
```

セキィリティログ - IPフィルタリングログ

```
2021/03/05 09:12:12 I001 100 172.30.30.41->202.230.200.207 GROUP_BLACKLIST ---
2021/03/05 09:12:34 I001 100 172.30.30.41->202.230.200.207 GROUP_BLACKLIST ---
```

セキィリティログ - 振る舞いログ

```
2021/03/05,09:14:49,0,100,1,172.30.30.41:0,202.230.200.207:0
2021/03/05,09:14:54,0,100,1,172.30.30.41:0,202.230.200.207:0
```

多数のブロックがあり許可したい
IPアドレスが分からない場合は、
先度アクセスを試しブロックさせれば該
当時間でIPアドレスを確認できます。