

サイバーセキュリティ見守りサービス

UTM 取扱説明書

補足資料

1. はじめに

本書はサイバーセキュリティ見守りサービス UTM 取扱説明書の補足資料です。

本書は以下について記載しています。

- UTM 取扱説明書に記載されていないセキュリティ機能の設定変更方法について

注意事項

- 工場出荷時のセキュリティ設定では、本書に記載しているセキュリティ機能は、通信のブロック機能を有効にしていません。通信のブロック機能を有効にした場合、**誤って設定すると業務上必要な通信をブロックしてしまう可能性があるため**、慎重に設定をお願いします。また、**ブロック機能の有効化はお客様の責任において実施することとします**。

2. セキュリティ機能の設定変更について

以下のセキュリティ機能の設定変更方法について説明します。

- URL フィルタリング
- アプリケーションガード
- IPv4 パケットフィルタ

なお、セキュリティ機能の設定変更には、UTM 装置の設定画面にアクセスする必要があります。アクセス先の URL が分からない場合、相談窓口にご連絡ください。

2.1. URL フィルタリング

監視対象の端末による Web サイトへのアクセスに対して、カテゴリ単位でのブロックやログへの記録を行います。

これにより、有害な Web サイトや業務に無関係な Web サイトなどへのアクセスの制限や、アクセス状況の把握ができます。

Web サイトのカテゴリ情報は定期的に更新されます。URL フィルタリングのブロック機能を使用している場合、カテゴリが更新されることで、今までブロックされていた Web サイトがブロックされなくなる場合や、逆に、今までブロックされていなかった Web サイトがブロックされるようになる場合がありますのでご注意ください。

URL フィルタリングの設定は以下の画面から行います。

以下の画面は、UTM 設定画面のトップページから[セキュリティ]-[URL フィルタリング (UF)]を選択することで表示できます。

URL フィルタリング | カテゴリ設定 | URL カテゴリクエリ | 個別許可

本機能は、指定されたカテゴリに属するウェブサイトへの通信を検出する機能です。

URL フィルタリング設定

機能を使用する

ブロック設定

カテゴリ設定で全て許可と設定されている場合は、「カテゴリ判定不可時にブロックする」のチェックボックスは無効扱いとなります。

カテゴリ不明サイトをブロックする

カテゴリ判定不可時にブロックする

設定

各タブの説明は以下です。

タブ	説明
URL フィルタリング	URL フィルタリング機能の使用有無とブロックの設定を行います。
カテゴリ設定	カテゴリごとの動作設定を行います。
URL カテゴリクエリ	特定の URL がどのカテゴリに所属するか確認する機能です。
個別許可	特定の URL を個別に許可する設定を行います。

2.1.1. URL フィルタリング

URL フィルタリング機能の使用有無とブロックの設定を行います。

設定変更後、「設定」ボタンをクリックし、「保存」ボタンをクリックすることで設定が有効になります。

「設定」ボタンをクリックしないと設定が有効になりませんので注意してください。

URL フィルタリング カテゴリ設定 URL カテゴリクエリ 個別許可

本機能は、指定されたカテゴリに属するウェブサイトへの通信を検出する機能です。

URL フィルタリング設定

機能を使用する

ブロック設定

カテゴリ設定で全て許可と設定されている場合は、「カテゴリ判定不可時にブロックする」のチェックボックスは無効扱いとなります。

カテゴリ不明サイトをブロックする

カテゴリ判定不可時にブロックする

設定

項目	説明
URL フィルタリング設定	
機能を使用する	URL フィルタリング機能の使用有無を設定します。
ブロック設定	
カテゴリ不明サイトをブロックする	カテゴリが不明の場合にブロックする場合は、本項目をチェックします。 アクセスした URL が本サービスのデータベースに登録されていない場合、カテゴリ不明となります。
カテゴリ判定不可時にブロックする	カテゴリが確認できない場合にブロックする場合は、本項目をチェックします。 カテゴリ判定時、UTM 装置がクラウド上のサーバとの通信に失敗した場合、カテゴリ判定不可となります。

2.1.2. カテゴリ設定

カテゴリごとの動作設定を行います。

設定変更後、「設定」ボタンをクリックし、「保存」ボタンをクリックすることで設定が有効になります。

「設定」ボタンをクリックしないと設定が有効になりませんので注意してください。

URL フィルタリング カテゴリ設定 URL カテゴリクエリ 個別許可

本設定は以下に示されたカテゴリに属するウェブサイト検出時の動作設定です。

スタンダード設定 ?

全てのカテゴリ

アダルトサイトカテゴリ SNSサイトカテゴリ

危険サイトカテゴリ エンターテインメントサイトカテゴリ

ブロックカテゴリ設定 ?

個別カテゴリ

カテゴリ	ブロック	ログのみ	許可
ポルノ / Pornography	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
アダルトサイト / Nudity and Potentially Adult Content	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
ギャンブル、宝くじ / Gambling and Lottery	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
アルコール、たばこ / Alcohol and Tobacco	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
ドラッグ / Abused Drug	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
過激論、人種差別 / Ultraism	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
中絶 / Abortion	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
犯罪行為 / Criminal Actions	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
暴力的なサイト / Violence and Bloody	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
気持ち悪いサイト / Gross	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

項目	説明
スタンダード設定	
ブロック	指定されたカテゴリに属する Web サイトへの通信をブロックし、ログ出力を行います。
ログのみ	指定されたカテゴリに属する Web サイトへの通信をブロックせず、ログ出力のみ行います。
許可	指定されたカテゴリに属する Web サイトへの通信をブロックせず、ログ出力も行いません。
全てのカテゴリ	全てのカテゴリが該当します。
アダルトサイトカテゴリ	以下のカテゴリが該当します。 ポルノ / Pornography アダルトサイト / Nudity and Potentially Adult Content ギャンブル、宝くじ / Gambling and Lottery アルコール、たばこ / Alcohol and Tobacco ドラッグ / Abused Drug 過激論、人種差別 / Ultraism 中絶 / Abortion 犯罪行為 / Criminal Actions

	暴力的なサイト / Violent and Bloody 気持ち悪いサイト / Gross 出会い系サイト / Dating
危険サイトカテゴリ	以下のカテゴリが該当します。 フィッシング詐欺 / Phishing and Fraud マルウェア / Malware BlackHat SEO サイト / BlackHat SEO Sites 危険アプリケーション / Malicious APPs
SNS サイトカテゴリ	以下のカテゴリが該当します。 インスタントメッセージ / Instant Messaging ソーシャルネットワーク / Social Network Web チャットルーム / Web Chat Room フォーラム、ニュースグループ / Forums and Newsgroups ブログと個人サイト / Blog and Personal Web
エンターテインメントサイトカテゴリ	以下のカテゴリが該当します。 ゲーム / Game ショッピング、オークション / Shopping and Auction ミュージック / Music コミック、アニメ / Comics and Anime エンターテインメント、芸術 / Entertainment and Arts ストリーミング、VoIP / Streaming and VoIP
ブロックカテゴリ設定	
個別カテゴリを非表示	カテゴリのリストを非表示にします。
カテゴリのリスト	カテゴリごとにブロック、ログのみ、許可設定を行います。

2.1.3. URL カテゴリクエリ

特定の URL がどのカテゴリに所属するか確認する機能です。

確認対象の URL をテキストボックスに入力し、「確認」ボタンをクリックすると、入力した URL が所属するカテゴリが表示されます。

URL フィルタリング
カテゴリ設定
URL カテゴリクエリ
個別許可

本機能は指定されたURLのウェブサイトが属するカテゴリを検索する機能です。
 URLのドメイン部のみ入力してください。

URL カテゴリクエリ

http(s)://

カテゴリ:
 ポータル、検索サイト / Portals

2.1.4. 個別許可

特定の URL を個別に許可する設定を行います。

URL フィルタリング | カテゴリ設定 | URL カテゴリクエリ | **個別許可**

個別許可設定を実行する場合、該当する通信は危険な通信であっても許可されます。
本設定を行う場合は、お客さま自身の責任で、慎重に設定してください。

個別許可リスト ?

URL	編集
example.com	削除
*.example.com	削除
example.com/exam	削除
<input type="text"/>	追加

項目	説明
個別許可リスト	
テキストボックス	個別に通信を許可したい URL を入力します。入力可能な形式は以下です。 <ドメイン名> *.<ドメイン名> <ドメイン名>/<パス> ※ パスは前方一致で判定します。
追加	テキストボックスに入力された URL が個別許可リストに追加されます。
削除	個別許可リストから削除されます。

2.2. アプリケーションガード

監視対象の端末に対して、アプリケーションの利用制限や、ログへの記録を行います。

これにより、ファイル交換ソフトや動画共有アプリ、メッセージアプリなどへのアクセスの制限や、アプリケーションの利用状況の把握ができます。

アプリケーションリストの情報は定期的に更新されます。アプリケーションガードのブロック機能を使用している場合、アプリケーションリストが更新されることで、今までブロックされていたアプリケーションがブロックされなくなる場合や、逆に、今までブロックされていなかったアプリケーションがブロックされるようになる場合がありますのでご注意ください。

アプリケーションガードの設定は以下の画面から行います。

以下の画面は、UTM 設定画面のトップページから[セキュリティ]-[アプリケーションガード (APG)]を選択することで表示できます。

アプリケーションガード アプリケーションリスト

本機能はアプリケーションの通信を検出する機能です。

アプリケーションガード設定

機能を使用する

設定

各タブの説明は以下です。

タブ	説明
アプリケーションガード	アプリケーションガード機能の使用有無の設定を行います。
アプリケーションリスト	ブロックするアプリケーションの設定を行います。

2.2.1. アプリケーションガード

アプリケーションガード機能の使用有無の設定を行います。

設定変更後、「設定」ボタンをクリックし、「保存」ボタンをクリックすることで設定が有効になります。

「設定」ボタンをクリックしないと設定が有効になりませんので注意してください。

アプリケーションガード アプリケーションリスト

本機能はアプリケーションの通信を検出する機能です。

アプリケーションガード設定

機能を使用する

設定

項目	説明
アプリケーションガード設定	
機能を使用する	アプリケーションガード機能の使用有無を設定します。

2.2.2. アプリケーションリスト

ブロックするアプリケーションの設定を行います。

設定変更後、「設定」ボタンをクリックし、「保存」ボタンをクリックすることで設定が有効になります。

「設定」ボタンをクリックしないと設定が有効になりませんので注意してください。

アプリケーションガード
アプリケーションリスト

本設定はアプリケーションを選択する設定です。

カテゴリ選択

COMMON ▼

シグネチャ更新により追加されるアプリケーションの設定 ?

ブロック
 ログのみ
 許可

ブロックアプリケーション設定 ?

全てブロックする
全てログのみにする
全て許可する

#	アプリケーションID	アプリケーション名	カテゴリ	ブロック	ログのみ	許可
1	0660_06	DNS (DataFlow)	COMMON	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
2	0953_06	FTP (DataFlow)	COMMON	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
3	1842_06	NTP (DataFlow)	COMMON	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
4	2018_06	POP3 (DataFlow)	COMMON	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
5	2224_06	SAMBA (DataFlow)	COMMON	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
6	2381_06	SMTP (DataFlow)	COMMON	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
7	3208_06	HTTP-Download (DataFlow)	COMMON	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
8	3217_06	STUN (DataFlow)	COMMON	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

項目	説明
カテゴリ選択	
ドロップダウンリスト	リストに表示するカテゴリを指定します。
シグネチャ更新により追加されるアプリケーションの設定	
※ 本項目はカテゴリ選択で「全て」を指定している場合表示されません。	
※ 本項目はファームウェアバージョン 1.2 以降のみ表示されます。	
ブロック	シグネチャ更新によってアプリケーションが追加された際、指定されているカテゴリに追加されたアプリケーションの通信をブロックし、ログ出力を行います。
ログのみ	シグネチャ更新によってアプリケーションが追加された際、指定されているカテゴリに追加されたアプリケーションの通信をブロックせず、ログ出力のみ行います。
許可	シグネチャ更新によってアプリケーションが追加された際、指定されているカテゴリに追加されたアプリケーションの通信をブロックせず、ログ出力も行いません。
ブロックアプリケーション設定	
ブロック	指定されたアプリケーションの通信をブロックし、ログ出力を行います。

ログのみ	指定されたアプリケーションの通信をブロックせず、ログ出力のみ行います。
許可	指定されたアプリケーションの通信をブロックせず、ログ出力も行いません。
全てブロックする	リストに表示されている全てのアプリケーションの設定をブロックにします。
全てログのみにする	リストに表示されている全てのアプリケーションの設定をログのみにします。
全て許可する	リストに表示されている全てのアプリケーションの設定を許可にします。

2.3. IPv4 パケットフィルタ

IP アドレスやポート番号を指定して、通信の通過、廃棄、拒否の設定を行います。

2.3.1. エントリー一覧画面

IPv4 パケットフィルタの設定は以下の画面から確認します。

以下の画面は、UTM 設定画面のトップページから[メンテナンス]-[フィルタ設定]-[IPv4 パケットフィルタ]を選択することで表示できます。

本画面の各項目の意味については、画面内のヘルプをご参照ください。

IPv4パケットフィルタ設定 - エントリー一覧									
IPv4パケットフィルタエントリー ?									
1~10	11~20	21~30	31~40	41~50					
エントリー番号 ?	種別 ?	方向 ?	プロトコル ?	送信元 ?	送信元ポート ?	宛先 ?	宛先ポート ?	編集 ?	削除 ?
1	permit	in	UDP	any	67	any	68	編集	削除
2								編集	削除
3								編集	削除
4								編集	削除
5								編集	削除
6								編集	削除
7								編集	削除
8								編集	削除
9								編集	削除
10								編集	削除

2.3.2. エントリー編集画面

IPv4 パケットフィルタの設定は以下の画面から行います。

以下の画面は「エントリー一覧画面」から「編集」をクリックすることで表示できます。

本画面の各項目の意味については、画面内のヘルプをご参照ください。

設定変更後、[設定]ボタンをクリックし、[保存]ボタンをクリックすることで設定が有効になります。

[設定]ボタンをクリックしないと設定が有効になりませんので注意してください。

IPv4パケットフィルタ設定 - エントリ編集

パケットフィルタエントリ編集 ?

エントリ番号	2
種別 ?	<input checked="" type="radio"/> 通過 <input type="radio"/> 廃棄 <input type="radio"/> 拒否
フィルタタイプ ?	<input checked="" type="radio"/> 転送 <input type="radio"/> 送受信
方向 ?	<input checked="" type="radio"/> in <input type="radio"/> out
プロトコル ?	IPすべて <input type="checkbox"/> プロトコル番号 <input type="text"/>
	TCP FLAG <input type="text"/> 指定なし <input type="text"/>
	<input type="checkbox"/> ack <input type="checkbox"/> fin <input type="checkbox"/> psh <input type="checkbox"/> rst <input type="checkbox"/> syn <input type="checkbox"/> urg
送信元IPアドレス ?	ICMP MESSAGE <input type="text"/> 指定なし <input type="text"/>
	TYPE <input type="text"/> CODE <input type="text"/>
送信元IPアドレス ?	<input checked="" type="radio"/> any <input type="radio"/> <input type="text"/> / <input type="text"/>
送信元ポート番号 ?	<input checked="" type="checkbox"/> any <input type="checkbox"/> <input type="text"/> - <input type="text"/>
宛先IPアドレス ?	<input checked="" type="radio"/> any <input type="radio"/> <input type="text"/> / <input type="text"/>
宛先ポート番号 ?	<input checked="" type="checkbox"/> any <input type="checkbox"/> <input type="text"/> - <input type="text"/>

設定

前のページへ戻る

サイバーセキュリティ見守りサービス

UTM 取扱説明書

補足資料

CSD-SEC-MI-22125-1

2022年10月 第1.0版

©2022 NEC Corporation

©2022 NEC Platforms, Ltd

日本電気株式会社

NECプラットフォームズ株式会社