NEC

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

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。

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。

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。

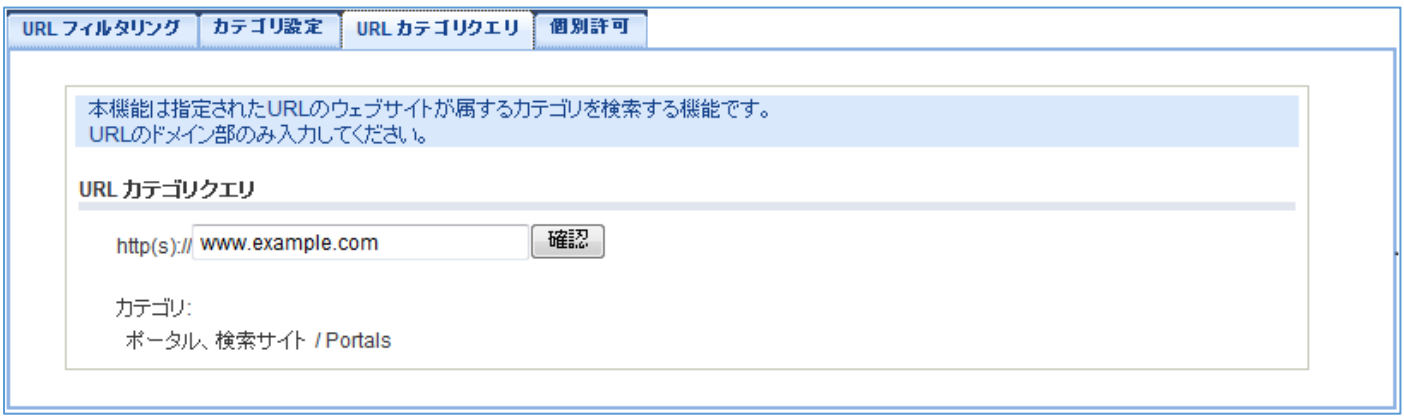
項目	説明
スタンダード設定	
ブロック	指定されたカテゴリに属する Web サイトへの通信をブロックし、ログ出力を行います。
ログのみ	指定されたカテゴリに属する Web サイトへの通信をブロックせず、ログ出力のみ行います。
許可	指定されたカテゴリに属する Web サイトへの通信をブロックせず、ログ出力も行いません。
全てのカテゴリ	全てのカテゴリが該当します。
アダルトサイトカテゴリ	以下のカテゴリが該当します。 ポルノ / Pornography アダルトサイト / Nudity and Potentially Adult Content ギャンブル、宝くじ / Gambling and 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

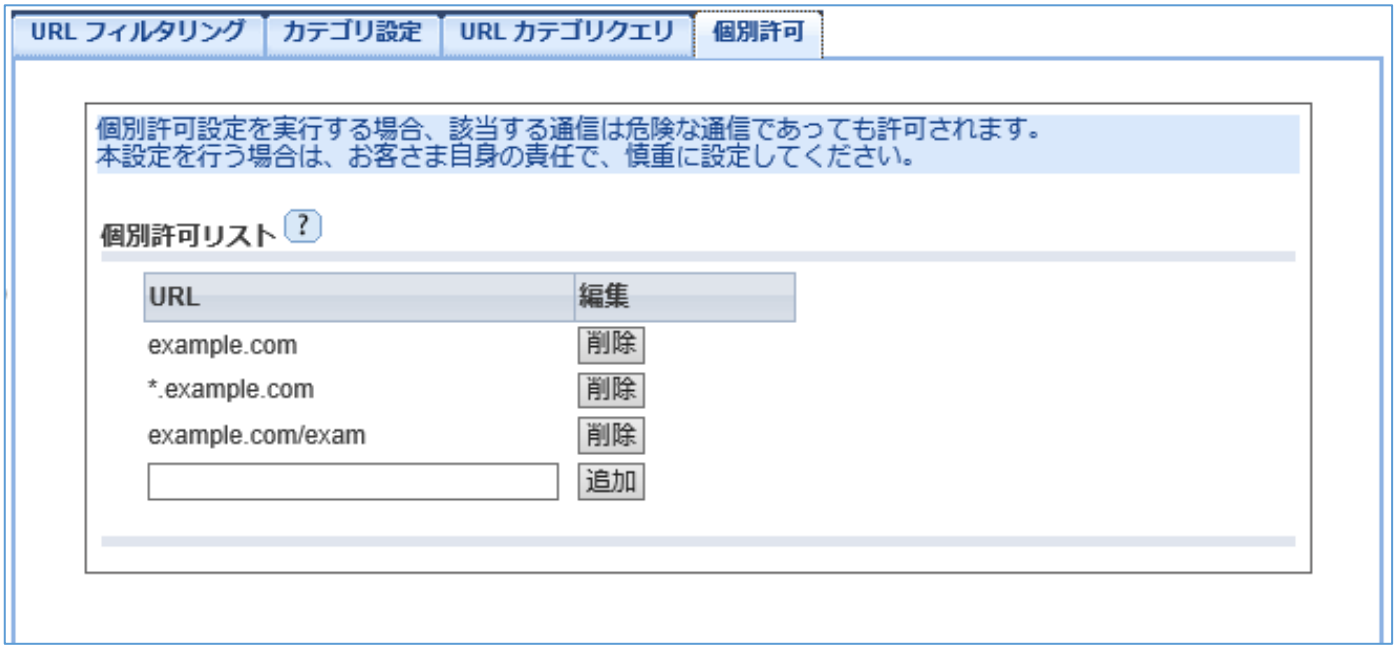
特定の URL がどのカテゴリに所属するか確認する機能です。

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。



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。



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

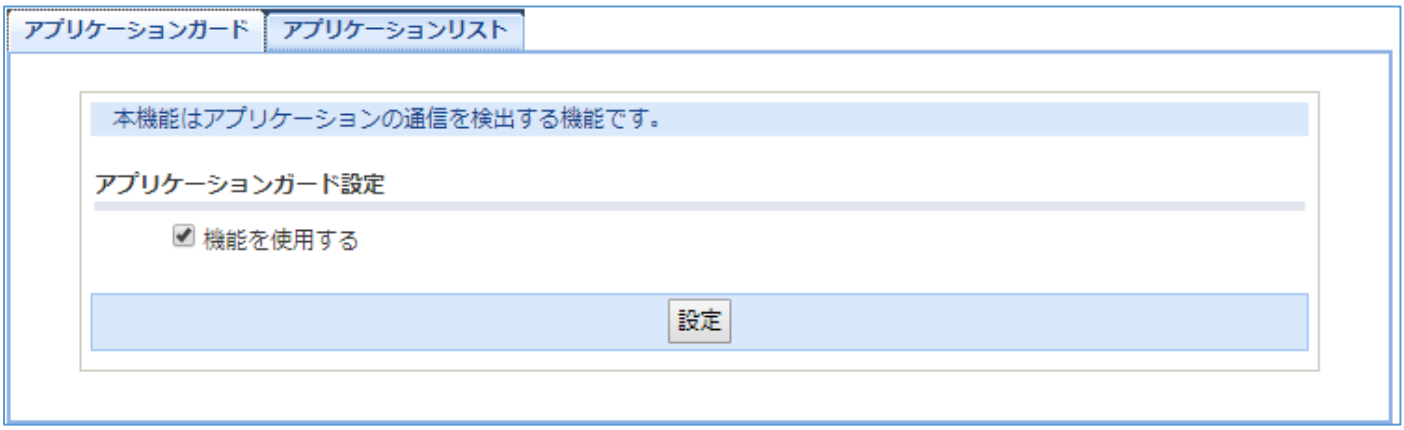
監視対象の端末に対して、アプリケーションの利用制限や、ログへの記録を行います。

これにより、ファイル交換ソフトや動画共有アプリ、メッセンジャー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。



各タブの説明は以下です。

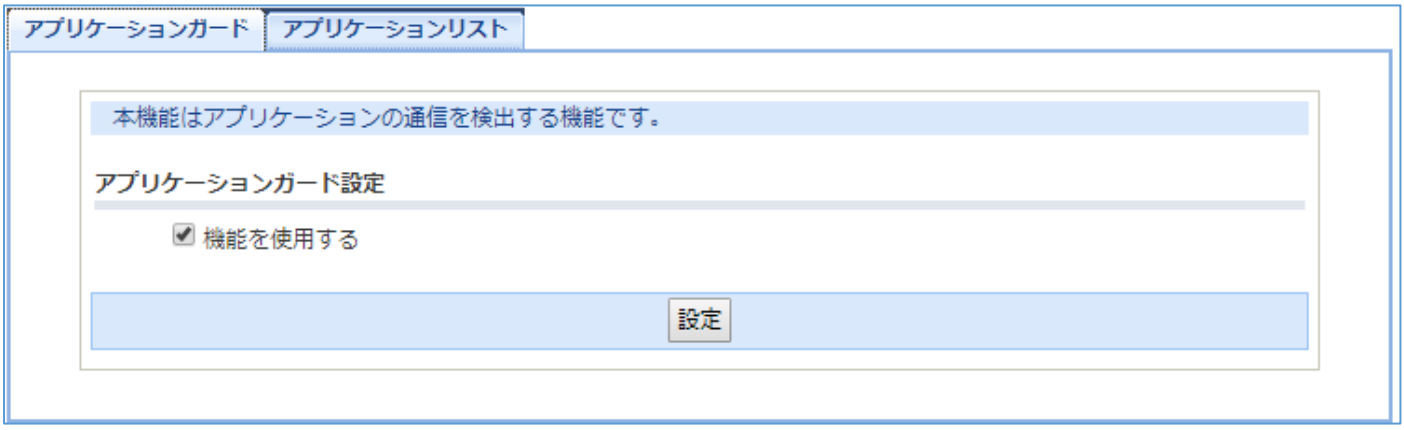
タブ	説明
アプリケーションガード	アプリケーションガード機能の使用有無の設定を行います。
アプリケーションリスト	ブロックするアプリケーションの設定を行います。

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。



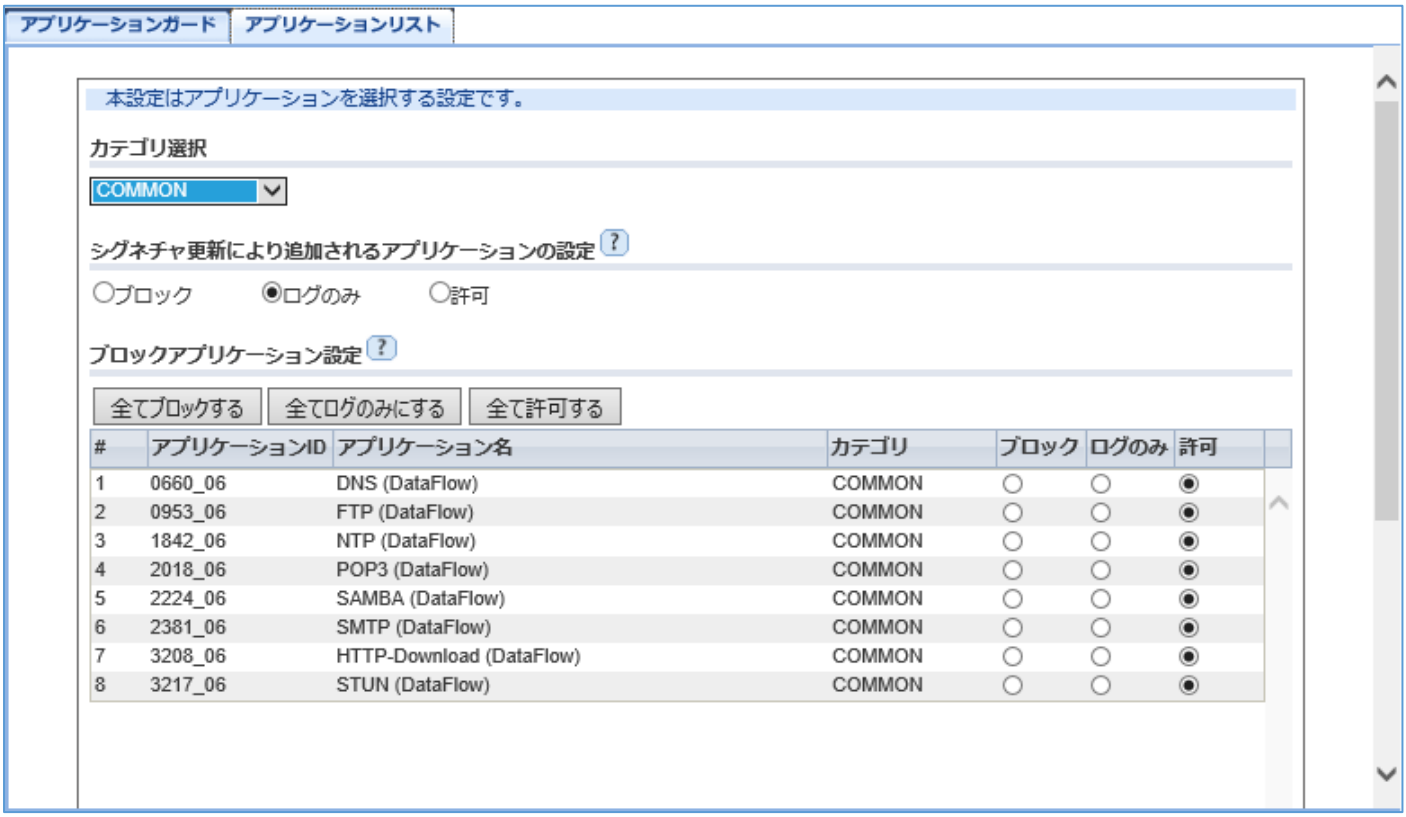
項目	説明
アプリケーションガード設定	
機能を使用する	アプリケーションガード機能の使用有無を設定します。

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。



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

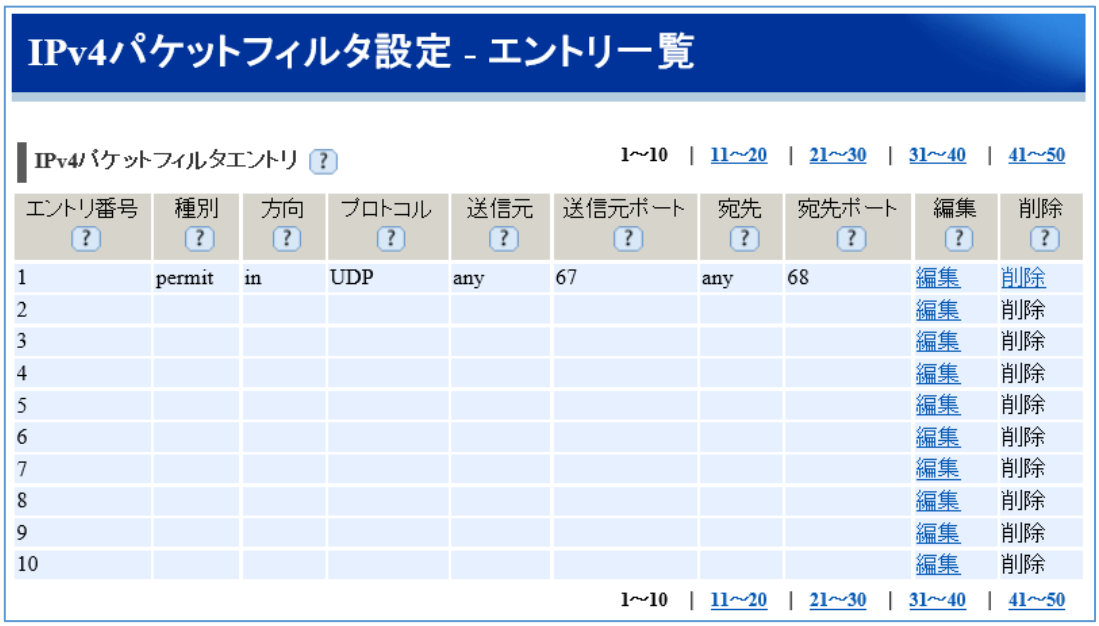
IP アドレスやポート番号を指定して、通信の通過、廃棄、拒否の設定を行います。

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。



2.3.2. エントリ編集画面

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	◉通過 ○廃棄 ○拒否
フィルタタイプ	◉転送 ○送受信
方向	◉in ○out
プロトコル	IPすべて プロトコル番号 TCP FLAG 指定なし ack fin psh rst syn urg ICMP MESSAGE 指定なし TYPE CODE
送信元IPアドレス	◉any ○ /
送信元ポート番号	☑any -
宛先IPアドレス	◉any ○ /
宛先ポート番号	☑any -

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

日本電気株式会社
ＮＥＣプラットフォームズ株式会社