OCN vUTMスタンダード ご利用ガイド

（ポータル操作編）

2.7版

docomo Business

はじめに

はじめに

本章では、ビジネスポータルからご利用できるOCN vUTMスタンダードの各種情報参照及び管理機能についてご説明およびご利用時の注意事項について記載いたします。

目次

はじめに

ご利用環境

下記のブラウザを通してご利用が可能です。

ご利用環境ブラウザ条件
Google Chrome 最新版
Mozilla Firefox 最新版
Internet Explorer 11以上
Microsoft Edge 最新版

OCN光 IPoE vUTMセットの契約番号

OCN光 IPoE vUTMセットの契約番号は、以下の2つの契約番号（N番号）で構成されています。

サービス名	契約サービスの内容
OCN 光 IPoE ●●プラン	拠点に敷設されたIPoE回線の契約番号
vUTMスタンダード	OCN光 IPoE vUTMセットで使用されているvUTMスタンダード機能の識別用契約番号(vUTM契約番号)

1. vUTMポータル

1-1　ログインおよびvUTM管理画面への遷移

① ビジネスポータルのログインページ「 https://b-portal.ntt.com/ 」へアクセスしてログインします。

※ビジネスポータルへのログイン手順詳細は、「ビジネスポータルご利用ガイド」をご参照ください。

② 「ダッシュボード」画面の「サービスメニュー」から「OCN for Business」-「OCN vUTM コントロールパネル」を選択しクリックします。

③ 該当VPNグループの「設定を変更する」をクリックします。

1-2 vUTMサービストップ画面

① トップ画面では各種リンクが表示されます。

他の画面よりTOP画面へ戻る場合には、ポータル画面上部のサービス名称左にある ＜ をクリックします。

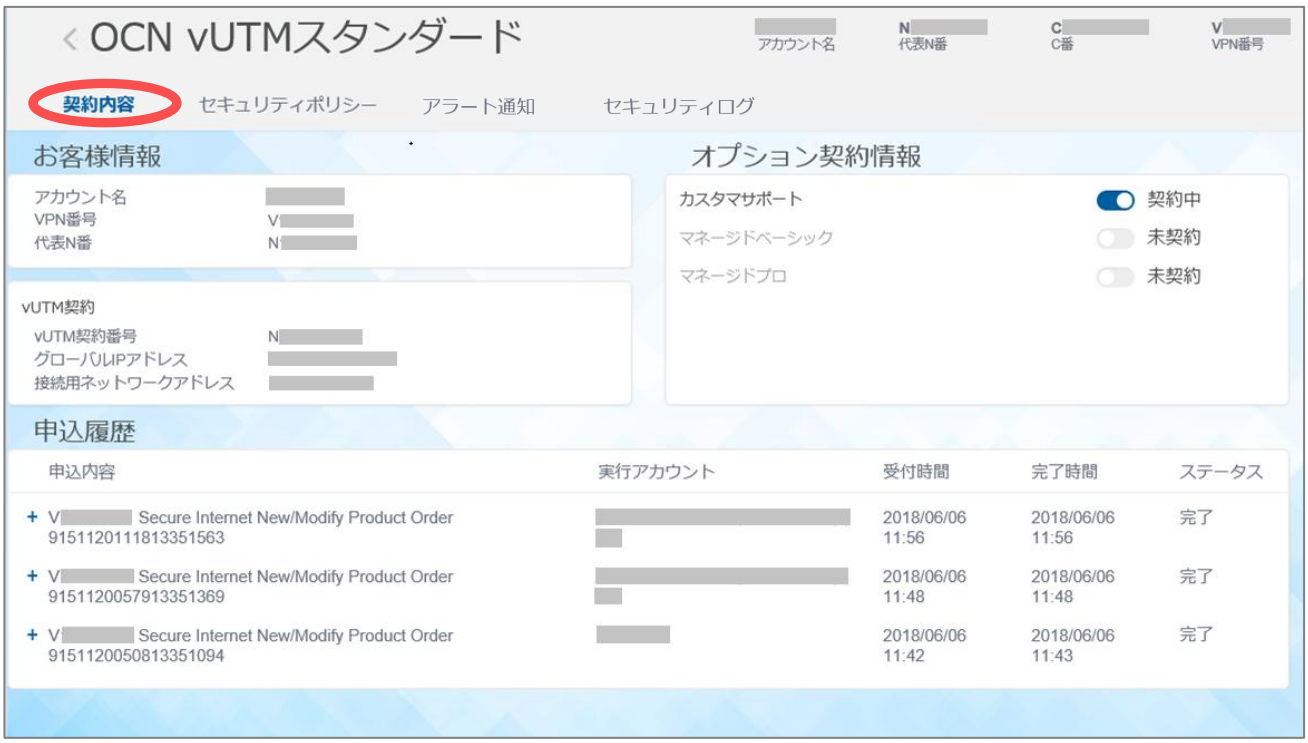
リンク先の設定項目の説明を以下に示します。

	項目	説明
1	契約内容確認・変更	ご契約内容、グローバルIPアドレス、接続用ネットワークアドレス、申込履歴の確認、ならびにカスタマサポートのお申し込みはこちらのリンク先から行います。
2	セキュリティポリシー設定	セキュリティポリシールールの確認およびカスタマイズはこちらのリンク先から行います。
3	アラート通知設定	アラートメール通知の設定変更はこちらのリンク先から行います。
4	セキュリティログ確認	セキュリティログを参照する場合はこちらのリンク先から行います。
5	アラート情報	日次アラートログ件数のグラフが表示されます。
6	申込み履歴	契約に関する申込み履歴が表示されます。
7	お知らせ	vUTMに関するお知らせが表示されます。

1. vUTMポータル

1-3　契約内容確認・変更画面

① 本画面にてvUTMのご契約内容、グローバルIPアドレス、接続用ネットワークアドレス、申込履歴の確認、ならびにカスタマーサポートのご契約申込みが可能です。



1-3-1　契約番号、グローバルIPアドレス、接続用ネットワークアドレスの確認

① 契約内容確認画面のお客様情報欄にて契約番号、グローバルIPアドレスおよび接続用ネットワークアドレスの確認ができます。

	項目	説明
1	vUTM契約番号	vUTM契約番号が表示されます。
2	グローバルIPアドレス	インターネット通信時の送信元となるアドレスが表示されます。お客様拠点からインターネット通信をする場合、お客様拠点アドレスは本項目で表示されるグローバルIPアドレスに変換されます。通信先となるアプリケーションサービス等で送信元アドレス認証などをしている場合にはこちらのアドレスをご利用ください。
3	接続用ネットワークアドレス	vUTM契約時に申込まれた接続用ネットワークアドレス/29が表示されます。

1-3-2　オプション契約（カスタマサポート）の確認・変更

① 契約内容確認画面のオプション欄にてカスタマサポートオプション契約のご確認およびお申し込みができます。

	項目	説明
1	カスタマサポート	ご利用状況の確認ができます。クリックにて契約の申込み/廃止を選択します。 カスタマサポートは、ポータルの利用方法、サービス内容に関するお問い合わせにお答えする有料オプションサービスです。ビジネスポータルのチケット作成のメニューから「ネットワーク」-「OCN for Business vUTM スタンダード」-「カスタマサポート/有料」よりお問合せチケットの作成が可能となります。
2	確定	お申し込み内容に間違いがないことをご確認のうえ、「確定」ボタンをクリックします。 契約のお申し込みが完了すると料金請求が発生します。

1-3-3　オプション契約（マネージドベーシック、マネージドプロ）の確認

① 契約内容確認画面のオプション欄にてマネージドベーシック、マネージドプロ契約の確認ができます。

各項目の説明を以下に示します。

	項目	説明
1	マネージドベーシック	契約のご利用状況が確認できます。 マネージドベーシックは、簡易なコンサルティングを提供する有料オプションサービスです。ポータルからのお申込みはできませんので、サービスのご利用を希望される場合は、営業担当または法人コンタクトセンター（0120-003300）へご連絡ください。
2	マネージドプロ	契約のご利用状況が確認できます。 マネージドプロは、セキュリティーポリシーの導入支援などを行うコンサルティングサービスです。ポータルからのお申込みはできませんので、サービスのご利用を希望される場合は、営業担当または法人コンタクトセンター（0120-003300）へご連絡ください。

1-3-4 申込履歴の確認

① 契約内容確認画面の申込履歴欄にて、契約に関するお申し込み内容や、セキュリティポリシーの設定変更の履歴が確認できます。

	項目	説明
1	申込履歴	契約に関するお申し込み内容や、セキュリティポリシーの設定変更の確認ができます。履歴は直近の操作履歴が先頭に表示されています。 • 申込内容：お申し込みに紐づいたVPN番号やオーダー番号が表示されています。該当のオーダーで「エラー」が発生している場合に、お申し込み内容の項目をチケット作成の際に記載してください。 • 実行アカウント：操作を行ったアカウントが表示されます。設定代行等でお申し込みいただいた場合は「NTT Com」が表示されます。 • 受付時間：お申し込みいただいた時間が表示されます。 • 完了時間：お申し込みいただいた内容の設定が完了した時間が表示されます。 • ステータス：お申込みいただいた操作の進捗が表示されます。エラーが発生した場合は「お問い合わせ」アイコンより、ネットワークカテゴリの「OCN for business vUTMスタンダード」から「故障（ポータル上でエラー表示）」にてチケットを作成してください。
2	＋	「＋」アイコンをクリックすると詳細が表示されます。

1. vUTMポータル

1-4 セキュリティポリシー設定画面

① 本画面にてセキュリティポリシーの一覧が閲覧可能です。
※vUTMの利用開始後に初めて本画面に遷移した際には、NTTドコモビジネス推奨の
セキュリティポリシーが表示されます。

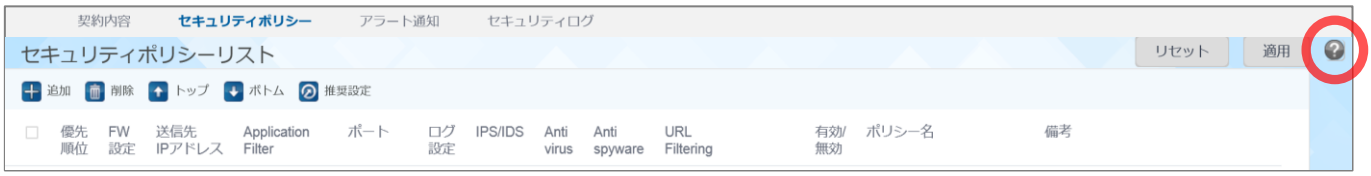
NTTドコモビジネス推奨セキュリティポリシーは以下の通りです。

項目	設定値	説明
送信先IPアドレス	制御なし（any）	ファイアウォールではステートフルパケットインスペクション機能が有効となっています。VPNからインターネットに接続する通信は、送信元IPアドレス/宛先IPアドレスでの制限がなく、すべて許可されます。また、インターネット発でVPNへ接続を開始する通信はすべてブロックされます。
アプリケーション	制御なし	特定のアプリケーションを指定した通信制御は行いません。
ポート	制御なし（any）	特定のプロトコル（TCP,UDP）、宛先ポート番号を指定した通信制御は行いません。
IPS/IDS	有効（IPS 中）	クライアントサーバーシステム上の脆弱性に対するネットワークを利用した攻撃を検出し防御します。「シグネチャ」と呼ばれる攻撃パターンのデータベースと一致する通信が発生し、重大度がCritical,High,Mediumに当てはまった場合にブロックします。
アンチウイルス	有効（中）	HTTP,FTP,SMB通信でアンチウイルスシグネチャに一致した場合は、全てブロックします。 SMTP,IMAP,POP3通信でアンチウィルスシグネチャに一致した場合は、ログのみ出力してそのまま通信を許可します。
アンチスパイウェア	有効（中）	スパイウェアおよびマルウェアのネットワーク通信を検知し防御します。アンチスパイウェアのシグネチャと一致する通信が発生し、重大度がCritical,High,Mediumに当てはまった場合にブロックします。
URLフィルタリング	有効（デフォルト）	以下のURLカテゴリに属するWebサイトへの通信をブロックします。 「ドラッグ」「アダルト」「コマンドアンドコントロール」「ギャンブル」「グレーウェア」「ハッキング」「マルウェア」「フィッシング」「ランサムウェア」「疑わしいサイト」「兵器」「スキャンアクティビティ」「侵害されたWebサイト」のURLカテゴリに属するWebサイトへの通信をブロックします。「暗号通貨」「人工知能(*)」「高リスク」「中リスク」「新規登録ドメイン」「リアルタイム検出」「リモートアクセス」「ファイルコンバーター」のURLカテゴリに属するWebサイトへの通信を監視します。

*細分化された「AIコードアシスタント」「AI会話アシスタント」「AIライティングアシスタント」「AIメディアサービス」「AI データおよびワークフロー最適化ツール」「AIプラットフォームサービス」「AI会議アシスタント」「AIウェブサイトジェネレーター」も含む

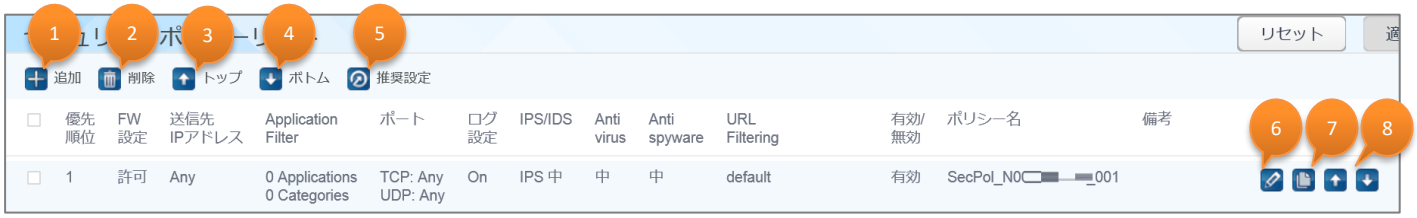
※セキュリティポリシー画面、セキュリティログ画面のヘルプウィンドウは、開閉可能です。
ヘルプウィンドウ上部の ✕ ボタンを押すことで閉じます。

ヘルプウィンドウを開く際は、? ボタンを押します。



1-4-1 セキュリティポリシーのカスタマイズ

① セキュリティポリシーリスト画面にて、以下の操作によりポリシールールのカスタマイズができます。NTTドコモビジネス推奨設定のポリシールールに対しても編集/削除が可能です。

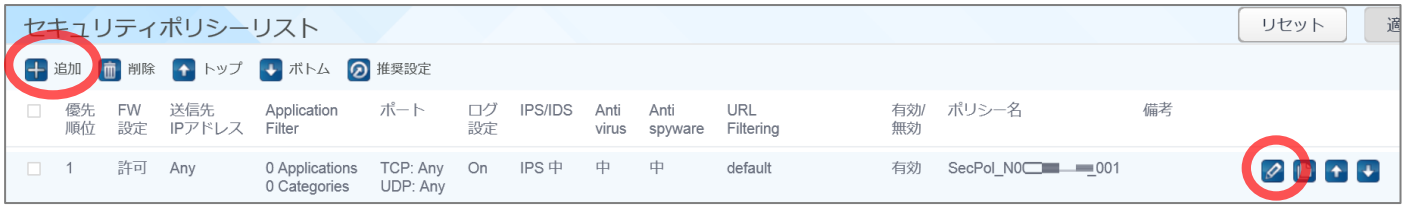


	項目	説明
1	追加	新しいポリシールールを追加します。新しいポリシールールは一番優先度の低いポリシールールとして追加されます。
2	削除	最左列にチェックを入れて選択したポリシールールを削除します。
3	トップ	最左列にチェックを入れて選択したポリシールールの優先度を一番高く変更します。
4	ボトム	最左列にチェックを入れて選択したポリシールールの優先度を一番低く変更します。
5	推奨設定	コムの推奨設定に戻ります。お客様にてカスタマイズしたポリシールールは全て削除されますのでご注意ください。
6		ポリシールールの上にマウスオーバーすることにより表示されます。該当行のポリシールールを対象として編集画面へ遷移します。
7		ポリシールールの上にマウスオーバーすることにより表示されます。該当行のポリシールールを複製します。
8		ポリシールールの上にマウスオーバーすることにより表示されます。クリックで該当行のポリシールールを上/下に一段毎移動します。

※ ポリシールール全ての削除はできません。最低1ルールは必須となります。
※ 画面上には表示されませんが、弊社運用用として、弊社保守用IPアドレスへのPing許可のルールが適用順位最優先で登録されています。このポリシールールの変更/削除はできません。

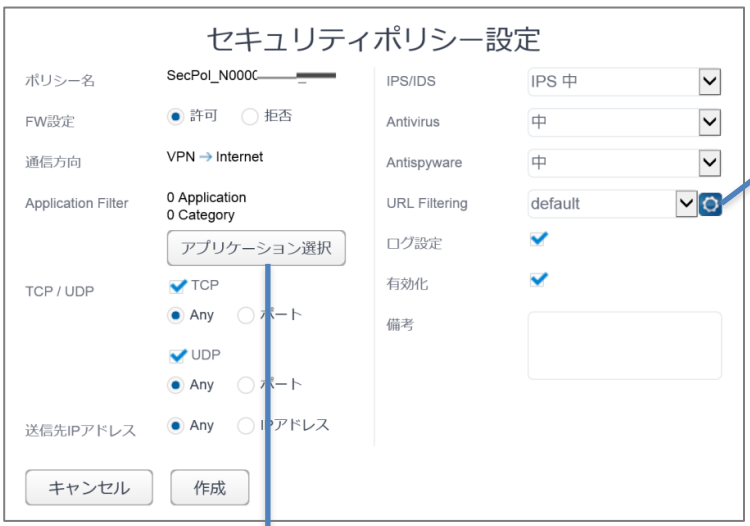
1-4-1 セキュリティポリシーのカスタマイズ

② 「追加」または、アイコンをクリックすると「セキュリティポリシー設定画面」が表示されます。



③ 各設定項目を入力します。

<セキュリティポリシー設定画面>



<URLフィルタリングプロファイル管理画面>

<アプリケーション選択画面>

<URLフィルタリングプロファイル作成画面>

1-4-1 セキュリティポリシーのカスタマイズ

＜セキュリティポリシー設定画面＞

	項目	説明
1	FW設定	ポリシールールに適合したトラフィックに対し、許可する/許可しないを指定します。
2	Application filter	web-browsingやdnsといったアプリケーションを指定して通信制御を行います。 アプリケーション選択のリンクをクリックし、「アプリケーション選択画面」へ遷移します。そこで選択したアプリケーションおよびアプリケーションカテゴリーの個数がこの欄に表示されます。
3	TCP/UDP	プロトコル（TCP,UDP）毎に、宛先ポート番号を指定して通信制御を行います。 全てのポートを指定する場合は“Any”を選択します。 個別ポートを指定する場合は、”ポート”を選択してから1～65535の範囲から指定できます。カンマ区切りで複数指定も可能です。また、ハイフンを使ってレンジ指定も可能です。入力可能最大文字数は100文字となります。 （例．53,80,443,50000-65535） ポートを１つも指定しない場合は、チェックボックスのチェックを外します。
4	送信先IPアドレス	宛先IPアドレスをホストアドレス、アドレスレンジ、またはサブネットマスクで指定して通信制御を行います。全てのアドレスを指定する場合は“Any”を選択します。 個別アドレスを指定する場合の入力形式は、XX.XX.XX.XX または、XX.XX.XX.XX/XX または、XX.XX.XX.XX-XX.XX.XX.XX のいずれかになります。カンマ区切りで複数指定も可能です。最大10個登録可能です。 （例．192.168.1.1, 172.16.10.10-172.16.10.20,10.10.10.0/24）
5	IPS/IDS	クライアントサーバーシステム上の脆弱性に対するネットワークを利用した攻撃を検出し通信制御を行います。セキュリティレベルに応じて、 「IPS 高」「IPS 中」「IPS 低」「IPS ログのみ」 「IDS 高」「IDS 中」「IDS 低」の中から一つプロファイルを指定できます。
6	Antivirus	アンチウイルス機能を有効にできます。セキュリティレベルに応じて、 「中」「高」「ログのみ」の中から一つプロファイルを指定できます。
7	Antispyware	スパイウェアおよびマルウェアのネットワーク通信を検知し防御できます。セキュリティレベルに応じて、 「中」「高」「低」「ログのみ」の中から一つプロファイルを指定できます。

1-4-1 セキュリティポリシーのカスタマイズ

（前ページの項目説明の続き）

	項目	説明
8	URL Filtering	お客様にてURLフィルタリングプロファイルを作成し、好ましくないWebサイトへの通信を遮断したりできます。設定アイコンをクリックすると「URLフィルタリングプロファイル管理画面」へ遷移します。そこで作成したURLフィルタリングプロファイルおよびNTT Com定義済みのデフォルトプロファイルがこちらの選択リストに表示されます。この中から一つプロファイルを指定できます。 予め用意されているNTTドコモビジネス定義済みの「default」プロファイルでは、以下のURLカテゴリに属するWebサイトへの通信をブロックします。 「ドラッグ」「アダルト」「コマンドアンドコントロール」「ギャンブル」「グレーウェア」「ハッキング」「マルウェア」「フィッシング」「疑わしいサイト」「兵器」「スキャンアクティビティ」「侵害されたWebサイト」 また「暗号通貨」「人工知能(*)」「高リスク」「中リスク」「新規登録ドメイン」「リアルタイム検出」「リモートアクセス」「ファイルコンバーター」のURLカテゴリに属するWebサイトへの通信を監視します。
9	ログ設定	ポリシールールが適用された場合に、ログとして記録する場合は「チェックあり」、記録しない場合は「チェックなし」を指定します。
10	有効/無効	検証目的等でポリシールール単位で無効の設定ができます。 ポリシールールを有効とする場合は「チェックあり」、無効とする場合は「チェックなし」を指定します。
11	備考	ポリシールールの説明などの用途として、任意で200文字まで登録ができます。

*細分化された「AIコードアシスタント」「AI会話アシスタント」「AIライティングアシスタント」「AIメディアサービス」「AI データおよびワークフロー最適化ツール」「AIプラットフォームサービス」「AI会議アシスタント」「AIウェブサイトジェネレーター」も含む

＜アプリケーション選択画面＞

	項目	説明
1	アプリケーション	NTTドコモビジネスが提供するアプリケーション一覧から指定いただきます。 最大50個まで指定可能です。
2	アプリケーション検索欄	アプリケーション名の検索が可能です。
3	カテゴリ	カテゴリにチェックを入れると、そのカテゴリに属するアプリケーションが右のアプリケーション一覧上で自動的にチェックがはいります。 カテゴリのチェックを外すと、そのカテゴリに属するアプリケーションが右のアプリケーション一覧上で自動的にチェックが外れます。

1-4-1 セキュリティポリシーのカスタマイズ

<URLフィルタリングプロファイル管理画面>

	項目	説明
1	追加	「URLフィルタリングプロファイル作成画面」へ遷移します。 URLフィルタリングプロファイルは、最大2個まで作成できます。 こちらで作成したプロファイルがセキュリティポリシー設定画面上に表示されて選択することが可能となります。
2		選択したURLフィルタリングプロファイルを削除します。
3		選択したURLフィルタリングプロファイルを対象として編集画面へ遷移します。

<URLフィルタリングプロファイル作成画面>

	項目	説明
1	プロファイル名	作成するURLフィルタリングプロファイルの名称を入力します。 半角英数字のみ入力可能です。
2	説明	作成するURLフィルタリングプロファイルの説明を入力します。

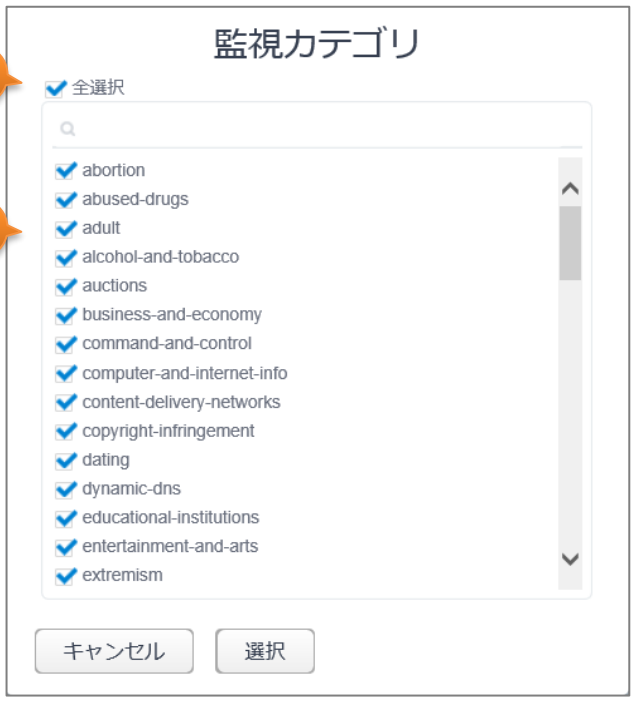
1-4-1 セキュリティポリシーのカスタマイズ

	項目	説明
3	許可リスト	許可するURLを最大15行まで入力可能です。 URLの「http://」、「https://」部分は省略して入力する必要があります。 ワイルドカード（*）を使用することが可能です。 「. / ? & = ; +」の7つは区切り文字として認識されます。 区切り文字の間に入力可能な文字は任意の長さの「ASCII文字」または「*」となります。 区切り文字の中に「ASCII文字」と「*」の双方を投入することはできません。 「*.ntt.com」は「www.ntt.com」を含みますが「ntt.com」は含みません。 双方を含む場合は「*.ntt.com」「ntt.com」の双方を定義する必要があります。 大文字と小文字は区別されます。 ※ワイルドカード（*）を使用される場合は、URL1行につき1つのみご使用ください。 ＜例＞ 「http://www.ntt.com/xxx/yyy/zzz.txt」とマッチさせたい場合、 「www.ntt.com/xxx」、「www.ntt.com/xxx/yyy」、 「www.ntt.com/xxx/yyy/zzz」のように区切り文字直前まで記述します。 ワイルドカードを使用する場合は、「*.ntt.com/」、 「*tt.com/xxx/yyy/zzz.」のように記述します。 「ww*.ntt.com」や「www.n*.com」のようには使用できません。
4	ブロックリスト	許可しないURLを最大15行まで入力可能です。 「3.許可リスト」の説明と同様の区切り文字やワイルドカードなどの条件が適用されます。 該当するページへアクセスした際はユーザ通知画面*を表示し、該当ページへの通信をブロックします。
5	監視/警告/ブロックURLカテゴリリスト※	カテゴリリストの中から、Webサイトのカテゴリを選択するための画面を開きます。選択済みのカテゴリ名が表示されます。 各カテゴリに該当するページへアクセスした際の動きは以下のとおりです。 • 監視カテゴリ 該当ページへのアクセスをURLフィルタリングのAlertログとして記録します。 ユーザ通知画面は表示されません。 • 警告カテゴリ アクセスして問題ないページかを確認させるユーザ通知画面*を表示します。「Continue」をクリックすると該当のページが属するカテゴリへ15分ほどアクセス可能となります。 • ブロックカテゴリ 通信をブロックした旨のユーザ通知画面*を表示し、該当カテゴリへの通信をブロックします。

※ httpsのサイトへアクセスした場合は、ユーザ通知画面は表示されずに、無応答（「安全な接続ができませんでした」等の画面表示）となります。
そのため警告カテゴリ設定時の「continue」ボタン押下による一時アクセス許可は行えません。

1-4-1　セキュリティポリシーのカスタマイズ

＜カテゴリ選択画面＞



	項目	説明
1	全選択	このチェックボックスにチェックを入れると、すべてのカテゴリへ一括でチェックを付けることが可能です。 また、チェックを外すとすべてのカテゴリのチェックが外れます。
2	個別選択	選択したいカテゴリを個別にチェックします。 既に選択済のカテゴリはチェックリスト上に表示されません。

カテゴリは以下のサイトで確認ができます。
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5hCAC

Webサイトがどのカテゴリに属するかは以下のサイトで確認できます。
https://urlfiltering.paloaltonetworks.com/

1-4-1 セキュリティポリシーのカスタマイズ

④ 各設定項目の入力を終えたら、「作成」ボタンをクリックします。
最大5個までセキュリティポリシールールの作成が可能です。

⑤ 作成したポリシールールはセキュリティポリシーリストの最下行に追加されます。
もしくは「トップ」、「ボトム」をクリックして優先順位を決めてから、「適用」をクリックします。申込み内容確認画面が表示されますので、お申込み内容に間違いがないことを確認のうえ、「確定」ボタンをクリックします。確定ボタンを押すと、UTMへ設定が反映されます。

1-5 アラート通知設定確認画面

① 本画面にてアラートメール通知の設定変更が可能です。

1-5-1 アラートメール通知の設定変更

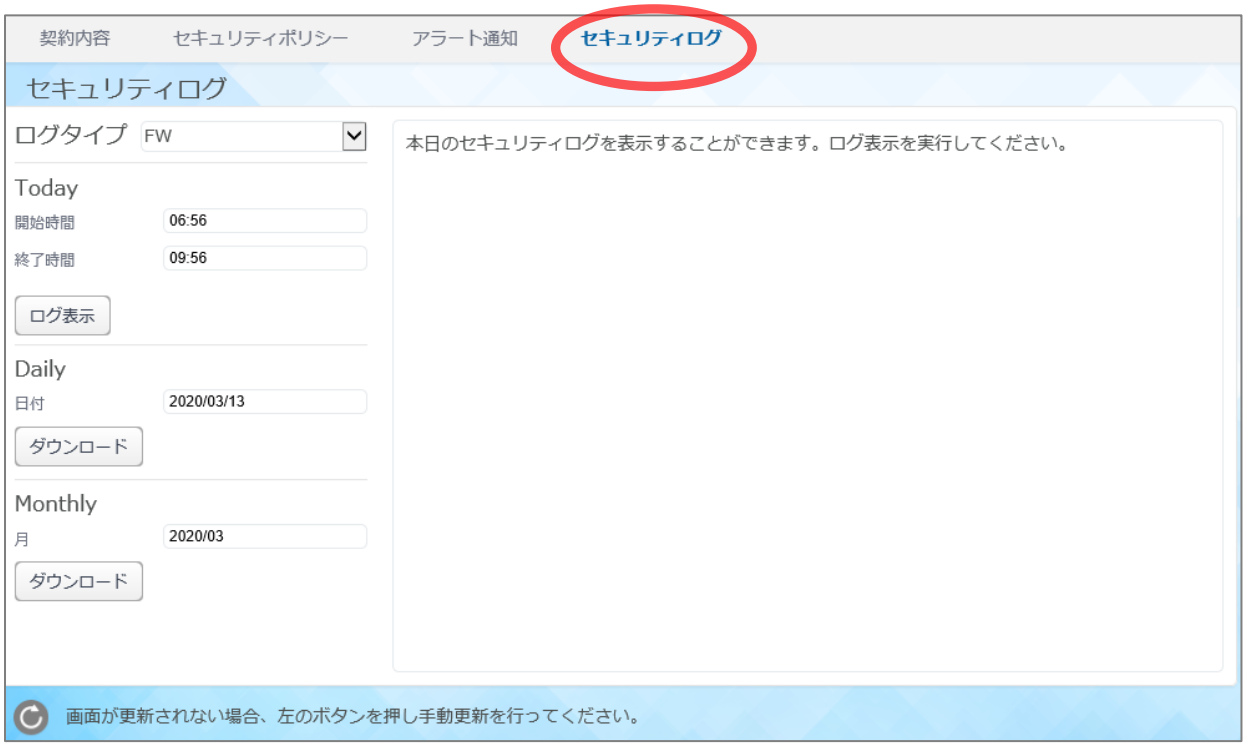
① メール通知欄にてアラートメール通知先の確認・変更および日次アラート通知のOFF/ONができます。「追加」をクリックするとメールアドレスの入力が可能になります。登録したら保存をクリックして確定を押下して設定は完了です。

	項目	説明
1	メールアドレス	vUTMの契約手続き完了メールやアラートメールの送付先が確認できます。日次アラート通知はセキュリティアラートおよびインターネット利用に関するアラート検出の件数を日単位で送付します。 ご利用にあたり、セキュリティポリシールール設定でログ出力がONになっていることが必要となります。「ログ設定」でログ保存をONとして保存したログを対象として日次アラート通知を行います。 メールアドレスは最大５つまで登録可能です。開通直後は新規お申込み時に登録した担当者のメールアドレスが保存されています。
2	担当者名	契約手続き完了メールの際、メール本文に記載される宛名となります。
3		登録されているメール送付先を削除します。
4		登録されているメール送付先を編集します。
5	追加	「追加」ボタンを押下して、メール送付先を追加します。
6	保存	「保存」ボタンを押下して、メール送付先を保存します。
7	日次アラート通知※	クリックで日次アラート通知のON/OFFの設定をします。
8	適用	クリックで申込み内容確認画面が表示されます。 お申込み内容に間違いがないことを確認のうえ、「確定」ボタンをクリックします。

※ メンテナンス及び故障等により、ログが保存されず欠損分のログが日次アラート通知メールに反映されない場合があります。
※ メンテナンス及び故障等により、日次アラート通知知ができない場合があります。
※ セキュリティアラートを100%検知することを保証するものではございません。

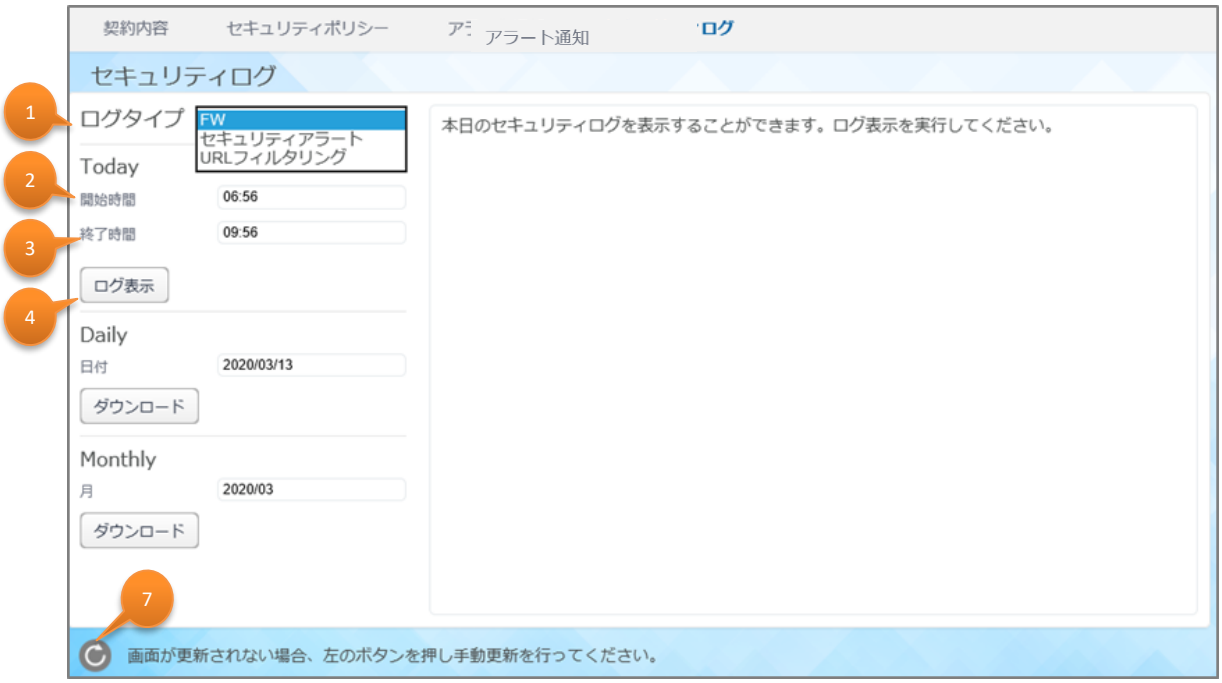
1-6 セキュリティログ確認画面

① 本画面にて、FWログ、セキュリティアラートログ、URLフィルタリングログの確認が可能です。



1-6-1　ログ参照

① セキュリティログ画面にて、各種ログの確認ができます。Todayログの確認手順は以下のとおりです。当日分（0時以降）のログは、時間を指定した絞り込みにより、画面上での閲覧が可能です。

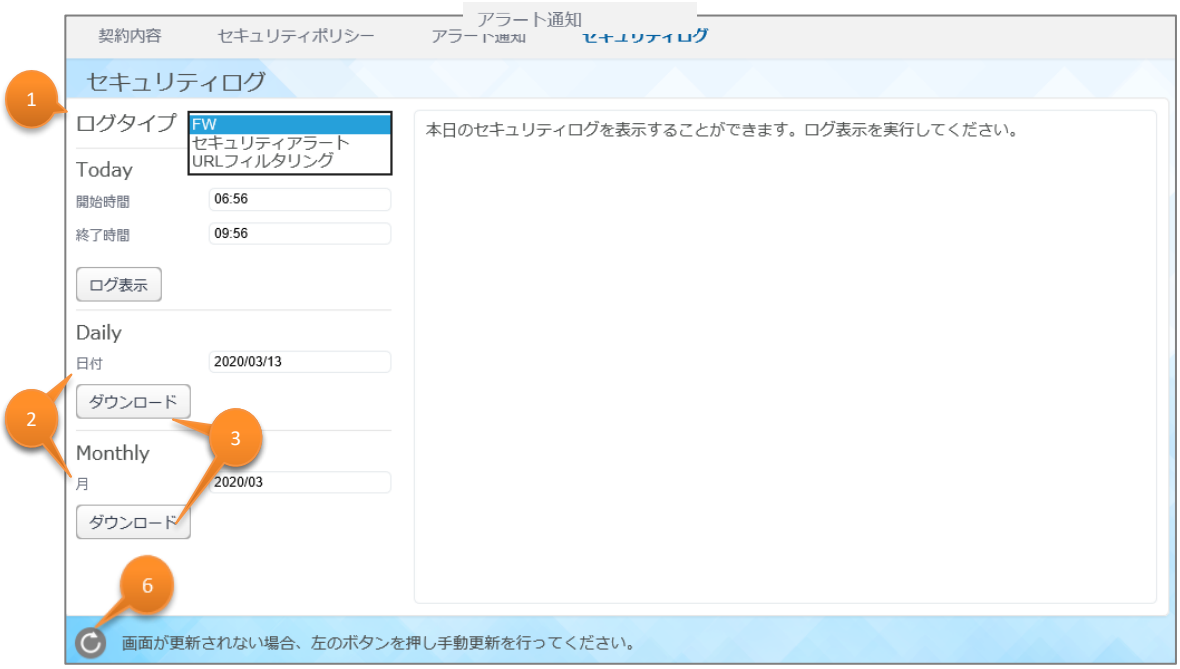


	項目	説明
1	ログタイプ	出力するログの種類をFW/セキュリティアラート/URLフィルタリングの中から選びます。 FWログは、deny処理のログが保存されます。 セキュリティアラートログは、Alert、Block処理のログが保存され、URLフィルタリングログでは、Alert、Continue、Block処理のログが保存されます。
2	開始時間	出力するログの絞り込みのために、開始時間を指定します。
3	終了時間	出力するログの絞り込みのために、終了時間を指定します。
4	ログ表示	「ログ表示」ボタンをクリックします。 ログ表示確認画面が表示されますので、「取得」ボタンをクリックします。 ログ出力の準備が終わると「取得したセキュリティログを表示」のボタンが表示されますのでクリックすると本日ログが画面上に表示されます。 ログ表示行数が10,000行を超える場合、複数ページに分割されます。ログ表示下部のページ番号をクリックすることで、参照したいページを表示します。
5		
6		
7	リロード	画面が更新されない場合、ボタンを押して手動更新します。

※ 出力する時間は3時間以内になるよう指定してください。

1-6-1　ログ参照

② Dailyログおよびログの確認手順は以下のとおりです。



	項目	説明
1	ログタイプ	出力するログの種類をFW/セキュリティアラート/URLフィルタリングの中から選びます。
2	日付/月	Dailyログの場合は日付を指定します。当月内の日にちを指定した絞り込みにより、csvのzipファイルにてダウンロードが可能です。 Monthlyログの場合は月を指定します。前月以前の月を指定した絞り込みにより、csvのzipファイルにてダウンロードが可能です。 ※2024年4月分のMonthlyログより、zipファイルの中に「vUTM_Service」というファイルが含まれます。 ※Monthlyログでは当月分でログがあった日ごとにzipファイルを出力します。
3 4 5	ダウンロード	「ダウンロード」ボタンをクリックします。 ログダウンロード確認画面が表示されますので、「ダウンロード」ボタンをクリックします。 ダウンロードが完了したファイルは「ダウンロード」ボタンの下にリンクが表示されますのでクリックにて保存できます。
6	リロード	リンクが表示されない場合、ボタンを押して手動更新します。

1-6-1　ログ参照

③ 保存されるログ内容は以下のとおりです。

- ログ保存は容量1GB、期間90日までとなります。1GBまたは90日間を超えた分は破棄されます。
  ※ 1GBはUTMから出力される全てのログ保存容量であり、実際にダウンロードできるログ出力項目はお客様向けに限定されますので、ダウンロードファイルのサイズは1GBを下回ります。
  ※メンテナンス及び故障等により、ログの保存ができない場合があります。
- ログを保存するには、セキュリティポリシールールの「ログ設定」でログ保存がONに設定されている必要があります。ログ設定がONのセキュリティポリシールールが適用された場合にログが保存されます。
- ファイアウォール機能では、拒否（Deny）処理のログが保存されます。
- アンチウイルス、IPS/IDS、アンチスパイウェアでは、Alert、Block処理のログが保存され、URLフィルタリングでは、Alert、Continue、Continue-block、Block処理のログが保存されます。
- ログの保存は各セッションの終了時に行われます。
- URL Filteringログは、大量のログ出力を抑えるためコンテナページのみログが保存されます。
- 出力されるログ内容は以下のとおりです。

<ログ出力項目一覧>

順番	出力項目名	FW	セキュリティアラート	URLフィルタリング	意味
1	Receive Time	○	○	○	ログを受信した時間
2	Type	○	○	○	ログのタイプ
3	Subtype	○	○	○	ログのサブタイプ
4	Source IP	○	○	○	お客様に払い出されたグローバルIPアドレス***1**
5	Destination IP	○	○	○	送信先IPアドレス***1**
6	Rule Name	○	○	○	システムで付与されたルール名***2**
7	Application	○	○	○	一致したアプリケーション名
8	Session ID	○	○	○	セッションID
9	Source Port	○	○	○	送信元ポート番号
10	Destination Port	○	○	○	送信先ポート番号
11	Protocol	○	○	○	IPプロトコル名
12	Action	○	○	○	実行したアクション名
13	Bytes	○			セッションの合計バイト数
14	Miscellaneous		○	○	一致したURL名
15	Threat ID		○	(9999)固定	脅威ID
16	Category	○	○	○	URLのカテゴリ
17	Severity		○	○	脅威の重大度

***1**：通信内容により、ログに記録される送信元IPと送信先IPが入れ替わることがあります。
***2**：システムが付与するルール名は、以下の通り

SecPol_<代表契約N番>_<通番>

1-6-1　　ログ参照

保存されるログの内容については、以下のサイトにて詳細を説明しています。（英語サイト）

＜FWログ＞
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/traffic-log-fields

＜セキュリティアラートログ／URLフィルタリングログ＞
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/threat-log-fields

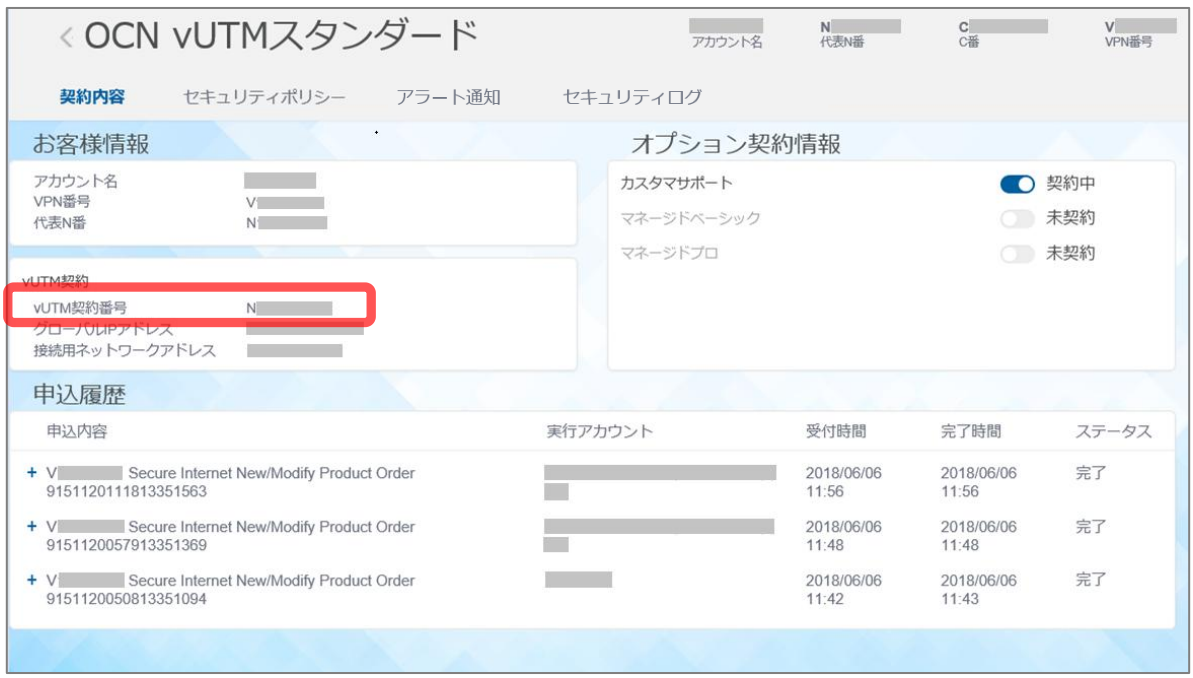
＜FWログ出力例＞
2016/12/12 08:40:24,TRAFFIC,end,11.20.174.1,210.145.254.162,SecPol_N160084020_001,dns,34797733,40465,53,udp,deny,202,any

＜セキュリティアラートログ出力例＞
2016/12/09 17:30:37,THREAT,virus,11.20.174.1,14.21.10.10,SecPol_N160092731_001,web-browsing,34507406,80,56688,tcp,deny,"eicar.com",Eicar Test File(100000),any,medium

＜URLフィルタリングログ出力例＞
2016/12/01 16:04:05,THREAT,url,11.20.174.1,118.215.187.173,recommend-TtoU-Permit-ANY,web-browsing,33919505,56560,80,tcp,block-url,"www.ntt.com/index.html",(9999),block-list,informational

2. お客様番号について

ご契約お客様番号として、Nから始まるOCN vUTMスタンダードのN番号があります。
トップ画面および契約内容確認・変更画面にてご確認いただけます。



お問い合わせのとき

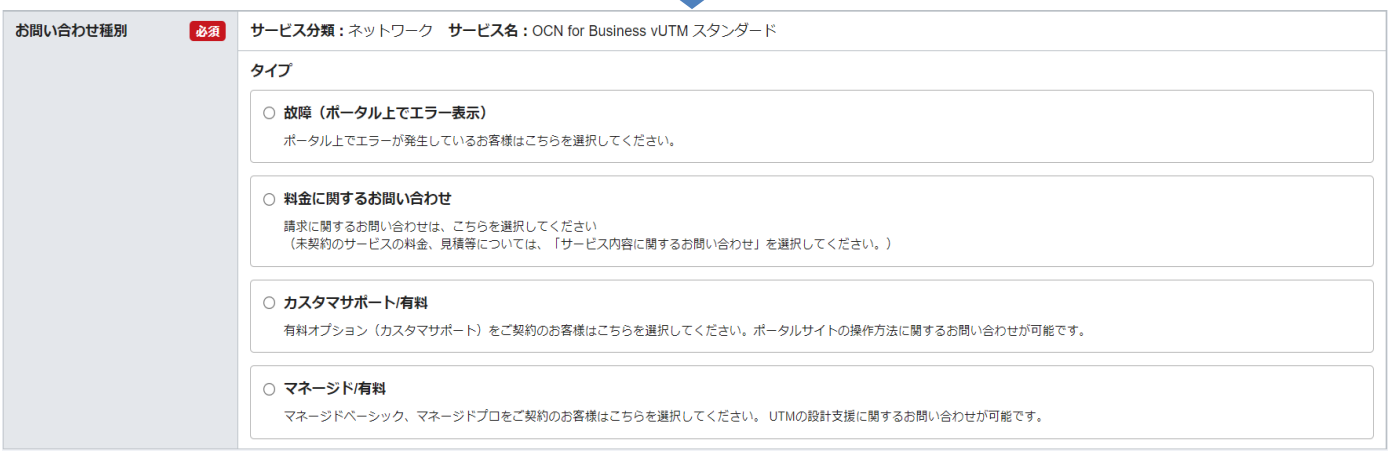
ビジネスポータルからチケットを起票する際に、vUTM契約番号（N番）をお知らせください。

3. vUTMお問い合わせ窓口

vUTMに関するお問い合わせは、ビジネスポータルの新規作成のメニューから「ネットワーク」-「OCN for business vUTMスタンダード」のカテゴリを選択しチケットを作成してください。

チケットのカテゴリについて

故障（ポータル上でエラー表示）
→ポータル操作によりエラーが表示された場合は、こちらを選択してください。
料金に関するお問い合わせ
→請求に関するお問い合わせは、こちらを選択してください。
カスタマサポート/有料
→ポータルの利用方法、サービス内容に関するお問い合わせは、こちらを選択してください。
※カスタマサポートのご契約がない状態でチケットを作成いただいてもお答えいたしかねますのでご了承ください。未契約の状態でチケットを作成してしまった場合は、カスタマーサポートのお申し込み後に再度チケットを作成していただく必要があります。
カスタマサポートのお申し込み方法は、
「1-3-2　オプション契約（カスタマサポート）の確認・変更」をご参照ください。
※セキュリティポリシー設計に関するお問い合わせはカスタマサポートではお受けいたしかねます。弊社営業担当または法人コンタクトセンター（0120-106107）までご連絡ください。
マネージド/有料
→マネージドベーシック、マネージドプロをご契約のお客様はこちらを選択してください。UTMの設計支援に関するお問い合わせが可能です。



※ネットワーク装置故障などによる通信障害は24時間365日の対応となりますが、vUTMの設定に関するポータル障害・設定サポートのお問い合わせへの対応は平日10：00～17：00となります。
※チケット作成の詳細入力画面でお客様のvUTM契約番号が表示されない場合は、カテゴリ選択画面に戻り「ネットワーク」の「OCN for business」から「申込に関するお問い合わせ」よりチケットを作成してください。

セキュリティポリシーの設計に関するご相談は、弊社営業担当またはドコモビジネスコンタクトセンター（0120-003300）までご連絡ください。

●工事情報・故障情報について　（下記URLにアクセスし、「OCN光 IPoE vUTMセット」をご参照ください。）
「NTTドコモビジネスお客様サポート」
工事情報・故障情報 URL： https://support.ntt.com/maintenance/

4. DNSのご利用について

インターネット上で名前解決を実施するDNSサーバーを、NTTドコモビジネスでご用意しております。お客さまLANにおけるインターネット利用端末、ないしCommunicationターミナルのDHCP機能によるDNSサーバーIPアドレス払い出しの設定に、必要に応じて下記IPアドレスを設定し、ご利用ください。

- インターネット接続用DNSサーバー　IPアドレス（推奨） -

プライマリDNSサーバーIP　210.145.254.162
セカンダリDNSサーバーIP　125.170.93.226

上記DNSでは、マルウェア不正通信ブロックサービスによりC&Cサーバへの通信を遮断します。本機能を利用したくない場合は、下記のDNSサーバを設定しご利用ください。

- インターネット接続用DNSサーバー　IPアドレス -

プライマリDNSサーバーIP　122.28.103.6
セカンダリDNSサーバーIP　125.170.93.174

5. ご利用時の注意点

- OCN vUTMスタンダードは、インターネット発でお客様拠点へ接続を開始する通信をすべて遮断します。
  そのため、サービスを利用しての外部サーバ公開やリモートアクセス等を行う事はできません。

- 混雑時にはスループットが約1Mbps程度まで低下しパケット廃棄が発生する場合があります。

- セキュリティインシデントをすべて検知/ブロックすることを保証するものではありません。

- ポータルからのvUTMスタンダード申込み可能時間は以下のとおりです。
  - 設定変更　：　時間制限なし
    ※ ただし、利用可能時間内であっても故障や緊急メンテナンスのためポータルが使えない場合があります。

- トラフィックレポートを参照する際は、ビジネスポータルへログイン後、「サービスメニュー」
  -「OCN for Business」-「トラフィックレポート」-「OCN vUTMスタンダード」からご確認ください。

  OCN光 IPoE VPN/vUTMセット：IPoE回線のトラフィックレポートを表示します（15分単位）
  OCN vUTMスタンダード　　：OCN網内のvUTM装置を経由したトラフィックレポートを表示します（5分単位）

- 1G以上のファイルサイズはダウンロードに時間がかかるため、タイムアウトによりファイルのダウンロードが失敗する場合があります。