Arcstar Universal One

インターネット接続機能（vUTMプレミアム）ご利用ガイド

（ポータル操作編）

2.29版

はじめに

本章では、ビジネスポータルからご利用できるvUTM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。

はじめに

目次

はじめに

目次

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

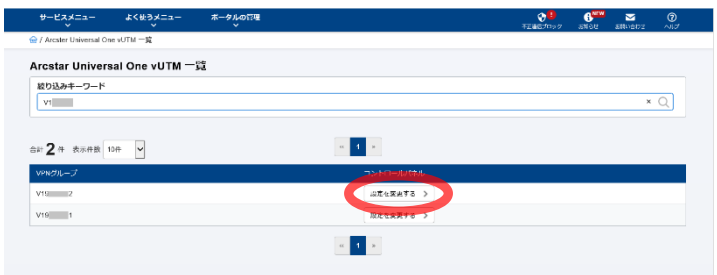
1. vUTMポータル

1-1　ログインおよびvUTM管理画面への遷移

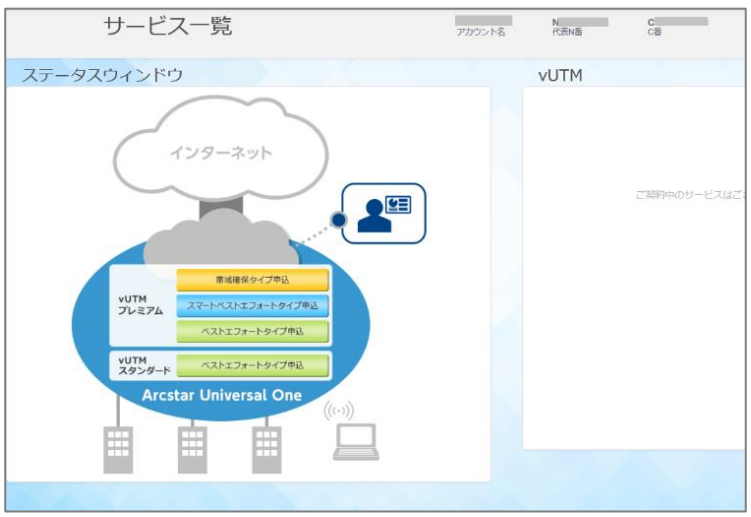
① ビジネスポータルのログインページ「 https://b-portal.ntt.com/ 」へアクセスしてログインします。

※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「Arcstar Universal One」-「vUTM」を選択しクリックします。



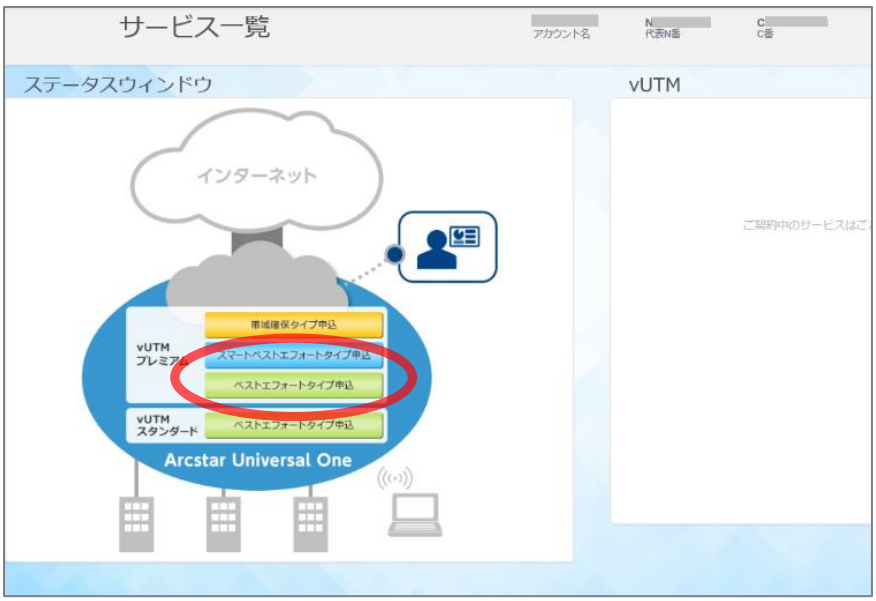
③ 該当VPNグループの「設定を変更する」をクリックします。



④ vUTMの管理トップ画面が表示されます。こちらの画面からvUTMにかかわる各種情報参照及び管理機能がご利用できます。

1-2 vUTMの起動

① 本サービスを起動するには、ステータスウィンドウの「ベストエフォートタイプ申込」もしくは「スマートベストエフォートタイプ申込」のボタンをクリックします。
※本申込み可能時間は、平日9時30分～17時30分となります。



② vUTMプレミアム申込画面が表示されます。各設定項目を入力し、「確認」ボタンをクリックします。

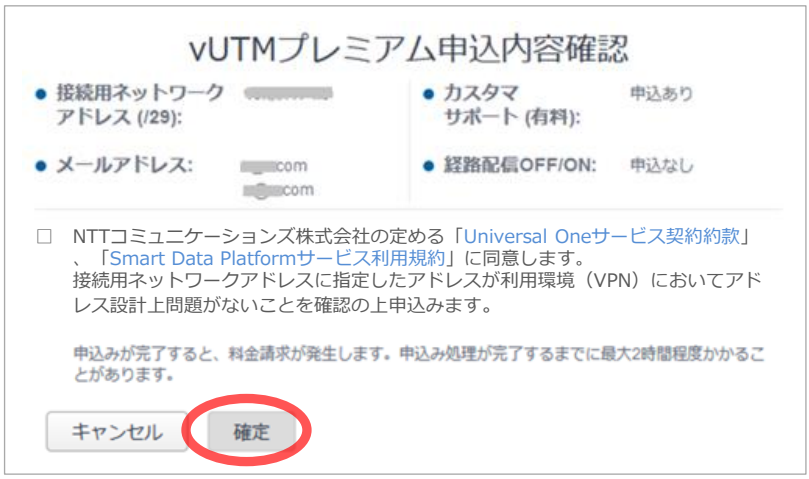
1-2 vUTMの起動

	項目	説明
1	接続用ネットワークアドレス	接続用ネットワークアドレスを指定してください。お客様ネットワーク内（網内利用アドレス含む）で重複しないプライベートIPアドレスを指定してください。後からの変更はできませんのでお間違えの無いようご注意ください。サブネットマスクは/29のネットワークアドレス固定です。
2	メールアドレス	お客様のメールアドレスを1つ以上入力してください。契約手続き完了の連絡やセキュリティアラート連絡先として利用します。別途修正、追加は可能です。
3	担当者名	担当者名を記載してください。メール送信時の宛名として利用させて頂きます。
4	カスタマサポート（有料）	カスタマサポートオプション（有料）を申し込まれる場合は選択します。
5	経路配信OFF/ON	通常はデフォルト設定ONのままとします。 既存でご利用のインターネット接続回線からvUTMへ切り替える際に、vUTMは起動するが、デフォルトルートを各拠点へ配信したくない場合にはOFFとして申し込みます。OFFとした場合は、デフォルトルートが配信されないため、vUTM経由でのインターネット通信ができない状態となります。vUTM起動後は平日9時30分～17時30分の時間制限に関係なく、任意のタイミングでONとしてデフォルトルートを配信することが可能です。

1-2 vUTMの起動

③ vUTMプレミアム申込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。お申込みが完了すると料金請求が発生します。

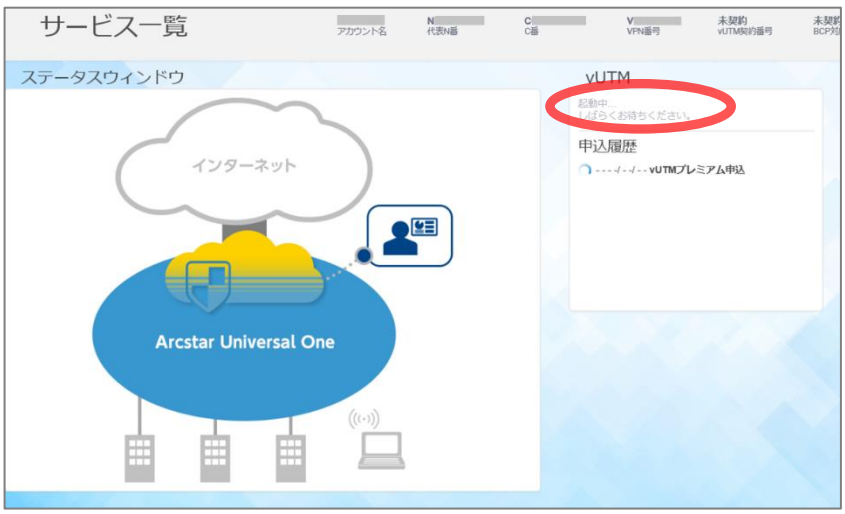
＜vUTMプレミアム（ベストエフォートタイプ）をお申込みの場合＞



＜vUTMプレミアム（スマートベストエフォートタイプ）をお申込みの場合＞

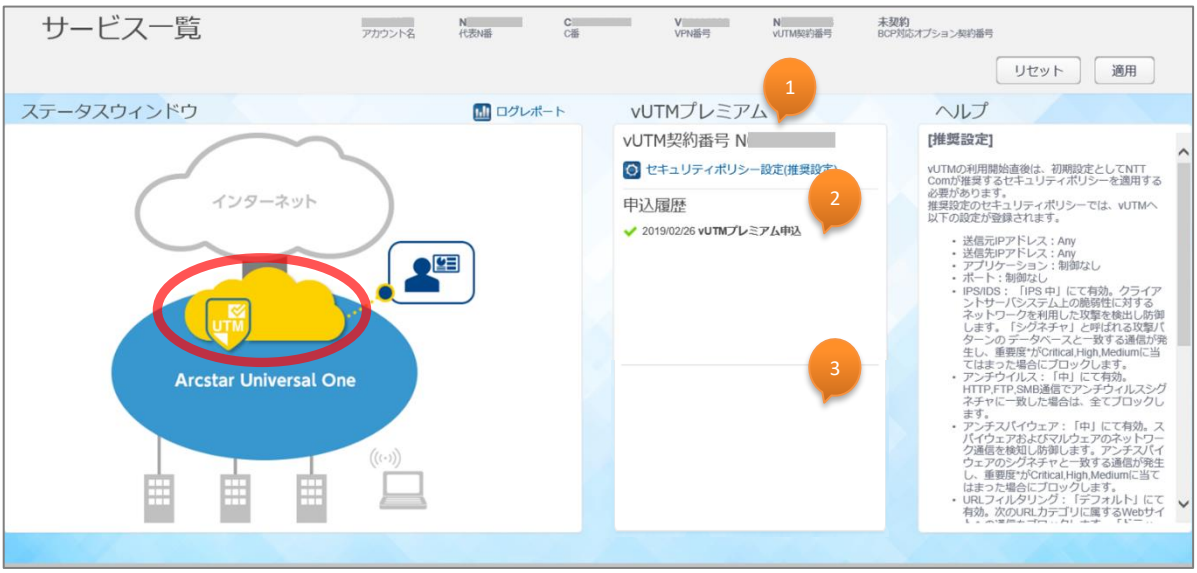
1-2 vUTMの起動

④ 「起動中… しばらくお待ちください。」が表示されます。起動完了までに最大2時間程度かかる場合があります。



1-2 vUTMの起動

⑤ サービスが起動されると、ステータスウィンドウのvUTMアイコンが黄色に変わり、vUTM契約番号が表示されます。この時点でVPNからインターネットに接続する通信はすべて許可*されるデフォルトポリシーが適用されます。続けて、ドコモビジネス推奨セキュリティポリシーを適用するために「1-3」を実施ください。
＊経路配信OFFとして起動した場合は、デフォルトルートが配信されないためインターネット通信はできない状態となります。



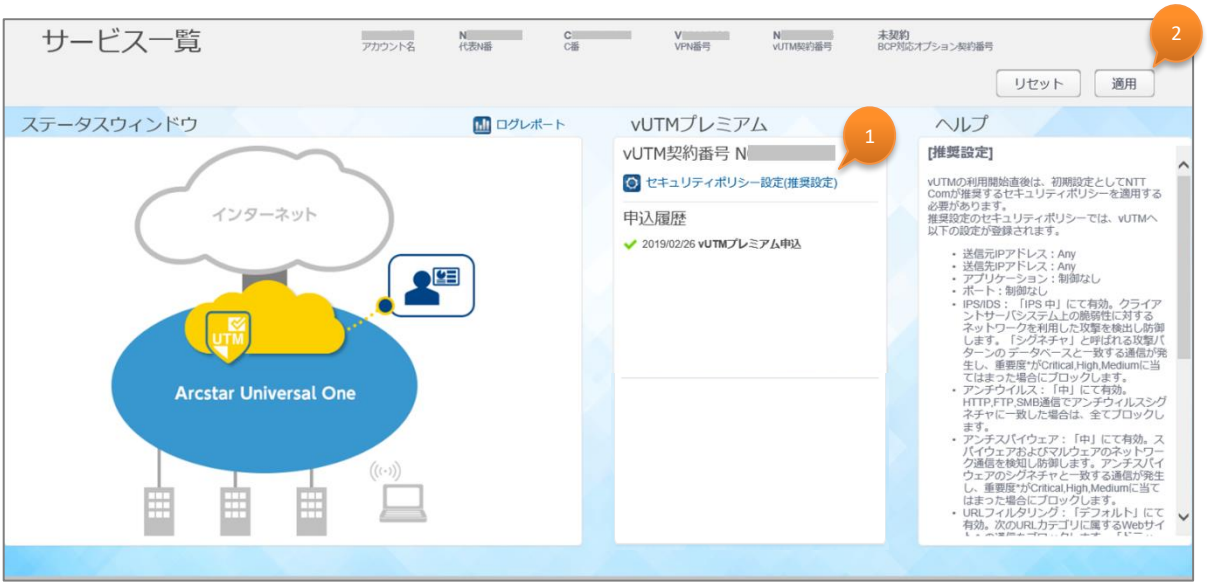
	項目	説明
1	vUTM契約番号	vUTMの契約番号です。お問い合わせの際は本契約番号をご利用ください。
2	申込み履歴	契約に関する申込み履歴が表示されます。
3	お知らせ	vUTMに関するお知らせが表示されます。

デフォルトポリシーは以下の通りです。

項目	設定値	説明
送信元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、インターネット発通信でVPNへ接続する通信はすべてブロックされます。
送信先IPアドレス	制御なし（any）	
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	無効	IPS/IDSプロファイルは適用されません。
アンチウイルス	無効	アンチウイルスプロファイルは適用されません。
アンチスパイウェア	無効	アンチスパイウェアプロファイルは適用されません。
URLフィルタリング	無効	URLフィルタリングプロファイルは適用されません。

1-3 ドコモビジネス推奨セキュリティポリシーの適用

① セキュリティポリシー設定（推奨設定）をクリックすることでドコモビジネスがあらかじめ用意した推奨のセキュリティポリシーを適用することができます。



	項目	説明
1	セキュリティポリシー設定（推奨設定）	ドコモビジネスが予め指定したセキュリティポリシー推奨設定を適用する場合はこちらをクリックします。 セキュリティポリシー推奨設定適用後は、お客様にてセキュリティポリシーのカスタマイズも可能となります。
2	適用	クリックで申込み内容確認画面が表示されます。
3	確定	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、ドコモビジネスが予め指定したセキュリティポリシー推奨設定が適用されます。

1-4 ドコモビジネス推奨セキュリティポリシーの説明

① ドコモビジネス推奨の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
送信元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。
送信先IPアドレス	制御なし（any）	
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）	「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。 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」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

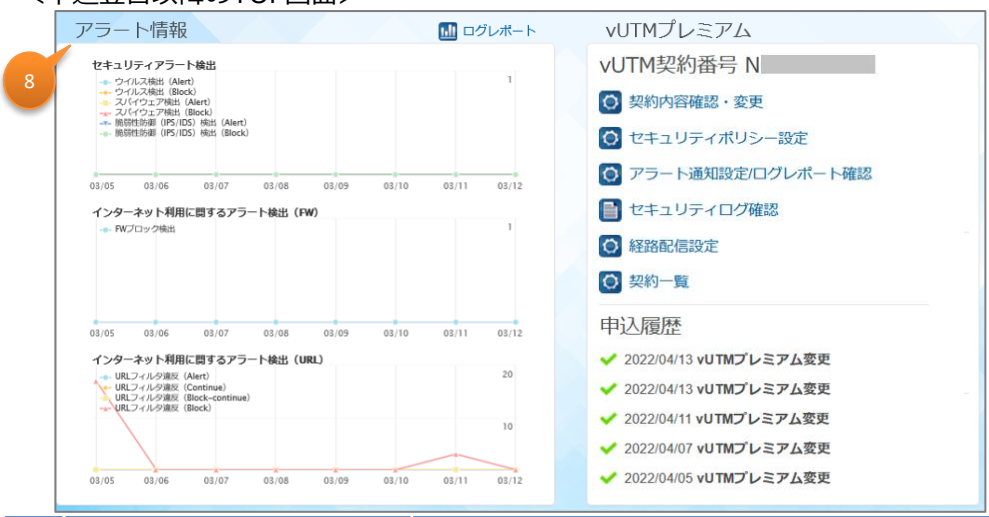
1-5 ドコモビジネス推奨セキュリティポリシーの適用後の画面遷移

① セキュリティポリシー設定（推奨設定）適用後は各種リンクが表示されるようになります。
また、申込翌日よりアラート情報が表示されるようになります。

＜申込当日のTOP画面＞

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。

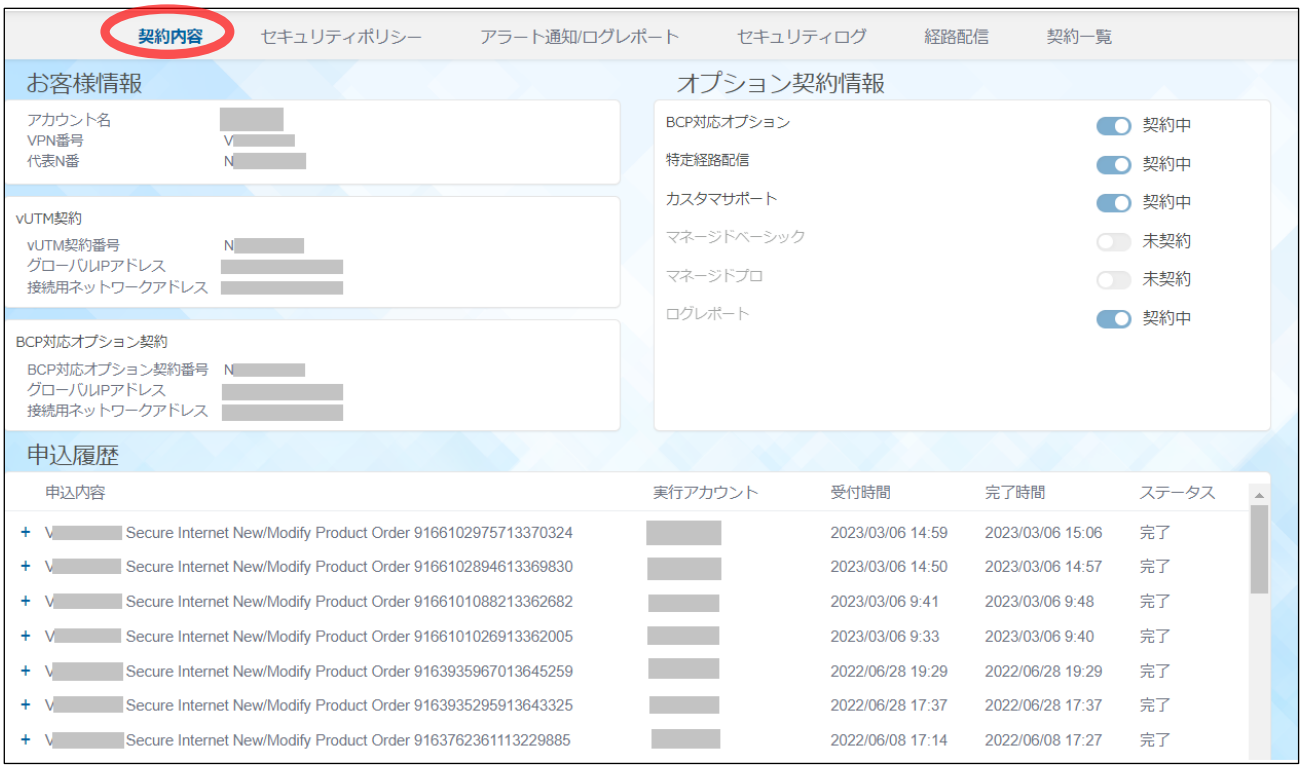
＜申込翌日以降のTOP画面＞



	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、BCP対応オプションの申込み、およびvUTM契約の廃止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/ログレポート確認	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。また、ログレポートオプションをご契約の場合は、ログレポートのダウンロードおよびリアルタイムアラート通知の設定変更が可能です。
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	経路配信設定	経路配信OFF/ONの設定変更はこちらのリンク先から行います。また、特定経路配信オプションの申込みおよび設定変更が可能です。
6	契約一覧	同一VPN番号で契約中のvUTM情報が表示されます。
7	ログレポート	ログレポート画面を起動します。
8	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。

1-6 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、ならびにカスタマサポート、BCP対応オプションの契約申込み、およびvUTM契約の廃止が可能です。



1-6-1　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。
4	BCP対応オプション契約	BCP対応オプションをご契約の場合は、BCP対応オプション用のvUTM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が表示されます。グローバルIPアドレスは上記の「2.グローバルIPアドレス」と同様に、BCP切替時におけるインターネット通信時の送信元IPアドレスとなります。

1-6-2　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確認および申込みができます。

	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」-「Arcstar Universal One vUTM」-「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。 契約のお申込みが完了すると料金請求が発生します。

1-6-3 オプション契約（マネージドベーシック、マネージドプロ、ログレポート、特定経路配信）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、ログレポート、および特定経路配信契約の確認ができます。

	項目	説明
1	特定経路配信	契約のご利用状況が確認できます。 特定経路配信は、お客様が指定した任意のグローバルIPアドレス（上限50個）のみをvUTM経由で通信することを可能とするサービスです。サービスのご利用を希望される場合は、「経路配信」タブ画面よりお申込みください。
2	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、営業担当へご連絡ください。
3	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、営業担当へご連絡ください。
4	ログレポート	契約のご利用状況が確認できます。 ログレポートは、契約中のvUTMのログを取得し、「ログレポート」、「リアルタイムアラート通知」を提供するサービスです。サービスのご利用を希望される場合は、「アラート通知/ログレポート」タブ画面よりお申込みください。

1-6-4　オプション契約（BCP対応オプション）の確認・変更

① 契約内容確認画面のオプション欄にてBCP対応オプション契約の確認および申込みができます。

	項目	説明
1	BCP対応オプション	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。 BCP対応オプションは、インターネット接続ポイントを西日本にも追加するサービスです。地震などの大規模災害に強く、盤石なネットワーク基盤が構築可能です。BCP切替は自動で行われ、設定されたセキュリティポリシーは引き継がれます。 ※BCP対応オプションの申込みと廃止を同日に行うことはできません。

② 本サービスを申込むには、BCP対応オプションをクリックにてオンにします。
※本申込み可能時間は、平日9時30分～17時30分となります。

③ BCP対応オプションは他の申込と同時に行えない旨の確認画面が表示されます。他の申込がないことを確認のうえ、「確認」ボタンをクリックします。

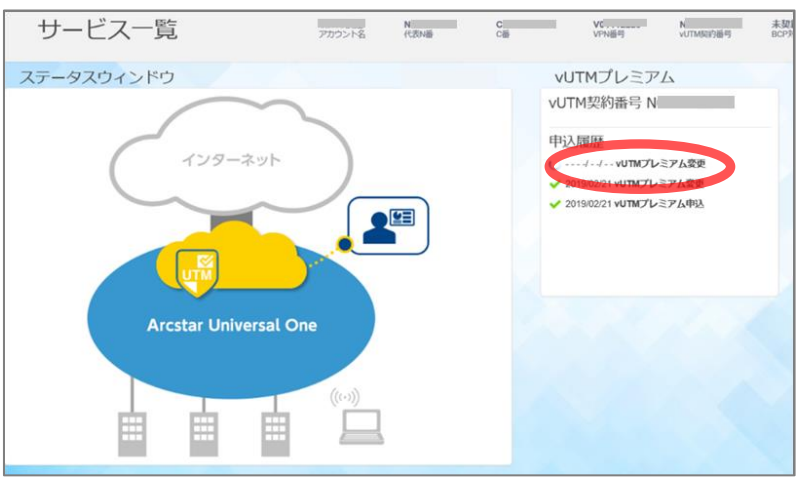
1-6-4 オプション契約（BCP対応オプション）の確認・変更

④ BCP対応オプション申込画面が表示されます。接続用ネットワークアドレスを入力し、「確認」ボタンをクリックします。

	項目	説明
1	接続用ネットワークアドレス	接続用ネットワークアドレスを指定してください。お客様ネットワーク内（vUTM新規契約時に申込まれた「接続用ネットワークアドレス/29」および網内利用アドレス含む）で重複しないプライベートIPアドレスを指定してください。後からの変更はできませんのでお間違えの無いようご注意ください。サブネットマスクは/29のネットワークアドレス固定です。

⑤ 申込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。お申込みが完了すると料金請求が発生します。

⑥ 「vUTM変更」が表示されます。起動完了までに最大2時間程度かかる場合があります。



1-6-5　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：申込みに紐づいた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、申込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。設定代行等でお申込みいただいた場合は「ドコモビジネス」が表示されます。 • 受付時間：お申込みいただいた時間が表示されます。 • 完了時間：お申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「Arcstar Universal One vUTM」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。 チケット作成の詳細入力画面でお客様の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カテゴリの「Arcstar Universal One」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。
2	＋	「＋」アイコンをクリックすると詳細が表示されます。

1-6-6　vUTM契約の廃止

① 契約内容確認画面のvUTM契約状態欄をクリックしてvUTMの解約ができます。
※本申込み可能時間は、平日9時30分～17時30分となります。

	項目	説明
1	vUTM契約状態	vUTMの契約状態が確認できます。サービスを廃止する場合はこのアイコンをクリックしてください。 *申込当日の廃止申込はできません。翌営業日以降改めてお申込みください。 *BCP対応オプションご契約中の場合は、BCP対応オプションを廃止した上でお申込みください。
2	確定	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。 お申込みが完了するとvUTMが廃止されご利用ができなくなります。

1-7 セキュリティポリシー設定画面

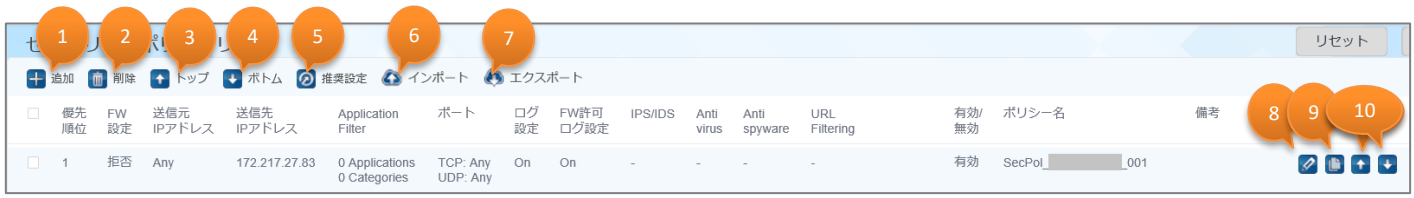
① 本画面にてセキュリティポリシーの一覧が閲覧可能です。
※vUTMの利用開始後にはじめて　本画面に遷移したさいには、ドコモビジネス推奨の
セキュリティポリシーが表示されます。

※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。

1-7-1 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。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。

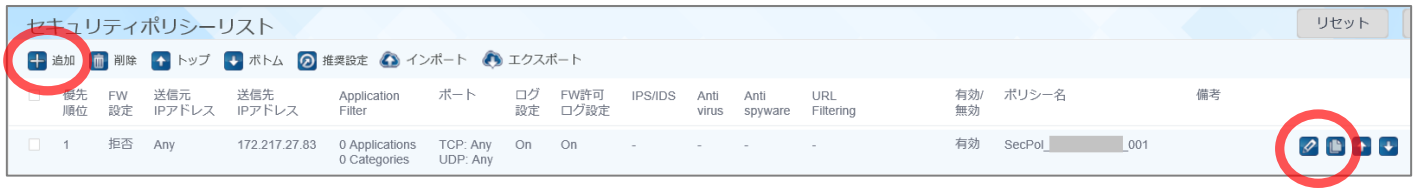


	項目	説明
1	追加	新しいポリシールールを追加します。新しいポリシールールは一番優先度の低いポリシールールとして追加されます。
2	削除	最左列にチェックを入れて選択したポリシールールを削除します。
3	トップ	最左列にチェックを入れて選択したポリシールールの優先度を一番高く変更します。
4	ボトム	最左列にチェックを入れて選択したポリシールールの優先度を一番低く変更します。
5	推奨設定	コムの推奨設定に戻ります。お客様にてカスタマイズしたポリシールールは全て削除されますのでご注意ください。
6	インポート	エクスポートしたファイルを読み込みます。
7	エクスポート	現在設定しているセキュリティポリシーをファイルに出力します。
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。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。
9		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、設定画面へ推移します。
10		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。

1-7-1 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>

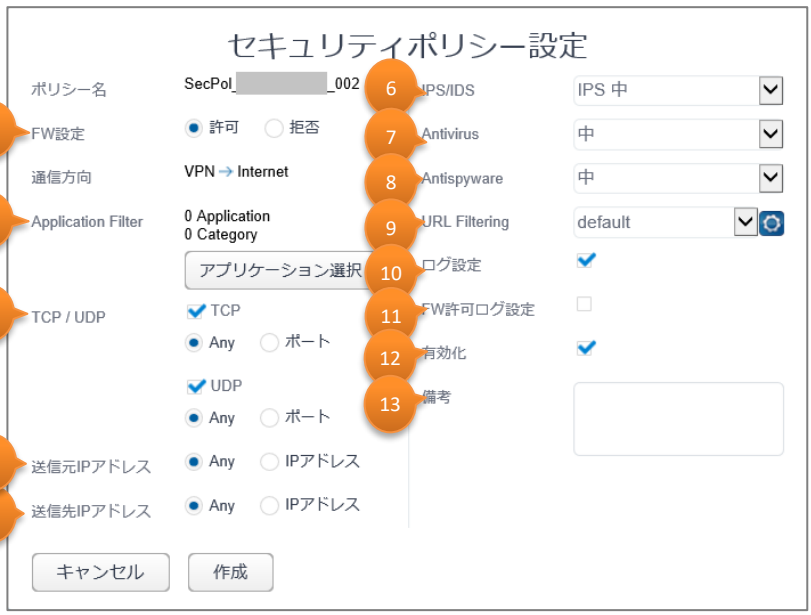
<URLフィルタリングプロファイル作成画面>

<アプリケーション選択画面>

<URLカテゴリ選択画面>

1-7-1 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	送信元IPアドレス	送信元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 のいづれかになります。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	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。入力規則は送信元IPアドレスと同じとなります。
6	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。
7	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。
8	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。

1-7-1 セキュリティポリシーのカスタマイズ

	項目	説明
9	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ドコモビジネス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」「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」 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」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
10	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。
11	FW許可ログ設定	FW設定を許可にしたログを記録する場合は、「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。 ※ログ設定が「チェックなし」の場合、FW許可ログはチェックの有無に関わらず記録されません。FW許可ログを記録したい場合は必ずログ設定も「チェックあり」にしてください。
12	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。
13	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。

1-7-1 セキュリティポリシーのカスタマイズ

<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	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。

<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50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。

1-7-1 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。
3	許可リスト	許可するURLを最大300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。 「*.example.com」は「www.example.com」を含みますが「example.com」は含みません。 双方を含む場合は「*.example.com」「example.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.example.com/xxx/yyy/zzz.txt」とマッチさせたい場合、「www.example.com/xxx」、「www.example.com/xxx/yyy」、「www.example.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、「*.example.com/」のように記述します。 「ww*.example.com」や「www.e*.com」のようには使用できません。“

1-7-1 セキュリティポリシーのカスタマイズ

	項目	説明
4	ブロックリスト	許可しないURLを最大300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。

1-7-1　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。 既に選択済み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/

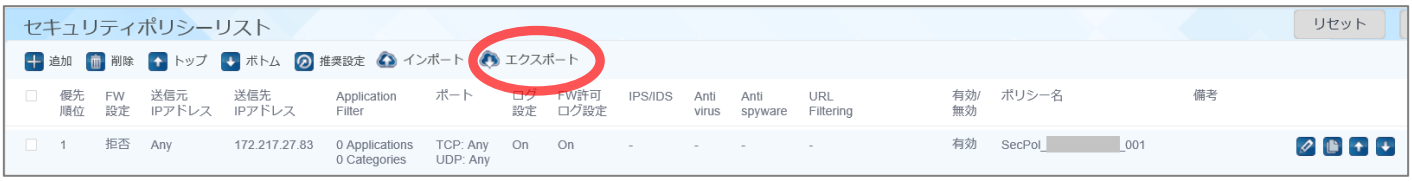
1-7-1 セキュリティポリシーのカスタマイズ

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50個までセキュリティポリシールールの作成が可能です。

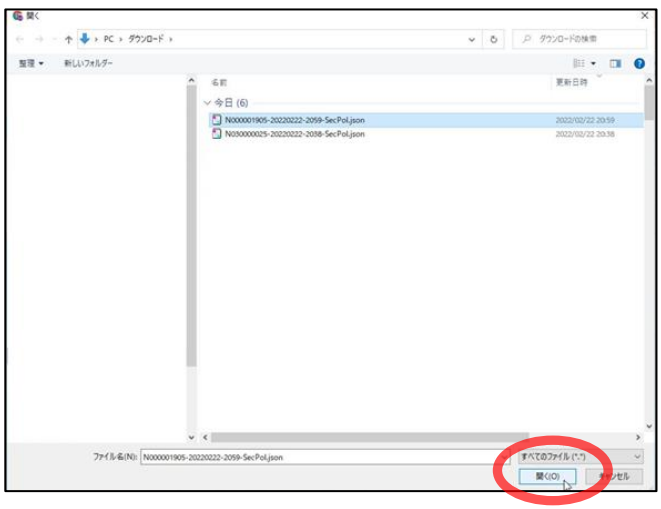
⑤ 作成したポリシールールはセキュリティポリシーリストの最下行に追加されます。
もしくは「トップ」、「ボトム」をクリックして優先順位を決めてから、「適用」をクリックします。申込み内容確認画面が表示されますので、お申込み内容に間違いがないことを確認のうえ、「確定」ボタンをクリックします。確定ボタンを押すと、UTMへ設定が反映されます。

1-7-2 セキュリティポリシーのエクスポート/インポート

① エクスポートをクリックすると確認画面が表示されます。「確認」ボタンをクリックするとファイルが保存されます。



② インポートをクリックするとフォルダが表示されます。①で保存したファイルを選択し「開く」ボタンをクリックするとポリシーは反映されます。



1-8 アラート通知設定/ログレポート確認画面

① 本画面にてアラートメール通知の設定変更およびログレポートオプション契約の確認とお申込みができます。また、ログレポートオプションをご契約の場合は、月次レポートのダウンロード、ログレポート画面の起動およびリアルタイムアラート通知の設定変更が可能です。

※ ログ保存上限は容量10GBであるため、超えた分は破棄されレポートの対象外となります。
※ 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、ログレポートおよびリアルタイム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、リアルタイムアラート通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。

1-8-1 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。

	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。 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。 また、ログレポートオプションをご契約の場合は、リアルタイムアラートの送付先としても使われます。
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。

1-8-2 ログレポートの確認とリアルタイムアラート通知の設定変更

① ログレポートオプションのお申込み、および契約有無の確認が行えます。ご契約がある場合は、ログレポート欄にて月次レポートのダウンロードおよびログレポート画面の起動が可能となります。また、リアルタイムアラート通知欄にてリアルタイムアラート通知の設定変更も可能となります。

	項目	説明
1	ログレポート（有料）	• 契約のご利用状況が確認できます。 • ログレポートは、契約中のvUTMのログを監視し、「ログレポート」、「月次レポート」と「リアルタイムアラート通知」を提供するサービスです。 • ログレポートオプション（有料）をお申込みする場合は「ON」を指定します。 • ログレポートオプション（有料）を廃止する場合は「OFF」を指定します。 ＊ 本項目は本オプション契約申込みと廃止を指定する項目となります。OFF/ONを繰り返し申込みすると契約した回数分の課金が発生してしまいますのでご注意ください。 • 利用にあたり、vUTMが起動中であり、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レポート作成とリアルタイムアラート通知を行います。
2	ログレポートダウンロード	• ログレポートオプションのご契約がある場合は、月次レポートのダウンロードが可能となります。 • 毎月10日までに前月分の月次レポートが自動生成され、ダウンロード可能となります。 • 出力形式は、ダウンロード時はZip形式で解凍後はPdf形式のファイルとなります。

1-8-2 ログレポートの確認とリアルタイムアラート通知の設定変更

	項目	説明
3	ログレポート	• ログレポートオプションのご契約がある場合に、ログレポート画面を提供します。 • データ期間指定、グラフの追加、削除、編集が可能です。 • 作成した画面構成の保存、PDFファイル化が可能です。 • ログレポートオプション未契約の場合でも、ログレポート画面の無料トライアル利用が1回のみ実行できます。（無料トライアル開始日より30日間有効）
4	リアルタイムアラート通知	• アラートの種類毎に、アラート通知のOFF/ON設定と、アラート通知ルールとして、検出件数の閾値とインターバルの設定が可能です。設定した閾値に達したアラートが発生した場合にリアルタイムでメール通知を行います。 • インターバルは、5分、10分、30分、1時間、2時間、6時間、12時間の何れかを一つ選択します。 • 検出件数の閾値は1~999の範囲で指定します。 • アラート種別は以下のとおりです。 - ウイルス検出(Alert)、ウイルス検出(Block) - スパイウェア検出(Alert)、スパイウェア検出(Block) - 脆弱性防御（IPS/IDS）検出（Alert)、脆弱性防御（IPS/IDS）検出(Block) - FWブロック検出 - URLフィルタ違反(Alert)、URLフィルタ違反(Continue)、URLフィルタ違反(Continue-block)、URLフィルタ違反(Block) • メール通知は最初のアラートが発生した後、お客様が指定したインターバル内で検出件数の閾値を超えた場合に行います。
5	適用	クリックでログレポートオプションのお申込み確認、またはリアルタイムアラート通知の設定変更確認画面が表示されます。
6	確定	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。 ログレポートオプションのお申込みを行った場合は、契約のお申込みが完了すると料金請求が発生します。

1-8-2　ログレポートの確認とリアルタイムアラート通知の設定変更

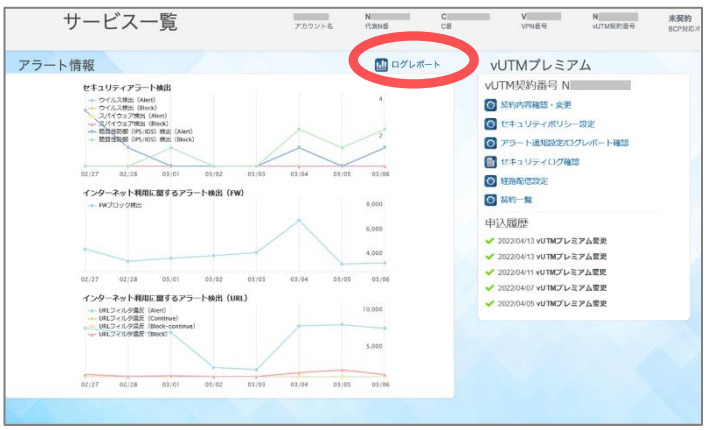
② 月次レポートに出力されるデフォルト設定の内容は以下のとおりです。
お客様にて月次レポート出力内容のカスタマイズも可能です。

月次レポート種類	出力内容（デフォルト設定）
ファイアウォール通信	• 通信回数（全体） • 許可とブロックの比率 • 許可通信量の多いアプリケーション • 許可回数の多いURLカテゴリ • ブロック回数の多いアプリケーション • ブロック回数の多い送信元
セキュリティアラート	• 検知・ブロック回数の多い攻撃・ウイルス名 • 検知・ブロック回数の多い送信元
URLフィルタリング	• ブロック回数の多いURL • ブロック回数の多い送信元

1-8-3　ログレポート画面の起動

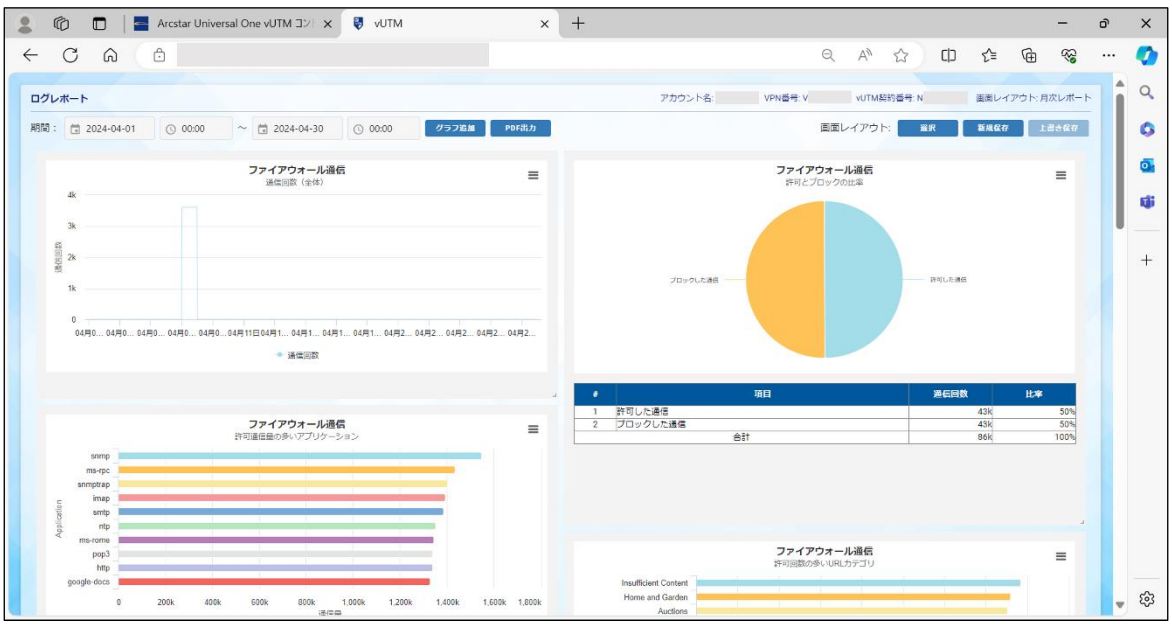
vUTMポータルTOP画面、もしくはアラート通知/ログレポート画面より「ログレポート」ボタンを
クリックすると、別タブでログレポート画面が開きます。
なお、ログレポートオプション未契約の場合は、無料トライアル利用確認のポップアップが表示されます。
ログレポート画面の操作方法については、「1-11　ログレポート画面操作」を参照ください。

<vUTMポータルTOP画面>

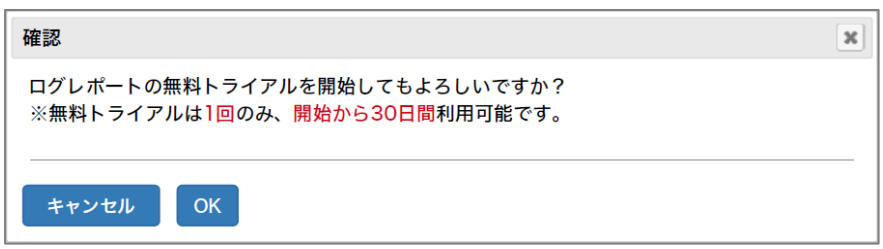


<アラート通知/ログレポート画面>

<ログレポート画面～ログレポートオプション契約中の場合～>

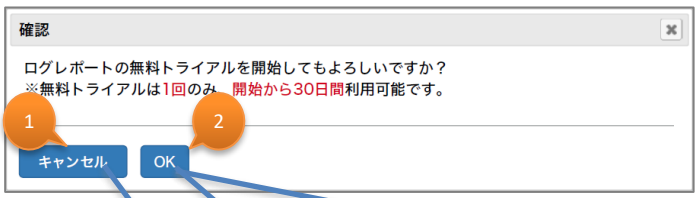


<無料トライアル利用確認のポップアップ～ログレポートオプション未契約の場合～>



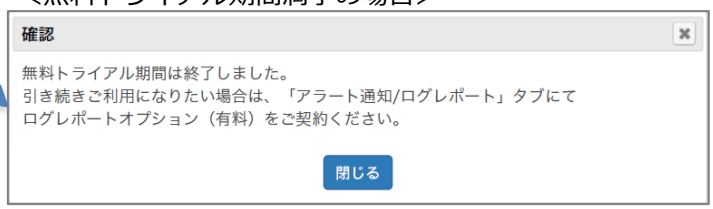
1-8-3　ログレポート画面の起動

ログレポートオプション未契約の場合は、無料トライアル利用確認のポップアップが表示されます。
無料トライアルは1回のみ、利用開始から30日間利用可能です。



＜無料トライアル利用を開始した場合＞

＜無料トライアル期間満了の場合＞

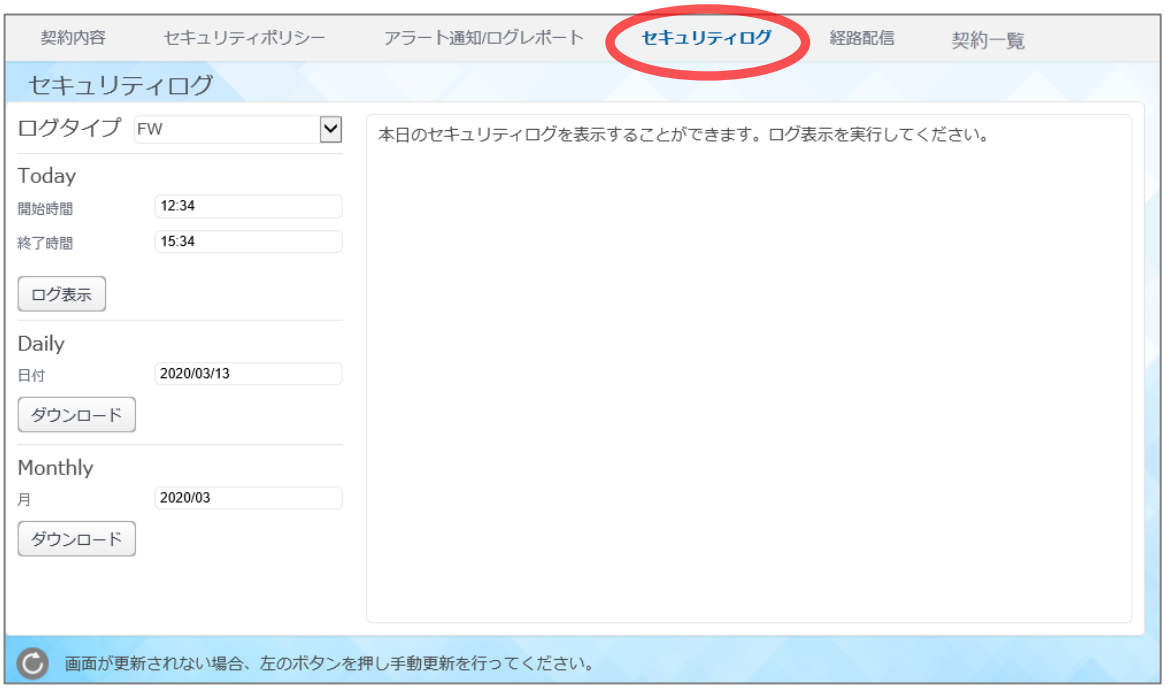


＜無料トライアル利用を開始しない場合＞

	項目	説明
1	キャンセル	ログレポートの無料トライアル利用をキャンセルします。
2	OK	「OK」ボタンをクリックした時点より、ログレポートの無料トライアル利用を開始します。 ※無料トライアル利用済みの場合は、無料トライアル期間満了のポップアップが出ます。
3	無料トライアル期限	ログレポートの無料トライアルの利用期限が表示されます。 例）2019-04-18 11:18まで

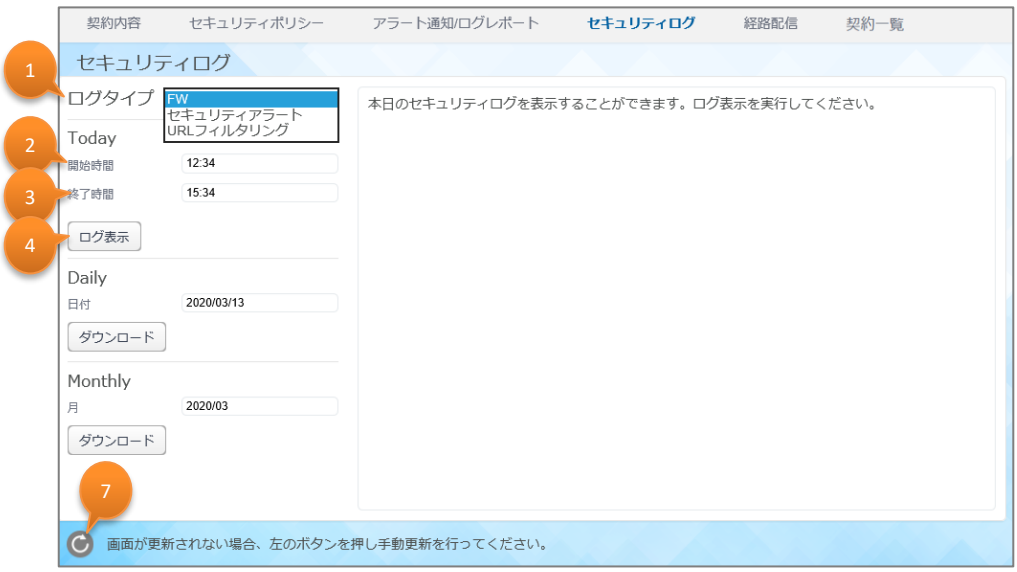
1-9 セキュリティログ確認画面

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。



1-9-1 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。

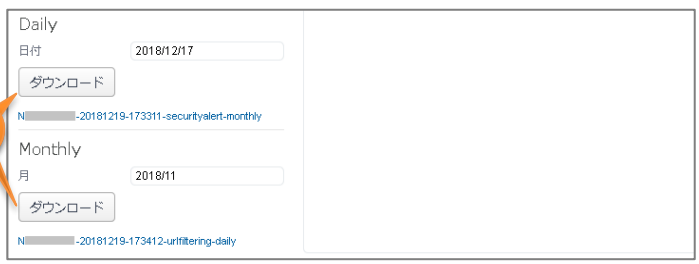


	項目	説明
1	ログタイプ	出力するログの種類をFW/セキュリティアラート/URLフィルタリングの中から選びます。 FWログは、denyおよびallow処理のログが保存されます。 セキュリティアラートログは、Alert、Block処理のログが保存され、URLフィルタリングログでは、Alert、Continue、Block処理のログが保存されます。
2	開始時間	出力するログの絞り込みのために、開始時間を指定します。
3	終了時間	出力するログの絞り込みのために、終了時間を指定します。
4	ログ表示	「ログ表示」ボタンをクリックします。 ログ表示確認画面が表示されますので、「取得」ボタンをクリックします。 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60,000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。

1-9-1 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。

1-9-1 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10GB、期間90日までとなります。10GBまたは90日間を超えた分は破棄されます。
  ※ 10GB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10GB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）および許可（Allow）処理のログが保存されます。
  ※許可（Allow）処理のログを保存する場合、セキュリティポリシー設定で「FW許可ログ設定」をONにする必要があります。
- 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	○	○	○	送信元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

recommend-TtoU-Permit-ANY　推奨設定にて登録されたルール
SecPol_<代表契約N番>_<通番>　追加登録を行ったルール

1-9-1　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,192.168.0.25,210.145.254.162,SecPol_N160084020_001,dns,34797733,40465,53,udp,allow,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,213.211.198.62,192.168.1.25,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,10.70.166.1,118.215.187.173,recommend-TtoU-Permit-ANY,web-browsing,33919505,56560,80,tcp,block-url,"www.ntt.com/index.html",(9999),block-list,informational

1-10 経路配信設定画面

① 本画面にて経路配信OFF/ONの変更、ならびに特定経路配信契約の申込みおよび設定変更が可能です。

1-10-1　経路配信OFF/ONの設定変更

① 経路配信OFF/ON欄にて、経路配信の設定変更ができます。

	項目	説明
1	経路配信OFF/ON	vUTMからお客様VPN網内への経路配信状態の確認および設定変更が可能です。経路配信OFF/ONをクリックして「OFF」と「ON」を切り替えます。 特定経路配信（有料）をご利用中でない場合 • 経路配信「ON」の場合にデフォルトルートを配信します。 • 経路配信「OFF」の場合は経路配信を行いません。vUTM経由でのインターネット接続ができなくなります。（vUTMを経由したビジネスポータルへのアクセスも切断されます） 特定経路配信（有料）をご利用中の場合 • 経路配信「ON」の場合に特定経路配信でお客様が登録した経路を対象として配信します。 • 経路配信「OFF」の場合は経路配信を行いません。vUTM経由でのインターネット接続ができなくなります。
2	適用	クリックで申込み内容確認画面が表示されます。
3	確定	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。 ＊ 設定が反映されるまで10分程度かかります。

※ 設定変更を行う際に数パケットの通信断が発生します。

1-10-2 オプション契約（特定経路配信）の確認・変更および設定変更

① 特定経路配信（有料）欄にて、特定経路配信のお申込みおよび設定変更ができます。

	項目	説明
1	特定経路配信（有料）	• 特定経路配信（有料）をお申込みする場合は「ON」を指定します。 • 特定経路配信（有料）を廃止する場合は「OFF」を指定します。 ＊ 本項目は本オプション契約申込みと廃止を指定する項目となります。OFF/ONを繰り返し申込みすると契約した回数分の課金が発生してしまいますのでご注意ください。 ＊ 特定経路配信の配信経路設定はグローバルIPアドレス指定で最大50経路までの登録となります。お客様が指定した経路のみvUTMからお客様VPN網内へ経路配信を行います。これにより指定した経路のみvUTM経由でインターネット通信を可能とします。 ＊ 本機能を有効化することでDNS等の通信も制御されるため、登録するアドレスには十分にご留意ください。
2	経路指定	ラジオボタンのチェックを入れると、配信経路に登録したグローバルIPアドレスを配信します。 ＊ 配信経路にグローバルIPをひとつも登録していない場合は、配信する経路がないため、vUTM経由でのインターネット接続ができなくなります。
3	デフォルトルート	ラジオボタンのチェックを入れると、デフォルトルート（0.0.0.0/0）を配信します。 ＊ 配信経路にグローバルIPを登録している場合でも、デフォルトルートを配信します。
4	配信経路	グローバルIPアドレスのみ指定可能です。プリフィックス形式（「/32」など）でサブネットマスクを付加して入力します。 ＊ デフォルトルート0.0.0.0/0の登録はできません。 ＊ 配信経路に登録したグローバルIPは、デフォルトルートにチェックを入れた後も情報を保持します。再度、経路指定にチェックを入れた際には保持されたグローバルIPが再利用できます。
5	備考	登録した配信経路の説明などの用途として、任意で10文字まで登録ができます。
6		登録されている配信経路情報を削除します。
7		登録されている配信経路情報を編集します。

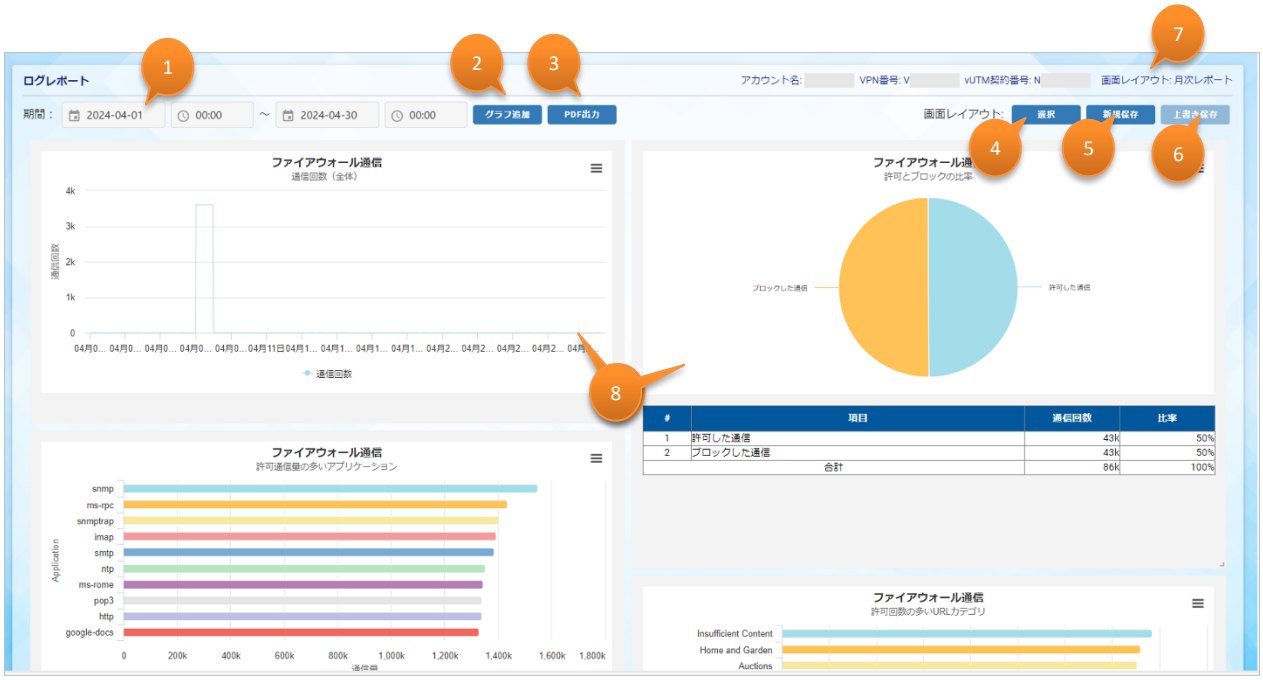
1-10-2　オプション契約（特定経路配信）の確認・変更および設定変更

	項目	説明
8	追加	「追加」ボタンを押下して、配信経路入力欄を追加します。
9	保存	「保存」ボタンを押下して、入力した配信経路情報を保存します。
10	適用	クリックで申込み内容確認画面が表示されます。
11	確定	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。契約のお申込みが完了すると料金請求が発生します。 ＊ 設定が反映されるまで10分程度かかります。

※ 設定変更を行う際に数パケットの通信断が発生します。

1-11 ログレポート画面操作

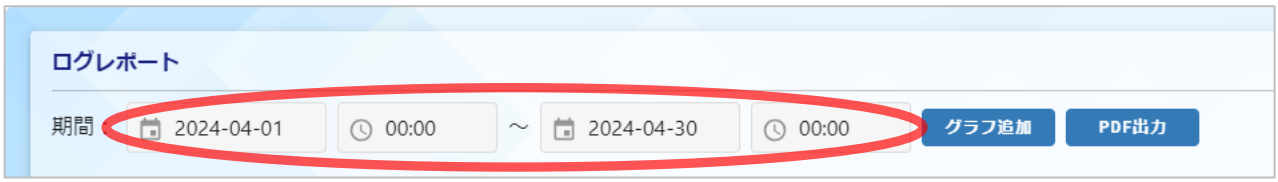
① お客様にて任意にグラフのデータ期間指定、追加、削除、およびドリルダウンが可能です。
また、作成した画面レイアウトの保存、PDFファイル出力が可能です。
ログレポート画面を終了させたい場合は、ブラウザタブの×をクリックして閉じてください。



	項目	説明
1	期間	表示するグラフの開始日時と終了日時を指定します。
2	グラフ追加	ログレポート画面にグラフを追加します。最大40グラフまで追加可能です。
3	PDF出力	表示中の画面をPDFファイルでダウンロードが可能です。 ※Internet ExplorerではPDFダウンロード機能はご利用できません。
4	選択	画面レイアウトの選択画面が開きます。
5	新規保存	表示中の画面レイアウトを新規に保存します。
6	上書き保存	表示中の画面レイアウトを上書き保存します。
7	画面レイアウト	現在選択中の画面レイアウト名を表示します。
8	グラフ	デフォルトで10グラフ表示されます。 表示サイズの変更や配置を入れ替えることが可能です。

1-11-1　期間指定

① グラフデータに表示させる期間を指定します。
期間表示エリアをクリックすると、カレンダーが表示されます。

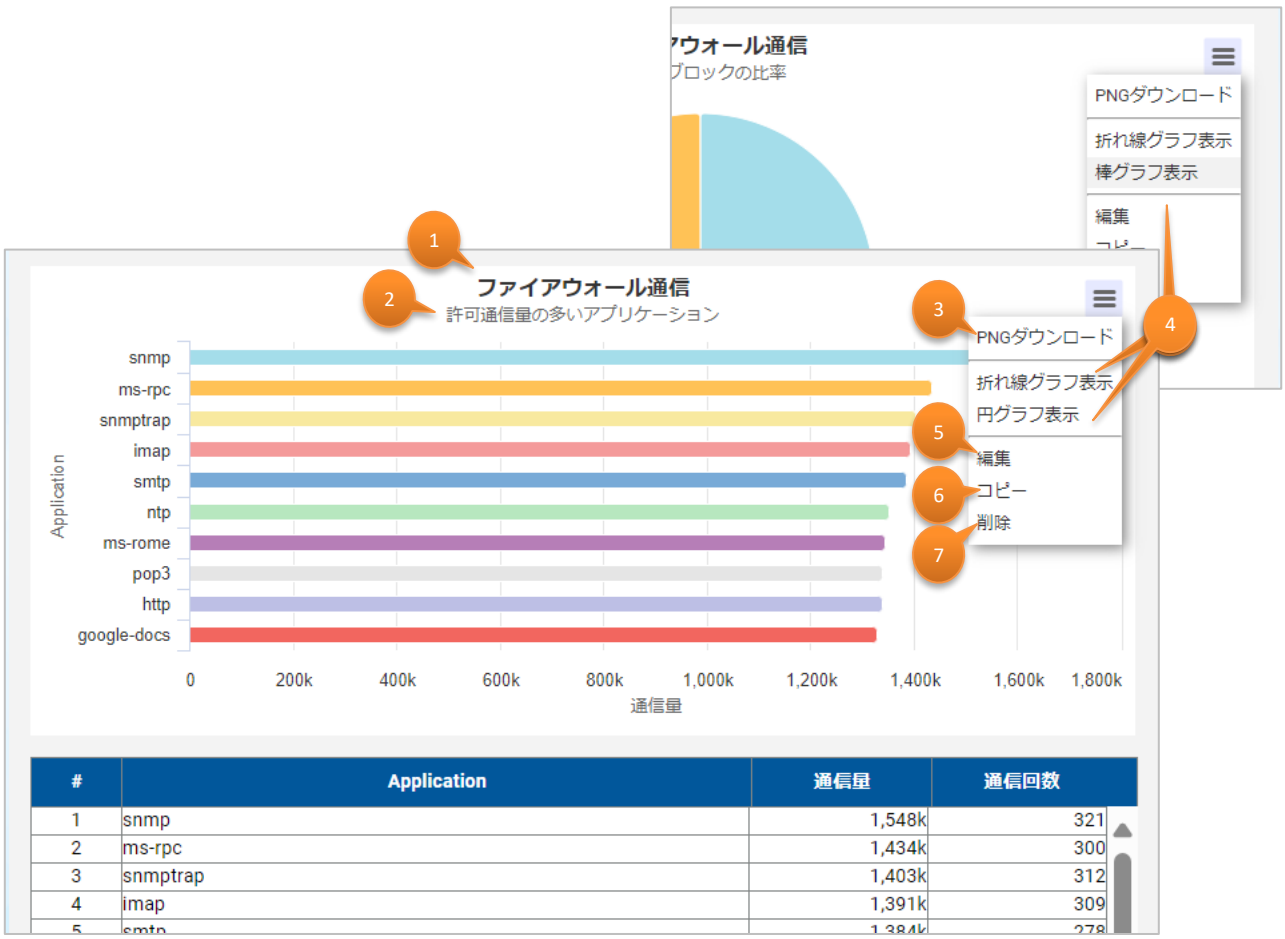


② カレンダーより、グラフデータに表示させる期間を指定します。
指定できる期間は最大で現在日時から過去3ヶ月分です。
※ログレポートオプション契約直後は過去1ヶ月分のデータのみ保持しています。
3ヶ月分のデータが取得できるまでには数日かかることがあります。

	項目	説明
1	開始日	開始日をクリックして指定します。
2	開始時刻	▲▼をクリックして開始時間を指定します。最短5分単位で選択できます。
3	＜ ＞	表示されているカレンダーの月を変更します。
4	終了日	終了日をクリックして指定します。
5	終了時刻	▲▼をクリックして終了時間を指定します。最短5分単位で選択できます。
6	現在時刻	終了時刻を現在日時に指定します。
7	OK	指定した期間でグラフを表示します。

1-11-2 グラフ操作

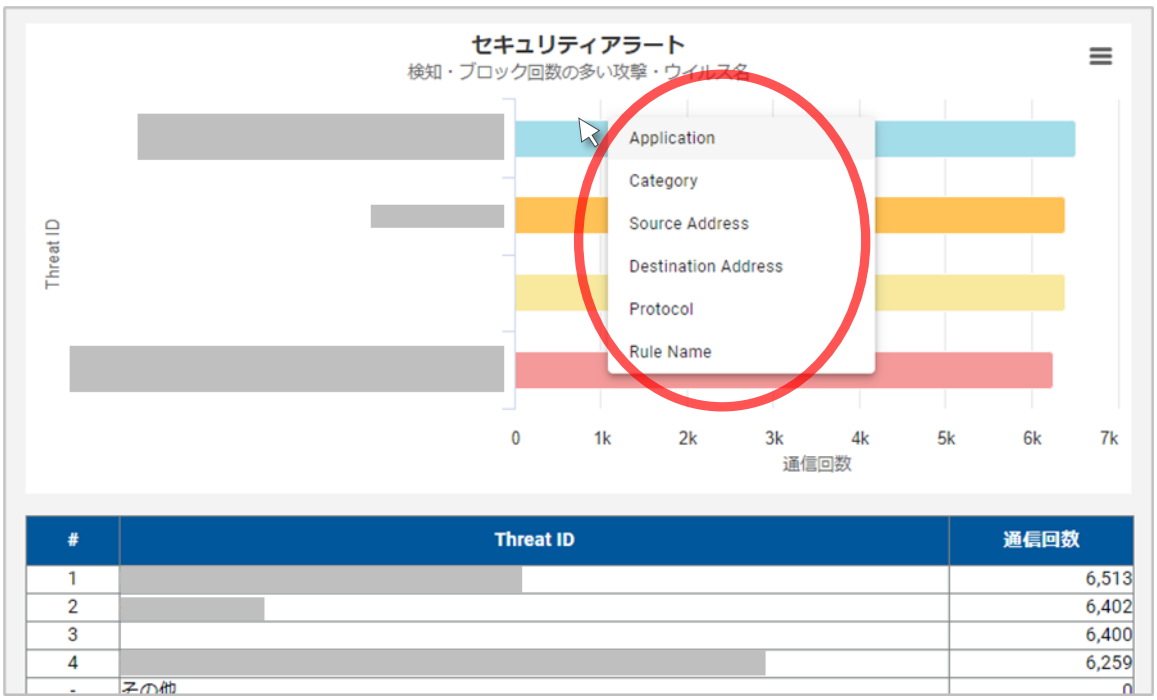
① 各グラフは個別にPNGファイルダウンロード、表示種別変更、編集、コピー、削除が行えます。
グラフ右上の ☰ をクリックして操作します。



	項目	説明
1	タイトル	グラフのタイトルを表示します。
2	グラフの説明	グラフの説明文を表示します。
3	PNGダウンロード	PNG形式のファイルでグラフをダウンロードします。
4	グラフ表示	棒グラフ/折れ線グラフ/円グラフへ表示を変更します。
5	編集	グラフの条件設定画面を開きます。
6	コピー	選択したグラフをコピーします。
7	削除	選択したグラフを削除します。

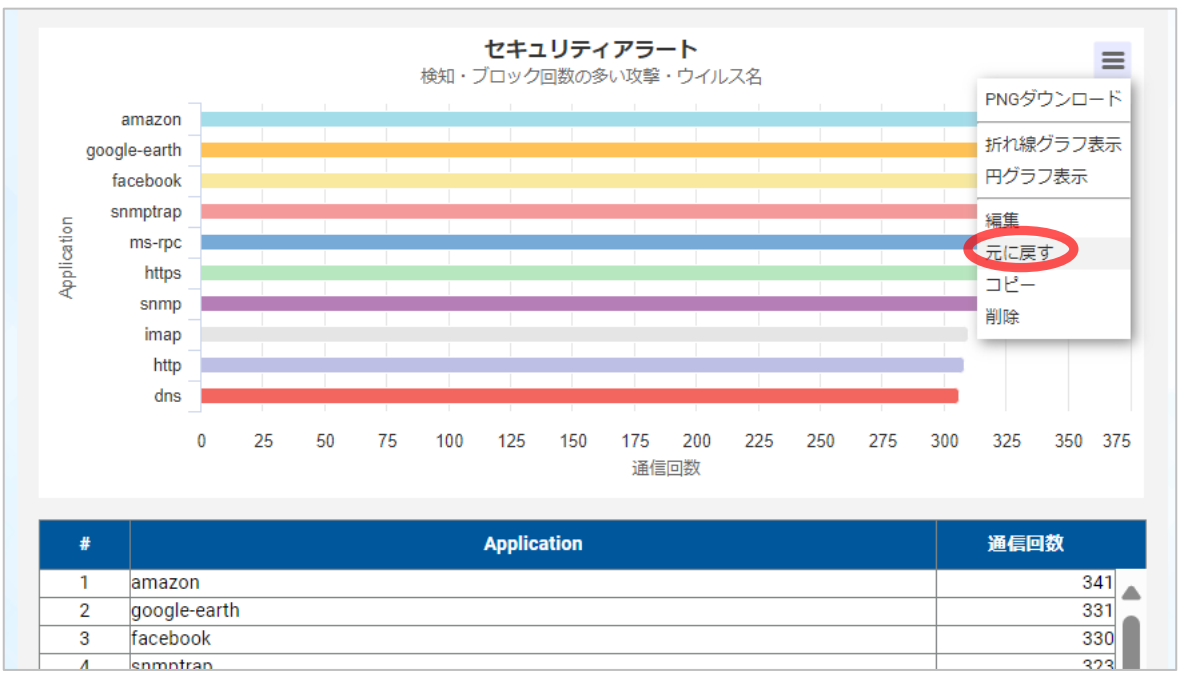
1-11-2 グラフ操作

② 表示されているデータを特定の項目で絞って表示（ドリルダウン）できます。
対象のデータをクリックして、絞りたい項目を選択します。



#	Threat ID	通信回数
1		6,513
2		6,402
3		6,400
4		6,259
-	その他	0

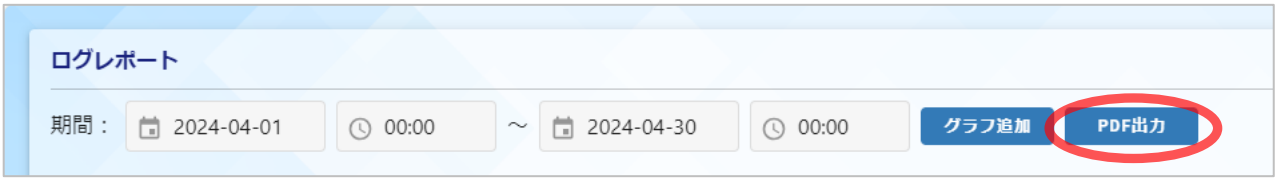
③ 「元に戻す」をクリックすると、絞る前のグラフに戻せます。



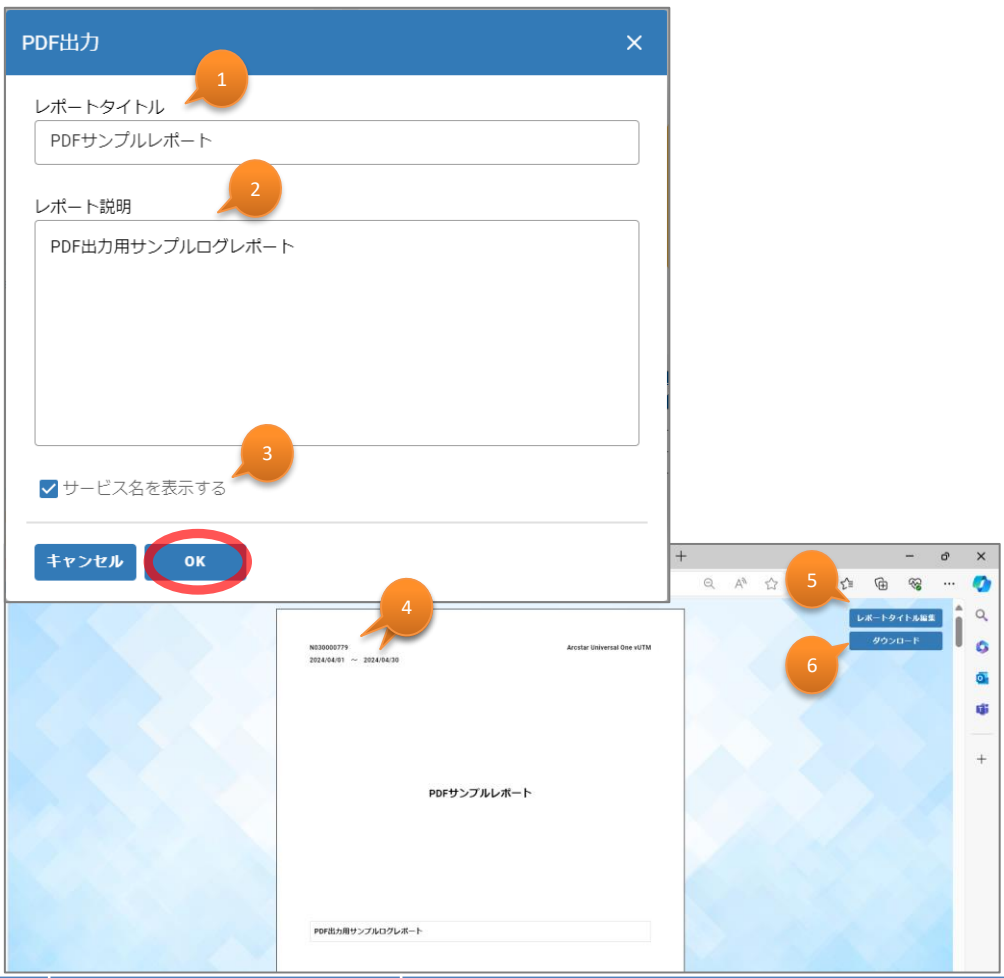
#	Application	通信回数
1	amazon	341
2	google-earth	331
3	facebook	330
4	snmptrap	323

1-11-3　PDF出力

① 表示中の画面をPDFファイルにてダウンロードします。「PDF出力」ボタンをクリックすると、ログレポートの表紙の編集画面が表示されます。PDFファイルには表紙がつき、タイトル等の編集が可能です。※InternetExploreでは本機能はご利用できません。



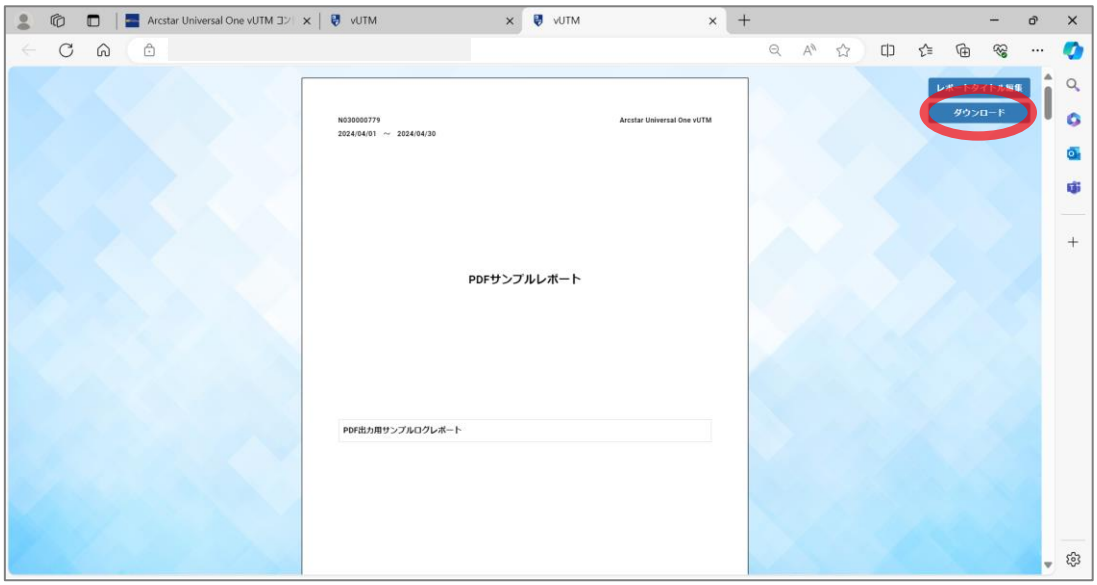
② 「OK」ボタンをクリックすると、別タブでPDFファイルのプレビュー画面が表示されます。



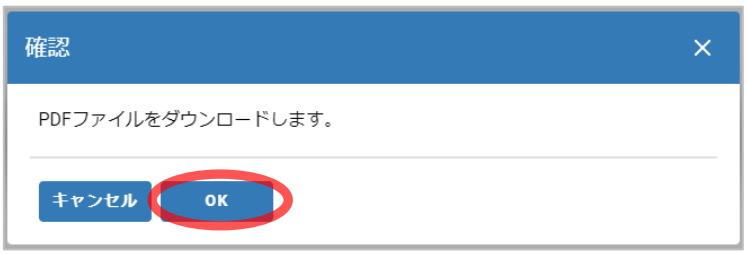
	項目	説明
1	レポートタイトル	表紙のタイトルを入力します。
2	レポート説明	表紙の下に載せる説明文を入力します。最大400文字まで入力可能です。
3	サービス名を表示する	表紙に「Arcstar Universal One vUTM」を表示します。 デフォルト設定ではチェックが入っています。
4	vUTM契約番号、期間	vUTM契約番号と指定した期間が表示されます。削除できません。
5	レポートタイトル編集	PDFの表紙の編集画面を開きます。
6	ダウンロード	PDFファイルをダウンロードします。

1-11-3　PDF出力

③　「ダウンロード」ボタンをクリックすると、PDFダウンロードの確認画面が表示されます。



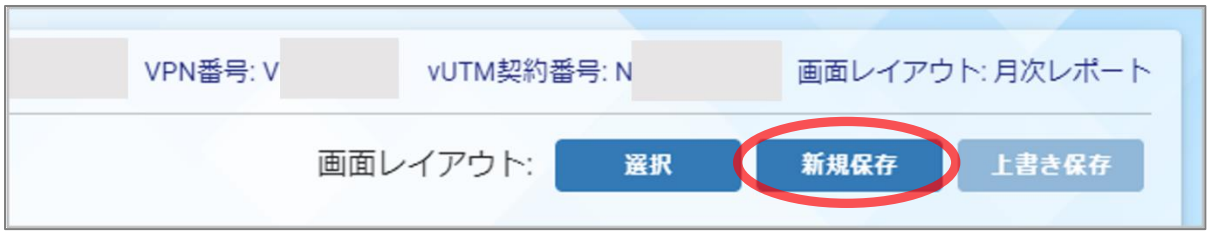
④　「OK」ボタンをクリックすると、PDFダウンロードを開始します。



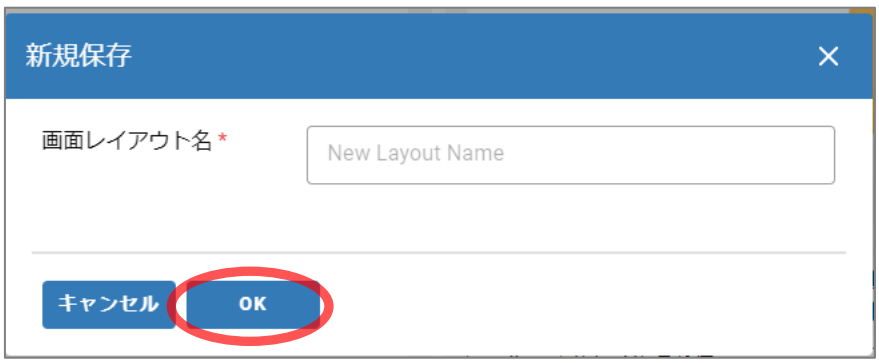
ダウンロードしたファイルは「vUTMログレポートNxxxxxxxx_yyyymmddHHMM.pdf*」のファイル名で保存されます。
* “Nxxxxxxxx”はvUTM契約番号、“yyyymmddHHMM”はダウンロードした日時が反映されます。

1-11-4　画面レイアウトの保存

① 表示中のログレポート画面のレイアウトを名前を付けて保存することができます。
「新規保存」ボタンをクリックすると、新規保存画面が表示されます。



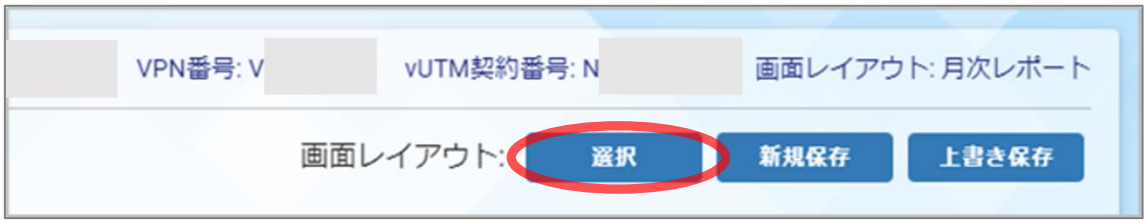
② レイアウト名を入力して「OK」ボタンをクリックします。
※最大20文字まで
※レイアウト保存件数は最大9個まで（デフォルトで登録されているレイアウトは除く）



③ 「上書き保存」ボタンをクリックすると、表示中の画面レイアウトに上書き保存されます。

1-11-4　画面レイアウトの保存

④ 保存されている画面レイアウトを選択し、表示します。また、月次レポート（自動生成）用の画面レイアウトを設定します。
「選択」ボタンをクリックすると、画面レイアウトの選択リストが表示されます。



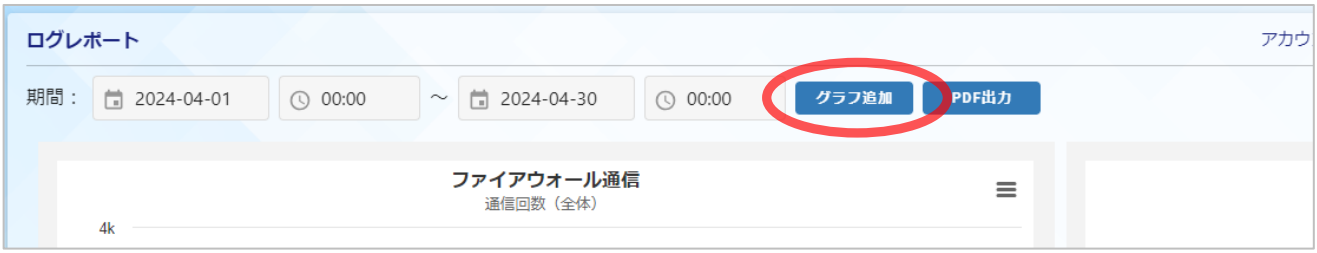
⑤ 表示させたい画面レイアウトの「選択」ボタンをクリックすると、ログレポート画面に反映されます。

⑥ 選択した画面レイアウト名がログレポート画面右上に表示されます。

	項目	説明
1	画面レイアウト	表示中のログレポート画面のレイアウトを名前を付けて保存することができます。 デフォルトで「月次レポート」が登録されています。本項目は上書き保存や削除はできません。
2	月次レポート（自動生成）	月次レポート（自動生成）は、vUTMポータル「アラート通知/ログレポート」タブの「ダウンロード」ボタンから出力できます。 設定中：対象の画面レイアウトを月次レポート（自動生成）に設定しています。 設定：「設定」ボタンをクリックすると、対象の画面レイアウトを月次レポート（自動生成）に設定します。
3	選択	表示させたい画面レイアウトを選択します。
4	削除	対象の画面レイアウトを削除します。

1-11-5　ログレポートのカスタマイズ

① ログレポート画面にグラフを追加します。
「グラフ追加」ボタンをクリックすると、条件設定画面が表示されます。



② プリセットより選択、または詳細設定で個別に条件が指定できます。

	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	プリセット	あらかじめ用意されているグラフ種別を選択して設定できます。
3	タイトル	グラフのタイトルを入力します。 ログタイプを選択すると自動で入力されます。手入力も可能です。
4	グラフの説明	グラフの説明文を入力します。 プリセットを選ぶと自動で入力されます。手入力も可能です。
5	詳細設定	詳細設定画面が開きます。
6	OK	指定した内容でグラフを追加します。

1-11-5　ログレポートのカスタマイズ

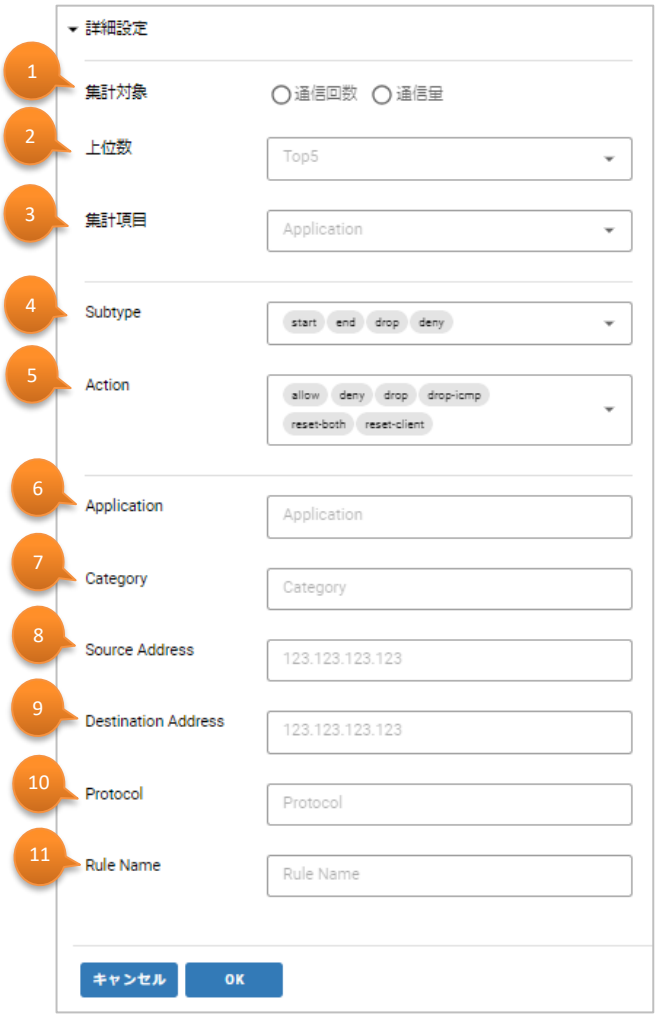
③　プリセット内容は以下の通りです。

ログ種別	プリセット内容
ファイアウォール通信	• 通信回数（全体） • 許可とブロックの比率 • 通信回数の多い送信元 • 通信回数の多い送信先 • 通信回数の多いプロトコル • 適用回数の多いルール名 • 通信回数の多いアプリケーション • 通信回数の多いアプリケーションと送信元数 • 許可適用回数の多いルール名 • 許可回数の多いアプリケーション • 許可通信量の多いアプリケーション • ブロック回数の多い送信元 • ブロック回数の多い送信先 • ブロック回数の多いプロトコル • ブロック適用回数の多いルール名 • ブロック回数の多いアプリケーション • 許可回数の多いURLカテゴリ
セキュリティアラート	• 検知回数の多い攻撃名 • 検知回数の多い送信元 • 検知回数の多い送信先 • 検知回数の多いルール名 • ブロック回数の多い攻撃名 • ブロック回数の多い送信元 • ブロック回数の多い送信先 • ブロック回数の多いルール名 • ウイルス検知回数の多いウイルス名 • ウイルス検知回数の多い送信元 • ウイルス検知回数の多い送信先 • ウイルス検知回数の多いルール名 • ウイルスブロック回数の多いウイルス名 • ウイルスブロック回数の多い送信元 • ウイルスブロック回数の多い送信先 • ウイルスブロック回数の多いルール名 • 検知・ブロック回数の多い攻撃・ウイルス名 • 検知・ブロック回数の多い送信元
URLフィルタリング	• ブロック回数の多いURL • ブロック回数の多いカテゴリ • ブロック回数の多いルール名 • ブロック回数の多い送信元

1-11-5　ログレポートのカスタマイズ

④　詳細設定の内容は、選択したログタイプによって変わります。

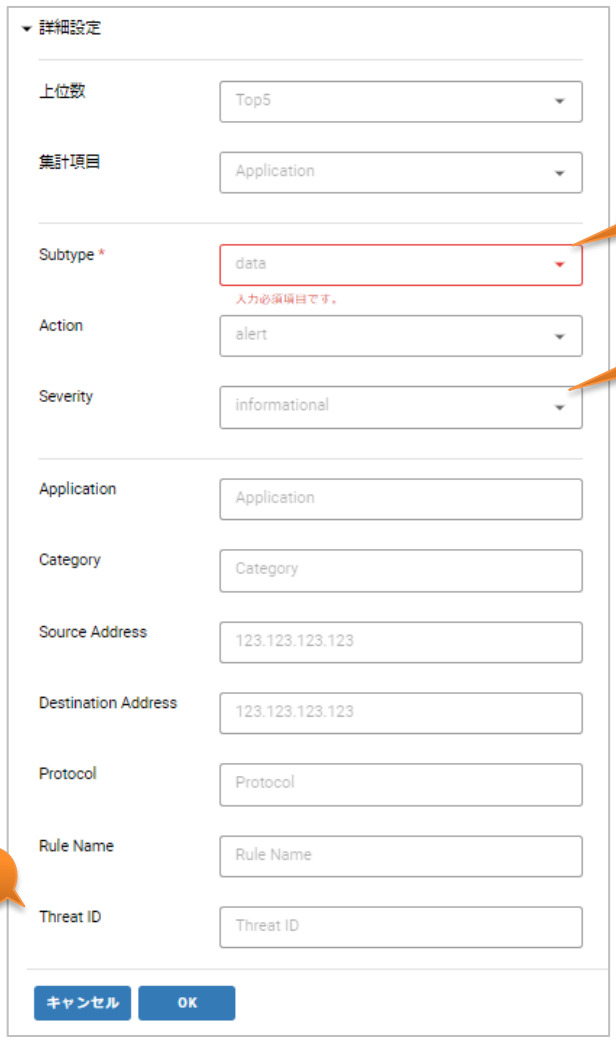
<ログタイプでFWを選択した場合>



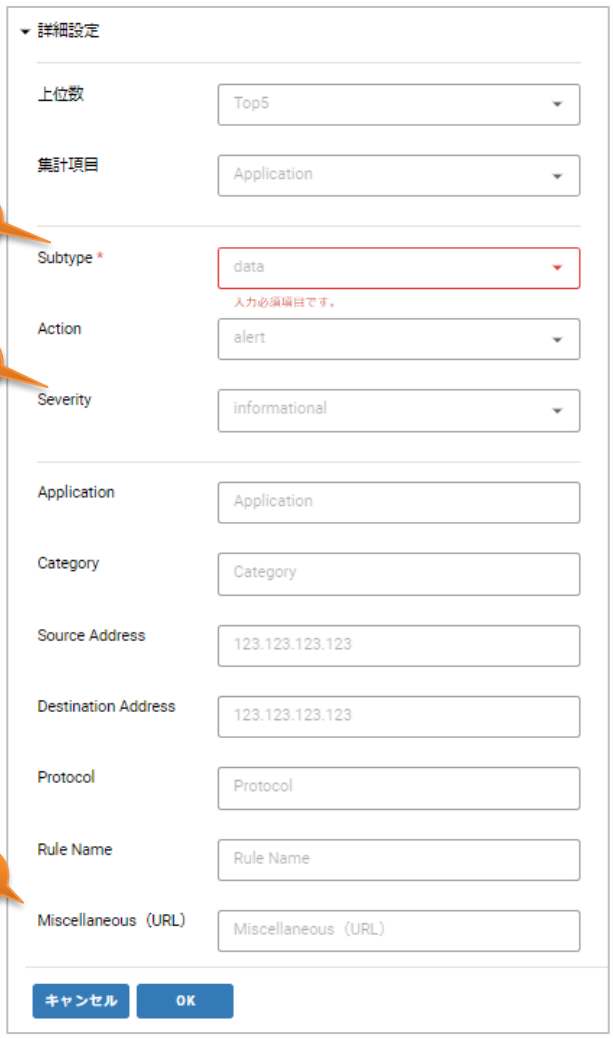
	項目	説明
1	集計対象	通信回数もしくは通信量のどちらかを選択します。※FW選択時のみ表示されます。
2	上位数	グラフに表示させるデータの数を選択します。Top5、Top10、Top30、Top50、Top100から選択できます。
3	集計項目1	集計する項目を指定します。
4	Subtype	選択した値をログのSubtype列から抽出します。複数選択可能です。
5	Action	選択した値をログのAction列から抽出します。複数選択可能です。
6	Application	入力した値をログのApplication列から抽出します。
7	Category	入力した値をログのCategory列から抽出します。
8	Source Address	入力した値をログのSource Address列から抽出します。
9	Destination Address	入力した値をログのDestination Address列から抽出します。
10	Protocol	入力した値をログのProtocol列から抽出します。
11	Rule Name	入力した値をログのRule Name列から抽出します。

1-11-5　ログレポートのカスタマイズ

<ログタイプでセキュリティアラートを選択した場合>



<ログタイプでURLフィルタリングを選択した場合>



	項目	説明
1	Subtype	選択した値をログのSubtype列から抽出します。 入力必須項目のため、未選択時は赤枠になります。
2	Severity	選択した値をログのSeverity列から抽出します。複数選択可能です。 ※セキュリティアラート、URLフィルタリング選択時のみ表示されます。
3	Threat ID	入力した値をログのThreat ID列から抽出します。 ※セキュリティアラート選択時のみ表示されます。
4	Miscellaneous（URL）	入力した値をログのMiscellaneous列から抽出します。 ※URLフィルタリング選択時のみ表示されます。

1-12 契約一覧画面

① 本画面にて同一VPN番号で契約しているvUTMの一覧が閲覧可能です。 vUTMの契約が１つの場合は契約追加が表示されます。

② 追加でvUTMを契約すると契約一覧に追加したvUTMの契約情報が表示されます。

1-12-1 vUTMの追加申し込み

① 契約一覧にて契約情報を確認することができます。また契約追加ではvUTMの追加申し込みができます。

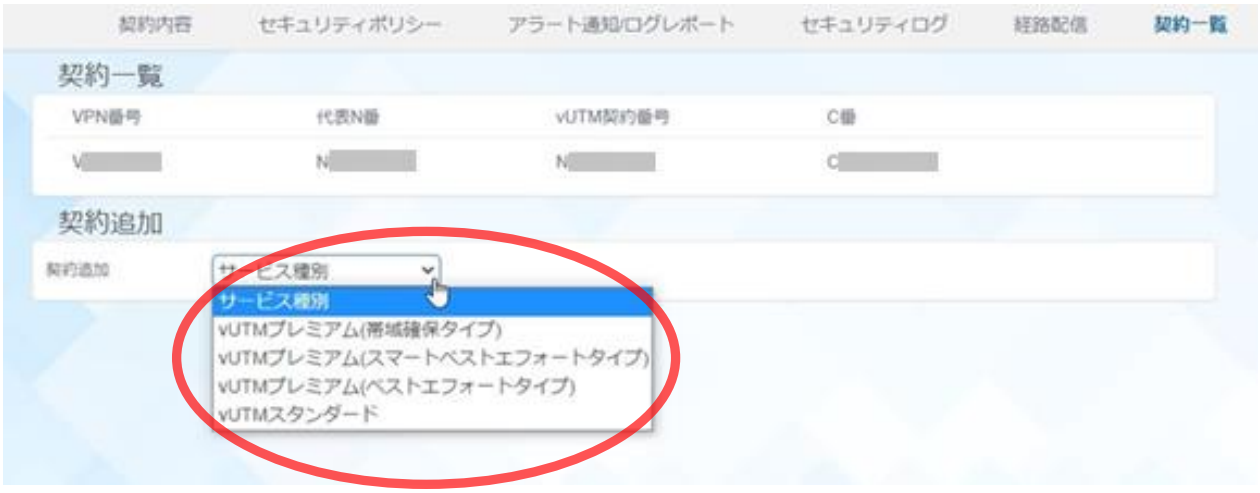
	項目	説明
1	契約一覧	• 契約中のVPN番号、代表N番、vUTM契約番号、C番が表示されます。

2	契約追加	• サービスの追加申し込みができます。同一VPN番号でvUTMを2つ契約している場合この項目は表示されません。
		• 追加できるサービスは以下の通りです。
		  • vUTMプレミアム（帯域確保タイプ）
		  • vUTMプレミアム（スマートベストエフォートタイプ）
		  • vUTMプレミアム（ベストエフォートタイプ）
		  • vUTMスタンダード

3	表示	• 別のvUTMポータルが表示されます。

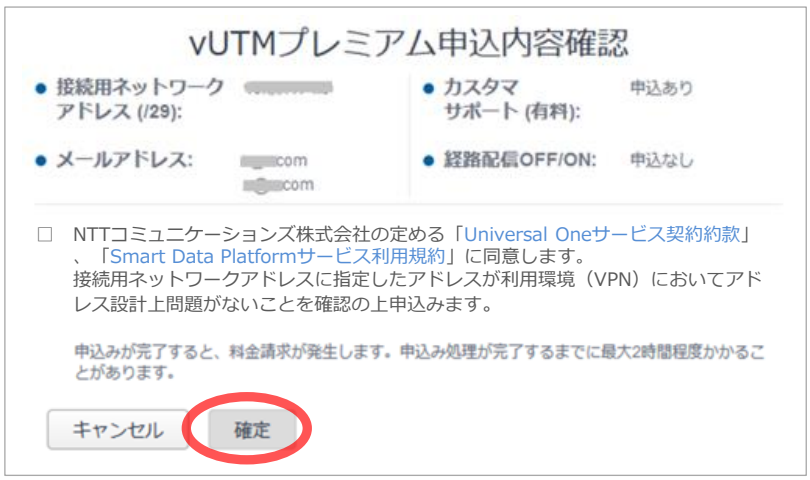
1-12-1 vUTMの追加申し込み

② 本サービスを申し込む場合、契約追加にあるドロップダウンリストから追加するサービス種別を選択します。
※本申込み可能時間は、平日9時30分～17時30分となります。



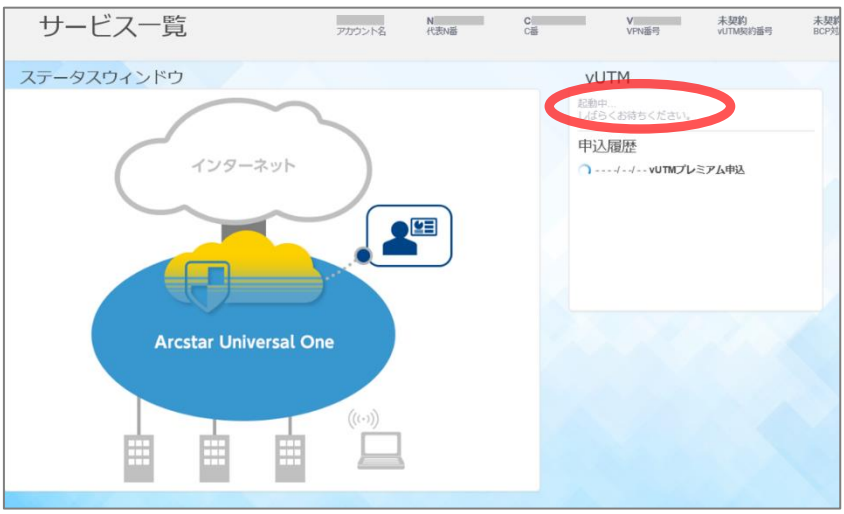
③ サービスを選択すると申込画面が表示されます。各設定項目を入力し、経路配信のボタンクリックし「OFF」にした状態で「確認」ボタンをクリックします。
※各設定項目の詳細はP8「1-2 vUTMの起動」をご覧ください。

④ 申込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。お申込みが完了すると料金請求が発生します。

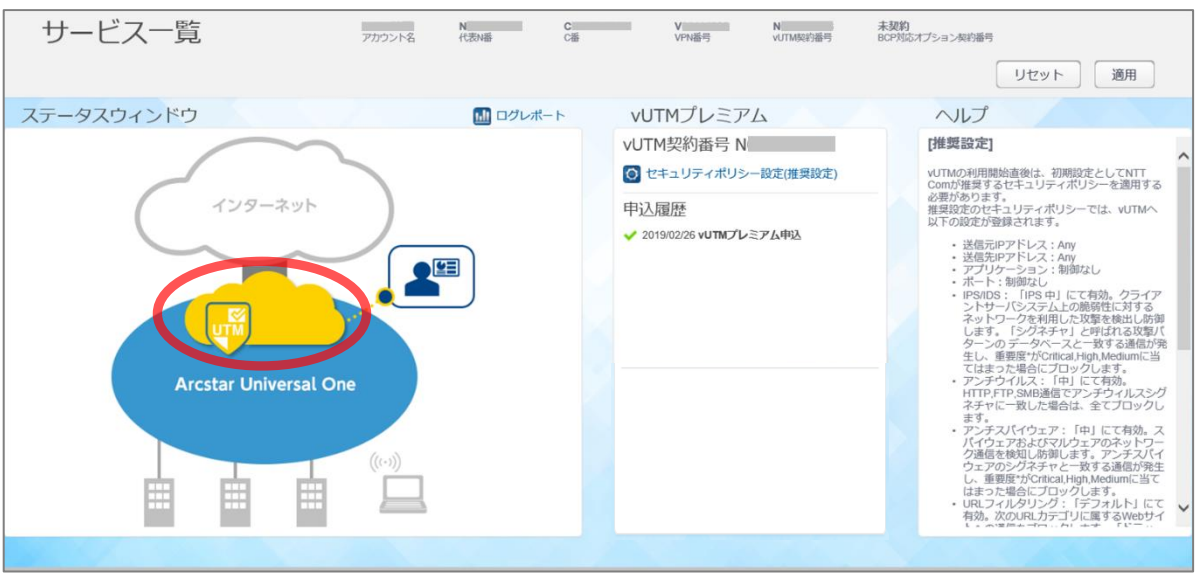


1-12-1 vUTMの追加申し込み

⑤ 新しいvUTMポータルへ自動遷移し「起動中…　しばらくお待ちください。」が表示されます。
起動完了までに最大2時間程度かかる場合があります。



⑥ サービスが起動されると、ステータスウィンドウが各サービスのvUTMアイコンに変わり、vUTM契約番号が表示されます。
※経路配信OFFとして起動しているためデフォルトルートが配信されずインターネット通信はできない状態となります。



※追加のvUTMにてオプション契約（カスタマサポート、特定経路配信、ログレポート、BCP対応オプション）をご利用されたい場合、お客様にてオプション契約の申し込みをする必要があります。申し込み方法についてはP16以降にあります「オプション契約（カスタマサポート）の確認・変更」をご覧ください。

1-12-2 経路配信の変更

① 経路配信画面にて経路配信OFF/ONのボタンをクリックし、経路配信の設定変更を行います
※ 経路配信の設定方法についてはP45「1-10-1　経路配信OFF/ONの設定変更」をご覧ください。
※ vUTM経由でビジネスポータルにアクセスしている場合、経路配信が「OFF」の際にビジネスポータルへのアクセスも切断されます。

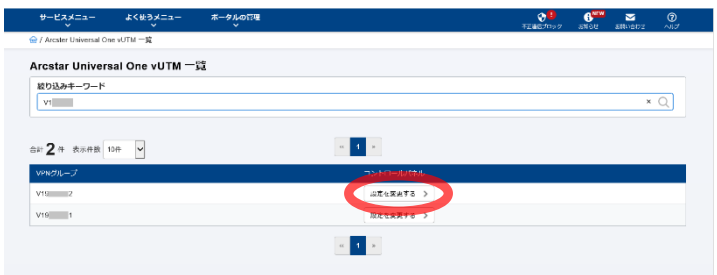
② vUTMを2つご利用する場合、片方のvUTMにて特定経路配信の設定変更をする必要があります。
※特定経路配信の設定方法についてはP46「1-10-2　オプション契約（特定経路配信）の確認・変更および設定変更」をご覧ください。

1-12-3 vUTMの追加申し込み後のログインおよび管理画面への遷移

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「Arcstar Universal One」-「vUTM」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。

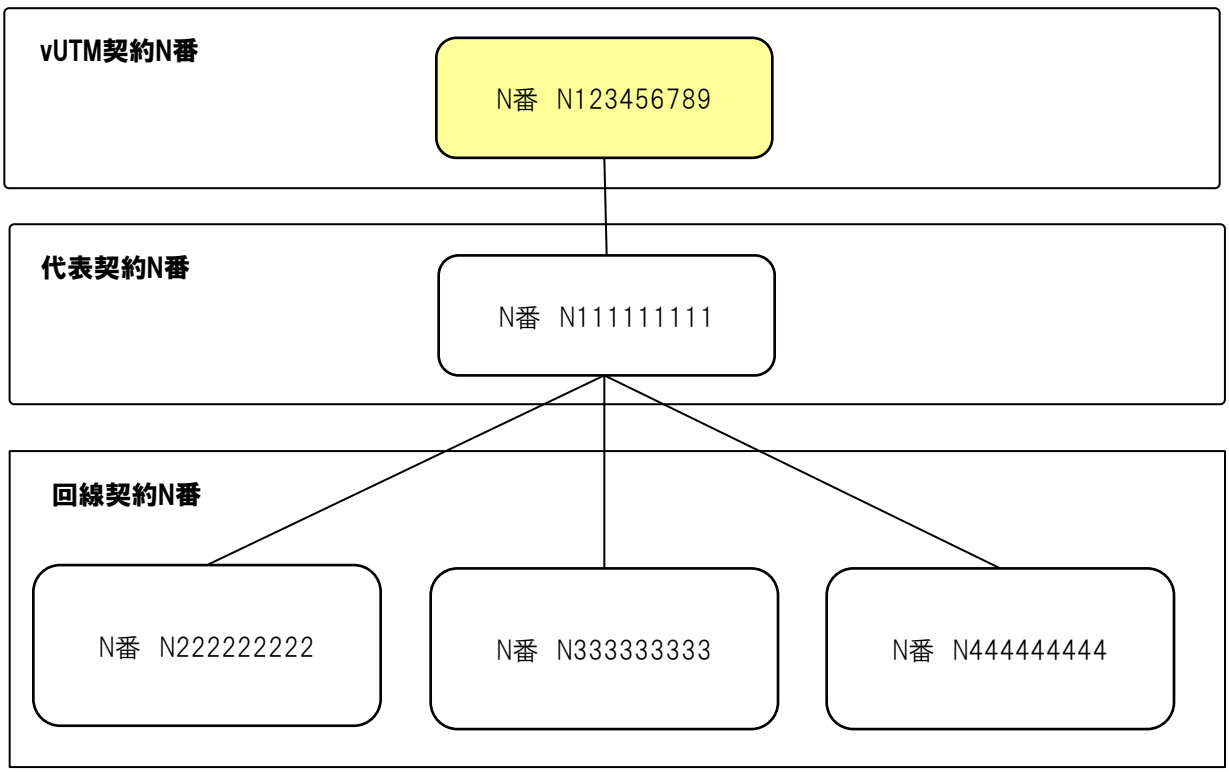
④ 表示させたいvUTM契約情報にカーソルを移動させ、右側の「表示」ボタンをクリックします。

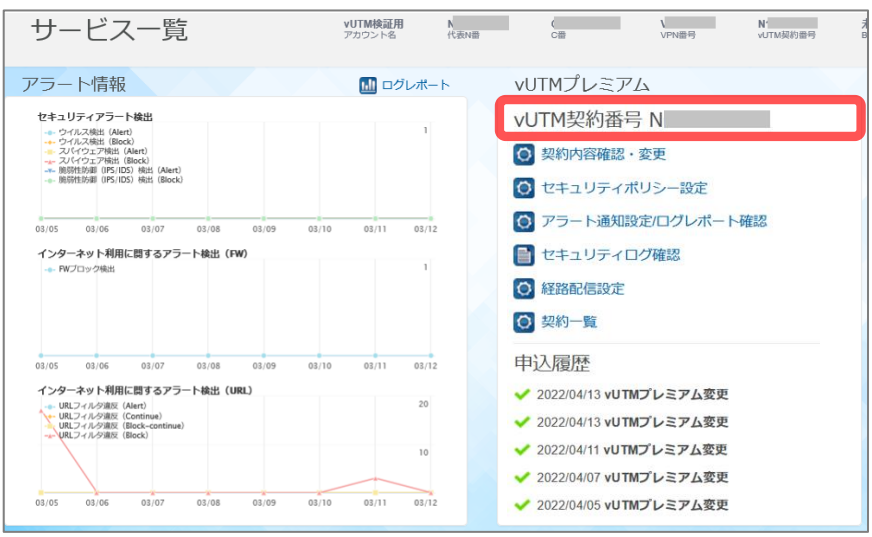
1-12-3 vUTMの追加申し込み後のログインおよび管理画面への遷移

⑤ vUTMの管理トップ画面が表示されます。こちらの画面からvUTMにかかわる各種情報参照及び管理機能がご利用できます。

2. お客様番号について

以下のとおり、ご契約お客様番号として、Nから始まるArcstar Universal One インターネット接続機能（vUTMプレミアム ベストエフォートタイプ）またはArcstar Universal One インターネット接続機能（vUTMプレミアム スマートベストエフォートタイプ）のN番号（以下N番）があります。
vUTM起動後にカスタマポータル上にてご確認いただけます。





お問い合わせのとき

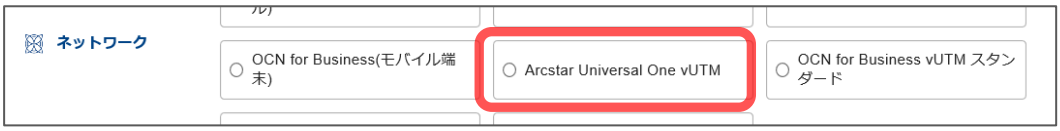
ビジネスポータルからチケットを起票するさいに、vUTM契約番号（N番）をお知らせください。

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「Arcstar Universal One vUTM」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（インターネット接続不可）
→インターネット接続ができないお客様はこちらを選択してください。
故障（ポータル上でエラー表示）
→ポータル上でエラーが発生しているお客様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契約が無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込み方法は、
「1-4-2　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。弊社営業担当までご連絡ください。
マネージド・ログレポート/有料
→マネージドベーシック、マネージドプロ、ログレポート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、ログレポート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「ネットワークサービス」の「Arcstar Universal One」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、Universal Oneサービスをご参照ください。）
「お客様サポートサイト」 工事情報・故障情報 URL： http://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、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Universal One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

• インターネット接続機能（vUTMプレミアム ベストエフォートタイプ）およびインターネット接続機能（vUTMプレミアム スマートベストエフォートタイプ）は、VPN通信とインターネット通信のトラフィックを重畳しているため、トラフィックが相互に影響する場合があります。

• インターネット接続機能（vUTMプレミアム ベストエフォートタイプ）およびインターネット接続機能（vUTMプレミアム スマートベストエフォートタイプ）は、インターネット発でVPNへ接続を開始する通信をすべて遮断します。その為、本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10Mbps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。なお10Mbpsは目安であり、その値に満たない場合もあります。

• 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プレミアム申込み可能時間は以下のとおり。
  - 新設および廃止　：　平日9時30分～17時30分
  - 設定変更　：　時間制限なし

  ※但し、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」-「Arcstar Universal One」-「日本国内」を選択してください。

• 1 G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

• 同一VPN番号で2つのvUTMを同時に利用しデフォルトルートを利用する場合、どちらか一方のみデフォルトルートにしてください。