KDDI クラウドプラットフォームサービス
拡張ファイアウォール

Customer Control System 操作マニュアル

Version　　01.08
最終更新日　　2020/03/05

改版履歴

年月日	バージョン	項番	内容	作成者/変更者
2013/11/11	01.00		初版作成	KDDI
2013/11/27	01.01	2.7	ログ情報および保存期間について訂正	KDDI
		2.3	誤記訂正	KDDI
2014/02/12	01.02	2.3.1	使用できないポリシー名の訂正	KDDI
2017/03/16	01.03	1.2	ブラウザ要件の変更	KDDI
		2.3.1	「ポリシーの設定」説明文の変更	KDDI
		2.4.2	機能変更（アドレスグループ追加・編集画面にてアドレスグループが追加できない）に伴う変更	KDDI
		2.4.3	機能変更（アプリケーショングループ追加・編集画面にて「グループを設定する」リンクの削除）に伴う変更	KDDI
		2.7 2.10	画面の「注意」文言変更に伴う画像の差替え	KDDI
2017/12/08	01.04		P3 問い合わせ先の変更、バージョンアップに伴う内容確認	KDDI
2018/05/17	01.05	1.2 2.3.1 2.4	動作環境の制限事項に関して、KCPS1/2での制限値を記載 「ポリシーの設定」欄の通信元アドレス、通信先アドレスに注意文言を追記 2.4.1「アドレスの設定」、2.4.2「新しいアドレスグループ」欄のオブジェクト名の入力可能文字数を 3～31 文字に修正 2.4.1「アドレスの設定」欄の IP アドレスに注意文言を追記	KDDI
2018/07/11	01.06	2.9	パスワード変更機能 パスワードの文字数が 15 文字となっている個所を 8 文字以上、14 文字以内と修正	KDDI
2018/07/26	01.07	2.8.6	攻撃トラフィック リスクの表記を数字表記(1,2,3,4,5)から文字(informational, low, medium, high, critical)に変更	KDDI
2020/03/05	01.08	1.2	ブラウザ要件の変更	KDDI

問合せ先

≪操作方法≫

担当 SE にお問い合わせください。

≪KDDI クラウドプラットフォームサービスの故障・お問い合わせ窓口≫

KDDI クラウド運用担当　０１２０－９９－３６９６（無料）

目次

0 前提条件 5
0.1 本書の解説範囲 5
0.2 注意事項 5
1 カスコンシステム概要 6
1.1 機能概要 6
1.2 動作環境について 6
2 操作説明 7
2.1 ログイン 7
2.2 メイン画面 8
2.3 ポリシー設定 9
2.3.1 ポリシーの定義 9
2.4 オブジェクト設定 14
2.4.1 アドレスの定義 14
2.4.2 アドレスグループの定義 16
2.4.3 アプリケーショングループの定義 18
2.4.4 アプリケーションフィルターの定義 20
2.4.5 サービスの定義 22
2.5 コミット 24
2.6 ロールバック 27
2.7 ログモニタリング 29
2.7.1 ファイアウォールログ 29
2.7.2 IPS/IDS ログ 30
2.7.3 Web ウィルスチェックログ 33
2.7.4 スパイウェアチェックログ 35
2.8 レポート 37
2.8.1 アプリケーション（期間指定） 38
2.8.2 アプリケーション（日単位） 39
2.8.3 通信元アドレス 40
2.8.4 通信先アドレス 41
2.8.5 通信先トラフィック（国毎） 42
2.8.6 攻撃トラフィック 43
2.9 パスワード変更機能 44
2.10 コンフィグダウンロード機能 45

0　前提条件

0.1 本書の解説範囲

このマニュアルは、Customer Control System の操作方法について説明します。
このマニュアルの対象読者は、ファイアウォールの導入、運用、保守を担当するシステム管理者です。

0.2 注意事項

本書は著作権法により著作権等の権利が保護されています。
本書のすべてまたは一部を無断で複写・複製・転載・転用されますと、著作権等の権利侵害となる場合がありますのでご注意ください。
また、本書はあくまでも参考資料であり、掲載されている情報は予告なしに変更されることがあります。
本書を用いることにより発生したいかなる損害も弊社は補償することはできません。

1 カスコンシステム概要

1.1 機能概要

Customer Control System は、ファイアウォール機能の設定及びモニタリングを Web ブラウザベースで行えるシステムです。

1.2 動作環境について

- ブラウザ要件

  Customer Control System の対応ブラウザは KDDI クラウドプラットフォームサービス ナレッジサイトの対応ブラウザを参照ください。

- 制限事項

  Customer Control System にて設定可能なファイアウォール情報の上限値は以下の通りです。

説明	上限値	
	KCPS ver1	KCPS ver2
ポリシー登録数	199	199
アドレスオブジェクト登録数	200	200
アドレスグループオブジェクト登録数	20	20
１つのアドレスグループへ登録可能なメンバ数	200	200
アプリケーショングループオブジェクト登録数	100	100
１つのアプリケーショングループへ登録可能なメンバ数	200	200
アプリケーションフィルタオブジェクト登録数	100	100
サービスオブジェクト登録数	10	30

- 注意事項
  - ブラウザ機能の「戻る」「更新」機能には対応していません。これらの機能を利用した場合、設定途中の内容が失われる場合があります。
  - システム利用終了時は必ずログオフ処理を実施して下さい。ログオフをせずにブラウザを終了させた場合、一定時間再ログインができなくなります。

2　操作説明

2.1　ログイン

ファイアウォール設定を行う最初のステップでは、Web ブラウザにて Customer Control System にログインします。アクセス URL およびログイン ID,パスワード,ファイアウォール ID については、開通通知書を確認ください。

(1) InternetExplorer ブラウザを起動し、Customer Control System ログインページへアクセスします。

アクセス URL:<https:// 【サイト情報】/mng/customer/login/loginSCR.do>

※URL 情報は拡張 Firewall 開通情報にてご案内させて頂きます。URL の【サイト情報】部分は利用サイト毎に異なります。

(2) ［ログイン ID］と［パスワード］および［ファイアウォール ID］の全てを入力し［ログイン］をクリックすると［メイン］ページが開きます。

✧ 初回ログイン時はパスワード変更ページが開きます。新旧パスワードを入力し、OK ボタンをクリックすると、パスワード変更結果のメッセージを表示後に[メイン]ページが開きます。

※注意：

- ✧　３０分間内に１０回ログインに失敗した場合不正ログインとみなし、以降３０分間ログインができない状態となります。
- ✧　ログイン後一定時間（３０分間）無操作の場合、自動的にログイン状態を解除します。
- ✧　システム利用終了時は必ずログオフ処理を実施して下さい。ログオフをせずにブラウザを終了させた場合、一定時間（最大３０分間）再ログインができなくなります。

2.2　メイン画面

［メイン］ページには、管理メニュー、お知らせメッセージ、マニュアルダウンロードが表示されます。

Customer Control System を終了する際は、［ログアウト］ボタンにより終了することができます。

2.3　ポリシー設定

2.3.1　ポリシーの定義

ポリシーは、トラフィックの属性（通信元ゾーン、通信先ゾーン、通信元アドレス、通信先アドレス、アプリケーションおよびサービス（HTTP など））に基づいて新しいネットワークセッションの許可または拒否（ブロック）を指定します。
受信トラフィックは一番上に設定されたポリシーから順に照合され、条件に一致した最初のポリシーが適用され、定義されたアクションに従って、許可または拒否します。どのポリシーにも一致しないトラフィックは拒否されます。
ポリシーは必要に応じて適用範囲を指定できます。

ポリシーを定義するには、以下の手順を実行します。

(1) メニューの［ファイアウォール設定］-［ポリシー設定］をクリックし、［ポリシー設定］を開きます。

(2) 新しいポリシーを追加するには、ページの上下部にある［ポリシーの追加］をクリックします。新しいポリシー名を入力し[OK]をクリックすると、新しいポリシーがデフォルトの設定でリストの最上部に追加されます。

(3) 新しいまたは既存のポリシーのフィールドを変更するには、現在のフィールドの値をクリックして以下に示した適切な情報を指定し、[OK]をクリックします。

※　通信元:Untrust から通信先:Trust、通信元:Trust から通信先:Untrust への通信はサービス上制限されております。カスコンにてポリシーの登録はできますが通信の制限は解除されません。

ポリシーの設定

フィールド	説明
ポリシー名	ポリシー名を設定します。定義するポリシーを表す名前（最大 31 文字）を入力します。英字、数字、ハイフン、およびアンダースコア（全て半角）のみ使用可能です。この名前は、名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。 ※注意 以下の名称はシステム内にて利用しているため、ポリシー名として使用できません。 「all_deny」
通信元ゾーン 通信先ゾーン	ポリシーを適用する通信元と通信先のゾーンを選択します。 ● any 全てのゾーンが対象となります。 ● 選択する １つ以上の通信元ゾーンと通信先ゾーンを選択します。 ➢ Trust_xx 信頼された内部ポート側を指します。 ➢ Untrust_xx 信頼されていない外部ポート側(Internet 網)を指します。 ➢ DMZ_x_xx DMZ ポートを指します。 （注意）通信元:Untrust から通信先:Trust および通信元:Trust から通信先:Untrust への通信はサービス上制限されております。カスコンにてポリシーの登録はできますが通信の制限は解除されません。
通信元アドレス 通信先アドレス	ポリシーを適用する通信元と通信先の IP アドレスを選択します。 ● any 全てのアドレスが対象となります。 ● 選択する

	オブジェクト選択にあるアドレスの横にあるチェックボックスをオンにします。 個別にアドレスを定義する場合は、追加アドレス欄に 1 つ以上の IP アドレスを（1 行ごとに 1 つ）入力します。ネットワークマスクは任意に指定が可能です。一般的な形式は以下のとおりです。 〈ip_address〉/〈mask〉 ※オブジェクトは、お客様が作成したアドレスが表示されます。 ※注意 mask 値に「/0」の指定はできません。万が一「/0」を指定しますと、コミット時エラーになりますのでご注意ください。
アプリケーション	ポリシーを適用する特定のアプリケーションを選択します。 ● any アプリケーションを特定しない場合に選択します。 ● 選択する 表示されているアプリケーションの一覧の中から、設定したいアプリケーションを選び[追加]をクリックします。「選択中のアプリケーション」に選択した分のアプリケーションが追加されるので、確認後[OK]をクリックします。 アプリケーションの一覧表示は絞り込みを行うことが可能です。絞り込み方法は２種類あり、また両方同時に行うことも可能です。 ➢ 検索による絞りこみ 検索フィールドに検索文字列を入力して[Enter]をクリックすると、アプリケーション名での一致したアプリケーションが、一覧に表示されます。（部分一致） ➢ 規定された条件による絞りこみ 絞り込み条件（カテゴリー、サブカテゴリー、テクノロジー、リスク）のチェックボックスにチェックを入れると、それぞれの条件に属するアプリケーションが絞り込まれます。 アプリケーションの選択はアプリケーションフィルターの登録も可能です。 ➢ アプリケーションフィルターの登録 [フィルターを設定する]をクリックし、登録済みのアプリケーションフィルターから任意のものを選択し

	ます。 アプリケーションを定義する方法については、「アプリケーションの定義」を参照してください。 またアプリケーションフィルターを定義する方法については、「アプリケーションフィルターの定義」を参照してください。
Web ウィルスチェック	ポリシーの条件に一致するトラフィックのウィルスチェックの有無を定義します。 ● ○：利用する ウィルスチェックを行います。 ● ×：利用しない ウィルスチェックを行いません。
スパイウェアチェック	ポリシーの条件に一致するトラフィックのスパイウェアチェックの有無を定義します。 ● ○：利用する スパイウェアチェックを行います。 ● ×：利用しない スパイウェアチェックを行いません。
サービス	特定のアプリケーションにポリシーを定義する場合、1 つ以上のサービスを選択して、アプリケーションで使用できるポート番号を制限できます。 ● any プロトコルやポートを特定しない場合に選択します。 ● application-default アプリケーションで任意のアプリケーションを選択している場合（[any]でない場合）は、本項目を選択してください。 [application-default]は、アプリケーションが[any]の場合には使用できません。 ● 選択する 以下のいずれかの操作を実行します。 ➢ オブジェクト選択で該当するサービスの横にあるチェックボックスをオンにします。一般的なサービスは予め定義されています。 ➢ サービスを削除するには、該当するオブジェクトのチェックボックスをオフにするか、[any]を選択して個々のサービスおよびグループをすべてクリアします。

	新しいサービスを定義する方法については、「サービスの定義」を参照してください。 新しいサービスグループを定義する方法については、「サービスグループの定義」を参照してください。
IPS/IDS	ポリシーの条件に一致するトラフィックの脆弱性チェックの有無を定義します。 ● ○：利用する トラフィックに対して脆弱性チェックを行います。 ● ×：利用しない トラフィックに対して脆弱性チェックを行いません。
アクション	ポリシーの条件に一致するトラフィックの新しいネットワークセッションの扱いを定義します。 ● allow：許可する トラフィックを許可します。 ● deny：許可しない トラフィックを拒否します。

(4) リスト内でポリシーを削除するには、ポリシー番号の横のラジオボタンをクリックして該当するポリシーを選択し、ページ上下部にある［ポリシー削除］を選択します。

(5) リスト内でポリシーを移動するには、ポリシー番号の横のラジオボタンをクリックして該当するポリシーを選択し、ページ上下部にある［ポリシーの移動］を選択します。移動する範囲は、［一番上へ移動］［一番下へ移動］［一つ上へ移動］［一つ下へ移動］になります。

2.4　オブジェクト設定

2.4.1　アドレスの定義

特定の通信元アドレスまたは通信先アドレスのポリシーを定義するには、まず、アドレスおよびアドレス範囲を定義します。同じセキュリティ設定が必要なアドレスをアドレスグループにまとめることで、ポリシーの作成を簡略化できます（「アドレスグループの定義」を参照）。

アドレスを定義するには、以下の手順を実行します。

(1)　［オブジェクト設定］メニューで、［アドレス］をクリックして［アドレス設定］ページを開きます。

(2)　新しいアドレスまたはアドレス範囲を追加するには、以下の手順を実行します。

a.　［オブジェクトの追加］をクリックして［アドレス追加］ページを開きます。

b.　以下の情報を指定します。

アドレスの設定

フィールド	説明
オブジェクト名	定義するアドレスを表す名前（3～31 文字）を入力します。この名前は、ポリシーを定義するときにアドレスのリストに表示されます。名前の大文字と小文字は区別されます。また、一意

	の名前にする必要があります。英字、数字、ハイフン、およびアンダースコア（全て半角）のみ使用可能です。
IP アドレス	IP アドレスを指定します。 以下の形式でアドレスまたはネットワークを入力します。 ip_address/mask または ip_address ここで、mask は重要な意味を持つ 2 進数で、アドレスのネットワーク部を表すために使用されます。 例: 「192.168.80.150/32」は 1 つのアドレスを表し、「192.168.80.0/24」は 192.168.80.0～192.168.80.255 のすべてのアドレスを表します。 ※注意 mask 値に「/0」の指定はできません。万が一「/0」を指定しますと、コミット時エラーになりますのでご注意ください。
IP レンジ	アドレス範囲を指定するには、[IP レンジ]を選択してアドレス範囲を入力します。形式は以下のとおりです。 ip_address-ip_address 例: 「192.168.80.10-192.168.80.20」

c. ［OK］をクリックして新しいアドレスエントリを入力するか、［Cancel］をクリックして変更を廃棄します。

(3) 必要に応じて、以下の作業を実行します。

a. エントリを変更するには、エントリのリンクをクリックして変更を指定し、［OK］をクリックします。

b. エントリを削除するには、チェックボックスをオンにして［オブジェクトの削除］をクリックします。

2.4.2　アドレスグループの定義

ポリシーの作成を簡略化するには、同じセキュリティ設定が必要なアドレスをアドレスグループにまとめます。

アドレスグループを定義するには、以下の手順を実行します。

(1)　［オブジェクト設定］メニューで、［アドレスグループ］をクリックして［アドレスグループ設定］ページを開きます。

(2)　新しいアドレス グループを追加するには、以下の手順を実行します。

a.［オブジェクトの追加］をクリックして［アドレスグループ追加］ページを開きます。

b. 以下の情報を指定します。

新しいアドレス グループ

フィールド	説明
オブジェクト名	アドレスグループを表す名前（3～31 文字）を入力します。この名前は、ポリシーを定義するときにアドレスのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。英字、数字、ハイフン、およびアンダースコア（全て半角）のみ使用可能です。
設定済み IP アドレス	このグループに含めるアドレスの横に

あるチェックボックスをオンにします。

c. ［OK］をクリックして新しいアドレスグループを入力するか、［Cancel］をクリックして変更を廃棄します。

(3) 必要に応じて、以下の作業を実行します。

a. エントリを変更するには、エントリのリンクをクリックして変更を指定し、［OK］をクリックします。

b. エントリを削除するには、チェックボックスをオンにして［オブジェクトの削除］をクリックします。

2.4.3　アプリケーショングループの定義

ポリシーの作成を簡略化するには、同じセキュリティ設定が必要なアプリケーションをアプリケーショングループにまとめます。

アプリケーショングループを定義するには、以下の手順を実行します。

(1)　［オブジェクト設定］メニューで、［アプリケーショングループ］をクリックして［アプリケーショングループ設定］ページを開きます。

(2)　アプリケーショングループを追加するには、以下の手順を実行します。

a.　［オブジェクトの追加］をクリックして［アプリケーショングループ追加］ページを開きます。

b.　アプリケーショングループの名前を入力します。

c.　ウィンドウの上部で、アプリケーションの絞り込みの基準として使用する項目をクリックします。　たとえば、［networking］カテゴリーのみをリストに表示するには、［networking］のチェックボックスをオンにします。

d.　その他の列で絞り込みを行うには、列のエントリのチェックボックスをオンにします。絞り込みは連続的で、カテゴリー、サブカテゴリー、テクノロジー、リスク、の順に適用されます。

選択するとページ下部のアプリケーションのリストが自動的に更新されます。

e.　絞り込みを解除するには、［フィルターの解除］ボタンを選択します。

f. アプリケーションを追加するには、表示アプリケーション横の［追加］ボタンで追加します。追加後、下部一覧に表示されます。

g. アプリケーションフィルターを追加するには、［フィルターを設定する］にて、追加対象のフィルターのチェックボックスをクリックし、［OK］をクリックするか、［Cancel］をクリックして変更を破棄します。

h. アプリケーションフィルターを削除するには、選択一覧から［削除］ボタンをクリックし、削除します。

i. ［OK］をクリックして新しいアプリケーショングループを定義するか、［Cancel］をクリックして変更を廃棄します。

(3) 必要に応じて、以下の作業を実行します。

a. エントリを変更するには、エントリのリンクをクリックして変更を指定し、［OK］をクリックします。

b. エントリを削除するには、チェックボックスをオンにして［オブジェクトの削除］をクリックします。

2.4.4　アプリケーションフィルターの定義

アプリケーションフィルターはカテゴリーなどのフィルター条件のみを定義するため、制御対象のアプリケーションのカテゴリー、サブカテゴリー等を予め定義しておくことで、アプリケーションが増えた際に自動的に制御対象となり、逐次アプリケーションをポリシーに追加する必要がありません。

アプリケーションフィルターを定義するには、以下の手順を実行します。

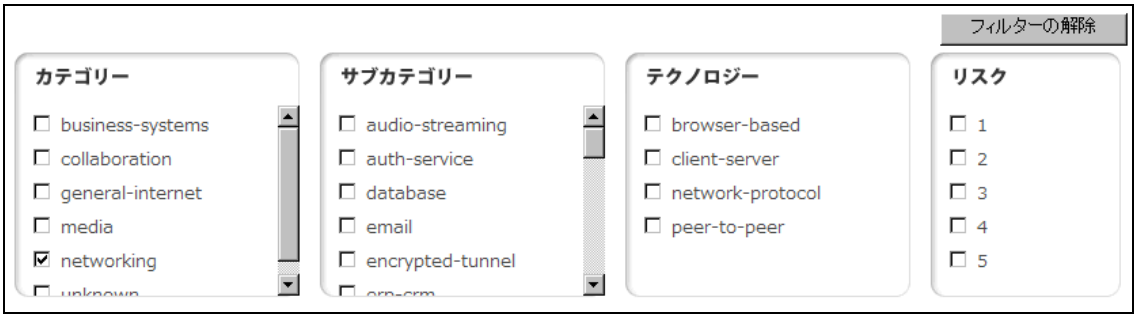
(1)　［オブジェクト設定］メニューで、［アプリケーションフィルター］をクリックして［アプリケーションフィルター設定］ページを開きます。

(2)　新しいアプリケーションフィルターを追加するには、以下の手順を実行します。

a.　［オブジェクトの追加］をクリックして［アプリケーションフィルター追加］ページを開きます。

b.　フィルターの名前を入力します。

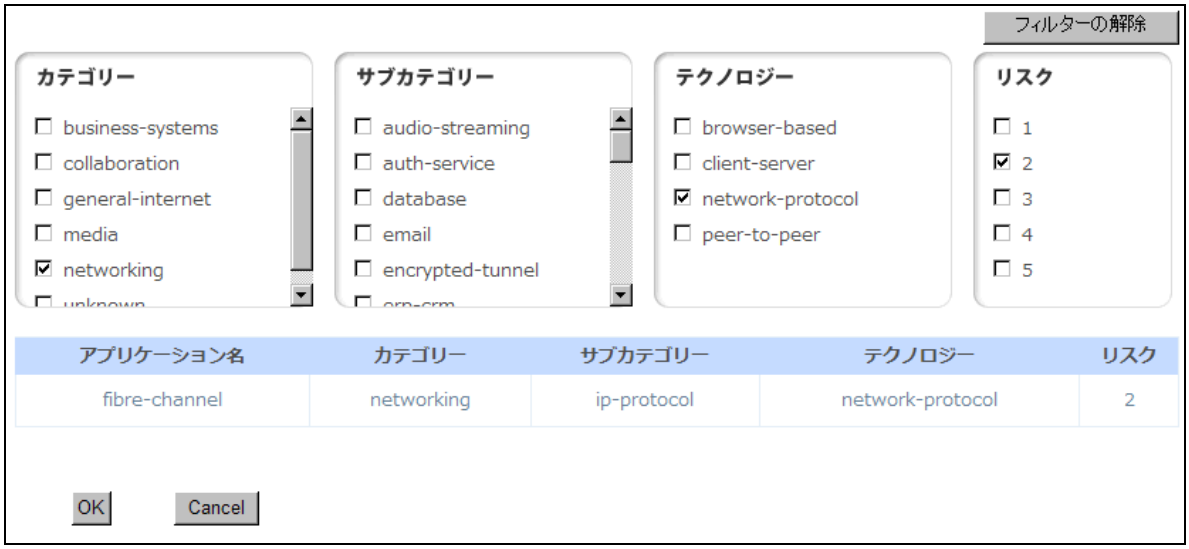
c.　ウィンドウの上部で、フィルタリングの基準として使用する項目をクリックします。 たとえば、［networking］カテゴリーのみをリストに表示するには、［networking］のチェックボックスをオンにします。



その他の列にフィルターを適用するには、列のエントリのチェックボックスをオンにします。フィルタリングは連続的で、カテゴリフィルター、サブカテゴリフィルター、テクノロジフィルター、リスクフィルターの順に適用されます。
選択するとページ下部のアプリケーションのリストが自動的に更新されます。

d. 選択したフィルターを解除するには、［フィルターの解除］ボタンを選択します。
e. ［OK］をクリックして新しいアプリケーションフィルターを定義するか、［Cancel］をクリックして変更を廃棄します。

(3) 必要に応じて、以下の作業を実行します。
a. エントリを変更するには、エントリのリンクをクリックして変更を指定し、［OK］をクリックします。
b. エントリを削除するには、チェックボックスをオンにして［オブジェクトの削除］をクリックします。



2.4.5　サービスの定義

1 つ以上のサービスを選択して、アプリケーションで使用できるポート番号を制限できます。一般的なサービスは予め定義されています（変更・削除不可）が、他のサービスの定義を追加することができます。

※初期登録しているサービスオブジェクトについて、「service-https」「service-https_443」はオブジェクト名は異なりますが同じ設定内容となります。どちらを利用しても問題ありません。

サービスを定義するには、以下の手順を実行します。

(1)　［オブジェクト設定］メニューで、［サービス］をクリックして［サービス設定］ページを開きます。

(2)　新しいアドレス グループを追加するには、以下の手順を実行します。

a.［オブジェクトの追加］をクリックして［サービス追加］ページを開きます。

b. 以下の情報を指定します。

新しいサービス

フィールド	説明
オブジェクト名	サービス名を表す名前（最大 31 文字）を入力します。この名前

	は、ポリシーを定義するときにアドレスのリストに表示されます。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。英字、数字、ハイフン、およびアンダースコア（全て半角）のみ使用可能です。
プロトコル	サービスで使用するプロトコル(TCP または UDP)を選択します。
ポート	サービスで使用するポート番号(0～65535)またはポート番号の範囲(ポート 1-ポート 2)を入力します。複数のポートまたはポート範囲はコンマで区切ります。

c. ［OK］をクリックして新しいサービスを入力するか、［Cancel］をクリックして変更を廃棄します。

(3) 必要に応じて、以下の作業を実行します。

a. エントリを変更するには、エントリのリンクをクリックして変更を指定し、［OK］をクリックします。

b. エントリを削除するには、チェックボックスをオンにして［オブジェクトの削除］をクリックします。

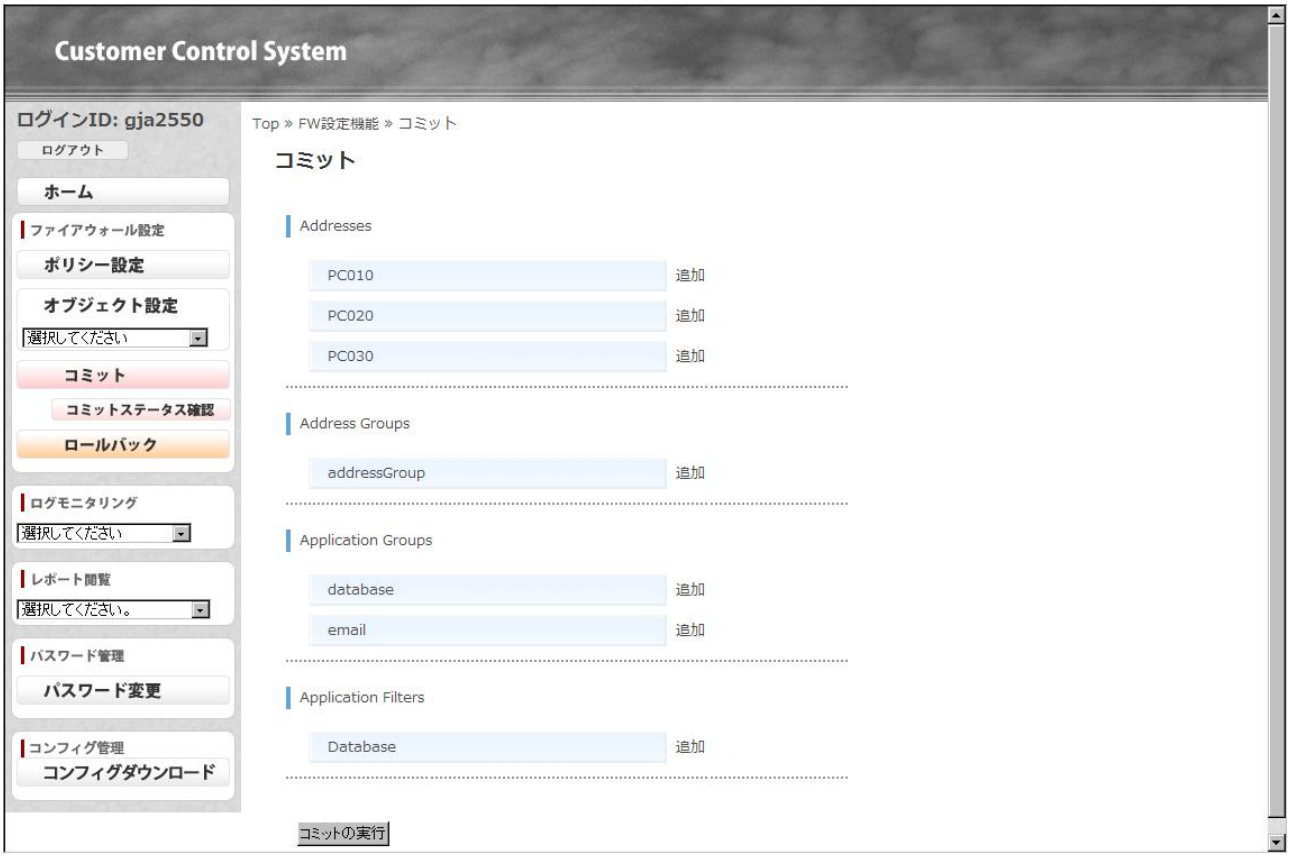
2.5　コミット

設定を変更して[OK]をクリックすると、現在の変更内容が保存されます。保存された設定内容をファイアウォールに適用（コミット）させるにはコミット処理をする必要があります。

(1) 設定内容をファイアウォールにコミットするには、以下の手順を実行します。

a. ［ファイアウォール設定］メニューで、［コミット］をクリックします。設定変更がある場合に［コミット］ページが表示されます。

b. 変更内容を確認します。



c. ［コミットの実行］をクリックすると確認ダイアログが表示され、［OK］をクリックしてコミット処理を開始します。［Cancel］をクリックしてコミット処理を中止できます。

d.　コミット処理が正常に受け付けられると、［受付完了］ページが表示されます。

e. 定期的に［コミットステータス確認］ページを確認し、処理状態が［処理完了］となれば、コミット処理が完了となります。

※注意

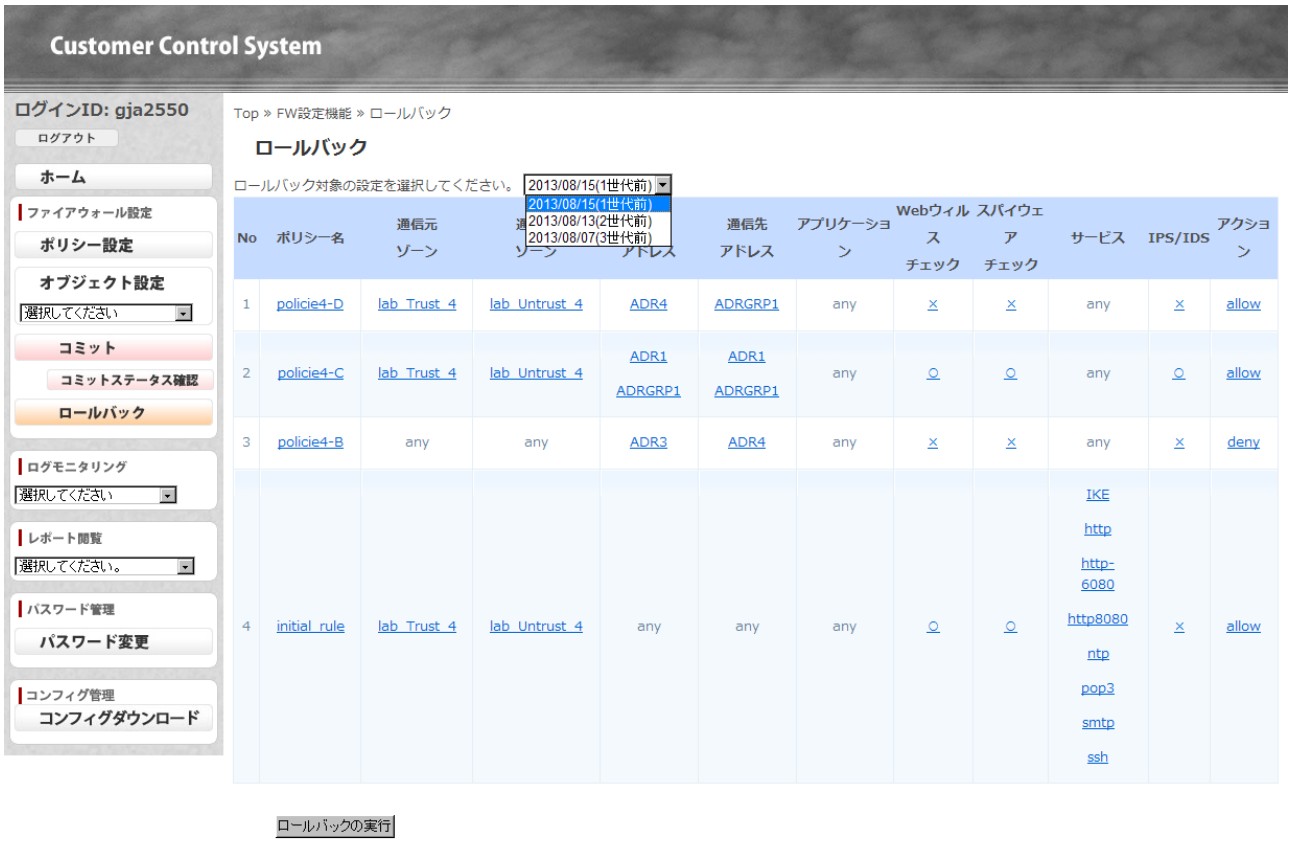
- ✧ コミット処理はポリシー数、オブジェクト数に比例して処理時間が長くなります。
- ✧ 他の利用者がコミット，ロールバック処理を行っている場合、待ち状態となりコミット処理が失敗するケースがあります。その際は、３～５分後に再度コミット処理を実行してください。
- ✧ コミット処理中の間は、ポリシー設定，オブジェクト設定，コミット，ロールバック機能を利用することはできません。

2.6　ロールバック

前回コミットまでの 3 世代分の設定が保存されています。過去の設定内容を必要に応じてファイアウォールに適用することが可能です。

(1) 過去の設定内容をファイアウォールに適用するには、以下の手順を実行します。

a. ［ファイアウォール設定］メニューで、［ロールバック］をクリックして［ロールバック］ページを開きます。



b. ［ロールバック対象の設定を選択してください。］ドロップダウンリストから過去の設定内容を確認します。各オブジェクトの設定内容を確認するには、現在のフィールドの値をクリックして確認することができます。

c. ［ロールバックの実行］をクリックすると確認ダイアログが表示され、［OK］をクリックしてロールバック処理を開始します。［Cancel］をクリックしてロールバック処理を中止できます。

d. ロールバック処理が正常に受け付けられると、［受付完了］ページが表示されます。

e. 定期的に［コミットステータス確認］ページを確認し、処理状態が［処理完了］となれば、ロールバック処理が完了となります。

※注意

- ✧ 他の利用者がコミット，ロールバック処理を行っている場合、待ち状態となりロールバック処理が失敗するケースがあります。その際は、３～５分後に再度ロールバック処理を実行してください。
- ✧ ロールバック処理中の間は、ポリシー設定，オブジェクト設定，コミット，ロールバック機能を利用することはできません。

2.7 ログモニタリング

Customer Control System では、ファイアウォールのトラフィック、IPS/IDS、Web ウィルス、スパイウェアチェックのログ情報が当日＋過去 2 日分閲覧できます。また、ログ更新は 1 時間に 1 回行われます。

ログを表示するには、以下の手順を実行します。

(1) ［ログモニタリング］メニューで、ログタイプをクリックします。

(2) 特定文字列によるログ検索が可能です。
検索対象となる文字列を入力します。対象より検索対象の列を選択します。［検索する］ボタンをクリックすると、検索されたリストが表示されます。

(3) 1 ページの表示行数変更が可能です。
［表示行数］ドロップダウンリストより、表示行数を選択します。表示行数が変更され表示されます。

(4) ログデータを CSV 形式ファイルでのダウンロードが可能です。
ダウンロードするログの期間を指定します。左側テキストボックスボックスに開始日を入力します。テキストボックスをクリックすることによりカレンダーが表示されますので、開始日を選択して下さい。入力も可能です。
右側テキストボックスに終了日を入力します。開始日と同様な操作となります。

開始日、終了日ともに入力後、［ダウンロードする］ボタンによりログのダウンロードが開始されます。ダウンロードされるログは ZIP 圧縮され保存されます。ダウンロードされるログは検索結果にかかわらず、指定期間分すべてのログをダウンロードします。

※注意

ログの保存期間は当日＋過去 2 日分となります。

ダウンロードを行う際はダウンロードの確認ダイアログウィンドウが表示されるため、
InternetExplorer にて以下の設定を行ってください。

1．「ツール」⇒「インターネットオプション」⇒「セキュリティ」⇒該当するゾーンを選択⇒「レベルのカスタマイズ」をクリック。

2．「ダウンロード」⇒「ファイルのダウンロード」の項目にて
「有効にする」を選択し、「OK」をクリック。

2.7.1 ファイアウォールログ

各セッションの終了のエントリが表示されます。各エントリには、以下の項目が含まれています。

フィールド	説明
日時	ログが出力された日時
タイプ	ログ種別：「TRAFFIC」
通信元アドレス	通信元の IP アドレス
通信先アドレス	通信先の IP アドレス
ポリシー名	適用されたポリシー名
アプリケーション	アプリケーション名
通信元ゾーン	通信元のゾーン名
通信先ゾーン	通信先のゾーン名
通信元ポート	通信元のポート
通信先ポート	通信先のポート
プロトコル	プロトコル名（TCP/UDP/IP/ICMP）
アクション	ルールアクション ［deny］：トラフィックを拒否しました ※ファイアウォールログは[deny]のみ表示されます。
転送量	トラフィック転送量

2.7.2　IPS/IDS ログ

ファイアウォールで生成された各セキュリティアラームのエントリが表示されます。各エントリには、以下の項目が含まれています。

フィールド	説明
日時	ログが出力された日時
タイプ	ログ種別：「THREAT」
通信元アドレス	通信元の IP アドレス
通信先アドレス	通信先の IP アドレス
ポリシー名	適用されたポリシー名
アプリケーション	アプリケーション名
通信元ゾーン	通信元のゾーン名
通信先ゾーン	通信先のゾーン名
通信元ポート	通信元のポート
通信先ポート	通信先のポート
アクション	アラートアクション [alert]：スレットを検出しました（拒否はしない） [drop]：スレットを検出し、関連セッションを切断しました [drop-all-packets]：スレットを検出し、全パケットをドロップしました(セッションは残る) [reset-client]：スレットを検出し、TCP RST をクライアントへ送信しました [reset-server]：スレットを検出し、TCP RST をサーバへ

送信しました [reset-both]：スレットを検出し、TCP RST を サーバ/クライアント両方へ送信しました

2.7.3　Web ウィルスチェックログ

Web ウィルスチェックで生成された各セキュリティアラームのエントリが表示されます。各エントリには、以下の項目が含まれています。

フィールド	説明
日時	ログが出力された日時
タイプ	ログ種別：「THREAT」
通信元アドレス	通信元の IP アドレス
通信先アドレス	通信先の IP アドレス
ポリシー名	適用されたポリシー名
アプリケーション	アプリケーション名
通信元ゾーン	通信元のゾーン名
通信先ゾーン	通信先のゾーン名
通信元ポート	通信元のポート
通信先ポート	通信先のポート
アクション	アラートアクション [alert]：スレットを検出しました（拒否はしない） [drop]：スレットを検出し、関連セッションを切断しました [drop-all-packets]：スレットを検出し、全パケットをドロップしました(セッションは残る)

	[reset-client]：スレットを検出し、TCP RST を クライアントへ送信しました [reset-server]：スレットを検出し、TCP RST をサーバへ 送信しました [reset-both]：スレットを検出し、TCP RST を サーバ/クライアント両方へ送信しました

2.7.4　スパイウェアチェックログ

スパイウェアチェックで生成された各セキュリティアラームのエントリが表示されます。各エントリには、以下の項目が含まれています。

フィールド	説明
日時	ログが出力された日時
タイプ	ログ種別：「THREAT」
通信元アドレス	通信元の IP アドレス
通信先アドレス	通信先の IP アドレス
ポリシー名	適用されたポリシー名
アプリケーション	アプリケーション名
通信元ゾーン	通信元のゾーン名
通信先ゾーン	通信先のゾーン名
通信元ポート	通信元のポート
通信先ポート	通信先のポート
アクション	アラートアクション [alert]：スレットを検出しました（拒否はしない） [drop]：スレットを検出し、関連セッションを切断しました [drop-all-packets]：スレットを検出し、全パケットをドロップしました(セッションは残る)

	[reset-client]：スレットを検出し、TCP RST を クライアントへ送信しました [reset-server]：スレットを検出し、TCP RST をサーバへ 送信しました [reset-both]：スレットを検出し、TCP RST を サーバ/クライアント両方へ送信しました

2.8 レポート

Customer Control System では、ファイアウォールで集計したトラフィック統計情報レポートが表示できます。

レポートを表示するには、以下の手順を実行します。

(1) ［レポート閲覧］メニューで、ドロップダウンリストよりレポート名をクリックします。

(2) アプリケーション（トラフィック）以外のレポートについては、デフォルトで前の暦日のレポートがすべて表示されます。過去のいずれかの日のレポートを表示するには、ページの上位の［レポート取得対象を選択してください。］のドロップダウンリストからレポートの生成日を選択します。

2.8.1　アプリケーション（期間指定）

アプリケーションごとのトラフィック集計（上位 50 件）を表示します。

リスク	アプリケーション	セッション数	転送量(byte)	カウント数
4	web-browsing	187	2,215,962	0
4	dns	85	13,633	0
4	ssl	12	144,968	0
4	facebook-base	7	124,838	0
2	snmp-base	6	2,142	0
2	twitter-base	5	41,963	0
4	yahoo-douga	2	2,091,504	0
3	facebook-social-plugin	2	15,750	0
4	icmp	1	70	0
4	flash	1	304,138	0
3	google-update	1	2,384	0
5	youtube-base	1	11,071	0

フィールド	説明
リスク	アプリケーションの危険度
アプリケーション	アプリケーション名
セッション数	アプリケーションのセッション数累計（期間内）
転送量	アプリケーションの転送量累計（期間内）
カウント数	検出された脅威の数

2.8.2　アプリケーション（日単位）

アプリケーションごとのアクセス数集計（上位 50 件）を表示します。

アプリケーション	リスク	転送量	セッション数
web-browsing	4	32,009,064	3,156
dns	4	50,187	290
facebook-social-plugin	3	1,532,531	73
http-video	5	112,902,689	49
snmp-base	2	13,926	39
ms-update	4	1,596,306	35
facebook-base	4	256,661	30
ssl	4	187,296	18
flash	4	3,797,882	11
youtube-base	5	31,264,131	5
google-analytics	2	32,218	2
silverlight	2	484,876	2
google-update	3	8,809	2

フィールド	説明
アプリケーション	アプリケーション名
リスク	アプリケーションの危険度
転送量	アプリケーションの転送量合計（日単位）
セッション数	アプリケーションのセッション数合計（日単位）

2.8.3　通信元アドレス

通信元アドレスごとのアクセス集計（上位 50 件）を表示します。

フィールド	説明
通信元	通信元の IP アドレス
通信元（ホスト名）	通信元のホスト名
通信元ユーザ	通信元のユーザ（非表示）
転送量	通信元の転送量合計（日単位）
セッション数	通信元のセッション数合計（日単位）

2.8.4　通信先アドレス

通信先アドレスごとのアクセス集計（上位 50 件）を表示します。

フィールド	説明
通信先	通信先の IP アドレス
通信先（名前解決済み）	通信先のホスト名
通信先ユーザ	通信先のユーザ（非表示）
転送量	通信先の転送量合計（日単位）
セッション数	通信先のセッション数合計（日単位）

2.8.5　通信先トラフィック（国毎）

トラフィックを送信した国ごとのアクセス集計（上位 50 件）　を表示します。

フィールド	説明
通信先	通信先の国名
転送量	通信先の転送量合計（日単位）
セッション数	通信先のセッション数合計（日単位）

2.8.6　攻撃トラフィック

攻撃トラフィックを送信したスレットの集計（上位 50 件） を表示します。

フィールド	説明
リスク	スレットの危険度 (informational, low, medium, high, critical)
スレット ID	スレット名称
tid	スレットの識別 ID
タイプ	スレットのタイプ
回数	スレットの検出回数

2.9　パスワード変更機能

ログインパスワードを変更します。パスワードは有効期限があり、定期的に変更する必要があります。パスワードには、英小文字、英大文字、記号、数字（全て半角）を混在させてください。

(1)　［パスワード管理］メニューで、［パスワード変更］をクリックして［パスワード変更］ページを開きます。

(2)　パスワードを変更するには、以下の手順を実行します。

a. 以下の情報を指定します。

パスワード変更

フィールド	説明
現在のパスワード	現在のパスワードを入力します。
変更後のパスワード 変更後のパスワード（再入力）	ユーザのパスワード(8 文字以上、14 文字以内)を入力し、確認のためにパスワードを再入力します。これらのパスワードの大文字と小文字は区別されます。

b. ［OK］をクリックして変更を完了します。また、［Clear］をクリックして変更を廃棄します。

2.10 コンフィグダウンロード機能

ファイアウォールの設定情報（コンフィグ情報）をテキスト形式のファイルでダウンロードできます。

(1) ［コンフィグ管理］メニューで、［コンフィグダウンロード］をクリックして［コンフィグダウンロード]ページを開きます。

(2) コンフィグ設定をダウンロードするには、[ダウンロードする]ボタンを押してファイル保存先を指定します。