

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 01.07 最終更新日 2018/07/26

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	KDD I
2013/11/27	01.01	2.7	ログ情報および保存期間について訂正	KDD I
		2.3	誤記訂正	KDD I
2014/02/12	01.02	2.3.1	使用できないポリシー名の訂正	KDD I
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	KDDI
			画面にてアドレスグループが追加できな	
			い)に伴う変更	
		2.4.3	機能変更(アプリケーショングループ追	KDDI
			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	
		2.7	画面の「注意」文言変更に伴う画像の差	KDD I
		2.10	替え	
2017/12/08	01.04		P3 問い合わせ先の変更、バージョンアッ	KDD I
			プに伴う内容確認	
2018/05/17	01.05	1.2	動作環境の制限事項に関して、KCPS1/2	KDD I
			での制限値を記載	
		2.3.1	「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	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	
2018/07/11	01.06	2.9	パスワード変更機能	KDD I
			「いる個所を8文子以上、14 文子以内と修 」 一	
2019/07/26	01.07	296		
2010/07/20	01.07	2.0.0	攻革ドラフィック 	
			ラハノの农品を数于农品(1,2,3,4,3)が ら文字(informational low medium	
			「システ(Informational, Tow, medium,	
2018/07/26	01.07	2.8.6	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 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

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	4
2.4.1 アドレスの定義	4
2.4.2 アドレスグループの定義	6
2.4.3 アプリケーショングループの定義	8
2.4.4 アプリケーションフィルターの定義2	20
2.4.5 サービスの定義	2?
2.5 コミット	24
2.6 ロールパック	?7
2.7 ログモニタリング	29
2.7.1 ファイアウォールログ	?9
2.7.2 IPS/IDS ログ	30
2.7.3 Web ウィルスチェックログ	3
2.7.4 スパイウェアチェックログ	35
2.8 レポート	37
<i>2.8.1 アプリケーション(期間指定)</i> :	8
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	10
2.8.4 通信先アドレス	1
2.8.5 通信先トラフィック(国毎)	12
2.8.6 攻撃トラフィック	13
2.9 パスワード変更機能	4
2.10 コンフィグダウンロード機能	15

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は、以下のブラウザに対応しています。 > Internet Explorer 11 (Windows7) > Firefox 50.1.0 (Windows7) 上記ブラウザ以外は、サポート対象外となります。

● 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。

<u>アクセス</u>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。

Customer Control System
ログインID
パスワード
ファイアウォールID

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。

2.2 メイン画面

IグインID: gja2550 ログアウト	お知らせ	
ホーム		
ファイアウォール設定		
ポリシー設定		
オブジェクト設定	マニュアルダウンロード	
選択してください 💽	» 操作マニュアル	
コミット		
コミットステータス確認		
ロールバック		
ログモニタリング		
訳してください		
レボート開発		
バスワード管理		
パスワード変更		
コンフィグ管理		
コンフィグダウンロード		

[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(プロック)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。

コグインID: gja2550 ログアウト	То	p » F 术!	-W設定機能 » リシー設定	ポリシー設定									
ホーム	त्रहे	1=1-	一の窓動・「選	視してください。	- ポリ:	ノーの追加	ポリシー	一の削除					
ファイアウォール設定 ポリシー設定	31	No.	ポリシー名	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 ヨン	Webウィ ルス チェック	スパイウ ェア チェック	サービス	IPS/IDS	アクショ ン
オフシェクト設定 選択してください ・	c	1	policie4-D	lab_Trust_4	lab_Untrust_4	ADR4	ADRGRP1	any	×	×	any	×	allow
コミット	c	2	policie4-C	lab_Trust_4	lab_Untrust_4	ADR1 ADRGRP1	ADR1 ADRGRP1	any	<u>0</u>	<u>0</u>	any	0	allow
ロールバック	c	3	policie4-B	any	any	ADR3	ADR4	any	×	×	any	×	deny
ログモニタリング	c	4	initial_rule	lab_Trust_4	lab_Untrust_4	any	any	any	Q	<u>o</u>	http 6080 http8080 IKE ntp pop3 smtp ssh	×	allow

- (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	
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	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。
通信先ゾーン	• 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) <u>通信元:Untrust から通信先:Trust および通信元:Trust</u>
	<u>から通信先:Untrust への通信はサービス上制限されておりま</u>
	<u>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</u>
	除されません。
通信元アドレス	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
通信先アドレス	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。

KDDI クラウドプラットフォームサービス 拡張 FW Customer Control System 操作マニュアル

	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。
	● x : 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
	<i>د</i> ۱.
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:
	^r 192.168.80.10-192.168.80.20 J
	「 「しいアドレスエントリを入力するか、 [Cancel]をクリックして

- 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。

1 グアウト	アドレスグノ	*////////////////////////////////////	ノ政定	
アイアウォール設定	オブジェク	トの追加 オブジェクトの利	间除	
ポリシー設定		オブジェクト名	メンバー数	アドレス
オブジェクト設定		ADRGRP1	2	ADR1,ADR2
新してくたさい 形してくたさい ドレス		ADRGRP3	3	ADR1,ADR2,ADR3
ブリケーショングループ ブリケーションフィルター ビス ロールバック		APGRP2	2	ADR3
ガエークリング	オブジェク	トの追加 オブジェクトの利	川除	
択してください				
- ポート開覧				
択してください。 💽				
詳決してください。	1			
RRUてください。 パスワード管理 パスワード管理 パスワード変更				
諸択してください。 パスワード管理 パスワード変更 コンフィグ管理				

(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。

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。

新しいアドレス グループ

- 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。

Customer Contr	ol Sy	vstem		
ログインID: gja2550 ログアウト	Top >	»FW設定機能 » アプリケーシ	オブジェクト設 ヨングループ	走 » アブリケーショングループ設定 プ 設定
ホーム ファイアウォール設定 ポリシー設定		オブジェクトロ	Dieto	オブジェクトの削除
		オブジェクト名	メンバー数	アプリケーション・フィルター
オフシェクト設定		ap_grp4	4	2ch,gnutella,unknown-tcp,unknown-udp
選択してください		ap4_db	з	mysql,oracle,postgres
アドレスグループ		apg4_mail	8	100bao, 1 und 1-mail, 2 ch, 2 ch-posting, 360-safeguard-update, 3 pc, 4 shared, 4 sync
サービス ロールバック ログモニタリング 選択してください		オブジェクト(り追加	オブジェクトの削除
レボート閲覧 選択してください。				
バスワード管理 パスワード変更				
コンフィグ管理 コンフィグダウンロード				

- (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。

				フィルタ	一の解除
カテゴリー	サブカテゴリー	テクノロ	ジー	リスク	
 □ business-systems □ collaboration □ general-internet □ media ☑ networking ☑ unknown 	audio-streaming auth-service database email encrypted-tunnel	brows client- m netwo peer-t	er-based server rk-protocol o-peer	□ 1 ■ 2 □ 3 □ 4 □ 5	
アプリケーション名	カテゴリー	サブカテゴリー	テクノロジー	-	リスク
fibre-channel	networking	ip-protocol	network-proto	col	2
OK Cancel					

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。 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。

Customer Control System							
ログインID: gja2550 ^{ログアウト} ホーム	Top » FW設定機能 » オ サービス設定	ブジェクト設定 » サービス設定					
ファイアウォール設定	オブジェクトのえ	自加オブジェクトの削除					
ポリシー設定		オプジェクト名	プロトコル	ボート			
オブジェクト設定		domain-tcp	tcp	53			
選択してください ・		domain-udp	udp	53			
アドレス アドレス フドレスグループ アドレスグループ	m	ftp	tcp	21			
テラリケーションライルダー サービス	E	http	tcp	80			
u-10/177	=	http8080	tcp	8080			
ログモニタリング	E	IKE	udp	500			
選択してくたさい	E	imap	tcp	143			
レポート開覧	E	IPsecoverUDP	udp	4500			
	E	MessageSubmission	top	587			
バスワード管理		ntp	udp	123			
パスワード変更		рор3	tcp	110			
コンフィグ管理	=	rdp3389	tcp	3389			
JJJ7799990-F		rtsp	tcp	554			
	П	service-http	tcp	80,8080			

(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。

コグインID: gja2550	Top » FW設定機能 » コミット		
ログアウト	コミット		
ホーム			
ファイアウォール設定	Addresses		
ポリシー設定	PC010	這加	
オブジェクト設定	PC020	追加	
選択してください 💽	PC030	追加	
コミット			
コミットステータス確認	Address Groups		
ロールバック	addressGroup	;eh0	
ログモニタリング		Accurate	
選択してください 💽	Application Groups		
レポート閲覧	database	追加	
朝してください。	email	追加	
バスワード管理	1		
パスワード変更	Application Filters		
コンフィグ管理	Database	追加	
コンフィグダウンロード			

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。

Customer Cont	rol System	
ログインID: gja2550 ログアウト	Top » FW設定機能 » I コミット	JEWH
ホーム	Commit Operation	
ファイアウォール設定 ポリシー設定 オブジェクト設定	Operation 受付時間 処理状態 メッセージ	コミット 2013/08/15 12:38:44 受付完了 コミット処理を受け付けました。一定時間後、コミットステータス確認画面にて処理結果を確認してください。
「選択してください」 ・ コミット コミット コールバック		
 選択してください レポート閲覧 選択してください。 		
バスワード管理 パスワード変更		
コンフィク管理 コンフィグダウンロード		

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。

Customer Cont	rol System	
ログインID: gja2550 ログアウト	Top » FW設定機能 » コミットステータス確認	
ホーム	Commit/Rollback Operation	
ファイアウォール設定	Operation	コミット
ポリシー設定	受付時間 処理状態	2013/08/15 12:38:44 コミット成功
オブジェクト設定	メッセーシ	コミット処理が元子しました。
選択してください		
コミット		
コミットステータス確認		
ロールバック		
ログモニタリング		
選択してください・		
レポート閲覧	1	
「選択してください。・		
パスワード管理]	
パスワード変更		
コンフィグ管理 コンフィグダウンロード		

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。

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。

Customer Contr	rol Sy	/stem										
ログインID: gja2550 ログアウト	Top E	»FW設定機能; コールバック	▶ ロールバック 7									
ホーム ファイアウォール設定 ポリシー設定	No	ルバック対象の: ポリシー名	設定を選択してくた 通信元 ゾーン	ださい。 2013/08/15 2013/08/15 道 2013/08/13 2013/08/07 >	(1世代前) (1世代前) (2世代前) (3世代前) アトレス	適信先 アドレス	アプリケーショ ン	Webウィル ス チェック	スパイウェ ア チェック	サービス	IPS/IDS	アクション
オブジェクト設定 選択してください	1	policie4-D	lab Trust 4	lab Untrust 4	ADR4	ADRGRP1	апу	×	×	апу	×	allow
コミット コミットステータス確認 ロールバック	2	policie4-C	lab Trust 4	lab Untrust 4	ADR1 ADRGRP1	ADR1 ADRGRP1	any	Q	Q	any	Q	allow
ーログモニタリング	3	policie4-B	any	any	ADR3	ADR4	any	×	×	any	≚	<u>deny</u>
選択してください 選択してください レボート開覧 選択してください。 ・ バスワード管理 パスワード変更 コンフィグ管理 コンフィグダウンロード	4	initial rule	lab Trust 4	jab Untrust 4	any	any	any	٩	0	IKE http- 6080 http8080 ntp pop3 smtp ssh	×	allow

ロールバックの実行

- 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。

- ◇ 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 KIP 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

<u>ログの保存期間は当日+過去2日分となります。</u>

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。

- 「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

Customer Contr	ol System										
ログインID: ofl1974 ログアウト キーム	Top » ログモニタリング » IPS/IDSログ	IPS/IDSD-	Ď								
ファイアウォール的学	» ログ検索 横索する										
ポリシー設定	表示件数: 20 💌 検	察キーワート	:	(検索対象	: 🗖 通信元:	アドレス 🗆 逼	冒先アドレス 「	□ 通信元ポー	トロ通信先	ポート ロア	プリケーシ
オブジェクト設定	ヨン) 対象期間:]~[(例: 201	1/05/01)						
	» ログダウンロード	ウンロードする	※検索キーワー	ードにかかわらず、指	定した対象期	明闇内のすべての	0ログをダウン	ロードします。			
	No. 10 10 10 10 10 10 10 10 10 10 10 10 10										
コミットステータス確認	(注意) ダワンロートを 1、「ツール」⇒「イ 2、「ダウンロード」:	行う際はInt ンターネット ⇒「ファイ』	ternetExplorerにて ヽオプション」⇒「 しのダウンロード」	こ以下の設定を行って。 セキュリティ」⇒該当 の項目で「有効にする	ください。 するゾーン? 」を選択し、	を選択⇒「レベ」	しのカスタマイ ック	ズ」をクリッ	ク		
コミットステータス構設 ロールバック ログモニタリング	【注意】タウンロートを 1. 「ツール」⇒「イ 2. 「ダウンロード」:	行う際はInt ンターネット コ「ファイル	ernetExplorerにて ヽオプション」⇒「 レのダウンロード」	□以下の設定を行ってく セキュリティ」⇒該当 の項目で「有効にする	ください。 けるゾーン? 」を選択し、 1	を選択⇒「レベ∪ 、「OK」をクリ	しのカスタマイ ック	ズ」をクリッ	9		
コミットステータス構成 ロールバック ログモニタリング 翻訳してください	(注意) タウンロートを 1. 「ツール」⇒「イ 2. 「ダウンロード」: 日時	行う際はInt ンターネット ⇒「ファイル タイプ	ernetExplorerにて トオプション」⇒「 しのダウンロード」 適借元アドレス	は下の設定を行ってく セキュリティ」⇒該当 の項目で「有効にする 通信先アドレス	<たさい。 するゾーン? 」を選択し、 1 ポリシー名	を選択⇒「レペ↓ 、「OK」をクリ アプリケーション	しのカスタマイ ック ン適信元ゾーン	ズ」をクリッ 通信先ゾーン	ク 通信元ポー1	▶週信先术一	トアクション
コミットステータス確認 ロールバック ログモニタリング 訳化してください レポート開覧	は登録 ダウシロート名 1. 「ジール」⇒「イ 2. 「ダウンロード」: 日時 2013/04/10 17:09:33	行う際はInt ンターネット ⇒「ファイル <mark>タイプ</mark> THREAT	emetExplorerにて ・オプション」 ⇒ F しのダウンロード」 適信元アドレス 61.250.176.20	・以下の設定を行って、 セキュリティ」→該当 の項目で「有効にする 通信先アドレス 210.150.178.115	<ださい。 するソーン うしを選択し、 1 ポリシー名 。 Ping	を選択⇒「レペパ 「OK」をクリ アプリケーショ) msrpc	しのカスタマイ ック ン通信元ゾーン Untrust_3	ズ」をクリッ 適信先ゾーン Trust_3	ク 通信元ポー 1846	▶週信先ボー 139	トアクション reset-s
コミットステータス確認 ロールバック ログモニタリング 朝见してください マート閲覧 朝见してください。	は美国 ダウンロートで 1. 「ツール」⇒「イ 2. 「ダウンロード」: 日時 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際はInt ンターネット ⇒「ファイ川 サイプ THREAT THREAT	emetExplorerにて オプションJ ⇒ F のダウンロードJ 適信元アドレス 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」→設当 の項目で「有効にする 違信先アドレス 210.150.178.115 210.150.178.115	<ださい。 するソーンで 」を選択し、 1 ポリシー名 、 Ping Ping	を選択⇒「レペリ 「OK」をクリ アプリケーション msrpc msrpc	しの力スタマイ ック ン適信元ゾーン Untrust_3 Untrust_3	ズ」をクリッ 適信先ゾーン Trust_3 Trust_3	ク 適信元ポー1 1846 1846	▶ 通信先ボー 139 139	ト アクション reset-s reset-s
コミットステータス確認 ロールバック ログモニタリング 部队してください 部队してください。 マ バスワード管理	は美国 タウンロート名 1. 「ソール」⇒「イ 2. 「タウンロード」: 日時 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際はInt ンターネット ⇒「ファイル THREAT THREAT THREAT	emetExploreにで オプション」⇒ F のダウンロード」 通信元アドレス 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」→設当 の項目で「有効にする 違信先アドレス 210.150.178.115 210.150.178.115 210.150.178.115	(ださい。 するソーン・ するソーン・ 」を選択し、 1 ポリシー名。 Ping Ping Ping Ping	を選択⇒「レペリ 、「OK」をクリ アプリケーショ) msrpc msrpc msrpc	レのカスタマイ ック ン適信元ソーン Untrust_3 Untrust_3 Untrust_3	ズ」をクリッ 適信先ソーン Trust_3 Trust_3 Trust_3	ク 通信元ポー1 1846 1846 1846	・運信先ボー 139 139 139	トアクション reset-s reset-s reset-s
コミットステータス確認 ロールバック ログモニタリング 閉ルしてください 部ルしてください。 ・ バスワード管理 バスワード変更	は登録」ダウンロート名 1. 「ゾール」⇒「イ 2. 「ダウンロード]: 日時 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際はInt ンターネット ⇒「ファイパ THREAT THREAT THREAT THREAT	emetExplorent て オプション」⇒ Г 20ダウンロード」 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティJ ⇒該当 の項目で「有効にする 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	ください。 するソーンで する する ジーンで り を選択し、 1 ポリシー名、 Ping Ping Ping Ping	を選択⇒「レペリ 「OK」をクリ アプリケーショ: msrpc msrpc msrpc	レのカスタマイ ック ン適信元ゾーン Untrust_3 Untrust_3 Untrust_3 Untrust_3	ズ」をクリッ 適信先ソーン Trust_3 Trust_3 Trust_3 Trust_3	ク 通信元ポート 1846 1846 1846 1846	・通信先ボー 139 139 139 139	トアクション reset-s reset-s reset-s reset-s
コミットステータス確認 ロールバック ログモニタリング 朝知してください レポート開覧 朝知してください。 マ バスワード管理 バスワード変更	は美別 タウンロート名 1. 「ツール」⇒「イ 2. 「タウンロート日」 日時 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際はIntr ンターネット ⇒「ファイパ THREAT THREAT THREAT THREAT THREAT	remetExplorentこで オプション」⇒「 のダウンロード」 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」→設当 の項目で「有効にする 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	にさい。 (たさい。 するソーンは 」を選択し、 1 ポリシー名、 Ping Ping Ping Ping Ping	を選択 ドレベリ 「OK」をクリ アプリケーション msrpc msrpc msrpc msrpc	レのカスタマイ ック ジ海信元ゾーン Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3	道信先ソーン Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3	ク 連信元ポー1 1846 1846 1846 1846 1846 4885	▶ 適信先ポー 139 139 139 139 139 139	reset-s reset-s reset-s reset-s reset-s alert
コミットステータス確認 ロールバック ログモニタリング 朝知してください 9 レボート開覧 朝知してください。9 バスワード管理 バスワード管理 コンフィグ管理 コンフィグ管理 コンフィグダウンロード	は美国 タウシロート名 1. 「ソール」⇒「イ 2. 「タウンロート日」 日時 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:08:38 2013/04/10 17:08:38	行う際はIntr ンターネット ⇒「ファイバ サイズ THREAT THREAT THREAT THREAT THREAT THREAT	remetExplorentにて オプション」 = 「 のダウンロード」 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」→設当 の項目で「有効にする 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	にさい。 するソーン・ 」を選択し、 1 ポリシー名 Ping Ping Ping Ping Ping Ping	を選択 テ 「レベリ 「OK」をクリ アプリケーション msrpc msrpc msrpc msrpc msrpc msrpc	レのカスタマイ ック ン連信元ソーン Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3	ス」をクリッ 適信先ソーン Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3	ク 連病元ポー1 1846 1846 1846 1846 4885 4885	 通信先求一 139 139 139 139 139 139 139 139 139 	reset-s reset-s reset-s reset-s reset-s alert reset-s

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 +

9 °	
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

IグインID: of11974	Top » ログモニタリング ×	IPS/IDSD	グ								
+-1	IPS/IDSU/										
<u>"-д</u>	» ログ検索 検索する										
アイアウォール設定											
ドリシー設定	表示件数: 20 🗾 検	索キーワート	S : [(検索対象	: 🗆 通信元	アドレス 🗆 通	冒先アドレス	□通信元ポー	トロ通信先	ポートロア	プリケージ
オブジェクト設定	対象期間:		~	(例: 201	1/05/01)						
Rしてください 💽			-								
コミット	» ログダウンロード 9	774-194	> ※検索キーワ	ードにかかわらず、指	定した対象	期間内のすべての)ログをダウン	ロードします。			
コミットステータス確認	【注意】ダウンロードを	行う際はIn	ternetExplorerCC	に以下の設定を行って	ください。						
ロールバック	 「ヅール」⇒「イ 「ガウンワード」 	ンターネット	>オプション」⇒「	セキュリティ」⇒該当	するソーン	を選択⇒「レベ」	しのカスタマイ	ズ」をクリッ	ク		
	E				2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	10/ 2/71	331 17				
	and the second second second		NJ J J L 13	の項目に「有効にする	日を進択し	、10K」をクリ	ック				
デモニタリング				の項目で「有効にする	1	、 10KJ をクリ	ック				
デモニタリング してください	日時	タイプ	通信元アドレス	通信先アドレス	5」を選択し 1 ポリシー名	、 TOK」をクリ (アプリケーショ)	ック ン通信元ゾーン	通信先ゾーン	通信元术一十	→通信先ボー	トアクショ
デモニタリング してください ・ ドート開覧	日時 2013/04/10 17:09:33	ອາງ Threat	通信元アドレス 61.250.176.20	辺境目で「有効にする 通信先アドレス 210.150.178.115	5] を選択し 1 ボリシー名 Ping	、 10KJ をクリ アプリケーショ) msrpc	ック ン通信元ゾーン Untrust_3	通信先ゾーン Trust_3	通信元ポー↑ 1846	→通信先ボー 139	トアクショ reset-
Fモニタリング してください ・ ベート閲覧 してください。 ・	日時 2013/04/10 17:09:33 2013/04/10 17:09:33	ອາງ THREAT	 適信元アドレス 61.250.176.20 61.250.176.20 	通信先アドレス 210.150.178.115 210.150.178.115	」を選択し 1 ポリシー名 Ping Ping	、 TOKJ をクリ (アプリケーショ) msrpc msrpc	ック ン通信元ゾーン Untrust_3 Untrust_3	適信先ゾーン Trust_3 Trust_3	通信元ポー↑ 1846 1846	→通信先ボー 139 139	トアクショ reset・ reset
ドモニタリング してください 💌 ドート開覧 してください。 💌	日時 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33	タイプ THREAT THREAT	通信元アドレス 61.250.176.20 61.250.176.20 61.250.176.20	通信先アドレス 210.150.178.115 210.150.178.115 210.150.178.115	」を選択し 1 ポリシー名 Ping Ping Ping	、TOKJ をクリ アプリケーショ) msrpc msrpc	ック ン適信元ゾーン Untrust_3 Untrust_3 Untrust_3	通信先ソーン Trust_3 Trust_3 Trust_3	通信元术— 1846 1846	>通信先ボー 139 139 139	reset
ゲモニタリング してください ▼ に一ト閲覧 してください。 ▼ スワード管理	日時 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33	タイプ THREAT THREAT THREAT	通信元アドレス 61.250.176.20 61.250.176.20 61.250.176.20	通信先アドレス 210.150.178.115 210.150.178.115 210.150.178.115	」を選択し I ポリシー名 Ping Ping Ping	、TOKJ をクリ アプリケーショ) msrpc msrpc msrpc	ック ン通信元ソーン Untrust_3 Untrust_3 Untrust_3	通信先ソーン Trust_3 Trust_3 Trust_3	適信元ポート 1846 1846 1846	- <mark>通信先ボー</mark> 139 139 139	トアクショ reset reset
ゲモニタリング してください ■ ドート開覧 してください。 ■ Kワード管理 ベスワード変更	EB6 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33	タイプ THREAT THREAT THREAT THREAT	週信元アドレス 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	通信先アドレス 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	」を選択し 1 ポリシー名 Ping Ping Ping Ping	、TOKJ をクリ スプリケーショ、 msrpc msrpc msrpc msrpc	ック ン適信元ソーン Untrust_3 Untrust_3 Untrust_3 Untrust_3	<mark>適信先ソーン</mark> Trust_3 Trust_3 Trust_3 Trust_3	適信元ポート 1846 1846 1846 1846	·通信先术— 139 139 139 139	reset- reset- reset- reset-
アモニタリング してください ■ ドート開覧 してください。■ スワード管理 ベスワード変更	EB6 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:08:38	タイプ THREAT THREAT THREAT THREAT THREAT	週信元アドレス 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	通信先アドレス 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	I ボリシー名 Ping Ping Ping Ping Ping Ping	、TOKJ をクリ msrpc msrpc msrpc msrpc msrpc msrpc	ック ン通信元ゾーン Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3	適信先ソーン Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3	道信元ポート 1846 1846 1846 1846 4885	通信先ボー 139 139 139 139 139 139	トアクショ reset- reset- reset- reset- alert
アモニタリング してください ・ ドート開覧 してください。 ・ スワード管理 ・ バスワード変更 ・ フィグ管理 コンフィグダウンロード	EB6 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:08:38 2013/04/10 17:08:38	947 THREAT THREAT THREAT THREAT THREAT	週信元アドレス 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	通信先アドレス 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	I ポリシー名 Ping Ping Ping Ping Ping Ping Ping	TOKJ をクリ ToKJ をクリ msrpc msrpc msrpc msrpc msrpc msrpc msrpc msrpc msrpc	ック シ連信元ソーン Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3	適信先ソーン Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3	通信元术一十 1846 1846 1846 1846 4885 4885	·通信先求一 139 139 139 139 139 139	トアクショ reset reset reset reset alert
ゲモニタリング RUTください ■ ボート開覧 RUTください。 ■ スワード管理 バスワード変更 ンフィグ管理 コンフィグダウンロード	EB6 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:08:38 2013/04/10 17:08:38 2013/04/10 17:08:38	917 THREAT THREAT THREAT THREAT THREAT THREAT	通信元アドレス 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	道信先アドレス 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	1 ポリシー名 Ping Ping Ping Ping Ping Ping Ping Ping	TOKJ をクリ	ック 連信元ゾーン Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3	遺伝先ソーン Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3	通信元术一十 1846 1846 1846 1846 4885 4885 4885	·通信先术— 139 139 139 139 139 139	トアクショ reset reset reset alert reset

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

ログインID: of11974	Top » ログモニタリング »	スパイウェ	アチェックログ								
ログアウト	スパイウェアチュ	wクロ	ブ								
ホーム											
ファイアウォール設定	»ログ検索 検索する										
ポリシー設定	表示件数: 20 💌 検	索キーワート	S :	(検索対象	: 🗋 通信元)	アドレス 🗆 通	言先アドレス	□ 通信元ボー	ト 🗖 通信先	ポート ロフ	プリケー
オブジェクト設定	ヨン) 対象期間:		~	(例: 201	1/05/01)						
択してください 📃											
コミット	» ログダウンロード	フンロードする	5 ※検索キーワ・	ードにかかわらず、措	定した対象関	間間内のすべての	ログをダウン	ロードします。			
	the state of the s										
227 - 7 7 - 7 7 9122	【注意】ダウンロードを	:行う際(dIn	ternetExplorerにて	以下の設定を行って	ください。						
ロールバック	【注意】ダウンロードを 1、「ツール」⇒「イ」 2、「ダウンロードと	:行う際はIn ンターネット	ternetExplorerにて トオブション」⇒「	:以下の設定を行って。 セキュリティ」⇒該当	ください。 するソーン	を選択⇒「レベ」	しのカスタマイ	ズ」をクリッ	þ		
ロールバック	【注意】ダウンロードを 1、「ツール」⇒「イ 2、「ダウンロード」=	「行う際はIn ンターネット ⇒「ファイ)	ternetExplorerにて トオプション」⇒「 レのダウンロード」	:以下の設定を行って。 セキュリティ」⇒該当 の項目で「有効にする	ください。 行るソーン 」を選択し、	を選択⇒「レベ」 「OK」をクリ	しのカスタマイ ック	ズ」をクリッ	0		
コミットステータス構成 ロールバック	【注意】ダウンロードを 1、「ツール」⇒「イ 2、「ダウンロード」=	:行う際(dIn ンターネット ⇒「ファイ)	ternetExplorerにて トオブション」⇒「 レのダウンロード」。	:以下の設定を行って・ セキュリティ」⇒該当 の項目で「有効にする	ください。 約するゾーン・ い」を選択し、 1	を選択⇒「レベ」 「OK」をクリ	しのカスタマイ ック	ズ」をクリッ	þ		
ユミットステージス構成 ロールバック がモニタリング RUTで(ださい) ・	(注意) ダウンロードを 1. 「ツール」⇒「イ 2. 「ダウンロード」= 日時	行う際(din ンターネッ) ⇒「ファイ) タイプ	ternetExplorerにて トオプション」⇒「 しのダウンロード」。 適信元アドレス	以下の設定を行って。 セキュリティ」⇒該当 の項目で「有効にする 通信先アドレス	ください。 (するソーン!)」を選択し、 1 ポリシー名)	2選択⇒「レペ」 「OK」をクリ アプリケーション	しのカスタマイ ック ン連信元ゾーン	ズ」をクリッ・	ク 通信元ポート	、通信先术一	トアクショ
ロールバック ログモニタリング IRUでください マ ・ボート開覧	(注意) ダウンロードを 1. 「ツール」⇒「イ、 2. 「ダウンロード」・ 日時 2013/04/10 17:09:33	行う際はIn ンターネット ⇒「ファイ) タイプ THREAT	ternetExplorerにて トオプション」⇒ F しのダウンロード」 通信元アドレス 61.250.176.20	以下の設定を行って。 セキュリティ」⇒該当 の項目で「有効にする 通信先アドレス 210.150.178.115	ください。 第するソーン1 」を選択し、 1 ポリシー名。 Ping	を選択⇒「レベル 「OK」をクリ アプリケーション msrpc	いのカスタマイ ック ン連信元ゾーン Untrust_3	ズ」をクリッ ・通信先ゾーン Trust_3	ク 通信元ポート 1845	▶ <mark>通信先ボー</mark> 139	トアクシ: reset
ロールバック ログモニタリング RUてください マ ポート開覧 RUTください。 マ	(注意) ダウンロードを 1. 「ツール」⇒「イ」 2. 「ダウンロード」= 日時 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際はIn ンターネット ⇒「ファイ) サイプ THREAT THREAT	ternetExplorerにて トオプション」 ⇒ F しのダウンロード」 4 適信元アドレス 61.250.176.20 61.250.176.20	(以下の設定を行って、 セキュリティ」 ⇒ 該当 の項目で「有効にする 適信先アドレス 210.150.178.115 210.150.178.115	ください。 約3るソーン1 1 を選択し、 1 ポリシー名。 Ping Ping	E運択⇒「レペリ 「OK」をクリ アプリケーション msrpc msrpc	Lのカスタマイ ック ン通信元ゾーン Untrust_3 Untrust_3	ズ」をクリッ ・通信先ゾーン Trust_3 Trust_3	ク 通信元ポート 1846 1846	▲信先术一 139 139	トアクショ reset reset
ロールバック ログモニタリング 見してください ボート開覧 見してください。 マ スワード管理	(注意) ダウンロードを 1. 「ツール」⇒「イ) 2. 「ダウンロード」= 日時 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際はIn ンターネット ⇒「ファイ) サイプ THREAT THREAT THREAT	temetExplorerにて オプション」→ F しのダウンロード」 適信元アドレス 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」 ⇒級当 の項目で「有効にする 連信先アドレス 210.150.178.115 210.150.178.115 210.150.178.115	ください。 するソーン うを選択し、 1 ポリシー名: Ping Ping Ping	と準択⇒「レペリ 「OK」をクリ アプリケーション msrpc msrpc msrpc	レのカスタマイ ック ン連信元ソーン Untrust_3 Untrust_3 Untrust_3	ズ」をクリッ [・] 通信先ゾーン Trust_3 Trust_3 Trust_3	ク 通信元ポート 1846 1846 1846	ン通信先ボー 139 139 139	F70>: reset reset reset
コニッドハナー・入業に ロールバック グモニタリング RUてください。 マ メート問覧 RUてください。 マ スワード管理 バスワード変更	(注意) ダウンロードを 1. 「ツール」⇒「イ」 2. 「ダウンロード」= 日時 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際(stn ンターネット ⇒「ファイ) サートファイ) THREAT THREAT THREAT THREAT	ternetExplorerにて オプションJ ⇒ F しのダウンロードJ d 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行ってく セキュリティ」 = 該当 の項目で「有効にする 違信先アドレス 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	ください。 ダオるソーン・ オ オ ボリシー名、 Ping Ping Ping Ping	と選択⇒「レベリ 「OK」をクリ アプリケーション msrpc msrpc msrpc	レのカスタマイ ック ン連信元ソーン Untrust_3 Untrust_3 Untrust_3 Untrust_3	ズ」をクリッ ・適信先ソーン Trust_3 Trust_3 Trust_3 Trust_3	ク 通信元ポート 1846 1846 1846 1846	>通信先求一 139 139 139 139 139	reset reset reset reset
ロールバック グモニタリング RUてください ボート開覧 RUてください。 マ スワード管理 バスワード変更 ンフィグ管理	(注意) ダウンロードを 1. 「ツール」⇒「イ」 2. 「ダウンロード」= 日時 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:08:38	行う際はIII ンターネット ⇒「ファイ) THREAT THREAT THREAT THREAT THREAT	ternetExplorerにて オプションJ ⇒ F しのダウンロードJ d 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」 ⇒ 該当 の項目で「有効にする 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	ください。 (するソーン・) を選択し、 1 米リシー名: Ping Ping Ping Ping Ping	を選択⇒「レペリ TOK」をクリ アプリケーショ: msrpc msrpc msrpc msrpc msrpc	いのカスタマイ ック シ連信元ソーン Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3	ズ」をクリッ 「猫信先ソーン Trust_3 Trust_3 Trust_3 Trust_3 Trust_3	2 通信元术一 1846 1846 1846 1846 1846 4885	· 通信先术	トアクシ: reset reset reset reset aleri
コンフィグダウンロード コンフィグダウンロード コンフィグダウンロード	(注意) ダウンロードを 1. 「ツール」⇒「イ) 2. 「ダウンロード」 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:08:38 2013/04/10 17:08:38	行う隙(din ンターネット ⇒「ファイ) サー「ファイ) THREAT THREAT THREAT THREAT THREAT	temetExplorerにて オプション」→ F しのダウンロード」 4 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」 ⇒該当 の項目で「有効にする 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	ください。 するソーン・ するソーン・ する 単語の 単語の 単語の 単語の 単語の 単語の 単語の	を選択⇒「レベリ 「OK」をクリ アプリケーション msrpc msrpc msrpc msrpc msrpc msrpc	レのカスタマイ ック シン連合元ソーン Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3	ス」をクリッ 適信先ソーン Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3	2 通信元水一 1846 1846 1846 1846 4885 4885	 連信先ボー 139 139 139 139 139 139 139 139 139 	トアクショ reset reset reset aler reset

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

コグインID: of11974	Top » ログモニタリング »	スパイウェ	アチェックログ								
ログアウト	フパイウェアチョ		M								
ホーム	X/(1)1/)1										
ファイアウォール設定	»ログ検索 検索する										
ポリシー設定	表示件数: 20 💌 検	常キーワート	S :	(検索対象	: □ 通信元:	アドレス 🗆 通	信先アドレス	□ 通信元ボー	トロ通信先	ボートロア	プリケー
オブジェクト設定	ヨン) of Spitter F		~	(81-201	1/05/01)						
見してください 💽	vissoniei - I		1	(10). 201	.1/05/01)						
コミット	» ログダウンロードダ	ウンロードする	る ※検索キーワ	ードにかかわらず、指	定した対象関	期間内のすべての	ロログをダウン	ロードします。	e e e e e e e e e e e e e e e e e e e		
127 FX7-9 X988	【注意】ダウンロードを	行う際(dIn	ternetExplorer(CT	以下の設定を行って	ください。						
ロールバック	【注意】ダウンロードを 1.「ツール」⇒「イ 2.「ダウンロード」	行う際はIn ンターネット	ternetExplorerにて トオプション」⇒「	に以下の設定を行って。 セキュリティ」⇒該当 のほうで「ちかにする	ください。 するソーン	を選択⇒「レベ」	しのカスタマイ	ズ」をクリッ	þ		
ロールバック	【注意】ダウンロードを 1、「ツール」⇒「イ」 2、「ダウンロード」:	行う際(dIn ンターネット ⇒「ファイ)	ternetExplorerにて トオプション」⇒「 レのダウンロード」	に以下の設定を行って。 セキュリティ」⇒該当 の項目で「有効にする	ください。 (するゾーン) 」を選択し、	を選択⇒「レベ」 「OK」をクリ	レのカスタマイ ック	ズ」をクリッ	þ		
コミッドステージス構成 ロールバック グモニタリング	【注意】ダウンロードを 1、「ゾール」⇒「イ 2、「ダウンロード」。	行う際(din ンターネット ⇒「ファイ)	ternetExplorerにて トオプション」⇒「 しのダウンロード」	に以下の設定を行って・ セキュリティ」⇒該当 の項目で「有効にする	ください。 対るソーン 」を選択し、 1	を選択⇒「レベ」 「OK」をクリ	レのカスタマイ ック	ズ」をクリッ	þ		
ロールバック グモニタリング れてください	(注意) ダウンロードを 1. 「ツール」⇒「イ 2. 「ダウンロード」= 日時	行う際(din ンターネッ† ⇒「ファイ) タイプ	ternetExplorerにて トオプション」⇒「 しのダウンロード」 通信元アドレス	に以下の設定を行って。 セキュリティ」⇒該当 の項目で「有効にする 通信先アドレス	ください。 (するゾーン! 」を選択し、 1 ポリシー名。	を選択⇒「レベ」 「OK」をクリ アプリケーショ	しのカスタマイ ック ン連信元ゾーン	ズ」をクリッ 通信先ゾーン	ク 通信元ポー	→通信先ボー	トアクショ
ロールバック グモニタリング れてください 。	(注意) ダウンロードを 1. 「ツール」⇒「イ、 2. 「ダウンロード」・ 日時 2013/04/10 17:09:33	行う際はIn ンターネット ⇒「ファイ) タイプ THREAT	ternetExplorerにて トオプション」⇒「 レのダウンロード」 通信元アドレス 61.250.176.20	は下の設定を行ってく セキュリティ」⇒該当 の項目で「有効にする 通信先アドレス 210.150.178.115	ください。 約7るソーン・ 1 を選択し、 1 ポリシー名 : Ping	を選択⇒「レベル 「OK」をクリ アプリケーショ msrpc	レのカスタマイ ック ン連信元ゾーン Untrust_3	ズ」をクリッ [•] 通信先ゾーン Trust_3	ク 通信元ポー1 1846	、通信先ボー 139	ト アクシ : reset
ロールバック ヴモニタリング れてください ボート開催 れてください。 単	(注意) ダウンロードを 1. 「ツール」⇒「イ」 2. 「ダウンロード」= 日時 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際はIn ンターネット ⇒「ファイ) サイプ THREAT THREAT	ternetExplorerにて トオプションJ ⇒ F レのダウンロードJ 適信元アドレス 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」 ⇒ 該当 の項目で「有効にする 追信先アドレス 210.150.178.115 210.150.178.115	ください。 ぼするソーン・ し を選択し、 1 ポリシー名。 Ping Ping	を選択⇒「レペ」 「OK」をクリ アプリケーショ: msrpc msrpc	レのカスタマイ ック ン運信元ソーン Untrust_3 Untrust_3	ズ」をクリッ 通信先ゾーン Trust_3 Trust_3	ク 通信元ポート 1846 1846	・運信先ボー 139 139	トアクシ reset reset
コミット・ハー・スイロシ ロールバック グモニタリング むてください マ ボート開覧 むてください。 マ スワード管理	(注意) ダウンロードを 1. 「ツール」⇒「イ」 2. 「ダウンロード」= EI時 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際はIn ンターネット ⇒「ファイ) サイプ THREAT THREAT THREAT	ternetExplorerにて トオプション」→「 しのダウンロード」 適信元アドレス 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」 ⇒ 該当 の項目で「有効にする 210.150.178.115 210.150.178.115 210.150.178.115	ください。 (するソーン) うを選択し、 1 ポリシー名。 Ping Ping Ping	を選択⇒「レペ」 「OK」をクリ アプリケーショ: msrpc msrpc msrpc	レのカスタマイ ック ン連信元ソーン Untrust_3 Untrust_3 Untrust_3	ズ」をクリッ ² 通信先ゾーン Trust_3 Trust_3 Trust_3	ク 通信元ポー1 1846 1846 1846	▶ 通信先术 — 139 139 139	reset reset
ロールバック ウモニタリング むてください ▼ ボート開覧 むてください。 ▼ なスワード管理 バスワード変更	(注意) ダウンロードを 1. 「ツール」⇒「イ」 2. 「ダウンロード」 日時 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際(はIn ンターネット ⇒「ファイ) THREAT THREAT THREAT THREAT	ternetExplorerにて トオプションJ ⇒ 「 しのダウンロード」 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」 ⇒ 該当 の項目で「有効にする 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	ください。 なするソーン・ 」を選択し、 1 ボリシー名、 Ping Ping Ping Ping	を選択⇒「レペ」 「OK」をクリ アプリケーショ msrpc msrpc msrpc	レのカスタマイ ック ン運信元ゾーン Untrust_3 Untrust_3 Untrust_3 Untrust_3	ズ」をクリッ 通信先ソーン Trust_3 Trust_3 Trust_3 Trust_3	ク 通信元ポート 1846 1846 1846 1846	通信先ボー 139 139 139 139	reset reset reset reset
ユミナドメテーナス構築 ロールバック グモニタリング れてください ▼ ボート開覧 れてください。 ▼ スワード管理 パスワード変更 シフィグ等理	C注意)ダウンロードを 1. 「ツール」⇒「イ」 2. 「ダウンロード」= 日時 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際(dIn ンターネット =「ファイ) THREAT THREAT THREAT THREAT THREAT THREAT	ternetExplorerにて トオプション」→「 しのダウンロード」 信1.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」 ⇒該当 の項目で「有効にする 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	ください。 するソーン・ する選択し、 1 米リシー名: Ping Ping Ping Ping Ping	を選択⇒「レベリ 「OK」をクリ アプリケーショ msrpc msrpc msrpc msrpc msrpc	レのカスタマイ ック ン連信元ソーン Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3	ズ」をクリッ 酒信先ソーン Trust_3 Trust_3 Trust_3 Trust_3 Trust_3	ク 連信元ポー 1846 1846 1846 1846 1846 4885	· 遵信先术 139 139 139 139 139	トアクショ reset reset reset reset aleri
ロールバック グモニタリング RUてください ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	日本 ダウンロードを 1. 「ツール」⇒「イ」 2. 「ダウンロード」 日本 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33 2013/04/10 17:09:33	行う際(dIn ンターネット ⇒「ファイ) サート THREAT THREAT THREAT THREAT THREAT THREAT	ternetExplorerにて トオプション」→「 ルのダウンロード」 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20 61.250.176.20	以下の設定を行って、 セキュリティ」 ⇒ 録当 の項目で「有効にする 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115 210.150.178.115	ください。 はするソーン・ はずるソーン・ して 単一 が り い り い り の り の の の の の の の の し つ い い い つ い い い い い い い い い い い い い い	を選択⇒「レベリ 「OK」をクリ アプリケーショ: msrpc msrpc msrpc msrpc msrpc	レのカスタマイ ック ン連信元ソーン Untrust_3 Untrust_3 Untrust_3 Untrust_3 Untrust_3	ズJ をクリッ 適信先ソーン Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3 Trust_3	ク 通信元ポー1 1846 1846 1846 1846 4885 4885	· 遵信先术 139 139 139 139 139 139	トアウシ reset reset reset reset aler reset

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。

ログインID: test002	Top » レポート	間覧 » アプリケーション(期間指定)			
ホーム	- 7703				
ファイアウォール設定	Last Hour	 ・レポート取得対象を選択してください。 			
ポリシー設定	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
オブジェクト設定	4	web-browsing	187	2,215,962	0
選択してください	.4	dns	85	13,633	0
コミット	4	ssl	12	144,968	0
コミットステータス確認	4	facebook-base	7	124,838	0
ロールバック	2	snmp-base	6	2,142	0
ログモニタリング	2	twitter-base	5	41,963	0
選択してください	4	yahoo-douga	2	2,091,504	0
レポート開覧	:3	facebook-social-plugin	2	15,750	0
選択してください。 ・ 選択してください。	4	icmp	1	70	0
アプリケーション(日単位) 通信元アドレス	4	flash	1	304,138	0
週間ホイドレス 通信先トラフィック(国毎) 攻撃トラフィック	3	google-update	1	2,384	0
コンフィグ管理	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。

Customer Contr	rol System			
ログインID: test002	Top » レポート閲覧 » アブリケーション(日単位) アプリケーション(日単位)			
ホーム	- アプリケーションごとのアクセス数集計(上位50件)			
ファイアウォール設定	2013/01/13 : レポート取得対象を選択してください。			
ポリシー設定	アプリケーション	リスク	転送量	セッション数
オブジェクト設定	web-browsing	4	32,009,064	3,156
「選択してください	dns	4	50,187	290
コミット	Facebook-social-plugin	3	1,532,531	73
コミットステータス確認	http-video	5	112,902,689	49
ロールバック	snmp-base	2	13,926	39
ログモニタリング	ms-update	4	1,596,306	35
選択してください	facebook-base	4	256,661	30
レボート閲覧	ssl	4	187,296	18
選択してくたさい。 選択してくたさい。 アプリケードはいば期間指定)	flash	4	3,797,882	11
アラリケーション(日単位) 通信元アドレス	youtube-base	5	31,264,131	5
通信先トラフィック(国毎) 攻撃トラフィック	google-analytics	2	32,218	2
コンフィグ管理	silverlight	2	484,876	2
コンフィクタウンロード	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。

1グインID: test002	Top » レポート閲覧 » 通信元アド	レス			
ログアウト	通信元アドレス				
ホーム	- 通信元アドレスごとのアク	セス集計(上位50件)			
ファイアウォール設定	2013/01/13 • : レボート取得対象	象を選択してください。			
ポリシー設定	運信元アドレス	通信元(ホスト名)	通信元ユーザ	転送量	セッション数
オブジェクト設定	10.0.0.10	10.0.0.10		183,521,794	3,683
選択してください	10.0.0.12	10.0.0.12		614,782	29
コミット					
コミットステータス確認					
ロールバック					
ログモニタリング	1				
選択してください 💽					
レポート閲覧					
留訳してください。 留訳してください。 アグリケーション(期間指定) アグリケーション(相単位) 第6元アドレス 都信先アドレス 第6年たラフム・ク(同業)					
2撃トラフィック					

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。

Customer Contr	ol System				
ログインID: test002 ログアウト	Top » レポート閲覧 » 通信先アドレス 通信先アドレス				
ホーム	- 通信先アドレスごとのアクセス集	計(上位50件)			
ファイアウォール設定	2013/01/13 :レポート取得対象を選択	Rしてください。			
ポリシー設定	遵信先アドレス	適信先(ホスト名)	通信先ユーザ	転送量(byte)	セッション数
オブジェクト設定	138.108.7.20	138.108.7.20		1,655,536	786
選択してください 💽	66.235.138.18	66.235.138.18		1,637,988	405
コミット	8.8.8.8	8.8.8		50,187	290
コミットステータス確認	65.55.84.48	65.55,84.48		317,192	136
ロールバック	65.55.249.87	65.55.249.87		243,700	136
ログモニタリング	23.59.14.98	23.59.14.98		230,838	89
訳してください	207.46.70.198	207.46.70.198		2,049,032	77
レポート開覧	64.4.21.39	64.4.21.39		156,422	71
観してください。 観してください。	65.55.5.232	65.55.5.232		343,155	66
ブリケーション(日単位) ブリケーション(日単位) 信元アドレス	65.55.239.146	65.55.239.146		152,025	65
信先トラフィック(国毎) 撃トラフィック	111.221.21.78	111.221.21.78		127,263	63
コンフィグ管理	72.246.189.226	72.246.189.226		112,131	56
コンフィグダウンロード	72,246,189,241	72.246.189.241		174,338	55
	65.55.17.225	65.55.17.225		1,718,303	52

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。

ログアウト	Top » レポート閲覧 » 通信先トラフィック(国毎) 通信先トラフィック(国毎)		
ホーム	- トラフィックの宛先の国ごとのアクセス集計(上位50件)		
7ァイアウォール設定	2013/01/13 : レボート取得対象を選択してください。		
ポリシー設定	通信先	転送量	セッション数
オブジェクト設定	United States	148,770,499	3,417
訳してください	Singapore	502,693	205
コミット	Japan	34,849,458	51
コミットステータス確認	192,168.0.0-192,168,255,255	13,926	39
aゲモニタリング 扱してください ・ボート開覧 扱してください。 取してください。 ア クノケーション(相単位) 音大アドレス 音大アドレス 音大アドレス 音大アドレス 音大アドレス 音大アドレス 音大アトレス 音大アトレス			
増先アドレス 高先トラフィック(国毎) 撃トラフィック			

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。

ログインID: test002	Top » レポート開覧 »	攻撃トラフィック			
ログアウト	攻撃トラフィッ	ク			
ホーム	- 攻撃トラフィッ	クを送信したスレットの集計(上位50件)			
ファイアウォール設定	2018/07/12 ン:レポー	ト取得対象を選択してください。			
ポリシー設定	リスク	ZLyhid	tid	タイプ	回数
オプジェクト設定	high	HTTP /etc/passwd access attempt	35,107	vulnerability	20
選択してください・	critical	Microsoft IIS WebDAV ScStoragePathFromUrl Buffer Overflow Vulnerability	30,464	vulnerability	2
コミット	high	Oracle WebLogic WLS Security Component Remote Code Execution Vulnerability	38,865	vulnerability	1
ロールバック					

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。

コグインID: gja2550	Top » バスワード管理 » バスワード室	2 更
ログアウト ホーム	パスワード変更	
ファイアウォール設定	ログイン ID	Recum
ポリシー設定	ファイアウォールID	And Liperintited
オブジェクト設定	現在のバスワード	
薯択してください	変更後のパスワード	
コミット	変更後のパスワード(再入力)	
コミットステータス確認		-
ログモニタリング 射沢してください	OK Clear	
レポート開覧 翻訳してください。 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・		
パスワード変更		
コンフィグ管理		

(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	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
変更後のパスワード(再入力)	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。

Customer Control System		
ログインID: test002 ログアウト ホーム	Top » コンフィグ管理 » コンフィグダウンロード FWコンフィグ設定ダウンロード	
ボリシー設定 オブジェクト設定 「選択してください 。 コミット コミットステータス確認 ロールバック 「ログモニタリング 「選択してください 。 「レボート開覧 「選択してください。 」 パスワード管理 パスワード管理 コンフィグ管理 コンフィグ学理	> FWコンフィグ設定ダウンロード ダウンロードする *FW設定をダウンロードします。 「注意】ダウンロードを行う際はInternetExplorerにて以下の設定を行ってください。 1. 「ツール」⇒「インターネットオブション」⇒「ビキュリティ」=認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」の項目で「有効にする」を選択し、「OK」をクリック	

(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。