HITACHI
Inspire the Next

ファイアウォールログ解析ソフトウェア

FIREWALLstaff

取扱説明書（基本機能編）

株式会社 日立ソリューションズ

■ 対象製品

FIREWALLstaff 02-08

■ 輸出時の注意

本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。

なお，ご不明な場合は，弊社または弊社販売店の担当窓口へお問い合わせください。

■ 商標類

- Word，Windows，Windows Server は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Microsoft は，米国およびその他の国における米国 Microsoft Corp.の登録商標です。
- NETSCREEN，JUNIPER NETWORKS はそれぞれジュニパーネットワークス社の登録商標です。
- FORTIGATE はフォーティネット社の登録商標です。
- PALO ALTO NETWORKS はパロアルトネットワークス社の商標です。
- チェック・ポイント，VPN-1 UTM は，Check Point Software Technologies Ltd.およびその関連会社の商標，又は登録商標です。
- IPCOM は，富士通株式会社の登録商標です。
- Cisco，Cisco Systems，および Cisco Systems ロゴは，米国 Cisco Systems，Inc. の米国および他の国々における登録商標です。
- FIREWALLstaff は，株式会社日立ソリューションズの登録商標です。
- その他，本マニュアル記載の会社名，製品名は，それぞれの会社の商号，登録商標または商品名称です。

■ 発行

2021 年 12 月

はじめに

このマニュアルは，FIREWALLstaff の使い方について説明したものです。

■ 対象読者

FIREWALLstaff を運用，管理するシステム管理者を対象としています。

このマニュアルの記述は，次の事項を前提にしています。

- Windows の基本操作を習得している。
- コンピュータの管理者として必要な知識がある。
- ネットワークに関する基本的な知識がある。
- セキュリティに関する基本的な知識がある。
- ファイアウォールの設定変更ができる。

■ このマニュアルでの表記

このマニュアルでは製品名称について次のように表記しています。ただし，それぞれの製品についての表記が必要な場合はそのまま表記しています。

製品名称	表記
Juniper NetScreen	NetScreen
Juniper SSG	SSG
Juniper SRX	SRX
Fortinet FortiGate	FortiGate
Palo Alto Networks PA	Palo Alto
CheckPoint Software Blade	CheckPoint
IPCOM EX IN/SC	IPCOM
Cisco ASA	Cisco

■ このマニュアルで使用する略語

このマニュアルで使用する英略語の一覧を次に示します。

英略語	英字の表記
CIDR	Classless Inter-Domain Routing
DMZ	demilitarized zone
FTP	File Transfer Protocol
HTML	HyperText Markup Language
IP	Internet Protocol
IPv4	Internet Protocol version 4
LEA	Log Export API
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TELNET	Telecommunication network
UDP	User Datagram Protocol

■ 画面操作説明で使う表記

画面操作説明で使う表記を次に示します。

記号	意味
[ ]	ボタンやテキストボックスなど，画面に表示されている要素を示します。
[ ] − [ ]	画面に表示されるメニューやアイコンなどを選択する操作を示します。

■ 常用漢字以外の漢字の使用について

このマニュアルでは常用漢字を使用することを基本としていますが，次に示す用語については常用漢字

以外の漢字を使用しています。
鍵（かぎ）　個所（かしょ）　必須（ひっす）

■ MB（メガバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト）はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイトです。

■ 最大文字数表記について

「1 「メイン画面」において「最大 n 文字まで指定できます」という表記は全角文字，半角文字の区別なく n 文字指定できるという意味になります。改行を指定可能な場合，改行文字もカウントします。

目次

1 「メイン画面」の設定

1.1　FIREWALLstaff AE Server のメイン画面

1.1.1　FIREWALLstaff AE Server メイン画面

デスクトップにある FIREWALLstaff AE Server のショートカット，または Windows の[スタート]－[すべてのプログラム]－[FIREWALLstaff]－[FIREWALLstaff AE Server]から FIREWALLstaff AE Server メイン画面を起動してください。

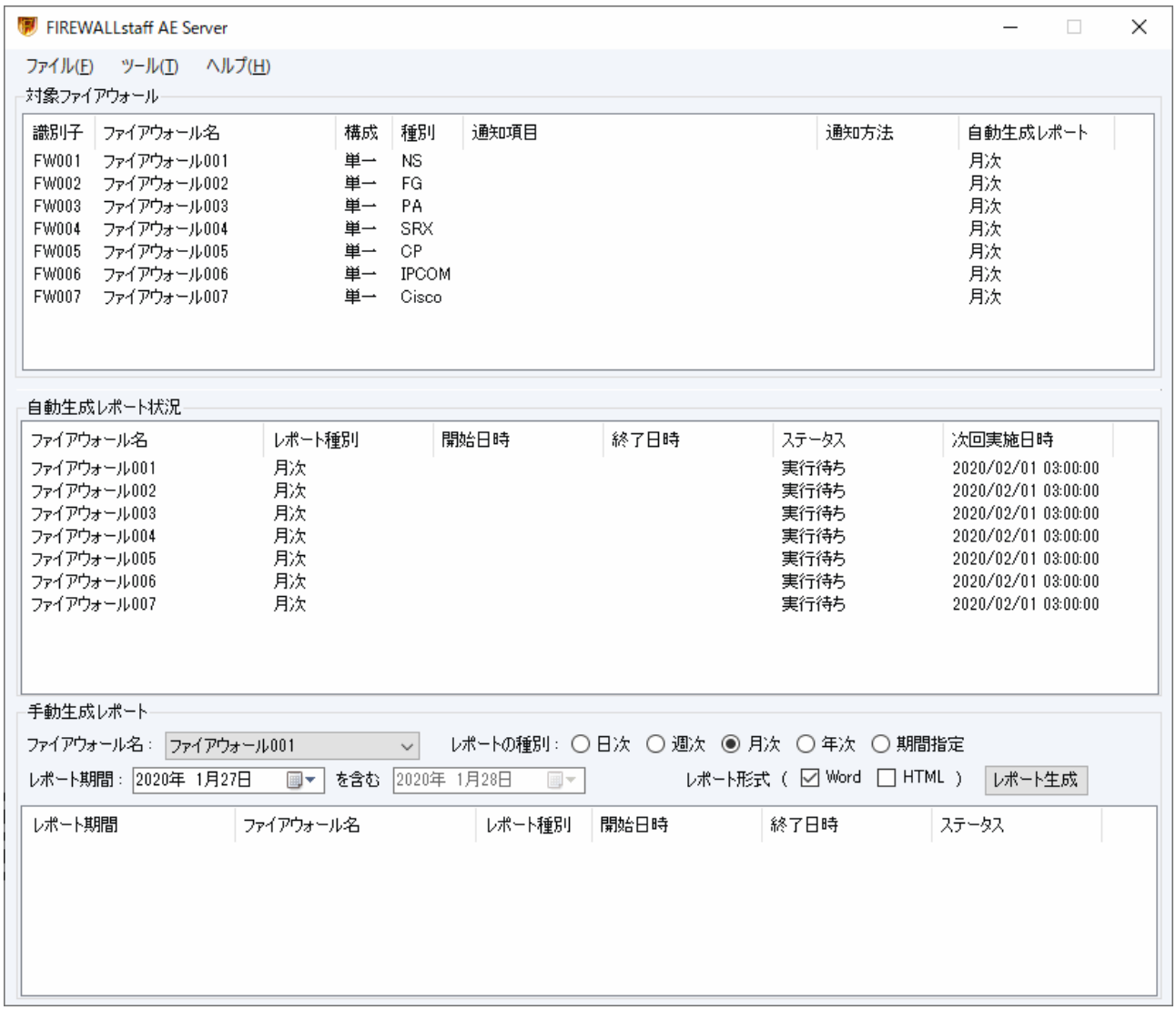


図 1 FIREWALLstaff AE Server メイン画面

(1) [対象ファイアウォール]グループボックス

FIREWALLstaff でレポートを作成するファイアウォールの情報と，定期的に生成するレポートの種類を表示します。

各レコードのことを[プロファイル]と呼びます。

製品ライセンスキーを１つインストールすることで，プロファイルを１つ追加することができます。

(a)［識別子］項目

プロファイル毎にFIREWALLstaffが一意に採番した識別子で，設定変更することはできません。FW001，FW002，FW003，・・・の順に自動採番されます。

(b)［ファイアウォール名］項目

FIREWALLstaff において，プロファイルを識別するための名称です。［ファイアウォールの指定］パネルの［名称］で指定した名称です。

(c)［構成］項目

インストールしたライセンスキーの構成を表示します。

表 1.1-1 [構成]の表示と内容

項番	[構成]の表示	内容
1	単一	・「FIREWALLstaff 対象FW単一構成ライセンス」 がインストールされています
2	冗長	・「FIREWALLstaff 対象FW冗長構成ライセンス」 ・「FIREWALLstaff 対象FW単一構成ライセンス」 ＋「FIREWALLstaff 冗長構成変更ライセンス」 のいずれかがインストールされています

(d)［種別］項目

インストールしたライセンスキーの対応ファイアウォールを表示します。

表 1.1-2 [種別]の表示と内容

項番	[種別]の表示	内容
1	NS	NetScreen/SSG用のライセンスがインストールされています
2	FG	FortiGate用のライセンスがインストールされています
3	PA	Palo Alto用のライセンスがインストールされています
4	SRX	SRX用のライセンスがインストールされています
5	CP	CheckPoint用のライセンスがインストールされています
6	IPCOM	IPCOM用のライセンスがインストールされています
7	Cisco	Cisco用のライセンスがインストールされています

(e)［自動作成レポート］項目

定期的に作成するレポートの種類を表示します。

表 1.1-3 [自動作成レポート]の表示と内容

項番	[自動作成レポート]の表示	内容
1	日次	日次のレポートを作成します
2	週次（月／日曜日始まり）	週次のレポートを作成します
3	月次	月次のレポートを作成します
4	年次	年次のレポートを作成します

(2) [自動生成レポート状況]グループボックス

FIREWALLstaff が定期的に生成するレポートの生成状況を表示します。

ファイアウォール名とレポート種別の組み合わせで，最後に生成したレポートの状況を表示します。

(a) [ファイアウォール名]項目

FIREWALLstaff において，プロファイルを識別するための名称です。

(b) [レポート種別]項目

日次のレポートは[日次]，週次のレポートは[週次（月曜日始まり）]，[週次（日曜日始まり）]，月次のレポートは[月次] ，年次のレポートは[年次]と表示されます。

(c) [開始日時]項目

レポートの生成を開始した日時を表示します。

(d) [終了日時]項目

レポートの生成が終了した日時を示します。

(e) [ステータス]項目

レポートの生成結果を表示します。[成功]または[失敗]のいずれかで，インストール直後は[実行待ち]というステータスになります。

(f) [次回実行日時]項目

レポートが次回生成開始する日時を示します。

(3) [手動生成レポート]グループボックス

手動実行にてレポートを生成することができます。

(a) [ファイアウォール名]コンボボックス

レポートを生成するファイアウォールを選択します。

(b) [日次]ラジオボタン

日次のレポートを生成する場合に選択します。

(c) [週次]ラジオボタン

週次のレポートを生成する場合に選択します。

(d) [月次]ラジオボタン

月次のレポートを生成する場合に選択します。

(e) [年次]ラジオボタン

年次のレポートを生成する場合に選択します。

(f) [期間指定]ラジオボタン

任意の期間を指定したレポートを生成する場合に選択します。

このラジオボタンを選択すると，「(g) [レポート期間]-[開始日付]カレンダリスト」と「(h) [レポート期間]-[終了日付]カレンダリスト」の間のラベルが「を含む」から「から」に切り替わり，「(h) [レポート期間]-[終了日付]カレンダリスト」が活性状態になります。

指定できる期間は，最小 2 日，最大 400 日です。

(g) [レポート期間]-[開始日付]カレンダリスト

レポート期間の左側のカレンダリストを[開始日付]カレンダリストと呼びます。(b)～(e)のラジオボタンを選択している場合は，ここにレポートしたい期間に含まれる日付を指定します。

(f)のラジオボタンを選択している場合は,ここにレポートしたい期間の開始日付を指定します。

(h) [レポート期間]-[終了日付]カレンダリスト

レポート期間の右側のカレンダリストを[終了日付]カレンダリストと呼びます。(f)のラジオボタンを選択している場合は，ここにレポートしたい期間の終了日付を指定します。

(i) [Word]チェックボックス

Word レポートを生成する場合に選択します。

(j) [HTML]チェックボックス

HTML レポートを生成する場合に選択します。

(k) [レポート生成]ボタン

手動生成リストビューに手動生成レポートの設定内容を追加します。

[Word]チェックボックスと[HTML]チェックボックスのどちらか一方が選択されていないと[レポート生成]ボタンは非活性となります。

レポートの生成処理は同時に実行されませんので，自動生成レポートの実行中，または複数の手動生成レポートを追加した場合は順次実行されていきます。

レポート生成完了から 1 日経過することでリスト上から削除されます。レポート生成中でない場合は,該当行を右クリックして「削除」(または「キャンセル」)を選択するか，Delete キーを押すことで削除することができます。レポート生成中に削除したい場合は FIREWALLstaff Scheduler サービスを停止させた後，上記の削除手順を実行してください。

2 「プロファイル」の設定

2.1　FIREWALLstaff AE Server のプロファイル画面

プロファイルの各パネルについて説明します。FIREWALLstaff AE Server メイン画面の[対象ファイアウォール]欄のプロファイルをダブルクリックして，プロファイル画面を起動します。

画面左のツリーについて，NetScreen においては，[アプリケーション]パネル，[アプリケーションのレポート]パネル，[許可したアプリケーション]パネル，[遮断したアプリケーション]パネルへのリンク，Cisco においては，加えて[ウイルス]パネルへのリンクが表示されません。

2.1.1　[ファイアウォールの設定]パネル　【CheckPoint 以外】

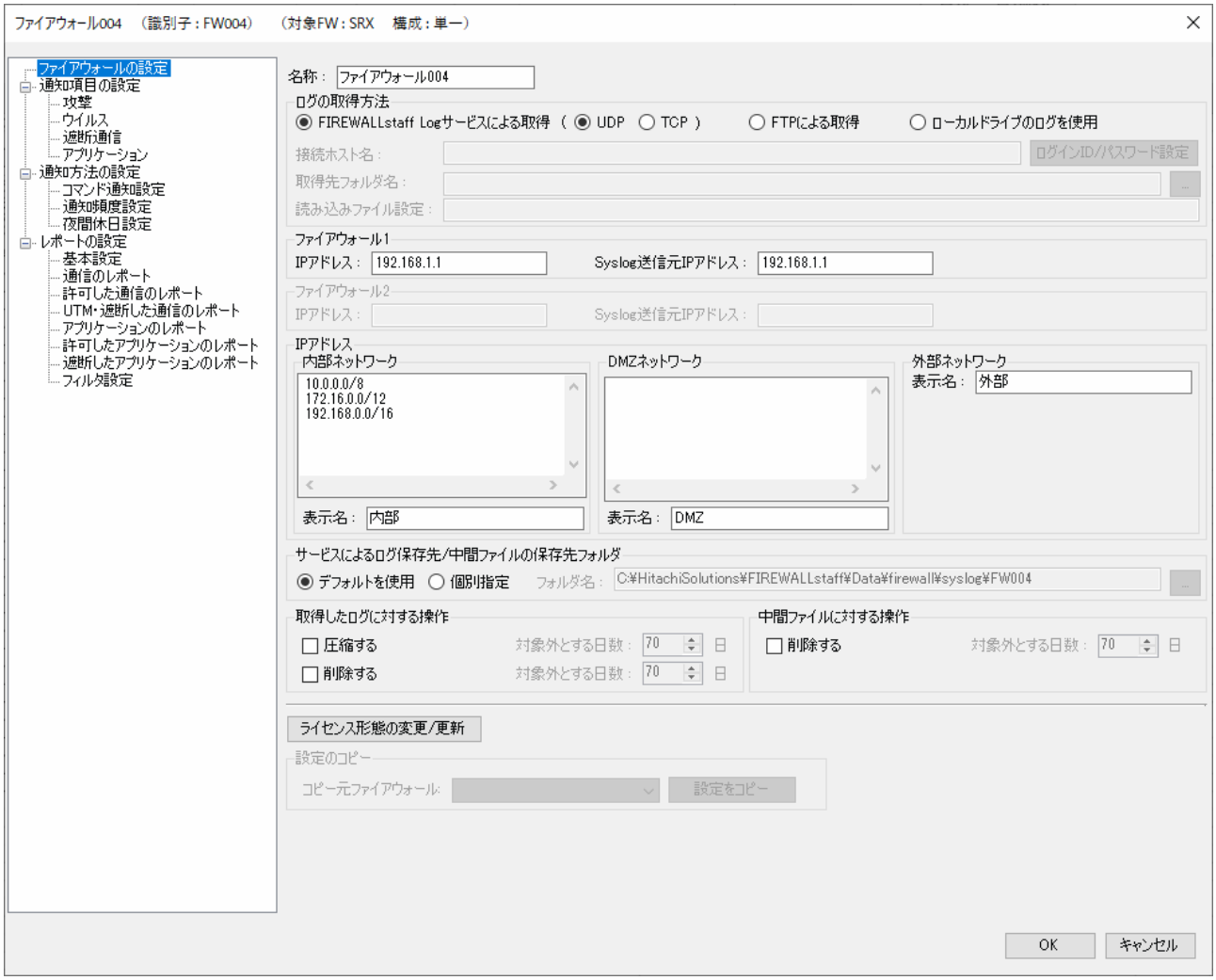


図 2 [ファイアウォールの設定]パネル（CheckPoint 以外）

(1)　[名称]テキストボックス

FIREWALLstaff におけるプロファイルを一意に識別するための名称です。最大 15 文字まで指定できます。

(2) [ログの取得方法]グループボックス

FIREWALLstaff で解析するログの取得方法を選択します。

(a) [FIREWALLstaff Log サービスによる取得]ラジオボタン

FIREWALLstaff がインストールされたサーバで Syslog を受信する場合に選択します。

(ア) [UDP]ラジオボタン

Syslog を UDP で受信する場合に選択します。ポート番号は「5.1.1 [Syslog 設定]パネル」にて設定します。

(イ) [TCP]ラジオボタン

Syslog を TCP で受信する場合に選択します。ポート番号は「5.1.1 [Syslog 設定]パネル」にて設定します。

(b) [FTP による取得] ラジオボタン

FIREWALLstaff がインストールされたサーバ以外に蓄積されたログを FTP で取得しレポートを生成する場合に選択します。**取得する対象のファイルは，ファイル名（およびディレクトリ名）から年月日を特定できる必要があります**。解析可能なファイルは

・圧縮されていない，テキスト形式のファイル

・ZIP 形式で圧縮された，テキスト形式のファイル（拡張子が「.zip」）

・GZIP 形式で圧縮された，テキスト形式のファイル（拡張子が「.gz」）

のみです。

FIREWALLstaff がアクセスする FTP サーバのディレクトリ名およびファイル名は，「半角英数字」「_」「-」「.」からなる必要があります。

FTP 接続を行う際に Proxy の設定が必要な場合は「5.1.5 [Proxy 設定]パネル」で必要な設定を行ってください。

(ア) 「[接続ホスト名]テキストボックス」に接続先の IP アドレスを指定します。FTP による接続を行う際にログイン ID とパスワードを設定する場合は「[ログイン ID/パスワード設定]ボタン」を押して出力されたダイアログに値を設定します。

(イ) 「[取得先フォルダ名]テキストボックス」に FTP サーバ上でログが配置されているディレクトリの絶対パスを指定します。ディレクトリの区切り文字は「/」を使用してください。表 2.1-1 の日付置換文字を使用することができます。
「|」記号を用いて複数のフォルダを指定することもできます。

(ウ) 「[読み込みファイル設定]テキストボックス」に取得対象となるファイル名を指定します。表 2.1-1 の日付置換文字を使用することができます。

表 2.1-1 日付置換文字

#	日付置換文字	説明
1	%yyyy%	4 桁の西暦の年。例）2014/4/1 の場合は「2014」

2	%MM%	桁揃えされた 2 桁の月。例）2014/4/1 の場合は「04」
3	%dd%	桁揃えされた 2 桁の日。例）2014/4/1 の場合は「01」
4	%yy%	西暦の年の下 2 桁。例）2014/4/1 の場合は「14」
5	%M%	桁揃えされていない月。例）2014/4/1 の場合は「4」
6	%d%	桁揃えされていない日。例）2014/4/1 の場合は「1」

例 1）/tmp/log ディレクトリに日毎のローテーションでログが作成される場合

ログのファイル名は前に「サーバ名」（ここでは「server」とします）を付加し，桁揃えされた年月日は区切り文字として「-」を用いており拡張子は「.log」であり，以下のようにログが作成されているとします。

/tmp/log/server2011-04-01.log
/tmp/log/server2011-04-02.log
/tmp/log/server2011-04-03.log
...

この場合は「[取得先フォルダ名]テキストボックス」に「/tmp/log」，「[読み込みファイル設定]テキストボックス」に「server%yyyy%-%MM%-%dd%.log」と指定します。

例 2）/tmp ディレクトリに月毎，日毎のローテーションでログが作成される場合

ログは桁揃えされた年のディレクトリ内に，ファイル名として前に「サーバ名」（ここでは「server」とします）を付加し，桁揃えされた月と日を付加し，拡張子は「.log」であり，以下のようにログが作成されているとします。

/tmp/2011/server0401.log
/tmp/2011/server0402.log
/tmp/2011/server0403.log
...

この場合は「[取得先フォルダ名]テキストボックス」に「/tmp/%yyyy%」，「[読み込みファイル設定]テキストボックス」に「server%MM%%dd%.log」と指定します。

(c)［ローカルドライブのログを使用］ラジオボタン

FIREWALLstaff がインストールされたサーバ内にあるログでレポートを生成する場合に選択します。

【ログファイルの条件】

・圧縮されていない，テキスト形式のファイル
・ZIP 形式で圧縮された，テキスト形式のファイル（拡張子が「.zip」）
・GZIP 形式で圧縮された，テキスト形式のファイル（拡張子が「.gz」）

また，「ファイル名」に含まれるピリオドの数は 1 つ以下である必要があります。

(ア)「[取得先フォルダ名]テキストボックス」にログが配置されているフォルダの絶対パスを指定します（[...]ボタンをクリックするとフォルダの参照ダイアログが呼び出されますのでそこから選択することも可能です）。ローカルドライブにあるフォルダを指定し，フォルダの区切り文字は「¥」を使用してください。表 2.1-1 の日付置換文字を使用することができます。
「|」記号を用いて複数のフォルダを指定することもできます。

(イ)「[読み込みファイル設定]テキストボックス」に取得対象となるファイル名を指定します。「*」（アスタリスク，0 文字以上の任意の文字列にマッチ）を 1 つ使用することができます。

注 意

「|」記号を用いて複数のフォルダを指定している場合は，[...]ボタンを用いてフォルダを選択しないでください。

例 1）C:¥tmp¥log に日毎かつ一定容量のローテーションでログが作成される場合

ログのファイル名は，日毎かつ一定容量でローテーションされ，以下のようにログが作成されているとします。

```
C:¥tmp¥log¥2013_05_07.log
C:¥tmp¥log¥2013_05_07a.log
C:¥tmp¥log¥2013_05_07b.log
C:¥tmp¥log¥2013_05_08.log
C:¥tmp¥log¥2013_05_09.log
C:¥tmp¥log¥2013_05_09a.log
C:¥tmp¥log¥2013_05_09b.log
...
```

この場合は「[取得先フォルダ名]テキストボックス」に「C:¥tmp¥log」，「[読み込みファイル設定]テキストボックス」に「*」や「*.log」のように指定します。

(3) [ファイアウォール *n*]フィールド

FIREWALLstaff でログを解析するファイアウォールを指定します。単一構成ライセンスをインストールした場合は[ファイアウォール 1]のみが有効となります。冗長構成ライセンスをインストールした場合は[ファイアウォール 1][ファイアウォール 2]両方が有効となります。

(a) [IP アドレス]テキストボックス

FIREWALLstaff が接続されている側のファイアウォールの実 IP アドレスを指定します。

(b) [Syslog 送信元 IP アドレス]テキストボックス

FIREWALLstaff がインストールされたサーバで Syslog を受信する場合，Syslog の送信元の IP アドレスを指定します。

(4) [IP アドレス]グループボックス

ファイアウォールによって分割された 3 つのゾーン（外部，内部，DMZ）の情報を，FIREWALLstaff で設定する必要があります。

(a) [内部ネットワーク] グループボックス

内部の IP アドレスを指定します。「*」（アスタリスク）または CIDR 記法による指定が可能です。また，レポートの文章において，内部ネットワークに相当する表現を[表示名]で指定することができます。

(b) [DMZ ネットワーク] グループボックス

DMZ の IP アドレスを指定します。「*」（アスタリスク）または CIDR 記法による指定が可能です。また，レポートの文章において，DMZ ネットワークに相当する表現を[表示名]で指定することができます。

(c) [外部ネットワーク] グループボックス

レポートの文章において，外部ネットワークに相当する表現を[表示名]で指定することができます。

(5) [サービスによるログ保存先/中間ファイルの保存先フォルダ]グループボックス

サービスによるログ保存先/中間ファイルの保存先フォルダ（以降「保存先フォルダ」と表記）の設定を行います。

(a) [デフォルトを使用]ラジオボタン

保存先フォルダとしてデフォルトのフォルダを使用する場合に選択します。

デフォルトのフォルダは，

[FIREWALLstaff データフォルダ]¥firewall¥syslog¥[ファイアウォール識別子]

です。

(b) [個別指定]ラジオボタン

保存先フォルダを個別に指定する場合はこのラジオボタンを選択し，[...]ボタンからフォルダを選択します。

(c) [フォルダ名]テキストボックス

保存先フォルダのパスが表示されます。

(d) [...]ボタン

[個別指定]ラジオボタンを選択した場合に活性状態になります。ボタンを押すとフォルダ選択ダイアログが表示されますので，保存先フォルダを選択してください。選択できるフ

ォルダはローカルハードディスクドライブに存在するフォルダのみです。

注　意

保存先フォルダを変更する場合は，FIREWALLstaff のすべてのサービスを停止し，変更前のフォルダ内に含まれるすべてのフォルダとファイルを変更後のフォルダにコピーしてから設定を変更し，FIREWALLstaff のすべてのサービスを開始してください。

注　意

「(2)(c)［ローカルドライブのログを使用］ラジオボタン」を選択した場合は，　取得先フォルダ名に指定したパスと同じパスを指定しないでください。

(6) ［取得したログに対する操作］グループボックス

FIREWALLstaff の Syslog サービスにより取得したログファイルに対する操作を指定します。0 時を過ぎたタイミングで 1 日に 1 回だけ実行されます

(a) ［圧縮する］チェックボックス

取得したログファイルを，［対象外とする日数］経過後に，圧縮します。

(b) ［削除する］チェックボックス

取得したログファイルを，［対象外とする日数］経過後に，削除します。

(7) ［中間ファイルに対する操作］グループボックス

ログを解析した情報を保持する中間ファイルに対する操作を指定します。0 時を過ぎたタイミングで 1 日に 1 回だけ実行されます。

(a) ［削除する］チェックボックス

中間ファイルを，［対象外とする日数］経過後に，削除します。

(8) ［ライセンス形態の変更/更新］ボタン

「FIREWALLstaff 対象 FW 単一構成ライセンス」でログ解析を行っているファイアウォールの構成が，単一構成から冗長構成に変更となった場合，FIREWALLstaff も冗長構成に対応したライセンスをインストールする必要があります。［ライセンス形態の変更/更新］ボタンをクリックして［ライセンス形態の変更/更新］ダイアログを開き，「FIREWALLstaff 対象 FW 冗長構成変更ライセンス」を入力して，［インストール］をクリックしてください。

(9) [設定のコピー]グループボックス

他のプロファイルの設定をコピーすることができます。コピー元ファイアウォールとして選択可能なのは，自身を除く同じファイアウォール種別のプロファイルです。同じファイアウォール種別のプロファイルが他にない場合，本グループボックスは非活性状態になります。

設定をコピーしたいコピー元のプロファイルを選択し，[設定のコピー]ボタンを押すと，コピー元プロファイルの以下の設定を除くすべての設定をコピーします。

- [ファイアウォールの設定]パネルの内容
- [レポートの設定]-[基本設定]パネルの「Word レポート保存先フォルダ」と「HTML レポート保存先フォルダ」の内容

設定のコピーを行う際は，事前に設定ファイル(user_data.xml)のバックアップを取得しておくことを推奨します。デフォルトの設定でインストールした場合，設定ファイルは以下のパスに配置されています。

例）C:¥HitachiSolutions¥FIREWALLstaff¥Data¥user¥user_data.xml

2.1.2 ［ファイアウォールの設定］パネル 【CheckPoint】

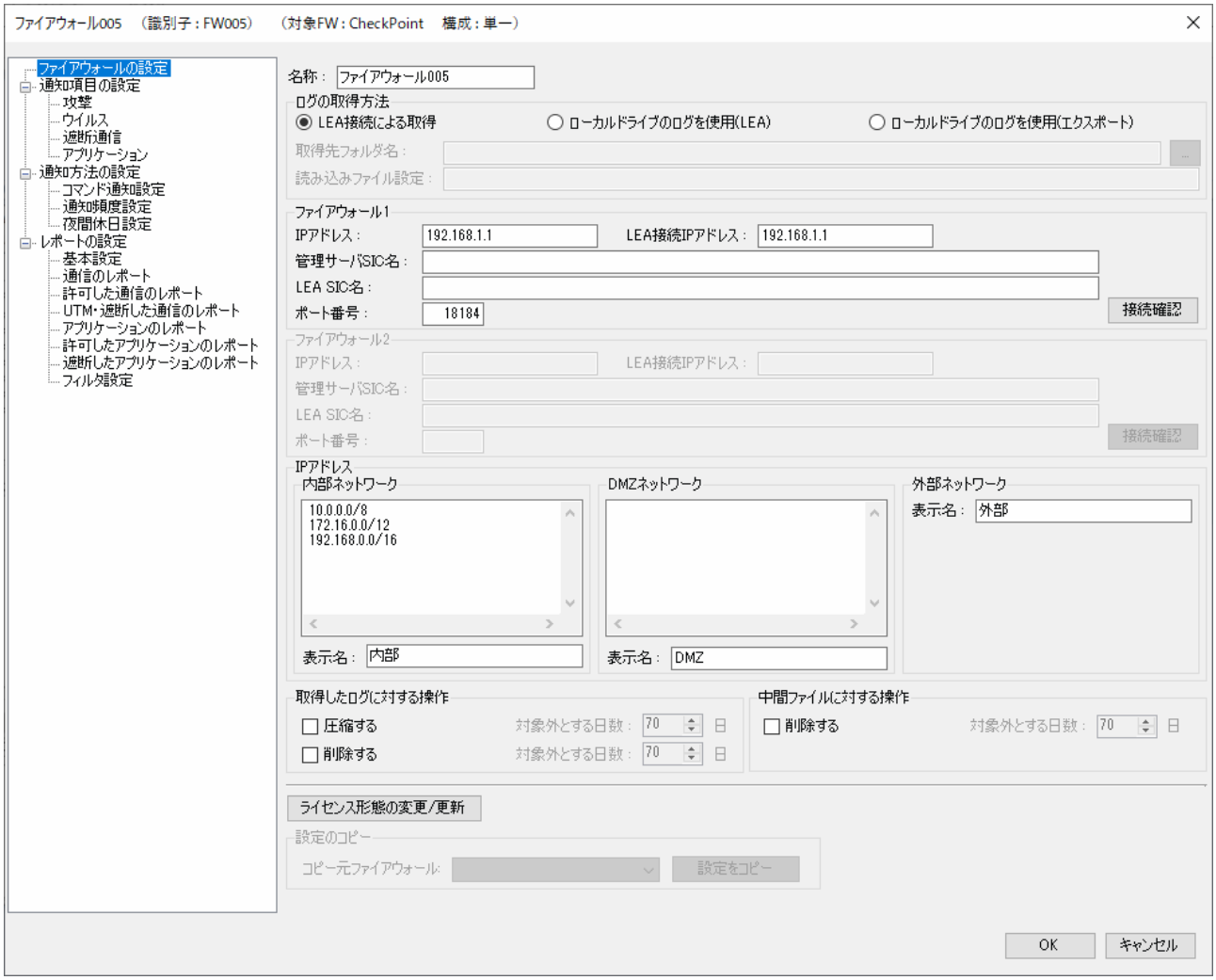


図 3 [ファイアウォールの設定]パネル（CheckPoint）

(1) ［名称］テキストボックス

FIREWALLstaff におけるプロファイルを一意に識別するための名称です。最大 15 文字まで指定できます。

(2) ［ログの取得方法］グループボックス

FIREWALLstaff で解析するログの取得方法を選択します。

(a) [LEA 接続による取得]ラジオボタン

FIREWALLstaff がインストールされたサーバから CheckPoint に，LEA 接続でアクセスしてログを収集する場合に選択します。

(b) [ローカルドライブのログを使用(LEA)] ラジオボタン

FIREWALLstaff がインストールされたサーバ内にある「FIREWALLstaff によって LEA 接続で取得した」ログでレポートを生成する場合に選択します。

【ログファイルの条件】

・圧縮されていない，テキスト形式のファイル

・ZIP 形式で圧縮された，テキスト形式のファイル（拡張子が「.zip」）

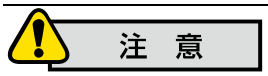
・GZIP 形式で圧縮された，テキスト形式のファイル（拡張子が「.gz」）

また，「ファイル名」に含まれるピリオドの数は 1 つ以下である必要があります。

(ア)「[取得先フォルダ名]テキストボックス」にログが配置されているフォルダの絶対パスを指定します（[...]ボタンをクリックするとフォルダの参照ダイアログが呼び出されますのでそこから選択することも可能です）。ローカルドライブにあるフォルダを指定し，フォルダの区切り文字は「¥」を使用してください。表 2.1-1 の日付置換文字を使用することができます。

「|」記号を用いて複数のフォルダを指定することもできます。

(イ)「[読み込みファイル設定]テキストボックス」に取得対象となるファイル名を指定します。「*」（アスタリスク，0 文字以上の任意の文字列にマッチ）を 1 つ使用することができます。



注　意

「|」記号を用いて複数のフォルダを指定している場合は，[...]ボタンを用いてフォルダを選択しないでください。

例 1）C:¥tmp¥log に日毎かつ一定容量のローテーションでログが作成される場合

ログのファイル名は，日毎かつ一定容量でローテーションされ，以下のようにログが作成されているとします。

C:¥tmp¥log¥2013_05_07.log
C:¥tmp¥log¥2013_05_07a.log
C:¥tmp¥log¥2013_05_07b.log
C:¥tmp¥log¥2013_05_08.log
C:¥tmp¥log¥2013_05_09.log
C:¥tmp¥log¥2013_05_09a.log
C:¥tmp¥log¥2013_05_09b.log
...

この場合は「[取得先フォルダ名]テキストボックス」に「C:¥tmp¥log」，「[読み込みファイル設定]テキストボックス」に「*」や「*.log」のように指定します。

(c) [ローカルドライブのログを使用(エクスポート)] ラジオボタン

CheckPoint のエクスポートしたログを用いてレポートを生成する場合に選択します。「エクスポートしたログ」とは，セミコロン「;」で区切られたテキスト形式のファイルです。

[取得先フォルダ名]と[読み込みファイル設定]の設定については，「(b) [ローカルドライブのログを使用(LEA)] ラジオボタン」を参照ください。

(3) [ファイアウォール *n*]フィールド

FIREWALLstaff でログを解析するファイアウォールを指定します。単一構成ライセンスをインストールした場合は[ファイアウォール 1]のみが有効となります。冗長構成ライセンスをインストールした場合は[ファイアウォール 1][ファイアウォール 2]両方が有効となります。

(a) [IP アドレス]テキストボックス

CheckPoint の IP アドレスを指定します。

(b) [LEA 接続 IP アドレス]テキストボックス

OPSEC LEA によってログを取得する，CheckPoint の IP アドレスを指定します。

(c) [管理サーバ SIC 名]テキストボックス

「管理サーバ SIC 名」を指定します。値の確認方法は，『取扱説明書（ファイアウォール設定編）』の「5.1.2(1)(b) LEA 接続の設定」を参考にしてください。

例）cn=cp_mgmt, O=cpmodule..uvwxyz

(d) [LEA SIC 名]テキストボックス

「LEA SIC 名」を指定します。値の確認方法は，『取扱説明書（ファイアウォール設定編）』の「5.1.2(1)(b) LEA 接続の設定」を参考にしてください。

例）CN=hitachi,O=cpmodule..uvwxyz

(e) [ポート番号]テキストボックス

CheckPoint 側で開けている LEA 接続用のポート番号を指定します。デフォルトは，18184 です。

(f) [接続確認]ボタン

OPSEC LEA による接続の動作確認を行うことができます。

(a)から(e)の各項目を設定し，「opsec.p12」ファイルを配置した上で[接続確認]ボタンをクリックすると接続確認コマンドが実行され，しばらくして確認結果ダイアログが表示されます。

接続に失敗した場合はエラー情報の出力先ファイル名が確認結果ダイアログに表示されますので，表 2.1-2 を参考に設定を見直してください。エラー情報は以下の書式で出力されます。

```
name=LEA_object ip= CheckPoint_IP function=Fnc_name message=error_string
```

変数名	内容
LEA_object	OPSEC LEA アプリケーション名
CheckPoint_IP	CheckPoint ファイアウォールの IP アドレス
Fnc_name	プログラム内の関数名
error_string	エラー内容

表 2.1-2 LEA 接続エラー情報

#	エラー内容	確認内容
1	opsec_session_end_reason returned: SIC_FAILURE	[管理サーバ SIC 名]または[LEA SIC 名]が間違っている可能性があります。設定を見直してください。
2	opsec_session_end_reason returned: COMM_IS_DEAD	[LEA 接続 IP アドレス]または[ポート番号]が間違っている可能性があります。設定を見直してください。
3	time-out occurred.	[LEA 接続 IP アドレス]または[ポート番号]が間違っているまたはネットワークが繋がっていない可能性があります。 合わせて CheckPoint 側で FIREWALLstaff インストールマシンからのアクセスが可能なルールが設定されているか確認してください。
4	opsec_session_end_reason returned: PEER_ENDED	LastRecord_notify.txt または LastRecord_report.txt の設定情報が誤っている場合に発生します。この場合は 2 つのファイルを削除してください。

注 意

CheckPoint のサービスを起動や停止した場合，CheckPoint の設定を変更した場合は，FIREWALLstaff Log サービスを再起動してください。

注 意

「opsec.p12」ファイルの作成手順は，『取扱説明書（ファイアウォール設定編）』の「5.2 opsec.p12 ファイルの作成」を参照してください。

(4) [IP アドレス]グループボックス

ファイアウォールによって分割された 3 つのゾーン（外部，内部，DMZ）の情報を，FIREWALLstaff で設定する必要があります。

(a) [内部ネットワーク]グループボックス

内部の IP アドレスを指定します。「*」（アスタリスク）または CIDR 記法による指定が可能です。また，レポートの文章において，内部ネットワークに相当する表現を[表示名]で指定することができます。

(b) [DMZ ネットワーク]グループボックス

DMZ の IP アドレスを指定します。「*」（アスタリスク）または CIDR 記法による指定が可能です。また，レポートの文章において，DMZ ネットワークに相当する表現を[表示名]で指定することができます。

(c) [外部ネットワーク]グループボックス

レポートの文章において，外部ネットワークに相当する表現を[表示名]で指定することができます。

(5) [取得したログに対する操作]グループボックス

FIREWALLstaff の Syslog サービスにより取得したログファイルに対する操作を指定します。0 時を過ぎたタイミングで 1 日に 1 回だけ実行されます

(a) [圧縮する]チェックボックス

取得したログファイルを，[対象外とする日数]経過後に，圧縮します。

(b) [削除する]チェックボックス

取得したログファイルを，[対象外とする日数]経過後に，削除します。

(6) [中間ファイルに対する操作]グループボックス

ログを解析した情報を保持する中間ファイルに対する操作を指定します。0 時を過ぎたタイミングで 1 日に 1 回だけ実行されます。

(a) [削除する]チェックボックス

中間ファイルを，[対象外とする日数]経過後に，削除します。

(7) [ライセンス形態の変更/更新]ボタン

「FIREWALLstaff 対象 FW 単一構成ライセンス」でログ解析を行っているファイアウォールの構成が，単一構成から冗長構成に変更となった場合，FIREWALLstaff も冗長構成に対応したライセンスをインストールする必要があります。[ライセンス形態の変更/更新]ボタンをクリックして[ライセンス形態の変更/更新]ダイアログを開き，「FIREWALLstaff 対象 FW 冗長構成変更ライセンス」を入力して，[インストール]をクリックしてください。

(8) [設定のコピー]グループボックス

他のプロファイルの設定をコピーすることができます。コピー元ファイアウォールとして選択可能なのは，自身を除く同じファイアウォール種別のプロファイルです。同じファイアウォール種別のプロファイルが他にない場合，本グループボックスは非活性状態になります。

設定をコピーしたいコピー元のプロファイルを選択し，[設定のコピー]ボタンを押すと，コピー元プロファイルの以下の設定を除くすべての設定をコピーします。

- [ファイアウォールの設定]パネルの内容

・ ［レポートの設定]-[基本設定]パネルの「Word レポート保存先フォルダ」と「HTML レポート保存先フォルダ」の内容

注 意

設定のコピーを行う際は，事前に設定ファイル(user_data.xml)のバックアップを取得しておくことを推奨します。デフォルトの設定でインストールした場合，設定ファイルは以下のパスに配置されています。

例）C:¥HitachiSolutions¥FIREWALLstaff¥Data¥user¥user_data.xml

3 「通知」の設定

本章では，通知の設定方法について説明します。通知は「ログの取得方法」において，「FIREWALLstaff Log サービスによる取得」（CheckPoint 以外）または「LEA 接続による取得」（CheckPoint）を選択している場合に実行可能となります。

3.1　通知項目の設定

3.1.1　[攻撃]パネル

ファイアウォールが検知してログに出力した攻撃のうち，FIREWALLstaff が通知する攻撃を設定します。[通知項目の設定：攻撃]パネルを図 4 に示します。

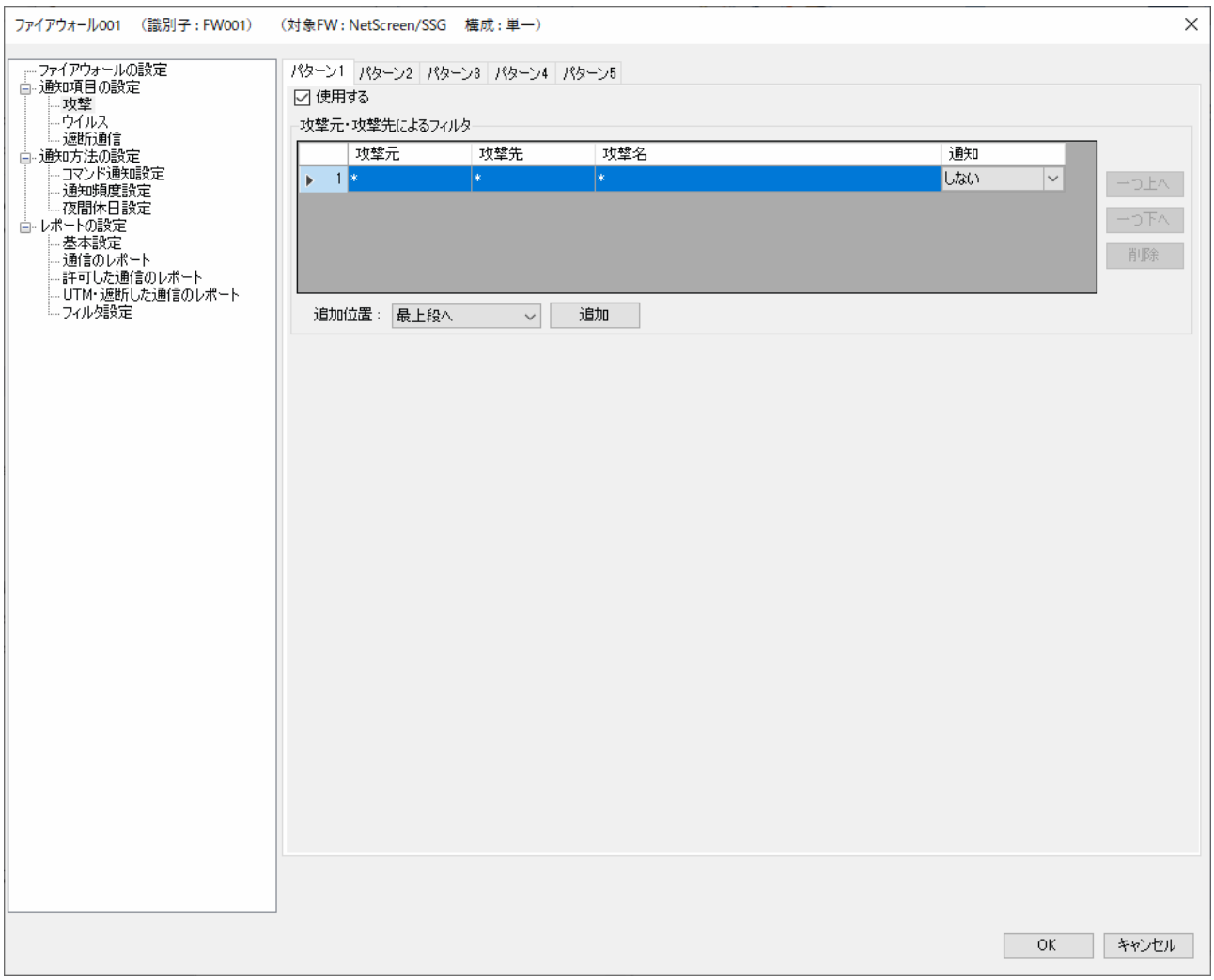


図 4 [通知項目の設定：攻撃]パネル

ファイアウォールがログに出力した攻撃すべてを FIREWALLstaff で通知すると，大量に通知される場合があります。そのため，[攻撃元・攻撃先によるフィルタ]によって，通知しない攻撃と通知する攻撃を指定することができます。

(1) [パターン]タブ

[パターン 1]から[パターン 5]までのタブにより，合計 5 パターンの条件を設定することができます。各タブの先頭にある[使用する]チェックボックスをチェックすることで，チェックしたタブの判定が有効になります。

タブ間での条件の判定は番号の小さい方から順に行われます。タブ毎の[攻撃元・攻撃先によるフィルタ]の条件に該当した場合にそのタブで設定した内容が適用され，以降のタブの判定は行いません。すべての条件に該当しない場合，通知は行われません。

あるタブで[攻撃元・攻撃先によるフィルタ]の条件として，攻撃元に「*」，攻撃先に「*」，攻撃名に「*」を指定すると，そのタブでの条件が成立するため以降のタブでの判定は行われません。

(2) [攻撃元・攻撃先によるフィルタ]グループボックス

攻撃元，攻撃先によって通知する攻撃を選別することができます。

設定したフィルタを上からチェックして行き，合致したレコードの[通知]項目の指定によって動作します。

[攻撃元][攻撃先][攻撃名]には「*」（アスタリスク）を指定することができます（IP アドレス中，指定単語の一部にも使用可能）。

(a) [番号]項目

上から順に，1，2，3，・・・と自動採番されます。小さい番号から順にチェックします。

(b) [攻撃元]項目

攻撃元を指定します。

(c) [攻撃先]項目

攻撃先を指定します。

(d) [攻撃名]項目

攻撃名を指定します。任意の値を指定する場合は「*」（アスタリスク）を指定します。

(e) [通知]項目

[する][しない]のいずれかを指定します。

初期値は,

番号	攻撃元	攻撃先	攻撃名	通知
1	*	*	*	しない

です。

例）DNS サーバ（IP アドレス，XXX.108.200.3）への攻撃のみを通知対象とする場合

番号	攻撃元	攻撃先	攻撃名	通知
1	*	XXX.108.200.3	*	する

例）Web サーバ（IP アドレス，XXX.108.200.5）への攻撃は通知しないが，それ以外の攻撃はすべて通知対象とする場合

番号	攻撃元	攻撃先	攻撃名	通知
1	*	XXX.108.200.5	*	しない
2	*	*	*	する

(f) フィルタ定義の操作方法

フィルタの定義を行う際の操作方法を説明します。

表 3.1-1 フィルタ定義の操作方法

項番	画面部品	説明
1	[追加位置]コンボボックス	フィルタ定義を 1 行分追加する際の位置を指定します。[最上段へ][最下段へ][選択行の一つ上へ][選択行の一つ下へ]の 4 種類を選択することができます。
2	[追加]ボタン	フィルタ定義を 1 行分追加します。追加する位置は[追加位置]コンボボックスで指定してください。
3	[一つ上へ]ボタン	選択行を 1 つ上に移動させます。
4	[一つ下へ]ボタン	選択行を 1 つ下に移動させます。
5	[削除]ボタン	選択行を削除します。

3.1.2　[ウイルス]パネル

ファイアウォールが検知してログに出力したウイルスのうち，FIREWALLstaff が通知するウイルスを設定します。本パネルは，Cisco 以外で表示されます。[通知項目の設定：ウイルス]パネルを図 5 に示します。

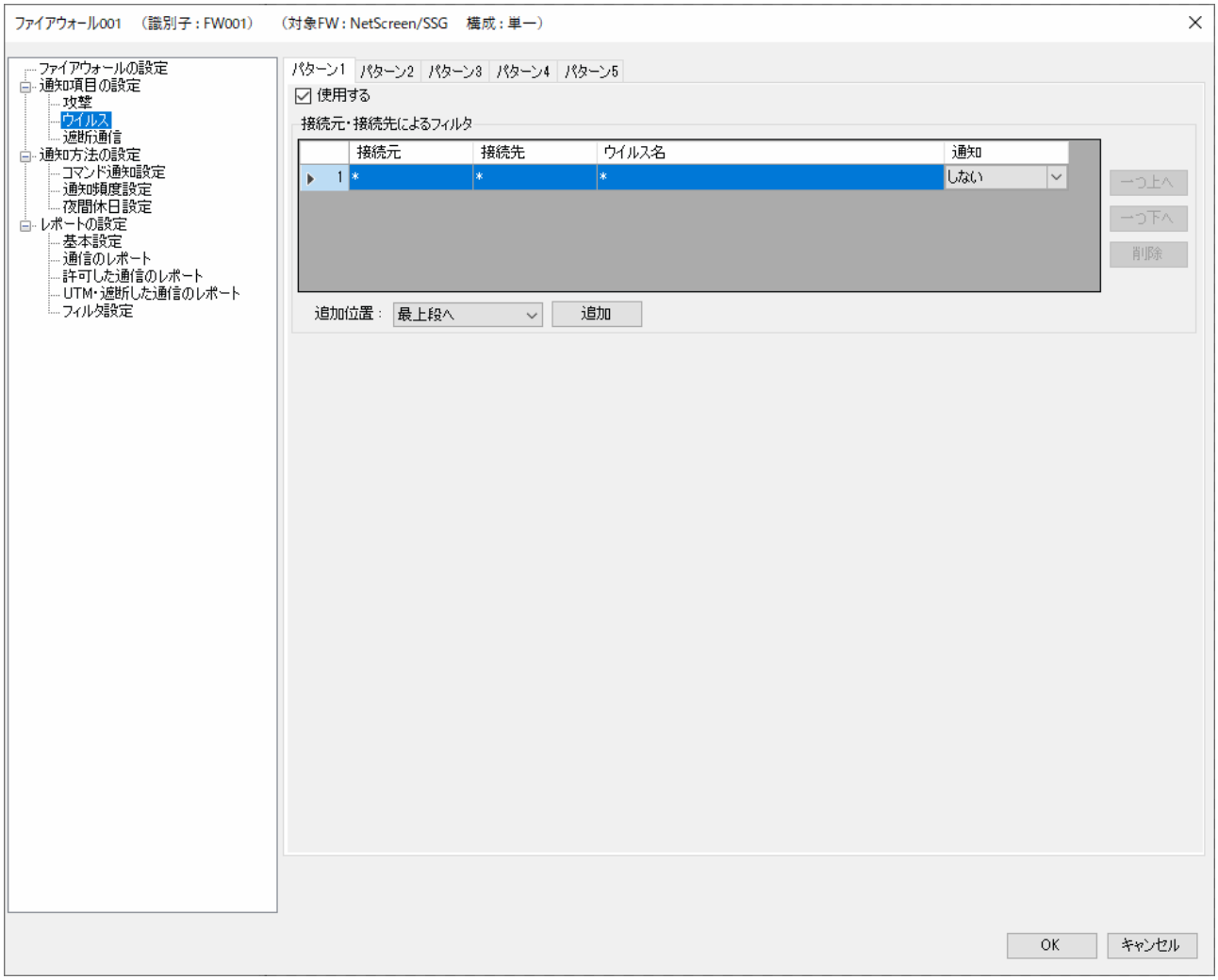


図 5 [通知項目の設定：ウイルス]パネル

ファイアウォールがログに出力したウイルスすべてを FIREWALLstaff で通知すると，大量に通知される場合があります。そのため，[接続元・接続先によるフィルタ]によって，通知しないウイルスと通知するウイルスを指定することができます。

(1)　[パターン]タブ

[パターン 1]から[パターン 5]までのタブにより，合計 5 パターンの条件を設定することができます。各タブの先頭にある[使用する]チェックボックスをチェックすることで，チェックしたタブの判定が有効になります。

タブ間での条件の判定は番号の小さい方から順に行われます。タブ毎の[接続元・接続先によるフィルタ]の条件に該当した場合にそのタブで設定した内容が適用され，以降のタブの判定は行いません。すべての条件に該当しない場合，通知は行われません。

あるタブで[接続元・接続先によるフィルタ]の条件として，接続元に「*」，接続先に「*」，ウイルス名に「*」を指定すると，そのタブでの条件が成立するため以降のタブでの判定は行われません。

(2) [接続元・接続先によるフィルタ]グループボックス

接続元，接続先によって通知するウイルスを選別することができます。

設定したフィルタを上からチェックして行き，合致したレコードの[通知]項目の指定によって動作します。

[接続元][接続先][ウイルス名]には「*」（アスタリスク）を指定することができます（IP アドレス中，指定単語の一部にも使用可能）。

(a) [番号]項目

上から順に，1，2，3，・・・と自動採番されます。小さい番号から順にチェックします。

(b) [接続元]項目

接続元を指定します。

(c) [接続先]項目

接続先を指定します。

(d) [ウイルス名]項目

ウイルス名を指定します。任意の値を指定する場合は「*」（アスタリスク）を指定します。

(e) [通知]項目

[する][しない]のいずれかを指定します。

初期値は,

番号	接続元	接続先	ウイルス名	通知
1	*	*	*	しない

です。

例）DNS サーバ（IP アドレス，XXX.108.200.3）へのウイルスのみを通知対象とする場合

番号	接続元	接続先	ウイルス名	通知
1	*	XXX.108.200.3	*	する

例）Web サーバ（IP アドレス，XXX.108.200.5）へのウイルスは通知しないが，それ以外のウイルスはすべて通知対象とする場合

番号	接続元	接続先	ウイルス名	通知
1	*	XXX.108.200.5	*	しない
2	*	*	*	する

(f) フィルタ定義の操作方法

フィルタの定義を行う際の操作方法に関しては「表 3.1-1 フィルタ定義の操作方法」を参照ください。

3.1.3　[遮断通信]パネル

ファイアウォールが検知してログに出力した遮断通信のうち，FIREWALLstaff が通知する遮断通信を設定します。[遮断通信]パネルを図 6 に示します。

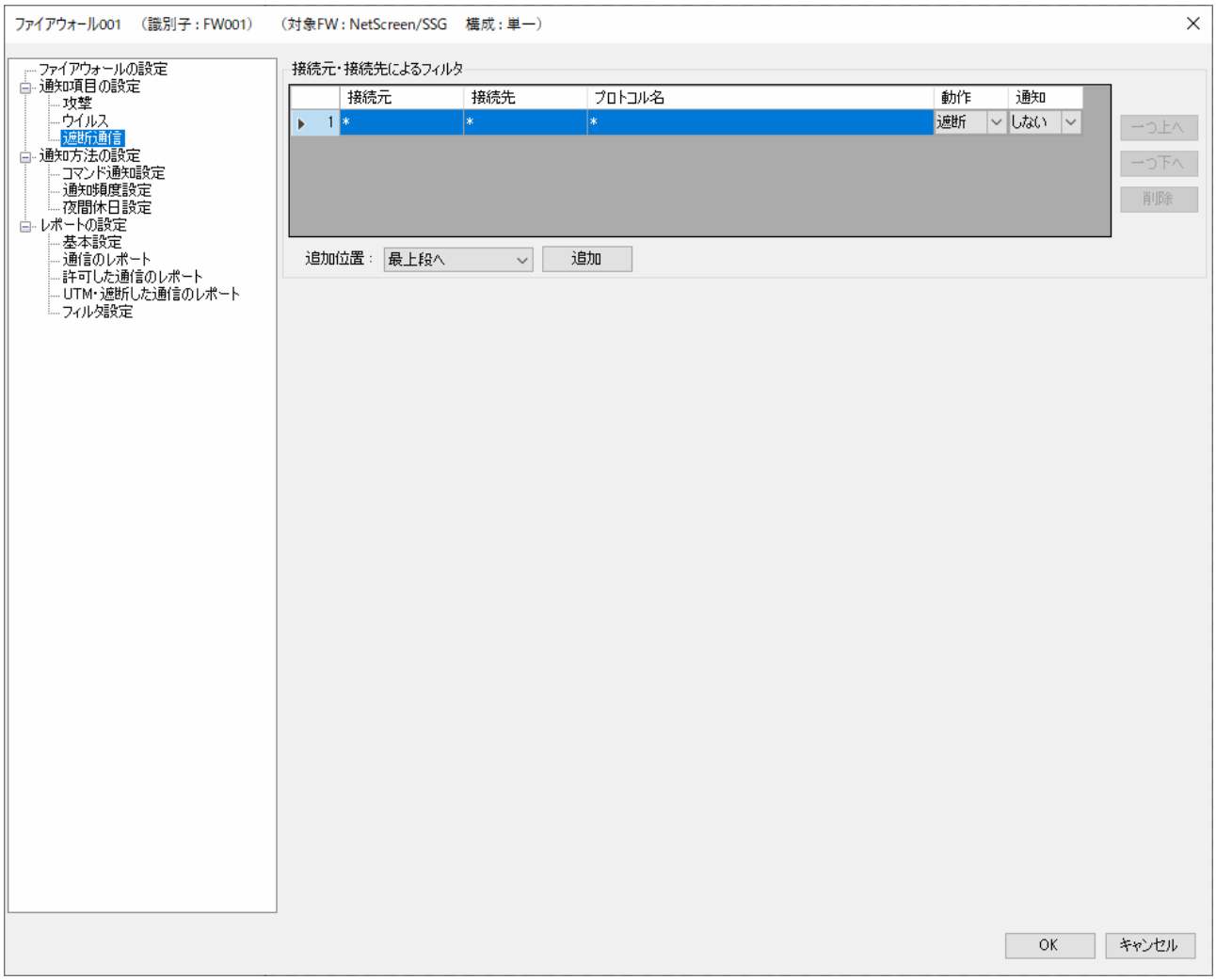


図 6 [通知項目の設定：遮断通信]パネル

ファイアウォールがログに出力した遮断通信すべてを FIREWALLstaff で通知すると，大量に通知される場合があります。そのため，[接続元・接続先によるフィルタ]によって，通知しない遮断通信と通知する遮断通信を指定することができます。

(1) [接続元・接続先によるフィルタ]グループボックス

接続元，接続先によって通知する遮断通信を選別することができます。また，必要に応じてプロトコル名でも選別することができます。

設定したフィルタを上からチェックして行き，合致したレコードの[通知]項目の指定によって動作します。

[接続元][接続先][プロトコル名]には「*」（アスタリスク）を指定することができます（IP アドレス中，指定単語の一部にも使用可能）。

(a) [番号]項目

上から順に，1，2，3，・・・と自動採番されます。小さい番号から順にチェックします。

(b) [接続元]項目

接続元を指定します。

(c) [接続先]項目

接続先を指定します。

(d) [プロトコル名]項目

フィルタするプロトコル名を指定します。プロトコル名の指定方法は，次のとおりです。

表 3.1-2 通信の指定方法

項番	ファイアウォール	指定方法
1	NetScreen/SSG	ログの service の値 例）「…policy_id=1 service=ftp proto=6 …」における「ftp」
2	FortiGate	ログの service の値 例）「…proto=6 service=25/tcp app_type=N/A …」における「25/tcp」
3	Palo Alto	宛先ポート番号と TCP/UDP 種別を，次の形式で指定する 宛先ポート番号/tcp　または　宛先ポート番号/udp 例）25/tcp
4	SRX	ログのプロトコル情報の値 例）「…TCP FIN: 192.168.1.34/4691->192.168.252.222/ 8080 junos-http…」における「junos-http」 None の場合は，宛先ポート番号と TCP/UDP 種別を指定してください。 例）「25/tcp」
5	CheckPoint	ログの proto の値が tcp または udp の時，ログの service の値，ログの proto の値が tcp または udp 以外の時，proto の値 例 1)「…rule=1 src=192.168.2.1 dst=10.220.2.1 service="http" proto="tcp"」における「tcp」 例 2)「…rule=1 src=192.168.2.1 dst=10.220.2.1 service="http" proto="icmp"」における「http」
6	IPCOM	宛先ポート番号と TCP/UDP 種別を，次の形式で指定する 宛先ポート番号/tcp　または　宛先ポート番号/udp 例 1）25/tcp また，ICMP の場合はログの proto の値 例 2）「…src=192.168.50.2 dst=133.108.231.87 proto=icmp icmp-type=8 icmp-code=0…」の「icmp」
7	Cisco	宛先ポート番号と TCP/UDP 種別を，次の形式で指定する 宛先ポート番号/tcp　または　宛先ポート番号/udp 例）25/tcp

(e) [動作]項目

[遮断]を指定します。

(f) [通知]項目

[する][しない]のいずれかを指定します。

初期値は,

番号	接続元	接続先	プロトコル名	動作	通知
1	*	*	*	遮断	しない

です。

例）内部クライアント（192.168.1.0/24）から，プロトコルに http を用いた遮断通信のみを通知対象とする場合

番号	接続元	接続先	プロトコル名	動作	通知
1	192.168.1.*	*	http	遮断	する

(g) フィルタ定義の操作方法

フィルタの定義を行う際の操作方法に関しては「表 3.1-1 フィルタ定義の操作方法」を参照ください。

3.1.4　[アプリケーション]パネル

ファイアウォールが検知してログに出力したアプリケーションのうち，FIREWALLstaff が通知するアプリケーションを設定します。本パネルは，FortiGate，Palo Alto，SRX，IPCOM でのみ表示されます。[通知項目の設定：アプリケーション]パネルを図 7 に示します。

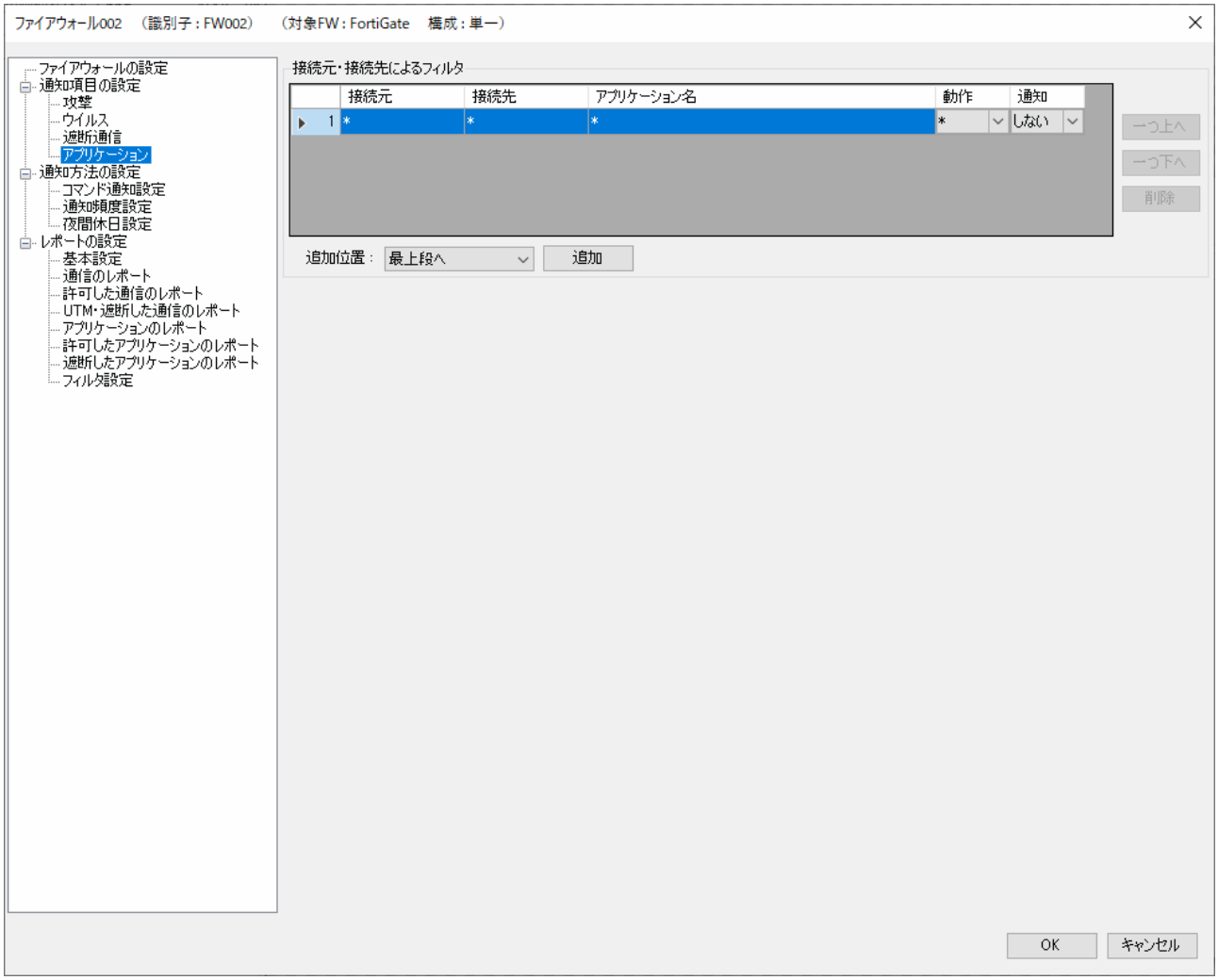


図 7 [通知項目の設定：アプリケーション]パネル

ファイアウォールがログに出力したアプリケーションすべてを FIREWALLstaff で通知すると，大量に通知される場合があります。そのため，[接続元・接続先によるフィルタ]によって，通知しないアプリケーションと通知するアプリケーションを指定することができます。

(1) [接続元・接続先によるフィルタ]グループボックス

接続元，接続先によって通知するアプリケーションを選別することができます。また，必要に応じてアプリケーション名と動作でも選別することができます。

設定したフィルタを上からチェックして行き，合致したレコードの[通知]項目の指定によって動作します。

[接続元][接続先][アプリケーション名][動作]には「*」（アスタリスク）を指定することができます（IP アドレス中，指定単語の一部にも使用可能）。

(a) [番号]項目

上から順に，1，2，3，・・・と自動採番されます。小さい番号から順にチェックします。

(b) [接続元]項目

接続元を指定します。

(c) [接続先]項目

接続先を指定します。

(d) [アプリケーション名]項目

フィルタするアプリケーション名を指定します。

各ファイアウォールで指定できるアプリケーション名は，次のとおりです。

表 3.1-3 各ファイアウォールで指定できるアプリケーション名

項番	ファイアウォール	指定できるアプリケーション名
1	FortiGate	ログの app の値 例）「…applist="default" appcat="Web.Client" app="HTTP.BROWSER_IE" action="block"…」における「HTTP.BROWSER_IE」
2	Palo Alto	ログのカンマ区切りで 15 番目の値 例）「<14>Feb 19 13:26:32 1,2010/02/19 13:26:32,0006C100945, TRAFFIC,end,12,2010/02/19 13:26:31,10.212.200.110,158.213.204.102,0.0.0.0,0.0.0.0,rule1,,,http-proxy,vsys1,TAPZONE,」における「http-proxy」
3	SRX	下記ログ例における<app1>の値，または<app1>(<app2>) 「…0x0 source rule nsw-src-interface N/A N/A 17 av01 Internal Internet 53159 0(0) 0(0) 62 <app1> <app2> N/A(N/A) ge-0/0/1.0 UNKNOWN」 例 1)<app1>が「DNS」，<app2>が「UNKNOWN」または「INCONCLUSIVE」の場合，アプリケーション名は「DNS」 例 2)<app1>が「HTTP」，<app2>が「UNKNOWN」または「INCONCLUSIVE」以外(例えば「MIXI」の場合)，アプリケーション名は「HTTP(MIXI)」
4	CheckPoint	ログの appi_name の値 例）「…appi_name="Facebook" app_category="Social Networking"…」における「Facebook」
5	IPCOM	ログの app-name の値 例）「…app-category=management-protocol app-name=syslog…」における「syslog」

(e) [動作]項目

該当するアプリケーション通信の動作を指定します。[*][許可][遮断]のいずれかを指定します。

(f) [通知]項目

[する][しない]のいずれかを指定します。

初期値は,

番号	接続元	接続先	アプリケーション名	動作	通知
1	*	*	*	*	しない

です。

例）【FortiGate】内部クライアント（192.168.1.0/24）から，Wikipedia へアクセスを試みた遮断通信のみを通知対象とする場合

番号	接続元	接続先	アプリケーション名	動作	通知
1	192.168.1.*	*	Wikipedia	遮断	する

(g) フィルタ定義の操作方法

フィルタの定義を行う際の操作方法に関しては「表 3.1-1 フィルタ定義の操作方法」を参照ください。

3.1.5　[通知方法の設定：コマンド通知設定]パネル

コマンドで通知する場合の，通知先と通知メッセージとコマンド引数を指定します。

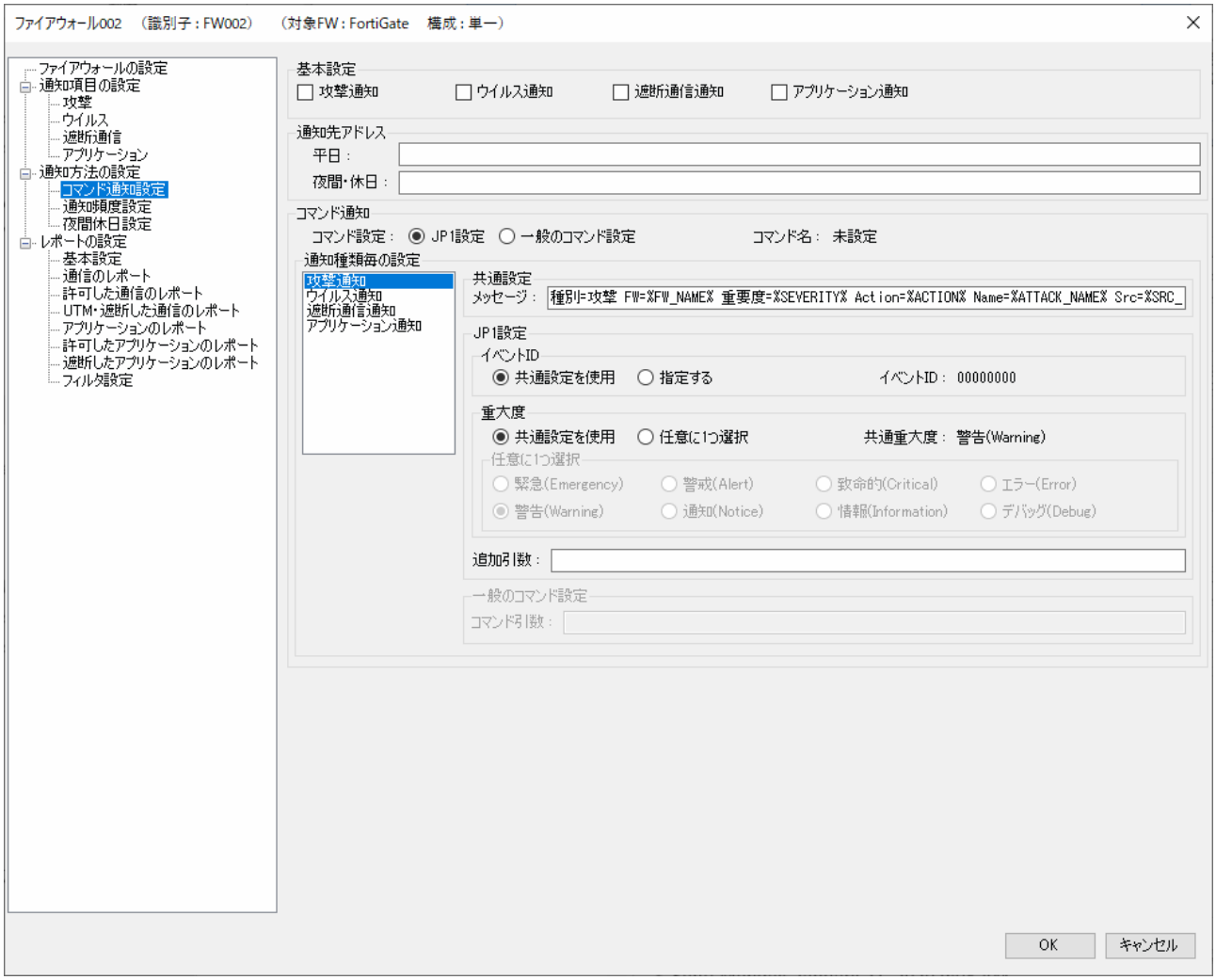


図 8 [通知方法の設定：コマンド通知設定]パネル

(1) [基本設定]グループボックス

(a) [攻撃通知]チェックボックス

[攻撃]パネルで指定した攻撃を検知した場合に通知を行います。

(b) [ウイルス通知]チェックボックス

[ウイルス]パネルで指定したウイルスを検知した場合に通知を行います。このチェックボックスは，NetScreen，FortiGate，Palo Alto，SRX，CheckPoint，IPCOM でのみ表示されます。

(c) [遮断通信通知]チェックボックス

[遮断通信]パネルで指定した遮断通信を検知した場合に通知を行います。

(d) [アプリケーション通知]チェックボックス

[アプリケーション]パネルで指定したアプリケーションを検知した場合の通知方法を指定します。このチェックボックスは，FortiGate，Palo Alto，SRX，CheckPoint，IPCOM でのみ表示されます。

(2) [連絡先アドレス]グループボックス

コマンドで通知する際の通知先 IP アドレスを指定します。平日の通知先と，夜間・休日の通知先を区別して指定することができます。

(a) [平日]テキストボックス

平日の通知先 IP アドレスを指定します。「,」（カンマ）区切りで，最大 10 まで指定できます。

コマンド設定で「一般のコマンド設定」を選択した場合，通知先 IP アドレスが存在しない場合でも，通知を行う場合はダミーの値(0.0.0.0)を 1 つ指定してください。

(b) [夜間・休日]テキストボックス

夜間・休日の通知先 IP アドレスを指定します。「,」（カンマ）区切りで，最大 10 まで指定できます。

コマンド設定で「一般のコマンド設定」を選択した場合，通知先 IP アドレスが存在しない場合でも，通知を行う場合はダミーの値(0.0.0.0)を 1 つ指定してください。

(3) [コマンド通知]グループボックス

攻撃やウイルスなどを検知した際に通知する，メッセージとコマンド引数に関する設定を行います。

「(a) [コマンド設定]ラベル」で設定した内容は 1 つのプロファイル内で 1 つの設定値が保持されます。[通知種類毎の設定]グループボックス内の設定内容は「(c) 通知種類リストボックス」内の選択項目毎にそれぞれ保持されます。

(a) [コマンド設定]ラベル

「JP1 設定」か「一般のコマンド設定」のいずれかを選択します。

[JP1 設定]ラジオボタンはコマンド通知を実行するコマンドとして，JP1/Base のコマンド（jevsend または jevsendd）を設定した場合に選択します。この設定を選択した場合，コマンド実行時の引数を自動的に組み立ててコマンドを実行します。[JP1 設定]ラジオボタンが選択されている場合は，「(d) [共通設定]グループボックス」と「(e)[JP1 設定]グループボックス」が活性状態になります。

[一般のコマンド設定]ラジオボタンが選択されている場合は「(d) [共通設定]グループボックス」と「(f)[一般のコマンド設定]グループボックス」が活性状態になります。

(b) [コマンド名]ラベル

「5.1.6［コマンド通知]パネル」で設定した実行コマンドのファイル名を表示します。ファイル名が取得できない場合は「未設定」と表示されます。

以降では，[通知種類毎の設定]グループボックス内の設定内容について説明します。

(c) 通知種類リストボックス

コマンド通知はファイアウォール毎に以下の項目が設定可能です。

表 3.1-4 コマンド通知種類

項番	項目	ファイアウォール						
		NetScreen/SSG	FortiGate	Palo Alto	SRX	CheckPoint	IPCOM	Cisco
1	攻撃通知	○	○	○	×	○	○	○
2	攻撃(IDS)通知	×	×	×	○	×	×	×
3	攻撃(IDP)通知	×	×	×	○	×	×	×
4	ウイルス通知	○	○	○	○	○	○	×
5	遮断通信通知	○	○	○	○	○	○	○
6	アプリケーション通知	×	○	○	○	○	○	×

○：設定できる

×：設定できない

(d) [共通設定]グループボックス

通知時に使用するメッセージを[メッセージ]テキストボックスに指定します。最大 400 文字まで指定できます。

(e) [JP1 設定]グループボックス

［イベント ID]グループボックスでは引数に指定するイベント ID の設定を行います。イベント ID が未設定の場合はコマンド実行時に引数を省略します。

［共通設定を使用]ラジオボタンを選択した場合は，「5.1.6(2)(a)［共通イベント ID]グループボックス」にて設定した共通イベント ID を使用します。共通イベント ID が[イベント ID]ラベルの右に表示されます。

任意にイベント ID を指定する場合は，[指定する]ラジオボタンを選択すると[イベント ID]ラベルの右がテキストボックスに切り替わるので任意のイベント ID を指定します。

［重大度］グループボックスでは引数に指定する重大度の設定を行います。

［共通設定を使用］ラジオボタンを選択した場合は，「5.1.6(2)(b) ［共通重大度］グループボックス」にて設定した共通重大度を使用します。共通重大度が［共通重大度］ラベルの右に表示されます。

任意に重大度を指定する場合は，［任意に 1 つ選択］ラジオボタンを選択すると［任意に 1 つ］選択グループボックスが活性状態になりますので，任意の重大度を選択します。

［追加引数］テキストボックスでは，拡張属性の引数等を指定することができます。最大 1000 文字まで指定できます。

注 意

コマンド設定で［JP1 設定］を選択した場合以下の書式でコマンドを実行します。

コマンド -i イベント ID -d 通知先アドレス -e SEVERITY=重大度
-m ″メッセージ″ 追加引数

追加引数指定時は上記の書式を念頭に置いた上で指定してください。

(f) ［一般のコマンド設定］グループボックス

［コマンド引数］テキストボックスにコマンドの引数を指定することができます。最大 1000 文字まで指定できます。また，［コマンド引数］テキストボックス内では以下のコマンド引数置換変数が使用可能です。

コマンド引数置換変数	内容
%CMDP_HOST%	「(2)(a) ［平日］テキストボックス」または「(2)(b) ［夜間・休日］テキストボックス」で指定された通知先アドレスに置換されます。 複数指定されていた場合は，複数の通知先に対しそれぞれコマンドを実行します。
%CMDP_MSG%	「(d)［共通設定］グループボックス」内で指定されたメッセージに置換されます。

注 意

コマンド設定で［一般のコマンド設定］を選択した場合以下の書式でコマンドを実行します。

コマンド コマンド引数

例えば，指定したコマンドが，以下の書式で通知先アドレスに対してメッセージを送信するものであるとします。

コマンド -host=通知先アドレス -message=″メッセージ″

この場合，［コマンド引数］テキストボックスには，「-host=%CMDP_HOST% -message="%CMDP_MSG%"」と指定すれば期待通りの実行結果が得られます。

(4) ［コマンド通知］通知メッセージ

コマンド通知先で表示されるデフォルトの通知メッセージを示します。ファイアウォール毎に対応する通知については，「3.1.5［通知方法の設定：コマンド通知設定］パネル 表 3.1-4 コマンド通知種類」を参照してください。

(a) 攻撃通知

攻撃を検知した場合に送信するメッセージの内容は次のとおりです。この内容は，変更できます。

表 3.1-5 攻撃の通知

項番	名称	内容	
1	メッセージ	書式	種別=攻撃 FW=%FW_NAME%［重要度=%SEVERITY%］{ Action=%ACTION%} Name=%ATTACK_NAME% Src=%SRC_IP% Dst=%DST_IP% 日時=%DATE%
		置換文字	%DATE%…「yyyy/MM/dd HH:mm:ss」形式の日時 %FW_NAME%…ファイアウォール名 %SRC_IP%…攻撃を行った IP アドレス %DST_IP%…攻撃を受けた IP アドレス %ATTACK_NAME%…検知した攻撃名 %ACTION%…ファイアウォールの動作 %SEVERITY%…ファイアウォールが設定した重要度
		例	種別=攻撃 FW=ファイアウォール１号機［重要度=Warning］{ Action=drop} Name=SYN flood Src=192.168.1.51 Dst=133.108.xxx.111 日時=2010/10/02 00:10:08

注意：{}内は FortiGate，Palo Alto，CheckPoint のみ。また，Cisco では[]内は出力されません。

(b) 攻撃(IDS)通知

IDS による攻撃を検知した場合に送信するメッセージの内容は次のとおりです。この内容は，変更できます。

表 3.1-6 IDS による攻撃の通知

項番	名称	内容	
1	メッセージ	書式	種別=攻撃(IDS) FW=%FW_NAME% Name=%ATTACK_NAME% Src=%SRC_IP% Dst=%DST_IP% 日時=%DATE%

		置換文字	%DATE%…「yyyy/MM/dd HH:mm:ss」形式の日時 %FW_NAME%…ファイアウォール名 %SRC_IP%…攻撃を行った IP アドレス %DST_IP%…攻撃を受けた IP アドレス %ATTACK_NAME%…検知した攻撃名
		例	種別=攻撃(IDS) FW=ファイアウォール１号機 Name=SYN flood Src=192.168.1.51 Dst=133.108.xxx.111 日時=2010/10/02 00:10:08

(c) 攻撃(IDP)通知

IDP による攻撃を検知した場合に送信するメッセージの内容は次のとおりです。この内容は，変更できます。

表 3.1-7 IDP による攻撃の通知

項番	名称	内容	
1	メッセージ	書式	種別=攻撃(IDP) FW=%FW_NAME% 重要度=%SEVERITY% Action=%ACTION% Name=%ATTACK_NAME% Src=%SRC_IP% Dst=%DST_IP% 日時=%DATE%
		置換文字	%DATE%…「yyyy/MM/dd HH:mm:ss」形式の日時 %FW_NAME%…ファイアウォール名 %SRC_IP%…攻撃を行った IP アドレス %DST_IP%…攻撃を受けた IP アドレス %ATTACK_NAME%…検知した攻撃名 %ACTION%…ファイアウォールの動作 %SEVERITY%…ファイアウォールが設定した重要度
		例	種別=攻撃(IDP) FW=ファイアウォール１号機 重要度=Warning Action=drop Name=SYN flood Src=192.168.1.51 Dst=133.108.xxx.111 日時=2010/10/02 00:10:08

(d) ウイルス通知

ウイルスを検知した場合に送信するメッセージの内容は次のとおりです。この内容は，変更できます。

表 3.1-8 ウイルスの通知

項番	名称	内容	
1	メッセージ	書式	種別=ウイルス FW=%FW_NAME% {Action=%ACTION% }Name=%VIRUS_NAME% Src=%SRC_IP% Dst=%DST_IP% 日時=%DATE%
		置換文字	%DATE%…「yyyy/MM/dd HH:mm:ss」形式の日時 %FW_NAME%…ファイアウォール名 %SRC_IP%…ウイルスを送った IP アドレス %DST_IP%…ウイルスを送られた IP アドレス %VIRUS_NAME%…検知したウイルス名 %ACTION%…ファイアウォールの動作
		例	種別=ウイルス FW=ファイアウォール２号機 {Action=drop } Name=EICAR TEST Src=192.168.100.100 Dst=133.108.yyy.29 日時=2010/10/02 00:10:08

注意：{}内は，Palo Alto，CheckPoint，IPCOM のみ。

(e) 遮断通信通知

遮断通信を検知した場合に送信するメッセージの内容は次のとおりです。この内容は，変更できます。

表 3.1-9 遮断通信の通知

項番	名称	内容	
1	メッセージ	書式	種別=遮断通信 FW=%FW_NAME% 方向=%DIRECTION% Proto=%PROTOCOL% Src=%SRC_IP% Dst=%DST_IP% 日時=%DATE%
		置換文字	%DATE%…「yyyy/MM/dd HH:mm:ss」形式の日時 %FW_NAME%…ファイアウォール名 %DIRECTION%…通信方向 %PROTOCOL%…プロトコル名 %SRC_IP%…送信元の IP アドレス %DST_IP%…送信先の IP アドレス
		例	種別=遮断通信 FW=ファイアウォール２号機 方向=DMZ から内部へ Proto=ftp Src=192.168.100.100 Dst=133.108.yyy.29 日時=2010/10/02 00:10:08

(f) アプリケーション通知

アプリケーション制御により検知すべき通信が発生した場合に送信するメッセージの内容は次のとおりです。この内容は，変更できます。

表 3.1-10 アプリケーション通知

項番	名称	内容	
1	メッセージ	書式	種別=アプリ FW=%FW_NAME% {Action=%ACTION% }Proto=%PROTOCO L% Name=%APPLICATION_NAME% Src=%SRC_IP% Dst=%DST_IP% 日時=%DATE%
		置換文字	%DATE%…「yyyy/MM/dd HH:mm:ss」形式の日時 %FW_NAME%…ファイアウォール名 %SRC_IP%…ウイルスを送った IP アドレス %DST_IP%…ウイルスを送られた IP アドレス %APPLICATION_NAME%…検知したアプリケーション名 %ACTION%…ファイアウォールの動作 %PROTOCOL%…使用された[プロトコル|ポート番号]
		例	種別=アプリ FW=ファイアウォール２号機 Action= block Proto= tcp/55555 Name=Winny Src=192.168.100.100 Dst=133.108.yyy.29 日時=2010/10/02 00:10:08

注意：{}内は FortiGate，Palo Alto のみ。

3.1.6　[通知方法の設定：通知頻度設定]パネル

FIREWALLstaff が検知した事項の，通知する頻度を指定します。なお，このパネルでの「1単位時間」とは，xx 時 00 分 00 秒～xx 時 59 分 59 秒のレンジを指します。

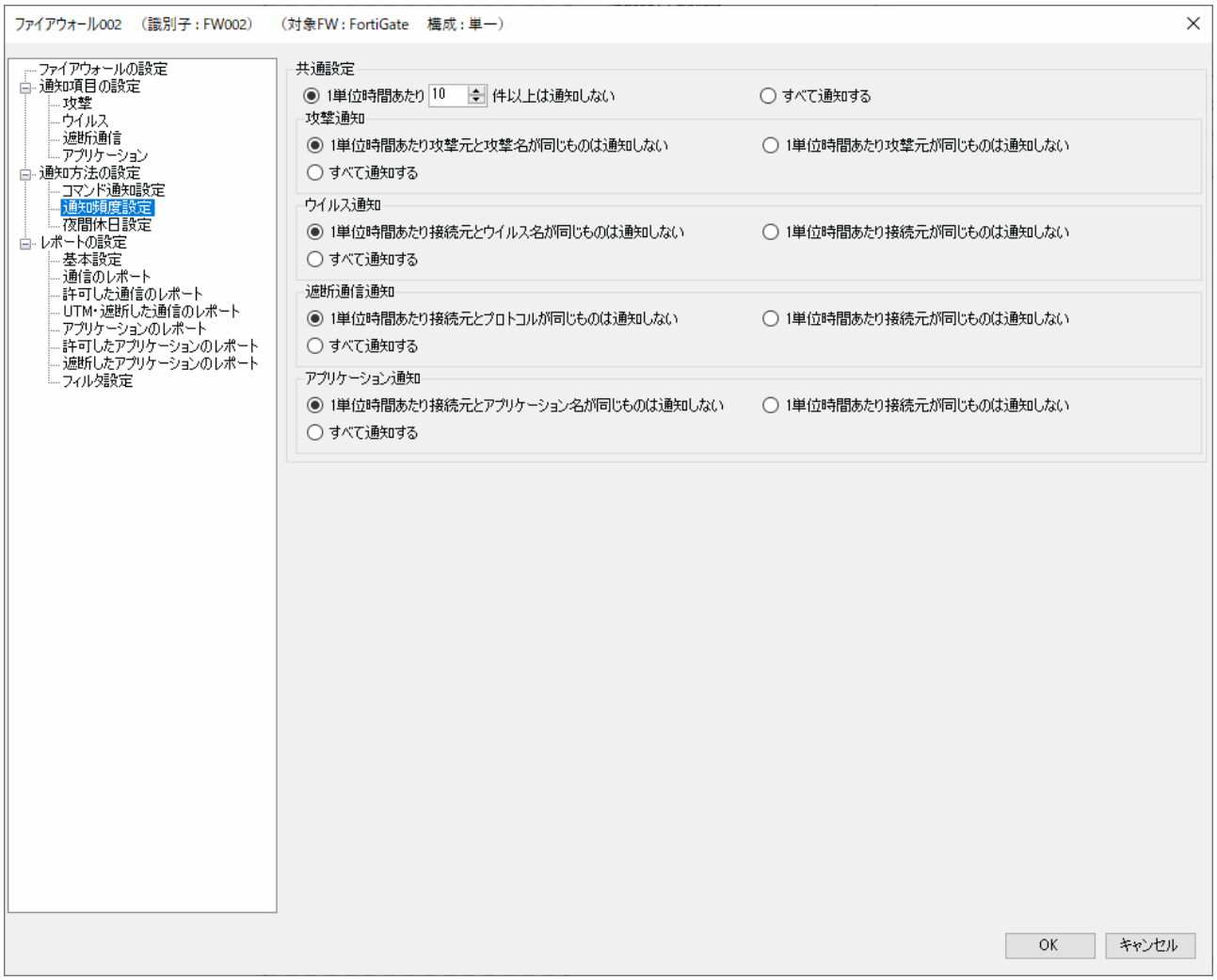


図 9 [通知方法の設定：通知頻度設定]パネル

(1) [共通設定]グループボックス

1 単位時間あたりに，最大通知する件数を指定します。

(a) [1 単位時間あたり XX 件以上は通知しない]ラジオボタン

1 単位時間あたりに通知する件数を制限する場合に選択します。さらに，1 時間あたりに通知する，最大数を指定します。

(b) [すべて通知する]ラジオボタン

1 単位時間あたりの通知数を制限せず，すべて通知する場合に選択します。

(2) [攻撃通知]グループボックス

攻撃の通知について指定します。

(a) [1 単位時間あたり攻撃元と攻撃名が同じものは通知しない]ラジオボタン

攻撃元と攻撃名が同じ攻撃を検知した場合，一度通知した後同一 1 単位時間内は通知しないようにする場合は，選択します。

(b) [1 単位時間あたり攻撃元が同じものは通知しない]ラジオボタン

攻撃元が同じ攻撃を検知した場合，一度通知した後同一 1 単位時間内は通知しないようにする場合は，選択します。

(c) [すべて通知する]ラジオボタン

攻撃を検知し常に通知する場合は，選択します。大量の通知が行われる可能性がありますので，選択する際は注意してください。

(3) [ウイルス通知]グループボックス

ウイルスの通知について指定します。

(a) [1 単位時間あたり送信元とウイルス名が同じものは通知しない]ラジオボタン

送信元とウイルス名が同じウイルスを検知した場合，一度通知した後同一 1 単位時間内は通知しないようにする場合は，選択します。

(b) [1 単位時間あたり送信元が同じものは通知しない]ラジオボタン

送信元が同じウイルスを検知した場合，一度通知した後同一 1 単位時間内は通知しないようにする場合は，選択します。

(c) [すべて通知する]ラジオボタン

ウイルスを検知し常に通知する場合は，選択します。大量の通知が行われる可能性がありますので，選択する際は注意してください。

(4) [遮断通信通知]グループボックス

遮断通信の通知について指定します。

(a) [1 単位時間あたり送信元とプロトコル名が同じものは通知しない]ラジオボタン

送信元とプロトコル名が同じ遮断通信を検知した場合，一度通知した後同一 1 単位時間内は通知しないようにする場合は，選択します。

(b) [1 単位時間あたり送信元が同じものは通知しない]ラジオボタン

送信元が同じ遮断通信を検知した場合，一度通知した後同一 1 単位時間内は通知しないようにする場合は，選択します。

(c) [すべて通知する]ラジオボタン

遮断通信を検知し常に通知する場合は，選択します。大量の通知が行われる可能性があり

ますので，選択する際は注意してください。

(5) [アプリケーション通知]グループボックス

アプリケーションの通知について指定します。このグループボックスは，FortiGate，Palo Alto，SRX，CheckPoint，IPCOM でのみ表示されます。

(a) [1 単位時間あたり送信元とアプリケーション名が同じものは通知しない]ラジオボタン

送信元とアプリケーション名が同じアプリケーションを検知した場合，一度通知した後同一 1 単位時間内は通知しないようにする場合は，選択します。

(b) [1 単位時間あたり送信元が同じものは通知しない]ラジオボタン

送信元が同じアプリケーションを検知した場合，一度通知した後同一 1 単位時間内は通知しないようにする場合は，選択します。

(c) [すべて通知する]ラジオボタン

アプリケーションを検知し常に通知する場合は，選択します。大量の通知が行われる可能性がありますので，選択する際は注意してください。

3.1.7　[通知方法の設定：夜間休日設定]パネル

FIREWALLstaff が検知した事項を，通知する場合，営業時間帯と夜間・休日の通知先を分けることができます。このパネルでは，夜間時間帯と休日を設定します。

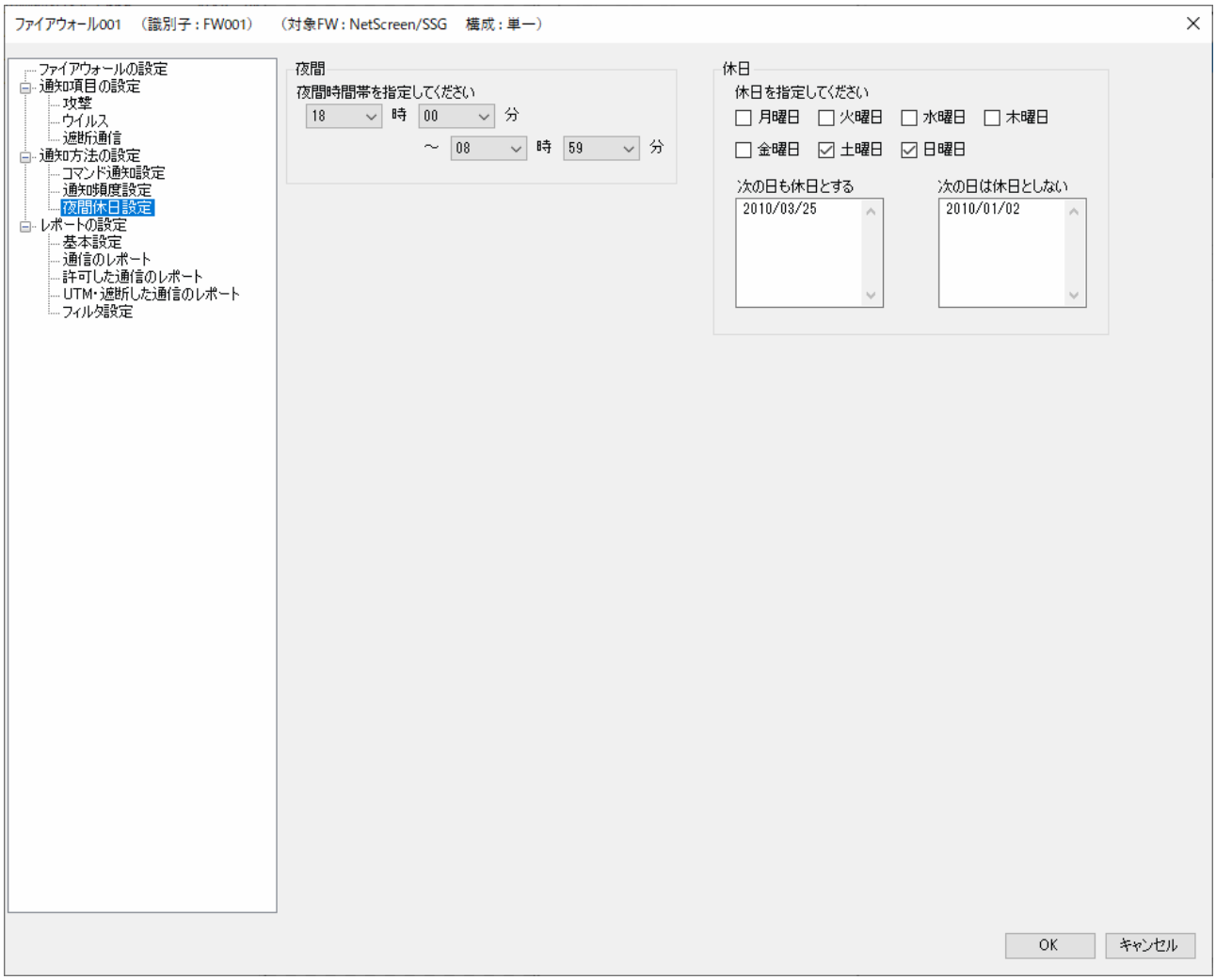


図 10 [通知方法の設定：夜間休日設定]パネル

(1) [夜間]グループボックス

夜間の時間帯を，24 時間制で指定してください。24 時をまたいで指定することができます。

例えば，[18]時[00]分～[08]時[59]分と指定した場合は，09 時 00 分 00 秒～17 時 59 分 59 秒が営業時間帯，18 時 00 分 00 秒～翌日 08 時 59 分 59 秒が夜間時間帯となります。

注　意

夜間の時間帯を指定しない場合は，[00]時[00]分～[00]時[00]分を指定してください。

(2) [休日]グループボックス

休日とする曜日を選択します。

(a) [次の日も休日とする]テキストボックス

月曜日～日曜日の選択だけでは指定しきれない特別な休日を，yyyy/mm/dd 形式で指定してください。複数指定する場合は，改行してください。

(b) [次の日は休日としない]テキストボックス

月曜日～日曜日の非選択だけでは指定しきれない特別な営業日を，yyyy/mm/dd 形式で指定してください。複数指定する場合は，改行してください。

[次の日も休日とする]テキストボックスと[次の日は休日としない]テキストボックスに同じ日付が指定された場合，[次の日は休日としない]テキストボックスの設定が優先されます。

4 「レポート」の設定

本章では，『4.1 レポート全般設定』～『4.4UTM・遮断した通信のレポート』は SRX の場合のダイアログ，『4.5 アプリケーションのレポート』～『4.7 遮断したアプリケーションのレポート』は PaloAlto の場合のダイアログ，で説明します。

4.1　レポート全般設定

4.1.1　[基本設定]パネル

レポート全般に関する設定をします。

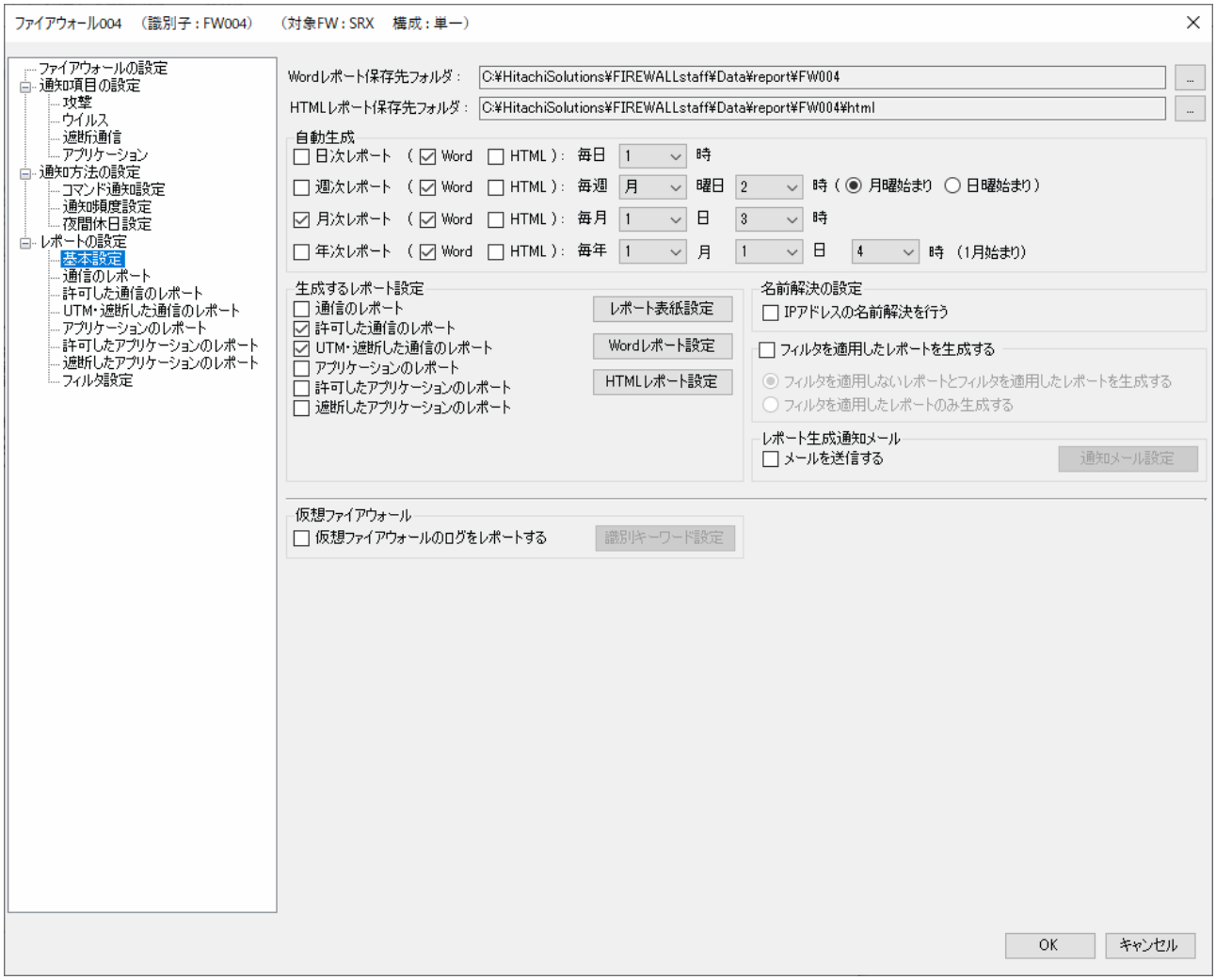


図 11 [基本設定]パネル

(1)　[Word レポート保存先フォルダ]テキストボックス

Word レポートを保存するフォルダを指定します。ローカルドライブのみ指定可能です。

(2)　[HTML レポート保存先フォルダ]テキストボックス

HTML レポートを保存するフォルダを指定します。ローカルドライブのみ指定可能です。

(3)　[自動生成]グループボックス

日次レポート，週次レポート，月次レポート，年次レポートを，作成開始する時刻を指定します（指定できる時刻は「時」単位で，「分」単位の指定はできません）。

[Word]チェックボックスを選択した場合は Word のレポートを，[HTML]チェックボックスを選択した場合は HTML のレポートを生成します。

(a) [日次レポート]チェックボックス

日次レポートを生成する場合に，選択します。また，前日分の日次レポートを作成開始する時刻を指定します。

(b) [週次レポート]チェックボックス

週次レポートを生成する場合に，選択します。また，前週分の週次レポートを作成開始する曜日と時刻を指定します。

- [月曜始まり]ラジオボタン
  週次レポートを，月曜日～日曜日を 1 週間とする場合に，選択します。
- [日曜始まり]ラジオボタン
  週次レポートを，日曜日～土曜日を 1 週間とする場合に，選択します。

(c) [月次レポート]チェックボックス

月次レポートを生成する場合に，選択します。また，前月分の月次レポートを作成開始する日と時刻を指定します。

(d) [年次レポート]チェックボックス

年次レポートを生成する場合に，選択します。[開始月]コンボボックスで選択した月を起点に 1 年間をレポート範囲とします。また，前年分の年次レポートを作成開始する日と時刻を指定します。

(4) [生成するレポート設定]グループボックス

生成するレポートを選択します。

項番	項目	生成するレポート
1	通信のレポート	「通信のレポート」を生成します
2	許可した通信のレポート	「許可した通信のレポート」を生成します
3	UTM・遮断した通信のレポート	「UTM・遮断した通信のレポート」を生成します
4	アプリケーションのレポート	「アプリケーションのレポート」を生成します
5	許可したアプリケーションのレポート	「許可したアプリケーションのレポート」を生成します
6	遮断したアプリケーションのレポート	「遮断したアプリケーションのレポート」を生成します

(a) [レポート表紙設定]ボタン

レポートの表紙のタイトル，ヘッダ，フッタを指定することができます。[レポート表紙設定]ボタンをクリックすると，[レポート表紙設定]パネルが表示されます。詳細は「4.1.2 [レポート表紙設定]パネル」を参照ください。

(b) [Word レポート設定]ボタン

Word レポートに関する設定を行います。[Word レポート設定]ボタンをクリックすると，[Word レポート設定]パネルが表示されます。詳細は「4.1.3 [Word レポート設定]パネル」を参照ください。

(c) [HTML レポート設定]ボタン

HTML レポートに関する設定を行います。[HTML レポート設定]ボタンをクリックすると，[HTML レポート設定]パネルが表示されます。詳細は「4.1.4 [HTML レポート設定]パネル」を参照ください。

(5) [名前解決の設定]グループボックス

レポート中の IP アドレスを名前解決する場合は，[IP アドレスの名前解決を行う]チェックボックスを選択します。なお，利用する DNS サーバは，FIREWALLstaff をインストールしたコンピュータで指定されている DNS サーバとなります。

名前解決は，IP アドレス毎に集計した後に行われます。異なる IP アドレスが同一の FQDN 名を持つ場合，レポート上では同じ名称が複数表示されることがあります。

(6) [フィルタを適用したレポートを生成する]チェックボックス

フィルタを適用したレポートを作成する場合に，選択します。フィルタの設定は，「4.8.1 [フィルタ設定]パネル」を参照してください。

(a) [フィルタを適用しないレポートとフィルタを適用したレポートを生成する]ラジオボタン

フィルタを適用しないレポートと，フィルタを適用したレポートの両方を生成する場合に選択します。

(b) [フィルタを適用したレポートを生成する]ラジオボタン

フィルタを適用したレポートのみを生成する場合に選択します。

(7) [レポート生成通知メール]グループボックス

レポートを生成したタイミングでメールを送信する場合は，[メールを送信する]チェックボックスを選択します。

(a) [通知メール設定]ボタン

通知メールに関する設定を行います。[通知メール設定]ボタンをクリックすると，[通知メール設定]パネルパネルが表示されます。詳細は「4.1.5 [通知メール設定]パネル」を参照ください。

(8) [仮想ファイアウォール]グループボックス

1 つのログファイルに複数の仮想ファイアウォールのログが含まれおり，仮想ファイアウォール別にレポートする場合は，[仮想ファイアウォールのログをレポートする]チェックボックスを選択します。

(a) [識別キーワード設定]ボタン

当該プロファイルに，特定の仮想ファイアウォールを紐付けるための設定を行います。[識別キーワード設定]ボタンをクリックすると，[識別キーワード設定]パネルが表示されます。詳細は「4.1.6 [識別キーワード設定]パネル」を参照ください。

レポートを作成する**仮想ファイアウォール台数分の，FIREWALLstaff ライセンスが必要**です。

4.1.2　[レポート表紙設定]パネル

「4.1.1(4) [生成するレポート設定]グループボックス」内の[レポート表紙設定]ボタンを押して[レポート表紙設定]パネルを起動します。

図 12 [レポート表紙設定]パネル

(1) [通信のレポート]グループボックス

「通信のレポート」の表紙の設定を行います。

(a) [タイトル]テキストボックス

レポート表紙のタイトルを指定します。最大 3 行指定でき，1 行あたり 50 文字まで指定できます。

(b) [ヘッダ]テキストボックス

レポート表紙のヘッダを指定します。最大 3 行指定でき，1 行あたり 30 文字まで指定できます。

(c) [フッタ]テキストボックス

レポート表紙のフッタを指定します。最大 3 行指定でき，1 行あたり 30 文字まで指定できます。

(d) [出力位置]グループボックス

出力位置を指定します。

- 左寄せ …出力位置を左に揃えます
- 中央…出力位置を中央に揃えます
- 右寄せ …出力位置を右に揃えます

(2) [許可した通信のレポート]グループボックス

「許可した通信のレポート」の表紙の設定を行います。

(3) [UTM・遮断した通信のレポート]グループボックス

「UTM・遮断した通信のレポート」の表紙の設定を行います。

(4) [アプリケーションのレポート]グループボックス

「アプリケーションのレポート」の表紙の設定を行います。

(5) [許可したアプリケーションのレポート]グループボックス

「許可したアプリケーションのレポート」の表紙の設定を行います。

(6) [遮断したアプリケーションのレポート]グループボックス

「遮断したアプリケーションのレポート」の表紙の設定を行います。

4.1.3　[Word レポート設定]パネル

「4.1.1(4) [生成するレポート設定]グループボックス」内の[Word レポート設定]ボタンを押して[Word レポート設定]パネルを起動します。

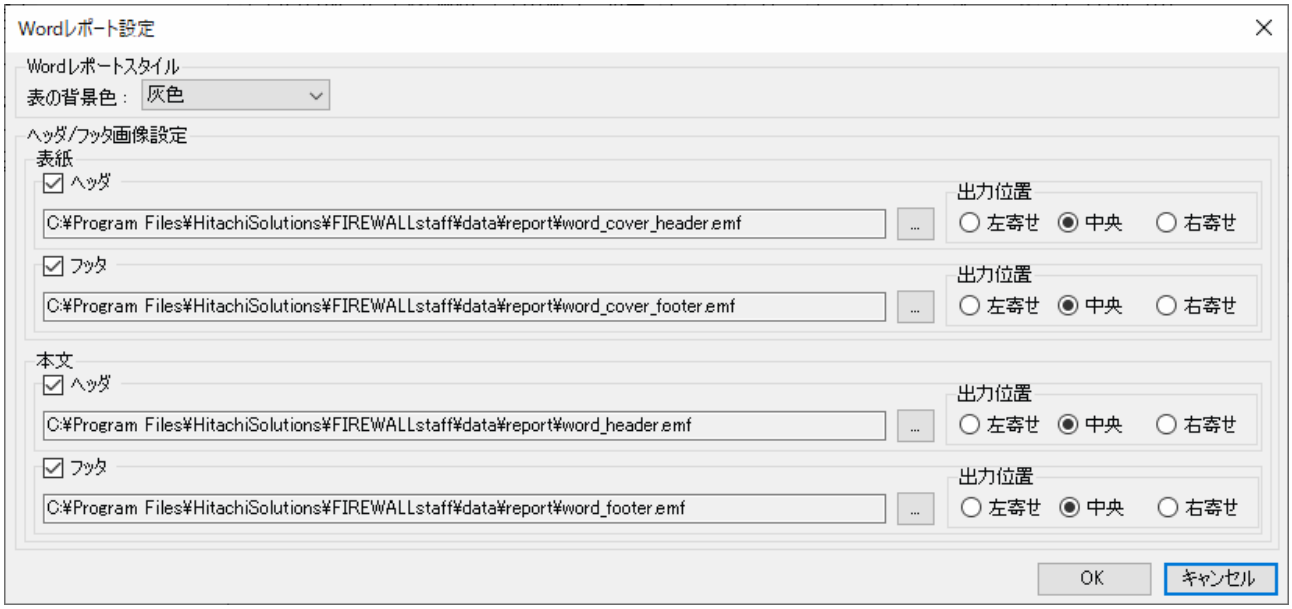


図 13 [Word レポート設定]パネル

(1) [Word レポートスタイル]グループボックス

(a) [表の背景色]コンボボックス

Word レポートの表のヘッダの背景色を指定します。

表 4.1-1 表の背景色

項番	選択項目	内容
1	なし	表のヘッダの背景色を指定しません
2	青色	表のヘッダの背景色として青色を指定します
3	赤色	表のヘッダの背景色として赤色を指定します
4	灰色	表のヘッダの背景色として灰色を指定します

(2) [ヘッダ/フッタ画像設定]グループボックス

Word レポートのヘッダ画像，フッタ画像の設定を行います。ヘッダ画像，フッタ画像を独自に用意する場合は，emf 形式の画像を準備してください。

(a) [表紙]グループボックス

表紙に使用するヘッダ画像，フッタ画像の設定を行います。

(b) [表紙]-[ヘッダ]グループボックス

表紙のヘッダに画像を使用する場合，チェックボックスをチェックします。[...]ボタンから画像を選択してください。[クリア]ボタンを押すとテキストボックス内の内容を削除します。出力位置として「左寄せ」，「中央」，「右寄せ」のいずれかを選択します。

(c) [表紙]-[フッタ]グループボックス

表紙のフッタに画像を使用する場合，チェックボックスをチェックします。[...]ボタンから画像を選択してください。[クリア]ボタンを押すとテキストボックス内の内容を削除します。出力位置として「左寄せ」，「中央」，「右寄せ」のいずれかを選択します。

(d) [本文]グループボックス

本文に使用するヘッダ画像，フッタ画像の設定を行います。

(e) [本文]-[ヘッダ]グループボックス

本文のヘッダに画像を使用する場合，チェックボックスをチェックします。[...]ボタンから画像を選択してください。[クリア]ボタンを押すとテキストボックス内の内容を削除します。出力位置として「左寄せ」，「中央」，「右寄せ」のいずれかを選択します。

(f) [本文]-[フッタ]グループボックス

本文のフッタに画像を使用する場合，チェックボックスをチェックします。[...]ボタンから画像を選択してください。[クリア]ボタンを押すとテキストボックス内の内容を削除します。出力位置として「左寄せ」，「中央」，「右寄せ」のいずれかを選択します。

4.1.4　[HTML レポート設定]パネル

「4.1.1(4) [生成するレポート設定]グループボックス」内の[HTML レポート設定]ボタンを押して[HTML レポート設定]パネルを起動します。

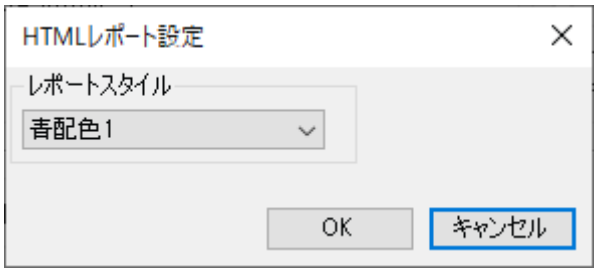


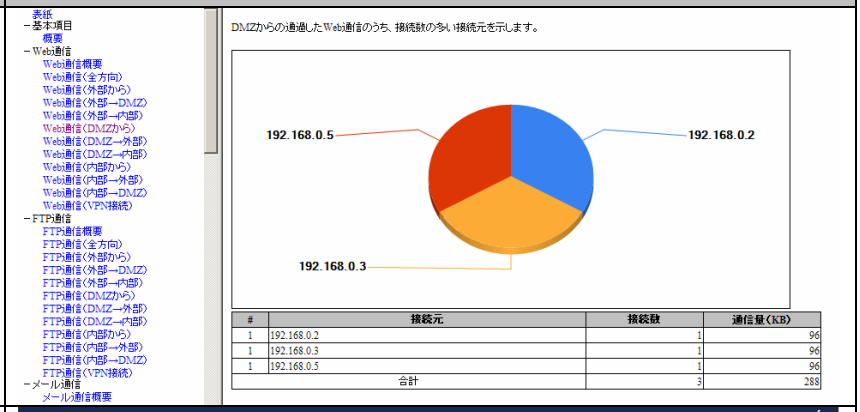
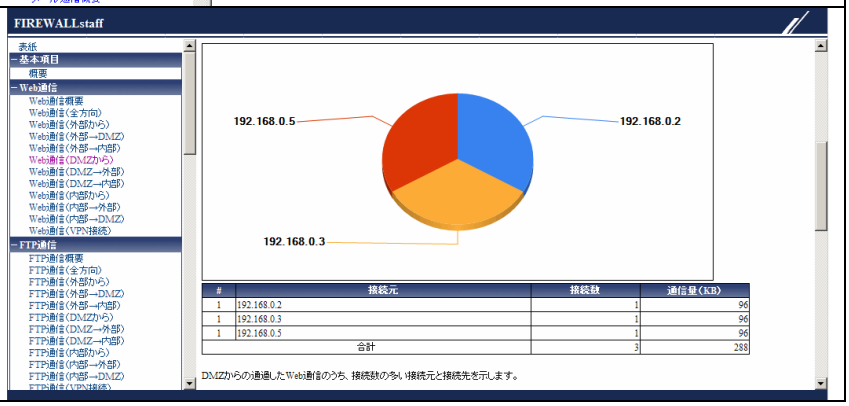
図 14 [HTML レポート設定]パネル

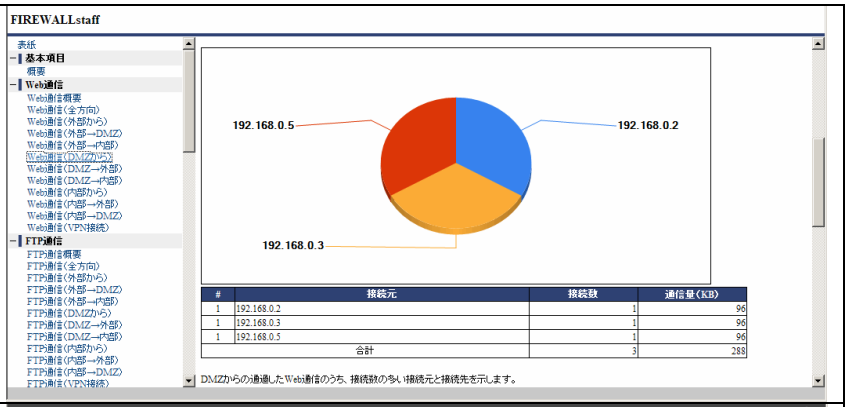
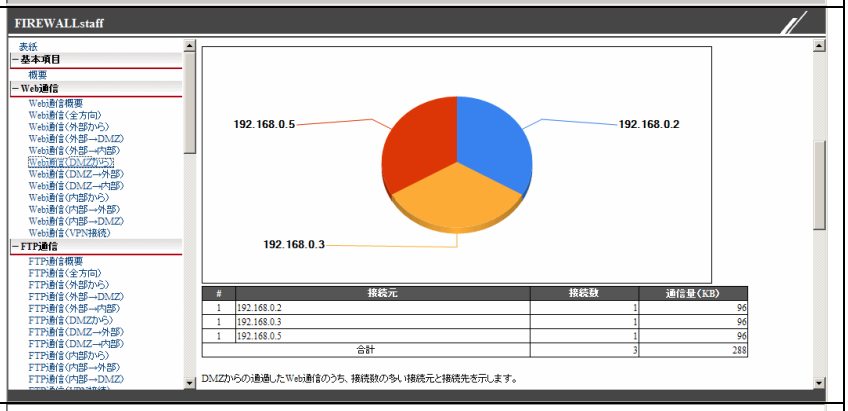
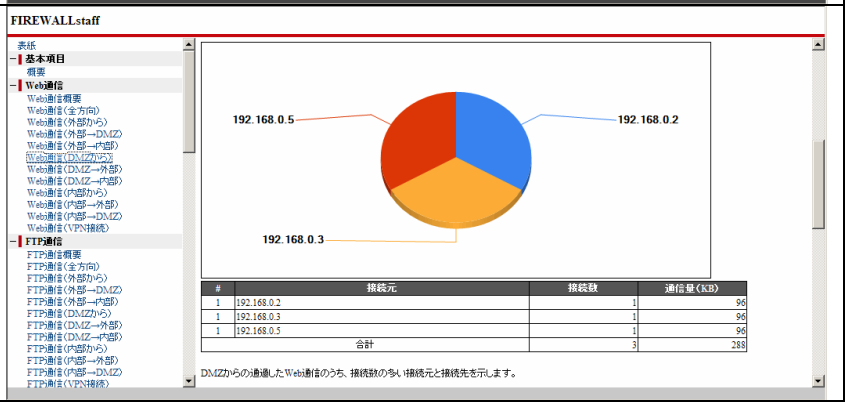
(1) [レポートスタイル]グループボックス

(a) [レポートスタイル]コンボボックス

HTML レポートのスタイルの設定を行います。必要に応じて，指定してください。選択可能な項目は以下のとおりです。

表 4.1-2 表の背景色

項番	スタイル	イメージ
1	なし	
2	青配色 1	

3	青配色 2	
4	赤配色 1	
5	赤配色 2	

4.1.5　[通知メール設定]パネル

「4.1.1(7)[レポート生成通知メール]グループボックス」内の[通知メール設定]ボタンを押して[通知メール設定]パネルを起動します。

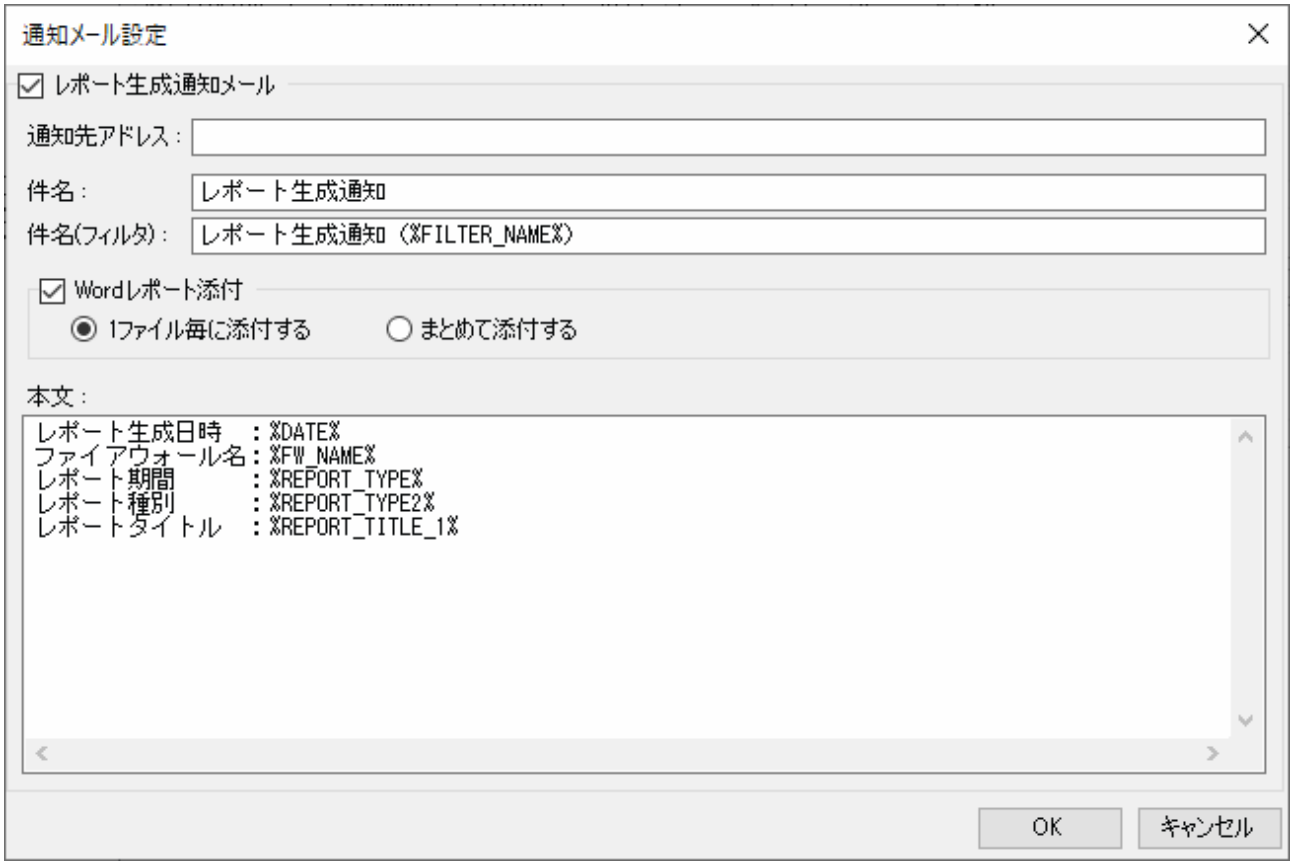


図 15 [通知メール設定]パネル

(1) [レポート生成通知メール]チェックボックス

レポート生成のタイミングでメール通知する場合に選択します。

(a) [通知先アドレス]テキストボックス

送信するメールアドレスを指定します。「,」（カンマ）区切りで，最大 10 まで指定できます。

(b) [件名]テキストボックス

レポートの生成通知メールの件名を指定します。最大 200 文字まで指定できます。

(c) [件名（フィルタ）]テキストボックス

フィルタしたレポートの生成通知メールの件名を指定します。最大 200 文字まで指定できます。

(d) [Word レポート添付]チェックボックス

生成した Word レポートを通知メールに添付する場合に選択します。

- [1 ファイル毎に添付する]ラジオボタン

1 メールに 1 ファイルを添付する場合に選択します。ファイル数のメールが送られます。

- [まとめて添付する]ラジオボタン

  1 メールにすべてのファイルを添付する場合に選択します。

(e) [本文]テキストボックス

メールの本文を指定します。最大 4000 文字まで指定できます。送信するメールの件名と本文には，次の変数を使用することができます。

変数名	内容
%DATE%	「yyyy/mm/dd HH:mm:ss」形式の日時
%FW_NAME%	FIREWALLstaff におけるファイアウォール名
%REPORT_TYPE%	「日次」「週次」「月次」「年次」のいずれか
%REPORT_TYPE2%	「通信のレポート」「許可した通信のレポート」「UTM・遮断した通信のレポート」「アプリケーションのレポート」「許可したアプリケーションのレポート」「遮断したアプリケーションのレポート」のいずれか 【注意】[Word レポート添付]を選択し，[1 ファイル毎に添付する]を選択した場合のみ有効
%REPORT_TITLE_1%	レポート表紙のタイトル(4.1.2 [レポート表紙設定]パネル参照)の 1 行目 【注意】[Word レポート添付]を選択し，[1 ファイル毎に添付する]を選択した場合のみ有効
%REPORT_TITLE_ALL%	レポート表紙のタイトル(4.1.2 [レポート表紙設定]パネル参照) 【注意】[Word レポート添付]を選択し，[1 ファイル毎に添付する]を選択した場合のみ有効
%FILTER_NAME%	フィルタ名(4.8.1(2)(a) [フィルタ名]テキストボックス参照)

注　意

送信されるメールの数は，次となります。

項番	条件	メールの数
1	[Word レポート添付]を選択していない場合	1
2	[Word レポート添付]を選択し，[1 ファイル毎に添付する]を選択した場合	A×B
3	[Word レポート添付]を選択し，[まとめて添付する]を選択した場合	A

A:「フィルタなし」「フィルタ 1」～「フィルタ 5」の内，レポート作成を行う数（最大 6）
B:生成するレポートの数（4.1.1(4) [生成するレポート設定]グループボックスで選択した数）

4.1.6　[識別キーワード設定]パネル

「4.1.1(8) [仮想ファイアウォール]グループボックス」内の[識別キーワード設定]ボタンを押して[識別キーワード設定]パネルを起動します。

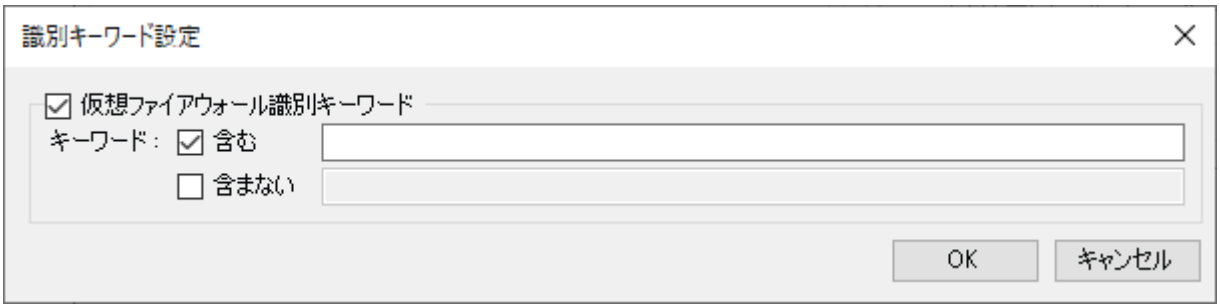


図 16 [識別キーワード設定]パネル

(1) [仮想ファイアウォール識別キーワード]チェックボックス

1 ファイルに複数の仮想ファイアウォールのログがまとまっており，仮想ファイアウォールごとにレポートする場合に選択します。

特定の仮想ファイアウォールのログ（レコード）を抽出するための[キーワード]を，[含む][含まない]テキストボックスに指定します。[含む][含まない]両方を指定した場合は，AND となります。

(a) [含む]テキストボックス

キーワードを「|」（パイプライン）区切りで，複数指定できます。複数指定した場合は，指定したキーワードのいずれかを含むレコードがレポート対象となります。

(b) [含まない]テキストボックス

キーワードを「|」（パイプライン）区切りで，複数指定できます。複数指定した場合は，指定したキーワードのいずれも含まないレコードがレポート対象となります。

注　意

「|」（パイプライン）をキーワードに含めることはできません。

4.2　通信のレポート

ファイアウォールが出力する「トラフィックログ」を集計対象とします。

4.2.1　[通信のレポート]パネル

「通信のレポート」に含めるレポート項目について設定します。[通信のレポート]パネルを図 17 に示します。

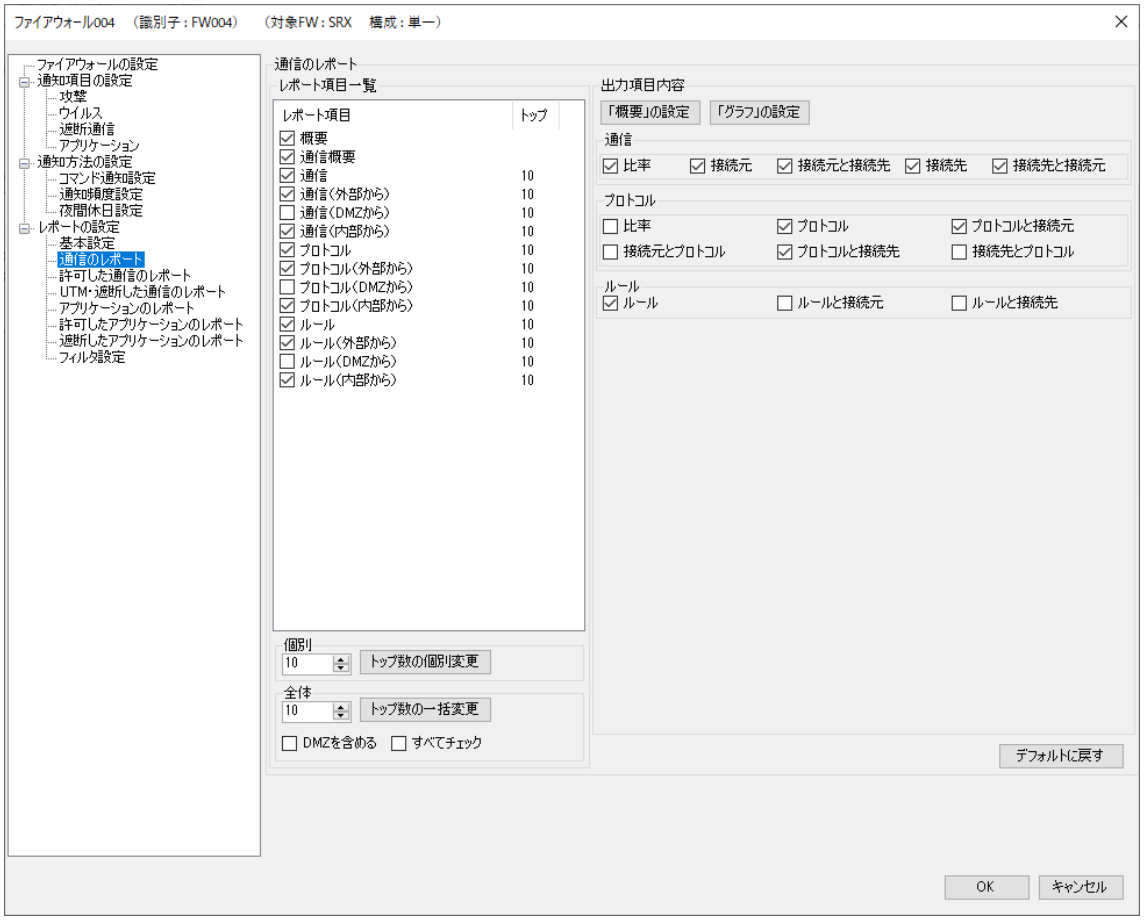


図 17 [通信のレポート]パネル

(1)　[レポート項目一覧]グループボックス

レポートに含めるレポート項目，および各レポート項目に含める表のトップ数を指定します。

(a)　[個別]グループボックス

レポート項目一覧にてトップ数を変更したいレポート項目を選択し，スピンボックスに変更したい値を入力して[トップ数の個別変更]ボタンを押します。1～100 が指定可能です。

(b) [全体]グループボックス

すべてのレポート項目のトップ数を一度に変更したい場合，スピンボックスに変更したい

値を入力して[トップ数の一括変更]ボタンを押します。1～100 が指定可能です。

「[DMZ を含める]チェックボックス」をチェックすると，DMZ を含むすべてのレポート項目がチェックされます。チェックを外すと通信方向に DMZ を含むすべてのレポート項目のチェックが外れます。

「[すべてチェック]チェックボックス」をチェックすると，すべてのレポート項目がチェックされます。チェックを外すとすべてのレポート項目のチェックが外れます。

(2) [グラフの設定]ボタン

レポートに出力するグラフを指定します。[グラフの設定]ボタンをクリックすると，[グラフの設定]パネルが表示されます。詳細は「4.2.3 [「グラフ」の設定]パネル」を参照ください。

(3) [通信]グループボックス

通信に関するレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	比率	通過した通信と遮断した通信の比率の表
2	接続元	接続元を基準として集計した表
3	接続元と接続先	接続元を基準とし，その接続元がどの接続先にアクセスしたかを集計した表
4	接続先	接続先を基準として集計した表
5	接続先と接続元	接続先を基準とし，その接続先がどの接続元からアクセスされたかを集計した表

(4) [プロトコル]グループボックス

プロトコルに関するレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	比率	通過した通信と遮断した通信の比率の表
2	プロトコル	プロトコルを基準として集計した表
3	プロトコルと接続元	プロトコルを基準とし，そのプロトコルを用いてどの接続元からアクセスされたかを集計した表
4	接続元とプロトコル	接続元を基準とし，その接続元がどのプロトコルを用いてアクセスしたかを集計した表
5	プロトコルと接続先	プロトコルを基準とし，そのプロトコルを用いてどの接続先にアクセスしたかを集計した表
6	接続先とプロトコル	接続先を基準とし，その接続先がどのプロトコルを用いてアクセスされたかを集計した表

(5) [ルール]グループボックス

ルールに関するレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	ルール	ルールを基準として集計した表
2	ルールと接続元	ルールを基準とし，そのルールが適用された通信の接続元も集計した表
3	ルールと接続先	ルールを基準とし，そのルールが適用された通信の接続先も集計した表

(6) [デフォルトに戻す]ボタン

レポート項目の選択状態とトップ数の値，各グループボックス内の設定をデフォルト値に戻します。

4.2.2 [「概要」の設定]パネル

「概要」レポート項目に出力する内容を設定します。

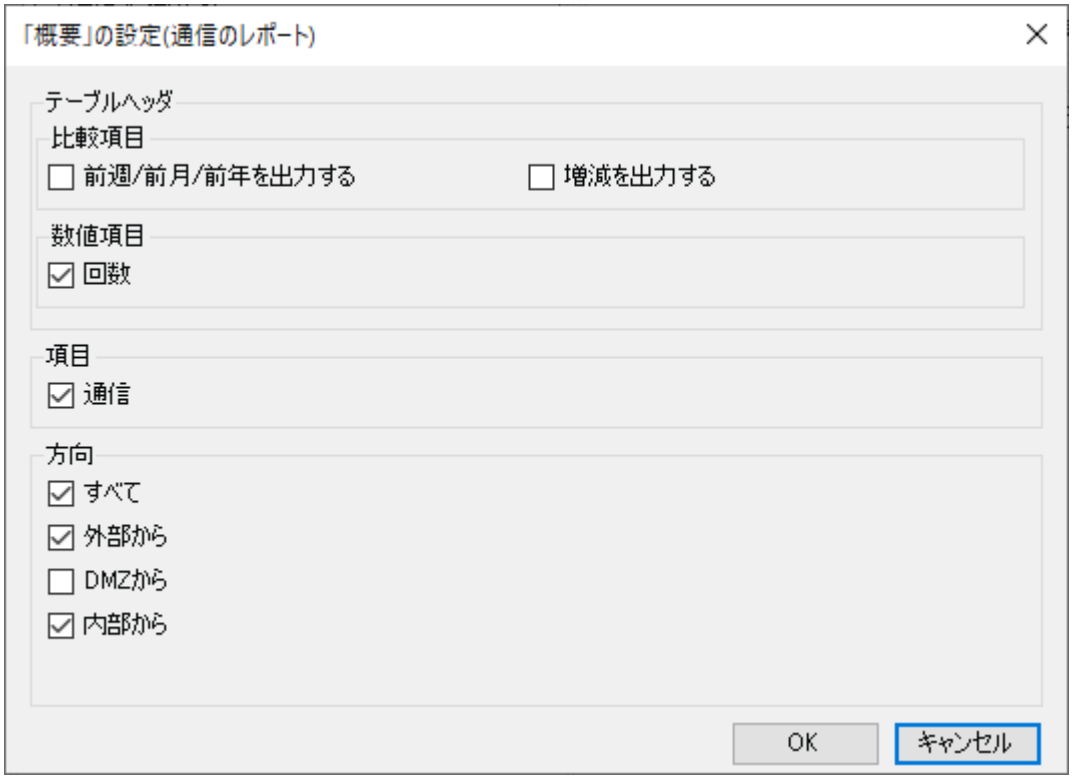


図 18 [「概要」の設定]パネル

(1) [ヘッダ]グループボックス

「概要」レポート項目は，表からなります。出力する列に関する設定を行います。

項番	項目	レポートの内容
1	前週/前月/前年を出力する	前週/前月/前年の情報を出力
2	増減を出力する	増減を出力

項番	項目	レポートの内容
1	回数	回数を出力

(2) [項目]グループボックス

「概要」レポート項目に出力する，項目に関する設定を行います。

項番	項目	レポートの内容
1	通信	通信に関する項目を出力

項番	項目	レポートの内容
1	すべて	すべての通信について集計した結果を出力
2	外部から	外部からの通信について集計した結果を出力
3	DMZ から	DMZ からの通信について集計した結果を出力
4	内部から	内部からの通信について集計した結果を出力

4.2.3 ［「グラフ」の設定]パネル

「通信のレポート」に含めるグラフについて設定します。

図 19 [「グラフ」の設定]パネル

(1) ［通信]グループボックス

通信に関するレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	回数の時系列のグラフ
2	比率	通過した通信と遮断した通信の比率を示す円グラフ
3	接続元（時系列）	接続元（トップ 5）の時系列のグラフ
4	接続元（棒）	接続元（トップ 10）の棒グラフ
5	接続元（円）	接続元（トップ 10）の円グラフ
6	接続先（時系列）	接続先（トップ 5）の時系列のグラフ
7	接続先（棒）	接続先（トップ 10）の棒グラフ
8	接続先（円）	接続先（トップ 10）の円グラフ

(a) [概要]グループボックス

「xxxxx 概要」レポート項目に含める内容を指定します。

項番	項目	グラフの内容
1	ゾーン別	接続元別の時系列グラフ

項番	項目	レポートの内容
1	DMZ	グラフから，DMZ を除く

(2) ［プロトコル]グループボックス

プロトコルのレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容

1	時系列	回数の時系列のグラフ
2	比率	通過した通信と遮断した通信の比率を示す円グラフ
3	プロトコル（時系列）	プロトコル（トップ 5）の時系列のグラフ
4	プロトコル（棒）	プロトコル（トップ 10）の棒グラフ
5	プロトコル（円）	プロトコル（トップ 10）の円グラフ

(3) [ルール]グループボックス

ルールのレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
2	ルール（時系列）	ルール（トップ 5）の時系列のグラフ
3	ルール（棒）	ルール（トップ 10）の棒グラフ
4	ルール（円）	ルール（トップ 10）の円グラフ

4.3　許可した通信のレポート

ファイアウォールが出力する「トラフィックログ」の内，ファイアウォールが許可したトラフィックのログを集計対象とします。

4.3.1　[許可した通信のレポート]パネル

「許可した通信のレポート」に含めるレポート項目について設定します。

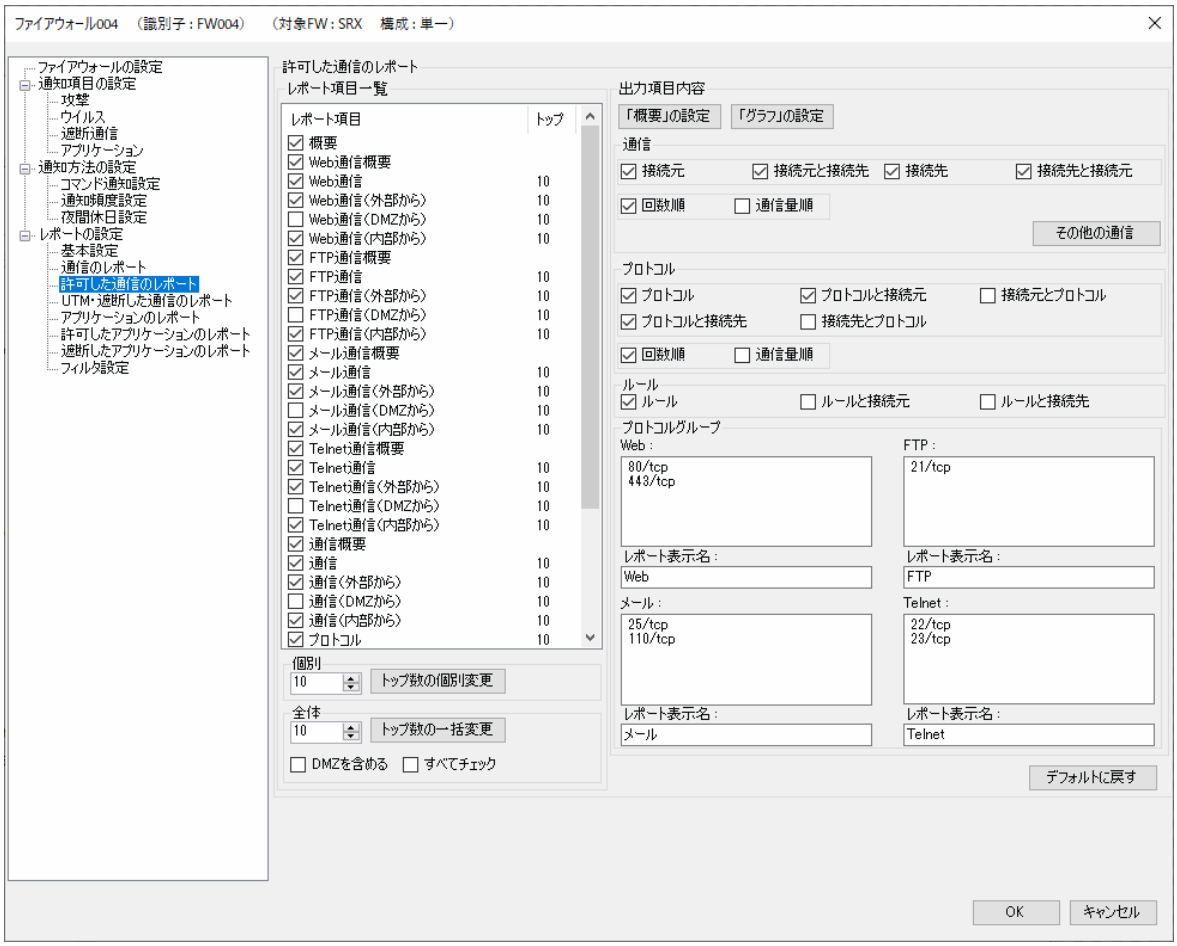


図 20 [許可した通信のレポート]パネル

(1)　[レポート項目一覧]グループボックス

「4.2.1 [通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2)　[概要の設定]ボタン

「概要」レポート項目に出力する内容を指定します。[「概要」の設定]ボタンをクリックすると，[「概要」の設定]パネルが表示されます。詳細は「4.3.2 [「概要」の設定]パネル」を参照ください。

(3) [「グラフ」の設定]ボタン

レポートに出力するグラフを指定します。[「グラフ」の設定]ボタンをクリックすると，[「グラフ」の設定]パネルが表示されます。詳細は「4.3.3 [「グラフ」の設定]パネル」を参照ください。

(4) [通信]グループボックス

通信に関するレポート項目において，レポートに含める内容と集計方法を指定します。

項番	項目	レポートの内容
1	接続元	接続元を基準として集計した表
2	接続元と接続先	接続元を基準とし，その接続元がどの接続先にアクセスしたかを集計した表
3	接続先	接続先を基準として集計した表
4	接続先と接続元	接続先を基準とし，その接続先がどの接続元からアクセスされたかを集計した表

項番	項目	集計方法
1	回数順	接続数の多い順に集計
2	通信量順	通信量の多い順に集計

(a) [その他の通信]ボタン

デフォルトで定義された Web，FTP，メール，Telnet 以外に集計対象としたいプロトコルを定義してレポートを作成することができます。[その他の通信]ボタンをクリックすると，[その他の通信]パネルが表示されます。詳細は「4.3.4 [その他の通信]パネル」を参照ください。

(5) [プロトコル]グループボックス

プロトコルに関するレポート項目において，レポートに含める内容と集計方法を指定します。

項番	項目	レポートの内容
1	プロトコル	プロトコルを基準として集計した表
2	プロトコルと接続元	プロトコルを基準とし，そのプロトコルを用いてどの接続元からアクセスされたかを集計した表
3	接続元とプロトコル	接続元を基準とし，その接続元がどのプロトコルを用いてアクセスしたかを集計した表
4	プロトコルと接続先	プロトコルを基準とし，そのプロトコルを用いてどの接続先にアクセスしたかを集計した表
5	接続先とプロトコル	接続先を基準とし，その接続先がどのプロトコルを用いてアクセスされたかを集計した表

項番	項目	集計方法
1	回数順	接続数の多い順に集計
2	通信量順	通信量の多い順に集計

(6) [ルール]グループボックス

ルールに関するレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	ルール	ルールを基準として集計した表
2	ルールと接続元	ルールを基準とし，そのルールが適用された通信の接続元も集計した表
3	ルールと接続先	ルールを基準とし，そのルールが適用された通信の接続先も集計した表

(7) [プロトコルグループ]グループボックス

「許可した通信のレポート」において，「Web」「メール」「FTP」「TELNET」と判断するプロトコル（ポート番号）を指定します。複数指定する場合は，改行で区切ってください。指定方法は，次のとおりです。

表 4.3-1 プロトコル（ポート番号）の指定方法

項番	ファイアウォール	指定方法
1	NetScreen/SSG FortiGate Palo Alto SRX CheckPoint IPCOM Cisco	宛先ポート番号と TCP/UDP 種別を，次の形式で指定してください。複数指定する場合は，改行で区切ってください tcp/宛先ポート番号　または　宛先ポート番号/tcp udp/宛先ポート番号　または　宛先ポート番号/udp 例）tcp/25 25/tcp udp/53 53/udp また，宛先ポート番号をレンジ指定することも可能です。その場合は， (宛先ポート番号-宛先ポート番号) と指定してください。 例）tcp/(5001-6000) (6001-8000)/udp

(a) [Web]テキストボックス

レポートにおいて，Web 通信と判断する通信を指定します。

(b) [FTP]テキストボックス

レポートにおいて，FTP 通信と判断する通信を指定します。

(c) [メール]テキストボックス

レポートにおいて，メール通信と判断する通信を指定します。

(d) [Telnet]テキストボックス

レポートにおいて，Telnet 通信と判断する通信を指定します。

注 意

「Web」「FTP」「メール」「Telnet」に加えて，最大 6 通信までレポートすることができます。設定方法は，「4.3.4 [その他の通信]パネル」を参照ください。

(8) [デフォルトに戻す]ボタン

レポート項目の選択状態とトップ数の値，各グループボックス内の設定をデフォルト値に戻します。

4.3.2 [「概要」の設定]パネル

「概要」レポート項目に出力する内容を設定します。

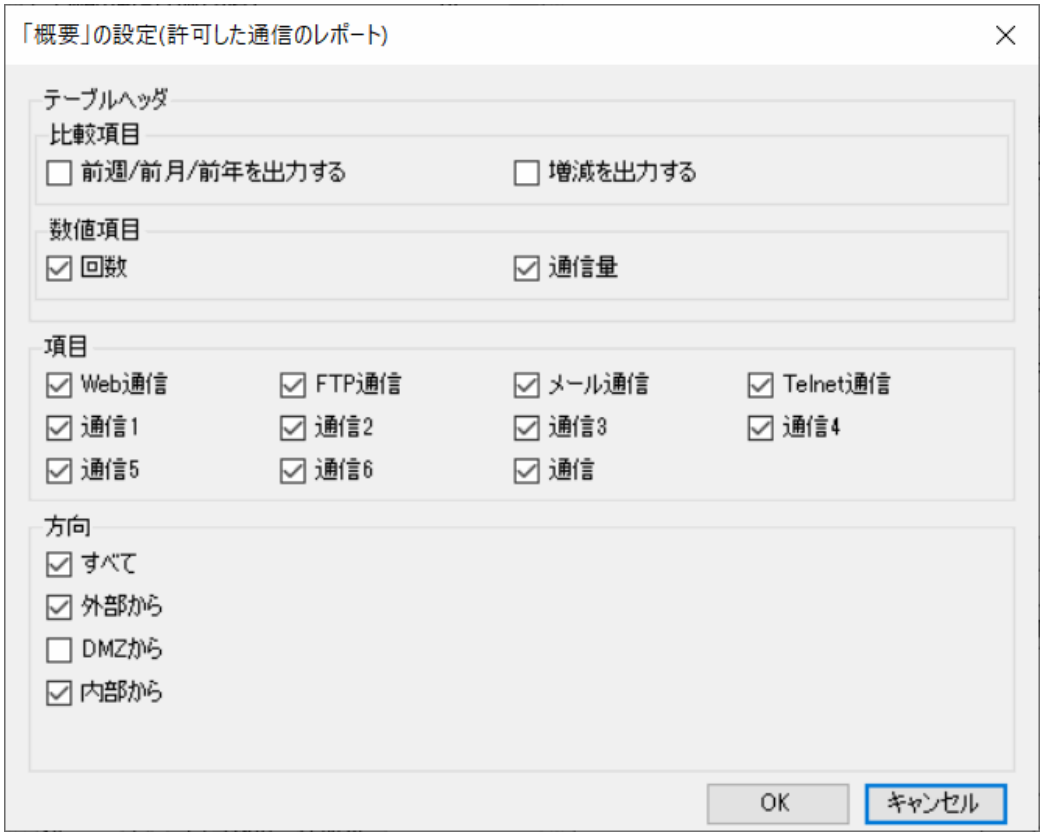


図 21 [「概要」の設定]パネル

(1) [ヘッダ]グループボックス

「概要」レポート項目は，表からなります。出力する列に関する設定を行います。

項番	項目	レポートの内容
1	前週/前月/前年を出力する	前週/前月/前年の情報を出力
2	増減を出力する	増減を出力

項番	項目	レポートの内容
1	回数	回数を出力
2	通信量	通信量を出力

(2) [項目]グループボックス

「概要」レポート項目に出力する，項目に関する設定を行います。

項番	項目	レポートの内容

1	Web 通信	Web に関する項目を出力
2	FTP 通信	FTP に関する項目を出力
3	メール通信	メールに関する項目を出力
4	Telnet 通信	Telnet に関する項目を出力
5	通過通信 *n*	通信 *n* に関する項目を出力
6	通過通信	通過した通信に関する項目を出力

項番	項目	レポートの内容
1	すべて	すべての通信について集計した結果を出力
2	外部から	外部からの通信について集計した結果を出力
3	DMZ から	DMZ からの通信について集計した結果を出力
4	内部から	内部からの通信について集計した結果を出力

[通信 1～6]チェックボックスをチェックしていても，対応するプロトコルの定義がない場合は出力されません。対応するプロトコルの定義については，「4.3.4 [その他の通信]パネル」を参照ください。

4.3.3 ［「グラフ」の設定］パネル

「通信のレポート」に含めるグラフについて設定します。

図 22［「グラフ」の設定］パネル

(1) ［通信］グループボックス

通信に関するレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	回数，通信量の時系列のグラフ
2	接続元（時系列）	接続元（トップ 5）の時系列のグラフ
3	接続元（棒）	接続元（トップ 10）の棒グラフ
4	接続元（円）	接続元（トップ 10）の円グラフ
5	接続先（時系列）	接続先（トップ 5）の時系列のグラフ
6	接続先（棒）	接続先（トップ 10）の棒グラフ
7	接続先（円）	接続先（トップ 10）の円グラフ

(a) ［概要］グループボックス

「xxxxx 概要」レポート項目に含める内容を指定します。

項番	項目	グラフの内容
1	ゾーン別	接続元別の回数，通信量の時系列グラフ

項番	項目	レポートの内容
1	DMZ	グラフから，DMZ を除く

(2) ［プロトコル］グループボックス

プロトコルのレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	回数，通信量の時系列のグラフ

2	プロトコル（時系列）	プロトコル（トップ 5）の時系列のグラフ
3	プロトコル（棒）	プロトコル（トップ 10）の棒グラフ
4	プロトコル（円）	プロトコル（トップ 10）の円グラフ

(3) [ルール]グループボックス

ルールのレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
2	ルール（時系列）	ルール（トップ 5）の時系列のグラフ
3	ルール（棒）	ルール（トップ 10）の棒グラフ
4	ルール（円）	ルール（トップ 10）の円グラフ

4.3.4　[その他の通信]パネル

Web，FTP，メール，Telnet に加えて，集計対象としたいプロトコルを設定します。

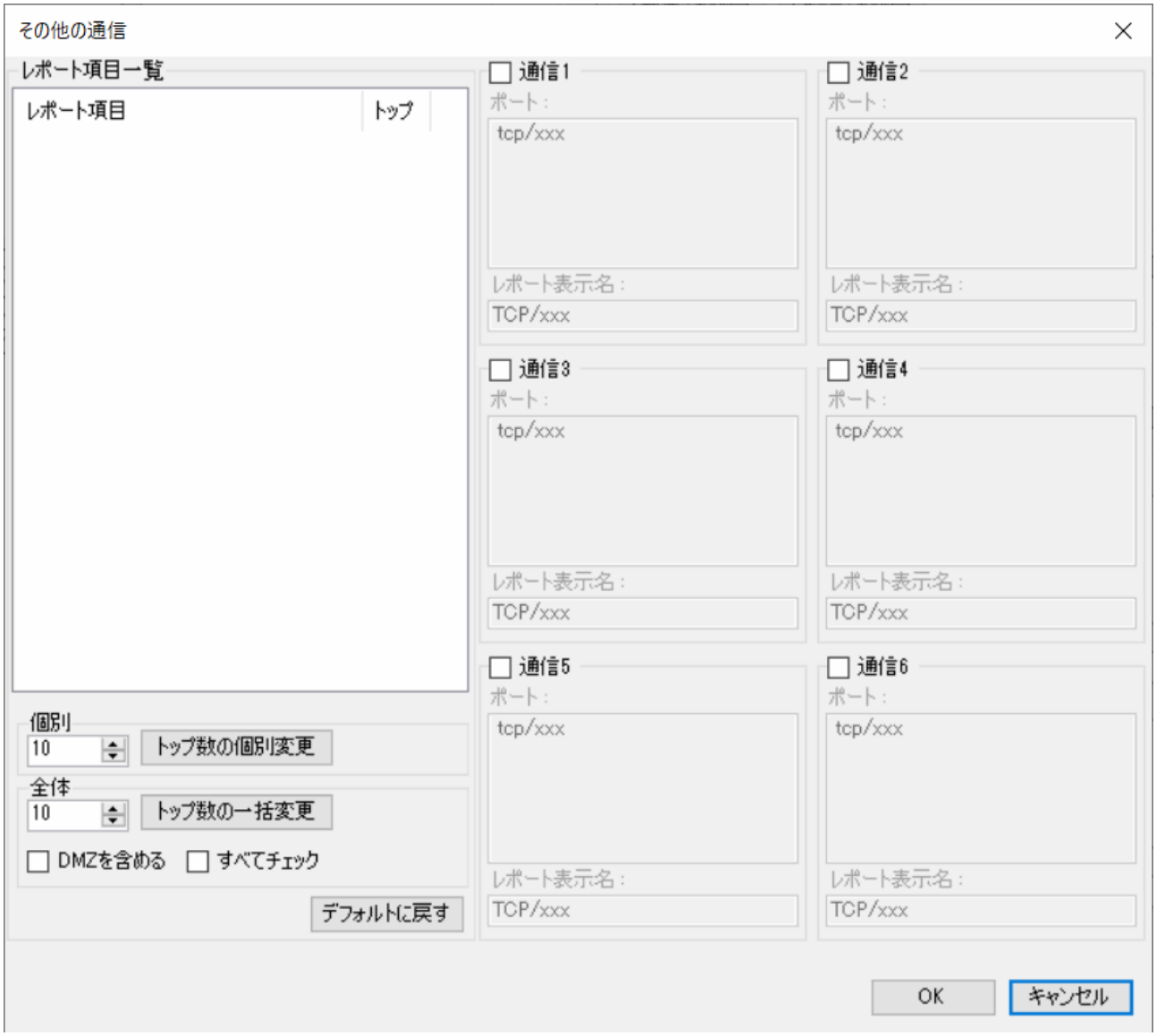


図 23 [その他の通信]パネル

(1) [レポート項目一覧]グループボックス

「4.2.1 [通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2) [通信 *n*]グループボックス

指定したプロトコルの通信を集計します。

[通信 *n*]チェックボックスをチェックすると，[プロトコル]テキストボックスと[レポー

ト表示名]テキストボックスが活性状態になります。

項番	項目	指定する内容
1	プロトコル	集計対象とするプロトコル（またはポート番号） 例）tcp/80 指定方法は，「表 4.3-1 プロトコル（ポート番号）の指定方法」を参照
2	レポート表示名	レポート中に使用する表示名 例）TCP/80

4.4　UTM・遮断した通信のレポート

ファイアウォールが出力する「UTM 機能のログ」と，ファイアウォールが出力する「トラフィックログ」の内，ファイアウォールが遮断したトラフィックのログを集計対象とします。

4.4.1　[UTM・遮断した通信のレポート]パネル

「UTM・遮断した通信のレポート」に含めるレポート項目について設定します。

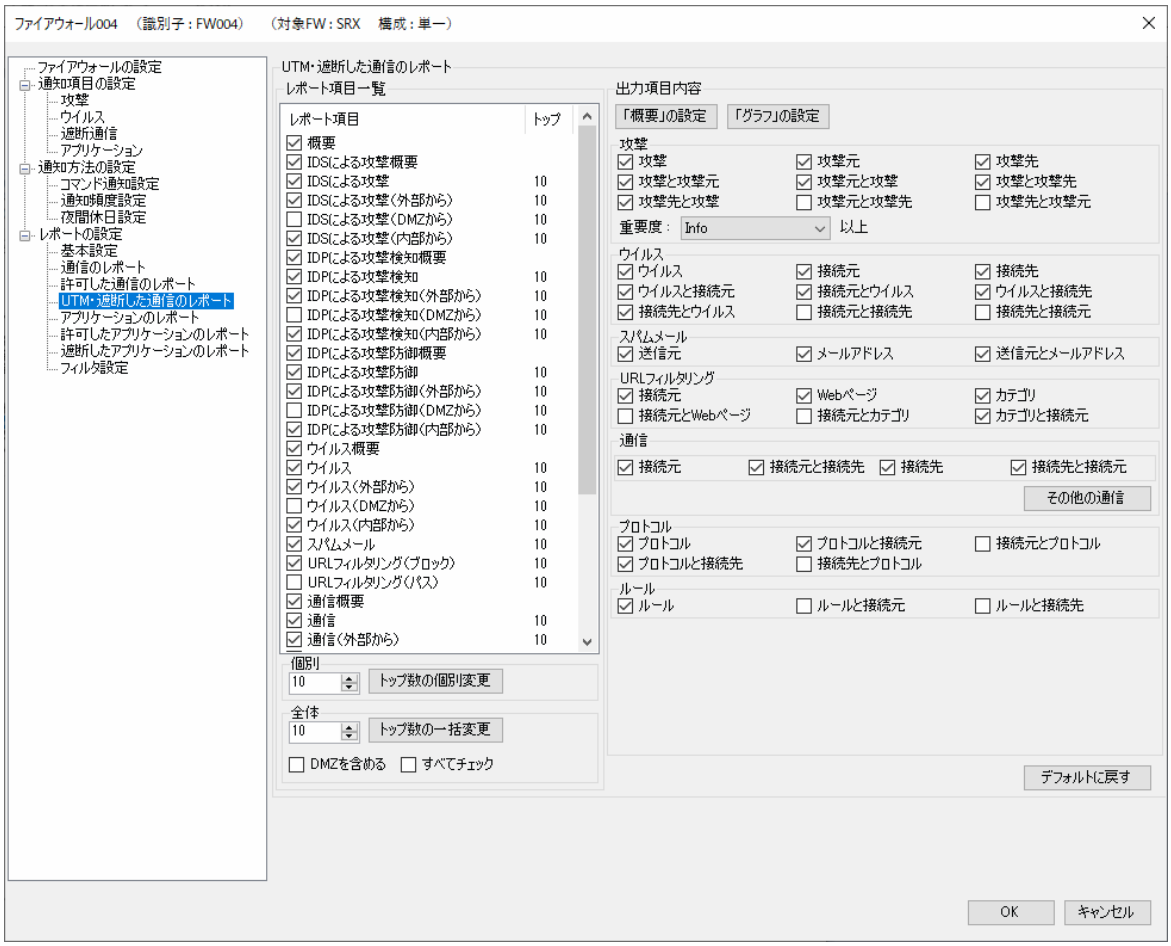


図 24 [UTM・遮断した通信のレポート]パネル

(1) [レポート項目一覧]グループボックス

「4.2.1 [通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2) [「概要」の設定]ボタン

「概要」レポート項目に出力する内容を指定します。[「概要」の設定]ボタンをクリックすると，[「概要」の設定]パネルが表示されます。詳細は「4.3.2 [「概要」の設定]パネル」を参照ください。

(3) [「グラフ」出力設定]ボタン

レポートに出力するグラフを指定します。[「グラフ」の設定]ボタンをクリックすると，[「グラフ」の設定]パネルが表示されます。詳細は「4.4.3 [「グラフ」の設定]パネル」を参照ください。

(4) [攻撃]グループボックス

攻撃に関するレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	攻撃	攻撃を基準として集計した表
2	攻撃元	攻撃元を基準として集計した表
3	攻撃先	攻撃先を基準として集計した表
4	攻撃と攻撃元	攻撃を基準とし，その攻撃がどの攻撃元から行われたかを集計した表
5	攻撃元と攻撃	攻撃元を基準とし，その攻撃元からどの攻撃が行われたかを集計した表
6	攻撃と攻撃先	攻撃を基準とし，その攻撃が行われた攻撃先を集計した表
7	攻撃先と攻撃	攻撃先を基準とし，その攻撃先にどの攻撃が行われたかを集計した表
8	攻撃元と攻撃先	攻撃元を基準とし，その攻撃がどの攻撃先に行われたかを集計した表
9	攻撃先と攻撃元	攻撃先を基準とし，その攻撃がどの攻撃元から行われたかを集計した表

(a) [重要度]コンボボックス

攻撃のレコード中に記録されている重要度を元に，指定した重要度以上のレコードのみを集計対象とすることができます。但し，重要度が記録されていないレコード（NetScrenn/SSG の Screening，SRX の IDS による攻撃検知・防御のレコード）は，すべて集計対象となります。

(5) [ウイルス]グループボックス

ウイルスに関するレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	ウイルス	ウイルスを基準として集計した表
2	接続元	接続元を基準として集計した表
3	接続先	接続先を基準として集計した表
4	ウイルスと接続元	ウイルスを基準とし，そのウイルスによる通信がどの接続元から行われたかを集計した表
5	接続元とウイルス	接続元を基準とし，その接続元からどのウイルスによる通信が行われたかを集計した表
6	ウイルスと接続先	ウイルスを基準とし，そのウイルスによる通信の接続先を集計した表
7	接続先とウイルス	接続先を基準とし，その接続先にどのウイルスによる通信が行われたかを集計した表
8	接続元と接続先	接続元を基準とし，ウイルスによる通信がどの接続先に行われたかを集

		計した表
9	接続先と接続元	接続先を基準とし，ウイルスによる通信がどの接続元から行われたかを集計した表

(6) [スパムメール]グループボックス

スパムメールに関するレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	送信元	送信元を基準として集計した表
2	メールアドレス	メールアドレスを基準として集計した表
3	送信元とメールアドレス	送信元を基準とし，スパムメールの送り先となったメールアドレスを集計した表

(7) [URL フィルタリング]グループボックス

URL フィルタリングに関するレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	接続元	接続元を基準として集計した表
2	Web ページ	Web ページを基準として集計した表
3	カテゴリ	カテゴリを基準として集計した表
4	接続元と Web ページ	接続元を基準とし，その接続元がアクセスした Web ページを集計した表
5	接続元とカテゴリ	接続元を基準とし，その接続元がアクセスした Web ページのカテゴリを集計した表
6	カテゴリと接続元	カテゴリを基準とし，そのカテゴリで URL フィルタされた接続元を集計した表

(8) [通信]グループボックス

遮断した通信のレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	接続元	接続元を基準として集計した表
2	接続元と接続先	接続元を基準とし，その接続元がどの接続先にアクセスしたかを集計した表
3	接続先	接続先を基準として集計した表
4	接続先と接続元	接続先を基準とし，その接続先がどの接続元からアクセスされたかを集計した表

(a) [その他の通信]ボタン

集計対象としたいプロトコルを定義して，遮断した通信のレポートを作成することができます。[その他の通信]ボタンをクリックすると，[その他の通信]パネルが表示されます。詳細は「4.4.4 [その他の通信]パネル」を参照ください。

(9) [プロトコル]グループボックス

プロトコルのレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	プロトコル	プロトコルを基準として集計した表
2	プロトコルと接続元	プロトコルを基準とし，そのプロトコルを用いてどの接続元からアクセスされたかを集計した表
3	接続元とプロトコル	接続元を基準とし，その接続元がどのプロトコルを用いてアクセスしたかを集計した表
4	プロトコルと接続先	プロトコルを基準とし，そのプロトコルを用いてどの接続先にアクセスしたかを集計した表
5	接続先とプロトコル	接続先を基準とし，その接続先がどのプロトコルを用いてアクセスされたかを集計した表

(10) [ルール]グループボックス

ルールのレポート項目において，レポートに含める内容を指定します。

項番	項目	レポートの内容
1	ルール	ルールを基準として集計した表
2	ルールと接続元	ルールを基準とし，そのルールが適用された通信の接続元も集計した表
3	ルールと接続先	ルールを基準とし，そのルールが適用された通信の接続先も集計した表

(11) [デフォルトに戻す]ボタン

レポート項目の選択状態とトップ数の値，各グループボックス内の設定をデフォルト値に戻します。

4.4.2 ［「概要」の設定]パネル

「概要」レポート項目に出力する内容を設定します。

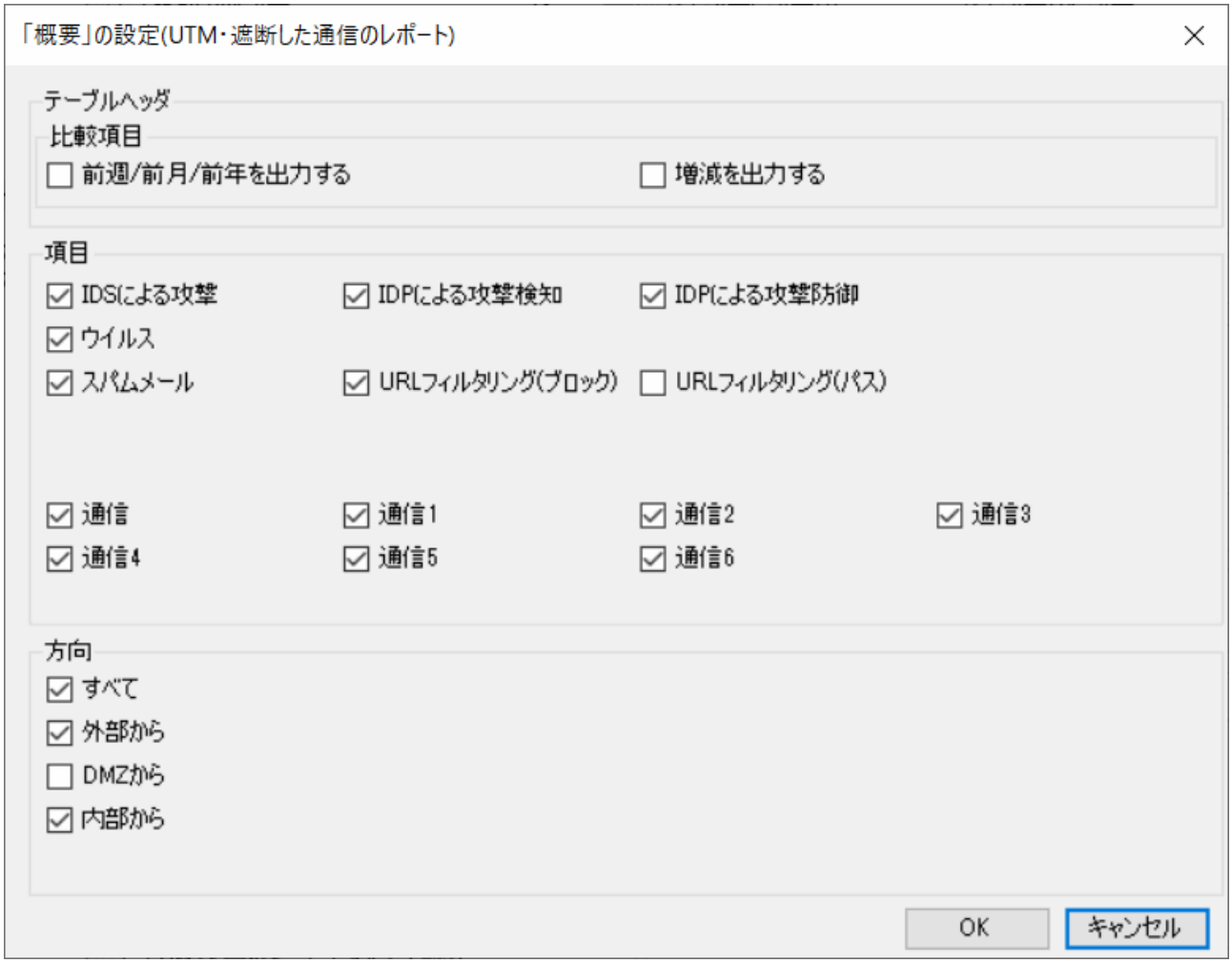


図 25 [「概要」の設定]パネル

(1) ［ヘッダ]グループボックス

「概要」レポート項目は，表からなります。出力する列に関する設定を行います。

項番	項目	レポートの内容
1	前週/前月/前年を出力する	前週/前月/前年の情報を出力
2	増減を出力する	増減を出力

(2) ［項目]グループボックス

「概要」レポート項目に出力する，項目に関する設定を行います。

項番	項目	レポートの内容

1	IDS による攻撃	IDS による攻撃に関する項目を出力
2	IDP による攻撃検知	IDP による攻撃検知に関する項目を出力
3	IDP による攻撃防御	IDP による攻撃防御に関する項目を出力
4	ウイルス	ウイルスに関する項目を出力
5	スパムメール	スパムメールに関する項目を出力
6	URL フィルタリング（ブロック）	URL フィルタリング（ブロック）に関する項目を出力
7	URL フィルタリング（パス）	URL フィルタリング（パス）に関する項目を出力
8	遮断通信	遮断した通信に関する項目を出力
9	遮断通信 *n*	通信 *n* に関する項目を出力

※　ファイアウォールの種類により，項目は異なります

項番	項目	レポートの内容
1	すべて	すべての通信について集計した結果を出力
2	外部から	外部からの通信について集計した結果を出力
3	DMZ から	DMZ からの通信について集計した結果を出力
4	内部から	内部からの通信について集計した結果を出力

［通信 1～6］チェックボックスをチェックしていても，対応するプロトコルの定義がない場合は出力されません。対応するプロトコルの定義については，「4.3.4［その他の通信］パネル」を参照ください。

4.4.3 ［「グラフ」の設定］パネル

「通信のレポート」に含めるグラフについて設定します。

図 26 ［「グラフ」の設定］パネル

(1) ［攻撃］グループボックス

攻撃に関するレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	攻撃数の時系列のグラフ
2	攻撃（時系列）	攻撃（トップ 5）の時系列のグラフ
3	攻撃（棒）	攻撃（トップ 10）の棒グラフ
4	攻撃（円）	攻撃（トップ 10）の円グラフ
5	攻撃元（時系列）	攻撃元（トップ 5）の時系列のグラフ
6	攻撃元（棒）	攻撃元（トップ 10）の棒グラフ
7	攻撃元（円）	攻撃元（トップ 10）の円グラフ
8	攻撃先（時系列）	攻撃先（トップ 5）の時系列のグラフ
9	攻撃先（棒）	攻撃先（トップ 10）の棒グラフ
10	攻撃先（円）	攻撃先（トップ 10）の円グラフ

『「概要」で DMZ を除く』をチェックした場合，攻撃に関する「xxx 概要」レポート項目

のグラフから，「DMZ から」が除外されます。

(2) [ウイルス]グループボックス

ウイルスに関するレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	ウイルス数の時系列のグラフ
2	ウイルス（時系列）	ウイルス（トップ 5）の時系列のグラフ
3	ウイルス（棒）	ウイルス（トップ 10）の棒グラフ
4	ウイルス（円）	ウイルス（トップ 10）の円グラフ
5	接続元（時系列）	接続元（トップ 5）の時系列のグラフ
6	接続元（棒）	接続元（トップ 10）の棒グラフ
7	接続元（円）	接続元（トップ 10）の円グラフ
8	接続先（時系列）	接続先（トップ 5）の時系列のグラフ
9	接続先（棒）	接続先（トップ 10）の棒グラフ
10	接続先（円）	接続先（トップ 10）の円グラフ

(3) [スパムメール]グループボックス

スパムメールに関するレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	スパムメール数の時系列のグラフ
2	送信元（時系列）	送信元（トップ 5）の時系列のグラフ
3	送信元（棒）	送信元（トップ 10）の棒グラフ
4	送信元（円）	送信元（トップ 10）の円グラフ
5	メールアドレス（時系列）	メールアドレス（トップ 5）の時系列のグラフ
6	メールアドレス（棒）	メールアドレス（トップ 10）の棒グラフ
7	メールアドレス（円）	メールアドレス（トップ 10）の円グラフ

(4) [URL フィルタリング]グループボックス

URL フィルタリングに関するレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	スパムメール数の時系列のグラフ
2	接続元（時系列）	接続元（トップ 5）の時系列のグラフ
3	接続元（棒）	接続元（トップ 10）の棒グラフ
4	接続元（円）	接続元（トップ 10）の円グラフ
5	ページ（時系列）	ページ（トップ 5）の時系列のグラフ

6	ページ（棒）	ページ（トップ 10）の棒グラフ
7	ページ（円）	ページ（トップ 10）の円グラフ
8	カテゴリ（時系列）	カテゴリ（トップ 5）の時系列のグラフ
9	カテゴリ（棒）	カテゴリ（トップ 10）の棒グラフ
10	カテゴリ（円）	カテゴリ（トップ 10）の円グラフ

(5) [通信]グループボックス

遮断した通信のレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	回数の時系列のグラフ
2	接続元（時系列）	接続元（トップ 5）の時系列のグラフ
3	接続元（棒）	接続元（トップ 10）の棒グラフ
4	接続元（円）	接続元（トップ 10）の円グラフ
5	接続先（時系列）	接続先（トップ 5）の時系列のグラフ
6	接続先（棒）	接続先（トップ 10）の棒グラフ
7	接続先（円）	接続先（トップ 10）の円グラフ

(a) [概要]グループボックス

「xxxxx 概要」レポート項目に含める内容を指定します。

項番	項目	グラフの内容
1	ゾーン別	接続元別の時系列グラフ

項番	項目	レポートの内容
1	DMZ	グラフから，DMZ を除く

(6) [プロトコル]グループボックス

プロトコルのレポート項目において，レポートに含めるグラフを指定します。

項番	項目	レポートの内容
1	時系列	回数の時系列のグラフ
2	プロトコル（時系列）	プロトコル（トップ 5）の時系列のグラフ
3	プロトコル（棒）	プロトコル（トップ 10）の棒グラフ
4	プロトコル（円）	プロトコル（トップ 10）の円グラフ

(7) [ルール]グループボックス

ルールのレポート項目において，レポートに含めるグラフを指定します。

項番	項目	レポートの内容

1	ルール（時系列）	ルール（トップ 5）の時系列のグラフ
2	ルール（棒）	ルール（トップ 10）の棒グラフ
3	ルール（円）	ルール（トップ 10）の円グラフ

4.4.4　　[その他の通信]パネル

集計対象としたいプロトコルを設定します。

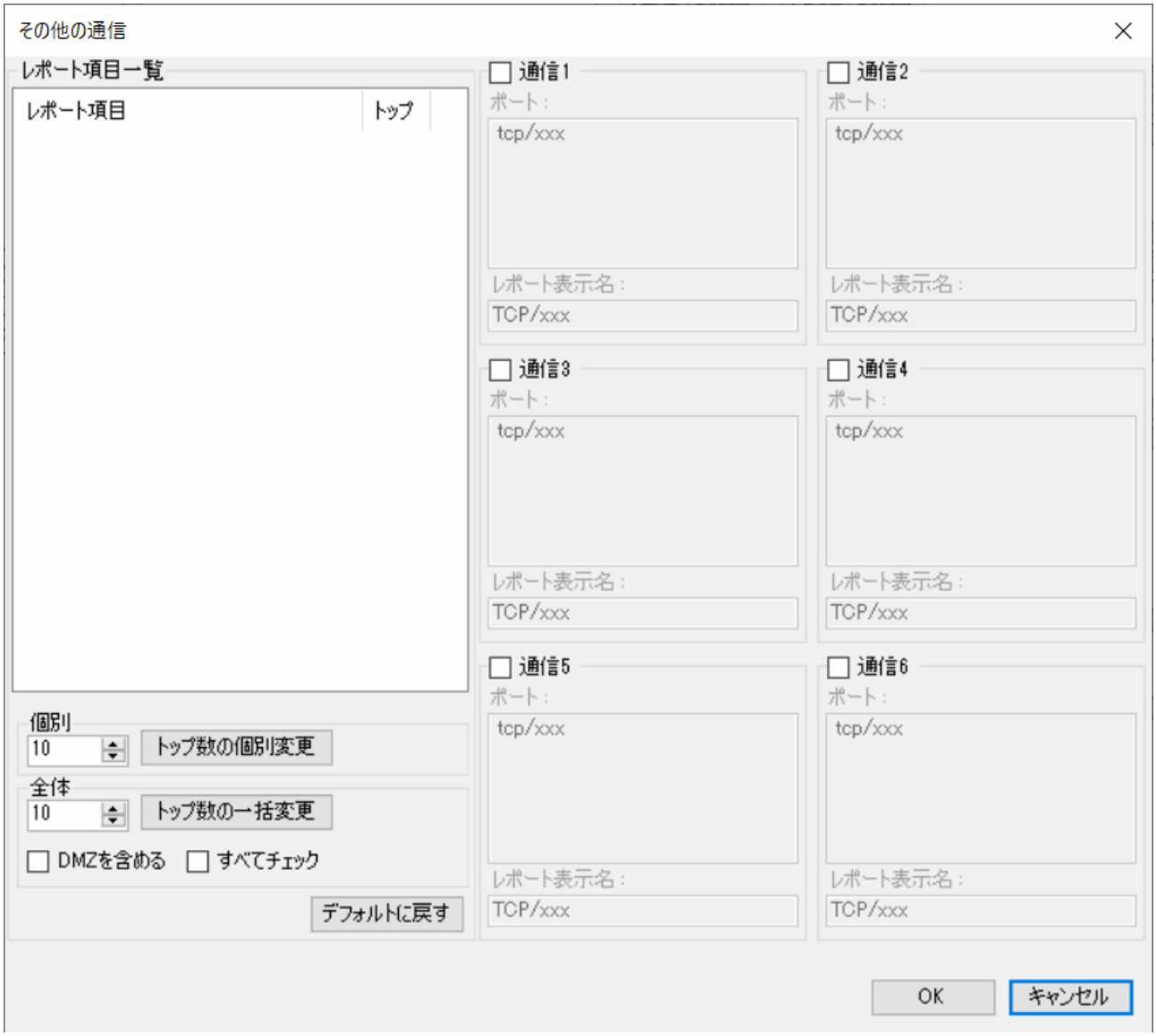


図 27 [その他の通信]パネル

(1) [レポート項目一覧]グループボックス

「4.2.1 [通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2) [通信 *n*]グループボックス

「4.3.4 [その他の通信]パネル (2) [通信 *n*]グループボックス」を参照してください。

4.5　アプリケーションのレポート

ファイアウォールが出力する「アプリケーションログ」を集計対象とします。

4.5.1　[アプリケーションのレポート]パネル

「アプリケーションのレポート」に含めるレポート項目について設定します。

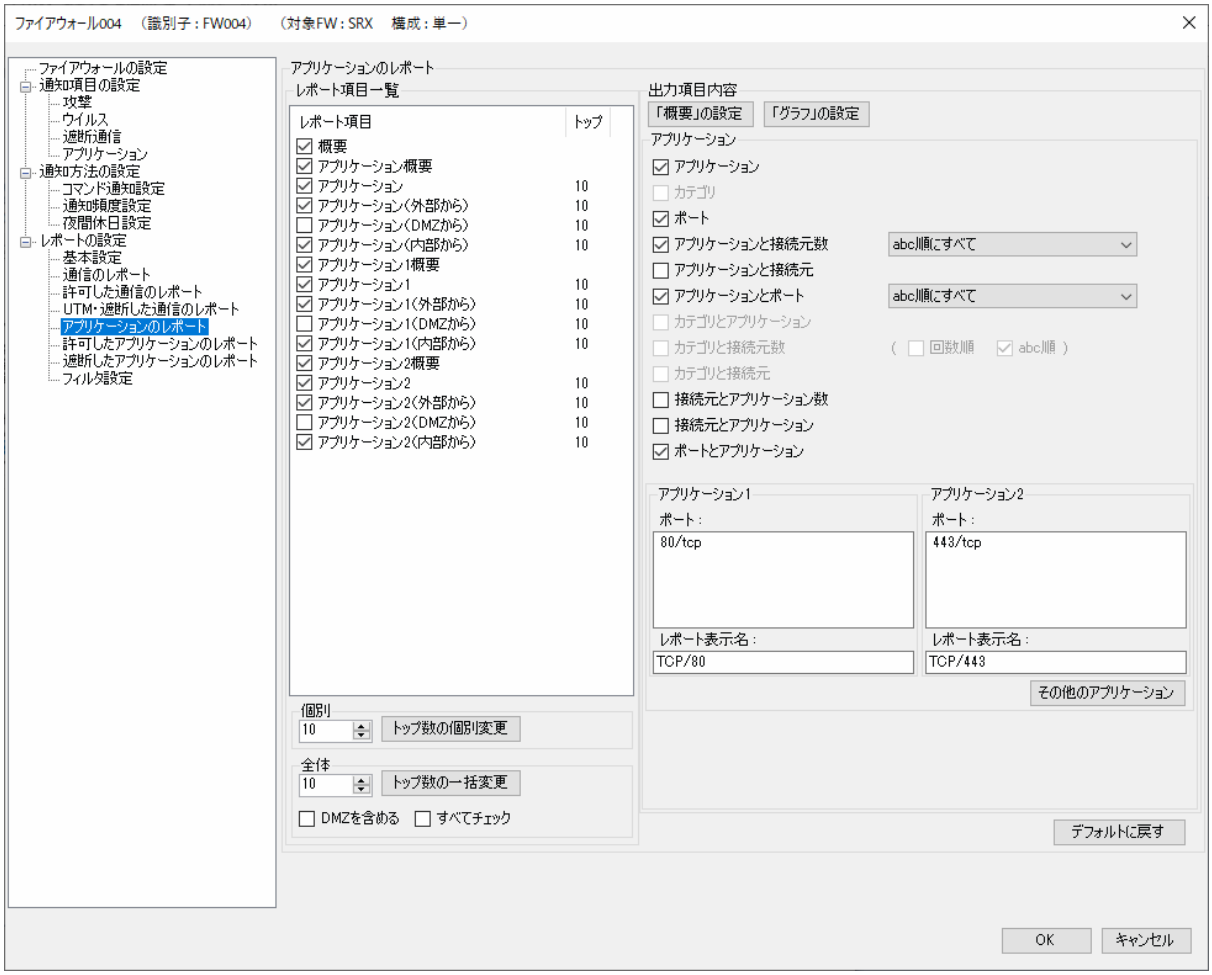


図 28 [アプリケーションのレポート]パネル

(1)　[レポート項目一覧]グループボックス

「4.2.1 [通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2)　[「概要」の設定]ボタン

「概要」レポート項目に出力する内容を指定します。[「概要」の設定]ボタンをクリックすると，[「概要」の設定]パネルが表示されます。詳細は「4.5.2 [「概要」の設定]パネル」を参照ください。

(3) [「グラフ」の設定]ボタン

レポートに出力するグラフを指定することができます。[「グラフ」の設定]ボタンをクリックすると，[「グラフ」の設定]パネルが表示されます。詳細は「4.5.3 [「グラフ」の設定]パネル」を参照ください。

(4) [ハイリスク]スピンボックス

ハイリスクレポートに含めるリスクの値を指定します。スピンボックスで指定された値以上のリスクを持つアプリケーションがレポート対象となります。

(5) [アプリケーション]グループボックス

レポートに含める内容を指定します。

項番	項目	レポートの内容
1	アプリケーション	アプリケーションを基準として集計した表
2	カテゴリ	カテゴリを基準として集計した表
3	ポート	ポート番号を基準として集計した表
4	アプリケーションと接続元数	アプリケーションを基準とし，そのアプリケーションの接続元の数を集計した表
5	アプリケーションと接続元	アプリケーションを基準とし，そのアプリケーションの接続元 IP アドレスを集計した表
6	アプリケーションとポート	アプリケーションを基準とし，そのアプリケーションに含まれるポート番号を集計した表
7	カテゴリとアプリケーション	カテゴリを基準とし，そのカテゴリに含まれるアプリケーションを集計した表
8	カテゴリと接続元数	カテゴリを基準とし，そのカテゴリの接続元の数を集計した表
9	カテゴリと接続元	カテゴリを基準とし，そのカテゴリの接続元 IP アドレスを集計した表
10	接続元とアプリケーション数	接続元を基準とし，その接続元が使用したアプリケーションの数を集計した表
11	接続元とアプリケーション	接続元を基準とし，その接続元が使用したアプリケーションを集計した表
12	ポートとアプリケーション	ポート番号を基準とし，そのポート番号が使用したアプリケーションを集計した表

(6) [アプリケーション *n*]グループボックス

指定したポート番号に発生しているアプリケーションを集計します。

[アプリケーション *n*]チェックボックスをチェックすると，[ポート番号]テキストボックスと[レポート表示名]テキストボックスが活性状態になります。

項番	項目	指定する内容
1	ポート番号	集計対象とするポート番号 例）tcp/80 指定方法は，「表 4.3-1 プロトコル（ポート番号）の指定方法」を参照
2	レポート表示名	レポート中に使用する表示名 例）TCP/80

(7) [その他のアプリケーション]ボタン

[アプリケーション 1][アプリケーション 2]に加えて，指定したポート番号に発生しているアプリケーションを集計することができます。[その他のアプリケーション]ボタンをクリックすると，[その他のアプリケーション]パネルが表示されます。詳細は「4.5.4 [その他のアプリケーション]パネル」を参照ください。

(8) [デフォルトに戻す]ボタン

レポート項目の選択状態とトップ数の値，各グループボックス内の設定をデフォルト値に戻します。

4.5.2 [「概要」の設定]パネル

「概要」レポート項目に出力する内容を設定します。

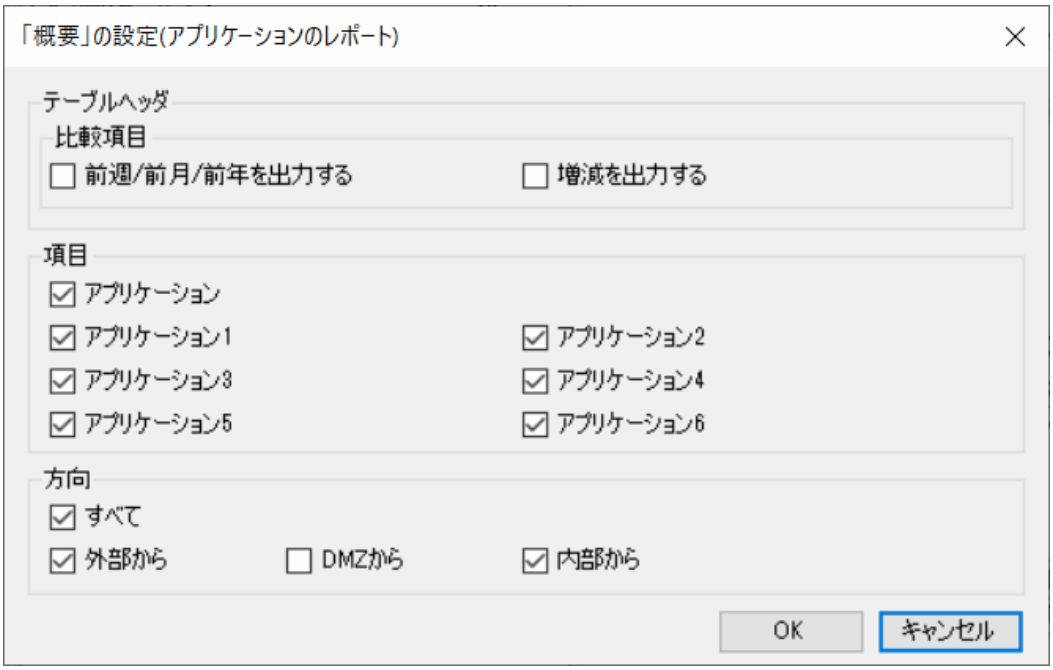


図 29 [「概要」の設定]パネル

(1) [ヘッダ]グループボックス

「概要」レポート項目は，表からなります。出力する列に関する設定を行います。

項番	項目	レポートの内容
1	前週/前月/前年を出力する	前週/前月/前年の情報を出力
2	増減を出力する	増減を出力

(2) [項目]グループボックス

「概要」レポート項目に出力する，項目に関する設定を行います。

項番	項目	レポートの内容
1	アプリケーション	アプリケーションに関する項目を出力
2	アプリケーション *n*	アプリケーション *n* に関する項目を出力

項番	項目	レポートの内容
1	すべて	すべてのアプリケーションについて集計した結果を出力
2	外部から	外部からのアプリケーションについて集計した結果を出力
3	DMZ から	DMZ からのアプリケーションについて集計した結果を出力

4	内部から	内部からのアプリケーションについて集計した結果を出力

注　意

［アプリケーション 1～6］チェックボックスをチェックしていても，対応するポートの定義がない場合は出力されません。対応するポートの定義については，「4.3.4［その他の通信］パネル」を参照ください。

4.5.3 [「グラフ」の設定]パネル

「アプリケーションのレポート」に含めるグラフについて設定します。

図 30 [「グラフ」の設定]パネル

(1) [概要]グループボックス

概要レポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列（回数順）	回数の時系列のグラフ

『「xxx 概要」グラフで DMZ を表示しない』をチェックした場合，「xxx 概要」レポート項目のグラフから，「DMZ から」が除外されます

(2) [アプリケーション]グループボックス

アプリケーションに関するレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	回数の時系列のグラフ
2	アプリケーション（時系列）	アプリケーション（トップ 5）の時系列のグラフ
3	アプリケーション（棒）	アプリケーション（トップ 10）の棒グラフ
4	アプリケーション（円）	アプリケーション（トップ 10）の円グラフ
5	カテゴリ（時系列）	カテゴリ（トップ 5）の時系列のグラフ
6	カテゴリ（棒）	カテゴリ（トップ 10）の棒グラフ
7	カテゴリ（円）	カテゴリ（トップ 10）の円グラフ

4.5.4　[その他のアプリケーション]パネル

[アプリケーション 1][アプリケーション 2]に加えて，指定したポート番号に発生しているアプリケーションを集計します。

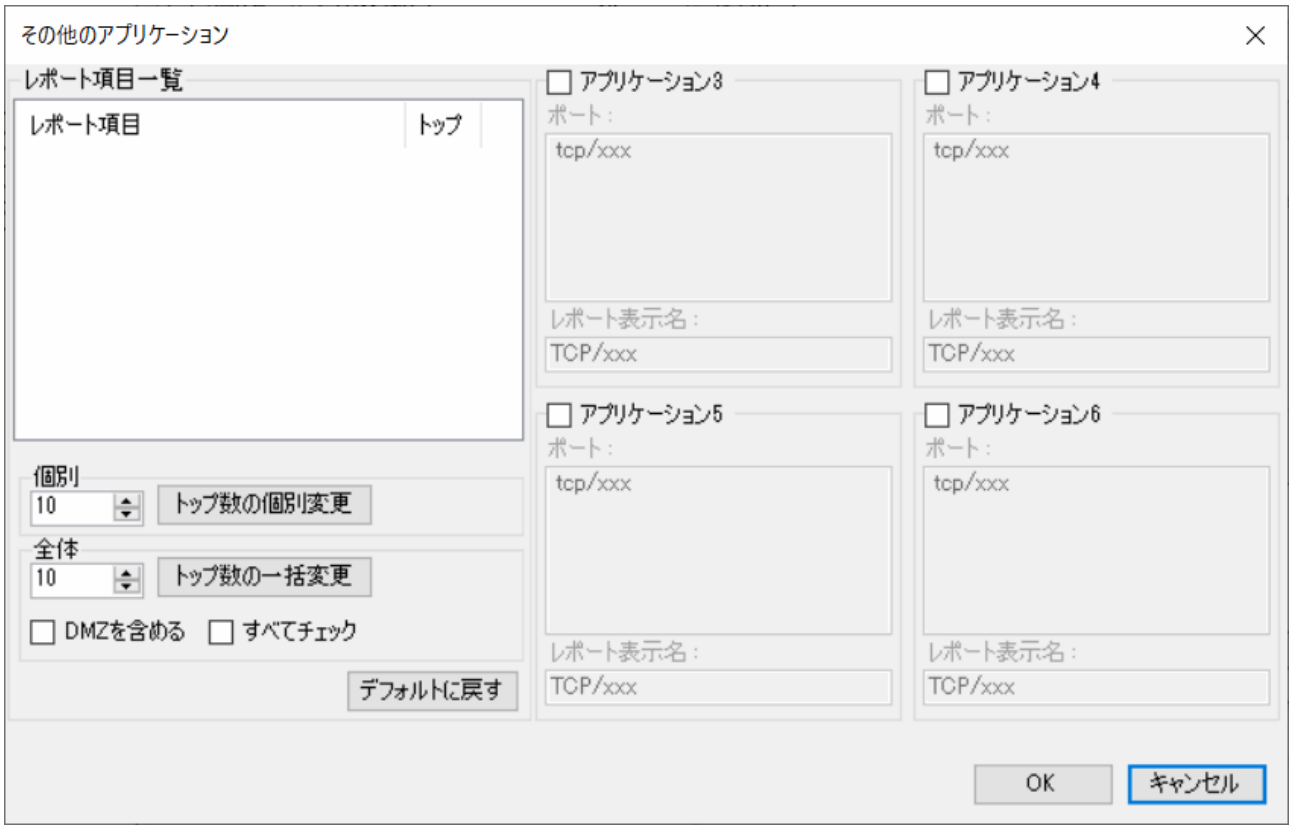


図 31 [その他のアプリケーション]パネル

(1) [レポート項目一覧]グループボックス

「4.2.1 [通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2) [アプリケーション *n*]グループボックス

「4.5.1 [アプリケーションのレポート]パネル (6) [アプリケーション *n*]グループボックス」を参照してください。

4.6　許可したアプリケーションのレポート

ファイアウォールが出力する「アプリケーションログ」の内，ファイアウォールが許可したアプリケーションのログを集計対象とします

4.6.1　[許可したアプリケーション]パネル

「許可したアプリケーションのレポート」に含めるレポート項目について設定します。

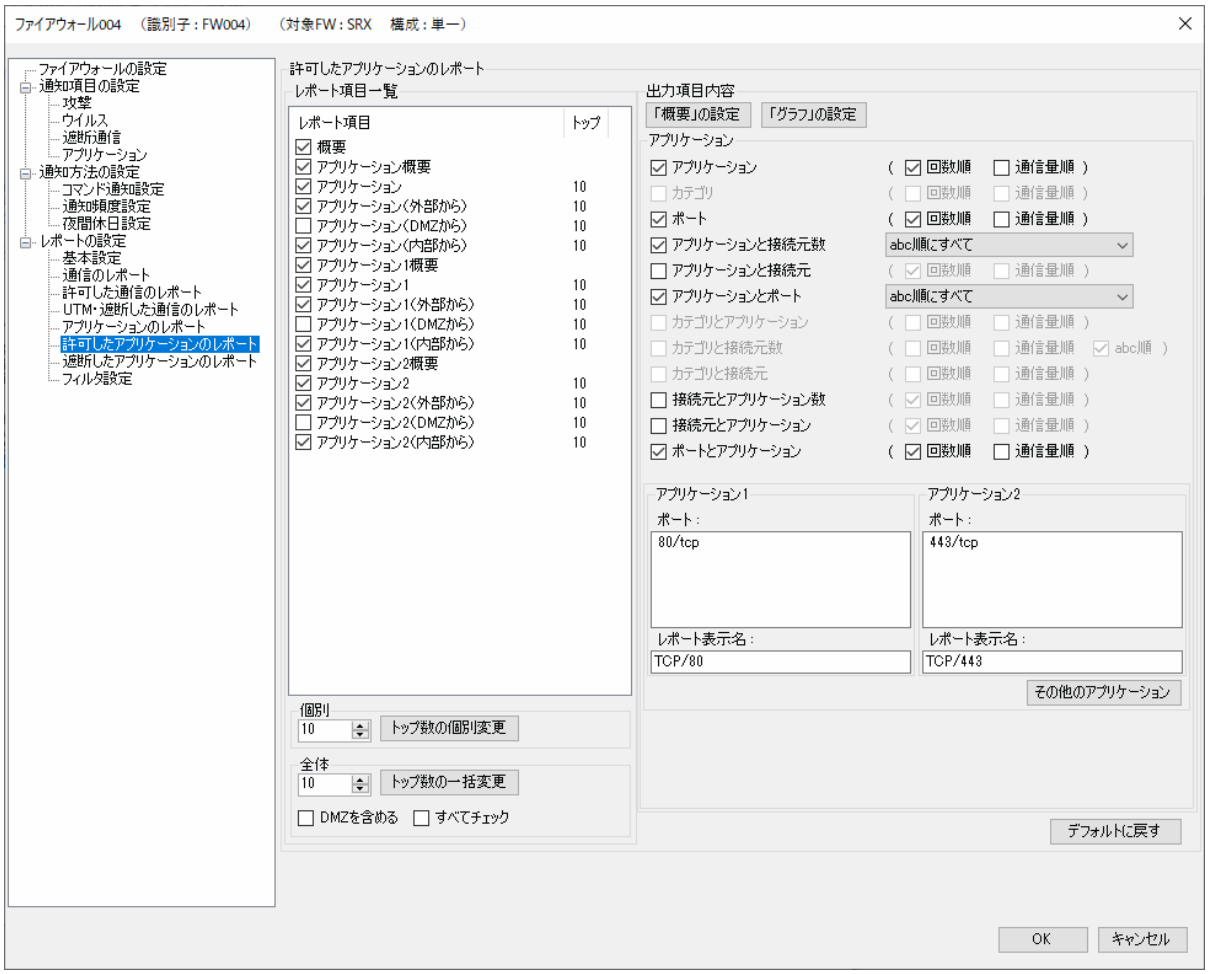


図 32 [許可したアプリケーション]パネル

(1)　[レポート項目一覧]グループボックス

「4.2.1 [通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2)　[「概要」の設定]ボタン

「概要」レポート項目に出力する内容を指定します。[「概要」の設定]ボタンをクリックすると，[概要の設定]パネルが表示されます。詳細は「4.6.2 [「概要」の設定]パネル」を

参照ください。

(3) [「グラフ」の設定]ボタン

レポートに出力するグラフを指定します。[グラフの設定]ボタンをクリックすると，[グラフの設定]パネルが表示されます。詳細は「4.6.3 [「グラフ」の設定]パネル」を参照ください。

(4) [ハイリスク]スピンボックス

ハイリスクレポートに含めるリスクの値を指定します。スピンボックスで指定された値以上のリスクを持つアプリケーションがレポート対象となります。

(5) [アプリケーション]グループボックス

レポートに含める内容を指定します。

項番	項目	レポートの内容
1	アプリケーション	アプリケーションを基準として集計した表
2	カテゴリ	カテゴリを基準として集計した表
3	ポート	ポート番号を基準として集計した表
4	アプリケーションと接続元数	アプリケーションを基準とし，そのアプリケーションの接続元の数を集計した表
5	アプリケーションと接続元	アプリケーションを基準とし，そのアプリケーションの接続元 IP アドレスを集計した表
6	アプリケーションとポート	アプリケーションを基準とし，そのアプリケーションに含まれるポート番号を集計した表
7	カテゴリとアプリケーション	カテゴリを基準とし，そのカテゴリに含まれるアプリケーションを集計した表
8	カテゴリと接続元数	カテゴリを基準とし，そのカテゴリの接続元の数を集計した表
9	カテゴリと接続元	カテゴリを基準とし，そのカテゴリの接続元 IP アドレスを集計した表
10	接続元とアプリケーション数	接続元を基準とし，その接続元が使用したアプリケーションの数を集計した表
11	接続元とアプリケーション	接続元を基準とし，その接続元が使用したアプリケーションを集計した表
12	ポートとアプリケーション	ポート番号を基準とし，そのポート番号が使用したアプリケーションを集計した表

(6) [アプリケーション *n*]グループボックス

指定したポート番号に発生しているアプリケーションを集計します。「4.5.1 [アプリケーションのレポート]パネル (6) [アプリケーション *n*]グループボックス」を参照してください。

(7) [その他のアプリケーション]ボタン

[アプリケーション 1][アプリケーション 2]に加えて，指定したポート番号に発生しているアプリケーションを集計することができます。[その他のアプリケーション]ボタンをクリックすると，[その他のアプリケーション]パネルが表示されます。詳細は「4.6.4 [その他のアプリケーション]パネル」を参照ください。

(8) [デフォルトに戻す]ボタン

レポート項目の選択状態とトップ数の値，各グループボックス内の設定をデフォルト値に戻します。

4.6.2 [「概要」の設定]パネル

「概要」レポート項目に出力する内容を設定します。

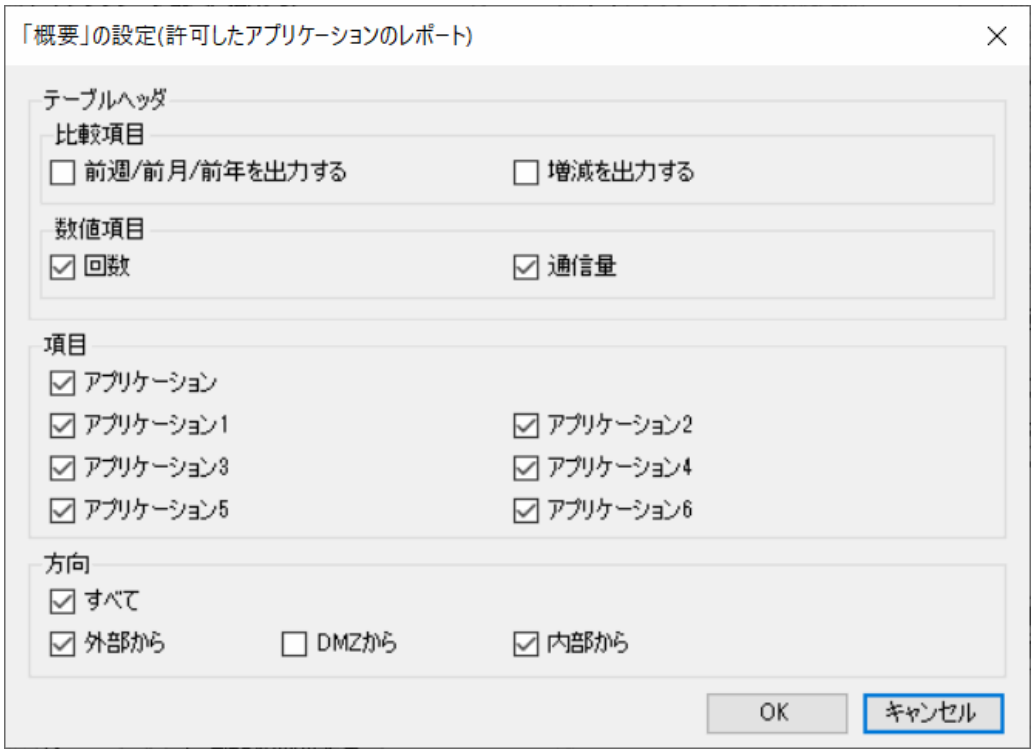


図 33 [「概要」の設定]パネル

(1) [ヘッダ]グループボックス

「概要」レポート項目は，表からなります。出力する列に関する設定を行います。

項番	項目	レポートの内容
1	前週/前月/前年を出力する	前週/前月/前年の情報を出力
2	増減を出力する	増減を出力

項番	項目	レポートの内容
1	回数	回数を出力
2	通信量	通信量を出力

(2) [項目]グループボックス

「概要」レポート項目に出力する，項目に関する設定を行います。

項番	項目	レポートの内容
1	アプリケーション	アプリケーションに関する項目を出力
2	アプリケーション *n*	アプリケーション *n* に関する項目を出力

項番	項目	レポートの内容
1	すべて	すべてのアプリケーションについて集計した結果を出力
2	外部から	外部からのアプリケーションについて集計した結果を出力
3	DMZ から	DMZ からのアプリケーションについて集計した結果を出力
4	内部から	内部からのアプリケーションについて集計した結果を出力

注　意

［アプリケーション 1～6］チェックボックスをチェックしていても，対応するポートの定義がない場合は出力されません。対応するポートの定義については，「4.3.4［その他の通信］パネル」を参照ください。

4.6.3 [「グラフ」の設定]パネル

「許可したアプリケーションのレポート」に含めるグラフについて設定します。

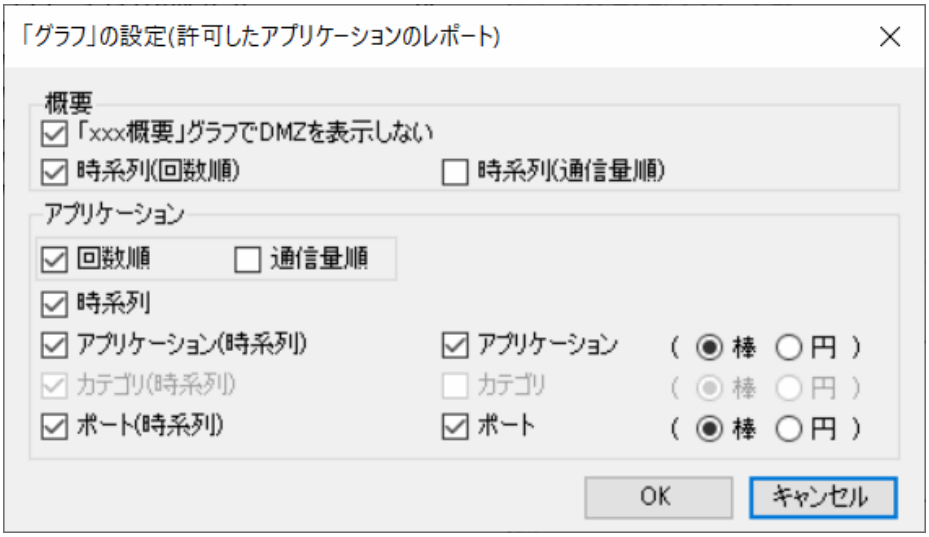


図 34 [「グラフ」の設定]パネル

(1) [概要]グループボックス

概要レポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列（回数順）	回数の時系列のグラフ
2	時系列（通信量順）	通信量の時系列のグラフ

『「xxx 概要」グラフで DMZ を表示しない』をチェックした場合，「xxx 概要」レポート項目のグラフから，「DMZ から」が除外されます

(1) [アプリケーション]グループボックス

アプリケーションに関するレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	回数，通信量の時系列のグラフ
2	アプリケーション（時系列）	アプリケーション（トップ 5）の時系列のグラフ
3	アプリケーション（棒）	アプリケーション（トップ 10）の棒グラフ
4	アプリケーション（円）	アプリケーション（トップ 10）の円グラフ
5	カテゴリ（時系列）	カテゴリ（トップ 5）の時系列のグラフ
6	カテゴリ（棒）	カテゴリ（トップ 10）の棒グラフ
7	カテゴリ（円）	カテゴリ（トップ 10）の円グラフ

4.6.4 [その他のアプリケーション]パネル

[アプリケーション 1][アプリケーション 2]に加えて，指定したポート番号に発生しているアプリケーションを集計します。

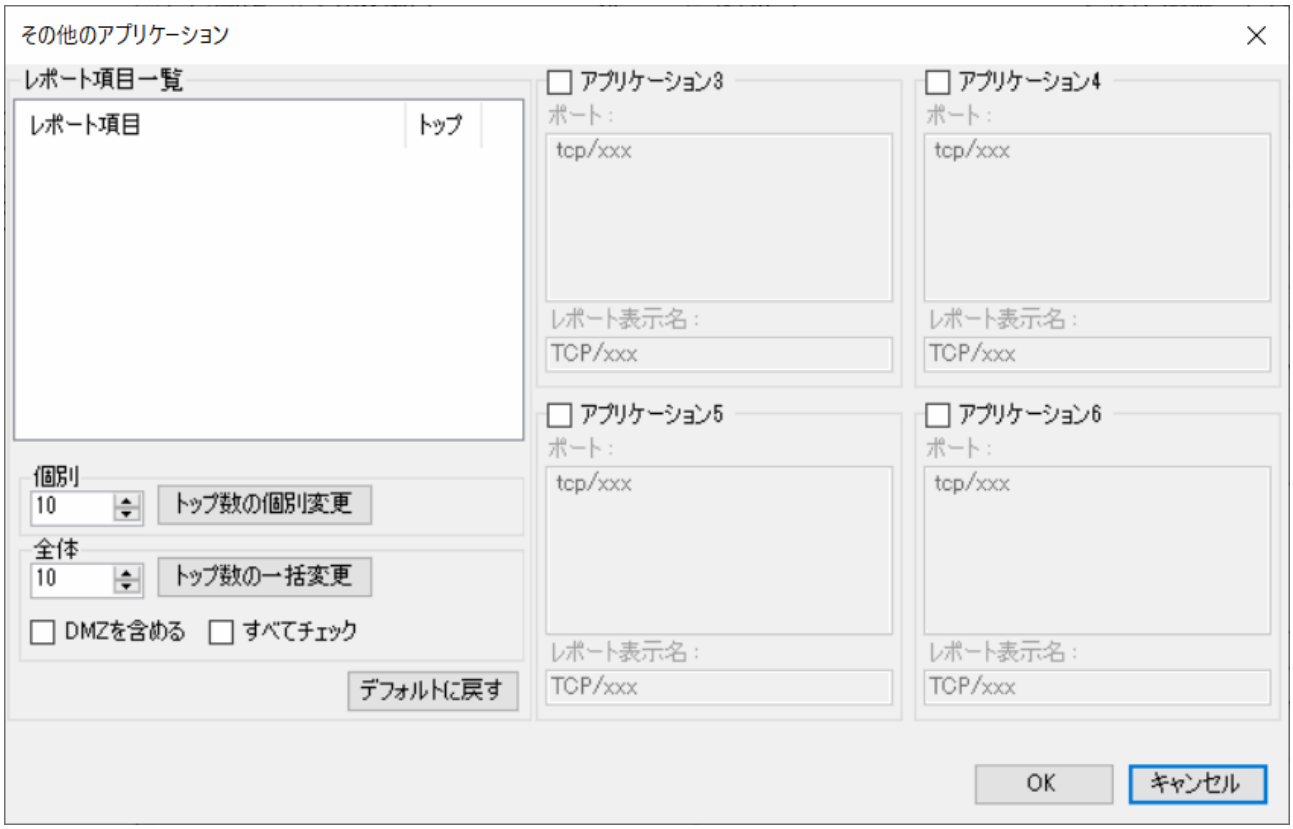


図 35 [その他のアプリケーション]パネル

(1) [レポート項目一覧]グループボックス

「4.3.1 [許可した通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2) [アプリケーション *n*]グループボックス

「4.5.1 [アプリケーションのレポート]パネル (6) [アプリケーション *n*]グループボックス」を参照してください。

4.7　遮断したアプリケーションのレポート

ファイアウォールが出力する「アプリケーションログ」の内，ファイアウォールが遮断したアプリケーションのログを集計対象とします

4.7.1　[遮断したアプリケーション]パネル

「遮断したアプリケーションのレポート」に含めるレポート項目について設定します。

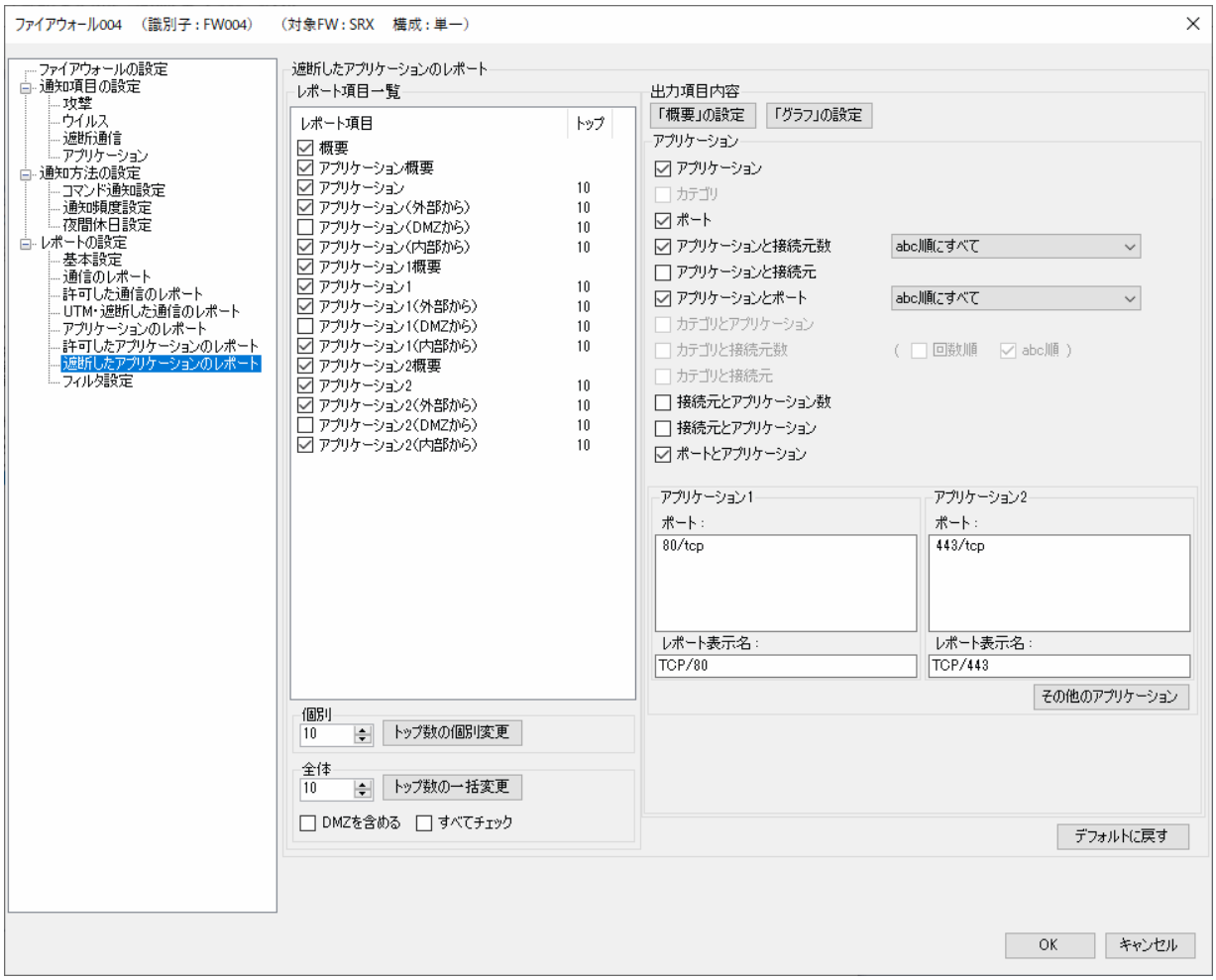


図 36 [遮断したアプリケーション]パネル

(1)　[レポート項目一覧]グループボックス

「4.2.1 [通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2)　[「概要」の設定]ボタン

「概要」レポートに出力する項目を指定します。[「概要」の設定]ボタンをクリックすると，[「概要」の設定]パネルが表示されます。詳細は「4.7.2 [「概要」の設定]パネル」を

参照ください。

(3) [グラフの設定]ボタン

レポートに出力するグラフを指定します。[グラフの設定]ボタンをクリックすると，[「グラフ」の設定]パネルが表示されます。詳細は「4.7.3 [「グラフ」の設定]パネル」を参照ください。

(4) [ハイリスク]スピンボックス

ハイリスクレポートに含めるリスクの値を指定します。スピンボックスで指定された値以上のリスクを持つアプリケーションがレポート対象となります。

(5) [アプリケーション]グループボックス

レポートに含める内容を指定します。

項番	項目	レポートの内容
1	アプリケーション	アプリケーションを基準として集計した表
2	カテゴリ	カテゴリを基準として集計した表
3	ポート	ポート番号を基準として集計した表
4	アプリケーションと接続元数	アプリケーションを基準とし，そのアプリケーションの接続元の数を集計した表
5	アプリケーションと接続元	アプリケーションを基準とし，そのアプリケーションの接続元 IP アドレスを集計した表
6	アプリケーションとポート	アプリケーションを基準とし，そのアプリケーションに含まれるポート番号を集計した表
7	カテゴリとアプリケーション	カテゴリを基準とし，そのカテゴリに含まれるアプリケーションを集計した表
8	カテゴリと接続元数	カテゴリを基準とし，そのカテゴリの接続元の数を集計した表
9	カテゴリと接続元	カテゴリを基準とし，そのカテゴリの接続元 IP アドレスを集計した表
10	接続元とアプリケーション数	接続元を基準とし，その接続元が使用したアプリケーションの数を集計した表
11	接続元とアプリケーション	接続元を基準とし，その接続元が使用したアプリケーションを集計した表
12	ポートとアプリケーション	ポート番号を基準とし，そのポート番号が使用したアプリケーションを集計した表

(6) [アプリケーション *n*]グループボックス

指定したポート番号に発生しているアプリケーションを集計します。「4.5.1 [アプリケーションのレポート]パネル (6) [アプリケーション *n*]グループボックス」を参照してください。

(7) [その他のアプリケーション]ボタン

アプリケーション１とアプリケーション２以外にも，集計対象としたいポート別にレポートを作成することができます。[その他のアプリケーション]ボタンをクリックすると，[その他のアプリケーション]パネルが表示されます。詳細は「4.7.4 [その他のアプリケーション]パネル」を参照ください。

(8) [デフォルトに戻す]ボタン

レポート項目の選択状態とトップ数の値，各グループボックス内の設定をデフォルト値に戻すことができます。

4.7.2 [「概要」の設定]パネル

「概要」レポート項目に出力する内容を設定します。

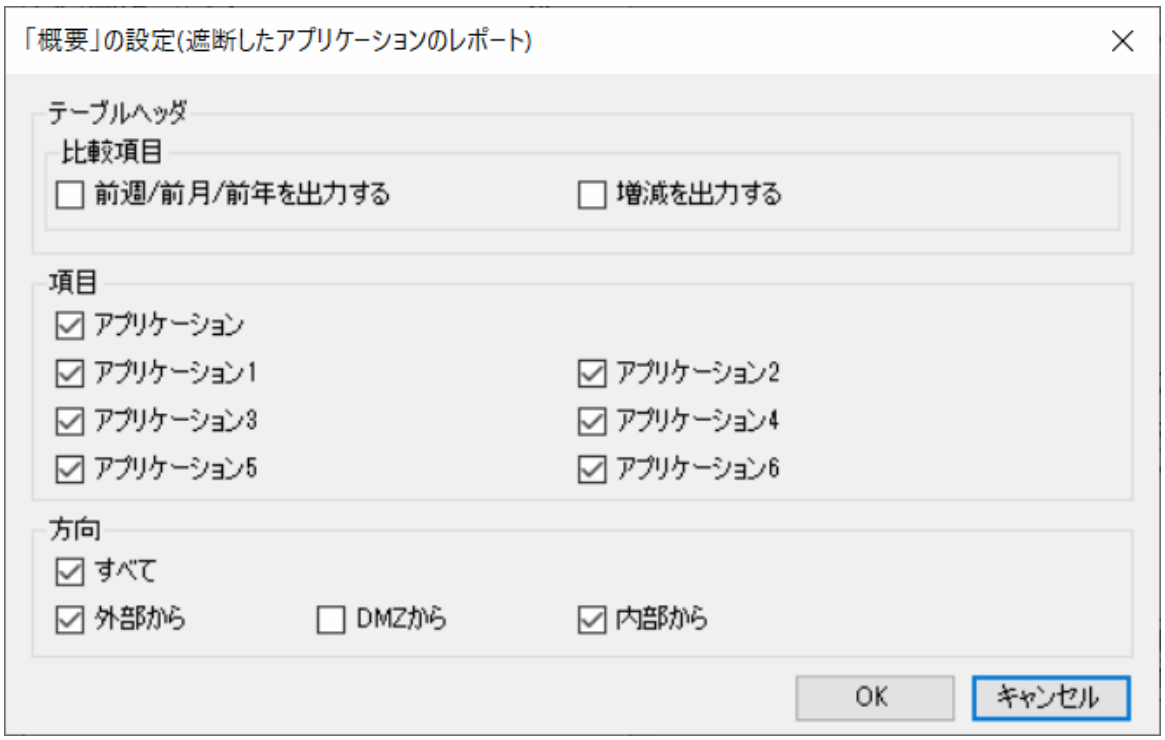


図 37 [「概要」の設定]パネル

(1) [ヘッダ]グループボックス

「概要」レポート項目は，表からなります。出力する列に関する設定を行います。

項番	項目	レポートの内容
1	前週/前月/前年を出力する	前週/前月/前年の情報を出力
2	増減を出力する	増減を出力

項番	項目	レポートの内容
1	回数	回数を出力
2	通信量	通信量を出力

(2) [項目]グループボックス

「概要」レポート項目に出力する，項目に関する設定を行います。

項番	項目	レポートの内容
1	アプリケーション	アプリケーションに関する項目を出力
2	アプリケーション *n*	アプリケーション *n* に関する項目を出力

項番	項目	レポートの内容
1	すべて	すべてのアプリケーションについて集計した結果を出力
2	外部から	外部からのアプリケーションについて集計した結果を出力
3	DMZ から	DMZ からのアプリケーションについて集計した結果を出力
4	内部から	内部からのアプリケーションについて集計した結果を出力

注　意

［アプリケーション 1～6］チェックボックスをチェックしていても，対応するポートの定義がない場合は出力されません。対応するポートの定義については，「4.3.4［その他の通信］パネル」を参照ください。

4.7.3 ［「グラフ」の設定]パネル

「遮断したアプリケーションのレポート」に含めるグラフについて設定します。

図 38 [「グラフ」の設定]パネル

(1) ［概要]グループボックス

概要レポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列（回数順）	回数の時系列のグラフ

『「xxx 概要」グラフで DMZ を表示しない』をチェックした場合，「xxx 概要」レポート項目のグラフから，「DMZ から」が除外されます

(2) ［アプリケーション]グループボックス

アプリケーションに関するレポート項目において，レポートに含めるグラフを指定します。

項番	項目	グラフの内容
1	時系列	回数，通信量の時系列のグラフ
2	アプリケーション（時系列）	アプリケーション（トップ 5）の時系列のグラフ
3	アプリケーション（棒）	アプリケーション（トップ 10）の棒グラフ
4	アプリケーション（円）	アプリケーション（トップ 10）の円グラフ
5	カテゴリ（時系列）	カテゴリ（トップ 5）の時系列のグラフ
6	カテゴリ（棒）	カテゴリ（トップ 10）の棒グラフ
7	カテゴリ（円）	カテゴリ（トップ 10）の円グラフ

4.7.4 [その他のアプリケーション]パネル

[アプリケーション 1][アプリケーション 2]に加えて，指定したポート番号に発生しているアプリケーションを集計します。

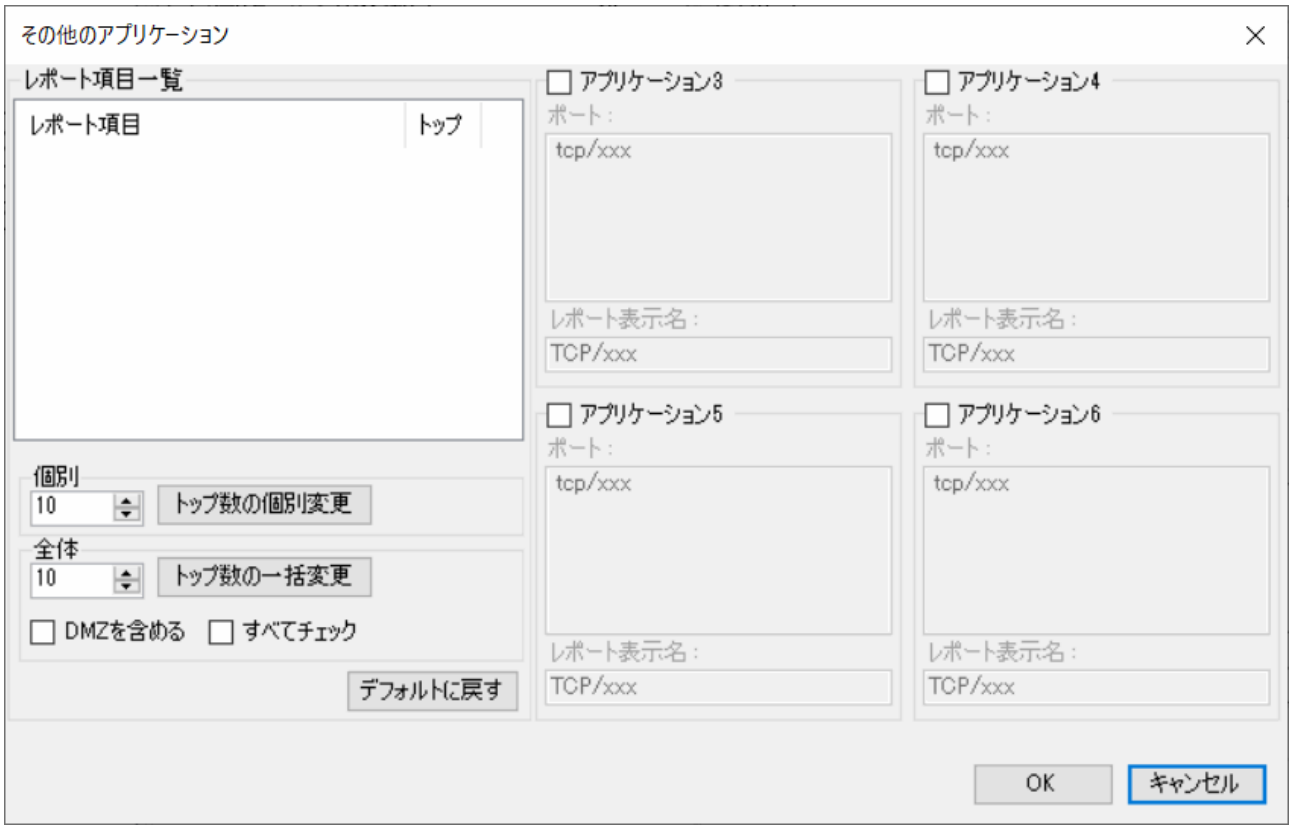


図 39 [その他のアプリケーション]パネル

(1) [レポート項目一覧]グループボックス

「4.3.1 [許可した通信のレポート]パネル (1) [レポート項目一覧]グループボックス」を参照してください。

(2) [アプリケーション 3～6]グループボックス

「4.5.1 [アプリケーションのレポート]パネル (6) [アプリケーション *n*]グループボックス」を参照してください。

4.8　フィルタ設定

接続元や接続先で，フィル足したレポートを作成する場合に設定します。フィルタすることの出来る項目は，以下のとおりです。

項番	ログの種類	フィルタ項目		
		接続元	接続先	プロトコル
1	トラフィック	○	○	○
2	UTM	○	○	×
3	アプリケーション	○	○	○

○：フィルタ出来る項目，×：フィルタ出来ない項目

4.8.1　[フィルタ設定]パネル

「遮断したアプリケーションのレポート」に含めるレポート項目について設定します。

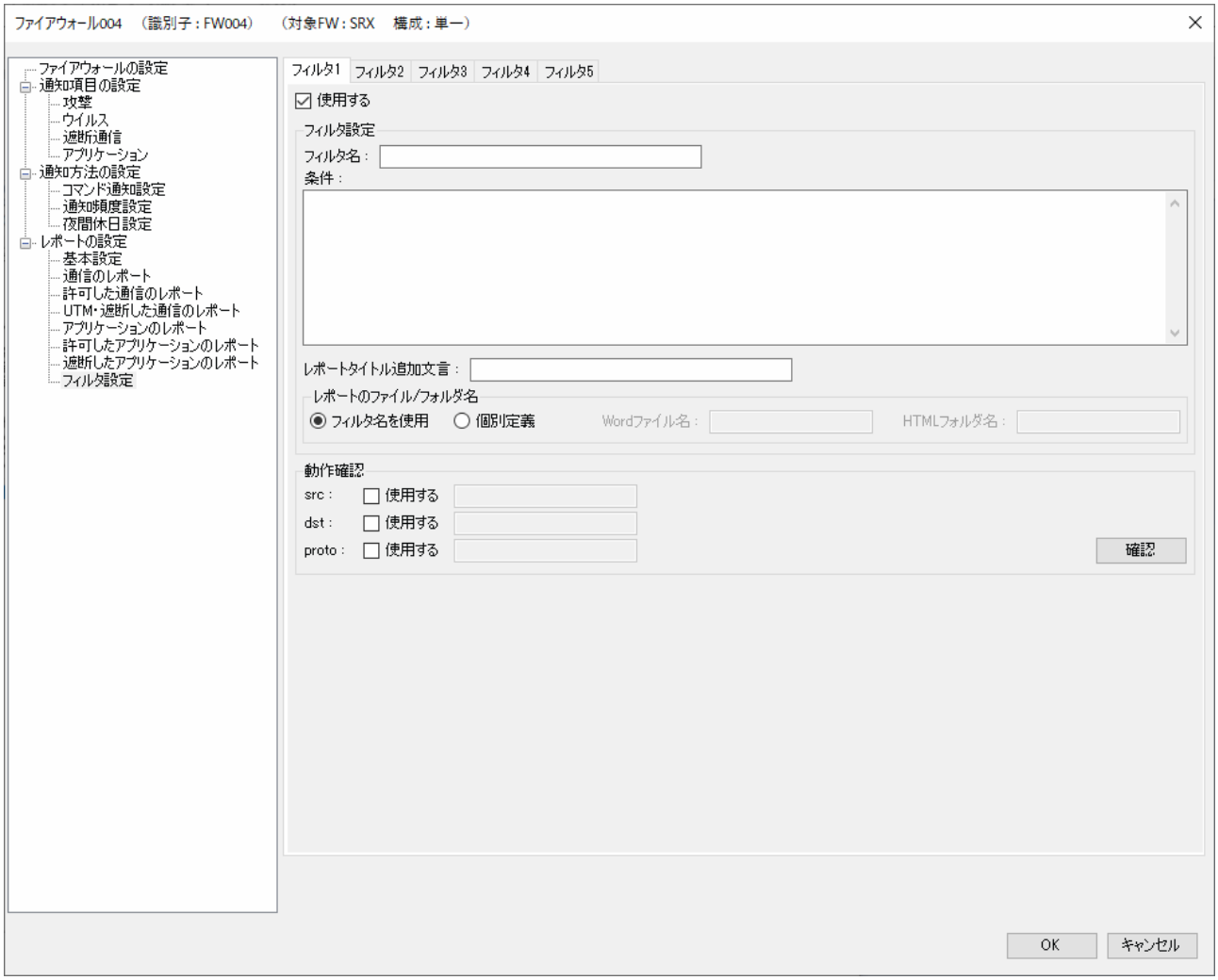


図 40 [フィルタ設定]パネル

(1) [使用する]チェックボックス

[フィルタ *n*]を有効にする場合に，設定します。

(2) [フィルタ設定]グループボックス

(a) [フィルタ名]テキストボックス

フィルタの名称を指定します。

(b) [条件]テキストボックス

フィルタの条件を指定します。記述ルールは，以下のとおりです。

```
<条件>::=(<論理式>)|(<論理式> AND <論理式>)|(<論理式> OR <論理式>)
<論理式>::=<フィールド識別子><演算子><値>
<フィールド識別子>::='src'|'dst'|'proto'
<演算子>::='='|'!='
<値>::="(任意の文字列)"
```

- 条件は，論理式単独か，論理式を AND で連結したものか，論理式を OR で連結したものとします
- カッコ（「(」と「)」）で優先順位を付けられます。また，カッコは省略可能です
- カッコが省略された場合は，AND の連結が優先となります
- 論理式は，「<フィールド識別子><演算子><値>」という書式で記述します

  例）

  src="133.108.182.*"

  dst!="192.168.*"

- 演算子の意味は，以下の通りです

  = ：フィールド識別子は，値を「含む」ことを意味します

  != ：フィールド識別子は，値を「含まない」ことを意味します

- 値は「"」で括られた任意の文字列を指定できますが，値に「"」を含むことは出来ません

(c) [レポートタイトル追加文言]テキストボックス

レポート表紙のタイトル（**4.1.2** [レポート表紙設定]パネル**参照**）に追加する文言を指定します。50 文字まで指定できます。

(d) [レポートのファイル/フォルダ名]グループボックス

フィルタしたレポートの「Word レポートのファイル名」に指定できる置換文字「%FILTER_WORD%」と「HTML レポートのフォルダ名」に指定できる置換文字「%FILTER_HTML%」（5.1.4 [生成レポートファイル設定]パネル 表 5.1-1 置換文字 参照）の値をそれぞれ指定します。

[フィルタ名を使用]を選択した場合は，(a)[フィルタ名]テキストボックスに指定した値となります。[個別定義]を選択した場合は，[Word ファイル名][HTML フォルダ名]を各々指

定できます。

Windows のファイル名で使用できない文字（/ ¥ など）を指定すると，レポートの生成が失敗します。

(3) [動作確認]グループボックス

[src][dst][proto]で指定した値のレコードが，指定した[条件]でレポート対象となるかレポート対象とならないかを，検証することが出来ます。

5 共通の設定

5.1　FIREWALLstaff の共通設定

FIREWALLstaff システムにおける共通の事項を設定します。[ツール]－[オプション]で[オプション]ダイアログを開きます。

5.1.1　[Syslog 設定]パネル

FIREWALLstaff システムにおける Syslog 受信に関する設定をします。

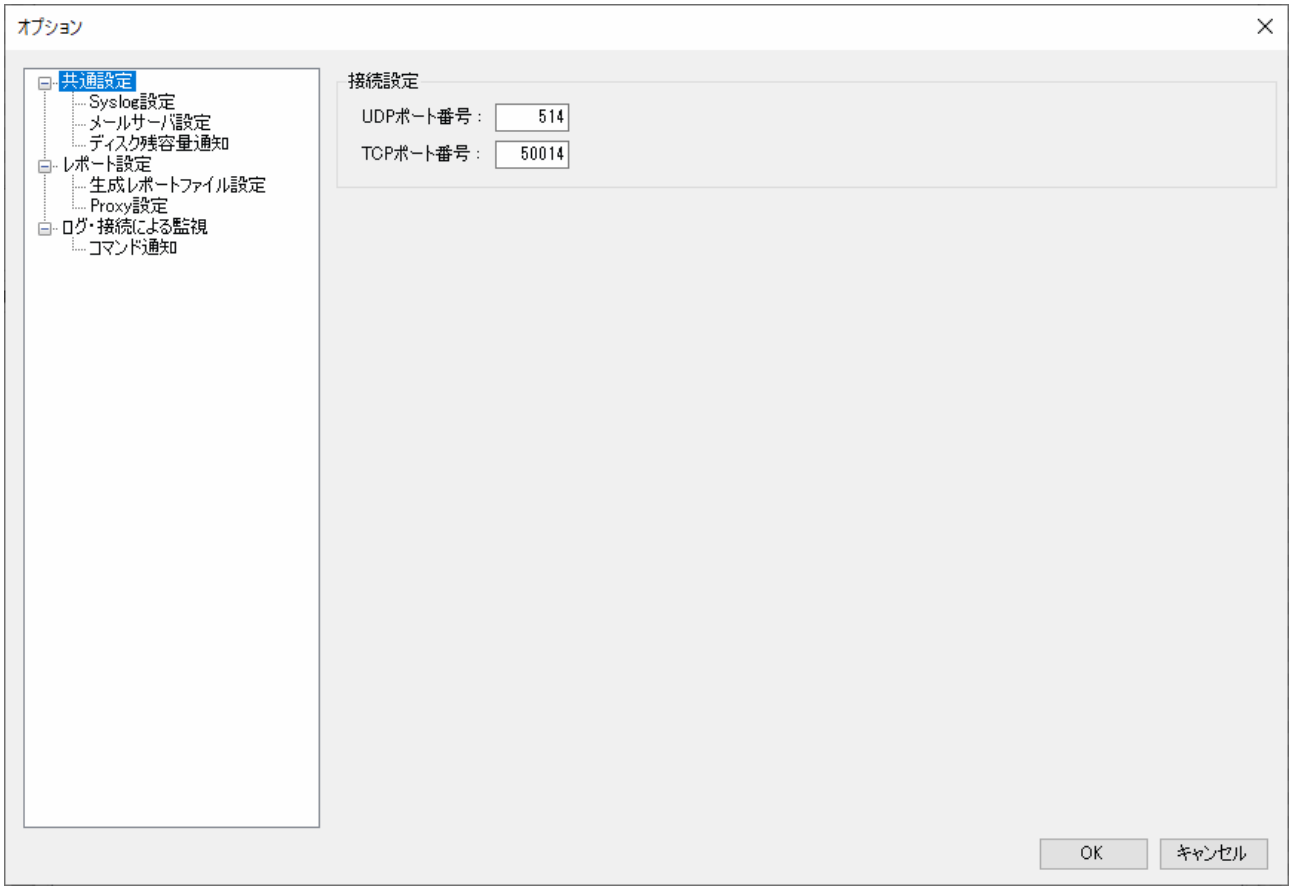


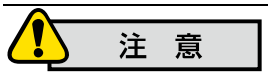
図 41 [Syslog 設定]パネル

(1)　[UDP ポート番号]テキストボックス

ファイアウォールから送られてくる Syslog を受信する UDP のポート番号を 0～65535 の範囲で指定します。デフォルトは，514 です。**ポート番号を変更した場合は FIREWALLstaff Log サービスを再起動する必要があります。**

(2)　[TCP ポート番号]テキストボックス

ファイアウォールから送られてくる Syslog を受信する TCP のポート番号を 0～65535 の範囲で指定します。デフォルトは，50014 です。**ポート番号を変更した場合は FIREWALLstaff Log サービスを再起動する必要があります。**



FIREWALLstaff では，TCP の Syslog 受信は RFC 6587 で紹介されている「3.4.2. 非透過フレーミング」方式にのみに対応しています。

RFC 6587 で紹介されている「3.4.1. オクテットカウント」の方式には対応していませんのでご注意ください。

5.1.2　[メールサーバ設定]パネル

FIREWALLstaff システムにおけるメールサーバの設定をします。

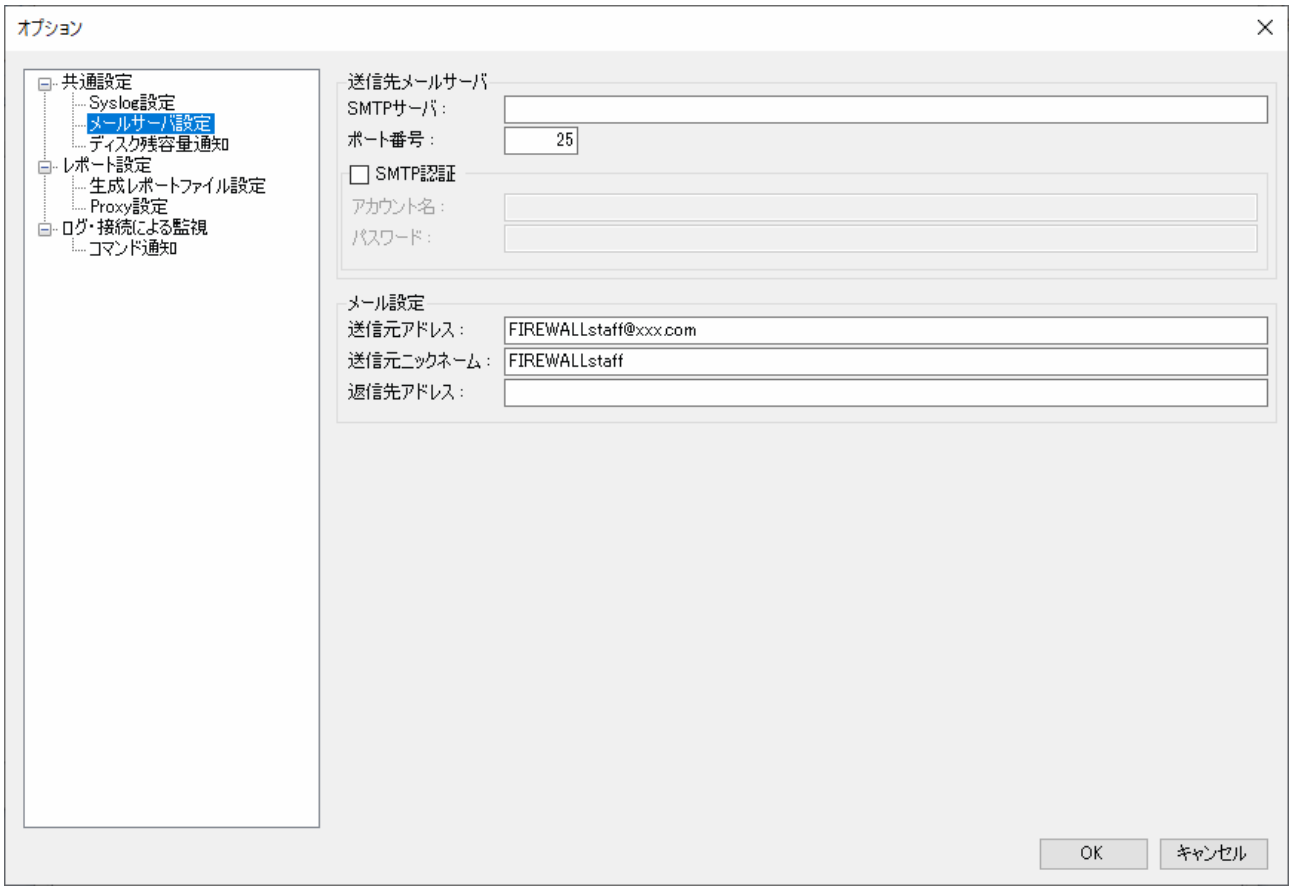


図 42 [メールサーバ設定]パネル

(1) [送信先メールサーバ]グループボックス

FIREWALLstaff がメールを発信するときに使用する，SMTP サーバの指定を行います。

(a) [SMTP サーバ]テキストボックス

SMTP サーバの IP アドレスを指定します。

(b) [ポート番号]テキストボックス

SMTP サーバの通信ポートのポート番号を 0～65535 の範囲で指定します。デフォルトは，25 です。

(c) [SMTP 認証]チェックボックス

SMTP サーバがメール送信時に認証を行う場合，選択してください。認証を行わない場合は選択しないでください。対応している SMTP 認証方式は，PLAIN，LOGIN，CRAM-MD5 です。

(d) [アカウント名]テキストボックス

SMTP サーバが認証を行う際の，アカウント名を指定します。

(e) [パスワード]テキストボックス

SMTP サーバが認証を行う際の，アカウント名に対するパスワードを指定します。

(2) [メール設定]グループボックス

(a) [送信元アドレス]テキストボックス

FIREWALLstaff がメールを発信するときに使用する，差出人アドレスを指定します。指定した SMTP サーバに存在するアカウントのメールアドレスを設定してください。

(b) [送信元ニックネーム]テキストボックス

FIREWALLstaff がメールを発信するときに使用する，送信者名(From 情報)を指定します。

(c) [返信先アドレス]テキストボックス

FIREWALLstaff が発信したメールの返信先を送信メールアドレスと変えたい場合に，返信先のメールアドレスを指定します。ここを省略すると，送信メールアドレスが返信先になります。

5.1.3　[ディスク残容量通知]パネル

データフォルダがあるドライブのディスク容量が少なくなった場合に，メールにより通知を行うことができます。

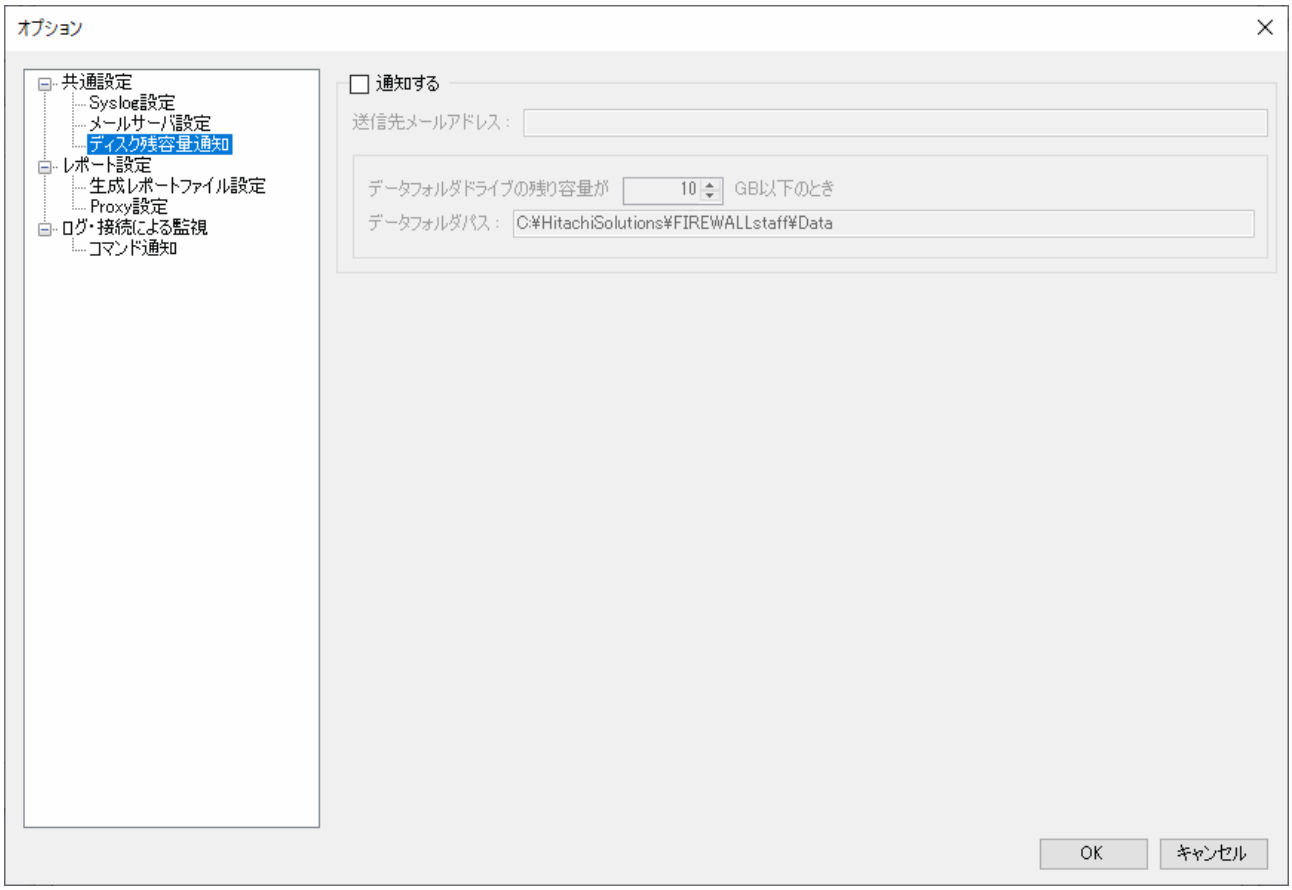


図 43 [ディスク残容量通知]パネル

(1) [通知する]チェックボックス

データフォルダがあるドライブのディスク容量が少なくなった場合にメール通知する場合，選択します

(a) [送信先メールアドレス]テキストボックス

通知する宛先メールアドレスを指定します。「,」（カンマ）区切りで，最大 10 まで指定できます。

(b) [残容量]スピンボタン

通知するディスク残容量を指定します。毎日午前 0 時にディスク容量のチェックを行います。

(c) [データフォルダパス]テキストボックス

インストール時に指定した FIREWALLstaff データフォルダを表示します。

5.1.4　[生成レポートファイル設定]パネル

FIREWALLstaff システムにおけるレポート生成に関する共通の設定をします。

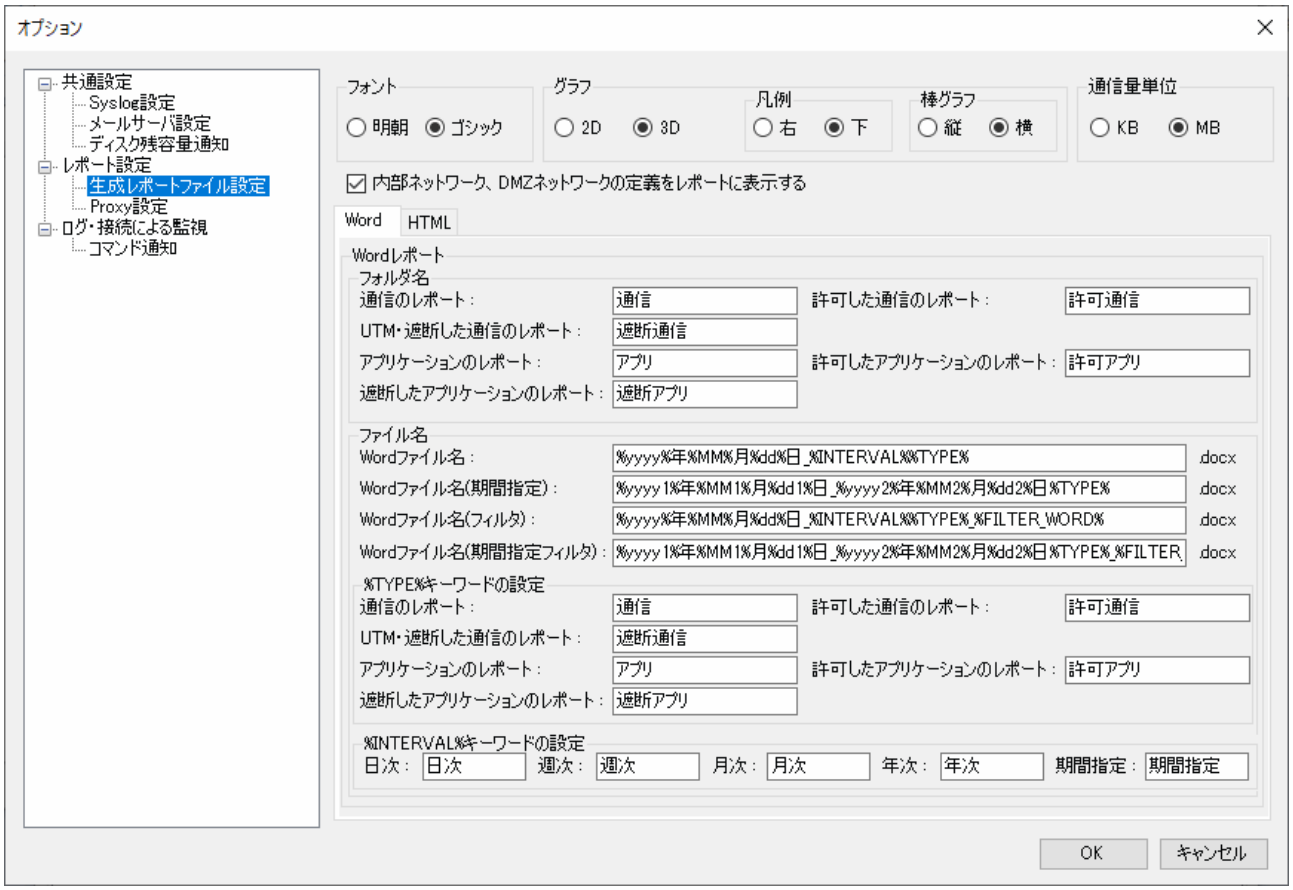


図 44 [生成レポートファイル設定]パネル(Word)

(1) [フォント]グループボックス

レポートのフォントを，明朝とゴシックから指定できます。

(2) [グラフ]グループボックス

グラフを，2D と 3D から指定できます。

(a) [凡例]グループボックス

棒グラフの凡例の位置を，右と下から指定できます。

(b) [棒グラフ]グループボックス

棒グラフを，縦棒グラフと横棒グラフから指定できます。

(3) [通信量単位]グループボックス

通信量の単位を，KB と MB から指定できます。

(4) [内部ネットワーク、DMZ ネットワークの定義をレポートに表示する]チェックボックス

内部ネットワークおよびDMZ ネットワークの定義をレポートに表示させる場合に選択します。選択した場合，各レポートの表紙の次に，以下の内容を表示します。

【CheckPoint 以外】の場合

- 「2.1.1(4)(a) [内部ネットワーク] グループボックス」で設定した内容
- 「2.1.1(4)(b) [DMZ ネットワーク] グループボックス」で設定した内容

【CheckPoint】の場合

- 「2.1.2(4)(a) [内部ネットワーク]グループボックス」で設定した内容
- 「2.1.2(4)(b) [DMZ ネットワーク]グループボックス」で設定した内容

(5) [Word レポート]グループボックス

Word レポートを生成するときに使用する，フォルダ名とファイル名の指定を行います。

(a) [フォルダ名]グループボックス

Word レポートを保存するフォルダ名を指定します。20 文字まで指定できます。

(b) [ファイル名]グループボックス

Word レポートのファイル名を指定します。表 5.1-1 の置換文字を使用できます。100 文字まで指定できます。

表 5.1-1 置換文字

置換文字	説明
%yyyy%	西暦 4 桁
%yy%	西暦下 2 桁(桁揃え 0 埋めあり:00～99)
%MM%	月 2 桁(桁揃え 0 埋めあり:01～12)
%M%	月 1～2 桁(桁揃え 0 埋めなし:1～12)
%dd%	日 2 桁(桁揃え 0 埋めあり:01～31)
%d%	日 1～2 桁(桁揃え 0 埋めなし:1～31)
%yyyy1%	期間指定レポートの開始日付の西暦 4 桁
%yy1%	期間指定レポートの開始日付の西暦下 2 桁(桁揃え 0 埋めあり:00～99)
%MM1%	期間指定レポートの開始日付の月 2 桁(桁揃え 0 埋めあり:01～12)
%M1%	期間指定レポートの開始日付の月 1～2 桁(桁揃え 0 埋めなし:1～12)
%dd1%	期間指定レポートの開始日付の日 2 桁(桁揃え 0 埋めあり:01～31)
%d1%	期間指定レポートの開始日付の日 1～2 桁(桁揃え 0 埋めなし:1～31)
%yyyy2%	期間指定レポートの終了日付の西暦 4 桁

%yy2%	期間指定レポートの終了日付の西暦下 2 桁(桁揃え 0 埋めあり:00～99)
%MM2%	期間指定レポートの終了日付の月 2 桁(桁揃え 0 埋めあり:01～12)
%M2%	期間指定レポートの終了日付の月 1～2 桁(桁揃え 0 埋めなし:1～12)
%dd2%	期間指定レポートの終了日付の日 2 桁(桁揃え 0 埋めあり:01～31)
%d2%	期間指定レポートの終了日付の日 1～2 桁(桁揃え 0 埋めなし:1～31)
%TYPE%	レポート種別。値は「%TYPE%キーワードの設定」で指定できます
%INTERVAL%	レポート期間(日次/週次/月次/年次/期間指定)。値は「%INTERVAL%キーワードの設定」で指定できます
%FW_NAME%	ファイアウォール名（2.1.1[ファイアウォールの設定]パネルの[名称]テキストボックスで指定した値）
%FILTER_NAME%	フィルタ名（4.8.1[フィルタ設定]パネルの[フィルタ名]テキストボックスで指定した値）
%FILTER_WORD%	フィルタ用 Word ファイル名（4.8.1[フィルタ設定]パネルの[Word ファイル名]テキストボックスで指定した値）
%FILTER_HTML%	フィルタ用 HTML フォルダ名（4.8.1[フィルタ設定]パネルの[HTML フォルダ名]テキストボックスで指定した値）

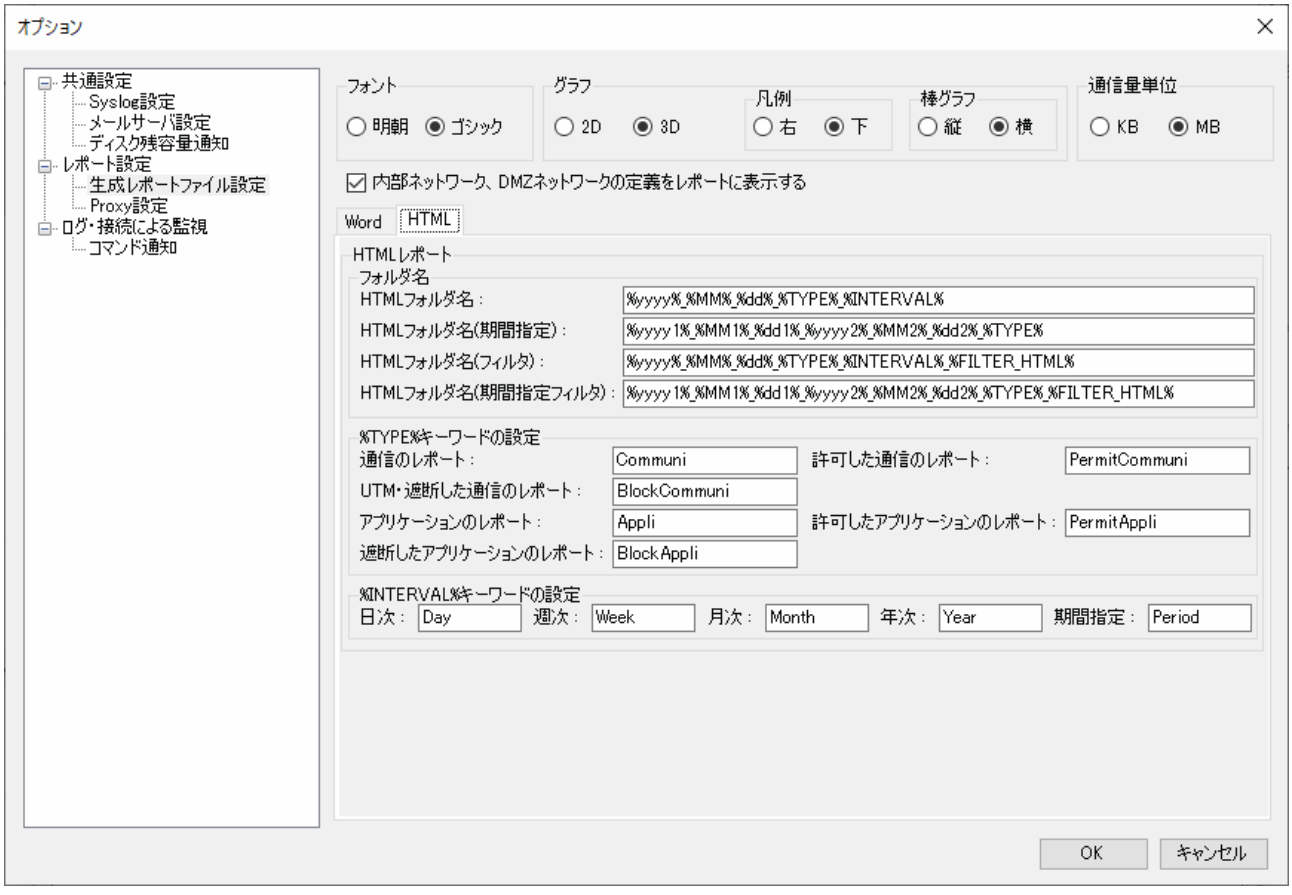


図 45 [生成レポートファイル設定]パネル(HTML)

(6) [HTML レポート]グループボックス

HTML レポートを生成するときに使用する，フォルダ名の指定を行います。

(a) [フォルダ名]グループボックス

Word レポートを保存するフォルダ名を指定します。表 5.1-1 の置換文字を使用できます。100 文字まで指定できます。

注 意

Windows のファイル名で使用できない文字（/ ¥ など）を指定すると，レポートの生成が失敗します。

5.1.5　[Proxy 設定]パネル

FTP を利用してログを取得するときに,Proxy サーバを使用するかしないかを設定します。

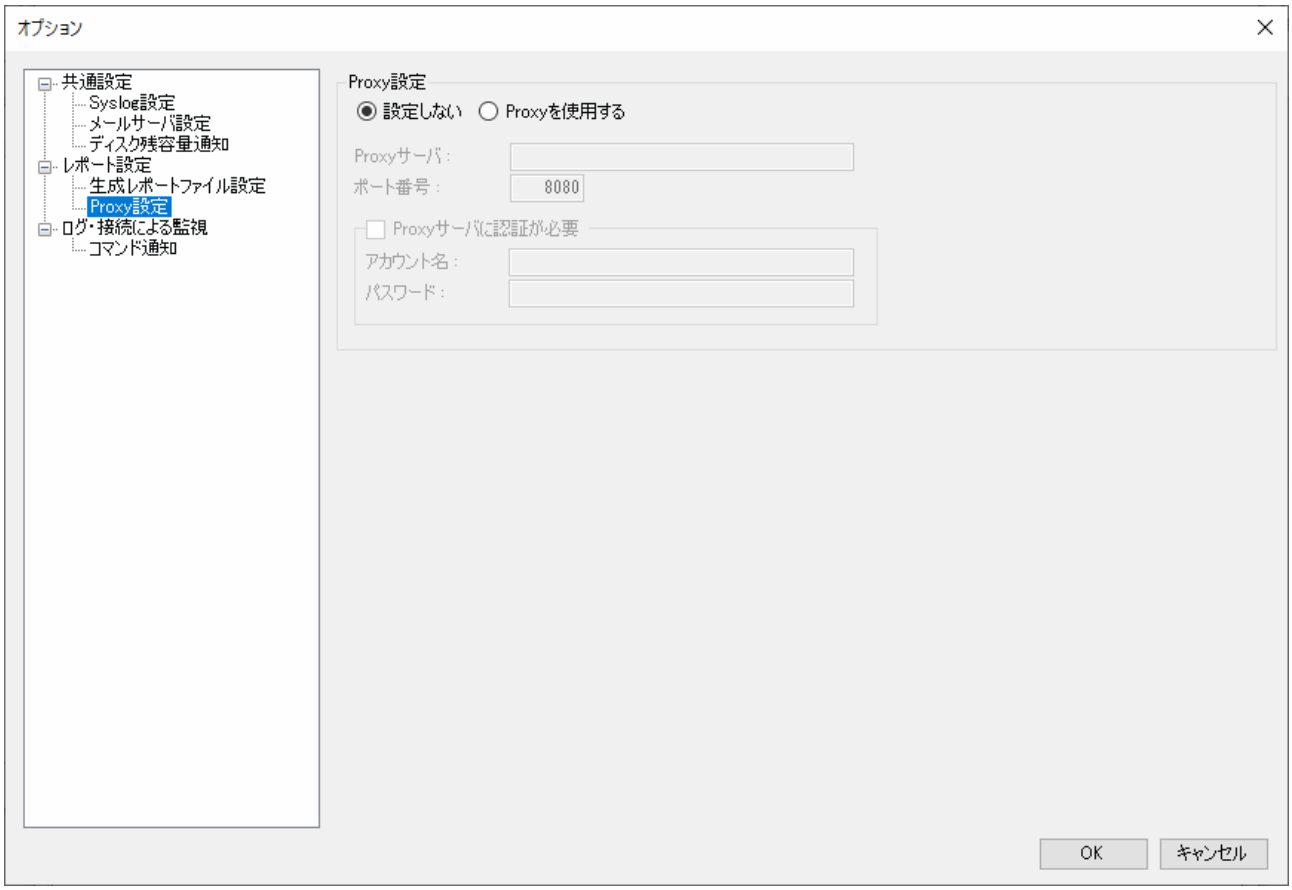


図 46 [Proxy 設定]パネル

(1)　[Proxy 設定]グループボックス

(a)　[設定しない]ラジオボタン

Proxy サーバを使用しない場合，選択します。

(b) [Proxy を使用する]ラジオボタン

Proxy サーバを使用する場合，選択します。

(c) [Proxy サーバ]テキストボックス

Proxy サーバの IP アドレスを指定します。

(d) [ポート番号]テキストボックス

Proxy サーバの通信ポートのポート番号を 0～65535 の範囲で指定します。

(2)　[Proxy サーバに認証が必要]グループボックス

Proxy サーバを使用する際に認証が必要な場合，選択します。

(a) [アカウント名]テキストボックス

Proxy サーバが認証を行う際の，アカウント名を指定します。

(b) [パスワード]テキストボックス

Proxy サーバが認証を行う際の，アカウント名に対するパスワードを指定します。

5.1.6　[コマンド通知]パネル

FIREWALLstaff システムにおけるコマンド通知に関する共通の設定をします。[コマンド通知]パネルを図 47 に示します。

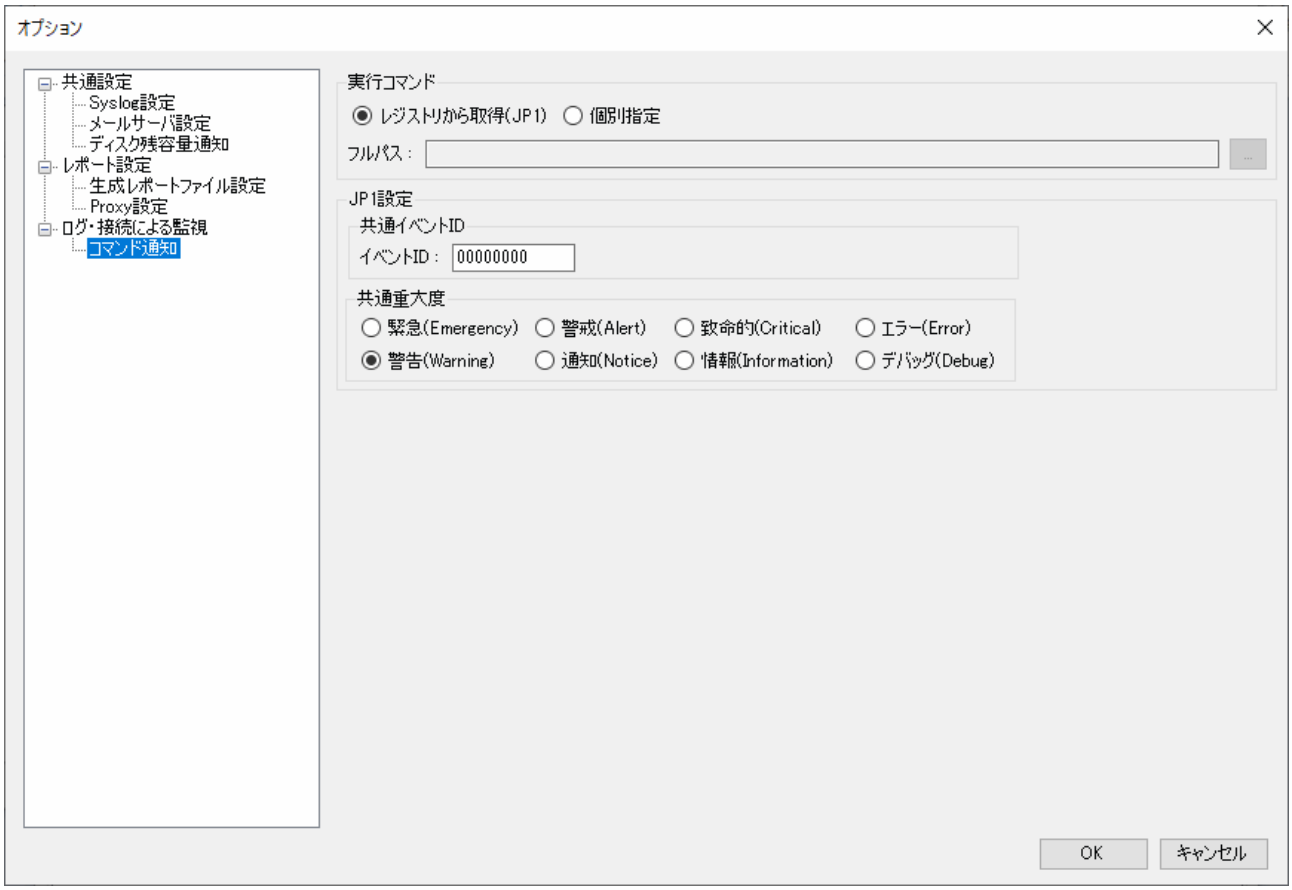


図 47 [コマンド通知]パネル

(1) [実行コマンド]グループボックス

コマンド通知を実行するときに使用する，コマンドの指定を行います。

(a) [レジストリから取得(JP1)]ラジオボタン

通知を実行するコマンドとして JP1/Base の jevsendd コマンドを使用します。レジストリから該当コマンドのフルパスが取得できた場合は[フルパス]テキストボックスにフルパスが表示されます。

(b) [個別指定]ラジオボタン

通知を実行するコマンドを個別に指定する場合はこのラジオボタンを選択し，[...]ボタンからコマンドを選択します。

(c) [...]ボタン

[個別指定]ラジオボタンを選択した場合に活性状態になります。ボタンを押すとファイル選択ダイアログが表示されますので，通知を実行するコマンドを選択してください。選択できるコマンドはローカルハードディスクドライブに存在するファイルのみです。選択し

たコマンドのフルパスが[フルパス]テキストボックスに表示されます。

(2) [JP1 設定]グループボックス

コマンド通知に JP1/Base のコマンド（jevsend または jevsendd）を使用する場合に有効となる設定です。

(a) [共通イベント ID]グループボックス

FIREWALLstaff システムにおいて共通使用する JP1/Base のコマンドの引数となるイベント ID を指定します。デフォルトとして，「00000000」が設定されています。

(b) [共通重大度]グループボックス

FIREWALLstaff システムにおいて共通使用する JP1/Base のコマンドの引数となる重大度を指定します。デフォルトとして，「警告(Warning)」が選択されています。

5.2　中間ファイルの削除

ログを解析した情報を保持する中間ファイルを手動で削除する場合に使用します。［ツール］－［中間ファイルの削除］で［中間ファイルの削除］ダイアログを開きます。

5.2.1　［中間ファイルの削除］ダイアログ

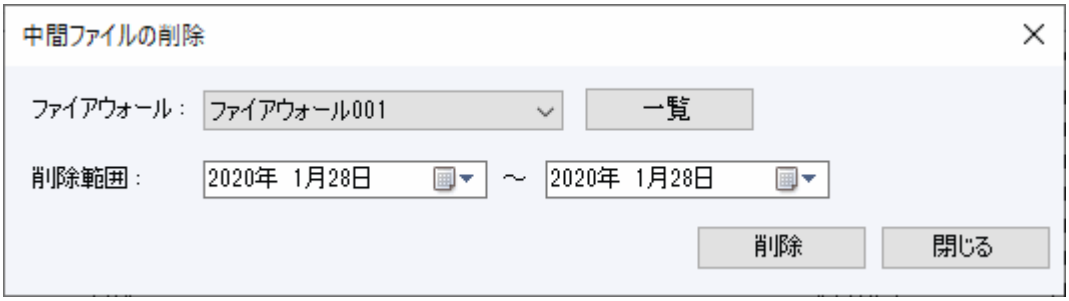


図 48 [中間ファイルの削除]ダイアログ

(1) ［ファイアウォール］コンボボックス

中間ファイルの削除を行いたいファイアウォール名を選択します。

(2) ［一覧］ボタン

選択したファイアウォール名の，中間ファイルの一覧を表示します。

(3) ［削除範囲］カレンダリスト

削除したい中間ファイルが含まれる期間を指定します。

(4) ［削除］ボタン

［削除］ボタンをクリックすると，中間ファイルの削除を行います。

(5) ［閉じる］ボタン

［閉じる］ボタンをクリックすると，［中間ファイルの削除］ダイアログを閉じます。

6 FIREWALLstaff の運用・保守

6.1　サービス

FIREWALLstaff インストール時にサーバにインストールされれるサービスを表 6.1-1 に示します。サービスの起動や停止を行う場合は，Windows の[コントロールパネル]から，[管理ツール]－[サービス]を開きます。

表 6.1-1 FIREWALLstaff のサービス

項番	サービス名	プロセス名
1	FIREWALLstaff Log	fstaff_syslog.exe
2	FIREWALLstaff Monitor	fstaff_monitor.exe
3	FIREWALLstaff Scheduler	fstaff_scheduler.exe

6.2 バックアップ・リストア

(1) バックアップ

FIREWALLstaff で使用する情報は，「FIREWALLstaff データフォルダ」に格納されています。以下の設定を変更している場合は，変更先もバックアップ対象に加えてください。

（ア）「2.1.1(5) [サービスによるログ保存先/中間ファイルの保存先フォルダ]グループボックス」にて設定を変更している場合

（イ）「4.1.1(1) [Word レポート保存先フォルダ]テキストボックス」にて設定を変更している場合

（ウ）「4.1.1(2) [HTML レポート保存先フォルダ]テキストボックス」にて設定を変更している場合

バックアップを取得する場合は，すべてのサービスを停止してから行ってください。

(2) リストア

バックアップしたデータをリストアする場合は，以下の手順を実行してください。

1. FIREWALLstaff のすべてのサービスを停止します。
2. FIREWALLstaff データフォルダをバックアップした FIREWALLstaff データフォルダと入れ替えてください。
3. （ア）～（ウ）のいずれかに該当する場合は，それぞれに対してバックアップしたデータと入れ替えてください。
4. 停止したサービスを起動してください。

注 意

異なる FIREWALLstaff のバージョン間での，バックアップ・リストアは出来ません。

6.3 Palo Alto 用カテゴリリスク定義ファイル

お客様が定義したアプリケーションがある場合は,

<FIREWALLstaff データフォルダ>¥user¥paloalto_user_apprisk.xml

を下記記述方法で書き換えてください。

paloalto_user_apprisk.xml は以下のような構造になっています。

```
<?xml version="1.0" encoding="utf-8"?>
<PaloAltoData xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/
2001/XMLSchema">
  <categoryList>
    <PaloAltoCategory>
      <categoryName>file-sharing</categoryName>
      <appList>
        <PaloAltoApplication>
          <appName>myapp01</appName>
          <appRisk>1</appRisk>
        </PaloAltoApplication>
        <PaloAltoApplication>                    1つのアプリケーション
          <appName>myapp02</appName>
          <appRisk>3</appRisk>
        </PaloAltoApplication>
      </appList>
    </PaloAltoCategory>
  </categoryList>                                              1つのカテゴリ
</PaloAltoData>
```

図 49 Palo Alto 用カテゴリリスク定義ファイルの構造

上記では以下の事柄を定義しています。

- カテゴリ「file-sharing」にアプリケーション「myapp01」と「myapp02」が属している。
- アプリケーション「myapp01」のリスクは「1」である。
- アプリケーション「myapp02」のリスクは「3」である。

上記を参考に必要なカテゴリとアプリケーションとリスクの組み合わせを paloalto_user_apprisk.xml に定義してください。

日立ソリューションズ

http://www.hitachi-solutions.co.jp/