HITACHI
Inspire the Next

ファイアウォールのログ収集と、レポート作成

FIREWALLstaff 体験版の手引き

対象バージョン：02-08

株式会社 日立ソリューションズ

2022年1月版

1 - 1 インストール

FIREWALLstaffをインストールします。インストール手順の概略は、次のとおりです。

（１）Microsoft .NET Frameworkとして、以下のいずれかがインストールされていることを確認
　　Microsoft .NET Framework 4.5.1～4.8
　　→『取扱説明書（インストール編）』 2.2.1 前提ソフトウェアの確認
（２）FIREWALLstaffのインストール
　　・32ビットOSの場合はsetup_x86.exeをダブルクリック
　　・64ビットOSの場合はsetup_x64.exeをダブルクリック
　して、ウィザードに従いインストールを行います
（３）Windowsファイアウォールの例外設定

詳細なインストール手順は、『取扱説明書（インストール編）』を参照してください。

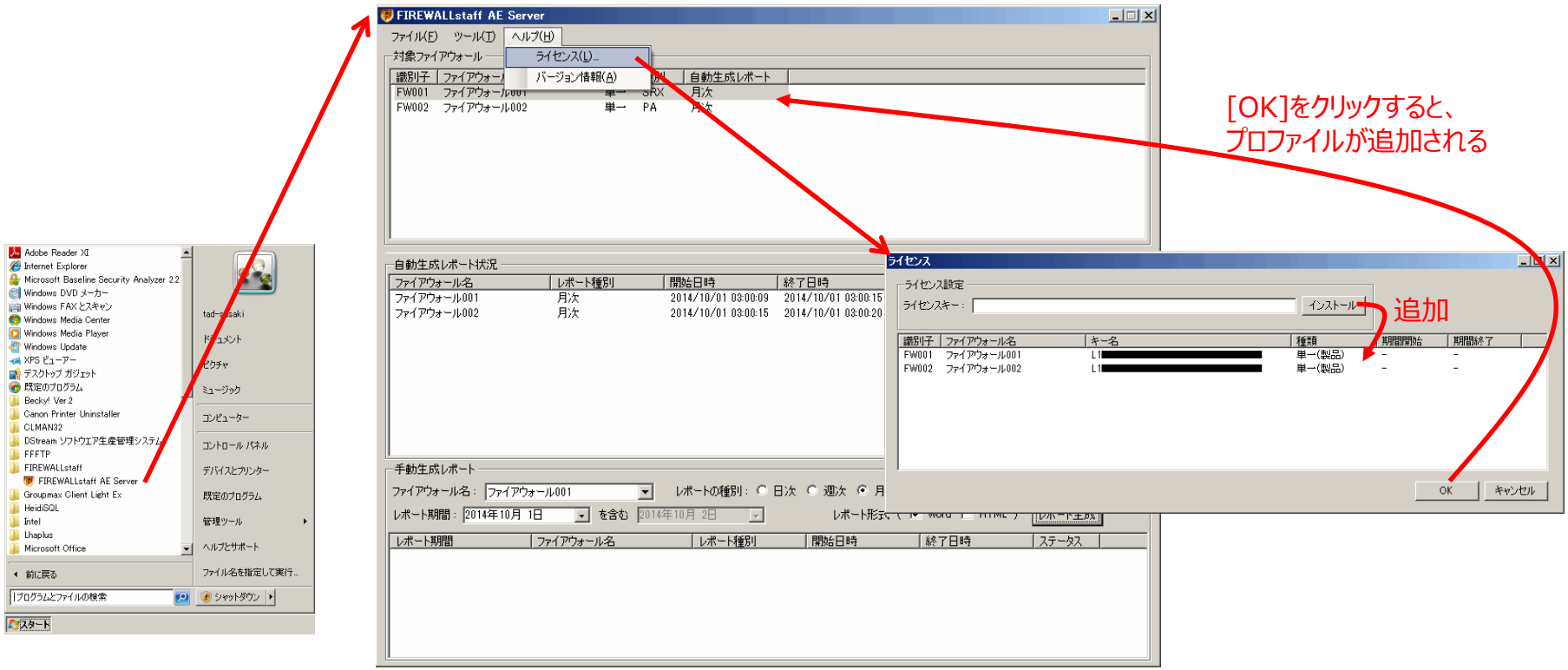
以下、本手引きでは、インストール時に指定した『インストールフォルダ』『データフォルダ』を、デフォルトの
　インストールフォルダ：
　　C:¥Program Files¥HitachiSolutions¥FIREWALLstaff
　データフォルダ：
　　C:¥HitachiSolutions¥FIREWALLstaff¥Data
として説明します。

1 - 2 ライセンスキーのインストール

WindowsOSの[スタート]→[FIREWALLstaff]→[FIREWALLstaff AE Server]を順にクリックすると、
　　FIREWALLstaff AE Serverメイン画面
を表示します。

FIREWALLstaff AE Serverメイン画面の[ヘルプ]→[ライセンス]をクリックすると、
　　ライセンスダイアログ
を表示しますので、[ライセンスキー]項目にライセンスキーを入力して[インストール]をクリックします。そして[OK]をクリックします。

ライセンスキーをインストールする度に、FIREWALLstaff AE Serverメイン画面の[対象ファイアウォール]に、プロファイルが追加されます。



FIREWALLstaff AE Server メイン画面

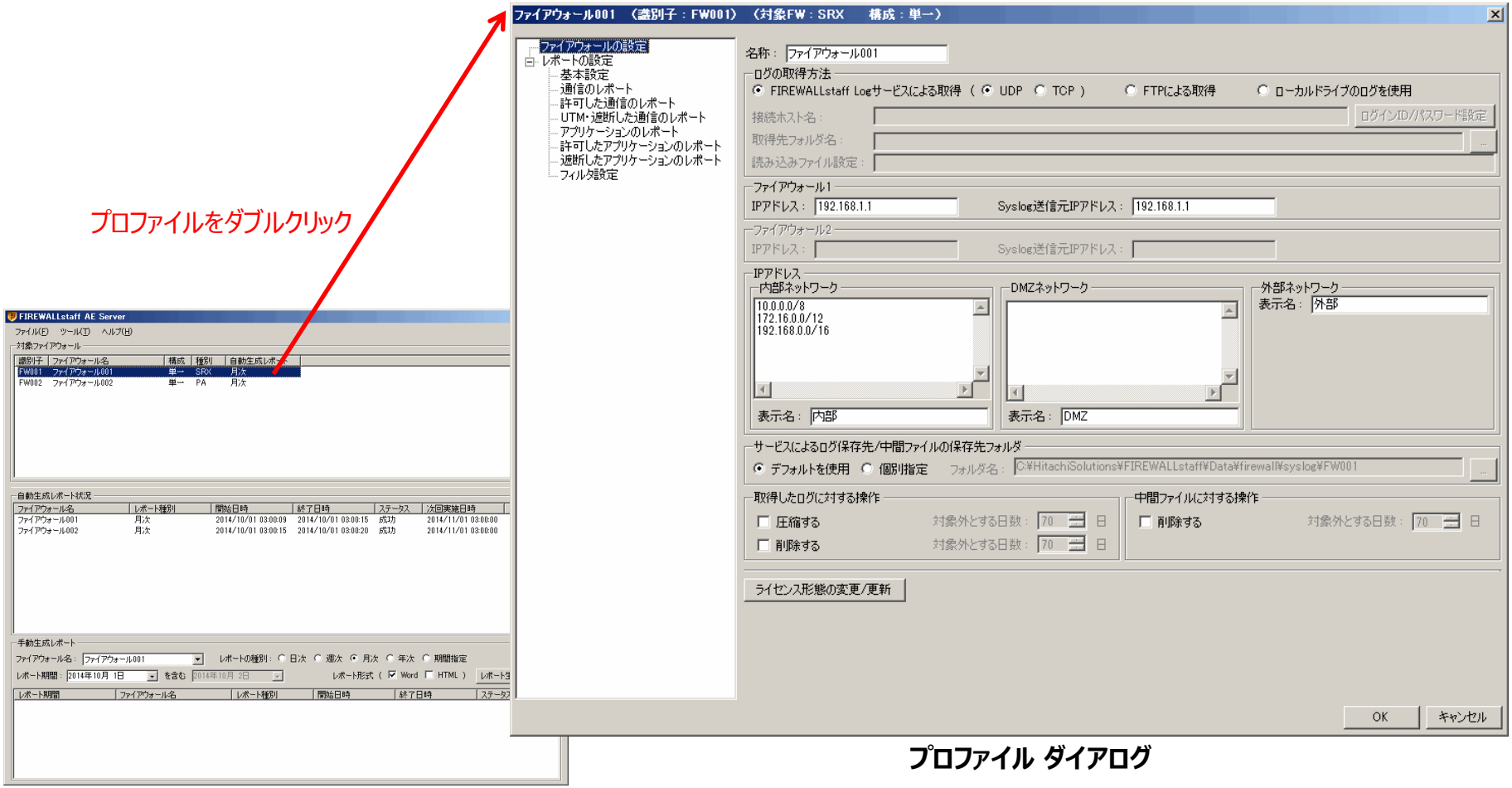
1 - 3 ファイアウォールの設定変更

ファイアウォールからログを出力する設定を行います。設定方法は、『取扱説明書（ファイアウォール設定編）』を参照してください。

設定変更手順の概略は、次のとおりです。
（１）ログ送信の設定
（２）ポリシ毎のログ出力の設定

1 - 4 プロファイルダイアログ

FIREWALLstaff AE Serverメイン画面の[対象ファイアウォール]のプロファイルをクリックすると、
　　プロファイルダイアログ
を表示します。

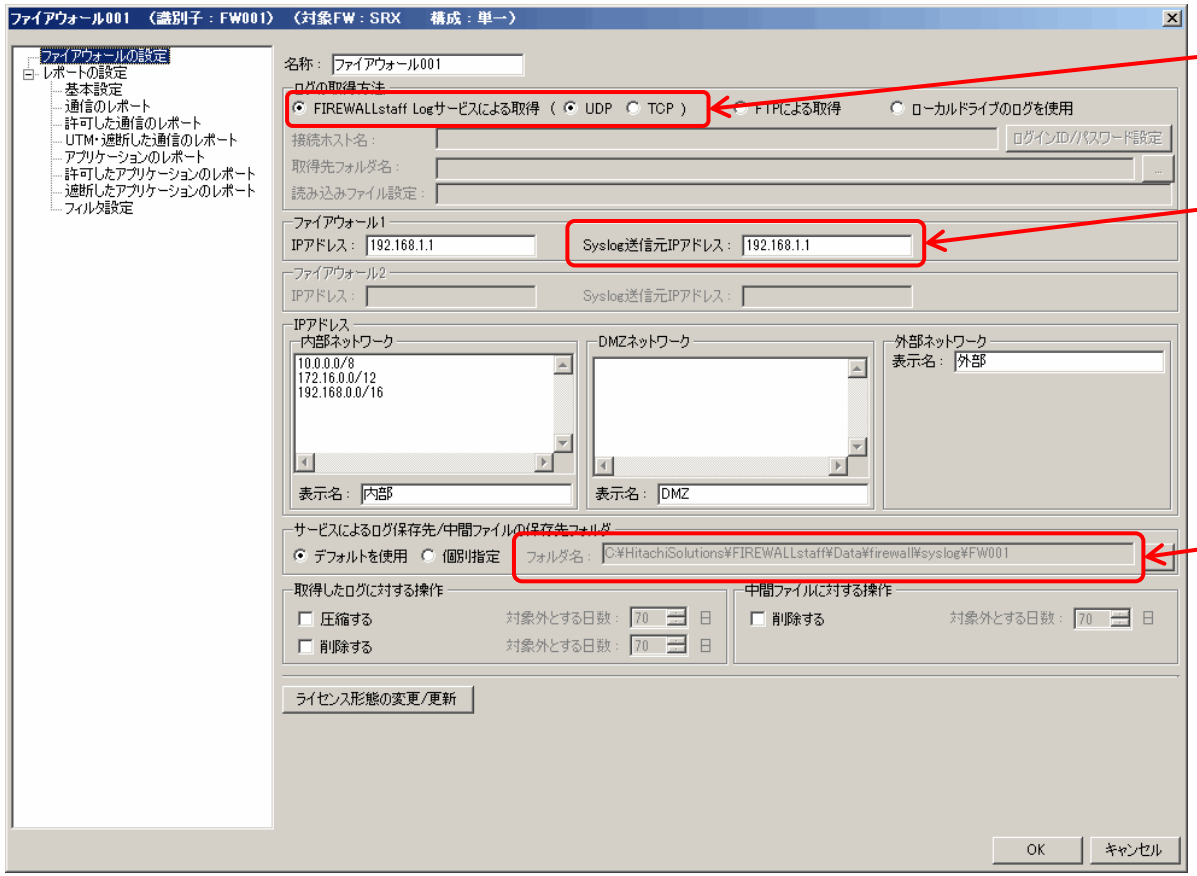


プロファイル ダイアログ

1 - 5 ログの取り込み方法

FIREWALLstaffでログを解析するための、ログの取り込み方法は3通りあります。本手引きでは、
（１）Syslogサービスによる取得
（２）ローカルドライブのログを使用
の2通りについて説明します。

（１） Syslogサービスによる取得



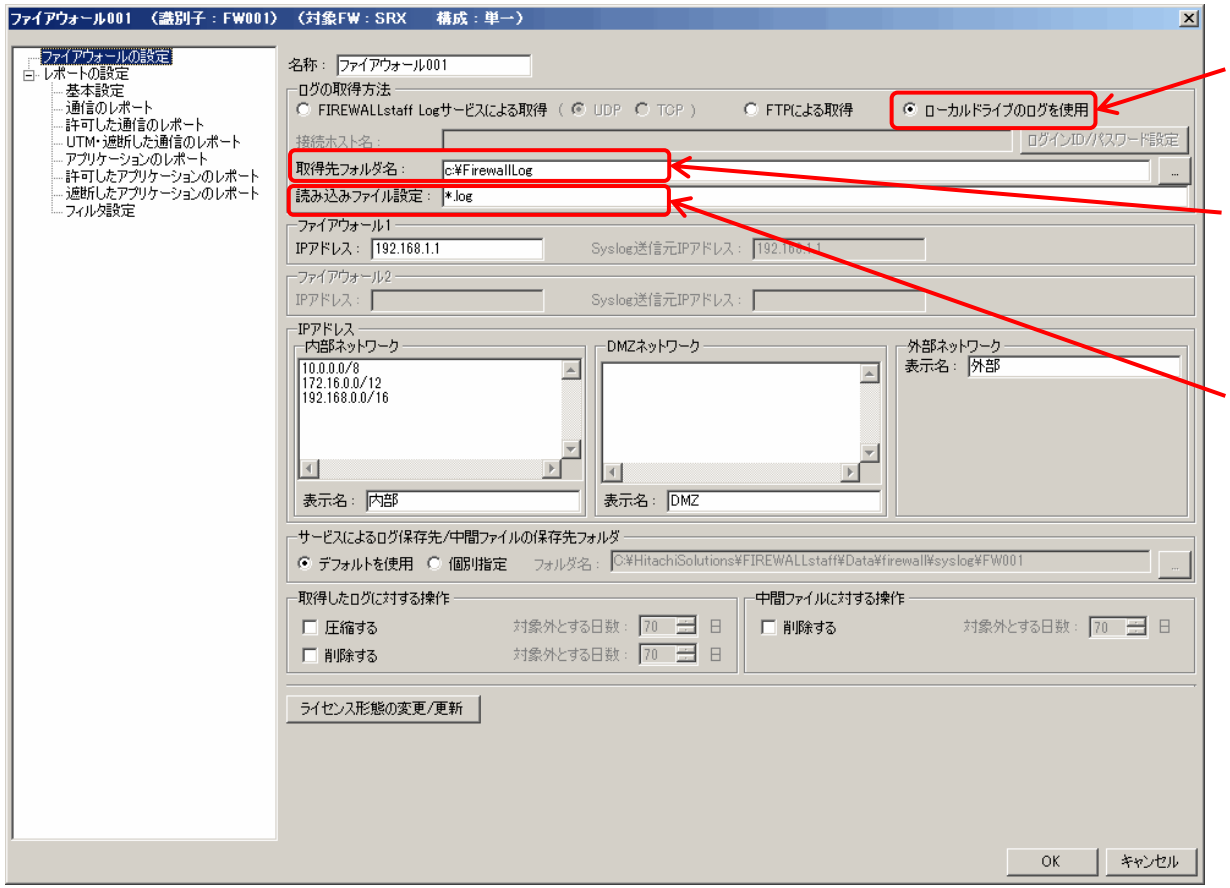
「FIREWALLstaff Logサービスによる取得」を選択

Syslog送信元（通常は、ファイアウォール）の
IPアドレスを指定

このフォルダに、Syslogを保存します

1 - 5 ログの取り込み方法

（２）ローカルドライブのログを使用



「ローカルドライブのログを使用」を選択

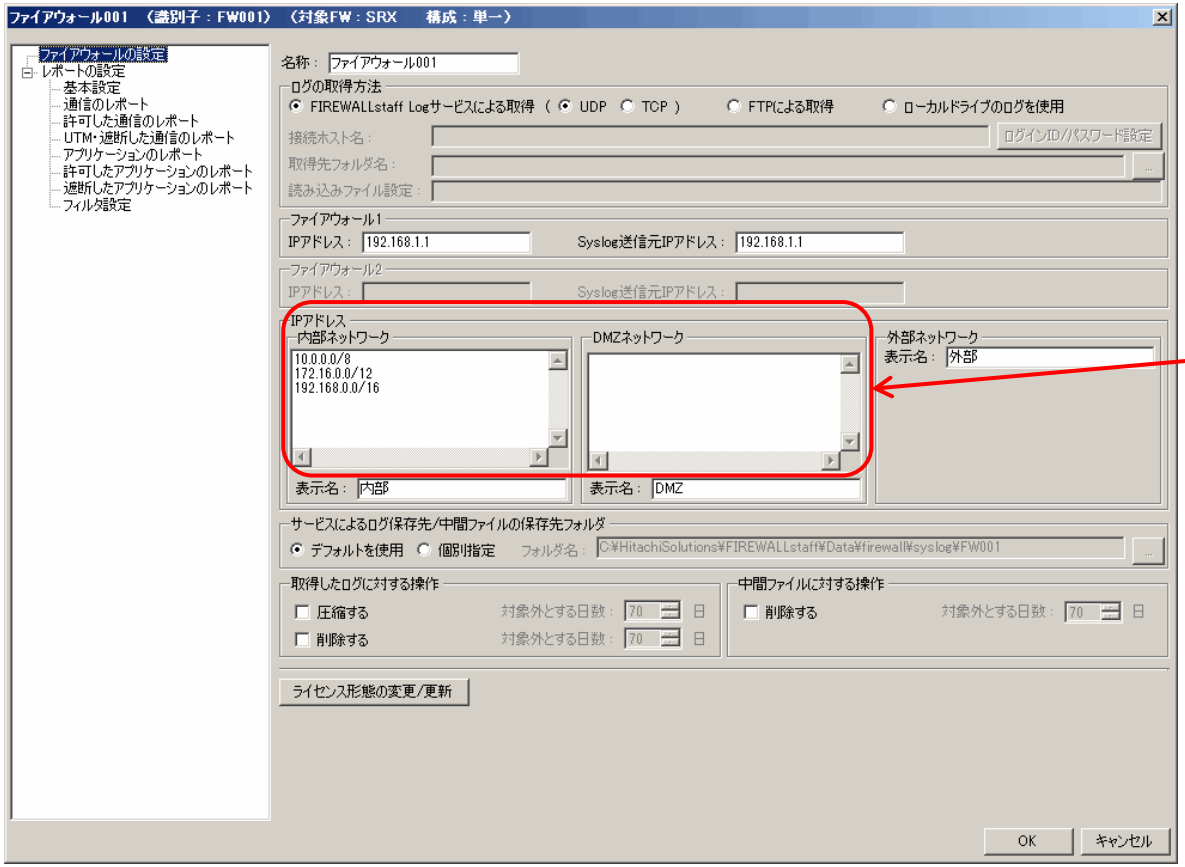
ログファイルのある、ローカルドライブのフォルダを指定

解析対象とするログファイル名を指定します
例）*.log

【参考】 ネットワークドライブにあるログを解析する場合は、『4-1　ネットワークドライブのログを解析する』を参照してください。

1 - 6 IPアドレスの指定

FIREWALLstaffでは、ファイアウォールが分割する3つのゾーン（外部、内部、DMZ）別にレポートすることができます。
そのため、IPアドレスを指定する必要があります。

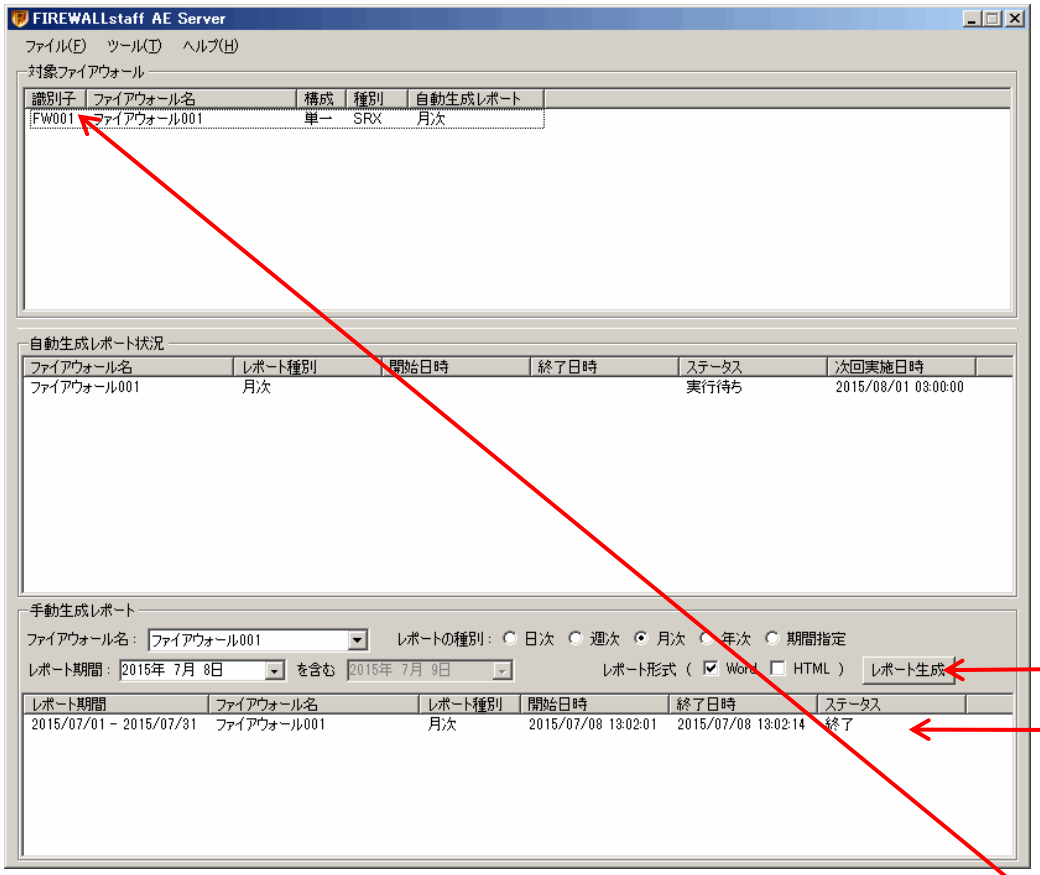


IPアドレスを指定

「*」（アスタリスク）またはCIDR記法による指定が可能です
例）192.168.0.0/16
　　192.168.*

1 - 7 手動でのレポート作成

手動でレポートを作成します。



[レポート生成]をクリックすると、レポートの作成を開始します

[ステータス]が「成功」となれば、レポート作成が終了しています

レポートを作成したプロファイルの「識別子」

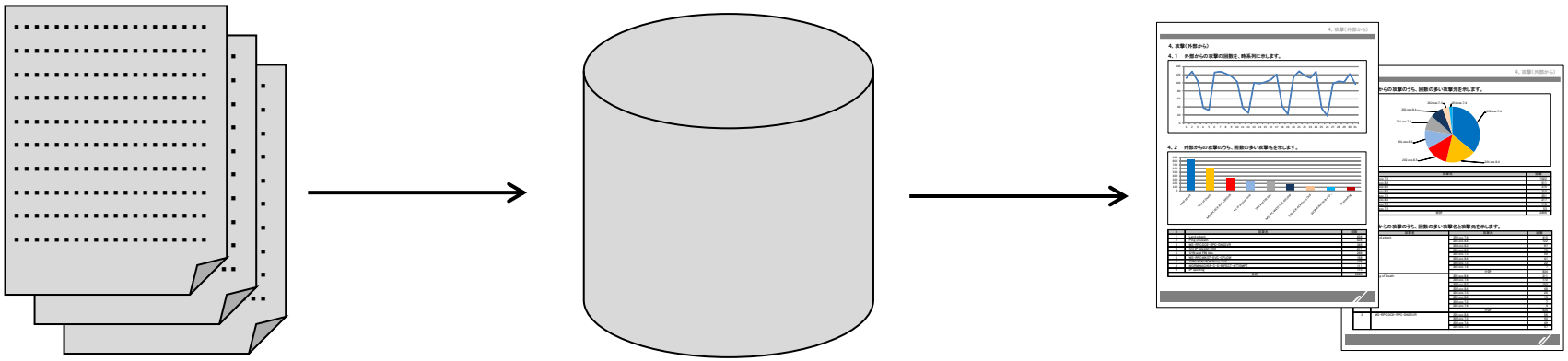
C:¥HitachiSolutions¥FIREWALLstaff¥Data¥report¥ FW001

配下に、フォルダとファイルが生成されておりますので、内容を確認してください。

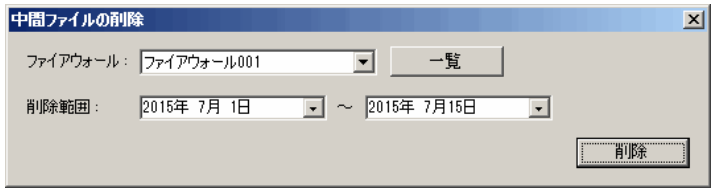
【参考】 レポートが出力されるフォルダとファイル名は、『2-1』『2-2』『2-3』を参照してください。

1-8 中間ファイル

FIREWALLstaffでは、解析したログの内容を1日単位に『中間ファイル』という独自形式で保持することで、レポート作成時にログ解析を何度も行わないようにしています。
そのため、FIREWALLstaffで設定を変更した場合は、中間ファイルを削除しないと、レポートの内容に反映されない場合があります。
特に、いろいろと設定を変更する評価期間中は注意してください。

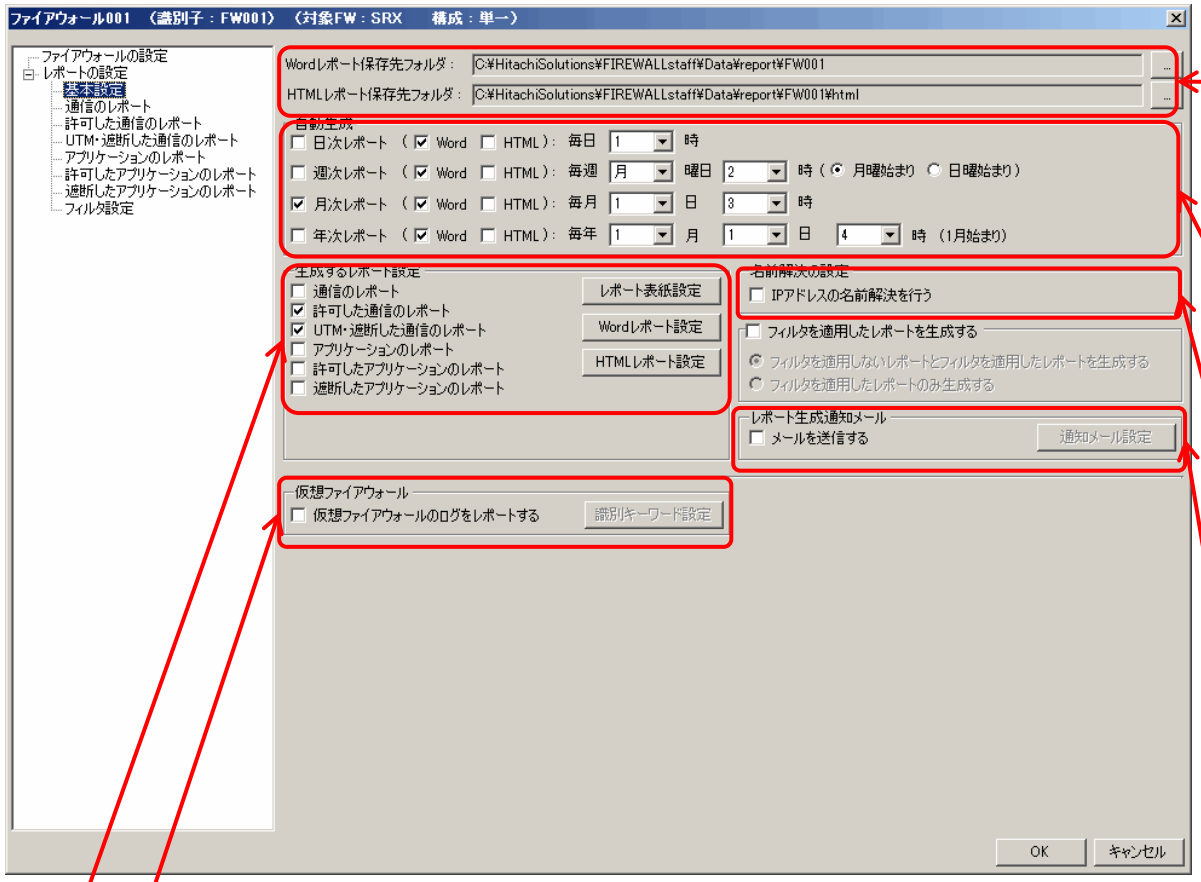


『中間ファイル』の削除は、
　FIREWALLstaff AE Serverダイアログの、[ツール]-[中間ファイルの削除]
で[中間ファイルの削除]ダイアログにより行います。



2-1 レポートの出力

レポートの出力に関する設定を行います。



レポートの出力先フォルダを指定します。
レポートのファイル名は、『2-2』『2-3』を参照してください

自動でレポートを作成する場合に、指定します。
図の設定例では、
毎月1日3時に、前月の月次レポートをWord形式で作成
します

レポート中のIPアドレスを名前解決する場合に、指定します。『3-3(5)』を参照してください

自動でレポートを作成する場合、レポート作成のタイミングでメールで通知することができます。
→メールサーバの指定が必要です。
『3-4(2)』を参照してください
また、Word形式のレポートは、通知メールに添付することができます

仮想ファイアウォールのログ（＝1ログファイルに、複数台のファイアウォールのログが含まれている）を解析する場合に、指定します。
本指定を誤ると、想定外のレポートとなる場合がありますので、『4-2』を参照して、**<u>必要な場合のみ指定してください</u>**

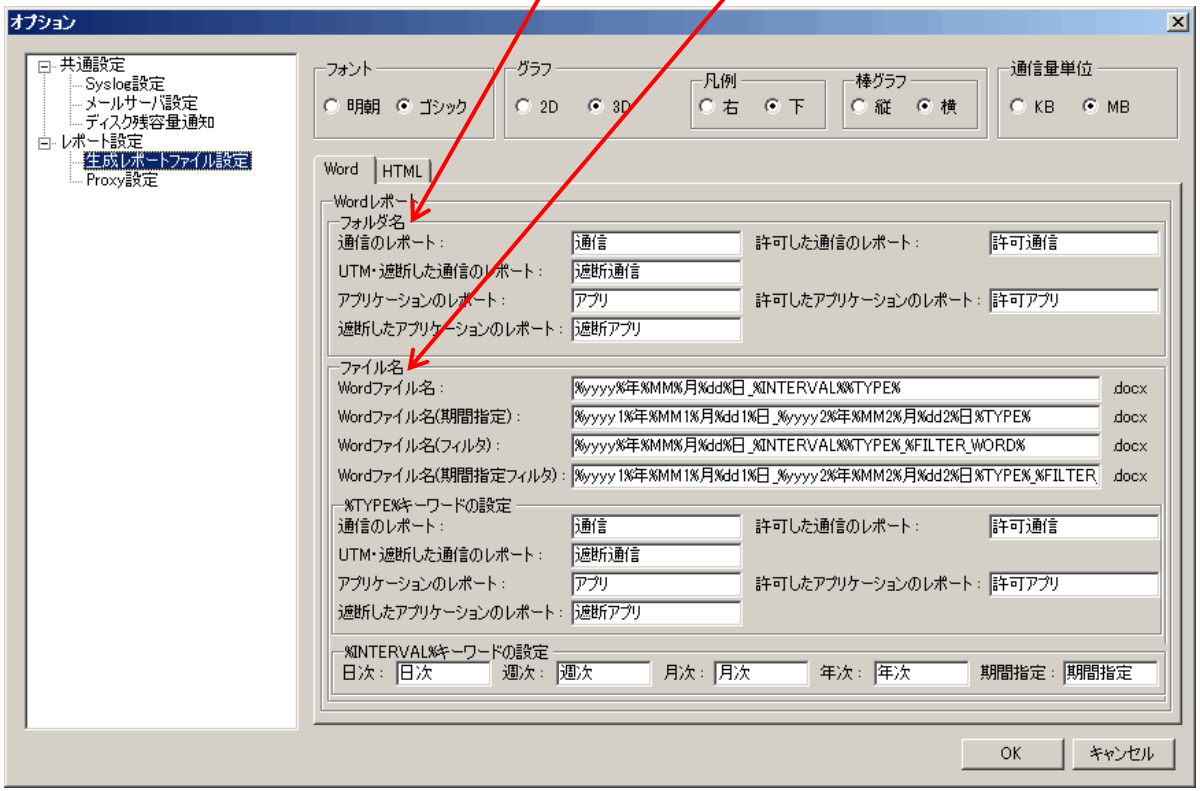
生成するレポートの種類を指定します。また、レポート表紙の文言、ヘッダフッタを設定します

2 - 2 Wordレポートの保存先とファイル名

Wordレポートの、保存先とファイル名は、

[Wordレポート保存先フォルダ] ¥ フォルダ名 ¥ ファイル名.docx

となります。



上の設定では、2015年7月の「UTM・遮断した通信のレポート」は、

[Wordレポート保存先フォルダ]¥遮断通信¥2015年07月01日_月次遮断通信.docx

となります。

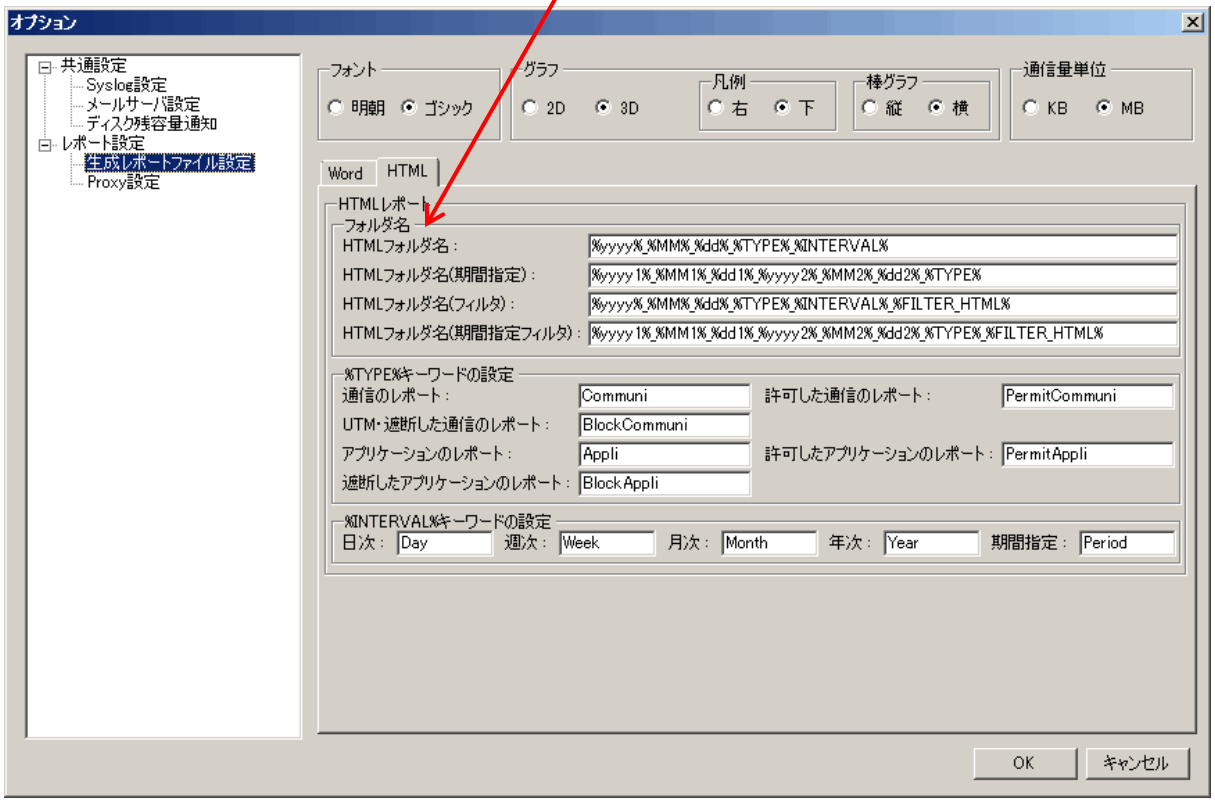
2 - 3 HTMLレポートの保存先とファイル名

HITACHI
Inspire the Next

HTMLレポートの、保存先フォルダ名とファイルは、

[HTMLレポート保存先フォルダ] ¥ フォルダ名 ¥ index.html

となります。



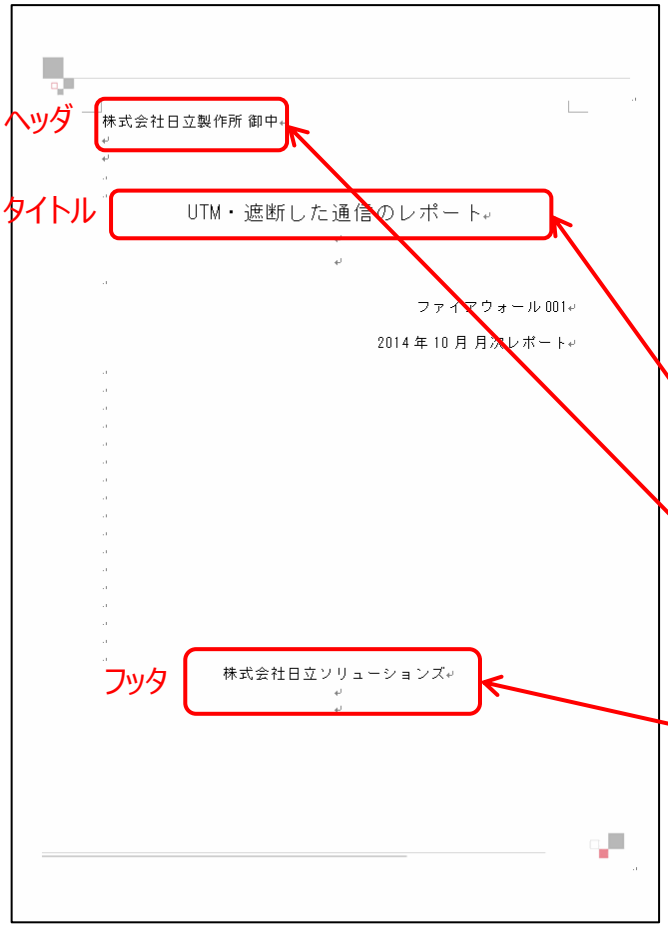
上の設定では、2015年7月の「UTM・遮断した通信のレポート」は、

[HTMLレポート保存先フォルダ]¥2015_07_01_BlockCommuni_Month¥index.html

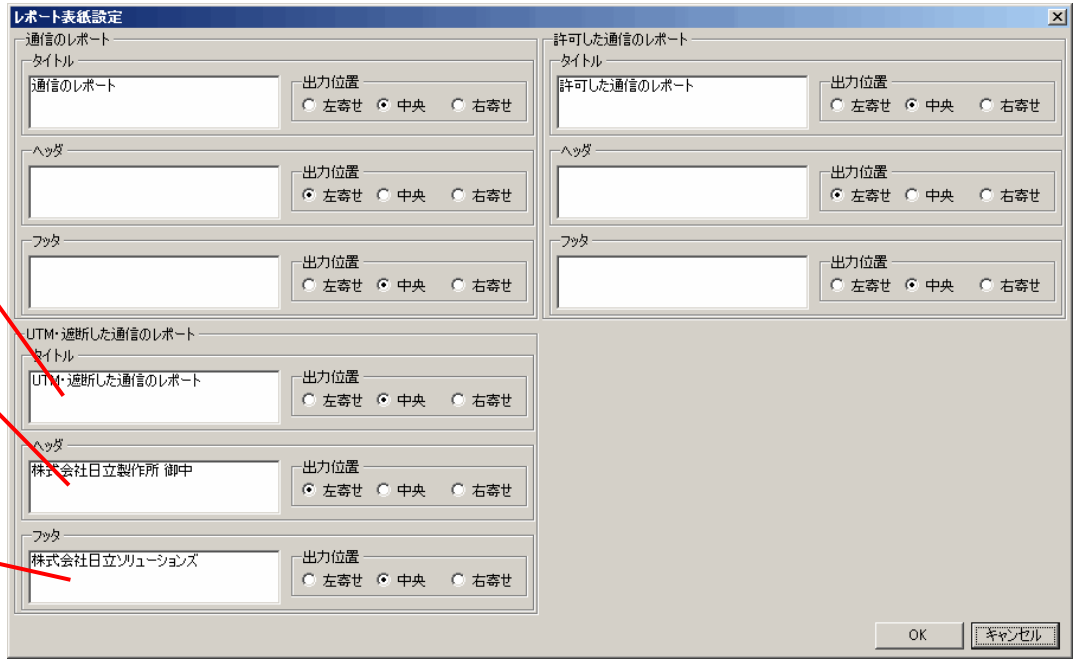
から参照します。

3 - 1 表紙の「タイトル」「ヘッダ」「フッタ」表記

レポート表紙の「タイトル」「ヘッダ」「フッタ」部分の表記を、設定できます。
プロファイルダイアログの、[レポートの設定]-[基本設定]-[レポート表紙設定]で、設定します。



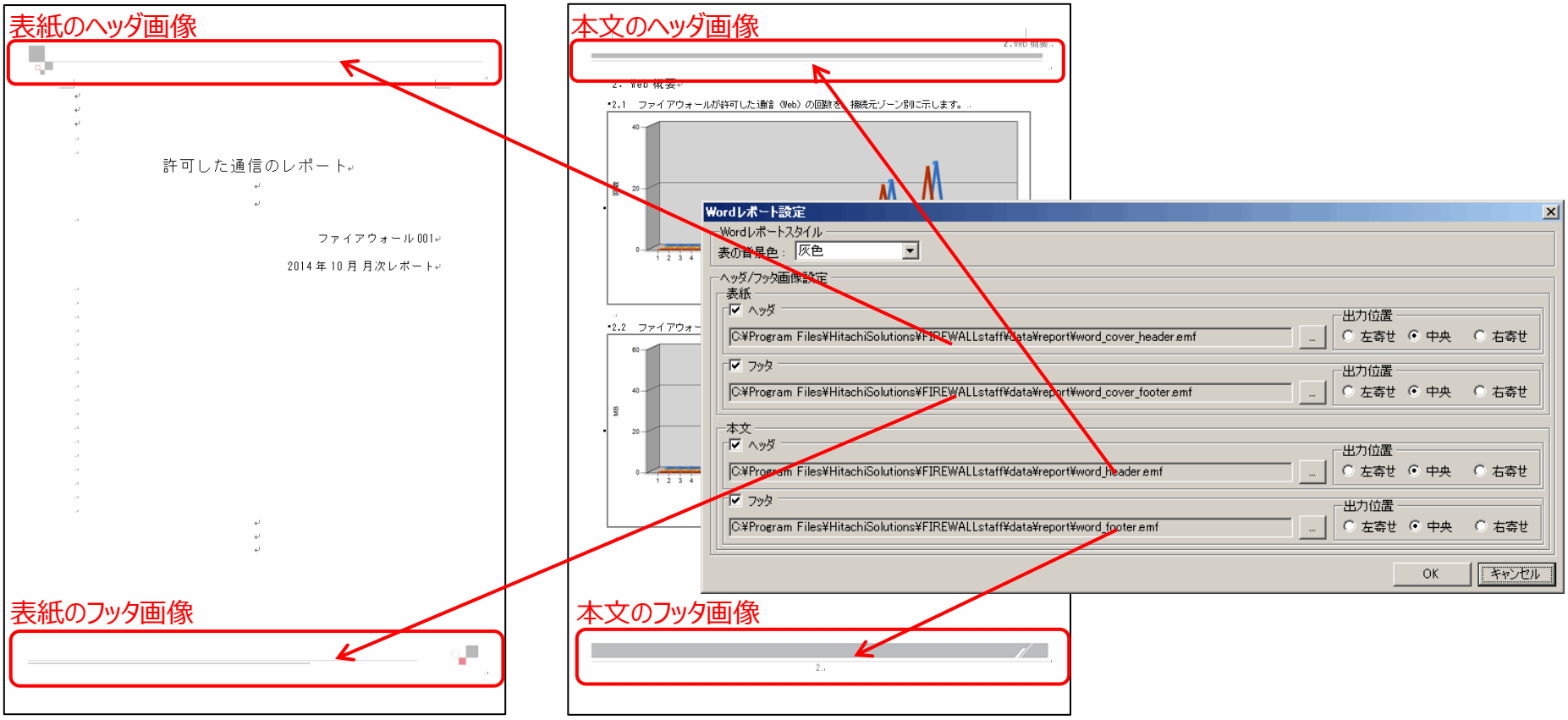
「UTM・遮断した通信のレポート」表紙



3 - 2 「ヘッダ」「フッタ」画像

レポートの「ヘッダ」「フッタ」部分の画像を、設定できます。
プロファイルダイアログの、[レポートの設定]-[基本設定]-[Wordレポート設定]で、設定します。

お客様が作成した画像を使用することもできます。詳細は、
　　『取扱説明書（基本機能編）』 3.1.3 [Wordレポート設定]パネル
を参照してください。



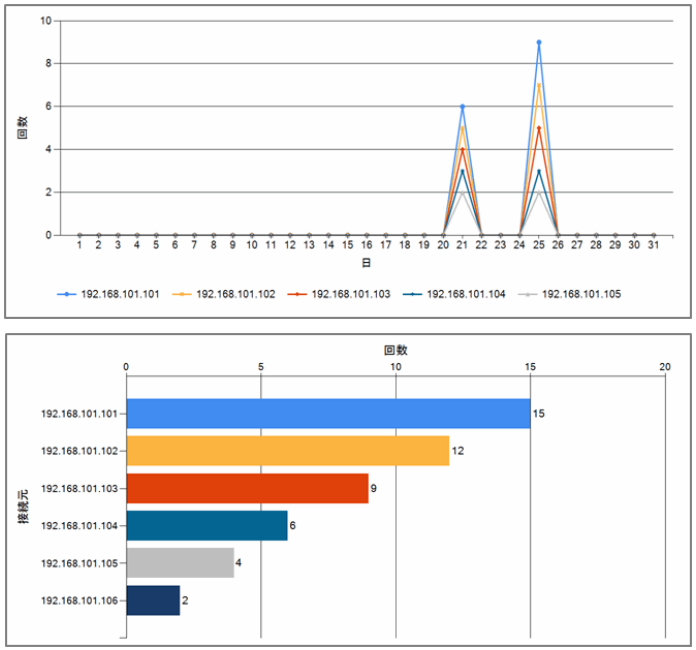
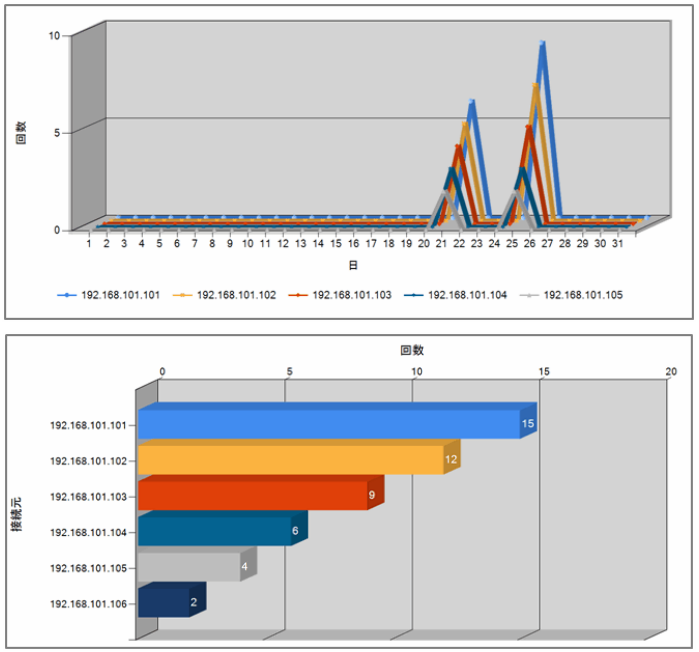
表紙　　**本文**

3-3 本文のデザイン・内容

（１）レポート本文のフォントの設定
レポート本文のフォントを、「明朝」「ゴシック」から選択できます。
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[生成レポートファイル設定]の「フォント」で指定します。

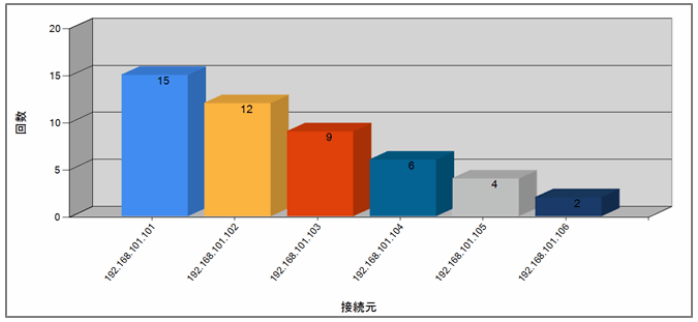
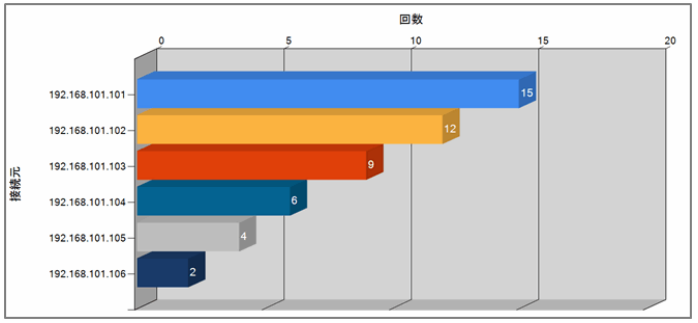
明朝	ゴシック **デフォルト**
ファイアウォールが遮断した外部からの通信のうち、回数の多い接続元を示します。	**ファイアウォールが遮断した外部からの通信のうち、回数の多い接続元を示します。**

（２）グラフの、２D・３D
グラフを、2Dと3Dから選択できます。
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[生成レポートファイル設定]の「グラフ」で指定します。

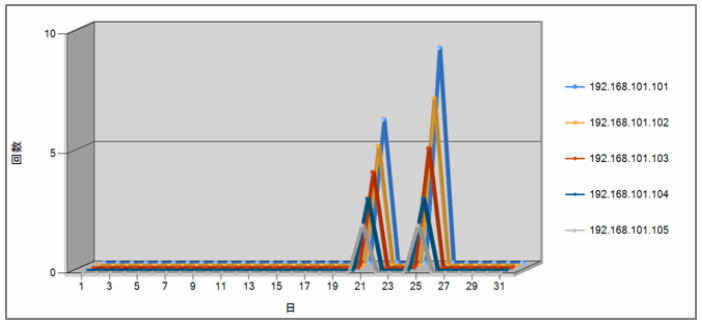
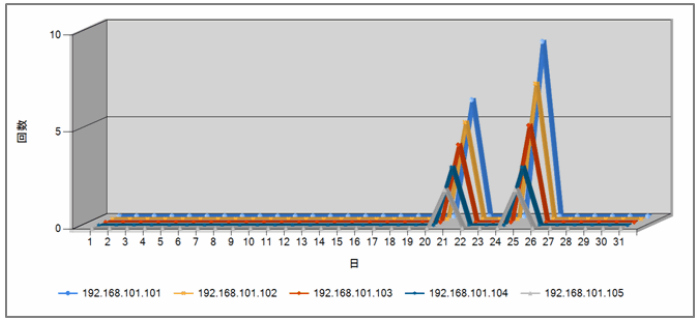
２D	3D **デフォルト**
	

3 - 3 本文のデザイン・内容

（３）棒グラフ
棒グラフを、「縦棒グラフ」「横棒グラフ」から選択できます。
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[生成レポートファイル設定]の「グラフ」で指定します。

縦棒グラフ	横棒グラフ デフォルト
	

（４）折れ線グラフの凡例の位置
折れ線グラフの凡例の位置を、「右」「下」から選択できます。
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[生成レポートファイル設定]の「グラフ」で指定します。

右	下 デフォルト
	

3-3 本文のデザイン・内容

（５）名前解決
ログに記録されているIPアドレスを、名前解決してレポートすることができます。
プロファイルダイアログの、[レポートの設定]-[基本設定]-[名前解決の設定]で指定します。

名前解決しない **デフォルト**

#	接続元	回数	通信量(MB)
1	133.108.231.21	10	10
2	133.108.231.22	8	8
3	133.108.231.23	7	7
4	133.108.231.24	5	5
5	133.108.231.25	2	2
合計		32	32

名前解決する

#	接続元	回数	通信量(MB)
1	kam021.kam.hitachi-sk.co.jp	10	10
2	kam022.kam.hitachi-sk.co.jp	8	8
3	kam023.kam.hitachi-sk.co.jp	7	7
4	kam024.kam.hitachi-sk.co.jp	5	5
5	kam025.kam.hitachi-sk.co.jp	2	2
合計		32	32

（６）「通信量」の単位
通信量の単位を、「KB」「MB」から選択できます。なお、 1MB＝1024KB＝1048576Bです。
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[生成レポートファイル設定]の「通信量単位」で指定します。

KB

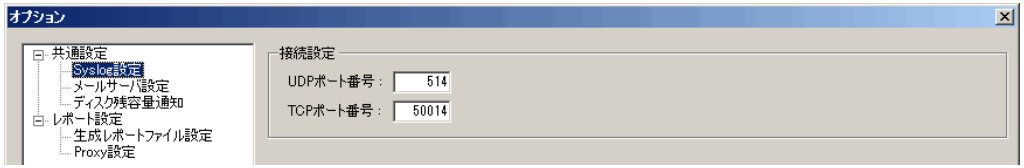
#	接続元	回数	通信量(KB)
1	133.108.231.21	10	10240
2	133.108.231.22	8	8192
3	133.108.231.23	7	7168
4	133.108.231.24	5	5120
5	133.108.231.25	2	2048
合計		32	32768

MB **デフォルト**

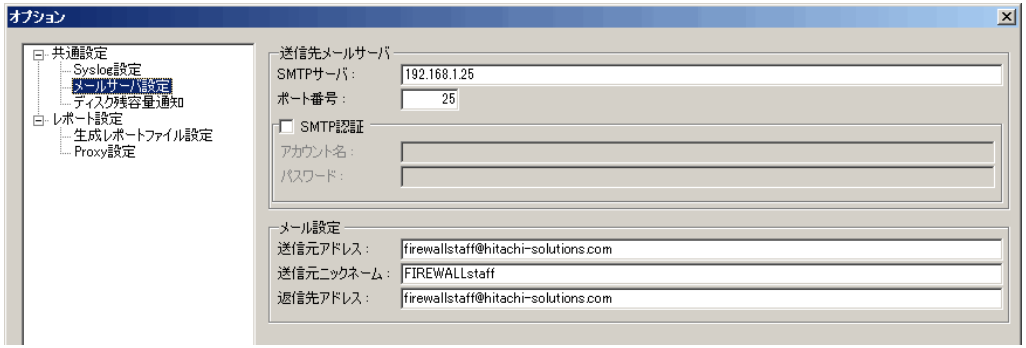
#	接続元	回数	通信量(MB)
1	133.108.231.21	10	10
2	133.108.231.22	8	8
3	133.108.231.23	7	7
4	133.108.231.24	5	5
5	133.108.231.25	2	2
合計		32	32

3 - 4 環境の設定

（１）Syslogサーバ ポート番号の設定
Syslogサーバのポート番号を指定することができます。
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[Syslog設定]で指定します。



（２）メールサーバの指定
FIREWALLstaffでメールを送信する場合は、メールサーバを指定する必要があります。
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[メールサーバ設定]で指定します。



（３）ディスク残容量通知
『データフォルダ』のドライブのディスク残容量が少なくなった場合に、メールで通知することができます。1日に1回、0時にチェックを行います。
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[ディスク残容量通知]で指定します。

4-1 ネットワークドライブのログを解析する

ネットワークドライブに存在しているログを解析する場合は、下記の手順で設定を行ってください。

（1）FIREWALLstaff関連の画面を開いている場合はすべて閉じた後、データフォルダにあるuser_data.xmlファイルの内容を、次のように変更してください。

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

<isNetworkDriveEnable>false</isNetworkDriveEnable>

↓

<isNetworkDriveEnable>true</isNetworkDriveEnable>

（2）接続先で、ネットワークの共有設定を行ってください。また、指定したユーザ名とパスワードでアクセスできるように設定してください。

（3）接続元となるOS上（FIREWALLstaffをインストールしたOS上）で以下の設定を行ってください。

・接続先にアクセスするユーザを、OS上に追加してください

→ユーザ名とパスワードは（2）で設定した、接続先にアクセス可能なものとします。

・OS上に追加したユーザを、管理者にしてください

→Administratorsグループに含めてください。

（4）[コントロールパネル]->[管理ツール]->[サービス]で、FIREWALLstaffのサービス

・FIREWALLstaff Log
・FIREWALLstaff Monitor
・FIREWALLstaff Scheduler

に対して、次を行ってください。

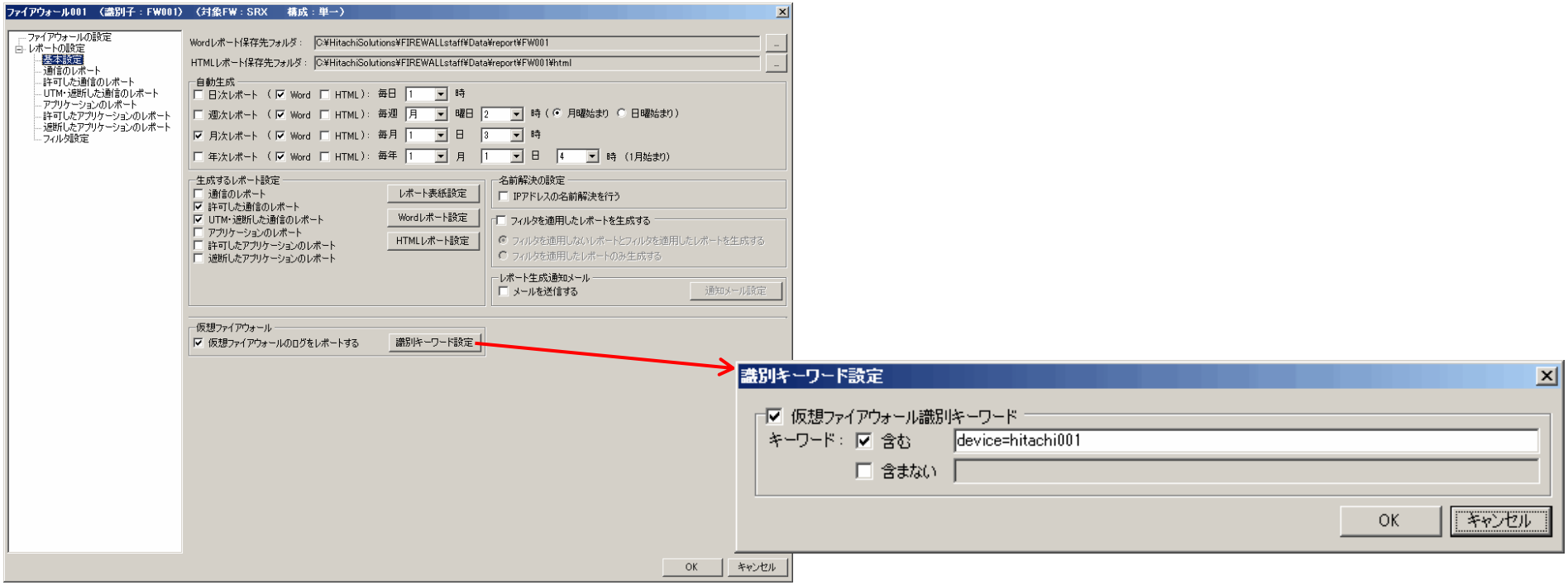
・サービスを停止します
・[プロパティ]-[ログオン]タブで、[アカウント]ラジオボタンを選択して、（2）で設定したユーザ名とパスワードを指定します
・サービスを起動します

（5）『1-5 ログの取り込み方法 (2)ローカルドライブのログを使用』を参考に、設定を行ってください。
そして、[取得先フォルダ名]にネットワークドライブを指定してください。その際、必ず
UNCパス（例：「¥¥server¥share」）形式で指定
してください。

【注意事項】 ネットワークの切断・遮断などによっていかなる不具合が発生しても、サポート対象外となります。

4-2 仮想ファイアウォールのログを解析する

仮想ファイアウォールのログのように、1ログファイルに複数台のファイアウォールのレコードが混在しているログファイルを、解析対象とすることができます。
プロファイルダイアログの、[レポートの設定]-[基本設定]-[仮想ファイアウォール]で、設定します。



【例１】
上記のように、
　device=hitachi001
を指定すると、右図の [ ] のレコードのみが解析対象となります。

```
time="2014-10-21 17:01:00" device=hitachi002 src=xxx dst=xxx .....
time="2014-10-21 17:02:00" device=hitachi001 src=xxx dst=xxx .....
time="2014-10-21 17:03:00" device=hitachi003 src=xxx dst=xxx .....
time="2014-10-21 17:04:00" device=hitachi001 src=xxx dst=xxx .....
time="2014-10-21 17:05:00" device=hitachi002 src=xxx dst=xxx .....
time="2014-10-21 17:06:00" device=hitachi001 src=xxx dst=xxx .....
time="2014-10-21 17:07:00" device=hitachi003 src=xxx dst=xxx .....
```

4-2 仮想ファイアウォールのログを解析する

【例２】仮想ファイアウォールのログを解析する際の、具体的な設定

FIREWALLstaffの設定

プロファイル001 「仮想ファイアウォールA」のログを解析し、レポートを作成	・[ログの取得方法]として、「FIREWALLstaff Logサービスによる取得」を指定 →Syslogは「プロファイル001」で受信 ・[識別キーワード設定]で、「仮想ファイアウォールA」のレコードを特定できるキーワードを指定
プロファイル002 「仮想ファイアウォールB」のログを解析し、レポートを作成	・[ログの取得方法]として、「ローカルドライブのログを使用」を指定し、「プロファイル001」が取得したログのパスを指定 ・[識別キーワード設定]で、「仮想ファイアウォールB」のレコードを特定できるキーワードを指定
プロファイル003 「仮想ファイアウォールC」のログを解析し、レポートを作成	・[ログの取得方法]として、「ローカルドライブのログを使用」を指定し、「プロファイル001」が取得したログのパスを指定 ・[識別キーワード設定]で、「仮想ファイアウォールC」のレコードを特定できるキーワードを指定

【注意事項】 ログを解析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。

4-3 解析結果レポートを出力する

「UTM・遮断した通信のレポート」において、解析結果レポートを出力する場合は、下記の手順で設定を行ってください。

（１）FIREWALLstaff関連の画面を開いている場合はすべて閉じた後、データフォルダにあるuser_data.xmlファイルの内容を、次のように変更してください。

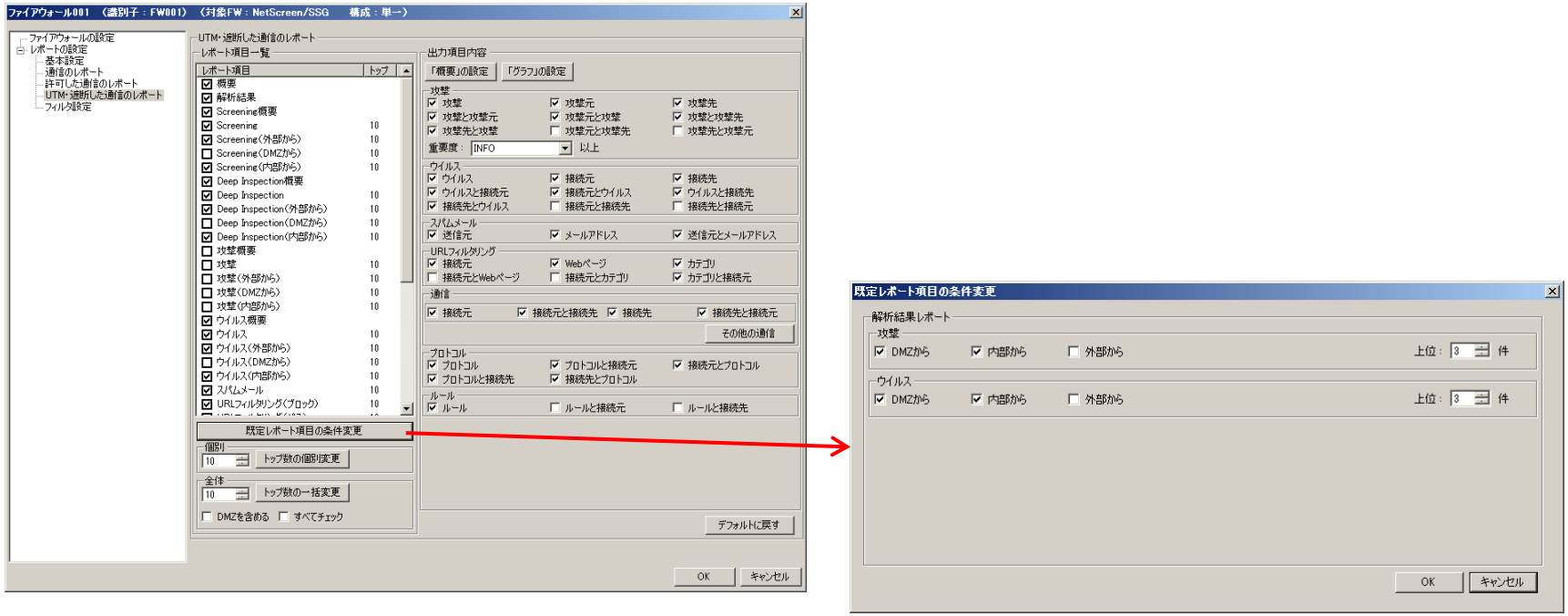
例）C:¥HitachiSolutions¥FIREWALLstaff¥Data¥user¥user_data.xml

<isExtAnalyze>false</isExtAnalyze>

↓

<isExtAnalyze>true</isExtAnalyze>

（２）解析結果レポートに関する設定は、プロファイルダイアログの、[レポートの設定]-[UTM・遮断した通信のレポート]-[既定レポート項目の条件変更]で、変更できます。



お問合わせ

本手引きについてのお問い合わせは、電子メールで
　　firewallstaff@hitachi-solutions.com
宛にお願いします。

体験版は、
　　https://www.hitachi-solutions.co.jp/firewallstaff/
からダウンロードできます。

HITACHI
Inspire the Next

END

ファイアウォールのログ収集と、レポート作成
FIREWALLstaff体験版の手引き

株式会社 日立ソリューションズ