



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

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。

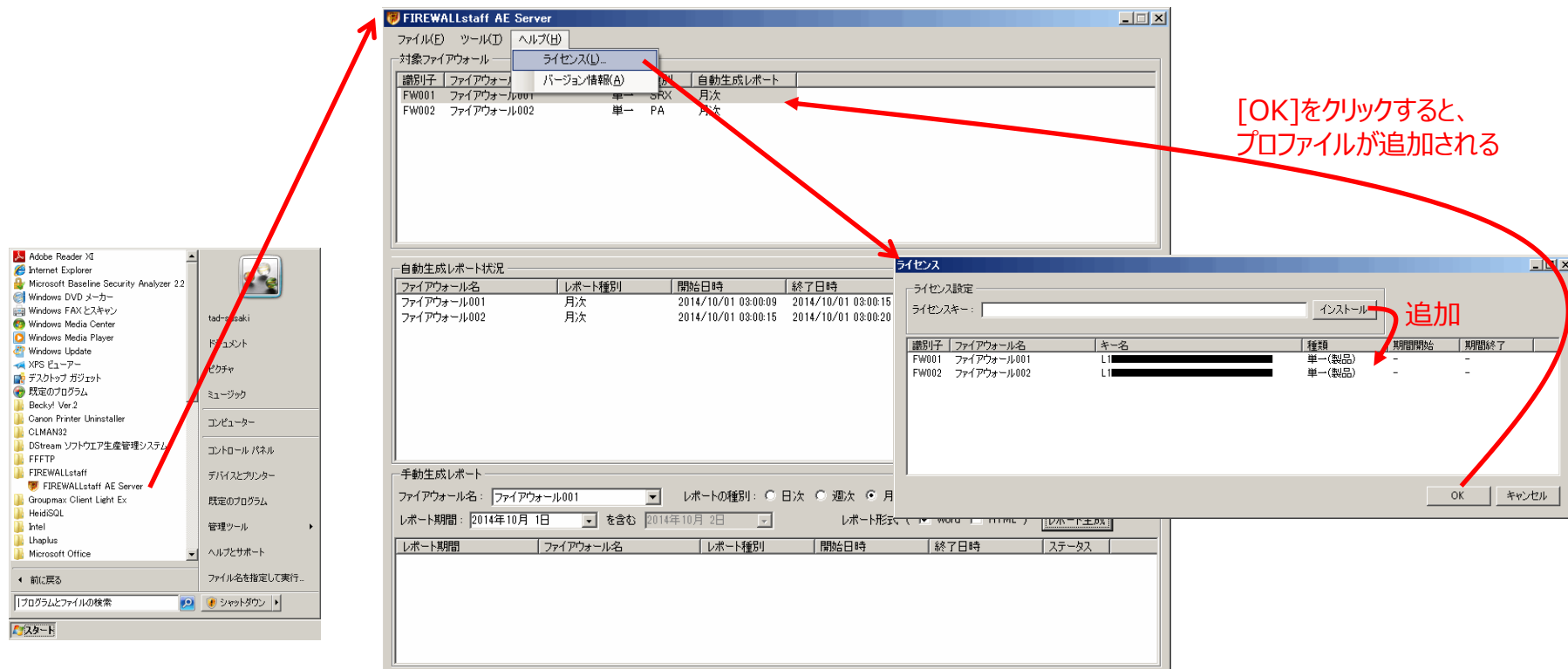
1 - 2 ライセンスキーのインストール

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）ポリシー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。

プロファイルをダブルクリック

The screenshot shows the FIREWALLstaff AE Server main window. The '対象ファイアウォール' (Target Firewall) table is visible, listing two profiles: 'ファイアウォール001' (FW001) and 'ファイアウォール002' (FW002). A red arrow points from the 'ファイアウォール001' entry to the 'ファイアウォール001' (識別子: FW001) (対象FW: SRX 構成: 単一) dialog box. The dialog box contains various settings for the firewall profile, including log acquisition method, host name, IP addresses, and log storage options.

ファイアウォール001 (識別子: FW001) (対象FW: SRX 構成: 単一)

名称: ファイアウォール001

ログの取得方法
☒ FIREWALLstaff Logサービスによる取得 (☒ UDP ☐ TCP) ☐ FTPによる取得 ☐ ローカルドライブのログを使用

接続ホスト名: ログインID/パスワード設定

取得先フォルダ名:

読み込みファイル設定:

ファイアウォール1
IPアドレス: Syslog送信元IPアドレス:

ファイアウォール2
IPアドレス: Syslog送信元IPアドレス:

IPアドレス
内部ネットワーク
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

DMZネットワーク
表示名:

外部ネットワーク
表示名: 外部

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
☒ デフォルトを使用 ☐ 個別指定 フォルダ名:

取得したログに対する操作
☐ 圧縮する 対象外とする日数: 日
☐ 削除する 対象外とする日数: 日

中間ファイルに対する操作
☐ 削除する 対象外とする日数: 日

ライセンス形態の変更/更新

OK キャンセル

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

The screenshot shows the 'ファイアウォール001' (Firewall 001) configuration window. The 'ログの取得方法' (Log Acquisition Method) section has three radio buttons: 'FIREWALLstaff Logサービスによる取得' (selected), 'FTPによる取得' (selected), and 'ローカルドライブのログを使用' (selected). The 'Syslog送信元IPアドレス' (Syslog Source IP Address) is set to '192.168.1.1'. The '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' (Log Storage Location/Intermediate File Storage Location) is set to 'C:\Hitachi\Solutions\FIREWALLstaff\Data\Firewall\Syslog\FW001'. The '取得したログに対する操作' (Operation for Acquired Logs) and '中間ファイルに対する操作' (Operation for Intermediate Files) sections are also visible.

「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

ファイアウォール001 (識別子: FW001) (対象FW: SRX 構成: 単一)

ファイアウォールの設定

レポートの設定

基本設定

通信のレポート

許可した通信のレポート

UTM・逆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

逆断したアプリケーションのレポート

フィルタ設定

名称: ファイアウォール001

ログの取得方法

☐ FIREWALLstaff Logサービスによる取得 (UDP TOP) ☐ FTPによる取得 ☒ ローカルドライブのログを使用

接続ホスト名:

取得先フォルダ名: c:\FirewallLog

読み込みファイル設定: *.log

ファイアウォール1

IPアドレス: 192.168.1.1 Syslog送信元IPアドレス: 192.168.1.1

ファイアウォール2

IPアドレス: Syslog送信元IPアドレス:

IPアドレス

内部ネットワーク

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

DMZネットワーク

外部ネットワーク

表示名: 外部

表示名: 内部

表示名: DMZ

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

☒ デフォルトを使用 ☐ 個別指定 フォルダ名: C:\Hitachi\Solutions\FIREWALLstaff\Data\Firewall\Syslog\FW001

取得したログに対する操作

☐ 圧縮する 対象外とする日数: 70 日

☐ 削除する 対象外とする日数: 70 日

中間ファイルに対する操作

☐ 削除する 対象外とする日数: 70 日

ライセンス形態の変更/更新

OK キャンセル

「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。

The screenshot shows the 'FIREWALL001 (識別子: FW001) (対象FW: SRX 構成: 単一)' configuration window. The left sidebar lists various settings, with 'ファイアウォールの設定' expanded. The main area shows configuration for 'ファイアウォール1' and 'ファイアウォール2'. A red box highlights the 'IPアドレス' section, which includes three lists: '内部ネットワーク' (Internal Network) containing '10.0.0.0/8', '172.16.0.0/12', and '192.168.0.0/16'; 'DMZネットワーク' (DMZ Network); and '外部ネットワーク' (External Network) with '表示名: 外部'. Below these lists are fields for '表示名' (Display Name) set to '内部' and 'DMZ'. The bottom of the window contains options for log storage and file operations, and a 'ライセンス形態の変更/更新' button.

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。

The screenshot shows the 'FIREWALLstaff AE Server' window. It has three main sections: '対象ファイアウォール' (Target Firewall), '自動生成レポート状況' (Automatic Report Generation Status), and '手動生成レポート' (Manual Report Generation). A red arrow points from the 'FW001' entry in the first table to the 'FW001' part of the file path in the text below.

識別子	ファイアウォール名	構成	種別	自動生成レポート
FW001	ファイアウォール001	単一	SRX	月次

ファイアウォール名	レポート種別	開始日時	終了日時	ステータス	次回実施日時
ファイアウォール001	月次			実行待ち	2015/08/01 03:00:00

手動生成レポート

ファイアウォール名: レポートの種別: ☐ 日次 ☐ 週次 ☒ 月次 ☐ 年次 ☐ 期間指定

レポート期間: を含む レポート形式 (☒ Word ☐ HTML)

レポート期間	ファイアウォール名	レポート種別	開始日時	終了日時	ステータス
2015/07/01 - 2015/07/31	ファイアウォール001	月次	2015/07/08 13:02:01	2015/07/08 13:02:14	終了

[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

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

レポートを作成したプロファイルの「識別子」

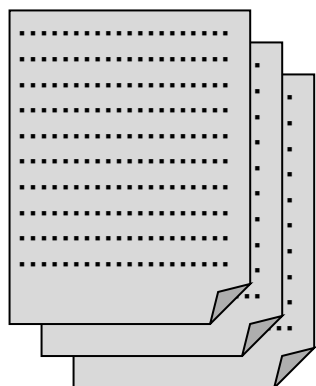
配下に、フォルダとファイルが生成されておりますので、内容を確認してください。

【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。

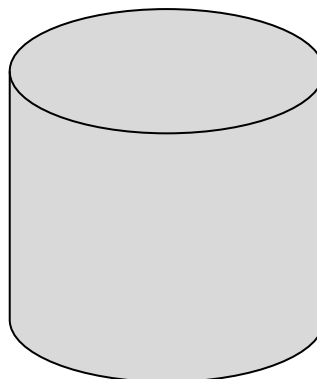
1 - 8 中間ファイル

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。



ファイアウォールのログ



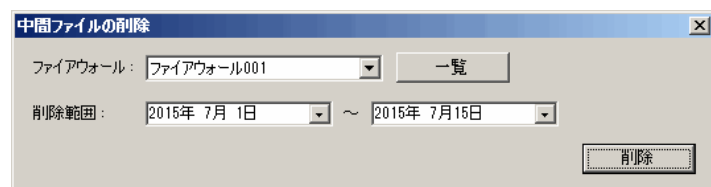
中間ファイル



レポート

『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、**必要な場合のみ指定してください**

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

HITACHI
Inspire the Next

となります。

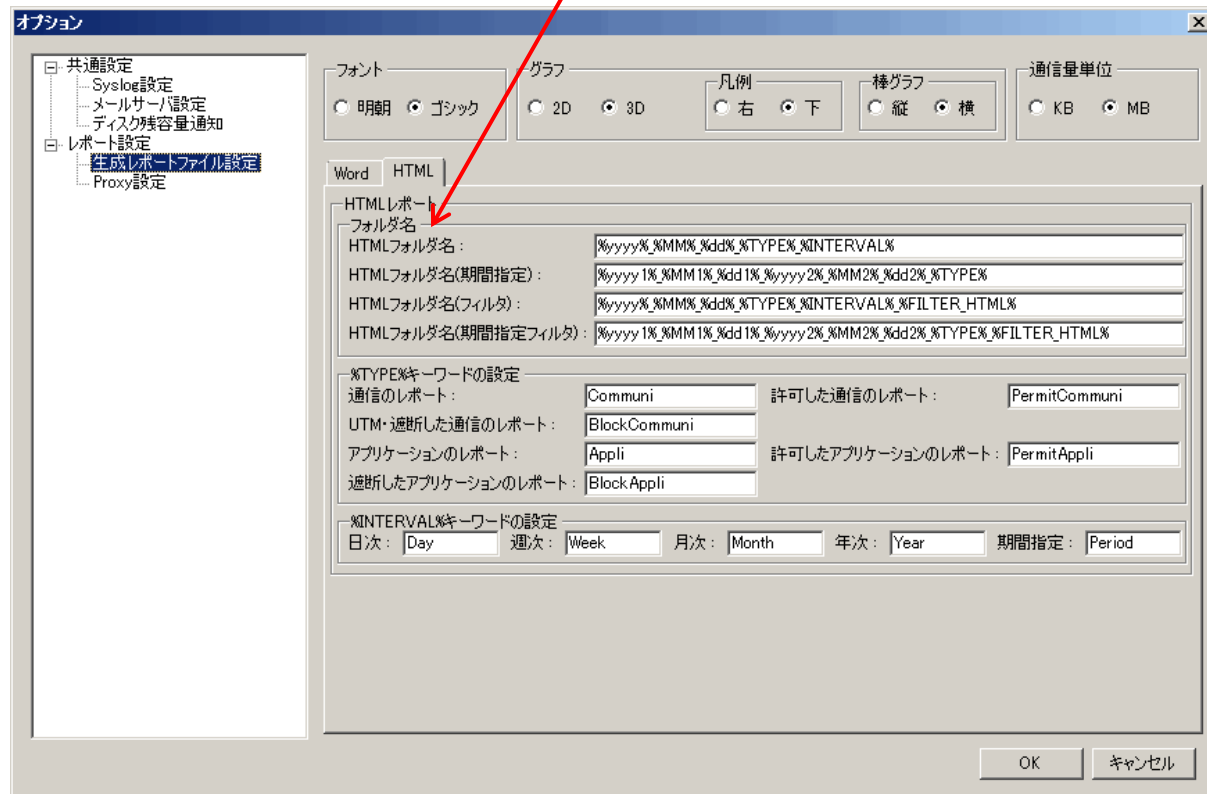
となります。

2 - 3 HTMLレポートの保存先とファイル名

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。



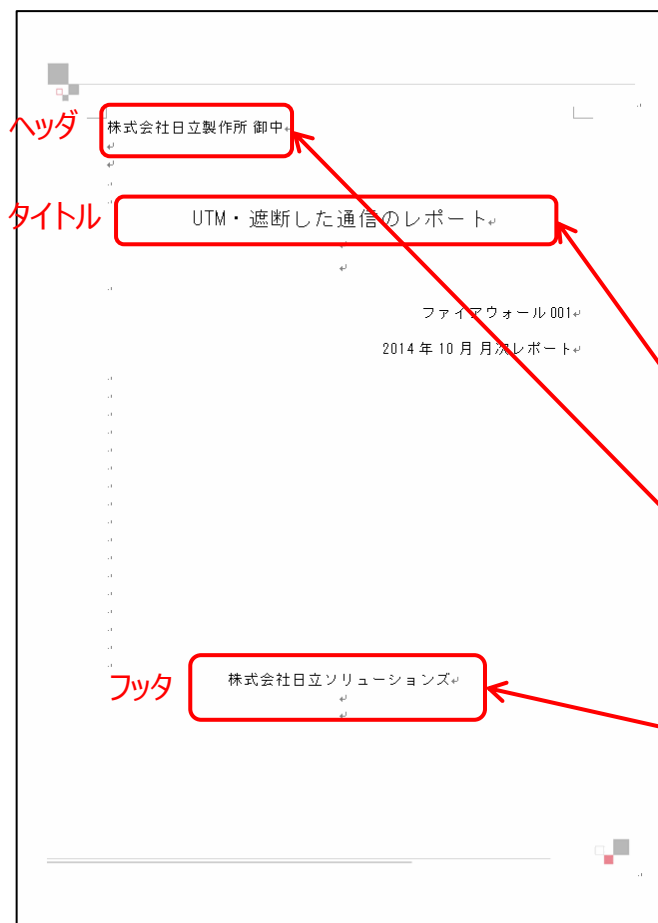
上の設定では、2015年7月の「UTM・遮断した通信のレポート」は、

[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。

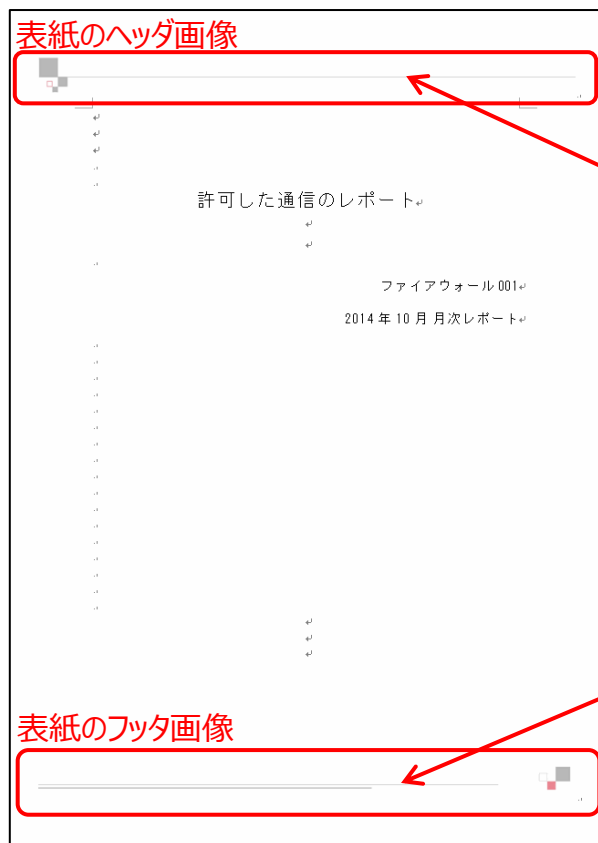


「UTM・遮断した通信のレポート」表紙

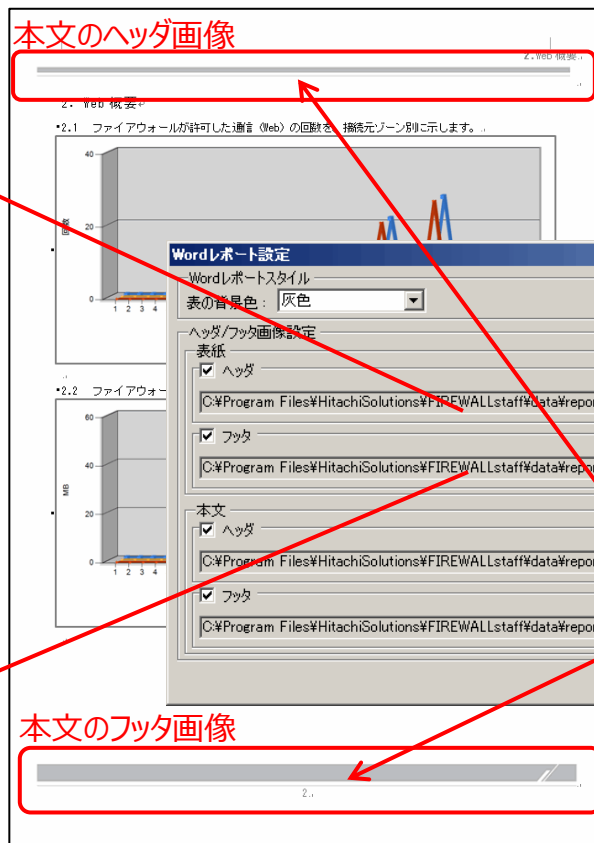
3-2 「ヘッダ」「フッタ」画像

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。

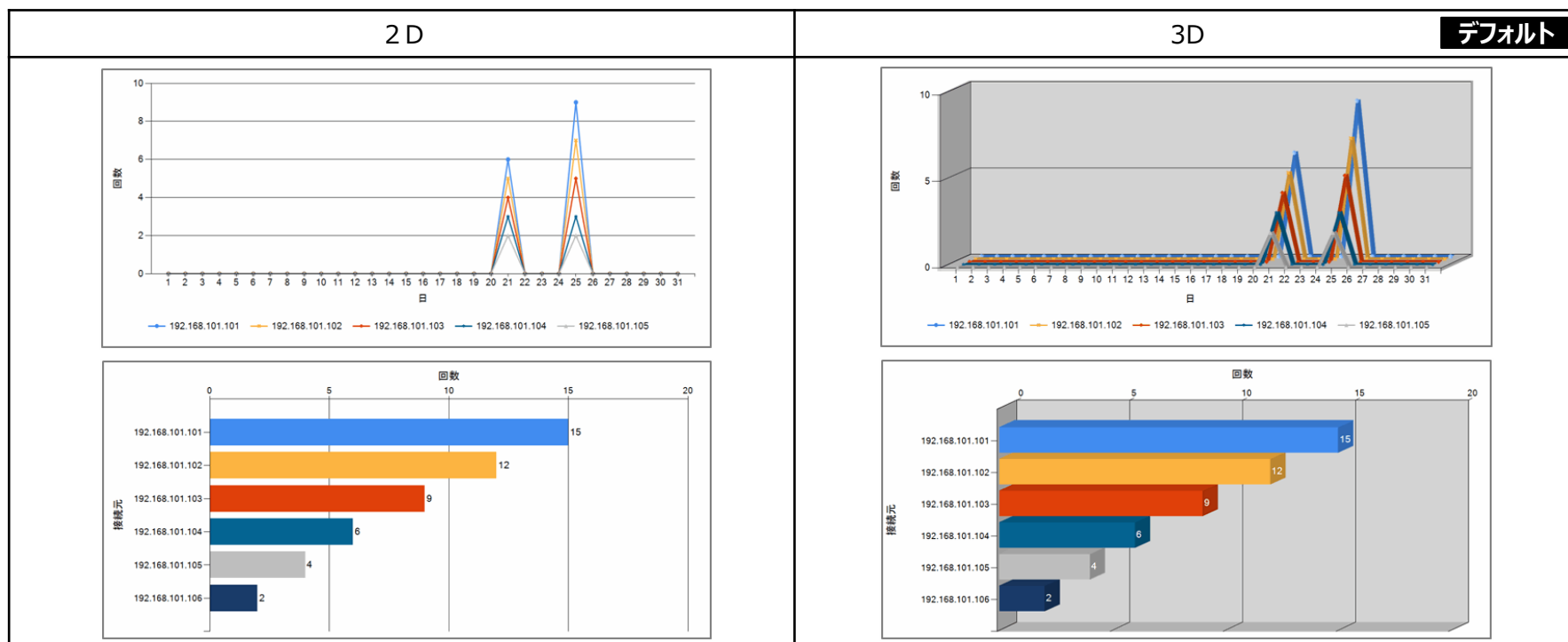
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[生成レポートファイル設定]の「フォント」で指定します。

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。

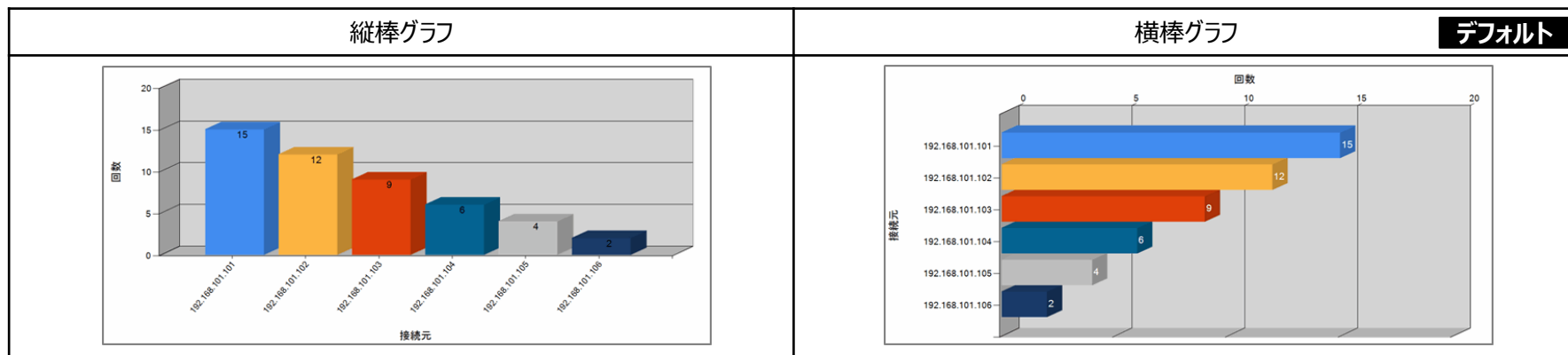


3-3 本文のデザイン・内容

(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。

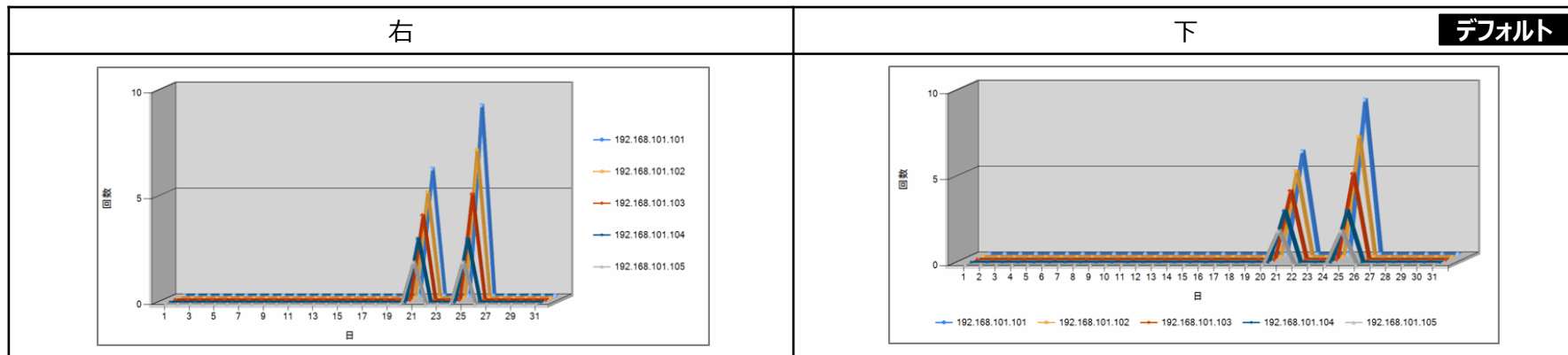
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[生成レポートファイル設定]の「グラフ」で指定します。



(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。



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	名前解決する			
#	接続元	回数	通信量(MB)		#	接続元	回数	通信量(MB)
1	133.108.231.21	10	10		1	kam021.kam.hitachi-sk.co.jp	10	10
2	133.108.231.22	8	8		2	kam022.kam.hitachi-sk.co.jp	8	8
3	133.108.231.23	7	7		3	kam023.kam.hitachi-sk.co.jp	7	7
4	133.108.231.24	5	5		4	kam024.kam.hitachi-sk.co.jp	5	5
5	133.108.231.25	2	2		5	kam025.kam.hitachi-sk.co.jp	2	2
合計		32	32		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

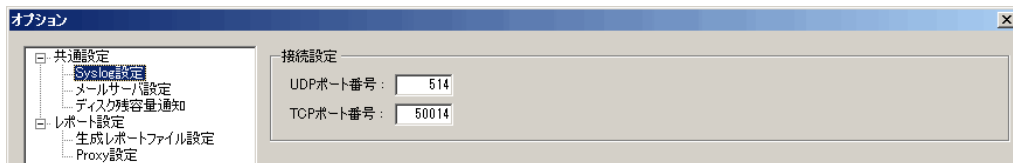
MB			デフォルト
#	接続元	回数	通信量(MB)
1	133.108.231.21	10	10
2	133.108.231.22	8	8
3	133.108.231.23	7	7
4	133.108.231.24	5	5
5	133.108.231.25	2	2
合計		32	32

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。

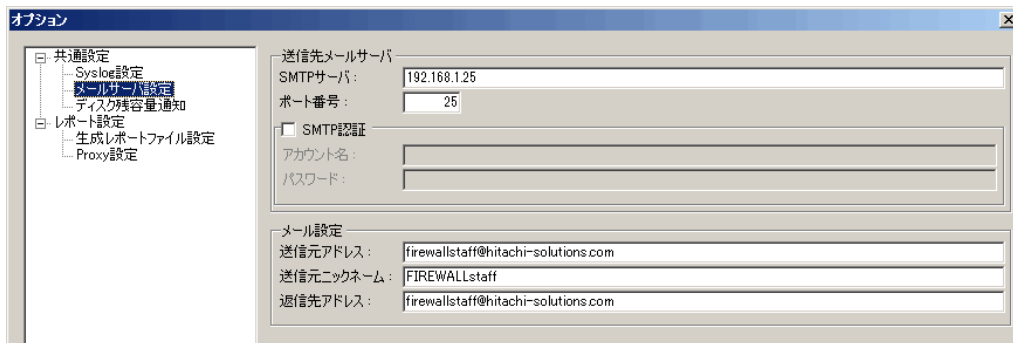
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[Syslog設定]で指定します。



(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。

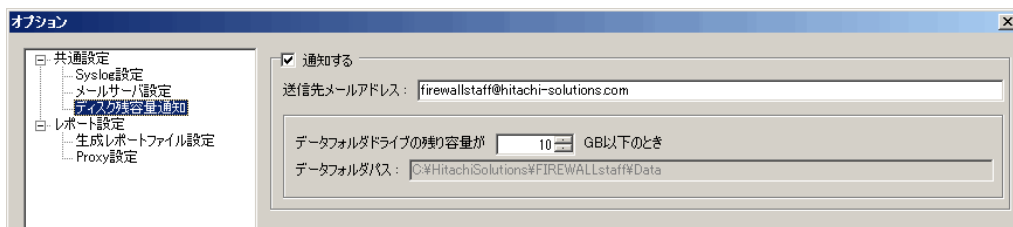
FIREWALLstaff AE Serverメイン画面の、[ツール]-[オプション]-[メールサーバ設定]で指定します。



(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

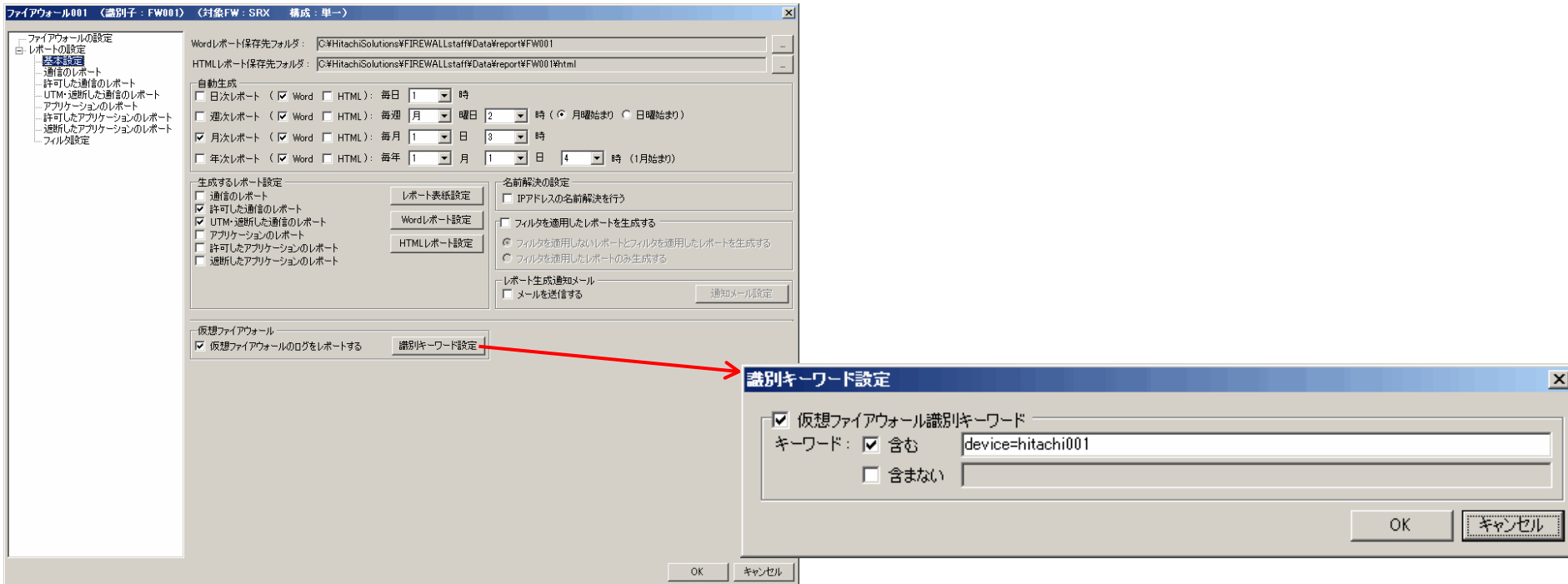
- (5) 『1-5 ログの取り込み方法 (2)ローカルドライブのログを使用』を参考に、設定を行ってください。

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。

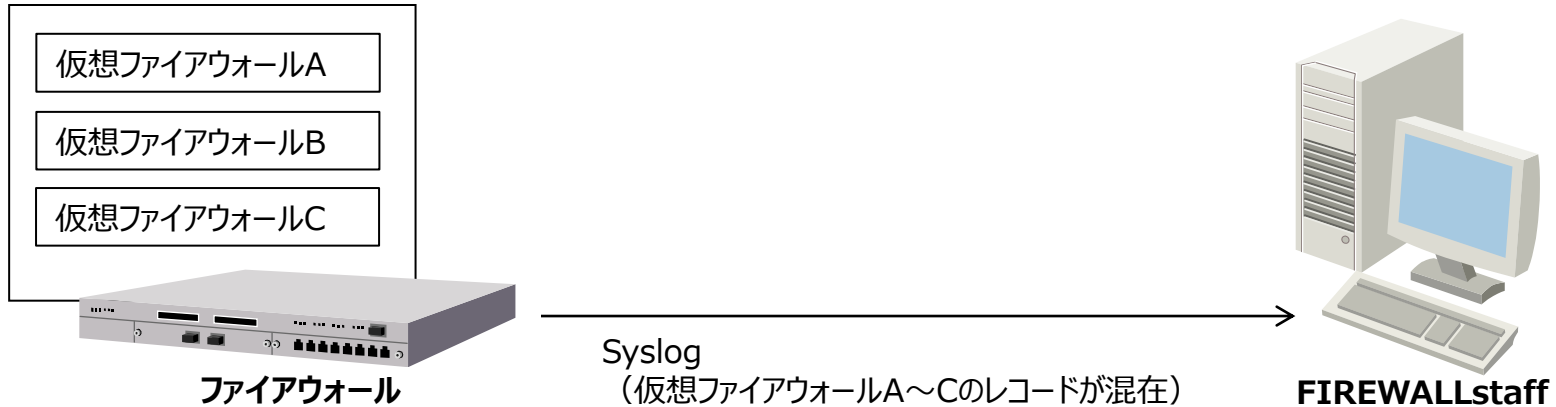


【例1】
上記のように、
device=hitachi001
を指定すると、右図の device=hitachi001 のレコードのみが解析対象となります。

```
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	<ul style="list-style-type: none">・[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	<ul style="list-style-type: none">・[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	<ul style="list-style-type: none">・[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。

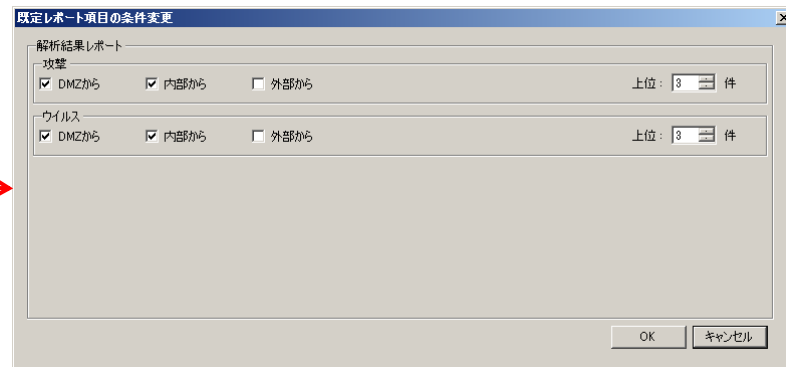
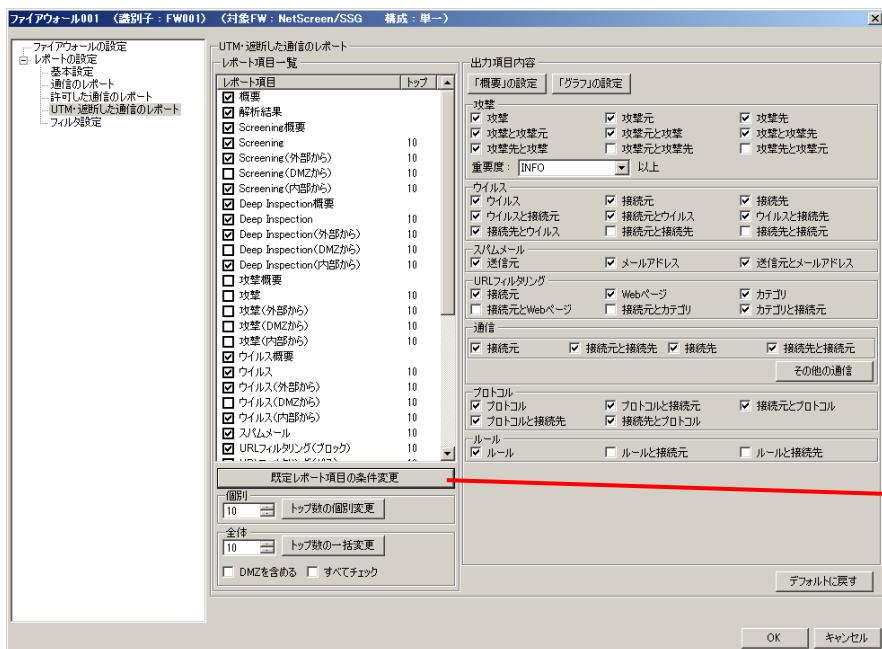
例) C:\HitachiSolutions\FIREWALLstaff\Data\user\user_data.xml

```
<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。



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。

- ※ 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。
- ※ その他記載の会社名、製品名はそれぞれの会社の商標もしくは登録商標です。

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