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 ご紹介

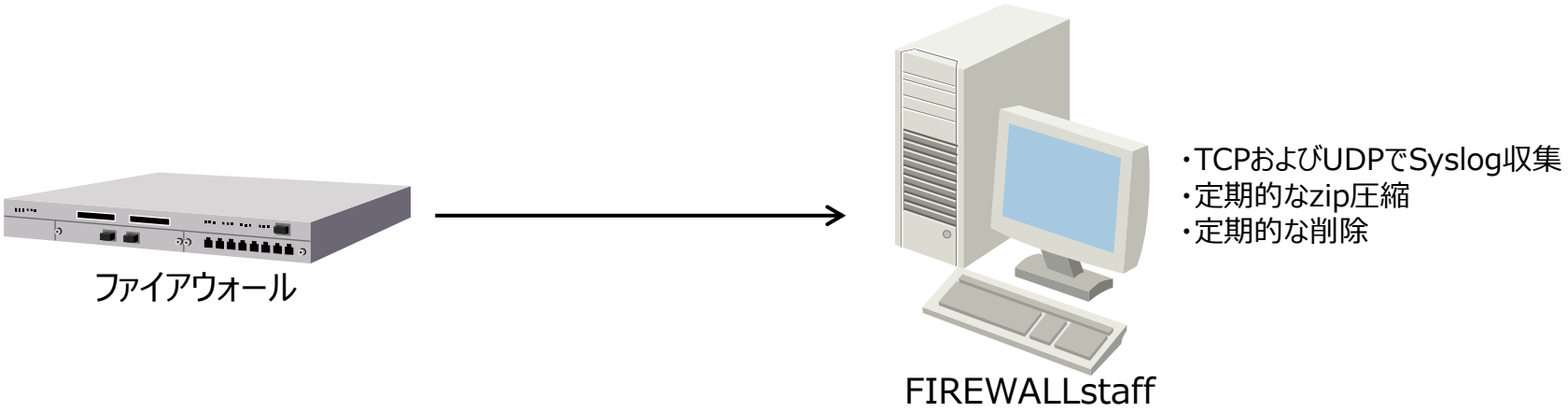
対象バージョン：02-08

株式会社 日立ソリューションズ

2022年1月版

1 - 1 ログ収集

FIREWALLstaffのSyslog収集機能を用いて、ファイアウォールから送られてくるSyslogを収集できます。



■ TCP/UDPでのSyslog収集

・UDPに加えて、TCPでもSyslogを収集できます
・TCPおよびUDPの待ち受けポート番号は、変更できます
・受信したログは、テキスト形式で、受信した日毎のファイルに分けて、保存します

■ ログの圧縮

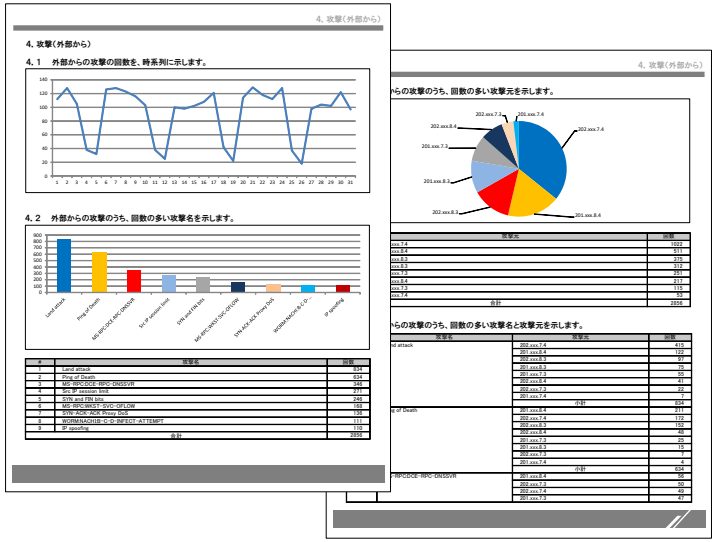
・指定した日数を経過したログを、定期的にzip圧縮します

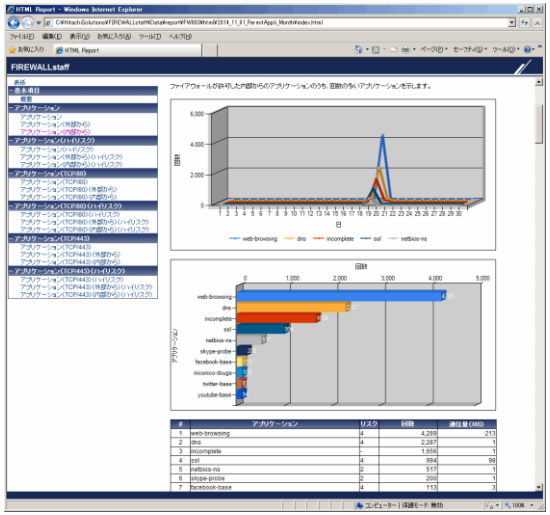
■ ログの削除

・指定した日数を経過したログを、定期的に削除します

ファイアウォールがCheckPointの場合は、FIREWALLstaffがLEAによるアクセスでログを収集します

1 - 2 レポート作成





■ 1000種類以上のレポート

・グラフ（折れ線、棒、円グラフ）と表からなる、1000種類以上のレポート
・日次、週次、月次、年次のレポートを、指定したタイミングで作成します

■ レポートのファイル形式

・Word形式およびHTML形式でレポートを作成します

■レポートの内容

・トレンドレポート、Web通信レポート、メール通信レポート、攻撃レポート、ウイルスレポート、など
・詳細は、「付録　レポートの内容」を参照してください

1 - 3 レポート作成のためのログの取り込み方法

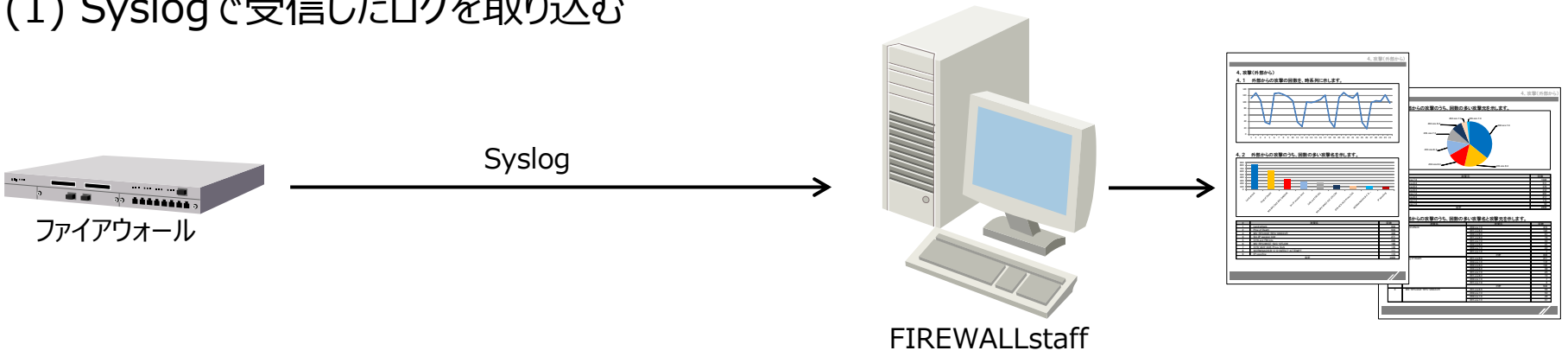
CheckPointを除く

HITACHI
Inspire the Next

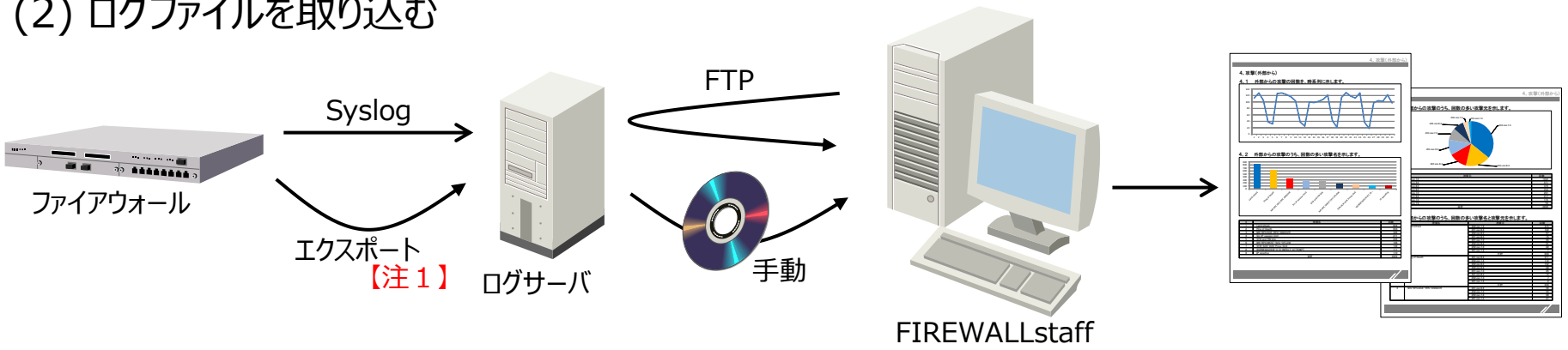
FIREWALLstaffでレポートを作成するため、ログを取り込む方法は2通りあります。
取り込むログは、テキスト形式である必要があります。

CheckPointの場合は、次ページをご覧ください

(1) Syslogで受信したログを取り込む



(2) ログファイルを取り込む



【注１】エクスポートしたログは、Syslogで送信(受信)したログと形式・内容が同一である必要があります

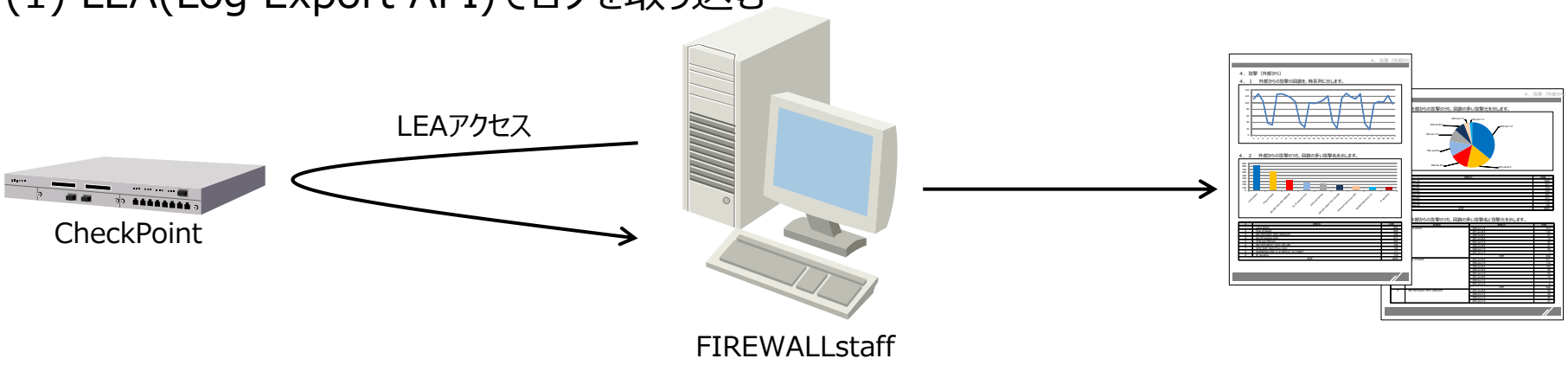
1 - 4 レポート作成のためのログの取り込み方法

CheckPointの場合

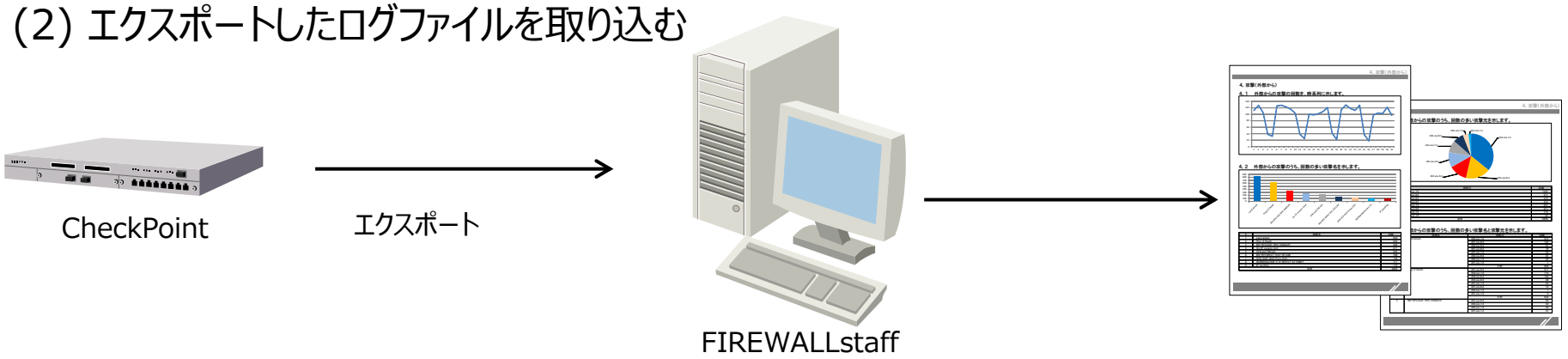
HITACHI
Inspire the Next

FIREWALLstaffでレポートを作成するため、ログを取り込む方法は2通りあります。
取り込むログは、テキスト形式である必要があります。

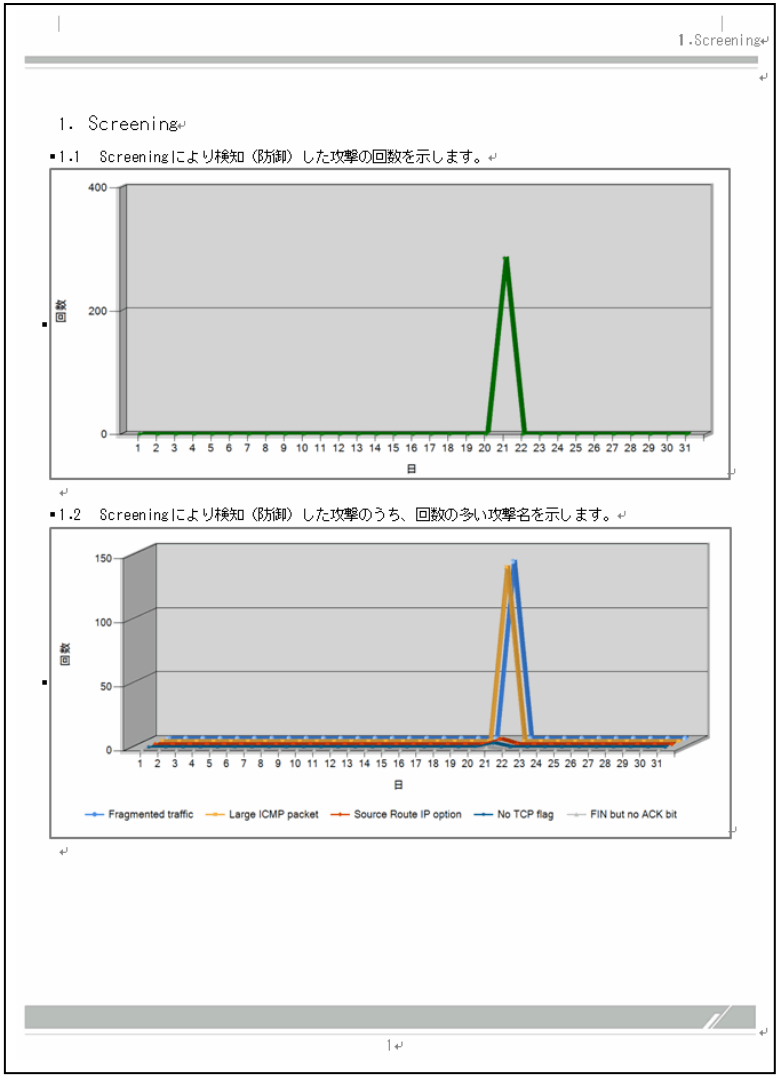
(1) LEA(Log Export API)でログを取り込む

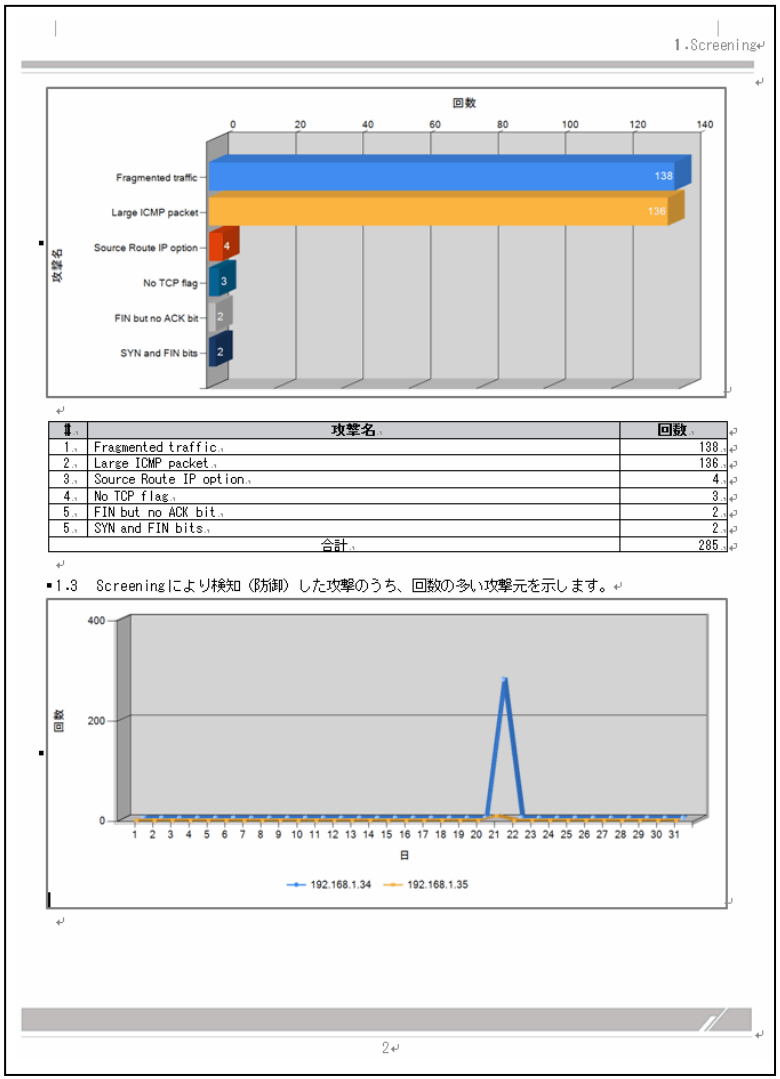


(2) エクスポートしたログファイルを取り込む



1 - 5 レポートイメージ





レポートのサンプルを、https://www.hitachi-solutions.co.jp/firewallstaff/ に公開しています。

2-1 動作環境

HITACHI
Inspire the Next

■ ハードウェア要件

カテゴリ	内容
導入機種	「ソフトウェア要件」に示すOSが動作するPC/AT互換機であること
CPU	以下のスペックを満たしていること。 インテル Core i5 2.6GHz以上
メモリ容量	2GB以上の容量を持つこと
HDD容量	NTFS形式で100GB以上の空き容量を持つこと

■ ソフトウェア要件

カテゴリ	内容
OS	以下のいずれかのOSが正しく稼動すること（カッコ内はビット数を表します）。 ・Windows Server 2012（64） ・Windows Server 2012 R2（64） ・Windows 8.1（32, 64） ・Windows 10（32, 64） ・Windows Server 2016 ・Windows Server 2019
ソフトウェア	以下のソフトウェアのいずれかが正しく稼動すること。 ・Microsoft .NET Framework 4.5.1～4.8

■ 仮想環境への対応について

VMWareおよびHyper-Vによる仮想環境に対応しています。

■ クラスタリングへの対応について

クラスタリングには対応していません。

2-2 対応ファイアウォール

HITACHI
Inspire the Next

FIREWALLstaffでレポート作成できる主なファイアウォールと、レポート対象のログは下記の通りです。

ファイアウォール	OS／ファームウェア	FIREWALLstaffがレポートできるログの種類
Juniper NetScreen/SSG シリーズ	ScreenOS 5.4 ～ ScreenOS 6.3	・トラフィックログ ・UTM機能のログ
Fortinet FortiGate シリーズ	FortiOS 4.0MR3 ～ FortiOS 6.4.6	・トラフィックログ ・UTM機能のログ ・アプリケーション制御機能のログ
Palo Alto PA シリーズ	PANOS 3.1.x ～ PANOS 9.1.x	・トラフィックログ ・UTM機能のログ ・アプリケーション制御機能のログ
Juniper SRX シリーズ	JUNOS 10.0 ～ JUNOS 20.4R3	・トラフィックログ ・UTM機能のログ ・アプリケーション制御機能のログ
CheckPoint シリーズ	R70 ～ R81	・トラフィックログ ・UTM機能のログ ・アプリケーション制御機能のログ

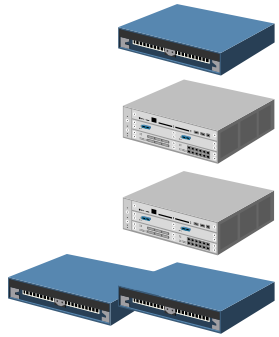
2 - 3 ライセンスの考え方

ログ収集、レポート作成を行うファイアウォールの 台数分 のライセンスが必要です。
仮想ファイアウォールの場合も、ログを解析する仮想ファイアウォールの 台数分 のライセンスが必要です。

ファイアウォールの種類、構成（単一構成、冗長構成）によって製品名が異なります。

- 単一構成のSRXを1台
- 単一構成のFortiGateを2台
- 冗長構成のSRXを1組（2台で1組）

のログを収集して、レポートの作成を行う場合



SRX（単一構成）
FortiGate（単一構成）
FortiGate（単一構成）
SRX（冗長構成）

区分	製品名	必要な数量
ライセンス	FIREWALLstaff 対象FW単一構成ライセンス (SRX用) 1Firewall	1
	FIREWALLstaff 対象FW単一構成ライセンス (FortiGate用) 1Firewall	2
	FIREWALLstaff 対象FW冗長構成ライセンス (SRX用) 1Firewall	1
保守	FIREWALLstaff 保守サポート (SRX用) 1Firewall	2
	FIREWALLstaff 保守サポート (FortiGate用) 1Firewall	2

2-4 製品名と形名

HITACHI
Inspire the Next

■ ライセンス

対象ファイアウォール	製品名	形名
Juniper NetScreen/SSG シリーズ	FIREWALLstaff 対象FW単一構成ライセンス (NetScreen/SSG用) 1Firewall	Y-VB1-AP02333
	FIREWALLstaff 対象FW冗長構成ライセンス (NetScreen/SSG用) 1Firewall	Y-VB1-AP02334
Fortinet FortiGate シリーズ	FIREWALLstaff 対象FW単一構成ライセンス (FortiGate用) 1Firewall	Y-VB1-AP02336
	FIREWALLstaff 対象FW冗長構成ライセンス (FortiGate用) 1Firewall	Y-VB1-AP02337
Palo Alto PA シリーズ	FIREWALLstaff 対象FW単一構成ライセンス (PaloAlto用) 1Firewall	Y-VB1-AP02339
	FIREWALLstaff 対象FW冗長構成ライセンス (PaloAlto用) 1Firewall	Y-VB1-AP02340
Juniper SRX シリーズ	FIREWALLstaff 対象FW単一構成ライセンス (SRX用) 1Firewall	Y-VB1-AP02386
	FIREWALLstaff 対象FW冗長構成ライセンス (SRX用) 1Firewall	Y-VB1-AP02387
CheckPoint シリーズ	FIREWALLstaff 対象FW単一構成ライセンス (CheckPoint用) 1Firewall	Y-VB1-AP02391
	FIREWALLstaff 対象FW冗長構成ライセンス (CheckPoint用) 1Firewall	Y-VB1-AP02392

■ 保守

対象ファイアウォール	製品名	形名
Juniper NetScreen/SSG シリーズ	FIREWALLstaff 保守サポート (NetScreen/SSG用) 1Firewall	Y-VB1-AS02333#02
Fortinet FortiGate シリーズ	FIREWALLstaff 保守サポート (FortiGate用) 1Firewall	Y-VB1-AS02336#02
Palo Alto PA シリーズ	FIREWALLstaff 保守サポート (PaloAlto用) 1Firewall	Y-VB1-AS02339#02
Juniper SRX シリーズ	FIREWALLstaff 保守サポート (SRX用) 1Firewall	Y-VB1-AS02386#02
CheckPoint シリーズ	FIREWALLstaff 保守サポート (CheckPoint用) 1Firewall	Y-VB1-AS02391#02

3 - 1 体験版

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

付録(1) FIREWALLstaffの活用シーン

FIREWALLstaffの活用シーン(1)

HITACHI
Inspire the Next

(1) 自社で管理しているFWのSyslogを集計して、レポートで確認したい。

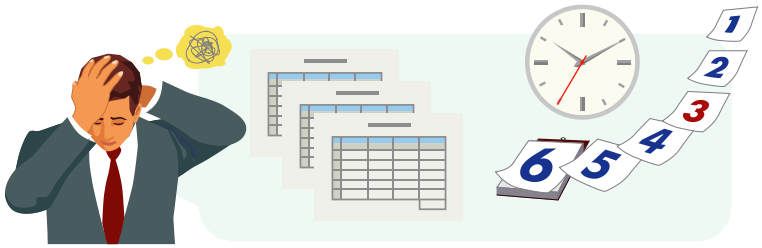
課題：手作業だとFWログの集計・分析に時間がかかる

- ログを目視確認するため、時間がかかりミスも発生する

⇒ 大量のFWログも、**高速で収集してレポート出力**します。

課題：FWログの保管期間が短く集計できない

- 問題発生時に過去の
  FWログを確認できない



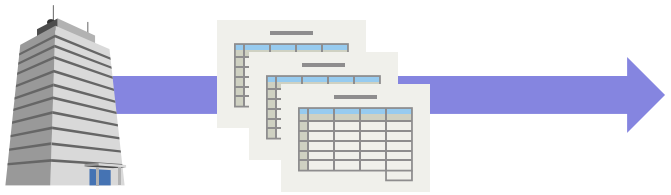
⇒ **ログの保管期間を指定**できます（デフォルトでは無制限）。
保管期間を過ぎたログは定期的に圧縮して管理します。

FIREWALLstaffの活用シーン(2)

HITACHI
Inspire the Next

(2) お客様のFWを管理しており、FWのSyslogを集計したレポートをお客様へ提出したい。

課題：お客様先からFWログを持ち出しできない

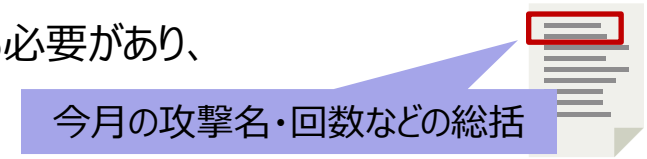


- FWのデータ量が多く、
  持ち出し申請も煩雑だ

お客様先にFWログ分析ソフトを導入するので、
FWログの持ち出しは不要です。

課題：月次レポートの冒頭に総括を添えるのに手間がかかる

- 月次レポートを読んで内容をまとめる必要があり、
  時間と手間がかかる



出力したレポートの**総括を自動的に作成**します。

付録(2)　他製品と比較した当製品の強みと弱み

FIREWALLstaffの強み

HITACHI
Inspire the Next

■通信方向別のレポートを生成できる

どのIPアドレスからどのIPアドレスへ通信しているかもレポーティングできます。
このため、不審サイトへアクセスしている社内のマシンを見つけたり、
社外から攻撃を受けている社内サーバを特定するようなことに役立ちます。

＃ NATやProxyを利用する環境の場合、IPアドレス以上の情報を得られず特定ができない場合があります。

■Word形式でレポートを出力できる

作成するレポートは、内容の修正ができないPDFや、加工が必須となるCSVではありません。
内容の流用ができ、編集も容易なWord形式でレポートを出力できるため、
FWユーザ様へのFW運用報告レポートを効率的に作成できます。

■FWのログを長期保管できる

FWのログの保管期限に制限を設けていないため、1年を超えるFWのログも保管できます。

■FWのトラフィック以外のログも保管できる

Syslogで受信した情報はすべて、指定したファイルに出力され、ファイルは日ごとに
ローテーションされますので、簡易Syslogサーバとして使用することもできます。
このため、FW機器本体のログを調査する場合にも役立ちます。

FIREWALLstaffの弱み

HITACHI
Inspire the Next

■Webブラウザ経由で操作ができない

FIREWALLstaffはネイティブアプリとなります。
ただし、レポートは自動メール送付され、設定変更も頻繁には行わないケースが多いため、
お客様がGUIを操作する機会は多くありません。

■対応OSがWindowsのみである

■レポートにリアルタイム性がない

日次、週次、月次、年次といったタイミングでレポートを作成するため、
今この時のFWの状況を確認するのには不向きです。
なお、任意のタイミングで手動にてレポートを作成することは可能です。

付録(3) レポートの内容

4-1 許可したトラフィックのレポート

HITACHI
Inspire the Next

■ Web通信レポート

下記の内容を、「接続回数順」「使用帯域量順」に集計してレポートします。

- 接続元ゾーンを区別して、集計することができます

外部ネットワークから接続され、FWが許可したWeb通信の、
・上位接続元IPアドレス一覧
・上位接続元IPアドレスと接続先IPアドレス一覧
・上位接続先IPアドレス一覧
・上位接続先IPアドレスと接続先IPアドレス一覧

内部ネットワークから接続され、FWが許可したWeb通信の、
・上位接続元IPアドレス一覧
・上位接続元IPアドレスと接続先IPアドレス一覧
・上位接続先IPアドレス一覧
・上位接続先IPアドレスと接続先IPアドレス一覧

DMZから接続され、FWが許可したWeb通信の、
・上位接続元IPアドレス一覧
・上位接続元IPアドレスと接続先IPアドレス一覧
・上位接続先IPアドレス一覧
・上位接続先IPアドレスと接続先IPアドレス一覧

- 接続元ゾーンを区別せずに、集計することもできます

FWが許可したWeb通信の、
・上位接続元IPアドレス一覧
・上位接続元IPアドレスと接続先IPアドレス一覧
・上位接続先IPアドレス一覧
・上位接続先IPアドレスと接続先IPアドレス一覧

■ メール通信レポート、FTP通信レポート、Telnet通信レポート

「Web通信レポート」と同様の内容のレポートを作成することができます。

4-1 許可したトラフィックのレポート

HITACHI
Inspire the Next

■ 指定したプロトコルのレポート

● 「Web通信レポート」「メール通信レポート」「FTP通信レポート」「Telnet通信レポート」のみならず、
指定したプロトコルの通信について、「Web通信レポート」と同様の内容のレポートを作成することができます
例）・DNS通信レポート
・NTP通信レポート

■ ファイアウォールが許可した通信のレポート

下記の内容を、「接続回数順」「使用帯域量順」（（※）については、「ルールに合致した回数順」）に集計してレポートします。

● 接続元ゾーンを区別して、集計することができます

外部ネットワークから接続され、FWが許可した通信の、
・上位接続元IPアドレス一覧
・上位接続元IPアドレスと接続先IPアドレス一覧
・上位接続先IPアドレス一覧
・上位接続先IPアドレスと接続先IPアドレス一覧
・上位プロトコル一覧
・上位プロトコルと接続元IPアドレス一覧
・上位プロトコルと接続先IPアドレス一覧
・上位接続元IPアドレスとプロトコル一覧
・上位接続先IPアドレスとプロトコル一覧
・上位ルール一覧（※）

内部ネットワークから接続され、FWが許可した通信の、
： （同上）

DMZから接続され、FWが許可した通信の、
： （同上）

● 接続元ゾーンを区別せずに、集計することもできます

FWが許可した通信の、
： （同上）

4-2 遮断したトラフィックのレポート

HITACHI
Inspire the Next

■ ファイアウォールが遮断した通信のレポート

下記の内容を、「接続回数順」（（※）については、「ルールに合致した回数順」）に集計してレポートします。

- 接続元ゾーンを区別して、集計することができます

外部ネットワークから接続され、FWが遮断した通信の、
- ・上位接続元IPアドレス一覧
- ・上位接続元IPアドレスと接続先IPアドレス一覧
- ・上位接続先IPアドレス一覧
- ・上位接続先IPアドレスと接続先IPアドレス一覧
- ・上位プロトコル一覧
- ・上位プロトコルと接続元IPアドレス一覧
- ・上位プロトコルと接続先IPアドレス一覧
- ・上位接続元IPアドレスとプロトコル一覧
- ・上位接続先IPアドレスとプロトコル一覧
- ・上位ルール一覧（※）

内部ネットワークから接続され、FWが遮断した通信の、
：　（同上）

DMZから接続され、FWが遮断した通信の、
：　（同上）

- 接続元ゾーンを区別せずに、集計することもできます

FWが遮断した通信の、
：　（同上）

4-3 UTMレポート

HITACHI
Inspire the Next

■ 攻撃レポート

下記の内容を、発生回数順に集計してレポートします。

- 攻撃元ゾーンを区別して、集計することができます

外部ネットワークから接続された攻撃の、
・上位攻撃名一覧
・上位攻撃元IPアドレス一覧
・上位攻撃先IPアドレス一覧
・上位攻撃名と攻撃元IPアドレス一覧
・上位攻撃元IPアドレスと攻撃名一覧
・上位攻撃名と攻撃先IPアドレス一覧
・上位攻撃先IPアドレスと攻撃名一覧

内部ネットワークから接続された攻撃の、
：　（同上）

DMZから接続された攻撃の、
：　（同上）

- 接続元ゾーンを区別せずに、集計することもできます

発生した攻撃の、
：　（同上）

※ 次のファイアウォールにおいては、「攻撃検知」と「攻撃防御」に分けてレポートします
・Fortinet FortiGateシリーズ
・Palo Alto PAシリーズ
・Juniper SRXシリーズ
・CheckPointシリーズ

4-3 UTMレポート

HITACHI
Inspire the Next

■ ウイルスレポート

下記の内容を、発生回数順に集計してレポートします。

● ウイルス送信の接続元ゾーンを区別して、集計することができます

外部ネットワークから接続されたウイルスの、
- ・上位ウイルス名一覧
- ・上位接続元IPアドレス一覧
- ・上位接続先IPアドレス一覧
- ・上位ウイルス名と接続元IPアドレス一覧
- ・上位接続元IPアドレスとウイルス名一覧
- ・上位ウイルス名と接続先IPアドレス一覧
- ・上位接続先IPアドレスとウイルス名一覧

内部ネットワークから接続されたウイルスの、
：　（同上）

DMZから接続されたウイルスの、
：　（同上）

●ウイルス送信の接続元ゾーンを区別せずに、集計することもできます

発生したウイルスの、
：　（同上）

※ 次のファイアウォールにおいては、「ウイルス検知」と「ウイルス防御」に分けてレポートします
- ・Palo Alto PAシリーズ
- ・CheckPointシリーズ

4-3 UTMレポート

■ スパムメールレポート

下記の内容を、発生回数順に集計してレポートします。

・上位接続元IPアドレス一覧
・上位送信元メールアドレス一覧
・上位接続元IPアドレスと送信元メールアドレス一覧

■ URLフィルタリングレポート

下記の内容を、発生回数順に集計してレポートします。

ブロックされたWebアクセスの、
・上位接続元IPアドレス一覧
・上位アクセス先URL（FQDN）一覧
・上位アクセス先カテゴリ一覧
・上位接続元IPアドレスとアクセス先URL（FQDN）一覧
・上位接続元IPアドレスとアクセス先カテゴリ一覧
・上位アクセス先カテゴリと接続元IPアドレス一覧

4-4 アプリケーションレポート

HITACHI
Inspire the Next

■ アプリケーション制御機能が許可した通信のレポート

下記の内容を、発生回数順に集計してレポートします。

- 接続元ゾーンを区別して、集計することができます

外部ネットワークから接続され、アプリケーション制御機能が許可した通信の、
- ・上位アプリケーション一覧
- ・上位カテゴリ一覧
- ・上位アプリケーションと接続元数一覧
- ・上位アプリケーションと接続元一覧
- ・上位カテゴリとアプリケーション一覧
- ・上位カテゴリと接続元数一覧
- ・上位カテゴリと接続元一覧
- ・上位接続元とアプリケーション数一覧
- ・上位接続元とアプリケーション一覧

内部ネットワークから接続され、アプリケーション制御機能が許可した通信の、
：　（同上）

DMZから接続接続され、アプリケーション制御機能が許可した通信の、
：　（同上）

- 接続元ゾーンを区別せずに、集計することもできます

アプリケーション制御機能が許可した通信の、
：　（同上）

4-4 アプリケーションレポート

HITACHI
Inspire the Next

■ アプリケーション制御機能が遮断した通信のレポート

下記の内容を、発生回数順に集計してレポートします。

- 接続元ゾーンを区別して、集計することができます

外部ネットワークから接続され、アプリケーション制御機能が遮断した通信の、
- ・上位アプリケーション一覧
- ・上位カテゴリ一覧
- ・上位アプリケーションと接続元数一覧
- ・上位アプリケーションと接続元一覧
- ・上位カテゴリとアプリケーション一覧
- ・上位カテゴリと接続元数一覧
- ・上位カテゴリと接続元一覧
- ・上位接続元とアプリケーション数一覧
- ・上位接続元とアプリケーション一覧

内部ネットワークから接続され、アプリケーション制御機能が遮断した通信の、
：　（同上）

DMZから接続接続され、アプリケーション制御機能が遮断した通信の、
：　（同上）

- 接続元ゾーンを区別せずに、集計することもできます

アプリケーション制御機能が遮断した通信の、
：　（同上）

お問合わせ

本製品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。

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 ご紹介

株式会社 日立ソリューションズ