



# WatchGuard XTM

## ログ&レポート設定ガイド

### Ver. 11.7 – 11.9



ウォッチガード・テクノロジー・ジャパン株式会社

2014 年 8 月 Rev-01

## 目次

ログサーバーおよびレポートサーバーについて .....	3
ログサーバー .....	3
レポートサーバー .....	3
注意点 .....	3
ログサーバーおよびレポートサーバーのインストール .....	4
ログサーバーの構成 .....	7
初期設定ウィザード .....	7
ログサーバーの設定 .....	13
XTM 側のログ送信設定 .....	17
ログ受信確認 .....	20
レポートサーバーの構成 .....	21
レポートサーバーの各種設定 .....	22
ログおよびレポートの表示方法 .....	29
アクセス方法 .....	29
ログの表示 .....	31
ログの閲覧 .....	31
ログのダウンロード .....	33
レポートの表示 .....	35
レポートの閲覧 .....	35
PDF レポートのダウンロード .....	39

## ログサーバーおよびレポートサーバーについて

WatchGuard ログサーバーとレポートサーバーは、WSM に含まれているサーバーソフトウェアです。

### ログサーバー

ログサーバーは XTM デバイスから送られてくるログを受信し、データベースに保存します。そのログは閲覧、ダウンロード、レポート生成に用いることができます。

### レポートサーバー

レポートサーバーはログサーバーからデータを取得し、XTM デバイスのアクティビティに関するレポートを作成します。

### 注意点

WatchGuard のサーバーソフトウェアは、XTM をご利用のお客様には**無償でご提供**しています。

これらサーバーソフトウェアをご利用の際には、別途サーバーマシンが必要となります。要求スペックなどは WSM のリリースノートをご覧ください。

なお、このガイドはログ&レポートサーバーを動作させるために必要な情報にフォーカスし、手早く動作させることを目的としています。

このガイドで説明されていない設定項目や、各設定項目の詳細な解説については、各画面のヘルプボタンをクリックし、参照されることをおすすめいたします。

このガイドを参考にいただき、ご活用いただければ幸いです。

## ログサーバーおよびレポートサーバーのインストール

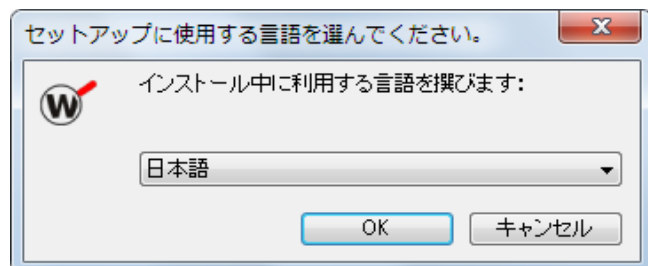
ログサーバーとレポートサーバーはどちらもサーバーソフトウェアとして同時にインストールすることができます。

インストール後は WSC (WatchGuard Server Center) というサーバーソフトウェアの管理コンソールから設定することができます。

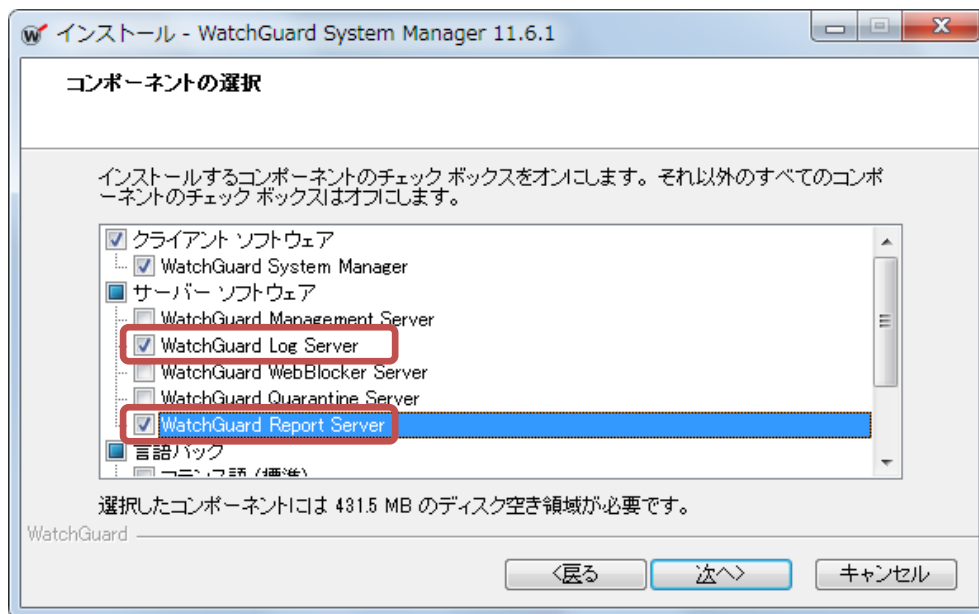
WSM のインストーラーを実行します。



セットアップ中の言語を選択します。日本語で OK ボタンをクリックします。

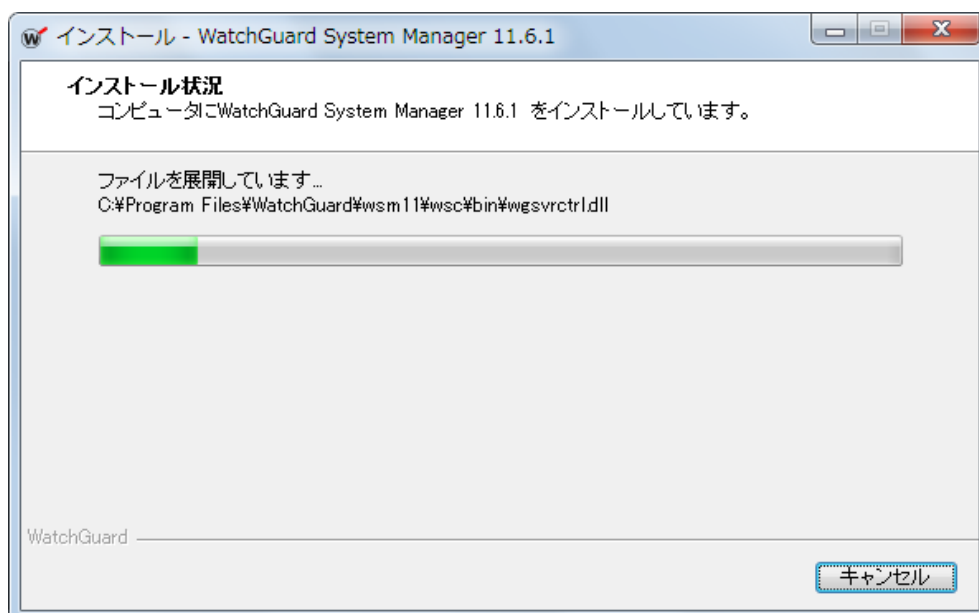


コンポーネントの選択でサーバーソフトウェアのツリーにある「Watchguard Log Server」と「Watchguard Report Server」にチェックを入れて次に進みます。



クライアントソフトウェアがインストールしてある場合は、そのインストール先にインストールが始まります。クライアントソフトウェアも含めてはじめてのインストールであればインストール先を選択する画面が出ますので、デフォルトのまま次に進みます。

するとファイルのコピーが始まります。



しばらくするとインストールが完了します。



完了ボタンをクリックします。

インストールは以上です。

### 初期設定ウィザード

インストール後、タスクトレイに WatchGuard Server Center のアイコンが表示されます。これをダブルクリックし、WSC を起動させます。



初回の起動なので、構成されていないサーバーの設定ウィザードが始まります。次へ。



組織名を入力し、次へ。



WatchGuard Server Center Setup Wizard

全般設定：組織名の指定

組織名：

 組織名は、このシステムの WatchGuard サーバーが使用する、自己署名認証機関 (CA) 証明書の識別名 (DN) に使用されます。

管理者のパスワードを入力します。WSC を起動するときに入力するものです。



WatchGuard Server Center Setup Wizard

全般設定：管理者のパスワードの設定

管理者アカウント：

管理者のパスワード：

パスワードの確認：

 サーバにログインして変更を行う場合は、管理者のパスワードを使用してください。8 文字以上を使用してください。

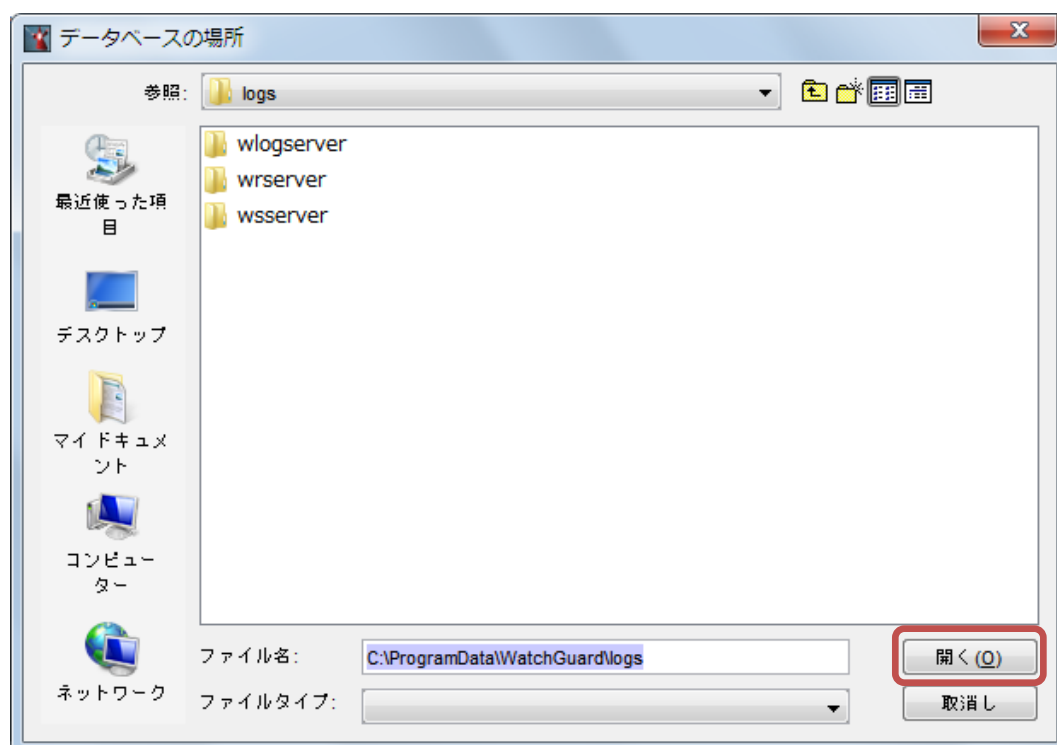


暗号化キーを入力します。これは XTM 側にログ送信の設定をする際に必要となります。



データベースの場所は参照ボタンをクリックします。

ログの場所は、特に決めてなければデフォルトの場所を、ログのために確保した領域があればそこを指定します。



データベースの場所が入ったら次へ。

WatchGuard Server Center Setup Wizard

Log Server: 暗号化キーおよびデータベースの場所の設定

暗号化キー: [Masked]

暗号化キーの確認: [Masked]

ウィザードは、Log Server データベースを指定されたディレクトリにインストールします。

データベースの場所: C:\ProgramData\WatchGuard\logs [参照]

*i* 暗号化キーは、デバイスとサーバー間にセキュリティチャネルを確立し、第三者による盗聴などを防止するために使用されます。

[ヘルプ] [戻る] [次へ>] [キャンセル]

設定の確認をし、次へ。

WatchGuard Server Center Setup Wizard

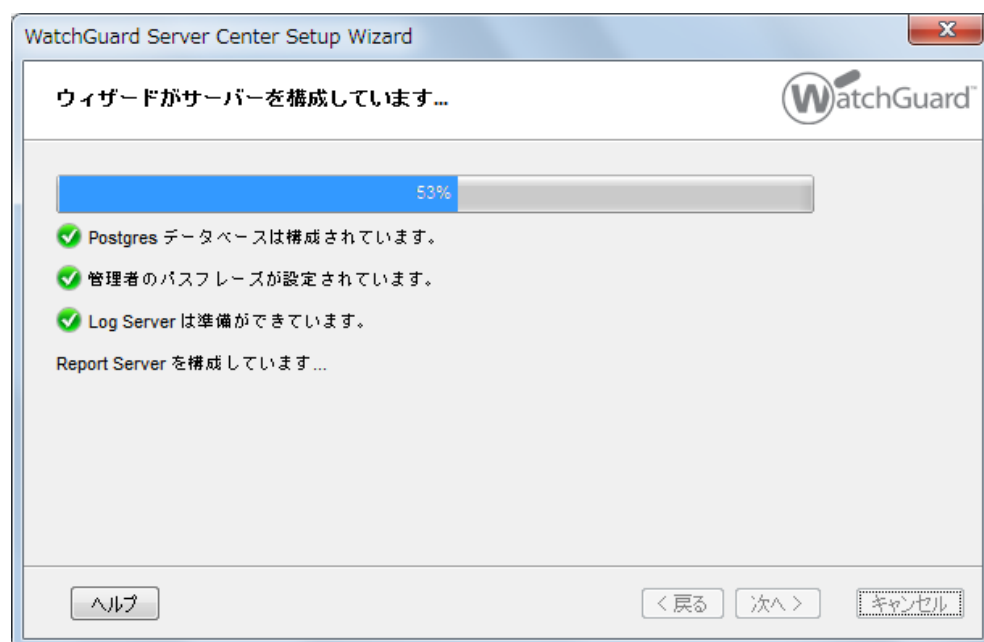
設定の確認

変更を確認します。[次へ]をクリックした後で変更することはできません。

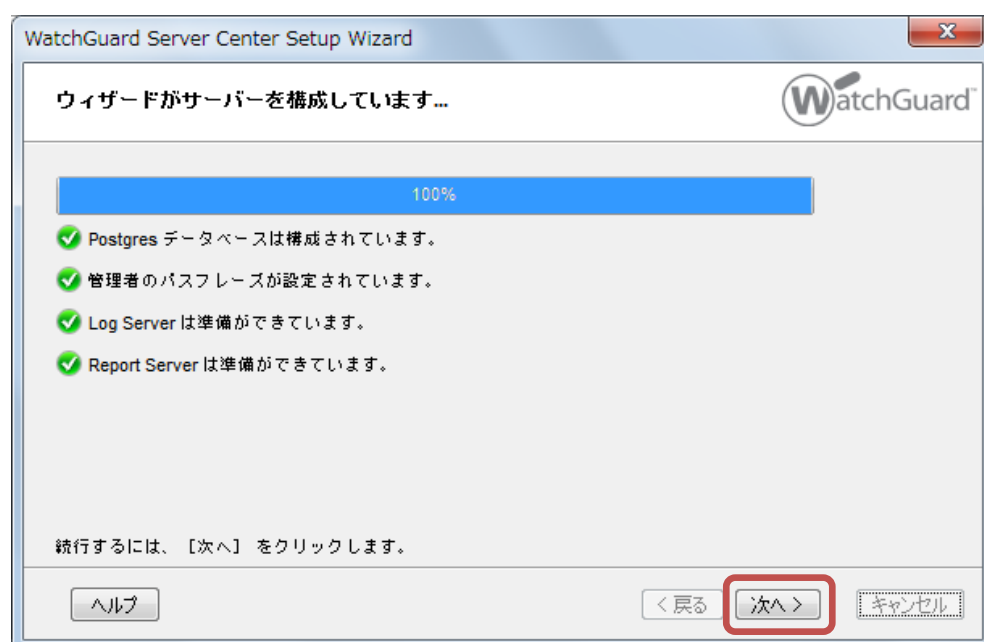
[全般] 設定	認証パスワードの設定、CA 組織: WatchGuard
Log Server の設定	暗号化キー の設定
Report Server の設定	Log ServerのIP アドレスが、Report Server と同じです

[ヘルプ] [戻る] [次へ>] [キャンセル]

設定が反映されます。



100%まで進んだら、次へ。

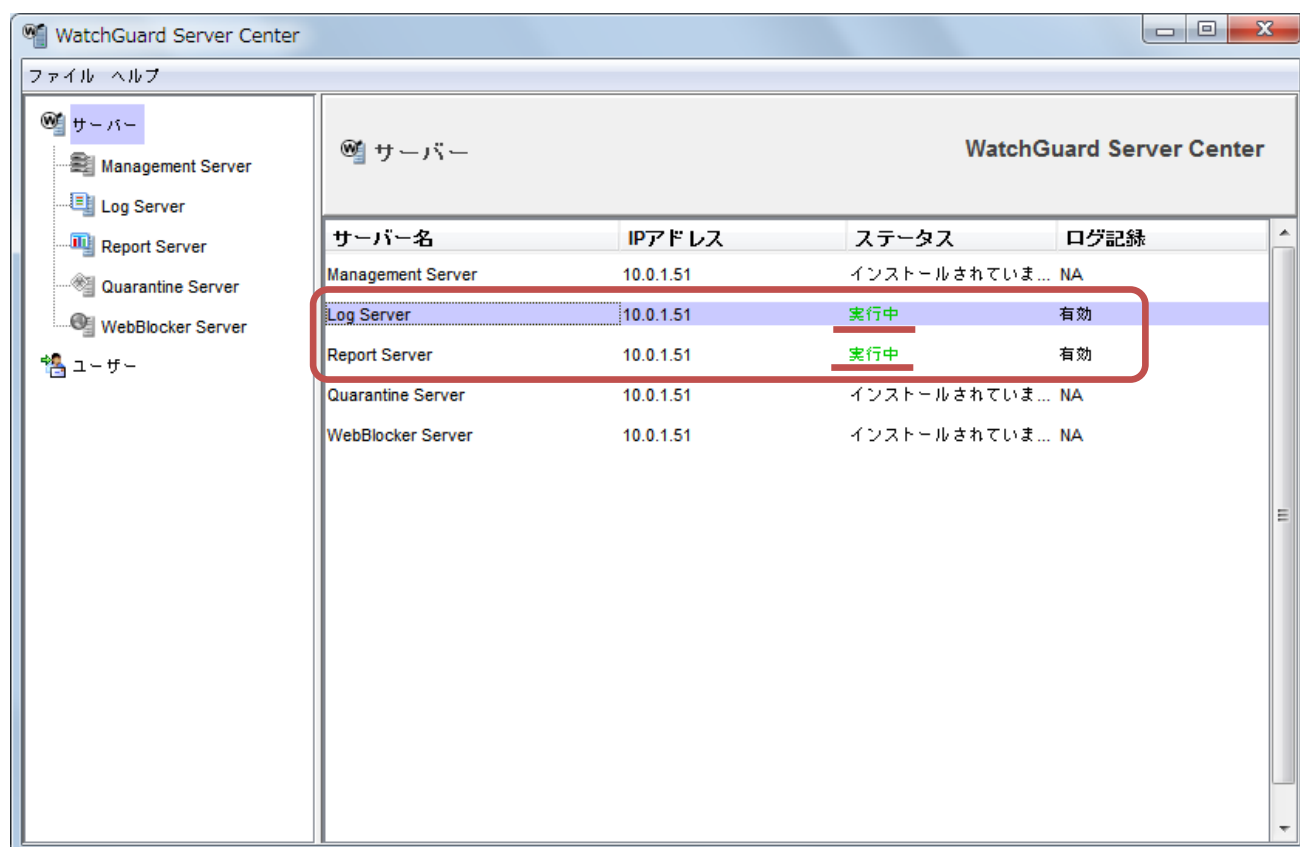


Wizard が完了します。完了ボタンをクリックします。



WSC が起動し、サーバーのステータスが表示されます。

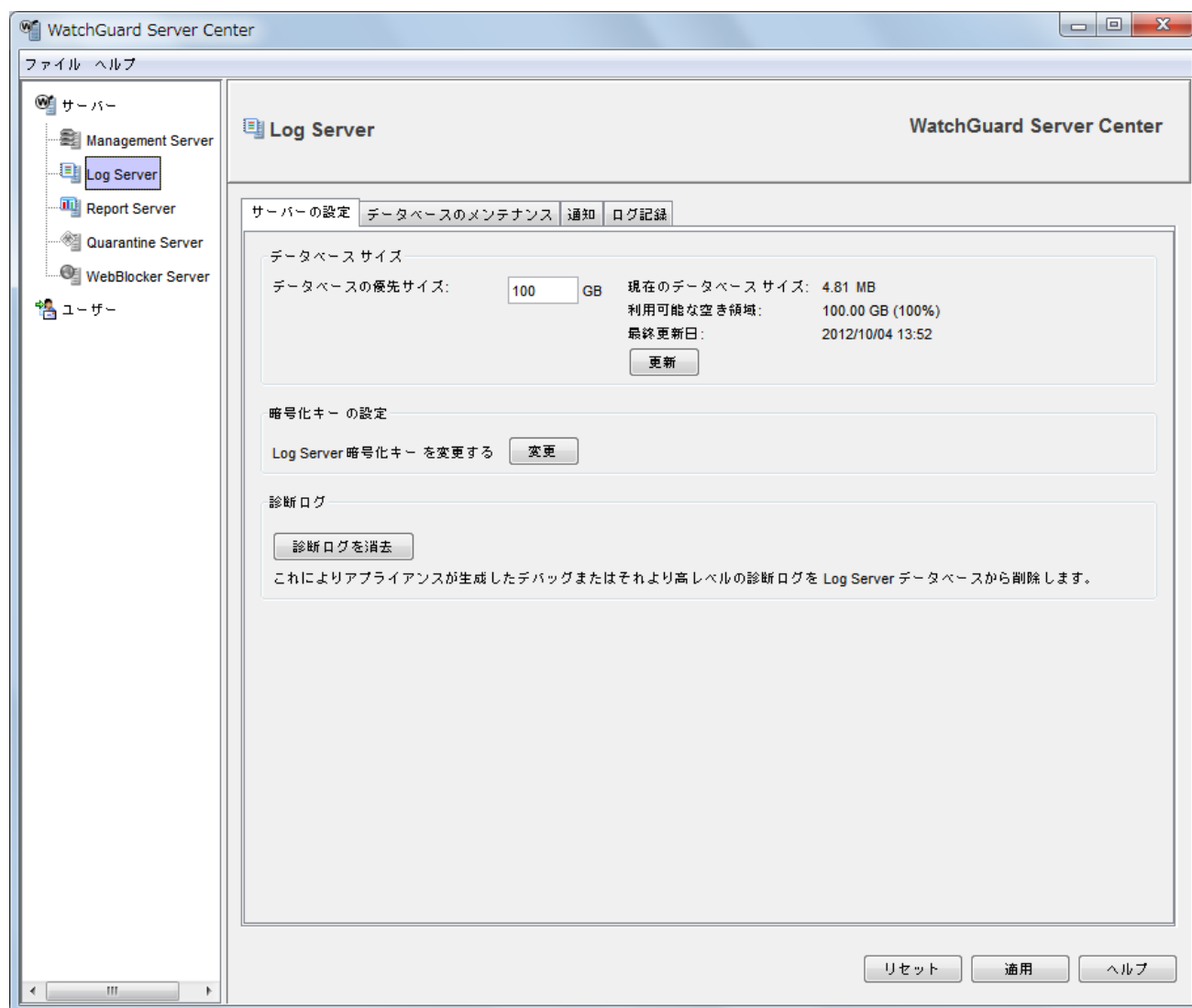
Log Server と Report Server が実行中であることを確認してください。



## ログサーバーの設定

左側メニューの Log Server をクリックすると、ログサーバーの詳細設定をすることができます。

ウィザードで設定できなかった項目や、変更したい項目も、こちらから設定できます。



それではタブごとの各種設定について解説します。

## ● サーバーの設定タブ

「データベースサイズ」のセクションで、ログを保存するデータベースのサイズを設定できます。ディスクの空き容量に見合うサイズを設定します。この値を超えた場合は、古いデータから順次削除されてゆきます。

サーバーの設定 | データベースのメンテナンス | 通知 | ログ記録

データベース サイズ

データベースの優先サイズ: 100 GB

現在のデータベース サイズ: 4.81 MB

利用可能な空き領域: 100.00 GB (100%)

最終更新日: 2012/10/04 13:52

更新

暗号化キー の設定

Log Server 暗号化キー を変更する 変更

診断ログ

診断ログを消去

これによりアプライアンスが生成したデバッグまたはそれより高レベルの診断ログを Log Server データベースから削除します。

## ● データベースのメンテナンスタブ

「データベースのバックアップ設定」セクションでは、ログデータのバックアップスケジュールを設定できます。「データベースの設定」セクションでは、外部の PostgreSQL サーバーをログ DB として使いたい場合は、データベースの設定のセクションで指定できます。

サーバーの設定 | データベースのメンテナンス | 通知 | ログ記録

データベースのバックアップ設定

☐ ログメッセージを自動的にバックアップ

ログデータをバックアップする間隔: 1 日間

最後のバックアップ日:

ログデータをバックアップする時間: 11:30

予定されている次のバックアップ: 2012/10/04 11:30

バックアップファイルのディレクトリパス: C:\ProgramData\WatchGuard\wlogserver\tmp

参照

バックアップ ログ ファイルを復元する

今すぐバックアップを作成します。

データベースの設定

☒ 組み込みデータベース ☐ 外部 PostgreSQL データベース

ログデータはこの場所で保存および管理されています:

C:\ProgramData\WatchGuard\logs

データベースの設定

☐ 組み込みデータベース ☒ 外部 PostgreSQL データベース

ログデータはこの場所で保存および管理されています:

データベース名: wglogdb

IP アドレス: 10.0.1.110

ポート: 5432

データベース ユーザー: loguser

パスワード: ●●●●●●●●●●

接続のテスト

詳細については、【ヘルプ】をクリックしてください。

※ 必ず接続のテストをしてください

## ● 通知タブ

デバイスのポリシーで通知を有効にしたい場合や障害イベントを通知したい場合、ここで設定します。

**通知のタイミング**

イベント

電子メールの通知を送信する:

- ☒ この Log Server で障害イベントが発生したとき
- ☒ 任意のデバイスまたはサーバーからイベント通知を受信するとき
- ☒ データベースからログ メッセージを削除するとき

**メールの送信設定**

SMTP サーバーの設定

送信電子メール サーバー (SMTP):   
例: smtp.mydomain.com または smtp.mydomain.com:<port number>

☐ 電子メール サーバーにユーザー認証情報を送信

ユーザー名:

パスワード:

**通知設定**

この送信先に電子メールを送信:   
例: administrator@mycompany.com

電子メールの送信者:   
例: logServer@mycompany.com

件名:

電子メールのテスト

## ● ログ記録タブ

ログを送信してくる XTM デバイスが一覧に表示されます。後ほどデバイス側の設定で触れます。

サーバーの設定 データベースのメンテナンス 通知 ログ記録

**Firebox のステータス**

Log Serverに接続されているすべてのFireboxデバイスが、このリストに表示されます。

IP アドレス	シリアル番号	Fireboxの種類	Firebox のステータス
接続されログを送信してきている XTM デバイスが、ここに一覧表示されます。			

更新 現在 Log Server に接続している Firebox のデバイスはありません。 削除

**Windows イベント ビューア**

☐ ログ メッセージをWindows イベント ビューアに送信

ログ レベルを選択:

**ファイルのパス**

☒ ログ メッセージをファイルに送信

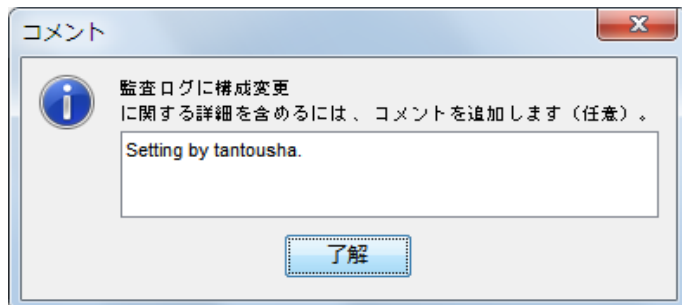
ファイルの場所:  参照

ログ レベルを選択:

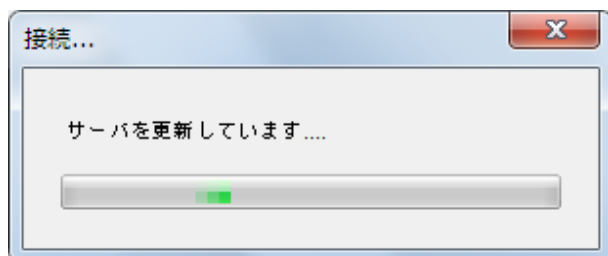
ログサーバーを一通り設定したら、左下にある適用ボタンをクリックします。



構成変更時にはコメントの入力が求められますので、入力して了解ボタンをクリックします。



サーバーが再起動されます。



設定が反映されます。

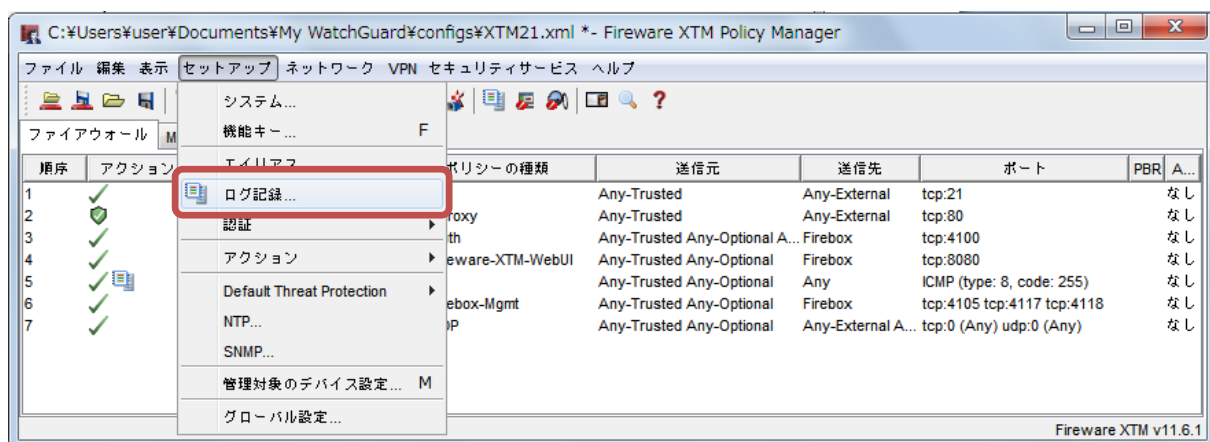




## XTM 側のログ送信設定

XTM デバイス側に、ログサーバーにログを送信する設定について解説します。

ポリシーマネージャのメニュー **セットアップ** – **ログ記録** をクリックします。

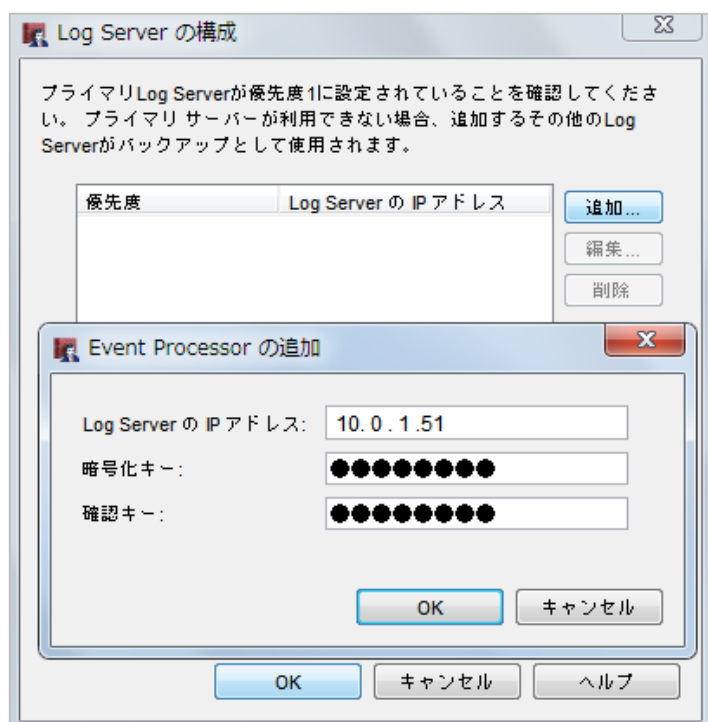


ログ記録のセットアップ画面で、構成ボタンをクリックします。



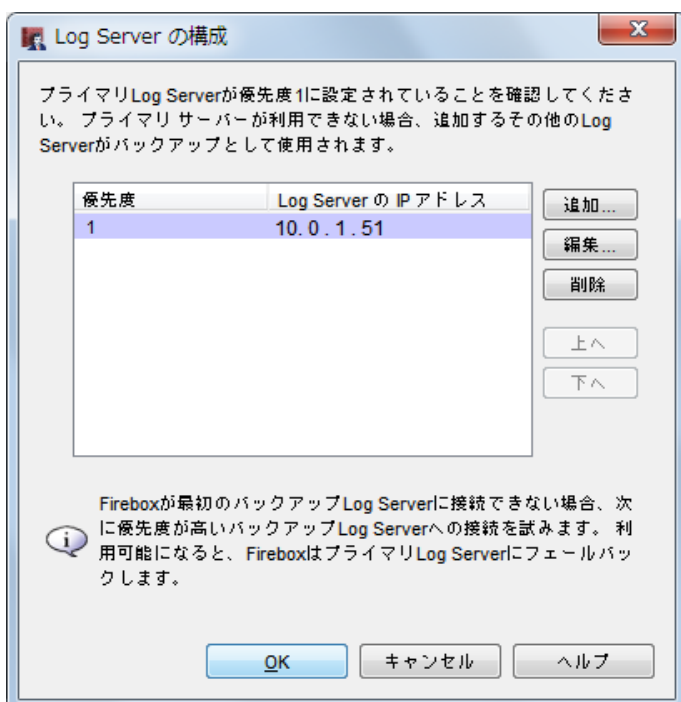
LogServer の構成画面で追加ボタンをクリックします。

EventProcessor の追加画面で、ログサーバーの IP アドレスとログサーバー側で設定した暗号化キーを入力します。

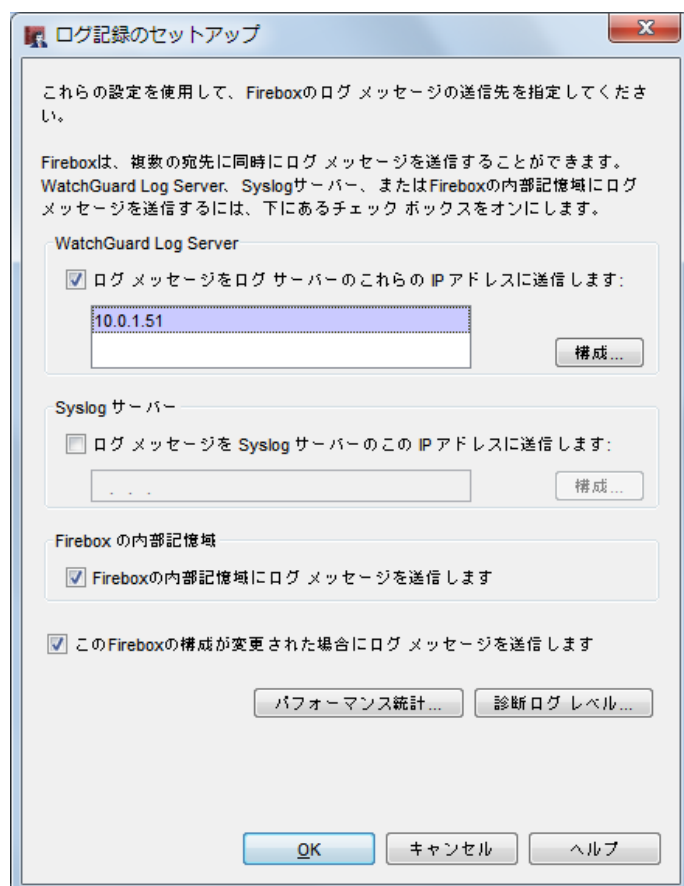


暗号化キーのフレーズが合致すると、ログサーバーに接続し、ログ受信が許可されます。

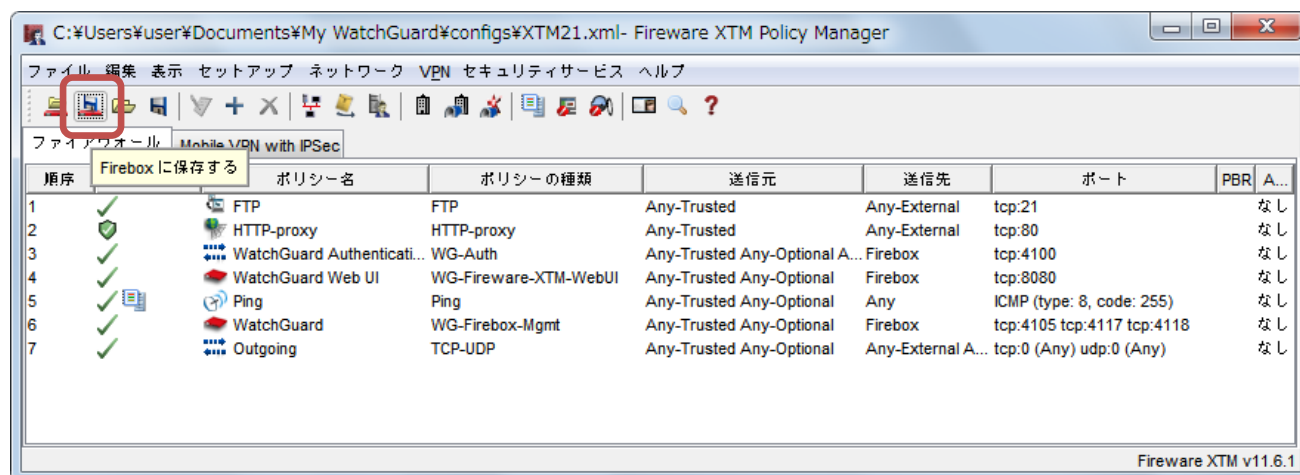
OK で抜けると以下のように、ログサーバーの一覧に表示されます。



ログ記録のセットアップ画面に戻り、ログサーバーが追加されたことを確認し、OK をクリック

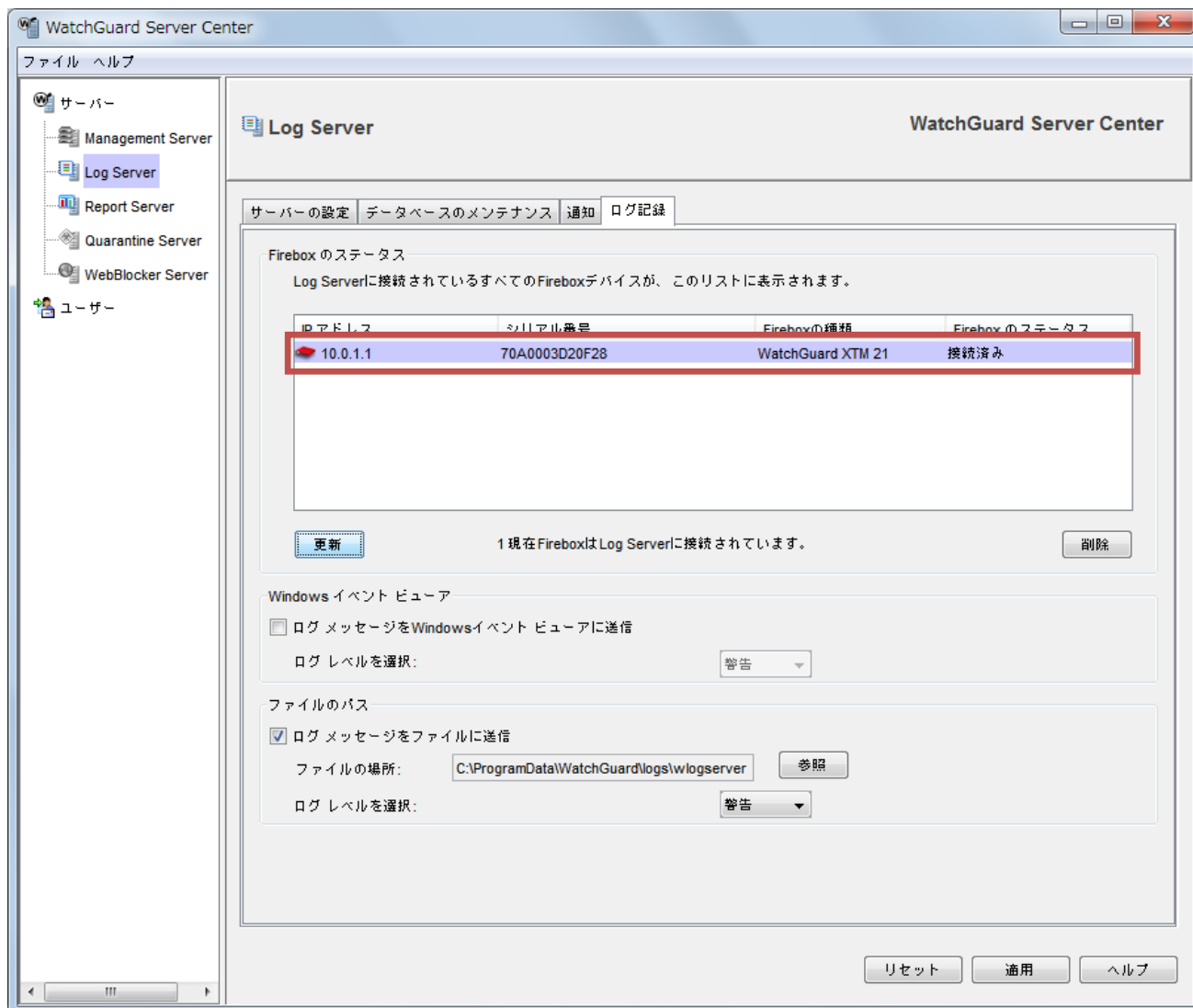


以上の設定をしたら、デバイスに設定を保存しましょう。



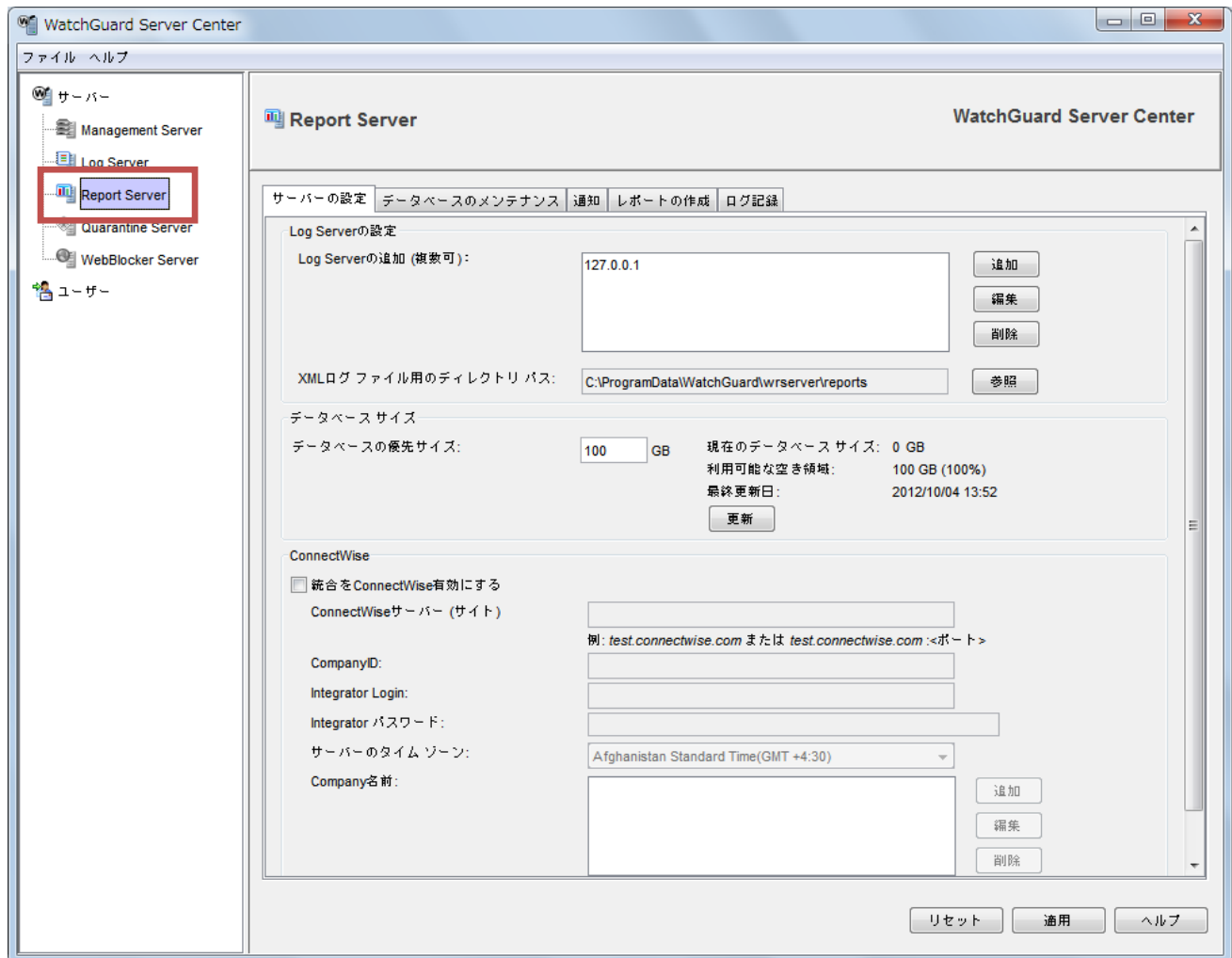
## ログ受信確認

WSC のログサーバーをクリックし、ログ記録タブを選択すると、ログ送信の設定をしたデバイスが一覧に表示され、ステータスが「接続済み」になっていればログ受信ができていることが確認できます。



## レポートサーバーの構成

WSC の左側にあるサーバーツリーの「Report Server」を選択します。



レポートサーバーは以下のような設定項目に分かれています。

- サーバーの設定
- データベースのメンテナンス
- 通知
- レポートの作成
- ログ記録

次頁から各種の設定について解説します。

## レポートサーバーの各種設定

### ● サーバーの設定 タブ

「Log Server の設定」セクションでは、レポートサーバーが接続できる Log Server を指定します。

サーバーの設定 | データベースのメンテナンス | 通知 | レポートの作成 | ログ記録

Log Server の設定

Log Server の追加 (複数可): 10.0.1.51

XML ログ ファイル用のディレクトリ パス: C:\ProgramData\WatchGuard\wserver\reports

データベース サイズ

データベースの優先サイズ: 100 GB

現在のデータベース サイズ: 0 GB

利用可能な空き領域: 100 GB (100%)

最終更新日: 2012/10/04 13:52

更新

追加ボタンをクリックし、あらかじめ設定してある Log Server の IP アドレスとパスワードを入力します。

Log Server の追加

Log Server の IP アドレスとパスワードを入力してください。

IP アドレス: 10.0.1.51

パスワード: ●●●●●●●●

OK キャンセル

その下の「データベースサイズ」セクションでは、レポート用データベースの最大サイズを指定します。  
最大サイズに達した場合、最も古いレポートデータを削除して、新規レポートのスペースを確保します。

データベース サイズ

データベースの優先サイズ: 800 GB

現在のデータベース サイズ: 0.00 GB

利用可能な空き領域: 800 GB (100%)

最終更新日: 2012/10/04 13:52

更新

## ● データベースのメンテナンス

ここではレポートサーバーのレポートデータ削除の設定と、データベースの設定を構成することができます。

「レポート削除の設定」セクションでは、レポートを保持する期間を設定できます。保持する期間はデフォルトで 30 日、最低で 1 日、最大で 365 日（1 年間）です。

サーバーの設定   データベースのメンテナンス   通知   レポートの作成   ログ記録

レポートの削除の設定

Report Server にレポートを保持する期間: 30 日間   最後に削除されたメッセージ:

有効期限切れのレポートを削除する時間: 8:55   予定されている次の削除: 2012/10/05 08:55

データベースの設定

☒ 組み込みデータベース   ☐ 外部 PostgreSQL データベース

ログ データはこの場所で保存および管理されています:

C:\ProgramData\WatchGuard\logs

「データベースの設定」セクションでは、レポート用のデータベースの設定ができます。

外部のデータベースを指定するには、次のように「外部 PostgreSQL データベース」にチェックを入れて、データベースアクセスに必要な情報を入力します。

データベースの設定

☐ 組み込みデータベース   ☒ 外部 PostgreSQL データベース

ログ データはこの場所で保存および管理されています:

データベース名: wgreport

IP アドレス: 10.0.1.111   ポート: 5432

データベース ユーザー: reportuser

パスワード: ●●●●●●●●   接続のテスト

詳細については、【ヘルプ】をクリックしてください。

※ データベースの設定を変更する場合、変更を反映するために、レポートサーバーを再起動する必要があります

※ 必ず接続のテストボタンをクリックし、問題ないことを確認してください

## ● 通知

通知タブでは、失敗したイベントとデータベースのサイズについてのアラートを、指定した送信先に通知する設定ができます。「イベント」セクションで、通知してほしい項目にチェックを入れます。

サーバーの設定 データベースのメンテナンス **通知** レポートの作成 ログ記録

イベント

☒ 失敗したイベントに関する通知を有効にする

☒ データベースのサイズが警告のしきい値に達した場合に電子メールで通知を送信

警告のしきい値: 80 %

SMTP サーバーの設定

送信電子メール サーバー (SMTP): mail.company.domain  
例: smtp.mydomain.com または smtp.mydomain.com:<port number>

☐ 電子メール サーバーにユーザー認証情報を送信

ユーザー名:

パスワード:

通知設定

この送信先に電子メールを送信: JPNSales@watchguard.com  
例: administrator@mycompany.com

電子メールの送信者: wrsrrserver@localhost  
例: ReportServer@mycompany.com

件名: WatchGuard Report Server Notification

本文: Please check the log message.

「イベント」セクションの失敗したイベントとは、データベースへの接続が失われた、データベース側のエラー、レポート作成時のエラー、Log Server への接続エラーが該当します。

「SMTP サーバーの設定」セクションでメールサーバーを指定します。

「通知設定」セクションで TO、From、件名、本文を指定します。



## ● レポートの作成

レポートサーバーにはアーカイブされたレポートとオンデマンドレポートを作成します。そしてそれらのレポートを表示するためには、元データとなる XML を定期的に生成しなければなりません。

このレポート作成タブでは、XML ファイルを生成するスケジュールを設定します。

The screenshot shows a web-based configuration interface for report creation. At the top, there is a navigation bar with tabs: 'サーバーの設定', 'データベースのメンテナンス', '通知', 'レポートの作成' (highlighted with a red box), and 'ログ記録'. Below the tabs, the main content area is titled 'レポートの作成の設定'. It contains a text box for '概要レポートに含まれるレコード数' with the value '50'. Below this is a section titled 'レポートスケジュール' with the subtitle 'レポート作成のためのスケジュール作成および管理'. This section contains a table with columns '名前', '説明', and '種類'. To the right of the table are three buttons: '追加', '編集', and '削除'. Below the table is a section titled 'レポートグループ' with the subtitle '選択済みのグループメンバー'. It contains two text boxes for 'グループ名:' and '選択済みのグループメンバー'. To the right of these text boxes are three buttons: '追加', '編集', and '削除'. At the bottom of the interface are three buttons: 'リセット', '適用', and 'ヘルプ'.

「レポートスケジュール」セクションの追加ボタンをクリックします。

This is a close-up screenshot of the 'レポートスケジュール' section from the previous image. It shows the table with columns '名前', '説明', and '種類'. To the right of the table, the '追加' button is highlighted with a red box. Below it are the '編集' and '削除' buttons.

新しいスケジュール画面が表示されます。スケジュール名を入力します。

「スケジュール設定」タブで、どのデバイスのレポートを作成するか、どの種類のレポート作成を有効にするか、どれくらいの頻度で作成するかを指定します。

The screenshot shows the '新しいスケジュール' (New Schedule) dialog box. It has a title bar with a close button (X). The main area is divided into several sections:

- スケジュール名:** A text field containing 'Dairy Report'. A callout bubble points to it with the text 'スケジュール名を入力'.
- 説明 (任意):** An empty text field.
- スケジュール設定** (highlighted with a red box), **エンドユーザー通知**, and **詳細設定** tabs.
- このスケジュールの詳細を指定する** section:
  - デバイス:** A list box showing 'すべてのデバイス' (selected) and 'XTM21 [70A0003D20F28]'.
  - レポートの種類:** A list box showing 'WatchGuard レポート', 'コンプライアンス レポート', 'Application Control', 'BUM レポート', and 'Firebox レポート', all of which are checked.
- スケジュールをレポートする** section:
  - 1回実行:** Radio button, date '2012/10/05', and time '10:15'.
  - 繰り返し実行:** Selected radio button, dropdown menu set to '毎日' (Daily).
  - メモ:** Text area with '日次レポートにはレポートが生成される前...'.
  - 毎週再現:** Unchecked checkbox.
  - 再現範囲:** Section with '開始' (Start) date '2012/10/05' and time '10:15', and '終了日なし' (No end date) selected.
  - 終了期限:** Radio button, date '2012/10/05', and time '10:15'.

At the bottom are buttons for 'OK', 'キャンセル' (Cancel), and 'ヘルプ' (Help).

Callout bubbles provide additional instructions:

- '対象デバイスを指定' (Specify target device) points to the device list.
- 'レポートの種類を指定' (Specify report type) points to the report type list.
- 'レポートデータ生成の頻度を指定。日次でレポートを閲覧する場合は「毎日」を設定します' (Specify report data generation frequency. If viewing reports daily, set '毎日') points to the '毎日' dropdown.

「詳細設定」タブでは、レポートを HTML もしくは PDF 形式で出力する設定ができます。  
この機能を有効にするために「外部で使用するレポートの生成」にチェックを入れます。

The screenshot shows the 'WatchGuard report' configuration window. The 'スケジュール名' (Schedule Name) is 'Dairy Report'. The '詳細設定' (Detailed Settings) tab is selected. The '外部で使用するレポートの生成' (Generate reports for external use) checkbox is checked. The '書式' (Format) is set to 'PDF'. The '場所' (Location) is 'C:\ProgramData\WatchGuard'. Callouts explain: 'このチェックで有効になります' (This check makes it effective), '出力形式を選択します' (Select the output format), and '指定した場所に出力されます' (Output to the specified location).

新しいスケジュール

スケジュール名: Dairy Report

説明 (任意):

スケジュール設定 エンドユーザー通知 **詳細設定**

WatchGuard report アプリケーション (例: IIS Web サーバー) 以外で使用するレポートを生成するには、このチェックボックスを有効にします。

☒ 外部で使用するレポートの生成

☒ グループ内のデバイスごとに 1 つのレポート  
☐ グループ内のすべてのデバイスを合わせたデータに対して 1 つのレポート

書式: ☐ HTML ☒ PDF

Display dates and times using: 現地タイムゾーン (日本標準時: UTC+9)

場所: C:\ProgramData\WatchGuard 参照

OK キャンセル ヘルプ

このチェックで有効になります

出力形式を選択します

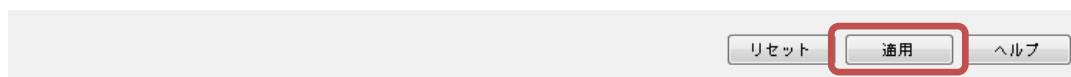
指定した場所に出力されます

HTML か PDF で出力されます。場所はレポートサーバーの都合のよい場所をしてします。

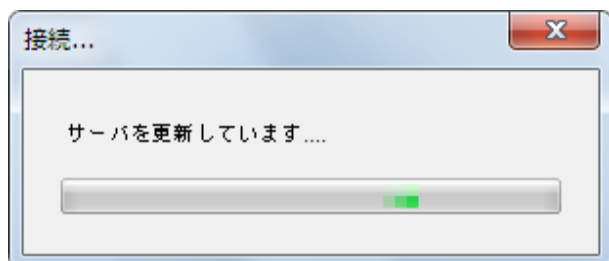
デバイスごとのレポートが必要なら「グループ内のデバイスごとに一つのレポート」にチェックを入れます。(グループを設定していなければこちら)

以上が設定できたら、OK ボタンをクリックします。

最後に画面右下の適用ボタンをクリックします。



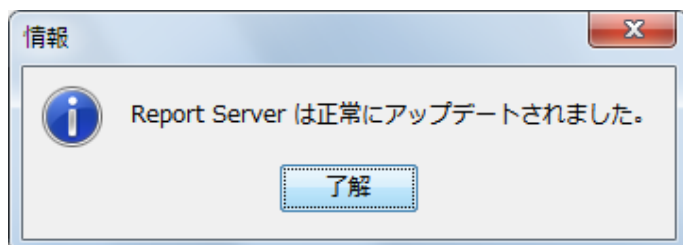
設定の更新がかかります。



構成変更時にはコメントの入力が求められますので、入力して了解ボタンをクリックします。



設定が反映されました。了解ボタンをクリックします。



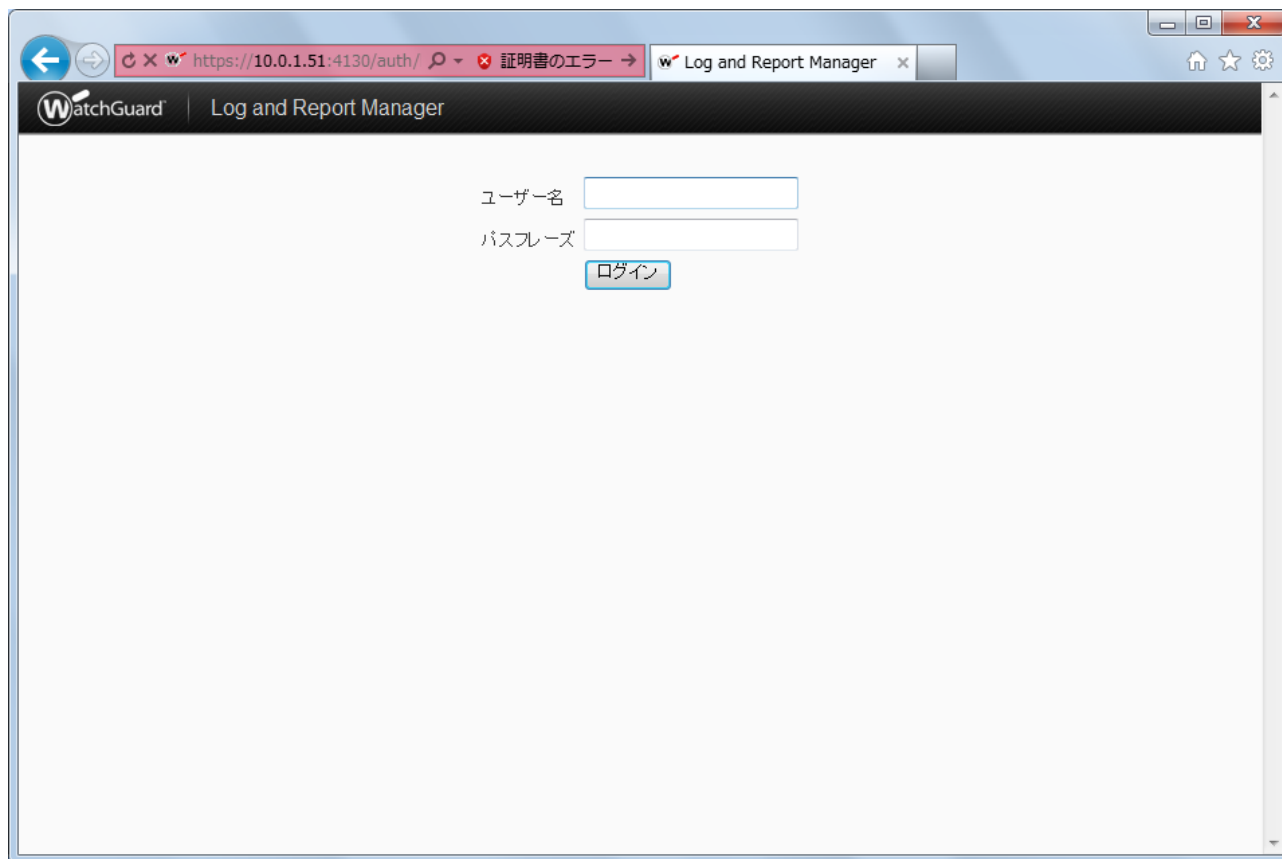
## ログおよびレポートの表示方法

WSM11.6.からは、ログもレポートも Web ブラウザで閲覧できるようになりました。

### アクセス方法

ウェブブラウザから、<https://レポートサーバーの IP アドレス:4130/> でアクセスします。

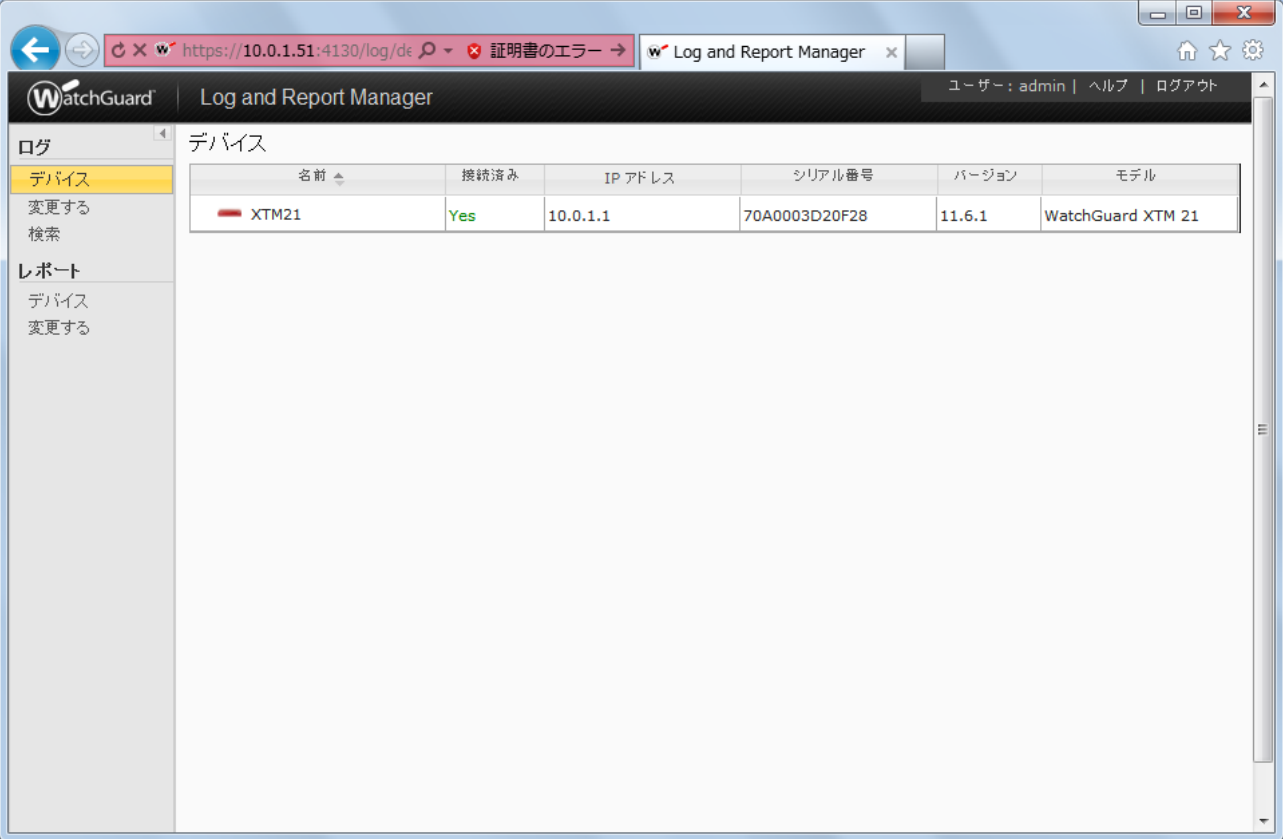
証明書の警告が出てでも続行します。するとレポートサーバーのログイン画面が表示されます。委託



WSC の管理者アカウントでログインします。

ユーザー名	<input type="text" value="admin"/>
パスワード	<input type="password" value="●●●●●●"/>
	<input type="button" value="ログイン"/>

ログ&レポートサーバーに接続しているデバイスの一覧が表示されます。



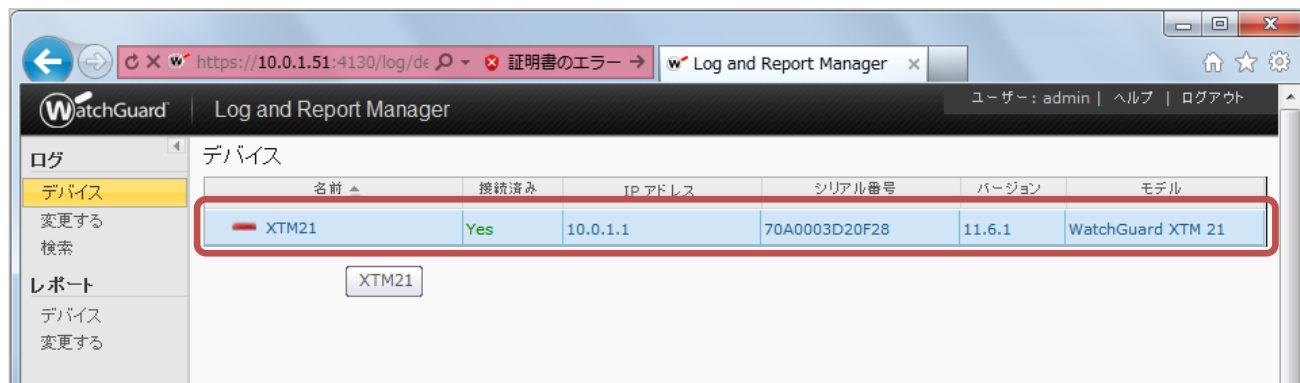
The screenshot shows the WatchGuard Log and Report Manager web interface. The browser address bar displays `https://10.0.1.51:4130/log/de` with a warning icon and the text "証明書のエラー" (Certificate Error). The page title is "Log and Report Manager" and the user is logged in as "admin". The left sidebar contains a "ログ" (Log) section with a "デバイス" (Device) link highlighted, and a "レポート" (Report) section with "デバイス" and "変更する" (Change) links. The main content area is titled "デバイス" and displays a table of connected devices.

名前	接続済み	IP アドレス	シリアル番号	バージョン	モデル
XTM21	Yes	10.0.1.1	70A0003D20F28	11.6.1	WatchGuard XTM 21

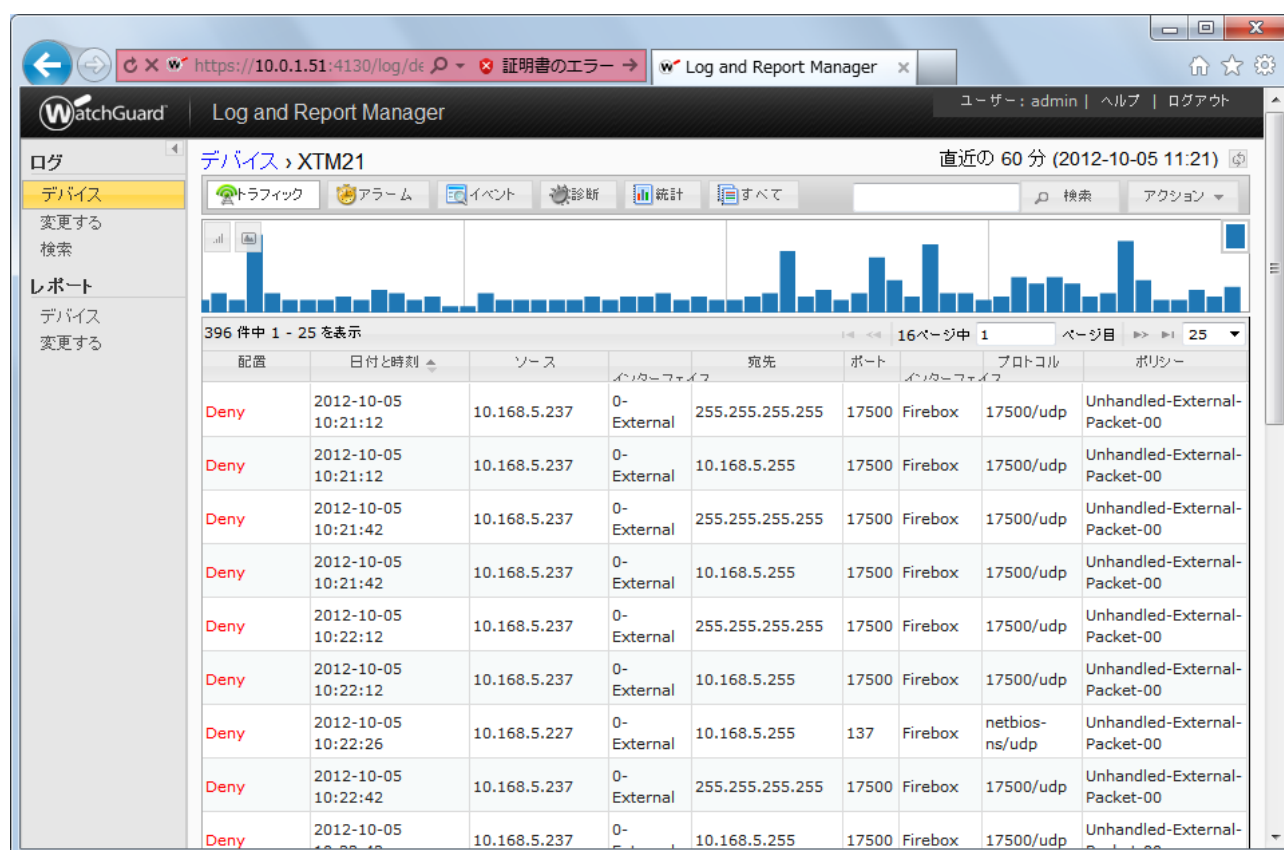
## ログの表示

### ログの閲覧

ログを見たいデバイスをクリックします。



すると直近の 60 分のログが表示されます。



検索機能を使用すると、ログの検索や絞り込みができます。



検索結果から、さらに時間の範囲やログの種類、検索語一致条件も指定できます。

The screenshot shows the 'Log and Report Manager' interface with the search results for 'HTTP'. The breadcrumb is '検索 > XTM21'. The search criteria are highlighted with a red box: '時間範囲' (Time Range) is set to '過去1時間' (Last 1 hour), 'ログの種類' (Log Type) is set to 'トラフィック' (Traffic), and the search term is 'HTTP'. Below the search criteria are buttons for '+ または' (Add or), '検索' (Search), '読み込み' (Load), and '保存' (Save). The search results show 79 records. The first record is highlighted.

検索完了: 79 レコード    エクスポート    クリア

日付と時刻	メッセージ
2012-10-05 10:54:53	ProxyMatch, ProxyStrip: <b>HTTP</b> Header match, pri=6, disp=Allow, policy=HTTP-proxy-00, protocol=http/tcp, src_ip=10.0.1.51, src_port=6689, dst_ip=173.194.38.104, dst_port=80, src_intf=0-Local-Net, dst_intf=0-External, rc=592, proxy_act=HTTP-Client.2, header=X-Content-Type-Options: nosniff\x0d\x0a, rule_name=Default
2012-10-05 10:54:53	ProxyMatch, ProxyStrip: <b>HTTP</b> Header match, pri=6, disp=Allow, policy=HTTP-proxy-00, protocol=http/tcp, src_ip=10.0.1.51, src_port=6689, dst_ip=173.194.38.104, dst_port=80, src_intf=0-Local-Net, dst_intf=0-External, rc=592, proxy_act=HTTP-Client.2, header=X-XSS-Protection: 1; mode=block\x0d\x0a, rule_name=Default
2012-10-05 10:54:53	ProxyMatch, ProxyStrip: <b>HTTP</b> Header match, pri=6, disp=Allow, policy=HTTP-proxy-00, protocol=http/tcp, src_ip=10.0.1.51, src_port=6689, dst_ip=173.194.38.104, dst_port=80, src_intf=0-Local-Net, dst_intf=0-External, rc=592, proxy_act=HTTP-Client.2, header=X-Frame-Options: SAMEORIGIN\x0d\x0a, rule_name=Default
2012-10-05	ProxyMatch, ProxyStrip: <b>HTTP</b> Header match, pri=6, disp=Allow, policy=HTTP-proxy-00, protocol=http/tcp, src_ip=10.0.1.51, src_port=6690, dst_ip=74.125.235.133, dst_port=80, src_intf=0-Local-Net, dst_intf=0-External



## ログのダウンロード

検索ボタンの右横に「アクション」のダイアログボックスがあり、ここからログ表示の期間指定やログのエクスポートができます。CSV 形式でエクスポートされます。

The screenshot shows the 'Log and Report Manager' interface. At the top, it says 'Log and Report Manager' and 'ユーザー: admin | ヘルプ | ログアウト'. Below that, it says 'デバイス > XTM21' and '直近の 60 分 (2012-10-05 11:21)'. There are several tabs: 'トラフィック', 'アラーム', 'イベント', '診断', '統計', 'すべて'. A search bar is on the right. Below the tabs is a bar chart showing traffic over time. Below the chart is a table with 396 items, showing 1 to 25. The table has columns: '配置', '日付と時刻', 'ソース', '宛先', 'ポート', 'プロトコル', 'アクション'. The 'アクション' column is highlighted. A red box highlights the 'アクション' menu, which includes options like 'Date-Time Filter', '過去30分', '過去1時間', '直近の 6 時間', '直近の 12 時間', '直近の 24 時間', '直近の 48 時間', '過去1週間', 'カスタム時間範囲', 'タイムスライスの分析', and 'ログのエクスポート (.csv)'.

配置	日付と時刻	ソース	宛先	ポート	プロトコル	アクション
Deny	2012-10-05 10:21:12	10.168.5.237	0-External	255.255.255.255	17500	Firebox
Deny	2012-10-05 10:21:12	10.168.5.237	0-External	10.168.5.255	17500	Firebox
Deny	2012-10-05 10:21:42	10.168.5.237	0-External	255.255.255.255	17500	Firebox
Deny	2012-10-05 10:21:42	10.168.5.237	0-External	10.168.5.255	17500	Firebox
Deny	2012-10-05 10:22:12	10.168.5.237	0-External	255.255.255.255	17500	Firebox
Deny	2012-10-05 10:22:12	10.168.5.237	0-External	10.168.5.255	17500	Firebox

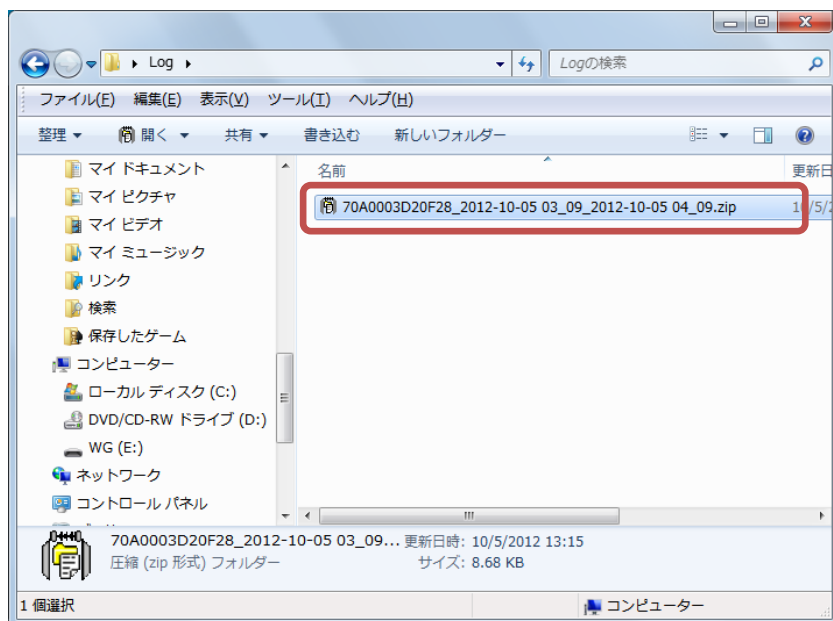
アクションのメニューからログのエクスポートをクリックします。

This screenshot is a zoomed-in view of the 'アクション' (Action) menu. It shows options like 'Date-Time Filter', '過去30分', '過去1時間', '直近の 6 時間', '直近の 12 時間', '直近の 24 時間', '直近の 48 時間', '過去1週間', 'カスタム時間範囲', 'タイムスライスの分析', and 'ログのエクスポート (.csv)'. The 'ログのエクスポート (.csv)' option is highlighted with a red box.

保存します。

The screenshot shows a file save dialog box. It says '次のファイルを開こうとしています:' (Attempting to open the following file:). The file name is '70A0003D20F28\_2012-10-08 23\_47\_2012-10-09 00\_47.zip ...'. The file type is 'ZIP ファイル (17.2 KB)' and the location is 'https://10.0.1.51:4130'. Below this, it asks 'このファイルをどのように処理するか選んでください' (Please select how to handle this file). There are two radio buttons: 'プログラムで開く (O):' (Open with program) and 'ファイルを保存する (S):' (Save file). The 'ファイルを保存する (S):' option is selected and highlighted with a red box. There is also a checkbox for '今後この種類のファイルは同様に処理する (A)' (Treat files of this type the same way in the future). At the bottom are 'OK' and 'キャンセル' (Cancel) buttons.

ZIP 形式で保存されます。



ZIP を展開し、エクセルやテキストエディタで開くことができます。

A screenshot of a Microsoft Excel spreadsheet titled 'cluster\_traffic\_20121005\_030900\_20121005\_040900.csv [Read-Only] - Microsoft Excel'. The spreadsheet displays network traffic data with columns for 'sid', 'cluster', 'sn', 'tag\_id', 'raw\_id', 'disp', 'direction', 'pri', 'policy', 'protocol', 'src\_ip', and 'src\_port'. The data is organized into rows, with the first row (row 1) containing headers and subsequent rows (rows 2-24) containing specific traffic records. The 'sid' column is highlighted in blue. The status bar at the bottom shows 'Ready' and '100%' zoom level.

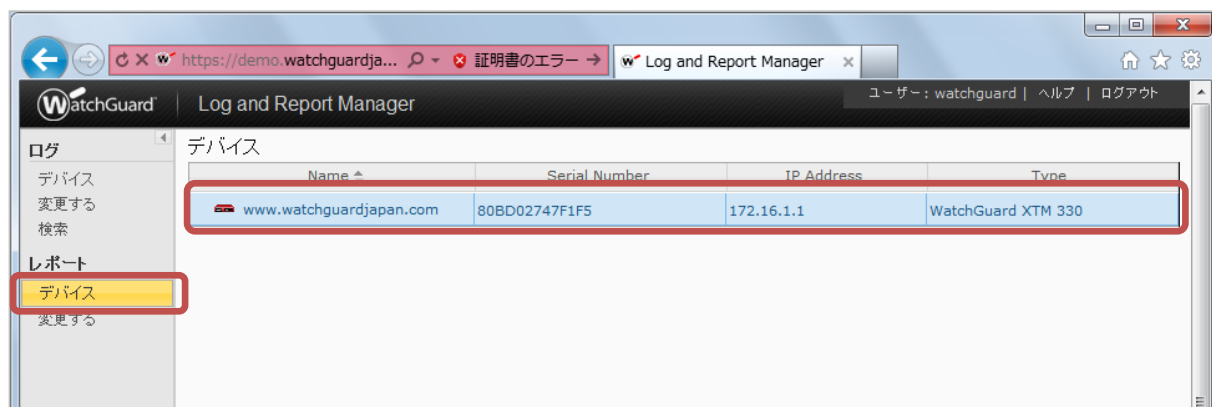
	A	B	C	D	E	F	G	H	I	J	K	L
	sid	cluster	sn	tag_id	raw_id	disp	direction	pri	policy	protocol	src_ip	src_port
2	2319		70A0003D20F28	1001	740	2	0	4	Unhandled-External-Packet-00	netbios-dgm/udp	10.168.5.227	108
3	2322		70A0003D20F28	1006	743	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
4	2321		70A0003D20F28	1006	742	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
5	2320		70A0003D20F28	1006	741	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
6	2328		70A0003D20F28	1006	769	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
7	2327		70A0003D20F28	1006	768	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
8	2326		70A0003D20F28	1006	767	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
9	2325		70A0003D20F28	1006	766	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
10	2341		70A0003D20F28	1001	816	2	0	4	Unhandled-External-Packet-00	netbios-ns/udp	10.168.5.242	108
11	2340		70A0003D20F28	1001	815	2	0	4	Unhandled-External-Packet-00	netbios-ns/udp	10.168.5.254	108
12	2343		70A0003D20F28	1001	824	2	0	4	Unhandled-External-Packet-00	bootps/udp	0.0.0.0	108
13	2342		70A0003D20F28	1001	823	2	0	4	Unhandled-External-Packet-00	bootps/udp	0.0.0.0	108
14	2344		70A0003D20F28	1001	825	2	0	4	Unhandled-External-Packet-00	netbios-ns/udp	10.168.5.246	108
15	2345		70A0003D20F28	1001	826	2	0	4	Unhandled-External-Packet-00	netbios-dgm/udp	10.168.5.246	108
16	2347		70A0003D20F28	1001	829	2	0	4	Unhandled-External-Packet-00	netbios-ns/udp	10.168.5.246	108
17	2346		70A0003D20F28	1001	828	2	0	4	Unhandled-External-Packet-00	netbios-dgm/udp	10.168.5.246	108
18	2354		70A0003D20F28	1006	855	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
19	2353		70A0003D20F28	1006	854	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
20	2352		70A0003D20F28	1006	853	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
21	2351		70A0003D20F28	1006	852	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
22	2350		70A0003D20F28	1006	851	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
23	2349		70A0003D20F28	1006	849	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108
24	2348		70A0003D20F28	1006	848	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	108

## レポートの表示

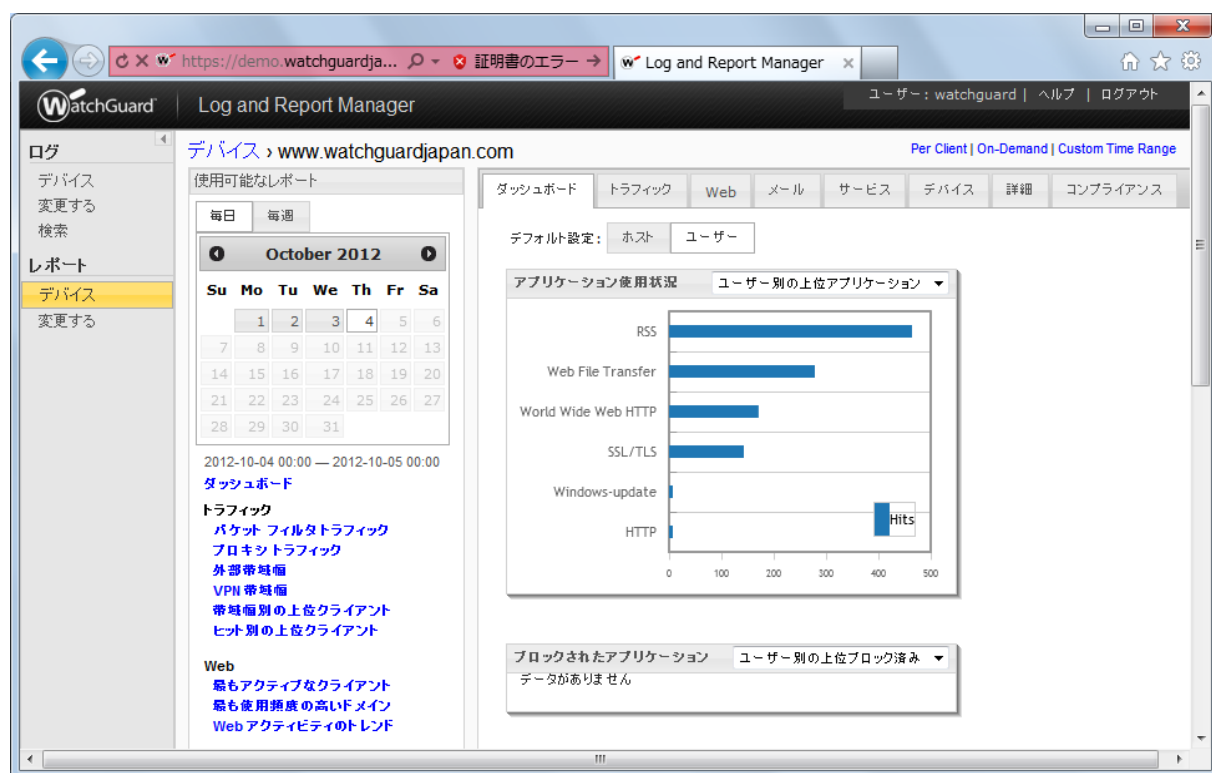
### レポートの閲覧

ログイン後、左側メニュー レポートの下「デバイス」のリンクをクリックします。

レポート表示可能なデバイスの一覧が表示されますので、これをクリックします。<sup>1</sup>



最初にダッシュボードの表示になります。代表的なレポート項目のサマリーが表示されます。



<sup>1</sup> レポートデータが生成されないと表示されません。表示されない場合は、スケジュールの頻度にもよりますが、時間を置いて(1日1回であれば翌日)再度表示してみてください。

カレンダーの「毎日」「毎週」タブを選択し、デイリーレポートもしくはウィークリーレポートを切り替えます。  
また、カレンダー下の各リンクから、閲覧したいレポートをクリックします。

Log and Report Manager

デバイス > www.watchguardjapan

使用可能なレポート

毎日 毎週

October 2012

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

2012-10-04 00:00 — 2012-10-05 00:00

[ダッシュボード](#)

**トラフィック**

- [バケット フィルタトラフィック](#)
- [プロキシトラフィック](#)

**外部帯域幅**

- [VPN 帯域幅](#)
- [帯域幅別の上位クライアント](#)
- [ヒット別の上位クライアント](#)

**Web**

- [最もアクティブなクライアント](#)
- [最も使用頻度の高いドメイン](#)
- [Web アクティビティのトレンド](#)

**メール**

- [SMTP プロキシ](#)

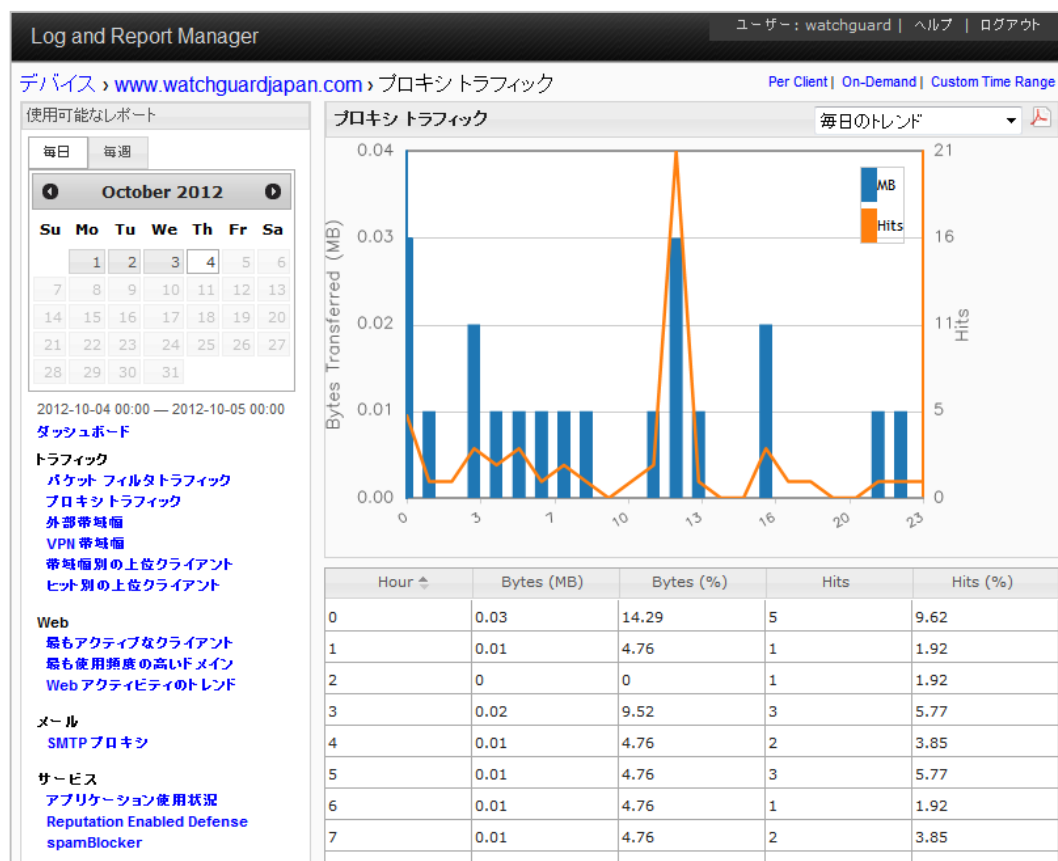
**サービス**

- [アプリケーション使用状況](#)
- [Reputation Enabled Defense](#)
- [spamBlocker](#)

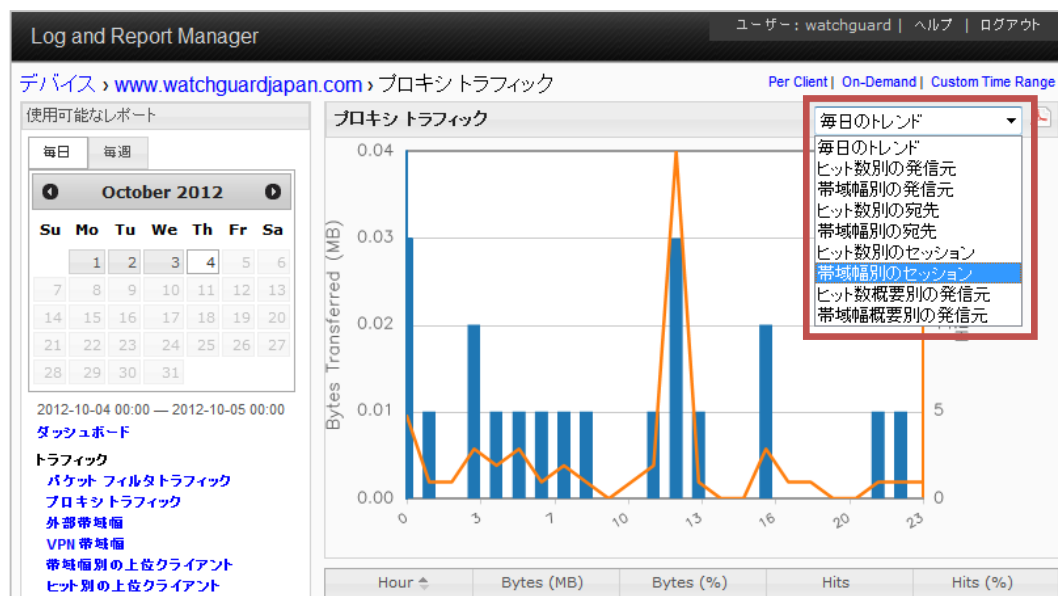
タブでデイリーレポートかウィークリーレポートかを切り替えます

表示したいレポートの種類を選択します

一例ですが、以下はデイリーの「プロキシトラフィック」を表示しています。

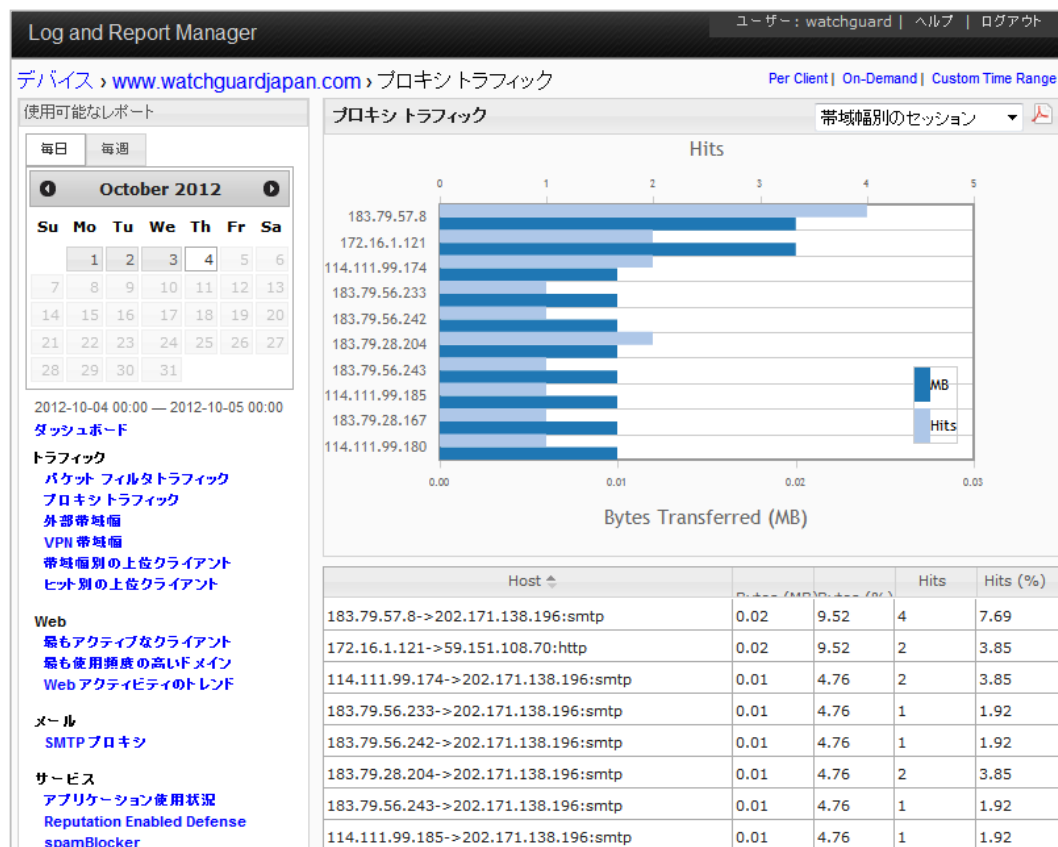


右上のドロップダウンリストから、同じレポートでも、分析する観点を変更することができます。



たとえば「帯域幅別のセッション」を選択します。

同じプロキシトラフィックのグラフですが、通信先による帯域幅別で表示されました。



## PDF レポートのダウンロード

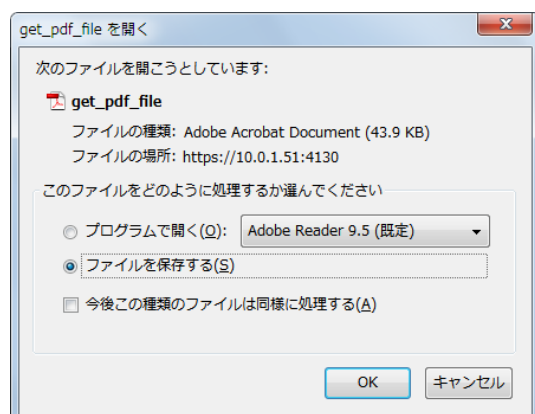
表示したレポートを PDF ファイルでダウンロードすることができます。

レポート画面の右上にある PDF アイコンをクリックします。

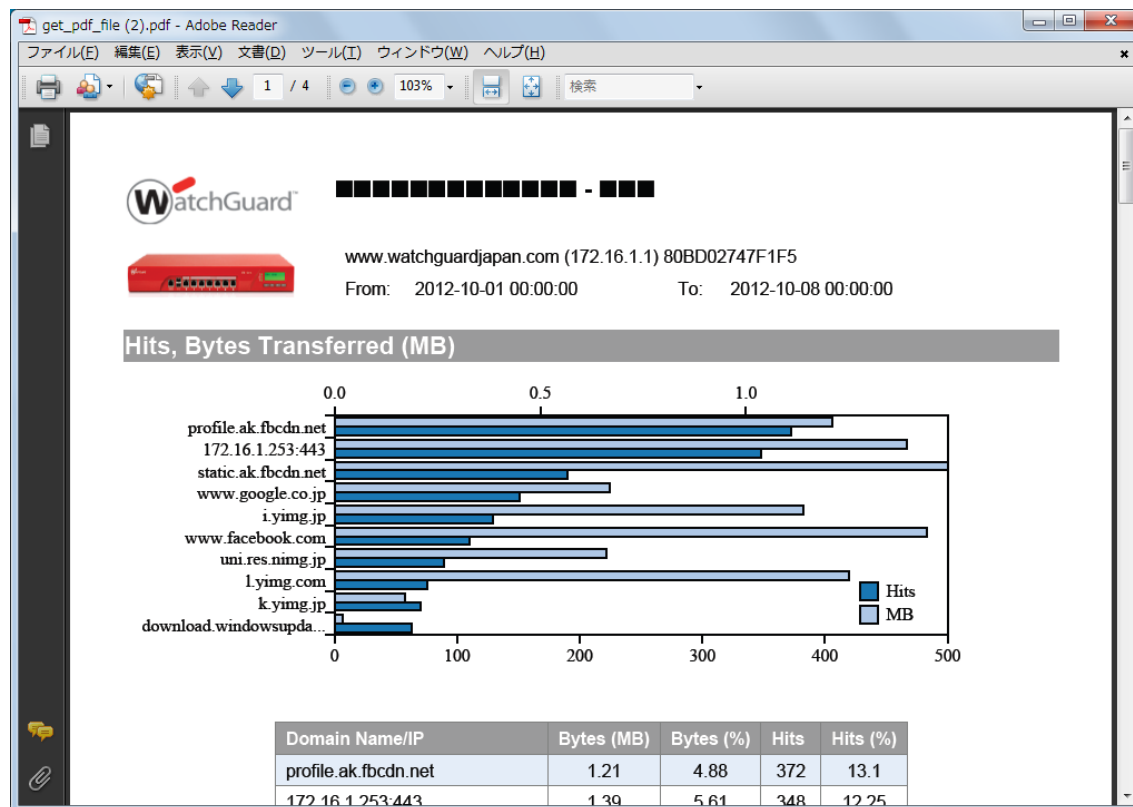


PDF のダウンロードのダイアログで保存か開くかを選択します。

(環境によってそのまま開く場合もあります)



PDF 形式でレポートを閲覧することができます。



WSM ログサーバー & レポートサーバーの設定は以上です。

このガイドを通して、ウォッチガードの提供するログ・レポートサーバーによってセキュリティの見える化がいか  
に容易に実現できるか、実感していただけたと思います。

ウォッチガードの製品が、御社のセキュリティ向上に貢献できれば幸いです。