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エアです。

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エアは、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エ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していただき、ご活用いただければ幸いです。

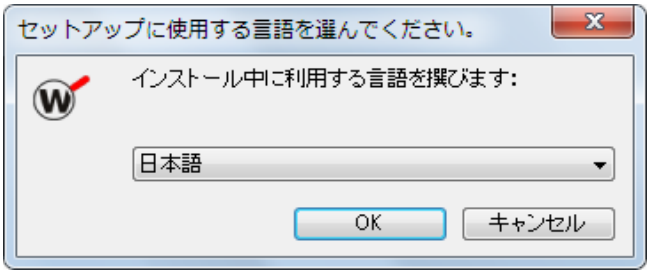
ログサーバーおよびレポートサーバーのインストール

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エアとして同時にインストールすることができます。

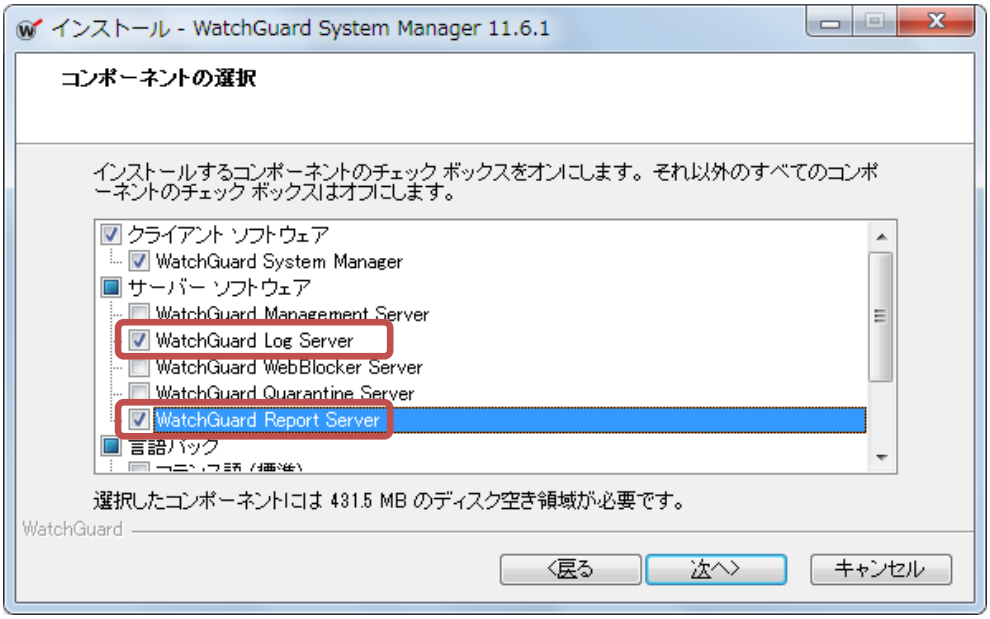
インストール後は WSC (WatchGuard Server Center)というサーバーソフトウエアの管理コンソールから設定することができます。

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。

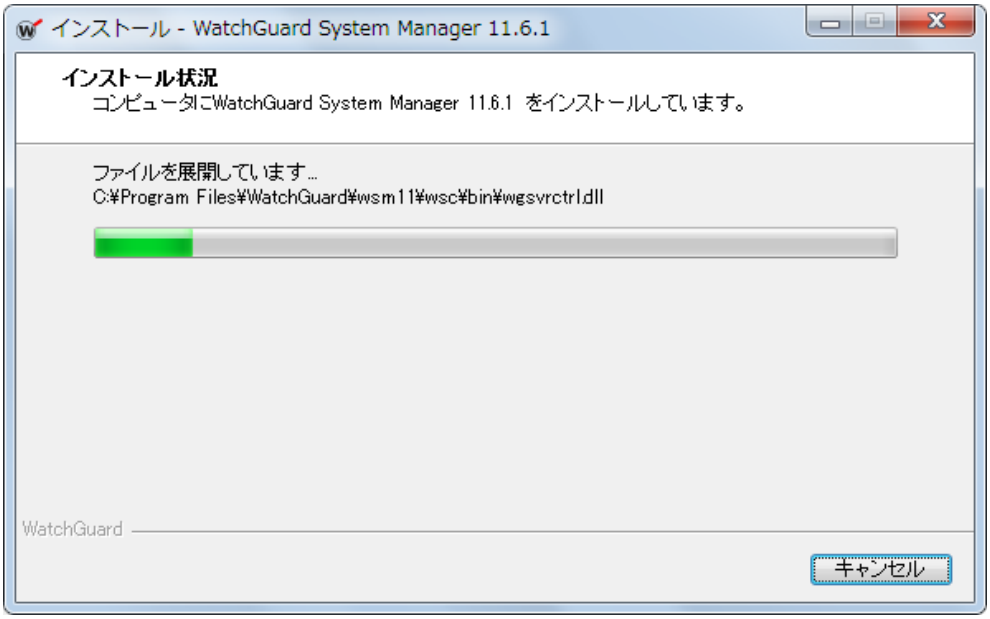


コンポーネントの選択でサーバーソフトウエアのツリーにある「Watchguard Log Server」と「Watchguard Report Server」にチェックを入れて次に進みます。



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。

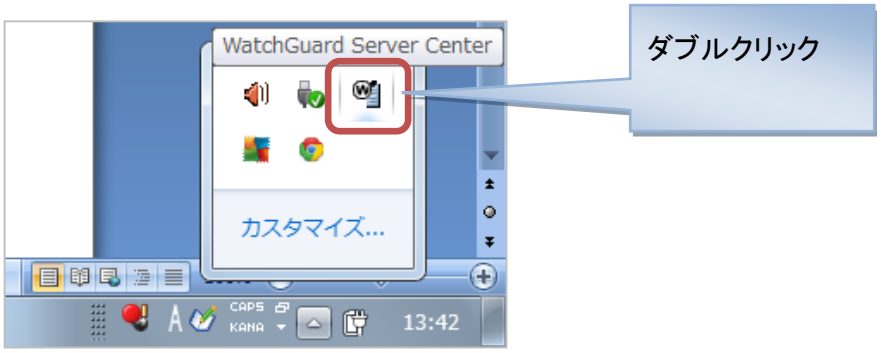
完了ボタンをクリックします。

インストールは以上です。

ログサーバーの構成

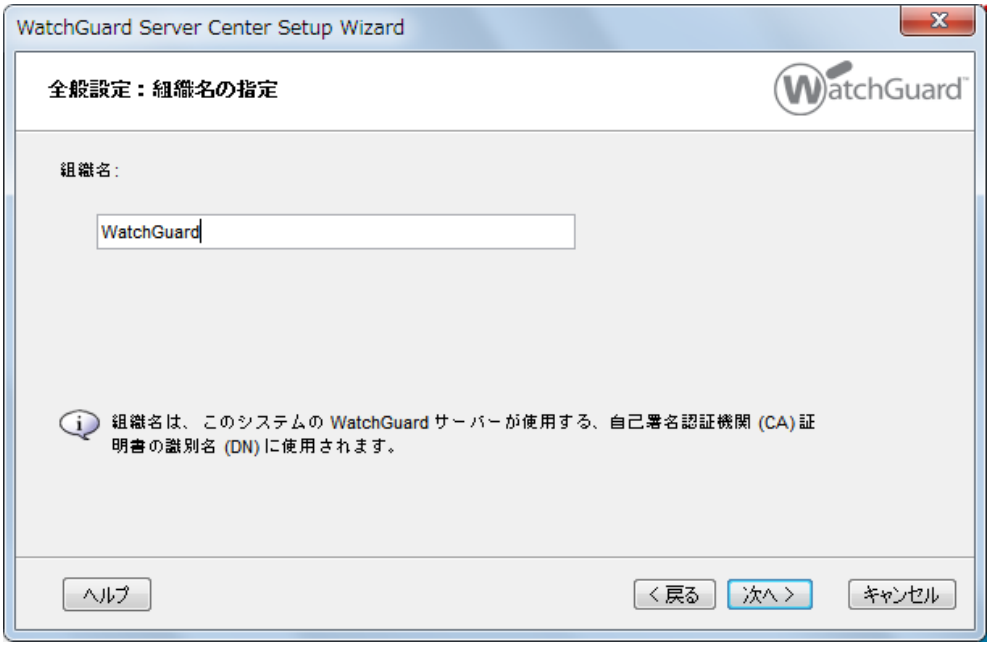
初期設定ウィザード

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

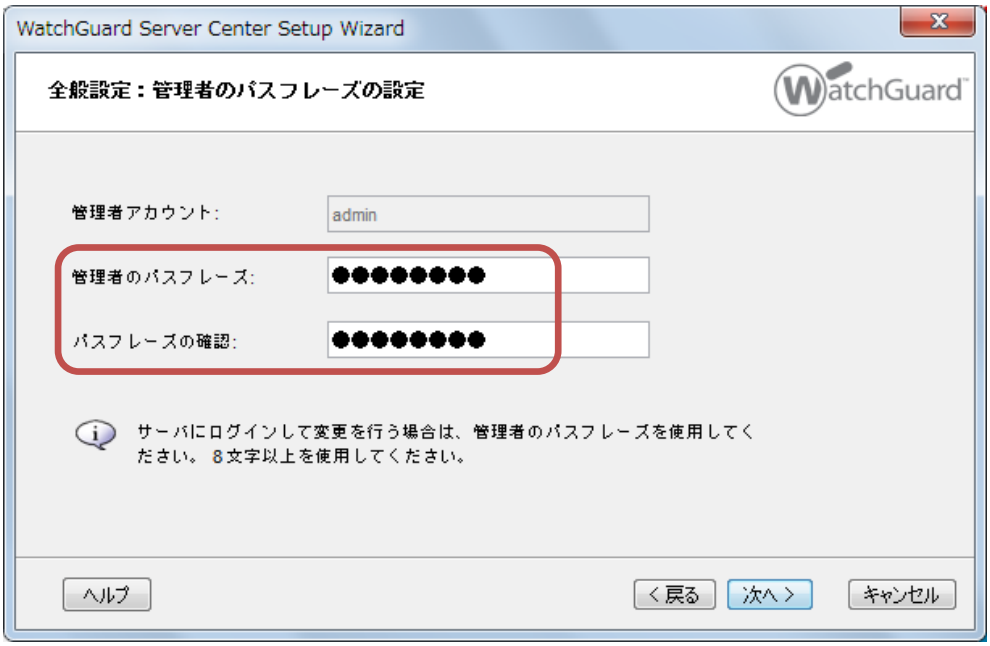


初回の起動なので、構成されていないサーバーの設定ウィザードが始まります。次へ。

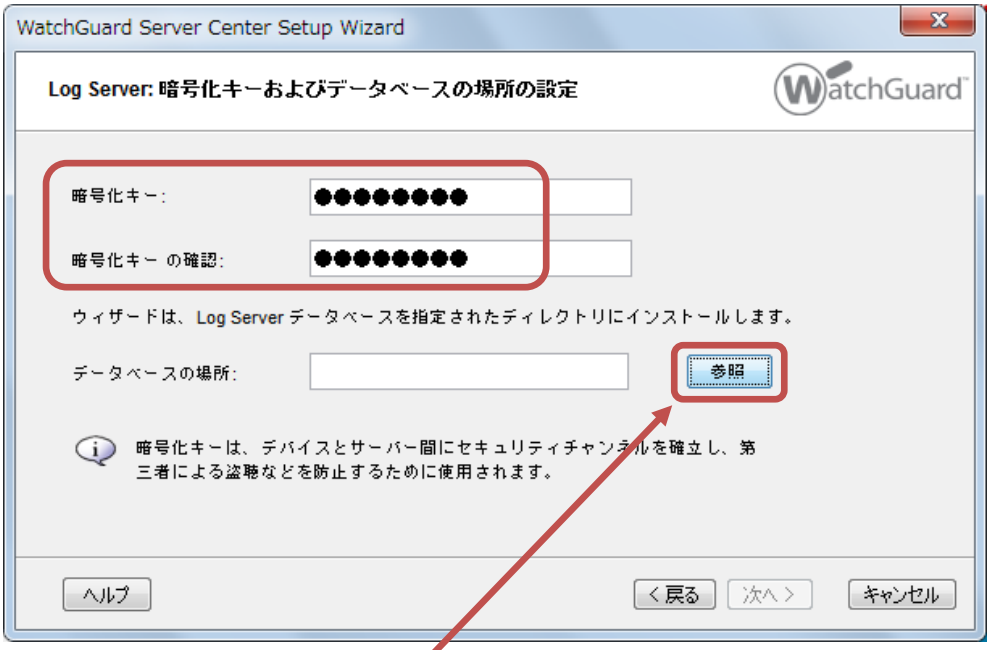
組織名を入力し、次へ。



管理者のパスフレーズを入力します。WSC を起動するときに入力するものです。

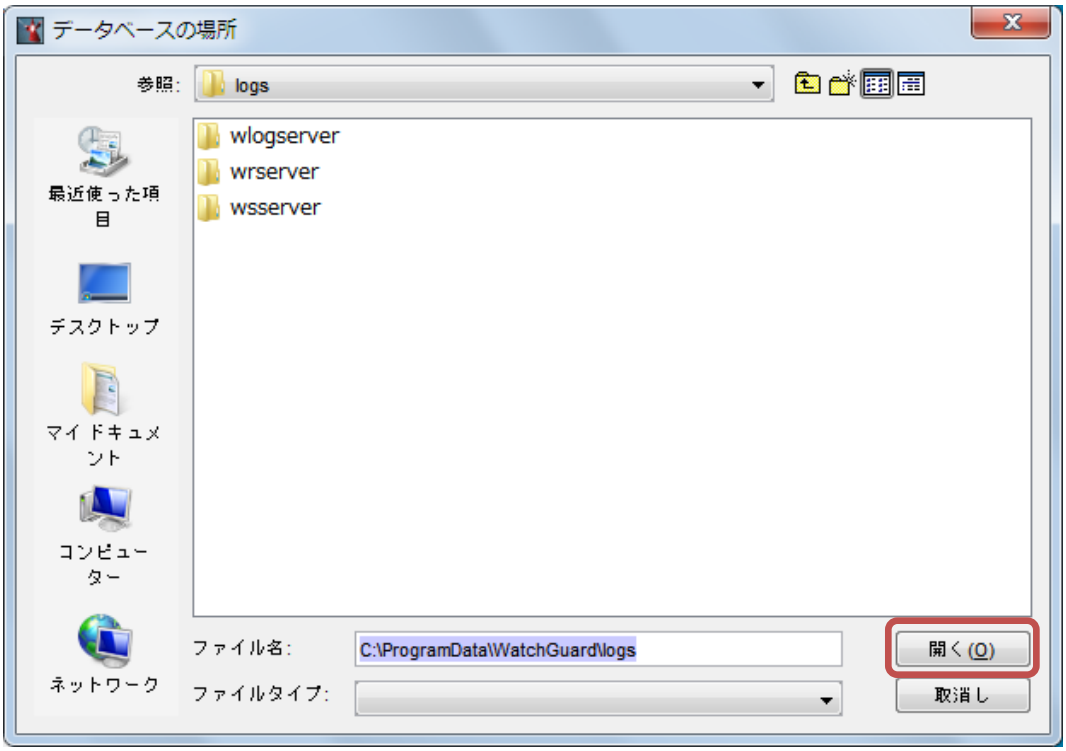


暗号化キーを入力します。これは XTM 側にログ送信の設定をする際に必要となります。

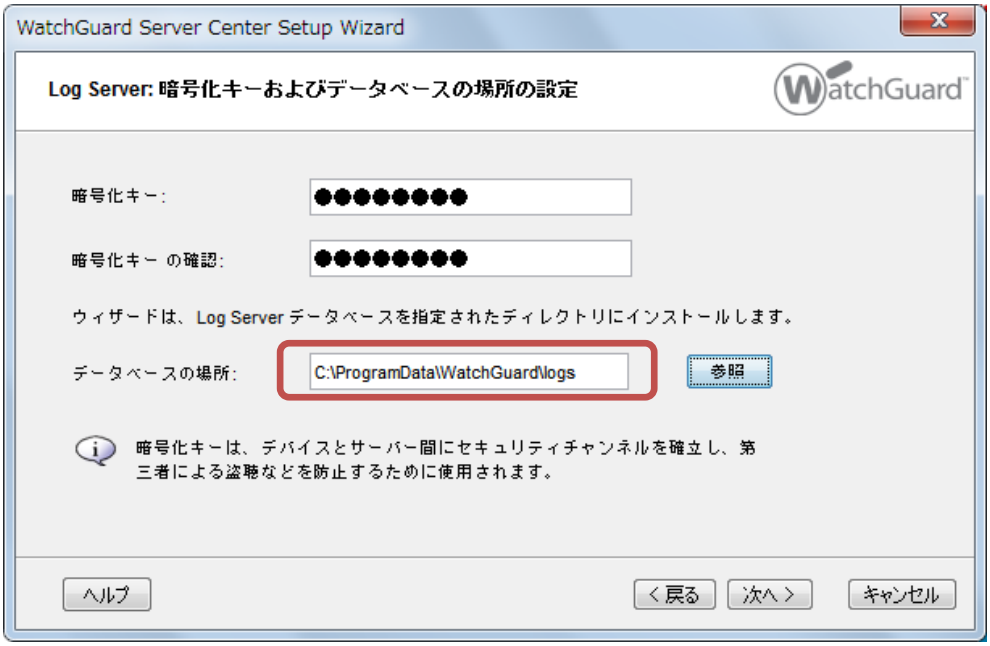


データベースの場所は参照ボタンをクリックします。

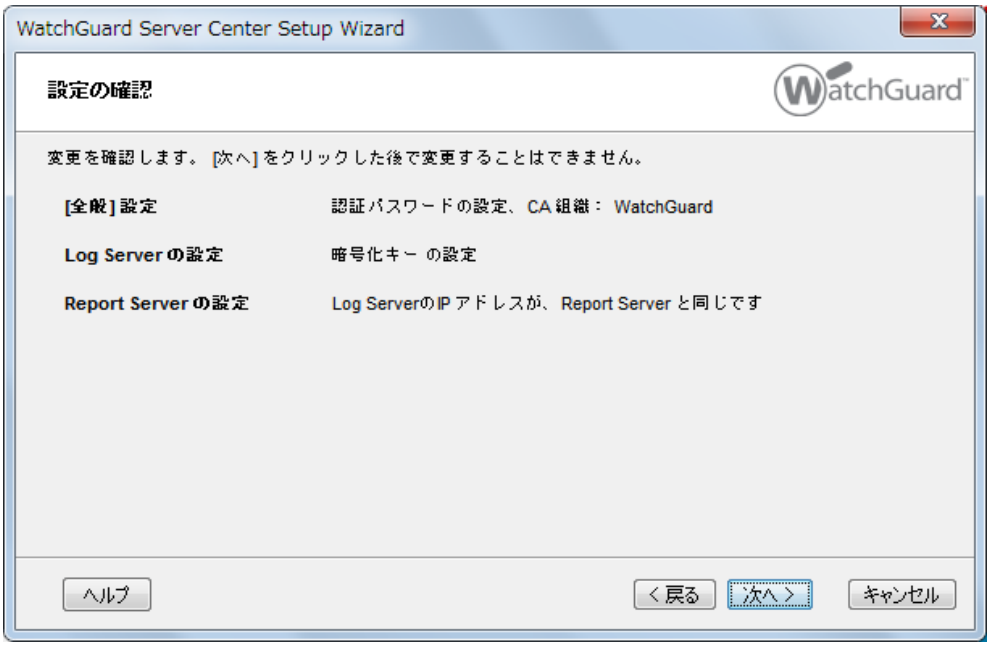
ログの場所は、特に決めてなければデフォルトの場所を、ログのために確保した領域があればそこを指定します。



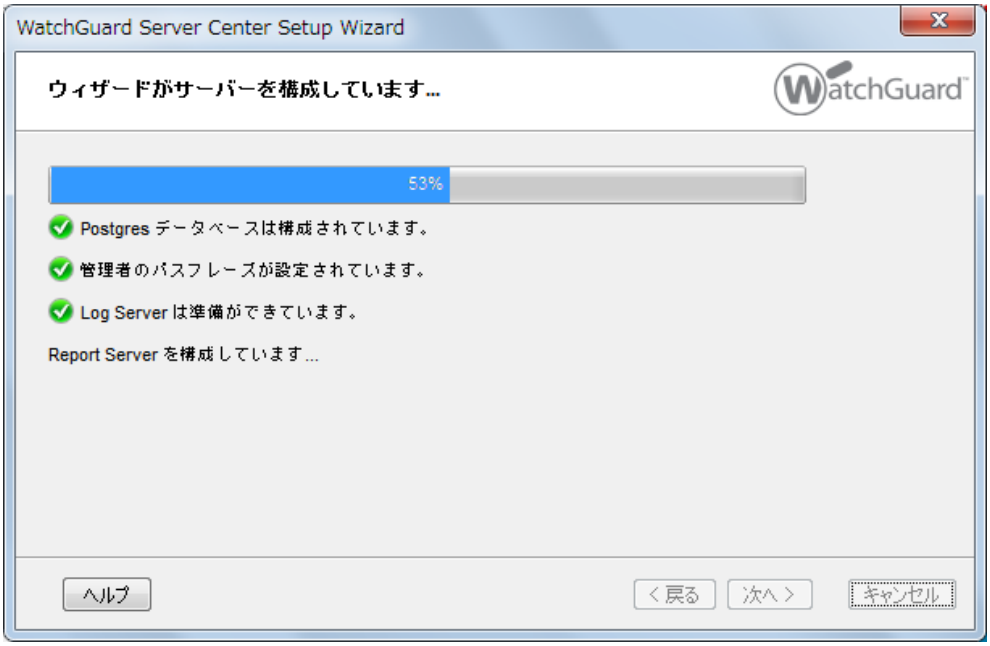
データベースの場所が入ったら次へ。



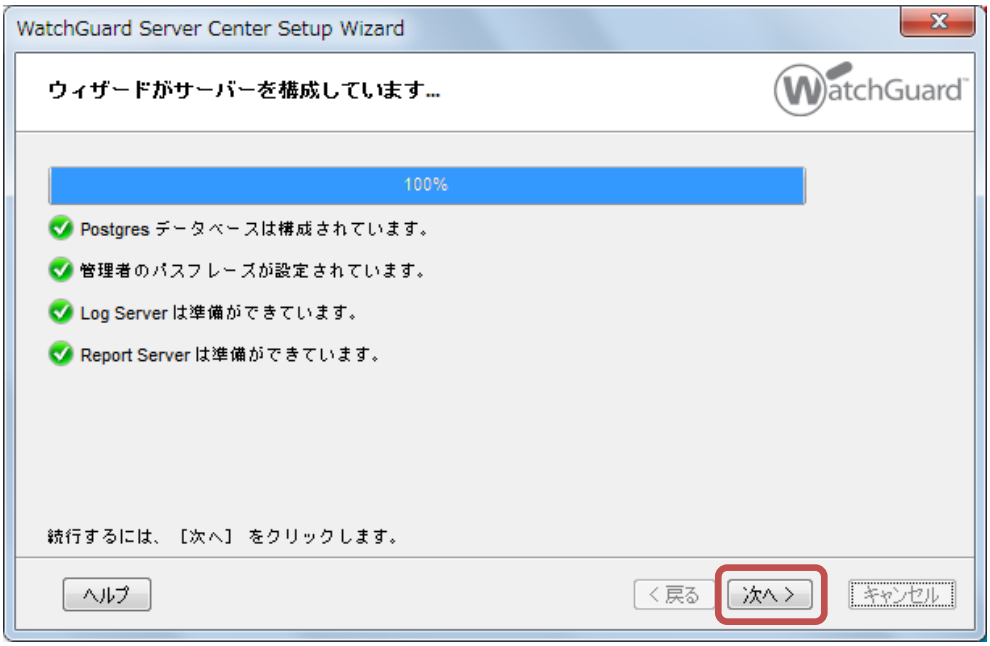
設定の確認をし、次へ。



設定が反映されます。



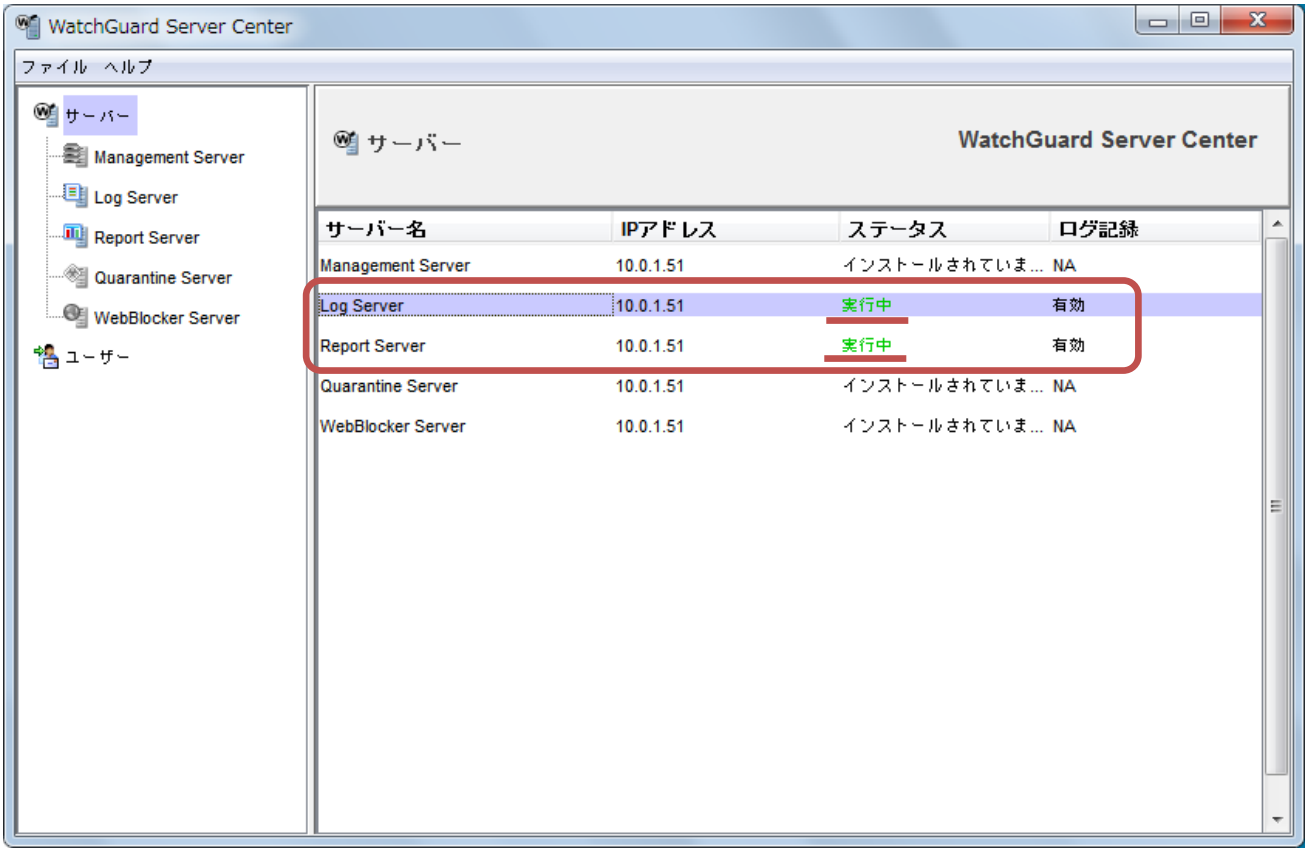
100%まで進んだら、次へ。



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。

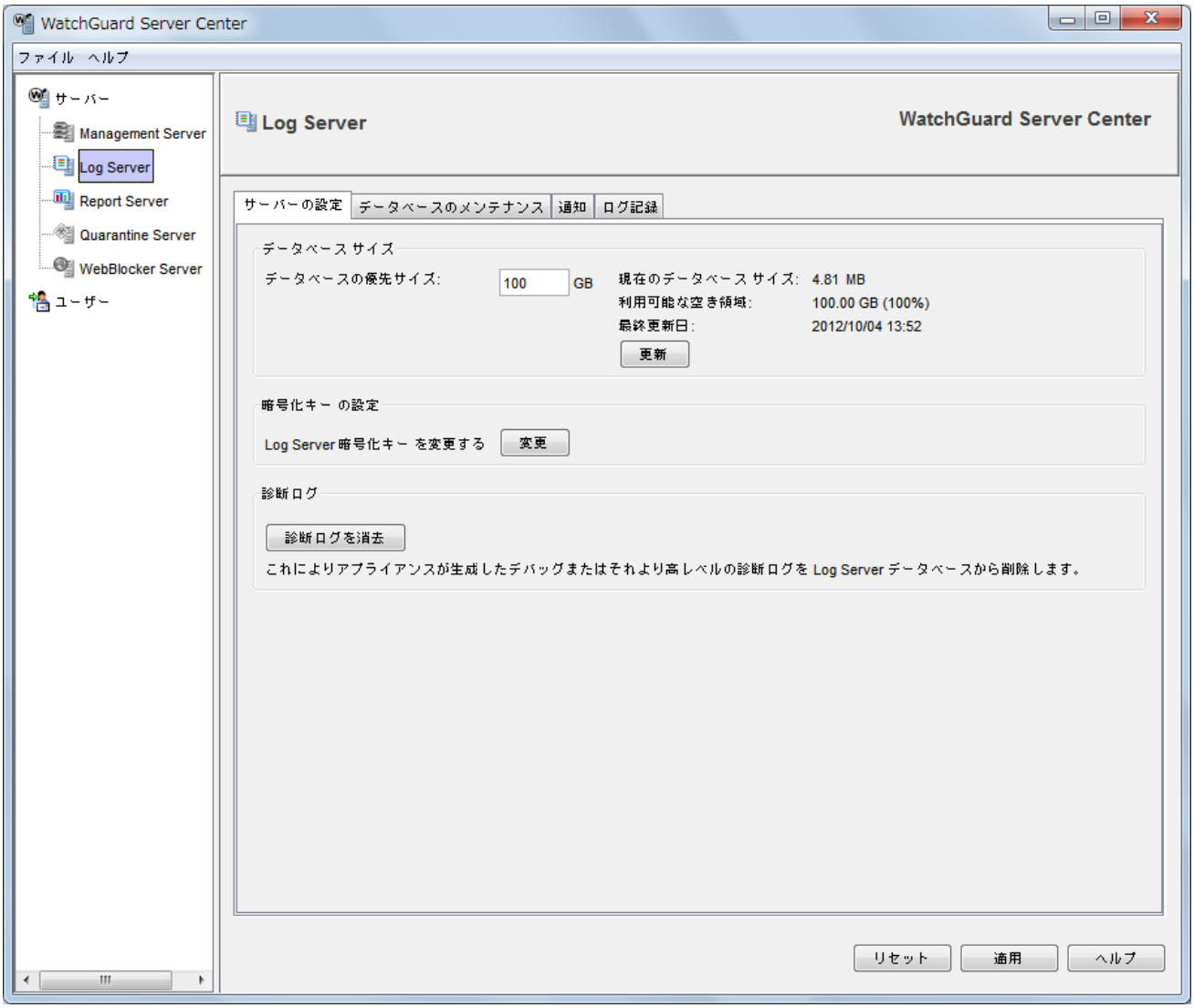
Log Server と Report Server が実行中であることを確認してください。



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。

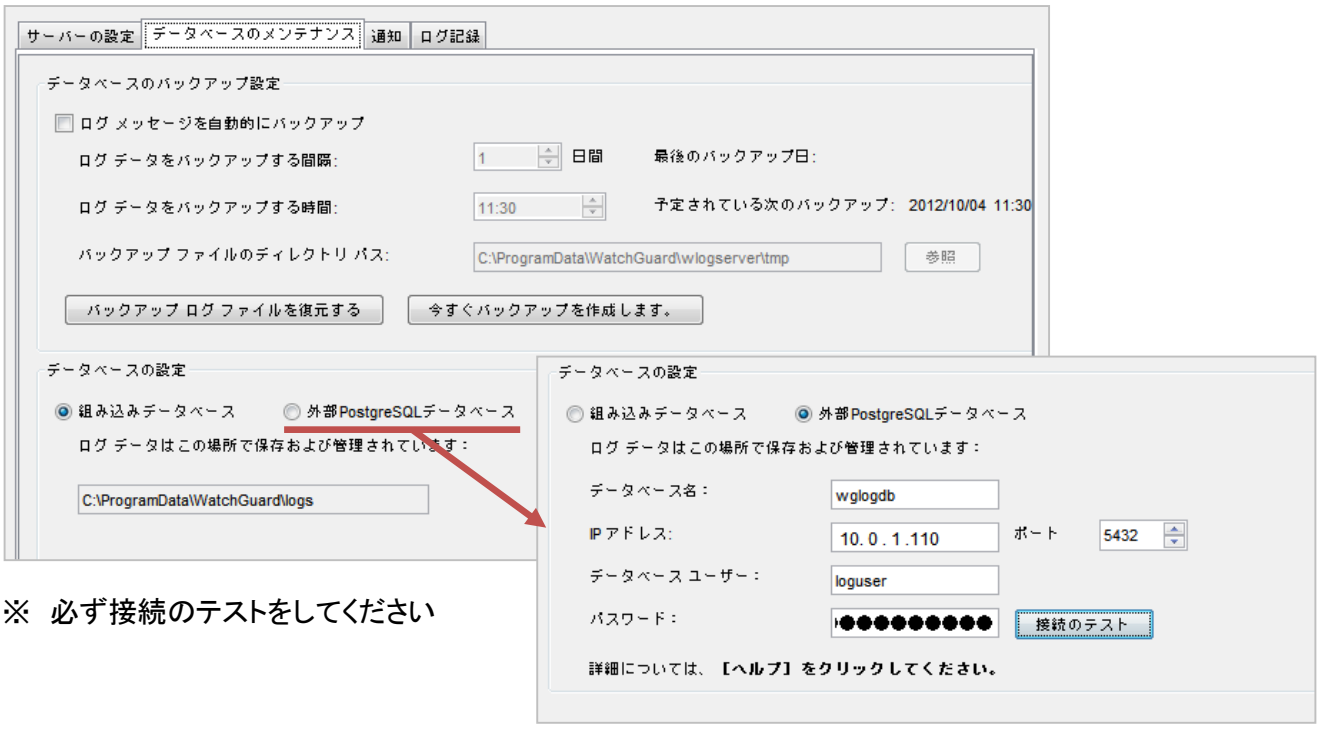
- サーバーの設定タブ

「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。

- 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。

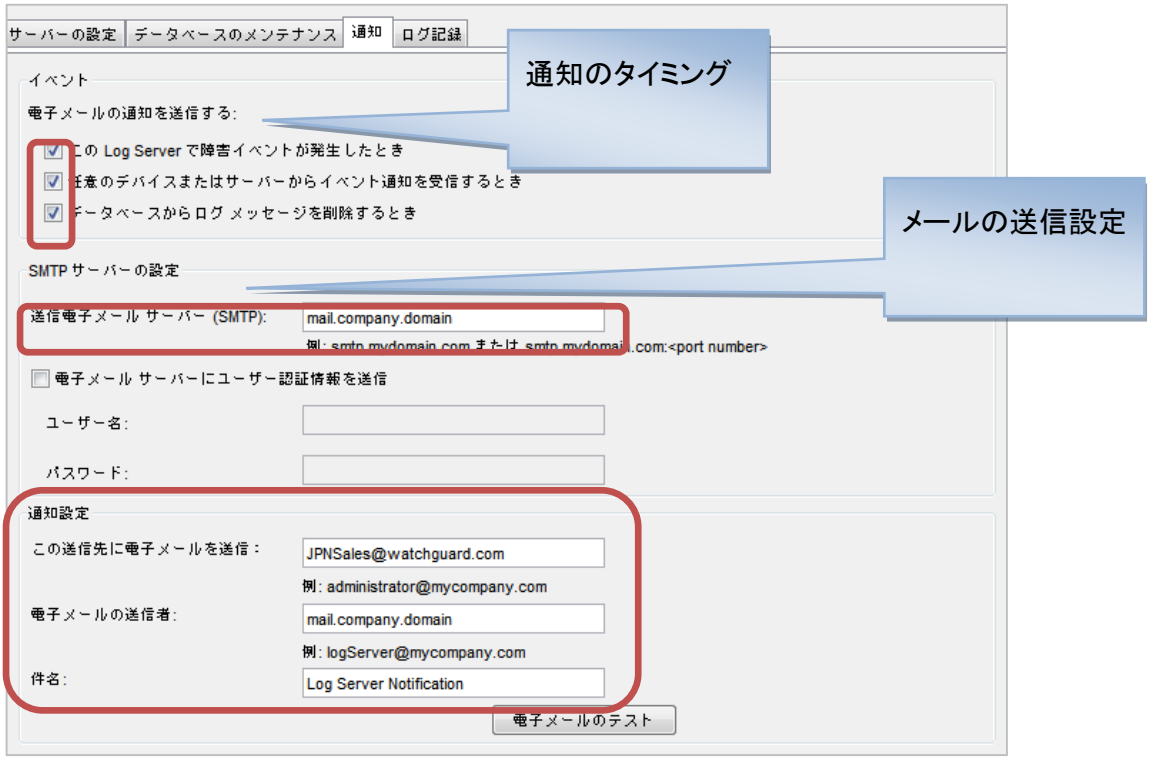
「データベースの設定」セクションでは、外部の PostgreSQL サーバーをログ DB として使いたい場合は、データベースの設定のセクションで指定できます。



※ 必ず接続のテストをしてください

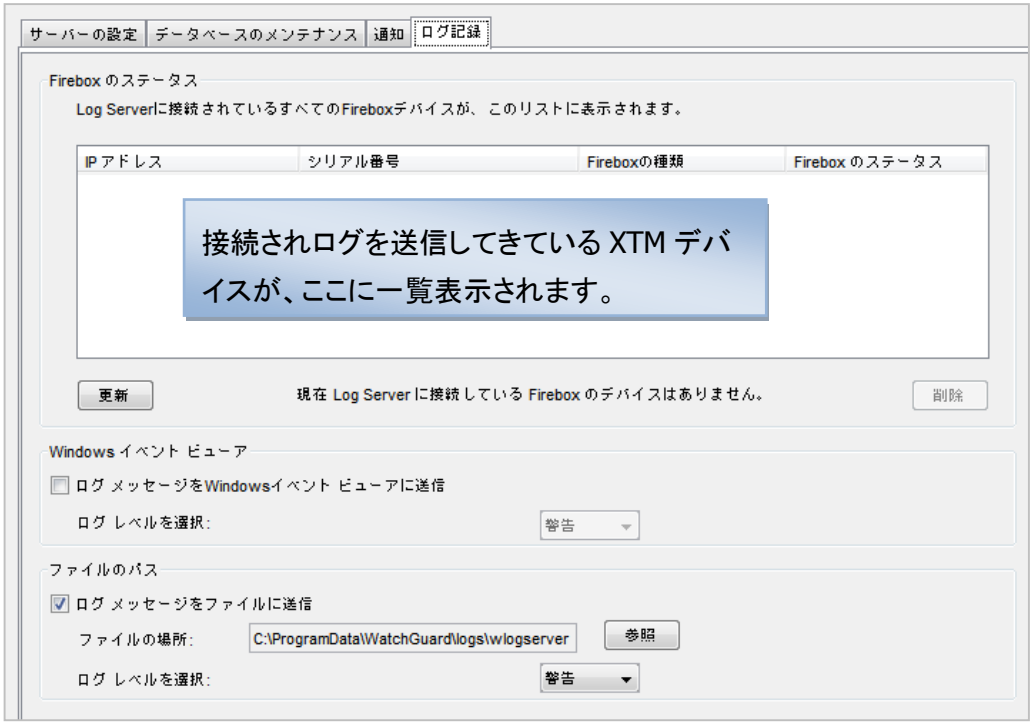
- 通知タブ

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。

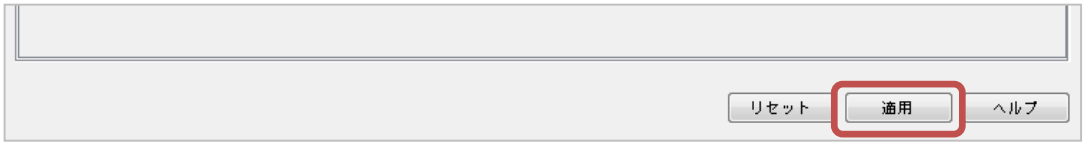


- ログ記録タブ

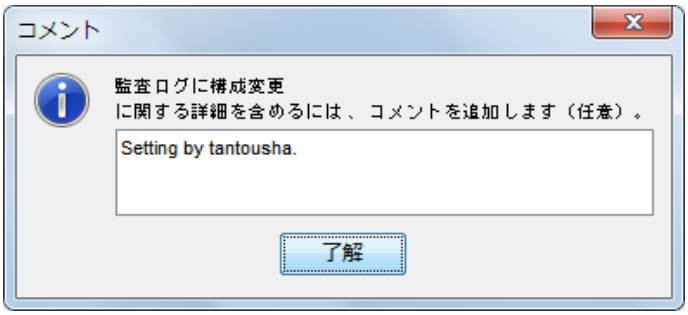
ログを送信してくる XTM デバイスが一覧に表示されます。後ほどデバイス側の設定で触れます。



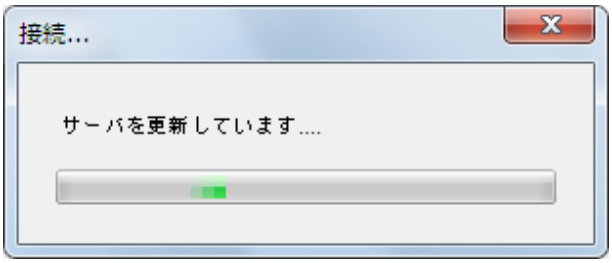
ログサーバーを一通り設定したら、左下にある適用ボタンをクリックします。



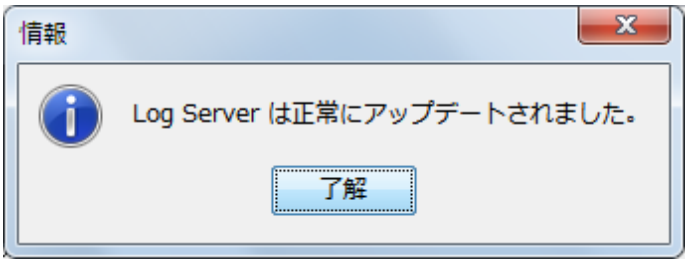
構成変更時にはコメントの入力が求められますので、入力して了解ボタンをクリックします。



サーバーが再起動されます。



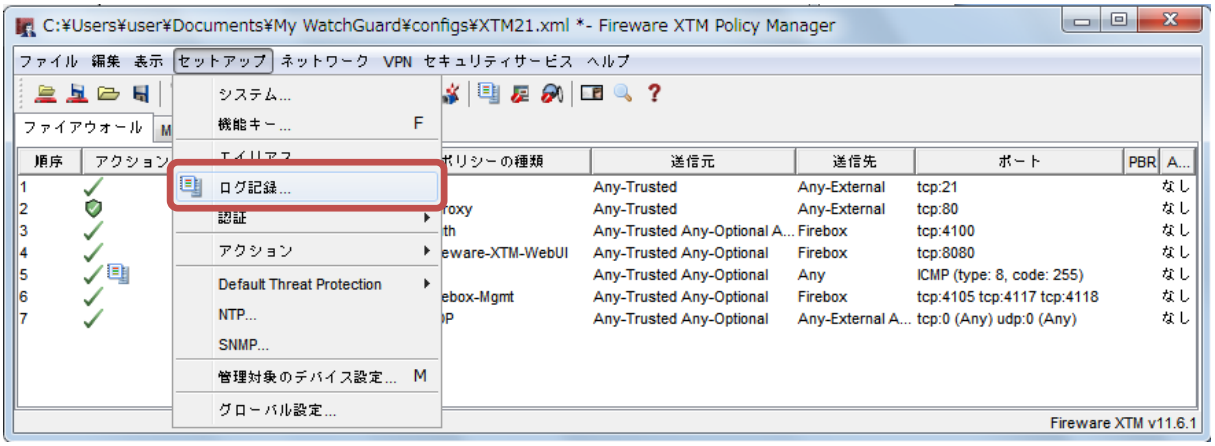
設定が反映されます。



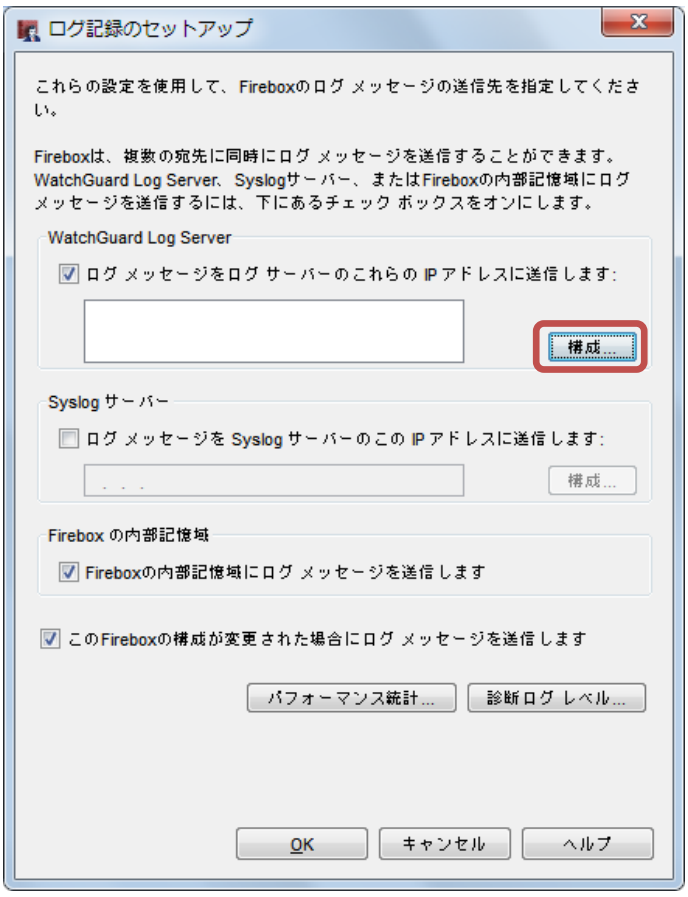
XTM 側のログ送信設定

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。

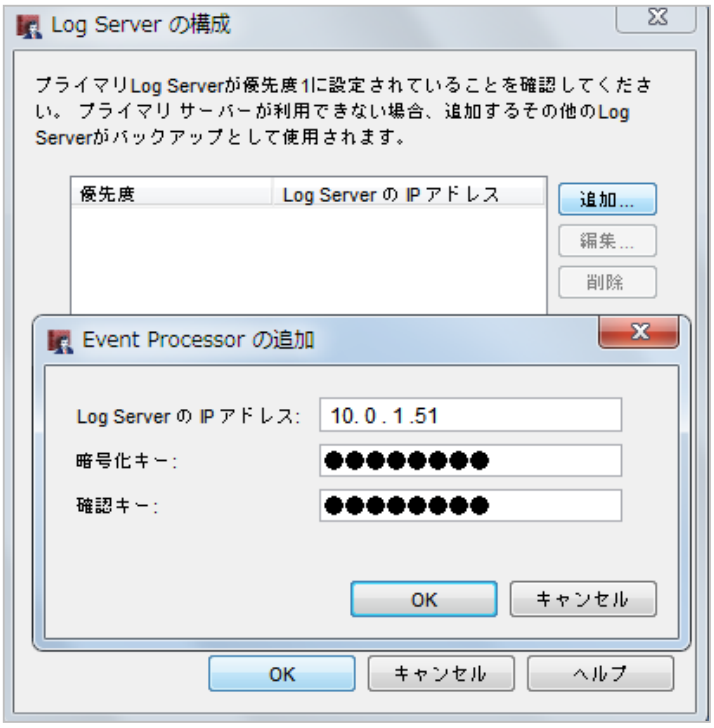


ログ記録のセットアップ画面で、構成ボタンをクリックします。

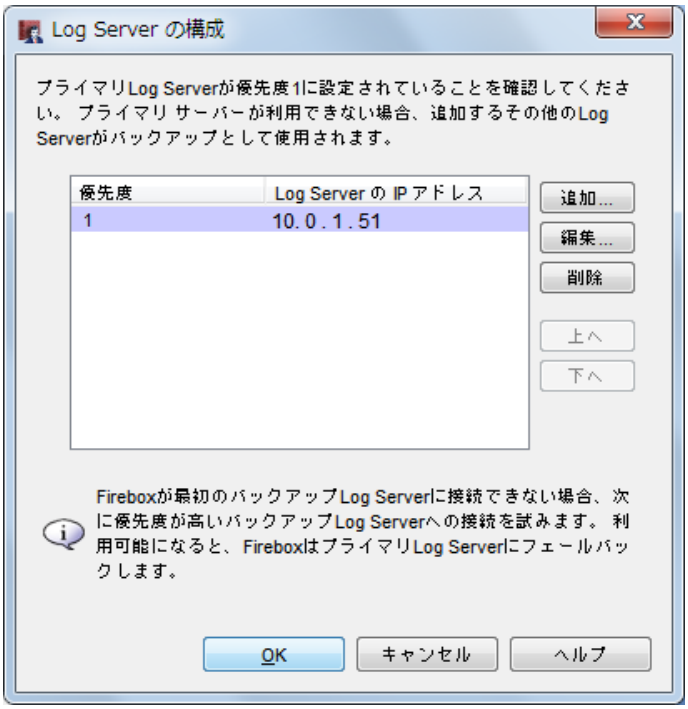


LogServer の構成画面で追加ボタンをクリックします。

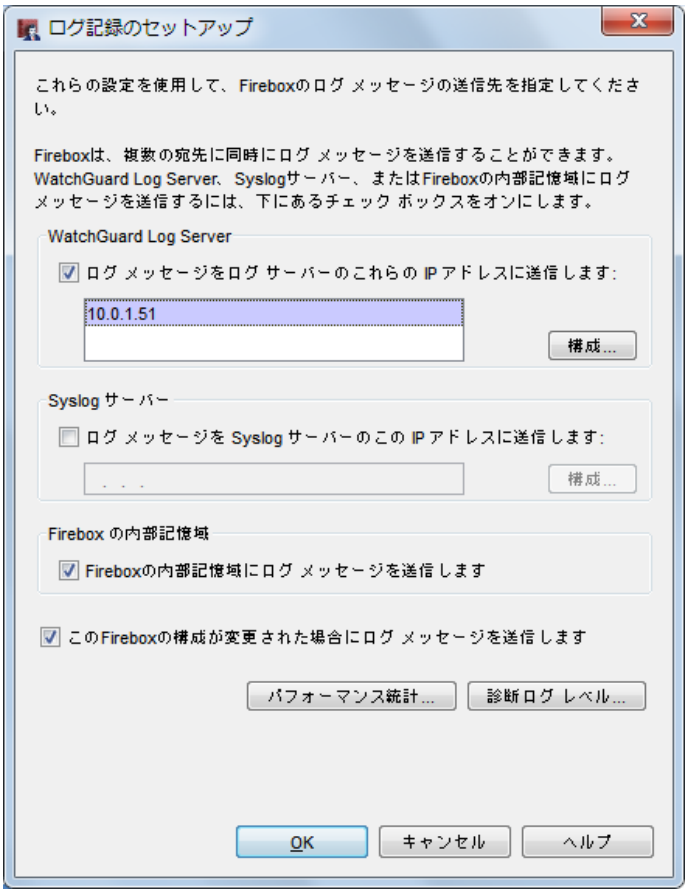
EventProcessor の追加画面で、ログサーバーの IP アドレスとログサーバー側で設定した暗号化キーを入力します。



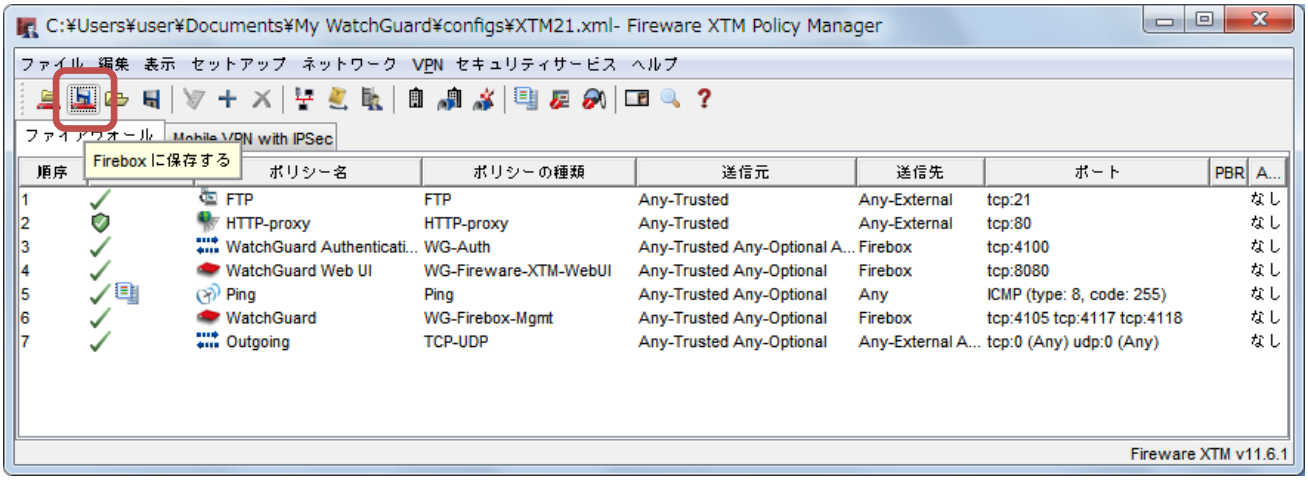
暗号化キーのフレーズが合致すると、ログサーバーに接続し、ログ受信が許可されます。
OK で抜けると以下のように、ログサーバーの一覧に表示されます。



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

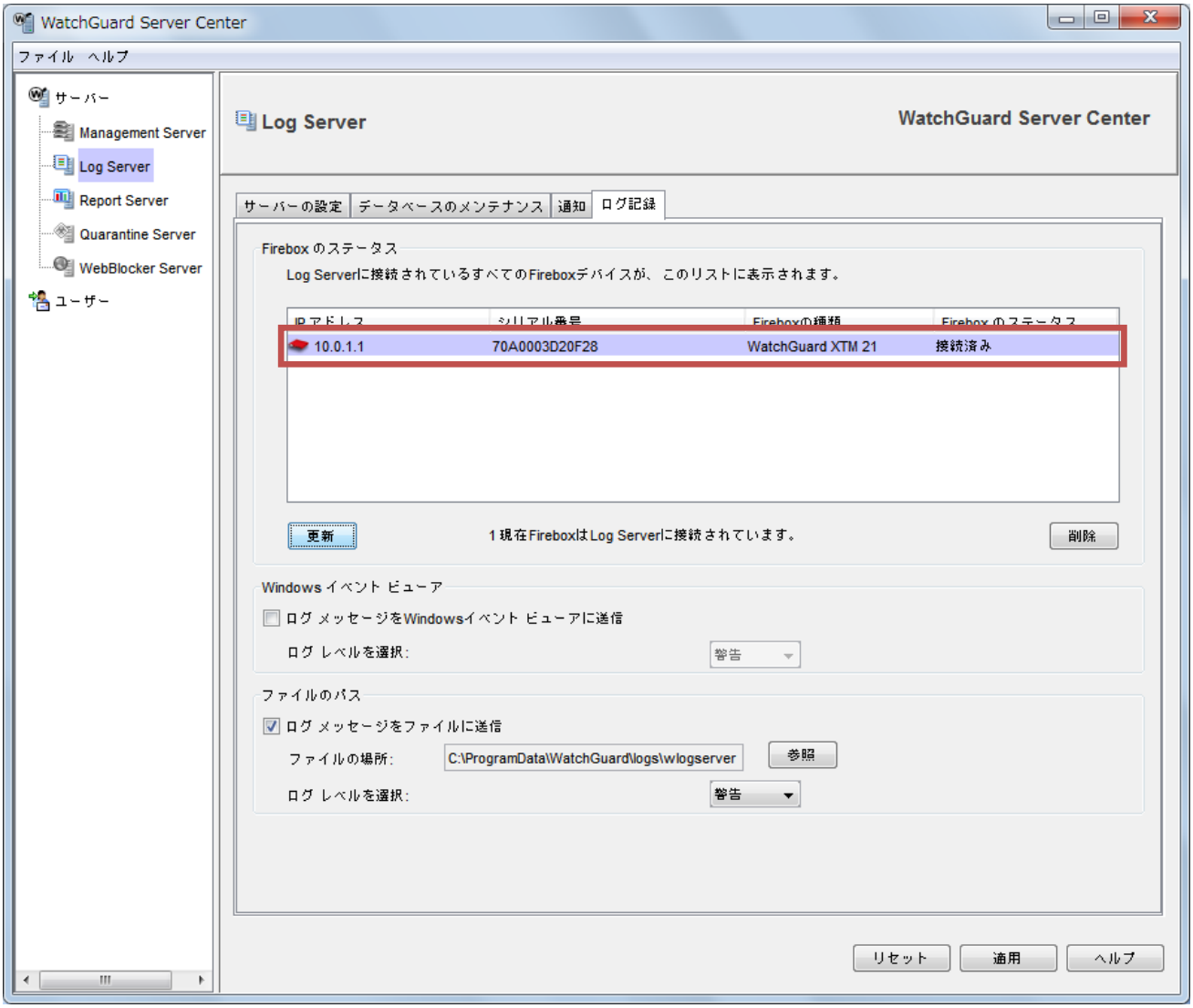


以上の設定をしたら、デバイスに設定を保存しましょう。



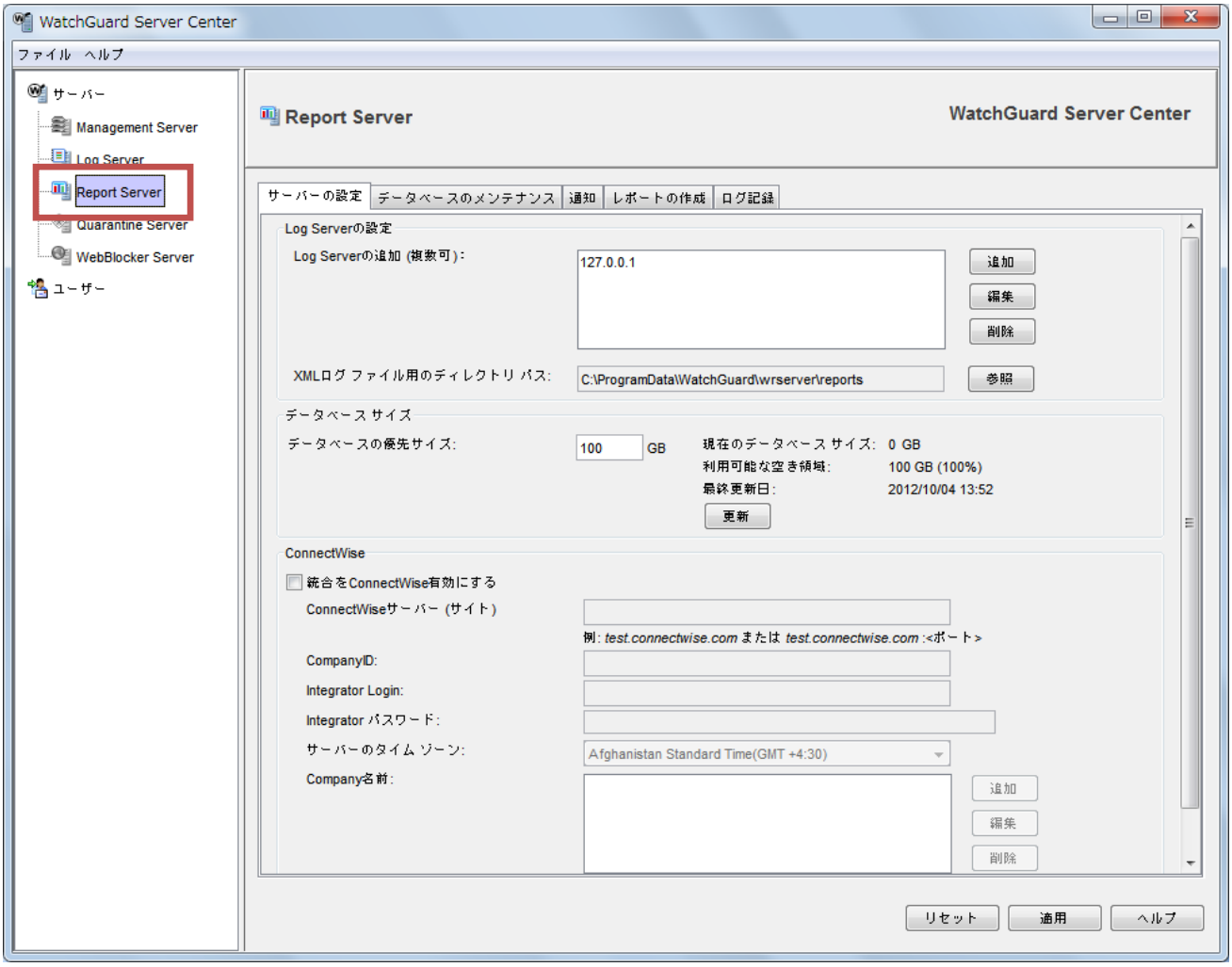
ログ受信確認

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

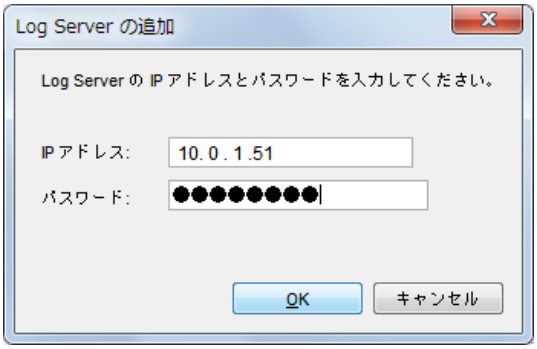
次頁から各種の設定について解説します。

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。

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。



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。

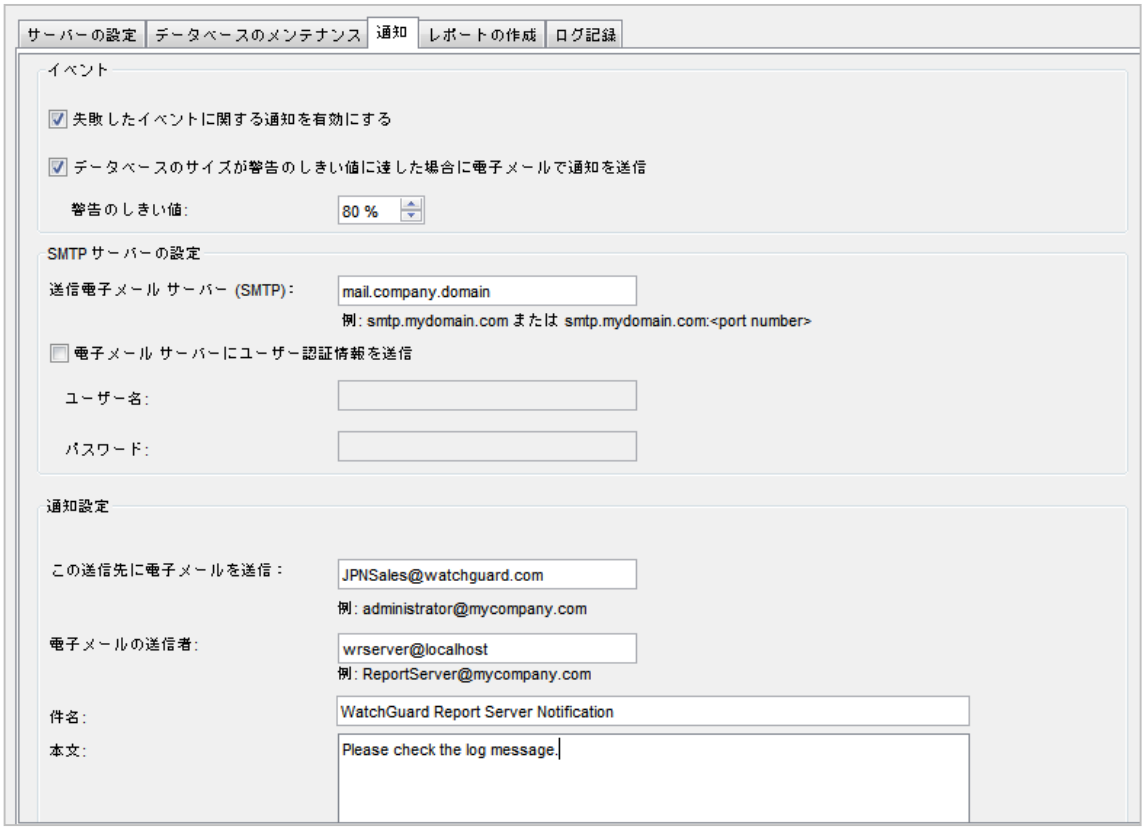
「データベースの設定」セクションでは、レポート用のデータベースの設定ができます。
外部のデータベースを指定するには、次のように「外部 PostgreSQL データベース」にチェックを入れて、データベースアクセスに必要な情報を入力します。

※ 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。



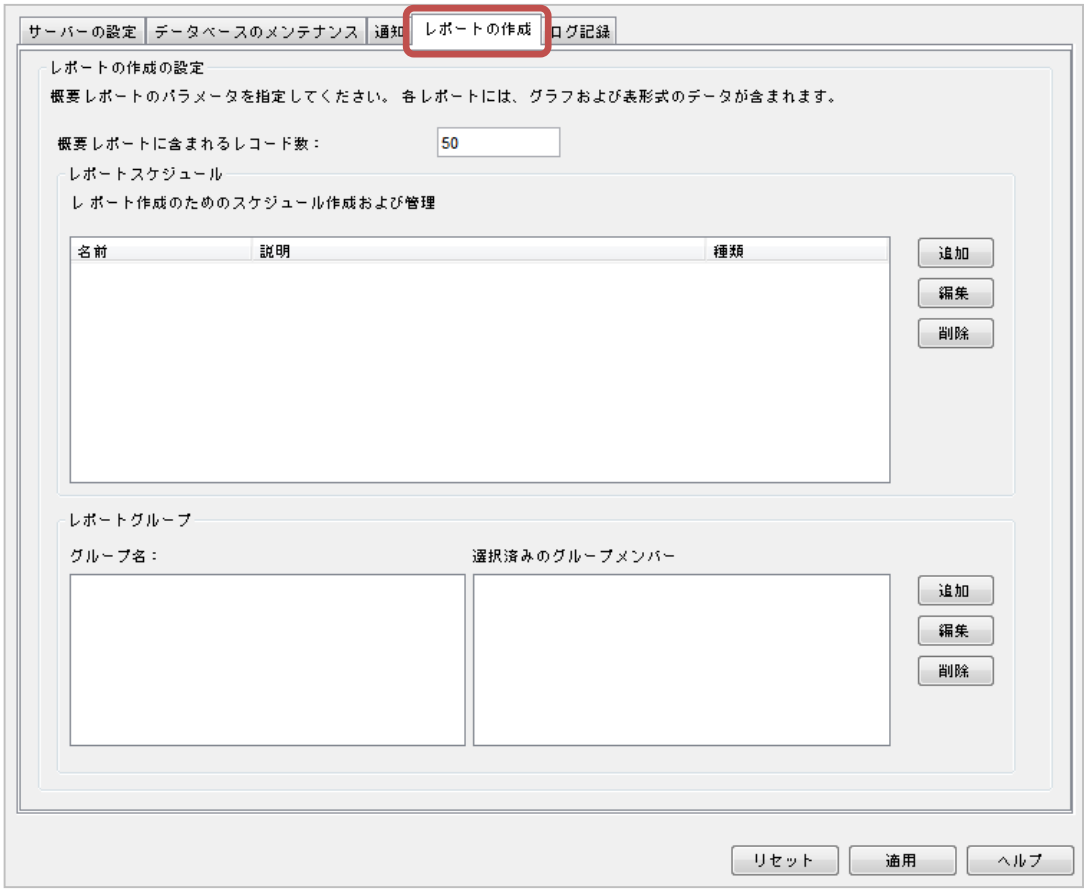
「イベント」セクションの失敗したイベントとは、データベースへの接続が失われた、データベース側のエラー、レポート作成時のエラー、Log Server への接続エラーが該当します。

「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。

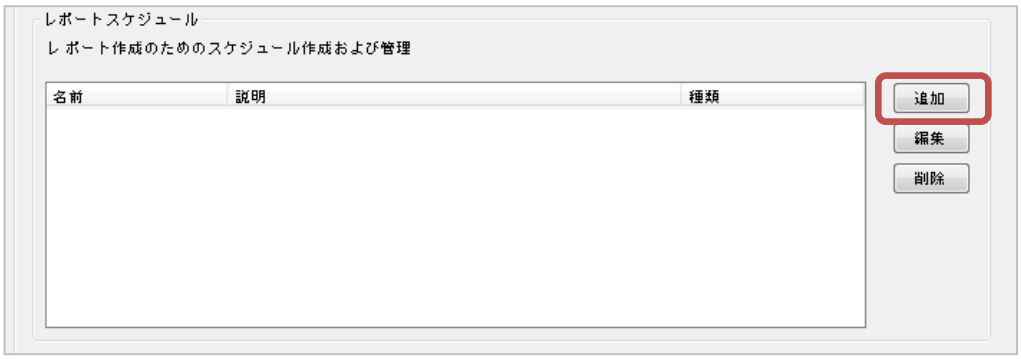
「通知設定」セクションで TO、From、件名、本文を指定します。

- レポートの作成

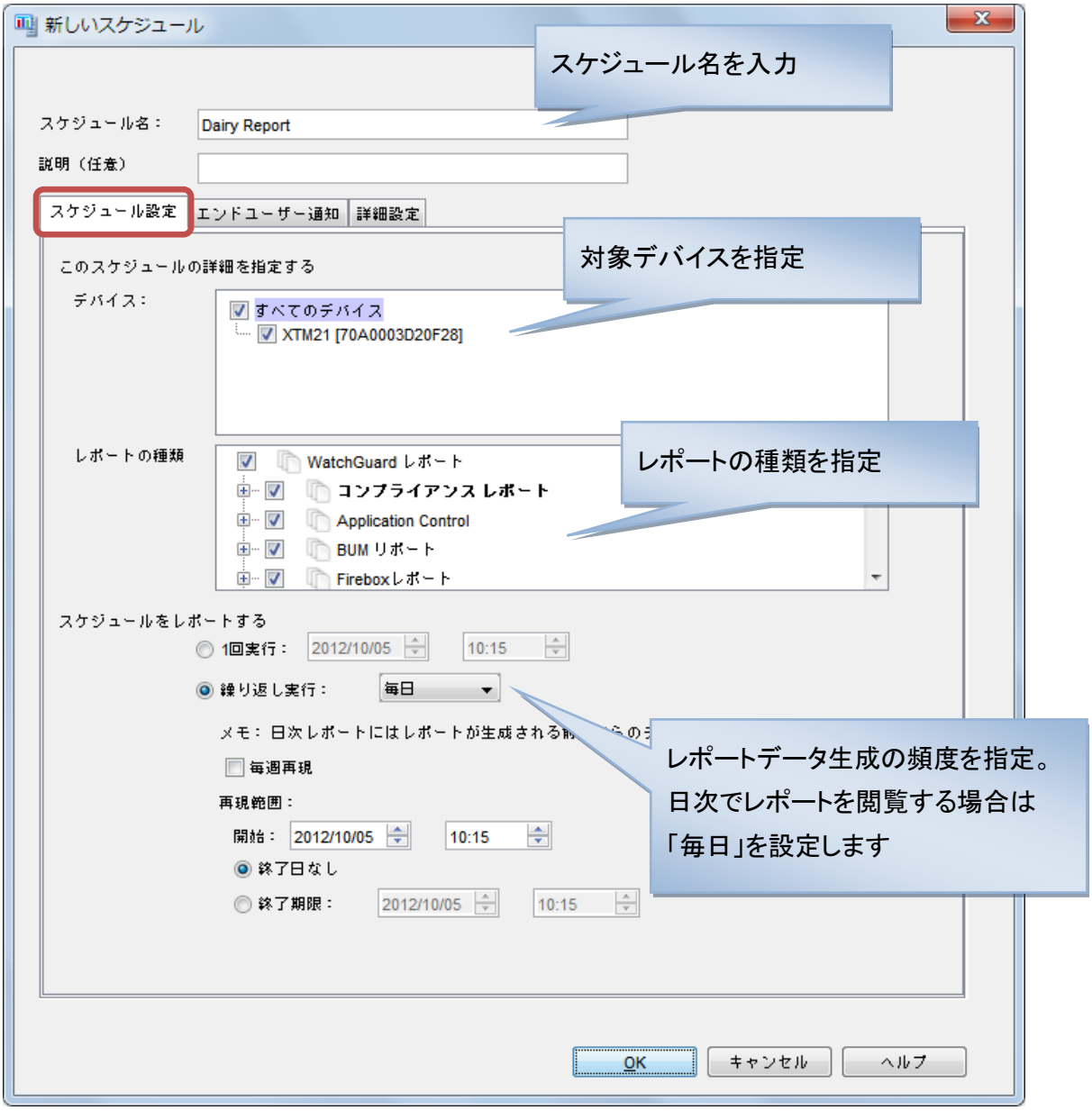
レポートサーバーにはアーカイブされたレポートとオンデマンドレポートを作成します。そしてそれらのレポートを表示するためには、元データとなる XML を定期的に生成しなければなりません。
このレポート作成タブでは、XML ファイルを生成するスケジュールを設定します。



「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。

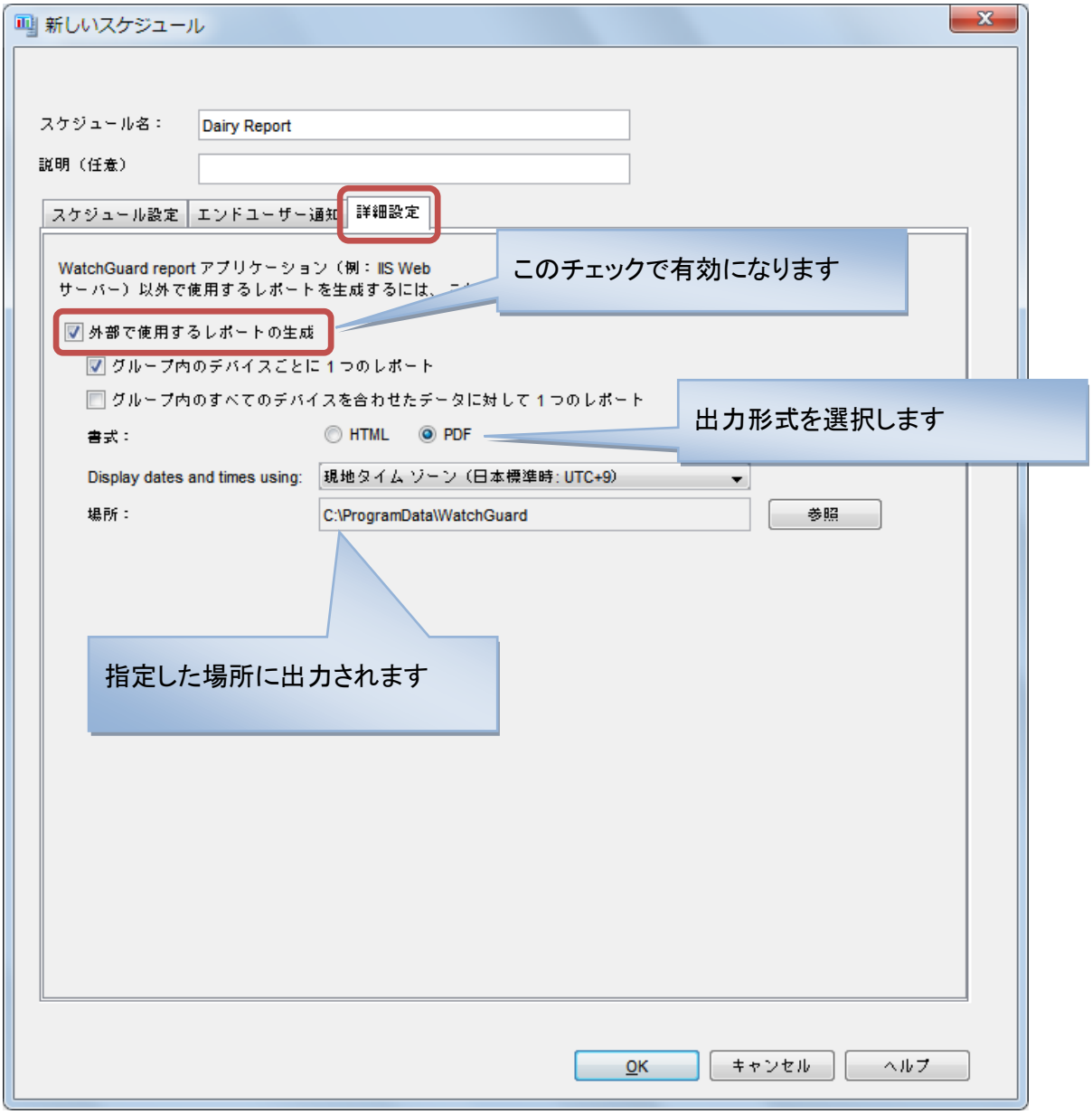


新しいスケジュール画面が表示されます。スケジュール名を入力します。
「スケジュール設定」タブで、どのデバイスのレポートを作成するか、どの種類のレポート作成を有効にするか、どれくらいの頻度で作成するかを指定します。



「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。

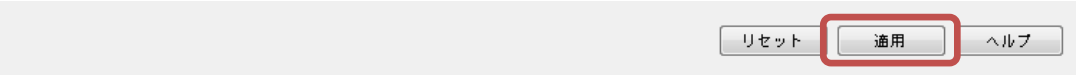


HTML か PDF で出力されます。場所はレポートサーバーの都合のよい場所をしてします。

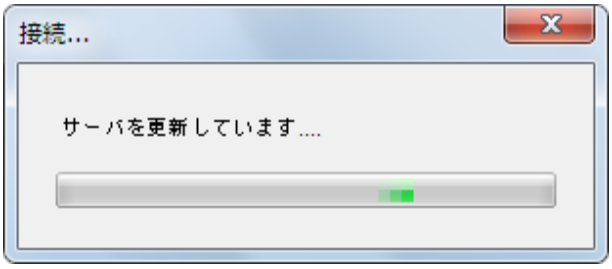
デバイスごとのレポートが必要なら「グループ内のデバイスごとに一つのレポート」にチェックを入れておきます。(グループを設定していなければこちら)

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。

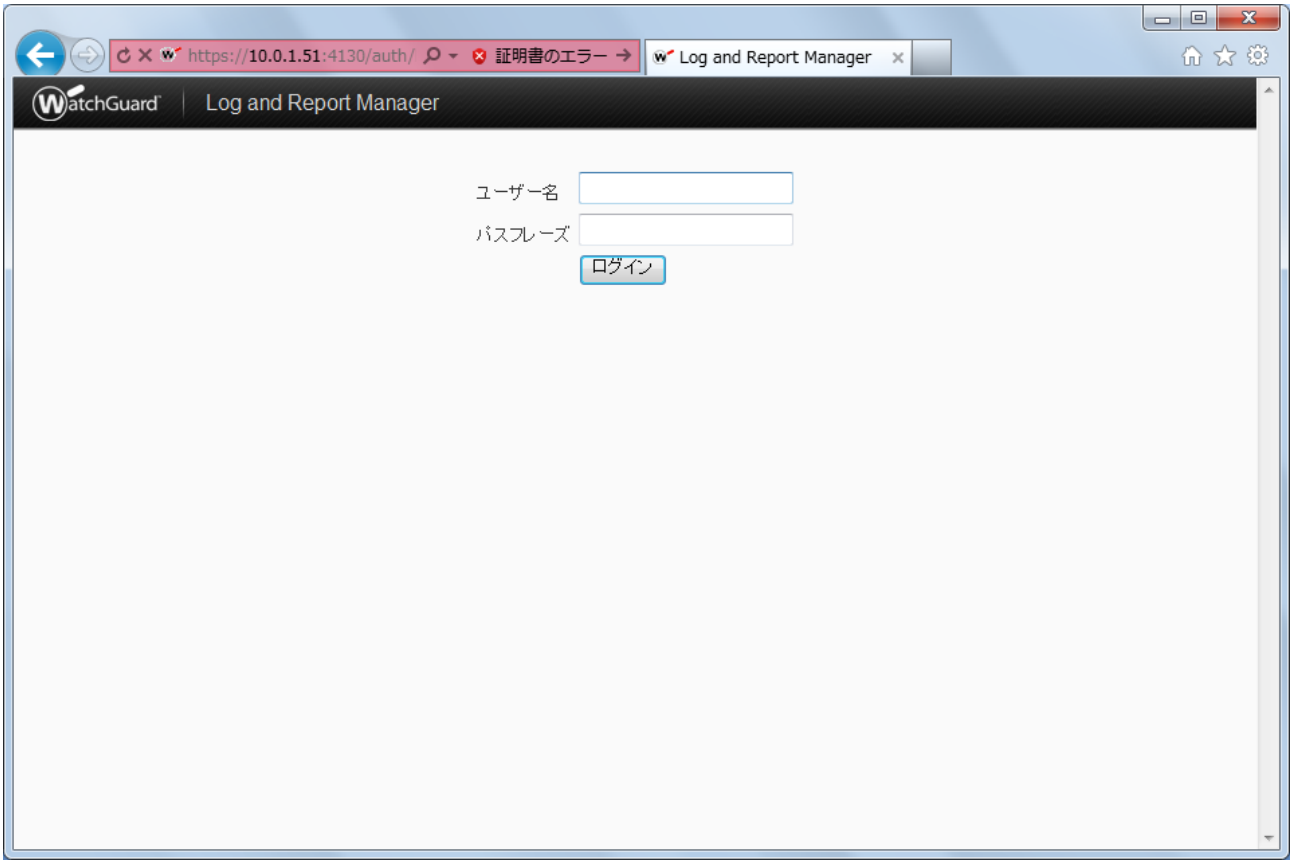
ログおよびレポートの表示方法

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

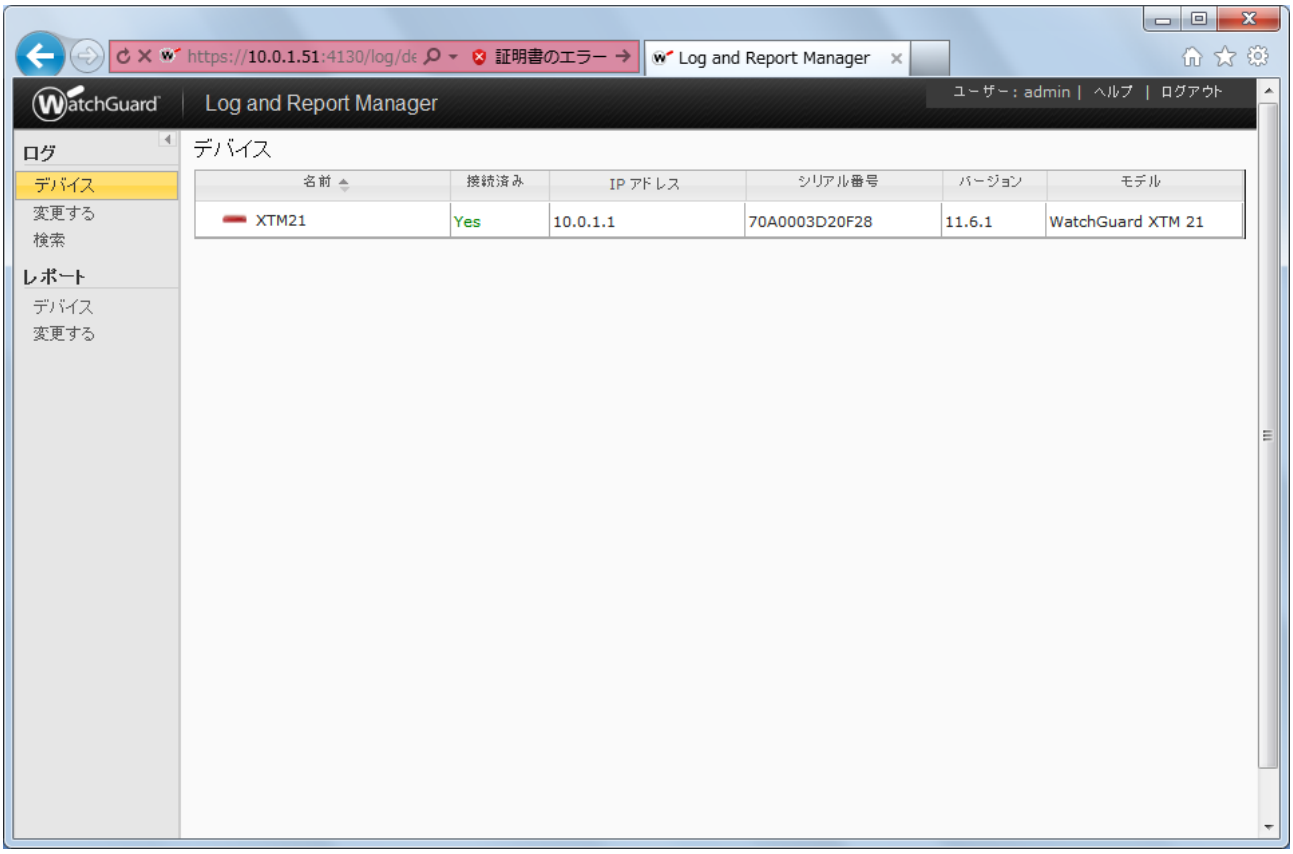
ウェブブラウザから、https://レポートサーバーの IP アドレス:4130/ でアクセスします。

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。

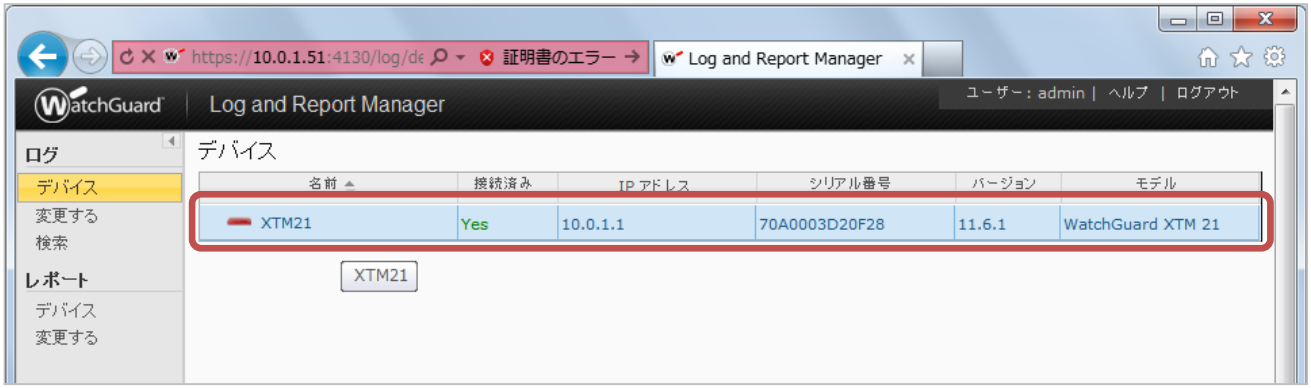
ログ&レポートサーバーに接続しているデバイスの一覧が表示されます。



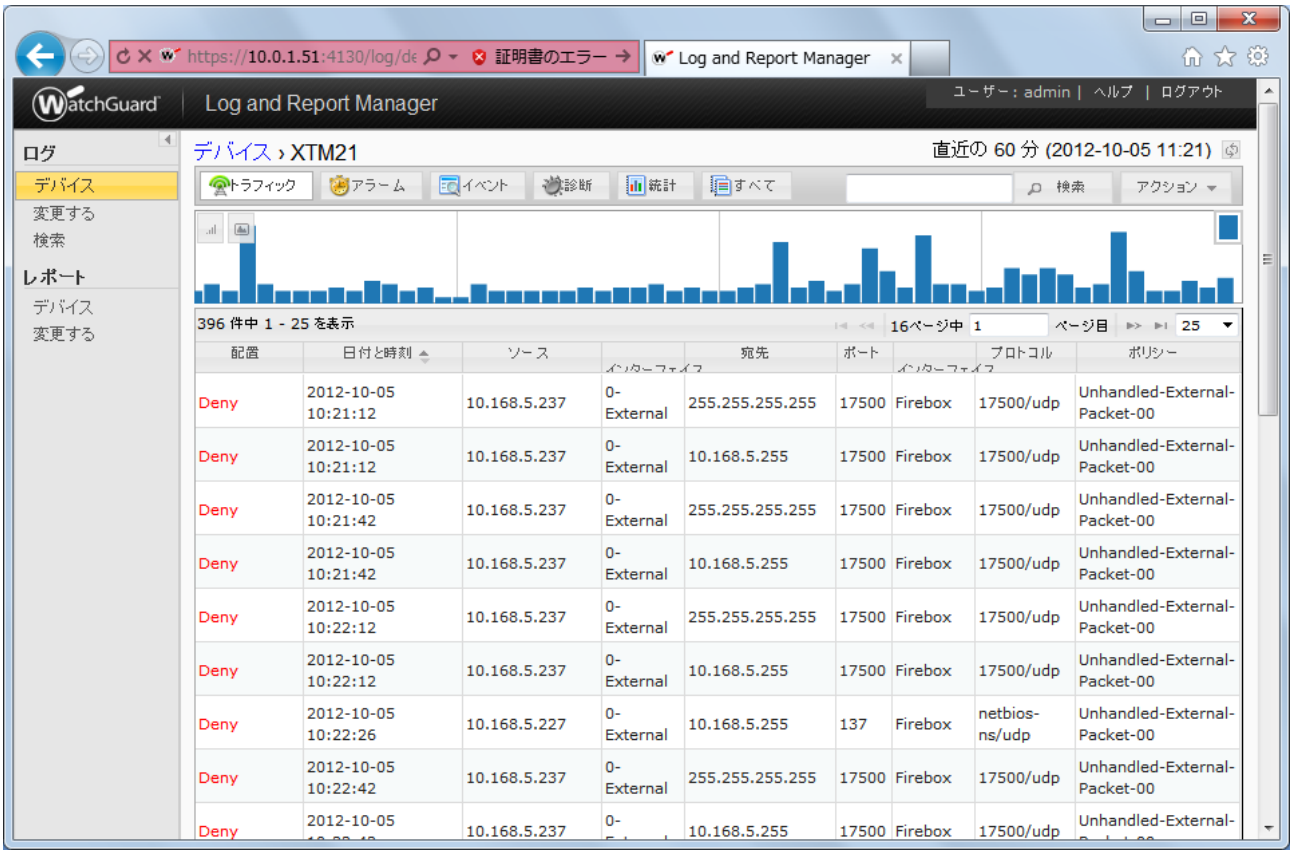
ログの表示

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。

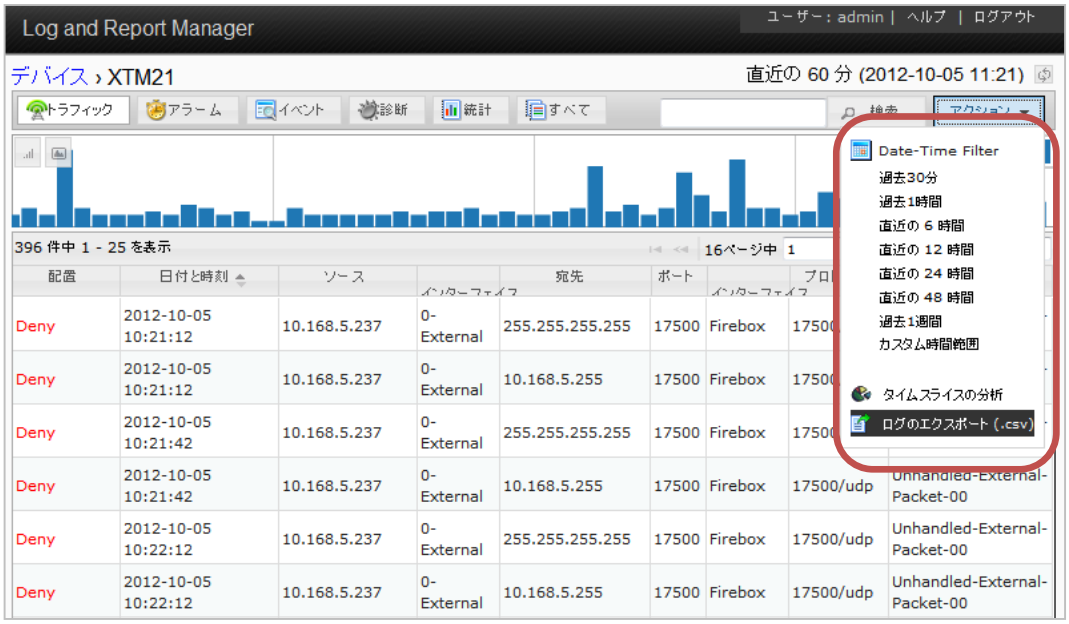


検索機能を使用すると、ログの検索や絞込みができます。

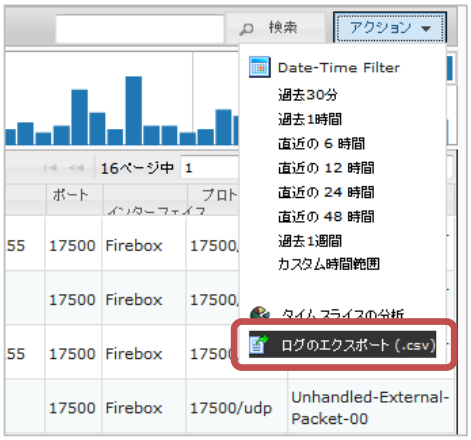
検索結果から、さらに時間の範囲やログの種類、検索語一致条件も指定できます。

ログのダウンロード

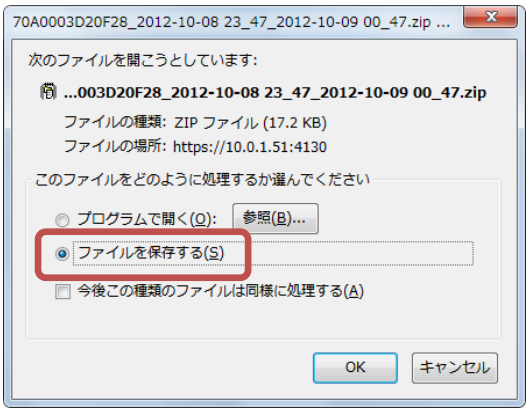
検索ボタンの右横に「アクション」のダイアログボックスがあり、ここからログ表示の期間指定やログのエクスポートができます。CSV 形式でエクスポートされます。



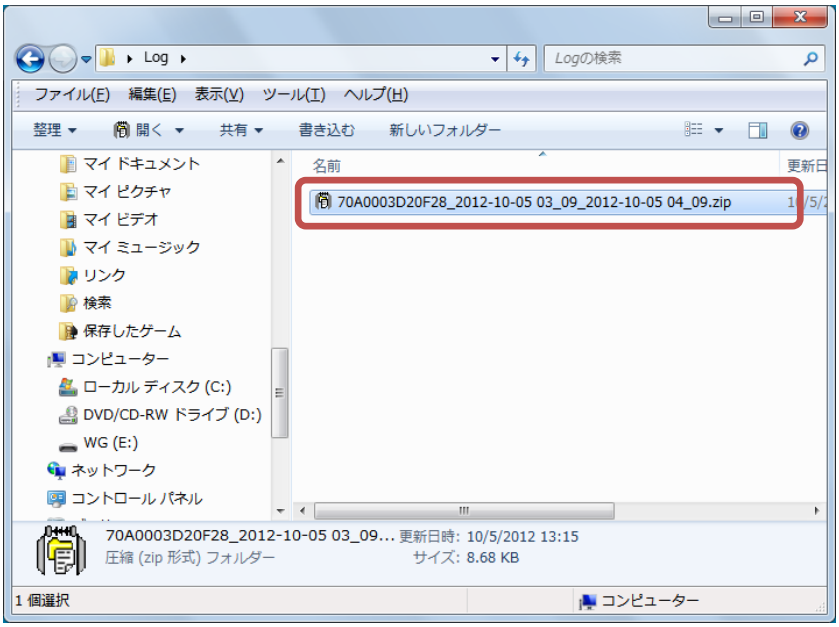
アクションのメニューからログのエクスポートをクリックします。



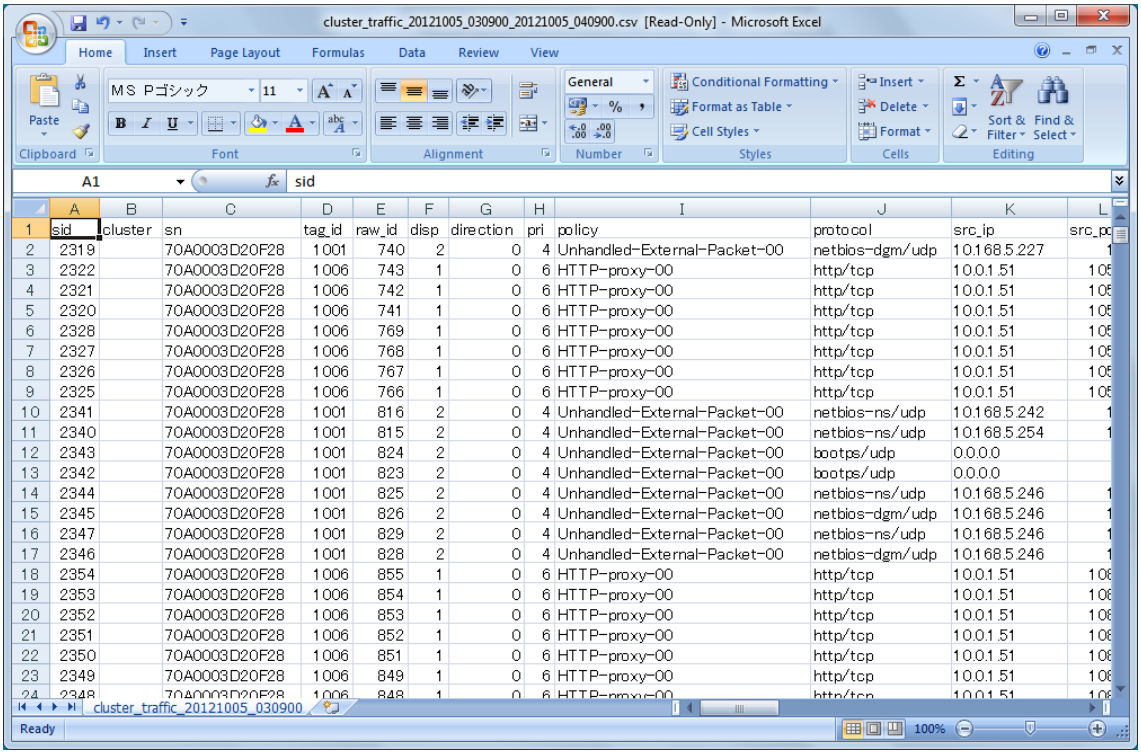
保存します。



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。



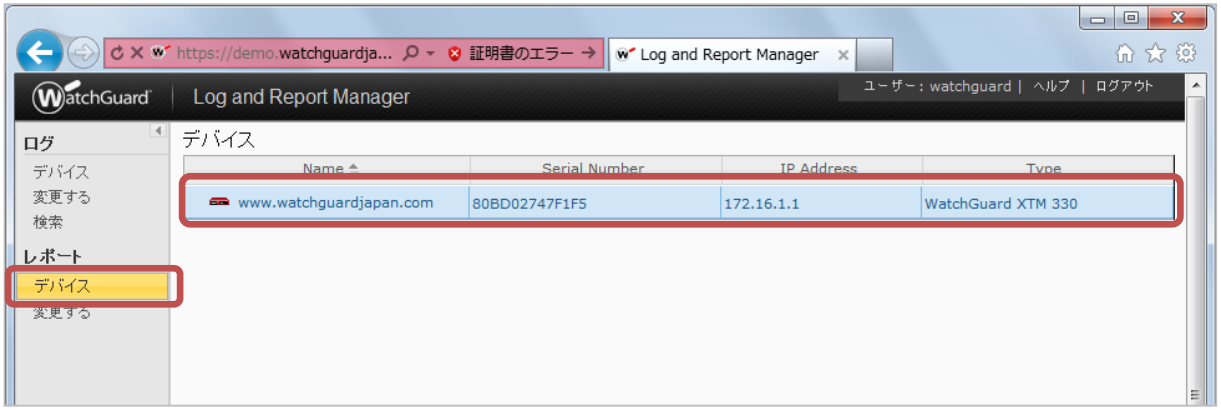
	A	B	C	D	E	F	G	H	I	J	K	L
1	sid	cluster	sn	tag_id	raw_id	disp	direction	pri	policy	protocol	src_ip	src_po
2	2319		70A0003D20F28	1001	740	2	0	4	Unhandled-External-Packet-00	netbios-dgm/udp	10.168.5.227	1
3	2322		70A0003D20F28	1006	743	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	105
4	2321		70A0003D20F28	1006	742	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	105
5	2320		70A0003D20F28	1006	741	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	105
6	2328		70A0003D20F28	1006	769	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	105
7	2327		70A0003D20F28	1006	768	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	105
8	2326		70A0003D20F28	1006	767	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	105
9	2325		70A0003D20F28	1006	766	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	105
10	2341		70A0003D20F28	1001	816	2	0	4	Unhandled-External-Packet-00	netbios-ns/udp	10.168.5.242	1
11	2340		70A0003D20F28	1001	815	2	0	4	Unhandled-External-Packet-00	netbios-ns/udp	10.168.5.254	1
12	2343		70A0003D20F28	1001	824	2	0	4	Unhandled-External-Packet-00	bootps/udp	0.0.0.0	
13	2342		70A0003D20F28	1001	823	2	0	4	Unhandled-External-Packet-00	bootps/udp	0.0.0.0	
14	2344		70A0003D20F28	1001	825	2	0	4	Unhandled-External-Packet-00	netbios-ns/udp	10.168.5.246	1
15	2345		70A0003D20F28	1001	826	2	0	4	Unhandled-External-Packet-00	netbios-dgm/udp	10.168.5.246	1
16	2347		70A0003D20F28	1001	829	2	0	4	Unhandled-External-Packet-00	netbios-ns/udp	10.168.5.246	1
17	2346		70A0003D20F28	1001	828	2	0	4	Unhandled-External-Packet-00	netbios-dgm/udp	10.168.5.246	1
18	2354		70A0003D20F28	1006	855	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	106
19	2353		70A0003D20F28	1006	854	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	106
20	2352		70A0003D20F28	1006	853	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	106
21	2351		70A0003D20F28	1006	852	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	106
22	2350		70A0003D20F28	1006	851	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	106
23	2349		70A0003D20F28	1006	849	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	106
24	2348		70A0003D20F28	1006	848	1	0	6	HTTP-proxy-00	http/tcp	10.0.1.51	106

レポートの表示

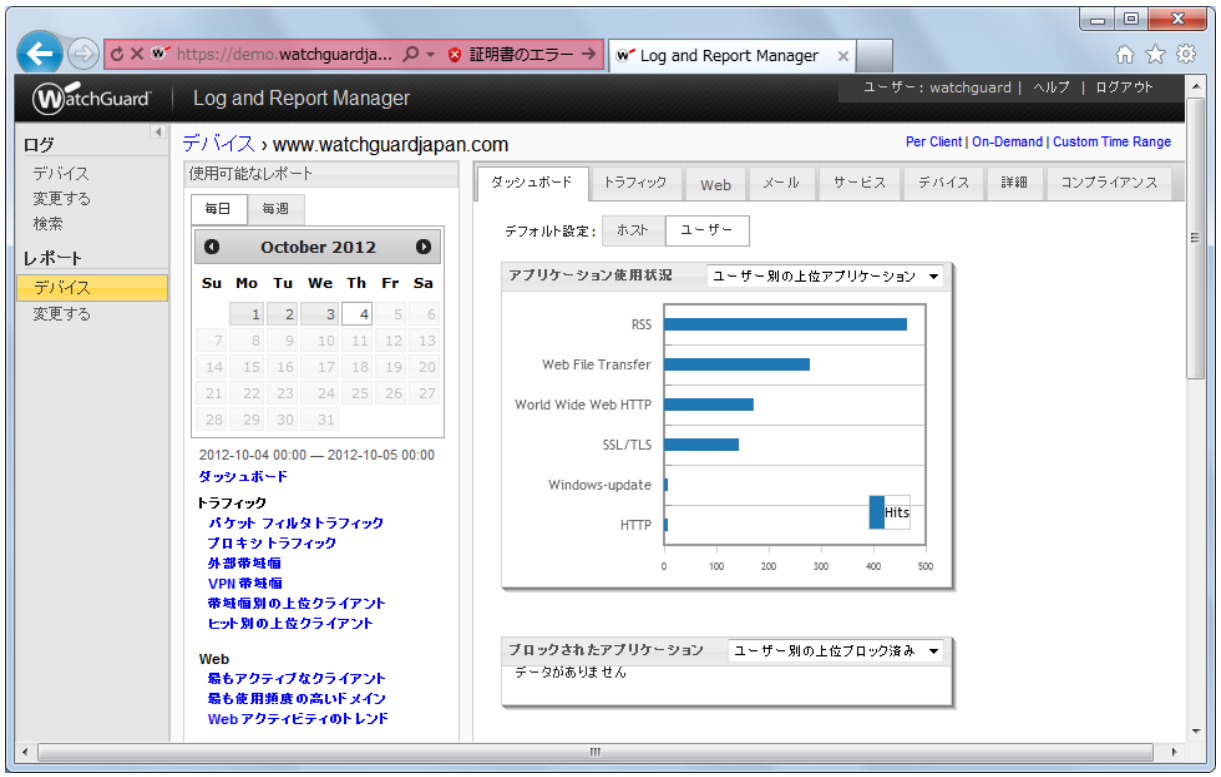
レポートの閲覧

ログイン後、左側メニュー レポートの下の「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。[1]



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。

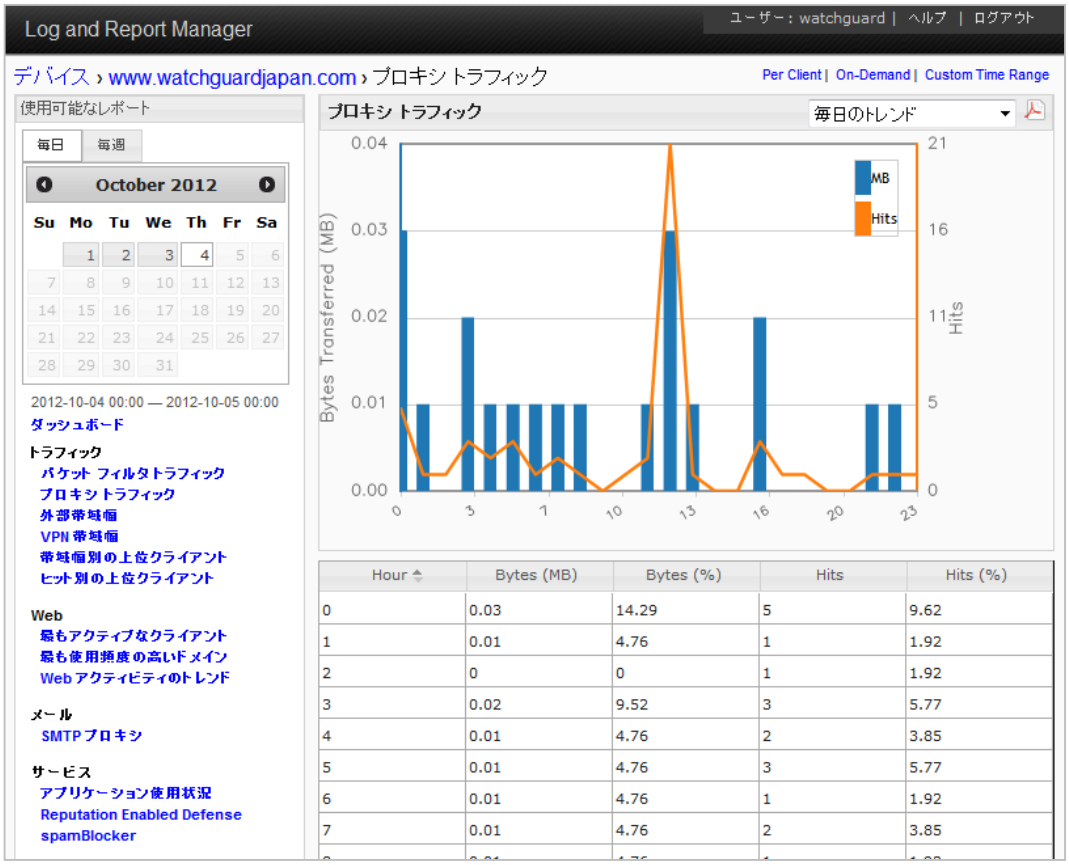


[1] レポートデータが生成されないと表示されません。表示されない場合は、スケジュールの頻度にもよりますが、時間を置いて(1 日 1 回であれば翌日)再度表示してみてください。

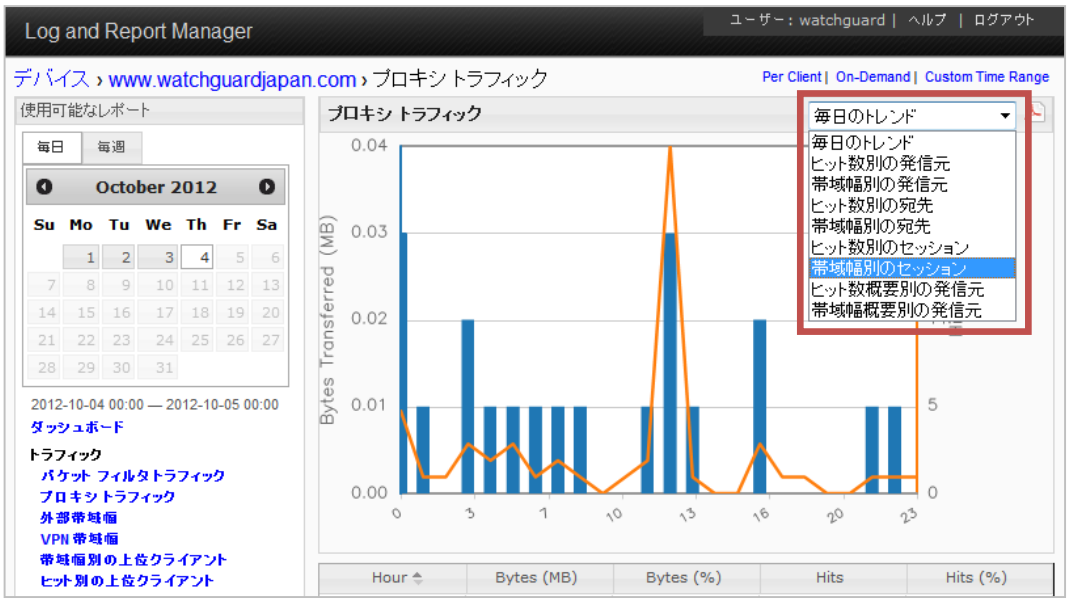
カレンダーの「毎日」「毎週」タブを選択し、デイリーレポートもしくはウィークリーレポートを切り替えます。

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。

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。

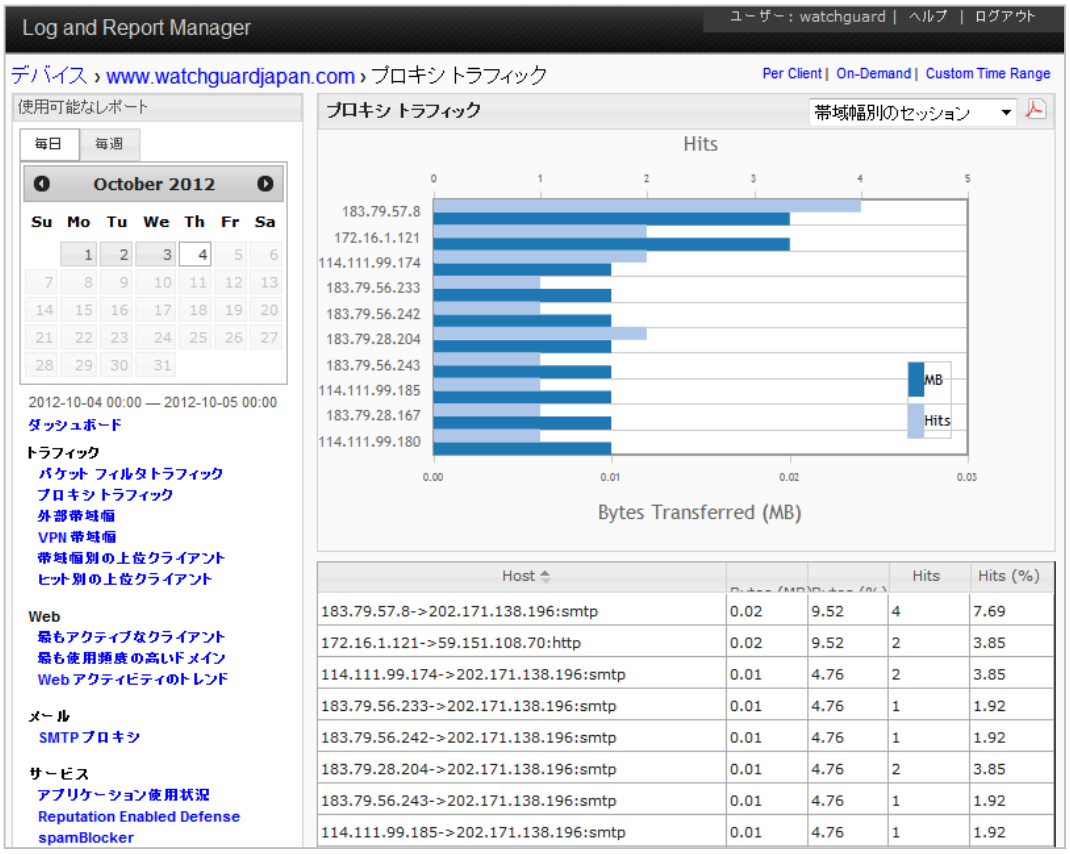


右上のドロップダウンリストから、同じレポートでも、分析する観点を変更することができます。



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。

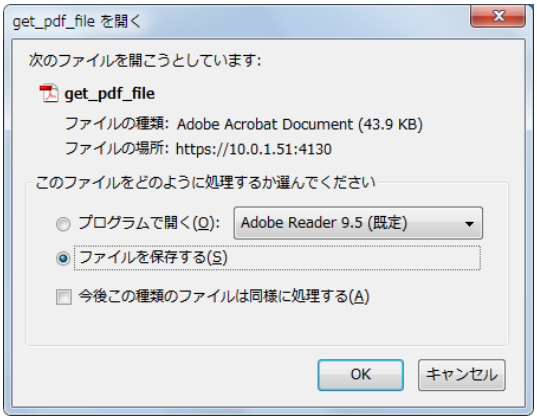


PDF レポートのダウンロード

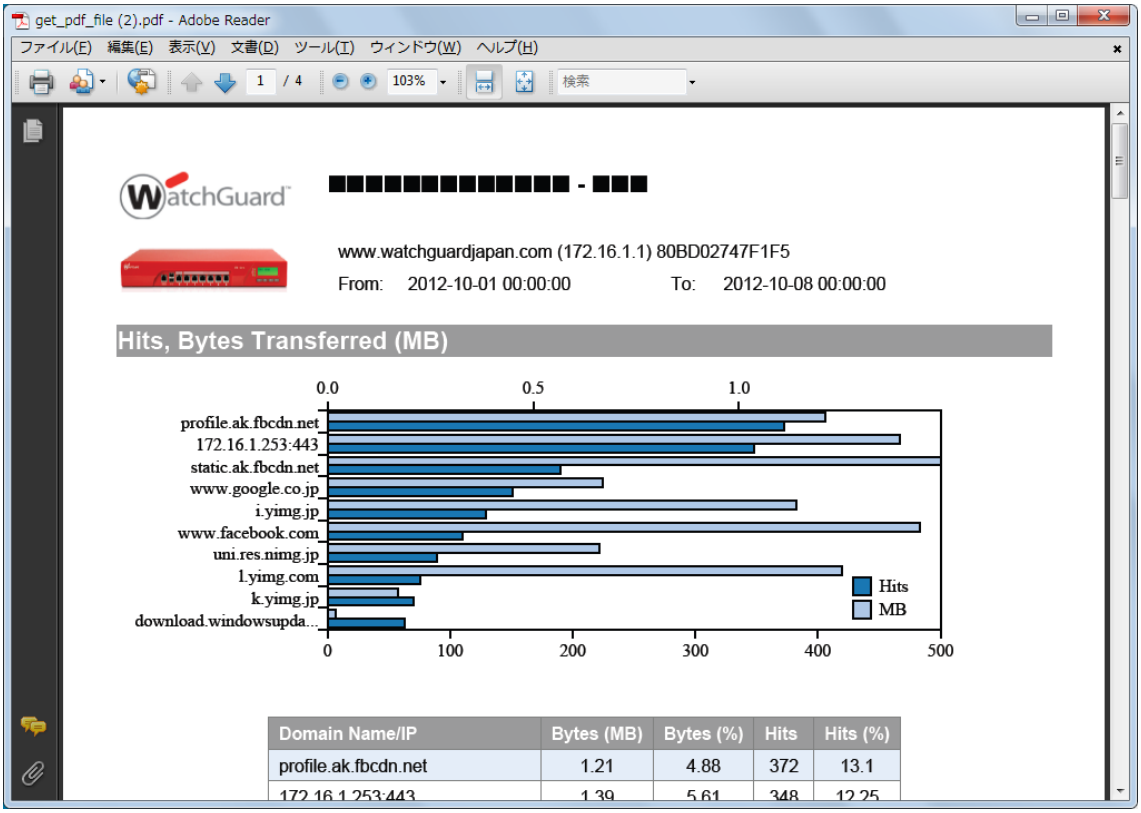
表示したレポートを PDF ファイルでダウンロードすることができます。

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。