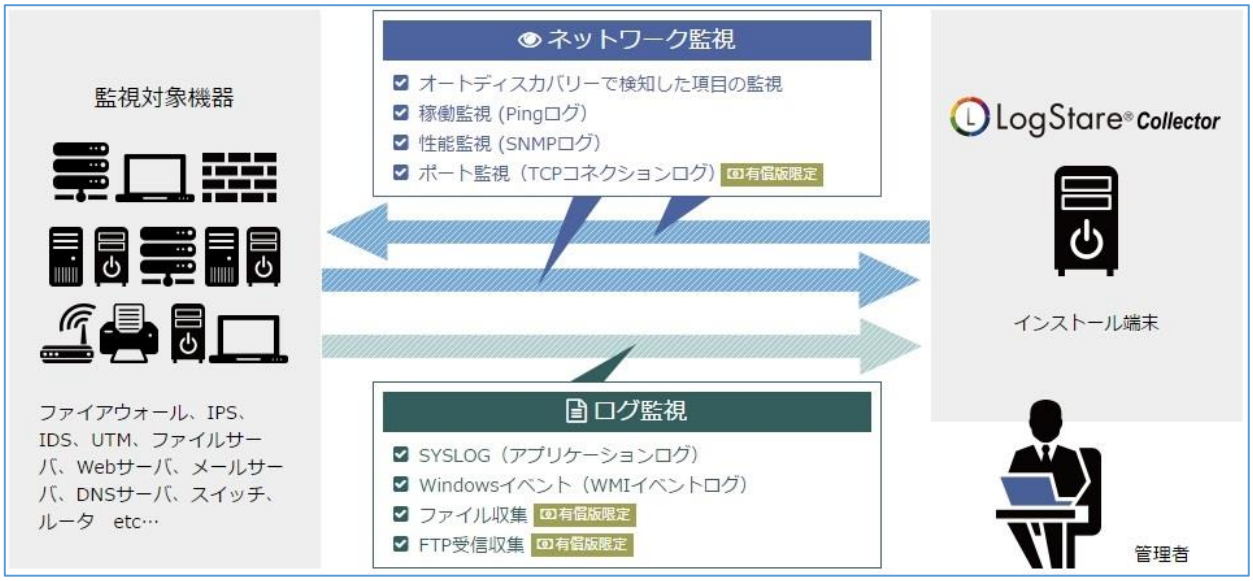
目 次

LogStare Collector の概要

LogStare Collector 動作イメージ

【動作イメージ図】



LogStare Collector の機能は大きく「システム管理」、「監視・ログ収集設定」、「ログデータ」、「監視・モニタリング」の 4 つで構成されています。

機能	内容
システム管理	メール設定など監視以外の環境設定を行うことができます。
監視・ログ収集設定	監視したいデバイスの設定を行うことができます。
ログデータ	収集したログの内容を確認することができます。
監視・モニタリング	監視しているデバイスの状況を Dynamic Status Viewer やダッシュボードなどで視覚的に確認することができます。

動作環境

LogStare Collector の動作には、以下のソフトウェア、ハードウェア環境が必要です。

動作環境		
OS	Windows	・Windows 7 ・Windows 8.1 ・Windows 10 ・Windows Server 2008 R2 ・Windows Server 2012 R2 ・Windows Server 2016
	Linux	・Red Hat Enterprise Linux 6 ・Red Hat Enterprise Linux 7 ・CentOS 6 ・CentOS 7
ブラウザ	Google Chrome 推奨	
Java	JDK12	
CPU	2GHz 以上 ／ 2core 以上	
メモリ	4GB 以上	
HDD	空き容量 20GB 以上 ※ログサイズおよび保管期間等により異なる	
その他	・Linux OS で SYSLOG 収集機能を利用する場合は、root ユーザでの起動が必要 ・Linux OS で WMI 収集機能を利用する場合は、wmi パッケージのインストールが必要 ・SYSLOG 収集を利用する場合、LogStare Collector サーバの IP アドレスは 固定 IP アドレスが必要 ・LogStare Collector からのお知らせや、監視・収集設定に関するデータ更新 （アップデート）を行うために、下記管理サーバへの接続が必要 － FQDN：pacific.netstare.jp － ポート：443/TCP	

LogStare Collector のインストール

Windows へのインストール事前準備手順

Windows へのインストール作業の事前準備手順を記載しています。
インストール前に次の 2 点を確認してください。

1. Java Development Kit(JDK)の確認

LogStare Collector の動作には JDK が必要となります。
※LogStare Collector では Java のバージョン 12(JDK12)が必要です。

JDK がインストールされていない場合は、以下の記事をご参照ください。
https://www.secuavail.com/product/logstarecollector/kb/references/ref-190610_01/

2. LogStare Collector の実行ファイルのダウンロード

セキュアヴェイル社の Web サイトから Windows 版の実行ファイルをダウンロードし、LogStare Collector をインストールする Windows 上に配置します。

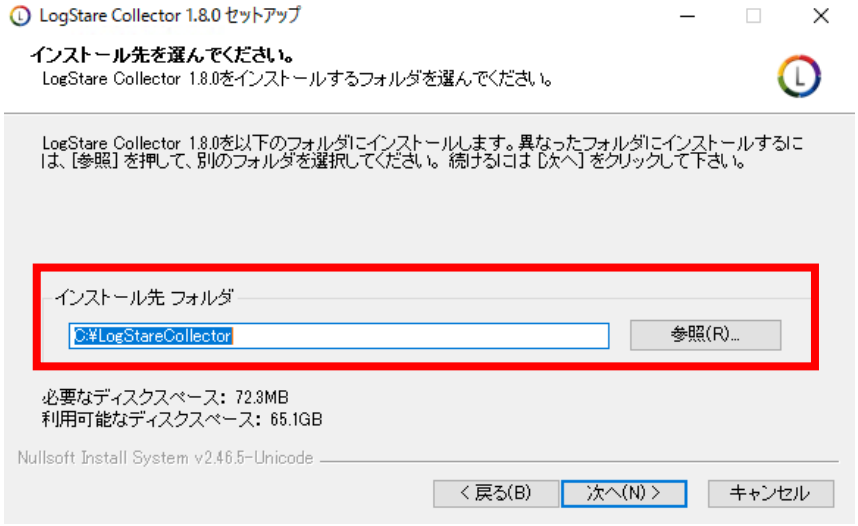
Windows への LogStare Collector インストール

ダウンロードした実行ファイル(exe ファイル)を実行し、セットアップを行います。

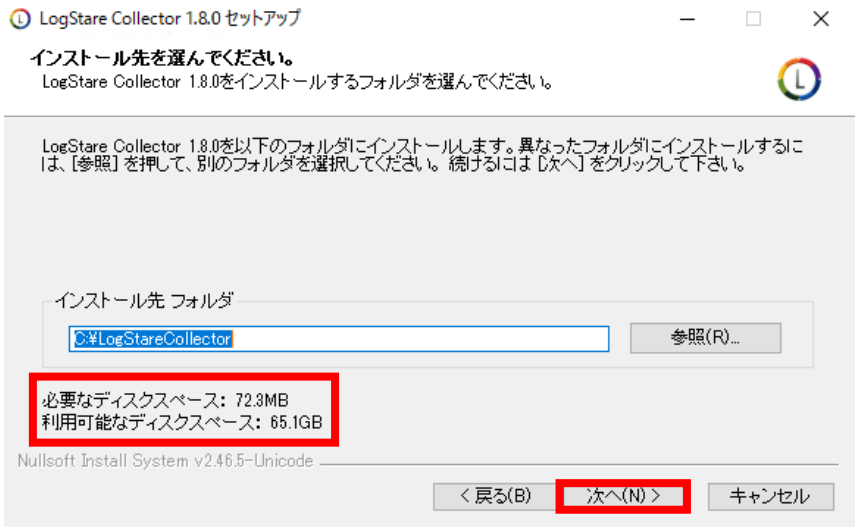
「次へ」をクリックします。

インストール先フォルダを指定します。

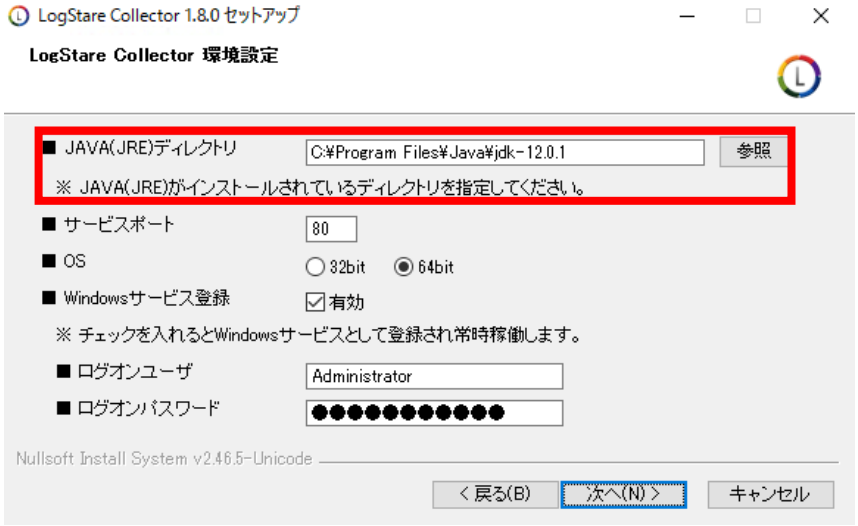
デフォルトでは C ドライブ直下に「LogStare Collector」フォルダを作成し、その場所を指定しています。



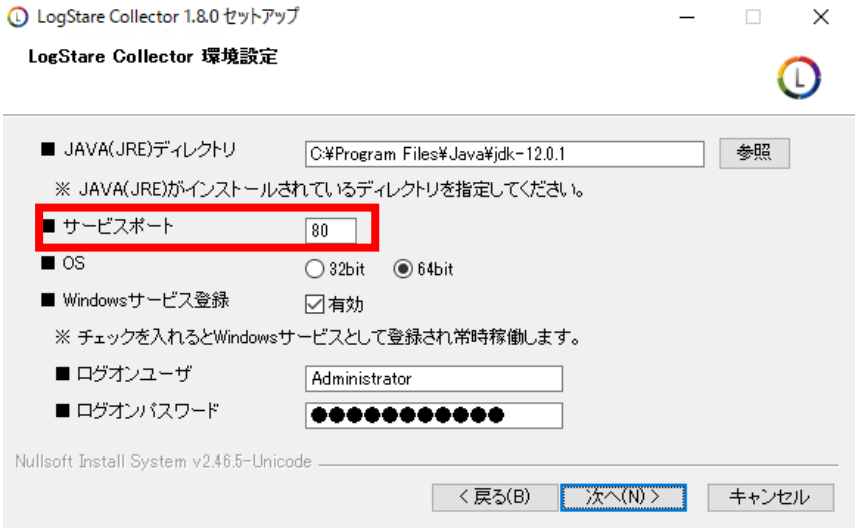
利用可能なディスクスペースが必要なディスクスペースに対して不足していないことを確認し、「次へ」をクリックします。



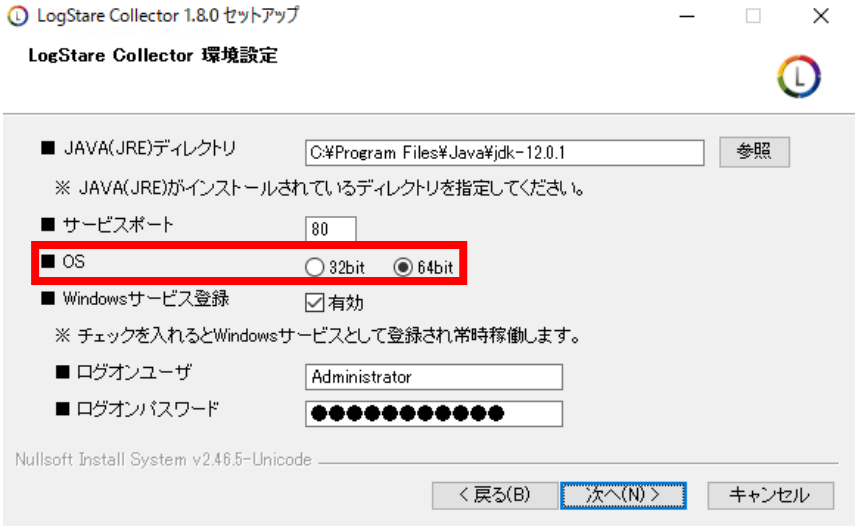
JDK ディレクトリに、JDK12 が配置されているパスを指定してください。



LogStare Collector が使用するポート番号を指定ができます。
ポート番号はデフォルトで 80 番がセットされています。

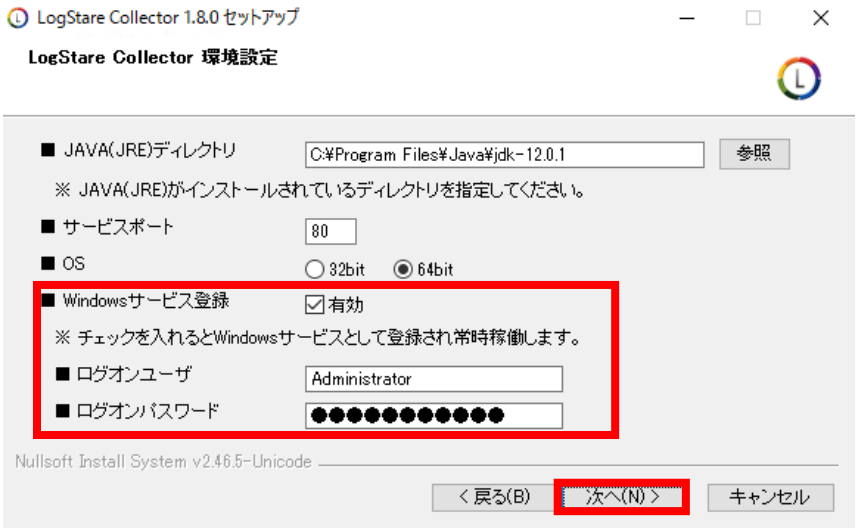


LogStare Collector の OS の種類を選択することができます。
OS はデフォルトで 64bit がセットされています。

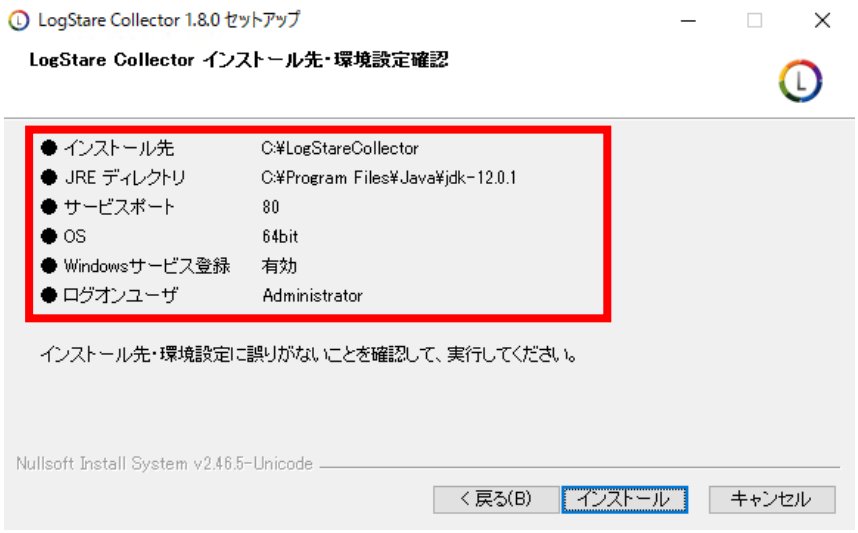


Windows サービス登録の選択ができます。
サービス登録を行うと Windows のサービス機能で LogStare Collector の「自動起動」「手動」「無効」等の設定が行える様になります。（※Windows 版 LogStare Collector の起動と停止 参照）
また、Windows からログオフをしてもサービスが起動し続けます。

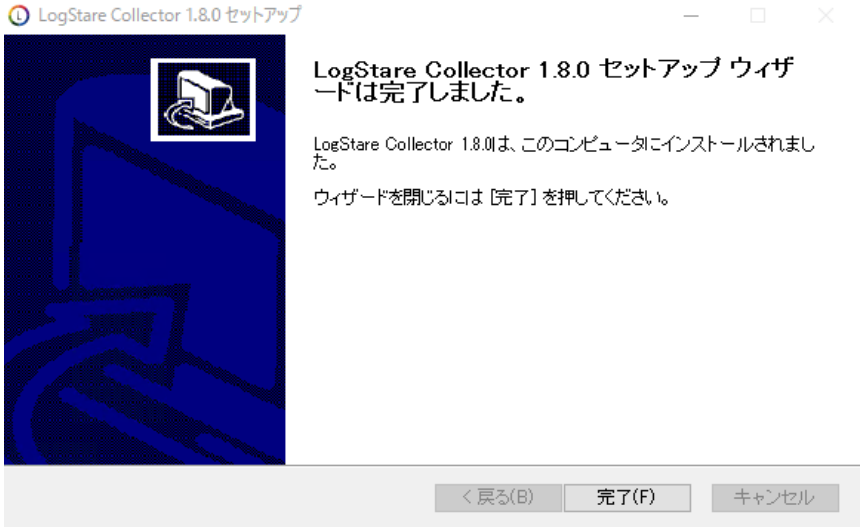
LogStare Collector をインストール・実行するユーザとパスワードを入力して「次へ」をクリックします。
※LogStare Collector では、権限の関係上、ビルトインの Administrator での設定を推奨します。



「インストール先」、「JDK ディレクトリ」、「サービスポート」の設定に誤りがないことを確認して、「インストール」をクリックします。



「完了」をクリックして、セットアップウィザードを終了します。



Windows 版 LogStare Collector の起動と停止

【LogStare Collector の起動/停止方法】

【起動方法】

デスクトップ上に作成されるショートカット「LogStare Collector（開始）」をダブルクリックして実行します。

コマンドプロンプトが開き、LogStare Collector 起動処理が終わるとコマンドプロンプトが閉じます。

LogStare Collector の管理画面へのログイン方法は「LogStare Collector へのログイン及びログアウト(Windows/Linux 共通)」を参照してください。

【停止方法】

デスクトップ上に作成されるショートカット「LogStare Collector（終了）」をダブルクリックして実行します。

コマンドプロンプトが開き、LogStare Collector 終了処理が終わるとコマンドプロンプトが閉じます。

※ショートカットで起動/停止した時にタスクトレイアイコンのメニュー画面が起動する場合がございますが、その際は「start」ボタンもしくは「stop」ボタンをクリックすることで起動/停止が可能です。

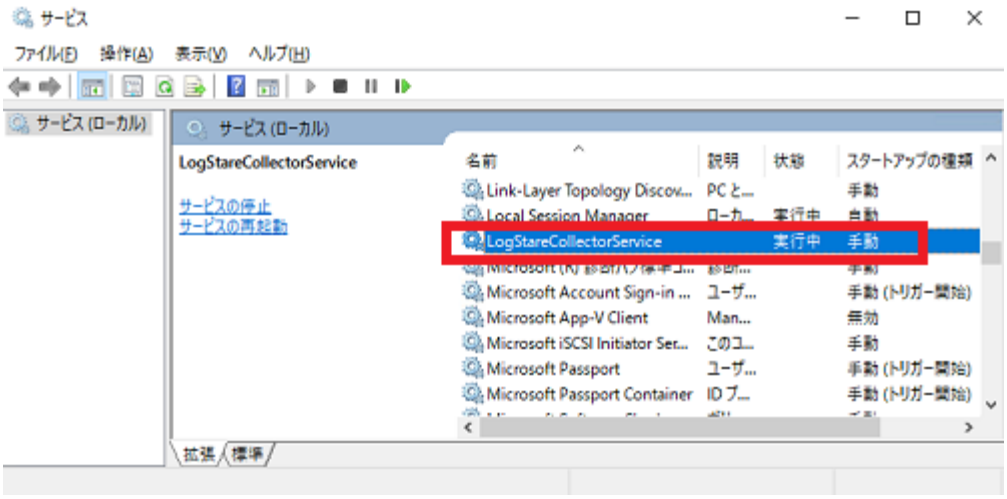
なお、タスクトレイアイコンについては、その他画面・ボタンは開発中のものであり、現段階では動作しないためご注意ください。

【Windows サービスでの起動方法】

インストール時に Windows サービス登録を行った場合は、Windows のサービス機能で LogStare Collector の「自動起動」「手動」「無効」等の設定が可能です。

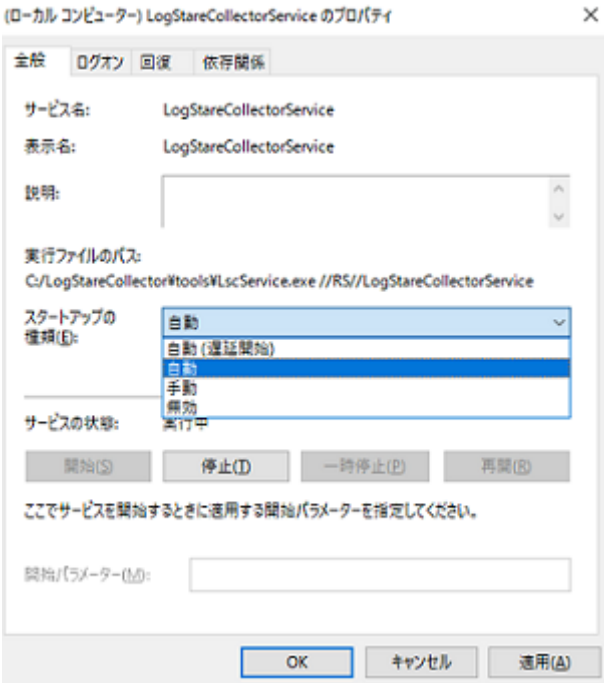
Windows の「サービス」の画面を起動します。

「LogStareCollectorService」の項目を選択後、右クリックから「プロパティ」を選択します。



「スタートアップの種類」から起動方法を選択します。

「適用」した後に「OK」を押します。



（下図は「自動」を選択した場合の例になります。）

Windows を再起動すると、「スタートアップの種類」で選択した方法で
LogStare Collector が起動します。

・「自動」を選択して再起動した場合　→　LogStare Collector が自動で起動します。
・「手動」を選択して再起動した場合　→　LogStare Collector を手動で起動する必要があります。
　（※Windows 版 LogStare Collector の起動と停止　参照）
・「無効」を選択して再起動した場合　→　LogStare Collector のサービスが無効状態になります。

Linux へのインストール事前確認

Linux へのインストール作業の事前準備手順を記載しています。
インストール前に次の 2 点を確認してください。

1. Java Runtime Environment(JDK)の確認

LogStare Collector の動作には JDK が必要となります。
※LogStare Collector では Java のバージョン 12(JDK12)が必要です。

JDK がインストールされていない場合は、以下の記事をご参照ください。
https://www.secuavail.com/product/logstarecollector/kb/references/ref-190606_01/

2. LogStare Collector の実行ファイルのダウンロード

セキュアヴェイル社の Web サイトから Linux 版の実行ファイルをダウンロードし、LogStare Collector をインストールする Linux 上に配置します。

Linux への LogStare Collector インストール

ダウンロードした実行ファイル(bin ファイル)を以下の手順で実行し、セットアップを行います。

ターミナルウィンドウからコマンドを実行します。

コマンド「cd /ダウンロードファイルの保存先ディレクトリ」

コマンド「chmod +x logstare-collector-1.8.0-setup.bin」で実行権限を与えます。

コマンド「./logstare-collector-1.8.0-setup.bin」でセットアップが開始されます。

LogStare Collector のインストール先を指定して、「Enter」キーを押してください。
デフォルトとして「/usr/local」が設定されています。

```
=== LogStare Collector 初期設定 ===

LogStare Collector のインストール先を指定してください。デフォルトは /usr/local になります。
指定先に LogStare Collector が存在する場合はアップデートを行います。
[インストール先]:
```

JDK12 が配置されているパスを指定して、「Enter」キーを押してください。

```
LogStare Collector が使用する JRE パスを指定してください。デフォルトは /usr/java/default になります。
(Java Runtime Environment 7 以上の JRE パスをご指定ください)
[JRE]:/usr/lib/jdk-12.0.1
```

LogStare Collector が使用するポート番号を指定して、「Enter」キーを押してください。
ポート番号はデフォルトで 80 番がセットされています。

```
LogStare Collector が使用するサービスポートを指定してください。デフォルトは 80 になります。
[サービスポート:80] :
```

「インストール先」、「JRE」、「サービスポート」の設定に誤りがないことを確認してください。

```
=== LogStare Collector インストール先・環境設定確認 ====
インストール先・環境設定に誤りがないことを確認してください
[インストール先]：/usr/local
[JRE]：/usr/lib/jdk-12.0.1
[サービスポート]：80
```

誤りが無ければ「y」を押して「Enter」キーを押してください。インストールが開始します。

```
=== LogStare Collector インストール先・環境設定確認 ====
インストール先・環境設定に誤りがないことを確認してください
[インストール先]：/usr/local
[JRE]：/usr/lib/jdk-12.0.1
[サービスポート]：80

LogStare Collector のインストールを行いますか?[y/N]：
```

以下の様にインストールの進行状況が表示されます。

```
LogStare Collector インストール中...
LogStare Collector Install Finish
```

正常にインストールが終了すると「LogStare Collector Install Finish」というメッセージが表示されます。
「Enter」キーを押して、プロンプト表示に戻ります。

【参考：JDK パスが不明な場合】

ユーティリティ「alternatives」コマンドを使用して現在登録されている java 情報から確認できます。

コマンド「alternatives --config java」にて登録されている java の一覧を表示します。

JDK パスを確認したら、使用する Java の選択番号を押して「Enter」キーを押します。

※/bin/java より前の部分が JDK パスとなります。

```
# alternatives --config java

1 プログラムがあり 'java' を提供します。

  選択          コマンド
-----------------------------------------------
*+ 1            /usr/lib/jdk-12.0.1/bin/java

Enter を押して現在の選択 [+] を保持するか、選択番号を入力します:
```

Linux 版 LogStare Collector の起動と停止

【LogStare Collector の起動/停止方法】

インストール先/sbin ディレクトリ内（例：/usr/local/logstarecollector/sbin）のシェルスクリプト実行で起動及び停止を行います。

【起動方法】

コマンド：「./start_kallista.sh」（LogStare Collector 起動シェルスクリプト実行）

```
# ./start_kallista.sh
```

ターミナル上に起動ログが出力され、最後に「Started @XXXXms」が表示されたら起動は完了です。
「Enter」キーを押してプロンプト表示に戻ってください。

LogStare Collector の管理画面へのログイン方法は「LogStare Collector へのログイン及びログアウト(Windows/Linux 共通)」を参照してください。

【停止方法】

コマンド：「./stop_kallista.sh」（LogStare Collector 停止シェルスクリプト実行）

```
# ./stop_kallista.sh
```

LogStare Collector へのログイン及びログアウト(Windows/Linux 共通)

ここでは、サービスを起動した LogStare Collector にログイン及びログアウトする手順を記載しています。

【ログイン方法】

ブラウザを開き、URL に LogStare Collector サーバ IP アドレスと、インストール時に指定したポート番号を入力します。

例:「http://192.168.xxx.xxx:80/」

※ポート番号は、Windows 版では「kallista_env.cmd」、Linux 版では「kallista_env.sh」を編集して変更ができます。

LogStare Collector に接続が成功すると下図のログイン画面が表示されます。

① ID とパスワードを入力します。(デフォルトユーザ ID:admin　パスワード:root1234)

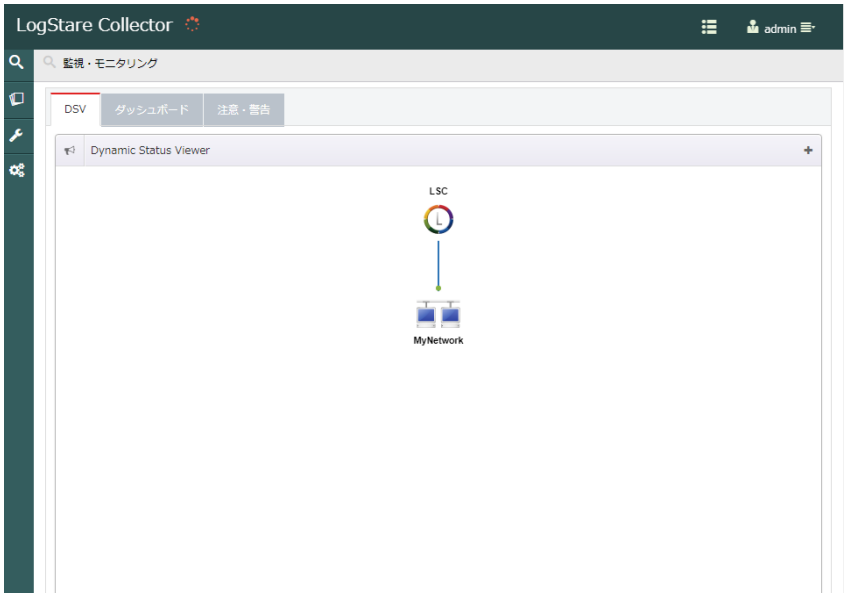
② 「ログイン」をクリックします。

※初期パスワードは必ず変更してください。

(※ログインパスワードの変更　参照)

ログインに成功すると、LogStare Collector の画面が表示されます。

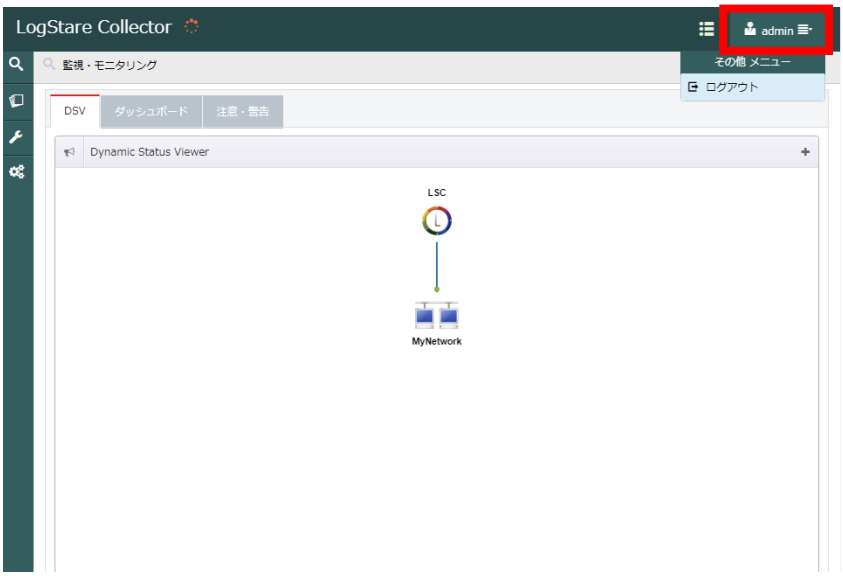
LogStare Collector トップ画面イメージ



※LogStare Collector への接続に失敗する場合は、OS のファイアウォール設定などをご確認ください。

【ログアウト方法】

画面右上にある「admin」にマウスカーソルを合わせます。



カーソルを合わせると「ログアウト」が表示されるので、「ログアウト」をクリックします。

ログアウトすると、LogStare Collector のログイン前の画面に切り替わります。

LogStare Collector のアップデート

Windows での LogStare Collector アップデート

ダウンロードした実行ファイル(exe ファイル)を以下の手順で実行し、セットアップを行います。

LogStare Collector を停止します。
（※Windows 版 LogStare Collector の起動と停止 参照）

LogStare Collector のインストールを行います。
（※Windows への LogStare Collector インストール 参照）

Linux での LogStare Collector アップデート

ダウンロードした実行ファイル(bin ファイル)を以下の手順で実行し、セットアップを行います。

LogStare Collector を停止します。

（※Linux 版 LogStare Collector の起動と停止 参照）

ターミナルウィンドウからコマンドを実行します。

コマンド「cd /ダウンロードファイルの保存先ディレクトリ」

コマンド「chmod +x logstare-collector-1.8.0-setup.bin」で実行権限を与えます。

コマンド「./logstare-collector-1.8.0-setup.bin」でセットアップが開始されます。

LogStare Collector のインストール先を指定して、「Enter」キーを押してください。
デフォルトとして「/usr/local」が設定されています。

```
=== LogStare Collector 初期設定 ===

LogStare Collector のインストール先を指定してください。デフォルトは /usr/local になります。
指定先に LogStare Collector が存在する場合はアップデートを行います。
[インストール先]：
```

「y」を押して「Enter」キーを押してください。インストールが開始します。

```
LogStare Collector が既にインストールされています。
LogStare Collector のアップデートを行いますか？[y]
```

以下の様にアップデートの進行状況が表示されます。

```
LogStare Collector アップデート中...
LogStare Collector のアップデートが完了しました。
```

正常にインストールが終了すると「LogStare Collector のアップデートが完了しました。」というメッセージが表示されます。
「Enter」キーを押して、プロンプト表示に戻ります。

LSCv1.7.1 以前から LSCv1.8.0 以降へアップデートする場合は、バージョンアップ後に Java:JDK12 を参照する設定へと変更する必要がございますので、以下の記事をご参照の上、設定をお願いいたします。
https://www.secuavail.com/product/logstarecollector/kb/references/ref-190606_01/

LogStare Collector 利用手順

デバイスを監視するまでの流れ

LogStare Collector でデバイスを監視するには、次の手順で設定を行います。

1．LogStare Collector利用環境設定

ログインパスワードの変更（必須）
メールアラートの設定など
目的にあわせてLogStare Collectorのご利用環境を設定していただけます。

2．LogStare Collector監視対象デバイス登録

お客様独自の監視単位グループを作成し監視対象デバイスを登録します。
登録されたデバイスは、スキャンを行うことで
監視推奨項目の検出・監視設定を行う事ができます。

3．登録デイバスへの監視/収集設定

登録された監視対象デバイスに対して、監視及び収集設定を行います。
設定した閾値やキーワードに合致した場合にアラートメール通知などを
行うことができます。

4．監視状況確認

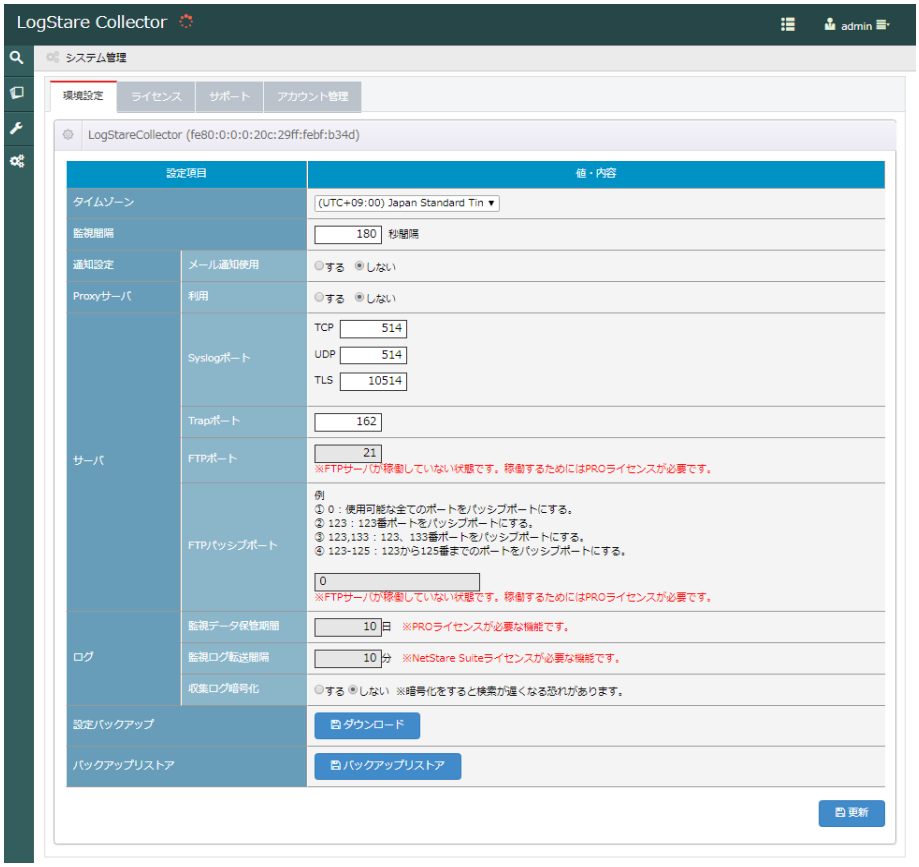
Dynamic Status Viewer（DSV）やダッシュボード画面で
監視デバイスのアラート状況やトラフィック、リソース状況などを視覚的に確認できます。
また、この確認結果から対象ログの抽出などにより具体情報の確認も行えます。

LogStare Collector 利用環境の設定

ここでは、LogStare Collector を利用する際の各種設定に関する手順を記載しています。

メニューの「システム管理」から「環境設定」をクリックします。

【システム管理画面】



メールの通知設定

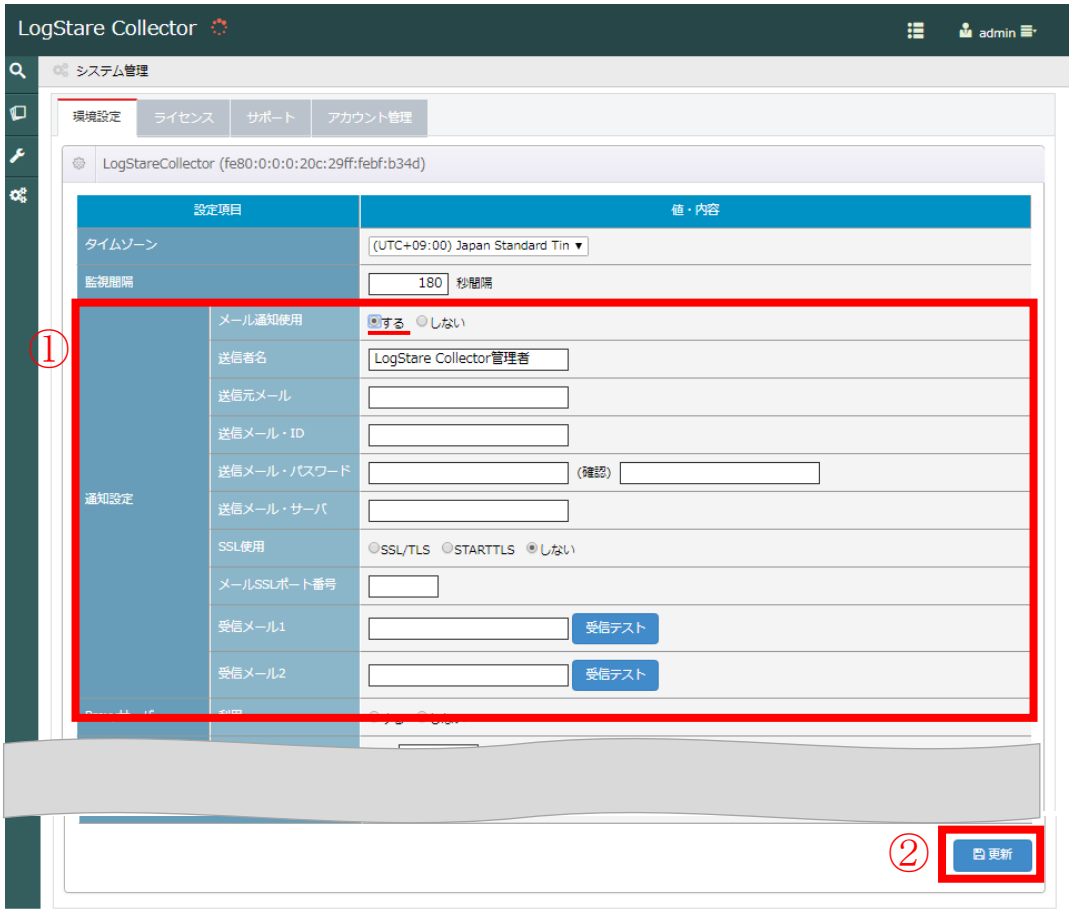
メール通知を設定する手順を記載しています。
各監視設定でメールアラート通知を行う場合この設定が必要です。

「メール通知使用」項目で「する」にチェックします。

①表示された「通知設定」項目で設定を行います。

※受信テストは必ず行ってください。

②「更新」をクリックします。



更新確認画面が表示されますので「はい」をクリックします。

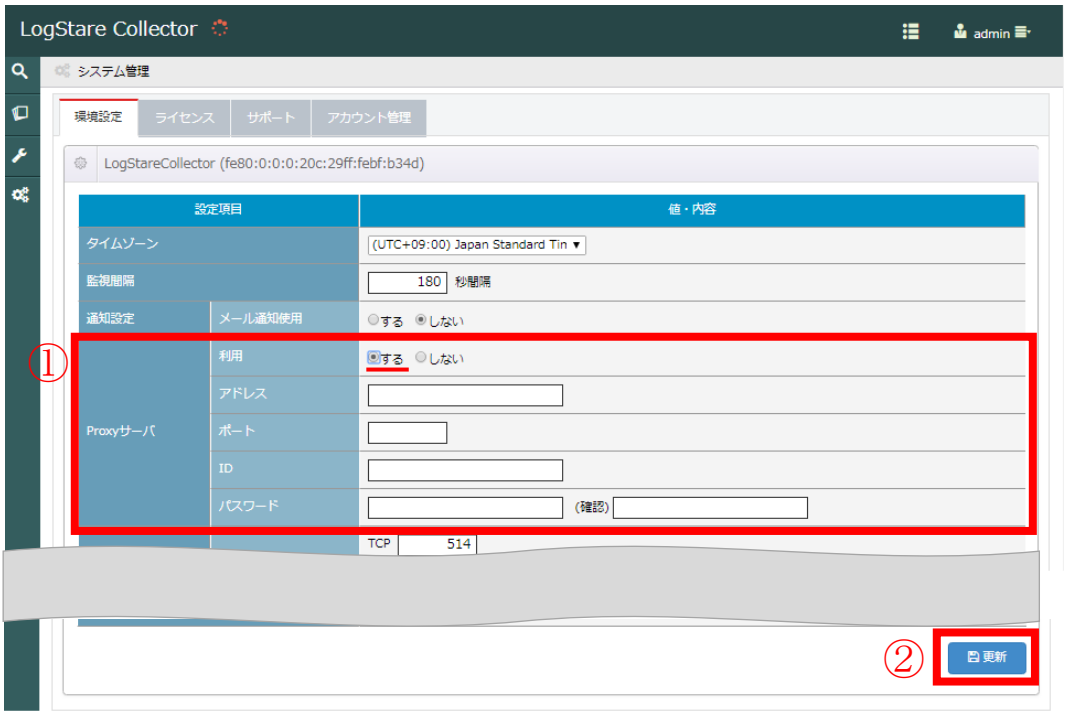
Proxy サーバを設定

Proxy サーバを設定する手順を記載しています。

「Proxy サーバ」項目の「利用」で「する」にチェックします。

① 表示された「Proxy サーバ」項目で設定を行います。

② 「更新」をクリックします。



更新確認画面が表示されますので「はい」をクリックします。

任意ポートの設定

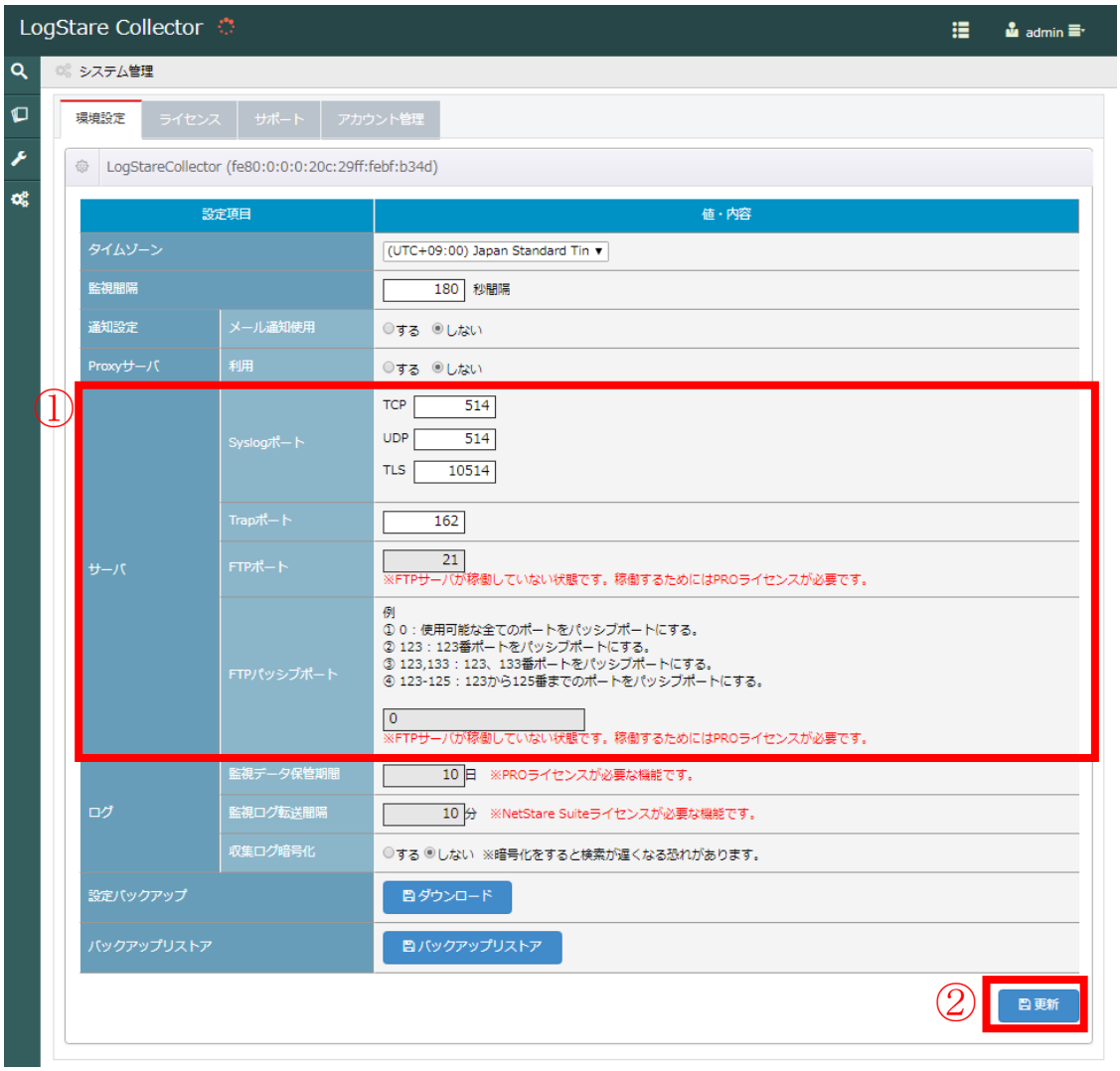
監視での利用ポートを任意ポートに設定する手順を記載しています。
ここでは「SYSLOG ポート」「SNMP Trap ポート」「FTP ポート」「FTP パッシブポート」のポート番号を任意に設定することができます。

「サーバ」項目で変更します。

①任意のポートを設定します。

※1023 以下のポート番号はウェルノウンポートの為、非推奨です。

②「更新」をします。



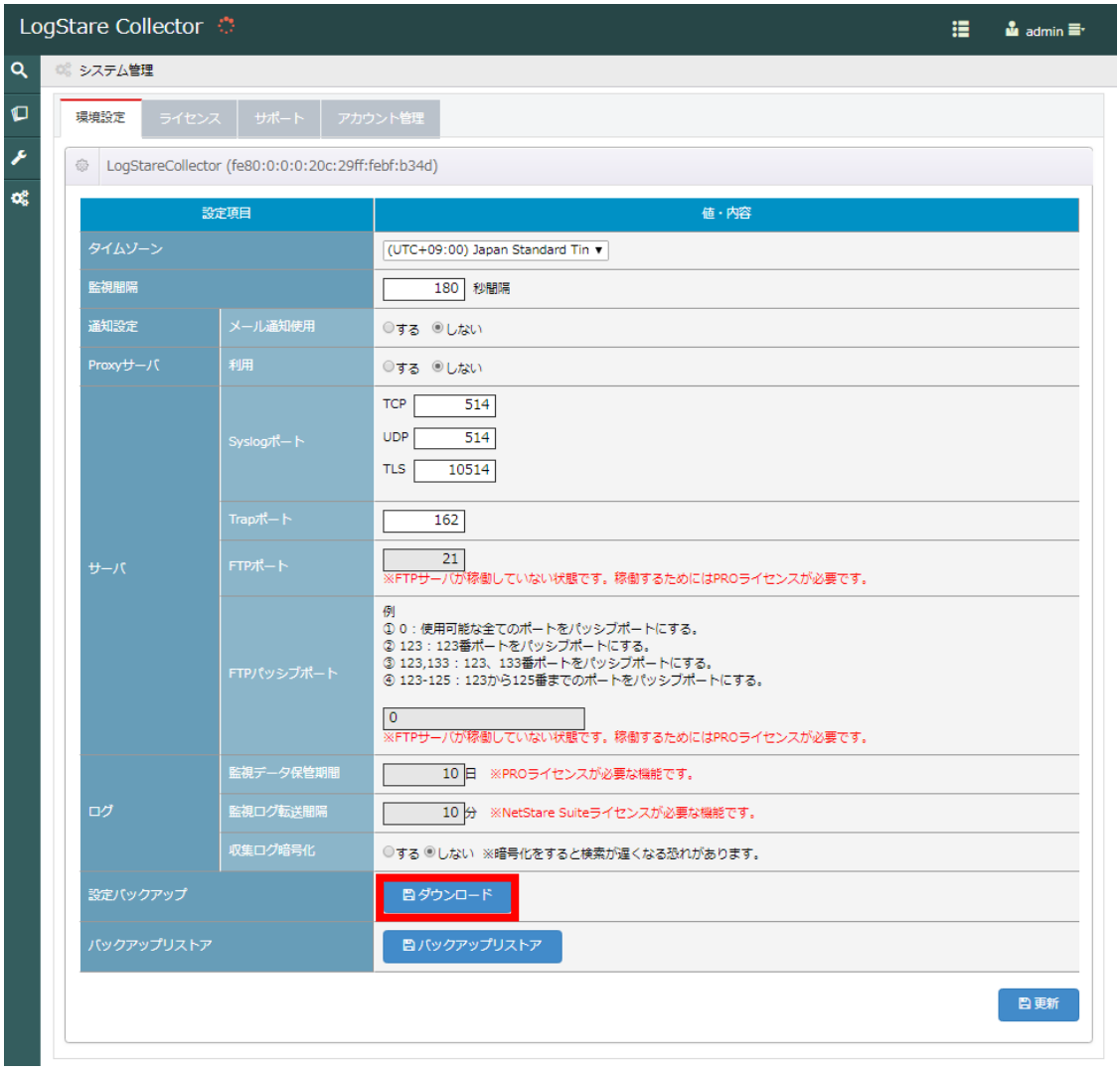
更新確認画面が表示されますので「はい」をクリックします。

設定バックアップの取得手順

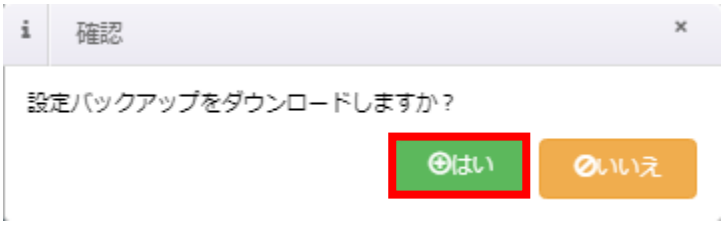
設定バックアップの取得手順を記載しています。

※ログデータのバックアップは保存されません。

設定バックアップの「ダウンロード」を選択します。



表示された「確認」画面の「はい」をクリックします。

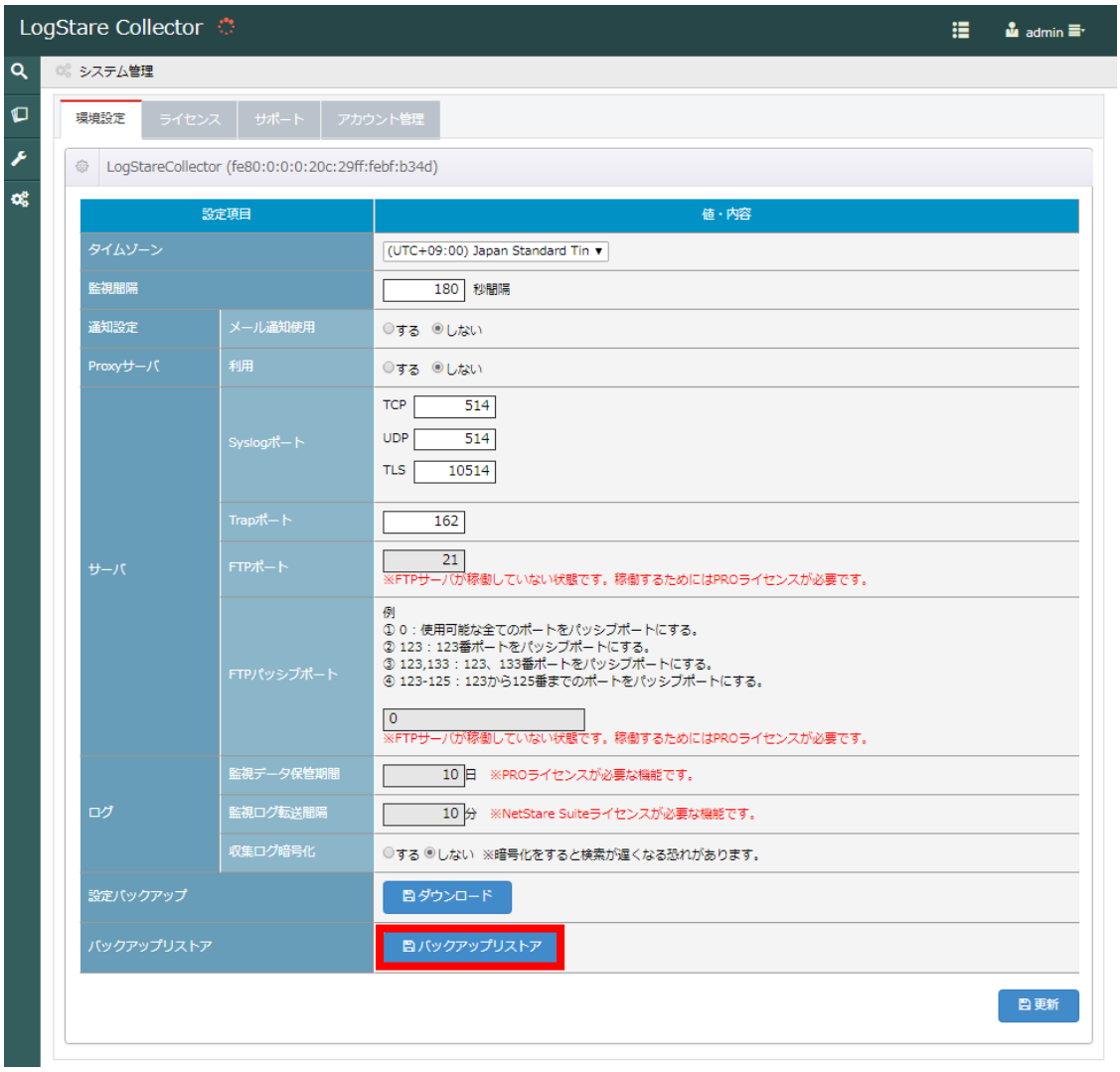


ファイル名「lsc_backup_xxxxxxxx.bak」がローカルに保存されます。

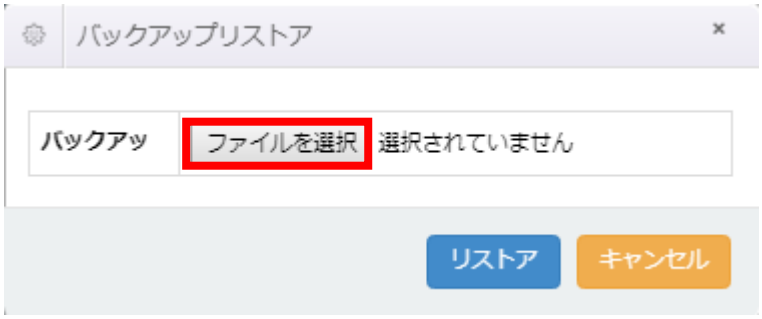
バックアップリストア手順

設定バックアップの取得手順を記載しています。

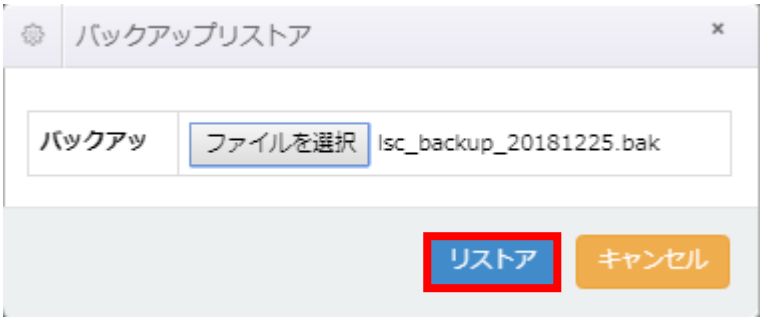
バックアップリストアの「バックアップリストア」を選択します。



表示された「バックアップリストア」画面の「ファイル選択」をクリックします。

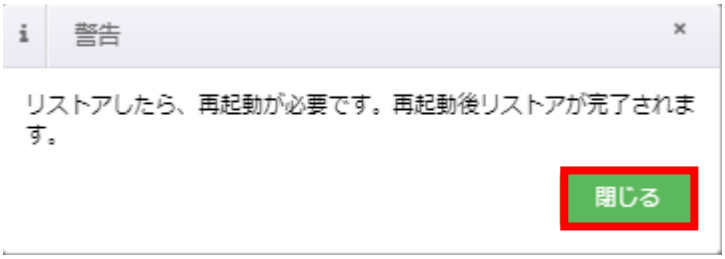


バックアップファイルを選択して、「リストア」をクリックします。



更新確認画面が表示されますので「はい」をクリックします。

警告画面が表示されますので「閉じる」をクリックし、LogStare Collector を再起動します。
（※Windows 版 LogStare Collector の起動と停止 参照）
（※Linux 版 LogStare Collector の起動と停止 参照）



監視基本設定

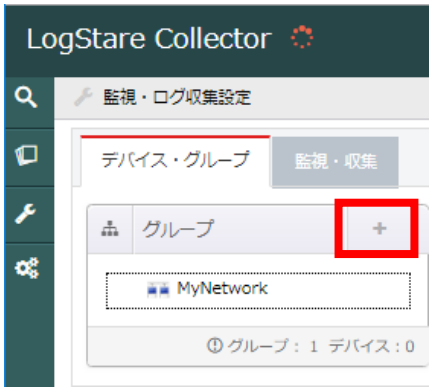
グループの作成

LogStare Collector 上での管理用グループを設定する手順を記載しています。

デバイスを監視するには、監視するデバイスを LogStare Collector 上の管理用グループに登録する必要があります。初期設定で「MyNetwork」が生成されていますが、グループは目的に応じて任意で作成することができます。

メニューの「監視・ログ収集設定」から「デバイス・グループ」をクリックします。

表示された「監視・ログ収集設定」画面のグループの「＋」をクリックします。



表示されたグループ追加画面で、親グループを選択してください。(最上位)ならば一番上に追加され、グループを選択すれば、そのグループの配下にグループが追加されます。

作成グループ名とアイコンを指定します。

①グループ名のテキストボックスに、任意のグループ名を入力します。

②Dynamic Status Viewer で表示されるアイコンを選択します。

③「追加」をクリックします。

追加確認画面が表示されますので「はい」をクリックします。

「グループ」に追加されたことが確認できたらグループ設定作業は完了です。
グループを複数作成したい場合はこの操作を繰り返します。

監視対象デバイスの設定

LogStare Collector 上の監視対象のデバイスを設定する手順を記載しています。

【デバイスを設定】

LogStare Collector では「サーバ」、「ファイアウォール」、「L2/L3 スイッチ」など多種多様なデバイスを監視することができ、デバイスごとに監視項目や収集するログを設定できます。

メニューの「監視・ログ収集設定」から「デバイス・グループ」をクリックします。

表示された「監視・ログ収集設定」画面で、デバイスを追加するグループを選択します。

①デバイスを追加する「グループ」を選択してください。

②「＋」をクリックします。

表示された「デバイス追加」画面で追加するデバイス情報を設定します。

①監視デバイスの情報を設定します。下図の例では SNMP バージョン 2 を選択した場合の設定画面です。

※無償版では監視データ保管期間及び収集ログ保管期間は 10 日固定です。

②「追加」をクリックします。

登録確認画面が表示されますので「はい」をクリックします。

デバイスが追加されたことを確認したらデバイス設定作業は完了です。

デバイスを複数設定したい場合はこの操作を繰り返します。

SNMP 情報で設定する項目は、選択したバージョンによって必要な入力情報が異なります。
SNMP バージョン 3 を選択した場合は以下の情報を設定します。

バージョン 3 を選択した場合、選択した「セキュリティレベル」によって入力が必要な項目が変わります。
①「セキュリティレベル」に合わせて必要な項目を入力します。
②「追加」をクリックします。

登録確認画面が表示されますので「はい」をクリックします。

監視対象デバイスの設定変更及び削除

【監視対象デバイス設定の変更】

「デバイス一覧」から設定情報を変更するデバイスをクリックします。

表示された「デバイス更新」画面で設定情報の変更を行います。

①表示された「デバイス更新」の画面で設定値を変更します。

②「更新」をクリックします。

更新確認画面が表示されますので「はい」をクリックします。

【監視対象デバイスの削除】

「デバイス一覧」から削除する項目をクリックします。

表示された「デバイス更新」画面で「削除」をクリックします。

削除確認画面が表示されますので「はい」をクリックします。

スキャンで取得した監視項目の設定

監視項目スキャンとは監視を推奨している項目について自動的に検出して監視項目を設定します。
監視項目スキャンで収集されない項目については「監視・収集」から別途設定することができます。
ここでは、監視項目スキャンで検出された監視項目を設定する方法を記載しています。

【監視項目スキャン】

「デバイス一覧」から監視項目スキャンを実施する項目をクリックします。

「監視項目スキャン」をクリックします。
デバイスに対して監視項目を自動的に検出します。監視項目の設定は行われません。

「監視項目スキャン」の結果がボタンの下に表示されます。
スキャン結果は下図のように監視項目ごとに（PING、SNMP）タブが分かれて表示されます。

※監視対象デバイスの SNMP バージョンとコミュニティとが一致していないと監視項目は
スキャンされませんのでご注意ください。

「監視項目スキャン」の結果を監視項目として追加することができます。監視項目追加方法はスキャン結果から特定の監視項目を追加する方法と、全ての項目を追加する方法の 2 種類があります。

【特定の監視項目を追加する手順】

スキャン結果から特定の項目を監視項目として追加する手順です。

①追加したい監視項目のラジオボタンをクリックして選択する。

※無償版では監視項目に設定できる項目数は 1 デバイスあたり 5 個までとなります。

②「監視項目追加」ボタンをクリックする。

追加確認画面が表示されますので「はい」をクリックします。

これで、スキャン結果から選択した監視項目が「監視・収集」に追加されます。

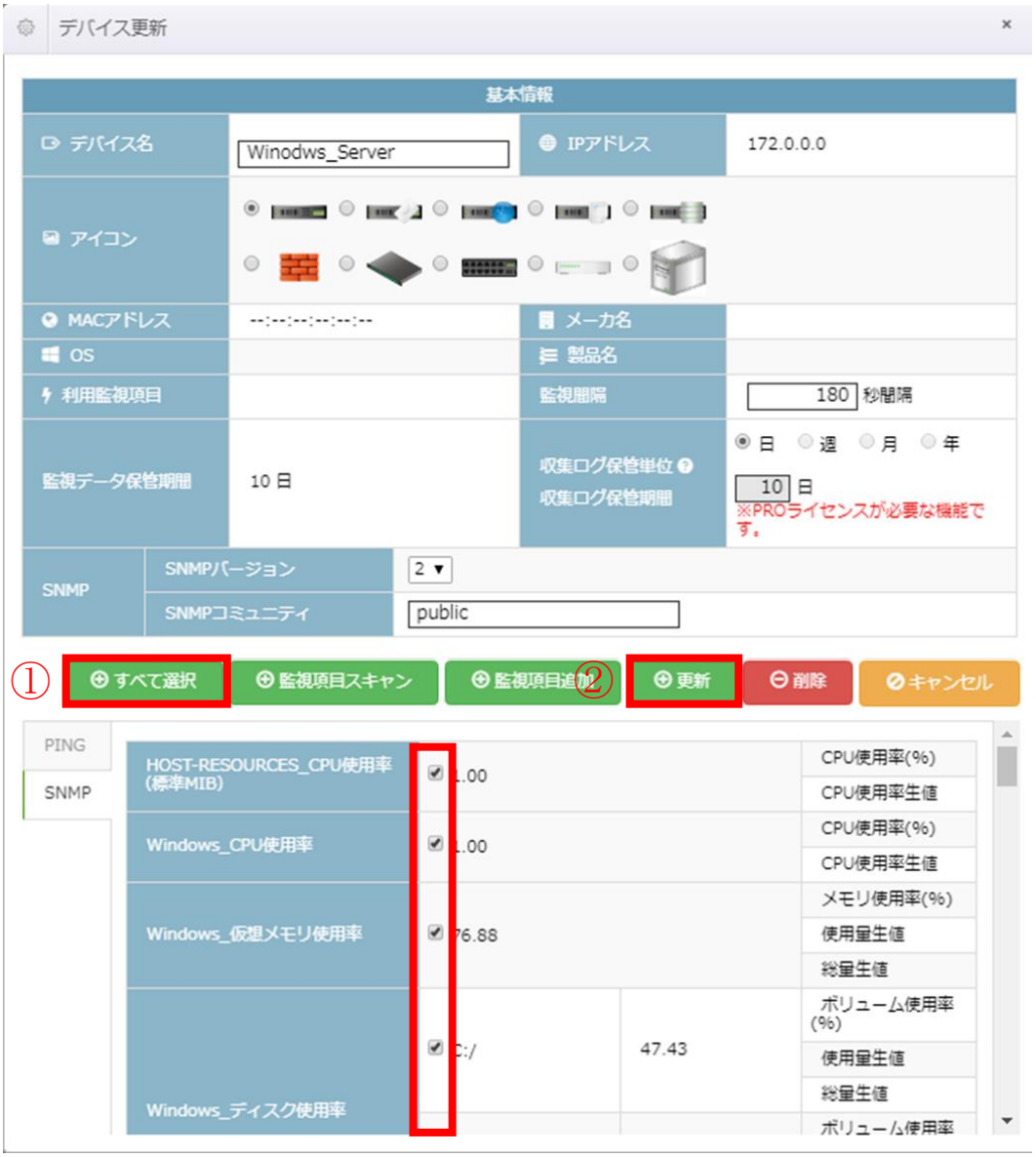
【全ての項目を追加する手順】

スキャン結果の全ての項目を監視項目として追加する手順です。

①「すべて選択」ボタンをクリックする。「監視項目スキャン」の結果が全て選択される。

※無償版では監視項目に設定できる項目数は 1 デバイスあたり 5 個までとなます。

②「監視項目追加」ボタンをクリックする。



追加確認画面が表示されますので「はい」をクリックします。

これで、スキャン結果の全ての監視項目が「監視・収集」に追加されます。

監視及びログ収集設定

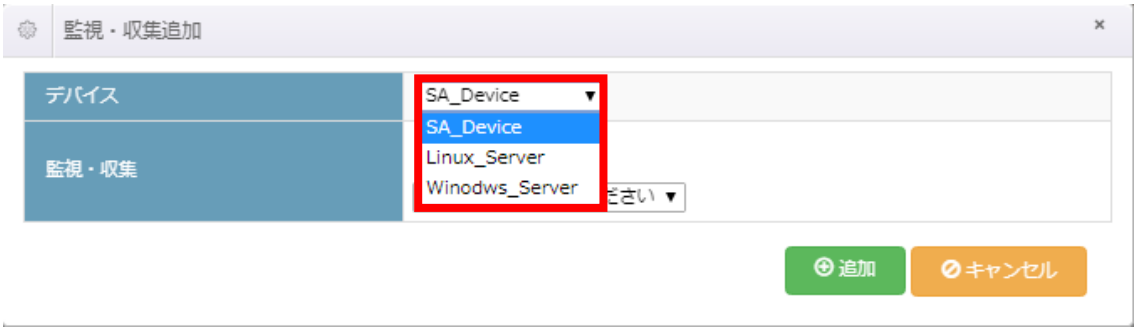
設定対象デバイスの選択

ここでは、作成したデバイスの監視及び情報収集の設定手順を記載しています。
設定項目として、「PING 監視」、「SNMP 監視」、「PORT 監視」、「SNMP トラップ監視」、「WMI 取得」、「SYSLOG 収集」の項目があります。

メニューの「監視・ログ収集設定」から「監視・収集」をクリックします。

監視・収集一覧の「＋」をクリックします。

表示された「監視・収集追加」画面から設定対象のデバイスをプルダウンメニューから選択します。



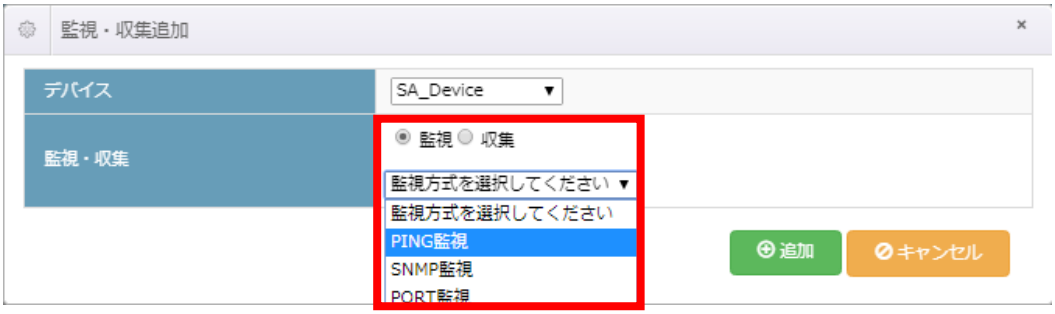
次に「監視・収集項目」を設定します。

PING 監視の設定

選択したデバイスに対して、PING 監視を設定する手順を記載しています。

【PING 監視設定】

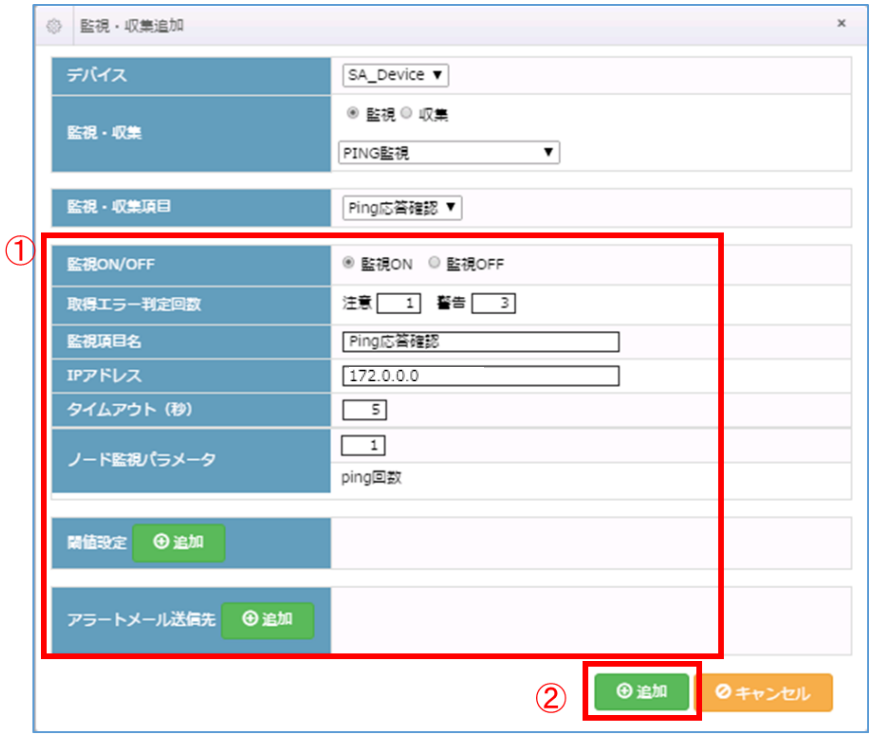
「監視・収集」項目の「監視」ボタンを選択し、プルダウンメニューから「PING 監視」を選択します。



表示された項目に PING 監視情報を設定します。

①PING 回数、閾値、アラート通知など必要な設定を行います。

②「追加」をクリックします。



追加確認画面が表示されますので「はい」をクリックします。

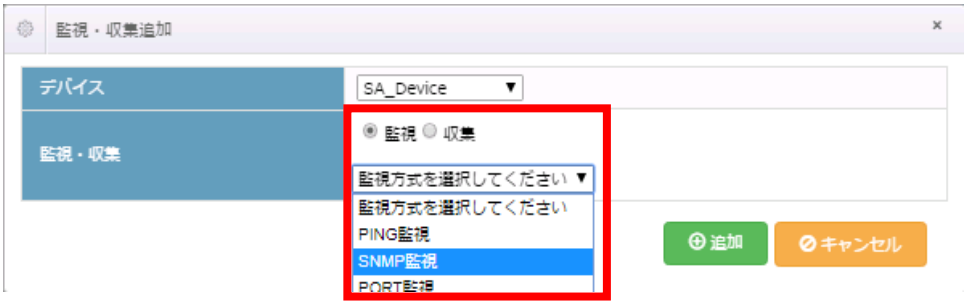
SNMP 監視の設定

選択したデバイスに対して SNMP 監視を設定する手順を記載しています。

※監視対象デバイスの SNMP Service が開始状態で、LogStare Collector からの SNMP パケットを受け付ける設定が事前に必要です。

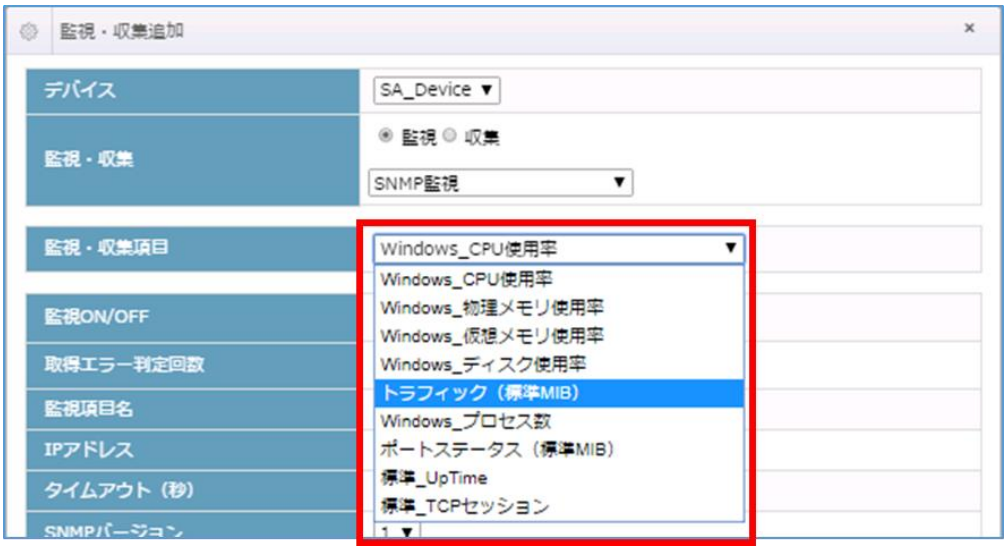
【SNMP 監視設定】

「監視・収集」項目の「監視」ボタンを選択し、プルダウンメニューから「SNMP 監視」を選択します。



選択デバイスに応じて「監視・収集項目」のプルダウンメニューに表示される項目が変わります。

下図は Windows の SNMP 監視項目のプルダウンメニュー表示です。



以下の手順は、例として「監視・収集項目」を「トラフィック（標準 MIB）」を選択した場合の画面を記載しています。

①「監視収集項目」のプルダウンメニューから「トラフィック監視（標準 MIB）」を選択します。

②表示された「SNMP（トラフィック監視）」項目に必要な設定を行います。

③「追加」をクリックします。

追加確認画面が表示されますので「はい」をクリックします。

PORT 監視の設定 有償版限定

選択したデバイスに対して PORT 監視を設定する手順を記載しています。

【PORT 監視設定】

「監視・収集」項目の「監視」ボタンを選択し、プルダウンメニューから「PORT 監視」を選択します。

表示された「監視収集追加」画面で PORT 監視情報を入力します。

①PORT 監視情報を設定します。

②「追加」をクリックします。

追加確認画面が表示されますので「はい」をクリックします。

SNMP トラップ監視の設定

選択したデバイスに対して SNMP トラップ監視を設定する手順を記載しています。
対象機器から SNMP トラップを検知した場合、設定項目と一致したものがあればメール通知を行うための設定です。

【SNMP トラップ監視設定】

「監視・収集」項目の「監視」ボタンを選択し、プルダウンメニューから「SNMP トラップ監視」を選択します。

※この項目は 1 デバイスにつき、1 つしか設定ができません。

表示された項目に SNMP トラップ監視情報を設定します。

①SNMP バージョン、コミュニティ名、OID など SNMP トラップ検知に必要な情報を設定します。

※OID とインスタンス値が完全一致していない場合、SNMP トラップ監視はできません。
設定は最大 5 つまで設定が可能です。

②「追加」をクリックします。

追加確認画面が表示されますので「はい」をクリックします。

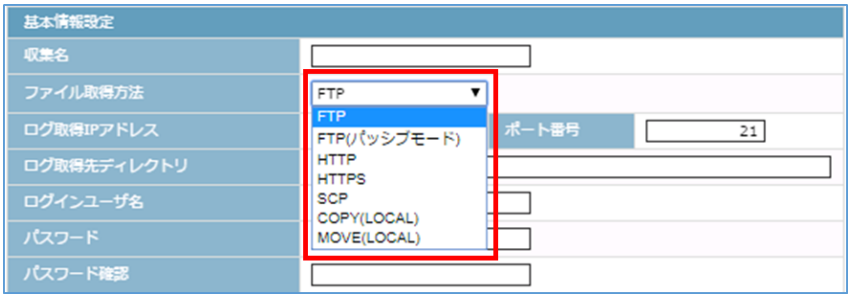
ファイル収集/ログ監視の設定 有償版限定

選択したデバイスに対してファイル収集を設定する手順を記載しています。
監視対象デバイスに保管されているログファイルなどを取得することができます。

【ファイル収集設定】

「監視・収集」項目の「収集」ボタンを選択し、プルダウンメニューから「ファイル収集」を選択します。

表示されたファイル収集設定項目から、まずは「基本情報設定」として「収集名」、「ファイル取得方法」取得先機器のログイン情報などを設定します。



ファイル収集方法は
・監視対象デバイスからのファイル収集：「FTP」、「FTP(パッシブモード)」、「HTTP」、「HTTPS」、「SCP」
・LogStare Collector サーバのファイル収集：「COPY(LOCAL)」、「MOVE(LOCAL)」
の 2 タイプ毎に設定項目が異なります。

下図の例では「FTP」を選択しています。

①ファイル取得情報を設定します。

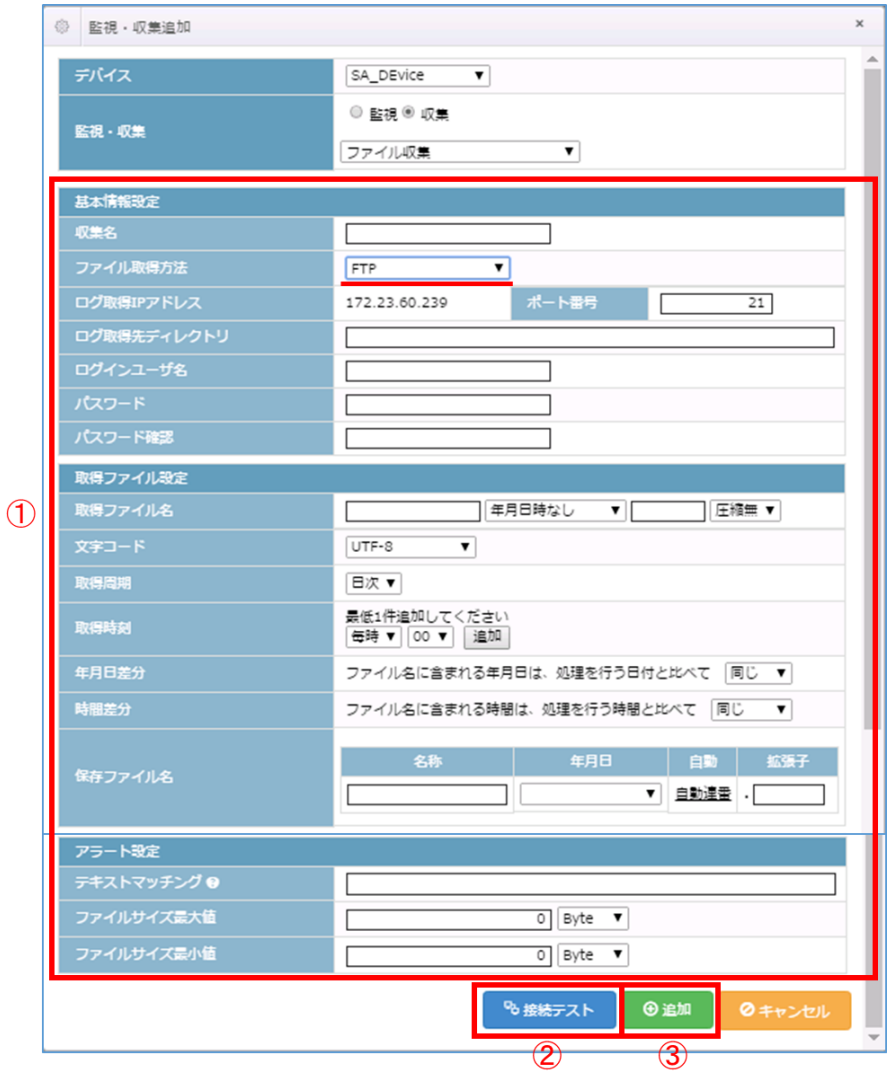
※取得時刻は必ず設定してください。取得するファイル名に hh の情報がない場合は、日単位（1 日 1 回のみ）の取得となります。

②「接続テスト」をクリックします。（設定した情報で対象デバイスへの接続確認を行います。）

※対象機器との疎通、ポート開放状態確認を接続テスト画面に表示します。

なお、このテストは対象機器にログインが出来たか否かの判断はできません。

③「接続テスト」に成功したら「追加」をクリックします。



追加確認画面が表示されますので「はい」をクリックします。

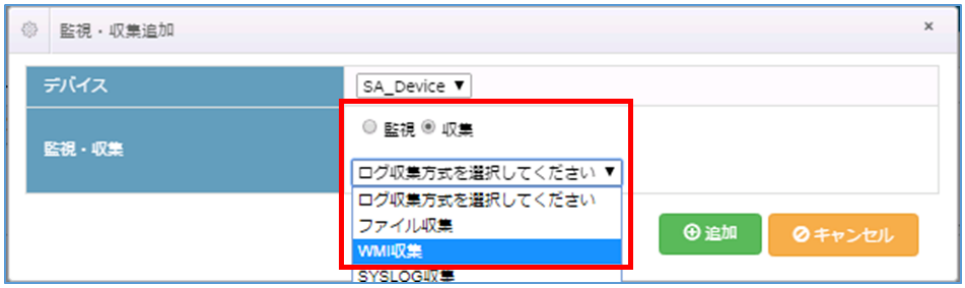
WMI 収集の設定

選択した Windows デバイスに対して WMI によるイベントログ収集を行う方法を記載しています。

【WMI 取得設定】

「監視・収集」項目の「収集」ボタンを選択し、プルダウンメニューから「WMI 収集」を選択します。

※この項目は 1 デバイスにつき、1 つしか設定ができません。



表示された WMI 用「監視・収集追加」画面にて設定を行います。

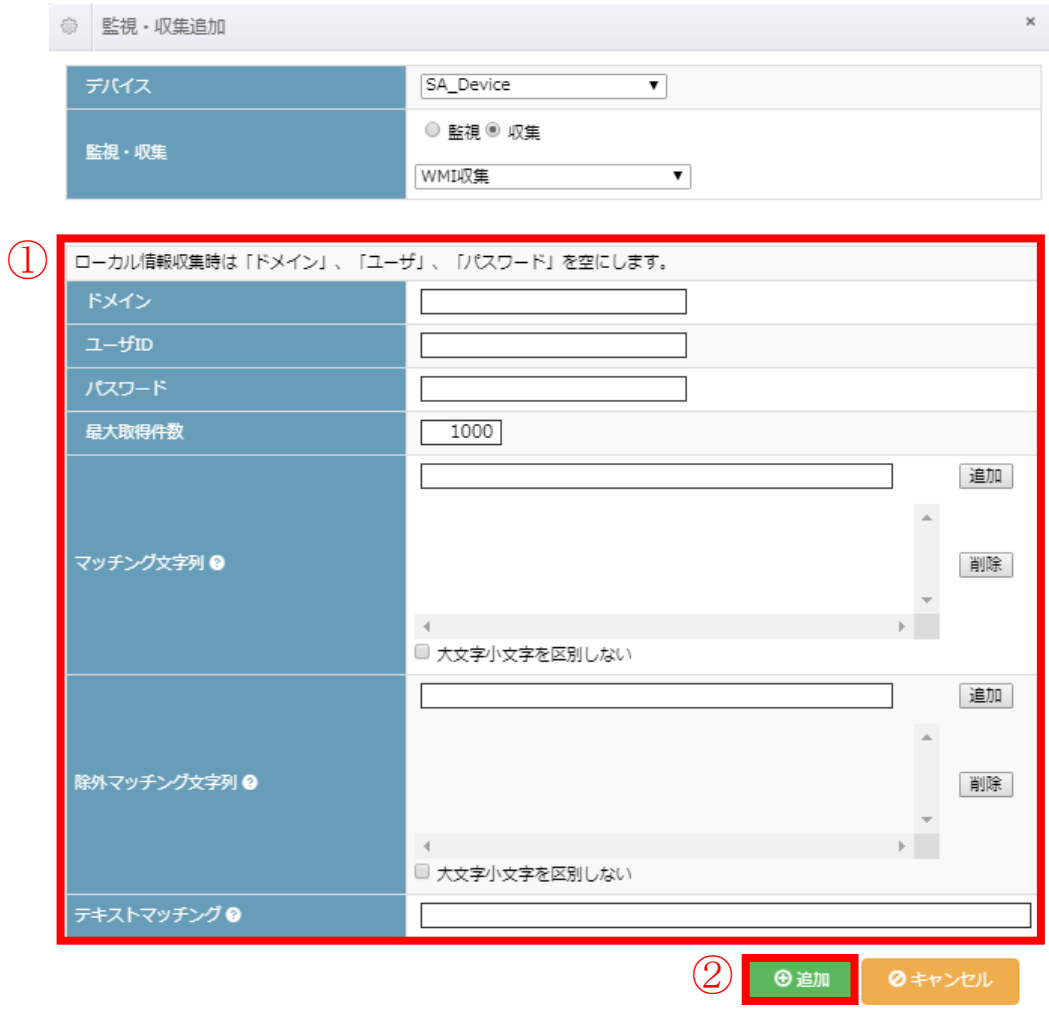
① WMI 収集情報を入力します。

※『ローカル情報取得時は「ドメイン」、「ユーザ」、「パスワード」を空にします』とは
LogStare Collector をインストールしている Windows 自身への情報取得を指します。
リモートでの情報取得時は、ビルトインの Administrator アカウントでの設定を推奨します。
追加アカウントの場合は、WMI 通信やイベントログへのアクセスに必要な権限が無いと
WMI 収集が失敗したり、取得できないイベントログが発生する可能性があります。

※マッチング文字列設定項目を設定時の WMI 収集動作は下表のとおりです。

設定項目	設定内容	ログ取得内容
マッチング文字列	文字列設定なし	全てのログを収集する。
除外マッチング文字列	文字列設定なし	
マッチング文字列	文字列設定あり	マッチング文字列に一致したログを取得する。
除外マッチング文字列	文字列設定あり	除外マッチング文字列以外を取得する。
マッチング文字列	文字列設定あり	除外マッチング文字列以外でマッチング文字列に合致したログを取得する。
除外マッチング文字列	文字列設定あり	

※テキストマッチング項目では、「マッチング文字列」「除外マッチング文字列」の選別結果に対して設定した文字列がマッチした場合に、メール通知されます。



②「追加」をクリックします。

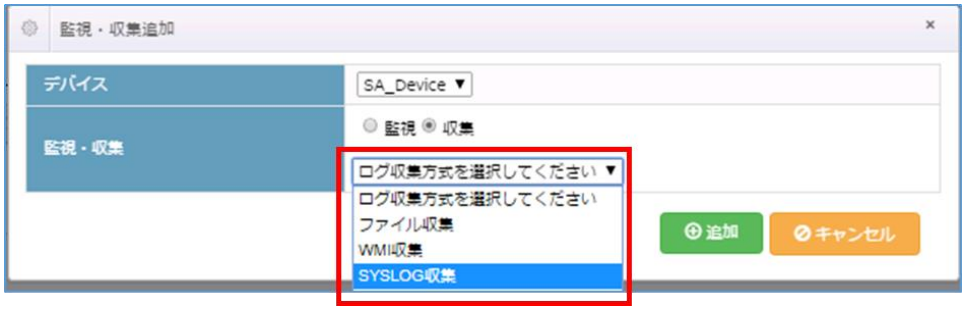
追加確認画面が表示されますので「はい」をクリックします。

SYSLOG 収集/ログ監視の設定

「共通監視設定」にて選択したデバイスに対して SYSLOG を収集する方法を記載しています。

【SYSLOG 収集設定】

「監視・収集」項目の「収集」ボタンを選択し、プルダウンメニューから「SYSLOG 収集」を選択します。



表示された「監視・収集追加」画面にて SYSLOG 収集に必要な設定を行います。

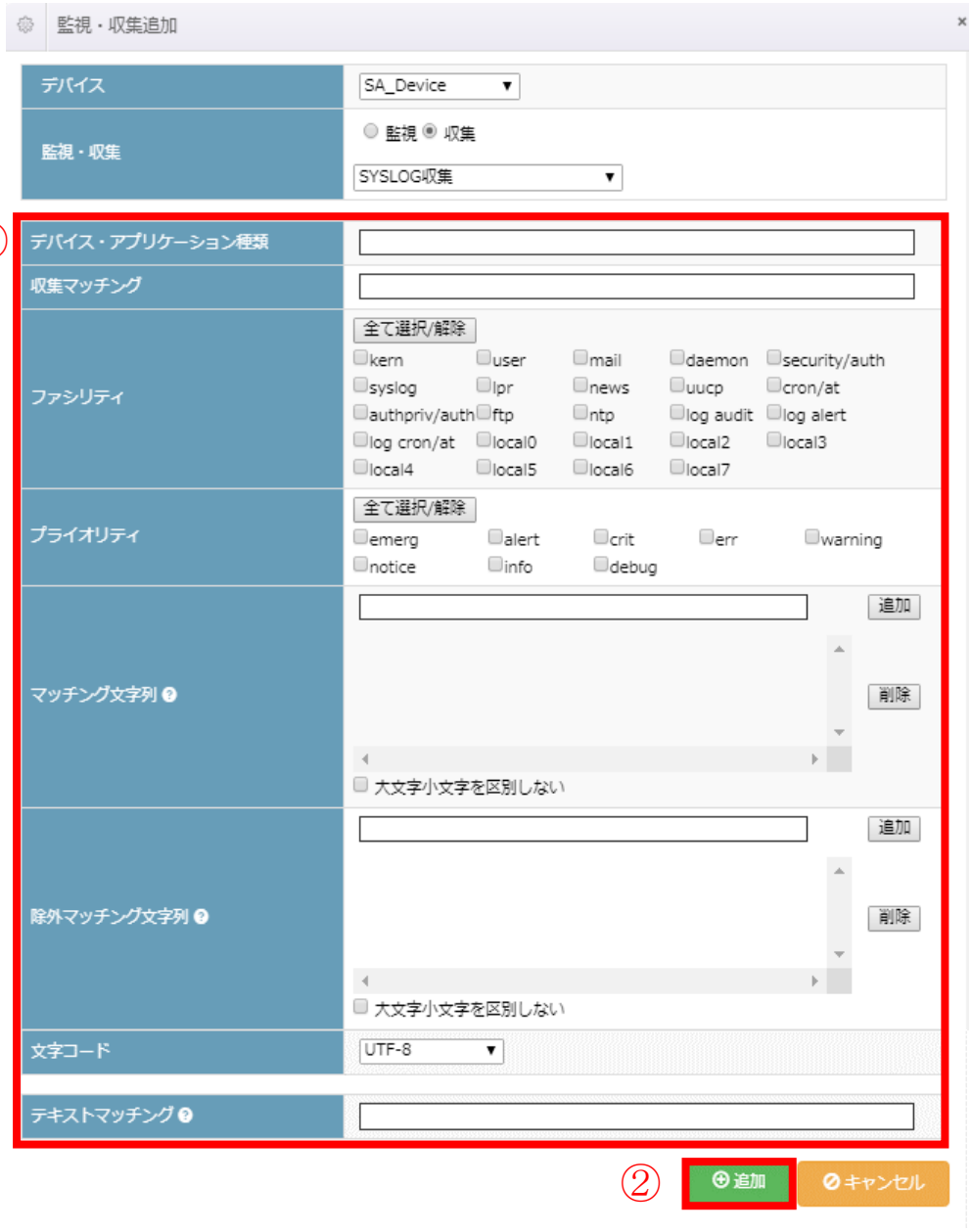
①SYSLOG 収集情報を設定します。

※マッチング文字列設定項目を設定時の SYSLOG 取得動作は下表のとおりです。

設定項目	設定内容	ログ取得内容
マッチング文字列	文字列設定なし	全てのログを収集する。
除外マッチング文字列	文字列設定なし	
マッチング文字列	文字列設定あり	マッチング文字列に一致したログを取得する。
除外マッチング文字列	文字列設定あり	除外マッチング文字列以外を取得する。
マッチング文字列	文字列設定あり	除外マッチング文字列以外でマッチング文字列に合致したログを取得する。
除外マッチング文字列	文字列設定あり	

※文字コード設定項目で「指定なし」を選択した場合は、「UTF-8」として処理が行われます。

※テキストマッチング項目では、「マッチング文字列」「除外マッチング文字列」の選別結果に対して設定した文字列がマッチした場合に、メール通知されます。



②「追加」をクリックします。

追加確認画面が表示されますので「はい」をクリックします。

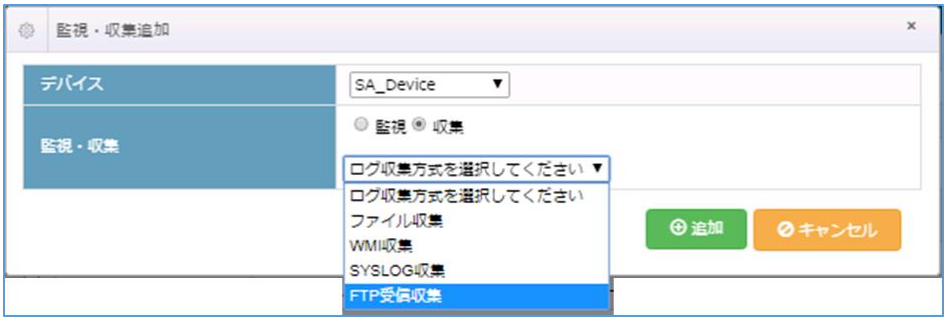
FTP 受信収集/ログ監視の設定 有償版限定

LogStare Collector に FTP サーバを立て、FTP サーバに置かれたファイルを収集するための設定方法を記載しています。

※LogStare Collector が立てた FTP サーバは、ファイルを置く(PUT)処理のみ可能です。

【FTP 受信収集設定】

「監視・収集」項目の「収集」ボタンを選択し、プルダウンメニューから「FTP 受信収集」を選択します。



表示された「監視・収集追加」画面にて FTP 受信収集に必要な設定を行います。

①FTP 受信収集情報を設定します。

※ログインユーザ名及びパスワード項目では、ファイルサーバへアクセスする際のユーザ名とパスワードを設定してください。

※取得ファイル名項目では取得ファイルの拡張子も入力してください。
また圧縮形式のファイル取得する場合は圧縮形式の場合は必ず選択してください。

※取得時刻項目は必ず設定してください。取得するファイル名に hh の情報がない場合は、日単位(1 日 1 回のみ)の取得となります。

※アラート設定でのファイルサイズで検知を行った場合でも、ファイル収集は行われています。

※取得できるファイルの最大値は 4GByte までです。4GByte を超えるサイズのファイルは収集されません。

②「追加」クリックします。

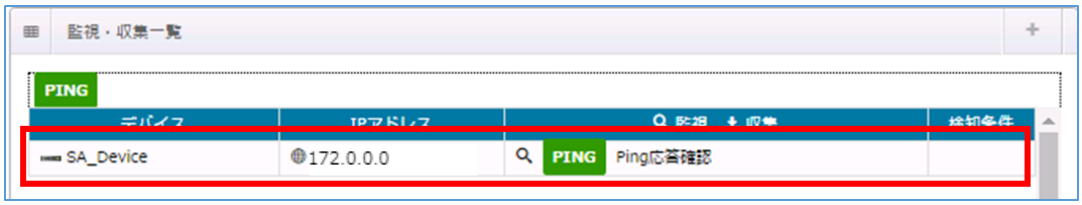
追加確認画面が表示されますので「はい」をクリックします。

監視及び収集設定の設定変更と削除

これまで設定した監視及び収集設定の変更と削除の手順を記載しています。
以下の例では PING 監視の設定変更と削除の手順を記載しています。

【PING 監視設定情報の変更】

「監視・収集一覧」から変更する項目をクリックします。

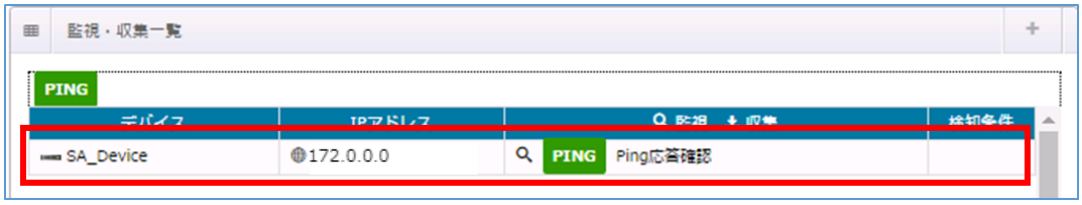


「監視・収集変更」の画面で情報の変更を行い、「更新」をクリックします。

更新確認画面が表示されますので「はい」をクリックします。

【PING 監視設定の削除】

監視・収集一覧」から削除する項目をクリックします。



「監視・収集変更」の画面で「削除」をクリックします。

削除確認画面が表示されますので「はい」をクリックします。

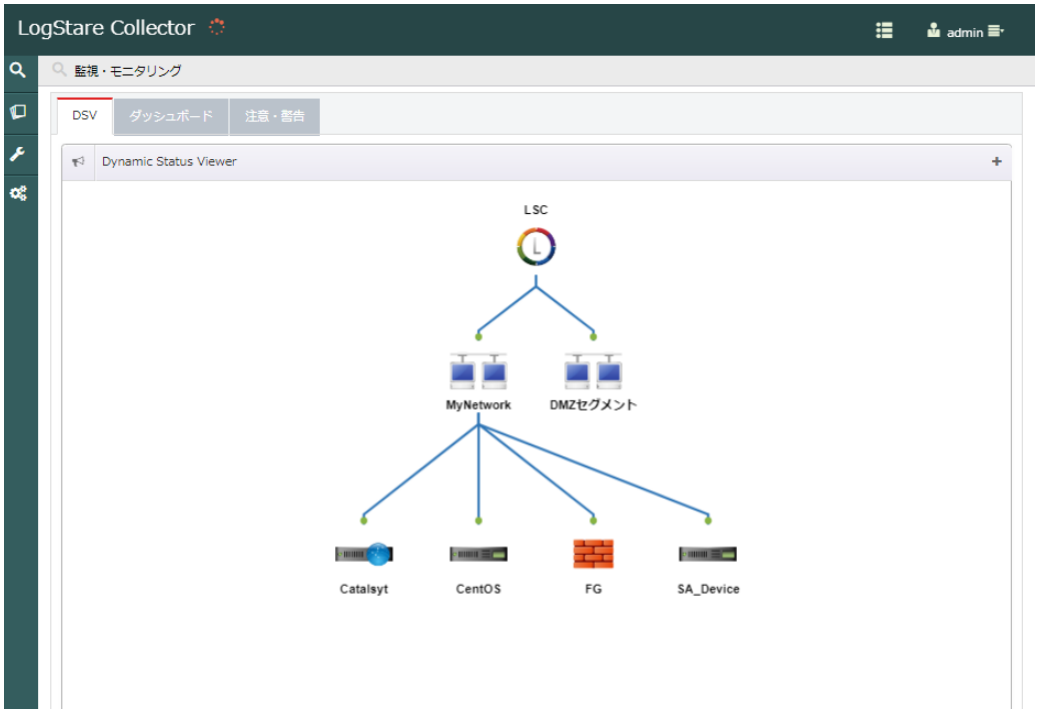
LogStare Collector で収集した情報の確認

LogStare Collector では、監視対象デバイスのログを収集することができます。設定を追加することによってグラフなどで視覚的に確認し、閾値を設定して警告通知することができます。

※無償版は収集したログは収集日から 10 日間保持します。

Dynamic Status Viewer の確認と編集

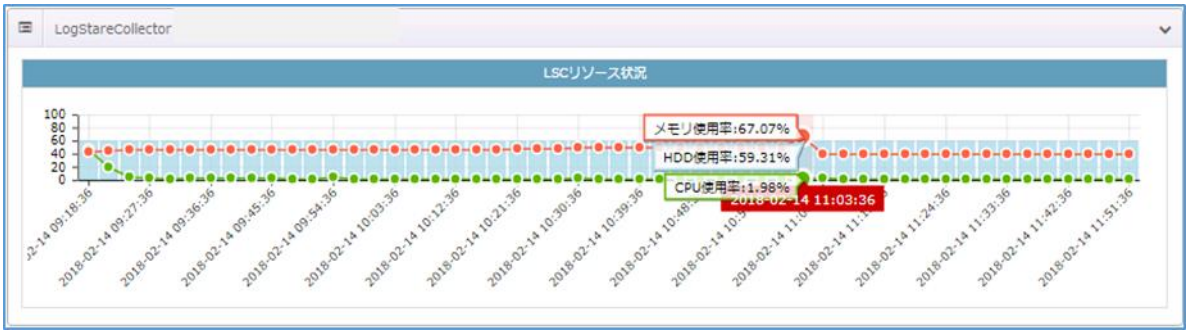
LogStare Collector にログインした際にはまずこの画面が表示されます。ここでは LogStare Collector をインストールしているサーバの状態と監視対象デバイスのマッピング情報が確認できます。登録済のデバイスの集約管理情報が Dynamic Status Viewer(略称:DSV)で表示されます。サーバが安定稼働していることやどのデバイスがどのグループに紐づいているのか、視覚的に確認できます。



メニューからは「監視・モニタリング」の「DSV」で表示ができます。

【LogStare Collector を起動しているサーバのシステム情報】

「DSV」画面上の「LSC リソース状況」にて LogStare Collector をインストールしているサーバの「メモリ使用率」、「CPU 使用率」、「HDD 使用率」を表示します。



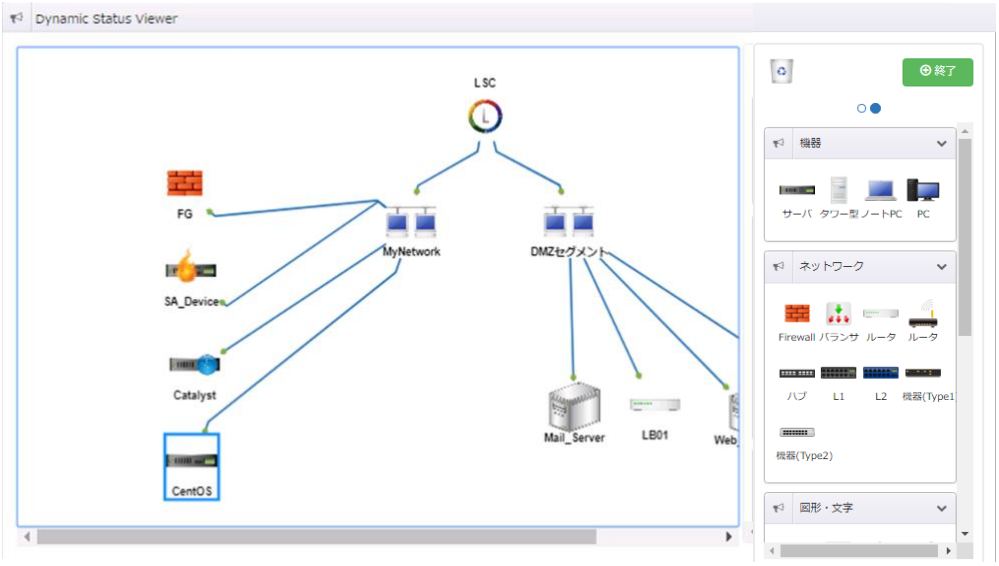
グラフ上にマウスを合わせると上図のように使用率値が表示されます。

これらの値から、LogStare Collector サーバの稼働状態を常に確認することができます。

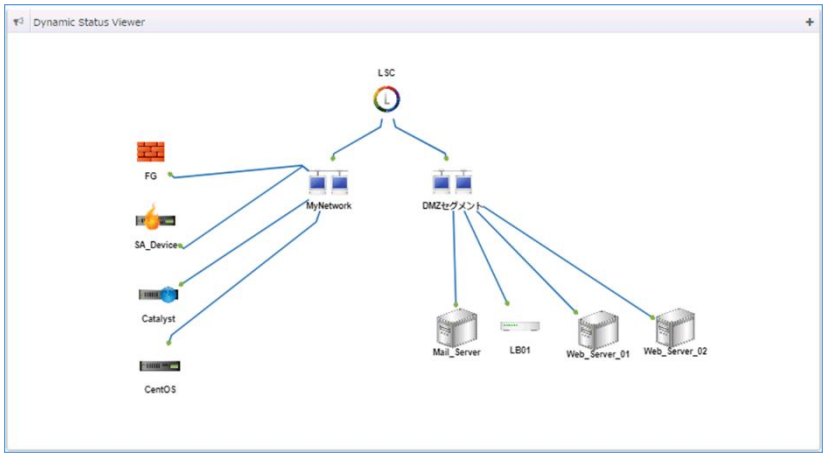
※自動設定で収集している為、設定の変更等はできません。

【Dynamic Status Viewer を確認】

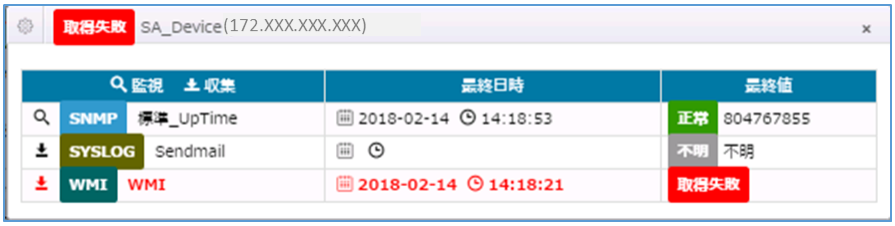
表示されるグループやデバイスのアイコンは、DSV メニューを開き、DSV 画面上でドラッグして自由に位置を調整することができます。



DSV 画面で、確認したいデバイスアイコンをダブルクリックすると、デバイスの状態情報が表示されます。



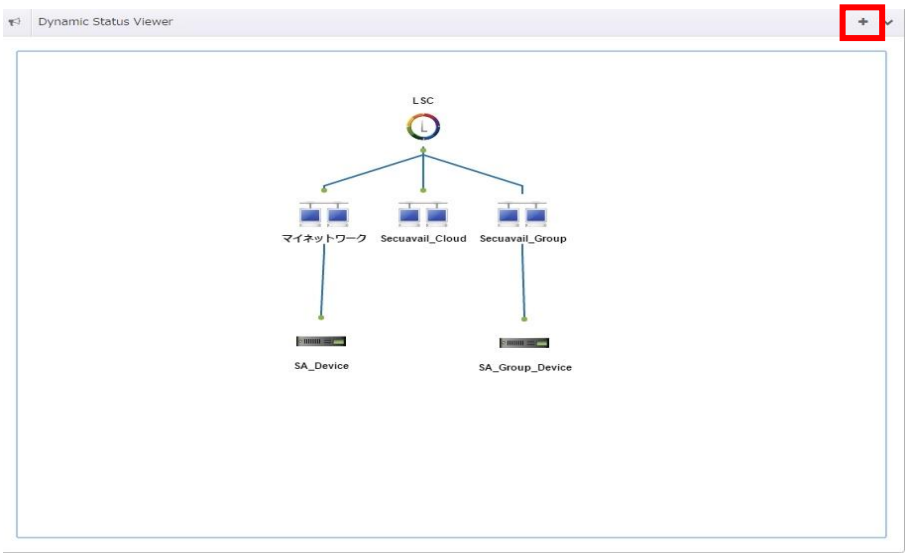
以下の例では DSV 画面上アラート表示（炎マーク）になっている「SA_Device」の監視状況を表示しています。



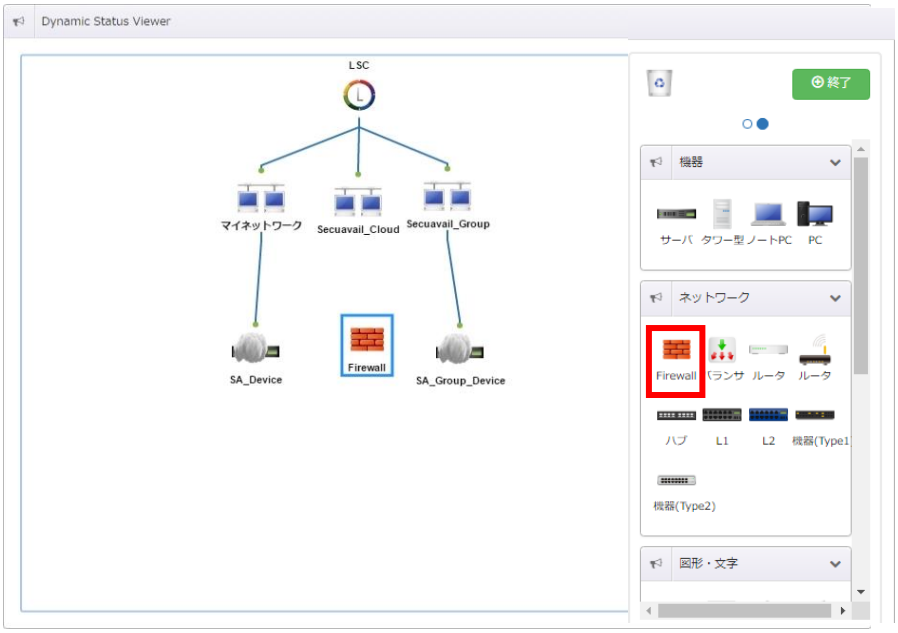
【Dynamic Status Viewer の編集】

初期画面としてデバイス・グループから登録されたものが表示されています。

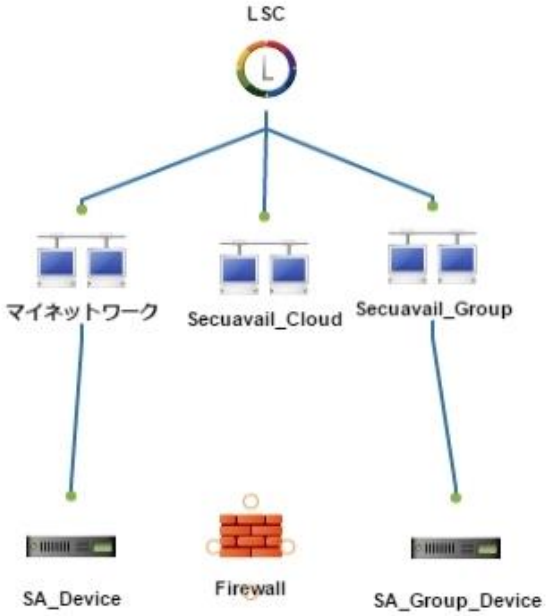
「+」を押すと DSV のメニューが開きます。



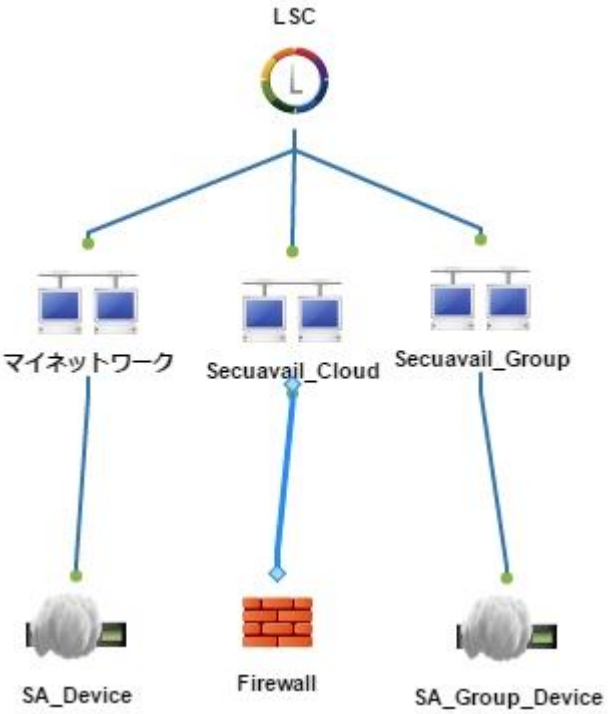
画面右側に表示されているアイコンをドラッグ &ドロップで DSV 内に配置することが出来ます。



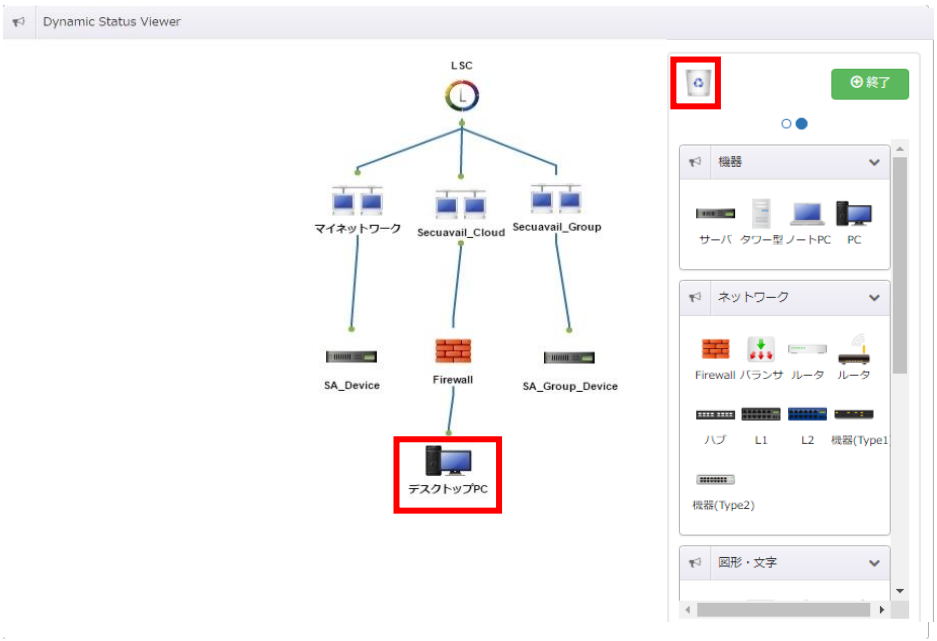
DSV に配置したアイコンにマウスカーソルを充てると上下左右にオレンジの○が表示されます。



オレンジ○をクリックしたまま、接続したいアイコンにマウスカーソルを充てると二つのアイコンを繋ぐことが出来ます。



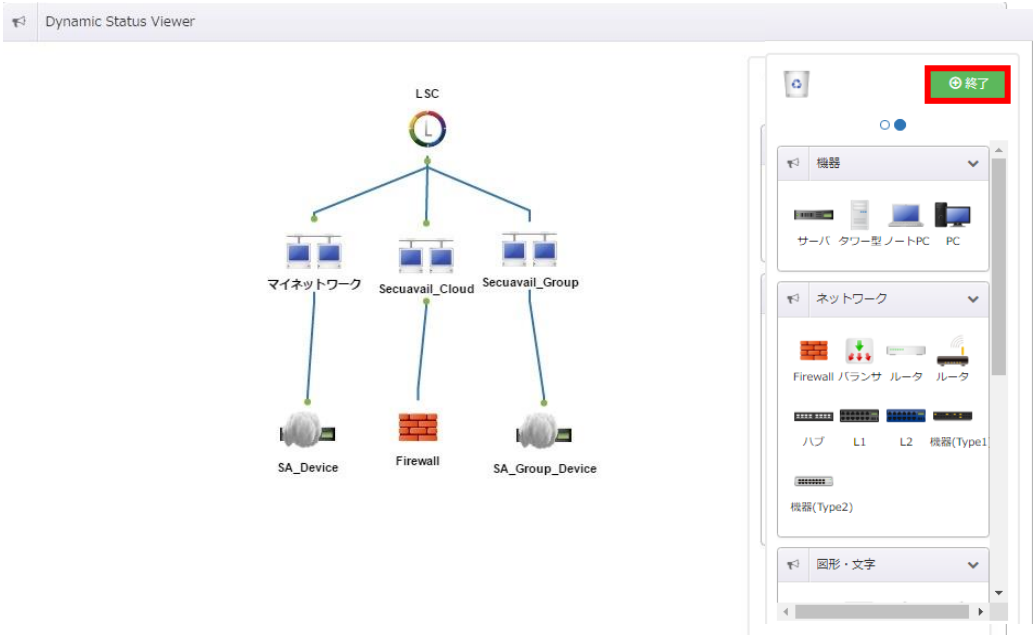
配置したアイコンを削除する場合、削除したいアイコンを右上にあるゴミ箱アイコンへドラッグアンドドロップします。



削除確認画面が表示されますので「はい」をクリックします。

これで DSV 上からアイコンが削除されます。
削除したいアイコンを選択し、キーボード「Delete」キーを押すことでも、アイコンを削除できます。
（この場合確認画面は表示されません）

編集内容については、DSV メニュー画面下にある「終了」ボタンをクリックし、DSV メニューを終了すると内容が保存されます。

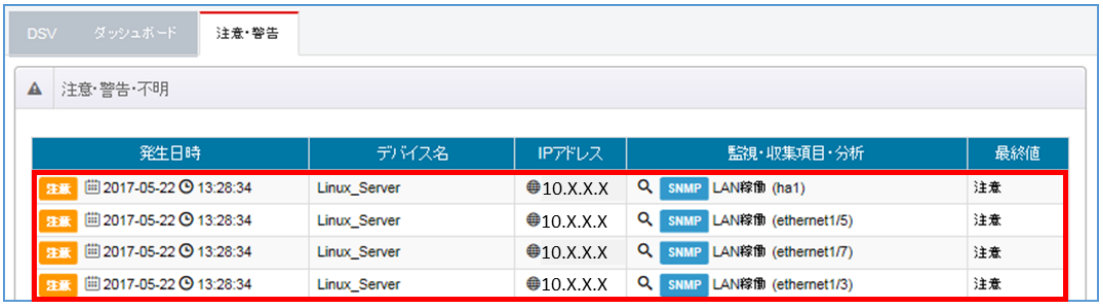


注意・警告の確認

監視設定を行っているデバイスにおいて、監視データが取得できない、注意・警告の設定閾値を超えるなどの異常が発生した時に「注意・警告」画面に表示されます。
注意・警告の閾値の設定は監視・収集項目の「SNMP 監視」のみ設定ができます。

「監視・モニタリング」の「注意・警告」から確認ができます。

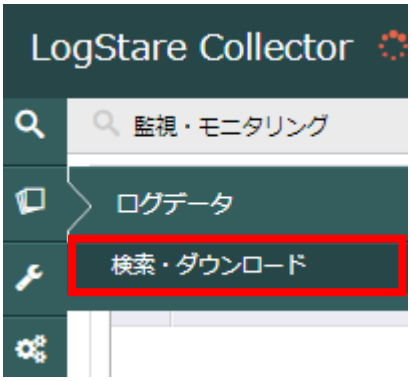
異常が発生した場合、上記のように注意及び警告が表示されます。
メールアラートの送信設定がされていると、設定先にメールが送信されます。



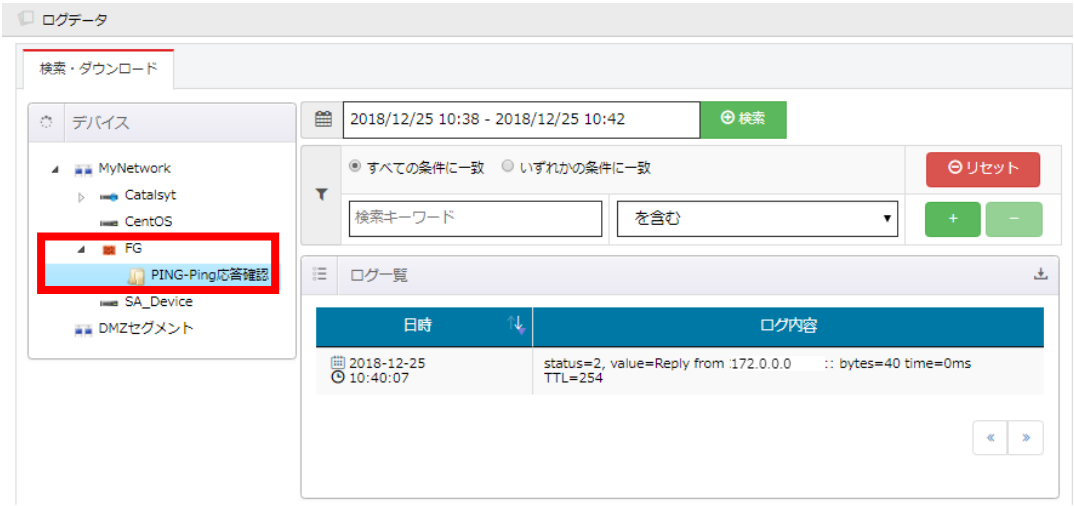
収集ログの検索及びダウンロード

監視対象デバイスから収集したログ内容の検索やダウンロード（有償版のみ）を行う手順を記載しています。

メニューから「ログデータ」の「検索・ダウンロード」から確認できます。



「デバイス」の一覧から、ログを表示したいデバイス名の△をクリック（もしくはダブルクリック）し、表示された取得ログの一覧から確認する監視ログを選択します。
画面右側「ログ一覧」に選択したログが表示されます。

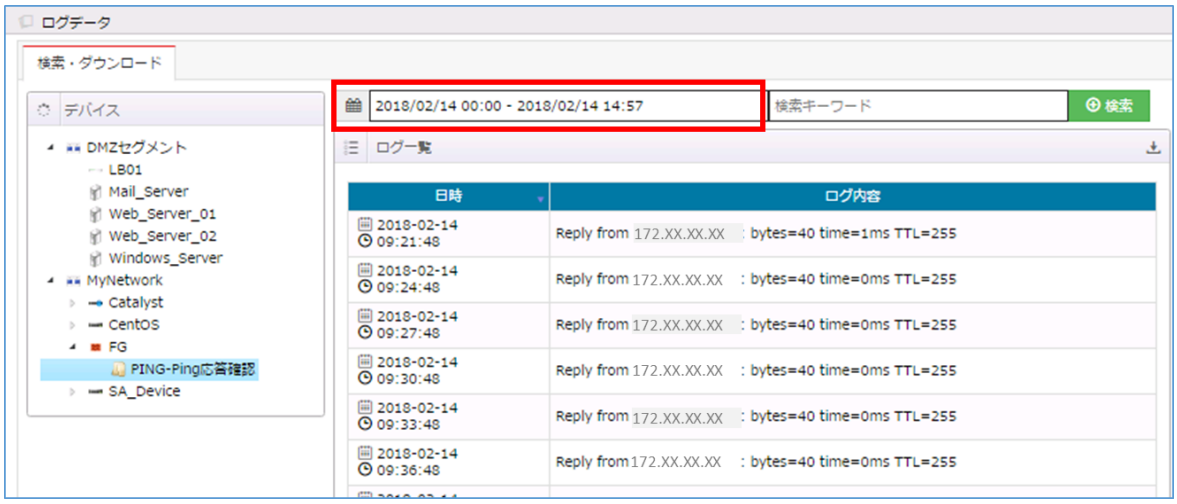


選択した監視ログによって表示されるログの内容は異なります。（上記例では ping 応答ログ）
表示されるログはログ表示を実施した 3 分前から現在時刻までをデフォルトで表示しています。

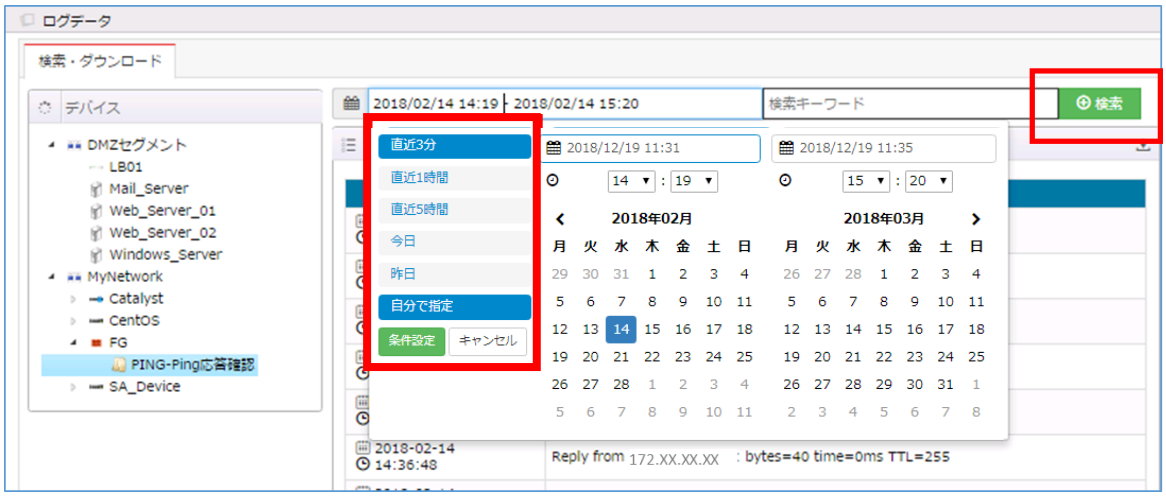
【ログの表示期間の変更】

表示させるログ日時を指定することができます。

赤枠内の期間ログを表示しています。
赤枠をクリックすることで期間指定ができます。



表示されたログ表示期間メニューを利用してログ表示期間を設定します。

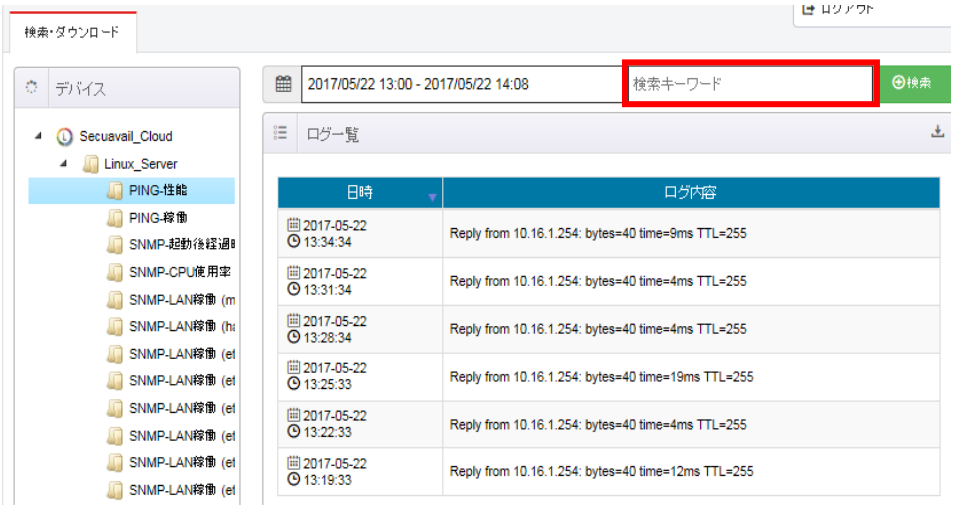


期間指定として、「直近 3 分」「直近 1 時間」「直近 5 時間」「今日」「昨日」「自分で指定」から指定し、「検索」をクリックすると対象期間のログが表示されます。
「自分で指定」の場合、ログの表示の開始（時計/左側カレンダー）から終了（時計/右側カレンダー）までの期間を選択します。

【ログ検索】

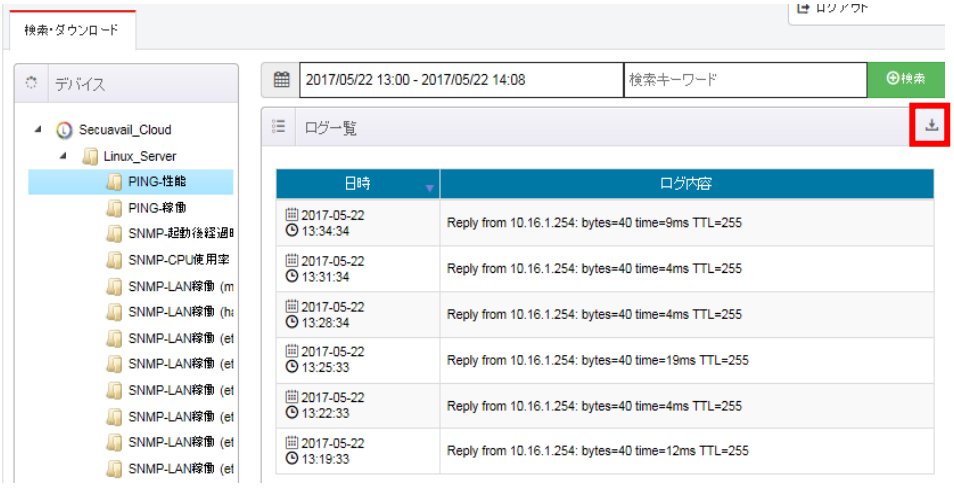
検索キーワード欄に任意の文字列を入力し、「検索」をクリックすると入力された文字列を含むログが表示されます。

※有償版では複数条件検索が可能です。



【ログのダウンロード】(有償版のみ)

赤枠で示したダウンロードボタンをクリックすることで現在の検索結果を CSV 形式でダウンロードする事が可能です。



※収集ログの削除のタイミングについて

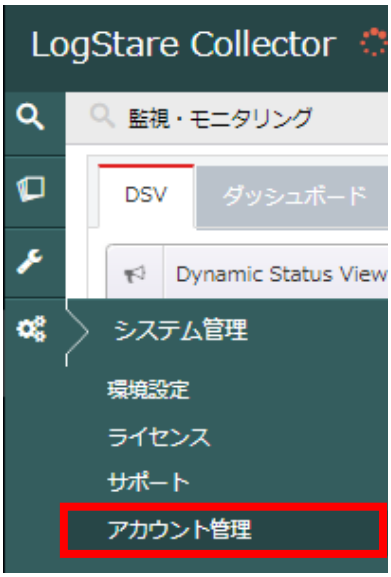
ログ保存期間を過ぎた日の 0 時から 1 時間以内に期間超過のログが削除されます。

LogStare Collector でのアカウント管理

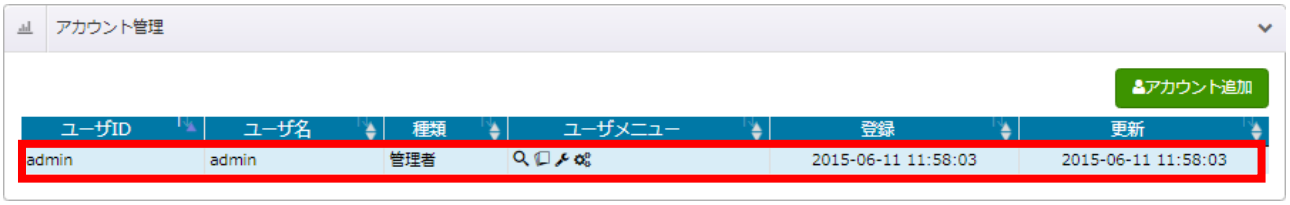
ログインパスワードの変更

ログインパスワードの変更手順を記載しています。

メニューの「システム管理」から「アカウント管理」をクリックします。



表示された「アカウント管理」画面にて、変更するアカウントを選択します。



① 「現在のパスワード」と「新しいパスワード」、「新しいパスワード確認」に必要な値を入力します。

初期パスワードは「root1234」で設定されています。

※初期パスワードは必ず変更してください。
※パスワードは 6 文字以上で設定してください。

② 「更新」をクリックすると、変更ができます。

更新確認画面が表示されますので「はい」をクリックします。

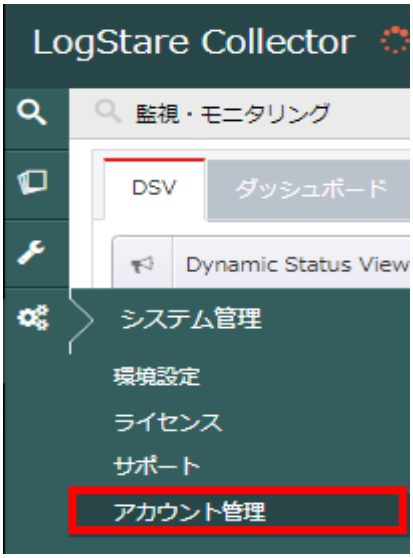
アカウントの設定

LogStare Collector 上のアカウントを設定する手順を記載しています。

【アカウントを設定】

LogStare Collector ではアカウントごとに機能を設定できます。

メニューの「システム管理」から「アカウント管理」をクリックします。



表示された「アカウント管理」画面で、「アカウント追加」をクリックします。

表示された「アカウント追加」画面で、追加するアカウント情報を設定します。

表示された「監視・ログ収集設定」画面で、アカウントを追加するグループを選択します。

①アカウントの情報を設定します。

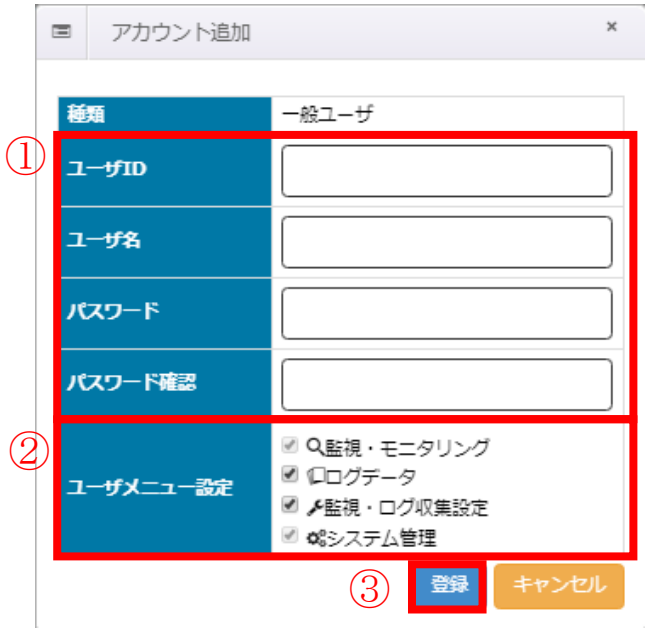
※ユーザ ID がログイン時に使用するユーザ ID となります。

②アカウントに許可する機能を選択します。

※「ログデータ」を選択すると取得したログの参照が可能となります。

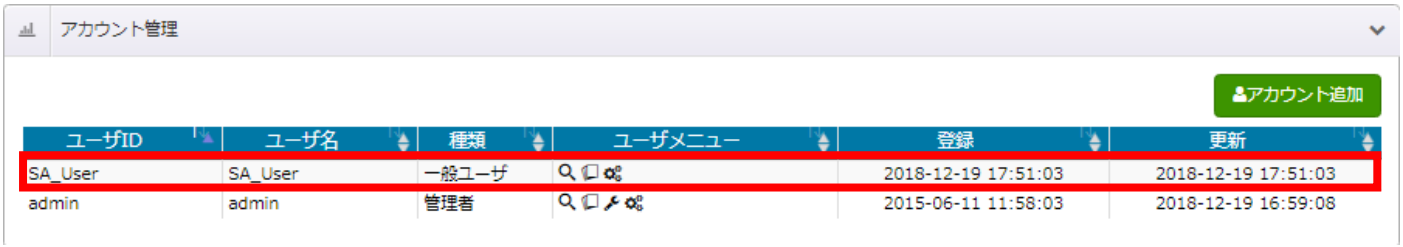
※「監視・ログ収集設定」を選択すると監視項目の設定が可能となります。

③「登録」をクリックします。



登録確認画面が表示されますので「はい」をクリックします。

アカウントが追加されたことを確認したらアカウント設定作業は完了です。



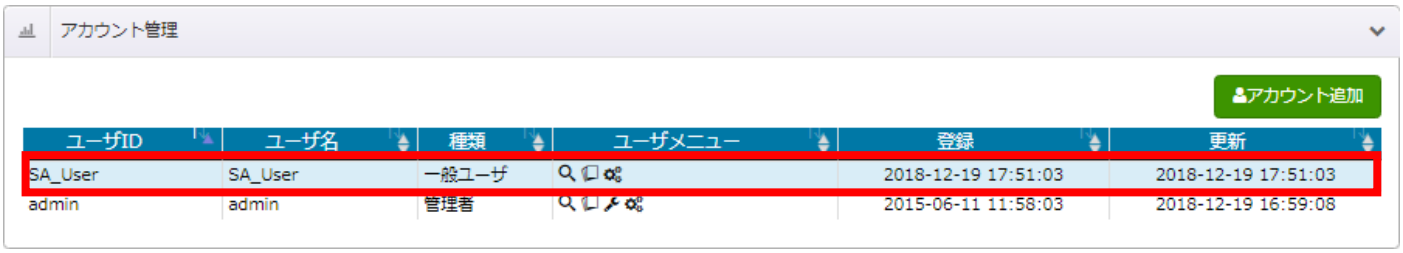
アカウントを複数設定したい場合はこの操作を繰り返します。

※DSV はアカウントごとの管理となります。

アカウントの設定変更及び削除

【アカウント設定の変更】

「アカウント管理」から設定情報を変更するアカウントをクリックします。



表示された「ユーザ管理」画面で設定情報の変更を行います。

①表示された「ユーザ管理」の画面で設定値を変更します。

②「更新」をクリックします。

更新確認画面が表示されますので「はい」をクリックします。

【アカウント設定の削除】

「アカウント管理」から削除するアカウントをクリックします。

表示された「ユーザ管理」画面で「削除」をクリックします。

削除確認画面が表示されますので「はい」をクリックします。

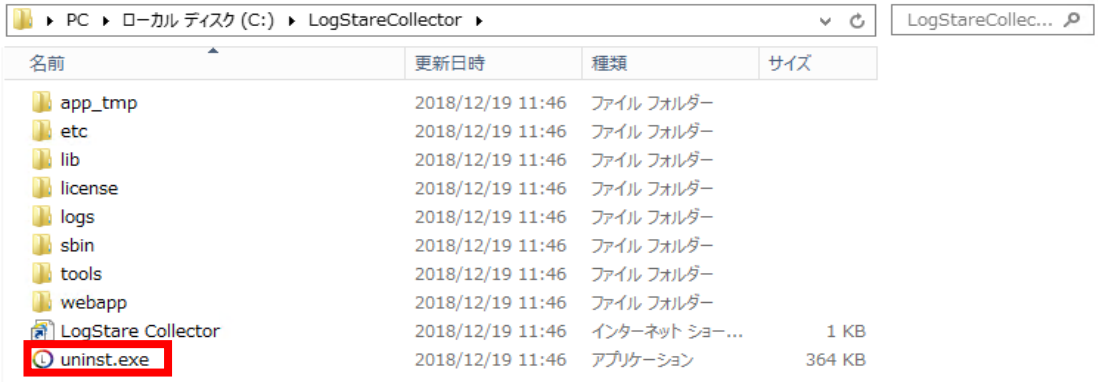
LogStare Collector のアンインストール

Windows での LogStare Collector アンインストール

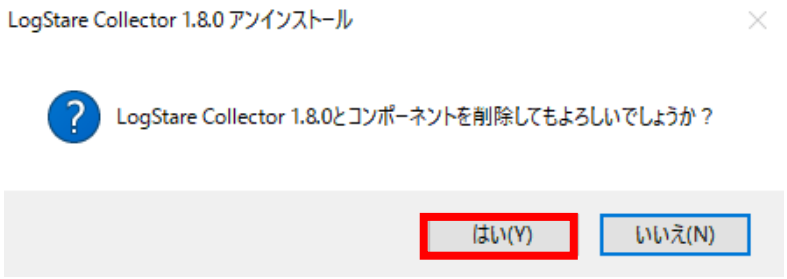
LogStare Collector のアンインストール手順を記載しています。

LogStare Collector を停止します。
（※Windows 版 LogStare Collector の起動と停止 参照）

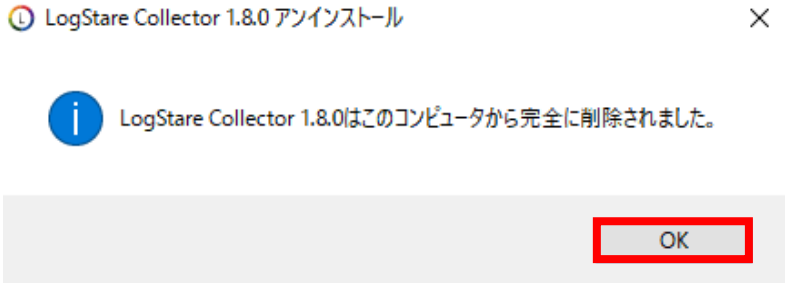
LogStare Collector をインストールしたディレクトリから「uninst.exe」をダブルクリックします。



LogStare Collector をアンインストールでよければ「はい」をクリックします。



アンインストールが完了したメッセージが表示されますので、「OK」をクリックします。



「LogStare Collector」ディレクトリの削除も含めアンインストールは完了です。

Linux での LogStare Collector アンインストール

LogStare Collector を停止します。
（※Linux 版 LogStare Collector の起動と停止 参照）

インストール先に設定したディレクトリに移動し、ディレクトリ情報を表示してください。

```
# cd /usr/local
# ls
…　logstarecollector　…
```

「logstarecollector」のディレクトリを削除します。
コマンド「rm –rf logstarecollector」でディレクトリの削除を実施できます。

```
# rm -rf logstarecollector
```

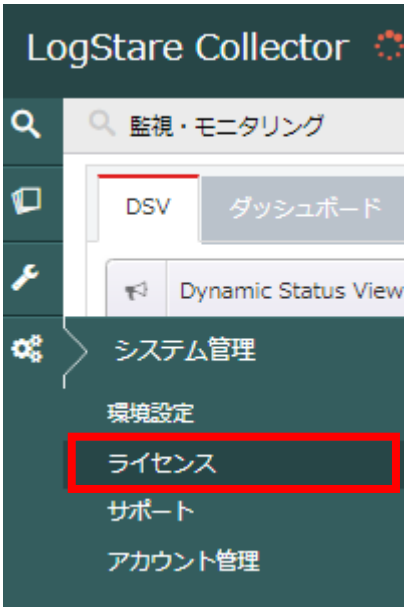
ディレクトリ削除を行ったら、再度コマンド「ls」でディレクトリ情報を表示して、「logstarecollector」がディレクトリ削除されていることを確認できればアンインストールは完了です。

ライセンス登録

LogStare Collector のライセンスを登録する

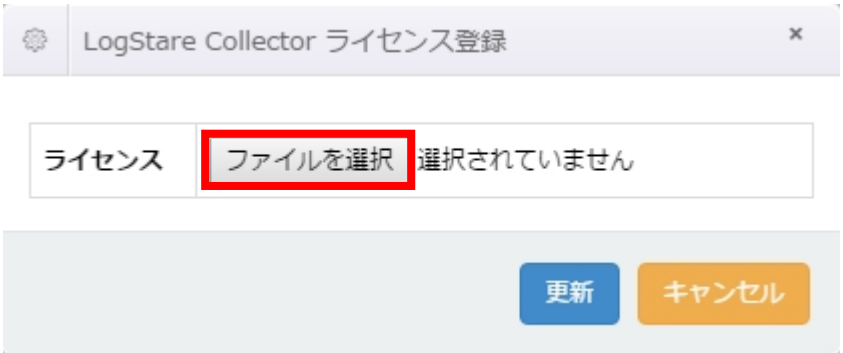
LogStare Collector Pro ライセンスを購入いただくと、制限されていた機能が全てご利用いただけます。ここでは LogStare Collector のライセンス登録の方法を記載しております。

メニューの「システム管理」から「ライセンス」を選択します。



表示された「ライセンス」画面の「LogStare Collector ライセンス」タブにある「+」をクリックします。

表示された「LogStare Collector ライセンス登録」画面の「ファイルを選択」をクリックします。



ライセンスファイルを選択して、「更新」をクリックします。

更新確認画面が表示されますので「はい」をクリックします。

LogStare Collector のライセンスが追加されると「ライセンスタイプ」、「有効期限」、「ライセンスコード」の情報が追加されます。

LogStare Collector ライセンス	
ライセンスタイプ	有償版
有効期間	2020/12/01
ライセンスコード	32a4f681a5cb9c2f2ea4d23ae729a557

※LogStare Collector Pro ライセンスの有効期限が切れた場合、有償版の機能は停止します。
※新規インストールまたはライセンス未適用の環境からのバージョンアップ時に適用される
プロモーションライセンスは LogStare Collector Pro ライセンスと同様の機能が使用できます。

Appendix

リリース履歴

LogStare Collector の各バージョンについて、更新情報を記載します。

リリース日	バージョン	主な更新点
2018 年 2 月 24 日	1.5.0	初期リリースバージョン。
2018 年 4 月 12 日	1.5.1	WMI 収集機能にマッチング文字列機能とテキストマッチング機能を追加。
2018 年 10 月 17 日	1.5.2	Windows サービス登録機能を追加。
2019 年 1 月 10 日	1.6.0	アカウント管理機能を追加。 90 日間有効なプロモーションライセンスが同梱。
2019 年 2 月 20 日	1.6.1	いくつかの不具合を修正。
2019 年 3 月 18 日	1.7.0	SSL 化(HTTPS 化)に対応。
2019 年 3 月 27 日	1.7.1	いくつかの不具合を修正。
2019 年 6 月 13 日	1.8.0	JDK12 に対応。

SecuAvail
株式会社セキュアヴェイル