



目次

LOGSTARE COLLECTOR の概要5
LogStare Collector 動作イメージ5
動作環境6
LOGSTARE COLLECTOR のインストール7
Windows へのインストール事前準備手順7
Windows への LogStare Collector インストール8
Windows 版 LogStare Collector の起動と停止13
Linux へのインストール事前確認16
Linux への LogStare Collector インストール17
Linux 版 LogStare Collector の起動と停止20
LogStare Collector へのログイン及びログアウト(Windows/Linux 共通)
LOGSTARE COLLECTOR のアップデート24
Windows での LogStare Collector アップデート24
Linux での LogStare Collector アップデート25
LOGSTARE COLLECTOR 利用手順
デバイスを監視するまでの流れ26
LOGSTARE COLLECTOR 利用環境の設定27
メールの通知設定

Proxy サーバを設定
任意ポートの設定
設定バックアップの取得手順
バックアップリストア手順
監視基本設定
グループの作成
監視対象デバイスの設定
監視対象デバイスの設定変更及び削除
スキャンで取得した監視項目の設定
監視及びログ収集設定
設定対象デバイスの選択
PING 監視の設定
SNMP 監視の設定
PORT 監視の設定
SNMP トラップ監視の設定
ファイル収集/ログ監視の設定
WMI 収集の設定
SYSLOG 収集/ログ監視の設定
FTP 受信収集/ログ監視の設定

監視及び収集設定の設定変更と削除	D
LOGSTARE COLLECTOR で収集した情報の確認62	2
Dynamic Status Viewer の確認と編集62	2
注意・警告の確認	9
収集ログの検索及びダウンロード	D
LOGSTARE COLLECTOR でのアカウント管理73	3
ログインパスワードの変更7	3
アカウントの設定	5
アカウントの設定変更及び削除72	7
LOGSTARE COLLECTOR のアンインストール79	Э
Windows での LogStare Collector アンインストール79	9
Linux での LogStare Collector アンインストール 80	D
ライセンス登録81	1
LogStare Collector のライセンスを登録する8	1
APPENDIX83	3
リリース履歴	3

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			
		•Windows 7	
	Windows	•Windows 8.1	
		•Windows 10	
		•Windows Server 2008 R2	
OS		•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		
НОО	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		
	・Linux OS で SY	SLOG 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 WM	II 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	E利用する場合、LogStare Collector サーバの IP アドレスは	
その曲	固定 IP アドレス	が必要	
~C 071B	•LogStare Collec	stor 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:pac 	ific.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



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。

① LogStare Collector 1.8.0 セットアップ	– 🗆 🗙
インストール先を選んでください。 LogStare Collector 1.8.0をインストールするフォルダを選んでください。	
LogStare Collector 1.8.0を以下のフォルダにインストールします。異なったフォルダ は、[参照] を押して、別のフォルダを選択してください。 続けるには [次へ] をクリッ?	にインストールするに クして下さい。
- インストール先 フォルダ	
©¥LogStareCollector	参照(R)
必要なディスクスペース: 72.3MB 利用可能なディスクスペース: 65.1GB	
Nullsoft Install System v2.46.5-Unicode	
< 戻る(B) 次へ(N)	> キャンセル

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。

🕕 LogStare Collector 1.8.0 セットアップ	_	
インストール先を選んでください。 LogStare Collector 1.8.0をインストールするフォルダを選んでください。		
LogStare Collector 18.0を以下のフォルダにインストールします。異なったフォルタ は、「参照]を押して、別のフォルダを選択してください。 続けるには [次へ] をクリッ	ミレインスト クレイ下す	ールするに れい。
インストール先 フォルダ C¥LogStareCollector	参照()	₹)
必要なディスクスペース: 72.3MB 利用可能なディスクスペース: 65.1GB Nullsoft Install System v2.46.5-Unicode		
< 戻る(B) 次へ(N)>	キャンセル

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 1.8.0 セットアップ		×
LogStare Collector 環境設定		
■ JAVA(JRE)ディレクトリ ※ JAVA(JRE)がインストールさ	C:¥Program Files¥Java¥jdk-12.0.1 れているディレクトリを指定してください。	参照
■ サービスポート ■ OS ■ Windowsサービス登録	80 〇 32bit ④ 64bit ▽ 友なh	
※ チェックを入れるとWindowsサ	ービスとして登録され常時稼働します。	
■ ログオンユーザ	Administrator	
■ ログオンバスワード	•••••	
Nullsoft Install System v2.46.5–Unico	de 〈 戻る(B) // 次へ(N) >	キャンセル

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 1.8.0 セットアップ Х LogStare Collector 環境設定 L ■ JAVA(JRE)ディレクトリ C:¥Program Files¥Java¥jdk-12.0.1 参照 ※ JAVA(JRE)がインストールされているディレクトリを指定してください。 ■ サービスポート 80 OS 🔘 32bit 🛛 💿 64bit ■ Windowsサービス登録 ☑有効 ※ チェックを入れるとWindowsサービスとして登録され常時稼働します。 ■ ログオンユーザ Administrator ■ ログオンバスワード ********* Nullsoft Install System v2.46.5-Unicode -

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。

🕓 LogStare Collector 1.8.0 セットアップ		—	
LogStare Collector 環境設定			
■ JAVA(JRE)ディレクトリ	C:¥Program Files¥Java¥jdk-12.0.1		参照
※ JAVA(JRE)がインストールされ	1ているディレクトリを指定してください。		
■ サービスポート	80		
■ OS	🔿 32bit 💿 64bit		
■ Windowsサービス登録	☑有効		
※ チェックを入れるとWindowsサ	ービスとして登録され常時稼働します。		
■ ログオンユーザ	Administrator		
■ ログオンパスワード	•••••		
Nullsoft Install System v2.46.5-Unicod	le		
	< 戻る(B) 次へ(N) >		キャンセル

< 戻る(B) 次へ(N) > キャンセル

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。

🛈 LogStare Collector 1.8.0 セットアップ	_	□ ×
LogStare Collector 環境設定		
■ IA\/A(IRE)ディークトロー 「ヘソワー・・・・ File-Y IoY' 10.0.1		<u>+</u> 177
■ Shortkolic 25 4 D 2 F 3 C #Program Files#Java#jak=12.0.1 ※ JAVA(JRE)がインストールされているディレクトリを指定してください。		30.XH
■ サービスポート 80		
■ OS 🔷 32bit		
■ Windowsサービス登録		
※ チェックを入れるとWindowsサービスとして登録され常時稼働します。		
■ ログオンユーザ Administrator		
Nullsoft Install System v2.46.5-Unicode		
< 戻る(B) 次へ(N) >		キャンセル

「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。

● インストール先	C:¥LogStareCollector	
▶ JRE ディレクトリ	C:¥Program Files¥Java¥jdk-12.0.1	
▶ サービスボート	80	
OS 🛛	64bit	
●Windowsサービス登録	有効	
●ログオンユーザ	Administrator	

「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。

😘 サービス					_		×
ファイル(E) 操作(A)	表示(M) ヘルブ(出)						
	3 📑 🛛 📷 🕨 💷 II 🕨						
🔍 サービス (ローカル)	④ サービス (ローカル)						
	LogStareCollectorService	名前 ^	說明	状態	スタート	アップの種	頬 ^
	サービスの停止	Link-Layer Topology Discov Local Session Manager	PC と ローカ	事行中	手動		
	サービスの再起動	LogStareCollectorService		実行中	手動		
		Microsoft (N) (S) (M) / (S) (M)	ೂಟ್ 1-ザ		于 <u>影</u> 手動(トリガー開き	台)
		Alicrosoft App-V Client	Man		無効		
		Microsoft iSCSI Initiator Ser	このコ		手動		
		Microsoft Passport	ユーザ		手動(トリガー開き	音)
		Microsoft Passport Container	ID 7		手勳(トリガー間が	â) 🗸
		<	200				>
	\拡張 /標準/						

「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。

(ローカル コンピューター)	LogStareCollectorService のブロパティ	\times
全般 ログオン 日	回復 依存關係	
サービス名:	LogStareCollectorService	
表示名:	LogStareCollectorService	
說明:		0
実行ファイルのパス: C:/LogStareColle	ctor¥tools¥LscService.exe //RS//LogStareCollectorService	
スタートアップの 檀頭(E):	自動 自動(理証開始) 自動 手動	~
サービスの状態:	無効 高订平	- 1
開始(5)	停止(D) 一時停止(P) 再開(B)	
ここでサービスを開始	aするとさに適用する開始パラメーターを指定してください。	
開始パラメーター(<u>M</u>):	
	OK キャンセル 適用	(A)

(下図は「自動」を選択した場合の例になります。)

(ローカル コンビューター)) LogStareCollectorService のブロバティ	×
全般 ログオン	回復 依存豐係	
サービス名:	LogStareCollectorService	
表示名:	LogStareCollectorService	
說明:		< >
実行ファイルのパス: C:/LogStareColle	: ector¥tools¥LscService.exe //RS//LogStareCollectorServic	
スタートアップの 種類(<u>E</u>):	自動]~
サービスの状態:	奥行中	
開始(5)	停止① 一時停止(P) 再關(B)
ここでサービスを開き	始するときに適用する開始パラメーターを指定してください。	
開始パラメーターIM	0:	
	OK キャンセル ii	1用(<u>A</u>)

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。



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。

alternativesconfig 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。

	LogStare Collector こ IDとパスワードを入力してください!
	▲ ユーザID
(])	▲ パスワード
	2 D7720

※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。

Lc	ogStare Collector 🔅	≣	å admin ≣•
٩	○、 監視・モニタリング		
P	DSV ダッシュポード 注意・書告		
۶	📢 Dynamic Status Viewer		+
¢	LSC U I MyNetwork		

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。

LogStare Collector 🔅	📰 🎴 admin ≣•
 Q 監視・モニタリング 	その他メニュー
DSV ダッシュボード 注意・書告	E LOVOR
Y Dynamic Status Viewer	+
LSC	

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 🗘 IDとパスワードを入力してください!
▲ ユーザID
■ パスワード
ログイン 🛛



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。



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】

tare Collector	0		:	🏜 adm
システム管理				
環境設定 ライセン	ス サポート アカ	ウント管理		
LogStareCollect	or (fe80:0:0:0:20c:29ff	:febf:b34d)		
3	定項目	值·内容		
タイムソーン		(UTC+09:00) Japan Standard Tin ▼		
監視間隔		180 秒關隅		
通知設定		್ರಕನ @しねい		
Proxyサーバ		್ರಕる ⊛しねい		
		TCP 514 UDP 514 TLS 10514		
		162		
サーバ		21 ※FTPサーバ切稼働していない状態です。稼働するためにはPROライセンスが必要です。		
		例 ① 0.使用可能な全てのボートをパッシブボートにする。 ② 123:123番ボートをパッシブボートにする。 ③ 123:133:123、133番ボートをパッシブボートにする。 ③ 123:125:123から125番までのボートをパッシブボートにする。 ③ 0 0 0 0 0 0 0 0 0 0 0 0 0		
	監視データ保管期間	10日 ※PROライセンスが必要な機能です。		
ログ		10 分 ※NetStare Suiteライセンスが必要な機能です。		
設定パックアップ		■ <i>ダ</i> ウンロード		
バックアップリストア		■パックアップリストア		
				日東

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。

Lo	gSt	tare Collect	cor 🔿	☷ 🎍 admin •
۹	00	システム管理		
		環境設定 ライ	イセンス サポート アカウ	ワント管理
۶		LogStareCo	ollector (fe80:0:0:0:20c:29ff:	febf:b34d)
0 8			設定項目	值·内容
		タイムソーン		(UTC+09:00) Japan Standard Tin ▼
		監視間隔		180 秒腦隔
	-		メール通知使用	
(D			LogStare Collector管理者
				(SetS)
		通知設定		
				SSL/TLS STARTTLS OLD
			メールSSLポート番号	
				受信テスト
				受信テスト
		D		

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。

Lo	gSta	are Collector			🏜 admin 🚍
۹	0 8 B	システム管理			
	現	環境設定 ライセンス	ス サポート アカ:	シント管理	
۶	1	LogStareCollecto	or (fe80:0:0:0:20c:29ff:	febf:b34d)	
o;		32 23	定項目	值·内容	
		タイムゾーン		(UTC+09:00) Japan Standard Tin ▼	
		監視間隔		180 秒間隔	
		通知設定	メール通知使用	್ರಕる ⊛ರಿಸು	
	$\widehat{\mathbb{D}}$		利用		
			パスワード	(確認)	
				TCP 514	
				2	□ 更新

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。

L	ogSi	tare Collector	¢.		≣	🏜 admin 🚍
٩	03	システム管理				
	ſ	環境設定 ライセンス	マロン サポート アカウ	リント管理		
۶		LogStareCollecto	r (fe80:0:0:0:20c:29ff:1	febf:b34d)		
08			定項目	值·内容		
		タイムソーン		(UTC+09:00) Japan Standard Tin 🔻		
		監視間隔		180 秒間隔		
		通知設定	メール通知使用	○する ◎しない		
		Proxyサーバ	利用	◎する ◎しない		
1	1		Syslog7t – ト	TCP 514 UDP 514 TLS 10514		
				162		
		א– ע		21 ※FTPサーバが稼働していない状態です。稼働するためにはPROライセンスが必要です。		
				例 ① 0: 使用可能な全てのボートをパッシブボートにする。 ② 123:123番ボートをパッシブボートにする。 ③ 123:133:123、133番ボートをパッシブボートにする。 ④ 123-125:123から125番までのボートをパッシブボートにする。		
				※FTPサーバが稼働していない状態です。稼働するためにはPROライセンスが必要です。		
			監視データ保管期間	10日 ※PROライセンスが必要な機能です。		
		ログ	監視ログ転送間隔	10 分 ※NetStare Suiteライセンスが必要な機能です。		
			収集ログ暗号化	◎する ◉しない ※暗号化をすると検索が遅くなる恐れがあります。		
		設定バックアップ		В ダウンロード		
		バックアップリストア		В バックアップリストア		
					2	日 更新

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。

システム管理				
環境設定 ライセンス	ス サポート アカ	ウント管理		
LogStareCollecto	r (fe80:0:0:0:20c:29f	f:febf:b34d)		
32 32	定項目	植・内容		
タイムソーン		(UTC+09:00) Japan Standard Tin ▼	注意 ▲	
監視間隔		180 秒間隔		
通知設定	メール通知使用	್ರಕನ @しない		
Proxyサーバ		○する ◎しない		
		TCP 514 UDP 514 TLS 10514		
		162		
		21 ※FTPサー/仿稼働していない状態です。稼働するためにはPROライセンスが必要です。		
		例 ① 0:使用可能な全てのポートをパッシブポートにする。 ② 123:122番ボートをパッシブポートにする。 ③ 123:133:123、13番ボートをパッシブポートにする。 ③ 123-125:123から125番までのポートをパッシブポートにする。 ①		
		※FTPサーバが稼動していない状態です。稼働するためにはPROライセンスが必要です。		
	監視データ保管期間	10 日 ※PROライセンスが必要な機能です。		
ログ	監視ログ転送間隔	10 分 ※NetStare Suiteライセンスが必要な機能です。		
	収集ログ暗号化	○する ◉しない ※暗号化をすると検索が遅くなる恐れがあります。		
設定バックアップ		習 ダウンロード		
バックアップリストア		■ パックアップリストア		

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_xxxxxx.bak」がローカルに保存されます。

	設定パックアップ		■ダウンロード	
	バックアップリストア	-	🖺 バックアップリストア	
			四 更新	
Copyright	t SecuAvail Inc. LogStare Collecto	or ver. 1.5.4		
🗋 Iso	z_backup_20181bak ^		すべて表示	×

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。

システム管理					
環境設定 ライセ	ンス サポート アカ	ウント管理			
LogStareCollector (fe80:0:0:020c:29ff;febf;b34d)					
<u>設定項目</u> タイムソーン 監視開端		值,内容			
		(UTC+09:00) Japan Standard Tin ▼			
		180 秒間隔			
通知設定	メール通知使用	್ರಕる ⊛しない			
Proxyサーバ		○する ⊛しない			
		TCP 514 UDP 514 TLS 10514			
		162			
זע-ש		21 ※FTPサーバが稼働していない状態です。稼働するためにはPROライセンスが必要です。			
		例 ① 0:使用可能な全てのポートをパッシブポートにする。 ② 123:123番ボートをパッシブポートにする。 ③ 123:133:123、133番ポートをパッシブポートにする。 ③ 123:125:123から125番までのポートをパッシブポートにする。 ③ メビアササーノ(が感動) ていない状態です。感動するためにはPROライヤンスが必要です。			
	監視データ保管期間	10日 ※PROライセンスが必要な機能です。			
ログ	監視ログ転送間隔	10分 ※NetStare Suiteライセンスが必要な機能です。			
	収集ログ暗号化				
設定バックアップ		₽// ₽// 20-			
バックアップリスト		■バックアップリストア			

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。

◎ バックアップリストア	×
パックアッ ファイルを選択 選択されていません	
リストア キャ	2 2 1 2

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。

v
 ●追加 ● キャンセル

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。

◎ グループ追加	×
親グループ (最上位) ▼	
グループ名 ①	
ארבא 🛛 🖲 🖬 🖓 🖬	

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。

	#	グループ	+	デバイス一覧	2 +
		Secuavail_Cloud	I	デバイス	ΙΡ アド レス
(1)		📗 Secuavail_Group	þ	デー	ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー
		🔎 マイネットワーク	,		
		① グループ:3 デ	バイス:0		

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。

ł	◎ デバイス追	bo			×
\bigcirc	デバイス名				
	IPアドレス				
	アイコン	•			
	監視データ保留	會期間	10日	収集ログ保管単位 収集ログ保管期間	 日 過 月 年 10 日 ※PROライセンスが必要な機能です。
	SNMP	SNMP,	バージョン	2 🔻	
		SNMP	⊐ミュニティ	public	
				2	●追加 ◎キャンセル

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。

#	グループ	+	⊞	デバイス	(一覧		+
4	MyNetwork			アイコン	デバイス	IPアドレス	
	IIIII JA_DEVICE				SA_Device	# 172.0.0.0	
	① グループ:1 デ	バイス:1					

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。

÷.	》 デバイス追	1		د	ε
	デバイス名				
	IPアドレス				
	アイコン	•			
	監視データ保	管期間	10日	収集ログ保管単位 ♀ ● 日 ● 週 ● 月 ● 年 収集ログ保管期間 ● 日 ● 週 ● 月 ● 年 10 日 ************************************	
$\widehat{1}$		SNMP	バージョン	3 🔻	
		ש–ב	名		
	SNMP	セキュ	リティレベル	noAuthNoPriv 🔻	
		コンテ	キスト名		
		エンジ	i>ID		
				 ② ③ 追加 Ø キャンセル 	

②「追加」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】

「デバイスー覧」から設定情報を変更するデバイスをクリックします。

■ デバイス	一覧	+
アイコン	デバイス	IPアドレス
	SA_Device	⊕ 172.0.0.0
4	Linux_Server	# 172.0.0.0
	Winodws_Server	⊕ 172.0.0.0

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。

	0	デバイス更	新					×
					本基	情報		
(1)	U	⊃ デバイスネ	3	Winodws_Server		● IPアドレス	172.0.0.0	
	,	9 アイコン		• • • • • •		0 mm) 0 mm) 0 mm 0 mm)		
		◎ MACアドL	ス	:::		💀 メーカ名		
		🗧 OS				賃 製品名		
		▶ 利用監視項				監視間隔	180 秒間隔	
	1	監視データ保	管期間	10日		収集ログ保管単位 ● 収集ログ保管期間	 日 週 月 年 10 H ※PROライセンスが必要な機能です。 	
		SNMP	SNMP/(ージョン	2 🔻			
			SNMP_	ミユニテイ	public			
				●監視項目スキャ	ン 【 ● 監	見項目追迎 ● 更新	○ 削除 ○ キャンセル	

【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。

■ デバイス	一覧	+
アイコン	デバイス	IPアドレス
	SA_Device	⊕ 172.0.0.0
	Linux_Server	⊕ 172.0.0.0
	Winodws_Server	⊕ 172.0.0.0
	Linux_Server Winodws_Server	

表示された「デバイス更新」画面で「削除」をクリックします。

基本情報 © デバイス名 Winodws_Server ● IPアドレス 172.0.0 ● アイコン ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	1111230
・ デバイス名 ・ Winodws_Server ・ アゲレス ・ ア アゲレス ・ アゲレス <t< th=""><th></th></t<>	
・ アイコン ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	デバイス名
 ◇ MACアドレス ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	アイコン
Image: OS Image:	MACアドレス
	OS 利用監視項目
監視データ保管期間 10日 収集ログ保管単位 10日 収集ログ保管単位 収集ログ保管期間 10日 収集ログ保管期間 10日	見データ保管期間
SNMP/(ージョン 2 ▼ SNMPコミュニティ public	MP
● 監視項目スキャン ● 監視項目追加 ● 更新 ● 削除 ● キャンセノ	I

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】

「デバイスー覧」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。

⊞	デバイス	一覧	+
Ì	アイコン	デバイス	IPアドレス
		SA_Device	⊕ 172.0.0.0
	41	Linux_Server	# 172.0.0.0
		Winodws_Server	⊕ 172.0.0.0

「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。

デ/	バイス更	新							×
				基本	情報				
₽₹	デバイス名		Winodws_Server	·	● IPアドレス		172.0.0.0		
8 7	ァイコン		• • • • • • •						
😌 M	IACアドレ	ス	(())		■ メーカ名				
a 0)S			;≡ 製品名					
り利	用監視項				監視間隔		180	秒間隔	
監視:	データ保留	會期間	10日		収集ログ保管単 収集ログ保管期	位 ② 間	●日 ○週 10日 ※PROライセン す。	 ●月 ● 年 スが必要な機能で 	2
SNM	P -	SNMP)(-ジョン ミュニティ	2 v public					
			● 監視項目スキャ	ン ● 監	現有自追加	④更新	⊖削除	⊘ ≠r>セ	ıl

「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。

◎ デバイス	又更新							×
			基本	情報				
D デバイ:	ス名	Winodws_Server		🔹 ፤ዮፖド	レス	172.0.0.0		
🛢 713	>	• • • • • • • • •		·				
MAC P	ドレス	:::		■ メーカ	2			
● OS	项目			〕 ● 製品名 監視開隔		180	秒間隔	
 監視データ	·保管期間	10日		収集ログ保 収集ログ保	管単位 🛛	 ●日 ○週 10日 ※PROライセンス す。 	○月 ○年 び必要な機能で	
SNMP	SNMP/(-ジョン ミュニティ [2 V public					
(⊕ 3	すべて選択	● 監視項目スキャン	∫ ⊛≊	規項目追加	⊕ 更新	⊖削除	●キャンセ	IL
PING SNMP	HOST-RES (標準MIB) Windows	SOURCES_CPU使用率	1.001.00			СРИ8 СРИ8 СРИ8	更用率(%) 更用率生値 更用率(%)	
	Windows_	仮想メモリ使用率	76.88			CPU(又モ! 使用5 19日4	使用率生値 J使用率(%) 配生値 ±値	
	Windows	ディフク体中支	C:/		47.43	*** ボリ: (%) 使用館 総量的	ユーム使用率 ヨーム使用率 副生値 主値	
	windows_	ティスク使用学				ボリ	ユーム使用率	*

※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。

			基本	情報				
ゆ デバイ	72名	Winodws_Serve	er	● וףדו	レス	172.0.0.0		
		• •	.	0	·			
₩ <i>ア</i> イコ	>	◎ 🗱 ◎ 🖣	<u>ه</u> د	0	•			
😌 МАС7	パドレス	:::		. メーカ	8			
🖽 os				≢ 製品名				
9 利用監視	現項目			監視間隔		180	秒間隔	
監視データ保管期間						●日 ◎週	◎月 ◎年	
		10日		収集ログ保管単位		10 日	10 日	
				10342 C 7 U		※PR0ライセン す。	スが必要な機能で	
	SNMP/	ージョン	2 🔻					
SNMP	SNMP	ミュニティ	public					
	t			1975-01-01-0	() THE		0. h . h .	
	9へい進伏	● 監視県日人十		说供白追加	७ इस		07720	
PING	HOST DES			1		CPU	使用率(%)	
SNMP	(標準MIB)	SOURCES_CPUBOR	2) 🗹 1.00			CPU	使用率生值	
	Windows	COLUERS		-		CPU	CPU使用率(%)	
	windows_	_CPU使用举	1.00			CPU	使用率生值	
						XE	リ使用率(%)	
	Windows_仮想メモリ使用率			76.88			口牛注	
	Windows_	仮想メモリ使用率	76.88				重土但	
	Windows_	「仮想メモリ使用率	76.88			総量	生値	
	Windows_	仮想メモリ使用率	76.88			総量 ポリ (%)	車王値 生値 ユーム使用率	
	Windows_	仮想メモリ使用率	C:/		47.43	総量 ボリ (%) 使用	<u>車</u> ±値 生値 ユーム使用率 量生値	
	Windows_	仮想メモリ使用率 ディスク使用率	C:/		47.43	総量 ポリ (%) 使用 総量	^重 ±値 生値 ユーム使用率 量生値 生値	

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。

● デバイス	ス更新								
基本情報									
ರ್ ೯バイ	72名	Winodws_Server			IPアド	~	172.0.0.0		
🖻 アイコ	>	• • •	0	m	• •••• ••				
		◎ 🚟 🏻 ┥	•		0	•			
MAC	パドレス	::::			🛛 メーカ名	3			
🧮 OS					╞■ 製品名				
9 利用監視	現項目				監視開隔		180) 秒間隔	
監視データ	7保管期間	10日			収集ログ保 収集ログ保	管単位 ♀ 管期間	 ●日 週 10日 ※PR0ライセン す。 	 ○月 ○年 →スが必要な機能 	c
SNMP	SNMP/(ジョン ミュニティ	2 🔻	ic					
	すべて選択	● 監視項目スキャ	> [⊕ ≊ #		⊕ 更新	〇削除	0=+v>t	ะม
PING	HOST-RES	GOURCES CPU使用率					CPU	U使用率(%)	
SNMP	(標準MIB)			00			CPU	J使用率生值	
	Windows	CDI W在田校	1/# III				CPU	J使用率(%)	
	windows_	CP000000	Ű				CPU	J使用率生值	
							ж	ミリ使用率(%)	
	Windows_	仮想メモリ使用率		76.88			使用	月量生値	
							総量	2生値	
			ä				ポリ (%)	リユーム使用率	
				C:/		47.43	使用	月量生値	
	Windows	ディスク使用率					#85	建生植	
							ポリ	リューム使用率	

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。

▲ デバイス	≡	監視・	収集一	覧				- +
MyNetwork SA_Device		NO	t⊯	選択	デバイス	IPアドレス	♀ 監視 ▲ 収集	検知条件
Winodws_Server			ĺ			データがありません。		
① デバイス:3 設定:0								

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。

◎ 監視・収集追加	x	¢
デバイス	SA_Device	
監視・収集	SA_Device Linux_Server Winodws_Server Eさい ▼	
	●追加 ◎キャンセル	

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。

-	監視・収集追加			×
5	デバイス	SA_Device V		
Ē	≦視・収集	◉ 監視 ◯ 収集		
		監視方式を選択してください ▼		
		PING監視	●追加 ◎キャンセル	
		SNMP監視 PORT監視		

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。

	100	≫ 監視・収集追加	×
		デバイス	SA_Device V
		監視・収集	● 監視 © 収集 PING監視 ▼
		監視・収集項目	Ping応答確認 ▼
1		監視ON/OFF	◎ 監視ON ◎ 監視OFF
		取得エラー判定回数	注意 1 警告 3
		監視項目名	Ping応答確認
		IPアドレス	172.0.0.0
		タイムアウト (秒)	5
		ノード監視パラメータ	」 ping回致
		間値設定 ④ 追加	
		アラートメール送信先 ● 追加	
			2 ●追加 ●キャンセル

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。

4	影響では「「「「「」」を見ていた。		×
	デバイス	SA_Device V	_
Ē	B⊏28 . J∏ ==	◉ 監視 ◎ 収集	
		監視方式を選択してください ▼	
		監視方式を選択してください	
		SNMP監視	⊕ 追加 Ø キャンセル
L		PORTEN	

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。

 		×
デバイス	SA_Device ¥	
監視・収集	● 監視 ◎ 収集 SNMP監視	
監視・収集項目	Windows_CPU使用率 Windows_CPU使用率	
監視ON/OFF	Windows- Windows 仮想メモリ使用率 Windows 仮想メモリ使用率	
取得エラー判定回数	Windows_ディスク使用率	
監視項目名	トラフィック (標準MIB) Windows_プロセス数	
IPアドレス	ポートステータス (標準MIB)	
タイムアウト (秒)	標準_UpTime 標準_TCPセッション	
SNMPバージョン	1 🗸	

SecuAvail

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。

	◎ 監視・収集追加	
	デバイス	SA_Device V
	監視・収集	◎ 監視 ◎ 収集 SNMP監視
1	監視・収集項目	トラフィック (標準MIB)
	監視ON/OFF	◎ 監視ON ◎ 監視OFF
	取得エラー判定回数	注意 1 警告 3
	監視項目名	トラフィック (標準MIB)
	IPアドレス	172.0.0.0
	タイムアウト (秒)	5
0	SNMPバージョン	1 V
Ŀ	SNMPコミュニティ	Public
	トラフィック量パラメータ	マッチング文字列
	開植設定 🛛 追加	
	アラートメール送信先 🛛 🛞 追加	
		●テスト ●追加 ●キャンセル
		(3)

PORT 監視の設定 回有償版限定

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。

	SA_Device T
監視・収集	● 監視 ● 収集 PORT監視 ▼
ボート	

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。

	0	② 監視・収集追加	×
		デバイス	SA_DEvice
		監視・収集	 ● 監視 ◎ 収集 PORT監視
		監視・収集項目	TCPボートOPEN確認 ▼
1	l	監視ON/OFF	⑧ 監視ON ◎ 監視OFF
	I	取得エラー判定回数	注意 1 警告 3
	l	監視項目名	TCPボートOPEN確認
	I	IPアドレス	172.0.0.0
	l	タイムアウト (秒)	5
		ポート監視パラメータ	53,80,22-23 ポート署号列
		マッチング検知 🛛 🕝 追加	[OPEN CHECK ERRとマッチしたら異常][検知回数が[1]で注意 , [3]で警告] [毎月][毎週][毎日][毎時]
		アラートメール送信先	
			 ② 追加 0キャンセル

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。

監視・収集追加		
デバイス	SA_DEvice V	
監視・収集	 ● 監視 ○ 収集 ■ 脳視方式を選択してください ▼ 	
	監視方式を選択してください PING監視 PORT監視 PORT監視	● 追加 ◎ キャンセル
	SNMPトラップ監視	

表示された項目に SNMP トラップ監視情報を設定します。

SNMP 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。

◎ 監視·収	集追加		×
デバイス		SA_Device V	
	1	 ● 監視 ○ 収集 SNMPトラップ監視 	
監視設定			
SNMP/(-	ジョン	2 🗸	
SNMPコミ	ᠴ᠋ᡔ᠇	public	
監視条件		◎ どれかひとつでも一致する ◎ すべて一致する	
SNMP-Tra	p設定		
	OID(インスタンス)	インスタンス値 通知文言	
設定1			
設定2			
設定3			
設定4			
設定5			
		 ② ③ 追加 Ø キャンセル 	

ファイル収集/ログ監視の設定 回有償版限定

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。

◎ 監視・収集追加		x
デバイス	SA_DEvice V	
監視・収集	○ 監視 ◉ 収集	
	ログ収集方式を選択してください ▼	
	ログ収集方式を選択してください	
	ファイル収集	●追加 のませいたい
	WMI収集	
	SYSLOG47	

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。

基本情報設定	
収集名	
ファイル取得方法	FTP
ログ取得IPアドレス	FTP FTP(パッシブモード) ポート番号 21
ログ取得先ディレクトリ	HTTP HTTPS
ログインユーザ名	
パスワード	MOVE(LOCAL)
パスワード確認	

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。

参 監視・収集追加	
デバイス	SA_DEvice V
監視・収集	
tra-iters.co	
23年1月18-33年 回集文	
ファイル取得方法	
	172 22 60 220 #_LEP 21
ログ取得キディレクトリ	172.23.00.239
バスワード確認	
取得ファイル設定	
取得ファイル名	(年月日時なし ▼) 圧縮無 ▼
文字コード	UTF-8 V
取得周期	□次 ▼
取得時刻	最低1件追加してください 毎時 ▼ 00 ▼
年月日差分	ファイル名に含まれる年月日は、処理を行う日付と比べて 同じ ▼
時間差分	ファイル名に含まれる時間は、処理を行う時間と比べて 同じ 🔻
保存ファイル名	名称 年月日 自動 拡張子 ・ ・ ・
アラート設定	
テキストマッチング 🛛	
ファイルサイズ最大値	0 Byte ▼
ファイルサイズ最小値	0 Byte ▼
	◎ 追加 ◎ キャンセル
	2 3

③「接続テスト」に成功したら「追加」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。

③ 監視・収集追加		×
デバイス	SA_Device V	•
監視・収集	 ◎ 監視 ◎ 収集 ログ収集方式を選択してください ▼ 	
	ログ収集方式を選択してください ファイル収集 WMN収集 SYSLOGUV集	●追加 ◎キャンセル

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
除外マッチング文字列	文字列設定あり	文字列に合致したログを取得する。

※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。

-	◎ 監視・収集追加		×
	デバイス	SA_Device	
	監視・収集	◎ 監視 ® 収集 WMI収集	
			_
(\mathbf{I})	ローカル情報収集時は「ドメイン」、「ユーサ	f」、「パスワード」を空にします。	
	ドメイン		
	ユー ザ ID		
	パスワード		
	最大取得件数	1000	
	マッチング文字列 🕑	 追加 前除 ● 	
	除外マッチング文字列	 道加 前除 ● ★ ● 	
	テキストマッチング 🕑		
		 ② ●追加 Øキャンセル 	

②「追加」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。

監視・収集追加		×
デバイス	SA_Device V	
5-19. (Dec	◎ 監視 ⑧ 収集	
	ログ収集方式を選択してください ▼	
	ロク40乗方式を選択してくたさい ファイル収集 WMI収集	● 追加 ◎キャンセル
	SYSLOG収集	

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
除外マッチング文字列	文字列設定あり	文字列に合致したログを取得する。

※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。

SecuAvail

デバイス	SA_Device V
陸組・収集	◎ 監視 ◉ 収集
	SYSLOG収集 ▼
デバイス・アプリケーション種類	
収集マッチング	
ファシリティ	全て選択/解除 kern user mail daemon security/auth syslog lpr news uucp cron/at authpriv/auth ftp ntp log audit log alert log cron/at local0 local1 local2 local3 local4 local5 local6 local7
プライオリティ	全て選択/解除 emerg alert Crit Perr Warning notice Dinfo debug
マッチング文字列 📀	 道加 前除 ●
除外マッチング文字列 😡	通加 ● ● ● ● ● ●
	UTF-8
テキストマッチング ?	

②「追加」をクリックします。

FTP 受信収集/ログ監視の設定 回有償版限定

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。

② 監視・収集追加		×
デバイス	SA_Device V	
監視・収集	◎ 監視 ● 収集	
	ログ収集方式を選択してください ▼ ログ収集方式を選択してください	
	ファイル収集)追加 0キャンセル
	FTP受信収集	

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。

SecuAvail

監視・収集追加	
デバイス	SA_Device V
17-19. (17-6k)	○ 監視 [●] 収集
四代, 47年	FTP受信収集 ▼
基本情報設定	
収集名	
ログインユーザ名	
パスワード	
パスワード確認	
取得ファイル設定	
取得ファイル名	年月日時なし ▼ 圧縮無 ▼
文字コード	UTF-8 V
取得周期	田次 V
取得時刻	最低1件追加してください 毎時 ▼ 00 ▼ 1追加
年月日差分	ファイル名に含まれる年月日は、処理を行う日付と比べて 同じ 🔻
時間差分	ファイル名に含まれる時間は、処理を行う時間と比べて 同じ 🔻
保存ファイル名	名称 年月日 自動 拡張子 □ □ □ □
アラート設定	
テキストマッチング 🛛	
ファイルサイズ最大値	0 Byte 🔻
ファイルサイズ最小値	O Byte ▼
	 (2) (1) 追加 (1) (1) (1) (1) (2) (1) (1) (1) (1) (3) (1) (1) (1) (4) (1) (1) (1) (4) (

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。

囲 監視·収集一覧				
PING				
デバイ フ	1P7 KL/7	Q 55:28 4 IV 11	烩钢备件	1
SA_Device	€172.0.0.0	Q PING Ping応答確認		

「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。

参 監視・収集変更	×
デバイス	SA_Device
監視・収集	PING
監視・収集項目	Ping応答確認
監視ON/OFF	⑧ 監視ON ◎ 監視OFF
取得エラー判定回数	注意 1 警告 3
監視項目名	Ping応答確認
IPアドレス	172.0.0.0
タイムアウト (秒)	5
ノード監視パラメータ	」 ping回数
開値設定 \ominus 追加	
アラートメール送信先 🛛 追加	
	●更新

【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。

Ⅲ 監視·収集一覧							
PING							
ギバイマ	1P77 KL/7	Q (5%28) 🕹 (17) 🗰 🔧	: 知冬 件	^			
see SA_Device	172.0.0.0	Q PING Ping応答確認					

「監視・収集変更」の画面で「削除」をクリックします。

参 監視・収集変更		×
デバイス	SA_Device	
監視・収集	PING	
監視・収集項目	Ping応答確認	
監視ON/OFF	● 監視ON ◎ 監視OFF	
取得エラー判定回数	注意 1 警告 3	
監視項目名	Ping応答確認	
IPアドレス	172.0.0.0	
タイムアウト (秒)	5	
ノード監視パラメータ	」 ping回题	
開値設定 \varTheta 追加		
アラートメール送信先 🛛 追加		
	● 更新 ○ 削除 ◎ キャンセル	

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。

Ę	取得失敗 SA_Device(172.XXX.XXX.XXX)							
		9、監視 土収集	最終日時	最終値				
	Q	SNMP 標準_UpTime	iii 2018-02-14 🕑 14:18:53	正常 804767855				
	Ŧ	SYSLOG Sendmail	ii •	不明不明				
	±	WMI WMI	······································	取得失敗				

【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〇が表示されます。



オレンジ〇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)



•

4

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。

DSV ダッシュボード 注意・警告	-			
▲ 注意·警告·不明				
発生日時	デバイス名	IPアドレス	監視·収集項目·分析	最終値
2017-05-22 🕑 13:28:34	Linux_Server	10.X.X.X	Q、SNMP LAN稼働 (ha1)	注意
2017-05-22 🕑 13:28:34	Linux_Server	@10.X.X.X	Q SNMP LAN稼働 (ethernet1/5)	注意
😥 🗮 2017-05-22 🕑 13:28:34	Linux_Server	@10.X.X.X	Q SNMP LAN稼働 (ethernet1/7)	注意
☜瓣 🕮 2017-05-22 🕑 13:28:34	Linux_Server	@10.X.X.X	Q SNMP LAN稼働 (ethernet1/3)	注意

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「ログー覧」に選択したログが表示されます。

🔽 ログデータ					
検索・ダウンロード					
<i>े </i>		2018/12/25 10:38 - 2018	/12/25 10:42	● 検索	
MyNetwork	T	 ● すべての条件に一致 ○ し 検索キーワード 	ばれかの条件に一致 を含む	_	●リセット+ -
III PING-Ping応答確認	ë	ログ一覧			<u>+</u>
■ DMZセグメント		日時		ログ内容	
	O	2018-12-25 10:40:07	status=2, value=Reply fr TTL=254	om :172.0.0.0 :: bytes=40	time=0ms
					« »

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。

ログデータ				
検索・ダウンロード				
े <i>इ</i> ग्रेन्द्र	2018/02/14 00:00	- 2018/02/14 14:57	検索キーワード	● 検索
▲ I DMZセグメント → LB01 愛 Mail_Server	三 ログ一覧			
	日時	*	ログ内容	
Web_Server_01 Web_Server_02	☐ 2018-02-14 ④ 09:21:48	Reply from 172.XX.XX.XX	bytes=40 time=1ms TTL=255	
Windows_Server		Reply from 172.XX.XX.XX	: bytes=40 time=0ms TTL=255	
 → Catalyst → CentOS 	2018-02-14 O 09:27:48	Reply from 172.XX.XX.XX	: bytes=40 time=0ms TTL=255	
▲ FG	2018-02-14 O 09:30:48	Reply from 172.XX.XX.XX	: bytes=40 time=0ms TTL=255	
> - SA_Device	2018-02-14 O 09:33:48	Reply from 172.XX.XX.XX	: bytes=40 time=0ms TTL=255	
	2018-02-14 Ø 09:36:48	Reply from 172.XX.XX.XX	: bytes=40 time=0ms TTL=255	

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。

検索・	・ダウンロード					
¢	デバイス		2017/05/22 13:00 - 20	17/05/22 14:08	検索キーワード	⊕ ŧệ;
4	O Secuavail_Cloud	:=	ログ一覧			
	Linux_Server					
	🎧 PING-性能		日時 🚽		ログ内容	
	/// PING-稼働	(11)	2017-05-22	Deels from 40.40.4.054, buter	40 Kima One TTL 000	
	🏭 SNMP-起動後経過8	C	13:34:34	Reply from 10.16.1.254: bytes=	40 time=9ms 11L=255	
	🏭 SNMP-CPU使用率		2017-05-22	Reply from 10.16.1.254; bytes=	40 time=4ms TTL=255	
	🏭 SNMP-LAN稼働 (m	e	13:31:34			
	🏭 SNMP-LAN稼働 (h:	e	2017-05-22	Reply from 10.16.1.254: bytes=	40 time=4ms TTL=255	
	🏭 SNMP-LAN稼働 (et		2017.05.22			
	🏭 SNMP-LAN稼働 (et	ē	13:25:33	Reply from 10.16.1.254: bytes=	40 time=19ms TTL=255	
	🏭 SNMP-LAN稼働 (et	[:::	2017-05-22	Rook from 10.16.1.254; buton-	40 time=4me TTL=255	
	🏭 SNMP-LAN稼働 (et	C	13:22:33	rvepiy irom ru. 16.1.254: bytes=	40 time=4ms TTL=200	
	🏭 SNMP-LAN稼働 (et		2017-05-22	Reply from 10.16.1.254: bytes=	40 time=12ms TTL=255	
	🧾 SNMP-LAN稼働 (et	G	10.18.00			

【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。

検索・タウンロート					
ਂ <u>ਜ</u> ਸਮੁਤ		2017/05/22 13:00 - 20	17/05/22 14:08	検索キーワード	●検索
🔺 🕔 Secuavail_C	Noud ≋≡	ログ一覧			÷
🔺 🍶 Linux_S	Server				
🗐 PIN	IG-性能	日時 🚽		ログ内容	
iii Pin iii SN	IG-稼働 MP-起動後経過B	≣ 2017-05-22 ᠑ 13:34:34	Reply from 10.16.1.254: bytes=4	0 time=9ms TTL=255	
iii SN	MP-CPU使用率 MP-LAN稼働 (m	≣ 2017-05-22 ⊇ 13:31:34	Reply from 10.16.1.254: bytes=4	0 time=4ms TTL=255	
🥼 SN	MP-LAN稼働 (h:	≣ 2017-05-22 ⊇ 13:28:34	Reply from 10.16.1.254: bytes=4	0 time=4ms TTL=255	
iii SN	MP-LAN稼働 (et (≣ 2017-05-22 Э 13:25:33	Reply from 10.16.1.254: bytes=4	0 time=19ms TTL=255	
i sn ii sn	MP-LAN稼働 (et)(MP-LAN稼働 (et)(2017-05-22 13:22:33	Reply from 10.16.1.254: bytes=4	0 time=4ms TTL=255	
iii sn iii sn	MP-LAN稼働 (et)(MP-LAN稼働 (et)(≣ 2017-05-22 Э 13:19:33	Reply from 10.16.1.254: bytes=4	0 time=12ms TTL=255	

※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。
SecuAvail

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。

<u>.u.</u>	アカウント管理・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・								
							▲アカウント追加		
	ューザID 「	🍬 ユーザ名	👌 種類	👆 ב=עלי–ב		登録	🛓 更新 🏷		
ad	Imin	admin	管理者	$Q \square \not \sim \infty$		2015-06-11 11:58:03	2015-06-11 11:58:03		

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。

	■ ユーザ管理	×
	ユーザID	admin
	<u> ፲</u> –ቻ <u>ጸ</u>	admin
	種類	管理者
2	現在のパスワード	now password
	新しいパスワード	new password
	新しいパスワード確認	confirm new password
	ユーザメニュー設定	 ✓ Q監視・モニタリング ✓ □ログデータ ✓ ♪監視・ログ収集設定 ✓ ぱシステム管理
		① 更新 キャンセル

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。

<u>al</u> P	アカウント管理							
							▲アカウント追	DO
_	LーザID 🕓	ユーザ名	種類	└ৡ ユーザメニュー	\	登録	更新	1. 1
admin		admin	管理者	Q [] K of		2015-06-11 11:58:03	2015-06-11 11:58:03	

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。

	■ アカウント追加	x
	種類	一般ユーザ
\mathbb{D}	םד ע -יב	
	ユ− ቻጿ	
	パスワード	
	パスワード確認	
2	ユーザメニュー設定	 ④ Q監視・モニタリング ④ □ログデータ ✓ ♪監視・ログ収集設定 ◎ \$ ◎\$>ステム管理
		 3 5 (***)

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。

通 アカウント	アカウント管理 🗸								
						▲アカウント追加			
ユーザル) 🐚 ユーザ名	- 👌 種類 \	コーザメニュー		登録	• 更新 👆			
SA_User	SA_User	一般ユーザ	Q 🖓 🕫		2018-12-19 17:51:03	2018-12-19 17:51:03			
admin	admin	管理者	Q 🖓 🔎 🖉 🕫		2015-06-11 11:58:03	2018-12-19 16:59:08			

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。

<u>.ul</u>	アカウント管理・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・							
▲ アカ						▲アカウント追加		
	ユーザID 🐚		種類	ב	♦ 登録 ¹	更新		
SĄ	_User	SA_User	一般ユーザ	Q 💭 🕫	2018-12-19 17:51:03	2018-12-19 17:51:03		
adı	nin	admin	管理者	Q₽₽¢₿	2015-06-11 11:58:03	2018-12-19 16:59:08		

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。

	■ ユーザ管理		×
(]) ב- ע -ב	SA_User	
		SA_User	
	種類	一般ユーザ	
	新しいパスワード	new password]
	新しいパスワード確認	confirm new password]
	ユーザメニュー設定	 ✓ Q監視・モニタリング ✓ □ログデータ ✓ ● ✓ 監視・ログ収集設定 ✓ ペシステム管理 	
		(2) 更新 削除 キャンセノ	L

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。

표 アカ	アカウント管理							
								▲アカウント追加
<u>ב</u> -	-ザID 🕓	그 ザ名	種類	ユーザメニュー		登録		更新 🛛 🕌
SA_Use	r	SA_User	一般ユーザ	Q [] ¢ ;		2018-12-19 17:51:03		2018-12-19 17:51:03
admin		admin	管理者	Q [] & \$		2015-06-11 11:58:03		2018-12-19 16:59:08

表示された「ユーザ管理」画面で「削除」をクリックします。

■ ユーザ管理	×
ユーザID	SA_User
ユ− ቻΆ	SA_User
種類	一般ユーザ
新しいパスワード	new password
新しいパスワード確認	confirm new password
ユーザメニュー設定	 ✓ Q監視・モニタリング ✓ □ログデータ ✓ 監視・ログ収集設定 ✓ \$ ✓ \$ >>ステム管理
	更新 削除 キャンセル

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。

🎍 🕨 PC 🕨 ローカル ディスク (C:) 🕨 Lo	LogStareCollec ,			
名前				
🐌 app_tmp	2018/12/19 11:46	ファイル フォルダー		
퉬 etc	2018/12/19 11:46	ファイル フォルダー		
鷆 lib	2018/12/19 11:46	ファイル フォルダー		
퉬 license	2018/12/19 11:46	ファイル フォルダー		
퉬 logs	2018/12/19 11:46	ファイル フォルダー		
퉬 sbin	2018/12/19 11:46	ファイル フォルダー		
퉬 tools	2018/12/19 11:46	ファイル フォルダー		
퉬 webapp	2018/12/19 11:46	ファイル フォルダー		
🔊 LogStare Collector	2018/12/19 11:46	インターネット ショー	1 KB	
🕓 uninst.exe	2018/12/19 11:46	アプリケーション	364 KB	

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。



「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「Is」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。

	LogStare Collector ライセンス	+
ライセンスタイプ	無償版	
有効期間		
ライセンスコード		

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。

\$	LogStar	e Collector ライセンス登録 ×
∍	イセンス	ファイルを選択 選択されていません
		百新したないたか

SecuAvail

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。
2010 年 1 日 10 日	1.6.0	アカウント管理機能を追加。
2019 - 1 月 10 日		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。



