

Windows SNMP-L2

製品マニュアル

株式会社ロジックベイン Tel: 044-852-4200 Fax: 044-854-0979 e-mail: <u>support@lvi.co.jp</u>

目次

1	製品概要	3
2	インストール	4
3	環境設定	6
4	プロセス監視	7
5	サービス監視	10
6	CPU 監視	12
7	メモリ監視	15
8	ログ監視	18
	8-1 アプリケーションログの監視設定	18
	8-2 Windows イベントログの監視設定	19
9	アンインストール	20
10) Windows SNMP のインストール/設定	21
	10-1 インストール(Windows server 2008/2008 R2)	21
	10-2 インストール(Windows 7)	23
	10−3 Windows SNMPの設定	25

※「Windows SNMP-L 無料版」について

Windows SNMP-L の「無料版」プログラムは、使用期間に制限はなく、「製品版」と同様の機能で使用することが可能です。

ただし「無料版」に対して、基本的に電話/メールでのサポートは行いません。

1 製品概要

本モジュールは Windows-OS を搭載したサーバのリソース監視を強化するためのモジュールです。 Windows にデフォルトで実装されている SNMP エージェントを利用し、閾値を設定し障害検知時に は SNMP マネージャーへトラップを転送します。



本モジュールにて監視できる項目は以下のとおりです。

- ➢ Windows サービス監視
- ▶ プロセス監視
- ➢ CPU 利用率
- ▶ メモリ使用量
- Windows イベントログ
- ▶ テキスト形式のログファイル

【動作環境】

機能項目	SNMP Agent モジュール	
OS	Windows Vista/7/8 (32/64bit)	
	Windows server 2003 R2/2008/2008 R2/2012/2012 R2 (32/64bit)	
必要プログラム	SNMP エージェント(Windows 付属)	
Java Runtime Enviroment 7 以上		
	.NetFramework 4.5.1 以上	

LogicVein

2 インストール

SNMP-L2 インストールする際は、Administrator 権限を持つユーザーでログインしインストールして ください。

- 1. インストーラーを起動します。
- 2. 「次へ」をクリックします。



3. 「同意します」を選択し、「次へ」をクリックします。



4. インストールディレクトリを選択し、「次へ」をクリックします。

牵 WindowsSNMP-L セットアップ	
インストール先を選んでください。 WindowsSNMP-しきインストールするフォルダを選んでください。	4
Wedwei5NMP-Lを以下のフォルグロインストールします。夏なったフォル 第1 を押して、別のフォルタを確認していたさい。続けないましたく1 をクリ	タコンインストールするこえ しき ックして下さい。
ィインストール先 フォルダ	
	942(R).
必要なディスクスペース: 33MB 利用可能なディスクスペース: 3723GB	
· Select Intel System of A 《 要选(B)	>次へ(N)> キャンセル

5. フォルダ名を入力し、「インストール」をクリックします。



以下の画面でインストール完了です。



3 環境設定

環境設定では、MIBを取得するためのコミュニティ名やトラップの送信先設定を行います。

🔜 SNMP-L 設定 💦 💦 💦 🥐 🔀
プロセス サービス メモリ/HDD CPU ログ 環境設定
- トラップ送信先設定
管理サーバ1: 127.0.0.1
管理サーバ2:
ポート: 162 文字コード: Shift_JIS ▼
コミュニティ: public
- SNMPサービス
読取りコミュニティ: public
アクセスモード: SNMP V1
ポーリング間隔: 10 (秒) ポート: 161
<u> </u>
- SNMP V3認証
認証: MD5 V/V:
ユーザ: パスワード:
ステータス再取
メインサービス: 実行中
ログサービス: 実行中

項目		説明	
トラップ送信先設定 管理サーバ1		トラップ送信先の IP アドレス(IPv4/v6)	
	管理サーバ 2	2の設定は任意	
	ポート	トラップ送信先のポート	
	文字コード	トラップの文字コード	
	コミュニティ	トラップコミュニティの設定	
基本設定	読み取りコミュニティ	MIB を取得する際のコミュニティ名	
	アクセスモード	SNMP のバージョン設定	
インターバル IPv6 対応		MIB の取得間隔	
		サーバが IPv6 のみ対応している場合に使用	
		Windows SNMPとの接続確認	
	**	設定の保存	

LogicVein

4 プロセス監視

稼動しているプロセスの監視設定をします。

【設定手順】

	プロセス: snmpc32.exe	-	
L	ノきい値設定: snmpc32.exe > ▼ 0		
N=	シプメッセージ:		
		×	
	MIB を取 現在稼動	れ得して 姉しているプ	ロヤス
クロセスリスト			_ 🗆
 プロセス名	1/2	パラメータ	
okserv.exe	C:¥Program Files (x86)¥SNMPc Network M		
conhost.exe	¥??¥C:¥Windows¥system32¥		
conhost.exe	¥??¥C:¥Windows¥system32¥		
cpqnimgt.exe	C:¥Windows¥system32¥CPQNiMgt¥		
cpqrcmc.exe	C:¥Windows¥system32¥		
cpqteam.exe	C:¥Program Files¥HP¥NCU¥		
cqmghost.exe	C:¥Windows¥system32¥CpqMgmt¥cqmgho		
cqmgserv. exe	C:¥Windows¥system32¥CpqMgmt¥cqmgser		
cqmgstor.exe	C:¥Windows¥system32¥CpqMgmt¥cqmgstor¥		
crserv. exe	C:¥Program Files (x86)¥SNMPc Network M		
csrss. exe	%SystemRoot%¥system32¥		
	% System Poot% Youtom 20Y		
csrss. exe	703y3CEITINUUC70#5y3CEITI32#		
csrss. exe csrss. exe	%SystemRoot%¥system32¥		
csrss. exe csrss. exe dbex. exe	%SystemRoot%¥system32¥ C:¥Program Files (x86)¥SNMPc Network M		
csrss. exe csrss. exe dbex. exe discagt. exe	%SystemRoot%¥system32¥ C:¥Program Files (x86)¥SNMPc Network M C:¥Program Files (x86)¥SNMPc Network M		
csrss.exe csrss.exe dbex.exe discagt.exe dwm.exe	%SystemRoot%¥system32¥ C:¥Program Files (x86)¥SNMPc Network M C:¥Program Files (x86)¥SNMPc Network M C:¥Windows¥system32¥		
csrss.exe csrss.exe dbex.exe discagt.exe dwm.exe explorer.exe	%SystemRoot%¥system32¥ C:¥Program Files (x86)¥SNMPc Network M C:¥Program Files (x86)¥SNMPc Network M C:¥Windows¥system32¥ C:¥Windows¥		

2. 「しきい値設定」にて、条件を入力します。



【入力例】

snmp32.exe	> 5	snmp32.exe が 6 個以上存在する場合にトラップ送信
snmp32.exe	>= 5	snmp32.exe が 5 個以上存在する場合にトラップ送信
snmp32.exe	< 5	snmp32.exe が4個以下の場合にトラップ送信
snmp32.exe	<= 5	snmp32.exe が 5 個以下の場合にトラップ送信
snmp32.exe	!= 5	snmp32.exe が 6 個以上、4 個以下の場合にトラップ送信
snmp32.exe	= 5	snmp32.exe が 5 個存在する場合にトラップ送信

3. 「トラップメッセージ」欄にトラップが送信された際のメッセージを入力します。このメッセージに は以下の引数を使用することが可能です。

> トラップメッセージ: \$Pがしきい値を超過しました。(現在値: \$c) \$s (しきい値: \$o)

引数	説明	
\$P	プロセス名	
\$s	不等号	
\$c	現在の稼働数	
\$o	しきい値で設定されたプロセス数	

【入力例】



4. 1 ボタンをクリックして設定を保存します。

プロセス名	条件	プロセス数	トラップメッセージ
snmpc32.exe	>	5	\$Pがしきい値を超過しました

5 サービス監視

サービスの稼働状況を監視します。万がー、サービスがダウンした場合にはサービスを起動する 設定を行うことが可能です。

【設定手順】

 「サービス」欄に監視するサービスを入力、または、 50 をクリックし登録されているサービス 一覧から監視するプロセスを選択します。



サービスが停止した場合に起動させたい場合にはチェックを有効にし、コマンドを入力します。
 ※この設定はオプションです。必須ではありません。



3. 「トラップメッセージ」欄にトラップが送信された際のメッセージを入力します。このメッセージに は以下の引数を使用することが可能です。

トラップメッセージ:	
\$Sサービスが停止しました。	ľ

引数	説明
\$S	プロセス名

【入力例】



4. 1 ボタンをクリックして設定を保存します。

再起動	サービス名	再起動コマンド	トラップメッセージ
	netLD	net start netLD	\$Sサービスが停止しまし

6 CPU 監視

サーバの CPU 利用率の監視を行います。この監視では、「HrProcessorEntry」の MIB テーブルを 使用し監視を行います。Windows タスクマネージャーのパフォーマンスタブで確認できる CPU 利用 率とは少し異なりますのでご注意ください。

【設定方法】

1. 🔜 をクリックししきい値を設定する index を選択します。



2. 「設定」にしきい値と積算回数(もしくは連続回数)を設定します。

<積算回数選択時>	<連続回数選択時>
しきい値: 30 %	しきい値: 30 %
連続回数(回): ▼ 3	積算回数(回): ▼ 3

【入力例】・・・しきい値:30 (インターバルタイム:60秒)







3. 「トラップメッセージ」欄にトラップが送信された際のメッセージを入力します。このメッセージに は以下の引数を使用することが可能です。



引数	説明
\$C	CPU 使用率
\$Т	しきい値
\$O	連続回数
\$o	積算回数

【入力例】

トラップメッセージ欄	CPU 利用率 30%を\$o 回超過しました。	
トラップメッセージ	CPU 利用率 30%を 3 回超過しました。	

4.
1 ボタンをクリックして設定を保存します。

No	index	しきい値	超過時間	超過回数	メッセージ
1	2	30	0	3	CPU利用率30%を\$o回超

7 メモリ監視

サーバのメモリ使用量の監視を行います。

【設定方法】

1. S をクリックししきい値を設定する index を選択します。

	 メモリ使用量 タイプ: サイズ: 使用量: トラップメッセ 	ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ: ジ:	GB 💌	
***	<u></u>	MIB 現在	を取得して での値を表示	
index	タイプ		サイズ	 使用量
index 1	タイプ hrStorageFixedDisk	説明 C:¥ Label: Serial Number 88abd681	サイズ 499.017G	使用量 99.639G
index 1 2	タイプ hrStorageFixedDisk hrStorageVirtualMemory	説明 C:¥ Label: Serial Number 88abd681 Virtual Memory	サイズ 499.017G 25.746G	使用量 99.639G 4.34G
index 1 2 3	タイプ hrStorageFixedDisk hrStorageVirtualMemory hrStorageRam	説明 C:¥ Label: Serial Number 88abd681 Virtual Memory Physical Memory	サイズ 499.017G 25.746G 12.874G	使用 <u>量</u> 99.639G 4.34G 3.614G

2. 「設定」にしきい値と積算回数(もしくは連続回数)を設定します。

<積算回数選択時>

設定 しきい値: 4	GB 💌
連続回数(回): 🔻	3

<連続回数選択時>

-設定 しきい値:	4	GB	•
積算回数(回]): 🔻	3	

【入力例】・・・しきい値:4GB (インターバルタイム:60秒)

積算回数 1 メモリ使用量が 4GB を 1回超えた場合にトラップ送信

しきい値		
		トラップ送信
	60 秒	





3. 「トラップメッセージ」欄にトラップが送信された際のメッセージを入力します。このメッセージに は以下の引数を使用することが可能です。



引数	説明
\$U	メモリ使用量
\$Т	しきい値
\$O	連続回数
\$o	積算回数

【入力例】

 トラップメッセージ欄
 メモリ使用量が 4GB を\$o 回超過しました。現在値:\$UGB

 トラップメッセージ
 メモリ使用量が 4GB を 3 回超過しました。現在値:4.23GB

4.
ゴ ボタンをクリックして設定を保存します。

No	index	しきい値	超過時間	超過回数	メッセージ
1	2	30	0	3	CPU利用率30%を\$o回超

8 ログ監視

サーバ稼働しているアプリケーションのログや Windows のイベントログの監視を行います。特定の 文字列を指定し、その文字列が含まれていたログを検知しマネージャーへトラップ送信します。 ※アプリケーションのログはテキスト形式に限ります。バイナリ形式のログは監視できません。

8-1 アプリケーションログの監視設定

アプリケーションのログの監視では、ログタイプを「FileLog」に設定します。

1. ログタイプを「FileLog」に設定し、Saleをクリックして監視するログファイルを指定します。

- 監視ログ	指定			
名前:	testLog0	ログタイプ:	FileLog	•
ファイル	パス: C:¥Users¥Ad	mini <i>s</i> trator¥D	esktop¥logs¥testL	

2. ファイルの文字コードを指定後、マッチルールに検知する文字列を入力します。

文字コード:	Shift_JIS
マッチルール:	,*error.*

※マッチルールは正規表現で指定します。

3. トラップメッセージを指定し、 Mereory Structure Structure



4. 最後にとしをクリックし、設定を反映させます。

トラップメッセージ:	+ ×	H
testLog0 : \$M		

※ きクリック後、ログファイル監視のプログラムが自動で再起動し、設定が反映されます。

LogicVein

8-2 Windows イベントログの監視設定

アプリケーションのログの監視では、ログタイプを「WinLog」に設定します。

1. ログタイプを「WinLog(xxx)」に設定します。監視したいログに合わせて指定して下さい。

□ 監視ログ指定 -			
名前: testL	.og0	ログタイプ:	WinLog (Applicatic -
ファイルパス:			FileLog
	1		WinLog (Application)
文字コード:	Shift ITC		WinLog (System)
		<u> </u>	WinLog (Security)
		Ξ	Windows ログ
			🛃 アプリケーション
			🛃 セキュリティ
			🗐 Setup
			🛃 システム
			Forwarded Events

2. マッチルールに検知する文字列を入力します。

マッチルール: .*error.*	
※マッチルールは正規表現で指定します。	

3. トラップメッセージを指定し、 🔜をクリックし追加します。

トラップメッセージ:	-	×	H
testLog0 : \$M			

4. 最後にとしをクリックし、設定を反映させます。



※ きクリック後、ログファイル監視のプログラムが自動で再起動し、設定が反映されます。

9 アンインストール

1. Windows のコントロールパネルを開き、「WindowsSNMP-L」をアンインストールします。



2. 「アンインストール」をクリックし、アンインストールします。

🎯 WindowsSNMP-L 🤈	シインストール		_ 🗆 🗙
WindowsSNMP-Lの WindowsSNMP-Lをこ	アンインストール のコンピュータから削除します。	l	8
WindowsSNMP-LIま、 「アンインストール」 をクリッ	以下のフォルダからアンインストールされます。 っクして下さい。	、アンインストールを始めるには	
アンインストール元:	C#Program Files (x86)#WindowsSNMP-L		
Nullsoft Install System	v2.46	アンインストール(U) キャン・	tu

10 Windows SNMP のインストール/設定

Windows SNMP-L が動作するためには、Windows SNMP がインストール/設定されている必要があります。

10-1 インストール(Windows server 2008/2008 R2)

- 1. Windows のスタートから「コントロールパネル」を開きます。
- 2. 「Windows の機能の有効化または無効化」をクリックします。



3. 機能を選択し、「機能の追加」を選択します。

		_ 🗆 ×
加または削除します。		
	👔 機能の概要ヘルプ	
	a 1版 配 00月11P本	

4. 「SNMP サービス」にチェックを挿入し、「次へ」をクリックします。

##20週加ウィザード 機能の選択		B
我我的 ##22 :通问时状况: #5#	20サーバービインストールする機能を10以上式研します。 検知20 ・ NET Framework 3.5.1 の機能(インストールされています)。 Briticker ドライブ暗発化 BranchCache DirectAccess 管理ゴンソール。 HTTP プロキッを提出した PRG UPR ポート モニター RDG (Renote Differential Compression) SAN 開起後坂マネージャー Simple TCP/IP Services SMTP サーバー Tohet サーバー TFTP クライアント URD パーム ファリケーション/用サブシステム Windows Server パックアック機能 Windows Server パックアック機能	1898 <u>858 2547-5898701-16 (SHMP)</u> <u>4-19377</u> Simp 4-12 Simp WMT707(4-#821)Cog
	(前下四) (这本(()	> (1028-000) (##5000)

5. 「インストール」をクリックし、インストールします。

秋秋 日前日 1月1日日大元	はの役割、役割サービス、または掲載をインストールするには、【インストール】をクリックしてくだたい。 ① 次の1 件の場間メッセージ
15 4	 ④ インストールの売了値に、このサーバーの両起動が必要になる場合があります。 ● SNMP サービス SNMP サービス WHI SNMP プロパイダー
	この情報を印刷、電ディールで決任。または住存

以下の画面が表示されれば、インストール完了です。

根金の追加ウィザード			•
インストールの結果			
	次の役割、役割サービス、または秘訣が正常に	インストールされました	
	SNMP サービス たの間他がインストールそれました SNMP サービス WHI SNMP プロパイダー	🤣 インストールが正常に完了しました	
	インストールレポートな印刷、電子メール逆域	2011/211	
		NAE) Sta(U) NOC	1

10-2 インストール(Windows 7)

- 1. Windows のスタートから「コントロールパネル」を開きます。
- 2. プログラムと機能をクリックします。



3. 「Windows の機能の有効化または無効化」をクリックします。



4. 「簡易ネットワーク管理プロトコル(SNMP)」にチェックを入れ、OK をクリックします。

Windows の機能	×
Windows の機能の有効化または開始化	0
機能を有効にするには、チェック ポックスをオンにしてください。機能を開効にするには、 りつぶされたチェック ポックスは、機能の一部が有効になっていることを表します。	チェック ポックスをオフにしてください。 道
E Windows Search	
E Windows TIFF I Filter	
三丁。 Windows ガジェット プラットフォーム	
🗄 🔜 🖉 Windows プロセス起動サービス	
■ XP5 サービス	
■ XP5 ビューアー	
∃ 🚮 インターネット インフォメーション サービス	
二人 インターネット インフォメーション サービスのホスト可能な Web コア	
二】 インデックス サービス	
日 二月 ゲーム	
∃ ■ ▲ メディア機能	
3 単 印刷とドキュメント サービス	
10 「「「「「「」」「」「」」「「」」「」」(echo、 daytime など)	
③ 2014 新潟ネットワーク管理プロトコル (SNMP)	-
	OK キャンセル

Microsoft Windows	
しばらくお待ちください。 処理には数分かかることが	傍時に変要を加えています。この あります。
	(##>/m/



10-3 Windows SNMPの設定

- 1. Windows のサービスを開きます。
- 2. サービス一覧より、「SNMP Service」を右クリック->[プロパティ]をクリックします。

サーバーマネージャ	4-P2					操作
1941	名前 -	规明	状態 [2	タートアップの理想	0232	サービス
日本日本 1985 日 日 イベトビュ	Security Accounts Server Shell Hardware Det	2009. 2001.	開始 E 開始 E 開始 D	載力 載力 載力	Local S., Local S., Local S.,	MONT
 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	Smart Card Smart Card Remov.	200-		#b #b	Local S. Local S.	(LOH)_
 ● タスクスケシ ● セキュリティオ ● サービス ● サービス ● サービス ● サービス ● ローカル ユー ● 記憶塔 	SNMP Trap SNMPC OnLineID. SNMPC (NoTP) SNMPC (2)/97. SNMPC	(存止(0) - 1519 - 1519 - 1519 - 1519 - 1519 - 一 一 一 日 日 日 一 一 日 日 一 一 日 日 一 一 日 日 一 一 一 日 一 一 一 一 日 一 一 一 日 一 一 一 日 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	ELOT ELOT 82.200() 新聞に更好(F) 4(R)	• JEE(MML)	Local S. Local S. Local S. Local S. Local S. Local S. Network Local S. Local S.	

3. 「セキュリティ」タブに移動し、コミュニティ名やアクセスできるホストの設定をします。

(SNMP10) SNMP Service のプロパティ	×
全般 ログオン 回復 エージェント トラップ セキュリティ 依存関係	
☑ 認証トラップを送信する(U)	
受け付けるコミュニティ名(N)	
追加(D) 編集(E) 削除(R)]
 ○ すべてのホストから SNMP パケットを受け付ける(C) ○ これらのホストから SNMP パケットを受け付ける(T) Localbost 	
<u>這加</u> 編集(1) 削除(M)	
の詳細を表示します	
OK キャンセル	適用(A)

4. 「OK」をクリックします。

以上で設定が完了します。

LogicVein