# 2-1. ZABBIXで可能な監視

監視リスト記入内容

通信4社としてZABBIXにて行っている監視設定、メッセージ種別、重要度の定義は以下の通りです。

- ◆基本監視項目◆ ◆その他監視項目◆ ◆メッセージ種別◆
- ◆アラートレベル(重要度)の定義◆

#### ◆基本監視項目◆

監視項目

III. 170 - X 14		THE 120 2 - 1	1 HD > 11 3 H		, , , , , , , , , , , , , ,				001141110			
	監視項目 1	監視項目 2	監視対象			有無				UX		
PING監視	PNG	vip	IP	Virtual IPからのPing応答 ※瞬断を考慮し3回連続失敗で発報	【xx】[xx]ホスト名の疎通が確認できません	無	0	0	0	0	0	0
		rip	IP	実IPからのPing応答 ※瞬断を考慮し3回連続失敗で発報	【xx】[xx]ホスト名の疎通が確認できません	無	0	0	0	0	0	0
ZABBIX Agent監 視	AGE	age	-	Agentの可用性のチェック	【xx】[ZABBIX]ZABBIXエージェントが停止しました	有	0	0	0	0	0	0
CPU使用率監視	CPU	сри	閾値(%)	CPU使用率(%)	【xx】[xx]CPU使用率がxxを超過しました	有	0	0	0	0	0	0
メモリ監視	MEM	mem	閾値(%)	メモリ使用率(Windows, Solaris, 他) ※total - free / total = 使用率	【xx】[xx]メモリ使用率がxxを超過しました	有	0		0			
			閾値(%)	メモリ使用率(Linux, HP-UX, 他) ※total - (free + buffers + cached) / total = 使用率	【xx】[xx]メモリ使用率がxxを超過しました	有		0		0	0	0
ディスクI/0監視 (Windows)	1/0	rbs	閾値 (Byte)	読み込み処理中にディスクにデータ が転送される速度(バイト/秒)	【xx】[xx]読込DiskI/OがxxByte/secを超過しました	有	0					
		wbs	閾値(Byte)	書込み処理中にディスクにデータが 転送される速度(バイト/秒)	【xx】[xx]書込DiskI/OがxxByte/secを超過しました	有	0					
		dql	閾値(個)	ディスクに残っている処理待ちま たは処理中のキューの要求数	【xx】[xx] Disk queueがxxを超過しました	有	0					
ディスクI/0監視 (Linux)	I/0	rbs	閾値(sectors)	読込み処理中にディスクにデータ が転送される速度(sectors/秒)	【xx】[xx] 読込DiskI/Oが xx sectors/secを超過しました	有		0				
		wbs	閾値(sectors)	書込み処理中にディスクにデータが 転送される速度(sectors/秒)	【xx】[xx]書込DiskI/Oが xx sectors/secを超過しました	有		0				
ディスクI/0監視 (Solaris)	I/0	rbs	閾値 (Byte)	読み込み処理中にディスクにデータ が転送される速度(バイト/秒)	【xx】[xx]読込DiskI/OがxxByte/secを超過しました	有			0			
		wbs	閾値(Byte)	書込み処理中にディスクにデータが 転送される速度(バイト/秒)	【xx】[xx]書込DiskI/OがxxByte/secを超過しました	有			0			
ディスクI/0監視 (HP-UX)	1/0	rbs	閾値(Byte)	読み込み処理中にディスクにデータ が転送される速度(バイト/秒)	【xx】[xx]読込DiskI/OがxxByte/secを超過しました	有				0	0	0
		wbs	閾値 (Byte)	書込み処理中にディスクにデータが 転送される速度(バイト/秒)	【xx】[xx]書込DiskI/OがxxByte/secを超過しました	有						
ネットワークイ ンタフェース監 視	NIF	nii	eth0/閾値(パケット)	ネットワークインタフェースeth0の 受信統計(パケット数)	【xx】[xx]ネットワークインタフェースの受信統計が xxを超過しました	有		0				
※eth0のみ設定		nio	eth0/閾値(パケット)	ネットワークインタフェースeth0の 送信統計(パケット数)	【xx】[xx]ネットワークインタフェースの送信統計が xxを超過しました	有		0				

アラームメッセージ内容

## ◆その他監視項目◆

監視項目	監視リスト記入内容		卜記入内容	監視内容	アラームメッセージ内容		Win	Linux	Solaris	HP-	AIX	Tru64
	監視項目1	監視項目 2	監視対象			有無				UX		
サービス監視	SRV	srv	サービス名	任意のwindowsサービスの停止	【xx】[xx]サービス名が停止しました	有	0					
プロセス監視	PRC	prc	プロセス名/最小起動数	プロセスの最小起動数 ※255バイト以下のプロセス名	【xx】[xx] プロセス名プロセスが閾値を下回りました	有	0	0	0	0	0	0
				プロセスの超過起動数 ※255バイト以下のプロセス名	or 【xx】[xx]プロセス名プロセスが閾値を超過しまし た	有	0	0	0	0	0	0
		cmd	<user><cmdline>最 小起動数</cmdline></user>	コマンドラインでのプロセス起動 数		有		0	0	0	0	0
ロードアベレー ジ監視	CPU	lod	閾値(浮動小数点)	CPUのロードアベレージ(浮動小数点)	【xx】[xx]Load Averageがxxを超過しました	有		0	0	0	0	0
スワップメモリ 監視	SME	mem	閾値(%)	スワップメモリ使用率	【xx】[xx]スワップメモリ使用率がxx%を超過しました	有	0	0	0	0	0	0
ディスク使用率 監視	DSK	cdr∼zdr	閾値(%)	C~Zドライブの使用率	【xx】[xx]・・・のディスク使用率がxx%を超過しました	有	0					
		pat	パス/閾値(%)	パーティションの使用率		有		0	0	0	0	0
ファイルシステ ム監視	FIL	fil	パス/閾値(Byte)	ファイルサイズの監視	【xx】 [xx】・・・ファイルのサイズ容量がxxByteを 超過しました	有	0	0	0	0	0	0
		ind	パス/閾値(%)		【xx】[xx]・・・のiノード使用率がxx%を超過しました	有		0	0	0	0	0
		exi	パス	ファイル存在の監視	【xx】[xx] ・・・ファイル名が存在しないことを 検知しました	有	0	0	0	0	0	0

					【xx】[xx] ・・・ファイル名の存在を検知しました							
ファイルタイム スタンプ監視		tsp	パス	対象のタイムスタンプと監視実行 時の時刻の差の監視	【xx】[xx] ・・・ファイル名が更新されていません	有	0	0	0	0	0	0
ネットワークイ ンタフェース監 視	NIF	nii	インタフェース名/ 閾値(パケット)	ネットワークインタフェースの受信統計(パケット数)	【xx】[xx] ネットワークインタフェースの受信統計がxxを超過しました	有		0	0	0		
※eth0以外		nio	インタフェース名/ 閾値(パケット)	ネットワークインタフェースの送 信統計(パケット数)	【xx】[xx]ネットワークインタフェースの送信統計がxxを超過しました	有		0	0	0		
パフォーマンス カウンター監視	PER	per	オブジェクト名/カ ウンタ名/インスタ ンス名/閾値	パフォーマンスカウンター値の監 視 	【xx】[xx]・・・がxxを超過しました	有	0					
Windowsイベント ログ監視	LOG	osl dbl apl	ログファイル	EventlogのOS_LOG監視	【xx】[xx]エラーをEventlogで検知しました	有	0					
ログ監視			ログファイル	OS、アプリケーション、ミドルウェアのログ監視	【xx】[xx] エラーをファイル名で検知しました	有	0	0	0	0	0	0
時刻ずれ監視	TIM	tim	時刻ずれ	Zabbixマネージャと localホストの時刻ずれ(秒)	【xx】[xx]xx秒以上の時刻ずれを検知しました	有	0	0	0	0	0	0
サービスポート (TCP) 監視	PRT	tcp	ポート番号	指定したポート番号のコネクション監視 (TCPのみ)	【xx】[xx]Portxxの接続に失敗しました	無	0	0	0	0	0	0
WEB監視	URL	url	URL/要求文字列/タ イムアウト値(s)	指定したURLの正常性チェック	【xx】[xx]URLへのWEBアクセスに失敗しました	無	0	0	0	0	0	0
		pur	URL/プロキシサー バのホスト名とIP アドレス/参照先の ポート番号/タイム アウト値(s)	Proxy経由の指定URL正常性チェック	【xx】 [xx] Proxy名経由でのURLへのWEBアクセスに 失敗しました	無	0	0	0	0	0	0
SNMPトラップ監 視	SNMP	trp	SNMPトラップ	対象機器のSNMPエージェントから 送信されるトラップの監視	【xx】[xx]ホスト名(IPアドレス)任意のメッセージ	無	0	0	0	0	0	0
SNMPポーリング 監視		pol	SNMP	対象機器のSNMPエージェントに対 してのポーリング監視	【xx】[xx]ホスト名(IPアドレス)任意のメッセージ	有	0	0	0	0	0	0
DNS監視	DNS	dns	ドメイン名	ZABBIXマネージャからDNSを指定 してのnslookupによる名前解決 確認	【xx】 [xx] xx用DNSにて外部名前解決が失敗しました。         or [xx】 [xx] ドメイン名 ドメインの名前解決に失敗しました。	無	0	0	0	0	0	0
		pdn	ドメイン名	監視対象上でのnslookupによる 名前解決確認 (監視対象上で設定されている DNSでの名前解決確認)	【xx】[xx]ドメイン名 ドメインの名前解決に失敗しました	有	0	0	0	0	0	0
Latency監視	LTC	psc	IP (閾値:ミリ秒)	NW応答時間の監視	【xx】[xx]ネットワーク応答時間がxxを超過しました	無	0	0	0	0	0	0
		spf	サービス, ポート 番号 (閾値:ミリ秒)	サービスのパフォーマンス監視 (サービスは、ssh、 ntp、 Idap、smtp、ftp、http、pop、 nntp、imap、topの何れか1つ)	【xx】[xx]サービスへの接続時間がxxを超過しました	無	0	0	0	0	0	0

内容

## ◆メッセージ種別◆

メッセージグループ名称

カテゴリ

	メッセーフッルーフ石が	23 7 4 9	LAM.
基本(固定)	AP	AP	アプリケーションエラーに関するメッセージ
	Job	Job	ジョブに関するメッセージ
	Database		データベースに関連するメッセージ
	Database_C1		データベースに関連するメッセージ (基盤用)
	Database_C2		データベースに関連するメッセージ (基盤用)
	Database_C3	Database	データベースに関連するメッセージ (基盤用)
	Database_C4		データベースに関連するメッセージ (基盤用)
	Database_Y		データベースに関連するメッセージ (基盤用)
	Performance		性能低下や資源不足に関するメッセージ
	Performance_C1		性能低下や資源不足に関するメッセージ(基盤用)
	Performance_C2	Performance	性能低下や資源不足に関するメッセージ(基盤用)
	Performance_C3		性能低下や資源不足に関するメッセージ(基盤用)
	Performance_Y		性能低下や資源不足に関するメッセージ(基盤用)
	Hardware		OSやI/Oの誤動作に関連するメッセージ
	Hardware_C1	HW	OSやI/Oの誤動作に関連するメッセージ (基盤用)
	Hardware_Y		OSやI/Oの誤動作に関連するメッセージ (基盤用)
	Network		ネットワーク、接続性に関連するメッセージ
	Network_C1		ネットワーク、接続性に関連するメッセージ (基盤用)
	Network_C2	NW	ネットワーク、接続性に関連するメッセージ (基盤用)
	Network_C3		ネットワーク、接続性に関連するメッセージ (基盤用)
	Network_Y		ネットワーク、接続性に関連するメッセージ (基盤用)
	OS	OS	OSやI/Oの誤動作に関連するメッセージ
	0S_C1		OSやI/Oの誤動作に関連するメッセージ (基盤用)
		1	

	0S_C2		OSやI/Oの誤動作に関連するメッセージ (基盤用)
	OS_C3		OSやI/Oの誤動作に関連するメッセージ (基盤用)
	OS_Y		OSやI/Oの誤動作に関連するメッセージ (基盤用)
	Middleware		ミドルウェアに関するメッセージ
	Middleware_C1		ミドルウェアに関するメッセージ (基盤用)
	Middleware_C2	NAME OF THE PROPERTY OF THE PR	監視システム(ZABBIX)に関するメッセージ
	Middleware_C3	MW	ミドルウェアに関するメッセージ (基盤用)
	Middleware_C4		ミドルウェアに関するメッセージ (基盤用)
	Middleware_Y		ミドルウェアに関するメッセージ (基盤用)
	ストレージ残量		
	HA		
廃止	Security		
	Backup		
	R3		

※各システムで登録されているグループは、こちらから各システムの監視リストをダウンロードしてご確認ください。
※「廃止」のメッセージグループ、もしくは基本(固定)以外のメッセージグループを使用している場合は、別途「基本(固定)」へ移行する調整をさせて頂きます。

#### ◆アラートレベル(重要度)の定義◆

	事象	基本対応						
アラート	内容	サービス	インシデ゛ント	エスカレ	業務影響			
レベル		影響	登録	メール	電話	確認		
危険域	システムに異常が発生しており、一部のサービスが利用不可、または特定のデータ不正や処理異常が発生する可能性が ある	あり (or可能性 あり)	あり	あり	あり	あり		
重要警戒域	システムに異常が発生しているが、即時に適切な対処をする 事でサービスへの影響は発生しない	なし	あり	あり	あり	なし		
警戒域	システムに異常が発生しているが、翌日以降に適切な対処を する事でサービスへの影響は発生しない	なし	あり	あり	なし	なし		
特別 注意域	システムリソースの注意を促すイベントであり、経過観察が 必要な事象である。サービスへの影響は発生しない	なし	なし	あり	なし	なし		
注意域	システムの軽微な警告やインシデントの予防を促すイベント であり、対処を実施しなくてもサービスへの影響は発生しな い		なし	なし	なし	なし		
未分類	監視設定部門が必要に応じて使用。	-	-	-	-	-		