

プロセス監視一覧

No.	対象プロセス情報				監視方法	検知条件		重要度	備考
	種別	製品／ソフトウェア名称	プロセス／サービス名称	検索文字列	監視間隔 (分)	条件	連続回数		
記述要領	監視対象の種別 (OS, PP, AP等) を記入する。	監視対象の製品／ソフトウェ ア名を記入する。	プロセス／サービスの名称を記 入する。	プロセス／サービスを特定するための検索文字列を記述する。	監視間隔 (分)	プロセス数の範囲や サービスの状態を記 入する。	連続何回条件に 合致したら検知と するかを記入する ※Datadogは 15秒毎にプロセ ス状態を収集	条件に合致した場合の 重要度を記入する。 重要度一覧にあるものに 合わせること。	特記すべきことがあれば記入す る。
1	OS(Linux)	Redhat Enterprise Linux	crond (スケジューラ)	/usr/sbin/crond	1	1～99 以外	3	危険	
2									
3			sshd (SSHサーバ)	/usr/sbin/sshd	1	1～99 以外	3	危険	
4									
5			chronyd (時刻同期)	/usr/sbin/chronyd	1	1～99 以外	3	危険	
6									

## メトリクス監視一覧

No.	種別	対象リソース情報				監視方法			検知条件	重要度	備考
		リソース名称	メトリクス名称	Datadogクエリタグ	監視間隔 (分)	評価期間 (分)	集計	条件			
記述要領	監視対象 (OS,AWSサービス) を記入する。	リソースの名称を記入する。	CloudWatchメトリクスを監視する場合、メトリクス名(Datadog上の名称)を記入する。	Datadogモニター、ダッシュボード上でメトリクス値を取得する際に指定するタグ	監視間隔（分） 当該時間毎に集計値を算出し、閾値との比較を行う	評価期間（分） を記入する。 本パラメータで設定した直近の時間幅で、集計を行う。	集計方法	使用率やメトリクスの範囲などの条件を記述する。	条件に合致した場合の重要度を記入する。 重要度一覧にあるものに合わせる。	特記すべきことがあれば記入する。	
1	OS(Linux)	EC2 StatusCheck 監視	aws.ec2.status_check_failed	host	1	5	平均値	-	警告		
2								1以下	危険		
3								-			
4		合計のCPU使用率	100-avg:system.cpu.idle	host	1	5	平均値	-	警告		
5								90%以上	危険		
6								-			
7		メモリ使用率(実メモリ)	1 - system.mem.pct_usable	host	1	5	平均値	-	警告		
8								90%以上	危険		
9								-			
10		ディスク使用率(/root)	system.disk.in_use * 100	host	1	5	平均値	-	警告		
11								90% 以上	危険		
12								-			
13	RDS	CPU使用率 (CPU使用率)	aws.rds.cpuutilization	dbinstanceidentifier	1	5	平均値	-	警告		
14								90% 以上	危険		
15								-			
16		空きメモリ量	aws.rds.freeable_memory	dbinstanceidentifier	1	5	平均値	-	警告		
17								10% 以下	危険		
18								-			
22		ディスクのキュー	aws.rds.disk_queue_depth	dbinstanceidentifier	1	5	平均値	-	警告		
23								120 reqs 以下	危険		
24								-			
25		読み取り IOPS	aws.rds.read_iops	dbinstanceidentifier	1	5	平均値	-	警告		
26								-	危険		
27								-			
28		合計読み取り待機時間	aws.rds.read_latency	dbinstanceidentifier	1	5	平均値	-	警告		
29								-	危険		
30								-			
31		読み取りスループット	aws.rds.read_throughput	dbinstanceidentifier	1	5	平均値	-	警告		
32								734000000 byte以下	危険		
33								-			
34	書き込み IOPS	aws.rds.write_iops	dbinstanceidentifier	1	5	平均値	-	警告			
35							-	危険			
36							-				
37	合計書き込み待機時間	aws.rds.write_latency	dbinstanceidentifier	1	5	平均値	-	警告			
38							-	危険			
39							-				
40	書き込みスループット	aws.rds.write_throughput	dbinstanceidentifier	1	5	平均値	-	警告			
41							734000000 byte以下	危険			
42							-				
43	RDS(cluster)	空きディスク量（ローカルストレージ）	aws.rds.free_local_storage	dbinstanceidentifier	1	5	平均値	30%以下	警告		
44								10%以下	危険		
45								-			
46		ディスク使用率（クラスタストレージ）	aws.rds.volume_bytes_used / 1.407e+14 * 100	dbclusterIdentifier	1	5	平均値	30%以下	警告		
47	10%以下							危険			
48							-				
49	ALB	正常なホストの数	aws.applicationelb.healthy_host_count	loadbalancer	1	5	合計値	-	警告		
50								0以下	危険		
51		異常なホストの数	aws.applicationelb.un_healthy_host_count	loadbalancer	1	5	合計値	-	警告		
52								1以上	危険		
53							-				
54		リクエストの平均値	aws.applicationelb.request_count_per_target	loadbalancer	1	5	平均値	-	警告		
55								15000reqs以上	危険		
56							-				
57		リクエスト応答時間平均値	aws.applicationelb.target_response_time.average	loadbalancer	1	5	平均値	-	警告		
58								8sec 以上	危険		
59						-					
60	5xxで返却されたリクエストの数	aws.applicationelb.httpcode_elb_5xx	loadbalancer	1	5	合計値	-	警告			
61							10以上	危険			
62						-					
63						-					
64	NLB	正常なホストの数	aws.networkelb.healthy_host_count	loadbalancer	1	5	合計値	-	警告		
65								0以下	危険		
66							-				
67		異常なホストの数	aws.networkelb.un_healthy_host_count	loadbalancer	1	5	合計値	-	警告		
68								1以上	危険		
69							-				
70		パケットの流量数	aws.networkelb.processed_packets	loadbalancer	1	5	平均値	-	警告		
71								0以下	危険		
72						-					
73	同時フロー数	aws.networkelb.active_flow_count	loadbalancer	1	5	平均値	-	警告			
74							100以下	危険			
75						-					
76	Lambda	エラー数	aws.lambda.errors	functionname	1	5	平均値	-	警告		
77								1以上	危険		
78						-					
79	Route53	ステータスチェック	aws.route53.health_check_status	healthcheckid	1	5	平均値	-	警告		
80								1以下	危険		
81						-					
82	WAF	ブロックされたリクエスト数	aws.wafv2.blocked_requests	webacl	1	5	平均値	-	警告		
83								50以上	危険		
84						-					
85	NAT Gateway	パケットドロップカウント	aws.natgateway.packets_drop_count	natgatewayid	1	5	平均値	-	警告		
86								1pkts以上	危険		
87								-			