ネットアシスト監視サービス仕様書

v 0.4

改訂履歴

版数	日付	改定内容	作成者
0.1	2015/12/14	ドラフト作成	向井
	2015/12/26	文面の修正	堀
	2015/12/27	注釈作成	堀
	2015/12/31	監視項目の追加	堀
0.2	2016/01/04	しきい値表現の修正と各監視備考の追加	當間
0.3	2016/01/21	監視項目表記の整理	當間
0.4	2016/01/26	「監視対応の流れ」追加	當間

はじめに

本書は株式会社ネットアシスト（以下、当社）が提供する監視サービスに関する仕様について説明する目的で作成しています。
本書の内容は今後の監視サービス追加等により変更される可能性があります。

サービス概要

当社の監視システムより、お客様のサーバ・ネットワーク機器（以下、監視対象）に対して、インターネットを介し以下の監視を実施致します。

- 死活監視
  対象の IP アドレスに対して、Ping コマンドを定期実行し、到達性及び応答速度を確認する事で、監視対象のホスト稼働状況を監視致します。
- サービス監視
  対象のサービスポートに対して、接続コマンドを定期実行し、到達性及び応答状況を確認する事で、監視対象のサービス稼働状況を監視致します。
- リソース監視
  対象に導入された監視エージェント※1 に対して、要求コマンドを定期実行し、リソース値を取得する事で、監視対象のリソース使用状況を監視致します。

これらの監視は、監視項目毎に定められた下記パラメータに基づき実行されます。

- 監視間隔（通常時）
- 監視間隔（異常検知時）
- 異常判断基準
- 障害認定回数

異常判断に基づき異常が検出された場合は、監視間隔を「通常時」から「異常検知時」に切り替えて再監視を行います。
再監視は正常状態が検出されるか、連続した異常を障害認定回数に達するまで繰り返し行います。
後者の場合は『障害』と認定し、お客様への連絡を始めとした一次対応を実施致します。

監視対応の流れ

- 正常時

正常状態→チェック→正常値検出(1)→正常状態

- 異常検知時

正常状態→チェック→異常値検出(1)→異常状態

- 障害認定まで

異常状態→チェック→異常値検出(2～5)→障害認定

- 状態復旧

異常状態→チェック→正常値検出(1)→正常状態

監視システム環境

以下に当社監視システムの環境情報を記載致します。

- ホスト情報
  - ✧ 監視システム A (210.188.231.100)
  - ✧ 監視システム B (211.10.202.12)
- 利用ソフトウェア
  - ✧ Nagios※2
  - ✧ Net-SNMP※3
  - ✧ NRPE※4

監視条件

下記条件が満たされない場合、監視サービスをご利用いただけない場合があります。

- 監視対象に IP アドレスが設定されており、当社監視システムから通信が行える事
- 監視対象に監視エージェントが導入されており、設定変更が可能である事
  ※監視エージェントが未導入の監視対象へは弊社にて導入致します。

監視項目

本項目では当社が設定する監視項目の基本値を記載致します。
なお、お客様の希望により監視項目の基本値を変更する事も可能です。

監視間隔と障害認定回数

監視間隔（通常時）	5 分
監視間隔（異常検知時）	1 分
障害認定回数	5 回

死活監視

Ping

監視設定名称	**Ping**
監視概要	Ping コマンドによる死活監視
異常判断基準	下記のいずれかに該当する場合 1. しきい値以上の応答遅延を検知 2. しきい値以上のパケットロスを検知 3. 無応答を検知
しきい値	5 秒・80%
備考	-

サービス監視

SSH

監視設定名称	**SSH**
監視概要	SSH サービスポート(TCP:22)への接続監視
異常判断基準	下記のいずれかに該当する場合 1. しきい値以上の応答遅延を検知 2. 接続不能を検知
しきい値	10 秒
備考	-

FTP

監視設定名称	**FTP**
監視概要	FTP サービスポート(TCP:21)への接続監視
異常判断基準	下記のいずれかに該当する場合 1. しきい値以上の応答遅延を検知 2. 接続不能を検知
しきい値	10 秒
備考	-

HTTP

監視設定名称	**HTTP**
監視概要	HTTP サービスポート(TCP:80)への接続監視
異常判断基準	下記のいずれかに該当する場合 1. しきい値以上の応答遅延を検知 2. 接続不能を検知 3. 500 番台のステータスコード※5 を検知
しきい値	10 秒
備考	下記カスタム監視が可能 ● URL 指定 URL アドレスへの接続監視 ● String 接続先ページ内容で指定文字列有無の確認監視

HTTPS

監視設定名称	**HTTPS**
監視概要	HTTPS サービスポート(TCP:443)への接続監視
異常判断基準	下記のいずれかに該当する場合 1. しきい値以上の応答遅延を検知 2. 接続不能を検知 3. 500 番台のステータスコードを検知
しきい値	10 秒
備考	下記カスタム監視が可能 ● URL 指定 URL アドレスへの接続監視 ● String 接続先ページ内容で指定文字列有無の確認監視

SMTP

監視設定名称	**SMTP**
監視概要	SMTP サービスポート(TCP:25)への接続監視
異常判断基準	下記のいずれかに該当する場合 1. しきい値以上の応答遅延を検知 2. 接続不能を検知
しきい値	10 秒
備考	-

Submission_Port

監視設定名称	**Submission_Port**
監視概要	サブミッションポート(TCP:587)への接続監視
異常判断基準	下記のいずれかに該当する場合 1.　しきい値以上の応答遅延を検知 2.　接続不能を検知
しきい値	10 秒
備考	-

POP3

監視設定名称	**POP**
監視概要	POP3 サービスポート(TCP:110)への接続監視
異常判断基準	下記のいずれかに該当する場合 1.　しきい値以上の応答遅延を検知 2.　接続不能を検知
しきい値	10 秒
備考	-

IMAP4

監視設定名称	**IMAP**
監視概要	IMAP4 サービスポート(TCP:143)への接続監視
異常判断基準	下記のいずれかに該当する場合 1.　しきい値以上の応答遅延を検知 2.　接続不能を検知
しきい値	10 秒
備考	-

MySQL

監視設定名称	**MySQL**
監視概要	MySQL サービスへのログイン接続監視
異常判断基準	下記のいずれかに該当する場合 1.　ログインが行なわれない 2.　接続不能を検知
しきい値	-

備考	MySQL ユーザアカウント・パスワードが必要

MySQL_replication

監視設定名称	**MySQL_replication**
監視概要	MySQL のレプリケーション状態監視
異常判断基準	下記のいずれかに該当する場合 1. Slave_IO_Running※6 が「No」である事を検知 2. Slave_SQL_Running※7 が「No」である事を検知 3. 接続不能を検知
しきい値	-
備考	REPLICATION CLIENT 権限を持った MySQL ユーザアカウント・パスワードが必要

PostgreSQL

監視設定名称	**PostgreSQL**
監視概要	PostgreSQL サービスへのログイン接続監視
異常判断基準	下記のいずれかに該当する場合 1. ログインが行なわれない 2. 接続不能を検知
しきい値	-
備考	PostgreSQL ユーザアカウント・パスワードが必要

TCP_Port

監視設定名称	**TCP_Port**
監視概要	任意の TCP ポート接続監視
異常判断基準	下記のいずれかに該当する場合 1. しきい値以上の応答遅延を検知 2. 接続不能を検知
しきい値	10 秒
備考	-

リソース監視

LoadAverage※8

監視設定名称	**LoadAverage**
監視概要	LoadAverage 値の監視

異常判断基準	しきい値以上の値を検知
しきい値	監視対象の CPU 数×10
備考	Linux サーバの MIB オブジェクト ID※9 を利用

Disk_Use

監視設定名称	**Disk_Use**
監視概要	パーティション毎の Disk 使用率監視
異常判断基準	しきい値以上の値を検知
しきい値	80%
備考	Linux サーバの MIB オブジェクト ID を利用

Swap_Use

監視設定名称	**Swap_Use**
監視概要	SWAP 使用率監視
異常判断基準	しきい値以上の値を検知
しきい値	70%
備考	Linux サーバの MIB オブジェクト ID を利用

Process

監視設定名称	**Process_Total**
監視概要	稼働中のプロセス総数の監視
異常判断基準	プロセス総数がしきい値範囲を逸脱した場合
しきい値	～700
備考	-

監視設定名称	**Process_Zombie**
監視概要	ゾンビプロセス※10 数の監視
異常判断基準	ゾンビプロセス数がしきい値範囲を逸脱した場合
しきい値	～5
備考	-

監視設定名称	**Process_any**
監視概要	任意のプロセス数の監視
異常判断基準	監視対象プロセス数がしきい値範囲を逸脱した場合
しきい値	1～

備考	しきい値は最小・最大値を指定

ログ監視

Log

監視設定名称	**CHECK_LOG**
監視概要	ログファイル内容からキーワード監視
異常判断基準	任意のキーワードが監視対象ファイルから検出された場合
しきい値	-
備考	対象ログファイルとキーワードの指定が必要

※1 監視エージェント
SNMP エージェント、NRPE エージェントを指す
※2 Nagios
オープンソースのホスト・ネットワーク監視ソフトウェア
※3 Net-SNMP
ネットワーク管理を行う為のプロトコル(Simple Network Management Protocol)
※4 NRPE
Nagios の監視対象ホスト上で任意のコマンドを実行する際に必要となるプラグイン
(Nagios Remote Plugin Executer)
※5 5xx Server Error の HTTP ステータスコード
サーバ側の問題により、リクエストが処理されなかった場合のステータス
※6 Slave_IO_Running
I/O スレッドの動作状況。Master に接続できない、バイナリログが読み取れない等で停止する。
※7 Slave_SQL_Running
SQL スレッドの動作状況。Slave で更新系 SQL を発行した、Slave に存在しないデータを削除した等で停止する。
※8 LoadAverage
CPU 処理待ちプロセス数の平均値
※9 MIB のオブジェクト ID
機器の持つ情報をツリー構造で保存したもの、その一部を指す ID
(Management information base Object ID)
※10 ゾンビプロセス
処理が完了した子プロセスからの処理終了シグナルを親プロセスが正常に受け取れない場合に残り続ける子プロセスの事