平成 25 年 11 月 1 日

バリューアップ　プライベート監視サービス
仕様書

第2.0版

NTT スマートコネクト株式会社

改訂履歴

版数	制定･改訂年月日	内容
2.0	2013 年 11 月 1 日	制定

1. サービス概要

バリューアッププライベート監視サービス（以下、「本サービス」といいます。）はエヌ・ティ・ティ・スマートコネクト
データセンターを利用されているお客様のシステムに対し、監視機能と監視運用をセットで提供するサービスです。

1-1. 監視サービス

本サービスは 24 時間 365 日、システムの稼働状況を監視し、異常検知時および復旧時に通知いたします。
下記の監視項目からご選択いただけます。
また、通知方法としてはメールで行うタイプ 1 と、電話及びメールで行うタイプ 2 をご選択いただきます。
なお、同一ご契約者様でタイプ1とタイプ2の混在はできません。

監視項目	対象	監視方法	対応ネットワーク	エージェント
Ping 監視	IP アドレスを持つインターフェース	ICMP echo(ping)による監視	インターネット/監視セグメント	不要
URL 監視	HTTP サービスポート ※HTTPS も含む	HTTP サーバにアクセスしページ内に含まれる文字列を監視する	インターネット/監視セグメント	不要
http 監視	HTTP サービスポート ※HTTPS も含む	HTTP サーバにアクセスし応答コードによる監視をする	インターネット/監視セグメント	不要
TCP ポート監視	TCP サービスポート	TCP ポートにアクセスし、サービス稼動状況を監視する	インターネット/監視セグメント	不要
DNS 監視	DNS サービスポート	DNS サーバへアクセスしレコードの参照を実施して動作を監視する	インターネット/監視セグメント	不要
SNMP Trap 監視	SNMP Trap を出力する機器	対象機器から SNMP Trap 受信による監視をする	インターネット/監視セグメント	不要
CPU 使用率監視	SNMP に対応する機器	SNMP を用いて、CPU 使用率を監視する	インターネット/監視セグメント	必要（SNMP）
ロードアベレージ監視	SNMP に対応する機器	SNMP を用いて、ロードアベレージの負荷状況を監視する	インターネット/監視セグメント	必要（SNMP）
メモリ使用率監視	SNMP に対応する機器	SNMP を用いて、メモリ使用率を監視する	インターネット/監視セグメント	必要（SNMP）
プロセス監視	SNMP に対応する機器	SNMP を用いて、プロセス起動数を監視する	インターネット/監視セグメント	必要（SNMP）
ディスク使用率監視	SNMP に対応する機器	SNMP を用いて、ディスク使用率を監視する	インターネット/監視セグメント	必要（SNMP）
SWAP 使用率監視	SNMP に対応する機器	SNMP を用いて、SWAP 使用率を監視する	インターネット/監視セグメント	必要（SNMP）
トラフィック使用量監視	SNMP に対応する機器	SNMP を用いて、トラフィックの使用状況を監視する	インターネット/監視セグメント	必要（SNMP）
インターフェース状態監視	SNMP に対応する機器	SNMP を用いて、インターフェース状況を監視する	インターネット/監視セグメント	必要（SNMP）
ログイン数監視	SNMP に対応する機器	SNMP を用いて、ログイン数を監視する	インターネット/監視セグメント	必要（SNMP）
ログファイル監視	Linux サーバ	指定ログファイルから、指定した文字列の有無を監視する	インターネット/監視セグメント	必要（NRPE）
Windows イベントログ監視	Windows サーバ	イベントログから、重要度の高いメッセージの有無を監視する	インターネット/監視セグメント	必要（NRPE）

監視項目	対象	監視方法	対応ネットワーク	エージェント
SMTP 監視	SMTP サービスポート	SMTP サーバにアクセスし、サービス稼動状況を監視する	インターネット/監視セグメント	不要
POP3 監視	POP3 サービスポート	POP3 サーバにアクセスし、サービス稼動状況を監視する	インターネット/監視セグメント	不要
IMAP4 監視	IMAP4 サービスポート	IMAP4 サーバにアクセスし、サービス稼動状況を監視する	インターネット/監視セグメント	不要
FTP 監視	FTP サービスポート	FTP サーバにアクセスし、サービス稼動状況を監視する	インターネット/監視セグメント	不要
NTP 監視	NTP サービスポート	NTP サーバにアクセスし、時刻配信が行なえているか監視する	インターネット/監視セグメント	不要
SSH 監視	SSH サービスポート	SSH サーバにアクセスしサービス稼動状況を監視する監視する	インターネット/監視セグメント	不要
LDAP 監視	LDAP サービスポート	LDAP サーバにアクセスし、サービス稼動状況を監視する	インターネット/監視セグメント	不要
RADIUS 監視	RADIUS サービスポート	RADIUS サーバにアクセスし、サービス稼動状況を監視する	インターネット/監視セグメント	不要
MySQL 監視	MySQL サービスポート	MySQL サーバにアクセスし、サービス稼動状況を監視する	インターネット/監視セグメント	不要
PostgreSQL 監視	PostgreSQL サービスポート	PostgreSQL サーバにアクセスし、サービス稼動状況を監視する	インターネット/監視セグメント	不要

1-2. レポートサービス

本サービスは 24 時間 365 日、サーバおよびネットワーク機器のリソースを測定し、公開用 Web サーバにてレポートを公開します。
下記の監視項目を、お客様の監視対象に合わせてご選択いただけます。

監視項目	対象	監視方法	対応ネットワーク	エージェント
CPU 使用率	SNMP に対応する機器	SNMP を用いて、CPU 使用率をグラフ化する	インターネット/監視セグメント	必要（SNMP）
ロードアベレージ	SNMP に対応する機器	SNMP を用いて、ロードアベレージをグラフ化する	インターネット/監視セグメント	必要（SNMP）
メモリ使用率	SNMP に対応する機器	SNMP を用いて、メモリ使用率をグラフ化する	インターネット/監視セグメント	必要（SNMP）
SWAP 使用率	SNMP に対応する機器	SNMP を用いて、SWAP 使用率をグラフ化する	インターネット/監視セグメント	必要（SNMP）
ディスク使用率	SNMP に対応する機器	SNMP を用いて、ディスク使用率をグラフ化する	インターネット/監視セグメント	必要（SNMP）
トラフィック使用量	SNMP に対応する機器	SNMP を用いて、インターフェースのトラフィック使用量推移をグラフ化する	インターネット/監視セグメント	必要（SNMP）

2. サービス詳細

2-1. 監視サービス詳細

24 時間 365 日選択された項目について稼働状況を監視し、異常(閾値オーバー)を検出した場合、および復旧時に通知いたします。
2-1-1 に通知方法を、2-1-2 に各監視項目の監視詳細を示します。

2-1-1. 通知方法

(1) タイプ1
異常(閾値オーバー)を検出した場合、および復旧時に「メール」にて通知します。
メールアドレスは 3 アドレスまで登録でき、登録アドレス全てに同報・通知します。

(2) タイプ2
異常(閾値オーバー)を検出した場合、および復旧時に「電話」及び「メール」にて通知します。
電話は 3 つの番号まで登録でき、登録された 1 つの番号に連絡がつくまで 2 回巡回連絡します。
なお、電話連絡がつかなかった場合はその旨メールにて連絡します。
メールアドレスは 3 アドレスまで登録でき、登録アドレス全てに同報・通知します。

2-1-2. 監視項目詳細

監視項目	監視方法
Ping 監視	64Bytes の ICMP echo パケットを 5 分間隔で送信して監視する。 5 秒以上のタイムアウトが発生した場合、1 分後にリトライして再度結果がタイムアウトであった場合は障害とする。
URL 監視	指定 URL へ 5 分間隔でアクセスして監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト(10 秒)が発生 ②サーバから取得したデータ内に指定した文字列(ASCII)が含まれない ※契約中のホスティングサービス上で利用する IP アドレスに関する FQDN のみ指定可能 ※指定 URL に関して DNS ラウンドロビン、ロードバランシングをしている場合など、監視サーバが DNS を参照したタイミング等の影響で、監視対象が正常な場合でも異常検出通知が行われる可能性があるものとする。 同じく、DNS サーバ等の関連システムに障害が発生した場合も、異常検出通知が行われるものとする。
http 監視	指定 URL へ 5 分間隔でアクセスして監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト(10 秒)が発生 ②サーバからのレスポンスコードが指定したコードと一致しない
TCP ポート監視	任意の TCP ポートに 5 分間隔でアクセスして監視する。 タイムアウト(10 秒)が発生した場合は 1 分後にリトライして再度タイムアウトが発生した場合は障害とする。
DNS 監視	指定 FQDN のレコード参照を 5 分間隔でアクセスして監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト(10 秒)が発生 ②サーバからレコードが参照できない ③参照したレコードと、指定した文字列(ホスト名、IP アドレス)が一致しない ※レコードの種類は、A, AAAA, MX, PTR が指定可能 ※DNS ラウンドロビンをしている場合など、1 つの FQDN に複数のレコードが存在する場合は、複数のレコードのいずれかと指定した 1 つの文字列(ホスト名、IP アドレス)が一致すれば正常と判断する。
SNMPTrap 監視	監視対象から通知される SNMP Trap を監視サーバにて受信する。 ※「2-1-3 SNMP Trap OID 一覧」参照
CPU 使用率監視	CPU 使用率を 5 分間隔で監視する。 その値が閾値※を超えた場合は 1 分後にリトライして再度結果が閾値※を超える場合は障害とする。 ※閾値・・・90～100%の間から任意の値をお客様にて指定(デフォルトは 90%) ※CPU を複数搭載している場合は全ての CPU(論理 CPU コア全て)の CPU 使用率の平均を監視する。
ロードアベレージ監視	ロードアベレージを 5 分間隔で監視する。 その値が閾値※を超えた場合は 1 分後にリトライして再度結果が閾値※を超える場合は障害とする。 ※閾値・・・0.9 以上の任意の値をお客様にて指定。(デフォルトは 0.9、上限はなし) ※Linux のみ対応

監視項目	監視方法
メモリ使用率監視	物理メモリの使用量を 5 分間隔で監視する。 その値が閾値※を超えた場合は 1 分後にリトライして再度結果が閾値を超える場合は障害とする。 ※閾値･･･90～100%の間から任意の値をお客様にて指定（デフォルトは 90%） 以下の式で算出する。 ①Linux （メモリ総量 － メモリ空き容量 － キャッシュ使用量 － バッファ使用量） / メモリ総量 × 100% ②Windows メモリ使用量 / メモリ総量 × 100%
プロセス監視	指定プロセスの起動数を 5 分間隔で監視する。 その値が閾値（0）と等しい場合に障害と判断する。 ①Linux プロセスの生存数のチェックにはコマンド“ps -e”の結果で検索されるプロセス名を使用する。 ②Windows タスクマネージャのプロセスタブに表示される名前で検索されるプロセス名を使用する。
ディスク使用率監視	ディスクのパーティションの使用率を 5 分間隔で監視する。 その値が閾値※を超えた場合は 1 分後にリトライして再度結果が閾値を超える場合は障害とする。 ※閾値･･･80～100%の間から任意の値をお客様にて指定。（デフォルトは 80%）
SWAP 使用率監視	仮想メモリの使用率を 5 分間隔でポーリングし監視する。 その値が閾値※を超えた場合は 1 分後にリトライして再度閾値を超える場合は障害とする。 ※閾値･･･90～100%の間から任意の値をお客様にて指定（デフォルトは 90%）
トラフィック使用量監視	インターフェースのトラフィック使用量を 5 分間隔で監視する。 その値が閾値※を超えた場合は 1 分後にリトライして再度結果が閾値を超える場合は障害とする。 ※閾値･･･1～1000Mbps の間から任意の値をお客様にて指定（デフォルト値はなし） ※専用コネクティビティオプション契約時のみ申込可能、閾値はコネクティビティの契約帯域を考慮して決定する。 5 分間の通信量から 1 秒当たりの通信量を算出した値を監視する。 ①受信方向（IN） 5 分間の受信データ量（Octets） ×8（bit） / 300（秒） ②送信方向（OUT） 5 分間の送信データ量（Octets） ×8（bit） / 300（秒）
インターフェース状態監視	指定インターフェースのステータスを 5 分間隔で監視する。 ステータスがダウン状態であった場合は 1 分後にリトライして再度ダウン状態であった場合は障害とする。
ログイン数監視	指定サーバにログインしているユーザ数を 5 分間隔で監視する。 その値が閾値※を超えた場合に障害と判断する。 ※閾値･･･1 以上の任意の値をお客様にて指定（デフォルトは 1）
ログファイル監視	指定のログファイルを 5 分間隔で監視する。 指定したキーワードを含むログを検出した場合は障害とする。 ※Linux のみ対応 ※NRPE エージェントが必要 ※ログファイル、キーワードの指定が必要 ※監視用アカウントがログの読み込み権限を有すること
Windows イベントログ監視	イベントビューアのアプリケーションログとシステムログを 5 分間隔で監視する。 直近 5 分間に発生した警告ログとエラーログを検出した場合は障害とする。 ※Windows のみ対応。 ※NRPE エージェントが必要
SMTP 監視	SMTP サーバの指定ポートに 5 分間隔でアクセスを実施して監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト（10 秒）が発生 ②サーバに接続後、最初の応答コードが“220”以外である ③認証に失敗（※ログイン認証(AUTH-LOGIN)を選択した場合）
POP3 監視	POP3 サーバの指定ポートに 5 分間隔でアクセスを実施して監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト（10 秒）が発生 ②サーバに接続後、最初の応答文字列に“OK”が含まれない ③認証に失敗（※ログイン認証（POP3 認証）を選択した場合）
IMAP4 監視	IMAP サーバの指定ポートに 5 分間隔でアクセスを実施して監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト（10 秒）が発生 ②サーバに接続後、最初の応答文字列に“OK”が含まれない ③認証に失敗（※ログイン認証（LOGIN）を選択した場合）

監視項目	監視方法
FTP 監視	FTP サーバの指定ポートに 5 分間隔でアクセスを実施して監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト（10 秒）が発生 ②サーバに接続後、最初の応答コードが“220”以外である ③認証に失敗（※基本認証（匿名認証は未対応）を選択した場合）
NTP 監視	NTP サーバの指定ポートに 5 分間隔でアクセスを実施して監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト（10 秒）が発生 ②Offset（被監視サーバと被監視サーバが参照しているNTP サーバとの時刻の差異）が 0.02 秒を超えた（※Offset 監視を選択した場合のみ） ※Offset 監視は被監視サーバが「NTP プロトコルモード 6(NTP Control Messages)」に対応している必要があります。
SSH 監視	SSH サーバの任意のポートに 5 分間隔でアクセスして監視する。 タイムアウト（10 秒）が発生した場合は 1 分後にリトライして再度タイムアウトが発生した場合は障害とする。
LDAP 監視	LDAP サーバの任意のポートに 5 分間隔でアクセスして監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト（10 秒）が発生 ②認証に失敗 ③検索条件にマッチしない ※監視用の認証アカウントが必要
RADIUS 監視	RADIUS サーバの任意のポートに 5 分間隔でアクセスして監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト（30 秒）が発生 ②認証に失敗 ※監視用の認証アカウントを発行していただく ※RADIUS サーバにクライアントとしてアクセスするための共有鍵を発行していただく ※RADIUS サーバに当社監視セグメントを RADIUS クライアントとして登録いただく ※平文による認証のみ対応
MySQL 監視	MySQL サーバの任意のデータベースに 5 分間隔でアクセスして監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト（10 秒）が発生 ②データベースにアクセスができない ※データベースにアクセスするためのアカウントとパスワードとデータベース名が必要
PostgreSQL 監視	PostgreSQL サーバの任意のデータベースに 5 分間隔でアクセスして監視する。 結果が以下のいずれかの場合は、1 分後にリトライして再度結果が以下のいずれかの場合は障害とする。 ①タイムアウト（10 秒）が発生 ②データベースにアクセスができない ※データベースにアクセスするためのアカウントとパスワードとデータベース名が必要

2-1-3. SNMP Trap OID 一覧

オブジェクト名	OID	説明
coldStart	1.3.6.1.6.3.1.1.5.1	対象機器が初期化スタートした場合に発報
warmStart	1.3.6.1.6.3.1.1.5.2	対象機器が初期化されずにスタートした場合に発報
linkDown	1.3.6.1.6.3.1.1.5.3	インターフェースがダウンした場合に発報
LinkUp	1.3.6.1.6.3.1.1.5.4	インターフェースがアップした場合に発報

2-2. レポートサービス詳細

24 時間 365 日選択された項目について 5 分間隔で測定し、レポート公開用 Web サーバにて
グラフをレポート公開します。グラフ表示は、日次、週次、月次、年次[*1]で表示可能です。

監視項目	監視方法
CPU 使用率	CPU 使用率を 5 分間隔で取得し、グラフ表示する。
ロードアベレージ(Linux)	ロードアベレージを 5 分間隔で取得し、グラフ表示する。
メモリ使用率	物理メモリの使用量を 5 分間隔で取得し、グラフ表示する。
ディスク使用率	ディスクパーティションの使用量を 5 分間隔で取得し、グラフ表示する。
SWAP 使用率	仮想メモリの使用量を 5 分間隔で取得し、グラフ表示する。
トラフィック使用量	インターフェースの通信量(Octets)の積算値を 5 分毎に取得し、 1 秒当たりの通信量(bps)を計算してその値をグラフ表示する。 以下の式で算出する。 ① 受信方向(IN) 受信データ量(Octets) ×8(bit) / 300(秒) ②送信方向(OUT) 送信データ量(Octets) ×8(bit) / 300(秒)

[*1] 1 年間の表示となります。

3. その他

3-1. 監視サービス提供形態および責任分界点

(1) グローバル接続の場合(グローバルセグメント監視)
インターネットを介して、お客様システムを監視します。
この場合当社システム責任分界点は当社システムのインターネット接続ポイントとします。
(インターネット経路上の障害、遅延等により誤報が生じる可能性がありますのでご了承ください。)

(2) プライベート接続の場合(プライベートセグメント監視)
お客様のプライベートセグメントに個別に接続(1 接続)することにより、お客様システムを監視します。
この場合の当社システム責任分界点はお客様ラック内に設置されたパッチパネルの RJ45 メスロとなります。

3-2. サービス提供条件

(1) グローバル接続の場合(グローバルセグメント監視)
被監視機器がグローバル IP アドレスを持っておりインターネットに接続可能な事、
監視サーバより監視項目に応じて使用するプロトコルが到達可能であることが必要です。

※ 当社監視サーバの Source アドレス : 210.150.27.32/27
: 2001:2c0:803:2::/64

(2) プライベート接続の場合(プライベートセグメント監視)
監視サーバより監視項目に応じて使用するプロトコルが到達可能であることが必要です。
お客様にて、監視サーバへのルーティングを設定頂く必要があります。

※ 当社監視サーバの Source アドレス 210.150.27.64/26

(3) エージェントソフトが必要な場合
エージェントソフトが必要な場合は当社にて、当社指定のエージェントソフトのインストール作業代行を実施いたします。
エージェントソフトインストール作業の実施には作業用のアカウントを発行して頂く必要があります。
作業用アカウントには次の管理者権限を設定して頂く必要があります。

Windows サーバ	「Administrators」グループ、「Remote Desktop Group」グループ
Linux サーバ	root パスワードもしくは sudo 設定

エージェントソフトインストール対象機器には、次のプロトコルを使用してログインします。

Windows サーバ	リモートデスクトップ(デフォルト TCP:3389)
Linux サーバ	SSH(デフォルト TCP:22)

なお、監視対象機器には次のプロトコルへのアクセス許可を設定して頂く必要があります。

SNMP エージェント	UDP:161
NRPE エージェント	TCP:5666

エージェントソフトに起因するいかなる障害及び、障害について当社は一切の責任を負い兼ねます。
また、インストール代行作業はお客様が各ソフトの利用許諾条件を確認し、同意されたことを前提として実施させて頂きます。

エージェントソフト動作確認済み OS は下記の通りです。下記以外の OS につきましては
個別相談とさせていただきます。

ア　SNMP エージェント

エージェントソフト動作確認済み OS	当社指定エージェントソフト
・Solaris 9 ～ 10	net-snmp エージェント
・RedHat Enterprise Linux 4 ～ 6	
・Fedora 16	
・CentOS 5 ～ 6	
・Windows Server 2003 (R2)	Microsoft 標準 SNMP エージェント
・Windows Server 2008 (R2)	

イ　NRPE(Nagios Remote Plugin Executor)エージェント

エージェントソフト動作確認済み OS	当社指定エージェントソフト
CentOS 5 ～ 6	NRPE エージェント
RedHat Enterprise Linux 5 ～ 6	
Windows Server 2003 (R2)	NRPE_NT エージェント
Windows Server 2008 (R2)	

3-3. セキュリティについて

(1) 監視システム

本システムはグローバル監視とプライベート監視を提供しておりますが、外部接続部分に
ファイアウォールを設置することでセキュリティ対策を実施しております。
レポート公開用 Web サーバは SSL(公的署名証明書利用)を使用し、お客様端末とサーバ間の通信を
暗号化しています。また、ユーザ認証 ID、パスワードによって閲覧を制限します。

(2) お客様プライベートネットワーク

各お客様プライベートネットワークセグメントについては、各セグメント間で通信疎通できないよう
各ユーザセグメント毎に VLAN を作成しております。
また、ルータのアクセスフィルタ機能によりセキュリティ対策を実施しております。

3-4. 非監視について

プライベート監視サービスの一時的な監視解除が必要な場合は、事前に非監視申請をお願いいたします。
なお、非監視のご連絡を頂いた場合、プライベート監視サービスの監視項目全体が非監視対象となります。
サーバ毎、監視項目毎など個々に非監視とすることはできませんのであらかじめご了承ください

(1) 非監視申請 WEB フォームによりご申請ください。

＊ http://www.nttsmc.com/center/　にアクセスし「非監視申請」を選択してご申請ください。
＊ 定期的(毎月/週/日)に非監視とする方法と必要の都度、非監視申請する方法があります。
＊ 取り消し及び時間変更については再度メール申請いただくか
　オペレーションセンタ(0120-802030)までご連絡ください。

(2) 入室時間帯において非監視とする場合は入室申請と一緒に申請することができます。

＊ 入室申請の WEB フォームに下記チェック項目がありますので、ここにチェックしてください。
（ http://www.nttsmc.com/center/ より「入室申請」を選択 ）

Value-up プライベート監視サービス	☐ 入室時間帯は非監視とする （ご利用のお客様のみチェックをお願いします。）

4. サービス提供場所

NTT スマートコネクト堂島データセンター内にて本サービスを提供します。

5. 連絡窓口一覧

お問い合わせ内容	お問い合わせ時間	お問い合わせ先
故障問い合わせ 緊急問い合わせ	24 時間 365 日	スマートコネクト オペレーションセンター TEL:0120-802030
非監視申請	24 時間 365 日	http:// www.nttsmc.com/center/ 「プライベート監視サービス非監視申請」
ご利用上の問い合わせ (技術的質問等) 営業に関する問い合わせ (仕様、価格等)	平日 9:30～18:00	スマートコネクト IDC ビジネス部 TEL:06-6147-5192 E-mail: support@mcnet.ad.jp