App Bridge Monitor
応答監視サービスガイド

Ver.1.19.0

目次

１．本書の役割

本書は、App Bridge Monitor が提供する Ping 応答監視、HTTP/HTTPS 応答監視、TCP ポート応答監視について説明するものです。

２．応答監視概要

2.1 応答監視とは

応答監視とは、HTTP（含む HTTPS）、Ping、TCP ポートを用いた応答有無、応答時間の監視です。App Bridge Monitor では、インターネット環境、イントラネット環境での応答監視を用意しており、応答時間を統計情報として提供します。

2.2 ノードとエンドポイント

応答監視を実施するためには、対象のサーバまたはネットワークデバイス（※1）をノードとして登録し、監視対象となるエンドポイント（※2）を設定します。1 つのノードに複数のエンドポイントを設定することが可能であり、App Bridge Monitor は登録されたエンドポイントに対して応答監視を実施します。

※1：ルータ、ファイアウォールなどのネットワーク機器
※2：HTTP 監視の場合 URL、Ping 監視の場合 FQDN、TCP ポート監視の場合 FQDN とポート番号

2.3 HTTP 監視

HTTP 監視は、指定された URL（エンドポイント）に HTTP（または HTTPS）アクセスし、応答の有無を監視すると共に、応答時間の統計を記録します。
HTTP 監視は、4 回の HTTP アクセスを 1 つのセットとして実行します。4 回の HTTP アクセスが 1 度でも成功した場合、監視状態は正常と判定され、応答時間の統計は成功した HTTP アクセスの平均で記録されます。
4 回の HTTP アクセスがすべて失敗した場合、リトライインターバルを設けたのちに、再度 4 回の HTTP アクセスを実行します。再度実行された 4 回の HTTP アクセスが全て失敗した場合、エラーと判定され、通知されます。

HTTP 監視の監視間隔、タイムアウト、リトライインターバルは、以下のとおりです。

監視内容	監視間隔(分)	タイムアウト	リトライインターバル
HTTP 監視	5	30,000 ミリ秒	1,000 ミリ秒

App Bridge Monitor では、オーナ単位にスレッドを最大 5 つ準備し、HTTP 監視を実行します。このため、オーナ単位で 5 つ以上のエンドポイントが HTTP 監視登録されている場合、処理待ちが発生し、オーナ単位の HTTP 監視実行時間が 5 分を越える可能性があります。

オーナ単位の HTTP 監視が 5 分未満で終了した場合、次回 HTTP 監視は前回 HTTP 監視開始時刻の 5 分後に開始されます。例えば、1 回目の HTTP 監視が 09:00 に開始され、HTTP 監視に 1 分要した場合、次回 HTTP 監視は 09:05 に開始されます。

オーナ単位の HTTP 監視に 5 分以上要した場合、次回 HTTP 監視は前回 HTTP 監視終了時刻＋αに開始されます。例えば、1 回目の HTTP 監視が 09:00 に開始され、HTTP 監視に 6 分要した場合、次回 HTTP 監視は 09:06 以降に開始されます。

2.4 Ping 監視

Ping 監視は、指定された FQDN または IP アドレス（エンドポイント）に Ping アクセスし、応答の有無を監視すると共に、応答時間の統計を記録します。

Ping 監視は、4 回の Ping アクセスを 1 つのセットとして実行します。4 回の Ping アクセスが 1 度でも成功した場合、監視状態は正常と判定され、応答時間の統計は成功した Ping アクセスの平均で記録されます。

4 回の Ping アクセスがすべて失敗した場合、リトライインターバルを設けたのちに、再度 4 回の Ping アクセスを実行します。再度実行された 4 回の Ping アクセスが全て失敗した場合、エラーと判定され、通知されます。

Ping 監視の監視間隔、タイムアウト、リトライインターバルは、以下のとおりです。

監視内容	監視間隔(分)	タイムアウト	リトライインターバル
Ping 監視	5	1,000 ミリ秒	5,000 ミリ秒

App Bridge Monitor では、オーナ単位にスレッドを最大 5 つ準備し、Ping 監視を実行します。このため、オーナ単位で 5 つ以上のエンドポイントが Ping 監視登録されている場合、処理待ちが発生し、オーナ単位の Ping 監視実行時間が 5 分を越える可能性があります。

オーナ単位の Ping 監視が 5 分未満で終了した場合、次回 Ping 監視は前回 Ping 監視開始時刻の 5 分後に開始されます。例えば、1 回目の Ping 監視が 09:00 に開始され、Ping 監視に 1 分要した場合、次回 Ping 監視は 09:05 に開始されます。

オーナ単位の Ping 監視に 5 分以上要した場合、次回 Ping 監視は前回 Ping 監視終了時刻＋αに開始されます。例えば、1 回目の Ping 監視が 09:00 に開始され、Ping 監視に 6 分要した場合、次回 Ping 監視は 09:06 以降に開始されます。

2.5 TCP ポート監視

TCP ポート監視は、指定された FQDN または IP アドレスのポート番号（エンドポイント）に TCP ポートコネクションオープンを実施し、応答の有無を監視すると共に、応答時間の統計を記録します。

TCP ポート監視は、4 回の TCP ポートコネクションオープンを 1 つのセットとして実行します。4 回の TCP ポートコネクションオープンが 1 度でも成功した場合、監視状態は正常と判定され、応答時間の統計は TCP ポートコネクションオープンに要した時間の平均で記録されます。

4 回の TCP ポートコネクションオープンがすべて失敗した場合、リトライインターバルを設けたのちに、再度 4 回の TCP ポートコネクションオープンを実行します。再度実行された 4 回の TCP ポートコネクションオープンが全て失敗した場合、エラーと判定され、通知されます。

TCP ポート監視の監視間隔、タイムアウト、リトライインターバルは、以下のとおりです。

監視内容	監視間隔(分)	タイムアウト	リトライインターバル
TCP ポート監視	5	30,000 ミリ秒	1,000 ミリ秒

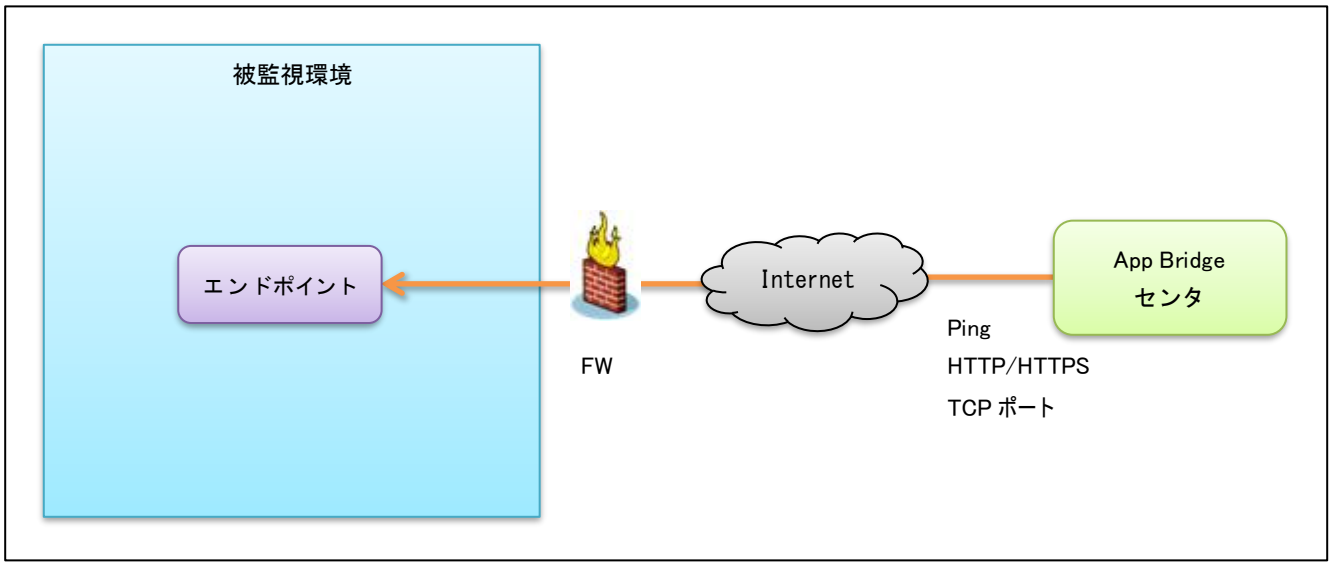
App Bridge Monitor では、オーナ単位にスレッドを最大 5 つ準備し、TCP ポート監視を実行します。このため、オーナ単位で 5 つ以上のエンドポイントが TCP ポート監視登録されている場合、処理待ちが発生し、オーナ単位の TCP ポート監視実行時間が 5 分を越える可能性があります。

オーナ単位の TCP ポート監視が 5 分未満で終了した場合、次回 TCP ポート監視は前回 TCP ポート視開始時刻の 5 分後に開始されます。例えば、1 回目の TCP ポート監視が 09:00 に開始され、監視に 1 分要した場合、次回 TCP ポート監視は 09:05 に開始されます。

オーナ単位の TCP ポート監視に 5 分以上要した場合、次回 TCP ポート監視は前回 TCP ポート監視終了時刻＋αに開始されます。例えば、1 回目の TCP ポート監視が 09:00 に開始され、監視に 6 分要した場合、次回 TCP ポート監視は 09:06 以降に開始されます。

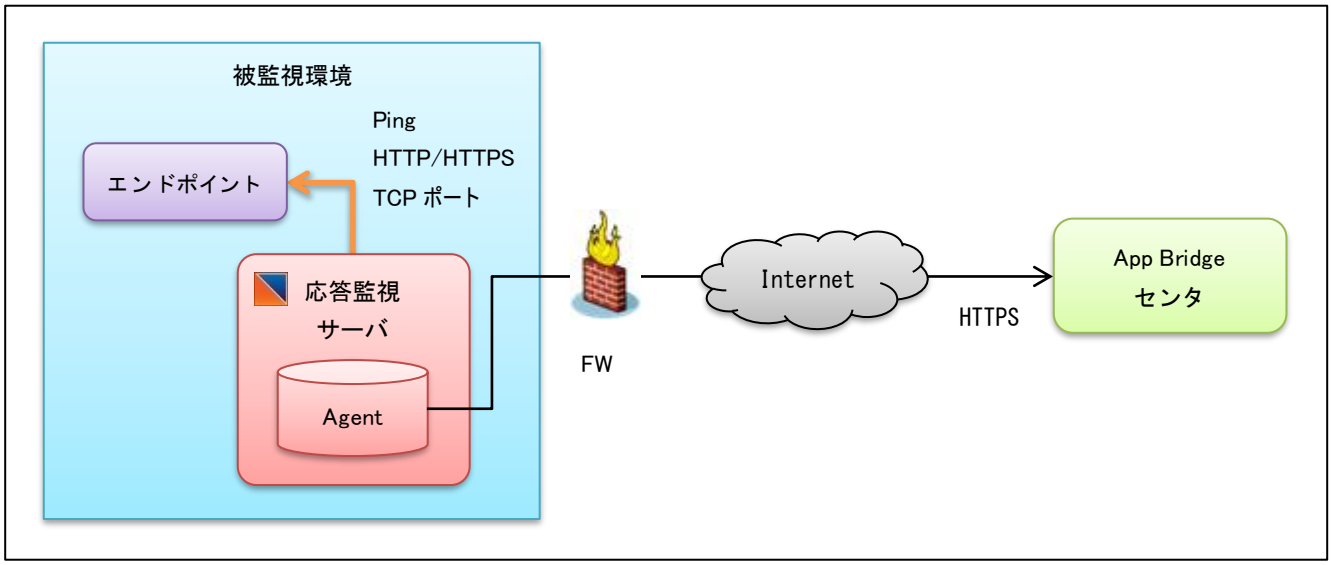
2.6 インターネット環境での応答監視

インターネット環境に接続されたサーバ、機器に対しては、App Bridge センタより監視します。監視対象のエンドポイントは、App Bridge センタから通信可能な環境であり、IPv4 の IP アドレスを保有する必要があります。



2.7 イントラネット環境の応答監視

イントラネット環境に接続されたサーバ、機器を監視するためには、同イントラネット環境に接続され、App Bridge Monitor Agent がインストールされた Windows サーバ（以下、イントラネット応答監視サーバ）が必要です。イントラネット応答監視サーバは、エンドポイントに対して応答監視を実施し、その結果を App Bridge センタに送信します。



2.8 AWS VPC 内の応答監視

イントラネット環境の応答監視を利用することで、Amazon Virtual Private Cloud（VPC）内で稼働するローカル IP アドレスしか持たないサーバインスタンスも監視対象とできます。

2.9 Azure Virtual Machines 内の応答監視

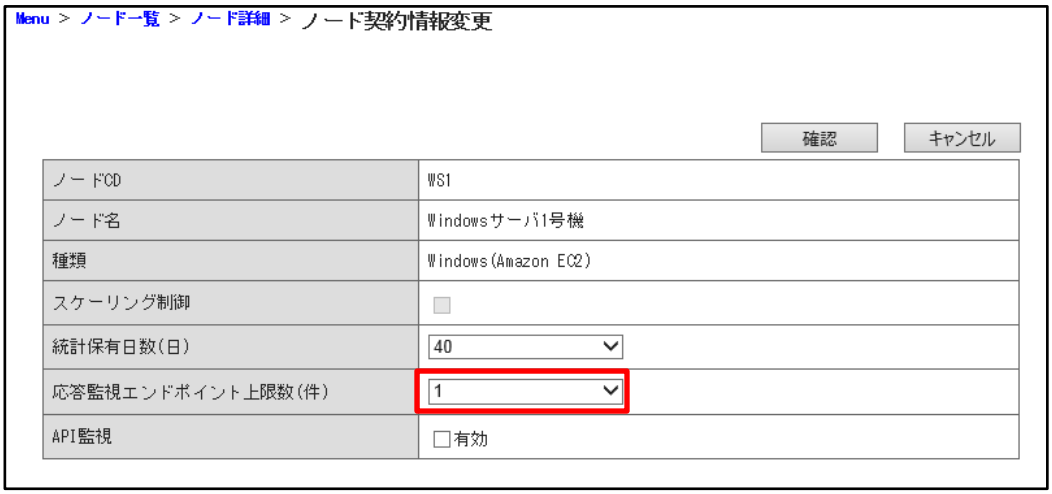
イントラネット環境の応答監視を利用することで、Cloud Service 内で稼働するローカル IP アドレスしか持たないサーバインスタンスも監視対象とできます。

３．応答監視設定

3.1 ノード管理

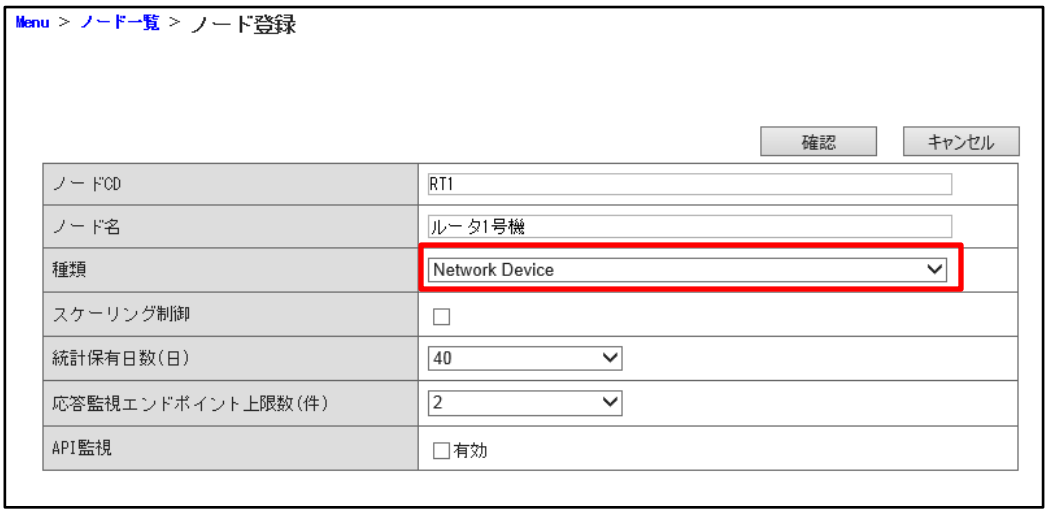
3.1.1 Windows サーバ、Linux サーバへの応答監視

Windows サーバ、Linux サーバにエンドポイントを設定することで、Agent によるサーバ監視に加え、応答監視を実施することができます。
既存の Windows サーバ、Linux サーバを応答監視対象とするためには、＜メインメニュー/ノード管理/ノード一覧/対象ノードを選択/ノード詳細＞で［ノード契約情報変更]ボタンをクリックし、応答監視エンドポイント上限数を設定して下さい。



3.1.2 ネットワークデバイスへの応答監視

ルータやファイアウォールなどのネットワークデバイスを応答監視対象とするためには、＜メインメニュー/ノード管理/ノード一覧＞で[ノード登録]ボタンをクリックし、種類：NetworkDevice のノードを登録して下さい。



3.2 HTTP 応答監視

3.2.1 HTTP 応答監視のエンドポイント設定

HTTP 応答監視エンドポイントの追加、変更、削除は、＜メインメニュー/監視設定/ノード一覧/対象ノード選択/ノード詳細＞で[応答監視エンドポイント]をクリックします。

HTTP 応答監視エンドポイントを追加する場合、[HTTP 追加]ボタンをクリックします。

表示された画面で監視内容を入力します。

項目名称	設定内容	備考
表示名	エンドポイントを識別する任意の名称を入力します	
URL	監視対象の URL を入力します。サーバポートの指定も可能です	
所属ネットワーク	エンドポイントの監視元となる所属ネットワークを選択します	
有効にする	指定したエンドポイントを監視する場合、チェックを付けます	
User-Agent を指定する	HTTP 監視を実施する際、HTTP User-Agent に「App Bridge HTTP Watcher」を指定する場合チェックします。チェックしない場合、User-Agent は設定されません	

【所属ネットワーク】

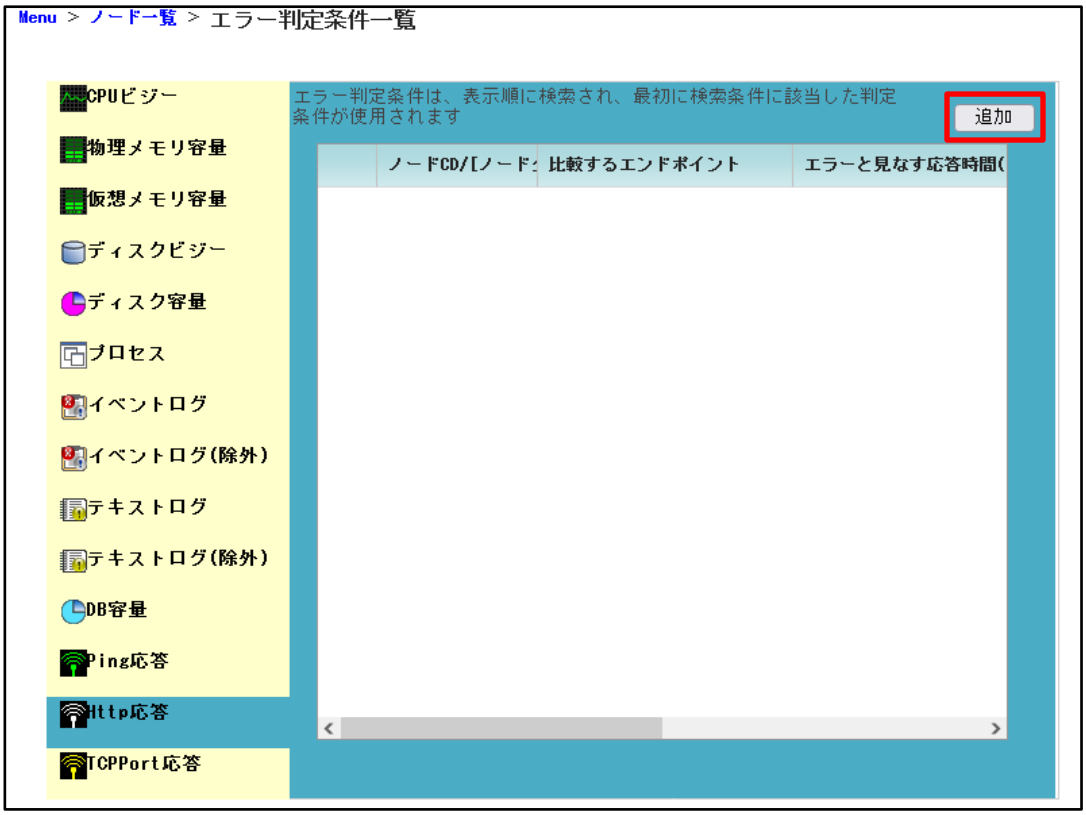
所属ネットワーク	内容	備考
Internet	App Bridge センタより監視します	
Intranet1	イントラネット応答監視サーバより監視します。監視させたいイントラネット応答監視サーバと同じ所属ネットワーク選択して下さい。 イントラネット外部サーバの設定は、後述のイントラネット応答監視サーバの構築でご確認下さい	
Intranet2		
Intranet3		
Intranet4		
Intranet5		

所属ネットワークが Internet の場合、本設定後、数分から数十分で応答監視が開始されます。所属ネットワークが Intranet1～5 の場合、後述のイントラネット応答監視サーバの構築が必要となります。

3.2.2 HTTP 応答監視の条件設定

HTTP 応答監視では、応答が得られない場合に加え、応答時間が HTTP 応答監視エラー判定条件に設定した閾値を越えたとき、異常と判定します。
HTTP 応答監視エラー判定条件を設定するには、＜メインメニュー/監視設定/ノード一覧＞の[エラー判定条件]をクリックし、[Http 応答]タブを選択します。

新しいエラー判定条件を追加する場合は[追加]ボタンを、既存のエラー判定条件を変更する場合は[編集]リンクをクリックします。



一覧のソート順は以下の通りです。

優先順位	キー	昇降順	備考
1	ノード CD/[ノードタグ]	昇順	"(指定ノードなし)"は最下位とみなします
2	比較するエンドポイントの判定項目	URL→表示名→比較なし	
3	比較するエンドポイントの比較値	昇順	
4	利用開始日時	昇順	

表示された画面でエラー判定条件を入力します。

【検索条件】

項目	内容	備考
ノード CD	対象のノードを指定します。(全ノード) を選択した場合、全てのノードを対象とします	
ノードタグ	対象のノードタグを指定します。ノードに設定されたタグと比較され、何れか 1 つでも一致すれば対象となります。	複数のノードタグが設定可能です
有効にする	チェックオフの場合、本条件は無効となります	
利用開始日時	現在時刻が利用開始日時未満の場合、本条件は無効となります	
利用終了日時	現在時刻が利用終了日時以降の場合、本条件は無効となります	
比較するエンドポイント	対象とする表示名、または URL を設定します	

【判定条件】

項目	内容	備考
エラーと見なす応答時間	異常と判定する閾値をミリ秒で指定します	

3.2.3 HTTP 応答監視の条件選出

HTTP 応答監視のエラー判定で使用されるエラー判定条件は 1 つであり、有効であり、且つ対象期間に該当するものの中から、以下の順で選出されます。

適用順	エラー判定条件			対象となる監視データ
	ノード CD	ノードタグ	エンドポイント	
1	ノード指定	なし	比較する	指定ノードであり、指定エンドポイントの監視データ
2	同上	なし	比較しない	指定ノードの監視データ
3	ノード指定なし	あり	比較する	ノードタグに該当するノードであり、指定エンドポイントの監視データ
4	同上	同上	比較しない	ノードタグに該当するノードの監視データ
5	同上	なし	比較する	指定エンドポイントの監視データ
6	同上	同上	比較しない	全ての監視データ

3.2.4 HTTP アクセスごとの条件判定

HTTP 監視は、4 回の HTTP アクセスを 1 つのセットとして実行し、4 回の HTTP アクセスで 1 度も HTTP ステータス 200 が得られなかった場合、リトライインターバルを設けたのちに、再度 4 回の HTTP アクセスを実行します。このため、HTTP 応答監視では、1 度の監視で 4 回、または 8 回の HTTP アクセスを実施します。

選出されたエラー条件を使用し、アクセスのごとの条件判定を実施します。該当するエラー判定条件が存在しないとき、応答時間の判定は OK とみなされます。

（1）ネットワークエラー
以下の何れかが発生した場合、NG と判定します。

- DNS 名前解決に失敗した場合
- タイムアウト（30 秒）が発生した場合
- 何らかの通信障害が発生した場合

（2）HTTP ステータス評価
通信が成功し、HTTP ステータスが得られた場合、下記表に従い HTTP ステータス評価します。

HTTP ステータス	HTTP レスポンスの Location ヘッダ	HTTP ステータス評価
200	ー	OK
301 Moved Permanently	指定された URL が存在する	OK
	指定された URL が存在しない	NG
302 Moved Temporarily	指定された URL が存在する	OK
	指定された URL が存在しない	NG
303 See Other	指定された URL が存在する	OK
	指定された URL が存在しない	NG
307 Temporary Redirect	指定された URL が存在する	OK
	指定された URL が存在しない	NG
上記以外	ー	NG

（３）応答時間

HTTP ステータス評価が OK の場合、選出されたエラー条件を使用し、エラー判定を以下のとおり実施します。該当するエラー判定条件が存在しないとき、応答時間の判定は OK とみなされます。

判定結果	条件
OK	応答時間≦エラーと見なす応答時間（ミリ秒）
NG	上記以外

3.2.5 HTTP 応答監視の条件判定

アクセスごとの条件判定を使用し、条件判定を以下のとおり実施します。

判定結果	条件
Good	全てのアクセスが OK である
Warning	1 つ以上のアクセスが OK である
Error	全てのアクセスが NG である

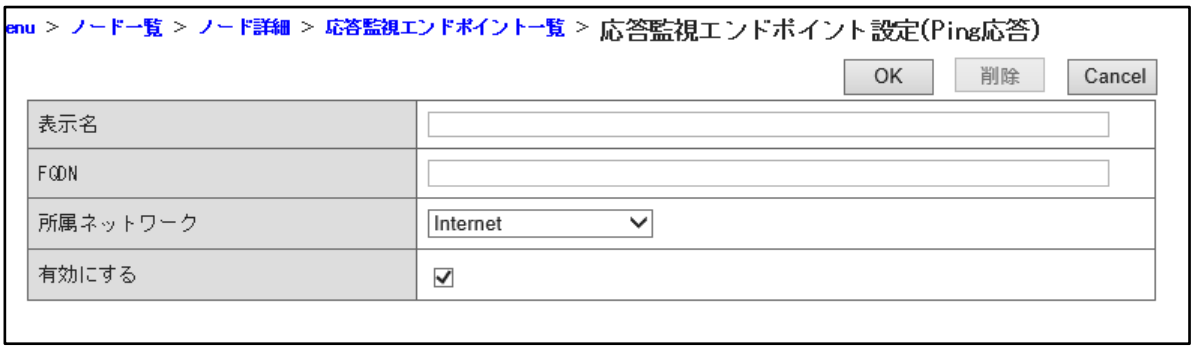
3.3 Ping 応答監視

3.3.1 Ping 応答監視のエンドポイント設定

Ping 応答監視エンドポイントの追加、変更、削除は、＜メインメニュー/監視設定/ノード一覧/対象ノード選択/ノード詳細＞で[応答監視エンドポイント]をクリックします。

Ping 応答監視エンドポイントを追加する場合、[Ping 追加]ボタンをクリックします。

表示された画面で監視内容を入力します。



項目名称	設定内容	備考
表示名	エンドポイントを識別する任意の名称を入力します	
FQDN	監視対象の FQDN を入力します	
所属ネットワーク	エンドポイントの監視元となる所属ネットワークを選択します	
有効にする	指定したエンドポイントを監視する場合、チェックを付けます	

【所属ネットワーク】

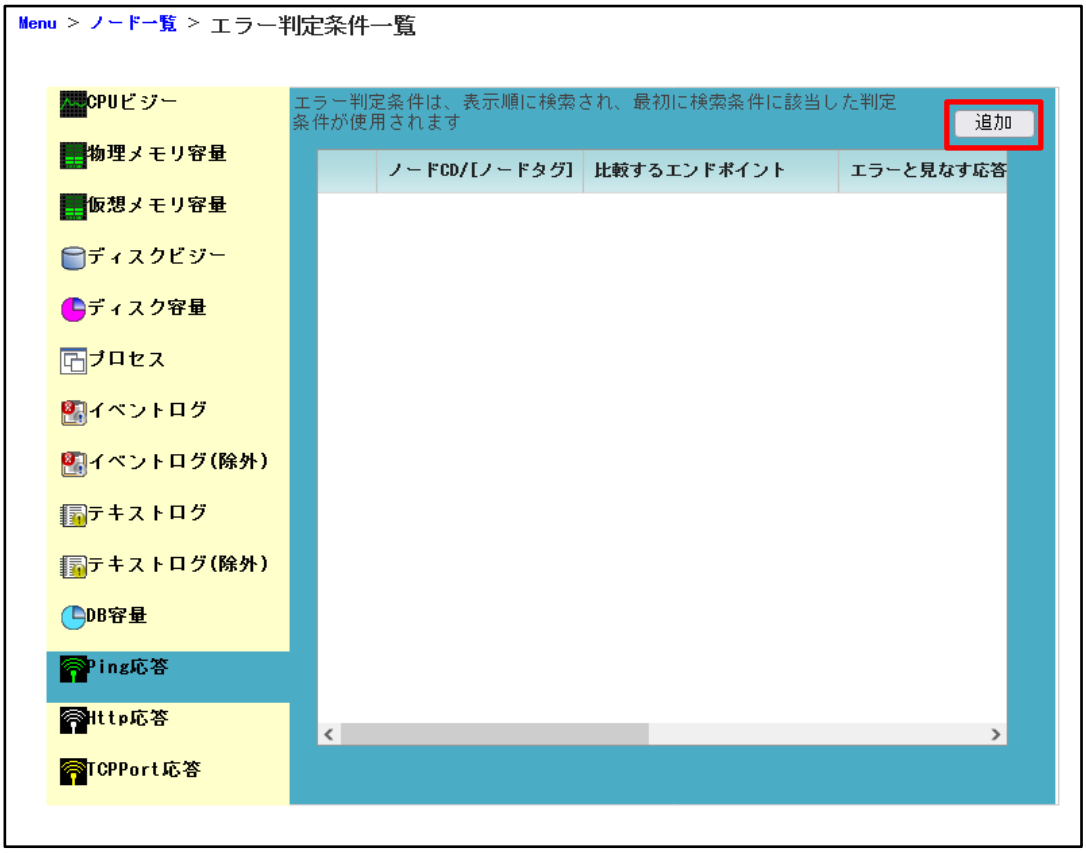
所属ネットワーク	内容	備考
Internet	App Bridge センタより監視します	
Intranet1	イントラネット応答監視サーバより監視します。監視させたいイントラネット応答監視サーバと同じ所属ネットワーク選択して下さい。 イントラネット外部サーバの設定は、後述のイントラネット応答監視サーバの構築でご確認下さい	
Intranet2		
Intranet3		
Intranet4		
Intranet5		

所属ネットワークが Internet の場合、本設定後、数分から数十分で応答監視が開始されます。所属ネットワークが Intranet1～5 の場合、後述のイントラネット応答監視サーバの構築が必要となります。

3.3.2 Ping 応答監視の条件設定

Ping 応答監視では、応答が得られない場合に加え、応答時間が Ping 応答監視エラー判定条件に設定した閾値を越えたとき、異常と判定します。
Ping 応答監視エラー判定条件を設定するには、＜メインメニュー/監視設定/ノード一覧＞の[エラー判定条件]をクリックし、[Ping 応答]タブを選択します。

新しいエラー判定条件を追加する場合は[追加]ボタンを、既存のエラー判定条件を変更する場合は[編集]リンクをクリックします。



一覧のソート順は以下の通りです。

優先順位	キー	昇降順	備考
1	ノード CD/[ノードタグ]	昇順	"(指定ノードなし)"は最下位とみなします
2	比較するエンドポイントの判定項目	FQDN→表示名→比較なし	
3	比較するエンドポイントの比較値	昇順	
4	利用開始日時	昇順	

表示された画面でエラー判定条件を入力します。

【検索条件】

項目	内容	備考
ノード CD	対象のノードを指定します。(全ノード) を選択した場合、全てのノードを対象とします	
ノードタグ	対象のノードタグを指定します。ノードに設定されたタグと比較され、何れか 1 つでも一致すれば対象となります。	複数のノードタグが設定可能です
有効にする	チェックオフの場合、本条件は無効となります	
利用開始日時	現在時刻が利用開始日時未満の場合、本条件は無効となります	
利用終了日時	現在時刻が利用終了日時以降の場合、本条件は無効となります	
比較するエンドポイント	対象とする表示名、または FQDN を設定します	

【判定条件】

項目	内容	備考
エラーと見なす応答時間	異常と判定する閾値をミリ秒で指定します	

3.3.3 Ping 応答監視の条件選出

Ping 応答監視のエラー判定で使用されるエラー判定条件は 1 つであり、有効であり、且つ対象期間に該当するものの中から、以下の順で選出されます。

適用順	エラー判定条件			対象となる監視データ
	ノード CD	ノードタグ	エンドポイント	
1	ノード指定	なし	比較する	指定ノードであり、指定エンドポイントの監視データ
2	同上	なし	比較しない	指定ノードの監視データ
3	ノード指定なし	あり	比較する	ノードタグに該当するノードであり、指定エンドポイントの監視データ
4	同上	同上	比較しない	ノードタグに該当するノードの監視データ
5	同上	なし	比較する	指定エンドポイントの監視データ
6	同上	同上	比較しない	全ての監視データ

3.3.4 Ping アクセスごとの条件判定

Ping 応答監視では、4 回の Ping アクセスを 1 つのセットとして実行し、4 回の Ping アクセスで 1 度も応答が得られなかった場合、リトライインターバルを設けたのちに、再度 4 回の Ping アクセスを実行します。このため、Ping 応答監視では、1 度の監視で 4 回、または 8 回の Ping アクセスを実施します。

選出されたエラー条件を使用し、アクセスのごとの条件判定を実施します。該当するエラー判定条件が存在しないとき、応答時間の判定は OK とみなされます。

判定結果	条件
OK	アクセスが成功し、応答時間≦エラーと見なす応答時間（ミリ秒）
NG	上記以外

3.3.5 Ping 応答監視の条件判定

アクセスごとの条件判定を使用し、条件判定を以下のとおり実施します。

判定結果	条件
Good	全てのアクセスが OK である
Warning	1 つ以上のアクセスが OK である
Error	全てのアクセスが NG である

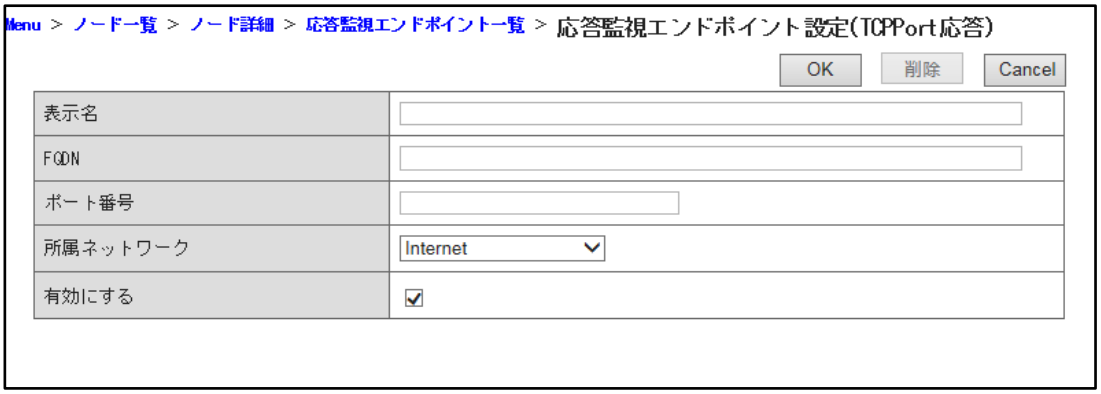
3.4 TCP ポート応答監視

3.4.1 TCP ポート応答監視のエンドポイント設定

TCP ポート応答監視エンドポイントの追加、変更、削除は、＜メインメニュー/監視設定/ノード一覧/対象ノード選択/ノード詳細＞で[応答監視エンドポイント]をクリックします。

TCP ポート応答監視エンドポイントを追加する場合、[TCPPort 追加]ボタンをクリックします。

表示された画面で監視内容を入力します。



項目名称	設定内容	備考
表示名	エンドポイントを識別する任意の名称を入力します	
FQDN	監視対象の FQDN を入力します	
ポート番号	監視対象のポート番号を入力します	
所属ネットワーク	エンドポイントの監視元となる所属ネットワークを選択します	
有効にする	指定したエンドポイントを監視する場合、チェックを付けます	

【所属ネットワーク】

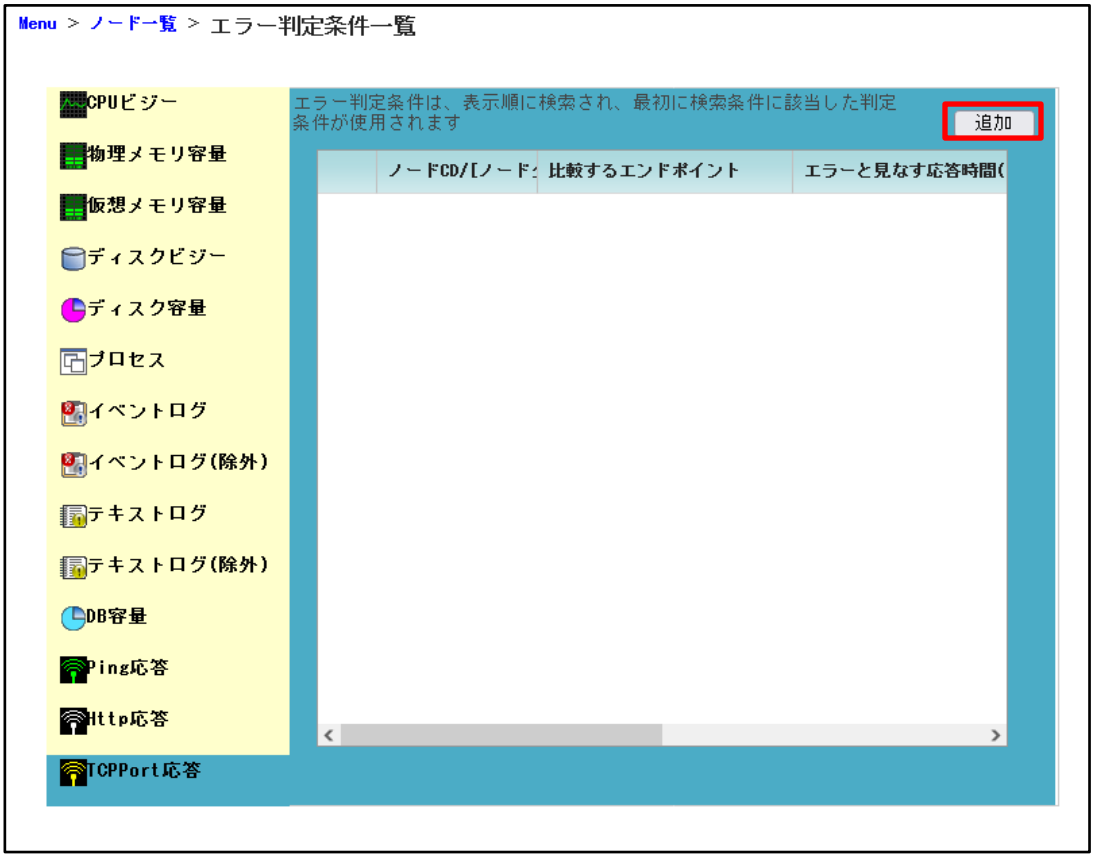
所属ネットワーク	内容	備考
Internet	App Bridge センタより監視します	
Intranet1	イントラネット応答監視サーバより監視します。監視させたいイントラネット応答監視サーバと同じ所属ネットワーク選択して下さい。 イントラネット外部サーバの設定は、後述のイントラネット応答監視サーバの構築でご確認下さい	
Intranet2		
Intranet3		
Intranet4		
Intranet5		

所属ネットワークが Internet の場合、本設定後、数分から数十分で応答監視が開始されます。所属ネットワークが Intranet1～5 の場合、後述のイントラネット応答監視サーバの構築が必要となります。

3.4.2 TCP ポート応答監視の条件設定

TCP ポート応答監視では、応答が得られない場合に加え、応答時間が TCP ポート応答監視エラー判定条件に設定した閾値を越えたとき、異常と判定します。
TCP ポート応答監視エラー判定条件を設定するには、＜メインメニュー/監視設定/ノード一覧＞の[エラー判定条件]をクリックし、[TCPPort 応答]タブを選択します。

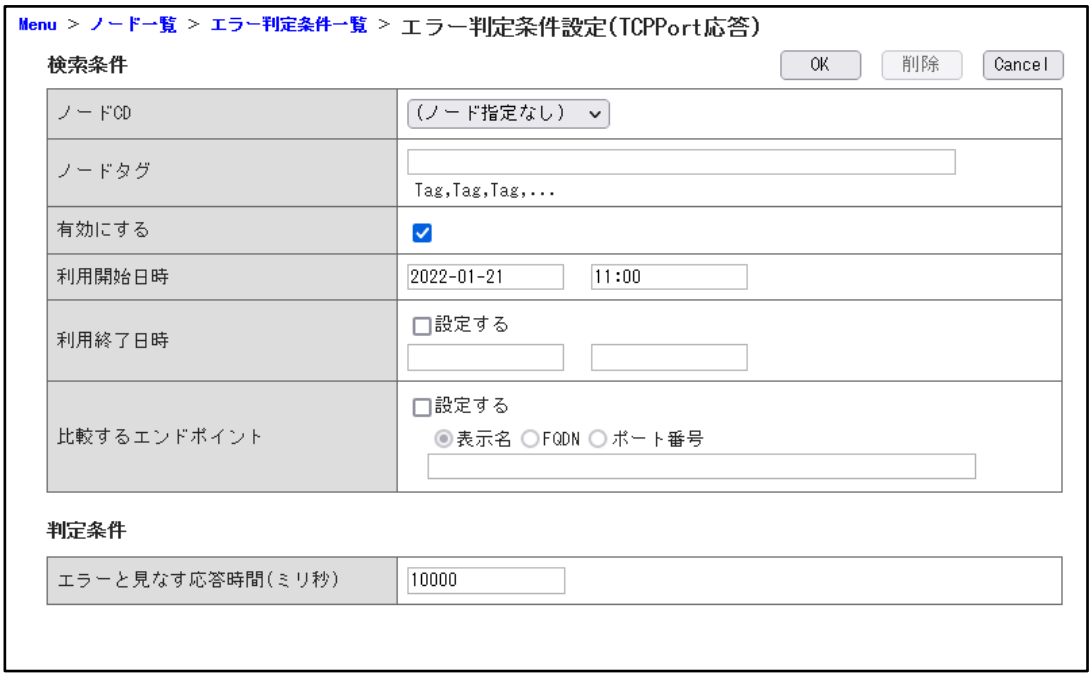
新しいエラー判定条件を追加する場合は[追加]ボタンを、既存のエラー判定条件を変更する場合は[編集]リンクをクリックします。



一覧のソート順は以下の通りです。

優先順位	キー	昇降順	備考
1	ノード CD/[ノードタグ]	昇順	"(指定ノードなし)"は最下位とみなします
2	比較するエンドポイントの判定項目	表示名→ポート番号→FQDN→比較なし	
3	比較するエンドポイントの比較値	比較するエンドポイントの判定項目の選択値による	表示名のとき、表示名の昇順 ポート番号のとき、ポート番号の昇順（文字としてではなく数値に変換して比較する） FQDN のとき、FQDN の昇順 比較なしのとき、比較せず（ソートキーなし）
4	利用開始日時	昇順	

表示された画面でエラー判定条件を入力します。



【検索条件】

項目	内容	備考
ノード CD	対象のノードを指定します。(全ノード) を選択した場合、全てのノードを対象とします	
ノードタグ	対象のノードタグを指定します。ノードに設定されたタグと比較され、何れか 1 つでも一致すれば対象となります。	複数のノードタグが設定可能です
有効にする	チェックオフの場合、本条件は無効となります	
利用開始日時	現在時刻が利用開始日時未満の場合、本条件は無効となります	
利用終了日時	現在時刻が利用終了日時以降の場合、本条件は無効となります	
比較するエンドポイント	対象とする表示名、FQDN、ポート番号を設定します	

【判定条件】

項目	内容	備考
エラーと見なす応答時間	異常と判定する閾値をミリ秒で指定します	

3.4.3 TCP ポート応答監視の条件選出

TCP ポート応答監視のエラー判定で使用されるエラー判定条件は 1 つであり、有効であり、且つ対象期間に該当するものの中から、以下の順で選出されます。

適用順	エラー判定条件			対象となる監視データ
	ノード CD	ノードタグ	エンドポイント	
1	ノード指定	なし	比較する	指定ノードであり、指定エンドポイントの監視データ
2	同上	なし	比較しない	指定ノードの監視データ
3	ノード指定なし	あり	比較する	ノードタグに該当するノードであり、指定エンドポイントの監視データ
4	同上	同上	比較しない	ノードタグに該当するノードの監視データ
5	同上	なし	比較する	指定エンドポイントの監視データ
6	同上	同上	比較しない	全ての監視データ

3.4.4 TCP ポートアクセスごとの条件判定

TCP ポート応答監視では、4 回の Ping アクセスを 1 つのセットとして実行し、4 回の TCP ポートアクセスで 1 度も応答が得られなかった場合、リトライインターバルを設けたのちに、再度 4 回の TCP ポートアクセスを実行します。このため、TCP ポート応答監視では、1 度の監視で 4 回、または 8 回の TCP ポートアクセスを実施します。

選出されたエラー条件を使用し、アクセスのごとの条件判定を実施します。該当するエラー判定条件が存在しないとき、応答時間の判定は OK とみなされます。

判定結果	条件
OK	アクセスが成功し、応答時間≦エラーと見なす応答時間（ミリ秒）
NG	上記以外

3.4.5 TCP ポート応答監視の条件判定

アクセスごとの条件判定を使用し、条件判定を以下のとおり実施します。

判定結果	条件
Good	全てのアクセスが OK である
Warning	1 つ以上のアクセスが OK である
Error	全てのアクセスが NG である

４．イントラネット応答監視サーバの構築

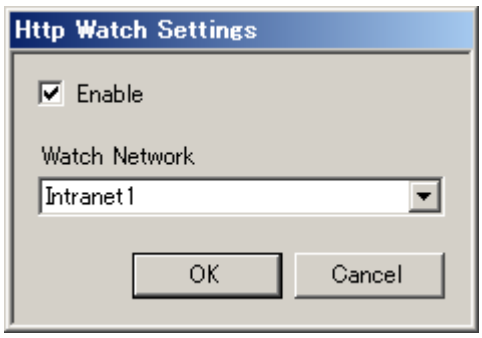
4.1 イントラネット応答監視サーバの要件

イントラネット応答監視には、Windows Agent をインストールしたサーバ（以下イントラネット応答監視サーバ）が必要です。イントラネット応答監視サーバとするためには、下記の何れかでノード登録されている必要があります。また、イントラネット応答監視サーバでスケーリング制御を利用できません。

#	種類	内容
1	Windows (On-Premises)	通常イントラネット環境内の応答監視を実施する場合に選択します。
2	Windows (Windows Azure Virtual Machines)	Azure Virtual Machines 環境内の応答監視を実施する場合に選択します。
3	Windows (Amazon EC2)	Amazon Virtual Private Cloud（VPC）内の応答監視を実施できます

4.2 HTTP 監視の設定

イントラネット応答監視サーバで HTTP 監視を実施させるためには､所属ネットワークの指定が必要です。所属ネットワークを設定するには、対象サーバで Service Control を起動します。Service Control のメニューから「Setting」 - 「Watch Service」 - 「Http」（※1）をクリックし、監視対象とする所属ネットワークを指定します。この設定により、選択した所属ネットワークに登録されたエンドポイントの監視が開始されます。

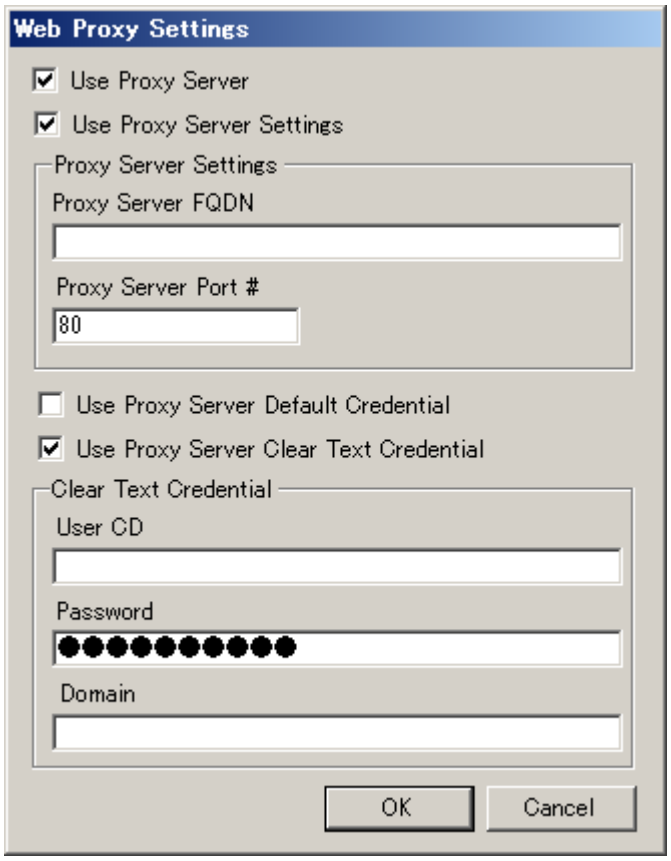


【入力ガイド】

項目名称	設定内容	備考
Enable	イントラネット応答監視サーバとしてHTTP監視を実施する場合、チェックを入れます	
Watch Network	所属ネットワークを選択します	

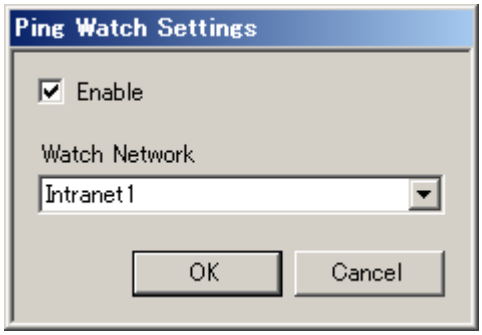
※1：Agent の導入時期によっては、メニュー「Setting」 - 「Watch Service」 - 「Http」が表示されない場合があります。メニューに「Http」が表示されない場合は、後述の「4.5 イントラネット応答監視のメニューが表示されない場合の対処」を参照し、対応下さい。

HTTP 監視を行なうイントラネット応答監視サーバでは HTTP 監視時に使用するプロキシの設定を行なうことができます。プロキシを設定するためには、Service Control を起動します。Service Control のメニューから「Setting」 - 「Watching Service」 - 「Http Proxy」をクリックし、プロキシサーバの情報を入力して下さい。



4.3 Ping 監視の設定

イントラネット応答監視サーバでPing監視を実施させるためには､所属ネットワークの設定が必要です。所属ネットワークを設定するには、対象サーバで Service Control を起動します。Service Control のメニューから「Setting」 - 「Watch Service」 - 「Ping」(※1) をクリックし、監視対象とする所属ネットワークを指定します。この設定により、選択した所属ネットワークに登録されたエンドポイントの監視が開始されます。



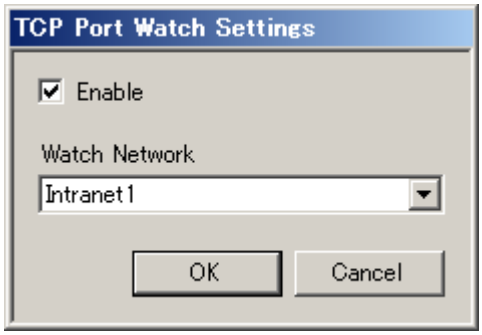
【入力ガイド】

項目名称	設定内容	備考
Enable	イントラネット応答監視サーバとしてPing監視を実施する場合、チェックを入れます	
Watch Network	所属ネットワークを選択します	

※1：Agent の導入時期によっては、メニュー「Setting」 - 「Watch Service」 - 「Ping」が表示されない場合があります。メニューに「Ping」が表示されない場合は、後述の「4.5 イントラネット応答監視のメニューが表示されない場合の対処」を参照し、対応下さい。

4.4 TCP ポート監視の設定

イントラネット応答監視サーバで TCP ポート監視を実施させるためには、所属ネットワークの指定が必要です。所属ネットワークを設定するには、対象サーバで Service Control を起動します。Service Control のメニューから「Setting」 - 「Watch Service」 - 「TCP Port」(※1) をクリックし、監視対象とする所属ネットワークを指定します。この設定により、選択した所属ネットワークに登録されたエンドポイントの監視が開始されます。



【入力ガイド】

項目名称	設定内容	備考
Enable	イントラネット応答監視サーバとして TCP ポート監視を実施する場合、チェックを入れます	
Watch Network	所属ネットワークを選択します	

※1：Agent の導入時期によっては、メニュー「Setting」 - 「Watch Service」 - 「TCP Port」が表示されない場合があります。メニューに「TCP Port」が表示されない場合は、後述の「4.5 イントラネット応答監視のメニューが表示されない場合の対処」を参照し、対応下さい。

4.5 イントラネット応答監視のメニューが表示されない場合の対処

Agent の導入時期によっては、以下のメニューが表示されない場合があります。

- 「Setting」 - 「Watch Service」 - 「Http」
- 「Setting」 - 「Watch Service」 - 「Ping」
- 「Setting」 - 「Watch Service」 - 「TCP Port」

これらのメニューを表示する場合、Windows Agent を最新バージョンにアップグレードいただいた上で、Smart Controller を使用し、「ノードの再設定」（Change Config）を実施して下さい。

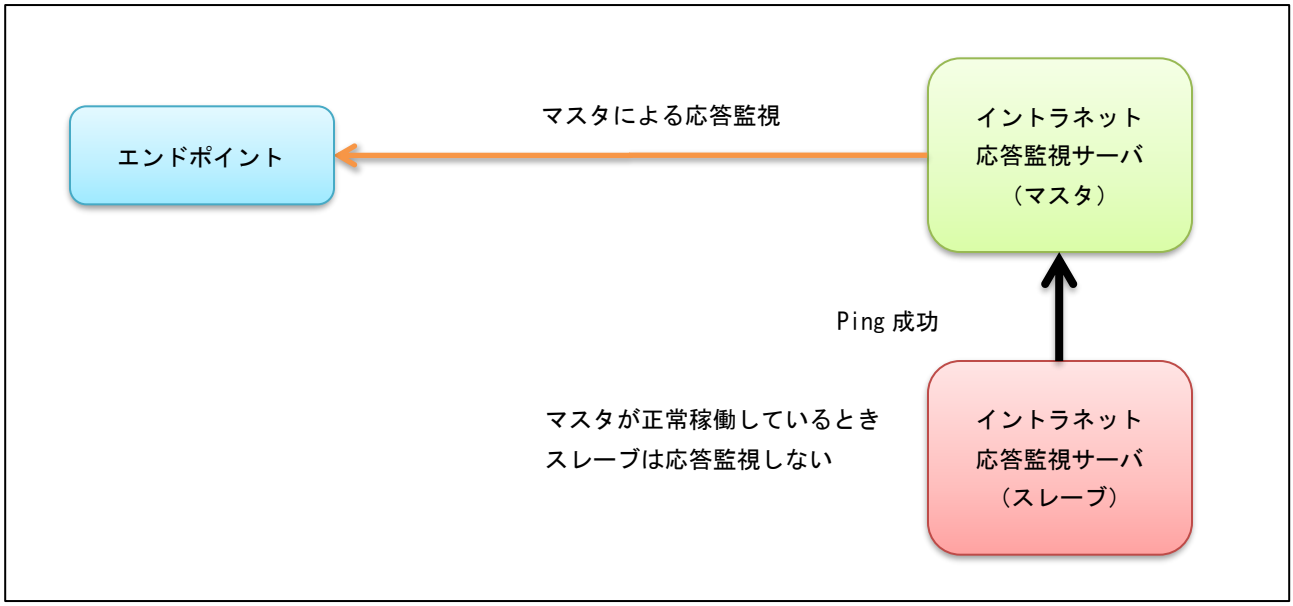
手順の詳細については、「App Bridge Monitor Agent 監視サービス Windows Agent インストールガイド」の「Windows Agent のアップグレード」、「ノードの再設定」を参照ください。

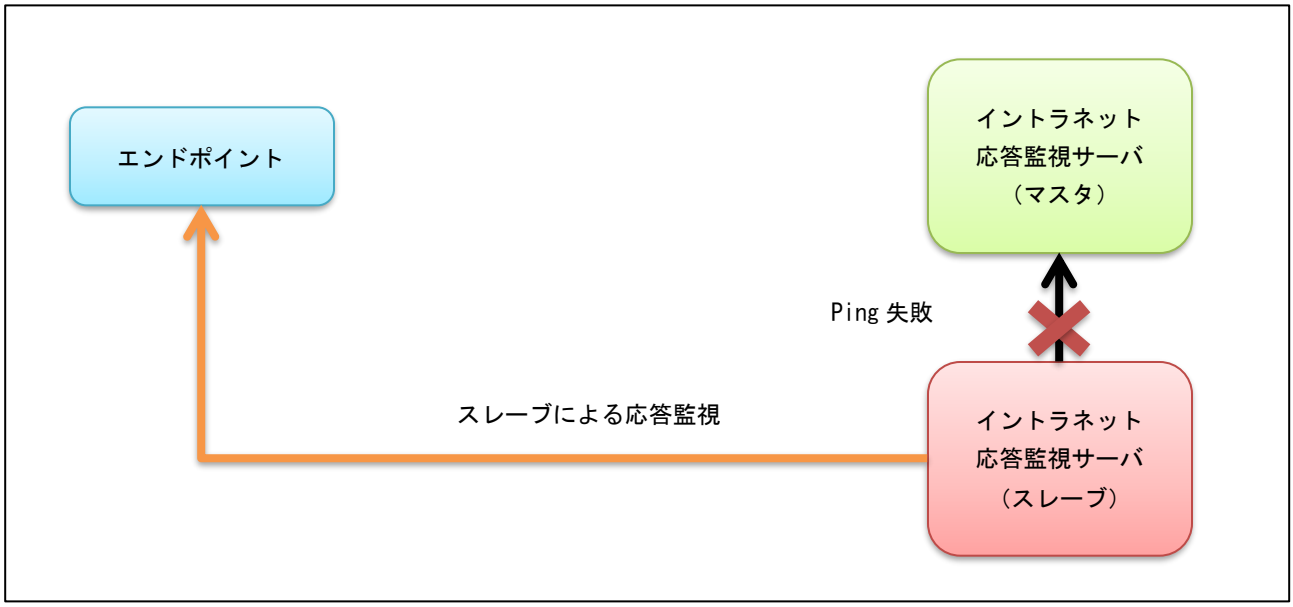
なお、「Windows Agent のアップグレード」、「ノードの再設定」を実施しても、各種監視設定は維持されます。

4.6 イントラネット応答監視サーバの二重化

4.6.1 イントラネット応答監視サーバの二重化とは

イントラネット応答監視サーバはコールドスタンバイの予備機を設置することで二重化することができます。通常稼働するイントラネット応答監視サーバを「マスタ」、マスタがダウンした時に稼働するイントラネット応答監視サーバを「スレーブ」と呼びます。スレーブはマスタを Ping 監視しており、Ping に応答しないとき、「マスタは正常稼働していない」と判断し、自らが応答監視を実施します。





4.6.2 マスタサーバの設定

マスタサーバには、イントラネット応答監視サーバとしての設定に加え、スレーブからの状態確認を可能とするため、ICMP の Echo 要求（受信）を許可する必要があります。

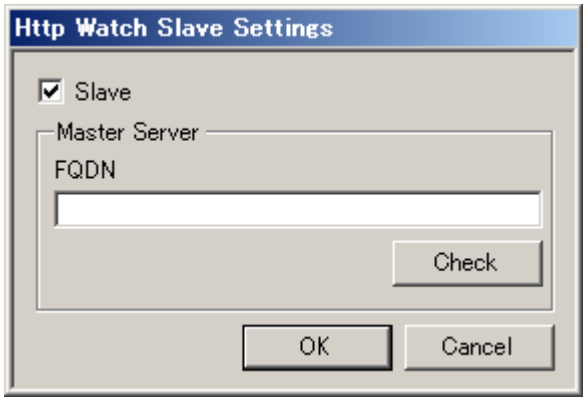
「セキュリティが強化された Windows ファイアウォール」で「受信の規則（Inbound Rules）/ICMP の Echo 要求」を有効化して下さい。

4.6.3 スレーブサーバの設定

スレーブサーバには、イントラネット応答監視サーバの設定に加え、以下の設定を実施します。

（１）HTTP のスレーブ設定

Service Control を起動します。Service Control のメニューから「Setting」 - 「Watch Service」 - 「Http (Slave)」をクリックし、スレーブの設定をします。

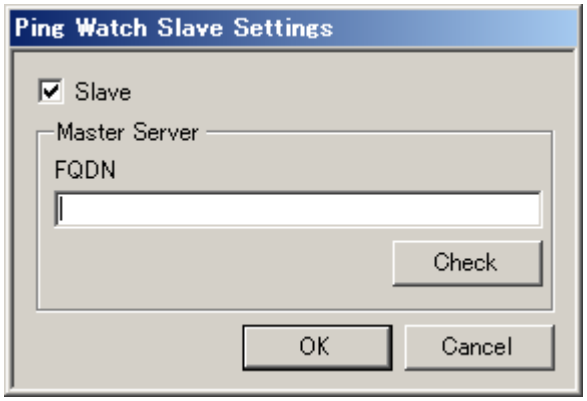


【入力ガイド】

項目名称	設定内容	備考
Slave	HTTP 監視のスレーブとして有効にする場合、チェックを付けます	
FQDN	HTTP 監視のマスタの FQDN または IP アドレスを入力します	

（２）Ping のスレーブ設定

Service Control を起動します。Service Control のメニューから「Setting」 - 「Watch Service」 - 「Ping (Slave)」をクリックし、スレーブの設定をします。

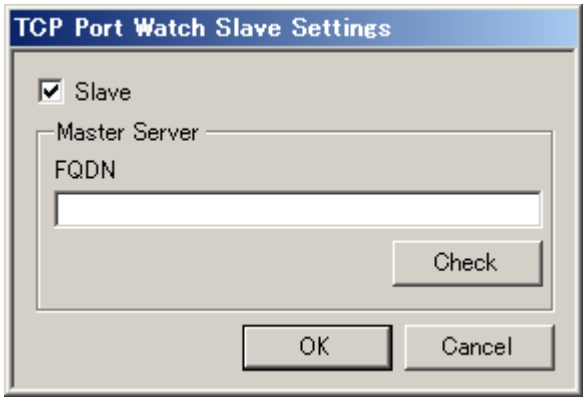


【入力ガイド】

項目名称	設定内容	備考
Slave	Ping 監視のスレーブとして有効にする場合、チェックを付けます	
FQDN	Ping 監視のマスタの FQDN または IP アドレスを入力します	

（３）TCPPort のスレーブ設定

Service Control を起動します。Service Control のメニューから「Setting」 - 「Watch Service」 - 「TCP Port (Slave)」をクリックし、スレーブの設定をします。



【入力ガイド】

項目名称	設定内容	備考
Slave	TCP ポート監視のスレーブとして有効にする場合、チェックを付けます	
FQDN	TCP ポート監視のマスタの FQDN または IP アドレスを入力します	