BOM for Windows Ver.7.0
ユーザーズ マニュアル

2020 年 4 月 28 日

免責事項

本書に記載された情報は、予告無しに変更される場合があります。セイ・テクノロジーズ株式会社は、本書に関していかなる種類の保証（商用性および特定の目的への適合性の黙示の保証を含みますが、これに限定されません）もいたしません。セイ・テクノロジーズ株式会社は、本書に含まれた誤謬に関しての責任や、本書の提供、履行および使用に関して偶発的または間接的に起こる損害に対して、責任を負わないものとします。

著作権

■ 目次

本ユーザーズマニュアルについて

製品表記

本ユーザーズマニュアルでは、下記の製品や製品の既定値について略称を使用しております。

正式名称	本マニュアルでの呼称（略称）
BOM for Windows Ver.6.0	BOM 6.0
BOM for Windows Ver.7.0 SR3	BOM 7.0
BOM Oracle オプション Ver.7.0 SR3	Oracle オプション 7.0
BOM Linux オプション Ver.7.0 SR3	Linux オプション 7.0
BOM VMware オプション Ver.7.0 SR3	VMware オプション 7.0
BOM 7.0 マネージャー	BOM マネージャー
BOM 7.0 集中監視コンソール	BOM 集中監視コンソール
BOM 7.0 監視サービス	BOM 監視サービス
BOM 7.0 アーカイブマネージャー	BOM アーカイブマネージャー
BOM 7.0 アーカイブデータベース管理メニュー	BOM アーカイブデータベース管理メニュー
BOM 7.0 コントロールパネル	BOM コントロールパネル
BOM 7.0 ヘルパーサービス	BOM ヘルパーサービス
BOM 7.0 アーカイブサービス	BOM アーカイブサービス
Windows Server 2008 R2、Windows 7、Windows 8.1、Windows Server 2012、Windows 10、Windows Server 2016、Windows Server 2019	Windows Server 2008 以降
Windows 7、Windows 8.1、Windows 10	Windows クライアント OS
SQL Server 2008、SQL Server 2012、SQL Server 2014、SQL Server 2016、SQL Server 2017、SQL Server 2019	SQL Server
Microsoft Management Console	MMC
Amazon Web Services	AWS
Amazon Simple Storage Service	Amazon S3
AWS Identity and Access Management	IAM
HPE Integrated Lights-Out	iLO
integrated Remote Management Controller	iRMC
C:¥Program Files¥SAY Technologies	BOM 7.0 インストールフォルダー

使用方法

このユーザーズマニュアルには、BOM 7.0 を使用する際に必要となる詳細な情報と手順が記載されています。

なお、BOM 7.0 のインストールに関しては‘BOM for Windows Ver.7.0 インストールマニュアル’を参照ください。

本書はインストールが正常終了した後の実際の使用方法について記述しています。

このユーザーズマニュアルを使用するには、Microsoft Windows オペレーティングシステムについての実践的な知識が必要です。

表記規則

本ユーザーズマニュアルでは、下記の表記規則を使用しています。

表記	解説
‘参照先’	シングルクォート内（‘と’）は本マニュアル内、あるいは別のマニュアルの参照を示します。
[ボタン]	角括弧内（[と]）はボタン名を示します。
<キー>	山括弧（不等号記号）内（<と>）はキーボード入力を示します。

第1章 はじめに

BOM 7.0 は、きわめて強力で豊富な機能を持つシステム監視と管理のためのプログラムです。
従来のサーバー監視プログラムに比べ、導入、設定、運用が容易で柔軟であることを特長としています。

1 .1 BOM 7.0 監視ソリューション

A. ハードウェア、ミドルウェア、アプリケーションのすべてを監視

BOM 7.0 は、プロセッサ、メモリ、ディスクといったサーバーのリソースに関する監視に利用することができます。
また、イベントログ、パフォーマンスカウンター、サービスログ、またはテキストログに有効な情報を書き込む製品であれば、
ハードウェアをはじめ、サーバー上で稼働するミドルウェア、アプリケーションも監視対象として簡単に設定することができます。

B. 豊富な監視テンプレートを無償公開

BOM 7.0 では、各種のハードウェア、ミドルウェア、アプリケーションの監視に必要な評価を行い、推奨の監視項目としきい値を
セットにした監視テンプレートを無償で公開しています。
ご利用予定もしくはご利用中のハードウェア、ミドルウェア、アプリケーションに合致する監視テンプレートをインポートするだけで、
面倒な監視設定を行わなくても、直ぐに監視がスタートできます。
監視テンプレートのインポート後、数週間程度運用を行っていただき、お客様の環境に合わせてしきい値を微調整いただく
だけで、お客様の環境に最適な監視ソリューションを実現することができます。
また、新しい監視テンプレートは随時 Web で公開しております。

C. 自立分散型と代理監視型　選択できる監視モデル

BOM 7.0 は、監視対象コンピューターに BOM 7.0 を導入するだけで、監視だけではなくさまざまな通知や自動リカバリまでを、
すべて自己で完結して実行できる自立分散型監視モデルを採用しています。
コンピューター監視は最小限のシステムリソースで稼働するため、BOM 7.0 専用の監視サーバーを構築する必要は
ありません。

なお、セキュリティポリシーなどで監視対象コンピューターに余計なプログラムを導入できない場合、BOM 7.0 を導入した
他の監視コンピューターから、リモートで監視を行うことができる代理監視機能を選択することもできます。
（自立分散型監視モデルと同じ監視機能を利用することができます。）

これらの BOM 7.0 の監視機能・監視モデルにより、システム管理者はさまざまなシステム環境やネットワーク構成、特殊用途の
システム監視にも柔軟に対応することができます。

1.2 特長と使用方法

A. セキュリティ

セキュリティ確保のため、サーバー管理者が監視設定を行うコンピューターの権限を制限することや、アクセス範囲を特定のコンピューターに限定することが可能です。

●管理者モードと参照モード

1 台のコンピューターに監視設定変更操作できるのは 1 人に限定されます（管理者モード）。

1 台のコンピューターに複数のサーバー管理者が同時接続する場合には、参照モードで参照することができますが、設定変更は管理者モードのみ実行できます。

B. 問題の監視

BOM 7.0 を適切に設定することで、システム障害の発生を迅速に検出することができます。

想定されるシステム障害の内容に応じて、リカバリを行うアクション機能を設定しておくことができます。

C. 障害予兆の監視

障害が発生する前のシステム動作の不良を検出できるため、今後発生する可能性がある事象に対して早期に対応を行うことが可能になります。

D. リソースの監視

BOM 7.0 は、メモリやハードディスクドライブなど、システムリソースのステータスを監視します。

ダウンしたシステムや、極端にパフォーマンスが低下したシステムに、プロアクティブに対処することが可能になります。

E. パフォーマンスの監視

BOM 7.0 でシステムのパフォーマンスを監視することにより、サービスレベルの低下を防止することができます。

F. 対象コンピューターのセキュリティ監視

BOM 7.0 は、オペレーティングシステム（OS）が生成するイベントログを監視し、不正なアクセスやログオンの失敗を検出します。

1.3 コンポーネント

BOM 7.0 は複数のコンポーネントで構成されています。

これらのコンポーネントは、1 台のコンピューターに導入することも、複数台のコンピューターに分散導入することもできます。

●各コンポーネントは OS のセーフモードでは動作しませんので、通常モードで動作させてください。

●JIS2004 の文字列を使用した監視内容（監視対象名、監視項目名、インストールパス、検索する文字列等）については対応しておりません。

BOM 7.0 のコンポーネントには、管理者が必要に応じて設定を行うアプリケーションと、バックグラウンドで動作するサービスがあります。

A. 設定を行うアプリケーション

●BOM マネージャー

BOM 7.0 の監視設定や監視ログといった各種ログの確認を行うには、BOM マネージャーが少なくとも 1 つ必要です。

BOM マネージャーは、監視グループ、監視項目、アクション項目、通知項目などを設定するために使用できますので、
監視対象として着目した項目（ステータス、イベントなど）が、どのような状態になったときに、どのような対処を行うのかを
設定することができます。
また、BOM マネージャーには各種ログビューアー機能が用意されており、設定を行った監視項目、アクション項目、通知項目の
実行結果や監視によって検出したイベントログを確認することができます。

BOM マネージャーは Windows 標準のシステム管理インターフェイスである“マイクロソフト管理コンソール（MMC）”の
スナップインとして提供されます。
標準インストールの場合、BOM マネージャーは BOM 監視サービスと同時に導入されます。
リモートにある対象コンピューターの監視項目などの設定や監視ログなどの確認は、そのコンピューターに接続している
BOM マネージャーから行うことができます。

●BOM 集中監視コンソール

BOM 集中監視コンソールを利用することで、個々の対象システムから監視データを収集し、数多くのシステムのステータスを
集中監視することができます。
BOM 7.0 の旧バージョンである BOM 6.0 インスタンス、Linux 6.0 インスタンス、VMware 6.0 インスタンス、
BOM 5.0 インスタンス、Linux 5.0 インスタンス、VMware 5.0 インスタンスによる監視状況も含め、
1 つの画面で確認することができます。

リモートおよびローカルの対象システムで稼働する BOM ヘルパーサービスから集中監視 Web サービスに情報を収集し、
監視用端末のブラウザーで集中監視 Web サービスに接続することで、BOM 集中監視コンソールを利用することができます。
詳細は ‘集中監視コンソールユーザーズマニュアル’ を参照してください。

●BOM アーカイブマネージャー

BOM アーカイブマネージャーは BOM 7.0 のアーカイブデータベースに蓄積されたデータを閲覧するためのコンソールです。
BOM アーカイブマネージャーは Windows 標準のシステム管理インターフェイスである“マイクロソフト管理コンソール（MMC）”の
スナップインとして提供されます。
詳細は ‘アーカイブ ユーザーズマニュアル’ を参照してください。

●BOM コントロールパネル

BOM マネージャーや BOM 集中監視コンソールの起動、インスタンスの開始と終了を行うことができます。

またバックアップとリストアのためのツール、複数のコンピューターを対象とした監視設定内容の収集と配布、
一括配布を行うツール、SNMP マネージャーサービスの設定、BOM バックアップサービスの設定、
インストールした BOM 7.0 の各モジュールのバージョンの確認を行うツールが含まれています。
詳細は ‘第 10 章 BOM コントロールパネル’ を参照してください。

B. バックグラウンドで動作する BOM 7.0 のコンポーネント

●BOM 監視サービス（インスタンス）

システム監視を実行するには、BOM 監視サービスが少なくとも 1 つ必要です。
BOM 監視サービスは監視設定値を使用して実際の監視を行い、取得したデータはテキストもしくはデータベースに格納します。

また、BOM 監視サービスは同一の監視元コンピューターに複数作成することができます。
BOM 7.0 では 1 つの BOM 監視サービスをインスタンスと呼び、代理監視の場合、インスタンスが 1 つ独立して割り当てられます。

●BOM ヘルパーサービス

BOM ヘルパーサービスは、前述の‘A.設定を行うアプリケーション’や‘B.バックグラウンドで動作する BOM 7.0 のコンポーネント’
間の通信部分の処理を行います。

●集中監視 Web サービス

集中監視 Web サービスは BOM ヘルパーサービスと通信を行い、インスタンスの監視データを収集/蓄積します。
集中監視 Web サービスにブラウザーで接続することで、BOM 集中監視コンソールを利用することができます。
詳細は ‘集中監視コンソール ユーザーズマニュアル’ を参照してください。

●BOM アーカイブサービス

BOM アーカイブサービスは BOM 監視サービスごとに動作し、BOM 7.0 の監視取得値を定期的にアーカイブデータベースに
蓄積します。
詳細は ‘アーカイブ ユーザーズマニュアル’ を参照してください。

●BOM SNMP マネージャーサービス

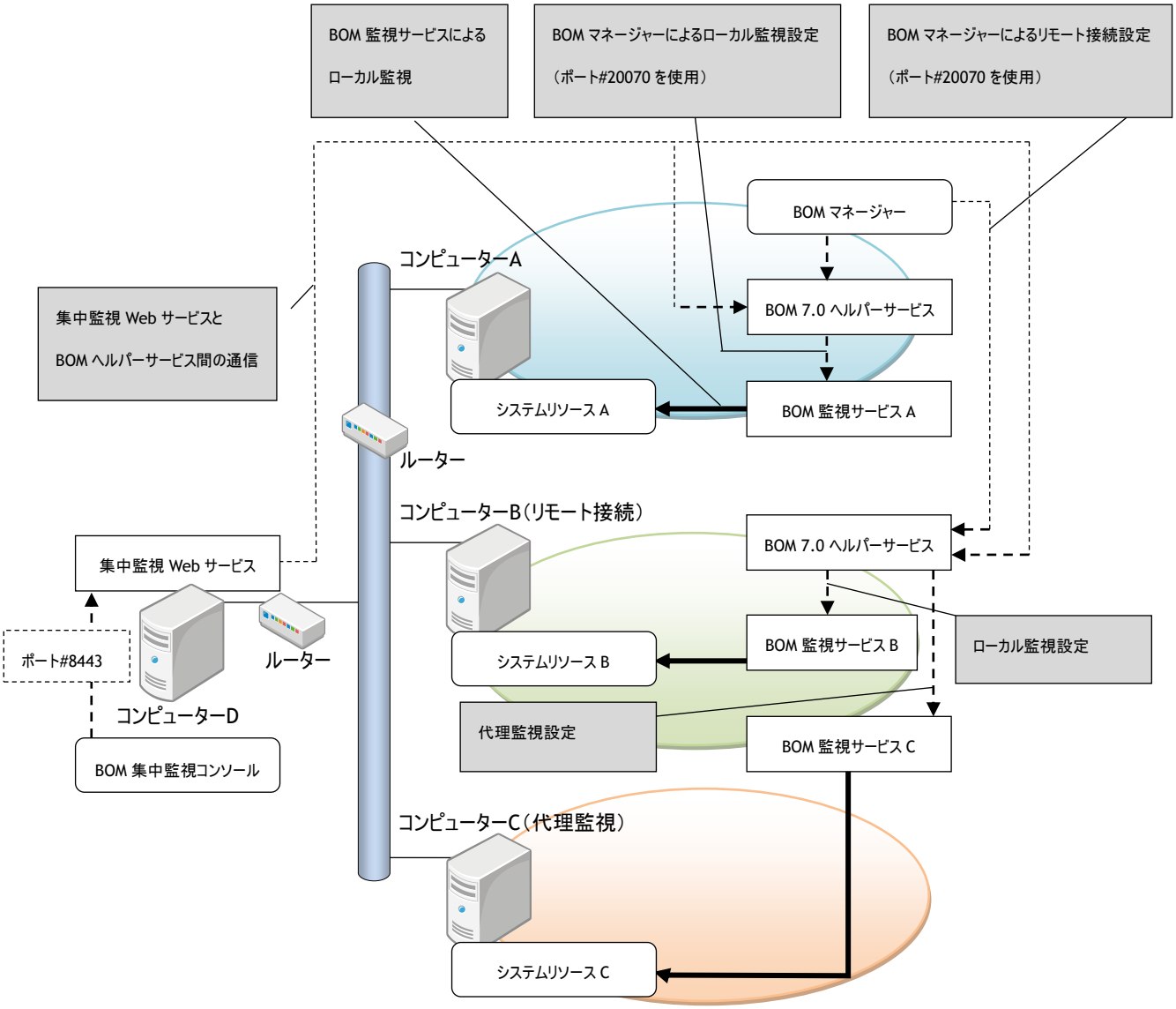
BOM SNMP マネージャーサービスは SNMP トラップを受信し、Windows のイベントログに書き込み処理を行います。
詳細は ‘SNMP トラップ受信機能 ユーザーズマニュアル’ を参照してください。

●BOM バックアップサービス

BOM バックアップサービスは BOM バックアップ機能を使用する際にバックグラウンドで動作する、ドライブ単位やフォルダー、
ファイル単位でバックアップを行うためのサービスです。
BOM バックアップ機能を使用することで、ローカルマシン、リモートマシンのフォルダー・ファイルを簡単にバックアップできます。
詳細は ‘バックアップ機能ユーザーズマニュアル’ を参照してください。

1 .4 BOM 7.0 の構成とコンポーネント間通信

BOM 7.0 のコンポーネント間の通信は、TCP/IP を使用しています。これは、コンポーネントが同じコンピューター上で稼働するスタンドアローン環境でも、別々のコンピューター上で稼働する分散環境でも同じです。



BOM 7.0 の構成例と各通信の概略図を上記に示します。この図は BOM 監視システムの機能を解説するために、下記の通り最小限の台数のネットワーク接続されたコンピューターのネットワーク構成図です。

●図中のルーターは、BOM 7.0 環境に必須のコンポーネントではありません。

●コンピューターA はスタンドアローン構成で、コンピューターB はルーターを越えた分散環境にあります。

●BOM ヘルパーサービスのインストール時に、BOM ヘルパーサービスを Windows ファイアウォールの例外に追加することができます。
詳細は、‘BOM for Windows Ver.7.0 インストールマニュアル’を参照ください。

●BOM ヘルパーサービスのポート番号の変更手順は、‘10 .3 .2 BOM ヘルパーサービス設定’を参照ください。

●BOM ヘルパーサービスのポート番号を変更した際には、BOM マネージャーおよび BOM 監視サービスの待ち受けポート番号を、‘2 .3 .2 全般’の手順で変更後のポート番号に合わせる必要があります。

●BOM ヘルパーサービスのポート番号を変更した際には、集中監視 Web サービスに登録されたインスタンスごとにヘルパーサービス
ポート番号を変更後のポート番号に合わせる必要があります。変更方法については
‘BOM for Windows Ver.7.0 集中監視コンソールユーザーズ マニュアル’を参照してください

コンピューターD の集中監視 Web サービスとブラウザー間の通信は、8443 番ポートを使用します。

●集中監視 Web サービスとブラウザー間のポート番号の変更手順については、‘10 .8「集中監視 Web サービス」タブ’および、
‘BOM for Windows Ver.7.0 集中監視コンソールユーザーズ マニュアル’を参照ください。

●集中監視 Web サービスとブラウザー間のポート番号を変更した際には、集中監視 Web サービスの接続先 URL のポート番号を
変更後のポート番号に合わせる必要があります。
詳細は、‘BOM for Windows Ver.7.0 集中監視コンソールユーザーズ マニュアル’を参照ください。

A. コンピューターA

（BOM 監視サービス A、BOM ヘルパーサービス、BOM マネージャーを導入）

このコンピューターは、BOM 7.0 の標準インストール直後の状態を表しています。
管理者は BOM マネージャーを起動することにより、ローカル接続またはリモート接続で、BOM ヘルパーサービスを通じて
監視設定を行うことができます。
ローカル接続では、コンピューターA のすべての監視設定が可能です。
BOM マネージャーがコンピューターA に導入されているため、BOM 監視サービスが稼働するシステムの監視設定は、
すべてコンピューターA から設定を行うことができます。
この場合、BOM 監視サービス A が稼働するコンピューターA、BOM 監視サービス B と BOM 監視サービス C が稼働する
コンピューターB は、すべてコンピューターA から監視設定を行うことができます。

B. コンピューターB

（BOM 監視サービス B、BOM 監視サービス C、および BOM マネージャー、BOM ヘルパーサービスを導入）

コンピューターA の BOM マネージャーからリモート接続してコンピューターB の監視設定を行います。また、コンピューターB から
コンピューターC を代理監視するため、BOM 監視サービス B の他に BOM 監視サービス C が設定されています。
代理監視とは、BOM 7.0 を導入したコンピューターから BOM 7.0 を導入していないコンピューターに対して、ネットワークを通じて
監視を行う監視方法です。（エージェントレス監視）
コンピューターA からのリモート接続によるコンピューターB、およびコンピューターC の監視設定、また、コンピューターD からの
BOM 集中監視コンソールのステータス確認は、BOM ヘルパーサービスを通じて実施されます。

C. コンピューターC

（BOM 7.0 のコンポーネントは未導入）

このコンピューターには、BOM 7.0 のコンポーネントが導入されていません。
コンピューターB の BOM 監視サービス C が、リモートにあるこの対象コンピューターC を監視するために割り当てられています。
コンピューターB からネットワークを通じてコンピューターC を代理監視していますが、代理監視を行うには管理者権限で

コンピューターC にログオン可能なログオンアカウントなどの適切な権限が必要です。

D. コンピューターD

（集中監視 Web サービスのみを導入）

このコンピューターには集中監視 Web サービスのみが導入されています。集中監視 Web サービスは、コンピューターA と
コンピューターB の BOM ヘルパーサービスを通じて監視ステータスを収集して蓄積するサービスです。
集中監視 Web サービスに、コンピューターD のブラウザーで接続することで、収集した監視情報の結果すべてを
BOM 集中監視コンソールに表示します。
コンピューターD に BOM マネージャーを導入した場合、コンピューターD からコンピューターA、コンピューターB、コンピューターC の
すべての監視設定を実施することができます。

第2章 BOM マネージャー

2 .1 BOM マネージャーの解説

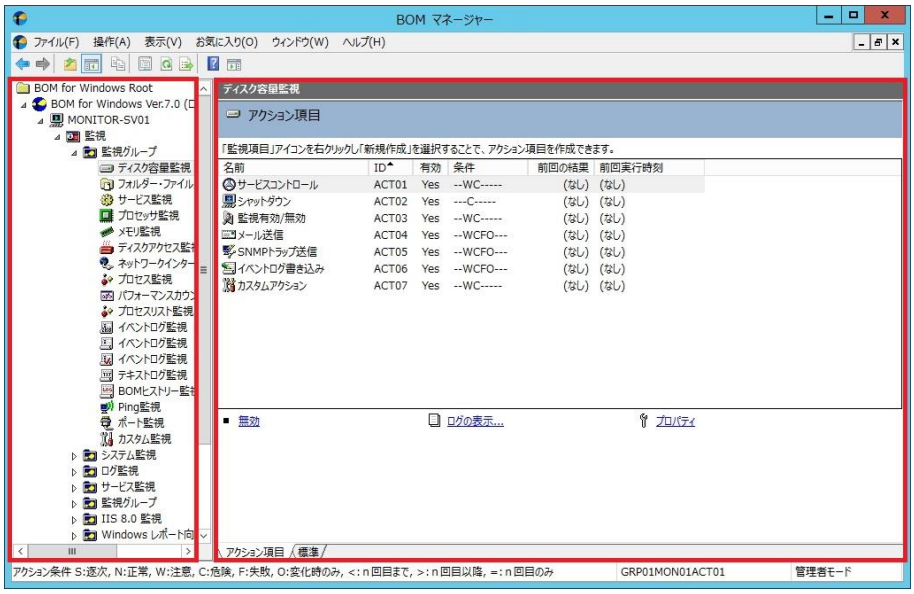
BOM マネージャーは Windows のエクスプローラー画面のように、さまざまな項目がフォルダーツリーのような階層内に設定されています。

本マニュアルでは、BOM マネージャーの左側のペインをスコープペインと呼び、右側のペインはリザルト（結果）ペインと呼びます。

スコープペインに表示されるものを“ノード”といい、リザルトペインには“ノード”のもつ情報を表示します。

●スコープペインには、BOM 7.0 の監視グループ、監視項目等が配置されています。

●リザルトペインには、スコープペインで選択した項目に属する内容が表示されます。



↑スコープペイン　　↑リザルトペイン

2 .2 初期スタートアップ

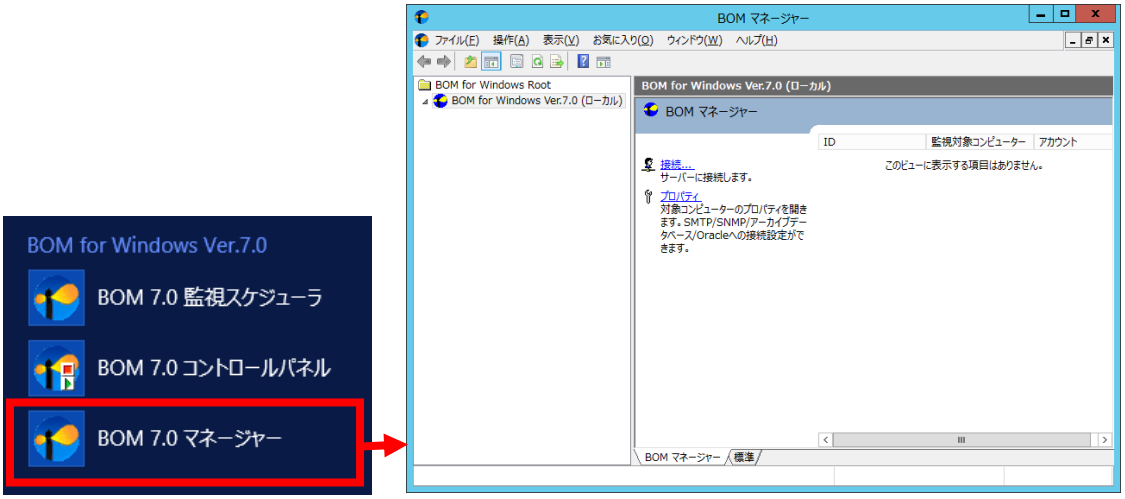
1. BOM マネージャーを起動するには、OS のスタート画面で右クリックし、“すべてのアプリ”を選択したのちに表示される“BOM 7.0 マネージャー”をクリックします。

   ●Windows Server 2008 R2 の場合は、[スタート]→“すべてのプログラム”→“BOM”→“BOM for Windows Ver.7.0”配下に“BOM 7.0 マネージャー”が表示されます。

   ●BOM マネージャーの起動には、管理者権限が必要です。

   ●BOM マネージャーは、OS のセーフモードでは動作しません。通常モードで起動してください。

2. BOM マネージャーのリザルトペインにある“接続…”をクリックします。



2 .2 .1 アカウントとパスワード

BOM 7.0 には、管理者モードと参照モードの 2 つのモードがあります。

管理者モードでは、管理者が BOM 7.0 の設定変更を行う時に使用します。

A. 参照モード

参照モードはログインした管理者は監視設定の参照のみに限定され、編集権限はありません。

参照モードの場合、同じ監視インスタンスに対して 2 台以上の BOM マネージャーから同時に接続することができます。

B. 管理者モード

●排他制御

管理者モードで同時にログインできる管理者は一人のみです。管理者の 1 人が管理者モードでログインすると他の管理者は参照モードでのみログイン可能で、監視設定を変更することはできません。管理者モードログイン時に他のマネージャーが管理者モードでログインしようとすると“管理者モードはすでに使用されている”というメッセージが出ます。

●セッションタイムアウト

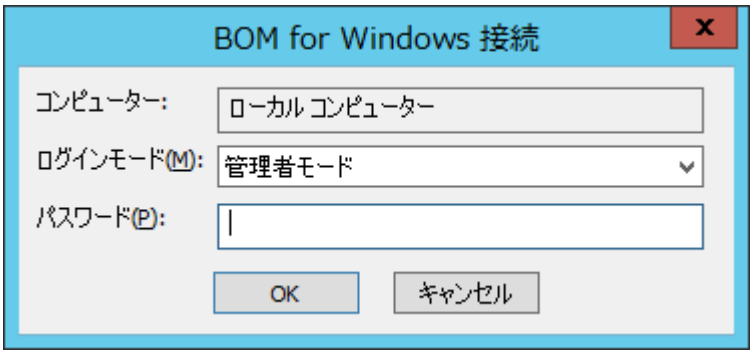
管理者モードでは 2 つ以上のマネージャーからの同時接続はできないため、BOM マネージャーが管理者モードで切断することを忘れた時に、他の BOM マネージャーから、管理者モードで接続できなくなることを防ぐために、BOM 7.0 はセッションタイムアウト機能を備えています。管理者モードで接続のまま 5 分以上無操作状態が続くと、他の BOM マネージャーから管理者モードで接続が可能になります。

（3 日以上無操作状態で操作しようとすると“ログオンセッションが無効です”というエラーとなりますので、再接続してください。）

●セッションタイムアウト時間の変更

管理者モードから参照モードに移行するまでの無操作状態の時間は既定値で 5 分に設定されていますが、この時間を変更したい場合には、秒単位で設定することができます。詳細は、‘10 .3 .2 BOM ヘルパーサービス設定’を参照ください。

C. BOM マネージャーの接続



1. 前述の‘A.参照モード’、‘B.管理者モード’を参考に、使用するモードを選択します。
2. パスワードを入力して、[OK]ボタンをクリックします。

●BOM 7.0 の管理者モードおよび参照モードの既定値パスワードは、<bom>（半角英 3 文字）です。

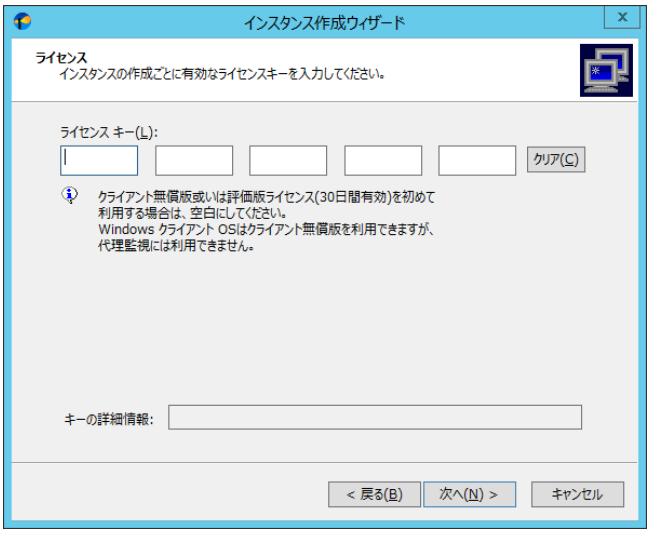
●インストール時に、“システム設定ウィザード”をキャンセルした場合、もしくは、システム設定ウィザードの“BOM for Windows マネージャー接続アカウント”画面で何も変更せずに[次へ]ボタンをクリックした場合は既定のパスワードが設定されています。

●パスワード変更するには“BOM for Windows Ver.7.0（ローカル）”を右クリックし、コンテキストメニューの“パスワードの変更..”をクリックします。古いパスワードと新しいパスワードを入力し、新しいパスワードを確認します。

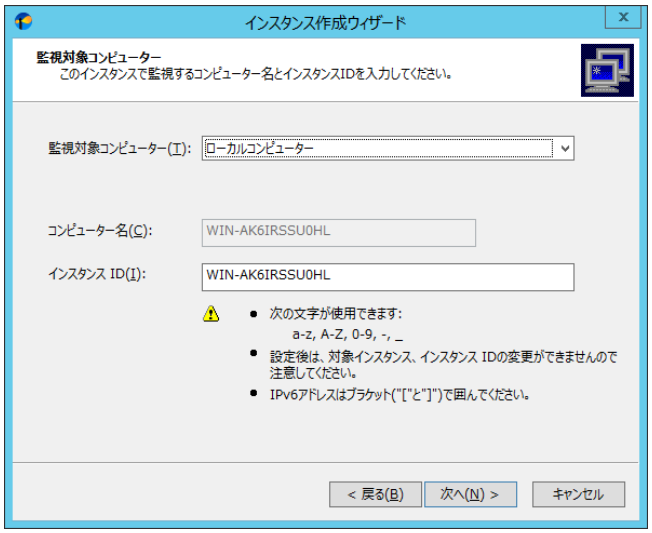
●管理者モード、参照モードを問わず、BOM マネージャーの起動自体に Windows の管理者権限が必要です。

2 .2 .2 インスタンス作成

1. 接続後、“BOM for Windows Ver.7.0 （ローカル）”を右クリックし、コンテキストメニューの
   “新規作成”→“監視インスタンス...”の順にクリックします。
   または、メニューバーに移動し、“操作”→“新規作成”→“監視インスタンス...”の順にクリックします。
2. “インスタンス作成ウィザード”が開始されるので[次へ]ボタンをクリックすると、“インスタンス作成ウィザード ライセンス”画面が
   表示されます。



3. 製品パッケージに同梱されているライセンスキーを入力し、[次へ]ボタンをクリックすると、
   “インスタンス作成ウィザード 監視対象コンピューター”画面が表示されます。
   ●BOM 7.0 を期限付きの評価版として使用する場合は、フィールドはブランクのまま、[次へ]ボタンをクリックします。
   ●評価版ライセンスでは、製品版と同じ機能を備えた評価版を 30 日間試用できます。
   評価期間終了後に引き続き BOM 7.0 を使用するためには、有効なライセンスキーを入力する必要があります。



4. ローカルコンピューターの監視をする場合、“監視対象コンピューター”フィールドで、“ローカルコンピューター”を選択します。

   ●“代理監視コンピューター”選択時には“コンピューター名”フィールドに、対象となるコンピューター名を入力します。

5. “インスタンス ID”フィールドに、BOM マネージャー等での表示名となるインスタンス ID を入力します。

   ●インスタンス ID は一意でなければならず、また後で変更することはできません。

   ●使用可能な文字は半角英数字、ハイフン、およびアンダーバーのみで、100 文字まで入力可能です。

6. [次へ]ボタンをクリックすると、“インスタンス作成ウィザード ログオン アカウント”画面が表示されます。

7. 監視に利用するアカウントを、ローカルシステムアカウントとユーザーアカウントのどちらかで、指定することができます。

   ●代理監視の設定の詳細は‘3 .3 代理監視の初期スタートアップ’を参照ください。

   ●ユーザーアカウントを指定すると、そのアカウントに自動的に“バッチジョブとしてログオン”権限が付与されます。

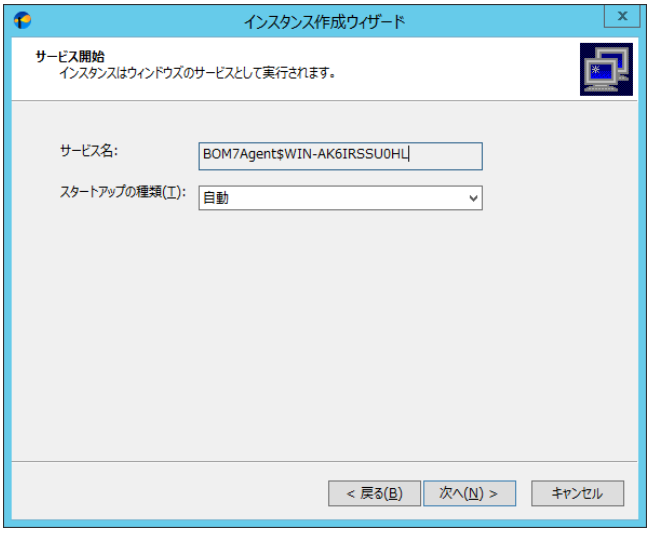
   ●ユーザーアカウントを指定する際は、UAC をオフにする必要があります。

   詳細については、‘3 .3 .3 代理監視設定が正しく監視できない場合のトラブルシューティング’の

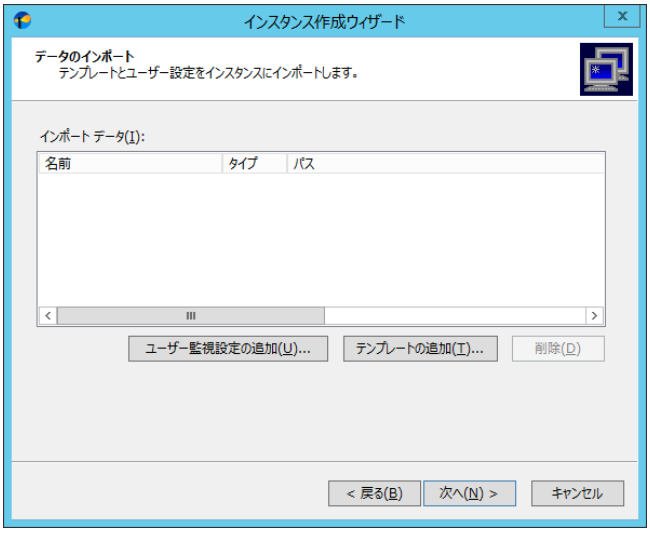
   ‘F.ユーザーアカウント制御(UAC)’を参照してください。

8. [次へ]ボタンをクリックすると、“インスタンス作成ウィザード サービス開始”画面が表示され、BOM 監視サービスのスタートアップの種類を選択できます。

   ●“自動”を選択すると、OS 起動時に BOM 監視サービスが自動で起動され、監視を開始します。



9. [次へ]ボタンをクリックすると、“インスタンス作成ウィザード データのインポート”画面が表示されるので、
監視設定のエクスポートファイルがある場合は、[ユーザー監視設定の追加..]ボタンをクリックし、
ファイルを選択してから[次へ]ボタンをクリックします。追加した監視設定は、該当するインスタンスにインポートされます。



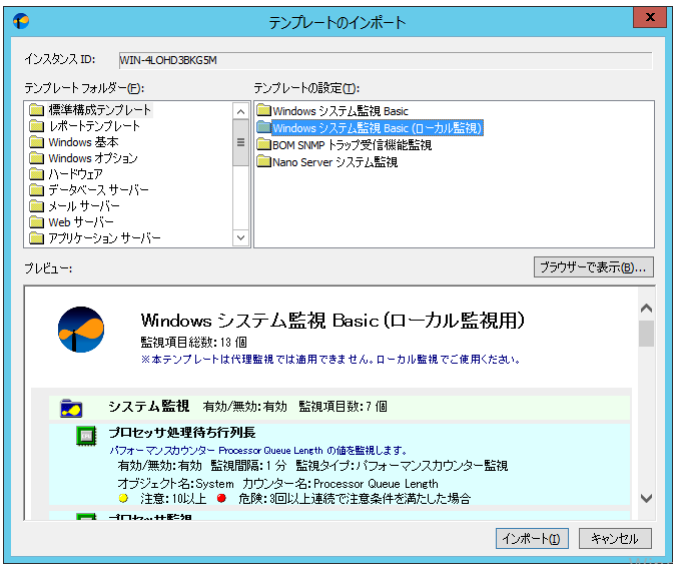
●BOM 7.0 の“監視設定のエクスポート”で生成した、拡張子が CAB のファイル（以降 CAB ファイル）を選択します。
“監視設定のエクスポート”の詳細は、‘3 .7 .2 監視設定のエクスポートとインポート’を参照ください。

●監視設定ファイルのファイル名は変更できますが、監視設定ファイルをインポートした際にエラーが出る場合には、
監視設定の CAB ファイルではない可能性があるため、正しい監視設定の CAB ファイルを選択してください。

●BOM 6.0 の“監視設定のエクスポート”で生成した CAB ファイルは、BOM 7.0 との互換性がないため、監視項目の
インポートを行うことはできません。

10. [テンプレートの追加..]ボタンをクリックすると、“テンプレートのインポート”画面が表示されます。
“テンプレート フォルダー”→“テンプレートの設定”の順で監視テンプレートを指定すると、下のプレビュー画面に
指定した監視テンプレートの監視設定内容が表示されます。
このプレビュー画面を見ることで、監視テンプレートのインポート前に監視設定内容を確認することができます。

●[ブラウザーで表示]ボタンをクリックすると、プレビュー画面で表示された情報をブラウザーで表示することができます。



11. [インポート]ボタンをクリックしてテンプレートの監視設定項目をインポートし、テンプレートのインストールを完了します。
    テンプレートのインストールは、設定完了後もインポートして追加することができます。
12. テンプレートをインストールすると現状のインスタンス ID がインスタンス作成ウィザード画面に表示されます。
    続けてインスタンスを追加する場合には[追加]ボタン、変更をする場合には[変更]ボタン、削除する場合には[削除]ボタンをクリックします。

以上でインスタンス作成の準備が整いました。設定したインスタンス ID とライセンス内容を確認ください。

[開始]ボタンをクリックするとインスタンス作成が開始されます。

●一度に追加できるインスタンスは 10 個までです。

●インスタンス作成終了時になんらかの原因で“中断”、“警告”が出ることがあります。

“中断”の場合には、再度インスタンス作成を実行してください。

“警告”の場合には、画面に出たメッセージに従い操作をしてください。

2.3 BOM for Windows Ver.7.0（ローカル）のプロパティ

“BOM for Windows Ver.7.0（ローカル）”配下のツリーの各インスタンスで共通で使用される
SMTP メールサーバーの設定、SNMP トラップ先の設定、アーカイブデータベースの設定および、Oracle 監視の接続設定は、
“BOM for Windows Ver.7.0（ローカル）”のプロパティ画面より実施します。

●この設定変更はすべてのインスタンスを停止してからでないと変更できません。

2.3.1 動作環境のインポート・エクスポート

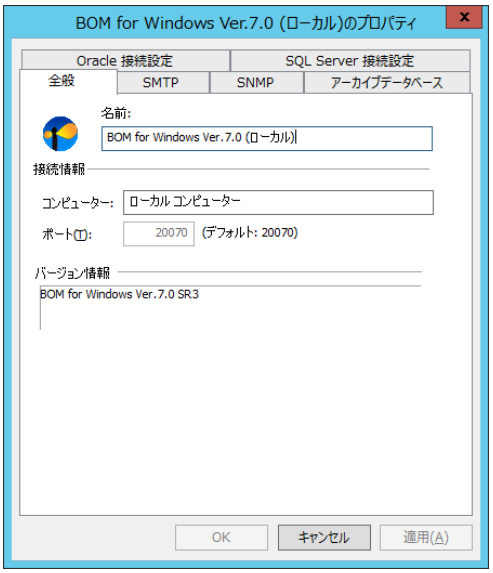
“BOM for Windows Ver.7.0（ローカル）”を右クリックすると、コンテキストメニューに“動作環境のインポート”と
“動作環境のエクスポート”があります。

●動作環境とは、“BOM for Windows Ver.7.0（ローカル）”の“プロパティ”画面で設定した、ポート番号、SMTP、SNMP、
アーカイブデータベース、Oracle データベースへの接続設定を示します。

これらの設定の保存は“動作環境のエクスポート”を使用し、保存した内容の復元は“動作環境のインポート”を使用します。

2.3.2 全般

1. BOM マネージャーで“BOM for Windows Ver.7.0（ローカル）”アイコンを右クリックし、コンテキストメニューの“プロパティ”を
クリックします。



2. コンピューターの監視区分、BOM ヘルパーサービスの待ち受けポート、バージョン情報が確認できます。

2 .3 .3 SMTP 情報の設定

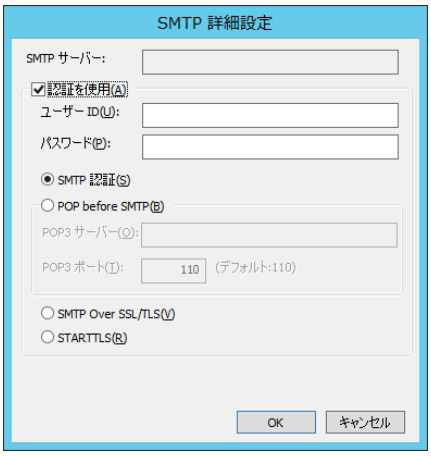
SMTP 情報は、BOM 7.0 の初期インストール時、あるいは必要に応じて設定を行う必要があります。

●SMTP 情報は、メール送信アクション項目を機能させるために入力する必要があります。

●SMTP 情報は、“SMTP サーバー1”と“SMTP サーバー2”の 2 台まで登録が可能です。

1. SMTP 情報を設定するには、BOM マネージャーで“BOM for Windows Ver.7.0（ローカル）”アイコンを右クリックします。
2. コンテキストメニューの“プロパティ”をクリックして、“プロパティ”画面の「SMTP」タブに移動します。

3. “SMTP サーバー1”フィールドの“サーバー”テキストフィールドに SMTP サーバーの IP アドレスあるいはホスト名を入力します。
4. “ポート”フィールドの SMTP サーバーの既定値のポートは“25”になっています。
   ポート番号を変更する場合には、“1”から“65535”までの整数を入力してください。
5. “送信元”フィールドには、送信者メールアドレスを入力します。
6. [詳細設定..]ボタンをクリックすると、“SMTP 詳細設定”画面が表示されます。
   ●認証方法を持つ SMTP サーバーに関しての認証指定が可能です。
   ●認証方法については SMTP 認証情報と POP before SMTP 認証のどちらかが指定できます。



7. SMTP 認証の場合、“SMTP 認証”ラジオボタンを選択してください。
   “ユーザーID”フィールドには、SMTP 認証で使用するユーザーID を、“パスワード”フィールドには SMTP 認証で使用するユーザーID のパスワードを入力してください。
   ●SMTP 認証については、CRAM-MD5 方式と PLAIN 方式と LOGIN 方式に対応しています。
8. POP before SMTP 認証の場合、“POP before SMTP”ラジオボタンを選択してください。
   “POP3 サーバー”フィールドには、POP3 サーバーの IP アドレスを入力します。
   “POP3 ポート”フィールドにはポート番号を、“1”～“65535”の間で入力してください。
   ●ユーザーID とパスワードを使用して POP before SMTP 認証を実行しますので、同時に指定してください。
   ●“POP before SMTP”ラジオボタンを選択すると、SMTP サーバーと同一名が“POP3 サーバー”フィールドにコピーされますが、変更可能です。

9. SMTP Over SSL/TLS 認証の場合、“SMTP Over SSL/TLS”ラジオボタンを選択してください。
   “ユーザーID”フィールドには、SMTP Over SSL/TLS 認証で使用するユーザーID を、“パスワード”フィールドには SMTP Over SSL/TLS 認証で使用するユーザーID のパスワードを入力してください。
10. STARTTLS 認証の場合、“STARTTLS”ラジオボタンを選択してください。
    “ユーザーID”フィールドには、STARTTLS 認証で使用するユーザーID を、“パスワード”フィールドには STARTTLS 認証で使用するユーザーID のパスワードを入力してください。

2.3.4 SNMP 情報の設定

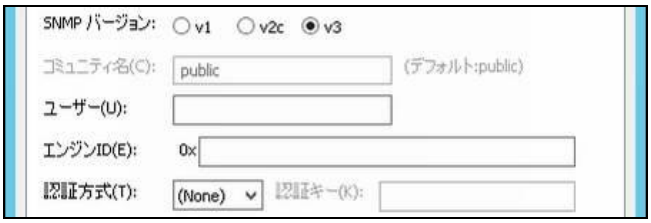
SNMP 情報の設定を行うことで、BOM 7.0 から SNMP トラップを送信することができます。
●BOM 7.0 の SNMP トラップアクション機能を用いて SNMP トラップを送信するためには、事前に SNMP 情報の設定が必要です。
●代理監視の場合には、代理監視先コンピューターではなく、代理監視元コンピューターの IP アドレスが SNMP マネージャーに通知されます。SNMP マネージャー側の設定を行う際には、代理監視元コンピューターの IP アドレスを登録してください。
●SNMP マネージャーを IPv6 アドレスで指定する場合、もしくはホスト名であっても IPv4 に変換できない場合、SNMP バージョンは“v2c”もしくは“v3”を選択する必要があります。
（“v1”は trap-agent-address フィールドが IPv6 アドレスに対応していないため、SNMP トラップ送信時にエラーとなります。）
（デュアルスタックで IPv6 優先の OS 設定下であっても、IPv4 アドレスに変換が出来れば問題はありません。）

1. SNMP トラップ情報を設定するには、BOM マネージャーで“BOM for Windows Ver.7.0（ローカル）”アイコンを右クリックします。

2. コンテキストメニューの“プロパティ”をクリックして、「SNMP」タブに移動します。

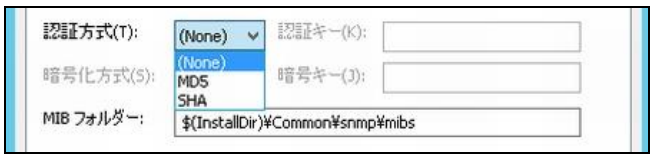
3. “マネージャー”フィールドに、SNMP トラップ送信先の SNMP マネージャーの“ホスト名”か“IP アドレス”を入力します。
4. “ポート”フィールドは既定値が 162 になっています。“1”～“65535”までの値を入力することができます。
5. “SNMP バージョン”フィールドは SNMP トラップのバージョンを選択します。既定値が“v1”になっています。
6. “コミュニティ名”フィールドは既定値が public になっています。お客様の環境に合わせて変更してください。

   ●SNMP バージョンにて“v3”ラジオボタンを選択した場合、V3 トラップ用のユーザー設定が必要になります。



7. “ユーザー”フィールドに、SNMP マネージャーで設定した“ユーザー名”と同じ値を入力します。
8. “エンジン ID”フィールドに、SNMP マネージャーで設定した“エンジン ID”と同じ値を入力します。

   ●BOM 7.0 の SNMP トラップでは、BOM 7.0 固有のエンジン ID はありません。
9. “認証方式”フィールドでは、“(None)”(認証方式を認証なし)、“MD5”、“SHA”から選択します。



10. “認証キー”フィールドでは、認証方式を指定した場合に設定できます。認証方式にて使用するキーを入力します。
11. “暗号化方式”フィールドでは、“(None)”(暗号化方式を平文)、“DES”、“AES”から選択します。

12.“暗号キー”フィールドでは、暗号化/復号する時に使用するキーを入力します。

2.3.5 アーカイブデータベースの設定

アーカイブサービスにてデータ蓄積を構成する場合に設定します。詳細は‘BOM for Windows Ver.7.0 アーカイブ ユーザーズ マニュアル’を参照ください。

2.3.6 「Oracle 詳細設定」タブについて

「Oracle 詳細設定」タブは Oracle オプション 7.0 をご使用時に必要になる設定です。

Oracle オプション 7.0 の監視対象となる Oracle データベースの接続情報を設定することができます。

詳細は、‘BOM Oracle オプション Ver.7.0 ユーザーズマニュアル’を参照ください。

2.3.7 「SQL Server 詳細設定」タブについて

「SQL Server 詳細設定」タブは SQL Server.オプション 7.0 をご使用時に必要になる設定です。

SQL Server オプション 7.0 の監視対象となる SQL Server インスタンスの接続情報を設定することができます。

詳細は、‘BOM SQL Server オプション Ver.7.0 ユーザーズマニュアル’を参照ください。

2.3.8 オンラインヘルプについて

下記のいずれかの手段で、BOM マネージャーのオンラインヘルプを起動することができます。

●キーボードのファンクションキー1<F1>を押下

●ツールバーのヘルプアイコンをクリック

●“BOM for Windows Ver.7.0（ローカル）”内のノードを右クリックし、コンテキストメニューの“ヘルプ”をクリック

集中監視コンソールについては‘BOM for Windows Ver.7.0 集中監視コンソール ユーザーズ マニュアル’を参照ください。

BOM アーカイブマネージャーについては BOM マネージャーと同じ起動方法です。

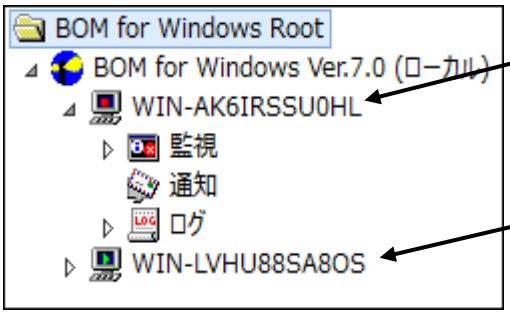
第3章 ローカル監視、代理監視、リモート接続

3 .1 インスタンスの解説

BOM 7.0 では“インスタンス”という概念を採用しております。監視設定を行う前に、“インスタンス”作成を行わなければいけません。
インスタンスには監視項目数の制限がありますが、同一コンピューターに複数設定できます。
また、BOM 7.0 を導入していないコンピューターに対して監視を行う代理監視については 1 インスタンスを使用し、独立した監視が実施されます。

3 .1 .1 インスタンスの監視開始と監視終了

1. インスタンスの監視開始とは、設定した監視項目を実際に動作させることです。
   インスタンスの“サーバーアイコン”を右クリックし、コンテキストメニューの“開始”をクリックします。
   インスタンスの監視が既に開始している場合、“開始”は灰色表示され、選択できるのは“停止”と“再起動”です。
   BOM マネージャーの“インスタンス管理”スコープペインで、インスタンスをクリックし、続いてリザルトペインの“開始”をクリックしてしてもインスタンスが開始します。



●インスタンスが停止すると、サーバーアイコンの上に赤い正方形が表示されます。BOM 7.0 の監視設定の変更を行う際は、インスタンスを停止する必要があります。

●インスタンスが開始すると、サーバーアイコンの上に緑の三角形が表示されます。
監視を行う際は、インスタンスを開始する必要があります。

2. インスタンスが 1 台のコンピューターに複数ある場合には、同時にすべてのインスタンスを開始、停止が可能です。
   “BOM for Windows Ver.7.0 （ローカル）”を右クリックし、コンテキストメニューの“全てのインスタンス監視開始”をクリックします。
   ●一斉に停止する場合には、“全てのインスタンス監視停止”をクリックします。
   ●設定した監視項目が監視を行うには、監視グループ・監視項目も有効にする必要があります。
   また、アクションが起動するには、アクションも有効になっている必要があります。既定値では、全て有効になっています。

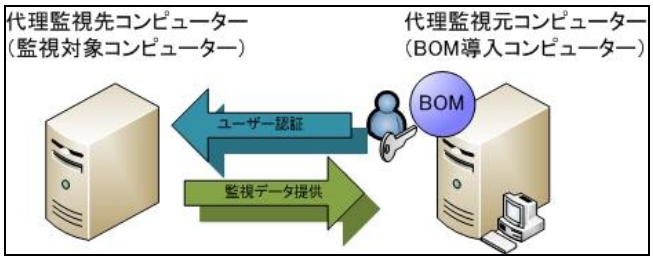
3 .2 監視の方法

3 .2 .1 ローカル監視

ローカル監視は、BOM 7.0 をインストールしたローカルコンピューターを監視対象とする監視のことです。
同一ローカルコンピューターに複数のローカル監視のインスタンス（ローカルインスタンス）を作成することができます。
1 インスタンスあたり 200 監視項目数までという制限がありますので、監視項目数が 200 を超える場合には、
別途 2 つめのローカルインスタンスが必要となります。
なお、インスタンスごとにライセンスが必要です。ローカル監視の設定は‘2 .2 初期スタートアップ’を参照ください。

3.2.2 代理監視

エージェントレス監視とも呼ばれる監視方法で、監視対象コンピューターに BOM 7.0 をインストールせずに
リモートコンピューターから監視を行うことができます。
BOM 7.0 を導入したローカルコンピューター上の代理監視用のインスタンス（代理監視インスタンス）を使用して、
ネットワークを介してリモートコンピューターの監視を実施します。



●代理監視インスタンスに対してもライセンスが必要です。
　必要な数のライセンスさえあれば、1 台の BOM 7.0 を導入したコンピューターから、ネットワーク上の複数の
　リモートコンピューターを代理監視にて監視することができます。
●代理監視の設定は‘3.3 代理監視の初期スタートアップ’を参照ください。

3.2.3 リモート接続

既に BOM 7.0 を導入済みのコンピューターとの接続にはスナップインの追加により、リモートコンピューターの BOM 7.0 と
接続ができ（リモート接続）、リモートコンピューター上の BOM の監視設定をローカルコンピューターで管理することができます。
●リモート接続は、BOM 導入済みのリモートコンピューターに対する接続です。リモート接続用にライセンスは不要です。
●リモート接続の設定や接続条件などは、‘3.4 リモート接続の初期スタートアップ’を参照ください。

3.3 代理監視の初期スタートアップ

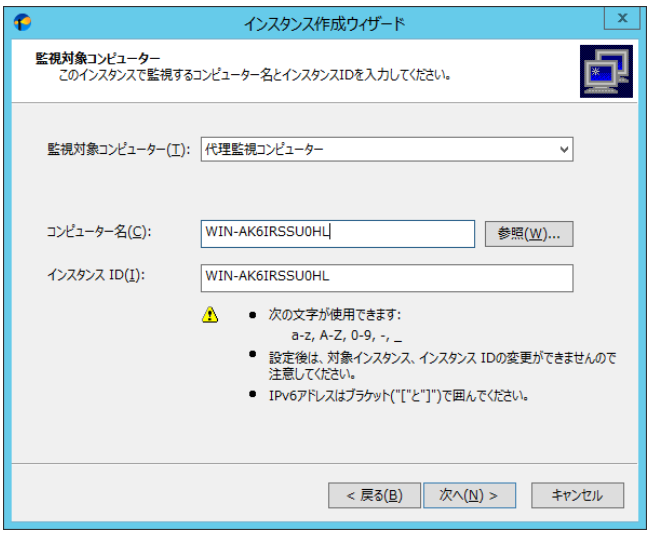
3.3.1 代理監視用インスタンスの作成手順

1. インストール時に作成したインスタンス以外にさらに代理監視インスタンスを追加作成するには、
　“BOM for Windows Ver.7.0（ローカル）”を右クリックし、コンテキストメニューの“新規作成”→“監視インスタンス...”の
　順にクリックします。
　または、“BOM for Windows Ver.7.0（ローカル）”をクリックした状態でメニューバーに移動し、“操作”→“新規作成”→
　“監視インスタンス...”の順にクリックします。
2. インスタンス作成ウィザードを開始します。[次へ]ボタンをクリックします。
　●インスタンスを追加する場合にはライセンスが必要です。

3. リモートインスタンスを作成する場合、下記“監視対象コンピューター”画面で“代理監視コンピューター”を選択する点を除き、インストールの後にインスタンスを作成する手順はローカルインスタンスを作成する場合と同じです。

●“コンピューター名”フィールドに、代理監視対象の“コンピューター名”もしくは、“IP アドレス”を入力します。

●“インスタンス ID”フィールドには、“コンピューター名”フィールドに入力した内容が“インスタンス ID”に反映されますが、他の名前に変えることもできます。



4. “ログオンアカウント”画面では、代理監視にて使用する“監視に利用するアカウント”を設定します。

“監視に利用するアカウント”は、代理監視元と代理監視先で同じユーザー名とパスワードを持ち、それぞれのコンピューターの管理者権限が必要です。“監視に利用するアカウント”はさまざまな条件を満たす必要があるために、必ず一度は‘3 .3 .2 代理監視設定のポイント’もしくは、‘3 .3 .3 代理監視設定が正しく監視できない場合のトラブルシューティング’を参照ください。

5. 以降は、ローカル監視インスタンスと同様に作成します。

3 .3 .2 代理監視設定のポイント

代理監視を行う場合に、ご注意いただきたい設定内容は下記の通りです。

A. 監視に利用するアカウントの準備

“監視に利用するアカウント”には、代理監視元と代理監視先の双方で利用できるユーザーアカウントが必要です。

●ワークグループユーザー認証の場合

双方のコンピューターに同一のアカウント名、パスワードを設定し、Administrators グループのメンバーとして追加します。

●ドメインユーザー認証の場合

任意のドメインアカウントを双方のコンピューターの Administrators グループのメンバーとして追加します。

B. 監視に利用するアカウントのローカルセキュリティポリシー

“監視に利用するアカウント”に対し、ローカルセキュリティポリシーの設定は基本的に必要ありません。

ただし、意図的に下記 2 つのポリシー設定に対し、既定値に与えられている“local service”と“network service”を削除した場合には、“監視に利用するアカウント”に対し下記 2 つのポリシーの許可を与えてください。

●プロセスレベルトークンの置き換え

●プロセスのメモリクォータの増加

C. 監視に利用するアカウントのその他特筆事項

●“監視に利用するアカウント”には、自動的に“バッチジョブとしてログオン”権限が付与されます。

●“監視に利用するアカウント”は、サービスアカウントとは異なりますのでご注意ください。

●“監視に利用するアカウント”のアカウント名やパスワードを代理監視先のコンピューターで変更した場合、
監視が失敗するようになり、監視項目のテストでもエラーが表示されます。
（その際、エラーメッセージは出力されず、エラーコードのみが表示されます。）

D. 認証、データ連携用ポートの開放

代理監視先コンピューターでは、ユーザー認証や監視データ取得のために、ポートを開放する必要があります。
Web で公開している下記サポート技術情報を参考にして、ポートを開放します。

サポート技術情報 000156 ‘代理監視で使用するポートについて’
http://www.say-tech.co.jp/support/bom-for-windows/bom50-3/index.shtml

E. 代理監視インスタンスの作成

代理監視先コンピューターを監視するための代理監視用インスタンスを、‘3 .3 .1 代理監視用インスタンスの作成手順’に従い作成します。

3 .3 .3 代理監視設定が正しく監視できない場合のトラブルシューティング

‘3 .3 .1 代理監視用インスタンスの作成手順’や‘3 .3 .2 代理監視設定のポイント’を元に代理監視インスタンスを作成しても正しく代理監視ができない場合には、下記の項目を確認してください。

A. 名前解決

インスタンス作成時に代理監視先コンピューターをコンピューター名で指定した場合、コンピューター名から IP アドレスに名前解決ができる必要があります。

●Ping、NSLookup などのコマンドにて、名前解決ができることを確認してください。

B. 通信遮断

代理監視元コンピューターと代理監視先コンピューターの経路上にファイアウォールが設置されている場合や、
代理監視先コンピューターの OS の Windows ファイアウォールが有効になっている場合には、
‘3 .3 .2 代理監視設定のポイント’の項目‘D.認証、データ連携用ポートの開放’で解説した通信をブロックしている可能性があります。

●経路上のファイアウォールが必要な通信をブロックしていないか確認してください。

●Windows ファイアウォールが必要な通信をブロックしていないか確認してください。

C. Remote Registry サービス

代理監視先コンピューターの監視データを取得するためには代理監視先コンピューターにて Remote Registry サービスが開始している必要があります。

●サービスが開始していない場合には開始してください。

●スタートアップの種類が“無効”または“手動”になっている場合には、“自動”に変更してください。

D. Guest 認証設定

代理監視先コンピューターのセキュリティポリシーにて、

ポリシー名“ネットワークアクセス:ローカルアカウントの共有とセキュリティモデル”の設定値が“Guest のみ”に設定されている場合、代理監視元コンピューターからの接続が Guest アカウントとして扱われ、管理者権限を取得できません。

●“ネットワークアクセス:ローカルアカウントの共有とセキュリティモデル”の設定値を“クラシック”に変更してください。

E. サービスアカウントの特権

代理監視元コンピューターにて動作する BOM 監視サービスは、“サービスのログオンアカウント”として“ローカルシステムアカウント”を設定しています。

“ローカルシステムアカウント”は、既定で特権“プロセス レベル トークンの置き換え”と“プロセスのメモリ クォータの増加”を保有しており、BOM 7.0 ではその特権を使用している関係上、“サービスのログオンアカウント”を“ローカルシステムアカウント”以外への変更や、“ローカルシステムアカウント”から特権を削除した場合には、代理監視にて不具合が発生します。

●BOM 監視サービスの“サービスのログオンアカウント”が、特権“プロセス レベル トークンの置き換え”と“プロセスのメモリ クォータの増加”を保有するように構成してください。

●BOM 7.0 の“監視に利用するアカウント”と OS の“サービスのログオンアカウント”は異なり、代理監視先コンピューターに接続するのは“監視に利用するアカウント”になりますのでご注意ください。

F. ユーザーアカウント制御（UAC）

Windows Server 2008 以降の OS では、既定でユーザーアカウント制御（UAC）が有効になっています。

その場合、ワークグループユーザー認証では、代理監視先コンピューターの管理者権限を取得できません。

●Web で公開している下記サポート技術情報を参考にして、UAC の対処を行います。

サポート技術情報 000188 ‘代理監視にてリモートコンピューターを監視する場合’

http://www.say-tech.co.jp/support/bom-for-windows/post-55/index.shtml

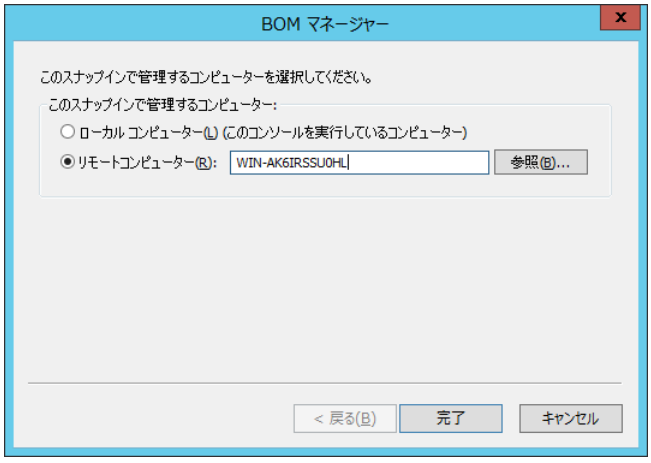
3 .4 リモート接続の初期スタートアップ

既に BOM 7.0 を導入済みのコンピューターとの接続にはスナップインの追加により、リモートコンピューターと BOM 7.0 同士で接続ができ(リモート接続)、リモートコンピューター上の BOM 7.0 の監視設定をローカルコンピューターで参照、あるいは変更することができます。

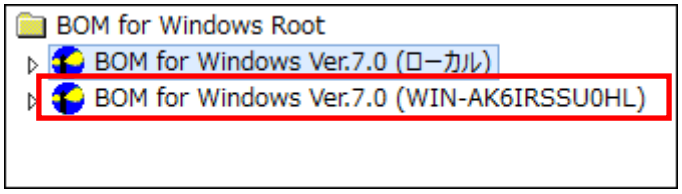
●BOM 7.0 アーカイブログビューアーや BOM 7.0 アーカイブマネージャーのスナップインの追加も同仕様です。

1. メニューバーに移動して、“ファイル”→“スナップインの追加と削除…”をクリックすると、“スナップインの追加と削除”画面が表示されます。

2. “スナップインの追加と削除”画面で“BOM 7.0 マネージャー”をクリックした後に[追加..]ボタンをクリックすると、“BOM マネージャー”画面が表示されます。
3. “BOM マネージャー”画面で、“リモートコンピューター”ラジオボタンを選択してから、[参照..]ボタンをクリックして、該当監視対象コンピューターを選択するか、直接コンピューター名を入力します。また、IP アドレスで指定する事も可能です。



4. [完了]ボタンをクリックすると“スナップインの追加と削除”画面に戻ります。
5. “スナップインの追加と削除”画面で[OK]ボタンをクリックして、“スナップインの追加と削除”画面を閉じると、BOM マネージャーのスコープペインに、追加した接続ノードが表示され、末尾に選択したリモートコンピューターの名前が表示されます。



リモートコンピューターに接続するには、リモートコンピューター上の BOM ヘルパーサービスを開始する必要があります。

リモートコンピューターに管理者モードでログインした場合は、BOM マネージャーを使用して監視設定変更を行うことができます。

監視設定変更内容は、リモートコンピューターの BOM 7.0 の監視設定に反映されます。

●“BOM for Windows Ver.7.0 （ローカル）”のスナップインと、前段で追加したリモートスナップインの間、または、
二つのリモートスナップインの間で、インスタンスあるいは監視設定を、ドラッグ＆ドロップで移動させることはできません。

●リモートコンピューター上の BOM ヘルパーサービスを開始するにはリモートコンピューター上の BOM コントロールパネルで
BOM ヘルパーサービスを起動する必要があります。詳細は‘第 10 章 BOM コントロールパネル’を参照ください。

●リモート接続の設定を行い“接続”した場合に、“接続できません（TCP エラー）”が出る場合にはリモートコンピューターとの通信が
できていませんので、ネットワーク環境や Windows ファイアウォールの設定などを再度ご確認ください。

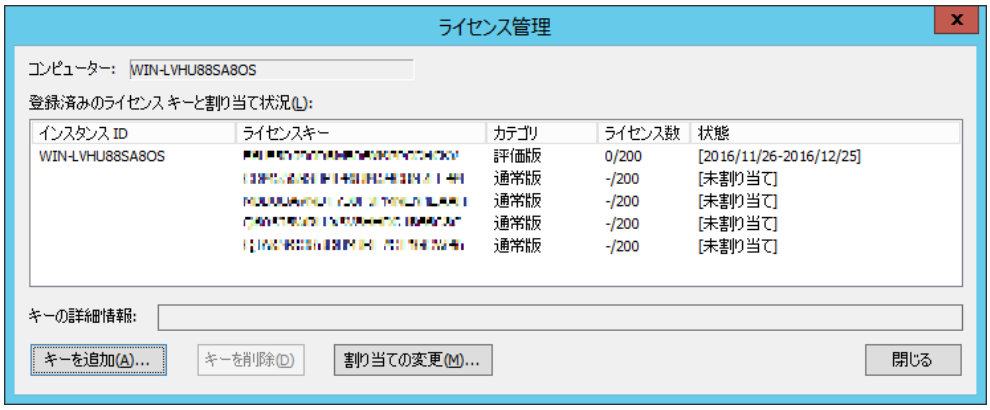
●“アクセス制限のため BOM7Helper 接続が拒否されました”のエラーが出る場合には、リモート接続先の BOM ヘルパーサービスの
“リモートアクセスの範囲”が制限されており、リモートアクセス範囲外（異なるセグメント間など）から接続しようとしたことが原因です。
詳細は、‘10 .3 .2 BOM ヘルパーサービス設定’より、“リモートアクセスの範囲”の設定値をご確認ください。

3 .5 ライセンス管理

インスタンスの作成には必ずライセンスキーが必要になります。ライセンスキーをインスタンスに割り当てて初めてインスタンスでの監視が可能になります。どのライセンスキーをどのインスタンスに割り当てているか、あるいは現在登録しているライセンスキーを違うインスタンスに割り当て直すなどの、ライセンス管理を行うのがライセンスマネージャーです。

ライセンスマネージャーは、BOM マネージャーの“BOM for Windows Ver.7.0 （ローカル）”を右クリックし、コンテキストメニューの“ライセンスマネージャー”をクリックして起動します。

※　ライセンスの操作を行う際は、対象のスナップイン（上記の場合、「BOM for Windows Ver.7.0 （ローカル）」）配下に存在するすべてのインスタンスの監視を停止させる必要があります。
　　監視実行中のインスタンスが存在する場合、ライセンス管理画面のボタンがグレーアウトし、変更などの操作ができません。



A. ライセンス管理画面

1. コンピューター

   どのコンピューターの情報かを示します。

2. 登録済みのライセンスキーと割り当て状況

   インスタンス ID とライセンスキー、そしてカテゴリ、ライセンス数、状態を表示します。

   ●“インスタンス ID”

   選択したコンピューターに登録したインスタンス ID をすべて表示します。

   ●“ライセンスキー”

   選択したコンピューターに登録されているライセンスキーをすべて表示します。

   ●“カテゴリ”

   登録されているライセンスキーの種類が“通常版”もしくは“評価版”と表示されます。

   ●“ライセンス数”

   1 インスタンス当たりに設定できる監視項目数の上限は 200 項目です。

   監視項目数は、n/200 の形式で表示されます。

   n の部分は、現在同一インスタンス ID に作成した監視項目数の合計が表示されます。

（12/200と表示される場合、最大200項目まで作成できるうち、12項目まで作成していることを示します。）

現状の監視グループ数、監視項目数、アクション項目数、通知項目数は‘3 .6 .2「情報」タブ’で確認することができます。

●“状態”

“未割り当て” ・・・ ライセンスキーがまだインスタンスIDに割り当てられていないことを示します。

“期限切れ” ・・・ ライセンスキーが評価版用のライセンスキーで期限が切れたことを示します。

“オプション” ・・・ 基本ライセンスキーかオプションライセンスキーかを示します。

“yyyy/mm/dd – yyyy/mm/dd” ・・・ 評価版のライセンスキーの使用期間を示します。

（yyyy:西暦年号、mm:月、dd:日を表します。）

3. キーの詳細情報

ライセンスキーにフォーカスを当てると“キーの詳細情報”フィールドに選択したキーの説明が表示されます。

オプションのライセンスキーを選択するとそのオプションが何のオプションかを表示します。

4. キーを追加

[キーを追加]ボタンをクリックすると、“ライセンスキー追加画面”が表示されます。

5. 割り当ての変更

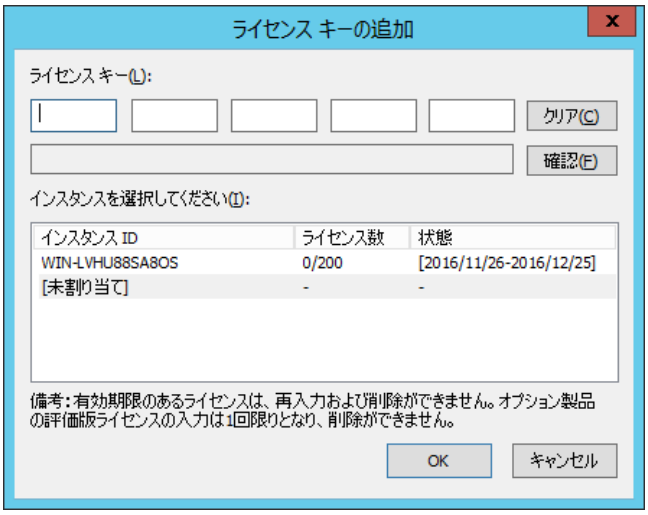
[割り当ての変更]ボタンをクリックすると、“ライセンス割り当ての変更画面”が表示されます。

B. ライセンス キーの追加画面

“ライセンス キーの追加”画面では、インスタンスの作成前にライセンスキーを登録しておくことが可能です。

なお、ライセンスキーはBOM本体及びBOMオプション製品、それぞれ別種です。

オプション製品のライセンスキー登録方法はオプション製品それぞれのユーザーズマニュアルをご参照ください。



1. ライセンスキーを入力します。

誤ったライセンスキーを入力した場合には[クリア]ボタンですべて空白に戻すか、間違った文字のところを変更してください。

2. [確認]ボタンをクリックすると、入力したライセンスキーが正しいかを確認することができます。

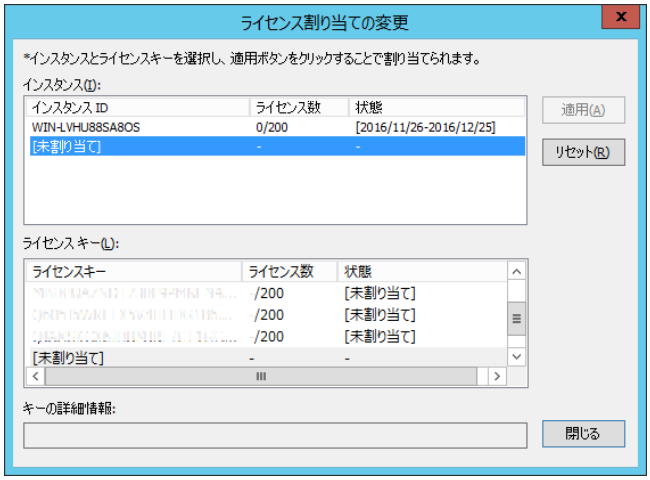
3. インスタンスに割り当てる場合には、割り当てるインスタンスIDを選択します。

●割り当てるインスタンスがなければ“未割り当て”を選択します。

●すでに割り当てているインスタンス ID に対して新規に追加したライセンスキーを割り当てると既存のライセンスキーは“未割り当て”になり、新規のライセンスキーが指定したインスタンス ID に割り当てされます。

●既に登録してあるライセンスキーを再度[OK]ボタンをクリックして登録しようとした場合、エラーが出力され登録はできません。

C. ライセンス割り当ての変更画面



1. 割り当てる“インスタンス ID”を選択し、“ライセンスキー”の一覧から割り当てたいライセンスキーを選択します。
2. [適用]ボタンをクリックすると割り当てます。
3. [リセット]ボタンをクリックすると、現在のすべてのインスタンス ID とライセンスキーの割り当てを解除します。

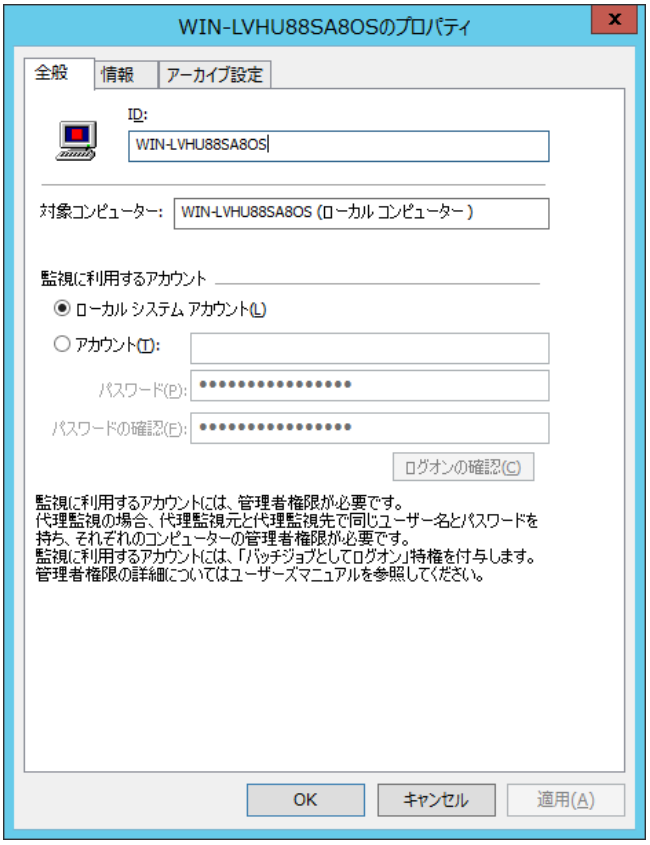
●既に割り当てているインスタンス ID に対しても未割り当てのライセンスキーの割り当ては可能です。
また、現在割り当てされているライセンスキーを異なったインスタンス ID に割り当てることも可能です。

●[リセット]ボタンをクリックし、すべてのライセンスキーがインスタンス ID から解除されても、監視設定が消えることはありません。
ただし監視を開始することはできません。また、監視設定を変更することもできません。
BOM マネージャーのインスタンスの監視起動のメニューがグレイアウトされ、インスタンス ID にライセンスキーを割り当てるまでアクティブになりません。

3 .6 インスタンスのプロパティ

インスタンスの“プロパティ”画面は、BOM マネージャーのインスタンスを右クリックし、コンテキストメニューの“プロパティ”をクリックして表示させます。

3 .6 .1 「全般」タブ



1. “ID”

   インスタンスの ID が表示されます。

2. “対象コンピューター”

   監視対象のコンピューターの名前が、ローカルコンピューターの場合は、“コンピューター名（ローカルコンピューター）”、代理監視コンピューターの場合は、“コンピューター名（代理監視コンピューター）”と表示されます。

3. “監視に利用するアカウント”

   監視に利用するアカウントを、“ローカル システム アカウント”と“ユーザーアカウント”から指定することができます。

   ●“ローカル システム アカウント”ラジオボタンを選択

   ローカルコンピューターのアカウントを用いて対象コンピューターにログオンします。

   ●“アカウント”ラジオボタンを選択

   任意のアカウントを用いて対象コンピューターにログオンします。

   この場合、そのアカウントにバッチジョブとしてのログオン権限が付与されます。

4. [ログオンの確認]ボタン

ログオンに成功した場合 ： “ログオンに成功しました”というダイアログが表示

失敗した場合 ： “ログオンに失敗しました”というダイアログが表示

●[ログオンの確認]ボタンはローカルコンピューターへのログオンの確認です。

●Windows Server 2008 以降を監視する場合でユーザーアカウントを指定する際は、UAC をオフにする必要があります。

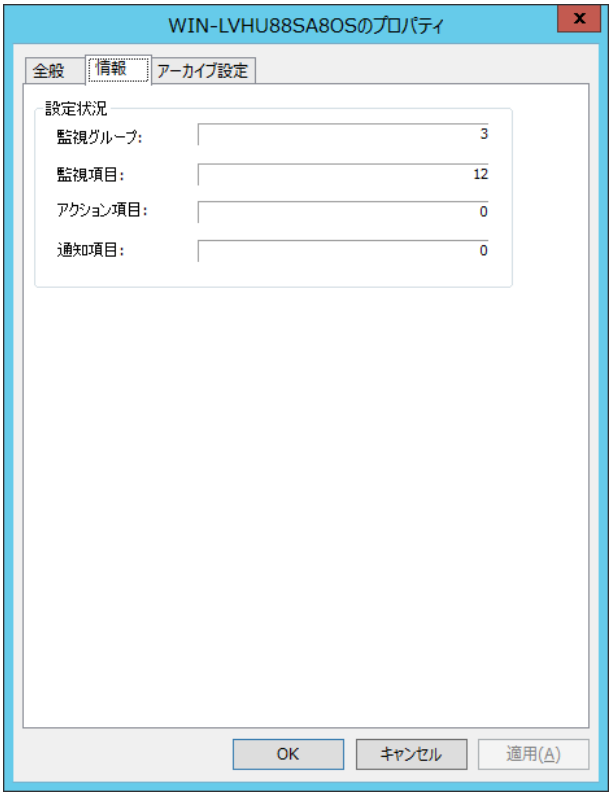
詳細は、‘3 .3 .3 ‘F.ユーザーアカウント制御（UAC）’を参照ください。

3 .6 .2 「情報」タブ

インスタンスの各種設定項目の数を示します。

1 インスタンス当たりの監視項目とアクション項目と通知項目を合わせた項目数の上限は 10000 項目です。

1 インスタンスに対して、10000 項目より多くの項目を設定することはできません。



1. “監視グループ”

現状の監視グループの数を示します。

2. “監視項目”

現状の監視項目の数を示します。1 インスタンスに設定できる監視項目数の上限は 200 項目です。

3. “アクション項目”

現状のアクション項目の数を示します。1 監視項目に設定できるアクション項目の上限は 99 項目です。

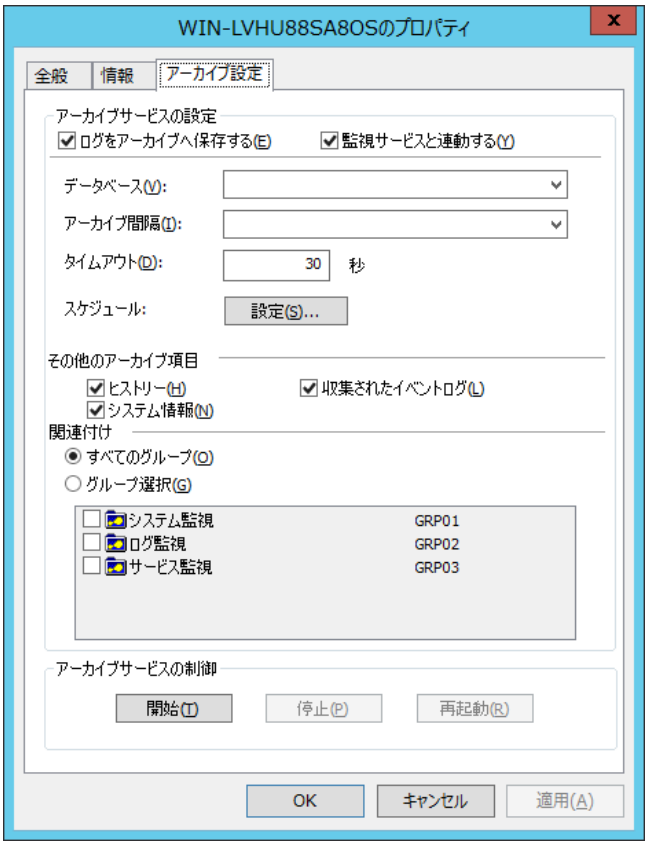
4. “通知項目”

現状の通知項目の数を示します。1 インスタンスに設定できる通知項目数の上限は 99 項目です。

3 .6 .3 「アーカイブ設定」タブ

アーカイブサービスの設定を行います。

タブを表示した段階で、アーカイブサービスの登録を行います。詳細は‘BOM for Windows Ver.7.0 アーカイブ ユーザーズ マニュアル’を参照ください。



1. “ログをアーカイブへ保存する”

   チェックボックスにチェックを入れると、ログをアーカイブデータベースに保存します

2. “監視サービスと連動する”

   監視サービスに合わせて、アーカイブサービスが起動・停止します。この機能は BOM マネージャーにより、監視サービスを開始する場合のみ機能するものです。BOM コントロールパネル及びサービスマネージャーから監視サービスを起動しても、アーカイブサービスは連動して開始しませんのでご注意ください。

3. “データベース”

   アーカイブデータベースを指定します。

   指定するアーカイブデータベースはアーカイブデータベースの設定で追加したリストから選択します。

   詳細は‘BOM for Windows Ver.7.0 アーカイブ ユーザーズ マニュアル’を参照ください。

4. “アーカイブ間隔”

   アーカイブデータベースにデータを送る間隔を、“30 分”、“1 時間”、“1.5 時間”、“2 時間”、“3 時間”、“4 時間”、“6 時間”、“8 時間”、“0.5 日（12 時間）”、“1 日”から指定できます。

5. “タイムアウト”

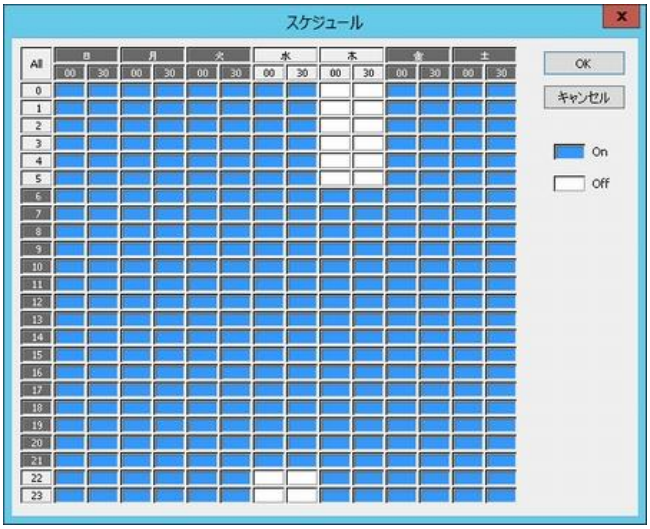
アーカイブデータベースにデータを蓄積する際のタイムアウト時間を指定します。

“0”～“999999999”秒を指定できます。“0”を指定した場合には、実行完了まで無制限に待機します。

6. “スケジュール”

「アーカイブ設定」タブ→[設定…]ボタンをクリックすると、“スケジュール画面”が表示されます。縦軸は“時間”、横軸は“曜日”と“毎時 00 分”、“毎時 30 分”のいずれかを指定します。青色がオン状態、白色がオフ状態です。

●下記は、毎週水曜日の 22 時から翌日木曜日の 6 時まで定期メンテナンスなどでアーカイブデータベースを停止させているため、該当するインスタンスからアーカイブデータベースへのデータ送信を Off（無効）にした例です。



7. “その他のアーカイブ”

項目監視ノード配下の監視データ以外のアーカイブデータの選択を行います。

ログノード配下の“ヒストリー”と“収集されたイベントログ”を選択することができます。

8. “関連付け”

●“すべてのグループ”ラジオボタンを選択した場合

すべての監視グループをアーカイブデータベースに保存します。

●“グループ選択”ラジオボタンを選択した場合

監視グループの一覧が表示されるため、アーカイブ対象としたい監視グループのチェックボックスにチェックを入れることで、該当する監視グループをアーカイブデータベースに保存します。

9. アーカイブサービスの制御

●[開始]ボタン

アーカイブサービスを開始します。

●[停止]ボタン

アーカイブサービスを停止します。

●[再起動]ボタン

アーカイブサービスを再起動します。

3.7 インスタンスのコンテキストメニュー

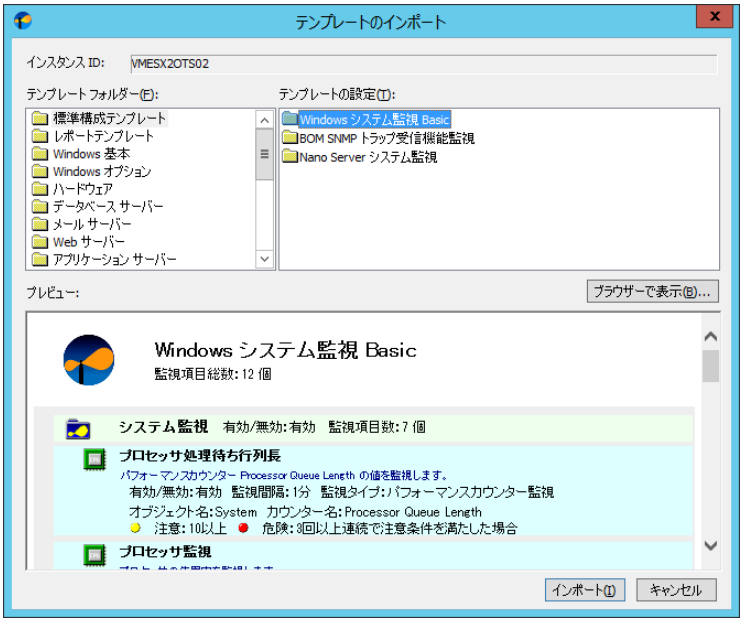
BOM マネージャーのインスタンスを右クリックしたときに表示される下記のコンテキストメニューについて解説します。

3.7.1 テンプレートのインポート

BOM 7.0 では、あらかじめよく使う監視項目が含まれたテンプレートをインストールできます。

それらはインポートするだけですぐに利用可能です。

“テンプレートのインポート”を実行すると、次のようなテンプレートを選択する“テンプレートのインポート”画面が表示されます。



1. “テンプレートフォルダー”

   種類ごとにまとめられた監視テンプレートが保存されたフォルダーを選択します。

2. “テンプレートの設定”

   監視テンプレートを選択します。

3. “プレビュー”

   選択した監視テンプレートに収録された監視項目の情報を表示します。

4. [ブラウザーで表示]ボタン

   プレビュー画面で表示された情報をブラウザーで表示します。

5. [インポート]ボタン

   クリックすると、“テンプレートのインポート”画面が閉じ、選択したテンプレートがインポートされ、スコープペインの“監視”にそのテンプレートが追加されます。

●インポートする項目数は 1 インスタンス当たり 200 項目以上の監視項目数があってもインポートはできますが、監視サービスを起動することができないため、インスタンス当たりの項目数を 200 項目以下にしてください。
1 インスタンス当たりの総項目数の確認については、‘3 .6 .2 「情報」タブ’で参照することができます。

●BOM 6.0 用に公開されている監視テンプレートを BOM 7.0 に適用した場合、BOM 7.0 と BOM 6.0 に互換性がないため、監視項目のインポートを行うことはできませんのでご注意ください。

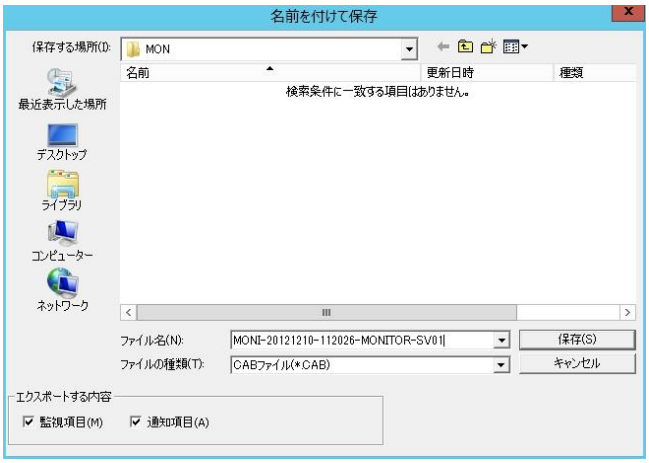
3 .7 .2 監視設定のエクスポートとインポート

BOM 7.0 インスタンスの設定を行った後に、監視設定のエクスポート機能を使ってインスタンス内の設定値を CAB ファイルに出力することができます。
同じような監視を行いたいインスタンスを追加する際には、エクスポートした設定値の CAB ファイルを監視設定のインポート機能を使って取り込むことで、設定値を複製して監視を直ぐに開始することができます。

●設定値の一部は、監視対象コンピューターの情報に合わせて変更する必要があります。

A. 監視設定のエクスポート

1. BOM マネージャーのスコープペインにて、監視設定をエクスポートしたいインスタンスを選択し、右クリックします。
2. コンテキストメニューの“設定のエクスポート”をクリックし、CAB ファイルの保存先フォルダーとファイル名を指定します。
   “監視項目”チェックボックスにチェックを入れることで、監視グループ、監視項目、アクション項目をエクスポート対象に含めることができます。“通知項目”チェックボックスにチェックを入れることで、通知項目をエクスポート対象に含めることができます。



フォルダー　：　<BOM 7.0 インストールフォルダー>¥BOMW7¥DAT¥MANAGER¥MON¥

ファイル名　：　MONI-yyyyMMdd-hhmmss-<インスタンス名>.CAB

（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

3. [保存]ボタンをクリックすることで、手順 1.で指定したインスタンスの設定値を手順 2.の条件で CAB ファイルに出力することができます。

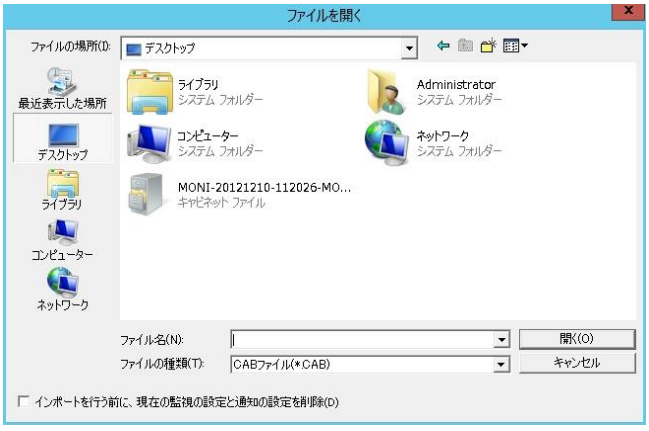
●エクスポート先のフォルダーは必ず、ログオンユーザーが書き込み権限を持つフォルダーを指定してください。
書き込み権限のないフォルダーあるいはプロテクトにより書き込めないメディアにエクスポートすると
“指定された保存場所には書き込みできません。ドライブの種別・アクセス権の有無を確認してください。”という
エラーになります。

B. 監視設定のインポート

エクスポートした設定値をインポートするには、設定値をインポートする対象のインスタンスが必要です。
新しいインスタンスの作成の詳細については、‘第 3 章ローカル監視、代理監視、リモート接続’を参照ください。

1. BOM マネージャーのスコープペインにて、監視設定をインポートしたいインスタンスを選択し、右クリックします。
2. コンテキストメニューの“設定のインポート”をクリックし、インポートする設定値の CAB ファイルを選択します。

●“インポートを行う前に、現在の監視の設定と通知の設定を削除”チェックボックスについて
チェックボックスにチェックを入れた場合：
インポート先のインスタンスの監視グループ、監視項目、アクション項目、通知項目の設定値をすべて削除した上で、新しい設定値をインポートします。この際、監視グループ ID はエクスポート時から変更せずインポートします。
チェックボックスのチェックを外した場合：
インポート先のインスタンスの監視グループ、監視項目、アクション項目、通知項目の設定値を残し、インポートする設定を追加します。事前に作成した設定値を残した上で設定値をインポートする場合や、複数の CAB ファイルをインポートする場合には、本チェックボックスからチェックを外してください。
この際、既存の監視設定と監視グループ ID が重複する可能性があるため、インポートした監視グループの ID には空いている ID を頭から割り振る動作をします。



3. [開く]ボタンをクリックすることで、手順 1.で指定したインスタンスに対し手順 2.の条件で設定値をインポートすることができます。

●あるインスタンスで監視設定した内容をエクスポートし、異なるインスタンスにインポートした場合、あるいは同一のインスタンスでもハードウェア環境、ソフトウェア環境を変更した後インポートする場合には、監視項目やアクション機能が失敗することがあります。その場合には、監視対象コンピューターに適合した監視設定に変更してください。

●インポートする項目数は 1 インスタンス当たり 200 項目以上の監視項目数があってもインポートはできますが、監視サービスを起動できませんので、1 インスタンス当たりの項目数を 200 項目以下にしてください。
1 インスタンス当たりの監視項目数の確認については、‘3 .6 .2 「情報」タブ’で参照することができます。

●オプション製品である、Linux インスタンス、VMware インスタンスでエクスポートした監視設定は、同じ製品にのみインポートが可能です。異なる製品にインポートを試みた場合には、警告メッセージが表示されます。

3 .7 .3 監視設定一覧の出力

監視インスタンス毎に監視グループ／監視項目／アクション項目／通知項目の監視設定の一覧を、XML 形式または CSV 形式のファイルで出力します。出力形式はファイルの種類から変更できます。
このファイルは、XML 形式、CSV 形式の読み込めるアプリケーション（Microsoft Excel 等）で読み込むことができます。

● ファイルに出力される内容

・インスタンス情報: インスタンス名
・監視グループ情報: グループ名、グループ ID、有効/無効、スケジュール設定の有無
・監視項目情報: 項目名、項目 ID、有効/無効、監視間隔、判定条件[注意]、判定条件[危険]
・アクション項目情報: 項目名、項目 ID、有効/無効、実行条件（※1）、実行頻度（※2）
・通知項目情報: 項目名、項目 ID、有効/無効、実行条件（※3）、実行頻度（※2）

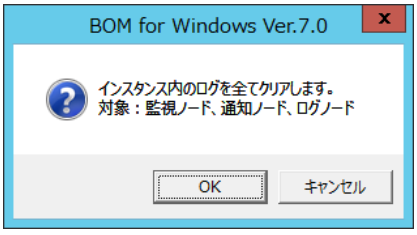
※1 N:正常、W:注意、C:危険、F:失敗
※2 -（ハイフン）:毎回または回数指定、O:変化時のみ
※3 監視結果による通知の場合 N:正常、W:注意、C:危険、F:失敗
アクション実行結果による通知の場合 S:成功、E:エラー、F:失敗

● 出力ファイル

既定値は以下の通りです。
・格納フォルダー:<BOM 7.0 インストールフォルダー>¥BOMW7¥DAT¥MANAGER¥LIST
・ファイル名:LIST-yyyyMMdd-hhmmss-<インスタンス名>.xml
（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

3 .7 .4 すべてのログのクリア

“すべてのログのクリア”をクリックすると、下記のメッセージが表示され、インスタンス内の監視及び通知、ログのログデータがすべて削除されます。



3.7.5 削除

“削除”ではインスタンスを削除できます。

対象のインスタンス情報、監視設定、ログなど、すべての情報が削除されます。

3.7.6 プロパティ

“プロパティ”では、監視アカウントの変更が可能です。

詳細は‘3.6 インスタンスのプロパティ’を参照ください。

3.8 メニュー一覧

BOM マネージャーはマイクロソフト管理コンソール（MMC）のスナップインとしてシステムにインストールされます。

ここでは MMC に共通のメニューについて解説します。

A. 開く

新しい MMC ファイル（*.msc）を開きます。

B. 列の追加と削除

リザルトペインに表示される列を追加、削除するダイアログを表示します。

C. 大きいアイコン

リザルトペインに表示されるアイコンを大きいアイコンにします。

D. 小さいアイコン

リザルトペインに表示されるアイコンを小さいアイコンにします。

E. 一覧

リザルトペインに表示されるアイコンを小さいアイコンで一覧表示にします。

F. 詳細

リザルトペインの表示を詳細表示にします。既定値ではこの状態です。

G. カスタマイズ

MMC およびスナップインの各要素（ツールバーなど）の表示をオン・オフすることが可能です。

H. ここから新しい画面

スコープペインで選択中の項目をルートにして、新しい画面を表示します。

I. 新しいタスクパッド表示

新しいタスクパッド表示ウィザードが起動します。

このウィザードではリザルトペインに表示される新しいタスクパッド（項目のリストとそれに対するタスクの表示されるページ）を追加することができます。

J. タスクパッド表示の編集

リザルトペインに表示されている現在のタスクパッド表示を編集できます。

K. タスクパッド表示の削除

リザルトペインに表示されている現在のタスクパッドを削除できます。

L. 削除

項目（監視インスタンス）を削除します。

削除を選択すると、削除しても問題ないかの確認ダイアログが出力されます。

M. 最新の情報に更新

リザルトペインの表示を最新の情報に更新します。

3 .8 .1 インスタンスステータスの表示

監視項目すべての“ステータス”、“前回の値”、“前回の実行時刻”、“前回の実行時間”、“前回の結果”、“アクション”の有無を表示します。

“インスタンスステータス”画面は“監視”ノードを右クリックし、コンテキストメニューの“インスタンスステータスの表示”をクリックします。

1. “失敗”、“危険”、“注意”、“正常”の各チェックボックスにチェックを入れると、手順 2.または手順 4.の操作を行うことで“インスタンスステータス”画面に表示される監視項目を、ステータスに該当する監視項目のみに絞込むことができます。
   ●ステータス“なし”の監視項目は、常に表示されます。
2. “自動更新”チェックボックスにチェックを入れると、手順 1.の条件で“インスタンスステータス”画面の表示を“30 秒間隔”で自動更新します。
3. “インスタンスステータス”画面に表示されている監視項目をクリックした状態で[ログの表示]ボタンをクリックすると、該当する監視項目の“ログビューアー”画面を表示させることができます。
   監視項目の“ログビューアー”画面の詳細は、‘5 .8 .1 ログの表示’を参照ください。
4. [更新]ボタンをクリックすると、手順 1.の条件で“インスタンスステータス”画面の表示を更新します。
5. [閉じる]ボタンをクリックすると、“インスタンスステータス”画面を閉じます。

3.8.2 一覧のエクスポート

一覧のエクスポートを行いたい各ノードを左クリックで選択後に右クリックし、コンテキストメニューの“一覧のエクスポート”をクリックします。本機能はインスタンスノード（BOM for Windows Ver.7.0 （ローカル））配下のすべてのノードで起動できます。

エクスポートされる内容は、BOM マネージャーの選択したノードのリザルトペインに表示する内容をテキストファイルにしたものです。

●“監視”ノードを指定（右クリック）した場合にエクスポートできる項目

“名前”、“ID”、“有効/無効”、“スケジュール”、“前回実行時刻”、“正常項目数”、“注意項目数”、“危険項目数”、“失敗項目数”、“未監視項目数”、“監視項目合計”）

1. リストをエクスポートするには、リストをエクスポートしたい該当インスタンスノード以下（インスタンスノードも含む）のいずれかのノード（例：“監視”、“監視グループ”、“各監視項目”、“各アクション”、“通知”、“ログ”等）を右クリックします。
2. コンテキストメニューの“一覧のエクスポート...”をクリックすると、“一覧のエクスポート”画面が表示されます。
3. ファイルを保存するフォルダーを選択して、ファイルに名前を付けます。
4. [保存]ボタンをクリックします。

第4章 監視グループ

4 .1 監視グループの解説

監視グループは、サーバーの監視を分類して管理する方法の 1 つです。
複数の監視グループを必要とする状況として考えられるのは、下記のようなケースです。

●監視項目を目的別に整理するために、監視グループを Windows のフォルダーのように使用
1 台のサーバー上で社内のさまざまな業務アプリケーションが稼働しており、アプリケーションによってシステム管理者が異なるため、システム管理者ごとに監視グループを設定し、設定変更時などのメンテナンス性を高めたい

例:
経理システムのバージョンアップを行うため、一定期間イベントログや経理システムが出力するログファイルの監視を強化し、大きなトラブルが起きなければ不要な監視項目の削除や監視設定を元に戻したいが、管轄外のアプリケーションの監視項目を誤って削除・変更してしまうリスクは出来るだけ避けたい場合など

●監視グループの監視の有効/無効スケジュール機能を使用
毎週の定期メンテナンスの際には、リソース監視は必ず異常を検知してしまうため定期メンテナンスの決まった時間帯は監視を止めたいが、リソース監視以外の監視は継続しておきたい

例:
毎週水曜日の 22 時から木曜日の 5 時までは定期メンテナンスを行っている関係上、CPU 使用率やメモリ使用率などのリソース監視は必ず異常を検知するので監視を自動で止めておきたいが、イベントログ監視などのリソースに直接関係のない監視項目は定期メンテナンスの作業ミスなどを検知できるため継続して行っておきたい場合など

●監視グループに属するすべての監視項目の監視間隔の設定機能を使用
月末に負荷が集中するサーバーがあり、月末の一定期間だけ不測の事態に備えるためにリソース監視の監視間隔は短くし、リソース監視以外の監視は監視間隔を長くしておきたい

例:
毎月 28 日から翌月の初日までは月末締めの各種バッチ処理が日中でも稼働しているため CPU 使用率やメモリ使用率などのリソース監視はすべて通常時よりも監視間隔を短くして不測の事態に備えたいが、各種バッチ処理の稼働中はサーバーの負荷が著しく上昇するため、リソース監視以外の監視間隔は長くすることで、少しでもサーバー負荷を軽減したい場合など

4.1.1 監視グループの作成

1. 該当するインスタンスの下にある“監視”ノードをクリックして選択します。
2. “監視”ノードを右クリックし、コンテキストメニューの“新規作成”→“監視グループ”の順にクリックします。
3. “監視グループ”ノードが“監視”のツリー下に新たに作成されます。
   新しい監視グループにフォーカスを当てると BOM マネージャーのリザルトペインに“監視項目”と表示されます。
4. 監視グループの名前を変更するには、下記のどちらかの手段で“プロパティ”画面を表示させます。
   ●リザルトペインで“監視グループ”をダブルクリック
   ●スコープペインかリザルトペインのどちらかで“監視グループ”を右クリックし、コンテキストメニューの“プロパティ”をクリック

4.1.2 監視グループのコピー

監視グループをコピーすると、監視グループに含まれる全監視項目、アクション項目の設定値等、監視グループのすべての設定がコピーされますので、監視要件が同じか類似の複数のサーバーを監視する場合に、設定時間を節約することができます。
コピーした監視グループは同じ名前とプロパティ設定値を持っていますので、設定値を変更する場合は、該当監視グループの“プロパティ”画面より行います。

1. 下記のどちらかの手段でコピーを行います。
   ●コピー元の監視グループを右クリックして、コンテキストメニューの“コピー”をクリック
   ●監視グループをクリックして選択してから、メニューバーに移動してメニューをクリックし、“操作”→“コピー”の順にクリック
2. コピーした監視グループを貼り付ける“監視”ノードを右クリックし、コンテキストメニューの“貼り付け”をクリックします。
   ●“監視”ノードを右クリックし、コンテキストメニューの“貼り付け”をクリックすると、グループ ID は自動で未使用の ID が割り振られます。

4.1.3 監視グループを有効にする

監視グループに属する監視項目全ての監視の有効/無効を制御することができます。

1. 下記のどちらかの手段で、監視グループの“プロパティ”画面を表示させます。
   ●リザルトペインで“監視グループ”をダブルクリック
   ●スコープペインかリザルトペインのどちらかで“監視グループ”を右クリックし、コンテキストメニューの“プロパティ”をクリック
2. 既定で“有効”になっていますので、監視グループを“無効”にしたい場合には、“有効”チェックボックスのチェックを外します。

●監視グループ単位での有効/無効制御のため、監視グループに所属する監視項目レベルで“無効”になっている監視項目の監視を“有効”にすることはできません。

4.1.4 監視グループの ID の変更

監視項目、アクション項目、および通知項目の ID も同じ手順で、変更することができます。

●アクション項目のプロパティ画面で、アクション項目を ID 番号順に実行するか否か（アクションの逐次処理を行う）を選択することにより、アクション項目を ID 番号順に実行させることができます。
詳細は‘7.7.3 アクション項目の概要’の項目の‘C.「実行条件」タブ’を参照ください。

1. 該当する監視グループを右クリックし、コンテキストメニューの“ID の変更...”をクリックすると“ID の変更”画面が表示されます。

2. 置き換える“新しい ID”を、“1”～“99”の任意の整数の中より入力します。
   ●この番号は未使用の ID でなければなりません。
   ●既に使用されている ID を割り当てると“この ID はすでに別の項目で使用されています”というエラーが出力されます。

4.1.5 監視グループのスケジューリング

監視が正常に実行されるためには、下記の 3 カ所の設定ですべて監視が有効になっていることが条件です。
一つでも監視が無効になっていれば監視は実行されません。

●監視グループで設定したスケジュールの監視オン/オフのスケジュールが“ON”である
●各監視グループの有効/無効が“有効”である
●監視グループ下の監視項目の有効/無効が“有効”であり、かつ、開始時刻の設定が該当する時間である

1. 下記のどちらかの手段で、監視グループの“プロパティ”画面を表示させます。

●リザルトペインで“監視グループ”をダブルクリック

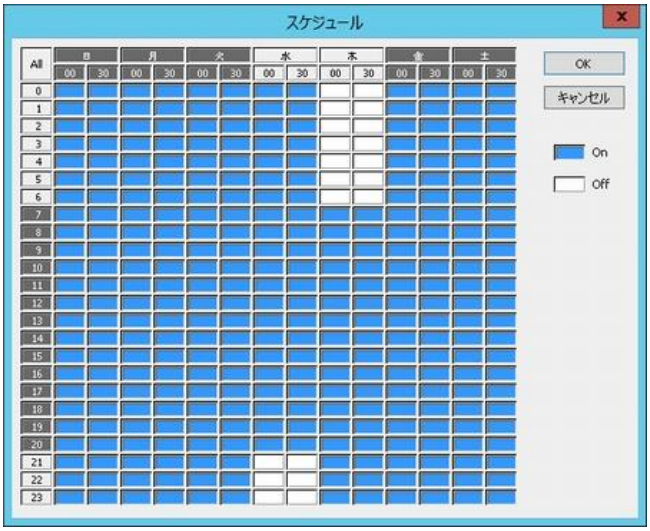
●スコープペインかリザルトペインのどちらかで“監視グループ”を右クリックし、コンテキストメニューの“プロパティ”をクリック

2. [設定..]ボタンをクリックし、“スケジュール”画面を表示させます。

既定値では監視グループは常に実行されるようにスケジュールされていますので、必要に応じてカーソルを

ドラッグするだけで、監視実行の選択（監視“On”）/選択解除（監視“Off”）をすることができます。

●下記は、毎週水曜日の 22 時から翌日木曜日の 6 時まで定期メンテナンスなどで、該当する監視グループの監視を Off（無効）にした例です。



4.1.6 監視項目の作成

監視項目は必ず監視グループに所属している必要があるため、監視グループから監視項目の作成を行います。

スコープペインの“監視グループ”を右クリックし、コンテキストメニューの“新規作成”をクリックすると、監視項目を作成することができます。監視項目の詳細は‘第 5 章監視項目’を参照ください。

4.1.7 監視項目リストのエクスポート

監視グループ内の情報は、タブ区切りのテキストファイルにエクスポートできます。

この情報は、BOM マネージャーのリザルトペインをテキストファイルにしたものです。

1. BOM マネージャーで監視項目リストをエクスポートしたい監視グループを右クリックします。
2. コンテキストメニューの“一覧のエクスポート”をクリックすると、“一覧のエクスポート”画面が表示されます。
3. ファイルを保存するフォルダーを選択して、ファイルに名前を付けます。
4. [保存]ボタンをクリックします。

監視項目リストのエクスポートでは、監視グループを選択した際のリザルトペインに表示されている下記項目が出力されます。

“項目名”、“各監視項目名”、“ID”、“有効/無効”、“監視間隔”、“注意”、“危険の条件”、“ステータス”、

“前回の値”、“前回実行時刻”

第5章 監視項目

5 .1 監視項目の解説

監視項目とは、システム管理者が監視設定する具体的な項目のことです。
BOM 7.0 では、イベントログのエントリから、ハードディスク、プロセス等、システム管理者にとって重要なものを監視できます。
監視を実行するには、監視項目を“有効”にする必要があります。

監視項目、またはそのアクション項目を作成/変更/削除するには、まずインスタンスを停止する必要があります。
なお、監視項目の最大数は 1 インスタンス当たり 200 項目です。

5 .2 監視項目の作成・削除

1. 監視項目を作成するには、該当する“監視グループ”を右クリックし、コンテキストメニューの“新規作成”をクリックします。
2. 表示されたコンテキストメニューの監視する項目（“ディスク容量監視”、“プロセス監視”、“プロセッサ監視”等）をクリックすると、
   “監視項目”が BOM マネージャーの“監視グループ”の直下に作成されます。
   “監視項目”は必要に応じて設定値を変更する必要があります。

監視項目を削除する際は、削除対象の監視項目上で右クリックし、コンテキストメニューの“削除”をクリックしてください。

以降のセクションでは、“監視項目”を“有効”にする方法、および各監視項目とその設定値の詳細について解説します。
各監視項目の“プロパティ”画面には複数のタブがあります。
●「全般」タブは、すべての監視項目で共通です。
●他のタブは、監視項目によって異なります。

5 .3 監視項目のコピー

“監視項目”をコピーすると、コピー先の監視グループの直下に表示されます。
コピーした項目は同じ名前とプロパティ設定値を持っていますので、設定値を変更する場合は“監視項目”の
“プロパティ”画面より行います。

1. “監視項目”を右クリックし、コンテキストメニューの“コピー”をクリックします。
2. “監視グループ”を右クリックし、コンテキストメニューの“貼り付け”をクリックします。
   ●ローカル監視もしくは代理監視のインスタンス間で監視項目を“コピー”し、“貼り付ける”ことができます。
   ●リモート接続時のスナップインノード間の監視項目のコピーはできません。

5.4 監視項目を有効にする

監視項目を“有効”にするには、下記のいずれかを実行します。

A. “監視項目”を右クリックし、コンテキストメニューの“有効”をクリックします。

B. “監視項目”を右クリックし、コンテキストメニューの“プロパティ”をクリックして“プロパティ”画面を表示させ、“有効”チェックボックスにチェックを入れます。

C. リザルトペインで“監視項目”をダブルクリックして“プロパティ”画面を表示させ、“有効”チェックボックスにチェックを入れます。

D. リザルトペインで“監視項目”をクリックし、リザルトペインの画面下部にある“有効”をクリックします。

●監視項目は既定値では“有効”チェックボックスにチェックが入っています。

●監視項目を“無効”にしたい際には、上記いずれかの手順で“無効”を選択します。

5.5 監視間隔の概念

各監視項目の“プロパティ”画面の「全般」タブにある“監視開始時刻”からの監視間隔を基準にして監視が実行されます。
なお、監視項目の“有効”チェックボックスのチェックを外しても時間間隔は刻まれているため、途中で監視項目の“有効”チェックボックスにチェックを入れた場合には、この間隔に沿って監視が行われます。

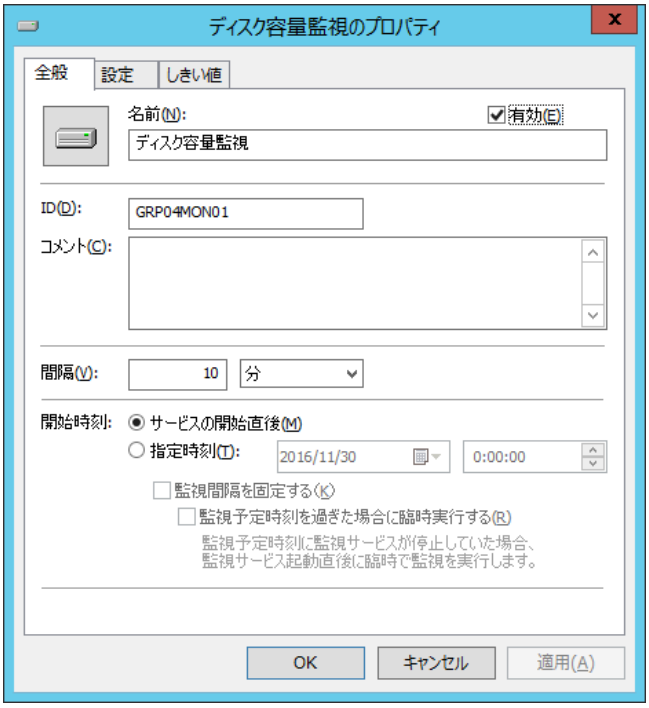
●“監視開始時刻”を“午前 0 時”に設定し、監視項目の監視間隔が“1 時間”の場合
午前 1 時、2 時、3 時・・・と 1 時間おきに監視が行われます。
1 時 10 分に監視項目の“有効”チェックボックスにチェックを入れた場合、次に監視が行われるのは 2 時です。

5.6 監視間隔の設定

監視間隔は監視項目ごとに設定しますが、設定方法は 2 パターンが存在するため、下記の例としてディスク容量監視のプロパティで監視間隔設定の画面を示して解説します。なお、手順 A.は監視項目ひとつひとつに対する設定であり、手順 B.は同一の監視グループ内の全監視項目に対し、まとめて監視間隔の変更を反映させることができます。

A. 監視項目のプロパティ手順

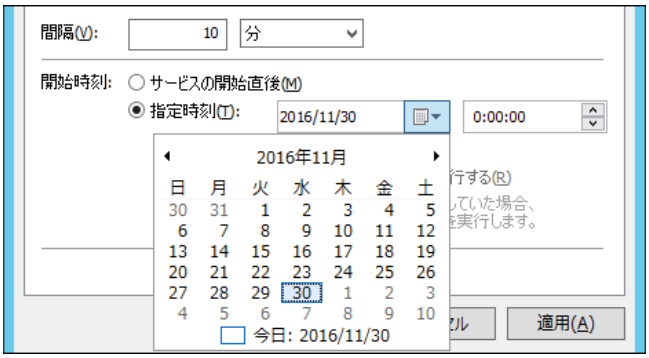
1. “監視項目”を右クリックし、コンテキストメニューの“プロパティ”をクリックして“プロパティ”画面を表示させます。



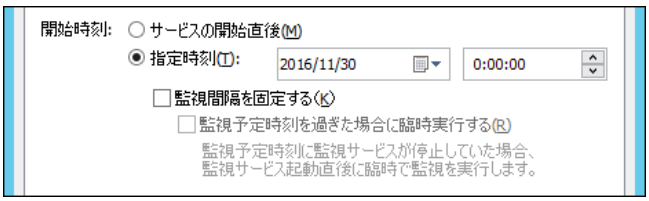
2. 「全般」タブの“間隔”フィールドは、この項目に対して監視を行う時間間隔（半角数値と時間単位）を入力します。
既定値の時間間隔は“10”分であり、監視間隔は“9999”日まで入力可能です。

3. “開始時刻”は、この監視項目の監視をいつ開始するのかを選択します。
“サービスの開始直後”ラジオボタンを選択するか、または“指定時刻:”ラジオボタンを選択して手順 4.と 5.で基準となる日時を指定します。

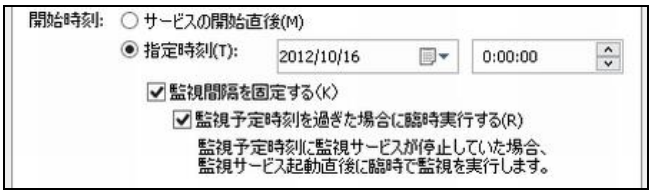
4. 手順 3.で監視の開始時刻の“指定時刻:”ラジオボタンを選択した場合
●“日付”フィールドのドロップダウンメニューのカレンダーより、“起動日”を指定します。



●“時刻”の入力は、“時”、“分”、“秒”を強調表示し、<上矢印>キーまたは<下矢印>キーを使用して変更を加えます。



5. “監視間隔を固定する”チェックボックスにチェックを入れると、“指定時刻”を起点に監視間隔を固定することができますので、監視サービス再起動によって監視時刻が変動しなくなります。



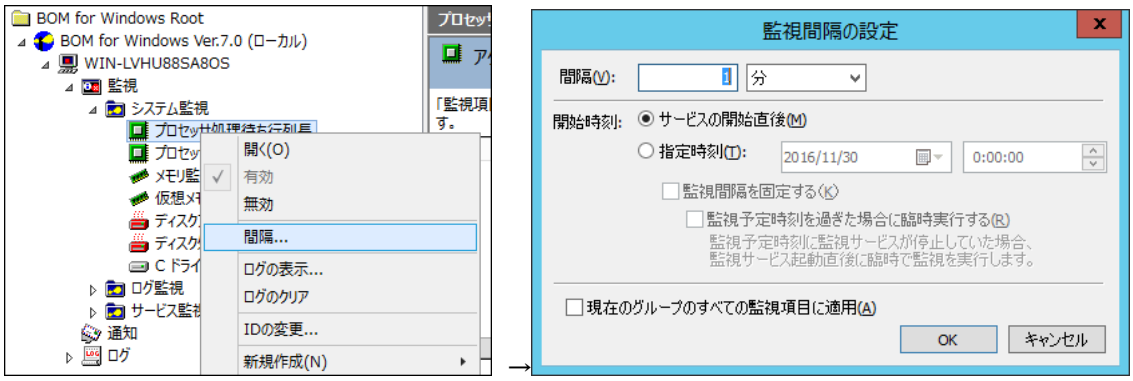
6. “監視予定時刻を過ぎた場合に臨時実行する”チェックボックスにチェックを入れると、監視サービス再起動などによって前回の監視から監視間隔以上を経過していた場合、臨時で監視を行わせることができます。

例:

毎日 10:00 に監視するように設定した上で、当日の 10:00 に監視サービスが起動していなかった場合に、10:20 に監視サービスを起動すると、当日は 10:20 に臨時で監視を行い、翌日以降は 10:00 に監視します。

B. 監視項目のコンテキストメニュー手順

1. “監視項目”を右クリックし、コンテキストメニューの“間隔”をクリックして“監視間隔の設定”画面を表示させます。



2. “間隔”フィールドは、該当監視項目の監視を行う時間間隔(半角数値と時間単位)を入力します。
監視間隔は“9999”日まで入力可能です。

3. 監視項目の“プロパティ”画面の「全般」タブの設定と同様に、サービスの開始直後から監視を始めるか、指定時刻から監視を始めるかを選択します。

4. “現在のグループのすべての監視項目に適用”チェックボックスにチェックを入れて[OK]ボタンをクリックした場合、手順 2.で指定した監視間隔を同一グループのすべての監視項目に適用することができます。
●“現在のグループのすべての監視項目に適用”チェックボックスのチェックを外して[OK]ボタンをクリックした場合、手順 2.で指定した監視間隔は、手順 1.で選択した監視項目のみに適用します。

5.7 監視ステータスについて

各監視項目は以下の 4 つの監視ステータスから成り立っています。

アイコン	監視ステータス名	説明
	正常	正常に監視が完了した状態
	注意	正常に監視が完了し、かつ設定した注意しきい値の条件に当てはまった状態 ※危険しきい値に当てはまった場合、ステータスは注意とならず危険になります
	危険	正常に監視が完了し、かつ設定した危険しきい値の条件に当てはまった状態
	失敗	監視対象のコンピューターから整数以外の値が返却された状態 （マイナスの値や Null データ、データ無し等）

監視ステータスの失敗については、BOM では基本的に正常に動作しているが監視対象から整数以外が返却された場合に監視結果として出力されます。

失敗ステータスが表示された場合には、監視元コンピューターと監視先コンピューター間または監視先コンピューターが正常に動作しているかを確認してください。

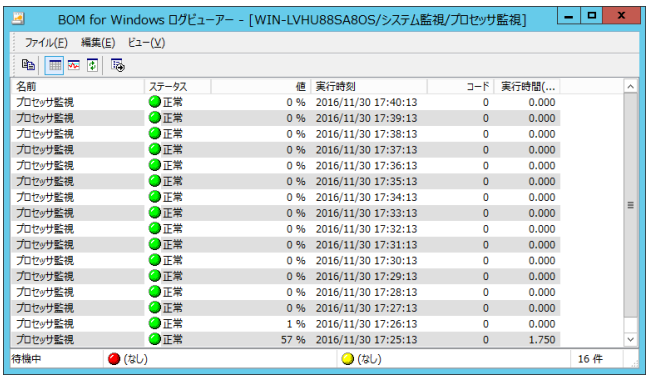
また、“ログ” → “ヒストリー” → “監視”に保存される監視ログレコードのプロパティに、詳細内容が記録されますのでご確認ください。

5.8 監視項目のログ

5.8.1 ログの表示

BOM 7.0 のログファイルは、BOM 7.0 で検出したシステム障害のトラブルシューティングを行う際に非常に役立ちます。

1. BOM マネージャーの“監視”ノード配下の各グループノード下の該当監視項目を右クリックし、コンテキストメニューの“ログの表示...”をクリックして“BOM ログビューアー”画面を表示させます。



2. タイトルバーに、現在表示されている“インスタンス”、“監視グループ”、および“監視項目”の名前が示されます。

一度に複数の“BOM ログビューアー”画面を開くこともできます。

1 監視項目当たりの最大ログ蓄積量の既定値は 15000 件です。

●“名前”列には、実行された監視項目がリストされます。

●“ステータス”列には、監視が行われたときの監視項目の状態(“正常”、“注意”、“危険”、“失敗”のいずれか)がリストされます。

●“値”列には、監視が行われた時点の項目の値がリストされます。
“N/A”は値が取得できなかった場合、あるいは必要なデータがすべて取得できなかった場合に表示されます。
“N/A”であっても“失敗”ステータスになるとは限りません。

●“実行時刻”列には、監視項目が実行された日時がリストされます。

●“コード”列には、BOM 監視プログラムからの“結果コード”がリストされます。

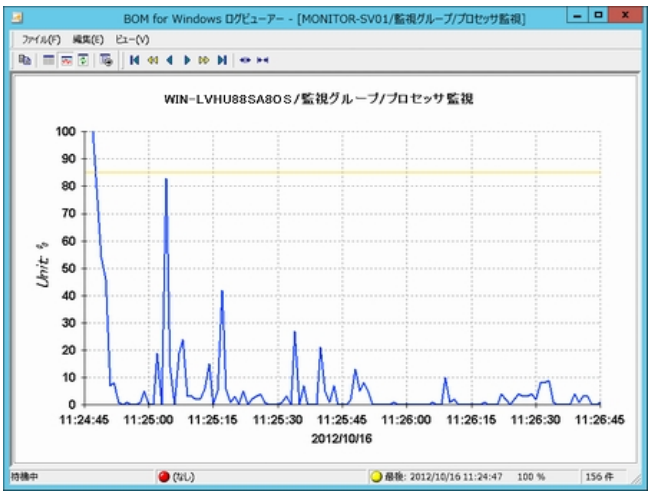
●“実行時間”列には、BOM 7.0 がその項目の監視を完了するまでにかかった時間がリストされます。

3. 最新の“注意”ステータスと“危険”ステータスの日時と値が、“BOM ログビューアー”画面最下部にあるステータスバーにリストされます。

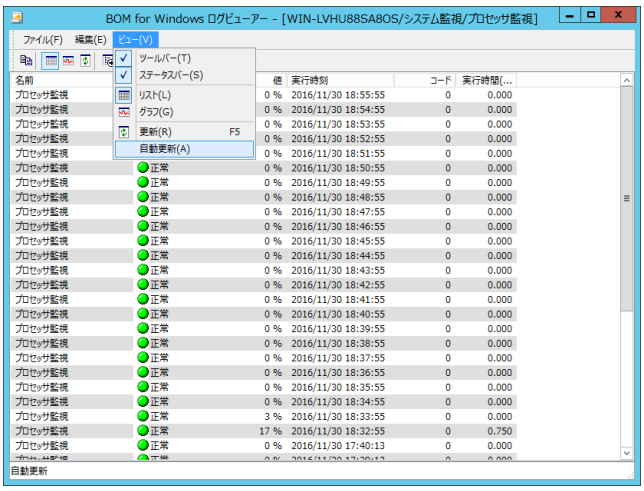
4. ログファイルの情報をグラフ表現で表示するには下記の 2 パターンがあり、下図のようなグラフが表示されます。
黄色い線は“注意”のしきい値、赤い線は“危険”のしきい値を示します。青い線は実際の値です。

●  をクリック

●“BOM ログビューアー”画面のメニューバーにある“ビュー”→“グラフ”の順にクリック。



5. “BOM ログビューアー”画面のメニューバーにある“ビュー”→“自動更新”の順にクリックすることで、自動的に最新情報を表示するように設定することができます。なお、“自動更新”の間隔は 2 秒です。



5 .8 .2 ログ蓄積量の最大件数の変更

監視項目のログは既定値で 15000 件まで保存できますが、最大件数を変更したい場合には下記の ini ファイルの一部を書き換えることで可能です。なお、設定は最初に監視項目のログが作成される場合に有効になります。

ログが既にある場合に最大件数を変更するには、‘9 .5 各種ログのクリア’の手順で監視項目のログを消去して、下記の ini ファイルの設定を変更してから、BOM ヘルパーサービス（BOM7Helper サービス）を再起動してください。

●ini ファイルの設定変更箇所

フォルダー : <BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Config¥

ファイル名 : MxHelper.ini

変更箇所 : [Option]

MaxMonLog = <XXXXX>

上記のパラメーターを追記し、<XXXXX>の数字を入力することで、保存できる件数を変更できます。

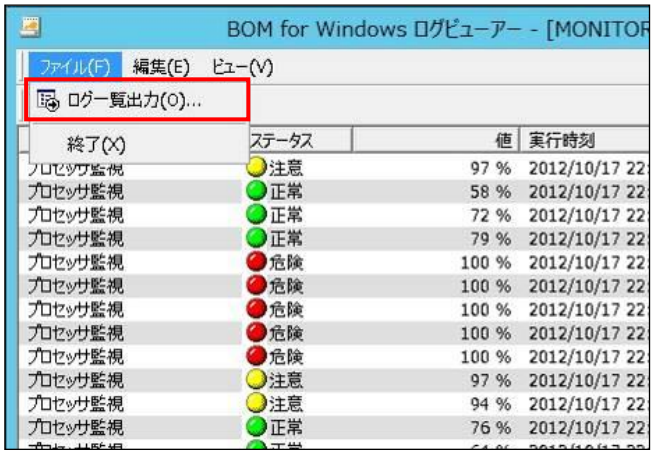
5 .9 監視ログリストのエクスポート

監視項目のログ情報は、タブ区切りのテキストファイルにエクスポートできます。

この情報は、“BOM ログビューアー”画面で表示されたデータをテキストファイルに出力するものです。

“BOM ログビューアー”画面の詳細は、‘5 .8 .1 ログの表示’を参照ください。

1. “BOM ログビューアー”のメニューバーにある“ファイル”→“ログ一覧出力”をクリックします。



2. ファイルを保存するフォルダーを選択して、ファイルに名前を付けます。

3. [保存]ボタンをクリックします。

出力される内容は、“各項目名”、“ステータス”、“実行時刻”、“項目名”、“取得値”、“コード”、“実行時間”です。

5.10 監視項目の詳細

5.10.1 監視項目の種類

BOM 7.0 基本製品で使用できる監視項目は下記の 21 種類です。

オプション製品をインストールしライセンスを適用することで、オプション製品固有の監視項目が追加で使用できるようになります。

オプション製品固有の監視項目の詳細は各オプション製品のユーザーズマニュアルを参照ください。

アイコン	監視項目名	説明
リソース監視系：8 種類		
	ディスク容量監視	論理ディスクの空き容量を監視
	フォルダー・ファイル監視	フォルダー、またはファイルの容量を監視
	プロセッサ監視	プロセッサ（CPU）の使用率を監視
	メモリ監視	メモリの空き容量を監視
	ディスクアクセス監視	ディスク負荷状況を監視
	ネットワークインターフェイス監視	ネットワークの負荷状況を監視
	プロセス監視	プロセスの各種パフォーマンスを監視
	パフォーマンスカウンター監視	パフォーマンスカウンターの値を監視
稼働監視系：2 種類		
	サービス監視	サービスの状態（開始/停止）を監視
	プロセスリスト監視	プロセス一覧を取得し、稼働状況を監視
ログ監視系：3 種類		
	イベントログ監視	アプリケーションとサービスログを含むログ監視
	テキストログ監視	テキストログファイルの監視
	BOM ヒストリー監視	BOM 7.0 のヒストリーログを監視
リモート監視系：2 種類		
	Ping 監視	特定サーバーとの Ping（ICMP ECHO）疎通監視
	ポート監視	特定サーバーとの TCP/UDP ポート疎通監視
その他の監視系：4 種類		
	インストールソフトウェア変更監視	インストールされているソフトウェアを監視
	Windows Update 監視	インストールされた WindowsUpdate の適用状況を監視
	AWS S3 ストレージ容量監視	Amazon S3 および、Amazon S3 互換ストレージ（※）上のバケット、フォルダー、ファイルのサイズ、数を監視
	iLO ログ監視	iLO 5 が出力する Integrated Management Log（IML）を監視
	iRMC ログ監視	iRMC が出力するログを監視
	カスタム監視	任意のプログラムを実行し、実行結果を監視

※　Amazon S3 互換ストレージについて、API 準拠をうたう全てのストレージでの動作を保証するものではありません。
弊社では、クラウディアン株式会社の CLOUDIAN HYPERSTORE について動作確認を取っており、今後の対応確認情報は
弊社ウェブサイト（www.say-tech.co.jp）で随時公開いたします。

5 .10 .2 監視項目の概要

設定を行いたい監視項目を右クリックし、コンテキストメニューの“プロパティ”をクリックすると、“プロパティ”画面が表示されます。
監視項目は作成しただけでは意図した監視が行えないため、“プロパティ”画面で監視項目の詳細な設定を行います。

A. 基本操作

1. “プロパティ”画面は、「全般」、「設定」などのタブで構成されています。
それぞれのタブをクリックすることで、該当するタブが表示され、設定を変更できます。

2. 変更した設定は、[OK]ボタン、または[適用]ボタンをクリックすることで BOM 7.0 に反映することができます。
変更した設定を破棄したい場合には[キャンセル]ボタンをクリックします。

B.「全般」タブ

「全般」タブは、“アイコン”、“ID”、“名前”、“間隔”に設定されている値を除き、すべての監視項目で共通です。
「全般」タブの概念は、‘5 .4 監視項目を有効にする’、‘5 .5 監視間隔の概念’、‘5 .6 監視間隔の設定’も参照ください。

1. [アイコン]ボタン

   [アイコン]ボタンは監視項目で設定されているアイコンが表示されています。

   既定では、監視項目の種類に合わせたアイコンが設定されています。

   [アイコン]ボタンをクリックすることで、アイコンを変更するための“アイコンの選択”画面を表示することができます。

   アイコンを変更する場合には、“アイコンの選択”画面にて変更したいアイコンをクリックし、[OK]ボタンをクリックします。

2. “有効”

   “有効”チェックボックスにチェックを入れることで監視を実行します。既定では“有効”チェックボックスにチェックが入っています。

   監視を行いたくない場合には、“有効”チェックボックスのチェックを外します。

3. “名前”フィールド

   “名前”フィールドには、“監視項目名”を入力します。既定値として監視項目の種類と同じ名称が入力されています。

   必要に応じて、分かりやすい名称に変更してください。この名前は、BOM マネージャーに表示される名前です。

4. “ID”フィールド

   “ID”フィールドには、“監視項目 ID”が表示されます。監視グループ番号と監視項目番号が含まれています。

   監視項目 ID は、インスタンス内で監視項目ごとに一意になるように、BOM 7.0 が自動的に設定します。

5. “コメント”フィールド

   “コメント”フィールドには、監視項目の補足情報を入力します。既定では空白です。必要に応じて入力してください。

6. “間隔”フィールド

   “間隔”フィールドには、監視項目の“監視間隔”を入力します。

   既定値として監視項目の種類ごとに定められた推奨値が入力されており、“1”から“9999”までの整数を入力できます。

   “間隔の単位”は、“秒”、“分”、“時”、または“日”から選択できます。

   ●“間隔”の設定は、監視項目を指定して右クリックし、コンテキストメニューの“間隔”をクリックして設定する内容と同じです。

7. “開始時刻”フィールド

   “開始時刻”には、監視項目を開始する日時を指定します。

   既定では、“サービスの開始直後”ラジオボタンが選択されています。

   ●“サービスの開始直後”ラジオボタンを選択した場合

   BOM 監視サービスの起動時に、監視が開始されます。

●“指定時刻”ラジオボタンを選択した場合

指定日時を選択し、初回の監視を実行します。

なお、初回以降の監視は、手順 6.で指定した“監視間隔”ごとに行われます。

8. “監視間隔を固定する”

“監視間隔を固定する”チェックボックスにチェックを入れることで指定時間を起点日時として監視間隔を固定にします。

“監視間隔を固定する”チェックボックスのチェックを外した場合、BOM 監視サービスを再起動すると前回の監視時刻を無視して監視を実行するため、監視サービス再起動によって監視間隔が変動することを防止したい場合には、

“監視間隔を固定する”チェックボックスにチェックを入れます。

●手順 7.で、“指定時刻”ラジオボタンを選択した場合にのみ利用できる機能です。

9. “監視予定時刻を過ぎた場合に臨時実行する”

“監視予定時刻を過ぎた場合に臨時実行する”は、チェックを入れることで監視サービス再起動などによって前回の監視から監視間隔以上を経過していた場合、臨時で監視を行います。

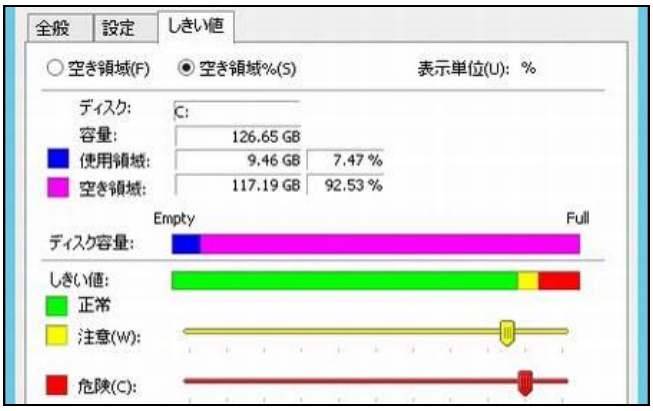
●“監視間隔を固定する”にチェックを入れた場合のみ利用できる機能です。

C. しきい値

すべての監視項目では、しきい値を設定する必要があります。しきい値に設定した条件に合致することで、監視ステータスが“注意”や“危険”に変化します。

しきい値に設定した条件に合致しない場合には監視ステータスが“正常”になります。

しきい値の設定方法は監視項目の種類によって異なります。



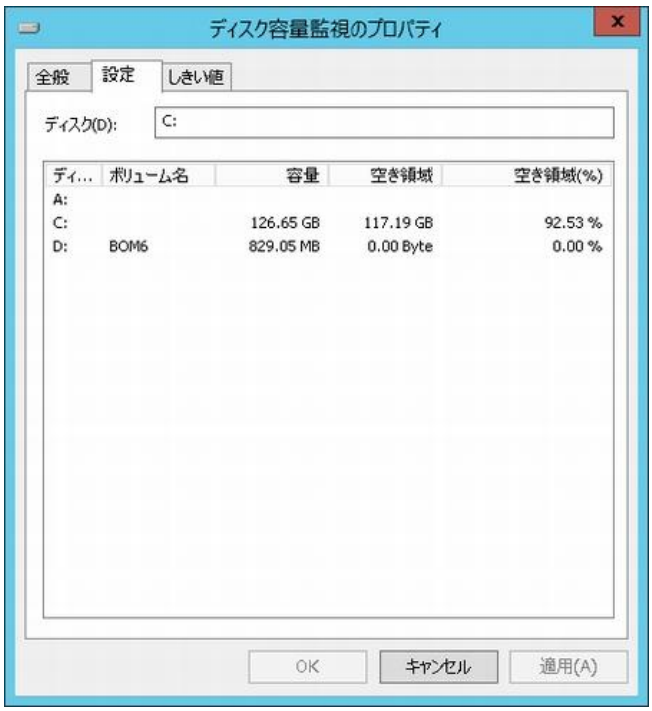
5 .10 .3 ディスク容量監視

監視対象コンピューターのハードディスク容量を監視します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ



1. BOM 7.0 は、コンピューター上にあるすべての論理ドライブを自動検出し、“ディスクドライブ情報”フィールドに表示させます。“ディスクドライブ情報”フィールドの監視対象のディスクドライブ名をダブルクリックし、“ディスク”フィールドに値を設定します。

C.「しきい値」タブ

1. 指定したディスクドライブのドライブの“空き領域”(容量)ラジオボタン、または“空き領域%”(パーセンテージ)ラジオボタンのどちらかを選択します。

2. “注意”フィールドと“危険”フィールドに、しきい値を下記のどちらかの手段で設定します。

●“注意”フィールドと“危険”フィールドに数値(“0”～“100”)を入力する。

●スライドバーを使用する。

スライドバーを使用するには、ハンドルをドラッグしてください。

黄色のハンドルをスライドすると、それに合わせて“注意”フィールド内の数値が変わります。

赤色のハンドルをスライドすると、それに合わせて“危険”フィールド内の数値が変わります。

3. 手順 1.で“空き領域”(容量)ラジオボタンを選択した場合、表示単位を選択することができます(既定値は“MB”)。

表示単位とは、BOM マネージャーに表示される単位です。

4. “危険”しきい値の設定は手順 2.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

●下記のように設定すると、連続して“9”回目の“注意”ステータスで、“危険”ステータスに変わります。

●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

5. 既に監視ログが蓄積されている場合、ディスク容量監視項目を計測する単位を変更すると(“パーセンテージ”→“MB”など)、次のダイアログボックスが表示されます。

●[はい]ボタンをクリックした場合

その監視項目のログファイルはクリアされます。

クリアされたログファイルは復旧できません。

●[いいえ]ボタンをクリックした場合

以前のデータを保持し以降のデータは追記されますが、ログ表示では指定した単位での表示になります。

以前設定した単位での表示になりませんのでご注意ください。

5 .10 .4 フォルダー・ファイル監視

監視対象コンピューターにある指定したフォルダー、あるいはファイルの使用サイズを監視します。

Windows Server 2008 以降のシンボリックリンクを使用したフォルダーへのフォルダー監視は、OS と動作が異なるのでご注意ください。

●OS 標準のエクスプローラーで見た場合

フォルダーとしても、ファイルとしても認識せず、ファイルサイズは 0byte と認識されます。

●BOM 7.0 のフォルダー監視の場合

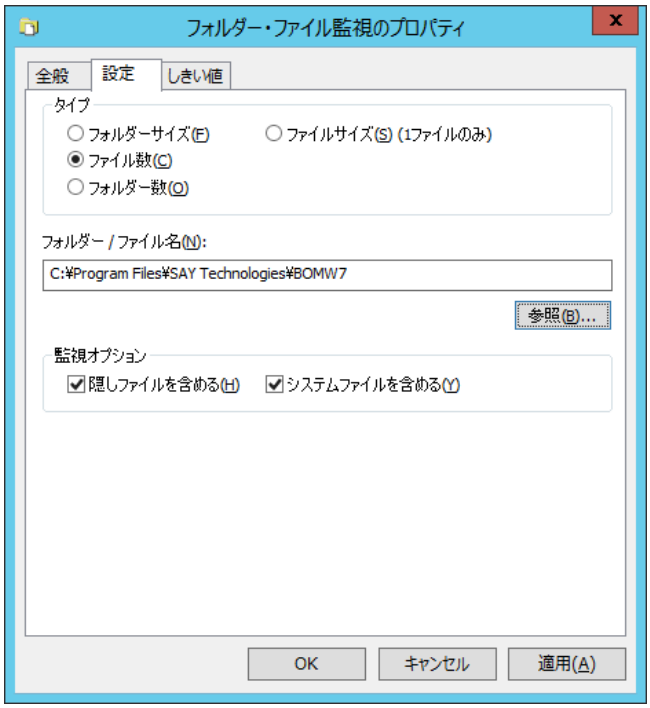
リンク先のフォルダー数、フォルダーサイズ、ファイル数、ファイルサイズを認識します。

シンボリックリンクによる無限ループ（参照した先に参照元のフォルダーがシンボリックリンク）がある場合には、監視に失敗します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ



1. “タイプ”フィールドは、監視対象を各対象のラジオボタンで選択します。

   ●複数の“タイプ”で監視したい場合は、フォルダー・ファイル監視項目を新しく作成する必要があります。

   ●新規作成した監視項目名の既定値は異なる“タイプ”でも同一ですので、異なるタイプの監視項目を区別するには、「全般」タブの“名前”フィールドで区別が容易な名称を付けます。

2. “フォルダー/ファイル名”フィールドは、下記のどちらかの手段で設定します。

   ●フォルダー、またはファイルの絶対パスを入力する。

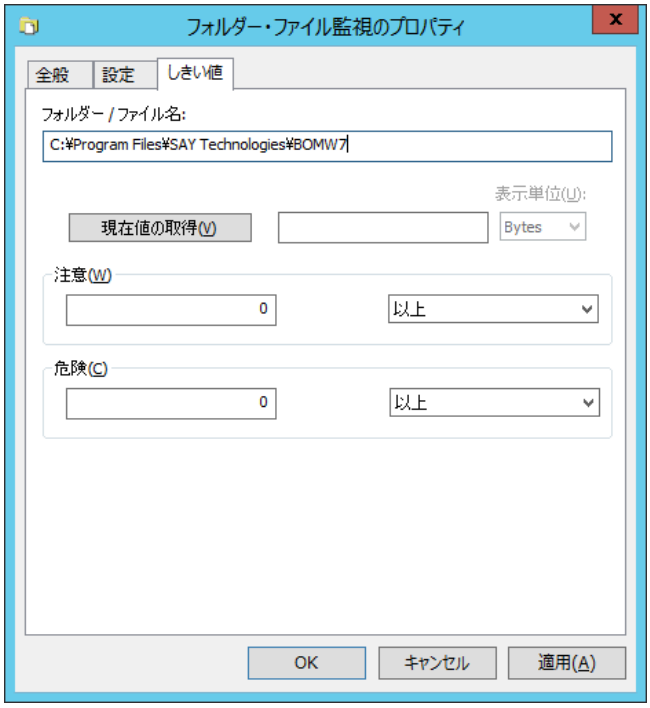
   ●[参照..]ボタンをクリックしてフォルダー、またはファイルを選択する。

   “参照”をクリックして表示される画面は、通常の Explorer と挙動が異なり、フォルダーを選択して<Enter>キーを押下した際、[OK]ボタンのクリックと同じ動作になります。

3. “監視オプション”フィールドで、必要なオプションを選択します。

   既定値では、“隠しファイル”と“システムファイル”を含むすべてのファイルが監視対象に含まれています。

C.「しきい値」タブ



1. 「設定」タブで選択したファイル・フォルダーの値を表示するには、[現在値の取得]ボタンをクリックします。
   ファイルまたはフォルダーのサイズを監視する場合、[現在の値を取得]ボタンの単位をドロップダウンメニューから選択します。
   なお、“表示単位”フィールドの単位を変更した場合、もう一度[現在値の取得]ボタンをクリックすると、
   変更した単位でサイズを再計算して表示することができるので、単位に合わせて最適なしきい値を設定してください。
   ●“表示単位”を“MB”→“Bytes”変更した場合
   [現在値の取得]ボタンクリック時にフィールドの数値が“86”の場合→“90,177,536”に変わります。
   (“1KB = 1024Bytes”で計算しています。)
2. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。
   ●しきい値
   テキスト入力フィールドに数値(“0”～“9999999”)を入力します。
   手順 2.で指定した“表示単位”に応じて、しきい値に対する適切な単位(“KB”、“MB”など)が自動で表示されます。
   ●しきい値の判定単位
   ドロップダウンメニューを使用して、しきい値に対する判定条件を、
   “より大きい”、“以上”、“より小さい”、“以下”の中から選択します
3. “危険”しきい値の設定は手順 3.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。
   ●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

4. 既に監視ログが蓄積されている場合、ファイル・フォルダー監視項目を計測する単位を
変更すると(“ファイルサイズ”→“ファイル数”など)、次のダイアログボックスが表示されます。

●[はい]ボタンをクリックした場合

その監視項目のログファイルはクリアされます。クリアされたログファイルは復旧できません。

●[いいえ]ボタンをクリックした場合

以前のデータを保持し以降のデータは追記されますが、ログ表示では指定した単位での表示になります。

以前設定した単位での表示になりませんのでご注意ください。

5 .10 .5 サービス監視

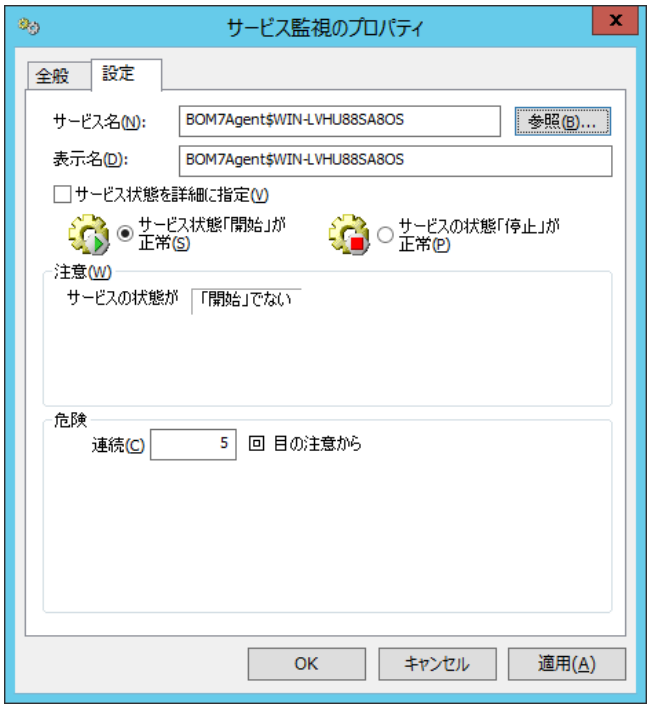
監視対象コンピューターのサービス状態の状態が、“開始”状態あるいは“停止”状態かを監視します。

サービス監視では他の監視項目と違い、文字列が監視結果となっているため‘5 .8 .1 ログの表示’のグラフ表示はできません。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ



1.「設定」タブの“サービス名”フィールドに、監視する“サービス名”を下記のどちらかの手段で設定します。

※ Windows 10 version 1803 および、Windows Server 2016 version 1803 の環境を代理監視による監視対象としている場合、[参照..]ボタンをクリックした際に「アクセスが拒否されました」というエラーでサービス一覧の取得に失敗することがあります。この際は“サービス名”フィールドへ監視するサービス名を直接入力してください。

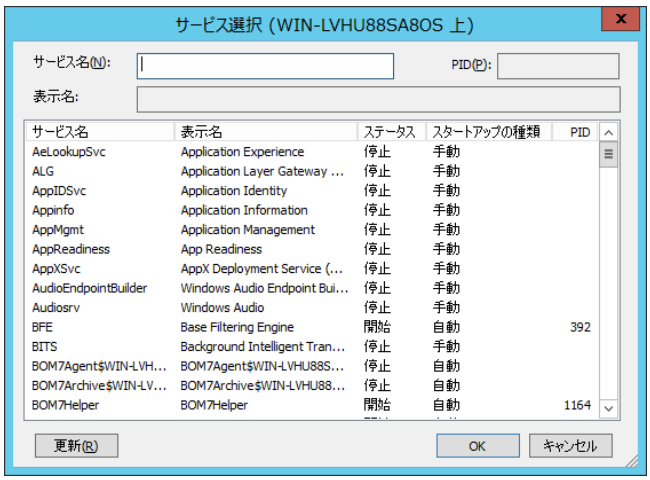
●“サービス名”を入力する。

●[参照..]ボタンをクリックし、“サービス選択”画面を表示させ、サービスのリストから“サービス名”を選択する。
監視対象のコンピューターに登録されているサービスとステータス(開始/停止)のリストを“サービス選択画面”に表示させ、リストから監視対象のサービスを選択することができます。

2.“サービス選択”画面の“サービス名”フィールドに、監視する“サービス名”を下記のどちらかの手段で設定します。

●“サービス名”を入力して、[OK]ボタンをクリックする。

●リストの“サービス名”をクリックして、[OK]ボタンをクリックする。



3. サービスのリストとステータスを最新表示するには[更新(R)]ボタンをクリックし、[OK]ボタンをクリックします。
4. “注意”フィールドに、しきい値を下記のどちらかの手段で設定します。

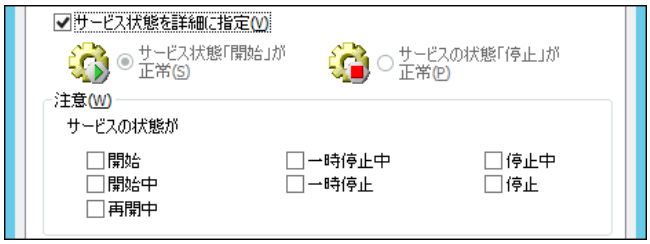
●“サービス状態を詳細に指定”チェックボックスのチェックを外した場合

“サービス状態「開始」が正常”ラジオボタンか、“サービス状態「停止」が正常”ラジオボタンより選択します。

既定値は“開始”状態です。その場合、監視対象サービスが“開始”状態ではない際に、“注意”ステータスになります。

●“サービス状態を詳細に指定”チェックボックスにチェックを入れた場合

サービスのステータスを“開始”、“開始中”、“再開中”、“一時停止中”、“一時停止”、“停止中”、“停止”の中から複数指定することができます。



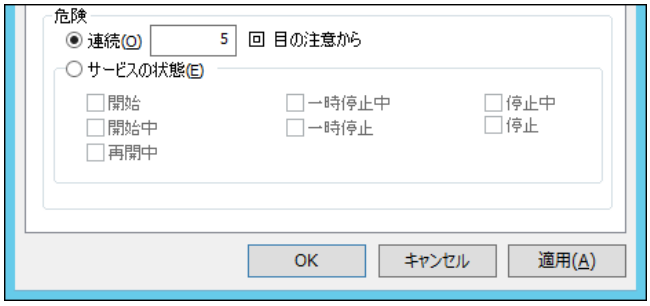
5. “危険”フィールドに、しきい値を下記のどちらかの手段で設定します。

●“連続”ラジオボタンを選択した場合

“注意”ステータスの“連続発生回数”を指定します。連続回数に指定できるのは、“1”～“99”の数値です。

●“サービスの状態”ラジオボタンを選択した場合

“サービスの状態”ラジオボタンを選択することで、サービスのステータスを“開始”、“開始中”、“再開中”、“一時停止中”、“一時停止”、“停止中”、“停止”の中から複数指定することができます。



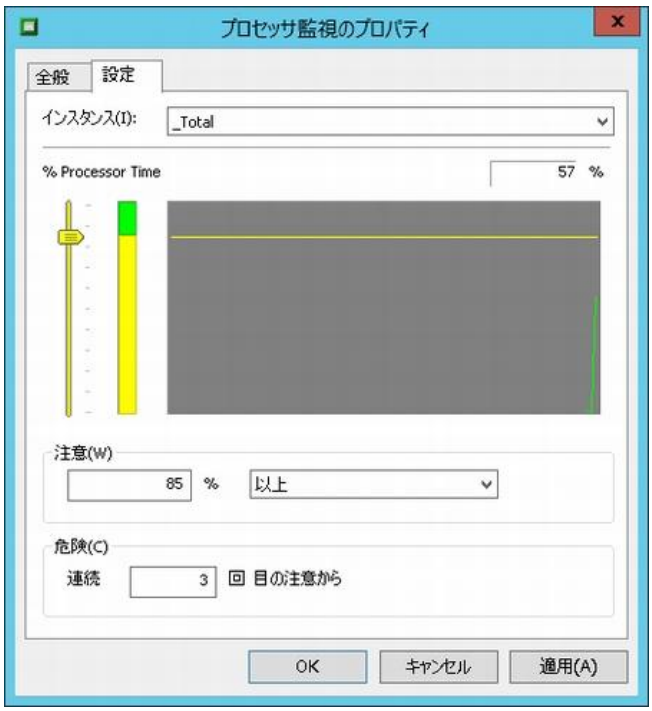
5 .10 .6 プロセッサ監視

監視対象コンピューターのプロセッサ(CPU)稼働状態を監視します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ



1. BOM 7.0 は、コンピューター上にあるすべてのプロセッサを自動検出し、“インスタンス”フィールドに表示させます。
   （4CPU システムでは、ドロップダウンメニューに、“_Total”の他“0”、“1”、“2”、“3”と 4 つのプロセッサが表示されます。）
   監視対象のプロセッサを、“インスタンス”フィールドのドロップダウンリストより選択します。
2. “注意”フィールドに、しきい値を下記のどちらかの手段で設定します。
   ●数値（“0”～“9999”）を入力する。
   ●スライドバーを使用する。
3. “危険”フィールドのしきい値に、“注意”ステータスの“連続発生回数”を指定します。
   ●連続回数に指定できるのは、“1”～“99”の数値です。

5 .10 .7 メモリ監視

監視対象コンピューターのメモリの使用できる空き容量を監視します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ

1. 使用する単位を“表示単位”より選択します。

   ●表示単位を変更すると上段の現在の“メモリの空き容量（Available Bytes）”の数値が表示スケールで表示されます。

   この数値を参考に、“注意”、“危険”のしきい値を決めることができます。

2. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

   ●しきい値

   テキスト入力フィールドに数値（“0”～“999999999”）を入力します。

   ●しきい値に対する判定条件

   ドロップダウンメニューを使用して、しきい値に対する判定条件を、

   “より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

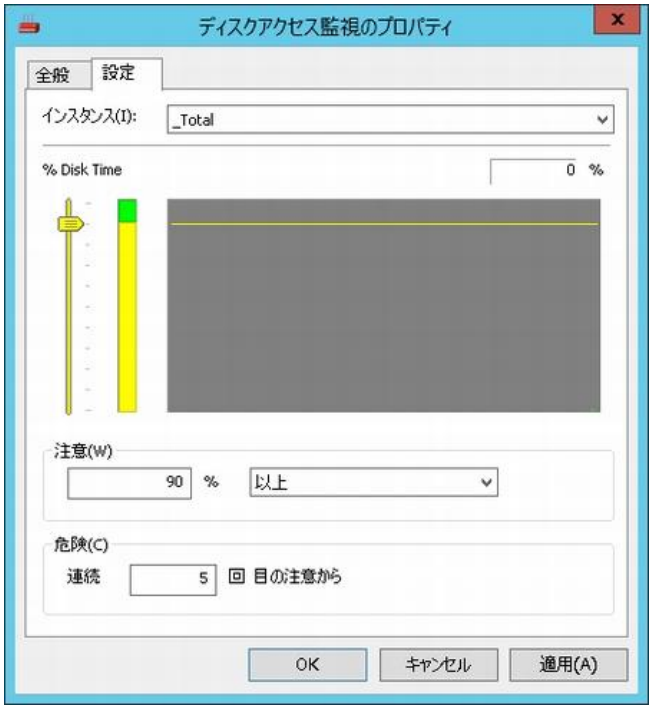
5 .10 .8 ディスクアクセス監視

監視対象コンピューターのディスクアクセスの状態を監視します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ



1. BOM 7.0 は、コンピューター上にあるすべての物理ディスクを自動検出し、“インスタンス”フィールドに表示させます。
   監視対象の物理ディスクを、“インスタンス”フィールドのドロップダウンリストより選択します。
   ●監視対象のコンピューター上に C ドライブと D ドライブが存在する場合、ドロップダウンメニューに“_Total”の他、
   “0 C:”、“1 D:”と 2 つのディスクドライブ名が表示されます。
2. “注意”フィールドに、しきい値を下記の通りそれぞれ設定します。
   ●しきい値
   テキスト入力フィールドに数値(“0”～“9999”)を入力するか、スライドバー(“0”～“100”)で設定します。
   ●しきい値に対する判定条件
   ドロップダウンメニューを使用して、しきい値に対する判定条件を、“より大きい”、“以上”の中から選択します。
3. “危険”フィールドのしきい値に、“注意”ステータスの“連続発生回数”を指定します。
   ●連続回数に指定できるのは、“1”～“99”の数値です。

●ディスクドライバによっては大量のファイル複製を行っている間にディスクを監視した場合、監視値が不定期で N/A に
なることがあります。

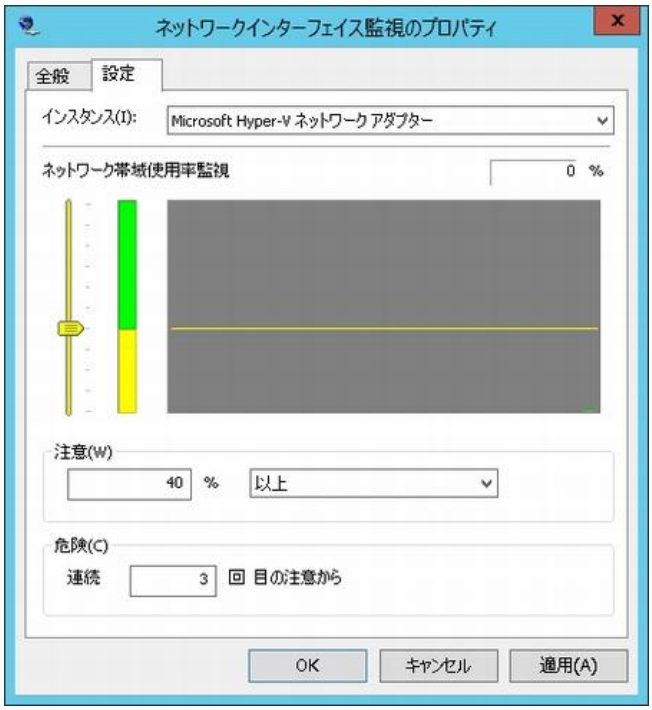
5 .10 .9 ネットワークインターフェイス監視

監視対象コンピューターの指定したネットワークアダプタ(NIC)での送受信パケット総合計の 1 秒間当たりの
ネットワーク帯域使用率を監視します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ



1. BOM 7.0 は、システムにインストールされているネットワークアダプタを自動検出し、“インスタンス”フィールドに表示させます。
   監視対象のネットワークインターフェイスを、“インスタンス”フィールドのドロップダウンリストより選択します。
2. “注意”フィールドに、しきい値を下記の通りそれぞれ設定します。
   ●しきい値
   テキスト入力フィールドに数値(“0”～“999”)を入力するか、スライドバー(“0”～“100”)で設定します。
   ●しきい値に対する判定条件
   ドロップダウンメニューを使用して、しきい値に対する判定条件を、“より大きい”、“以上”の中から選択します。
3. “危険”フィールドのしきい値に、“注意”ステータスの“連続発生回数”を指定します。
   ●連続回数に指定できるのは、“1”～“99”の数値です。

●ネットワークインターフェイス監視を新規作成した際には、インスタンス(どの NIC を監視するか)が指定されていません。
新規作成時には必ずインスタンスを指定してください。指定しない場合には正確な監視データを収集できません。
●半二重通信時は最大まで帯域を使用しても 50%になりますのでご注意ください。

5 .10 .10 プロセス監視

監視対象コンピューターの指定したプロセスのパフォーマンスや稼働状態を監視します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ

1. “インスタンス”

   “プロセス名を指定”ラジオボタンを選択している場合は監視対象の“プロセス名”を、“サービス名を指定”ラジオボタンを選択している場合は監視対象の“サービス名”を“インスタンス”フィールドで指定します。

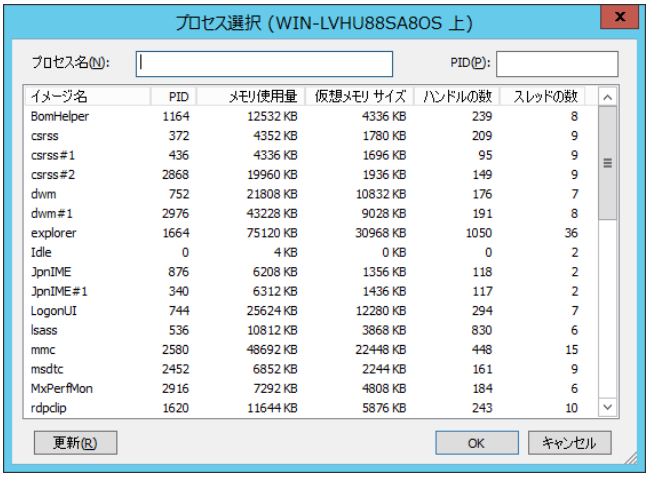
   指定方法は次のいずれかの方法から選択してください。

   ●“インスタンス”フィールドに、“プロセス名”もしくは“サービス名”を直接入力する。

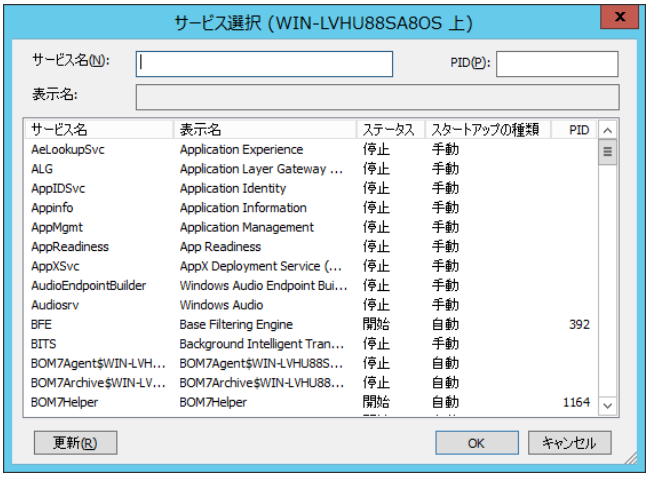
   ●[参照..]ボタンをクリックし、“プロセス”もしくは、“サービス”のリストから対象を選択する。

   ※ Windows 10 version 1803 および、Windows Server 2016 version 1803 の環境を代理監視による監視対象としている場合、“サービス名を指定”ラジオボタンを選択して[参照..]ボタンをクリックすると、「アクセスが拒否されました」というエラーでサービス一覧の取得に失敗することがあります。この際は“インスタンス”フィールドへ、監視対象とするサービス名を直接入力してください。

(1) “プロセス名を指定”ラジオボタンを選択した場合、下記の“プロセス”選択画面が表示されます。



(2) “サービス名を指定”ラジオボタンを選択した場合は、下記の“サービス選択”画面が表示されます。



(3) “プロセス選択”画面の“プロセス名”フィールドに、監視する“プロセス名”を下記のどちらかの手段で設定します。

※ “サービス名を指定”ラジオボタンを選択した場合は、“プロセス”を“サービス”に読み替えてください。

●“プロセス名”を入力して、[OK]ボタンをクリックする。

●リストの“プロセス名”をクリックして、[OK]ボタンをクリックする。

(4) リストを最新の状態にするには[更新]ボタンをクリック、“プロセス名”に問題がなければ[OK]ボタンをクリックします。

※ “サービス名を指定”ラジオボタンを選択した場合は、“プロセス”を“サービス”に読み替えてください。

(5) “PID”フィールドは、手順 1.で“インスタンス”フィールドの指定を行った際に、指定した“インスタンス”に該当する PID が自動で設定されます。

2. “インスタンスが存在しない場合も失敗としない”

●チェックボックスのチェックを外した場合

手順 1.で指定したプロセスもしくはサービスが監視時に存在しなかった場合、監視結果のステータスは“失敗”を返します。

●チェックボックスにチェックを入れた場合

手順 1.で指定したプロセスもしくはサービスが監視時に存在しなかった場合、監視結果の値は“0”を返します。

仮に、注意もしくは危険のしきい値で“0”を検知するように設定していた場合、監視結果のステータスは

“注意”もしくは“危険”になります。

3. “PID を指定する”チェックボックスにチェックを入れた場合、手順 1.で指定したインスタンスを無視して、手順 4.で設定した PID を元に監視を行います。

●手順 1.で“サービス名を指定”ラジオボタンを選択した場合、“PID を指定する”チェックボックスにチェックを

入れることができません。

●“PID を指定する”チェックボックスにチェックを入れた場合、手順 9.の複数の同一プロセスを集計するための

“集計”フィールドは設定することができません。

4. “カウンター”フィールドで、指定した“プロセス”または“サービス”の監視方法を選択します。

●各カウンターの詳細は、“カウンター”フィールド下部の画面に解説が表示されます。

5. “集計”フィールドで、複数の同一プロセスがある場合に、“カウンター”で設定した値の集計方法を選択します。

集計方法は下記の通りです。

●Count : 指定同一名プロセス個数を集計します。Count は“カウンター”設定は無効です。

●Sum : 指定同一名プロセスの“カウンター”設定した監視結果の合計を出力します。

●Min : 指定同一名プロセスの“カウンター”設定した監視結果の最小値を出力します。

●Max : 指定同一名プロセスの“カウンター”設定した監視結果の最大値を出力します。

●Avg : 指定同一名プロセスの“カウンター”設定した監視結果の平均値を出力します。

6. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

●しきい値

テキスト入力フィールドに数値(“0”～“999999999”)を入力します。

手順 7.で指定した“カウンター”に応じて、しきい値に対する適切な単位(“KB”、“Sec”など)が自動で表示されますが、

件数(スレッド数、ハンドル数、プロセス数)が対象の場合、単位はありません。

●しきい値の判定条件

ドロップダウンメニューを使用して、しきい値に対する判定条件を、

“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

7. “危険”しきい値の設定は手順 9.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

8. しきい値設定のため参考値を見るには、[現在値の取得]ボタンをクリックします。

取得値は、手順 7.で指定した“カウンター”の単位に応じて表示されます。

C. 応用編:プロセス自体の生死確認を行いたい場合

1. “プロセス名”あるいは“プロセス ID”を指定します。
2. “集計”に利用する関数を“Count”とします。
3. “注意”あるいは“危険”しきい値を“0 と等しい”に設定すると、プロセスが存在しなければ、
   “注意”ステータスあるいは“危険”ステータスになりますので、判定ができます。

D. 補足事項

●“インスタンスが存在しない場合も失敗としない”チェックボックスにチェックを入れている場合に監視対象のインスタンスが存在しない時には、[現在値の取得]ボタンをクリックすると結果は“0”になりますが、下記のカウンターの場合には“N/A”になります。

1. Creating Process ID
2. ID Process
3. Priority Base
4. System Idle Process

●同一“プロセス名”が複数ある場合には、プロセスの起動順序に“プロセス名”の後に“#1”～“n”がつきます。

例:
プロセス名、プロセス名 #1、プロセス名 #2・・・

同一“プロセス名”の一つを監視するにはその中から指定するか、直接インスタンスの箇所に
“プロセス名 #1”と指定してください。
また、途中でその中のプロセスが停止した場合には、順に番号は繰り上がりますのでご注意ください。

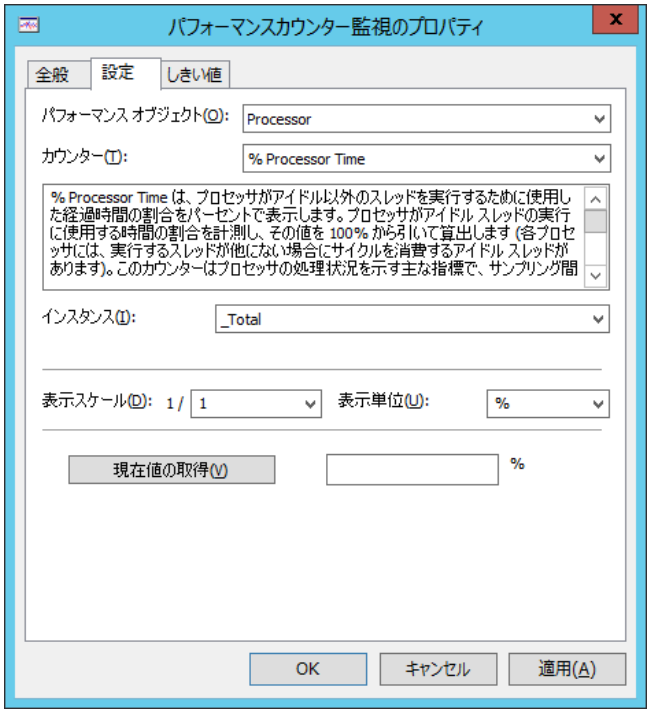
5 .10 .11 パフォーマンスカウンター監視

監視対象コンピューターのパフォーマンスを OS 標準のパフォーマンスデータを元に監視を行います。

A.「全般」タブ

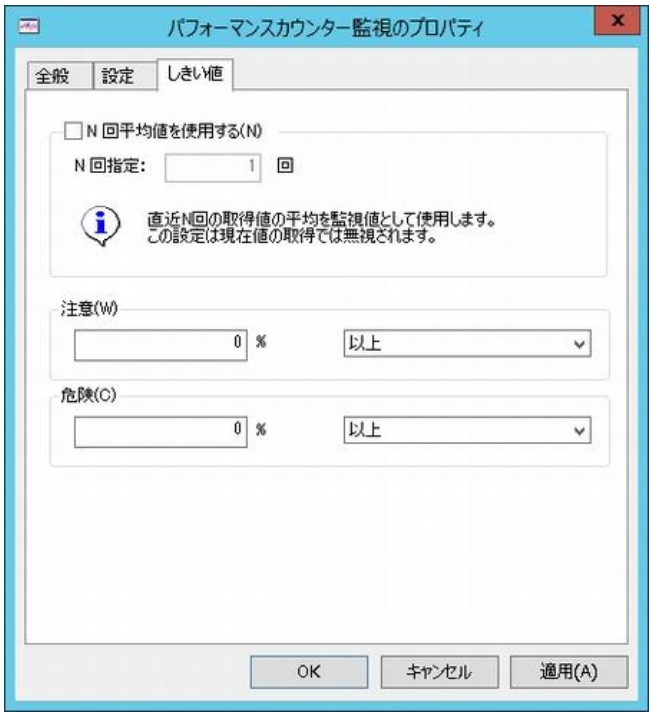
「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ



1. “パフォーマンス オブジェクト”フィールドで、監視するオブジェクトを選択します。
2. “カウンター”フィールドのリストは、手順 1.で指定した“パフォーマンス オブジェクト”によって異なります。
   ●各カウンターの詳細は、“カウンター”フィールド下部の画面に解説が表示されます。
3. “インスタンス”フィールドのリストは、手順 2.で指定した“カウンター”によって異なります(ブランクの場合もあります。)。
4. “表示スケール”は、監視値を指定したスケールに合わせてログに表示します。
   “表示スケール”の設定範囲は“1”～“2,000,000,000”の整数を入力することができます。
   小数点数値はドロップダウンリストから“0.1”、“0.01”、“0.001”、“0.0001”、“0.00001”、“0.000001”、“0.0000001”が選択できます。
   ●整数の“表示スケール”→整数の“表示スケール”に変更した際には、所得値は表示上でスケールに応じて変更されます。
   ●整数の“表示スケール”→小数点の“表示スケール”に変更した場合、もしくは逆の変更を行った場合、
   下記に表示される値が正しく表示できなくなりますので、スケールを変更した監視項目のログのクリアが必要です。
   1.BOM マネージャーのリザルトペインの“前回の値”
   2.ログのリスト表示
   3.インスタンスステータス表示の取得値
5. “表示単位”は、表示上、わかりやすく指定するもので、あらかじめ設定されている単位以外にも任意に変更可能です。
   この表示単位はスケールとは関係ありません。なお、“KB”では“1024”、“MB”では“1048576”と表示されます。
6. 現在選択されている“カウンター”の値を表示するには、[現在値の取得]ボタンをクリックします。

C.「しきい値」タブ



1. “N 回平均値を使用する”にチェックをすると、「設定」タブの監視条件で取得した値の、直近 N 回分の平均値をしきい値にすることができます。

   “N 回指定”フィールドには、具体的に直近何回分のデータを対象とするのかを数値(“1”～“99”)で入力します。

   ●「設定」タブの手順 6.で解説した[現在値の取得]ボタンをクリックすると平均値は取得できず、現在の値が表示されます。

   ●“N 回平均値を使用する”場合、指定した N 回分のデータが蓄積されるまでは、取得値は“N/A”になります。

2. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

   ●しきい値

   テキスト入力フィールドに数値(“0”～“999999999”)を入力します。

   「設定」タブの手順 2.で指定した“カウンター”に応じて、しきい値に対する適切な単位(“KB”、“Sec”など)が自動で表示されますが、件数(スレッド数、ハンドル数、プロセス数)が対象の場合、単位はありません。

   ●しきい値の判定条件

   ドロップダウンメニューを使用して、しきい値に対する判定条件を、

   “と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

3. “危険”しきい値の設定は手順 2.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

   ●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

D. 補足事項

●“Processor オブジェクト”の“Processor Queue Length”は BOM 7.0 の監視項目に応じて増加します。

しきい値を設定する際には、[現在値の取得]ボタンで表示される現在値を参考に設定してください。

●“カウンター”によっては本来もっているべきインスタンスが存在しない場合には説明文が表示されません。

5 .10 .12 プロセスリスト監視

監視対象コンピューターのプロセスの有無を監視します。プロセスリスト監視の使用方法は、下記の 2 種類があります。

●ブラックリストプロセス監視

監視対象コンピューター上で既存の問題あるプロセス（ブラックリスト）をあらかじめ列挙しておき、そのプロセスを監視します。

●ホワイトリストプロセス監視

あらかじめ監視対象コンピューター上で動作していても問題ないと判断するプロセスリスト（ホワイトリスト）を作成します。

プロセスリストには同一プロセスの個数も含められ、監視時に指定個数を超えるプロセスを検知すると、超えたプロセス数を取得値とし、該当プロセス一覧も取得できます。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ

●ブラックリストプロセス監視は、監視対象コンピューター上で動作すべきではないプロセスをあらかじめ登録します。

●ホワイトリストプロセス監視は、監視対象コンピューター上で動作していても問題のないプロセスをあらかじめ登録します。

1. ブラックリストプロセスとホワイトリストプロセスのどちらの監視を行いたいのか、“監視方式”フィールドに指定します。

   なお、“ホワイトリスト”→“ブラックリスト”に変更した場合、“プロセス数の個数が全て 1 に変更される”という趣旨のポップアップ画面が表示されます。

   ●ブラックリストプロセス監視

   “監視方式”フィールドに、“監視対象リストにあるプロセスの起動を監視（ブラックリスト）”を設定します。

●ホワイトリストプロセス監視

“監視方式”フィールドに、“監視対象リストにないプロセスの起動を監視（ホワイトリスト）”を設定します。

2. 監視するプロセス名を指定する場合には、下記のどちらかの手段で設定します。

●実行中のプロセスリストより選択

BOM 7.0 は、コンピューター上で実行中のプロセスを自動検出し、“実行中のプロセス”フィールドに表示させます。

“実行中プロセス”リストで、ブラックリスト、もしくはホワイトリスト対象の“プロセス名”をダブルクリックするか、

をクリックすることにより、“監視対象リスト”に登録します。

をクリックすると、“実行中プロセス”リストのすべてのプロセスを“監視対象リスト”に登録します。

●[新規..]ボタンをクリックし、“プロセスの追加”画面より選択

[新規..]ボタンをクリックすると、“プロセスの追加”画面が表示されますので、“プロセス名”と“プロセス数”を入力します。

●ブラックリストプロセス監視の場合、“プロセス数”は指定できません。

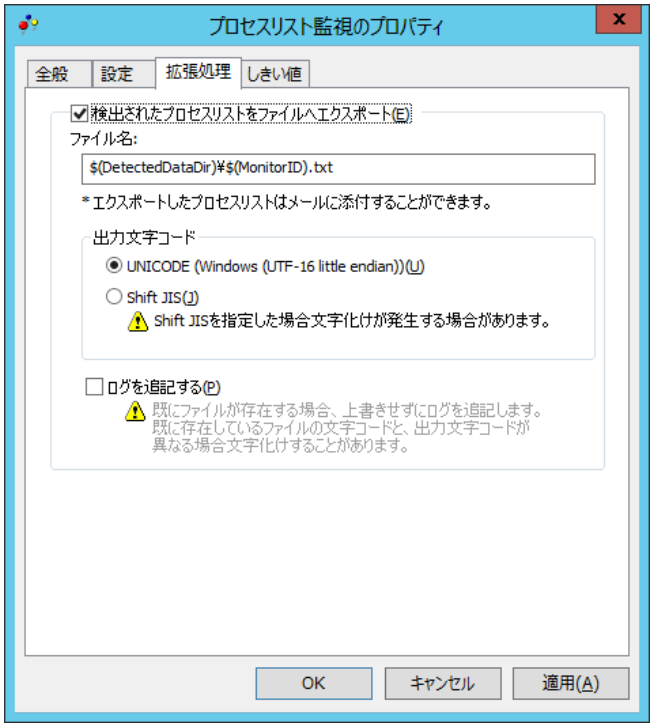
●“System Idle Process”は、“Idle”と表示されますのでご注意ください。

3. “実行中のプロセス”の最新“プロセス数”を表示するには、[最新のプロセス情報に更新]ボタンをクリックします。

4. “監視対象リスト”に登録したプロセス名を編集する場合は、該当“プロセス名”をダブルクリックするか、

[編集..]ボタンをクリックすることで、“プロセスの編集”画面を表示させ編集することができます。

C.「拡張処理」タブ



監視結果を調査する際や、監視結果を電子メールで送信する場合、“検出されたプロセスリストをファイルへエクスポート”にチェックを入れることで、下記の通り該当するプロセス名をテキストファイルに出力することができます。

●テキストファイル

下記のフォルダー・ファイル名で、テキストファイルを出力することができます。

フォルダー： <BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Instance¥<インスタンス名>¥DetectedData¥

ファイル名： GRPxxMONyy.txt （xx:グループ ID、yy:監視項目 ID を表します。）

●エクスポートファイルの“出力文字コード”を、“UNICODE”ラジオボタンもしくは“Shift JIS”ラジオボタンより選択することができます。

エクスポートするファイルが既に存在する場合、古いファイルは上書きしますが、“ログを追記する”チェックボックスにチェックを入れることで、古いファイルに追記することができます。

●この機能を使用すると、エクスポートするファイルが肥大化する場合がありますのでご注意ください。

●この機能を使用しますと、監視間隔毎に監視結果および、仕切り線“----------”がエクスポートしたファイルへ追記されます

●ブラックリスト監視の出力内容

ブラックリストプロセス監視の“監視対象リスト”に登録されている“プロセス”が起動していた場合、

該当する“プロセス名”をテキストファイルに記述します

例:

ブラックリストプロセス監視で指定したプロセスが、“notepad”の場合

プロセス“notepad”を検知した場合、テキストファイルに記述されるプロセス名は“notepad”です。

●ホワイトリスト監視の出力内容

ホワイトリストプロセス監視の“監視対象リスト”に登録されていない“プロセス”が起動していた場合、
該当する“プロセス名”をテキストファイルに記述します。
なお、“プロセス数”を指定していた場合には、“プロセス数”を超えた“プロセス名”を列挙します。

例:
ホワイトリストプロセス監視で指定したプロセスが、“notepad”かつ“プロセス数 2”の場合
プロセス“notepad”のプロセス数が“5”を検知した場合、テキストファイルに記述される
プロセス名は“notepad”、“notepad”、“notepad”と 3 つ列挙されます。

D.「しきい値」タブ

●ブラックリストプロセス監視の監視は、ブラックリスト(“監視対象リスト”)に登録した“プロセス”が、
監視実行時に起動している“プロセス数”を、監視結果とします。

例:
ブラックリスト(“監視対象リスト”)に“notepad”を登録の場合
監視時に“notepad”が“3 個”起動していた場合、監視結果は“3”です。

●ホワイトリストプロセス監視の監視は、ホワイトリスト（“監視対象リスト”）に登録した
プロセス（指定した個数も含めて）以外の監視実行時に起動している“プロセス数”を、監視結果とします。

例：
ホワイトリスト（“監視対象リスト”）中に“notepad”を“プロセス数 2 個”登録の場合
監視時のホワイトリスト（“監視対象リスト”）以外のプロセス“EXCEL”が“1 個”、
“notepad”が“3 個”起動していた場合、監視結果は“2”です。

1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。
   ●しきい値
   テキスト入力フィールドに数値（“0”～“999”）を入力します。
   しきい値の判定条件で“より小さい”を選択した場合には、数値に“0”を入力することができません。
   手順 2.で“連続した N 回目の注意から”を選択した場合には、数値に“1”～“99”しか入力できません。
   ●しきい値の判定条件
   ドロップダウンメニューを使用して、しきい値に対する判定条件を、
   “と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”の中から選択します。
2. “危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。
   ●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

E. 補足事項

●ホワイトリストプロセス監視を実行した際は BOM 7.0 以外のプロセスを対象とします。

BOM 7.0 が使用する下記のプロセスは、“実行中のプロセス”リストから除外されて監視が実行されます。

No	プロセス名	No	プロセス名	No	プロセス名
1	BomAgent.exe	26	BomOraMon.exe	51	MxDeployWizard.exe
2	BomAlProcMon.exe	27	BomPLink.exe	52	MxEvtlogMon.exe
3	BomArchiveDBAccess.exe	28	BomPSftp.exe	53	MxLinuxAct.exe
4	BomArchiveService.exe	29	BomPutEventLog.exe	54	MxLinuxMon.exe
5	BomArcMailPop.exe	30	BomQfeList.exe	55	MxLogViewer.exe
6	BomArcMailSmtp.exe	31	BomSNMPGet.exe	56	MxMail.exe
7	BomArcMailUnreachedChecker.exe	32	BomSNMPManager.exe	57	MxPerfMon.exe
8	BomBackupConfig.exe	33	BomSNMPUsmEncrypt.exe	58	MxProcListMon.exe
9	BomBackupService.exe	34	BomSNMPWizard.exe	59	MxSysConf.exe
10	BomCmd.exe	35	BOMSQLMon.exe	60	MxSysMon.exe
11	BomCmdInstance.exe	36	BomSQLServerMon.exe	61	MxTrap.exe
12	BomCmdLogtxt.exe	37	BomStatusViewer.exe	62	MxTxtlogMon.exe
13	BomCMon.exe	38	BomSwitchB.exe	63	MxTxtlogMonOpt.exe
14	BomCMonSub.exe	39	BomVer.exe	64	MxTxtlogMonOpt.exe
15	BomComExec.exe	40	BomVmAct.exe	65	MxWmiMon.exe
16	BomCsvImporter.exe	41	BomVmLogViewer.exe	66	ReportDisigner.exe
17	BomDBMon64.exe	42	BomVmMon.exe	67	ReportETL.exe
18	BomEasySettingWizard.exe	43	BomVmReportCreater.exe	68	ReportPrinter.exe
19	BomFindFiles.exe	44	BomWtsMon.exe	69	ReportPrintWizard.exe
20	BomHelper.exe	45	ccmenu.exe	70	ReportSetting.exe
21	BomHistoryMon.exe	46	ESM_BOM_Reg.exe	71	SendMessageWts.exe
22	BomImail.exe	47	ExShutdown.exe	72	SendPopup.exe
23	BomInstSwMon.exe	48	LogoffSessionWts.exe	73	SMARTMon.exe
24	BomMonScheduler.exe	49	MxAdminSub.exe		
25	BomNetMon.exe	50	MxDeployConfUI.exe		

5 .10 .13 イベントログ監視

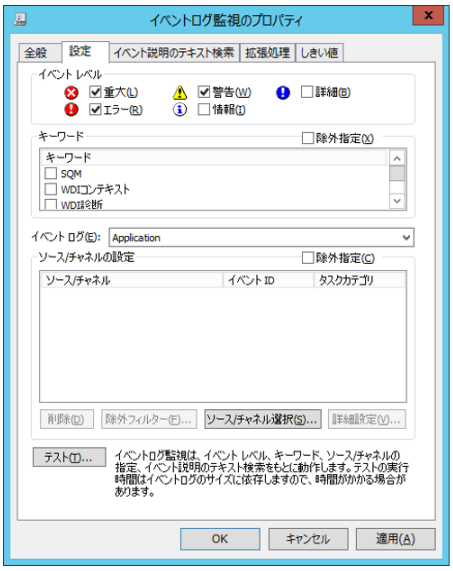
OS 標準のイベントビューアーには多種多様のイベントが記述されますが、BOM 7.0 のイベントログ監視は管理者が必要とするイベントログをフィルタリングしてイベントログの件数やリストを出力します。

A.「全般」タブ

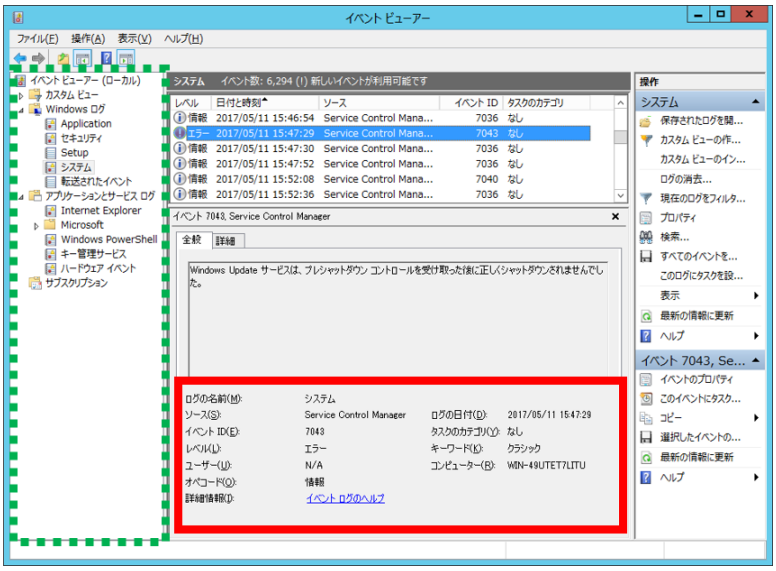
「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ

●同一“ソース名”で同一“イベント ID”が複数存在する場合、選択した同一“イベント ID”はすべて監視対象になります。
同一“イベント ID”で“メッセージ”が違うイベントのみを監視対象にする場合は、後述の「イベント説明のテキスト検索」タブで、対象となる“メッセージ”を絞り込んでください。



↑イベントログ監視の設定画面



↑OS のイベントビューアー画面

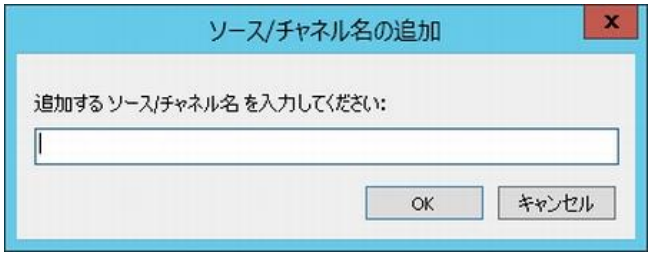
上図は“イベントログ監視”の設定画面（左）と OS のイベントビューアー画面（右）を表示しています。
右側の赤い実線部分で記述されている内容が左側の BOM 7.0 の設定画面でのフィルタリングで設定する内容です。

1. “イベント レベル”フィールドでは、“重大”、“警告”、“詳細”、“エラー”、“情報”の 5 種類からフィルタリングしたいレベルを選択します。
2. “キーワード”フィールドでは、“キーワード”リストから該当する“キーワード”を選択してフィルタリングします。
   ●“キーワード”フィールドの“除外指定”チェックボックスのチェックを外した場合
   選択指定 ： 選択した“キーワード”に該当するイベントログのみをフィルタリングします。
   ●“キーワード”フィールドの“除外指定”チェックボックスにチェックを入れた場合
   除外指定 ： 選択した“キーワード”に該当するイベントログを除外してフィルタリングします。
3. “イベント ログ”フィールドのドロップダウンリストには、上記イベントビューアー画面（右）の左側（緑の点線で囲ってある部分）の

“Windows ログ”と“アプリケーションとサービスログ”に表示されているログファイル“Application”、“セキュリティ”といったイベントログの種別が表示されます。

4. “ソース/チャネルの設定”フィールドでは、手順 3.で指定した“イベント ログ”から、さらに細かく“ソース/チャネル”を選択する場合に、[ソース/チャネル選択]ボタンをクリックすると、“ソース/チャネル選択”画面が表示されます。
   なお、“ソース/チャネルの設定”フィールドに表示された“ソース/チャネル”を選択後、[詳細設定]ボタンをクリックすると、手順 8.の、“イベントログ詳細設定”画面を表示させることができます。
   また、“除外指定”チェックボックスにチェックを入れると、[除外フィルター]ボタンが有効となります。このボタンおよび除外フィルター機能の詳細については ‘C 除外フィルター’ を参照してください。
   ●“ソース/チャネルの設定”フィールドの“除外指定”チェックボックスのチェックを外した場合
   選択指定 ： 選択した“ソース/チャネル”に該当するイベントログのみをフィルタリングします。
   ●“ソース/チャネルの設定”フィールドの“除外指定”チェックボックスにチェックを入れた場合
   除外指定 ： 選択した“ソース/チャネル”に該当するイベントログを除外してフィルタリングします。

5. “ソース/チャネル選択”画面で、現在監視対象コンピューターに登録されているソース/チャネルリストから、監視する対象の“ソース/チャネル”にチェックを入れます。監視対象の“ソース/チャネル”は、複数選択することができます。
6. [件数取得]ボタンをクリックすると、現在イベントログに実際に出力されているソース・チャネルの件数（合計、重大、エラー、警告等）が表示されます。手順 5.のソース/チャネルリストからの選択時の参考にしてください。
   ●システムにあらかじめ登録していないアプリケーションやお客様独自アプリケーションからイベントログを書き出している場合、“ソース/チャネル選択”画面で最初はソース/チャネルが表示されませんが、[件数取得]ボタンをクリックするとソースが表示され、件数がカウントされることがあります。
7. [ソース/チャネルの追加]ボタンをクリックすると、“ソース/チャネル選択”画面のリストに表示されていない“ソース/チャネル”を、“ソース/チャネル名の追加”画面から登録することができます。



8. ソース/チャネルリストから 1 つを選択し、[詳細設定]ボタンをクリックすると、“イベントログ詳細設定”画面を表示させることができます。

9. [現在のイベントログから ID 取得]ボタンをクリックすると、現在イベントログに出力されているログから表示されているソース名を検索して、同一“ソース名”の“イベント ID”、“メッセージ”、“件数”、“イベント種類”、“タスクカテゴリ”をリスト表示します。

●表示された“イベント ID”をクリックすると、該当する“イベント ID”の“メッセージ”と“タスクカテゴリ”の内容が下部の“メッセージ”ボックスに表示されます。

10. [Windows に登録されているイベント ID 取得]ボタンをクリックすると、監視対象コンピューターに登録されているイベントログから表示されているソース名を検索して、同一“ソース名”の“イベント ID”,“メッセージ”をリスト表示します。

●表示された“イベント ID”をクリックすると、該当する“イベント ID”の“メッセージ”内容が下部の“メッセージ”ボックスに表示されます。

11. 手順 9.もしくは手順 10.で表示させたリストから、監視対象とする“イベント ID”のチェックボックスにをチェックを入れます。

“イベント ID”のチェックボックスにチェックを入れていくと、“イベント ID”フィールドに“イベント ID”が追加されていきます。

●“イベント ID”を複数指定する表記法

“イベント ID”フィールドに、“イベント ID”、または“イベント ID”範囲を、カンマ区切やハイフンで複数指定できます。

●条件を除外する表記方法

“イベント ID”フィールドに、“イベント ID”を入力する際に、“イベント ID”の先頭に“負符号”を入力します。

例:

“イベント ID”フィールドに 1-10,12,-4 と入力した場合、

イベント ID1～10,12 を監視対象にし、ID1～10 の中から ID4 を監視対象から外す

12. “タスクカテゴリ”フィールドにも手順 11.と同じように、“タスクカテゴリ”のチェックボックスにチェックを入れることで、設定を行うことができます。

13.設定終了後、その時点での該当する件数を[テスト..]ボタンより確認することができます。

●手順 4.のソース/チャネルの除外指定と、手順 11.の負記号を組み合わせた場合の監視結果は下記の通りです。

イベントログの除外指定	イベント ID を通常指定	イベント ID を負記号で指定
ON	指定したソース/チャネル以外を監視し、 指定したソース/チャネルのイベント ID は監視	指定したソース/チャネル以外を監視し、 指定したソース/チャネルの負記号で指定したイベント ID 以外を監視
OFF	指定したソース/チャネルのうち、 指定したイベント ID のみ監視	指定したソース/チャネルのうち、 負記号で指定したイベント ID 以外を監視

C. 除外フィルター

“ソース/チャネルの設定”フィールドで“除外指定”チェックボックスにチェックを入れた場合、“ソース/チャネルの設定”フィールドの[除外フィルター]ボタンが有効となり、このボタンから除外フィルター設定画面を表示できます。

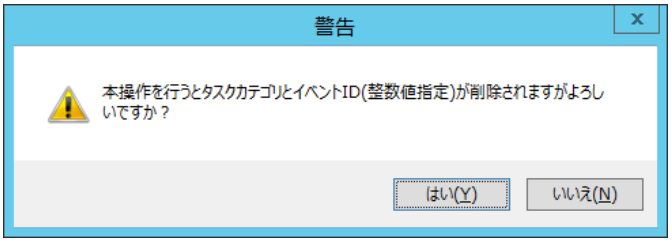
※　除外フィルター機能は、BOM 7.0 が収集したイベントログから除外対象を選択して指定するため、除外の判断ができる件数および種類のイベントログがあらかじめ収集されている必要があります。本機能は、一定期間イベントログ監視を実行し、イベントログを収集した上で実行してください。（収集されたイベントログとは、“ログ”ノード配下の“取集されたイベントログ”ノードに蓄積されているログを指します。）

ただし、他のインスタンスより除外設定ファイルをインポートする場合はこの限りではありません。

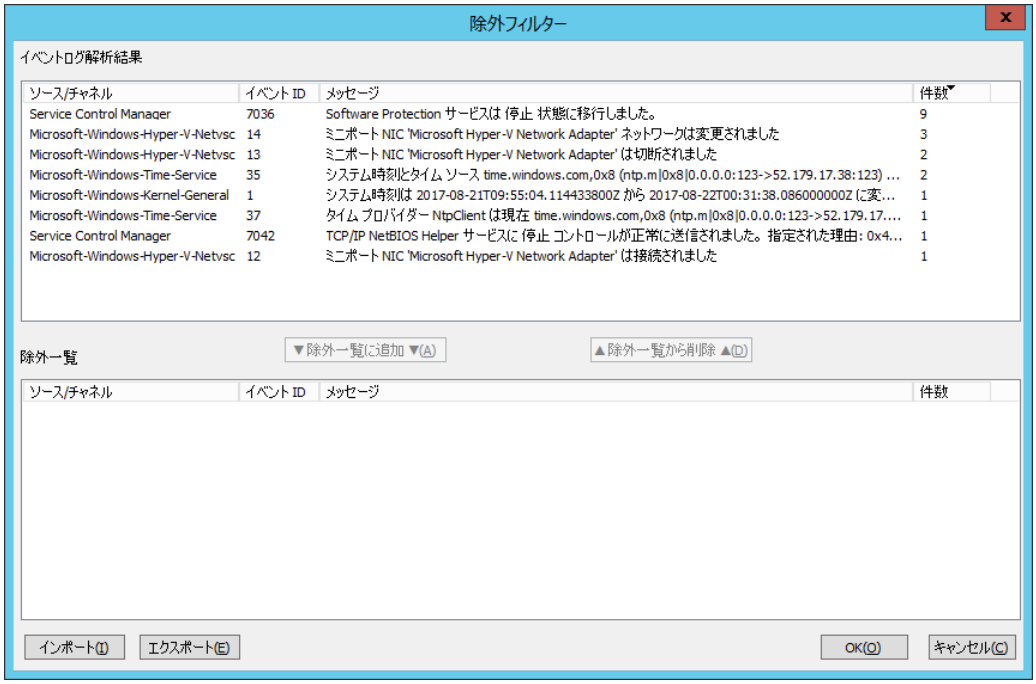
1. “ソース/チャネルの設定”フィールドで“除外指定”チェックボックスにチェックを入れ、[除外フィルター]ボタンをクリックします。
2. 以下の警告画面が表示されますので、除外フィルター機能を使用する場合は[はい]ボタンをクリックします。

※　すでに何らかの“ソース/チャネルの設定”が登録されている場合、除外フィルター機能を使用すると以下の登録内容は削除されます。問題がある場合は[いいえ]ボタンをクリックしてください。

- イベント ID で「-」(マイナス)指定されているもの以外のソース/チャネル指定
- タスクカテゴリの設定



3. 除外フィルター画面が表示されます。

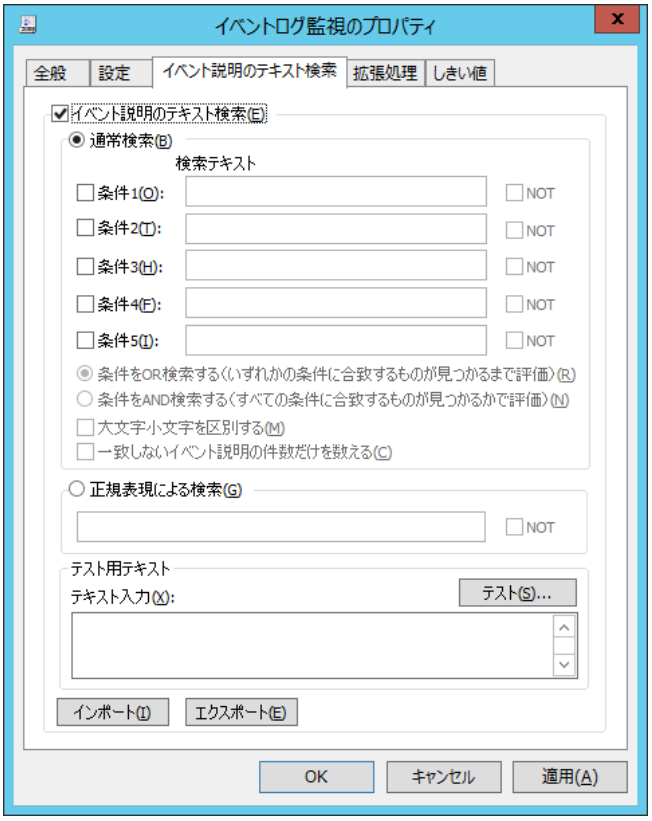


4. “イベントログ解析結果”フィールドに BOM 7.0 が収集したイベントログが一覧表示されます。
   除外したいイベントログを選択し、[▼除外一覧に追加▼]ボタンをクリックすると、選択したイベントログが“除外一覧”フィールドに移動し、除外の対象となります。
5. “除外一覧”フィールドには除外指定されたイベントログの一覧が表示されます。
   除外対象から外したいイベントログを選択し、[▲除外一覧から削除▲]ボタンをクリックすると、選択したイベントログが“イベントログ解析結果”フィールドに移動し、除外の対象から外れます。
6. [エクスポート]ボタンをクリックすると、除外フィルターの設定を“.json”形式のファイルにエクスポートできます。
7. [インポート]ボタンをクリックすると、他のインスタンスから“.json”形式でエクスポートした除外フィルターの設定をインポートできます。

D.「イベント説明のテキスト検索」タブ

イベントログのテキストを検索する場合、“イベント説明のテキスト検索”チェックボックスにチェックを入れます。

イベントログの“説明文”に対し、検索テキストに指定した文言条件に該当するイベントログを抽出します。



1. “通常検索”ラジオボタンを選択して下記を設定すると、テキスト検索が行えます。設定できる内容は下記の通りです。

●“条件 1”～“条件 5”

チェックをつけて検索キーワードを入力します。

●“NOT”

検索テキストに合致しないものを検索したい場合にチェックを入れます。

条件ごとの判定であるため、例えば NOT“1” or NOT“2” は、“(NOT“1”) or (NOT“2”)”という条件になり、“1”だった場合は NOT“2”で検知され、“2”だった場合は NOT“1”で検知されます。

1 でも 2 でもない値を検知させたい場合には NOT“1” and NOT“2”で指定します。

●“条件を OR 検索する”

“条件 1”～“条件 5”までの条件が 1 つでも合致した際に抽出したい場合、“条件を OR 検索する”ラジオボタンを選択します。

●“条件を AND 検索する”

“条件 1”～“条件 5”までの条件が 5 つすべて合致した際に抽出したい場合、“条件を AND 検索する”ラジオボタンを選択します。

●“大文字小文字を区別する”

半角英文字の大文字小文字を区別して検索を行いたい場合にチェックを入れます。

●“一致しないイベント説明の件数だけを数える”

“条件 1”～“条件 5”と、“条件を OR 検索する”、あるいは“条件を AND 検索する”で設定した検索キーワードに一致しない件数だけを抽出したい場合にチェックを入れます。

2. “正規表現による検索”ラジオボタンを選択し、“正規表現”フィールドにキーワードを入力すると（最大文字数は 1024 文字）正規表現による検索が行えます。

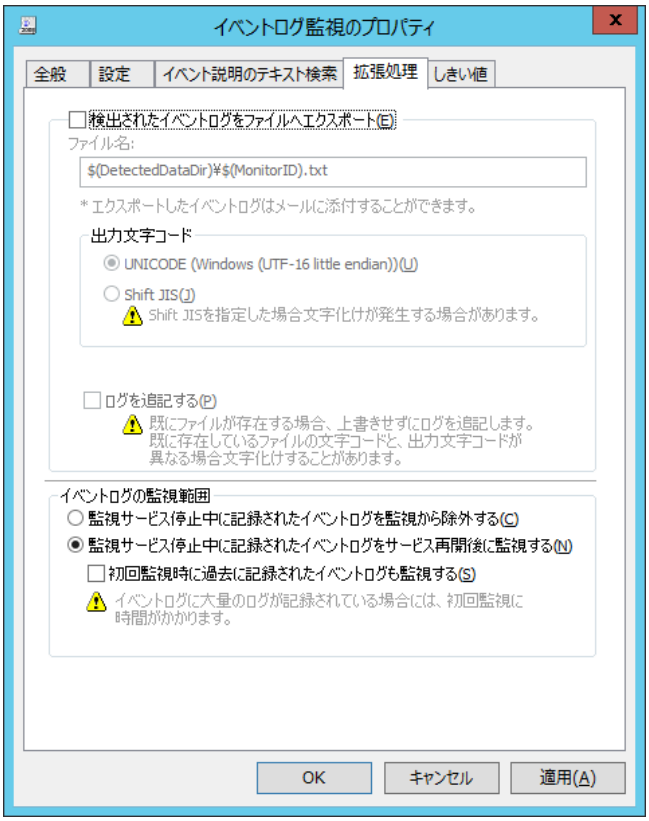
●正規表現とは、文字列の集合をパターンマッチ文字列で表現する方法であり、文字列から特定のパターンをもった文字列を抽出するときに使います。正規表現の詳細については、Web や書籍等を参照ください。

ここではパターンマッチ文字列のリストと特殊文字のリストを記載します。

パターンマッチ文字列	意味
¥	次に続く文字列を特殊文字、後方参照、リテラル文字列、8 進文字として解釈。
.	¥n 以外の任意の 1 文字。
^	先頭文字。
$	終端文字。
*	直前の文字または式の 0 回以上の繰り返し。
+	直前の文字または式の1回以上の繰り返し。
?	直前の文字または式の 0 回または 1 回の繰り返し。
{*n*}	直前の文字または式の n 回の繰り返し。
{*n*,}	直前の文字または式の n 回以上の繰り返し。
{*n*,*m*}	直前の文字または式の n 回以上 m 回以下の繰り返し。
?	*、+、?、{n}、{n,}、{n,m}のいずれかの後に付けると最小一致になる。
(*pattern*)	グループ化を定義。pattern に一致するとともに一致した文字列を記憶。
(?:*pattern*)	グループ化を定義。pattern に一致するが文字列は記憶しない。
(?=*pattern*)	pattern で指定した文字列が続く場合一致（肯定先読み）。
(?!*pattern*)	pattern で指定した文字列が続かない場合一致（否定先読み）。
x|*y*	x か y に一致。
[*xyz*]	カッコ内の任意の 1 文字（ここでは x か y かz）に一致。
[^*xyz*]	カッコ内のすべての文字に一致しない文字列（ここでは x、y、z 以外）に一致。
[*a*-*z*]	文字範囲に一致（ここでは、a、b、c、....、x、y、z）。
[^*a*-*z*]	文字範囲に含まれない文字に一致。
¥*n*	後方参照または 8 進数値。
¥0*n*	8 進数値。
¥x*nn*	16 進数値。
¥x{*nn*}	UNICODE16 進数値。
¥c*X*	コントロールコード
¥X*n*	UNICODE 文字。

3. [エクスポート]ボタンをクリックすると、「イベント説明のテキスト検索」タブの設定内容を“.json”形式のファイルにエクスポートできます。
4. [インポート]ボタンをクリックすると、“.json”形式でエクスポートした「イベント説明のテキスト検索」タブの設定内容をインポートできます。

E.「拡張処理」タブ



1. 監視結果を調査する際や、監視結果を電子メールで送信する場合、“検出されたイベントログをファイルへエクスポート”にチェックを入れることで、検出されたイベントログを下記の通りテキストファイルに出力することができます。

   ●テキストファイル

   下記のフォルダー・ファイル名で、テキストファイルを出力することができます。

   フォルダー：<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Instance¥<インスタンス名>¥DetectedData¥

   ファイル名：GRPxxMONyy.txt　　（xx:グループ ID、yy:監視項目 ID を表します。）

   ●エクスポートファイルの“出力文字コード”を、“UNICODE”ラジオボタンもしくは“Shift JIS”ラジオボタンより選択することができます。
2. エクスポートするファイルが既に存在する場合、古いファイルは上書きしますが、“ログを追記する”チェックボックスにチェックを入れることで、古いファイルに追記することができます。

   ●“検出されたイベントログをファイルへエクスポート”設定をした場合、書き出す件数は最大で 10 万件です。

   ●この機能を使用すると、エクスポートするファイルが肥大化する場合がありますのでご注意ください。
3. “イベントログの監視範囲”フィールドでは、BOM 監視サービスが停止した時、あるいは監視を無効に設定した時に出力されたイベントログの監視の要否を設定することができます。

●“監視サービス停止中に記録されたイベントログを監視から除外する”ラジオボタンを選択した場合

BOM 監視サービスが停止中に記録されたイベントログは切り捨て、監視サービスが実行中に記録されたイベントログのみを監視範囲に指定します。

●“監視サービス停止中に記録されたイベントログをサービス再開後に監視する”ラジオボタンを選択した場合

BOM 監視サービスが停止中に記録されたイベントログは、BOM 監視サービスを起動した際に監視範囲に含めるため、BOM 監視サービスが停止中に発生した障害も検知することができます。

既定値は“監視サービス停止中に記録されたイベントログをサービス再開後に監視する”ラジオボタンが選択されています。

●監視サービスが停止した後に監視が再開された際の監視範囲の相関表は下記の通りです。

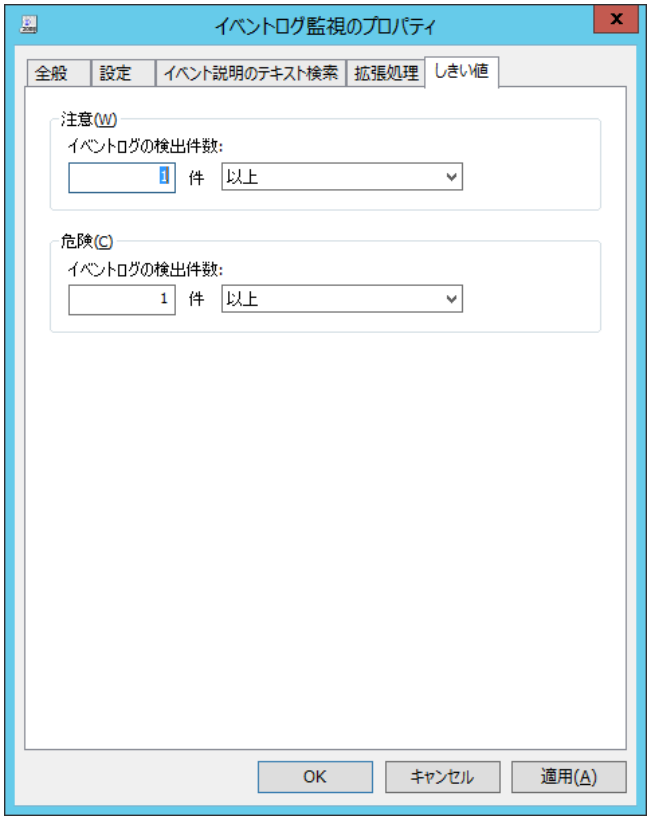
対象	監視サービスの制御方法	“監視から除外する”を選択	“再開後に監視する”を選択
監視グループ	プロパティ画面の有効/無効	監視無効期間のログ検知	監視無効期間のログ検知
	監視　有効/無効アクション	監視無効期間のログ検知	監視無効期間のログ検知
	スケジュール機能	監視無効期間のログ検知	監視無効期間のログ検知
監視項目	プロパティ画面の有効/無効	監視無効期間のログ検知なし	監視無効期間のログ検知
	監視　有効/無効アクション	監視無効期間のログ検知なし	監視無効期間のログ検知

4. “初回監視時に過去に記録されたイベントログも監視する”をチェックした場合、イベントログ監視項目を新規作成し、初回の監視実行時に、今までに出力されたすべてのイベントログを監視範囲に含めることができます。

●この機能を使用すると、イベントログファイルのサイズによっては初回監視時に実行時間が掛かりますのでご注意ください。

●過去のイベントログメッセージに含まれている一部のセキュリティ ID が、名前に変換されない場合があります。

F.「しきい値」タブ



1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

●しきい値

テキスト入力フィールドに数値(“0”～“999”)を入力します。

しきい値の判定条件で“より小さい”を選択した場合には、数値に“0”を入力することができません。

手順 2.で“連続した N 回目の注意から”を選択した場合には、数値に“1”～“99”しか入力できません。

●しきい値の判定条件

ドロップダウンメニューを使用して、しきい値に対する判定条件を、

“より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

2. “危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

●「設定」タブのプロパティを開き、[OK]ボタンをクリックするまでは設定が正常に保存されませんのでご注意ください。

5 .10 .14 テキストログ監視

監視対象コンピューターの指定したテキストログの内容をテキスト検索して監視します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ

1. “ファイル名”フィールドに、監視対象の“ファイル名”をどちらかの手段で設定します。

   ●入力する場合

   監視対象のファイルを、絶対パスで入力します。

   ●[参照]ボタンより設定する場合

   [参照]ボタンをクリックすると、“ファイル選択”画面が表示され、監視対象のファイルを指定します。

2. 監視対象テキストファイルの“文字コード”の種類と、ファイル内で使用されている“改行コード”の種類を選択します。
3. “検索開始位置”は下記のどちらかを選択します。

   ●“常にファイルの先頭から”ラジオボタンを選択した場合

   初回の監視時も含め、毎回ファイルの先頭から監視を行います。

   ●“前回の監視終了位置から”ラジオボタンを選択した場合

   監視対象ファイルの更新日時が前回監視実行時よりも新しい場合、かつ前回監視実行時の最終位置から検索します。

   前回監視実行時のファイルの中身が入れ替わっている場合にはファイルの先頭から検索します。

   初回の監視動作は最終ファイル位置を検索するため監視を行わず、2 回目以降の監視より監視を実行します。

4. “リトライ”フィールドでは、BOM 7.0 がテキストファイルを監視する間隔と試行回数を指定します。

   ●リトライが起こる原因としては検索対象のファイルを示すディレクトリが存在しない場合、リネームをされた場合等があります。

C.「テキスト検索」タブ

1. “通常検索”ラジオボタンを選択して下記を設定すると、テキスト検索が行えます。設定できる内容は下記の通りです。

   ●“条件 1”～“条件 5”

   チェックをつけて検索キーワードを入力します。

●“NOT”

検索テキストに合致しないものを検索したい場合にチェックを入れます。

条件ごとの判定であるため、例えば NOT“1” or NOT“2” は、“(NOT“1”) or (NOT“2”)”という条件になり、“1”だった場合は NOT“2”で検知され、“2”だった場合は NOT“1”で検知されます。

1 でも 2 でもない値を検知させたい場合には NOT“1” and NOT“2”で指定します。

●“条件を OR 検索する”

“条件 1”～“条件 5”までの条件が 1 つでも合致した際に抽出したい場合、“条件を OR 検索する”ラジオボタンを選択します。

●“条件を AND 検索する”

“条件 1”～“条件 5”までの条件が 5 つすべて合致した際に抽出したい場合、“条件を AND 検索する”ラジオボタンを選択します。

●“大文字小文字を区別する”

半角英文字の大文字小文字を区別して検索を行いたい場合にチェックを入れます。

●“一致しないイベント説明の件数だけを数える”

“条件 1”～“条件 5”と、“条件を OR 検索する”、あるいは“条件を AND 検索する”で設定した検索キーワードに一致しない件数だけを抽出したい場合にチェックを入れます。

2. “正規表現による検索”ラジオボタンを選択し、“正規表現”フィールドにキーワードを入力すると（最大文字数は 1024 文字）正規表現による検索が行えます。

●正規表現の解説とパターンマッチ文字列のリストと特殊文字のリストは、

‘5 .10 .13 イベントログ監視’の項目‘D 「イベント説明のテキスト検索」タブ’を参照ください。

3. [テスト]ボタンをクリックすると、下記の対象に対して、「テキスト検索」タブの検索条件のテスト実行を行うことができます。（テスト実行でのタイムアウト時間は 2 分です。）

●“設定タブで指定されたテキストログファイル”ラジオボタンを選択している場合

「設定」タブの“ファイル名”フィールドで選択したファイルに対して、テストを実行します。

●“テキスト入力”ラジオボタンを選択している場合

“テキスト入力”ラジオボタン下部の空の“テキストボックス”に内容を入力して、テストを実行します。

D.「拡張処理」タブ

1. 監視結果を調査する際や、監視結果を電子メールで送信する場合、“検出されたテキストログをファイルへエクスポート”にチェックを入れることで、検出されたテキストログを下記の通りテキストファイルに出力することができます。

- テキストファイル

  下記のフォルダー・ファイル名で、テキストファイルに出力することができます。

  フォルダー：<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Instance¥<インスタンス名>¥DetectedData¥

  ファイル名：GRPxxMONyy.txt　（xx:グループ ID、yy:監視項目 ID を表します。）

- テキストログ監視で出力できるテキストファイルの最大行数は、ファイルの先頭から 10 万行です。
- “出力文字コード”は、“UNICODE”ラジオボタンもしくは“Shift JIS”ラジオボタンより選択することができますが、改行コードは CRLF でエクスポートファイルを出力します。
- 出力形式は以下の例の通りで、変更はできません。

  カッコつきの※印部分は注記のため、実際の出力には存在しません。

  出力例：“c:¥textlog¥logfile.log(※1)”,”2020/04/06 18:52:55(※2)”,”+0900(※3)”,”2020/04/07 17:24:52(※4)”,”+0900(※5)”,1(※6),”System error(※7)”

※1	テキストログファイル名(格納パス含む)	※5	4 のタイムゾーン
※2	監視対象ファイル生成時刻	※6	対象文字列を検出した行番号
※3	2 のタイムゾーン	※7	検出行文字列
※4	監視対象ファイル最終更新時刻		

E.「しきい値」タブ

1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

   ●しきい値

   テキスト入力フィールドに数値(“0”～“999”)を入力します。

   しきい値の判定条件で“より小さい”を選択した場合には、数値に“0”を入力することができません。

   手順 2.で“連続した N 回目の注意から”を選択した場合には、数値に“1”～“99”しか入力できません。

   ●しきい値の判定条件

   ドロップダウンメニューを使用して、しきい値に対する判定条件を、

   “より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

2. “危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

   ●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

F. ワイルドカードを指定した場合の監視動作

1. テキストログ監視の対象ファイル名はワイルドカード(*、?)指定ができますが、指定できる対象ファイル名は
   ログローテーション等による下記の形式の規則的なファイルのみです。

形式	前回監視時	次回監視時	備考
リング形式 ※ファイルは上書き	SampleLog.SUN SampleLog.MON SampleLog.TUE SampleLog.WED SampleLog.THU SampleLog.FRI SampleLog.SAT	SampleLog.SUN SampleLog.MON SampleLog.TUE SampleLog.WED SampleLog.THU SampleLog.FRI SampleLog.SAT	曜日により上書き更新のファイルが変わる。 曜日の代わりに数字の場合もある。
連番追加形式 連番で新しいファイルが追加	Log20040501.dat Log20040502.dat Log20040503.dat Log20040504.dat	Log20040501.dat Log20040502.dat Log20040503.dat Log20040504.dat Log20040505.dat	一定期間ごとにファイルは破棄される。 日時を含むファイル名、 番号を含むファイル名が多い ←Log20040505.dat が新規追加
シフト形式 連番で古いファイルのファイル名がシフトしていく形式	SampleLog.000 SampleLog.001 SampleLog.002 SampleLog.003 : SampleLog.098 SampleLog.099	SampleLog.000 SampleLog.001 SampleLog.002 SampleLog.003 SampleLog.004 : SampleLog.099 破棄	←前回監視時の SampleLog.000 は、 次回監視時には SampleLog.001 にシフト (前回 SampleLog.001 以降も同様にシフト) ←常にファイルは追加され、一定数を超えた 古いファイル(前回 SampleLog.099)は シフトされずに破棄される。 ←次回監視時の SampleLog.000 が新規追加

2. ワイルドカード指定の場合、前回監視情報を持つファイルかどうかを、前回監視情報にあるファイル名と、
   該当監視ファイル名を比較して自動で判別します。
   ●検索対象ファイルが前回監視情報を持つ場合
   差分監視を行います。
   ●検索対象ファイルが前回監視情報を持たない場合
   全文検索を行います。
3. ワイルドカード指定時における、複数の対象ファイルが存在した場合の検索順序
   ●ワイルドカード指定時の検索順序と、上記 2.の前回監視情報については、関係がありません。
   ●同時刻に複数ファイルが書き込まれた場合、ファイルシステムの順序に従って検索順序が決まります。

4. ワイルドカード指定時における、リング形式でローテーションする複数の対象ファイルが存在した場合の検索順序

●リング形式でローテーションする際に、同時刻にファイルを複数リング形式の最初のファイルに戻すテキストログの場合

検索順序の最後が前回監視情報のあるファイルになることがあります。

例：“Sample.SUN”～“Sample.SAT”で、“Sample.SAT”から“Sample.SUN”に戻る場合

次回の監視はリング形式の最初のファイル“Sample.SUN”の先頭から監視が実行されます。

●リング形式のローテーションファイルで日が跨る異なるファイルの場合

ファイルは上書き保存する形式にのみ対応しております。

例：

“Sample.SUN”～“Sample.SAT”まで記述して、再び“SampleLog.SUN”に書き込む場合

“SampleLog.SUN”は、前回のデータを消去して記述する必要があります。

G. 監視対象ファイルが存在しなかった場合の監視動作

BOM 7.0 で監視対象のファイル（単一指定時、ワイルドカード指定時）が存在しない場合の監視結果は、下記の通りです。

・ステータス　：　正常

・値　　：　(N/A)

・コード　　：　1

H. 検索開始位置で“前回の監視終了位置から”ラジオボタンを選択した上で、監視が失敗した場合の監視動作

1. 本監視動作を満たす条件は、「設定」タブの検索開始位置で“前回の監視終了位置から”ラジオボタンを選択しており、かつ、ファイルが存在しなかった以外の何かしらの理由で監視が失敗した場合です。

●“前回の監視終了位置から”ラジオボタンを選択した場合、初回の監視動作は最終ファイル位置を検索するため監視を行わず、2 回目以降の監視より監視を実行します。

●“前回の監視終了位置から”ラジオボタン選択時の詳細は、‘5 .10 .14 テキストログ監視’の項目である‘B.「設定」タブ’を参照ください。

2. 初回のテキストログ監視時に、何かしらの理由で監視が失敗した場合、次回以降の監視でファイルを検知できた時点を起点として、以降の検出を行います。

3. 1 度でも監視が成功している場合、かつ、仮に何かしらの理由でそれ以降の監視が失敗した場合、次回監視時に監視が成功した際には、差分を正常に検出した上で監視結果を返します。

例：

上記を実際の監視に当てはめると、下記の通りです。

①回目の監視時に監視対象ファイルの排他制御が原因で監視が失敗

②回目が初回監視となり、次回以降の監視の起点を特定

③回目の監視は②回目の起点より監視を行い成功したため、最終ファイル位置を更新

④回目の監視で再度ファイル排他中になり監視が失敗

⑤回目の監視は③回目の最終ファイル位置より監視を行い成功したため、最終ファイル位置を更新

監視回数	監視対象ファイル		監視結果		
	中身	状態	値	コード	補足解説
①回目	AAA BBB	排他中	（N/A）	0x80070020	・左記コードはファイル排他時のエラーコードであり、 エラー原因により出力されるコードが異なります。
②回目	AAA BBB CCC	排他解除	0	0	・初回の監視時には最終ファイル位置を検索し 監視自体は行わないため、値は“0”になります。 ・CCC の後に次回以降の監視起点を設定します。
③回目	AAA BBB CCC DDD	排他解除	1	0	・③回目の監視は、CCC 終了時点が監視の 起点のため、DDD を検知し、値は“1”になります。 ・DDD の後に次回以降の監視起点を設定します。
④回目	AAA BBB CCC DDD EEE	排他中	（N/A）	0x80070020	・左記コードはファイル排他時のエラーコードであり、 エラー原因により出力されるコードが異なります。
⑤回目	AAA BBB CCC DDD EEE FFF	排他解除	2	0	・⑤回目の監視は、③回目の監視成功時の DDD 終了時点が監視の起点のため、 EEE、FFF を検知し、値は“2”になります。 ・FFF の後に次回以降の監視起点を設定します。

5 .10 .15 BOM ヒストリー監視

BOM ヒストリー監視では、BOM 7.0 が出力するヒストリーログを監視します。

A.「全般」タブ

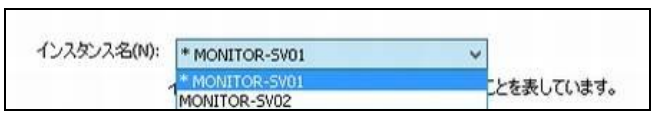
「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ

1. “インスタンス名”フィールドには、監視したいヒストリーログを保有する“インスタンス”を指定します。

   ●BOM マネージャーに複数のインスタンスを登録している場合、BOM ヒストリー監視は他のインスタンスのヒストリーログも監視対象にすることができます。その際に、BOM ヒストリー監視を設定する自分自身のインスタンスが簡単に識別できるように、インスタンス名の先頭に“*”が表示されます。

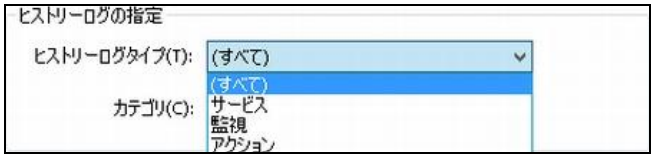
   ●代理監視など、同一コンピューター内に存在する別のインスタンスを監視対象に設定することができます。



2. “種類”フィールドには、BOM 7.0 が出力するヒストリーログのうち、監視対象にしたい“種類”を設定します。

3. “ヒストリーログタイプ”フィールドは、既定値で“（すべて）”です。

   ヒストリーログのタイプは、“サービス”、“監視”、“アクション”の 3 タイプより選択できます。



4. “カテゴリ”フィールドは、既定値で“（すべて）”です。

   手順 3.で、“ヒストリーログタイプ”を指定した場合に、“ヒストリーログタイプ”ごとに異なる“カテゴリ”を選択できます。

C. 「ヒストリーログのテキスト検索」タブ

1. “通常検索”ラジオボタンを選択して下記を設定すると、テキスト検索が行えます。設定できる内容は下記の通りです。

   ●“条件 1”～“条件 5”

   チェックをつけて検索キーワードを入力します。

   ●“NOT”

   検索テキストに合致しないものを検索したい場合にチェックを入れます。

   条件ごとの判定であるため、例えば NOT“1” or NOT“2” は、“(NOT“1”) or (NOT“2”)”という条件になり、“1”だった場合は NOT“2”で検知され、“2”だった場合は NOT“1”で検知されます。

   1 でも 2 でもない値を検知させたい場合には NOT“1” and NOT“2”で指定します。

●“条件を OR 検索する”

“条件 1”～“条件 5”までの条件が 1 つでも合致した際に抽出したい場合、“条件を OR 検索する”ラジオボタンを選択します。

●“条件を AND 検索する”

“条件 1”～“条件 5”までの条件が 5 つすべて合致した際に抽出したい場合、“条件を AND 検索する”ラジオボタンを選択します。

●“大文字小文字を区別する”

半角英文字の大文字小文字を区別して検索を行いたい場合にチェックを入れます。

●“一致しないイベント説明の件数だけを数える”

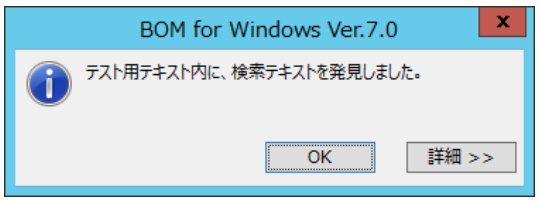
“条件 1”～“条件 5”と、“条件を OR 検索する”、あるいは“条件を AND 検索する”で設定した検索キーワードに一致しない件数だけを抽出したい場合にチェックを入れます。

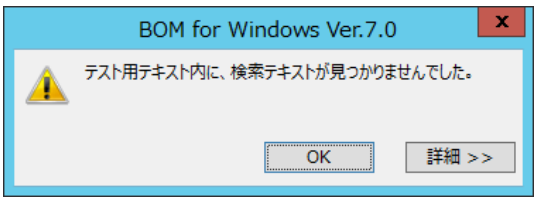
2. “正規表現による検索”ラジオボタンを選択し、“正規表現”フィールドにキーワードを入力すると（最大文字数は 1024 文字）正規表現による検索が行えます。

●正規表現の解説とパターンマッチ文字列のリストと特殊文字のリストは、

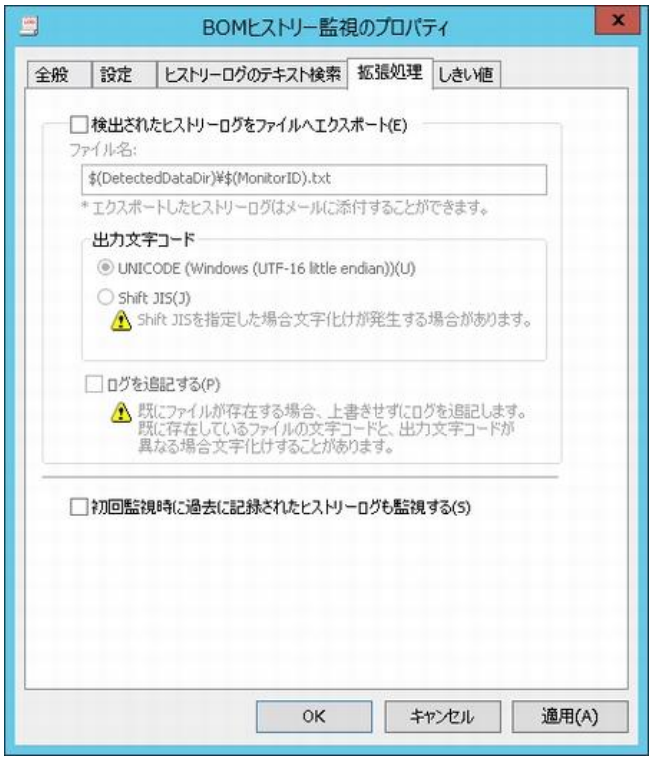
‘5 .10 .13 イベントログ監視’の項目‘D「イベント説明のテキスト検索」タブ’を参照ください。

3. “テキスト入力”フィールド下部の空の“テキストボックス”に内容を入力して、[テスト...]ボタンをクリックすると、「ヒストリーログのテキスト検索」タブの検索条件で、テスト実行を行うことができます。





D.「拡張処理」タブ



1. 監視結果を調査する際や、監視結果を電子メールで送信する場合、“検出されたヒストリーログをファイルへエクスポート”にチェックを入れることで、検出されたテキストログを下記の通りテキストファイルに出力することができます。

   ●テキストファイル

   下記のフォルダー・ファイル名で、テキストファイルを出力することができます。

   フォルダー：<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Instance¥<インスタンス名>¥DetectedData¥

   ファイル名：GRPxxMONyy.txt　（xx:グループ ID、yy:監視項目 ID を表します。）

   ●テキストログ監視で出力できるテキストファイルの最大行数は、ファイルの先頭から 10 万行です。

   ●エクスポートファイルの“出力文字コード”を、“UNICODE”ラジオボタンもしくは“Shift JIS”ラジオボタンより選択することができます。

2. エクスポートするファイルが既に存在する場合、通常は古いファイルを上書きしますが、“ログを追記する”チェックボックスにチェックを入れると、古いファイルに追記することができます。

   ●この機能を使用しますと、エクスポートするファイルが肥大化する場合がありますのでご注意ください。

3. “初回監視時に過去に記録されたイベントログも監視する”チェックボックスにチェックを入れると、BOM ヒストリー監視項目を新規作成した際の初回監視時にのみ、今までに出力されたすべての BOM ヒストリーログを監視範囲に含めます。

   ●この機能を使用すると、イベントログファイルのサイズによっては初回監視時に実行時間が掛かりますのでご注意ください。

E.「しきい値」タブ

1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

   ●しきい値

   テキスト入力フィールドに数値(“0”～“999”)を入力します。

   しきい値の判定条件で“より小さい”を選択した場合には、数値に“0”を入力することができません。

   手順 2.で“連続した N 回目の注意から”を選択した場合には、数値に“1”～“99”しか入力できません。

   ●しきい値の判定条件

   ドロップダウンメニューを使用して、しきい値に対する判定条件を、

   “より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

2. “危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

   ●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

5 .10 .16 Ping 監視

監視対象コンピューターから他のネットワーク機器や他のコンピューターに対して Ping によってネットワーク状態を監視します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ

1. “監視先”フィールドには、Ping 監視対象のコンピューターやネットワーク機器などの“IP アドレス”か“コンピューター名”を入力します。
2. “監視設定”は“平均レスポンス時間”ラジオボタンと“パケットロスト率”ラジオボタンのどちらかを選択します。

   ●“平均レスポンス時間”ラジオボタンを選択した場合

   Ping を“監視先”にリクエスト回数分実行した後のレスポンス時間の平均値を取得します。

   Ping を実行する条件は選択した“取得タイプ”フィールドの下の“パケットサイズ”、“タイムアウト時間”、“リクエスト回数”、“インターバル”を指定することによって設定します。

   ●“パケットロスト率”ラジオボタンを選択した場合

   Ping を“監視先”に実行した後のレスポンスでリクエスト回数のうち何回ロストしたかを%で取得します。
3. “パケットサイズ”、“タイムアウト時間”、“リクエスト回数”、“インターバル”で指定可能な値は下記の通りです。

   ●“パケットサイズ”:“1”～“65468”

   ●“タイムアウト時間”:“100”～“60000”

   ●“リクエスト回数”:“1”～“100”

   ●“インターバル”:“100”～“60000”
4. [現在値の取得]ボタンをクリックすると、“監視設定”フィールドの条件で値を取得します。
5. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

   ●しきい値

   テキスト入力フィールドに数値(パケットロスト率:“0”～“100”／平均レスポンス時間:“0”～“99999”)を入力します。

   しきい値の判定条件で“より小さい”を選択した場合には、数値に“0”を入力することができません。

   手順 6.で“連続した N 回目の注意から”を選択した場合には、数値に“1”～“99”しか入力できません。

●しきい値の判定条件

ドロップダウンメニューを使用して、しきい値に対する判定条件を、

“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

6. “危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

5 .10 .17 ポート監視

監視対象コンピューターの TCP・UDP ポートを監視します。

ポート監視では他の監視項目と違い、文字列が監視結果となっているため‘5 .8 .1 ログの表示’のグラフ表示はできません。

●UDP ポートを監視する場合、監視元コンピューターの Windows ファイアウォールを OFF にするか、Windows ファイアウォールの受信の規制で ICMP パケットを例外に追加する必要があります。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ

1. “監視先”の“ホスト名”フィールドに、ポート監視を実行する“ホスト名”あるいは“IP アドレス”を入力します。

●複数ネットワークカードがある場合、あるいは同一ネットワークカードに複数の IP アドレスを割り振っている場合には、監視対象の IP アドレスを指定してください。

2. “ポート番号”に、監視対象の“ポート番号”を指定します。

3. [参照]ボタンをクリックすると、ウェルノウンポート一覧が表示されます。

4. “監視設定”に、監視対象の“プロトコル”の種類と“ポート状態”を指定します。
5. [現在値の取得]ボタンをクリックすると、「設定」タブで指定した“プロトコル”の“ポート番号”が、
   “開いている”か“閉じている”かを確認することができます。
6. “注意”フィールドには、手順 4.で設定した“ポート状態”の条件に対する逆の状態を“注意”条件として自動設定します。
7. “危険”フィールドのしきい値に、“注意”ステータスの“連続発生回数”を指定します。
   ●連続回数に指定できるのは、“1”～“99”の数値です。

C. UDP ポート監視時の注意点

UDP パケットを送信したのち、下記の判断を順次行いポートの状態を決定しております。

●ICMP 到達不能メッセージ(type-3)を受信した場合

ポート“閉”状態

●受信タイムアウトした場合

Ping(echo request)を行い、Ping 応答(echo reply)があった場合、ポート“開”状態

Ping(echo request)を行い、Ping 応答(echo reply)がない(タイムアウト)の場合、ポート“閉”状態

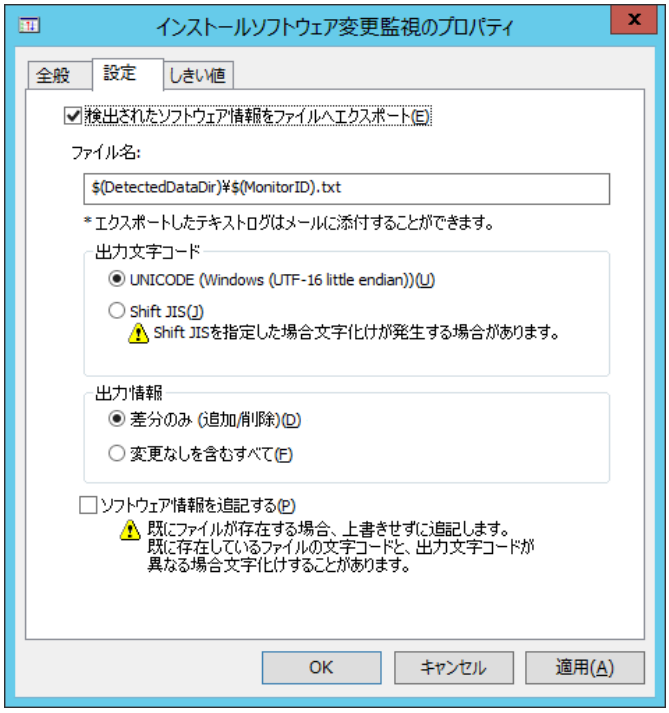
5 .10 .18 インストールソフトウェア変更監視

監視対象コンピューターのインストールされているソフトウェアの差分を検出し監視します。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「設定」タブ



1. 監視結果を調査する際や、監視結果を電子メールで送信する場合、“検出されたソフトウェア情報をファイルへエクスポート”にチェックを入れることで、検出されたソフトウェア情報を下記の通りテキストファイルに出力することができます。

   ●テキストファイル

   下記のフォルダー・ファイル名で、テキストファイルに出力することができます。

   フォルダー： <BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Instance¥<インスタンス名>¥DetectedData¥

   ファイル名： GRPxxMONyy.txt （xx:グループ ID、yy:監視項目 ID を表します。）

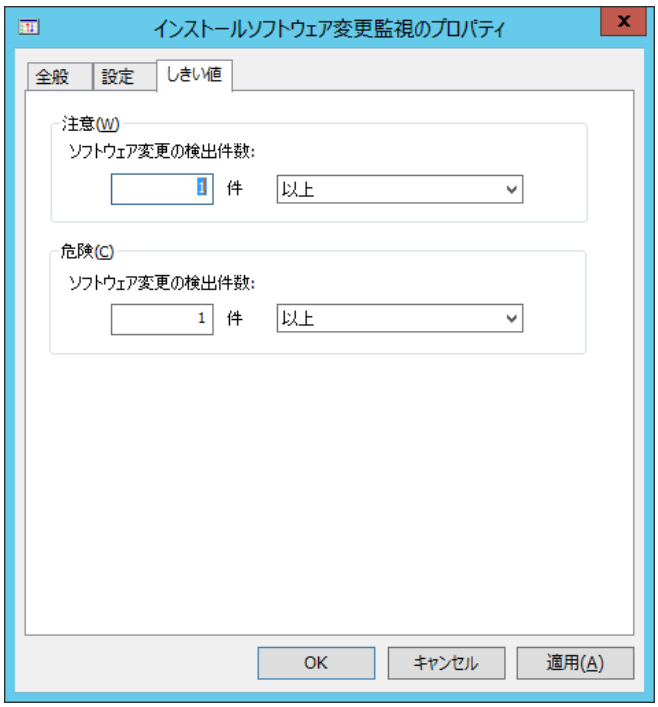
   ●エクスポートファイルの“出力文字コード”を、“UNICODE”ラジオボタンもしくは“Shift JIS”ラジオボタンより選択することができます。

2. エクスポートファイルの“出力情報を”、“差分のみ（追加/削除）”ラジオボタンもしくは“変更なしを含むすべて” ラジオボタンより選択することができます。

3. エクスポートするファイルが既に存在する場合、古いファイルは上書きしますが、“ソフトウェア情報を追記する”チェックボックスにチェックを入れることで、古いファイルに追記することができます。

   ※この機能を使用しますと、エクスポートするファイルが肥大化する場合がありますのでご注意ください。

C.「しきい値」タブ



1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

   ●しきい値

   テキスト入力フィールドに数値(“0”～“999”)を入力します。

   しきい値の判定条件で“より小さい”を選択した場合には、数値に“0”を入力することができません。

   手順 2.で“連続した N 回目の注意から”を選択した場合には、数値に“1”～“99”しか入力できません。

   ●しきい値の判定条件

   ドロップダウンメニューを使用して、しきい値に対する判定条件を、

   “より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

2. “危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

   ●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

   ●「設定」タブのプロパティを開き、[OK]ボタンをクリックするまでは設定が正常に保存されませんのでご注意ください。

5 .10 .19 カスタム監視

任意のプログラムを用いて監視を行いたい際に、任意の指定した実行プログラム（監視実行プログラム）を実行し、監視モジュールとしての戻り値（監視値、結果コード、メッセージ）を監視することができます。

●指定可能な実行プログラムはコンソールアプリケーション（.exe）、バッチファイル（.bat）です。
CScript 形式、PowerShell 形式のファイルについても、標準出力へ監視値を正しく出力できれば監視可能です

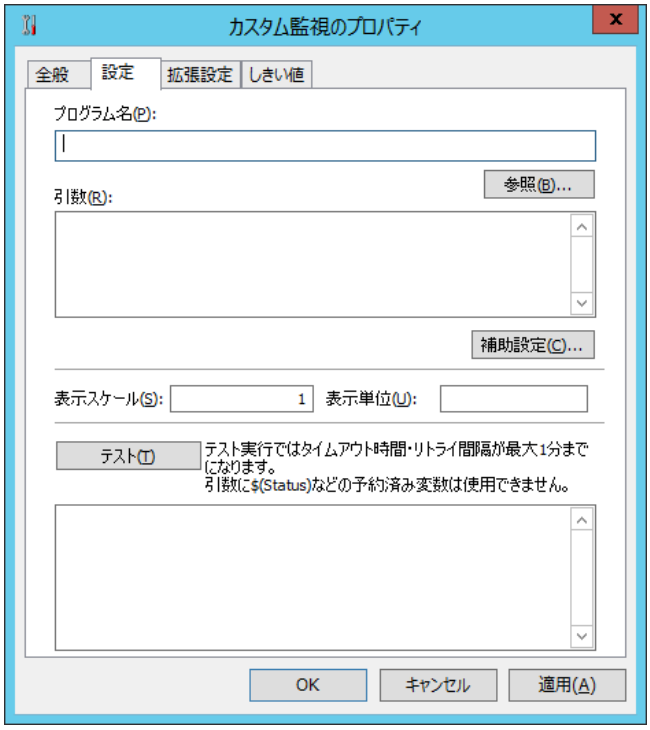
●設定した実行プログラムの返り値は、文字列および負の値を返り値とすることはできませんので、正の数値にしてください。
文字列の返り値の場合には（N/A）という値が返り、ステータスが正常になります。

●代理監視ではカスタム監視のプログラムはインスタンスを構築したローカルコンピューター上で実行されますので、代理監視先の情報を取得する場合には、指定するプログラムがリモートコンピューターを選択できるプログラムである必要があります。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目‘B.「全般」タブ’を参照ください。

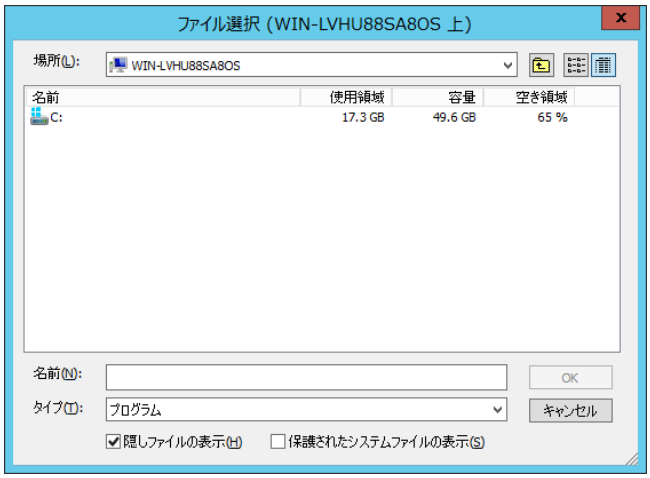
B.「設定」タブ



1. “プログラム名”フィールドに、任意の“監視実行プログラム名”を下記のどちらかの手段で設定します。

●“監視実行プログラム名”を、絶対パスで入力する。

●[参照..]ボタンをクリックして、“ファイル選択”画面より“監視実行プログラム”を選択する。
“隠しファイルの表示”チェックボックスもしくは“保護されたシステムファイルの表示”チェックボックスにチェックを入れると、条件に応じた該当ファイルが表示されます。



2. “引数”フィールドには監視実行プログラムの引数を記述します。

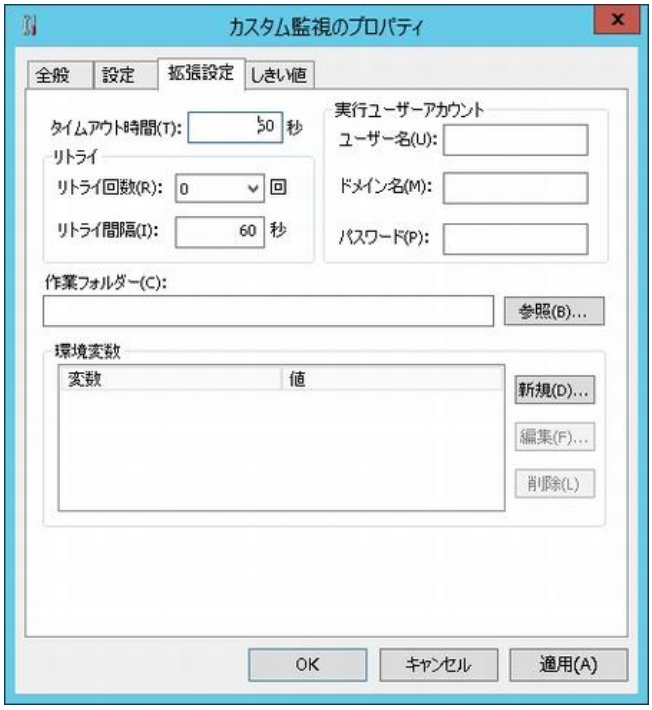
   ●手順 4.のテスト実行時の引数に、BOM 7.0 の予約済み変数は使用できません。

3. [補助設定]ボタンは、カスタム監視補助で使用します。詳細については“第 6 章カスタム監視補助”を参照してください。

4. [テスト]ボタンをクリックすると、「設定」タブ、「拡張設定」タブの両方の設定を加えてテスト実行します。

   ●テスト実行ではタイムアウト時間、リトライ時間が最大 1 分までです。

C.「拡張設定」タブ



「設定」タブで指定したプログラムの実行条件を設定します。

1. “タイムアウト時間”の既定値は“60”秒です。

   “0”～“2000000”までの整数を指定することができますが、“0”を指定すると必ずタイムアウトします。

2. “リトライ”フィールドの“リトライ回数”は“0”～“9”の整数を指定することができますが、“0”を指定するとリトライしません。

   リトライは下記の場合に実行します。

●プロセスの作成に失敗した場合。

●プロセス待機のタイムアウトが発生した場合。

●プロセス待機が失敗した場合。

●ユーザー指定プロセスが“0”以外の終了コードを返した場合。

●監視結果の出力を読み取れなかった場合。

3. “実行ユーザーアカウント”に“監視実行プログラム”を実行する際の“ユーザー名”、“ドメイン名”、“パスワード”を入力します。

●実行ユーザーアカウント指定時は、UAC をオフにする必要があります。

詳細は、‘3 .3 .3 代理監視設定が正しく監視できない場合のトラブルシューティング’の項目

‘F.ユーザーアカウント制御（UAC）’を参照ください。

●実行ユーザーアカウントは、Administrator もしくは Administrators グループのユーザーアカウントである必要があります。

それ以外のユーザーアカウントを指定した場合、監視が失敗します。

4. “作業フォルダー”フィールドに、プログラム実行する際の実行フォルダーを下記のどちらかの手段で設定します。

●“作業フォルダー”を、絶対パスで入力する。

●[参照..]ボタンをクリックし、“フォルダー選択”画面より“作業フォルダー”を選択する。

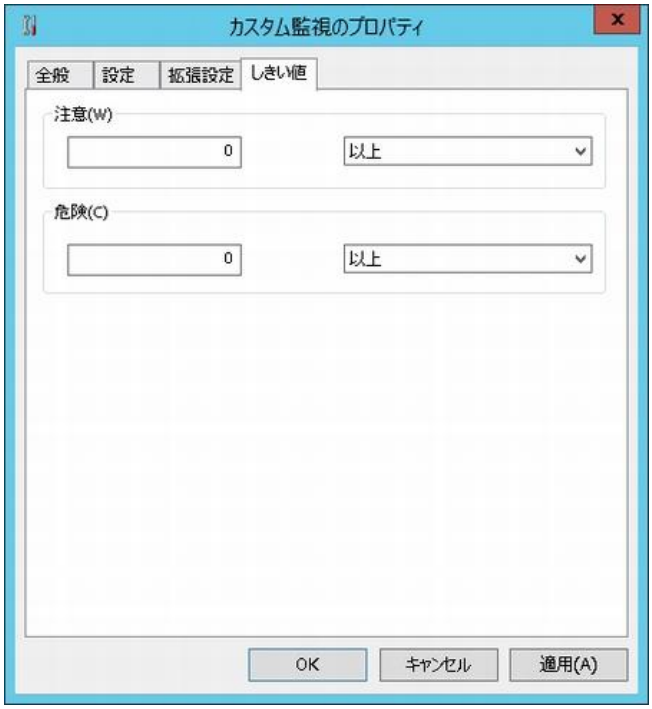
“隠しファイルの表示”チェックボックスもしくは“保護されたシステムファイルの表示”チェックボックスにチェックを入れると、

条件に応じた該当ファイルが表示されます。

5. “環境変数”はプログラムに必要な環境変数があれば、[新規..]ボタンをクリックし、“変数の編集”画面を表示して、

“変数名”と“変数値”を登録します。

D.「しきい値」タブ



1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

   ●しきい値

   テキスト入力フィールドに数値(“0”～“999999999”)を入力します。

   ●しきい値の判定条件

   ドロップダウンメニューを使用して、しきい値に対する判定条件を、

   “と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

2. “危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

   ●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

E. カスタム監視のバッチファイルの設定例

●プログラム名にバッチファイル名、引数にバッチファイルで使用される引数を指定します。

●バッチファイル内では標準出力が返り値になりますので、@echo off でエコー機能を off にしてください。

●本サンプルファイルは引数で指定した値を取得するバッチファイルです。

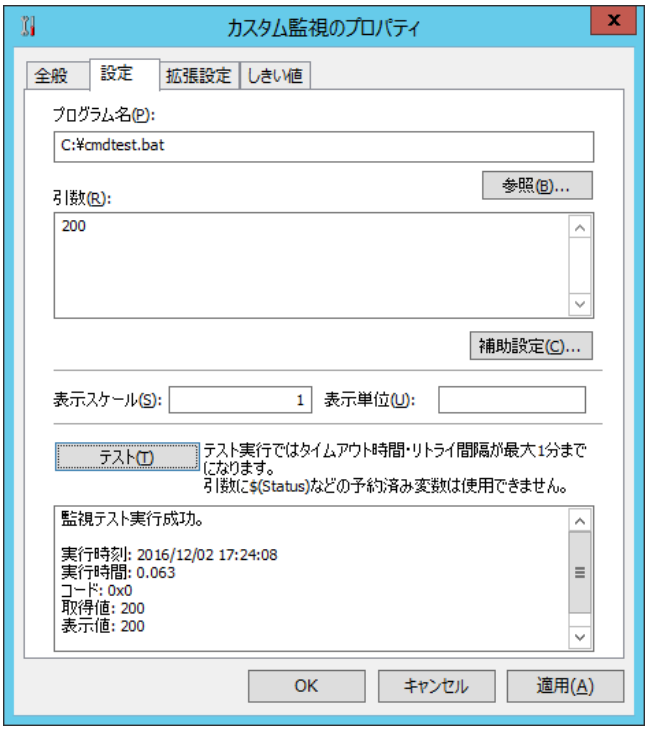
例:

バッチファイル(ファイル名 cmdtest.bat)のサンプルコードと設定、およびテスト実行結果は下記のようになります。

----------cmdtest.bat ここから

```
@echo off
if "%1" == "" goto error
echo %1        (この出力がバッチファイルの取得値となります)
goto end
:error
exit 1         (エラーの場合、0 以外の終了コードに指定します)
:end
exit 0         (正常終了の場合、終了コードは 0 に指定します)
```

----------cmdtest.bat ここまで



F. カスタム監視の WSH の Cscript で実行するファイルの設定例

●プログラム名に cscript.exe、引数に実行するファイル名を指定します。

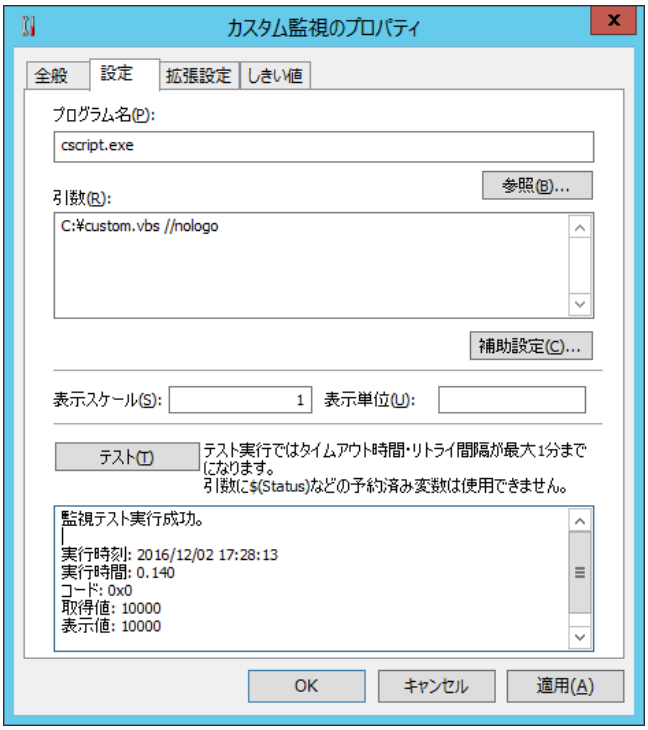
●WSH の Cscript で動作させる場合、エコー機能を off にするため、BOM 7.0 の引数設定に必ず//nologo を記述してください。

●本スクリプトは 10000 を取得値とするスクリプトです。

例:

実行ファイル(ファイル名 custom.vbs)のサンプルコードと設定、およびテスト実行結果は下記のようになります。

```
----------custom.vbs ここから
Dim objStdOut     '標準出力用オブジェクト
Dim intExitCode '終了コード
'標準出力用オブジェクトのインスタンス作成
Set objStdOut = Wscript.StdOut
objStdOut.WriteLine("10000")
'インスタンスの破棄
Set objStdOut    = Nothing
If Err.Number <> 0 Then
    intExitCode = 1 'エラー
Else
    intExitCode = 0 '正常
End If
'intExitCode が終了コードになります。
Wscript.Quit(intExitCode)
----------custom.vbs ここまで
```



5 .10 .20 Windows Update 監視

監視対象コンピューターのインストールされている Windows Update 状況を監視します。

※本監視は代理監視機能に対応していません。ローカル監視のみ対応しています。

監視した結果は、以下のフォルダーに csv 形式で格納されています。

フォルダー：<BOM 7.0 インストールフォルダー>¥BOMW7¥Temp

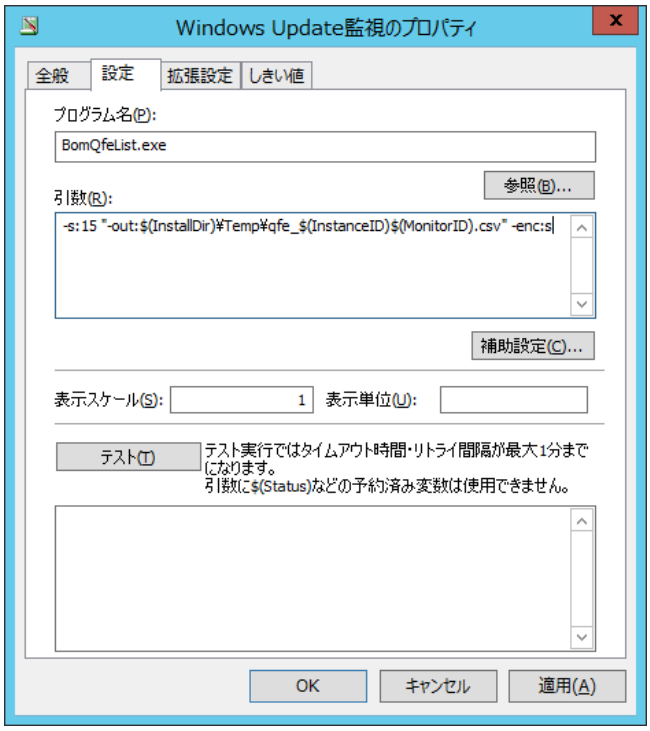
また、監視結果は CsvViewer を使用することにより確認することも可能です。

詳細については '6 .3 .4 CsvViewer について' を参照してください。

A.「全般」タブ

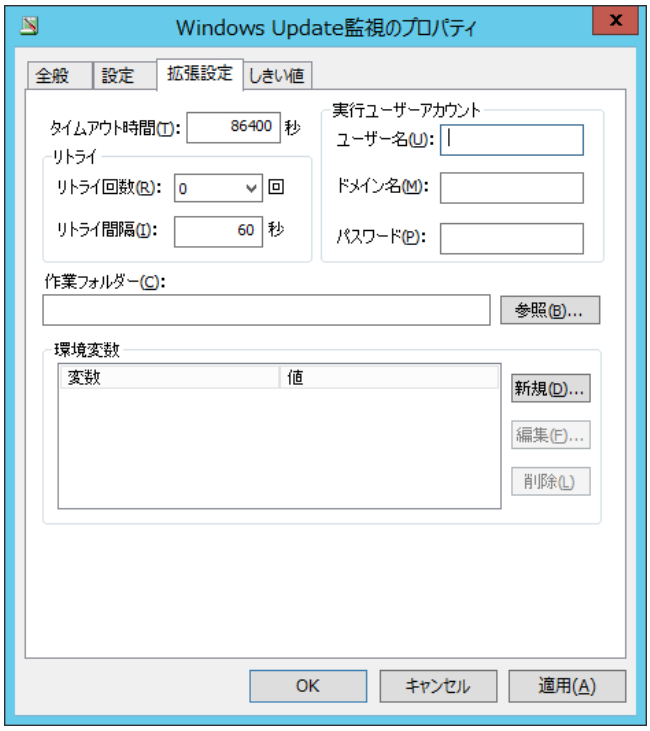
「全般」タブは、"ID"フィールド、"名前"フィールド、および既定値の"時間間隔"に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、'5 .10 .2 監視項目の概要'の項目'B.「全般」タブ'を参照ください。

B.「設定」タブ



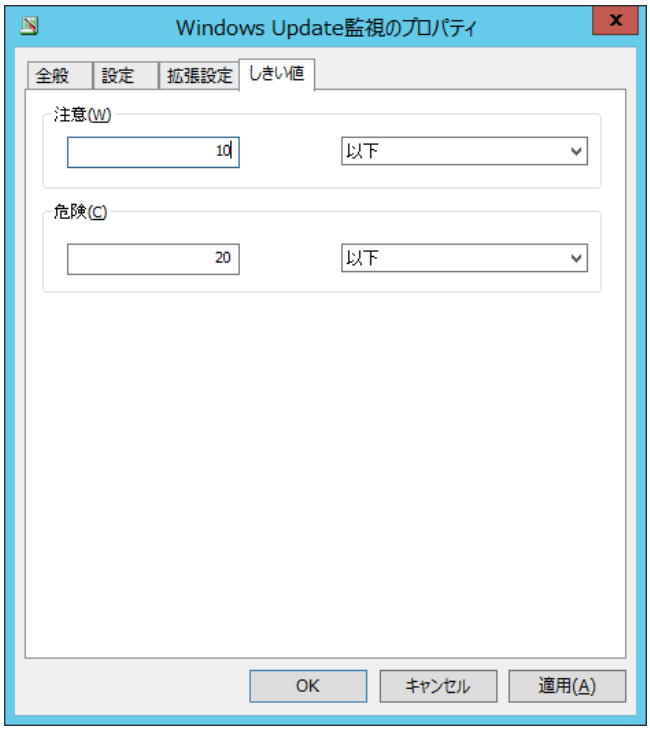
1. デフォルトで入力されている値以外に変更しないでください。変更された場合にはサポート対象外です。

C.「拡張設定」タブ



1. デフォルトで入力されている値以外に変更しないでください。変更された場合にはサポート対象外です。

D.「しきい値」タブ



1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

●しきい値

テキスト入力フィールドに数値(“0”～“999999999”)を入力します。

●しきい値の判定条件

ドロップダウンメニューを使用して、しきい値に対する判定条件を、

“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

2. “危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

●“連続した N 回目の注意から”に設定できる数値は、“1”～“99”です。

5 .10 .21 AWS S3 ストレージ容量監視

Amazon S3 および、Amazon S3 の API に完全準拠する Amazon S3 互換ストレージを監視対象とし、バケットのサイズ、フォルダーおよびファイルのサイズ、または数を監視します。

※ Amazon S3 互換ストレージについて、API 準拠をうたう全てのストレージでの動作を保証するものではありません。
弊社では、クラウディアン株式会社の CLOUDIAN HYPERSTORE について動作確認を取っており、今後の対応確認情報は弊社ウェブサイト（www.say-tech.co.jp）で随時公開いたします。

※ “AWS S3 ストレージ容量監視項目”を使用するためには、Microsoft .NET Framework Ver.3.5 SP1 を事前にインストールする必要があります。インストール方法については ‘第 14 章 Microsoft .NET Framework Ver.3.5 SP1 のインストール’ 参照してください。
また、このアクションは AWS への接続に TLS1.2 のプロトコルを使用するため、.Net Framework 3.5 SP1 インストール後、さらに TLS1.2 対応の更新プログラムを適用する必要があります。更新プログラムは Windows Update から適用するか、Microsoft 社のウェブサイトよりファイルをダウンロードして適用してください。（Windows Server 2016、Windows Server 2019 および Windows 10 では Windows Update を使用してください。）

（参考情報）
2020 年 4 月 10 日現在、該当のファイルは以下のサイトからダウンロードしていただけます。

Windows Server 2008 R2 SP1 Windows 7 SP1	Support for TLS v1.2 included in the .NET Framework version 3.5.1 https://support.microsoft.com/ja-jp/kb/3154518
Windows Server 2012	Support for TLS v1.2 included in the .NET Framework version 3.5 https://support.microsoft.com/ja-jp/kb/3154519
Windows Server 2012 R2 Windows 8.1	Support for TLS v1.2 included in the .NET Framework version 3.5 SP1 on Windows 8.1 and Windows Server 2012 R2 https://support.microsoft.com/ja-jp/kb/3154520

※ プロキシサーバーを利用する場合の資格情報の設定は、基本認証、NTLM 認証をサポートしております。

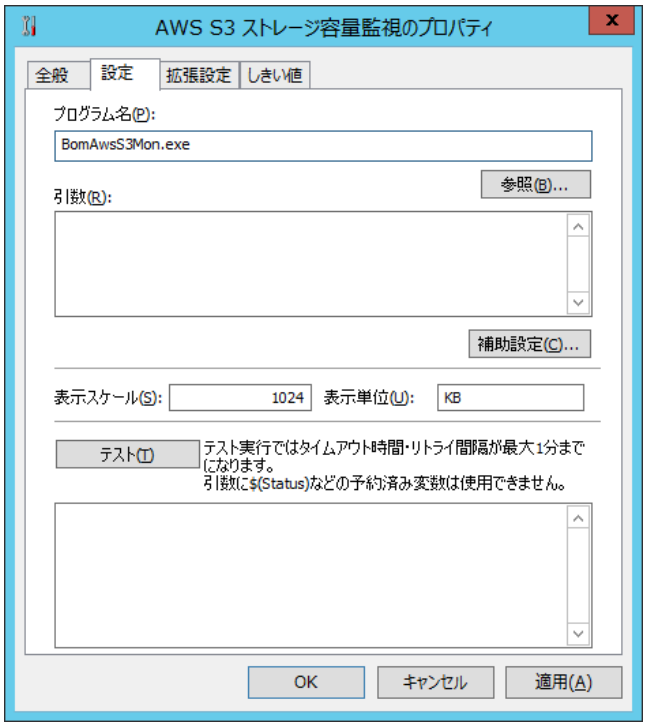
※ アマゾン ウェブ サービスの Amazon Simple Storage Service 開発者ガイド（API Version 2006-03-01）に記載されている、「使用しない方がよい文字」を含むフォルダー名、ファイル名には対応しておりません。

※ この監視では List リクエストでフォルダー・ファイルのメタデータを取得しており、このリクエストで取得できるメタデータ件数に上限（1 回あたり 1000 件）があります。このため、監視対象のバケット、フォルダー配下のフォルダー数、ファイル数に応じてリクエスト数が増加します。
List リクエスト数は次の式で計算できます。
“List リクエスト数”＝“指定したバケットまたはフォルダー配下のフォルダーとファイル数の合計”÷1000（端数切り上げ）

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’ の項目 ‘B.「全般」タブ’ を参照ください。

B.「設定」タブ



1. “プログラム名”フィールドにはあらかじめ“BomAwsS3Mon.exe”と入力されていますので、変更しないでください。
2. “引数”フィールド

   本監視では詳細な設定を後述の補助設定画面で行い、設定された内容は自動的に“引数”フィールドへ反映されます。

   この画面では“引数”フィールド内の入力および編集を行わないでください。
3. “表示スケール”フィールド

   監視で取得された値を“表示スケール”フィールドの入力値で割った数値を基に監視が実行されます。

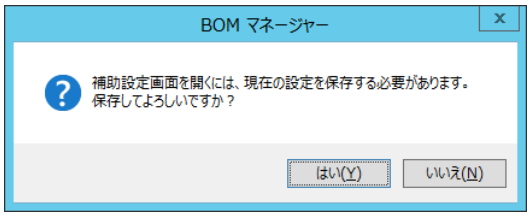
   既定値は“1024”ですが、特にファイル数およびフォルダー数の実数を監視する場合は“1”に変更してください。
4. “表示単位”フィールド

   表示に使用する単位を入力します。

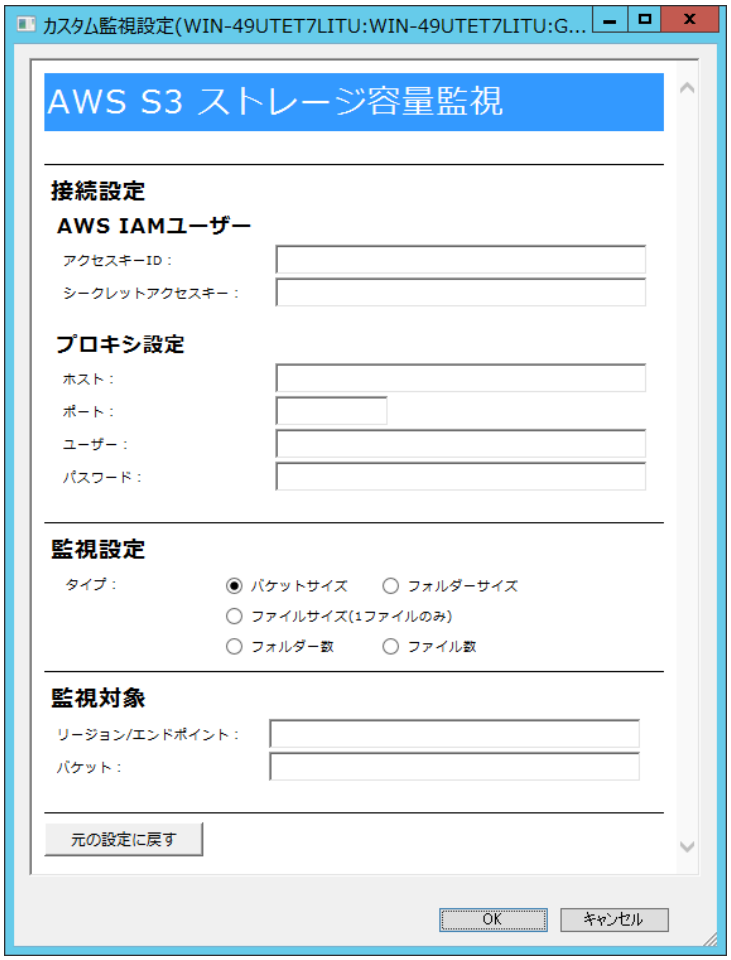
   既定値は“KB”（キロバイト）ですので、ファイル数およびフォルダー数の実数を監視する場合は適宜変更してください。
5. [テスト]ボタン

   クリックすると、「設定」タブ、「拡張設定」タブの両方の設定を加えてプログラムをテスト実行します。テスト実行ではタイムアウト時間、リトライ時間が最大 1 分となります。
6. [補助設定]ボタン

   クリックすると以下の要求が表示され、[はい]ボタンをクリックすると設定の保存後に「AWS S3 ストレージ容量監視」の補助設定画面が表示されます。



C.「AWS S3 ストレージ容量監視」補助設定



1. “AWS IAM ユーザー”フィールド（必須）

   Amazon S3 ストレージおよび、Amazon S3 互換ストレージについて、接続に必要なユーザー情報を入力します。

   （参考情報）

   Amazon S3 ストレージの場合、IAM でアクセスキーを作成し、“アクセスキーID”フィールドおよび、“シークレットアクセスキー”フィールドに入力します。IAM でのアクセスキー作成については、2020 年 4 月 10 日現在、アマゾン ウェブ サービスの以下のサイトに該当の手順が記載されています。

   “AWS Identity and Access Management ユーザーガイド - IAM ユーザーのアクセスキーの管理”

   http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_access-keys.html

2. “プロキシ設定”フィールド（任意）

   プロキシを使用して接続する場合、“ホスト”フィールドおよび、“ポート”フィールドの入力は必須です。またプロキシで認証が必要な場合は“ユーザー”フィールドおよび、“パスワード”フィールドに入力してください。

3. “監視設定”フィールド（選択必須）

   監視対象をラジオボタンで選択します。

   ● バケットサイズ

   バケット配下の全てのファイルの合計サイズを監視

- フォルダーサイズ

  サブフォルダーを含む、指定したフォルダー配下の全てのファイルの合計サイズを監視

- ファイルサイズ（1 ファイルのみ）

  指定したファイルのサイズを監視

- フォルダー数

  サブフォルダーを含む、指定したフォルダー配下の全てのフォルダー数の合計を監視

- ファイル数

  サブフォルダーを含む、指定したフォルダー配下の全てのファイル数の合計を監視

4. “監視対象”フィールド（必須）

   - “リージョン/エンドポイント”フィールド

     リクエスト先の Amazon S3 のリージョンコード、または Amazon S3 互換ストレージのエンドポイントを入力します。

     ※ エンドポイントを指定する場合は、必ず https://から始まる文字列を入力してください。

     例 1）リージョンコードでアジアパシフィック(東京)を指定： ap-northeast-1

     例 2）CLOUDIAN HYPERSTORE でエンドポイントを指定： https://xxxxxx.s3.cloudian.jp

     （参考情報）

     Amazon S3 における各リージョンの詳細なコードについては、2020 年 4 月 10 日現在、以下のアマゾン ウェブ サービスのリファレンスでご確認いただけます。

     “アマゾン ウェブ サービス 全般的なリファレンス - Amazon Simple Storage Service (Amazon S3)”

     http://docs.aws.amazon.com/ja_jp/general/latest/gr/rande.html#s3_region

   - “バケット”フィールド

     監視対象を含むバケット名を入力します。

   - “対象フォルダー”フィールド

     “監視設定”フィールドで“フォルダーサイズ”、“フォルダー数”、“ファイル数”を選択したときのみ表示されます。

     監視対象とする Amazon S3、または Amazon S3 互換ストレージのフォルダーを入力します。階層はスラッシュで区切ってください。

     例： saytech/bomforwin/demo/

   - “対象ファイル”フィールド

     “監視設定”フィールドで“ファイルサイズ（1 ファイルのみ）”を選択したときのみ表示されます。

     監視対象とするファイルを入力します。階層はスラッシュで区切ってください。

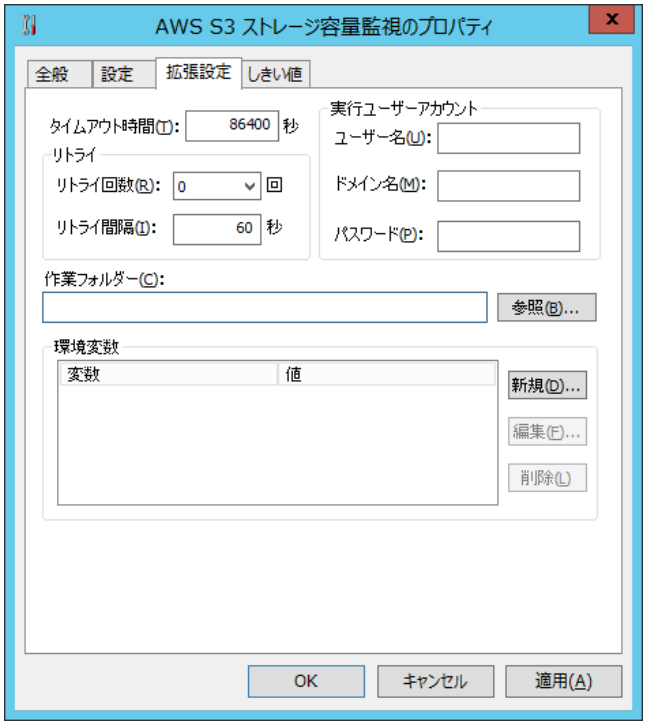
     例： saytech/bomforwin/demo/sample.txt

5. 各フィールドに必要事項を入力して[OK]ボタンをクリックすると、補助設定画面は閉じます。

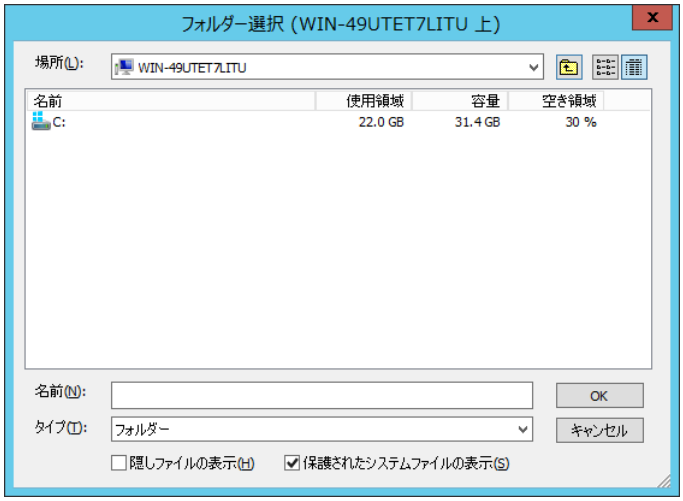
   継続して本監視項目の設定を行う場合は、改めてプロパティを開いてください。

D.「拡張設定」タブ

「設定」タブで指定したプログラムの実行条件を設定します。



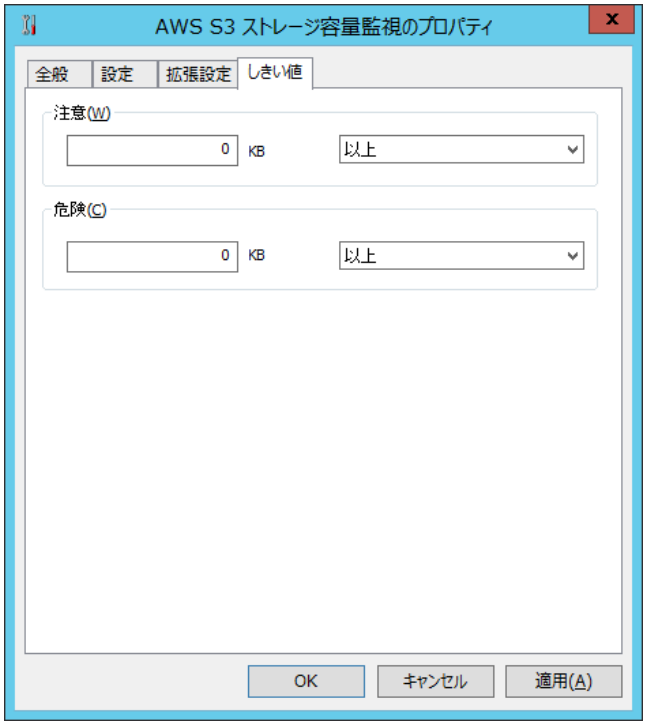
1. “タイムアウト時間”には“0”～“2000000”までの整数を設定でき、規定値は“86400”です。
   “0”を指定すると必ずタイムアウトします。
2. “リトライ”フィールドの“リトライ回数”は“0”～“9”までの整数を指定でき、“0”を指定するとリトライしません。
   リトライは以下の場合に実行されます。
   - プロセスの作成に失敗した場合。
   - プロセス待機のタイムアウトが発生した場合。
   - プロセス待機が失敗した場合。
   - プロセスが“0”以外の終了コードを返した場合。
   - 監視結果の出力を読み取れなかった場合。
3. “実行ユーザーアカウント”は、“監視実行プログラム（BomAwsS3Mon.exe）”を実行する際の“ユーザー名”、“ドメイン名”、“パスワード”を入力します。
   - 実行ユーザーアカウント指定時は、UAC をオフにする必要があります。
     詳細は、‘3 .3 .3 代理監視設定が正しく監視できない場合のトラブルシューティング’の項目‘F.ユーザーアカウント制御（UAC）’を参照ください。
   - 実行ユーザーアカウントは、Administrator もしくは Administrators グループのユーザーアカウントである必要があり、それ以外のユーザーアカウントを指定した場合、監視が失敗します。
4. “作業フォルダー”フィールドは、プログラム実行する際の実行フォルダーを下記のどちらかの手段で設定します。
   - “作業フォルダー”を、絶対パスで入力する。
   - [参照..]ボタンをクリックし、“フォルダー選択”画面より“作業フォルダー”を選択する。



“隠しファイルの表示”チェックボックスもしくは“保護されたシステムファイルの表示”チェックボックスにチェックを入れると、条件に応じた該当ファイルが表示されます。

5. “環境変数”フィールドは使用しないでください。

E.「しきい値」タブ



1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

- しきい値

  テキスト入力フィールドに数値(“0”～“999999999”)を入力します。

- しきい値の判定条件

  ドロップダウンメニューを使用して、しきい値に対する判定条件を、“と等しい”、“と等しくない”、“より大きい”、“以上”、

“より小さい”、“以下”の中から選択します。

“危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

5 .10 .22 iLO ログ監視

iLO を搭載した監視対象コンピューターに接続し、iLO が出力する Integrated Management Log（IML）の件数を監視します。

※ 本監視項目は、iLO 5 のみに対応します。

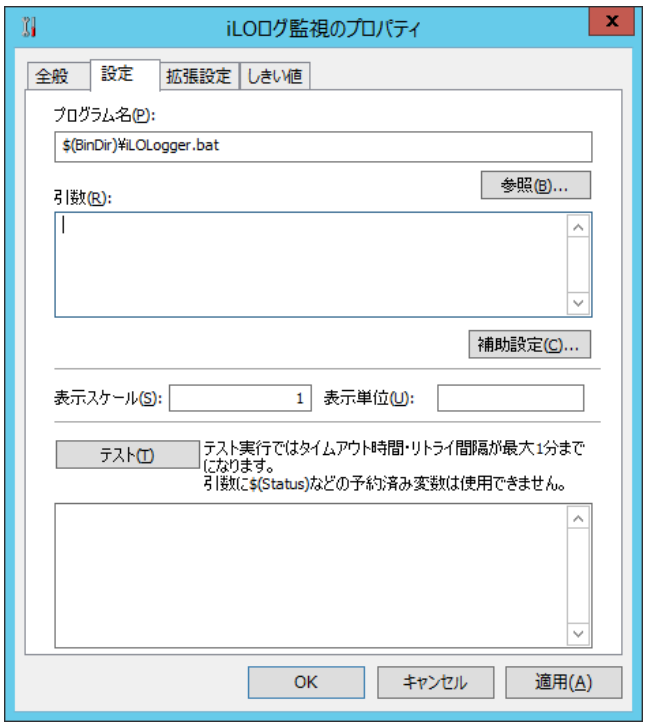
※ 監視対象とするログは Integrated Management Log（IML）のみです。iLO Event Log（IEL）は対象となりません。

※ 時刻が[NOTSET]となっているログは監視対象外です。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’ の項目 ‘B.「全般」タブ’ を参照ください。

B.「設定」タブ



1. “プログラム名”フィールドには既定値として“$(BinDir)¥iLOLogger.bat”と入力されていますので、変更しないでください。
2. “引数”フィールド

   本監視では詳細な設定を後述の補助設定画面で行い、設定された内容は自動的に“引数”フィールドへ反映されます。

   この画面では“引数”フィールド内の入力および編集を行わないでください。

   ※ 当フィールドに反映される補助設定画面での設定内容は、iLO のアカウントパスワードを含めてすべて平文となります。
3. “表示スケール”フィールドには既定値として“1”と入力されていますので、変更しないでください。

4. “表示単位”フィールド

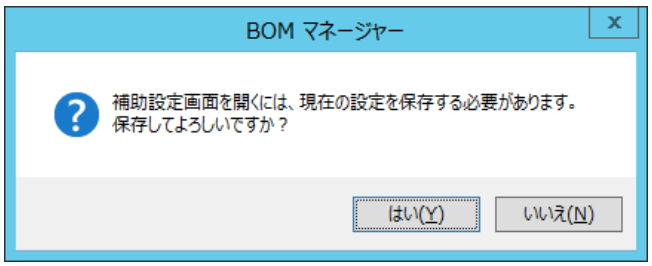
   表示に使用する単位を入力します。既定値は空欄となっています。

5. [テスト]ボタン

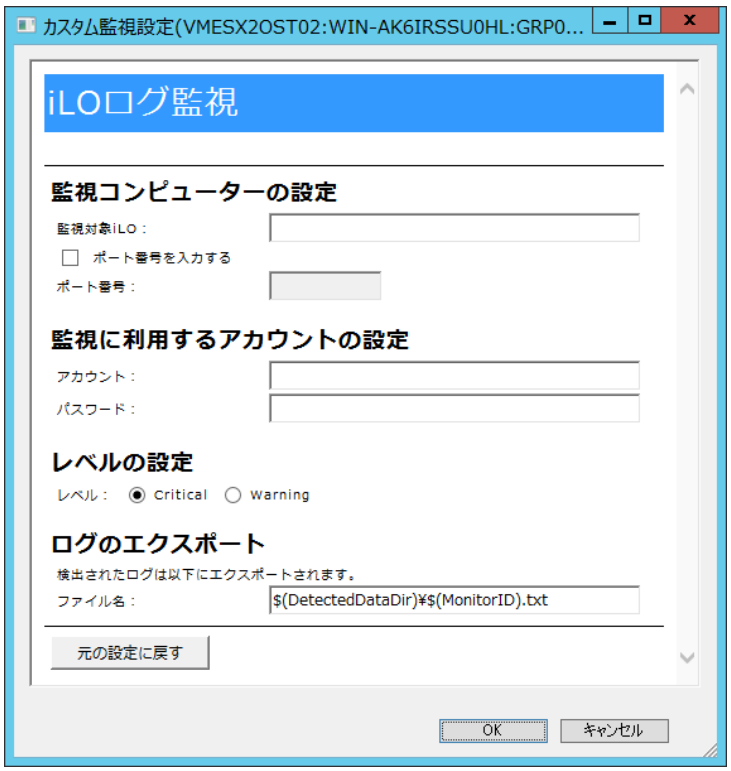
   本監視項目において、[テスト]ボタンは使用できません。

6. [補助設定]ボタン

   クリックすると以下の要求が表示され、[はい]ボタンをクリックすると設定の保存後に「iLO ログ監視」の補助設定画面が表示されます。



C.「iLO ログ監視」補助設定



1. “監視コンピューターの設定”フィールド（一部必須）

   “監視対象 iLO”フィールドには、監視対象とするコンピューターの IP アドレス（IPv4、IPv6）または、コンピューター名を入力します。このフィールドは入力必須です。

   ポート番号は既定値で“443”が設定されますが、変更する必要がある場合は“ポート番号を入力する”にチェックを入れ、“ポート番号”フィールドに任意の値を入力してください。

2. “監視に利用するアカウントの設定”フィールド（必須）

   “アカウント”および“パスワード”に、iLO へ接続するためのアカウント情報を入力します。

3. “レベルの設定”フィールド（選択必須）

   監視対象とするログのレベル（Critical または Warning）をラジオボタンで選択します。

   ※　必ずどちらかを指定する必要がありますので、Critical および Warning の両方を監視する場合は、iLO ログ監視をそれぞれに作成してください。

4. “ログのエクスポート”フィールド（参照のみ）

   本フィールドには既定値として“$(DetectedDataDir)¥$(MonitorID).txt”と設定されており、変更できません。

   本監視で検出されたログは上記の場所に出力され、通知メールに添付するなどが可能です。

   ● ログのエクスポートファイルについて

   txt 形式ファイルで、文字コードは Shift JIS 方式固定です。

   ● “$(DetectedDataDir)”および“$(MonitorID)”について

   それぞれ BOM 7.0 の予約済み変数です。値の詳細は ‘第 15 章　予約済み変数’ を参照してください。

   ● ログファイルについて

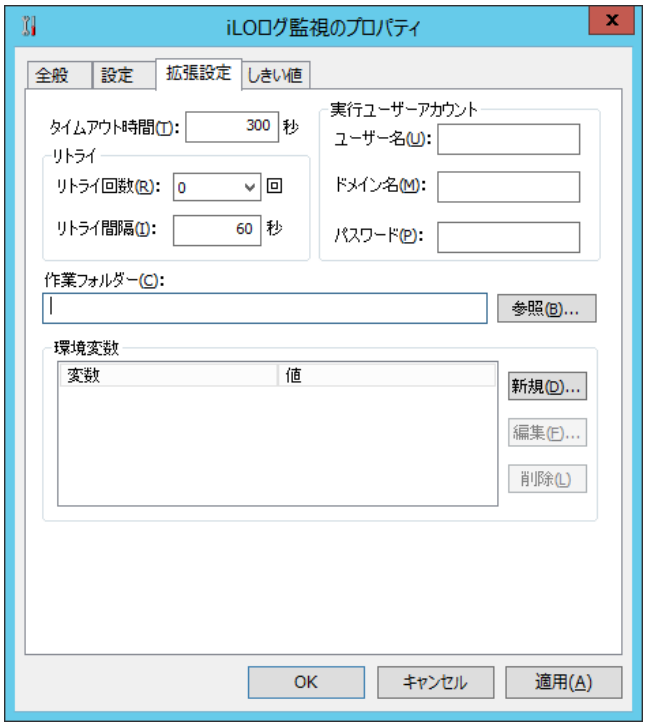
   ログファイルは監視間隔ごとに上書きされ、検出されたログが 0 件の場合は削除されます。

5. 各フィールドに必要事項を入力して[OK]ボタンをクリックすると、補助設定画面は閉じます。

   継続して本監視項目の設定を行う場合は、改めてプロパティを開いてください。

D.「拡張設定」タブ

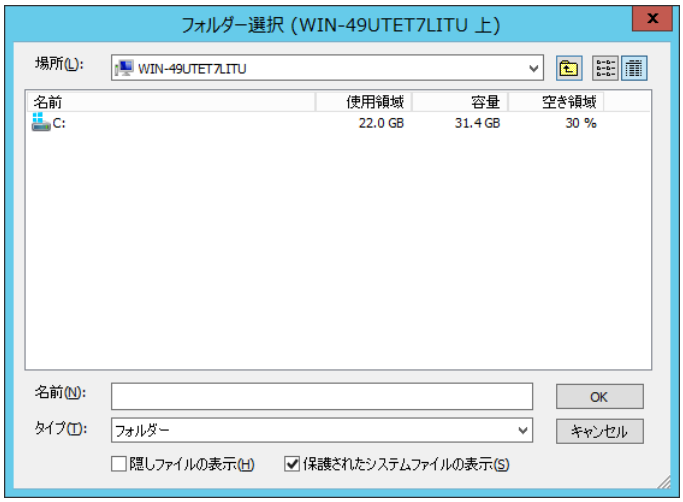
「設定」タブで指定したプログラムの実行条件を設定します。



1. “タイムアウト時間”には“0”～“2000000”までの整数を設定でき、規定値は“300”です。

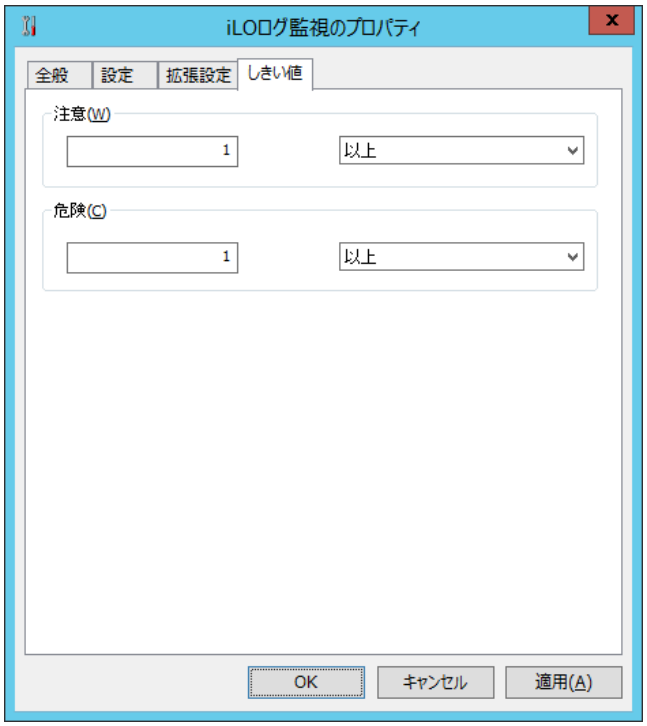
   “0”を指定すると必ずタイムアウトします。

2. “リトライ”フィールドの“リトライ回数”は“0”～“9”までの整数を指定でき、“0”を指定するとリトライしません。
   リトライは以下の場合に実行されます。
   - プロセスの作成に失敗した場合。
   - プロセス待機のタイムアウトが発生した場合。
   - プロセス待機が失敗した場合。
   - プロセスが“0”以外の終了コードを返した場合。
   - 監視結果の出力を読み取れなかった場合。
3. “実行ユーザーアカウント”は、“監視実行プログラム（iLOLogger.bat）”を実行する際の“ユーザー名”、“ドメイン名”、“パスワード”を入力します。
   - 実行ユーザーアカウント指定時は、UAC をオフにする必要があります。
     詳細は、‘3 .3 .3 代理監視設定が正しく監視できない場合のトラブルシューティング’ の項目 ‘F.ユーザーアカウント制御（UAC）’ を参照ください。
   - 実行ユーザーアカウントは、Administrator もしくは Administrators グループのユーザーアカウントである必要があり、それ以外のユーザーアカウントを指定した場合、監視が失敗します。
4. “作業フォルダー”フィールドは、プログラム実行する際の実行フォルダーを下記のどちらかの手段で設定します。
   - “作業フォルダー”を、絶対パスで入力する。
   - [参照..]ボタンをクリックし、“フォルダー選択”画面より“作業フォルダー”を選択する。



   “隠しファイルの表示”チェックボックスもしくは“保護されたシステムファイルの表示”チェックボックスにチェックを入れると、条件に応じた該当ファイルが表示されます。
5. “環境変数”フィールドは使用しないでください。

E.「しきい値」タブ



1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

   ● しきい値

   テキスト入力フィールドに数値(“0”～“999999999”)を入力します。

   ● しきい値の判定条件

   ドロップダウンメニューを使用して、しきい値に対する判定条件を、“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

   “危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

5 .10 .23 iRMC ログ監視

iRMC を搭載した監視対象コンピューターに接続し、iRMC が出力するシステムイベントログ(SEL)の件数を監視します。

※ 本監視項目は、iRMC S5 のみに対応します。

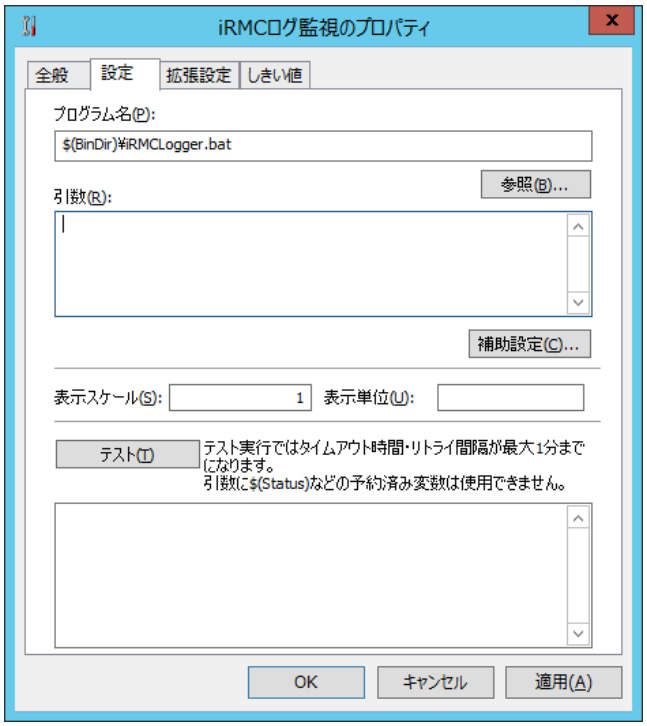
※ 監視対象とするログはシステムイベントログ(SEL)のみです。内部イベントログ(IEL)は対象となりません。

※ システムイベントログの上書きポリシーが「ログフル時に上書き」に設定されている場合、監視間隔以下の短時間に大量のログが出力されるような状況で、保存件数の上限に達した際に上書きされたログは監視できません。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および既定値の“時間間隔”に設定されている値を除き、全ての監視項目で共通です。「全般」タブの詳細は、‘5 .10 .2 監視項目の概要’の項目 ‘B.「全般」タブ’ を参照ください。

B.「設定」タブ



1. “プログラム名”フィールドには既定値として“$(BinDir)¥iRMCLogger.bat”と入力されていますので、変更しないでください。
2. “引数”フィールド

   本監視では詳細な設定を後述の補助設定画面で行い、設定された内容は自動的に“引数”フィールドへ反映されます。

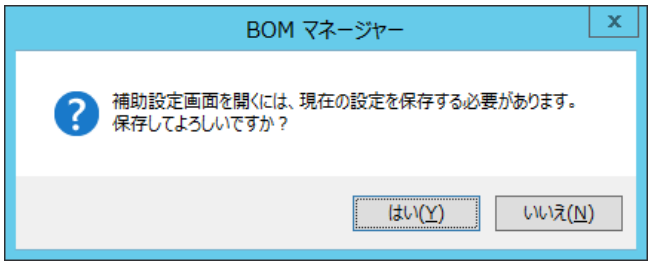
   この画面では“引数”フィールド内の入力および編集を行わないでください。

   ※　当フィールドに反映される補助設定画面での設定内容は、iRMC のアカウントパスワードを含めてすべて平文となります。
3. “表示スケール”フィールドには既定値として“1”と入力されていますので、変更しないでください。
4. “表示単位”フィールド

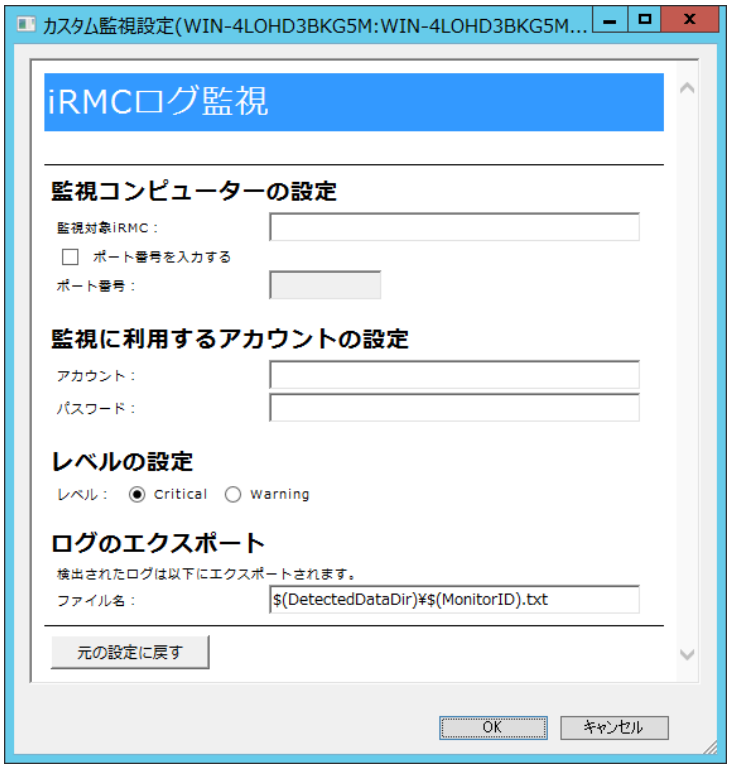
   表示に使用する単位を入力します。既定値は空欄となっています。
5. [テスト]ボタン

   本監視項目において、[テスト]ボタンは使用できません。
6. [補助設定]ボタン

   クリックすると以下の要求が表示され、[はい]ボタンをクリックすると設定の保存後に「iRMC ログ監視」の補助設定画面が表示されます。



C.「iRMC ログ監視」補助設定



1. “監視コンピューターの設定”フィールド（一部必須）

   “監視対象 iRMC”フィールドには、監視対象とするコンピューターの IP アドレス（IPv4、IPv6）または、コンピューター名を入力します。このフィールドは入力必須です。

   また、ポート番号を指定する必要がある場合は“ポート番号を入力する”にチェックを入れ、“ポート番号”フィールドに任意の値を入力してください。

2. “監視に利用するアカウントの設定”フィールド（必須）

   “アカウント”および“パスワード”に、iRMC へ接続するためのアカウント情報を入力します。

3. “レベルの設定”フィールド（選択必須）

   監視対象とするログのレベル（Critical または Warning）をラジオボタンで選択します。

   ※　必ずどちらかを指定する必要がありますので、Critical および Warning の両方を監視する場合は、iRMC ログ監視をそれぞれに作成してください。

4. “ログのエクスポート”フィールド（参照のみ）

   本フィールドには既定値として“$(DetectedDataDir)¥$(MonitorID).txt”と設定されており、変更できません。

   本監視で検出されたログは上記の場所に出力され、通知メールに添付するなどが可能です。

   - ログのエクスポートファイルについて

     txt 形式ファイルで、文字コードは Shift JIS 方式固定です。

   - “$(DetectedDataDir)”および“$(MonitorID)”について

     それぞれ BOM 7.0 の予約済み変数です。値の詳細は ‘第 15 章　予約済み変数’ を参照してください。

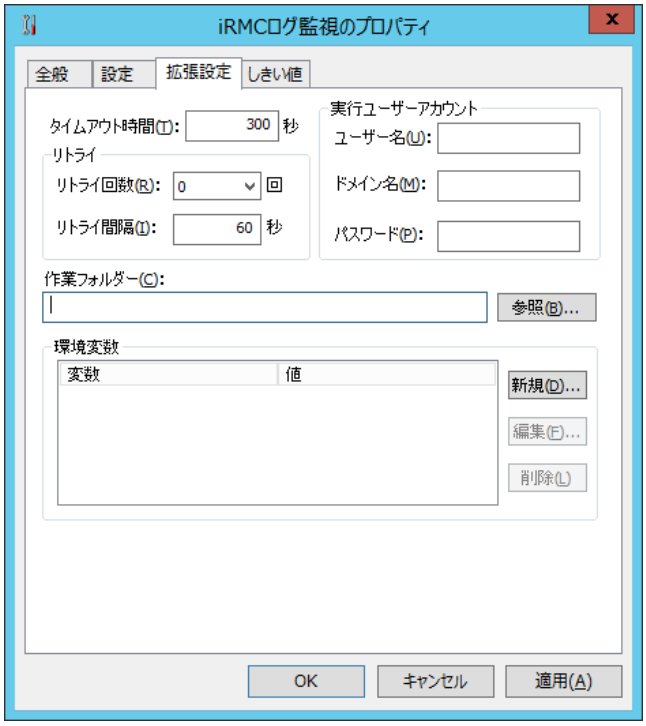
   - ログファイルについて

     ログファイルは監視間隔ごとに上書きされ、検出されたログが 0 件の場合は削除されます。

5. 各フィールドに必要事項を入力して[OK]ボタンをクリックすると、補助設定画面は閉じます。
   継続して本監視項目の設定を行う場合は、改めてプロパティを開いてください。

D.「拡張設定」タブ

「設定」タブで指定したプログラムの実行条件を設定します。

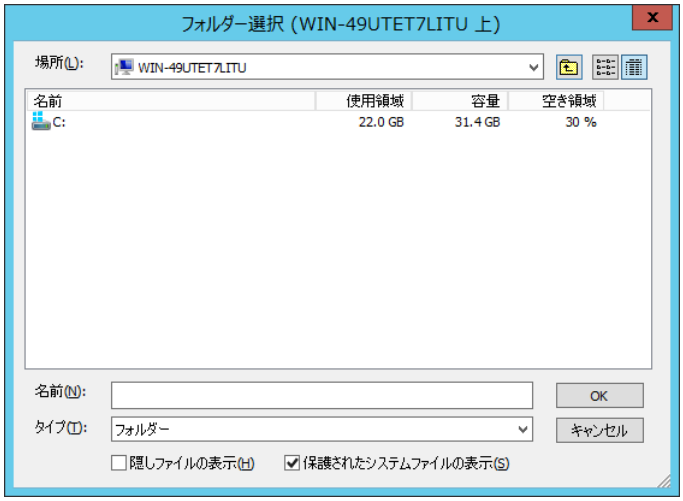


1. “タイムアウト時間”には“0”～“2000000”までの整数を設定でき、規定値は“300”です。
   “0”を指定すると必ずタイムアウトします。
2. “リトライ”フィールドの“リトライ回数”は“0”～“9”までの整数を指定でき、“0”を指定するとリトライしません。
   リトライは以下の場合に実行されます。
   - プロセスの作成に失敗した場合。
   - プロセス待機のタイムアウトが発生した場合。
   - プロセス待機が失敗した場合。
   - プロセスが“0”以外の終了コードを返した場合。
   - 監視結果の出力を読み取れなかった場合。
3. “実行ユーザーアカウント”は、“監視実行プログラム（iLOLogger.bat）”を実行する際の“ユーザー名”、“ドメイン名”、“パスワード”を入力します。
   - 実行ユーザーアカウント指定時は、UAC をオフにする必要があります。
     詳細は、‘3 .3 .3 代理監視設定が正しく監視できない場合のトラブルシューティング’ の項目 ‘F.ユーザーアカウント制御（UAC）’ を参照ください。
   - 実行ユーザーアカウントは、Administrator もしくは Administrators グループのユーザーアカウントである必要があり、それ以外のユーザーアカウントを指定した場合、監視が失敗します。

4. “作業フォルダー”フィールドは、プログラム実行する際の実行フォルダーを下記のどちらかの手段で設定します。

   ● “作業フォルダー”を、絶対パスで入力する。

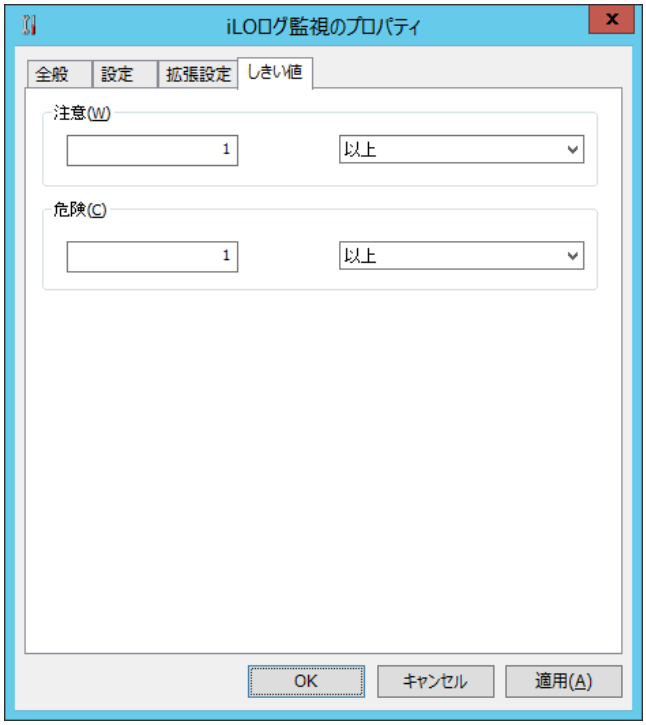
   ● [参照..]ボタンをクリックし、“フォルダー選択”画面より“作業フォルダー”を選択する。



“隠しファイルの表示”チェックボックスもしくは“保護されたシステムファイルの表示”チェックボックスにチェックを入れると、条件に応じた該当ファイルが表示されます。

5. “環境変数”フィールドは使用しないでください。

E. 「しきい値」タブ



1. “注意”フィールドと“危険”フィールドに、しきい値を下記の通りそれぞれ設定します。

   ● しきい値

   テキスト入力フィールドに数値(“0”～“999999999”)を入力します。

● しきい値の判定条件

ドロップダウンメニューを使用して、しきい値に対する判定条件を、“と等しい”、“と等しくない”、“より大きい”、“以上”、“より小さい”、“以下”の中から選択します。

“危険”しきい値の設定は手順 1.に加え、“注意”ステータスの“連続発生回数”をしきい値にすることができます。

第6章 カスタム監視補助

特定の監視テンプレートを適用することにより、従来の監視項目とは異なる監視を行うことができます。

なお、カスタム監視補助については、従来のカスタム監視を拡張した機能となるため画面についてはカスタム監視の UI をそのまま利用しています。

カスタム監視補助の設定は、別途補助画面を用意しております。補助画面上で設定変更を行うようにしてください。引数を直接変更はしないようにしてください。

変更された場合にはサポート対象外です。

6 .1 カスタム監視補助用のテンプレート適用方法

カスタム監視補助用テンプレートの適用方法は、以下に案内する方法で行うことが可能です。

※ 本内容は必要な手順のみを抜粋しています。テンプレートインポートの詳細手順については、‘3 .7 .1 テンプレートのインポート’を参照してください

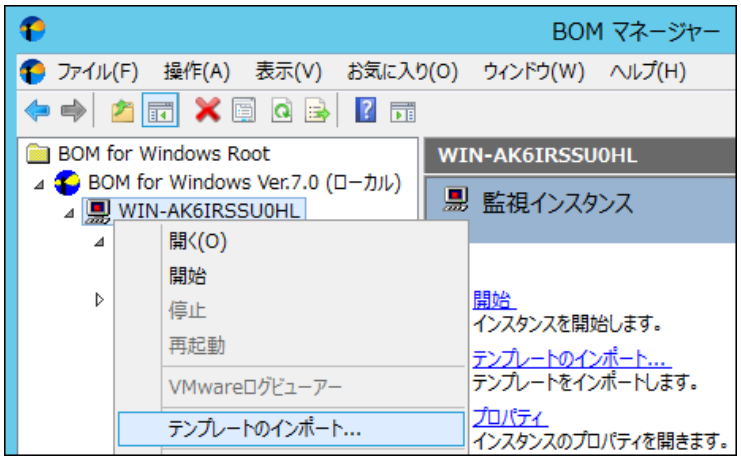
6 .1 .1 カスタム監視補助用監視項目の作成

カスタム監視補助用監視項目を作成する手順は以下の通りです。

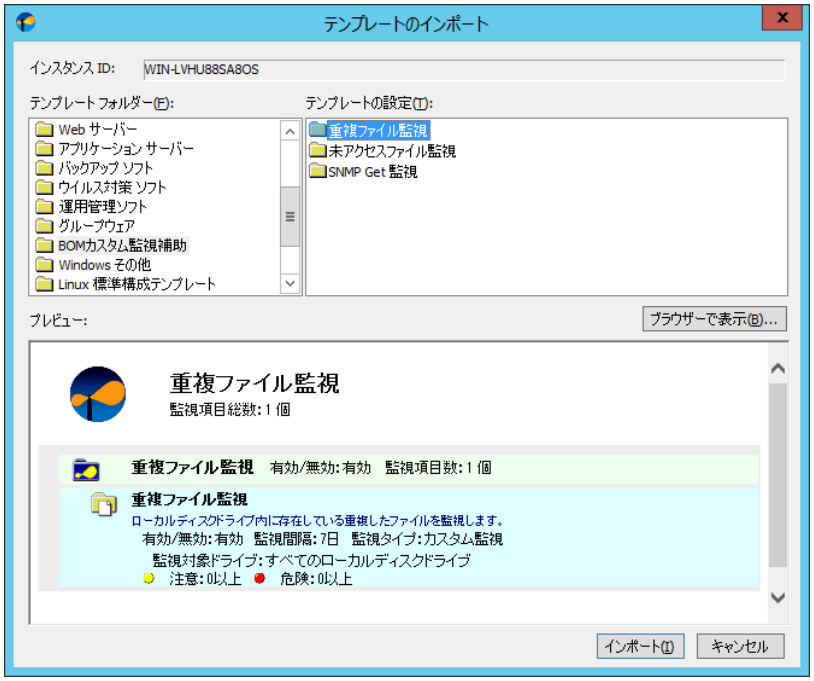
1. スタート画面より、“BOM 7.0 マネージャー”を選択します。

2. BOM マネージャーにて“接続”をクリックし、監視コンピューターに接続します。

3. スコープペインにて、カスタム監視補助を使用し監視を行いたい Windows 監視インスタンスを選択後、右クリックメニューから“テンプレートのインポート”をクリックします。

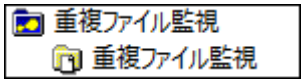


4. “テンプレートフォルダー”にて“BOM カスタム監視補助”を、“テンプレートの設定”にてインポートしたいテンプレートを選択します。



5. [インポート]ボタンをクリックし、テンプレートをインポートします。

6. スコープペインにて選択したテンプレートの監視グループ及び監視項目が作成されたことを確認します。

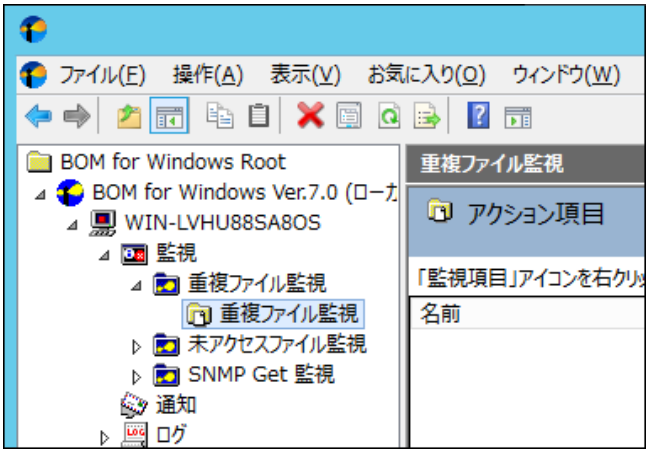


6 .2 カスタム監視補助の設定

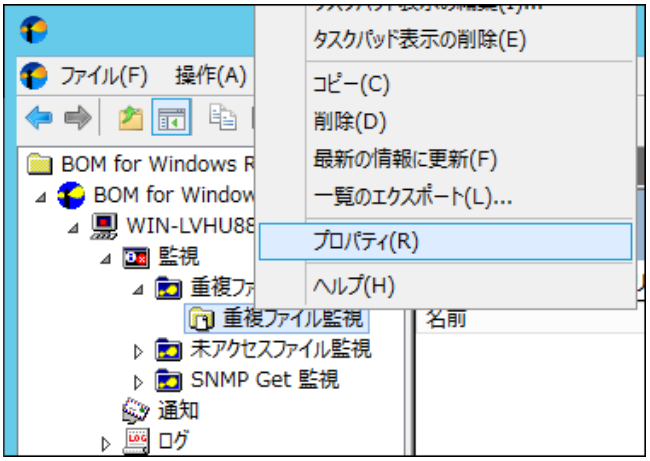
カスタム監視補助の設定を行う際、カスタム監視項目の設定内容を保存した上で実施する必要があります。

手順は以下の通りです。

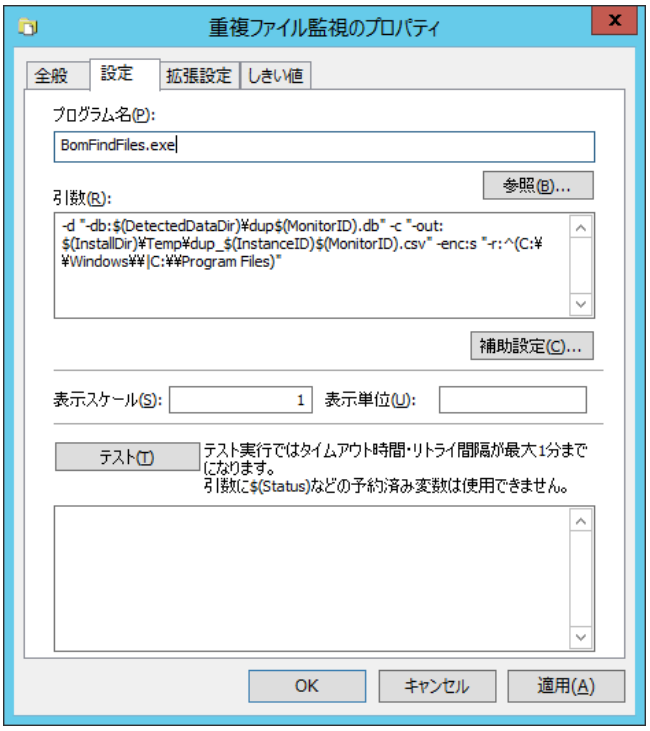
1. 設定したいカスタム監視を選択します。



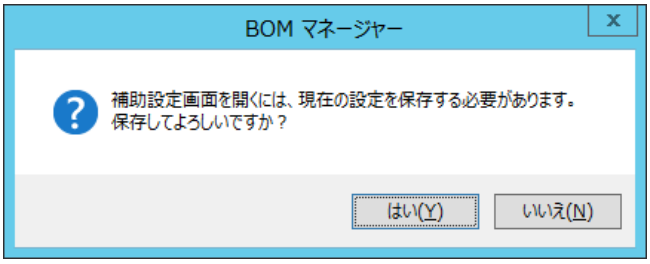
2. 監視項目を選択後、右クリックメニューから“プロパティ”を選択します。



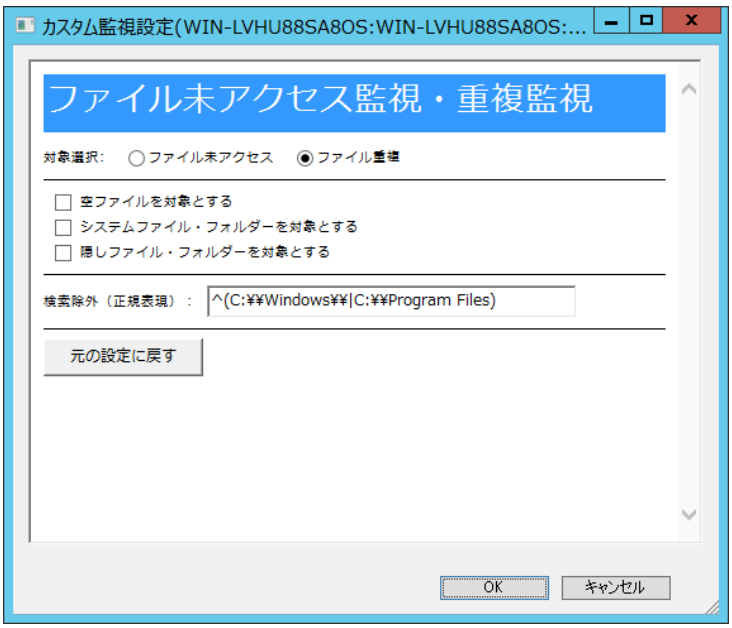
3. プロパティ画面から「設定」タブを選択後、[補助設定]ボタンをクリックします。



4. [補助設定]ボタンをクリックすると以下の要求が表示されますので[はい]ボタンをクリックします。



5. 保存が完了すると、選択した内容の補助画面が表示されます。



6 .3 カスタム監視補助の詳細

6 .3 .1 SNMP Get 監視

SNMP Get 監視は対象サーバーとOIDを指定することにより、そのOIDに対応するオブジェクトの値を取得することが可能です。

SNMP バージョンによって、設定していただく内容が異なりますのでご注意ください。

※本監視は代理監視機能に対応していません。ローカル監視のみ対応しています。

※しきい値については、補助設定画面のしきい値の項目で設定してください。

（カスタム監視のプロパティの「しきい値」タブに設定されている値は変更しないでください。）

対象のテンプレート名：SNMP Get 監視

対応 RFC 番号　　：2578,2579,2580

※　MIB ファイルは以下のフォルダーへ格納してください

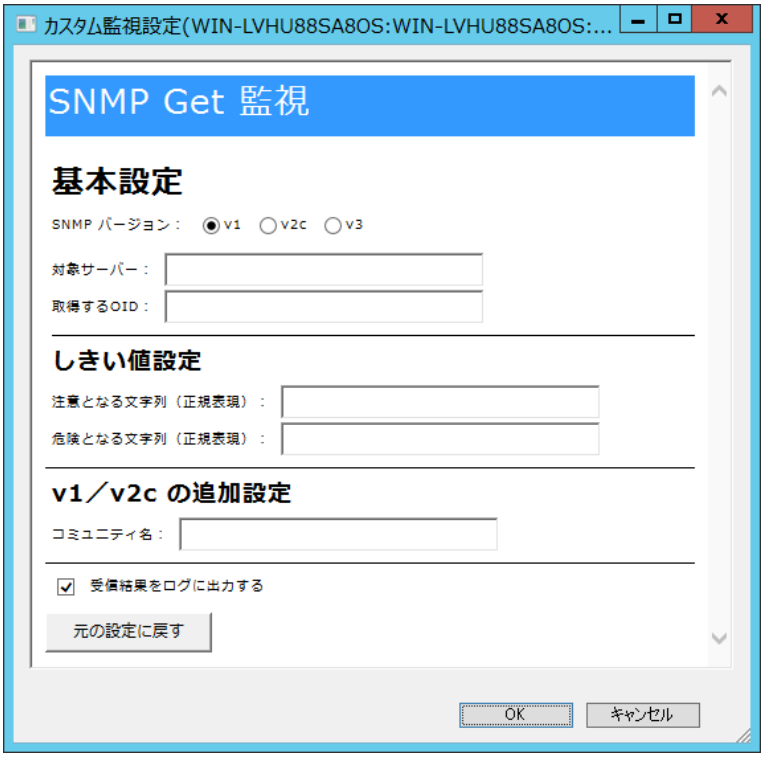
<BOM 7.0 インストールフォルダー>¥BOMW7¥Common¥snmp¥mibs

※　正常に読み込めない MIB ファイルがあった場合には、監視が失敗し、以下のログファイルに詳細が記載されます。

監視が失敗した際にはログファイルを確認してください

<BOM 7.0 インストールフォルダー>¥BOMW7¥Common¥snmp¥logs¥BomSnmpGet.txt

A. 共通設定



1. “SNMP バージョン”ラジオボタン（必須）

   SNMPGet 監視を行う SNMP バージョンを“V1”,“V2c”,“V3”から指定することが可能です。

2. “対象サーバー”フィールド（必須）

   SNMPGet コマンドを送信する対象サーバーを指定します。

3. “取得する OID”フィールド（必須）

   “対象サーバー”フィールドで指定した対象サーバーから取得する OID を、上限 2000 文字までで指定します。

   複数の OID を指定することはできません。複数を指定する場合は、SNMP Get 監視を必要な件数分作成してください。

   SNMP Trap の OID と、本フィールドで指定する SNMP Get の OID は異なります。SNMP Trap の OID は SNMP Get に流用できませんので、対象とする機器で使用できる SNMP Get の OID をご確認の上で設定してください。

   OID は部分一致ではなく完全一致で動作しますので、取得したい OID の文字列をそのまま入力してください。

4. “注意となる文字列（正規表現）”フィールド（任意）

   監視結果として注意となる文字列を正規表現を使用し指定することが可能です。

   注意となる正規表現の指定は部分一致になります。（完全一致ではありません）

5. “危険となる文字列（正規表現）”フィールド（任意）

   監視結果として危険となる文字列を正規表現を使用し指定することが可能です。

   危険となる正規表現の指定は部分一致になります。（完全一致ではありません）

6. “受信結果をログに出力する”チェックボックス（任意）

   “受信結果をログに出力する”チェックボックスにチェックを入れることにより、受信した結果を出力することが可能です。

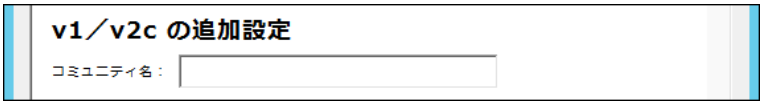
   受信した結果を出力したくない場合には、チェックボックスのチェックを外してください。

   出力したログは以下のフォルダーへ出力されます。（追記型）

   <BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Instance¥（インスタンス名）¥DetectedData

※ 監視インスタンスのログクリアを実施した場合、本ログも削除されますのでご注意ください

B. V1 / V2c の追加設定



1. “コミュニティ名”フィールド（必須）

   ‘対象サーバー’フィールドで指定した対象サーバーのうち、取得するコミュニティ名を指定します。

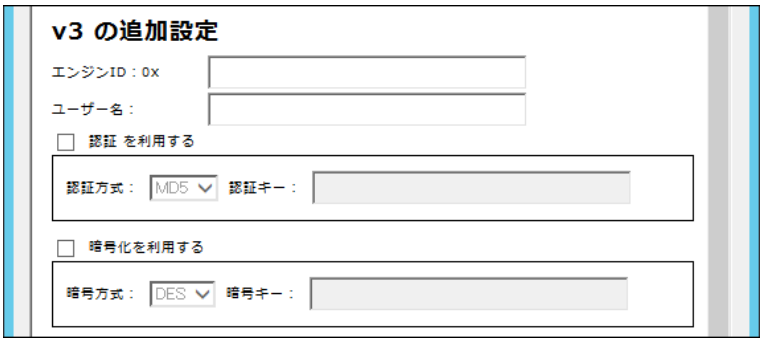
   入力できる文字列の上限は 255 文字です。

   以下の文字列に関しては入力することができません

   ※ 禁則文字制限

   ¥ ” < > | & % ^ (半角スペース)

C. V3 の追加設定



1. “エンジン ID”フィールド（任意）

   “対象サーバー”フィールドで指定したサーバーでエンジン ID を指定している場合に設定します。

   ※ RFC の規定に沿い、最大 64 文字までの入力が有効となります。

2. “ユーザー名”フィールド（必須）

   “対象サーバー”フィールドで指定したサーバーで有効なユーザー名を指定します。

3. “認証を利用する”チェックボックス（任意）

   認証を利用したい場合には、“認証を利用する”チェックボックスにチェックをいれます。

4. “認証方式”プルダウン（任意）

   “認証を利用する”チェックボックスにチェックを入れた場合、認証方式を“MD5”または“SHA”から選択します。

5. “認証キー”フィールド（任意）

   “認証方式”プルダウンで指定した暗号方式の認証キーを入力します。

   ※ 認証キーの値は、設定値をローカルの設定ファイルに保存します。

   ※ 通信は暗号化された状態で行われますが、設定ファイルは暗号化されません。

6. “暗号化を利用する”チェックボックス（任意）

   暗号化を利用したい場合には、“暗号化を利用する”チェックボックスにチェックをいれます。

7. “暗号方式”プルダウン（任意）

   “暗号化を利用する”チェックボックスにチェックを入れた場合、暗号方式を“DES”、“AES”から選択します。

8. “暗号キー”フィールド（任意）

   “暗号キー”フィールドでは、暗号化/複合するときに使用するキーを入力します。

   ※ 暗号キーの値は、設定値をローカルの設定ファイルに保存します。

   ※ 通信は暗号化された状態で行われますが、設定ファイルは暗号化されません。

6 .3 .2 重複ファイル監視

重複ファイル監視は、監視対象の論理ドライブへ対し、重複しているファイル名、ファイル属性（システムファイル、隠し属性）を基に監視を行うことが可能です。

※本監視は代理監視機能に対応していません。ローカル監視のみ対応しています。

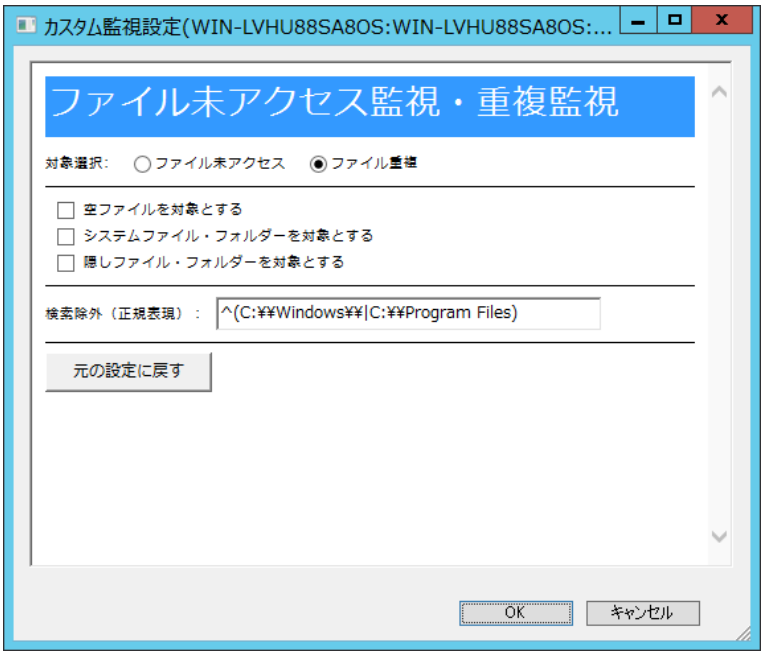
対象のテンプレート名：重複ファイル監視

監視した結果は、以下のフォルダーに csv 形式で格納されています。

フォルダー：<BOM 7.0 インストールフォルダー>¥BOMW7¥Temp

また、監視結果は CsvViewer を使用することにより確認することも可能です。

詳細については ‘6 .3 .4 CsvViewer について’ を参照してください。



1. “空ファイルを対象とする”チェックボックス

   “空ファイルを対象とする”チェックボックスにチェックを入れることにより、空ファイルを監視対象に含めることができます。空ファイルを監視対象に含めたくない場合には、チェックボックスのチェックを外してください。

2. “システムファイル・フォルダーを対象とする”チェックボックス

   “システムファイル・フォルダーを対象とする”チェックボックスにチェックを入れることにより、システムファイル・フォルダーを監視対象に含めることができます。システムファイル・フォルダーを監視対象に含めたくない場合には、チェックボックスのチェックを外してください。

3. “隠しファイル・フォルダーを対象とする”チェックボックス

   “隠しファイル・フォルダーを対象とする”チェックボックスにチェックを入れることにより、隠しファイル・フォルダーを監視対象に含めることができます。隠しファイル・フォルダーを監視対象に含めたくない場合には、チェックボックスのチェックを外してください。

4. “検索除外（正規表現）”フィールド

   監視対象から除外したいフォルダー・ファイル・または文字列を、正規表現を使用して指定することが可能です。

6 .3 .3 未アクセスファイル監視

未アクセスファイル監視は、監視対象の論理ドライブへ対し、最終アクセス日が 6 か月以上前のファイルを対象に監視を行うことが可能です。

※本監視は代理監視機能に対応していません。ローカル監視のみ対応しています。

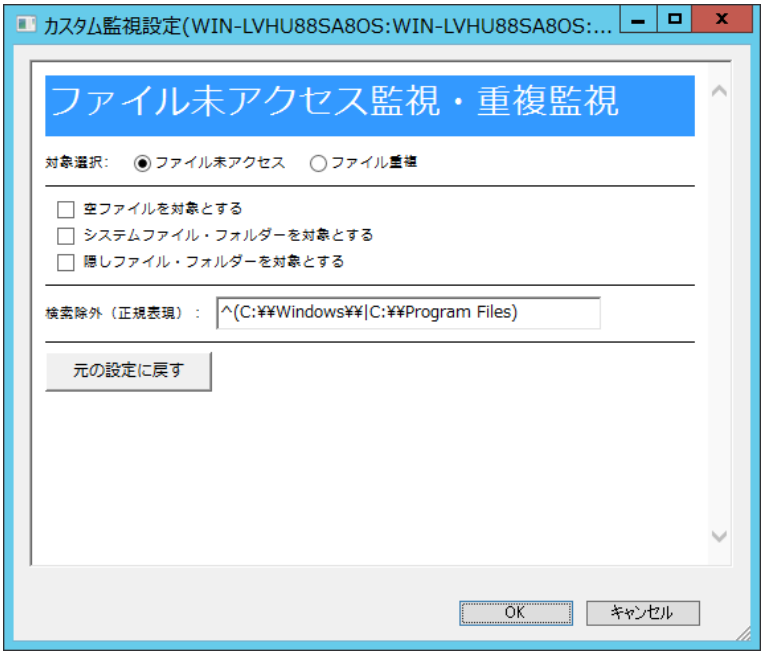
対象のテンプレート名：未アクセスファイル監視

監視した結果は、以下のフォルダーに csv 形式で格納されています。

フォルダー：<BOM 7.0 インストールフォルダー>¥BOMW7¥Temp

また、監視結果は CsvViewer を使用することにより確認することも可能です。

詳細については ‘6 .3 .4 CsvViewer について’ を参照してください。



1. “空ファイルを対象とする”チェックボックス

   “空ファイルを対象とする”チェックボックスにチェックを入れることにより、空ファイルを監視対象に含めることができます。

空ファイルを監視対象に含めたくない場合には、チェックボックスのチェックを外してください。

2. “システムファイル・フォルダーを対象とする”チェックボックス

   “システムファイル・フォルダーを対象とする”チェックボックスにチェックを入れることにより、システムファイル・フォルダーを監視対象に含めることができます。システムファイル・フォルダーを監視対象に含めたくない場合には、チェックボックスのチェックを外してください。

3. “隠しファイル・フォルダーを対象とする”チェックボックス

   “隠しファイル・フォルダーを対象とする”チェックボックスにチェックを入れることにより、隠しファイル・フォルダーを監視対象に含めることができます。隠しファイル・フォルダーを監視対象に含めたくない場合には、チェックボックスのチェックを外してください。

4. “検索除外（正規表現）”フィールド

   監視対象から除外したいフォルダー・ファイル・または文字列を正規表現を使用し指定することが可能です。

6.3.4 CsvViewer について

重複ファイル監視や未アクセスファイル監視、WindowsUpdate 監視で監視した結果は、CsvViewer を使用することにより確認が可能です。

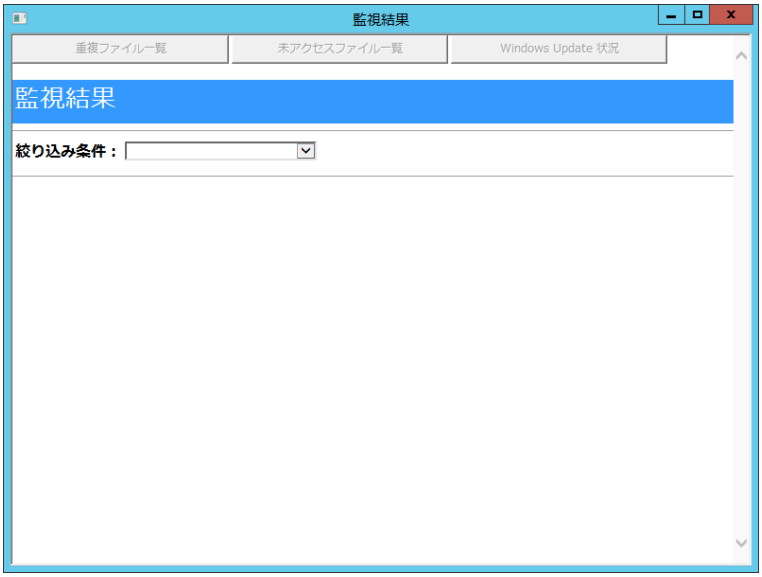
A. CsvViewer の起動方法

CsvViewer を起動する手順は以下の通りです。

1. BOM 7.0 の媒体をコンピューターに挿入します。
2. 媒体内の TOOLS フォルダーを開きます。

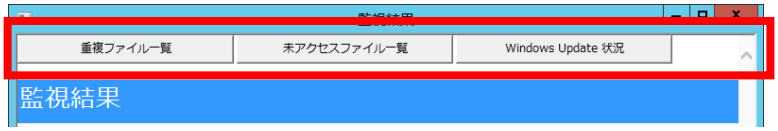
   光学ドライブが D の場合“D:¥TOOLS”
3. TOOLS フォルダー内にある“CsvViewer”フォルダーを選択し、デスクトップ等任意の場所へコピーします。
4. コピー完了後、CsvViewer フォルダーを開き、“start.bat”ファイルを起動します。

5. “start.bat”ファイルを起動すると、監視結果ウィンドウが開きます。



B. CsvViewer の操作方法

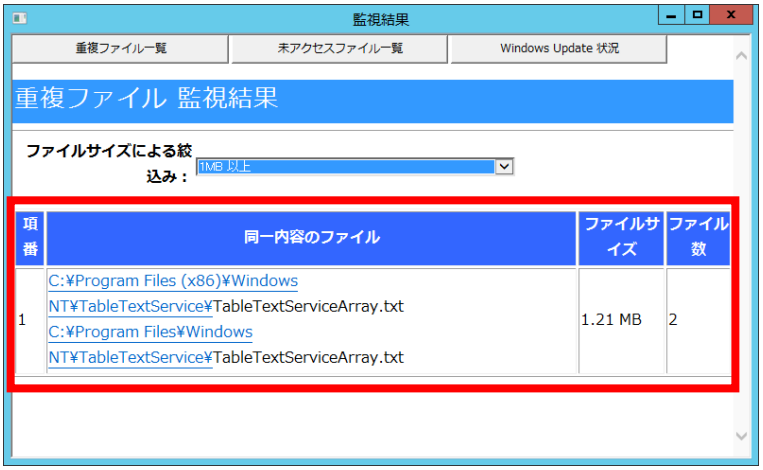
1. 確認したいログを、上部ボタン（重複ファイル一覧や、未アクセスファイル一覧等）から選択します。



2. 該当するログが画面上に出力されます。

3. 絞り込みを行いたい場合には、プルダウンメニューから絞り込みたい条件を選択します。

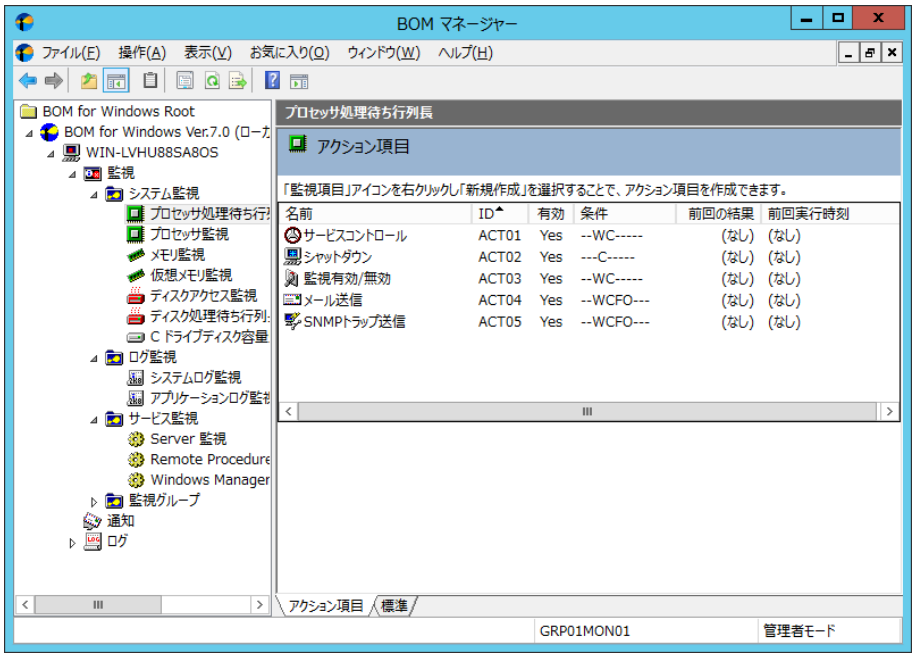
4. 選択後、画面下部に結果が出力されます。



第7章 アクション項目

7 .1 アクション項目の解説

アクション項目とは、‘第 5 章_監視項目’の監視項目のステータスである“正常”、“注意”、“危険”、“失敗”をトリガーに実行させることができる特定のアクションです。



A. アクション項目の変数

シャットダウンのメッセージ送信で挿入できる変数は、必ずメッセージ送信の事前テストを行って内容を確認してからご使用ください。

既定値の値を使用する場合には変換がされますが、カスタマイズする場合にはアクション終了コード、アクション実行結果、検出されたデータの出力先フォルダーは変換されない変数です。

B. アクションが実行中あるいは実行のキューに入っている間に監視を停止した場合

アクションが実行中あるいは実行のキューに入っている間に監視を停止した場合には、下記の 3 つの結果が想定されます。

●停止してから 60 秒を超えても実行されずキューに入っているままの場合、スキップされた主旨のエラーメッセージがヒストリーログに表示されます。

●停止してから 60 秒を超えても実行中のままの場合、結果が戻らない旨のエラーメッセージがヒストリーログに表示されます。

●停止してから 60 秒以内に実行が完了できた場合、完了メッセージがヒストリーログに表示されます。

7.2 アクション項目の作成

1. アクション項目を作成するには、アクション項目を設定したい監視項目を右クリックし、コンテキストメニューの“新規作成”をクリックします。
2. 表示されたコンテキストメニューの実行させたいアクション(“サービスコントロール”、“シャットダウン”等)をクリックすると、アクション項目が BOM マネージャーの監視項目のリザルトペインに作成されます。
   アクション項目は必要に応じて設定値を変更する必要があります。

以降のセクションでは、アクション項目を有効にする方法、および使用可能なアクション項目とその設定値の詳細について解説します。

●「全般」タブと「実行条件」タブは、“シャットダウン”アクション項目を除き、すべてのアクション項目で共通です。

●シャットダウンアクション項目の「全般」タブでは、既定値で“1 度だけ実行(実行後、自動的にアクションが無効になります)”のチェックボックスにチェックが入っています。

●他のタブは、アクション項目によって異なります。

7.3 アクション項目のコピー

アクション項目をコピーすると、コピー先の監視項目のリザルトペインに表示されます。コピーした項目は、同じ名前とプロパティ設定値を持っていますので、設定値を変更する場合は、アクション項目の“プロパティ”画面より行います。

1. アクション項目を右クリックし、コンテキストメニューの“コピー”をクリックします。
2. コピー先の監視項目のリザルトペインを右クリックし、コンテキストメニューの“貼り付け”をクリックします。

●インスタンス間でアクション項目を“コピー”し、“貼り付ける”ことができます。

●リモート接続時のスナップインノード間の監視項目のコピーはできません。

7.4 アクション項目を有効にする

アクション項目を実行するには“有効”にしておく必要があります。

アクション項目を“有効”にするには、下記のいずれかを実行します。

A. “アクション項目”を右クリックし、コンテキストメニューの“有効”をクリックします。

B. “アクション項目”を右クリックし、コンテキストメニューの“プロパティ”をクリックして“プロパティ”画面を表示させ、“有効”チェックボックスにチェックを入れます。

C. リザルトペインで“アクション項目”をダブルクリックして“プロパティ”画面を表示させ、“有効”チェックボックスにチェックを入れます。

D. “アクション項目”をクリックし、リザルトペインの画面下部にある“有効”をクリックします。

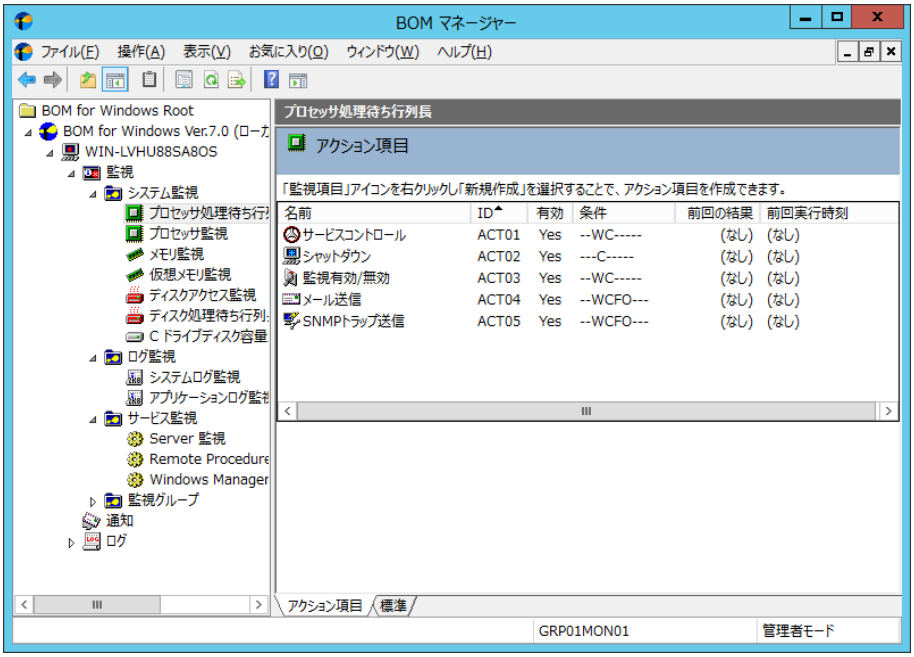
●アクション項目を“無効”にしたい際には、上記 A.、B.、C.いずれかの手順で“無効”を選択します。

●各アクションの「全般」タブの下部“1 回のみ実行(実行後、自動的にアクションが無効となります)”チェックボックスにチェックを入れた場合、該当のアクション項目が 1 回のみ実行された後、自動的に“無効”になります。
問題を解消した後などにアクションを引き続き実行したい場合、アクション項目の“プロパティ”画面などから、再度“有効”にする必要があります。

7 .5 アクション項目のログ

7 .5 .1 リザルトペイン表示

BOM マネージャーの監視項目をクリックすると、リザルトペインに“アクション項目”の状態が下記の通り表示されます。



●“名前”列には、実行されるアクション項目がリストされます。

●“ID”列には、アクション項目の“BOM ID”がリストされます。

●“有効”列には、アクション項目が“有効”か“無効”かが表示されます。

●“条件”列には、アクション項目を実行させるために設定した下記の条件が、リスト表示されます。

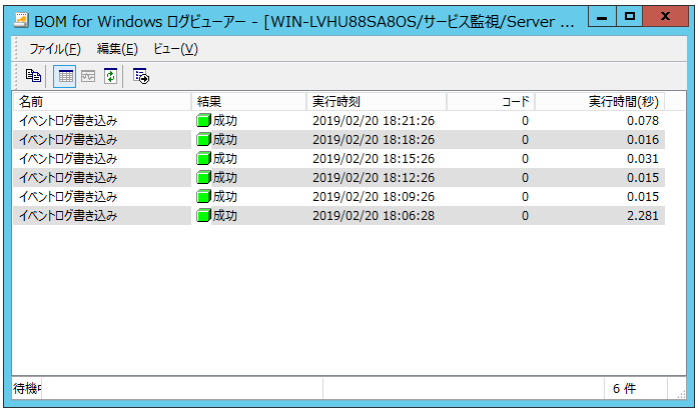
条件記号	条件名	アクション項目の“プロパティ”の設定内容
S	逐次	“アクションの逐次処理を行う”チェックボックスにチェックが入っている状態
N	正常	“正常”チェックボックスにチェックが入っている状態
W	注意	“注意”チェックボックスにチェックが入っている状態
C	危険	“危険”チェックボックスにチェックが入っている状態
F	失敗	“失敗”チェックボックスにチェックが入っている状態
O	変化時のみ	“変化時のみ”ラジオボタンを選択した状態
<	N 回目まで	“回数指定”ラジオボタンを選択し、“回目まで”を選択した状態
>	N 回目以降	“回数指定”ラジオボタンを選択し、“回目以降”を選択した状態
=	N 回目のみ	“回数指定”ラジオボタンを選択し、“回目のみ”を選択した状態
NNN(数値)	実行回数(NNN 回)	“回数指定”ラジオボタンを選択した際の実行回数

●“前回の結果”列には、アクション項目の実行結果がリストされます。

●“前回実行時刻”列には、アクション項目が実行された日時がリストされます。

7.5.2 ログの表示

BOM のログファイルは、BOM 7.0 が検出したシステム障害のトラブルシューティングを行う際に非常に役立ちます。



1. BOM マネージャーで監視項目をクリックし、リザルトペインにアクション項目を表示させます。
2. アクション項目を右クリックし、コンテキストメニューの“ログの表示...”をクリックして、アクション項目の“BOM ログビューアー”画面を表示します。
3. タイトルバーに、現在表示されているインスタンス、監視グループ、監視項目、およびアクション項目の名前が表示されます。
   一度に複数の“BOM ログビューアー”画面を開くこともできます。
   1 アクション項目当たりの最大ログ蓄積量の既定値は 15000 件です。
   ●“名前”列には、実行されたアクション項目がリストされます。
   ●“結果”列では、アクション項目の実行結果が、“成功”、“エラー”、“失敗”のいずれかでリストされます。
   ・“エラー”とは、アクションの実行モジュールが正常に動作し、結果的に期待される動作をしなかった場合を意味します。
   ・“失敗”とは、アクションの実行モジュールそのものが正常に動作しなかった場合を意味します。
   ・カスタムアクションでは指定された外部アプリケーションの動作に依存するため、上記の動作とならない場合もあります。
   ●“実行時刻”列には、アクション項目が実行された日時がリストされます。
   ●“コード”列には、エラーコードがリストされます。この値は、アクション項目が正常に実行された場合は“0”となります。
   ●“実行時間”列には、BOM 7.0 がそのアクション項目を完了するまでにかかった時間が秒単位でリストされます。

7.5.3 ログ蓄積量の最大件数の変更

アクション項目のログは、1 アクション項目あたり既定値で 15000 件まで保存できますが、最大件数を変更したい場合には、下記の ini ファイルの一部を書き換えることで可能です。なお、設定は最初にアクション項目のログが作成される場合に有効になります。ログが既にある場合に最大件数を変更するには、‘9.5 各種ログのクリア’の手順でアクション項目のログを消去して、下記の ini ファイルの設定を変更してから、BOM ヘルパーサービス（BOM7Helper）サービスを再起動してください。

●ini ファイルの設定変更箇所

フォルダー　：　<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Config¥

ファイル名　：　MxHelper.ini

変更箇所　：　[Option]

MaxActLog = <XXXXX>

<XXXXX>の数字を変更することで、保存できる件数を変更できます。

7 .6 ローカル監視と代理監視のアクション機能の違い

ローカル監視では BOM マネージャーのアクションはローカルコンピューターに対して実行されますが、

代理監視のアクションの場合には、下記の表に示すように、実行するコンピューターが異なります。

アクション名	監視元のコンピューター	代理監視先のコンピューター
サービスコントロール	-	代理監視先コンピューターのサービスを制御
シャットダウン	-	代理監視先コンピューターをシャットダウン
監視 有効/無効	監視元コンピューターの設定を変更 （代理監視先コンピューターの監視 ON/OFF）	-
メール送信	監視元コンピューターから、 指定した SMTP サーバーに送信	-
SNMP トラップ送信	監視元コンピューターから、 指定した SNMP マネージャーに送信	-
イベントログ書き込み	代理監視先コンピューターで検知した内容を 監視元コンピューターのイベントログに書込み	-
カスタムアクション	監視元コンピューターから、 代理監視先コンピューターに対して実行	カスタムアクションの設定内容や 監視実行プログラムの内容に依存

7.7 アクション項目の詳細

7.7.1 アクション項目の種類

BOM 7.0 で使用できるアクション項目は、下記の 10 種類です。

オプション製品をインストールしライセンスを適用することで、オプション製品固有のアクション項目が追加で使用できるようになります。オプション製品固有のアクション項目の詳細は各オプション製品のユーザーズマニュアルを参照ください。

アイコン	アクション項目名	説明
リカバリーアクション系：3 種類		
	サービスコントロール	サービスの開始/停止/再起動を制御
	シャットダウン	Windows のシャットダウン/再起動を制御
	監視 有効/無効	監視グループ/監視項目の有効化/無効化制御
通知アクション系：4 種類		
	メール送信	SMTP 形式のメール通知
	SNMP トラップ送信	SNMP 形式のトラップ送信による通知
	イベントログ書き込み	Windows イベントログへの書き込みによる通知
	syslog 送信	syslog サーバーへ監視結果を送信
その他のアクション系：3 種類		
	AWS S3 ファイル送信アクション	Amazon S3 および、Amazon S3 互換ストレージ（※）へ、任意のファイルを送信
	HTTPS 送信	HTTPS プロトコルを使用したファイル/通知の送信
	カスタムアクション	外部アプリケーションを利用した制御/通知

※ Amazon S3 互換ストレージについて、API 準拠をうたう全てのストレージでの動作を保証するものではありません。
弊社では、クラウディアン株式会社の CLOUDIAN HYPERSTORE について動作確認を取っており、今後の対応確認情報は弊社ウェブサイト（www.say-tech.co.jp）で随時公開いたします。

7.7.2 メール送信と SNMP トラップ送信に必要な環境設定

BOM 7.0 で使用できるアクション項目のうち、メール送信と SNMP トラップ送信は、
“BOM for Windows Ver.7.0 （ローカル）のプロパティ”画面より、事前に下記の設定を行う必要があります。

●メール送信の場合

メールを送信するために必要な SMTP サーバーの情報

詳細は‘2.3.3 SMTP 情報の設定’を参照ください。

●SNMP トラップ送信の場合

BOM 7.0 より送信した SNMP トラップを受信させる SNMP マネージャー情報

詳細は‘2.3.4 SNMP 情報の設定’を参照ください。

7.7.3 アクション項目の概要

アクション項目は、作成しただけでは意図したアクションが行えません。アクション項目は、作成した後に設定を行います。

アクション項目の設定は、下記のいずれかの手段で“プロパティ”画面を表示させ行います。

●監視項目をクリックし、設定を行いたいアクション項目を右クリックし、コンテキストメニューの“プロパティ”をクリック

●監視項目をクリックし、設定を行いたいリザルトペインのアクション項目をクリックし、画面下部の“プロパティ”をクリック

●監視項目をクリックし、設定を行いたいリザルトペインのアクション項目をダブルクリック

A. 基本操作

1. タブ

“プロパティ”画面は、「全般」、「実行条件」、「設定」などのタブで構成されています。

それぞれのタブをクリックすることで、該当するタブが表示され、設定を変更できます。

2. 変更した設定の反映とは破棄

変更した設定は、[OK]ボタン、または[適用]ボタンをクリックすることで BOM 7.0 に反映することができます。

変更した設定を破棄したい場合には[キャンセル]ボタンをクリックします。

B. 「全般」タブ

「全般」タブは、“アイコン”、“ID”、“名前”に設定されている値を除き、すべてのアクション項目で共通です。

「全般」タブに登場するアクション項目の基本概念に関する詳細は、‘7 .4 アクション項目を有効にする’も参照ください。

1. [アイコン]ボタン

   [アイコン]ボタンはアクション項目で設定されているアイコンが表示されています。

   既定では、アクション項目の種類に合わせたアイコンが設定されています。

   [アイコン]ボタンをクリックすることで、アイコンを変更するためのダイアログを表示することができます。

   アイコンを変更する場合には、ダイアログにて変更したいアイコンをクリックし、[OK]ボタンをクリックします。

2. “有効”

   “有効”チェックボックスにチェックを入れることで、アクションを実行します。

   既定では“有効”チェックボックスにチェックが入っています。

   アクションを行いたくない場合には、“有効”チェックボックスのチェックを外します。

3. “名前”フィールド

   “名前”フィールドには、アクション項目名を入力します。既定値としてアクション項目の種類と同じ名称が入力されています。

   必要に応じて、分かりやすい名称に変更してください。この名前は、BOM マネージャーに表示される名前です。

4. “ID”フィールド

   “ID”フィールドには、アクション項目 ID が表示されます。

   監視グループ番号と監視項目番号とアクション項目番号が含まれています。

   アクション項目 ID は、インスタンス内でアクション項目ごとに一意になるように、BOM 7.0 が自動的に設定します。

5. “コメント”フィールド

   “コメント”フィールドには、アクション項目の補足情報を入力します。既定では空白です。必要に応じて入力してください。

6. “1 回のみ実行”

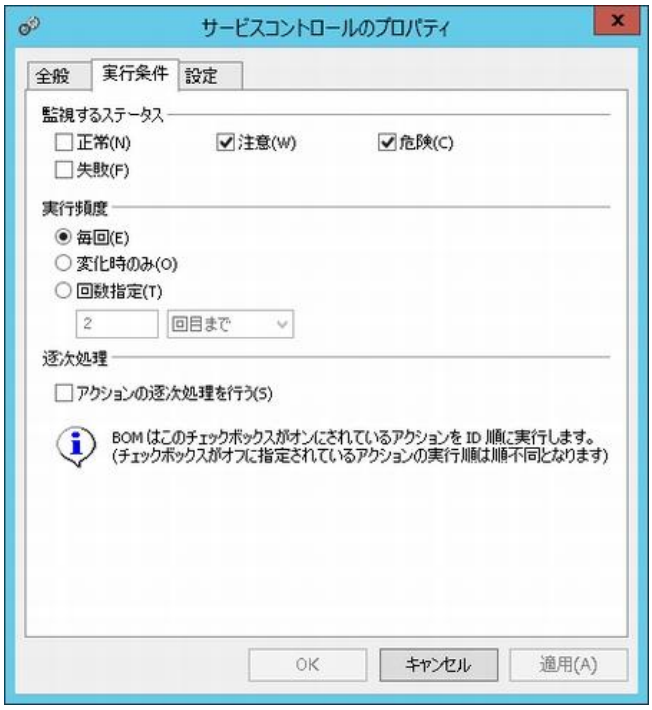
   “1 回のみ実行”チェックボックスにチェックが入っている場合、アクション項目が実行された時に上記 2.の

   “有効”チェックボックスのチェックを自動で外します。そのため、再び手動で“有効”チェックボックスにチェックを入れるまで、

   そのアクション項目は起動しません。

   シャットダウンアクションを除き、既定では“1 回のみ実行”チェックボックスのチェックが外れています。

C.「実行条件」タブ



「実行条件」タブは、アクション項目を実行するための条件を設定します。

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。

●「全般」タブで“1 回のみ実行”チェックボックスにチェックを入れた場合、1 度アクションが実行されるとアクション項目が無効状態になるため、“実行頻度”フィールドの設定がどのような値であっても実行されません。

1. 監視するステータス

   監視項目の監視結果（ステータス）を、アクションの起動条件として指定することができます。

   指定できるステータスは、“正常”、“注意”、“危険”、“失敗”の 4 つがあり、各ステータスのチェックボックスにチェックを入れて起動条件を満たした際に、アクションを実行することができます。

   既定では、“注意”と“危険”チェックボックスにチェックが入っています。

2. 実行頻度

   上記 1.で選択した同一のステータスが連続して発生した際のアクションの動作条件を指定することができます。

   既定では、“毎回”ラジオボタン（毎回アクションが実行される）が選択されています。

   ●“毎回”ラジオボタンを選択した場合

   アクションが起動するステータス条件を満たしていた際に、アクションを毎回実行します。

   ●“変化時のみ”ラジオボタンを選択した場合

   アクションが起動するステータス条件を満たしていたとしても、前回のステータスと同一であった時にはアクションは実行しません。

   ●“回数指定”ラジオボタンを選択した場合

   アクションが起動するステータス条件を満たしていた際に、ステータスが何回連続して発生したのかがカウントされ、下記の

通りアクションを実行します。回数指定の数値（N 回）入力フィールドには、“2”～“999”までの整数を入力できます。

●“回数指定”のドロップダウンリストで、“回目まで”を選択した場合

カウントした値が“N”回に達するまで、アクションを実行します。

●“回数指定”のドロップダウンリストで、“回目以降”を選択した場合

カウントした値が“N”回を超えた場合に、アクションを実行します。

●“回数指定”のドロップダウンリストで、“回目のみ”を選択した場合

カウントした値が“N”回と一致した場合にのみ、アクションを実行します。

3. “アクションの逐次処理を行う”

1 つの監視項目に対して複数のアクション項目を作成している場合、「全般」タブのアクション“ID”順（昇順）に逐次処理をさせることができますので、アクションの実行順序を制御したい場合に使用します。

●チェックがついている場合の動作条件

1.同一監視項目に作成されている他のアクション項目にチェックが入っているか否かを確認し、チェックが入っているすべてのアクション項目をアクション項目“ID”順（昇順）で逐次実行します。

2.“監視するステータス”および“実行頻度”は、アクション項目“ID”順（昇順）で先頭（1 番目）のアクション項目の指定のみが適用され、2 番目以降のアクションに指定した“監視するステータス”および“実行頻度”は無視されます。

その際に、‘7 .5 .1 リザルトペイン表示’の“監視するステータス”および“実行頻度”には、“-”で表示がされます。

3.逐次実行対象のアクションが途中で失敗した場合、それ以降の逐次対象の実行アクションは実行されません。

4.逐次実行アクションの中で 1 回のみ実行の設定のアクションがある場合、2 回目以降はそのアクションも含め、それ以降の ID の逐次実行アクションは実行されません。

●チェックが外れている場合の動作条件

チェックが外れているアクション項目は、他のアクション項目の実行条件や状況に影響をうけずに、並列処理を行います。

D.「設定」タブ

「設定」タブは、アクション項目のコントロール対象とコントロール方法を設定します。

設定方法はアクション項目の種類によって異なります。

7 .7 .4 サービスコントロールアクション

サービスコントロールアクション項目は、アクションを実行させたい監視項目がしきい値のレベルに達した場合、
またはしきい値のレベルが変化した場合に、特定の指定したサービスを“開始”または“停止”させることができます。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、
全てのアクション項目で共通です。
「全般」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。
「実行条件」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ

1. コントロールを行いたいサービスを下記のどちらかの手段で設定します。

●“現在の監視項目で監視されるサービス”ラジオボタンを選択した場合

サービス監視に対して、サービスコントロールアクションを作成した場合、既定値で選択されています。
監視対象のサービスに対して、コントロールを行います。

●“別のサービスを指定”ラジオボタンを選択した場合

サービス監視以外の監視項目に対して、サービスコントロールアクションを作成した場合、既定値で選択されています。
コントロールするサービス名を、手順 2.で指定します。

2. 下記のいずれかの方法で、“サービス名”フィールドにコントロール対象の“サービス名”を設定します。

※ Windows 10 version 1803 および、Windows Server 2016 version 1803 の環境を代理監視による監視対象としている場合、[サービスステータスの更新]ボタンをクリックした際に「アクセスが拒否されました」というエラーでサービス一覧の取得に失敗することがあります。この際は“サービス名”フィールドへ監視するサービス名を直接入力してください。

●“サービス名”フィールドへ監視するサービス名を直接入力する

●[サービスステータスの更新]ボタンをクリックして、サービスを選択する

監視対象コンピューターに導入されているすべてのサービスをリスト表示しますので、コントロール対象のサービスをクリックした状態で[選択]ボタンをクリックするか、ダブルクリックすることで“サービス名”フィールドに設定することができます。

3. “制御の種類”フィールドに、コントロール方法を設定します。

●“開始”ラジオボタンを選択した場合

このアクション項目のための条件が満たされたときに、選択されたサービスを開始します。

●“停止”ラジオボタンを選択した場合

このアクション項目のための条件が満たされたときに、選択されたサービスを停止します。

●“再起動”ラジオボタンを選択した場合

このアクション項目のための条件が満たされたときに、選択されたサービスを再起動します。

7.7.5 シャットダウンアクション

シャットダウンアクション項目は、アクションを実行させたい監視項目がしきい値のレベルに達した場合、
またはしきい値のレベルが変化した場合に、監視対象コンピューターをシャットダウンさせることができます。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、
全てのアクション項目で共通です。
シャットダウンアクションのみ、“1 回のみ実行（実行後、自動的にアクションが無効となります）”チェックボックスにチェックが入っています。
「全般」タブの詳細は、‘7.7.3 アクション項目の概要’の項目‘B.「全般」タブ’を参照ください。

●“1 回のみ実行（実行後、自動的にアクションが無効となります）”チェックボックスにチェックを入れた場合、
BOM 7.0 が監視対象コンピューターをシャットダウンするのは 1 回だけです。
監視対象コンピューターが再起動され、BOM 7.0 が自動的にスタートアップすると、シャットダウンアクション項目は“無効”になっていますので、必要に応じて手動で“有効”にする必要があります。

●BOM 監視サービスを“自動スタートアップ”に設定した上で、“1 回のみ実行（実行後、自動的にアクションが無効となります）”チェックボックスのチェックを外してシャットダウンアクションの実行条件が毎回満たされた場合に下記の例のように
監視対象コンピューターのスタートアップとシャットダウンの無限ループが発生する可能性があります。

例：

ディスク容量監視でのディスク使用率が“90%”をしきい値としており、シャットダウンアクションを起動させた場合、

監視対象コンピューターはシャットダウンされます。

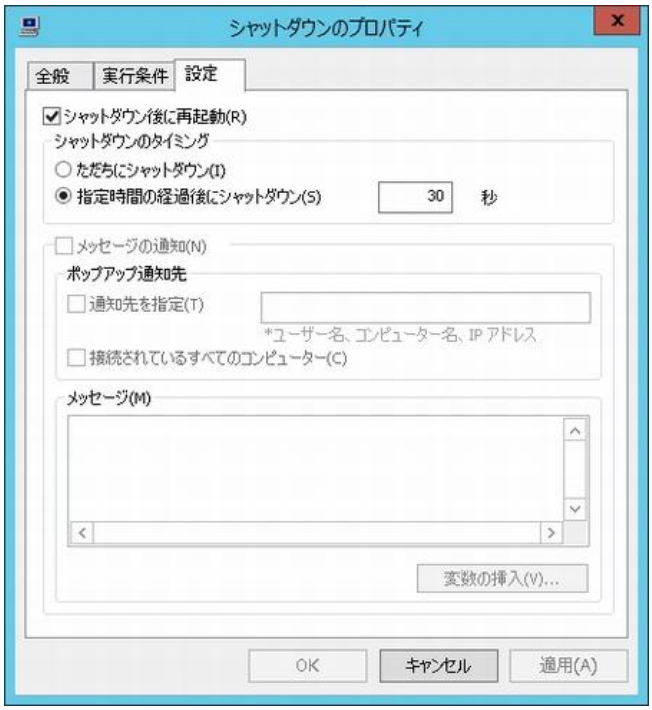
次に、BOM 監視サービスが“自動スタートアップ”に設定されている場合、監視対象コンピューターが再起動した後に、BOM 7.0 のディスク容量監視が“90%”の使用率を検出し、再度コンピューターをシャットダウンします。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。

「実行条件」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ



1. “シャットダウン後に再起動”チェックボックスにチェックを入れることで、監視対象コンピューターのシャットダウン後に再起動させることができます。
2. “シャットダウンのタイミング”は、シャットダウンの方法を下記のどちらかより指定することができます。
   - ●“ただちにシャットダウン”ラジオボタンを選択した場合

     条件が満たされた直後に、システムをシャットダウンします。
   - ●“時間指定の経過後にシャットダウン”ラジオボタンを選択した場合

     条件が満たされた直後より、“指定時間”フィールドに入力した秒数が経過するまで待ってから、監視対象コンピューターをシャットダウンします。
3. “メッセージの通知”チェックボックスは使用できません。

   同様に“メッセージの通知”エリアに含まれる各設定(“ポップアップ通知先”、“メッセージ”)についても使用できません。

7 .7 .6 監視有効/無効アクション

監視有効/無効アクション項目は、アクションを実行させたい監視項目がしきい値のレベルに達した場合、
またはしきい値のレベルが変化した場合に、指定した監視グループあるいは監視項目の有効/無効を制御します。

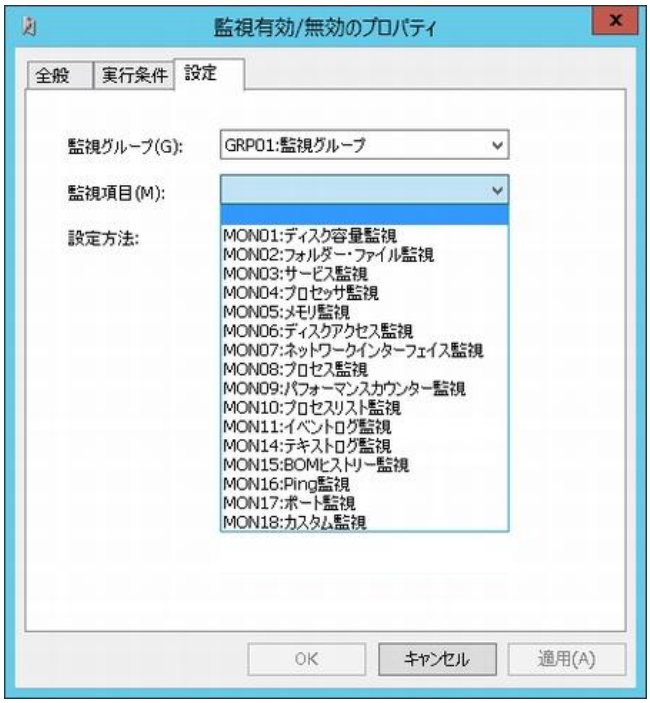
A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、
全てのアクション項目で共通です。
「全般」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。
「実行条件」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ



1. 対象の“監視グループ”、あるいは“監視グループ”と“監視項目”を指定します。
2. 手順 1.で指定した“監視グループ”または“監視項目”を、“有効”にするか“無効”にするかをラジオボタンで選択します。
   なお、監視項目に対する“有効”、“無効”のアクション結果は、指定した“監視項目”の「全般」タブの“開始時刻”を
   基準に反映されます。
   ●“監視項目”の「全般」タブで、“サービスの開始直後”ラジオボタンを選択している場合
   監視サービスが起動してからを基準とします。

●“監視項目”の「全般」タブで、“指定時刻”ラジオボタンを選択している場合

“指定時刻”を基準としますので、監視開始時刻からの基準で監視間隔単位の監視有効/無効を判断します。

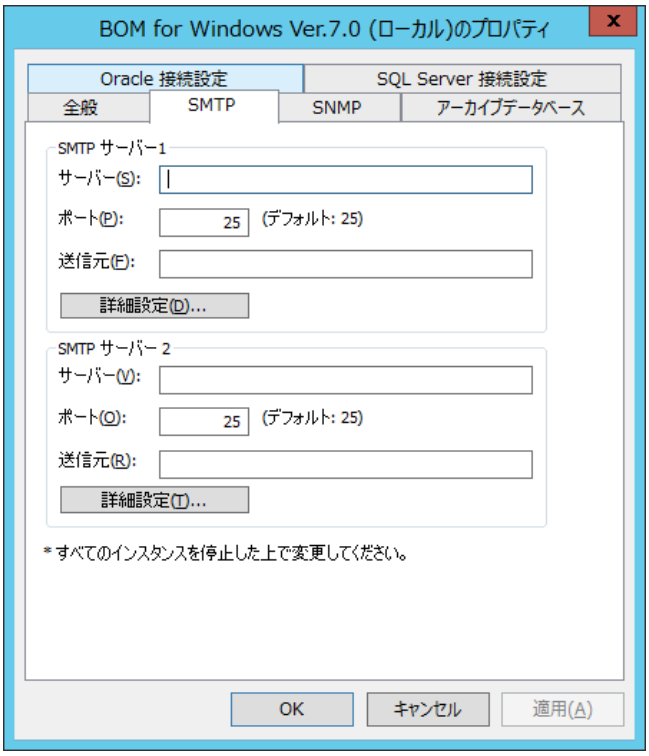
例:

監視開始時刻が午前 0 時に始まり、途中監視有効から無効になった監視項目 A が監視間隔 1 時間で存在する場合、他の監視項目 B のアクションが監視項目 A に対して午前 0 時 30 分で監視有効のアクションが起きた時に、実際に監視項目 A の監視が開始するのは午前 1 時になります。

7 .7 .7 メール送信アクション

メール送信アクション項目は、アクションを実行させたい監視項目がしきい値のレベルに達した場合、
またはしきい値のレベルが変化した場合に、指定したメールアドレスにメールを送信します。

●事前に、BOM マネージャーのスコープペインの“BOM for Windows Ver.7.0 （ローカル）”の“プロパティ”画面の「SMTP」タブで“SMTP サーバー”設定値を設定する必要があります。詳細は‘2 .3 .3 SMTP 情報の設定’を参照ください。



A. 「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、
全てのアクション項目で共通です。

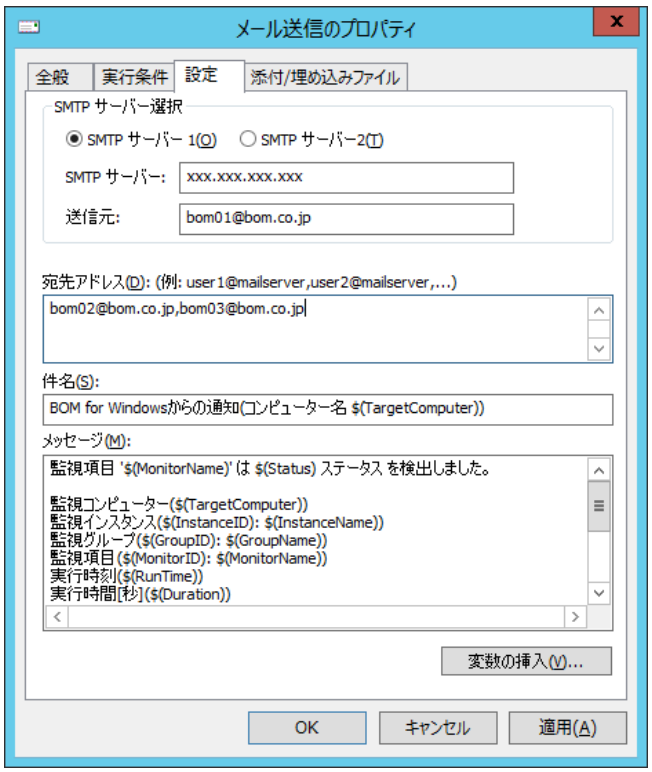
「全般」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘B.「全般」タブ’を参照ください。

B. 「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。

「実行条件」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ



1. “SMTP サーバー選択”フィールドで、“SMTP サーバー1”ラジオボタンまたは“SMTP サーバー2”ラジオボタンのいずれかを選択します。

   ●上記を選択後、“SMTP サーバー”フィールドと“送信元”フィールドに情報が何も表示されない場合、“SMTP サーバー”に関する情報を設定する必要があります。詳細は‘2 .3 .3 SMTP 情報の設定’を参照ください。

2. “宛先アドレス”フィールドに、メッセージの宛先となる電子メールアカウントを入力します。

   ●複数のアドレスを指定する際には、カンマで区切って入力します。

   ●宛先アドレスの最大文字数は 1000 文字です。

3. “件名”フィールドに、メールの件名を入力します。

   ●既定値で設定されている件名の変数は、[変数の挿入]ボタンをクリックすることで変数リストを表示させて確認ができます。

4. “メッセージ”フィールドに、メールの本文を入力します。

   ●“メッセージ”の最大文字数は 2500 文字です。

   ●[変数の挿入]ボタンより 2500 文字を超える入力をした場合、“メッセージ”フィールドに反映されるのは 2500 文字です。

   ●変数に関しては展開後の文字数で換算されますが、展開後 2500 文字を超えた場合でも問題なくアクションは実行します。

   ●メール送信のメッセージは RFC2822 より、メール本文の 1 行あたりの文字数が決まっており、BOM 7.0 では、1 行における文字列が 991 バイト以上になった時点で強制改行します。

D.「添付/埋め込みファイル」タブ

●[変数の挿入]ボタンより変数名を指定することで、テキストログ監視やイベントログ監視でエクスポートしたテキストファイルをメールに添付することができます。

1. “ファイルを添付あるいは埋め込む”チェックボックスにチェックを入れることで、メール送信アクションにファイルを添付する、または添付ファイルの中身をメール本文に埋め込むことができます。
   ●ファイルを埋め込む場合には、埋め込むファイルはテキストファイルである必要があります。
2. “ファイル名”フィールドに、下記のいずれかの手段で添付したいファイルの“ファイル名”を設定します。
   手順 3.の[追加]ボタンをクリックするまで、選択したファイルは添付ファイルの対象にはなっておりませんのでご注意ください。
   ●添付したいファイルの絶対パスを入力する。
   ●[...]ボタンをクリックし、“ファイル選択”画面より添付ファイルを選択する。
   ●[変数の挿入]ボタンをクリックし、テキストログ監視やイベントログ監視でエクスポートしたテキストファイルを選択したい場合
   “変数の挿入”画面で“検出テキストのエクスポートファイル名を指定”チェックボックスにチェックを入れた後、[挿入]ボタンをクリックすることで、<$(DetectedDataDir)¥$(MonitorID).txt>という文字が設定され、テキストログ監視やイベントログ監視でエクスポートしたテキストファイルを指定することができます。
   ●[変数の挿入]ボタンをクリックし、独自のファイル名形式で変数を使用しているようなファイルを選択したい場合
   “変数の挿入”画面で“検出テキストのエクスポートファイル名を指定”チェックボックスのチェックを外した後、変数リストの対象変数をクリックして[挿入]ボタンをクリックするか、直接変数をダブルクリックすることで、“変数の挿入”フィールドに、変数を含んだ“ファイル名”を設定します。
3. [追加]ボタンをクリックすると、手順 2.で指定したファイルを、添付ファイルの対象として下部の“ファイル”フィールドに表示します。

4. ファイルをメール本文に埋め込みたい場合、手順 3.の“ファイル”フィールドの“ファイル名”の横にあるチェックボックスにチェックを入れます。

   ●JIS、Shift JIS 以外のテキストファイルの埋め込みはできません。

5. “ファイルを Zip 形式で圧縮（ファイルを添付する場合にのみ有効）”チェックボックスにチェックを入れることで、手順 4.でメール本文の埋め込み対象にしなかった添付ファイル一式を圧縮することができます。

   ●手順 4.で、埋め込み対象に指定したファイルは圧縮の対象にはなりません。

   ●圧縮した添付ファイルに対して、パスワードによる暗号化を行う場合には、“パスワードによる暗号化”チェックボックスにチェックを入れて、“パスワード”と“パスワードの確認入力”を入力します。

7 .7 .8 SNMP トラップ送信アクション

SNMP トラップ送信アクション項目は、アクションを実行させたい監視項目がしきい値のレベルに達した場合、またはしきい値のレベルが変化した場合に、指定した SNMP マネージャーに SNMP トラップを送信します。

●事前に、BOM マネージャーのスコープペインの“BOM for Windows Ver.7.0 （ローカル）”の“プロパティ”画面の「SNMP」タブで“SNMP マネージャー”設定値を設定する必要があります。詳細は‘2 .3 .4 SNMP 情報の設定’を参照ください。

●代理監視の場合には、代理監視元コンピューターではなく、代理監視はコンピューターの IP アドレスが SNMP マネージャーに通知されます。SNMP マネージャー側の設定を行う際には、代理監視先コンピューターの IP アドレスも登録してください。

A. 「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、全てのアクション項目で共通です。

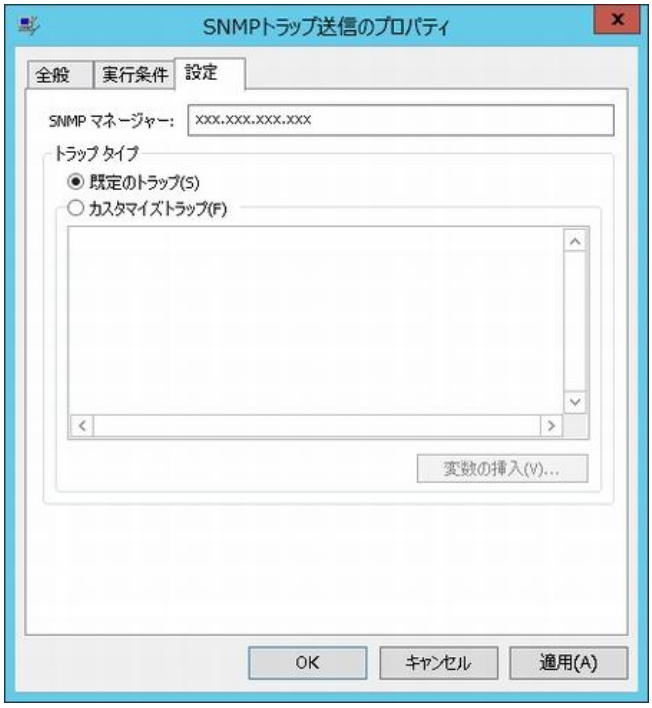
「全般」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。

「実行条件」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ



1. “SNMP マネージャー”フィールドに、情報が何も表示されない場合、“SNMP マネージャー”に関する情報を設定する必要があります。詳細は‘2 .3 .4 SNMP 情報の設定’を参照ください。
2. “トラップ タイプ”フィールドは、下記のどちらかを設定します。
   ●“既定のトラップ”ラジオボタンを選択した場合
   メッセージは BOM 7.0 の既定のトラップ内容と共にトラップ送信されます。
   ●“カスタマイズトラップ”ラジオボタンを選択した場合
   “メッセージ”フィールドに指定した内容でトラップ送信されます。
3. “メッセージ”フィールドは、手順 2.で“カスタマイズトラップ”ラジオボタンを選択した際に、トラップ送信される内容です。
   ●“メッセージ”の最大データサイズは 255byte です。制限を超えている場合、エラーとなり SNMP トラップが実行されません。
   ●変数の展開後のデータサイズが 255byte を超える場合、エラーとなり SNMP トラップが実行されません。
4. [変数の挿入]ボタンをクリックすると、手順 2.の“メッセージ”フィールドに挿入可能な、BOM 7.0 の予約済み変数をリストから選択することができる“変数の挿入”画面を表示させることができます。
   ●予約済み変数については ‘第 15 章 予約済み変数’ を参照してください。
   ●[変数の挿入]ボタンより、“グループ名”、“監視名”、“アクション名”に格納される最大文字数は 63 文字です。
   制限数を超えているとエラーになり、SNMP トラップが実行されません。

D. SNMP トラップの送信内容

SNMP トラップの送信内容は、各“OID”に設定されています。“OID”の詳細は下記の表を参照ください。

●既定のトラップ内容

送信コンピューター名（TargetComputer）、インスタンス ID（InstanceID）、グループ名（GroupName）、

監視項目名（MonitorName）、監視取得値（Value）、監視結果（ResultCode）で、各内容に“OID”が対応しております。

●カスタマイズトラップ時の送信内容

カスタマイズトラップメッセージ（$（UserMsg））

OID	オブジェクト名	通知内容
監視アイテム（オブジェクト）		
1.3.6.1.4.1.10035.2.10.1.1.1	mxTargetComputer	コンピューター名
1.3.6.1.4.1.10035.2.10.1.1.3	mxInstanceID	インスタンス ID
1.3.6.1.4.1.10035.2.10.1.1.6	mxGroupName	監視グループ名
1.3.6.1.4.1.10035.2.10.1.1.8	mxMonitorName	監視項目名
1.3.6.1.4.1.10035.2.10.1.1.10	mxActionName	アクション名
1.3.6.1.4.1.10035.2.10.1.1.13	mxResultCode	監視結果コード
1.3.6.1.4.1.10035.2.10.1.1.14	mxMonitorValue	監視取得値
1.3.6.1.4.1.10035.2.10.1.1.15	mxMonitorStatus	監視ステータス
1.3.6.1.4.1.10035.2.10.1.1.16	mxExitCode	終了コード
1.3.6.1.4.1.10035.2.10.1.1.25	mxUserMsg	ユーザーメッセージ
監視ステータス（トラップ）		
1.3.6.1.4.1.10035.2.10.1.2.0.20	mxMonitorFailure	監視失敗
1.3.6.1.4.1.10035.2.10.1.2.0.21	mxStatusNormal	監視正常
1.3.6.1.4.1.10035.2.10.1.2.0.22	mxStatusWarning	監視注意
1.3.6.1.4.1.10035.2.10.1.2.0.23	mxStatusCritical	監視危険
アクションステータス（トラップ）		
1.3.6.1.4.1.10035.2.10.1.2.0.30	mxActionFailure	アクション失敗
1.3.6.1.4.1.10035.2.10.1.2.0.31	mxActionSuccess	アクション成功
1.3.6.1.4.1.10035.2.10.1.2.0.32	mxActionError	アクションエラー
その他（トラップ）		
1.3.6.1.4.1.10035.2.10.1.2.0.41	mxUserMessage	ユーザー定義

7 .7 .9 イベントログ書き込みアクション

イベントログ書き込みアクション項目は、アクションを実行させたい監視項目がしきい値のレベルに達した場合、
またはしきい値のレベルが変化した場合に、指定した事項をイベントログに書き込みます。

●イベントログに書き込む内容はあらかじめ既定値が決まっており、「設定」タブの“既定のメッセージ”フィールドの内容は必ず書き込まれます。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、
全てのアクション項目で共通です。

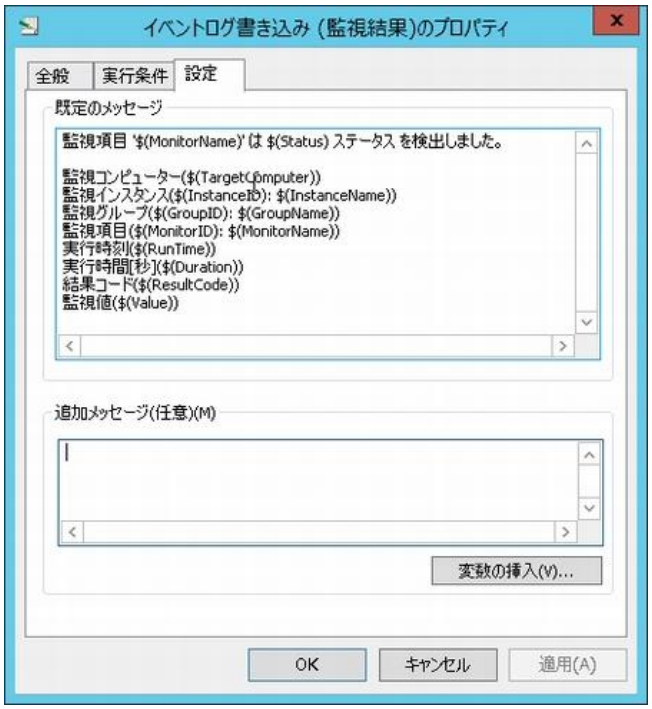
「全般」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。

「実行条件」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ



1. “既定のメッセージ”フィールドの内容は必ずイベントログに書き込まれます。
   ●“既定のメッセージ”中の“$”で始まる記号は変数になっています。
   ●[変数の挿入]ボタンをクリックして変数の内容を確認することができます。

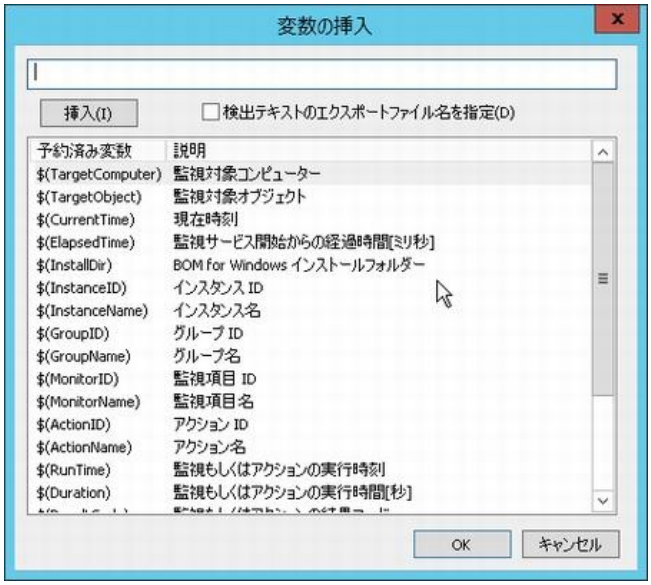
2. “追加メッセージ(任意)”フィールドに入力した内容は、既定値以降に付け加えてイベントログに書き込むことができます。

●[変数の挿入]ボタンをクリックし、変数を使用することもできます。

●追加メッセージの最大文字数は 2000 文字です。

●[変数の挿入]ボタンより 2000 文字を超える入力をした場合、“メッセージ”フィールドに反映されるのは 2000 文字です。

●変数に関しては展開後の文字数で換算されますが、展開後 2000 文字を超えた場合でも問題なくアクションは実行します。



D. イベントログの出力内容

イベントログ書き込みアクションで、実際にイベントログに書き込まれる内容は下記の通りです。

●イベントログの種別

“アプリケーション”

●ソース

“Bom7Action”

●分類

“なし”

●イベントの種類

監視ステータスによって、イベントの種類が変わります。ステータス、イベントの種類、イベント ID の相関は下記の通りです。

イベント ID	監視ステータス	イベントログ出力	
		種類	説明
3300	正常	情報	説明本文は全て共通で既定のメッセージが書き込まれます。 追加メッセージが設定されていれば既定メッセージに追記されます。
3301	注意	警告	
3302	危険	エラー	
3303	失敗	エラー	

7 .7 .10 カスタムアクション

カスタムアクション項目は、アクションを実行させたい監視項目がしきい値のレベルに達した場合、
またはしきい値のレベルが変化した場合に、サードパーティ製のコマンドラインベースのプログラムや、独自に記述した
テキストベースのスクリプトプログラム（バッチファイルや WSH、PowerShell など）を実行させることができます。

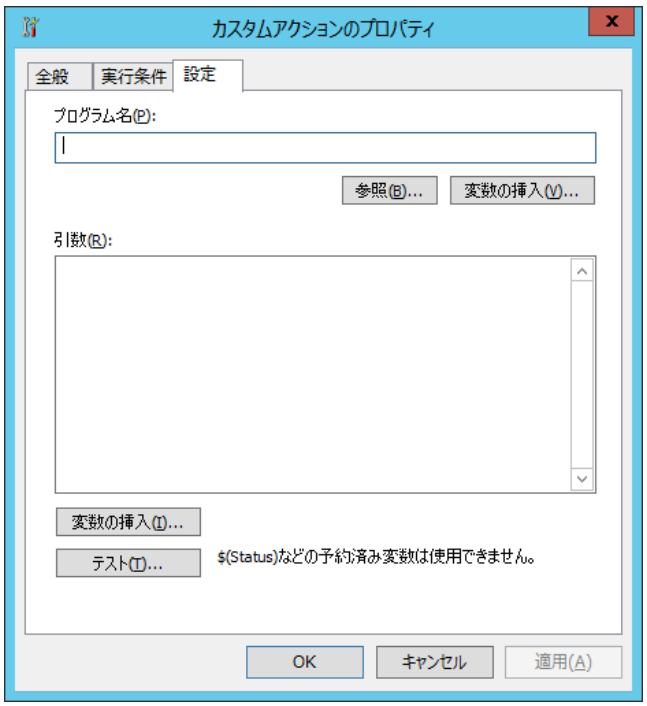
A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、
全てのアクション項目で共通です。
「全般」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。
「実行条件」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ



1. “プログラム名”フィールドに、任意の“実行プログラム名”を下記のどちらかの手段で設定します。

   ●“実行プログラム名”を、絶対パスで入力する。

   “プログラム名”フィールドの[変数の挿入]ボタンをクリックし、“プログラム名”のパスに BOM 7.0 の予約済み変数を
   使用することもできます。予約済み変数については ‘第 15 章 予約済み変数’ を参照してください。

●[参照..]ボタンをクリックして、“ファイル選択”画面より“実行プログラム”を選択する。

“隠しファイルの表示”チェックボックスもしくは“保護されたシステムファイルの表示”チェックボックスにチェックを入れると、条件に応じた該当ファイルが表示されます。

2. “引数”フィールドには実行プログラムの引数を記述します。

●“引数”フィールドの[変数の挿入]ボタンをクリックし、“引数”に変数を指定することができますが、手順 4.のテスト実行時に BOM 7.0 の予約済み変数を使用することはできません。

予約済み変数については‘第 15 章　予約済み変数’を参照してください。

3. [テスト]ボタンをクリックすると、“アクションのテスト”画面を表示させ、「設定」タブの設定を加えてテスト実行します。

●コンソールプログラムをカスタムアクションとして設定する場合には、BOM 監視サービスと BOM ヘルパーサービスのサービスアカウントをローカルシステムアカウントとし、デスクトップとの対話にチェックしてください。

●代理監視の場合にはコンソールプログラムは指定ができません。

●アクションの終了待ち時間は、既定値で 2 時間です。2 時間経過後、アクションのプロセスは強制終了されます。

7 .7 .11 syslog 送信アクション

syslog 送信アクション項目は、アクションを実行させたい監視項目がしきい値のレベルに達した場合、
またはしきい値のレベルが変化した場合に、任意の送信先ホストに指定した事項を syslog 形式で送信します。

※ syslog Protocol としては、RFC 3164（The BSD syslog Protocol）にのみ対応しています。

※ UDP を使用して送信するため、syslog サーバー側で取りこぼしが発生する可能性があります。

※ メッセージの送信文字コードは UTF-8 です。また、ASCII コード 33(0x21)～126(0x1E) + 32(0x20) 以外の文字のロギング（日本語などがロギングまたは表示されるかどうかなど）は受信先の syslog サーバーの仕様によります。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、
全てのアクション項目で共通です。

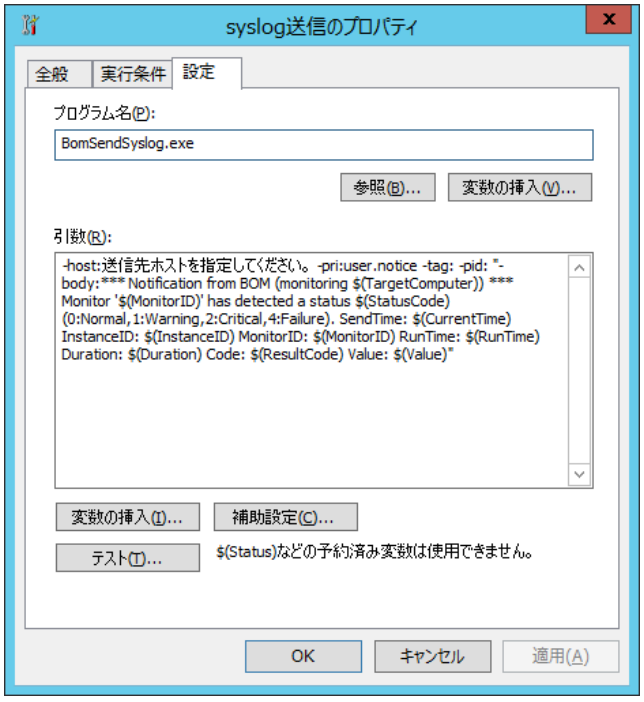
「全般」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。

「実行条件」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

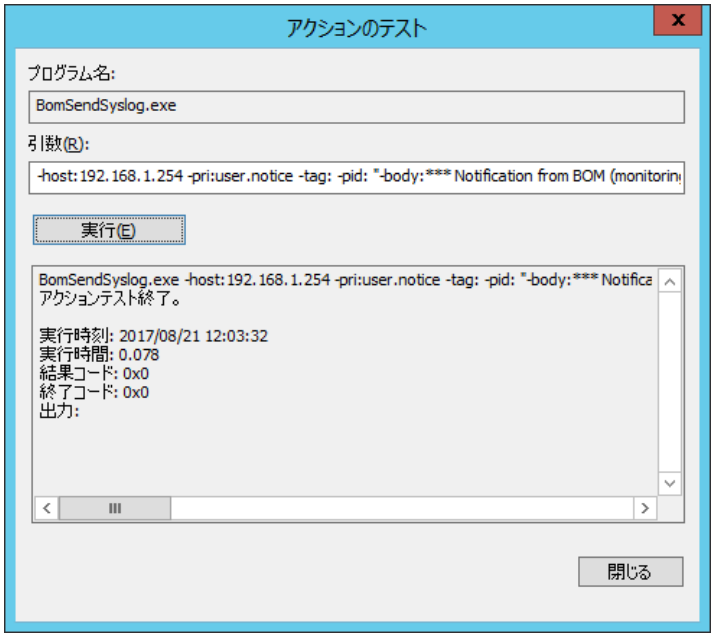
C.「設定」タブ



1. “プログラム名”フィールドにはあらかじめ“BomSenSyslog.exe”と入力されていますので、変更しないでください。
   また、“プログラム名”フィールドの[参照]ボタンおよび[変数の挿入]ボタンは使用しないでください。
2. “引数”フィールドは以下の内容で設定および入力してください。

- 引数“-host:”について、“送信先ホストを指定してください。”部分を削除し、syslog を送信するホストの IP アドレス（IPv4、IPv6）またはコンピューター名で指定します。
- 引数“-body:”から末尾の「”」（ダブルクォーテーション）の間に、送信する情報が設定できます。変数を使用する場合は、“引数”フィールドの[変数の挿入]ボタンから入力してください。

3. “引数”フィールドの[変数の挿入]ボタンをクリックすると、“引数フィールド”に使用できる予約済み変数が表示されます。
   一覧から予約済み変数を選択し、[挿入]ボタン→[OK]ボタンをクリックすると、“引数フィールド”のカーソルの位置に選択した変数が挿入されます。
   - 予約済み変数については‘第 15 章 予約済み変数’を参照してください。
4. [補助設定]ボタンは使用できません。
5. [テスト]ボタンをクリックすると、“アクションのテスト”画面を表示し、「設定」タブの設定を加えてテスト実行します。
   - テスト実行時に BOM 7.0 の予約済み変数を使用することはできません。



7.7.12 AWS S3 ファイル送信アクション

AWS S3 ファイル送信アクション項目は、アクションを実行させたい監視項目がしきい値のレベルに達した場合、またはしきい値のレベルが変化した場合に、Amazon S3 および、Amazon S3 の API に完全準拠する Amazon S3 互換ストレージ上のバケットへ指定したファイルをアップロードすることができます。

※ Amazon S3 互換ストレージについて、API 準拠をうたう全てのストレージでの動作を保証するものではありません。
弊社では、クラウディアン株式会社の CLOUDIAN HYPERSTORE について動作確認を取っており、今後の対応確認情報は弊社ウェブサイト(www.say-tech.co.jp)で随時公開いたします。

※ “AWS S3 ファイル送信アクション項目”を使用するためには、Microsoft .NET Framework Ver.3.5 SP1 を事前にインストールする必要があります。インストール方法については ‘第 14 章 Microsoft .NET Framework Ver.3.5 SP1 のインストール’ 参照してください。
また、このアクションは AWS への接続に TLS1.2 のプロトコルを使用するため、.Net Framework 3.5 SP1 インストール後、さらに TLS1.2 対応の更新プログラムを適用する必要があります。更新プログラムは Windows Update から適用するか、Microsoft 社のウェブサイトよりファイルをダウンロードして適用してください。(Windows Server 2016、Windows Server 2019 および Windows 10 では Windows Update を使用してください。)

(参考情報)

2020 年 4 月 10 日現在、該当のファイルは以下のサイトからダウンロードしていただけます。

Windows Server 2008 R2 SP1 Windows 7 SP1	Support for TLS v1.2 included in the .NET Framework version 3.5.1 https://support.microsoft.com/ja-jp/kb/3154518
Windows Server 2012	Support for TLS v1.2 included in the .NET Framework version 3.5 https://support.microsoft.com/ja-jp/kb/3154519
Windows Server 2012 R2 Windows 8.1	Support for TLS v1.2 included in the .NET Framework version 3.5 SP1 on Windows 8.1 and Windows Server 2012 R2 https://support.microsoft.com/ja-jp/kb/3154520

※ プロキシサーバーを利用する場合の資格情報の設定は、基本認証、NTLM 認証をサポートしております。

※ 名前の末尾が“.”(半角ピリオド)の S3 上のフォルダーを送信先として指定すると、ファイル送信アクションは失敗します。この現象は.Net Framework 3.5 の仕様です。

※ 送信対象としてフォルダーを指定する場合、そのフォルダー配下のシンボリックリンクとそのリンク先はアップロードされません。送信対象としてシンボリックリンクを直接指定した場合は、そのリンク先のファイルはアップロードされます。

例) C:¥Program Data¥link (シンボリックリンク)

上記の場合、“C:¥Program Data”を送信対象として指定すると、link(シンボリックリンク)はアップロード対象として除外されます。

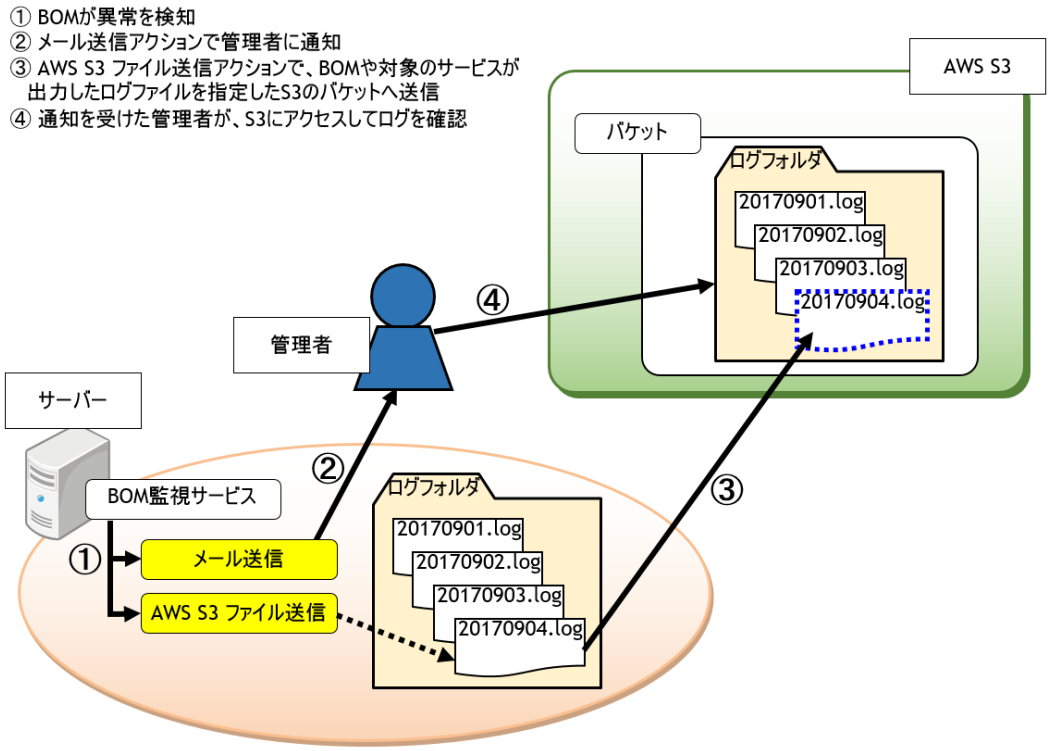
“C:¥Program Data¥link(シンボリックリンク)”を送信対象として指定した場合は、“link(シンボリックリンク)”フォルダーとそのリンク先のファイルをアップロードします。

※ 送信可能なファイルサイズ上限は 5TB です。

※ ファイル送信の処理時間が 2 時間を経過した場合、カスタムアクションの仕様により強制終了します。

※　100MB を超えるファイルをアップロードする場合は、マルチパートアップロードによるアップロードに切り替わるため、Put リクエスト数が増加することがあります。

● 運用例



例えば管理者が外出中の場合や、サーバーへのアクセス権限がないユーザーでも、S3 へログインできる環境があればログから状況を確認できます。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、全てのアクション項目で共通です。

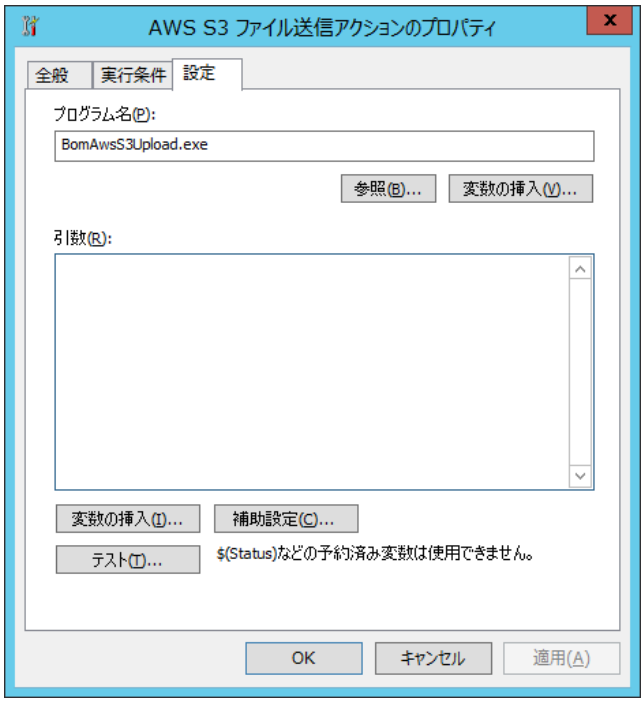
「全般」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘B.「全般」タブ’を参照ください。

B.「実行条件」タブ

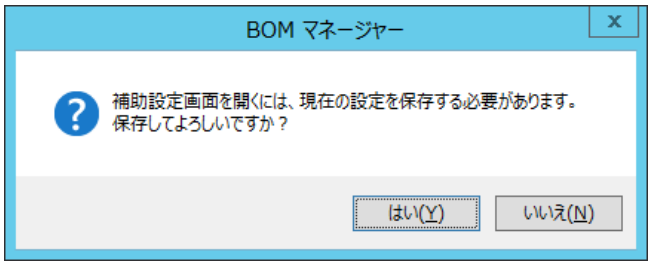
「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべてのアクション項目で共通です。

「実行条件」タブの詳細は、‘7 .7 .3 アクション項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ

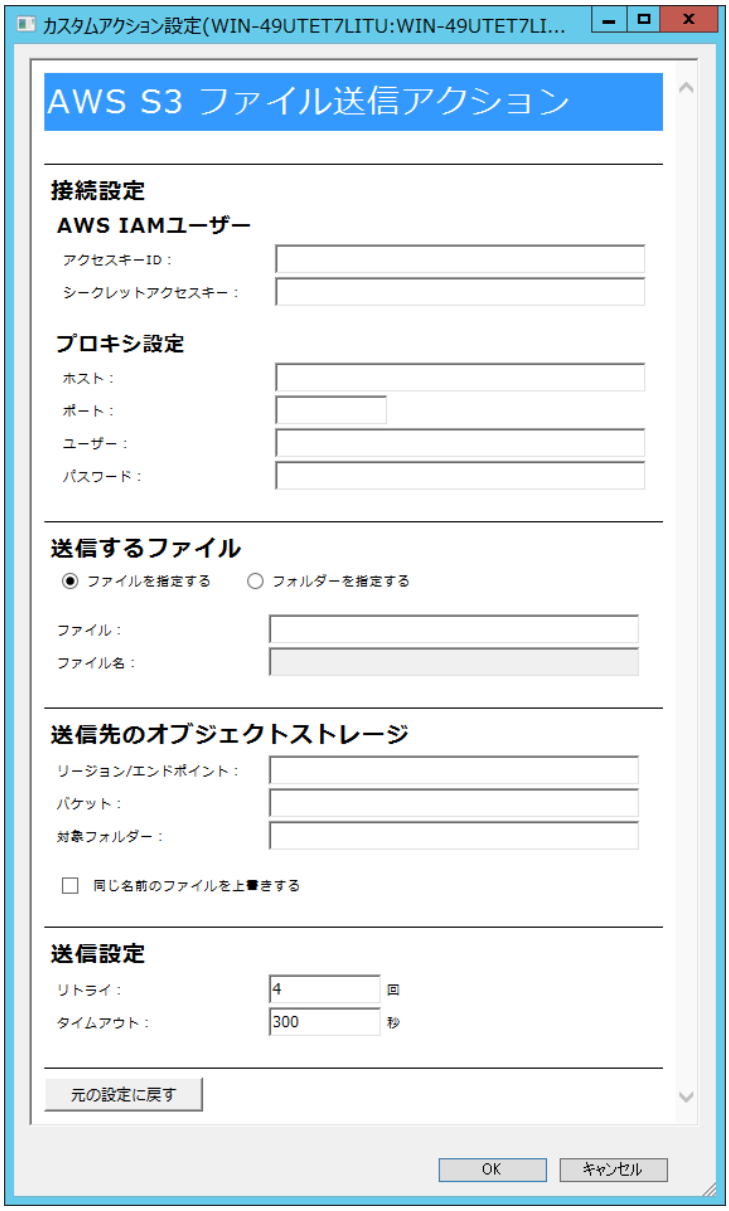


1. “プログラム名”フィールドにはあらかじめ“BomAwsS3Upload.exe”と入力されていますので、変更しないでください。
   本アクションの詳細な設定は補助設定画面で行い、設定後は“引数”フィールドへ自動的に必要な値が入力されます。
   この画面では“引数”フィールド内の入力および編集を行わないでください。
2. [補助設定]ボタンをクリックします。
3. [補助設定]ボタンをクリックすると以下の要求が表示されますので、[はい]ボタンをクリックします。



4. 保存が完了すると、「AWS S3 ファイル送信アクション」の補助設定画面が表示されます。

D.「AWS S3 ファイル送信アクション」補助設定



1. “AWS IAM ユーザー”フィールド(必須)

   ファイル送信先の Amazon S3 および、Amazon S3 互換ストレージについて、接続に必要なユーザー情報を入力します。

   (参考情報)

   Amazon S3 の場合、IAM でアクセスキーを作成し、“アクセスキーID”フィールドおよび、“シークレットアクセスキー”フィールドに入力します。IAM でのアクセスキー作成については、2020 年 4 月 10 日現在、アマゾン ウェブ サービスの以下のサイトに該当の手順が記載されています。

   “AWS Identity and Access Management ユーザーガイド - IAM ユーザーのアクセスキーの管理”

   http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_access-keys.html

2. “プロキシ設定”フィールド(任意)

   プロキシを使用して接続する場合、“ホスト”フィールドおよび、“ポート”フィールドの入力は必須です。またプロキシで認証が必要な場合は“ユーザー”フィールドおよび、“パスワード”フィールドに入力してください。

3. “送信するファイル”フィールド

   送信するファイルの条件を設定します。

   ● “ファイルを指定する”、“フォルダーを指定する”(選択必須)

   ファイル単位で送信する対象を指定する場合は“ファイルを指定する”にチェックします。

   フォルダー単位で送信する対象を指定する場合は“フォルダーを指定する”にチェックします。

   ● “ファイル”フィールド(必須)

   “ファイルを指定する”を選択した場合に表示されます。

   送信したいローカルコンピューター上のファイルを入力してください。

   例: C:¥Program Files¥appriction¥log¥applog.log

   ● “フォルダー”フィールド(必須)

   “フォルダーを指定する”を選択した場合に表示されます。

   送信したいファイルが保存されているローカルコンピューター上のフォルダーを入力してください。

   例: C:¥Program Files¥appriction¥log¥

   ● “ファイル名”フィールド

   “フォルダーを指定する”を選択した場合に入力が有効となります。

   “フォルダー”フィールドで指定したフォルダー配下のファイルについて、送信するファイルを絞り込むための条件(ワイルドカード使用可)を入力します。未入力の場合は、指定フォルダー配下のサブフォルダーを含むすべてのファイルが送信対象となります。

   例 1: *.txt

   例 2: log*.log

4. “送信先のオブジェクトストレージ”フィールド(必須)

   ● “リージョン/エンドポイント”フィールド

   ファイル送信先の Amazon S3 のリージョンコード、または Amazon S3 互換ストレージのエンドポイントを入力します。

   ※ エンドポイントを指定する場合は、必ず https://から始まる文字列を入力してください。

   例 1) リージョンコードでアジアパシフィック(東京)を指定: ap-northeast-1

   例 2) CLOUDIAN HYPERSTORE でエンドポイントを指定: https://xxxxxx.s3.cloudian.jp

   (参考情報)

   Amazon S3 における各リージョンの詳細なコードについては、2020 年 4 月 10 日現在、以下のアマゾン ウェブ サービスのリファレンスでご確認いただけます。

   “アマゾン ウェブ サービス 全般的なリファレンス - Amazon Simple Storage Service (Amazon S3)”

   http://docs.aws.amazon.com/ja_jp/general/latest/gr/rande.html#s3_region

   ● “バケット”フィールド

   ファイルの送信先となる Amazon S3 または Amazon S3 互換ストレージのバケット名を入力します。

● “対象フォルダー”フィールド

ファイルの送信先となる Amazon S3 または Amazon S3 互換ストレージ上のフォルダーを入力します。

階層はスラッシュで区切ってください。

例： server01/bomaction/log/

● “同じ名前のファイルを上書きする”チェックボックス

Amazon S3 または Amazon S3 互換ストレージの指定したフォルダー内に、ローカルコンピューターから送信したファイルと同名のファイルが存在した場合の動作を指定します。

チェックをした場合　　:ファイルを上書きします。

チェックしていない場合 :ファイルを送信せずスキップします。このスキップは送信失敗と見做しません。

5. “送信設定”フィールド

ファイル送信に失敗した際の、リトライ回数及びタイムアウト（単位：秒）の条件を設定します。

デフォルト値はリトライ 4 回、タイムアウト 300 秒です。

6. 各フィールドに必要事項を入力して[OK]ボタンをクリックすると、補助設定画面は閉じます。

継続して本アクションの設定を行う場合は、改めてプロパティを開いてください。

7 .7 .13 HTTPS 送信アクション

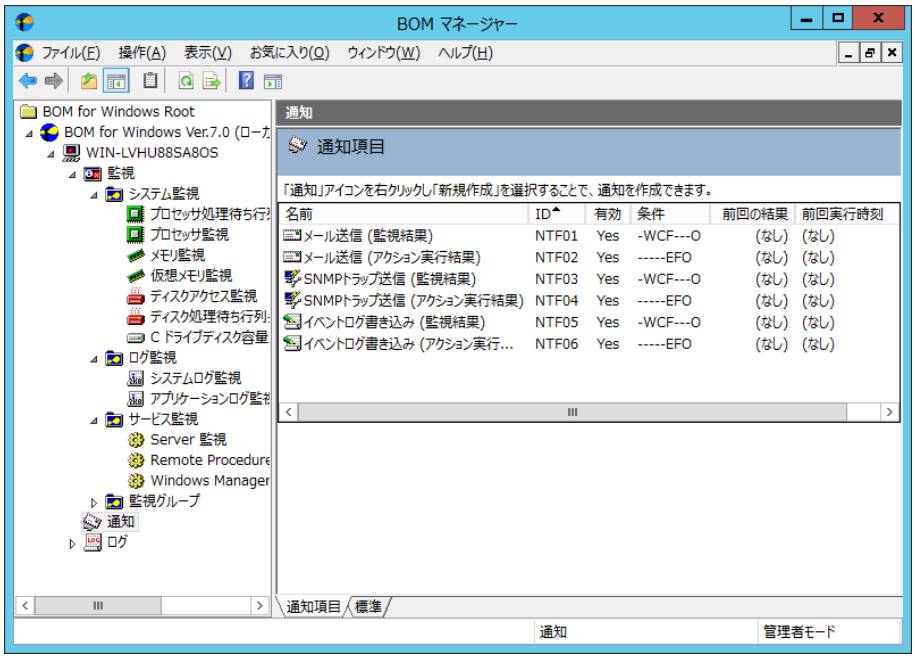
HTTPS 送信アクション項目は、HTTPS プロトコルを使用して、アクションを実行させたい監視項目がしきい値のレベルに達した場合に、監視結果の情報や任意のファイルを指定した Internet Information Services の動作する Web サーバーへ送信します。

本アクションの詳細については、‘BOMW7.0-HTTPS 送受信マニュアル’を参照してください。

第8章 通知

8 .1 通知の解説

通知項目とは、‘第 5 章監視項目’の監視項目のステータスである“正常”、“注意”、“危険”、“失敗”と、‘第 7 章アクション項目’のアクション項目のステータスである“成功”、“エラー”、“失敗”をトリガーに、メール送信、SNMP トラップ送信、イベントログへの書き込みなどを実行させることができます。



“通知項目”と“アクション項目”の機能は、下記の点で大きく異なります。

●起動条件

インスタンス内のすべての“監視項目”だけではなく、“アクション項目”の各ステータスを起動条件に指定することができます。

“カスタムアクション”より実行したバッチファイルの実行結果が失敗したことをトリガーに、システム管理者に“メール送信”を行うなどの制御ができます。

●起動対象

“監視項目グループ”単位で“通知項目”の起動対象を指定できますので、指定した“監視グループ”に属するすべての“監視項目”と“アクション項目”を、“通知項目”の起動対象に指定することができます。

8 .2 通知項目の作成

1. BOM マネージャーのスコープペインの“通知”を右クリックし、コンテキストメニューの新規作成をクリックします。
2. 表示されたコンテキストメニューの通知項目(“メール送信”、“SNMP トラップ送信”等)をクリックします。
3. 通知項目の起動条件である“監視結果による通知”または“アクション実行結果による通知”のどちらかをクリックすると、通知項目が BOM 7.0 マネージャーの“通知”のリザルトペインに表示されます。

●監視項目は必要に応じて設定値を変更する必要があります。

以降のセクションでは、通知項目を有効にする方法、および使用可能なアクション項目とその設定値の詳細について解説します。

●「全般」タブと「実行条件」タブは、すべてのアクション項目で共通です。

●他のタブは、通知項目によって異なります。

8.3 通知項目のコピー

通知項目をコピーすると、“通知”のリザルトペインに表示されます。

コピーした項目は、同じ名前とプロパティ設定値を持っていますので、設定値を変更する場合は、通知項目の“プロパティ”画面より行います。

1. “通知項目”を右クリックし、コンテキストメニューの“コピー”をクリックします。
2. “通知”を右クリックするか、“通知”のリザルトペインを右クリックし、コンテキストメニューの“貼り付け”をクリックします。
   ●インスタンス間で“通知項目”を“コピー”し、“貼り付ける”ことができます。
   ●リモート接続時のスナップインノード間の“通知項目”のコピーはできません。

8.4 通知項目を有効にする

“通知項目”を実行するには“有効”にしておく必要があります。

“通知項目”を“有効”にするには、下記のいずれかを実行します。

A. “通知項目”を右クリックし、コンテキストメニューの“有効”をクリックします。

B. “通知項目”を右クリックし、コンテキストメニューの“プロパティ”をクリックして“プロパティ”画面を表示させ、“有効”チェックボックスにチェックを入れます。

C. リザルトペインで“通知項目”をダブルクリックして“プロパティ”画面を表示させ、“有効”チェックボックスにチェックを入れます。

D. “通知項目”をクリックし、リザルトペインの画面下部にある“有効”をクリックします。

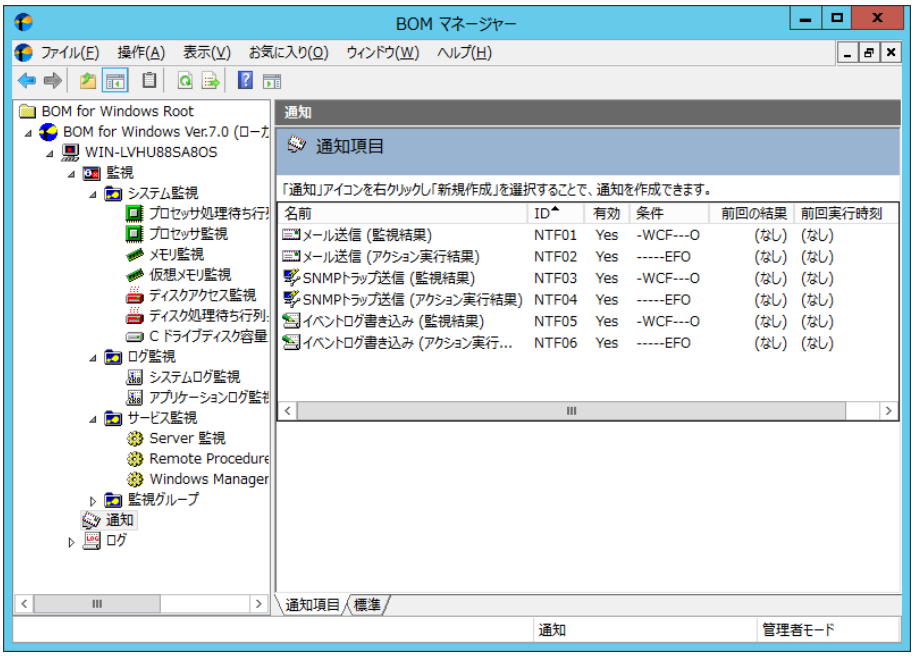
●“通知項目”を“無効”にしたい際には、上記 A.、B.、C.いずれかの手順で“無効”を選択します。

●各通知の「全般」タブの下部“1 回のみ実行（実行後、自動的にアクションが無効となります）”チェックボックスにチェックを入れた場合
該当の通知項目が 1 回のみ実行された後、自動的に“無効”になります。
問題を解消した後などにアクションを引き続き実行したい場合、通知項目の“プロパティ”画面などから、再度“有効”にする必要があります。

8 .5 通知項目のログ

8 .5 .1 リザルトペイン表示

BOM マネージャーの“通知”をクリックすると、リザルトペインに“通知項目”の状態が下記の通り表示されます。



●“名前”列には、実行されるアクション項目がリストされます。

●“ID”列には、通知項目の“BOM ID”がリストされます。

●“有効”列には、通知項目が“有効”か“無効”かが表示されます。

●“条件”列には、通知項目を実行させるために設定した下記の条件が、リスト表示されます。

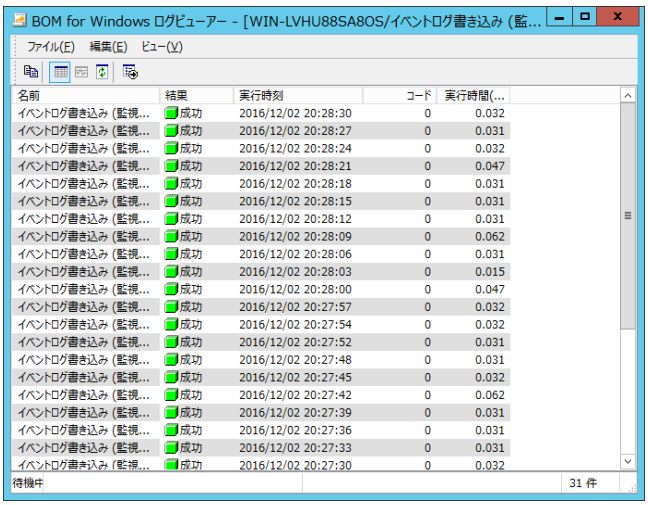
条件記号	条件名	通知項目の“プロパティ”の設定内容
N	正常	“監視するステータス”フィールドの“正常”チェックボックスにチェックが入っている状態
W	注意	“監視するステータス”フィールドの“注意”チェックボックスにチェックが入っている状態
C	危険	“監視するステータス”フィールドの“危険”チェックボックスにチェックが入っている状態
F	失敗	“監視するステータス”フィールドの“失敗”チェックボックスにチェックが入っている状態
S	成功	“アクションの実行結果”フィールドの“成功”チェックボックスにチェックが入っている状態
E	エラー	“アクションの実行結果”フィールドの“エラー”チェックボックスにチェックが入っている状態
F	失敗	“アクションの実行結果”フィールドの“失敗”チェックボックスにチェックが入っている状態
O	変化時のみ	“変化時のみ”ラジオボタンを選択した状態

●“前回の結果”列には、アクション項目の実行結果がリストされます。

●“前回実行時刻”列には、アクション項目が実行された日時がリストされます。

8 .5 .2 ログの表示

BOM のログファイルは、BOM 7.0 が検出したシステム障害のトラブルシューティングを行う際に非常に役立ちます。



1. BOM マネージャーで“通知”ノードをクリックし、リザルトペインに“通知項目”を表示させます。
2. 通知項目を右クリックし、コンテキストメニューの“ログの表示...”をクリックして“通知項目”の“BOM ログビューアー”画面を表示させます。
3. タイトルバーに、現在表示されているインスタンス、通知項目の名前が表示されます。

   一度に複数の“BOM ログビューアー”画面を開くこともできます。

   1 通知項目当たりの最大ログ蓄積量の既定値は 15000 件です。

   ●“名前”列には、実行された通知項目がリストされます。

   ●“結果”列では、通知項目が正常に実行されたかどうかがリストされます。

   ●“実行時刻”列には、通知項目が実行された日時がリストされます。

   ●“コード”列には、エラーコードがリストされます。この値は、通知項目が正常に実行された場合は“0”となります。

   ●“実行時間”列には、BOM 7.0 がその通知項目を完了するまでにかかった時間が秒単位でリストされます。

8 .5 .3 ログ蓄積量の最大件数の変更

通知項目のログは、1 通知項目あたり既定値で 15000 件まで保存できますが、最大件数を変更したい場合には、下記の ini ファイルの一部を書き換えることで可能です。なお、設定は最初に通知項目のログが作成される場合に有効になります。ログが既にある場合に最大件数を変更するには、‘9 .5 各種ログのクリア’の手順で通知項目のログを消去して、下記の ini ファイルの設定を変更してから、BOM ヘルパーサービス（BOM7Helper）サービスを再起動してください。

●ini ファイルの設定変更箇所

フォルダー　：　<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Config¥

ファイル名　：　MxHelper.ini

変更箇所　：　[Option]

MaxNtfLog = <XXXXX>

<XXXXX>の数字を変更することで、保存できる件数を変更できます。

8.6 ローカル監視と代理監視のアクション機能の違い

ローカル監視では BOM マネージャーの通知項目はローカルコンピューターに対して実行されますが、

代理監視の通知項目の場合には、下記の表に示すように、実行するコンピューターが異なります。

アクション名	監視元のコンピューター	代理監視先のコンピューター
メール送信	監視元コンピューターから、 指定した SMTP サーバーに送信	-
SNMP トラップ送信	監視元コンピューターから、 指定した SNMP マネージャーに送信	-
イベントログ書き込み	代理監視先コンピューターで検知した内容を 監視元コンピューターのイベントログに書込み	-
syslog 送信	監視元コンピューターから、 指定した syslog サーバーに送信	
カスタム通知	監視元コンピューターから、 代理監視先コンピューターに対して実行	カスタム通知の設定内容や 監視実行プログラムの内容に依存

8.7 通知項目の詳細

8.7.1 通知項目の種類

BOM 7.0 で使用できる通知項目は、下記の 5 種類です。

アイコン	通知項目名	説明
通知アクション系：4 種類		
	メール送信	SMTP 形式のメール通知
	SNMP トラップ送信	SNMP 形式のトラップ送信による通知
	イベントログ書き込み	Windows イベントログへの書き込みによる通知
	syslog 送信	syslog サーバーへの syslog 送信による通知
その他のアクション系：1 種類		
	カスタム通知	外部アプリケーションを利用した制御/通知

8.7.2 メール送信と SNMP トラップ送信に必要な環境設定

BOM 7.0 で使用できる通知項目のうち、メール送信と SNMP トラップ送信は、

“BOM for Windows Ver.7.0（ローカル）”の“プロパティ”画面より、事前に下記の設定を行う必要があります。

●メール送信の場合

メールを送信するために必要な SMTP サーバーの情報

詳細は‘2.3.3 SMTP 情報の設定’を参照ください。

●SNMP トラップ送信の場合

BOM 7.0 より送信した SNMP トラップを受信させる SNMP マネージャー情報

詳細は‘2 .3 .4 SNMP 情報の設定’を参照ください。

8 .7 .3 通知項目の概要

通知項目は、作成しただけでは意図したアクションが行えません。通知項目は、作成した後に設定を行います。

通知項目の設定は、下記のいずれかの手段で“プロパティ”画面を表示させ行います。

●“通知”をクリックし、設定を行いたい通知項目を右クリックし、コンテキストメニューの“プロパティ”をクリック

●“通知”をクリックし、設定を行いたいリザルトペインの通知項目をクリックし、画面下部の“プロパティ”をクリック

●“通知”をクリックし、設定を行いたいリザルトペインの通知項目をダブルクリック

A. 基本操作

1. タブ

“プロパティ”画面は、「全般」、「実行条件」、「設定」などのタブで構成されています。

それぞれのタブをクリックすることで、該当するタブが表示され、設定を変更できます。

2. 変更した設定の反映とは破棄

変更した設定は、[OK]ボタン、または[適用]ボタンをクリックすることで BOM 7.0 に反映することができます。

変更した設定を破棄したい場合には[キャンセル]ボタンをクリックします。

B.「全般」タブ

「全般」タブは、“アイコン”、“ID”、“名前”に設定されている値を除き、すべての通知項目で共通です。

「全般」タブに登場する監視項目の基本概念に関する詳細は、‘8 .4 通知項目を有効にする’も参照ください。

1. [アイコン]ボタン

   [アイコン]ボタンは項目で設定されているアイコンが表示されています。

   既定では、通知項目の種類に合わせたアイコンが設定されています。

   [アイコン]ボタンをクリックすることで、アイコンを変更するためのダイアログを表示することができます。

   アイコンを変更する場合には、ダイアログにて変更したいアイコンをクリックし、[OK]ボタンをクリックします。

2. “有効”

   “有効”チェックボックスにチェックを入れることで、アクションを実行します。

   既定では“有効”チェックボックスにチェックが入っています。

   アクションを行いたくない場合には、“有効”チェックボックスのチェックを外してください。

3. “名前”フィールド

   “名前”フィールドには、“通知項目名”を入力します。既定値として通知項目の種類と同じ名称が入力されています。

   必要に応じて、分かりやすい名称に変更してください。この名前は、BOM マネージャーに表示される名前です。

4. “ID”フィールド

   “ID”フィールドには、通知項目 ID が表示されます。

   監視グループ番号と監視項目番号と通知項目番号が含まれています。

   通知項目 ID は、インスタンス内で通知項目ごとに一意になるように、BOM 7.0 が自動的に設定します。

5. “コメント”フィールド

   “コメント”フィールドには、通知項目の補足情報を入力します。既定では空白です。必要に応じて入力してください。

6. “1 回のみ実行”

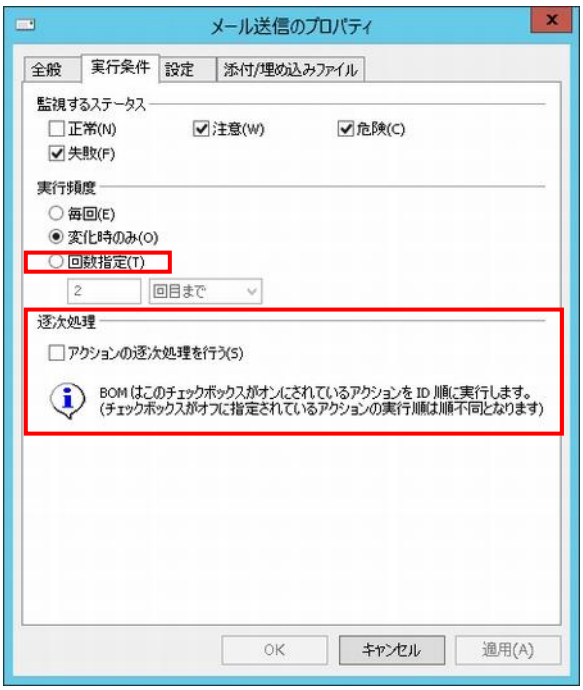
   “1 回のみ実行”チェックボックスにチェックが入っている場合、通知項目が実行された時に上記 2.の“有効”チェックボックスのチェックを自動で外します。

   そのため、再び手動で“有効”チェックボックスにチェックを入れるまで、その通知項目は起動しません。

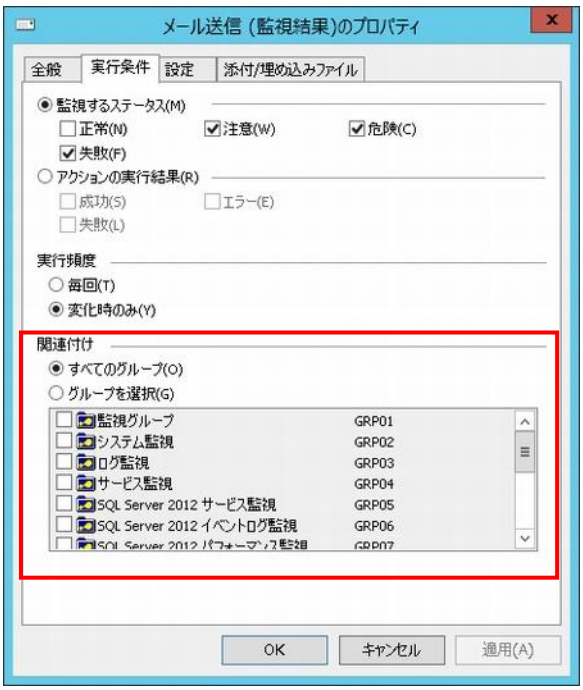
C.「実行条件」タブ

通知項目を実行するための条件を設定することができ、“監視ステータス”、“実行頻度”の既定値を除き、すべての通知項目で共通です。

●アクション項目のプロパティ画面



●通知項目のプロパティ画面



上記はどちらもメール送信アクションの「実行条件」タブですが、左側が“アクション項目”、右側が“通知項目”のアクションです。

“アクション項目”と“通知項目”は、“実行頻度”、“逐次処理”、“関連付け”の 3 項目で設定できる内容が異なります。

●「全般」タブで“1 回のみ実行”チェックボックスにチェックを入れた場合には、1 度アクションが実行されると通知項目が無効状態になるため、“実行頻度”フィールドの設定がどのような値であっても実行されません。

1. 監視するステータス

   監視項目の監視結果（ステータス）を、アクションの起動条件として指定することができます。

   指定できるステータスは、“正常”、“注意”、“危険”、“失敗”の 4 つがあり、各ステータスのチェックボックスにチェックを入れて起動条件を満たした際に、アクションを実行することができます。

2. アクションの実行結果

   アクション項目の実行結果（ステータス）を、アクションの起動条件として指定することができます。

   指定できるステータスは、“成功”、“エラー”、“失敗”の 3 つがあり、各ステータスのチェックボックスにチェックを入れて起動条件を満たした際に、アクションを実行することができます。

3. 実行頻度

   上記 1.もしくは 2.で選択にした、同一のステータスが連続して発生した際のアクションの動作条件を指定することができます。

   ●“毎回”ラジオボタンを選択した場合

   アクションが起動するステータス条件を満たしていた際に、アクションを毎回実行します。

●“変化時のみ”ラジオボタンを選択した場合

アクションが起動するステータス条件を満たしていたとしても、前回のステータスと同一であった時には

アクションは実行しません。

4. 関連付け

手順 1.、2.、3.で設定した通知項目の起動条件を、どの“監視グループ”に対して適用するかを下記より選択します。

●“すべてのグループ”ラジオボタンを選択した場合

すべての“監視グループ”に属する“監視項目”もしくは“アクション項目”のステータスをアクションの起動対象とします。

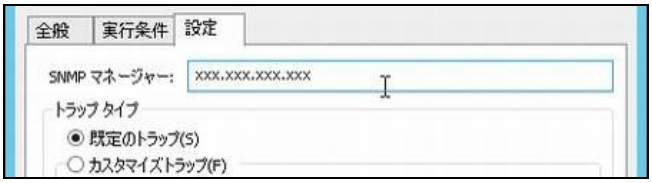
●“グループを選択”ラジオボタンを選択した場合

“グループ選択”フィールドに表示された“監視グループ”の各チェックボックスにチェックを入れることで、

該当する“監視グループ”に属する“監視項目”もしくは“アクション項目”のステータスを、アクションの起動条件とします。

D.「設定」タブ

「設定」タブは、通知項目のコントロール対象とコントロール方法を設定します。設定方法は通知項目の種類によって異なります。



8 .7 .4 メール送信アクション(通知項目)

メール送信アクションは、“通知項目”で指定した“監視グループ”に属する“監視項目”のステータスもしくは“アクション項目”の実行結果と、それらの実行頻度といった起動条件を満たした場合に、指定したメールアドレスにメールを送信します。

●事前に、BOM マネージャーのスコープペインの“BOM for Windows Ver.7.0 (ローカル)”の“プロパティ”画面の「SMTP」タブで“SMTP サーバー”設定値を設定する必要があります。詳細は‘2 .3 .3 SMTP 情報の設定’を参照ください。

A.「全般」タブ

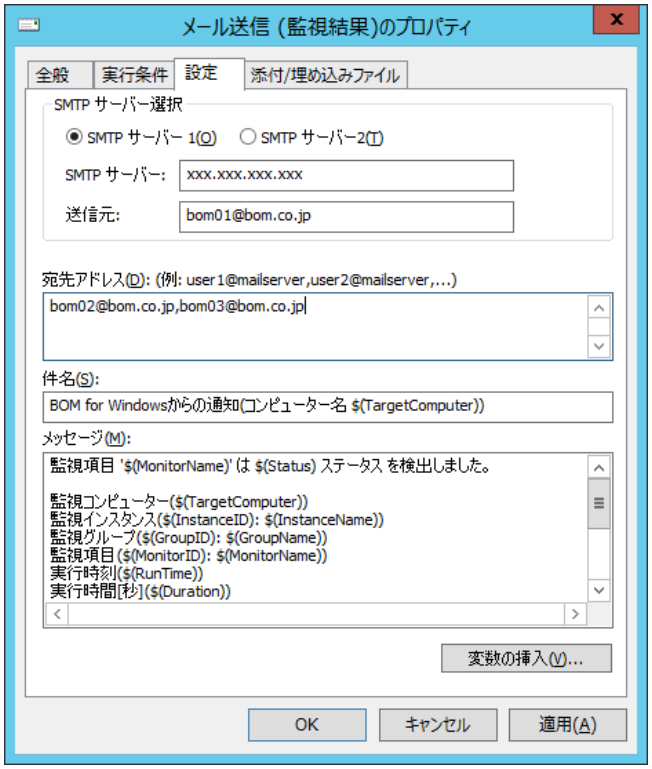
「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、全ての項目で共通です。「全般」タブの詳細は、‘8 .7 .3 通知項目の概要’の項目‘A「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべての通知項目で共通です。

「実行条件」タブの詳細は、‘8 .7 .3 通知項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ



1. “SMTP サーバー選択”フィールドで、“SMTP サーバー1”ラジオボタンまたは“SMTP サーバー2”ラジオボタンのいずれかを選択します。

   ●上記を選択後、“SMTP サーバー”フィールドと“送信元”フィールドに情報が何も表示されない場合、“SMTP サーバー”に関する情報を設定する必要があります。詳細は‘2 .3 .3 SMTP 情報の設定’を参照ください。

2. “宛先アドレス”フィールドに、メッセージの宛先となる電子メールアカウントを入力します。

   ●複数のアドレスを指定する際には、カンマで区切って入力します。

   ●宛先アドレスの最大文字数は 1000 文字です。

3. “件名”フィールドに、メールの件名を入力します。

   ●既定値で設定されている件名の変数は、[変数の挿入]ボタンをクリックすることで変数リストを表示させて確認ができます。

4. “メッセージ”フィールドに、メールの本文を入力します。

   ●“メッセージ”の最大文字数は 2500 文字です。

   ●[変数の挿入]ボタンより 2500 文字を超える入力をした場合、“メッセージ”フィールドに反映されるのは 2500 文字です。

   ●変数に関しては展開後の文字数で換算されますが、展開後 2500 文字を超えた場合でも問題なくアクションは実行します。

   ●メール送信のメッセージは RFC2822 より、メール本文の 1 行あたりの文字数が決まっており、BOM 7.0 では、1 行における文字列が 991 バイト以上になった時点で強制改行します。

D.「添付/埋め込みファイル」タブ

●[変数の挿入]ボタンより変数名を指定することで、テキストログ監視やイベントログ監視でエクスポートしたテキストファイルをメールに添付することができます。

1. “ファイルを添付あるいは埋め込む”チェックボックスにチェックを入れることで、メール送信アクションにファイルを添付する、または添付ファイルの中身をメール本文に埋め込むことができます。

   ●ファイルを埋め込みたい場合には、埋め込むファイルはテキストファイルである必要があります。

2. “ファイル名”フィールドに、下記のいずれかの手段で添付したいファイルの“ファイル名”を設定します。

   手順 3.の[追加]ボタンをクリックするまで、選択したファイルは添付ファイルの対象にはなっておりませんのでご注意ください。

   ●添付したいファイルの絶対パスを入力する。

   ●[...]ボタンをクリックし、“ファイル選択”画面より添付ファイルを選択する。

   ●[変数の挿入]ボタンをクリックし、テキストログ監視やイベントログ監視でエクスポートしたテキストファイルを選択したい場合
   “変数の挿入”画面で“検出テキストのエクスポートファイル名を指定”チェックボックスにチェックを入れた後、[挿入]ボタンをクリックすることで、<$(DetectedDataDir)¥$(MonitorID).txt>という文字が設定され、テキストログ監視やイベントログ監視でエクスポートしたテキストファイルを指定することができます。

   ●[変数の挿入]ボタンをクリックし、独自のファイル名形式で変数を使用しているようなファイルを選択したい場合
   “変数の挿入”画面で“検出テキストのエクスポートファイル名を指定”チェックボックスのチェックを外した後、変数リストの対象変数をクリックして[挿入]ボタンをクリックするか、直接変数をダブルクリックすることで、“変数の挿入”フィールドに、変数を含んだ“ファイル名”を設定します。

3. [追加]ボタンをクリックすると、手順 2.で指定したファイルを、添付ファイルの対象として下部の“ファイル”フィールドに表示します。

4. ファイルをメール本文に埋め込みたい場合、手順 3.の“ファイル”フィールドの“ファイル名”の横にあるチェックボックスにチェックを入れます。

   ●JIS、Shift JIS 以外のテキストファイルの埋め込みはできません。

5. “ファイルを Zip 形式で圧縮（ファイルを添付する場合にのみ有効）”チェックボックスにチェックを入れることで、手順 4.でメール本文の埋め込み対象にしなかった添付ファイル一式を圧縮することができます。

   ●手順 4.で、埋め込み対象に指定したファイルは圧縮の対象にはなりません。

   ●圧縮した添付ファイルに対して、パスワードによる暗号化を行う場合には、“パスワードによる暗号化”チェックボックスにチェックを入れて、“パスワード”と“パスワードの確認入力”を入力します。

8 .7 .5 SNMP トラップ送信アクション（通知項目）

SNMP トラップ送信アクションは、“通知項目”で指定した“監視グループ”に属する“監視項目”のステータスもしくは“アクション項目”の実行結果と、それらの実行頻度といった起動条件を満たした場合に、指定した SNMP マネージャーに SNMP トラップを送信します。

●事前に、BOM マネージャーのスコープペインの“BOM for Windows Ver.7.0 （ローカル）”の“プロパティ”画面の「SNMP」タブで“SNMP マネージャー”設定値を設定する必要があります。詳細は‘2 .3 .4 SNMP 情報の設定’を参照ください。

●代理監視の場合には、代理監視元コンピューターではなく、代理監視はコンピューターの IP アドレスが SNMP マネージャーに通知されます。SNMP マネージャー側の設定を行う際には、代理監視先コンピューターの IP アドレスも登録してください。

A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、

全ての項目で共通です。「全般」タブの詳細は、‘8 .7 .3 通知項目の概要’の項目‘「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべての通知項目で共通です。

「実行条件」タブの詳細は、‘8 .7 .3 通知項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ

1. “SNMP マネージャー”フィールドに、情報が何も表示されない場合、“SNMP マネージャー”に関する情報を設定する必要があります。詳細は‘2 .3 .4 SNMP 情報の設定’を参照ください。
2. “トラップ タイプ”フィールドは、下記のどちらかを設定します。
   ●“既定のトラップ”ラジオボタンを選択した場合
   メッセージは BOM 7.0 の既定のトラップ内容と共にトラップ送信されます。
   ●“カスタマイズトラップ”ラジオボタンを選択した場合
   “メッセージ”フィールドに指定した内容でトラップ送信されます。
3. “メッセージ”フィールドは、手順 2.で“カスタマイズトラップ”ラジオボタンを選択した際に、トラップ送信される内容です。
   ●“メッセージ”の最大文字数は 255 文字です。制限数を超える場合、エラーとなり SNMP トラップが実行されません。
   ●変数の展開後の文字数が 255 文字を超える場合、エラーとなり SNMP トラップが実行されません。
4. [変数の挿入]ボタンをクリックすると、手順 2.の“メッセージ”フィールドに挿入可能な、BOM 7.0 の予約済み変数をリストから選択することができる“変数の挿入”画面を表示させることができます。
   ●[変数の挿入]ボタンより、“グループ名”、“監視名”、“アクション名”に格納される最大文字数は 63 文字です。
   制限数を超えているとエラーになり、SNMP トラップが実行されません。
   ●予約済み変数については ‘第 15 章 予約済み変数’ を参照してください。

D. SNMP トラップの送信内容

SNMP トラップの送信内容は、各“OID”に設定されています。“OID”の詳細は下記の表を参照ください。

●既定のトラップ内容かつ、「実行条件」タブの“監視するステータス”ラジオボタンを選択している場合

送信コンピューター名（TargetComputer）、インスタンス ID（InstanceID）、グループ名（GroupName）、
監視項目名（MonitorName）、監視取得値（Value）、監視結果（ResultCode）で、各内容に“OID”が対応しております。

●既定のトラップ内容かつ、「実行条件」タブの“アクションの実行結果”ラジオボタンを選択している場合

送信コンピューター名（TargetComputer）、インスタンス ID（InstanceID）、グループ名（GroupName）、
監視項目名（MonitorName）、監視取得値（Value）、監視ステータス（Status）、アクション名（ActionName）、
アクション実行結果（ExitCode）、監視結果（ResultCode）、です

●カスタマイズトラップ時の送信内容

カスタマイズトラップメッセージ（$（UserMsg））

OID	オブジェクト名	通知内容
監視アイテム（オブジェクト）		
1.3.6.1.4.1.10035.2.10.1.1.1	mxTargetComputer	コンピューター名
1.3.6.1.4.1.10035.2.10.1.1.3	mxInstanceID	インスタンス ID
1.3.6.1.4.1.10035.2.10.1.1.6	mxGroupName	監視グループ名
1.3.6.1.4.1.10035.2.10.1.1.8	mxMonitorName	監視項目名
1.3.6.1.4.1.10035.2.10.1.1.10	mxActionName	アクション名
1.3.6.1.4.1.10035.2.10.1.1.13	mxResultCode	監視結果コード
1.3.6.1.4.1.10035.2.10.1.1.14	mxMonitorValue	監視取得値
1.3.6.1.4.1.10035.2.10.1.1.15	mxMonitorStatus	監視ステータス
1.3.6.1.4.1.10035.2.10.1.1.16	mxExitCode	終了コード
1.3.6.1.4.1.10035.2.10.1.1.25	mxUserMsg	ユーザーメッセージ
監視ステータス（トラップ）		
1.3.6.1.4.1.10035.2.10.1.2.0.20	mxMonitorFailure	監視失敗
1.3.6.1.4.1.10035.2.10.1.2.0.21	mxStatusNormal	監視正常
1.3.6.1.4.1.10035.2.10.1.2.0.22	mxStatusWarning	監視注意
1.3.6.1.4.1.10035.2.10.1.2.0.23	mxStatusCritical	監視危険
アクションステータス（トラップ）		
1.3.6.1.4.1.10035.2.10.1.2.0.30	mxActionFailure	アクション失敗
1.3.6.1.4.1.10035.2.10.1.2.0.31	mxActionSuccess	アクション成功
1.3.6.1.4.1.10035.2.10.1.2.0.32	mxActionError	アクションエラー
その他（トラップ）		
1.3.6.1.4.1.10035.2.10.1.2.0.41	mxUserMessage	ユーザー定義

8 .7 .6 イベントログ書き込みアクション（通知項目）

イベントログ書き込みアクションは、“通知項目”で指定した“監視グループ”に属する“監視項目”のステータスもしくは“アクション項目”の実行結果と、それらの実行頻度といった起動条件を満たした場合に、指定した事項をイベントログに書き込みます。

●イベントログに書き込む内容はあらかじめ既定値が決まっており、「設定」タブの“既定のメッセージ”フィールドの内容は必ず書き込まれます。

A.「全般」タブ

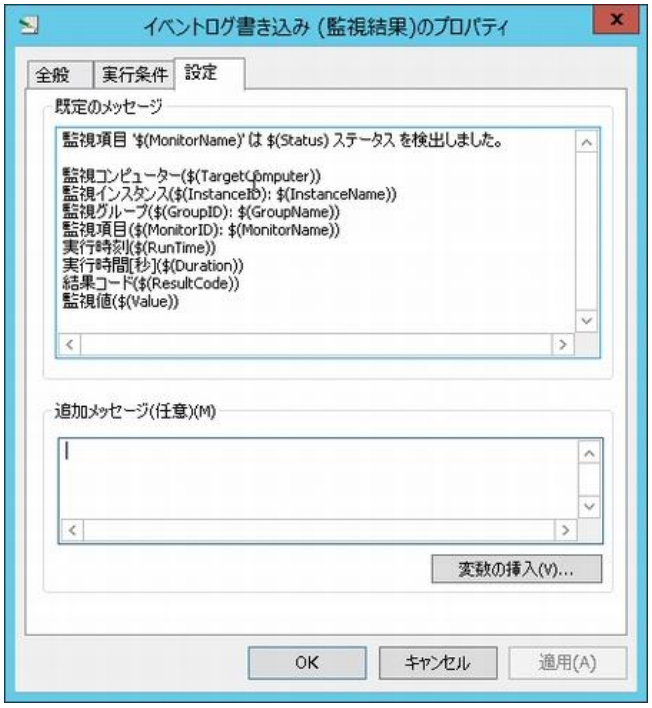
「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、全ての項目で共通です。「全般」タブの詳細は、‘8 .7 .3 通知項目の概要’の項目‘B.「全般」タブ「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべての通知項目で共通です。

「実行条件」タブの詳細は、‘8 .7 .3 通知項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ



1. “既定のメッセージ”フィールドの内容は必ずイベントログに書き込まれます。

   ●“既定のメッセージ”中の“$”で始まる記号は変数になっています。

   [変数の挿入]ボタンをクリックして変数の内容を確認することができます。

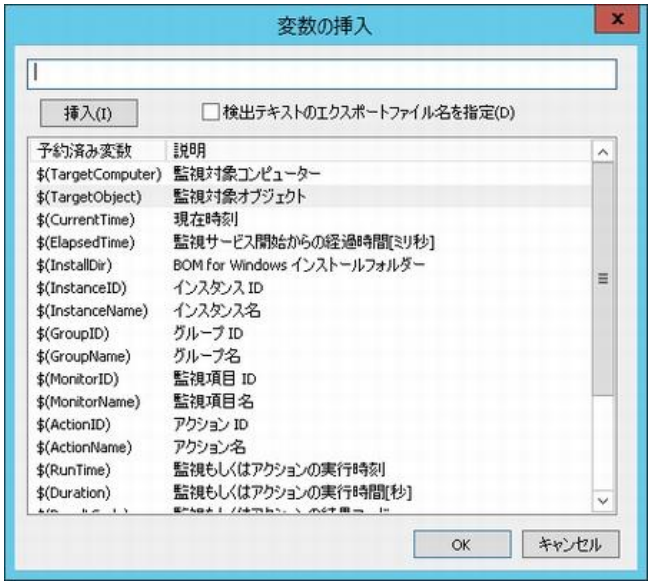
2. “追加メッセージ(任意)”フィールドに入力した内容は、既定値以降に付け加えてイベントログに書き込むことができます。

●[変数の挿入]ボタンをクリックして、変数を使用することもできます。

●追加メッセージの最大文字数は 2000 文字です。

●[変数の挿入]ボタンより 2000 文字を超える入力をした場合、“メッセージ”フィールドに反映されるのは 2000 文字です。

●変数に関しては展開後の文字数で換算されますが、展開後 2000 文字を超えた場合でも問題なくアクションは実行します。



D. イベントログの出力内容

イベントログ書き込みアクションで、実際にイベントログに書き込まれる内容は下記の通りです。

●イベントログの種別

“アプリケーション”

●ソース

“Bom7Action”

●分類

“なし”

●イベントの種類

監視ステータスによって、イベントの種類が変わります。ステータス、イベントの種類、イベント ID の相関は下記の通りです。

イベント ID	監視ステータス	イベントログ出力	
		種類	説明
3300	正常	情報	説明本文は全て共通で既定のメッセージが書き込まれます。 追加メッセージが設定されていれば既定メッセージに追記されます。
3301	注意	警告	
3302	危険	エラー	
3303	失敗	エラー	

8 .7 .7 カスタム通知（通知項目）

カスタム通知は、“通知項目”で指定した“監視グループ”に属する“監視項目”のステータスもしくは“アクション項目”の実行結果と、それらの実行頻度といった起動条件を満たした場合に、サードパーティ製のコマンドラインベースのプログラムや、独自に記述したテキストベースのスクリプトプログラム（バッチファイルや WSH、PowerShell など）を実行させることができます。

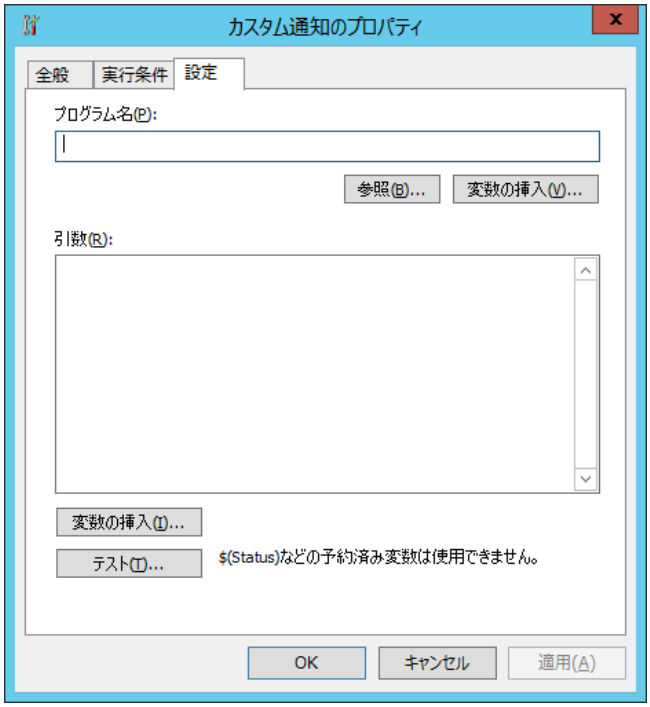
A.「全般」タブ

「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、全ての項目で共通です。「全般」タブの詳細は、‘8 .7 .3 通知項目の概要’の項目‘B.「全般」タブ「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべての通知項目で共通です。
「実行条件」タブの詳細は、‘8 .7 .3 通知項目の概要’の項目‘C.「実行条件」タブ’を参照ください。

C.「設定」タブ



1. “プログラム名”フィールドに、任意の“実行プログラム名”を下記のどちらかの手段で設定します。

   ●“実行プログラム名”を、絶対パスで入力する。

   “プログラム名”フィールドの[変数の挿入]ボタンをクリックし、“プログラム名”のパスに BOM 7.0 の予約済み変数を使用することもできます。予約済み変数については ‘第 15 章 予約済み変数’ を参照してください。

   ●[参照..]ボタンをクリックして、“ファイル選択”画面より“実行プログラム”を選択する。

   “隠しファイルの表示”チェックボックスもしくは“保護されたシステムファイルの表示”チェックボックスにチェックを入れると、条件に応じた該当ファイルが表示されます。

2. “引数”フィールドには実行プログラムの引数を記述します。
   ●“引数”フィールドの[変数の挿入]ボタンをクリックし、“引数”に BOM 7.0 の予約済み変数を指定できますが、テスト実行時は使用できません。予約済み変数については‘第 15 章　予約済み変数’を参照してください。
3. [テスト]ボタンをクリックすると、“アクションのテスト”画面を表示させ、「設定」タブの設定を加えてテスト実行します。
   ●コンソールプログラムをカスタム通知として設定する場合には、BOM 監視サービスと BOM ヘルパーサービスのサービスアカウントをローカルシステムアカウントとし、デスクトップとの対話にチェックしてください。
   ●代理監視の場合にはコンソールプログラムは指定ができません。
   ●アクションの終了待ち時間は、既定値で 2 時間です。2 時間経過後、アクションのプロセスは強制終了されます。

8 .7 .8 syslog 送信アクション（通知項目）

syslog 送信アクションは、“通知項目”で指定した“監視グループ”に属する“監視項目”のステータスもしくは“アクション項目”の実行結果と、それらの実行頻度といった起動条件を満たした場合に、指定した事項を送信先ホストへ送信します。

※　syslog Protocol としては、RFC 3164（The BSD syslog Protocol）にのみ対応しています。

※　UDP を使用して送信するため、syslog サーバー側で取りこぼしが発生する可能性があります。

※　メッセージの送信文字コードは UTF-8 です。また、ASCII コード 33(0x21)～126(0x1E) + 32(0x20)　以外の文字のロギング（日本語などがロギングまたは表示されるかどうかなど）は受信先の syslog サーバーの仕様によります。

A.「全般」タブ

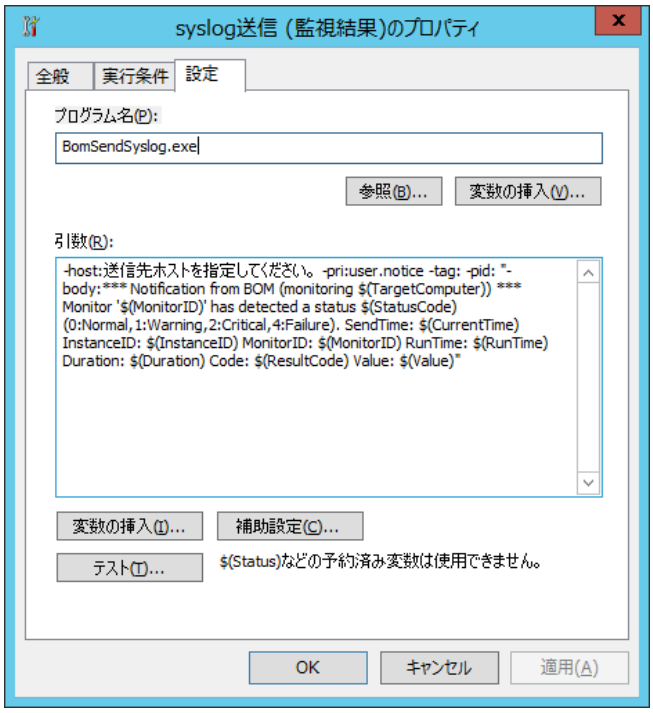
「全般」タブは、“ID”フィールド、“名前”フィールド、および“1 回のみ実行”に設定されている値を除き、全ての項目で共通です。「全般」タブの詳細は、‘8 .7 .3　通知項目の概要’の項目 ‘B.「全般」タブ「全般」タブ’を参照ください。

B.「実行条件」タブ

「実行条件」タブは、“監視ステータス”、“実行頻度”の既定値を除き、すべての通知項目で共通です。

「実行条件」タブの詳細は、‘8 .7 .3　通知項目の概要’の項目 ‘C.「実行条件」タブ’を参照ください。

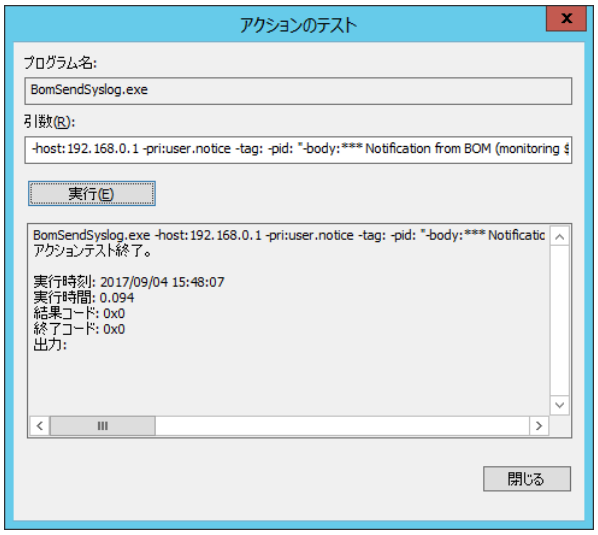
C.「設定」タブ



1. “プログラム名”フィールドにはあらかじめ“BomSenSyslog.exe”と入力されていますので、変更しないでください。
   また、“プログラム名”フィールドの[参照]ボタンおよび[変数の挿入]ボタンは使用しないでください。
2. “引数”フィールドは以下の内容で設定および入力してください。
   - 引数“-host:”について、“送信先ホストを指定してください。”部分を削除し、syslog を送信するホストの IP アドレス（IPv4、IPv6）またはコンピューター名で指定します。
   - 引数“-body:”から末尾の「”」（ダブルクォーテーション）の間に、送信する情報が設定できます。変数を使用する場合は、“引数”フィールドの[変数の挿入]ボタンから入力してください。
3. “引数”フィールドの[変数の挿入]ボタンをクリックすると、“引数”フィールドに使用できる予約済み変数の一覧を表示します。
   一覧から予約済み変数を選択し、[挿入]ボタン→[OK]ボタンをクリックすると、“引数”フィールドのカーソルの位置に選択した変数が挿入されます。
   - 予約済み変数については‘第 15 章 予約済み変数’を参照してください。
4. [補助設定]ボタンは使用できません。

5. [テスト]ボタンをクリックすると、“アクションのテスト”画面を表示し、「設定」タブの設定を加えてテスト実行します。

● テスト実行時に BOM 7.0 の予約済み変数を使用することはできません。



第9章 ログ

9 .1 ログの解説

BOM 7.0 では、これまでの章で下記のログを解説しました。

●“監視項目”のログ

詳細は、‘5 .8 監視項目のログ’を参照ください。

●“アクション項目”のログ

詳細は、‘7 .5 アクション項目のログ’を参照ください。

●“通知項目”のログ

詳細は、‘8 .5 通知項目のログ’を参照ください。

本章では、BOM 7.0 マネージャーの“ログ”ノード配下のログについて解説します。

9 .2 収集されたイベントログ

イベントログ監視で監視設定した内容に該当するイベントログは“収集されたイベントログ”ノードに蓄積されます。

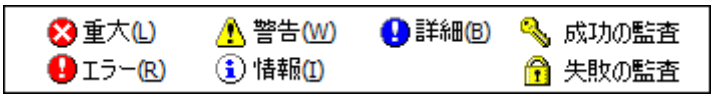
9 .2 .1 収集されたイベントログの表示

BOM マネージャーで、“ログ”ノード→“収集されたイベントログ”以下は、収集したデータが存在する場合に各ノード(“Application”、“セキュリティ”、“システム”等以下、ログノード)が表示されます。

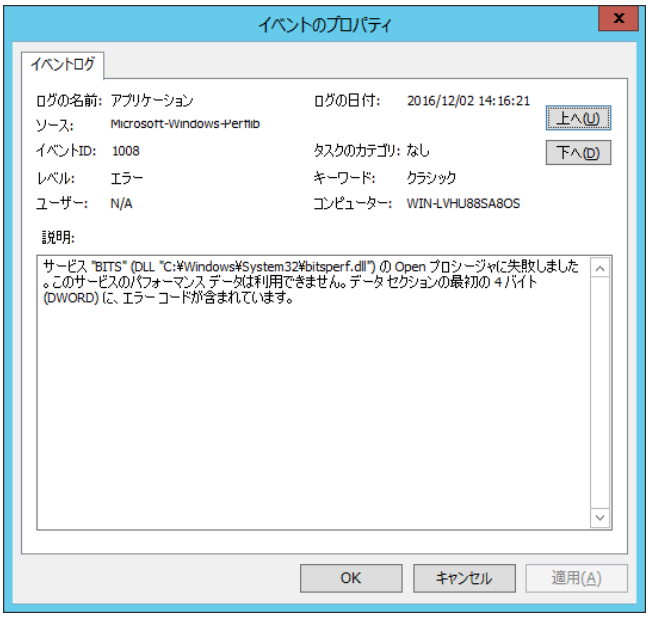
各ログノードをクリックするとリザルトペインに、“収集されたイベントログ”がリスト表示されます。

A. 収集されたイベントログの表示(アイコン部分)

●ステータスアイコン/表示



B. 各イベントログのプロパティ表示



C. イベントログのフィルタリング

収集されたイベントログは、フィルタリングして表示することができます。

1. “ログ”ノード→“収集されたイベントログ”ノード→“アプリケーション”（イベントログの種別）を右クリックし、
   コンテキストメニューの“プロパティ”をクリックします。
   表示する“イベントのレベル”にチェックを入れ、“ソース名”、“分類”、“タスクのカテゴリ”、“キーワード”を選択します。
2. “イベント ID”、“ユーザー名”、“コンピューター名”を入力します。
3. “開始日時”と“終了日時”を指定して、イベントログに記述されたイベントログ時刻で、イベントログが絞り込めます。

9 .2 .2 収集されたイベントログのローテーション

収集されたイベントログは、100000 件まで各収集されたイベントログに保存されるよう設定されています。
100000 件を超えると古いログから上書きされていきますので、ご注意ください。

●“収集されたイベントログ”ノードをクリックした場合、リザルトペインに表示される件数は、
最大で最新の 1000 件分です。

●すべてのログを表示したい場合には“収集されたイベントログ”ノードを右クリックし、コンテキストメニューの
“すべてのレコードを表示”をクリックしてください。

9 .2 .3 収集されたイベントログ蓄積量の最大件数の変更

収集されたイベントログは、既定値で 100000 件までのログを保存できますが、最大件数を変更したい場合には、
下記の ini ファイルの一部を書き換えることで可能です。なお、設定は最初にイベントログ監視の収集ログが作成される場合に有効になります。ログが既にある場合に最大件数を変更するには、‘9 .5 各種ログのクリア’の手順でイベントログ監視の収集ログを消去して、下記の ini ファイルの設定を変更してから、BOM ヘルパーサービス（BOM7Helper サービス）を再起動してください。

●ini ファイルの設定変更箇所

フォルダー　：　<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Config¥

ファイル名　：　BomEvtlogMon.ini

変更箇所　：　[LOG_ROTATION_SETTINGS]

DEFAULT= <XXXXX>　（項目がない、マイナスの場合は、100000 が適用）

BOM_LOG_System= <XXXXX>　（項目がない、マイナスの場合は、上記 DEFAULT の設定値が適用）

BOM_LOG_Application= <XXXXX>（項目がない、マイナスの場合は、上記 DEFAULT の設定値が適用）

上記の System および Application とは、イベントログファイル名あるいは、チャネル名を表しています。

上記の<XXXXX>の数字を変更することで、保存できる件数を変更できます。

9 .3 ヒストリー

“ヒストリー”ノード以下には、“監視”、“アクション”、“サービス”の 3 つの主要なヒストリーログがあり、これらは各機能のログを示しています。

●“監視”

すべての“監視項目”のログが蓄積されます。

●“アクション”

すべての“アクション項目”のログが蓄積されます。

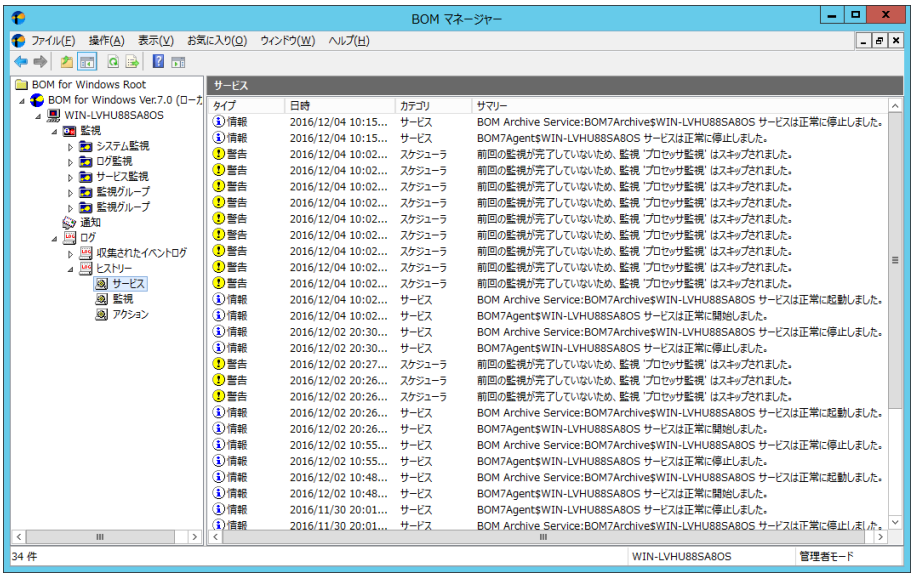
●“サービス”

BOM 7.0 の“サービスのステータス”のログが蓄積されます。

9 .3 .1 ヒストリーログの表示

BOM マネージャーのスコープペインの“ヒストリー”をクリックすると、リザルトペインに 3 種類のヒストリーログが表示されます。

蓄積された各種“ヒストリーログ”の、より詳細な解説を表示するには該当する行をダブルクリックします。



A. 監視ヒストリーログ

監視項目 ID と共にスキップされたと記述されることがあります。

これは前回の監視項目の実行時間が長く、次の監視実行時刻に監視が行われなかった場合に書き込まれるログです。

●“正常”ステータスに変化した場合

アイコンは Information（緑）

●“注意”ステータス、“危険”ステータスに変化した場合

アイコンは Warning（黄）

●監視失敗の場合

アイコンは Error（赤）

B. アクションヒストリーログ

●アクションが成功した場合

アイコンは Information（緑）

●アクションに失敗した場合

アイコンは Error（赤）

C. サービスヒストリーログ

●サービス起動に成功した場合

アイコンは Information（緑）

●サービス起動に失敗した場合

アイコンは Error（赤）

9 .3 .2 ヒストリーログ蓄積量の最大件数の変更

ヒストリーログは、既定値で10000 件までのログを保存できますが、最大件数を変更したい場合には、下記の ini ファイルの一部を書き換えることで可能です。なお、設定は最初にヒストリーログが作成される場合に有効になります。

ログが既にある場合に最大件数を変更するには、‘9 .5 各種ログのクリア’の手順でヒストリーログを消去して、

下記の ini ファイルの設定を変更してから、BOM ヘルパーサービス（BOM7Helper サービス）を再起動してください。

●ini ファイルの設定変更箇所

フォルダー　：　<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Config¥

ファイル名　：　MxHelper.ini

変更箇所　：　[Option]

MaxHistory = <XXXXX>

上記のパラメーターを追記し、<XXXXX>の数字を変更し、保存件数を変更します。

●最大件数は“ヒストリー”配下の各ノードのログ数の合計件数です。

各ノードのログの数がトータル 10000 件を超えると古いログから上書きされていきますので、ご注意ください。

●アーカイブ設定をしている場合には、アーカイブされる前にデータが上書きされないよう、上記パラメーターでの最大件数と監視間隔を調整してください。

各ノードのログの数がトータル 10000 件を超えると古いログから上書きされていきますので、ご注意ください。

9 .4 各種ヒストリーログのエクスポート

1. “収集されたイベントログ”あるいは“ヒストリー”等のリザルトペインに見えているデータをエクスポートするには、
   “収集されたイベントログ”あるいは“ヒストリー”ノード配下の各ノードを右クリックし、コンテキストメニューの
   “一覧のエクスポート…”をクリックします。

2. “一覧のエクスポート…”画面で、“保存する場所”フィールドのドロップダウンメニューを使用してファイルの保存先とするフォルダーを選択します。
3. “ファイル名”フィールドに、ヒストリーテキストファイルの名前を指定します。
4. 終了したら[保存]ボタンをクリックします。

   例:

   ヒストリーのサービス

タイプ	日時	カテゴリ	サマリー
情報	2018/10/26 11:45:41	サービス	BOM7Agent$<インスタンス名> サービスは正常に停止しました。
情報	2018/10/26 0:00:25	サービス	BOM7Agent$<インスタンス名> サービスは正常に動作中です。
情報	2018/10/25 18:32:22	サービス	BOM7Agent$<インスタンス名> サービスは正常に開始しました。
情報	2018/10/21 11:08:37	サービス	BOM7Agent$<インスタンス名> サービスは正常に停止しました。

9.5 各種ログのクリア

9.5.1 ログの種類

ログの種類と削除対象は下記の通りです。

A. 監視グループを選択した場合

監視グループ内の監視項目、アクション項目のログをすべて消去します。

B. 監視項目を選択した場合

監視項目、アクション項目のログを全てクリアします。

C. アクション項目を選択した場合

アクション項目のログを全てクリアします。

D. 通知項目を選択した場合

通知項目のログを全てクリアします。

E. ログノードを選択した場合

ログノード配下のイベントログで収集されたログ、ヒストリーのログを全てクリアします。

F. イベントログで収集されたログノードを選択した場合

イベントログで収集されたログを全てクリアします。

G. ヒストリーノードを選択した場合

ヒストリー（サービス・監視・アクション・通知）ログを全てクリアします。

9.5.2 ログの削除手順

各ログを削除する手順は、右クリックで選択する箇所が異なるだけで、基本的な手順は共通です。

1. 監視項目、またはグループやアクション項目のログをクリアするには、削除したい該当“監視グループ”、“監視項目”、“アクション項目”、“通知項目”、“ログ”ノード、“イベントログで収集されたログ”ノード、あるいは“ヒストリー”ノードを右クリックします。
2. コンテキストメニューの“ログのクリア”をクリックします。

●クリアしたログは復旧させることができません。

このため、ログのクリアを実行するかどうかを確認するダイアログボックスが表示されます。

第10章 BOM コントロールパネル

10 .1 BOM コントロールパネルの解説

BOM コントロールパネルは、下記の通り各コンポーネントの制御をするものです。

A. 監視サービス関連

●BOM 7.0 の各種サービスの制御

BOM ヘルパーサービス、BOM 監視サービスに対する、“開始”、“停止”ができます。

B. アーカイブサービス関連

●アーカイブサービスの制御

アーカイブサービスに対する、“開始”、“停止”、“登録”、“解除”ができます。

C. ツール関連

●設定とログのバックアップ

ローカルコンピューターに登録されているインスタンスの監視設定および監視ログを

CAB ファイル、ZIP ファイルに出力することができます。

●設定とログのリストア

リストア処理では、ローカルコンピューター、あるいはリモートコンピューターのバックアップ処理で出力された

CAB ファイルまたは ZIP ファイル、および設定配布ツールで収集された監視設定の CAB ファイルを

ローカルコンピューターにリストアすることができます。

●各種 BOM 7.0 製品の起動

BOM マネージャー、BOM 集中監視コンソール、BOM アーカイブマネージャーを起動することができます。

D. 設定ユーティリティ関連

●BOM 7.0 の各種設定の収集/配布

BOM 7.0 設定一括配布ツール、BOM 7.0 設定収集配布ツールを起動することができます。

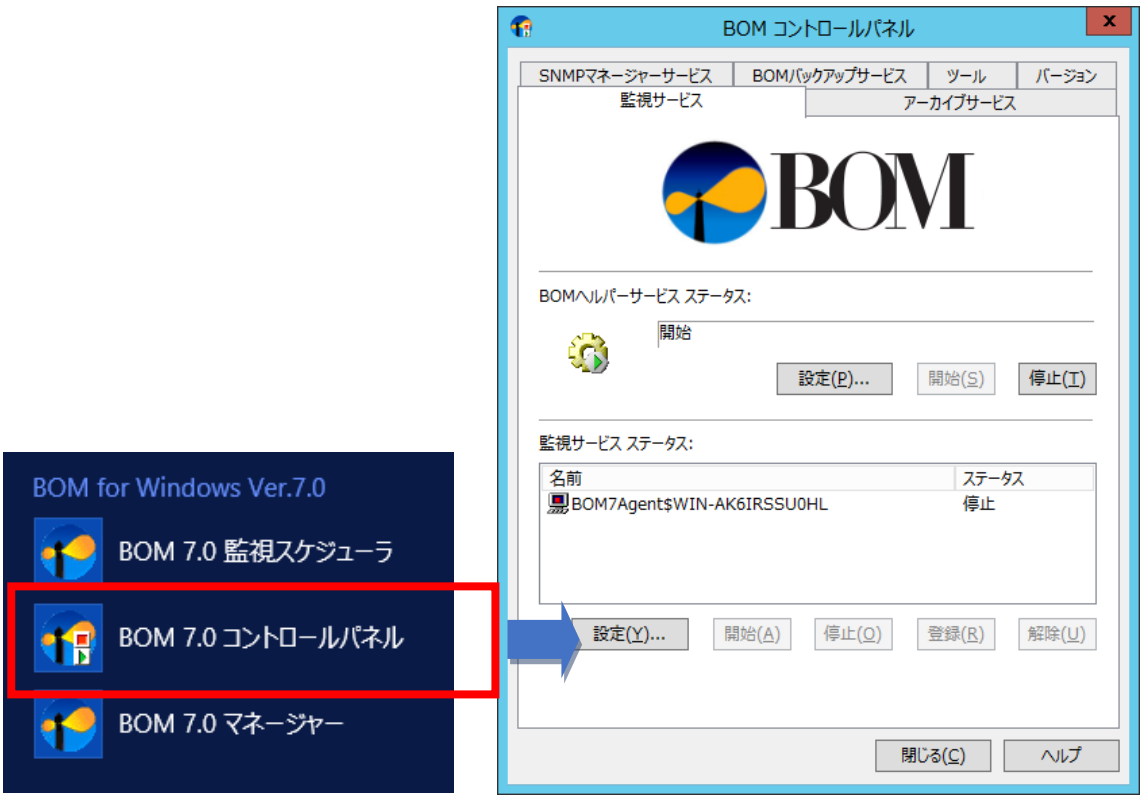
E. バージョン関連

●BOM 7.0 のバージョン

インストールした BOM 7.0 のバージョン確認、インストールしたファイルごとのバージョンを確認することができます。

10 .2 BOM コントロールパネルの起動

BOM コントロールパネルを起動するには、OS のスタート画面で右クリックし、“すべてのアプリ”を選択したのちに表示される“BOM 7.0 コントロールパネル”をクリックします。



●BOM コントロールパネルの起動には、管理者権限が必要です。

10 .3 「監視サービス」タブ

ローカルコンピューターに登録されている、“BOM ヘルパーサービス”と“BOM 監視サービス”の“設定”、“開始”、“停止”処理を行うことができます。

●“BOM ヘルパーサービス”または“BOM 監視サービス”の“設定”を行う際には、BOM マネージャーを終了する必要があります。

10 .3 .1 BOM ヘルパーサービス ステータス

“BOM ヘルパーサービス ステータス”フィールドでは、“BOM ヘルパーサービス”の“設定”、“開始”、“停止”処理を行うことができます。

●ステータス アイコンの表示： 開始  停止 

1. [開始]ボタンをクリックすると、BOM ヘルパーサービスを“開始”します。
2. [停止]ボタンをクリックすると、BOM ヘルパーサービスを“停止”します。
3. [設定]ボタンをクリックすると、“ヘルパーサービス設定”画面を表示します。
   詳細は‘10 .3 .2 BOM ヘルパーサービス設定’を参照ください。

10 .3 .2 BOM ヘルパーサービス設定

“リモートアクセスの範囲”の既定値は、“監視対象サーバーコンピューターと同じローカルセグメント（サブネット）”です。

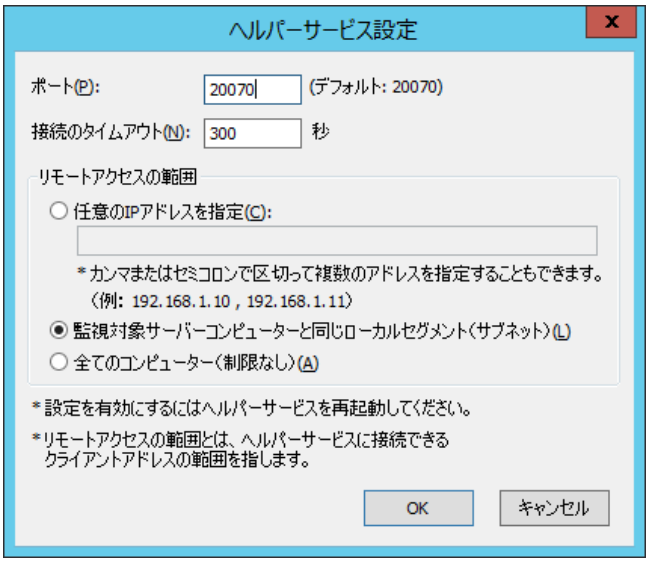
具体的に下記の機能に影響が出ますので、異なるセグメント間のコンピューターを監視/管理したいような場合には、
運用に合わせて適切な値を設定してください。

●リモート接続時の監視元コンピューターの監視サービスとリモート接続先の BOM ヘルパーサービスの通信

リモート接続の詳細は、‘3 .2 .3 リモート接続’を参照ください。

●BOM 集中監視コンソールの集中監視 Web サービスと BOM ヘルパーサービスの通信

BOM 集中監視コンソールの集中監視 Web サービスの詳細は、‘集中監視コンソール ユーザーズマニュアル’を参照ください。



1. “ポート”フィールドは、BOM ヘルパーサービスが使用するポート番号を、“1”～“65535”の範囲で設定します。

   ●変更したポート番号を有効にするには BOM ヘルパーサービスを、‘10 .3 .1 BOM ヘルパーサービス ステータス’を参考に再起動する必要があります。

   ●BOM マネージャーに登録されているローカルコンピューター上の各インスタンスの BOM ヘルパーサービスのポート番号、および集中監視コンソールに登録されているインスタンスの BOM ヘルパーサービスのポート番号は、BOM ヘルパーサービスのポート番号と同じ番号に設定する必要があります。

   ●BOM 7.0 インストール時に、BOM ヘルパーサービスを Windows ファイアウォールの例外に追加することができます。

2. “接続のタイムアウト”は、BOM ヘルパーサービスへの無操作最大接続時間を、“0”～“86400”の範囲（秒単位）で設定します。

   ●BOM マネージャーが管理者モードで接続してから、無操作状態で管理者モードを維持できる時間を設定します。詳細は、‘2 .2 .1 アカウントとパスワード’を参照ください。

   ●設定の配布時は管理者モードに接続して実行しますが、“接続のタイムアウト”はその際にも適用されます。

3. “リモートアクセスの範囲”は、ローカルコンピューター上の BOM ヘルパーサービスに接続できる範囲を設定します。
   なお、設定した“リモートアクセスの範囲”以外よりリモート接続しようとすると、“アクセス制限のため BOM7Helper 接続が拒否されました”というエラーが出力されます。

   ●“任意のIPアドレス”ラジオボタンを選択した場合

   指定した IP アドレスからの接続のみを許可します。

   カンマで区切って複数の IP アドレスを指定でき、指定できる最大文字数は 1000 文字です。

   ●“監視対象サーバーコンピューターと同じローカルセグメント（サブネット）”ラジオボタンを選択した場合

監視対象コンピューターとローカルセグメント上のコンピューターから接続のみを許可します。

●“全てのコンピューター（制限なし）”ラジオボタンを選択した場合

全てのコンピューターからの接続を許可します。

10 .3 .3 BOM 監視サービス ステータス

“監視サービス ステータス”フィールドでは、BOM 監視サービスの一覧が表示され、

BOM 監視サービスの“設定”、“開始”、“停止”、サービスコントロールへの“登録”、“解除”といった制御を行うことができます。

A. BOM 監視サービスの一覧

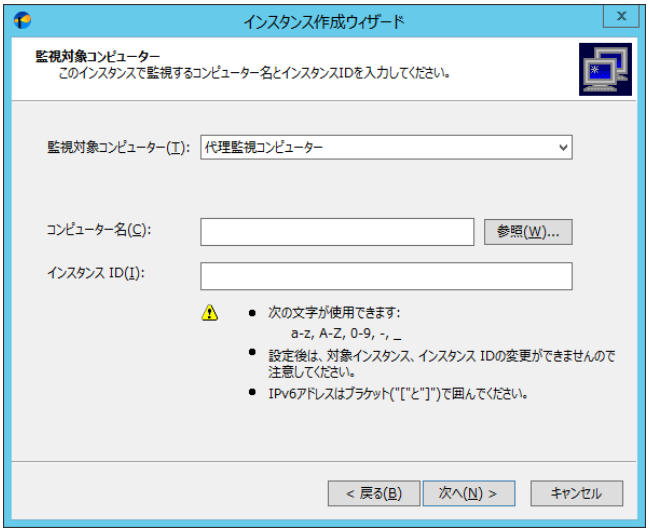
ローカルコンピューターに登録されているすべての BOM 監視サービスのステータスを表示します。

BOM マネージャーで作成したインスタンスごとに 1 つの監視サービスが作成されます。

●“名前”は BOM 監視サービスの名前を、“ステータス”は“開始”、“停止”、“未登録”のいずれかを表示します。

●BOM 監視サービスの名前は、BOM7Agent$InstanceID の規則に準じて名前が付けられています。

（InstanceID（インスタンス ID）は、下記インスタンスの作成時に任意の名称に設定することができます。）



B. BOM 監視サービスの制御

1. [開始]ボタンをクリックすると、BOM 監視サービスを“開始”します。

   BOM 監視サービスを“開始”するには、有効な基本製品ライセンスが必要となります。

2. [停止]ボタンをクリックすると、BOM 監視サービスを停止します。

3. [登録]ボタンをクリックすると、BOM 監視サービスがサービスコントロール（Windows のサービスマネージャー）に登録されます。

●該当の BOM 監視サービスが Windows サービスマネージャーに登録されていないと BOM 監視サービスは使用できません。

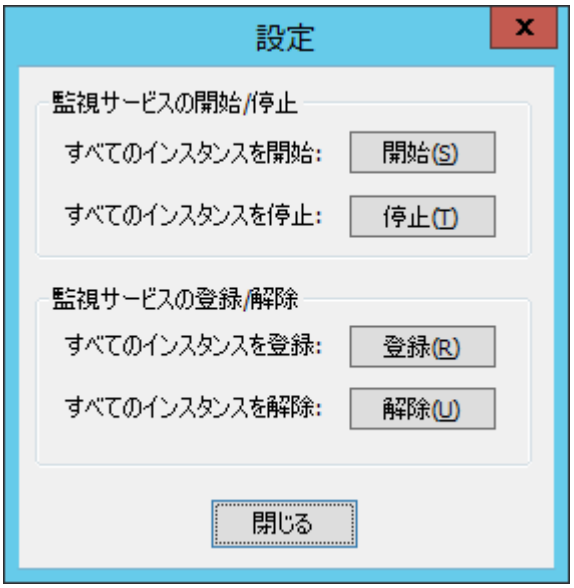
4. [解除]ボタンをクリックすると、BOM 監視サービスがサービスコントロール（Windows のサービスマネージャー）から解除されます。
5. [設定]ボタンをクリックすると、‘10 .3 .4 BOM 監視サービスの設定’の BOM 監視サービスの設定画面が表示されます。

●BOM マネージャーの管理者モードで接続している場合、[設定]ボタンをクリックしてもエラー画面が表示されます。

10 .3 .4 BOM 監視サービスの設定

監視サービス設定では、一度に全インスタンスを“開始”、“停止”、“登録”、“解除”制御したい場合に使用します。

個別のインスタンスの監視サービスを制御するには、‘10 .3 .3 BOM 監視サービス ステータス’を参照ください。



1. [開始]ボタンをクリックすると、すべてのインスタンスの BOM 監視サービスを開始します。
   インスタンスを監視するにはインスタンスごとに有効な基本製品ライセンスが必要となります。
2. [停止]ボタンをクリックすると、すべてのインスタンスの BOM 監視サービスを停止します。
3. [登録]ボタンをクリックすると、すべてのインスタンスの BOM 監視サービスを Windows のサービスマネージャーに登録します。

●該当の BOM 監視サービスが Windows サービスマネージャーに登録されていないと BOM 監視サービスは使用できません。

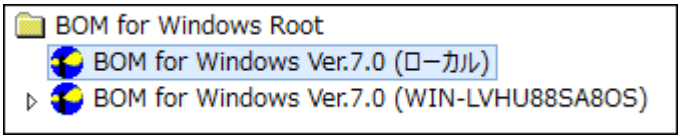
4. [解除]ボタンをクリックすると、すべてのインスタンスの BOM 監視サービスを Windows のサービスマネージャーから削除します。

●主にすべての監視機能を削除したい場合に、“解除”を使用します。

10 .3 .5 リモートコンピューターの BOM ヘルパーサービス、監視サービスの制御

BOM マネージャー画面で、“BOM for Windows Root”の以下、“BOM for Windows Ver.7.0 （ローカル）”に属さない

リモート接続したリモートコンピューター上のインスタンスの“開始”、“停止処理”は、インスタンスごとに操作する必要があります。



●リモート接続したリモートコンピューター上の BOM 7.0 コントロールパネルを起動するには、Windows のリモート接続機能で

リモートコンピューターに接続するか、該当するコンピューターで直接操作する必要があります。

●リモート接続したリモートコンピューター上の BOM ヘルパーサービスを制御するには、該当するコンピューター上の BOM コントロールパネルから操作するか、Windows の管理ツールの“サービス”画面の“サービス(ローカル)”ノードを右クリックして、“別のコンピューターへ接続”で操作する必要があります。

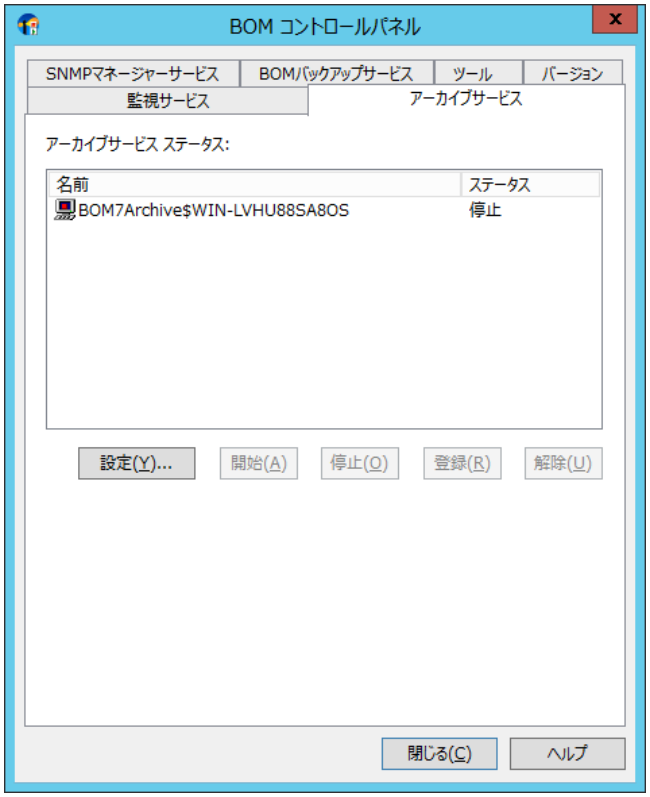
10 .4 「アーカイブサービス」タブ

ローカルコンピューター上の監視サービス(インスタンス)ごとに出力されたログを、アーカイブデータベースに保存するアーカイブサービスの“登録”、“削除”、サービスコントロールへの“登録”、“解除”処理を行うことができます

●インスタンスごとのアーカイブの詳細設定は、BOM マネージャーで行います。

アーカイブサービスタブの詳細は‘3 .6 .3 「アーカイブ設定」タブ’をご参照ください。

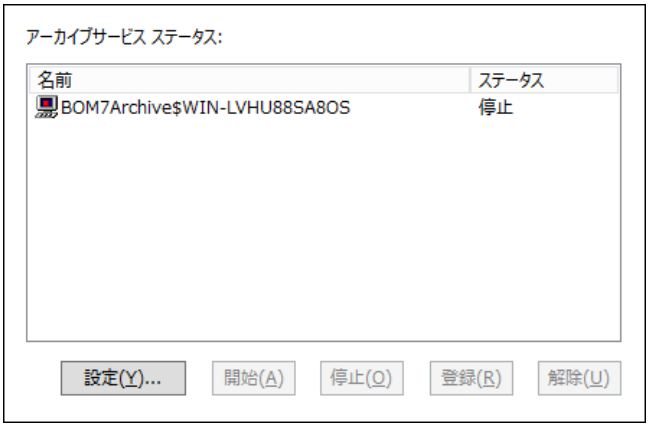
また、アーカイブの詳細については ‘アーカイブ ユーザーズマニュアル’ をご参照ください



10 .4 .1 アーカイブサービスステータス

“アーカイブサービス ステータス”フィールドでは、BOM アーカイブサービスの一覧が表示され、

アーカイブサービスの“設定”、“開始”、“停止”、サービスコントロールへの“登録”、“解除”といった制御を行うことができます。



A. アーカイブサービスの一覧

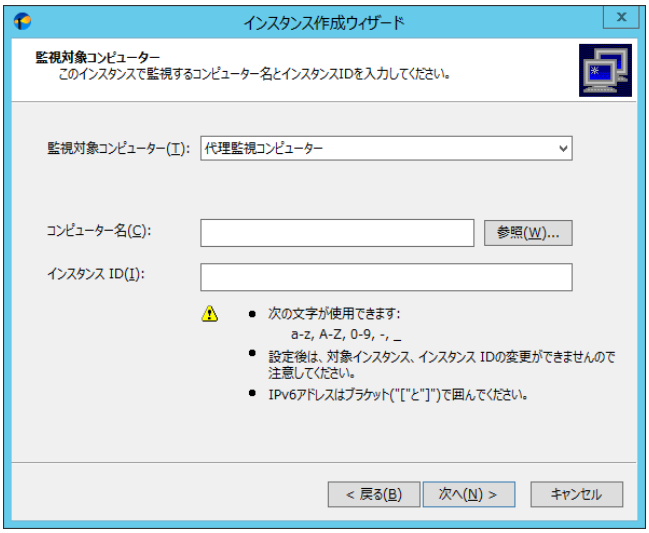
ローカルコンピューターに登録されているすべてのアーカイブサービスのステータスを表示します。

アーカイブサービスはインスタンスごと作成されます。

●“名前”は、BOM アーカイブサービスの名前を表示します。

●BOM アーカイブサービスの名前は、BOM7Archive$InstanceID の規則に準じて名前が付けられています。

（InstanceID（インスタンス ID）は、インスタンスの作成時に任意の名称に設定することができます。）



●“ステータス”は、“開始”、“停止”、“未登録”のいずれかを表示します。

B. アーカイブサービスの制御

1. [開始]ボタンをクリックすると、アーカイブサービスを“開始”します。
2. [停止]ボタンをクリックすると、アーカイブサービスを“停止”します。
3. [登録]ボタンをクリックすると、アーカイブサービスをサービスコントロール（Windows のサービスマネージャー）に“登録”します。

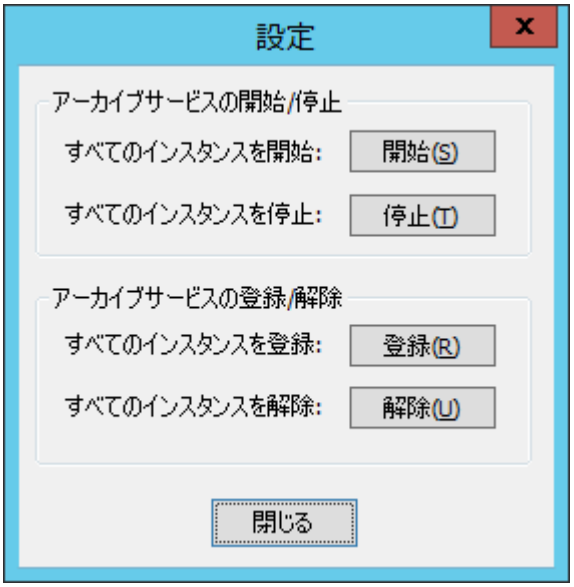
   ●該当のアーカイブサービスが Windows サービスマネージャーに登録されていないとアーカイブサービスは使用できません。
4. [解除]ボタンをクリックすると、アーカイブサービスをサービスコントロール（Windows のサービスマネージャー）から“削除”します。
5. [設定]ボタンをクリックすると、アーカイブサービスの設定画面が表示されます。

詳細は、‘10 .4 .2 アーカイブサービスの設定’を参照ください。

10 .4 .2 アーカイブサービスの設定

アーカイブサービス設定では、一度に全インスタンスのアーカイブサービスを“開始”、“停止”、“登録”、“解除”制御したい場合に使用します。

個別のインスタンスのアーカイブサービスを制御するには、‘10 .4 .1 アーカイブサービスステータス’を参照ください。



1. [開始]ボタンをクリックすると、すべてのインスタンスのアーカイブサービスを“開始”します。
2. [停止]ボタンをクリックすると、すべてのインスタンスのアーカイブサービスを“停止”します。
3. [登録]ボタンをクリックすると、すべてのインスタンスのアーカイブサービスを Windows のサービスマネージャーに“登録”します。
   ●該当の BOM 監視サービスが Windows サービスマネージャーに登録されていないと BOM 監視サービスは使用できません。
4. [解除]ボタンをクリックすると、すべてのインスタンスのアーカイブサービスを Windows のサービスマネージャーから削除します。
   ●主にすべてのアーカイブ機能を削除したい場合に、“解除”を使用します。

10 .5 「ツール」タブ

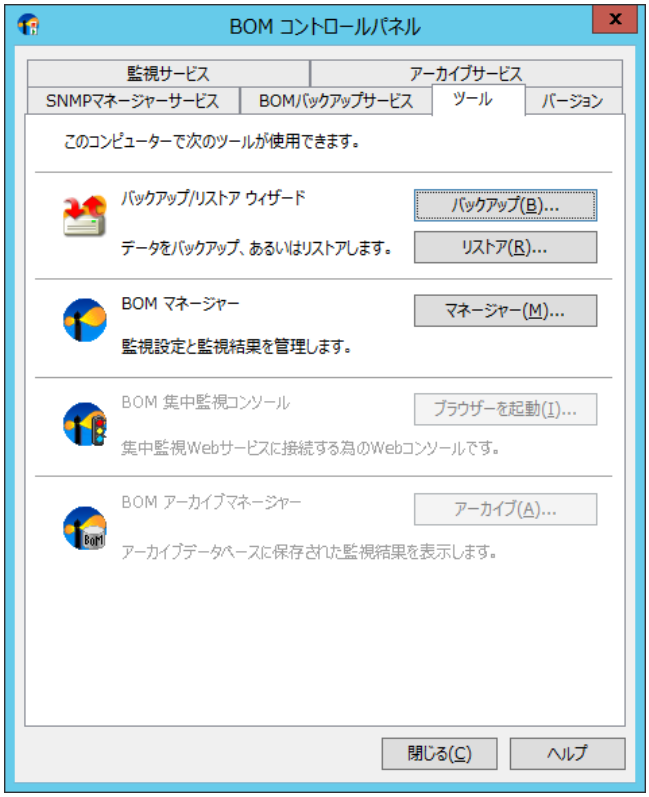
「ツール」タブから下記の機能を起動することができます。

- バックアップ/リストア ウィザード
- BOM マネージャー
- BOM 集中監視コンソール
- BOM アーカイブマネージャー

各機能の詳細について、BOM マネージャーは‘第 2 章 BOM マネージャー’、BOM 集中監視コンソールは‘集中監視コンソールユーザーズマニュアル’、BOM アーカイブマネージャーは‘アーカイブ ユーザーズマニュアル’を参照ください。

●以上の各対象コンポーネントがインストールされていない場合、各ボタンをクリックすることができません。

●以上のコンポーネントが既に起動済みの場合、各コンポーネントのウィンドウを最前面に表示させることができます。



●[バックアップ]ボタンをクリックすると、バックアップウィザードが起動します。

●[リストア]ボタンをクリックすると、リストアウィザードが起動します。

●[マネージャー]ボタンをクリックすると、BOM マネージャーが起動します。

●[ブラウザーを起動...]ボタンをクリックすると、既定で指定されているブラウザーの URL に
“https://localhost:8443/Indicator/view/”を指定した状態で、BOM 集中監視コンソールを起動します。
集中監視 Web サービスが起動していない場合、既定で指定されているブラウザーが起動しますが、“このページは表示できません”
というエラーが表示されます。

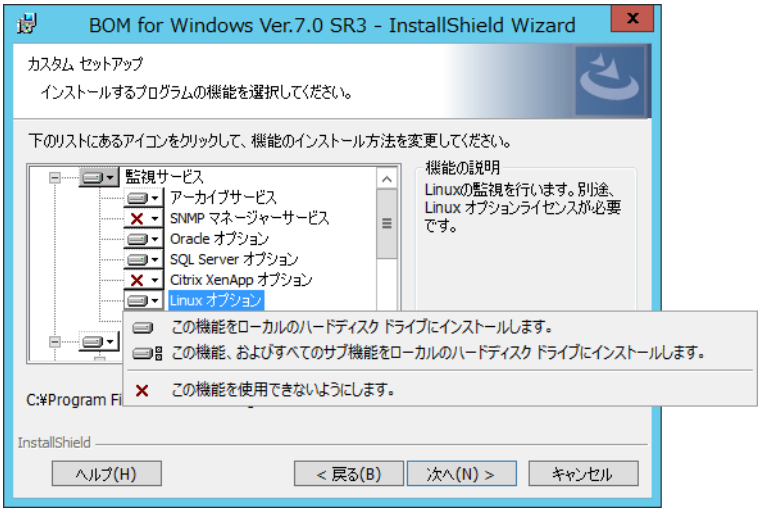
●[アーカイブ]ボタンをクリックすると、BOM アーカイブマネージャーが起動します。

10 .5 .1 バックアップ時とリストア前後の BOM 7.0 の構成について

バックアップデータをリストアするには、バックアップ時とリストア時の、BOM 7.0 の構成が同一、あるいはそれ以上の構成であることが条件です。

●構成情報は、BOM 7.0 媒体から“変更セットアップ”を選択することにより確認ができます。

コンポーネント名の頭に“×”がついていないコンポーネントは導入済みを表します。



●BOM 7.0 を“基本製品”の“標準”でインストールした場合の標準構成は、監視サービス、BOM ヘルパーサービス、BOM コントロールパネル、BOM マネージャー、BOM 監視テンプレートがインストールされます。

10 .5 .2 バックアップ処理

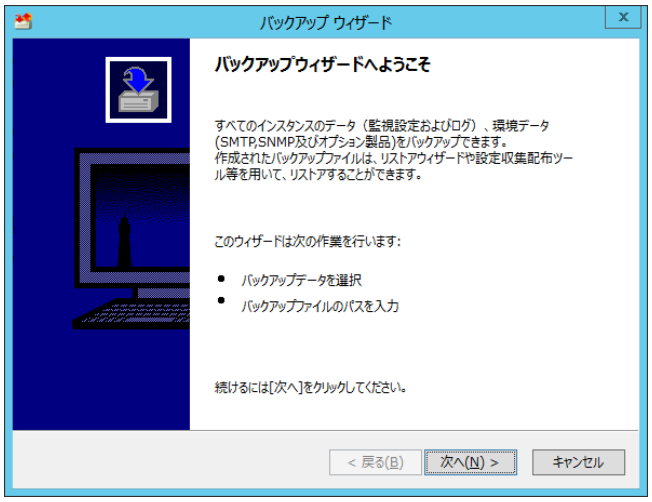
バックアップ処理は、ローカルコンピューター上に登録されている全てのインスタンスに関する“環境設定”、“監視設定”および“監視ログ”を CAB ファイル、ZIP ファイルに出力することができます。

●監視項目数が 200、監視項目ごとにアクション数が 99 を1つのインスタンスに登録した場合、設定のみをバックアップするには、約 100MB のハードディスクの空き容量が必要となります。

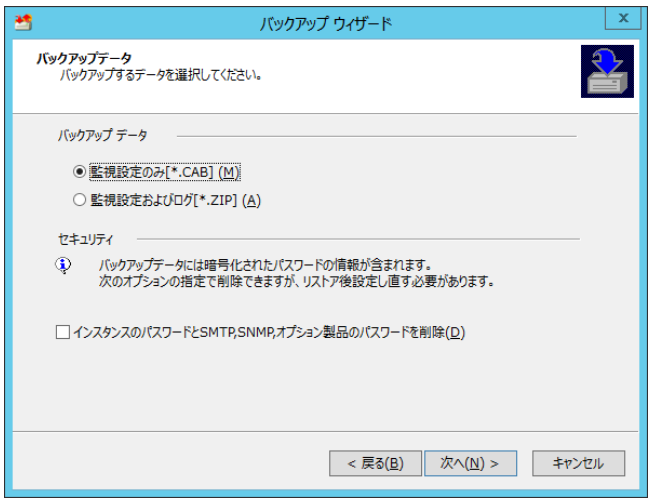
●監視設定及び監視ログ共にバックアップする場合は、<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Instance フォルダー配下のディスク使用量の約 2 倍のディスク空容量が必要となります。

●SNMP トラップ受信機能に関する設定(<BOM 7.0 インストールフォルダー>¥BOMW7¥Common¥snmp¥Config 配下のファイルおよび、BOM コントロールパネルの「SNMP マネージャーサービス」タブからおこなう設定)は、バックアップの対象となりません。

1. [バックアップ]ボタンをクリックすると、“バックアップ ウィザード”画面が表示されます。



2. [次へ]ボタンをクリックすると、“バックアップデータ”選択画面が表示されます。



3. “バックアップデータ”フィールドは、下記のどちらかを選択します。

●“監視設定のみ”ラジオボタンを選択した場合

監視ログを除いた、すべての設定が CAB ファイルに保存することができます。

バックアップファイル名は、BKNL-yyyyMMdd-hhmmss-コンピューター名.CAB です。

（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

●“監視設定及びログ”ラジオボタンを選択した場合

監視設定および監視ログをすべて ZIP ファイルに保存することができます。

バックアップファイル名は、BKLO-yyyyMMdd-hhmmss-コンピューター名.ZIP です。

（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

4. “セキュリティ”フィールドの“インスタンスのパスワードと SMTP、SNMP、オプション製品のパスワードを削除”チェックボックスにチェックを入れると BOM マネージャーより設定した下記該当箇所のパスワードをバックアップデータから除外することができます。

●インスタンスそれぞれのプロパティ画面

「全般」タブより設定するアカウントの“パスワード”および“パスワードの確認”

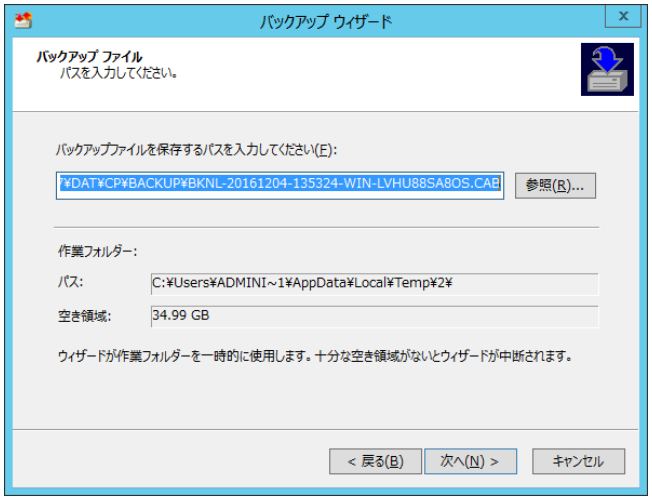
●BOM for Windows Ver.7.0（ローカル）のプロパティ画面

「SMTP」タブより設定する SMTP サーバーそれぞれの“パスワード”

「SNMP」タブより設定する“認証キー”と“暗号キー”

「Oracle 接続設定」および「SQL Server 接続設定」タブより設定する、接続設定リストそれぞれの“パスワード”

5. [次へ]ボタンをクリックすると、“バックアップファイル選択”画面が表示されます。

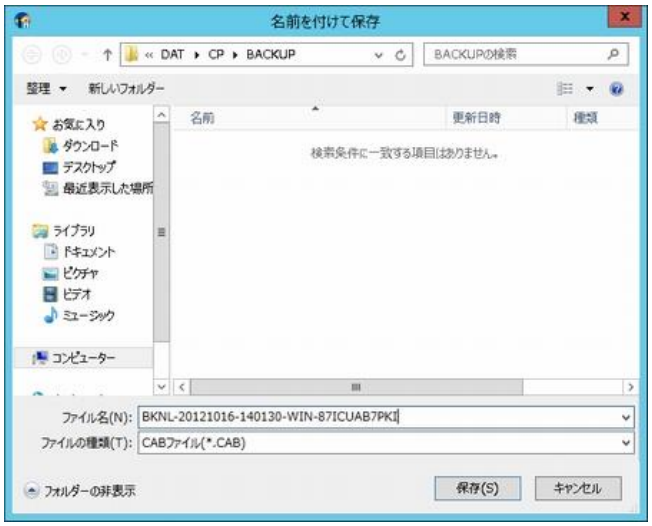


6. “バックアップファイルを保存するパスを入力してください”フィールドに、バックアップ先のフォルダーとファイル名を入力するか、[参照]ボタンをクリックして、“名前を付けて保存”画面より選択します。

●バックアップ出力先の既定値には下記のフォルダーが指定されています。

〈BOM 7.0 インストールフォルダー〉¥BOMW7¥DAT¥CP¥BACKUP

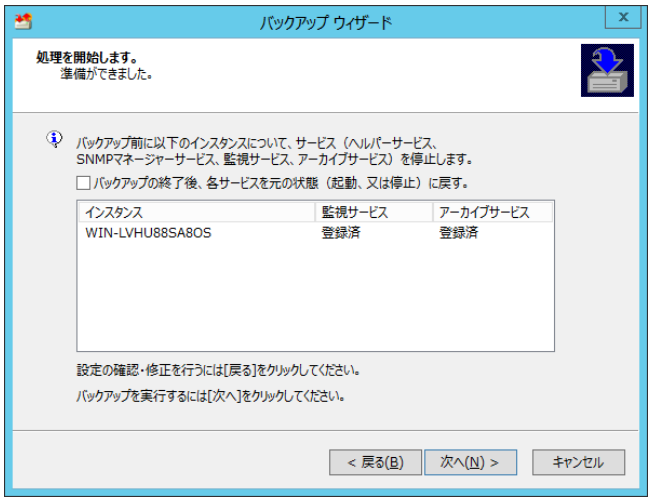
●バックアップファイル名の既定値は、手順 3.の通りです。



7. “バックアップファイル選択”画面で、[次へ]ボタンをクリックすると、“処理を開始します”確認画面が表示されます。

●インスタンスに監視サービス、アーカイブサービスが登録されているかが表示されます。

●BOM ヘルパーサービスはインスタンスが作成された時点で作成されていますので、画面上では表示されません。



8. バックアップの終了後、各サービスを元の状態に戻すかどうかを選択します。

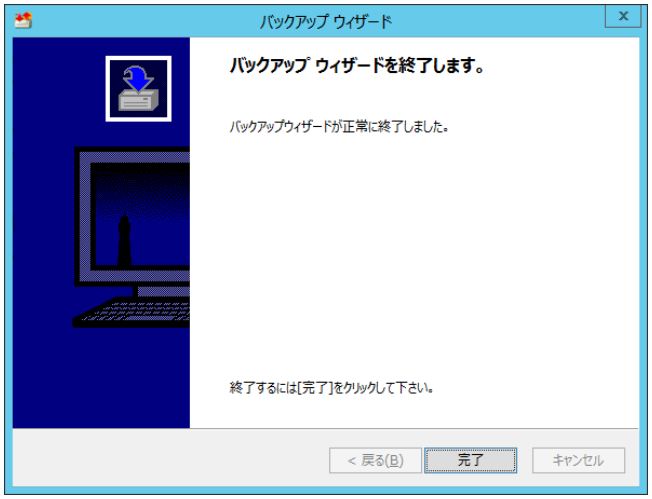
●“バックアップの終了後、各サービスを元の状態に戻す”チェックボックスにチェックを入れた場合

バックアップ時点で BOM 監視サービスなどが起動中であれば、バックアップ中に各サービスを一旦停止し、バックアップ終了後、再起動します。BOM ヘルパーサービスはバックアップ後、必ず起動されます。

●“バックアップの終了後、各サービスを元の状態に戻す”チェックボックスのチェックを外した場合

バックアップ時点で BOM 監視サービスなどが起動中であれば、バックアップ中に各サービスを一旦停止し、全サービスは停止したままになります。

9. [次へ]ボタンをクリックすると、バックアップ処理が開始され、バックアップ処理が完了すると“バックアップウィザード終了”画面が表示されるので、[完了]ボタンをクリックすると BOM コントロールパネルに戻ります。



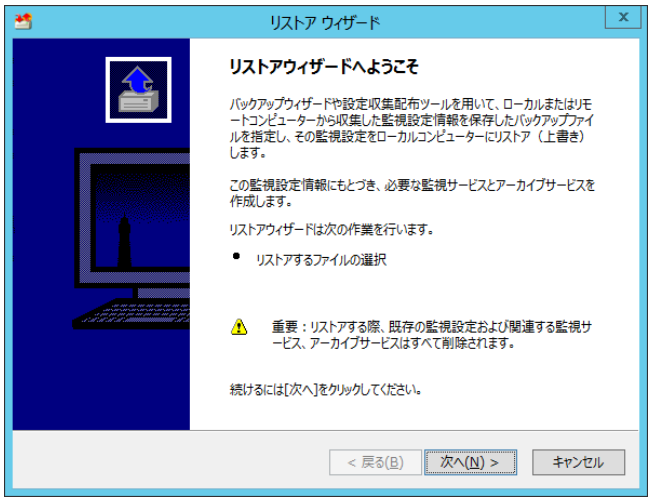
10 .5 .3 リストア処理

リストア処理は、ローカルコンピューターあるいはリモートコンピューターのバックアップ処理で出力された CAB ファイルまたは ZIP ファイル、および BOM 7.0 設定収集配布ツールで収集された監視設定の CAB ファイルをローカルコンピューターに復元することができます。

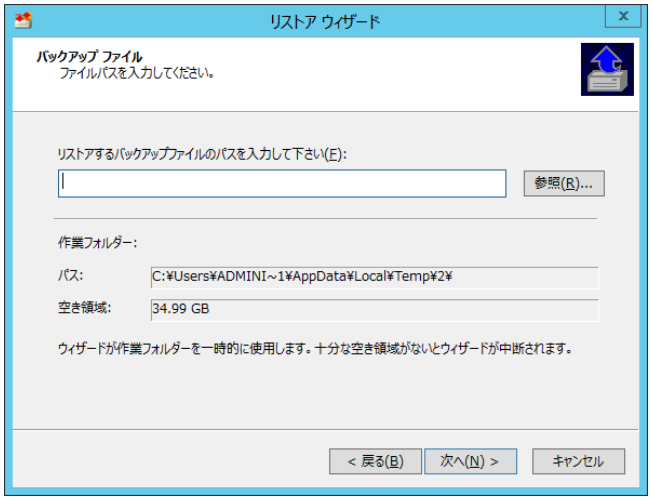
●リストアする際、既存の監視設定および関連する監視サービス、アーカイブサービスといった現在のデータがすべて削除され、リストアするデータで置き換えられます。

●リストア処理を実行する際、全てのサービスが停止されます。

1. [リストア]ボタンをクリックすると、“リストア ウィザード”画面が表示されます。



2. [次へ]ボタンをクリックすると、“バックアップ ファイル”選択画面が表示されます。



3. “リストアするバックアップファイルのパスを入力してください”フィールドに、バックアップファイルのフォルダーとファイル名を入力するか、[参照]ボタンをクリックして、“名前を付けて保存”画面より選択します。

   ●バックアップ処理で作成したバックアップファイルを選択する場合

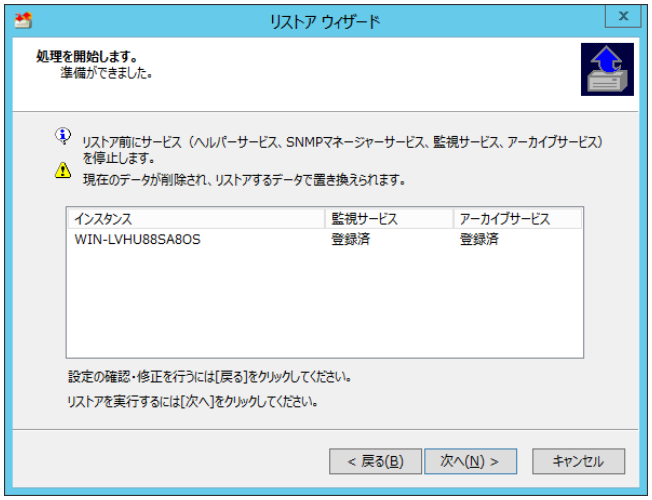
   [参照]ボタンをクリックするだけで、“<BOM 7.0 インストールフォルダー>¥BOMW7¥DAT¥CP¥BACKUP”フォルダーが表示されます。

   ●BOM 7.0 設定収集配布ツールで収集された CAB ファイルを選択する場合

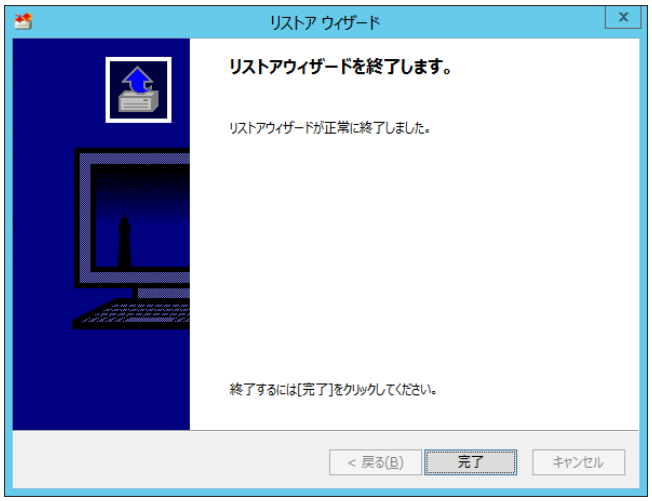
   “<BOM 7.0 インストールフォルダー>¥BOMW7¥DAT¥CP¥GATHER¥DEF”フォルダーまで移動してください。

4. “バックアップファイル選択”画面で、[次へ]ボタンをクリックすると、“処理を開始します”確認画面が表示されます。

   ●リストアによって削除されるインスタンスに監視サービス、アーカイブサービスが登録されているかが表示されます。



5. [次へ]ボタンをクリックすると、リストア処理が開始され、リストア処理が完了すると“リストアウィザード終了”画面が表示されるので、[完了]ボタンをクリックすると BOM コントロールパネルに戻ります。



10 .5 .4 パスワードが削除されたバックアップファイルをリストアした場合の注意事項

設定のバックアップ時に、“インスタンスのパスワードと SMTP、SNMP、オプション製品のパスワードを削除”チェックボックスにチェックを入れた場合、下記のパスワード情報がすべて削除されていますので必要に応じて BOM マネージャーより設定する必要があります。

●インスタンスそれぞれのプロパティ画面

「全般」タブより設定するアカウントの“パスワード”および“パスワードの確認”

詳細は、‘3 .6 インスタンスのプロパティ’を参照ください。

●BOM for Windows Ver.7.0 （ローカル）のプロパティ画面

「SMTP」タブより設定する SMTP サーバーそれぞれの“パスワード”

「SNMP」タブより設定する“認証キー”と“暗号キー”

「Oracle 接続設定」タブより設定する接続設定リストそれぞれの“パスワード”

詳細は、‘2 .3 BOM for Windows Ver.7.0 （ローカル）のプロパティ’を参照ください。

10 .5 .5 “設定収集配布ツール”で収集した設定ファイルをリストアした場合の注意事項

インスタンスは表示されますが、サービスコントロール（Windows のサービスマネージャー）にサービスとして登録されていないため、監視設定の変更ができません。また、ライセンスキーをインスタンスに設定しないと監視が開始できません。

●サービス登録

BOM コントロールパネルから、“BOM 監視サービス”と“アーカイブサービス”の“登録”設定を行います。

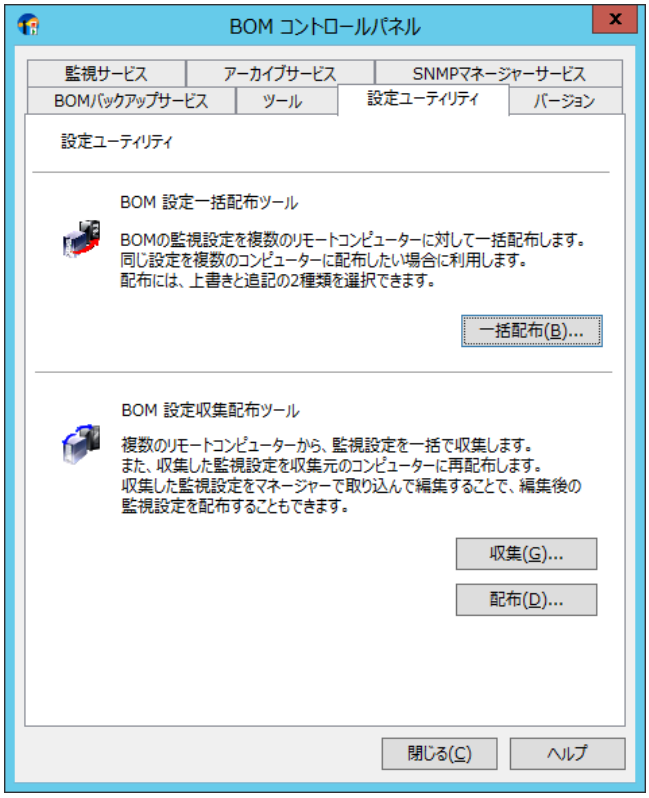
詳細は、‘10 .3 .3 BOM 監視サービス ステータス’および‘10 .4 .1 アーカイブサービスステータス’を参照ください。

●インスタンスに対するライセンスキーへの設定

BOM マネージャーのライセンスマネージャーで行います。詳細は、‘3 .5 ライセンス管理’を参照ください。

10 .6 「設定ユーティリティ」タブ

BOM 7.0 インストール時に、“設定配布ユーティリティ”を選択した場合、「設定ユーティリティ」タブが表示されます。



●設定一括配布ツール、および設定収集配布ツールの対象は、BOM 7.0 のみです。

A. BOM 設定一括配布ツール

BOM 7.0 の監視設定を複数のリモートコンピューターに対して配布します。

●[一括配布]ボタンをクリックすると、“BOM 設定一括配布”画面が起動します。

B. BOM 設定収集配布ツール

複数のリモートコンピューターから、監視設定をまとめて収集し、監視設定を収集元のコンピューターに再配布するツールです。

●[収集]ボタンをクリックすると、“BOM 監視設定収集”画面が起動します。

●[配布]ボタンをクリックすると、“BOM 監視設定配布”画面が起動します。

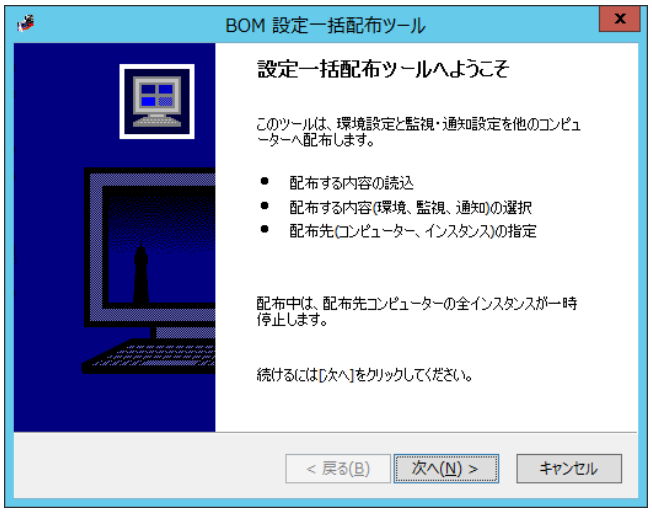
10 .6 .1 BOM 設定一括配布ツール

主に同じ設定を複数のコンピューターに配布したい場合に、BOM 7.0 の監視設定を複数のリモートコンピューターに対して一括して配布することができます。

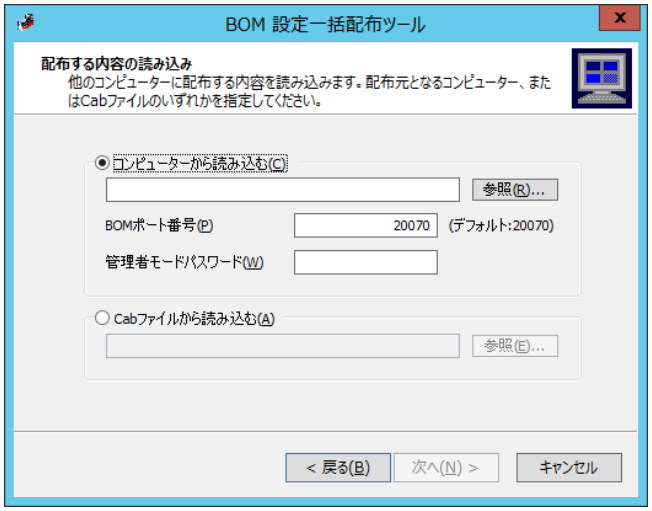
●バックアップファイル、ログファイルの領域確保の観点から、BOM 7.0 を導入するハードディスクドライブには 500MB 以上の空き領域があることを推奨いたします。

●本機能は Linux オプション 7.0、VMware オプション 7.0 のインスタンスには対応しておりません。

1. [一括配布..]ボタンをクリックすると、BOM 設定一括配布ウィザードが開始します。



2. [次へ]ボタンをクリックすると、配布元の指定画面が表示されます。



3. 配布する対象を下記のどちらかより選択します。

●“コンピューターから読み込む”ラジオボタンを選択した場合

BOM 7.0 を導入しているコンピューターから、BOM 7.0 の設定を読み込むことができます。対象の“コンピューター名”または“IP アドレス”、“BOM ポート番号(既定値:20070)”、“管理者パスワード”を指定して、[次へ]ボタンをクリックします。

(BOM マネージャー等で、管理者モードの接続をしている場合、配布設定を読み込むことができません。)

●“CAB ファイルから読み込む”ラジオボタンを選択した場合

BOM 7.0 バックアップファイルなどの監視設定ファイルから BOM 7.0 の設定を読み込むことができます。

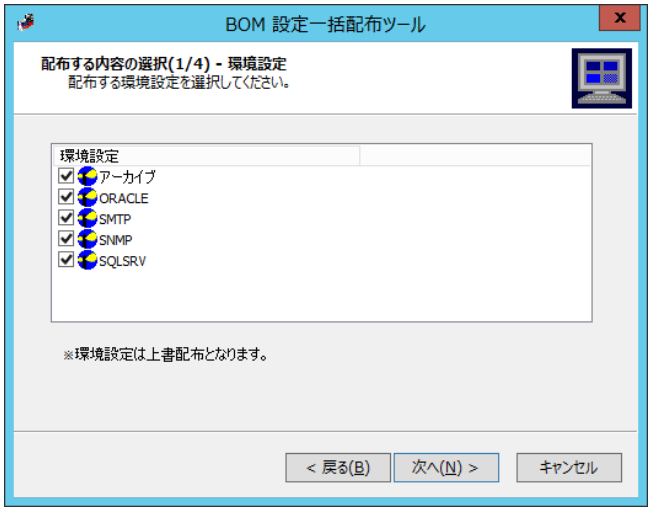
対象の CAB ファイルを指定して、[次へ]ボタンをクリックします。なお、バックアップファイルの作成時に、

“インスタンスのパスワードと SMTP、SNMP、オプション製品のパスワードを削除”チェックボックスにチェックを入れた場合、

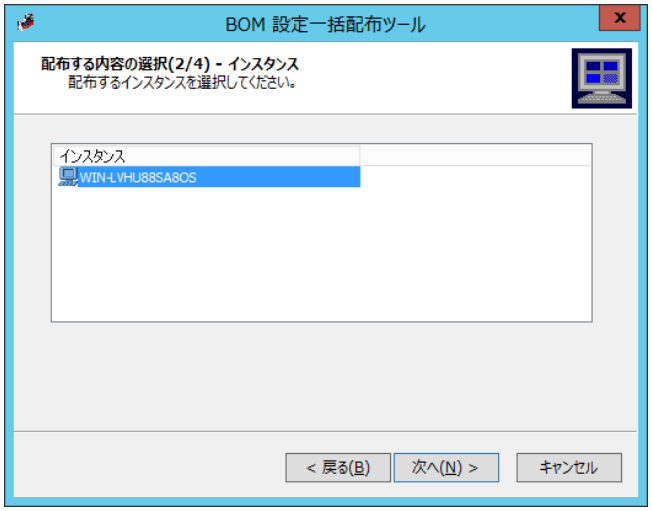
該当箇所のパスワード情報がすべて削除されておりますので、必要に応じて配布先に対して

‘10 .5 .4 パスワードが削除されたバックアップファイルをリストアした場合の注意事項’を参考に、設定を行ってください。

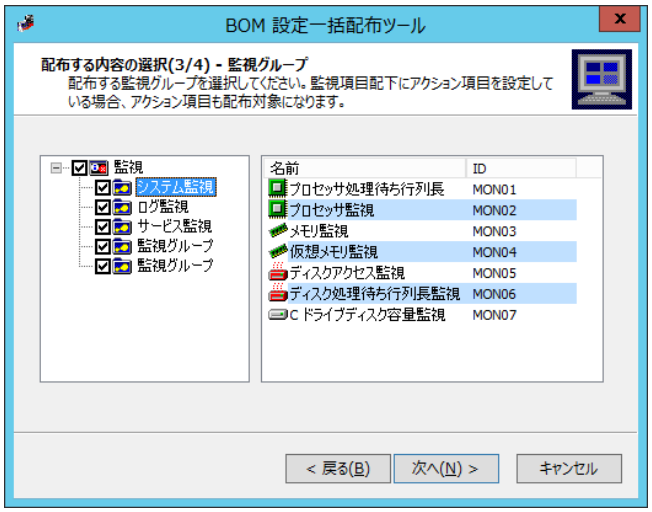
4. “配布内容選択の環境設定”画面が表示されるので、BOM 7.0 の環境に設定に関する配布元の設定リストより、
   配布したい環境設定情報のチェックボックスにチェックを入れた上で、[次へ]ボタンをクリックします。
   ●環境設定は上書きされます。



5. “配布内容選択のインスタンス”画面が表示されるので、配布対象のインスタンスを選択した上で[次へ]ボタンをクリックします。
   ●監視設定 CAB など、インスタンス情報がないファイル、またはインスタンスを作成していない BOM 7.0 から設定を
   読み込んだ場合には、既定値インスタンスと表示されます。

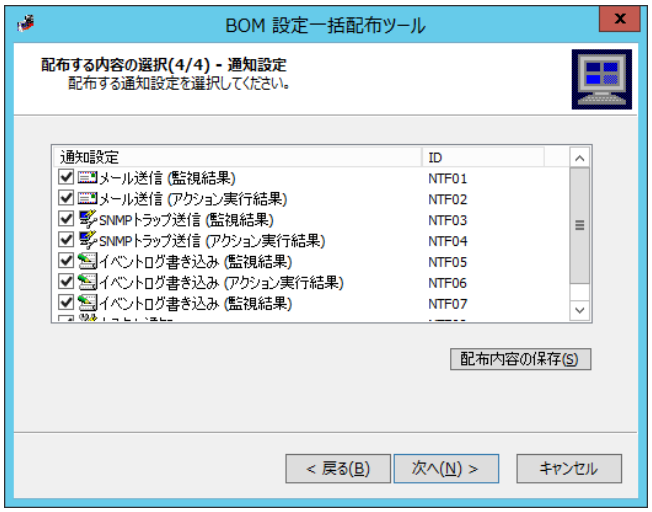


6. “配布内容選択の監視設定”画面が表示されるので、配布したい監視グループを選択した上で[次へ]ボタンをクリックすると、選択した監視グループ配下のすべての監視項目と、すべてのアクション項目が配布されます。

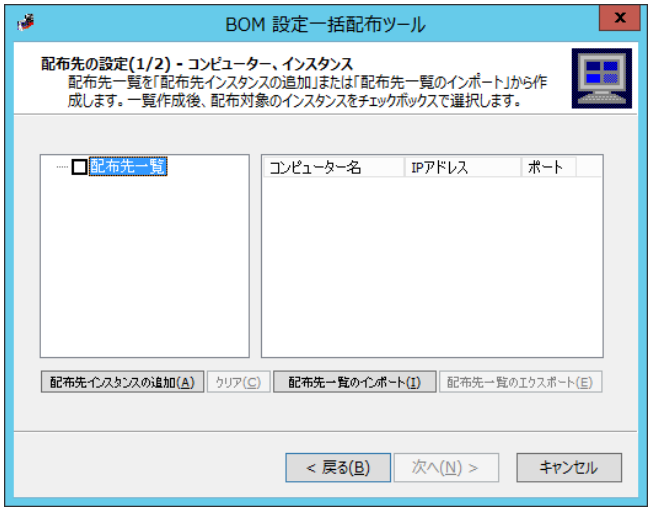


7. “配布内容選択の通知設定”画面が表示されるので、配布したい通知項目を選択した上で、[次へ]ボタンをクリックします。

●[配布内容の保存]ボタンは、他のコンピューターへの配布時に手順 3.の“CAB ファイルから読み込む”で再利用できます。



8. “配布先の一覧”画面で、[配布先インスタンスの追加]ボタンをクリックすると、“インスタンス追加”画面が表示されます。



9. “インスタンス追加”画面にて、配布先コンピューターの“BOM ポート番号（既定値：20070）”と“管理者パスワード”を指定します。配布先コンピューターの指定は、下記のどちらかの手段で設定すると、コンピューターが配布先に追加されます。

●“自動探索”ラジオボタンを選択した場合

[実行]ボタンをクリックすると、自身のコンピューターを含め BOM 7.0 を導入しているコンピューターのすべてを検索できます。

●“IP アドレス範囲から検索”ラジオボタンを選択した場合

ネットワークに接続しており BOM 7.0 を導入しているコンピューターを“IP アドレス”と“範囲（ビット長）”から検索できます。

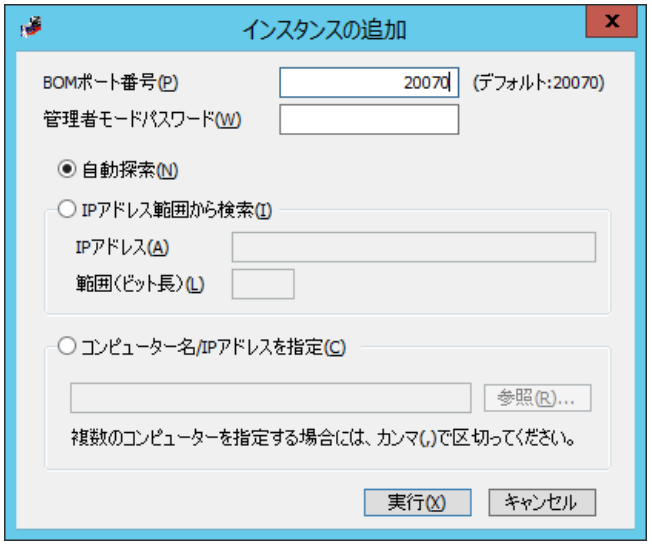
配布先の“IP アドレス”と“範囲（ビット長）”を指定して、[実行]ボタンをクリックします。

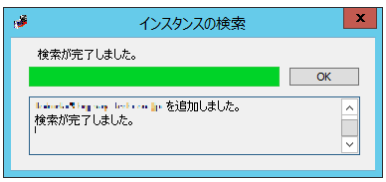
“範囲（ビット長）”の入力範囲は、IPv4 アドレスの場合は 16～32、IPv6 アドレスの場合は 112～128 です。

●“コンピューター名 / IP アドレスを指定”ラジオボタンを選択した場合

コンピューター名 / IP アドレスを直接指定することができます。

配布先のコンピューターを[参照..]ボタン、または“コンピューター名”フィールドに入力して、[実行]ボタンをクリックします。





10.“配布先の一覧”画面にて、配布したくないコンピューターが検出された場合には、チェックボックスのチェックを外し、
配布先一覧に問題がなければ、[次へ]ボタンをクリックします。

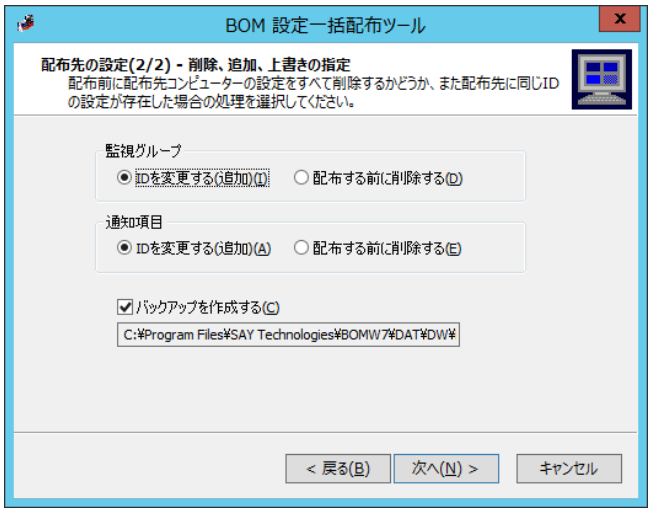
●[クリア]ボタンをクリックすれば配布先一覧をすべて削除することができます。

●[配布先一覧のエクスポート]ボタンをクリックすると、配布先一覧を保存することができます。
保存したファイルは、[配布先一覧のインポート]ボタンを使用して読み込むことができます。

11.“配布方法設定”画面が表示されるので、“監視グループ”に対して下記のどちらかを選択します。

●“ID を変更する（追加）”ラジオボタンを選択した場合
配布先に事前に登録されていた監視グループを残して追加配布することができます。

●“配布する前に削除する”ラジオボタンを選択した場合
配布先に事前に登録されていた監視グループをすべて削除した上で、今回配布したものだけを設定することができます。



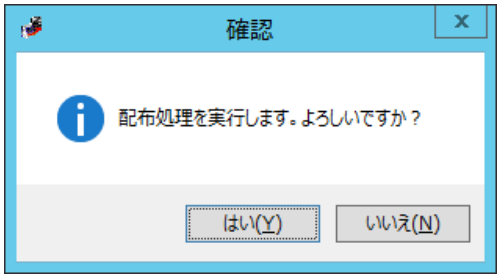
12.“配布方法設定”画面が表示されるので、“通知項目”に対して下記のどちらかを選択します。

●“ID を変更する（追加）”ラジオボタンを選択した場合
配布先に事前に登録されていた通知項目を残して追加配布することができます。

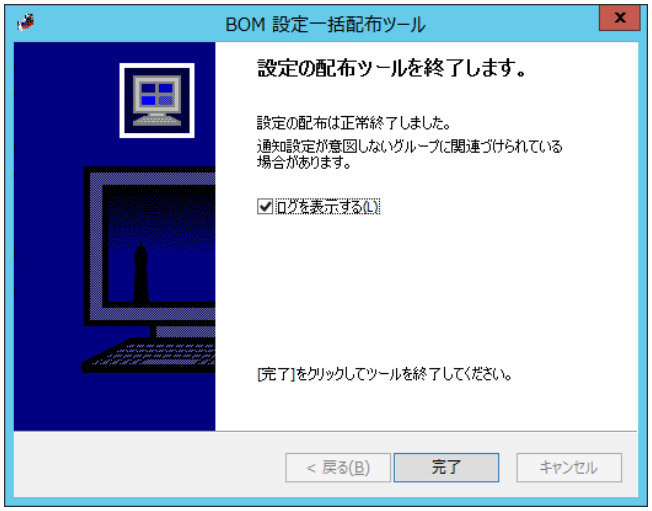
●“配布する前に削除する”ラジオボタンを選択した場合
配布先に事前に登録されていた通知項目をすべて削除した上で、今回配布したものだけを設定することができます。

13.“バックアップを作成する”チェックボックスにチェックを入れると、配布先の現在の状態をバックアップすることができます。

14.[次へ]ボタンをクリックすると“確認”画面が表示されるので、[はい]ボタンをクリックして、配布を実行します。



15. 処理が完了するとメッセージが表示されますので、[次へ]ボタンをクリックし、[完了]ボタンをクリックすると終了します。



16. “ログを表示する”チェックボックスにチェックを入れると、配布完了時に配布状況を示すログを表示させることができます。

10 .6 .2 BOM 設定収集配布ツール

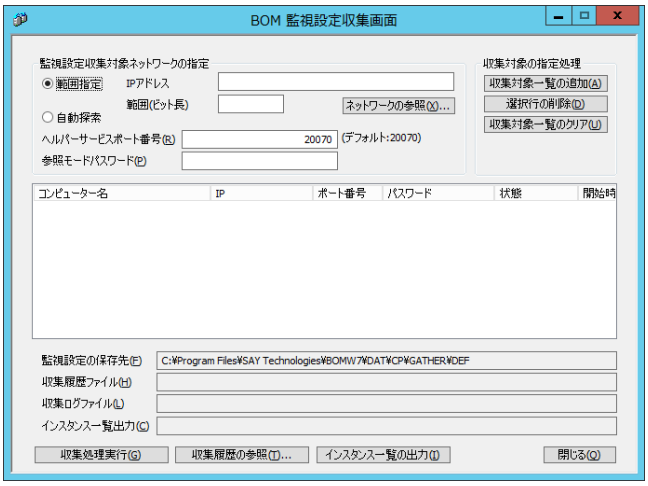
BOM 7.0 の監視設定を複数のリモートコンピューターから収集、再配布する場合に使用します。
コンピューターごとに設定が違う場合に、それぞれの設定を 1 度にまとめて収集後、下記の手順で設定内容を編集し、
再配布する場合に利用します。

1. ネットワーク上で起動する BOM 7.0 の監視設定を BOM 設定収集配布ツールが起動したコンピューターで収集します。
2. 手順 1.のコンピューター上で収集した設定をリストアし、変更したい内容に編集し、バックアップします。
   ●リストアの手順は、‘10 .5 .3 リストア処理’を参照ください。
   ●バックアップの手順は、‘10 .5 .2 バックアップ処理’を参照ください。
   “監視設定のみ”でバックアップを行ってください。“監視設定およびログ”では、再配布を行うことができません。
   バックアップ時に“インスタンスのパスワードと SMTP、SNMP、オプション製品のパスワードを削除”チェックボックスにチェックを
   入れた場合、該当箇所のパスワード情報がすべて削除されていますので、必要に応じて配布先に対して
   ‘10 .5 .4 パスワードが削除されたバックアップファイルをリストアした場合の注意事項’を参考に、設定を行ってください。
3. 手順 2.でバックアップした内容を設定収集配布ツールで配布します。

●Windows クライアント OS には TCP 接続の制限があり、監視設定配布ツールが動作する Windows クライアント OS の
ネットワーク接続状態がビジーで不完全な TCP 送信接続が 10 以上ある場合にはタイムアウトエラーとなります。
本現象は Windows サーバー OS では起きません。

A. 監視設定収集

[収集]ボタンをクリックすると、“BOM 監視設定収集”画面が起動します。



●監視設定収集画面では、BOM 7.0 がインストールされている複数のコンピューターから監視設定を収集して
保存することができます。
●監視設定および収集履歴は収集処理が実行する度に保存されます。
●監視設定はコンピューター別に収集され、CAB ファイルに保存されます。複数のインスタンスを持つコンピューターの

監視設定は一つの CAB ファイルに保存されます。

●収集履歴を参照して再度収集処理を行うことができます。

1. “監視設定収集対象ネットワーク”フィールドに、下記の通り設定を行います。

   ●“IP アドレス”フィールドと“範囲（ビット長）”フィールドに、監視設定の収集対象となるコンピューターの“IP アドレス”と“範囲（ビット長）”を指定します。入力範囲は、IPv4 アドレスの場合は 16～32、IPv6 アドレスの場合は 112～128 です。[ネットワークの参照]ボタンをクリックすると、コンピューターにインストールされているネットワークカードの一覧が表示され、それらに割り振られている IP アドレスと範囲が自動的に設定されます。

   ●“ヘルパーサービスポート番号”では、BOM ヘルパーサービスが使用する“ポート番号（既定値：20070）”を設定します。

   ●“参照モードパスワード”では、収集に用いる参照モードの“パスワード”を指定します。

2. “収集対象の指定処理”フィールドの下記を用いて、収集対象のリストを作成します。

   ●[収集対象一覧の追加]ボタンをクリックすると、手順 1.で指定した接続情報を用いてネットワークから参照モードパスワードで接続できる BOM 7.0 がインストールされているコンピューターを検出し収集対象一覧に追加します。収集の対象となるコンピューター上の BOM ヘルパーサービスが停止している場合、該当するコンピューターは収集対象一覧に表示されません。
   既に収集対象一覧に表示されている場合、状態欄は“エラー”となり、エラーとなった監視設定は収集されません。

   ●[選択行の削除]ボタンをクリックすると、収集対象一覧で選択した行（複数行も可）を削除します。

   ●[収集対象一覧のクリア]ボタンをクリックすると、収集対象一覧で表示されている行をすべて削除します。

3. “監視設定の保存先”には、監視設定の保存先に関する下記情報が表示されます。

   フォルダー　：　<BOM 7.0 インストールフォルダー>¥BOMW7¥DAT¥CP¥GATHER¥DEF¥

   ファイル名　：　BCFG-yyyyMMdd-hhmmss-コンピューター名.CAB

   （yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

4. “収集履歴ファイル”には、[収集処理実行]ボタンにより出力された履歴ファイルに関する下記の情報が表示されます。

   フォルダー:

   <BOM 7.0 インストールフォルダー>¥BOMW7¥DAT¥CP¥GATHER¥DEF¥BCFG-yyyyMMdd-hhmmss-GATHER¥

   ファイル名：BCFG-yyyyMMdd-hhmmss-GATHER.lsv

   （yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

5. “収集ログファイル”には、[収集処理実行]ボタンでエラーが発生した場合に記録される収集ログファイルに関する下記情報が表示されます。

   フォルダー:

   <BOM 7.0 インストールフォルダー>¥BOMW7¥DAT¥CP¥GATHER¥DEF¥BCFG-yyyyMMdd-hhmmss-GATHER¥

   ファイル名：BCFG-yyyyMMdd-hhmmss-GATHER.log

   （yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

6. [収集処理実行]ボタンをクリックすると、“IP アドレス”、“ポート番号”、“参照モードパスワード”で監視対象コンピューターに接続して監視設定ファイルを収集します。

   ●収集処理の履歴を手順 4.“収集履歴ファイル”に保存、エラーが発生した場合は手順 5.“収集ログファイル”にエラー内容を記録します。収集の“状態”は画面に表示され、各種ログファイルに書き込まれます。

   収集済　：　収集対象コンピューターに監視設定ファイルが正常に転送されます。

接続不能 ： 収集対象コンピューターに参照モードパスワードで接続できない。

エラー ： 上記以外に発生したエラー。

7. [収集履歴の参照]ボタンをクリックすると“ファイルを開く”画面が表示され、収集履歴ファイル(*.LSV)を選択することで、選択した LSV ファイルに記録された収集履歴が収集対象一覧に表示されます

8. [インスタンス一覧出力]ボタンをクリックすると、“収集対象一覧”の CAB ファイルからインスタンス一覧を取得して、集中監視コンソールにインポートできる CSV 形式で出力します。

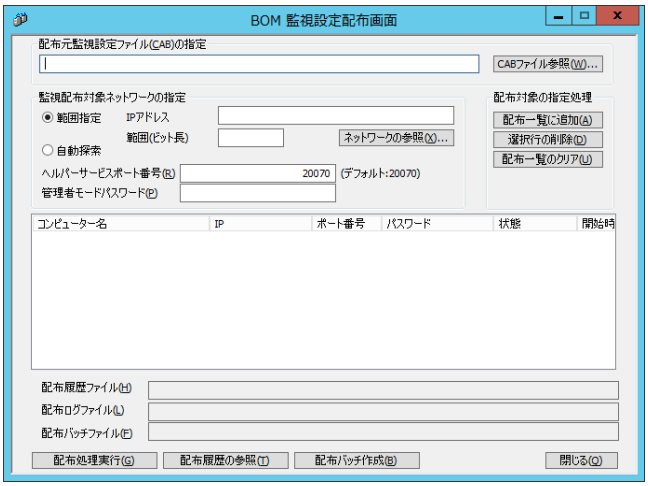
フォルダー ： <BOM 7.0 インストールフォルダー>¥BOMW7¥DAT¥CP¥GATHER¥INS

ファイル名 ： BCFG-yyyyMMdd-hhmmss-INSTANCE-LIST.csv

(yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。)

B. 監視設定配布

[配布]ボタンをクリックすると、“BOM 監視設定配布”画面が起動します。



●監視設定配布画面では、コンピューター別の監視設定ファイルを選択し、それぞれのコンピューターに配布することができます

配布先コンピューター上のインスタンス名とインスタンス数は配布の対象となる CAB ファイルの内容と一致する必要があります。

●‘10 .6 .2 BOM 設定収集配布ツール’で監視設定を収集し、それを編集した後の監視設定ファイルを配布してください。

●配布処理は、画面上の[配布処理実行]ボタンをクリックして直ちに実行することができます。

●“配布バッチ作成”で作成したバッチは、OS のタスクスケジュールに登録して指定した時刻に実行させることもできます。

1. “配布元監視設定ファイル(CAB)の指定”フィールドに、CAB ファイルの絶対パスを入力するか、[CAB ファイル参照]ボタンクリックして、配布対象のファイルを選択することができます。

2. “監視配布対象ネットワーク”フィールドに、下記の通り設定を行います。

●“IP アドレス”フィールドと“範囲(ビット長)”フィールドに、監視設定の配布対象となるコンピューターの“IP アドレス”と“範囲(ビット長)”を指定します。入力範囲は、IPv4 アドレスの場合は 16～32、IPv6 アドレスの場合は 112～128 です。[ネットワークの参照]ボタンをクリックすると、コンピューターにインストールされているネットワークカードの一覧が表示され、それらに割り振られている IP アドレスと範囲が自動的に設定されます。

●“ヘルパーサービスポート番号”では、BOM ヘルパーサービスが使用する“ポート番号(既定値:20070)”を設定します。

●“管理者モードパスワード”では、配布に用いる管理者モードの“パスワード”を指定します。

3. “配布対象の指定処理”フィールドの下記を用いて、配布対象のリストを作成します。

●[配布一覧に追加]ボタンをクリックすると、手順 2.で指定した接続情報を用いてネットワークから
管理者モードパスワードで接続できる BOM 7.0 がインストールされているコンピューターを検出し、配布一覧に追加します。
収集の対象となるコンピューター上の BOM ヘルパーサービスが停止している状態、あるいは BOM マネージャーが
管理者モードで BOM ヘルパーサービスに接続している場合は、該当するコンピューターは配布一覧に表示されません。
既に配布対象一覧に表示されている場合、状態欄は“エラー”となります。

●[選択行の削除]ボタンをクリックすると、配布一覧で選択した行（複数行も可）を削除します。

●[配布一覧のクリア]ボタンをクリックすると、配布一覧で表示されている行をすべて削除します。

4. “配布履歴ファイル”には、[配布処理実行]ボタンをクリックすることで出力された履歴ファイルに関する情報が表示されます。
5. “配布ログファイル”には、[配布処理実行]ボタンをクリックすることでエラーが発生した場合に記録される配布ログファイルに関する情報が表示されます。
6. [配布処理実行]ボタンをクリックすると、“IP アドレス”、“ポート番号”、“管理者モードパスワード”で監視対象コンピューターに接続して監視設定ファイルを配布します。

●配布処理を実行する際、配布先コンピューター上の BOM ヘルパーサービス以外の監視サービスおよびアーカイブサービスはすべて停止処理が実行しますが、Windows のサービスマネージャーからサービスの停止要求を受けて約 1 分間内に停止できなかった場合は、配布処理のタイムアウトとなり、配布処理が失敗になります。

●インスタンスに処理時間の長い監視項目が登録されている場合、該当インスタンスは事前に停止することを推奨します。

●配布処理が正常に完了後、配布先コンピューターの監視サービス、アーカイブサービスの起動/停止状態は、配布処理が実行される前の状態に戻されます。

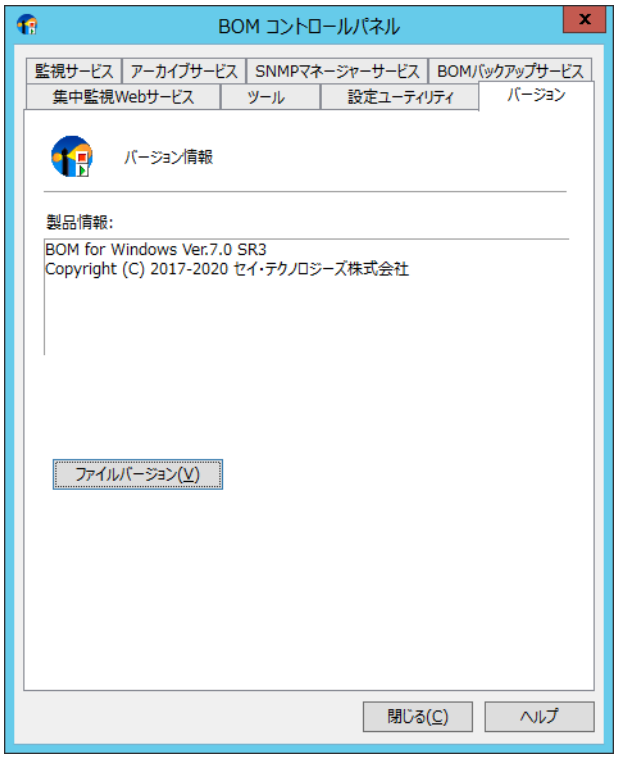
●配布処理の履歴を手順 4.“配布履歴ファイル”に保存、エラーが発生した場合は手順 5.“配布ログファイル”にエラー内容を記録します。収集の“状態”は画面に表示され、各種ログファイルに書き込まれます。

収集済　：　配布対象コンピューターに監視設定ファイルが正常に転送された。
接続不能：　配布対象コンピューターに管理者モードパスワードで接続できない。
エラー　：　上記以外に発生したエラー。

7. [配布履歴の参照]ボタンをクリックすると“ファイルを開く”画面が表示され、配布履歴ファイル（*.LSV）を選択することで、選択した LSV ファイルに記録された配布履歴が配布対象一覧に表示されます。
8. [配布バッチ作成]ボタンをクリックすると、配布対象一覧に設定されている配布情報で“配布バッチファイル”を作成します。“配布バッチファイル”の情報は、“配布バッチファイル”フィールドに表示されます。

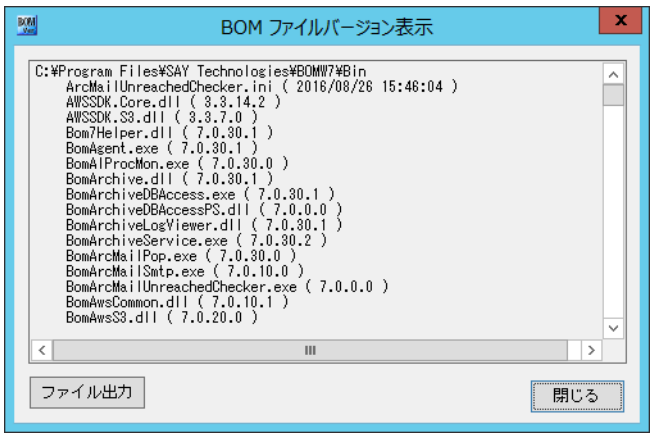
10 .7 「バージョン」タブ

バージョンタブでは、本製品のバージョンが確認できます。



1. [ファイルバージョン]ボタンをクリックすると、同梱されている各ファイルのバージョンが確認できます。

   ●各モジュール単位に内部バージョンが表示されます。なお、下記画面はサンプルです。

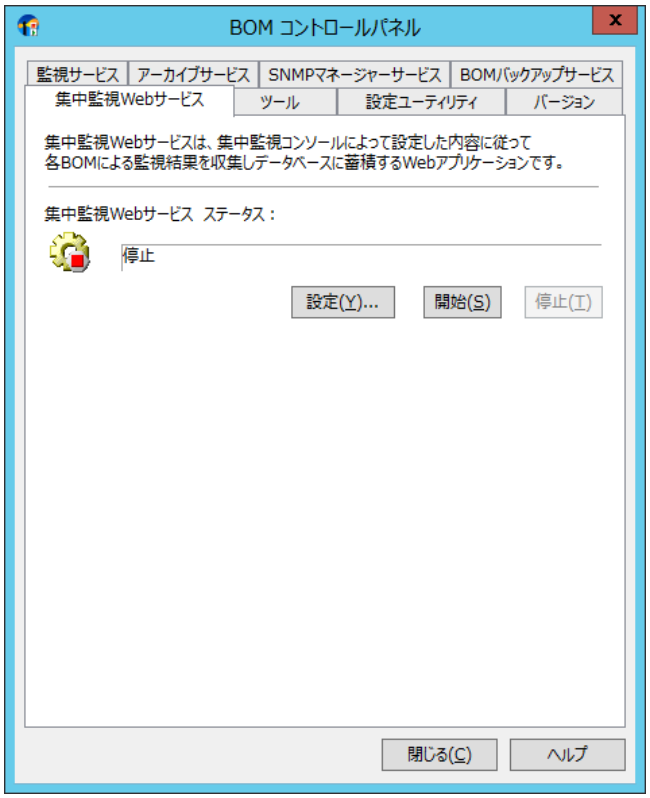


2. [ファイル出力]ボタンをクリックすると、手順 2.で表示されたバージョン情報をテキストファイルに出力することができます。

   ファイル名 ： VER-yyyyMMdd-hhmmss.txt （yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

10 .8 「集中監視 Web サービス」タブ

「集中監視 Web サービス」タブでは、集中監視 Web サービスの各種制御を行うことができます。



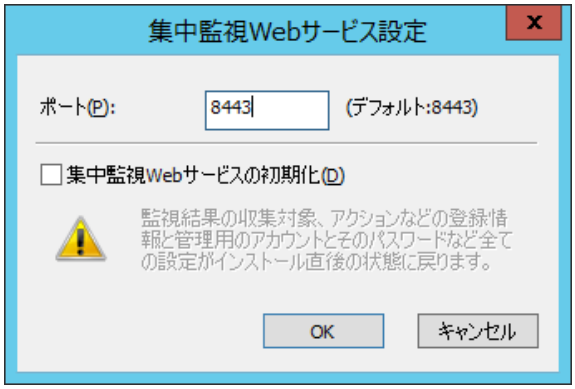
1. “集中監視 Web サービス ステータス”フィールドは、集中監視 Web サービスの“開始”と“停止”制御を行うことができます。

   ●[開始]ボタンをクリックすることで、集中監視 Web サービスを“開始”させることができます。

   ●[停止]ボタンをクリックすることで、集中監視 Web サービスを“停止”させることができます。

   “停止”状態の際には、[設定]ボタンが有効になります。

2. “集中監視 Web サービス ステータス”フィールドの[設定]ボタンをクリックすると、“集中監視 Web サービス設定”画面が表示されます。

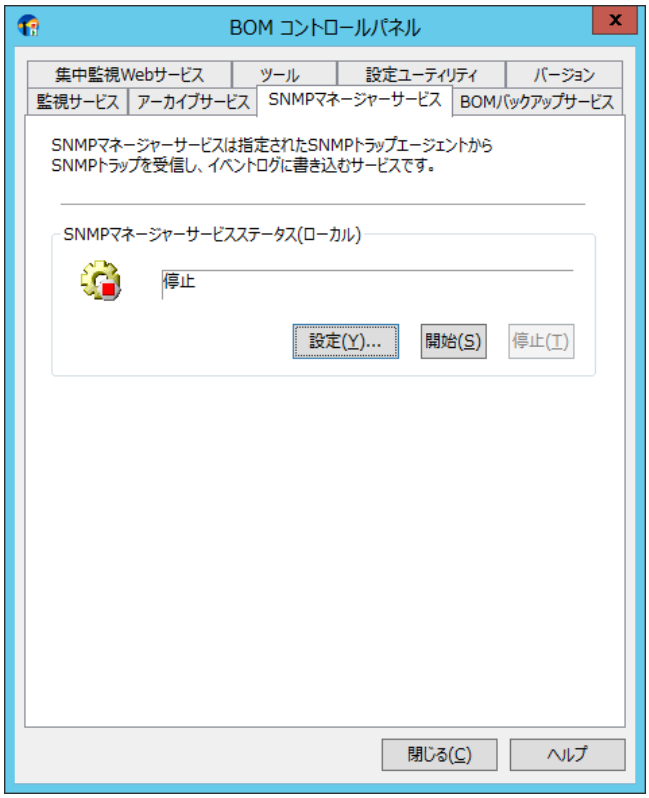


3. “ポート”フィールドには、集中監視 Web サービスが用いるポート番号を、“1”~“65535”の範囲で指定することができます。
4. “集中監視 Web サービスの初期化”チェックボックスにチェックを入れて[OK]ボタンをクリックすると、BOM 集中監視コンソールより行ったすべての設定をインストール直後の状態に初期化することができます。

   その他詳細については、‘集中監視コンソール ユーザーズマニュアル’を参照してください。

10 .9 「SNMP マネージャーサービス」タブ

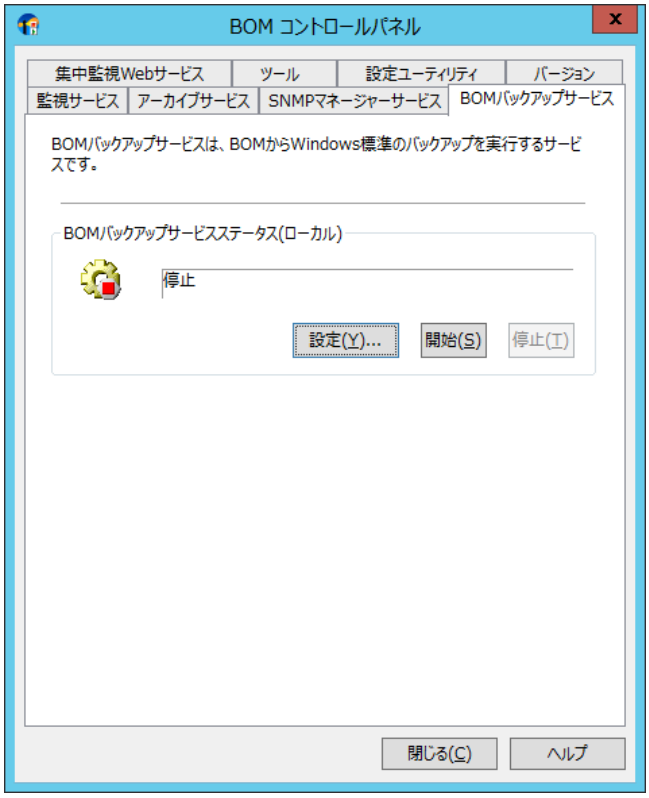
「SNMP マネージャーサービス」タブでは、SNMP マネージャーサービスの各種制御を行うことができます。



詳細については‘SNMP トラップ受信機能ユーザーズマニュアル’を参照してください。

10 .10 「BOM バックアップサービス」タブ

「BOM バックアップサービス」タブでは、バックアップサービスの各種制御を行うことができます。



詳細については‘バックアップ機能ユーザーズマニュアル’を参照してください。

第11章 障害リカバリ

11 .1 バックアップとリストア

BOM 7.0 インスタンスのすべての設定値をバックアップするには、BOM コントロールパネルを開き、バックアップ/リストアユーティリティを使用します。詳細は、‘10 .5 .2 バックアップ処理’と‘10 .5 .3 リストア処理’を参照ください。

11 .2 コマンドラインツール

BOM 7.0 インスタンスの設定データの保存と復元はコマンドラインからも実行できます。

●コマンドラインツールは、下記のフォルダーに格納されています。

<BOM 7.0 インストールフォルダー>¥BOMW7¥Bin

11 .2 .1 BomCmd.exe

BomCmd.exe は以下の設定ファイルをインポート/エクスポートすることができます。

・動作環境

・SNMP トラップ受信設定

・監視設定

BomCmd.exe コマンド

-HELP　　ヘルプを表示します。

BomCmd ImportEnvironment

-h:ホスト名　　必須　接続先ホスト

-p:ポート番号　　接続先ポート 省略時:20070

-pw:パスワード　　必須　接続パスワード

-in:入力ファイル名　必須

解説:動作環境・SNMP トラップ受信設定をインポートします。

BomCmd ExportEnvironment

-h:ホスト名　　必須　接続先ホスト

-p:ポート番号　　接続先ポート 省略時:20070

-pw:パスワード　　必須　接続パスワード

-out:出力ファイル名 必須

解説:動作環境・SNMP トラップ受信設定をエクスポートします。

BomCmd ImportSetting

-h:ホスト名	必須	接続先ホスト
-p:ポート番号		接続先ポート 省略時:20070
-pw:パスワード	必須	接続パスワード
-in:入力ファイル名	必須	
-i:インスタンス名	必須	
-or		旧設定を上書きする

解説:監視設定をインポートします。

BomCmd ExportSetting

-h:ホスト名	必須	接続先ホスト
-p:ポート番号		接続先ポート 省略時:20070
-pw:パスワード	必須	接続パスワード
-out:出力ファイル名	必須	
-i:インスタンス名	必須	
-type:ALL|MON|NTF		ALL:すべて MON:監視 NTF:通知 省略時:ALL

解説:監視設定をエクスポートします。

11 .2 .2 MxSysConf.exe

MxSysConf.exe はバックアップリストアを実行できます。

MxSysConf.exe –backup

-file:バックアップファイル	必須	バックアップファイルのパスを指定する
-dlpw		パスワード設定除去オプション
		本オプションを指定した場合、暗号化パスワードをバックアップから除去する。
		本オプションを指定しない場合、暗号化パスワードもバックアップする。
-keep		サービス状態保持オプション
		バックアップ取得時は、監視サービス、アーカイブサービスが停止する。
		本オプションを指定した場合、バックアップ完了後に各サービスを元に戻す。
		本オプションを指定しない場合、バックアップ完了後もサービスを開始しない。
-log:ログファイル		バックアップ実行結果を保存するログファイルのパスを指定する

解説:BOM 7.0 のバックアップを行います。

MxSysConf.exe –restore

-file:バックアップファイル	必須	リストアするバックアップファイルのパスを指定する
-log:ログファイル		リストア実行結果を保存するログファイルのパスを指定する

解説:BOM 7.0 のリストアを行います。

第12章 トラブルシューティング

制限事項、注意事項の最新情報については、リリースノートあるいは弊社ホームページを参照ください。

A. BOM 7.0 が監視を実行しない

監視を実行しないインスタンスの監視サービスが開始していることを確認します。

BOM 7.0 ツリー内で監視を実行した監視項目のグループと監視項目が有効になっていることを確認します。

また、監視グループのスケジュールと各監視項目の有効の設定が両方有効にならないと監視を実行しませんのでご注意ください。

B. BOM 7.0 が代理監視を実行しない

代理監視に必要な設定は、'BOM for Windows Ver.7.0 インストールマニュアル'、もしくは、本マニュアルの

'3 .3 .2 代理監視設定のポイント'や'3 .3 .3 代理監視設定が正しく監視できない場合のトラブルシューティング'を

参照ください。

C. BOM 7.0 がリモートインスタンスを監視しない

ping コマンドを使用してリモートシステムへのネットワーク接続を確認します。

D. BOM 7.0 が電子メールメッセージを送信しない

"BOM for Windows"を右クリックし、コンテキストメニューのプロパティをクリックし、"プロパティ"画面の SMTP サーバー情報の

設定値を確認します。

メール送信アクション項目が有効になっていることを確認します。

"メール送信のプロパティ"の「設定」タブに移動し、"宛先アドレス:"フィールドに正しい電子メールアドレスが

入力されていることを確認します。

E. BOM 7.0 がポップアップメッセージを送信しない

BOM 7.0 が稼働するシステムと、ポップアップメッセージを受信するシステムの両方で Messenger サービスが開始していることを

確認します。

Windows Server 2008 以降の OS には、Messenger サービスが存在しないので、ポップアップメッセージは送信できません。

F. SNMP トラップが機能しない

SNMP の設定を行っているかご確認ください。'2 .3 .4 SNMP 情報の設定'項目を参照ください。

G. TCP 接続エラー

BOM 7.0 が稼働するコンピューターがネットワークに接続していることを確認します。

または、最低限スイッチまたはハブに接続し、ネットワークが機能していることを確認します。

BOM マネージャーの“BOM for Windows Ver.7.0（ローカル）”プロパティ画面と、
BOM コントロールパネル→「監視サービス」タブ→“ヘルパーサービス設定”画面の
BOM ヘルパーサービスポート番号が同じであることを確認します。
また、コンピューターの BOM ヘルパーサービスが起動していることを確認します。

仮に代理監視元コンピューターと代理監視先コンピューターの経路上にファイアウォールが設置されている場合や、
代理監視先コンピューターの OS の Windows ファイアウォールが有効になっている場合には、
‘3 .3 .2 代理監視設定のポイント’の項目‘D.認証、データ連携用ポートの開放’で解説した通信をブロックしている
可能性があります。その場合には、経路上のファイアウォールもしくは Windows ファイアウォールが必要な通信を
ブロックしていないか確認します。

H. MMC ハングアップによる強制終了後、同インスタンスへの接続ができない

MMC がハングアップし、強制終了した場合の対処方法です。
BOM マネージャーを起動し、接続を試みても“管理者モードはすでに使用されています”というエラーメッセージが表示され、
接続できなくなります。
本件の対処方法は、BOM ヘルパーサービスをコントロールパネルのサービスから再起動してください。

I. インストール時に“1607:InstallShield Scripting Runtime をインストールできません”とポップアップがでる

インストールを開始すると、InstallShield より“1607:InstallShield Scripting Runtime をインストールできません”という
ポップアップがでるものの、インストール自体は進行します。

この原因は下記の問題が考えられるので、下記の該当する原因を取り除いた上で、再度インストールを行ってください。
●subst コマンドを使用して作成した仮想ドライブからセットアッププログラムを実行している。
●インストーラ Msiexec.exe が正しく登録されていない。
●ユーザーアカウントに、C:¥Windows¥Installer フォルダーにアクセスするためのアクセス許可がない。
●古いバージョンの Windows インストーラエンジンが、現在利用できなくなっているネットワークドライブからインストールした。
●コンピューターにソフトウェアをインストールするためのアクセス許可がユーザーアカウントにない。
●Msiexec.exe の別のインスタンスが実行されている。
●Windows インストーラベースの別のセットアッププログラムが実行されている。
●Windows OS が破損している。

J. インスタンスの停止処理がタイムアウトした場合の動作について

監視実行中に監視サービスが停止した場合にはインスタンスアイコンが灰色になり、BOM マネージャーの操作ができません。
監視が終了すると操作可能ですが、インスタンスアイコンは灰色のままです。
インスタンスの再接続あるいは BOM 7.0 スナップインを選択して最新の情報に更新してください。

また、本現象の後、テキストログ監視、イベントログ監視の場合、もし次の監視が実行されない場合には、下記の通り対処をお願いします。

●監視項目を再度新規作成する

●下記のファイルを削除してください。

フォルダー：<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Instance¥<該当インスタンス名>¥PersistentData¥

ファイル名：GRP<該当グループ No.>MON<該当監視項目 No.

K. 高負荷時のディスクアクセス監視の監視値の問題

高負荷時のディスクアクセス監視においてはステータスが失敗になります。

この原因はディスク関連のパフォーマンスデータによるものです。

L. カスタムアクション/カスタム通知でコンソールプログラム（メモ帳や Internet Explorer などの exe ファイル）を指定した場合、指定コンソールプログラムが画面上に見えない。

監視サービスと BOM ヘルパーサービスの設定で、デスクトップとの対話をサービスに許可をチェックいれてください。

この場合、BOM ヘルパーサービスの再起動が必要です。

ただし、代理監視の場合には、カスタムアクション/カスタム通知でコンソールプログラムは指定できません。

M. BOM ヘルパーサービス通信での失敗のタイムアウト時間を変更したい。

BOM ヘルパーサービスでの通信タイムアウトは既定値 3 分になっています。

下記の<XXX>部分を編集することで、タイムアウト時間を変更することができます。

フォルダー　：　<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Config¥

ファイル名　：　MxHelper.ini

変更箇所　：　[Option]

ProcessTimeout = <XXX>

N. ディスク容量監視での“前回の値”としきい値の関係

前回の値については端数を切り捨てて表示しています。

たとえば 12.7GB の値であっても 12GB に表示されますのでご注意ください。

O. 代理監視時の SNMP トラップの送信元について

代理監視の SNMP トラップアクションの場合、代理監視先コンピューターではなく、代理監視元コンピューターの IP アドレスが SNMP マネージャーに送信されます。

あらかじめ SNMP マネージャーには代理監視先だけではなく、代理監視元のコンピューターも登録してください。

P. プロセスタイムアウトのエラーが出る

多くの監視項目の設定を行っている場合等、その監視項目を複製しようとすると下記のエラーメッセージが出ることがあります。

このエラーメッセージが頻繁に出る場合には下記の設定を変更してください。
既定値は 180（秒）ですが、この数値を大きくすることで現象が回避できます。

フォルダー　：　<BOM 7.0 インストールフォルダー>¥BOMW7¥Environment¥Config¥
ファイル名　：　MxHelper.ini
変更箇所　：　[Option]
　　ProcessTimeout = 180

Q. Windows ファイアウォール等で TCP ポートをすべて遮断した場合の現象

Windows ファイアウォールにて、ポートをすべて遮断した場合、代理監視の設定/監視を行うことができないため、その際に一部の監視項目では監視項目のプロパティで、「設定」タブを押下したときにそれぞれ異なった問題が発生する場合があります。

1. システムのエラーメッセージ

●OS が返すエラーメッセージはすべてそのままエラーメッセージとして表示されます。

2. エラーメッセージが特殊なもの

●プロセッサ監視

インスタンスが取得できない。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●メモリ監視

Available Bytes の値が取得できない。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●ディスクアクセス監視

インスタンスが取得できない。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●ネットワークインターフェイス監視

インスタンスが取得できない。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●ディスク容量監視

ディスク一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

●フォルダー・ファイル監視

[参照]ボタンをクリックした際に、ディスク情報一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

●サービス監視

[参照]ボタンをクリックした際に、サービス一覧が取得できない。

“RPC サーバーを利用できません。”のエラーメッセージが出力される。

●プロセス監視

プロセス一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

●パフォーマンスカウンター監視

パフォーマンスオブジェクト一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

●テキストログ監視

[参照]ボタンをクリックした際に、ディスク情報一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

3. 影響がないもの

●Ping 監視

代理監視のインスタンスでも、ping を実際に実行するのは代理監視元であるため、ファイアウォールの影響を受けない。

●ポート監視

代理監視のインスタンスでも、ポートを実際に実行するのは代理監視元であるため、ファイアウォールの影響を受けない。

R. エクスポート先の書き込み権限について

BOM マネージャーを操作してファイルに直接書き出す操作（監視設定のエクスポート等）では、必ずログオンしたユーザーが指定したフォルダーに書き込める権限があることを確認してください。もし書き込める権限がない場合には、エラーになります。

S. リソース不足での監視サービス停止のエラーメッセージ

BOM 7.0 以外のコンピューター環境の影響で BOM 7.0 がリソースを確保できず、監視サービスが停止する場合には、BOM マネージャーの“ログ”→“ヒストリー”→“サービス”配下にメモリ容量不足というエラーメッセージが出力され、監視サービスは停止します。

上記のヒストリーのエラーメッセージの後、“ログ”→“ヒストリー”→“サービス”配下に情報メッセージが出力され、メモリ不足が原因で監視サービスが停止したことが確認できます。

第13章 エラーコード、エラー内容一覧

13 .1 BOM 7.0 監視サービスのヒストリー サービスログ記述内容一覧

カテゴリ	メッセージ内容	出力契機
情報	%1 サービスは正常に開始しました。 PID: %2 インスタンス ID: %3	サービス開始時
情報	%1 サービスは正常に停止しました。 PID: %2 インスタンス ID: %3 経過時間: %4 (ミリ秒)	サービス正常停止時
情報	%1 サービスは正常に動作中です。 PID: %2 インスタンス ID: %3 経過時間: %4 (ミリ秒) スケジューラ: %5 イベントハンドラ: %6 アクティブな監視ワーカーの数: %7 アクティブなアクションワーカーの数: %8	毎日 24 時に出力
情報	%1' でログオンしました。	代理監視 開始時(再接続時)
情報	%1 サービスは、メモリの不足またはエラーのため停止しました。 PID: %2 インスタンス ID: %3 経過時間: %4 (ミリ秒)	サービス異常停止時
警告	前回の監視が完了していないため、監視 '%1' は スキップされました。	前回の監視が完了する前に次の監視が 実施された場合(監視輻輳時)
情報	監視 '%2' のステータスが %10 に変化しました。 ID: %1 実行時間: %6 値: %9	監視ステータス変化時

カテゴリ	メッセージ内容	出力契機
エラー	監視 '%2' はコード %8 で失敗しました。 ID: %1 オブジェクト名: %3 値名: %4 オプション引数: %5 実行時間: %6 メッセージ: %11 ソース: %12 説明:%13	監視失敗時
情報	アクション [%1] '%2' は成功しました。 ID: %1 プログラム名: %3 引数: %4 実行時間: %5 経過時間: %6 出力:%8	アクション成功時
エラー	アクション [%1] '%2' はコード %7 で失敗しました。 ID: %1 プログラム名: %3 引数: %4 実行時間: %5 経過時間: %6 出力:%8	アクション失敗時
エラー	アクション [%1] '%2' はコード %7 で失敗しました。 ID: %1 プログラム名: %3 引数: %4 実行時間: %5 メッセージ: %6	アクション実行失敗時
情報	アクション [%1] '%2' は開始しました。	アクション開始時
情報	通知 [%1] '%2' は開始しました。	通知アクション開始時
警告	アクション [%1] はスキップされました。 インスタンスが停止しているため、アクション [%1] '%2' は スキップされました。	サービス停止時にアクション実行中で あった場合

カテゴリ	メッセージ内容	出力契機
警告	アクション実行が輻輳しています。 この状態が続くとアクションの実行が遅延し、最終的に 監視サービスが停止します。	アクション輻輳時
エラー	ライセンス情報の取得に失敗しました。%1	ライセンス情報取得失敗時
エラー	致命的なエラーが発生したためサービスを 継続できません。%r%1	バグ(予想外のエラー)
エラー	メモリ容量が不足しています。 致命的なエラーが発生したためサービスを継続できません。	メモリ不足時
エラー	設定ファイルの読み込みに失敗しました。(0x80000403) XML ファイルの読み込みに失敗しました (MonitorItem)。	監視設定ファイルの破損を検知した場合

13 .2 メール送信エラーコード

ErrorCode	日本語メッセージ	エラー内容
0	メール送信が完了しました。	送信成功
101	パラメーターが間違っています。 [%1!s!].	パラメーターエラー
102	パスワードの復号化に失敗しました。	パスワード復号化失敗
201	ソケットの初期化に失敗しました。 %1!s! サーバー:[%2!s!]	Socket 初期化エラー(SocketStartup)
202	サーバーの IP アドレスが見つかりません。 %1!s! サーバー:[%2!s!]	サーバーの IP Address が見つからない
203	ソケットの初期化に失敗しました。 %1!s! サーバー:[%2!s!]	Socket 初期化エラー(Create)
204		Socket 初期化エラー(CreateEvent)
205		Socket 初期化エラー(EventSelect)
206	ソケットの接続エラー。%1!s! サーバー:[%2!s!]	Socket 接続エラー
207	ソケットの接続がタイムアウトになりました。 %1!s! サーバー:[%2!s!]	Socket 接続タイムアウト
208	ソケットの接続エラー。%1!s! サーバー:[%2!s!]	Socket 接続エラー(EnumNetworkEvents)
209	ソケット切断エラー。	Socket 切断エラー
210	ソケット読み取りエラー。%1!s!	Socket Read エラー
211	ソケット送信エラー。%1!s!	Socket Send エラー
222	SMTP 接続エラー。 %1!s! %2!s!	SMTP 接続エラー
223	SMTP 初期化、ローカルホストが見つかりません。 %1!s!	SMTP 初期化 Localhost が見つからない
224	SMTP 初期化コマンドエラー。 %1s! %2!s!	SMTP 初期化 コマンドエラー
231	-	Base64 Encode に失敗

ErrorCode	日本語メッセージ	エラー内容
232	-	Base64 Decode に失敗
241	POP3 サーバー接続エラー。 %1!s! %2!s!	POP3 サーバー接続エラー
242	POP3 ユーザーエラー。 %1!s! %2!s!	POP3 ユーザーエラー
243	POP3 パスワードエラー。 %1!s! %2!s!	POP3 パスワードエラー
251	SMTP 認証（CRAM -MD5)がサポートされていません。	SMTP 認証 CRAM-MD5 未サポート
252	SMTP 認証（CRAM -MD5) に失敗しました。 %1!s! %2!s!	SMTP 認証 CRAM-MD5 エラー
261	SMTP 認証(PLAIN)がサポートされていません。	SMTP 認証 PLAIN 未サポート
262	SMTP 認証(PLAIN)に失敗しました。 %1!s! %2!s!	SMTP 認証 PLAIN エラー
271	SMTP 認証(CRAM- MD5, PLAIN)に失敗しました。	SMTP 認証 (PLAIN CRAM-MD5 共)エラー
281	SMTP 認証(LOGIN)がサポートされていません。	SMTP 認証 LOGIN 未サポート
282	SMTP 認証(LOGIN)に失敗しました。 %1!s! %2!s!	SMTP 認証 LOGIN エラー
301	メールアドレスが不正です。 %1!s!	メールアドレス不正
302	送信先アドレスがありません。	送信先なし
303	送信元表示名を設定できません。	送信元表示名エラー
304	ユーザー定義ヘッダー名とテキストの数は一致していません。	ユーザー定義ヘッダー不一致エラー (headname,headtext の数が一致しない)
305	ユーザー定義ヘッダーを設定できません。 %1!s!	ユーザー定義ヘッダー設定エラー
306	件名を設定できません。	件名設定エラー
307	本文メッセージを設定できません。	本文追加エラー
308	メール送信が失敗しました。	メール送信エラー
351	添付ファイル名が不正です。	添付ファイル名が不正
352	添付ファイル名は予約デバイス名です。	添付ファイル名が予約デバイス名
353	添付ファイルが見つかりません。	添付ファイルが見つからない
354	添付ファイル名はフォルダーです。	添付ファイル名がフォルダー
355	添付ファイルはアクセスが拒否されました。	添付ファイルアクセス拒否
356	ファイルを添付できません。	添付ファイルを添付できない
357	添付ファイルを圧縮できません。	添付ファイル圧縮エラー
371	埋め込みテキストファイル名が不正です。	本文埋め込みファイル名が不正
372	埋め込みテキストファイル名は予約デバイス名です。	本文埋め込みファイル名が予約デバイス名
373	埋め込みテキストファイルが見つかりません。	本文埋め込みファイルが見つからない
374	埋め込みテキストファイル名はフォルダーです。	本文埋め込みファイル名がフォルダー
375	埋め込みテキストファイルはアクセスが拒否されました。	本文埋め込みファイルアクセス拒否
376	埋め込みファイルはテキストファイルではありません。	本文埋め込みファイルがテキストファイルではない
377	埋め込みテキストファイルオープンエラー。	本文埋め込みファイルオープンエラー
378	埋め込みテキストファイル読み取りエラー	本文埋め込みファイルリードエラー

ErrorCode	日本語メッセージ	エラー内容
391	ファイルサイズリミットを超えています。	ファイルサイズオーバー
501	例外が発生しました。 %1!s! %2!s!	例外発生
502	メールデータの初期化エラー。	CoCreateInstance Error
503	351 又は 371 のエラーメッセージ	ファイル名不正
504	352 又は 372 のエラーメッセージ	予約デバイス名
505	353 又は 373 のエラーメッセージ	ファイルが見つからない
506	354 又は 374 のエラーメッセージ	指定ファイルがフォルダー
507	355 又は 375 のエラーメッセージ	アクセス拒否
---	その他のエラー。	上記以外のエラーが発生し、エラーメッセージが定義されていない場合に表示される

13 .3 シャットダウンアクション時のエラーコード表

エラーコード	エラー内容
0	正常終了
100	パラメーターが間違っています。
101	セッションの取得に失敗しました。（以下省略）
103	シャットダウンに失敗しました。（以下省略）

13 .4 SNMP トラップ送信のエラーコード表

MxTrap.exe ExitCode	Description
0	Success
1	snmptrap.exe 実行エラー
	（エラーの詳細は、標準出力に表示されるため、BOM 7.0 マネージャーのヒストリーを参照すること）
87	パラメーター エラー
	（エラーの詳細は、標準出力に表示されるため、BOM 7.0 マネージャーのヒストリーを参照すること）
1460	タイムアウト
	snmptrap.exe の終了待ちタイムアウト
GetLastError 値	CreateProcess エラー
	CreateProcess の結果の GetLastError 値
GetLastError 値	snmptrap.exe 終了コード取得エラー
	snmptrap.exe の GetExitCodeProcess 失敗時の GetLastError 値

13 .5 サービスコントロール時のエラーコード表

終了コード	エラー内容
87	パラメーターが間違っています。
1052	要求された制御はこのサービスに対して無効です。
1060	指定されたサービスはインストールされたサービスとして存在しません。
1460	タイムアウト期間が経過したため、この操作は終了しました。
1722	RPC サーバーを利用できません。

13 .6 イベントログ書き込みアクションのエラーコード

イベントログに表示される イベント ID	イベントログに書き込む エラーコード Define	備考
5010	ERROR_INVALID_PARAMETER_LOG	コマンドラインパラメーターエラー
		-s もしくは -m は無い
3407	ERROR_PUT_EVENTLOG	イベントログ書き込みエラー
3408	ERROR_APPLOG_FULL	アプリケーションログが一杯
5011	ERROR_REG_CANT_OPEN	レジストリがオープン不可
5012	ERROR_REG_QUERY_VALUE	レジストリ読み出しエラー
5013	ERROR_REG_CANT_CREATE	レジストリキー作成不可
5014	ERROR_REF_SET_VALUE	レジストリ書き込みエラー

13 .7 BomCmd.exe のエラーコード表

コード	メッセージ	備考
101	必須パラメーター(xxx)が有りません。	必須パラメーターがない場合
102	パラメーター(-xxx:xxx)で値のチェックエラーが発生しました。: %s	パラメーター値が間違えている場合に発生する。 詳細メッセージも表示する。
104	監視エージェント(xxx)が稼動している為コマンドを 実行できません。 全ての監視を停止してください。	
105	監視エージェント(xxx)が稼動している為コマンドを 実行できません。 このインスタンスの監視を停止してください。	
111	レジストリアクセス(xxx)でエラーが発生しました。	
112	ヘルパー(%s)でエラーが発生しました。	xxx にヘルパーからのエラーメッセージが入る。
113	ファイル出力でエラーが発生しました。:%s	
114	ファイル読込でエラーが発生しました。:%s	
115	ファイルチェックエラーが発生しました。:%s	
116	対応していないバージョンの BOM です。:%s	IMPORT 時のマニフェストチェックで、 エラーになった場合。 マニフェストファイルが無い場合。 ファイルが壊れている場合。 バージョンが違う場合等
901	内部処理でエラーが発生しました。:%s	

13 .8 MxSysConf.exe のエラーコード表

エラーコード	エラーメッセージ	説明
5000	OpenSCManager エラー。	SCM エラー
5005	CreateMutex エラー。(%1)	CreateMutex エラー
5010	BOM マネージャーを閉じてください。	バックアップ、リストア時に BOM マネージャーが 起動している場合
5011	このプログラムはすでに起動されています。	多重起動チェック
5012	%1 処理が中止されました。	管理者モードが接続されている場合

エラーコード	エラーメッセージ	説明
5020	モジュールを初期化できません(%1)。	Bom7Helper.dll 初期化確認
5021	インストールディレクトリが見つかりません。 (%1)	インストールディレクトリのチェック （HKEY_LOCAL_MACHINE ¥¥SOFTWARE¥¥SAY Technologies ¥¥BOMW7¥¥InstallDir）
		BIN ディレクトリのチェック （HKEY_LOCAL_MACHINE ¥¥SOFTWARE¥¥SAY Technologies ¥¥BOMW7¥¥BinDir）
5023	ファイルパスが正しくありません。	書庫解凍時エラー （-file に指定したディレクトリが存在しない）
5024	このファイルはバックアップファイルではありません。	バックアップファイル以外だった場合
5025		環境データをワークディレクトリにコピー時
		インスタンスデータをワークディレクトリにコピー時
		MANIFEST.MF 作成時
		INSTANCE.MF 作成時
		ワークディレクトリを圧縮時
		ワークディレクトリに解凍時
5026	%1 上記のファイル名は無効です。	-file オプションのファイル名に使用不可文字 『> < ? : / * | "』いずれかの文字が含まれる場合。 または 5 文字未満の場合。
5027	指定したログ出力先のフォルダーは存在しません。	-log オプションで存在しないフォルダーを指定した 場合
5100	―	AtatchConsole 関数は WindowsXP 以降でない OS に非対応の為本コマンドを実施しない。
5104	バックアップファイルが指定されていません。	パラメーターエラー（-file の指定がない）
5105	インスタンスの列挙に失敗しました。	インスタンス Enum 取得エラー
5107	バックアップファイル名とログファイル名が 同じファイルになっています。 異なるファイルにしてください。	file と log の出力先＋ファイル名が同じ場合
5108	リストアに失敗しました。 バックアップファイルが不正です。	バックアップファイルが不正（MANIFEST.MF と INSTANCE.MF が両方存在しない）
5109	拡張子が間違っています。	ファイル拡張子不一致 （ログを含めない場合は CAB、ログを含める場合は ZIP を指定する必要がある。）

エラーコード	エラーメッセージ	説明
5110	バックアップファイルのバージョンと BOM の バージョンが異なっています。	バックアップファイルのバージョン （MANIFEST.MF の MajorVersion）とリストア先の BOM の MajorVersion が異なる場合
5111	SMTP の設定ファイルがありません。 (%1)	バックアップでパスワードを消去しようとした場合に SMTP.xml が存在しない場合
-2147024882	この操作を完了するのに十分な記憶域が ありません	Windows エラーコード コネクト作成時のエラー（メモリ不足時）
GetLastError 値	GetLastError メッセージ	バックアップ Execute 時その他エラー

13 .9 エラーメッセージが特殊なもの

●プロセッサ監視

インスタンスが取得できない。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●メモリ監視

Available Bytes の値が取得できない。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●ディスクアクセス監視

インスタンスが取得できない。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●ネットワークインターフェイス監視

インスタンスが取得できない。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●イベントログ監視（除外指定）

ログファイルタイプや種類など、既定の情報がリセットされる。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●イベントログ監視（選択指定）

ログファイルタイプや種類など、既定の情報がリセットされる。

“ネットワークパスがみつかりません。”のエラーメッセージが出力される。

●ディスク容量監視

ディスク一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

●フォルダー・ファイル監視

[参照]ボタンをクリックした際に、ディスク情報一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

●サービス監視

[参照]ボタンをクリックした際に、サービス一覧が取得できない。

“RPC サーバーを利用できません。”のエラーメッセージが出力される。

●プロセス監視

プロセス一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

●パフォーマンスカウンター監視

パフォーマンスオブジェクト一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

●テキストログ監視

[参照]ボタンをクリックした際に、ディスク情報一覧が取得できない。

“ネットワークパスが見つかりません。”のエラーメッセージが出力される。

●AWS S3 ストレージ容量監視 AWS S3 ファイル送信アクション

.NET Framework 3.5.1 SP1 で TLS1.2 が使用できない。（.NET Framework 3.5.1 SP1 のアップデートが適用されていない）

“要求されたセキュリティ プロトコルは、サポートされていません。”のエラーメッセージが出力される。

●AWS S3 ファイル送信アクション

.NET Framework 3.5.1 SP1 で TLS1.2 が使用できない。（.NET Framework 3.5.1 SP1 のアップデートが適用されていない）

“要求されたセキュリティ プロトコルは、サポートされていません。”のエラーメッセージが出力される。

第14章 Microsoft .NET Framework Ver.3.5 SP1 のインストール

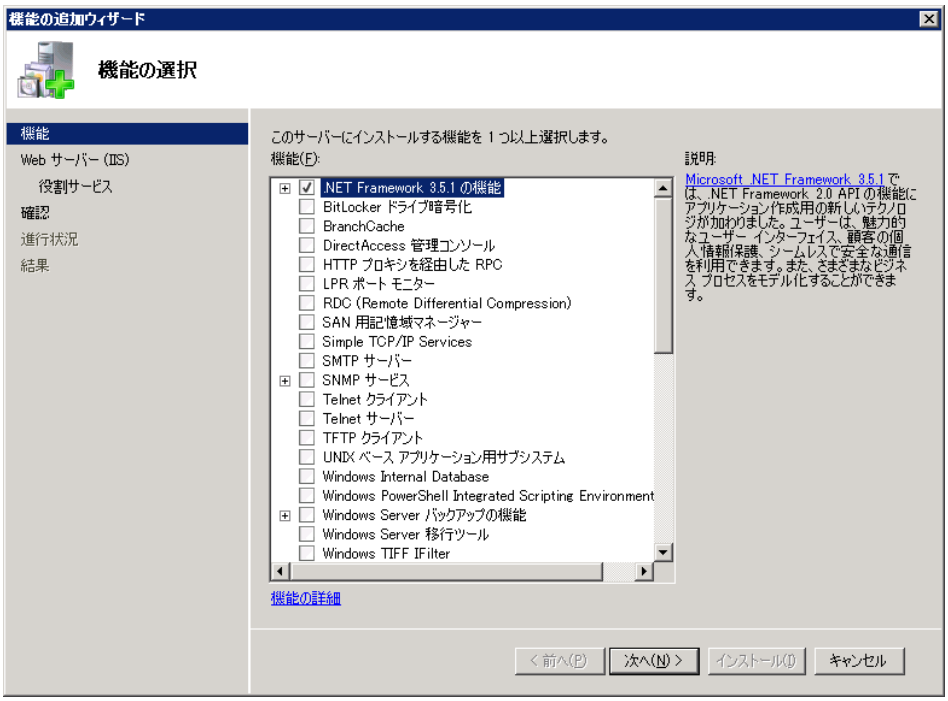
監視項目“AWS S3 ストレージ容量監視”(‘5 .10 .21 AWS S3 ストレージ容量監視’参照)および、アクション項目“AWS S3 ファイル送信アクション”(‘7 .7 .12 AWS S3 ファイル送信’参照)を使用する際は、事前に Microsoft .NET Framework Ver.3.5 SP1 をインストールする必要があります。

Microsoft .NET Framework Ver.3.5 SP1 がインストールされていない場合は、以下の作業を実施してください。

A. Windows Server 2008 R2 の場合

1. [スタート]ボタンより“管理ツール”、さらに“サーバー マネージャー”を選択します。
2. “機能”をクリックし、さらに“機能の追加”をクリックします。
3. 画面の左上より“Windows の機能の有効化または無効化”をクリックします。
4. “機能の追加ウィザード”にて表示された一覧の中から“.NET Framework 3.5.1 の機能”選択しインストールします。

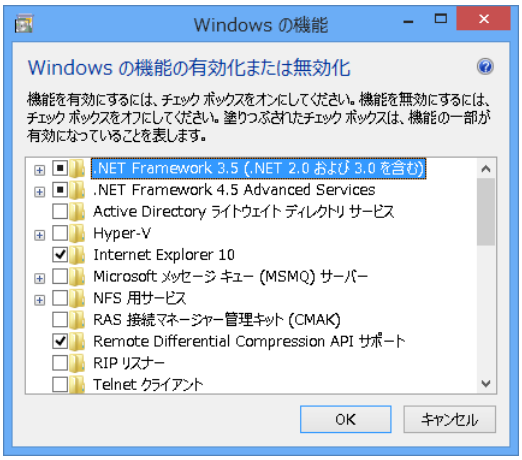
   ※ “Microsoft .NET Framework 3.5.1”と表記されています。



B. Windows 7/8.1/10 の場合

1. スタート画面の“すべてのアプリ”より、“コントロール パネル”を選択します。
2. カテゴリ“プログラム”の“プログラムの取得”をクリックします。コントロールパネルがクラシック表示の場合には、“プログラムと機能”をクリックします。
3. 画面の左上より“Windows の機能の有効化または無効化”をクリックします。
4. 表示された一覧の中から“.NET Framework 3.5(.NET 2.0 および 3.0 を含む)”選択し[OK]ボタンをクリックします。

   ※ Windows 7/8.1/10 では SP1 の表記がありません。

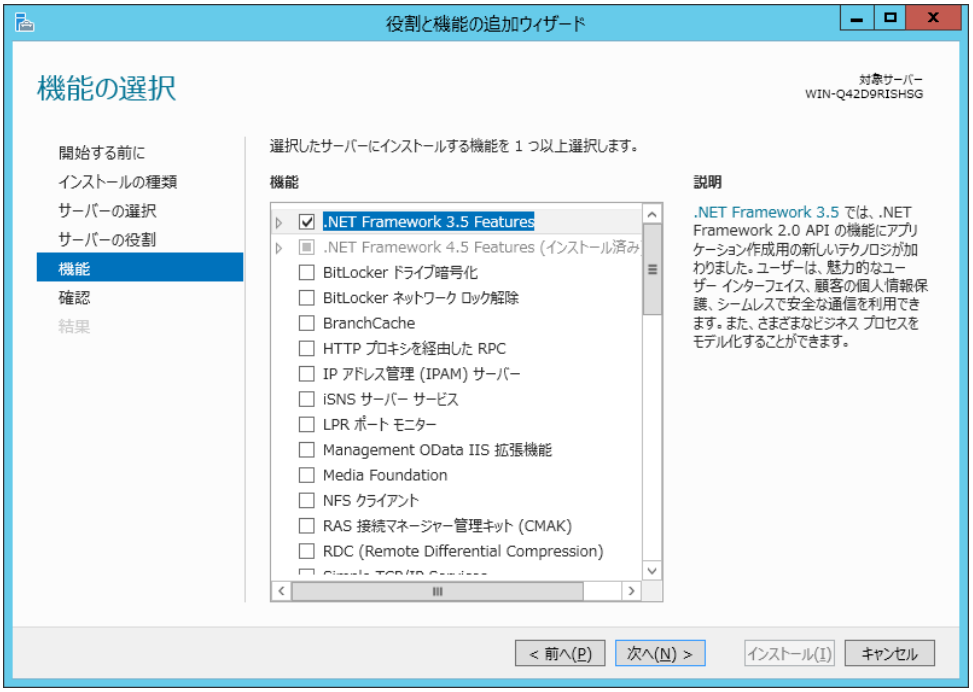


※　Windows 7 では“Microsoft .NET Framework 3.5.1”と表記されています。

C. Windows Server 2012/2012 R2/2016/2019

1. スタート画面より、“サーバー　マネージャー”を選択します。
2. カテゴリ“プログラム”の“役割と機能の追加”をクリックします。
3. “役割と機能の追加ウィザード”を“機能”まで進めます。
4. 表示された一覧の中から“.NET Framework 3.5 Features”選択しインストールします。

※　Windows Server 2012/2012 R2/2016/2019 では SP1 の表記がありません。



第15章 予約済み変数

BOM 7.0 では以下の予約済み変数を定義しており、アクション項目や通知項目でこの予約済み変数を設定すると、実行時には実際の値に展開されます。

予約済み変数		説明
$(TargetComputer)		監視対象コンピューター
$(TargetObject)		監視対象オブジェクト
$(CurrentTime)		現在時刻
$(ElapsedTime)		直近の監視サービス開始からの経過時間［ミリ秒］
$(InstallDir)		BOM for Windows のインストールフォルダー 既定導入時：“C:¥Program Files¥SAY Technologies¥BOMW7”
$(InstanceID)		インスタンス ID
$(InstanceName)		インスタンス名
$(GroupID)		グループ ID
$(GroupName)		グループ名
$(MonitorID)		監視項目 ID
$(MonitorName)		監視項目名
$(ActionID)		アクション項目 ID
$(ActionName)		アクション項目名
$(Runtime)		監視サービスにより、監視またはアクションが実行された時刻
$(Duration)		監視またはアクションの実行に要した時間［秒］
$(ResultCode)		監視またはアクションの実行結果を示す値
$(Value)		監視値
$(Status)		監視ステータス：(正常/注意/危険/失敗)
$(DetectedDataDir)		検出されたデータの出力先フォルダー $(InstallDir)¥Environment¥Instance¥$(InstanceID)¥DetectedData
$(ExitCode)	※1	アクション終了コード
$(Result)	※1	アクション実行結果：(成功/エラー/失敗)
$(ThresholdY)	※2	注意のしきい値
$(ThresholdR)	※2	危険のしきい値

※1 “$(ExitCode)”および“$(Result)”は通知項目のみで使用でき、アクション項目では使用できません。

※2 “$(ThresholdY)”および“$(ThresholdR)”は BOM マネージャー上の予約済み変数の一覧に表示されません。
これらの変数を使用する場合は文字列を手入力してください。
また VMware オプション 7.0 の「VMware ハードウェアステータス監視」を対象とするアクション項目、通知項目では、これらの変数で正しい値が表示されないため使用できません。

第16章 ライセンス表記

BOM 7.0 はそれぞれのライセンス形態に従ってオープンソースソフトウェアを利用しています。
各ソフトウェアを開発された開発者、および開発コミュニティの皆様に深く感謝いたします。

各ソフトウェアを開発された開発者、および開発コミュニティにより、同梱が定められているオープンソースのライセンス条文については、
<BOM 7.0 インストールフォルダー>¥BOMW7¥Common¥Licenses フォルダーに格納されていますのでご参照ください。

BOM 7.0 で使用している代表的なオープンソースソフトウェアの一例

- Apache Tomcat
- Apache License, Version 2.0
- ATL-Server
- Boost
- gSOAP
- Go
- NETSNMP
- OpenSSL
- picojson
- pugixml
- PuTTY
- SQLite
- WTL
- ZIP32

BOM for Windows Ver.7.0

ユーザーズ マニュアル

2017 年 1 月 1 日　初版
2020 年 4 月 28 日　改訂版

著者　　セイ・テクノロジーズ株式会社
発行者　セイ・テクノロジーズ株式会社
発行　　セイ・テクノロジーズ株式会社
バージョン　Ver.7.0.30.0