



**BOM for Windows Ver.8.0**

**集中監視コンソール**

**ユーザーズマニュアル**

---

## 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

本書のいかなる部分も、セイ・テクノロジーズ株式会社からの文書による事前の許可なしには、形態または手段を問わず決して複製・配布してはなりません。

## 商標

本ユーザーズマニュアルに記載されている「BOM」はセイ・テクノロジーズ株式会社の登録商標です。また、本文中の社名、製品名、サービス名等は各社の商標または登録商標である場合があります。

なお、本文および図表中では、「TM」（Trademark）、「(R）」（Registered Trademark）は明記しておりません。

---

## 目次

### 本書について

製品表記

使用方法

環境説明

### 第1章 BOM 集中監視コンソール

#### 1. BOM 集中監視コンソールの解説

- (1) グループ
- (2) インスタンス
- (3) アクション機能
- (4) ログ

#### 2. BOM 集中監視コンソールの構成

#### 3. 動作条件

- (1) 集中監視 Web サービス
  - A. コンピューターのスペック
  - B. 登録インスタンス数
- (2) BOM 集中監視コンソール
  - A. コンピューターのスペック
  - B. 表示検証ブラウザ

#### 4. インスタンスポーリング

- (1) インスタンスのポーリングを適用したい場合
- (2) グループのポーリング設定を適用したい場合

#### 5. BOM 集中監視コンソールのインストール

- (1) 追加インストール
- (2) 新規インストール
- (3) ポート番号の変更
- (4) サーバー証明書の設定

#### 6. BOM 集中監視コンソールへのログイン

- (1) BOM 集中監視コンソールへのログイン方法

#### 7. BOM 集中監視コンソールからのログアウト

#### 8. BOM 集中監視コンソールの表示

- (1) インスタンスのステータス表示
- (2) グループの表示
  - A. グループのアドレスバーを利用
  - B. ツリービューを利用
- (3) 全インスタンスステータスの確認および全インスタンス情報取得機能
- (4) 表示の更新
  - A. 自動更新
  - B. 手動更新
- (5) 表示枠のサイズ変更
- (6) ツリービュー表示
  - A. 「グループ」タブ
  - B. 「ステータス」タブ

- (7) 詳細ビュー表示
  - A. 「サマリー」タブ
  - B. 「アクション一覧」タブ
  - C. 「ステータス」タブ
  - D. 「ステータスログ」タブ
  - E. 「履歴ログ」タブ
  - F. 「アクションログ」タブ
  - G. 「受信ログ」タブ
- 9. BOM 集中監視コンソールの設定
  - (1) グループの設定
    - A. グループの追加
    - B. グループの編集
    - C. グループの削除
  - (2) インスタンスの設定-インスタンスの編集画面
    - A. インスタンスの追加
    - B. インスタンスの編集
    - C. インスタンスの削除
  - (3) インスタンス設定-インスタンス情報収集
  - (4) アクションの設定
    - A. アクションの追加-共通設定
    - B. アクションの追加-メール送信
    - C. アクションの追加-カスタムアクション
    - D. アクションの編集
    - E. アクションの削除
- 10. BOM 集中監視コンソールでのメール受信
  - (1) メール受信設定新規
  - (2) メール受信設定変更
  - (3) 自己署名証明書の設定
    - A. 自己署名証明書の取得について
    - B. 自己署名証明書の設定について
- 11. BOM 集中監視コンソールのログ
  - (1) ステータスログ
  - (2) 履歴ログ
  - (3) アクションログ
  - (4) 受信ログ
  - (5) システムログ
  - (6) サマリーログビュー
  - (7) ログファイル出力
- 12. 設定のエクスポート/インポート
  - (1) 集中監視 Web サーバーの設定をエクスポート
  - (2) インポート
- 13. ユーザー管理
  - (1) ユーザーの追加
  - (2) ユーザーの変更
  - (3) ユーザーの削除

#### 14. ライセンスチェック

#### 15. BOM 集中監視コンソールの環境設定変更

- (1) Administratorロールで変更できる設定内容
  - A. メンテナンス設定（ログイン時のみ有効）
  - B. ユーザー設定（再ログイン後有効）
  - C. システム設定（サービス再起動後有効）
- (2) read onlyロールで変更できる設定内容
  - A. メンテナンス設定（ログイン時のみ有効）
  - B. ユーザー設定（再ログイン後有効）

#### 16. 集中監視Webサービスおよび集中監視コンソール使用時の注意点

- (1) 集中監視 Web サービス使用時の注意点
- (2) 集中監視コンソール使用時の注意点

### 第2章 集中監視 Web サービス ポーリング スケジュール設定

#### 1. 集中監視コンソールのユーザー追加

#### 2. ポーリング設定

- (1) スケジュールを集中監視コンソールのグループ単位で行う場合
- (2) スケジュールを集中監視コンソールのインスタンス単位で行う場合

#### 3. ユーザー情報の暗号化と登録

#### 4. スケジュール設定

### 第3章 トラブルシューティング

---

# 本書について

## 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ます。

正式名称	本マニュアルでの呼称（略称）
BOM for Windows Ver.X.0 BOM for Windows Ver.X.0 SRx	BOM X.0
BOM Linux オプション Ver.X.0 BOM Linux オプション Ver.X.0 SRx	Linux オプション X.0
BOM VMware オプション Ver.X.0 BOM VMware オプション Ver.X.0 SRx	VMware オプション X.0
BOM 8.0 マネージャー	BOM マネージャー
BOM 8.0 集中監視コンソール	BOM 集中監視コンソール
BOM 8.0 監視サービス	BOM 監視サービス
BOM 8.0 コントロールパネル	BOM コントロールパネル
BOM 8.0 ヘルパーサービス	BOM ヘルパーサービス
Windows 10、Windows 11	Windows クライアント OS

※ 上記の"X"および"x"にはバージョン番号、SRバージョンの数字が入ります。通常、マニュアル中ではSRバージョンの表記を省略しますが、特定のSRバージョンを明示する際は末尾に記載します。

## 使用方法

このユーザーズマニュアルには、BOM 集中監視コンソール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。

- BOM 8.0および、BOM 集中監視コンソールのインストールに関しては'BOM for Windows Ver.8.0 インストールマニュアル'を参照してください。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と、BOM 8.0に関する基本的な知識が必要です。
- ユーザーズマニュアルには外部のウェブサイトへの URL が記載されている場合があります。PDF 形式のユーザーズマニュアルでは使用する PDF リーダーによってこの URL が自動的にリンク化される場合がありますが、URL に改行が含まれていると正しいリンク先に遷移できません。このような場合は URL をコピーし、ブラウザーに貼り付けて表示してください。
- 本書に更新・訂正などが生じた際は、弊社ウェブサイト上で情報を公開しますので、あわせて参照してください。

## 環境説明

- 本書では、コンピューターの操作画面として、主にWindows Server 2022および、Microsoft Edgeで取得した画像を使用しています。お使いの環境によって表示内容が若干異なる場合がありますが、適宜読み替えてください。

# 第1章 BOM 集中監視コンソール

## 1. BOM 集中監視コンソールの解説

BOM 集中監視コンソールは、監視を行っているインスタンスの監視ステータスを収集し、対象コンピューターあるいは対象インスタンスの状態をステータスアイコンで表示します。また、収集したステータスの変化に応じて、メールによる通知やカスタムアクションによる任意のバッチファイルの実行といったアクションをBOM 集中監視コンソールより設定しておくことができます。

- BOM 集中監視コンソールは、ブラウザで状況の確認やアクションなどの設定作業を行うことができます。
- 既定値では、2分間で画面の表示が自動更新されるように設定がされています。
- BOM 集中監視コンソール画面は大きく分けて、画面左上のツリービュー、画面右上の詳細ビュー、画面下部のサマリーログビューに大別することができます。
  - ブラウザーの[戻る]、[進む]ボタンは使用せず、集中監視コンソール上の[戻る]を利用してください。
- インスタンスは文字コード（ASCII）に従い表示されます。
  - 大文字小文字は区別しません。

編集	表示名	ステータス	前回実行時刻	ポーリング
編集	DC		--	5分間隔
編集	情報システム部		--	5分間隔
編集	AP-01		2022/03/10 18:02:00	5分間隔

タイプ	ターゲット	日時	カテゴリ	サマリー
情報	DB-06	2022/03/10 18:02:05	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)
情報	システム	2022/03/10 18:02:04	システムログ	root[0:0:0:0:0:0:1] インスタンス /root/関東本社/情報シス
情報	DB-02	2022/03/10 18:02:00	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:0)
エラー	AP-03	2022/03/10 18:02:00	ステータスログ	監視サービスが停止中、またはインスタンス情報が取得できませ



## (1) グループ

- グループは階層化させることができ、子グループのステータスのサマリーが、親グループのステータスとして表示されま  
す。
  - グループの作成数やネスト数に制限はありませんが、確認の手間などを考慮しできるだけ簡易な構成を推奨します。
- グループの配下にインスタンスを登録することができ、インスタンスのステータスのサマリーが、グループのステータス  
として表示されます。
- グループに対し、インスタンスのステータスを起動条件としたアクション機能を設定することができます。

## (2) インスタンス

- インスタンスに登録できる対象は、下記のとおりです。
  - ※ 下記条件を満たさないインスタンスは、BOM 8.0 集中監視コンソールから見付けることができません。
  - ※ 各BOMのSRバージョンアップモジュールおよび、適用が必要な各ファイルは、弊社ホームページからダウンロード  
できます。
  - BOM 8.0インスタンス、Linux オプション 8.0インスタンス、VMware オプション 8.0インスタンス
  - 以下、いずれかの条件を満たす、BOM 7.0インスタンス、Linux オプション 7.0インスタンス、VMware オプション  
7.0インスタンス
    - BOM 7.0 SR3以降であること。
    - BOM 7.0 SR2で、「BOM for Windows Ver.7.0 SR2 向けアップデートモジュール (201911) (2019/12/16  
公開)」が適用されていること。
  - 以下の条件を満たす、BOM 6.0インスタンス、Linux オプション 6.0インスタンス、VMware オプション 6.0インス  
タンス
    - BOM 6.0 SR2かつ、「BOM 6.0 SR2 Rollup Package 2019.11.15 (2019/11/27公開)」が適用されているこ  
と。
  - 以下の条件を満たす、BOM 5.0インスタンス、Linux オプション 5.0インスタンス、VMware オプション 5.0インス  
タンス
    - BOM 5.0 SR4かつ、「BOM 5.0 SR4 Rollup Package 2015.03.03 (2015/3/3 公開)」が適用されているこ  
と。

- インスタンスの登録数について

登録数にシステム的な制限はありませんが、1つの集中監視Webサービスあたり50インスタンスまでを推奨値としていま  
す。

ただし、コンピューターのスペックや設定するポーリング間隔などの要因によって快適に利用できる値は大きく上下する  
ため、実環境において動作の確認および登録インスタンス数調整の実施をお勧めします。

### (3) アクション機能

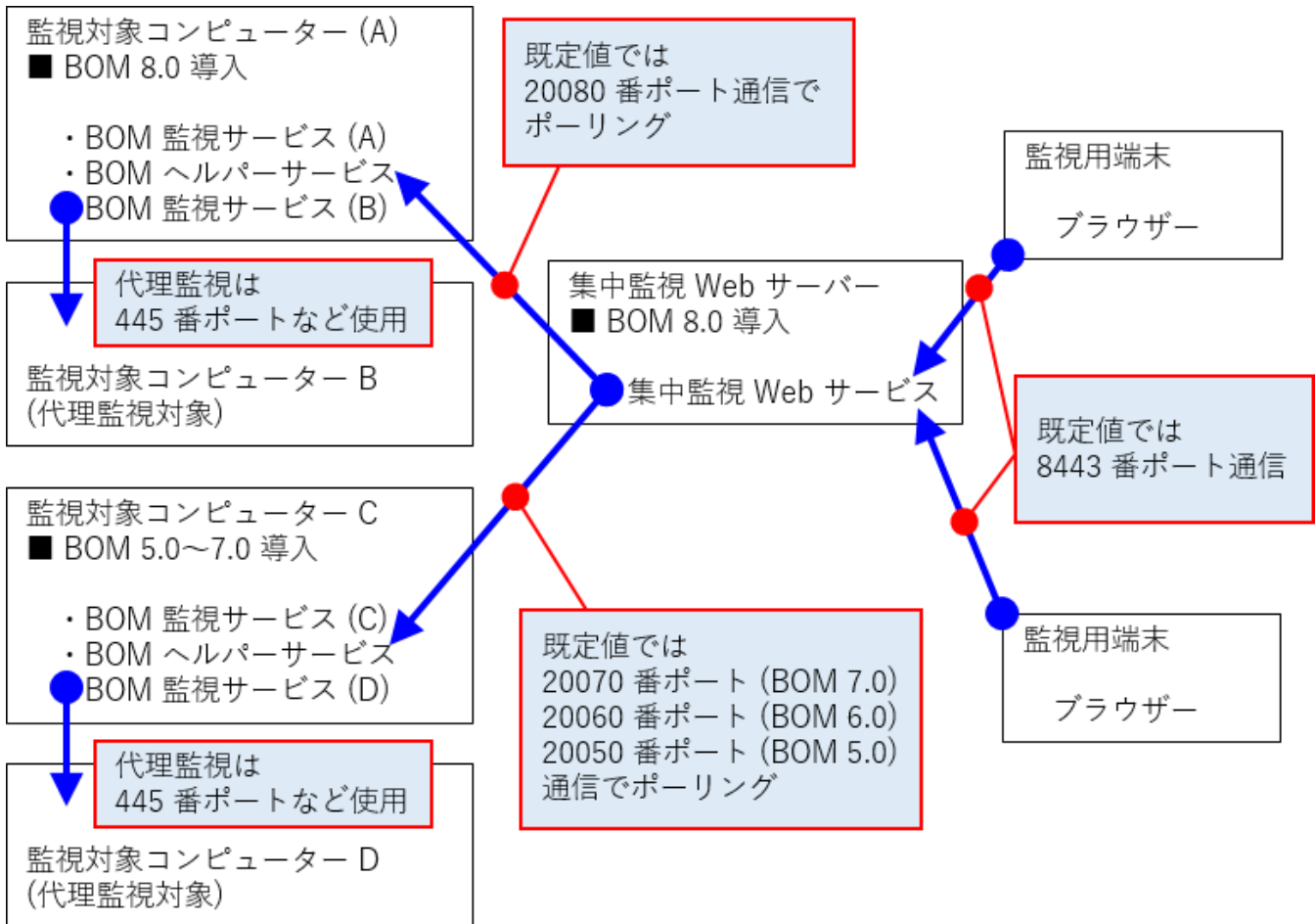
- グループのステータス変化に応じて、下記のアクションを起動することができます。
  - メール送信
  - カスタムアクション
- アクションは特定のグループに関連付けができます。
- グループが階層関係にある場合、親グループに設定したアクションは、子グループに適用されません。
- 登録できるアクション数に制限はありません。
- アクションの実行には、10分のタイムアウト時間が固定値として設定されています  
実行したアクションが10分以内に応答を返却しない場合、アクションは強制終了となりアクションにより起動されたプロセスも強制終了されます。その際には、'[ログ](#)'のアクションログに、タイムアウトのログが記録されます。

### (4) ログ

- BOM 集中監視コンソールでは、下記のログを照会することができます。ステータスやログを収集するポーリング間隔は、グループもしくはインスタンス単位で設定することができます。
  - ステータスログ  
BOM 集中監視コンソールに登録したインスタンスのステータス情報に関する監視サービスの実行状況や、監視結果のサマリー情報を、インスタンスごとに表示させることができます。
  - ヒストリーログ  
BOM 集中監視コンソールに設定したインスタンスのヒストリーログを表示させることができます。ヒストリーログの詳細は、'BOM for Windows Ver.8.0 ユーザーズマニュアル'を参照してください。
  - アクションログ  
BOM 集中監視コンソールに設定したアクションの実行結果を表示させることができます。
  - サマリーログ  
BOM 集中監視コンソールが出力している直近30分以内の"ステータスログ"、"システムログ"、"アクションログ"のすべてをサマリーログとして表示させることができます。  
直近の表示期間はBOM 集中監視コンソールの環境設定より変更することができます。
- 上記の各ログは、昇順/降順による並び替えや、キーワードによる部分一致で絞り込み検索を行うことができます。
- "ステータスログ"、"ヒストリーログ"、"アクションログ"はログファイル出力機能によりCSV形式でダウンロードすることができます。

## 2. BOM 集中監視コンソールの構成

BOM 5.0～8.0の監視データは、BOMヘルパーサービスのTCP/IP経由で集中監視Webサービスに蓄積させます。管理者の方は、管理用端末から集中監視Webサービスにブラウザで接続することで、BOM 集中監視コンソールを利用することができます。これらを図式化すると下記のとおりです。



- BOM 集中監視コンソールを利用するにあたっては、上記に該当するそれぞれのTCP/IP通信ができることが条件となります。
- 上記では監視対象コンピューターAから監視対象コンピューターBおよび、CからDを代理監視していますが、監視対象コンピューターBおよびDの監視データは、監視対象コンピューターAおよびCから集中監視用 Webサーバーに通信されます。
- 監視対象コンピューター/集中監視Webサーバー/監視用端末は、すべてを1台のコンピューターに同居させることもできます。
- BOM 5.0～8.0で、BOMヘルパーサービスが利用する既定のポート番号が異なることに注意してください。
- 通信に用いるそれぞれのポート番号は、BOMコントロールパネルより変更することができます。BOMヘルパーサービスのポート番号の変更手順については、'BOM for Windows Ver.8.0 ユーザーズマニュアル'を参照してください。また、集中監視Webサービスのポート番号の変更手順は、'[ポート番号の変更](#)'および'BOM for Windows Ver.8.0 ユーザーズマニュアル'を参照してください。
- 集中監視 Web サービスが、BOM ヘルパーサービスよりインスタンスのステータスを取得することを"ポーリング"と呼びますが、BOMヘルパーサービスの"リモートアクセスの範囲"の既定値は"同じローカルセグメント"です（BOM コントロールパネルより設定可能）。異なるセグメント間で運用を行う際の"リモートアクセスの範囲"の変更手順は'BOM for Windows Ver.8.0 ユーザーズマニュアル'を参照してください。

- 代理監視に用いるポートの詳細は、'BOM for Windows Ver.8.0 ユーザーズマニュアル'で「代理監視設定のポイント」を参照してください。

### 3. 動作条件

BOM 集中監視コンソールを快適に利用するための、集中監視WebサービスとBOM 集中監視コンソールの動作条件は下記のとおりです。

#### (1) 集中監視 Web サービス

集中監視 Web サービスの動作条件は下記のとおりです。

##### A. コンピューターのスペック

対象	最低条件
CPU	BOM for Windows Ver.8.0 SR1 の動作環境に準拠
メモリ	搭載量：Windows OSのハードウェア要件に準拠 空き容量：512MB 以上
LAN	BOM for Windows Ver.8.0 SR1 の動作環境に準拠
ストレージ	インストール時：200MBの空き容量 運用時：500MBの空き容量 1 インスタンスあたり：200MB程度の空き容量 ※ 集中監視デフォルト設定（ポーリング5分、ログ保持期間30日）
OS	BOM for Windows Ver.8.0 SR1 の動作環境に準拠

- BOM 8.0 の動作環境については、'BOM for Windows Ver.8.0 インストールマニュアル' で「BOM のシステム要件」を参照してください。
- Windows クライアント OSにはセッション数の上限があり、セッション数の上限を超えてブラウザから集中監視Web サービスに接続を試みた場合、超過分は接続に失敗します。

##### B. 登録インスタンス数

登録インスタンス数にシステム的な制限はありませんが、1つの集中監視Webサービスあたり50インスタンスまでを推奨値としています。

ただし、コンピューターのスペックや設定するポーリング間隔などの要因によって快適に利用できる値は大きく上下するため、実環境において動作の確認および登録インスタンス数の調整を実施してください。

利用環境に見合わないインスタンス数が登録された場合、インスタンス情報の取得が遅延することがあります。

#### (2) BOM 集中監視コンソール

BOM 集中監視コンソールの動作条件は下記のとおりです。

## A. コンピューターのスペック

対象	最低条件
CPU	各ブラウザの動作環境に準拠
メモリ	各ブラウザの動作環境に準拠
ディスク容量	各ブラウザの動作環境に準拠
ディスプレイ	BOM for Windows Ver.8.0 SR1 の動作環境に準拠
ネットワークインターフェース	BOM for Windows Ver.8.0 SR1 の動作環境に準拠

- BOM 8.0 の動作環境については、'BOM for Windows Ver.8.0 インストールマニュアル' で「BOM のシステム要件」を参照してください。

## B. 表示検証ブラウザ

下記のブラウザとバージョンで、BOM 集中監視コンソールの表示検証をしています。

- 接続の際はTLSv1.2を有効化する必要があります。
- BOM 集中監視コンソールを継続して快適に利用するため、定期的にブラウザを閉じてWebブラウザの使用メモリ増加を防止する必要があります。

ブラウザ名	バージョン
Internet Explorer	11にて表示検証
Microsoft Edge (Chromium ベース)	バージョン 116.0.1938.62 (公式ビルド) (64 ビット) にて表示検証
Google Chrome	バージョン: 116.0.5845.140 (Official Build) (64 ビット) にて表示検証

BOM 集中監視コンソールを下記に該当する環境で使用する場合、画面レイアウトが崩れることがあります。

- ツールバーを表示させたまま、BOM 集中監視コンソールを使用する。
- プラグインを使用した状態で、BOM 集中監視コンソールを使用する。
- ウィンドウのサイズを極端に小さくした状態で、BOM 集中監視コンソールを使用する。

## 4. インスタンスポーリング

インスタンスのステータスは、BOM ヘルパーサービスと集中監視 Web サービス間の通信で収集します。このステータスの収集を"ポーリング"と呼び、グループもしくはインスタンス単位で"ポーリング"の"有効"/"無効"と、"ポーリング"の"間隔"を設定することができます。

- インスタンスの編集（インスタンスの作成/削除、ポーリング設定の変更）を行うと、そのインスタンスは即時ポーリングを行います。
- グループの編集（グループの作成/削除、ポーリング設定の変更）を行うと、そのグループ直下のインスタンスすべてが即時ポーリングを行います。

### (1) インスタンスのポーリングを適用したい場合

インスタンスの設定で、"個別のポーリング設定を行う"ラジオボタンを選択します。

### (2) グループのポーリング設定を適用したい場合

インスタンスの設定で、"グループの設定に従う"ラジオボタンを選択すると、グループに所属するインスタンスはすべてグループのポーリング設定を基準とします。

※ グループが階層構造の場合、自身の"有効"/"無効"設定を適用します。

## 5. BOM 集中監視コンソールのインストール

BOM 集中監視コンソールに表示する監視ステータスを収集するために、集中監視Webサービスをインストールする必要があります。

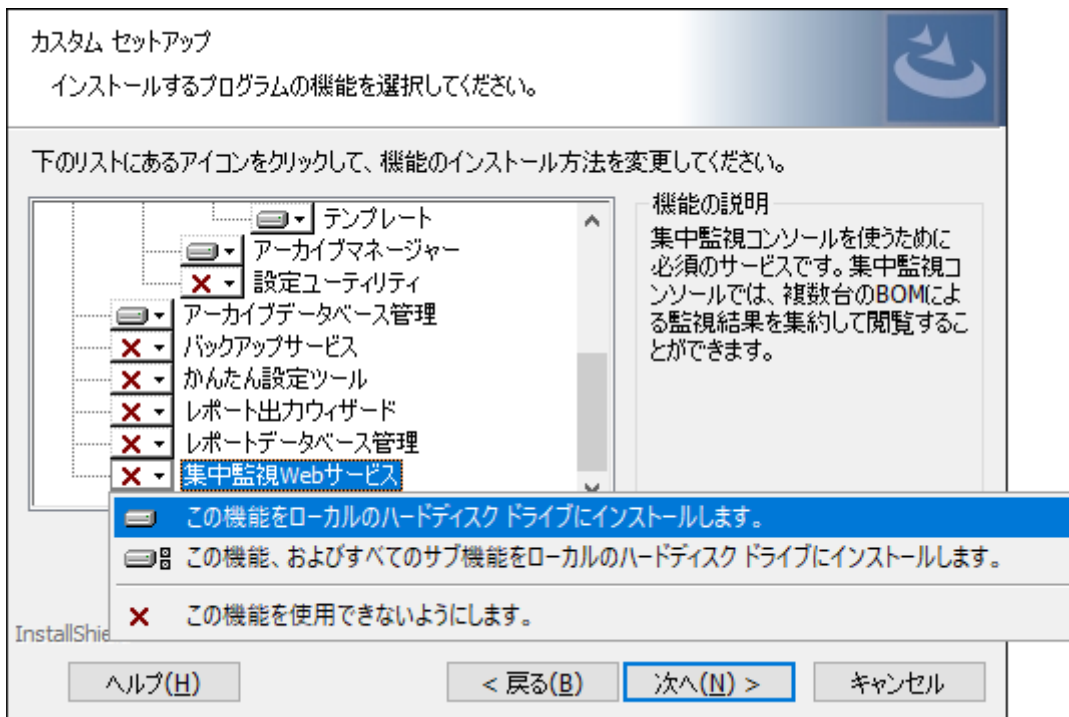
本項では、集中監視 Web サービスのインストールについてご説明します。

- インストール時に"すべて"を選択した場合と、"カスタム"で集中監視 Web サービスを選択してインストールした場合には、すでに集中監視 Web サービスがインストールされているので以下の操作は必要ありません。
- BOM 集中監視コンソールが必要とする、Apache Tomcat、Adoptium OpenJDKなどのモジュールや環境は、集中監視 Web サービスのインストールと同時にインストールされます。

### (1) 追加インストール

この項では、すでにBOM 8.0コンポーネントがインストール済みの環境に、集中監視 Web サービスを追加インストールする手順を説明します。

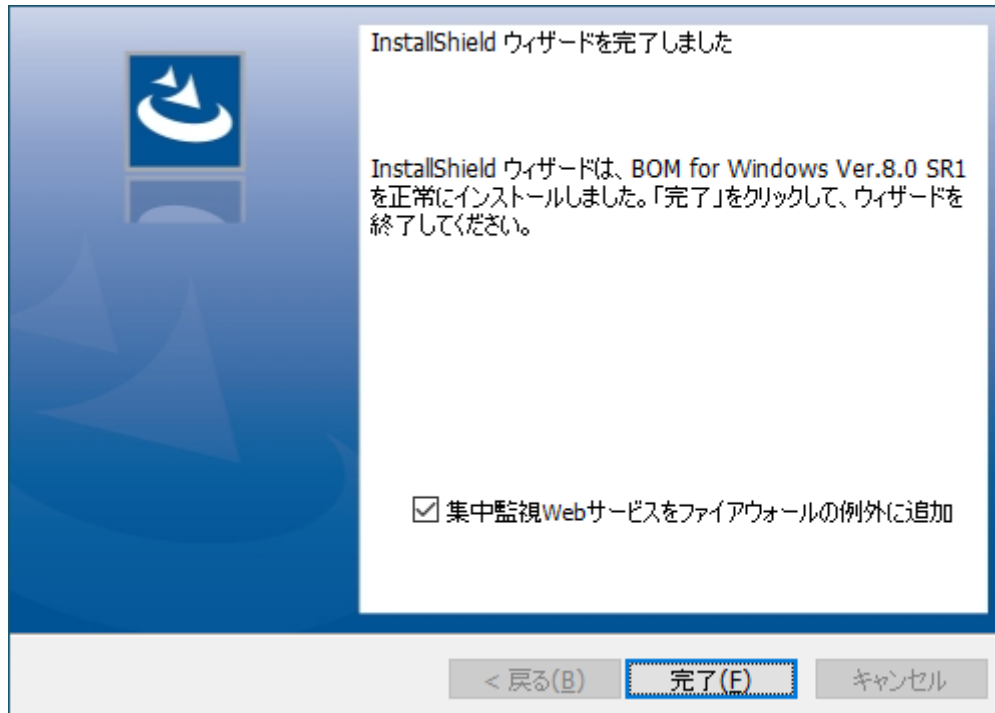
- BOM 8.0のインストールパッケージに格納されている"autorun.hta"を実行し、インストールランチャーを起動します。
- メニューから"集中監視コンソール"のリンクをクリックし、セットアップウィザードを起動します。
- "プログラムの保守"画面まで進め、"変更"ラジオボタンが有効になっていることを確認して[次へ]ボタンをクリックします。
- "カスタムセットアップ"画面で"集中監視Webサービス"のアイコンをクリックし、"この機能をローカルのハードディスクドライブにインストールします。"を選択して、[次へ]ボタンをクリックします。



- 以降はセットアップウィザードに従い、"集中監視Webサービス"のインストールを完了させます。



Windows機能のファイアウォールが実行されている場合には、"集中監視Webサービスをファイアウォールの例外に追加"チェックボックスのチェックを外さないでください。

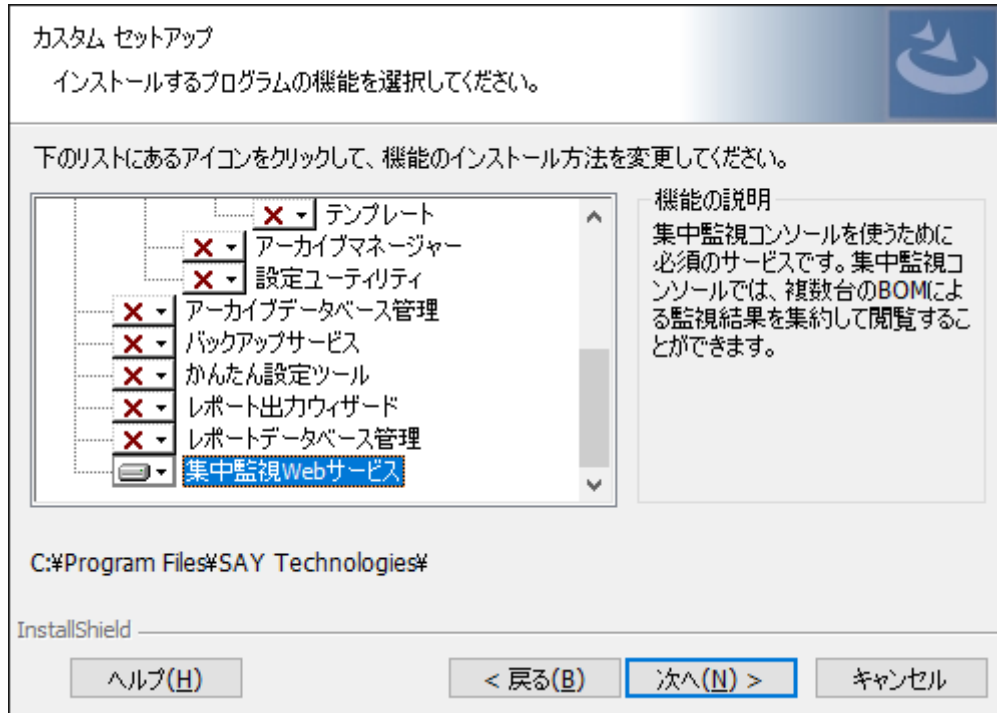


## (2) 新規インストール

この項では、集中監視Webサービスを単独でインストールする手順を説明します。

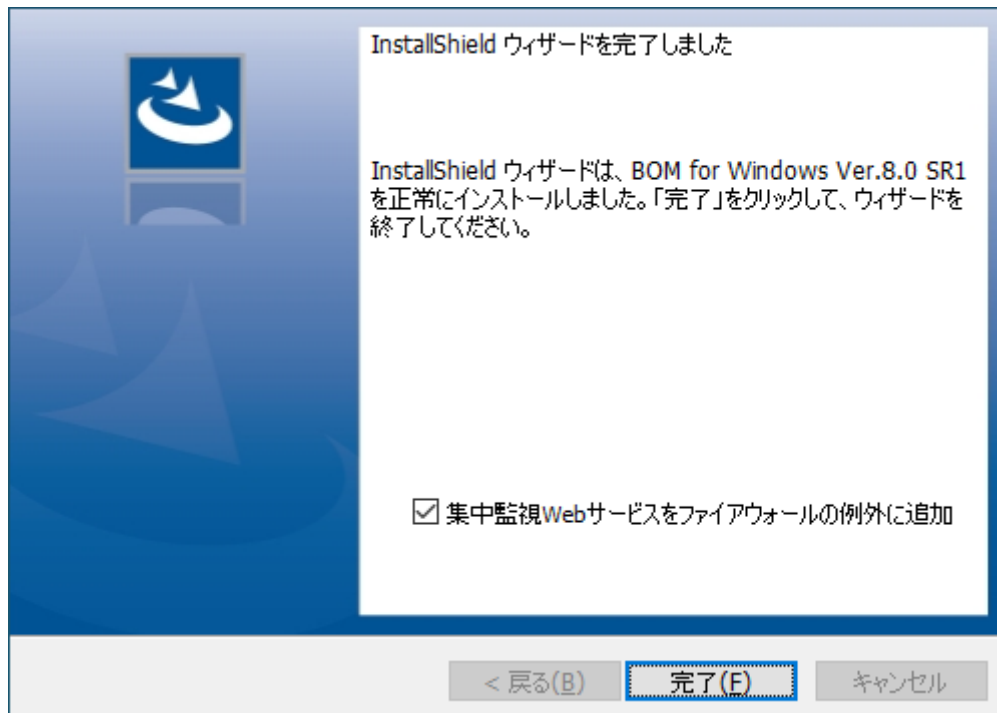
- 集中監視Webサービスの運用にBOM 8.0のライセンスは必要ありません。
1. BOM 8.0のインストールパッケージに格納されている"autorun.hta"を実行し、インストールランチャーを起動します。
  2. メニューから"集中監視コンソール"のリンクをクリックし、セットアップウィザードを起動します。
  3. "セットアップタイプ"画面まで進め、"標準"または"カスタム"を選択して[次へ]ボタンをクリックします。

4. "カスタム"を選択した場合は、"集中監視Webサービス"がインストール対象となっている（ハードディスクアイコンになっている）ことを確認し、必要に応じて他の機能の追加やインストール先の変更をおこなって、[次へ]ボタンをクリックします。



5. 以降はセットアップウィザードに従い、"集中監視Webサービス"のインストールを完了させます。

Windows機能のファイアウォールが実行されている場合には、"集中監視Webサービスをファイアウォールの例外に追加"チェックボックスのチェックを外さないでください。



### (3) ポート番号の変更

集中監視Webサービスとブラウザ間で使用するポート番号は既定値で「8443」に設定されていますが、この番号はBOMコントロールパネルより以下の手順で変更できます。

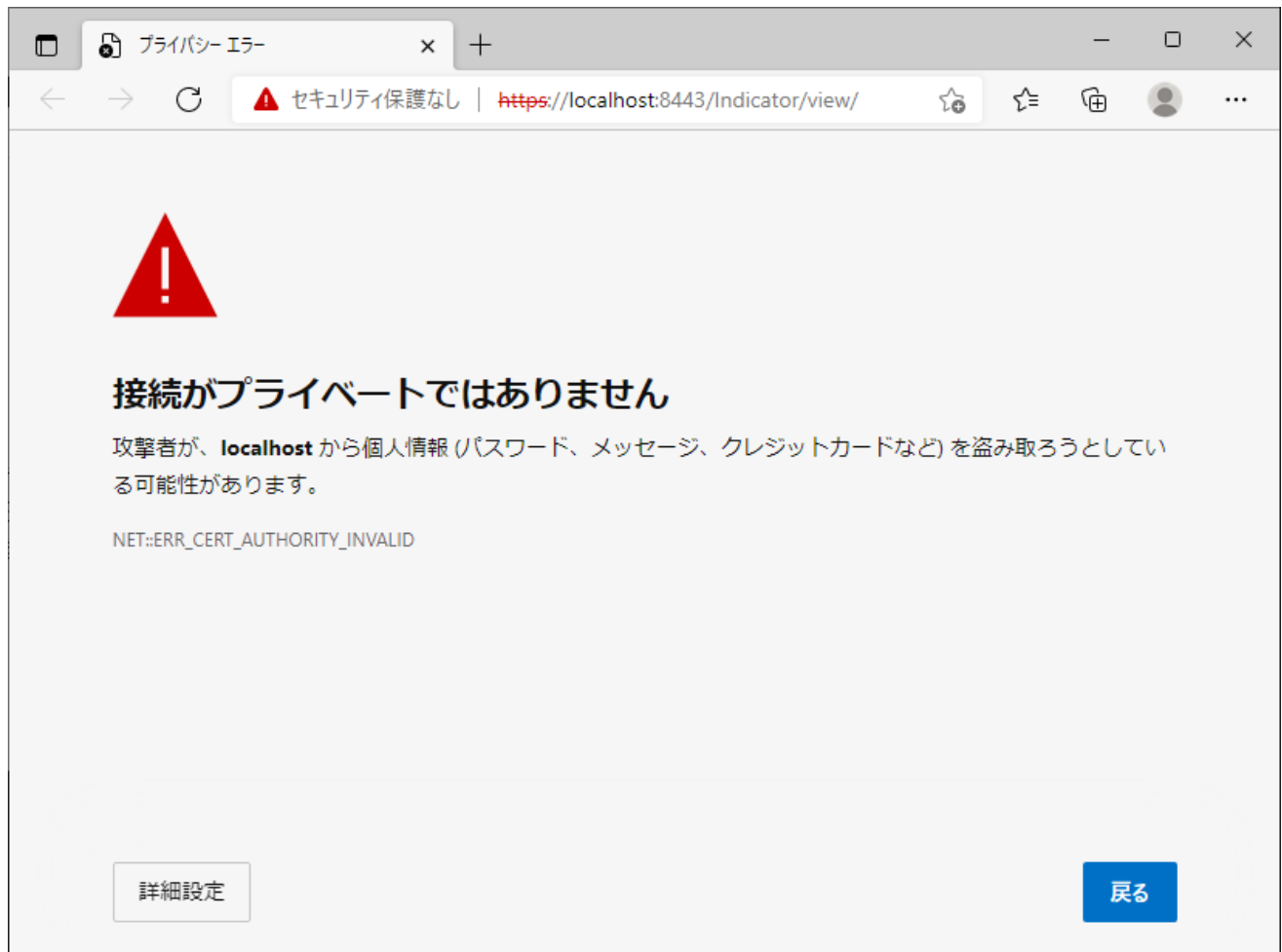
※ Apache Tomcatが内部的に使用するポートは変更できません。他のアプリケーションが使用するApache Tomcatとの共存が必要な場合は、他のアプリケーション側でポート番号を変更してください。他のアプリケーション側でもポート変更ができない場合は、集中監視Webサービスと他のアプリケーションとを、それぞれ別のコンピューターにインストールしてください。

1. Windowsのスタートメニューから、BOM 8.0 コントロールパネルを起動します。
2. 「BOMコントロールパネル」 → 「集中監視Webサービス」 タブを選択します。
3. 集中監視Webサービスが実行中の場合は、「停止」 ボタンをクリックしてサービスを停止します。
4. 「設定」 ボタンをクリックします。
5. 「集中監視Webサービス設定」 の「ポート(P):」 に任意のポート番号を入力し、「OK」 ボタンをクリックします。
6. 「集中監視Webサービス」 タブに戻り、「開始」 ボタンをクリックして集中監視Webサービスを開始します。

## (4) サーバー証明書の設定

BOM 集中監視コンソールは、HTTPSによるSSL（Secure Sockets Layer）を用いており、初期インストール状態ではセキュリティ証明書の警告メッセージが表示されます。

- Microsoft Edgeの表示例



このメッセージは、セキュリティ証明書の発行元が未登録であるために表示される警告メッセージで、詳細設定から「localhost に進む (安全ではありません)」をクリックすると、SSLの暗号化通信技術によるBOM 集中監視コンソールを使用することができます。

※ 上記はMicrosoft Edgeでの例です。使用するブラウザや、そのバージョンにより表示および操作内容は異なります。また、ご利用環境におけるセキュリティポリシー上、この警告メッセージを解消する必要がある場合は、セキュリティポリシーに沿ったセキュリティ証明書の設定を行ってください。

## 6. BOM 集中監視コンソールへのログイン

ローカルコンピューターに集中監視Webサービスがインストールされている場合、下記の設定が有効になります。

- BOM コントロールパネル→「ツール」タブ→[ブラウザを起動...]ボタンをクリックできるようになります。
- Windowsのスタートメニューに、BOM 8.0 集中監視コンソールのショートカットが作成されます。  
実行すると、URLに "https://localhost:8443/Indicator/view/" が指定された状態で、既定のブラウザが起動します。

### (1) BOM 集中監視コンソールへのログイン方法

1. 下記のどれかの手段で、集中監視 Web サービスに接続してBOM 集中監視コンソールを起動することができます。

- BOM 8.0 集中監視コンソールのショートカットより起動する。
- BOM コントロールパネル→「ツール」タブ→[ブラウザを起動...]ボタンをクリックして起動する。
- 任意のブラウザを立ち上げ、アドレスバーに "https://localhost:8443/Indicator/view/" と入力して起動する。

上記URLの"localhost"部分には、集中監視Webサービスをインストールしたコンピューターのホスト名もしくはIPアドレスを指定してください。（使用するセキュリティ証明書に応じて、ホスト名かIPアドレスかを使い分けてください。）

また集中監視 Web サービスのポート番号をBOM コントロールパネルより変更している場合には、上記URLのポート番号"8443"部分を変更したポート番号に置き換えてください。



2. "ユーザー名"と"パスワード"を入力し、[ログイン]ボタンをクリックするとBOM 集中監視コンソールにログインすることができます。

- 同一IPアドレスから同じ日に累計10回ログインに失敗した場合、翌日0時00分まで該当IPアドレスからログインができません。
- 既定値で"ユーザー名"は「root」（半角小文字）、「パスワード」は「Bom8Indicat@r」（半角）です。
- "ユーザー名"「root」は、集中監視 Web サービスがインストールされたコンピューターからのみログインできます。
- ユーザーの追加やパスワード変更は、BOM 集中監視コンソールのログイン後に行えます。
- "ログイン情報を保持する"チェックボックスにチェックを入れて[ログイン]ボタンをクリックすると、次回ログイン時にユーザー名とパスワードを入力する必要がありません。

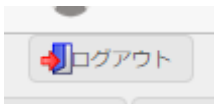
## 7. BOM 集中監視コンソールからのログアウト

集中監視 Web サービスとの接続（セッション）を切断し、BOM 集中監視コンソールからログアウトします。

- ログアウト後もセッションは残り続けますが、60分間（既定値、変更可能）何の応答もないセッションは、集中監視 Web サービスが自動的に切断するように制御されています。
- 短期間にセッションが多く滞留するとパフォーマンス低下の原因になります。

1. BOM 集中監視コンソールのコマンドバーの[ログアウト]ボタンをクリックします。

- ログアウトを行うと、ログイン画面に移動します。



## 8. BOM 集中監視コンソールの表示

### (1) インスタンスのステータス表示

BOM 集中監視コンソールは、BOM 8.0~5.0インスタンスと、それぞれのバージョンに該当するLinux オプションインスタンス、VMware オプションインスタンスの監視ステータスを収集し、監視対象インスタンスの状態を7つのステータスアイコンで表示します。

インスタンスステータスアイコンは下記のとおりです。優先度の高いものから順に解説します。

アイコン	説明
	監視対象コンピューターに接続できません。
	対象コンピューターのBOM ヘルパーサービスが停止しています。 BOM ヘルパーサービスのポート番号またはパスワードに相違があります。 インスタンスを削除したなどの理由により、インスタンス情報が取得できません。
	BOM 監視サービスが監視対象コンピューター上で開始されていません。
	BOM 監視サービスが開始していますが、1つ以上の監視項目が“失敗”しています。
	BOM 監視サービスが開始していますが、1つ以上の監視項目が“危険”ステータスにあります。
	BOM 監視サービスが開始していますが、1つ以上の監視項目が“注意”ステータスにあります。
	BOM 監視サービスが開始しており、1つ以上の監視項目が“正常”ステータスにあります。

### (2) グループの表示

グループの配下には、グループもしくはインスタンスを複数関連付けて、階層化させることができます。

階層化した際のグループ間の移動は、下記のとおり行います。

#### A. グループのアドレスバーを利用

BOM 集中監視コンソールの上部にあるアドレスバーを用いてグループ間の移動を行うことができます。

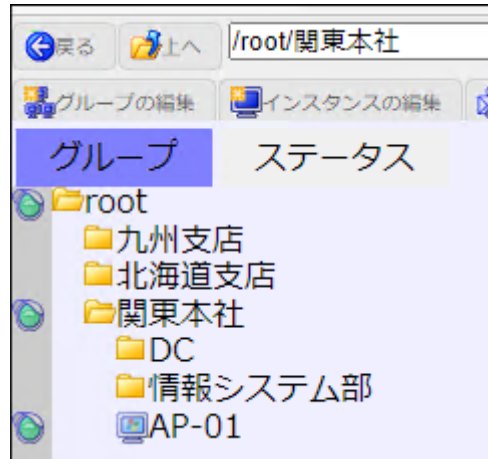
- アドレスバーには今現在どのグループを選択しているのかが表示されています。
- アドレスバーにグループのパスを直接入力した場合パスで指定したグループまで移動します。
- "戻る"をクリックした場合直前まで詳細ビューに表示していた画面に戻ります。
- "上へ"をクリックした場合選択しているグループの親グループに移動します。





## B. ツリービューを利用

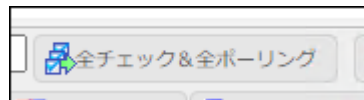
ツリービューに表示されたグループをクリックすることで、グループ間の移動を行うことができます。



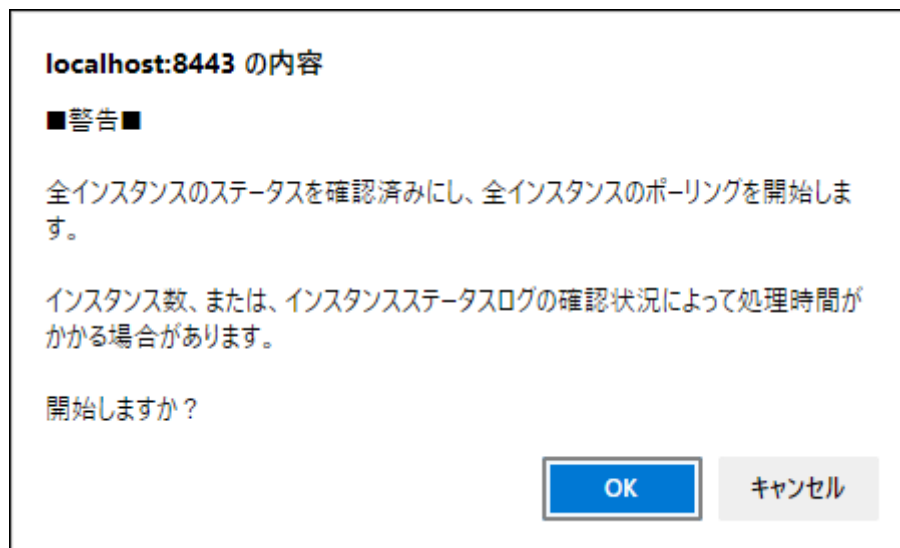
### (3) 全インスタンスステータスの確認および全インスタンス情報取得機能

「全チェック&全ポーリング」ボタンをクリックすることで、全インスタンスのステータスを確認し、ポーリング処理を一括で開始することが可能になります。

- ポーリング処理は一括で開始されますが、ブラウザ上で表示されているデータは自動で更新されません。
- ブラウザ上で表示されているデータを更新する場合には[更新]ボタンをクリックする必要があります。



なお、本機能を使用する際は、登録済みのインスタンスすべてに対してポーリングを行うため、下記の警告メッセージを表示します。



## (4) 表示の更新

BOM 集中監視コンソールには大きく分けて、画面左上のツリービュー、画面右上の詳細ビュー、画面下部のサマリーログビューに大別することができます。この3カ所の表示は、下記のどちらかの手段で更新することができます。

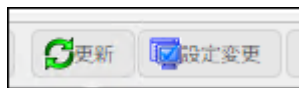
### A. 自動更新

既定値では、2分間に1度、表示が更新されるように設定されています。

更新間隔を変更する場合は、BOM 集中監視コンソールのコマンドバーの"設定変更"をクリックし、"設定変更"画面の"自動更新間隔"の値を変更します。詳細は、'[BOM 集中監視コンソールの環境設定変更](#)'を参照してください。

### B. 手動更新

BOM 集中監視コンソールのコマンドバーの"更新"をクリックすることで、表示を更新することができます。

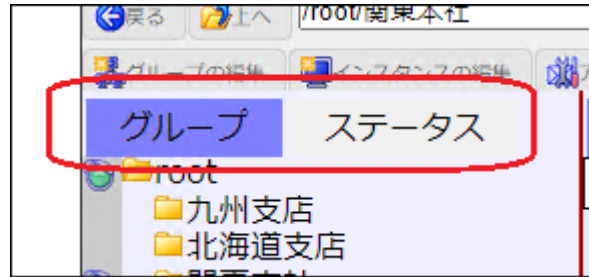


## (5) 表示枠のサイズ変更

画面左上のツリービュー、画面右上の詳細ビュー、画面下部のサマリーログビューの仕切り線をクリックしたまま移動させることで、それぞれのビューエリアの表示サイズを変更することができます。

## (6) ツリービュー表示

ツリービューには、「グループ」タブと「ステータス」タブが表示されています。



### A. 「グループ」タブ

グループとインスタンスが階層構造で表示され、グループもしくはインスタンスをクリックすると、詳細ビューに詳細を表示します。

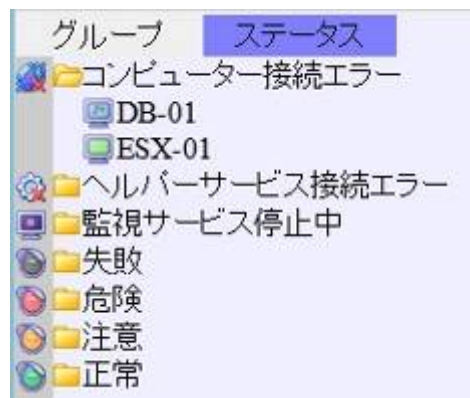
ステータスアイコンは、インスタンスステータスの中で一番優先度の高いアイコンが、左端に下記のとおり表示されます。

- 各インスタンスステータスの中で一番優先度の高いアイコンが、グループの代表ステータスとして表示されます。
- 各グループのインスタンスステータスの中で一番優先度の高いアイコンが、親グループの代表ステータスとして表示されます。



### B. 「ステータス」タブ

各インスタンスが検出したステータスのうち、最も優先度の高いステータスのアイコン箇所にのみ各インスタンス名が表示されます。ステータスから、調査や対応の優先順位を判断したい時などに活用できます。

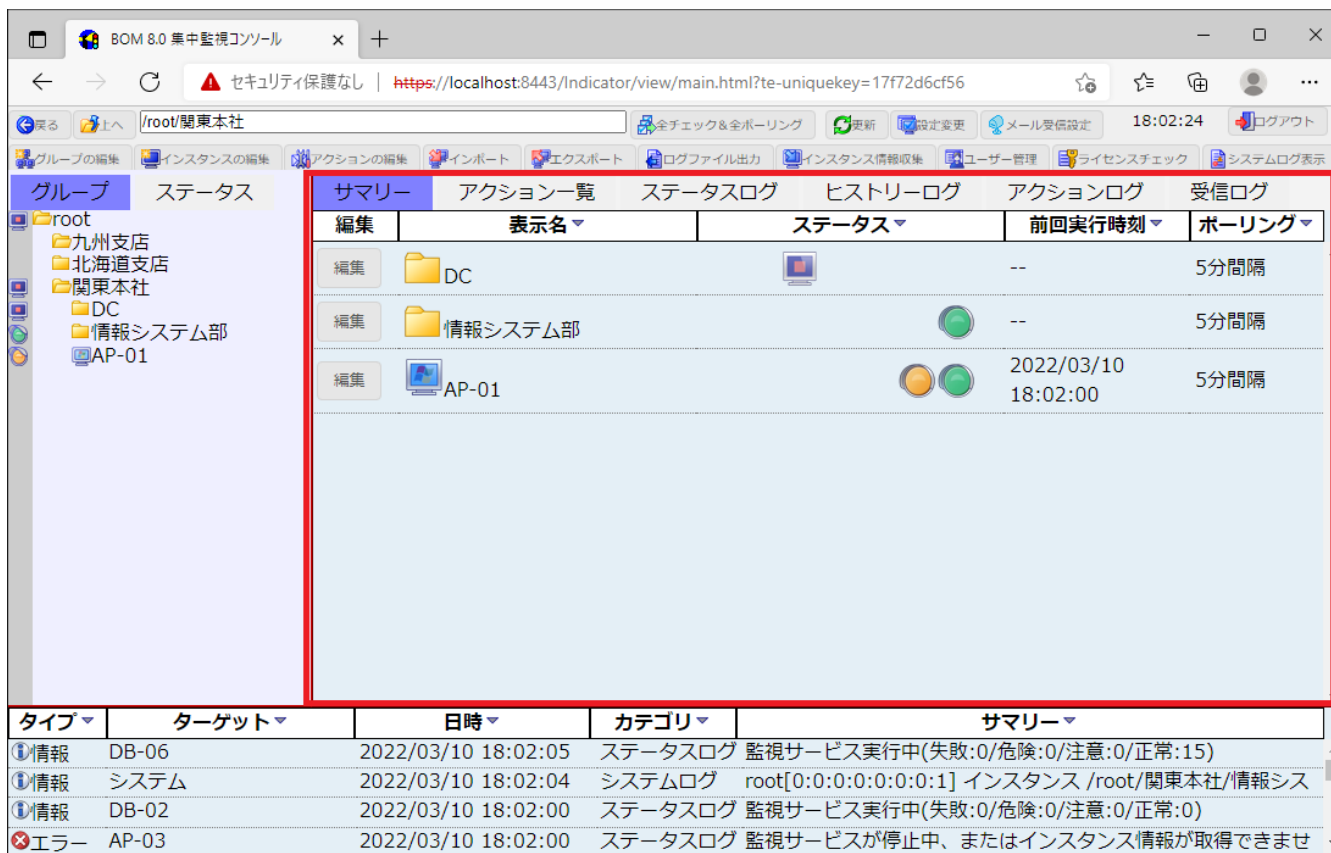


例：上記"DB-01"というインスタンスが"注意"と"コンピューター接続エラー"のステータスを検出している場合、"コンピューター接続エラー"ステータスアイコン箇所に"DB-01"というインスタンス名が表示されますが、"注意"ステータスアイコン箇所には"DB-01"というインスタンス名は表示されません。

## (7) 詳細ビュー表示

ツリービューの「グループ」タブや「ステータス」タブで選択した結果を、詳細ビューに表示します。

「サマリー」タブ、「アクション一覧」タブ、「ステータスログ」タブ、「履歴ログ」タブ、「アクションログ」タブ、「受信ログ」タブの中から設定内容や監視データを絞り込むことができます。



The screenshot shows the BOM 8.0 monitoring console. The main content area is divided into tabs: サマリー (Summary), アクション一覧 (Action List), ステータスログ (Status Log), ヒストリーログ (History Log), アクションログ (Action Log), and 受信ログ (Received Log). The 'Summary' tab is active, displaying a table of monitored items.




編集	表示名	ステータス	前回実行時刻	ポーリング
編集	DC		--	5分間隔
編集	情報システム部		--	5分間隔
編集	AP-01		2022/03/10 18:02:00	5分間隔

Below the main content area, there is a detailed log table:

タイプ	ターゲット	日時	カテゴリ	サマリー
情報	DB-06	2022/03/10 18:02:05	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)
情報	システム	2022/03/10 18:02:04	システムログ	root[0:0:0:0:0:0:1] インスタンス /root/関東本社/情報シス
情報	DB-02	2022/03/10 18:02:00	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:0)
エラー	AP-03	2022/03/10 18:02:00	ステータスログ	監視サービスが停止中、またはインスタンス情報が取得できませ

## A. 「サマリー」タブ

ツリービューでグループを選択している場合、選択したグループ直下のグループもしくはインスタンスの監視データの中に存在するステータスのアイコンが表示されます。

サマリー	アクション一覧	ステータスログ	ヒストリーログ	アクションログ	受信ログ
編集	表示名 ▼	ステータス ▼	前回実行時刻 ▼	ポーリング ▼	
編集	DC		--	5分間隔	
編集	情報システム部		--	5分間隔	
編集	AP-01		2022/03/10 18:02:00	5分間隔	

- [編集]ボタン

"グループの編集"画面、もしくは"インスタンスの編集"画面を表示させることができます。

詳細は、'[グループの設定](#)'、'[インスタンスの設定-インスタンスの編集画面](#)'を参照してください。

- "表示名"

対象のグループ名、もしくはインスタンス名が表示されます。

"グループ"をクリックすると、クリックした"グループ"に移動することができます。

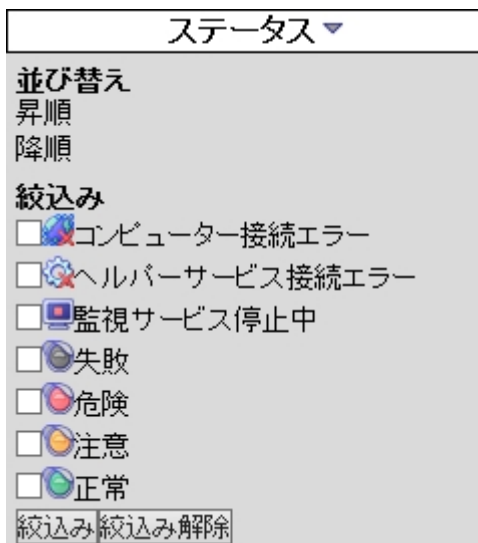
"インスタンス"をクリックすると、"インスタンス"全体のサマリー情報を表示させることができます。"表示名"の横にある"▼"をクリックすると、"表示名"で昇順/降順の並べ替えや、キーワードによる部分一致で絞り込みができます。



- "ステータス"

対象のグループ、もしくはインスタンスの監視データで発生しているステータスのうち、確認を行っていないステータスの監視データを表示します。ステータスアイコンの詳細は、'[インスタンスのステータス表示](#)'を参照してください。

"ステータス"の横にある"▼"をクリックすると、"ステータス"で昇順/降順の並べ替えができます。

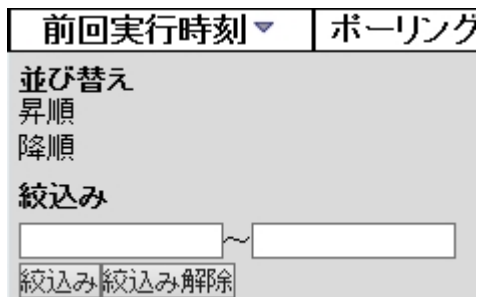


- "前回実行時刻"

対象のインスタンスが、最後にポーリングを実行した時刻が表示されます。

"前回実行時刻"の横にある"▼"をクリックすると、"前回実行時刻"で昇順/降順の並べ替えや、時刻の範囲指定による絞り込みができます。

- 時刻の範囲指定は、"yyyy/MM/dd hh:mm:ss"形式で入力します。  
(yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。)

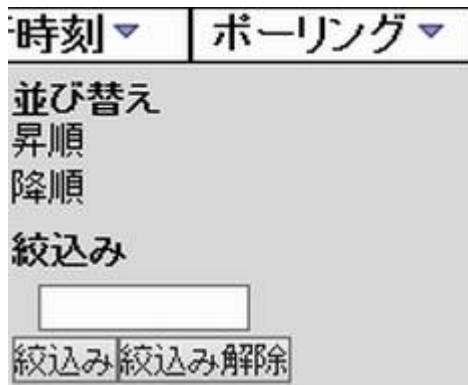


- "ポーリング"

対象のグループ、もしくはインスタンスのポーリング間隔を表示します。

"ポーリング"の横にある"▼"をクリックすると、"ポーリング"で昇順/降順の並べ替えや、キーワードによる部分一致で絞り込みができます。

- インスタンスのポーリング設定で、"グループの設定に従う"ラジオボタンを選択している場合  
親グループのポーリング間隔が表示され"個別のポーリング設定を行う"ラジオボタンを選択している場合はインスタンスのポーリング間隔が表示されます。



- ツリービューでインスタンスを選択している場合

選択したインスタンス全体のサマリー情報を表示させることができます。

サマリー情報は、"ステータス"フィールド、"ポーリング情報"フィールド、"インスタンス設定"フィールドと[編集]ボタンで構成されます。

- "ステータス"フィールド

選択したインスタンスの最終ポーリングの監視データをステータス別にサマリーした結果と、監視データの中で一番優先度の高いステータスが代表ステータスとして大枠に表示されます。

[ただちにポーリングを行う]ボタンをクリックすると、ポーリングを実行することができます。

ステータス		ただちにポーリングを行う
	 失敗	0
	 危険	0
	 注意	1
	 正常	13

- "ポーリング情報"フィールド

選択したインスタンスの各種ポーリング情報を表示します。

ポーリング情報	
次回ポーリング日時	2022/03/10 18:06:59
最終ポーリング日時	2022/03/10 18:02:00
ポーリング実行状態	実行中ではない
ポーリング設定	グループの設定に従う
ポーリング設定有効	--
ポーリング間隔	--

- "次回ポーリング日時"

前回ポーリングを開始した時刻にポーリング間隔を加えた予定日時を表示



- "最終ポーリング日時"

最後にポーリングが完了した日時を表示

- "ポーリング実行状態"

画面を表示した時点でのポーリングの"実行中"、"実行中ではない"という状態を表示

- "ポーリング設定"

"グループの設定に従う"と"個別のポーリング設定を行う"のどちらかの設定内容を表示

- "ポーリング設定有効"


"個別のポーリング設定を行う"場合に、"有効"と"無効"のどちらかの設定内容を表示

- "ポーリング間隔"

"個別のポーリング設定を行う"場合に、"ポーリング間隔"の設定内容を表示

- インスタンス設定

"インスタンスの編集"画面で設定した、選択したインスタンスの設定内容を表示させます。

インスタンス設定	
表示名	AP-01
監視対象コンピューター	localhost
ヘルパーサービスポート	20080
インスタンス種別	 BOM 8.0 基本製品 インスタンス
インスタンス名	WIN-NBIAMPVUFID

- "表示名"

インスタンスの表示名を表示

- "監視対象コンピューター"

監視対象コンピューターのIPアドレスもしくはコンピューター名を表示

- "ヘルパーサービスポート"

BOM ヘルパーサービスとの通信ポートを表示

- "インスタンス種別"

インスタンスの製品種別を表示

- "インスタンス名"

インスタンス名を表示

- [編集]ボタン

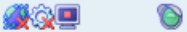

[編集]ボタンをクリックすると、"インスタンスの編集"画面を表示させることができ、選択したインスタンスの設定変更や削除、新規で別のインスタンスを追加することもできます。

"インスタンスの編集"画面の詳細は、'[インスタンスの設定-インスタンスの編集画面](#)'を参照してください。

## B. 「アクション一覧」タブ

ツリービューでグループを選択している場合に、詳細ビューに表示されます。

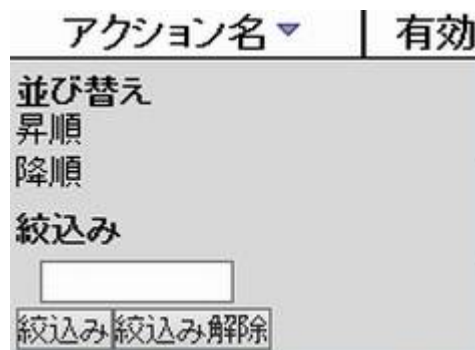
選択したグループに関連付けられたアクションの一覧が表示されます。

サマリー	アクション一覧	ステータスログ	ヒストリーログ	アクションログ	受信ログ
アクション名▼	有効▼	条件▼	概要▼		最終実行日時▼
ログ収集実行	有効		カスタムアクション[collect-log.bat]		
管理者向けメール通知	有効		メール送信[mail.say-tech.jp:25]		

- "アクション名"

アクション名が表示されます。アクションをクリックすると、"アクションの編集"画面を表示させることができます。詳細については、'[アクションの設定](#)'を参照してください。

"アクション名"の横にある"▼"をクリックすると、"アクション名"で昇順/降順の並び替えや、キーワードによる部分一致で絞り込みができます。



- "有効"

アクションの有効/無効状態が表示されます。"有効"の横にある"▼"をクリックすると、有効/無効で昇順/降順の並び替えや絞り込みができます。



- "条件"

アクションの実行条件が表示されます。"条件"の横にある"▼"をクリックすると、"条件"で昇順/降順の並び替えや、ステータスによる絞り込みができます。

条件 ▼
<b>並び替え</b> 昇順 降順
<b>絞込み</b> <input type="checkbox"/> コンピューター接続エラー <input type="checkbox"/> ヘルパーサービス接続エラー <input type="checkbox"/> 監視サービス停止中 <input type="checkbox"/> 失敗 <input type="checkbox"/> 危険 <input type="checkbox"/> 注意 <input type="checkbox"/> 正常
<input type="button" value="絞込み"/> <input type="button" value="絞込み解除"/>

- "概要"

アクションに設定した概要情報が表示されます。"概要"の横にある"▼"をクリックすると、"概要"で昇順/降順の並び替えや、キーワードによる部分一致で絞込みができます。

概要 ▼
<b>並び替え</b> 昇順 降順
<b>絞込み</b> <input type="text"/>
<input type="button" value="絞込み"/> <input type="button" value="絞込み解除"/>

- "最終実行日時"

該当するアクションが最後に実行した実行日時を表示します。"最終実行日時"の横にある"▼"をクリックすると、"最終実行日時"で昇順/降順の並び替えや、時刻の範囲指定による絞込みができます。

- 日時の範囲指定は、"yyyy/MM/dd hh:mm:ss"形式で入力します。（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

最終実行日時 ▼
<b>並び替え</b> 昇順 降順
<b>絞込み</b> <input type="text"/> ~ <input type="text"/>
<input type="button" value="絞込み"/> <input type="button" value="絞込み解除"/>

## C. 「ステータス」タブ

ツリービューでインスタンスを選択している場合に、詳細ビューに表示されます。

選択したインスタンスに登録されている監視項目の最新の監視結果一覧（ポーリング時点）が表示されます。

名前▼	ID▼	間隔▼	ステータス▼	前回の値	前回の時刻▼	コード	時間▼
 プロセッサ処理待ち行列長	GRP01M ON01	60分	 正常	2	2022/03/10 17:32:35	0x0	0.0秒
 プロセッサ監視	GRP01M ON02	60分	 正常	4%	2022/03/10 17:32:35	0x0	0.0秒
 メモリ監視	GRP01M ON03	60分	 注意	735MB	2022/03/10 17:32:35	0x0	0.0秒
 仮想メモリ監視	GRP01M ON04	60分	 正常	73%	2022/03/10 17:32:35	0x0	0.0秒
 ディスクアクセス監視	GRP01M ON05	60分	 正常	3%	2022/03/10 17:32:35	0x0	0.109秒
 ディスク処理待ち行列長監視	GRP01M ON06	60分	 正常	0	2022/03/10 17:32:35	0x0	0.109秒
 Cドライブディスク容	GRP01M	60分	 正常	20GB	2022/03/10	0x0	0.0秒

- "名前"

監視項目名が表示されます。"名前"の横にある"▼"をクリックすると、昇順/降順の並べ替えや監視項目名で絞り込みができます。

**名前▼**

---

並び替え

昇順

降順

絞り込み

絞り込み 絞り込み解除

- "ID"

監視項目の監視項目IDが表示されます。"ID"の横にある"▼"をクリックすると、昇順/降順の並べ替えや監視項目IDで絞り込みができます。

**ID▼** | **間隔▼** | **ステータス▼**

---

並び替え

昇順

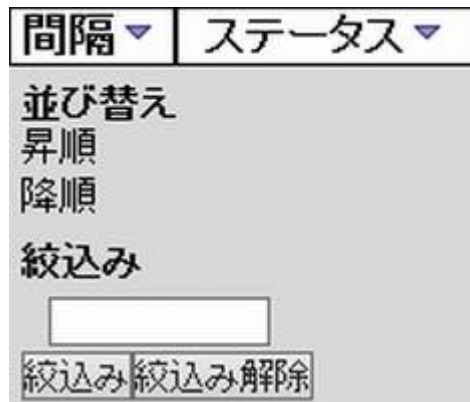
降順

絞り込み

絞り込み 絞り込み解除

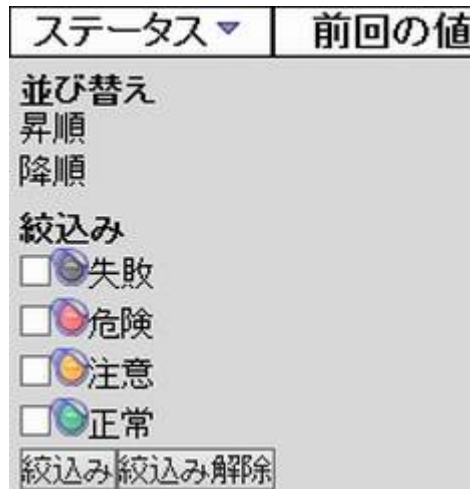
- "間隔"

監視項目の最新（ポーリング時点）の監視間隔が表示され、監視が無効状態の場合には"無効"と表示されます。"間隔"の横にある"▼"をクリックすると、昇順/降順の並び替えや監視間隔で絞り込みができます。



- "ステータス"

監視項目の最新（ポーリング時点）の監視ステータスが表示されます。"ステータス"の横にある"▼"をクリックすると、昇順/降順の並び替えやステータスによる絞り込みができます。



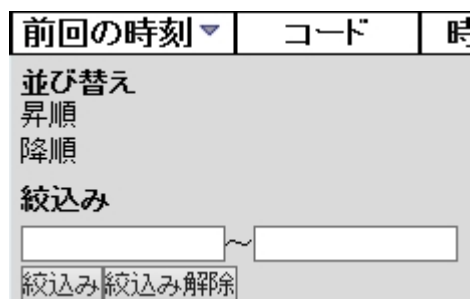
- "前回の値"

監視項目の最新（ポーリング時点）の監視値が表示されます。

- "前回の時刻"

監視項目の最新（ポーリング時点）の監視が実行された時刻が表示されます。"前回の時刻"の横にある"▼"をクリックすると、昇順/降順の並び替えや日時範囲による絞り込みができます。

- 時刻の範囲指定は、"yyyy/MM/dd hh:mm:ss"形式で入力します。（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

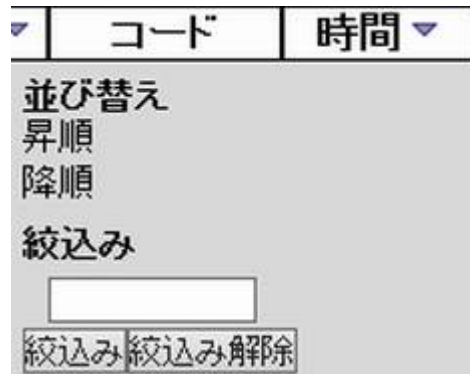


- "コード"

監視項目の最新（ポーリング時点）の監視実行結果コードが表示されます。

- "時間"

監視項目の最新（ポーリング時点）の監視が開始されてから終了するまでの実行時間が表示されます。"時間"の横にある"▼"をクリックすると、昇順/降順の並び替えや実行時間による絞り込みができます。



#### D. 「ステータスログ」タブ

BOM 集中監視コンソールに設定したグループもしくはインスタンスのステータス情報に関する監視サービスの実行状況や、監視結果のサマリー情報を、インスタンスごとに表示させます。

- "表示名"、"時刻"、"ステータス"、"概要"が表示され、それぞれの表示項目で並び替えやキーワードによる部分一致で絞り込み検索ができます。

ステータスログの詳細は、'[ステータスログ](#)'をして参照ください。

サマリー	アクション一覧	ステータスログ	履歴ログ	アクションログ	受信ログ
表示名	時刻	ステータス	概要		
<input type="checkbox"/> DB-06	2022/03/10 18:17:05		監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)		
<input type="checkbox"/> AP-03	2022/03/10 18:17:00		監視サービスが停止中、またはインスタンス情報が取得できません。		
<input type="checkbox"/> AP-01	2022/03/10 18:17:00		監視サービス実行中(失敗:0/危険:0/注意:1/正常:13)		
<input type="checkbox"/> DB-06	2022/03/10 18:12:05		監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)		
<input type="checkbox"/> AP-03	2022/03/10 18:12:00		監視サービスが停止中、またはインスタンス情報が取得できません。		
<input type="checkbox"/> AP-01	2022/03/10 18:12:00		監視サービス実行中(失敗:0/危険:0/注意:1/正常:13)		
<input type="checkbox"/> DB-06	2022/03/10 18:07:05		監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)		
<input type="checkbox"/> AP-03	2022/03/10 18:07:00		監視サービスが停止中、またはインスタンス情報が取得できません。		
<input type="checkbox"/> AP-01	2022/03/10 18:07:00		監視サービス実行中(失敗:0/危険:0/注意:1/正常:13)		

## E. 「履歴ログ」タブ

BOM 集中監視コンソールに設定したインスタンスの履歴ログを表示させることができます。履歴ログの詳細は、'BOM for Windows Ver.8.0 ユーザーズマニュアル'を参照ください。

- "タイプ"、"表示名"、"日時"、"カテゴリ"、"サマリー"が表示され、それぞれの表示項目で並び替えやキーワードによる部分一致で絞り込み検索ができます。

履歴ログの詳細は、'[履歴ログ](#)'を参照してください。

サマリー	アクション一覧	ステータスログ	履歴ログ	アクションログ	受信ログ
タイプ▼	表示名▼	日時▼	カテゴリ▼	サマリー▼	
情報	AP-01	2022/03/10 18:02:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN	
情報	AP-01	2022/03/10 17:32:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN	
警告	AP-01	2022/03/10 17:32:35	監視	監視 'メモリ監視' のステータスが 注意 に変化しました。 ID: GRP01MON03 実行時間:	
情報	AP-01	2022/03/10 17:02:38	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN	
情報	AP-01	2022/03/10 16:32:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN	
情報	AP-01	2022/03/10 16:02:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN	
情報	DB-06	2022/03/10 15:40:25	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 1920 インスタンス ID: SQL	
情報	AP-01	2022/03/10 15:32:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN	
情報	AP-01	2022/03/10 15:02:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN	

## F. 「アクションログ」タブ

BOM 集中監視コンソールに設定したアクションの実行結果を表示させることができます。

- "日時"、"アクション名"、"トリガー"、"結果"、"コード"、"概要"が表示され、それぞれの表示項目で並び替えやキーワードによる部分一致で絞り込み検索ができます。アクションログの詳細は、'[アクションログ](#)'を参照してください。

サマリー	アクション一覧	ステータスログ	履歴ログ	アクションログ	受信ログ
日時▼	アクション名▼	トリガー▼	結果▼	コード	概要▼
2022/03/10	ログ収集実行	AP-01	失敗	0xFFFFFFFF	外部コマンドの実行に失敗しました。 ("c:¥work¥collect-log.bat" )
2022/03/10	ログ収集実行	AP-01	成功	0x0	アクションは正常に終了しました。
2022/03/10	ログ収集実行	AP-01	成功	0x0	アクションは正常に終了しました。



## G. 「受信ログ」タブ

BOM 集中監視コンソールに設定したメール受信の受信結果を表示させることができます。

- "タイプ"、"件名"、"送信日時"、"送信元"、"本文"が表示され、それぞれの表示項目で並び替えやキーワードによる部分一致で絞り込み検索ができます。受信ログの詳細は、'[受信ログ](#)'を参照してください。

サマリー	アクション一覧	ステータスログ	ヒストリーログ	アクションログ	受信ログ
タイプ▼	件名▼	送信日時▼	送信元▼	本文▼	
 testmail	閾値変更	2022/02/14 17:16:56	say tech test@yam. on.jp	DB-01 プロセッサしきい値を変更しました	
 testmail	test	2022/02/14 17:16:11	say tech test@yam. on.jp	テストメール	
 testmail	testmail	2022/02/14 17:15:50	say tech test@yam. on.jp	テストメール	

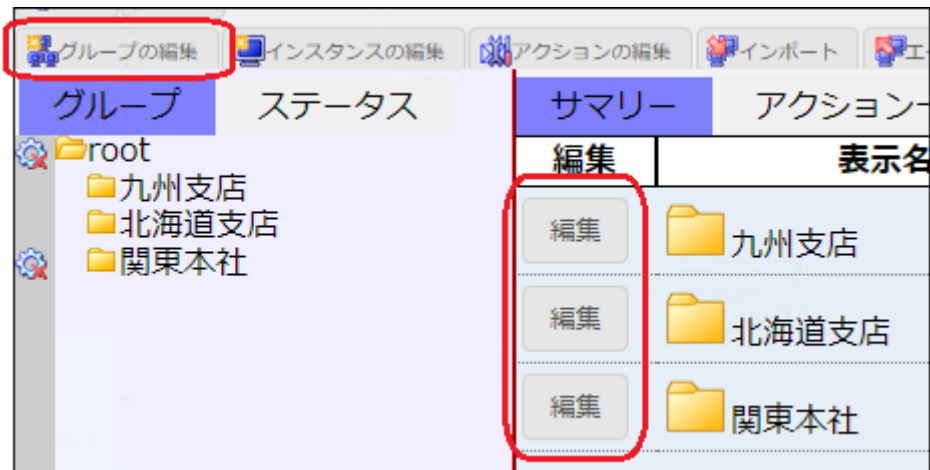
## 9. BOM 集中監視コンソールの設定

### (1) グループの設定

グループを設定する方法には"グループの編集"と"インポート"の2種類があり、本章では"グループの編集"方法を解説します。"インポート"方法については、[設定のエクスポート/インポート](#)を参照してください。

BOM 集中監視コンソールのインスタンスを整理するために、グループを"追加"、"変更"、"削除"することができます。これらの操作を行うには、"グループの編集"画面を下記のどちらかの手段で表示させます。

- ツリービューの編集を行いたいグループをクリックし、コマンドバーの"グループの編集"をクリック
  - 詳細ビューの編集を行いたいグループの横にある[編集]ボタンをクリック
- ※ グループは最大で7階層まで作成できます。



↓

## グループの編集



### グループの設定

親グループ

グループ名 root

ポーリング有効/無効 有効

ポーリング間隔 5 分

最終更新ユーザー root

最終更新日時 2022/03/10 20:03:22

追加

変更

削除

閉じる

### A. グループの追加

新規でグループを追加することができます。

1. "グループの編集"画面の[追加]ボタンをクリックし、"グループ新規追加"画面を表示させます。



グループ新規追加	
親グループ	<input type="text" value="/root"/>
グループ名	<input type="text"/>
ポーリング有効/無効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
ポーリング間隔	<input type="text" value="5分"/> ▼

確認      変更前に戻る      戻る      閉じる

2. "親グループ"フィールドに、作成するグループの所属先を入力します。
  - "/root"が頂点です。グループの階層が深くなる場合、"/"でグループを繋いでいきます。
  - 存在しない親グループを指定することや、親グループに"/"のみを指定することはできません。
3. "グループ名"フィールドに、BOM 集中監視コンソールに表示させたいグループ名を入力します。
4. "ポーリング有効/無効"は、下記のどちらかを選択します。

なお、ポーリングとは対象インスタンスのBOMヘルパーサービスと通信をしてステータス情報を収集することを指します。

  - "有効"ラジオボタンを選択した場合  
このグループ配下に含まれるインスタンスのうち、"グループの設定に従う"ラジオボタンを選択しているすべてのインスタンスのポーリングを"有効"にします。
  - "無効"ラジオボタンを選択した場合  
このグループ配下に含まれるインスタンスのうち、"グループの設定に従う"ラジオボタンを選択しているすべてのインスタンスのポーリングを"無効"にします。
5. "ポーリング間隔"は、このグループに所属するインスタンスのステータス情報を収集する間隔を設定することができます。
6. [確認]ボタンをクリックすると確認画面が表示されます。問題がなければ[確定]ボタンをクリックします。

## B. グループの編集

作成したグループの内容を編集することができます。

1. "グループの編集"画面の[変更]ボタンをクリックし、"グループ情報変更"画面を表示させます。



グループ情報変更	
親グループ	<input type="text" value="/root"/>
グループ名	<input type="text" value="九州支店"/>
ポーリング有効/無効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
ポーリング間隔	<input type="text" value="5分"/> ▼

確認      変更前に戻る      戻る      閉じる

2. "親グループ"フィールドに、所属したいグループを入力します。
  - "/root"が頂点です。グループの階層が深くなる場合、"/"でグループを繋いでいきます。
  - 自身のグループもしくは自身の子孫にあたるグループを指定するとエラーとなります。
  - "/root"を変更することはできません。

3. "グループ名"フィールドに、変更したいグループ名を入力します。

4. "ポーリング有効/無効"は、下記のどちらかを選択します。

なお、ポーリングとは対象インスタンスのBOMヘルパーサービスと通信をしてステータス情報を収集することを指します。

- "有効"ラジオボタンを選択した場合

このグループ配下に含まれるインスタンスのうち、"グループの設定に従う"ラジオボタンを選択しているすべてのインスタンスのポーリングを"有効"にします。

- "無効"ラジオボタンを選択した場合

このグループ配下に含まれるインスタンスのうち、"グループの設定に従う"ラジオボタンを選択しているすべてのインスタンスのポーリングを"無効"にします。

5. "ポーリング間隔"は、このグループに所属するインスタンスのステータス情報を収集する間隔を設定することができます。
6. [変更前に戻る]ボタンをクリックすると、手順2.~5.の変更内容を破棄することができます。
7. [確認]ボタンをクリックすると、確認画面が表示されるため、問題がなければ[確定]ボタンをクリックします。

## C.グループの削除

作成したグループを削除することができます。

1. "グループの編集"画面の[削除]ボタンをクリックし、"グループ情報削除"画面を表示させます。



2. 問題がなければ[確定]ボタンをクリックします。

## (2) インスタンスの設定-インスタンスの編集画面

インスタンスを設定する方法には"インスタンスの編集"、"インスタンス情報収集"および、"インポート"の3種類があり、本章では"インスタンスの編集"の方法を解説します。

- "インスタンス情報収集"方法は、'[インスタンス設定-インスタンス情報収集](#)'を参照してください。
- "インポート"方法は、'[設定のエクスポート/インポート](#)'を参照してください。

BOM 集中監視コンソールで監視するインスタンスを"追加"、"変更"、"削除"する際は、"インスタンスの編集"画面を下記のどれかの手段で表示させます。

- グループをクリックし、コマンドバーの"インスタンスの編集"をクリック
- グループをクリックし、詳細ビューに表示されたインスタンス横にある[編集]ボタンをクリック
- ツリービューのインスタンスをクリックし、詳細ビューのインスタンス画面下部にある[編集]ボタンをクリック



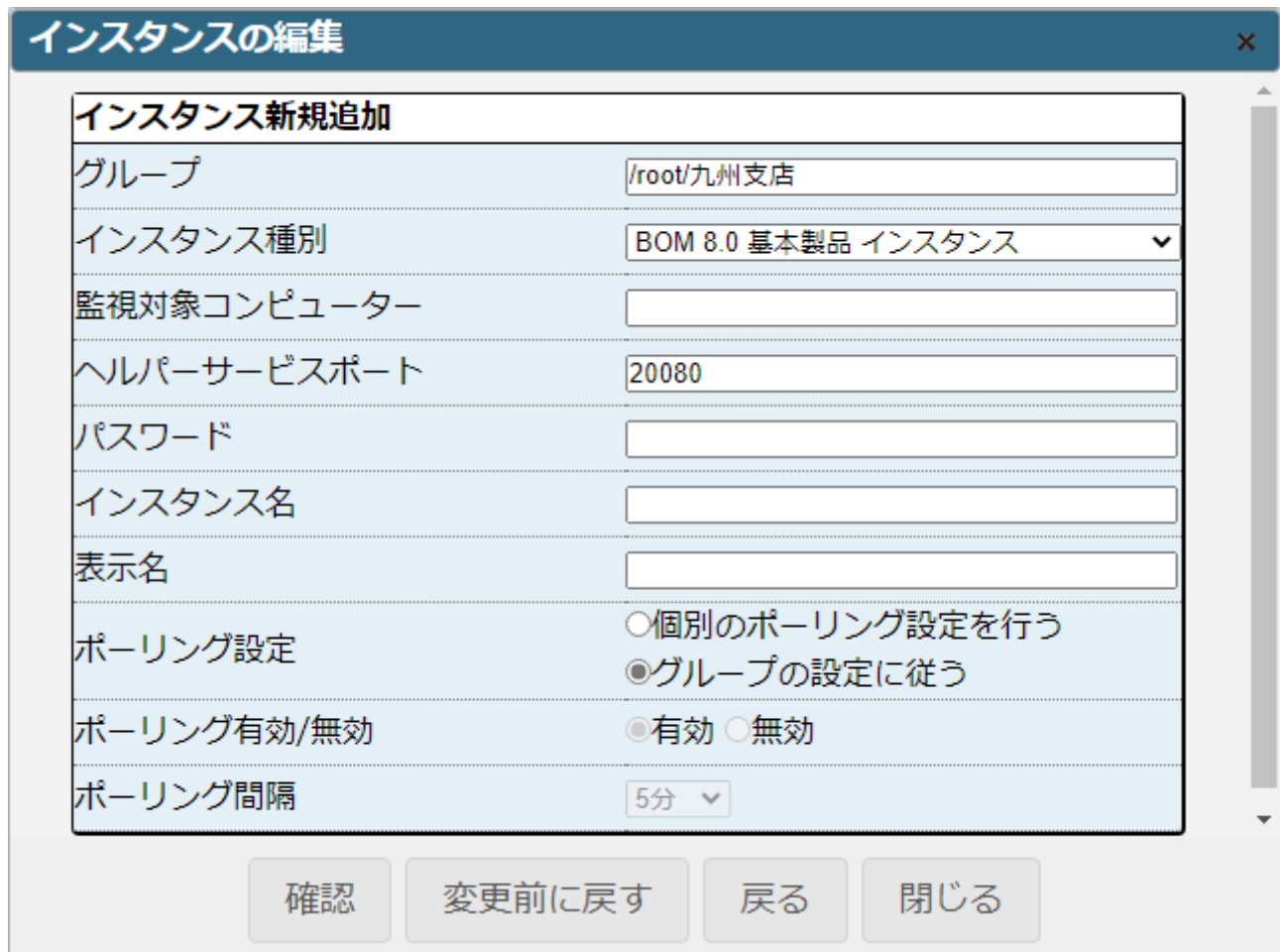


### A. インスタンスの追加

新規でインスタンスを追加することができます。



1. "インスタンスの編集"画面の[追加]ボタンをクリックし、"インスタンス新規追加"画面を表示させます。



インスタンス新規追加	
グループ	/root/九州支店
インスタンス種別	BOM 8.0 基本製品 インスタンス
監視対象コンピューター	
ヘルパーサービスポート	20080
パスワード	
インスタンス名	
表示名	
ポーリング設定	<input type="radio"/> 個別のポーリング設定を行う <input checked="" type="radio"/> グループの設定に従う
ポーリング有効/無効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
ポーリング間隔	5分

確認 変更前に戻す 戻る 閉じる

2. "グループ"フィールドに、作成するインスタンスの所属先を入力します。
  - "/root"が頂点です。所属させたいグループの階層が深くなる場合、"/"でグループを繋いでいきます。
3. "インスタンス種別"に、追加したいインスタンスの正しい種別を下記より選択します。
  - 下記に表示されていないインスタンスは、BOM 集中監視コンソールの対象外です。

BOM 5.0 基本製品 インスタンス  
BOM 5.0 Linuxオプション インスタンス  
BOM 5.0 VMwareオプション インスタンス  
BOM 6.0 基本製品 インスタンス  
BOM 6.0 Linuxオプション インスタンス  
BOM 6.0 VMwareオプション インスタンス  
BOM 7.0 基本製品 インスタンス  
BOM 7.0 Linuxオプション インスタンス  
BOM 7.0 VMwareオプション インスタンス  
BOM 8.0 基本製品 インスタンス  
BOM 8.0 Linuxオプション インスタンス  
BOM 8.0 VMwareオプション インスタンス

4. "監視対象コンピューター"フィールドに、BOM 5.0~8.0がインストールされている"コンピューター名"もしくは"IPアドレス"を入力します。
  - 代理監視を行っている場合、BOM 5.0~8.0が導入されている監視元コンピューターを"監視対象コンピューター"フィールドに入力してください。

- 登録できるインスタンスの条件については、'[インスタンス](#)'も参照してください。
5. "ヘルパーサービスポート"フィールドに、インスタンスのBOMヘルパーサービスとの通信に用いるポート番号を登録します。BOMヘルパーサービスのポート番号に関する詳細は、'BOM for Windows Ver.8.0 ユーザーズマニュアル'を参照してください。
  6. "パスワード"フィールドに、BOMヘルパーサービスに参照モードのパスワードが指定されている場合に、該当するパスワードを入力します。
  7. "インスタンス名"フィールドに、監視対象のインスタンスを下記のどちらかの手段で設定します。
    - "インスタンス名"を入力します。
    - "インスタンス名"フィールドにカーソルを合わせカーソルキーの上もしくは下を押下すると、手順4.で指定した"監視対象コンピューター"に登録されている"インスタンス"がリスト表示されるので、リストから登録したいインスタンス名を選択します。
  8. "表示名"フィールドに、BOM 集中監視コンソールに表示させるインスタンス名を入力します。
  9. "ポーリング設定"は、下記のどちらかを選択します。
    - "個別のポーリング設定を行う"ラジオボタンを選択した場合  
インスタンスが所属するグループの"ポーリング有効/無効"設定内容に影響を受けなくなるため、手順10.のインスタンスの"ポーリング有効/無効"の設定を最優先に採用します。
    - "グループの設定に従う"ラジオボタンを選択した場合  
インスタンスが所属するグループの"ポーリング有効/無効"設定内容に従います。
  10. "ポーリング有効/無効"は、手順9.で"個別のポーリング設定を行う"ラジオボタンを選択した場合に設定ができます。なお、ポーリングとは対象インスタンスのBOMヘルパーサービスと通信をしてステータス情報を収集することを指します。
    - "有効"ラジオボタンを選択した場合  
インスタンスのポーリングを"有効"にします。
    - "無効"ラジオボタンを選択した場合  
インスタンスのポーリングを"無効"にします。
  11. "ポーリング間隔"は、手順10.で"有効"ラジオボタンを選択した場合に、インスタンスのステータス情報を収集する間隔を設定することができます。
  12. [確認]ボタンをクリックすると、確認画面が表示されるため、問題がなければ[確定]ボタンをクリックします。
    - 確認時に、BOMヘルパーサービスへの接続確認とインスタンスの存在確認を行います。この際、接続確認または存在確認が失敗した場合、インスタンスは追加できません。

## B. インスタンスの編集

作成したインスタンスの内容を編集することができます。

1. "インスタンスの編集"画面の[変更]ボタンをクリックし、"インスタンス情報変更"画面を表示させます。



インスタンス情報変更	
グループ	/root/関東本社
インスタンス種別	BOM 8.0 基本製品 インスタンス
監視対象コンピューター	xxx.xxx.xxx.xxx
ヘルパーサービスポート	20080
パスワード	...
インスタンス名	WIN-NBIAMPVUFID
表示名	AP-01
ポーリング設定	<input type="radio"/> 個別のポーリング設定を行う <input checked="" type="radio"/> グループの設定に従う
ポーリング有効/無効	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
ポーリング間隔	5分

確認 変更前に戻す 戻る 閉じる

2. "グループ"フィールドに、インスタンスの所属先を入力します。
  - "/root"が頂点です。所属させたいグループの階層が深くなる場合、"/"でグループを繋いでいきます。
3. "インスタンス種別"に、インスタンスの正しい製品種別を下記より選択します。
  - 下記に表示されていない製品は、BOM 集中監視コンソールの対象外製品になりますのでご注意ください。

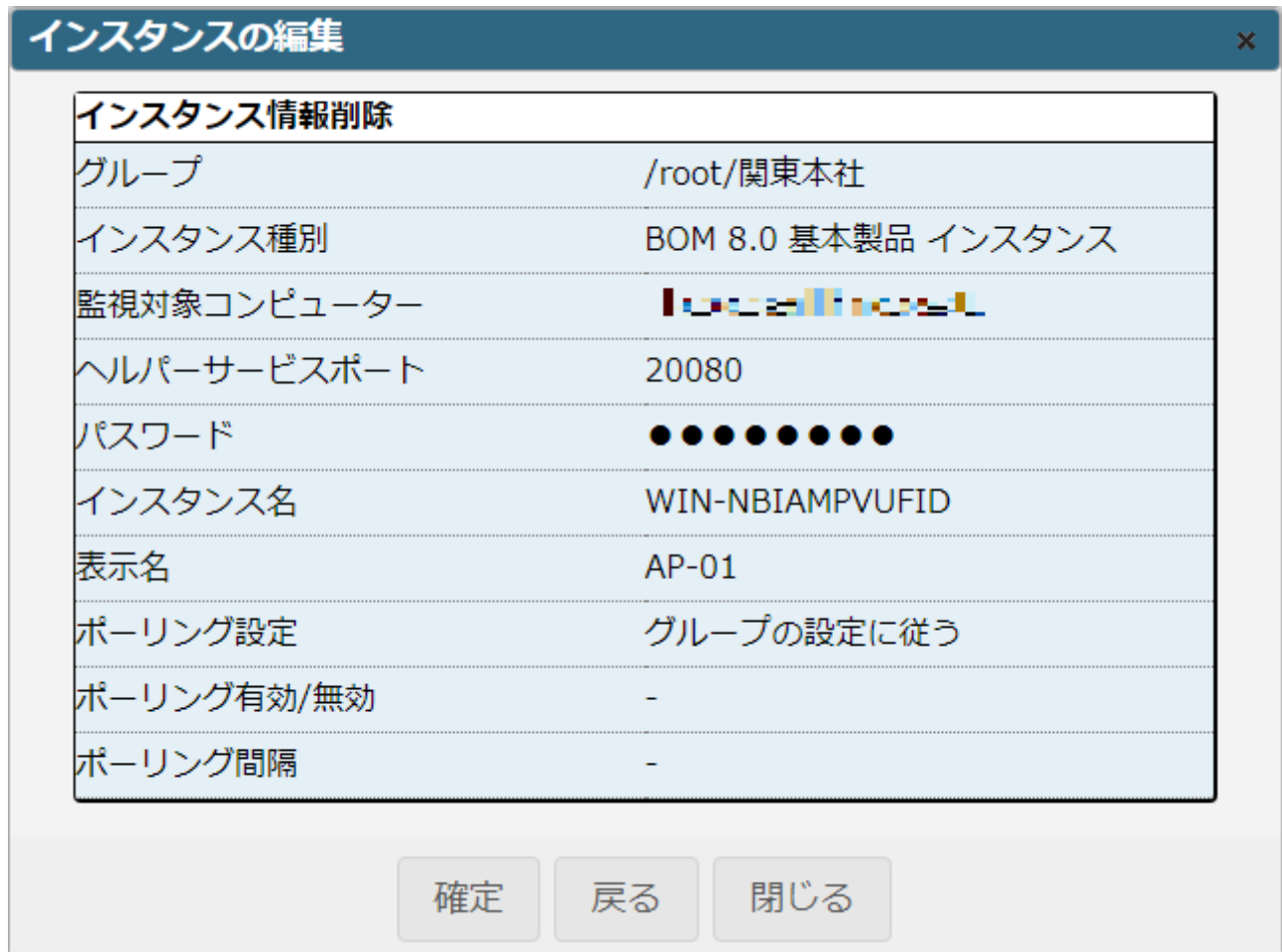
BOM 5.0 基本製品 インスタンス  
BOM 5.0 Linuxオプション インスタンス  
BOM 5.0 VMwareオプション インスタンス  
BOM 6.0 基本製品 インスタンス  
BOM 6.0 Linuxオプション インスタンス  
BOM 6.0 VMwareオプション インスタンス  
BOM 7.0 基本製品 インスタンス  
BOM 7.0 Linuxオプション インスタンス  
BOM 7.0 VMwareオプション インスタンス  
**BOM 8.0 基本製品 インスタンス**  
BOM 8.0 Linuxオプション インスタンス  
BOM 8.0 VMwareオプション インスタンス

4. "監視対象コンピューター"フィールドに、BOM 5.0~8.0がインストールされている"コンピューター名"もしくは"IPアドレス"を入力します。
  - 代理監視を行っている場合、BOM 5.0~8.0が導入されている監視元コンピューターを"監視対象コンピューター"フィールドに入力してください。
  - 登録できるインスタンスの条件については、'[インスタンス](#)'も参照してください。
5. "ヘルパーサービスポート"フィールドに、インスタンスのBOMヘルパーサービスとの通信に用いるポート番号を登録します。BOMヘルパーサービスのポート番号に関する詳細は、'BOM for Windows Ver.8.0 ユーザーズマニュアル'を参照ください。
6. "パスワード"フィールドに、BOMヘルパーサービスに参照モードのパスワードが指定されている場合に、該当するパスワードを入力します。
7. "インスタンス名"フィールドに、監視対象のインスタンスを下記のどちらかの手段で設定します。
  - "インスタンス名"を入力します。
  - "インスタンス名"フィールドにカーソルを合わせカーソルキーの上もしくは下を押下すると、手順4.で指定した"監視対象コンピューター"に登録されている"インスタンス"がリスト表示されるので、リストから登録したいインスタンス名を選択します。
8. "表示名"フィールドに、BOM 集中監視コンソールに表示させるインスタンス名を入力します。
9. "ポーリング設定"は、下記のどちらかを選択します。
  - "個別のポーリング設定を行う"  
"ラジオボタンを選択した場合インスタンスが所属するグループの"ポーリング有効/無効"設定内容に影響を受けなくなるため、手順10.のインスタンスの"ポーリング有効/無効"の設定を最優先に採用します。
  - "グループの設定に従う"ラジオボタンを選択した場合  
インスタンスが所属するグループの"ポーリング有効/無効"設定内容に従います。
10. "ポーリング有効/無効"は、手順9.で"個別のポーリング設定を行う"ラジオボタンを選択した場合に設定ができます。なお、ポーリングとは対象インスタンスのBOMヘルパーサービスと通信をしてステータス情報を収集することを指します。
  - "有効"ラジオボタンを選択した場合  
インスタンスのポーリングを"有効"にします。
  - "無効"ラジオボタンを選択した場合  
インスタンスのポーリングを"無効"にします。
11. "ポーリング間隔"は、手順10.で"有効"ラジオボタンを選択した場合に、インスタンスのステータス情報を収集する間隔を設定することができます。
12. [変更前に戻る]ボタンをクリックすると、手順2.~11.の変更内容を破棄することができます。
13. [確認]ボタンをクリックすると確認画面が表示されるため、問題がなければ[確定]ボタンをクリックします。

## C. インスタンスの削除

作成したインスタンスを削除することができます。

1. "インスタンスの編集"画面の[削除]ボタンをクリックし、"インスタンス情報削除"画面を表示させます。



インスタンス情報削除	
グループ	/root/関東本社
インスタンス種別	BOM 8.0 基本製品 インスタンス
監視対象コンピューター	[IP address]
ヘルパーサービスポート	20080
パスワード	●●●●●●●●
インスタンス名	WIN-NBIAMPVUFID
表示名	AP-01
ポーリング設定	グループの設定に従う
ポーリング有効/無効	-
ポーリング間隔	-

2. 問題がなければ[確定]ボタンをクリックします。

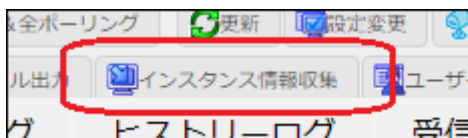
### (3) インスタンス設定-インスタンス情報収集

インスタンスを設定する方法には"インスタンスの編集"、"インスタンス情報収集"および、"インポート"の3種類があり、本章では"インスタンス情報収集"方法を解説します。

BOM 5.0~BOM 8.0を導入しているコンピューターを検索し、その検索結果よりインスタンスを追加することができます。

- "インスタンスの編集"は、'[インスタンスの設定-インスタンスの編集画面](#)'を参照してください。
- "インポート"方法は、'[設定のエクスポート/インポート](#)'を参照してください。
- 登録できるインスタンスの条件については、'[インスタンス](#)'も参照してください。

1. BOM 集中監視コンソールのコマンドバー"インスタンス情報収集"をクリックして"インスタンス情報収集"画面を表示します。



2. [探索]ボタンをクリックし、ネットワーク内のコンピューターを検索後、リスト表示します。

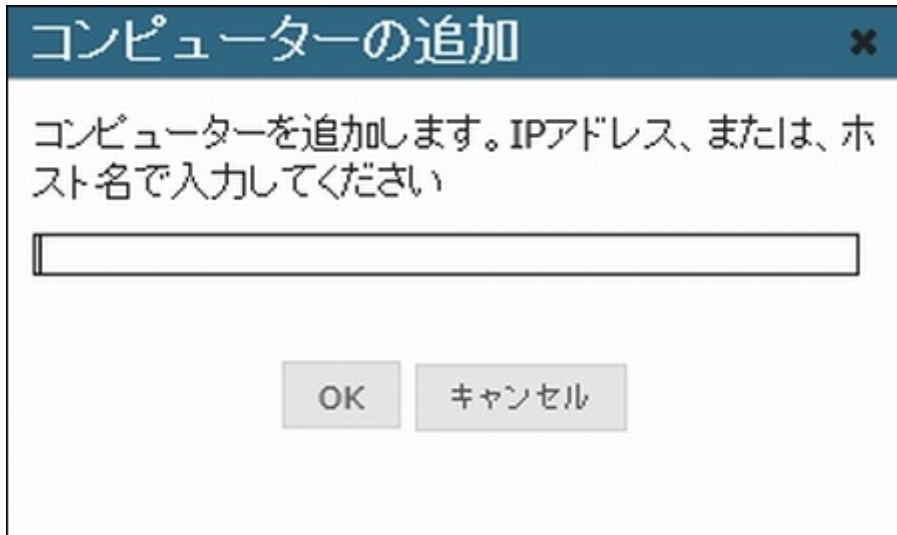
### インスタンス情報収集 ×

インスタンスを収集するコンピューターを選択してください。

<input type="checkbox"/> コンピューター
<input type="checkbox"/> [不明]
<input type="checkbox"/> [不明]
<input type="checkbox"/> [不明]
<input type="checkbox"/> [不明]
<input type="checkbox"/> [不明]
<input type="checkbox"/> [不明]
<input type="checkbox"/> [不明]

※ インスタンス情報収集実行時には、集中監視Webサービスが動作しているコンピューターのARPテーブルから、接続先コンピューター情報を取得した後ポートの確認を行っています。このため、集中監視Webサービスが動作するコンピューター上のARPテーブルにキャッシュされていないコンピューターは表示されない場合があります。

3. [コンピューターの追加]ボタンをクリックすると、"コンピューターの追加"画面を表示させて[探索]ボタンでは検出できなかったコンピューターを追加することができます。IPアドレス、またはコンピューターのホスト名を入力します。



コンピューターの追加

コンピューターを追加します。IPアドレス、または、ホスト名で入力してください

OK キャンセル

4. "インスタンス情報収集"画面で、インスタンスを登録したいコンピューターの左のチェックボックスにチェックを入れます。
- すべてのコンピューターを一度にチェックしたい場合は"コンピューター"フィールドの左のチェックボックスにチェックを入れます。
  - チェックを入れたコンピューターのBOM 5.0~8.0に登録されているインスタンスが、BOM 集中監視コンソールのインスタンスとして登録されます。
5. "インスタンス情報収集"画面で[次へ]ボタンをクリックすると、"収集するインスタンスの種類とパスワードを指定してください"画面が表示されるので、登録したいインスタンスの種類を選択して[次へ]ボタンをクリックします。
- 選択方法は、"BOMのバージョン"チェックボックスにチェックを入れた上で、"基本製品インスタンス"/"Linuxオプションインスタンス"/"VMwareオプションインスタンス"のチェックボックスにチェックを入れます。
  - 手順4.で選択したコンピューターに複数のインスタンスが登録されている場合、該当するインスタンスのチェックボックスにチェックを入れます。

- 画面をスクロールするとBOM 8.0インスタンスも指定できます。

### インスタンス情報収集

収集するインスタンスの種類とパスワードを指定してください。

<input checked="" type="checkbox"/> <b>BOM 5.0</b>	
ヘルパーサービス ポート番号	<input type="text" value="20050"/>
参照モード パスワード	<input type="text" value="..."/>
インスタンス種別	<input checked="" type="checkbox"/> 基本製品 インスタンス <input checked="" type="checkbox"/> Linuxオプション インスタンス <input checked="" type="checkbox"/> VMwareオプション インスタンス
<input checked="" type="checkbox"/> <b>BOM 6.0</b>	
ヘルパーサービス ポート番号	<input type="text" value="20060"/>
参照モード パスワード	<input type="text"/>
インスタンス種別	<input checked="" type="checkbox"/> 基本製品 インスタンス <input checked="" type="checkbox"/> Linuxオプション インスタンス <input checked="" type="checkbox"/> VMwareオプション インスタンス
<input checked="" type="checkbox"/> <b>BOM 7.0</b>	
ヘルパーサービス ポート番号	<input type="text" value="20070"/>
参照モード パスワード	<input type="text"/>
	<input checked="" type="checkbox"/> 基本製品 インスタンス

戻る      次へ      閉じる

6. 手順5.までの条件に基づき収集するインスタンスの展開先のグループを指定します。

- 既に存在するグループ名を指定することはできません。



- インスタンス情報の収集にかかる目安時間が表示されます。

### インスタンス情報収集

収集したインスタンスを追加する新しいグループを指定してください。

グループの指定	
親グループ	<input type="text" value="/root"/>
グループ名	<input type="text" value="AutoGathering_20220310212728"/>

**インスタンス情報の収集には約10秒程度かかります。  
開始ボタン押下後、処理完了までそのままの状態でお待ちください。**

7. [開始]ボタンをクリックすると、インスタンス情報の収集が開始され、収集処理が完了するとBOM 集中監視コンソール上から手順5.で指定したグループと該当するインスタンスを確認することができます。

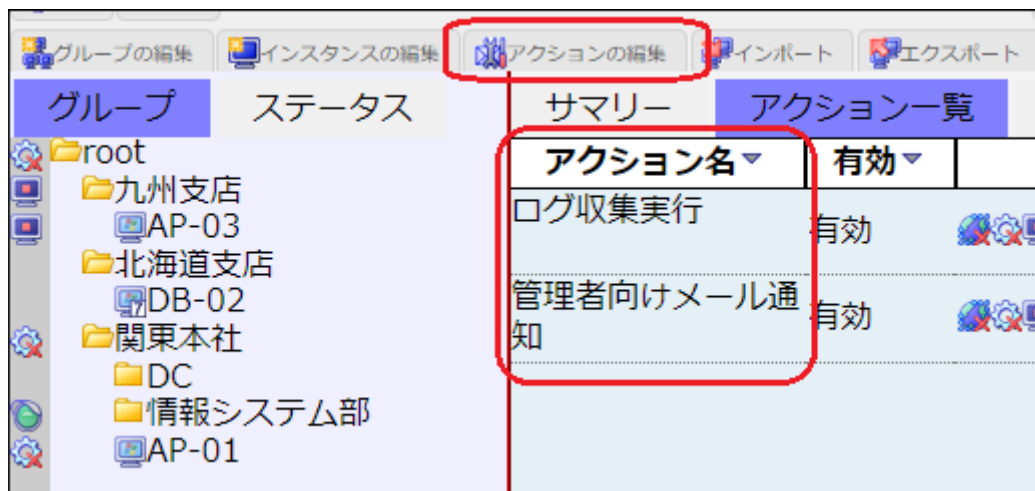
## (4) アクションの設定

アクションを設定する方法には"アクションの編集"および、"インポート"の2種類があり、本章では"アクションの編集"方法を解説します。

- "インポート"方法は、'[設定のエクスポート/インポート](#)'を参照してください。

BOM 集中監視コンソールのアクションを"追加"、"変更"、"削除"する操作を行う際は、下記のどちらかの手段で"アクションの編集"画面を表示します。"アクションの編集"画面には、既に設定済みのアクションのリストが表示されます。

- BOM 集中監視コンソールのコマンドバーの"アクションの編集"をクリック
- アクションを設定したグループをクリックし、"アクション一覧"をクリック後、リスト表示された"アクション名"をクリック



↓

## アクションの編集



	グループ	アクション名	有効/無効	概要
<input type="radio"/>	/root/関東本社	ログ収集実行	有効	カスタムアクション
<input type="radio"/>	/root/関東本社	管理者向けメール通知	有効	メール送信

追加

変更

削除

閉じる

## A. アクションの追加-共通設定

"メール送信アクション"と"カスタムアクション"について、追加設定の共通部分を説明します。

1. "アクションの編集"画面の[追加]ボタンをクリックし、"アクション新規追加"画面を表示します。

The screenshot shows a dialog box titled "アクションの編集" (Action Edit) with a close button (X) in the top right corner. Inside the dialog, there is a section titled "アクション新規追加" (Add New Action). Below this title, there are several fields and options:

- グループ** (Group): A text input field containing the value "/root".
- アクション名** (Action Name): An empty text input field.
- アクション有効/無効** (Action Enabled/Disabled): Two radio buttons, "有効" (Enabled) and "無効" (Disabled). The "有効" radio button is selected.
- 条件** (Condition): A list of checkboxes with corresponding status icons:
  - コンピューター接続エラー (Computer connection error)
  - ヘルパーサービス接続エラー (Helper service connection error)
  - 監視サービス停止中 (Monitoring service stopped)
  - 失敗 (Failure)
  - 危険 (Danger)
  - 注意 (Warning)
  - 正常 (Normal)

2. "グループ"フィールドに、アクションを適用したいグループを設定します。
  - "/root"が頂点です。グループの階層が深くなる場合、"/"でグループを繋いでいきます。
3. "アクション名"フィールドに、BOM 集中監視コンソールに表示するアクション名を入力します。
4. "アクション有効/無効"は、下記のどちらかを選択します。
  - "有効"ラジオボタンを選択した場合  
グループ配下に含まれるすべてのインスタンスを対象に手順5.の"条件"に合致した場合、指定したアクションが実行されます。
  - "無効"ラジオボタンを選択した場合  
指定したアクションは実行されません。
5. "条件"には、下記のいずれかのステータスで変化が生じた場合、アクションを実行させる条件を指定します。  
ステータスの詳細は、'[インスタンスのステータス表示](#)'を参照してください。
  - "コンピューター接続エラー"は、コンピューターが見つからない場合
  - "ヘルパーサービス接続エラー"は、BOMヘルパーサービスが停止、ポートやパスワードの設定が不適切などの場合
  - "監視サービス停止中"は、監視サービスが停止した場合
  - "失敗"は、監視ステータスが失敗に変化した場合
  - "危険"は、監視ステータスが危険に変化した場合
  - "注意"は、監視ステータスが注意に変化した場合
  - "正常"は、監視ステータスが正常に変化した場合

6. "アクション種別"では、"メール送信"または"カスタムアクション"を選択します。

以降はそれぞれの設定方法へ進んでください。

- [アクションの追加-メール送信](#)
- [アクションの追加-カスタムアクション](#)

## B. アクションの追加-メール送信

'[アクションの追加-共通設定](#)'以降の、新規でメール送信アクションを追加する手順です。

※ BOM 集中監視コンソールの"メール送信"アクションでは、認証方式にOAuth2.0は使用できません。

※ BOM 集中監視コンソールの"メール送信"アクションは、SSLプロトコルとしてTLSv1.2およびTLSv1.3のみに対応し、TLSv1.0およびTLSv1.1は使用できません。TLSv1.2またはTLSv1.3に対応するメールサーバーを指定してください。

1. "アクション種別"には、"メール送信"を選択します。

2. "SMTPサーバー"フィールドには、メール送信先SMTPサーバーを指定します。

3. "ポート"フィールドには、"1"~"65535"でメール送信の通信ポートを指定します。

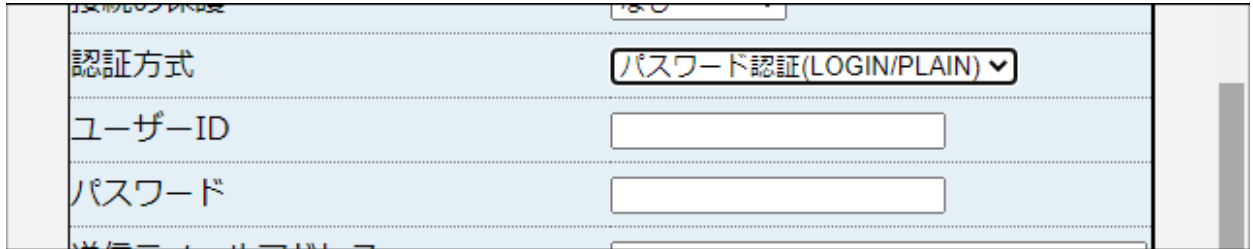
4. "接続の保護"は、下記のいずれかを選択します。

- "なし"を選択した場合  
手順3.の"ポート"に、"25"が自動設定されます。
- "SSL/TLS"を選択した場合  
手順3.の"ポート"に、"465"が自動設定されます。

- "STARTTLS"を選択した場合  
手順3の"ポート"に、"587"が自動設定されます。

5. "認証方式"は、"認証なし"と"パスワード認証 (LOGIN/PLAIN)"のどちらかを選択します。

- "パスワード認証 (LOGIN/PLAIN)"を選択した場合、下記の"ユーザーID"と"パスワード"入力フィールドが表示されるので、SMTPサーバーへの"ユーザーID"と"パスワード"を入力します。



6. "送信元メールアドレス"フィールドには、メールの送信元メールアドレスを入力します。

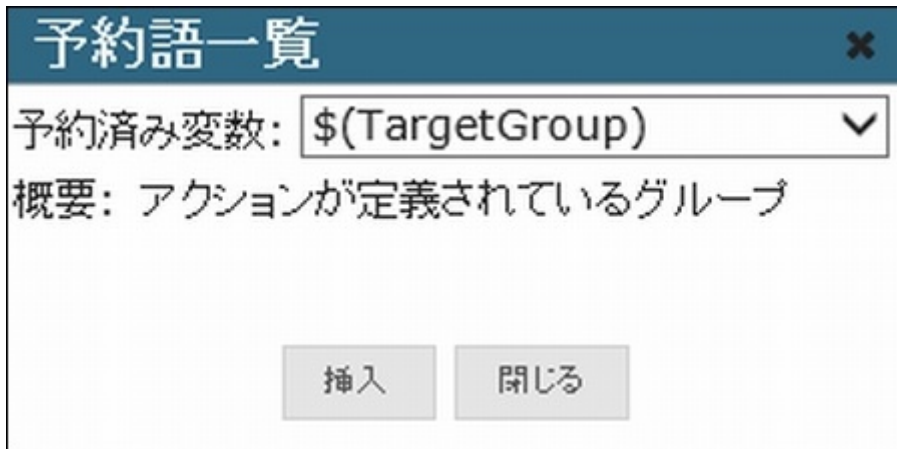
7. "宛先メールアドレス"フィールドには、メールの宛先を入力します。

- 複数の送信先を指定する場合は、入力するメールアドレスとメールアドレスの間を、カンマ区切りで入力します。

8. "件名"フィールドには、メールの件名を入力します。

9. "メッセージ本文"フィールドには、メール本文を入力します。

- [予約語一覧]ボタンをクリックすると、下記の"予約語一覧"画面が表示され、対象の変数を選択して[挿入]ボタンをクリックすることで"メッセージ本文"フィールドに変数名を設定することができます。



(予約済み変数一覧)

予約済み変数名	説明
\$(TargetGroup)	アクションが定義されているグループのパスを表示します。
\$(ActionName)	アクション名を表示します。
\$(InstanceID)	アクションのトリガーとなったBOMのインスタンス名を表示します。
\$(InstanceDisplayName)	アクションのトリガーとなったインスタンスの集中監視上での表示名を表示します。
\$(Status)	アクションのトリガーとなったステータスのうち最悪ステータスを表示します。

予約済み変数名	説明
\$(CurrentTime)	アクション実行時の現在時刻を表示します。実質的には\$(RunTime)と同じ値となります。
\$(RunTime)	アクション実行時刻を表示します。実質的には\$(CurrentTime)と同じ値となります。
\$(FullComputerName)	集中監視Webサービスが起動しているコンピューターのコンピューター名を表示します。
\$(InstallDir)	BOMのインストールディレクトリを表示します。

10. [テスト実行]ボタンをクリックすると、設定した条件でメール送信アクションのテスト実行を行い、"テスト実行結果"フィールドに結果を表示します。

- 予約語一覧から登録した予約済み変数の置き換えは行わず、変数の文字列がそのまま出力されます。
- テスト実行時のタイムアウト時間は1分です。

11. [確認]ボタンをクリックすると、確認画面が表示されるため、問題がなければ[確定]ボタンをクリックします。

## C. アクションの追加-カスタムアクション

'[アクションの追加-共通設定](#)'以降の、新規でカスタムアクションを追加する手順です。

1. "アクション種別"には、"カスタムアクション"を選択します。

アクションの編集

反映  
 注意  
 正常

アクション種別: カスタムアクション

プログラム名:

引数

作業フォルダー:

同時多重実行の禁止:  同時多重実行の禁止

テスト実行結果

2. "プログラム名"フィールドには、カスタムアクションで実行させたい実行プログラムを絶対パスで指定します。
  - 実行プログラムは、集中監視Webサービスが起動しているコンピューターに配置する必要があります。
3. "引数"フィールドには、手順2.で指定した実行プログラムを実行させた際の引数を指定します。
  - [予約語一覧]ボタンをクリックすると、下記の"予約語一覧"画面が表示され、対象の変数を選択して[挿入]ボタンをクリックすることで"引数"フィールドに変数名を設定することができます。

予約語一覧

予約済み変数: \$(TargetGroup)

概要: アクションが定義されているグループ

(予約済み変数一覧)



予約済み変数名	説明
\$(TargetGroup)	アクションが定義されているグループのパスを表示します。
\$(ActionName)	アクション名を表示します。
\$(InstanceID)	アクションのトリガーとなったBOMのインスタンス名を表示します。
\$(InstanceDisplayName)	アクションのトリガーとなったインスタンスの集中監視上での表示名を表示します。
\$(Status)	アクションのトリガーとなったステータスのうち最悪ステータスを表示します。
\$(CurrentTime)	アクション実行時の現在時刻を表示します。実質的には\$(RunTime)と同じ値となります。
\$(RunTime)	アクション実行時刻を表示します。実質的には\$(CurrentTime)と同じ値となります。
\$(FullComputerName)	集中監視Webサービスが起動しているコンピューターのコンピューター名を表示します。
\$(InstallDir)	BOMのインストールディレクトリを表示します。

4. "作業フォルダー"フィールドには、実行プログラムがファイルを出力する際に既定値で使用するフォルダーを指定することができます。
  - 作業フォルダーは、集中監視Webサービスが起動しているコンピューターのフォルダーを指定します。
5. "同時多重実行の禁止"はチェックボックスにチェックを入れることにより、カスタムアクションがすでに動作していた場合、新たに実行対象となるグループやインスタンスで実行条件にあてはまった状態変化が発生しても、新たに実行したカスタムアクションはスキップされません。
6. [テスト実行]ボタンをクリックすると、設定した条件でカスタムアクションのテスト実行を行い、"テスト実行結果"フィールドに結果を表示します。
  - 予約語一覧から登録した予約済み変数の置き換えは行わず、変数の文字列がそのまま出力されます。
  - テスト実行時のタイムアウト時間は1分です。
7. [確認]ボタンをクリックすると、確認画面が表示されるため、問題がなければ[確定]ボタンをクリックします。

## D. アクションの編集

作成したアクションの内容を編集することができます。

1. "アクションの編集"画面で設定を変更したいアクションをチェックし、[変更]ボタンをクリックすると"アクションの編集"画面が表示されます。



アクション情報変更	
グループ	/root/関東本社
アクション名	ログ収集実行
アクション有効/無効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
条件	<input checked="" type="checkbox"/> コンピューター接続エラー
	<input checked="" type="checkbox"/> ヘルパーサービス接続エラー
	<input checked="" type="checkbox"/> 監視サービス停止中
	<input type="checkbox"/> 失敗
	<input checked="" type="checkbox"/> 危険
	<input checked="" type="checkbox"/> 注意
	<input type="checkbox"/> 正常
アクション種別	カスタムアクション
プログラム名	c:\work\collect-log.bat

確認 変更前に戻す 戻る テスト実行 閉じる

2. 以降の項目説明は下記を参照してください。
  - ['アクションの追加-共通設定'](#)
  - ['アクションの追加-メール送信'](#)
  - ['アクションの追加-カスタムアクション'](#)

## E. アクションの削除

作成したアクションを削除することができます。

1. "アクションの編集"画面で設定を削除したいアクションをチェックし、[削除]ボタンをクリックすると"アクション情報削除"画面が表示されます。



2. 問題がなければ[確定]ボタンをクリックします。

## 10. BOM 集中監視コンソールでのメール受信

BOM 集中監視コンソールでは、メール受信を行うことができます。

使用可能なメール方式は以下のとおりです。

- POP3

- IMAP

- ※ メール受信の際に使用するSSLプロトコルはTLSv1.2およびTLSv1.3のみに対応し、TLSv1.0およびTLSv1.1は使用できません。TLSv1.2またはTLSv1.3に対応するメールサーバーを指定してください。

- ※ メール受信設定は、グループまたはインスタンスに紐づいた設定となります。

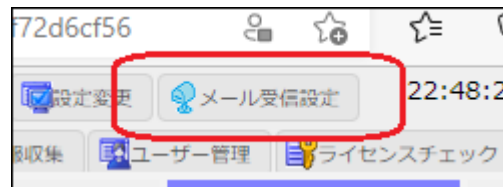
- ※ 受信するメールは、未読のメールすべてを受信します。（過去分でも未読であった場合は受信します。）

- ※ 受信メールはテキスト形式を推奨します。（html形式も受信できますが、タグ情報等が表示されます。）

- ※ 添付ファイルがあるメールの受信は行わないようにしてください、添付ファイルがあった場合添付ファイルは受信されません。

なお、メール受信サーバーで自己署名証明書を使用していた場合、集中監視コンソール側では正常に受信ができません。回避方法については、'[自己署名証明書の設定](#)'を参照してください。

1. BOM 集中監視コンソールのコマンドバーの"メール受信設定"をクリックし、"メール受信設定"画面を表示させます。



## メール受信設定



グループ	メール設定名	有効/無効	サーバー名	ユーザー名	最終受信日時
○/root	通知受信設定	有効	pop.mail.sayte ch.demo	saytech_mail demo	

追加

変更

削除

閉じる

### (1) メール受信設定新規

1. "メール受信設定"画面で、[追加]ボタンをクリックし、"メール受信設定新規追加"画面を表示させます。

### メール受信設定

#### メール受信設定新規追加

グループ・インスタンス	<input type="text" value="/root"/>
受信プロトコル	<input type="text" value="POP3"/>
メールサーバー	<input type="text"/>
受信ポート	<input type="text" value="110"/>
ユーザー名	<input type="text"/>
パスワード	<input type="text"/>
表示名	<input type="text"/>
接続の保護	<input type="checkbox"/> 接続をSSL/TLSで保護する
メール受信時削除	<input type="checkbox"/> 受信時にサーバー上のメッセージを削除する
受信有効/無効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

2. "グループ・インスタンス"フィールドに、メール受信機能を適用したいグループを設定します。
  - "/root"が頂点です。グループの階層が深くなる場合、"/"でグループを繋いでいきます。
3. "受信プロトコル"プルダウンでは、受信メールサーバーのプロトコルを"POP3"または"IMAP"から選択します。
4. "メールサーバー"フィールドには、メール受信サーバーのアドレスを入力します。
5. "受信ポート"フィールドには、項番4で設定した受信サーバーのポート番号を入力します。
6. "ユーザー名"フィールドには、受信に使用するユーザー名を入力します。
7. "パスワード"フィールドには、受信に使用するパスワードを入力します。
8. "表示名"フィールドには、メール受信設定の設定一覧に表示されるメール設定名を入力します。
9. "接続の保護"チェックボックスは、受信メールサーバーへ対し接続する際、SSL/TLSで接続するかを選択します。SSL/TLSで接続する場合にはチェックボックスのチェックを入れてください。SSL/TLSで接続しない場合には、チェックボックスのチェックを外してください。
10. "メール受信時削除"チェックボックスは、集中監視コンソールでメールを受信した際、メールサーバー上にあるメールを削除するかを選択します。集中監視コンソールでメールを受信後、メールサーバー上のメールを削除する場合にはチェックボックスのチェックを入れてください。メールを受信後、メールサーバー上のメールを削除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。
11. "受信有効/無効"ラジオボタンは、設定したメール受信機能を有効/無効にすることができます。設定を有効にしたい場合には、"有効"ラジオボタンに、設定を無効にしたい場合には、"無効"ラジオボタンを選択してください。
12. "受信間隔"プルダウンは、設定した内容の内容でメールを受信する間隔を選択します。選択できるのは"1分"~"60分"までの間です。

## (2) メール受信設定変更

作成したメール受信設定の内容を編集することができます。

"メール受信設定"画面で、設定の変更を行いたいメール受信設定をチェックし、[変更]ボタンをクリックすると"メール受信設定変更"画面が表示されます。

各項目の内容については'[メール受信設定新規](#)'を参照してください。

### メール受信設定

#### メール受信設定変更

グループ・インスタンス	<input type="text" value="/root"/>
受信プロトコル	<input type="text" value="POP3"/>
メールサーバー	<input type="text" value="pop.mail.saytech.demo"/>
受信ポート	<input type="text" value="110"/>
ユーザー名	<input type="text" value="saytech_maildemo"/>
パスワード	<input type="password" value="....."/>
表示名	<input type="text" value="通知受信設定"/>
接続の保護	<input type="checkbox"/> 接続をSSL/TLSで保護する
メール受信時削除	<input type="checkbox"/> 受信時にサーバー上のメッセージを削除する
受信有効/無効	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

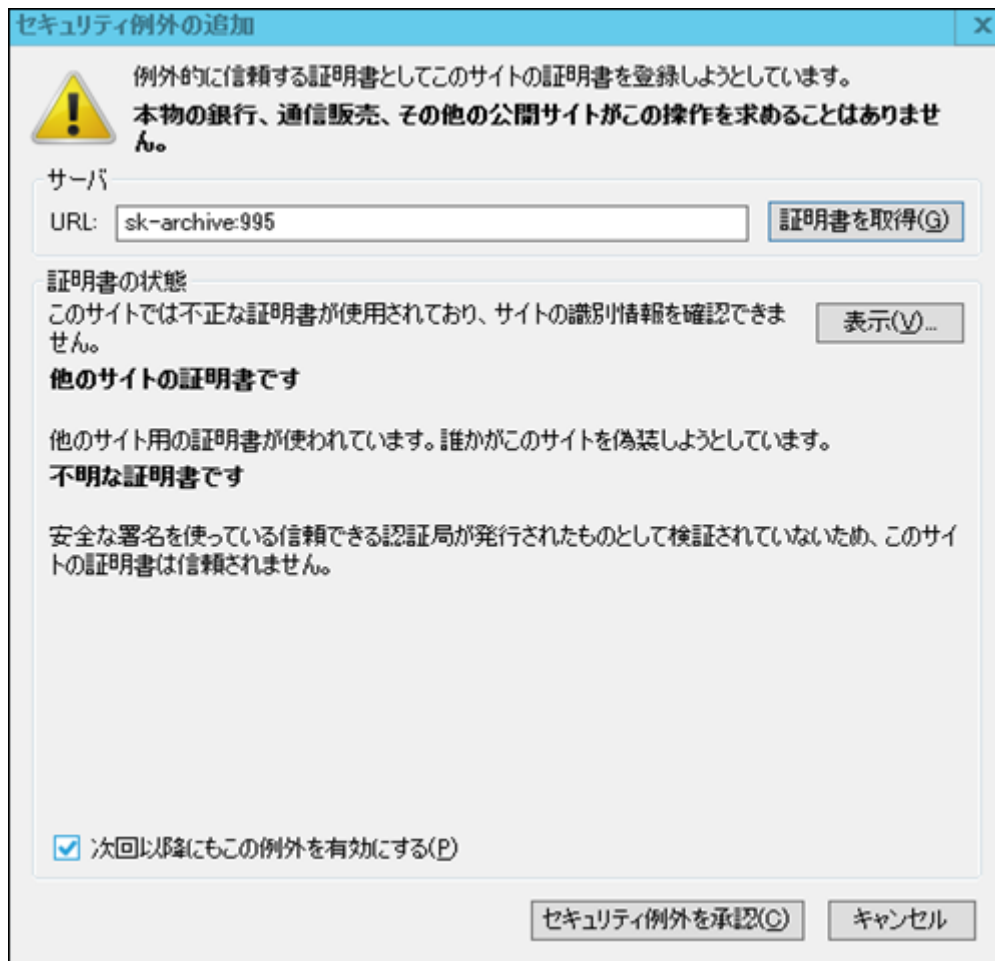
### (3)自己署名証明書の設定

メール受信サーバーで自己署名証明書を使用していた場合、BOM 集中監視コンソールでのメール受信に失敗します。以下の手順を参考に、自己署名証明書の登録をしてください。

#### A. 自己署名証明書の取得について

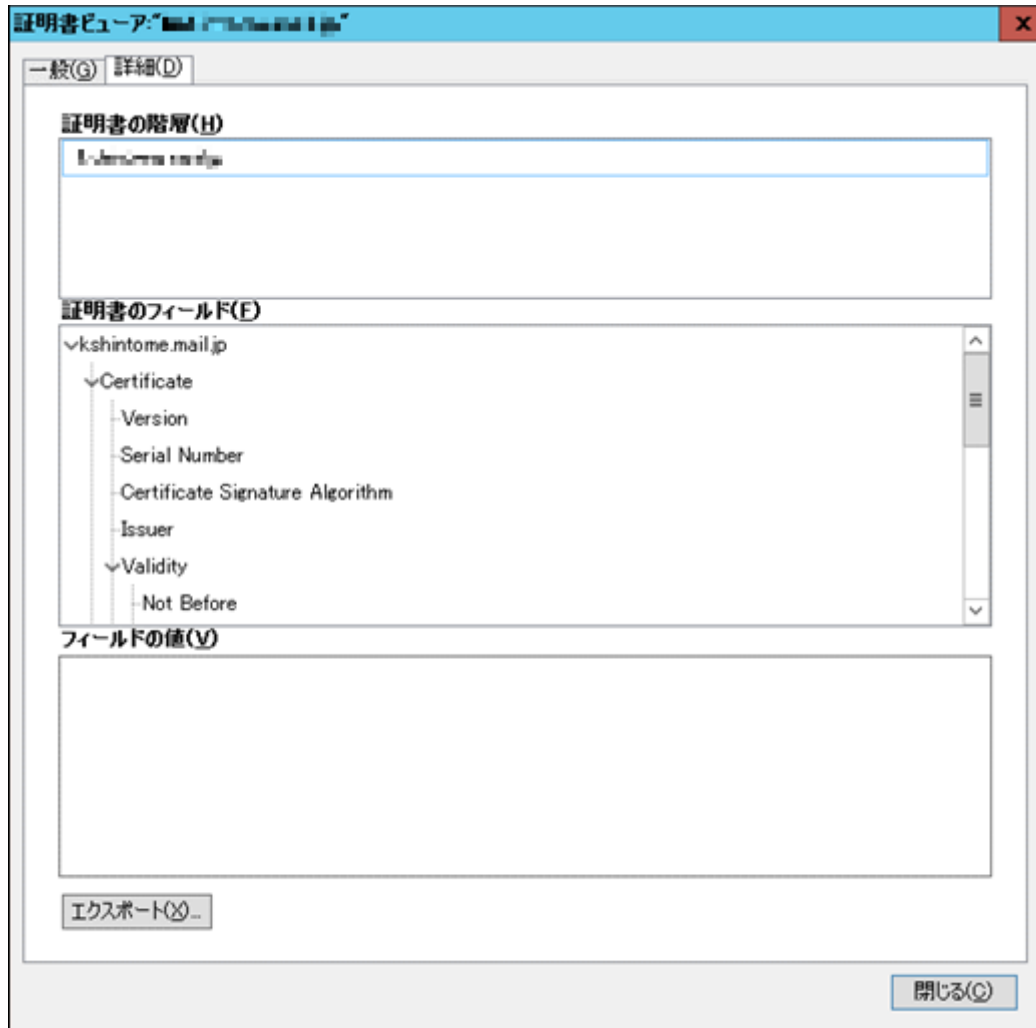
※ 以下はMozilla Thunderbird（Thunderbird）を使用する場合の手順例です。

1. Thunderbirdのメニューから、オプション → アカウントを選択し、アカウント設定からPOP3サーバーを設定します。
2. 受信を行おうとした際、"セキュリティ例外の追加"が表示されますので"表示"を選択します。





3. 証明書ビューアーが表示されますので「詳細」タブを選択後、[エクスポート]ボタンをクリックします。



4. エクスポートされた"cert"ファイルを'[自己署名証明書の設定について](#)'の手順に従い、Java Runtime Environment（以降JRE）に登録します。

## B. 自己署名証明書の設定について

以下の内容に従い、JREに登録をしてください。（赤字部分が入力する値です。）

なお、JREのデフォルトキーストア「jre%lib%security%cacerts」を-keystoreの引数に指定する必要があります。BOMの場合は、「BOMW8%Indicator%jre%lib%security%cacerts」を指定します。

[コマンド例]

※ キーストアファイルのデフォルトパスワードは changeit です。

---

01| C:%Program Files%SAY Technologies%BOMW8%Indicator%jre%bin \*\*keytool -importcert -v -trustcacerts -file c:%test00.crt -keystore cacerts\*\*

02| キーストアのパスワードを入力してください: \*\*changeit\*\*

03| 所有者: CN=test, OU=Department, O=Japanese Government C=JP

04| 発行者: CN=test, OU=Department, O=Japanese Government C=JP

05| シリアル番号: e7825960d3da5860

06| 有効期間の開始日: Sat Feb 26 11:50:14 JST 2022終了日: Fri Mar 25 11:50:14 JST 2022

07| 証明書のフィンガプリント:

08| MD5: 35:C4:32:65:01:A7:39:BC:0C:47:9D:12:03:E3:53:4E

09| SHA1: C6:C0:CA:06:3F:5E:91:11:DE:7C:5A:90:52:24:9A:1F:FA:39:7A:88

10| SHA256:A0:CE:F6:F8:13:94:F3:80:88:F2:01:8E:15:CF:E8:B0:3F:E5:96:0E:D2:3F:40:DD:8A:B6:C0:4  
A:E8:98:B9:09

11| 署名アルゴリズム名: SHA256withRSA

12| バージョン: 1

13| この証明書を信頼しますか。 [いいえ]: \*\*y\*\*

14| 証明書がキーストアに追加されました

15| [cacertsを格納中]

---

## 11. BOM 集中監視コンソールのログ

### (1) ステータスログ

BOM 集中監視コンソールに設定したインスタンスのステータス情報に関する下記のログを表示させることができます。

- 監視サービスの実行状況
- 監視結果のサマリー情報

ツリービューのグループ、もしくはインスタンスをクリックした後に、詳細ビューに表示される「ステータスログ」タブをクリックすることで、ステータスログリストを表示させることができます。

- グループをクリックした場合、該当グループと該当グループ配下に所属するすべてのインスタンスがステータスログの表示対象です。

サマリー	アクション一覧	ステータスログ	ヒストリーログ	アクションログ	受信ログ	
<input type="checkbox"/>	表示名	時刻	ステータス	概要		
<input type="checkbox"/>	AP-01	2022/03/11 10:49:15		監視サービス実行中(失敗:0/危険:0/注意:0/正常:14)		
<input type="checkbox"/>	DB-02	2022/03/11 10:48:35		監視サービスが停止中、またはインスタンス情報が取得できません。		
<input type="checkbox"/>	DB-06	2022/03/11 10:48:35		監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)		
<input type="checkbox"/>	AP-01	2022/03/11 10:48:15		監視サービス実行中(失敗:0/危険:0/注意:0/正常:14)		

- インスタンスをクリックした場合、選択したインスタンスのみがステータスログの表示対象です。

サマリー	ステータス	ステータスログ	ヒストリーログ	受信ログ			
<input type="checkbox"/>	時刻	ステータス					概要
<input type="checkbox"/>	2022/03/11 10:51:35		0	0	0	15	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)
<input type="checkbox"/>	2022/03/11 10:50:35		0	0	0	15	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)
<input type="checkbox"/>	2022/03/11 10:49:36		0	0	0	15	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)
<input type="checkbox"/>	2022/03/11 10:48:35		0	0	0	15	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)

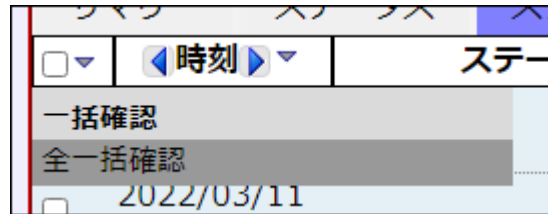
ステータスログの"□" (チェックボックス) は、チェックを入れることで該当するログが既に確認済みであることを後から判別するために使用します。

ステータスログを確認済み扱いにする方法は、下記の3種類です。

- 該当するステータスログのみ、確認済み扱いにしたい場合  
該当するステータスログの左端のチェックボックスにチェックを入れます。
- 現時点で画面に表示されているステータスログを確認済み扱いにしたい場合  
項目名欄のチェックボックスにチェックを入れます。

<input checked="" type="checkbox"/>	表示名
-------------------------------------	-----

- 対象インスタンスの過去を含むすべてのステータスログを確認済み扱いにしたい場合  
項目名欄の"□"にある"▼"をクリックし、表示される"全一括確認"をクリックします。



ステータスログに表示される各項目の情報は下記のとおりです。

また、各項目の右にある"▼"をクリックすることで、昇順/降順による並び替えや、キーワードによる部分一致で絞り込み検索を行うことができます。

- "表示名"

グループをクリックしてステータスログを表示させた場合、インスタンス名が表示されます。インスタンスをクリックしてステータスログを表示させた場合、"表示名"項目は非表示です。



- "時刻"

インスタンスに対して、ポーリングを行った時刻が表示されます。ログ表示件数を超えるログが存在する場合、"時刻"の両隣にある矢印（過去時間表示、未来時間表示）が表示され、矢印をクリックすると、リストに表示されていない過去や、過去から現在のステータスログを表示させることができます。

時刻の範囲指定は、"yyyy/MM/dd hh:mm:ss"形式で入力します。（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）



- "ステータス"

インスタンスの監視データに含まれるステータスアイコンが表示されます。

**ステータス** ▼

**並び替え**  
昇順  
降順

**絞り込み**  
 コンピュータ接続エラー  
 ヘルパーサービス接続エラー  
 監視サービス停止中  
 失敗  
 危険  
 注意  
 正常

確認の絞り込みを行わない  
 確認済みを絞り込む  
 未確認を絞り込む

絞り込み 絞り込み解除

- "ステータス"アイコン

インスタンスをクリックしてステータスログを表示させた場合のみ表示します。

"ステータス"アイコンと"ステータス"ごとのサマリー件数が表示されます。

失敗	危険	注意	正常	
5	3	1		並び替え 昇順 降順
0	0	0		絞り込み
0	0	0		絞り込み 絞り込み解除

- "概要"監視

インスタンスのポーリング結果と、ステータスのサマリー情報が表示されます。

概要の内容が長い場合に、ツールチップで全文を表示させることができます。

**概要** ▼

並び替え	部換:3/
昇順	
降順	部換:0/
絞り込み	
	はイン
絞り込み 絞り込み解除	(SQL=

"表示名"に表示されているインスタンス名をクリックすると、インスタンスのサマリー情報画面を表示させることができます。

インスタンスのサマリー情報画面の詳細は、'[「サマリー」タブ](#)'を参照してください。

## (2) ヒストリーログ

BOM 集中監視コンソールに設定したインスタンスのヒストリーログを表示させることができます。ヒストリーログの詳細については、'BOM for Windows Ver.8.0 ユーザーズマニュアル'を参照してください。

ツリービューのグループ、もしくはインスタンスをクリックした後に、詳細ビューに表示される「ヒストリーログ」タブをクリックすることで、ヒストリーログリストを表示させることができます。

- グループをクリックした場合、グループに所属するすべてのインスタンスがヒストリーログの表示対象です。

サマリー	アクション一覧	ステータスログ	ヒストリーログ	アクションログ	受信ログ
タイプ▼	表示名▼	日時▼	カテゴリ▼	サマリー▼	
情報	AP-01	2022/03/11 09:32:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WI	
警告	DB-06	2022/03/11 09:10:27	監視	監視 'IPアドレスまたは機器名称1 応答時間'のステータスが 危険 に変化しました。 ID:	
情報	AP-01	2022/03/11 09:02:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WI	
情報	AP-01	2022/03/11 08:32:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WI	

- インスタンスをクリックした場合、選択したインスタンスのみがヒストリーログの表示対象です。

サマリー	ステータス	ステータスログ	ヒストリーログ	受信ログ
タイプ▼	日時▼	カテゴリ▼	サマリー▼	
情報	2022/03/11 11:02:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN-NBIAMPVUFID 開始時刻: 11:02:36	
情報	2022/03/11 10:33:22	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN-NBIAMPVUFID 開始時刻: 10:32:36	
情報	2022/03/11 10:02:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN-NBIAMPVUFID 開始時刻: 10:02:36	
情報	2022/03/11 09:32:37	サービス	BOM Archive Service:アーカイブが終了しました。 PID: 2076 インスタンス ID: WIN-NBIAMPVUFID 開始時刻: 09:32:36	

ヒストリーログに表示される各項目の情報は下記のとおりです。

また、各項目の右にある"▼"をクリックすることで、昇順/降順による並び替えや、キーワードによる部分一致で絞り込み検索を行うことができます。

- "タイプ"

ヒストリーログのタイプは、"エラー"、"警告"、"情報"のどれかです。



- "表示名"

グループをクリックして履歴ログを表示させた場合、インスタンス名が表示されます。また、インスタンスをクリックして履歴ログを表示させた場合、"表示名"項目は非表示です。

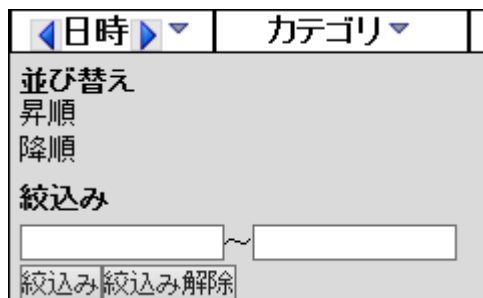


- "日時"

該当する履歴ログが出力された日時が表示されます。

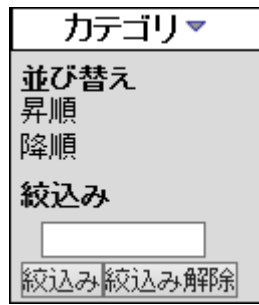
ログ表示件数を超えるログが存在する場合、"日時"の両隣にある矢印（過去時間表示、未来時間表示）が表示され、矢印をクリックすると、リストに表示されていない過去や、過去から現在の履歴ログを表示させることができます。

- 日時の範囲指定は、"yyyy/MM/dd hh:mm:ss"形式で入力します。（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）



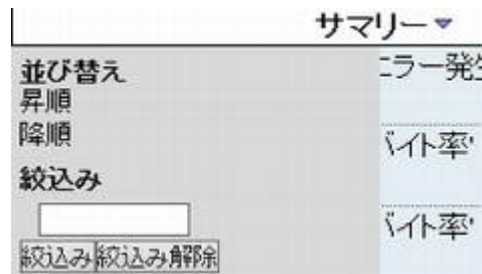
- "カテゴリ"

履歴ログのカテゴリである"サービス"、"監視"、"アクション"のどれかが表示されます。



- "サマリー"

ヒストリーログのメッセージに出力される内容が表示されます。



"表示名"に表示されているインスタンス名をクリックすると、インスタンスのサマリー情報画面を表示させることができます。インスタンスのサマリー情報画面の詳細は'[「サマリー」タブ](#)'を参照してください。



### (3) アクションログ

BOM 集中監視コンソールに設定したアクションの実行結果を表示させることができます。

ツリービューのグループをクリックした後に、詳細ビューに表示される「アクションログ」タブをクリックすることで、アクションログリストを表示させることができます。

- インスタンスにはアクションを関連付けることができないため、インスタンスをクリックした際に「アクションログ」タブは非表示です。

サマリー	アクション一覧	ステータスログ	履歴ログ	アクションログ	受信ログ
日時	アクション名	トリガー	結果	コード	概要
2022/03/10	ログ収集実行	[] AP-01	失敗	0xFFFFFFFF	外部コマンドの実行に失敗しました。 ("c:¥work¥collect-log.bat" )
2022/03/10	ログ収集実行	[] AP-01	成功	0x0	アクションは正常に終了しました。
2022/03/10	ログ収集実行	[] AP-01	成功	0x0	アクションは正常に終了しました。

アクションログに表示される各項目の情報は下記のとおりです。

また、各項目の右にある"▼"をクリックすることで、昇順/降順による並び替えや、キーワードによる部分一致で絞り込み検索を行うことができます。

- "日時"

アクションが実行された日時が表示されます。ログ表示件数を超えるログが存在する場合、"日時"の両隣にある矢印（過去時間表示、未来時間表示）が表示され、矢印をクリックすると、リストに表示されていない過去や、過去から現在のアクションログを表示させることができます。

日時の範囲指定は、"yyyy/MM/dd hh:mm:ss"形式で入力します。（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）

◀日時▶	アクション名
並び替え	
昇順	
降順	
絞り込み	
<input type="text"/> ~ <input type="text"/>	
絞り込み 絞り込み解除	

- "アクション名"

アクション名が表示されます。

アクション名 ▼
並び替え
昇順
降順
絞込み
<input type="text"/>
絞込み 絞込み解除

- "トリガー"

アクションがどのインスタンスのステータスで起動したのかが表示されます。また、BOM 集中監視コンソールでインスタンスを削除した場合、該当インスタンスのトリガー欄には"削除されました"と表示されます。

トリガー ▼	結果 ▼
並び替え	
昇順	
降順	
絞込み	
インスタンス名	
<input type="text"/>	
<input type="checkbox"/> コンピューター接続エラー	
<input type="checkbox"/> ヘルパーサービス接続エラー	
<input type="checkbox"/> 監視サービス停止中	
<input type="checkbox"/> 失敗	
<input type="checkbox"/> 危険	
<input type="checkbox"/> 注意	
<input type="checkbox"/> 正常	
絞込み 絞込み解除	

- "結果"

アクションの実行結果は、"成功"、"エラー"、"失敗"のどれかが表示されます。

結果 ▼	コード
並び替え	
昇順	
降順	
絞込み	
<input type="checkbox"/> 成功	
<input type="checkbox"/> エラー	
<input type="checkbox"/> 失敗	
絞込み 絞込み解除	

- "コード"

アクションの実行結果のコードが表示されます。コードによる絞込みを行うことはできません。

- "概要"

アクションの実行結果の実行メッセージが表示されます。



"トリガー"に表示されているインスタンス名をクリックすると、インスタンスのサマリー情報画面を表示させることができます。インスタンスのサマリー情報画面の詳細は'[「サマリー」タブ](#)'を参照してください。

## (4) 受信ログ

BOM 集中監視コンソールで設定したメール受信のログを確認することができます。

メール受信を設定したツリービューのグループまたは監視インスタンスをクリックした後に、詳細ビューに表示される「受信ログ」タブをクリックすることで、受信ログリストを表示させることができます。

サマリー	アクション一覧	ステータスログ	履歴ログ	アクションログ	受信ログ
タイプ▼	件名▼	送信日時▼	送信元▼	本文▼	
 testmail	閾値変更	2022/02/14 17:16:56	say tech test@yok. on.jp	DB-01 プロセッサしきい値を変更しました	
 testmail	test	2022/02/14 17:16:11	say tech test@yok. on.jp	テストメール	
 testmail	testmail	2022/02/14 17:15:50	say tech test@yok. on.jp	テストメール	

- "タイプ"

メール受信設定画面で設定した表示名が表示されます。

タイプ▼	件名▼
並び替え 昇順 降順	
絞り込み <input type="text"/>	
<input type="button" value="絞り込み"/> <input type="button" value="絞り込み解除"/>	

- 件名

メール受信時に記載されているメールの件名が表示されます。

件名▼	送信日時▼
並び替え 昇順 降順	
絞り込み <input type="text"/>	
<input type="button" value="絞り込み"/> <input type="button" value="絞り込み解除"/>	

- 送信日時

メール送信されたメール送信日時が表示されます。

送信日時▼	送信元▼
並び替え 昇順 降順	
絞り込み <input type="text"/>	
<input type="button" value="絞り込み"/> <input type="button" value="絞り込み解除"/>	

- 送信元

メール送信元のアドレスが表示されます。

送信元 ▼	本文 ▼
<b>並び替え</b> 昇順 降順	
<b>絞り込み</b> <input type="text"/>	
<input type="button" value="絞り込み"/> <input type="button" value="絞り込み解除"/>	

- 本文

メール本文が表示されます。

本文 ▼
<b>並び替え</b> 昇順 降順
<b>絞り込み</b> <input type="text"/>
<input type="button" value="絞り込み"/> <input type="button" value="絞り込み解除"/>

## (5) システムログ

BOM 集中監視コンソールのコマンドバーの"システムログ表示"をクリックすることで、システムログリストを表示させることができます。

システムログリストには、BOM 集中監視コンソールの操作履歴や動作に関するログ、BOM 集中監視コンソールのログインパスワードについて有効期限に関する通知が表示されます。

- ログインパスワード有効期限の通知は、有効期限が7日前に達した時点以降、ログイン時に表示されます。ログイン時のみ通知されるため、ログインした状態で7日前となった場合は表示されません。

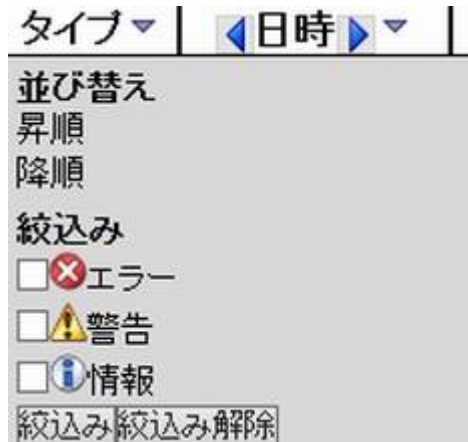
システムログ表示		
タイプ	日時	サマリー
情報	2022/03/11 11:19:48	root[0:0:0:0:0:0:1] グループ /root を変更しました。
情報	2022/03/11 11:19:29	root[0:0:0:0:0:0:1] インスタンス /root/九州支店/DB-02 を変更しました。
情報	2022/03/11 11:19:04	root[0:0:0:0:0:0:1] グループ /root/関東本社/DC を変更しました。
情報	2022/03/11 11:18:43	root ステータスログ100件の確認を行いました。
情報	2022/03/11 11:18:15	root[0:0:0:0:0:0:1] ステータスログ100件の確認を行いました。
エラー	2022/03/11 11:17:45	通知受信設定：メッセージ処理に失敗しました。「Connect failed」
	2022/03/11	通知受信設定：メッセージ処理に失敗しました。「Connect failed」

システムログに表示される各項目の情報は下記のとおりです。

下記の項目で、昇順/降順による並び替えや、キーワードによる部分一致で絞込み検索を行うことができます。

- "タイプ"

BOM 集中監視コンソールの操作履歴のタイプは、"エラー"、"警告"、"情報"のどれかが表示されます。



- "日時"

BOM 集中監視コンソールに対する操作が実行された日時が表示されます。

ログ表示件数を超えるログが存在する場合、"日時"の両隣にある矢印（過去時間表示、未来時間表示）が表示され、矢印をクリックすると、リストに表示されていない過去や、過去から現在のシステムログを表示させることができます。

日時の範囲指定は、"yyyy/MM/dd hh:mm:ss"形式で入力します。（yyyy:西暦年号、MM:月、dd:日、hh:時、mm:分、ss:秒を表します。）



- "サマリー"

BOM 集中監視コンソールに対する操作の具体的な内容が表示されます。



## (6) サマリーログビュー

BOM 集中監視コンソールの下記ログのうち、既定値では30分間分をサマリーログとして表示させることができます。サマリーログビューは、BOM 集中監視コンソールのツリービューと詳細ビューの画面下部に表示されます。

- ステータスログ
- システムログ
- アクションログ
  - サマリーログビューに表示されるログは最新の500件です。

タイプ	ターゲット	日時	カテゴリ	サマリー
情報	DB-06	2022/03/11 11:29:37	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)
エラー	DB-02	2022/03/11 11:29:32	ステータスログ	監視サービスが停止中、またはインスタンス情報が取得できません
エラー	AP-03	2022/03/11 11:29:27	ステータスログ	監視サービスが停止中、またはインスタンス情報が取得できません
情報	AP-01	2022/03/11 11:29:17	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:14)
情報	DB-06	2022/03/11 11:28:37	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)
情報	AP-01	2022/03/11 11:28:17	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:14)
エラー	システム	2022/03/11 11:27:52	システムログ	通知受信設定：メッセージ処理に失敗しました。「Connect failed」
情報	DB-06	2022/03/11 11:27:37	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)
情報	AP-01	2022/03/11 11:27:17	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:14)
情報	DB-06	2022/03/11 11:26:36	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:15)
情報	AP-01	2022/03/11 11:26:16	ステータスログ	監視サービス実行中(失敗:0/危険:0/注意:0/正常:14)

サマリーログビューに表示される各項目の情報は下記のとおりです。

また、各項目の右にある"▼"をクリックすることで、昇順/降順による並び替えや、キーワードによる部分一致で絞り込み検索を行うことができます。

- "タイプ"
  - ログのタイプが表示されます。

タイプ ▼	ターゲット
並び替え	
昇順	
降順	



- "ターゲット"

ログの種類に応じて、下記のどれかが表示されます。

- "インスタンス名"

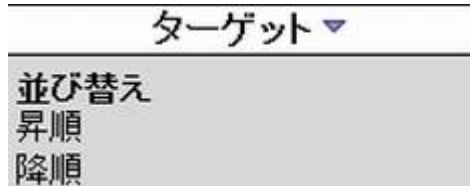
クリックすると、対象インスタンスのステータスログを表示します。

- "システム"

クリックするとシステムログリストを表示します。

- "アクション名"

クリックすると、そのアクションが属するグループのアクションログを表示します。



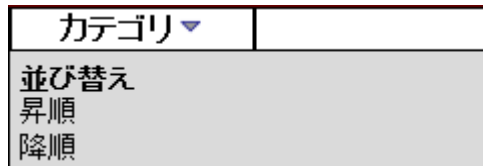
- "日時"

各ログが出力された日時が表示されます。



- "カテゴリ"

ログの種類に応じて、"ステータスログ"、"アクションログ"、"システムログ"のどれかが表示されます。



- "サマリー"

ログの詳細内容が表示されます。



## (7) ログファイル出力

BOM 集中監視コンソールのコマンドバーの"ログファイル出力"より下記のログデータをCSV形式でエクスポートすることができます。

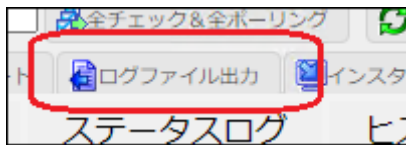
- ステータスログ
- ヒストリーログ
- アクションログ
- 受信ログ

※ インスタンス名やアクション名に機種依存文字やSJISに変換できない文字は空白で出力されます。

※ 受信ログのみUTF-8で出力されます。

※ Internet ExplorerでBOM 集中監視コンソールをご利用の場合、ログファイル出力画面でログファイルを"保存"や"名前を付けて保存"を行った際、"ダウンロードできませんでした"と表示されファイルがダウンロードできないことがあります。この際は、ブラウザの"暗号化されたページをディスクに保存しない"がOFFになっていないかを確認してください。

1. BOM 集中監視コンソールのコマンドバーの"ログファイル出力"をクリックし、"ログファイル出力"画面を表示させます。



2. "ターゲット種別"は、ログを出力したい"グループ"もしくは、"製品種別"を選択します。
3. "ターゲット"は、手順2.で選択した"グループ"もしくは、"製品種別"が所属するパスを入力します。
4. "ログ種別"は、ログをエクスポートしたい具体的な"ステータスログ"、"ヒストリーログ"、"アクションログ"、"受信ログ"のどれかを選択します。
5. "出力期間"は、ログをエクスポートしたい期間を指定します。

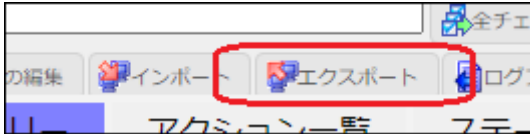
## 12. 設定のエクスポート/インポート

BOM 集中監視コンソールより、集中監視Webサーバーに対して登録を行ったグループ、インスタンス、監視アクション、ユーザー情報といった設定情報、および表示に関する設定を設定ファイルに保存することができます。

- エクスポートした設定ファイルをインポートすることで、同じ設定の集中監視 Web サーバーを簡単に複製することができます。集中監視 Web サーバーの位置づけについては、'[BOM 集中監視コンソールの構成](#)'を参照してください。
- BOM 5.0～BOM 7.0 集中監視コンソールのエクスポートファイルをBOM 8.0 集中監視コンソールへインポートできるため、旧環境のBOMからBOM 8.0へ簡単に移行することができます。
- Internet ExplorerでBOM 集中監視コンソールをご利用の場合エクスポート出力画面で、エクスポートファイルを"保存"や"名前を付けて保存"を行った際に、"ダウンロードできませんでした"と表示されファイルがダウンロードできない場合、ブラウザの"暗号化されたページをディスクに保存しない"がOFFになっていないかを確認してください。

### (1) 集中監視 Web サーバーの設定をエクスポート

1. BOM 8.0 集中監視コンソールのコマンドバーの"エクスポート"をクリックすると、"エクスポート"画面が表示されます。



2. エクスポートしたいファイルを下記のどちらかより選択します。

- "設定ファイル (XMLファイル)" ラジオボタンを選択した場合

グループ、インスタンス、監視アクション、ユーザー情報といった設定情報、および表示に関する設定情報をエクスポートすることができます。この設定ファイルは、'[インポート](#)'の手順でBOM 集中監視コンソールよりインポートすることができます。

- "インスタンス一覧 (CSVファイル)" ラジオボタンを選択した場合

集中監視Webサーバーに設定されているすべてのインスタンスの設定情報と、最新のポーリング実行結果のステータスをエクスポートすることができます。

3. エクスポートファイルは、ブラウザに設定したダウンロードフォルダーに保存されます。

- 設定ファイル

IndicatorSetting\_yyyyMMddhhmmss.xml

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

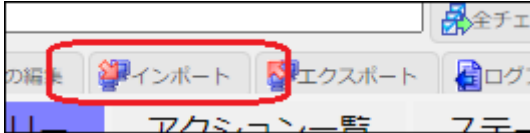
- インスタンス一覧ファイル

InstanceList\_yyyyMMddhhmmss.csv

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

## (2) インポート

1. BOM 集中監視コンソールのコマンドバーの"インポート"をクリックすると、"インポート"画面が表示されます。



2. [ファイルを選択]ボタンをクリックし、"アップロードするファイルの選択"画面より、インポートファイルを選択します。
3. "インポート"をクリックすると、手順2.で指定したインポートファイルをインポートします。
  - エクスポートファイルのファイル名を変更していた場合、ファイルの中身をエクスポート時から更新していない限り、インポートは正常に終了します。

※ インポート処理を実行した場合、現在ログインしているすべてのユーザーが強制ログアウトされます。

※ 警告画面でも表示されていますが、設定ファイルをインポートすると現在の設定およびログはすべて削除されます。

### 13. ユーザー管理

BOM 集中監視コンソールよりログインを行うユーザーの"追加"、"変更"、"削除"と、BOM 集中監視コンソールを使用するための各種ユーザー情報の管理を行うことができます。

BOM 集中監視コンソールのコマンドバーの"ユーザー管理"をクリックし、"ユーザー管理"画面より操作を行います。



#### ユーザー管理

	ユーザー名	ロール名	最終ログイン日時	最終更新ユーザー	最終更新日時
<input type="radio"/>	root	administrat or	2022/03/11 10:0 7:53	system	2022/03/10 16:3 9:34
<input type="radio"/>	system	system		system	2022/03/10 16:3 9:34

追加    変更    削除    閉じる

## (1) ユーザーの追加

1. BOM 集中監視コンソールの"ユーザーの管理画面"で[追加]ボタンをクリックし、"ユーザー新規追加"画面を表示させます。

### ユーザー管理

#### ユーザー新規追加

ユーザー名	<input type="text"/>
ロール	administrator ▼
パスワード ※最大32文字まで	<input type="password"/>
パスワード(確認)	<input type="password"/>

2. "ユーザー名"フィールドには、新規で追加するユーザーのユーザー名を入力します。

- "ユーザー名"は、BOM 集中監視コンソールのログイン画面で入力するユーザー名として使用します。  
※ ユーザー名に次の文字は使用できません。（区切り文字に使用している全角スラッシュを除きます。）

半角スペース/!/"/#/\$/%/&'/(/)\*+/;/.///:/;/</=/>/?/@/[/¥/]/^/'/{/|/}/~

3. "ロール"フィールドは以下の2種類から選択します。

- "administrator"

BOM 集中監視コンソールのすべての操作とログの照会ができます。

同一アカウントによる複数同時ログインはできず、同一アカウントによる同時ログインを行った場合、先にログインをしていたユーザーはログアウト状態になります。

- "read only"

集中監視コンソールのログの照会のみできます。

このロールを持つユーザーは、複数人で同時ログインができます。

4. "パスワード"フィールドには、新規で追加するユーザーのパスワードを設定します。

※ 規定値では、パスワードは実際の変更日時から90日経過した段階で、次回ログイン時にパスワード再設定画面が表示されます。このパスワード有効日数は、環境設定変更画面で変更できます。

※ パスワードは大文字アルファベット、小文字アルファベット、数字と記号の4種類を含んだ8文字以上32文字以内で指定する必要があります。使用できる記号は次のとおりです。（区切り文字に使用している全角スラッシュを除きます。）

@/!/"/#/\$/%/&'/(/)/\*/+/,/-./|/:/;/</=/>/?/[/]/^/\_/{/|/}/~

5. "パスワード (確認)"フィールドには、手順4.の入力内容を確認するために、再度手順4.と同じパスワードを入力します。
6. [確認]ボタンをクリックすると、確認画面が表示されるため、問題がなければ[作成]ボタンをクリックします。

## (2) ユーザーの変更

1. BOM 集中監視コンソールの"ユーザーの管理画面"で[変更]ボタンをクリックし、"ユーザー情報変更"画面を表示させます。

ユーザー情報変更	
ユーザー名	<input type="text" value="saytech"/>
ロール	<input type="text" value="administrator"/>
パスワード ※最大32文字まで	<input type="text"/>
パスワード(確認)	<input type="text"/>

確認    変更前に戻す    戻る    閉じる

2. "ロール"は、下記の2種類より選択します。
  - "administrator"
  - "read only"
3. "パスワード"フィールドには、変更したいパスワードを設定します。

- "パスワード (確認)"フィールドには、手順3の入力内容を確認するために、再度手順3.と同じパスワードを入力します。
- [確認]ボタンをクリックすると、確認画面が表示されるため、問題がなければ[変更]ボタンをクリックします。

### (3) ユーザーの削除

- BOM 集中監視コンソールの"ユーザーの管理画面"で[削除]ボタンをクリックし、"ユーザー情報削除"画面を表示させます。



ユーザー情報削除	
ユーザー名	saytech
ロール	administrator
パスワード	●●●●●●●●

削除    戻る    閉じる

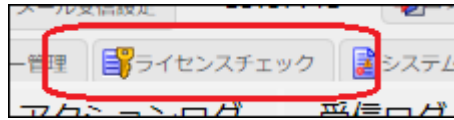
- [確認]ボタンをクリックすると、確認画面が表示されるため、問題がなければ[削除]ボタンをクリックします。



## 14. ライセンスチェック

BOM 集中監視コンソールに登録したインスタンスのライセンス情報をリスト表示します。

1. BOM 集中監視コンソールのコマンドバーの"ライセンスチェック"をクリックし、"ライセンスチェック"画面を表示させます。



↓

ライセンスチェック			
グループ名	表示名	ライセンスキー	ライセンス詳細
/root/関東本社	AP-01		BOM 8.0 基本製品 通常版ライセンス(ライセンス数 200)
/root/関東本社/情報システム部	DB-06		BOM 8.0 基本製品 通常版ライセンス(ライセンス数 200)
/root/九州支店	AP-03		BOM 8.0 基本製品 通常版ライセンス(ライセンス数 200)
/root/九州支店	DB-02		BOM 7.0 基本製品 クライアント版ライセンス(ライセンス数 200)

- "グループ名"  
インスタンスが所属するグループを表示します。
- "表示名"  
BOM 集中監視コンソールに設定したインスタンス名を表示します。
- "ライセンスキー"  
インスタンスのライセンスキーを表示し、フィルタリングで重複ライセンスをチェックすることができます。  
(有効なライセンスを確認できなかった場合は空白表示です。)
- "ライセンス詳細"  
ライセンスキーの詳細を表示します。

## 15. BOM 集中監視コンソールの環境設定変更

BOM 集中監視コンソールの環境設定を変更するには、BOM 集中監視コンソールのコマンドバーの"設定変更"をクリックし、"設定変更"画面より操作を行います。



- AdministratorロールとRead Onlyロールでは設定変更できる範囲が異なります。

### (1) Administratorロールで変更できる設定内容

メンテナンス設定(ログイン時のみ有効)	
画面の自動更新一時停止	<input type="radio"/> ON <input checked="" type="radio"/> OFF

ユーザー設定 (再ログイン後有効)	
自動更新間隔	2分 ▼
ログ表示件数	100件 ▼
サマリーログビューアーのログ表示期間	30分 ▼
自動ログアウト時間	なし ▼
ホーム画面に遷移するまでの時間	1日 ▼

システム設定 (サービス再起動後有効)	
ログ保存期間	30日 ▼
ログ削除処理実施時刻	0:00 ▼
インスタンスの多重登録を許す	<input type="radio"/> 許可 <input checked="" type="radio"/> 禁止
パスワードチェックを強化する	<input checked="" type="radio"/> 強化する <input type="radio"/> 強化しない
パスワード有効日数	90日 ▼

#### A. メンテナンス設定 (ログイン時のみ有効)

設定は[適用]ボタンを押した時点でログインユーザーに対して反映され、ユーザーがログアウトすると既定の設定に戻ります。

- "画面の自動更新一時停止"欄

メンテナンス作業用に、BOM 集中監視コンソールの"ツリービュー"、"詳細ビュー"、"サマリーログビュー"の表示の自動更新を一時的に停止させたい場合に、"ON"ラジオボタンを選択します。既定の設定は"OFF"です。

## B. ユーザー設定（再ログイン後有効）

設定はログインユーザーが再ログインした時点で、ログインユーザーに対して反映されます。

- "自動更新間隔"欄

BOM 集中監視コンソールの"ツリービュー"、"詳細ビュー"、"サマリーログビュー"の表示を自動更新する時間間隔を指定することができます。

- "ログ表示件数"欄

"詳細ビュー（ステータスログ、ヒストリーログ、アクションログ、受信ログ）"のログ表示件数を指定することができます。

- "サマリーログビューアーのログ表示期間"欄

サマリーログビューのログの表示期間を指定することができます。

※ ログ表示期間内でも500件を超えるログがあった場合には最新の500件までしか表示されません。

- "自動ログアウト時間"欄

集中監視コンソールが一定時間無操作であった場合に、自動でログイン画面に戻る時間を設定することができます。

- "ホーム画面に遷移するまでの時間"欄

集中監視コンソールが一定時間無操作であった場合に、自動でホーム画面に遷移する時間を設定できます。

## C. システム設定（サービス再起動後有効）

設定は"BOM 8.0 集中監視 Web サービス"を再起動した時点で、すべてのユーザーに対して反映されます。

- "ログ保存期間"欄

集中監視Webサービスに蓄積するログの保存期間を指定することができます。

このログには、ステータスログ、ヒストリーログ、アクションログ、受信ログ、システムログが含まれます。

- "ログ削除処理実行時刻"欄

"ログ保存期間"欄で指定したログ保存期間を過ぎたログを削除する時刻を指定することができます。

ログの削除中は、一時的に集中監視Webサービスの負荷が上がるため、BOM 集中監視コンソールを管理端末で操作しない時間帯に設定しておくことを推奨します。

- "インスタンスの多重登録を許す"欄

1つのインスタンスを複数のインスタンスとしてBOM 集中監視コンソールに登録を行いたい場合に、"許可"ラジオボタンを選択します。

- "パスワードチェックを強化する"欄

ログインユーザーのパスワードを指定する際、強固なパスワードルールを設定する場合には、パスワードチェックを"強化する"ラジオボタンを選択します。強固なパスワードルールを設定しない場合には"強化しない"ラジオボタンを選択します。

各ルールを指定した際のパスワードに設定できる条件は以下のとおりです。

- 強化するを選択した場合

大文字アルファベット小文字アルファベット数字と記号の4種類をすべて含んだ、8文字以上32文字以内で指定。使用できる記号については次のとおりです。（区切り文字に使用している全角スラッシュを除きます。）

@/!/"/#/\$/%/&/'/(/)/\*/+/,/-/.//:/;/</=/>/?/[/]/^/\_/{|/}/~

- 強化しないを選択した場合

大文字アルファベット小文字アルファベット数字または記号いずれかの文字を使用した、1文字以上32文字以内で指定。

使用できる記号については次のとおりです。（区切り文字に使用している全角スラッシュを除きます。）

@/!/"/#/\$/%/&/'/(/)/\*/+/,/-/.//:/;/</=/>/?/[/]/^/\_/{|/}/~

- "パスワード有効日数"欄

パスワードの有効日数を以下からプルダウンで選択します。

"30日" "60日" "90日" "120日" "150日" "180日" "360日" "無期限"

※ 有効日数は直近のパスワード変更日より起算します。

## (2) read onlyロールで変更できる設定内容

メンテナンス設定(ログイン時のみ有効)	
画面の自動更新一時停止	<input type="radio"/> ON <input checked="" type="radio"/> OFF
ユーザー設定 (再ログイン後有効)	
自動更新間隔	2分 ▼
ログ表示件数	100件 ▼
サマリーログビューアーのログ表示期間	30分 ▼
自動ログアウト時間	なし ▼
ホーム画面に遷移するまでの時間	1日 ▼

### A. メンテナンス設定 (ログイン時のみ有効)

設定は[適用]ボタンを押した時点でログインユーザーに対して反映され、ユーザーがログアウトすると既定の設定に戻ります。

- "画面の自動更新一時停止"欄

メンテナンス作業用に、BOM 集中監視コンソールの"ツリービュー"、"詳細ビュー"、"サマリーログビュー"の表示の自動更新を一時的に停止させたい場合に、"ON"ラジオボタンを選択します。

## B. ユーザー設定（再ログイン後有効）

設定はログインユーザーが再ログインした時点で、ログインユーザーに対して反映されます。

- "自動更新間隔"欄

BOM 集中監視コンソールの"ツリービュー"、"詳細ビュー"、"サマリーログビュー"の表示を自動更新する時間間隔を指定することができます。

- "ログ表示件数"欄

"詳細ビュー（ステータスログ、ヒストリーログ、アクションログ、受信ログ）"のログ表示件数を指定することができます。

- "サマリーログビューアーのログ表示期間"欄

サマリーログビューのログの表示期間を指定することができます。

※ ログ表示期間内でも500件を超えるログがあった場合には最新の500件までしか表示されません。

- "自動ログアウト時間"欄

集中監視コンソールが一定時間無操作であった場合に、自動でログイン画面に戻る時間を設定することができます。

- "ホーム画面に遷移するまでの時間"欄

集中監視コンソールが一定時間無操作であった場合に、自動でホーム画面に遷移する時間を設定することができます。

## 16. 集中監視Webサービスおよび集中監視コンソール使用時の注意点

### (1) 集中監視 Web サービス使用時の注意点

- 登録インスタンス数にシステム的な制限はありませんが、1つの集中監視Webサービスあたり50インスタンスまでを推奨値としています。

ただし、コンピューターのスペックや設定するポーリング間隔などの要因によって快適に利用できる値は大きく上下するため、実環境において動作の確認および登録インスタンス数の調整を実施してください。

利用環境に見合わないインスタンス数が登録された場合、インスタンス情報の取得が遅延することがあります。

- 同一IPアドレスから同じ日に累計10回ログインに失敗した場合、次の日の0時00分になるまで該当IPからはログインができません。
- グループ名、インスタンス名、アクション名に下記の半角文字が含まれていた場合、全角文字に変換してインポートします。(区切り文字に使用している全角スラッシュを除きます。)

```
!/"#/$/%/&'/(/)*+/,.///:/;/</=>/?/[¥/]/^/'/{|/}/~
```

- ユーザー名に次の文字は使用できません。(区切り文字に使用している全角スラッシュを除きます。)

```
半角スペース!/"#/$/%/&'/(/)*+/,.///:/;/</=>/?/[¥/]/^/'/{|/}/  
/~
```

- '[システム設定](#)'において「パスワードチェックを強化する」が有効("強化する")になっている場合、パスワードは大文字アルファベット、小文字アルファベット、数字と記号の4種類を含んだ8文字以上32文字以内で指定をする必要があります。使用できる記号は次のとおりです。(区切り文字に使用している全角スラッシュを除きます。)

```
@/!"#/$/%/&'/(/)*+/,./-.///:/;/</=>/?/[ ]/^/_/{|/}/~
```

- 規定値では、パスワードは実際の変更日時から90日経過した段階で、次回ログイン時にパスワード再設定画面が表示されます。このパスワード有効日数は、環境設定変更画面で変更できます。
- パスワード有効期限7日前の時点以降、該当のユーザーがログイン時した際に、システムログにその旨が表示されます。
- 警告画面でも表示されますが、設定ファイルをインポートすると現在の設定およびログはすべて削除されます。

### (2) 集中監視コンソール使用時の注意点

- 一つのブラウザーから同じ集中監視 Web サービスへの多重接続はできません。
- ブラウザーの[戻る]、[進む]ボタンは使用せず、集中監視コンソール上の"戻る"を利用してください。
- Webブラウザーの使用メモリ増加を防止し、継続してBOM 集中監視コンソールを快適にご利用いただくために、定期的にブラウザーを閉じていただく必要があります。
- "ユーザー名"「root」は集中監視 Web サービスをインストールしたシステムからのみログインが可能です。
- Windows クライアント OSには、セッション数の上限があります。

セッション数の上限を超えてブラウザーから集中監視Webサービスに接続を試みた場合、超過分は接続に失敗します。

## 第2章 集中監視 Web サービス ポーリング スケジュール設定

本章では、集中監視Webサービスが実行する監視対象へのポーリングについて、Windows標準のタスクスケジューラを用いて有効化・無効化をスケジュールリングするための設定手順を説明します。

### 1. 集中監視コンソールのユーザー追加

ポーリングを有効化・無効化する際は、集中監視コンソールに登録されたadministratorロールのユーザーを使用します。

ユーザー追加は必須ではなく既定のユーザーであるrootなども使用できますが、有効・無効の切り替え用のユーザーを別途用意する場合は、'[ユーザーの追加](#)'を参照し、administratorロールのユーザーを追加してください。

### 2. ポーリング設定

ポーリングのスケジュールは集中監視コンソールの"グループ単位"または"インスタンス単位"で設定できますが、それぞれ事前の設定が必要です。

#### (1) スケジュールを集中監視コンソールのグループ単位で行う場合

スケジュールを集中監視コンソールのグループ単位で設定する場合は、該当のグループに所属するスケジュールリング対象のインスタンスについて、ポーリング設定が"グループの設定に従う"となっている必要があります。

※ポーリング設定を"グループの設定に従う"とすることで、グループに対するポーリングの有効化・無効化操作がそのグループ配下のインスタンスに反映されます。"個別のポーリング設定を行う"に設定されているインスタンスは、グループに対するスケジュール設定の影響を受けません。

- 集中監視コンソールにadministratorロールを持ったユーザーでログインします。
- スケジュールリングの対象となるグループに所属するインスタンスをクリックします。
  - ※ スケジュールリング対象のインスタンスが複数ある場合は、以降の操作を対象のすべてのインスタンスで繰り返してください。
- [インスタンスの編集]ボタンをクリックします。

4. "インスタンスの編集"画面で"ポーリング設定"を確認します。

インスタンス設定	
グループ	/root/関東本社
インスタンス種別	BOM 8.0 基本製品 インスタンス
監視対象コンピューター	localhost
ヘルパーサービスポート	20080
パスワード	●●●●●●●●
インスタンス名	WIN-NBIAMPVUFID
表示名	AP-01
ポーリング設定	グループの設定に従う
ポーリング有効/無効	-
ポーリング間隔	-
最終更新ユーザー	root

追加    変更    削除    閉じる

- "グループの設定に従う"となっている場合

設定変更は必要ありません。[閉じる]ボタンをクリックして「インスタンスの編集」画面を閉じてください。

- "個別のポーリング設定を行う"となっている場合

[変更]ボタンをクリックします。

5. "ポーリング設定"で"グループの設定に従う"にチェックを入れ、[確認]ボタン→[確定]ボタンを順にクリックします。

6. [閉じる]ボタンをクリックして"インスタンスの編集"画面を閉じます。

## (2) スケジュールを集中監視コンソールのインスタンス単位で行う場合

スケジュールをインスタンス単位で設定する場合は、スケジュールリングの対象となるインスタンスのポーリング設定が"個別のポーリング設定を行う"となっている必要があります。

※ "グループの設定に従う"に設定されていると、インスタンスに対してポーリングの有効化・無効化操作を行っても反映されません。

1. 集中監視コンソールにadministratorロールを持ったユーザーでログインします。

2. スケジュールリングの対象となるグループに所属するインスタンスをクリックします。

※ スケジュールリング対象のインスタンスが複数ある場合は、以降の操作を対象のすべてのインスタンスで繰り返してください。

3. [インスタンスの編集]ボタンをクリックします。



4. "インスタンスの編集"画面で"ポーリング設定"を確認します。



インスタンス設定	
グループ	/root/関東本社
インスタンス種別	BOM 8.0 基本製品 インスタンス
監視対象コンピューター	localhost
ヘルパーサービスポート	20080
パスワード	●●●●●●●●
インスタンス名	WIN-NBIAMPVUFID
表示名	AP-01
ポーリング設定	個別のポーリング設定を行う
ポーリング有効/無効	無効
ポーリング間隔	-
最終更新ユーザー	root

追加 変更 削除 閉じる

- "個別のポーリング設定を行う"となっている場合

設定変更は必要ありません。[閉じる]ボタンをクリックして「インスタンスの編集」画面を閉じてください。

- "グループの設定に従う"となっている場合

[変更]ボタンをクリックします。

5. "ポーリング設定"で"個別のポーリング設定を行う"にチェックを入れ、[確認]ボタン→[確定]ボタンを順にクリックします。

6. [閉じる]ボタンをクリックして"インスタンスの編集"画面を閉じます。

### 3. ユーザー情報の暗号化と登録

集中監視Webサービスのポーリングを有効化・無効化する際に使用するadministratorロールのユーザーについて、以下の手順でこのユーザーのユーザーIDおよびパスワードを暗号化して登録します。

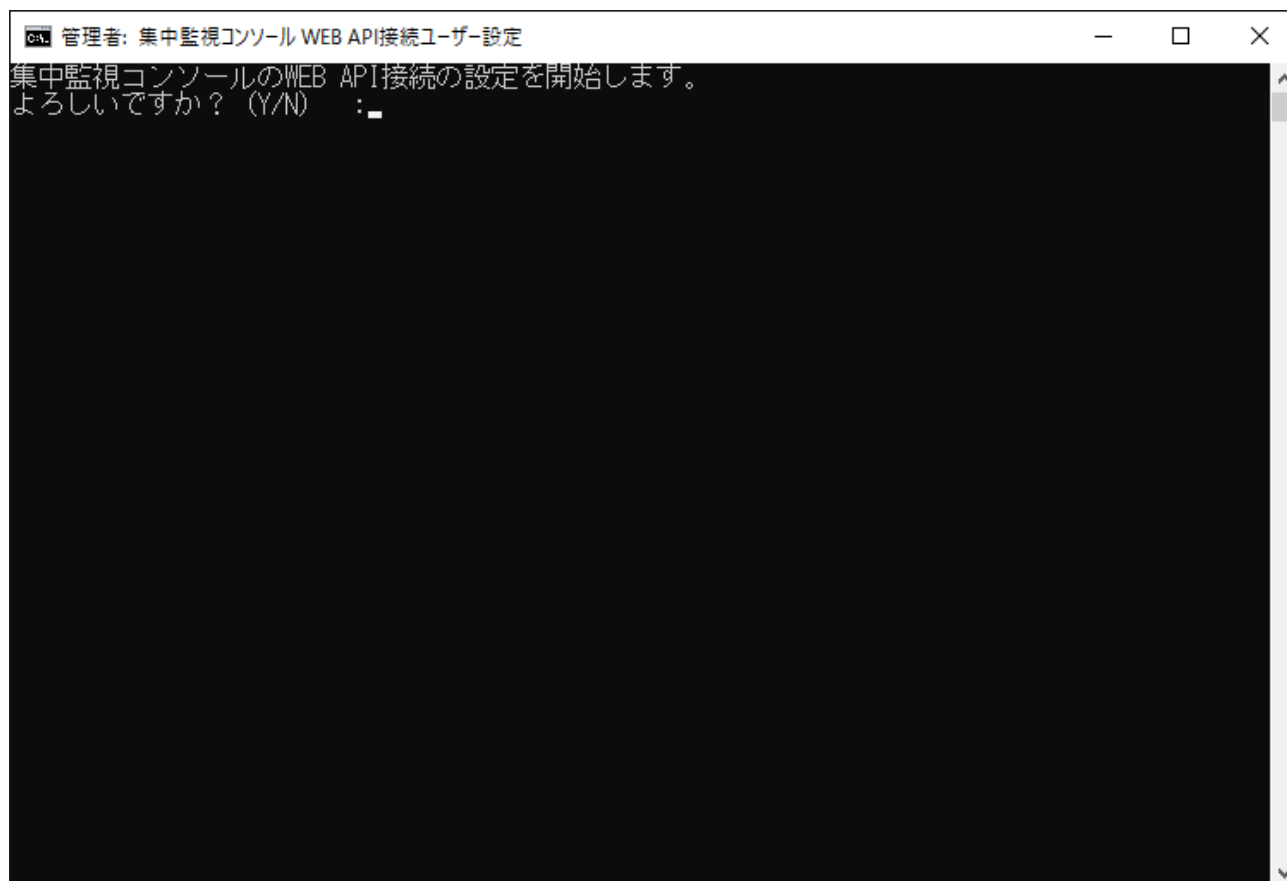
※ 本操作は集中監視Webサービスがインストールされたコンピューター上で実行してください。

1. 以下のフォルダーに格納されたバッチファイルを管理者として実行します。

```
[BOM 8.0 インストールフォルダー]¥BOMW8¥Indicator_client¥SetupApiUser.bat
```

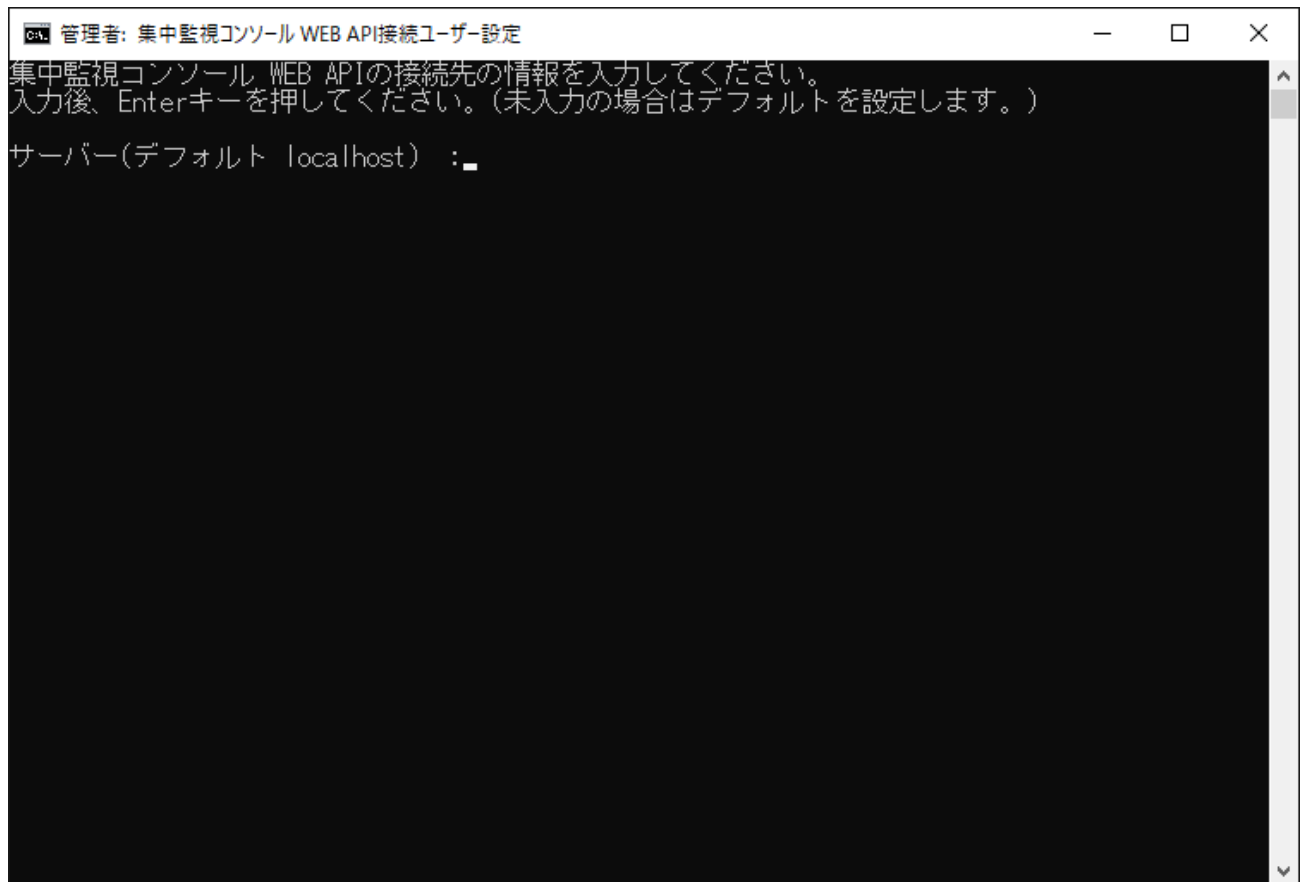
2. "集中監視コンソール WEB API接続ユーザー設定"画面が開きます。

"y"と入力し、「Enter」キーを押してください。



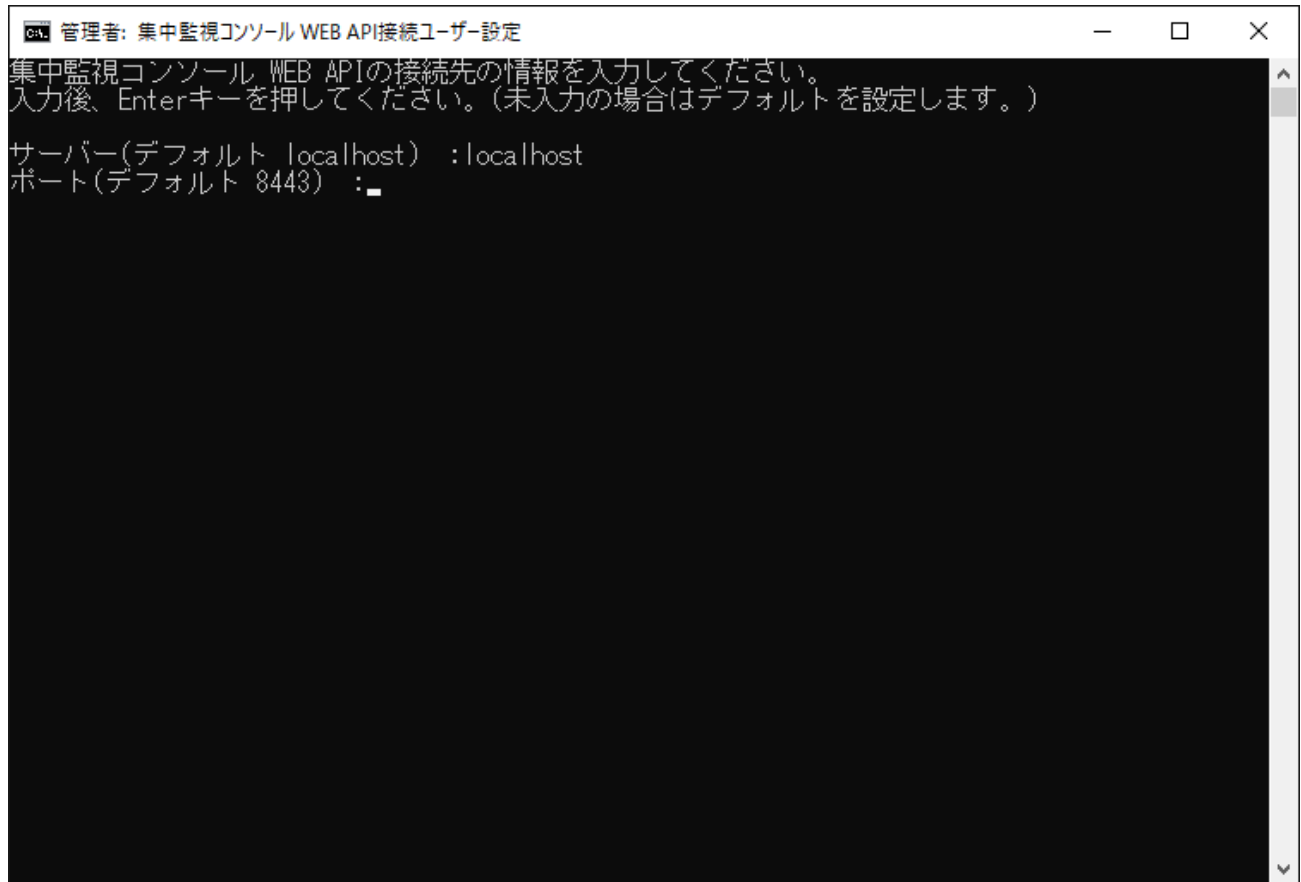
3. 以下の画面が表示されますが、ここでは何も入力せずに「Enter」キーを押してください。

自動的に"localhost"と入力され、ポート番号の指定に進みます。

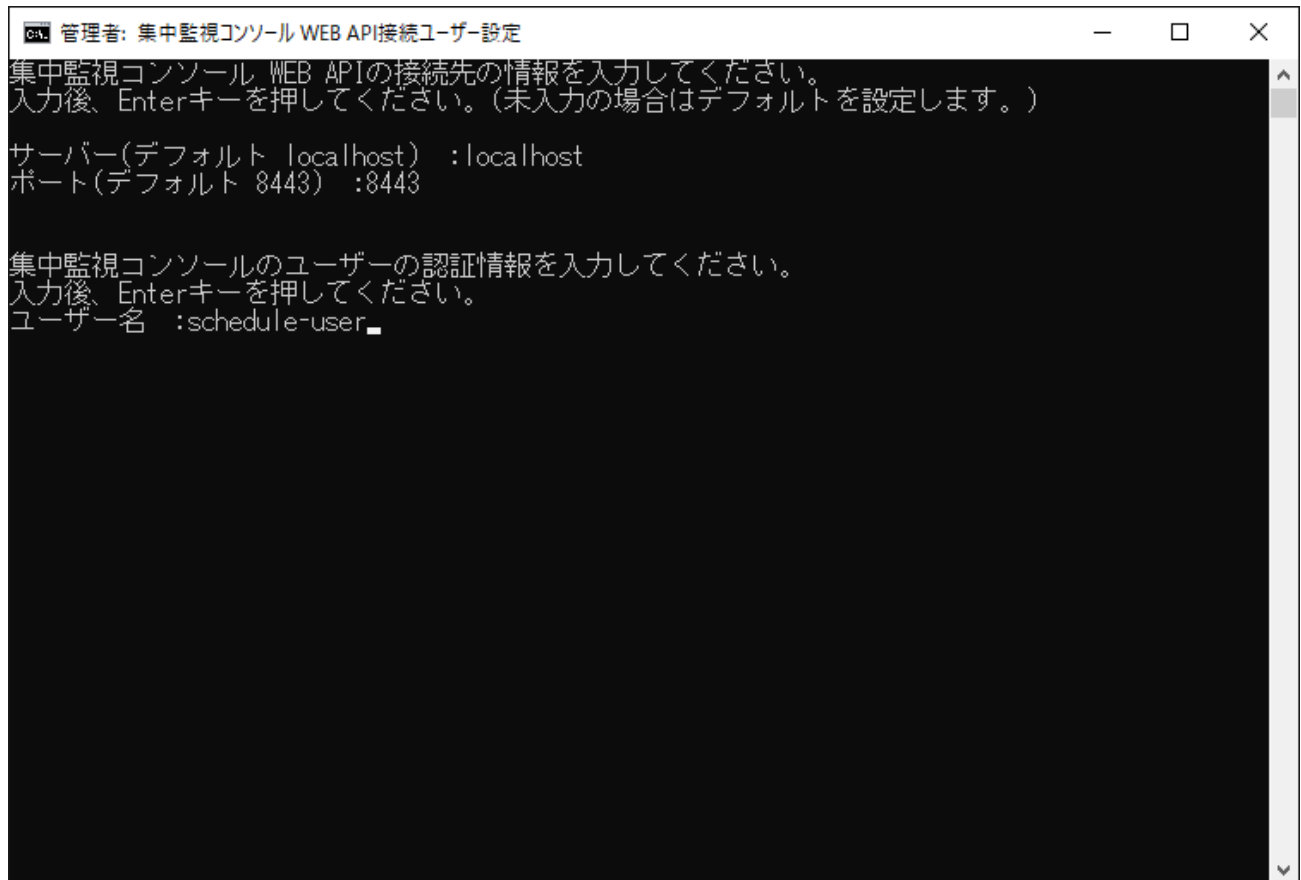


4. ポート番号の指定では、集中監視 Web サーバーに設定しているポート番号を入力し、「Enter」キーを押してください。

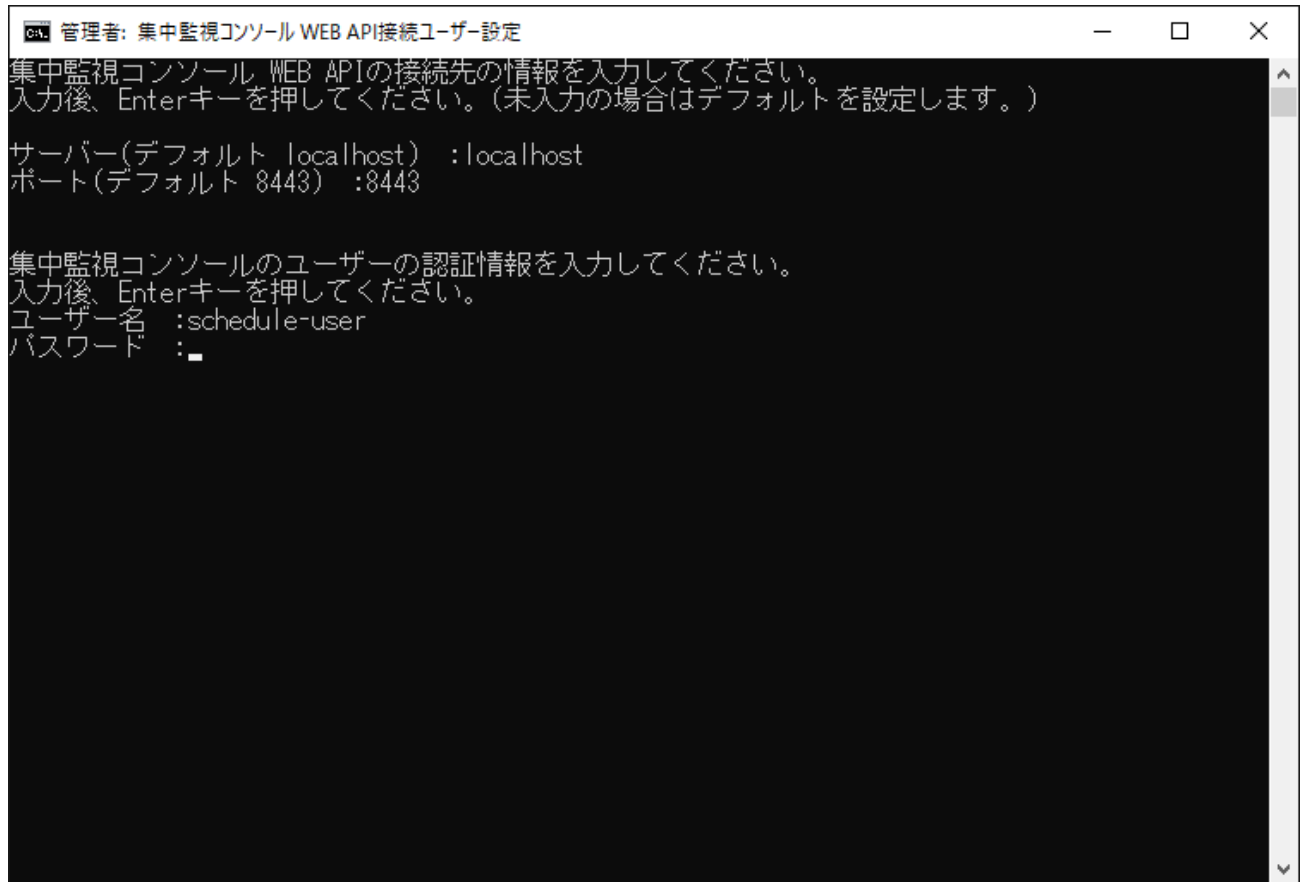
ポート番号を既定値（8443番）から変更していない場合は、未入力状態で「Enter」キーを押してください。



5. 下記の画面では、集中監視コンソール上でadministratorロールが付与された、ポーリングの有効化・無効化を実行するユーザー名を入力し、「Enter」キーを押します。



6. 5.のユーザーに設定されたパスワードを入力し、「Enter」キーを押します。



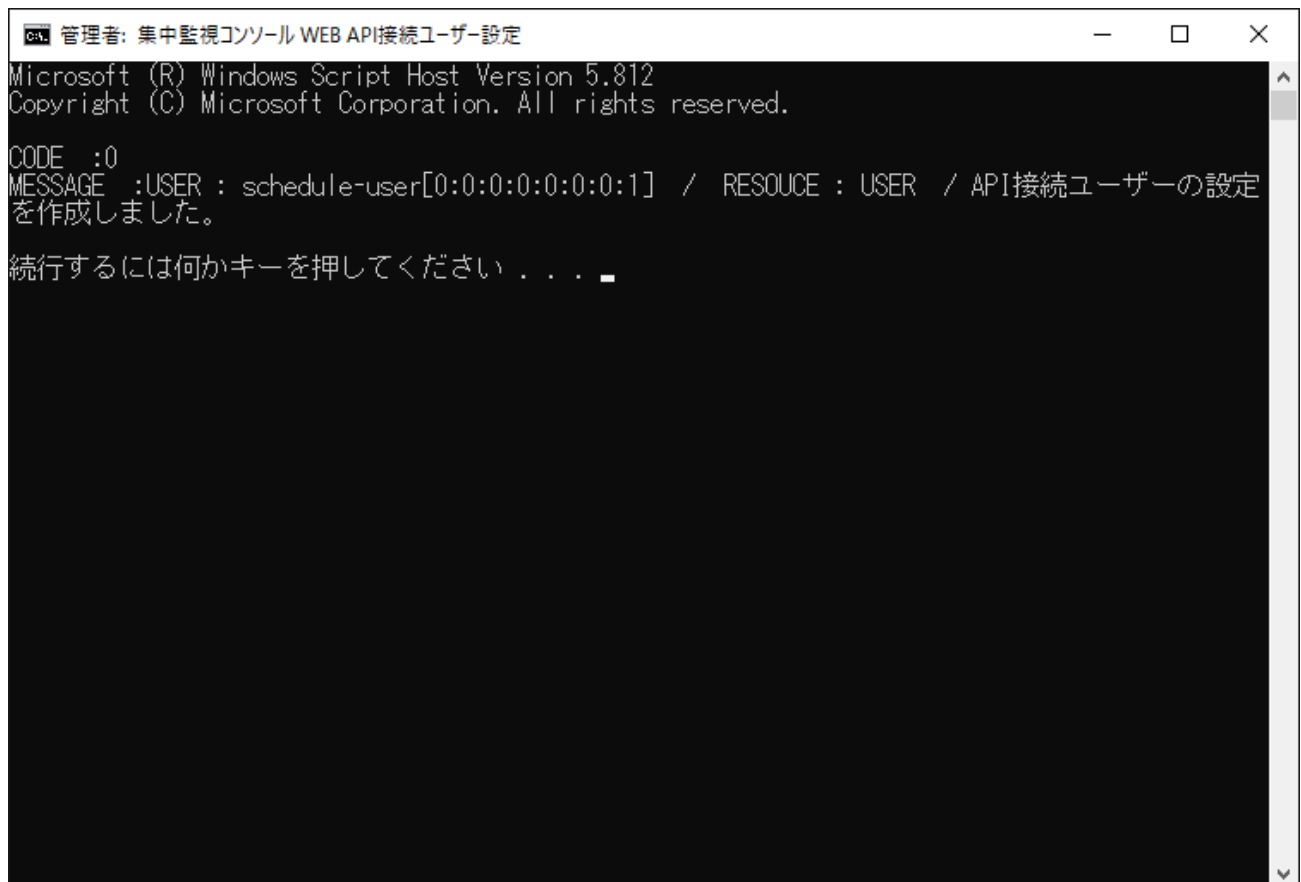
```
ca. 管理者: 集中監視コンソール WEB API接続ユーザー設定
集中監視コンソール WEB APIの接続先の情報を入力してください。
入力後、Enterキーを押してください。(未入力の場合はデフォルトを設定します。)

サーバー(デフォルト localhost) :localhost
ポート(デフォルト 8443) :8443

集中監視コンソールのユーザーの認証情報を入力してください。
入力後、Enterキーを押してください。
ユーザー名 :schedule-user
パスワード :■
```

7. 問題なくユーザー情報の暗号化および登録が完了すると、以下の画面が表示されます。

任意のキーを押して設定画面を閉じてください。



```
ca. 管理者: 集中監視コンソール WEB API接続ユーザー設定
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

CODE :0
MESSAGE :USER : schedule-user[0:0:0:0:0:0:1] / RESOURCE : USER / API接続ユーザーの設定
を作成しました。

続行するには何かキーを押してください . . . ■
```

- 入力された情報に誤りがある場合は、以下のようなエラーメッセージを表示して処理を終了します。この際は、改めて本手順の1.から実行してください。

[エラーメッセージ例]

- ポート番号に誤りがある場合

「セキュリティで保護されたチャネルサポートでエラーが発生しました。」

- ユーザー名、パスワードに誤りがある場合

「ユーザー名またはパスワードが正しくありません。」

## 4. スケジュール設定

ポーリング有効化・無効化の切り替えスケジュールは、Windows 標準のタスクスケジューラに登録します。

実行日時などをトリガーとし、切り替え内容（有効化/無効化）や対象（インスタンス、グループ）を引数として設定した特定のバッチファイルを実行することで、ポーリングの有効・無効をコントロールします。

ここではタスク スケジューラへのタスクの登録方法を記載します。

※ ポーリングの無効化、有効化それぞれに1件のタスクが必要です。そのため、ポーリングを停止～開始する場合は最低でも2件のタスクを登録しなければなりません。

1. Windows タスク スケジューラを起動します。
2. 任意のフォルダーを指定し、"操作" → "タスクの作成"をクリックします。
3. "タスクの作成"画面が表示されます。  
「全般」では以下の設定を行います。

タスクの作成

全般 トリガー 操作 条件 設定

名前(M): BOM8集中監視 [ポーリング無効]

場所: %SAY Technologies%BOM-Schedule

作成者: WIN-NBIAMPVUFID#Administrator

説明(D):

セキュリティ オプション

タスクの実行時に使うユーザー アカウント:  
WIN-NBIAMPVUFID#Administrator ユーザーまたはグループの変更(U)...

ユーザーがログオンしているときのみ実行する(R)

ユーザーがログオンしているかどうかにかかわらず実行する(W)

パスワードを保存しない(P) (タスクがアクセスできるのはローカル コンピューター リソースのみ)

最上位の特権で実行する(I)

表示しない(E) 構成(C): Windows Vista™, Windows Server™ 2008

OK キャンセル

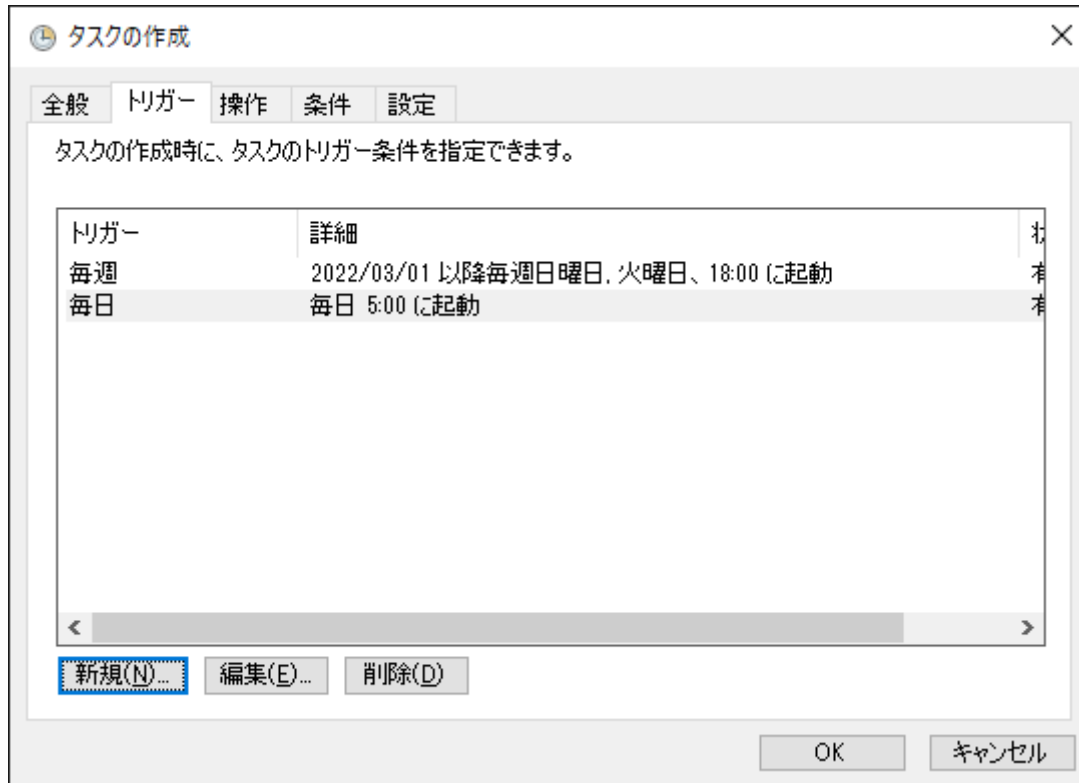
○ 名前(M):

任意の名称を入力します。登録するタスクの内容がわかる名称にすることをお勧めします。

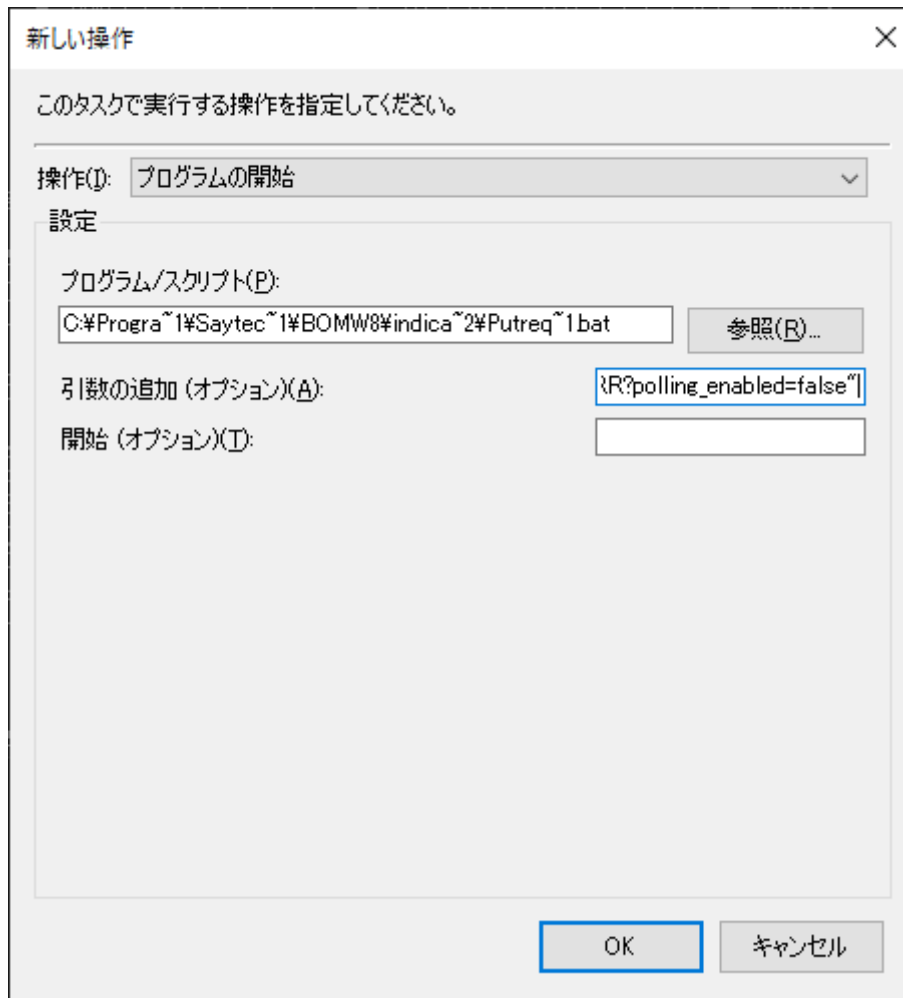
○ セキュリティオプション

"ユーザーがログオンしているかどうかにかかわらず実行する"にチェックを入れてください。また、タスク実行に使用するユーザーアカウントおよび、"最上位の特権で実行する"チェックについては環境に合わせて設定してください。

4. 「トリガー」タブを選択し、[新規]ボタンからタスクの実行条件（トリガー）を登録します。



5. 「操作」タブを選択し、[新規]ボタンをクリックします。
6. "新しい操作"画面では以下の設定を行い、[OK]ボタンをクリックします。





○ 操作(I):

"プログラムの開始"を選択してください。

○ プログラム/スクリプト(P):

以下の場所に格納されたバッチファイル (PutRequest.bat) を指定してください。

```
[BOM 8.0 インストールフォルダー]¥BOMW8¥Indicator_client¥PutRequest.bat
```

※ タスク スケジューラでは"プログラム/スクリプト"欄に入力した文字列と、"引数の追加"欄に入力した文字列の両方がダブルクォーテーションで括られている場合、実行に失敗することがあります。"引数の追加"欄では必ずダブルクォーテーションを使用するため、本現象に該当する場合は"プログラム/スクリプト"欄に入力する文字列にダブルクォーテーションが使用できません。

該当する環境で設定される場合は、"プログラム/スクリプト"欄を8.3形式の表記で入力してください。

[記載例]

```
C:¥Progra~1¥Saytec~1¥BOMW8¥indica~2¥Putreq~1.bat
```

○ 引数の追加 (オプション)(A):

以下の説明を確認し、目的および環境に合った文字列を入力してください。

※ 引数は前後を半角ダブルクォーテーションで括ったURL形式の文字列です。このダブルクォーテーションを含めた文字列を"引数の追加"欄に入力してください。

- 以下で例示する文字列については、前後の「" (半角ダブルクォーテーション) 」も含んで入力が必要です。
- 文字列の大文字・小文字は変更せず、そのまま入力してください。

"https://localhost:[A]/Indicator/api/v1/[B]/[C]?polling\_enabled=[D]"

[A] : ポート番号 (規定値は"8443"です)

[B] : 有効・無効切り替え単位の指定

- グループ単位は"groups"、インスタンス単位は"instances"

[C] : 切り替え対象のグループ、インスタンスの指定

- 集中監視コンソール上でのグループ (階層) 名および、表示名で指定します。
- 階層の区切りは"/ (スラッシュ) "で行い、末尾のスラッシュは不要です。

[D] : 有効化・無効化

- 有効にする場合は"true"、無効にする場合は"false"

○ (例1) 集中監視コンソールのグループ単位で有効無効を切り替える際の引数

ポート番号 **8443** の集中監視 Web サーバーに接続し、グループ ( **groups** ) " **root/BOM8-Demo** "へのポーリングを有効化 ( **true** ) する場合

```
"https://localhost:8443/Indicator/api/v1/groups/root/BOM8-Demo?polling_enabled=true"
```

◦ (例2) インスタンス単位で有効無効を切り替える際の引数

ポート番号 **12345** の集中監視 Web サーバーに接続し、グループ“ **root/BOM8-Demo** ”に所属するインスタンス ( **instances** ) である、表示名“ **192168110\_WIN-7U8EM0RP1RR** ”へのポーリングを無効化 ( **false** ) する場合

```
"https://localhost:12345/Indicator/api/v1/instances/root/BOM8-Demo/192168110_WIN-7U8EM0RP1RR?polling_enabled=false"
```

7. 「条件」タブ、「設定」タブに必須の設定項目はありません。必要に応じて設定を行ってください。
8. すべての設定が完了した後に、“タスクの作成”画面の[OK]ボタンをクリックしてください。
9. 実行ユーザーのアカウントを求められた場合は、画面の指示に沿って入力してください。
10. 本手順の2～9を繰り返し、必要なスケジュールを登録してください。

## 第3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してください。

**Q.** ブラウザーでBOM 集中監視Webサービスに接続できない。

**A.** BOM 8.0では脆弱性対応のため、TLSv1.0およびTLSv1.1での接続を無効化しています。各ブラウザからはTLSv1.2、TLSv1.3を使用して接続してください。

---

**Q.** BOM 集中監視コンソールが対象コンピューターを見つけられない。

**A.** 以下を確認してください。

- 対象コンピューターがネットワーク上に存在することを確認します。
  - 対象コンピューターとローカルコンピューターがファイアウォールで分離されていないことを確認します。
  - OpenSSL 1.1.1シリーズを使用するBOM 8.0では、異なるシリーズのOpenSSLを使用する旧バージョンのBOM製品との接続に制限があります。  
詳しくは'[インスタンス](#)'を参照してください。
  - 対象コンピューターでBOMヘルパーサービスが正常に起動しているか確認します。
  - 対象コンピューターで動作するBOMの管理者パスワードを間違えていないか確認します。
  - 対象コンピューターで動作するBOMヘルパーサービスの設定について、以下を確認します。  
詳しくは'BOM for Windows Ver.8.0 ユーザーズマニュアル'で、「BOMヘルパーサービス設定」を参照してください。
    - 対象コンピューターに設定されている"リモートアクセスの範囲"が正しいか。
    - "ヘルパーサービスポート"欄に入力されたポート番号と、実際に対象コンピューターで設定されたBOM ヘルパーサービスのポート番号が合致しているか。
- 

**Q.** BOM 集中監視コンソールがインスタンスのステータスを収集できない。

**A.** 以下を確認してください。

- "ヘルパーサービスポート番号"が、指定したコンピューターのBOMヘルパーサービスのポート番号と一致していることを確認します。
- 指定したコンピューターでBOMヘルパーサービスが開始していることを確認します。

- 対象コンピューターでBOMヘルパーサービスが正常に起動しているか確認します。
- 対象コンピューターで動作するBOMの管理者パスワードを間違えていないか確認します。
- 対象コンピューターで動作するBOMヘルパーサービスの設定について、以下を確認します。  
詳しくは'BOM for Windows Ver.8.0 ユーザーズマニュアル'で、「BOMヘルパーサービス設定」を参照してください。
  - 対象コンピューターに設定されている"リモートアクセスの範囲"が正しいか。
  - "ヘルパーサービスポート"欄に入力されたポート番号と、実際に対象コンピューターで設定されたBOM ヘルパーサービスのポート番号が合致しているか。
- 対象のコンピューターとの通信経路上において、ネットワークに問題が発生していないかを確認します。
  - 確認すべきポイントの例：  
中継機器の設定（パケットフィルタリング、ファイアウォール等）  
ネットワークケーブルやL2スイッチ等の物理的破損  
名前解決の失敗  
IPアドレスの重複  
MACアドレスの重複

---

**Q.** 保存された BOM 集中監視コンソールのログファイル数が非常に多くなっている。

**A.** BOM 集中監視コンソールが出力する動作ログファイルのうち、以下のログは障害対応などの際に遡って確認できるよう、ファイルが自動削除されません。また、これらのログファイルは日付単位でローテーションされるため、BOM 集中監視コンソールの運用が長期にわたる場合、保存されたファイル数が非常に多くなることが考えられます。

- ログファイルの出力先：[BOM 8.0 インストールフォルダー]¥Indicator¥tomcat¥logs
  - bom8indicator-stdout.YYYY-MM-DD.log（標準出力のログ）
  - bom8indicator-stderr.YYYY-MM-DD.log（標準エラーのログ）
  - commons-daemon.YYYY-MM-DD.log（サービスの動作ログ）
  - localhost\_access\_log.YYYY-MM-DD.txt（アクセスログ）

これらのファイルは、削除・移動しても BOM 集中監視 Web サービスや BOM 集中監視コンソールの動作に影響はありません。

保存されたログファイルの数を減らす場合は、当日日付のものを含めて直近の任意の日数分のみファイルを残し、調査や記録のため保存する場合はファイルを移動する、不要な場合は削除するなど、必要に応じて“logs”フォルダーから除外してください。

---

## **BOM for Windows 集中監視コンソールユーザーズマニュアル**

2022年5月11日 初版

2024年1月22日 改訂版

著者・発行者・発行

セイ・テクノロジーズ株式会社

バージョン Ver.8.0.10.0

(C) 2022 SAY Technologies, Inc.