純国産サーバー監視ツールのここがイイ！

BOM for Windows Ver.7.0 SR1 評価レビュー

「BOM for Windows」は、セイ・テクノロジーズ株式会社が開発・提供する、特にWindows ベースのサーバー監視を得意とする純国産のサーバー監視ソフトです。もともと、Windows NT のログ監視を効率化することを目的に開発された製品ですが、現在は、当初のコンセプトを引き継ぎながら、最新のWindows Server 2016 のOS 監視はもちろん、Linux や仮想環境、データベースを含めたIT 基盤の総合的な監視に対応しています。最新版をレビューし、その製品概要、最新版で追加された注目の新機能、および導入時のヒントをレポートします。

ライター／山内 和朗

山内 和朗（やまうち かずお）

フリーランスのテクニカルライター。大手 SIer のシステムエンジニア、IT 専門誌の編集者、地方の中堅企業のシステム管理者を経て、2008 年にフリーランスに。過去に「山市良」「三華和夫」の筆名で IT 専門誌に多数の記事を寄稿。最近は IT 系の Web メディアへの寄稿、IT ベンダーの Web コンテンツの制作、技術文書（ホワイトペーパー）の執筆、ユーザー事例取材などを中心に活動。2008 年 10 月より Microsoft MVP - Cloud and Datacenter Management（旧カテゴリ：Hyper-V）を毎年受賞。岩手県花巻市在住。

主な著書・訳書

- 『インサイドWindows 第7版』（訳書、日経BP社、2018年春の予定）
- 『Windows Sysinternals徹底解説 改定新版』（訳書、日経BP社、2017年）
- 『Windows Server 2016テクノロジ入門　完全版』（日経BP社、2016年）
- 『Windows Server 2016テクノロジ入門 Technical Previewエディション』（日経BP社、2015年）
- 『Windows Server 2012 R2テクノロジ入門』（日経BP社、2014年）
- 『Windows Server 2012テクノロジ入門』（日経BP社、2012年）
- 『Windows Sysinternals徹底解説』（訳書、日経BP社、2012年）
- 『Windows Server仮想化テクノロジ入門』（日経BP社、2011年）
- 『Windows Server 2008 R2テクノロジ入門』（日経BP社、2009年）

ブログ

山市良のえぬなんとかわーるど
http://yamanxworld.blogspot.jp/

自立分散型サーバ監視ソフト
BOM for Windows
Version 7.0

BOM for Windows の製品概要

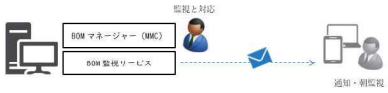
自立分散型サーバー監視ソフトと表現される「BOM for Windows」は、どのような製品なのか、最新版の「BOM for Windows Ver.7.0 SR1」に基づいて基本的な機能や特徴を紹介します。

自立分散型だからスタンドアロンから分散環境まで柔軟に対応できる

Windows Server は、イベントビューアーやパフォーマンスモニター、MMC（Microsoft 管理コンソール）スナップインの管理ツール、標準コマンド、Windows PowerShell など、システム構成やイベント、パフォーマンスを監視し、問題をトラブルシューティングするための豊富な機能や技術を標準で備えています。これらの標準ツールは、問題を認識したあとのトラブルシューティングでは大いに役立ちますが、日々の運用管理を標準ツールだけでこなすのは複数のツールを使い分ける必要があり、非効率的です。そのため、企業では通常、複数台のサーバーや IT 基盤全体を俯瞰的に監視および管理できる管理ツールを利用します。

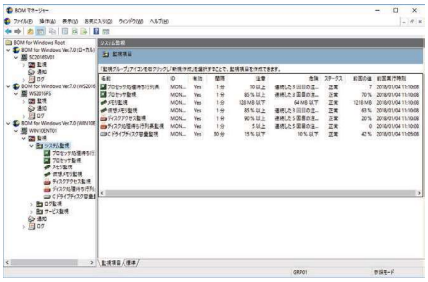
BOM for Windows は、Windows ベースのサーバーのイベントログの監視を中心とした稼働状況の正常性監視に特化したツールとして Windows NT 全盛の 90 年代に登場しました。現在は、ログ監視に加えて、サービス / プロセス、レスポンス、リソースの監視、通知、リカバリ（任意のコマンドの自動実行）機能を備え、Windows は標準で監視でき、Linux、VMware、Oracle、SQL Server、Citrix XenApp などもオプションで監視（いずれも BOM for Windows 経由での監視）できます。また、SNMP トラップや Syslog により、外部のネットワーク監視システムなどと連携することができます。

BOM for Windows の最小構成は、スタンドアロンの Windows Server（または 64 ビット Windows クライアント）へのインストールによるローカル監視です。BOM for Windows のインストールは、監視エージェントである「BOM 監視サービス」と MMC スナップイン形式の管理コンソール「BOM マネージャー」のセットであり、ローカルサーバーの監視や電子メールによる通知が可能です（図 1）。



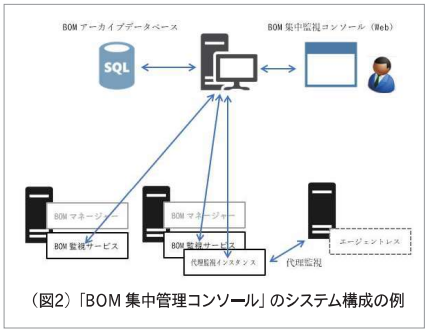
（図1）BOM for Windows の最小構成。
1台のサーバーに導入して監視できる。

少数のサーバーの場合も、各 Windows Server に同じように BOM for Windows をインストールして監視でき、管理者は 1 台のサーバーまたはクライアントの BOM マネージャーのスナップインを監視対象のサーバーにリモート接続することで、BOM マネージャーを 1 つの MMC コンソールにまとめて監視することができます（画面 1）。

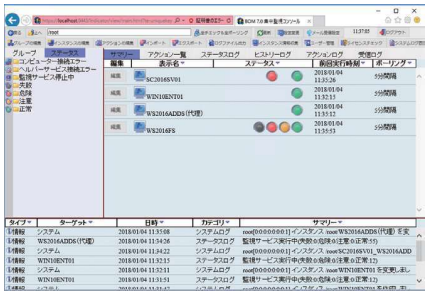


（画面1）MMC スナップイン形式の「BOM マネージャー」。
リモートの監視サービスに接続して複数台を監視できる。

監視対象のサーバーが多数の場合は、「BOM 集中管理コンソール」を導入することで、Web ベースの管理ポータルで全体を俯瞰的に監視することができます（図 2、画面 2）。さらに、「BOM アーカイブマネージャー」を導入することで、ログを蓄積し、長期間の監視データのリスト / グラフ表示やレポート出力できるように拡張できます。



（図2）「BOM 集中管理コンソール」のシステム構成の例

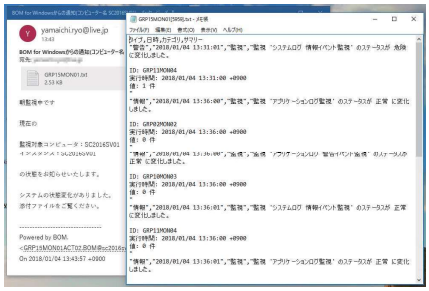

（画面2）「BOM 集中管理コンソール」による俯瞰的なサーバー監視

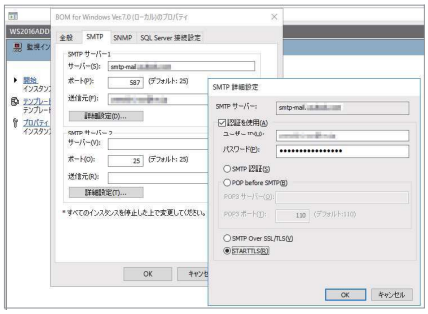
サーバーを変更しないエージェントレス管理（代理監視）

BOM for Windows の基本コンポーネントは、Windows Server 2012 R2 以降および 64 ビット版の Windows 7 SP1 以降にインストールでき、最新の Windows Server 2016 および Windows 10 にも対応済みです。必要なリソースは、監視インスタンスあたり占有メモリ 20MB、占有ディスク 50MB と非常に軽量です。監視対象にコンポーネントをインストールする必要のないエージェントレスの「代理監視」にも対応しているため、運用中のサーバーに一切変更を加えることなく、BOM for Windows による監視を開始することができます（ファイアウォールの調整が必要な場合はあります）。代理管理は、BOM for Windows の基本コンポーネントがインストールされたサーバー（またはクライアント）に、追加の代理監視インスタンスを作成することで可能となり、1 台の BOM for Windows で複数台のサーバーを代理監視の対象にできます。代理監視の場合でも、ローカルサーバーの通常の監視の場合と機能差はありません。

多様なメール環境に対応できるメール通知設定

BOM for Windows では、特定のイベントの発生を電子メールで管理者に通知することが可能です。また、「朝監視」という BOM 特有の機能があり、例えばシステム管理者が毎日チェックしなければならない項目を自動で実行し、その結果（異常の有無や状態の変化など）をまとめてメールで通知することも可能です（画面 3）。


（画面3）BOM for Windows の「朝監視」によるメール通知の例


（画面4）BOM for Windows の柔軟なメール送信設定

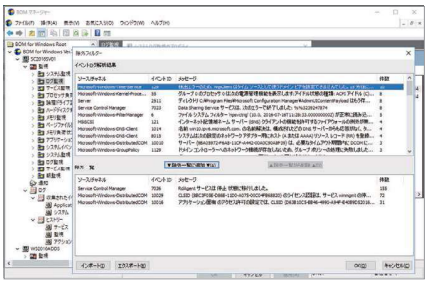
メール通知機能は一般的な監視ツールに標準的に備わっているものですが、その多くはメール送信設定の柔軟性に欠けています。例えば、監視ツールでメールサーバーと SMTP ポートの指定しかできない場合、サービスプロバイダーの多くが実施しているアウトバウンドポート 25 ブロッキング（OP25B）の制限や SSL/TLS 接続、SMTP の認証要求に対応できません。そのような監視ツールからのメール送信に対応するためには、社内のメールサーバーの転送設定を調整したり、あるいは外部のメールサービスへの中継のためだけに SMTP サーバーをセットアップしたりする必要があります。

BOM for Windows のメール通知機能は、SMTP 送信の詳細設定として、SMTP 認証、POP before SMTP、SMTP Over SSL/TLS、STARTTLS をサポートしており、外部のさまざまなメールサービスに柔軟に対応することができます。

Ver.7.0 SR1 の注目の新機能

システムやアプリケーションのログを監視することで、障害をすばやく検知できるほか、パフォーマンス問題や将来の障害につながる可能性のある予兆を捉えることができます。一方で、膨大に記録されるログの中には、一般的に無視できるエラー、あるいはそのシステムでは経験的に無視してよいエラーも多く含まれます。すべてのログを保持することは、管理者がログを調査する際に効率を下げるだけでなく、ディスクリソースの使用の無駄にもつながります。

BOM for Windows Ver.7.0 SR1 では、新たにログ監視の設定において、GUI で除外設定を行う機能が追加されました。その一部である「除外フィルター」を利用すると、収集済みのログの解析結果から選択する方法で除外設定を簡単に定義することができます（画面 5）。不要なログを取得しないことで、管理者は問題の調査に注力することができます。

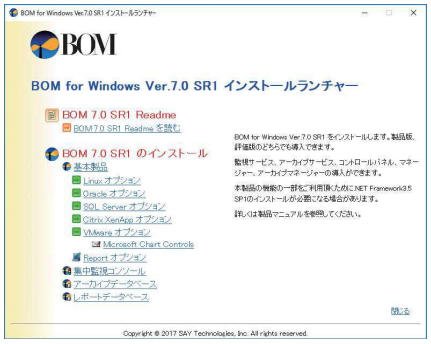

（画面5）イベントログの除外設定をGUIから設定できる機能は、Ver.7.0 SR1 の新機能。除外フィルターのインポート/エクスポートにも対応

簡単に導入し、すばやく監視を始める

最小構成では、BOM for Windows を 1 台のサーバーにインストールし、すばやくサーバーのローカル監視を開始できます。複数台のサーバーにインストールするか、代理監視を構成することで管理対象を拡大していくことができ、さらに BOM 集中監視コンソールを導入することで統合管理が可能になります。インストール手順は非常に簡単であり、定義済みの監視項目を含む豊富なテンプレートが用意されているので、監視対象のシステムの構成や用途に適した監視をすぐに開始できます。1 台のサーバーから簡単に導入でき、柔軟に規模を拡大できるのが、自立分散型である BOM for Windows の特徴です。

スタンドアロン環境への導入と監視

BOM for Windows を導入するには、監視対象のサーバーごとに、BOM for Windows のインストールランチャーの「基本製品」をクリックして、基本コンポーネントをインストールします（画面6）。インストール後に自動開始される「システム設定ウィザード」と「初期設定ウィザード」で、管理ユーザーと参照ユーザーのパスワードの設定、ライセンスの設定、テンプレートの選択、ファイアウォール例外設定の許可など、いくつかの設定を行えば、

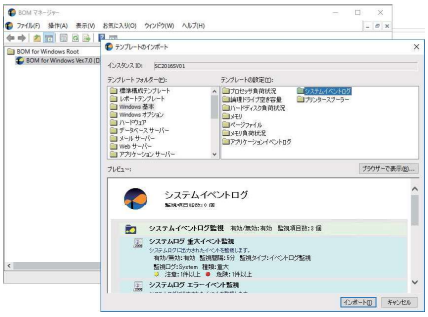


（画面6）インストールランチャーの「基本製品」をクリックして、BOM for Windows の基本コンポーネントをインストールする

すぐに監視が始まります。

「システム設定ウィザード」と「初期設定ウィザード」が開始しなかった場合は、管理ユーザーの既定の初期パスワード（インストールマニュアルに記載）で接続し、「BOM for Windows Ver.7.0（ローカル）」ノードを右クリックして「パスワード変更」と「ライセンスマネージャー」を選択することで、管理ユーザーと参照ユーザーのパスワード設定、ライセンス設定を行えます。また、「BOM for Windows Ver.7.0（ローカル）」ノードを右クリックして「全てのインスタンス監視停止」を選択し、続いて管理対象ノードを右クリックして「テンプレートのインポート」を選択することで、テンプレートに基づいた監視設定を行うことができます（画面7）。

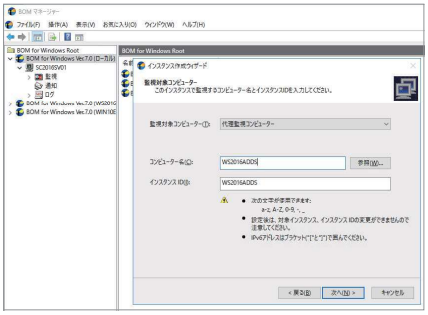
このように、BOM for Windows は、管理ユーザーと参照ユーザーのパスワードでローカルまたはリモートから接続できるため、サーバー監視のためのID 管理とネットワーク構成は非常にシンプルです。ActiveDirectory ドメインを準備したり、ドメインアカウントを作成したりする必要はありませんし、監視対象がドメインメンバーであるか、ワークグループ構成であるかどうかに左右されることがありません。



（画面7）豊富に用意されているテンプレートから1 つ以上のテンプレートをインポートすることで、そのシステムに適した監視をすばやく開始できる

代理監視インスタンスの作成

代理監視を利用すると、運用中のサーバーに BOM for Windows のコンポーネントを導入したり、システム設定を変更したりすることなく、BOM for Windows を導入済みの別のサーバー経由で監視することができます。それには、BOM マネージャーで「インスタンス作成ウィザード」を使用して、監視対象コンピューターとして「代理監視コンピューター」を選択し、コンピューター名と任意のインスタンス ID を指定します（画面 8）。



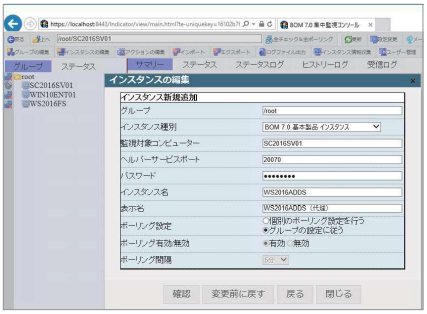
（画面8）BOM for Windows を導入したサーバーに、代理監視用の監視インスタンスを作成する

なお、代理監視でリモート接続するために監視対象のコンピューターにコンポーネントをインストールする必要は一切ありませんが、監視元と監視対象のコンピューターの両方に、共通のユーザー名、共通のパスワードを持つ、Administrators グループのメンバーアカウントが必要です（代理監視用のアカウントを作成することをお勧めします）。また、監視対象側でファイアウォールの例外設定を調整する必要がある場合があります。

BOM 集中監視コンソールの導入

複数台のサーバーを統合的に監視するには、1 台のサーバーに BOM 集中監視コンソールを導入します。MMC スナップインを複数のサーバーにリモート接続するのとは異なり、BOM 集中監視コンソールを利用すると同じページで複数台のサーバーの正常性を視覚的に監視することができます。

BOM 集中監視コンソールを導入するには、BOM for Windows のインストールランチャーの「集中監視コンソール」をクリックして、BOM 監視コンソールをインストールします。特別な設定は必要ありません。インストール後に Web ブラウザーで BOM 集中監視コンソール（https://localhost:8443/）にアクセスし、既定のユーザー名（root）とパスワード（ユーザーズマニュアルに記載）でログインしたら、パスワードの変更やリモート管理用ユーザーの作成（root はローカル接続のみ可能）を行い、監視グループ（既定は /root）に監視対象のインスタンスを追加します（画面 9）。



（画面9）グループに監視対象のインスタンスを追加する。代理監視の場合は、「監視対象コンピューター」にBOM for Windows のサーバーを指定し、「インスタンス名」に監視対象のサーバー名を指定する

トラブル解決には相応の技術力と経験がものを言う

BOM for Windows は、サーバーの正常性を継続的に監視することに特化し、それを得意としたシンプルな監視ツールです。メールや Syslog による通知やイベントログへの書き込みなどで、障害の発生や障害の兆候をすばやく把握することも可能です。しかし、シンプルな一方で、検知した異常な状態を解決するためには、Windows やアプリケーションの知識やトラブルシューティングの技術力と経験が必要です。

BOM for Windows に組み込まれたリカバリーアクションにより、条件に一致した場合のサービスの実行制御や Windows の再起動、カスタムアクションの実行（指定した外部プログラム）で自律的な回復を試みることはできるようですが、これらの方法で解決できない、原因不明のトラブルは常に発生する可能性があります。そのような場合には、やはり Windows が標準で備えている管理ツールや管理インターフェイス、コマンドライン環境、リモートデスクトップ接続などの出番です。例えば、BOM マネージャーのコンテキストメニューから、ローカルまたはリモートサーバーのこれらの標準機能にすばやくアクセスできれば、より便利な監視コンソールになるのではと感じました。

問題の発生から解決までを、監視データと紐づけて履歴として記録するような、インシデント管理や知識ベースの機能もほしいところです。目の前の問題をできるだけはやく解決することはもちろん重要ですが、その経験を知識としてシステム的に蓄積することで、将来に同じサーバー、または別のサーバーで発生する同様の問題に、すばやく対処できるようになるはずです。

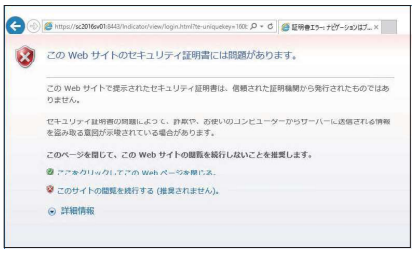
BOM for Windows Ver.7.0 SR1 評価版

BOM for Windows は、ライセンス入力なしまたは評価用ライセンス（代理監視の場合などに必要）を使用して、30日間無料で評価することができます。

BOM for Windows Ver.7.0 SR1 評価版ダウンロード 《 http://www.say-tech.co.jp/product/dl_bomwin.shtml 》

導入時のヒント―集中監視コンソールのSSL/TLS 設定

BOM 集中監視コンソールへのアクセスは、SSL/TLS で暗号化保護されますが、既定では自己署名証明書で構成されており、証明書の警告メッセージが表示されます（画面 10）。「閲覧を続行する」をクリックすることで警告を無視してアクセスすることは可能ですが、運用環境の場合は信頼された SSL/TLS 証明書を使用するように変更するべきでしょう（画面 11）。ただし、製品マニュアルやセイ・テクノロジーズのサポート技術情報には、詳しい手順は説明されていないようです。



（画面10）BOM 集中監視コンソールの既定の状態では、証明書エラーが発生する

（画面11）証明書エラーは解消するためには、このように信頼されたSSL/TLS 証明書に変更する必要がある

BOM 集中管理コンソールは、Apache Tomcat ベースの Web アプリケーションです。信頼された SSL/TLS 証明書に変更するためには、Apache Tomcat の構成が必要です。ここでは、Active Directory ドメイン環境で Active Directory 証明書サービス（AD CS）のエンタープライズ PKI（公開鍵基盤）が展開済みの環境を想定して、SSL/TLS 証明書の発行要求と証明書のインストール方法を紹介します。外部の証明機関を利用する場合も同様の手順で対応できるはずです。

コマンドプロンプトを管理者権限で開き、次のコマンドラインを実行します。以下の例では、既定の鍵ストアである .keystore ファイルをバックアップし、現在の設定（tomcat エイリアス）の設定を削除してから、証明書発行用の新しい鍵を生成しています（※ C:\...> や C:\...\bin> はプロンプトを示しており、コマンドラインには含まれません）。

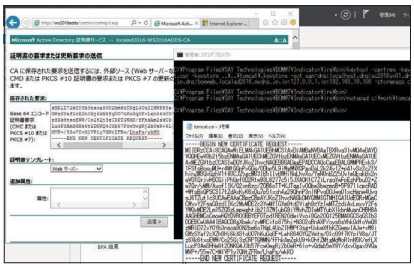
```
C:¥...> cd "C:¥Program Files¥SAY Technologies¥BOMw7¥Indicator¥jre¥bin"

C:¥...¥bin> copy ..¥..¥tomcat¥.keystore ..¥..¥tomcat¥.keystore.bak

C:¥...¥bin> keytool -delete -alias tomcat -keystore ..¥..¥tomcat¥.keystore -
storepass changeit

C:¥...¥bin> keytool -genkey  -alias tomcat -keyalg RSA -keysize 2048 -sigalg
SHA256withRSA -validity 3650 -keystore ..¥..¥tomcat¥.keystore -storepass
changeit

C:¥...¥bin> keytool -genkey -alias tomcat -keyalg RSA -keysize 2048 -sigalg
SHA256withRSA -validity 3650 -keystore ..¥..¥tomcat¥.keystore -storepass
changeit
```

最後のコマンドラインを実行したとき、姓名、組織単位名、組織名、都市名または地域名、都道府県名または州名、国コード（JP）が問われるので、適宜設定します。最後に、鍵パスワードとして changeit（鍵ストアの既定のパスワード）と入力します。

続いて、次のコマンドラインを実行して、新しい CSR（証明書署名要求）ファイルを生成します。この例では、localhost、bomweb、bomweb.ad.local の 3 つの DNS 名と、127.0.0.1 と 192.168.10.106 の 2 つの IP アドレスに対応した証明書を要求する、tomcat.csr を作成しています。

```
C:¥...¥bin> keytool -certreq -keyalg RSA -alias tomcat -file
c:¥work¥tomcat.csr -keystore ..¥..¥tomcat¥.keystore -ext
san=dns:localhost,dns:bomweb,dns:bomweb.ad.local,ip:127.0.0.1,ip:192.168.10.10
6 -storepass changeit
```

AD CS の「証明機関 Web 登録」ポータル（http://<AD CS のサーバー名 >/certsrv/）にアクセスし、「ようこそ：証明書を要求する」「証明書の要求：証明書の要求の詳細設定」「証明書の要求の詳細設定：Base 64 エンコード CME または KPCS #10 ファイルを使用して証明書を送信するか、または Base 64 エンコード PKCS #7 ファイルを使用して更新の要求を送信する」の順番にクリックして、「証明書の要求または更新要求の送信」ページに CSR ファイルの内容を貼り付け、証明書テンプレートとして「Web サーバー」（または適切なテンプレート）を選択し、「送信」ボタンをクリックします（画面 12）。



（画面12）CSR ファイルをAD CS に送信し、PKCS #7 形式の証明書の発行を要求する

「証明書は発行されました」と表示されたら、「DER エンコード」を選択し、「証明書チェーンのダウンロード」をクリックして、発行された証明書ファイル（certnew.p7b）をダウンロードします。なお、外部の証明機関の証明書を使用する場合は、生成した CSR（証明書署名要求）ファイルを認証機関に送信し、SSL/TLS 証明書を PKCS#7 形式（拡張子 .p7b）で取得してください。

最後に、発行された証明書ファイルを Apache Tomcat の鍵ストアにインポートし、BOM 集中管理コンソールのサービス（Bom7Indicator）を再起動します。それには、先ほどと同じコマンドプロンプトの同じディレクトリで以下のコマンドラインを実行します。

```
C:¥...¥bin> keytool -import -trustcacerts -alias tomcat -file
c:¥work¥certnew.p7b -keystore ..¥..¥tomcat¥.keystore -storepass changeit

C:¥...¥bin> net stop Bom7Indicator

C:¥...¥bin> net start Bom7Indicator
```

以上の手順により、BOM 集中管理コンソールで新しい SSL/TLS 証明書が有効になり、証明書エラーは表示されなくなります。

製造・開発元
セイ・テクノロジーズ株式会社
〒112-0005 東京都文京区水道1丁目12-15 白鳥橋三笠ビル8階
TEL.03-5803-2461 FAX.03-5803-2463 ご質問・ご相談 E-mail: sales@say-tech.co.jp