BOM for Windows Ver.8.0

Syslog 受信機能

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

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

表記について

本書では、以下のとおり省略した記載を行う場合があります。

製品名、または省略しない表記	本書での記載（略称）
BOM for Windows Ver.8.0 SR2	BOM 8.0
BOM for Windows Ver.8.0 Syslog 受信機能	BOM Syslog受信機能

使用方法

本書には、BOM Syslog受信機能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。
- 本書を使用するには、Microsoft Windowsオペレーティングシステムについての実際的な知識と、BOM 8.0、Syslog、およびJSONの記述に関する基本的な知識が必要です。
- 本書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で取得した画像を使用しています。お使いの OS 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。
- 本書では"ProgramData"フォルダーがCドライブ直下に存在することを前提としています。何らかの理由で移動させている場合は、現況に合わせて読み替えてください。

第1章 システム構成

1. 動作概要

BOM Syslog受信機能は、BOM 8.0が導入済みのWindowsコンピューターにBOM Syslog受信サービス（Bom8SyslogReceiveService）を追加インストールすることにより動作します。

本機能を使用することで、Linuxサーバーなど Syslog送信が可能な機器から送信されたSyslogメッセージを受信し、受信したSyslogメッセージをWindows OSのアプリケーションイベントログに出力することができます。

このイベントログに出力されたBOM Syslog受信機能のログをBOM 8.0のイベントログ監視で監視することにより、BOM 8.0の監視や各種アクションと連係した動作を実現することができます。

2. システム要件

- インストール先のOSやシステム構成が、BOM 8.0の動作要件に適合していること
- BOM 8.0がインストールされ正常に動作していること
- Syslogの受信に必要なポートが開放されていること
- インストール先ボリュームに10MB以上の空き容量があること

3. BOM Syslog受信機能の動作要件

- BOM Syslog受信機能は、Windowsベースのコンピューターで動作します。
  導入先コンピューターについては、'BOM for Windows Ver.8.0 インストールマニュアル'のシステム要件で確認してください。
- 受信対象のSyslogメッセージは、フォーマットとしてRFC 5424（The Syslog Protocol）のみに対応しています。
  RFC 3164（The BSD syslog Protocol）フォーマットの受信には対応しません。

第2章 インストール

1. 事前準備

BOM Syslog受信サービスをインストールするには、以下の設定を事前に行う必要があります。

- 管理者権限を持つアカウントにてログインしていること
- BOM 8.0 がインストールされ、Windows監視インスタンスのライセンスキーが登録してあること
  - 評価版ライセンスキーは評価期間が切れているものを使用することはできません。
- Syslogメッセージの受信が正常に行えること（受信に必要なポートが開放されていること）
- BOM 8.0 マネージャーを終了していること
  - 監視サービスは稼働していても問題ありません。
- BOM 8.0 コントロールパネルを終了していること

2. インストール手順

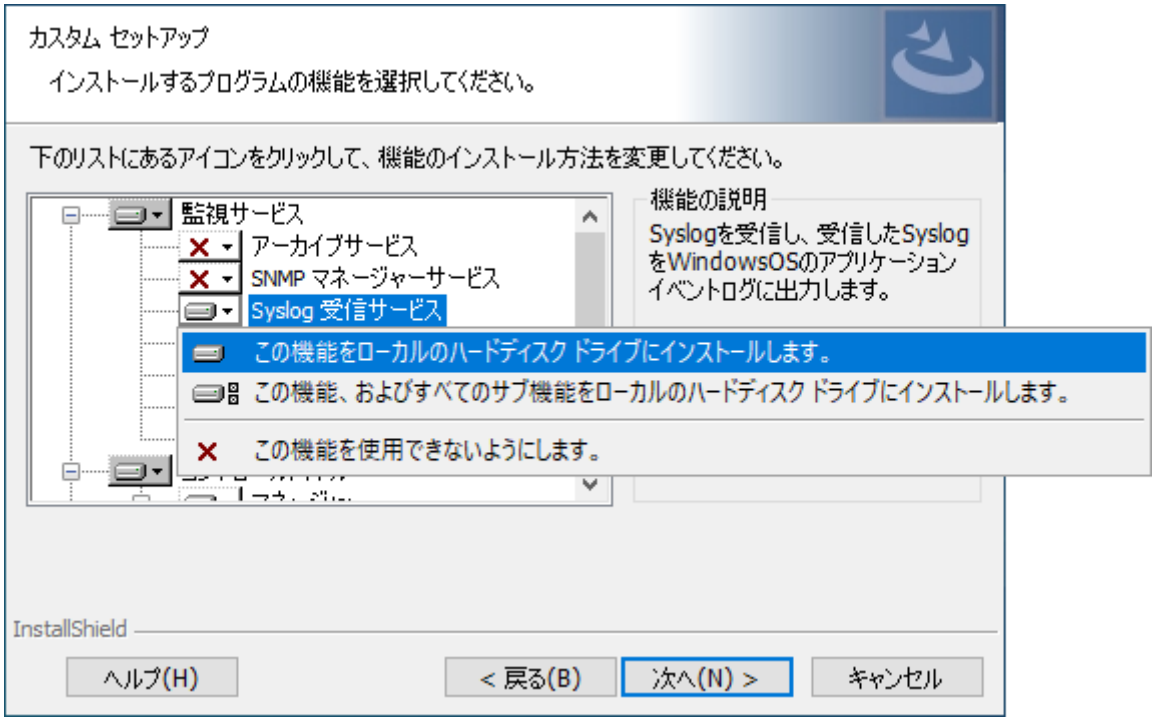
BOM Syslog受信機能を対象のコンピューターにインストールする手順は以下のとおりです。

なお、インストール作業には管理者権限が必要です。管理者権限を持つアカウントにてログオンの上、作業を行ってください。

- 以降の手順は必要な作業項目の概要のみを抽出した概略手順です。BOM 8.0の詳細な導入手順については、'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。

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. "BOM 8.0 のインストール"直下にある"基本製品"をクリックし、セットアップウィザードを起動します。
3. "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。

4. "カスタムセットアップ"画面で"Syslog 受信サービス"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。



5. 以降はセットアップウィザードに従い、"Syslog 受信サービス"のインストールを完了させます。
    - インストールの際、自動でBOM8.0 Syslog受信サービス（Bom8SyslogReceiveService）をWindows Defender ファイアウォールの「受信規則の例外」へ追加します。

第3章 アンインストール

1. 事前準備

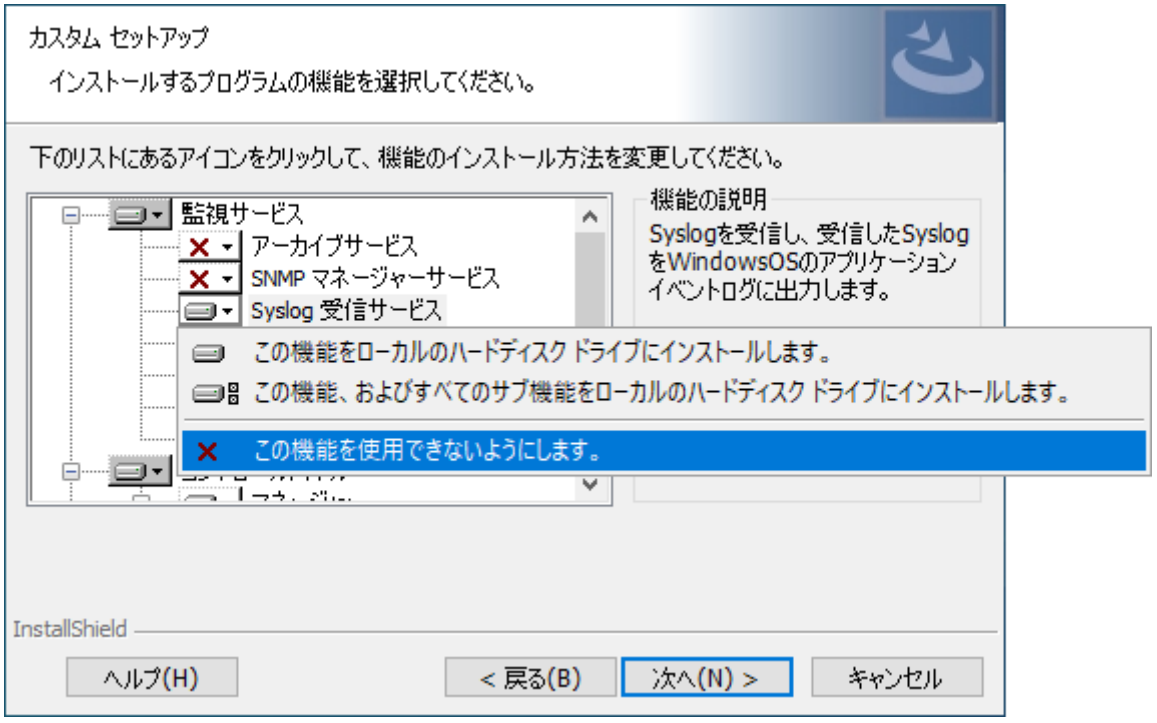
BOM Syslog受信機能をアンインストールする際、アンインストール作業前に下記の作業を実施しておく必要があります。

- 管理者権限を持つアカウントにてログインしていること
- Windowsのイベントビューアーウィンドウが開いていないこと
- BOM 8.0 マネージャーを終了していること
- BOM 8.0 コントロールパネルを終了していること

2. アンインストール手順

BOM Syslog受信機能を対象のコンピューターからアンインストールする手順は以下のとおりです。
なお、アンインストール作業には管理者権限が必要です。管理者権限を持つアカウントにてログオンの上で作業を行ってください。

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. "BOM 8.0 のインストール"直下にある"基本製品"をクリックし、セットアップウィザードを起動します。
3. "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。
4. "カスタムセットアップ"画面で"Syslog 受信サービス"のアイコンをクリックし、"この機能を使用できないようにします。"を選択して、[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、"Syslog 受信サービス"のアンインストールを完了します。

第4章 設定ファイルの編集

1. 設定ファイルの格納場所

Syslogメッセージの受信に必要な設定情報は、以下の設定ファイルに記述します。

C:¥ProgramData¥SAY Technologies¥BOMW8¥Environment¥Config¥syslog¥syslog.json

2. パラメーターおよび設定値

(1) パラメーター一覧

パラメーター	必須	設定値	説明
Protocols	○	-	配下に受信するプロトコルについての設定を記述します。
TCP / UDP / TLS	○	-	配下に、各プロトコルで使用する設定を記述します。各プロトコルは並列で待ち受けします。また使用しないプロトコルについても削除はしないでください。
Port	○	"1"～"65535"の整数値	配下に受信するプロトコルについての設定を記述します。
Certificate	※1	-	配下に、TLSでの受信に使用するサーバー証明書、および秘密鍵ファイルの配置場所を記述します。
CertFilePath	※1	絶対パスを指定 ※3	Syslog受信サーバー上に保存した、サーバー証明書ファイルの配置場所を指定します。
KeyFilePath	※1	絶対パスを指定 ※3	Syslog受信サーバー上に保存した、秘密鍵ファイルの配置場所を指定します。
Filters		-	配下に、Syslogメッセージをイベントログへ出力する際のフィルター条件などを記述します。 配列のため複数指定が可能です。またその際は上位に記述された条件ほど優先度が高くなります。
Condition	※2	"Include"：含まれる "Exclude"：含まれない "Match"：完全一致 "NotMatch"：完全一致しない "RegexInclude"： 　正規表現で含まれる "RegexExclude"： 　正規表現で含まれない	Syslogメッセージをイベントログへ出力する際のフィルター条件を指定します。キーの大文字小文字は区別されません。

Pattern	※2	文字列	"Condition" で検索させる文字列条件を指定します。キーの大文字小文字は区別されます。
Level		"Info"：情報 "Warn"：警告 "Error"：エラー	Syslogメッセージをイベントログへ出力する際のログレベルを指定します。指定がない場合は"Info"となります。また、キーの大文字小文字は区別されません。

※1 TLSを使用する場合は指定が必須です。また使用しない場合でもパラメーターは削除せず残してください。
※2 フィルター設定を行なう際は必須です。
※3 "￥"はエスケープ表記で"￥￥"と記述してください。また環境変数およびBOM 8.0固有の置き換えパスも使用できます。詳しくは 'CertFilePath、KeyFilePath指定の詳細' を参照してください。

(2) CertFilePath、KeyFilePath指定の詳細

"CertFilePath"と"KeyFilePath"にはOSに用意された環境変数、およびBOM 8.0固有の置き換えパスが使用できます。

- 環境変数の例
  - %COMPUTERNAME%
    コンピューター名に置き換えされます。
    - 環境変数を使用する場合、実際にその名称のフォルダーが存在した場合でも環境変数としての置き換えが優先されます。

    (例：コンピューター名が "syslog-server" の場合)
    指定文字列　：C:¥¥%COMPUTERNAME%¥¥server.crt
    実際の配置先：C:¥syslog-server¥server.crt

    この際、C: 直下に「%COMPUTERNAME%」という名称のフォルダーが存在する場合でも、環境変数として置き換えされます。

- BOM 8.0固有の置き換えパス
  - %DataDir%
    "ProgramData"フォルダー配下のBOM 8.0インストール先に置き換えされます。

    (例)
    指定文字列　：%DataDir%Environment¥¥Config¥¥syslog¥¥server.crt
    実際の配置先：C:¥ProgramData¥SAY Technologies¥BOMW8¥Environment¥Config¥syslog¥server.crt

3. フィルター設定の注意

- パラメーター "Filters"の配下は配列のため、"Filters"の直下は "[" "]" (大カッコ、ブラケット) で囲んでください。

4. 記述例

```
{
 "Protocols": {
  "TCP": { "Port": 1514 },
  "UDP": { "Port": 514 },
  "TLS": {
   "Port": 6514,
   "Certificate": {
    "CertFilePath": "%DataDir%Environment¥¥Config¥¥syslog¥¥server.crt",
    "KeyFilePath": "%DataDir%Environment¥¥Config¥¥syslog¥¥server.key"
   }
  }
 },
 "Filters": [
  {
   "Condition": "Include",
   "Pattern": "含まれる文字列",
   "Level": "Info"
  },
  {
   "Condition": "Exclude",
   "Pattern": "含まれない文字列",
   "Level": "Warn"
  },
  {
   "Condition": "Match",
   "Pattern": "完全一致する文字列",
   "Level": "error"
  },
  {
   "Condition": "NotMatch",
   "Pattern": "完全一致しない文字列"
  },
  {
   "Condition": "RegexInclude",
   "Pattern": "含まれる文字列を正規表現で記述"
  },
  {
   "Condition": "RegexExclude",
   "Pattern": "含まれない文字列を正規表現で記述"
  }
 ]
}
```

第5章 TLS通信を使用する場合

BOM Syslog受信機能でTLS通信を使用する際は、受信側 (サーバー)と送信側 (クライアント)のそれぞれで秘密鍵、証明書などの準備が必要です。

1. 受信 (サーバー) 側の準備について

受信側で必要な秘密鍵およびサーバー証明書には、"Syslog 受信サービス"を追加インストールした時点で生成される以下のファイルが使用できます。

```
秘密鍵ファイル：
  "C:¥ProgramData¥SAY Technologies¥BOMW8¥Environment¥Config¥syslog¥server.crt"
サーバー証明書ファイル：
  "C:¥ProgramData¥SAY Technologies¥BOMW8¥Environment¥Config¥syslog¥server.key"
```

各ファイルは以下の仕様で作成されています。

- 秘密鍵
  - RSA 4096bit
- サーバー証明書
  - SHA256
  - 有効期間 作成から10年

サーバー証明書を再作成する場合

以下の場所に、秘密鍵およびサーバー証明書ファイルの再作成に使用できるツールを格納しています。

```
[BOM 8.0 インストールフォルダー]¥BOMW8¥Bin¥BomSyslogGenerateCert.exe
```

※ 既定のインストールフォルダーは"C:¥Program Files¥SAY Technologies"です。

- 使用方法
  引数1に秘密鍵の出力先およびファイル名、引数2にサーバー証明書の出力先およびファイル名を指定して実行します。

  ```
  BomSyslogGenerateCert.exe [引数1 (秘密鍵の出力先およびファイル名)] [引数2 (サーバー証明書の出力先およびファイル名)]

  (例)
  BomSyslogGenerateCert.exe C:¥temp¥syslog¥server.key C:¥temp¥syslog¥server.crt
  ```

2. 送信 (クライアント) 側の準備について

送信 (クライアント) 側でクライアント証明書を作成、および配置してください。

作成方法と作成後の設定方法については、使用するOSやアプリケーションのガイドを参照してください。

第6章 サービスの開始・停止

1. Syslog 受信サービスの開始

Windows 管理ツールの「サービス」を起動し、「Bom8SyslogReceiveService」を開始してください。

サービスの開始後は、設定内容に基づいてフィルター後のSyslogメッセージがApplication イベントログに出力されます。出力されるイベントログの仕様は、「出力されるイベントログについて」を参照してください。

2. Syslog 受信サービスの停止

Windows 管理ツールの「サービス」を起動し、「Bom8SyslogReceiveService」を停止してください。

第7章 出力されるイベントログについて

Syslog受信サービスから出力されるイベントログは、以下の通りです。

- イベントログのノード：Windows イベントログ¥Application
- メッセージソース：BOM8SyslogReceiveService
- メッセージIDとレベル

メッセージID	イベントレベル	内容
1100	情報	BOM Syslog受信サービスの開始ログ
1101	情報	BOM Syslog受信サービスの停止ログ
1110	エラー	サービス実行に関する失敗ログ (内容は都度異なります)
1120	エラー	Syslogメッセージ受信処理に関するエラー (内容は都度異なります)
2000	エラー / 警告 / 情報	受信したSyslogメッセージ (設定により、イベントレベル、内容は異なります。)
6100	エラー	サービスの初期化で失敗した場合のログ
6103	エラー	有効なBOM 8.0のライセンスが存在しなかった場合のエラーログ

第8章 ライセンス表記

BOM Syslog受信機能では、それぞれのライセンス形態に従ってオープンソースソフトウェアを利用しています。
各ソフトウェアを開発された開発者、および開発コミュニティの皆様に深く感謝いたします。

- 各ソフトウェアを開発された開発者、および開発コミュニティにより同梱が定められたオープンソースのライセンス条文については、以下のフォルダーに同梱されています。

  ```
  [BOM 8.0 インストールフォルダー]¥BOMW8¥Common¥Licenses
  ```

  ※ 既定のインストールフォルダーは"C:¥Program Files¥SAY Technologies"です。

【BOM Syslog受信機能で使用しているオープンソースソフトウェアの例】

- asio
- A basic Windows service in C++ (CppWindowsService)
- fmt

BOM for Windows Ver.8.0 Syslog 受信機能ユーザーズマニュアル

2025年1月31日 初版

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 8.0.20.0