BOM for Windows Ver.8.0 SR2

Syslog受信機能ホワイトペーパー

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

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「™ (Trademark)」、「® (Registered Trademark)」を明記しておりません。

目次

第1章　はじめに

本書は、BOM for Windows Ver.8.0 SR2 (以降、BOMまたはBOM 8.0 SR2と表記) の新機能であるSyslog受信機能の概要と仕様、活用例を解説したホワイトペーパーです。BOM Syslog受信機能についてはBOM付属の「Syslog受信機能ユーザーズマニュアル」も併せてご参照ください。Syslogクライアントの構成や、BOM本体の操作方法および解説については、本書では省略しています。Syslogクライアントに関するドキュメントや製品マニュアル、BOM付属の各種マニュアルをご参照ください。

第2章　BOM Syslog受信機能について

2.1　概要

BOM Syslog受信機能は、BOMが導入済みのWindowsコンピューターにSyslog受信サービス (Bom8SyslogReceiveService) をインストールすることにより動作します。この機能は、Linuxサーバーやネットワーク機器、サーバーハードウェアのベースボード管理コントローラーが備えるシステムイベントログ (SEL) のSyslog送信機能など、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、受信したメッセージをWindowsのApplicationイベントログに出力します。BOM Syslog受信機能でWindowsコンピューターに集約されたイベントログは、BOMのイベントログ監視機能で監視することで障害などの異常を検知し、各種アクションと連携した動作を実現します。例えば、オープンソースの統合監視ツールとして人気のあるZabbixと連携 (Zabbixサーバーからのログの監視またはZabbixサーバーへのログ転送) すること可能です (図1) 。

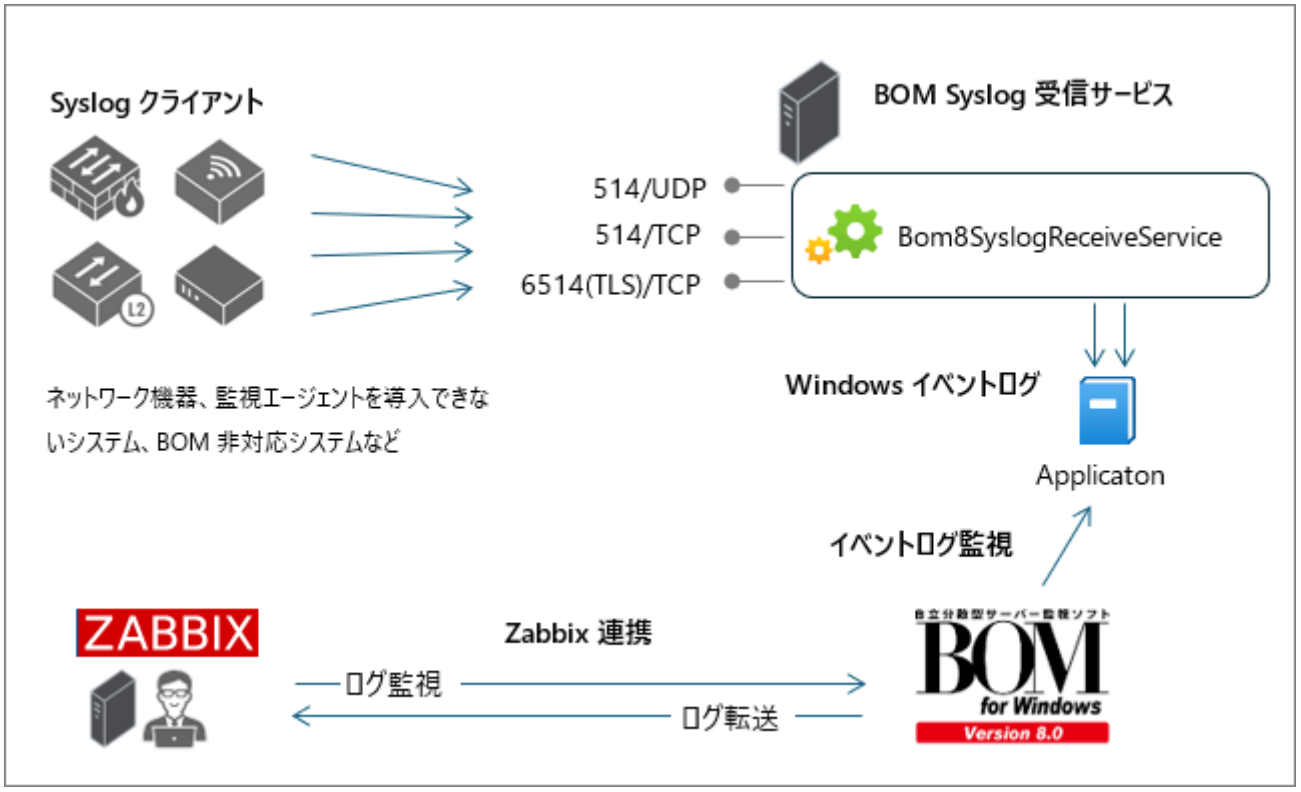


図1　BOMのSyslog受信機能の導入イメージ

2.1　動作要件

BOM Syslog受信サービスの動作要件は、以下に示した通りです。

- BOM Syslog受信サービスをインストールするWindowsコンピューターが、BOMの動作要件に適合しており、BOMがインストールされ、有効なBOMライセンス (評価版を含む) が割り当てられていること。
- Syslogの受信に必要なTCP/UDPポートが未使用であること。既定のポートは、 既定は514/TCP、514/UDP、6514/TLS over TCPであり設定ファイル (syslog.json) を使用して変更可能です。
- 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。

Zabbix連携の要件 (オプション)

このホワイトペーパーの第4章では、BOMのイベントログ監視機能によるSyslogメッセージの監視に加え、Zabbixとの連携した活用シナリオについて説明しています。このホワイトペーパーは、Zabbix Server 7.0 LTSおよびWindows用Zabbix Agent 2 v7.0を使用して動作検証を行いました。Zabbixとの連携を行う場合は、以下のいずれかの要件を満たす必要があります。

- BOM Syslog受信サービスで受信したログをZabbixサーバーから管理するためには、BOMのWindowsコンピューターにZabbix Agent 2がインストールされており、ZabbixサーバーにWindowsコンピューターが監視対象のホスト (Zabbix Agent Active) として登録されている必要があります。
- zabbix_senderを使用してZabbixサーバーにログを転送する場合は、Zabbix Agent 2またはZabbix Agentがインストールされている必要がありますが。BOMがインストールされたWindowsコンピューターのホスト登録は必須ではありません。

2.2　Syslog受信仕様

BOM Syslog受信サービスのSyslog受信機能は、以下の仕様に従います。

- RFC 5424 (https://datatracker.ietf.org/doc/html/rfc5424) に準拠
- 2,048バイトまでのメッセージを受信可能 (PRI部《存在する場合はLEN部》からMSG終端まで)
- 文字コードはUTF-8 (BOMなし) として処理される
- メッセージ長 (LEN部) が含まれる場合、それを無視してシングルパケットメッセージ単位で受信し処理される

注意:
BOM Syslog受信サービスは、RFC 5424 (IETF-syslog) 形式のメッセージのみを受信します。従来からのBOMの機能であるSyslog送信アクションは、RFC 3164 (https://datatracker.ietf.org/doc/html/rfc3164) 形式 (BSD-syslog) にのみ対応しています。そのため、BOMのSyslog送信アクションでBOM Syslog受信サービスに対して送信されたメッセージは、イベントログに書き込まれません。BOMのSyslog送信アクションについては、将来のリリースまたは修正パッチにより、RFC 5424に対応する予定です。

2.3　イベントログの仕様

BOM 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: Application

メッセージソース: BOM8SyslogReceiveService

イベントID、イベントレベル、イベント説明:

イベントID	イベントレベル	イベント説明
1100	情報	BOM Syslog受信サービス 開始しました
1101	情報	BOM Syslog受信サービス 停止しました
1110	エラー	サービスの失敗ログ (内容は都度異なる)
1120	エラー	受信処理の致命的エラー
2000	エラー、警告、または情報	受信したSyslogメッセージ、イベントのレベルは設定ファイル (syslog.json) のフィルター条件 (Filters) で制御
6100	エラー	BOM Syslog受信サービス の初期化に失敗しました.{エラー内容}
6103	エラー	有効なBOM8ライセンスが存在しません。BOM Syslog受信サービスを停止します

イベントID 2000のイベント説明には、ヘッダー (HEADER部)、構造化データ (STURCTURED-DATA部)、メッセージ (MSG部)で構成される、以下のRFC 5424形式のSyslogメッセージが書き込まれます。LEN部 (メッセージ長) は、Syslogクライアントによっては含まれない場合があります。PRI部は、メッセージのファシリティ (Facility) の番号を8倍したものに、重大度 (Severity) の番号を加えた数値を山括弧<>で囲んだものです。詳細については、RFC 2524でご確認ください。

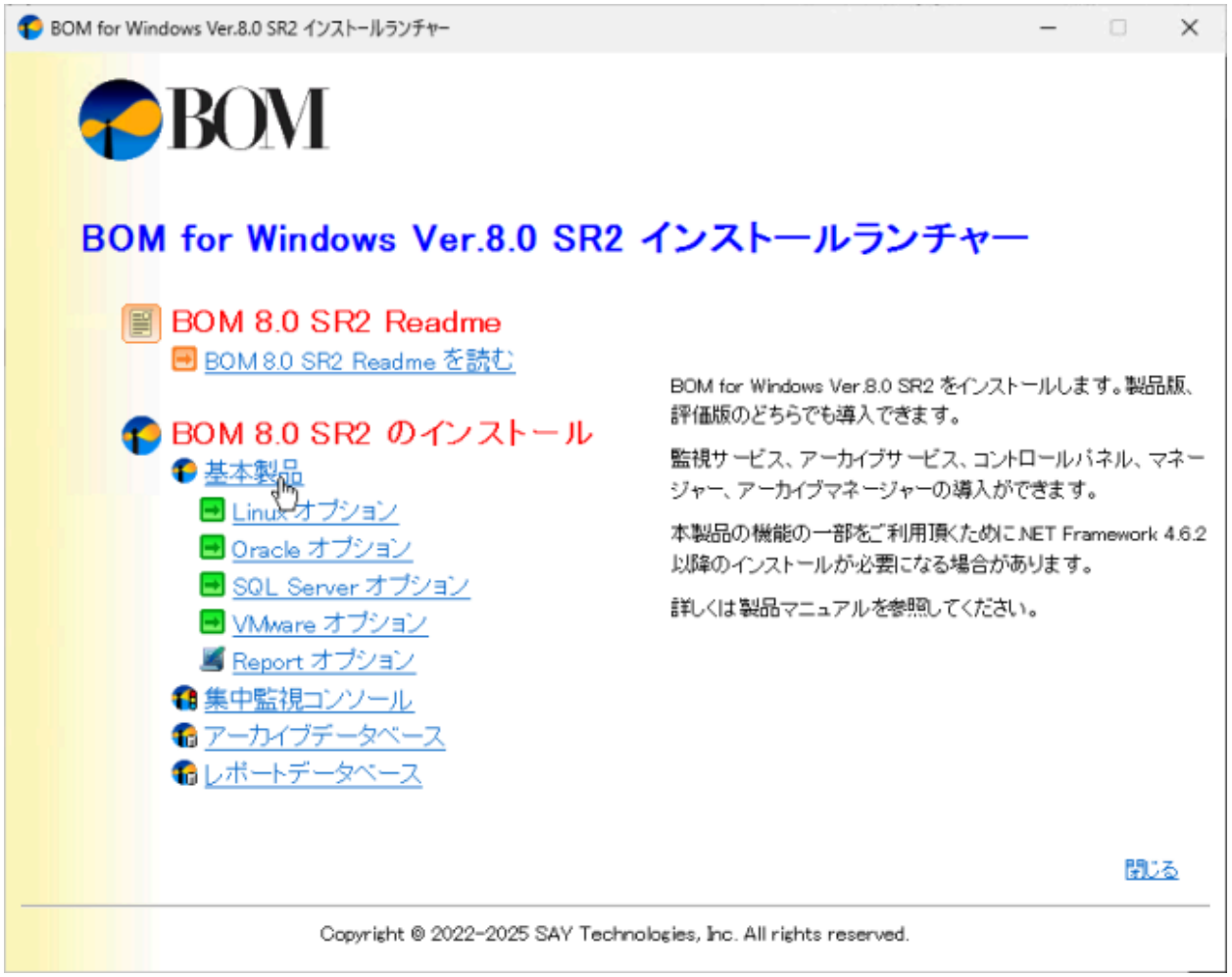
HEADER	STRUCTURED-DATA	MESSAGE
LEN PRIVERSION TIMESTAMP HOSTNAME APPLICATION PID MESSAGEID 例: <13>1 2025-02-03T09:57:51.166769+09:00 WS2022VM01 wsluser - 10 Notice: syslog test	[STRUCTURED-DATA] 例: [timeQuality tzKnown="1" isSynced="1" syncAccuracy="1025"])	MSG 例: Notice: syslog test

第3章　BOM Syslog受信サービスのインストールと構成

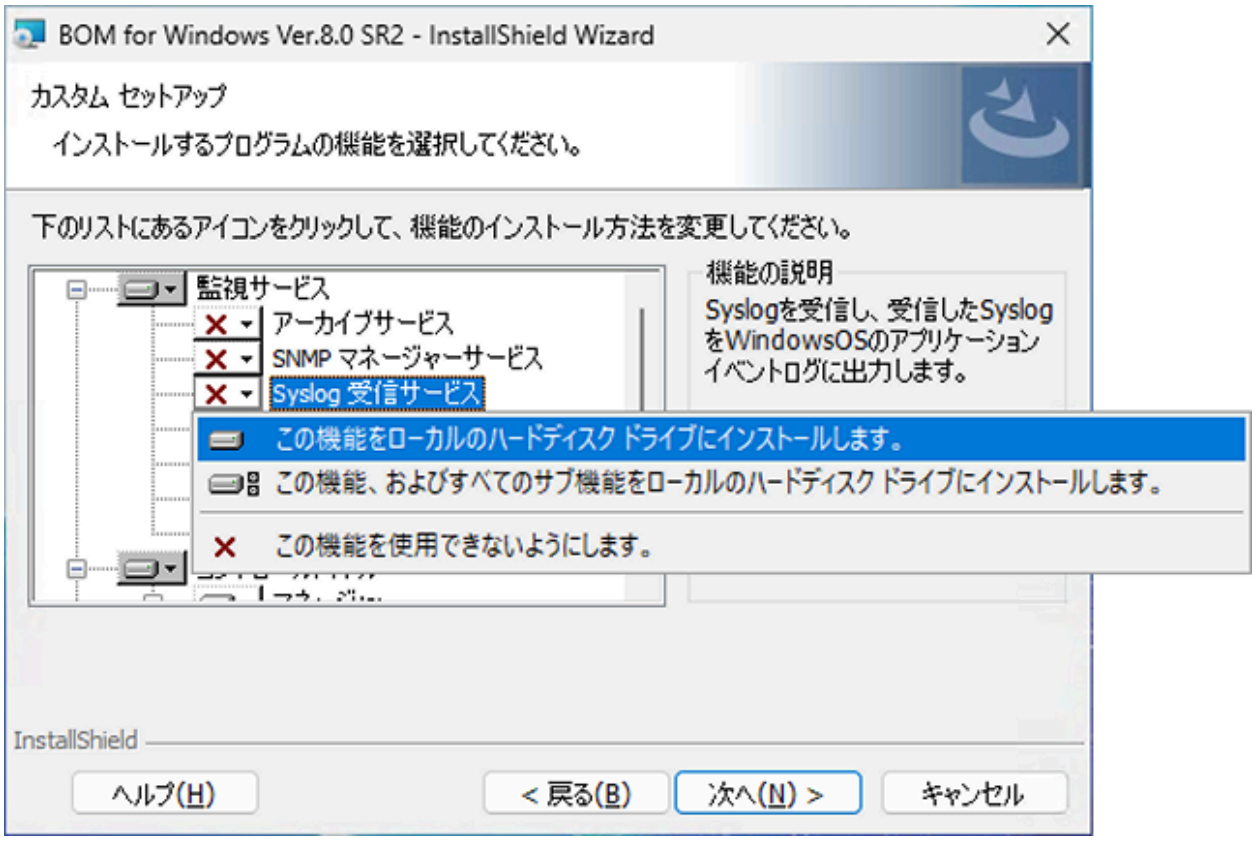
3.1　BOM Syslog受信サービスのインストール

BOMがインストールされているWindowsコンピューターに、BOM Syslog受信サービスを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 (ローカルやドメインのAdministratorなど、Administratorsローカルグループのメンバー) でログオンした上で作業を行ってください。

1. BOM 8.0 SR2のインストールメディアのルートにある「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 SR2のインストール」のすぐ下にある「基本製品」をクリックし、インストールウィザードを開始します。



3. 「次へ」をクリックして「プログラムの保守」の画面に進んだら、「変更」を選択して、「次へ」をクリックします。
4. 「カスタムセットアップ」の画面で「監視サービス」の下にある「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」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、インストールを完了します。

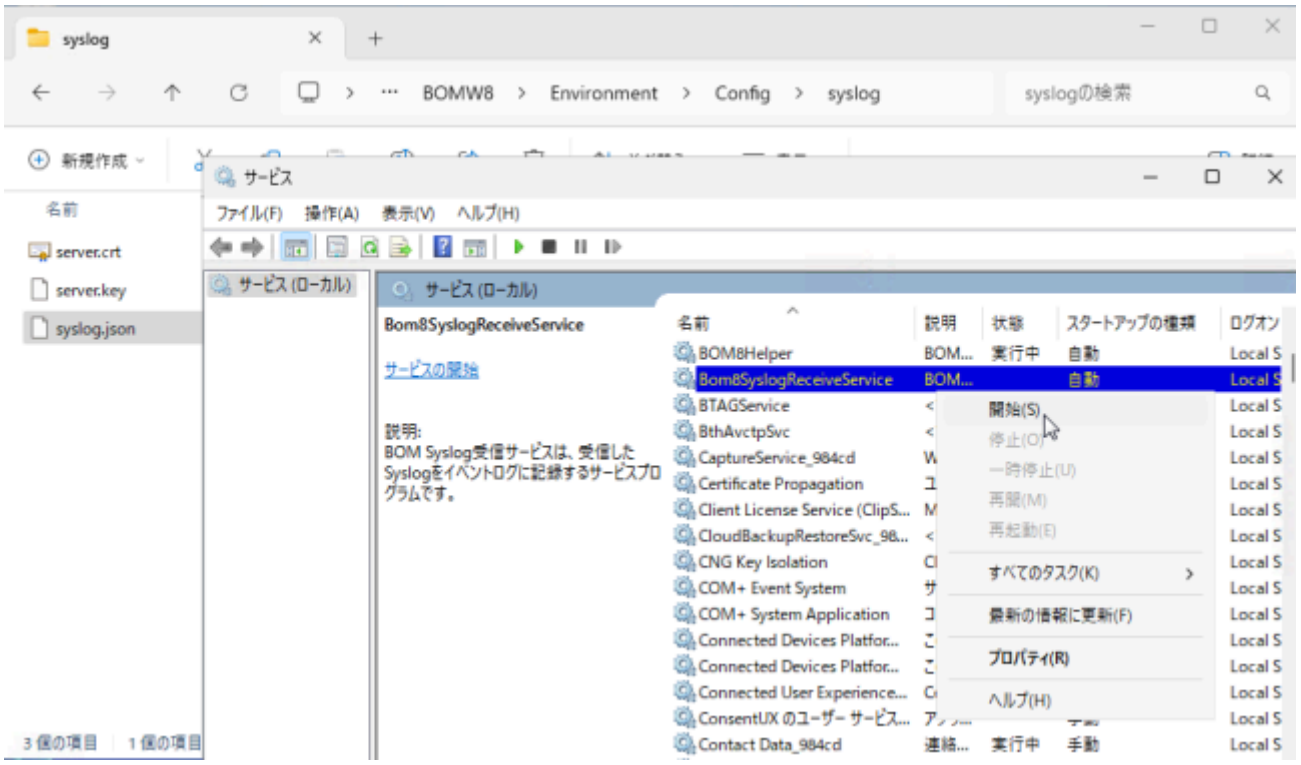
3.2　BOM Syslog受信サービスのポートと証明書の構成

BOM Syslog受信サービスの設定ファイル「syslog.json」は、以下の場所にあります。

```
%ProgramData%¥SAY Technologies¥BOMW8¥Environment¥Config¥syslog
```

設定ファイルには既定でTCP、UDP、TLS over TCPのポート番号 (514/UDP、514/TCP、6514/TCP) とTLS用の証明書の設定を含みます。ポート番号の変更が必要な場合や、独自の証明書を使用したい場合は、この設定ファイルを編集して上書き保存します。設定ファイルを変更したら、「Bom8SyslogReceiveService指定可能なパラメーターおよび設定値については、BOM付属の「Syslog受信機能ユーザーズマニュアル」をご参照ください。

設定ファイルを確認し、必要に応じて変更したら、「Bom8SyslogReceiveService」サービスを開始します。このサービスのスタートアップは「自動」ですが、BOM Syslog受信サービスをインストールした直後は自動開始されません。「サービス」スナップイン (Services.msc) を開いて、「Bom8SyslogReceiveService」サービスを右クリックし、「開始」をクリックします。これでSyslogクライアントからのメッセージを受信することができるようになります。



なお、BOM Syslog受信サービスをインストールすると、「セキュリティが強化されたWindows Defender ファイアウォール」 (wf.msc) の「受信の規則」に「BOM 8.0 Syslog受信サービス」という規則が追加され、すべてのファイアウォールプロファイルで有効になります。この規則はプログラム (BomSyslogReceiveService.exe) に対する受信の許可設定であるため、ポート番号を変更したとしても、そのポートに対する受信の規則を追加する必要はありません。

Syslog受信テスト

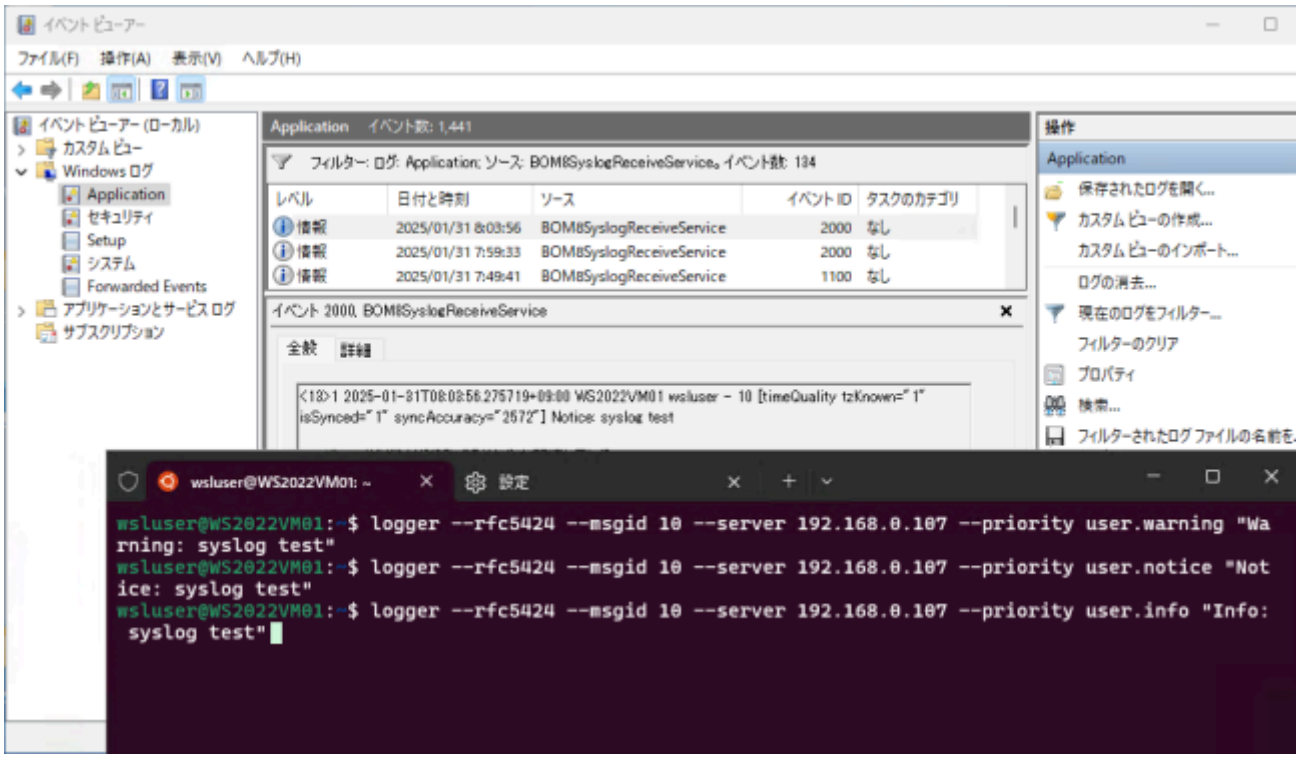
BOM Syslog受信サービスをインストールし、サービスを開始したら、SyslogクライアントからRFC 5424形式でSyslogメッセージを送信し、WindowsイベントログのApplicationログにイベントID「2000」のイベントとして書き込まれることを確認してください。メッセージがイベントログに書き込まれない場合は、SyslogクライアントがRFC 5424形式に対応しているかどうかを確認してください。

Linuxを利用可能な場合は、loggerコマンドを次のように実行することで、RFC 524形式でSyslogメッセージを指定したIPアドレスに送信することができます。なお、Loggerコマンドが送信可能なメッセージ (MSG部) は最大1,024バイトです。

```
logger --rfc5424 --msgid 10 --server <BOM Syslog受信サービスのIPアドレス> --priority user.warning "Warning: syslog test"
(ポート番号とプロトコルを指定する場合は --port <ポート番号> --udpまたは--tcp を指定)
```

Windows Server 2022以降の場合は、次のコマンドラインを実行して再起動することで、Windows Subsystem for Linuxバージョン2 (WSL 2) を有効化し、Ubuntuディストリビューションをインストールして、Ubuntuのシェルを Windows上で実行することができます。loggerコマンドはWSL 2のUbuntuのシェル環境から標準で利用できます。

```
wsl --install
```



参考:

Windows ServerにLinuxサブシステムをインストールする | Windows Server (Microsoft Learn)
https://learn.microsoft.com/ja-jp/windows/wsl/install-on-server

3.3　フィルター条件によるイベントレベルの制御

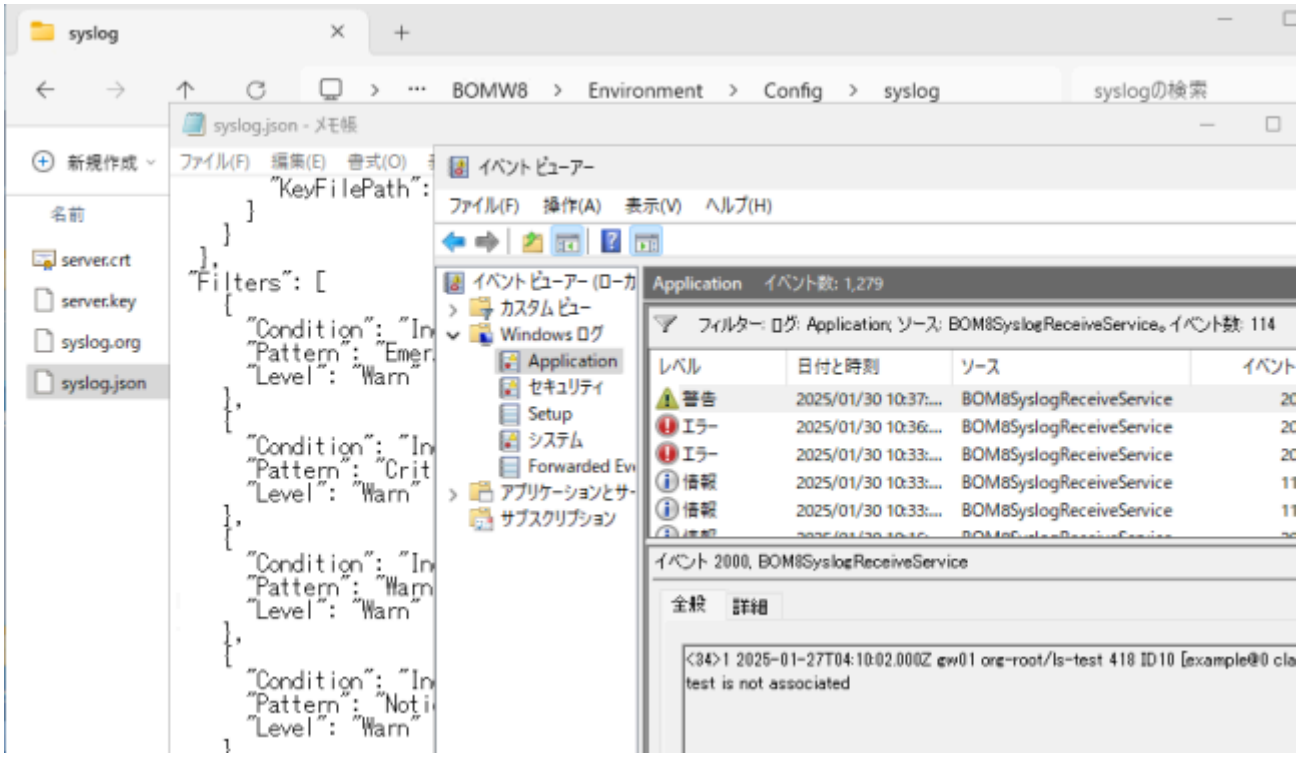
BOM Syslog受信サービスは受信したSyslogメッセージを、既定で「情報」レベルのイベントとしてApplicationログに書き込みます。設定ファイルにフィルター条件を追加すると、メッセージの内容に応じてイベントレベルを「情報 (Info) 」「警告 (Warn) 」「エラー (Error) 」に振り分けることができます。次のフィルターの設定例は、Syslog メッセージ (MSG) に重大度 (Severity) が含まれていることを前提としており、“Error”の文字列が含まれる場合に「エラー (Error) 」、重大度“Notice”以上の文字列が含まれる場合に「警告 (Warn) 」、それ以外は「情報 (Info) 」イベントとして書き込む例です。なお、フィルター条件以外の設定は既定値のままです。

syslog.jsonの記述例:

```
{
  "Protocols": {
    "TCP": {
      "Port": 514
    },
    "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": "Emergency",
      "Level": "Warn"
    },
    {
      "Condition": "Include",
      "Pattern": "Critical",
      "Level": "Warn"
    },
    {
      "Condition": "Include",
      "Pattern": "Warning",
      "Level": "Warn"
    },
    {
      "Condition": "Include",
      "Pattern": "Notice",
      "Level": "Warn"
    },
    {
      "Condition": "Include",
      "Pattern": "Error",
      "Level": "Error"
    },
    {
      "Condition": "Include",
      "Pattern": "Debug",
      "Level": "Info"
    },
    {
      "Condition": "Include",
      "Pattern": "Debug",
      "Level": "Info"
    }
  ]
}
```

(※ ConditionおよびLevelは大文字小文字を区別しませんが、Patternは大文字小文字が区別されます。)



ここで示したフィルター条件は、Syslogメッセージ (MSG) に Syslog の重大度を示す文字列 (Criticalや Errorなど) が含まれていることを前提に、その文字列で振り分けを制御するという簡単なものです。Syslogメッセージのヘッダー (HEADER) のPRI部 (<Facility番号×8＋Severity番号>) や構造化データ (STURCTURED-DATA) を完全一致 (Match、NotMatch)や正規表現 (RegexInclude、RegexExclude) でフィルターすることもできるでしょう。運用環境ではフィルター条件なしでしばらく運用し、実際に受信したメッセージに基づいて、フィルター条件を検討、設定してください。フィルター条件のすべてのオプションについては、BOM付属の「Syslog受信機能ユーザーズマニュアル」をご参照ください。なお、設定ファイルを変更したら、「Bom8SyslogReceiveService」サービスの再起動 (停止、開始) が必要です。

第4章　BOM Syslog受信機能の活用シナリオ

4.1　BOMのイベントログ監視: 複数デバイスからのSyslogメッセージを集中監視

BOM Syslog受信サービスを導入すると、ネットワーク上の複数のSyslogクライアントからSyslogメッセージが受信され、設定ファイル「syslog.json」のフィルター条件に基づいて、イベントレベル「情報」「エラー」「警告」のイベントに振り分けられ、WindowsイベントログのApplicationログにイベントソース「BOM8SyslogReceiveService」、イベントID「2000」のイベントとして書き込まれます。つまり、Applicationログには、複数のデバイスからのSyslogメッセージが集約されることになります。

BOM標準の監視項目「イベントログ監視」を使用すると、GUIを使用して、イベントレベル、ログ、イベントID、イベントの内容のテキスト検索などでWindowsイベントログをフィルターし、イベントの件数を監視したり、監視結果に基づいて各種アクション (メール通知やコマンド実行など) を自動実行させることができます (図2) 。

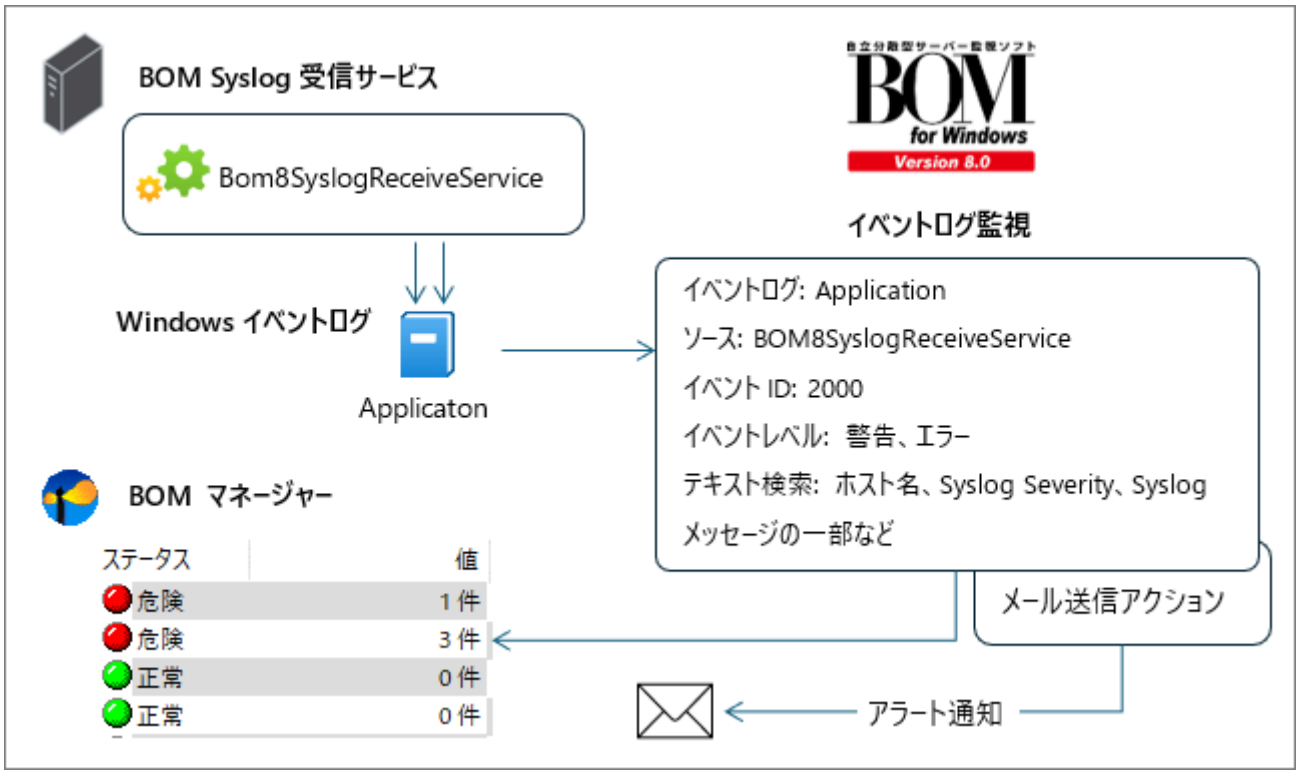
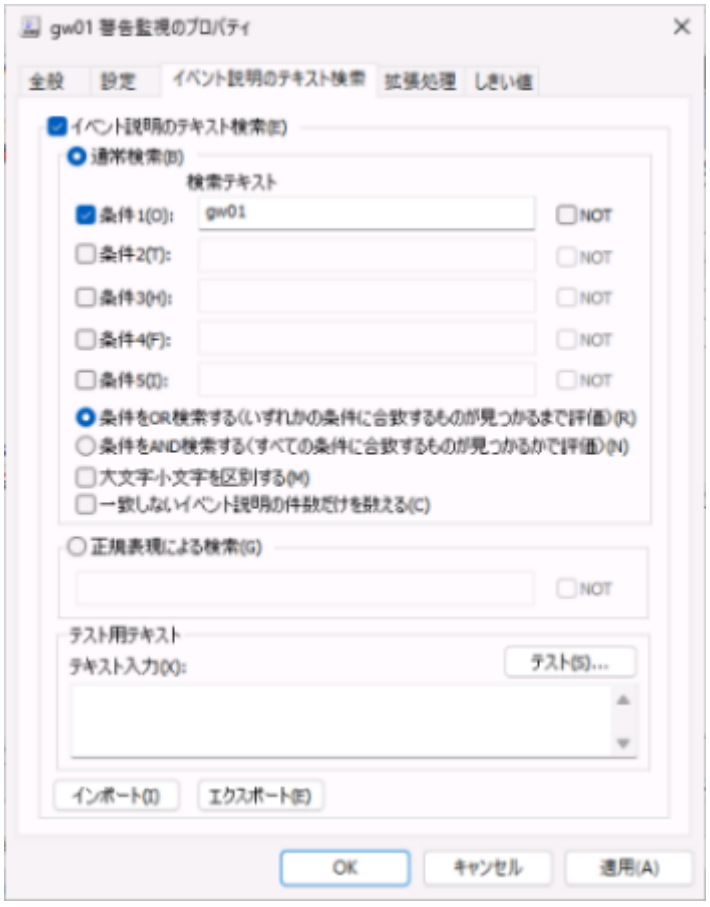


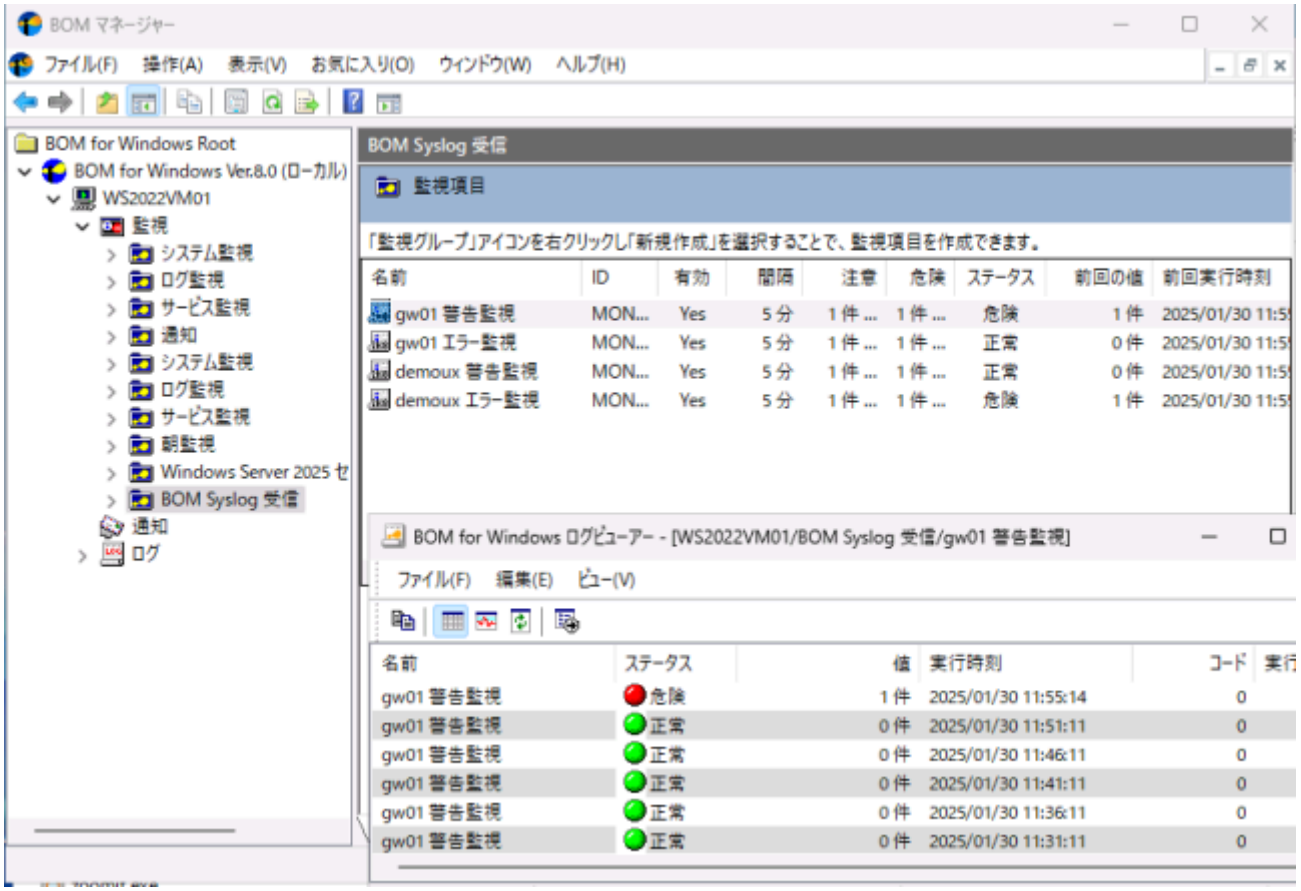
図2　BOMによる監視シナリオ、BOM Syslog受信サービスが集約したSyslogメッセージをBOMのイベントログ監視で監視する

特定のホストからの「警告」イベントを監視するには、監視項目「イベントログ監視」のプロパティの「設定」タブで、イベントレベル「警告」だけを選択し、イベントログ「Application」、ソース/チャネル「BOM8SyslogReceiveService」、イベントID「2000」を監視するように設定します。

さらに、特定のホストからのイベントだけをフィルターするために、「イベント説明のテキスト検索」タブでイベント説明に含まれるホスト名をテキスト検索の条件に設定します。



監視対象のホストごと、イベントレベルごとにこのような監視項目を設定することで、BOMのWindowsコンピューターに集約されたSyslogメッセージを監視して、デバイスごとの状態を把握することができます。



4.2　Zabbix連携: Zabbixアクティブエージェントによるログファイルのリモート監視

ZabbixとBOM Syslog受信機能の連携シナリオの1つは、BOM Syslog受信サービスが受信し、イベントログに書き込んだものを、Zabbixサーバーからリモートで監視することです。Windowsイベントログを Zabbixサーバーから監視する方法はいくつかありますが、ここではBOM側でイベントログをテキストログ化し、Zabbixサーバーのlog() キーアイテムを使用してリモート監視する方法を紹介します (図3) 。

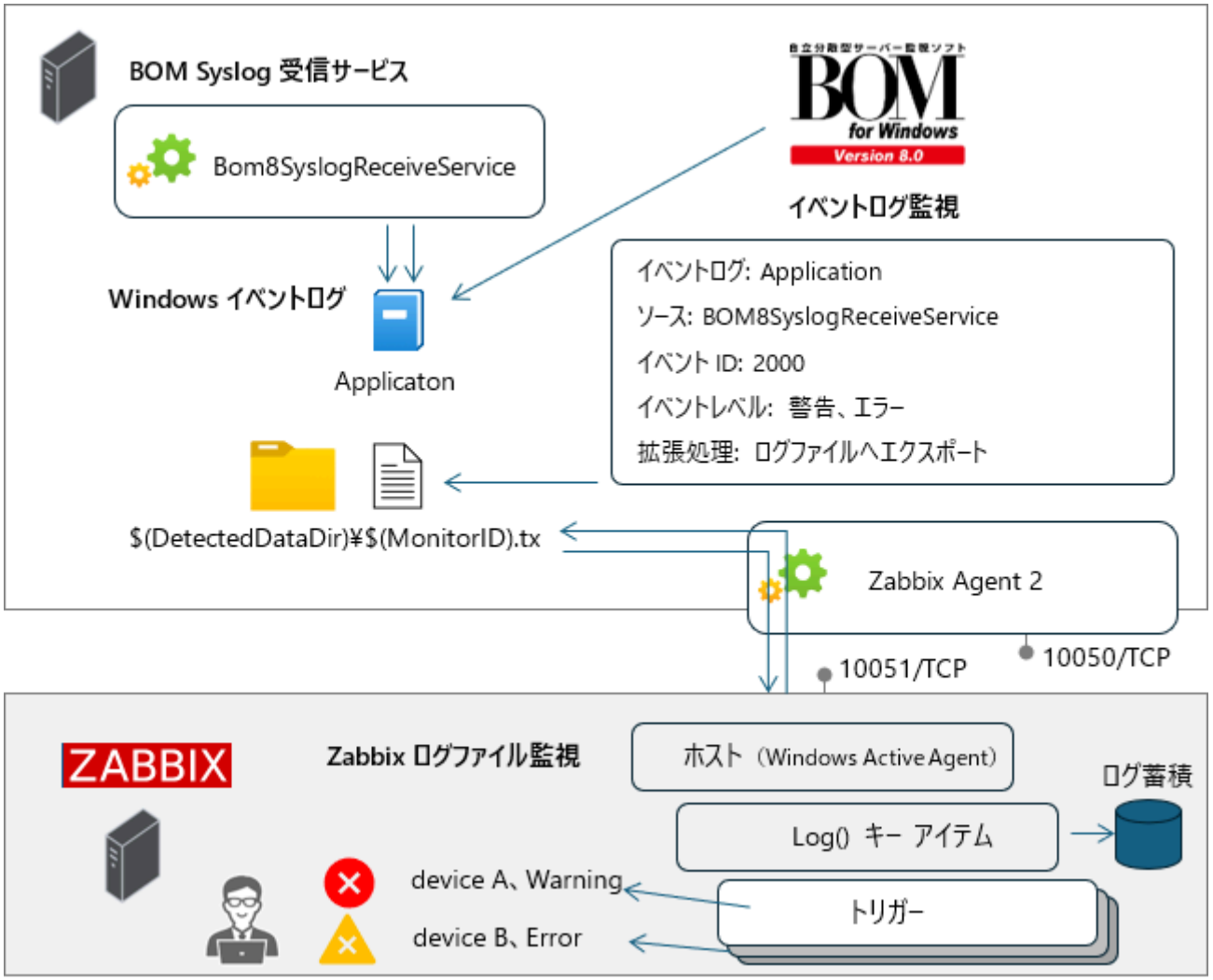


図3　Zabbixとの連携シナリオ、BOM側でフィルター後のイベントをテキストログに出力し、Windows用Zabbix Agent 2 (アクティブエージェント) 経由でZabbixサーバーからテキストログをリモート監視する。10050/TCP、10051/TCPはZabbixエージェントとZabbixサーバーの既定の受信ポート

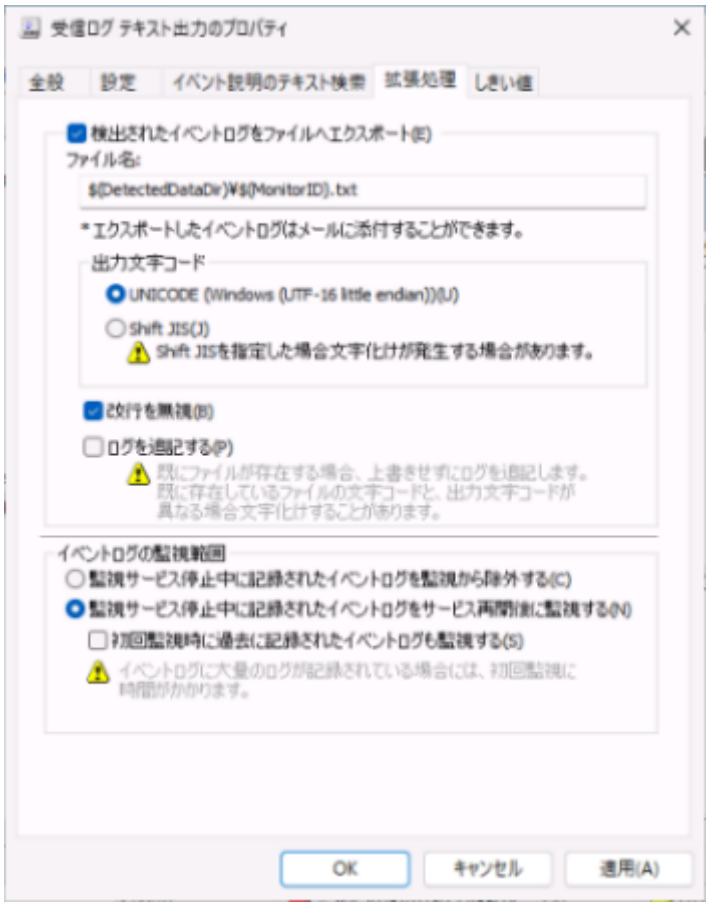
ZabbixサーバーからWindowsイベントログをリモートで監視する方法には他にも、eventlog() キーアイテムを使用する方法があります。具体的な方法については、以下のブログ記事をご参照ください。

vol.50　イベントログの監視｜BOMおじさんとZabbix (6) (かつて山市良とよばれたおじさんのブログ)
https://www.say-tech.co.jp/contents/blog/yamanxworld/2024vol050

4.2.1　BOMでフィルター後のイベントログをテキストログ化

BOMの監視項目「イベントログ監視」は、イベントログをフィルターするだけでなく、フィルター後のイベントログをテキストファイルにエクスポートすることが可能です。BOMにログエクスポート用の監視項目を作成し、監視項目のプロパティの「設定」タブで、イベントレベルとして「エラー」と「警告」を選択して、イベントログ「Application」、ソース/チャネル「BOM8SyslogReceiveService」、イベントID「2000」を監視するように設定します。

イベントログをファイルにエクスポートするには、監視項目のプロパティの「拡張処理」タブで「検出されたイベントログをファイルへエクスポート」をチェックし、出力文字コードとして「UNICODE」 (既定) または「Shift JIS」のいずれかを選択して、「改行を無視する」をチェックします。



なお、「改行を無視する」をチェックすることで、Zabbixサーバーからのログ監視に対応することができます。既定の文字コードでエクスポートした場合、Zabbixサーバー側のlog() キーアイテムでエンコード指定が必要になります。「Shift JIS」を選択した場合は、Zabbixサーバー側でのエンコード指定は不要です。

BOMの監視を開始し、BOM Syslog受信サービスがSyslogメッセージを受信すると、既定で以下の場所にイベントログがテキストファイル (UTF-16LEまたはShift JIS、エクスポート時の指定による) として出力されます。

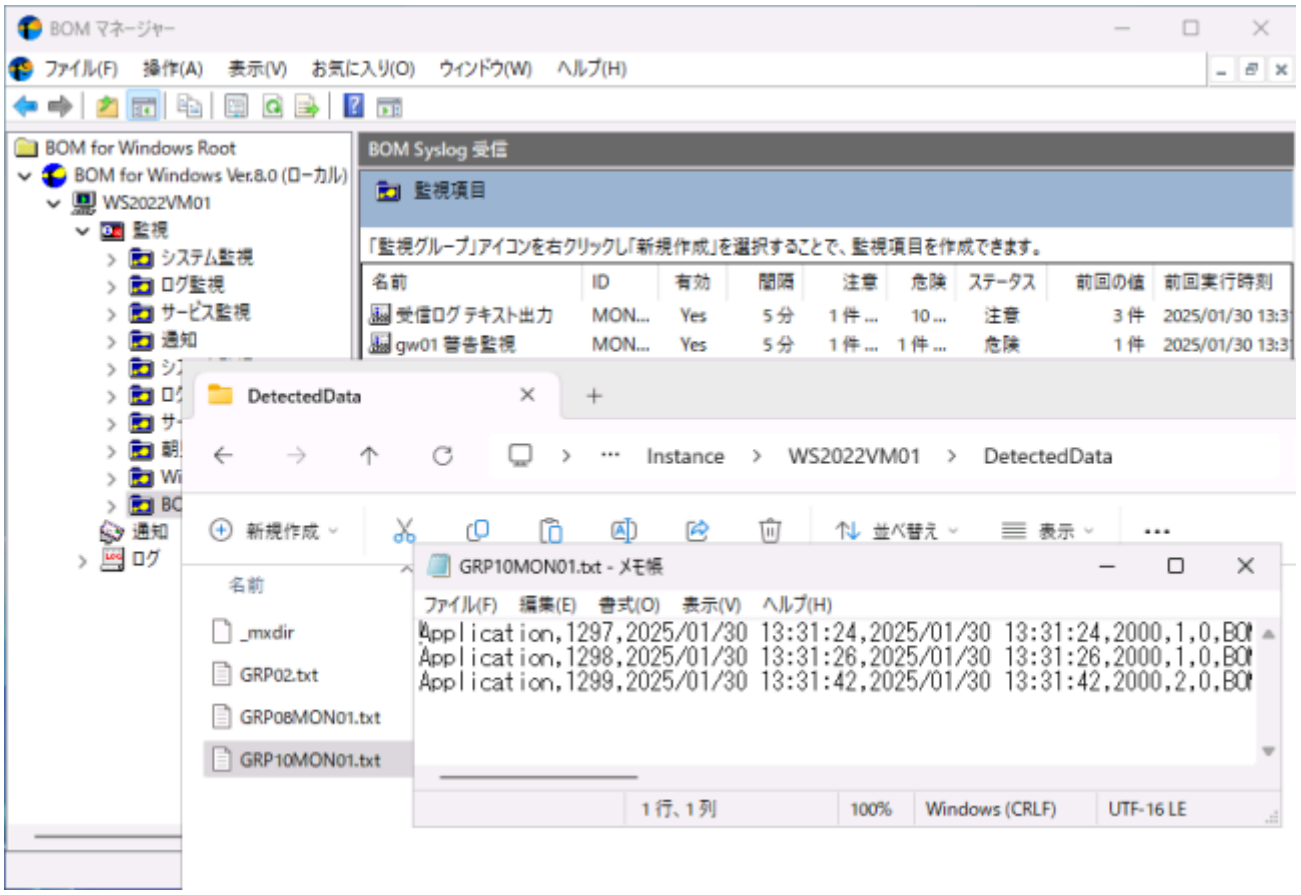
出力先	ファイル名
%ProgramData%¥SAY Technologies¥BOMW8¥Environment¥Instance<インスタンス名>¥DetectedData	GPRxxMONyy.txt

(※GPRxxは監視グループID、MONyyは監視項目ID、監視グループと監視項目のプロパティの「全般」タブで確認可能)

テキスト化されたログの形式は、以下に示した通りです。1行に1つのイベント (Syslogメッセージ) が書き込まれます。

Application,<イベントレコードID>,<ログの日付と時刻>,<ログの日付と時刻>,<イベントID>,<イベントレベル (1: エラー、2: 警告、3: 情報) >,0,BOM8SyslogReceiveService,<コンピューター名>,<イベント説明 (Syslogメッセージ) >,<BOMの監視インスタンス>,<監視グループID (GPRxx) >,<監視設定ID (MONyy) >

(※<数値>は無視してください)



4.2.2 Zabbixにアイテムを作成

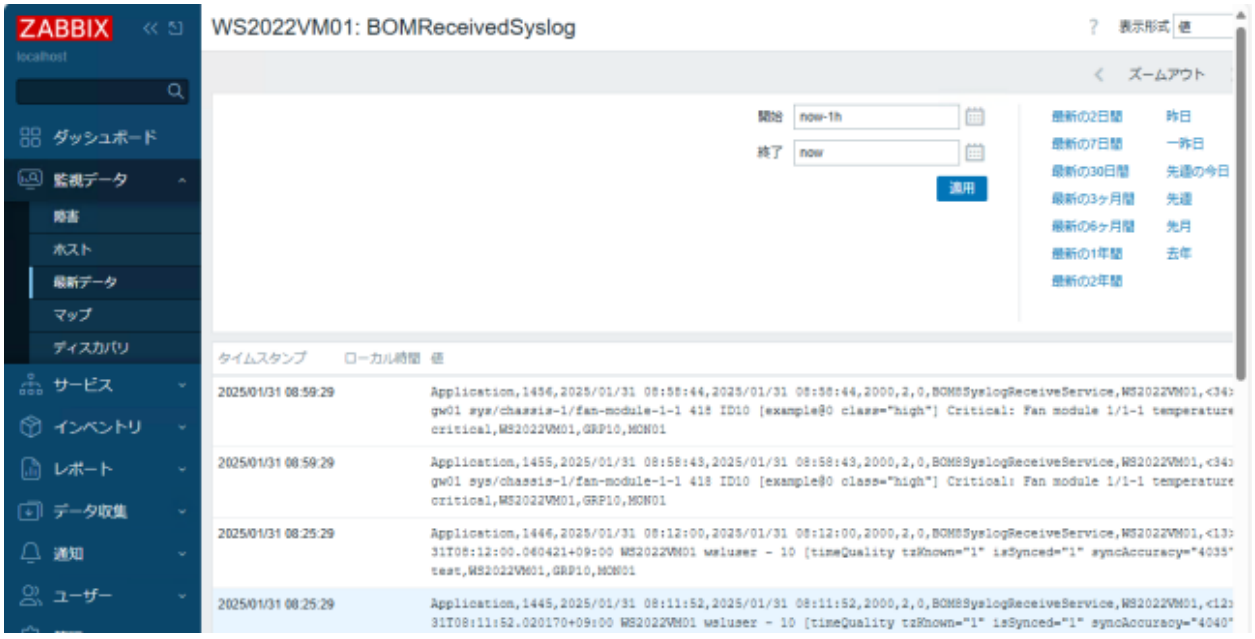
Zabbixサーバーには、BOMが稼働するWindowsコンピューターが、Zabbix Agent 2 (アクティブエージェント) で監視されるホストとして登録済みになっているものとします。Zabbixサーバーへの監視対象のホストの追加方法については省略します。Zabbixのドキュメントをご参照ください。

1. ZabbixのWebインターフェイスで「データ収集 > ホスト」(Zabbix 6.0以前は「設定 > ホスト」) を開き、BOMが稼働するWindowsコンピューターの「アイテム」リンクをクリックして開きます。
2. ページ右上にある「アイテムの作成」ボタンをクリックし、次のように設定して、「追加」ボタンをクリックします。これで、BOMが稼働するWindowsコンピューターの指定したログを1分間隔でリモート監視するようになります。

項目	設定
名前	アイテム名 (例: BOMReceivedSyslog)
タイプ	Zabbixエージェント (アクティブ)
キー	log["C:¥ProgramData¥SAY Technologies¥BOMW8¥Environment¥Instance¥BOMインスタンス名¥DetectedData¥GRPxxMONyy.txt",,"UTF-16LE"] (※BOMでイベントログをShift JIS形式でエクスポートした場合は「,,"UTF-16LE"」の指定は不要)
データ型	ログ
監視間隔	1m

項目	設定
その他の項目	既定値

3. 「監視データ > 最新データ」を開き、作成したアイテムを検索して、ログを収集できていることを確認します。



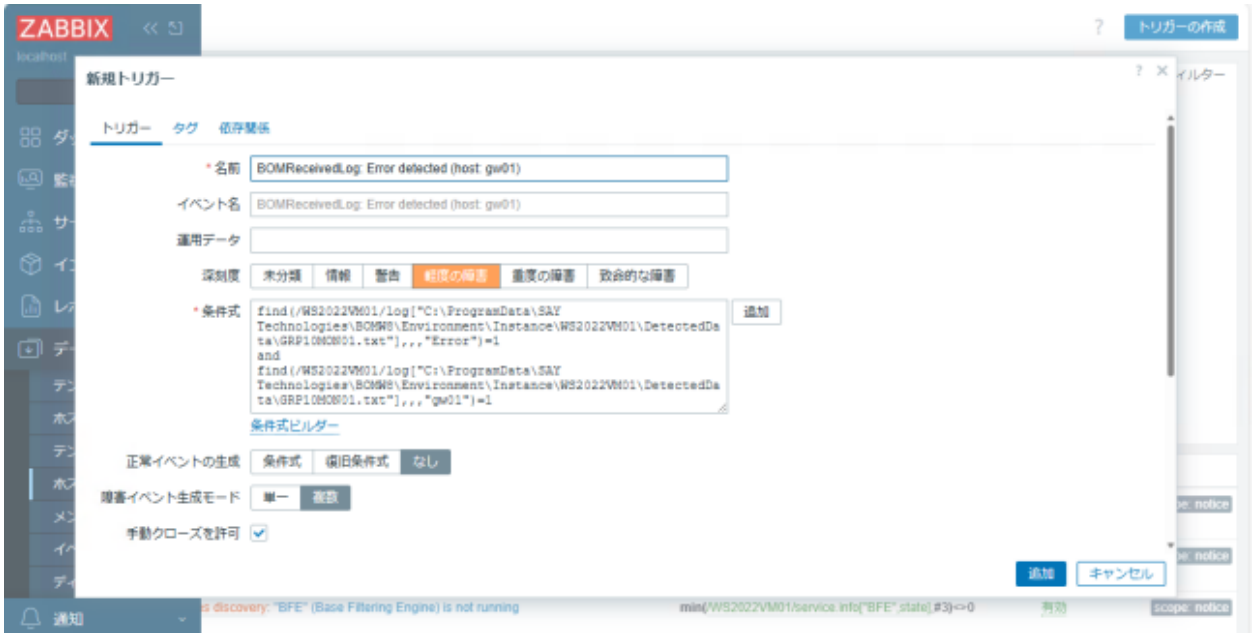
4.2.3　Zabbixにトリガーを作成

ここまでの設定で、BOM Syslog受信機能によってBOMのWindowsコンピューターに収集されたSyslogメッセージは、監視項目「イベントログ監視」でフィルターされ、テキストログにエクスポートされた後、テキスト形式のログとしてZabbixサーバーから監視できるようになりました。

Zabbixサーバーが取得するのは、BOM側で深刻度の高いものだけにフィルターされたものですが (この例の場合、「エラー」または「警告」イベント) 、それを障害として検知し、さらに次のアクションに進めるためには、トリガーを作成する必要があります。この連携シナリオの場合、Windowsコンピューター上のテキストログを監視することになるため、トリガーによる状態の変化はWindowsコンピューターの障害として検出されることに留意してください。トリガーでは、Syslogメッセージをテキスト検索するなどして、真の障害ホストがわかるように通知する必要があります。

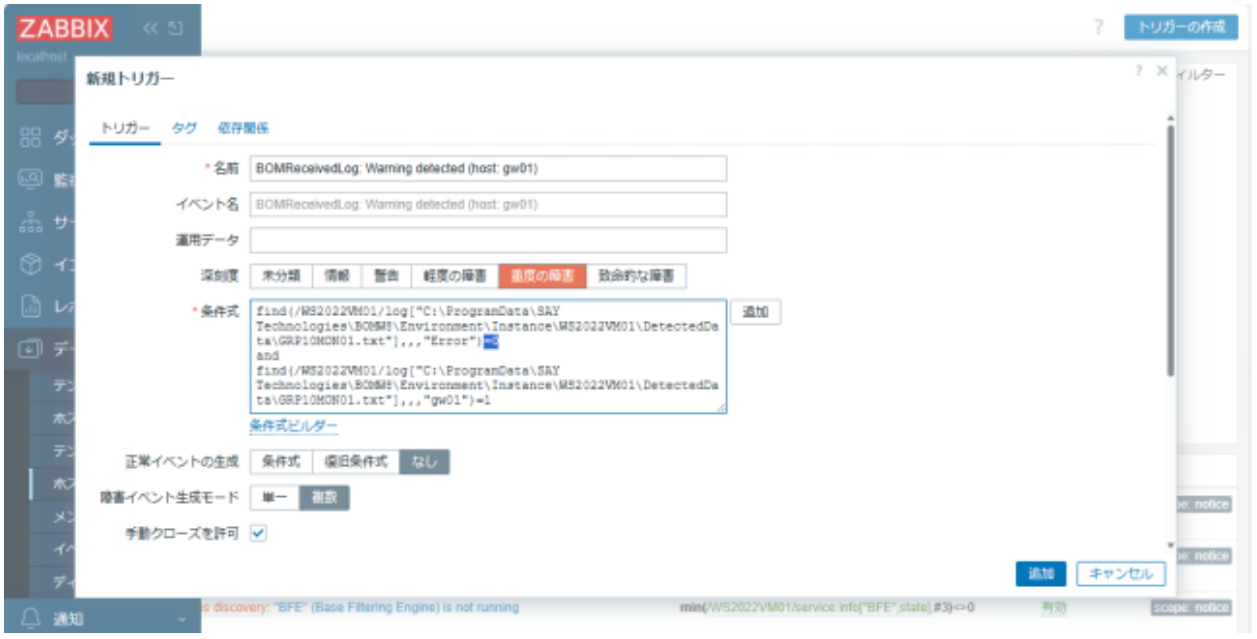
1. ZabbixのWebインターフェイスで「データ収集 > ホスト」(Zabbix 6.0以前は「設定 > ホスト」) を開き、BOMが稼働するWindowsコンピューターの「トリガー」リンクをクリックして開きます。
2. ページ右上にある「トリガーの作成」ボタンをクリックし、例えば、特定のホストのエラー (Syslogメッセージに“Error" を含む) イベントをトリガーとするには、次のように設定して「追加」ボタンをクリックします。

名前	トリガー名 (例: BOMReceivedLog: Error detected (host: <ホスト名>)
深刻度	軽度の障害
条件式	find(/<Windowsホスト>/<log() キーアイテム>,,,"Error")=1 and find(/<Windowsホスト>/<log() キーアイテム>,,,"<ホスト名>")=1
正常性イベントの生成	なし
障害イベント生成モード	単一または複数
手動クローズを許可	✓

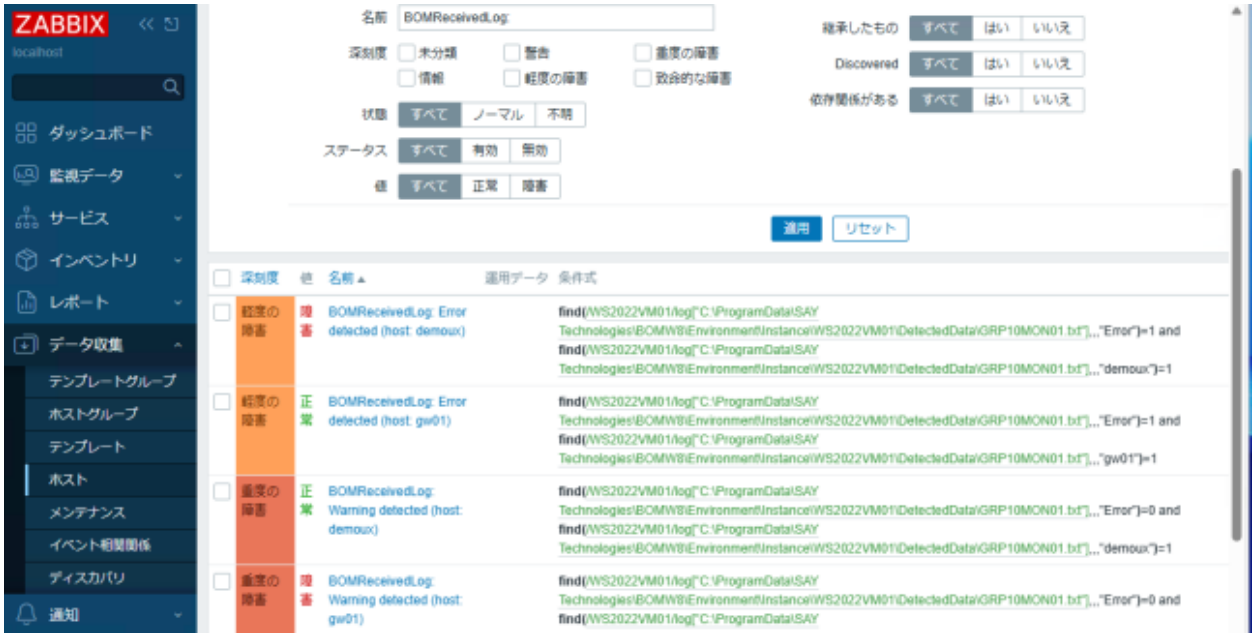


3. BOMによりエクスポートされたテキストログは「エラー」または「警告」イベントのみにフィルターされています。そのため、エラー以外 (“Notice" や "Warning" や "Critical") のログはすべて警告イベントとして扱うことができます。そのため、特定のホストのエラー以外のログは、次のトリガーで検知できます。

名前	トリガー名 (例: BOMReceivedLog: Warning detected (host: <ホスト名>)
深刻度	重度の障害
条件式	find(/<Windowsホスト>/<log() キーアイテム>,,,"Error")=0 and find(/<Windowsホスト>/<log() キーアイテム>,,,"<ホスト名>")=1
正常性イベントの生成	なし
障害イベント生成モード	単一または複数
手動クローズを許可	✓



4. 同じように、BOM Syslog受信サービスが受信するホストごとのトリガーを作成します。このトリガーの作成例は、簡単な例です。Syslogメッセージを詳細に解析して、より粒度の高い障害検知を行わせることも可能です。



以上の設定により、BOMの監視項目「イベントログ監視」が新たなログをエクスポートすると、1分以内にZabbix Webインターフェイスの「ダッシュボード」や「監視データ > 障害」に通知されるようになります。

4.3　Zabbix連携: Zabbix_senderを使用したZabbixサーバーへのログ転送

ZabbixとBOM Syslog受信機能の連携シナリオのもう1つは、BOM Syslog受信サービスが受信し、イベントログに書き込んだものを、BOMの監視項目「イベントログ監視」で監視して、そのアクション項目として検知した障害をZabbixサーバーにプッシュ送信する方法です (図4) 。Zabbix AgentおよびZabbix Agent 2には、zabbix_sender (Windows用はzabbix_sender.exe) が付属します。zabbix_senderを使用すると、Zabbixサーバーに作成したホストのZabbixトラッパーキーアイテムに対して指定して、数値や文字列の値を送信 (プッシュ) することができます。

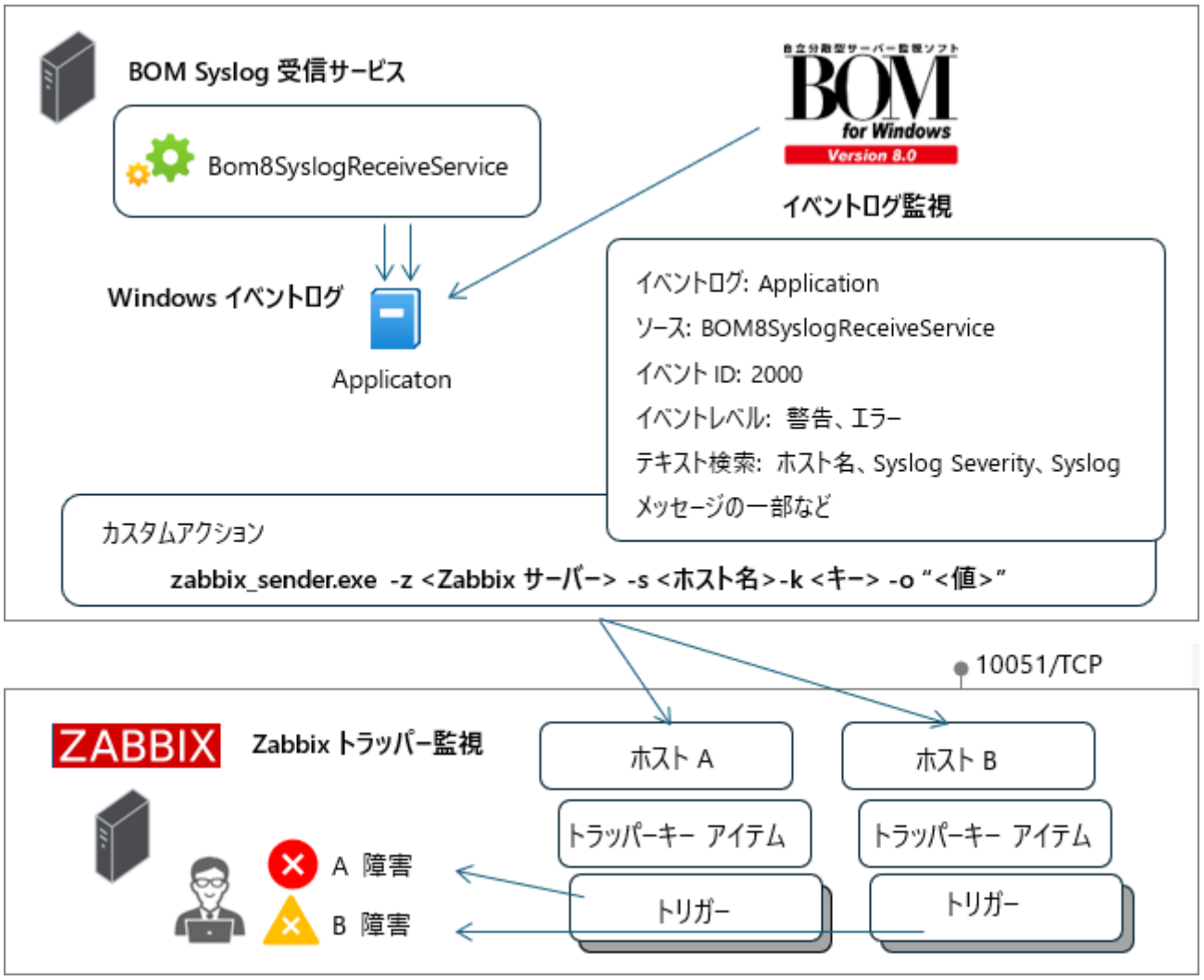


図4　Zabbixとの連携シナリオ、BOMのカスタムアクションでzabbix_senderを実行し、イベント発生をZabbixサーバーに転送する。10051/TCPはZabbixサーバーの既定の受信ポート

4.2のZabbix連携活用シナリオは、Syslog送信元のデバイスの状況を、BOM監視インスタンスを実行するWindowsコンピューターの状態 (障害) として検知します。これに対して、zabbix_senderを使用した連携方法は、エージェントレスでZabbixサーバーに登録したホストの状態 (障害) として検知できるという利点があります。

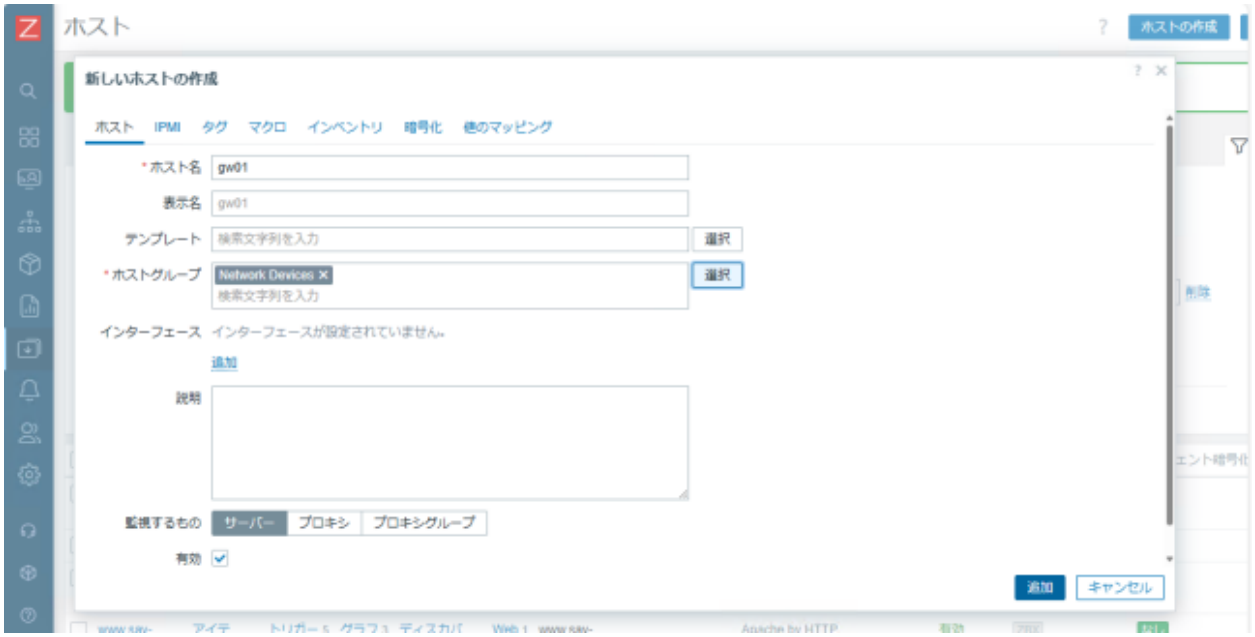
4.3.1　Zabbixに監視対象のホストを作成

まず、zabbix_senderからの値を受け取る監視対象のホストを、Syslogクライアントのデバイスごとに作成します。

1. ZabbixのWebインターフェイスで「データ収集 > ホスト」(Zabbix 6.0以前は「設定 > ホスト」) を開き、BOMが稼働するWindowsコンピューターの「アイテム」リンクをクリックして開きます。
2. ページ右上にある「ホストの作成」ボタンをクリックし、次のように設定して「追加」ボタンをクリックします。なお、このホストはエージェントやその他の方法でZabbixサーバーら監視できる必要はありませんし、(ICMPなどで) 直接的に通信できる必要もありません。

ホスト名	Syslogクライアントのホスト名
テンプレート	(なし)
ホストグループ	任意のホストグループ
監視するもの	サーバー

ホスト名	Syslogクライアントのホスト名
有効	✓



ホストグループの選択は、既定のホストグループから1つを使用することもできますが、「データ収集 > ホストグループ」で新たに作成することもできます。

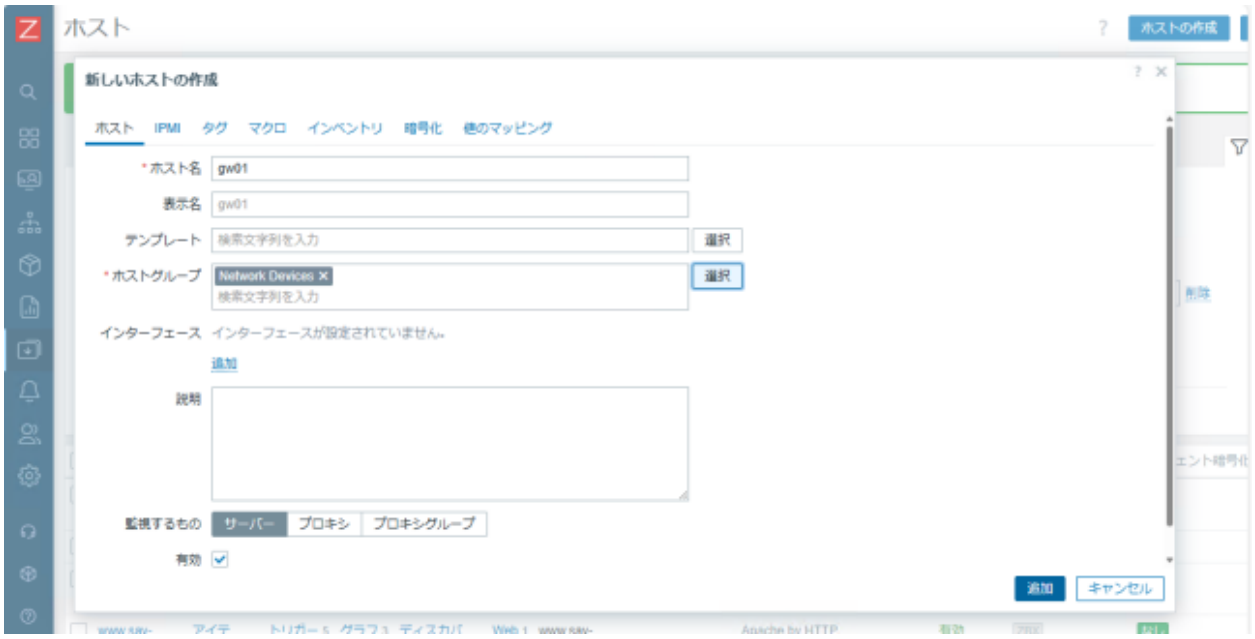
3. 同様に、BOM Syslog監視サービスが受信するSyslogクライアントのすべてに対応するホストを作成します。

4.3.2 ZabbixにZabbixトラッパーとキーの作成

zabbix_senderからの値を受け取るためには、ホストに「Zabbixトラッパー」キーアイテムを作成する必要があります。

1. ZabbixのWebインターフェイスで「データ収集 > ホスト」(Zabbix 6.0以前は「設定 > ホスト」) を開き、対象のホストの「アイテム」リンクをクリックします。
2. ページ右上にある「アイテムの作成」ボタンをクリックし、次のように設定して「追加」ボタンをクリックします。

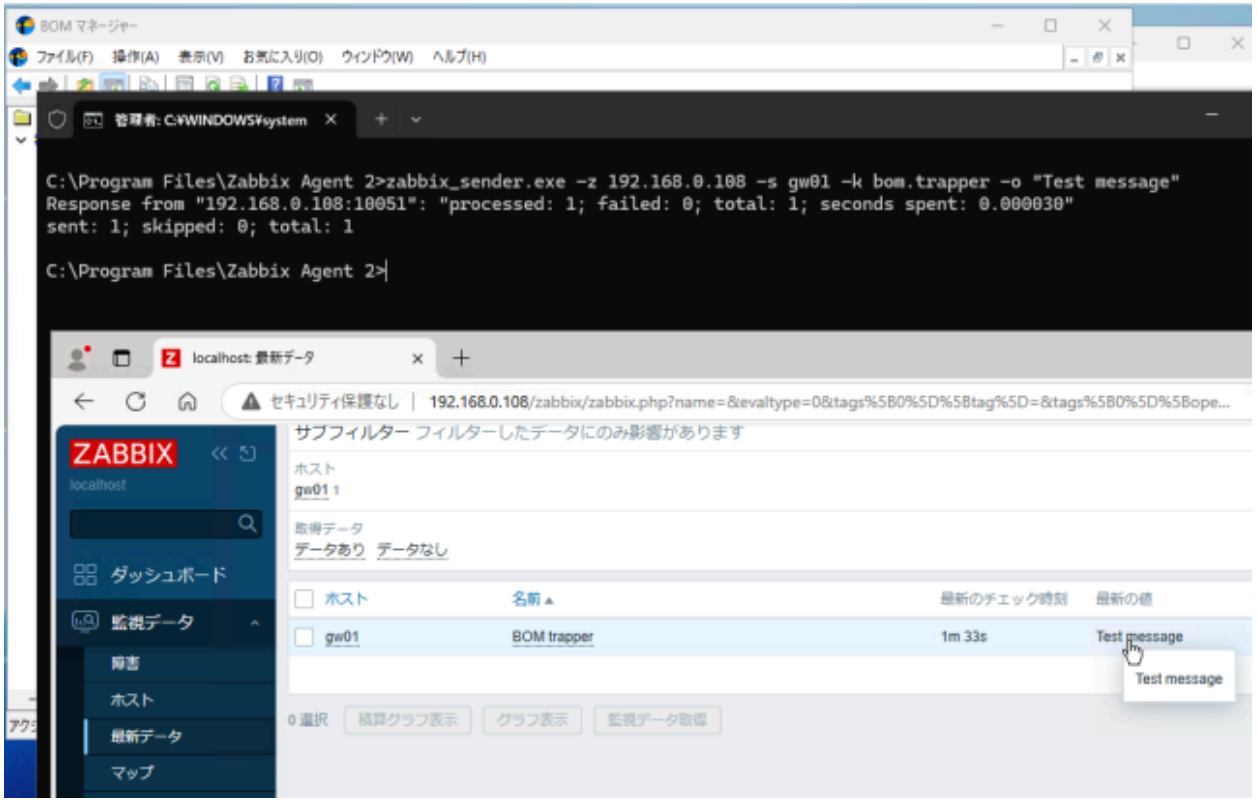
名前	アイテム名 (例: BOM Trapper)
タイプ	Zabbixトラッパー
キー	キー名 (例: bom.trapper)
データ型	文字列
ヒストリ	保存期間 31d (既定値)
許可されたホスト	BOM Syslog受信サービスのIPアドレス



3. Syslogクライアントのホストごとに、同じアイテム名、キー名で同様の設定を行います。
4. Zabbix AgentまたはZabbix Agent 2がインストールされた、BOMが稼働するWindowsコンピューターでコマンドプロンプト (cmd.exe) を開き、「C:¥Program Files¥Zabbix Agent」または「C:¥Program Files¥Zabbix Agent 2」に移動して、次のコマンドラインを実行し、プッシュ送信をテストします。実行時に、さらに-vvオプションを指定すれば、診断に役立つ詳細な情報を出力させることができます。

```
zabbix_sender.exe -z <ZabbixサーバーのIPアドレス> -s <Zabbixに作成したホスト名> -k <トラッパーキー (例: bom.trapper)> -o "Test Message"
```

5. Zabbix Webインターフェイスの「監視データ > 最新データ」を開き、zabbix_senderのホストのZabbixトラッパーキーアイテムに値が表示されることを確認します。



参考:

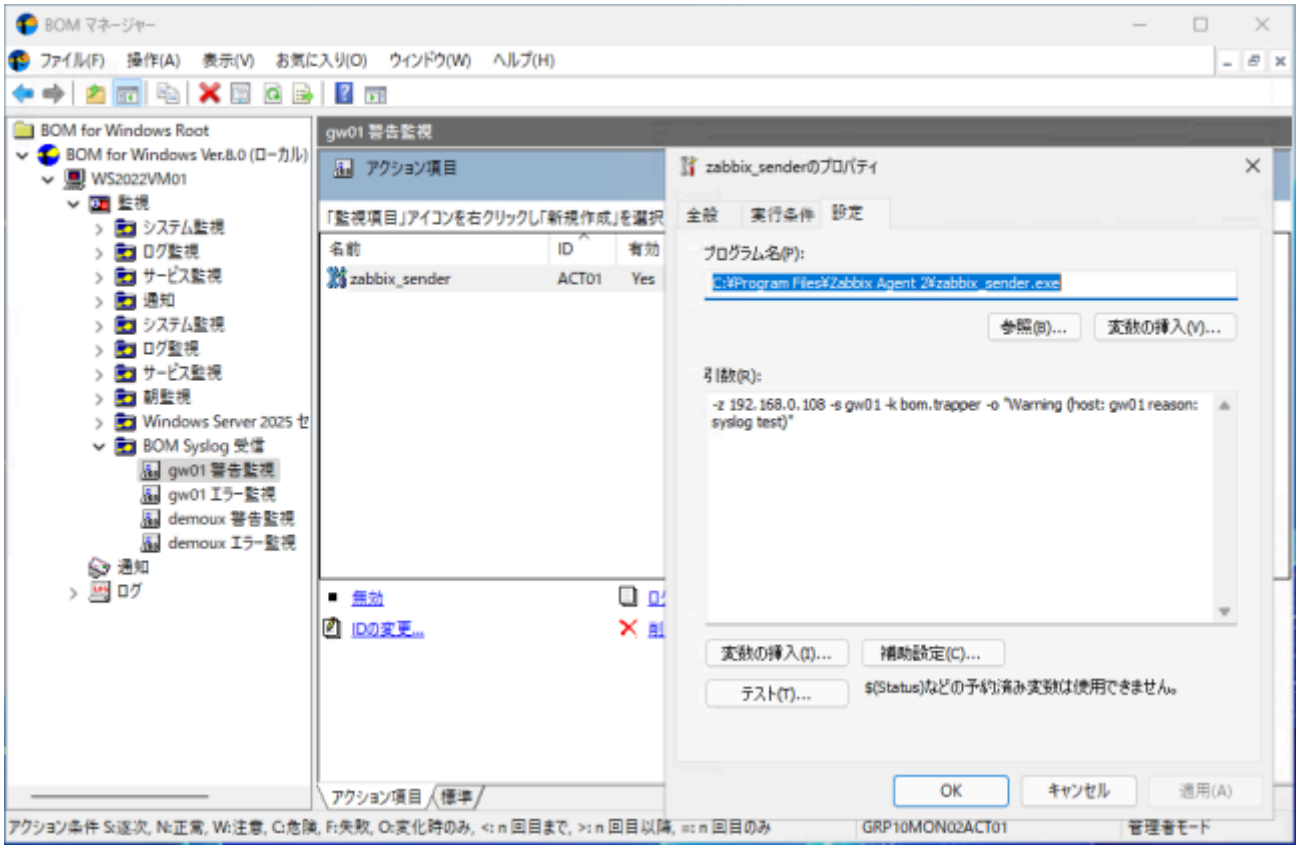
zabbix_sender | ZABBIX Documentation (zabbix.com)

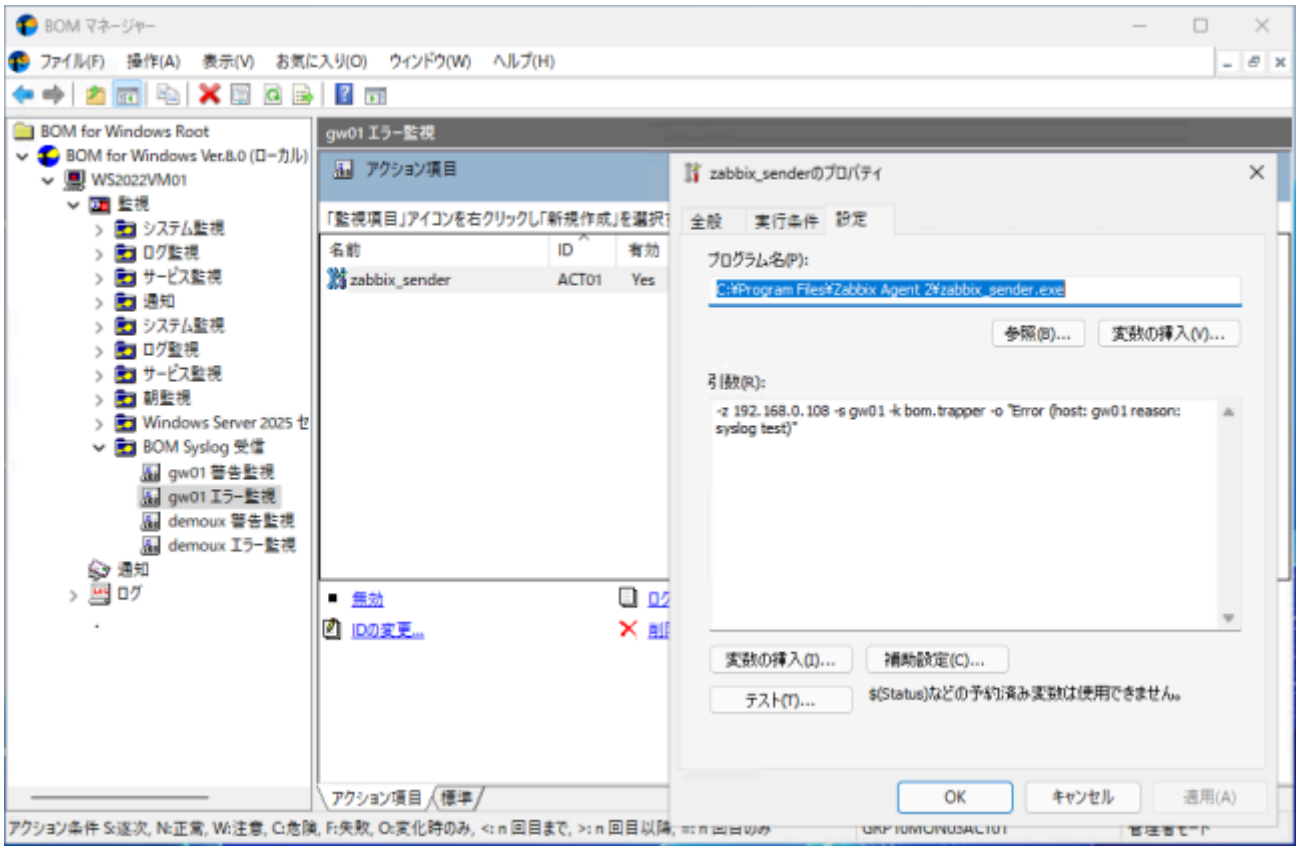
https://www.zabbix.com/documentation/7.0/en/manpages/zabbix_sender

4.3.3　BOMのカスタムアクションとzabbix_senderでログを転送

zabbix_senderによるZabbixサーバーへのプッシュ送信が確認できたら、BOMのカスタムアクションを使用してzabbix_senderを実行させるように設定します。この例では、4.1で作成した監視項目「イベントログ監視」に、カスタムアクションを作成します。BOMの監視設定では、ホストごと、イベントレベルごとに監視項目を作成しました。各監視項目に「zabbix_sender」という名前のカスタムアクションを作成して、次のコマンドラインを自動実行するように、プログラム名と引数を設定します。

```
zabbix_sender.exe -z <ZabbixサーバーのIPアドレス> -s <Zabbixに作成したホスト名> -k <トラッパーキー (例: bom.trapper)> -o "送信文字列 (例: Warning (host: gw01 reason: ...) "
```



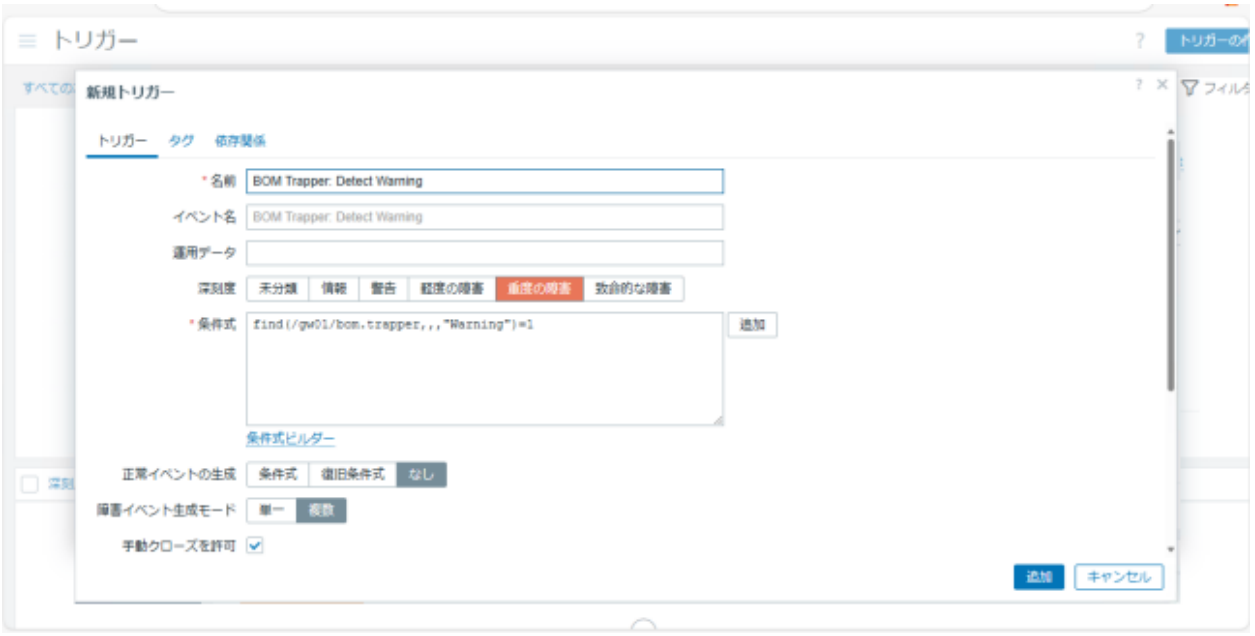


4.3.4　Zabbixにトリガーを作成

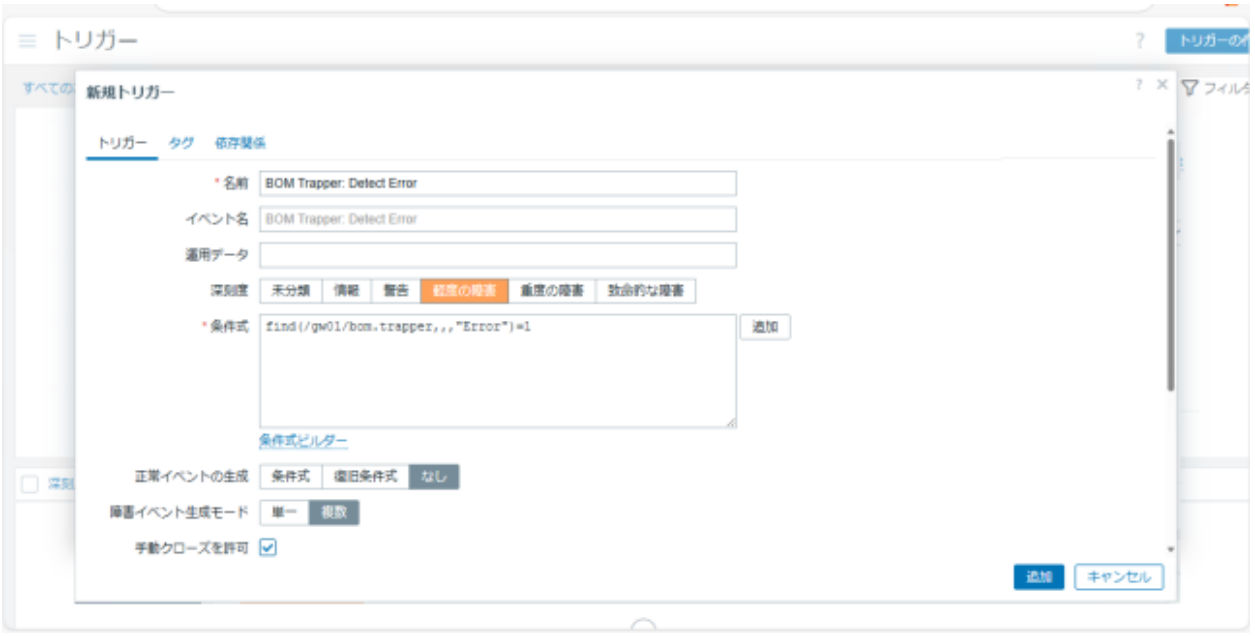
ホストのZabbixトラッパーキーアイテムが受信した値に基づいて障害を通知するように、トリガーを作成します。

1. ZabbixのWebインターフェイスで「データ収集 > ホスト」(Zabbix 6.0以前は「設定 > ホスト」) を開き、Syslogクライアントに対応するホストの「トリガー」リンクをクリックして開きます。
2. ページ右上にある「トリガーの作成」ボタンをクリックし、find() 関数などを使用してzabbix_senderで送信された文字列を検索し、障害の深刻度を設定して、「追加」ボタンをクリックします。この例に含まれる "Warning” や "Notice" は、Syslogメッセージに含まれる文字列ではなく、zabbix_senderにより送信された値であることに留意してください。

名前	(例: BOM Trapper: Detect Warning)
深刻度	重度の障害
条件式	find(/<ホスト>/<トラッパーキーアイテム>,,,"Warning")=1
正常性イベントの生成	なし
障害イベント生成モード	単一または複数
手動クローズを許可	✓



名前	(例: BOM Trapper: Detect Warning)
深刻度	軽度の障害
条件式	find(/<ホスト>/<トラッパーキーアイテム>,,,"Error")=1
正常性イベントの生成	なし
障害イベント生成モード	単一または複数
手動クローズを許可	✓



3. 監視対象のホストごとに、同じようにトリガー (同じトリガー名を使用できます) 。

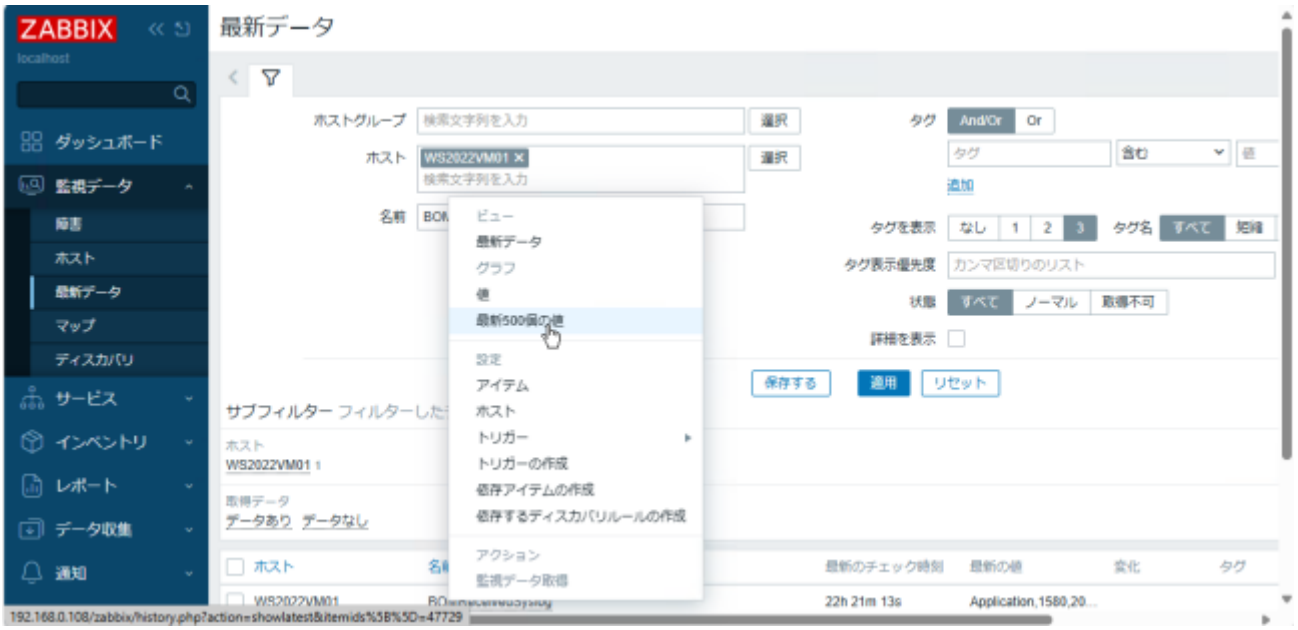
以上の設定により、BOMの監視項目「イベントログ監視」で検知した障害が、Zabbixサーバーにzabbix_senderを使用してプッシュ送信され、Syslogメッセージを最初に送信したホストの障害として検知できるようになりました。

4.4　Zabbixアクティブエージェントによるログ収集とzabbix_senderによるプッシュ送信の併用

4.2のZabbix連携活用シナリオは、BOMが収集したSyslogメッセージをテキストログとして監視し、Zabbix側のトリガーを使用してログの内容に基づいて障害の発生を検知するものです。前述したように、監視対象のテキストログはZabbixアクティブエージェントを実行するWindowsコンピューター上にあるため、Windowsコンピューターの障害として通知されるという留意点があります。また、障害の発生や深刻度の判断は、Zabbix側のトリガーとしてすべて用意する必要があり、詳細な監視のためにはトリガーの数が増え、各トリガーのフィルター条件も複雑になります。

一方、4.3のZabbix連携活用シナリオは、障害発生をBOM側でフィルターして検知し、zabbix_senderを使用してZabbixサーバーに登録したホストの障害としてプッシュ送信するため、Syslog送信元のデバイスの障害として検知できるという利点があります。zabbix_senderでプッシュ送信する値を詳細にすればするほど、BOM側のフィルターが増え、その内容も複雑になります。しかし、BOMでは、複雑なフィルター条件でもGUIだけで設定を完結でき、高いスキルを必要としません。

そこで、4.2をログ収集の目的で使用し (トリガーによる監視を行わず)、4.3によるzabbix_senderによる状態変化のプッシュ送信を併用することをお勧めします。併用することにより、デバイスの状態変化をいち早く検知し、必要に応じて、問題のデバイスに出向くことなく、Zabbixサーバーに蓄積されたSyslogメッセージのログ (ログの保存期間はアイテムのヒストリ保存期間で調整可能) を詳細に調査することができます。オリジナルのSyslogメッセージを調査することを前提とするなら、BOM側のフィルター条件の複雑さを大きく緩和できるはずです。


ZABBIX
localhost
最新データ
ダッシュボード
監視データ
障害
ホスト
最新データ
マップ
ディスカバリ
サービス
インベントリ
レポート
データ収集
通知
ホストグループ
検索文字列を入力
選択
ホスト
WS2022VM01
検索文字列を入力
選択
名前
タグ
And/Or
Or
タグ
含む
追加
タグを表示
なし
1
2
3
タグ名
すべて
短縮
タグ表示優先度
カンマ区切りのリスト
状態
すべて
ノーマル
取得不可
詳細を表示
保存する
適用
リセット
ビュー
最新データ
グラフ
値
最新500個の値
設定
アイテム
ホスト
トリガー
トリガーの作成
依存アイテムの作成
依存するディスカバリルールの作成
アクション
監視データ取得
サブフィルター
ホスト
WS2022VM01
取得データ
データあり
データなし
ホスト
最新のチェック時刻
最新の値
変化
タグ
22h 21m 13s
Application,1580,20...
192.168.0.108/zabbix/history.php?action=showlatest&itemids%5B%5D=47729


demoux systemwalker OD_star ID1198 [example@0 class="high"] Error : od10921:ObjectDirector initialization time out.,WS2022VM01,GRP10,MON01
2025/01/31 12:20:29
Application,1496,2025/01/31 12:01:56,2025/01/31 12:01:56,2000,1,0,BOM8SyslogReceiveService,WS2022VM01,<34>1 2025-01-27T04:10:02.000Z demoux systemwalker OD_star ID1198 [example@0 class="high"] Error : od10921:ObjectDirector initialization time out.,WS2022VM01,GRP10,MON01
2025/01/31 12:20:29
Application,1495,2025/01/31 11:55:14,2025/01/31 11:55:14,2000,1,0,BOM8SyslogReceiveService,WS2022VM01,<34>1 2025-01-27T04:10:02.000Z demoux systemwalker OD_star ID1198 [example@0 class="high"] Error : od10921:ObjectDirector initialization time out.,WS2022VM01,GRP10,MON01
2025/01/31 12:20:29
Application,1494,2025/01/31 11:55:07,2025/01/31 11:55:07,2000,2,0,BOM8SyslogReceiveService,WS2022VM01,<34>1 2025-01-27T04:10:02.000Z gw01 org-root/ls-test 418 ID10 [example@0 class="high"] Warning: Service profile test is not associated,WS2022VM01,GRP10,MON01
2025/01/31 12:20:29
Application,1493,2025/01/31 11:55:01,2025/01/31 11:55:01,2000,2,0,BOM8SyslogReceiveService,WS2022VM01,<34>1 2025-01-27T04:10:02.000Z gw01 sys/chassis-1/fan-module-1-1 418 ID10 [example@0 class="high"] Critical: Fan module 1/1-1 temperature: lower-critical,WS2022VM01,GRP10,MON01
2025/01/31 12:20:29
Application,1492,2025/01/31 11:54:59,2025/01/31 11:54:59,2000,2,0,BOM8SyslogReceiveService,WS2022VM01,<34>1 2025-01-27T04:10:02.000Z gw01 sys/chassis-1/fan-module-1-1 418 ID10 [example@0 class="high"] Critical: Fan module 1/1-1 temperature: lower-critical,WS2022VM01,GRP10,MON01
2025/01/31 10:01:29
Application,1482,2025/01/31 10:00:33,2025/01/31 10:00:33,2000,2,0,BOM8SyslogReceiveService,WS2022VM01,<34>1 2025-01-27T04:10:02.000Z gw01 sys/chassis-1/fan-module-1-1 418 ID10 [example@0 class="high"] Critical: Fan module 1/1-1 temperature: lower-critical,WS2022VM01,GRP10,MON01
2025/01/31 10:01:29
Application,1481,2025/01/31 10:00:29,2025/01/31 10:00:29,2000,2,0,BOM8SyslogReceiveService,WS2022VM01,<34>1 2025-01-27T04:10:02.000Z gw01 sys/chassis-1/fan-module-1-1 418 ID10 [example@0 class="high"] Critical: Fan module 1/1-1 temperature: lower-critical,WS2022VM01,GRP10,MON01
2025/01/31 10:01:29
Application,1480,2025/01/31 10:00:24,2025/01/31 10:00:24,2000,2,0,BOM8SyslogReceiveService,WS2022VM01,<34>1 2025-01-27T04:10:02.000Z gw01 org-root/ls-test 418 ID10 [example@0 class="high"] Warning: Service profile test is not associated,WS2022VM01,GRP10,MON01

BOM for Windows Ver.8.0 SR2 Syslog受信機能ホワイトペーパー
2025年2月15日 初版
著者・発行者・発行
セイ・テクノロジーズ株式会社