BOM for Windows Ver.8.0, Ver.7.0
イベントログ監視での除外設定方法
ガイドライン

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

1. はじめに

1.1. 製品表記

正式名称	略称
BOM for Windows Ver.X.0	BOM X.0

※ "X"にはバージョン番号が入ります。またSRバージョンを指定する場合は、末尾に追記される場合があります。

1.2. 対象製品

本書が対象とする製品は以下のとおりです。

- BOM for Windows Ver. 7.0 SR1 以降
- BOM for Windows Ver. 8.0

1.3. 本書の目的

BOM 8.0、7.0の「イベントログ監視」において、「設定」タブの「ソース/チャネルの設定」欄にある「除外指定」のチェックは、イベントソースを対象としています。

- チェック有り：指定したイベントソースを除外対象とする
- チェック無し：指定したイベントソースを検知対象とする

BOM 6.0の「イベントログ監視（除外指定）」にあったイベントソース単位に除外指定する機能は、BOM 8.0、7.0において、この「イベントログ監視」の「除外指定」が継承しています。
またBOM 6.0では「イベントログ監視（選択指定）」でのみイベントIDの指定が可能でしたが、BOM 8.0、7.0の「イベントログ監視」では、除外指定を含めてイベントIDの指定が可能になりました。

本書はまず、「イベントログ監視」で除外指定する場合によく使用される設定方法を説明し、その後に「イベントログ監視」の仕様と複雑な監視例について説明します。

「イベントログ監視」そのものの詳細な説明については、製品同梱のマニュアルを参照してください。

- BOM 7.0の場合：BOMW7.0-ユーザーズマニュアル.pdf (「5 .10 .13 イベントログ監視」)
- BOM 8.0の場合：BOM8-ユーザーズマニュアル.pdf (「第5章-11.-(14) イベントログ監視」)

2. よく使用されるイベントログ除外監視方法

2.1. あるイベントソースを監視したいが、特定のIDは除きたい

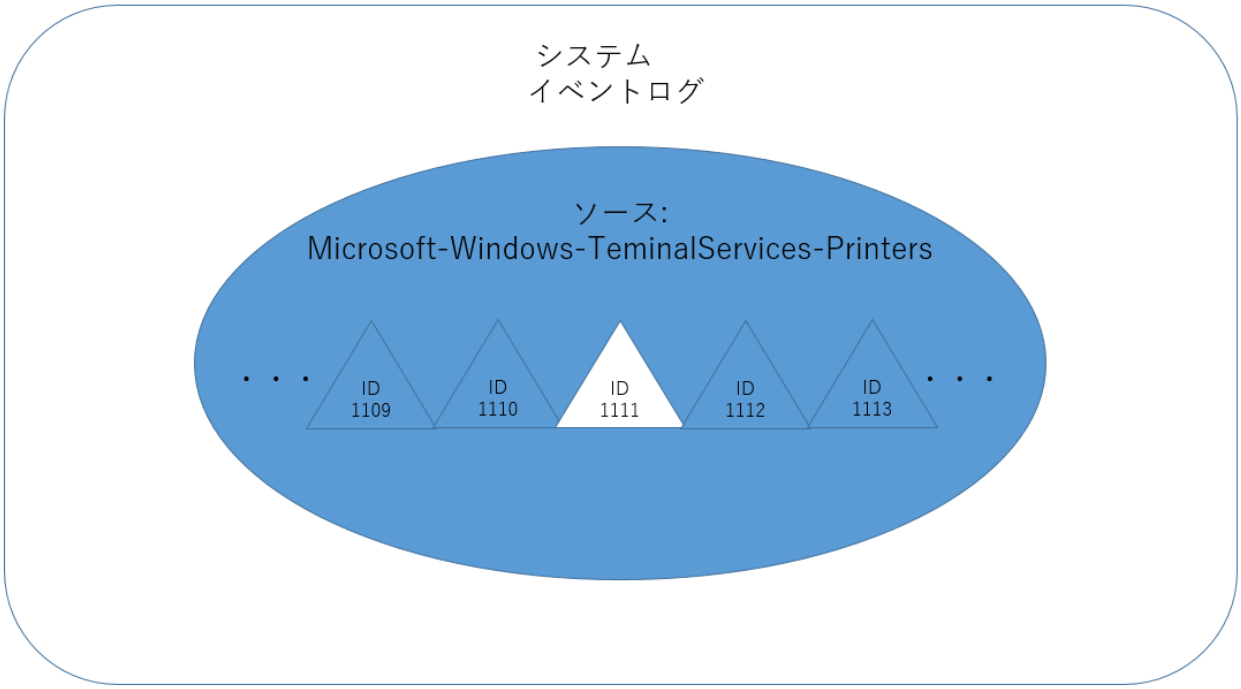
ここでは以下のような例をもとに説明します。

例：リモートデスクトップ接続時のプリンタードライバー関連のイベントログ(ID:1111)を対象から外す

2.1.1. 設定内容

- ソース/チャネルの設定:
  - 除外指定：オフ (チェックなし)
  - ソース名：Microsoft-Windows-TerminalServices-Printers
  - 除外ID: 1111 (設定では負記号付きで「-1111」と指定)

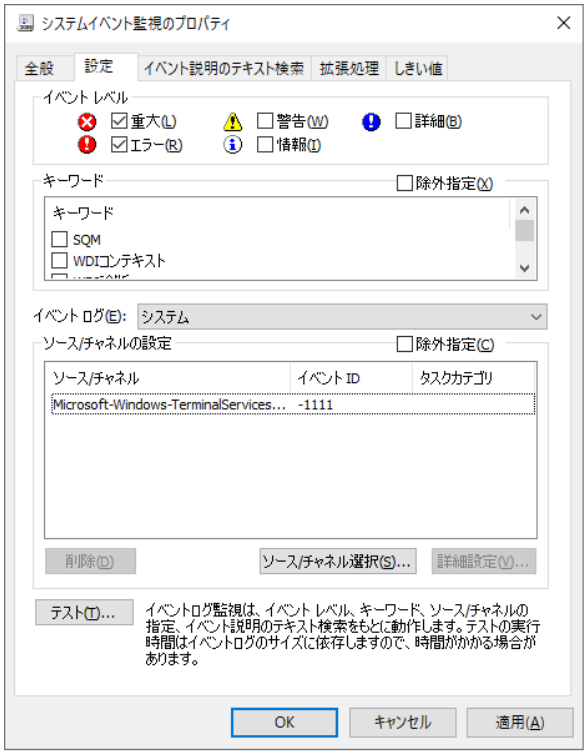
図の青い部分が対象範囲(プリンタードライバー関連の特定IDを除外)

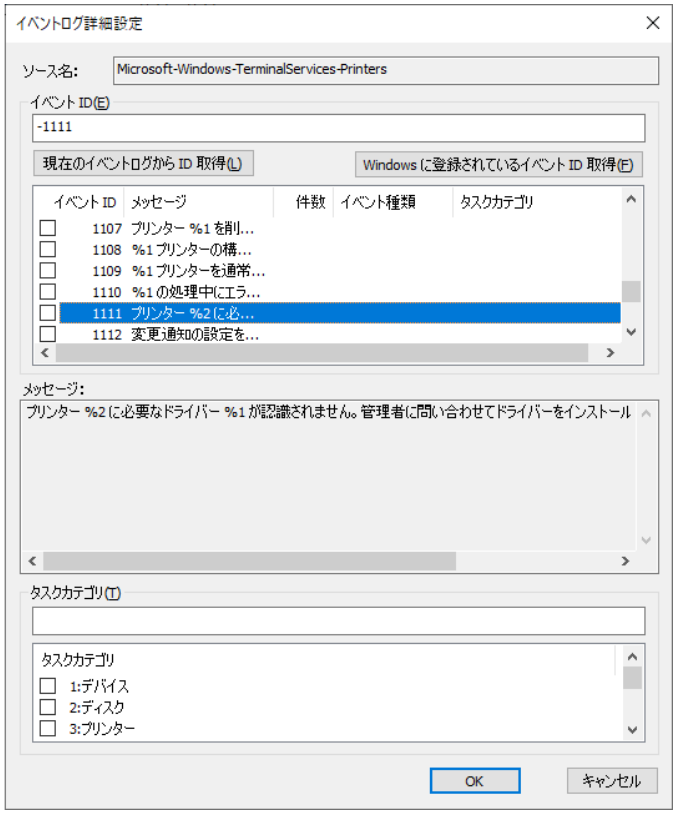


2.1.2. 設定方法

イベントログ監視のプロパティ画面で、以下のように設定します。

- 除外設定チェックは入れない。
- ソース/チャンネルは「Microsoft-Windows-TerminalServices-Printers」を指定する。
- イベントIDは [-ID] (負記号付き「-」ID)で指定する。





2.2. イベントログ全体から、あるイベントソースの特定IDだけ除外したい

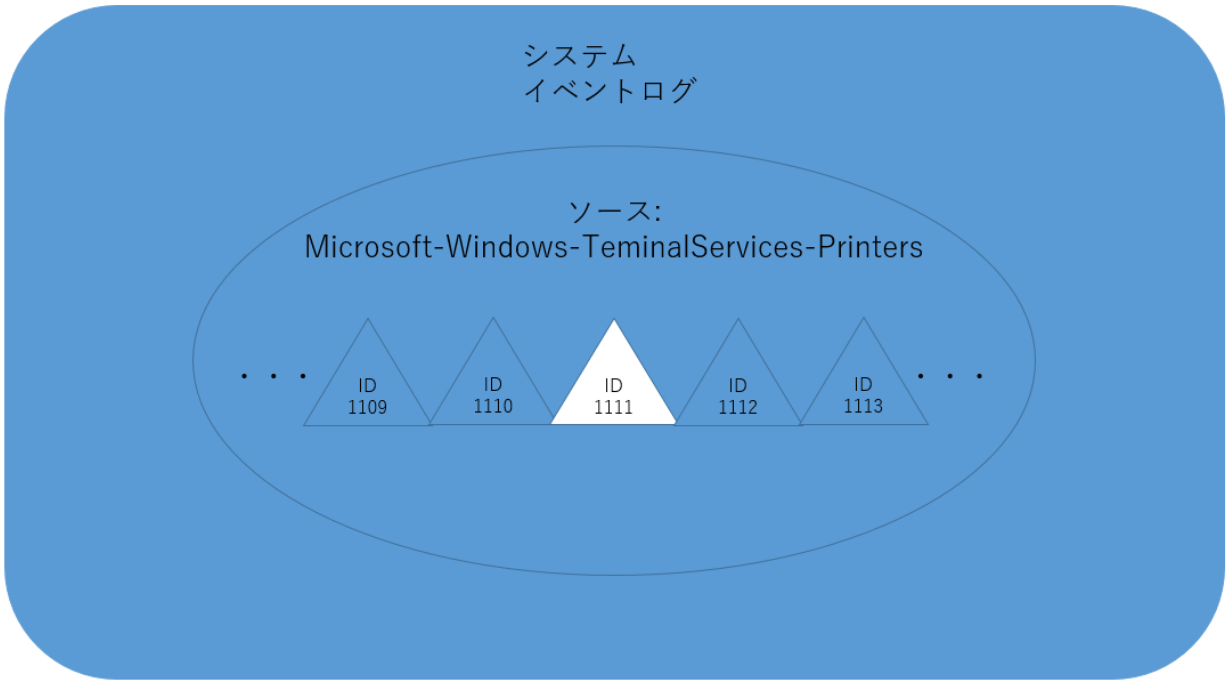
ここでは以下のような例をもとに説明します。

例：システムログ全体から「Microsoft-Windows-TerminalServices-Printers」の「ID:1111」を対象から外す

2.2.1. 設定内容

- ソース/チャネルの設定:
  - 除外指定：オン (チェックあり)
  - ソース名：Microsoft-Windows-TerminalServices-Printers
  - 除外ID: 1111 (設定では負記号付きで「-1111」と指定)

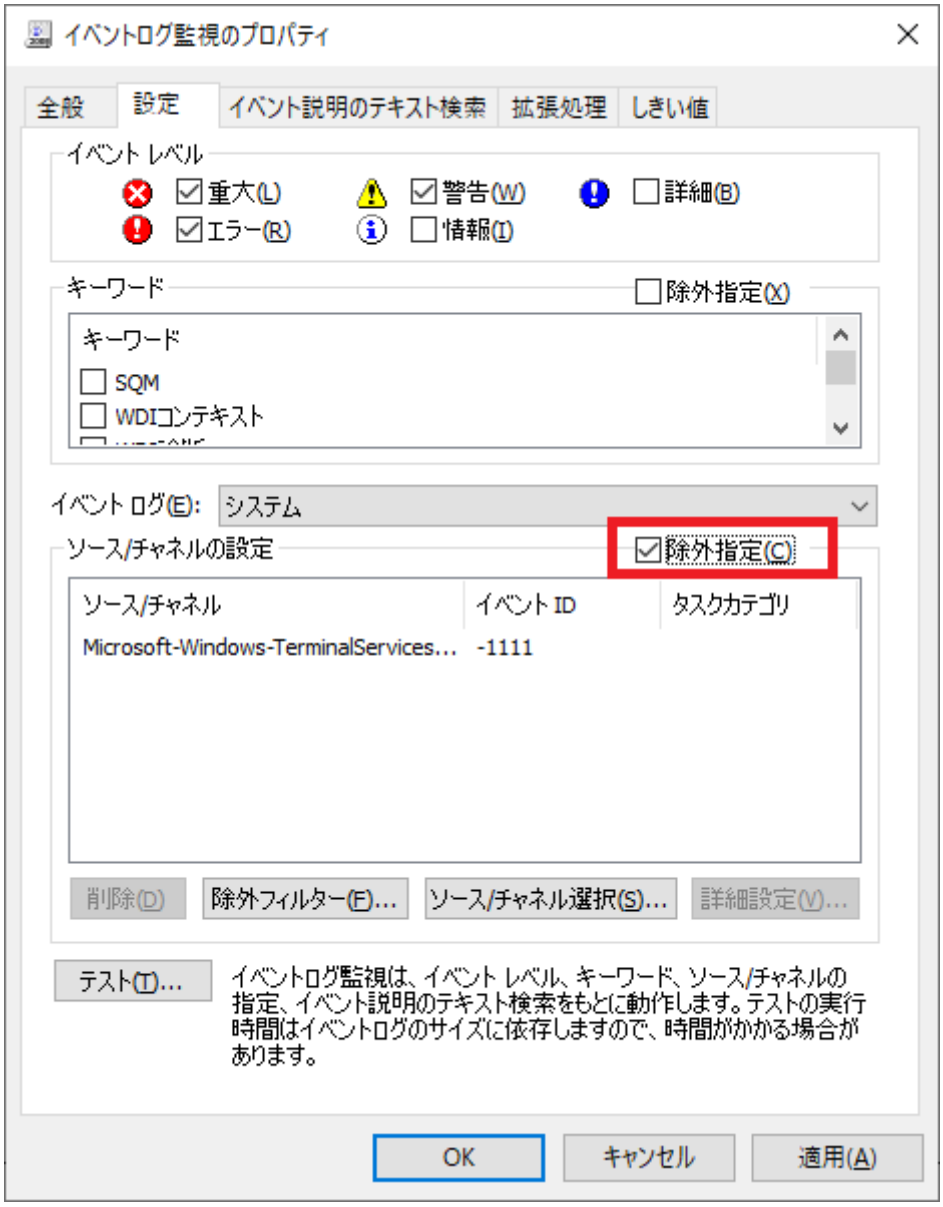
図の青い部分が対象範囲
(システムイベントログ全体からプリンタードライバー関連の特定IDを除外)



2.2.2. 設定方法

イベントログ監視のプロパティ画面で、以下のように設定します。

- 除外設定チェックを入れる。
- ソース/チャンネルは「Microsoft-Windows-TerminalServices-Printers」を指定する。
- イベントIDは [-ID] (負記号付き「-」ID)で指定する。



3. 既存のイベントログ監視に除外設定を追加する

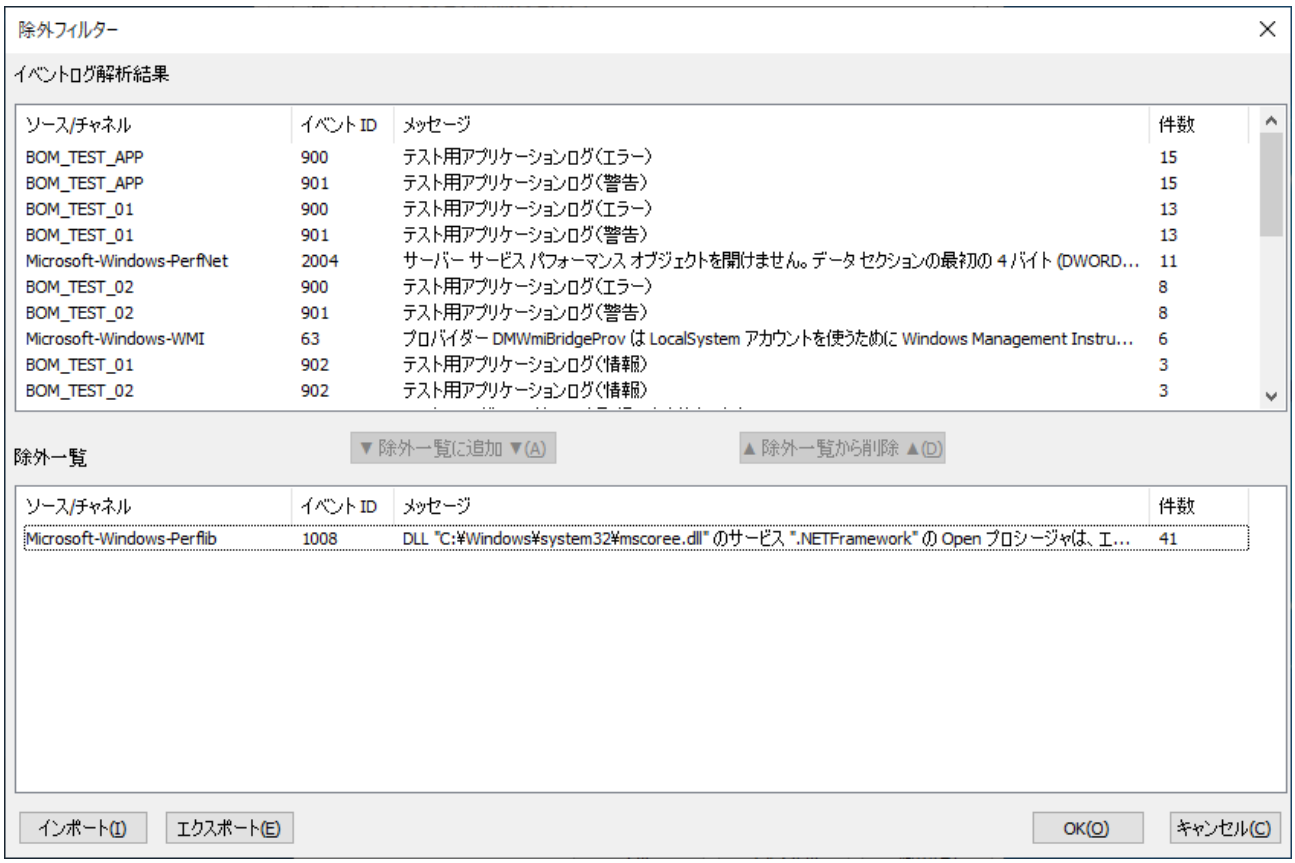
3.1. もともとソースが全く指定されていない場合

すでに監視を実施している環境で、もともとソースが全く指定されておらず不要なイベントログを検知してしまう場合など、監視が必要でないログ(特定ソースの特定ID)を除外する際の設定方法です。

例：Windows システム監視 Basic テンプレートで運用中の「アプリケーションログ監視」に、特定ソースの特定IDを除外する設定を追加する

3.1.1. 設定方法

1. 対象のイベントログ監視でプロパティを開き、「設定」タブを選択する。
2. [除外指定]チェックにチェックを入れる。
3. [除外フィルター]ボタンをクリックする。
4. [イベントログ解析結果]リストより必要でないイベントをクリックし、[除外一覧に追加]クリックする。



3.2. 既存のイベントログ監視にソースとイベントIDが指定されている場合

すでにイベントログ監視で特定のソースやイベントIDを指定して監視を運用中で、同一ソースから出る指定のイベントIDを追加で除外したい場合の除外設定方法です。

3.2.1. 設定方法

- 除外設定チェックは入れない。
- イベントIDは [-ID] (負記号付き「-」ID)で指定する。

この場合は、上記「あるイベントソースを監視したいが、特定のIDは除きたい」と同一設定です。

4. イベントログ監視の仕様について

4.1. 仕様 1

除外指定のチェックはイベントソース単位に除外するものです。

イベントソースだけが指定されている場合、そのイベントソースはイベントログ監視の監視対象から外れます。

4.2. 仕様 2

除外のチェックがあり、指定したイベントソースの中にイベントIDが含まれている場合は、そのイベントソースについては指定したイベントIDが監視対象になります。

例えば 除外指定のチェックが入っており、イベントソースAにイベントID:100が指定されていれば、そのイベントソースAについては、 イベントID:100が監視対象になります。間違えやすいため、注意が必要です。

また、イベントIDは複数指定ができます。イベントIDで100,110と複数指定があれば100と110も監視対象になります。

4.3. 仕様 3

イベントソースの中ではイベントID除外指定に 負記号「-」が使用できます。
負記号によるイベントID除外は除外指定チェックと組み合わさった場合でも、イベントソースの中では除外チェックの有無に影響されません。

例えば、除外指定チェックが入って、イベントソースAにイベントID:-200 が指定されている場合、イベントソースAについてはID:200以外が監視対象になります。

もし、これに負記号指定のないイベントIDが指定されていた場合には、負記号のないイベントIDが監視対象になります。

例えば、除外指定のチェックがあり、イベントソースAにイベントIDに100と-200が指定されていた場合、イベントソースAについてはID:100が監視対象になり、ID:100以外のIDは監視対象になりません。指定したIDのみが監視対象になります。

4.4. 仕様まとめ

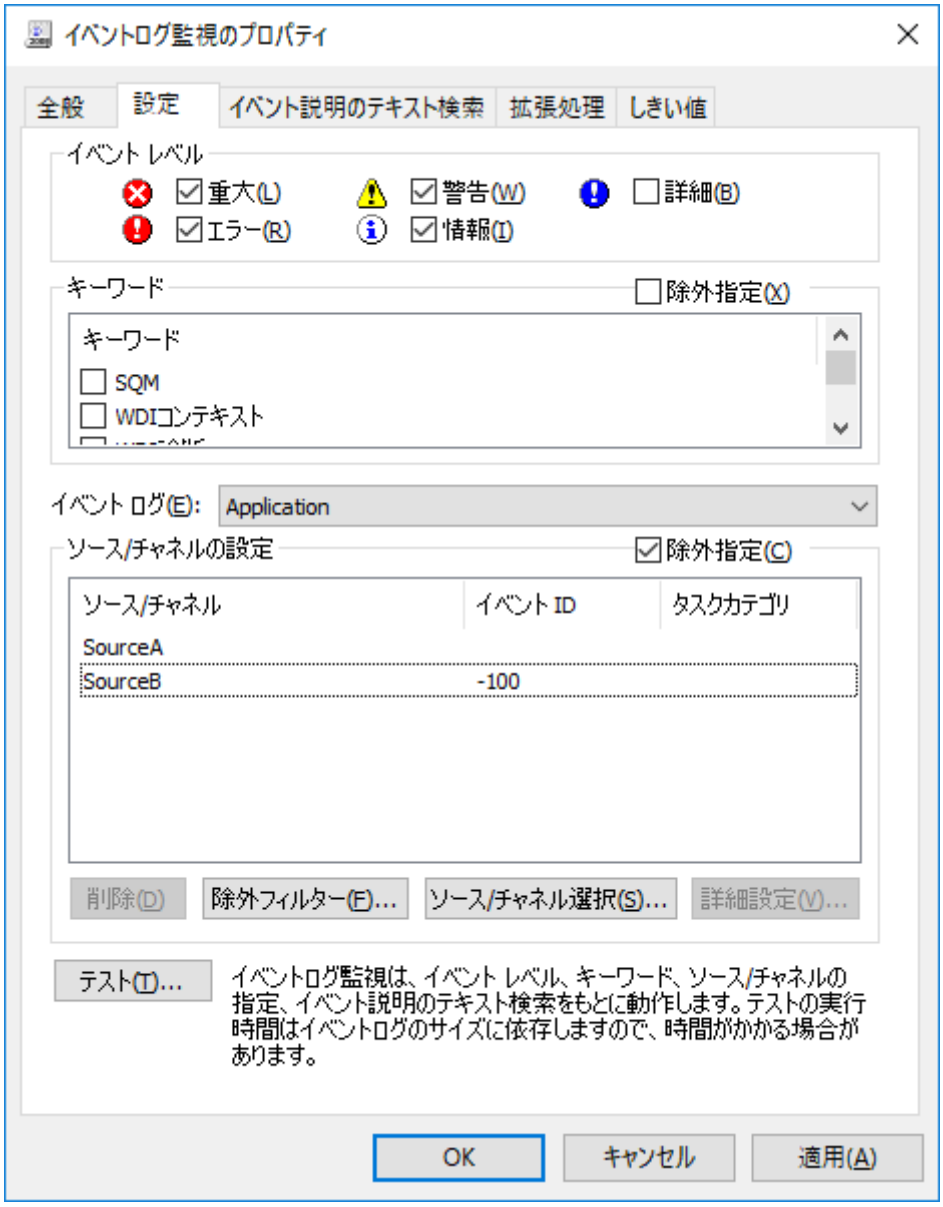
除外指定のチェックとイベントID指定とイベントIDの負記号の組み合わせをまとめると以下になります。

除外設定のチェック	イベントID指定	イベントID負記号
チェックあり	ソース：SourceA ID：100の場合 SourceA以外のソースと、SourceAのID：100以外を監視します。	ソース：SourceA ID：-100の場合 SourceAのID：100とSourceA以外のソースを監視します。
チェックなし	ソース：SourceA ID：100の場合 SourcAのID:100を監視します。	ソース：SourceA ID：-100の場合 SourceAのID：100以外を監視します。他のソースは監視しません。

5. 複雑な除外設定の例

複数のソースでの除外設定も可能です。

例えば、「特定のSourceAを除外する」の条件と「特定のSourceBの特定のイベントID100のみ除外する」の条件を組み合わせる場合は、以下の設定で対応できます。



ソース除外をするため除外指定をチェックし、各ソースの中の特定IDを除外する場合は負記号付きで指定します。

イベントログ監視での除外設定方法ガイドライン

2022年7月22日　初版

著者・発行者・発行
セイ・テクノロジーズ株式会社