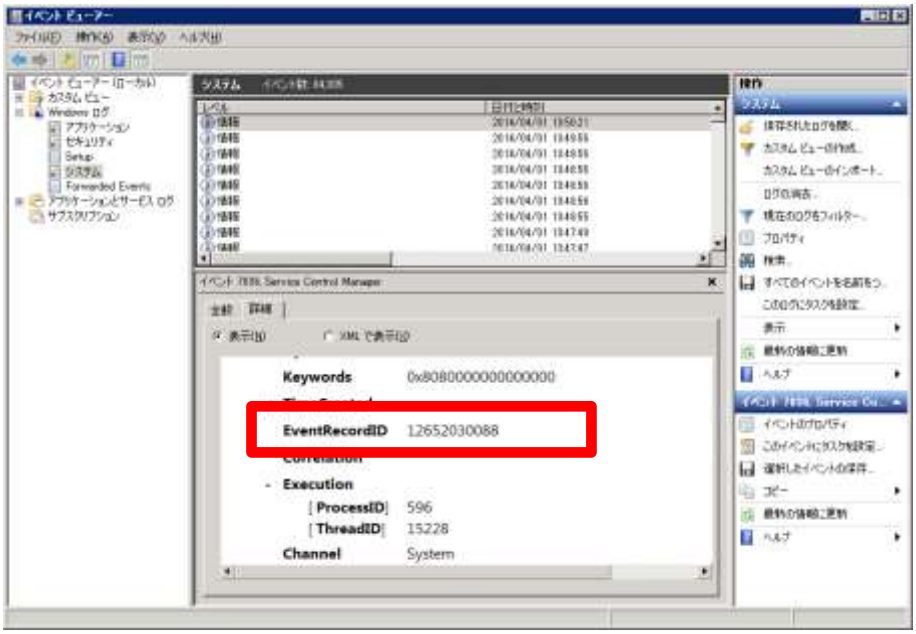
Windows イベントログファイル（Application.evtx,System,evtx 等）の出力先変更方法

本手順は、Windows のイベントログ（EventRecordID）が 42 億件を超えた際、BOM 側で監視が正しく行われない現象を改善するためにおこなう手順です。

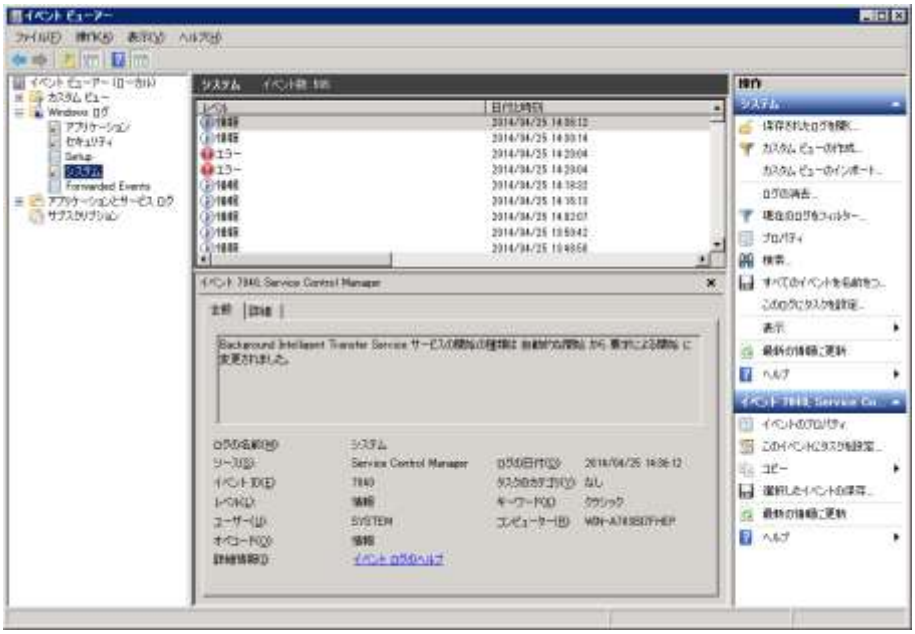
Windows のイベントログファイルへの書き込み先を変更することにより、正しく監視を行うことが可能です。



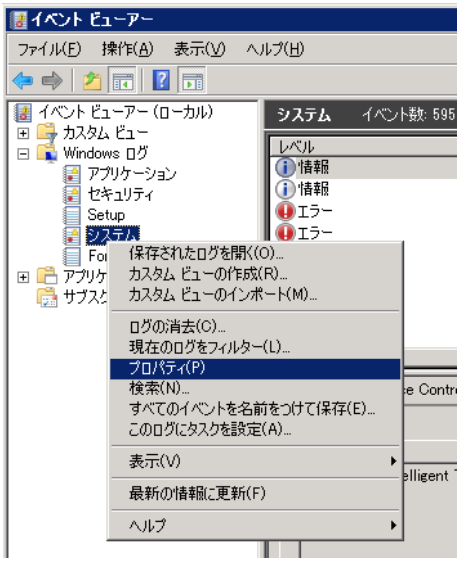
42 億（EventRecordID）を超えたイベントログ例

- イベントログファイルの出力先変更手順

1. 「スタート」→「管理ツール」→「イベントビューアー」を選択します
2. 「イベントビューアー（ローカル）」 → 「Windows ログ」 → 「システム」を選択します

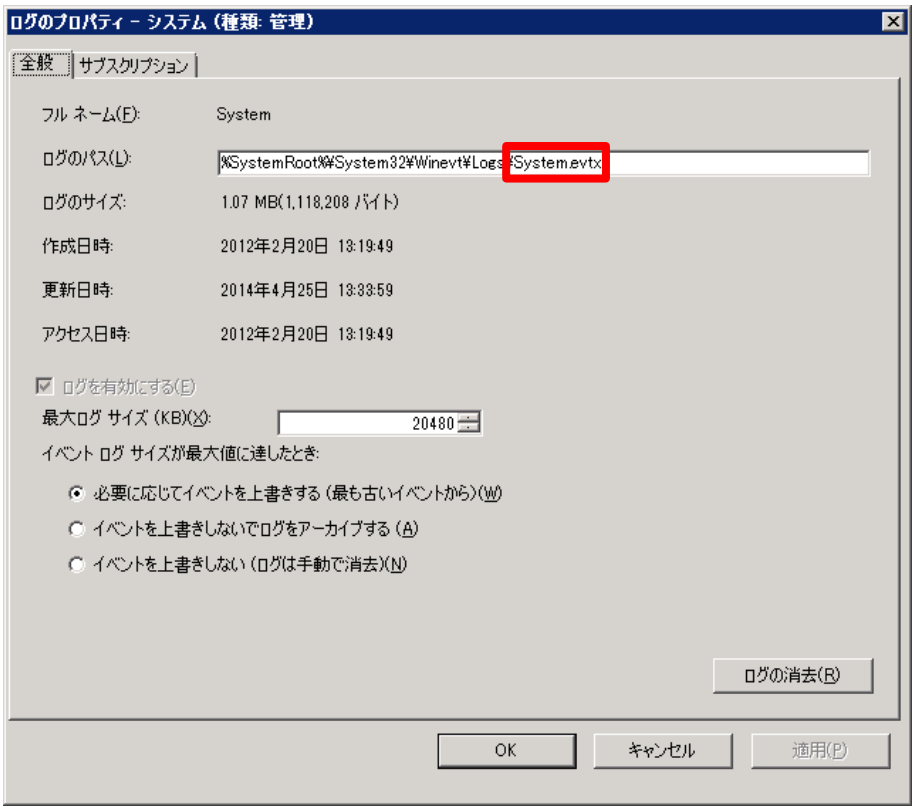


3. コンテキストメニューより「プロパティ(P)」を選択します

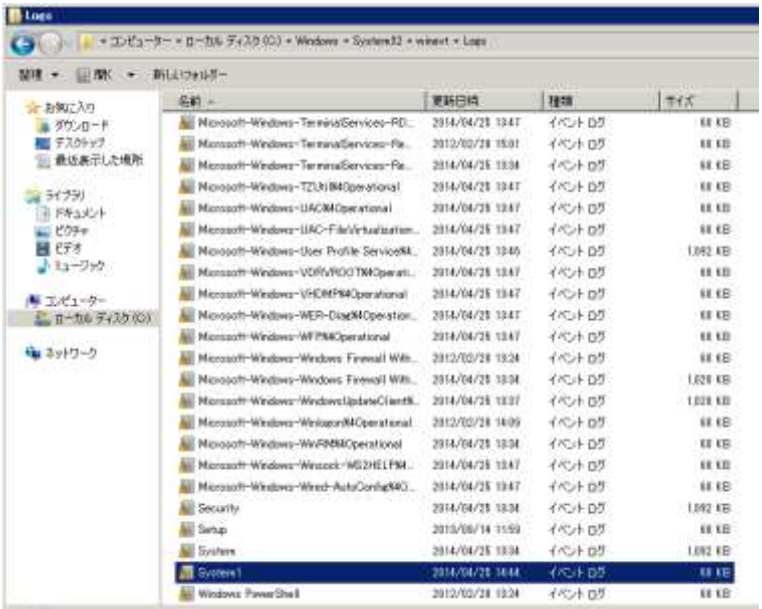


4. ログのプロパティ画面が開きますので、「ログのパス」内に表示されているファイル名を任意のファイル名へと変更し「OK」ボタンをクリックします。

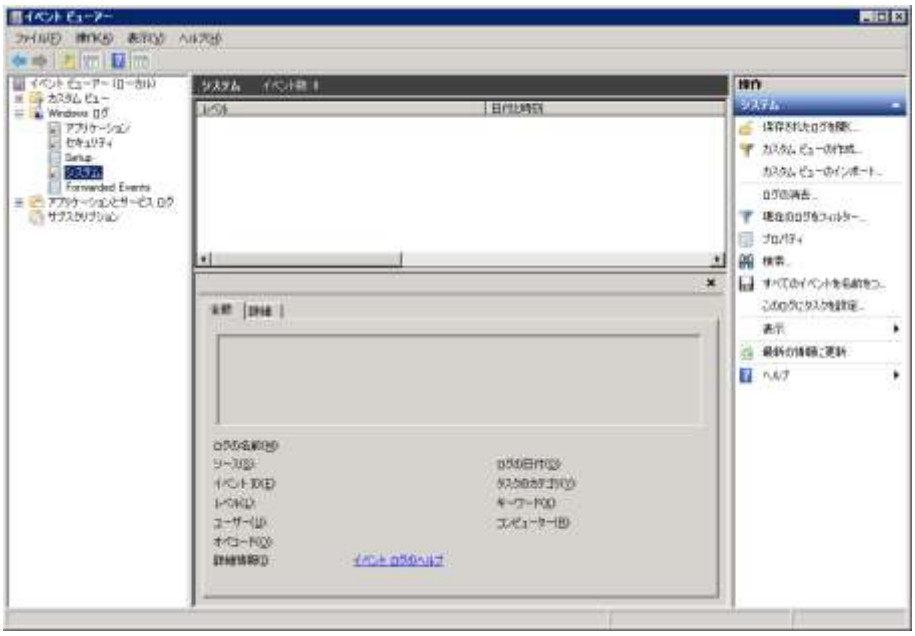
※ここでは「System1.evtx」と入力したものとします。



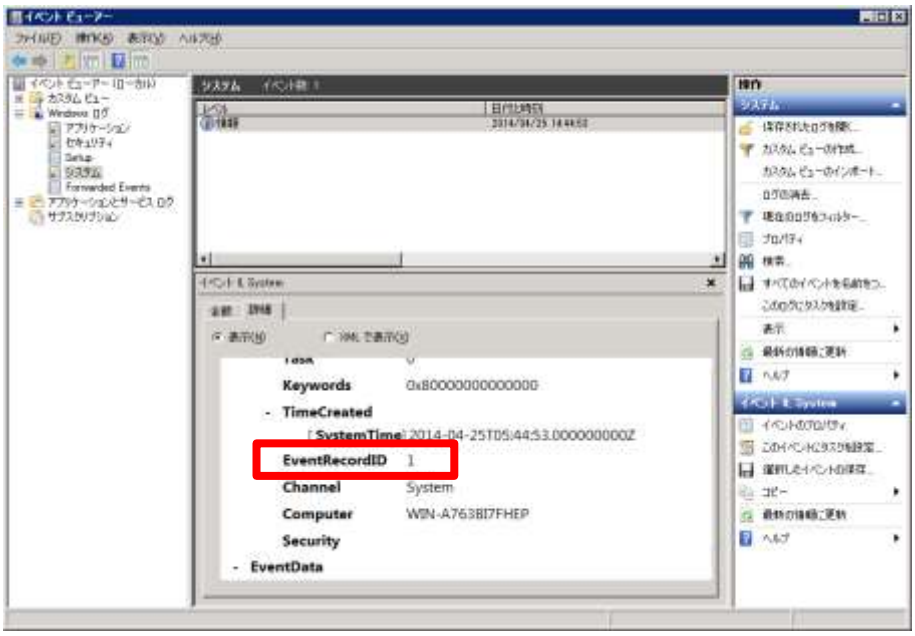
5. ログのパスに表示されているアドレスを確認すると、項番 4 で入力したファイル名でファイルが作成されていることが確認できます。



6. イベントビューアーを確認すると、イベントログ「システム」が新たなファイルで作成され、古いログが表示されていないことが確認できます。



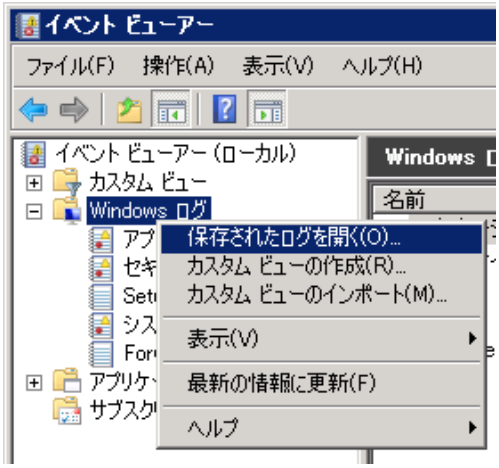
7. 新しいイベントログが書き込まれた際、「EventRecordID」が 1 番から採番されていることを確認することができます。



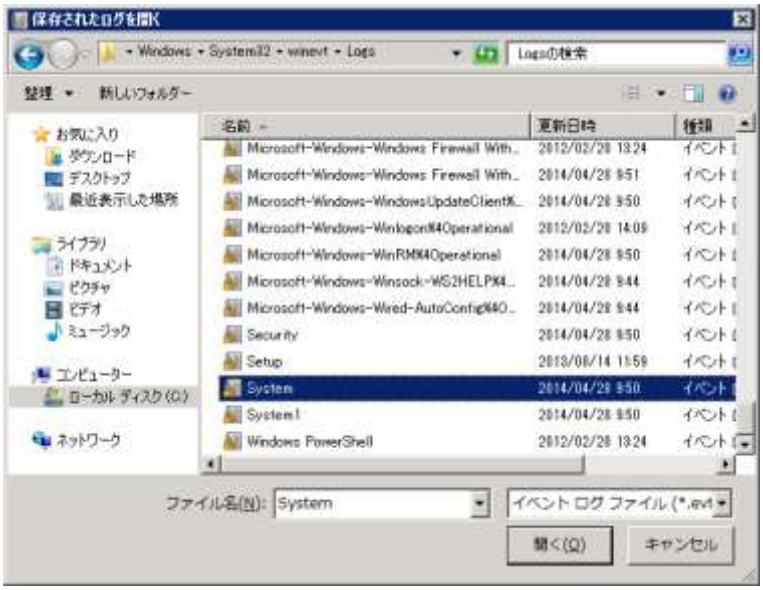
- 従来使用していたイベントログファイルの参照方法

  従来使用していたイベントログファイルを参照する方法を下記に記します。

  1. 「スタート」→「管理ツール」→「イベントビューアー」を選択します
  2. 「イベントビューアー（ローカル）」→「Windows ログ」を選択し、コンテキストメニューより「保存されたログを開く(O)...」を選択します。



  3. ファイルの保存場所を要求されますので、古いイベントログファイルがあるアドレスを指定し、該当ファイルを選択します。



4. 「保存されたログ」配下に表示されますので、必要に応じて古いイベントログを確認することができます。