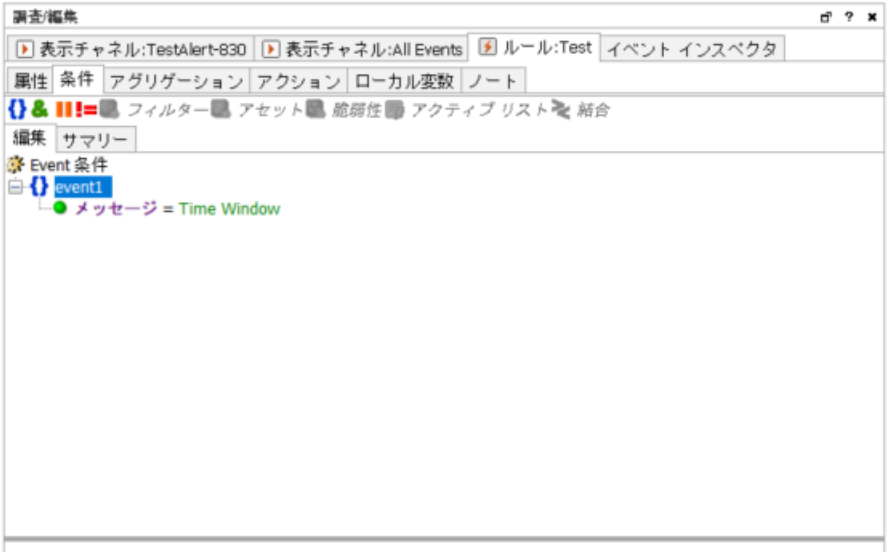
ルール アクション On Time Window Expiration （タイム ウィンドウの有効期限）の例

2023 年 3 月 16 日　ArcSight Support

1．ルールの設定

1.1 条件

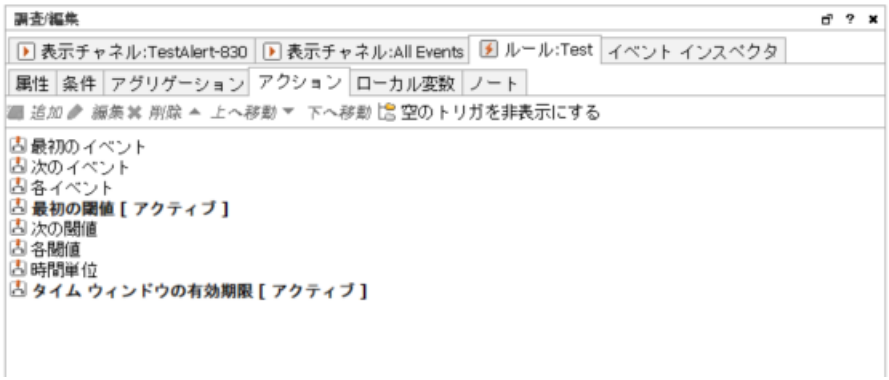


1.2 アグリゲーション

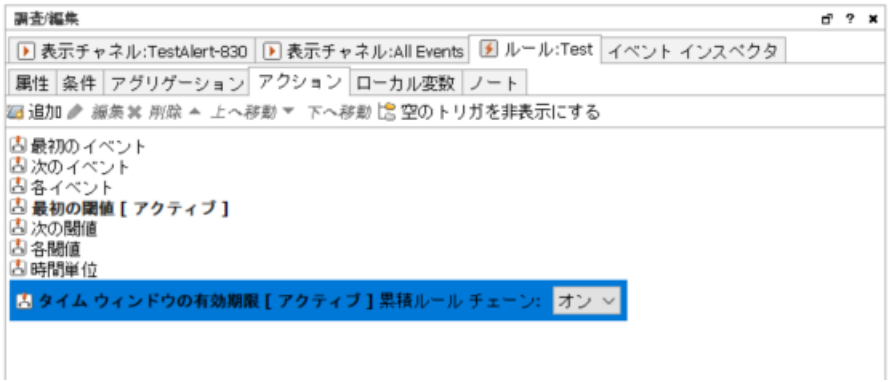
タイムフレーム 2 分、一致数 5 としています。

1.3 アクション

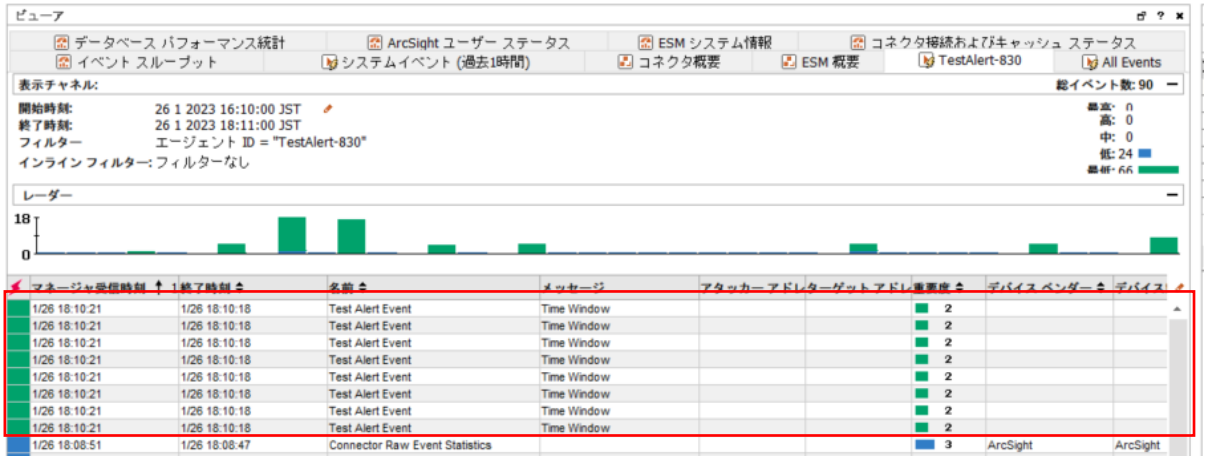
「最初の閾値」と「タイム ウィンドウの有効期限」をアクティブとしています。



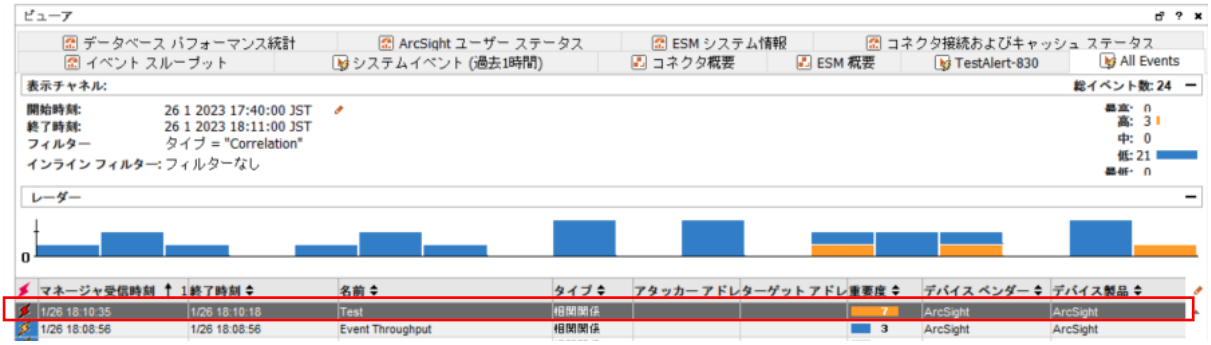
2. 累積ルールチェーンがオンの場合



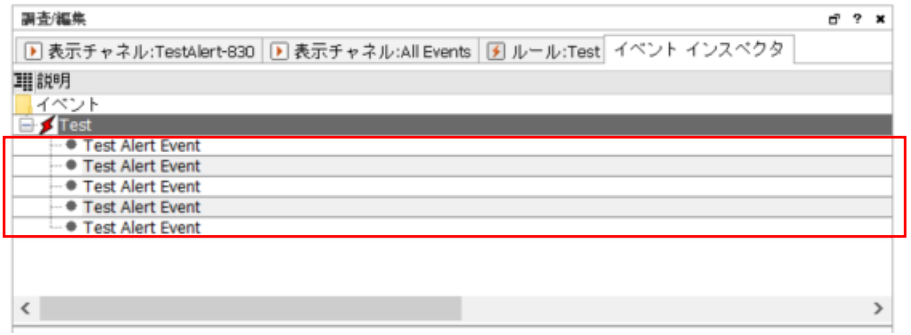
2.1 ルールの条件にマッチする 8 つのイベントを送付した場合



2.2 次の相関イベント（２分間で５つのイベント）が作成されます。こちらは「最初の閾値」アクションで作成された相関イベントです。

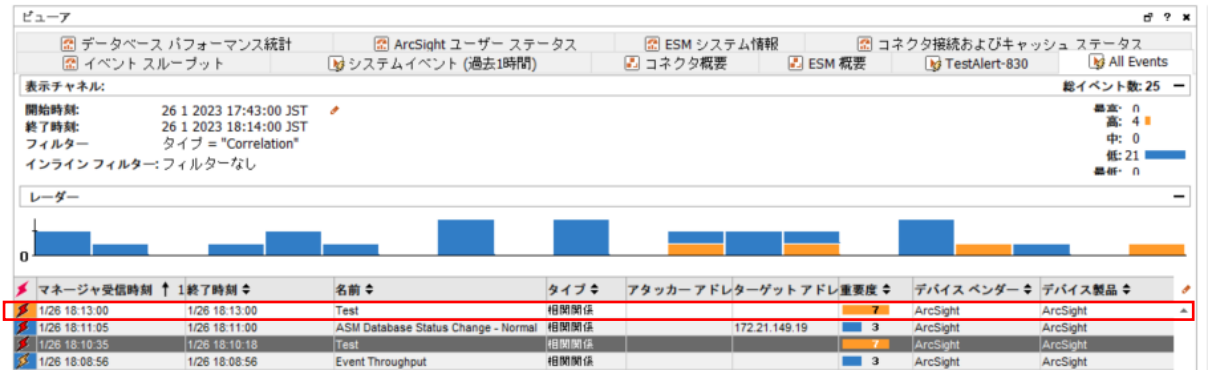


このイベントを右クリックし「イベント詳細表示」を選択すると次の様に表示されます。

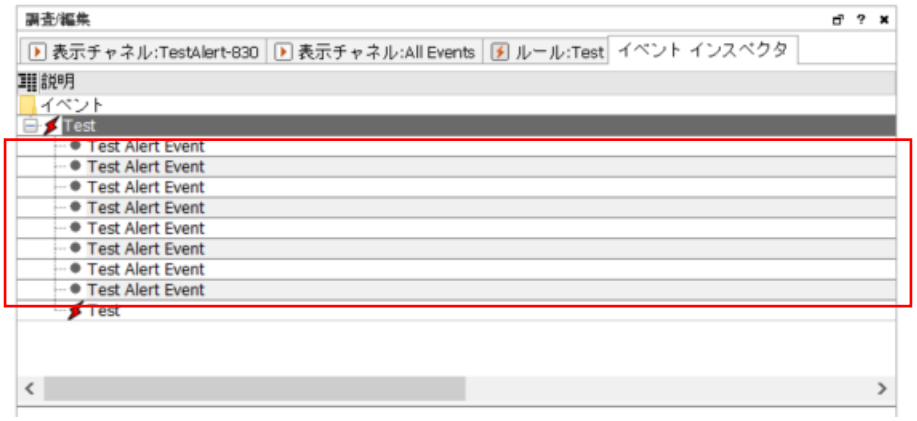


こちらはイベントのトリガとなった５つのベースイベントになります。

次に、ルールのタイムフレーム（今回は２分）経過すると次の追加の相関イベントが作成されます。こちらが「タイム ウィンドウの有効期限」アクションで作成された相関イベントになります。



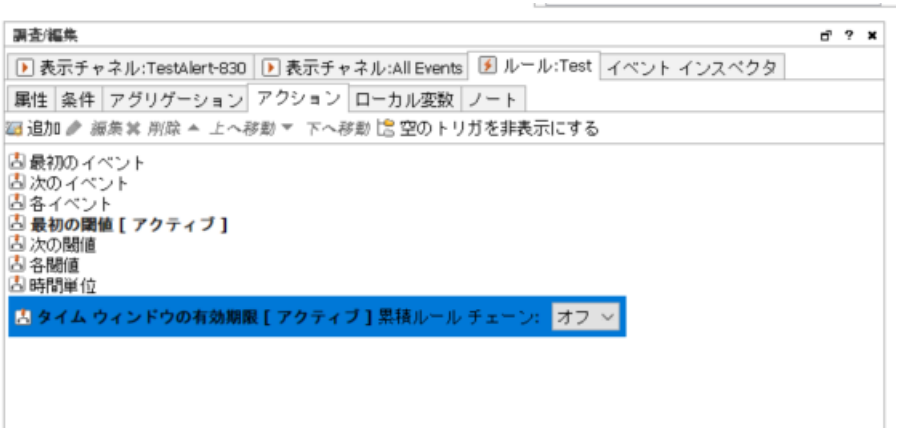
このイベントを右クリックし「イベント詳細表示」を選択すると次の様に表示されます。



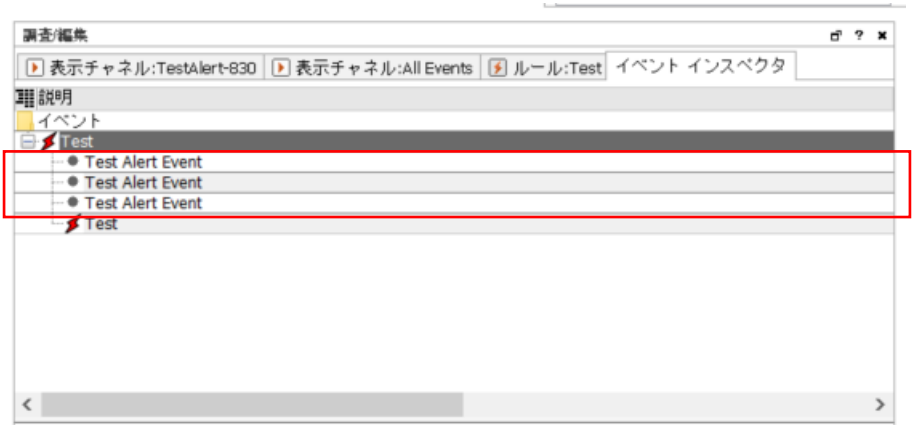
本来であれば後半の３つのベースイベントはトリガの要件を満たしていませんが、On Time Window Expiration （タイム ウィンドウの有効期限）をアクティブにしているためこの相関イベントが作成されます。

3. 累積ルールチェーンがオフの場合

なお、次の様に累積ルールチェーンがオフの場合には、



「タイム ウィンドウの有効期限」アクションで作成された相関イベントは、次の様にトリガの要件を満たしていない後半の 3 つのベースイベントとなります。



以上