IBM Tivoli Risk Manager
バージョン 4.2 フィックスパック 1
Readme

注:

本書および本書で紹介する製品をご使用になる前に、特記事項に記載されている情報をお読みください。

First Edition (September 2004)

本書は、IBM Tivoli Risk Manager バージョン 4.2、Fix Pack 1、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

目次

1 この Fix Pack について

このセクションでは、この Fix Pack についての一般情報を記載します。この Fix Pack をインストールする前に、この資料全体をお読みください。

この Readme 資料は PDF 形式でのみ提供されます。

この Fix Pack で提供されるローカリゼーション・パックについては、この Readme の『*ローカリゼーション・パック情報*』のセクションを参照してください。

1.1 Fix Pack の内容

この Fix Pack で提供されるものの内容は、以下のとおりです。

- Readme ファイル (当資料)
- この Fix Pack のイメージ・レポート
- この Fix Pack の CD-ROM イメージ

1.2 この Fix Pack によって置き換えられるパッチ

この Fix Pack によって置き換えられるパッチは、以下のとおりです。

- 4.2-RMG-0001LA
- 4.2-RMG-0002LA
- 4.2-RMG-0003LA
- 4.2-RMG-0004LA

1.3 サポートされるオペレーティング・システム

このセクションでは、この Fix Pack によってサポートされるプラットフォームおよびデータベースをリストしています。

サポートされるオペレーティング・システムのバージョン [1]	役割				オプションのコンポーネント			
	イベント・サーバー	分散相関サーバー	ゲートウェイ	クライアント	**Crystal Reports**	**ネットワーク IDS**	**Web IDS**	**Web アプリケーション**
AIX® 5L V5.1 (32 ビットまたは 64 ビット)	○	○	○	○		○[3]	○	○
AIX 5L V5.2 (32 ビットまたは 64 ビット)	○	○	○	○		○[3]	○	○
Solaris® 8 (SPARC) [2]	○	○	○	○		○	○	○
Solaris 9 (SPARC)	○	○	○	○		○	○	○
HP-UX 11i (32 ビットまたは 64 ビット)	○	○	○	○			○	○
Windows® 2000 Professional (SP3)	○	○	○	○	○		○	○
Windows 2000 Server (SP3)	○	○	○	○	○		○	○

サポートされるオペレーティング・システムのバージョン[1]	役割				オプションのコンポーネント			
	イベント・サーバー	分散相関サーバー	ゲートウェイ	クライアント	**Crystal Reports**	ネットワーク **IDS**	**Web IDS**	**Web** アプリケーション
Windows 2000 Advanced Server (SP3)	○	○	○	○	○		○	○
Windows XP Professional		○	○	○	○		○	○
Windows 2003 Server	○	○	○	○	○		○	○
Red Hat Enterprise Linux AS 2.1 (IA32)	○	○	○	○		○	○	○
Red Hat Enterprise Linux AS 3,0 (IA32)	○	○	○	○		○		
Red Hat Enterprise Linux ES 3.0 (IA32)	○	○	○	○		○		
SUSE LINUX Enterprise Server 8 (iA32)	○	○	○	○		○	○	○
SUSE LINUX Enterprise Server 8 (pSeries®)				○			○	
SUSE LINUX Enterprise Server 8 (zSeries®)	○	○	○	○		○	○	○
SUSE LINUX Enterprise Server 9 (iA32)	○	○	○	○		○		○

オペレーティング・システムの注:

1. この表に記載されている情報は、この Fix Pack が入手可能になった時点の情報に基づいています。この表は、オペレーティング・システムのベンダーが告知している使用可能期間が終了していないオペレーティング・システムを記載しています。最新のサポート情報については、IBM 提供のオンライン・サポートを参照してください。
2. Solaris とは、「Solaris オペレーティング環境」のことであり、これ以降は Solaris と表記します。
3. ネットワーク侵入検知システム (ネットワーク IDS) は、64 ビット・システム上ではサポートされません。

RDBMS ベンダー	バージョン
IBM DB2®	7.2 (FP8)、8.1 (FP2)
Oracle	9i、9i v2
Sybase	12
Microsoft SQL Server	7.0、2000

1.4 この Fix Pack の新規内容

このセクションでは、Tivoli Risk Manager 製品に加えられた変更点を記載しています。

- キュー管理のサポートが拡張されました。キューのサイズを制御し、キューの状態に関するイベントを送信する手段を提供するキーワードが備えられました。詳しくは、『資料の更新情報』を参照してください。
- 正規表現のサポートが拡張されました。さらに堅固で最新のバージョンの Xerces 正規表現ライブラリーが使用できるようになりました。これによって標準の正規表現構文のサポートが拡張されます。詳しくは、『資料の更新情報』を参照してください。
- FFDC (First Failure Data Capture) のサポートが追加されました。詳しくは、『資料の更新情報』を参照してください。
- RMAgent_Inactive イベントに組み込まれている msg 属性が拡張され、RMAgent_HeartBeat イベントを送信しなくなったエージェントのホスト名と IP アドレスが含められるようになりました。詳しくは、『資料の更新情報』を参照してください。
- Windows 2003 Server がサポートされるようになりました。

2 インストールおよび構成

2.1 前提条件

Tivoli Risk Manger Fix Pack 1 には、以下のソフトウェアが必要です。

- IBM Tivoli Risk Manager バージョン 4.2
- IBM Tivoli Enterprise Console バージョン 3.9、FP01 適用済み (イベント・サーバー役割の場合のみ)
- Red Hat Enterprise Linux の場合、推奨バージョンの Java ランタイムは IBM JRE 1.3.1-6 以降です。そのバージョンを使用できない場合は、IBM ソフトウェア・サポートに連絡してください。

2.2 インストールの注

このセクションでは、Tivoli Risk Manager 製品のインストールに関する付加的な情報を提供します。

- Tivoli Risk Manager 4.2.0-RMG-FP01 Fix Pack がインストール済みであり、Tivoli Risk Manager 製品の初期インストール時にインストールしなかったオプションのコンポーネント (Crystal Report など) をインストールしたい場合は、IBM ソフトウェア・サポートに連絡して、その手順を実行するために必要なインストール Fix Pack を入手してください。
- この Fix Pack は、フルインストールまたはパッチのいずれでもインストールできます。使用すべき方法の判別について詳しくは、『インストールの手順』のセクションを参照してください。
- Windows イベント・モニターは、Windows イベント・ログが読み取られた最後の場所をマーキングするレジストリー・キーを作成します。これらのエントリーは、イベント・モニターまたは Tivoli Risk Manager エージェントが再始動した場合に読み取りを開始する場所を判別するために使用されます。Tivoli Risk Manager 製品をアンインストールしても、アンインストーラーはこれらのレジストリー・キーをレジストリーから除去しません。イベント・モニターを再インストールした場合、イベント・モニターの次回の起動時はこの古いレジストリー・キーが使用され、イベント・モニターは古いイベントの読み取りを開始します。
  Windows イベント・モニターが現在の日付のみから読み取りを開始し、それより古いイベントは読み取らないようにするには、最初にイベント・モニターを開始する前に、以下のイベント・モニターのレジストリー・キーを削除してください。
  HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\Riskmgr\Agent\RMLogfile
- Tivoli Risk Manager Web アプリケーション・コンポーネントの Solaris システム上へのインストールは、非常に時間がかかったり停止したりする場合があります。オープン・ファイルのデフォルトの最大数は、WebSphere Application Server に対しては設定値が低すぎて、Tivoli Web アプリケーション・コンポーネントのインストールが正常に実行できない場合があります。これが原因で、WebSphere Application Server は、エラー・コードを戻さずに、継続的にインストールを再試行します。
  以下のコマンドを実行して、ファイル記述子の限度を決定することができます。

  ulimit -n

  Tivoli Risk Manager Web アプリケーション・コンポーネントを WebSphere Application Server 上で正常にインストールするには、Tivoli Risk Manager Web アプリケーションを以下の手順のいずれかでインストールする前に、1024 以上の最大ファイル記述子を設定して開始する必要があります (サンプル WebSphere Application Server アプリケーションが Tivoli Enterprise Console Web アプリケーションと共にインストールされると想定)。ただしこれを実行する前に Solaris の資料を必ず読んで、これらの変更を加える際の注意事項、実行手順、および副次的影響を確認してくださ

い。最大ファイル記述子の正確な値は、インストールする WebSphere Application Server アプリケーションの数に応じて変更することが必要な場合があります。

以下の方法の 1 つを使って最大ファイル記述子を変更します。

1. WebSphere Application Server を停止します。
2. 以下のコマンドを実行します。
   ulimit -n 1024
3. WebSphere Application Server を、**ulimit** コマンドを実行したのと同じコマンド・セッションから再始動します。
4. Tivoli Risk Manager 製品をインストールします。

これよりも永続的な解決策としては、以下の属性を /etc/system ファイルに設定して、ファイル記述子のシステム値を変更します。

```
rlim_fd_cur
rlim_fd_max
```

- Sybase データベースでの Tivoli Risk Manager 製品の新規インストールの場合、Tivoli Risk Manager 表が、Tivoli Enterprise Console 製品データベースのデフォルトのセグメントにインストールされます。Tivoli Enterprise Console インストール・システムで定義されているデフォルトのセグメントは非常に小さく、非常に限られた数の Tivoli Risk Manager アーカイブ表イベントしか保持しません。Tivoli Risk Manager 製品を Sybase 上でデフォルトのインプリメンテーションで使用するには、Tivoli Enterprise Console データベースのデフォルトのセグメントを、別のデバイスを追加して増やすことができます。

  以下の例では、200 MB のデバイスを TEC_SYSTEM_2 というデフォルトのセグメントに作成して、デフォルトのセグメント・サイズを増やす手順を示しています。

  注:
  - ALTER DATABASE ステートメントは、新規デバイスをデフォルトのセグメントに自動的に追加します。
  - Sybase システム用のユーザー ID を使用して Sybase 環境をセットアップし、この手順を実行します。このユーザー ID には、Sybase 環境に対する適切な権限がなければなりません。

  1. 以下のようにして、rm_exp_archive_table.syb.sql ファイルというスクリプトを作成します。

     ```
     use master
     go
     DISK INIT name="TEC_SYSTEM_2",
     physname="/data/sybase/data/TEC_SYSTEM_2",
     vdevno=14,
     size=102400
     go
     ALTER DATABASE tec
     on TEC_SYSTEM_2 = 200
     go
     ```
  2. 以下のパラメーターを評価し、インストール・システムの必要を満たすようにそれらを変更します。
     - **DISK INIT** name:インストール・システムに適した名前を選択します。
     - **physname**:作成するデバイスまでの、オペレーティング・システム・パス名を指定します。
     - **vdevno**:必ず使用されていない番号にしてください。以下のコマンドを実行すれば、現在使用されている番号を判別することができます。select distinct low/16777216 from sysdevices

3. 以下のコマンドを実行して、スクリプトを実行します。

   isql -Usa -P<*pw*> -S<*system*> -i rm_exp_archive_table.syb.sql

   変数 <*pw*> は SQL パスワードであり、変数 <*system*> はデータベースがインストールされているシステムの名前です。

- インストール時に以下のメッセージが表示され、Java 実行可能プログラムが見つからないことが示されます。

  "JVM not found"

  これは、一時ディレクトリーがあるファイル・システム上で使用可能なスペースが不十分であることが原因の場合があります。これが理由であれば、以下のいずれかを実行することができます。

  - ファイル・システム上でスペースを解放する
  - ファイル・システムに追加のスペースを割り当てる

  必要なスペースは、インストールされた Java JRE のサイズの最大で 3 倍にすることができます。

- Tivoli Risk Manager 製品を再インストールし、トランスポート・タイプを TME に変更する場合、以下のように、/etc/Tivoli/rma_eif_env.sh スクリプト・ファイル内の **TMEEndpoint** キーワードの値を true に変更します。

  TMEEndpoint=true

2.3 インストールの手順

このセクションでは、この Fix Pack のインストールについての情報を記載しています。

Tivoli Risk Manager 4.2.0-RMG-FP01 Fix Pack は、フルインストールまたはパッチ・インストールのいずれかでインストールできます。フルインストールは、以下の条件下では必ず実行する必要があります。

- Web アプリケーションを、DB2 以外の RDBMS 製品とともに使用する。
- この Fix Pack を以下のプラットフォームのいずれかにインストールする。

  Windows 2003 Server
  Red Hat Enterprise Linux AS 3.0
  Red Hat Enterprise Linux ES 3.0
  SUSE LINUX Enterprise Server 8 (iA32)
  SUSE LINUX Enterprise Server 9 (iA32)

フルインストールに使用すべきインストール・パッケージについては、IBM ソフトウェア・サポートに連絡してください。

2.3.1 パッチのインストール

以下のコマンドを実行して、パッチをインストールします。

rm4201_setup_<*platform*> [-silent | -console]

<*platform*> には、以下のいずれか 1 つのプラットフォームを指定します。

aix:	Tivoli Risk Manager 製品がサポートする AIX のバージョン
hpux:	Tivoli Risk Manager 製品がサポートする HP-UX のバージョン
linux:	Tivoli Risk Manager 製品がサポートする Linux (IA32) のバージョン
linuxppc:	Tivoli Risk Manager 製品がサポートする Linux (PPC) のバージョン
solaris:	Tivoli Risk Manager 製品がサポートする Solaris (SPARC) のバージョン
win:	Tivoli Risk Manager 製品がサポートする Windows のバージョン

以下のいずれか 1 つのオプションを指定できます。

-silent	このオプションではユーザー入力は必要ありません。インストール・ディレクトリーのログ・ファイルで非ゼロの戻りコードを調べて、インストールが成功しているかどうかを判断します。
-console	このオプションは、端末 (テキスト・モード) インストールを提供します。このオプションは、Windows プラットフォーム上では使用できないことに注意してください。

オプションを指定しないと、以下のウィンドウが表示されます。

- Language (言語)
- Welcome (ようこそ)
- Pre-installation (プレインストール)
- Post-installation (ポストインストール)

これらのウィンドウにはユーザー入力は必要ありません。それぞれのウィンドウが表示されるごとに、「**Next (次へ)**」をクリックしてください。

この Fix Pack をイベント・サーバー上にインストールした場合は、インストールの終了後に以下の手順を実行します。

1. 使用したいルール・ベースが現行のルール・ベースであることを確認します。
2. 以下のコマンドを実行します。
   rmcorr_cfg -update

   注:このコマンドはルール・ベースを更新します。さらにこれは Tivoli Enterprise Console イベント・サーバーを停止して再始動します。

2.4 ローカリゼーション・パック情報

4.2-RMG-FP01 Fix Pack に組み込まれているローカリゼーション・パックには、Tivoli Risk Manager バージョン 4.2 製品がサポートしているすべての言語の更新済み翻訳が入っています。このセクションでは、以下のローカリゼーション・パック情報を記載しています。

- ローカリゼーション・パックの注
- ローカリゼーション・パックのインストール手順

2.4.1 ローカリゼーション・パックの注

4.2-RMG-FP01 Fix Pack をインストールする前に、このセクションの情報を検討してください。

- この Fix Pack に組み込まれている更新された各国語リソースは、Tivoli Risk Manager のユーザー・インターフェースとメッセージの変更点を反映しています。
- フルインストールとパッチ・インストールとの違いは、インストールされるファイルの数と、インストール前に実行される前提条件のチェックです。
- パッチ・インストール時に表示されるウィンドウは、フルインストール時に表示されるものと同じです。

2.4.2 ローカリゼーション・パックのインストール手順

このセクションでは、ローカリゼーション・パックのインストール情報を記載しています。Tivoli Risk Manager バージョン 4.2 Fix Pack 01 のローカリゼーション・パックは、フルインストールまたはパッチ・

インストールのいずれかでインストールできます。基本製品のフルインストールを実行する場合は、フルインストールを実行します (詳しくは、前述の『インストールの手順』のセクションを参照してください)。基本製品のパッチ・インストールを実行する場合は、パッチ・インストールを実行します。

2.4.2.1 フルインストール

各国語リソースのフルインストールを実行するには、「*IBM Tivoli Risk Manager リリース情報 V4.2*」の『各国語サポート』のセクションにあるインストール手順を参照してください。

2.4.2.2 パッチ・インストール

パッチ・インストールを実行するには、以下のいずれかのコマンドを実行します。

Windows プラットフォームの場合:

```
rmlp4201_setupwin32.exe
```

UNIX および Linux プラットフォームの場合:

```
./rmlp4201_setup<platform>.bin
```

<*platform*> には、以下のいずれか 1 つのプラットフォームを指定します。

aix:	Tivoli Risk Manager 製品がサポートする AIX のバージョン
hp11x:	Tivoli Risk Manager 製品がサポートする HP-UX のバージョン
linux:	Tivoli Risk Manager 製品がサポートする Linux (IA32) のバージョン
linuxppc:	Tivoli Risk Manager 製品がサポートする Linux (PPC) のバージョン
solaris:	Tivoli Risk Manager 製品がサポートする Solaris (SPARC) のバージョン

Linux for zSeries (S/390) の場合:

```
java -Dis.javahome=/opt/IBMJava2-s390-131/jre -cp ./rmlp4201_setup.jar run
```

3 この Fix Pack によって訂正される APAR

このセクションでは、4.2.0-RMG-FP01 Fix Pack が提供する APAR フィックスの説明と解決内容を記載しています。

APAR:IY48016

症状:Web 侵入検知システム (Web IDS) の複数のインスタンスが同じシステム上で実行している場合、すべてのインスタンスが webids.lastread ファイルの同じコピーを使用するので、再開機能が正しく機能しない。

解決内容:Web IDS 機能の各インスタンスは、webids.lastread ファイルの個別のコピーを使用するようになりました。

APAR:IY50483

症状:Tivoli Risk Manager または Tivoli Enterprise Console サーバー上で、tec_rule プロセスが高い CPU 使用率を示す。これが、着信イベントが QUEUED 状態のままとなる原因となっている。

解決内容:インシデント・グループを生成するための Tivoli Risk Manager および Tivoli Enterprise Console のルールは修正され、パフォーマンスが改善されました。インシデント・グループ処理のための追加の構成オプションが、$RMADHOME/etc/tec/rules ディレクトリーの riskmgr_config.pro ファイルに追加されました。これらのオプションの使用の詳細については、riskmgr_config.pro ファイルの注釈を参照してください。

APAR:IY52322

症状:部分イベントを受信すると、分散相関サーバーが停止する。

解決内容:Tivoli Enterprise Console の新規 API キーワードである **ReadRetryInterval** を使用して、部分イベントの受信時に Event Integration Facility API が使用するタイムアウト値を構成します。

このキーワードのデフォルト値は 120 秒です。

Event Integration Facility の送信側が 2 KB より大きいイベントを扱う場合、そのイベントを、ソケット接続を使用して配信する 2 つのパケットに分割します。イベントが部分イベントであると受信側が判断した場合、2 番目のパケットを受け取るまでこのキーワードによって指定された時間だけ待機してから処理を完了します。この時間内に 2 番目のパケットが受信されない場合、受信済みの部分イベントは破棄され、メッセージがログに書き込まれます。

APAR:IY52323

症状:Tivoli Risk Manager エージェント間の未使用のソケット接続が、システムの再始動時にクローズされない。

解決内容:エージェント間の未使用のソケット接続は自動的にクローズされるようになりました。

APAR IY53525

症状:UNIX システム上で、イベント・モニターは、ログ・ファイルのローテーション時に作成された新規ログ・ファイルを読み取ることができない。

解決内容:イベント・モニターは、新規ログ・ファイルを正しく読み取るようになりました。

APAR IY53527

症状:イベント・モニターがサポートする正規表現構文の資料が必要である。

解決内容:正規表現のサポートが改善され、資料が備えられました。資料の変更については、『資料の更新情報』を参照してください。

APAR:IY53678

症状:イベント・モニターは Java ヌル・ポインター例外を生成するが、それがクラスのインデックス・パターンと一致するイベントを解析する場合であり、XML ファイルでそのクラスに定義されたクラス・パターンを解析する場合ではない。

解決内容:イベント・モニター処理は変更され、イベント・ストリングがクラスのインデックス・パターンに一致するが、クラス・パターンには一致しない場合、それはクラスの一致とは見なさずに、別の一致するクラスの検索を継続するようになりました。

APAR:IY53713

症状:データベースにイベントのグループが挿入され、挿入が部分的にしか成功していない場合、重複キー例外を受け取る。

解決内容:データベースへのイベントの挿入は正しく実行されるようになりました。それぞれのイベントは一度だけ挿入されます。重複キーが検出された場合、重複イベントを破棄するように処理が拡張されています。

APAR:IY54408

症状:**wrmadmin -i** コマンドを繰り返し使用すると、システムがメモリーを使い果たすため、システムが停止する。

解決内容:**wrmadmin -i** コマンドは、システム・メモリーの問題を引き起こさずに繰り返し使用できるようになりました。

APAR:IY54568

症状:Windows イベント・ログのイベント・モニターは、既に処理済みのイベントを再処理する。

解決内容:イベントは繰り返し再処理されることはなくなりました。

APAR:IY55241

症状:ネットワーク IDS ファイルを更新して、ぜい弱性 CAN-2002-0562 の正しいシグニチャーを組み込む必要がある。

解決内容:シグニチャー・ファイルは更新され、正しいシグニチャーが組み込まれました。

APAR:IY55319

症状:**wrmqueue** コマンドは、多数のイベントがキューに入っていると完了しない。

解決内容:**wrmqueue** コマンドに関係した内部処理が変更され、この問題は訂正されています。このコマンドについて詳しくは、『資料の更新情報』を参照してください。

APAR IY55895

症状:さまざまなアダプター・パッケージに同梱されている「*IBM Tivoli Risk Manager アダプター・ガイド*」および他の PDF 資料は Event Mapping Table に言及している。この表は Web サイトに掲載されておらず、ダウンロードしたり参照用に入手することができない。

解決内容:Event Mapping Table の資料 (DCF 1171204) は、以下の Risk Manager サポート Web サイトに掲載されるようになりました。
http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliRiskManager.html

APAR IY55927

症状:DBCS ロケールで実行すると、Tivoli Risk Manager エージェントは DBCS 文字を含むイベントを破棄する。以下のメッセージが Tivoli Risk Manager メッセージ・ログに書き込まれる。

HRMAG0135W An event integration facility TECAgent filtered the following event

解決内容:Tivoli Risk Manager エージェントは、DBCS 文字を含むイベントを正しく処理するようになりました。

APAR:IY56431

症状:Tivoli Risk Manager イベント・リポジトリーは、Microsoft SQL を、それが大文字小文字を区別するオプションとともにインストールされている場合にサポートしない。この問題が生じていることは以下の症状から知ることができる。

- イベントが Microsoft SQL イベント・アーカイブに書き込まれない。
- 以下のエラー・メッセージが Tivoli Risk Manager メッセージ・ログに書き込まれる。

HRMAG0082E SQL exception:[Microsoft] [SQLServer 2000 Driver for JDBC]

[SQLServer]Invalid object name 'RM_T_ARC41'

解決内容:以下のコマンドを実行して、この問題を訂正する DDL ファイルを実行してください。

```
osql -U tec -P <password> -d tec -S <server> -n -i %RMADHOME%\dbschema\rm_t_arc41_uc.ms.sql
```

4 既知の制限

このセクションでは、制限を一つ一つ説明し、有効な予備手段がある場合はそれを示しています。

4.1 インストール

制限:インストール中に、次のような誤った警告メッセージが表示される。

WARNING:could not copy log output /opt/RISKMGR/rminstall_log.txt

(No such file or directory)

予備手段:インストール中にエラーが発生したと思われる場合は、Tivoli Risk Manager 製品を再インストールし、インストール・コマンドで以下のオプションを指定して、/opt/RISKMGR 以外のディレクトリー内にログを作成します。

-l !<*fully qualified path*>

変数 <*fully qualified path*> は、rminstall_log.txt ファイルの完全修飾パスです。

4.2 相関サーバー

制限:Tivoli Risk Manager エージェントのイベント (たとえば RM_Sensor、RM_Error、RMAgent_Inactive、RMAgent_QueueProblem) が Tivoli Enterprise Console 製品に送信されず、イベント・コンソールに表示されない。この問題は、以下の基準が*両方とも* 当てはまるシステムのみが該当します。

- インストール・システムが、イベント・サーバーまたは分散相関サーバーである。
- デフォルトのインストールを実行しなかった。変更の選択として、インシデント・イベント (RM_Incident) のみを Tivoli Enterprise Console サーバーに送信するようにした。インストールの選択項目についての詳細は、「*Tivoli Risk Manager インストール・ガイド V4.2* 」の 102 および 114 ページを参照してください。

予備手段:この問題を解決するには、以下の手順を実行します。

1. 相関サーバーおよびイベント・サーバー上の $RMADHOME/etc/rmagent.xml ファイルを編集して、以下のフィルター定義を追加します。

```
<filter name = "nonSensorEvents">
   <OR>
      <isa value = "RM_AgentProblem"/>
      <NOT>
      <isa value = "RM_SensorEvent"/>
</NOT>
   </OR>
</filter>
```

2. 既存のコネクター定義の <withfilter name ="incidents"/> ステートメントを変更して、以下のように新規フィルター名 nonSensorEvents を指定します。

```
<connector>
   <from name ="correlation"/>
   <to name ="incident_sender"/>
   <withfilter name ="nonSensorEvents"/>
</connector>
```

3. 変更を有効にするために、エージェントを再始動します。

4.3 Tivoli Enterprise Console イベント・サーバー

制限:イベント・コンソールに送信された RMAgent_Inactive および RMAgent_QueueProblem イベントは、RM_SensorEvent グループ・ビューに、他のセンサー・イベントと混在して表示される。Tivoli イベント・コンソールまたは分散相関サーバーにデフォルト構成をデプロイした場合は、RM_SensorEvent グループ・ビューに多数のイベントが含まれることがあります。その場合、ネットワーク内の Tivoli Risk Manager のエージェントとキューの問題を警告する Tivoli Risk Manager エージェントのイベントを認識することが難しくなります。

予備手段:エージェントの問題をモニターしやすくするには、以下の手順を実行して、イベント・コンソールの RM_Error グループ・ビューに RMAgent_Inactive および RMAgent_QueueProblem イベントが入るようにカスタマイズします。

1. イベント・コンソールのメイン・ビューで、**「Windows」→「構成 (Configuration)」**をクリックする。
2. 左側にある**「イベント・グループ (Event Groups)」**をクリックする。
3. **「RM_Error」**をクリックする。
4. ウィンドウを右クリックして、**「フィルターの作成 (Create Filter)」**をクリックする。「イベント・グループ・フィルターの追加 (Add Event Group Filter)」ウィンドウが表示されます。
5. 「名前 (Name)」フィールドに、RM_AgentProblem と入力する。
6. 「説明 (Description)」フィールドに、フィルターの説明を入力する (オプション)。
7. **「制約の追加 (Add Constraint)」**をクリックする。
8. 属性リストから**「クラス (Class)」**を選択する。
9. オペレーター・リストから**「同種 (Like)」**を選択する。
10. 値として RMAgent_% を入力する。(この値は大文字小文字が区別されます。)
11. **「OK」**をクリックする。
12. 「イベント・グループ・フィルターの追加 (Add Event Group Filter)」ウィンドウで**「SQL のテスト (Test SQL)」**をクリックして、フィルターが正しい数のイベントを生成するかどうかを判別する。
13. **「OK」**をクリックして変更を保管する。
14. イベント・コンソールを停止して、再始動する。
15. **「Windows」→「サマリー・チャート・ビュー (Summary Chart View)」**をクリックして RM_Error コンソール・グループを開き、フィルターが正しく機能したかどうかを判別する。

4.4 Tivoli Risk Manager エージェント

- 制限:メモリーの制約からメモリー不足の問題が起こることがある。この問題が最も顕著に現れるのは、AIX システムです。これは、受信側または送信側の数が増加するか、rmagent.xml での宛先定義に **instanceCount** パラメーターが追加されると起こることがあります。また、この問題は、他のプラットフォームでも、送信側または **instanceCounts** が多数追加されると発生します。これは、いずれの場合も追加スレッドが作成されてメモリー使用量が増加するためです。

  Tivoli Risk Manager エージェントは Java プロセスであるため、Java 環境のメモリー割り振りの制約を受けます。AIX の場合、/etc/security/limits ファイルでのストレージ割り振りのデフォルト値が低いため、それがこのメモリー制限に大きく影響します。Tivoli Risk Manager を AIX のデフォルトのインストール・システムで実行できるようにするために、最大 Java ストレージが、

RMADHOME/etc/rmad.conf ファイル内で定義されている **RmagentMemMax** パラメーターで意図的に制限されています。AIX ではこの値は 92 MB に設定されていますが、この設定では基本サーバーのインストール・システムに十分なメモリー割り振りしか提供されません。

予備手段:どのプラットフォームでも、**RmagentMemMax** パラメーターを使用して、Tivoli Risk Manager が使用できる最大メモリーを増やすことができます。たとえば AIX の場合は、以下の手順を実行します。

1. 制限ファイル内のデータ、rss、スタックの値のデフォルト値を大きくする (または **ulimit** コマンドを使用する)。
2. rmad.conf ファイル内の RmagentMemMax の値を大きくする。
3. システムから一度ログオフしてからログオンする。
4. **wrmadmin -r** コマンドを実行して Tivoli Risk Manager エージェントを再始動する。

- 制限:永続ディレクトリーが置かれているディスクが満杯になっていると、Tivoli Risk Manager 製品を再始動できない。

  予備手段:Tivoli Risk Manager 製品を再始動する前に、十分な空きディスク・スペースがあることを確認してください。必要なディスク・スペース容量を判別するには、次の式を使用します。

  (1 + 宛先の数) × 20 MB

  この*宛先の数*は、rmagent.xml ファイルで定義されている宛先の数です。

- 制限:イベント属性の先頭文字が単一引用符の場合、イベント属性の単一引用符と最終文字が除去されて、そのイベントが破壊される。以下の例は、msg イベント属性に指定された先行引用符と、その結果を示しています。

  'myHostname' is acting suspiciously

  対応するアーカイブ・テーブルの MSG 列には、以下が入ります。

  myHostname' is acting suspiciousl

  予備手段:イベント属性での先行単一引用符の使用を、できるだけ避けてください。これ以外に有効な予備手段はありません。

4.5 DNS 解決

制限:Solaris の場合、**wrmdns** コマンドで DNS 解決が開始されない。

予備手段:DNS 解決を開始するには、以下の手順を実行します。

1. summary_engine.conf ファイルと incident_engine.conf ファイルを編集する。
2. 両方のファイルの dnsResolver=off エントリーを dnsResolver=on に変更する。
3. 以下のコマンドを実行して Tivoli Risk Manager エージェントを再始動する。

   wrmadmin -r

4.6 メッセージおよびトレース・ロギング

- 制限:Linux システムによっては、Linux のデフォルトの IP フィルタリングおよびファイアウォール保護が非常に制限的であるため、トレース・レベルおよびログ・レベルの設定を動的に変更できないことがある。

  Tivoli Risk Manager 製品に組み込まれている JLog パッケージには、Tivoli Risk Manager エージェントの実行中にトレースおよびログの設定を動的に変更できる機能があります。この機能の詳細については、「*IBM Tivoli Risk Manager 問題判別ガイド*」の『ロギング・コマンド行インターフェース』のセクションを参照してください。

Tivoli Risk Manager エージェントは開始時に JLog ログ・マネージャーを呼び出し、これはポート 9992 で listen するログ・コマンド・サーバーを作成します。**Logcmd** クライアント・プログラムとログ・コマンド・サーバーは、このポート上で通信を行います。Linux システムによっては、Tivoli Risk Manager エージェントの実行中はポート 9992 は listen されないため、**logcmd** コマンドは失敗し、Java ConnectionException が出されます。これは、インストールされている IP フィルターおよびファイアウォール保護に起因します。ご使用の Linux システムに以下のいずれかのプログラムがインストールされていて、Tivoli Risk Manager エージェントを開始してもポート 9992 が listen されていることを確認できない場合は、IP ファイアウォールがそのポートへのアクセスを妨げています。

- lokkit
- ipchains
- iptables
- ipfwadm

予備手段:ポート 9992 をアンロックする手順については、ご使用の Linux システムの資料を参照してください。セキュリティー上の理由でこのポートをロックしたままにしておいても、トレースの設定を動的に変更できないということ以外は、Tivoli Risk Manager エージェントの標準的なロギングの妨げになることはありません。

- 制限:UNIX システムでは、ログ・ファイルは循環すると圧縮されるため、ホスト IDS アダプターでは読み取れなくなる。

  予備手段:この問題を回避するには、最後に循環したログ・ファイルのログ圧縮機能をオフにします。

- 制限:以下のメッセージ (HRMAG0147I) の直前に反復メッセージがないことがある。

  The previous message was repeated {n} times

  この場合は、どのメッセージが反復されたかを判別する方法はありません。

  予備手段:有効な予備手段はありません。

4.7 ネットワーク IDS コンポーネント

制限:32 ビット AIX システム上でネットワーク IDS コンポーネントを開始しても、このコンポーネントが開始しないことがある。これは、ネットワーク IDS コンポーネントがネットワークをモニターするのに必要な /dev/bpf0 デバイスが定義されていないか、システムが最後にリブートされてから正しく開始していないために起こります。

予備手段:以下の手順で /dev/bpf0 デバイスを再設定または定義します。

1. AIX 端末セッションから **tcpdump** コマンドを実行する。
2. イーサネット接続が開始されたことを示す次のメッセージが表示されたら、Ctrl+c を押して **tcpdump** コマンドを終了する。

   listening on *xxx*

   文字 *xxx* は、イーサネット・デバイス番号を表しています (たとえば en0)。
3. 以下のコマンドを実行し、ネットワーク IDS プロセスを停止してから再始動する。

   stopnids

   startnids

4.8 Web IDS コンポーネント

- 制限:webids.cfg ファイル内に fileMatch_value=0 をコーディングして Web IDS コンポーネントのログ・ファイルのロールオーバーを無効にすると、エラー・メッセージが表示される。

  予備手段:この問題の予備手段はありません。ログ・ファイルのロールオーバーを無効にすることはできません。

- 制限:Web IDS コンポーネントを同一システム上の複数の Web サーバーをモニターするように構成し、各サーバーのアクセス・ログがすべて同一ディレクトリーにあると、その Web IDS コンポーネントはループする。

  予備手段:Web サーバーのアクセス・ログを、別々のディレクトリーに保管します。

- 制限:**webids -d** コマンドがデバッグ情報を標準出力 (STDOUT) に書き込まない。詳しくは、『資料の更新情報』を参照してください。

  予備手段:有効な予備手段はありません。

4.9 Web アプリケーション

- 制限 (APAR IY58098):Java コンソールを実行するシステムが WebSphere Application Server が稼働するローカル・サブネット上にない場合、Tivoli Risk Manager Web コンソールにログオンできないことがある。これは、Tivoli Risk Manager Web アプリケーションをインストールする際に、rmweb.pl スクリプトの更新で、Web アプリケーション・サーバーを実行するシステムのホスト名に、完全修飾ホスト名ではなく、短縮ホスト名が使用されたことが原因です。

  予備手段:以下の手順を実行して、Web アプリケーション・サーバーの完全修飾ホスト名を指定します。

  1. イベント・サーバーのディレクトリー RMADHOME/cgi-bin にある **rmweb.pl** スクリプトを編集する。
  2. 以下の行を見つける (行 47 近辺)。

     ```
     $output .= "METHOD=POST ACTION=\"http://server1:9080/rmwebapp42/logon\">');\n";
     ```

  3. URL ストリング内の短縮ホスト名を、完全修飾ホスト名 (たとえば server1.mycompany.com) に変更する。

- 制限:古いバージョンの Mozilla がインストールされていると、Web アプリケーションを使用できないことがある。

  予備手段:Mozilla バージョン 1.7.2 以降をインストールします。

- 制限:Tivoli Risk Manager Web アプリケーションをアンインストールしても、WebSphere Application Server のリソースとして、Tivoli Risk Manager JDBC プロバイダーが引き続き存在する。

  予備手段:以下の手順を実行して、Tivoli Risk Manager JDBC プロバイダーを除去します。

  1. WebSphere Application Server 管理コンソールに、管理者としてログオンする。
  2. 「**リソース (Resources)**」をクリックする。
  3. 「**JDBC プロバイダー (JDBC Providers)**」をクリックする。
  4. 有効範囲をサーバー・レベルに設定しておく。
  5. 「**Risk Manager JDBC プロバイダー (Risk Manager JDBC Provider)**」チェック・ボックスを選択する。
  6. 「**削除 (Delete)**」をクリックする。

- 制限:オンライン・ヘルプでの参照先に、アダプター・アドレスのヘルプが誤って表示される。「システム・アドレス (System Addresses)」ウィンドウで疑問符 (?) をクリックすると、システム情報を得るための選択項目として、以下がヘルプ・パネルに表示されます。

ソース・アドレス (Source Address)
宛先アドレス (Destination Address)
センサー・アドレス (Sensor Address)
アダプター・アドレス (Adapter Address)
その他 (Other)

予備手段:予備手段はありません。アダプター・アドレスの情報を得ることはできません。

5 資料の更新情報

このセクションでは、Tivoli Risk Manager バージョン 4.2 ライブラリーの資料の更新情報を記載しています。ライブラリーの訂正内容、および Tivoli Risk Manager 製品に加えられた機能の改善点を理解するには、続くいくつかのセクションで記載している情報を参照してください。

- 資料の種々の訂正
- キューの管理および操作
- FFDC およびその他のトレースに関する資料
- 正規表現のサポート

5.1 資料の種々の訂正

このセクションでは、Tivoli Risk Manager ライブラリーの資料の種々の訂正内容と、この Fix Pack で加えられた機能のマイナー変更に関する情報を記載しています。

5.1.1 IBM Tivoli Risk Manager 管理者ガイド

- 101 ページの『インシデント・ベースの相関ルールのカスタマイズ』のセクションに、以下の文を追加する必要があります。

ルールの <threshold> および <aggregate> エレメントにより、インシデントを生成する時点が決定されます。Tivoli Risk Manager 製品に付属しているデフォルト・ルールでは、各センサー・イベントの **rm_Level** 値を累積させることによりイベントの総計を求め、それが **thresholdCount** 値に達した時点でインシデントが生成されます。**rm_Level** 値は、各イベントの相対的な重みまたは重大度を表します。別のメソッドとして、イベント数をカウントし、そのカウントが特定のしきい値カウントに達するとインシデントを生成するというものがあります。イベントをカウントできるようにするには、ルールから <aggregate> エレメントを除去し、**thresholdCount** パラメーターをインシデントを生成するのに必要なイベント数になるように調整します。

ルールの <cloneable> エレメントの中の **attributeSet** パラメーターは、インシデントの候補になる可能性がある着信イベントの総計を求めるために、イベントのどの属性を使用するかを決定します。このパラメーターで使用される 3 つの標準相関属性は、**rm_SourceToken**、**rm_DestinationToken**、および **rm_CategoryToken** 属性の任意の組み合わせです。以下は、**attributeSet** パラメーターで指定できる使用可能な属性名のリストです。特に断りのない限り、ルールで使用される属性名は、着信イベントの属性名と同じです。

  - rm_SensorToken
  - rm_SourceToken
  - rm_DestinationToken
  - rm_CategoryToken (rm_ClassCategory と同義)
  - rm_CategoryDescription (rm_ClassCategoryDescription と同義)
  - rm_CustomerID
  - rm_Signature
  - rm_Timestamp32
  - rm_Level

- 103 ページの『Setting an Attribute to a Specific Value (特定の値への属性の設定)』のセクションに、以下の変更を加える必要があります。

ルールの <action> エレメント内の <parameters> エレメントを使用して、RM_Incident イベント属性の値を変更できます。ただし hostname および msg 属性は変更できません。

103 ページの 2 番目の例は msg 属性を用いていますが、この例は誤りであり、削除する必要があります。

- 125 ページの『Resource IDs and Dynamic Data (リソース ID および動的データ)』のセクションの最初の段落は、以下のように変更する必要があります。

  リソース ID および動的データ: これらの領域に表示されるテキストは、ハードコーディング・テキストまたはリソース ID で指定されます。

  テキストをハードコーディングすると、1 つのファイルを更新するだけで済み、変更を有効にするために WebSphere 製品を停止して再始動する必要もないため、テキストのコーディングにはこの方法のほうが簡単です。ただし、Tivoli Risk Manager 製品をローカリゼーション・パックを適用して使用する場合は、リソース ID メソッドを使用する必要があることにご注意ください。

  ハードコーディング・テキストを使用する場合は、テキスト・ストリングの始めと終わりを &quot. で囲みます。テキストをハードコーディングするには、以下の手順を実行します。

  1. AdvisorRules.xml ファイルを編集する。
  2. そのファイルに以下の行を追加する。

     ```
     title="&quot.View CVE Recommendation &quot."
     ```

  3. AdvisorRules.xml ファイルを保管する。

  Web ページが表示されると、タイトル領域に「*View CVE Recommendations*」が表示されます。

  ストリング内にイベントまたはインシデント属性を指定する変数をコーディングすれば、ハードコーディング・テキスト内で動的データを使用することもできます。たとえば、ハードコーディング・テキスト内に rm_Category 属性値を表示するには、ステップ 2 のテキストを以下のようにコーディングします。

  ```
  title="&quot.View Recommendations for &rm_Category Event &quot."
  ```

  125 ページの『Resource IDs and Dynamic Data (リソース ID および動的データ)』のセクションの残りの部分の変更はありません。この情報を検討して、動的データとリソース ID の使用法についての理解を深めてください。

- 47 ページの『属性のフィルター操作』のセクションを、以下のように変更する必要があります。

  ### 属性のフィルタリング

  属性をフィルター処理して、それらが Tivoli Enterprise Console サーバーに送信されないようにすることができます。

  エージェントおよび分散相関サーバーの eif_sender.conf ファイルに構成オプションを追加して、拡張スロットが Tivoli Enterprise Console サーバーに送信されないようすることができます。

  たとえば、以下の行を eif_sender.conf に追加します。

  ```
  filterAttributes=/opt/RISKMGR/etc/templates/sensorevent_attributeFilter.xml
  ```

  このフィルタリングの例については、RMADHOME /etc/templates/sensorevent_attributeFilter.xml ファイルを参照してください。

- 付録 A の『Event Integration Facility の送信側および受信側のキーワード』に、以下のキーワードの説明を記載する必要があります。

  filterAttributes=pathname ...

属性フィルタリング仕様を含む 1 つ以上の XML ファイルの絶対パス名を指定します。この仕様に基づくフィルター処理でイベントから拡張属性が除外された後に、イベントが送信されます。属性フィルタリングは、イベントを Tivoli Event Console サーバーに送信する Event Integration Facility の送信側サブコンポーネントに対して使用し、不要なネットワーク・トラフィックを削減して、パフォーマンスの向上に役立てることができます。

属性フィルタリング仕様ファイルのサンプルは、以下のファイルを参照してください。

RMADHOME /etc/templates/sensorevent_attributeFilter.xml

ReadRetryInterval=seconds

Event Integration Facility の受信側が部分イベントを受信したときに待機する秒数を指定します。イベントが部分イベントであると受信側が判断した場合、2 番目のパケットを受け取るまでこのキーワードによって指定された時間だけ待機してから処理を完了します。この時間内に 2 番目のパケットが受信されない場合、受信済みの部分イベントは破棄され、メッセージがログに書き込まれます。デフォルト値は 120 秒です。

- 192 ページの『Manually Configuring the Event Monitor (イベント・モニターの手動構成)』のセクションのステップ 3 にある例は、誤っています。<source name="monitor_receiver_webids" がある行は、以下のように <source name="monitor_receiver_nids" に変更する必要があります。

```
<!-- Event Monitor for NIDS -->
<source name="monitor_receiver_nids"
class="com.tivoli.RiskManager.Agent.Transports.Receivers.rmaMonitorReceiver">
<set key="RMA_conf" value="/opt/RISKMGR/etc/monitor_receiver_nids.conf"/>
</source>
```

- 87 ページの『ハートビートのモニター』のセクションを、以下のように変更する必要があります。

  Tivoli Risk Manager はネットワークにデプロイされたエージェントを自己モニターし、エージェントが非アクティブになると警告を出します。この警告は、相関サーバーの 1 つで生成される RMAgent_Inactive イベントです。RMAgent_Inactive イベントは Tivoli Enterprise Console データベースに入れられ、コンソールに表示されます。以下の警告メッセージが表示されます。

  Missing heartbeat for agent:<*hostname*>/<*ip address*>

  <*hostname*> と <*ip address*> は、RMAgent_HeartBeat イベントを送信しなくなったエージェントのホスト名と IP アドレスの値です。

  デフォルトでは、各エージェントが RMAgent_HeartBeat イベントを生成するように構成されています。各相関サーバーは、RMAgent_HeartBeat イベントをモニターして、エージェントが定期的な RMAgent_HeartBeat イベントの送信を停止すると、RMAgent_Inactive イベントを生成するように構成されています。デフォルトでは、RMAgent_HeartBeat イベントを生成する各エージェントを表す RM_Sensor イベントが作成されます。通常は、RMAgent_HeartBeat イベントは Tivoli Enterprise Console サーバーまたはデータベースには転送されません。

5.1.2 IBM Tivoli Risk Manager コマンド・リファレンス

25 ページに記載されている、**webids -d** コマンドを使用してデバッグ情報を標準出力 (STDOUT) に書き込み、それを別のファイルにリダイレクトできるという説明は誤りです。このオプションは正しく機能しないため、使用すべきではありません。

5.1.3 IBM Tivoli Risk Manager インストール・ガイド

付録 E の『コンポーネントの除去』は、以下の情報を組み込んで更新する必要があります。

Tivoli Risk Manager コンポーネントをアンインストールする前に、以下の作業を実行してください。

1. Tivoli Risk Manager のすべてのアダプターをシャットダウンする。
2. **wrmadmin -k** コマンドを実行して Tivoli Risk Manager 製品をシャットダウンする。
3. イベント・サーバーを除去する場合は、以下の作業を実行します。
   a. 以下のいずれかのコマンドを実行する。
      UNIX の場合:**rmcorr_cfg -delete**

      Windows の場合 **bash rmcorr_cfg -delete**

      注:このコマンドによって以下が実行されます。

      - デフォルトのルール・ベースをロードする。カスタマイズしたルール・ベースを使用する場合は、GUI または **wrb** コマンドを使用して手動でロードします。
      - Tivoli Enterprise Console イベント・サーバーを停止してから再始動する。

   b. **wrmadmin -k** コマンドを実行する。
4. コンポーネントをアンインストールする。除去対象のコンポーネントに使用するコマンドについては、177 ページの表 11 を参照してください。

注:

1. 変更された Tivoli Risk Manager のファイルや追加されたアダプター・ファイルは、Tivoli Risk Manager ディレクトリーから除去されません。
2. イベント・サーバーでは、Tivoli Risk Manager アーカイブ・テーブル、データベース・ビュー、およびイベント・コンソールのイベント・グループは、アンインストール時に除去されません。これらのコンポーネントを除去する場合は、手動で行う必要があります。

5.1.4 IBM Tivoli Risk Manager 問題判別ガイド

23 ページの『Tivoli Management Environment の送信接続タイプ』のセクションに、以下の情報を追加する必要があります。
Tivoli Risk Manager 製品の再インストール時にトランスポート・タイプが TME に変更されている場合は、/etc/Tivoli/rma_eif_env.sh スクリプト・ファイル内の TMEEndpoint キーワードの値を、以下のように true に変更する必要があります。

```
TMEEndpoint=true
```

5.2 キューの管理および操作

このセクションでは、APAR IY55319 のキューの操作と管理に加えられた拡張機能について記載しています。この変更は、永続キューに使用するディスク・スペースの管理の向上のために加えられたものです。この変更以前は、ある一定の期間にわたってイベントが、処理されるよりもキューに入れられるほうが速い場合に、Tivoli Risk Manager 製品ではエラーが発生し、管理者にはその理由が通知されませんでした。この問題を解決するために、構成パラメーターが追加され、キューを管理して、キューの状態が管理者に通知されるようになりました。それらの変更について詳しくは、「*IBM Tivoli Risk Manager 管理者ガイド*」の中の『キューおよびイベント持続性』のセクションの以下の変更内容を参照してください。

キューおよびイベントの永続性

コネクターの to 設定で rmagent.xml ファイル内で参照されるエージェントの各サブコンポーネントには、その処理にキューが関連付けられます。サブコンポーネントが処理する必要のあるイベントは、コネクターの from 設定で指定されたサブコンポーネントによって、関連付けられたキューに入れられます。処

理を実行するサブコンポーネントは、イベントの処理が実行可能になった場合に、キューからイベントを除去します。

永続性の説明

永続性は、rmagent.xml ファイル内の **persist** パラメーターで制御します。デフォルトでは、イベントはキューに入れられるとディスクに永続的に保管されます。処理を実行するサブコンポーネントがタスクを完了したら、イベントはディスクから除去されます。エンジンと宛先のコンポーネント・キューはどちらも、イベントをディスクに永続的に保管しないように構成することができます。イベントを永続的に保管するかどうかを決める前に、以下の情報を注意深く検討してください。

以下の表は、イベントの永続性を理解するために役立つ情報を示しています。

説明	永続性	非永続性
すべてのイベントをディスクに書き込む	はい	いいえ
エラーになったイベントをディスクに書き込む	はい	はい
エージェントの停止時にキューに入れられたイベントをディスクに書き込む (エラーになった再試行イベントとして)	いいえ	はい
エラーになった (再試行) イベントをエージェントの開始時に処理する	はい	はい
エラーになった (永続) イベントをディスクに書き込む	はい	はい

永続性を無効にする理由

イベント・データをディスクに書き込んだり、そのデータを後で除去したりする手間が省けるので、処理速度を向上させることができます。

永続性を有効にしておく理由

システムにはエージェントが利用できるメモリーが限りなく存在しているわけではありません。イベントがディスクに永続的に保管されない場合、それらはメモリー内に保持されなければなりません。予期しないエラー条件が原因でエージェントが終了した場合でも、イベントが消失しないようにする必要があります。永続性を無効にすると、イベント・データが消失する可能性があります。

永続性を無効にする必要はあるか

永続性を無効にするオプションは推奨しません。永続性を使用することを強くお勧めします。

永続性を無効にするには、rmagent.xml ファイルを編集して、以下の例ように persist="no" をサブコンポーネントの定義に追加します。

```
<destination name="eif_sender"
        class="com.tivoli.RiskManager.Agent.Transports.Senders.rmaEifSender"
        persist="no" >
</destination>
```

キューの管理および制御のパラメーター

rmagent.xml 構成ファイル内で以下のオプション・パラメーターを <destination> エレメントとともに使用すれば、キューの操作と管理を制御することができます。

- **persist**
- **queueMaxSize**

- **queueThresholdSize**
- **queueMessageInterval**
- **errorRoute**

イベントがキューに入れられるときに、キューのサイズと空きディスク・スペース容量が測定されます。キューのサイズが、**queueMaxSize** と **queueThresholdSize** パラメーターで指定されたサイズに近づいた場合、**errorRoute** パラメーターで指定されたイベント・コンソールに RMAgent_QueueProblem イベントが送信されます。**queueMessageInterval** パラメーターは、キュー警告イベントを送信する頻度を制御します。キューに入れるイベントがない場合や、キューがすでにいずれかの待機状態になっている場合、キュー・サイズとディスク・スペースは測定されず、キュー警告イベントも生成されません。

以下は、各パラメーターの説明です。

queueThresholdSize

- このパラメーターは、キューがどの程度のサイズになったらキュー警告イベントをイベント・コンソールに送信するかを指定します。最初のイベントは、この値に最初に達した時に、それ以降のイベントは、**queueMessageInterval** パラメーターで指定された時間間隔ごとに、**errorRoute** パラメーターで指定されたイベント・コンソールに送信されます。
- このパラメーターで指定されたサイズにキューが達しても、そのサブコンポーネントでのイベントの処理が停止することはありません。
- このパラメーターの値には、0～2147483647 の範囲の整数を指定できます。デフォルト値 0 は、サイズ制限がないことを示します。
- キューがこの状態になった場合、その状況は **wrmqueue -l** コマンドで Running(THRESHOLD) と表示されます。

queueMaxSize

- このパラメーターは、キューに入れることができるイベントの最大数を指定します。キュー内のイベント数がこの値に近づくと、キューにイベントを送信しているコンポーネントは処理を停止し、キュー警告イベントがイベント・コンソールに送信されます。最初のイベントは、この値に最初に達した時に、それ以降のイベントは、**queueMessageInterval** パラメーターで指定された時間間隔ごとに、**errorRoute** パラメーターで指定されたイベント・コンソールに送信されます。デフォルトの間隔は 15 分です。
- このパラメーターの値には、0～2147483647 の範囲の整数を指定できます。デフォルト値 0 は、サイズ制限がないことを示します。このパラメーターの値は、**queueThresholdsize** パラメーターの値より大きくなければなりません。
- キューが最大サイズに達した場合、その状況は **wrmqueue -l** コマンドで Waiting(MAX) と表示されます。

queueMessageInterval

- このパラメーターは、次の RMAgent_QueueProblem キュー警告イベントの送信までの時間 (ミリ秒単位) を指定します。このパラメーターを使用して、**queueMaxSize** または **queueThresholdSize** パラメーターで指定されたサイズをキューが超えたときに送信されるキュー警告イベントの数を制限します。
- デフォルト値は 900000 (15 分) です。

errorRoute

- このパラメーターは、**queueMaxSize** または **queueThresholdSize** パラメーターの値を超えたときのキュー警告イベントの送信先のコンポーネント (通常はイベント・コンソール) を指定します。
- キュー警告イベントは、該当するルートの他のすべてのイベントとともにキューに入れられます。このパラメーターを使用して、エラー・ルートに個別の宛先アドレスを定義することで、キュー警告イベントの送信の効率を上げます。これによって、キュー警告イベントの配信がタイムリーに行われるようになります。
- 複数のエラー・ルートを定義することができます。RMAgent_QueueProblem キュー警告イベントは、指定されたすべてのエラー・ルートに送信されます。
- デフォルトのエラー・ルートはありません。このパラメーターを指定しない場合、RMAgent_QueueProblem キュー警告イベントは送信されません。

キューの管理および制御のパラメーターの使用例

このセクションでは、以下のシナリオに基づいたキューの管理および制御の各パラメーターの使用例を示しています。

目的	使用するパラメーター	例
キューに入れるイベント数が 100000 を超えないようにする	queueMaxSize	queueMaxSize = "100000"
キューに入れられたイベント数が 10000 に達した時点で、キュー警告イベントを送信する	queueThresholdSize	queueThresholdSize="10000"
キュー警告イベントを送信する	errorRoute	例については以下を参照
1 分ごとにキュー警告イベントを送信する	queueMessageInterval	queueMessageInterval="60000"

以下の例は、上記の目的で指定したすべてのキュー・パラメーターを示しています。

```
<destination name = "incident_sender_slow" class =
"com.tivoli.RiskManager.Agent.Transports.Senders.rmaEIFSender" queueMaxSize =
"100000" queueThresholdSize="10000" queueMessageInterval="60000">
</destination>

<destination name = "error_route" class =
"com.tivoli.RiskManager.Agent.Transports.Senders.rmaEIFSender" errorRoute="yes">
<set key="RMA_conf" value="c:\IBM\RISKMGR\etc\error_route.conf"/>
</destination>
```

キュー管理イベントの例

このセクションでは、キュー管理イベントの例を示します。部分イベントだけを示していることに注意してください。

- 以下のイベントでは、キューに入れられたイベント数が、**queueThresholdSize** パラメーターで指定された構成済みのキューしきい値サイズに達したかまたはそれを超過したことが通知されます。

  RMAgent_QueueProblem

msg='QueueProblem:Component=db_sender:Reason=The queue threshold size has been exceeded.:currentSize=1001:thresholdSize=1000:maxSize=10000" severity=WARNING

- 以下のイベントでは、キューに入れられたイベント数が、**queueMaxSize** パラメーターで指定された構成済みのキュー最大サイズに近づいたかまたはそれを超過したことが通知されます。

  RMAgent_QueueProblem
  msg='QueueProblem:Component=db_sender:Reason=The queue maximum size has been exceeded.:currentSize=9992:thresholdSize=1000:maxSize=10000" severity=CRITICAL

- 以下のイベントでは、永続キューが使用しているハード・ディスク上に使用可能なスペースがなくなったことが通知されます。

  RMAgent_QueueProblem
  msg='QueueProblem:Component=db_sender:Reason=The disk the queue is using has no more space available.:currentSize=999:thresholdSize=1000:maxSize=10000" severity=CRITICAL

- 以下のイベントでは、キューにエラーが発生し、手動での介入が必要であることが通知されます。

  RMAgent_QueueProblem
  msg='QueueProblem Component=db_sender:Reason=The queue failed for an unknown reason.:currentSize=4567:thresholdSize=1000:maxSize=10000" severity=FATAL

wrmqueue -l コマンドの説明

「*IBM Tivoli Risk Manager コマンド・リファレンス*」の **wrmqueue** コマンドの **-l** オプションの説明は、以下のように変更する必要があります。

l または -list

このオプションは、キューに関する情報をリストで表示します。出力は 3 つのセクションに分けて表示され、以下の情報をこの順序どおりに示します。

1. キューの名前、状況、および定義
2. キュー内のイベントの数
3. 失敗したイベントの数

以下は **wrmqueue -l** の出力例です。

queue name	status	type	persist
summarization	Running	engine	yes
eif_sender1	Waiting(MAX)	sender	yes
eif_sender2	Running(THRESHOLD)	sender	no
eif_sender3	Waiting(DISKFULL)	sender	yes
eif_sender4	Failed	sender	no

queue name	# queued	# processed	#/second
summarization	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender1	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender2	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx

eif_sender3	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx
eif_sender4	xxxxxxxxxx	xxxxxxxxxx	xxxxx.xx

queue name	# failed
summarization	ttttttttttt(rrrrrrrrrr)
eif_sender1	ttttttttttt(rrrrrrrrrr)
eif_sender2	ttttttttttt(rrrrrrrrrr)
eif_sender3	ttttttttttt(rrrrrrrrrr)
eif_sender4	ttttttttttt(rrrrrrrrrr)

以下では、**wrmqueue** コマンドの **-l** オプションによる出力を説明しています。

列見出し	説明
queue name	キューの名前。
status	キュー (コンポーネントではない) の状況。状況は、以下の値の 1 つで示されます。 Running — キューは、問題なく機能しています。 Waiting(MAX) — 構成済みの最大キュー・サイズに達したので、このキューにイベントを送信しているすべてのコンポーネントは待機状態になります。 Running(THRESHOLD) — 構成済みのしきい値キュー・サイズを超えました。 Waiting(DISKFULL) — Tivoli Risk Manager 永続ファイルが保管されているディスクが満杯になったので、スペースが使用可能になるまでエージェントは待機します。 Failed — キューでエラーが発生しました。この問題の解決方法については、「*Tivoli Risk Manager 問題判別ガイド*」を参照してください。
type	このキューからイベントを読み取るコンポーネントの以下のタイプ。 • engine • sender
persist	イベントをメモリーに保管するか、またはハード・ディスクに保管するかを示します。
# queued	コンポーネントで処理するために入手できるイベントの数。
# processed	エージェントが最後に開始されて以降、正常に処理されたイベントの数。
#/second	最後に **wrmqueue -l** コマンドが実行されて以降、または **wrmqueue -l** コマンドが初めて実行された場合はエージェントの再始動以降の、秒あたりの処理されたイベント数。
# failed	*ttttttttt* は、エージェントの最後の開始以降にコンポーネントが処理できなかったイベントの合計数です。 *rrrrrrrrr* は、エージェントの再始動時に再試行される、失敗したキューの数です。

5.3 メッセージおよびトレース・ロギング

このセクションでは、新規の First Failure Data Capture (FFDC) 機能について、および「*IBM Tivoli Risk Manager 問題判別ガイド*」の中の第 2 章『メッセージ・ロギング、トレース・ロギングおよびその他の診断ツール』に加えられた他の変更点について記載しています。

トレース・ロギング

Tivoli Risk Manager 製品には、3 つのレベルのトレース明細が備えられています。デフォルトのレベルは、最下レベルの明細である DEBUG_MIN です。このレベルでは、エラー条件のみがトレースされます。続く 2 つのレベルは DEBUG_MID と DEBUG_MAX で、これらはさらに詳細な情報を提供します。これらのレベルは、ロギング構成ファイル内のパラメーターを変更するか、またはロギング・コマンド行インターフェースを呼び出すことによって変更できます。現在のところ、トレース・ログ・データは英語でしか利用できません。

デフォルトでは、メモリー・バッファーがすべてのトレース情報の保管に使用されます。これにより、システム・パフォーマンスに対するトレースの影響が最小限になります。このバッファーがディスクにフラッシュされるのは、例外の発生時のみです。トレース・ロギングをディスクに直接書き込むように構成して、例外の未発生時にトレース・データを保管することもできます。トレース・ロギングの構成方法の例は、『Tivoli Risk Manager エージェントおよびイベント・モニター・トレースのカスタマイズ』のセクションを参照してください。

トレース・ログは、以下のファイルとディレクトリーに置かれます。

- Linux および UNIX システム上の Tivoli Risk Manager C プログラムのトレース・ログは、/usr/ibm/tivoli/common/HRM/logs/<*application*>.error.log に置かれます。変数 <*application*> には、アプリケーションの名前を指定します。
- Windows システム上の Tivoli Risk Manager C プログラムのトレース・ログは、C:\Program Files\ibm\tivoli\common\HRM\logs\<*application*>.error.log に置かれます。変数 <*application*> には、アプリケーションの名前を指定します。
- Linux および UNIX システム用の Tivoli Risk Manager エージェント・コンポーネントのトレース・ログは、/usr/ibm/tivoli/common/HRM/logs/traceHRM*n*.log に置かれます。
- Windows システム用の Tivoli Risk Manager エージェント・コンポーネントのトレース・ログは、C:\Program Files\ibm\tivoli\common\HRM\logs\traceHRM*n*.log に置かれます。
- Tivoli Risk Manager データベース・ユーティリティーの wrmdbclose と wrmdbclear は、トレース・レコードを、それぞれ traceHRM_DBClose.log と traceHRM_DBClear.log の別個のファイルに書き込みます。

Tivoli Risk Manager のエージェントとイベント・モニターのトレース・レコードは、traceHRM*n*.log (*n* は番号) という通し番号付きファイルに書き込まれます。トレース・ロガーは、それぞれ 1 MB のサイズの最大 5 つのファイルに書き込みます。5 MB に収まらないトレース・レコードが書き込まれる場合、トレース・ファイルは折り返します。ロガー構成ファイルを使用すれば、これらのトレース・ファイルの制限事項はいずれもカスタマイズできます。トレース・ファイルの数を変更するには、**file.trace.maxFiles** パラメーターを使用します。各トレース・ファイルの最大サイズを変更するには、**file.trace.maxFileSize** パラメーターを使用します。

たいていのログ・メッセージは、メッセージ・ログとトレース・ログの両方に書き込まれます。すべてのメッセージを必ずトレース・ログに書き込むには、以下のように、メッセージ・ロガーの listenerNames をトレース・ファイルに追加します。

```
rmLogger.msg.listenerNames=file.message file.trace
```

First Failure Data Capture

First Failure Data Capture (FFDC) は、エラー条件の発生時のトレース情報のスナップショットです。トレース・ロギング構成をカスタマイズすれば、すべてのエラーまたは選択したエラーのトレース・スナップショットをとることができます。各スナップショットごとに固有のトレース・ファイルが作成され、これは後続のトレース・スナップショットによって上書きされることはありません。デフォルトでは、FFDC は Tivoli Risk Manager 製品では非アクティブです。アクティブにするには、トレース・ロギング構成を変更します。構成の変更の詳細については、『Tivoli Risk Manager エージェントおよびイベント・モニター・トレースのカスタマイズ』のセクションを参照してください。FFDC スナップショットは、Tivoli Risk Manager エージェントとイベント・モニターでのみ利用できます。

FFDC ログは、以下のファイルとディレクトリーに置かれています。

UNIX システムの場合: /usr/ibm/tivoli/common/HRM/FFDC/*YYYY.MM.DD*/traceHRM*n*.log

Windows システムの場合: C:\Program Files\ibm\tivoli\common\HRM\FFDC*YYYY.MM.DD*\traceHRM*n*.log

変数 *YYYY.MM.DD* はスナップショットがとられた日付、*n* は特定の日のスナップショットの順序を示す番号です。

ログ XML

以下のメッセージおよびトレースのログ・レコードの列は、Tivoli Risk Manager 製品によって使用されます。

Time	Millis	Server
ServerFormat	ProductID	Component
LogText	SourceFile	SourceMethod
Thread	Exception	MessageId
TraceLevel	Severity	

例

以下の照会では、メッセージ・ログ・ファイルの内容を ASCII で表示します。

```
viewer.sh -sascii /usr/ibm/tivoli/common/HRM/logs/msgHRM.log
```

以下の照会では、HTML のトレース・ログ・ファイルの内容を外部ファイルに書き込みます。

```
viewer.sh  /usr/ibm/tivoli/common/HRM/logs/traceHRM*.log > trace_logs.html
```

以下の照会では、HTML フォーマットのトレース・ログ・ファイルの選択した列を、外部ファイルに書き込みます。

```
viewer.sh -q “select
Time,Component,Thread,SourceFile,SourceMethod,LogText,EXCEPTION where true”
/usr/ibm/tivoli/common/HRM/logs/traceHRM*.log > trace_logs.html
```

以下の照会では、HTML フォーマットのメッセージ・ログ・ファイルの選択したエラー・メッセージの列を、外部ファイルに書き込みます。

```
viewer.sh -q “select
Time,MessageId,LogText,Component,Thread,SourceFile,SourceMethod where Severity
= ‘ERROR’”  /usr/ibm/tivoli/common/HRM/logs/msgHRM.log > error_log.html
```

Tivoli Risk Manager エージェントおよびイベント・モニター・トレースのカスタマイズ

Tivoli Risk Manager エージェントのトレース・ロギングは、$RMADHOME/etc/RMLogger.properties トレース・ロギング構成ファイル内のパラメーターで制御します。たとえば、**rmLogger.trc.level** パラメーターは、エージェントの実行中に収集されるトレース情報の量を制御します。**rmLogger.trc.listenerNames** パラメーターは、トレース情報をメモリーまたはディスク上のファイル

のどちらに書き込むかを制御します。エージェントが実行するトレース・ロギングの量を増やすには、通常はこの 2 つのパラメーターを両方とも変更して、取り込む情報量を増やし、情報をその作成時にディスクに書き込むようにする必要があります。

トレース構成に変更を加えるには、以下の 2 つの方法があります。

- RMLogger.properties ファイル内のパラメーター値を変更し、エージェントを再始動して、永続的に変更する

  たとえば、エージェント・トレース・ロギングを永続的に増やすには、以下の手順を実行します。

  1. $RMADHOME/etc/RMLogger.properties ファイルを編集して、以下のパラメーターを変更します。
     ```
     rmLogger.trc.level=DEBUG_MAX
     rmLogger.trc.listenerNames=file.trace
     ```
  2. エージェントを再始動します。

- ロギング・コマンド行インターフェースを使用してパラメーター値を変更し、一時的に変更する (『ロギング・コマンド行インターフェース』のセクションを参照) この方法で変更を加える場合は、エージェントが実行中でなければならず、有効なのはそのエージェントが実行している間のみです。

  たとえば、エージェントの実行中にエージェント・トレース・ロギングを一時的に増やすには、以下の手順を実行します。

  1. $RMADHOME/logviewer ディレクトリーに移動します。
  2. このディレクトリーから以下のコマンドを入力します。
     ```
     logcmd set rmLogger.trc level=DEBUG_MAX
     logcmd set rmLogger.trc listenerNames=file.trace
     ```

ログ記録される情報が増えるにつれて、トレース・ログは大きくなります。トレース・ファイルの最大数に達した後は、古い方のトレース・ファイルから順に新しいデータが上書きされます。デフォルトのトレースの構成は、それぞれが 1 MB の 5 つのトレース・ファイルです。トレース・ファイルの容量をそれぞれが 2 MB の 10 個のファイルに増やすには、以下のコマンドを実行します。

```
logcmd set file.trace maxFiles=10
logcmd set file.trace maxFileSize=2048
```

上記の設定は、エージェントの実行中のみ有効です。エージェントを停止してから再始動すると、この設定は元のデフォルト設定に戻ります。エージェントの実行中にエージェント・トレース・ロギングを減らすには、以下のコマンドを実行します。

```
logcmd set rmLogger.trc level=DEBUG_MIN
logcmd set rmLogger.trc listenerNames=memory
```

First Failure Data Capture (FFDC) スナップショットを使用可能にするには、トレース構成を以下のようにカスタマイズします。

```
rmLogger.trc.listenerNames=snap.memory
rmLogger.msg.listenerNames=file.message ffdc.snap
```

これらの構成のどの変更も、イベント・モニターを含め、Tivoli Risk Manager エージェントのすべてのコンポーネントに影響を与えます。イベント・モニターの構成を、他のエージェントとは異なるものにしたい場合、構成ファイルまたはコマンド行インターフェースで rmLogger.trc の代わりに

rmLogger.trc.monitor を使用します。たとえば、イベント・モニターのトレース・ロギングを中間レベルに設定し、別個のファイルに書き込むには、パラメーターを以下のように設定します。

```
rmLogger.trc.monitor.level=DEBUG_MID
rmLogger.trc.monitor.listenerNames=file.trace.monitor
file.trace.monitor.fileName=trace_monitor.log
```

構成内で定義されているすべてのトレース・ロガーのリストを表示するには、以下のコマンドを実行します。

```
logcmd list rmLogger.trc
```

トレース・ロガーの現在の設定のリストを表示するには、以下のコマンドを実行します。

```
logcmd config rmLogger.trc
```

イベント・モニターのトレース・ロガーの現在の設定のリストを表示するには、以下のコマンドを実行します。

```
logcmd config rmLogger.trc.monitor
```

5.4 正規表現のサポート

このセクションでは、APAR IY53527 の正規表現のサポートに加えられた拡張機能について説明します。正規表現の使用に関する以下の情報を、「*IBM Tivoli Risk Manager 管理者ガイド*」に追加する必要があります。

正規表現のサポート

IBM Tivoli Risk Manager バージョン 4.2 では、以下の新機能が、Tivoli Risk Manager 製品への正規表現サポートの導入に依存するイベント・モニターに追加されています。

- プレフィルター
- 索引
- イベント・パターンを指定する拡張機能

この新機能によって全体的なパフォーマンスが向上し、フォーマット・ファイルの作成が簡単になります。前のリリースで備えられていた単純なワイルドカード・トークンに加えて、フォーマット・ファイル内のイベント・パターンを正規表現で表すことができます。

これらの新機能をインプリメントするには、Xerces の正規表現ライブラリーを使用します。Xerces 正規表現マッチング・エンジンは、従来の (非 POSIX) 非決定性有限オートマトン (NFA) 正規表現エンジンのインプリメンテーションです。このライブラリーは、以下の、サポートされている正規表現構成の大半をサポートします。

構成	記号	説明	例	結果
シンプル文字クラス	[ ]	基本形式の文字クラス (または文字セット) この構成を使って、複数の文字のうちの 1 つだけを突き合わせます。	gr[ae]y	gray または grey に一致する
否定文字クラス	[^]	リストに記載された文字以外のすべての文字に突き合わせます。 左大括弧の後に脱字記号 (^) を入力すると、文字クラスが否定されます。	gr[^ae]y	gray または grey のどちらも一致しない
反復文字	? * +	先行トークンにゼロまたは 1 回突き合わせます。 先行トークンにゼロ回以上突き合わせます。		

		先行トークンに 1 回以上突き合わせます。		
省略文字	\d \D \s \S \w \W	任意の数字と突き合わせます。 任意の非数字と突き合わせます。 任意の空白文字と突き合わせます。 任意の非空白文字と突き合わせます。 任意のワード文字と突き合わせます。 任意の非ワード文字と突き合わせます。		
ドット	[.]	ほぼすべての文字に突き合わせます。この構成を使用する際は注意してください。ドット (ピリオド) は、最もよく使われるメタキャラクターの 1 つであるとともに、最もよく誤用されるメタキャラクターです。		
アンカー	^ $	文字の一致ではなく、位置を示すのに使用します。これは、文字の前、後、または文字間の位置に突き合わせられ、特定の位置の正規表現突き合わせを固定するために使われます。 行の先頭を示します。 行の末尾を示します。		
ワード境界	\b \B \w \W	ワード境界を示します。 ワード単位での突き合わせに使われます。 \b の否定バージョン。 非ワード文字の突き合わせに使われます。 \w の否定バージョン。	\b(is|art)\b	ワード is または ワード art のどちらかに一致する
範囲	[-]	値の範囲の指定に使用します。 文字クラス内の複数の範囲、または範囲とシングル文字の組み合せも指定できることに注意してください。	[0-9] [0-9a-fxA-FX]	0～9 の 1 つの数字に一致する 16 進数の数字または文字 X に一致する
数量詞	{}	表現をさらに定量化するには、数量詞を使います。 ?、*、および + も定量詞です。	{n} {n,} {n,m}	正確に *n* 回一致する 最低 *n* 回一致する 最低 *n* 回、最高 *m* 回の範囲内で一致する
先読み	(?=) (?!)	次に続く文字に突き合わせます。	q(?=u) q(?!u)	後に u が続く q に一致する 後に u が続かない q に一致する
後読み	(?<=)	先行する文字に突き合わせます。	(?<=a)b (?<!a)b	前に文字 a が先行する文字 b に一致する 前に文字 a が先行していない文字 b に一致する
グループ化代替	(a|e) gr[ae]y	複数の表現候補内の 1 つの正規表現に突き合わせます。 表現の先頭または末尾に '(' および ')' が指定	gr(a|e)y gr[ae]y (gray|grey)	gray または grey に一致する

		されていると、突き合わせは正しく実施されないことに注意してください。 これは Xerces ライブラリーの問題が原因です。		

以下の表は、サポートされていない構成と、その代わりに使用できる構成をリストしています。

構成	説明	代替構成
結合	複数の別個の文字クラスで構成される、単一文字クラスを指定します。結合の例としてたとえば [0-4[6-8]] では、5 を除く 0〜8 の任意の数字と一致します。	[0-46-8] と指定すると、大括弧のネストを避けて、同じ結果を実現できます。
交点	共通するすべてのものと突き合わせる単一文字クラスを指定します。交点の例としてたとえば [0-4&&[4678]] では、数字の 4 が一致します。交点は結合に似ており、類似の状況下で使われます。	結合で指定されているのと同じ代替構成を使用します。
減法	共通するもの以外のすべてと突き合わせる単一文字クラスを指定します。減法は、基本的に交点の否定です。減法の例としてたとえば [0-9&&[^345]] では、3、4、および 5 を除く 0〜9 の数字に一致します。	表現を肯定形式で指定します。例: [0-26-9]

6 追加または置換されるファイル

このセクションでは、この Fix Pack の新規および変更済みのファイルをリストしています。
RMADHOME は、RMADHOME 環境変数で参照される Tivoli Risk Manager のインストール・ディレクトリーです。

/etc/init.d/rc.rmagent (Solaris および Linux)
/etc/rc.rmagent (AIX)
/etc/Tivoli/rma_eif_env.sh (SUSE Linux バージョン 8 以上では LD_ASSUME_KERNEL を削除)
RMADHOME /bin/rma_webids-init (UNIX または Linux のみ)
RMADHOME/bin/RMCAH040201.sys (HPUX のみ)
RMADHOME/bin/RMCAL040201.sys (Linux のみ)
RMADHOME/bin/RMCAS040201.sys (Solaris のみ)
RMADHOME/bin/RMCAW040201.sys (Windows のみ)
RMADHOME/bin/RMCAX040201.sys (AIX のみ)
RMADHOME/bin/rmEventLog.dll (Windows のみ)
RMADHOME/bin/webids[.bat]
RMADHOME/bin/wrmadmin[.exe]
RMADHOME/bin/wrmdns (Windows と Solaris を除くすべて)
RMADHOME/bin/wrmqueue (Windows と Solaris を除くすべて)
RMADHOME/dbschema/rm_t_arc41_uc.ms.sql
RMADHOME/etc/incident_engine.conf
RMADHOME/etc/rmagent.dtd
RMADHOME/etc/rmclasspath.conf
RMADHOME/etc/RMLogger.properties
RMADHOME/etc/summary_engine.conf
RMADHOME/etc/tec/rules/riskmanager.wic
RMADHOME/etc/templates/baroc/rmagent.baroc
RMADHOME/etc/templates/incident_engine.conf
RMADHOME/etc/templates/rmagent.dtd
RMADHOME/etc/templates/rmclasspath.conf
RMADHOME/etc/templates/RMLogger.properties
RMADHOME/etc/templates/summary_engine.conf
RMADHOME/etc/templates/tec/rules/riskmgr_config.pro
RMADHOME/etc/templates/tec/rules/riskmanager.wic
RMADHOME/etc/templates/tec/rules/riskmgr_config.pro
RMADHOME/etc/tec/rules/riskmanager.wic
RMADHOME/lib/eif.jar
RMADHOME/lib/evd.jar
RMADHOME/lib/jffdc.jar
RMADHOME/lib/jlog.jar
RMADHOME/lib/rm_dbaccess.jar
RMADHOME/lib/rm_dbutil.jar
RMADHOME/lib/rm_util.jar
RMADHOME/lib/rmagent_msg.properties
RMADHOME/lib/rmagent.jar
RMADHOME/lib/rmeventmonitor.jar
RMADHOME/lib/rmsvrcfg.jar
RMADHOME/logviewer/logcmd.sh (UNIX または Linux のみ)
RMADHOME/logviewer/logcmd.bat (Windows のみ)
RMADHOME/msg_cat/C/rmeif.cat
RMADHOME/nids/templates/rules/www.rules
RMADHOME/reports/rm_ra_03.rpt (Windows のみ)
\Program Files/ibm/tivoli/common/HRM/scripts/getpd.bat (Windows のみ)
\Program Files/ibm/tivoli/common/HRM/scripts/getpdinfo.bat (Windows のみ)
/sbin/init.d/rc.rmagent (HP)
/usr/ibm/tivoli/common/HRM/scripts/getpdinfo (UNIX または Linux のみ)

7 ソフトウェア・サポートへのお問い合わせ

Tivoli 製品で問題が発生した場合は、以下の IBM ソフトウェア・サポート Web サイトをご覧ください。
http://www.ibm.com/software/sysmgmt/products/support/

ソフトウェア・サポートに連絡する場合は、以下の Web サイトの「IBM Software Support Guide」をご覧ください。

http://techsupport.services.ibm.com/guides/handbook.html

このガイドは、問題の重大度に応じた IBM ソフトウェア・サポートへの連絡方法と、以下の情報を記載しています。

- 登録および資格
- ユーザーの所在地に応じた電話番号および E メール・アドレス
- IBM ソフトウェア・サポートへの連絡の前にユーザーが準備する必要がある情報

8 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、または サービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の 製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの 評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について 実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、 商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示 もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が 禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、 改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、 便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものでは ありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部では ありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、 自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム（本プログラムを含む）との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用すること ができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他の ライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で 決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行

われた可能性がありますが、 その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、 もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、 他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、 予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、 あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、 名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでの プログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・ プラットフォームのアプリケーション・プログラミング・インターフェースに 準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、 いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、 配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性が あることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠した アプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は 表示されない場合があります。

商標

以下は、IBM Corporation の商標です。

IBM、IBM ロゴ、Tivoli、Tivoli ロゴ、AIX、DB2、Tivoli Enterprise Console、TME、pSeries、および zSeries は、IBM Corporation の商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、および Windows は、Microsoft Corporation の米国およびその他の国における商標です。

UNIX は、The Open Group の米国およびその他の国における登録商標です。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

Printed in Japan.