IBM Security QRadar Incident Forensics

バージョン 7.3.0

インストール・ガイド

注記

本書および本書で紹介する製品をご使用になる前に、 37 ページの『特記事項』に記載されている情報をお読みください。

本書は、本書の更新版に置き換えられない限り、IBM QRadar Security Intelligence Platform V7.3.0 および以降のリリースに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Security QRadar Incident Forensics
Version 7.3.0
Installation Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

IBM Security QRadar Incident Forensics のインストールの概要 v

第 1 章 QRadar Incident Forensics のアップグレード 1

第 2 章 QRadar Incident Forensics コンポーネントのインストール 3

第 3 章 QRadar Incident Forensics のインストールの概要 7
アクティベーション・キーおよびライセンス・キー 8
QRadar インストールの前提条件ハードウェア・アクセサリーおよびデスクトップ・ソフトウェア 8

第 4 章 ユーザーのアプライアンスへの QRadar Incident Forensics ソフトウェアのインストール 11
ユーザーのアプライアンスへの QRadar Incident Forensics のインストールの前提条件 11
ユーザーのアプライアンスへの QRadar インストール済み環境に対する Linux オペレーティング・システムのパーティション・プロパティー 12
ユーザーのアプライアンスへの RHEL のインストール 13

第 5 章 QRadar Incident Forensics アプライアンスへの QRadar Incident Forensics ソフトウェアのインストール 15

第 6 章 QRadar Incident Forensics の仮想アプライアンスへのインストール 17
仮想マシンの作成 18
仮想マシンでの QRadar Incident Forensics ソフトウェアのインストール 19

第 7 章 QRadar コンソールのインストール 21

第 8 章 QRadar Incident Forensics のインストール 23

第 9 章 QRadar Incident Forensics 管理対象ホストを QRadar コンソールに追加する . . 27
QRadar Incident Forensics 管理対象ホストの削除 28

第 10 章 パケット・キャプチャー・デバイスと QRadar Incident Forensics の間の接続 29
アプライアンスへの QRadar Packet Capture ソフトウェアのインストール 31
QRadar Incident Forensics ホストへのパケット・キャプチャー・デバイスの追加 34

特記事項 37
商標 38
製品資料に関するご使用条件 39
IBM オンラインでのプライバシー・ステートメント 40

IBM Security QRadar Incident Forensics のインストールの概要

IBM® Security QRadar® Incident Forensics のインストールおよび IBM Security QRadar との統合に関する情報。QRadar Incident Forensics アプライアンスには、プリインストールされたソフトウェアと Red Hat Enterprise Linux オペレーティング・システムが組み込まれています。ユーザーのハードウェアに QRadar Incident Forensics ソフトウェアをインストールすることもできます。

対象読者

QRadar Incident Forensics システムのインストールおよび構成を担当するネットワーク管理者。

管理者には、ネットワークおよび Linux オペレーティング・システムの実用的な知識が必要です。

技術文書

IBM Security QRadar の製品資料 (すべての翻訳資料を含む) を Web 上で探すには、IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリー内の技術資料にアクセスする方法については、Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) を参照してください。

お客様サポートへのお問い合わせ

お客様サポートへのお問い合わせ方法については、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業の内部と外部からの不正なアクセスの防止、検出、対応により、システムと情報を保護する必要があります。不正なアクセスにより、情報の改ざん、破壊、盗用、悪用が発生したり、使用しているシステムの損傷や、他のシステムに対する攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法かつ包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

注意**:**

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポリシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

注記

IBM Security QRadar Incident Forensics は、企業によるセキュリティー環境とデータの改善の支援を目的として設計されています。具体的には、IBM Security QRadar Incident Forensics は、企業がネットワーク・セキュリティー・インシデントで何が起きたのかを調査およびより詳細に把握できるように設計されています。本ツールを使用することにより、企業は収集済みのネットワーク・パケット・データ (PCAP) に索引を付けて検索することができ、また本ツールにはそのようなデータを元の形式に再構成する機能が組み込まれています。この再構成機能により、電子メール・メッセージを含むデータおよびファイル、添付ファイルおよび添付画像、VoIP 電話通話、ならびに Web サイトを再構成することができます。本プログラムの機能および構成方法に関する追加情報が、本プログラムに付属するマニュアルおよびその他の資料に記載されています。本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar Incident Forensics は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポリシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar Incident Forensics の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

第 1 章 QRadar Incident Forensics のアップグレード

デプロイメント環境内の IBM Security QRadar 製品をすべて同じバージョンにアップグレードする必要があります。アップグレード・インストーラーを使用して、IBM Security QRadar Incident Forensics V7.2.8 を V7.3.0 にアップグレードします。

データを維持したまま、QRadar Incident Forensics V7.2.4 以前のバージョンからアップグレードする場合は、IBM 営業担当員にお問い合わせください。または、QRadar Incident Forensics V7.2.4 以前のバージョンからアップグレードするが、データを維持する必要がない場合は、新規インストールで V7.3.0 に直接アップグレードしてください。

制約事項**:** 論理ボリューム・マネージャー (LVM) を使用した論理ボリュームのサイズ変更はサポートされていません。

手順

1. <*QRadar_patchupdate*>*.sfs* ファイルを IBM Fix Central (www.ibm.com/support/fixcentral) からダウンロードします。
2. SSH を使用して、root ユーザーとしてシステムにログインします。
3. パッチ・ファイルを、/tmp ディレクトリーまたは十分なディスク・スペースがある別の場所にコピーします。
4. /media/updates ディレクトリーを作成するために、以下のコマンドを入力します。

   ```
   mkdir -p /media/updates
   ```
5. パッチ・ファイルをコピーしたディレクトリーに移動します。
6. パッチ・ファイルを /media/updates ディレクトリーにマウントするために、以下のコマンドを入力します。

   ```
   mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates/
   ```
7. 以下のコマンドを入力して、アップグレード・インストーラーを実行します。

   ```
   /media/updates/installer
   ```

   パッチ・インストーラー・スクリプトの初回実行時は、パッチ・インストーラー・メニューが表示されるまで遅延が生じることがあります。
8. デプロイメント環境に応じて、インストール前の質問に回答してください。
9. アップグレード・インストーラーを使用して、デプロイメント環境内のすべてのホストをアップグレードします。

   「すべてにパッチを適用 **(Patch All)**」を選択していない場合、以下の順序でシステムをアップグレードする必要があります。
   - QRadar コンソール
   - QRadar Incident Forensics

アップグレードの実行中に SSH セッションが切断された場合でも、アップグレードは続行します。SSH セッションを再オープンし、インストーラーを再実行すると、インストールが再開します。

10. アップグレードの完了後に、以下のコマンドを使用して、ソフトウェア更新をアンマウントします。 **umount /media/updates**

次のタスク

パケット・キャプチャー・デバイスをアップグレードします。詳しくは、「*IBM Security QRadar Packet Capture* クイック・リファレンス・ガイド」を参照してください。

第 2 章 QRadar Incident Forensics コンポーネントのインストール

QRadar Incident Forensics は、IBM QRadar Security Intelligence Platform のスケーラブルなアーキテクチャーに統合されます。要件に応じて、IBM Security QRadar Incident Forensics のコンポーネントを 1 つのアプライアンスにインストールすることも (オールインワン)、複数のアプライアンスにインストールすることもできます。

インストール・オプション

インストールするコンポーネントによっては、一部のセキュリティー機能が使用できない場合があります。例えば、QRadar Incident Forensics を 1 つのアプライアンスにインストールした場合、ネットワーク Forensics 機能だけが使用可能になります。ただし、QRadar Incident Forensics 管理対象ホストをインストールした場合は、より多くのセキュリティー機能が使用可能になります。ほとんどのインストールの場合、1 つの QRadar コンソール、1 つ以上の QRadar Incident Forensics Processor、1 つ以上の QRadar Packet Capture アプライアンスをインストールします。

以下の図は、各種のセキュリティー機能と、IBM QRadar Security Intelligence Platform のアーキテクチャー・フレームワークの概要を示しています。

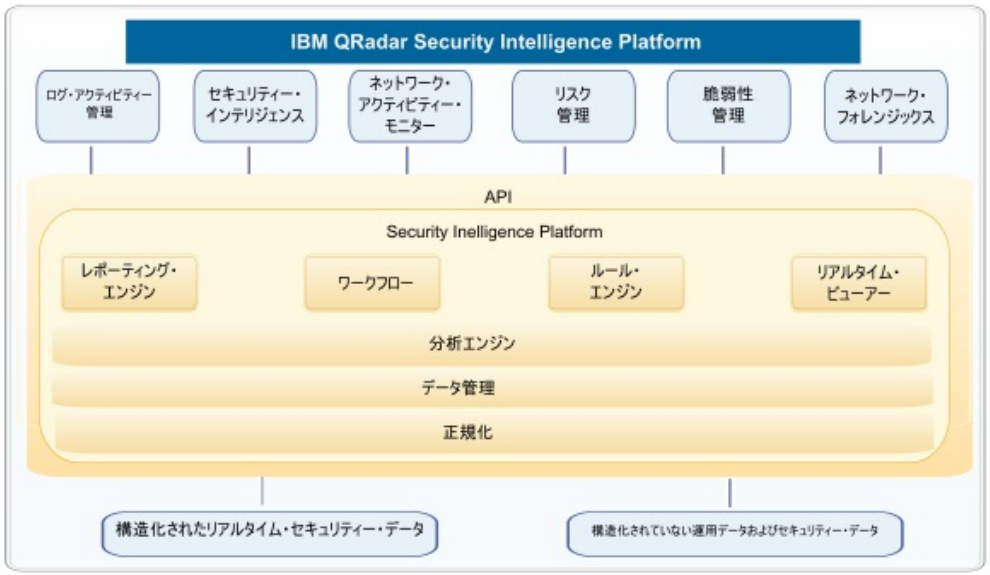


図 *1. QRadar Security Intelligence* アーキテクチャーの概要

オールインワン・デプロイメント

スタンドアロン・デプロイメントとオールインワン・デプロイメントでは、IBM Security QRadar Incident Forensics Standalone ソフトウェアをインストールします。これらの単一アプライアンス・デプロイメント環境は、1 つのアプライアンス

に QRadar コンソールと QRadar Incident Forensics 管理対象ホストをインストールする環境に似ていますが、ログ管理機能やネットワーク・アクティビティー・モニター機能などの Security Intelligence 機能を使用できない点が異なります。スタンドアロンのネットワーク Forensics ソリューションの場合、小規模から中規模のデプロイメント環境に QRadar Incident Forensics Standalone をインストールします。

以下の図のように、QRadar Packet Capture アプライアンスを IBM Security QRadar Incident Forensics Standalone に接続することができます。

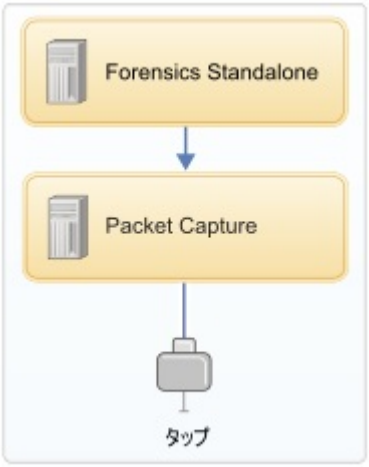


図 2. *IBM Security QRadar Incident Forensics Standalone* デプロイメント環境の例

制約事項: 管理対象ホストを QRadar Incident Forensics Standalone に追加することも、QRadar Incident Forensics Standalone を QRadar コンソールに接続することもできません。

分散デプロイメント

ネットワーク Forensics 分析機能とそれ以外の Security Intelligence 機能の両方が必要になるデプロイメント環境の場合、または Forensics リカバリーのワークロードを分散する必要がある場合は、QRadar コンソール と、1 つ以上の QRadar Incident Forensics 管理対象ホストをインストールします。 QRadar コンソールは、Security Information and Event Management (SIEM) 機能、ログ管理機能、アノマリ検出機能、リスク管理機能、脆弱性管理機能を提供します。

分散デプロイメント環境では、以下の 3 つのアプライアンスを使用します。

- QRadar コンソール
- QRadar Incident Forensics 管理対象ホスト (QRadar Incident Forensics Processor)
- QRadar Packet Capture (オプション)

デプロイメント環境内の IBM Security QRadar アプライアンスすべてのソフトウェア・バージョンとフィックス・レベルが一致している必要があります。デプロイメント環境内で異なるバージョンのソフトウェアの使用はサポートされていません。

以下の図は、複数の QRadar Incident Forensics 管理対象ホストを QRadar コンソールに接続できることを示しています。QRadar Packet Capture デバイスを QRadar Incident Forensics 管理対象ホスト (QRadar Incident Forensics Processor) に接続することができます。

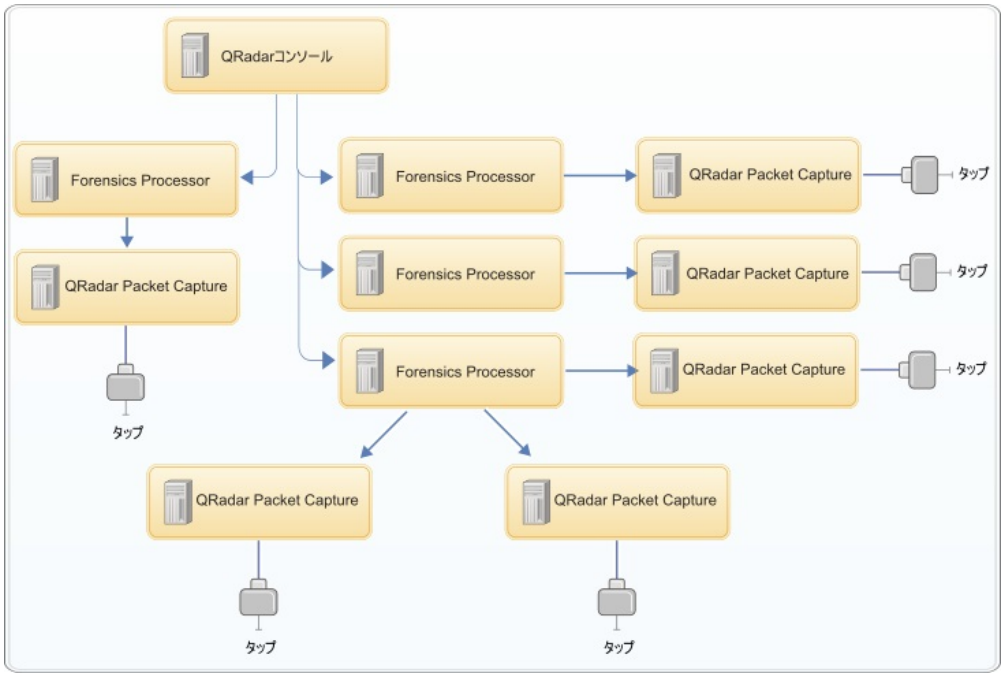


図 3. 分散デプロイメントの例

QRadar Incident Forensics コンポーネント

QRadar デプロイメントには、以下のコンポーネントを組み込むことができます。

QRadar コンソール

QRadar 製品のユーザー・インターフェースを提供します。インターフェースからリアルタイムのイベント・ビューとフロー・ビュー、レポート、オフェンス、アセット情報、管理機能が提供されます。

分散デプロイメント環境では、QRadar コンソールを使用して、複数の QRadar Incident Forensics Processor ホストを管理します。

QRadar Incident Forensics Processor

QRadar Incident Forensics 製品のインターフェースを提供します。このインターフェースは、サイバー犯罪者の動作をステップごとに再トレースするツール、セキュリティー・インシデントに関する未加工のネットワーク・データを再構成するツール、構造化されていない使用可能データを検索するツール、セッションとイベントを視覚的に再構成するツールを提供します。

Security Intelligence Forensics 機能を使用するには、最初に QRadar Incident Forensics Processor を管理対象ホストとして追加する必要があります。

QRadar Incident Forensics Standalone

QRadar Incident Forensics 製品のユーザー・インターフェースを提供します。QRadar Incident Forensics Standalone をインストールすると、

Forensics 調査を行うために必要な各種ツールを使用できるようになります。使用できるのは、Forensics 調査機能とそれに関連する管理機能だけです。

QRadar Packet Capture

オプションの QRadar Packet Capture アプライアンスをインストールすることができます。他のネットワーク・パケット・キャプチャー (PCAP) デバイスがデプロイされていない場合、このアプライアンスを使用して、QRadar Incident Forensics で使用されるデータを保管することができます。このアプライアンスをネットワーク・タップまたはサブネットワークとして必要な数だけインストールして、未加工のパケット・データを収集することができます。

パケット・キャプチャー・デバイスが接続されていない場合は、ユーザー・インターフェースまたは FTP を使用してパケット・キャプチャー・ファイルを手動でアップロードできます。

第 3 章 QRadar Incident Forensics のインストールの概要

所有するアプライアンスまたは仮想アプライアンスに QRadar Incident Forensics ソフトウェアをインストールします。QRadar Incident Forensics アプライアンスには、QRadar Incident Forensics ソフトウェアがインストールされています。

QRadar Incident Forensics は Red Hat Enterprise Linux オペレーティング・システム上にインストールする必要があります。

アプライアンス ID の選択

ほとんどの QRadar Incident Forensics では、少なくとも次の 2 つの ISO イメージをインストールします。

- QRadar コンソール

  QRadar 製品では、同じインストール・ソフトウェア・イメージを使用します。アクティベーション・キー により、アプライアンスのタイプおよびインストールするコンポーネントが決定されます。アクティベーション・キーを入力すると、アプライアンスのタイプを特定するように求めるプロンプトが出されます。QRadar コンソールをインストールする必要があります。
- 6000 QRadar Incident Forensics Processor (管理対象ホスト)

  輸出の管理のため、QRadar Incident Forensics コンポーネントは異なる ISO イメージからインストールされます。QRadar Incident Forensics 管理対象ホストをインストールし、これを QRadar コンソールに接続するように構成する必要があります。

オールインワン・インストールの場合、6100 QRadar Incident Forensics ISO イメージのみインストールして、QRadar Incident Forensics Standalone コンポーネントを選択します。

QRadar Incident Forensics のインストール時に、デフォルトのライセンス・キーにより、5 週間のアクセス権限が付与されます。デフォルトのライセンスの有効期限が切れる前に、ライセンス・キーをシステムに割り振る必要があります。

インストール手順

分散インストールの場合、以下のステップを参考にして、インストール・プロセスを実行してください。

1. ハードウェア要件およびソフトウェア要件を確認します。
2. QRadar コンソール・ソフトウェアをインストールします。
3. QRadar Incident Forensics 管理対象ホストをインストールします。
4. QRadar Incident Forensics 管理対象ホストをデプロイします。
5. パケット・キャプチャー・デバイスを追加します。

アクティベーション・キーおよびライセンス・キー

IBM Security QRadar アプライアンスをインストールするときには、アクティベーション・キーを入力する必要があります。インストール後に、ライセンス・キーを適用する必要があります。インストール・プロセスで誤ったキーを入力しないようにするには、これらのキーの違いを理解しておくことが重要です。

アクティベーション・キー

アクティベーション・キーは、IBM から受け取る、4 つの部分に区切られた 24 桁の英数字ストリングです。すべての QRadar 製品のインストールでは同じソフトウェアを使用します。ただし、アクティベーション・キーによって、各アプライアンス・タイプに適用されるソフトウェア・モジュールが指定されます。例えば IBM Security QRadar QFlow Collector のアクティベーション・キーを使用して QRadar QFlow Collector モジュールのみをインストールします。

アクティベーション・キーは以下の場所から入手できます。

- QRadar ソフトウェアがプリインストールされているアプライアンスを購入した場合、アクティベーション・キーは同梱されている CD 上の文書に記載されています。
- QRadar ソフトウェアまたは仮想アプライアンスのダウンロード版を購入した場合、「始めに *(Getting Started)*」文書にアクティベーション・キーのリストが記載されています。「始めに *(Getting Started)*」は確認 E メールに添付されています。

ライセンス・キー

ご使用のシステムには、QRadar ソフトウェアに 5 週間アクセスできる一時ライセンス・キーが含まれています。ソフトウェアのインストール後、デフォルトのライセンス・キーが有効期限切れになるまでの間に、購入したライセンスを追加する必要があります。

QRadar 製品を購入すると、永続ライセンス・キーが記載されている E メールが IBM から送信されます。このライセンス・キーにより、ご使用のアプライアンス・タイプの機能が拡張され、システム操作パラメーターが定義されます。デフォルト・ライセンスが有効期限切れになる前に、ライセンス・キーを適用する必要があります。

QRadar インストールの前提条件ハードウェア・アクセサリーおよびデスクトップ・ソフトウェア

IBM Security QRadar 製品をインストールする前に、必要なハードウェア・アクセサリーおよびデスクトップ・ソフトウェアが利用可能であることを確認してください。

ハードウェア・アクセサリー

以下のハードウェア・コンポーネントが利用できることを確認してください。

- モニターおよびキーボード

- データを保管するすべてのシステム (QRadar コンソール、イベント・プロセッサー・コンポーネント、QRadar QFlow Collector コンポーネントなど) 用の無停電電源装置 (UPS)。

重要: QRadar 製品は、ハードウェア・ベースの RAID (Redundant Arrays of Independent Disks) 実装をサポートしますが、ソフトウェア・ベースの RAID インストールはサポートしません。

デスクトップ・ソフトウェア要件

QRadar 製品ユーザー・インターフェースにアクセスするために使用するすべてのデスクトップ・システムに、以下のアプリケーションがインストールされていることを確認してください。

- Java™ ランタイム環境 (JRE) バージョン 1.7 または IBM 64-bit Runtime Environment for Java V7.0
- Adobe Flash バージョン 10.x

サポート対象の Web ブラウザー

次の表は、サポートされる Web ブラウザーを示しています。

表 *1. QRadar* 製品でサポートされる *Web* ブラウザー

Web ブラウザー	サポートされるバージョン
Mozilla Firefox	45.2 延長サポート版
64 ビット版の Microsoft Internet Explorer (Microsoft Edge モードを有効にすること)	11.0
Google Chrome	最新

Microsoft Internet Explorer を使用する場合、ドキュメント・モードおよびブラウザー・モードを有効にしてください。

1. Internet Explorer Web ブラウザーで、F12 を押して「開発者ツール」ウィンドウを開きます。
2. 「ブラウザー モード」をクリックし、ご使用の Web ブラウザーのバージョンを選択します。
3. 「ドキュメント モード」をクリックします。
   - Internet Explorer V9.0 の場合は、「**Internet Explorer 9** 標準」を選択します。
   - Internet Explorer V10.0 の場合は、「**Internet Explorer 10** 標準」を選択します。

QRadar Incident Forensics ホスト間の通信には開いているポートが必要

QRadar Incident Forensics ホスト間の通信で開いている必要があるポートを以下の表に示します。

表 2. ホスト間の開いているポート

ポート	説明
443	成果物分析に必要です。
28080	分散検索に必要です。

第 4 章 ユーザーのアプライアンスへの QRadar Incident Forensics ソフトウェアのインストール

ユーザーのアプライアンスへ IBM Security QRadar Incident Forensics を適切にインストールするには、Red Hat Enterprise Linux オペレーティング・システム、QRadar コンソール、および QRadar Incident Forensics 管理対象ホストをインストールする必要があります。

QRadar Incident Forensics を IBM Security QRadar と統合する新規のソフトウェア・インストールの場合、以下の 2 つの ISO ファイルをインストールします。

- QRadar

  1 つの ISO を使用して、QRadar Incident Forensics を除くすべての QRadar 製品がインストールされます。入力するアクティベーション・キーにより、インストールされる QRadar アプライアンスのタイプが決定されます。

- QRadar Incident Forensics

  この ISO イメージには、QRadar Incident Forensics Processor および QRadar Incident Forensics Standalone が含まれています。QRadar Incident Forensics Processor をインストールする必要があります。

ユーザーのアプライアンスへの QRadar Incident Forensics のインストールの前提条件

ユーザーのアプライアンスに Red Hat Enterprise Linux (RHEL) オペレーティング・システムをインストールする前に、ご使用のシステムがシステム要件を満たしていることを確認します。

以下の表で、システム要件について説明します。

表 3. ユーザーのアプライアンスへの *RHEL* のインストールのシステム要件

要件	詳細
サポートされるソフトウェアのバージョン	バージョン 6.7
ビット・バージョン	64 ビット
Kickstart ディスク	サポートされていません
Forensics プロセッサー用のメモリー (RAM)	最小 128 GB **重要:** QRadar をインストールする前に、システム・メモリーをアップグレードする必要があります。
Forensics プロセッサー用の空きディスク・スペース	合計ディスク・スペースの少なくとも 5% **重要:** 最適なパフォーマンスを得るため、最小ディスク・スペースの 2 倍から 3 倍の追加スペースが使用可能であることを確認してください。

表 3. ユーザーのアプライアンスへの *RHEL* のインストールのシステム要件 (続き)

要件	詳細
ファイアウォール構成	WWW (http、https) 有効 SSH 有効 **重要:** ファイアウォールを構成する前に、SELinux オプションを無効にしてください。QRadar インストール済み環境には、「システム・セットアップ」ウィンドウで更新可能なデフォルトのファイアウォール・テンプレートが含まれています。

制約事項: 論理ボリューム・マネージャー (LVM) を使用した論理ボリュームのサイズ変更はサポートされていません。

ユーザーのアプライアンスへの QRadar インストール済み環境に対する Linux オペレーティング・システムのパーティション・プロパティー

ユーザーのアプライアンスを使用する場合は、Red Hat Enterprise Linux オペレーティング・システムでデフォルトのパーティションを変更する代わりに、パーティションを削除してから再作成できます。

次の表に示す値を、Red Hat Enterprise Linux オペレーティング・システムでパーティションを再作成する際の参考として使用してください。

各パーティションのファイル・システムは XFS です。

表 4. *RHEL* のパーティショニングに関するガイド

マウント・パス	**LVM** はサポートされているか	ソフトウェア・インストールに存在するか。	サイズ
/boot	いいえ	はい	1 GB
/boot/efi	いいえ	はい	200 MB
/recovery	いいえ	いいえ	8 GB
/var	はい	はい	5 GB
/var/log	はい	はい	15 GB
/var/log/audit	はい	はい	3 GB
/opt	はい	はい	10 GB
/home	はい	はい	1 GB
/storetmp	はい	はい	15 GB
/tmp	はい	はい	3 GB

表 4. *RHEL* のパーティショニングに関するガイド (続き)

マウント・パス	**LVM** はサポートされているか	ソフトウェア・インストールに存在するか。	サイズ
swap	N/A	はい	スワップの式: スワップ・パーティションのサイズは RAM の 75% となるように構成します (最小値は 12 GiB、最大値は 24 GiB)。
/	はい	はい	最大 15 GB
/store	はい	はい	残りのスペースの 80%
/transient	はい	はい	残りのスペースの 20%

ユーザーのアプライアンスへの RHEL のインストール

QRadar Incident Forensics で使用する Red Hat Enterprise Linux オペレーティング・システムをユーザーのアプライアンスにインストールできます。

手順

1. Red Hat Enterprise Linux オペレーティング・システム DVD ISO を以下のポータブル・ストレージ・デバイスの 1 つにコピーします。
   - DVD (Digital Versatile Disk)
   - ブート可能な USB フラッシュ・ドライブ

     ブート可能な USB フラッシュ・ドライブの作成方法については、「*IBM Security QRadar* インストール・ガイド」を参照してください。
2. アプライアンスにポータブル・ストレージ・デバイスを挿入し、アプライアンスを再始動します。
3. 開始メニューから、以下のいずれかのオプションを選択します。
   - ブート・オプションとして USB または DVD ドライブを選択します。
   - Extensible Firmware Interface (EFI) をサポートするシステムにインストールするには、システムを**レガシー**・モードで始動する必要があります。
4. プロンプトが出されたら、root ユーザーとしてシステムにログインします。
5. イーサネット・インターフェースのアドレス名指定に関する問題を防ぐため、「ようこそ (Welcome)」ページでタブ・キーを押し、Vmlinuz initrd=initrd.image 行の末尾に biosdevname=0 を追加します。
6. インストール・ウィザードの指示に従って、インストールを完了します。
   a. 「基本ストレージ・デバイス **(Basic Storage Devices)**」オプションを選択します。
   b. ホスト名を構成するときには、「ホスト名 **(Hostname)**」プロパティーに文字、数字、ハイフンを使用できます。

c. ネットワークを構成するときには、「ネットワーク接続 (Network Connections)」ウィンドウで「システム **eth0 (System eth0)**」を選択し、「編集 **(Edit)**」をクリックして「自動的に接続する **(Connect automatically)**」を選択します。

d. 「**IPv4** 設定 **(IPv4 Settings)**」タブの「方式 **(Method)**」リストから、「手動 **(Manual)**」を選択します。

e. 「**DNS** サーバー **(DNS servers)**」フィールドに、コンマ区切りリストを入力します。

f. 「カスタム・レイアウトの作成 **(Create Custom Layout)**」オプションを選択します。

g. `/boot` パーティションのファイル・システム・タイプとして `EXT4` を構成します。

h. ファイル・システム・タイプとしてスワップを使用して、スワップ・パーティションを再フォーマットします。

i. 「基本サーバー **(Basic Server)**」を選択します。

7. インストールが完了したら、「リブート **(Reboot)**」をクリックします。
8. オンボード・ネットワーク・インターフェースの名前が `eth0`、`eth1`、`eth2`、および `eth3` であることを確認します。

次のタスク

21 ページの『第 7 章 QRadar コンソールのインストール』

第 5 章 QRadar Incident Forensics アプライアンスへの QRadar Incident Forensics ソフトウェアのインストール

IBM Security QRadar Incident Forensics アプライアンスには、Red Hat Enterprise Linux オペレーティング・システムと QRadar ソフトウェアがプリインストールされています。

QRadar Incident Forensics と IBM Security QRadar を統合する新しいソフトウェアをインストールする場合は、以下に示す 2 つのプリロード ISO ファイルを構成します。

- QRadar

  1 つの ISO を使用して、QRadar Incident Forensics を除くすべての QRadar 製品がインストールされます。入力するアクティベーション・キーにより、インストールされる QRadar アプライアンスのタイプが決定されます。

- QRadar Incident Forensics

  この ISO イメージには、QRadar Incident Forensics Processor と QRadar Incident Forensics Standalone が含まれています。QRadar Incident Forensics Processor をインストールする必要があります。

Forensics 機能だけが必要な場合に新しいソフトウェアをインストールするには、QRadar Incident Forensics Standalone を QRadar Incident Forensics ISO からインストールします。

第 6 章 QRadar Incident Forensics の仮想アプライアンスへのインストール

IBM Security QRadar Incident Forensics を仮想アプライアンスにインストールすることができます。サポートされており、最小システム要件を満たしている仮想アプライアンスを使用していることを確認してください。

仮想アプライアンスは、VMWare ESX 仮想マシンにインストールされている QRadar Incident Forensics ソフトウェアで構成される QRadar Incident Forensics システムです。

仮想アプライアンスが仮想ネットワーク・インフラストラクチャーで提供する可視性および機能は、QRadar アプライアンスが物理環境で提供する可視性および機能と同一です。

インストール・プロセス

仮想アプライアンスをインストールするには、次のタスクを順に実行します。

__ • 仮想マシンを作成します。

__ • 仮想マシンに IBM Security QRadar Incident Forensics ソフトウェアをインストールします。

__ • QRadar Incident Forensics Processor をインストールしてある場合、仮想アプライアンスをデプロイメントに追加します。

仮想アプライアンスのシステム要件

仮想アプライアンスをインストールする前に、以下の最小要件が満たされていることを確認してください。

表 5. 仮想アプライアンスの要件：

要件	説明
VMware クライアント	VMware ESXi バージョン 5.0 VMware ESXi バージョン 5.1 VMware ESXi バージョン 5.5 VMWare クライアントについて詳しくは、VMware Web サイト (www.vmware.com) を参照してください。
仮想ディスク・サイズ	最小: 256 GB **重要:** 最適なパフォーマンスを得るため、最小ディスク・スペースの 2 倍から 3 倍の追加の使用可能スペースを確保してください。

仮想マシンの作成

仮想アプライアンスをインストールするには、最初に VMWare ESX を使用して仮想マシンを作成する必要があります。

手順

1. VMware vSphere Client で「ファイル **(File)**」 > 「新規 **(New)**」 > 「仮想マシン **(Virtual Machine)**」をクリックします。
2. 「名前とロケーション **(Name and Location)**」を追加し、新しい仮想マシンの「データ・ストア」を選択します。
3. 以下のステップに従って、各項目の選択を行います。
   a. 「新規仮想マシンの作成 (Create New Virtual Machine)」ウィンドウの「構成 **(Configuration)**」ペインで、「カスタム **(Custom)**」を選択します。
   b. 「仮想マシンのバージョン **(Virtual Machine Version)**」ペインで「仮想マシンのバージョン**: 7 (Virtual Machine Version: 7)**」を選択します。
   c. 「オペレーティング・システム **(OS) (Operating System (OS))**」で「**Linux**」を選択してから「**Red Hat Enterprise Linux 6 (64-bit)**」を選択します。
   d. 「**CPU**」ページで、仮想マシンで必要とする仮想プロセッサーの数を構成します。40 以上を選択します。
   e. 「メモリー・サイズ **(Memory Size)**」フィールドで、デプロイメントに必要な RAM を入力または選択します。128 GB 以上を選択します。
   f. 次の表を使用してネットワーク接続を構成します。

表 6. ネットワーク構成パラメーターの説明

パラメーター	説明
接続する **NIC** の数 **(How many NICs do you want to connect)**	少なくとも 1 つのネットワーク・インターフェース・コントローラー (NIC) を追加する必要があります。
アダプター **(Adapter)**	VMXNET3

   g. 「**SCSI** コントローラー **(SCSI controller)**」ペインで「**VMware Paravirtual**」を選択します。
   h. 「ディスク **(Disk)**」ペインで「新規仮想ディスクの作成 **(Create a new virtual disk)**」を選択し、次の表を使用して仮想ディスク・パラメーターを構成します。

表 7. 仮想ディスク・サイズとプロビジョニング・ポリシーのパラメーターの設定

プロパティー	オプション
容量	2 以上 (TB)
ディスクのプロビジョニング (Disk Provisioning)	シン・プロビジョン
拡張オプション (Advanced options)	構成しない

4. 「完了する準備ができています **(Ready to Complete)**」ページで設定を確認し、「終了 **(Finish)**」をクリックします。

次のタスク

仮想マシンに QRadar ソフトウェアをインストールします。

仮想マシンでの QRadar Incident Forensics ソフトウェアのインストール

仮想マシンを作成したら、IBM Security QRadar ソフトウェアを仮想マシンにインストールする必要があります。

制約事項**:** 論理ボリューム・マネージャー (LVM) を使用した論理ボリュームのサイズ変更はサポートされていません。

手順

1. VMware vSphere Client の左側のナビゲーション・ペインで、仮想マシンを選択します。
2. 右側のペインで「サマリー」タブをクリックします。
3. 「コマンド」ペインで「設定の編集 **(Edit Settings)**」をクリックします。
4. 「仮想マシンのプロパティー **(Virtual Machine Properties)**」ウィンドウの左側のペインで「**CD/DVD** ドライブ **1 (CD/DVD Drive 1)**」をクリックします。
5. 「デバイスの状況 **(Device Status)**」ペインで、「電源オン時に接続する **(Connect at power on)**」チェック・ボックスを選択します。
6. 「装置タイプ」ペインで「データ・ストア **ISO** ファイル **(Datastore ISO File)**」を選択し、「参照 **(Browse)**」をクリックします。
7. 「データ・ストアの参照 (Browse Datastores)」ウィンドウで、製品の ISO ファイルを見つけて選択し、「オープン」、「**OK**」の順にクリックします。
8. 製品 ISO イメージがインストールされたら、仮想マシンを右クリックし、「電源 **(Power)**」 > 「電源オン **(Power On)**」をクリックします。
9. ユーザー名として `root` と入力して、仮想マシンにログインします。

   ユーザー名では大/小文字を区別します。
10. エンド・ユーザー使用許諾契約書 (EULA) が表示されることを確認します。

    ヒント**:** この文書を読み進むには、スペース・バーを押します。
11. 「アプライアンス **ID** の選択 **(Select the Appliance ID)**」ページで、インストールする QRadar Incident Forensics コンポーネントを選択します。
    - 分散インストールの場合は、「**6000 QRadar Incident Forensics Processor**」を選択します。
    - スタンドアロン・デプロイメントの場合は、「**6100 QRadar Incident Forensics Standalone**」を選択します。
12. セットアップの種類として「標準 **(normal)**」を選択します。
13. インストール・ウィザードの指示に従って、インストールを完了します。

    インストールを構成する際に役立つ説明と注意事項を以下の表に示します。

表 8. ネットワーク設定の説明

ネットワーク設定	説明
ホスト名	完全修飾ドメイン名
セカンダリー DNS サーバー・アドレス	オプション
ネットワーク・アドレス変換 (NAT) を使用するネットワークのパブリック IP アドレス	サポートされていません
E メール・サーバー名	E メール・サーバーがない場合は `localhost` を使用します。
ルート・パスワード	パスワードは、以下の基準を満たしている必要があります。 • 5 文字以上含まれている • スペースを含んでいない • 特殊文字 @、#、^、* は含めることができます。

インストール・パラメーターを構成すると、一連のメッセージが表示されます。このインストール・プロセスは、完了までに数分かかる場合があります。

次のタスク

IBM Security QRadar Incident Forensics Standalone をインストールしていない場合は、 27 ページの『第 9 章 QRadar Incident Forensics 管理対象ホストを QRadar コンソールに追加する』を参照してください。

第 7 章 QRadar コンソールのインストール

分散インストールの場合、QRadar コンソールを 1 つのアプライアンスにインストールし、IBM Security QRadar Incident Forensics 管理対象ホストを別のアプライアンスにインストールします。

制約事項: 1 デプロイメントでのすべてのアプライアンスのソフトウェア・バージョンは、バージョンとフィックス・レベルが同じである必要があります。複数の異なるバージョンのソフトウェアを使用するデプロイメントはサポートされていません。

始める前に

以下の要件を満たしていることを確認してください。

- 必要なハードウェアがインストールされている。
- アプライアンスの必須のライセンス・キーを持っている。
- キーボードおよびモニターが VGA 接続を使用して接続されている。
- www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/) を参照する (統合ネットワーク・インターフェースを構成する場合)。
- 期限切れライセンスがコンソールにも管理対象ホストにも存在しない。

重要: インストール・ウィザードが開始する前にユーザー名とパスワードの入力を求めるプロンプトが出された場合、ユーザー名には `root`、パスワードには `password` を入力してください。

手順

1. 独自のハードウェアまたは仮想マシンへのインストールの場合、ルート・ディレクトリーに QRadar コンソール ISO イメージを追加します。
   a. 以下のコマンドを入力して `/media/dvd` ディレクトリーを作成します。

      ```
      mkdir /media/dvd
      ```

   b. 以下のコマンドを入力して、QRadar コンソール ISO イメージをマウントします。

      ```
      mount -o loop <QRadar_ISO> /media/dvd
      ```

2. セットアップ・スクリプトを使用してインストールを開始します。
   a. 以下のコマンドを入力して作業ディレクトリーを変更します。 `cd /media/dvd`
   b. 以下のコマンドを入力してセットアップ・スクリプトを開始します。 `setup.sh`
3. インストール・ウィザードの指示に従います。

- 「以下にアクティベーション・キーを入力 **(Enter your activation key below)**」で、アクティベーション・キーの入力を求めるプロンプトが出されたら、IBM から受け取った、4 つの部分に区切られた 24 桁の英数字ストリングを入力します。

  文字 I と数字の 1 は同じものとして扱われます。文字 O と数字の 0 (ゼロ) も同じものとして扱われます。
- E メール・サーバーを使用していない場合は、「使用するネットワーク情報を入力 **(Enter the network information to use)**」ページで、「**E** メール・サーバー名 **(Email server name)**」フィールドに `localhost` と入力します。
- 「ルート・パスワード **(Root password)**」フィールドで、以下の条件を満たすパスワードを入力します。
  - 5 文字以上使用されていること
  - スペースが含まれていないこと
  - 特殊文字 @、#、^、* は含めることができます。

このインストール・プロセスは、完了までに数分かかる場合があります。

4. ライセンス・キーを適用します。
   a. QRadar にログインします。

      `https://`*`IP_Address_QRadar`*

      デフォルト・ユーザー名は `admin` です。パスワードは、root ユーザー・アカウントのパスワードです。
   b. 「**QRadar** にログイン」をクリックします。
   c. 「管理」タブをクリックします。
   d. ナビゲーション・ペインで、「システム構成」をクリックします。
   e. 「システムおよびライセンス管理」アイコンをクリックします。
   f. 「表示」リスト・ボックスから、「ライセンス」を選択して、ライセンス・キーをアップロードします。
   g. まだ割り振りられていないライセンスを選択し、「ライセンスへのシステムの割り振り」をクリックします。
   h. システムのリストからシステムを選択し、「ライセンスへのシステムの割り振り」クリックします。

次のタスク

これで、QRadar Incident Forensics をインストールすることができます。

第 8 章 QRadar Incident Forensics のインストール

分散インストールの場合、QRadar コンソールを 1 つのアプライアンスにインストールし、IBM Security QRadar Incident Forensics 管理対象ホスト (QRadar Incident Forensics Processor) を別のアプライアンスにインストールします。スタンドアロン・デプロイメントの場合、QRadar Incident Forensics Standalone コンポーネントのみインストールします。

制約事項**:** 1 デプロイメントでのすべてのアプライアンスのソフトウェア・バージョンは、バージョンとフィックス・レベルが同じである必要があります。複数の異なるバージョンのソフトウェアを使用するデプロイメントはサポートされていません。

始める前に

以下の要件を満たしていることを確認してください。

__ • 必要なハードウェアがインストールされている。

__ • キーボードおよびモニターが VGA 接続を使用して接続されている。

__ • アクティベーション・キーが使用可能である。

制約事項**:** 論理ボリューム・マネージャー (LVM) を使用した論理ボリュームのサイズ変更はサポートされていません。

手順

1. 独自のハードウェアまたは仮想マシンへのインストールの場合、ルート・ディレクトリーに QRadar Incident Forensics ISO イメージを追加します。
   a. 以下のコマンドを入力して /media/dvd ディレクトリーを作成します。

      ```
      mkdir /media/dvd
      ```

   b. 以下のコマンドを入力して、QRadar コンソール ISO イメージをマウントします。

      ```
      mount -o loop <QRadar_Incident_Forensics_ISO>/media/dvd
      ```

2. セットアップ・スクリプトを使用してインストールを開始します。
   a. 以下のコマンドを入力して作業ディレクトリーを変更します。 `cd /media/dvd`
   b. 以下のコマンドを入力してセットアップ・スクリプトを開始します。 `setup.sh`
3. インストール・ウィザードの指示に従います。

   「アプライアンス **ID** の選択 **(Select the Appliance ID)**」ページで、インストールする QRadar Incident Forensics コンポーネントを選択します。
   - 分散インストールの場合は、「**6000 QRadar Incident Forensics Processor**」を選択します。

- スタンドアロン・デプロイメントの場合は、「**6100 QRadar Incident Forensics Standalone**」を選択します。

制約事項**:** 以下の構成の選択は、QRadar Incident Forensics ではサポートされていません。

- 「セットアップのタイプの選択 (Choose the type of setup)」ページの「**HA** リカバリーのセットアップ **(HA Recovery Setup)**」オプション
- 「結合インターフェース構成モードを使用する場合に選択 (Select if you want to use bonded interface configuration mode)」ページの「結合インターフェース構成モードの使用 **(Use bonded interface configuration mode)**」オプション

QRadar Incident Forensics Processor をインストールする場合、このインストール・プロセスは、完了までに数分かかる場合があります。

4. ライセンス・キーを適用します。
   a. QRadar にログインします。

      `https://IP_Address_QRadar`

      デフォルト・ユーザー名は `admin` です。パスワードは、root ユーザー・アカウントのパスワードです。
   b. 「ログイン」をクリックします。
   c. 「管理」タブをクリックします。
   d. ナビゲーション・ペインで、「システム構成」をクリックします。
   e. 「システムおよびライセンス管理」アイコンをクリックします。
   f. 「表示」リスト・ボックスから「ライセンス」を選択して、ライセンス・キーをアップロードします。
   g. まだ割り振られていないライセンスを選択し、「ライセンスへのシステムの割り振り」をクリックします。
   h. ライセンスのリストからライセンスを選択して、「システムへのライセンスの割り振り」をクリックします。

   注**:** スタンドアロン・デプロイメント (6100) をインストールする場合、IBM Security QRadar Incident Forensics Standalone アプライアンスに 2 つのライセンス・キーを割り振る必要があります。1 つのライセンスは、QRadar Incident Forensics Standalone 用で、もう 1 つは「**Forensics**」タブへのアクセス用です。

   既存の IBM Security QRadar SIEM 環境への分散インストール (6000) ごとに、各 Forensics 管理対象ホスト (6000) のライセンスと、さらにコンソール上で「**Forensics**」タブを使用可能にするための単一のライセンスが必要になる場合があります。既存の QRadar コンソールのライセンス・キーを「**Forensics**」タブへのアクセス用に割り振る場合は、ライセンス・キーのみをインストールする必要があります。既存の QRadar コンソールのライセンス・キーを「**Forensics**」タブへのアクセス用に割り振らない場合は、ランセンス・キーと更新された Forensics 使用可能化キーをインストールする必要があります。

次のタスク

QRadar Incident Forensics Processor 管理対象ホストをデプロイします。詳しくは、 27 ページの『第 9 章 QRadar Incident Forensics 管理対象ホストを QRadar コンソールに追加する』を参照してください。

第 9 章 QRadar Incident Forensics 管理対象ホストを QRadar コンソールに追加する

分散インストール済み環境の場合、IBM Security QRadar Incident Forensics Processor を管理対象ホストとして QRadar コンソールに追加する必要があります。

管理対象ホスト とは、デプロイメント環境内のすべての非コンソール QRadar アプライアンスのことです。分散処理に対して、複数の QRadar Incident Forensics Processor を管理対象ホストとして追加することができます。

制約事項: デプロイメント・エディターを使用して QRadar Incident Forensics 管理対象ホストの追加や削除を行うことはできません。「システムおよびライセンス管理」ツールを使用する必要があります。

始める前に

最初に QRadar コンソール・ソフトウェアをインストールする必要があります。詳しくは、 21 ページの『第 7 章 QRadar コンソールのインストール』を参照してください。

手順

1. QRadar コンソールに管理者としてログインします。

   `https://IP_Address_QRadar`

   デフォルト・ユーザー名は `admin` です。パスワードは、インストール時に入力された、root ユーザー・アカウントのパスワードです。
2. 「管理」タブをクリックします。
3. 「システム構成」ペインで、「システムおよびライセンス管理」をクリックします。
4. ホスト・テーブルで QRadar コンソール・ホストをクリックし、次に > 「デプロイメント・アクション」 > 「ホストの追加」をクリックします。
5. QRadar Incident Forensics Processor アプライアンスの情報を入力して「追加」をクリックします。

   制約事項: 「ホストの暗号化」プロパティーと「ネットワーク・アドレス変換」プロパティーはサポートされていません。
6. 「管理」タブのメニュー・バーで、「変更のデプロイ」をクリックします。
7. Web ブラウザーを最新表示します。

   「**Forensics**」タブが表示されるようになります。

次のタスク

IBM Security QRadar Packet Capture デバイスを QRadar Incident Forensics Processor に追加することができます。詳しくは、 34 ページの『QRadar Incident

Forensics ホストへのパケット・キャプチャー・デバイスの追加』を参照してください。

QRadar Incident Forensics 管理対象ホストの削除

ネットワーク構成の設定を変更する場合や、「**Forensics**」タブの表示に問題がある場合は、QRadar Incident Forensics 管理対象ホスト (IBM Security QRadar Incident Forensics Processor) を QRadar のデプロイメント環境から削除することができます。QRadar Incident Forensics 管理対象ホストで Forensics リカバリーを実行した場合は、QRadar Incident Forensics Processor をもう一度追加するとデータの損失が発生します。

QRadar Incident Forensics 管理対象ホストは削除されていないが、停電などの問題で一時的に応答しなくなった場合は、この管理対象ホストのジョブはスケジュールされたままになり、この管理対象ホストがもう一度オンライン状態になると、スケジュールに従って処理されます。

制約事項**:** デプロイメント・エディターを使用して QRadar Incident Forensics 管理対象ホストの追加や削除を行うことはできません。「システムおよびライセンス管理」ツールを使用する必要があります。

手順

1. QRadar コンソールに管理者としてログインします。

   `https://IP_Address_QRadar`

   デフォルト・ユーザー名は `admin` です。パスワードは、インストール時に入力された、root ユーザー・アカウントのパスワードです。
2. 「管理」タブをクリックします。
3. 「システム構成」ペインで、「システムおよびライセンス管理」をクリックします。
4. ホスト・テーブルで、削除する QRadar Incident Forensics Processor ホストをクリックし、そして > 「デプロイメント・アクション」 > 「ホストの削除」をクリックします。
5. 「管理」タブのメニュー・バーで、「変更のデプロイ」をクリックします。
6. Web ブラウザーを最新表示します。

第 10 章 パケット・キャプチャー・デバイスと QRadar Incident Forensics の間の接続

パケット・キャプチャー・データを取得するには、1 つ以上のパケット・キャプチャー・デバイスを IBM Security QRadar Incident Forensics 管理対象ホストまたは QRadar Incident Forensics Standalone コンポーネントに接続する必要があります。パケット・キャプチャー・デバイスが接続されていない場合、ユーザー・インターフェースまたは FTP を使用して、パケット・キャプチャー・ファイルを手動でアップロードできます。

パケット・キャプチャーのマスター・システム

ネットワークおよびパケット・キャプチャーの要件に応じて、最大で 5 台のパケット・キャプチャー・デバイスを QRadar Incident Forensics アプライアンスに接続できます。リカバリーを実行依頼する場合、それぞれの QRadar Incident Forensics アプライアンス上の各パケット・キャプチャー・デバイスに、個別のジョブが実行依頼されます。例えば、2 つの QRadar Incident Forensics 管理対象ホストをインストールし、それぞれのホストに 2 つのパケット・キャプチャーがある場合、4 つのジョブが実行依頼されます。

次の図は、複数のパケット・キャプチャー・デバイスを QRadar Incident Forensics 管理対象ホスト (QRadar Incident Forensics Processor) または QRadar Incident Forensics Standalone アプライアンスに接続できることを示しています。

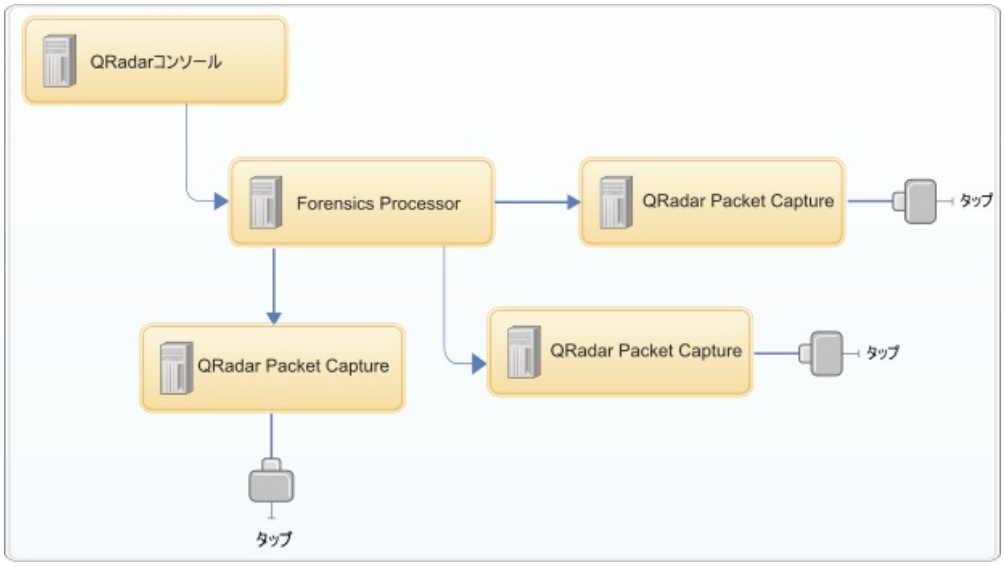


図 4. 複数のパケット・キャプチャー・デバイスを *QRadar Incident Forensics* 管理対象ホストに接続した例

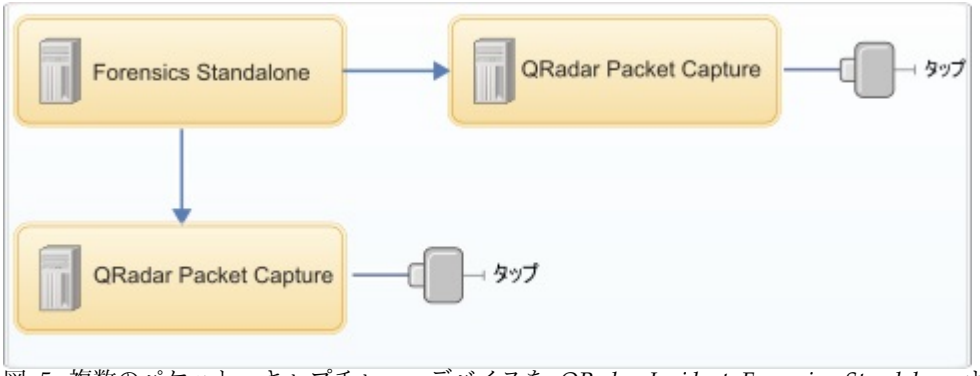
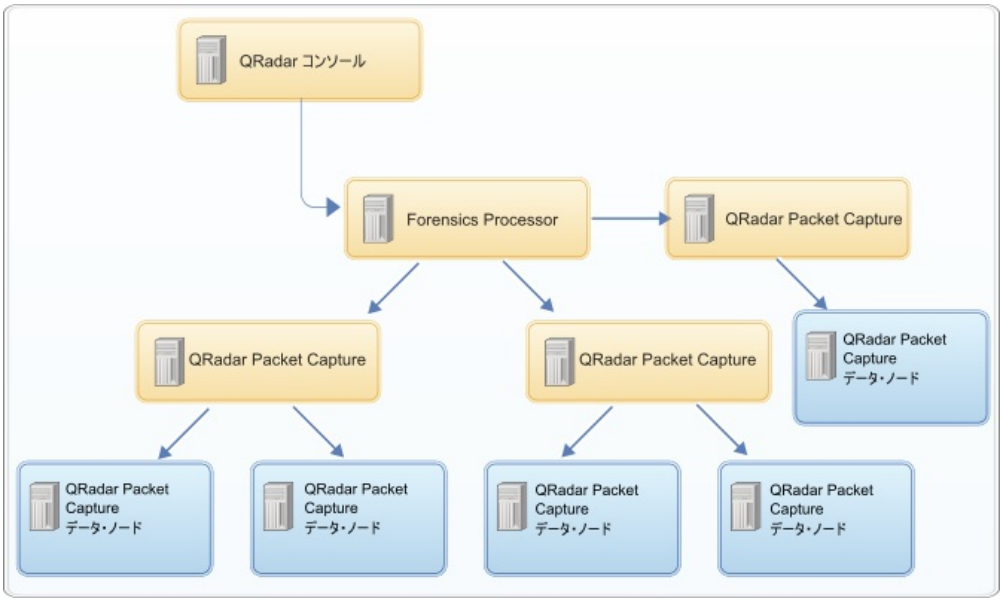


図 5. 複数のパケット・キャプチャー・デバイスを *QRadar Incident Forensics Standalone* ホストに接続した例

QRadar Packet Capture データ・ノード・アプライアンス

ストレージ容量を追加する場合、最大 2 台の QRadar Packet Capture データ・ノード・アプライアンスをそれぞれの QRadar Packet Capture マスター・システムに接続できます。それぞれの PCAP データ・ノード・アプライアンスは、37 TB の追加ストレージを提供します。



QRadar Packet Capture データ・ノード・アプライアンスをマスター・システムに接続した後、QRadar Packet Capture ユーザー・インターフェースでクラスターを構成できます。

マスター・アプライアンスから QRadar Packet Capture データ・ノード・アプライアンスへの物理接続について詳しくは、「*QRadar Packet Capture* クイック・リファレンス・ガイド」を参照してください。パケット・キャプチャー・クラスターの構成について詳しくは、「*QRadar Packet Capture* ユーザーズ・ガイド」を参照してください。

アプライアンスへの QRadar Packet Capture ソフトウェアのインストール

ユーザーのアプライアンスに IBM Security QRadar Packet Capture を正常にインストールするには、Red Hat Enterprise Linux オペレーティング・システムおよび QRadar Packet Capture ソフトウェアをインストールする必要があります。また、アプライアンスがシステム要件を満たしていることを確認する必要があります。

重要: QRadar Packet Capture ソフトウェアをインストールするシステムは、QRadar Packet Capture 専用であることが必要です。IBM で承認されていない RPM パッケージをインストールしないでください。未承認の RPM をインストールすると、アップグレード時に依存関係エラーが発生したり、デプロイメントでパフォーマンスの問題が生じたりする可能性があります。YUM を使用してオペレーティング・システムを更新したり、未承認のソフトウェアを QRadar Packet Capture システムにインストールしたりしないでください。

制約事項: 仮想マシンへのソフトウェア・インストールはサポートされていません。

始める前に

ご使用のアプライアンスが以下のシステム要件を満たしていることを確認してください。

表 9. *QRadar Packet Capture* ソフトウェアのインストールのシステム要件

仕様	説明
プロセッサー	Intel E5 シリーズ・プロセッサー V2 または V3。V4 バージョンでは 6 コア以上が必要です。
プロセッサー BIOS 設定	Intel により 2011 年に導入された Intel AES および AVX 標準をサポートしている必要があります。 ハイパー・スレッド機能が有効になるように BIOS システム設定を構成します。
メモリー	24 GB
ハードウェア RAID コントローラーとキャプチャーおよび抽出ストア	最小で 4 台のハード・ディスクにまたがる RAID 構成 (RAID 0、1 または 5 の組み合わせを使用) (各ハード・ディスクのパフォーマンスは 7200 RPM 以上、容量は 1 TB 以上)
オペレーティング・システム・ドライブ	500 GB で最小 7200 RPM のエンタープライズ・クラスのハード・ディスクである SATA または SAS
オペレーティング・システム	Red Hat Enterprise Linux V6.7 **注:** 専用の PCAP アプライアンスとして 1G PCAP をインストールするシステムに 1G SFS インストーラーをインストールする必要があります。これはパケット・キャプチャー以外のいかなる目的にも使用しないでください。

表 9. *QRadar Packet Capture* ソフトウェアのインストールのシステム要件 (続き)

仕様	説明
最小限の合計ディスク・スペース	4 TB
キャプチャー NIC (1G / 10G キャプチャー (1Gbp 以上もサポート) に対応する単一インターフェース)	Intel 製 PCI Express ネットワーク・カード: • Intel E1G44ET2BLK Ethernet PCI Express アダプター (http://ark.intel.com/products/49187/Intel-Gigabit-ET2-Quad-Port-Server-Adapter) • Intel X520-SR2 Dual Ports 10 Gigabit Ethernet Converged Network Adapter (PCI Express 2.0 x8、ロー・プロファイル) (http://ark.intel.com/products/39774/Intel-Ethernet-Converged-Network-Adapter-X520-SR2) または Intel イーサネット・コントローラー (マザーボードまたはネットワーク・アダプターが以下のコントローラーを使用して動作する必要があります): • Intel 82576 ギガビット・イーサネット・コントローラー (http://ark.intel.com/products/series/32261/Intel-82576-Gigabit-Ethernet-Controller) または Dell ベースのコンピューター・ネットワーク・カード: • Intel X520 DP 10Gb DA/SFP+ Server Adapter (DELL SKU#540-BBCT) (http://accessories.ap.dell.com/sna/productdetail.aspx?c=sg&l=en&s=dhs&cs=sgdhs1&sku=540-11353) • Intel Ethernet i350 QP 1Gb Network Daughter Card (DELL SKU#540-BBCB) (http://accessories.dell.com/sna/productdetail.aspx?c=us&l=en&s=gen&sku=430-4437) • Intel Ethernet i350 QP 1Gb Network PCI Express Card (DELL SKU#540-11357) (http://accessories.ap.dell.com/sna/productdetail.aspx?c=au&l=en&s=bsd&cs=aubsd1&sku=540-11357)
PCAP UI ネットワーク・インターフェース	任意の 1G (またはオプションで 10G) ネットワーク・インターフェース (例: eth0)。

所有するアプライアンスに QRadar Packet Capture ソフトウェアをインストールする前に、別個の 3 台の仮想ドライブをセットアップして構成することをお勧めし

ます。これらの仮想ドライブはそれぞれ OS 用、抽出用、およびストレージ用です。ストレージ・ドライブは 3 台の中で最大のサイズにする必要があります (最小要件は 4000 GB)。

以下の例を参照してください。

表 *10. QRadar Packet Capture* ソフトウェア・インストール済み環境の *RAID* 構成の例

仮想ドライブ	RAID レベル	サイズ
0	RAID 1	128 GB
1	RAID 1	3587 GB
2	RAID 5	33527 GB

手順

1. Red Hat Enterprise Linux オペレーティング・システムのディスクをアプライアンスに挿入し、アプライアンスを再始動します。
2. インストール・ウィザードの指示に従って、インストールを完了します。
   a. 「基本ストレージ・デバイス **(Basic Storage Devices)**」オプションを選択します。
   b. ホスト名を構成するときには、「ホスト名 **(Hostname)**」プロパティーに文字、数字、ハイフンを使用できます。
   c. 「**IPv4** 設定 **(IPv4 Settings)**」タブの「方式 **(Method)**」リストから、「手動 **(Manual)**」を選択します。
   d. 「どのタイプのインストールをしますか (Which type of installation would you like)」 ページで、「すべての領域を使用する **(Use All Space)**」を選択し、オペレーティング・システムのインストール先として最小パーティション (ブート・パーティション) を選択します。
   e. インストールのオプションとして「基本システム **(Base System)**」のみを選択します。
3. インストールが完了したら、「リブート **(Reboot)**」をクリックします。
4. QRadar Packet Capture SFS ファイルをアプライアンスにコピーします。
5. QRadar Packet Capture SFS ファイルをマウントします。
   a. 以下のコマンドを入力して `/tmp/qpc_install` ディレクトリーを作成します。

      ```
      mkdir -p /tmp/qpc_install
      ```

   b. 以下のコマンドを入力して QRadar Packet Capture SFS ファイルをマウントします。

      ```
      mount -o loop -t squashfs <QRadar_Packet_Capture_file.sfs>
      /tmp/qpc_install
      ```

   c. `/tmp/qpc_install` ディレクトリーに移動します。

      ```
      cd /tmp/qpc_install
      ```

6. 以下のコマンドを入力してインストール・スクリプトを実行します。

   ```
   sh installer.sh
   ```

QRadar Incident Forensics ホストへのパケット・キャプチャー・デバイスの追加

調査担当者がパケット・キャプチャー情報にアクセスできるようにするために、1 つの IBM Security QRadar Incident Forensics 管理対象ホストまたは IBM Security QRadar Incident Forensics Standalone ホストに最大 5 つのパケット・キャプチャー・デバイスを接続できます。接続されたパケット・キャプチャー・デバイスによって、Forensics Recovery 用のキャプチャー済みファイルが処理されます。

パケット・キャプチャー・デバイスが接続されていない場合は、ユーザー・インターフェースまたは FTP を使用してパケット・キャプチャー・ファイルを手動でアップロードできます。

制約事項: デプロイメント・エディターを使用してパケット・キャプチャー・デバイスを追加することはできません。「システムおよびライセンス管理」ツールを使用する必要があります。

始める前に

QRadar Incident Forensics 管理対象ホストをインストールしてデプロイするか、または QRadar Incident Forensics Standalone ホストをインストールする必要があります。詳しくは、23 ページの『第 8 章 QRadar Incident Forensics のインストール』および 27 ページの『第 9 章 QRadar Incident Forensics 管理対象ホストを QRadar コンソールに追加する』を参照してください。

以下の対話式ダイアグラムは、分散インストールでのインストール・プロセスの主要ステップを示しています。スタンドアロン・デプロイメントの場合もインストール・プロセスは同じですが、管理対象ホストはデプロイしません。

デフォルトでは、QRadar Packet Capture デバイスのタイム・ゾーンは UTC (協定世界時) に設定されています。

手順

1. QRadar コンソールに管理者としてログインします。

   `https://IP_Address_QRadar`

   デフォルト・ユーザー名は `admin` です。パスワードは、インストール時に入力された、root ユーザー・アカウントのパスワードです。
2. 「管理」タブをクリックします。
3. 「システム構成」ペインで、「システムおよびライセンス管理」をクリックします。
4. ホスト・テーブルで QRadar Incident Forensics Processor (「アプライアンスのタイプ」は 6000) または QRadar Incident Forensics Standalone ホスト (「アプライアンスのタイプ」は 6100) を選択し、「デプロイメント・アクション」 > 「ホストの編集」をクリックします。
5. 「コンポーネント管理」をクリックします。

6. パケット・キャプチャー・デバイスを追加するには、追加アイコン (+) をクリックし、デバイスに関する情報を入力します。

   ヒント: QRadar Packet Capture デバイスのデフォルトのユーザー名は `continuum` です。
7. 「保存」をクリックします。

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。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

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。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

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。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds 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 Oracle やその関連会社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。

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

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用度

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権限

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、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なしで提供されます。

IBM オンラインでのプライバシー・ステートメント

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21