IBM Security QRadar
バージョン **7.3.0**

アーキテクチャーおよびデプロイメント・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、 47 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
Version 7.3.0
Architecture and Deployment 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

QRadar デプロイメントの概要

「IBM® Security QRadar® デプロイメント・ガイド」は、QRadar のインストールを計画するときに役立ちます。

対象読者

この情報は、ネットワーク・セキュリティーの調査と管理を担当するセキュリティー管理者による使用を対象としています。本ガイドを使用するにあたっては、企業ネットワーク・インフラストラクチャーおよびネットワーキング・テクノロジーに関する知識が必要です。

技術資料

詳細な技術資料、技術情報、およびリリース情報にアクセスする方法については、Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) 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については、Support for IBM Security QRadar (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) を参照してください。

適切なセキュリティー対策に関する注意事項

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。

第 1 章 QRadar アーキテクチャーの概要

IBM Security QRadar デプロイメントを計画または作成するときは、QRadar アーキテクチャーをよく理解し、ネットワークで QRadar コンポーネントがどのように機能する可能性があるかを評価した後、QRadar デプロイメントを計画して作成すると役立ちます。

IBM Security QRadar は、ネットワーク・データをリアルタイムで収集、処理、集約、および保管します。 QRadar はそのデータを使用して、リアルタイムの情報とモニタリング、アラートとオフェンス、およびネットワーク脅威への対応を提供することで、ネットワーク・セキュリティーを管理します。

IBM Security QRadar SIEM (セキュリティー情報およびイベント管理) は、IT インフラストラクチャーのリアルタイムの可視性を提供するモジュラー・アーキテクチャーであり、これを使用して脅威を検出したり、優先順位を付けたりすることができます。QRadar をスケーリングして、ログおよびフローの収集や分析のニーズを満たすことができます。 QRadar Risk Manager、QRadar Vulnerability Manager、および QRadar Incident Forensics など、統合されたモジュールを QRadar プラットフォームに追加できます。

QRadar セキュリティー・インテリジェンス・プラットフォームの操作は 3 つのレイヤーで構成されており、サイズや複雑さに関係なく、すべての QRadar デプロイメント構造に適用されます。以下の図には、QRadar アーキテクチャーを構成するレイヤーが示されています。

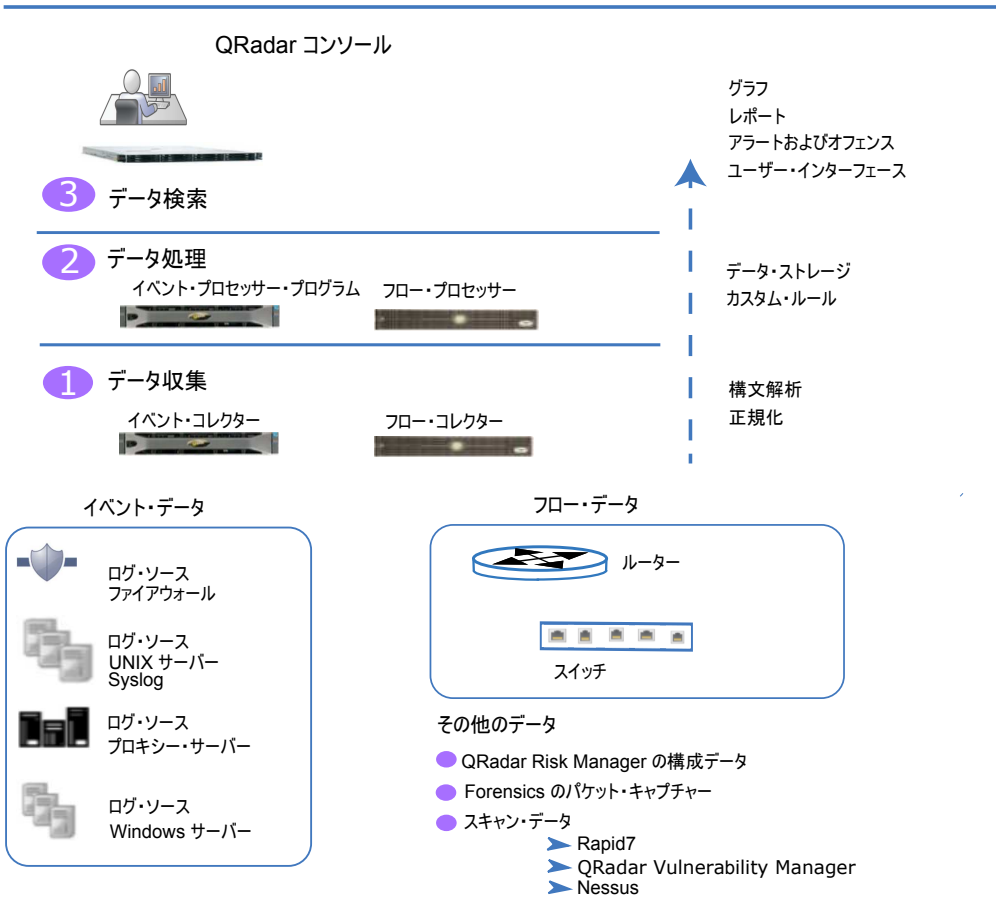


図 *1. QRadar* アーキテクチャー

QRadar アーキテクチャーは、デプロイメント内のコンポーネントのサイズや数に関係なく、同じように機能します。図に示されている以下の 3 つのレイヤーは、QRadar システムの主要機能を表しています。

データ収集

データ収集は、最初のレイヤーです。ここでは、イベントやフローなどのデータがネットワークから収集されます。オールインワン・アプライアンスを使用してネットワークから直接データを収集することも、QRadar イベント・コレクター や QRadar QFlow コレクター などのコレクターを使用してイベント・データやフロー・データを収集することもできます。データは構文解析され、正規化されてから、処理レイヤーに渡されます。未加工のデータが構文解析されると、そのデータは正規化され、構造化されて使用可能なフォーマットで表されます。

QRadar SIEM の主要機能では、イベント・データの収集とフローの収集に重点が置かれています。

イベント・データは、ユーザーのログイン、E メール、VPN 接続、ファイアウォールの拒否、プロキシー接続、およびデバイス・ログにログインする必要のあるその他のイベントなど、ユーザーの環境で特定の時点で発生するイベントを表しています。

フロー・データは、ネットワーク上の 2 つのホスト間のネットワーク・アクティビティー情報またはセッション情報であり、QRadar によってフロー・レコードに変換されます。 QRadar は、未加工のデータを IP アドレス、ポート、バイト数やパケット数、およびその他の情報に変換または正規化し、フロー・レコードにします。実質的に、これは 2 つのホスト間のセッションを表します。フロー・コレクターを使用してフロー情報を収集するほかに、完全なパケット・キャプチャーを QRadar Incident Forensics コンポーネントと併用できます。

データ処理

データ収集の後、2 番目のレイヤー、つまりデータ処理レイヤーでイベント・データとフロー・データがカスタム・ルール・エンジン (CRE) を介して実行され、オフェンスとアラートが生成されて、データがストレージに書き込まれます。

イベント・データとフロー・データは、イベント・プロセッサーまたはフロー・プロセッサーを追加しなくても、オールインワン・アプライアンスで処理できます。オールインワン・アプライアンスの処理能力を超えると、イベント・プロセッサー、フロー・プロセッサー、またはその他の処理アプライアンスを追加して、追加要件を処理する必要が生じる場合があります。また、ストレージ容量がさらに必要になる場合もあります。これは、データ・ノードを追加することで対処できます。

QRadar Risk Manager (QRM)、QRadar Vulnerability Manager (QVM)、または QRadar Incident Forensics など、その他の機能により、さまざまなタイプのデータが収集され、さらに機能が提供されます。

QRadar Risk Manager は、ネットワーク・インフラストラクチャー構成を収集し、ネットワーク・トポロジーのマップを提供します。このデータを使用して、ネットワークで構成を変更しルールを実装することによって、さまざまなネットワーク・シナリオをシミュレーションすることで、リスクを管理できます。

QRadar Vulnerability Manager を使用してネットワークをスキャンし、脆弱性データを処理したり、Nessus や Rapid7 などのその他のスキャナーから収集された脆弱性データを管理します。収集された脆弱性データを使用して、ネットワーク内のさまざまなセキュリティー・リスクが特定されます。

QRadar Incident Forensics を使用して詳細なフォレンジック調査を行い、すべてのネットワーク・セッションをリプレイします。

データ検索

3 番目、つまり最上位のレイヤーでは、QRadar によって収集および処理されたデータを使用して、ユーザーは検索、分析、レポート作成、およびアラートやオフェンスの調査を行えます。ユーザーは、QRadar コンソールのユーザー・インターフェースからネットワークに対するセキュリティー管理タスクを検索および管理できます。

オールインワン・システムでは、すべてのデータがオールインワン・アプライアンスで収集、処理、および保管されます。

分散環境では、QRadar コンソールはイベントとフローの処理、および保管は行いません。代わりに、主に QRadar コンソールがユーザー・インターフェースとして

使用されます。ユーザーはこれを使用して、検索、レポート作成、アラート、および調査を行えます。

QRadar コンポーネント

IBM Security QRadar コンポーネントを使用して QRadar デプロイメントをスケーリングし、分散ネットワークでデータの収集と処理を管理します。

重要: デプロイメントでのすべての IBM Security QRadar アプライアンスのソフトウェアのバージョンとフィックスパック・レベルが同じである必要があります。異なるバージョンのソフトウェアを使用したデプロイメントはサポートされていません。バージョンが混在した環境ではルールが起動されなかったり、オフェンスが作成および更新されなかったり、検索結果でエラーが発生したりする可能性があるためです。

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 コンソール には、QRadar ユーザー・インターフェース、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、および管理機能が用意されています。

分散 QRadar デプロイメントでは、QRadar コンソールを使用して他のコンポーネントが含まれているホストを管理します。

QRadar イベント・コレクター

イベント・コレクター は、ローカルとリモートのログ・ソースからイベントを収集し、未加工のログ・ソース・イベントを正規化して、QRadar で使用できるようにフォーマット設定します。イベント・コレクターはシステムの使用量を節約するために同一イベントをバンドルまたは統合し、データをイベント・プロセッサーに送信します。

- WAN リンクが低速であるリモート・ロケーションでは QRadar Event Collector 1501 を使用します。イベント・コレクター・アプライアンスは、イベントをローカルに保管しません。代わりに、これらのアプライアンスはイベントを収集して解析した後、イベント・プロセッサー・アプライアンスにイベントを送信して保管します。
- イベント・コレクターは、断続的接続など、WAN 制限を克服するために、帯域幅リミッターやスケジュールを使用してイベントをイベント・プロセッサーに送信することができます。
- イベント・コレクターは、接続先のイベント・プロセッサーと一致する EPS ライセンスに割り当てられます。

QRadar イベント・プロセッサー

イベント・プロセッサーは、1 つまたは複数の イベント・コレクター コンポーネントから収集されたイベントを処理します。イベント・プロセッサーは、カスタム・ルール・エンジン (CRE) を使用してイベントを処理します。コンソールに事前定義されている CRE カスタム・ルールとイベントが一致した場合、イベント・プロセッサーはルール応答に定義されているアクションを実行します。

イベント・プロセッサーにはローカル・ストレージがあり、イベント・データはプロセッサーに保管されます。あるいは、データ・ノードに保管することもできます。

イベントの処理速度は、イベント/秒 (EPS) ライセンスによって決まります。EPS 速度を超えると、イベントはバッファーに入れられ、速度が下がるまでイベント・コレクターのソース・キューに留まります。ただし、EPS ライセンス速度を超え続け、キューが満杯になると、システムによってイベントがドロップされ、QRadar はライセンスを受けている EPS 速度を超えているという警告を出します。

イベント・プロセッサーをオールインワン・アプライアンスに追加すると、イベント処理機能はオールインワンからイベント・プロセッサーに移動されます。

QRadar QFlow Collector

フロー・コレクターは、SPAN ポート、またはネットワーク TAP に接続してフローを収集します。IBM Security QRadar QFlow Collector では、ルーターからの NetFlow など、外部フロー・ベースのデータ・ソースの収集もサポートされています。

QRadar QFlow コレクター は、完全なパケット・キャプチャー・システムとしては設計されていません。完全なパケット・キャプチャーについては、QRadar Incident Forensics のオプションを確認してください。特に QRadar QFlow Collector 1310 アプライアンスはパケットを QRadar Packet Capture アプライアンスに転送できます。これにより、単一のパケット・ソースからフローの収集やパケットの収集を行えるようになります。

QRadar QFlow Collector をユーザーのハードウェアにインストールするか、または QRadar QFlow Collector アプライアンスの 1 つを使用することができます。

制約事項: QRadar Log Manager ではフロー収集およびフロー・コレクターはサポートされていません。これは、QRadar SIEM デプロイメントでのみサポートされています。

QRadar フロー・プロセッサー

フロー・プロセッサーは、1 つまたは複数の QRadar QFlow Collector アプライアンスからのフローを処理します。フロー・プロセッサー アプライアンスは、ネットワーク内のルーターから外部ネットワーク・フロー (NetFlow、J-Flow、sFlow など) を直接収集することもできます。フロー・プロセッサー・アプライアンスを使用して、QRadar デプロイメントをスケーリングし、より高いフロー/秒 (FPM) 速度を管理できます。フロー・プロセッサーには、オンボードのフロー・プロセッサーと、フロー・データ用の内部ストレージが組み込まれています。フロー・プロセッサーをオールインワン・アプライアンスに追加すると、処理機能はオールインワン・アプライアンスからフロー・プロセッサーに移動されます。

QRadar データ・ノード

新しい QRadar デプロイメント環境や既存の QRadar デプロイメント環境でデータ・ノードを使用すると、必要に応じてオンデマンドでストレージや

処理能力を追加することができます。データ・ノードは、検索照会を実行するハードウェア・リソースを増やすことで、デプロイメントでの検索速度を高めるのに役立ちます。

QRadar コンポーネントの管理について詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。

QRadar アプライアンスの仕様

デプロイメントでどのような場合に特定の QRadar アプライアンスを使用するかについて以下の表で説明します。

表 *1. QRadar* アプライアンスの概要

アプライアンス	説明
QRadar 2100	従業員が 10 人から 200 人のデプロイメント向けの拡張不可のソリューション
QRadar 3105 (All-in-One)	QRadar 2100 よりも強化された能力を提供し、イベント・プロセッサーおよびフロー・プロセッサーを追加する機能を提供します。
QRadar 3105 (Console)	デプロイメントが 5000 イベント/秒 (EPS) を超える処理を行う場合は、QRadar 3105 (Console) を分散イベント・プロセッサーとともに使用する必要があります。QRadar 3105 (Console) は、オフボード・イベント処理およびストレージを使用して、リソースを解放します。これにより、レポートや検索結果のサービスを提供し、UI アクションの速度を向上させます。
QRadar 3128 (All-in-One)	QRadar 3105 (All-in-One) よりも強化された能力を提供します。
QRadar 3128 (Console)	QRadar 3105 (Console) よりも強化された能力を提供します。
xx05 コレクターおよびプロセッサー	12 個のプロセッサー 64 GB の RAM 6.2 TB の使用可能ストレージ
xx28 コレクターおよびプロセッサー	28 個のプロセッサー 128 GB の RAM 40 TB の使用可能ストレージ パフォーマンスを向上させるには、xx28 コレクターおよびプロセッサーを QRadar 3128 (Console) とペアにして使用します。

QRadar アプライアンスについて詳しくは、「*IBM Security QRadar* ハードウェア・ガイド」を参照してください。

QRadar のイベントとフロー

IBM Security QRadar SIEM の主要な機能は、フローとイベントをモニターすることでネットワーク・セキュリティーを管理することです。

イベント・データとフロー・データの重要な相違点は、一般的に (ユーザー・ログインや VPN 接続など) 特定のアクションのログであるイベントは特定の時間に発生し、イベントはその時間にログに記録されますが、フローはセッション内のアクティビティーに応じて、数秒、数分、数時間、または数日間継続される可能性のあるネットワーク・アクティビティーのレコードであるということです。例えば、1 つの Web 要求によって、イメージ、広告、ビデオなど複数のファイルがダウンロードされ、その要求が 5 秒から 10 秒間継続される場合があります。また、Netflix ムービーを観ているユーザーによって、最大で数時間続くネットワーク・セッションが実行される場合もあります。フローとは、2 つのホスト間のネットワーク・アクティビティーのレコードです。

イベント

QRadar は、ネットワーク上にあるログ・ソースからイベント・ログを受け入れます。ログ・ソースとは、ファイアウォールや侵入防止システム (IPS) など、イベント・ログを作成するデータ・ソースです。

QRadar は、syslog、syslog-tcp、および SNMP などのプロトコルを使用して、ログ・ソースからイベントを受け入れます。QRadar では、アウトバウンド接続をセットアップして、SCP、SFTP、FTP、JDBC、Check Point OPSEC、および SMB/CIFS などのプロトコルを使用し、イベントを取得することもできます。

イベント・パイプライン

QRadar コンソールでイベント・データを表示および使用するには、その前に、ログ・ソースからイベントを収集し、イベント・プロセッサーによってイベントを処理しておく必要があります。QRadar オールインワン・アプライアンスはイベント・コレクターやイベント・プロセッサーとして機能し、QRadar コンソールのロールも果たします。

QRadar は、専用のイベント・コレクター・アプライアンスを使用するか、イベント収集サービスやイベント処理サービスがオールインワン・アプライアンスで実行されるオールインワン・アプライアンスを使用して、イベントを収集できます。

以下の図には、イベント・パイプラインのレイヤーが示されています。

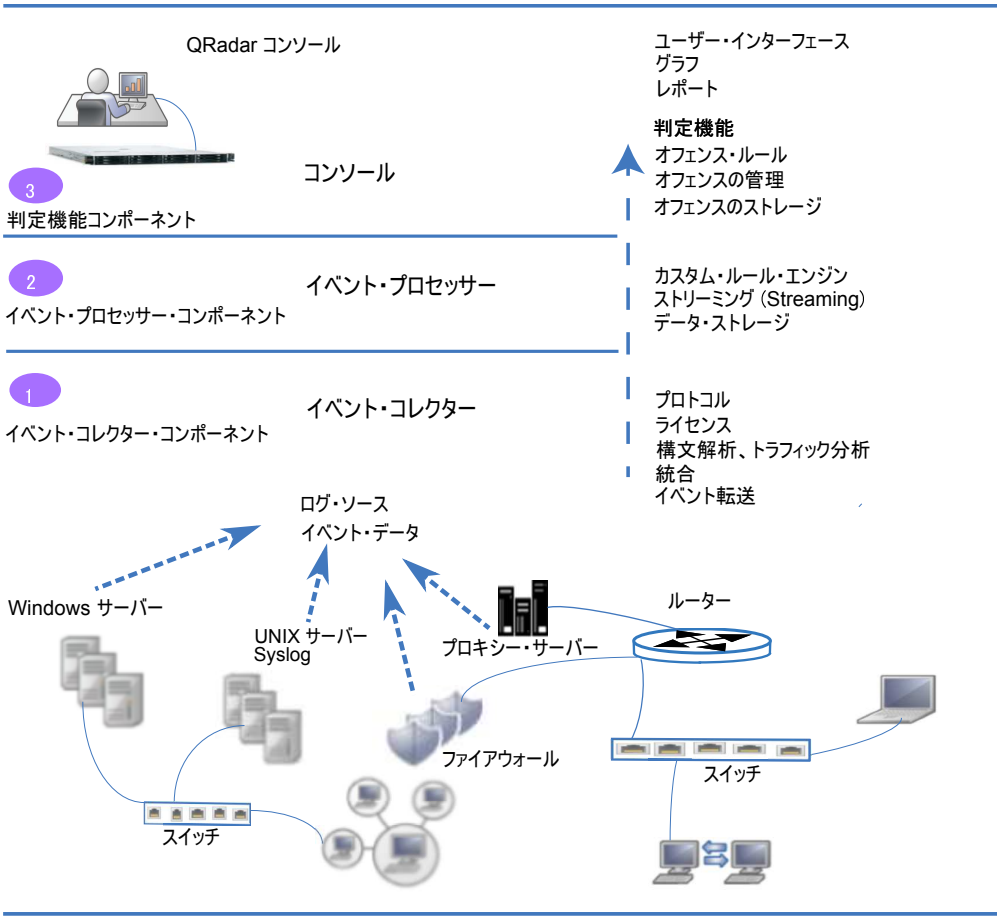


図 2. イベント・パイプライン

イベント収集

イベント・コレクター・コンポーネントには、以下の機能が備わっています。

- プロトコル

  Syslog、JDBC、OPSEC、ログ・ファイル、および SNMP などのログ・ソース・プロトコルを使用してデータを収集します。

- ライセンス・スロットル

  システムに対する着信イベントの数をモニターし、入力キューと EPS ライセンスを管理します。

- 構文解析

  送信元デバイスから未加工のイベントを取得し、QRadar で使用可能なフォーマットにフィールドを構文解析します。

- ログ・ソースのトラフィック分析および自動ディスカバー

  構文解析され、正規化されたイベント・データを、自動ディスカバリーがサポートされている使用可能な DSM に適用します。

- 統合

イベントは構文解析され、イベント全体で共通の属性に基づいて統合されます。

- イベント転送

  システムのルーティング・ルールを適用し、オフサイト・ターゲット、外部 Syslog システム、JSON システム、およびその他の SIEM にデータを転送します。

イベント・コレクターによってファイアウォールなどのログ・ソースからイベントが受け取られると、イベントは入力キューに入れられ、処理されます。
キューのサイズは使用されるプロトコルまたはメソッドによって異なります。また、これらのキューから、イベントは構文解析され、正規化されます。正規化のプロセスには、QRadar が使用できる IP アドレスなどのフィールドを持つフォーマットに未加工のデータを変換する作業が含まれています。

QRadar は、ヘッダーに含まれている送信元 IP アドレスまたはホスト名により、既知のログ・ソースを認識します。
QRadar はイベントを構文解析し、既知のログ・ソースからレコードに統合します。過去に検出されていない新規または不明なログ・ソースからのイベントは、トラフィック分析 (自動検出) エンジンにリダイレクトされます。

新しいログ・ソースが検出されると、ログ・ソースを追加する構成要求メッセージが QRadar コンソールに送信されます。自動検出が無効な場合、またはログ・ソースのライセンス交付を受けた制限を超えた場合、新しいログ・ソースは追加されません。

イベント処理

イベント・プロセッサー・コンポーネントには、以下の機能が備わっています。

- カスタム・ルール・エンジン (CRE)

  カスタム・ルール・エンジン (CRE) は、QRadar が受け取ったイベントを処理し、定義されたルールとそれらを比較して、長期にわたりインシデントに関連するシステムの追跡を行い、ユーザーへの通知を生成する役割を担います。イベントがルールと一致すると、イベント・プロセッサーから、特定のイベントによってルールがトリガーされた QRadar コンソールの判定機能に通知が送信されます。 QRadar コンソールの判定機能コンポーネントによって、オフェンスが作成および管理されます。ルールがトリガーされると、通知、syslog、SNMP、E メール・メッセージ、新規イベント、およびオフェンスなどの応答やアクションが生成されます。

- ストリーミング (Streaming)

  ユーザーがリアルタイム (ストリーミング) で「ログ・アクティビティー」タブからイベントを表示しているときに、リアルタイムのイベント・データを QRadar コンソールに送信します。ストリーミングされたイベントは、データベースからは提供されません。

- イベント・ストレージ (Ariel)

分単位でデータが保管されるイベント用の時系列データベース。データは、イベントが処理される場所に保管されます。

イベント・コレクターは、カスタム・ルール・エンジン (CRE) によってイベントが処理されるイベント・プロセッサーに、正規化されたイベント・データを送信します。 QRadar コンソールに事前定義されている CRE カスタム・ルールとイベントが一致すると、イベント・プロセッサーはルール応答に定義されているアクションを実行します。

QRadar コンソールの判定機能

判定機能コンポーネントには、以下の機能が備わっています。

- オフェンス・ルール

  E メール通知の生成など、オフェンスをモニターし、オフェンスに作用します。

- オフェンスの管理

  「オフェンス」タブから、アクティブなオフェンスを更新したり、オフェンスのステータスを変更したり、オフェンス情報へのユーザー・アクセス権限を提供したりします。

- オフェンスのストレージ

  Postgres データベースにオフェンス・データを書き込みます。

判定機能処理コア (MPC) は、複数のイベント・プロセッサー・コンポーネントからのイベント通知とオフェンスを相関させます。QRadar コンソールまたはオールインワン・アプライアンスのみに判定機能コンポーネントが含まれています。

フロー

QRadar のフローは、IP アドレス、ポート、バイト数およびパケット数、およびその他のデータをフロー・レコードに正規化することでネットワーク・アクティビティーを表します。実質的に、これは 2 つのホスト間のネットワーク・セッションのレコードです。フロー情報を収集および作成する QRadar のコンポーネントは QFlow と呼ばれます。

QRadar フロー・コレクションは、完全なパケット・キャプチャーではありません。複数の時間間隔 (分単位) にまたがるネットワーク・セッションの場合、フロー・パイプラインは、バイトやパケットなどのメトリックに応じて、現在のデータを使用して各分の最後にレコードをレポートします。「最初のパケットの時刻」が同じである複数のレコード (分単位) が QRadar にある場合がありますが、「最後のパケットの時刻」の値は時間の経過とともに増えていきます。

フロー・コレクターによって固有の送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびその他の特定のプロトコル・オプションを持つ最初のパケットが検出されると、フローが開始します。

新しい各パケットが評価されます。バイト数とパケット数がフロー・レコードの統計カウンターに追加されます。統計間隔の最後に、フローのステータス・レコード

がフロー・プロセッサーに送信され、フローの統計カウンターがリセットされます。設定された時間内にフローのアクティビティーが検出されないと、フローが終了します。

QFlow は、次の内部ソースまたは外部ソースからフローを処理できます。

- 外部ソースは、netflow、sflow、jflow などのフロー・ソースです。

  外部ソースは専用のフロー・コレクターに送信することも、QRadar Flow Processor 1705 アプライアンスなどのフロー・プロセッサーに送信することもできます。外部ソースではフローを作成するためにすべてのパケットが処理されるわけではないため、それほど多くの CPU 処理は必要ありません。この構成では、専用のフロー・コレクターとフロー・プロセッサーの両方でフロー・データの受信と作成を行える場合があります。小規模な環境 (50 Mbps 未満) では、1 つのオールインワン・アプライアンスですべてのデータ処理を行える場合があります。
- フロー・コレクターは、SPAN ポート、またはネットワーク TAP に接続して内部フローを収集します。

  QRadar QFlow Collector 1310 は、そのキャプチャー・カードからパケット・キャプチャー・アプライアンスにすべてのパケットを転送できますが、それ自体のすべてのパケットは収集しません。

以下の図には、ネットワークでフローを収集するためのオプションが示されています。

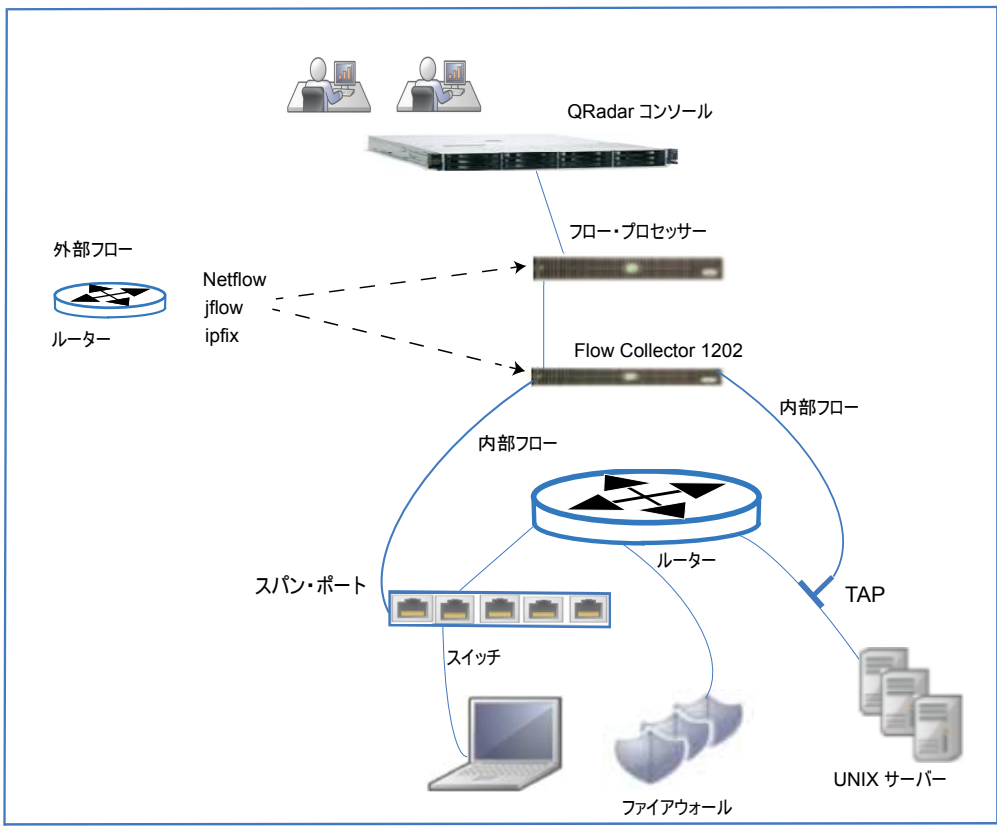


図 3. *QRadar* のフロー

フロー・パイプライン

フロー・コレクター は、SPAN、TAP、およびモニター・セッションなどのモニター・ポートから、あるいは netflow、sflow、jflow などの外部フロー・ソースから収集される未加工のパケットからフロー・データを生成します。次に、このデータは QRadar のフロー・フォーマットに変換され、パイプラインに送信されて処理されます。

フロー・プロセッサーは、以下の機能を実行します。

- フローの重複排除

  フローの重複排除は、複数のフロー・コレクターによってフロー・プロセッサー・アプライアンスにデータが提供される際に、重複フローを削除するプロセスです。
- 非対称再結合

  データが非対称的に提供される場合に、各フローの 2 つのサイドを結合します。このプロセスは、各サイドからのフローを認識し、それらのフローを 1 つのレコードに結合することができます。ただし、フローに 1 つのサイドしかない場合もあります。
- ライセンス・スロットル

  システムに対する着信フローの数をモニターし、入力キューとライセンスを管理します。

- 転送

  オフサイト・ターゲット、外部 Syslog システム、JSON システム、およびその他の SIEM へのフロー・データの送信など、システムのルーティング・ルールを適用します。

フロー・データはカスタム・ルール・エンジン (CRE) を通過し、構成されているルールと照合して関連付けられます。この相関に基づいて、オフェンスを生成することができます。オフェンスは、「オフェンス」タブに表示されます。

第 2 章 QRadar のデプロイメントの概要

IBM Security QRadar アーキテクチャーでは、すべてのソフトウェア・コンポーネントが 1 つのシステムで実行される単一ホスト・デプロイメント環境から、イベント・コレクター、フロー・コレクター、データ・ノード、イベント・プロセッサー、およびフロー・プロセッサーなどのアプライアンスが特定のロールを持っている複数ホスト環境まで、さまざまな規模やトポロジーのデプロイメントがサポートされています。

最初のデプロイメント例では、中規模会社向けの単一オールインワン・アプライアンス・デプロイメントを説明することに焦点を当てます。後の例では、会社の拡大に合わせたデプロイメント・オプションについて説明します。例を使用して、フロー・プロセッサー、イベント・コレクター、およびデータ・ノードなどの QRadar コンポーネントを追加するタイミングや、特定のコンポーネントを同一の場所に配置する必要が生じる状況を説明します。

QRadar デプロイメントの要件は、ネットワークで分析する必要のあるすべてのデータの処理と保管の両方を行うために選択したデプロイメントの容量によって異なります。

デプロイメントを計画する前に、以下の質問を検討してください。

- 会社ではインターネットをどのように使用しますか。ダウンロードと同じぐらいアップロードを行いますか。使用量が増えると、セキュリティー上の問題に遭遇する可能性が高まります。
- モニターする必要のある 1 秒当たりのイベント数 (EPS) と 1 分当たりのフロー数 (FPM) はどのくらいありますか。

  デプロイメント環境が発展するにつれて、EPS および FPM のライセンス・キャパシティー要件が増えます。
- どのくらいの量の情報をどのくらいの期間保管する必要がありますか。

以下の図には、QRadar デプロイメント環境でイベント・データとフロー・データを収集、処理、および保管するために使用できる QRadar コンポーネントが示されています。オールインワン・アプライアンスには、データ収集、処理、保管、モニター、検索、レポート作成、およびオフェンス管理機能が含まれています。

イベント・コレクター はネットワーク内のログ・ソースからイベント・データを収集し、そのイベント・データをイベント・プロセッサーに送信します。フロー・コレクターは、スイッチの SPAN ポートなどのネットワーク・デバイスからフロー・データを収集し、そのデータをフロー・プロセッサーに送信します。両方のプロセッサーによって、コレクターからのデータが処理され、QRadar コンソールにデータが提供されます。プロセッサー・アプライアンスでデータを保管することはできますが、データ・ノードを使用してデータを保管することもできます。QRadar コンソール・アプライアンスは、QRadar デプロイメントのモニター、データ検索、レポート作成、オフェンス管理、および管理を行うために使用されます。

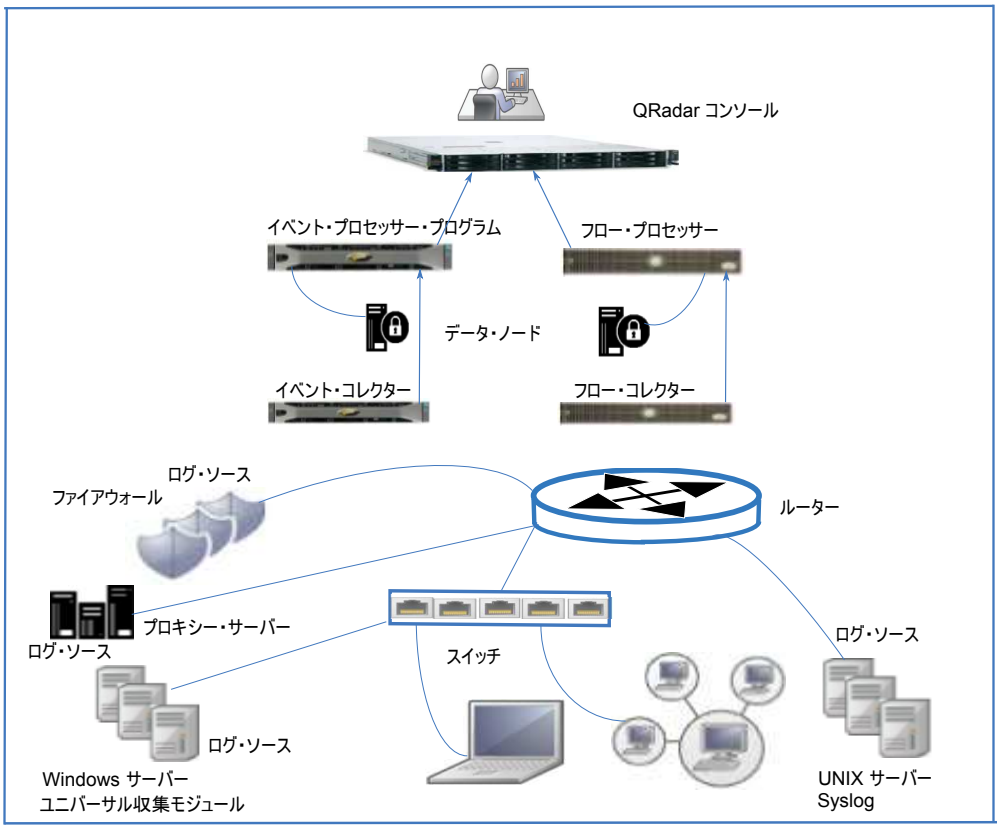


図 4. *QRadar* のイベントおよびフローのコンポーネント

オールインワン・デプロイメント

単一ホストの QRadar デプロイメントでは、ネットワークから、syslog イベント・データ・ログや Windows イベント、さらにはフロー・データなどのデータを収集する単一のサーバーであるオールインワン QRadar アプライアンスを使用できます。

オールインワン・アプライアンスは、インターネットに公開される程度が低い中規模企業や、テストおよび評価に適しています。単一サーバー・デプロイメントは、認証サービスやファイアウォール・アクティビティーなどのネットワーク・アクティビティーやイベントをモニターする企業に適しています。

オールインワン・アプライアンスでは、システムのライセンスやハードウェア仕様によって決定されている特定の能力まで、必要な機能を使用できます。例えば、QRadar 3105 (オールインワン) では、標準で最大 5000 EPS (1 秒当たりのイベント数) および 200,000 FPM (1 分当たりのフロー数) が処理されますが、QRadar 3128 (オールインワン) では、標準で最大 15,000 EPS および 300,000 FPM が処理されます。

製造会社で単一の **QRadar** サーバーをデプロイする

従業員が 1000 名未満の中規模製造会社であるとします。QRadar 3105 オールインワン・アプライアンスをデプロイして、イベント・データとフロー・データを収

集、処理、およびモニターします。このデプロイメントにより、最大で 5,000 イベント/秒 (EPS) と、200,000 フロー/分 (FPM) を収集できます。

次の図には、イベント・ソースとフロー・ソースからデータを収集し、データを処理して、セキュリティー脅威に対する検出、モニター、および対応を行える Web アプリケーションを提供するオールインワン・アプライアンスが示されています。

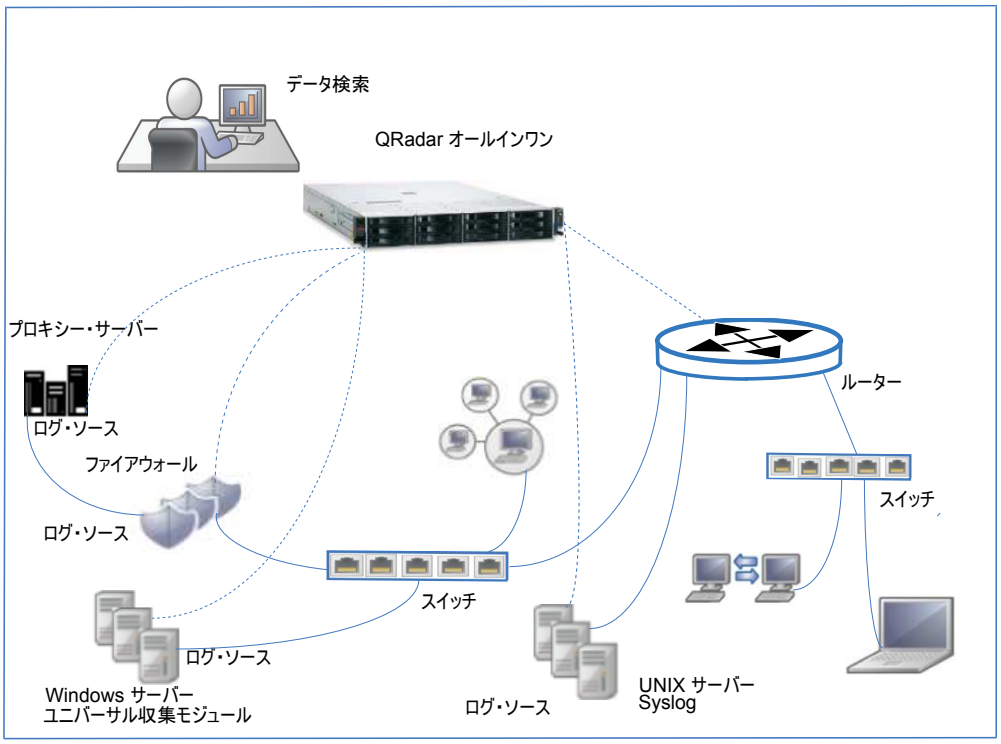


図 5. オールインワン・デプロイメント

QRadar オールインワン・アプライアンスは、以下のタスクを実行します。

- イベントおよびネットワーク・フロー・データを収集し、QRadar が使用できるデータ・フォーマットにデータを正規化します。
- データを分析および保管し、会社に対するセキュリティー脅威を特定します。
- QRadar Web アプリケーションにアクセスできるようにします。

データ・ソースの増加、または処理やストレージのニーズ拡大に合わせて、アプライアンスを追加してデプロイメントを拡張できます。

容量を増やすためのデプロイメントの拡張

業務上、処理またはデータの保管に必要な容量が不足したり、特定のデータ収集で必要になったりするために、IBM Security QRadar オールインワン・アプライアンスに用意されているものを超えて、デプロイメントを作成または拡張する必要が生じることがあります。

QRadar デプロイメントのトポロジーや構成は、ネットワークで分析する必要のあるすべてのデータを収集、処理、および保管するデプロイメントの能力と容量による影響を受けます。

デプロイメントで処理する必要のある 1 秒当たりのイベント数 (EPS) または 1 分当たりのフロー数 (FPM) の概算を得るには、ファイアウォール、プロキシー・サーバー、および Windows ボックスから収集されるログのサイズを使用します。

オールインワン・デプロイメントにイベント・コレクターまたはフロー・コレクターを追加する理由

以下のような場合、デプロイメントにフロー・コレクターまたはイベント・コレクターを追加する必要が生じることがあります。

- データ収集の要件が、オールインワン・アプライアンスの収集能力を超えている。
- オールインワン・アプライアンスがインストールされている場所とは異なる場所でイベントとフローを収集する必要がある。
- オールインワンで、50 Mbps 接続を超える速さの、大規模または高速パケット・ベース・フロー・ソースをモニターしている。

3128 オールインワン・アプライアンスは、最大で 15,000 イベント/秒 (EPS) と、300,000 フロー/分 (FPM) を収集できます。収集の要件がこれよりも大きい場合、イベント・コレクターおよびフロー・コレクターをデプロイメントに追加する必要が生じることがあります。例えば、最大で 3 Gbps を収集する QRadar QFlow Collector 1202 を追加できます。

オールインワン・アプライアンスは、収集されるイベントとフローを処理します。イベント・コレクターおよびフロー・コレクターを追加することで、通常、オールインワン・アプライアンスが検索や他のセキュリティー・タスクに行っている処理を使用できるようになります。

パケット・ベースのフロー・ソースでは、フロー・プロセッサーに接続されているか、フロー・プロセッサー・アプライアンスがないデプロイメントでオールインワン・アプライアンスに接続されているフロー・コレクターが必要です。 NetFlow や IPFIX などの外部フロー・ソースは、フロー・プロセッサーまたはオールインワン・アプライアンスで直接収集できます。

デプロイメントへのリモート・コレクターの追加

より多くのイベントをローカルで収集し、リモート・ロケーションからイベントとフローを収集する必要がある場合、QRadar イベント・コレクター または QRadar フロー・コレクター を追加してデプロイメントを拡張します。

例えば、QRadar オールインワン・デプロイメント環境のある製造会社が、e-コマースおよびリモート販売オフィスを追加するとします。現在、セキュリティー脅威をモニターする必要があり、PCI 監査の準備もしなくてはなりません。

従業員をさらに雇用し、インターネットの使用状況は大部分がダウンロードであった状況から、従業員とインターネットの間の両方向トラフィックに変わります。会社の詳細は次のとおりです。

- 現在のイベント/秒 (EPS) のライセンスは 1000 EPS です。
- 販売オフィスでイベントとフローを収集し、e-コマース・プラットフォームからイベントを収集する必要があります。

- e-コマース・プラットフォームからのイベント収集では、最大で 2000 イベント/秒 (EPS) が必要です。
- リモート販売オフィスからのイベント収集では、最大で 2000 イベント/秒 (EPS) が必要です。
- フロー/分 (FPM) ライセンスは、リモート・オフィスでフローを収集するには十分です。

以下を実行します。

1. 本社に e-コマース・プラットフォームを追加した後、リモート販売オフィスを開きます。
2. 本社でオールインワン・アプライアンスにインターネットを介してデータを送信するイベント・コレクターとフロー・コレクターをリモート販売オフィスでインストールします。
3. EPS ライセンスを 1000 EPS から 5000 EPS にアップグレードし、リモート・オフィスで収集される追加イベントに対する要件を満たします。

以下の図には、イベント・コレクターとフロー・コレクターがリモート・オフィスに追加される場合のデプロイメントの例が示されています。

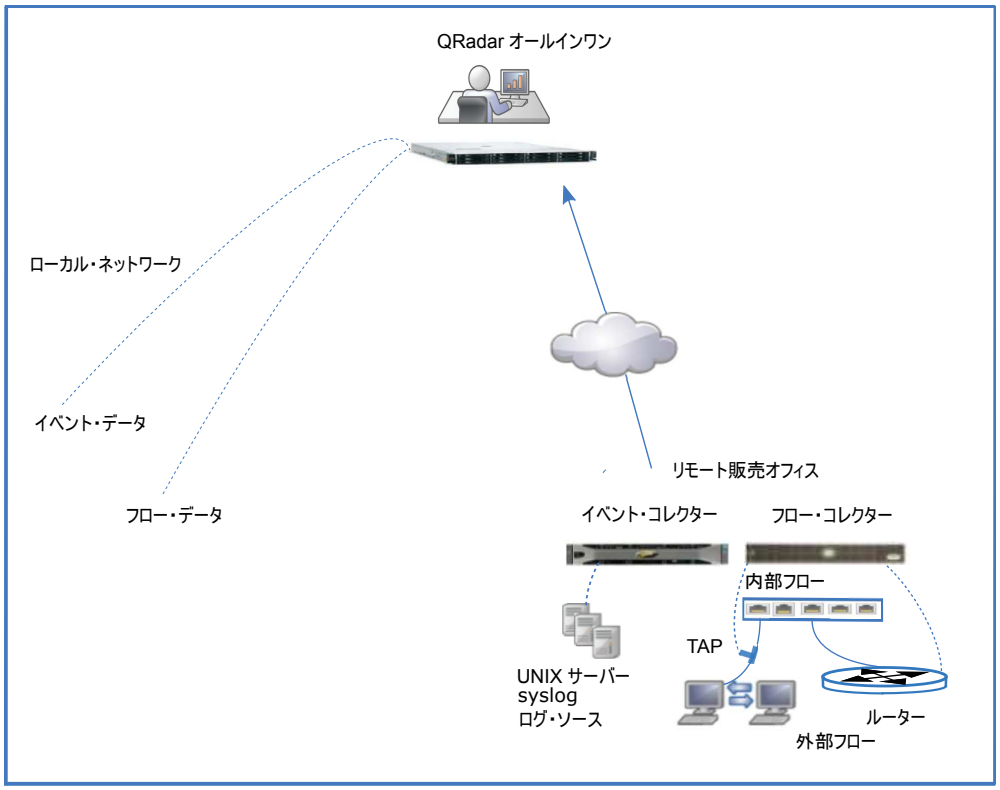


図 6. リモート・オフィスでのコレクター

このデプロイメントでは、次の処理が行われます。

- リモート・オフィスで、イベント・コレクターはログ・ソースからデータを収集し、フロー・コレクターはルーターとスイッチからデータを収集します。コレクターはデータを統合し、正規化します。

- コレクターはデータを圧縮し、広域ネットワークを介してオールインワン・アプライアンスに送信します。
- オールインワン・アプライアンスはデータを処理し、保管します。
- 会社は QRadar Web アプリケーションを使用してネットワーク・アクティビティーをモニターし、検索、分析、レポート作成、およびアラートとオフェンスの管理を行います。
- オールインワンは、ローカル・ネットワークからイベントを収集し、処理します。

オールインワン・デプロイメントへの処理能力の追加

イベント・プロセッサーとフロー・プロセッサーを QRadar デプロイメントに追加して、処理能力を高め、ストレージを増やします。プロセッサーを追加すると、処理やストレージに要する負荷が専用サーバーに移動されることによって、QRadar コンソールのリソースが解放されます。

イベント・プロセッサーまたはフロー・プロセッサーをオールインワン・アプライアンスに追加すると、オールインワンは QRadar コンソールのように動作します。オールインワン・アプライアンスの処理能力はプロセッサーによって送信されるデータの管理および検索専用に使用されるようになり、データはコンソールではなく、イベント・プロセッサーや他のストレージ・デバイスに保管されるようになります。

多くの場合、以下の理由でイベント・プロセッサーおよびフロー・プロセッサーを QRadar デプロイメントに追加します。

- デプロイメントが発展したため、作業負荷がオールインワン・アプライアンスの処理能力を超える。
- セキュリティー・オペレーション・センターで、より多くの同時検索を行うアナリストをさらに雇用する。
- モニター対象データの種類が増え、そのデータの保存期間が長くなったため、処理およびストレージ要件が増える。
- セキュリティー・アナリスト・チームが拡大したため、検索のパフォーマンスを高める必要がある。

複数の同時 QRadar 検索を実行したり、モニターするログ・ソースの種類を増やしたりすると、オールインワン・アプライアンスの処理パフォーマンスに影響が及ぼされます。検索数を増やしたり、モニター対象データの量を増やしたりする場合は、イベント・プロセッサーおよびフロー・プロセッサーを追加して、QRadar デプロイメントのパフォーマンスを高めてください。

最も強力なオールインワン・アプライアンスでの 15,000 EPS および 300,000 FPM を超えて QRadar デプロイメントを拡大する場合は、プロセッサー・アプライアンスを追加してデータを処理する必要があります。

例: デプロイメントへの QRadar イベント・プロセッサー の追加

最大で 40,000 EPS で収集および処理する QRadar Event Processor 1628 を追加できます。デプロイメントに QRadar Event Processor 1628 を追加するたびに、

40,000 EPS 分の能力が追加されます。最大で 1,200,000 FPM で収集および処理する QRadar Flow Processor 1728 を追加します。

QRadar Event Processor 1628 は、コレクターであり、プロセッサーでもあります。分散ネットワークを使用している場合、イベント・コレクターを追加して負荷を分散し、イベント・プロセッサー上のシステム・リソースを解放することをお勧めします。

次の図には、イベント・プロセッサーとフロー・プロセッサーが QRadar 3128 (All-in-One) に追加されることで処理能力が追加され、以下の変更が行われる様子を示しています。

- イベントおよびフローの処理が、オールインワン・アプライアンスからイベントおよびフローのプロセッサーに移されます。
- イベント処理能力が 40,000 EPS まで増加します。これには、オールインワンであったときの 15,000 EPS が含まれています。
- フロー処理能力が 1,200,000 FPM まで増加します。これには、オールインワンであったときの 300,000 FPM が含まれています。
- イベントおよびフロー・コレクターによって送信されるデータは、イベントおよびフローのプロセッサーで処理され、保管されます。

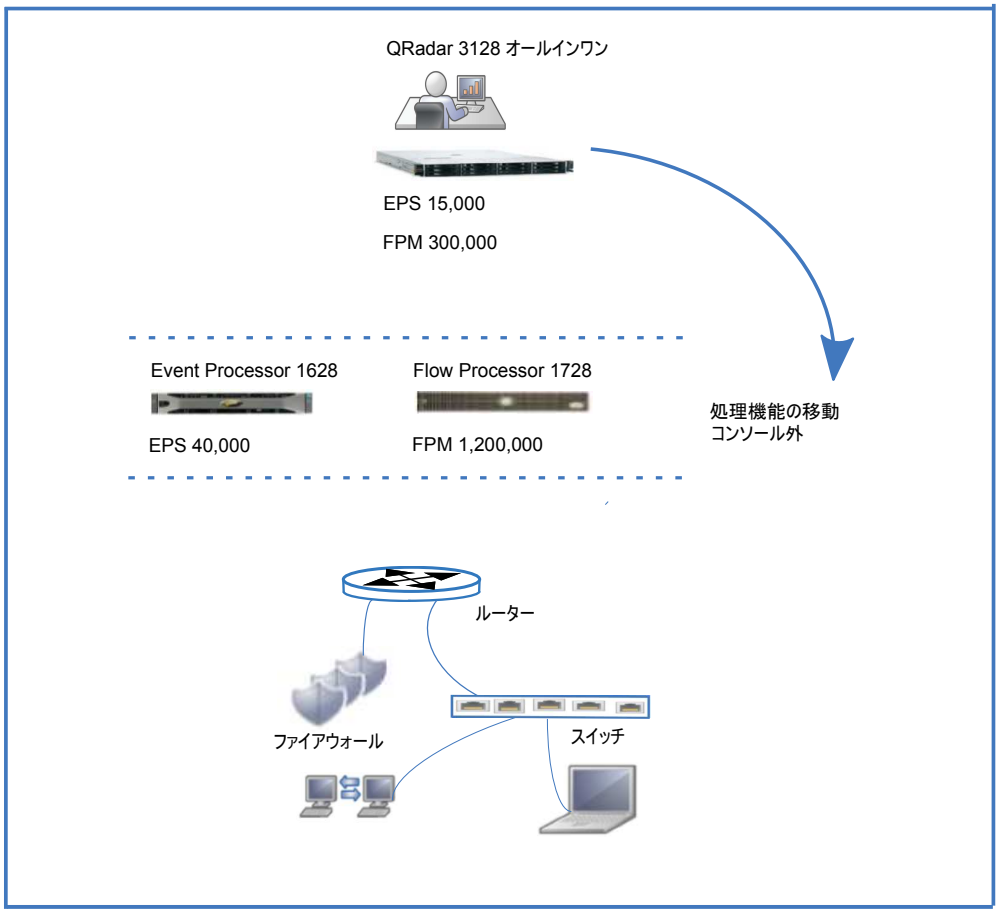


図 7. 処理能力の追加

イベント・プロセッサーおよびフロー・プロセッサーを QRadar コンソールと同じネットワークにインストールすると、検索パフォーマンスはより高速になります。

プロセッサーとコレクターを追加すると、QRadar デプロイメントの処理能力が拡張されます。また、デプロイメントのストレージ容量を増やすこともできます。会社のデータ保存のニーズが、トラフィックの増加や保存ポリシーの変更によって増える場合があります。デプロイメントにデータ・ノードを追加して、データ・ストレージ容量を拡張し、検索パフォーマンスを高めます。

プロセッサーにコレクターを追加するタイミング

イベント・コレクターおよびフロー・コレクターをイベント・プロセッサーおよびフロー・プロセッサーに追加する理由は、コレクターをオールインワン・アプライアンスに追加する理由と同じです。

- データ収集の要件が、プロセッサーの収集能力を超えている。
- プロセッサーがインストールされている場所とは異なる場所でイベントとフローを収集する必要がある。
- パケット・ベースのフロー・ソースをモニターしている。

注: イベント・コレクターはイベントをバッファーに入れることができますが、フロー・コレクターはフローをバッファーに入れることはできません。

コンソールと同じネットワーク上にプロセッサーがインストールされている場合、検索パフォーマンスは高まるため、コレクターをリモート・ロケーションに追加した後、そのデータをプロセッサーに送信すると、QRadar 検索のスピードが上がります。

地理的に分散されたデプロイメント

地理的に分散されたデプロイメントでは、リモート・データ・センターへの接続が断続的または不十分な場合、IBM Security QRadar デプロイメントがその影響を受ける可能性があります。元の場所にデータを維持しなければならないという特定の地方自治体や国の規制に従う場合など、地域の規制による影響を受ける場合もあります。このような状況では両方とも、コレクターをサイトに維持しておく必要があります。データを元の場所に維持する必要がある場合、プロセッサーをサイトに維持する必要も生じます。

例えば、会社が拡大し続け、その拡大によってネットワーク内のアクティビティーが増えるだけではなく、QRadar デプロイメントを他の国に展開する必要が生じることもあります。データ保存に関する法律は国ごとに異なるため、QRadar のデプロイメントはそれらの規制を考慮して計画する必要があります。

以下のような状況がこれに当てはまります。

- 会社で、接続が断続的なオフィス・ロケーションの 1 つからイベント・データを収集する必要があります。
- 会社は、データが収集される国のデータ保存規制に準拠する必要があります。例えば、ドイツでデータを国内に留めておく必要がある場合、そのデータをドイツ国外で保管することはできません。

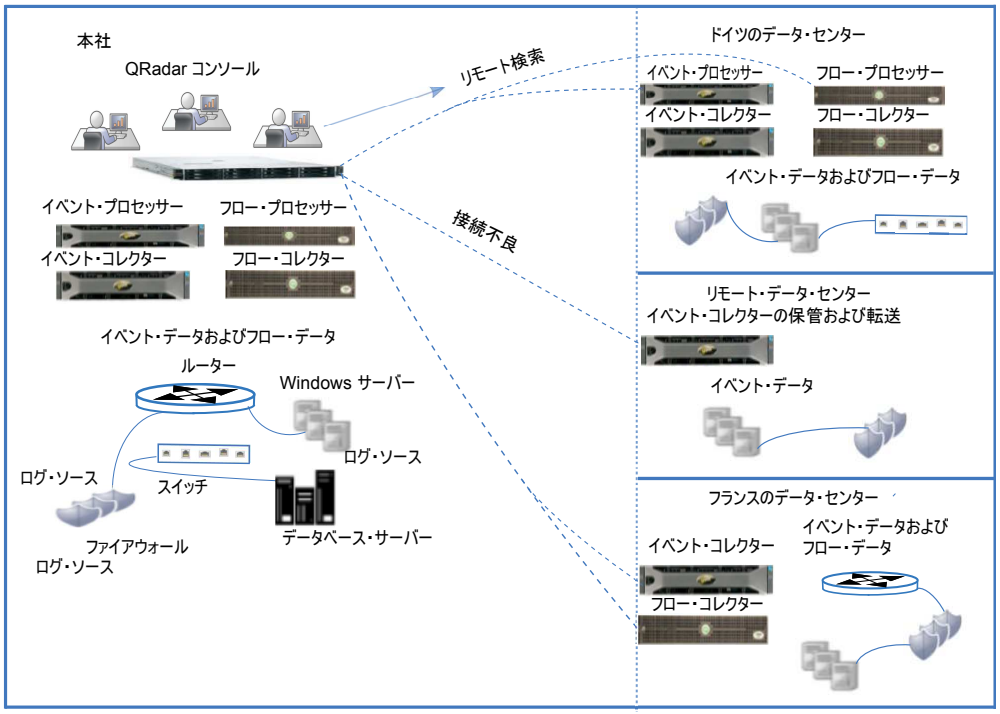


図 *8.* 地理的に分散されたデプロイメント

地理的に分散されたデプロイメントで、次の処理が行われます。

- 会社は、現地のデータ関連法に準拠するために、ドイツのデータ・センターにコレクターとプロセッサーをインストールします。
- 会社はフランスのデータ・センターにコレクターをインストールし、コレクターによってデータが本社に送信されるようにします。このデータは本社で処理され、保管されます。 QRadar コンソールと同じ高速ネットワーク・セグメントにプロセッサー・アプライアンスを配置することで、検索速度が上がります。
- 会社は、リモート・データ・センターに、スケジュール設定され、レート制限された転送接続を使用するストア・アンド・フォワード・イベント・コレクターを追加します。スケジュール設定され、レート制限された接続により、断続的なネットワーク接続が補われ、通常の業務時間中にさらに帯域幅が必要になる状況が回避されます。

リモート・プロセッサーでデータの検索を常に行う場合、QRadar コンソールと同じ高速ネットワーク・セグメントにプロセッサーを配置することをお勧めします。QRadar コンソールとリモート・プロセッサーの間の帯域幅が十分ではない場合、特に複数の同時検索を行うと、検索の待ち時間が長くなる可能性があります。

QRadar Vulnerability Manager デプロイメント

IBM Security QRadar Vulnerability Manager をデプロイして、ネットワーク内の脆弱性を見つけて、管理します。IBM BigFix® や IBM Security SiteProtector™ などのアドオン機能を統合することで、ネットワーク・セキュリティーを強化します。

IBM Security QRadar Vulnerability Manager は、ネットワーク・デバイス、アプリケーション、およびソフトウェア上の脆弱性を検出し、脆弱性にコンテキストを追加し、ネットワーク上のアセット・リスクに優先順位を付けて、検出された脆弱性の修復をサポートします。

QRadar Risk Manager を統合して保護を強化できます。これにより、ポリシー・コンプライアンスに基づき、アセットに対して、ネットワーク・トポロジー、アクティブな攻撃パス、およびハイリスク・アセットによるリスク・スコア調整を行えます。 QRadar Vulnerability Manager と QRadar Risk Manager は 1 つのオファリングに結合されており、どちらも単一の基本ライセンスを通じて有効化されます。

インストールする製品によって、および IBM Security QRadar をアップグレードするか新規システムをインストールするかによって、「脆弱性」タブが表示されない場合があります。IBM Security QRadar Vulnerability Manager にアクセスするには、「脆弱性」タブを使用します。IBM Security QRadar SIEM をインストールする場合は、「脆弱性」タブが一時ライセンス・キーを使用してデフォルトで有効化されます。QRadar Log Manager をインストールする場合は、「脆弱性」タブが有効化されません。「試用」オプションを使用して、QRadar Vulnerability Manager を 30 日間試用できます。 QRadar Vulnerability Manager のライセンスを別個に購入することで、ライセンス・キーを使用してこれを有効化できます。アップグレードについて詳しくは、「*IBM Security QRadar Upgrade Guide*」を参照してください。

QRadar Vulnerability Manager コンポーネント

以下は、QRadar Vulnerability Manager プロセッサーの情報です。

- スキャン・プロセッサーは、スキャンをスケジューリングおよび管理し、ネットワーク全体で分散される可能性のあるスキャナーに作業を委任します。
- QRadar デプロイメント内で使用できるスキャン・プロセッサーは 1 つのみです。
- オールインワン・システムに QRadar Vulnerability Manager をインストールし、ライセンス交付を受けると、脆弱性プロセッサーがご使用の QRadar コンソールに自動的にデプロイされ、スキャン・コンポーネントが組み込まれます。
- 脆弱性プロセッサーには、デフォルトでスキャン・コンポーネントが付属しています。また、必要に応じて、脆弱性プロセッサーをデプロイメント内の他の管理対象ホストに移動することができます。
- 600 管理対象ホスト・アプライアンスを追加し、QRadar Vulnerability Manager を初めて使用するときに、スキャン・プロセッサーが 600 管理対象ホスト・アプライアンスに割り当てられます。
- スキャン・プロセッサーは処理ライセンスによって管理されます。このライセンスによって、QRadar Vulnerability Manager で処理できるアセットの最大数が決まります。
- スキャン・プロセッサーは、QRadar コンソール または管理対象ホストで実行できます。

以下は、QRadar Vulnerability Manager スキャナーの情報です。

- スキャナーは仮想マシン上にデプロイすることも、ソフトウェアのみとしてデプロイすることもできます。
- QRadar Vulnerability Manager スキャナー専用スキャナー・アプライアンスをデプロイできます。これは、610 アプライアンスです。
- スキャナーは、QRadar コンソールにデプロイできます。または、フロー・コレクター、フロー・プロセッサー、イベント・コレクター、イベント・プロセッサー、またはデータ・ノードなどの管理対象ホストにデプロイできます。
- スキャナーでスキャンできるアセットの数は、スキャナーの容量によって決まります。ライセンス設定によって影響を受けることはありません。

コンポーネントおよびスキャン・プロセス

スキャン・ジョブは、1 つのプロセッサーと 1 つのスキャナー・コンポーネントによって実行されます。以下の図には、スキャン・コンポーネントと、実行するプロセスが示されています。

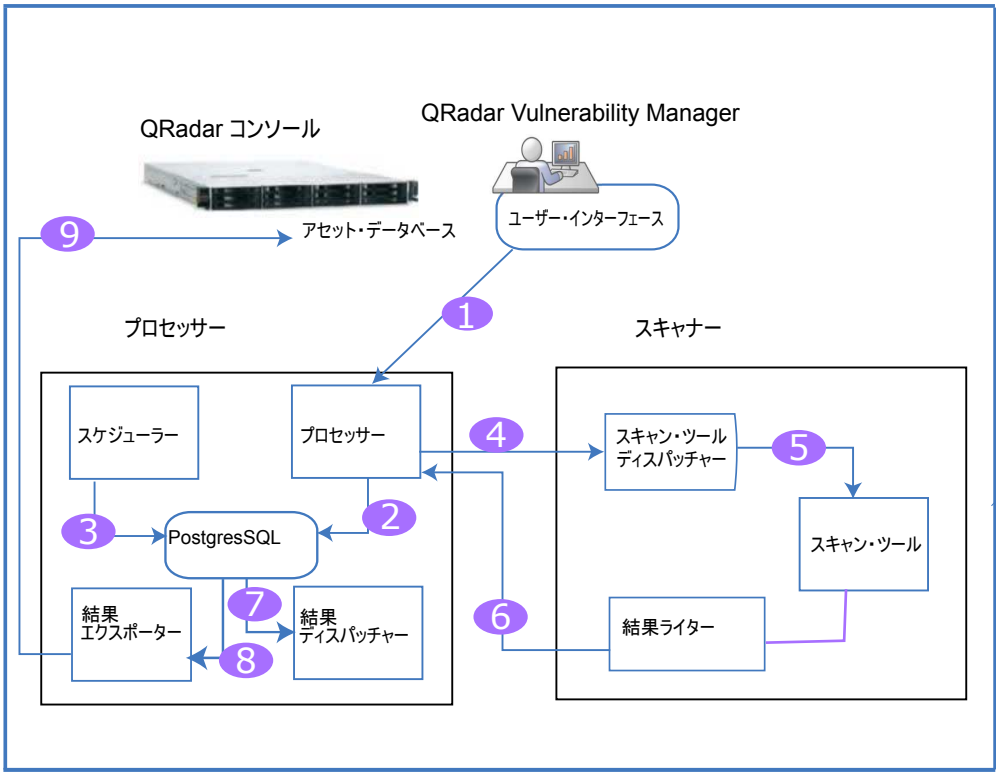


図 9. スキャン・コンポーネントおよびプロセス

以下のリストには、スキャン・プロセスのステップが説明されています。

1. アセットの IP アドレス、スキャンのタイプ、および認証対象スキャンに必要な資格情報などのパラメーターを指定することで、スキャン・ジョブを作成します。
2. スキャン・ジョブはプロセッサーによって受け入れられ、ジョブを実行するタイミングを決定するスケジューリング情報と共に、データベースに記録されて追加されます。

3. スケジューラー・コンポーネントは、スキャンのスケジューリングを管理します。スケジューラーによってスキャンが開始されると、スケジューラーは必要なツールのリストを判別し、呼び出されるまでそれらをキューに入れます。その後、関連するスキャナーにツールが割り当てられます。
4. 固有のスキャナー ID を送信してスキャン・プロセッサーが実行する必要のあるスキャン・ツールに対して、スキャナーはスキャン・プロセッサーを継続的にポーリングします。特定のスキャナーに関連する、キューに入れられたツールがスケジューラーにある場合、そのツールはスキャナーに送信されて呼び出されます。

   QRadar Vulnerability Manager はアタック・ツリー方式を使用してスキャンを管理し、どのツールが起動されるかを決定します。アセット・ディスカバリー、ポート/サービス・ディスカバリー、サービス・スキャン、およびパッチ・スキャンのフェーズがあります。
5. ディスパッチャーによって、リスト内の各スキャン・ツールが実行および管理されます。実行されるツールごとに、ディスパッチャーはスキャン・ツールが開始し、完了したことを示すメッセージをプロセッサーに送信します。
6. スキャン・ツールからの出力が結果ライターによって読み取られます。その後、結果ライターによってそれらの結果がプロセッサーに渡されて戻されます。
7. 結果ディスパッチャーは、スキャン・ツールからの未加工の結果を処理し、Postgres データベースに記録します。
8. 結果エクスポーターはプロセッサー・データベースで完了したスキャンを検出し、その結果を QRadar コンソールにエクスポートします。
9. エクスポートされた結果は、QRadar データベースに追加されます。ユーザーはこのデータベースでスキャン結果を確認し、管理できます。

オールインワン・デプロイメント

オールインワン・システムから QRadar Vulnerability Manager を実行できます。ここでは、スキャン機能と処理機能はコンソールに組み込まれています。以下に、基本的なセットアップで実行できることを示します。

- 最大で 255 個のアセットをスキャンする。
- 無制限の自動検出スキャンを実行する。
- DMZ スキャンでホスト・スキャナーを使用する。
- QRadar に統合されたサード・パーティー・スキャナーからスキャン・データを管理する。
- あらゆる管理対象ホストにスキャナーをデプロイする。
- 無制限のスタンドアロン・ソフトウェアまたは仮想スキャナーをデプロイする。

デプロイメントの拡張

デプロイメントの発展に合わせて、処理機能を QRadar コンソールから移動し、リソースを解放する必要が生じたり、スキャナーをアセットの近くにデプロイする必要が生じたりする場合があります。

デプロイメントにスキャナーを追加する理由を以下に示します。

- QRadar Vulnerability Manager プロセッサーとは異なる地理的地域でアセットをスキャンするため。
- 短時間で多数のアセットを同時にスキャンする必要があるため。
- ログ・ソースであるファイアウォールを介したスキャンを回避するために、スキャナーを追加する必要があるため。また、ファイアウォールをバイパスするスキャナー・ホストにインターフェースを追加することで、ネットワークに直接スキャナーを追加することも検討できます。

次の図には、管理対象ホストにデプロイされている外部スキャンとスキャナーを含むスキャン・デプロイメントが示されています。

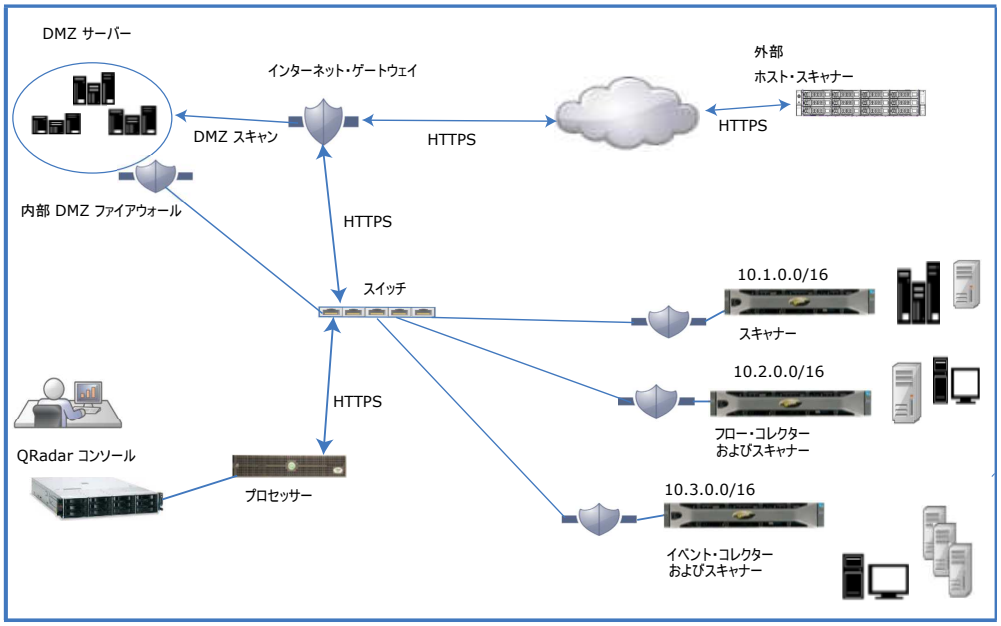


図 *10.* スキャン・デプロイメント

DMZ ホスト・スキャナー

ホスト・スキャナーは、パブリック IP アドレスを使用してインターネットから DMZ をスキャンします。DMZ 内のアセットで脆弱性がないかをスキャンする場合、DMZ にスキャナーをデプロイする必要はありません。ネットワークの外部にあるホスト IBM スキャナーを使用して QRadar Vulnerability Manager を構成する必要があります。詳しくは、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

QRadar Vulnerability Manager の統合

IBM Security QRadar Vulnerability Manager と IBM BigFix の統合により、修正可能な脆弱性をフィルタリングし、優先順位を付けることができます。 BigFix には、IT 運用とセキュリティーの間で共有される可視性と制御機能が備わっています。 BigFix は、QRadar Vulnerability Manager によって特定され、 BigFix に送信される優先度の高い脆弱性に Fixlet を適用します。Fixlet とは、特定の脆弱性を修復するために、アセットまたはエンドポイントにデプロイするパッケージです。

QRadar Vulnerability Manager は、侵入防止システム (IPS) ポリシーを指示できるように、IBM Security SiteProtector と統合されます。IBM Security SiteProtector を構成すると、スキャンによって検出された脆弱性が IBM Security SiteProtector に自動的に転送されます。IBM Security SiteProtector は、統合が構成された後でのみ実行された QRadar Vulnerability Manager スキャンからの脆弱性データを受信します。 IBM Security SiteProtector に接続します。

サード・パーティー・スキャナー

QRadar Vulnerability Manager によって、スキャン・データのソースに関係なく、効率的な脆弱性管理プラットフォームが提供されます。 QRadar Vulnerability Manager は、Nessus、nCircle、および Rapid 7 などのサード・パーティー・スキャナーとシームレスに統合されます。

以下のオプションを取得するには、QRadar Vulnerability Manager スキャンが必要です。

- イベント・ドリブンおよびオンデマンドのスキャン
- アセット・データベースおよびウォッチリスト・ベースのスキャン
- 既存の QRadar アプライアンスおよび管理対象ホストからのスキャン
- どのスキャン結果にも存在しない、新たに公開された脆弱性の検出

以下のオプションを取得するには、QRadar Risk Manager が必要です。

- アセット、脆弱性、およびトラフィック・ベースの脆弱性管理
- 調整された脆弱性スコアと、コンテキスト認識によるリスク・スコアリング

QRadar Risk Manager および QRadar Vulnerability Manager

IBM Security QRadar Risk Manager と IBM Security QRadar Vulnerability Manager を統合して、ネットワーク・セキュリティーを強化します。スキャン・データなどのデータ・ソースにより、QRadar Risk Manager はネットワーク内のセキュリティー、ポリシー、およびコンプライアンスのリスクを特定し、リスクが悪用される確率を算出できるようになります。

QRadar Vulnerability Manager と QRadar Risk Manager は 1 つのオファリングに結合されており、どちらも単一の基本ライセンスを通じて有効化されます。

QRadar Risk Manager 700 アプライアンスを追加すると、以下の機能を使用できるようになります。

- コンプライアンス評価
- リスクの高い脆弱性を素早く特定するのに役立つ、脆弱性データとリスク・スコアに基づいたリスク・ポリシー。
- ネットワーク・トポロジー・ビューを介した、潜在的脅威と非トラステッド・ネットワークからの潜在的エクスプロイト・パスに対する可視性。
- リスク・ポリシー・ベースのフィルタリング。
- トポロジーの可視化。
- 脆弱性評価でのフォールス・ポジティブの削減。
- ファイアウォールと侵入防止システム (IPS) によってブロックされる脆弱性に対する可視性。

QRadar Risk Manager アプライアンス

QRadar Risk Manager は、QRadar Risk Manager 700 アプライアンスとは別個にインストールします。

QRadar Risk Manager アプライアンスをセットアップおよび構成する前に、IBM Security QRadar コンソールをインストールする必要があります。 QRadar および QRadar Risk Manager を同じネットワーク・スイッチにインストールすることをお勧めします。

デプロイメントごとに必要な QRadar Risk Manager アプライアンスは 1 つのみです。

以下の図には、スキャナーと QRadar Risk Manager が含まれているデプロイメントが示されています。

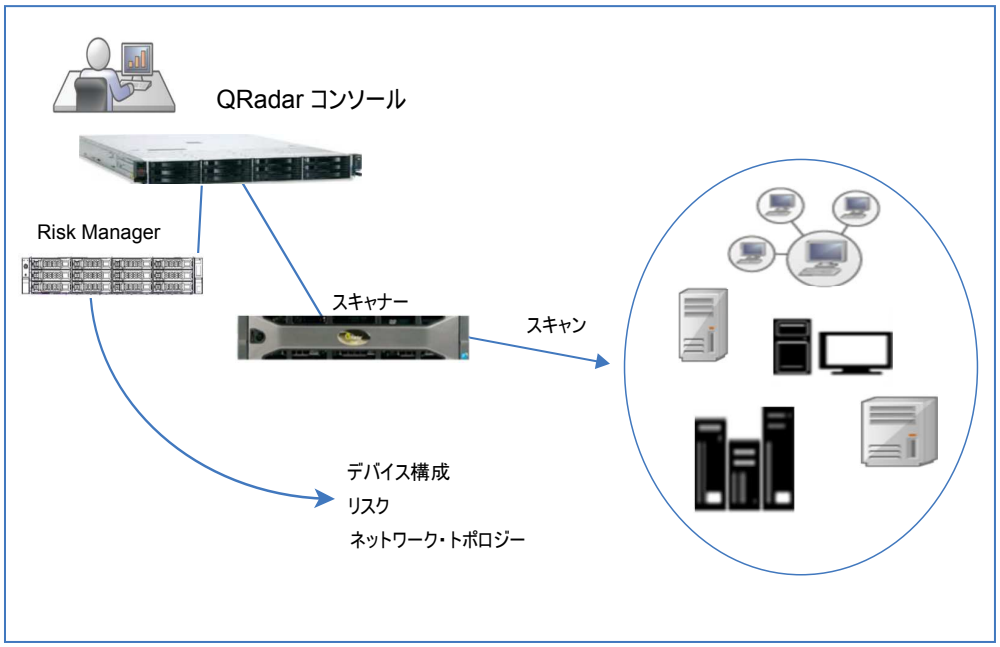


図 *11. Risk Manager* を使用したスキャン・デプロイメント

Risk Manager を使用して、以下のタスクを実行します。

- リスクを集中管理する。
- ネットワーク・トポロジーを表示およびフィルタリングする。
- デバイス構成をインポートおよび比較する。
- ネットワーク・デバイス間の接続を表示する。
- ファイアウォール・ルールを検索する。
- 既存のルールと、トリガーされたルールのイベント・カウントを表示する。
- デバイスとパスを検索する。
- ネットワーク接続を照会する。
- デバイス構成の更新で考えられる結果をシミュレートする。
- ネットワークをモニターして監査し、コンプライアンスを確保する。

- 仮想モデルに対する脅威または攻撃をシミュレートする。
- 脆弱性を検索する。

Forensics および完全なパケット収集

デプロイメント環境で IBM Security QRadar Incident Forensics を使用し、潜在的攻撃者のアクションをステップごとに再トレースしたり、悪意のあるネットワーク・セキュリティー・インシデントの疑いがあるものに対して詳細な Forensics 調査を行ったりします。

QRadar Incident Forensics は、セキュリティー・インシデントに関連する未加工のネットワーク・データを再構成して、元の形式に戻します。

QRadar Incident Forensics は IBM QRadar Security Intelligence Platform と統合されており、多数のサード・パーティー・パケット・キャプチャー・オファリングと互換性があります。

QRadar Incident Forensics には、デプロイされているネットワーク・パケット・キャプチャー (PCAP) デバイスが他にない場合に、QRadar Incident Forensics で使用されるデータを保管および管理するための、オプションの QRadar Packet Capture アプライアンスが用意されています。任意の数のアプライアンスを、ネットワークまたはサブネットワークにタップとしてインストールし、未加工のパケット・データを収集できます。

QRadar Packet Capture 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含めることができます。

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。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 プロセッサー ホストを管理します。

QRadar Incident Forensics プロセッサー
: 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 プロセッサー 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 スタンドアロン
: 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 スタンドアロン 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。

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。

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。

オールインワン・デプロイメント

スタンドアロン・デプロイメントやオールインワン・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 スタンドアロン をインストールします。

以下の図には、基本的な QRadar Incident Forensics オールインワン・デプロイメントが示されています。

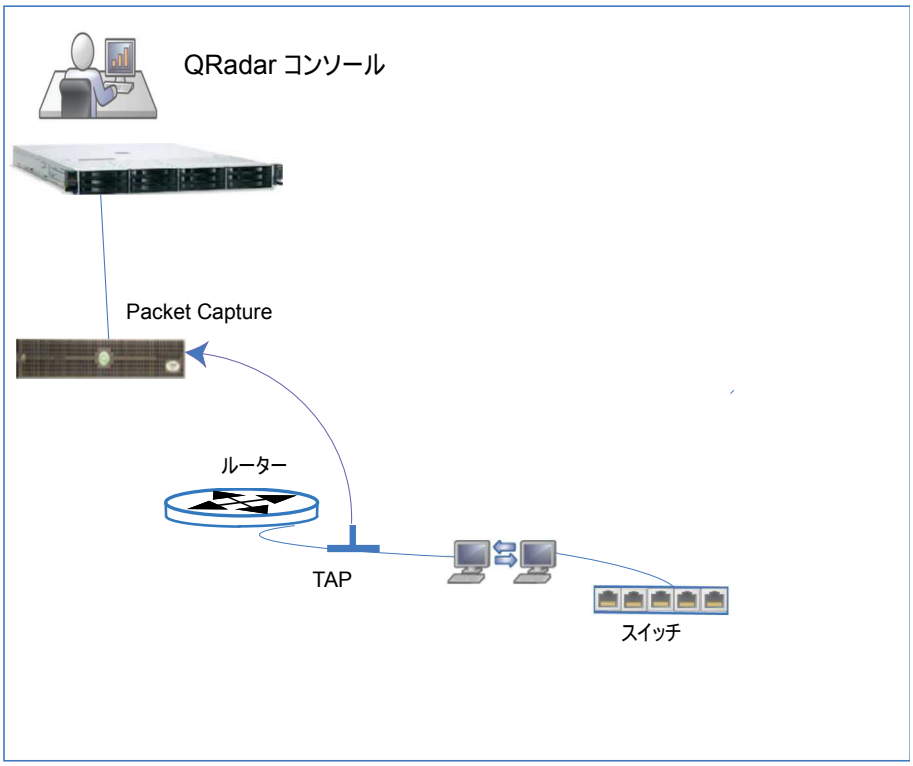


図 *12.* オールインワン・デプロイメント

分散デプロイメント

分散デプロイメントでは、以下の 3 つのアプライアンスを使用できます。

- QRadar コンソール
- QRadar Packet Capture 管理対象ホスト (QRadar Packet Capture プロセッサー)
- 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。

以下の図には、QRadar Incident Forensics 分散デプロイメントが示されています。

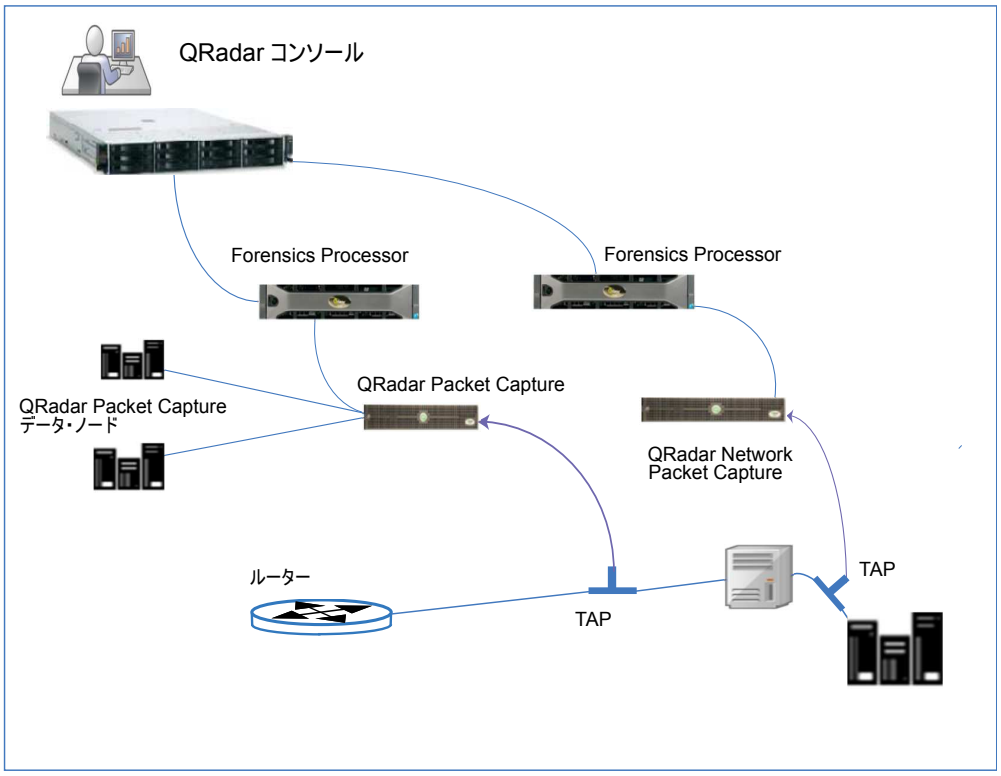


図 *13.* 分散デプロイメント

以下の図には、10G Napatech ネットワーク・カードを使用する IBM QRadar QFlow Collector 1310 から QRadar Packet Capture アプライアンスに転送されるパケットが示されています。

QRadar QFlow Collector は、専用の Napatech モニタリング・カードを使用して、着信パケットをカード上のあるポートから IBM Security QRadar Packet Capture アプライアンスに接続する別のポートへとコピーします。

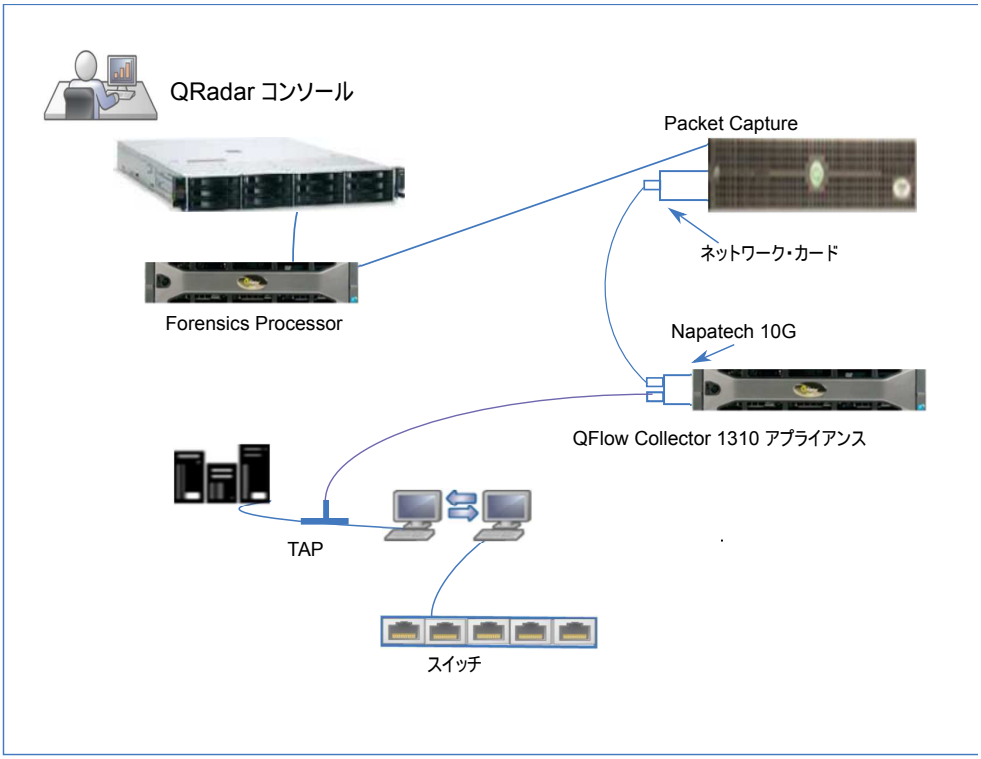


図 *14.* パケット転送

QRadar Packet Capture へのパケットの転送

生データ・パケットを IBM Security QRadar QFlow Collector 1310 アプライアンスに送信することにより、ネットワーク・トラフィックをモニターできます。QRadar QFlow Collector は、専用の Napatech モニタリング・カードを使用して、着信パケットをカード上のあるポートから IBM Security QRadar Packet Capture アプライアンスに接続する別のポートへとコピーします。

10G Napatech ネットワーク・カードを備えた QRadar QFlow Collector 1310 が既にある場合、トラフィックを QRadar Packet Capture にミラーリングできます。

次の図に示すように、10G Napatech ネットワーク・カードを備えた QRadar QFlow Collector 1310 が既にある場合、トラフィックを QRadar Packet Capture にミラーリングできます。

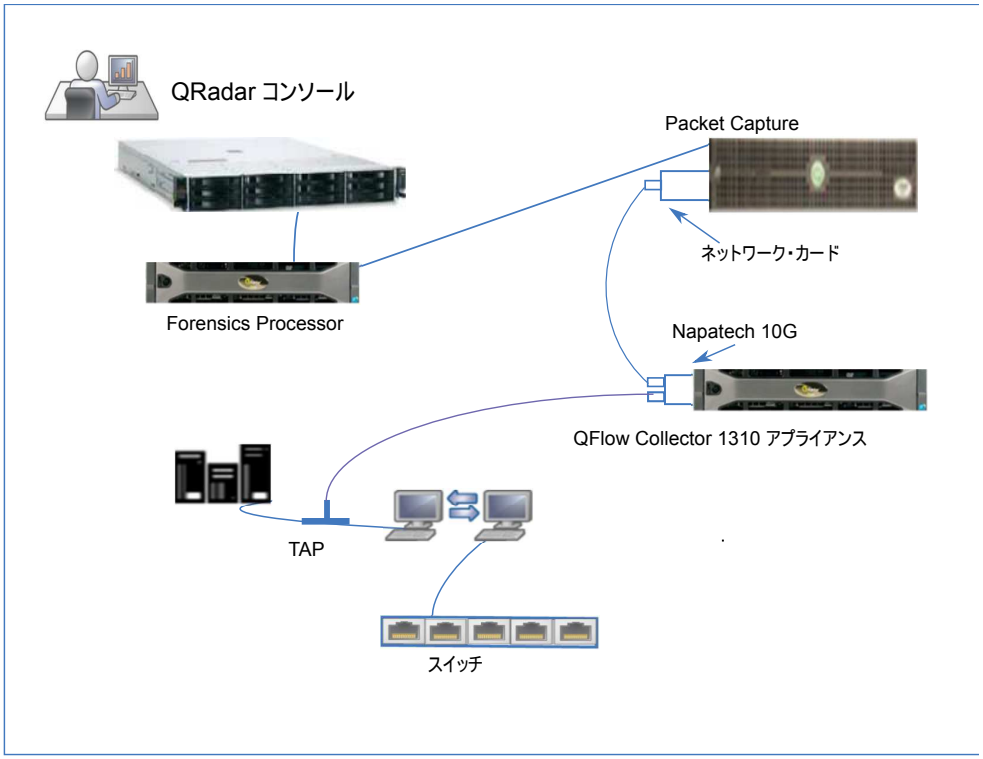


図 15. *Napatech* カードを使用して *QRadar QFlow Collector* から *QRadar Packet Capture* に転送されるパケット・データ

始める前に

以下のハードウェアがご使用の環境にセットアップされていることを確認してください。

- QRadar QFlow Collector 1310 アプライアンスの Napatech カードのポート 1 にケーブルを接続している。
- Napatech カードのポート 2 (転送ポート) に接続されているケーブルを QRadar Packet Capture アプライアンスに接続している。
- 両方のアプライアンスでリンク・ライトを確認してレイヤー 2 接続を検証します。

手順

1. IBM Security QRadar コンソールから、SSH を使用して root ユーザーとして QRadar QFlow Collector にログインします。QRadar QFlow Collector アプライアンスで、以下のファイルを編集します。

   ```
   /opt/qradar/init/apply_tunings
   ```

   a. 137 行目あたりにある、以下の行を見つけます。

   ```
   apply_multithread_qflow_changes()
   {
        APPLIANCEID=`$NVABIN/myver -a`
        if [ "$APPLIANCEID" == "1310" ]; then
             MODELNUM=$(/opt/napatech/bin/AdapterInfo 2>&1 | grep "Active FPGA Image" | cut -d'-' -f2)
             if [ "$MODELNUM" == "9220" ]; then..
   ```

   b. 上記のコードに続く一連の `AppendToConf` の行に、次の行を追加します。

```
AppendToConf SV_NAPATECH_FORWARD YES
AppendToConf SV_NAPATECH_FORWARD_INTERFACE_SRCDST "0:1"
```

これらのステートメントにより、パケット転送が有効になり、パケットがポート 0 からポート 1 に転送されます。

c. /opt/qradar/conf/nva.conf ファイルの以下の行を確認してマルチスレッド化 が有効になっていることを検証します。

```
MULTI_THREAD_ON=YES
```

2. 以下のコマンドを入力して apply_tunings スクリプトを実行し、QRadar QFlow Collector の構成ファイルを更新します。

```
./apply_tunings restart
```

3. 以下のコマンドを入力して IBM Security QRadar サービスを再始動します。

```
systemctl restart hostcontext
```

4. オプション: Napatech カードがデータを送受信しているか確認します。

a. Napatech カードがデータを受信しているか確認するには、以下のコマンドを入力します。

```
/opt/napatech/bin/Statistics -dec -interactive
```

カードがデータを受信している場合、「RX」パケットとバイトの統計が増加します。

b. Napatech カードがデータを送信しているか確認するには、以下のコマンドを入力します。

```
/opt/napatech/bin/Statistics -dec -interactive
```

カードがデータを送信している場合、「TX」統計が増加します。

5. オプション: QRadar Packet Capture が QRadar QFlow Collector アプライアンスからパケットを受信していることを検証します。

a. QRadar コンソールから、SSH を使用して root ユーザーとしてポート 4477 で QRadar Packet Capture アプライアンスにログインします。

b. 以下のコマンドを入力して、QRadar Packet Capture アプライアンスがパケットを受信していることを検証します。

```
watch -d cat /var/www/html/statisdata/int0.txt
```

データが QRadar Packet Capture アプライアンスに送信されるたびに int0.txt ファイルが更新されます。

パケット・キャプチャーについて詳しくは、*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 3 章 データ・ノードおよびデータ・ストレージ

IBM Security QRadar プロセッサー・アプライアンスとオールインワン・アプライアンスはデータを保管できますが、多くの企業はデータ・ノードの処理能力とスタンドアロン・ストレージを使用して、特定のストレージ要件に対応し、データ保存ポリシーの実施に役立てる必要があります。多くの企業は、特定の期間データ・レコードを維持することを課す規制や法律によって影響を受けます。

データ・ノードの情報

以下は、データ・ノードに関する情報です。

- データ・ノードによって、ストレージと処理能力が追加されます。
- データ・ノードは、プラグ・アンド・プレイであり、いつでもデプロイメント環境に追加できます。
- データ・ノードは、既存のデプロイメントとシームレスに統合されます。
- データ・ノードを使用すると、データ・ストレージ処理に要する負荷がプロセッサーから取り除かれることにより、プロセッサー・アプライアンスの処理負荷が削減されます。
- ユーザーは、データ収集とは別個にストレージや処理能力を拡大できます。
- QRadar V.7.2.7 以降、データが保管されるときに、ネイティブ・データ圧縮機能を使用してデータが圧縮されます。ネイティブ・データ圧縮機能により、古いバージョンの QRadar でデータ圧縮に使用されていた以前の圧縮アルゴリズムよりも、検索パフォーマンスを大幅に高めることができます。

以下の図には、デプロイメントでのデータ・ノードに関するいくつかの使用例が示されています。

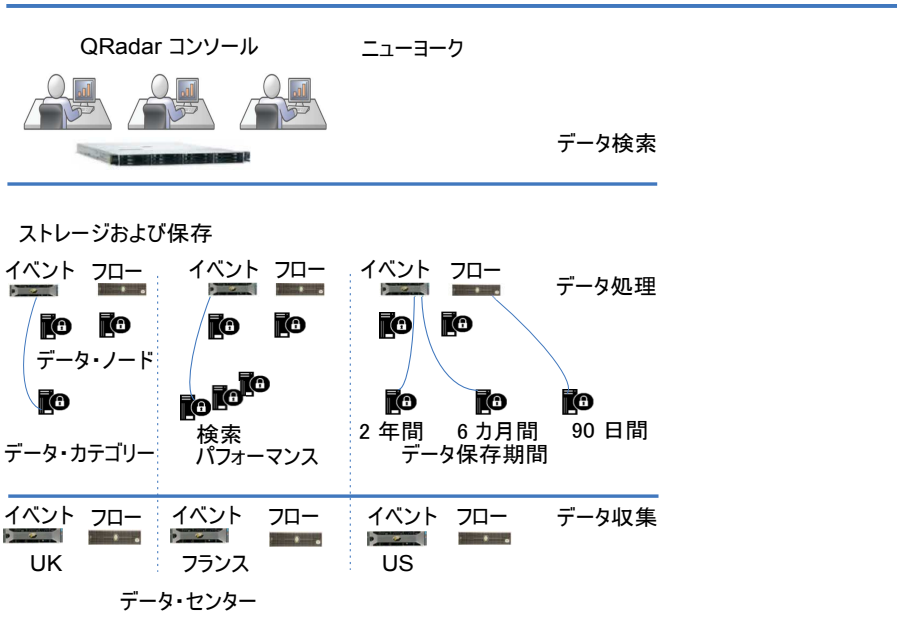


図 *16.* データ・ノード・アプライアンスを使用したデータ・ストレージの管理

以下に、データ・ノードをデプロイするときに考慮する必要があるさまざまな要素について説明します。

データ・クラスタリング

データ・ノードにより、デプロイメントにストレージ容量が追加され、複数のストレージ・ボリュームにわたって収集されるデータを分散することでパフォーマンスも高まります。データが検索されると、複数のホスト、つまりクラスターによって検索が行われます。クラスターを使用すると検索パフォーマンスを高めることができますが、複数のイベント・プロセッサーを追加する必要はありません。データ・ノードによって、各プロセッサーのストレージが増えます。

注: 1 つのデータ・ノードを接続できるプロセッサーは同時に 1 つのみですが、1 つのプロセッサーで複数のデータ・ノードをサポートできます。

デプロイメントの考慮事項

デプロイメントにデータ・ノードをセットアップするときは、以下の情報を考慮してください。

- データ・ノードは、QRadar V7.2.2 以降で使用できます。
- データ・ノードは、QRadar デプロイメント環境のイベント・プロセッサーやフロー・プロセッサーと類似する検索機能と分析機能を実行します。

  クラスターでの操作速度は、クラスター内の最も遅いメンバーによって影響を受けます。データ・ノードのシステム・パフォーマンスは、データ・ノードのサイズをデプロイメント環境内のイベント・プロセッサーやフロー・プロセッサーと同程度のサイズにすると向上します。データ・ノードと、イベントプロセッサーおよびフロー・プロセッサーとの

間の同様のサイズ変更を容易にするために、データ・ノードは XX05 コア・アプライアンスと XX28 コア・アプライアンスの両方で使用することができます。

- データ・ノードは、(ハードウェア上の) ソフトウェア、物理ノード、およびアプライアンスという 3 つの形式で使用できます。 1 つのクラスター内で、これらの形式を組み合わせて使用することができます。

帯域幅と待ち時間

クラスター内のホスト間に 1 Gbps のリンクを設定し、待ち時間が 10 ミリ秒未満になるようにしてください。多数の結果をもたらす検索には、より大きい帯域幅が必要です。

アプライアンスの互換性

データ・ノードは、イベント・プロセッサー・コンポーネントまたはフロー・プロセッサー・コンポーネント (オールインワン・アプライアンスを含む) を持つ、既存のすべての QRadar アプライアンスに対応しています。データ・ノードは、QRadar Incident Forensics PCAP アプライアンスには対応していません。

データ・ノードは、高可用性 (HA) をサポートしています。

データ・ノードのインストール

データ・ノードは標準の TCP/IP ネットワーキングを使用するため、専用の相互接続ハードウェアや特殊な相互接続ハードウェアは必要ありません。

他の QRadar アプライアンスをインストール場合と同様に、デプロイメント環境に追加するデータ・ノードを個別にインストールしてください。QRadar デプロイメント・エディターで、データ・ノードをイベント・プロセッサーまたはフロー・プロセッサーに関連付けます。詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。

複数のデータ・ノードを単一のイベント・プロセッサーに追加したり、多対 1 構成のフロー・プロセッサーに追加したりすることができます。

データ・ノード・アプライアンスを使用して高可用性 (HA) のペアをデプロイする場合、HA のペアを同期化する前に、HA アプライアンスを使用してデータのインストール、デプロイ、および再バランシングを行ってください。HA 用に使用されるデータの再バランシング処理と複製処理を組み合わせると、パフォーマンスが大幅に低下します。データ・ノードが導入されているアプライアンスに HA がセットアップされている場合、アプライアンスで HA を切断し、クラスターの再バランスが完了した後に HA を再接続します。

データ・ノードの使用中止

他の QRadar アプライアンスと同様に、デプロイメント・エディターを使用してデプロイメント環境からデータ・ノードを削除することができます。使用中止とはホスト上のデータを消去することではなく、データを他のアプライアンスに移動することでもありません。データ・ノードにあったデータへのアクセスを維持する必要がある場合、そのデータの移動先となる場所を特定する必要があります。

データの再バランシング

データ・ノードをクラスターに追加すると、各データ・ノードにデータが分散されます。可能な場合、データの再バランシングによって、各データ・ノードに、同じパーセンテージの使用可能なスペースが維持されます。クラスターに追加された新しいデータ・ノードによって、クラスターのイベント・プロセッサーとフロー・プロセッサーから追加の再バランス処理が開始され、新たに追加されたデータ・ノード・アプライアンス上に十分なディスク使用量が確保されます。

QRadar V7.2.3 以降、データの再バランシングは、照会やデータ収集などの他のクラスター・アクティビティーと並行して自動的に実行されるようになりました。データの再バランス処理中にダウン時間は発生しません。

データの再バランシングが完了するまで、データ・ノードによってクラスター内のパフォーマンスが向上することはありません。再バランス処理により、検索操作の実行中にパフォーマンスが多少低下することがありますが、データ収集やデータ処理が影響を受けることはありません。

注: データ・ノードとイベント・プロセッサーの間の暗号化されたデータ伝送はサポートされていません。イベント・プロセッサーとのデータ・ノード通信を行うには、以下のファイアウォール・ポートが開かれている必要があります。

- データ・ノードとイベント・プロセッサー・アプライアンスの間のポート 32006。
- データ・ノードとコンソールのイベント・プロセッサーの間のポート 32011。

管理と運用

データ・ノードには自己管理機能が備わっているため、ユーザーが通常の保守操作を定期的に行う必要はありません。QRadar は、データ・ノード・アプライアンスを含むすべてのホストに対して、データのバックアップなどのアクティビティー、高可用性、および保存ポリシーを管理します。

データ・ノードの障害

データ・ノードで障害が発生した場合、残りのクラスター・メンバーがデータの処理を続行します。

障害が発生したデータ・ノードが復旧すると、クラスター内の適切なデータ配分を維持するためのデータ再バランシングが実行され、その後通常の処理が再開されます。ダウン時間の間、障害が発生したデータ・ノードにあるデータを使用することはできません。また、QRadar ユーザー・インターフェースのログおよびネットワーク・アクティビティー・ビューアーでの検索結果に、発生した入出力エラーが表示されます。

アプライアンスの交換や QRadar の再インストールが必要になる重大な障害が発生した場合、デプロイメント環境でのデータ・ノードの使用を中止し、標準のインストール手順でそれらのデータ・ノードを置き換えてください。デプロイを行う前に、障害で失われずに残ったデータを、新しいデータ・ノードにすべてコピーしてください。再バランシング・アルゴリズムは、データ・ノードに存在するデータを対象にし、障害中に収集されたデータのみをシャッフルします。

HA のペアとともにデプロイされたデータ・ノードの場合、ハードウェアで障害が発生するとフェイルオーバーが実行されるため、システムは引き続き正常に稼働します。

SAN の概要

アプライアンスのストレージ容量を増やすために、データの一部をオフボード・ストレージ・デバイスに移動できます。/store、/store/ariel、または /store/backup の各ファイル・システムを移動できます。

外部ストレージの追加に、複数の方式 (iSCSI、ファイバー・チャネル、NFS (ネットワーク・ファイル・システム) など) を使用できます。/store/ariel ディレクトリーなど、UI でアクセス可能で検索可能なデータを保管するには、iSCSI またはファイバー・チャネルを使用し、データ・バックアップにのみ NFS の使用を確保しておく必要があります。

/store ファイル・システムを外部デバイスに移動すると、QRadar のパフォーマンスに影響を及ぼす可能性があります。

マイグレーション後、/store ファイル・システムに対するすべてのデータ入出力は、ローカル・ディスクでは実行されなくなります。 QRadar データを外部ストレージ・デバイスに移動する前に、以下の情報を検討する必要があります。

- 保存済みのマークが付けられている検索は、/transient ディレクトリー内にもあります。ローカル・ディスクで障害が発生した場合、これらの検索は保存されません。
- データを移動する前に存在していた一時パーティションは移動後も存在する可能性があるため、iSCSI やファイバー・チャネルのストレージにマウントされる可能性があります。

オフボード・ストレージについて詳しくは、「*IBM QRadar Security Intelligence* オフボード・ストレージ・ガイド」を参照してください。

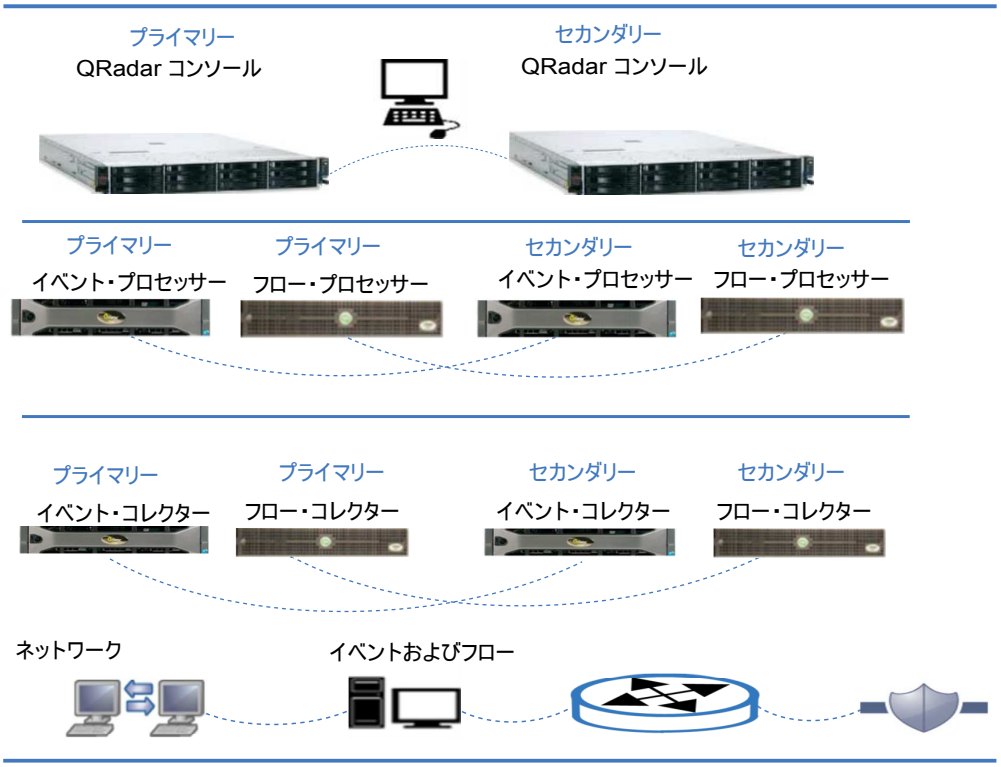
第 4 章 HA デプロイメント環境の概要

IBM Security QRadar デプロイメントに高可用性 (HA) を実装し、デプロイメント環境でハードウェアまたはソフトウェアの障害が発生した場合でも QRadar の機能が実行され続けるようにします。

高可用性を使用することで、何らかの障害が発生しても、イベント・データとフロー・データの収集、保管、および処理を続行できます。

HA を有効にするために、QRadar はプライマリー HA ホストをセカンダリー HA ホストに接続し、HA クラスターを作成します。

以下の図には、基本的な HA セットアップが示されています。



HA の概要

HA デプロイメントでは、以下のいずれかのシナリオでプライマリー・アプライアンスに障害が発生した場合に、デバイスのロールを引き継ぐセカンダリー・アプライアンスをインストールし、構成します。

- 電源装置に障害が発生した
- ネットワーク接続テストでネットワーク障害が検出された
- オペレーティング・システムの誤動作が発生し、ハートビート ping テストが遅延または停止した
- プライマリー HA ホストで完全な RAID 障害が発生した

- 手動フェイルオーバーが実行された
- プライマリー HA ホストで管理インターフェースに障害が発生した

大規模なデプロイメント環境で最適なパフォーマンスを得るために、HA クロスオーバーに 10 Gbps インターフェースを使用することを強くお勧めします。10 Gbps のインターフェースを使用すると、システム同期に必要な時間が短縮され、ペアの最適なパフォーマンスが確保されます。使用可能な 10 Gbps インターフェースがない場合、クロスオーバー用に 1 Gbps のインターフェースを複数結合することを検討してください。

HA について詳しくは、「*IBM Security QRadar SIEM* 高可用性ガイド」を参照してください。

第 5 章 バックアップ戦略

業務上重要な情報をバックアップして、データ損失から保護します。データの種類が異なれば、必要なバックアップ戦略も異なります。

QRadar データ・バックアップ

以下の理由により、バックアップ戦略ではデータ分類を考慮することが重要です。

- 個人識別情報 (PII) などのデータは、コンプライアンス上の理由から、安全に保管する必要があり、一括データ・バックアップとは別個に維持し、より長期間保持する必要があります。
- QRadar システム構成データは、イベントやフローなどのセキュリティー・データとは分離しておきます。システム構成は分離しておくほうが安全です。また、システム構成を別個に保管しておくほうが、データのリストアをより簡単に行えます。
- PCI データなどのデータは別の場所に保管し、監査員がデータを確認する必要がある場合に、容易にアクセスできるようにします。
- バックアップ戦略を作成するときは、データの種類と保存期間を考慮します。
- 特定の種類のデータを他のデータよりも頻繁にバックアップしたり、一部のデータにオフサイト・ストレージを使用してデータ損失から保護したりすることができます。

保存設定

QRadar バックアップ保存のデフォルト設定は 7 日間です。また、大規模な構成の変更を行った後、オンデマンド・バックアップを行うこともできます。このオンデマンド・バックアップにわかりやすい名前を付けておけば、この構成に戻る必要がある場合に、変更を簡単に見つけることができます。

スケジュール済みバックアップを行うと、それよりも古いスケジュール済みバックアップは上書きされます。オンデマンド・バックアップは無期限に維持されます。QRadar バックアップ・ボリュームが容量の 75% に到達すると、それ以降、スケジュール済みバックアップは実行されなくなります。

バックアップの場所

QRadar をデプロイするときは、バックアップの場所を考慮することも重要です。バックアップがホスト上に保持されたままである場合、そのホストに障害が発生すると、すべてのバックアップ・データが失われます。

外部システムにバックアップを作成したり、外部システムにバックアップをコピーしたりすることができます。

データ・セキュリティーをさらに高めるには、重要なデータのコピーをローカルとリモートの両方に保管します。

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。

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。

プライバシー・ポリシーに関する考慮事項

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