IBM Security QRadar

ログ・ソース・ユーザー・ガイド

2016 年 4 月

IBM

注記

本書および本書で紹介する製品を使用する前に、 65 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 V7.2.5 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
Log Sources User Guide
April 2016

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

このガイドについて

ログ・ソースは、収集、保管、解析、および処理のために IBM® Security QRadar® にイベントを送信するサード・パーティー・デバイスです。

対象読者

管理者には、QRadar のアクセス権限と、企業ネットワークおよびネットワーク技術に関する知識が必要です。

技術資料

すべての翻訳資料を含む IBM Security QRadar 製品資料を Web で見つけるには、IBM ナレッジ・センター(http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリーでより技術的な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。

注意事項:

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 ログ・ソース管理の概要

ネットワーク上のログ・ソースからイベント・ログを受け入れるように IBM Security QRadar を構成することができます。*ログ・ソース* とは、イベント・ログを作成するデータ・ソースのことです。

例えば、ファイアウォールや侵入防止システム (IPS) はセキュリティー・ベースのイベントをログに記録し、スイッチやルーターはネットワーク・ベースのイベントをログに記録します。

ログ・ソースからロー・イベントを受信するために、QRadar は多くのプロトコルをサポートしています。*パッシブ・プロトコル* は、特定のポートでイベントを listen します。*アクティブ・プロトコル* は、API などの通信手段を使用して、イベントのポーリングと取得を行う外部システムに接続します。

ライセンス制限に応じて、QRadar は、300 件を超えるログ・ソースからイベントを読み取って解釈することができます。

QRadar 用のログ・ソースを構成するには、以下のタスクを実行する必要があります。

1. ログ・ソースをサポートするデバイス・サポート・モジュール (DSM) をダウンロードしてインストールします。*DSM* は、元の形式のイベント・ログを識別して、QRadar が使用できる形式に構文解析するために必要なイベント・パターンを含むソフトウェア・アプリケーションです。DSM およびサポートされるログ・ソースについて詳しくは、「*DSM 構成ガイド*」を参照してください。
2. DSM の自動ディスカバリーがサポートされている場合は、QRadar が自動的にログ・ソースを構成済みのログ・ソースのリストに追加するまで待ちます。
3. DSM の自動ディスカバリーがサポートされていない場合は、手動でログ・ソース構成を作成します。

ログ・ソースの追加

ログ・ソースが自動的に検出されない場合、ネットワーク・デバイスまたはアプライアンスからイベントを受信するログ・ソースを手動で追加できます。

このタスクについて

以下の表は、すべてのログ・ソース・タイプに共通のログ・ソース・パラメーターを説明しています。

表 1. ログ・ソース・パラメーター

パラメーター	**説明**
ログ・ソース ID	ログ・ソースを識別する IPv4 アドレスまたはホスト名。 ネットワークに、単一の管理コンソールに接続された複数のデバイスが含まれる場合、イベントを作成した個々のデバイスの IP アドレスを指定します。それぞれの固有 ID (IP アドレスなど) を指定することにより、イベント検索で管理コンソールがすべてのイベントのソースとして識別されることを回避します。
有効	このオプションが有効にされていない場合、ログ・ソースはイベントを収集しないため、ライセンス制限にカウントされません。
信頼性	信頼性は、ログ・ソースによって作成されたイベントの整合性または有効性を表します。ログ・ソースに割り当てられている信頼性値は、着信イベントに基づいて増減されたり、ユーザーが作成したイベント規則に対応して調整されたりする場合があります。ログ・ソースからのイベントの信頼性は、オフェンスのマグニチュードの計算に反映され、オフェンスのマグニチュード値を増大または減少させる場合があります。
ターゲット・イベント・コレクター	リモート・ログ・ソースをポーリングする QRadar イベント・コレクターを指定します。 分散デプロイメントでは、コンソールのシステム・パフォーマンスを向上させるために、このパラメーターを使用してポーリング・タスクをイベント・コレクターに移動します。
イベントの統合	同じイベントが短い時間間隔内で複数回発生するとイベント数が増大します。統合されたイベントを使用することで、単一のイベント・タイプが発生する頻度を「**ログ・アクティビティー**」タブで表示し判別できます。 このチェック・ボックスがクリアされている場合、イベントは個別に表示され、イベントのバンドルは行われません。 自動的に検出された新規のログ・ソースは、「**管理**」タブの「**システム設定**」構成から、このチェック・ボックスの値を継承します。このチェック・ボックスを使用して、個々のログ・ソースに対するシステム設定のデフォルトの動作をオーバーライドできます。

手順

1. 「**管理**」タブをクリックします。
2. 「**ログ・ソース**」アイコンをクリックします。
3. 「**追加**」をクリックします。
4. ログ・ソースの共通パラメーターを構成します。
5. ログ・ソースのプロトコル固有のパラメーターを構成します。
6. 「**保存**」をクリックします。
7. 「**管理**」タブで「**変更のデプロイ**」をクリックします。

Blue Coat Web Security Service REST API プロトコルの構成オプション

Blue Coat Web Security Service からイベントを受信するには、Blue Coat Web Security Service REST API プロトコルを使用するようにログ・ソースを構成します。

Blue Coat Web Security Service REST API プロトコルは Blue Coat Web Security Service Sync API を照会して、クラウドから最新のログ・データを取得します。

Blue Coat Web Security Service REST API プロトコルのプロトコル固有のパラメーターを下の表で説明します。

表 2. Blue Coat Web Security Service REST API プロトコルのパラメーター

パラメーター	説明
API ユーザー名 (API Username)	Blue Coat Web Security Service での認証に使用される API ユーザー名。API ユーザー名は、Blue Coat Threat Pulse ポータルを使用して構成されます。
パスワード	Blue Coat Web Security Service での認証に使用されるパスワード。
パスワードの確認	「**パスワード**」フィールドの確認。
プロキシーの使用 (Use Proxy)	プロキシーを構成すると、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Blue Coat Web Security Service にアクセスします。 「**プロキシー IP またはホスト名 (Proxy IP or Hostname)**」、「**プロキシー・ポート**」、「**プロキシー・ユーザー名**」、および「**プロキシー・パスワード**」の各フィールドを構成します。プロキシーが認証を必要としない場合、「**プロキシー・ユーザー名**」フィールドと「**プロキシー**」「**パスワード**」フィールドはブランクのままでかまいません。
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	リストから「はい」を選択すると、QRadar は証明書をダウンロードし、ターゲット・サーバーを信頼して使用し始めます。
繰り返し (Recurrence)	ログがいつデータを収集するかを指定できます。フォーマットは、月/時刻/日を表す M/H/D です。デフォルトは 5 M です。

表 2. Blue Coat Web Security Service REST API プロトコルのパラメーター (続き)

パラメーター	説明
EPS スロットル	1 秒あたりの最大イベント数 (EPS) の上限。デフォルトは 5000 です。

Cisco NSEL プロトコルの構成オプション

Cisco Adaptive Security Appliance (ASA) からの NetFlow パケット・フローをモニターするには、Cisco Network Security Event Logging (NSEL) プロトコル・ソースを構成します。

Cisco NSEL を QRadar と統合するには、ログ・ソースを手動で作成して NetFlow イベントを受信する必要があります。QRadar が Cisco NSEL からの Syslog イベントに対してログソースを自動的にディスカバーおよび作成することはありません。詳しくは、「*DSM 構成ガイド*」を参照してください。

Cisco NSEL プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 3. Cisco NSEL プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Cisco NSEL**
ログ・ソース ID	ネットワークの中で複数のデバイスが管理コンソールに接続する場合は、イベントを作成した個々のデバイスの IP アドレスを指定できます。それぞれの固有 ID (IP アドレスなど) を指定することにより、イベント検索で管理コンソールがすべてのイベントのソースとして識別されることを回避します。
コレクター・ポート	Cisco ASA が NSEL イベントの転送に使用する UDP ポート番号。QRadar は、QRadar QFlow Collector のフロー・データにポート 2055 を使用します。NetFlow 用に Cisco Adaptive Security Appliance の別の UDP ポートを割り当てる必要があります。

EMC VMware プロトコルの構成オプション

仮想環境の VMWare Web サービスからイベント・データを受信するには、EMC VMWare プロトコルを使用するようにログ・ソースを構成します。

EMC VMware プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 4. EMC VMware プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**EMC VMware**
ログ・ソース ID	このパラメーターの値は「**VMware の IP (VMware IP)**」パラメーターに一致している必要があります。

表 4. EMC VMware プロトコルのパラメーター (続き)

パラメーター	説明
VMware の IP (VMware IP)	VMWare ESXi サーバーの IP アドレス (1.1.1.1 など)。VMware プロトコルは、イベント・データを要求する前に VMware ESXi サーバーの IP アドレスに HTTPS を付加します。

転送プロトコルの構成オプション

デプロイメント内の別のコンソールからイベントを受信するには、転送プロトコルを使用するようにログ・ソースを構成します。

通常、転送プロトコルは、イベントを別の QRadar コンソールに転送するために使用します。例えば、コンソール A でコンソール B がオフサイト・ターゲットとして構成されているとします。自動的にディスカバーされたログ・ソースからのデータはコンソール B に転送されます。コンソール A で手動で作成したログ・ソースも、転送プロトコルを使用してコンソール B にログ・ソースとして追加する必要があります。

IBM Tivoli Endpoint Manager SOAP プロトコルの構成オプション

IBM Tivoli® Endpoint Manager アプライアンスからログ・イベント拡張フォーマット (LEEF) 形式のイベントを受信するには、IBM Tivoli Endpoint Manager SOAP プロトコルを使用するログ・ソースを構成します。

このプロトコルの場合は、IBM Tivoli Endpoint Manager バージョン V8.2.x 以降と、Tivoli Endpoint Manager 用の Web レポート・アプリケーションが必要です。

Tivoli Endpoint Manager SOAP プロトコルは、HTTP または HTTPS によって 30 秒間隔でイベントを取得します。イベントを取得すると、IBM Tivoli Endpoint Manager DSM がイベントを構文解析して分類します。

IBM Tivoli Endpoint Manager SOAP プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 5. IBM Tivoli Endpoint Manager SOAP プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**IBM Tivoli Endpoint Manager SOAP**
HTTPS の使用	HTTPS で接続するために証明書が必要な場合は、必要な証明書をディレクトリー `/opt/qradar/conf/trusted_certificates` にコピーしてください。ファイル拡張子が `.crt`、`.cert`、または `.der` である証明書がサポートされています。ログ・ソースを保存してデプロイする前に、証明書を信頼証明書ディレクトリーにコピーしてください。
SOAP ポート (SOAP Port)	デフォルトでは、ポート 80 が IBM Tivoli Endpoint Manager と通信するためのポート番号です。ほとんどの構成で、HTTPS 通信にはポート 443 が使用されます。

JDBC プロトコルの構成オプション

QRadar は、JDBC プロトコルを使用して、複数のデータベース・タイプからのイベント・データを含む表またはビューから情報を収集します。

JDBC プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 6. JDBC プロトコル・パラメーター

パラメーター	説明
データベース・タイプ	リスト・ボックスから、イベントが含まれているデータベースのタイプを選択します。
データベース名	データベース名は、「**ログ・ソース ID**」フィールドで指定したデータベース名に一致している必要があります。
ポート	JDBC ポートは、リモート・データベースで構成されている listen ポートに一致している必要があります。データベースは、着信 TCP 接続を許可しなければなりません。MSDE データベース・タイプの場合に「**データベース・インスタンス**」を使用するとき、管理者は、ログ・ソース構成の「**ポート**」パラメーターを空白のままにしておく必要があります。
ユーザー名	データベースの QRadar 用ユーザー・アカウント。
パスワード	データベースへの接続に必要なパスワード。
パスワードの確認	データベースへの接続に必要なパスワード。
認証ドメイン	Windows ドメイン内の MSDE データベースに対してドメインを構成する必要があります。ネットワークがドメインを使用しない場合は、このフィールドを空白のままにしてください。
データベース・インスタンス	データベース・インスタンス (必要な場合)。MSDE データベースでは、単一のサーバーに複数の SQL サーバー・インスタンスを含めることができます。 標準以外のポートをデータベースに使用する場合、または SQL データベース解決のためのポート 1434 へのアクセスがブロックされる場合は、ログ・ソース構成の「**データベース・インスタンス**」パラメーターを空白にする必要があります。
定義済み照会	オプション。
テーブル名	イベント・レコードを含む表またはビューの名前。表名に使用できる特殊文字は、ドル記号 ($)、番号記号 (#)、下線 (_)、エヌ・ダッシュ (-)、ピリオド (.) です。
選択リスト	表をポーリングしてイベントを照会するときに含めるフィールドのリスト。コンマ区切りのリストを使用できるほか、* を入力して、表またはビューにあるすべてのフィールドを選択することができます。コンマ区切りのリストを定義する場合は、「**比較フィールド**」で定義したフィールドをリストに含める必要があります。

表 6. JDBC プロトコル・パラメーター (続き)

パラメーター	説明
比較フィールド	照会から次の照会までの間に表に追加された新しいイベントを識別する表またはビューにある、数値またはタイム・スタンプのフィールド。重複するイベントが作成されないように、このプロトコルが以前にポーリングしたイベントを識別できるようにします。
準備済みステートメントの使用 (Use Prepared Statements)	準備済みステートメントを使用すると、JDBC プロトコル・ソースで SQL ステートメントをセットアップし、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティー上およびパフォーマンス上の理由により、ほとんどの JDBC プロトコル構成で準備済みステートメントを使用することができます。
開始日時	開始時刻が定義されていない場合、このプロトコルは、ログ・ソース構成が保存されてデプロイされた後にイベントをポーリングしようとします。
ポーリング間隔 (Polling Interval)	デフォルトのポーリング間隔は 10 秒です。
EPS スロットル	許容する 1 秒当たりのイベント数 (EPS) の上限。
データベース・ロケール (Database Locale)	多言語インストール済み環境の場合は、「**データベース・ロケール (Database Locale)**」フィールドを使用して、使用する言語を指定します。
データベースのコード・セット (Database Codeset)	多言語インストール済み環境の場合は、「**コード・セット (Codeset)**」フィールドを使用して、使用する文字セットを指定します。
名前付きパイプ通信の使用 (Use Named Pipe Communication)	MSDE データベースの名前付きパイプ接続を使用する場合は、「ユーザー名」フィールドおよび「パスワード」フィールドで、データベースのユーザー名とパスワードではなく、Windows 認証のユーザー名とパスワードを使用する必要があります。ログ・ソースの構成では、MSDE データベースのデフォルトの名前付きパイプを使用する必要があります。
NTLMv2 の使用	「**NTLMv2 の使用**」チェック・ボックスを選択しても、NTLMv2 認証を必要としない MSDE 接続の通信には干渉しません。
Oracle 暗号化の使用 (Use Oracle Encryption)	Oracle の暗号化とデータ整合性の設定は Oracle Advanced Security とも呼ばれます。 これを選択した場合、Oracle JDBC 接続では、サーバーが同様の Oracle データ暗号化設定をクライアントとしてサポートすることが必要になります。
SSL	ご使用の接続で SSL がサポートされている場合は「SSL」チェック・ボックスを選択します。このオプションが表示されるのは MSDE の場合のみです。

JDBC SiteProtector の構成オプション

Java™ Database Connectivity (JDBC) SiteProtector™ プロトコルを使用してリモート側から IBM Proventia® Management SiteProtector® データベースをポーリングしてイベントを照会するように、ログ・ソースを構成することができます。

JDBC - SiteProtector プロトコルは、ログ・ソース・ペイロードの作成時に SensorData1 表と SensorDataAVP1 表の情報を結合します。SensorData1 表と SensorDataAVP1 表は、IBM Proventia® Management SiteProtector® データベースに存在します。1 回の照会で JDBC - SiteProtector プロトコルがポーリングできる行の最大数は 30,000 行です。

JDBC - SiteProtector プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 7. JDBC - SiteProtector プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**JDBC - SiteProtector**
データベース・タイプ	リストで、イベント・ソースに使用するデータベースのタイプとして「**MSDE**」を選択します。
データベース名	このプロトコルが接続できるデータベースの名前として `RealSecureDB` と入力します。
IP またはホスト名	データベース・サーバーの IP アドレスまたはホスト名。
ポート	データベース・サーバーが使用するポート番号。JDBC SiteProtector 構成のポートは、データベースのリスナー・ポートに一致する必要があります。データベースでは、着信 TCP 接続を有効にしておく必要があります。データベース・タイプが MSDE のときに「**データベース・インスタンス (Database Instance)**」を定義する場合は、ログ・ソース構成の「**ポート**」パラメーターを空白のままにする必要があります。
ユーザー名	JDBC プロトコルによるデータベースへのアクセスを追跡する場合は、ご使用の QRadar システムに特定のユーザーを作成できます。
認証ドメイン	MSDE を選択するときに、データベースが Windows 用に構成されている場合は、Windows ドメインを定義する必要があります。 ネットワークがドメインを使用しない場合は、このフィールドを空白のままにしてください。
データベース・インスタンス	MSDE を選択するときに、1 つのサーバーに複数の SQL サーバー・インスタンスがある場合は、接続先インスタンスを定義します。データベース構成で標準以外のポートを使用する場合、または SQL データベース解決用のポート 1434 へのアクセスがブロックされる場合は、構成で「**データベース・インスタンス**」パラメーターを空白のままにしておく必要があります。
定義済み照会	ログ・ソースに対する定義済みのデータベース照会。定義済みのデータベース照会は、特別なログ・ソース接続の場合にのみ使用できます。
テーブル名	`SensorData1`
AVP ビュー名 (AVP View Name)	`SensorDataAVP`

表 7. JDBC - SiteProtector プロトコルのパラメーター (続き)

パラメーター	説明
応答ビュー名 (Response View Name)	SensorDataResponse
選択リスト	テーブルまたはビューのすべてのフィールドを含めるには、* を入力します。
比較フィールド	SensorDataRowID
準備済みステートメントの使用 (Use Prepared Statements)	準備済みステートメントを使用すると、JDBC プロトコル・ソースで SQL ステートメントをセットアップし、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティーおよびパフォーマンス上の理由で、準備済みステートメントを使用するようにしてください。プリコンパイル・ステートメントを使用しない代替照会手法を使用する場合は、このチェック・ボックスをクリアできます。
監査イベントを含む	監査イベントを IBM SiteProtector® から収集する場合に指定します。
開始日時	オプション。プロトコルがデータベースのポーリングを開始できる開始日時。
ポーリング間隔 (Polling Interval)	イベント・テーブルに対する照会から次の照会までの間の時間。より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。指定子の H および M のない数値の場合は、秒単位のポーリングになります。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数。
データベース・ロケール (Database Locale)	多言語インストール済み環境の場合は、「**データベース・ロケール (Database Locale)**」フィールドを使用して、使用する言語を指定します。
データベースのコード・セット (Database Codeset)	多言語インストール済み環境の場合は、「**コード・セット (Codeset)**」フィールドを使用して、使用する文字セットを指定します。
名前付きパイプ通信の使用 (Use Named Pipe Communication)	データベース・タイプとして MSDE を選択した場合は、このチェック・ボックスを選択して、TCP/IP ポート接続の代替方式を使用します。名前付きパイプ接続を使用する場合は、ユーザー名とパスワードは、データベースのユーザー名とパスワードではなく、Windows 認証の適切なユーザー名とパスワードにする必要があります。ログ・ソースの構成ではデフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 (Database Cluster Name)	名前付きパイプ通信を正常に機能させるためのクラスター名。
NTLMv2 の使用	NTLMv2 認証を必要とする SQL サーバーの場合に、強制的に MSDE 接続で NTLMv2 プロトコルを使用します。「**NTLMv2 の使用**」チェック・ボックスを選択しても、NTLMv2 認証を必要としない MSDE 接続の通信には干渉しません。
SSL の使用 (Use SSL)	JDBC プロトコルに対して SSL 暗号化を有効化します。

表 7. JDBC - SiteProtector プロトコルのパラメーター (続き)

パラメーター	説明
ログ・ソース言語	ログ・ソースによって生成されるイベントの言語を選択します。ログ・ソース言語により、複数の言語でイベントを作成できる外部のアプライアンスまたはオペレーティング・システムからのイベントをシステムが構文解析できるようになります。

Juniper Networks NSM プロトコルの構成オプション

Juniper Networks NSM および Juniper Networks Secure Service Gateway (SSG) ログ・イベントを受信するには、Juniper Networks NSM プロトコルを使用するようにログ・ソースを構成します。

Juniper Networks Network and Security Manager プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 8. Juniper Networks NSM プロトコルのパラメーター

パラメーター	説明
ログ・ソース・タイプ	**Juniper Networks Network and Security Manager**
プロトコル構成	**Juniper NSM**

Juniper Security Binary Log Collector プロトコルの構成オプション

Security Binary Log Collector プロトコルを使用するようにログ・ソースを構成することができます。このプロトコルを使用すると、Juniper アプライアンスが監査イベント、システム・イベント、ファイアウォール・イベント、および侵入防止システム (IPS) イベントをバイナリー形式で QRadar に送信できます。

Juniper SRX または J シリーズ・アプライアンスのバイナリー・ログ形式は、UDP プロトコルを使用してストリーミングされます。バイナリー形式のイベントをストリーミングするための固有のポートを指定する必要があります。標準の Syslog ポート 514 をバイナリー形式のイベントに使用することはできません。Juniper アプライアンスからのストリーミング・バイナリー・イベントの受信用として割り当てられるデフォルト・ポートはポート 40798 です。

Juniper Security Binary Log Collector プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 9. Juniper Security Binary Log Collector のプロトコル・パラメーター

パラメーター	説明
プロトコル構成	**Security Binary Log Collector**

表 9. Juniper Security Binary Log Collector のプロトコル・パラメーター (続き)

パラメーター	説明
XML テンプレート・ファイルのロケーション	Juniper SRX または Juniper J シリーズ・アプライアンスからのバイナリー・ストリームのデコードに使用する XML ファイルのパス。デフォルトでは、バイナリー・ストリームをデコードするための XML ファイルがデバイス・サポート・モジュール (DSM) に含まれています。 この XML ファイルはディレクトリー `/opt/qradar/conf/security_log.xml` にあります。

ログ・ファイル・プロトコルの構成オプション

リモート・ホストからイベントを受信するには、ログ・ファイル・プロトコルを使用するようにログ・ソースを構成します。

ログ・ファイル・プロトコルは、日常イベントのログを書き込むシステムを対象としています。イベント・ファイルに情報を追加するデバイスにログ・ファイル・プロトコルを使用するのは不適切です。

ログ・ファイルは一度に 1 つずつ取得されます。ログ・ファイル・プロトコルは、プレーン・テキスト、圧縮ファイル、またはファイル・アーカイブを管理できます。アーカイブには、一度に 1 行ずつ処理できるプレーン・テキスト・ファイルが含まれている必要があります。ログ・ファイル・プロトコルがイベント・ファイルをダウンロードすると、そのファイルで受信された情報によって「**ログ・アクティビティー**」タブが更新されます。ダウンロードが完了した後にファイルに追加情報が書き込まれても、その追加情報は処理されません。

ログ・ファイル・プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 10. ログ・ファイル・プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**ログ・ファイル**
リモート・ポート	リモート・ホストが標準以外のポート番号を使用する場合は、ポートの値を調整してイベントを取得する必要があります。
SSH 鍵ファイル	鍵認証を使用するようにシステムを構成した場合の、SSH 鍵のパス。SSH 鍵ファイルを使用する場合は、「**リモート・パスワード**」フィールドが無視されます。
リモート・ディレクトリー	FTP の場合に、ログ・ファイルがリモート・ユーザーのホーム・ディレクトリーにある場合は、リモート・ディレクトリーを空白のままにしておくことができます。リモート・ディレクトリーのフィールドを空白にすると、作業ディレクトリーの変更 (CWD) コマンドが制限されているシステムがサポートされます。

表 10. ログ・ファイル・プロトコルのパラメーター (続き)

パラメーター	説明
再帰的 (Recursive)	このチェック・ボックスを有効にすると、FTP 接続または SFTP 接続を使用して、リモート・ディレクトリーのサブフォルダーを再帰的に検索してイベント・データを取得できます。サブフォルダーから収集するデータは、「FTP ファイル・パターン」の正規表現に一致するかどうかで決まります。SCP 接続の場合は、「**再帰的 (Recursive)**」オプションは使用できません。
FTP ファイル・パターン	リモート・ホストからダウンロードするファイルを識別するために必要な正規表現。
FTP 転送モード	FTP 経由で ASCII 転送を行う場合は、「**プロセッサー**」フィールドで「NONE」を選択し、「**イベント・ジェネレーター (Event Generator)**」フィールドで「LINEBYLINE」を選択する必要があります。
繰り返し (Recurrence)	新しいイベント・ログ・ファイルがあるかどうかリモート・ディレクトリーをスキャンする頻度を決定する時間間隔。時間間隔には時間数 (H)、分数 (M)、または日数 (D) の値を含めることができます。例えば、繰り返しが 2H の場合は、リモート・ディレクトリーを 2 時間ごとにスキャンします。
保存時に実行	ログ・ソース構成を保存した後、直ちにログ・ファイルのインポートを開始します。このチェック・ボックスを選択すると、以前にダウンロードされて処理されたファイルのリストがクリアされます。初回のファイル・インポートの後、ログ・ファイル・プロトコルは、管理者によって定義された開始時刻および繰り返しスケジュールに従います。
EPS スロットル	このプロトコルの上限とする 1 秒当たりのイベント数 (EPS)。
ローカル・ディレクトリーの変更	「**ターゲット・イベント・コレクター**」でローカル・ディレクトリーを変更してイベント・ログを保管してから処理します。
ローカル・ディレクトリー	「**ターゲット・イベント・コレクター**」のローカル・ディレクトリー。ログ・ファイル・プロトコルがイベントの取得を試行する前に、このディレクトリーが存在しなければなりません。
ファイルのエンコード (File Encoding)	ログ・ファイルのイベントで使用する文字エンコード。
フォルダーの区切り文字 (Folder Separator)	ご使用のオペレーティング・システムでフォルダーの区切りに使用する文字。ほとんどの構成で、「**フォルダーの区切り文字 (Folder Separator)**」フィールドのデフォルト値を使用できます。このフィールドは、別の文字を使用して個別のフォルダーを定義するオペレーティング・システムを対象としています。例えば、メインフレーム・システムの場合にフォルダーを区切るピリオドが該当します。

Microsoft DHCP プロトコルの構成オプション

Microsoft DHCP サーバーからイベントを受信するには、Microsoft DHCP プロトコルを使用するようにログ・ソースを構成します。

ログ・ファイル (管理共有 (C$) を含むフォルダー・パス) を読み取るには、管理共有 (C$) に対する NetBIOS 特権が必要です。ローカルまたはドメインの管理者は、管理共有にあるログ・ファイルにアクセスするための十分な特権を持っています。

ファイル・パスをサポートする Microsoft DHCP プロトコルのフィールドでは、管理者はドライブ名をパス情報付きで定義できます。例えば、管理共有の場合はフィールドに `c$/LogFiles/` ディレクトリーを指定でき、公開共有フォルダー・パスの場合は `LogFiles/` ディレクトリーを指定できますが、`c:/LogFiles` ディレクトリーを指定することはできません。

制約事項: Microsoft 認証プロトコル NTLMv2 は、Microsoft DHCP プロトコルではサポートされていません。

Microsoft DHCP プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 11. Microsoft DHCP プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Microsoft DHCP**
ドメイン	オプション。
フォルダー・パス	DHCP ログ・ファイルのディレクトリー・パス。
ファイル・パターン	イベント・ログを識別する正規表現。ログ・ファイルには必ず 3 文字の省略形の曜日が入ります。以下のいずれかのファイル・パターンを使用してください。 • IPv4 ファイルのパターン: `DhcpSrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat)¥.log` • IPv6 ファイルのパターン: `DhcpV6SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) ¥.log` • IPv4 と IPv6 が混在するファイルのパターン: `Dhcp.*SrvLog-(?:Sun|Mon|Tue|Wed|Thu|Fri|Sat) ¥.log`

Microsoft Exchange プロトコルの構成オプション

SMTP、OWA、Microsoft Exchange 2007 サーバーおよび 2010 サーバーからイベントを受信するには、サポート用の Microsoft Windows Exchange プロトコルを使用するようにログ・ソースを構成します。

ログ・ファイル (管理共有 (C$) を含むフォルダー・パス) を読み取るには、管理共有 (C$) に対する NetBIOS 特権が必要です。ローカルまたはドメインの管理者は、管理共有にあるログ・ファイルにアクセスするための十分な特権を持っています。

ファイル・パスをサポートする Microsoft Exchange プロトコルのフィールドでは、管理者はドライブ名をパス情報付きで定義できます。例えば、管理共有の場合はフ

ィールドに c$/LogFiles/ ディレクトリーを指定でき、公開共有フォルダー・パスの場合は LogFiles/ ディレクトリーを指定できますが、c:/LogFiles ディレクトリーを指定することはできません。

重要: Microsoft Exchange プロトコルは、Microsoft Exchange 2003 および Microsoft 認証プロトコル NTLMv2 セッションをサポートしていません。

Microsoft Exchange プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 12. Microsoft Exchange プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Microsoft Exchange**
ドメイン	オプション。
SMTP ログ・フォルダーのパス	このフォルダー・パスをクリアすると、SMTP イベント収集が無効になります。
OWA ログ・フォルダーのパス	このフォルダー・パスをクリアすると、OWA イベント収集が無効になります。
MSGTRK ログ・フォルダーのパス	メッセージ・トラッキングを使用できるのは、ハブ・トランスポート、メールボックス、またはエッジ・トランスポート・サーバーのロールが割り当てられている Microsoft Exchange 2007 サーバーまたは 2010 サーバーです。
ファイル・パターン	イベント・ログを識別する正規表現。デフォルトは .*¥.(?:log|LOG) です。
ファイル読み取りの強制 (Force File Read)	このチェック・ボックスをクリアした場合、QRadar が変更時刻またはファイル・サイズの変化を検出した場合にのみログ・ファイルが読み取られます。
スロットル・イベント数/秒	Exchange プロトコルが 1 秒当たり転送できるイベントの最大数。

Microsoft IIS プロトコルの構成オプション

Microsoft IIS プロトコルを使用するようにログ・ソースを構成することができます。このプロトコルは、Microsoft IIS Web サーバーに格納される W3C 形式ログ・ファイルの単一の収集ポイントをサポートします。

ログ・ファイル (管理共有 (C$) を含むフォルダー・パス) を読み取るには、管理共有 (C$) に対する NetBIOS 特権が必要です。ローカルまたはドメインの管理者は、管理共有にあるログ・ファイルにアクセスするための十分な特権を持っています。

ファイル・パスをサポートする Microsoft IIS プロトコルのフィールドでは、管理者はドライブ名をパス情報付きで定義できます。例えば、管理共有の場合はフィールドに c$/LogFiles/ ディレクトリーを指定でき、公開共有フォルダー・パスの場合は LogFiles/ ディレクトリーを指定できますが、c:/LogFiles ディレクトリーを指定することはできません。

制約事項: Microsoft 認証プロトコル NTLMv2 は、Microsoft IIS プロトコルではサポートされていません。

Microsoft IIS プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 13. Microsoft IIS のプロトコル・パラメーター

パラメーター	説明
プロトコル構成	**Microsoft IIS**
ファイル・パターン	イベント・ログを識別する正規表現。
スロットル・イベント数/秒	IIS プロトコルが 1 秒当たり転送できるイベントの最大数。

Microsoft Security Event Log プロトコルの構成オプション

Microsoft Security Event Log プロトコルを使用するようにログ・ソースを構成することができます。Microsoft Windows Management Instrumentation (WMI) を使用して、カスタマイズしたイベント・ログやエージェントレス Windows イベント・ログを収集することができます。

WMI API では、ファイアウォール構成が、ポート 135 のほか、DCOM に必要なすべての動的ポートで着信外部通信を受け入れる必要があります。以下では、Microsoft Security Event Log プロトコルを使用するログ・ソースの制約について説明します。

- システムでの 1 秒当たりのイベント数 (eps) が 50 を超える場合は、このプロトコルの処理能力を超える可能性があります。50 eps を超えるシステムの場合は、WinCollect を使用してください。
- QRadar をオールインワン・インストールした場合は、Microsoft Security Event Log プロトコルで最大 250 件のログ・ソースをサポートできます。
- 専用のイベント・コレクターは、Microsoft Security Event Log プロトコルを使用して最大 500 件のログ・ソースをサポートできます。

ネットワーク・リンクを経由してリモート・サーバーにアクセスする場合 (例えば、衛星回線や低速な WAN ネットワークなど、システムの往復遅延時間が長い場合) は、Microsoft Security Event Log プロトコルを推奨しません。往復の遅延を確認するには、サーバー ping 間の要求および応答時間を調べます。低速接続によって生じるネットワーク遅延は、これらのリモート・サーバーで使用可能な EPS スループットを低下させます。また、ビジー状態のサーバーやドメイン・コントローラーからのイベント収集が着信イベントに追随するためには、往復遅延時間が短くなければなりません。ネットワークの往復遅延時間を短縮できない場合は、WinCollect を使用して Windows イベントを処理することができます。

Microsoft Security Event Log は、Microsoft Windows Management Instrumentation (WMI) API を備えた以下のソフトウェア・バージョンをサポートしています。

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R3
- Microsoft Windows XP
- Microsoft Windows Vista

- Microsoft Windows 7

Microsoft Security Event Log プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 14. Microsoft Security Event Log プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Windows セキュリティー・イベント・ログ**

MQ プロトコルの構成オプション

メッセージ・キュー (MQ) サービスからメッセージを受信するには、MQ プロトコルを使用するようにログ・ソースを構成します。プロトコル名は、IBM Security QRadar では **MQ JMS** と表示されます。

IBM MQ がサポートされます。

MQ プロトコルは複数のメッセージ・キューをモニターできます (ログ・ソースごとに最大 50 件)。

MQ プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 15. MQ プロトコルのパラメーター

パラメーター	説明
プロトコル名 (Protocol Name)	**MQ JMS**
IP またはホスト名	プライマリー・キュー・マネージャーの IP アドレスまたはホスト名。
ポート	プライマリー・キュー・マネージャーとの通信に使用するデフォルト・ポートは 1414 です。
スタンバイ IP またはホスト名 (Standby IP or Hostname)	スタンバイ・キュー・マネージャーの IP アドレスまたはホスト名。
スタンバイ・ポート (Standby Port)	スタンバイ・キュー・マネージャーとの通信に使用するポート。
キュー・マネージャー (Queue Manager)	キュー・マネージャーの名前。
チャネル (Channel)	キュー・マネージャーがメッセージを送信するチャネル。デフォルトのチャネルは `SYSTEM.DEF.SVRCONN` です。
キュー (Queue)	モニター対象のキュー、またはキューのリスト。キューのリストはコンマ区切りのリストで指定します。
ユーザー名	MQ サービスでの認証に使用するユーザー名。
パスワード	**オプション:** MQ サービスでの認証に使用するパスワード。
EPS スロットル	1 秒当たりの最大イベント数 (EPS) の上限。
着信メッセージのエンコード (Incoming Message Encoding)	着信メッセージによって使用される文字エンコード。

Okta REST API プロトコルの構成オプション

Okta からイベントを受信するには、Okta REST API プロトコルを使用するようにログ・ソースを構成します。

Okta REST API プロトコルは、Okta Events and Users API エンドポイントを照会して、組織内のユーザーによって実行されたアクションに関する情報を取得します。

Okta REST API プロトコルのプロトコル固有のパラメーターについて、以下の表で説明します。

表 16. Okta REST API プロトコルのパラメーター

パラメーター	説明
IP またはホスト名	oktaprise.okta.com
認証トークン	Okta コンソールによって生成され、すべての API トランザクションで使用する必要がある単一認証トークン。
プロキシーの使用 (Use Proxy)	プロキシーが構成されている場合は、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Okta にアクセスします。 **「プロキシー IP またはホスト名 (Proxy IP or Hostname)」**、**「プロキシー・ポート」**、**「プロキシー・ユーザー名」**、および**「プロキシー・パスワード」**の各フィールドを構成します。プロキシーが認証を必要としない場合、**「プロキシー・ユーザー名」**フィールドと**「プロキシー・パスワード」**フィールドはブランクのままでかまいません。
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	リストから**「はい」**を選択すると、QRadar は証明書をダウンロードし、ターゲット・サーバーを信頼して使用し始めます。
繰り返し (Recurrence)	ログ・ソースがいつデータを収集するかを指定できます。フォーマットは、月/時刻/日を表す M/H/D です。デフォルトは、1 M です。
EPS スロットル	1 秒あたりのイベント数の最大限度。

OPSEC/LEA プロトコルの構成オプション

ポート 18184 でイベントを受信するには、OPSEC/LEA プロトコルを使用するようにログ・ソースを構成します。

OPSEC/LEA プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 17. OPSEC/LEA プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**OPSEC/LEA**
サーバー・ポート	QRadar が OPSEC/LEA プロトコルを使用してポート 18184 で通信できることを確認する必要があります。
統計レポートの間隔	Syslog イベント数が `qradar.log` ファイルに記録される期間を秒数で入力します。

表 17. OPSEC/LEA プロトコルのパラメーター (続き)

パラメーター	説明
OPSEC アプリケーション・オブジェクトの SIC 属性 (SIC 名)	SIC (Secure Internal Communications) 名は、アプリケーションの識別名 (DN) です (例えば CN=LEA,o=fwconsole..7psasx)。
ログ・ソースの SIC 属性 (SIC エンティティー名)	サーバーの SIC 名 (例えば cn=cp_mgmt,o=fwconsole..7psasx)。
OPSEC アプリケーション	証明書要求を実行するアプリケーションの名前。

重要: アップグレード後にエラー・メッセージ「**SSL 証明書をプルできません (Unable to pull SSL certificate)**」を受信した場合は、以下の手順を実行します。

1. 「**証明書の指定 (Specify Certificate)**」チェック・ボックスをクリアします。
2. 「**証明書パスワードのプル**」のパスワードを再入力します。

Oracle データベース・リスナー・プロトコルの構成オプション

Oracle データベース・サーバーから生成されるログ・ファイルをリモート側で収集するには、Oracle データベース・リスナー・プロトコル・ソースを使用するようにログ・ソースを構成します。

ログ・ファイルを処理のためにモニターするように Oracle データベース・リスナー・プロトコルを構成する前に、Oracle データベースのログ・ファイルのディレクトリー・パスを取得する必要があります。

Oracle データベース・リスナー・プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 18. Oracle データベース・リスナー・プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Oracle データベース・リスナー**
ファイル・パターン	イベント・ログを識別する正規表現。

PCAP と Syslog を組み合わせたプロトコルの構成オプション

パケット・キャプチャー (PCAP) データを転送する Juniper Networks SRX シリーズ・アプライアンスからイベントを収集するには、PCAP と Syslog を組み合わせたプロトコルを使用するようにログ・ソースを構成します。

PCAP と Syslog を組み合わせたプロトコルを使用するログ・ソースを構成する前に、Juniper Networks SRX アプライアンスで構成されている発信 PCAP ポートを判別してください。PCAP データをポート 514 に転送することはできません。

PCAP と Syslog を組み合わせたプロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 19. PCAP と Syslog を組み合わせたプロトコルのパラメーター

パラメーター	説明
プロトコル構成	**PCAP と Syslog の組み合わせ (PCAP Syslog Combination)**

表 19. PCAP と Syslog を組み合わせたプロトコルのパラメーター (続き)

パラメーター	説明
受信 PCAP ポート	Juniper Networks SRX シリーズ・アプライアンスで発信 PCAP ポートが編集されている場合は、ログ・ソースを編集して、着信 PCAP ポートを更新する必要があります。「**受信 PCAP ポート**」フィールドを編集した後、その変更内容をデプロイする必要があります。

SDEE プロトコルの構成オプション

Security Device Event Exchange (SDEE) プロトコルを使用するようにログ・ソースを構成することができます。QRadar はこのプロトコルを使用して、SDEE サーバーを使用するアプライアンスからイベントを収集します。

SDEE プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 20. SDEE プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**SDEE**
URL	ログ・ソースにアクセスするために必要な HTTP または HTTPS の URL (例えば https://www.mysdeeserver.com/cgi-bin/sdee-server)。 SDEE/CIDEE (Cisco IDS v5.x 以降) の場合は、URL の末尾が `/cgi-bin/sdee-server` でなければなりません。RDEP (Cisco IDS v4.x) を持つ管理者の場合は、URL の末尾が `/cgi-bin/event-server` でなければなりません。
サブスクリプションの強制	このチェック・ボックスを選択すると、プロトコルによって強制的に、サーバーが最もアクティブでない接続をドロップし、新規 SDEE サブスクリプション接続をこのログ・ソース用に受け入れるようになります。
イベントに対するブロックを待機する最大時間	コレクション要求が実行されたが新しいイベントを取得できない場合、このプロトコルではイベント・ブロックが有効になります。ブロックされるため、新しいイベントがなかったリモート・デバイスに対して別のイベント要求を実行できなくなります。このタイムアウトは、システム・リソースを節約することを目的としています。

SMB Tail プロトコルの構成オプション

SMB Tail プロトコルを使用するようにログ・ソースを構成することができます。このプロトコルは、イベント・ログに改行が追加される場合に、リモート側の Samba 共有でのイベントを監視し、Samba 共有からイベントを受信するために使用します。

SMB Tail プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 21. SMB Tail プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**SMB Tail**
ログ・フォルダー・パス	ログ・ファイルにアクセスするためのディレクトリー・パス。例えば、管理者が管理共有に `c$/LogFiles/` ディレクトリーを使用したり、公開共有フォルダー・パスに `LogFiles/` ディレクトリーを使用したりすることができます。しかし、`c:/LogFiles` ディレクトリーはログ・フォルダーのパスとしてサポートされていません。 ログ・フォルダーのパスに管理共有 (C$) が含まれている場合、その管理共有 (C$) に対する NetBIOS アクセス権を持つユーザーは、ログ・ファイルの読み取りに必要な特権を持っています。 ローカル・システム特権もドメイン管理者特権も、管理共有に存在するログ・ファイルにアクセスするために十分な権限を含んでいます。
ファイル・パターン	イベント・ログを識別する正規表現。
ファイル読み取りの強制 (Force File Read)	このチェック・ボックスをクリアした場合、QRadar が変更時刻またはファイル・サイズの変化を検出した場合にのみログ・ファイルが読み取られます。
スロットル・イベント数/秒	SMB Tail プロトコルが 1 秒当たり転送するイベントの最大数。

SNMPv2 プロトコルの構成オプション

SNMPv2 プロトコルを使用して SNMPv2 イベントを受信するようにログ・ソースを構成することができます。

SNMPv2 プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 22. SNMPv2 プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**SNMPv3**
コミュニティー	SNMP イベントが含まれているシステムにアクセスするために必要な SNMP コミュニティー名。
イベント・ペイロードに OID を含める (Include OIDs in Event Payload)	イベント・ペイロード形式ではなく、名前と値のペアを使用して SNMP イベント・ペイロードを構成するように指定します。 「**ログ・ソース・タイプ**」リストから特定のログ・ソースを選択した場合は、SNMPv2 イベントまたは SNMPv3 イベントを処理するためにイベント・ペイロードの OID が必要です。

SNMPv3 プロトコルの構成オプション

SNMPv3 プロトコルを使用して SNMPv3 イベントを受信するようにログ・ソースを構成することができます。

SNMPv3 プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 23. SNMPv3 プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**SNMPv3**
認証プロトコル	SNMP トラップの認証に使用するアルゴリズム。
イベント・ペイロードに OID を含める (Include OIDs in Event Payload)	標準のイベント・ペイロード形式ではなく、名前と値のペアを使用して SNMP イベント・ペイロードを構成するように指定します。「**ログ・ソース・タイプ**」リストから特定のログ・ソースを選択した場合は、SNMPv2 イベントまたは SNMPv3 イベントを処理するためにイベント・ペイロードの OID が必要です。

Seculert Protection REST API プロトコルの構成オプション

Seculert からイベントを受信するには、Seculert Protection REST API プロトコルを使用するようにログ・ソースを構成します。

Seculert Protection は、アクティブに情報の通信または引き出しを行っているマルウェアの確認済みインシデントに関するアラートを生成します。

Seculert のログ・ソースを構成するには、事前に Seculert Web ポータルから API 鍵を入手する必要があります。

1. Seculert Web ポータルにログインします。
2. ダッシュボードで、「**API**」タブをクリックします。
3. 「**Your API Key**」の値をコピーします。

Seculert Protection REST API プロトコルのプロトコル固有のパラメーターについて、以下の表で説明します。

表 24. Seculert Protection REST API プロトコルのパラメーター

パラメーター	説明
API 鍵	Seculert Protection REST API での認証に使用される API 鍵。API 鍵の値は Seculert Web ポータルから入手します。
プロキシーの使用 (Use Proxy)	プロキシーを構成すると、ログ・ソースのすべてのトラフィックが QRadar 用のプロキシーを経由して Seculert Protection REST API にアクセスします。 「**プロキシー IP またはホスト名 (Proxy IP or Hostname)**」、「**プロキシー・ポート**」、「**プロキシー・ユーザー名**」、および「**プロキシー・パスワード**」の各フィールドを構成します。プロキシーが認証を必要としない場合、「**プロキシー・ユーザー名**」フィールドと「**プロキシー・パスワード**」フィールドはブランクのままでかまいません。

表 24. Seculert Protection REST API プロトコルのパラメーター (続き)

パラメーター	説明
サーバー証明書を自動的に獲得 (Automatically Acquire Server Certificate(s))	リストから「**はい**」を選択すると、QRadar は証明書をダウンロードし、ターゲット・サーバーを信頼して使用し始めます。
繰り返し (Recurrence)	ログがいつデータを収集するかを指定します。フォーマットは、月/時刻/日を表す M/H/D です。デフォルトは、1 M です。
EPS スロットル	API から受信するイベントの、1 秒当たりの最大イベント数 (eps) の上限。

Sophos Enterprise Console JDBC プロトコルの構成オプション

Sophos Enterprise Console からイベントを受信するには、Sophos Enterprise Console JDBC プロトコルを使用するようにログ・ソースを構成します。

Sophos Enterprise Console JDBC プロトコルは、アプリケーション制御ログ、デバイス制御ログ、データ制御ログ、改ざんからの保護ログ、およびファイアウォール・ログからのペイロード情報を vEventsCommonData 表に結合します。Sophos Enterprise Console が Sophos Reporting Interface を備えていない場合は、標準の JDBC プロトコルを使用してアンチウィルス・イベントを収集できます。

Sophos Enterprise Console JDBC プロトコル用のパラメーターについて、以下の表で説明します。

表 25. Sophos Enterprise Console JDBC プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Sophos Enterprise Console JDBC**
データベース・タイプ	**MSDE**
データベース名	データベース名は、「**ログ・ソース ID**」フィールドで指定したデータベース名に一致している必要があります。
ポート	Sophos Enterprise Console での MSDE のデフォルト・ポートは 1168 です。JDBC 構成ポートは、QRadar と通信するための Sophos データベースのリスナー・ポートに一致している必要があります。Sophos データベースでは、着信 TCP 接続を有効にしておく必要があります。 MSDE データベース・タイプの場合に「**データベース・インスタンス**」を使用するときは、「**ポート**」パラメーターを空白のままにしておく必要があります。
認証ドメイン	ネットワークがドメインを使用しない場合は、このフィールドを空白のままにしてください。

表 25. Sophos Enterprise Console JDBC プロトコルのパラメーター (続き)

パラメーター	説明
データベース・インスタンス	データベース・インスタンス (必要な場合)。MSDE データベースでは、単一のサーバーに複数の SQL サーバー・インスタンスを含めることができます。 標準以外のポートをデータベースに使用する場合、または管理者が SQL データベース解決のためのポート 1434 へのアクセスをブロックしている場合は、「**データベース・インスタンス**」パラメーターを空白にする必要があります。
テーブル名	`vEventsCommonData`
選択リスト	*
比較フィールド	`InsertedAt`
準備済みステートメントの使用 (Use Prepared Statements)	準備済みステートメントを使用すると、プロトコル・ソースで SQL ステートメントをセットアップし、その SQL ステートメントを別のパラメーターで何度でも実行できるようになります。セキュリティー上およびパフォーマンス上の理由により、ほとんどの構成で準備済みステートメントを使用することができます。プリコンパイル・ステートメントを使用しない代替照会手法を使用する場合は、このチェック・ボックスをクリアしてください。
開始日時	オプション。プロトコルがデータベースのポーリングを開始できる開始日時。開始時刻が定義されていない場合、このプロトコルは、ログ・ソース構成が保存されてデプロイされた後にイベントをポーリングしようとします。
ポーリング間隔 (Polling Interval)	ポーリング間隔。データベースに対する照会から次の照会までの時間です。より長いポーリング間隔を定義するには、H (時間) または M (分) を数値に付加します。最大ポーリング間隔はどの時刻形式の場合も 1 週間です。指定子の H および M のない数値の場合は、秒単位のポーリングになります。
EPS スロットル	このプロトコルが超過できないようにするイベント/秒 (EPS) の数。
名前付きパイプ通信の使用 (Use Named Pipe Communication)	データベース・タイプとして MSDE を構成した場合、管理者はこのチェック・ボックスを選択して、TCP/IP ポート接続の代替方式を使用することができます。 MSDE データベースの名前付きパイプ接続を使用する場合は、「ユーザー名」フィールドおよび「パスワード」フィールドで、データベースのユーザー名とパスワードではなく、Windows 認証のユーザー名とパスワードを使用する必要があります。ログ・ソースの構成では、MSDE データベースのデフォルトの名前付きパイプを使用する必要があります。
データベース・クラスター名 (Database Cluster Name)	SQL サーバーをクラスター環境で使用する場合は、クラスター名を定義して、名前付きパイプ通信が確実に正しく機能するようにします。

表 25. *Sophos Enterprise Console JDBC プロトコルのパラメーター (続き)*

パラメーター	説明
NTLMv2 の使用	NTLMv2 認証を必要とする SQL サーバーの場合に、強制的に MSDE 接続で NTLMv2 プロトコルを使用します。このチェック・ボックスはデフォルトで選択されています。 「**NTLMv2 の使用**」チェック・ボックスを選択しても、NTLMv2 認証を必要としない MSDE 接続の通信には干渉しません。

Sourcefire Defense Center Estreamer プロトコルの構成オプション

Sourcefire Defense Center Estreamer (イベント・ストリーマー) サービスからイベントを受信するには、Sourcefire Defense Center Estreamer プロトコルを使用するようにログ・ソースを構成します。

Sourcefire Defense Center DSM を構成すると、イベント・ファイルが QRadar にストリーミングされて処理されます。

Sourcefire Defense Center Estreamer プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 26. *Sourcefire Defense Center Estreamer プロトコルのパラメーター*

パラメーター	説明
プロトコル構成	**Sourcefire Defense Center Estreamer**
サーバー・ポート	Sourcefire Defense Center Estreamer の場合に QRadar が使用するデフォルト・ポートは 8302 です。
鍵ストア・ファイル名	鍵ストアの秘密鍵と関連証明書のディレクトリー・パスおよびファイル名。デフォルトで、インポート・スクリプトが鍵ストア・ファイルを作成するディレクトリーは `/opt/qradar/conf/estreamer.keystore` です。
トラストストア・ファイル名	トラストストア・ファイルは、クライアントから信頼されている証明書を保持します。デフォルトで、インポート・スクリプトがトラストストア・ファイルを作成するディレクトリーは `/opt/qradar/conf/estreamer.truststore` です。
追加データの要求 (Request Extra Data)	Sourcefire Defense Center Estreamer からの追加データを要求するには、このオプションを選択します。例えば、追加データには、イベントの元の IP アドレスなどがあります。
拡張要求の使用 (Use Extended Requests)	eStreamer ソースからイベントを取得する代替メソッドを使用するには、このオプションを選択します。 拡張要求は、Sourcefire DefenseCenter Estreamer バージョン 5.0 以降でサポートされます。

Syslog リダイレクト・プロトコルの概要

Syslog リダイレクト・プロトコルは、Syslog プロトコルの代わりに使用します。このプロトコルは、イベントを送信した特定のデバイス名を QRadar に識別させる場合に使用します。QRadar は、UDP ポート 517 で Syslog イベントを受動的に listen できます。

Syslog リダイレクト・プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 27. Syslog リダイレクト・プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**Syslog リダイレクト**
ログ・ソース ID 正規表現 (Log Source Identifier RegEx)	`devname=([¥w-]+)`
Listen ポート	`517`
プロトコル	**UDP**

TCP 複数行 Syslog プロトコルの構成オプション

TCP 複数行 Syslog プロトコルを使用するログ・ソースを構成することができます。単一行イベントを作成するために、このプロトコルは正規表現を使用して、複数行イベントの開始パターンおよび終了パターンを識別します。

複数行イベントの例を以下に示します。

```
06/13/2012 08:15:15 PM
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5156
EventType=0
TaskCategory=Filtering Platform Connection
Keywords=Audit Success
Message=The Windows Filtering Platform permitted a connection.
Process ID: 4
Application Name: System
Direction: Inbound
Source Address: 1.1.1.1
Source Port: 80
Destination Address: 1.1.1.12
Destination Port:444
```

TCP 複数行 Syslog プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 28. TCP 複数行 Syslog プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**TCP 複数行 Syslog**
Listen ポート	デフォルトの Listen ポートは 12468 です。
イベント・フォーマッター (Event Formatter)	特に Windows 用に書式設定された複数行イベントの場合は、「**Windows 複数行 (Windows Multiline)**」オプションを使用します。

表 28. TCP 複数行 Syslog プロトコルのパラメーター (続き)

パラメーター	説明
イベント開始パターン (Event Start Pattern)	TCP 複数行イベント・ペイロードの開始を識別するために必要な正規表現。通常、Syslog ヘッダーは日時スタンプで始まります。このプロトコルでは、イベント開始パターン (タイム・スタンプなど) のみに基づく単一行イベントを作成できます。開始パターンしか使用できない場合、このプロトコルは、それぞれの開始値の間にあるすべての情報を取り込んで有効なイベントを作成します。
イベント終了パターン (Event End Pattern)	TCP 複数行イベント・ペイロードの最後のフィールドを識別するために必要な正規表現。Syslog イベントがすべて同じ値で終了する場合は、正規表現を使用してイベントの終了を判別することができます。このプロトコルでは、イベント終了パターンのみに基づくイベントをキャプチャーできます。終了パターンしか使用できない場合、このプロトコルは、それぞれの終了値の間にあるすべての情報を取り込んで有効なイベントを作成します。

TLS Syslog プロトコルの構成オプション

TLS Syslog イベント転送をサポートする最大 50 台のネットワーク・デバイスから暗号化された Syslog イベントを受信するには、TLS Syslog プロトコルを使用するようにログ・ソースを構成します。

ログ・ソースは、着信 TLS Syslog イベントの listen ポートを作成し、ネットワーク・デバイスに対する証明書ファイルを生成します。最大50 台のネットワーク・アプライアンスが、ログ・ソースに対して作成された listen ポートにイベントを転送することができます。50 台を超えるネットワーク・アプライアンスが必要な場合は、追加の listen ポートを作成してください。

TLS Syslog プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 29. TLS Syslog プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**TLS Syslog**
TLS listen ポート	デフォルトの TLS listen ポートは 6514 です。
認証モード (Authentication Mode)	TLS 接続が認証されるモード。「**TLS およびクライアント認証 (TLS and Client Authentication)**」オプションを選択した場合は、証明書パラメーターを構成する必要があります。
クライアント証明書パス (Client Certificate Path)	ディスク上のクライアント証明書の絶対パス。証明書は、このログ・ソースのコンソールまたはイベント・コレクターに保管する必要があります。
証明書タイプ (Certificate Type)	認証に使用する証明書のタイプ。「**証明書の提供 (Provide Certificate)**」オプションを選択した場合は、サーバー証明書および秘密鍵のファイル・パスを構成する必要があります。

表 29. TLS Syslog プロトコルのパラメーター (続き)

パラメーター	説明
提供されているサーバー証明書のパス (Provided Server Certificate Path)	サーバー証明書の絶対パス。
提供されている秘密鍵のパス (Provided Private Key Path)	秘密鍵の絶対パス。 **注:** 対応する秘密鍵は、DER エンコードの PKCS8 鍵でなければなりません。他の鍵形式の場合は、構成に失敗します。
最大接続数 (Maximum Connections)	「**最大接続数 (Maximum Connections)**」パラメーターは、各イベント・コレクターについて TLS Syslog プロトコルが許容できる同時接続の数を制御します。各イベント・コレクターについて、すべての TLS Syslog ログ・ソース構成で 1000 接続の制限があります。各デバイス接続のデフォルトは 50 です。 **注:** 別のログ・ソースとリスナーを共有する、自動的にディスカバーされたログ・ソースは、この制限に対して 1 回のみカウントされます。例えば、同一のイベント・コレクターで同一のポートを使用する場合です。

TLS Syslog のユース・ケース

作成できる構成の例を以下のユース・ケースに示します。

クライアント認証

このプロトコルがクライアント認証に関与できるようにするクライアント証明書を提供できます。このオプションを選択して証明書を提供すると、着信接続がクライアント証明書に照らして検証されます。

ユーザー提供のサーバー証明書

専用のサーバー証明書および対応する秘密鍵を構成できます。構成した TLS Syslog プロバイダーは、その証明書と鍵を使用します。着信接続には、自動的に生成された TLS Syslog 証明書ではなく、ユーザー提供の証明書が提示されます。

デフォルト認証

デフォルト認証方式を使用するには、「**認証モード (Authentication Mode)**」および「**証明書タイプ (Certificate Type)**」の各パラメーターにデフォルト値を使用します。ログ・ソースが保存されると、ログ・ソース・デバイスに対して `syslog-tls` 証明書が作成されます。この証明書を、暗号化された Syslog データを転送するネットワーク上のすべてのデバイスにコピーする必要があります。

UDP 複数行 Syslog プロトコルの構成オプション

単一行 Syslog イベントを複数行イベントから作成するには、UDP 複数行プロトコルを使用するようにログ・ソースを構成します。UDP 複数行 Syslog プロトコルは、正規表現を使用して複数行 Syslog メッセージを識別し、単一のイベント・ペイロードに再組み立てします。

元のイベントに含まれる値が正規表現を繰り返しており、その正規表現によって複数行イベントを識別して再組み立てできる必要があります。例えば、以下のイベントでは特定の値が繰り返されています。

```
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SEARCH RESULT tag=101
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH base="dc=iso-n,dc=com"
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH attr=gidNumber
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=1 SRCH base="dc=iso-n,dc=com"
```

UDP 複数行 Syslog プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 30. UDP 複数行 Syslog プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**UDP Multiline Syslog**
メッセージ ID のパターン	イベント・ペイロード・メッセージをフィルタリングするために必要な正規表現。UDP 複数行イベント・メッセージでは、イベント・メッセージの各行で共通の識別値が繰り返されている必要があります。

ログ・ソースが保存されると、ログ・ソースに対して syslog-tls 証明書が作成されます。この証明書を、暗号化された Syslog を転送するように構成されたネットワーク上のすべてのデバイスにコピーする必要があります。syslog-tls 証明書ファイルおよび TLS listen ポート番号を持つ他のネットワーク・デバイスは、TLS Syslog ログ・ソースとして自動的にディスカバーできます。

VMware vCloud Director プロトコルの構成オプション

VMware vCloud Director 仮想環境からイベントを収集するために、VMware vCloud Director プロトコルを使用するログ・ソースを作成できます。

VMware vCloud Director プロトコル用のプロトコル固有のパラメーターについて、以下の表で説明します。

表 31. VMware vCloud Director プロトコルのパラメーター

パラメーター	説明
プロトコル構成	**VMware vCloud Director**
vCloud URL	REST API にアクセスするために VMware vCloud アプライアンスで構成されている URL。この URL は、vCloud サーバーの VCD 公開 REST API の基本 URL として構成されているアドレス (`https://1.1.1.1.` など) に一致していなければなりません。
ユーザー名	vCloud サーバーへのリモート・アクセスに必要なユーザー名 (`console/user@organization` など)。vCloud Director プロトコルとともに使用する読み取り専用のアカウントを構成するには、ユーザーに「コンソール・アクセス専用 (Console Access Only)」権限が必要です。

バルク・ログ・ソースの追加

一度に最大 500 個の Microsoft Windows またはユニバーサル DSM のログ・ソースを追加できます。複数のログ・ソースを同時に追加する場合は、QRadar でバルク・ログ・ソースを追加します。バルク・ログ・ソースは、共通の構成を共有する必要があります。

手順

1. 「**管理**」タブをクリックします。
2. 「**ログ・ソース**」アイコンをクリックします。
3. 「**一括アクション**」リストから「**一括追加**」を選択します。
4. バルク・ログ・ソースのパラメーターを構成します。
   - ファイル・アップロード - 1 行に 1 つのホスト名または IP が含まれるテキスト・ファイルをアップロードします。
   - 手動 - 追加するホストのホスト名または IP を入力します。
5. 「**保存**」をクリックします。
6. 「**続行**」をクリックして、ログ・ソースを追加します。
7. 「**管理**」タブで「**変更のデプロイ**」をクリックします。

ログ・ソースの構文解析順序の追加

イベントがターゲット・イベント・コレクターで構文解析されるときの順序として、優先順位を割り当てることができます。

このタスクについて

共通の IP アドレスまたはホスト名を共有するログ・ソースに対して構文解析順序を定義することで、ログ・ソースの重要度を指定できます。ログ・ソースの構文解析順序を定義すると、ログ・ソース構成が変更されても、特定のログ・ソースが特定の順序で解析されるようになります。解析順序により、不要な解析が防止され、ログ・ソース構成に対する変更によってシステム・パフォーマンスが影響を受けることがなくなります。解析順序により、より重要なログ・ソースより先に低レベルのイベント・ソースが解析されることがなくなります。

手順

1. 「**管理**」タブをクリックします。
2. 「**ログ・ソースの構文解析順序**」アイコンをクリックします。
3. ログ・ソースを選択します。
4. オプション: 「**選択されたイベント・コレクター**」リストから、ログ・ソース構文解析順序を定義するイベント・コレクターを選択します。
5. オプション: 「**ログ・ソースのホスト**」リストから、ログ・ソースを選択します。
6. ログ・ソースの構文解析順序の優先順位を設定します。
7. 「**保存**」をクリックします。

第 2 章 ログ・ソース拡張

拡張文書により、特定のログ・ソースのエレメントを構文解析する方法を拡張したり変更したりすることができます。拡張文書を使用して、構文解析の問題を修正したり、既存の DSM からのイベントに対するデフォルトの構文解析をオーバーライドしたりすることができます。

拡張文書は、ネットワーク内のアプライアンスまたはセキュリティー・デバイスのイベントを解析する DSM が存在しないときにイベントのサポートを提供することもできます。

拡張文書は Extensible Markup Language (XML) 形式の文書であり、一般的な任意のテキスト・エディター、コード・エディター、またはマークアップ・エディターを使用して作成したり編集したりすることができます。複数の拡張文書を作成できますが、1 つのログ・ソースに適用できる拡張文書は 1 つだけです。

XML 形式では、すべての正規表現パターンを文字データ (CDATA) セクションに記述して、正規表現に必要な特殊文字がマークアップ書式に干渉しないようにする必要があります。例として、プロトコルを検出するための正規表現を以下のコードに示します。

```
<pattern id="ProtocolPattern" case-insensitive="true" xmlns="">
<![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
```

`(TCP|UDP|ICMP|GRE)` は正規表現パターンです。

ログ・ソース拡張の構成は、以下のセクションから構成されます。

パターン
特定のフィールド名に関連付ける正規表現パターン。パターンは、ログ・ソース拡張ファイル内で何度も参照されます。

比較グループ
構文解析される比較グループ内のエンティティー (EventName など)。構文解析のために適切なパターンおよびグループと組み合わせます。拡張文書には任意の数の比較グループを記述できます。

QRadar フォーラムでのログ・ソース拡張の例

サポートされる DSM がないログ・ソースの場合は、ログ・ソース拡張 (LSX) を作成できます。過去に作成した既存の拡張を変更すると、独自のログ・ソース拡張 (DSM 拡張とも呼びます) を簡単に作成できます。

DSM 拡張やカスタム・プロパティーなどの正規表現関連トピックのディスカッション・フォーラム (https://www.ibm.com/developerworks/community/forums/html/forum?id=11111111-0000-0000-0000-000000003046&ps=25) のログ・ソース拡張の例 (https://www.ibm.com/developerworks/community/forums/html/topic?id=d15cac8d-b0fa-4461-bb1e-dc1b291de440&ps=25) にアクセスできます。

IBM Security QRadar のフォーラムはオンラインのディスカッション・サイトであり、ユーザーと対象分野の専門家が共同作業したり情報を共有したりしています。

関連概念:

42 ページの『ログ・ソース拡張文書の作成』
サポートされる DSM がないログ・ソースの場合、情報の欠落や誤りがあるイベントを修復する場合、または関連付けた DSM が結果の生成に失敗するときにイベントを構文解析する場合には、ログ・ソース拡張 (LSX) を作成します。

ログ・ソース拡張文書のパターン

正規表現を特定のフィールド名に直接関連付けるのではなく、拡張文書の先頭で別個にパターン (patterns) を宣言します。これらの正規表現パターンは、ログ・ソース拡張ファイルの中で何度でも参照できます。

開始タグ <pattern> と終了タグ </pattern> の間にあるすべての文字が、パターンの構成要素と見なされます。パターンや <CDATA> 表現の内側や前後には余分なスペースや改行を記述しないでください。余分な文字やスペースがあると、意図したパターンに DSM 拡張が一致しなくなる可能性があります。

表 32. パターン・パラメーターの説明

パターン	タイプ	説明
id (必須)	ストリング	拡張文書の中で固有の、通常のストリング。
case-insensitive (オプション)	ブール値	true の場合は、大文字と小文字の違いを無視します。例えば、abc は ABC と同じです。 指定しない場合、このパラメーターはデフォルトで false になります。
trim-whitespace (オプション)	ブール値	true の場合は、ホワイト・スペースおよび改行を無視します。CDATA セクションを複数の行に分割しても、余分なスペースおよび改行がパターンの一部として解釈されることはありません。 指定しない場合、このパラメーターはデフォルトで false になります。

比較グループ

比較グループ (match-group) は、1 つ以上のイベント・タイプを構文解析または変更するために使用する一連のパターンです。

比較機能 は、構文解析される比較グループの中のエンティティー (EventName など) であり、構文解析のために適切なパターンおよびグループと組み合わせます。拡張文書には任意の数の比較グループを記述できます。

表 33. 比較グループ・パラメーターの説明

パラメーター	説明
order (必須)	比較グループを実行する順序を定義する正の整数。拡張文書の中で固有でなければなりません。
description (オプション)	比較グループの説明。任意のストリングを記述できます。この情報はログに出力できます。 指定しない場合、このパラメーターはデフォルトで空になります。
device-type-id-override (オプション)	別のデバイス ID を定義して QID をオーバーライドします。特定の比較グループが、指定のデバイスでイベント・タイプを検索できるようにします。有効なログ・ソース・タイプ ID でなければならず、整数で表す必要があります。ログ・ソース・タイプ ID のリストについては、 54 ページの表 40を参照してください。 指定しない場合のこのパラメーターのデフォルトは、拡張を接続するログ・ソースのログ・ソース・タイプです。

比較グループは以下のエンティティーを持つことができます。

- 『比較機能 (matcher)』
- 38 ページの『単一イベント修飾子 (event-match-single)』
- 38 ページの『複数イベント修飾子 (event-match-multiple)』

比較機能 (matcher)

比較機能エンティティーは、構文解析されるフィールド (EventName など) であり、構文解析のために適切なパターンおよびグループと組み合わせます。

比較機能には順序が関連付けられます。同じフィールド名に対して複数の比較機能が指定された場合は、正常に構文解析されるまで、または構文解析に失敗するまで、記述された順序で比較機能が実行されます。

表 34. 比較機能のパラメーターの説明

パラメーター	説明
field (必須)	パターンの適用対象フィールド (EventName や SourceIp など)。有効な比較機能フィールド名のリストの表に示した任意のフィールド名を使用できます。

表 34. 比較機能のパラメーターの説明 (続き)

パラメーター	説明
pattern-id (必須)	ペイロードにあるフィールドを構文解析するときに使用するパターン。この値は、以前にパターン ID パラメーター (32 ページの表 32) で定義したパターンの ID パラメーターに (大文字と小文字の違いも含めて) 一致していなければなりません。
order (必須)	同じフィールドに割り当てた比較機能の中で、このパターンを適用する順序。EventName フィールドに 2 つの比較機能を割り当てた場合は、order が最も小さいものが最初に適用されます。
capture-group (オプション)	正規表現における、小括弧 ( ) の内側を参照します。これらのキャプチャーの添字は 1 から始まり、パターンの左から右へ処理されます。capture-group フィールドは、パターンに存在するキャプチャー・グループの数以下の正の整数でなければなりません。デフォルト値は 0 であり、一致全体に相当します。 例えば、送信元 IP アドレスおよびポートに対して単一のパターンを定義できます。この場合、SourceIp という比較機能でキャプチャー・グループ 1 を使用し、SourcePort という比較機能でキャプチャー・グループ 2 を使用することができますが、定義する必要があるパターンは 1 つだけです。 enable-substitutions パラメーターと組み合わせた場合、このフィールドには 2 つの目的が備わります。 例については、拡張文書の例を参照してください。

表 34. 比較機能のパラメーターの説明 (続き)

パラメーター	説明
enable-substitutions (オプション)	ブール値 true に設定した場合は、連続したグループ・キャプチャーで適切にフィールドを表記することができません。複数のグループを追加のテキストと組み合わせて値を作成することができます。 このパラメーターにより、capture-group パラメーターの意味が変化します。capture-group パラメーターは新しい値を作成し、¥x (x は 1 から 9 までのグループ番号) を使用してグループ置換が指定されます。グループは何度でも使用でき、自由な形式の任意のテキストを値に挿入することもできます。例として、グループ 1 から値を生成し、その後に下線、グループ 2、@ が続いた後に再度グループ 1 が続く値を生成する場合に適したキャプチャー・グループの構文を以下のコードに示します。 capture-group="¥1_¥2@¥1" 別の例を示します。MAC アドレスはコロンで区切りますが、QRadar では通常 MAC アドレスをハイフンで区切ります。個々の部分を構文解析してキャプチャーする構文を以下の例に示します。 capture-group="¥1:¥2:¥3:¥4:¥5:¥6" 置換が有効であるがキャプチャー・グループでグループが指定されていない場合は、直接テキスト置換が実行されます。 デフォルトは false です。
ext-data (オプション)	拡張で比較機能フィールドが提供できる追加のフィールド情報および書式設定を定義する、追加のデータ・パラメーター。 このパラメーターを使用するフィールドは DeviceTime のみです。 例えば、デバイスが固有のタイム・スタンプを使用してイベントを送信するが、そのイベントを標準のデバイス時刻に書式設定し直したい場合が該当します。このイベントの日時スタンプを書式設定し直すには、DeviceTime フィールドに組み込んだ ext-data パラメーターを使用します。詳しくは、有効な比較機能フィールド名のリストを参照してください。

有効な比較機能フィールド名を以下の表に示します。

表 35. 有効な比較機能フィールド名のリスト

フィールド名	説明
EventName (必須)	イベントを識別するための、QID から取得するイベント名。 **注:** このパラメーターは、「**ログ・アクティビティー**」タブのフィールドとしては表示されません。
EventCategory	event-match-single エンティティーまたは event-match-multiple エンティティーによって処理されないカテゴリーを持つイベントに対するイベント・カテゴリー。 EventCategory は、EventName と組み合わせて QID でイベントを検索するために使用します。QIDmap ルックアップに使用するフィールドでは、既にデバイスが QRadar に認識されているときにオーバーライド・フラグをセットする必要があります。以下に例を示します。 `<event-match-single event-name= "Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity= "OverrideAndNeverSend" />` `force-qidmap-lookup-on-fixup="true"` がフラグのオーバーライドです。 **注:** このパラメーターは、「**ログ・アクティビティー**」タブのフィールドとしては表示されません。
SourceIp	メッセージの送信元 IP アドレス。
SourcePort	メッセージの送信元ポート。
SourceIpPreNAT	ネットワーク・アドレス変換 (NAT) 実行前のメッセージの送信元 IP アドレス。
SourceIpPostNAT	NAT 実行後のメッセージの送信元 IP アドレス。
SourceMAC	メッセージの送信元 MAC アドレス。
SourcePortPreNAT	NAT 実行前のメッセージの送信元ポート。
SourcePortPostNAT	NAT 実行後のメッセージの送信元ポート。
DestinationIp	メッセージの宛先 IP アドレス。
DestinationPort	メッセージの宛先ポート。
DestinationIpPreNAT	NAT 実行前のメッセージの宛先 IP アドレス。
DestinationIpPostNAT	NAT 実行後のメッセージの宛先 IP アドレス。
DestinationPortPreNAT	NAT 実行前のメッセージの宛先ポート。
DestinationPortPostNAT	NAT 実行後のメッセージの宛先ポート。

表 35. 有効な比較機能フィールド名のリスト (続き)

フィールド名	説明
DestinationMAC	メッセージの宛先 MAC アドレス。
DeviceTime	デバイスで使用する時刻および形式。デバイスによっては、この日時スタンプがイベントの送信時刻を表します。このパラメーターはイベントの受信時刻を表すわけではありません。ext-data の比較機能属性を使用することによって、`DeviceTime` フィールドでイベントのカスタム日時スタンプを使用できます。 `DeviceTime` フィールドで使用できる日時スタンプ形式の例を以下に示します。 • ext-data="dd/MMM/YYYY:hh:mm:ss" 11/Mar/2015:05:26:00 • ext-data="MMM dd YYYY / hh:mm:ss" Mar 11 2015 / 05:26:00 • ext-data="hh:mm:ss:dd/MMM/YYYY" 05:26:00:11/Mar/2015 データおよびタイム・スタンプの形式に使用可能な値について詳しくは、Joda-Time の Web ページ (http://www.joda.org/joda-time/key_format.html) を参照してください。 DeviceTime は、オプション・パラメーター ext-data を使用する唯一のイベント・フィールドです。
Protocol	イベントに関連付けるプロトコル (TCP、UDP、ICMP など)。
UserName	イベントに関連付けるユーザー名。
HostName	イベントに関連付けるホスト名。一般に、このフィールドはアイデンティティー・イベントに関連付けます。
GroupName	イベントに関連付けるグループ名。一般に、このフィールドはアイデンティティー・イベントに関連付けます。
NetBIOSName	イベントに関連付ける NetBIOS 名。一般に、このフィールドはアイデンティティー・イベントに関連付けます。
ExtraIdentityData	イベントに関連付けるユーザー固有データ。一般に、このフィールドはアイデンティティー・イベントに関連付けます。
SourceIpv6	メッセージの IPv6 送信元 IP アドレス。
DestinationIpv6	メッセージの IPv6 宛先 IP アドレス。

複数イベント修飾子 (event-match-multiple)

複数イベント修飾子 (event-match-multiple) は、pattern-id パラメーターおよび capture-group-index パラメーターでの指定に従って、一定の範囲のイベント・タイプに一致し、そのイベント・タイプを変更します。

この比較はペイロードに対して行われるのではなく、既にペイロードから構文解析された EventName 比較機能の結果に対して行われます。

このエンティティーにより、デバイス・イベント・カテゴリー、重大度、またはイベントがアイデンティティー・イベントの送信に使用する方式を変更して、正常なイベントを変換することができます。capture-group-index は整数値でなければならず (置換はサポートされていません)、pattern-ID は既存のパターン・エンティティーを参照する必要があります。それ以外のプロパティーは、いずれも単一イベント修飾子の対応するプロパティーと同じです。

単一イベント修飾子 (event-match-single)

単一イベント修飾子 (event-match-single) は、必須の EventName パラメーター (大文字と小文字を区別します) の指定に従って 1 つのイベント・タイプのみに一致し、それを変更します。

このエンティティーにより、デバイス・イベント・カテゴリー、重大度、またはアイデンティティー・イベントの送信方式を変更して、正常なイベントを変換することができます。

このイベント名に一致するイベントを構文解析するときには、デバイス・カテゴリー、重大度、およびアイデンティティー・プロパティーを結果イベントに適用します。

event-name 属性を設定する必要があります。この属性の値は **EventName** フィールドの値に一致します。そのほか、event-match-single エンティティーは以下のオプション・プロパティーから構成されます。

表 36. 単一イベント・パラメーターの説明

パラメーター	説明
device-event-category	イベントの QID を検索するための新規カテゴリー。このパラメーターは、一部のデバイスではすべてのイベントに同じカテゴリーが使用されることによる最適化パラメーターです。
severity	イベントの重大度。このパラメーターは 1 から 10 までの整数値でなければなりません。 1 未満または 10 を超える重大度を指定した場合は、デフォルトで 5 になります。 指定しない場合のデフォルトは、QID で検出した値です。

表 36. 単一イベント・パラメーターの説明 (続き)

パラメーター	説明
send-identity	イベントからのアイデンティティー変更情報を送信することを指定します。次のオプションのいずれかを選択してください。 • UseDSMResults DSM がアイデンティティー・イベントを返す場合は、そのイベントが渡されます。DSM がアイデンティティー・イベントを返さない場合、拡張はアイデンティティー情報を作成も変更もしません。 このオプションは、値が指定されていない場合のデフォルト値です。 • SendIfAbsent DSM がアイデンティティー情報を作成する場合、アイデンティティー・イベントは変更されずに渡されます。DSM がアイデンティティー・イベントを生成しないが、アイデンティティー・イベントの作成に十分な情報がイベントに存在する場合は、関連したフィールドがすべて設定されたイベントが生成されます。 • OverrideAndAlwaysSend 十分な情報がある場合は、DSM によって返されたアイデンティティー・イベントを無視し、新しいアイデンティティー・イベントを作成します。 • OverrideAndNeverSend DSM によって返されたアイデンティティー情報をすべて抑止します。アセット更新に渡すイベントを処理しない場合は、このオプションを推奨します。

拡張文書のテンプレート

ここに示す拡張文書の例では、特定のタイプの Cisco FWSM を構文解析し、誤ったイベント名でイベントが送信されないようにする方法を示します。

例として、以下のように session という単語がイベント名の中間に埋め込まれており、その単語を解決する場合を考えます。

```
Nov 17 09:28:26 129.15.126.6 %FWSM-session-0-302015:
Built UDP connection for faddr 38.116.157.195/80
gaddr 129.15.127.254/31696 laddr 10.194.2.196/2157
duration 0:00:00 bytes 57498 (TCP FINs)
```

この状態では DSM がイベントをまったく認識せず、すべてのイベントが構文解析されずに汎用ロガーに関連付けられてしまいます。

QID の検索にはテキスト・ストリングの一部 (302015) しか使用しませんが、イベントが Cisco FWSM から送信されたことはテキスト・ストリング全体 (%FWSM-session-0-302015) で示されています。テキスト・ストリング全体では有効にならないため、DSM はイベントが有効でないと見なします。

特定のイベント・タイプを構文解析するための拡張文書の例

FWSM デバイスには多くのイベント・タイプがあり、多くが固有の形式を持っています。以下の拡張文書の例では、特定のイベント・タイプを構文解析する方法を示します。

注: 構文解析するフィールド名にパターン ID が一致する必要はありません。以下の例ではパターンをコピーしていますが、この場合は SourceIp フィールドおよび SourceIpPreNAT フィールドにまったく同じパターンを使用できます。ただし、すべての FWSM イベントにこの状況が当てはまるとは限りません。

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z¥-]*¥d-(¥d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(tcp|udp|icmp|gre)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(¥d{1,6})]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
      <matcher field="EventName" order="1" pattern-id="EventNameFWSM_Pattern" capture-group="1"/>
      <matcher field="SourceIp" order="1" pattern-id="SourceIp_Pattern" capture-group="1" />
      <matcher field="SourcePort" order="1" pattern-id="SourcePort_Pattern" capture-group="2"/>
      <matcher field="SourceIpPreNAT" order="1" pattern-id="SourceIpPreNAT_Pattern" capture-group="1" />
      <matcher field="SourceIpPostNAT" order="1" pattern-id="SourceIpPostNAT_Pattern" capture-group="1" />
      <matcher field="SourcePortPreNAT" order="1" pattern-id="SourcePortPreNAT_Pattern" capture-group="2" />
      <matcher field="SourcePortPostNAT" order="1" pattern-id="SourcePortPostNAT_Pattern" capture-group="2" />
      <matcher field="DestinationIp" order="1" pattern-id="DestinationIp_Pattern" capture-group="1" />
      <matcher field="DestinationPort" order="1" pattern-id="DestinationIp_Pattern" capture-group="2" />
      <matcher field="Protocol" order="1" pattern-id="Protocol_Pattern" capture-group="1" />
      <matcher field="Protocol" order="2" pattern-id="Protocol_6_Pattern" capture-group="TCP" enable-substitutions=true/>
      <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
   </match-group>
</device-extension>

<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
<!-- Do not remove the "allEventNames" value -->
<pattern id="EventName-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceIp-Fakeware_Pattern" xmlns=""><![CDATA[]]</pattern>
<pattern id="SourcePort-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="SourceMAC-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationIp-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
<pattern id="DestinationPort-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<pattern id="Protocol-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
<match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceIp" order="1" pattern-id="SourceIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="SourcePort" order="1" pattern-id="SourcePort-Fakeware_Pattern" capture-group="1"/>
   <matcher field="SourceMAC" order="1" pattern-id="SourceMAC-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationIp" order="1" pattern-id="DestinationIp-Fakeware_Pattern" capture-group="1" />
   <matcher field="DestinationPort" order="1" pattern-id="SDestinationPort-Fakeware_Pattern" capture-group="1" />
   <matcher field="Protocol" order="1" pattern-id="Protocol-Fakeware_Pattern" capture-group="1" />
   <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall"/>
</match-group>
</device-extension>
```

構文解析の基礎

前記の拡張文書の例では、構文解析の基本的な側面のうち、以下のものを示しました。

- IP アドレス
- ポート
- プロトコル
- グループが異なるが同じパターンを使用する複数のフィールド

この例では、指定したパターンに従うすべての FWSM イベントを構文解析します。イベントの内容が異なる場合は、構文解析対象のフィールドがそのイベントに存在しない場合があります。

イベントで使用できなかった、この構成を作成するために必要であった情報は以下のとおりです。

- イベント名は、イベントの %FWSM-session-0-302015 部分の末尾 6 桁 (302015) のみです。
- FWSM は、Cisco ファイアウォールのデバイス・イベント・カテゴリーがハードコーディングされたものです。
- FWSM DSM は Cisco Pix QIDmap を使用するため、比較グループで device-type-id-override="6" というパラメーターを指定しています。Pix ファイアウォール・ログ・ソース・タイプの ID は 6 です。詳しくは、54 ページの『ログ・ソース・タイプの ID』を参照してください。

注: QID 情報が指定されていない場合や使用できない場合は、イベントのマッピングを変更できます。詳しくは、「*IBM Security QRadar SIEM ユーザーズ・ガイド*」の『イベントのマッピングの変更』を参照してください。

イベント名とデバイス・イベント・カテゴリー

QIDmap の検索時には、イベント名とデバイス・イベント・カテゴリーが必要です。このデバイス・イベント・カテゴリーはデータベース内のグループ化パラメーターであり、デバイス内の類似イベントの定義に役立ちます。比較グループの末尾にある event-match-multiple ではカテゴリーをハードコーディングしています。event-match-multiple は、構文解析したイベント名に対して EventNameId パターンを使用して 6 桁までの比較を行います。このパターンは、ペイロード全体に対してではなく、EventName フィールドとして構文解析された部分のみに対して実行されます。

EventName パターンはイベントの %FWSM 部分を参照します (すべての Cisco FWSM イベントに %FWSM 部分が含まれています)。例に示したパターンは、%FWSM の後に任意の数 (0 個以上) の英字およびダッシュが続いたものに一致します。このパターン・マッチングにより、イベント名の中間に埋め込まれた単語 session を削除する必要がある点が解決されます。イベントの重大度 (Cisco によるもの) の後にダッシュが続き、その後に QRadar が必要とする本当のイベント名が続きます。(¥d{6}) というストリングは、EventNameFWSM パターンの中のストリングで、唯一キャプチャー・グループを持っています。

イベントの IP アドレスとポートはすべて同じ基本パターンに従っており、IP アドレスの後にコロンとポート番号が続きます。このパターンは、データの 2 つの部分 (IP アドレスとポート) を構文解析し、matcher セクションで異なるキャプチャー・グループを指定しています。

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=¥[(¥d{2}/¥w{3}/¥d{4}:¥d{2}:¥d{2}:¥d{2})¥] </pattern>
<pattern id="Username">(TLSv1)</pattern>
<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1"
```

```
        capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
    <matcher field="UserName" order="1" pattern-id="Username" capture-group="1"/>
</match-group>
</device-extension>
```

IP アドレスとポートのパターン

IP アドレスとポートのパターンは、1 桁から 3 桁の数値 4 組をピリオドで区切ったものの後に、コロンとポート番号を続けたものです。IP アドレスの部分は 1 つのグループになっています。ポート番号も同様ですが、コロンは異なります。これらのフィールドに対する matcher セクションは同じパターン名を参照していますが、別のキャプチャー・グループを参照しています (IP アドレスはグループ 1 であり、ポートはグループ 2 です)。

プロトコルは共通のパターンであり、ペイロードで TCP、UDP、ICMP、または GRE のうち最初のものを検索します。パターンには大文字と小文字を区別しないパラメーターを指定しているため、すべての場合に一致します。

例で使用しているイベントに 2 番目のプロトコル・パターンは出現しませんが、順序を 2 として 2 番目のプロトコル・パターンを定義しています。順序の値が最も小さいプロトコル・パターンが一致しない場合は、次のパターンが適用されます (以後同様)。2 番目のプロトコル・パターンには直接置換も示しています。このパターンに比較グループはありませんが、enable-substitutions パラメーターが有効であるため、protocol=6 の代わりにテキスト TCP を使用できます。

ログ・ソース拡張文書の作成

サポートされる DSM がないログ・ソースの場合、情報の欠落や誤りがあるイベントを修復する場合、または関連付けた DSM が結果の生成に失敗するときにイベントを構文解析する場合には、ログ・ソース拡張 (LSX) を作成します。

公式な DSM がないログ・ソースの場合は、ユニバーサル DSM (UDSM) を使用してログ・ソースを統合します。それにより、ログ・ソース拡張 (デバイス拡張とも呼びます) が UDSM に適用されて、ログを構文解析するためのロジックが提供されます。LSX は Java 正規表現に基づいており、あらゆるログ・プロトコル (Syslog、JDBC、LFPS など) に対して使用できます。値をログから抽出して、QRadar 内のすべての共通フィールドにマップすることができます。

ログ・ソース拡張を使用してコンテンツの欠落や誤りを修復する場合は、ログ・ソース拡張によって生成されるすべての新規イベントが、元のペイロードの構文解析に失敗したログ・ソースに関連付けられます。拡張を作成すると、不明なイベントや未分類のイベントが IBM Security QRadar に「不明」として保管されることがなくなります。

ログ・ソース拡張を作成するには、以下の手順を実行します。

1. ログ・ソースが QRadar で作成されていることを確認します。

   リストにない項目を処理するには、ログ・ソースのタイプとしてユニバーサル DSM を使用します。ログ・ソースを手動で作成して、ログが自動的に分類されないようにすることもできます。

2. 使用可能なフィールドを判別するには、「**ログ・アクティビティー**」タブを使用してログをエクスポートした上で評価します。
3. 拡張文書のサンプル・テンプレートを使用して、使用できるフィールドを判別します。(39 ページの『拡張文書のテンプレート』).

   テンプレートにあるフィールドをすべて使用する必要はありません。ログ・ソースに存在し、拡張文書テンプレートのフィールドにマップできる値を判別します。詳しくは、 39 ページの『拡張文書のテンプレート』を参照してください。
4. 使用していないフィールドとそれに対応するパターン ID をログ・ソース拡張文書から削除します。
5. 拡張文書をアップロードして、拡張をログ・ソースに適用します。
6. イベントを、QIDmap の対応する要素にマップします。

   「**ログ・アクティビティー**」タブのこの手動アクションを使用すると、不明なログ・ソース・イベントが既知の QRadar イベントにマップされ、分類と処理が可能になります。

関連概念:

31 ページの『QRadar フォーラムでのログ・ソース拡張の例』
サポートされる DSM がないログ・ソースの場合は、ログ・ソース拡張 (LSX) を作成できます。過去に作成した既存の拡張を変更すると、独自のログ・ソース拡張 (DSM 拡張とも呼びます) を簡単に作成できます。

ユニバーサル DSM の作成

ユニバーサル DSM を作成するには、まず IBM Security QRadar でログ・ソースを作成します。ログ・ソースを作成するとき、ログは自動的に分類されないため、ログをエクスポートして検討することができます。

手順

1. 「**管理**」タブで、「**ログ・ソース**」アイコンをクリックして新しいソースを作成します。
2. 「**追加**」をクリックします。
3. 「**ログ・ソース名**」フィールドに名前を指定します。
4. 「**ログ・ソース・タイプ**」リストで「**ユニバーサル DSM**」を選択します。

   ログ・ソース拡張をまだ QRadar コンソールに適用していないときは、「**ログ・ソース拡張**」が表示されない場合があります。
5. 「**プロトコル構成**」リストで、使用するプロトコルを指定します。

   この手段は、サポートされていないログ・ソースからログを取得するために QRadar が使用します。
6. 「**ログ・ソース ID**」に、サポートされていないログ・ソースの IP アドレスまたはホスト名のいずれかを入力します。
7. 「**保存**」をクリックして新しいログ・ソースを保存し、ウィンドウを閉じます。
8. 「**管理**」タブで「**変更のデプロイ**」をクリックします。

次のタスク

『ログのエクスポート』

ログのエクスポート

ユニバーサル DSM を作成したら、作成されたログをエクスポートします。

このタスクについて

通常、検討のためにはかなりの数のログが必要です。サポートされていないログ・ソースの EPS レートによっては、全体をカバーできるログ・サンプルの取得に数時間かかる場合があります。

QRadar がログ・ソース・タイプを検出できない場合、イベントは収集されますが、構文解析されません。これらの構文解析されないイベントにフィルターを適用して、最後に受信したシステム通知を確認することができます。システム通知を検討した後、その時間フレームに基づいた検索を作成できます。

手順

1. 構文解析されないイベントのみを参照するために、ログをフィルタリングします。
   a. 「**ログ・アクティビティー**」タブをクリックします。
   b. 「**フィルターの追加**」をクリックします。
   c. 「**未解析のイベント**」を選択します。

      ヒント: 「**パラメーター**」テキスト・ボックスの中に入力して、「**未解析のイベント**」項目を表示します。
   d. 時間フレームを選択します。
   e. システム通知からの「**情報**」イベントが表示される場合は、右クリックして除外します。
   f. 「**送信元 IP**」列を確認して、イベントを送信しているデバイスを判別します。

      ロー・イベント・ペイロードを表示できます。通常、製造元では識別可能な製品名をヘッダーに書き込むため、検索を「**表示: Raw Event**」に設定すると、それぞれのイベントを手作業で開かなくてもペイロードを表示できます。ネットワークでソートする方法も、イベントの発信元である特定のデバイスを探すのに有効です。
2. ログをエクスポートするための検索を作成します。
   a. 「**ログ・アクティビティー**」タブで「**検索**」 > 「**検索の編集**」を選択します。
   b. 「**時刻範囲**」で、ログ・ソース作成からの十分な経過時間 (例えば 6 時間) を指定します。
   c. 「**パラメーター**」リストの「**検索パラメーター**」で、「**ログ・ソース (索引付き) (Log Source (Indexed))**」を選択し、「**演算子**」リストで「**次と等しい**」を選択し、「**ログ・ソース・グループ**」リストで「**その他**」を選択し、ユニ

バーサル DSM の作成時に作成されたログ・ソースを指定します。

注: 設定によっては、「**パラメーター**」リストに「**ログ・ソース (索引付き) (Log Source (Indexed))**」ではなく、「**ログ・ソース**」が表示される場合があります。

d. 「**検索**」をクリックして結果を表示します。

3. コンソールの結果を検討し、ペイロードを確認します。
4. オプションで、「**アクション**」 > 「**XML にエクスポート**」 > 「**完全エクスポート (すべての列)**」をクリックして結果をエクスポートすることができます。

「**CSV にエクスポート**」は選択しないでください。理由は、ペイロードが複数の列に分割される場合があり、ペイロードの検索が難しくなるためです。イベントの検討に適した形式は XML です。

a. 圧縮ファイルをダウンロードするように指示するプロンプトが出されます。圧縮ファイルを開き、生成されたファイルを開きます。

b. ログを検討します。

イベント・ペイロードは以下のタグの間にあります。

```
<payloadAsUTF>
...
</payloadAsUTF>
```

ペイロードの例を以下のコードに示します。

```
<payloadAsUTF>ecs-ep (pid 4162 4163 4164) is running... </payloadAsUTF>
```

ユニバーサル DSM の作成にあたっては、使いやすさの観点からログを検討することが重要です。少なくとも、イベント名にマップできる値がログに存在しなければなりません。イベント名は、さまざまなログ・タイプを識別できる固有の値でなければなりません。

使用可能なログの例を以下のコードに示します。

```
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root'
from 192.168.50.80:3364
May 20 17:16:26 dropbear[22331]: password auth succeeded for
'root' from 192.168.50.80:3364
May 20 16:42:19 kernel: DROP IN=vlan2 OUT=
MAC=00:01:5c:31:39:c2:08:00 SRC=172.29.255.121
DST=255.255.255.255 PROTO=UDP SPT=67 DPT=68
```

やや使いにくいログを以下のコード例に示します。

```
Oct 26 08:12:08 loopback 1256559128 autotrace[215824]: W: trace:
no map for prod 49420003, idf 010029a2, lal 00af0008
Oct 26 16:35:00 sxpgbd0081 last message repeated 7 times
Nov 24 01:30:00 sxpgbd0081 /usr/local/monitor-rrd/sxpgbd0081/.rrd
(rc=-1, opening '/usr/local/monitor-rrd/sxpgbd0081/.rrd':
No such file or directory)
```

一般的な正規表現

ログ・ソース・ファイルでテキストのパターンを比較するには、正規表現を使用します。メッセージで英字、数字、またはそれら両方の組み合わせのパターンをスキャンできます。例えば、送信元や宛先の IP アドレス、ポート、MAC アドレスなどに一致する正規表現を作成できます。

一般的な正規表現のいくつかを以下のコードに示します。

```
¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3} ¥d{1,5}
(?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2} (TCP|UDP|ICMP|GRE)
¥w{3}¥s¥d{2}¥s¥d{2}:¥d{2}:¥d{2}
¥s ¥t .*?
```

エスケープ文字 ¥ は、リテラル文字を示すために使用します。例えば、. 文字は「任意の 1 文字」を意味し、A、B、1、X などに一致します。. という文字に一致させる (リテラル比較を行う) には、¥. を使用する必要があります。

表 37. 一般的な正規表現

タイプ	正規表現
タイプ	¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}
IP アドレス	¥d{1,5}
ポート番号	(?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2}
プロトコル	(TCP|UDP|ICMP|GRE)
デバイス時刻	¥w{3}¥s¥d{2}¥s¥d{2}:¥d{2}:¥d{2}
ホワイト・スペース	¥s
タブ	¥t
すべてのストリングに一致	.*?

ヒント: 誤って別の文字に一致しないように、英数字以外の文字は必ずエスケープしてください。

正規表現パターンの作成

ユニバーサル DSM を作成するには、正規表現を使用して、サポートされていないログ・ソースからのテキスト・ストリングと比較します。

このタスクについて

以下の例に、参照するログ項目をステップに分けて示します。

```
May 20 17:24:59 kernel: DROP MAC=5c:31:39:c2:08:00
SRC=172.29.255.121 DST=10.43.2.10 LEN=351 TOS=0x00 PREC=0x00 TTL=64 ID=9582
PROTO=UDP SPT=67 DPT=68 LEN=331
May 20 17:24:59 kernel: PASS MAC=5c:14:ab:c4:12:59
SRC=192.168.50.10 DST=192.168.10.25 LEN=351 TOS=0x00 PREC=0x00 TTL=64
ID=9583 PROTO=TCP SPT=1057 DPT=80 LEN=331
May 20 17:24:59 kernel: REJECT
MAC=5c:ad:3c:54:11:07 SRC=10.10.10.5 DST=192.168.100.25 LEN=351
TOS=0x00 PREC=0x00 TTL=64 ID=9584 PROTO=TCP SPT=25212 DPT=6881 LEN=331
```

手順

1. サポートされていないログ・ソースを目視で分析し、固有のパターンを見つけ出します。

それらのパターンを、後で正規表現に変換します。

2. 比較するテキスト・ストリングを探します。

   ヒント: 基本的なエラー検査を実装するには、値の前後の文字を含めて、類似した値が意図せずに一致してしまう事態を防ぎます。後で、実際の値を余分な文字から分離することができます。

3. 比較パターンの疑似コードを作成して、パターンの先頭と末尾を示すスペース文字を含めます。

   引用符は無視して構いません。例に示したログ項目では、イベント名は DROP、PASS、および REJECT です。使用可能なイベント・フィールドを以下に示します。

   - EventName: " kernel: VALUE "
   - SourceMAC: " MAC=VALUE "
   - SourceIp: " SRC=VALUE "
   - DestinationIp: " DST=VALUE "
   - Protocol: " PROTO=VALUE "
   - SourcePort: " SPT=VALUE "
   - DestinationPort: " DPT=VALUE "

4. スペースは ¥s という正規表現で置き換えてください。

   英数字以外の文字には必ずエスケープ文字を使用してください。例えば = は ¥= とし、: は ¥: とします。

5. 疑似コードを正規表現に変換します。

表 38. 疑似コードから正規表現への変換

フィールド	疑似コード	正規表現
EventName	" kernel: VALUE "	¥skernel¥:¥s.*?¥s
SourceMAC	" MAC=VALUE "	¥sMAC¥=(?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2}¥s
SourceIP	" SRC=VALUE "	¥sSRC¥=¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥s
DestinationIp	" DST=VALUE "	¥sDST¥=¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥s
Protocol	" PROTO=VALUE "	¥sPROTO¥=(TCP|UDP|ICMP|GRE)¥s
SourcePort	" SPT=VALUE "	¥sSPT¥=¥d{1,5}¥s
DestinationPort	" DPT=VALUE "	¥sDPT¥=¥d{1,5}¥s

6. キャプチャー・グループを指定します。

   キャプチャー・グループは、正規表現の中の特定の値を分離します。

   例えば、前記の例に示した SourcePort パターンでは、スペースおよび SRC=<code> を含んでいるため、値全体を渡すことができません。代わりに、キャプチャー・グループを使用してポート番号のみを指定します。キャプチャー・グループの値は、IBM Security QRadar の関連フィールドに渡される値です。

   以下のように、取り込む値の前後に小括弧を挿入します。

表 39. 正規表現からイベント・フィールドのキャプチャー・グループへのマッピング

フィールド	正規表現	キャプチャー・グループ
EventName	¥skernel¥:¥s.*?¥s	¥skernel¥:¥s(.*?)¥s
SourceMAC	¥sMAC¥=(?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2}¥s	¥sMAC¥=((?:[0-9a-fA-F]{2}¥:){5}[0-9a-fA-F]{2})¥s
SourceIP	¥sSRC¥=¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥s	¥sSRC¥=(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})¥s
Destination IP	¥sDST¥=¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥s	¥sDST¥=(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})¥s
Protocol	¥sPROTO¥=(TCP¦UDP¦ICMP¦GRE)¥s	¥sPROTO¥=((TCP¦UDP¦ICMP¦GRE))¥s
SourcePort	¥sSPT¥=¥d{1,5}¥s	¥sSPT¥=(¥d{1,5})¥s
DestinationPort	¥sDPT¥=¥d{1,5}¥s	¥sDPT¥=(¥d{1,5})¥s

7. パターンおよびキャプチャー・グループをログ・ソース拡張文書に移行します。

   使用する文書の一部を以下のコード・スニペットに示します。

```
<device-extension xmlns="event_parsing/device_extension">
<pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z¥-]*¥d-(¥d{1,6})]]></pattern>
<pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})/([¥d]{1,5})]]></pattern>
<pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
<pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
<pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(¥d{1,6})]]></pattern>
```

QRadar への拡張文書のアップロード

複数の拡張文書を作成してアップロードし、さまざまなログ・ソース・タイプに関連付けることができます。それにより、ログ・ソース拡張 (LSX) によるロジックが、サポートされていないログ・ソースからのログを構文解析するために使用されます。

IBM Security QRadar にアップロードするまで、拡張文書は任意の場所に保管しておくことができます。

手順

1. 「**管理**」タブで「**データ・ソース**」 > 「**ログ・ソース拡張**」をクリックします。
2. 「ログ・ソース拡張の追加 (Add Log Source Extensions)」ウィンドウで「**追加**」をクリックします。
3. 名前を割り当てます。
4. ユニバーサル DSM を使用する場合は、「**ログ・ソース・タイプ**」のデフォルトとして拡張文書を選択しないでください。

   ユニバーサル DSM をデフォルトとして選択すると、関連付けたすべてのログ・ソースに影響が及びます。ユニバーサル DSM は、複数のカスタム・イベント・ソースおよびサポートされないイベント・ソースの構文解析ロジックを定義するために使用できます。
5. オプション: このログ・ソース拡張を特定のログ・ソース・タイプの複数のインスタンスに適用する場合は、使用可能な「**ログ・ソース・タイプ**」リストからログ・ソース・タイプを選択し、追加の矢印をクリックしてデフォルトとして設定します。

デフォルトのログ・ソース・タイプを設定すると、そのログ・ソース拡張が特定のログ・ソース・タイプ (および自動的にディスカバーされたログ・ソース) のすべてのイベントに適用されます。

イベントが正しく構文解析されるように、必ず最初にログ・ソース・タイプに対する拡張をテストしてください。

6. 「**参照**」をクリックして、保存してある LSX を見つけ、「**アップロード**」をクリックします。

   QRadar は、その文書を内部 XSD に照らして検証し、文書の妥当性を検査してから、拡張文書をシステムにアップロードします。

7. 「**保存**」をクリックしてウィンドウを閉じます。
8. ログ・ソース拡張をログ・ソースに関連付けます。
   a. 「**管理**」タブで「**データ・ソース**」 > 「**ログ・ソース**」をクリックします。
   b. 拡張文書の作成対象ログ・ソース・タイプをダブルクリックします。
   c. 「**ログ・ソース拡張**」リストから、作成した文書を選択します。
   d. 「**保存**」をクリックしてウィンドウを閉じます。

不明なイベントのマッピング

初期状態では、ユニバーサル DSM からのすべてのイベントが、QRadar の「**ログ・アクティビティー**」タブに「不明」と表示されます。手作業で、不明なすべてのイベントを QID マップの同等のものにマップする必要があります。

ログ・ファイルに表示すると、イベント名 (DROP、DENY、ACCEPT など) が分かりやすい値になっていることがありますが、QRadar は、これらの値が何を表すかを認識できません。QRadar にとってこれらの値は、既知のいずれの値にもマップされていないテキスト・ストリングです。これらの値は想定どおりに出力され、手作業でマップしない限り正規化イベントと見なされます。

侵入検知システム (IDS) や侵入検知防御システム (IDP) など、場合によっては数千件のイベントが存在し、そのマッピングが必要になります。このような場合には、イベント名そのものではなく、イベント名としてカテゴリーをマップすることができます。例えば以下の例では、マップの数を削減するために、イベント名に name フィールドを使用する代わりに category フィールドを使用しています。カスタム・プロパティーを使用すると、イベント名 (Code Red v412) を表示できます。

```
date: "Feb 25 2010 00:43:26"; name: "SQL Slammer v312"; category: "Worm
Activity"; source ip: "100.100.200.200";■date:
"Feb 25 2015 00:43:26"; name: "Code Red v412"; category: "Worm Activity";
source ip: "100.100.200.200"; date: "Feb 25 2015 00:43:26"; name:
"Annoying Toolbar"; category: "Malware"; source ip: "100.100.200.200";
```

イベント名に name フィールドを使用する代わりに、カテゴリー・フィールドを使用します。実際のイベント名 (Code Red v412 など) は、カスタム・プロパティーを使用して表示できます。

始める前に

ログ・ソース拡張文書をアップロードしてユニバーサル DSM に適用しておく必要があります。詳しくは、48 ページの『QRadar への拡張文書のアップロード』を参照してください。

手順

1. 「**ログ・アクティビティー**」タブで「**検索**」 > 「**検索の編集**」をクリックします。
2. 「**時刻範囲**」オプションから、ログ・ソース拡張をユニバーサル DSM に適用してからの十分な経過時間 (例えば 15 分) を選択します。
3. 「**検索パラメーター**」で、「**パラメーター**」リストから「**ログ・ソース [索引] (Log Source [Index])**」を選択し、「**演算子**」リストから「**次と等しい**」を選択し、「**ログ・ソース・グループ**」および「**ログ・ソース・リスト (Log Source lists)**」から作成したログ・ソースを選択します。
4. 「**検索**」をクリックして結果を表示します。

   すべてのイベントが「不明」と表示されます。
5. 「不明」の項目をダブルクリックして、イベントの詳細を表示します。
6. ツールバーにある「**イベントのマップ**」をクリックします。

   値「**ログ・ソースのイベント ID**」に、ログ・ソース拡張にある「**EventName 値 (EventName value)**」 (DROP、DENY、ACCEPT など) が表示されます。この値が空白になることはありません。値が空白である場合は、ログ・ソース拡張文書にエラーがあります。
7. 「**ログ・ソースのイベント ID**」として表示された値を、適切な QID にマップします。

   「**カテゴリー別に参照 (Browse By Category)**」、「**QID の検索**」、またはこれら両方を使用して、「**ログ・ソースのイベント ID**」の値に最もよく一致する値を探します。例えば、値 DROP は「**QID ファイアウォールの拒否 - イベント CRE (QID Firewall Deny - Event CRE)**」にマップできます。

   名前に「イベント CRE」を持つ QID を使用してください。大部分のイベントは、特定のログ・ソース・タイプに固有のものです。例えば、ランダム・ファイアウォールにマップする場合、「**拒否 QID (Deny QID)**」は、ユニバーサル DSM を別のログ・ソース・タイプからのイベントにマップする処理に似ています。「イベント CRE」という名前を含む QID 項目は汎用のものであり、特定のログ・ソース・タイプには結合されません。
8. 不明なすべてのイベントが正常にマップされるまで、上記の手順を繰り返します。

   これ以降は、特定のログ・ソース・イベント ID を含むユニバーサル DSM からのすべてのイベントが、指定した QID として表示されます。QID マッピングより前に受信したイベントは「不明」のままになります。前のイベントを現在の QID にマップする手段はサポートされていません。不明なすべてのイベント・タイプが正常に QID にマップされるまで、この処理を繰り返す必要があります。

構文解析の問題と例

ログ・ソース拡張を作成するときに、構文解析の問題が発生する場合があります。以下の XML 例を使用して、具体的な構文解析の問題を解決していきます。

プロトコルの変換

ペイロードのいずれかの位置で TCP、UDP、ICMP、または GRE を検索する代表的なプロトコル変換を以下の例に示します。この検索パターンは、なんらかの単語境界 (タブ、スペース、行末など) で囲まれています。また、大文字と小文字の違いを無視しています。

```
<pattern id="Protocol" case-insensitive="true" xmlns="">
<![CDATA[¥b(TCP|UDP|ICMP|GRE)¥b]]>
</pattern>
<matcher field="Protocol" order="1" pattern-id="Protocol" capture-group="1" />
```

1 回の置換

送信元 IP アドレスを構文解析し、その結果をオーバーライドして IP アドレスを 100.100.100.100 に設定し、ペイロードにある IP アドレスを無視する置換を以下の例に示します。

この例では、送信元 IP アドレスが SrcAddress=10.3.111.33 のような形式であり、その後にコンマが続くと想定しています。

```
<pattern id="SourceIp_AuthenOK" xmlns="">
<![CDATA[SrcAddress=(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}),]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIp_AuthenOK"
capture-group="100.100.100.100" enable-substitutions="true"/>
```

コロン区切りの MAC アドレスの生成

QRadar は、コロン区切りの形式の MAC アドレスを検出します。すべてのデバイスがこの形式を使用するとは限らないため、以下の例では、その状況に対処する方法について説明します。

```
<pattern id="SourceMACWithDashes" xmlns="">
    <![CDATA[SourceMAC=([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-
    ([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})]]>
</pattern>
 <matcher field="SourceMAC" order="1" pattern-id="
    SourceMACWithDashes" capture-group="¥1:¥2:¥3:¥4:¥5:¥6" />
```

前記の例では、SourceMAC=12-34-56-78-90-AB を 12:34:56:78:90:AB の MAC アドレスに変換します。

パターンからダッシュを削除すると、そのパターンによって MAC アドレスが変換されます (区切り記号なしです)。スペースを挿入すると、パターンによってスペース区切りの MAC アドレスが変換されます。

IP アドレスとポートの結合

通常、IP アドレスとポートは 1 つのフィールドに結合され、コロンによって区切られます。

以下の例では、1 つのパターンで複数のキャプチャー・グループを使用しています。

```
pattern id="SourceIPColonPort" xmlns="">
<! [CDATA[Source=(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}):([¥d]{1,5})]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIPColonPort" capture-group="1" />
<matcher field="SourcePort" order="1" pattern-id="SourceIPColonPort" capture-group="2" />
```

イベント・カテゴリーの変更

デバイス・イベントのカテゴリーをハードコーディングしたり、重大度を調整したりすることができます。

以下の例では、単一のイベント・タイプを対象として重大度を調整します。

```
<event-match-single event-name="TheEvent" device-event-category="Actual
Category" severity="6" send-identity="UseDSMResults" />
```

アイデンティティー変更イベントの抑止

DSM は、アイデンティティー変更イベントを必要以上に送信する場合があります。

アイデンティティー変更イベントが単一のイベント・タイプおよびイベント・グループから送信されないように抑止する方法を以下の例に示します。

```
// Never send identity for the event with an EventName of Authen OK
<event-match-single event-name="Authen OK" device-event-category="ACS"
severity="6" send-identity="OverrideAndNeverSend" />

// Never send any identity for an event with an event name starting with 7,
followed by one to five other digits:
<pattern id="EventNameId" xmlns=""><![CDATA[(7¥d{1,5})]]>
</pattern>

<event-match-multiple pattern-id="EventNameId" capture-group-index="1"
device-event-category="Cisco Firewall" severity="7"
send-identity="OverrideAndNeverSend"/>
```

ログのエンコード

以下のエンコード形式がサポートされています。

- US-ASCII
- UTF-8

US-ASCII 形式にも UTF-8 形式にも合致しないエンコードのログをシステムに転送できます。拡張フラグを構成すると、構文解析および保管の目的で入力を UTF-8 に再エンコードできるようにすることが可能です。

例えば、ソース・ログを SHIFT-JIS (ANSI/OEM 日本語) エンコードで受信したい場合は、以下のコードを入力します。

```
<device-extension source-encoding=SHIFT-JIS xmlns=event_parsing/device_extension>
```

ログは UTF-8 形式で保管されます。

イベント日時スタンプの書式設定

ログ・ソース拡張は、イベントの各種の日時スタンプ形式を検出できます。

デバイスの製造元は標準的な日時スタンプの形式に従っていないため、ext-data というオプション・パラメーターをログ・ソース拡張に組み込んで、DeviceTime を書式設定し直せるようにします。イベントを書式設定し直して日時スタンプの形式を修正する方法を以下の例に示します。

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=¥[(¥d{2}/¥w{3}/¥d{4}:¥d{2}:¥d{2}:¥d{2})¥]</pattern>
<pattern id="Username">(TLSv1)</pattern>

<match-group order="1" description="Full Test">
   <matcher field="EventName" order="1" pattern-id="EventName1_Pattern" capture-group="1"/>
   <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1_Pattern"
   capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
   <matcher field="UserName" order="1" pattern-id="Username_Pattern" capture-group="1"/>
</match-group>
</device-extension>
```

単一ログ・ソース内の複数のログ形式

場合によっては、単一のログ・ソース内に複数のログ形式が存在します。

```
May 20 17:15:50 kernel: DROP IN=vlan2 OUT= MAC= SRC=67.149.62.133
DST=239.255.255.250 PROTO=UDP SPT=1900 DPT=1900
May 20 17:16:26 dropbear[22331]: password auth succeeded for 'root' from 192.168.50.80:3364
May 20 17:16:28 dropbear[22331]: exit after auth (root): Exited normally </br>
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root' from 192.168.50.80:3364
```

例えば、ファイアウォール・イベントと認証イベントでログ形式が異なっているとします。このイベントを構文解析するには、複数のパターンを記述しなければなりません。構文解析する順序を指定できます。通常は、頻度の高いイベントを最初に構文解析し、その後に頻度の低いイベントを処理します。すべてのイベントを構文解析するために必要な数のパターンを記述することができます。order 変数により、パターンの比較順序が決定されます。

複数の形式を EventName フィールドと UserName フィールドに指定する例を以下に示します。

固有の各ログ・タイプを構文解析するために、個別のパターンを記述しています。正規化済みフィールドに値を割り当てるときに、両方のパターンが参照されます。

```
<pattern id="EventName-DDWRT-FW_Pattern" xmlns=""><![CDATA[kernel¥:¥s(.*?)¥s]]></pattern>
<pattern id="EventName-DDWRT-Auth_Pattern" xmlns=""><![CDATA[sdrophear¥[¥d{1,5}¥]|:¥s(.*?¥s.*?)¥s]]>
</pattern>

<pattern id="UserName_DDWRT-Auth1__Pattern" xmlns=""><![CDATA[¥sfor¥s¥'(.*?)¥'s]]></pattern>
<pattern id="UserName_DDWRT-Auth2__Pattern" xmlns=""><![CDATA[¥safter¥sauth¥s¥((.*?)¥)¥:]]></pattern>

<match-group order="1" description="DD-WRT Device Extensions xmlns="">
   <matcher field="EventName" order="1" pattern-id="EventName-DDWRT-FW_Pattern" capture-group="1"/>
   <matcher field="EventName" order="2" pattern-id="EventName-DDWRT-Auth_Pattern" capture-group="1"/>

   <matcher field="UserName" order="1" pattern-id="UserName-DDWRT-Auth1_Pattern" capture-group="1"/>
   <matcher field="UserName" order="2" pattern-id="UserName-DDWRT-Auth2_Pattern" capture-group="1"/>
```

CSV ログ形式の構文解析

CSV 形式のログ・ファイルは、複数のキャプチャー・グループを持つ単一のパーサーを使用できます。このログ・タイプを構文解析する場合、必ずしも複数のパターン ID を作成する必要はありません。

このタスクについて

以下のログ・サンプルを使用します。

```
Event,User,Source IP,Source Port,Destination IP,Destination Port
Failed Login,bjones,192.168.50.100,1024,10.100.24.25,22
Successful Login,nlabadie,192.168.64.76,1743,10.100.24.25,110
Privilege Escalation,bjones,192.168.50.100,1028,10.100.1.100,23
```

手順

1. 前記のパターンを使用して、関連したすべての値に一致するパーサーを作成します。

   ```
   .*?¥,.*?¥,¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}
   ¥,¥d{1,5}¥,¥d{1,3}¥.¥d{1,3} ¥.¥d{1,3}¥.¥d{1,3}¥,¥d{1,5}
   ```

2. それぞれの値を囲むキャプチャー・グループを記述します。

   ```
   (.*?)\,(.*?)¥,(¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.
   ¥d{1,3})¥,(¥d{1,5})¥,(¥d{1,3} ¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3})¥,(¥d{1,5})
   ```

3. 各キャプチャー・グループのマップ先フィールドを、移動につれて値を増加させながらマップします。

   ```
   1 = Event, 2 = User, 3 = Source IP,
   4 = Source Port, 5 = Destination IP, 6 = Destination Port
   ```

4. キャプチャー・グループを関連イベントにマップすることによって、値をログ・ソース拡張に組み込みます。

   キャプチャー・グループから関連イベントへのマップ例の一部を以下のコードに示します。

   ```
   <pattern id="CSV-Parser_Pattern" xmlns=""><![CDATA 9.*?)\,(.*?)¥,(¥d{1,3}¥.¥{1,3}¥.{1,3}]]></pattern>
   <match-group order="1" description="Log Source Extension xmlns="">
      <matcher field="EventName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="1"/>
      <matcher field="SourceIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="3"/>
      <matcher field="SourcePort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="4"/>
      <matcher field="DestinationIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="5"/>
      <matcher field="DestinationPort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="6"/>
      <matcher field="UserName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="2"/>
   ```

5. ログ・ソース拡張をアップロードします。
6. イベントをマップします。

関連タスク:

49 ページの『不明なイベントのマッピング』

初期状態では、ユニバーサル DSM からのすべてのイベントが、QRadar の「**ログ・アクティビティー**」タブに「不明」と表示されます。手作業で、不明なすべてのイベントを QID マップの同等のものにマップする必要があります。

ログ・ソース・タイプの ID

IBM Security QRadar は多くのログ・ソースをサポートしており、各ログ・ソースには ID が割り当てられています。ログ・ソース・タイプ ID は `match-group` ステートメントで使用します。

サポートされるログ・ソース・タイプとその ID を以下の表に示します。

表 40. ログ・ソース・タイプの ID

ID	ログ・ソース・タイプ
2	Snort Open Source IDS

表 40. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
3	Check Point Firewall-1
4	構成可能なファイアウォール・フィルター
5	Juniper Networks ファイアウォールおよび VPN
6	Cisco PIX ファイアウォール
7	構成可能な認証メッセージ・フィルター
9	Enterasys Dragon Network IPS
10	Apache HTTP Server
11	Linux OS
12	Microsoft Windows Security Event Log
13	Windows IIS
14	Linux iptables ファイアウォール
15	IBM Proventia Network Intrusion Prevention System (IPS)
17	Juniper Networks 侵入検知防御 (IDP)
19	TippingPoint 侵入防止システム (IPS)
20	Cisco IOS
21	Nortel Contivity VPN スイッチ
22	Nortel Multiprotocol Router
23	Cisco VPN 3000 シリーズ・コンセントレーター
24	Solaris オペレーティング・システム認証メッセージ
25	McAfee IntruShield ネットワーク IPS アプライアンス
26	Cisco CSA
28	Enterasys Matrix E1 スイッチ
29	Solaris オペレーティング・システム sendmail ログ
30	Cisco 侵入防御システム (IDS)
31	Cisco ファイアウォール・サービス・モジュール (FWSM)
33	IBM Proventia Management SiteProtector
35	Cyberguard FW/VPN KS ファミリー
36	Juniper Networks Secure Access (SA) SSL VPN
37	Nortel Contivity VPN スイッチ
38	Top Layer 侵入防止システム (IPS)
39	ユニバーサル DSM
40	Tripwire Enterprise
41	Cisco Adaptive Security Appliance (ASA)

表 40. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager (NSM)
46	Squid Web プロキシー
47	Ambiron TrustWave ipAngel 侵入防止システム (IPS)
48	Oracle RDBMS 監査レコード
49	F5 Networks BIG-IP LTM
50	Solaris オペレーティング・システム DHCP ログ
55	Array Networks SSL VPN アクセス・ゲートウェイ
56	Catalyst スイッチ用 Cisco CatOS
57	ProFTPD サーバー
58	Linux DHCP サーバー
59	Juniper Networks Infranet Controller
64	Juniper JunOS プラットフォーム
68	Enterasys Matrix K/N/S シリーズ・スイッチ
70	Extreme Networks ExtremeWare オペレーティング・システム (OS)
71	Sidewinder G2 Security Appliance
73	Fortinet FortiGate セキュリティー・ゲートウェイ
78	SonicWall UTM/ファイアウォール/VPN デバイス
79	Vericept Content 360
82	Symantec Gateway Security (SGS) Appliance
83	Juniper Steel Belted Radius
85	IBM AIX サーバー
86	Metainfo MetaIP
87	SymantecSystemCenter
90	Cisco ACS
92	Forescout CounterACT
93	McAfee ePolicy Orchestrator
95	Cisco NAC アプライアンス
96	TippingPoint X シリーズ・アプライアンス
97	Microsoft DHCP サーバー
98	Microsoft IAS サーバー
99	Microsoft Exchange Server
100	Trend Interscan VirusWall
101	Microsoft SQL Server

表 40. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
102	MAC OS X
103	Bluecoat SG アプライアンス
104	Nortel Switched Firewall 6000
106	3Com 8800 シリーズ・スイッチ
107	Nortel VPN Gateway
108	Nortel Threat Protection System (TPS) Intrusion Sensor
110	Nortel Application Switch
111	Juniper DX アプリケーション・アクセラレーション・プラットフォーム
112	SNARE Reflector Server
113	Cisco 12000 シリーズ・ルーター
114	Cisco 6500 シリーズ・スイッチ
115	Cisco 7600 シリーズ・ルーター
116	Cisco Carrier Routing System
117	Cisco サービス統合型ルーター
118	Juniper M シリーズ・マルチサービス・エッジ・ルーター
120	Nortel Switched Firewall 5100
122	Juniper MX シリーズ・イーサネット・サービス・ルーター
123	Juniper T シリーズ・コア・プラットフォーム
134	Nortel イーサネット・ルーティング・スイッチ 8300/8600
135	Nortel イーサネット・ルーティング・スイッチ 2500/4500/5500
136	Nortel Secure Router
138	OpenBSD OS
139	Juniper Ex シリーズ・イーサネット・スイッチ
140	Sysmark Power Broker
141	Oracle データベース・リスナー
142	Samhain HIDS
143	Bridgewater Systems AAA サービス・コントローラー
144	名前と値のペア
145	Nortel Secure Network Access Switch (SNAS)
146	Starent Networks Home Agent (HA)
148	IBM AS/400 iSeries
149	Foundry Fastiron

表 40. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
150	Juniper SRX シリーズ・サービス・ゲートウェイ
153	CRYPTOCard CRYPTOShield
154	Imperva Securesphere
155	Aruba モビリティー・コントローラー
156	Enterasys NetsightASM
157	Enterasys HiGuard
158	Motorola SymbolAP
159	Enterasys HiPath
160	Symantec Endpoint Protection
161	IBM RACF
163	RSA Authentication Manager
164	Redback ASE
165	Trend Micro Office Scan
166	Enterasys XSR セキュリティー・ルーター
167	Enterasys スタック可能スイッチおよびスタンドアロン・スイッチ
168	Juniper Networks AVT
169	OS サービスの Qidmap
170	Enterasys A シリーズ
171	Enterasys B2 シリーズ
172	Enterasys B3 シリーズ
173	Enterasys C2 シリーズ
174	Enterasys C3 シリーズ
175	Enterasys D シリーズ
176	Enterasys G シリーズ
177	Enterasys I シリーズ
178	Trend Micro Control Manager
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module (WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	HP Tandem
188	Sentrigo Hedgehog
189	Sybase ASE
191	Microsoft ISA
192	Juniper SRC
193	Radware DefensePro

表 40. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
194	Cisco ACE Firewall
195	IBM DB2
196	Oracle Audit Vault
197	Sourcefire Defense Center
198	Websense V Series
199	Oracle RDBMS OS 監査レコード
206	Palo Alto PA シリーズ
208	HP ProCurve
209	Microsoft Operations Manager
210	EMC VMWare
211	IBM WebSphere Application Server
213	F5 Networks BIG-IP ASM
214	FireEye
215	Fair Warning
216	IBM Informix
217	CA Top Secret
218	Enterasys NAC
219	System Center Operations Manager
220	McAfee Web Gateway
221	CA Access Control Facility (ACF2)
222	McAfee Application / Change Control
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Cyber-Ark Vault
228	Itron スマート・メーター
230	Bit9 Parity
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper Networks vGW
239	Oracle BEA WebLogic
240	Sophos Web セキュリティー・アプライアンス
241	Sophos Astaro Security Gateway
243	Infoblox NIOS
244	Tropos Control
245	Novell eDirectory

表 40. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
249	IBM Guardium
251	Stonesoft Management Center
252	SolarWinds Orion
254	Great Bay Beacon
255	Damballa Failsafe
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI
263	Digital China Networks DCS および DCRS シリーズ・スイッチ
264	Juniper Security Binary Log Collector
265	Trend Micro Deep Discovery
266	Tivoli Access Manager for e-business
268	Verdasys Digital Guardian
269	Huawei S シリーズ・スイッチ
271	HBGary Active Defense
272	APC UPS
272	Cisco Wireless LAN Controller
276	IBM Customer Information Control System (CICS)
278	Barracuda Spam & Virus Firewall
279	Open LDAP
280	Application Security DbProtect
281	Barracuda Web Application Firewall
283	Huawei AR シリーズ・ルーター
286	IBM AIX 監査
289	IBM Tivoli Endpoint Manager
290	Juniper Junos WebApp Secure
291	Nominum Vantio
292	Enterasys 800 シリーズ・スイッチ
293	IBM zSecure Alert
294	IBM Security Network Protection (XGS)
295	IBM Security Identity Manager
296	F5 Networks BIG-IP AFM
297	IBM Security Network IPS (GX)
298	Fidelis XPS
299	Arpeggio SIFT-IT
300	Barracuda Web Filter
302	Brocade FabricOS

表 40. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
303	ThreatGRID Malware Threat Intelligence Platform
304	IBM Security Access Manager for Enterprise Single Sign-On
306	Venustech Venusense Unified Threat Management
307	Venustech Venusense Firewall
308	Venustech Venusense Network Intrusion Prevention System
309	ObserveIT
311	Pirean Access: One
312	Venustech Venusense Security Platform
313	PostFix MailTransferAgent
314	Oracle ファイングレイン監査
315	VMware vCenter
316	Cisco Identity Services Engine
318	Honeycomb Lexicon File Integrity Monitor
319	Oracle Acme Packet SBC
320	Juniper 無線 LAN
330	Arbor Networks Peakflow SP
331	Zscaler Nss
332	Proofpoint Enterprise Protection/Enterprise Privacy
338	Microsoft Hyper-V
339	Cilasoft QJRN/400
340	Vormetric Data Security
341	SafeNet DataSecure/KeySecure
343	STEALTHbits StealthINTERCEPT
344	Juniper DDoS Secure
345	Arbor Networks Pravail
346	Trusteer Apex
348	IBM Security Directory Server
349	Enterasys A4 シリーズ
350	Enterasys B5 シリーズ
351	Enterasys C5 シリーズ
354	Avaya VPN Gateway
356	DG Technology MEAS
358	CloudPassage Halo
359	CorreLog Agent for IBM zOS
360	WatchGuard Fireware OS
361	IBM Fiberlink MaaS360

表 40. ログ・ソース・タイプの ID (続き)

ID	ログ・ソース・タイプ
362	Trend Micro Deep Discovery Analyzer
363	AccessData InSight
364	IBM Privileged Session Recorder
367	Universal CEF
369	FreeRADIUS
370	Riverbed SteelCentral NetProfiler
372	SSH CryptoAuditor
373	IBM WebSphere DataPower
374	Symantec Critical System Protection
375	Kisco Information Systems SafeNet/i
376	IBM Federated Directory Server
378	Lastline Enterprise
379	genua genugate
383	Oracle Enterprise Manager

第 3 章 ログ・ソース拡張の管理

ログ・ソース拡張を作成すると、特定のデバイスの構文解析ルーチンを拡張したり変更したりすることができます。

ログ・ソース拡張 とは、イベント・ペイロードからのイベントを識別し分類するために必要な正規表現パターンをすべて格納している XML ファイルです。構文解析の問題を修正する必要がある場合や、DSM からのイベントに対するデフォルトの構文解析をオーバーライドする必要がある場合は、拡張ファイルを使用してイベントを構文解析できます。ネットワーク内のアプライアンスまたはセキュリティー・デバイスのイベントを構文解析する DSM が存在しないときは、拡張によってイベントのサポートを提供できます。「**ログ・アクティビティー**」タブには、以下の基本的なタイプのログ・ソース・イベントが示されます。

- イベントを適切に構文解析するログ・ソース。適切に構文解析されたイベントは、正しいログ・ソース・タイプおよびカテゴリーに割り当てられます。この場合は介入も拡張も不要です。
- イベントを構文解析したが、「**ログ・ソース**」パラメーターの値が「**不明**」であるログ・ソース。不明なイベントとは、ログ・ソース・タイプが識別されるが、DSM がペイロード情報を認識できないログ・ソース・イベントのことです。システムが、使用可能な情報からイベント ID を判別してイベントを適切に分類することができません。この場合は、イベントをカテゴリーにマップするか、ログ・ソース拡張を作成して不明なイベントに対するイベント構文解析を修復することができます。
- ログ・ソース・タイプを識別できず、「**ログ・ソース**」パラメーターの値が「**保管**」イベントであるログ・ソース。イベントが保管される場合は、DSM ファイルを更新するか、ログ・ソース拡張を作成してイベントを適切に構文解析する必要があります。イベントを構文解析すると、イベントをマップできます。

ログ・ソース拡張を追加するには、拡張文書を作成する必要があります。拡張文書は XML 文書であり、任意の一般的なワード・プロセッサーやテキスト編集アプリケーションで作成できます。複数の拡張文書を作成してアップロードし、さまざまなログ・ソース・タイプに関連付けることができます。拡張文書の形式は、標準の XML スキーマ文書 (XSD) に従わなければなりません。拡張文書を作成するには、XML のコーディングに関する知識と経験が必要です。

ログ・ソース拡張の追加

ログ・ソース拡張を追加すると、特定のデバイスの構文解析ルーチンを拡張したり変更したりすることができます。

手順

1. 「**管理**」タブをクリックします。
2. 「**ログ・ソース拡張**」アイコンをクリックします。
3. 「**追加**」をクリックします。

4. 「**ログ・ソース・タイプ**」リストで、以下のいずれかのオプションを選択します。

オプション	説明
使用可能	このオプションは、デバイス・サポート・モジュール (DSM) がログ・ソースのほとんどのフィールドを正しく解析するときに選択します。正しく解析されないフィールドの値は、新しい XML 値で拡張されます。
次の項目のデフォルトに設定	拡張構文解析に追加するログ・ソース、または拡張構文解析から削除するログ・ソースを選択します。ログ・ソースに拡張を追加したり、ログ・ソースから拡張を削除したりすることができます。 ログ・ソース拡張がログ・ソースの「**次の項目のデフォルトに設定**」に設定されている場合は、同じ「**ログ・ソース・タイプ**」の新しいログ・ソースがその割り当てられたログ・ソース拡張を使用します。

5. 「**参照**」をクリックして、ログ・ソース拡張の XML 文書を見つけます。
6. 「**アップロード**」をクリックします。ログ・ソース拡張の内容が表示されます。適切な拡張ファイルをアップロードしようとしていることを確認します。ファイルのアップロード時には、拡張ファイルにエラーがないか XSD に照らして評価されます。
7. 「**保存**」をクリックします。

タスクの結果

拡張ファイルにエラーがない場合は、新しいログ・ソース拡張が作成されて有効になります。ログ・ソース拡張をログ・ソースに適用せずにアップロードすることができます。拡張の状況が変化すると、その内容が直ちに適用され、管理対象ホストまたはコンソールでログ・ソース拡張の新しいイベント構文解析パラメーターが適用されます。

次のタスク

「**ログ・アクティビティー**」タブで、イベントの構文解析パターンが正常に適用されていることを確認します。ログ・ソースがイベントを「**保管**」に分類している場合は、ログ・ソース拡張の構文解析パターンを調整する必要があります。ログ・ソース・イベントと拡張ファイルを照合することで、イベント構文解析の問題を特定することができます。

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

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

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

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

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

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

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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

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

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

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

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

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。

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

商標

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。

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

Java およびすべての Java 関連の商標およびロゴは 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。

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。

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。

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。

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。

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

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。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[タ行]

[ナ行]

[ラ行]

C

E

I

J

M

O

P

S

T

U

V

X

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