IBM Security QRadar

バージョン 7.2.6

ユーザーズ・ガイド

注記

本書および本書で紹介する製品を使用する前に、 275 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。

この資料は、IBM QRadar Security Intelligence Platform V7.2.6 に適用されます。また、この資料の更新版が公開されない限り、これ以降のリリースにも適用されます。

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 7.2.6
Users 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

このガイドについて ix

第 1 章 QRadar V7.2.6 のユーザー用の新機能 1

第 2 章 QRadar SIEM について 5
Security Intelligence 製品の機能 5
サポート対象の Web ブラウザー 7
Internet Explorer でのドキュメント・モードおよびブラウザー・モードの有効化 7
IBM Security QRadar ログイン 7
RESTful API 8
ユーザー・インターフェースの各タブ 9
「ダッシュボード」タブ 10
「オフェンス」タブ 10
「ログ・アクティビティー」タブ 10
「ネットワーク・アクティビティー」タブ 10
「アセット」タブ 10
「レポート」タブ 11
IBM Security QRadar Risk Manager 11
「管理」タブ 12
QRadar の共通手順 12
メッセージの表示 12
結果のソート 14
ユーザー・インターフェースの最新表示と一時停止 15
IP アドレスの調査 15
ユーザー名の調査 17
システム時刻 18
ユーザー設定の更新 18
オンライン・ヘルプへのアクセス 19
列のサイズ変更 19
ページ・サイズ 20

第 3 章 ダッシュボードの管理 21
デフォルトのダッシュボード 21
カスタム・ダッシュボード 21
ダッシュボードのカスタマイズ 22
フロー検索 22
オフェンス 23
ログ・アクティビティー 23
最新レポート 25
システム・サマリー 25
「リスクのモニター」ダッシュボード 25
ポリシー・コンプライアンスのモニター 26
リスクの変化のモニター 28
「脆弱性管理 (Vulnerability Management)」の項目 29
システム通知 30
インターネット脅威インフォメーション・センター 31
カスタム・ダッシュボードの作成 31
ダッシュボードを使用したログまたはネットワーク・アクティビティーの調査 32
グラフの構成 33
ダッシュボード項目の削除 35

ダッシュボード項目の切り離し 35
ダッシュボードの名前変更 35
ダッシュボードの削除 36
システム通知の管理 36
「項目の追加」リストへの検索ベースダッシュボード項目の追加 37

第 4 章 オフェンスの管理 39
オフェンスの概要 39
オフェンスに関する権限の考慮事項 39
重要な用語 39
オフェンスの保存 40
オフェンスのモニター 40
「すべてのオフェンス」ページや「自分のオフェンス」ページのモニター 41
カテゴリーでグループ化されたオフェンスのモニター 42
送信元 IP でグループ化されたオフェンスのモニター 43
宛先 IP でグループ化されたオフェンスのモニター 43
ネットワークでグループ化されたオフェンスのモニター 44
オフェンスの管理タスク 45
メモの追加 45
オフェンスの非表示 45
非表示のオフェンスの表示 46
オフェンスのクローズ 46
オフェンスの保護 47
オフェンスの保護解除 48
オフェンスのエクスポート 49
ユーザーへのオフェンスの割り当て 49
E メール通知の送信 50
フォローアップ項目のマーク付け 51
「オフェンス」タブ・ツールバーの機能 52
オフェンスのパラメーター 56

第 5 章 ログ・アクティビティーの調査 77
「ログ・アクティビティー」タブの概要 77
「ログ・アクティビティー」タブ・ツールバー 77
右クリック・メニューのオプション 82
ステータス・バー 82
ログ・アクティビティーのモニター 83
ストリーミング・イベントの表示 83
正規化イベントの表示 84
ロー・イベントの表示 87
グループ化されたイベントの表示 88
イベントの詳細 93
「イベントの詳細 (Event details)」ツールバー 97
関連するオフェンスの表示 98
イベントのマッピングの変更 99
フォールス・ポジティブのチューニング 100
PCAP データ 101
「PCAP データ」列の表示 101
PCAP 情報の表示 102
デスクトップ・システムへの PCAP ファイルのダウンロード 103
イベントのエクスポート 104

第 6 章 ネットワーク・アクティビティーの調査 105
「ネットワーク」タブの概要 105
「ネットワーク・アクティビティー」タブ・ツールバー 105
右クリック・メニューのオプション 108

ステータス・バー 109
オーバーフロー・レコード 109
ネットワーク・アクティビティーのモニター 110
ストリーミング・フローの表示 110
正規化フローの表示 111
グループ化されたフローの表示 114
フローの詳細 118
「フローの詳細 (Flow Details)」ツールバー 122
フォールス・ポジティブのチューニング 123
フローのエクスポート 124

第 7 章 アセットの管理 125
アセット・データのソース 126
入力アセット・データのワークフロー 127
アセット・データへの更新 127
アセット調整除外ルール 128
例: IP アドレスをブラックリストから除外するように調整されたアセット除外ルール 129
アセットのマージ 130
異常なアセット増加の検出 131
異常なアセット増加を示すシステム通知 132
例: ログ・ソース拡張の構成エラーが異常なアセット増加の原因になる過程 133
通常サイズしきい値を超えるアセット・プロファイルのトラブルシューティング 133
新規アセット・データのアセット・ブラックリストへの追加 134
アセット・ブラックリストとアセット・ホワイトリスト 135
アセット・ブラックリスト 135
アセット・ホワイトリスト 136
「アセット・プロファイル (Assets profile)」ページのパラメーター 137
アセット・プロファイル 137
脆弱性 138
「アセット」タブの概要 138
「アセット」タブのリスト 139
右クリック・メニューのオプション 141
アセット・プロファイルの表示 142
アセット・プロファイルの追加または編集 145
アセット・プロファイルの検索 150
アセット検索条件の保存 151
アセット検索グループ 152
検索グループの表示 152
新規検索グループの作成 153
検索グループの編集 154
別のグループへの保存済み検索のコピー 154
グループの削除またはグループからの保存済み検索の削除 154
アセット・プロファイルの管理タスク 155
アセットの削除 155
アセット・プロファイルのインポート 155
アセットのエクスポート 156
アセットの脆弱性の調査 157

第 8 章 グラフの管理 161
グラフの管理 161
時系列グラフの概要 162
グラフの凡例 163
グラフの構成 164

第 9 章 データの検索 167
イベントとフローの検索 167

基準と一致する項目の検索 167
検索条件の保存. 173
スケジュール済み検索 174
拡張検索オプション 175
AQL 検索ストリングの例 177
クイック・フィルターの検索オプション 181
オフェンスの検索 183
「自分のオフェンス」および「すべてのオフェンス」ページでのオフェンスの検索 183
「送信元 IP 別」ページでのオフェンスの検索 190
「宛先 IP 別」ページでのオフェンスの検索 192
「ネットワーク別 (By Networks)」ページでのオフェンスの検索 194
「**オフェンス**」タブでの検索条件の保存 195
検索条件の削除. 196
検索結果を詳細化するサブ検索の使用 197
検索結果の管理. 198
検索のキャンセル 198
検索結果の削除. 199
検索グループの管理 199
検索グループの表示 199
新規検索グループの作成. 200
検索グループの編集 201
保存済み検索の別のグループへのコピー 201
グループの削除またはグループからの保存済み検索の削除 201

第 10 章 カスタム・イベント・プロパティーとカスタム・フロー・プロパティー. 203
必要な権限 203
カスタム・プロパティー・タイプ. 203
正規表現ベースのカスタム・プロパティーの作成 204
計算ベースのカスタム・プロパティーの作成 206
カスタム・プロパティーの変更 208
カスタム・プロパティーのコピー. 210
カスタム・プロパティーの削除 210

第 11 章 ルールの管理 213
ルールの権限の考慮事項. 213
ルールの概要 213
ルールのカテゴリー 213
ルールのタイプ. 214
ルール条件 215
ルールの応答 215
ルールの表示 217
ルールの作成 218
アノマリ検出ルールの作成 220
ルール管理タスク 222
ルールの有効化と無効化. 222
ルールの編集 223
ルールのコピー. 223
ルールの削除 224
ルール・グループの管理. 224
ルール・グループの表示. 224
グループの作成. 225
項目のグループへの割り当て 225
グループの編集. 225
別のグループへの項目のコピー 226
グループからの項目の削除 226
グループの削除. 226

ビルディング・ブロックの編集 227
ルール・ページのパラメーター 227
「ルール」ページ・ツールバー 229
「ルールの応答」ページのパラメーター 231

第 12 章 ヒストリカル相関 243
ヒストリカル相関の概要 244
ヒストリカル相関プロファイルの作成 245
ヒストリカル相関の実行に関する情報の表示 246

第 13 章 X-Force Threat Intelligence フィードの統合 249
X-Force Threat Intelligence の更新およびサーバー 250
IBM Security QRadar での X-Force ルールの有効化 250
拡張された X-Force Threat Intelligence ルール 251
特定のタイプの Web サイトへのアクセスをモニターするための URL 分類を使用したルールの作成 252
X-Force Exchange での IP アドレスおよび URL 情報のルックアップ 253
フォールス・ポジティブの管理 254

第 14 章 レポートの管理 257
レポートのレイアウト 258
グラフ・タイプ 258
「レポート」タブ・ツールバー 259
グラフ・タイプ 261
カスタム・レポートの作成 262
レポートの編集 267
生成済みレポートの表示 267
生成されたコンテンツの削除 268
レポートの手動生成 268
レポートの複製 269
レポートの共有 269
レポートへの商標の設定 270
レポート・グループ 271
レポート・グループの作成 271
グループの編集 271
レポート・グループの共有 272
レポートのグループへの割り当て 273
別のグループへのレポートのコピー 274
レポートの削除 274

特記事項 275
商標 276
プライバシー・ポリシーに関する考慮事項 277

用語集 279
A 279
B 279
C 280
D 280
E 281
F 281
G 281
H 281
I 282
K 282
L 282
M 283

N 283
O 283
P 284
Q 284
R 284
S 285
T 286
V 286
W 286

索引 287

このガイドについて

「IBM® Security QRadar® SIEM ユーザーズ・ガイド」には、IBM Security QRadar SIEM の管理に関する情報が記載されています。この情報には、「ダッシュボード」、「オフェンス」、「ログ・アクティビティー」、「ネットワーク・アクティビティー」、「アセット」、および「レポート」の各タブに関する情報も含まれています。

対象読者

このガイドは、ネットワーク・セキュリティーの調査と管理を担当するすべての QRadar SIEM ユーザーを対象としています。このガイドは、QRadar SIEM へのアクセス権限とご使用の企業ネットワークとネットワーキング・テクノロジーに関する知識をお持ちの方を想定して記述されています。

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 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、企業内および企業外からの不適切なアクセスの防止、検出、およびそれらのアクセスへの対応により、システムおよび情報を保護する必要があります。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、あるいはご使用のシステムの損傷または他のシステムへの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 QRadar V7.2.6 のユーザー用の新機能

IBM Security QRadar V7.2.6 では、最適化された索引、プロパティーを比較する新しい CRE テスト、ライセンスの改善などが導入されています。

最適化された索引による検索パフォーマンスの向上

以前のリリースでは、索引が 1 分間の間隔ごとに作成されていました。QRadar V7.2.6 のスーパー索引では、索引データの構造が最適化され、毎時間の終わりに単一のスーパー索引が作成されるようになりました。特に複数時間検索では、QRadar はより最適に索引をスキャンするようになり、その結果、危殆化を示す痕跡 (IOC) タイプの検索では、パフォーマンスが 10 倍まで向上します。IOC タイプの検索のいくつかの例は、IP アドレス、ドメイン、およびホスト名に対する検索です。QRadar によって新規に受信されたすべてのデータには、自動的に新しい形式で索引が付けられます。

新規に受信されたデータの索引のみが最適化されます。ヒストリカル・データのパフォーマンスの向上について詳しくは、技術情報『Optimizing your Ariel indexes in 7.2.6』(http://www.ibm.com/support/docview.wss?uid=swg21968002) を参照してください。

新しい CRE テスト

新しいカスタム・ルール・エンジン (CRE) テストを使用して、プロパティー同士を比較することができます。カスタム・プロパティーとの比較も可能です。

送信元 IP アドレスを宛先 IP アドレスと比較できるようになりました。ユーザー名をカスタム・プロパティーと比較できます。詳細...

AQL WHERE 節文法を使用して、カスタム・ルール・エンジン (CRE) 内で複雑な比較を作成します。AND/OR ロジック、参照コンテナー・ルックアップ、およびアセット・モデル照会を使用できます。WHERE 節の作成時には、条件のみを入力します。詳細...

ライセンスの拡張

QRadar V7.2.6 では、イベントがご使用のライセンスに計上される方法が変更されます。以前のリリースでは、QRadar によって生成されたすべてのイベント (EPS 通知、システム通知、内部に生成されたログなど) がライセンスの対象としてカウントされました。このリリースでは、以下の内部イベントはライセンスの対象としてカウントされません。

- システム通知
- カスタム・ルール・エンジン (CRE)
- 監査
- ADE

- アセット・プロファイラー
- スケジュール済み検索の結果
- 正常性メトリック
- QRadar Risk Manager の質問、シミュレーション、内部ロギング。

お客様のオンプレミス環境にあるデバイスで生成されたイベントのみがライセンスに対してカウントされます。また、ルーティング・ルールを使用してドロップしたイベントの 60% が、最大で 2000 イベント/秒 (EPS) まで計上されます。

ルールおよび検索結果のリファレンス・セットの表示

データへのアクセスが拡張されています。以前は、管理者特権を持たないユーザーは、リファレンス・セット情報を使用できませんでした。このリリースでは、管理者は、ユーザーが検索結果および共通ルールにリファレンス・セットを表示できるように、アクセス権限を付与できます。ユーザーは、リファレンス・セットを検索および共通ルールに含めることができるようになりました。ユーザーは、リファレンス・セットのリスト (リファレンス・セットの内容) を表示したり、リファレンス・セットをエクスポートしたりすることができます。詳細...

右クリック・メニューのクイック・フィルター

このリリースでは、右クリック・メニューにイベントおよびフローの「クイック・フィルター」オプションが含まれています。クイック・フィルター基準を使用して、調査中にデータのピボット操作を行います。選択内容に一致する項目または一致しない項目を検索できます。一致/不一致フィルターを追加すると、より多くの検索基準を右クリック・メニューで使用できるようになります。詳細...

照会ワークフローの改善によるデータへのアクセスの迅速化

QRadar では、ユーザーがデータと対話する方法が改善されています。また、オフェンスの発生の前後の時間を簡単に拡張できます。「ネットワーク・アクティビティー」タブおよび「ログ・アクティビティー」タブにある時系列グラフのオプションを使用すると、アクティビティー・ビューを閉じなくても、表示される期間を簡単に変更できます。例えば、あるエンドポイントで火曜日の午後 4:30 に発生したオフェンスを調査している場合は、オフェンス自体からイベントにドリルダウンできます。「**検索の編集**」ページを開かなくても、注目している期間の数分前または数分後に発生したイベントを表示できます。期間を分単位で指定するか、ドロップダウン・リストから期間を拡張することができます。詳細...

ヒストリカル相関の機能拡張

IBM Security QRadar V7.2.6 では、脅威およびヒストリカル相関プロファイルと結果の管理の可視性が改善されています。

実際に発生している脅威の可視性の改善

IBM Security QRadar V7.2.5 では、ヒストリカル・オフェンスは、ヒストリカル相関の実行中にトリガーされたすべてのルールに対して作成されていま

した。V7.2.6 では、ヒストリカル・オフェンスは、検出されたイベントに対してオフェンスを作成する必要があることを指定するルールがトリガーされた場合にのみ作成されます。

監査の改善

監査レコードは、ヒストリカル相関プロファイルが実行またはキャンセルされるごとに作成されます。この変更により、モニター機能が拡張され、ヒストリカル相関を実行またはキャンセルしているユーザーを表示するための可視性が改善されます。

新しいオフェンス検索機能

選択されたヒストリカル相関プロファイルから作成されたオフェンスを検索できるようになりました。保存済み検索からヒストリカル相関結果を除外することもできます。これらの新しい検索パラメーターを使用して、レポート作成のためにリアルタイムのオフェンスからヒストリカル相関オフェンスを分離できます。

ヒストリカル相関プロファイルの管理の改善

処理しているヒストリカル・データのボリュームおよび指定する基準によっては、相関が完了するまでに長い時間がかかることがあります。実行されているかまたは実行キューに入れられたヒストリカル相関プロファイルをキャンセルできるようになりました。

「ヒストリカル相関」ウィンドウ内の列をソートおよびフィルタリングすると、探している情報を簡単に見つけることができます。

プロファイルの実行履歴を表示すると、ある実行で作成されたオフェンスの数を簡単に確認できます。シングルクリック操作で、ヒストリカル相関カタログをドリルダウンして、プロファイル基準に一致したイベントまたはフローのリストを表示します。

詳細...

新しい AQL ストリングおよび統計機能

ストリングの位置を特定するか、正規表現内のストリングを置換する場合は、拡張検索内で以下の Ariel 照会言語 (AQL) 機能を使用します。

機能	説明
strpos	ストリングが別のストリング内のどの位置にあるかを返します。
regex_replace	検索条件として正規表現を使用してストリングを置換します。
first	指定された列の最初のインスタンスを返します。
last	指定された列の最後のインスタンスを返します。
stddev	サンプル標準偏差を返します。
stddevp	母集団標準偏差を返します。

詳しくは、「*IBM Security QRadar Ariel 照会言語ガイド*」のサポートされる機能のセクションを参照してください。

第 2 章 QRadar SIEM について

QRadar SIEM は、ネットワーク・セキュリティー管理のプラットフォームで、フロー・ベースのネットワーク・ナレッジ、セキュリティー・イベント相関、およびアセット・ベースの脆弱性のアセスメントを組み合わせることによって、状況認識とコンプライアンスのサポートを提供します。

デフォルトのライセンス・キー

デフォルトのライセンス・キーでは、ユーザー・インターフェースへのアクセスを 5 週間提供します。 QRadar SIEM にログイン後、ウィンドウには一時的なライセンス・キーの有効期限が切れる日付が表示されます。ライセンス・キーのインストールの詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

セキュリティーの例外と証明書

Mozilla Firefox Web ブラウザーを使用する場合、Mozilla Firefox に例外を追加して QRadar SIEM にログインする必要があります。詳しくは、ご使用の Mozilla Firefox Web ブラウザーの資料を参照してください。

Microsoft Internet Explorer Web ブラウザーを使用する場合、QRadar SIEM システムにアクセスすると、Web サイトのセキュリティー証明書のメッセージが表示されます。 QRadar SIEM にログインするには、「**このサイトの閲覧を続行する**」オプションを選択する必要があります。

Web ベース・アプリケーションのナビゲート

QRadar SIEM を使用する場合、ご使用の Web ブラウザーの「**戻る**」ボタンではなく、QRadar SIEM のユーザー・インターフェース内で使用できるナビゲーション・オプションを使用します。

Security Intelligence 製品の機能

IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、およびヒストリカル相関などの機能について説明します。これらの機能は、一部の QRadar 製品では使用できないことがあります。使用している製品によっては、記載されているいくつかの機能をデプロイメント内で使用できないことがあります。必要な情報を利用できるように、各製品の機能を確認してください。

IBM Security QRadar SIEM には、オンプレミス・デプロイメント用のすべての Security Intelligence 機能が含まれています。QRadar SIEM は、ネットワーク上に分散しているデバイス・エンドポイントとアプリケーションからのログ・ソース・イベント・データを統合し、生データに対して正規化および相関アクティビティーを即時に実行して、実際に発生している脅威とフォールス・ポジティブを区別します。

IBM Security Intelligence on Cloud を使用して、ホストされた環境内のネットワークおよびセキュリティーの大量のイベント・ログを収集、分析、アーカイブ、および保管します。データを分析して、進展しつつある脅威を可視化し、コンプライアンスのモニターおよびレポートの要件に対応すると共に、総所有コストを引き下げます。

IBM Security QRadar Log Manager を使用して、ネットワークおよびセキュリティーの大量のイベント・ログを収集、分析、アーカイブ、および保管します。QRadar Log Manager は、データを分析して、進展しつつある脅威を可視化し、コンプライアンスのモニターおよびレポートの要件に対応できるように支援します。

詳しくは、各製品の機能を示している以下の表を参照してください。

表 1. QRadar 機能の比較

機能	QRadar SIEM	IBM Security Intelligence on Cloud	IBM Security QRadar Log Manager
ホストされたデプロイメントのサポート	いいえ	はい	いいえ
カスタマイズ可能なダッシュボード	はい	はい	はい
カスタム・ルール・エンジン	はい	はい	はい
ネットワーク・イベントおよびセキュリティー・イベントの管理	はい	はい	はい
ホストおよびアプリケーションのログの管理	はい	はい	はい
しきい値ベースのアラート	はい	はい	はい
コンプライアンス・テンプレート	はい	はい	はい
データ・アーカイブ	はい	はい	はい
IBM Security X-Force® Threat Intelligence IP レピュテーション・フィードの統合	はい	はい	はい
WinCollect スタンドアロン・デプロイメント	はい	はい	はい
WinCollect 管理対象デプロイメント	はい	いいえ	はい
QRadar Vulnerability Manager の統合	はい	いいえ	はい
ネットワーク・アクティビティーのモニター	はい	いいえ	いいえ
アセット・プロファイル	はい	はい	いいえ [1]
オフェンス管理	はい	はい	いいえ
ネットワーク・フローのキャプチャーと分析	はい	いいえ	いいえ
ヒストリカル相関	はい	はい	いいえ
QRadar Risk Manager の統合	はい	いいえ	いいえ
QRadar Incident Forensics の統合	はい	いいえ	いいえ

[1] QRadar Log Manager では、QRadar Vulnerability Manager がインストールされている場合にのみアセット・データが追跡されます。

サポート対象の Web ブラウザー

IBM Security QRadar 製品の機能が正しく動作するためには、サポート対象の Web ブラウザーを使用する必要があります。

QRadar システムにアクセスすると、ユーザー名とパスワードの入力を求められます。このユーザー名とパスワードは、管理者が事前に構成しておく必要があります。

以下の表に、サポートされる Web ブラウザーのバージョンをリストします。

表 2. QRadar 製品でサポートされる Web ブラウザー

Web ブラウザー	**サポート対象のバージョン**
Mozilla Firefox	38.0 延長サポート版
32 ビット版の Microsoft Internet Explorer (ドキュメント・モードおよびブラウザー・モードを有効にすること)	10.0
32 ビット版および 64 ビット版の Microsoft Internet Explorer (ドキュメント・モードで Microsoft Internet Explorer 10 を選択すること)	11.0
Google Chrome	バージョン 46

Internet Explorer でのドキュメント・モードおよびブラウザー・モードの有効化

Microsoft Internet Explorer を使用して IBM Security QRadar 製品にアクセスする場合は、ドキュメント・モードおよびブラウザー・モードを有効にする必要があります。

手順

1. Internet Explorer Web ブラウザーで、F12 を押して「開発者ツール」ウィンドウを開きます。
2. 「**ブラウザー モード**」をクリックし、ご使用の Web ブラウザーのバージョンを選択します。
3. 「**ドキュメント モード**」をクリックし、ご使用の Internet Explorer リリースの「**Internet Explorer 標準 (Internet Explorer standards)**」を選択します。

IBM Security QRadar ログイン

IBM Security QRadar は、Web ベースのアプリケーションです。QRadar は、URL、ユーザー名、パスワードに関するデフォルトのログイン情報を使用します。

IBM Security QRadar コンソールにログインする場合は、以下の表の情報を参照してください。

表 3. *QRadar* のデフォルト・ログイン情報

ログイン情報	デフォルト
URL	https://<IP Address> (<IP Address> は、QRadar コンソールの IP アドレスです)。 IPv6 環境または混合環境で QRadar にログインするには、次のように IP アドレスを大括弧で囲みます。 `https://[<IP Address>]`
ユーザー名	admin
パスワード	インストール・プロセスで QRadar に割り当てられたパスワード。
ライセンス・キー	デフォルトのライセンス・キーを使用すると、システムに 5 週間アクセスすることができます。

RESTful API

Representational State Transfer (REST) アプリケーション・プログラミング・インターフェース (API) を使用して、HTTPS 照会を作成し、IBM Security QRadar を他のソリューションに統合します。

アクセス権限とユーザー・ロール権限

RESTful API にアクセスして使用するには、QRadar で管理ユーザー・ロール権限が付与されている必要があります。ユーザー・ロール権限の管理方法については、「*Administration Guide*」を参照してください。

REST API 技術資料のユーザー・インターフェースへのアクセス

API ユーザー・インターフェースは、以下の REST API インターフェースの説明および機能を提供します。

表 4. *REST API* インターフェース

REST API	説明
`/api/ariel`	データベース、検索、検索 ID、および検索結果を照会する。
`/api/asset_model`	モデル内のすべてのアセットのリストを返します。使用可能なすべてのアセット・プロパティー・タイプと保存済み検索をリスト表示したり、アセットを更新したりすることもできます。
`/api/auth`	現行セッションをログアウトし、無効化する。
`/api/help`	API 機能のリストに戻る。
`/api/siem`	すべてのオフェンスのリストを返します。
`/api/qvm`	QRadar Vulnerability Manager データの確認と管理を行います。
`/api/reference_data`	リファレンス・データ収集の表示と管理を行います。

表 4. REST API インターフェース (続き)

REST API	説明
/api/qvm	アセット、脆弱性、ネットワーク、オープン・サービス、フィルターを取得します。修復チケットの作成や更新を行うこともできます。
/api/scanner	スキャン・プロファイルに関連するリモート・スキャンの表示、作成、開始を行います。

REST API 技術資料のインターフェースは、他の製品に QRadar の機能を実装するために必要なコードの収集に使用できるフレームワークを提供します。

1. 技術資料インターフェースにアクセスするには、Web ブラウザーで https://*コンソールの IP アドレス*/api_doc という URL を入力してください。
2. アクセスする API のヘッダー (**/ariel** など) をクリックします。
3. アクセスしたいエンドポイントのサブヘッダーをクリックします (例えば **/databases**)。
4. 「試験 (Experimental)」または「プロビジョナル (Provisional)」のサブヘッダーをクリックします。

   注:

   API エンドポイントには、*experimental* または *stable* といういずれかの注釈が付けられます。

   Experimental
   API エンドポイントが完全にはテストされておらず、将来予告なしに変更または削除される可能性があることを示します。

   Stable API エンドポイントが完全にテストされ、サポートされていることを示します。
5. 「**Try it out**」をクリックすると、適切な形式の HTTPS 応答を受信します。
6. サード・パーティーのソリューションで実装する必要がある情報を検討して収集します。

QRadar API フォーラムとコード・サンプル

API フォーラムでは、よくある質問に対する回答や、テスト環境で使用できるサンプルの注釈付きコードなど、REST API に関する詳細情報を参照することができます。詳しくは、API フォーラム (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca) を参照してください。

ユーザー・インターフェースの各タブ

各機能は、それぞれのタブに分割されています。ログインすると、「**ダッシュボード**」タブが表示されます。

必要なデータや機能を見つけるために、各タブを簡単にナビゲートすることができます。

「ダッシュボード」タブ

「**ダッシュボード**」タブは、ログイン時に表示されるデフォルトのタブです。

「**ダッシュボード**」タブには、複数のダッシュボードをサポートするワークスペース環境が用意されています。このワークスペース環境で、QRadar によって収集されたネットワーク・セキュリティー、アクティビティー、データのビューを表示することができます。 5 つのデフォルト・ダッシュボードを使用することができます。各ダッシュボードには、ネットワークで発生したオフェンスに関するサマリー情報と詳細情報が示されます。セキュリティー操作やネットワーク操作に焦点を当てたカスタム・ダッシュボードを作成することもできます。 「ダッシュボード」タブの使用について詳しくは、ダッシュボードの管理を参照してください。

「オフェンス」タブ

「**オフェンス**」タブを使用すると、ネットワーク内で発生したオフェンスを表示し、さまざまなナビゲーション・オプションや強力な検索機能を使用してそのオフェンスを見つけることができます。

「**オフェンス**」タブから、オフェンスを調査して、問題の根本原因を判別することができます。問題を解決することもできます。

「**オフェンス**」タブについて詳しくは、オフェンスの管理を参照してください。

「ログ・アクティビティー」タブ

「**ログ・アクティビティー**」タブを使用すると、QRadar に送信されるイベント・ログをリアルタイムで調査したり、高度な検索を実行したり、構成可能な時系列グラフを使用してログ・アクティビティーを表示したりすることができます。

「**ログ・アクティビティー**」タブを使用すると、イベント・データを詳細に調査することができます。

詳しくは、ログ・アクティビティーの調査を参照してください。

「ネットワーク・アクティビティー」タブ

「**ネットワーク・アクティビティー**」タブを使用すると、送信されるフローをリアルタイムで調査したり、強力な検索を実行したり、構成可能な時系列グラフを使用してネットワーク・アクティビティーを表示したりできます。

フローとは、2 つのホスト間の通信セッションのことです。フロー情報を確認することにより、トラフィックの通信状況、(コンテンツ・キャプチャー・オプションが有効になっている場合は) 通信内容、および通信者を判別できます。フロー・データには、プロトコル、ASN 値、IFIndex 値、および優先順位などの詳細情報も含まれます。

詳しくは、ネットワーク・アクティビティーの調査を参照してください。

「アセット」タブ

QRadar は、ネットワーク内で稼働しているアセット、サーバー、ホストを自動的にディスカバーします。

自動ディスカバリーは、パッシブ・フロー・データと脆弱性データに基づいて実行され、QRadar によるアセット・プロファイルの作成を可能にします。

アセット・プロファイルは、ネットワーク内の既知の各アセットについて、アイデンティティー情報 (使用可能な場合) や各アセットで実行されているサービスなどの情報を提供します。このプロファイル・データは、フォールス・ポジティブを減少させるための相関の目的で使用されます。

例えば、特定のアセットで稼働している特定のサービスの使用を試みる攻撃が実行されたとします。この場合 QRadar は、この攻撃とアセット・プロファイルを相関させることにより、そのアセットがこの攻撃に対して脆弱であるかどうかを判別することができます。「**アセット**」タブを使用すると、検討済みのアセットを表示したり、特定のアセットを検索してそのアセットのプロファイルを表示したりすることができます。

詳しくは、アセットの管理を参照してください。

「レポート」タブ

「**レポート**」タブを使用して、QRadar 内のすべてのデータに関するレポートを作成、配布、および管理することができます。

レポート機能を使用すると、運用および実行用にカスタマイズされたレポートを作成することができます。レポートを作成するために、(セキュリティーまたはネットワークなどの) 情報を単一のレポートに組み合わせることができます。 QRadar に組み込まれている、プリインストールされたレポート・テンプレートを使用することもできます。

「**レポート**」タブを使用すると、カスタマイズされたロゴを使用してレポートにブランドを付けることもできます。このようなカスタマイズを行うとレポートをさまざまな対象者に配布する際に役立ちます。

レポートについて詳しくは、レポートの管理を参照してください。

IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager は、デバイス構成のモニター、ネットワーク環境に対する変更のシミュレート、およびネットワーク内のリスクおよび脆弱性の優先順位付けを行うための、別個にインストールされるアプライアンスです。

IBM Security QRadar Risk Manager は、ネットワークおよびセキュリティー・デバイス (ファイアウォール、ルーター、交換機、IPS など)、脆弱性フィード、およびベンダー・セキュリティー・ソースから得られる構成データによって収集されたデータを使用します。このデータは、ネットワーク・セキュリティー・インフラストラクチャー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識別し、またそれらのリスクがエクスプロイトされている可能性を示すために使用されます。

注: IBM Security QRadar Risk Manager について詳しくは、営業担当員にお問い合わせください。

「管理」タブ

管理者は、「管理」タブを使用して、ユーザー、システム、ネットワーク、プラグイン、コンポーネントの構成と管理を行うことができます。管理特権を持つユーザーは、「**管理**」タブにアクセスすることができます。

管理者が「**管理**」タブでアクセスできる管理ツールを 表 1 に示します。

表 5. QRadar で使用できる管理ツール

管理ツール	説明
システム構成 (System Configuration)	システムとユーザーの管理オプションを構成します。
データ・ソース	ログ・ソース、フロー・ソース、および脆弱性のオプションを構成します。
リモート・ネットワークおよびサービス構成	リモート・ネットワークとサービス・グループを構成します。
デプロイメント・エディター	QRadar デプロイメントの各コンポーネントを管理します。

「**管理**」タブで行った構成の更新は、すべてステージング・エリアに保存されます。すべての変更が完了したら、デプロイメント環境内の管理対象ホストに対する構成の更新内容をデプロイすることができます。

QRadar の共通手順

QRadar ユーザー・インターフェースの各種コントロールは、ほとんどのユーザー・インターフェース・タブで共通しています。

これらの共通手順について、以下の各セクションで説明します。

メッセージの表示

ユーザー・インターフェースの右上隅にある「**メッセージ**」メニューから、システム通知を読み取り、管理できるウィンドウにアクセスできます。

始める前に

「**メッセージ**」ウィンドウでシステム通知を表示するには、管理者が各通知メッセージ・タイプに基づくルールを作成し、「**カスタム・ルール・ウィザード**」で「**通知**」チェック・ボックスを選択する必要があります。

このタスクについて

「**メッセージ**」メニューには、システム内に存在する未読のシステム通知の数が示されます。このインディケーターでは、システム通知を閉じるまで数が増分します。「**メッセージ**」ウィンドウには、各システム通知のサマリーと、システム通知が作成された日付のスタンプが示されます。通知にマウス・ポインターを移動させることで、詳細を表示することができます。「**メッセージ**」ウィンドウの機能を使用して、システム通知を管理できます。

システム通知は、「**ダッシュボード**」タブとオプションのポップアップ・ウィンドウ (ユーザー・インターフェースの左下隅に表示できる) にも表示されます。「**メッセージ**」ウィンドウで実行するアクションは、「**ダッシュボード**」タブとポップアップ・ウィンドウに伝搬されます。例えば、「**メッセージ**」ウィンドウからシステム通知を閉じた場合、そのシステム通知はすべてのシステム通知表示対象から除外されます。

「ダッシュボード」のシステム通知について詳しくは、システム通知の項目について参照してください。

「**メッセージ**」ウィンドウでは、以下の機能が提供されます。

表 6. 「メッセージ」ウィンドウで使用できる機能

機能	説明
すべて	システム通知をすべて表示する場合は、「**すべて**」をクリックします。このオプションはデフォルトです。したがって、「**すべて**」をクリックするのは、別のオプションを選択した後で、すべてのシステム通知を再表示する場合のみです。
正常性	重大度レベルが「正常性」であるシステム通知のみを表示する場合は、「**正常性**」をクリックします。
エラー	重大度レベルが「エラー」であるシステム通知のみを表示する場合は、「**エラー**」をクリックします。
警告	重大度レベルが「警告」であるシステム通知のみを表示する場合は、「**警告**」をクリックします。
情報	重大度レベルが「情報」であるシステム通知のみを表示する場合は、「**情報**」をクリックします。
すべて消去 (Dismiss All)	システムからのシステム通知をすべて消去する場合は、「**すべて消去 (Dismiss All)**」をクリックします。「**正常性**」、「**エラー**」、「**警告**」、または「**情報**」アイコンを使用して、システム通知リストをフィルターした場合は、「**すべて表示**」アイコンのテキストが以下のいずれかのオプションに変わります。 • **すべてのエラーを閉じる (Dismiss All Errors)** • **すべての正常性を閉じる (Dismiss All Health)** • **すべての警告を閉じる (Dismiss All Warnings)** • **すべての警告を閉じる (Dismiss All Warnings)** • **すべての通知を閉じる (Dismiss All Info)**

表 6. 「メッセージ」ウィンドウで使用できる機能 (続き)

機能	説明
すべて表示	「**ログ・アクティビティー**」タブでシステム通知イベントを表示する場合は、「**すべて表示**」をクリックします。「**正常性**」、「**エラー**」、「**警告**」、または「**情報**」アイコンを使用して、システム通知リストをフィルターした場合は、「**すべて表示**」アイコンのテキストが以下のいずれかのオプションに変わります。 • **すべてのエラーを表示 (View All Errors)** • **すべての正常性を表示 (View All Health)** • **すべての警告を表示** • **すべての通知を表示 (View All Info)**
閉じる (Dismiss)	システムからのシステム通知を閉じる場合は、システム通知の横にある「**閉じる (Dismiss)**」アイコンをクリックします。

手順

1. QRadar にログインします。
2. ユーザー・インターフェースの右上隅にある「**メッセージ**」をクリックします。
3. 「**メッセージ**」ウィンドウで、システム通知の詳細を表示します。
4. オプション。システム通知リストを絞り込むには、以下のいずれかのオプションをクリックします。
   - **エラー**
   - **警告**
   - **情報**
5. オプション。システム通知を閉じるには、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
すべて消去 (Dismiss All)	システム通知をすべて閉じる場合にクリックします。
閉じる (Dismiss)	閉じるシステム通知の横にある「**閉じる (Dismiss)**」アイコンをクリックします。

6. オプション。システム通知の詳細を表示するには、システム通知にマウス・ポインターを移動します。

結果のソート

表内の結果は、列見出しをクリックすることでソートできます。列の最上部にある矢印はソート方向を示します。

手順

1. QRadar にログインします。

2. 表を降順でソートする場合は列見出しを 1 回クリックし、表を昇順でソートする場合は 2 回クリックします。

ユーザー・インターフェースの最新表示と一時停止

タブに表示されたデータを手動で最新表示、一時停止、および再生することができます。

このタスクについて

「**ダッシュボード**」タブと「**オフェンス**」タブは、60 秒ごとに自動的に最新表示されます。

「**ログ・アクティビティー**」タブおよび「**ネットワーク・アクティビティー**」タブは、「最後の間隔 (自動最新表示) (Last Interval (auto refresh))」モードでタブを表示している場合、 60 秒ごとに自動的に最新表示されます。

インターフェースの右上の隅にあるタイマーは、タブが自動的に最新表示されるまでの時間を示しています。

「**ログ・アクティビティー**」または「**ネットワーク・アクティビティー**」タブを「リアルタイム (ストリーミング) (Real Time (streaming))」または「過去 1 分間 (自動最新表示) (Last Minute (auto refresh))」モードで表示する場合、「**一時停止**」アイコンを使用して、現在の表示を一時停止できます。

「**ダッシュボード**」タブで現在の表示を一時停止することもできます。ダッシュボード項目内の任意の場所をクリックすると、そのタブは自動的に一時停止します。タイマーが赤く明滅し、現在の表示が一時停止していることを示しています。

手順

1. QRadar にログインします。
2. 表示するタブをクリックします。
3. 次のオプションのいずれかを選択してください。

オプション	説明
最新表示 (Refresh)	タブの右隅の「**最新表示 (Refresh)**」をクリックすると、タブが最新表示されます。
一時停止	クリックすると、タブ上の表示が一時停止します。
再生 (Play)	タイマーを一時停止した後でクリックすると、タイマーを再開します。

IP アドレスの調査

「ダッシュボード」、「ログ・アクティビティー」、「ネットワーク・アクティビティー」タブ上の IP アドレスに関する情報を調査するには、いくつかの方法を使用できます。

手順

1. QRadar にログインします。
2. 表示するタブをクリックします。
3. IP アドレスの上にマウス・ポインターを移動させると、その IP アドレスのロケーションが表示されます。
4. IP アドレスまたはアセット名を右クリックし、下で説明するオプションのいずれかを選択します。

表 7. IP アドレスの情報

オプション	説明
「ナビゲート」 > 「ネットワーク別に表示 (View by Network)」	選択された IP アドレスに関連付けられたネットワークを表示します。
「ナビゲート」 > 「送信元のサマリーの表示」	選択された送信元 IP アドレスに関連付けられたオフェンスを表示します。
「ナビゲート」 > 「宛先のサマリーの表示」	選択された宛先 IP アドレスに関連付けられたオフェンスを表示します。
「情報」 > 「DNS ルックアップ (DNS Lookup)」	IP アドレスに基づく DNS エントリーを検索します。
「情報」 > 「WHOIS ルックアップ (WHOIS Lookup)」	リモート IP アドレスの登録済みの所有者を検索します。デフォルトの WHOIS サーバーは whois.arin.net です。
「情報」 > 「ポート・スキャン」	選択された IP アドレスのネットワーク・マッパー (NMAP)・スキャンを実行します。このオプションは、ご使用のシステムに NMAP がインストールされている場合のみ使用可能です。NMAP のインストールについて詳しくは、ベンダーの資料を参照してください。
「情報」 > 「アセット・プロファイル」	アセット・プロファイル情報を表示します。 このオプションは、IBM Security QRadar Vulnerability Manager を購入してライセンス交付を受けている場合に表示されます。詳細については、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。 このメニュー・オプションは、 QRadar がプロファイル・データをスキャンによってアクティブに取得した場合、またはフロー・ソースによってパッシブに取得した場合のいずれかで使用可能です。 詳しくは、*IBM Security QRadar SIEM 管理ガイド* を参照してください。
「情報」 > 「イベントの検索」	この IP アドレスに関連付けられているイベントを検索します。
「情報」 > 「フローの検索 (Search Flows)」	この IP アドレスに関連付けられているフローを検索します。

表 7. IP アドレスの情報 (続き)

オプション	説明
「情報」 > 「接続の検索」	この IP アドレスに関連付けられている接続を検索します。このオプションは、IBM Security QRadar Risk Manager を購入し、QRadar と IBM Security QRadar Risk Manager アプライアンスが接続されている場合にのみ表示されます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。
「情報」 > 「スイッチ・ポート・ルックアップ (Switch Port Lookup」	この IP アドレスに対する Cisco IOS デバイス上のスイッチ・ポートを判別します。このオプションは、**「リスク (Risks)」**タブ上の**「デバイスのディスカバー (Discover Devices)」**オプションを使用してディスカバーされるスイッチにのみ適用されます。 **注:** このメニュー・オプションは、QRadar Log Manager で使用できません。
「情報」 > 「トポロジーの表示」	**「リスク (Risks)」**タブを表示します。このタブには、ご使用のネットワークのレイヤー 3 のトポロジーが描画されます。このオプションは、IBM Security QRadar Risk Manager を購入し、QRadar と IBM Security QRadar Risk Manager アプライアンスが接続されている場合に使用することができます。
脆弱点スキャンの実行	**「脆弱点スキャンの実行」**オプションを選択して、IBM Security QRadar Vulnerability Manager スキャンをこの IP アドレスに対して実行します。このオプションは、IBM Security QRadar Vulnerability Manager を購入してライセンス交付を受けている場合のみ、表示することができます。詳細については、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

ユーザー名の調査

ユーザー名を右クリックすると、追加のメニュー・オプションにアクセスすることができます。これらのオプションを使用して、ユーザー名または IP アドレスに関する詳しい情報を表示します。

IBM Security QRadar Vulnerability Manager を購入してライセンス交付を受けている場合、ユーザー名を調査することができます。詳細については、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

ユーザー名を右クリックすると、以下のメニュー・オプションを選択することができます。

表 8. ユーザー名を調査するためのメニュー・オプション

オプション	説明
アセットの表示	選択されたユーザー名に関連する現在のアセットを表示します。アセットの表示については、アセットの管理を参照してください。
ユーザー履歴の表示	直近の 24 時間について、選択されたユーザー名に関連するすべてのアセットを表示します。
イベントの表示	選択されたユーザー名に関連するイベントを表示します。「イベントのリスト」ウィンドウについて詳しくは、ログ・アクティビティーのモニターを参照してください。

右クリック・メニューのカスタマイズについて詳しくは、製品の「*Administration Guide*」を参照してください。

システム時刻

QRadar のユーザー・インターフェースの右隅には、システム時刻が表示されます。このシステム時刻は、コンソール上の時刻です。

コンソールの時刻によって、QRadar デプロイメント内の各 QRadar システムの時刻が同期されます。正確な時刻同期の相関のために、コンソールの時刻を使用して、イベントが他のデバイスからいつ受信されたかが判別されます。

分散デプロイメントでは、コンソールのタイム・ゾーンがご使用のデスクトップ・コンピューターのタイム・ゾーンとは異なっている場合があります。

「**ログ・アクティビティー**」タブと「**ネットワーク・アクティビティー**」タブで時間ベースのフィルターと検索を適用していた場合、時刻範囲を指定するには、コンソールのシステム時刻を使用する必要があります。

「**ログ・アクティビティー**」タブで時間ベースのフィルターと検索を適用していた場合、時刻範囲を指定するには、コンソールのシステム時刻を使用する必要があります。

ユーザー設定の更新

ロケールなどのユーザー設定を、メインの IBM Security QRadar SIEM ユーザー・インターフェースで設定できます。

手順

1. ユーザー情報にアクセスするには、「**設定**」をクリックします。
2. 設定を更新します。

オプション	説明
ユーザー名	ユーザー名を表示します。このフィールドを編集することはできません。

オプション	説明
パスワード	QRadar のユーザー・パスワードは、ソルト付き SHA 256 ストリングとして保管されます。 パスワードは以下の基準を満たしている必要があります。 • 最小 6 文字 • 最大 255 文字 • 特殊文字が 1 つ以上含まれている • 大文字が 1 つ含まれている
パスワード (確認) (Password (Confirm))	パスワードの確認
E メール・アドレス (Email Address)	E メール・アドレスは以下の要件を満たしている必要があります。 • 最小 10 文字 • 最大 255 文字
ロケール	QRadar は、英語、中国語 (簡体字)、中国語 (繁体字)、日本語、韓国語、フランス語、ドイツ語、イタリア語、スペイン語、ロシア語、およびポルトガル語 (ブラジル) で利用可能です。 別の言語を選択すると、ユーザー・インターフェースは英語で表示されます。関連付けられているその他の国/地域別情報 (文字タイプ、照合、日時の形式、通貨単位など) は使用されます。
ポップアップ通知を有効にする (Enable Popup Notifications)	ユーザー・インターフェースに表示されるポップアップ・システム通知を有効にする場合は、このチェック・ボックスを選択します。

関連概念:

181 ページの『クイック・フィルターの検索オプション』
イベントおよびフローのペイロードを検索するには、単純な語句を使用してテキスト検索ストリングを入力します。

オンライン・ヘルプへのアクセス

QRadar オンライン・ヘルプには、QRadar のメイン・ユーザー・インターフェースからアクセスすることができます。

オンライン・ヘルプにアクセスするには、「**ヘルプ**」 > 「**ヘルプの目次 (Help Contents)**」をクリックします。

列のサイズ変更

QRadar のいくつかのタブで列をサイズ変更することができます。

列を区切る線にマウス・ポインターを合わせて、その列の端を新しい位置にドラッグしてください。列を区切る線をダブルクリックして、列をサイズ変更することもできます。このようにすると、その列が、最大フィールドの幅に自動的にサイズ変更されます。

注: Microsoft Internet Explorer バージョン 7.0 Web ブラウザーで、ストリーム・モードでタブにレコードが表示されている場合は、列のサイズ変更は使用できません。

ページ・サイズ

管理特権を持つユーザーは、QRadar の各種タブの表に表示される結果の最大数を構成することができます。

第 3 章 ダッシュボードの管理

「**ダッシュボード**」タブは、ログインしたときに表示されるデフォルト・ビューです。

このタブには、複数のダッシュボードをサポートするワークスペース環境が用意されています。このワークスペース環境で、収集されたネットワーク・セキュリティー、アクティビティー、データのビューを表示することができます。

ダッシュボードを使用すると、ダッシュボード項目を機能的なビューに編成することができます。このビューにより、ネットワークの特定の領域に焦点を当てることができます。

「ダッシュボード」タブを使用すると、セキュリティー・イベントの動作をモニターすることができます。

ダッシュボードはカスタマイズすることができます。「**ダッシュボード**」タブに表示される内容は、ユーザー固有の内容です。セッション内で行われた変更は、ユーザーのシステムにのみ影響します。

デフォルトのダッシュボード

デフォルトのダッシュボードを使用して、各項目をカスタマイズして機能のビューに組み込みます。これらの機能のビューでは、ネットワークの特定の領域に焦点を当てます。

「**ダッシュボード**」タブには、セキュリティー、ネットワーク・アクティビティー、アプリケーション・アクティビティー、システム・モニター、およびコンプライアンスに焦点を当てた、5 つのデフォルトのダッシュボードが備わっています。

各ダッシュボードには、デフォルトのダッシュボード項目一式が表示されます。これらのダッシュボード項目は、より詳細なデータにナビゲートするための開始点として機能します。次の表には、デフォルトのダッシュボードが定義されています。

カスタム・ダッシュボード

ダッシュボードはカスタマイズすることができます。「**ダッシュボード**」タブに表示される内容は、ユーザー固有の内容です。 QRadar セッション内で行われた変更は、ユーザーのシステムにのみ影響します。

「**ダッシュボード**」タブをカスタマイズするには、以下の操作を実行します。

- 業務に関連するカスタム・ダッシュボードを作成します。ユーザー当たりのダッシュボードの最大数は 255 ですが、作成するダッシュボードの数が 10 を超えると、パフォーマンスの問題が発生する可能性があります。
- デフォルトまたはカスタムのダッシュボードで、ダッシュボード項目の追加と削除を行います。

- 要件に合わせて、項目の移動と配置を行います。項目を配置すると、ダッシュボードに比例して、各項目のサイズが自動的に変更されます。
- すべてのデータに基づくカスタム・ダッシュボード項目を追加します。

例えば、時系列のグラフや上位 10 件のネットワーク・アクティビティーを表す棒グラフを指定するダッシュボード項目を追加することができます。

カスタム項目を作成するには、「**ネットワーク・アクティビティー**」タブまたは「**ログ・アクティビティー**」タブで保存済み検索を作成し、その結果をダッシュボードでどのように表示するかを選択します。各ダッシュボード・グラフには、リアルタイムの最新データが表示されます。ダッシュボード上の時系列グラフは、5 分ごとに最新表示されます。

ダッシュボードのカスタマイズ

デフォルト・ダッシュボードまたはカスタム・ダッシュボードにいくつかのダッシュボード項目を追加することができます。

ダッシュボードをカスタマイズして、ネットワーク・セキュリティー要件を満たすダッシュボード項目の表示と編成を行うことができます。

5 つのデフォルト・ダッシュボードが用意されています。これらのダッシュボードには、「**ダッシュボード**」タブの「**ダッシュボードの表示**」リスト・ボックスからアクセスすることができます。ダッシュボードを表示している状態で「**ダッシュボード**」タブに戻った場合、最後に表示していたダッシュボードが表示されます。

フロー検索

「**ネットワーク・アクティビティー**」タブで、保存済み検索条件に基づくカスタムのダッシュボード項目を表示することができます。

フロー検索項目は、「**項目の追加**」 > 「**ネットワーク・アクティビティー**」 > 「**フロー検索**」メニューにリストされます。フロー検索項目の名前は、その項目の基礎になっている保存済み検索条件の名前に一致します。

デフォルトの保存済み検索条件を使用することができます。これは、「**ダッシュボード**」タブ・メニューにフロー検索項目を表示するために事前構成された検索条件です。「**ダッシュボード**」タブ・メニューに、さらにフロー検索ダッシュボード項目を追加することができます。詳しくは、「項目の追加」リストへの検索ベースダッシュボード項目の追加を参照してください。

フロー検索ダッシュボード項目には、検索結果としてリアルタイムの最新データがグラフで表示されます。サポート対象のグラフ・タイプは、時系列グラフ、表、円グラフ、および棒グラフです。デフォルトのグラフ・タイプは棒グラフです。これらのグラフは構成することができます。グラフの構成について詳しくは、グラフの構成を参照してください。

時系列グラフは対話式です。時系列グラフを使用してタイムラインの拡大とスキャンを行うことにより、ネットワーク・アクティビティーを調査することができます。

オフェンス

オフェンスに関連したいくつかの項目をダッシュボードに追加できます。

注: 非表示のオフェンスまたはクローズされたオフェンスは、「**ダッシュボード**」タブに表示される値には含まれません。非表示のイベントまたはクローズされたイベントについて詳しくは、オフェンスの管理を参照してください。

次の表で、オフェンス項目について説明します。

表 9. オフェンス項目

ダッシュボード項目	説明
最新のオフェンス	最新の 5 つのオフェンスが識別され、マグニチュードを示すバーでそのオフェンスの重要性が示されます。オフェンスの名前にマウス・ポインターを合わせると、該当の IP アドレスに関する詳しい情報が表示されます。
最も重大なオフェンス	最も重大な 5 つのオフェンスが識別され、マグニチュードを示すバーでそのオフェンスの重要性が示されます。オフェンスの名前にマウス・ポインターを合わせると、該当の IP アドレスに関する詳しい情報が表示されます。
自分のオフェンス	「**自分のオフェンス**」項目には、自分に割り当てられた最新の 5 件のオフェンスが表示されます。オフェンスが識別され、マグニチュードを示すバーでそのオフェンスの重要性が示されます。IP アドレスにマウス・ポインターを合わせると、該当の IP アドレスに関する詳しい情報が表示されます。
上位の送信元	「**上位の送信元**」項目には、上位のオフェンスの送信元が表示されます。各送信元が識別され、マグニチュードを示すバーでその送信元の重要性が示されます。IP アドレスにマウス・ポインターを合わせると、該当の IP アドレスに関する詳しい情報が表示されます。
上位のローカル宛先	「**上位のローカル宛先**」項目には、上位のローカル宛先が表示されます。各宛先が識別され、マグニチュードを示すバーでその宛先の重要性が示されます。IP アドレスにマウス・ポインターを合わせると、該当の IP アドレスに関する詳しい情報が表示されます。
カテゴリー	「**上位のカテゴリー・タイプ**」項目には、最多数のオフェンスに関連した上位 5 件のカテゴリーが表示されます。

ログ・アクティビティー

「**ログ・アクティビティー**」ダッシュボード項目を使用すると、イベントのモニターと調査をリアルタイムで行うことができます。

注: 非表示のイベントやクローズされたイベントは、「**ダッシュボード**」タブに表示される値には含まれません。

表 10. ログ・アクティビティー項目

ダッシュボード項目	説明
イベント検索	「ログ・アクティビティー」タブで、保存済み検索条件に基づくカスタムのダッシュボード項目を表示することができます。イベント検索項目は、「**項目の追加**」 > 「**ネットワーク・アクティビティー**」 > 「**イベント検索**」メニューにリストされます。イベント検索項目の名前は、その項目の基礎になっている保存済み検索条件の名前に一致します。 QRadar には、デフォルトの保存済み検索条件が組み込まれています。これは、「**ダッシュボード**」タブ・メニューにイベント検索項目を表示するために事前構成された検索条件です。「**ダッシュボード**」タブ・メニューに、さらにイベント検索ダッシュボード項目を追加することができます。詳しくは、『「項目の追加」リストへの検索ベースダッシュボード項目の追加』を参照してください。 「**ログ・アクティビティー**」ダッシュボード項目では、検索結果としてリアルタイムの最新データがグラフで表示されます。サポート対象のグラフ・タイプは、時系列グラフ、表、円グラフ、および棒グラフです。デフォルトのグラフ・タイプは棒グラフです。これらのグラフは構成することができます。 時系列グラフは対話式です。タイムラインの拡大とスキャンを行うことにより、ログ・アクティビティーを調査することができます。
重大度別のイベント (Events By Severity)	「**重大度別のイベント (Events By Severity)**」ダッシュボード項目には、重大度別にグループ化されたアクティブ・イベントの数が表示されます。この項目を使用して、受信したイベントの数を、割り当てられた重大度レベル別に確認することができます。重大度は、オフェンスの送信元による脅威の大きさを、宛先における攻撃に対する準備の程度と対比して示します。重大度の範囲は 0 (低) から 10 (高) までです。サポート対象のグラフ・タイプは、表、円グラフ、棒グラフです。

表 10. ログ・アクティビティー項目 (続き)

ダッシュボード項目	説明
上位のログ・ソース	「**上位のログ・ソース**」ダッシュボード項目には、直近の 5 分間にイベントを QRadar に送信した上位 5 個のログ・ソースが表示されます。 指定されたログ・ソースから送信されたイベントの数が円グラフで表示されます。この項目を使用すると、潜在的な動作の変化を確認することができます。例えば、通常は上位 10 件のリストには含まれないファイアウォール・ログ・ソースが全体のメッセージ数のうちの大きな比率を占めるようになった場合は、その原因を調査する必要があります。サポート対象のグラフ・タイプは、表、円グラフ、棒グラフです。

最新レポート

「**最新レポート**」ダッシュボード項目を使用して、最近生成された上位レポートを表示します。

レポートのタイトル、生成日時、フォーマットが表示されます。

システム・サマリー

「**システム・サマリー**」ダッシュボード項目には、過去 24 時間のアクティビティー全体のサマリーが表示されます。

サマリー項目内では、次の情報を確認することができます。

- **現在のフロー数/秒 (Current Flows Per Second)** - 1 秒当たりのフロー・レートを表示します。
- **フロー (過去 24 時間) (Flows (Past 24 Hours))** - 過去 24 時間に確認されたアクティブ・フローの総数を表示します。
- **現在のイベント数/秒** - 1 秒当たりのイベント・レートを表示します。
- **新規イベント数 (過去 24 時間)** - 過去 24 時間に受信された新規イベントの総数を表示します。
- **更新されたオフェンス数 (過去 24 時間)** - 過去 24 時間に作成、または新しい証拠で変更されたオフェンスの総数を表示します。
- **データ削減率** - 過去 24 時間に検出されたイベントの合計、および過去 24 時間に変更されたオフェンスの数に基づく削減されたデータの比率を表示します。

「リスクのモニター」ダッシュボード

アセット、ポリシー、およびポリシー・グループのポリシー・リスクおよびポリシー・リスクの変化をモニターするには、「**リスクのモニター**」ダッシュボードを使用します。

デフォルトでは、「**リスクのモニター**」ダッシュボードに「**リスク**」および「**リスクの変化**」という項目が表示されます。これらの項目により、脆弱性が高、中、低の各ポリシー・グループに属するアセットのポリシー・リスク・スコアのほか、CISポリシー・グループのポリシー・リスク・スコアのコンプライアンス合格率および変化の履歴をモニターします。

IBM Security QRadar Risk Manager のライセンス交付を受けない限り、「リスクのモニター」ダッシュボードの項目に結果は表示されません。詳しくは「QRadar Risk Manager ユーザーズ・ガイド」を参照してください。

デフォルトの「**リスクのモニター**」ダッシュボードを表示するには、「**ダッシュボード**」タブで「**ダッシュボードの表示**」 > 「**リスクのモニター**」を選択します。

関連タスク:

『ポリシー・コンプライアンスのモニター』
選択したアセット、ポリシー、およびポリシー・グループのポリシー・コンプライアンス合格率およびポリシー・リスク・スコアを表示するためのダッシュボード項目を作成します。

28 ページの『リスクの変化のモニター』
選択したアセット、ポリシー、およびポリシー・グループのポリシー・リスクの変化を日単位、週単位、および月単位で表示するダッシュボード項目を作成します。

ポリシー・コンプライアンスのモニター

選択したアセット、ポリシー、およびポリシー・グループのポリシー・コンプライアンス合格率およびポリシー・リスク・スコアを表示するためのダッシュボード項目を作成します。

手順

1. 「**ダッシュボード**」タブをクリックします。
2. ツールバーで「**新規ダッシュボード**」をクリックします。
3. ポリシー・コンプライアンス・ダッシュボードの名前および説明を入力します。
4. 「**OK**」をクリックします。
5. ツールバーで「**項目の追加**」 > 「**リスク・マネージャー (Risk Manager)**」 > 「**リスク**」を選択します。

   「**リスク・マネージャー (Risk Manager)**」ダッシュボード項目は、IBM Security QRadar Risk Manager のライセンス交付を受けている場合にのみ表示されます。
6. 新しいダッシュボード項目のヘッダーで、黄色の「**設定**」アイコンをクリックします。
7. 「**グラフ・タイプ**」、「**表示: 上位**」および「**ソート**」の各リストを使用してグラフを構成します。
8. 「**グループ**」リストから、モニターするグループを選択します。詳しくは、ステップ 9 の表を参照してください。

   「**アセット**」オプションを選択すると、「**リスク**」 > 「**ポリシー管理 (Policy Management)**」 > 「**アセット別**」ページへのリンクが、「**リスク**」ダッシュボ

ード項目の下部に表示されます。「**アセット別**」ページには、選択した「**ポリシー・グループ**」に対して返されたすべての結果についての詳細情報が表示されます。 特定のアセットに関する詳細情報が必要な場合、「**グラフ・タイプ**」リストから「**表**」を選択し、「**アセット**」列でリンクをクリックして、「**アセット別**」ページでアセットに関する詳細を表示します。

「**ポリシー**」オプションを選択すると、「**リスク**」 > 「**ポリシー管理 (Policy Management)**」 > 「**ポリシー別 (By Policy)**」ページへのリンクが、「**リスク**」ダッシュボード項目の下部に表示されます。「**ポリシー別 (By Policy)**」ページには、選択した「**ポリシー・グループ**」に対して返されたすべての結果についての詳細情報が表示されます。 特定ポリシーに関する詳細情報が必要な場合、「**グラフ・タイプ**」リストから「**表**」を選択し、「**ポリシー**」列でリンクをクリックして、「**ポリシー別 (By Policy)**」ページでポリシーに関する詳細を表示します。

9. 「**グラフ**」リストから、使用するグラフ・タイプを選択します。詳しくは、以下の表を参照してください。

グループ	アセット合格率	ポリシー・チェック合格率 (Policy Checks Passed Percentage)	ポリシー・グループ合格率	ポリシーのリスク・スコア
すべて	アセット、ポリシー、およびポリシー・グループにわたる平均アセット合格率 (パーセント) を返します。	アセット、ポリシー、およびポリシー・グループにわたる平均ポリシー・チェック合格率 (パーセント) を返します。	すべてのアセット、ポリシー、およびポリシー・グループにわたる平均ポリシー・グループ合格率を返します。	すべてのアセット、ポリシー、およびポリシー・グループにわたる平均ポリシー・リスク・スコアを返します。
アセット	アセットがアセット・コンプライアンスに合格しているかどうか (100%=合格、0%=不合格) を返します。 ポリシー・グループに関連付けられたアセットのうち、コンプライアンスに合格したセットを表示するには、この設定を使用します。	アセットが合格したポリシー・チェックの割合を返します。 ポリシー・グループに関連付けられた各アセットについて、合格したポリシー・チェックの割合を表示するには、この設定を使用します。	コンプライアンスに合格したアセットに関連付けられたポリシー・サブグループの割合を返します。	各アセットに関連付けられたポリシーの質問に対するすべての重要度因子の値の合計を返します。 選択したポリシー・グループに関連付けられた各アセットのポリシー・リスクを表示するには、この設定を使用します。

グループ	アセット合格率	ポリシー・チェック合格率 (Policy Checks Passed Percentage)	ポリシー・グループ合格率	ポリシーのリスク・スコア
ポリシー	ポリシー・グループに属する各ポリシーに関連付けられたすべてのアセットがコンプライアンスに合格しているかどうかを返します。 ポリシー・グループに属する各ポリシーに関連付けられたすべてのアセットが合格したかどうかをモニターするには、この設定を使用します。	ポリシー・グループに属するポリシーごとの、合格したポリシー・チェックの割合を返します。 不合格になったポリシー・チェックの数をポリシーごとにモニターするには、この設定を使用します。	コンプライアンスに合格したポリシーが属するポリシー・サブグループの割合を返します。	ポリシー・グループに属するポリシーの質問ごとの重要度因子の値を返します。 ポリシー・グループに属する各ポリシーの重要度因子を表示するには、この設定を使用します。
ポリシー・グループ	選択したポリシー・グループ全体のうち、コンプライアンスに合格したアセットの割合を返します。	ポリシー・グループ全体のうち、ポリシーごとの合格したポリシー・チェックの割合を返します。	コンプライアンスに合格したポリシー・グループ内のポリシー・サブグループの割合を返します。	ポリシー・グループに属するすべてのポリシーの質問のすべての重要度因子の値の合計を返します。

10. 「**ポリシー・グループ**」リストから、モニターするポリシー・グループを選択します。
11. 「**保存**」をクリックします。

リスクの変化のモニター

選択したアセット、ポリシー、およびポリシー・グループのポリシー・リスクの変化を日単位、週単位、および月単位で表示するダッシュボード項目を作成します。

このタスクについて

ポリシー・グループのポリシー・リスク・スコア、ポリシー・チェック、およびポリシー値の変化を経時的に比較するには、このダッシュボード項目を使用します。

「**リスクの変化**」ダッシュボード項目は、矢印を使用して、選択した期間における選択した値のポリシー・リスクの変化が増加、減少、横ばいのいずれであったかを示します。

- 赤い矢印の下の数値は、リスクが増加した値を示します。
- グレーの矢印の下の数値は、リスクに変化がない値を示します。
- 緑の矢印の下の数値は、リスクが減少した値を示します。

手順

1. 「**ダッシュボード**」タブをクリックします。
2. ツールバーで「**新規ダッシュボード**」をクリックします。
3. 「ヒストリカル・ポリシー・コンプライアンス」ダッシュボードの名前および説明を入力します。
4. 「**OK**」をクリックします。
5. ツールバーで「**項目の追加**」 > 「**リスク・マネージャー (Risk Manager)**」 > 「**リスクの変化**」を選択します。

   「**リスク・マネージャー (Risk Manager)**」ダッシュボード項目は、IBM Security QRadar Risk Manager のライセンス交付を受けている場合にのみ表示されます。
6. 新しいダッシュボード項目のヘッダーで、黄色の「**設定**」アイコンをクリックします。
7. 「**ポリシー・グループ**」リストから、モニターするポリシー・グループを選択します。
8. 「**比較する値**」リストからオプションを選択します。
   - 選択したポリシー・グループ内のすべてのポリシーの質問を対象として重要度因子の累積的な変化を表示する場合は、「**ポリシーのリスク・スコア**」を選択します。
   - 選択したポリシー・グループ内の変化したポリシー・チェックの数を表示する場合は、「**ポリシー・チェック (Policies Checks)**」を選択します。
   - 選択したポリシー・グループ内の変化したポリシーの数を表示する場合は、「**ポリシー**」を選択します。
9. 以下のように、モニターするリスク変化の期間を「**差分期間**」リストから選択します。
   - 今日深夜 0 時からのリスクの変化を昨日のリスクの変化と比較する場合は、「**日**」を選択します。
   - 今週月曜日深夜 0 時からのリスクの変化を先週のリスクの変化と比較する場合は、「**週**」を選択します。
   - 今月 1 日深夜 0 時からのリスクの変化を先月のリスクの変化と比較する場合は、「**月**」を選択します。
10. 「**保存**」をクリックします。

「脆弱性管理 (Vulnerability Management)」の項目

「脆弱性管理 (Vulnerability Management)」ダッシュボード項目は、IBM Security QRadar Vulnerability Manager を購入してそのライセンス交付を受けている場合にのみ表示されます。

詳細については、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

「**脆弱性**」タブで、保存済み検索条件に基づくカスタムのダッシュボード項目を表示することができます。各検索項目は、「**項目の追加**」 > 「**脆弱性管理**

(Vulnerability Management)」 > 「**脆弱性検索 (Vulnerability Searches)**」メニュー内にリストされます。検索項目の名前は、その項目が基づく保存済み検索条件の名前に一致します。

QRadar には、デフォルトの保存済み検索条件が組み込まれています。これは、「**ダッシュボード**」タブ・メニューに検索項目を表示するために事前構成された検索条件です。検索ダッシュボード項目は、さらに「**ダッシュボード**」タブ・メニューに追加することができます。

サポート対象のグラフ・タイプは、表、円グラフ、棒グラフです。デフォルトのグラフ・タイプは棒グラフです。これらのグラフは構成することができます。

システム通知

「システム通知 (Systems Notification)」ダッシュボード項目には、システムで受信されたイベント通知が表示されます。

「**システム通知**」ダッシュボード項目内に表示する通知の場合、管理者は各通知メッセージ・タイプに基づいたルールを作成し、「カスタム・ルール・ウィザード」内の「**通知**」チェック・ボックスを選択する必要があります。

イベント通知の構成およびイベント・ルールの作成方法について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

「**システム通知**」ダッシュボード項目では、次の情報を表示することができます。

- **フラグ (Flag)** - 通知の重大度レベルを示す記号を表示します。重大度レベルに関する詳細を表示するには、記号を指示します。
  - 「**正常性**」アイコン
  - 「**情報**」アイコン (?)
  - 「**エラー**」アイコン (X)
  - 「**警告**」アイコン (!)
- 「**作成日**」 - 通知が作成されてから経過した時間を表示します。
- 「**説明**」 - 通知に関する情報を表示します。
- 「**閉じる (Dismiss)**」**アイコン (x)** - システム通知を閉じることができます。

通知の上をマウス・ポインターで指示すると、次の詳細を確認できます。

- 「**ホスト IP**」 - 通知を発信したホストの IP アドレスを表示します。
- 「**重大度**」 - この通知を生成した発生事象の重大度レベルを表示します。
- 「**下位カテゴリー**」 - この通知を生成した発生事象に関連付けられている下位カテゴリーを表示します。例えば、「サービスの中断 (Service Disruption)」です。
- 「**ペイロード (Payload)**」 - この通知を生成した発生事象に関連付けられているペイロードの内容を表示します。
- 「**作成日**」 - 通知が作成されてから経過した時間を表示します。

「**システム通知**」ダッシュボード項目を追加した場合、システム通知は QRadar ユーザー・インターフェース内にポップアップ通知として表示することもできます。これらのポップアップ通知は、選択しているタブに関係なく、ユーザー・インターフェースの右下隅に表示されます。

ポップアップ通知は、管理権限を持つユーザーのみが使用でき、デフォルトでは有効になっています。ポップアップ通知を無効にするには、「**ユーザー設定 (User Preferences)**」を選択し、「**ポップアップ通知を有効にする (Enable Pop-up Notifications)**」チェック・ボックスをクリアします。

「システム通知」ポップアップ・ウィンドウでは、キュー内の通知の数が強調表示されます。例えば、(1 - 12) がヘッダー内に表示されている場合、現在の通知は、12 件のうちの 1 件目の通知が表示されています。

「システム通知」ポップアップ・ウィンドウには、次のオプションがあります。

- 「**次へ」アイコン (>)** - 次の通知メッセージを表示します。例えば、現在の通知メッセージが 6 件のうちの 3 件目の場合、このアイコンをクリックして 6 件のうちの 4 件目を表示します。
- 「**閉じる」アイコン (X)** - この通知ポップアップ・ウィンドウを閉じます。
- 「**(詳細 (details))**」 - このシステム通知に関する詳細情報を表示します。

インターネット脅威インフォメーション・センター

インターネット脅威インフォメーション・センター・ダッシュボード項目は、セキュリティーに関する問題、日次脅威影響評価、セキュリティー・ニュース、脅威リポジトリーに関する最新の注意情報を提供する組み込み RSS フィードです。

「現在の脅威レベル」ダイアグラムは、現在の脅威レベルを示し、IBM Internet Security Systems Web サイトの『Current Internet Threat Level』ページへのリンクを提供します。

現在の注意情報は、ダッシュボード項目にリスト表示されます。注意情報のサマリーを表示するには、その情報の隣にある**矢印**アイコンをクリックします。この操作により、注意情報が展開されて、サマリーが表示されます。**矢印**アイコンをもう一度クリックすると、サマリーが非表示になります。

注意情報の詳細をすべて確認するには、関連するリンクをクリックします。別のブラウザー・ウィンドウで IBM Internet Security Systems Web サイトが開き、その注意情報の詳細がすべて表示されます。

カスタム・ダッシュボードの作成

カスタム・ダッシュボードを作成して、特定の要件を満たすダッシュボード項目のグループを表示することができます。

このタスクについて

カスタム・ダッシュボードを作成すると、新規ダッシュボードが「**ダッシュボード**」タブ内に表示され、また「**ダッシュボードの表示**」リスト・ボックス内にリストされます。新規のカスタム・ダッシュボードはデフォルトでは空です。したがって、このダッシュボードに項目を追加する必要があります。

手順

1. 「**ダッシュボード**」タブをクリックします。
2. 「**新規ダッシュボード (New Dashboard)**」アイコンをクリックします。

3. 「**名前**」フィールドに、ダッシュボードの固有の名前を入力します。最大長は 65 文字です。
4. 「**説明**」フィールドに、ダッシュボードの説明を入力します。最大長は 255 文字です。この説明は、「**ダッシュボードの表示**」リスト・ボックス内のダッシュボード名のツールチップに表示されます。
5. 「**OK**」をクリックします。

ダッシュボードを使用したログまたはネットワーク・アクティビティーの調査

検索ベースのダッシュボード項目には、「**ログ・アクティビティー**」や「**ネットワーク・アクティビティー**」タブへのリンクがあり、ログやネットワーク・アクティビティーをさらに詳しく調査することができます。

このタスクについて

「**ログ・アクティビティー**」ダッシュボード項目からフローを調査するには、以下を実行します。

1. 「**ログ・アクティビティーで表示 (View in Log Activity)**」リンクをクリックします。「**ログ・アクティビティー**」タブが表示され、ダッシュボード項目のパラメーターに一致する結果と 2 つのグラフが示されます。

「**ネットワーク・アクティビティー**」ダッシュボード項目からフローを調査するには、以下を実行します。

1. 「**ネットワーク・アクティビティーで表示 (View in Network Activity)**」リンクをクリックします。「ネットワーク・アクティビティー」タブが表示され、ダッシュボード項目のパラメーターに一致する結果と 2 つのグラフが示されます。

「**ネットワーク・アクティビティー**」タブが表示され、ダッシュボード項目のパラメーターに一致する結果と 2 つのグラフが示されます。「**ログ・アクティビティー**」と「**ネットワーク・アクティビティー**」タブに表示されるグラフのタイプは、ダッシュボード項目に構成されているグラフによって異なります。

グラフ・タイプ	説明
棒グラフ、円グラフ、表 (Bar, Pie, and Table)	「**ログ・アクティビティー**」タブまたは「**ネットワーク・アクティビティー**」タブに、棒グラフ、円グラフ、およびフローの詳細を示す表が表示されます。

グラフ・タイプ	説明
時系列 (Time Series)	「**ログ・アクティビティー**」または「**ネットワーク・アクティビティー**」タブに、以下の基準に従ってグラフが表示されます。 1. 時刻範囲が 1 時間以下の場合、時系列グラフ、棒グラフ、およびイベントまたはフローの詳細を示す表が表示されます。 2. 時刻範囲が 1 時間を超える場合、時系列グラフが表示され、「詳細の更新」をクリックするよう求めるプロンプトが出されます。これを行うと検索が開始され、イベントまたはフローの詳細が取り込まれて棒グラフが生成されます。検索が完了すると、棒グラフと、イベントまたはフローの詳細を示す表が表示されます。

グラフの構成

該当する場合、「**ログ・アクティビティー**」、「**ネットワーク・アクティビティー**」、および「**接続**」のダッシュボード項目を構成して、グラフ・タイプおよび表示するデータ・オブジェクトの数を指定することができます。

このタスクについて

表 11. グラフの構成： パラメーターのオプション。

オプション	説明
グラフで表す値 (Value to Graph)	リスト・ボックスから、グラフで表すオブジェクト・タイプを選択します。このオプションには、ご使用の検索パラメーターに含まれた、正規化されたカスタム・イベントまたはカスタム・フローのパラメーターがすべて含まれています。

表 11. グラフの構成 (続き): パラメーターのオプション。

オプション	説明
グラフ・タイプ	リスト・ボックスから、表示するグラフ・タイプを選択します。オプションは、以下のとおりです。 1. **棒グラフ (Bar Chart)** - データを棒グラフで表示します。このオプションを使用できるのは、グループ化されたイベントまたはフローの場合のみです。 2. **円グラフ (Pie Chart)** - データを円グラフで表示します。このオプションを使用できるのは、グループ化されたイベントまたはフローの場合のみです。 3. **表** - データを表形式で表示します。このオプションを使用できるのは、グループ化されたイベントまたはフローの場合のみです。 4. **時系列 (Time Series)** - 指定された時間間隔ごとの一致したレコードを表す、インタラクティブな折れ線グラフを表示します。
表示する上位件数 (Display Top)	リスト・ボックスから、グラフ内に表示するオブジェクトの数を選択します。オプションには、**5** と **10** が含まれています。デフォルトは **10** です。
時系列データのキャプチャー	このチェック・ボックスは、時系列のキャプチャーを有効にする場合に選択します。このチェック・ボックスを選択すると、グラフ機能で時系列グラフ・データの累積が開始されます。デフォルトでは、このオプションは無効になっています。
時刻範囲	リスト・ボックスから、表示する時刻範囲を選択します。

カスタムのグラフ構成は保存されるため、「**ダッシュボード**」タブにアクセスするたびに、これらのグラフが構成されたとおりに表示されます。

時系列の保存済み検索を実行する際に、前の期間のデータの表示に使用できるイベント・データまたはフロー・データのキャッシュが存在しているように、データは累積されます。累積されるパラメーターは、「**グラフで表す値 (Value to Graph)**」リスト・ボックス内でアスタリスク (*) で示されています。グラフで表す値に累積されない (アスタリスクが付いていない) 値を選択した場合、時系列データは利用できません。

手順

1. 「**ダッシュボード**」タブをクリックします。
2. 「**ダッシュボードの表示**」リスト・ボックスから、カスタマイズする項目が含まれたダッシュボードを選択します。

3. 構成するダッシュボード項目のヘッダーで、「**設定 (Settings)**」アイコンをクリックします。
4. グラフのパラメーターを構成します。

ダッシュボード項目の削除

ダッシュボードから項目を削除することができます。削除した項目はいつでも再追加できます。

このタスクについて

ダッシュボードから項目を削除しても、その項目は完全には削除されません。

手順

1. 「**ダッシュボード**」タブをクリックします。
2. 「**ダッシュボードの表示**」リスト・ボックスから、項目を削除するダッシュボードを選択します。
3. ダッシュボード項目の見出しで赤の「x」アイコンをクリックすると、その項目がダッシュボードから削除されます。

ダッシュボード項目の切り離し

ダッシュボードから項目を切り離して、デスクトップ・システム上の新しいウィンドウに表示することができます。

このタスクについて

ダッシュボード項目を切り離すと、元のダッシュボード項目は「**ダッシュボード**」タブにそのまま残され、コピーされたダッシュボード項目を含む切り離されたウィンドウは開いたままとなって、スケジュールされた間隔で最新表示されます。QRadar アプリケーションを閉じると、切り離されたウィンドウがモニター用に開いたままとなり、手動で閉じられるまで、またはコンピューター・システムがシャットダウンするまで、引き続き最新表示されます。

手順

1. 「**ダッシュボード**」タブをクリックします。
2. 「**ダッシュボードの表示**」リスト・ボックスから、項目を切り離すダッシュボードを選択します。
3. ダッシュボード項目の見出しで緑のアイコンをクリックすると、ダッシュボード項目が切り離されて、別のウィンドウに表示されます。

ダッシュボードの名前変更

ダッシュボードの名前を変更し、説明を更新することができます。

手順

1. 「**ダッシュボード**」タブをクリックします。

2. 「**ダッシュボードの表示**」リスト・ボックスから、編集するダッシュボードを選択します。
3. ツールバーで、「**ダッシュボードの名前変更**」アイコンをクリックします。
4. 「**名前**」フィールドに、ダッシュボードの新しい名前を入力します。最大長は 65 文字です。
5. 「**説明**」フィールドに、ダッシュボードの新しい説明を入力します。最大長は 255 文字です。
6. 「**OK**」をクリックします。

ダッシュボードの削除

ダッシュボードを削除することができます。

このタスクについて

ダッシュボードを削除すると、「**ダッシュボード**」タブが最新表示され、「**ダッシュボードの表示**」リスト・ボックスで最初にリストされているダッシュボードが表示されます。削除したダッシュボードは、「**ダッシュボードの表示**」リスト・ボックスに表示されなくなります。

手順

1. 「**ダッシュボード**」タブをクリックします。
2. 「**ダッシュボードの表示**」リスト・ボックスから、削除するダッシュボードを選択します。
3. ツールバーで、「**ダッシュボードの削除**」をクリックします。
4. 「**はい**」をクリックします。

システム通知の管理

「**システム通知**」ダッシュボード項目に表示する通知の数を指定することができます。読み終わったシステム通知は閉じることができます。

始める前に

「**システム通知**」ダッシュボード項目がダッシュボードに追加されていることを確認してください。

手順

1. 「システム通知」ダッシュボード項目のヘッダーで、「**設定 (Settings)**」アイコンをクリックします。
2. 「**表示**」リスト・ボックスから、表示するシステム通知の数を選択します。
   - 選択肢は、**5**、**10** (デフォルト)、**20**、**50**、および「**すべて**」です。
   - 過去 24 時間以内に記録されたすべてのシステム通知を表示するには、「**すべて**」をクリックします。
3. システム通知を閉じるには、「**削除**」アイコンをクリックします。

「項目の追加」リストへの検索ベースダッシュボード項目の追加

検索ベースのダッシュボード項目を「**項目の追加**」メニューに追加することができます。

始める前に

イベント検索とフロー検索のダッシュボード項目を「**ダッシュボード**」タブ上の「**項目の追加**」メニューに追加するには、「**ログ・アクティビティー**」タブまたは「**ネットワーク・アクティビティー**」タブにアクセスして、検索結果を「**ダッシュボード**」タブに表示できることを指定する検索条件を作成する必要があります。また、検索条件で、検索結果がパラメーターに基づいてグループ化されることを指定する必要もあります。

手順

1. 次のいずれかを選択します。
   - フロー検索のダッシュボード項目を追加するには、「**ネットワーク・アクティビティー**」タブをクリックします。
   - イベント検索のダッシュボード項目を追加するには、「**ログ・アクティビティー**」タブをクリックします。
2. 「**検索**」リスト・ボックスから、次のオプションのいずれかを選択します。
   - 検索を作成するには、「**新規検索**」を選択します。
   - 保存済み検索を編集するには、「**検索の編集**」を選択します。
3. 必要に応じて、検索パラメーターを構成または編集します。
   - 「検索の編集」ペインで、「**ダッシュボードに含める**」オプションを選択します。
   - 「列定義」ペインで、任意の列を選択して「**列の追加**」アイコンをクリックし、その列を「**グループ化の基準**」リストに移動します。
4. 「**フィルター (Filter)**」をクリックします。 検索結果が表示されます。
5. 「**条件の保存**」をクリックします。『「オフェンス」タブでの検索条件の保存』を参照してください
6. 「**OK**」をクリックします。
7. 保存済み検索条件によって、イベント検索またはフロー検索のダッシュボード項目が「**項目の追加**」リストに正常に追加されたことを確認します
   a. 「**ダッシュボード**」タブをクリックします。
   b. 次のオプションのいずれかを選択してください。
   a. イベント検索項目を確認するには、「**項目の追加**」 > 「**ログ・アクティビティー**」 > 「**イベント検索**」 > 「**項目の追加**」を選択します。
   b. フロー検索項目を確認するには、「**項目の追加**」 > 「**ネットワーク・アクティビティー**」 > 「**フロー検索**」を選択します。 ダッシュボード項目が、保存済み検索条件と同じ名前でリスト上に表示されます。

第 4 章 オフェンスの管理

複数のネットワークに宛先 IP アドレスが存在する、同じオフェンスのイベントおよびフローを、相互に関連付けることができます。これにより、ネットワーク内の各オフェンスを効率良く調査することができます。

制約事項: IBM Security QRadar Log Manager ではオフェンスを管理できません。IBM Security QRadar SIEM と IBM Security QRadar Log Manager の相違点について詳しくは、5 ページの『Security Intelligence 製品の機能』を参照してください。

「**オフェンス**」タブのさまざまなページをナビゲートすることにより、イベントおよびフローの詳細を調査し、オフェンスの原因となった特定のイベントおよびフローを判別できます。

オフェンスの概要

「**オフェンス**」タブを使用して、ネットワーク内のオフェンス、送信元および宛先 IP アドレス、ネットワーク動作、およびアノマリを調査できます。

さまざまな基準に基づいてオフェンスを検索できます。 オフェンスの検索について詳しくは、183 ページの『オフェンスの検索』を参照してください。

オフェンスに関する権限の考慮事項

すべてのユーザーは、どのログ・ソースまたはフロー・ソースがオフェンスに関連しているかにかかわらず、すべてのオフェンスを表示することができます。

「**オフェンス**」タブは、各ユーザーが表示できるオフェンスを判別するためにデバイス・レベルのユーザー権限を使用しません。判別はネットワーク権限によって行われます。

デバイス・レベル権限の詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

重要な用語

「**オフェンス**」タブを使用して、オフェンス、送信元 IP アドレス、宛先 IP アドレスにアクセスして分析を行うことができます。

項目	説明
オフェンス	1 つのオフェンスには、1 つのソース (ホストやログ・ソースなど) から発生した複数のイベントやフローが含まれます。「**オフェンス**」タブにはオフェンスが表示されます。これらのオフェンスには、共同して特定のオフェンスのマグニチュードを検証するトラフィックと脆弱性が含まれます。オフェンスのマグニチュードは、オフェンスの再評価のたびに実行されるいくつかのテストによって判別されます。再評価は、イベントがオフェンスに追加されたときに実行されます。また、スケジュールされた間隔でも実行されます。
送信元 IP アドレス	送信元 IP アドレスは、ネットワーク上のコンポーネントのセキュリティーを侵害しようとするデバイスを指定します。送信元 IP アドレスでは、さまざまな攻撃手段 (無許可アクセスを試みるためのスキャン行為やサービス妨害 (DoS) 攻撃など) が使用される可能性があります。
宛先 IP アドレス	宛先 IP アドレスは、送信元 IP アドレスがアクセスを試みるネットワーク・デバイスを指定します。

オフェンスの保存

「**管理**」タブで、オフェンス保存期間のシステム設定を構成して、構成された期間の経過後にオフェンスをデータベースから削除することができます。

デフォルトのオフェンス保存期間は 3 日です。「**管理**」タブにアクセスしてシステム設定を構成するには、管理権限が必要です。しきい値を構成するときに、定義したしきい値に 5 日間追加されます。

オフェンスを閉じるする場合、閉じるしたオフェンスは、オフェンス保存期間の経過後にデータベースから削除されます。あるオフェンスに関するイベントがその後さらに発生した場合は、新しいオフェンスが作成されます。クローズされたオフェンスが含まれた検索を実行した場合、そのオフェンスがデータベースからまだ削除されていないときは、その項目が検索結果に表示されます。

オフェンスのモニター

「**オフェンス**」タブで使用可能な各種のビューを使用することにより、オフェンスをモニターして、ネットワークで現在発生しているオフェンスを判別できます。

オフェンスは、マグニチュードが最も大きなものから順にリストされます。特定のオフェンスの詳細を見つけて表示し、必要に応じてそのオフェンスに関してアクションを実行することができます。

各種のビューのナビゲートを開始すると、タブの先頭に、現在のビューまでのナビゲーション・トレールが表示されます。前に表示したページに戻るには、ナビゲーション・トレールにあるページ名をクリックしてください。

「**オフェンス**」タブのナビゲーション・メニューから、以下の表にリストされているページにアクセスできます。

表 12. 「**オフェンス**」*タブからアクセスできるページ*

ページ	説明
自分のオフェンス	自分に割り当てられたすべてのオフェンスを表示します。
すべてのオフェンス	ネットワーク上のすべてのグローバルなオフェンスを表示します。
カテゴリー別 (By Category)	すべてのオフェンスを、高位カテゴリーと下位カテゴリー別にグループ化して表示します。
送信元 IP 別	すべてのオフェンスを、特定のオフェンスに関連する送信元 IP アドレス別にグループ化して表示します。
宛先 IP 別	すべてのオフェンスを、特定のオフェンスに関連する宛先 IP アドレス別にグループ化して表示します。
ネットワーク別	すべてのオフェンスを、特定のオフェンスに関連するネットワーク別にグループ化して表示します。
ルール	「ルール」ページにアクセスできるようにします。このページからカスタム・ルールを表示および作成できます。このオプションは、「カスタム・ルールの表示」ロールの権限を持っている場合にのみ表示されます。詳しくは、ルールの管理を参照してください。

「すべてのオフェンス」ページや「自分のオフェンス」ページのモニター

「すべてのオフェンス」ページや「自分のオフェンス」ページでオフェンスをモニターすることができます。

始める前に

「すべてのオフェンス」ページには、ご使用のネットワークで発生しているすべてのオフェンスのリストが表示されます。「自分のオフェンス」ページには、自分に割り当てられたオフェンスのリストが表示されます。

このタスクについて

表の先頭には、検索結果に適用されるオフェンス検索パラメーター (ある場合) の詳細が表示されます。これらの検索パラメーターをクリアするには、「**フィルターのクリア**」をクリックできます。オフェンスの検索について詳しくは、 オフェンスの検索を参照してください。

注: さらに詳細なサマリー・ページのペインを表示するには、関連するツールバー・オプションをクリックします。例えば、送信元 IP アドレスの詳細を表示するには、「**送信元**」をクリックします。ツールバー・オプションについて詳しくは、「オフェンス」タブ・ツールバーの機能 を参照してください。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**すべてのオフェンス**」または「**自分のオフェンス**」を選択します。
3. 以下のオプションを使用して、オフェンスのリストを詳細化することができます。
   - 「**次のオフェンスを表示します**」リスト・ボックスから、特定の時間フレームでオフェンスのリストをフィルタリングするオプションを選択します。
   - 「**現在の検索パラメーター**」ペインに表示されている各フィルターの横にある、「**フィルターのクリア**」リンクをクリックします。
4. 表示するオフェンスをダブルクリックします。
5. 「オフェンスのサマリー」ページで、オフェンスの詳細を確認します。オフェンスのパラメーターを参照してください。
6. オフェンスに対して必要なアクションがあれば実行します。

カテゴリーでグループ化されたオフェンスのモニター

「カテゴリー別の詳細 (By Category Details)」ページで、オフェンスをモニターすることができます。このページは、上位カテゴリーでグループ化されたオフェンスのリストを表示します。

このタスクについて

「**イベント数**」、「**フロー数**」、および「**ソース数**」などの「数」フィールドでは、ユーザーのネットワーク権限は考慮されません。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**カテゴリー別 (By Category)**」をクリックします。
3. 特定の上位カテゴリーの下位カテゴリー・グループを表示するには、上位カテゴリー名の横にある矢印アイコンをクリックします。
4. 下位カテゴリーのオフェンスのリストを表示するには、その下位カテゴリーをダブルクリックします。
5. 表示するオフェンスをダブルクリックします。

6. 「オフェンスのサマリー」ページで、オフェンスの詳細を確認します。オフェンスのパラメーター を参照してください。
7. オフェンスに対して必要なアクションがあれば実行します。オフェンスの管理タスク (Offense management tasks) を参照してください。

送信元 IP でグループ化されたオフェンスのモニター

「送信元」ページで、送信元 IP アドレスでグループ化されたオフェンスをモニターできます。

このタスクについて

送信元 IP アドレスは、システムへの攻撃の結果としてオフェンスを生成したホストを示します。すべての送信元 IP アドレスは、最大値を先頭にしてリストされます。オフェンスのリストは、アクティブなオフェンスを伴う送信元 IP アドレスのみを表示します。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**送信元 IP 別**」をクリックします。
3. 以下のオプションを使用して、オフェンスのリストを詳細化することができます。
   - 「**次のオフェンスを表示します**」リスト・ボックスから、特定の時間フレームでオフェンスのリストをフィルタリングするオプションを選択します。
   - 「**現在の検索パラメーター**」ペインに表示されている各フィルターの横にある、「**フィルターのクリア**」リンクをクリックします。
4. 表示するグループをダブルクリックします。
5. 送信元 IP アドレスに対するローカル宛先 IP アドレスのリストを表示するには、「送信元」ページのツールバーで「**宛先**」をクリックします。
6. この送信元 IP アドレスに関連付けられたオフェンスのリストを表示するには、「送信元」ページのツールバーで「**オフェンス**」をクリックします。
7. 表示するオフェンスをダブルクリックします。
8. 「オフェンスのサマリー」ページで、オフェンスの詳細を確認します。オフェンスのパラメーターを参照してください。
9. オフェンスに対して必要なアクションがあれば実行します。オフェンスの管理タスク (Offense management tasks) を参照してください。

宛先 IP でグループ化されたオフェンスのモニター

「宛先」ページで、ローカル宛先 IP アドレスでグループ化されたオフェンスをモニターすることができます。

このタスクについて

すべての宛先 IP アドレスは、最大値を先頭にしてリストされます。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**宛先 IP 別**」をクリックします。
3. 以下のオプションを使用して、オフェンスのリストを詳細化することができます。
   - 「**次のオフェンスを表示します**」リスト・ボックスから、特定の時間フレームでオフェンスのリストをフィルタリングするオプションを選択します。
   - 「**現在の検索パラメーター**」ペインに表示されている各フィルターの横にある、「**フィルターのクリア**」リンクをクリックします。
4. 表示する宛先 IP アドレスをダブルクリックします。
5. この宛先 IP アドレスに関連付けられたオフェンスのリストを表示するには、「宛先」ページのツールバーで「**オフェンス**」をクリックします。
6. この宛先 IP アドレスに関連付けられた送信元 IP アドレスのリストを表示するには、「宛先」ページのツールバーで「**送信元**」をクリックします。
7. 表示するオフェンスをダブルクリックします。
8. 「オフェンスのサマリー」ページで、オフェンスの詳細を確認します。オフェンスのパラメーターを参照してください。
9. オフェンスに対して必要なアクションがあれば実行します。オフェンスの管理タスク (Offense management tasks) を参照してください。

ネットワークでグループ化されたオフェンスのモニター

ネットワーク・ページで、ネットワークでグループ化されたオフェンスをモニターすることができます。

このタスクについて

すべてのネットワークは、最も高いマグニチュードを先頭にしてリストされます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ネットワーク別**」をクリックします。
3. 表示するネットワークをダブルクリックします。
4. このネットワークに関連付けられた送信元 IP アドレスのリストを表示するには、「ネットワーク」ページのツールバーで「**送信元**」をクリックします。
5. このネットワークに関連付けられた宛先 IP アドレスのリストを表示するには、「ネットワーク」ページのツールバーで「**宛先**」をクリックします。
6. このネットワークに関連付けられたオフェンスのリストを表示するには、「ネットワーク」ページのツールバーで「**オフェンス**」をクリックします。
7. 表示するオフェンスをダブルクリックします。
8. 「オフェンスのサマリー」ページで、オフェンスの詳細を確認します。オフェンスのパラメーターを参照してください。
9. オフェンスに対して必要なアクションがあれば実行します。オフェンスの管理タスク (Offense management tasks) を参照してください。

オフェンスの管理タスク

オフェンスをモニターするときに、オフェンスに関してアクションを実行することができます。

以下のアクションを実行することができます。

- メモを追加する
- オフェンスを削除する
- オフェンスを保護する
- オフェンスのデータを XML または CSV にエクスポートする
- オフェンスを他のユーザーに割り当てる
- E メール通知を送信する
- オフェンスにフォローアップ対象としてのマークを付ける
- すべてのオフェンス・リストのオフェンスを非表示にしたり閉じるしたりする

1 つのアクションを複数のオフェンスに対して実行するには、Ctrl キーを押したまま、アクションの対象にしたいそれぞれのオフェンスを選択してください。オフェンスの詳細を新規ページに表示するには、Ctrl キーを押したまま、オフェンスをダブルクリックしてください。

メモの追加

「**オフェンス**」タブ上ですべてのオフェンスにメモを追加することができます。メモには、オフェンスについてキャプチャーしたい、「お客様サポート」のチケット番号やオフェンスの管理情報などの情報を含めることができます。

このタスクについて

メモには、文字を 2000 文字まで含めることができます。

手順

1. 「**オフェンス**」タブをクリックします。
2. メモを追加するオフェンスにナビゲートします。
3. オフェンスをダブルクリックします。
4. 「**アクション**」リスト・ボックスから、「**メモの追加**」を選択します。
5. このオフェンスに含めるメモを入力します。
6. 「**メモの追加**をクリックします。

タスクの結果

このメモが、オフェンスのサマリーの「直近 5 件のメモ」ペイン内に表示されます。「**メモ**」アイコンが、**オフェンス**のリストのフラグ列内に表示されます。「**オフェンス**」リストの「**フラグ**」列で、マウス・ポインターをメモのインディケーターの上に移動すると、そのオフェンスのメモが表示されます。

オフェンスの非表示

「**オフェンス**」タブにオフェンスが表示されないようにするために、オフェンスを非表示にすることができます。

このタスクについて

オフェンスを非表示にすると、「**オフェンス**」タブのリスト (例えば、「すべてのオフェンス」) にオフェンスが表示されなくなります。ただし、非表示にしたオフェンスが含まれる検索を実行すると、該当する項目が検索結果に表示されます。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**すべてのオフェンス**」をクリックします。
3. 非表示にするオフェンスを選択します。
4. 「**アクション**」リスト・ボックスから、「**非表示**」を選択します。
5. 「**OK**」をクリックします。

非表示のオフェンスの表示

「**オフェンス**」タブでは非表示のオフェンスは表示されませんが、非表示のオフェンスを再度表示する必要がある場合には表示可能です。

このタスクについて

非表示のオフェンスを表示するには、非表示のオフェンスを含む検索を実行する必要があります。検索結果には、非表示と非表示ではないオフェンスを含む、すべてのオフェンスが含まれます。オフェンスは、「**フラグ (Flag)**」列の「**非表示 (Hidden)**」アイコンで非表示として指定されます。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**すべてのオフェンス**」をクリックします。
3. 次のように、非表示のオフェンスを検索します。
   a. 「**検索**」リスト・ボックスから、「**新規検索**」を選択します。
   b. 「検索パラメーター」ペインの「**除外オプション (Exclude option)**」リストで、「**非表示のオフェンス**」チェック・ボックスをクリアします。
   c. 「**検索**」をクリックします。
4. 表示する非表示のオフェンスを見つけて選択します。
5. 「**アクション**」リスト・ボックスから、「**表示**」を選択します。

オフェンスのクローズ

オフェンスは、システムから完全に削除するために閉じるすることができます。

このタスクについて

オフェンスを閉じる (削除) すると、そのオフェンスは「**オフェンス**」タブのすべてのリスト (例えば、「すべてのオフェンス」) で表示されなくなります。クローズされたオフェンスは、オフェンスの保存期間が過ぎた後にデータベースから削除されます。デフォルトのオフェンス保存期間は 3 日です。あるオフェンスに関するイベントがその後さらに発生した場合は、新しいオフェンスが作成されます。クローズされたオフェンスが含まれた検索を実行した場合、そのオフェンスがデータベースからまだ削除されていないときは、その項目が検索結果に表示されます。

オフェンスを閉じるする場合、オフェンスを閉じるする理由を選択する必要があり、またメモを追加することができます。「**メモ**」フィールドには、前のオフェンスのクローズで入力されたメモが表示されます。メモは、2,000 文字を超えることはできません。メモは、対象のオフェンスの「メモ」ペイン内に表示されます。「オフェンスのクローズの管理 (Manage Offense Closing)」権限を保持している場合、新規のカスタムの理由を「**クローズの理由 (Reason for Closing)**」リスト・ボックスに追加できます。

詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**すべてのオフェンス**」をクリックします。
3. 次のオプションのいずれかを選択してください。
   - 閉じるするオフェンスを選択した後、「**アクション**」リスト・ボックスから「**閉じる**」を選択します。
   - 「**アクション**」リスト・ボックスから、「**リスト項目のクローズ**を選択します。
4. 「**クローズの理由 (Reason for Closing)**」リスト・ボックスから、理由を選択します。デフォルトの理由は、「**問題なし (non-issue)**」です。
5. オプション。「**メモ**」フィールドに、このオフェンスのクローズに関する詳しい情報を指定するためにメモを入力します。
6. 「**OK**」をクリックします。

タスクの結果

オフェンスを閉じた後、「**オフェンス**」タブの「カテゴリー別 (By Category)」ペインのカウント表示が、閉じるされたオフェンスを反映するために数分かかる可能性があります。

オフェンスの保護

オフェンスが保存期間の経過後にデータベースから削除されないようにすることができます。

このタスクについて

オフェンスは、構成可能な保存期間の間保持されます。デフォルトの保存期間は 3 日間ですが、管理者は保存期間をカスタマイズできます。保存期間とは関係なく保持する必要のあるオフェンスが存在する場合があります。そうしたオフェンスが保存期間の経過後にデータベースから削除されないようにすることができます。

オフェンス保存期間の詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

注意:
SIM データ・モデルが「ハード・クリーン (Hard Clean)」オプションからリセットされると、保護されたオフェンスを含むすべてのオフェンスがデータベースおよびディスクから削除されます。SIM データ・モデルをリセットするには管理特権が必要です。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**すべてのオフェンス**」をクリックします。
3. 次のオプションのいずれかを選択してください。
   - 保護するオフェンスを選択した後、「**アクション**」リスト・ボックスから「**保護 (Protect)**」を選択します。
   - 「**アクション**」リスト・ボックスから、「**リスト項目の保護 (Protect Listed)**」を選択します。
4. 「**OK**」をクリックします。

タスクの結果

保護されたオフェンスは、「**フラグ (Flag)**」列の「**保護 (Protected)**」アイコンによって示されます。

オフェンスの保護解除

削除されないように以前に保護されたオフェンスの保護は、そのオフェンスの保存期間が経過したら解除することができます。

このタスクについて

保護されたオフェンスのみをリストする場合は、保護されたオフェンスのみが表示されるようにフィルターする検索を実行できます。「**保護 (Protected)**」チェック・ボックスをクリアして、「検索パラメーター」ペインの「**除外オプション (Excludes option)**」リストで他のすべてのオプションが確実に選択されている場合は、保護されたオフェンスのみが表示されます。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**すべてのオフェンス**」をクリックします。
3. オプション。保護されたオフェンスのみを表示する検索を実行します。
4. 次のオプションのいずれかを選択してください。
   - 保護するオフェンスを選択して、「アクション」リスト・ボックスから「**保護の解除**」を選択します。
   - 「**アクション**」リスト・ボックスから、「**リスト項目の保護解除**」を選択します。
5. 「**OK**」をクリックします。

オフェンスのエクスポート

オフェンスは XML (Extensible Markup Language) 形式または CSV (comma-separated values) 形式でエクスポートできます。

このタスクについて

オフェンスのデータを再使用または保管する場合は、オフェンスをエクスポートできます。例えば、オフェンスをエクスポートして、QRadar 以外の製品に基づくレポートを作成できます。また、予備用に長期保存する目的でオフェンスをエクスポートすることもできます。カスタマー・サポート部門は、トラブルシューティングの目的で、オフェンスのエクスポートが必要となる場合があります。

生成された XML または CSV ファイルには、検索パラメーターの「列定義」ペインで指定されたパラメーターが含まれています。データのエクスポートに必要な時間の長さは、指定したパラメーターの数によって変わります。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**すべてのオフェンス**」をクリックします。
3. エクスポートするオフェンスを選択します。
4. 次のオプションのいずれかを選択してください。
   - オフェンスを XML 形式でエクスポートするには、「アクション」リスト・ボックスから「**アクション**」 > 「**XML にエクスポート**」を選択します。
   - オフェンスを CSV 形式でエクスポートするには、「アクション」リスト・ボックスから「**アクション**」 > 「**CSV にエクスポート**」を選択します。
5. 次のオプションのいずれかを選択してください。
   - リストを開きすぐに表示するには、「**アプリケーションから開く (Open with)**」オプションを選択し、リスト・ボックスからアプリケーションを選択します。
   - リストを保存するには、「**ディスクに保存 (Save to Disk)**」オプションを選択します。
6. 「**OK**」をクリックします。

ユーザーへのオフェンスの割り当て

「**オフェンス**」タブを使用すれば、調査のためにオフェンスをユーザーに割り当てることができます。

このタスクについて

オフェンスがあるユーザーに割り当てられられている場合、そのオフェンスは、そのユーザーの「自分のオフェンス」ページに表示されます。オフェンスをユーザーに割り当てるには、適切な特権を保持している必要があります。

オフェンスのユーザーへの割り当ては、「**オフェンス**」タブまたは「オフェンスのサマリー」ページのいずれかで行うことができます。この手順では、「**オフェンス**」タブでオフェンスを割り当てる方法について説明しています。

注: 「**ユーザー名**」リスト・ボックスに表示されるユーザーは、「**オフェンス**」タブの特権を保持するユーザーのみです。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**すべてのオフェンス**」をクリックします。
3. 割り当てるオフェンスを選択します。
4. 「**アクション**」リスト・ボックスから、「**割り当て**」を選択します。
5. 「**ユーザー名**」リスト・ボックスから、このオフェンスの割り当て先のユーザーを選択します。
6. 「**保存**」をクリックします。

タスクの結果

オフェンスが選択したユーザーに割り当てられました。オフェンスが割り当てられたことを示すために、「**ユーザー (User)**」アイコンが「**オフェンス**」タブの「フラグ (Flag)」列内に表示されます。指定されたユーザーは、このオフェンスをそのユーザーの「自分のオフェンス」ページで確認できます。

E メール通知の送信

オフェンスのサマリーを含む E メールを、すべての有効な E メール・アドレスに送信することができます。

このタスクについて

E メール・メッセージの本文には、以下の情報が含まれます (取得可能な場合)。

- 送信元 IP アドレス
- 送信元ユーザー名、ホスト名、またはアセット名
- 送信元の総数
- マグニチュードで上位 5 個の送信元
- 送信元ネットワーク
- 宛先 IP アドレス
- 宛先ユーザー名、ホスト名、またはアセット名
- 宛先の総数
- マグニチュードで上位 5 個の宛先
- 宛先ネットワーク
- イベントの総数
- オフェンスまたはイベント・ルールの起動を引き起こしたルール
- オフェンスまたはイベント・ルールの詳しい説明
- オフェンス ID
- 上位 5 個のカテゴリー
- オフェンスの開始時刻またはイベント生成時刻
- 上位 5 個の注釈
- オフェンスのユーザー・インターフェースへのリンク

- 要因となる CRE ルール

手順

1. 「**オフェンス**」タブをクリックします。
2. E メール通知を送信する対象のオフェンスにナビゲートします。
3. オフェンスをダブルクリックします。
4. 「**アクション**」リスト・ボックスから、「**E メール**」を選択します。
5. 以下のパラメーターを構成します。

オプション	**説明**
パラメーター	説明
宛先 (To)	選択されたオフェンスに対して変化が起こった場合に通知するユーザーの E メール・アドレスを入力します。複数の E メール・アドレスはコンマで分離します。
送信者 (From)	デフォルトの発信元 E メール・アドレスを入力します。デフォルトは root@localhost.com です。
E メールの件名	E メールのデフォルトの件名を入力します。デフォルトはオフェンス ID です。
E メール・メッセージ	通知 E メールに記載する標準のメッセージを入力します。

6. 「**送信**」をクリックします。

フォローアップ項目のマーク付け

「**オフェンス**」タブを使用して、フォローアップ対象のオフェンス、送信元 IP アドレス、宛先 IP アドレス、およびネットワークをマークできます。これにより、特定の項目を追跡してさらなる調査を行うことができます。

手順

1. 「**オフェンス**」タブをクリックします。
2. フォローアップのためにマークするオフェンスにナビゲートします。
3. オフェンスをダブルクリックします。
4. 「**アクション**リスト・ボックスから、「**フォローアップ**」を選択します。

タスクの結果

オフェンスの「**フラグ**」列に、このオフェンスがフォローアップ対象であることを示すフラグが表示されます。フラグ付きオフェンスがオフェンス・リストに表示されない場合は、リストをソートしてしてすべてのフラグ付きオフェンスが先頭に表示されるようにすることができます。オフェンス・リストをフラグ付きオフェンスでソートするには、「**フラグ**」列の見出しをダブルクリックします。

「オフェンス」タブ・ツールバーの機能

「**オフェンス**」タブのそれぞれのページと表には、特定のアクションを実行したりオフェンスの要因を調べたりするために必要な機能を提供するツールバーが用意されています。

表 13. 「オフェンス」タブ・ツールバーの機能

機能	説明
メモの追加	オフェンスに対して新しいメモを追加するには、「**メモの追加**」をクリックします。このオプションは、「オフェンスのサマリー」ページの最後の 5 つの「メモ」ペインでのみ使用することができます。

表 13. 「オフェンス」タブ・ツールバーの機能 (続き)

機能	説明
アクション	「**アクション**」リスト・ボックスで選択可能なオプションは、ページ、表、項目 (オフェンスや送信元 IP アドレスなど) によって異なります。そのため、「**アクション**」リスト・ボックスのオプションは、以下のとおりに表示されないことがあります。 「**アクション**」リスト・ボックスで、以下のいずれかのアクションを選択することができます。 • **フォローアップ** - 詳細なフォローアップの対象として項目にマークを付けるには、このオプションを選択します。フォローアップ項目のマーク付けを参照してください。 • **非表示** - オフェンスを非表示にするには、このオプションを選択します。オフェンスの非表示については、オフェンスの非表示を参照してください。 • **表示** - 非表示になっているすべてのオフェンスを表示するには、このオプションを選択します。 • **オフェンスの保護** - オフェンスを保護するには、このオプションを選択します。オフェンスの保護については、オフェンスの保護を参照してください。 • **閉じる** - オフェンスを閉じるするには、このオプションを選択します。オフェンスのクローズについて詳しくは、オフェンスのクローズを参照してください。 • **リスト項目のクローズ** - リストされたオフェンスを閉じるするには、このオプションを選択します。リストされたオフェンスをクローズする方法については、オフェンスのクローズを参照してください。 • **E メール** - オフェンスのサマリーを 1 人以上の受信者に E メールで送信するには、このオプションを選択します。詳しくは、E メール通知の送信を参照してください。 • **メモの追加** - オフェンスに対してメモを追加するには、このオプションを選択します。詳しくは、メモの追加を参照してください。 • **割り当て** - ユーザーにオフェンスを割り当てるには、このオプションを選択します。詳しくは、ユーザーへのオフェンスの割り当てを参照してください。 • **印刷** - オフェンスを印刷するには、このオプションを選択します。
注釈	特定のオフェンスに関するすべての注釈を表示するには、「**注釈**」をクリックします。 • **注釈** - この注釈の詳細を指定します。注釈は、テキスト記述です。ルールは、ルール応答の一部として、注釈をオフェンスに自動的に追加することができます。 • **時刻** - この注釈が作成された日時を指定します。

表 13. 「オフェンス」タブ・ツールバーの機能 (続き)

機能	説明
アノマリ	アノマリ検出ルールによってオフェンスが生成される原因となった保存済みの検索結果を表示するには、「**アノマリ**」をクリックします。 **注:** このボタンは、そのオフェンスがアノマリ検出ルールによって生成された場合のみ表示されます。
カテゴリー	オフェンスに関するカテゴリー情報を表示するには、「**カテゴリー**」をクリックします。 特定のカテゴリーに関連するイベントをさらに調べるには、そのカテゴリーを右クリックして、「**イベント**」または「**フロー**」を選択します。あるいは、カテゴリーを強調表示して、「イベント・カテゴリーのリスト」ツールバーの「**イベント**」アイコンまたは「**フロー**」アイコンをクリックすることもできます。
接続	接続についてさらに調べるには、「**接続**」をクリックします。 **注:** このオプションは、IBM Security QRadar Risk Manager> を購入してライセンス交付を受けている場合のみ選択することができます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。 「**接続**」アイコンをクリックすると、イベント検索条件が事前に取り込まれた接続検索条件ページが、新規ページとして表示されます。 検索パラメーターは、必要に応じてカスタマイズすることができます。接続情報を表示するには「**検索**」をクリックします。
宛先	特定のオフェンス、送信元 IP アドレス、またはネットワークのすべてのローカル宛先 IP アドレスを表示するには、「**宛先**」をクリックします。 **注:** 宛先 IP アドレスがリモートの場合、そのリモート宛先 IP アドレスに関する情報が個別のページに表示されます。
表示	「オフェンスのサマリー」ページには、特定のオフェンスに関連する情報を示すさまざまな表が表示されます。特定の表を探すには、表示したい表までスクロールするか、「**表示**」リスト・ボックスからオプションを選択します。
イベント	特定のオフェンスに関するすべてのイベントを表示するには、「**イベント**」をクリックします。「**イベント**」をクリックすると、イベントの検索結果が表示されます。
フロー	特定のオフェンスに関連するフローをさらに調べるには、「**フロー**」をクリックします。「**フロー**」をクリックすると、フローの検索結果が表示されます。
ログ・ソース	特定のオフェンスに関するすべてのログ・ソースを表示するには、「**ログ・ソース**」をクリックします。
ネットワーク	特定のオフェンスに関するすべての宛先ネットワークを表示するには、「**ネットワーク**」をクリックします。

表 13. 「オフェンス」タブ・ツールバーの機能 (続き)

機能	説明
メモ	特定のオフェンス、送信元 IP アドレス、宛先 IP アドレス、またはネットワークに関するすべてのメモを表示するには、「**メモ**」をクリックします。メモについて詳しくは、メモの追加を参照してください。
オフェンス	特定の送信元 IP アドレス、宛先 IP アドレス、またはネットワークに関連するオフェンスのリストを表示するには、「**オフェンス**」をクリックします。
印刷	特定のオフェンスを印刷するには、「**印刷**」をクリックします。
ルール	特定のオフェンスの原因となったすべてのルールを表示するには、「**ルール**」をクリックします。そのオフェンスを作成したルールがリストの先頭に表示されます。 ルールを編集するための適切な権限を持っている場合、該当のルールをダブルクリックすると「ルールの編集 (Edit Rules)」ページが開始されます。 ルールが削除されている場合、そのルールの隣に赤のアイコン (x) が表示されます。削除されているルールをダブルクリックすると、そのルールは存在しないことを示すメッセージが表示されます。
条件の保存	オフェンスの検索後に「**条件の保存**」をクリックすると、将来使用する目的で検索条件が保存されます。
レイアウトの保存	デフォルトでは、「カテゴリー別の詳細 (By Category Details)」ページは、「オフェンス数」パラメーターによってソートされます。ソート順を変更する場合や、別のパラメーターでソートする場合は、「**レイアウトの保存**」をクリックすると、現在の表示がデフォルト・ビューとして保存されます。次に「**オフェンス**」タブにログインすると、保存されたレイアウトが表示されます。
検索	このオプションは、「ローカル宛先のリスト」表のツールバーでのみ選択することができます。 特定の送信元 IP アドレスの宛先 IP アドレスをフィルタリングするには、「**検索**」をクリックします。宛先をフィルタリングするには、以下の手順を実行します。 1. 「**検索**」をクリックします。 2. 次の各パラメーターの値を入力します。 • **宛先ネットワーク** - フィルタリングしたいネットワークをリスト・ボックスから選択します。 • **マグニチュード** - 構成された値について、等しいマグニチュード、より小さなマグニチュード、より大きなマグニチュードのいずれをフィルタリングするのかを、リスト・ボックスから選択します。 • **ソート順** - フィルター結果のソート方法をリスト・ボックスから選択します。 3. 「**検索**」をクリックします。

表 13. 「オフェンス」タブ・ツールバーの機能 (続き)

機能	説明
非アクティブのカテゴリーを表示する	「カテゴリー別 (By Category)」詳細ページでは、各カテゴリーの件数が、下位カテゴリーの値から集計されます。関連するオフェンスが存在する下位カテゴリーには、矢印が示されます。この矢印をクリックすると、関連する下位カテゴリーを表示することができます。すべてのカテゴリーを表示する場合は、「**非アクティブのカテゴリーを表示する**」をクリックします。
送信元	特定のオフェンス、宛先 IP アドレス、またはネットワークに関するすべての送信元 IP アドレスを表示するには、「**送信元**」をクリックします。
サマリー	「**表示**」リスト・ボックスからオプションをクリックした場合、「**サマリー**」をクリックすると、詳細なサマリー・ビューに戻ることができます。
ユーザー	特定のオフェンスに関連するすべてのユーザーを表示するには、「**ユーザー**」をクリックします。
攻撃パスの表示 (View Attack Path)	特定のオフェンスの攻撃パスをさらに調べるには、「**攻撃パスの表示 (View Attack Path)**」をクリックします。「**攻撃パスの表示 (View Attack Path)**」アイコンをクリックすると、「現在のトポロジー (Current Topology)」ページが新規ページとして表示されます。 **注:** このオプションは、IBM Security QRadar Risk Manager> を購入してライセンス交付を受けている場合のみ選択することができます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。
トポロジーの表示	特定のオフェンスの送信元をさらに調べるには、「**トポロジーの表示**」をクリックします。「**トポロジーの表示**」アイコンをクリックすると、「現在のトポロジー (Current Topology)」ページが新規ページとして表示されます。 **注:** このオプションは、IBM Security QRadar Risk Manager を購入してライセンス交付を受けている場合のみ、選択することができます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。

オフェンスのパラメーター

以下の表では、「オフェンス」タブで提供されるパラメーターについて説明します。

表 14. オフェンスのパラメーター

パラメーター	ロケーション	説明
注釈	「上位 5 件の注釈」表	注釈の詳細を指定します。注釈は、テキスト記述です。ルールは、ルール応答の一部として、注釈をオフェンスに自動的に追加することができます。
アノマリ	「最後の 10 件のイベント (アノマリ・イベント) (Last 10 Events (Anomaly Events))」表	このオプションを選択すると、アノマリ検出ルールによってイベントが生成される原因となった、保存済みの検索結果が表示されます。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
アノマリ・テキスト (Anomaly Text)	「最後の 10 件のイベント (アノマリ・イベント) (Last 10 Events (Anomaly Events))」表	アノマリ検出ルールによって検出されたアノマリな動作の説明を指定します。
アノマリ値 (Anomaly Value)	「最後の 10 件のイベント (アノマリ・イベント) (Last 10 Events (Anomaly Events))」表	アノマリ検出ルールによってオフェンスが生成される原因となった値を指定します。
アプリケーション	「最後の 10 件のフロー (Last 10 Flows)」表	フローに関連したアプリケーションを指定します。
アプリケーション名 (Application Name)	「オフェンスのタイプ」が「アプリケーション・アイデンティティー」の場合は、「オフェンスの送信元」表	オフェンスを作成したフローに関連するアプリケーションを指定します。
ASN 索引 (ASN Index)	「オフェンスのタイプ」が「送信元 ASN」または「宛先 ASN」の場合は、「オフェンスの送信元」表	オフェンスを作成したフローに関連する ASN 値を指定します。
アセット名 (Asset Name)	「オフェンスのタイプ」が「送信元 IP」または「宛先 IP」の場合は、「オフェンスの送信元」表	アセット名を指定します。この名前は、「アセット・プロファイル」機能を使用して割り当てることができます。詳しくは、アセットの管理を参照してください。
アセット重要度	「オフェンスのタイプ」が「送信元 IP」または「宛先 IP」の場合は、「オフェンスの送信元」表	アセットの重みを指定します。この重みは、「アセット・プロファイル」機能を使用して割り当てることができます。詳しくは、アセットの管理を参照してください。
割り当て先 (Assigned to)	「オフェンス」表	オフェンスに割り当てられているユーザーを指定します。 ユーザーが割り当てられない場合は、このフィールドには「未割り当て (Not assigned)」が指定されます。オフェンスをユーザーに割り当てるには、「未割り当て (Not assigned)」をクリックします。詳しくは、ユーザーへのオフェンスの割り当てを参照してください。
カテゴリー (Category)	「最後の 10 件のイベント (Last 10 Events)」表	イベントのカテゴリーを指定します。
カテゴリー名 (Category Name)	「カテゴリー別の詳細 (By Category Details)」ページ	上位カテゴリー名を指定します。
チェーン (Chained)	• 「オフェンスのタイプ」が「宛先 IP」の場合は、「オフェンスの送信元」表 • 「上位 5 個の宛先 IP (Top 5 Destination IP's)」表	宛先 IP アドレスがチェーニングされているかどうかを指定します。 チェーニングされた宛先 IP アドレスは、他のオフェンスと関連付けられています。例えば、ある宛先 IP アドレスが他のオフェンスの送信元 IP アドレスになることがあります。宛先 IP アドレスがチェーニングされている場合、**「はい」**をクリックして、チェーニングされたオフェンスを表示します。
作成日	「直近 5 件のメモ」表	メモが作成された日時を指定します。
信頼性	「オフェンス」表	送信元デバイスから得られた信頼性格付けによって決められた、オフェンスの信頼性を指定します。例えば、複数のオフェンスで同じイベントまたはフローが報告されている場合、信頼性が高くなります。
現在の検索パラメーター	• 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ	表の上部に、検索結果に適用された検索パラメーターの詳細が表示されます。これらの検索パラメーターをクリアするには、**「フィルターのクリア」**をクリックしてください。 **注:** このパラメーターはフィルターの適用後にのみ表示されます。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
説明	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「オフェンス」表 • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ • 「オフェンスのタイプ」が「ログ・ソース」の場合は、「オフェンスの送信元」表 • 「上位 5 件のログ・ソース」表	オフェンスまたはログ・ソースの説明を指定します。
宛先 IP	• 「最後の 10 件のイベント (Last 10 Events)」表 • 「最後の 10 件のフロー (Last 10 Flows)」表	イベントまたはフローの宛先 IP アドレスを指定します。
宛先 IP	• 「上位 5 個の宛先 IP (Top 5 Destination IP's)」表 • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「ネットワーク別 - ローカル宛先のリストページ	宛先の IP アドレスを指定します。「管理」タブで DNS ルックアップが有効になっている場合、マウス・ポインターを IP アドレスに合わせることにより、DNS 名を表示することができます。
宛先 IP (Destination IP(s))	「オフェンス」表	ローカルまたはリモート宛先の IP アドレスおよび (使用可能な場合には) アセット名を指定します。リンクをクリックすると詳細が表示されます。
宛先 IP	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ	ローカルまたはリモート宛先の IP アドレスおよび (使用可能な場合には) アセット名を指定します。オフェンスに複数の宛先 IP アドレスが関連付けられている場合、このフィールドには「複数」が指定され、宛先 IP アドレスの数が示されます。
宛先 IP	• 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	このオフェンスに関連した宛先の IP アドレスおよび (使用可能な場合には) アセット名を指定します。「管理」タブで DNS ルックアップが有効になっている場合、マウス・ポインターを IP アドレスまたはアセット名に合わせることにより、DNS 名を表示することができます。
宛先 IP	「ネットワークの詳細別 (By Network Details)」ページ	ネットワークに関連した宛先 IP アドレスの数を指定します。
宛先ポート	「最後の 10 件のフロー (Last 10 Flows)」表	このフローの宛先ポートを指定します。
宛先 (Destination(s))	• 「上位 5 件の送信元 IP」表 • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - 送信元のリスト」ページ	オフェンスを作成したイベントまたはフローに関連した、QID マップで識別されたイベント名を指定します。イベント名にマウス・ポインターを合わせると、QID が表示されます。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
イベント/フローの数	「カテゴリー別の詳細 (By Category Details)」ページ	カテゴリー内のオフェンスに関連した、アクティブなイベントまたはフロー (クローズまたは非表示になっていないイベントまたはフロー) の数を指定します。 新規のイベントまたはフローが受信されない場合、オフェンスは一定期間のみアクティブ状態に維持されます。オフェンスは引き続き「オフェンス」タブに表示されますが、このフィールドではカウントされません。
イベント/フローの数	「宛先」ページ 「ネットワーク」ページ	オフェンスに関して発生したイベントおよびフローの数と、カテゴリーの数を指定します。 オフェンスに関連したイベントをさらに調査するには、イベント・リンクをクリックします。イベント・リンクをクリックすると、イベント検索結果が表示されます。 オフェンスに関連したフローをさらに調査するには、フロー・リンクをクリックします。フロー・リンクをクリックすると、フロー検索結果が表示されます。 **注:** フロー・カウントに「N/A」が表示される場合、オフェンスの開始日が、QRadar 製品をバージョン 7.1.0 (MR1) にアップグレードした日付より前である可能性があります。したがって、フローをカウントすることはできません。ただし、N/A リンクをクリックすることにより、フロー検索結果内の関連フローを調査することができます。
イベント/フローの数	「カテゴリー別の詳細 (By Category Details)」ページ	カテゴリー内のオフェンスに関連した、アクティブなイベントまたはフロー (クローズまたは非表示になっていないイベントまたはフロー) の数を指定します。 新規のイベントまたはフローが受信されない場合、オフェンスは一定期間のみアクティブ状態に維持されます。オフェンスは引き続き「オフェンス」タブに表示されますが、このフィールドではカウントされません。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
イベント/フローの数	「宛先」ページ 「ネットワーク」ページ	オフェンスに関して発生したイベントおよびフローの数と、カテゴリーの数を指定します。 オフェンスに関連したイベントをさらに調査するには、イベント・リンクをクリックします。イベント・リンクをクリックすると、イベント検索結果が表示されます。 オフェンスに関連したフローをさらに調査するには、フロー・リンクをクリックします。フロー・リンクをクリックすると、フロー検索結果が表示されます。 **注:** フロー・カウントに「N/A」が表示される場合、オフェンスの開始日が、QRadar 製品をバージョン 7.1.0 (MR1) にアップグレードした日付より前である可能性があります。したがって、フローをカウントすることはできません。ただし、N/A リンクをクリックすることにより、フロー検索結果内の関連フローを調査することができます。
イベント	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	オフェンスに関するイベントの数を指定します。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
イベント/フロー	• 「オフェンスの送信元」表 (「オフェンスのタイプ」が「送信元 IP」、「宛先 IP」、「ホスト名」、「ユーザー名」、「送信元ポート」、「宛先ポート」、「イベント名」、「ポート」、「送信元 MAC アドレス」、「宛先 MAC アドレス」、「ログ・ソース」、「送信元 IPv6」、「宛先 IPv6」、「送信元 ASN」、「宛先 ASN」、「ルール」、「アプリケーション・アイデンティティー」の場合) • 「上位 5 件の送信元 IP」表 • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「送信元の詳細」ページ • 「上位 5 件の宛先 IP」表 • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「ネットワーク別 - ローカル宛先のリストページ • 「上位 5 件のユーザー」表 • 「上位 5 件のログ・ソース」表 • 「上位 5 個のカテゴリー (Top 5 Categories)」表 • 「ネットワークの詳細別 (By Network Details)」ページ • 「上位 5 個のカテゴリー (Top 5 Categories)」表	送信元 IP アドレス、宛先 IP アドレス、イベント名、ユーザー名、MAC アドレス、ログ・ソース、ホスト名、ポート、ログ・ソース、ASN アドレス、IPv6 アドレス、ルール、ASN、アプリケーション、ネットワーク、またはカテゴリーと関連付けられたイベントの数またはフローの数を指定します。リンクをクリックすると詳細が表示されます。
最初のイベント/フローの確認日時	「送信元の詳細」ページ	送信元 IP アドレスが最初のイベントまたはフローを生成した日時を指定します。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
フラグ (Flag)	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	オフェンスに関して実行されるアクションを示します。アクションは以下のアイコンで表示されます。 • フラグ (Flag) - そのオフェンスにフォローアップの対象としてのマークが付けられていることを示します。これにより、特定の項目を追跡して、さらに調査することができます。オフェンスにフォローアップの対象としてマークを付ける方法については、フォローアップ項目のマーク付けを参照してください。 • ユーザー (User) - そのオフェンスがユーザーに割り当てられていることを示します。オフェンスがあるユーザーに割り当てられられている場合、そのオフェンスは、そのユーザーの「自分のオフェンス」ページに表示されます。ユーザーへのオフェンスの割り当てについて詳しくは、ユーザーへのオフェンスの割り当てを参照してください。 • メモ - そのオフェンスに対して、ユーザーがメモを追加したことを示します。「メモ」には、そのオフェンスに関して取り込みたいすべての情報を含めることができます。例えば、オフェンスに自動的に含まれない情報 (お客様サポート・チケット番号またはオフェンス管理情報など) を示すメモを追加できます。メモの追加について詳しくは、メモの追加を参照してください。 • 保護 (Protected) - そのオフェンスが保護されていることを示します。保護機能は、指定されたオフェンスが保存期間の経過後にデータベースから削除されるのを防ぎます。保護されたオフェンスについて詳しくは、オフェンスの保護を参照してください。 マウス・ポインターをアイコンに合わせると、追加情報が表示されます。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
フラグ (Flag) (続き)		• 非アクティブなオフェンス - オフェンスが非アクティブであることを示します。オフェンスは、最後のイベントを受信してから 5 日経つと非アクティブになります。また、すべてのオフェンスは、QRadar 製品ソフトウェアがアップグレードされると非アクティブになります。 非アクティブのオフェンスを再びアクティブにすることはできません。オフェンスについて新規イベントが検出されると、新規のオフェンスが作成され、オフェンスの保存期間が経過するまで非アクティブのオフェンスが保持されます。非アクティブのオフェンスに対して実行できるアクションとしては、保護、フォローアップ対象としてのフラグ付け、メモの追加、およびユーザーへの割り当てがあります。
フラグ (Flag)	• 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワークの詳細別 (By Network Details)」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「ネットワーク別 - ローカル宛先のリストページ	送信元 IP アドレス、宛先 IP アドレス、またはネットワークに対して実行されるアクションを指定します。例えば、フラグが表示された場合、オフェンスにはフォローアップのためにフラグが立てられています。マウス・ポインターをアイコンに合わせると、追加情報が表示されます。
フロー	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	オフェンスに関するフローの数を指定します。 **注:** 「フロー」列に「N/A」が表示される場合、オフェンスの開始日が、QRadar を 7.1.0 (MR1) にアップグレードした日付より前である可能性があります。
グループ	• 「オフェンスのタイプ」が「ログ・ソース」の場合は、「オフェンスの送信元」表 • 「上位 5 件のログ・ソース」表	ログ・ソースが属しているグループを指定します。
グループ (Group(s))	「オフェンスのタイプ」が「ルール」の場合は、「オフェンスの送信元」表	ルールが属しているルール・グループを指定します。
上位カテゴリー	「オフェンスのタイプ」が「イベント名」の場合は、「オフェンスの送信元」表	イベントの上位カテゴリーを指定します。 上位カテゴリーについて詳しくは、*IBM Security QRadar SIEM 管理ガイド* を参照してください。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
ホスト名	「オフェンスのタイプ」が「送信元 IP」または「宛先 IP」の場合は、「オフェンスの送信元」表	送信元 IP アドレスまたは宛先 IP アドレスに関連したホスト名を指定します。ホスト名が識別されない場合、このフィールドには「不明」が指定されます。
ヒストリカル相関プロファイル名	• オフェンスのサマリー	オフェンスを作成したヒストリカル相関プロファイルの名前を指定します。
ヒストリカル相関カタログ	• オフェンスのサマリー	オフェンスをトリガーしたイベントを含むヒストリカル相関カタログを指定します。 カタログのすべてのイベントを表示するには、「ヒストリカル相関」ウィンドウで**「履歴の表示」**をクリックします。
ヒストリカル相関プロファイル ID	• オフェンスのサマリー	オフェンスを作成したヒストリカル相関プロファイルの固有 ID を指定します。
ホスト名	「オフェンスのタイプ」が「ホスト名」の場合は、「オフェンスの送信元」表	オフェンスを作成したフローに関連するホスト名を指定します。
ID	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ	QRadar がオフェンスに割り当てている固有の識別番号を指定します。
IP	• 「オフェンスのタイプ」が「送信元 IP」または「宛先 IP」の場合は、「オフェンスの送信元」表 • 「送信元の詳細」ページ	オフェンスを作成したイベントまたはフローに関連する送信元 IP アドレスを指定します。
IP/DNS 名 (IP/DNS Name)	「宛先」ページ	宛先の IP アドレスを指定します。**「管理」**タブで DNS ルックアップが有効になっている場合、マウス・ポインターを IP アドレスまたはアセット名に合わせることにより、DNS 名を表示することができます。 詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
IPv6	「オフェンスのタイプ」が「送信元 IPv6」または「宛先 IPv6」の場合は、「オフェンスの送信元」表	オフェンスを作成したイベントまたはフローに関連する IPv6 アドレスを指定します。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
最後のイベント/フロー	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「上位 5 件の送信元 IP」表 • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「上位 5 件の宛先 IP」表 • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - ローカル宛先のリストページ • 「上位 5 個のカテゴリー (Top 5 Categories)」表	オフェンス、カテゴリー、送信元 IP アドレス、または宛先 IP アドレスに関して最後のイベントまたはフローが観察されてからの経過時間を指定します。
最後のイベント/フローの確認日時	「送信元の詳細」ページ	送信元 IP アドレスと関連するイベントまたはフローが最後に生成された日時を指定します。
最後のイベント/フローの時刻	「オフェンスのタイプ」が「ログ・ソース」の場合は、「オフェンスの送信元」表	システムでログ・ソースが最後に観察された日時を指定します。
最後に認識されたグループ (Last Known Group)	「オフェンスのタイプ」が「ユーザー名」、「送信元 MAC アドレス」、「宛先 MAC アドレス」、または「ホスト名」の場合は、「オフェンスの送信元」表	ユーザー、MAC アドレス、またはホスト名が属している、現在のグループを指定します。どのグループにも関連付けられていない場合、このフィールドの値は「不明」になります。 **注:** このフィールドには、履歴情報は表示されません。
最後に認識されたホスト (Last Known Host)	「オフェンスのタイプ」が「ユーザー名」、「送信元 MAC アドレス」、または「宛先 MAC アドレス」の場合は、「オフェンスの送信元」表	ユーザーまたは MAC アドレスが関連付けられている、現在のホストを指定します。ホストが識別されない場合、このフィールドには「不明」が指定されます。 **注:** このフィールドには、履歴情報は表示されません。
最後に認識された IP (Last Known IP)	「オフェンスのタイプ」が「ユーザー名」、「送信元 MAC アドレス」、「宛先 MAC アドレス」、または「ホスト名」の場合は、「オフェンスの送信元」表	ユーザー、MAC、またはホスト名の現在の IP アドレスを指定します。IP アドレスが識別されない場合、このフィールドには「不明」が指定されます。 **注:** このフィールドには、履歴情報は表示されません。
最後に認識された MAC (Last Known MAC)	「オフェンスのタイプ」が「ユーザー名」または「ホスト名」の場合は、「オフェンスの送信元」表	ユーザー名またはホスト名の、最後に認識された MAC アドレスを指定します。MAC が識別されない場合、このフィールドには「不明」が指定されます。 **注:** このフィールドには、履歴情報は表示されません。
最後に認識されたマシン (Last Known Machine)	「オフェンスのタイプ」が「ユーザー名」、「送信元 MAC アドレス」、「宛先 MAC アドレス」、または「ホスト名」の場合は、「オフェンスの送信元」表	ユーザー、MAC アドレス、またはホスト名に関連付けられている、現在のマシン名を指定します。マシン名が識別されない場合、このフィールドには「不明」が指定されます。 **注:** このフィールドには、履歴情報は表示されません。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
最後に認識されたユーザー名 (Last Known Username)	「オフェンスのタイプ」が「送信元 MAC アドレス」、「宛先 MAC アドレス」、または「ホスト名」の場合は、「オフェンスの送信元」表	MAC アドレスまたはホスト名の現在のユーザーを指定します。MAC アドレスが識別されない場合、このフィールドには「不明」が指定されます。 **注:** このフィールドには、履歴情報は表示されません。
最後の監視日 (Last Observed)	「オフェンスのタイプ」が「ユーザー名」、「送信元 MAC アドレス」、「宛先 MAC アドレス」、または「ホスト名」の場合は、「オフェンスの送信元」表	システムでその MAC アドレスまたはホスト名が最後に観察された日時を指定します。
最後のパケットの時刻 (Last Packet Time)	「最後の 10 件のフロー (Last 10 Flows)」表	フローに関するパケットが最後に送信された日時を指定します。
ローカル宛先の数 (Local Destination Count)	「上位 5 個のカテゴリー (Top 5 Categories)」表 「カテゴリー別の詳細 (By Category Details)」ページ	カテゴリーに関連したローカル宛先 IP アドレスの数を指定します。
ローカル宛先 (Local Destination(s))	「送信元の詳細」ページ	この送信元 IP アドレスに関連したローカル宛先 IP アドレスを指定します。宛先 IP アドレスに関する詳細を表示するには、該当の IP アドレス、または表示されている用語をクリックします。 複数の宛先 IP アドレスがある場合、「複数」という用語が表示されます。
ロケーション	• 「オフェンスのタイプ」が「送信元 IP」または「宛先 IP」の場合は、「オフェンスの送信元」表 • 「上位 5 件の送信元 IP」表 • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「送信元の詳細」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - 送信元のリスト」ページ	送信元 IP アドレスまたは宛先 IP アドレスのネットワーク・ロケーションを指定します。ロケーションがローカルである場合、リンクをクリックしてネットワークを表示することができます。
ログ・ソース	「最後の 10 件のイベント (Last 10 Events)」表	イベントを検出したログ・ソースを指定します。
ログ・ソース ID	「オフェンスのタイプ」が「ログ・ソース」の場合は、「オフェンスの送信元」表	ログ・ソースのホスト名を指定します。
ログ・ソース名	「オフェンスのタイプ」が「ログ・ソース」の場合は、「オフェンスの送信元」表	オフェンスを作成したイベントに関連する、「ログ・ソース」表で識別されたログ・ソース名を指定します。 **注:** ログ・ソース・オフェンスに関して表示される情報は、「管理」タブの「ログ・ソース」ページから得られます。「管理」タブにアクセスしてログ・ソースを管理するには、管理アクセス権限が必要です。ログ・ソースの管理について詳しくは、「*Managing Log Sources Guide*」を参照してください。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
ログ・ソース	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	オフェンスに関連したログ・ソースを指定します。そのオフェンスに複数のログ・ソースが関連付けられている場合、このフィールドには「複数」が指定され、ログ・ソースの数が示されます。
下位カテゴリー	「オフェンスのタイプ」が「イベント名」の場合は、「オフェンスの送信元」表	イベントの下位カテゴリーを指定します。
MAC	• 「オフェンスのタイプ」が「送信元 IP」または「宛先 IP」の場合は、「オフェンスの送信元」表 • 「上位 5 件の送信元 IP」表 • 「上位 5 件の宛先 IP」表 • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「ネットワーク別 - ローカル宛先のリストページ	オフェンスが開始したときの送信元 IP アドレスまたは宛先 IP アドレスを指定します。MAC アドレスが不明な場合、このフィールドには「不明」が指定されます。
MAC アドレス	「オフェンスのタイプ」が「送信元 MAC アドレス」または「宛先 MAC アドレス」の場合は、「オフェンスの送信元」表	このオフェンスを作成したイベントに関連する MAC アドレスを指定します。MAC アドレスが識別されない場合、このフィールドには「不明」が指定されます。
マグニチュード	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「オフェンス」表 • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ • 「上位 5 個のカテゴリー (Top 5 Categories)」表 • 「最後の 10 件のイベント (Last 10 Events)」表 • 「ネットワークの詳細別 (By Network Details)」ページ • 「ネットワーク」ページ	オフェンス、カテゴリー、イベント、またはネットワークの相対的な重要性を指定します。マグニチュードを示すバーにより、相関するすべての変数が視覚的に表現されます。変数には、関連性、重大度、および信頼性が含まれます。マウス・ポインターをマグニチュードを示すバーに合わせると、値および計算されたマグニチュードが表示されます。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
マグニチュード	• 「オフェンスのタイプ」が「送信元 IP」または「宛先 IP」の場合は、「オフェンスの送信元」表 • 「上位 5 件の送信元 IP」表 • 「上位 5 件の宛先 IP」表 • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「送信元の詳細」ページ • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「宛先」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「ネットワーク別 - ローカル宛先のリストページ	送信元 IP アドレスまたは宛先 IP アドレスの相対的な重要性を指定します。マグニチュードを示すバーにより、IP アドレスと関連するアセットの CVSS リスク値が視覚的に表現されます。マウス・ポインターをマグニチュードを示すバーに合わせると、計算されたマグニチュードが表示されます。
名前	• 「上位 5 件のログ・ソース」表 • 「上位 5 件のユーザー」表 • 「上位 5 個のカテゴリー (Top 5 Categories)」表 • 「ネットワーク」ページ	ログ・ソースの名前、ユーザー、カテゴリー、ネットワーク IP アドレス、または名前を指定します。
ネットワーク	「ネットワークの詳細別 (By Network Details)」ページ	ネットワークの名前を指定します。
ネットワーク (Network(s))	「オフェンス」表	オフェンスに関する宛先ネットワークを指定します。オフェンスの宛先ネットワークが 1 つである場合、このフィールドにはそのネットワーク・リーフが表示されます。リンクをクリックするとネットワーク情報が表示されます。オフェンスの宛先ネットワークが複数ある場合、「複数」という用語が表示されます。リンクをクリックすると詳細が表示されます。
メモ	• 「オフェンスのタイプ」が「ルール」の場合は、「オフェンスの送信元」表 • 「直近 5 件のメモ」表	このルールに関するメモを指定します。
オフェンス数	「カテゴリー別の詳細 (By Category Details)」ページ	各カテゴリー内のアクティブなオフェンスの数を指定します。アクティブなオフェンスとは、非表示またはクローズ状態になっていないオフェンスのことです。 「カテゴリー別の詳細 (By Category Details)」ページに「非表示のオフェンスの除外 (Exclude Hidden Offenses)」フィルターが含まれている場合、「オフェンス数」パラメーターに表示されるオフェンス数が正確ではない可能性があります。「カテゴリー別」ペインに合計数を表示させるには、「カテゴリー別の詳細 (By Category Details)」ページの「非表示のオフェンスの除外 (Exclude Hidden Offenses)」フィルターの隣にある**「フィルターのクリア」**をクリックします。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
オフェンスの送信元	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	オフェンスの送信元に関する情報を指定します。**「オフェンスの送信元」**フィールドに表示される情報は、オフェンスのタイプによって異なります。例えば、オフェンスのタイプが「送信元ポート」である場合、**「オフェンスの送信元」**フィールドには、そのオフェンスを作成したイベントの送信元ポートが表示されます。
オフェンスのタイプ	• 「自分のオフェンス」ページ • 「オフェンス」表 • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	オフェンスのタイプを指定します。オフェンスのタイプは、そのオフェンスを作成したルールによって決まります。例えば、オフェンスのタイプがログ・ソース・イベントである場合、そのオフェンスを生成したルールは、そのイベントを検出したデバイスに基づくイベントを相互に関連付けます。 オフェンスのタイプには、以下のものがあります。 • 送信元 IP • 宛先 IP • イベント名 • ユーザー名 (User Name) • 送信元 MAC アドレス • 宛先 MAC アドレス • ログ・ソース • ホスト名 • 送信元ポート • 宛先ポート • 送信元 IPv6 • 宛先 IPv6 • 送信元 ASN • 宛先 ASN • ルール • アプリケーション・アイデンティティー オフェンスのタイプにより、「オフェンスの送信元のサマリー」ペインに表示される情報のタイプが決まります。
オフェンス (Offense(s))	• 「送信元の詳細」ページ • 「宛先」ページ	送信元 IP アドレスまたは宛先 IP アドレスに関連する、オフェンスの名前を指定します。オフェンスに関する詳細を表示するには、表示されている名前または用語をクリックします。 複数のオフェンスがある場合、「複数」という用語が表示されます。
実行されたオフェンス (Offense(s) Launched)	「ネットワーク」ページ	ネットワークから実行されたオフェンスを指定します。 複数のオフェンスが関与している場合、このフィールドには「複数」が指定され、オフェンスの数が示されます。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
ターゲットとなったオフェンス (Offense(s) Targeted)	「ネットワーク」ページ	ネットワークでターゲットとなったオフェンスを指定します。 複数のオフェンスが関与している場合、このフィールドには「複数」が指定され、オフェンスの数が示されます。
オフェンス	• 「オフェンスの送信元」表 (「オフェンスのタイプ」が「送信元 IP」、「宛先 IP」、「イベント名」、「ユーザー名」、「送信元 MAC アドレス」、「宛先 MAC アドレス」、「ログ・ソース」、「ホスト名」、「送信元ポート」、「宛先ポート」、「送信元 IPv6」、「宛先 IPv6」、「送信元 ASN」、「宛先 ASN」、「ルール」、「アプリケーション・アイデンティティー」の場合) • 「上位 5 件の送信元 IP」表 • 「上位 5 件の宛先 IP」表 • 「上位 5 件のログ・ソース」表 • 「上位 5 件のユーザー」表 • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「ネットワーク別 - ローカル宛先のリストページ	送信元 IP アドレス、宛先 IP アドレス、イベント名、ユーザー名、MAC アドレス、ログ・ソース、ホスト名、ポート、IPv6 アドレス、ASN、ルール、またはアプリケーションと関連付けられたオフェンスの数を指定します。リンクをクリックすると詳細が表示されます。
実行されたオフェンス (Offenses Launched)	「ネットワークの詳細別 (By Network Details)」ページ	ネットワークから発生したオフェンスの数を指定します。
ターゲットとなったオフェンス (Offenses Targeted)	「ネットワークの詳細別 (By Network Details)」ページ	ネットワークでターゲットとなったオフェンスの数を指定します。
ポート	「オフェンスのタイプ」が「送信元ポート」または「宛先ポート」の場合は、「オフェンスの送信元」表	オフェンスを作成したイベントまたはフローに関連するポートを指定します。
関連性	「オフェンス」表	オフェンスの相対的な重要性を指定します。
応答 (Response)	「オフェンスのタイプ」が「ルール」の場合は、「オフェンスの送信元」表	ルールの応答タイプを指定します。
ルールの説明	「オフェンスのタイプ」が「ルール」の場合は、「オフェンスの送信元」表	ルール・パラメーターのサマリーを指定します。
ルール名	「オフェンスのタイプ」が「ルール」の場合は、「オフェンスの送信元」表	オフェンスを作成したイベントまたはフローに関連するルールの名前を指定します。 **注:** ルール・オフェンスに関して表示される情報は、「**ルール**」タブから得られます。
ルール・タイプ (Rule Type)	「オフェンスのタイプ」が「ルール」の場合は、「オフェンスの送信元」表	オフェンスのルール・タイプを指定します。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
重大度	• 「オフェンスのタイプ」が「イベント名」の場合は、「オフェンスの送信元」表 • 「オフェンス」表	イベントまたはオフェンスの重大度を指定します。重大度は、オフェンスがもたらす脅威の大きさを、攻撃に対する宛先 IP アドレスでの準備の程度と対比して示します。この値は、そのオフェンスに関連するイベント・カテゴリーに直接マップされます。例えば、サービス妨害 (DoS) 攻撃の重大度は 10 であり、重大なオカレンスを表します。
送信元数	「カテゴリー別の詳細 (By Category Details)」ページ	カテゴリー内のオフェンスに関連した送信元 IP アドレスの数を指定します。ある送信元 IP アドレスが 5 つの異なる下位カテゴリー内のオフェンスに関連している場合、その送信元 IP アドレスは 1 回しかカウントされません。
送信元 IP	• 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「上位 5 件の送信元 IP」表 • 「最後の 10 件のフロー (Last 10 Flows)」表	ネットワーク内のコンポーネントのセキュリティーを侵害しようとするデバイスの IP アドレスまたはホスト名を指定します。「管理」タブで DNS ルックアップが有効になっている場合、マウス・ポインターを IP アドレスに合わせることにより、DNS 名を表示することができます。 詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
送信元 IP (Source IP(s))	「オフェンス」表	ネットワーク内のコンポーネントのセキュリティーを侵害しようとするデバイスの IP アドレスまたはホスト名を指定します。リンクをクリックすると詳細が表示されます。 送信元 IP アドレスについて詳しくは、送信元 IP でグループ化されたオフェンスのモニターを参照してください。
送信元 IP (Source IPs)	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	ネットワーク内のコンポーネントのセキュリティーを侵害しようとするデバイスの IP アドレスまたはホスト名を指定します。そのオフェンスに複数の送信元 IP アドレスが関連付けられている場合、このフィールドには「複数」が指定され、送信元 IP アドレスの数が示されます。「管理」タブで DNS ルックアップが有効になっている場合、マウス・ポインターを IP アドレスまたはアセット名に合わせることにより、DNS 名を表示することができます。 詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
送信元 IP (Source IPs)	「ネットワークの詳細別 (By Network Details)」ページ	ネットワークに関連した送信元 IP アドレスの数を指定します。
送信元ポート	「最後の 10 件のフロー (Last 10 Flows)」表	このフローの送信元ポートを指定します。
送信元	• 「上位 5 件の宛先 IP」表 • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ	宛先 IP アドレスに関連した送信元 IP アドレスの数を指定します。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
送信元	• 「宛先」ページ • 「ネットワーク」ページ	宛先 IP アドレスまたはネットワークに関連しているオフェンスの送信元 IP アドレスを指定します。送信元 IP アドレスに関する詳細を表示するには、表示されている IP アドレス、アセット名、または用語をクリックします。 単一の送信元 IP アドレスが指定されている場合、(使用可能な場合には) IP アドレスとアセット名が表示されます。IP アドレスまたはアセット名をクリックして、送信元 IP アドレスの詳細を表示することができます。複数の送信元 IP アドレスがある場合、このフィールドには「複数」が指定され、送信元 IP アドレスの数が示されます。
送信元	「ネットワーク別 - ローカル宛先のリストページ	宛先 IP アドレスに関連した送信元 IP アドレスの数を指定します。
開始 (Start)	「オフェンス」表	オフェンスに対してイベントまたはフローが最初に発生した日時を指定します。
開始日 (Start Date)	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	オフェンスに関連する最初のイベントまたはフローの日時を指定します。
状況 (Status)	「オフェンスのタイプ」が「ログ・ソース」の場合は、「オフェンスの送信元」表	このログ・ソースの状況を指定します。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
状況 (Status)	「オフェンス」表	オフェンスの状況を示すアイコンを表示します。状況アイコンには、以下のものがあります。 **「非アクティブのオフェンス」**。オフェンスは、最後のイベントを受信してから 5 日経つと非アクティブになります。すべてのオフェンスは、QRadar 製品ソフトウェアがアップグレードされると非アクティブになります。 非アクティブのオフェンスを再びアクティブにすることはできません。オフェンスについて新規イベントが検出されると、新規のオフェンスが作成され、オフェンスの保存期間が経過するまで非アクティブのオフェンスが保持されます。非アクティブのオフェンスに対して、保護、フォローアップ対象としてのフラグ付け、メモの追加、ユーザーへの割り当てを行うことができます。 「すべてのオフェンス」ページの**「非表示のオフェンス」**フラグは、そのオフェンスが非表示になっていることを示します。非表示のオフェンスを検索する場合、それらは「すべてのオフェンス」ページにのみ表示されます。ここで、それらのオフェンスには非表示のオフェンスであることを示すフラグが立てられています。詳しくは、オフェンスの非表示を参照してください。 **「ユーザー」**は、オフェンスがユーザーに割り当てられていることを示します。オフェンスがユーザーに割り当てられられている場合、そのオフェンスは、そのユーザーの「自分のオフェンス」ページに表示されます。詳しくは、ユーザーへのオフェンスの割り当てを参照してください。 **「保護」**は、指定したオフェンスが保存期間の経過後にデータベースから削除されないようにします。詳しくは、『オフェンスの保護』を参照してください。 **「クローズされたオフェンス」**は、そのオフェンスがクローズされていることを示します。詳しくは、『オフェンスのクローズ』を参照してください。
時刻	• 「最後の 10 件のイベント (Last 10 Events)」表 • 「最後の 10 件のイベント (アノマリ・イベント) (Last 10 Events (Anomaly Events))」表	正規化イベントで最初のイベントが検出された日時を指定します。この日時は、イベントを検出したデバイス別に示されます。
時刻	「上位 5 件の注釈」表	この注釈が作成された日時を指定します。
合計バイト数 (Total Bytes)	「最後の 10 件のフロー (Last 10 Flows)」表	フローの合計バイト数を指定します。
イベント/フローの総数	• 「上位 5 件のログ・ソース」表 • 「上位 5 件のユーザー」表	ログ・ソースまたはユーザーに関するイベントの総数を指定します。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
ユーザー (User)	• 「オフェンスのタイプ」が「送信元 IP」、「宛先 IP」、または「ユーザー名」の場合は、「オフェンスの送信元」表 • 「上位 5 件の送信元 IP」表 • 「上位 5 件の宛先 IP」表 • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「ネットワーク別 - ローカル宛先のリストページ	送信元 IP アドレスまたは宛先 IP アドレスに関連したユーザーを指定します。ユーザーが識別されない場合、このフィールドには「不明」が指定されます。
ユーザー名	「オフェンスのタイプ」が「ユーザー名」の場合は、「オフェンスの送信元」表	オフェンスを作成したイベントまたはフローに関連するユーザー名を指定します。 **注:** マウス・ポインターを「ユーザー名」パラメーターに合わせると、表示されるツールチップには、そのオフェンスを作成したイベントやフローに関連するユーザー名ではなく、「アセット」タブから得られる最近のユーザー名情報に関連したユーザー名が示されます。
ユーザー名	「直近 5 件のメモ」表	このメモを作成したユーザーを指定します。
ユーザー	• 「すべてのオフェンス」ページ • 「自分のオフェンス」ページ • 「送信元 IP 別 - オフェンスのリスト」ページ • 「ネットワーク別 - オフェンスのリスト」ページ • 「宛先 IP 別 - オフェンスのリスト」ページ	オフェンスに関連したユーザー名を指定します。オフェンスに複数のユーザー名が関連付けられている場合、このフィールドには「複数」が指定され、ユーザー名の数が示されます。ユーザーが識別されない場合、このフィールドには「不明」が指定されます。
次のオフェンスを表示します	• 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ	このページで表示するオフェンスをフィルターに掛けるには、このリスト・ボックスからオプションを選択します。すべてのオフェンスを表示したり、時刻範囲に基づいてオフェンスをフィルターに掛けたりすることができます。リスト・ボックスから、フィルター基準として使用したい時刻範囲を選択します。
脆弱性	「オフェンスのタイプ」が「送信元 IP」または「宛先 IP」の場合は、「オフェンスの送信元」表	送信元 IP アドレスまたは宛先 IP アドレスに関連する、識別された脆弱性の数を指定します。この値には、アクティブな脆弱性の数およびパッシブな脆弱性の数も含まれます。
脆弱性	「宛先 IP 別 - 送信元のリスト」ページ	送信元 IP アドレスに脆弱性があるかどうかを指定します。

表 14. オフェンスのパラメーター (続き)

パラメーター	ロケーション	説明
脆弱性	• 「上位 5 件の送信元 IP」表 • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「上位 5 件の宛先 IP」表 • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「ネットワーク別 - ローカル宛先のリストページ	送信元 IP アドレスまたは宛先 IP アドレスに脆弱性があるかどうかを指定します。
重み	• 「上位 5 件の送信元 IP」表 • 「上位 5 件の宛先 IP」表 • 「送信元 IP 別 - ローカル宛先のリスト」ページ • 「送信元 IP の詳細別 (By Source IP Details)」ページ • 「宛先 IP の詳細別 (By Destination IP Details)」ページ • 「宛先 IP 別 - 送信元のリスト」ページ • 「ネットワーク別 - 送信元のリスト」ページ • 「ネットワーク別 - ローカル宛先のリストページ • 「上位 5 件の注釈」表	送信元 IP アドレス、宛先 IP アドレス、または注釈の重みを指定します。IP アドレスの重みは「**アセット**」タブで割り当てられます。詳しくは、アセットの管理を参照してください。

第 5 章 ログ・アクティビティーの調査

イベントをリアルタイムでモニターおよび調査したり、拡張検索を実行したりできます。

「**ログ・アクティビティー**」タブを使用することにより、ログ・アクティビティー (イベント) をリアルタイムでモニターおよび調査したり、拡張検索を実行したりできます。

「ログ・アクティビティー」タブの概要

イベントは、ファイアウォールやルーター・デバイスなどのログ・ソースから取得されるレコードで、ネットワークやホスト上でのアクションを記述します。

「**ログ・アクティビティー**」タブは、オフェンスに関連するイベントを指定します。

「**ログ・アクティビティー**」タブを表示するには、権限が必要になります。

「ログ・アクティビティー」タブ・ツールバー

「ログ・アクティビティー」ツールバーから、いくつかのオプションにアクセスすることができます。

このツールバーを使用して、以下のオプションにアクセスすることができます。

表 15. 「ログ・アクティビティー」ツールバーのオプション

オプション	説明
検索	イベントに関する拡張検索を行うには、「**検索**」をクリックします。オプションは、以下のとおりです。 • **新規検索** - 新しいイベント検索を作成するには、このオプションを選択します。 • **検索の編集** - イベント検索を選択して編集するには、このオプションを選択します。 • **検索結果の管理** - 検索結果を表示および管理するには、このオプションを選択します。
クイック検索	このリスト・ボックスから、以前に保存した検索を実行することができます。「**クイック検索**」リスト・ボックスにオプションが表示されるのは、「**クイック検索に含める**」オプションが指定された検索条件が保存されている場合だけです。
フィルターの追加	現在の検索結果にフィルターを追加するには、「**フィルターの追加**」をクリックします。
条件の保存	現在の検索条件を保存するには、「**条件の保存**」をクリックします。

表 15. 「ログ・アクティビティー」ツールバーのオプション (続き)

オプション	説明
結果の保存	現在の検索結果を保存するには、「**結果の保存**」をクリックします。このオプションは、検索が完了するまで表示されません。このオプションは、ストリーム・モードでは使用不可になります。
キャンセル	進行中の検索を取り消すには、「**キャンセル**」をクリックします。このオプションは、ストリーム・モードでは使用不可になります。
フォールス・ポジティブ	「**フォールス・ポジティブ**」をクリックすると、「フォールス・ポジティブのチューニング」ウィンドウが開きます。このウィンドウを使用して、フォールス・ポジティブであることが分かっているイベントによってオフェンスが生成されないようにすることができます。 このオプションは、ストリーム・モードでは使用不可になります。フォールス・ポジティブのチューニングについては、フォールス・ポジティブのチューニングを参照してください。

表 15. 「ログ・アクティビティー」ツールバーのオプション (続き)

オプション	説明
ルール	「ルール」オプションは、ルールを表示するための権限を持っている場合のみ表示されます。 カスタムのイベント・ルールを構成するには、「**ルール**」をクリックします。オプションは、以下のとおりです。 • **ルール** - ルールを表示または作成するには、このオプションを選択します。ルールを表示する権限しか持っていない場合は、「ルール」ウィザードのサマリー・ページが表示されます。カスタム・ルールを保守する権限を持っている場合は、「ルール」ウィザードが表示され、ルールを編集することができます。アノマリ検出ルール・オプション (「しきい値ルールの追加」、「振る舞い型ルールの追加」、および「アノマリ・ルールの追加」) を有効にするには、集約された検索条件を保存する必要があります。これは、保存済み検索条件によって、必要なパラメーターが指定されるためです。 **注:** アノマリ検出ルール・オプションは、「**ログ・アクティビティー**」 > 「**カスタム・ルールの保守**」権限を持っている場合のみ表示されます。 • **しきい値ルールの追加** - しきい値ルールを作成するには、このオプションを選択します。しきい値ルールは、イベント・トラフィックをテストして、構成されているしきい値を超えるアクティビティーがないかどうかを調べます。しきい値は、QRadar によって収集されたすべてのデータに基づいて設定することができます。例えば、午前 8 時から午後 5 時までの間は 220 を超えるクライアントはサーバーにログインできないことを指定するしきい値ルールを作成した場合、221 番目のクライアントがログインしようとすると、このルールによってアラートが生成されます。 「**しきい値ルールの追加**」オプションを選択すると、しきい値ルールを作成するための適切なオプションが事前に指定された「ルール」ウィザードが表示されます。

表 15. 「ログ・アクティビティー」ツールバーのオプション (続き)

オプション	説明
ルール (続き)	• **振る舞い型ルールの追加** - 動作ルールを作成するには、このオプションを選択します。動作ルールは、イベント・トラフィックをテストして、異常なアクティビティー (新しいトラフィックや未知のトラフィックの存在など) がないかどうかを調べます。このようなアクティビティーには、トラフィックの突然の停止や、オブジェクトがアクティブになっている時間の割合の変化などがあります。 例えば、直近 5 分間のトラフィックの平均量を直近 1 時間のトラフィックの平均量と比較するための動作ルールを作成することができます。40% を超える変動があった場合、このルールによって応答が生成されます。 「**振る舞い型ルールの追加**」オプションを選択すると、動作ルールを作成するための適切なオプションが事前に指定された、「ルール」ウィザードが表示されます。 • **アノマリ・ルールの追加** - アノマリ・ルールを作成するには、このオプションを選択します。アノマリ・ルールは、イベント・トラフィックをテストして、アノマリなアクティビティー (新しいトラフィックや未知のトラフィックの存在など) がないかどうかを調べます。このようなアクティビティーとしては、トラフィックの突然の停止や、オブジェクトがアクティブになっている時間の割合の変化などがあります。 例えば、アジア地域とは通信しないネットワークのエリアが、アジア地域にあるホストとの通信を開始した場合、アノマリ・ルールによってアラートが生成されます。 「**アノマリ・ルールの追加**」オプションを選択すると、アノマリ・ルールを作成するための適切なオプションが事前に指定された「ルール」ウィザードが表示されます。

表 15. 「ログ・アクティビティー」ツールバーのオプション (続き)

オプション	説明
アクション	以下のアクションを実行するには、「**アクション**」をクリックします。 • **すべて表示 (Show All)** - 検索条件に対するフィルターをすべて削除して、フィルタリングされていないイベントをすべて表示するには、このオプションを選択します。 • **印刷** - ページに表示されているイベントを印刷するには、このオプションを選択します。 • **「XML にエクスポート」 > 「表示列」** - 「ログ・アクティビティー」タブに表示される列だけをエクスポートするには、このオプションを選択します。これは推奨されるオプションです。詳しくは、『イベントのエクスポート』を参照してください。 • **「XML にエクスポート」 > 「完全エクスポート (すべての列)」** - すべてのイベント・パラメーターをエクスポートするには、このオプションを選択します。完全エクスポートは、完了までに長時間かかります。詳しくは、イベントのエクスポートを参照してください。 • **「CSV にエクスポート」 >「表示列」** - 「ログ・アクティビティー」タブに表示される列だけをエクスポートするには、このオプションを選択します。これは推奨されるオプションです。詳しくは、イベントのエクスポートを参照してください。 • **「CSV にエクスポート」 > 「完全エクスポート (すべての列)」** - すべてのイベント・パラメーターをエクスポートするには、このオプションを選択します。完全エクスポートは、完了までに長時間かかります。詳しくは、イベントのエクスポートを参照してください。 • **削除** - 検索結果を削除するには、このオプションを選択します。詳しくは、検索結果の管理を参照してください。 • **通知** - 選択された検索の完了時に E メールで通知を受け取りたい場合には、このオプションを選択します。このオプションは、進行中の検索についてのみ有効になります。 **注: 「印刷」、「XML にエクスポート」、「CSV にエクスポート」**の各オプションは、ストリーム・モードの場合と、検索結果の一部を表示している場合は無効になります。
検索ツールバー	**拡張検索** 取得するフィールドを指定するための Ariel 照会言語 (AQL) の検索ストリングを入力するには、リスト・ボックスから「**拡張検索**」を選択します。 **クイック・フィルター (Quick Filter)** 単純な語句を使用してペイロードを検索するには、リスト・ボックスから「クイック・フィルター」を選択します。

表 15. 「ログ・アクティビティー」ツールバーのオプション (続き)

オプション	説明
表示 (View)	**「ログ・アクティビティー」**タブのデフォルトの表示は、リアルタイム・イベントのストリームです。**「表示」**リストには、指定の期間に発生したイベントも表示するオプションが用意されています。**「表示」**リストから指定する期間を選択した後、**「開始時刻」**フィールドおよび**「終了時刻」**フィールドで日時の値を変更することで、表示させる時間を変更することができます。

右クリック・メニューのオプション

「ログ・アクティビティー」タブのイベントを右クリックして、より詳しいイベント・フィルター情報にアクセスできます。

右クリック・メニュー・オプションには、以下のものがあります。

表 16. 右クリック・メニューのオプション

オプション	説明
フィルター対象 (Filter on)	このオプションを選択すると、選択したイベントで指定したパラメーターに従って、そのイベントをフィルターに掛けることができます。
フォールス・ポジティブ	このオプションを選択すると、「フォールス・ポジティブ」ウィンドウが開きます。このウィンドウを使用して、フォールス・ポジティブであることが知られているイベントによってオフェンスが生成されないようにチューニングすることができます。このオプションは、ストリーム・モードでは使用不可になります。フォールス・ポジティブのチューニングを参照してください。
その他のオプション (More options):	IP アドレスまたはユーザー名を調査するには、このオプションを選択します。IP アドレスの調査について詳しくは、『IP アドレスの調査』を参照してください。ユーザー名の調査について詳しくは、ユーザー名の調査を参照してください。 **注:** このオプションは、ストリーム・モードでは表示されません。
クイック・フィルター (Quick Filter)	フィルター操作により、選択内容に一致する項目または一致しない項目を抽出します。

ステータス・バー

イベントのストリーミングが発生している場合、ステータス・バーには 1 秒当たりに受信された結果の平均数が表示されます。

これは、コンソールがイベント・プロセッサーから正常に受信した結果の数です。この 1 秒当たりの結果の数値が 40 を超える場合、表示される結果は 40 のみで

す。残りの結果数は、結果バッファーに集計されます。状況情報をさらに表示するには、マウス・ポインターをステータス・バーの上に移動します。

イベントのストリーミングが発生していない場合、ステータス・バーには現在タブ上に表示されている検索結果の数、およびその検索結果の処理に要した時間が表示されます。

ログ・アクティビティーのモニター

デフォルトでは、「**ログ・アクティビティー**」タブには、ストリーム・モードでイベントが表示されます。これにより、イベントをリアルタイムで表示することができます。

ストリーム・モードについて詳しくは、ストリーミング・イベントの表示を参照してください。「**表示**」リスト・ボックスを使用して、イベントをフィルタリングするための別の時刻範囲を指定することができます。

デフォルトとして構成されている保存済み検索条件がある場合、「**ログ・アクティビティー**」タブにアクセスすると、その検索の結果が自動的に表示されます。検索条件の保存に関する詳細については、検索条件の保存を参照してください。

ストリーミング・イベントの表示

ストリーム・モードでは、システムに入るイベント・データを表示することができます。このモードでは、最後の 50 件のイベントを表示することで、現在のイベント・アクティビティーをリアルタイムで確認できます。

このタスクについて

ストリーム・モードを有効にする前に、「**ログ・アクティビティー**」タブまたは検索条件にフィルターを適用する場合、そのフィルターはストリーム・モードで保持されます。ただし、ストリーム・モードでは、グループ化されたイベントを含む検索はサポートされません。グループ化されたイベントまたはグループ化された検索条件でストリーム・モードを有効にすると、「**ログ・アクティビティー**」タブに正規化イベントが表示されます。正規化イベントの表示を参照してください。

イベントを選択して詳細を表示するか、アクションを実行する場合は、ストリーミングを一時停止してからイベントをダブルクリックする必要があります。ストリーミングが一時停止すると、最後の 1,000 件のイベントが表示されます。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. 「**表示**」リスト・ボックスから、「**リアルタイム (ストリーミング) (Real Time (streaming))**」を選択します。 ツールバー・オプションについては、表 4-1 を参照してください。ストリーム・モードで表示されるパラメーターについて詳しくは、表 4-7 を参照してください。
3. オプション。ストリーミング・イベントを一時停止または再生します。次のオプションのいずれかを選択してください。
   - イベント・レコードを選択するには、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。

- ストリーム・モードを再始動するには、「**再生 (Play)**」アイコンをクリックします。

正規化イベントの表示

イベントはロー・フォーマットで収集されてから、「**ログ・アクティビティー**」タブに表示するために正規化されます。

このタスクについて

正規化では、ロー・イベント・データを構文解析し、タブに関する読み取り可能な情報を表示するためのデータを準備します。イベントが正規化されると、システムは名前も正規化します。したがって、「**ログ・アクティビティー**」タブに表示される名前は、イベントで表示される名前と一致しない場合があります。

注: 表示する時間フレームを選択した場合は、時系列グラフが表示されます。時系列グラフの使用について詳しくは、時系列グラフの概要を参照してください。

「**ログ・アクティビティー**」タブには、正規化イベントの表示時に以下のパラメーターが表示されます。

表 17. 「ログ・アクティビティー」タブ - デフォルト (正規化) のパラメーター

パラメーター	説明
現在のフィルター	表の最上部に、検索結果に適用されるフィルターの詳細が表示されます。これらのフィルター値を消去するには、「**フィルターのクリア**」をクリックします。 **注:** このパラメーターはフィルターの適用後にのみ表示されます。
表示	リスト・ボックスから、フィルター対象の時刻範囲を選択できます。

表 17. 「ログ・アクティビティー」タブ - デフォルト (正規化) のパラメーター (続き)

パラメーター	説明
現在の統計	リアルタイム (ストリーミング) モードや過去 1 分間 (自動最新表示) モードでない場合は、次のような現在の統計が表示されます。 **注:** 統計を表示または非表示にする場合は、「**現在の統計**」の横にある矢印をクリックしてください。 • **合計結果数** - 検索条件に一致した結果の総数を示します。 • **検索されたデータ・ファイル** - 指定された期間内に検索されたデータ・ファイルの総数を示します。 • **検索された圧縮データ・ファイル** - 指定された期間内に検索された圧縮データ・ファイルの総数を示します。 • **索引ファイル数** - 指定された期間内に検索された索引ファイルの総数を示します。 • **期間** - 検索期間を示します。 **注:** 現在の統計はトラブルシューティングに役立ちます。イベントのトラブルシューティングについて、お客様サポートに問い合わせたときに、現在の統計情報の提供を求められる場合があります。
グラフ (Charts)	時間間隔とグループ・オプションで一致したレコードを表す構成可能グラフを表示します。表示対象からグラフを除外する場合は、「**グラフの非表示**」をクリックします。グラフは、「最後の間隔 (自動最新表示) (Last Interval (auto refresh))」以上の時間フレーム、および表示するグループ・オプションを選択した後にのみ表示されます。グラフの構成について詳しくは、グラフの管理を参照してください。 **注:** ブラウザーとして Mozilla Firefox を使用し、広告ブロッカー・ブラウザー拡張機能がインストールされている場合、グラフは表示されません。グラフを表示するには、広告ブロッカー・ブラウザー拡張機能を削除する必要があります。詳しくは、ご使用のブラウザーの資料を参照してください。
「オフェンス」アイコン	このイベントに関連付けられているオフェンスの詳細を表示する場合は、このアイコンをクリックします。詳しくは、『グラフの管理』を参照してください。 **注:** 製品によっては、このアイコンを使用できない場合があります。IBM Security QRadar SIEMが必要です。

表 17. 「ログ・アクティビティー」タブ - デフォルト (正規化) のパラメーター (続き)

パラメーター	説明
開始時刻	ログ・ソースによって QRadar に報告された最初のイベントの時刻を示します。
イベント名	イベントの正規化された名前を示します。
ログ・ソース	イベントを発生させたログ・ソースを示します。このイベントに関連付けられたログ・ソースが複数ある場合、このフィールドには「複数」という語とログ・ソースの数が指定されます。
イベント数	この正規化イベントにバンドルされているイベントの総数を示します。イベントは、同じ送信元および宛先 IP アドレスの同じタイプの多数のイベントが短時間で検出される場合にバンドルされます。
時刻	QRadar がイベントを受信した日時を示します。
下位カテゴリー	このイベントに関連付けられている下位カテゴリーを示します。 イベント・カテゴリーについて詳しくは、*IBM Security QRadar SIEM 管理ガイド* を参照してください。
送信元 IP	このイベントの送信元 IP アドレスを指定します。
送信元ポート	イベントの送信元ポートを指定します。
宛先 IP	このイベントの宛先 IP アドレスを指定します。
宛先ポート	イベントの宛先ポートを指定します。
ユーザー名	このイベントに関連付けられているユーザー名を示します。多くの場合、ユーザー名は認証関連イベントで使用できます。ユーザー名を使用できない他のすべてのタイプのイベントでは、このフィールドに N/A が示されます。
マグニチュード	このイベントのマグニチュードを示します。変数には、信頼性、関連性、および重大度が含まれます。マウス・ポインターをマグニチュードを示すバーに合わせると、値および計算されたマグニチュードが表示されます。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. 「**表示**」リスト・ボックスから、「**デフォルト (正規化)**」を選択します。
3. 「**表示**」リスト・ボックスから、表示する時間フレームを選択します。
4. 「**一時停止**」アイコンをクリックして、ストリーミングを一時停止します。

5. さらに詳細に表示するイベントをダブルクリックします。詳しくは、『イベントの詳細』を参照してください。

ロー・イベントの表示

ロー・イベント・データ (ログ・ソースからの解析されていないイベント・データ) を表示することができます。

このタスクについて

ロー・イベント・データの表示時に、「**ログ・アクティビティー**」タブには各イベントの以下のパラメーターが示されます。

表 18. ロー・イベントのパラメーター

パラメーター	説明
現在のフィルター	表の最上部に、検索結果に適用されるフィルターの詳細が表示されます。これらのフィルター値を消去するには、「**フィルターのクリア**」をクリックします。 **注:** このパラメーターはフィルターの適用後にのみ表示されます。
表示	リスト・ボックスから、フィルター対象の時刻範囲を選択できます。
現在の統計	リアルタイム (ストリーミング) モードや過去 1 分間 (自動最新表示) モードでない場合は、次のような現在の統計が表示されます。 **注:** 統計を表示または非表示にする場合は、「**現在の統計**」の横にある矢印をクリックしてください。 • **合計結果数** - 検索条件に一致した結果の総数を示します。 • **検索されたデータ・ファイル** - 指定された期間内に検索されたデータ・ファイルの総数を示します。 • **検索された圧縮データ・ファイル** - 指定された期間内に検索された圧縮データ・ファイルの総数を示します。 • **索引ファイル数** - 指定された期間内に検索された索引ファイルの総数を示します。 • **期間** - 検索期間を示します。 **注:** Current®統計はトラブルシューティングに役立ちます。イベントのトラブルシューティングについて、お客様サポートに問い合わせたときに、現在の統計情報の提供を求められる場合があります。

表 18. ロー・イベントのパラメーター (続き)

パラメーター	説明
グラフ (Charts)	時間間隔とグループ・オプションで一致したレコードを表す構成可能グラフを表示します。表示対象からグラフを除外する場合は、「**グラフの非表示**」をクリックします。グラフは、「最後の間隔 (自動最新表示) (Last Interval (auto refresh))」以上の時間フレーム、および表示するグループ・オプションを選択した後にのみ表示されます。 **注:** ブラウザーとして Mozilla Firefox を使用し、広告ブロッカー・ブラウザー拡張機能がインストールされている場合、グラフは表示されません。グラフを表示するには、広告ブロッカー・ブラウザー拡張機能を削除する必要があります。詳しくは、ご使用のブラウザーの資料を参照してください。
「オフェンス」アイコン	このイベントに関連付けられているオフェンスの詳細を表示する場合は、このアイコンをクリックします。
開始時刻	ログ・ソースによって QRadar に報告された最初のイベントの時刻を示します。
ログ・ソース	イベントを発生させたログ・ソースを示します。このイベントに関連付けられたログ・ソースが複数ある場合、このフィールドには「複数」という語とログ・ソースの数が指定されます。
ペイロード (Payload)	元のイベント・ペイロード情報を UTF-8 フォーマットで指定します。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. 「**表示**」リスト・ボックスから、「**ロー・イベント (Raw Events)**」を選択します。
3. 「**表示**」リスト・ボックスから、表示する時間フレームを選択します。
4. さらに詳細に表示するイベントをダブルクリックします。イベントの詳細を参照してください。

グループ化されたイベントの表示

「**ログ・アクティビティー**」タブを使用して、さまざまなオプションごとにグループ化されているイベントを表示することができます。「**表示**」リスト・ボックスから、イベントのグループ化に使用するパラメーターを選択します。

このタスクについて

「表示」リスト・ボックスはストリーム・モードでは表示されません。これは、ストリーム・モードではグループ化されたイベントがサポートされないためです。グループ化されていない検索条件を使用してストリーム・モードに入った場合は、このオプションが表示されます。

「表示」リスト・ボックスには以下のオプションが示されます。

表 19. グループ化されたイベントのオプション

グループ・オプション	説明
下位カテゴリー	イベントの下位カテゴリー別にグループ化されているイベントのサマリー・リストを表示します。 カテゴリーについて詳しくは、*IBM Security QRadar SIEM 管理ガイド* を参照してください。
イベント名	イベントの正規化された名前別にグループ化されているイベントのサマリー・リストを表示します。
宛先 IP	イベントの宛先 IP アドレス別にグループ化されているイベントのサマリー・リストを表示します。
宛先ポート	イベントの宛先ポート・アドレス別にグループ化されているイベントのサマリー・リストを表示します。
送信元 IP	イベントの送信元 IP アドレス別にグループ化されているイベントのサマリー・リストを表示します。
カスタム・ルール (Custom Rule)	関連するカスタム・ルール別にグループ化されているイベントのサマリー・リストを表示します。
ユーザー名	イベントに関連付けられているユーザー名別にグループ化されているイベントのサマリー・リストを表示します。
ログ・ソース	QRadar にイベントを送信したログ・ソース別にグループ化されているイベントのサマリー・リストを表示します。
上位カテゴリー	イベントの上位カテゴリー別にグループ化されているイベントのサマリー・リストを表示します。
ネットワーク	イベントに関連付けられているネットワーク別にグループ化されているイベントのサマリー・リストを表示します。
送信元ポート	イベントの送信元ポート・アドレス別にグループ化されているイベントのサマリー・リストを表示します。

「**表示**」リスト・ボックスからオプションを選択すると、データの列レイアウトは選択したグループ・オプションよって決まります。イベント表内の各行はイベント・グループを表します。「**ログ・アクティビティー**」タブには、各イベント・グループの以下の情報が示されます。

表 20. グループ化されたイベントのパラメーター

パラメーター	**説明**
グループ化の基準	検索がグループ化されるパラメーターを指定します。
現在のフィルター	表の最上部に、検索結果に適用されるフィルターの詳細が表示されます。これらのフィルター値を消去するには、「**フィルターのクリア**」をクリックします。
表示	リスト・ボックスから、フィルター対象の時刻範囲を選択します。
現在の統計	リアルタイム (ストリーミング) モードや過去 1 分間 (自動最新表示) モードでない場合は、次のような現在の統計が表示されます。 **注:** 統計を表示または非表示にする場合は、「**現在の統計**」の横にある矢印をクリックしてください。 • **合計結果数** - 検索条件に一致した結果の総数を示します。 • **検索されたデータ・ファイル** - 指定された期間内に検索されたデータ・ファイルの総数を示します。 • **検索された圧縮データ・ファイル** - 指定された期間内に検索された圧縮データ・ファイルの総数を示します。 • **索引ファイル数** - 指定された期間内に検索された索引ファイルの総数を示します。 • **期間** - 検索期間を示します。 **注:** 現在の統計はトラブルシューティングに役立ちます。イベントのトラブルシューティングについて、お客様サポートに問い合わせたときに、現在の統計情報の提供を求められる場合があります。

表 20. グループ化されたイベントのパラメーター (続き)

パラメーター	説明
グラフ (Charts)	時間間隔とグループ・オプションで一致したレコードを表す構成可能グラフを表示します。表示対象からグラフを除外する場合は、「**グラフの非表示**」をクリックします。 各グラフには凡例が表示されます。この凡例は、グラフ・オブジェクトとそれが表すパラメーターとの関連付けを行うための、参照用の表示情報です。凡例機能を使用して、以下のアクションを実行できます。 • 凡例項目にマウス・ポインターを移動して、示されるパラメーターの詳細を表示する。 • 凡例項目を右クリックして、その項目をさらに詳しく調べる。 • 凡例項目をクリックして、グラフで項目を非表示にする。凡例項目を再度クリックすると、非表示項目が表示されます。対応するグラフ項目をクリックして、項目の表示と非表示を切り替えることもできます。 • グラフ表示から凡例を除外する場合は、「**凡例 (Legend)**」をクリックする。 **注:** グラフは、「最後の間隔 (自動最新表示) (Last Interval (auto refresh))」以上の時間フレーム、および表示するグループ・オプションを選択した後にのみ表示されます。 **注:** ブラウザーとして Mozilla Firefox を使用し、広告ブロッカー・ブラウザー拡張機能がインストールされている場合、グラフは表示されません。グラフを表示するには、ブラウザー拡張機能の広告ブロッカーを削除する必要があります。詳しくは、ご使用のブラウザーの資料を参照してください。
送信元 IP (固有の数)	このイベントに関連付けられている送信元 IP アドレスを指定します。このイベントに関連付けられている IP アドレスが複数ある場合、このフィールドには「複数」という用語と IP アドレスの数が指定されます。
宛先 IP (固有の数) (Destination IP (Unique Count))	このイベントに関連付けられている宛先 IP アドレスを指定します。このイベントに関連付けられている IP アドレスが複数ある場合、このフィールドには「複数」という用語と IP アドレスの数が指定されます。

表 20. グループ化されたイベントのパラメーター (続き)

パラメーター	説明
宛先ポート (固有の数)	このイベントに関連付けられている宛先ポートを指定します。このイベントに関連付けられているポートが複数ある場合、このフィールドには「複数」という用語とポートの数が指定されます。
イベント名	イベントの正規化された名前を示します。
ログ・ソース (合計)	このイベントを QRadar に送信したログ・ソースを指定します。このイベントに関連付けられたログ・ソースが複数ある場合、このフィールドには「複数」という語とログ・ソースの数が指定されます。
上位カテゴリー (固有の数) (High Level Category (Unique Count))	このイベントの上位カテゴリーを指定します。このイベントに関連付けられているカテゴリーが複数ある場合、このフィールドには「複数」という用語とカテゴリーの数が指定されます。 カテゴリーについて詳しくは、*IBM Security QRadar Log Manager Administration Guide* を参照してください。
下位カテゴリー (固有の数) (Low Level Category (Unique Count))	このイベントの下位カテゴリーを指定します。このイベントに関連付けられているカテゴリーが複数ある場合、このフィールドには「複数」という用語とカテゴリーの数が指定されます。
プロトコル (固有の数) (Protocol (Unique Count))	このイベントに関連付けられているプロトコル ID を指定します。このイベントに関連付けられているプロトコルが複数ある場合、このフィールドには「複数」という用語とプロトコル ID の数が指定されます。
ユーザー名 (固有の数) (Username (Unique Count))	このイベントに関連付けられているユーザー名 (使用可能な場合) を指定します。このイベントに関連付けられているユーザー名が複数ある場合、このフィールドには「複数」という用語とユーザー名の数が指定されます。
マグニチュード (最大) (Magnitude (Maximum))	グループ化されたイベントに対して計算された最大マグニチュードを示します。マグニチュードの計算に使用される変数には、信頼性 (credibility)、関連性 (relevance)、および重大度 (severity) が含まれます。信頼性 (credibility)、関連性 (relevance)、および重大度 (severity) について詳しくは、用語集を参照してください。

表 20. グループ化されたイベントのパラメーター (続き)

パラメーター	説明
イベント数 (合計) (Event Count (Sum))	この正規化イベントにバンドルされているイベントの総数を示します。イベントは、同じ送信元および宛先 IP アドレスの同じタイプの多数のイベントが短時間で検出される場合にバンドルされます。
数	このイベント・グループ内の正規化イベントの総数を指定します。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. 「**表示**」リスト・ボックスから、表示する時間フレームを選択します。
3. 「表示」リスト・ボックスから、イベントをグループ化するパラメーターを選択します。表 2 を参照してください。イベント・グループがリストされます。イベント・グループについて詳しくは、表 1 を参照してください。
4. グループの「イベントのリスト」ページを表示するには、調査対象のイベント・グループをダブルクリックします。「イベントのリスト」ページでは、「**ログ・アクティビティー**」タブに定義されている可能性のあるグラフ構成は保持されません。「イベントのリスト」ページのパラメーターについて詳しくは、表 1 を参照してください。
5. イベントの詳細を表示するには、調査対象のイベントをダブルクリックします。イベントについて詳しくは、表 2 を参照してください。

イベントの詳細

ストリーム・モードやイベント・グループなどの各種モードでイベントのリストを表示することができます。どのモードでイベントを表示する場合でも、単一のイベントの詳細を探して表示することができます。

「イベントの詳細 (Event Details)」ページには、以下の情報が表示されます。

表 21. イベントの詳細

パラメーター	説明
イベント名	イベントの正規化された名前を示します。
下位カテゴリー	このイベントの下位カテゴリーを指定します。 カテゴリーについて詳しくは、*IBM Security QRadar SIEM 管理ガイド* を参照してください。
イベントの説明	イベントの説明を指定します (使用可能な場合)。
マグニチュード	このイベントのマグニチュードを示します。マグニチュードについて詳しくは、用語集を参照してください。
関連性	このイベントの関連性を指定します。関連性について詳しくは、用語集を参照してください。

表 21. イベントの詳細 (続き)

パラメーター	説明
重大度	このイベントの重大度を指定します。重大度について詳しくは、用語集を参照してください。
信頼性	このイベントの信頼性を指定します。信頼性について詳しくは、用語集を参照してください。
ユーザー名	このイベントに関連付けられているユーザー名 (使用可能な場合) を指定します。
開始時刻	このイベントをログ・ソースから受け取った時刻を指定します。
保管時刻 (Storage Time)	このイベントが QRadar データベースに保管された時刻を指定します。
ログ・ソースの時刻	イベント・ペイロードのログ・ソースで報告されたシステム時刻を指定します。
アノマリ検出情報: このペインは、このイベントがアノマリ検出ルールによって生成された場合のみ表示されます。「**アノマリ**」アイコンをクリックすると、アノマリ検出ルールによってこのイベントが生成される原因となった保存済みの検索結果が表示されます。	
ルールの説明	このイベントを生成したアノマリ検出ルールを指定します。
アノマリの説明 (Anomaly Description)	アノマリ検出ルールによって検出されたアノマリな動作の説明を指定します。
アラート値アノマリ (Anomaly Alert Value)	アノマリ・アラート値を指定します。
送信元および宛先の情報	
送信元 IP	このイベントの送信元 IP アドレスを指定します。
宛先 IP	このイベントの宛先 IP アドレスを指定します。
送信元アセット名	イベント・ソースのユーザー定義アセット名を指定します。アセットについて詳しくは、『アセットの管理』を参照してください。
宛先アセット名	イベント宛先のユーザー定義アセット名を指定します。アセットについて詳しくは、『アセットの管理』を参照してください。
送信元ポート	このイベントの送信元ポートを指定します。
宛先ポート	このイベントの宛先ポートを指定します。
NAT 前の送信元 IP (Pre NAT Source IP)	ネットワーク・アドレス変換 (NAT) 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用される前の送信元 IP アドレスが指定されます。NAT は、あるネットワーク内の IP アドレスを、別のネットワーク内の異なる IP アドレスに変換します。

表 21. イベントの詳細 (続き)

パラメーター	説明
NAT 前の宛先 IP (Pre NAT Destination IP)	NAT 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用される前の宛先 IP アドレスが指定されます。
NAT 前の送信元ポート	NAT 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用される前の送信元ポートが指定されます。
NAT 前の宛先ポート (Pre NAT Destination Port)	NAT 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用される前の宛先ポートが指定されます。
NAT 後の送信元 IP (Post NAT Source IP)	NAT 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用された後の送信元 IP アドレスが指定されます。
NAT 後の宛先 IP (Post NAT Destination IP)	NAT 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用された後の宛先 IP アドレスが指定されます。
NAT 後の送信元ポート	NAT 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用された後の送信元ポートが指定されます。
NAT 後の宛先ポート (Post NAT Destination Port)	NAT 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用された後の宛先ポートが指定されます。
NAT 後の送信元ポート	NAT 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用された後の送信元ポートが指定されます。
NAT 後の宛先ポート (Post NAT Destination Port)	NAT 対応のファイアウォールまたは他のデバイスの場合、このパラメーターにより、NAT 値が適用された後の宛先ポートが指定されます。
IPv6 送信元	このイベントの送信元 IPv6 アドレスを指定します。
IPv6 宛先 (IPv6 Destination)	このイベントの宛先 IPv6 アドレスを指定します。
送信元 MAC	このイベントの送信元 MAC アドレスを指定します。
宛先 MAC	このイベントの宛先 MAC アドレスを指定します。
ペイロード情報	

表 21. イベントの詳細 (続き)

パラメーター	説明
ペイロード (Payload)	このイベントからのペイロードの内容を指定します。このフィールドには、ペイロードを表示するための以下の 3 つのタブが用意されています。 • Universal Transformation Format (UTF): 「UTF」をクリックします。 • 16 進数 (Hexadecimal): 「HEX」をクリックします。 • Base64: 「Base64」をクリックします。
追加情報	
プロトコル	このイベントに関連するプロトコルを指定します。
QID	このイベントの QID を指定します。それぞれのイベントは、固有の QID を持っています。QID のマッピングについて詳しくは、イベント・マッピングの変更を参照してください。
ログ・ソース	このイベントを QRadar に送信したログ・ソースを指定します。このイベントに関連付けられたログ・ソースが複数ある場合、このフィールドには「複数」という語とログ・ソースの数が指定されます。
イベント数	この正規化イベントにバンドルされているイベントの総数を示します。イベントは、同じ送信元および宛先 IP アドレスの同じタイプの多数のイベントが短時間で検出される場合にバンドルされます。
カスタム・ルール	このイベントに一致するカスタム・ルールを指定します。
部分的に一致するカスタム・ルール (Custom Rules Partially Matched)	このイベントに部分的に一致するカスタム・ルールを指定します。
注釈	このイベントの注釈を指定します。注釈は、テキスト記述です。ルールは、ルールの応答の一部として、注釈をイベントに自動的に追加することができます。
「アイデンティティー情報」 - QRadar は、アイデンティティー情報をログ・ソース・メッセージから収集します (アイデンティティー情報が使用可能な場合)。アイデンティティー情報は、ネットワーク上のアセットに関する追加の詳細情報を提供します。QRadar に送信されたログ・メッセージに、IP アドレスと、ユーザー名または MAC アドレスのいずれか (あるいはその両方) が含まれている場合のみ、ログ・ソースによってアイデンティティー情報が生成されます。必ずしもすべてのログ・ソースでアイデンティティー情報が生成されるわけではありません。ID とアセットについて詳しくは、アセットの管理を参照してください。	
ID ユーザー名 (Identity Username)	このイベントに関連するアセットのユーザー名を指定します。

表 21. イベントの詳細 (続き)

パラメーター	説明
ID IP (Identity IP)	このイベントに関連するアセットの IP アドレスを指定します。
ID NetBIOS 名 (Identity Net Bios Name)	このイベントに関連するアセットの Network Base Input/Output System (Net Bios) 名を指定します。
「**ID 拡張 (Identity Extended)**」フィールド	このイベントに関連するアセットについての追加情報を指定します。このフィールドの内容は、ユーザー定義のテキストです。このフィールドの内容は、ネットワーク上の、アイデンティティー情報を提供する使用可能なデバイスによって異なります。例としては、デバイスの物理ロケーション、関連ポリシー、ネットワーク・スイッチ、ポート名などがあります。
ID を持つ (フラグ) (Has Identity (Flag))	QRadar によって、このイベントに関連するアセットについてのアイデンティティー情報を収集した場合に、True を指定します。 アイデンティティー情報を送信するデバイスについては、「*IBM Security QRadar DSM Configuration Guide*」を参照してください。
ID ホスト名 (Identity Host Name)	このイベントに関連するアセットのホスト名を指定します。
ID MAC (Identity MAC)	このイベントに関連するアセットの MAC アドレスを指定します。
ID グループ名 (Identity Group Name)	このイベントに関連するアセットのグループ名を指定します。

「イベントの詳細 (Event details)」ツールバー

「イベントの詳細 (Event details)」ツールバーには、イベントの詳細を表示するためのいくつかの機能が用意されています。

「**イベントの詳細 (event details)**」ツールバーには、以下の機能が用意されています。

表 22. 「イベントの詳細 (event details)」ツールバー

イベント・リストに戻る (Return to Events List)	「**戻る (Return)**」をクリックすると、「**イベント・リスト (Events List)**」がイベントのリストに戻ります。
オフェンス	「**オフェンス**」をクリックすると、そのイベントに関連するオフェンスが表示されます。

表 22. 「イベントの詳細 (event details)」ツールバー (続き)

アノマリ	**「アノマリ」**をクリックすると、アノマリ検出ルールによってこのイベントが生成される原因となった保存済みの検索結果が表示されます。 **注:** このアイコンは、このイベントがアノマリ検出ルールによって生成された場合のみ表示されます。
イベントのマップ	**「イベントのマップ」**をクリックすると、イベントのマッピングを編集することができます。詳しくは、イベント・マッピングの変更を参照してください。
フォールス・ポジティブ	フォールス・ポジティブ・イベントからオフェンスが生成されないように QRadar をチューニングするには、**「フォールス・ポジティブ」**をクリックします。
プロパティーの抽出	選択されたイベントからカスタム・イベント・プロパティーを作成するには、**「プロパティーの抽出」**をクリックします。
前へ	**「前へ」**をクリックすると、イベント・リスト内の直前のイベントが表示されます。
次へ	**「次へ」**をクリックすると、イベント・リスト内の次のイベントが表示されます。
PCAP データ	**注:** このオプションは、QRadar コンソールが Juniper JunOS Platform DSM と統合するように構成されている場合のみ表示されます。PCAP データの管理について詳しくは、PCAP データの管理を参照してください。 • **「PCAP 情報の表示」** - PCAP 情報を表示するには、このオプションを選択します。詳しくは、PCAP 情報の表示を参照してください。 • **「PCAP ファイルのダウンロード」** - PCAP ファイルをデスクトップ・システムにダウンロードするには、このオプションを選択します。詳しくは、デスクトップ・システムへの PCAP ファイルのダウンロードを参照してください。
印刷	イベントの詳細を印刷するには、**「印刷」**をクリックします。

関連するオフェンスの表示

「ログ・アクティビティー」タブから、イベントに関連付けられているオフェンスを表示することができます。

このタスクについて

イベントがルールと一致する場合は、「**オフェンス**」タブでオフェンスを生成できます。

ルールについて詳しくは、*IBM Security QRadar SIEM 管理ガイド* を参照してください。

「**ログ・アクティビティー**」タブからオフェンスを表示する際に、判定機能により、選択されたイベントに関連付けられているオフェンスがまだディスクに保存されていないか、データベースからオフェンスがパージされている場合は、オフェンスが表示されない可能性があります。このような場合は、システムから通知されます。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. オプション。イベントをストリーム・モードで表示している場合は、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。
3. 調査対象のイベントの横にある「**オフェンス**」アイコンをクリックします。
4. 関連するオフェンスを表示します。

イベントのマッピングの変更

正規化されたイベントまたはロー・イベントを上位または下位のカテゴリー (QID) に手動でマッピングできます。

始める前に

この手動アクションは、不明なログ・ソース・イベントを適切にカテゴリー化して処理できるよう、それを既知の QRadar イベントにマッピングする際に使用されます。

このタスクについて

正規化する目的で、QRadar はログ・ソースのイベントを上位および下位のカテゴリーに自動的にマッピングします。

イベント・カテゴリーについて詳しくは、*IBM Security QRadar SIEM 管理ガイド* を参照してください。

システムがカテゴリー化できないログ・ソースからイベントを受信する場合、そのイベントは不明とカテゴリー化されます。このようなイベントには以下のものがあり、いくつかの理由で発生します。

- **ユーザー定義のイベント** - Snort など一部のログ・ソースでは、ユーザー定義のイベントを作成できます。
- **新規イベントまたは古いイベント** - ベンダーのログ・ソースは、 QRadar がサポートしていない新しいイベントをサポートする保守リリースで、そのソフトウェアを更新する可能性があります。

注: 上位レベルのカテゴリーが SIM 監査であるか、ログ・ソース・タイプが Simple Object Access Protocol (SOAP) である場合は、イベントの「**イベントのマップ**」アイコンが無効になります。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. オプション。イベントをストリーム・モードで表示している場合は、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。
3. マッピングするイベントをダブルクリックします。
4. 「**イベントのマップ**」をクリックします。
5. このイベントにマップする QID がわかっている場合、「**QID を入力 (Enter QID)**」フィールドに QID を入力します。
6. このイベントにマップする QID がわかっていない場合、以下のようにして特定の QID を検索することができます。
   a. 次のオプションのいずれかを選択してください。カテゴリーで QID を検索するには、「上位カテゴリー」リスト・ボックスから上位カテゴリーを選択します。 カテゴリーで QID を検索するには、「下位カテゴリー」リスト・ボックスから下位カテゴリーを選択します。 ログ・ソース・タイプで QID を検索するには、「ログ・ソース・タイプ」リスト・ボックスからログ・ソース・タイプを選択します。 名前で QID を検索するには、「QID/名前」フィールドに名前を入力します。
   b. 「**検索**」をクリックします。
   c. このイベントに関連付ける「**QID**」を選択します。
7. 「**OK**」をクリックします。

フォールス・ポジティブのチューニング

フォールス・ポジティブのチューニング機能を使用して、フォールス・ポジティブのイベントでオフェンスが作成されないようにすることができます。

始める前に

フォールス・ポジティブのイベントは、「イベント・リスト (event list)」または「イベントの詳細 (event details)」ページからチューニングできます。

このタスクについて

フォールス・ポジティブのイベントは、「イベント・リスト (event list)」または「イベントの詳細 (event details)」ページからチューニングできます。

フォールス・ポジティブをチューニングするためにカスタマイズされたルールを作成するには適切な権限が必要です。

ロールの詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

フォールス・ポジティブについて詳しくは、用語集を参照してください。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. オプション。イベントをストリーム・モードで表示している場合は、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。
3. チューニングするイベントを選択します。
4. 「**フォールス・ポジティブ**」をクリックします。
5. 「フォールス・ポジティブ」ウィンドウの「イベント/フロー・プロパティー」ペインで、以下のオプションのいずれかを選択します。
   - <イベント> の特定のイベント QID を持つイベント/フロー (Event/Flow(s) with a specific QID of <Event>)
   - <イベント> の下位カテゴリーを持つすべてのイベント/フロー (Any Event/Flow(s) with a low-level category of <Event>)
   - <イベント> の高位カテゴリーを持つすべてのイベント/フロー (Any Event/Flow(s) with a high-level category of <Event>)
6. 「トラフィックの方向」ペインで、以下のオプションのいずれかを選択します。
   - <送信元 IP アドレス> から <宛先 IP アドレス>
   - <送信元 IP アドレス> から任意の宛先へ
   - 任意の送信元から <宛先 IP アドレス> へ
   - 任意の送信元から任意の宛先へ
7. 「**チューニング (Tune)**」をクリックします。

PCAP データ

QRadar コンソールが Juniper JunOS Platform DSM と統合するように構成されている場合、Juniper SRX-Series サービス・ゲートウェイ・ログ・ソースからパケット・キャプチャー (PCAP) を受信して処理し、データを保管することができます。

Juniper JunOS Platform DSM について詳しくは、「*IBM Security QRadar DSM Configuration Guide*」を参照してください。

「PCAP データ」列の表示

「**PCAP データ**」列は、デフォルトでは「**ログ・アクティビティー**」タブに表示されません。検索条件を作成する際に、「列定義」ペインで「**PCAP データ**」列を選択する必要があります。

始める前に

「**ログ・アクティビティー**」タブに PCAP データを表示するには、PCAP と Syslog を組み合わせたプロトコルを指定して Juniper SRX シリーズ・サービス・ゲートウェイ・ログ・ソースを構成する必要があります。ログ・ソース・プロトコルの構成について詳しくは、*Managing Log Sources Guide* を参照してください。

このタスクについて

「**PCAP データ**」列を含む検索を実行すると、イベントに PCAP データがある場合に、検索結果の「**PCAP データ**」列にアイコンが表示されます。「**PCAP**」アイコ

ンを使用して、PCAP データを表示するか、または **PCAP** ファイルをデスクトップ・システムにダウンロードできます。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. 「**検索**」リスト・ボックスから、「**新規検索**」を選択します。
3. オプション。PCAP データがあるイベントを検索するには、次の検索条件を構成します。
   a. 最初のリスト・ボックスから、「**PCAP データ**」を選択します。
   b. 2 番目のリスト・ボックスから、「**次と等しい (Equals)**」を選択します。
   c. 3 番目のリスト・ボックスから、「**True**」を選択します。
   d. 「**フィルターの追加**」をクリックします。
4. 「**PCAP データ**」列が含まれるように列定義を構成します。
   a. 「列定義」ペインの「**使用可能な列**」リストで、「**PCAP データ**」をクリックします。
   b. 下部のアイコン・セットにある「**列の追加**」アイコンをクリックして、「**PCAP データ**」列を「**列**」リストに移動します。
   c. オプション。上部のアイコン・セットにある「**列の追加**」アイコンをクリックして、「**PCAP データ**」列を「**グループ化の基準**」リストに移動します。
5. 「**フィルター (Filter)**」をクリックします。
6. オプション。イベントをストリーム・モードで表示している場合は、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。
7. 調査するイベントをダブルクリックします。

次のタスク

PCAP データの表示とダウンロードについて詳しくは、以下のセクションを参照してください。

- PCAP 情報の表示
- デスクトップ・システムへの PCAP ファイルのダウンロード

PCAP 情報の表示

「**PCAP データ**」ツールバー・メニューから、PCAP ファイルの読み取り可能バージョンのデータを表示したり、デスクトップ・システムに PCAP ファイルをダウンロードすることができます。

始める前に

PCAP 情報を表示する前に、「**PCAP データ**」列を表示する検索を実行するか選択する必要があります。

このタスクについて

PCAP データを表示する前に、ユーザー・インターフェースで表示する PCAP ファイルを取得する必要があります。ダウンロード・プロセスに長時間かかる場合は、「PCAP パケット情報のダウンロード中 (Downloading PCAP Packet information)」

ウィンドウが表示されます。ほとんどの場合、ダウンロード・プロセスは迅速に行われるため、このウィンドウは表示されません。

ファイルが取得されると、ポップアップ・ウィンドウに読み取り可能なバージョンの PCAP ファイルが示されます。ウィンドウに表示される情報を読み取ったり、デスクトップ・システムに情報をダウンロードすることができます。

手順

1. 調査対象のイベントについて、以下のいずれかのオプションを選択します。
   - イベントを選択して、「**PCAP**」アイコンをクリックします。
   - イベントの「**PCAP**」アイコンを右クリックして、「**その他のオプション**」 > 「**PCAP 情報の表示**」を選択します。
   - 調査対象のイベントをダブルクリックして、イベントの詳細ツールバーから「**PCAP データ**」 > 「**PCAP 情報の表示**」を選択します。
2. デスクトップ・システムに情報をダウンロードする場合は、以下のいずれかのオプションを選択します。
   - 外部アプリケーションで使用される元の PCAP ファイルをダウンロードする場合は、「**PCAP ファイルのダウンロード (Download PCAP File)**」をクリックします。
   - .TXT フォーマットで PCAP 情報をダウンロードする場合は、「**PCAP テキストのダウンロード (Download PCAP Text)**」をクリックします。
3. 次のオプションのいずれかを選択してください。
   - すぐにファイルを開いて表示する場合は、「**アプリケーションから開く (Open with)**」オプションを選択し、リスト・ボックスからアプリケーションを選択します。
   - リストを保存する場合は、「**ファイルの保存 (Save File)**」オプションを選択します。
4. 「**OK**」をクリックします。

デスクトップ・システムへの PCAP ファイルのダウンロード

PCAP ファイルを、保管のため、または他のアプリケーションで使用するために、デスクトップ・システムにダウンロードすることができます。

始める前に

PCAP 情報を表示するには、「PCAP データ」列を表示する検索を実行または選択する必要があります。『「**PCAP データ」列の表示**』を参照してください。

手順

1. 調査対象のイベントについて、以下のいずれかのオプションを選択します。
   - イベントを選択して、「**PCAP**」アイコンをクリックします。
   - イベントの「PCAP」アイコンを右クリックし、「**その他のオプション**」 > 「**PCAP ファイルのダウンロード**」を選択します。
   - 調査するイベントをダブルクリックし、イベント詳細ツールバーから「**PCAP データ**」 > 「**PCAP ファイルのダウンロード**」を選択します。
2. 次のオプションのいずれかを選択してください。

- すぐにファイルを開いて表示する場合は、「**アプリケーションから開く (Open with)**」オプションを選択し、リスト・ボックスからアプリケーションを選択します。
- リストを保存する場合は、「**ファイルの保存 (Save File)**」オプションを選択します。

3. 「**OK**」をクリックします。

イベントのエクスポート

イベントは XML (Extensible Markup Language) 形式または CSV (Comma-Separated Values) 形式でエクスポートできます。

始める前に

データのエクスポートに必要な時間の長さは、指定したパラメーターの数によって変わります。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. オプション。イベントをストリーム・モードで表示している場合は、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。
3. 「**アクション**」リスト・ボックスから、次のいずれかのオプションを選択します。
   - 「**XML にエクスポート**」 > 「**表示列**」 - 「ログ・アクティビティー」タブに表示される列のみをエクスポートするには、このオプションを選択します。これは推奨されるオプションです。
   - 「**XML にエクスポート**」 > 「**完全エクスポート (すべての列)**」 - すべてのイベント・パラメーターをエクスポートするには、このオプションを選択します。完全エクスポートは、完了までに長時間かかります。
   - 「**CSV にエクスポート**」 > 「**表示列**」 - 「**ログ・アクティビティー**」タブに表示される列のみをエクスポートするには、このオプションを選択します。これは推奨されるオプションです。
   - 「**CSV にエクスポート**」 > 「**完全エクスポート (すべての列)**」 - すべてのイベント・パラメーターをエクスポートするには、このオプションを選択します。完全エクスポートは、完了までに長時間かかります。
4. エクスポートの進行中にアクティビティーを再開するには、「**完了時に通知 (Notify When Done)**」をクリックします。

タスクの結果

エクスポートが完了した時に、エクスポートの完了を示す通知を受け取ります。「**完了時に通知 (Notify When Done)**」アイコンを選択しなかった場合は、「状況 (Status)」ウィンドウが表示されます。

第 6 章 ネットワーク・アクティビティーの調査

「**ネットワーク・アクティビティー**」タブを使用して、ネットワーク・アクティビティー (フロー) をリアルタイムでモニターおよび調査したり、拡張検索を実行したりできます。

「ネットワーク」タブの概要

「**ネットワーク・アクティビティー**」タブを使用することにより、ネットワーク・アクティビティー (フロー) をリアルタイムでモニターおよび調査したり、拡張検索を実行したりできます。

「**ネットワーク・アクティビティー**」タブを表示するには、権限が必要になります。

権限と役割の割り当ての詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

「**ネットワーク・アクティビティー**」タブを選択して、フロー・データをリアルタイムで視覚的にモニターおよび調査したり、拡張検索を実行して表示されるフローをフィルターに掛けたりします。フローとは、2 つのホスト間の通信セッションのことです。フロー情報を確認することにより、トラフィックの通信状況、および (コンテンツ・キャプチャー・オプションが有効になっている場合は) 通信内容を判別できます。フロー情報には、プロトコル、自律システム番号 (ASN) 値、またはインターフェース索引 (IFIndex) 値などの詳細情報が含まれることがあります。

「ネットワーク・アクティビティー」タブ・ツールバー

「**ネットワーク・アクティビティー**」タブ・ツールバーからいくつかのオプションにアクセスできます。

「**ネットワーク・アクティビティー**」タブ・ツールバーからは以下のオプションにアクセスできます。

表 23. 「ネットワーク・アクティビティー」タブ・ツールバーのオプション

オプション	説明
検索	フローに関する拡張検索を行うには、「**検索**」をクリックします。以下の検索オプションがあります。 • **新規検索** - 新規のフロー検索を作成するには、このオプションを選択します。 • **検索の編集** - フロー検索を選択および編集するには、このオプションを選択します。 • **検索結果の管理** - 検索結果を表示および管理するには、このオプションを選択します。 検索機能について詳しくは、データの検索を参照してください。

表 23. 「ネットワーク・アクティビティー」タブ・ツールバーのオプション (続き)

オプション	説明
クイック検索	このリスト・ボックスから、以前に保存した検索を実行することができます。「**クイック検索**」リスト・ボックスにオプションが表示されるのは、「**クイック検索に含める**」オプションが指定された検索条件が保存されている場合だけです。
フィルターの追加	現在の検索結果にフィルターを追加するには、「**フィルターの追加**」をクリックします。
条件の保存	現在の検索条件を保存するには、「**条件の保存**」をクリックします。
結果の保存	現在の検索結果を保存するには、「**結果の保存**」をクリックします。このオプションは、検索が完了するまで表示されません。このオプションは、ストリーム・モードでは使用不可になります。
キャンセル	進行中の検索を取り消すには、「**キャンセル**」をクリックします。このオプションは、ストリーム・モードでは使用不可になります。
フォールス・ポジティブ	「**フォールス・ポジティブ**」をクリックすると、「フォールス・ポジティブのチューニング」ウィンドウが開きます。このウィンドウを使用して、フォールス・ポジティブであることが分かっているフローによってオフェンスが生成されないようにすることができます。フォールス・ポジティブについて詳しくは、用語集を参照してください。 このオプションは、ストリーム・モードでは使用不可になります。フローのエクスポートを参照してください。

表 23. 「ネットワーク・アクティビティー」タブ・ツールバーのオプション (続き)

オプション	説明
ルール	「**ルール**」オプションは、カスタム・ルールを表示するための権限を持っている場合のみ表示されます。 次のオプションのいずれかを選択します。 ルールを表示または作成する場合は、「**ルール**」を選択します。ルールを表示するための権限を持っている場合は、ルール・ウィザードのサマリー・ページが表示されます。カスタム・ルールを保守する権限を持っている場合は、ルールを編集することができます。 **注:** アノマリ検出ルール・オプションは、「**ネットワーク・アクティビティー**」 > 「**カスタム・ルールの保守**」権限を持っている場合にのみ表示されます。 アノマリ検出ルール・オプションを有効にするには、集約された検索条件を保存する必要があります。保存済み検索条件により、必要なパラメーターが指定されます。次のオプションのいずれかを選択してください。 しきい値ルールを作成する場合は、「**しきい値ルールの追加**」を選択します。しきい値ルールは、フロー・トラフィックをテストして、構成されたしきい値を超えるアクティビティーが発生していないかどうかを調べます。しきい値は、収集されたすべてのデータに基づいて設定することができます。例えば、午前 8 時から午後 5 時までの間は 220 を超えるクライアントはサーバーにログインできないことを指定するしきい値ルールを作成した場合、221 番目のクライアントがログインしようとすると、このルールによってアラートが生成されます。 動作ルールを作成する場合は、「**動作ルールの追加**」を選択します。動作ルールは、フロー・トラフィックをテストして、通常の周期パターンで発生する動作にボリューム変化が生じていないかどうか調べます。例えば、メール・サーバーが通常は深夜に 1 秒当たり 100 のホストと通信する場合で、突然 1 秒当たり 1000 のホストと通信し始めた場合は、動作ルールがアラートを生成します。 アノマリ・ルールを作成する場合は、「**アノマリ・ルールの追加**」を選択します。アノマリ・ルールは、フロー・トラフィックをテストして、アノマリなアクティビティー (新規のトラフィックや未知のトラフィックなど) がないかどうかを調べます。例えば、最近 5 分間のトラフィックの平均ボリュームを最近 1 時間のトラフィックの平均ボリュームと比較するための、アノマリ・ルールを作成することができます。40% を超える変動があった場合、このルールによって応答が生成されます。 詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

表 23. 「ネットワーク・アクティビティー」タブ・ツールバーのオプション (続き)

オプション	説明
アクション	以下のアクションを実行するには、「**アクション**」をクリックします。 • **すべて表示 (Show All)** - 検索条件のすべてのフィルターを除去して、フィルターに掛けられていないすべてのフローを表示するには、このオプションを選択します。 • **印刷** - ページに表示されるフローを印刷するには、このオプションを選択します。 • **XML にエクスポート** - フローを XML フォーマットでエクスポートするには、このオプションを選択します。フローのエクスポートを参照してください。 • **CSV にエクスポート** - フローを CSV フォーマットでエクスポートするには、このオプションを選択します。フローのエクスポートを参照してください。 • **削除** - 検索結果を削除するには、このオプションを選択します。データの検索を参照してください。 • **通知** - 選択された検索の完了時に E メールで通知を受け取りたい場合には、このオプションを選択します。このオプションは、進行中の検索についてのみ有効になります。 **注:** 「**印刷**」、「**XML にエクスポート**」、および「**CSV にエクスポート**」の各オプションは、ストリーム・モードの場合と、検索結果の一部を表示している場合は無効になります。
検索ツールバー	**拡張検索** リスト・ボックスから「**拡張検索**」を選択した後、取得するフィールドを指定するための Ariel 照会言語 (AQL) の検索ストリングを入力します。 **クイック・フィルター** 単純な語句を使用してペイロードを検索するには、リスト・ボックスから「**クイック・フィルター**」を選択します。
表示 (View)	「**ネットワーク・アクティビティー**」タブのデフォルト表示はリアルタイム・イベントのストリームです。「**表示**」リストには、指定の期間に発生したイベントも表示するオプションが用意されています。「**表示**」リストから指定する期間を選択した後、「**開始時刻**」フィールドおよび「**終了時刻**」フィールドで日時の値を変更することで、表示させる時間を変更することができます。

右クリック・メニューのオプション

「**ネットワーク・アクティビティー**」タブでフローを右クリックして、より多くのフロー・フィルター基準にアクセスできます。

右クリック・メニュー・オプションには、以下のものがあります。

表 24. 右クリック・メニューのオプション

オプション	説明
「フィルター対象 (Filter on)」	このオプションを選択すると、選択したフローで指定したパラメーターに従って、そのフローをフィルターに掛けることができます。
フォールス・ポジティブ	このオプションを選択すると、「フォールス・ポジティブのチューニング」ウィンドウが開きます。このウィンドウを使用して、フォールス・ポジティブであることが知られているフローによってオフェンスが生成されないようにチューニングすることができます。このオプションは、ストリーム・モードでは使用不可になります。フローのエクスポートを参照してください。
その他のオプション (More options):	IP アドレスを調査するには、このオプションを選択します。 IP アドレスの調査を参照してください。 **注:** このオプションは、ストリーム・モードでは表示されません。
クイック・フィルター (Quick Filter)	フィルター操作により、選択内容に一致する項目または一致しない項目を抽出します。

ステータス・バー

フローのストリーミングが発生している場合、ステータス・バーには 1 秒当たりに受信された結果の平均数が表示されます。

これは、コンソールがイベント・プロセッサーから正常に受信した結果の数です。この 1 秒当たりの結果の数値が 40 を超える場合、表示される結果は 40 のみです。残りの結果数は、結果バッファーに集計されます。状況情報をさらに表示するには、マウス・ポインターをステータス・バーの上に移動します。

フローのストリーミングが発生していない場合、ステータス・バーには現在表示されている検索結果の数、およびその検索結果の処理に要した時間が表示されます。

オーバーフロー・レコード

管理権限を持つユーザーは、QRadar QFlow コレクター からイベント・プロセッサーに送信するフローの最大数を指定することができます。

管理権限を持つユーザーは、QRadar QFlow コレクター からイベント・プロセッサーに送信するフローの最大数を指定することができます。フローの数が構成された制限値に達した後で収集されたすべてのデータは、1 つのフロー・レコードにグループ化されます。このフロー・レコードは、「**ネットワーク・アクティビティー**」タブに、送信元 IP アドレス 127.0.0.4 および宛先 IP アドレス 127.0.0.5 と共に表示されます。このフロー・レコードは、「**ネットワーク・アクティビティー**」タブでオーバーフローを指定します。

ネットワーク・アクティビティーのモニター

デフォルトでは、「**ネットワーク・アクティビティー**」タブには、ストリーム・モードでフローが表示されます。これにより、フローをリアルタイムで表示することができます。

ストリーム・モードについて詳しくは、ストリーミング・フローの表示を参照してください。「**表示**」リスト・ボックスを使用して、フローをフィルタリングするための別の時刻範囲を指定することができます。

デフォルトとして構成されている保存済み検索基準がある場合、「**ネットワーク・アクティビティー**」タブにアクセスすると、その検索の結果が自動的に表示されます。検索条件の保存に関する詳細については、検索条件の保存を参照してください。

ストリーミング・フローの表示

ストリーム・モードでは、システムに入るフロー・データを表示することができます。このモードでは、最後の 50 個のフローを表示することで、現在のフロー・アクティビティーをリアルタイムで確認できます。

このタスクについて

ストリーム・モードを有効にする前に、「ネットワーク・アクティビティー」タブまたは検索条件にフィルターを適用する場合、そのフィルターはストリーム・モードで保持されます。ただし、ストリーム・モードでは、グループ化されたフローを含む検索はサポートされません。グループ化されたフローまたはグループ化された検索条件でストリーム・モードを有効にすると、「ネットワーク・アクティビティー」タブに正規化フローが表示されます。『正規化フローの表示』を参照してください。

フローを選択して詳細を表示するか、アクションを実行する場合は、ストリーミングを一時停止してからイベントをダブルクリックする必要があります。ストリーミングが一時停止すると、最後の 1,000 個のフローが表示されます。

手順

1. 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「表示」リスト・ボックスから、「**リアルタイム (ストリーミング) (Real Time (streaming))**」を選択します。

ツールバー・オプションについては、表 5-1 を参照してください。ストリーム・モードで表示されるパラメーターについて詳しくは、表 5-3 を参照してください。

3. オプション。ストリーミング・フローを一時停止または再生します。次のオプションのいずれかを選択してください。
   - イベント・レコードを選択するには、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。
   - ストリーム・モードを再始動するには、「**再生 (Play)**」アイコンをクリックします。

正規化フローの表示

データ・フローは収集され、正規化されてから「**ネットワーク・アクティビティー**」タブに表示されます。

このタスクについて

正規化では、タブに関する読み取り可能な情報を表示するためのフロー・データを準備します。

注: 表示する時間フレームを選択した場合は、時系列グラフが表示されます。時系列グラフの使用について詳しくは、時系列グラフの概要を参照してください。

「**ネットワーク・アクティビティー**」タブには、正規化フローの表示時に以下のパラメーターが表示されます。

表 25. 「ネットワーク・アクティビティー」タブのパラメーター

パラメーター	説明
現在のフィルター	表の最上部に、検索結果に適用されるフィルターの詳細が表示されます。これらのフィルター値を消去するには、「**フィルターのクリア**」をクリックします。 **注:** このパラメーターはフィルターの適用後にのみ表示されます。
表示	リスト・ボックスから、フィルター対象の時刻範囲を選択できます。
現在の統計	リアルタイム (ストリーミング) モードや過去 1 分間 (自動最新表示) モードでない場合は、次のような現在の統計が表示されます。 **注:** 統計を表示または非表示にする場合は、「現在の統計」の横にある矢印をクリックしてください。 • **合計結果数** - 検索条件に一致した結果の総数を示します。 • **検索されたデータ・ファイル** - 指定された期間内に検索されたデータ・ファイルの総数を示します。 • **検索された圧縮データ・ファイル** - 指定された期間内に検索された圧縮データ・ファイルの総数を示します。 • **索引ファイル数** - 指定された期間内に検索された索引ファイルの総数を示します。 • **期間** - 検索期間を示します。 **注:** 現在の統計はトラブルシューティングに役立ちます。フローのトラブルシューティングについて、お客様サポートに問い合わせたときに、現在の統計情報の提供を求められる場合があります。

表 25. 「ネットワーク・アクティビティー」タブのパラメーター (続き)

パラメーター	説明
グラフ (Charts)	時間間隔とグループ・オプションで一致したレコードを表す構成可能グラフを表示します。表示対象からグラフを除外する場合は、「**グラフの非表示**」をクリックします。 グラフは、「最後の間隔 (自動最新表示) (Last Interval (auto refresh))」以上の時間フレーム、および表示するグループ・オプションを選択した後にのみ表示されます。グラフの構成について詳しくは、グラフの構成を参照してください。 **注:** ブラウザーとして Mozilla Firefox を使用し、広告ブロッカー・ブラウザー拡張機能がインストールされている場合、グラフは表示されません。グラフを表示するには、ブラウザー拡張機能の広告ブロッカーを削除する必要があります。詳しくは、ご使用のブラウザーの資料を参照してください。
「**オフェンス**」アイコン	このフローに関連付けられているオフェンスの詳細を表示する場合は、「**オフェンス**」アイコンをクリックします。
フロー・タイプ (Flow Type)	フロー・タイプを指定します。フロー・タイプは、発信アクティビティーに対する着信アクティビティーの比率で測定されます。フロー・タイプを以下に示します。 • **標準フロー (Standard Flow)** - 双方向トラフィック • **タイプ A (Type A)** - 単一から多数へ (単一方向)。例えば、ネットワーク・スキャンを実行する単一ホストなどです。 • **タイプ B (Type B)** - 多数から単一へ (単一方向)。例えば、分散 DoS (DDoS) 攻撃などです。 • **タイプ C (Type C)** - 単一から単一へ (単一方向)。例えば、ホストからホストへのポート・スキャンなどです。
最初のパケットの時刻 (First Packet Time)	フローが受信された日時を示します。
保管時刻 (Storage time)	フローが QRadar データベースに保管される時刻を示します。
送信元 IP	このフローの送信元 IP アドレスを指定します。
送信元ポート	このフローの送信元ポートを指定します。
宛先 IP	このフローの宛先 IP アドレスを指定します。
宛先ポート	このフローの宛先ポートを指定します。

表 25. 「ネットワーク・アクティビティー」タブのパラメーター (続き)

パラメーター	説明
送信元バイト数	送信元ホストから送信されたバイトの数を示します。
宛先バイト数	宛先ホストから送信されたバイトの数を示します。
合計バイト数 (Total Bytes)	フローに関連付けられているバイトの総数を示します。
送信元のパケット数	送信元ホストから送信されたパケットの総数を示します。
宛先のパケット数 (Destination Packets)	宛先ホストから送信されたパケットの総数を示します。
パケットの総数 (Total Packets)	フローに関連付けられているパケットの総数を示します。
プロトコル	フローに関連付けられているプロトコルを示します。
アプリケーション	フローの検出されたアプリケーションを示します。アプリケーションの検出について詳しくは、*IBM Security QRadar Application Configuration Guide* を参照してください。
ICMP タイプ/コード (ICMP Type/Code)	Internet Control Message Protocol (ICMP) のタイプとコードを指定します (該当する場合)。 フローに既知のフォーマットの ICMP タイプとコードの情報がある場合、このフィールドは、タイプ <A>. コード <B> (ここで、<A> および <B> はタイプとコードの数値です) として表示されます。
送信元のフラグ	ソース・パケットで検出された伝送制御プロトコル (TCP) フラグを示します (該当する場合)。
宛先のフラグ (Destination Flags)	宛先パケットで検出された TCP フラグを示します (該当する場合)。

表 25. 「ネットワーク・アクティビティー」タブのパラメーター (続き)

パラメーター	説明
送信元の QoS	フローのサービス品質 (QoS) サービス・レベルを指定します。QoS により、ネットワークでのフローのさまざまなサービス・レベルの提供が可能になります。QoS では以下の基本サービス・レベルが提供されます。 • **ベスト・エフォート (Best Effort)** - このサービス・レベルでは配信は保証されません。フローの配信はベスト・エフォートと見なされます。 • **差異化サービス (Differentiated Service)** - 特定のフローが他のフローより優先されます。この優先順位はトラフィックの分類別に付けられます。 • **保証されたサービス (Guaranteed Service)** - このサービス・レベルでは、特定フローのネットワーク・リソースの予約が保証されます。
宛先の QoS	宛先フローの QoS サービス・レベルを指定します。
フロー・ソース	フローを検出したシステムを示します。
フロー・インターフェース (Flow Interface)	フローを受信したインターフェースを示します。
送信元の If 索引	送信元のインターフェース索引 (IFIndex) 番号を指定します。
宛先の If 索引	宛先の IFIndex 番号を指定します。
送信元 ASN	送信元の自律システム番号 (ASN) の値を指定します。
宛先 ASN	宛先 ASN の値を指定します。

手順

1. 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**表示**」リスト・ボックスから、「**デフォルト (正規化)**」を選択します。
3. 「**表示**」リスト・ボックスから、表示する時間フレームを選択します。
4. 「**一時停止**」アイコンをクリックして、ストリーミングを一時停止します。
5. さらに詳細に表示するフローをダブルクリックします。フローの詳細を参照してください。

グループ化されたフローの表示

「**ネットワーク・アクティビティー**」タブを使用して、さまざまなオプションごとにグループ化されているフローを表示することができます。「**表示**」リスト・ボックスから、フローのグループ化に使用するパラメーターを選択できます。

このタスクについて

「**表示**」リスト・ボックスはストリーム・モードでは表示されません。これは、ストリーム・モードではグループ化されたフローがサポートされないためです。グループ化されていない検索条件を使用してストリーム・モードに入った場合は、このオプションが表示されます。

「**表示**」リスト・ボックスには以下のオプションが示されます。

表 26. グループ化されたフローのオプション

グループ・オプション	説明
送信元 IP または宛先 IP (Source or Destination IP)	フローに関連付けられている IP アドレス別にグループ化されているフローのサマリー・リストを表示します。
送信元 IP	フローの送信元 IP アドレス別にグループ化されているフローのサマリー・リストを表示します。
宛先 IP	フローの宛先 IP アドレス別にグループ化されているフローのサマリー・リストを表示します。
送信元ポート	フローの送信元ポート別にグループ化されているフローのサマリー・リストを表示します。
宛先ポート	フローの宛先ポート別にグループ化されているフローのサマリー・リストを表示します。
送信元ネットワーク	フローの送信元ネットワーク別にグループ化されているフローのサマリー・リストを表示します。
宛先ネットワーク	フローの宛先ネットワーク別にグループ化されているフローのサマリー・リストを表示します。
アプリケーション	フローの発生元のアプリケーション別にグループ化されているフローのサマリー・リストを表示します。
地理 (Geographic)	地理的位置別にグループ化されているフローのサマリー・リストを表示します。
プロトコル	フローに関連付けられているプロトコル別にグループ化されているフローのサマリー・リストを表示します。
フロー・バイアス (Flow Bias)	フローの向き別にグループ化されているフローのサマリー・リストを表示します。
ICMP タイプ (ICMP Type)	フローの ICMP タイプ別にグループ化されているフローのサマリー・リストを表示します。

「**表示**」リスト・ボックスからオプションを選択すると、データの列レイアウトは選択したグループ・オプションよって決まります。フロー表内の各行はフロー・グループを表します。「**ネットワーク・アクティビティー**」タブには、各フロー・グループの以下の情報が示されます。

表 27. グループ化されたフローのパラメーター

パラメーター	説明
グループ化の基準	検索がグループ化されるパラメーターを指定します。
現在のフィルター	表の最上部に、検索結果に適用されるフィルターの詳細が表示されます。これらのフィルター値を消去するには、「**フィルターのクリア**」をクリックします。
表示	リスト・ボックスから、フィルター対象の時刻範囲を選択します。
現在の統計	リアルタイム (ストリーミング) モードや過去 1 分間 (自動最新表示) モードでない場合は、次のような現在の統計が表示されます。 **注:** 統計を表示または非表示にする場合は、「**現在の統計**」の横にある矢印をクリックしてください。 • **合計結果数** - 検索条件に一致した結果の総数を示します。 • **検索されたデータ・ファイル** - 指定された期間内に検索されたデータ・ファイルの総数を示します。 • **検索された圧縮データ・ファイル** - 指定された期間内に検索された圧縮データ・ファイルの総数を示します。 • **索引ファイル数** - 指定された期間内に検索された索引ファイルの総数を示します。 • **期間** - 検索期間を示します。 **注:** 現在の 統計はトラブルシューティングに役立ちます。フローのトラブルシューティングについて、お客様サポートに問い合わせたときに、現在の統計情報の提供を求められる場合があります。

表 27. グループ化されたフローのパラメーター (続き)

パラメーター	説明
グラフ (Charts)	時間間隔とグループ・オプションで一致したレコードを表す構成可能グラフを表示します。表示対象からグラフを除外する場合は、「**グラフの非表示**」をクリックします。 グラフは、「最後の間隔 (自動最新表示) (Last Interval (auto refresh))」以上の時間フレーム、および表示するグループ・オプションを選択した後にのみ表示されます。グラフの構成について詳しくは、グラフの構成を参照してください。 **注:** ブラウザーとして Mozilla Firefox を使用し、広告ブロッカー・ブラウザー拡張機能がインストールされている場合、グラフは表示されません。グラフを表示するには、ブラウザー拡張機能の広告ブロッカーを削除する必要があります。詳しくは、ご使用のブラウザーの資料を参照してください。
送信元 IP (固有の数)	このフローの送信元 IP アドレスを指定します。
宛先 IP (固有の数) (Destination IP (Unique Count))	このフローの宛先 IP アドレスを指定します。このフローに関連付けられている宛先 IP アドレスが複数ある場合、このフィールドには「複数」という用語と IP アドレスの数が示されます。
送信元ポート (固有の数)	フローの送信元ポートを表示します。
宛先ポート (固有の数)	このフローの宛先ポートを指定します。このフローに関連付けられている宛先ポートが複数ある場合、このフィールドには「複数」という用語とポートの数が指定されます。
送信元ネットワーク (固有の数)	フローの送信元ネットワークを指定します。このフローに関連付けられている送信元ネットワークが複数ある場合、このフィールドには「複数」という用語とネットワークの数が指定されます。
宛先ネットワーク (固有の数) (Destination Network (Unique Count))	フローの宛先ネットワークを指定します。このフローに関連付けられている宛先ネットワークが複数ある場合、このフィールドには「複数」という用語とネットワークの数が指定されます。
アプリケーション (固有の数) (Application (Unique Count))	フローの検出されたアプリケーションを示します。このフローに関連付けられているアプリケーションが複数ある場合、このフィールドには「複数」という用語とアプリケーションの数が指定されます。
送信元バイト数 (合計)	送信元からのバイトの数を指定します。
宛先バイト数 (合計)	宛先からのバイトの数を指定します。

表 27. グループ化されたフローのパラメーター (続き)

パラメーター	説明
合計バイト数 (合計) (Total Bytes (Sum))	フローに関連付けられているバイトの総数を示します。
送信元のパケット数 (合計)	送信元からのパケットの数を指定します。
送信元のパケット数 (合計)	送信元からのパケットの数を指定します。
送信元のパケット数 (合計)	送信元からのパケットの数を指定します。
宛先のパケット数 (合計) (Destination Packets (Sum))	宛先からのパケットの数を指定します。
パケットの総数 (合計) (Total Packets (Sum))	フローに関連付けられているパケットの総数を示します。
数	送信または受信されるフローの数を指定します。

手順

1. 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**表示**」リスト・ボックスから、表示する時間フレームを選択します。
3. 「**表示**」リスト・ボックスから、フローをグループ化するパラメーターを選択します。表 2 を参照してください。 フロー・グループがリストされます。フロー・グループの詳細について詳しくは、表 1 を参照してください。
4. グループの「フローのリスト (List of Flows)」ページを表示するには、調査対象のフロー・グループをダブルクリックします。 「フローのリスト (List of Flows)」ページでは、「**ネットワーク・アクティビティー**」タブに定義されている可能性のあるグラフ構成は保持されません。「フローのリスト (List of Flows)」のパラメーターについて詳しくは、表 2 を参照してください。
5. フローの詳細を表示するには、調査対象のフローをダブルクリックします。フローの詳細について詳しくは、表 1 を参照してください。

フローの詳細

ストリーム・モードやフロー・グループなどの各種モードでフローのリストを表示することができます。どのモードでフローを表示する場合でも、単一のフローの詳細を探して表示することができます。

「フローの詳細 (flow details)」ページには、以下の情報が表示されます。

表 28. フローの詳細

パラメーター	説明
フロー情報	
プロトコル	このフローに関連するプロトコルを指定します。 プロトコルについて詳しくは、*IBM Security QRadar Application Configuration Guide* を参照してください。

表 28. フローの詳細 (続き)

パラメーター	説明
アプリケーション	フローの検出されたアプリケーションを示します。アプリケーションの検出について詳しくは、*IBM Security QRadar Application Configuration Guide* を参照してください。
マグニチュード	このフローのマグニチュードを指定します。マグニチュードについて詳しくは、用語集を参照してください。
関連性	このフローの関連性を指定します。関連性について詳しくは、用語集を参照してください。
重大度	このフローの重大度を指定します。重大度について詳しくは、用語集を参照してください。
信頼性	このフローの信頼性を指定します。信頼性について詳しくは、用語集を参照してください。
最初のパケットの時刻 (First Packet Time)	フロー・ソースによって報告される、このフローの開始時刻を指定します。 フロー・ソースの詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
最後のパケットの時刻 (Last Packet Time)	フロー・ソースによって報告される、このフローの終了時刻を指定します。
保管時刻 (Storage Time)	フローが QRadar データベースに保管される時刻を示します。
フロー名 (Flow Name)	このフローの正規化名を指定します。
下位カテゴリー	このフローの下位カテゴリーを指定します。 カテゴリーについて詳しくは、*IBM Security QRadar SIEM 管理ガイド* を参照してください。
フローの説明 (Flow Description)	フローの説明を指定します (使用可能な場合)。
送信元および宛先の情報	
送信元 IP	このフローの送信元 IP アドレスを指定します。
宛先 IP	このフローの宛先 IP アドレスを指定します。
送信元アセット名	このフローの送信元アセット名を指定します。アセットについて詳しくは、アセットの管理を参照してください。
宛先アセット名	このフローの宛先アセット名を指定します。アセットについて詳しくは、アセットの管理を参照してください。

表 28. フローの詳細 (続き)

パラメーター	説明
IPv6 送信元	このフローの送信元 IPv6 アドレスを指定します。
IPv6 宛先 (IPv6 Destination)	このフローの宛先 IPv6 アドレスを指定します。
送信元ポート	このフローの送信元ポートを指定します。
宛先ポート	このフローの宛先ポートを指定します。
送信元の QoS	送信元フローのサービスの QoS レベルを指定します。
宛先の QoS	宛先フローの QoS サービス・レベルを指定します。
送信元 ASN	送信元 ASN 番号を指定します。 **注:** このフローに複数のフロー・ソースからの重複レコードが含まれている場合、対応する送信元 ASN 番号がリストされます。
宛先 ASN	宛先 ASN 番号を指定します。 **注:** このフローに複数のフロー・ソースからの重複レコードが含まれている場合、対応する宛先 ASN 番号がリストされます。
送信元の If 索引	送信元 IFIndex 番号を指定します。 **注:** このフローに複数のフロー・ソースからの重複レコードが含まれている場合、対応する送信元 IFIndex 番号がリストされます。
宛先の If 索引	宛先の IFIndex 番号を指定します。 **注:** このフローに複数のフロー・ソースからの重複レコードが含まれている場合、対応する送信元 IFIndex 番号がリストされます。
送信元のペイロード	送信元のペイロードのパケット数とバイト数を指定します。
宛先のペイロード	宛先のペイロードのパケット数とバイト数を指定します。
ペイロード情報	

表 28. フローの詳細 (続き)

パラメーター	説明
送信元のペイロード	このフローからの送信元ペイロードの内容を指定します。このフィールドには、ペイロードを表示するための以下の 3 つの形式が用意されています。 • Universal Transformation Format (UTF): 「UTF」をクリックします。 • 16 進数 (Hexidecimal): 「HEX」をクリックします。 • Base64: 「Base64」をクリックします。 **注:** フロー・ソースが Netflow v9 または IPFIX である場合、これらのソースの未解析フィールドが「**送信元のペイロード**」フィールドに表示されることがあります。未解析フィールドの形式は <name>=<value> です。例えば、`MN_TTL=x` のようになります。
宛先のペイロード	このフローからの宛先ペイロードの内容を指定します。このフィールドには、ペイロードを表示するための以下の 3 つの形式が用意されています。 • Universal Transformation Format (UTF): 「**UTF**」をクリックします。 • 16 進数 (Hexidecimal): 「**HEX**」をクリックします。 • Base64: 「**Base64**」をクリックします。
追加情報	
フロー・タイプ (Flow Type)	フロー・タイプを指定します。フロー・タイプは、発信アクティビティーに対する着信アクティビティーの比率で測定されます。フロー・タイプを以下に示します。 • 標準: 双方向トラフィック • タイプ A: 1 対多 (単一方向) • タイプ B: 多対 1 (単一方向) • タイプ C: 1 対 1 (単一方向)

表 28. フローの詳細 (続き)

パラメーター	説明
フローの向き (Flow Direction)	フローの方向を指定します。フローの方向を以下に示します。 • L2L: あるローカル・ネットワークから別のローカル・ネットワークへの内部トラフィック。 • L2R: ローカル・ネットワークからリモート・ネットワークへの内部トラフィック。 • R2L: リモート・ネットワークからローカル・ネットワークへの内部トラフィック。 • R2R: あるリモート・ネットワークから別のリモート・ネットワークへの内部トラフィック。
カスタム・ルール	このフローに一致するカスタム・ルールを指定します。 ルールについて詳しくは、*IBM Security QRadar SIEM 管理ガイド* を参照してください。
部分的に一致するカスタム・ルール (Custom Rules Partially Matched)	このフローに部分的に一致するカスタム・ルールを指定します。
フロー・ソース/インターフェース	このフローを検出したシステムのフロー・ソース名を指定します。 **注:** このフローに複数のフロー・ソースからの重複レコードが含まれている場合、対応するフロー・ソースがリストされます。
注釈	このフローの注釈またはメモを指定します。注釈は、テキスト記述です。ルールは、ルールの応答の一部として、注釈をフローに自動的に追加することができます。

「フローの詳細 (Flow Details)」ツールバー

「フローの詳細 (flow details)」ツールバーには、さまざまな機能が用意されています。

「フローの詳細 (flow details)」ツールバーには、以下の機能が用意されています。

表 29. 「フローの詳細」ツールバーの説明

機能	説明
結果に戻る (Return to Results)	**「結果に戻る (Return to Results)」**をクリックすると、フローのリストに戻ります。
プロパティーの抽出	選択されたフローからカスタム・フロー・プロパティーを作成するには、**「プロパティーの抽出」**をクリックします。詳しくは、「カスタム・イベント・プロパティーとカスタム・フロー・プロパティー」を参照してください。

表 29. 「フローの詳細」ツールバーの説明 (続き)

機能	説明
フォールス・ポジティブ	「**フォールス・ポジティブ**」をクリックすると、「フォールス・ポジティブのチューニング」ウィンドウが開きます。このウィンドウを使用して、フォールス・ポジティブであることが分かっているフローによってオフェンスが生成されないようにすることができます。このオプションは、ストリーム・モードでは使用不可になります。詳しくは、フローのエクスポートを参照してください。
前へ	「**前へ**」をクリックすると、フロー・リスト内の前のフローが表示されます。
次へ	「**次へ**」をクリックすると、フロー・リスト内の次のフローが表示されます。
印刷	フローの詳細を印刷するには、「**印刷**」をクリックします。
オフェンス	「**オフェンス**」が選択可能な場合は、クリックするとオフェンスの「サマリー」ページが表示されます。

フォールス・ポジティブのチューニング

フォールス・ポジティブのチューニング機能を使用して、フォールス・ポジティブのフローでオフェンスが作成されないようにすることができます。フォールス・ポジティブのフローは、フロー・リストまたはフローの詳細ページからチューニングできます。

このタスクについて

注: フォールス・ポジティブのフローは、サマリーまたは詳細ページからチューニングできます。

フォールス・ポジティブをチューニングするためにカスタマイズされたルールを作成するには適切な権限が必要です。フォールス・ポジティブについて詳しくは、用語集を参照してください。

手順

1. 「**ネットワーク・アクティビティー**」タブをクリックします。
2. オプション。フローをストリーム・モードで表示している場合は、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。
3. チューニングするフローを選択します。
4. 「**フォールス・ポジティブ**」をクリックします。
5. 「フォールス・ポジティブ」ウィンドウの「イベント/フロー・プロパティー」ペインで、以下のオプションのいずれかを選択します。
   - <イベント> の特定のイベント QID を持つイベント/フロー (Event/Flow(s) with a specific QID of <Event>)

- <イベント> の下位カテゴリーを持つすべてのイベント/フロー (Any Event/Flow(s) with a low-level category of <Event>)
- <イベント> の高位カテゴリーを持つすべてのイベント/フロー (Any Event/Flow(s) with a high-level category of <Event>)

6. 「トラフィックの方向」ペインで、以下のオプションのいずれかを選択します。
   - <送信元 IP アドレス> から <宛先 IP アドレス>
   - <送信元 IP アドレス> から任意の宛先へ
   - 任意の送信元から <宛先 IP アドレス> へ
   - 任意の送信元から任意の宛先へ
7. 「**チューニング (Tune)**」をクリックします。

フローのエクスポート

フローは XML (Extensible Markup Language) 形式または CSV (Comma Separated Values) 形式でエクスポートできます。データのエクスポートに必要な時間の長さは、指定したパラメーターの数によって変わります。

手順

1. 「**ネットワーク・アクティビティー**」タブをクリックします。
2. オプション。フローをストリーム・モードで表示している場合は、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。
3. 「**アクション**」リスト・ボックスから、次のいずれかのオプションを選択します。
   - 「**XML にエクスポート**」 > 「**表示列**」 - 「ログ・アクティビティー」タブに表示される列のみをエクスポートするには、このオプションを選択します。これは推奨されるオプションです。
   - 「**XML にエクスポート**」 > 「**完全エクスポート (すべての列)**」 - すべてのフロー・パラメーターをエクスポートするには、このオプションを選択します。完全エクスポートは、完了までに長時間かかります。
   - 「**CSV にエクスポート**」 > 「**表示列**」 - 「ログ・アクティビティー」タブに表示される列のみをエクスポートするには、このオプションを選択します。これは推奨されるオプションです。
   - 「**CSV にエクスポート**」 > 「**完全エクスポート (すべての列)**」 - すべてのフロー・パラメーターをエクスポートするには、このオプションを選択します。完全エクスポートは、完了までに長時間かかります。
4. アクティビティーを再開するには、「**完了時に通知 (Notify When Done)**」をクリックします。

タスクの結果

エクスポートが完了した時に、エクスポートの完了を示す通知を受け取ります。「**完了時に通知 (Notify When Done)**」アイコンを選択しなかった場合は、「状況 (Status)」ウィンドウが表示されます。

第 7 章 アセットの管理

アセット・データを収集して表示すると、脅威および脆弱性の識別に役立ちます。アセット・データベースが正確であれば、ネットワーク内の物理アセットまたは仮想アセットにシステムで起動したオフェンスを接続することが一層容易になります。

制約事項: QRadar Log Manager では、QRadar Vulnerability Manager がインストールされている場合にのみアセット・データが追跡されます。IBM Security QRadar SIEM と IBM Security QRadar Log Manager の相違点について詳しくは、5 ページの『Security Intelligence 製品の機能』を参照してください。

アセット・データ

アセット とは、ネットワーク・インフラストラクチャー全体でデータを送受信するすべてのネットワーク・エンドポイントのことです。例えば、ノートブック、サーバー、仮想マシン、ハンドヘルド・デバイスなどはすべてアセットです。アセット・データベース内のすべてのアセットには固有 ID が割り当てられ、他のアセット・レコードと区別することができます。

デバイスの検出は、アセットに関する履歴情報のデータ・セットの作成にも役立ちます。アセット情報の変更の追跡は、ネットワークでのアセット使用状況のモニターに役立ちます。

アセット・プロファイル

アセット・プロファイル とは、特定のアセットに関して IBM Security QRadar SIEM が長期間にわたり収集したすべての情報のコレクションのことです。このプロファイルには、アセット上で実行するサービスに関する情報や、既知のアイデンティティー情報が含まれます。

QRadar SIEM はアイデンティティー・イベントおよび双方向フロー・データ、または脆弱性アセスメント・スキャン (構成されている場合) から、アセット・プロファイルを自動的に作成します。データは*アセット調整* と呼ばれるプロセスによって相関付けられ、QRadar が新しい情報を受け取ると、プロファイルが更新されます。アセット名は、以下の優先順位で、アセット更新の情報から派生したものになります。

- 指定された名前
- NetBIOS ホスト名
- DNS ホスト名
- IP アドレス

アセット・データの収集

アセット・プロファイルは、イベント・データまたはフロー・データからパッシブに取り込まれたアイデンティティー情報から、または脆弱点スキャン中に QRadar によってアクティブに検出されたデータから、動的に作成されます。アセット・デ

ータをインポートしたり、アセット・プロファイルを手動で編集したりすることもできます。

アセット・データのソース

アセット・データは、IBM Security QRadar デプロイメント内の複数の異なるソースから受信されます。

アセット・データはアセット・データベースに増分的に書き込まれます。通常は 2、3 個のデータが同時に書き込まれます。ネットワーク脆弱性スキャナーからの更新を除き、各アセット更新に含まれる情報は、一度に 1 つのアセットについてのみです。

アセット・データは、通常は以下のいずれかのアセット・データ・ソースから生じます。

イベント

イベント・ペイロード (DHCP または認証サーバーによって作成されたものなど) には、多くの場合、ユーザー・ログイン、IP アドレス、ホスト名、MAC アドレス、その他のアセット情報が含まれています。このデータは即時にアセット・データベースに提供され、アセット更新の適用先となるアセットを判別するのに役立ちます。

イベントは、異常なアセット増加の主要な原因です。

フロー フロー・ペイロードには、一定の構成可能間隔で収集された IP アドレス、ポート、およびプロトコルなどの通信情報が含まれています。各間隔の終わりに、データは一度に 1 つの IP アドレスずつ、アセット・データベースに提供されます。

フローからのアセット・データは単一の ID である IP アドレスに基づいてアセットとペアにされるため、フロー・データが異常なアセット増加の原因となることはありません。

脆弱性スキャナー

QRadar には、IBM 提供とサード・パーティー提供の両方の脆弱性スキャナーが組み込まれています。それらの脆弱性スキャナーは、オペレーティング・システム、インストール済みソフトウェア、およびパッチ情報などのアセット・データを提供できます。データのタイプはスキャナーごとに異なっており、スキャンごとに異なる場合もあります。新規アセット、ポート情報、および脆弱性が検出されると、スキャンで定義されている CIDR 範囲に基づいて、データがアセット・プロファイルに入ります。

スキャナーが異常なアセット増加の原因となる可能性もありますが、まれです。

ユーザー・インターフェース

アセット・ロールを持つユーザーは、アセット情報をアセット・データベースに直接インポートまたは提供できます。ユーザーによって直接提供されるアセット更新は、特定のアセットを対象としたものであるため、アセット調整ステージはバイパスされます。

ユーザーによって提供されるアセット更新は、異常なアセット増加の原因にはなりません。

ドメイン認識アセット・データ

アセット・データ・ソースがドメイン情報で構成されると、そのデータ・ソースから生じるすべてのアセット・データは、同じドメインで自動的にタグ付けされます。アセット・モデル内のデータはドメインを認識するため、ドメイン情報は、アイデンティティー、オフェンス、アセット・プロファイル、およびサーバー・ディスカバリーを含む、すべての QRadar コンポーネントに適用されます。

アセット・プロファイルを表示すると、一部のフィールドがブランクである場合があります。ブランクのフィールドが存在するのは、システムがその情報をアセット更新で受け取っていない場合か、または情報がアセット保存期間を超過している場合です。デフォルトの保存期間は 120 日です。 IP アドレスが 0.0.0.0 と表示される場合は、アセットに IP アドレス情報が含まれていないことを示します。

入力アセット・データのワークフロー

このワークフローは、QRadar が、イベント・ペイロードでアイデンティティー情報を使用して、新規アセットを作成するかまたは既存のアセットを更新するかを判断する方法を示します。

1. QRadar はイベントを受け取ります。アセット・プロファイラーは、アイデンティティー情報についてイベント・ペイロードを調べます。
2. アイデンティティー情報に、アセット・データベース内のアセットと既に関連付けられている MAC アドレス、NetBIOS ホスト名、または DNS ホスト名が含まれている場合、そのアセットは新しい情報があればその情報で更新されます。
3. 入手できるアイデンティティー情報が IP アドレスのみである場合、システムは同じ IP アドレスを持つ既存のアセットに対する更新を調整します。
4. アセット更新に、既存のアセットと一致する IP アドレスが含まれているものの、既存のアセットとは一致しない別のアイデンティティー情報も含まれている場合、システムは他の情報を使用して、既存のアセットを更新する前にフォールス・ポジティブ一致を排除します。
5. アイデンティティー情報がデータベース内の既存のアセットと一致しない場合、イベント・ペイロードの情報に基づいて新規アセットが作成されます。

アセット・データへの更新

IBM Security QRadar は、イベント・ペイロードでアイデンティティー情報を使用して、新規アセットを作成するかまたは既存のアセットを更新するかを決定します。

各アセット更新には、単一のアセットに関するトラステッド情報が含まれている必要があります。 QRadar がアセット更新を受け取ると、システムはその更新の適用先のアセットを判別します。

アセット*調整* とは、アセット更新とアセット・データベース内の関連アセットとの間の関係を判別するプロセスのことです。アセット調整は、QRadar が更新を受け取った後から、アセット・データベースに情報が書き込まれる前までの期間内に実行されます。

アイデンティティー情報

すべてのアセットには、少なくとも 1 つのアイデンティティー・データが含まれている必要があります。その同じアイデンティティー・データが 1 つ以上含まれている後続の更新は、そのデータを所有するアセットで調整されます。 IP アドレスに基づく更新は、フォールス・ポジティブのアセット一致を回避するために注意深く処理されます。フォールス・ポジティブのアセット一致は、1 つの物理アセットに、システム内の別のアセットが以前に所有していた IP アドレスの所有権が割り当てられているときに起きます。

複数のアイデンティティー・データが提供されている場合、アセット・プロファイラーは以下の順序で情報の優先順位付けを行います。

- MAC アドレス (最も確定的である)
- NetBIOS ホスト名
- DNS ホスト名
- IP アドレス (最も低い優先度で決定)

MAC アドレス、NetBIOS ホスト名、および DNS ホスト名は固有でなければならないため、最も確実なアイデンティティー・データと見なされます。受け取った更新で、IP アドレスしか既存のアセットと一致しないものは、より限定的なアイデンティティー・データと一致する更新とは異なる方法で処理されます。

関連概念:

『アセット調整除外ルール』

IBM Security QRadar が受け取る各アセット更新では、アセット調整除外ルールにより、アセット更新の MAC アドレス、NetBIOS ホスト名、DNS ホスト名、および IP アドレスに対してテストが適用されます。

アセット調整除外ルール

IBM Security QRadar が受け取る各アセット更新では、アセット調整除外ルールにより、アセット更新の MAC アドレス、NetBIOS ホスト名、DNS ホスト名、および IP アドレスに対してテストが適用されます。

デフォルトでは、各アセット・データが追跡される期間は 2 時間です。アセット更新内のいずれかのアイデンティティー・データが 2 時間以内に複数回の疑わしい振る舞いを示す場合、そのデータはアセット・ブラックリストに追加されます。テストされるアイデンティティー・アセット・データのタイプごとに、別個のブラックリストが備えられています。

ドメイン認識環境では、アセット調整除外ルールは、ドメインごとにアセット・データの振る舞いを別個に追跡します。

アセット調整除外ルールは、以下のシナリオをテストします。

表 30. ルールのテストおよび対応

シナリオ	ルールの応答
MAC アドレスが 2 時間以内に 3 つ以上の異なる IP アドレスに関連付けられる場合	MAC アドレスをアセット調整ドメイン MAC ブラックリストに追加する

表 30. ルールのテストおよび対応 (続き)

シナリオ	ルールの応答
DNS ホスト名が 2 時間以内に 3 つ以上の異なる IP アドレスに関連付けられる場合	DNS ホスト名をアセット調整ドメイン DNS ブラックリストに追加する
NetBIOS ホスト名が 2 時間以内に 3 つ以上の異なる IP アドレスに関連付けられる場合	NetBIOS ホスト名をアセット調整ドメイン NetBIOS ブラックリストに追加する
IPv4 アドレスが 2 時間以内に 3 つ以上の異なる MAC アドレスに関連付けられる場合	IP アドレスをアセット調整ドメイン IPv4 ブラックリストに追加する
NetBIOS ホスト名が 2 時間以内に 3 つ以上の異なる MAC アドレスに関連付けられる場合	NetBIOS ホスト名をアセット調整ドメイン NetBIOS ブラックリストに追加する
DNS ホスト名が 2 時間以内に 3 つ以上の異なる MAC アドレスに関連付けられる場合	DNS ホスト名をアセット調整ドメイン DNS ブラックリストに追加する
IPv4 アドレスが 2 時間以内に 3 つ以上の異なる DNS ホスト名に関連付けられる場合	IP アドレスをアセット調整ドメイン IPv4 ブラックリストに追加する
NetBIOS ホスト名が 2 時間以内に 3 つ以上の異なる DNS ホスト名に関連付けられる場合	NetBIOS ホスト名をアセット調整ドメイン NetBIOS ブラックリストに追加する
MAC アドレスが 2 時間以内に 3 つ以上の異なる DNS ホスト名と関連付けられる場合	MAC アドレスをアセット調整ドメイン MAC ブラックリストに追加する
IPv4 アドレスが 2 時間以内に 3 つ以上の異なる NetBIOS ホスト名に関連付けられる場合	IP アドレスをアセット調整ドメイン IPv4 ブラックリストに追加する
DNS ホスト名が 2 時間以内に 3 つ以上の異なる NetBIOS ホスト名に関連付けられる場合	DNS ホスト名をアセット調整ドメイン DNS ブラックリストに追加する
MAC アドレスが 2 時間以内に 3 つ以上の異なる NetBIOS ホスト名に関連付けられる場合	MAC アドレスをアセット調整ドメイン MAC ブラックリストに追加する

これらのルールは、「**オフェンス**」タブで、「**ルール**」をクリックし、ドロップダウン・リストで「**アセット調整除外**」グループを選択することで表示できます。

関連概念:

『例: IP アドレスをブラックリストから除外するように調整されたアセット除外ルール』
アセット除外ルールをチューニングすることで、IP アドレスをブラックリストから除外することができます。

例: IP アドレスをブラックリストから除外するように調整されたアセット除外ルール

アセット除外ルールをチューニングすることで、IP アドレスをブラックリストから除外することができます。

ネットワーク・セキュリティー管理者は、IP アドレスのリースが通常は短期間であり頻繁に行われる公衆 WiFi ネットワーク・セグメントを含む、企業ネットワークを管理します。ネットワークのこのセグメントのアセットは、どちらかといえば一

時的なものであり、主に、公衆 WiFi へのログイン/ログアウトを頻繁に行うノートブックやハンドヘルド・デバイスです。一般的には、単一の IP アドレスが、短期間でさまざまなデバイスによって複数回使用されます。

それ以外のデプロイメントでは、慎重に管理されたネットワークを使用します。このネットワークは、目録に記載されて適切に名前が付けられた企業デバイスのみで構成されています。ネットワークのこの部分では、IP アドレスのリース期間はずっと長く、IP アドレスには認証のみでアクセスします。このネットワーク・セグメントでは、異常なアセット増加が発生している場合は即時に把握し、アセット調整除外ルールのデフォルト設定を維持する必要があります。

ブラックリストへの IP アドレスの登録

この環境では、デフォルトのアセット調整除外ルールにより、ネットワーク全体が短時間で誤ってブラックリストに入れられてしまうことがあります。

セキュリティー・チームは、WiFi セグメントで生成されるアセット関連通知は不要なものであると考えています。 WiFi が異常なアセット増加の通知をそれ以上出さないようにする必要があります。

アセット調整ルールのチューニングによる一部のアセット更新の無視

最新のシステム通知の「**Asset deviation by log source**」レポートを確認します。ブラックリストに挙げられたデータは、WiFi の DHCP サーバーから受け取ったものであることを確認します。

「**AssetExclusion: Exclude IP By MAC Address**」ルールに対応する行の「**イベント数**」列、「**フロー数**」列、および「**オフェンス数**」列の値は、WiFi DHCP サーバーによってこのルールがトリガーされたことを示しています

テストを既存のアセット調整除外ルールに追加して、ルールが WiFi データをブラックリストに追加することを中止します。

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

更新されたルールは、WiFi の DHCP サーバー上にないログ・ソースからのイベントのみをテストします。さらに、WiFi の DHCP イベントがさらにコストが高いリファレンス・セットおよび動作分析のテストを受けないようにするために、このテストをテスト・スタックの最上位に移動しました。

アセットのマージ

アセットのマージ とは、別々のアセットの情報を、それらが実際には同じ物理アセットであるという前提の下に結合させるプロセスのことです。

アセットのマージは、アセット更新に、2 つの異なるアセット・プロファイルと一致するアイデンティティー・データが含まれているときに実行されます。例えば、

あるアセット・プロファイルと一致する NetBIOS ホスト名と、別のアセット・プロファイルと一致する MAC アドレスが単一の更新に含まれていると、アセットのマージが開始されることがあります。

システムによっては、2 つの異なる物理アセットからのアイデンティティー情報を単一のアセット更新に誤って結合してしまうアセット・データ・ソースがあるため、大量のアセットのマージが行われる可能性があります。このようなシステムの例としては、以下のような環境があります。

- イベント・プロキシーとして機能する中央 Syslog サーバー
- 仮想マシン
- 自動化されたインストール済み環境
- iPad や iPhone などのアセットに共通の、固有でないホスト名
- 共有 MAC アドレスがある仮想プライベート・ネットワーク
- アイデンティティー・フィールドが `OverrideAndAlwaysSend=true` であるログ・ソース拡張

多くの IP アドレス、MAC アドレス、またはホスト名があるアセットは、アセット増大での逸脱を示し、システム通知が起動する場合があります。

関連概念:

『異常なアセット増加の検出』

IBM Security QRadar では、アセット・データ・ソースによって作成される更新を適切に処理するために、手動での修復が必要となることがあります。異常なアセット増加の原因に応じて、問題の原因となっているアセット・データ・ソースを修正するか、またはそのデータ・ソースからのアセット更新をブロックすることができます。

異常なアセット増加の検出

IBM Security QRadar では、アセット・データ・ソースによって作成される更新を適切に処理するために、手動での修復が必要となることがあります。異常なアセット増加の原因に応じて、問題の原因となっているアセット・データ・ソースを修正するか、またはそのデータ・ソースからのアセット更新をブロックすることができます。

異常なアセット増加 は、単一のデバイスに対するアセット更新の数が、特定のアイデンティティー情報タイプの保存しきい値によって設定されている制限を超えた場合に発生します。異常なアセット増加に適切に対処することは、正確なアセット・モデルを維持する上で重要です。

異常なアセット増加が発生する原因は、アセット・モデルを更新するには信頼できないデータが含まれているアセット・データ・ソースにあります。異常なアセット増加が発生している可能性が検出されたら、その情報源を調べ、そのアセットで大量のアイデンティティー・データが集計される適切な理由があるかどうかを判断します。異常なアセット増加の原因は、環境固有です。

DHCP サーバーのアセット・プロファイルでの不自然なアセット増大の例

動的ホスト構成プロトコル (DHCP) ネットワーク内の仮想プライベート・ネットワーク (VPN) サーバーについて考えてみます。 VPN サーバーは、着信 VPN クライアントに対して、そのクライアントの代わりに DHCP 要求をネットワークの DHCP サーバーに委任することで、IP アドレスを割り当てるように構成されています。

DHCP サーバーからすると、同じ MAC アドレスが多くの IP アドレス割り当てを繰り返し要求しているように見えます。ネットワーク操作のコンテキストでは、VPN サーバーは IP アドレスをクライアントに委任しますが、DHCP サーバー側では要求が代理の別のアセットによって出されたとしても区別できません。

DHCP サーバー・ログ (QRadar ログ・ソースとして構成される) は、VPN サーバーの MAC アドレスと、VPN クライアントに割り当てられた IP アドレスを関連付ける、DHCP 確認応答 (DHCP ACK) イベントを生成します。アセット調整が行われるときに、システムはこのイベントを MAC アドレスにより調整します。この結果、単一の既存のアセットで、解析される DHCP ACK イベントごとに IP アドレスが 1 つ増えることになります。

最終的に、1 つのアセット・プロファイルに、VPN サーバーに割り振られたすべての IP アドレスが含まれることになります。この異常なアセット増加は、複数のアセットに関する情報が含まれるアセット更新が原因で起きます。

しきい値の設定

データベース内のアセットのプロパティーが特定の数に達すると (複数の IP アドレスや複数の MAC アドレスなど)、QRadar はアセットがそれ以上の更新を受け取らないようにブロックします。

アセットの更新をブロックする条件は、アセット・プロファイラーのしきい値設定で指定します。アセットはこのしきい値に達するまでは、正常に更新されます。システムがしきい値を超えるのに十分なデータを収集すると、アセットは異常なアセット増加を示すようになります。アセットに対するそれ以降の更新は、増大逸脱が修正されるまでブロックされます。

異常なアセット増加を示すシステム通知

IBM Security QRadar は、ご使用の環境内での異常なアセット増加の識別および管理に役立つシステム通知を生成します。

以下のシステム・メッセージは、QRadar が異常なアセット増加の可能性を識別したことを示しています。

- `The system detected asset profiles that exceed the normal size threshold`
- `The asset blacklist rules have added new asset data to the asset blacklists`

システム通知メッセージには、増大逸脱があるアセットの識別に役立つレポートへのリンクが含まれています。

変更の頻度が高いアセット・データ

アセットの増加は、大量のアセット・データが正当な理由で変更されることが原因で発生することがあります。次にそのような状況を示します。

- オフィス間を頻繁に移動するモバイル・デバイスには、ログインするたびに新しい IP アドレスが割り当てられます。
- 大学構内など、IP アドレス・リースが短い公衆 WiFi に接続するデバイスは、1 学期の間に大量のアセット・データを収集することがあります。

例: ログ・ソース拡張の構成エラーが異常なアセット増加の原因になる過程

カスタマイズしたログ・ソース拡張は、正しく構成されていないと、異常なアセット増加の原因になることがあります。

カスタマイズしたログ・ソース拡張は、中央のログ・サーバーにあるイベント・ペイロードからのユーザー名を解析することで、アセット更新を QRadar に提供するように構成します。ログ・ソース拡張は、イベント・ホスト名プロパティーをオーバーライドするように構成します。そうすることで、カスタム・ログ・ソースによって生成されるアセット更新は、必ず中央のログ・サーバーの DNS ホスト名を指定するようになります。

QRadar がユーザーのログイン先のアセットのホスト名を持つ更新を受け取る代わりに、ログ・ソースがすべて同じホスト名を持つアセット更新を多数生成します。

この状態では、異常なアセット増加は、多数の IP アドレスとユーザー名が含まれる 1 つのアセット・プロファイルが原因で発生します。

通常サイズしきい値を超えるアセット・プロファイルのトラブルシューティング

IBM Security QRadar は、単一のアセット下でのデータの累積が、アイデンティティー・データに対して構成されたしきい値限度を超えると、以下のシステム通知を生成します。

```
The system detected asset profiles that exceed the normal size threshold
```

説明

通知のペイロードには、逸脱の頻度が最も高い上位 5 つのアセットのリストと、システムによって各アセットに増大逸脱のマークが付けられた理由が示されます。以下の例に示すように、ペイロードには、アセット・サイズしきい値を超えたアセット増加の試行回数も示されます。

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

アセット・データが構成済みのしきい値を超えると、QRadar はアセットがそれ以降は更新されないようにブロックします。この介入により、システムは破損したデータをそれ以上受け取ることがなくなり、システムが異常な大きさのアセット・プロファイルと突き合わせて受け取った更新を調整しようとした場合に生じる可能性がある、パフォーマンスへの影響を軽減します。

必要なユーザー処置

通知ペイロードの情報を使用して、異常なアセット増加の原因となっているアセットを識別し、異常な増大を引き起こしている原因を判別します。通知には、過去 24 時間で異常なアセット増加が発生したすべてのアセットのレポートへのリンクがあります。

ご使用の環境内での異常なアセット増加を解決した後は、レポートを再度実行できます。

1. 「**ログ・アクティビティー**」タブをクリックし、「**検索**」 > 「**新規検索**」をクリックします。
2. 「**Deviating Asset Growth: Asset Report**」という保存済み検索を選択します。
3. このレポートを使用して、逸脱中に作成された不正確なアセット・データを識別して修復します。

アセット・データが無効である場合、QRadar 管理者は、QRadar の「**管理**」タブにある「**アセット・プロファイラー構成**」で、IP アドレス、MAC アドレス、NetBIOS ホスト名、および DNS ホスト名のしきい値限度を引き上げることができます。

新規アセット・データのアセット・ブラックリストへの追加

IBM Security QRadar は、アセット・データが異常なアセット増加にあたる振る舞いを示すときに、以下のシステム通知を生成します。

```
The asset blacklist rules have added new asset data to the asset blacklists
```

説明

アセット除外ルールは、一貫性と整合性についてアセット・データをモニターします。このルールは特定のアセット・データを長期間追跡し、それらが妥当な時間内に同じデータのサブセットとともに一貫して監視されていることを確認します。

例えば、アセット更新に MAC アドレスと DNS ホスト名の両方が含まれている場合、一定の期間、MAC アドレスはその DNS ホスト名と関連付けられています。MAC アドレスがアセット更新に含まれていれば、その MAC アドレスを含む後続のアセット更新にも、対応する同じ DNS ホスト名が含まれます。 MAC アドレスが急に短期間だけ別の DNS ホスト名と関連付けられた場合、その変更はモニターされます。 MAC アドレスが再び短期間だけ変更された場合、MAC アドレスには、逸脱したアセット増大または異常なアセット増大のインスタンスの原因であるとしてフラグが立てられます。

必要なユーザー処置

通知ペイロードの情報を使用して、アセット・データのモニターに使用されるルールを識別します。通知内の「**Asset deviations by log source**」リンクをクリックして、過去 24 時間以内に発生したアセット逸脱を確認します。

アセット・データが有効な場合、QRadar 管理者は、問題を解決するように QRadar を構成できます。

- ブラックリストへのデータ追加の頻度が高すぎる場合は、ブラックリストにデータを追加するアセット調整除外ルールをチューニングすることができます。
- データをアセット・データベースに追加する場合は、アセット・データをブラックリストから削除し、対応するアセット・ホワイトリストに追加することができます。アセット・データをホワイトリストに追加すると、誤ってブラックリストに再掲載してしまうことが避けられます。

アセット・ブラックリストとアセット・ホワイトリスト

IBM Security QRadar は、アセット調整ルールのグループを使用して、アセット・データを信頼できるかどうかを判断します。アセット・データが疑わしい場合、QRadar は、アセット・ブラックリストとアセット・ホワイトリストを使用して、アセット・プロファイルをアセット・データで更新するかどうかを判断します。

アセット・ブラックリスト とは、IBM Security QRadar が信頼できないと見なすデータのコレクションのことです。アセット・ブラックリストに挙げられたデータは、異常なアセット増加の原因となっている可能性があるため、QRadar はそのデータがアセット・データベースに追加されないようにします。

アセット・ホワイトリスト は、アセット・ブラックリストに追加されるデータに関するアセット調整エンジン・ロジックをオーバーライドする、アセット・データのコレクションです。システムでは、ブラックリストとの一致が検出されると、ホワイトリストにその値が含まれているかどうかが調べられます。アセット更新が、ホワイトリストに含まれているデータに一致すると、変更が調整され、アセットが更新されます。ホワイトリストに挙げられたアセット・データは、すべてのドメインに対してグローバルに適用されます。

QRadar 管理者は、今後の異常なアセット増加を防止するために、アセット・ブラックリストとアセット・ホワイトリストのデータを変更できます。

アセット・ブラックリスト

アセット・ブラックリスト とは、アセット調整除外ルールに基づいて IBM Security QRadar が信頼できないと見なすデータのコレクションのことです。アセット・ブラックリストに挙げられたデータは、異常なアセット増加の原因となっている可能性があるため、QRadar はそのデータがアセット・データベースに追加されないようにします。

QRadar のすべてのアセット更新は、アセット・ブラックリストと照合されます。ブラックリストに挙げられたアセット・データは、すべてのドメインに対してグローバルに適用されます。アセット更新に、ブラックリストに挙げられているアイデン

ティティー情報 (MAC アドレス、NetBIOS ホスト名、DNS ホスト名、または IP アドレス) が含まれていると、受け取った更新は破棄され、アセット・データベースは更新されません。

以下の表に、アイデンティティー・アセット・データのタイプごとの、リファレンス・コレクション名とタイプを示します。

表 31. アセット・ブラックリスト・データのリファレンス・コレクション名

アイデンティティー・データのタイプ	リファレンス・コレクション名	リファレンス・コレクション・タイプ
IP アドレス (v4)	アセット調整 IPv4 ブラックリスト	リファレンス・セット [セット・タイプ: IP]
DNS ホスト名	アセット調整 DNS ブラックリスト	リファレンス・セット [セット・タイプ: ALNIC*]
NetBIOS ホスト名	アセット調整 NetBIOS ブラックリスト	リファレンス・セット [セット・タイプ: ALNIC*]
MAC アドレス	アセット調整 MAC ブラックリスト	リファレンス・セット [セット・タイプ: ALNIC*]
* ALNIC は、ホスト名と MAC アドレスの両方の値に対応できる、英数字タイプです。		

QRadar 管理者は、新規アセット・データが正しく処理されるように、ブラックリスト項目を変更できます。

アセット・ホワイトリスト

アセット・ホワイトリストを使用して、IBM Security QRadar アセット・データがアセット・ブラックリストに誤って再び追加されることを防止できます。

アセット・ホワイトリスト は、アセット・ブラックリストに追加されるデータに関するアセット調整エンジン・ロジックをオーバーライドする、アセット・データのコレクションです。システムでは、ブラックリストとの一致が検出されると、ホワイトリストにその値が含まれているかどうかが調べられます。アセット更新が、ホワイトリストに含まれているデータに一致すると、変更が調整され、アセットが更新されます。ホワイトリストに挙げられたアセット・データは、すべてのドメインに対してグローバルに適用されます。

QRadar 管理者は、新規アセット・データが正しく処理されるように、ホワイトリスト項目を変更できます。

ホワイトリストの使用例

ホワイトリストは、有効なアセット更新であるにもかかわらずブラックリストに継続的に追加されるアセット・データがある場合に役立ちます。例えば、5 つの IP アドレスのセットを循環するように構成されているラウンドロビン DNS ロード・バランサーがあるとします。アセット調整除外ルールにより、1 つの DNS ホスト名に関連付けられている複数の IP アドレスが、異常なアセット増加を示すものと判断され、この DNS ロード・バランサーがブラックリストに追加されることがあります。この問題を解決するには、この DNS ホスト名を Asset Reconciliation DNS Whitelist に追加します。

アセット・ホワイトリストへの大量入力

アセット・データベースが正確であれば、ネットワーク内の物理アセットまたは仮想アセットにシステムで起動したオフェンスを接続することが一層容易になります。アセット・ホワイトリストに大量の項目を追加してアセットの異常を無視することは、正確なアセット・データベースを作成する上では役立ちません。ホワイトリストに大量の項目を追加する代わりに、アセット・ブラックリストを調べ、異常なアセット増加の原因を特定し、その修正方法を決定します。

アセット・ホワイトリストのタイプ

各タイプのアイデンティティー・データはそれぞれ個別のホワイトリストに保持されます。以下の表に、アイデンティティー・アセット・データのタイプごとの、リファレンス・コレクション名とタイプを示します。

表 32. アセット・ホワイトリスト・データのリファレンス・コレクション名

データのタイプ	リファレンス・コレクション名	リファレンス・コレクション・タイプ
IP アドレス	Asset Reconciliation IPv4 Whitelist	リファレンス・セット [セット・タイプ: IP]
DNS ホスト名	Asset Reconciliation DNS Whitelist	リファレンス・セット [セット・タイプ: ALNIC*]
NetBIOS ホスト名	Asset Reconciliation NetBIOS Whitelist	リファレンス・セット [セット・タイプ: ALNIC*]
MAC アドレス	Asset Reconciliation MAC Whitelist	リファレンス・セット [セット・タイプ: ALNIC*]
* ALNIC は、ホスト名と MAC アドレスの値に対応できる、英数字タイプです。		

「アセット・プロファイル (Assets profile)」ページのパラメーター

「アセットのサマリー」ペイン、「ネットワーク・インターフェース」ペイン、「脆弱性」ペイン、「サービス」ペイン、「パッケージ」ペイン、「Windows パッチ」ペイン、「プロパティー」ペイン、「リスク・ポリシー」ペイン、および「製品」ペインについて、「アセット・プロファイル」ページのパラメーターの説明が見つかります。

この解説書には、「**アセット・プロファイル**」タブの各ペイン内に表示されるパラメーターについての説明が記載された表が含まれています。

アセット・プロファイル

アセット・プロファイルでは、各アセットで実行されているサービスを含む、ネットワーク内の認識されているアセットそれぞれに関する情報を提供します。

アセット・プロファイル情報は、相関の目的で使用され、誤検出を低減するために役立ちます。例えば、ソースが、あるアセット上で実行されている特定のサービスのエクスプロイトを試みた場合、QRadar では、この攻撃をそのアセット・プロファイルに相関させることによって、そのアセットがこの攻撃に脆弱であるかどうかを判断します。

フロー・データまたは脆弱性のアセスメント (VA) スキャンを構成している場合、アセット・プロファイルは自動的にディスカバーされます。フロー・データをアセット・プロファイルに取り込むには、双方向フローが必要です。アセット・プロファイルは、ID イベントから自動的に作成することもできます。 VA について詳しくは、「*IBM Security QRadar Vulnerability Assessment Guide*」を参照してください。

フロー・ソースの詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

脆弱性

QRadar Vulnerability Manager とサード・パーティーのスキャナーを使用して、脆弱性を特定することができます。

サード・パーティーのスキャナーでは、Open Source Vulnerability Database (OSVDB)、 National Vulnerability Database (NVDB)、Critical Watch などの外部リファレンスを使用して、検出された脆弱性を特定して報告します。サード・パーティーのスキャナーの例としては、 QualysGuard や nCircle ip360 などがあります。OSVDB では、固有のリファレンス ID (OSVDB ID) をそれぞれの脆弱性に割り当て、また各外部リファレンスでも、固有のリファレンス ID をそれぞれの脆弱性に割り当てます。外部データ・リファレンス ID の例としては、Common Vulnerability and Exposures (CVE) ID や Bugtraq ID があります。スキャナーと脆弱性の評価について詳しくは、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

QRadar Vulnerability Manager は、別途購入して、ライセンス・キーを使用して有効にできるコンポーネントです。QRadar Vulnerability Manager は、ネットワークに存在するアプリケーション、システム、またはデバイスに内在する脆弱性を認識するネットワーク・スキャン・プラットフォームです。スキャンで脆弱性が特定されると、脆弱性データの検索および確認、脆弱性の修復、および新しいリスクのレベルを評価するためのスキャンの再実行を行うことができます。

QRadar Vulnerability Manager が有効になっている場合、「**脆弱性**」タブで脆弱性の評価タスクを実行することができます。「**アセット**」タブで、選択したアセットに対して各スキャンを実行することができます。

詳細については、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

「アセット」タブの概要

「**アセット**」タブには、ワークスペースが提供されています。このワークスペースからネットワーク・アセットを管理でき、またアセットの脆弱性、ポート、アプリケーション、履歴、およびその他の関連付けを調べることができます。

「**アセット**」タブを使用すれば、以下のことを行うことができます。

- すべてのディスカバーされたアセットを表示する。
- アセット・プロファイルを手動で追加する。
- 特定のアセットを検索する。

- ディスカバーされたアセットに関する情報を表示する。
- 手動で追加したか、またはディスカバーされたアセットのアセット・プロファイルを編集する。
- 誤検出の脆弱性をチューニングする。
- アセットをインポートする。
- アセット・プロファイルを印刷またはエクスポートする。
- アセットをディスカバーする。
- サード・パーティーの脆弱性スキャンを構成および管理する。
- QRadar Vulnerability Manager によるスキャンを開始する。

ナビゲーション・ペインの「サーバー・ディスカバリー」オプションについては、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

ナビゲーション・ペインの「VA スキャン (VA Scan)」オプションについて詳しくは、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。

「アセット」タブのリスト

「アセット・プロファイル」ページには、ID、IP アドレス、アセット名、総計 CVSS スコア、脆弱性、およびサービスに関する情報が表示されます。

「アセット・プロファイルページには、各アセットに関する次の情報が表示されます。

表 33. 「アセット・プロファイル」ページのパラメーター

パラメーター	説明
ID	アセットのアセット ID 番号を表示します。アセット ID 番号は、アセット・プロファイルを手動で追加した際、あるいはアセットがイベント、フロー、または脆弱性スキャンによってディスカバーされた際に自動的に生成されます。
IP アドレス	アセットの、最後に認識された IP アドレスを表示します。
アセット名 (Asset Name)	アセットの指定されている名前、NetBios 名、DSN 名、または MAC アドレスを表示します。不明な場合、このフィールドには最後に認識された IP アドレスが表示されます。 **注:** これらの値は、優先度順で表示されます。例えば、アセットに指定されている名前がない場合、集約 NetBios 名が表示されます。 アセットが自動的にディスカバーされた場合、このフィールドには自動的にアセット名が取り込まれますが、必要な場合はこのアセット名を編集できます。

表 33. 「アセット・プロファイル」ページのパラメーター (続き)

パラメーター	説明
リスク・スコア	次の「共通脆弱性評価システム (Common Vulnerability Scoring System: CVSS)」のスコアのいずれかを表示します。 • 統合された総計の環境 CVSS スコア (Coalesced aggregate environmental CVSS score) • 総計の現状 CVSS スコア (Aggregate temporal CVSS score) • 総計 CVSS 基本スコア (Aggregate CVSS base score) • これらのスコアは、優先度順で表示されます。例えば、「統合された総計の環境 CVSS スコア (coalesced aggregate environmental CVSS score)」を利用できない場合、「総計の現状 CVSS スコア (aggregate temporal CVSS score)」が表示されます。 CVSS のスコアは、脆弱性の重大度用のアセスメント (評価) の測定基準です。 CVSS スコアを使用して、ある脆弱性の重大度を他の脆弱性と比較して測定することができます。 CVSS のスコアは、次のユーザー定義のパラメーターをから計算されます。 • 二次的被害の可能性 • 機密性要件 • 可用性要件 • 整合性要件 これらのパラメーターの構成方法について詳しくは、 145 ページの『アセット・プロファイルの追加または編集』を参照してください。 CVSS について詳しくは、 http://www.first.org/cvss/ を参照してください。
脆弱性	このアセットで検出された固有の脆弱性の数を表示します。この値には、アクティブな脆弱性の数およびパッシブな脆弱性の数も含まれます。
サービス	このアセット上で実行される固有のレイヤー 7 アプリケーションの数を表示します。
最後のユーザー (Last User)	アセットに最後に関連付けられたユーザーを表示します。

表 33. 「アセット・プロファイル」ページのパラメーター (続き)

パラメーター	説明
最後に確認されたユーザー	アセットに最後に関連付けられたユーザーが最後に確認された時刻を表示します。

右クリック・メニューのオプション

「アセット」タブでアセットを右クリックすると、イベント・フィルターの情報の詳細に関するメニューが表示されます。

「**アセット**」タブで、アセットを右クリックするとイベント・フィルターの情報にさらにアクセスできます。

表 34. 右クリック・メニューのオプション

オプション	説明
ナビゲート	「**ナビゲート**」メニューには、次のオプションがあります。 • **ネットワーク別に表示 (View by Network)** - 「ネットワークのリスト (List of Networks)」ウィンドウを表示します。このウィンドウには、選択した IP アドレスに関連付けられているすべてのネットワークが表示されます。 • **送信元のサマリーの表示** - 「オフェンスのリスト」ウィンドウを表示します。このウィンドウには、選択した送信元 IP アドレスに関連付けられているすべてのオフェンスが表示されます。 • **宛先のサマリーの表示** - 「オフェンスのリスト」ウィンドウを表示します。このウィンドウには、選択した宛先 IP アドレスに関連付けられているすべてのオフェンスが表示されます。

表 34. 右クリック・メニューのオプション (続き)

オプション	説明
情報	「**情報**」メニューには、次のオプションがあります。 • **DNS ルックアップ (DNS Lookup)** - IP アドレスに基づいている DNS エントリーを検索します。 • **WHOIS ルックアップ (WHOIS Lookup)** - リモート IP アドレスの登録済みオーナーを検索します。デフォルトの WHOIS サーバーは whois.arin.net です。 • **ポート・スキャン** - 選択した IP アドレスの Network Mapper (NMAP) のスキャンを実行します。このオプションは、ご使用のシステムに NMAP がインストールされている場合のみ使用可能です。NMAP のインストールについて詳しくは、ベンダーの資料を参照してください。 • **アセット・プロファイル** - アセット・プロファイル情報を表示します。このメニュー・オプションは、プロファイル・データがスキャンによってアクティブに獲得されるか、フロー・ソースによってパッシブに獲得される場合にのみ使用できます。 • **イベントの検索** - 「**イベントの検索**」オプションは、この IP アドレスに関連付けられているイベントを検索する場合に選択します。 • **フローの検索 (Search Flows)** - 「フローの検索 (Search Flows)」オプションは、この IP アドレスに関連付けられているフローを検索する場合に選択します。
脆弱点スキャンの実行	このオプションは、選択したアセットに対して Vulnerability Manager のスキャンを実行する場合に選択します。 このオプションは、QRadar Vulnerability Manager のインストール後にのみ表示されます。

アセット・プロファイルの表示

「**アセット**」タブのアセット・リストから、アセット・プロファイルを選択して表示することができます。アセット・プロファイルには各プロファイルに関する情報が示されます。

このタスクについて

アセット・プロファイル情報は、「サーバー・ディスカバリー」により自動的にディスカバーされるか、あるいは手動で構成されます。自動生成されたアセット・プロファイル情報は編集可能です。

「アセット・プロファイル」ページには、いくつかのペインに編成される、アセットに関する情報が示されます。ペインを表示する場合は、ペインの矢印 **(>)** をクリックして詳細を表示するか、ツールバーの「**表示**」リスト・ボックスからペインを選択できます。

「アセット・プロファイル」ページ・ツールバーでは、以下の機能が提供されます。

表 35. 「アセット・プロファイル」ページ・ツールバーの機能

オプション	説明
アセット・リストに戻る	アセット・リストに戻る場合はこのオプションをクリックします。
表示	リスト・ボックスから、「アセット・プロファイル」ペインに表示するペインを選択できます。「アセットのサマリー」ペインと「ネットワーク・インターフェースのサマリー」ペインは常に表示されます。 各ペインに表示されるパラメーターについて詳しくは、「アセット・プロファイル (Assets profile)」ページのパラメーターを参照してください。
アセットの編集	アセット・プロファイルを編集する場合はこのオプションをクリックします。 145 ページの『アセット・プロファイルの追加または編集』を参照してください。
ネットワーク別に表示 (View by Network)	このアセットがオフェンスに関連付けられている場合は、このオプションを使用して、このアセットに関連付けられているネットワークのリストを表示できます。「**ネットワーク別に表示 (View By Network)**」をクリックすると、「ネットワークのリスト (List of Networks)」ウィンドウが表示されます。 44 ページの『ネットワークでグループ化されたオフェンスのモニター』を参照してください。
送信元のサマリーの表示	このアセットがオフェンスの送信元である場合は、このオプションを使用して、送信元のサマリー情報を表示できます。「**送信元のサマリーの表示**」をクリックすると、「オフェンスのリスト」ウィンドウが表示されます。 43 ページの『送信元 IP でグループ化されたオフェンスのモニター』を参照してください。

表 35. 「アセット・プロファイル」ページ・ツールバーの機能 (続き)

オプション	説明
宛先のサマリーの表示	このアセットがオフェンスの宛先である場合は、このオプションを使用して、宛先のサマリー情報を表示できます。 **宛先のサマリーの表示**」をクリックすると、「宛先のリスト (List of Destinations)」ウィンドウが表示されます。 43 ページの『宛先 IP でグループ化されたオフェンスのモニター』を参照してください。
履歴	このアセットのイベント履歴情報を表示する場合は 「**履歴**」をクリックします。「**履歴**」アイコンをクリックすると、イベント検索条件が事前に取り込まれた「イベント検索 (Event Search)」ウィンドウが表示されます。 検索パラメーターは必要に応じてカスタマイズすることができます。イベント履歴情報を表示するには、「**検索**」をクリックします。
アプリケーション	このアセットのアプリケーション情報を表示する場合は、「**アプリケーション**」をクリックします。「**アプリケーション**」アイコンをクリックすると、イベント検索条件が事前に取り込まれた「フロー検索 (Flow Search)」ウィンドウが表示されます。 検索パラメーターは、必要に応じてカスタマイズすることができます。アプリケーション情報を表示するには、「**検索**」をクリックします。
接続の検索	接続を検索するには、「**接続の検索**」をクリックします。「接続検索 (Connection Search)」ウィンドウが表示されます。 このオプションは、IBM Security QRadar Risk Manager を購入してライセンス交付を受けている場合のみ、表示することができます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。
トポロジーの表示	アセットをさらに調べる場合は「**トポロジーの表示**」をクリックします。「現在のトポロジー (Current Topology)」ウィンドウが表示されます。 このオプションは、IBM Security QRadar Risk Manager を購入してライセンス交付を受けている場合のみ、表示することができます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。

表 35. 「アセット・プロファイル」ページ・ツールバーの機能 (続き)

オプション	説明
アクション	「**アクション**」リストから、「**脆弱性の履歴 (Vulnerability History)**」を選択します。 このオプションは、IBM Security QRadar Risk Manager を購入してライセンス交付を受けている場合のみ、表示することができます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 表示するアセットをダブルクリックします。
4. ツールバーのオプションを使用して、アセット・プロファイル情報のさまざまなペインを表示します。アセット・プロファイルの編集を参照してください。
5. 関連する脆弱性を調べるには、「脆弱性」ペインで各脆弱性をクリックします。表 10-10 を参照してください。
6. 必要に応じて、アセット・プロファイルを編集します。アセット・プロファイルの編集を参照してください。
7. 必要に応じて、「**アセット・リストに戻る (Return to Assets List)**」をクリックし、別のアセットを選択して表示します。

アセット・プロファイルの追加または編集

アセット・プロファイルは自動的にディスカバーおよび追加されます。ただし、プロファイルを手動で追加する必要がある場合があります。

このタスクについて

「サーバー・ディスカバリー」オプションを使用してアセットがディスカバーされると、一部のアセット・プロファイルの詳細が自動的に取り込まれます。アセット・プロファイルには情報を手動で追加して、特定のパラメーターを編集することができます。

編集できるのは、手動で入力されたパラメーターのみです。システムによって生成されたパラメーターはイタリックで表示され、編集できません。システム生成パラメーターは必要に応じて削除することができます。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 次のオプションのいずれかを選択してください。
   - アセットを追加するには、「**アセットの追加**」をクリックして、「**新規 IP アドレス**」フィールドにアセットの IP アドレスまたは CIDR 範囲を入力します。

- アセットを編集するには、表示するアセットをダブルクリックして、「**アセットの編集**」をクリックします。

4. 「MAC および IP アドレス (MAC & IP Address)」ペインでパラメーターを構成します。次の 1 つ以上のオプションを構成してください。
   - 「**新規 MAC アドレス**」アイコンをクリックして、ダイアログ・ボックスに MAC アドレスを入力します。
   - 「**新規 IP アドレス**」アイコンをクリックして、ダイアログ・ボックスに IP アドレスを入力します。
   - 「**不明な NIC**」がリストされている場合は、この項目を選択し、「**編集**」アイコンをクリックして、ダイアログ・ボックスに新しい MAC アドレスを入力できます。
   - リストから MAC アドレスまたは IP アドレスを選択し、「**編集**」アイコンをクリックして、ダイアログ・ボックスに新しい MAC アドレスを入力します。
   - リストから MAC アドレスまたは IP アドレスを選択して、「**削除**」アイコンをクリックします。
5. 「名前および説明 (Names & Description)」ペインでパラメーターを構成します。次の 1 つ以上のオプションを構成してください。

パラメーター	説明
DNS	次のオプションのいずれかを選択してください。 • DNS 名を入力して、「**追加**」をクリックします。 • リストから DNS 名を選択して、「**編集**」をクリックします。 • リストから DNS 名を選択して、「**削除**」をクリックします。
NetBIOS	次のオプションのいずれかを選択してください。 • NetBIOS 名を入力して、「**追加**」をクリックします。 • リストから NetBIOS 名を選択して、「**編集**」をクリックします。 • リストから NetBIOS 名を選択して、「**削除**」をクリックします。
指定された名前 (Given Name)	このアセット・プロファイルの名前を入力します。
ロケーション (Location)	このアセット・プロファイルのロケーションを入力します。
説明	アセット・プロファイルの説明を入力します。
ワイヤレス AP (Wireless AP)	このアセット・プロファイルのワイヤレス・アクセス・ポイント (AP) を入力します。

パラメーター	説明
ワイヤレス SSID (Wireless SSID)	このアセット・プロファイルのワイヤレス・サービス・セット ID (SSID) を入力します。
スイッチ ID (Switch ID)	このアセット・プロファイルのスイッチ ID を入力します。
スイッチ・ポート ID (Switch Port ID)	このアセット・プロファイルのスイッチ・ポート ID を入力します。

6. 「オペレーティング・システム (Operating System)」ペインで、以下のようにパラメーターを構成します。
   a. 「**ベンダー**」リスト・ボックスから、オペレーティング・システム・ベンダーを選択します。
   b. 「**製品**」リスト・ボックスから、アセット・プロファイルのオペレーティング・システムを選択します。
   c. 「**バージョン**」リスト・ボックスから、選択したオペレーティング・システムのバージョンを選択します。
   d. 「**追加**」アイコンをクリックします。
   e. 「**オーバーライド**」リスト・ボックスから、以下のいずれかのオプションを選択します。
      - **次のスキャンまで (Until Next Scan)** - このオプションを選択すると、スキャナーによってオペレーティング・システム情報が提供され、情報を一時的に編集できるように指定されます。オペレーティング・システムのパラメーターを編集すると、スキャナーによって、その次のスキャンで情報がリストアされます。
      - **無制限 (Forever)** - 手動でオペレーティング・システム情報を入力する必要があり、スキャナーによって情報が更新されないように指定するには、このオプションを選択します。
   f. リストからオペレーティング・システムを選択します。
   g. オペレーティング・システムを選択して、「**オーバーライドの切り替え (Toggle Override)**」アイコンをクリックします。
7. 「CVSS および重み (CVSS & Weight)」ペインでパラメーターを構成します。次の 1 つ以上のオプションを構成してください。

パラメーター	説明
二次的被害の可能性	このアセットの損害または窃盗によるライフまたは物理アセットの損失の可能性を示すように、このパラメーターを構成します。このパラメーターを使用して、生産性または収益の経済的損失の可能性を示すこともできます。二次的被害の可能性が増えると、「CVSS スコア」パラメーターの計算値が増えます。 「**二次的被害の可能性**」リスト・ボックスから、以下のいずれかのオプションを選択します。 • なし • 低 • 低から中 • 中から高 • 高 • 未定義 「**二次的被害の可能性**」パラメーターを構成すると、「**重み**」パラメーターが自動的に更新されます。
機密性要件	このアセットの脆弱性をエクスプロイトされた場合の機密性への影響を示すように、このパラメーターを構成します。機密性への影響が増すと、「CVSS スコア」パラメーターの計算値が増えます。 「**機密性要件**」リスト・ボックスから、以下のいずれかのオプションを選択します。 • 低 • 中 • 高 • 未定義

パラメーター	説明
可用性要件	脆弱性をエクスプロイトされた場合のアセットの可用性への影響を示すように、このパラメーターを構成します。ネットワーク帯域幅、プロセッサー・サイクル、またはディスク・スペースを消費する攻撃は、アセットの可用性に影響します。可用性への影響が増すと、「CVSS スコア」パラメーターの計算値が増えます。 「**可用性要件**」リスト・ボックスから、以下のいずれかのオプションを選択します。 • 低 • 中 • 高 • 未定義
整合性要件	脆弱性をエクスプロイトされた場合のアセットの保全性への影響を示すには、このパラメーターを構成します。保全性とは、情報の信頼性および保証された信憑性を意味します。保全性への影響が増すと、「CVSS スコア」パラメーターの計算値が増えます。 「**整合性要件**」リスト・ボックスから、以下のいずれかのオプションを選択します。 • 低 • 中 • 高 • 未定義
重み	「**重み**」リスト・ボックスから、このアセット・プロファイルの重みを選択します。範囲は 0 から 10 です。 「**重み**」パラメーターを構成すると、「**二次的被害の可能性**」パラメーターが自動的に更新されます。

8. 「所有者 (Owner)」ペインでパラメーターを構成します。次の 1 つ以上のオプションを選択してください。

パラメーター	説明
ビジネス・オーナー (Business Owner)	アセットのビジネス・オーナーの名前を入力します。ビジネス・オーナーの例として、部長などがあります。最大長は 255 文字です。
ビジネス・オーナーの連絡先 (Business Owner Contact)	ビジネス・オーナーの連絡先情報を入力します。最大長は 255 文字です。

パラメーター	説明
テクニカル・オーナー	アセットのテクニカル・オーナーを入力します。テクニカル・オーナーの例として、IT マネージャーやディレクターなどがあります。最大長は 255 文字です。
テクニカル・オーナーの連絡先 (Technical Owner Contact)	テクニカル・オーナーの連絡先情報を入力します。最大長は 255 文字です。
テクニカル・ユーザー (Technical User)	リスト・ボックスから、このアセット・プロファイルに関連付けるユーザー名を選択します。 このパラメーターを使用して、IBM Security QRadar Vulnerability Manager の脆弱性の自動修復を有効にすることができます。自動修復について詳しくは、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

9. 「**保存**」をクリックします。

アセット・プロファイルの検索

「**アセット**」タブの「アセット」ページから、調査するアセット・プロファイルのみを表示するように、検索パラメーターを構成することができます。

このタスクについて

「**アセット**」タブにアクセスすると、ネットワークで検出されたすべてのアセットが取り込まれた「アセット」ページが表示されます。このリストを絞り込むために、調査するアセット・プロファイルのみを表示するように検索パラメーターを構成することができます。

「アセット検索 (Asset Search)」ページから、アセット検索グループを管理することができます。アセット検索グループについて詳しくは、『アセット検索グループ』を参照してください。

検索機能を使用すれば、ホスト・プロファイル、アセット、およびアイデンティティー情報を検索できます。アイデンティティー情報には、DNS 情報、ユーザー・ログイン、および MAC アドレスを含む、ネットワーク上のログ・ソースに関する詳細が示されます。

アセット検索機能を使用して、外部データ・リファレンスによるアセット検索を行うことで、デプロイメントに既知の脆弱性が存在するかどうかを判断できます。

例:

CVE ID: CVE-2010-000 がフィールドでアクティブに使用されていることを示す通知を受け取ります。このエクスプロイトに対して脆弱なホストがデプロイメント内にあるかどうかを確認するために、検索パラメーター・リストから「**脆弱性外部リファレンス**」を選択し、「**CVE**」を選択してから、

```
2010-000
```

を入力できます。

これにより、その特定の CVE ID に対して脆弱なすべてのホストのリストが表示されます。

注: OSVDB について詳しくは、 *http://osvdb.org/* を参照してください。 NVDB について詳しくは、 *http://nvd.nist.gov/* を参照してください。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. ツールバーで、「**検索**」 > 「**新規検索**」をクリックします。
4. 次のオプションのいずれかを選択してください。
   - 以前に保存した検索をロードする場合は、ステップ 5 に進みます。
   - 新規検索を作成する場合は、ステップ 6 に進みます。
5. 以下のように、以前に保存した検索を選択します。
   a. 次のオプションのいずれかを選択してください。
      - オプション。「**グループ**」リスト・ボックスから、「**使用可能な保存済み検索**」リストに表示するアセット検索グループを選択します。
      - 「**使用可能な保存済み検索**」リストから、ロードする保存済み検索を選択します。
      - 「**保存済み検索の入力またはリストから選択**」フィールドに、ロードする検索の名前を入力します。

   b. 「**ロード**」をクリックします。
6. 「検索パラメーター」ペインで、以下のように検索条件を定義します。
   a. 最初のリスト・ボックスから、検索対象のアセット・パラメーターを選択します。例えば、「**ホスト名**」、「**脆弱性リスク分類**」、または「**テクニカル・オーナー**」などです。
   b. 2 番目のリスト・ボックスから、検索に使用する修飾子を選択します。
   c. 入力フィールドに、検索パラメーターに関連する具体的な情報を入力します。
   d. 「**フィルターの追加**」をクリックします。
   e. 検索条件に追加するフィルターごとにこれらのステップを繰り返します。
7. 「**検索**」をクリックします。

タスクの結果

アセット検索条件を保存することができます。アセット検索条件の保存を参照してください。

アセット検索条件の保存

「**アセット**」タブでは、構成済み検索条件を再使用できるように保存することができます。保存済み検索条件の有効期限が切れることはありません。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 検索を実行します。
4. 「**条件の保存**」をクリックします。
5. 次の各パラメーターの値を入力します。

パラメーター	説明
この検索の名前を入力してください (Enter the name of this search)	この検索条件に割り当てる固有名を入力します。
グループの管理	検索グループを管理するには、「**グループの管理**」をクリックします。このオプションは、管理権限がある場合にのみ表示されます。
グループへの検索の割り当て	この保存済み検索を割り当てるグループのチェック・ボックスを選択します。グループを選択しない場合、この保存済み検索はデフォルトで「**その他**」グループに割り当てられます。
クイック検索に含める	この検索を「**クイック検索**」リスト・ボックス (「**アセット**」タブ・ツールバーにあります) に含める場合は、このチェック・ボックスを選択します。
デフォルトとして設定	「**アセット**」タブへのアクセス時にこの検索をデフォルトとして設定する場合は、このチェック・ボックスを選択します。
全員と共有	検索要件をすべてのユーザーと共有する場合は、このチェック・ボックスを選択します。

アセット検索グループ

「アセット検索グループ」ウィンドウを使用すれば、アセット検索グループの作成および管理を行うことができます。

これらのグループによって、「**アセット**」タブで保存済み検索条件を簡単に見つけることができます。

検索グループの表示

「アセット検索グループ」ウィンドウを使用して、グループとサブグループのリストを表示します。

このタスクについて

「アセット検索グループ」ウィンドウから、グループの説明やグループが最後に変更された日付を含む、各グループの詳細を表示できます。

グループに割り当てられていない保存済み検索はすべて「**その他**」グループに含まれます。

「アセット検索グループ」ウィンドウには、各グループの以下のパラメーターが表示されます。

表 36. 「アセット検索グループ」ウィンドウ・ツールバーの機能

機能	説明
新規グループ	新規検索グループを作成する場合は、「**新規グループ**」をクリックできます。『新規検索グループの作成』を参照してください。
編集	既存の検索グループを編集する場合は、「**編集**」をクリックできます。『検索グループの編集』を参照してください。
コピー	保存済み検索を別の検索グループにコピーする場合は、「**コピー**」をクリックできます。『別のグループへの保存済み検索のコピー』を参照してください。
削除	検索グループ、または検索グループから保存済み検索を削除するには、削除する項目を選択してから、「**削除**」をクリックします。『グループの削除またはグループからの保存済み検索の削除』を参照してください。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 「**検索**」 > 「**新規検索**」を選択します。
4. 「**グループの管理**」をクリックします。
5. 検索グループを表示します。

新規検索グループの作成

「アセット検索グループ」ウィンドウでは、新規検索グループを作成することができます。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 「**検索**」 > 「**新規検索**」を選択します。
4. 「**グループの管理**」をクリックします。
5. 新規グループをあるグループの下に作成するために、その上位のグループのフォルダーを選択します。
6. 「**新規グループ**」をクリックします。
7. 「**名前**」フィールドに、新規グループの固有名を入力します。
8. オプション。「**説明**」フィールドに、説明を入力します。
9. 「**OK**」をクリックします。

検索グループの編集

検索グループの「**名前**」フィールドと「**説明**」フィールドを編集することができます。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 「**検索**」 > 「**新規検索**」を選択します。
4. 「**グループの管理**」をクリックします。
5. 編集するグループを選択します。
6. 「**編集**」をクリックします。
7. 「**名前**」フィールドに新しい名前を入力します。
8. 「**説明**」フィールドに新しい説明を入力します。
9. 「**OK**」をクリックします。

別のグループへの保存済み検索のコピー

保存済み検索を別のグループにコピーすることができます。また、保存済み検索を複数のグループにコピーすることもできます。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 「**検索**」 > 「**新規検索**」を選択します。
4. 「**グループの管理**」をクリックします。
5. コピーする保存済み検索を選択します。
6. 「**コピー**」をクリックします。
7. 「項目グループ」ウィンドウで、保存済み検索のコピー先となるグループのチェック・ボックスを選択します。
8. 「**グループの割り当て**」をクリックします。

グループの削除またはグループからの保存済み検索の削除

「**削除**」アイコンを使用して、グループから検索を削除したり、検索グループを削除することができます。

このタスクについて

グループから保存済み検索を削除しても、その保存済み検索はシステムからは削除されません。保存済み検索は、グループから削除され、自動的に「**その他**」グループに移動されます。

次のグループはシステムから削除できません。

- アセット検索グループ
- その他

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 「**検索**」 > 「**新規検索**」を選択します。
4. 「**グループの管理**」をクリックします。
5. グループから削除する保存済み検索を選択します。
   - グループから削除する保存済み検索を選択します。
   - 削除するグループを選択します。

アセット・プロファイルの管理タスク

「アセット」タブを使用して、アセット・プロファイルの削除、インポート、およびエクスポートを行うことができます。

このタスクについて

「**アセット**」タブを使用すれば、アセット・プロファイルの削除、インポート、およびエクスポートを行うことができます。

アセットの削除

特定のアセットまたはリストされているすべてのアセット・プロファイルを削除することができます。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 削除するアセットを選択し、「**アクション**」リスト・ボックスから「**アセットの削除 (Delete Asset)**」を選択します。
4. 「**OK**」をクリックします。

アセット・プロファイルのインポート

アセット・プロファイル情報をインポートすることができます。

始める前に

インポートするファイルは以下の形式の CSV ファイルでなければなりません。

```
ip,name,weight,description
```

各項目の意味は次のとおりです。

- **IP** - ドット 10 進形式の有効な IP アドレスを指定します。例えば、192.168.5.34 などです。
- **Name** - 255 文字までの長さのアセット名を指定します。このフィールドではコンマは無効です。コンマを使用すると、インポート・プロセスが無効になります。正しい例として、WebServer01 などがあります。
- **Weight** - ネットワークでのこのアセットの重要度を示す、0 から 10 までの数値を指定します。値 0 は重要度が低いことを示し、10 は非常に高いことを示します。

- **Description** - 255 文字までの長さのアセットのテキスト説明を指定します。この値はオプションです。

例えば、以下のような項目が CSV ファイルに含まれます。

```
192.168.5.34,WebServer01,5,Main Production Web Server
```

```
192.168.5.35,MailServ01,0,
```

インポート・プロセスでは、インポートされたアセット・プロファイルが、システムに現在保管されているアセット・プロファイル情報にマージされます。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 「**アクション**」リスト・ボックスから、「**アセットのインポート**」を選択します。
4. 「**参照**」をクリックし、インポートする CSV ファイルを見つけて選択します。
5. 「**アセットのインポート**」をクリックして、インポート・プロセスを開始します。

アセットのエクスポート

リストされたアセット・プロファイルを拡張マークアップ言語 (XML) ファイルまたはコンマ区切り値 (CSV) ファイルにエクスポートすることができます。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. 「**アクション**」リスト・ボックスから、次のいずれかのオプションを選択します。
   - XML にエクスポート
   - CSV にエクスポート
4. 状況ウィンドウを表示して、エクスポート・プロセスの状況を確認します。
5. オプション: エクスポートの進行中に他のタブとページを使用する場合は、「**完了時に通知 (Notify When Done)**」リンクをクリックします。

   エクスポートが完了すると、「ファイルのダウンロード (File Download)」ウィンドウが表示されます。
6. 「ファイルのダウンロード (File Download)」ウィンドウで、以下のいずれかのオプションを選択します。
   - **オープン** - 任意のブラウザーでエクスポート結果を開く場合は、このオプションを選択します。
   - **保存** - デスクトップに結果を保存する場合は、このオプションを選択します。
7. 「**OK**」をクリックします。

アセットの脆弱性の調査

「アセット・プロファイル」ページの「脆弱性」ペインには、アセットについて検出された脆弱性のリストが表示されます。

このタスクについて

対象の脆弱性をダブルクリックして、脆弱性の詳細を表示することができます。

「脆弱性調査の詳細」ウィンドウには、以下の詳細が示されます。

パラメーター	説明
脆弱性 ID (Vulnerability ID)	脆弱性の ID を指定します。脆弱性 ID は、脆弱性情報システム (VIS) によって生成される固有 ID です。
公開日 (Published Date)	OSVDB で脆弱性の詳細が公開された日付を示します。
名前	脆弱性の名前を指定します。
アセット	ネットワーク内の、この脆弱性があるアセットの数を指定します。リンクをクリックすると、アセット・リストが表示されます。
例外を含むアセット (Assets, including exceptions)	ネットワーク内の、脆弱性例外を含むアセットの数を指定します。リンクをクリックすると、アセット・リストが表示されます。
CVE	脆弱性の CVE ID を指定します。CVE ID は NVDB で指定されます。 詳細情報を取得するには、リンクをクリックします。リンクをクリックすると、新しいブラウザー・ウィンドウに NVDB の Web サイトが表示されます。
xforce	脆弱性の X-Force ID を指定します。 詳細情報を取得するには、リンクをクリックします。リンクをクリックすると、新しいブラウザー・ウィンドウに IBM Internet Security Systems の Web サイトが表示されます。
OSVDB	脆弱性の OSVDB ID を指定します。 詳細情報を取得するには、リンクをクリックします。リンクをクリックすると、新しいブラウザー・ウィンドウに OSVDB の Web サイトが表示されます。

パラメーター	説明
プラグイン詳細	QRadar Vulnerability Manager ID を指定します。 リンクをクリックすると、脆弱性についての Oval 定義、Windows 知識ベースの項目、または UNIX アドバイザリーが表示されます。 この機能により、パッチのスキャン中に QRadar Vulnerability Manager が脆弱性の詳細を検査する方法に関する情報が提供されます。これを使用すると、アセットに関する脆弱性が生じた (または生じなかった) 理由を特定できます。
CVSS スコアのベース (CVSS Score Base)	このアセットの脆弱性の共通脆弱性評価システム (CVSS) の総スコアを表示します。CVSS のスコアは、脆弱性の重大度用のアセスメント (評価) の測定基準です。 CVSS スコアを使用して、ある脆弱性の重大度を他の脆弱性と比較して測定することができます。 CVSS スコアは、以下のユーザー定義パラメーターを使用して算出されます。 • 二次的被害の可能性 • 機密性要件 • 可用性要件 • 整合性要件 これらのパラメーターの構成方法について詳しくは、145 ページの『アセット・プロファイルの追加または編集』を参照してください。 CVSS について詳しくは、*http://www.first.org/cvss/* を参照してください。
影響 (Impact)	この脆弱性をエクスプロイトされた場合に予測できる損失や損害のタイプを表示します。
CVSS 基本メトリック (CVSS Base Metrics)	CVSS の基本スコアを算出するために使用される以下のようなメトリックを表示します。 • アクセス・ベクトル • アクセスの複雑さ • 認証 • 機密性への影響 • 保全性への影響 • 可用性への影響

パラメーター	説明
説明	検出された脆弱性の説明を指定します。この値は、ご使用のシステムで VA ツールが統合されている場合にのみ使用可能です。
問題 (Concern)	脆弱性がネットワークに与える可能性のある影響を示します。
解決方法 (Solution)	示される指示に従って、脆弱性を解決してください。
仮想パッチ (Virtual Patching)	この脆弱性に関連付けられている仮想パッチ情報 (使用可能な場合) を表示します。仮想パッチは、最近検出された脆弱性の短期緩和解決方法です。この情報は侵入防止システム (IPS) のイベントから得られます。仮想パッチをインストールする場合は、IPS ベンダー情報を参照してください。
リファレンス (Reference)	以下のような外部リファレンスのリストを表示します。 • **リファレンス・タイプ (Reference Type)** - 通知 URL やメール・ポスト・リストなど、リストされるリファレンスのタイプを指定します。 • **URL** - リファレンスを表示するためにクリックできる URL を指定します。 詳細情報を取得するには、リンクをクリックします。リンクをクリックすると、新しいブラウザー・ウィンドウに外部リソースが表示されます。
製品	この脆弱性に関連付けられている製品のリストを表示します。 • **ベンダー** - 製品のベンダーを指定します。 • **製品** - 製品名を指定します。 • **バージョン** - 製品のバージョン番号を指定します。

手順

1. 「**アセット**」タブをクリックします。
2. ナビゲーション・メニューで、「**アセット・プロファイル**」をクリックします。
3. アセット・プロファイルを選択します。
4. 「脆弱性」ペインで、調査する脆弱性の「**ID**」または「**脆弱性**」パラメーター値をクリックします。

第 8 章 グラフの管理

さまざまなグラフ構成オプションを使用して、データを表示することができます。

「**ログ・アクティビティー**」タブと「**ネットワーク・アクティビティー**」タブでグラフを使用することにより、さまざまなグラフ構成オプションを指定してデータを表示することができます。

グラフの管理

さまざまなグラフ構成オプションを使用してデータを表示することができます。

時間フレーム・オプションまたはグループ化オプションを選択してデータを表示すると、イベント・リストまたはフロー・リストの上部にグラフが表示されます。

グラフは、ストリーム・モードでは表示されません。

グラフを構成して、作図するデータを選択することができます。複数のグラフを相互に独立して構成することにより、異なる視点から検索結果を表示することができます。

グラフのタイプを以下に示します。

- 棒グラフ (Bar Chart) - データを棒グラフで表示します。このオプションは、グループ化されたイベントの場合のみ選択可能することができます。
- 円グラフ (Pie Chart) - データを円グラフで表示します。このオプションは、グループ化されたイベントの場合のみ選択可能することができます。
- 表 - データを表形式で表示します。このオプションは、グループ化されたイベントの場合のみ選択可能することができます。
- 時系列 (Time Series) - 指定された時間間隔ごとの一致したレコードを表す、インタラクティブな折れ線グラフを表示します。時系列の検索条件の構成については、時系列グラフの概要を参照してください。

グラフの構成後に以下の操作を実行した場合、グラフの構成は保持されます。

- 「**表示**」リスト・ボックスを使用してビューを変更する。
- フィルターを適用する。
- 検索条件を保存する。

以下の操作を実行した場合、グラフの構成は保持されません。

- 新しい検索を開始する。
- クイック検索にアクセスする。
- グループ化された結果を分岐ウィンドウで表示する。
- 検索結果を保存する。

注: Mozilla Firefox Web ブラウザーを使用していて、ブラウザー拡張機能の広告ブロッカーがインストールされている場合、グラフは表示されません。グラフを

表示するには、ブラウザー拡張機能の広告ブロッカーを削除する必要があります。詳しくは、ご使用のブラウザーの資料を参照してください。

時系列グラフの概要

時系列グラフとは、時間の経過とともに表されたアクティビティーのグラフィカル表現です。

グラフ内に表示される山と谷は、大量のアクティビティーと少量のアクティビティーを表しています。時系列グラフは、データの短期および長期のトレンド分析に役立ちます。

時系列グラフを使用すれば、さまざまな視点や角度から、ログ・アクティビティーまたはネットワーク・アクティビティーに対するアクセス、ナビゲート、および調査を行うことができます。

注: 時系列グラフを管理および表示するには、適切なロール権限が必要です。

時系列グラフを表示するには、時系列とグループ化のオプションが組み込まれた検索を作成して保存する必要があります。時系列検索は 100 個まで保存できます。

デフォルトの保存済み時系列検索は、イベント検索またはフロー検索のページの使用可能な検索のリストからアクセスできます。

検索名は検索条件で指定された時刻範囲と共に追加されるため、保存済み時系列検索は「**クイック検索**」 メニューで容易に識別できます。

検索パラメーターが列定義とグループ化のオプション用に前に保存済みの検索に一致する場合、時系列グラフが検索結果に自動的に表示される場合があります。時系列グラフが、保存されていない検索条件に対して自動的には表示されない場合、検索パラメーターに一致する、前に保存済みの検索条件は存在しません。この状態が発生した場合、時系列データのキャプチャーを有効にして、検索条件を保存する必要があります。

アクティビティーを調べるために、時系列グラフ上のタイムラインを拡大してスキャンできます。次の表は、時系列グラフの表示に使用できる機能を示しています。

表 37. 時系列グラフの機能

機能	説明
データをさらに詳細に表示する	ズーム機能を使用すれば、イベント・トラフィックのさらに短い時間セグメントを調査できます。 • マウス・ポインターをグラフの上に移動してから、マウス・ホイールを使用してグラフを拡大します (マウス・ホイールをロールアップ (画面上方送り) する)。 • 拡大するグラフの領域を強調表示します。マウス・ボタンを放すと、グラフにはさらに短い時間セグメントが表示されます。これで、グラフをクリックおよびドラッグしてグラフをスキャンすることができます。 時系列グラフを拡大すると、グラフはさらに短い時間セグメントを表示するために更新されます。
さらに長い期間のデータを表示する	ズーム機能を使用すれば、さらに長い時間セグメントを調べたり、最大の時刻範囲に戻ったりすることができます。次のいずれかのオプションを使用して、時刻範囲を拡張できます。 • グラフの左上隅の「ズーム・リセット (Zoom Reset)」をクリックします。 • マウス・ポインターをグラフの上に移動してから、マウス・ホイールを使用して表示を拡張します (マウス・ホイールをロールダウン (画面下方送り) する)。
グラフをスキャンする	時系列グラフを拡大している場合、グラフをクリックしてから左または右にドラッグして、タイムラインをスキャンできます。

グラフの凡例

各グラフには凡例が表示されます。この凡例は、グラフ・オブジェクトとそれが表すパラメーターとの関連付けを行うための、参照用の表示情報です。

凡例機能を使用して、以下のアクションを実行できます。

- 凡例項目または凡例のカラー・ブロックにマウス・ポインターを移動して、それが表すパラメーターに関する詳細情報を表示する。
- 凡例項目を右クリックして、その項目をさらに詳しく調べる。
- 円グラフまたは棒グラフの凡例項目をクリックして、グラフ内でその項目を非表示にする。凡例項目を再度クリックすると、非表示項目が表示されます。対応するグラフ項目をクリックして、項目の表示と非表示を切り替えることもできます。

- 「**凡例 (Legend)**」をクリックするか、その隣の矢印をクリックして、グラフ内で凡例を非表示にする。

グラフの構成

構成オプションを使用して、グラフ・タイプ、グラフで表すオブジェクト・タイプ、およびグラフ上で表されるオブジェクトの数を変更することができます。時系列グラフの場合は、時刻範囲を選択したり、時系列データのキャプチャーを有効にしたりすることもできます。

始める前に

グラフは、イベントまたはフローを「リアルタイム (ストリーミング) (Real Time (streaming))」モードで表示している場合は表示されません。グラフを表示するには、「**ログ・アクティビティー**」タブまたは「**ネットワーク・アクティビティー**」タブにアクセスして、次のオプションのいずれかを選択する必要があります。

- 「**表示**」と「**表示**」のリスト・ボックスからオプションを選択した後、ツールバーの「**条件の保存**」をクリックします。検索基準の保存を参照してください。
- ツールバーで、「**クイック検索**」リストから保存済み検索を選択します。
- グループ化された検索を実行してから、ツールバーの「**条件の保存**」をクリックします。

時系列グラフの構成を計画している場合、必ず保存済み検索条件をグループ化し、また保存済み検索条件で時刻範囲を指定してください。

このタスクについて

時系列検索を実行する際に、前の期間のデータを表示するためにデータのキャッシュを使用できるように、データを累積できます。選択したパラメーターに対して時系列データのキャプチャーを有効にすると、「グラフで表す値 (Value to Graph)」リスト・ボックス内のそのパラメーターの隣にアスタリスク (*) が表示されます。

手順

1. 「**ログ・アクティビティー**」 タブまたは「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「グラフ (Charts)」ペインで、「**構成 (Configure)**」アイコンをクリックします。
3. 次のパラメーターの値を構成します。

オプション	**説明**
パラメーター	説明
グラフで表す値 (Value to Graph)	リスト・ボックスから、グラフの Y 軸で表すオブジェクト・タイプを選択します。 このオプションには、ご使用の検索パラメーターに含まれた、正規化されたカスタム・イベントまたはカスタム・フローのパラメーターがすべて含まれています。

オプション	説明
表示する上位件数 (Display Top)	リスト・ボックスから、グラフ内に表示するオブジェクトの数を選択します。デフォルトは 10 です。10 項目を超えるグラフを作成すると、グラフのデータが読めなくなる場合があります。
グラフ・タイプ	リスト・ボックスから、表示するグラフ・タイプを選択します。 棒グラフ、円グラフ、または表グラフが 1 時間を超える時刻範囲を持つ保存済み検索条件に基づいている場合、「**詳細の更新**」をクリックしてグラフを更新し、イベントの詳細にデータを取り込む必要があります
時系列データのキャプチャー	このチェック・ボックスは、時系列データのキャプチャーを有効にする場合に選択します。このチェック・ボックスを選択すると、グラフ機能で時系列グラフのデータの累積が開始されます。デフォルトでは、このオプションは無効になっています。 このオプションを選択できるのは、時系列グラフについてのみです。
時刻範囲	リスト・ボックスから、表示する時刻範囲を選択します。 このオプションを選択できるのは、時系列グラフについてのみです。

4. 「**時系列グラフ**」オプションを選択し、「**時系列データのキャプチャー**」オプションを有効にした場合は、ツールバーの「**条件の保存**」をクリックします。
5. 時刻範囲が 1 時間を超えている場合にイベントまたはフローのリストを表示するには、「**詳細の更新**」をクリックします。

第 9 章 データの検索

「**ログ・アクティビティー**」タブ、「**ネットワーク・アクティビティー**」タブ、および「**オフェンス**」タブで特定の基準を使用して、イベント、フロー、およびオフェンスを検索することができます。

新しい検索を作成することも、以前に保存された一連の検索条件をロードすることもできます。検索結果として表示するデータ列の選択、編成、グループ化を行うことができます。

イベントとフローの検索

「**ログ・アクティビティー**」タブと「**ネットワーク・アクティビティー**」タブで検索を実行することができます。

検索を実行したら、検索条件と検索結果を保存することができます。

基準と一致する項目の検索

指定した検索条件と一致するデータを検索することができます。

このタスクについて

データベース全体が検索されるため、データベースのサイズによっては検索に時間がかかることがあります。

「**クイック・フィルター**」検索パラメーターを使用して、指定したテキスト・ストリングと一致する項目をイベント・ペイロードで検索することができます。

以下の表に、イベント・データまたはフロー・データを検索する際に使用できる検索オプションを示します。

表 38. 検索オプション

オプション	説明
グループ	「**使用可能な保存済み検索**」リストで表示するイベント検索グループまたはフロー検索グループを選択します。
保存済み検索の入力またはリストから選択	保存済み検索の名前を入力するか、「**使用可能な保存済み検索**」リストをフィルタリングするためのキーワードを入力します。
使用可能な保存済み検索	このリストには、「**グループ**」または「**保存済み検索の入力またはリストから選択**」オプションを使用してリストをフィルタリングしない限り、使用可能なすべての検索が表示されます。このリストで、表示または編集する保存済み検索を選択することができます。

表 38. 検索オプション (続き)

オプション	説明
検索	「**検索**」アイコンは、検索ページの複数のペインで使用できます。検索の構成が終了したら、「検索」をクリックして結果を表示することができます。
クイック検索に含める	この検索を「**クイック検索**」メニューに含める場合は、このチェック・ボックスを選択します。
ダッシュボードに含める	保存済み検索からのデータを「**ダッシュボード**」タブに組み込む場合は、このチェック・ボックスを選択します。「**ダッシュボード**」タブについて詳しくは、『ダッシュボードの管理』を参照してください。 **注:** このパラメーターは、検索がグループ化されている場合にのみ表示されます。
デフォルトとして設定	この検索をデフォルトの検索として設定する場合は、このチェック・ボックスを選択します。
全員と共有	この検索を他のユーザー全員と共有する場合は、このチェック・ボックスを選択します。
リアルタイム (ストリーミング) (Real Time (streaming))	結果をストリーム・モードで表示します。ストリーム・モードについて詳しくは、ストリーミング・イベントの表示を参照してください。 **注:** 「リアルタイム (ストリーミング) (Real Time (streaming))」が有効になっているときは、検索結果をグループ化できません。「列定義」ペインでグループ化オプションを選択すると、エラー・メッセージが表示されます。
最後の間隔 (自動最新表示) (Last Interval (auto refresh))	検索結果を自動最新表示モードで表示します。 自動最新表示モードでは、「**ログ・アクティビティー**」タブと「**ネットワーク・アクティビティー**」タブが 1 分間隔で最新表示されて最新情報が表示されます。
最新	検索に対して定義済みの時刻範囲を選択します。このオプションを選択した後に、リスト・ボックスから時刻範囲のオプションを選択する必要があります。
特定の間隔	検索に対してカスタムの時刻範囲を選択します。このオプションを選択した後に、「**開始時刻**」および「**終了時刻**」のカレンダーから日時の範囲を選択する必要があります。

表 38. 検索オプション (続き)

オプション	説明
データ集計	このペインは、保存済み検索をロードした場合にのみ表示されます。 他の多数の保存済み検索およびレポートと共有されている集計データに対する固有カウントを有効にすると、システム・パフォーマンスが低下する可能性があります。 保存済み検索をロードすると、このペインに次のオプションが表示されます。 • この保存済み検索に対してデータが集計されていない場合は、「**この検索ではデータが集計されていません (Data is not being accumulated for this search)**」という情報メッセージが表示されます。 • この保存済み検索に対してデータが集計されている場合は、次のオプションが表示されます。 – 「**列**」 - このリンクをクリックするか、このリンクにマウスを移動すると、データを集計している列のリストが表示されます。 – 「**固有カウントの有効化**」/「**固有カウントの無効化**」 - このリンクでは、ある期間の平均の数ではなく、固有のイベントおよびフローの数を検索結果に表示できるようにする、または表示できないようにすることができます。「**固有カウントの有効化**」リンクをクリックすると、ダイアログ・ボックスが開き、集計データを共有する保存済み検索とレポートが表示されます。
現在のフィルター	このリストには、この検索に適用されるフィルターが表示されます。「**現在のフィルター**」リストの上には、フィルターを追加するためのオプションが表示されます。
検索の完了時に結果を保存 (Save results when search is complete)	検索結果に名前を付けて保存する場合は、このチェック・ボックスを選択します。
表示	検索結果に表示するように設定されている定義済みの列を指定する場合は、このリストを選択します。

表 38. 検索オプション (続き)

オプション	説明
列を入力するか、リストから選択してください (Type Column or Select from List)	フィールドを使用して、「使用可能な列」リストに表示される列をフィルタリングすることができます。 配置する列の名前を入力するか、列名のリストを表示するためのキーワードを入力します。例えば、列名に「デバイス」を含む列のリストを表示するには、**「デバイス」**と入力します。
使用可能な列	このリストには、使用可能な列が表示されます。この保存済み検索で現在使用されている列が、**「列」**リスト内で強調表示されます。
列アイコンの追加と削除 (上部セット) (Add and remove column icons (top set))	上部セットのアイコンを使用して、**「グループ化の基準」**リストをカスタマイズします。 • **「列の追加」** - **「使用可能な列」**リストから 1 つ以上の列を選択し、**「列の追加」**アイコンをクリックします。 • **「列の削除」** - **「グループ化の基準」**リストから 1 つ以上の列を選択し、**「列の削除」**アイコンをクリックします。
列アイコンの追加と削除 (下部セット) (Add and remove column icons (bottom set))	下部セットのアイコンを使用して、**「列」**リストをカスタマイズします。 • **「列の追加」** - 「使用可能な列」リストから 1 つ以上の列を選択し、**「列の追加」**アイコンをクリックします。 • **「列の削除」** - 「列」リストから 1 つ以上の列を選択し、**「列の削除」**アイコンをクリックします。
グループ化の基準	このリストでは、保存済み検索の結果をグループ化する列を指定します。次のオプションを使用して、「グループ化の基準」リストをさらにカスタマイズできます。 • 「上に移動」 - 列を選択し、**「上に移動」**アイコンを使用してその列を優先順位リスト内で上に移動します。 • 「下に移動」 - 列を選択し、**「下に移動」**アイコンを使用してその列を優先順位リスト内で下に移動します。 優先順位リストは、結果をグループ化する順序を指定します。検索結果は、**「グループ化の基準」**リストの 1 列目でグループ化された後、リストの次の列でグループ化されます。

表 38. 検索オプション (続き)

オプション	説明
列	検索に対して選択される列を指定します。「**使用可能な列**」リストから追加の列を選択できます。次のオプションを使用して、「**列**」リストをさらにカスタマイズできます。 • 「**上に移動**」 - 選択した列を優先順位リスト内で上に移動します • 「**下に移動**」 - 選択した列を優先順位リスト内で下に移動します 列のタイプが数値または時刻ベースである場合に、「**グループ化の基準**」リストに項目があるときは、列にリスト・ボックスが表示されます。このリスト・ボックスを使用して、列をどのようにグループ化するかを選択します。 列のタイプがグループである場合は、グループに含めるレベルの数を選択するためのリスト・ボックスが列に表示されます。
順序	最初のリスト・ボックスから、検索結果のソート基準となる列を選択します。次に、2 番目のリスト・ボックスから、検索結果を表示する順序を選択します。指定可能なオプションは、「**降順**」と「**昇順**」です。
結果の制限	「検索の編集」ウィンドウに返される検索結果の行数を指定することができます。また、「結果」ウィンドウには、「**結果の制限**」フィールドも表示されます。 • 保存済み検索の場合、保存済み検索内に制限が保管され、検索のロード時に再適用されます。 • 行の制限が存在する検索結果で列によるソートを行う場合、データ・グリッドに表示される制限された行でのみソートが実行されます。 • グループ別検索で時系列グラフがオンになっている場合、行の制限はデータ・グリッドに対してのみ適用されます。この場合も、時系列グラフの「**上位 N**」ドロップダウンにより、グラフに取り込む時系列の数が制御されます。

手順

1. 次のオプションのいずれかを選択してください。
   • イベントを検索する場合は、「**ログ・アクティビティー**」タブをクリックします。

- フローを検索する場合は、「**ネットワーク・アクティビティー**」タブをクリックします。

2. 「**検索**」リスト・ボックスから、「**新規検索**」を選択します。
3. 以前に保存した検索を選択する場合は、以下の手順に従います。
   a. 「使用可能な保存済み検索 (Available Saved Searches)」リストからロードする保存済み検索を選択するか、または、「保存済み検索の入力またはリストから選択」フィールドに、ロードする検索の名前を入力します。
   b. 「**ロード**」をクリックします。
   c. 「検索の編集」ペインで、この検索に必要なオプションを選択します。表 1 を参照してください。
4. 検索を作成する場合は、「時刻範囲」ペインで、この検索用にキャプチャーする時刻範囲のオプションを選択します。
5. オプション。「データ集計」ペインで、固有の数を有効にします。
   a. 「**固有カウントの有効化**」をクリックします。
   b. 「警告」ウィンドウで、警告メッセージを読み、「**続行**」をクリックします。固有の数の有効化について詳しくは、表 1を参照してください。
6. 「検索パラメーター」ペインで、以下のように検索条件を定義します。
   a. 最初のリスト・ボックスから、検索対象のパラメーターを選択します。例えば、「デバイス (Device)」、「送信元ポート」、「イベント名」などです。
   b. 2 番目のリスト・ボックスから、検索に使用する修飾子を選択します。
   c. 入力フィールドに、検索パラメーターに関連する具体的な情報を入力します。
   d. 「**フィルターの追加**」をクリックします。
   e. 検索条件に追加するフィルターごとに、a から d までのステップを繰り返します。
7. オプション。検索完了時に検索結果を自動的に保存する場合は、「**検索の完了時に結果を保存 (Save results when search is complete)**」チェック・ボックスを選択し、保存済み検索の名前を入力します。
8. 「列定義」ペインで、結果の表示に使用する列および列のレイアウトを定義します。
   a. 「**表示**」リスト・ボックスから、この検索に関連付けるように設定された事前構成済みの列を選択します。
   b. 「**拡張ビュー定義**」の横にある矢印をクリックして、拡張検索パラメーターを表示します。
   c. 検索結果に表示する列をカスタマイズします。表 1 を参照してください。
   d. オプション。「**結果の制限**」フィールドに、検索結果の行数を入力します。
9. 「**フィルター (Filter)**」をクリックします。

タスクの結果

右上隅に、「**進行中 (<数値>% 完了) (In Progress (<percent>%Complete))**」状況が表示されます。

.

部分的な検索結果が表示されている間に、検索エンジンがバックグラウンドで稼働して検索を完了させ、部分的な結果を最新表示してビューを更新します。

検索が完了すると、右上隅に「**完了 (Completed)**」状況が表示されます。

検索条件の保存

構成済みの検索条件は、保存することができます。保存済み検索条件を今後の検索で再使用したり、レポートなどの他のコンポーネントで使用したりすることができます。保存済み検索条件の有効期限が切れることはありません。

このタスクについて

検索に時刻範囲を指定すると、指定した時刻範囲が検索名に付加されます。例えば、保存済み検索の名前が「エクスプロイト (送信元別)」、指定した時刻範囲が「過去 5 分間」の場合は、「エクスプロイト (送信元別) - 過去 5 分間」となります。

以前に保存した検索の列セットを変更し、その検索条件を同じ名前で保存すると、それまでの時系列グラフの集計が失われます。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 検索を実行します。
3. 「**条件の保存**」をクリックします。
4. 次の各パラメーターの値を入力します。

オプション	説明
パラメーター	説明
検索名	この検索条件に割り当てる固有名を入力します。
グループへの検索の割り当て	この保存済み検索を割り当てるグループのチェック・ボックスを選択します。グループを選択しない場合は、この保存済み検索がデフォルトで「その他」グループに割り当てられます。詳しくは、検索グループの管理を参照してください。
グループの管理	検索グループを管理するには、「**グループの管理**」をクリックします。詳しくは、検索グループの管理を参照してください。

オプション	説明
期間オプション: (Timespan options:)	次のオプションのいずれかを選択してください。 • **リアルタイム (ストリーミング)** - ストリーム・モードで検索結果をフィルタリングするには、このオプションを選択します。 • **最後の間隔 (自動最新表示)** - 自動最新表示モードで検索結果をフィルタリングするには、このオプションを選択します。「**ログ・アクティビティー**」タブと「**ネットワーク・アクティビティー**」タブは、1 分間隔で最新表示されて最新情報が表示されます。 • 「**最新**」 - このオプションを選択する場合は、リスト・ボックスでフィルター対象の時刻範囲を選択します。 • **特定の間隔**- このオプションを選択する場合は、カレンダーでフィルター対象の日時範囲を選択します。
クイック検索に含める	この検索をツールバーの「**クイック検索**」リスト・ボックスに含める場合は、このチェック・ボックスを選択します。
ダッシュボードに含める	保存済み検索からのデータを「**ダッシュボード**」タブに組み込む場合は、このチェック・ボックスを選択します。「**ダッシュボード**」タブについて詳しくは、『ダッシュボードの管理』を参照してください。 **注:** このパラメーターは、検索がグループ化されている場合にのみ表示されます。
デフォルトとして設定	この検索をデフォルトの検索として設定する場合は、このチェック・ボックスを選択します。
全員と共有	検索要件をすべてのユーザーと共有する場合は、このチェック・ボックスを選択します。

5. 「**OK**」をクリックします。

スケジュール済み検索

「スケジュール済み検索」オプションを使用して、検索をスケジュールして結果を表示します。

日中または夜間の特定の時間に実行する検索をスケジュールできます。

例:
夜間に実行する検索をスケジュールした場合、朝に調査できます。レポートとは異なり、検索結果をグループ化してさらに調査するオプションがあります。ネットワーク・グループ内の失敗したログインの数を検索できます。通常の結果は 10 であり、検索の結果が 100 の場合は、検索結果をグループ化して調査を容易にすること

ができます。ログインに最も失敗しているユーザーを確認するために、ユーザー名でグループ化できます。さらに調査を続行できます。

「**レポート**」タブからイベントまたはフローの検索をスケジュールできます。スケジューリングでは、事前に保存済みの検索条件のセットを選択する必要があります。

1. レポートの作成

   「**レポート・ウィザード**」ウィンドウで以下の情報を指定します。

   - グラフ・タイプは「イベント/ログ」または「フロー」です。
   - このレポートは保存済み検索に基づいています。
   - オフェンスを作成します。

     「**個別のオフェンスの作成**」オプションまたは「**既存のオフェンスに結果を追加**」オプションを選択できます。

     手動検索を生成することもできます。

2. 検索結果の表示

「**オフェンス**」タブからスケジュール済み検索の結果を表示できます。

- スケジュール済み検索のオフェンスは「**オフェンスのタイプ**」列によって識別されます。

  個別のオフェンスを作成する場合、レポートが実行される度にオフェンスが生成されます。既存のオフェンスに保存済み検索結果を追加する場合、レポートの初回実行時にオフェンスが作成されます。後続のレポート実行はこのオフェンスに追加されます。結果が返されない場合は、システムによってオフェンスが追加されることも作成されることもありません。

- 「オフェンスのサマリー」ウィンドウに最新の検索結果を表示するには、オフェンス・リスト内のスケジュール済み検索のオフェンスをダブルクリックします。すべてのスケジュール済み検索実行のリストを表示するには、「**最後の 5 件の検索結果**」ペインの「**検索結果**」をクリックします。

スケジュール済み検索のオフェンスをユーザーに割り当てることができます。

関連タスク:

167 ページの『基準と一致する項目の検索』
指定した検索条件と一致するデータを検索することができます。

49 ページの『ユーザーへのオフェンスの割り当て』
「**オフェンス**」タブを使用すれば、調査のためにオフェンスをユーザーに割り当てることができます。

拡張検索オプション

必要なフィールドと、照会を実行するためのグループ化方法を指定する Ariel 照会言語 (AQL) を入力するには、「**拡張検索**」フィールドを使用します。

「**拡張検索**」フィールドには、オートコンプリートおよび構文強調表示の機能が備わっています。

オートコンプリートおよび構文強調表示の機能は照会の作成に便利です。サポートされる Web ブラウザーについて詳しくは、 7 ページの『サポート対象の Web ブラウザー』を参照してください。

拡張検索へのアクセス

「**ネットワーク・アクティビティー**」タブおよび「**ログ・アクティビティー**」タブにある「**検索**」ツールバーから「**拡張検索**」オプションにアクセスし、AQL 照会を入力します。

「**検索**」ツールバーにあるリスト・ボックスから「**拡張検索**」を選択します。

「**拡張検索**」フィールドを展開するには、以下の手順を実行します。

1. フィールドの右側にある展開アイコンをドラッグします。
2. Shift キーを押しながら Enter キーを押して次の行に移動します。
3. Enter を押します。

検索結果にある任意の値を右クリックして、その値をフィルター処理できます。

検索結果の任意の行をダブルクリックすると詳細が表示されます。

検索はすべて (AQL 検索も含めて) 監査ログに記録されます。

AQL 検索ストリングの例

AQL 検索ストリングの例を以下の表に示します。

表 39. AQL 検索ストリングの例

説明	例

イベントにあるデフォルトの列を選択します。
 	
フローにあるデフォルトの列を選択します。
	`SELECT * FROM events`
	
	`SELECT * FROM flows`

特定の列を選択します。	`SELECT sourceip, destinationip FROM events`
特定の列を選択して結果を並べ替えます。	`SELECT sourceip, destinationip FROM events ORDER BY destinationip`
集約された検索照会を実行します。	`SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip`
SELECT 節で関数呼び出しを実行します。	`SELECT CATEGORYNAME(category) AS namedCategory FROM events`
WHERE 節を使用して検索結果をフィルター処理します。	`SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1`
ルール名またはルール名に含まれる一部のテキストに基づいて、特定のルールをトリガーしたイベントを検索します。	`SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'`
フィールド名を二重引用符で囲むことによって、特殊文字 (算術記号やスペースなど) を含むフィールド名を参照します。	`SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'`

以下の表には、X-Force の AQL 検索ストリングの例が示されています。

表 40. X-Force の AQL 検索ストリングの例

説明	例
IP アドレスは信頼値を使用して X-Force カテゴリーと突き合わせて確認します。	`select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)>3`
URL と関連付けられている X-Force URL のカテゴリーを検索します。	`select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL`
IP と関連付けられている X-Force IP のカテゴリーを検索します。	`select sourceip, XFORCE_IP_CATEGORY (sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL`

関数、検索フィールド、および演算子について詳しくは、「*Ariel 照会言語ガイド*」を参照してください。

AQL 検索ストリングの例

Ariel データベースのイベント、フロー、および simarc 表の特定のフィールドを検索するには、Ariel 照会言語 (AQL) を使用します。

注: AQL 照会を作成するときに、単一引用符を含むテキストを文書からコピーして、このテキストを IBM Security QRadar に貼り付けると、照会が解析されません。これを回避するためには、テキストを QRadar に貼り付けてから単一引用符を再入力するか、または IBM Knowledge Center からテキストをコピーして貼り付ける方法があります。

アカウント使用状況のレポート

ユーザー・コミュニティーごとに脅威や使用状況のインディケーターを変えることができます。

いくつかのユーザー・プロパティー (部門、ロケーション、マネージャーなど) に関するレポートを作成するには、リファレンス・データを使用します。

外部リファレンス・データを使用できます。

以下の照会は、ログイン・イベントに含まれるユーザーに関するメタデータ情報を返します。

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

複数のアカウント ID での情報抽出

この例では、個々のユーザーがネットワーク全体にわたって複数のアカウントを持っているとします。組織にはユーザー・アクティビティーの単一ビューが必要です。

ローカル・ユーザー ID をグローバル ID にマップするには、リファレンス・データを使用します。

以下の照会は、疑わしい振る舞いというフラグが立てられたイベントで使用されているユーザー・アカウントをグローバル ID ごとに返します。

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

以下の照会は、完了したアクティビティーをグローバル ID ごとに表示します。

```
SELECT
QIDNAME(qid) as 'Event name',
starttime as 'Time',
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

疑わしい長期的なビーコンの識別

多くの脅威は、コマンドとコントロールを使用して、数日、数週間、および数カ月にわたり定期的に通信します。

拡張検索により、経時的な接続パターンを識別できます。例えば、IP アドレス間または IP アドレスと地理的位置との間で日/週/月ごとの、整合している接続、短時間の接続、低ボリュームの接続、接続数を照会できます。

オフェンスを生成したり、リファレンス・セットまたはリファレンス・テーブルをデータ設定したりするには、IBM Security QRadar REST API を使用します。

以下の照会は、1 時間ごとに作動するビーコンの可能性があるインスタンスを検出します。

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'hh')) as 'different hours',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection = 'L2R'
GROUP BY sourceip, destinationip
HAVING 'different hours' > 20
AND 'total flows' < 25
LAST 24 hours
```

ヒント: この照会に変更を加えて、プロキシー・ログなどのイベント・タイプで機能させることができます。

以下の照会は、1 日ごとに作動するビーコンの可能性があるインスタンスを検出します。

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'dd'))as 'different days',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection='L2R'
GROUP BY sourceip, destinationip
HAVING 'different days' > 4
AND 'total flows' < 14
LAST 7 days
```

以下の照会は、送信元 IP と宛先 IP の間で毎日作動するビーコンを検出します。ビーコンが作動する時刻は毎日一定しているわけではありません。ビーコンは短い間隔で作動します。

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG( hourofday*hourofday) - (AVG(hourofday)^2))as variance,
COUNT(*) as 'total flows'
FROM flows
GROUP BY sourceip, destinationip
HAVING variance < 01 and 'total flows' < 10
LAST 7 days
```

以下の照会は、プロキシー・ログ・イベントを使用することで、毎日ドメインに送信されるビーコンを検出します。ビーコンが作動する時刻は毎日一定しているわけではありません。ビーコンは短い間隔で作動します。

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and 'total events' < 10
LAST 7 days
```

url_domain プロパティーはプロキシー・ログのカスタム・プロパティーです。

外部脅威情報

使用状況およびセキュリティーのデータを外部脅威情報データと相関させると、重要な脅威のインディケーターを実現できます。

拡張検索では、外部脅威情報インディケーターを他のセキュリティー・イベントおよび使用状況データと相互リファレンスできます。

数日、数週間、または数カ月にもわたる外部脅威データのプロファイルを作成して、アセットおよびアカウントのリスク・レベルを判定し、優先順位を付ける方法を以下の照会に示します。

```
選択
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

アセット情報および構成

脅威および使用状況のインディケーターは、アセット・タイプ、オペレーティング・システム、脆弱性の状況、サーバー・タイプ、分類などのパラメーターによって異なります。

この照会では、拡張検索およびアセット・モデルにより、ロケーションに対する運用上の情報を得ることができます。

Assetproperty 関数はアセットからプロパティー値を取得します。この値を使用してアセット・データを結果に含めることができます。

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

アセット・モデルで拡張検索およびユーザー・アイデンティティー・トラッキングを使用する方法を以下の照会に示します。

AssetUser 関数はアセット・データベースからユーザー名を取得します。

```
SELECT
APPLICATIONNAME(applicationid) as App,
ASSETUSER(sourceip, now()) as srcAssetUser,
COUNT(*) as 'Total Flows'
FROM flows
WHERE srcAssetUser IS NOT NULL
GROUP BY App, srcAssetUser
ORDER BY 'Total Flows' DESC
LAST 3 HOURS
```

ネットワーク・ルックアップ関数

ネットワーク・ルックアップ関数を使用すると、IP アドレスに関連付けられたネットワーク名を取得できます。

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

ルール・ルックアップ関数

ルール・ルックアップ関数を使用すると、ルールの ID からルール名を取得できます。

```
SELECT RULENAME(123) FROM events
```

以下の照会は、特定のルール名をトリガーしたイベントを返します。

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

全文検索

「**拡張検索**」オプションを使用すると、TEXT SEARCH 演算子を使用して全文検索を実行できます。

この例では、ペイロードに「firewall」という単語が含まれる多数のイベントがあるとします。「**ログ・アクティビティー**」タブで「**クイック・フィルター**」オプションおよび「**拡張検索**」オプションを使用して、これらのイベントを検索できます。

- 「**クイック・フィルター**」オプションを使用するには、「**クイック・フィルター**」ボックスに 'firewall' というテキストを入力します。
- 「**拡張検索**」オプションを使用するには、「**拡張検索**」ボックスに次の照会を入力します。

  ```
  SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
  ```

カスタム・プロパティー

「**拡張検索**」オプションを使用すると、イベントおよびフローのカスタム・プロパティーにアクセスできます。

次の照会では、カスタム・プロパティー「MyWebsiteUrl」を使用して、特定 Web URL を基準にイベントをソートしています。

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

関連概念:

『クイック・フィルターの検索オプション』
イベントおよびフローのペイロードを検索するには、単純な語句を使用してテキスト検索ストリングを入力します。

関連タスク:

204 ページの『正規表現ベースのカスタム・プロパティーの作成』
イベントまたはフローのペイロードを正規表現と突き合わせる正規表現ベースのカスタム・プロパティーを作成できます。

クイック・フィルターの検索オプション

イベントおよびフローのペイロードを検索するには、単純な語句を使用してテキスト検索ストリングを入力します。

検索のフィルター操作は以下の場所で行えます。

「ログ・アクティビティー」ツールバーおよび「ネットワーク・アクティビティー」ツールバー

「**検索**」ツールバーのリスト・ボックスから「**クイック・フィルター**」を選択し、テキスト検索ストリングを入力します。「**クイック・フィルター**」アイコンをクリックして、「**クイック・フィルター**」をイベントまたはフローのリストに適用します。

「フィルターの追加」ダイアログ・ボックス

「**ログ・アクティビティー**」タブまたは「**ネットワーク・アクティビティー**」タブで「**フィルターの追加**」アイコンをクリックします。

フィルター・パラメーターとして「**クイック・フィルター**」を選択し、テキスト検索ストリングを入力します。

フロー検索ページ
クイック・フィルターをフィルターのリストに追加します。

リアルタイム (ストリーミング) または最後の間隔モードで「**フロー**」を表示する場合は、単純な語句のみを「**クイック・フィルター**」フィールドに入力できます。時刻範囲内の「**イベント**」 または「**フロー**」を表示する場合は、以下の構文ガイドラインに従ってください。

表 41. クイック・フィルターの構文ガイドライン

説明	例
ペイロードで検索する任意のプレーン・テキストを含める。	`Firewall`
完全一致の語句を検索するには、複数の用語を二重引用符で囲む。	`"Firewall deny"`
単一文字ワイルドカードと複数文字ワイルドカードを含める。検索語の先頭にワイルドカードを使用することはできません。	`F?rewall` または `F??ew*`
論理式 (AND、OR、NOT など) で用語をグループ化する。構文および演算子を検索語ではなく論理式として認識させるには、大文字でなければなりません。	`(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`
NOT 論理式を含む検索条件を作成する場合は、他のタイプの論理式を少なくとも 1 つ含める必要があります。さもなければ結果が返されません。	`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
以下の文字が検索語の一部であることを示すには、その文字の前に円記号 (¥) を付ける必要があります。`+ - && || ! () {} [] ^ " ~ * ? : ¥`	`"%PIX¥-5¥-304001"`

検索語は、ペイロード語句の先頭文字から順に突き合わせされます。検索語 `user` は `user_1` および `user_2` に一致しますが、語句 `ruser`、`myuser`、`anyuser` には一致しません。

クイック・フィルター検索では英語ロケールが使用されます。*ロケール*は、言語や地理学上の地域を識別するため、および照合、ケース変換、文字種別、メッセージの言語、日付と時刻/時間の表記、数値の表記などの書式設定規則を判別するための設定です。

ロケールはオペレーティング・システムにより設定されます。オペレーティング・システムのロケール設定をオーバーライドするように QRadar を構成できます。例えば、ロケールを「**英語**」に設定し、QRadar コンソールを「**イタリア語**」に設定できます。

クイック・フィルター検索照会で Unicode 文字を使用すると、予期しない検索結果が返される場合があります。

英語以外のロケールを選択する場合、イベントおよびペイロード・データを検索するために、QRadar で「拡張検索」オプションを使用できます。

関連概念:

167 ページの『第 9 章 データの検索』
「**ログ・アクティビティー**」タブ、「**ネットワーク・アクティビティー**」タブ、および「**オフェンス**」タブで特定の基準を使用して、イベント、フロー、およびオフェンスを検索することができます。

175 ページの『拡張検索オプション』
必要なフィールドと、照会を実行するためのグループ化方法を指定する Ariel 照会言語 (AQL) を入力するには、「**拡張検索**」フィールドを使用します。

177 ページの『AQL 検索ストリングの例』
Ariel データベースのイベント、フロー、および simarc 表の特定のフィールドを検索するには、Ariel 照会言語 (AQL) を使用します。

関連タスク:

18 ページの『ユーザー設定の更新』
ロケールなどのユーザー設定を、メインの IBM Security QRadar SIEM ユーザー・インターフェースで設定できます。

オフェンスの検索

特定の基準を使用してオフェンスを検索し、検索条件に一致するオフェンスを結果リストに表示することができます。

新しい検索を作成することも、以前に保存された一連の検索条件をロードすることもできます。

「自分のオフェンス」および「すべてのオフェンス」ページでのオフェンスの検索

「**オフェンス**」タブの「自分のオフェンス」および「すべてのオフェンス」ページで、指定した基準と一致するオフェンスを検索することができます。

このタスクについて

以下の表に、「**自分のオフェンス**」および「**すべてのオフェンス**」ページでオフェンス・データを検索する際に使用できる検索オプションを示します。

カテゴリーについては、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

表 42. 「自分のオフェンス」および「すべてのオフェンス」ページの検索オプション

オプション	説明
グループ	このリスト・ボックスでは、「**使用可能な保存済み検索**」リストに表示するオフェンス検索グループを選択できます。

表 42. 「自分のオフェンス」および「すべてのオフェンス」ページの検索オプション (続き)

オプション	説明
保存済み検索の入力またはリストから選択	このフィールドには、保存済み検索の名前を入力するか、「**使用可能な保存済み検索**」リストをフィルタリングするためのキーワードを入力できます。
使用可能な保存済み検索	このリストには、「グループ」または「保存済み検索の入力またはリストから選択」オプションを使用してリストにフィルターを適用しない限り、使用可能なすべての検索が表示されます。このリストで、表示または編集する保存済み検索を選択することができます。
すべてのオフェンス	このオプションでは、時刻範囲に関係なくすべてのオフェンスを検索することができます。
最新	このオプションでは、フィルターとして使用する定義済みの時刻範囲を選択することができます。このオプションを選択した後に、リスト・ボックスから時刻範囲のオプションを選択する必要があります。
特定の間隔	このオプションでは、検索に対してカスタムの時刻範囲を構成することができます。このオプションを選択した後に、次のいずれかのオプションを選択する必要があります。 • **「開始日が次の期間内にある」** - 特定の期間に開始されたオフェンスを検索する場合は、このチェック・ボックスを選択します。このチェック・ボックスを選択した後に、リスト・ボックスで検索する日付を選択します。 • **「最後のイベント/フローが次の期間内に発生」** - 最後に検出されたイベントが特定の期間内に発生しているオフェンスを検索する場合は、このチェック・ボックスを選択します。このチェック・ボックスを選択した後に、リスト・ボックスで検索する日付を選択します。
検索	「**検索**」アイコンは、検索ページの複数のペインで使用できます。検索の構成が終了したら、「**検索**」をクリックして結果を表示することができます。
オフェンス ID (Offense Id)	このフィールドには、検索するオフェンス ID を入力できます。
説明	このフィールドには、検索する説明を入力できます。
割り当て先ユーザー (Assigned to user)	このリスト・ボックスから、検索するユーザー名を選択できます。

表 42. 「自分のオフェンス」および「すべてのオフェンス」ページの検索オプション (続き)

オプション	説明
方向 (Direction)	このリスト・ボックスから、検索するオフェンスの方向を選択できます。オプションは、以下のとおりです。 • ローカルからローカル • ローカルからリモート • リモートからローカル • リモートからリモート • ローカルからリモートまたはローカル • リモートからリモートまたはローカル
送信元 IP	このフィールドには、検索対象の送信元 IP アドレスまたは CIDR 範囲を入力できます。
宛先 IP	このフィールドには、検索する宛先 IP アドレスまたは CIDR 範囲を入力できます。
マグニチュード	このリスト・ボックスから、マグニチュードを指定し、マグニチュードが設定値と等しい、設定値より小さい、または設定値より大きいオフェンスのみを表示するように選択できます。範囲は 0 から 10 です。
重大度	このリスト・ボックスから、重大度を指定し、重大度が設定値と等しい、設定値より小さい、または設定値より大きいオフェンスのみを表示するように選択できます。範囲は 0 から 10 です。
信頼性	このリスト・ボックスから、信頼性を指定し、信頼性が設定値と等しい、設定値より小さい、または設定値より大きいオフェンスのみを表示するように選択できます。範囲は 0 から 10 です。
関連性	このリスト・ボックスから、関連性を指定し、関連性が設定値と等しい、設定値より小さい、または設定値より大きいオフェンスのみを表示するように選択できます。範囲は 0 から 10 です。
ユーザー名を含む (Contains Username)	このフィールドには、特定のユーザー名を含んでいるオフェンスを検索するための正規表現 (regex) ステートメントを入力できます。カスタムの正規表現パターンを定義する場合は、Java™ プログラミング言語で規定されている正規表現のルールに従ってください。詳しくは、Web で提供されている正規表現のチュートリアルを参照してください。
送信元ネットワーク	このリスト・ボックスから、検索する送信元ネットワークを選択できます。
宛先ネットワーク	このリスト・ボックスから、検索する宛先ネットワークを選択できます。

表 42. 「自分のオフェンス」および「すべてのオフェンス」ページの検索オプション (続き)

オプション	説明
上位カテゴリー	このリスト・ボックスから、検索する上位カテゴリーを選択できます。
下位カテゴリー	このリスト・ボックスから、検索する下位カテゴリーを選択できます。
除外	このペインのオプションを使用して、検索結果から除外するオフェンスを指定できます。オプションは、以下のとおりです。 • アクティブなオフェンス • 非表示のオフェンス • クローズされたオフェンス • 非アクティブなオフェンス • 保護されたオフェンス
クローズしたユーザー	このパラメーターは、「除外」ペインで「**クローズされたオフェンス**」チェック・ボックスをクリアした場合にのみ表示されます。 このリスト・ボックスから、クローズされたオフェンスの検索対象となるユーザー名を選択するか、または「**すべて**」を選択してクローズされたオフェンスをすべて表示できます。
クローズの理由 (Reason For Closing)	このパラメーターは、「除外」ペインで「**クローズされたオフェンス**」チェック・ボックスをクリアした場合にのみ表示されます。 このリスト・ボックスから、クローズされたオフェンスの検索対象となる理由を選択するか、または「**すべて**」を選択してクローズされたオフェンスをすべて表示できます。
イベント数 (Events)	このリスト・ボックスから、イベント数を指定し、イベント数が設定値と等しい、設定値より小さい、または設定値より大きいオフェンスのみを表示するように選択できます。
フロー	このリスト・ボックスから、フロー数を指定し、フロー数が設定値と等しい、設定値より小さい、または設定値より大きいオフェンスのみを表示するように選択できます。
イベント/フローの総数	このリスト・ボックスから、イベントとフローの総数を指定し、イベントとフローの総数が設定値と等しい、設定値より小さい、または設定値より大きいオフェンスのみを表示するように選択できます。

表 42. 「自分のオフェンス」および「すべてのオフェンス」ページの検索オプション (続き)

オプション	説明
宛先数 (Destinations)	このリスト・ボックスから、宛先 IP アドレス数を指定し、宛先 IP アドレス数が設定値と等しい、設定値より小さい、または設定値より大きいオフェンスのみを表示するように選択できます。
ログ・ソース・グループ	このリスト・ボックスから、検索するログ・ソースを含んでいるログ・ソース・グループを選択できます。「**ログ・ソース**」リスト・ボックスには、選択したログ・ソース・グループに割り当てられているすべてのログ・ソースが表示されます。
ログ・ソース	このリスト・ボックスから、検索するログ・ソースを選択できます。
ルール・グループ (Rule Group)	このリスト・ボックスから、検索する要因ルールを含んでいるルール・グループを選択できます。「**ルール**」リスト・ボックスには、選択したルール・グループに割り当てられているすべてのルールが表示されます。
ルール	このリスト・ボックスから、検索する要因ルールを選択できます。
オフェンスのタイプ	このリスト・ボックスから、検索するオフェンスのタイプを選択できます。「**オフェンスのタイプ**」リスト・ボックスのオプションについて詳しくは、表 31 を参照してください。

以下の表に、「**オフェンスのタイプ (Offense Type)**」リスト・ボックスで選択可能なオプションを示します。

表 43. 「オフェンスのタイプ (Offense Type)」のオプション

オフェンスのタイプ	説明
すべて	このオプションでは、オフェンスの送信元がすべて検索されます。
送信元 IP	特定の送信元 IP アドレスでオフェンスを検索する場合は、このオプションを選択し、検索する送信元 IP アドレスを入力します。
宛先 IP	特定の宛先 IP アドレスでオフェンスを検索する場合は、このオプションを選択し、検索する宛先 IP アドレスを入力します。

表 43. 「オフェンスのタイプ (Offense Type)」のオプション (続き)

オフェンスのタイプ	説明
イベント名	特定のイベント名でオフェンスを検索する場合は、「**参照**」アイコンをクリックしてイベント・ブラウザーを開き、検索するイベント名 (QID) を選択します。 特定の QID を検索するには、次のいずれかのオプションを使用します。 • QID をカテゴリーで検索する場合は、「**カテゴリー別に参照 (Browse by Category)**」チェック・ボックスを選択し、リスト・ボックスから上位カテゴリーまたは下位カテゴリーを選択します。 • • QID をログ・ソース・タイプで検索する場合は、「**ログ・ソース・タイプ別に参照 (Browse by Log Source Type)**」チェック・ボックスを選択し、「**ログ・ソース・タイプ**」リスト・ボックスからログ・ソース・タイプを選択します。 • QID を名前別に検索する場合は、「**QID の検索 (QID Search)**」チェック・ボックスを選択し、「**QID/名前**」フィールドに名前を入力します。
ユーザー名	特定のユーザー名でオフェンスを検索する場合は、このオプションを選択し、検索するユーザー名を入力します。
送信元 MAC アドレス	特定の送信元 MAC アドレスでオフェンスを検索する場合は、このオプションを選択し、検索する送信元 MAC アドレスを入力します。
宛先 MAC アドレス	特定の宛先 MAC アドレスでオフェンスを検索する場合は、このオプションを選択し、検索する宛先 MAC アドレスを入力します。
ログ・ソース	「**ログ・ソース・グループ**」リスト・ボックスから、検索するログ・ソースを含んでいるログ・ソース・グループを選択できます。「**ログ・ソース**」リスト・ボックスには、選択したログ・ソース・グループに割り当てられているすべてのログ・ソースが表示されます。 「**ログ・ソース**」リスト・ボックスから、検索するログ・ソースを選択できます。
ホスト名	特定のホスト名でオフェンスを検索する場合は、このオプションを選択し、検索するホスト名を入力します。

表 43. 「オフェンスのタイプ (Offense Type)」のオプション (続き)

オフェンスのタイプ	説明
送信元ポート	特定の送信元ポートでオフェンスを検索する場合は、このオプションを選択し、検索する送信元ポートを入力します。
宛先ポート	特定の宛先ポートでオフェンスを検索する場合は、このオプションを選択し、検索する宛先ポートを入力します。
送信元 IPv6	特定の送信元 IPv6 アドレスでオフェンスを検索する場合は、このオプションを選択し、検索する送信元 IPv6 アドレスを入力します。
宛先 IPv6	特定の宛先 IPv6 アドレスでオフェンスを検索する場合は、このオプションを選択し、検索する宛先 IPv6 アドレスを入力します。
送信元 ASN	特定の送信元 ASN でオフェンスを検索する場合は、「**送信元 ASN**」リスト・ボックスから送信元 ASN を選択できます。
宛先 ASN	特定の宛先 ASN でオフェンスを検索する場合は、「**宛先 ASN**」リスト・ボックスから宛先 ASN を選択できます。
ルール	特定のルールに関係しているオフェンスを検索する場合は、検索するルールを含んでいるルール・グループを「**ルール・グループ (Rule Group)**」リスト・ボックスから選択できます。「**ルール・グループ (Rule Group)**」リスト・ボックスには、選択したルール・グループに割り当てられているすべてのルールが表示されます。「**ルール**」リスト・ボックスから、検索するルールを選択できます。
アプリケーション・アイデンティティー	アプリケーション ID でオフェンスを検索する場合は、「**アプリケーション・アイデンティティー**」リスト・ボックスからアプリケーション ID を選択できます。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**検索**」リスト・ボックスから、「**新規検索**」を選択します。
3. 次のオプションのいずれかを選択してください。
   - 以前に保存した検索をロードする場合は、ステップ 4 に進みます。
   - 新規に検索を作成する場合は、ステップ 7 に進みます。
4. 次のいずれかのオプションを使用して、以前に保存した検索を選択します。
   - 「**使用可能な保存済み検索**」リストから、ロードする保存済み検索を選択します。

- 「**保存済み検索の入力またはリストから選択**」フィールドに、ロードする検索の名前を入力します。

5. 「**ロード**」をクリックします。
6. オプション。この検索をデフォルトの検索として設定する場合は、「検索の編集」ペインで「**デフォルトとして設定**」チェック・ボックスを選択します。この検索をデフォルトの検索として設定すると、「**オフェンス**」タブにアクセスするたびに、この検索が自動的に実行されて結果が表示されます。
7. 「時刻範囲」ペインで、この検索用にキャプチャーする時刻範囲のオプションを選択します。表 1 を参照してください。
8. 「検索パラメーター」ペインで、具体的な検索条件を定義します。表 30 を参照してください。
9. 「オフェンスの送信元」ペインで、検索するオフェンスのタイプおよびオフェンスの送信元を指定します。
   a. リスト・ボックスから、検索するオフェンスのタイプを選択します。
   b. 検索パラメーターを入力します。表 31 を参照してください。
10. 「列定義」ペインで、結果をソートする順序を定義します。
    a. 最初のリスト・ボックスから、検索結果のソート基準となる列を選択します。
    b. 2 番目のリスト・ボックスから、検索結果を表示する順序を選択します。指定可能なオプションは、「降順」と「昇順」です。
11. 「**検索**」をクリックします。

次のタスク

「オフェンス」タブでの検索条件の保存

「送信元 IP 別」ページでのオフェンスの検索

このトピックでは、「**オフェンス**」タブの「**送信元 IP 別**」ページでのオフェンスの検索手順について説明します。

このタスクについて

以下の表では、「送信元 IP 別」ページでオフェンス・データを検索するために使用できる検索オプションについて説明します。

表 44. 「送信元 IP 別」ページの検索オプション

オプション	説明
すべてのオフェンス	このオプションを選択することで、時刻範囲に関係なく、すべての送信元 IP アドレスを検索できます。
最新	このオプションを選択し、このリスト・ボックスから、検索対象の時刻範囲を選択することができます。

表 44. 「送信元 IP 別」ページの検索オプション (続き)

オプション	説明
特定の間隔	検索間隔を指定する場合は、「特定の間隔」オプションを選択してから、以下のオプションのいずれかを選択できます。 • **開始日が次の期間内にある** - このチェック・ボックスを選択すると、一定期間内に開始されたオフェンスに関連付けられている送信元 IP アドレスが検索されます。このチェック・ボックスを選択したら、リスト・ボックスを使用して、検索対象の日付を選択します。 • **最後のイベント/フローが次の期間内に発生** - このチェック・ボックスを選択すると、一定期間内に発生し、最後に検出されたイベントに関するオフェンスに関連付けられている送信元 IP アドレスが検索されます。このチェック・ボックスを選択したら、リスト・ボックスを使用して、検索対象の日付を選択します。
検索	「**検索**」アイコンは、検索ページの複数のペインで使用できます。検索の構成が終了したら、「**検索**」をクリックして結果を表示することができます。
送信元 IP	このフィールドには、検索対象の送信元 IP アドレスまたは CIDR 範囲を入力できます。
マグニチュード	このリスト・ボックスから、マグニチュードを指定して、構成値と等しい、より小さい、またはより大きいマグニチュードのオフェンスのみを表示するように選択できます。範囲は 0 から 10 です。
VA リスク	このリスト・ボックスから、VA リスクを指定して、構成値と等しい、より小さい、またはより大きい VA リスクのオフェンスのみを表示するように選択できます。範囲は 0 から 10 です。
イベント/フロー	このリスト・ボックスから、イベントまたはフローの数を指定して、構成値と等しい、より小さい、またはより大きいマグニチュードのオフェンスのみを表示するように選択できます。

表 44. 「送信元 IP 別」ページの検索オプション (続き)

オプション	説明
除外	検索結果から除外するオフェンスのチェック・ボックスを選択できます。オプションは以下のとおりです。 • **アクティブなオフェンス** • **非表示のオフェンス** • **クローズされたオフェンス** • **非アクティブなオフェンス** • **保護されたオフェンス**

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**送信元 IP 別**」をクリックします。
3. 「**検索**」リスト・ボックスから、「**新規検索**」を選択します。
4. 「時刻範囲」ペインで、この検索用にキャプチャーする時刻範囲のオプションを選択します。表 1 を参照してください。
5. 「検索パラメーター」ペインで、具体的な検索条件を定義します。表 1 を参照してください。
6. 「列定義」ペインで、次のようにして、結果のソート順を定義します。
   a. 最初のリスト・ボックスから、検索結果のソート基準となる列を選択します。
   b. 2 番目のリスト・ボックスから、検索結果を表示する順序を選択します。指定可能なオプションは、「**降順**」と「**昇順**」です。
7. 「**検索**」をクリックします。

次のタスク

「オフェンス」タブでの検索条件の保存

「宛先 IP 別」ページでのオフェンスの検索

「**オフェンス**」タブの「**宛先 IP 別**」ページで、宛先 IP アドレス別にグループ化されているオフェンスを検索することができます。

このタスクについて

以下の表で、「宛先 IP 別」ページでオフェンスを検索するために使用できる検索オプションについて説明します。

表 45. 「宛先 IP 別」ページの検索オプション

オプション	説明
すべてのオフェンス	このオプションを選択することで、時刻範囲に関係なく、すべての宛先 IP アドレスを検索できます。

表 45. 「宛先 IP 別」ページの検索オプション (続き)

オプション	説明
最新	このオプションを選択し、このリスト・ボックスから、検索対象の時刻範囲を選択することができます。
特定の間隔	検索対象の特定の間隔を指定する場合は、「**特定の間隔**」オプションを選択してから、以下のオプションのいずれかを選択できます。 • 検索対象の特定の間隔を指定する場合は、「**特定の間隔**」オプションを選択してから、以下のオプションのいずれかを選択できます。 • **最後のイベント/フローが次の期間内に発生** - このチェック・ボックスを選択すると、一定期間内に発生し、最後に検出されたイベントに関するオフェンスに関連付けられている宛先 IP アドレスが検索されます。このチェック・ボックスを選択した後に、リスト・ボックスで検索する日付を選択します。
検索	「**検索**」アイコンは、検索ページの複数のペインで使用できます。検索の構成が終了したら、「**検索**」をクリックして結果を表示することができます。
宛先 IP	検索対象の宛先 IP アドレスまたは CIDR 範囲を入力できます。
マグニチュード	このリスト・ボックスから、マグニチュードを指定して、構成値と等しい、より小さい、またはより大きいマグニチュードのオフェンスのみを表示するように選択できます。
VA リスク	このリスト・ボックスから、VA リスクを指定して、構成値と等しい、より小さい、またはより大きい VA リスクのオフェンスのみを表示するように選択できます。範囲は 0 から 10 です。
イベント/フロー	このリスト・ボックスから、イベント数またはフロー数のマグニチュードを指定して、構成値と等しい、より小さい、またはより大きいイベント数またはフロー数のオフェンスのみを表示するように選択できます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**宛先 IP 別**」をクリックします。
3. 「**検索**」リスト・ボックスから、「**新規検索**」を選択します。

4. 「時刻範囲」ペインで、この検索用にキャプチャーする時刻範囲のオプションを選択します。表 1 を参照してください。
5. 「検索パラメーター」ペインで、具体的な検索条件を定義します。表 1 を参照してください。
6. 「列定義」ペインで、次のようにして、結果のソート順を定義します。
   a. 最初のリスト・ボックスから、検索結果のソート基準となる列を選択します。
   b. 2 つ目のリスト・ボックスから、検索結果の表示順を選択します。指定可能なオプションは、「**降順**」と「**昇順**」です。
7. 「**検索**」をクリックします。

次のタスク

「オフェンス」タブでの検索条件の保存

「ネットワーク別 (By Networks)」ページでのオフェンスの検索

「**オフェンス**」タブの「**ネットワーク別 (By Networks)**」ページで、関連ネットワーク別にグループ化されているオフェンスを検索することができます。

このタスクについて

以下の表で、「ネットワーク別」ページでオフェンス・データを検索するために使用できる検索オプションについて説明します。

表 46. 「ネットワーク別」ページでオフェンス・データを検索する場合の検索オプション

オプション	説明
ネットワーク	このリスト・ボックスから、検索対象のネットワークを選択することができます。
マグニチュード	このリスト・ボックスから、マグニチュードを指定して、構成値と等しい、より小さい、またはより大きいマグニチュードのオフェンスのみを表示するように選択できます。
VA リスク	このリスト・ボックスから、VA リスクを指定して、構成値と等しい、より小さい、またはより大きい VA リスクのオフェンスのみを表示するように選択できます。
イベント/フロー	このリスト・ボックスから、イベントまたはフローの数を指定して、構成値と等しい、より小さい、またはより大きいイベントまたはフローの数のオフェンスのみを表示するように選択できます。

手順

1. 「**オフェンス**」タブをクリックします。
2. 「**ネットワーク別 (By Networks)**」をクリックします。
3. 「**検索**」リスト・ボックスから、「**新規検索**」を選択します。

4. 「検索パラメーター」ペインで、具体的な検索条件を定義します。表 1 を参照してください。
5. 「列定義」ペインで、次のようにして、結果のソート順を定義します。
   a. 最初のリスト・ボックスから、検索結果のソート基準となる列を選択します。
   b. 2 つ目のリスト・ボックスから、検索結果の表示順を選択します。指定可能なオプションは、「**降順**」と「**昇順**」です。
6. 「**検索**」をクリックします。

次のタスク

「オフェンス」タブでの検索条件の保存

「オフェンス」タブでの検索条件の保存

「**オフェンス**」タブでは、構成した検索条件を、今後の検索で再使用できるように保存することができます。保存済み検索条件の有効期限が切れることはありません。

手順

1. 手順
2. 検索を実行します。『オフェンスの検索』を参照してください。
3. 「**条件の保存**」をクリックします。
4. 次の各パラメーターの値を入力します。

オプション	**説明**
パラメーター	説明
検索名	この検索条件に割り当てる名前を入力します。
グループの管理	検索グループを管理するには、「**グループの管理**」をクリックします。『検索グループの管理』を参照してください。

オプション	説明
期間オプション: (Timespan options:)	次のオプションのいずれかを選択してください。 • 「**すべてのオフェンス**」 - 時刻範囲に関係なくすべてのオフェンスを検索する場合は、このオプションを選択します。 • 「**最新**」 - このオプションを選択する場合は、リスト・ボックスで検索する時刻範囲を選択します。 • 「**特定の間隔**」 - 検索する特定の間隔を指定するには、「**特定の間隔**」 オプションを選択してから、次のいずれかのオプションを選択します。「開始日が次の期間内にある」 - 特定の期間に開始されたオフェンスを検索するには、このチェック・ボックスを選択します。このチェック・ボックスを選択した後に、リスト・ボックスで検索する日付を選択します。「最後のイベント/フローが次の期間内に発生」 - 特定の期間内で最後に検出されたイベントの発生対象となったオフェンスを検索するには、このチェック・ボックスを選択します。このチェック・ボックスを選択した後は、リスト・ボックスを使用して、検索する日付を選択してください。「最後のイベントが次の期間内に発生 (Last Event between)」 - 特定の期間内で最後に検出されたイベントの発生対象となったオフェンスを検索するには、このチェック・ボックスを選択します。このチェック・ボックスを選択した後に、リスト・ボックスで検索する日付を選択します。
デフォルトとして設定	この検索をデフォルトの検索として設定する場合は、このチェック・ボックスを選択します。

5. 「**OK**」をクリックします。

検索条件の削除

検索条件を削除することができます。

このタスクについて

保存済み検索を削除すると、その保存済み検索に関連付けられているオブジェクトが機能しなくなることがあります。保存済み検索条件を使用する QRadar オブジェクトには、レポートやアノマリ検出ルールがあります。保存済み検索を削除した後に、関連するオブジェクトを編集して引き続き機能するようにしてください。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」リスト・ボックスから、「**新規検索**」または「**検索の編集**」を選択します。
3. 「保存済み検索 (Saved Searches)」ペインで、「**使用可能な保存済み検索**」リスト・ボックスから保存済み検索を選択します。
4. 「**削除**」をクリックします。
   - この保存済み検索条件が他の QRadar オブジェクトに関連付けられていない場合は、確認ウィンドウが表示されます。
   - この保存済み検索条件が他のオブジェクトに関連付けられている場合は、「保存済み検索の削除 (Delete Saved Search)」ウィンドウが表示されます。このウィンドウには、削除する保存済み検索に関連付けられているオブジェクトがリストされます。関連付けられているオブジェクトを書き留めます。
5. 「**OK**」をクリックします。
6. 次のオプションのいずれかを選択してください。
   - 「**OK**」をクリックして処理を進めます。
   - 「**キャンセル**」をクリックして「保存済み検索の削除 (Delete Saved Search)」ウィンドウを閉じます。

次のタスク

保存済み検索条件が他の QRadar オブジェクトに関連付けられていた場合は、書き留めた関連オブジェクトにアクセスし、削除した保存済み検索との関連を削除するか、または置換するようにそのオブジェクトを編集します。

検索結果を詳細化するサブ検索の使用

サブ検索を使用して、一連の完了した検索結果内で検索を実行することができます。サブ検索は、データベースを再度検索せずに検索結果を詳細化するために使用します。

始める前に

サブ検索のベースとして使用する検索を定義する際には、必ず「リアルタイム (ストリーミング) (Real Time (streaming))」オプションを無効にして、検索がグループ化されないようにしてください。

このタスクについて

この機能は、グループ化された検索、進行中の検索、またはストリーム・モードの検索には使用できません。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。

- 「**ネットワーク・アクティビティー**」タブをクリックします。

2. 検索を実行します。
3. 検索が完了したら、以下のようにして他のフィルターを追加します。
   a. 「**フィルターの追加**」をクリックします。
   b. 最初のリスト・ボックスから、検索対象のパラメーターを選択します。
   c. 2 番目のリスト・ボックスから、検索に使用する修飾子を選択します。使用可能な修飾子のリストは、最初のリストで選択された属性によって異なります。
   d. 入力フィールドに、検索に関連する具体的な情報を入力します。
   e. 「**フィルターの追加**」をクリックします。

タスクの結果

「元のフィルター」ペインに、ベース検索に適用する元のフィルターが示されます。「現在のフィルター」ペインには、サブ検索に適用するフィルターが示されます。ベース検索を再開せずにサブ検索フィルターをクリアすることができます。クリアするフィルターの隣にある「**フィルターのクリア**」リンクをクリックします。「元のフィルター」ペインからフィルターをクリアすると、ベース検索が再実行されます。

保存したサブ検索条件のベース検索条件を削除しても、保存したサブ検索条件には引き続きアクセス可能です。フィルターを追加すると、サブ検索機能による検索は以前に検索されたデータ・セットにはもはや基づかなくなるため、サブ検索はデータベース全体を検索します。

次のタスク

検索条件の保存

検索結果の管理

複数の検索を開始し、これらの検索がバックグラウンドで実行されている間に他のタブにナビゲートして他のタスクを実行することができます。

検索の完了時に E メール通知を受信するように検索を構成することができます。

検索の実行中にいつでも「**ログ・アクティビティー**」タブまたは「**ネットワーク・アクティビティー**」タブに戻って、検索結果の一部または全部を表示することができます。

検索のキャンセル

検索がキューに入れられている間か、または進行中の間は、「検索結果の管理」ページでこの検索をキャンセルすることができます。

このタスクについて

検索をキャンセルした際にその検索が進行中の場合、その累積された検索結果は取り消されるまで保持されます。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」メニューから、「**検索結果の管理**」を選択します。
3. キャンセルする、キューに入れられたか、または進行中の検索結果を選択します。
4. 「**キャンセル**」をクリックします。
5. 「**はい**」をクリックします。

検索結果の削除

検索結果が不要となった場合は、「検索結果の管理」ページからその検索結果を削除できます。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」メニューから、「**検索結果の管理**」を選択します。
3. 削除する検索結果を選択します。
4. 「**削除**」をクリックします。
5. 「**はい**」をクリックします。

検索グループの管理

「検索グループ (Search Groups)」ウィンドウを使用して、イベント検索グループ、フロー検索グループ、およびオフェンス検索グループの作成を管理を行うことができます。

これらのグループを使用すると、「**ログ・アクティビティー**」タブ、「**ネットワーク・アクティビティー**」タブ、「**オフェンス**」タブ、「レポート」ウィザードで、保存済み検索条件を簡単に探すことができます。

検索グループの表示

グループとサブグループのデフォルト・セットを使用することができます。

このタスクについて

「イベント検索グループ」、「フロー検索グループ」、または「オフェンス検索グループ」の各ウィンドウで検索グループを表示することができます。

グループに割り当てられていない保存済み検索はすべて「**その他**」グループに含まれます。

「イベント検索グループ」、「フロー検索グループ」、および「オフェンス検索グループ」ウィンドウには、各グループの以下のパラメーターが表示されます。

表 47. 検索グループ・ウィンドウのパラメーター

パラメーター	説明
名前	検索グループの名前を指定します。
ユーザー (User)	検索グループを作成したユーザーの名前を示します。
説明	検索グループの説明を指定します。
変更日 (Date Modified)	検索グループが変更された日付を示します。

「イベント検索グループ」、「フロー検索グループ」、および「オフェンス検索グループ」の各ウィンドウ・ツールバーでは、以下の機能が提供されます。

表 48. 検索グループ・ウィンドウ・ツールバーの機能

機能	説明
新規グループ	新規検索グループを作成する場合は、「**新規グループ**」をクリックできます。新規検索グループの作成を参照してください。
編集	既存の検索グループを編集する場合は、「**編集**」をクリックできます。検索グループの編集を参照してください。
コピー	保存済み検索を別の検索グループにコピーする場合は、「**コピー**」をクリックできます。別のグループへの保存済み検索のコピーを参照してください。
削除	検索グループ、または検索グループから保存済み検索を削除するには、削除する項目を選択してから、「**削除**」をクリックします。グループ、またはグループからの保存済み検索の削除を参照してください。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」 >「**検索の編集**」を選択します。
3. 「**グループの管理**」をクリックします。
4. 検索グループを表示します。

新規検索グループの作成

新規検索グループを作成することができます。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」 > 「**検索の編集**」を選択します。

3. 「**グループの管理**」をクリックします。
4. 新規グループをあるグループの下に作成するために、その上位のグループのフォルダーを選択します。
5. 「**新規グループ**」をクリックします。
6. 「**名前**」フィールドに、新規グループの固有の名前を入力します。
7. オプション。「**説明**」フィールドに、説明を入力します。
8. 「**OK**」をクリックします。

検索グループの編集

検索グループの「**名前**」フィールドおよび「**説明**」フィールドを編集できます。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」 > 「**検索の編集**」を選択します。
3. 「**グループの管理**」をクリックします。
4. 編集するグループを選択します。
5. 「**編集**」をクリックします。
6. パラメーターを以下のように編集します。
   - 「**名前**」フィールドに新しい名前を入力します。
   - 「**説明**」フィールドに新しい説明を入力します。
7. 「**OK**」をクリックします。

保存済み検索の別のグループへのコピー

保存済み検索は、1 つ以上のグループにコピーすることができます。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」 > 「**検索の編集**」を選択します。
3. 「**グループの管理**」をクリックします。
4. コピーする保存済み検索を選択します。
5. 「**コピー**」をクリックします。
6. 「項目グループ」ウィンドウで、保存済み検索のコピー先グループのチェック・ボックスを選択します。
7. 「**グループの割り当て**」をクリックします。

グループの削除またはグループからの保存済み検索の削除

「**削除**」アイコンを使用して、グループから検索を削除したり、検索グループを削除することができます。

このタスクについて

グループから保存済み検索を削除しても、その保存済み検索はシステムからは削除されません。保存済み検索は、グループから削除され、自動的に「**その他**」グループに移動されます。

次のグループはシステムから削除できません。

- イベント検索グループ
- フロー検索グループ
- オフェンス検索グループ
- その他

手順

1. 次のオプションのいずれかを選択してください。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」 > 「**検索の編集**」を選択します。
3. 「**グループの管理**」をクリックします。
4. 次のオプションのいずれかを選択してください。
   - グループから削除する保存済み検索を選択します。
   - 削除するグループを選択します。
5. 「**削除**」をクリックします。
6. 「**OK**」をクリックします。

第 10 章 カスタム・イベント・プロパティーとカスタム・フロー・プロパティー

カスタム・イベント・プロパティーとカスタム・フロー・プロパティーを使用して、通常は QRadar によって正規化も表示もされないログ内の情報について、検索、表示、および報告します。

カスタム・イベント・プロパティーとカスタム・フロー・プロパティーは、「**ログ・アクティビティー**」タブまたは「**ネットワーク・アクティビティー**」タブの複数の場所で作成することができます。

- 「**ログ・アクティビティー**」タブで、イベントをダブルクリックし、「**プロパティーの抽出**」をクリックします。
- 「**ネットワーク・アクティビティー**」タブで、フローをダブルクリックし、「**プロパティーの抽出**」をクリックします。
- 「検索」ページで、カスタム・イベント・プロパティーまたはカスタム・フロー・プロパティーの作成や編集を行うことができます。「検索」ページでカスタム・プロパティーを作成すると、そのプロパティーは特定のイベントやフローから派生したものではないため、「カスタム・イベント・プロパティー」ウィンドウにはデータが事前に取り込まれません。他のソースからペイロード情報をコピーして貼り付けることができます。

必要な権限

カスタム・プロパティーを作成するには、適切な権限が必要です。

ユーザー定義のイベント・プロパティー権限またはユーザー定義のフロー・プロパティー権限が必要です。

管理権限がある場合は、「管理」タブからカスタム・プロパティーの作成および変更を行うこともできます。

「**管理**」 > 「**データ・ソース**」 > 「**カスタム・イベント・プロパティー**」 > 、または「**管理**」 > 「**データ・ソース**」 > 「**カスタム・フロー・プロパティー**」をクリックします。

管理者に連絡を取って、正しい権限を得ていることを確認してください。

詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

カスタム・プロパティー・タイプ

カスタム・プロパティーのタイプを作成することができます。

カスタム・プロパティーを作成する際に、Regex プロパティー・タイプまたは計算プロパティー・タイプのいずれかを選択することができます。

正規表現 (Regex) ステートメントを使用することにより、イベントまたはフローのペイロードから、正規化されていないデータを抽出することができます。

例えば、Oracle サーバーでユーザー権限の変更を行うすべてのユーザーを報告するレポートが作成されます。その際、ユーザーのリストと、それらのユーザーが他のアカウントの権限を変更した回数が報告されます。ただし通常は、変更された実際のユーザー・アカウントや権限を表示することはできません。この情報をログから抽出するためのカスタム・プロパティーを作成し、検索やレポートでそのプロパティーを使用することができます。この機能を使用するには、正規表現 (Regex) に関する十分な知識が必要になります。

Regex は、カスタム・プロパティーとして使用されるフィールドを定義します。Regex ステートメントを入力したら、そのステートメントをペイロードと対比して検証することができます。カスタムの正規表現パターンを定義する場合は、Java プログラミング言語で規定されている正規表現のルールに従ってください。

詳しくは、Web で提供されている正規表現のチュートリアルを参照してください。1 つのカスタム・プロパティーを複数の正規表現と関連付けることができます。

イベントまたはフローを解析する際に、ペイロードに一致する Regex パターンが見つかるまで、各 Regex パターンがそのイベントまたはフローでテストされます。イベントまたはフローのペイロードに一致する最初の Regex パターンにより、抽出されるデータが決まります。

計算ベースのカスタム・プロパティーを使用することにより、既存の数値イベント・プロパティーまたはフロー・プロパティーでの計算を実行して、計算プロパティーを作成することができます。

例えば、ある数値プロパティーを別の数値プロパティーで除算してパーセンテージを表示するプロパティーを作成することができます。

正規表現ベースのカスタム・プロパティーの作成

イベントまたはフローのペイロードを正規表現と突き合わせる正規表現ベースのカスタム・プロパティーを作成できます。

このタスクについて

正規表現ベースのカスタム・プロパティーを構成するときに、「カスタム・イベント・プロパティー」ウィンドウまたは「カスタム・フロー・プロパティー」ウィンドウに、パラメーターが表示されます。一部のパラメーターのリファレンス情報を次の表に示します。

表 49. 「カスタム・イベント・プロパティー」ウィンドウのパラメーター (正規表現)

パラメーター	説明
フィールドのテスト (Test field)	
新規プロパティー (New Property)	新しいプロパティー名に、正規化プロパティーの名前 (username、Source IP、Destination IP など) を使用することはできません。

表 49. 「カスタム・イベント・プロパティー」ウィンドウのパラメーター (正規表現) (続き)

パラメーター	説明
ルール、レポート、および検索の構文解析を最適化 (Optimize parsing for rules, reports, and searches)	イベントまたはフローが最初に受信されたときにプロパティーを解析し格納します。このチェック・ボックスを選択すると、プロパティーはレポート、検索、ルールのテストの構文解析をそれ以上必要としません。 このチェック・ボックスをクリアすると、レポート、検索、またはルールのテストが適用するたびにプロパティーが解析されます。
ログ・ソース	複数のログ・ソースがこのイベントに関連付けられている場合、このフィールドは「複数」という語とログ・ソースの数を指定します。
正規表現	ペイロードからデータを抽出するために使用する正規表現。正規表現では、大/小文字を区別します。 サンプルの正規表現を次の例に示します。 • Email: `(.+@[^¥.].*¥.[a-z]{2,}$)` • URL: `(http¥://[a-zA-Z0-9¥-¥.]+¥.[a-zA-Z]{2,3}(/¥S*)?$)` • ドメイン名: `(http[s]?://(.+?)["/?:])` • 浮動小数点数: `([-+]?¥d*¥.?¥d*$)` • 整数: `([-+]?¥d*$)` • IP アドレス: `(¥b¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥.¥d{1,3}¥b)` キャプチャー・グループは括弧で囲む必要があります。
キャプチャー・グループ	キャプチャー・グループは複数の文字を 1 つの単位として扱います。キャプチャー・グループでは、文字は一連の括弧内でグループ化されます。
有効 (Enabled)	このチェック・ボックスをクリアすると、このカスタム・プロパティーは検索フィルターや列リストに表示されず、このプロパティーはペイロードから構文解析されません。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. イベントまたはフローをストリーム・モードで表示している場合は、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。

3. カスタム・プロパティーの基にするイベントまたはフローをダブルクリックします。
4. カスタム・プロパティーの基にするイベントをダブルクリックします。
5. 「**プロパティーの抽出**」をクリックします。
6. 「**プロパティー・タイプの選択**」ペインで、「**正規表現ベース**」オプションを選択します。
7. カスタム・プロパティーのパラメーターを構成します。
8. 「**テスト (Test)**」をクリックして、正規表現をペイロードと比較してテストします。
9. 「**保存**」をクリックします。

タスクの結果

検索ページの使用可能な列のリストに、カスタム・プロパティーがオプションとして表示されます。カスタム・プロパティーをイベントまたはフローのリストに含めるには、検索の作成時に、使用可能な列のリストからそのカスタム・プロパティーを選択する必要があります。

関連概念:

177 ページの『AQL 検索ストリングの例』
Ariel データベースのイベント、フロー、および simarc 表の特定のフィールドを検索するには、Ariel 照会言語 (AQL) を使用します。

計算ベースのカスタム・プロパティーの作成

計算ベースのカスタム・プロパティーは、ペイロードを正規表現に一致させるように作成することができます。

このタスクについて

計算ベースのカスタム・プロパティーを構成するときに、「カスタム・イベント・プロパティー」ウィンドウまたは「カスタム・フロー・プロパティー」ウィンドウに、次のパラメーターが表示されます。

表 50. 「カスタム・プロパティー定義 (Custom property definition)」ウィンドウのパラメーター (計算)

パラメーター	説明
プロパティー定義	
プロパティー名	このカスタム・プロパティーに固有の名前を入力します。新規のプロパティー名は、「ユーザー名」、「送信元 IP」、「宛先 IP」などの正規化されたプロパティーの名前にはできません。
説明	このカスタム・プロパティーの説明を入力します。
プロパティーの計算の定義	

表 50. 「カスタム・プロパティー定義 (Custom property definition)」ウィンドウのパラメーター (計算) (続き)

パラメーター	説明
プロパティー 1 (Property 1)	リスト・ボックスから、計算で使用する最初のプロパティーを選択します。オプションには、数値の正規化されたカスタム・プロパティーと数値のカスタム・プロパティーがすべて含まれています。 特定の数値を指定することもできます。「**プロパティー 1 (Property 1)**」リスト・ボックスから、「**ユーザー定義 (User Defined)**」オプションを選択します。「**数値プロパティー**」パラメーターが表示されます。特定の数値を入力します。
演算子	リスト・ボックスから、計算で、選択したプロパティーに適用する演算子を選択します。オプションは、以下のとおりです。 • 加算 (Add) • 減算 (Subtract) • 乗算 (Multiply) • 除算 (Divide)
プロパティー 2 (Property 2)	リスト・ボックスから、計算で使用する 2 番目のプロパティーを選択します。オプションには、数値の正規化されたカスタム・プロパティーと数値のカスタム・プロパティーがすべて含まれています。 特定の数値を指定することもできます。「**プロパティー 1 (Property 1)**」リスト・ボックスから、「**ユーザー定義 (User Defined)**」オプションを選択します。「**数値プロパティー**」パラメーターが表示されます。特定の数値を入力します。
有効 (Enabled)	このチェック・ボックスを選択すると、このカスタム・プロパティーが有効化されます。 このチェック・ボックスをクリアすると、このカスタム・プロパティーはイベント検索またはフロー検索のフィルター、あるいは列リストに表示されず、イベント・プロパティーまたはフロー・プロパティーがペイロードから解析されません。

手順

1. 次のいずれかを選択してください。「**ログ・アクティビティー**」タブをクリックします。

2. オプション。イベントまたはフローをストリーム・モードで表示している場合は、「**一時停止**」アイコンをクリックしてストリーミングを一時停止します。
3. カスタム・プロパティーの基にするイベントまたはフローをダブルクリックします。
4. 「**プロパティーの抽出**」をクリックします。
5. 「プロパティー・タイプの選択」ペインで、「**計算ベース**」オプションを選択します。
6. カスタム・プロパティーのパラメーターを構成します。
7. 「**テスト (Test)**」をクリックして、正規表現をペイロードと比較してテストします。
8. 「**保存**」をクリックします。

タスクの結果

検索ページの使用可能な列のリストに、カスタム・プロパティーがオプションとして表示されるようになります。カスタム・プロパティーをイベントまたはフローのリストに組み込むには、検索の作成時に、使用可能な列のリストからこのカスタム・プロパティーを選択する必要があります。

カスタム・プロパティーの変更

カスタム・プロパティーを変更することができます。

このタスクについて

「カスタム・イベント・プロパティー」ウィンドウまたは「カスタム・フロー・プロパティー」ウィンドウを使用して、カスタム・プロパティーを変更することができます。

カスタム・プロパティーについて、以下の表で説明します。

表 51. カスタム・プロパティー・ウィンドウの列

列	説明
プロパティー名	このカスタム・プロパティーに固有の名前を示します。
タイプ (Type)	このカスタム・プロパティーのタイプを示します。
プロパティーの説明 (Property Description)	このカスタム・プロパティーの説明を示します。
ログ・ソース・タイプ	このカスタム・プロパティーを適用するログ・ソース・タイプの名前を示します。 この列は、「カスタム・イベント・プロパティー」ウィンドウにのみ表示されます。

表 51. カスタム・プロパティー・ウィンドウの列 (続き)

列	説明
ログ・ソース	このカスタム・プロパティーが適用されるログ・ソースを示します。 このイベントまたはフローに関連付けられたログ・ソースが複数ある場合、このフィールドには「複数」という語とログ・ソースの数が示されます。 この列は、「カスタム・イベント・プロパティー」ウィンドウにのみ表示されます。
式 (Expression)	このカスタム・プロパティーの式を示します。式はカスタム・プロパティーのタイプによって以下のように異なります。 正規表現ベースのカスタム・プロパティーの場合、このパラメーターはペイロードからデータを抽出するために使用する正規表現を指定します。 計算ベースのカスタム・プロパティーの場合、このパラメーターはカスタム・プロパティー値を生成するために使用する計算式を指定します。
ユーザー名	このカスタム・プロパティーを作成したユーザーの名前を示します。
有効 (Enabled)	このカスタム・プロパティーが有効かどうかを示します。このフィールドには、「True」または「False」のいずれかが表示されます。
作成日	このカスタム・プロパティーが作成された日付を示します。
変更日 (Modification Date)	このカスタム・プロパティーが最後に変更された日付が表示されます。

「カスタム・イベント・プロパティー (Custom Event Property)」および「カスタム・フロー・プロパティー(Custom Flow Property)」ツールバーには、以下の機能があります。

表 52. カスタム・プロパティー・ツールバーのオプション

オプション	説明
追加	新規のカスタム・プロパティーを追加するには、「**追加**」をクリックします。
編集	選択したカスタム・プロパティーを編集するには、「**編集**」をクリックします。
コピー	選択したカスタム・プロパティーをコピーするには、「**コピー**」をクリックします。

表 52. カスタム・プロパティー・ツールバーのオプション (続き)

オプション	説明
削除	選択したカスタム・プロパティーを削除するには、「**削除**」をクリックします。
有効化/無効化	選択したカスタム・プロパティーに対する構文解析の実行、および検索フィルターや列リストでの表示を有効化または無効化するには、「**有効化/無効化**」をクリックします。

手順

1. 次のいずれかを選択します。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」リスト・ボックスから、「**検索の編集**」を選択します。
3. 「**カスタム・プロパティーの管理**」をクリックします。
4. 編集するカスタム・プロパティーを選択して、「**編集**」をクリックします。
5. 必要なパラメーターを編集します。
6. オプション。正規表現を編集した場合は、「**テスト (Test)**」をクリックして、正規表現をペイロードと比較してテストします。
7. 「**保存**」をクリックします。

カスタム・プロパティーのコピー

既存のカスタム・プロパティーに基づいている、新規カスタム・プロパティーを作成するために、既存のカスタム・プロパティーをコピーしてから、パラメーターを変更することができます。

手順

1. 次のいずれかを選択します。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**検索**」リスト・ボックスから、「**検索の編集**」を選択します。
3. 「**カスタム・プロパティーの管理**」をクリックします。
4. コピーするカスタム・プロパティーを選択して、「**コピー**」をクリックします。
5. 必要なパラメーターを編集します。
6. オプション。正規表現を編集した場合は、「**テスト (Test)**」をクリックして、正規表現をペイロードと比較してテストします。
7. 「**保存**」をクリックします。

カスタム・プロパティーの削除

別のカスタム・プロパティーに関連付けられていないカスタム・プロパティーは、削除することができます。

手順

1. 次のいずれかを選択します。
   - 「**ログ・アクティビティー**」タブをクリックします。
   - 「**ネットワーク・アクティビティー**」タブをクリックします。
2. 「**ログ・アクティビティー**」タブをクリックします。
3. 「**検索**」リスト・ボックスから、「**検索の編集**」を選択します。
4. 「**カスタム・プロパティーの管理**」をクリックします。
5. 削除するカスタム・プロパティーを選択し、「**削除**」をクリックします。
6. 「**はい**」をクリックします。

第 11 章 ルールの管理

「**ログ・アクティビティー**」タブ、「**ネットワーク・アクティビティー**」タブ、および「**オフェンス**」タブで、ルールを表示して保守することができます。

このトピックは、「**カスタム・ルールの表示 (View Custom Rules)**」または「**カスタム・ルールの保守**」のユーザー・ロール権限を持つユーザーを対象としています。

ルールの権限の考慮事項

「カスタム・ルールの表示」または「カスタム・ルールの保守」のユーザー・ロール権限を持つユーザーは、自分がアクセスできるネットワークの領域に関するルールを表示および管理することができます。

アノマリ検出ルールを作成するには、ルールを作成したいタブに対して適切な「**カスタム・ルールの保守**」権限を持っている必要があります。例えば、「ログ・アクティビティー」タブでアノマリ検出ルールを作成するには、「**ログ・アクティビティー**」 > 「**カスタム・ルールの保守**」権限が必要です。

ユーザー・ロール権限について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

ルールの概要

ルールは、イベント、フロー、またはオフェンスに対してテストを実行し、すべてのテスト条件が満たされた場合に応答を生成します。

各ルールで実行されるテストは、他のビルディング・ブロックおよびルールを参照することもできます。ルールを特定の順序で作成する必要はありません。新規ルールが追加、編集、または削除されるたびに、システムが依存関係を検査するからです。他のルールによって参照されているルールが削除されたり無効にされたりすると、警告が表示され、いかなるアクションも実行されません。

デフォルト・ルールの完全なリストについては、*IBM Security QRadar SIEM 管理ガイド*を参照してください。

ルールのカテゴリー

ルールには、カスタム・ルールとアノマリ・ルールの 2 つのカテゴリーがあります。

カスタム・ルールは、イベント、フロー、およびオフェンスでテストを実行し、ネットワーク内の異常なアクティビティーを検出します。

アノマリ検出ルールは、ネットワークでアノマリなトラフィック・パターンが発生したときにそれを検出するために、保存済みのフローまたはイベント検索の結果に対してテストを実行します。

アノマリ検出ルールは、ネットワークでアノマリなトラフィック・パターンが発生したときにそれを検出するために、保存済みのフローまたはイベント検索の結果に対してテストを実行します。このルール・カテゴリーには、アノマリ、しきい値、および動作の各ルール・タイプがあります。

アノマリ・ルールは、イベント・トラフィックおよびフロー・トラフィックをテストして、アノマリなアクティビティー (新規または未知のトラフィックの存在など) がないか調べます。このようなアクティビティーとしては、トラフィックの突然の停止や、オブジェクトがアクティブになっている時間の割合の変化などがあります。例えば、最近 5 分間のトラフィックの平均ボリュームを最近 1 時間のトラフィックの平均ボリュームと比較するための、アノマリ・ルールを作成することができます。40% を超える変動があった場合、このルールによって応答が生成されます。

しきい値ルールは、イベント・トラフィックおよびフロー・トラフィックをテストして、構成されたしきい値と比較して小さいアクティビティー、等しいアクティビティー、または大きいアクティビティー、あるいは指定された範囲内のアクティビティーを検出します。しきい値は、収集されたすべてのデータに基づいて設定することができます。例えば、午前 8 時から午後 5 時までの間は 220 を超えるクライアントがサーバーにログインできないことを指定するしきい値ルールを作成することができます。221 番目のクライアントがログインを試みると、このしきい値ルールによってアラートが生成されます。

動作ルールは、イベント・トラフィックおよびフロー・トラフィックをテストして、通常の周期パターンで発生する動作にボリューム変化が生じていないかどうか調べます。例えば、メール・サーバーが通常は深夜に 1 秒当たり 100 のホストと通信する場合で、突然 1 秒当たり 1000 のホストと通信し始めた場合は、動作ルールがアラートを生成します。

ルールのタイプ

ルールには、イベント、フロー、共通、オフェンスという 4 つの異なるタイプがあります。

イベント・ルール

イベント・ルールは、イベント・プロセッサーによってリアルタイムで処理されているイベントについて、テストを実行します。特定のプロパティー内の単一イベント、またはイベント・シーケンスを検出するためのイベント・ルールを作成することができます。 例えば、ネットワークをモニターして、失敗したログイン試行、複数ホストへのアクセス、エクスプロイトが後に続くスキャン行為イベントを調べるために、イベント・ルールを作成することができます。通常、イベント・ルールは、応答としてオフェンスを作成します。

フロー・ルール

フロー・ルールは、QFlow コレクターによってリアルタイムで処理されているフローについて、テストを実行します。特定のプロパティー内の単一フロー、またはフロー・シーケンスを検出するためのフロー・ルールを作成することができます。 通常、フロー・ルールは、応答としてオフェンスを作成します。

共通ルール

共通ルールは、イベント・レコードとフロー・レコードに共通のフィールドについて、テストを実行します 例えば、特定の送信元 IP アドレスを持つイベントとフローを検出するための共通ルールを作成することができます。通常、共通ルールは、応答としてオフェンスを作成します。

オフェンス・ルール

オフェンス・ルールは、オフェンスが変更された場合のみ (新規イベントが追加された場合や、オフェンスの再評価がシステムによってスケジュールされた場合など)、オフェンスの処理を行います。通常、オフェンス・ルールは、応答として通知を E メールで送信します。

ルール条件

各ルールには関数、ビルディング・ブロック、またはテストが含まれることがあります。

関数により、ビルディング・ブロックおよび他のルールを使用して複数イベント、複数フロー、または複数オフェンスの機能を作成できます。ブール演算子 (OR や AND など) をサポートする関数を使用して、ルールを結合させることができます。例えば、イベント・ルールを結合させたい場合で、イベントが以下のルールのいずれかまたはすべてに一致する場合、関数を使用することができます。

ビルディング・ブロックは応答を伴わないルールであり、複数のルールで共通変数として使用したり、他のルールで使用したい複雑なルールまたは論理を構築するために使用したりします。テストのグループをビルディング・ブロックとして保存して、他の機能で使用することができます。ビルディング・ブロックを使用すると、特定のルール・テストを他のルールで再使用することができます。例えば、ネットワーク内のすべてのメール・サーバーの IP アドレスを含むビルディング・ブロックを保存して、それらのメール・サーバーを別のルールから除外するために、そのビルディング・ブロックを使用することができます。デフォルトのビルディング・ブロックはガイドラインとして提供されています。これらのビルディング・ブロックを見直して、ご使用のネットワークのニーズに合うように編集する必要があります。

注: デフォルトでは、ビルディング・ブロックはロードされません。ビルディング・ブロックを作成するためのルールを定義してください。

ビルディング・ブロックの完全なリストについては、*IBM Security QRadar SIEM 管理ガイド*を参照してください。

イベント、フロー、またはオフェンスのプロパティー (送信元 IP アドレス、イベントの重大度、またはレート分析など) についてテストを実行することができます。

ルールの応答

ルール条件が満たされると、1 つ以上の応答がルールによって生成される場合があります。

ルールにより、以下に示す 1 つ以上の応答が生成される場合があります。

- オフェンスを作成する。
- E メールを送信する。
- ダッシュボード機能でシステム通知を生成する。
- データをリファレンス・セットに追加する。
- リファレンス・データ・コレクションにデータを追加する。
- 外部システムへの応答を生成する。
- ルール・テストで使用可能なリファレンス・データ・コレクションにデータを追加する。
- イベントに対する応答としてカスタム・アクション・スクリプトを実行する。

リファレンス・データ収集のタイプ

リファレンス・データ収集にデータを送信するためのルール応答を構成するには、コマンド・ライン・インターフェース (CLI) を使用してリファレンス・データ収集を作成しておく必要があります。QRadar は、以下のデータ収集タイプをサポートします。

リファレンス・セット
ネットワークで発生するイベントとフローから取得されたエレメントのセット (IP アドレスやユーザー名のリストなど)。

リファレンス・マップ
キーを 1 つの値にマップするレコードにデータが保管されます。例えば、ネットワーク上のユーザー・アクティビティーを相互に関連させるには、**「ユーザー名」**パラメーターをキーとして使用し、ユーザーの**グローバル ID** を値として使用するリファレンス・マップを作成します。

セットのリファレンス・マップ
キーを複数の値にマップするレコードにデータが保管されます。例えば、ある特許権への許可アクセスをテストする場合は、**Patent ID** のカスタム・イベント・プロパティーをキーとして使用し、**Username** パラメーターを値として使用します。セットのマップを作成して、許可されているユーザーのリストを取得します。

マップのリファレンス・マップ
あるキーを別のキーにマップするレコードにデータが保管されてから、このキーが単一値にマップされます。例えば、ネットワーク帯域幅の違反が発生していないかどうかをテストする場合は、マップのマップを作成します。**Source IP** パラメーターを最初のキーとして使用し、**Application** パラメーターを 2 番目のキーとして使用して、**Total Bytes** パラメーターを値として使用します。

リファレンス・テーブル
リファレンス・テーブルでは、あるキーを別のキーにマップするテーブルにデータが保管されてから、このキーが単一値にマップされます。2 番目のキーには、割り当て済みタイプが含まれています。このマッピングは、表内の各列が 1 つのタイプに関連付けられているデータベース表に類似しています。例えば、リファレンス・テーブルを作成し、このテーブルに **Username** パラメーターを最初のキーとして保管し、ユーザー定義の割り当て済みタイプ (**Source IP** パラメーターや **Source Port** パラメーターを値として持つ

IP タイプなど) が設定されている複数のセカンダリー・キーを保管することができます。テーブル内に定義されているキーを 1 つ以上追加するためのルール応答を構成することができます。このルール応答には、カスタム値を追加することもできます。このカスタム値は、セカンダリー・キーのタイプに対して有効な値でなければなりません。

注: リファレンス・セットとリファレンス・データ収集について詳しくは、「*Administration Guide*」を参照してください。

ルールの表示

テスト、ビルディング・ブロック、および応答を含む、ルールの詳細を表示することができます。

始める前に

ユーザー・ロール権限に応じて、「**オフェンス**」、「**ログ・アクティビティー**」、または「**ネットワーク・アクティビティー**」タブからルール・ページにアクセスすることができます。

ユーザー・ロール権限の詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

このタスクについて

ルール・ページには、ルールのリストが関連するパラメーターとともに表示されます。開いて詳細を表示するルールを見つける場合、「グループ」リスト・ボックスまたはツールバーの「**ルールの検索**」フィールドを使用できます。

手順

1. 次のオプションのいずれかを選択してください。
   - 「**オフェンス**」タブをクリックしてから、ナビゲーション・メニューの「**ルール**」をクリックします。
   - 「**ログ・アクティビティー**」タブをクリックして、ツールバーの「**ルール**」リスト・ボックスから「**ルール**」を選択します。
   - 「**ネットワーク・アクティビティー**」タブをクリックして、ツールバーの「**ルール**」リスト・ボックスから「**ルール**」を選択します。
2. 「**表示**」リスト・ボックスから、「**ルール**」を選択します。
3. 表示するルールをダブルクリックします。
4. ルールの詳細を確認します。

タスクの結果

「**カスタム・ルールの表示 (View Custom Rules)**」権限があっても、「**カスタム・ルールの保守**」権限がない場合、「**ルールのサマリー**」ページが表示され、ルールを編集することはできません。「**カスタム・ルールの保守**」権限がある場合は、「**ルール・テスト・スタック・エディター**」ページが表示されます。ルールの詳細を確認して、編集することができます。

ルールの作成

ルールは、ルール・テスト条件に対して入力データを評価して、システムからの応答を生成します。ルールの条件が満たされると、いくつかのアクションが実行される場合があります。例えば、オフェンスの生成、E メールの送信、スキャンの開始、リファレンス・データの追加、値 (重大度など) の増減のように、ルールに対するさまざまなシステム応答を構成できます。

始める前に

新規ルールを作成するには、「**オフェンス**」 > 「**カスタム・ルールの保守**」権限が必要です。

このタスクについて

ルール・テストを定義するときには、検索を扱うのと同じ方法でルールを扱い、テストの対象となるデータをできるだけ小さくします。この方法でテストすると、ルール・テストのパフォーマンスが向上し、高負荷のルールを作成しないで済みます。パフォーマンスを最適化するには、一般的なカテゴリーから開始して、ルール・テストが評価するデータを絞り込みます。例えば、特定のログ・ソース・タイプ、ネットワーク・ロケーション、フロー・ソース、またはコンテキスト (R2L、L2R、L2L) に対するルール・テストから開始します。中位のテストを実行するときには、IP アドレス、ポート・トラフィック、またはその他の関連するテストが含まれることがあります。ペイロードおよび正規表現のテストは、最後のルール・テストとして保留しておきます。

多くのルール・テストは、単一の条件 (リファレンス・データ・コレクション内のエレメントの存在、またはイベントのプロパティーに対する値のテストなど) を評価します。複雑な比較のために、WHERE 節条件を含む Ariel 照会言語 (AQL) 照会を作成して、イベント・ルールをテストできます。すべての WHERE 節関数を使用して、複雑な基準を作成できます。こうすると、個別のテストを数多く実行する必要がなくなります。例えば、AQL WHERE 節を使用して、インバウンド SSL トラフィックまたは Web トラフィックのどちらがリファレンス・セット上で追跡されているかを検査します。

手順

1. 「**オフェンス**」から、「**ログ・アクティビティー**」タブまたは「**ネットワーク・アクティビティー**」タブを選択し、「**ルール**」をクリックします。
2. 「**アクション**」リストから、ルール・タイプを選択します。

   各ルール・タイプは、さまざまなソースからの入力データに対してリアルタイムでテストされます。例えば、イベント・ルールは、入力ログ・ソース・データをテストします。オフェンス・ルールは、オフェンスのパラメーターをテストして、より多くの応答をトリガーします。
3. 「ルール・テスト・スタック・エディター」ページの「ルール」ペインで、「**適用**」テキスト・ボックスに、このルールに割り当てる固有の名前を入力します。
4. リスト・ボックスから、「**ローカル (Local)**」または「**グローバル (Global)**」を選択します。

ローカルのルールでは、イベントとフローをローカルのイベント・プロセッサーに送信して、ルールをトリガーします。これがデフォルトのアクションです。

グローバルのルールでは、イベントとフローを中央のイベント・プロセッサーに送信します。この送信によって、コンソールのパフォーマンスが低下する場合があります。コンソール上のカスタム・ルール・エンジン (CRE) は、デプロイメント内の各管理対象ホストによって提供されるイベント一致を追跡します。部分一致が発生するか、カウンターの更新が必要になると、各管理対象ホストは、コンソール上の CRE に更新を送信します。ルール全体が true になると、コンソールは、ルールの応答をトリガーします。

ローカルおよびグローバルのルール・テストについて詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

5. 「**テスト・グループ**」リストから、このルールに追加する 1 つ以上のテストを選択します。CRE は、ルール・テストを行単位で順番に評価します。最初のテストが評価され、true である場合は、次の行が評価されます。以下同様に、最終テストに到達するまで続行されます。

   新規イベント・ルールに対して「**イベントがこの AQL フィルター照会に一致する場合 (when the event matches this AQL filter query)**」テストを選択する場合は、「**AQL フィルター照会の入力**」テキスト・ボックスに AQL WHERE 節照会を入力します。

   イベントが検出されない場合にルールを使用する方法の詳細:

   以下の場合のルール・テストは個別にトリガーできますが、同じルール・テスト・スタック内の後続のルール・テストには影響を与えません。

   - **この秒数の間、これらのログ・ソース・タイプの 1 つ以上によってイベントが検出されなかった場合 (when the event(s) have not been detected by one or more of these log source types for this many seconds)**
   - **この秒数の間、これらのログ・ソースの 1 つ以上によってイベントが検出されなかった場合 (when the event(s) have not been detected by one or more of these log sources for this many seconds)**
   - **この秒数の間、これらのログ・ソース・グループの 1 つ以上によってイベントが検出されなかった場合 (when the event(s) have not been detected by one or more of these log source groups for this many seconds)**

   これらのルール・テストは受信イベントによってはアクティブ化されませんが、代わりに、構成済みの特定の時間間隔の間に特定のイベントが検出されなかった場合にアクティブ化されます。QRadar は、イベントが最後に検出された時刻 (最終確認時刻) を定期的に照会する監視タスク を使用して、ログ・ソースごとに、イベントのこの時刻を保管します。ルールがトリガーされるのは、この最終確認時刻と現在時刻の差が、ルールに構成された秒数を超えたときです。

6. 構成したルールを他のルールと共に使用するためにビルディング・ブロックとしてエクスポートするには、「**ビルディング・ブロックとしてエクスポート**」をクリックします。

   ビルディング・ブロックとは、応答を持たないルール・テストのサブセットのことです。ビルディング・ブロックは、他のルール内で使用できる再使用可能なル

ール・テストのセットであると考えてください。一般的な例の 1 つは、BB:Host Definition ビルディング・ブロックにサーバーのアドレスを取り込む場合です。こうすると、管理者は、VPN サーバー、メール・サーバー、LDAP サーバーなどの特定のサーバー・タイプごとにルール・テストを除外したり、組み込んだりすることができます。

7. 「ルールの応答 (Rule Responses)」ページで、このルールに生成させる応答を構成します。

   ルールの応答とは、すべてのルール・テストが true である場合に QRadar アプライアンスが実行するアクションのことです。ルールの応答 (E メール、syslog メッセージ、転送イベントなど) は、ルールが true になると、ローカルのルールの場合はプロセッサー上で、グローバルのルールの場合はコンソール上で実行されます。

関連概念:

231 ページの『「ルールの応答」ページのパラメーター』

ルールがトリガーされたときの IBM Security QRadar の応答方法を指定するには、「ルールの応答」ページのパラメーターを構成します。

アノマリ検出ルールの作成

「アノマリ検出ルール (Anomaly Detection Rule)」ウィザードを使用して、「データと時刻 (Data and Time)」の各テストによって時刻範囲条件を適用するルールを作成します。

始める前に

新規のアノマリ検出ルールを作成するには、以下の要件を満たす必要があります。

- 「カスタム・ルールの保守」権限を保持している。
- グループ化された検索を実行する。

アノマリ検出オプションは、グループ化された検索を実行して検索条件を保存すると表示されます。

このタスクについて

アノマリ検出ルールを作成できる、適切なロール権限が必要です。

「ログ・アクティビティー」タブでアノマリ検出ルールを作成するには、**「ログ・アクティビティー」**の**「カスタム・ルールの保守」**ロール権限が必要です。

「ネットワーク・アクティビティー」タブでアノマリ検出ルールを作成するには、**「ネットワーク」**の**「カスタム・ルールの保守」**ロール権限が必要です。

アノマリ検出ルールでは、ルールが基準とする保存済み検索条件から取得したすべてのグループ化とフィルター基準を使用しますが、検索条件の時刻範囲は一切使用しません。

アノマリ検出ルールを作成すると、そのルールにはデフォルトのテスト・スタックが取り込まれます。デフォルトのテストを編集することも、テスト・スタックにテ

ストを追加することもできます。少なくとも 1 つの「集計プロパティー (Accumulated Property)」テストがテスト・スタックに組み込まれている必要があります。

デフォルトでは、「ルール・テスト・スタック・エディター」ページで「**各 [グループ] の [選択された累積型プロパティー] 値を個別にテストする (Test the [Selected Accumulated Property] value of each [group] separately)**」オプションが選択されます。

このため、アノマリ検出ルールではイベント・グループまたはフロー・グループごとに選択された集計プロパティーを個別にテストします。例えば、選択された累積値が **UniqueCount(sourceIP)** の場合、ルールでは、イベント・グループまたはフロー・グループごとにそれぞれの固有の送信元 IP アドレスをテストします。

この「**各 [グループ] の [選択された累積型プロパティー] 値を個別にテストする (Test the [Selected Accumulated Property] value of each [group] separately)**」 オプションは動的です。「**[選択された累積型プロパティー] ([Selected Accumulated Property])**」の値は、デフォルトのテスト・スタックの「**この累積型プロパティーのテスト (this accumulated property test)**」フィールドで選択しているオプションによって決まります。「**[グループ] ([group])**」の値は、保存済み検索条件に指定されているグループ化オプションによって決まります。複数のグループ化オプションが組み込まれている場合、テキストが切り捨てられる場合があります。すべてのグループを表示するには、テキストの上にマウス・ポインターを移動します。

手順

1. 「**ログ・アクティビティー**」 タブまたは「**ネットワーク・アクティビティー**」タブをクリックします。
2. 検索を実行します。
3. 「**ルール**」メニューから、作成するルール・タイプを選択します。オプションは、以下のとおりです。
   - アノマリ・ルールの追加
   - しきい値ルールの追加
   - 振る舞い型ルールの追加
4. 「ルール」ウィザード上の概要のテキストを読みます。「**次へ**」をクリックします。 前に選択したルールが選択されています。
5. 「**次へ**」をクリックして、「ルール・テスト・スタック・エディター」ページを表示します。
6. 「**ルール名をここに入力してください (enter rule name here)**」フィールドに、このルールに割り当てる固有の名前を入力します。
7. テストをルールに追加するには、次のようにします。
   a. オプション。「テスト・グループ (Test Group)」リスト・ボックス内のオプションをフィルタリングするには、フィルタリングするテキストを「入力してフィルタリング (Type to filter)」フィールドに入力します。
   b. 「テスト・グループ (Test Group)」リスト・ボックスから、このルールに追加するテストのタイプを選択します。

c. ルールに追加するテストごとに、そのテストの横にある + 記号を選択します。

d. オプション。テストを除外されたテストと識別させるには、「ルール」ペイン内のそのテストの先頭にある「および (and)」をクリックします。「および (and)」が「および次のテストではない (and not)」と表示されます。

e. 下線付きの構成可能なパラメーターをクリックして、テストの変数をカスタマイズします。

f. ダイアログ・ボックスから変数の値を選択した後、「**送信**」をクリックします。

8. オプション。すべての選択された集計プロパティーをイベント・グループまたはフロー・グループごとにテストするには、「**各 [グループ] の [選択された累積型プロパティー] 値を個別にテストする (Test the [Selected Accumulated Property] value of each [group] separately)**」チェック・ボックスをクリアします。

9. 「グループ (groups)」ペインで、このルールの割り当て先の各グループのチェック・ボックスを選択します。詳しくは、ルール・グループの管理を参照してください。

10. 「**メモ**」フィールドに、このルールに含めるすべてのメモを入力します。「**次へ**」をクリックします。

11. 「ルールの応答 (Rule Responses)」ページで、このルールに生成させる応答を構成します。 231 ページの『「ルールの応答」ページのパラメーター』

12. 「**次へ**」をクリックします。

13. 構成したルールを確認します。「**終了 (Finish)**」をクリックします。

ルール管理タスク

カスタム・ルールとアノマリ・ルールを管理することができます。

必要に応じて、ルールの有効と無効を切り替えることができます。また、ルールの編集、コピー、削除を行うこともできます。

アノマリ検出ルールは、「**ログ・アクティビティー**」タブと「**ネットワーク・アクティビティー**」タブでのみ作成することができます。

デフォルトのアノマリ検出ルールと、以前に作成されたアノマリ検出ルールを管理するには、「**オフェンス**」タブの「ルール」ページを使用する必要があります。

ルールの有効化と無効化

ご使用のシステムがその環境にとって重大なオフェンスを確実に生成するようにするには、システムのチューニング時に該当するルールを有効化または無効化する必要があります。

このタスクについて

ルールを有効または無効にするには、「**オフェンス**」 > 「**カスタム・ルールの保守**」ロールの権限が必要です。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**ルール**」ページの「**表示**」リスト・ボックスから、「**ルール**」を選択します。
4. 有効化または無効化するルールを選択します。
5. 「**アクション**」リスト・ボックスから、「**有効化/無効化**」を選択します。

ルールの編集

ルールを編集して、ルール名、ルール・タイプ、テスト、応答を変更できます。

このタスクについて

ルールを有効または無効にするには、「**オフェンス**」 > 「**カスタム・ルールの保守**」ロールの権限が必要です。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**ルール**」ページの「**表示**」リスト・ボックスから、「**ルール**」を選択します。
4. 編集するルールをダブルクリックします。
5. 「**アクション**」リスト・ボックスから、「**オープン**」を選択します。
6. オプション。ルール・タイプを変更する場合は、「**戻る (Back)**」をクリックしてから新しいルール・タイプを選択します。
7. 「ルール・テスト・スタック・エディター」ページで、パラメーターを編集します。
8. 「**次へ**」をクリックします。
9. 「ルールの応答」ページで、パラメーターを編集します。
10. 「**次へ**」をクリックします。
11. 編集したルールを確認します。「**終了 (Finish)**」をクリックします。

ルールのコピー

既存のルールをコピーし、そのルールに新しい名前を入力してから、必要に応じて、その新しいルールのパラメーターをカスタマイズすることができます。

このタスクについて

ルールを有効または無効にするには、「**オフェンス**」 > 「**カスタム・ルールの保守**」ロールの権限が必要です。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**表示**」リスト・ボックスから、「**ルール**」を選択します。
4. コピーするルールを選択します。

5. 「**アクション**」リスト・ボックスから、「**コピー (Duplicate)**」を選択します。
6. 「コピーしたルールに名前を入力してください (Enter name for the copied rule)」フィールドに、新規ルールの名前を入力します。「**OK**」をクリックします。

ルールの削除

システムからルールを削除することができます。

このタスクについて

ルールを有効または無効にするには、「**オフェンス**」 > 「**カスタム・ルールの保守**」ロールの権限が必要です。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**表示**」リスト・ボックスから、「**ルール**」を選択します。
4. 削除するルールを選択します。
5. 「**アクション**」リスト・ボックスから「**削除**」 を選択します。

ルール・グループの管理

管理者は、ルールのグループを作成、編集、および削除することができます。ルールまたはビルディング・ブロックをグループに分類すると、ルールを効率良く表示および追跡することができます。

例えば、コンプライアンスに関連するすべてのルールを表示することができます。

新規ルールを作成する際に、そのルールを既存のグループに割り当てることができます。ルール・ウィザードの使用によるグループの割り当てについては、カスタム・ルールの作成またはアノマリ検出ルールの作成を参照してください。

ルール・グループの表示

「ルール」ページでは、ルールまたはビルディング・ブロックをフィルタリングして、特定のグループに属しているルールまたはビルディング・ブロックのみを表示することができます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**表示**」リスト・ボックスから、ルールを表示するかビルディング・ブロックを表示するかを選択します。
4. 「**フィルター (Filter)**」リスト・ボックスから、表示するグループ・カテゴリーを選択します。

グループの作成

「ルール」ページには、デフォルトのルール・グループが提示されますが、新しいグループを作成することもできます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**グループ (Groups)**」をクリックします。
4. ナビゲーション・ツリーから、新しい下位グループを作成するグループを選択します。
5. 「**新規グループ**」をクリックします。
6. 次の各パラメーターの値を入力します。
   - 「**名前**」 - 新しいグループに割り当てる固有の名前を入力します。名前の長さは 255 文字までです。
   - 「**説明**」 - このグループに割り当てる説明を入力します。説明の長さは 255 文字までです。
7. 「**OK**」をクリックします。
8. オプション。新しいグループの場所を変更するには、新しいグループをクリックし、ナビゲーション・ツリー内の新たな場所までグループをドラッグします。

項目のグループへの割り当て

選択したルールまたはビルディング・ブロックをグループに割り当てることができます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. グループに割り当てるルールまたはビルディング・ブロックを選択します。
4. 「**アクション**」リスト・ボックスから、「**グループの割り当て**」を選択します。
5. ルールまたはビルディング・ブロックの割り当て先のグループを選択します。
6. 「**グループの割り当て**」をクリックします。
7. 「**グループの選択**」ウィンドウを閉じます。

グループの編集

グループを編集して、その名前や説明を変更することができます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**グループ (Groups)**」をクリックします。
4. ナビゲーション・ツリーから、編集するグループを選択します。
5. 「**編集**」をクリックします。
6. 以下のパラメーターの値を更新します。

- 「**名前**」 - 新しいグループに割り当てる固有の名前を入力します。名前の長さは 255 文字までです。
- 「**説明**」 - このグループに割り当てる説明を入力します。説明の長さは 255 文字までです。

7. 「**OK**」をクリックします。
8. オプション。グループのロケーションを変更するには、ナビゲーション・ツリー内で新しいグループをクリックして、そのフォルダーを新しいロケーションにドラッグしてください。

別のグループへの項目のコピー

ルールまたはビルディング・ブロックをあるグループから別のグループにコピーすることができます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**グループ (Groups)**」をクリックします。
4. ナビゲーション・ツリーから、別のグループにコピーするルールまたはビルディング・ブロックを選択します。
5. 「**コピー**」をクリックします。
6. ルールまたはビルディング・ブロックのコピー先のグループのチェック・ボックスを選択します。
7. 「**コピー**」をクリックします。

グループからの項目の削除

項目をグループから削除することができます。項目をグループから削除した場合、ルールまたはビルディング・ブロックはグループから削除されるだけです。つまり、それらは「ルール」ページでは引き続き使用できます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**グループ (Groups)**」をクリックします。
4. ナビゲーション・ツリーを使用して、削除する項目にナビゲートして選択します。
5. 「**削除**」をクリックします。
6. 「**OK**」をクリックします。

グループの削除

グループを削除することができます。グループを削除しても、そのグループのルールやビルディング・ブロックは引き続き「ルール」ページで使用可能です。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**グループ (Groups)**」をクリックします。
4. ナビゲーション・ツリーで、削除するグループにナビゲートし、そのグループを選択します。
5. 「**削除**」をクリックします。
6. 「**OK**」をクリックします。

ビルディング・ブロックの編集

デプロイメントの必要に応じて、デフォルトのビルディング・ブロックを編集することができます。

このタスクについて

ビルディング・ブロックとは、他のルール内にコンポーネントとして組み込むことができる再使用可能なルール・テスト・スタックのことです。

例えば、「BB:HostDefinition: Mail Servers」というビルディング・ブロックを編集して、デプロイメント内のすべてのメール・サーバーを識別できます。その後で、ご使用のメール・サーバーをルール・テストから除外するルールを構成できます。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**表示**」リスト・ボックスから、「**ビルディング・ブロック (Building Blocks)**」を選択します。
4. 編集するビルディング・ブロックをダブルクリックします。
5. ビルディング・ブロックを必要に応じて更新します。
6. 「**次へ**」をクリックします。
7. ウィザードの残りを続行します。詳しくは、カスタム・ルールの作成を参照してください。
8. 「**終了 (Finish)**」をクリックします。

ルール・ページのパラメーター

「ルール」ページのパラメーターについて説明します。

デプロイされたルールのリストでは、それぞれのルールについて以下の情報が提供されます。

表 53. ルール・ページのパラメーター

パラメーター	説明
ルール名	ルールの名前を表示します。

表 53. ルール・ページのパラメーター (続き)

パラメーター	説明
グループ	このルールが割り当てられているグループを表示します。グループについて詳しくは、ルール・グループの管理を参照してください。
ルール・カテゴリー (Rule Category)	このルールのルール・カテゴリーを表示します。オプションには、「カスタム・ルール (Custom Rule)」と「アノマリ検出ルール (Anomaly Detection Rule)」があります。
ルール・タイプ (Rule Type)	ルール・タイプを表示します。 ルール・タイプには、以下のものがあります。 • イベント • フロー • 共通 • オフェンス • アノマリ • しきい値 • 動作 ルール・タイプについて詳しくは、ルールのタイプを参照してください。
有効 (Enabled)	そのルールが有効か無効かを示します。ルールの有効化および無効化について詳しくは、ルールの有効化と無効化を参照してください。
応答 (Response)	ルールの応答がある場合には、それを表示します。ルールの応答には、以下のものがあります。 • 新規イベントのディスパッチ • E メール • ログ通知 • SNMP • リファレンス・セット • リファレンス・データ • IF-MAP 応答 ルールの応答について詳しくは、ルールの応答を参照してください。
イベント/フローの数	ルールがオフェンスの原因となった場合に、そのルールに関連するイベントまたはフローの数を表示します。
オフェンス数	ルールによって生成されたオフェンスの数を表示します。

表 53. ルール・ページのパラメーター (続き)

パラメーター	説明
オリジン	ルールがデフォルト・ルール (システム) であるかカスタム・ルール (ユーザー) であるかを表示します。
作成日	ルールが作成された日時を指定します。
変更日 (Modification Date)	ルールが変更された日時を指定します。

「ルール」ページ・ツールバー

「ルール」ページのツールバーを使用して、ルール、ビルディング・ブロック、またはグループを表示することができます。ルール・グループを管理したり、ルールを使って作業したりすることができます。

「ルール」ページ・ツールバーには、以下の機能があります。

表 54. 「ルール」ページ・ツールバーの機能

機能	説明
表示	このリスト・ボックスから、ルールまたはビルディング・ブロックのどちらをルール・リストに表示するかを選択します。
グループ	このリスト・ボックスから、ルール・リストに表示するルール・グループを選択します。
グループ (Groups)	ルール・グループを管理するには、「**グループ (Groups)**」をクリックします。

表 54. 「ルール」ページ・ツールバーの機能 (続き)

機能	説明
アクション	「**アクション**」をクリックして、以下のいずれかのオプションを選択します。 • **新規イベント・ルール** - 新規イベント・ルールを作成するには、このオプションを選択します。 • **新規フロー・ルール** - 新規フロー・ルールを作成するには、このオプションを選択します。 • **新規共通ルール** - 新規共通ルールを作成するには、このオプションを選択します。 • **新規オフェンス・ルール** - 新規オフェンス・ルールを作成するには、このオプションを選択します。 • **有効化/無効化** - 選択したルールを有効化または無効化するには、このオプションを選択します。 • **コピー (Duplicate)** - 選択したルールをコピーするには、このオプションを選択します。 • **編集** - 選択したルールを編集するには、このオプションを選択します。 • **削除** - 選択したルールを削除するには、このオプションを選択します。 • **グループの割り当て** - 選択したルールをルール・グループに割り当てるには、このオプションを選択します。
ルールを戻す	変更されたシステム・ルールをデフォルト値に戻すには、「**ルールを戻す**」をクリックします。「**ルールを戻す**」をクリックすると、確認ウィンドウが表示されます。ルールを戻すと、以前の変更内容は永久に削除されます。 ルールを戻し、かつ変更済みバージョンを維持するには、ルールをコピーしてから、変更したルールに「**ルールを戻す**」オプションを適用してください。

表 54. 「ルール」ページ・ツールバーの機能 (続き)

機能	説明
ルールの検索	「**ルールの検索**」フィールドに検索条件を入力して、「**ルールの検索**」アイコンをクリックするか、または、キーボードで Enter を押してください。指定した検索条件に一致するすべてのルールがルール・リストに表示されます。 検索条件に基づく一致を見つけるために、以下のパラメーターが検索されます。 • ルール名 • ルール (説明) (Rule (description)) • メモ • 応答 (Response) 「ルールの検索」機能は、直接テキスト・ストリングの一致の検出を試みます。一致するものが検出されない場合、「ルールの検索」機能は正規表現 (regex) の一致を見つけようと試みます。

「ルールの応答」ページのパラメーター

ルールがトリガーされたときの IBM Security QRadar の応答方法を指定するには、「ルールの応答」ページのパラメーターを構成します。

注: AQL 照会を作成するときに、単一引用符を含むテキストを文書からコピーして、このテキストを IBM Security QRadar に貼り付けると、照会が解析されません。これを回避するためには、テキストを QRadar に貼り付けてから単一引用符を再入力するか、または IBM Knowledge Center からテキストをコピーして貼り付ける方法があります。

以下の表に、「ルールの応答」ページのパラメーターを示します。

表 55. 「イベント (Event)」、「フロー (Flow)」、および「共通 (Common)」の「ルールの応答」ページのパラメーター

パラメーター	説明
イベントに注釈を付ける (Annotate event)	このイベントに注釈を追加するには、このチェック・ボックスを選択して、イベントに追加する注釈を入力します。
検出されたイベントを分岐 (Drop the detected event)	通常は判定機能コンポーネントに送信されるイベントを、報告用または検索用に Ariel データベースに送信する場合は、このチェック・ボックスを選択します。ドロップされたイベントは、ストレージに書き込まれ、ルール・テストをバイパスします。 このイベントは、「**オフェンス**」タブには表示されません。

表 55. 「イベント (Event)」、「フロー (Flow)」、および「共通 (Common)」の「ルールの応答」ページのパラメーター (続き)

パラメーター	説明
新規イベントのディスパッチ (Dispatch New Event)	元のイベントまたはフローのほかに新規イベントをディスパッチする場合は、このチェック・ボックスを選択します。新規イベントは、システム内の他のすべてのイベントと同様に処理されます。 元のイベントのほかに新規イベントをディスパッチする場合は、このチェック・ボックスを選択します。新規イベントは、システム内の他のすべてのイベントと同様に処理されます。 「**新規イベントのディスパッチ (Dispatch New Event)**」パラメーターは、このチェック・ボックスを選択した場合に表示されます。デフォルトでは、このチェック・ボックスはクリアされています。
イベント名 (Event Name)	「**オフェンス**」タブに表示されるイベントの固有名を入力します。
イベントの説明	イベントの説明を入力します。この説明は、イベント詳細の「注釈」ペインに表示されます。
重大度 (Severity)	リスト・ボックスから、イベントの重大度を選択します。範囲は 0 (最低) から 10 (最高) までで、デフォルトは 0 です。この重大度は、イベント詳細の「注釈」ペインに表示されます。
信頼性 (Credibility)	リスト・ボックスから、イベントの信頼性を選択します。範囲は 0 (最低) から 10 (最高) までで、デフォルトは 10 です。この信頼性は、イベント詳細の「注釈」ペインに表示されます。
関連性 (Relevance)	リスト・ボックスから、イベントの関連性を選択します。範囲は 0 (最低) から 10 (最高) までで、デフォルトは 10 です。この関連性は、イベント詳細の「注釈」ペインに表示されます。
上位カテゴリー	リスト・ボックスから、イベントの処理時にこのルールで使用する上位イベント・カテゴリーを選択します。
下位カテゴリー	リスト・ボックスから、イベントの処理時にこのルールで使用する下位イベント・カテゴリーを選択します。
このオフェンスに注釈を付ける (Annotate this offense)	このオフェンスに注釈を追加するには、このチェック・ボックスを選択して注釈を入力します。
E メール	E メール・オプションを表示するには、このチェック・ボックスを選択します。 **注:** 「**E メールのロケール**」設定を変更するには、「**管理**」タブで「**システム設定**」を選択します。
通知先の E メール・アドレスを入力 (Enter email addresses to notify)	このルールが生成された場合に通知を送信する E メール・アドレスを入力します。複数の E メール・アドレスを指定する場合は、各アドレスをコンマで区切ってください。

表 55. 「イベント (Event)」、「フロー (Flow)」、および「共通 (Common)」の「ルールの応答」ページのパラメーター (続き)

パラメーター	説明
イベント/フロー E メール・テンプレートの選択	このルールに関連付ける E メールの E メール・テンプレートを選択します。カスタム E メール通知の構成について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
SNMP トラップ	このパラメーターは、システム設定で SNMP 設定パラメーターが構成されている場合にのみ表示されます。 このルールで SNMP 通知 (トラップ) を送信できるようにするには、このチェック・ボックスを選択します。 SNMP トラップの出力には、MIB で定義されているシステム時刻、トラップ OID、通知データが含まれます。
ローカル SysLog に送信	イベントまたはフローをローカルに記録するには、このチェック・ボックスを選択します。 デフォルトでは、このチェック・ボックスはクリアされています。 **注:** ローカルのアプライアンスに記録できるのは、正規化イベントだけです。生イベント・データを送信するには、「宛先転送に送信」オプションを使用して、データをリモートの syslog ホストに送信する必要があります。
宛先転送に送信	イベントまたはフローを転送宛先で記録するには、このチェック・ボックスを選択します。転送宛先とは、SIEM システム、チケット発行システム、アラート・システムなどのベンダー・システムです。このチェック・ボックスを選択すると、転送宛先のリストが表示されます。イベントまたはフローの送信先となる転送宛先のチェック・ボックスを選択してください。 転送宛先の追加、編集、削除を行うには、「**宛先の管理**」リンクをクリックします。
通知	このルールの結果として生成されたイベントを「ダッシュボード」タブの「システム通知」項目に表示するには、このチェック・ボックスを選択します。 通知を有効にする場合は、「**応答リミッター**」パラメーターを構成してください。

表 55. 「イベント (Event)」、「フロー (Flow)」、および「共通 (Common)」の「ルールの応答」ページのパラメーター (続き)

パラメーター	説明
リファレンス・セットに追加 (Add to Reference Set)	このルールの結果として生成されたイベントのデータをリファレンス・セットに追加するには、このチェック・ボックスを選択します。 リファレンス・セットにデータを追加するには、以下の手順を実行します。 1. 最初のリスト・ボックスを使用して、追加したいデータを選択します。すべての正規化データまたはカスタム・データが、オプションとして表示されます。 2. 2 番目のリスト・ボックスを使用して、指定されたデータの追加先となるリファレンス・セットを選択します。 「**リファレンス・セットに追加 (Add to Reference Set)**」ルール応答には、以下の機能が用意されています。 **最新表示** 最初のリスト・ボックスを最新表示して最新のリストを表示するには、「**最新表示 (Refresh)**」をクリックします。 **リファレンス・セットの構成** リファレンス・セットを構成するには、「**リファレンス・セットの構成**」をクリックします。このオプションは、管理権限を持っている場合のみ選択することができます。

表 55. 「イベント (Event)」、「フロー (Flow)」、および「共通 (Common)」の「ルールの応答」ページのパラメーター (続き)

パラメーター	説明
リファレンス・データに追加 (Add to Reference Data)	このルール応答を使用するには、コマンド・ライン・インターフェース (CLI) を使用してリファレンス・データ・コレクションを作成しておく必要があります。リファレンス・データ収集の作成方法と使用方法について詳しくは、「*Administration Guide*」を参照してください。 このルールの結果として生成されたイベントをリファレンス・データ・コレクションに追加するには、このチェック・ボックスを選択します。このチェック・ボックスを選択してから、以下のいずれかのオプションを選択してください。 **リファレンス・マップに追加** 単一キーと複数値のペアのコレクションにデータを送信するには、このオプションを選択します。データ・レコードのキーと値を選択してから、そのデータ・レコードの追加先となるリファレンス・マップを選択してください。 **セットのリファレンス・マップに追加** キーと単一値のペアのコレクションにデータを送信するには、このオプションを選択します。データ・レコードのキーと値を選択してから、そのデータ・レコードの追加先となるセットのリファレンス・マップを選択してください。 **マップのリファレンス・マップに追加** 複数キーと単一値のペアのコレクションにデータを送信するには、このオプションを選択します。最初のマップのキーを選択し、2 番目のマップのキーを選択してから、データ・レコードの値を選択する必要があります。データ・レコードの追加先となるマップのリファレンス・マップも選択する必要があります。 **リファレンス・テーブルに追加** 複数キーと単一値のペアのコレクションにデータを送信するには、このオプションを選択します。タイプは、セカンダリー・キーに割り当てられています。データの追加先となるリファレンス・テーブルを選択してから、プライマリー・キーを選択します。そのデータ・レコードについて、内部キー (セカンダリー・キー) とその値を選択します。

表 55. 「イベント (Event)」、「フロー (Flow)」、および「共通 (Common)」の「ルールの応答」ページのパラメーター (続き)

パラメーター	説明
カスタム・アクションの実行	ネットワーク・イベントに対する応答として特定のアクションを実行するスクリプトを作成できます。例えば、何度もログインに失敗した場合にネットワークから特定の送信元 IP アドレスをブロックするファイアウォール・ルールを作成するためのスクリプトを作成できます。 このチェック・ボックスを選択し、**「実行するカスタム・アクション」**リストからカスタム・アクションを選択します。 カスタム・アクションを追加して構成するには、**「管理」**タブの**「アクションの定義」**アイコンを使用します。
IF-MAP サーバーでの公開	IF-MAP パラメーターが構成されてシステム設定にデプロイされている場合、IF-MAP サーバーに関するイベント情報を公開するには、このオプションを選択します。
応答リミッター	このルールの応答頻度を構成するには、このチェック・ボックスを選択してリスト・ボックスを使用します。
ルールを有効にする	このルールを有効にするには、このチェック・ボックスを選択します。

以下の表で、ルールのタイプが「オフェンス」である場合の「ルールの応答」ページのパラメーターについて説明します。

表 56. 「オフェンス・ルール応答 (Offense Rule Response)」ページのパラメーター

パラメーター	説明
検出されたオフェンスの命名/注釈付け (Name/Annotate the detected offense)	「名前」オプションを表示するには、このチェック・ボックスを選択します。
新規オフェンス名 (New Offense Name)	このオフェンスに割り当てる名前を入力します。
オフェンスの注釈 (Offense Annotation)	「オフェンス」タブに表示されるオフェンスの注釈を入力します。
オフェンス名 (Offense Name)	次のオプションのいずれかを選択します。 **この情報を、オフェンスの名前に反映する** 「イベント名」の情報をオフェンスの名前に反映する場合は、このオプションを選択します。 **この情報で、オフェンスの名前を設定または置換する** 構成されている「イベント名」をオフェンスの名前にする場合は、このオプションを選択します。
E メール	E メール・オプションを表示するには、このチェック・ボックスを選択します。 **注: 「E メールのロケール」**設定を変更するには、**「管理」**タブで**「システム設定」**を選択します。
通知先の E メール・アドレスを入力 (Enter email address to notify)	このイベントが生成された場合に通知を送信する E メール・アドレスを入力します。複数の E メール・アドレスを指定する場合は、各アドレスをコンマで区切ってください。

表 56. 「オフェンス・ルール応答 (Offense Rule Response)」ページのパラメーター (続き)

パラメーター	説明
SNMP トラップ (SNMP Trap)	このパラメーターは、システム設定で SNMP 設定パラメーターが構成されている場合にのみ表示されます。 このルールで SNMP 通知 (トラップ) を送信できるようにするには、このチェック・ボックスを選択します。オフェンス・ルールに関する SNMP トラップの出力には、MIB で定義されているシステム時刻、トラップ OID、通知データが含まれます。
ローカル SysLog に送信	イベントまたはフローをローカルに記録するには、このチェック・ボックスを選択します。
宛先転送に送信	イベントまたはフローを転送宛先で記録するには、このチェック・ボックスを選択します。転送宛先とは、SIEM システム、チケット発行システム、アラート・システムなどのベンダー・システムです。このチェック・ボックスを選択すると、転送宛先のリストが表示されます。イベントまたはフローの送信先となる転送宛先のチェック・ボックスを選択してください。 転送宛先の追加、編集、削除を行うには、「**宛先の管理**」リンクをクリックします。
IF-MAP サーバーでの公開	IF-MAP パラメーターが構成されてシステム設定にデプロイされている場合、IF-MAP サーバーに関するオフェンス情報を公開するには、このオプションを選択します。
応答リミッター	このルールの応答頻度を構成するには、このチェック・ボックスを選択してリスト・ボックスを使用します。
ルールの有効化 (Enable Rule)	このルールを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。

以下の表で、ルール・タイプが「アノマリ」である場合の「ルールの応答」ページのパラメーターについて説明します。

表 57. 「アノマリ検出ルール応答 (Anomaly Detection Rule Response)」ページのパラメーター

パラメーター	説明
新規イベントのディスパッチ (Dispatch New Event)	このルールが、元のイベントまたはフローのほかに新規イベントをディスパッチすることを指定します。新規イベントは、システム内の他のすべてのイベントと同様に処理されます。デフォルトでは、このチェック・ボックスは選択されていて、クリアすることはできません。
イベント名	「オフェンス」タブに表示されるイベントの固有名を入力します。
イベントの説明	イベントの説明を入力します。この説明は、イベント詳細の「注釈」ペインに表示されます。

表 57. 「アノマリ検出ルール応答 (Anomaly Detection Rule Response)」ページのパラメーター (続き)

パラメーター	説明
オフェンスの命名 (Offense Naming)	次のオプションのいずれかを選択してください。 **この情報を、関連付けられたオフェンスの名前に反映する** 「イベント名」の情報をオフェンスの名前に反映する場合は、このオプションを選択します。 **この情報は、関連付けられたオフェンスの名前を設定または置換する** 構成されている「イベント名」をオフェンスの名前にする場合は、このオプションを選択します。 **注:** オフェンスの名前を置換した後、そのオフェンスをクローズするまでは名前は変更されません。例えば、オフェンスが複数のルールに関連付けられているときに、最後のイベントが、オフェンスの名前をオーバーライドするように構成されたルールをトリガーしない場合、オフェンスの名前は最後のイベントで更新されません。オフェンス名は、オーバーライド・ルールで設定されている名前のままになります。 **この情報を、関連付けられたオフェンスの命名に反映しない** 「イベント名」の情報をオフェンスの名前に反映しない場合は、このオプションを選択します。
重大度 (Severity)	リスト・ボックスを使用してイベントの重大度を選択します。範囲は 0 (最低) から 10 (最高) までで、デフォルトは 5 です。この重大度は、イベント詳細の「注釈」ペインに表示されます。
信頼性	リスト・ボックスを使用してイベントの信頼性を選択します。範囲は 0 (最低) から 10 (最高) までで、デフォルトは 5 です。この信頼性は、イベント詳細の「注釈」ペインに表示されます。
関連性	リスト・ボックスを使用してイベントの関連性を選択します。範囲は 0 (最低) から 10 (最高) までで、デフォルトは 5 です。この関連性は、イベント詳細の「注釈」ペインに表示されます。
上位カテゴリー	リスト・ボックスから、イベントの処理時にこのルールで使用する上位イベント・カテゴリーを選択します。
下位カテゴリー	リスト・ボックスから、イベントの処理時にこのルールで使用する下位イベント・カテゴリーを選択します。
このオフェンスに注釈を付ける (Annotate this offense)	このオフェンスに注釈を追加するには、このチェック・ボックスを選択して注釈を入力します。

表 57. 「アノマリ検出ルール応答 (Anomaly Detection Rule Response)」ページのパラメーター (続き)

パラメーター	説明
ディスパッチされたイベントをオフェンスの一部にする (Ensure that the dispatched event is part of an offense)	この規則の結果として、イベントが判定機能コンポーネントに転送されます。オフェンスが存在する場合は、このイベントが追加されます。「オフェンス」タブでオフェンスが作成されていない場合、新しいオフェンスが作成されます。 以下のオプションが表示されます。 **オフェンスの索引付けの基準** イベント名に基づいて新しいオフェンスの索引付けを行うことを指定します。このパラメーターは、デフォルトで有効になっています。 **この時点以降に検出された、イベント名によるイベントをオフェンスに含める。期間: 秒** ソースから検出されたイベントまたはフローを「**オフェンス**」タブに含めるには、このチェック・ボックスを選択して、必要な秒数を入力します。
E メール	E メール・オプションを表示するには、このチェック・ボックスを選択します。 **注:** 「**E メールのロケール**」設定を変更するには、「**管理**」タブで「**システム設定**」を選択します。
通知先の E メール・アドレスを入力 (Enter email address to notify)	このルールが生成された場合に通知を送信する E メール・アドレスを入力します。複数の E メール・アドレスを指定する場合は、各アドレスをコンマで区切ってください。
イベント E メール・テンプレートの選択	このルールに関連付ける E メールの E メール・テンプレートを選択します。カスタム E メール通知の構成について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。
通知	このルールの結果として生成されたイベントを「**ダッシュボード**」タブの「システム通知」項目に表示するには、このチェック・ボックスを選択します。通知を有効にする場合は、「**応答リミッター**」パラメーターを構成してください。
ローカル SysLog に送信	イベントまたはフローをローカルに記録するには、このチェック・ボックスを選択します。デフォルトでは、このチェック・ボックスはクリアされています。 **注:** ローカルの QRadar アプライアンスに記録できるのは、正規化イベントだけです。生イベント・データを送信するには、「宛先転送に送信」オプションを使用して、データをリモートの syslog ホストに送信する必要があります。

表 57. 「アノマリ検出ルール応答 (Anomaly Detection Rule Response)」ページのパラメーター (続き)

パラメーター	説明
リファレンス・セットに追加 (Add to Reference Set)	このルールの結果として生成されたイベントのデータをリファレンス・セットに追加するには、このチェック・ボックスを選択します。 リファレンス・セットにデータを追加するには、以下の手順を実行します。 1. 最初のリスト・ボックスを使用して、追加したいデータを選択します。すべての正規化データまたはカスタム・データが、オプションとして表示されます。 2. 2 番目のリスト・ボックスを使用して、指定されたデータの追加先となるリファレンス・セットを選択します。 **「リファレンス・セットに追加 (Add to Reference Set)」**ルール応答には、以下の機能が用意されています。 **最新表示** 最初のリスト・ボックスを最新表示して最新のリストを表示するには、**「最新表示 (Refresh)」**をクリックします。 **リファレンス・セットの構成** リファレンス・セットを構成するには、**「リファレンス・セットの構成」**をクリックします。このオプションは、管理権限を持っている場合のみ選択することができます。

表 57. 「アノマリ検出ルール応答 (Anomaly Detection Rule Response)」ページのパラメーター (続き)

パラメーター	説明
リファレンス・データに追加 (Add to Reference Data)	このルール応答を使用するには、コマンド・ライン・インターフェース (CLI) を使用してリファレンス・データ・コレクションを作成しておく必要があります。リファレンス・データ収集の作成方法と使用方法について詳しくは、「*Administration Guide*」を参照してください。 このルールの結果として生成されたイベントをリファレンス・データ・コレクションに追加するには、このチェック・ボックスを選択します。このチェック・ボックスを選択してから、以下のいずれかのオプションを選択してください。 **リファレンス・マップに追加** 単一キーと複数値のペアのコレクションにデータを送信するには、このオプションを選択します。データ・レコードのキーと値を選択してから、そのデータ・レコードの追加先となるリファレンス・マップを選択してください。 **セットのリファレンス・マップに追加** キーと単一値のペアのコレクションにデータを送信するには、このオプションを選択します。データ・レコードのキーと値を選択してから、そのデータ・レコードの追加先となるセットのリファレンス・マップを選択してください。 **マップのリファレンス・マップに追加** 複数キーと単一値のペアのコレクションにデータを送信するには、このオプションを選択します。最初のマップのキーを選択し、2 番目のマップのキーを選択してから、データ・レコードの値を選択する必要があります。データ・レコードの追加先となるマップのリファレンス・マップも選択する必要があります。 **リファレンス・テーブルに追加** 複数キーと単一値のペアのコレクションにデータを送信するには、このオプションを選択します。タイプは、セカンダリー・キーに割り当てられています。データの追加先となるリファレンス・テーブルを選択してから、プライマリー・キーを選択します。そのデータ・レコードについて、内部キー (セカンダリー・キー) とその値を選択します。

表 57. 「アノマリ検出ルール応答 (Anomaly Detection Rule Response)」ページのパラメーター (続き)

パラメーター	説明
カスタム・アクションの実行	ネットワーク・イベントに対する応答として特定のアクションを実行するスクリプトを作成できます。例えば、何度もログインに失敗した場合にネットワークから特定の送信元 IP アドレスをブロックするファイアウォール・ルールを作成するためのスクリプトを作成できます。 このチェック・ボックスを選択し、「**実行するカスタム・アクション**」リストからカスタム・アクションを選択します。 カスタム・アクションを追加して構成するには、「**管理**」タブの「**アクションの定義**」アイコンを使用します。
IF-MAP サーバーでの公開	IF-MAP パラメーターが構成されてシステム設定にデプロイされている場合、IF-MAP サーバーに関するオフェンス情報を公開するには、このオプションを選択します。
応答リミッター	このルールの応答頻度を構成するには、このチェック・ボックスを選択してリスト・ボックスを使用します。
ルールの有効化 (Enable Rule)	このルールを有効にするには、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。

SNMP 通知の例を以下に示します。

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name:
 ICMP Destination Unreachable Communication with Destination Host is
 Administratively Prohibited, QID: 1000156, Category: 1014, Notes:
 Offense description"
```

syslog 出力の例を以下に示します。

```
Sep 28 12:39:01 localhost.localdomain ECS:
 Rule 'Name of Rule' Fired: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID:
 1000398, Category: 1011, Notes: Event description
```

関連タスク:

218 ページの『ルールの作成』

ルールは、ルール・テスト条件に対して入力データを評価して、システムからの応答を生成します。ルールの条件が満たされると、いくつかのアクションが実行される場合があります。例えば、オフェンスの生成、E メールの送信、スキャンの開始、リファレンス・データの追加、値 (重大度など) の増減のように、ルールに対するさまざまなシステム応答を構成できます。

第 12 章 ヒストリカル相関

ヒストリカル相関を使用して、カスタム・ルール・エンジン (CRE) を通じて過去のイベントおよびフローを実行することにより、既に発生した脅威またはセキュリティー・インシデントを識別します。

制約事項: IBM Security QRadar Log Manager ではヒストリカル相関を使用できません。IBM Security QRadar SIEM と IBM Security QRadar Log Manager の相違点について詳しくは、5 ページの『Security Intelligence 製品の機能』を参照してください。

デフォルトでは、IBM Security QRadar SIEM デプロイメントにより、ほぼリアルタイムでログ・ソースおよびフロー・ソースから収集された情報が分析されます。ヒストリカル相関では、開始時刻またはデバイス時刻により相関付けを行うことができます。*開始時刻*は、QRadar がイベントを受信した時刻です。*デバイス時刻*は、デバイスでイベントが発生した時刻です。

ヒストリカル相関は、次の場合に役立ちます。

一括データを分析する。

QRadar デプロイメント内にデータを一括ロードする場合は、ヒストリカル相関を使用して、リアルタイムで収集されたデータに対してデータの相関付けを行うことができます。例えば、通常の営業時間中にパフォーマンスが低下しないようにするために、毎晩深夜に複数のログ・ソースからイベントをロードします。ヒストリカル相関を使用して、デバイス時刻によってデータの相関付けを行うことにより、過去 24 時間における一連のネットワーク・イベントを発生順に表示できます。

新しいルールをテストする。

ヒストリカル相関を実行して新しいルールをテストできます。例えば、ご使用のサーバーのいずれかが、対応するルールを用意していない新しいマルウェアにより最近攻撃されたとします。そのマルウェアを検査するルールを作成できます。次に、ヒストリカル相関を使用して、ヒストリカル・データに対してルールを検査することにより、攻撃時にルールを用意していた場合に、そのルールで応答がトリガーされるかどうかを確認できます。同様に、ヒストリカル相関を使用して、最初の攻撃の時期や攻撃の頻度を特定できます。ルールのチューニングを続行し、その後、実稼働環境内にルールを移動することができます。

損失したオフェンスまたは消去されたオフェンスを再作成する。

システムで、障害や他の理由によりオフェンスが失われた場合、その期間中に発生したイベントおよびフローに対してヒストリカル相関を実行することで、オフェンスを再作成できます。

以前に発生した隠れた脅威を識別する。

最新のセキュリティーの脅威に関する情報が認識されるのに応じて、ヒストリカル相関を使用して、既に発生したがイベントをトリガーしなかったネッ

トワーク・イベントを識別できます。組織のシステムまたはデータを既に危殆化した脅威を簡単にテストできます。

ヒストリカル相関の概要

ヒストリカル相関プロファイルを構成して、分析するヒストリカル・データおよびテストする対象のルール・セットを指定します。ルールがトリガーされると、オフェンスが作成されます。調査および修復のためにオフェンスを割り当てることができます。

データ選択

プロファイルは、保存済み検索を使用して、実行時に使用するヒストリカル・イベント・データおよびヒストリカル・フロー・データを収集します。ヒストリカル相関の実行に含めるイベントおよびフローを表示する権限がセキュリティー・プロファイルによって付与されていることを確認してください。

ルール選択および処理

QRadar コンソールは、ヒストリカル相関プロファイルで指定されたルールのみに照らしてデータを処理します。

イベントとフローの両方の共通ルール・テスト・データ。イベントとフローの両方を表示する権限を持っていなければ、共通ルールをプロファイルに追加することはできません。イベントとフローの両方を表示する権限を持たないユーザーがプロファイルを編集すると、自動的に共通ルールがプロファイルから削除されます。

無効なルールをヒストリカル相関プロファイルに含めることができます。プロファイルの実行時には、無効なルールが入力イベントおよびフローに対して評価されます。ルールがトリガーされ、ルール・アクションでオフェンスの生成が指定されている場合は、ルールが無効になっていても、オフェンスが作成されます。不要な情報によって注意が妨げられないように、ヒストリカル相関中は、ルールの応答 (レポート生成やメール通知など) が無視されます。

ヒストリカル相関の処理は単一のロケーションで実行されるため、プロファイルに含まれているルールはグローバル・ルールとして扱われます。この処理によってルールがローカルからグローバルに変更されることはありませんが、ヒストリカル相関の実行時には、ルールはグローバルであるかのように扱われます。ステートフル・ルールなどの一部のルールは、ローカルのイベント・プロセッサーで実行される通常の相関の場合と同じ応答を起動しないことがあります。例えば、5 分以内に同一のユーザー名からの 5 回のログイン失敗がないかを追跡するローカルのステートフル・ルールは、通常の相関の実行とヒストリカル相関の実行では振る舞いが異なります。通常の相関では、このローカル・ルールは、ローカルの各イベント・プロセッサーが受け取ったログイン失敗数のカウンターを維持します。ヒストリカル相関では、このルールは QRadar システム全体を対象とする単一のカウンターを維持します。この状態では、通常の相関の実行と比べて、オフェンスの作成の仕方が異なる場合があります。

オフェンス作成

ヒストリカル相関の実行では、ルールがトリガーされたときにのみオフェンスが作成され、作成すべきオフェンスはルール・アクションが指定します。ヒストリカル相関の実行は、リアルタイムのオフェンスには反映されず、同じプロファイルを使用されている場合でも、前のヒストリカル相関の実行から作成されたオフェンスには反映されません。

ヒストリカル相関の実行によって作成できるオフェンスの最大数は 100 件です。制限に達すると、ヒストリカル相関の実行が停止します。

リアルタイムのオフェンスを確認するのと同時に、「脅威およびセキュリティーのモニター」ダッシュボードおよび「**オフェンス**」タブにヒストリカル・オフェンスを表示できます。

ヒストリカル相関プロファイルの作成

カスタム・ルール・エンジン (CRE) を通じて過去のイベントおよびフローを再実行するには、ヒストリカル相関プロファイルを作成します。プロファイルには、データ・セットに関する情報と、実行中に使用するルールが入ります。

制約事項: ヒストリカル・プロファイルは IBM Security QRadar SIEM でのみ作成できます。IBM Security QRadar Log Manager ではヒストリカル・プロファイルは作成できません。

始める前に

イベントとフローの両方の共通ルール・テスト・データ。イベントとフローの両方を表示する権限を持っていなければ、共通ルールをプロファイルに追加することはできません。イベントとフローの両方を表示する権限を持たないユーザーがプロファイルを編集すると、自動的に共通ルールがプロファイルから削除されます。

このタスクについて

開始時刻またはデバイス時刻のいずれかによって相関するようにプロファイルを構成することができます。*開始時刻* は、イベントがイベント・コレクターに到達した時刻です。*デバイス時刻*は、デバイスでイベントが発生した時刻です。イベントは開始時刻またはデバイス時刻により相関付けを行うことができます。フローは開始時刻でのみ相関付けを行うことができます。

無効なルールをプロファイルに含めることができます。無効なルールは、ルール・リストのルール名の後に「**(無効)**」と示されます。

ヒストリカル相関の実行は、リアルタイムのオフェンスには反映されず、同じプロファイルを使用されている場合でも、前のヒストリカル相関の実行から作成されたオフェンスには反映されません。

手順

1. 「ヒストリカル相関」ダイアログ・ボックスを開きます。
   - 「**ログ・アクティビティー**」タブで、「**アクション**」 > 「**ヒストリカル相関**」をクリックします。

- 「**ネットワーク・アクティビティー**」タブで、「**アクション**」 > 「**ヒストリカル相関**」をクリックします。
- 「**オフェンス**」タブで、「**ルール**」 > 「**アクション**」 > 「**ヒストリカル相関**」をクリックします。

2. 「**追加**」 をクリックし、「**イベント・プロファイル**」または「**フロー・プロファイル**」を選択します。
3. プロファイルの名前を入力し、保存済み検索を選択します。 非集約保存済み検索のみを使用できます。
4. 「**ルール**」タブで、ヒストリカル・データに対して実行するルールを選択し、相関時刻を選択します。

   「**すべての有効なルールを使用**」チェック・ボックスを選択する場合は、無効なルールをプロファイルに含めることができません。有効なルールと無効なルールの両方をプロファイルに含める場合は、ルール・リストから個別に選択して「**選択項目の追加**」をクリックする必要があります。
5. 「**スケジュール**」タブで、保存済み検索の時刻範囲を入力してプロファイルのスケジュールを設定します。
6. 「**サマリー**」タブで構成を確認し、プロファイルを直ちに実行するかどうかを選択します。
7. 「**保存**」をクリックします。

   プロファイルは処理のためにキューに入れられます。スケジュールに基づいてキューに入れられたプロファイルは、手動の実行よりも優先されます。

ヒストリカル相関の実行に関する情報の表示

ヒストリカル相関プロファイルの履歴を表示して、プロファイルの過去の実行に関する情報を確認します。実行中に作成されたオフェンスのリスト、およびプロファイル内でトリガーされたルールに一致するイベントまたはフローのカタログを表示できます。さまざまな状態 (キュー待機、実行中、完了、エラーで完了、およびキャンセル) のヒストリカル相関の実行の履歴を表示できます。

このタスクについて

オフェンスが作成されなかった場合でも、実行中に、固有の送信元 IP アドレスそれぞれについてトリガーされたルールごとにヒストリカル相関カタログが作成されます。カタログには、トリガーされたルールに完全または部分的に一致したすべてのイベントまたはフローが入ります。

ヒストリカル相関データのレポートを QRadar から直接作成することはできません。サード・パーティー製のプログラムを使用してレポートを作成する場合は、データを QRadar からエクスポートできます。

手順

1. 「ヒストリカル相関」ダイアログ・ボックスを開きます。
   - 「**ログ・アクティビティー**」タブで、「**アクション**」 > 「**ヒストリカル相関**」をクリックします。

- 「**ネットワーク・アクティビティー**」タブで、「**アクション**」 > 「**ヒストリカル相関**」をクリックします。
- 「**オフェンス**」タブで、「**ルール**」 > 「**アクション**」 > 「**ヒストリカル相関**」をクリックします。

2. プロファイルを選択し、「**履歴の表示**」をクリックします。
   a. ヒストリカル相関の実行状況が「**完了**」であり、かつ「**オフェンス数**」が 0 である場合は、プロファイル・ルールがオフェンスをトリガーしていません。
   b. ヒストリカル相関の実行でオフェンスが作成された場合は、「**オフェンス数**」列のリンクをクリックすると、作成されたオフェンスのリストが表示されます。 オフェンスが 1 つしか作成されなかった場合は、オフェンスのサマリーが表示されます。
3. 「**カタログ**」列のリンクをクリックすると、プロファイル・ルールに完全または部分的に一致したイベントのリストが表示されます。

   イベント・リストの「**開始時刻**」列は、QRadar がイベントを受信した時刻を表します。
4. 「**閉じる**」をクリックします。

第 13 章 X-Force Threat Intelligence フィードの統合

IBM Security X-Force Threat Intelligence フィードは、悪意のある可能性がある IP アドレスおよび URL の最新リストを提供します。この情報は、ルール、オフェンス、およびイベントに取り込むことができ、望ましくないアクティビティーがネットワークの安定性を脅かす前に、ネットワーク環境内でそのようなアクティビティーを識別するために使用できます。

X-Force Threat Intelligence フィードを QRadar と併用するには、QRadar ライセンス拡張機能が必要です。

X-Force Threat Intelligence フィード内のコンテンツには、脅威スコアが与えられます。この脅威スコアを使用して、このコンテンツを通じて生成されるインシデントおよびオフェンスに優先順位を付けることができます。これらの情報ソースからのデータは QRadar の相関および分析機能に自動的に取り込まれ、インターネットの脅威データによって脅威検出機能が強化されます。これらのアドレスを含むすべてのセキュリティー・イベント・データまたはネットワーク・アクティビティー・データに自動的にフラグが立てられるため、セキュリティー・インシデントの分析および調査に対して有用なコンテキストが追加されます。

脅威に優先順位を付け、詳細な調査が必要なセキュリティー・インシデントを識別するために、QRadar のルール、オフェンス、およびイベントに取り込む X-Force フィードを選択できます。例えば、フィードを使用して以下のタイプのインシデントを識別できます。

- 動的 IP アドレス範囲に対する連続したログイン試行
- ビジネス・パートナー・ポータルへの匿名プロキシー接続
- 内部エンドポイントと既知のボットネット・コマンドやコントロールの間の接続
- エンドポイントと既知のマルウェア配布サイトの間の通信

X-Force Threat Intelligence フィードは、IP アドレスをカテゴリーに分類してから、このカテゴリーに信頼性評価値を割り当てます。0 から 100 までの信頼性係数値が IP レピュテーション・データのカテゴリーに割り当てられます。この信頼値は、この IP アドレスからのデータが正確なカテゴリーに分類されているかどうかについて、X-Force が評価する信頼性を表します。スパムの IP レピュテーション・カテゴリーの信頼性係数値が 0 である場合は、送信元 IP のトラフィックが確実にスパムではないことを示します。100 である場合は、送信元 IP のトラフィックが確実にスパムであることを示します。ルールをチューニングするときに、信頼性係数値を使用して、ルール・トリガーの感度を調整できます。この信頼性係数値を調整して、生成されるオフェンスの数を調整します。

IP アドレスは以下のカテゴリーにグループ化されています。

- マルウェア・ホスト
- スパム送信元
- 動的 IP アドレス
- 匿名プロキシー

- ボットネット・コマンドとコントロール
- IP アドレスのスキャン

X-Force Threat Intelligence フィードは、URL アドレスも分類します。例えば、URL アドレスが出会い系、ギャンブル、またはポルノ・サイトとして分類される場合があります。URL 分類用のカテゴリーの詳細なリストについては、IBM X-Force Exchange Web サイト (https://exchange.xforce.ibmcloud.com/faq) を参照してください。

URL ベースのルールを使用するには、カスタム・イベント・プロパティーを作成し、ペイロードから URL を抽出する必要があります。URL カスタム・プロパティーは、Blue Coat SG や Juniper Networks Secure Access など、多くのソースによるイベントに対して既に定義されています。

カスタム・イベント・プロパティーの作成方法について詳しくは、カスタム・イベント・プロパティーとカスタム・フロー・プロパティーを参照してください。

X-Force Threat Intelligence の更新およびサーバー

IBM Security X-Force Threat Intelligence フィードを QRadar に追加した直後から、拡張された脅威データを受信できます。

全体として、X-Force からのデータ・セットは 3 分ごとに更新され、QRadar コンソールはすべての外部通信を処理します。

X-Force のデータ更新、ライセンス、ダッシュボード・ウィジェット・フィード、および QRadar の自動更新のために、以下のサーバーに接続します。

表 58. X-Force サーバー

接続先のサーバー	サーバーの説明
www.iss.net	QRadar 用の X-Force Threat Intelligence ダッシュボード・ウィジェット (AlertCon / RSS フィード)
update.xforce-security.com	IP レピュテーションおよび URL データ用の X-Force Threat Intelligence フィード更新サーバー
license.xforce-security.com	X-Force Threat Intelligence ライセンス・サーバー
qmmunity.q1labs.com	QRadar 自動更新。自動更新サーバーについて詳しくは、www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881) を参照してください。

IBM Security QRadar での X-Force ルールの有効化

X-Force IP Reputation Intelligence Feed のライセンスを QRadar システムに追加すると、拡張 X-Force ルールが追加されます。

手順

1. 「**ログ・アクティビティー**」タブをクリックします。
2. ツールバーで、「**ルール**」 > 「**ルール**」をクリックします。
3. 「**グループ**」メニューから、「**XForce Premium**」をクリックします。

「**グループ**」列には、レガシー・ルールと拡張ルールの両方が表示されることがあります。デフォルトでは、X-Force レガシー・ルールは無効になっています。しかし、有効になっているレガシー・ルールが表示されることがあります。リモート・ネットを使用するレガシー・ルールではなく、新しい拡張ルールを使用してください。リモート・ネット・オプションは削除されています。

4. ルール行を選択し、「**アクション**」 > 「**有効化/無効化**」をクリックして、すべてのレガシー・ルール (X-Force Premium ルール) を無効にします。

拡張された X-Force Threat Intelligence ルール

X-Force Threat Intelligence フィードを QRadar に追加した後で、拡張 X-Force ルール・グループからのルールの使用を開始できます。

以下のルールは「**拡張 X-Force ルール**」グループの一部です。これらはそのまま使用することも、カスタマイズすることもできます。

以下のルールは IP ベースです。

X-Force Premium: マルウェアの可能性があるホストへの内部接続 (X-Force Premium: Internal Connection to Possible Malware Host)

この通信は、クライアント・システムへの感染が試行されたか、マルウェアがダウンロードされた可能性が高いことを示します。

X-Force Premium: 内部ホストと匿名プロキシーとの通信 (X-Force Premium: Internal Hosts Communicating With Anonymous Proxies)

匿名プロキシー は、ID をマスキングするための既知のアドレスです。多くの場合、外部ソースとの通信の発信元を隠蔽するために、マルウェアによって使用されたり、永続的かつ高度な脅威にさらされている間に使用されたりします。これらのアドレスは、マルウェア通信やデータ引き出しなどのアクティビティーに関連している可能性があります。

X-Force Premium: 内部メール・サーバーからスパムの可能性があるホストへのメール送信 (X-Force Premium: Internal Mail Server Sending Mail to Possible SPAM Host)

通常、スパム・ホストと通信するメール・サーバーは悪用されています。

X-Force Premium: メール・サーバー以外のマシンによる既知のスパム送信ホストとの通信 (Force Premium: Non-Mail Servers Communicating with Known SPAM Sending Hosts)

この動作は、サーバーが危険にさらされており、スパムの中継点として使用されている可能性が高いことを示します。

X-Force Premium: サーバー以外のマシンによる外部の動的 IP との通信 (X-Force Premium: Non-Servers Communicating with an External Dynamic IP)

通常、動的に割り当てられた IP アドレスは、インターネット上の正当なサーバーに関連付けられていません。内部のワークステーションが動的アドレスと通信している場合は、疑わしい内部アクティビティー、マルウェアやボットネットのアクティビティーが実行されている可能性があります。

X-Force Premium: サーバーによる動的ホストとの接続の開始 (X-Force Premium: Server Initiated Connection to Dynamic Hosts)
通常、サーバーは、動的 IP アドレスではなく、固定 ID を持つホストと通信します。

URL は転送されるデータを詳細に示すため、URL ベースのルールは IP ベースのルールより精度が高くなる場合があります。

以下のルールは URL ベースです。

X-Force Premium: 内部ホストによるボットネット・コマンドとコントロール URL との通信 (X-Force Premium: Internal Host Communicating with Botnet Command and Control URL)
正当なサーバーが、特定の URL アドレスでのボットネット接続の拠点として使用されることがあります。

X-Force Premium: 内部ホストによるマルウェア URL との通信 (X-Force Premium: Internal Host Communication with Malware URL)
正当なサーバーが、特定の URL アドレスへのマルウェアの配布に使用されることがあります。

特定のタイプの Web サイトへのアクセスをモニターするための URL 分類を使用したルールの作成

ギャンブルの Web サイトとして分類されている URL アドレスに内部ネットワークのユーザーがアクセスしている場合に E メール通知を送信するルールを作成することができます。

始める前に

URL 分類ルールを使用するには、X-Force Threat Intelligence フィードへのサブスクリプションが必要です。

新規ルールを作成するには、「**オフェンス**」 > 「**カスタム・ルールの保守**」権限が必要です。

手順

1. 「**オフェンス**」タブをクリックします。
2. ナビゲーション・メニューで、「**ルール**」をクリックします。
3. 「**アクション**」リストから、「**新規イベント・ルール**」を選択します。
4. ルール・ウィザードで概要説明を読み、「**次へ**」をクリックします。
5. 「**イベント**」をクリックしてから「**次へ**」をクリックします。
6. 「**テスト・グループ**」リスト・ボックスから「**X-Force テスト (X-Force Tests)**」を選択します。
7. 「**この URL プロパティーが X-Force によって以下のいずれかのカテゴリーとして分類された場合 (when this URL property is categorized by X-Force as one of the following categories)**」というテストの横にあるプラス (+) 記号をクリックします。

8. 「ルール」ペインの「**ルール名をここに入力してください (enter rule name here)**」フィールドに、このルールに割り当てる固有の名前を入力します。
9. リスト・ボックスから、「**ローカル (Local)**」または「**グローバル (Global)**」を選択します。
10. 下線付きの構成可能なパラメーターをクリックして、テストの変数をカスタマイズします。
    a. 「**URL (カスタム) (URL (custom))**」をクリックします。
    b. ペイロードから抽出された URL を含む URL プロパティーを選択して「**送信**」をクリックします。
    c. 「**以下のいずれかのカテゴリー (one of the following categories)**」をクリックします。
    d. X-Force の URL カテゴリーから「**ギャンブル/くじ (Gambling / Lottery)**」を選択し、「**追加 +**」をクリックしてから「**送信**」をクリックします。
11. 構成したルールを他のルールと共に使用するためにビルディング・ブロックとしてエクスポートするには、次のようにします。
    a. 「**ビルディング・ブロックとしてエクスポート (Export as Building Block)**」をクリックします。
    b. このビルディング・ブロックに固有の名前を入力します。
    c. 「**保存**」をクリックします。
12. 「グループ (Groups)」ペインで、このルールの割り当て先の各グループのチェック・ボックスを選択します。
13. 「**メモ**」フィールドに、このルールに指定するメモを入力し、「**次へ**」をクリックします。
14. 「ルール応答」ページで「**E メール**」をクリックし、通知を受信するための E メール・アドレスを入力します。 イベント・ルールのその他の応答パラメーターについて詳しくは、「イベント」、「フロー」、「共通」の「ルールの応答」ページのパラメーターを参照してください。
15. 「**次へ**」をクリックします。
16. ルールに間違いがなければ「**終了**」をクリックします。

X-Force Exchange での IP アドレスおよび URL 情報のルックアップ

IBM Security QRadar の右クリック・メニューのオプションを使用して、IBM Security X-Force Exchange にある IP アドレスおよび URL に関する情報をルックアップできます。QRadar の検索、オフェンス、およびルールからの情報を使用して、IP アドレスや URL についてさらに調査したり、それらの情報を X-Force Exchange コレクションに追加したりすることができます。

このタスクについて

セキュリティー上の問題を調査するときは、コレクション内のデータを追跡するために、公開情報または秘密情報のいずれかを提供できます。

コレクション とは、調査中に検出される情報を保管するリポジトリーのことです。コレクションを使用して、X-Force Exchange のレポート、コメント、または他のすべての内容を保存できます。 X-Force Exchange レポートには、保存時バージョンの

レポートと、現在バージョンのレポートへのリンクの両方が含まれます。さらにコレクションには、Wiki スタイルのノートパッドがあるセクション (タイムライン) があります。ここにはコレクションに関連するコメントを追加できます。

X-Force Exchange について詳しくは、X-Force Exchange (https://exchange.xforce.ibmcloud.com/) を参照してください。

手順

1. X-Force Exchange で QRadar からの IP アドレスをルックアップするには、以下の手順を実行します。
   a. 「**ログ・アクティビティー**」 タブまたは「**ネットワーク・アクティビティー**」タブを選択します。
   b. X-Force Exchange で表示する IP アドレスを右クリックし、「**その他のオプション**」 > 「**プラグイン・オプション**」 > 「**X-Force Exchange ルックアップ (X-Force Exchange Lookup)**」を選択して、X-Force Exchange インターフェースを開きます。
2. X-Force Exchange で QRadar からの URL をルックアップするには、以下の手順を実行します。
   a. 「**オフェンス**」タブ、または「**オフェンス**」で選択できるイベント詳細ウィンドウを選択します。
   b. X-Force Exchange でルックアップする URL を右クリックし、「**プラグイン・オプション**」>「**X-Force Exchange ルックアップ (X-Force Exchange Lookup)**」を選択して、X-Force Exchange インターフェースを開きます。

フォールス・ポジティブの管理

ネットワーク内のフォールス・ポジティブの数を減少させることができるように、X-Force Threat Intelligence を使用して、ルール・トリガーの感度を管理します。フォールス・ポジティブのチューニングを使用して、イベントおよびフローでオフェンスへの相関付けが行われないようにします。

信頼性係数

X-Force は、IP レピュテーション・データをカテゴリーに分類し、そのカテゴリーに 0 から 100 までの信頼性係数値を割り当てます。ここで、0 は信頼性がないことを表し、100 は確実であることを表します。例えば、X-Force は、ある送信元 IP アドレスを、信頼性係数が 75 であるスキャン IP としてカテゴリーに分類することがあります。これは、中程度に高い信頼性レベルです。

信頼値の入力方法

信頼値は、QRadar の以下の X-Force ルール・テストで入力します。「**このホスト・プロパティーが X-Force によってこの量と等しい信頼値を持つこのカテゴリーとして分類された場合 (when this host property is categorized by X-Force as this category with confidence value equal to this amount)**」

信頼値を設定するためのガイドライン

信頼性係数は、トリガーされたルールによって作成されるオフェンスの数を制限するために使用できる主要な手段の 1 つです。必要な保護のレベルに応じて、ネットワーク環境にとって最適なレベルに信頼値を調整できます。

DMZ では多くのオフェンスを調査する必要がないため、この領域では、高い信頼値 (例えば、95% 以上) を選択することをお勧めします。この信頼性レベルでは、IP アドレスは、リストされているカテゴリーに一致する可能性が高くなります。あるホストがマルウェアを提供していることが 95% 確実である場合、ユーザーはそのことを認識する必要があります。

サーバー・プールなどのより安全なネットワーク領域では、信頼値を低くします。信頼性レベルを低くすると、より多くの脅威が検出される可能性があります。脅威は特定のネットワーク・セグメントに関連するため、調査に費やされる労力は少なくて済みます。

フォールス・ポジティブの最適なチューニングのためには、ルール・トリガーをセグメントごとに管理します。ネットワーク・インフラストラクチャーを検討し、高いレベルの保護が必要であるアセットおよび必要でないアセットを決定します。ネットワーク・セグメントごとに異なる信頼値を適用できます。ビルディング・ブロックを使用して、よく使用されるテストをグループ化しておくと、それらのビルディング・ブロックをルール内で使用できます。

URL ベースのルール

共有仮想ホスティング・サイトからのフォールス・ポジティブが表示されることがあります。これは、1 つのサイトが正当なコンテンツを提供していても、同じ IP アドレスの別のサイトはマルウェアを提供していることがあるからです。共有仮想ホスティング・セットアップでは、URL は転送されるデータを詳細に示すため、URL 情報が役立ちます。URL ベースのルールは IP ベースのルールより精度が高くなる場合があります。

URL ベースのルールでは、カスタム・イベント・プロパティーを作成して、ペイロードから URL を抽出する必要があります。

フォールス・ポジティブのチューニングについては、「*チューニング・ガイド*」を参照してください。

第 14 章 レポートの管理

「**レポート**」タブを使用して、レポートを作成、編集、配布、および管理することができます。

詳細で柔軟なレポート作成オプションが使用できるため、PCI コンプライアンスなどのさまざまな規制基準を満たすことができます。

独自のカスタム・レポートを作成することも、デフォルト・レポートを使用することもできます。デフォルト・レポートをカスタマイズしてブランドを付け直し、他のユーザーに配布することができます。

システムに多数のレポートが含まれている場合、「**レポート**」タブの最新表示には時間がかかることがあります。

注: Microsoft Exchange Server 5.5 を実行している場合、E メールで送信されるレポートの件名行に無効なフォントの文字が表示されることがあります。この問題を解決するには、Microsoft Exchange Server 5.5 の Service Pack 4 をダウンロードしてインストールしてください。詳しくは、Microsoft のサポートにお問い合わせください。

タイム・ゾーンの考慮事項

レポート機能でデータのレポート作成に正しい日時を使用するようにするには、ご使用のセッションをご使用のタイム・ゾーンと同期する必要があります。

タイム・ゾーンは、QRadar 製品のインストールとセットアップ中に構成されます。管理者に問い合わせて、ご使用の QRadar セッションがご使用のタイム・ゾーンと同期するようにしてください。

「レポート」タブの権限

管理ユーザーは、他のユーザーが作成したすべてのレポートを表示することができます。

非管理ユーザーは、自分で作成したレポート、および他のユーザーによって共有されているレポートを表示できます。

「レポート」タブのパラメーター

「**レポート**」タブには、デフォルト・レポートとカスタム・レポートのリストが表示されます。

「**レポート**」タブから、レポート・テンプレートに関する統計情報の表示、レポート・テンプレートに対するアクションの実行、生成されたレポートの表示、生成されたコンテンツの削除を行うことができます。

レポートで間隔スケジュールが指定されていない場合、レポートの手動生成が必要になります。

マウス・ポインターをすべてのレポートに合わせると、ツールチップにレポートのサマリーがプレビューされます。このサマリーでは、レポートの構成と、そのレポートで生成されるコンテンツのタイプが指定されます。

レポートのレイアウト

レポートは複数のデータ・エレメントから構成することができ、ネットワークおよびセキュリティーのデータを、表、折れ線グラフ、円グラフ、棒グラフなどのさまざまなスタイルで表現できます。

レポートのレイアウトを選択する際は、作成するレポートのタイプに配慮してください。例えば、多数のオブジェクトを表示するグラフ・コンテンツの場合は、小さなグラフ・コンテナーを選択しないでください。各グラフには、凡例と、コンテンツの派生元になったネットワークのリストが含まれます。それらのデータを格納できる十分な大きさのコンテナーを選択してください。各グラフでデータがどのように表示されるのかをプレビューするには、グラフ・タイプを参照してください。

グラフ・タイプ

レポートの作成時に、そのレポートに組み込むそれぞれのグラフのグラフ・タイプを選択する必要があります。

グラフ・タイプにより、生成されたレポートでデータとネットワーク・オブジェクトがどのように表示されるかが決まります。複数の特性を備えたデータをグラフ化して、生成された単一レポート内でそのグラフを作成することができます。

以下のタイプのグラフを使用できます。

- **なし** - レポートに空のコンテナーを表示するには、このオプションを使用します。このオプションは、レポートに空白を設けたい場合に役立ちます。すべてのコンテナー用に「**なし**」オプションを選択した場合、そのコンテナーについてそれ以上の構成を行う必要はありません。
- **アセットの脆弱性** - デプロイメント内の定義された各アセットの脆弱性データを表示するには、このグラフを使用します。「アセットの脆弱性」グラフは、VA スキャンで脆弱性が検出されたときに生成することができます。このグラフは、IBM Security QRadar Vulnerability Manager のインストール後に使用可能になります。
- **接続** - このグラフ・オプションは、IBM Security QRadar Risk Manager を購入してそのライセンス交付を受けている場合にのみ表示されます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。
- **デバイス・ルール** - このグラフ・オプションは、IBM Security QRadar Risk Manager を購入してそのライセンス交付を受けている場合にのみ表示されます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。
- **デバイス未使用オブジェクト** - このグラフ・オプションは、IBM Security QRadar Risk Manager を購入してそのライセンス交付を受けている場合にのみ表示されます。詳細については、「*IBM Security QRadar Risk Manager User Guide*」を参照してください。

- **イベント/ログ** - イベント情報を表示するには、このグラフを使用します。「**ログ・アクティビティー**」タブから得られる保存済み検索のデータを基に、グラフを作成することができます。生成されるレポートで表示するデータをカスタマイズすることができます。構成可能な期間にわたってデータを作図するようにグラフを構成することができます。この機能は、イベントの傾向を検出するために役立ちます。保存済み検索について詳しくは、データの検索を参照してください。
- **ログ・ソース** - このグラフはログ・ソースをエクスポートする場合やログ・ソースに基づいてレポートを作成する場合に使用します。レポートに表示したいログ・ソースおよびログ・ソース・グループを選択します。レポート列でログ・ソースをソートします。定義済みの期間の間報告されていないログ・ソースを含めます。指定された時刻に作成されたログ・ソースを含めます。
- **フロー** - フロー情報を表示するには、このグラフを使用します。「ネットワーク・アクティビティー」タブから得られる保存済み検索のデータを基に、グラフを作成することができます。これにより、生成されるレポートで表示するデータをカスタマイズすることができます。保存済み検索を使用して、構成可能な期間にわたってフロー・データを作図するようにグラフを構成することができます。この機能は、フローの傾向を検出するために役立ちます。保存済み検索について詳しくは、データの検索を参照してください。
- **上位の宛先 IP** - 選択したネットワーク・ロケーションにおける上位の宛先 IP を表示するには、このグラフを使用します。
- **上位のオフェンス** - 選択したネットワーク・ロケーションで現在発生している上位のオフェンスを表示するには、このグラフを使用します。
- **上位の送信元 IP** - ネットワーク・アセットまたはビジネス・アセットを攻撃する上位のオフェンスの送信元 (IP アドレス) の表示およびソートを行うには、このグラフを使用します。
- **脆弱性** - 脆弱性オプションは、IBM Security QRadar Vulnerability Manager を購入してライセンス交付を受けている場合にのみ表示されます。詳細については、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

「レポート」タブ・ツールバー

このツールバーを使用して、レポートに対していくつかのアクションを実行できます。

次の表で、「レポート」ツールバーのオプションを示し、それらについて説明します。

表 59. 「レポート」ツールバーのオプション

オプション	説明
グループ	
グループの管理	レポート・グループを管理するには、「**グループの管理**」をクリックします。「グループの管理」機能を使用することにより、レポートを機能グループ別に編成できます。レポート・グループを他のユーザーと共有することができます。

表 59. 「レポート」ツールバーのオプション (続き)

オプション	説明
アクション	以下のアクションを実行するには、「**アクション**」をクリックします。 • **作成 (Create)** - 新規レポートを作成するには、このオプションを選択します。 • **編集** - 選択したレポートを編集するには、このオプションを選択します。レポートをダブルクリックしてコンテンツを編集することもできます。 • **コピー (Duplicate)** - 選択したレポートをコピーまたは名前変更するには、このオプションを選択します。 • **割り当て** - 選択したレポートをレポート・グループに割り当てるには、このオプションを選択します。 • **共有 (Share)** - 選択したレポートを他のユーザーと共有するには、このオプションを選択します。レポートを共有するには、管理特権が必要です。 • **スケジューリングの切り替え (Toggle Scheduling)** - 選択したレポートをアクティブ状態または非アクティブ状態に切り替えるには、このオプションを選択します。 • **レポートの実行** - 選択したレポートを生成するには、このオプションを選択します。複数のレポートを生成するには、Ctrl キーを押したまま、生成したいレポートをクリックしてください。 • **Raw data でレポートを実行** - 生データを使用して選択したレポートを生成するには、このオプションを選択します。このオプションは、必要な集計データが得られる前にレポートを生成したい場合に役立ちます。例えば、レポートを作成してからまだ 1 週間経過していないときに週次レポートを実行したい場合、このオプションを使用してレポートを生成することができます。 • **レポートの削除** - 選択したレポートを削除するには、このオプションを選択します。複数のレポートを削除するには、Ctrl キーを押したまま、削除するレポートをクリックしてください。 • **生成されたコンテンツの削除** - 選択した行に関して生成されたすべてのコンテンツを削除するには、このオプションを選択します。複数の生成済みレポートを削除するには、Ctrl キーを押したまま、削除する生成済みレポートをクリックしてください。
非アクティブ・レポートの非表示	非アクティブなレポートを非表示にするには、このチェック・ボックスを選択します。「**レポート**」タブが自動的に最新表示され、アクティブなレポートのみが表示されるようになります。非表示になっている非アクティブ・レポートを表示するには、このチェック・ボックスをクリアします。

表 59. 「レポート」ツールバーのオプション (続き)

オプション	説明
レポートの検索 (Search Reports)	「**レポートの検索 (Search Reports)**」フィールドに検索条件を入力して、「**レポートの検索 (Search Reports)**」アイコンをクリックします。以下のパラメーターで検索が実行され、指定された基準に一致するレポートが判別されます。 • レポート・タイトル • レポートの説明 • レポート・グループ (Report Group) • レポート・グループ (Report Groups) • レポート作成者のユーザー名 (Report Author User Name)

グラフ・タイプ

各グラフ・タイプでは、データを表示する際に使用できる各種のグラフ・タイプがサポートされます。

ネットワーク構成ファイルにより、ネットワーク・トラフィックを表すためにグラフで使用される色が決まります。各 IP アドレスは固有の色で表示されます。以下の表に、グラフ内でのネットワーク・データとセキュリティー・データの使用例を示します。この表では、各タイプのグラフで使用可能なグラフ・タイプを示しています。

表 60. グラフ・タイプ

グラフ・タイプ	使用可能なグラフ・タイプ
折れ線	• イベント/ログ • フロー • 接続 • 脆弱性
積み重ね線	• イベント/ログ • フロー • 接続 • 脆弱性
棒	• イベント/ログ • フロー • アセット脆弱性接続 (Asset Vulnerabilities Connections) • 接続 • 脆弱性
横棒	• 上位の送信元 IP • 上位のオフェンス • 上位の宛先 IP

表 60. グラフ・タイプ (続き)

グラフ・タイプ	使用可能なグラフ・タイプ
積み重ね棒	• イベント/ログ • フロー • 接続
円	• イベント/ログ • フロー • アセットの脆弱性 • 接続 • 脆弱性
表	• イベント/ログ • フロー • 上位の送信元 IP • 上位のオフェンス • 上位の宛先 IP • 接続 • 脆弱性 表の内容を表示するには、全ページ幅コンテナーを使用してレポートを設計する必要があります。
集計表	アセットの脆弱性グラフで使用することができます。 表の内容を表示するには、全ページ幅コンテナーを使用してレポートを設計する必要があります。

QRadar Log Manager のレポートでは、以下のグラフ・タイプを使用することができます。

- 折れ線グラフ (Line Graph)
- 積み重ね折れ線グラフ (Stacked Line Graph)
- 棒グラフ (Bar Graph)
- 積み重ね棒グラフ (Stacked Bar Graph)
- 円グラフ (Pie Graph)
- 表グラフ (Table Graph)

注: 棒グラフや積み重ね棒グラフのレポートを作成する場合、固定形式の凡例が表示されます。ここでは多くの場合、棒または棒の各セクションが色分けされたラベルで表されます。x 軸の値として時間を選択すると、x 軸上に時間間隔を作成できます。

カスタム・レポートの作成

レポート・ウィザードを使用して、新規のレポートを作成およびカスタマイズします。

始める前に

生成されたレポートを他のユーザーと共有するには、適切なネットワーク権限が必要です。

権限の詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

このタスクについて

レポート・ウィザードでは、レポートの設計、スケジューリング、および生成の手順が段階的に示されます。

このウィザードでは、以下の主要な要素を使用してレポートの作成を支援します。

- **レイアウト** - 各コンテナーの位置とサイズ
- **コンテナー** - フィーチャー・コンテンツのプレースホルダー
- **コンテンツ** - コンテナーに配置されるグラフの定義

週に 1 回または月に 1 回生成されるレポートを作成した場合は、スケジュールした時間が経過しないと、生成されたレポートから結果が返されません。スケジュールされたレポートの場合は、スケジュールされた時間が経過するまでレポートが作成されません。例えば、週に 1 回の検索では、データが作成されるまでに 7 日間を要します。この検索では、7 日後に結果が返されます。

レポートの出力フォーマットを指定する際には、選択した出力フォーマットに応じて、生成されるレポートのファイル・サイズが 1 メガバイトから 2 メガバイトになるようにすることを検討してください。PDF 形式は、サイズが小さく、ディスク・ストレージ・スペースを大量に使用しません。

手順

1. 「**レポート**」タブをクリックします。
2. 「**アクション**」リスト・ボックスから「**作成 (Create)**」を選択します。
3. 「レポート・ウィザードへようこそ」ウィンドウで、「**次へ**」をクリックします。
4. 次のオプションのいずれかを選択します。

オプション	説明
手動	デフォルトでは、レポートは 1 回生成されます。レポートは、必要な回数生成できます。

オプション	説明
毎時 (Hourly)	各時間の終わりに、レポートが生成されるようにスケジュールします。前の時間からのデータが使用されます。 リスト・ボックスから、レポート作成サイクルの開始と終了を指定する時間フレームを選択します。レポートは、この時間フレーム内で 1 時間ごとに生成されます。時刻は、30 分単位で指定できます。デフォルトは、「**開始 (From)**」フィールドも「**終了 (To)**」フィールドも 1:00 a.m. です。
毎週	前週のデータを使って週に 1 回レポートが生成されるようにスケジュールします。 レポートを生成する曜日を選択します。デフォルトは月曜日です。リスト・ボックスから、レポート作成サイクルの開始時刻を選択します。時刻は、30 分単位で指定できます。デフォルトは 1:00 a.m. です。
毎月	前月のデータを使って月に 1 回レポートが生成されるようにスケジュールします。 リスト・ボックスから、レポートを生成する日付を選択します。デフォルトは月の初日です。レポート作成サイクルの開始時刻を選択します。時刻は、30 分単位で指定できます。デフォルトは 1:00 a.m. です。

5. 「**このレポートの手動生成を許可しますか**」ペインで、「**はい**」または「**いいえ**」を選択します。
6. レポートのレイアウトを構成します。
   a. 「**方向**」リスト・ボックスから、ページの方向として「**縦長**」または「**横長**」を選択します。
   b. レポート・ウィザードに表示される 6 つのレイアウト・オプションから 1 つを選択します。
   c. 「**次へ**」をクリックします。
7. 次の各パラメーターの値を指定します。

パラメーター	値
レポート・タイトル	タイトルの最大長は 100 文字です。特殊文字は使用しないでください。
ロゴ	リスト・ボックスからロゴを選択します。
ページ編集オプション	リスト・ボックスから、レポートに表示するページ番号の場所を選択します。ページ番号の非表示も選択できます。

パラメーター	値
レポートの分類	このレポートの分類を入力します。最大 75 文字入力できます。先行スペース、特殊文字、および 2 バイト文字を使用できます。レポートの分類は、レポートのヘッダーおよびフッターに表示されます。必要に応じてレポートを「機密 (confidential)」、「高機密 (highly confidential)」、「重要 (sensitive)」、または「内部」として分類します。

8. レポート内の各コンテナーを構成します。
   a. 「**グラフ・タイプ**」リスト・ボックスから、グラフ・タイプを選択します。
   b. 「コンテナー詳細」ウィンドウで、グラフのパラメーターを構成します。

      注: アセットの保存済み検索も作成できます。「**使用する検索**」リスト・ボックスから、保存済み検索を選択します。
   c. 「**コンテナー詳細の保存**」をクリックします。
   d. 複数のコンテナーを選択した場合、ステップ a から c を繰り返します。
   e. 「**次へ**」をクリックします。
9. 「レイアウトのプレビュー」ページをプレビューし、「**次へ**」をクリックします。
10. 生成するレポート・フォーマットのチェック・ボックスを選択し、「**次へ**」をクリックします。

    重要: Extensible Markup Language (XML) は、表にのみ使用できます。
11. レポートの配布チャネルを選択し、「**次へ**」をクリックします。配布チャネルには以下のオプションがあります。

オプション	説明
レポート・コンソール	生成されたレポートを「**レポート**」タブに送信する場合は、このチェック・ボックスを選択します。「**レポート・コンソール**」はデフォルトの配布チャネルです。
生成されたレポートを表示可能にするユーザーを選択してください。(Select the users that should be able to view the generated report.)	このオプションは、「**レポート・コンソール**」チェック・ボックスを選択すると表示されます。 ユーザーのリストから、生成されたレポートを表示する権限を付与するユーザーを選択します。

オプション	説明
すべてのユーザーを選択 (Select all users)	このオプションは、「**レポート・コンソール**」チェック・ボックスを選択した場合にのみ表示されます。生成されたレポートを表示する権限をすべてのユーザーに付与する場合は、このチェック・ボックスを選択します。 生成されたレポートを他のユーザーと共有するには、適切なネットワーク権限が必要です。
E メール	生成されたレポートを E メールで配布する場合は、このチェック・ボックスを選択します。
レポートの宛先 E メール・アドレスの入力 (複数可)(Enter the report distribution email address(es))	このオプションは、「**E メール**」チェック・ボックスを選択した場合にのみ表示されます。 生成されたレポートの各受信者の E メール・アドレスを入力します。E メール・アドレス間はコンマで区切ってください。このパラメーターの最大長は 255 文字です。 E メールの受信者は、このメールを no_reply_reports@qradar から受け取ります。
レポートを添付ファイルとして含める (HTML 以外のみ)	このオプションは、「**E メール**」チェック・ボックスを選択した場合にのみ表示されます。生成されたレポートを添付ファイルとして送信する場合は、このチェック・ボックスを選択します。
レポート・コンソールへのリンクを含める	このオプションは、「**E メール**」チェック・ボックスを選択した場合にのみ表示されます。E メールにレポート・コンソールへのリンクを含める場合は、このチェック・ボックスを選択します。

12. 「完了」ページで、以下のパラメーターの値を入力します。

オプション	説明
レポートの説明	このレポートの説明を入力します。この説明は、「レポートのサマリー」ページおよび生成されたレポートの配布 E メールに表示されます。
このレポートをメンバーにするグループをすべて選択してください	このレポートを割り当てるグループを選択します。グループについて詳しくは、『レポート・グループ』を参照してください。
今すぐこのレポートを実行しますか?	ウィザード完了時にレポートを生成する場合は、このチェック・ボックスを選択します。このチェック・ボックスはデフォルトで選択されます。

13. 「**次へ**」をクリックしてレポートのサマリーを表示します。
14. 「レポートのサマリー」ページで、サマリー・レポートのタブを選択してレポート構成をプレビューします。

タスクの結果

レポートは即時に生成されます。ウィザードの最後のページで「**今すぐこのレポートを実行しますか?**」チェック・ボックスをクリアした場合は、レポートが保存され、スケジュールした時間に生成されます。レポート・タイトルは、生成されるレポートのデフォルトのタイトルです。レポートを再構成して新しいレポート・タイトルを入力すると、レポートが新しい名前を持つ新規のレポートとして保存され、元のレポートはそのまま保持されます。

レポートの編集

レポート・ウィザードでは、デフォルトのレポートやカスタム・レポートを編集して変更することができます。

このタスクについて

数多くのデフォルト・レポートを使用したり、カスタマイズしたりすることができます。デフォルトの「**レポート**」タブには、レポートのリストが表示されます。各レポートには、取り込まれた既存のデータが表示されます。

注: 手動で生成するスケジュール済みレポートをカスタマイズする場合、「**開始日**」を選択する前に期間の「**終了日**」を選択します。

手順

1. 「**レポート**」タブをクリックします。
2. カスタマイズするレポートをダブルクリックします。
3. レポート・ウィザードで、レポートをカスタマイズするためのパラメーターを変更して、必要なコンテンツを生成します。

タスクの結果

レポートを再構成して新しいレポート・タイトルを入力すると、レポートが新しい名前を持つ新規のレポートとして保存され、元のレポートはそのまま保持されます。

生成済みレポートの表示

レポートの内容が生成されている場合は、「**レポート**」タブの「**フォーマット (Formats)**」列にアイコンが表示されます。このアイコンをクリックして、レポートを表示することができます。

このタスクについて

レポートの内容が生成されると、「**生成済みレポート**」列にリスト・ボックスが表示されます。リスト・ボックスには、レポートのタイム・スタンプ別に編成された

生成済みの内容がすべて表示されます。リストの最上部には最新レポートが表示されます。レポートの内容が生成されていない場合は、「**生成済みレポート**」列に「**なし**」という値が表示されます。

「**フォーマット**」列には、生成済みレポートのレポート・フォーマットを表すアイコンが表示されます。

レポートは PDF、HTML、RTF、XML、および XLS フォーマットで生成できます。

注: XML と XLS フォーマットは、単一のグラフ表フォーマット (縦長または横長) を使用するレポートでのみ使用できます。

管理者からアクセス権が付与されているレポートのみを表示することができます。管理ユーザーはすべてのレポートにアクセスできます。

Mozilla Firefox Web ブラウザーを使用して、RTF レポート・フォーマットを選択すると、Mozilla Firefox Web ブラウザーで新しいブラウザー・ウィンドウが開始されます。この新しいウィンドウの起動は Mozilla Firefox Web ブラウザーの構成結果であり、QRadar への影響はありません。ウィンドウを閉じて、QRadar セッションを続行できます。

手順

1. 「**レポート**」タブをクリックします。
2. 「**生成済みレポート**」列のリスト・ボックスから、表示するレポートのタイム・スタンプを選択します。
3. 表示するフォーマットのアイコンをクリックします。

生成されたコンテンツの削除

生成されたコンテンツを削除すると、レポート・テンプレートから生成されたすべてのレポートが削除されますが、レポート・テンプレートは保持されます。

手順

1. 「**レポート**」タブをクリックします。
2. 生成されたコンテンツを削除するレポートを選択します。
3. 「**アクション**」リスト・ボックスで、「**生成されたコンテンツの削除**」をクリックします。

レポートの手動生成

レポートは自動生成されるように構成できますが、いつでも手動でレポートを生成することができます。

このタスクについて

レポートを生成する間には、「次の実行時刻」列に以下の 3 つのメッセージのいずれかが表示されます。

- 「**生成中 (Generating)**」 - レポートは生成中です。

- 「**待機中 (キューで待機) (Queued (position in the queue))**」 - レポートは生成を待機中です。このメッセージには、キュー内のレポートの位置が示されます。例えば、「1 of 3」などです。
- 「**(x 時間 x 分 y 秒) ((x hour(s) x min(s) y sec(s)))**」 - レポートは実行をスケジュールされています。このメッセージは、レポートが次にいつ実行されるかを示すカウントダウン・タイマーです。

「**最新表示 (Refresh)**」アイコンを選択することで、「**次の実行時刻**」列の情報などの表示を最新にすることができます。

手順

1. 「**レポート**」タブをクリックします。
2. 生成するレポートを選択します。
3. 「**レポートの実行**」をクリックします。

次のタスク

レポートを生成した後、「生成済みレポート」列からレポートを表示できます。

レポートの複製

既存のレポートによく似たレポートを作成する場合は、モデルとなるレポートをコピーしてカスタマイズすることができます。

手順

1. 「**レポート**」タブをクリックします。
2. コピーするレポートを選択します。
3. 「**アクション**」リスト・ボックスから「**コピー (Duplicate)**」を選択します。
4. レポートに対し、スペースを含まない新しい名前を入力します。

次のタスク

複製したレポートをカスタマイズすることができます。

レポートの共有

レポートを他のユーザーと共有することができます。レポートを共有する場合は、他のユーザーが編集やスケジュールするために、選択したレポートのコピーを提供します。

このタスクについて

ユーザーが共有レポートを更新しても、元のバージョンのレポートには影響しません。

レポートを共有するには管理特権が必要になります。また、新規ユーザーがレポートを表示し、レポートにアクセスするためには、管理ユーザーが、この新規ユーザーと必要なすべてのレポートを共有する必要があります。

レポートは、適切なアクセス権を持つユーザーとのみ共有できます。

手順

1. 「**レポート**」タブをクリックします。
2. 共有するレポートを選択します。
3. 「**アクション**」リスト・ボックスで、「**共有 (Share)**」をクリックします。
4. ユーザーのリストから、このレポートを共有するユーザーを選択します。

レポートへの商標の設定

レポートに商標を設定するために、ロゴと特定の画像をインポートすることができます。カスタムのロゴを使用してレポートに商標を設定するには、レポート・ウィザードの使用を開始する前にそのロゴをアップロードして構成する必要があります。

始める前に

使用する図形は、必ず白の背景の 144 x 50 ピクセルにしてください。

ブラウザーで新しいロゴを確実に表示するように、ブラウザーのキャッシュをクリアしてください。

このタスクについて

複数のロゴをサポートしている場合、レポートに商標を設定することはお客様の企業にとって役立ちます。画像をアップロードすると、その画像は PNG (Portable Network Graphic) として自動的に保存されます。

新規画像をアップロードして、その画像をデフォルトとして設定した場合、そのデフォルトの新規画像は以前に生成されたレポートには適用されません。以前に生成されたレポート上のロゴを更新するには、新規コンテンツをそのレポートから手動で生成する必要があります。

レポート・ヘッダーでサポートできる長さよりも長い画像をアップロードした場合、その画像はヘッダーに収まるように自動的にサイズ変更されます。このサイズは高さが約 50 ピクセルです。

手順

1. 「**レポート**」タブをクリックします。
2. ナビゲーション・メニューで、「**商標 (Branding)**」をクリックします。
3. 「**参照**」をクリックして、システム上に配置されたファイルを参照します。
4. アップロードするロゴが含まれたファイルを選択します。「**オープン**」をクリックします。
5. 「**画像のアップロード (Upload Image)**」をクリックします。
6. デフォルトとして使用するロゴを選択して、「**デフォルトの画像を設定 (Set Default Image)**」をクリックします。

レポート・グループ

レポートを機能グループに分類することができます。レポートをグループに分類すると、レポートを効率良く編成および検出することができます。

例えば、Payment Card Industry Data Security Standard (PCIDSS) コンプライアンスに関連するすべてのレポートを表示することができます。

デフォルトでは、「**レポート**」タブにはすべてのレポートのリストが表示されますが、レポートを以下のように分類することができます。

- コンプライアンス
- エグゼクティブ
- ログ・ソース
- ネットワーク管理
- セキュリティー
- VoIP
- その他

新規レポートを作成する際に、そのレポートを既存のグループに割り当てたり、新規グループを作成したりできます。グループを作成、編集、または削除するためには、管理アクセス権限が必要です。

ユーザー・ロールの詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

レポート・グループの作成

新規グループを作成することができます。

手順

1. 「**レポート**」タブをクリックします。
2. 「**グループの管理**」をクリックします。
3. ナビゲーション・ツリーを使用して、新規グループをあるグループの下に作成するためにその上位のグループを選択します。
4. 「**新規グループ**」をクリックします。
5. 次の各パラメーターの値を入力します。
   - **名前** - 新規グループの名前を入力します。名前の長さは 255 文字までです。
   - 「**説明**」 - オプション。このグループの説明を入力します。説明の長さは 255 文字までです。
6. 「**OK**」をクリックします。
7. 新規グループの位置を変更するには、新規グループをクリックして、ナビゲーション・ツリーの新規の位置にそのフォルダーをドラッグします。
8. 「レポート・グループ (Report Groups)」ウィンドウを閉じます。

グループの編集

レポート・グループを編集して、名前や説明を変更することができます。

手順

1. 「**レポート**」タブをクリックします。
2. 「**グループの管理**」をクリックします。
3. ナビゲーション・ツリーから、編集するグループを選択します。
4. 「**編集**」をクリックします。
5. 必要に応じて、以下のパラメーターの値を更新します。
   - **名前** - 新規グループの名前を入力します。名前の長さは 255 文字までです。
   - 「**説明**」 - オプション。このグループの説明を入力します。説明の長さは 255 文字までです。このフィールドはオプションです。
6. 「**OK**」をクリックします。
7. 「レポート・グループ (Report Groups)」ウィンドウを閉じます。

レポート・グループの共有

レポート・グループを他のユーザーと共有することができます。

始める前に

レポート・グループを他のユーザーと共有するには、管理権限が必要です。

権限の詳細については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

コンテンツ・マネジメント・ツール (CMT) を使用してレポート・グループを共有することはできません。

CMT について詳しくは、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

このタスクについて

「レポート・グループ」ウィンドウのレポート・リストで、共有済みユーザーはレポート・グループを表示できます。

ユーザーが共有レポートを更新しても、元のバージョンのレポート・グループには影響しません。所有者のみが削除または変更できます。

ユーザーが共有レポートを複製または実行すると、レポートのコピーが作成されます。ユーザーは、コピーされたレポート・グループ内でレポートを編集またはスケジュールできます。

グループ共有オプションにより、グループ内のレポートに対して構成された前のレポート共有オプションはオーバーライドされます。

手順

1. 「**レポート**」タブをクリックします。
2. 「**レポート**」ウィンドウで、「**グループの管理**」をクリックします。

3. 「**レポート・グループ**」ウィンドウで、共有するレポート・グループを選択し、「**共有**」をクリックします。
4. 「**共有オプション**」ウィンドウで、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
デフォルト (親から継承)	レポート・グループは共有されません。 コピーされたレポート・グループまたは生成されたレポートは、ユーザー・レポート・リストに残ります。 構成済みの親レポートの共有オプションがある場合は、グループ内の各レポートに割り当てられます。
全員と共有	レポート・グループはすべてのユーザーと共有されます。
以下の基準に一致するユーザーと共有...	レポート・グループは特定のユーザーと共有されます。 **ユーザー・ロール** ユーザー・ロールのリストから選択し、追加アイコン (+) を押します。 **セキュリティー・プロファイル** セキュリティー・プロファイルのリストから選択し、追加アイコン (+) を押します。

5. 「**保存**」をクリックします。

タスクの結果

「レポート・グループ」ウィンドウのレポート・リストで、共有済みユーザーにはレポート・グループが表示されます。生成されたレポートでは、セキュリティー・プロファイル設定に基づきコンテンツが表示されます。

レポートのグループへの割り当て

「**グループの割り当て**」オプションを使用して、レポートを別のグループに割り当てることができます。

手順

1. 「**レポート**」タブをクリックします。
2. グループに割り当てるレポートを選択します。
3. 「**アクション**」リスト・ボックスから、「**グループの割り当て**」を選択します。
4. 「**項目グループ**」リストから、このレポートに割り当てるグループのチェック・ボックスを選択します。
5. 「**グループの割り当て**」をクリックします。

別のグループへのレポートのコピー

「**コピー**」アイコンを使用して、レポートを 1 つ以上のレポート・グループにコピーします。

手順

1. 「**レポート**」タブをクリックします。
2. 「**グループの管理**」をクリックします。
3. ナビゲーション・ツリーから、コピーするレポートを選択します。
4. 「**コピー**」をクリックします。
5. レポートのコピー先の 1 つ以上のグループを選択します。
6. 「**グループの割り当て**」をクリックします。
7. 「レポート・グループ (Report Groups)」ウィンドウを閉じます。

レポートの削除

グループからレポートを削除するには、「**削除**」アイコンを使用します。

このタスクについて

グループからレポートを削除しても、「**レポート**」タブにはそのレポートが表示されたままとなります。システムからそのレポートは削除されません。

手順

1. 「**レポート**」タブをクリックします。
2. 「**グループの管理**」をクリックします。
3. ナビゲーション・ツリーから、削除するレポートが含まれているフォルダーにナビゲートします。
4. グループのリストから、削除するレポートを選択します。
5. 「**削除**」をクリックします。
6. 「**OK**」をクリックします。
7. 「レポート・グループ (Report Groups)」ウィンドウを閉じます。

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。

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。

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。

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。

用語集

この用語集には、[製品名] のソフトウェアと製品で使用する用語と定義が記載されています。

この用語集では、以下の相互リファレンスを使用しています。

- 「*...を参照*」という表現は、非優先用語の場合は優先用語を参照し、略語の場合は正式な用語を参照するように促すための表現です。
- 「*...も参照*」という表現は、関連する用語や対比的な用語を参照するように促すための表現です。

その他の用語および定義については、IBM Terminology Web サイト (新しいウィンドウで開きます) を参照してください。

『A』 『B』 280 ページの『C』 280 ページの『D』 281 ページの『E』 281 ページの『F』 281 ページの『G』 281 ページの『H』 282 ページの『I』 282 ページの『K』 282 ページの『L』 283 ページの『M』 283 ページの『N』 283 ページの『O』 284 ページの『P』 284 ページの『Q』 284 ページの『R』 285 ページの『S』 286 ページの『T』 286 ページの『V』 286 ページの『W』

A

アキュムレーター (accumulator)
特定の演算の 1 つのオペランドを格納するためのレジスター。このオペランドは、その演算の結果によって置き換えられる。

アクティブ・システム (active system)
高可用性 (HA) クラスターにおいて、すべてのサービスが稼働しているシステム。

アドレス解決プロトコル (ARP) (Address Resolution Protocol (ARP))
ローカル・エリア・ネットワーク内で IP アドレスをネットワーク・アダプター・アドレスに動的にマップするプロトコル。

管理共有 (administrative share)
管理特権のないユーザーに非表示になっているネットワーク・リソース。管理共有により、管理者はネットワーク・システム上のすべてのリソースにアクセスできる。

アノマリ (anomaly)
予期されるネットワークの動作からの逸脱。

アプリケーション・シグニチャー (application signature)
パケット・ペイロードの検証によって取得された一連の固有の特性。特定のアプリケーションを識別するために使用される。

ARP 「アドレス解決プロトコル (Address Resolution Protocol)」を参照。

ARP リダイレクト (ARP Redirect)
ネットワーク上に問題が存在する場合に、その問題をホストに通知するための ARP 方式。

ASN 「自律システム番号 (autonomous system number)」を参照。

アセット (asset)
稼働環境にデプロイされているか、デプロイされる予定の管理可能オブジェクト。

自律システム番号 (ASN) (autonomous system number (ASN))
TCP/IP において、IP アドレスの割り当てを行う同じ中央認証局によって自律システムに割り当てられる番号。自律システム番号を自動ルーティング・アルゴリズムで使用すると、自律システムを識別することができる。

B

動作 (behavior)
特定の操作やイベントについて、その結果を含めた監視可能な影響。

結合インターフェース (bonded interface)
リンク集約 (link aggregation)を参照。

急増 (burst)
ライセンス交付を受けたフローやイベント

の速度制限を超えるような、着信イベントまたはフローの突然で急激な増加。

C

CIDR 「クラスレス・ドメイン間ルーティング (Classless Inter-Domain Routing)」を参照。

クラスレス・ドメイン間ルーティング (CIDR) (Classless Inter-Domain Routing (CIDR))
クラス C のインターネット・プロトコル (IP) アドレスを追加するための方式。このアドレスはインターネット・サービス・プロバイダー (ISP) に提供され、そのプロバイダーのユーザーによって使用される。CIDR アドレスによってルーティング・テーブルのサイズが削減されるため、組織内でより多くの IP アドレスを使用できるようになる。

クライアント (client)
サーバーからのサービスを要求するソフトウェア・プログラムまたはコンピューター。

クラスター仮想 IP アドレス (Cluster virtual IP address)
プライマリー・ホストまたはセカンダリー・ホストと HA クラスターとの間で共有される IP アドレス。

統合間隔 (coalescing interval)
イベントがバンドルされる間隔。イベントのバンドルは 10 秒間隔で実行され、現在のいずれの統合イベントにも一致しない最初のイベントから開始される。統合間隔の間に、一致する最初の 3 つのイベントがバンドルされ、イベント・プロセッサーに送信される。

共通脆弱性評価システム (CVSS) (Common Vulnerability Scoring System (CVSS))
脆弱性の重大度を測定するための評価システム

コンソール (console)
オペレーターがシステム操作の制御と監視を行うためのディスプレイ装置。

コンテンツ・キャプチャー (content capture)
構成可能なペイロード量を取得し、そのデータをフロー・ログに格納するプロセス。

資格情報 (credential)
ユーザーまたはプロセスに対して特定のアクセス権を付与する情報のセット。

信頼性 (credibility)
イベントやオフェンスの保全性を判別するために使用される 0 から 10 までの数値による評価。複数のソースが同じイベントまたはオフェンスを報告すると、信頼性が高くなる。

CVSS 「共通脆弱性評価システム (Common Vulnerability Scoring System)」を参照。

D

データベース・リーフ・オブジェクト (database leaf object)
データベース階層内の終端のオブジェクトまたはノード。

データ・ポイント (datapoint)
特定の時点におけるメトリックの計算値。

デバイス・サポート・モジュール (DSM) (Device Support Module (DSM))
複数のログ・ソースから受信したイベントを解析し、出力として表示可能な標準分類形式に変換する構成ファイル。

DHCP 「動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)」を参照。

DNS 「ドメイン・ネーム・システム (Domain Name System)」を参照。

ドメイン・ネーム・システム (DNS) (Domain Name System (DNS))
ドメイン名を IP アドレスにマップする分散データベース・システム。

DSM 「デバイス・サポート・モジュール (Device Support Module)」を参照。

重複フロー (duplicate flow)
異なる複数のフロー・ソースから受信した、同じデータ伝送の複数のインスタンス。

動的ホスト構成プロトコル (DHCP) (Dynamic Host Configuration Protocol (DHCP))
構成情報を一元的に管理するために使用される通信プロトコル。例えば DHCP は、

ネットワーク内のコンピューターに対して自動的に IP アドレスを割り当てる。

E

暗号化 (encryption)
コンピューター・セキュリティーにおいて、元のデータを取得できないように判読不能な形式にデータを変換するプロセス。暗号化解除プロセスを使用しない限り、元のデータを取得することはできない。

エンドポイント (endpoint)
環境内の API またはサービスのアドレス。API は、エンドポイントを公開し、同時に他のサービスのエンドポイントを呼び出す。

外部スキャン・アプライアンス (external scanning appliance)
ネットワーク内のアセットに関する脆弱性情報を収集するためにネットワークに接続されているマシン。

F

フォールス・ポジティブ (false positive)
ポジティブ (サイトが攻撃に対して脆弱であることを示す) として分類されるが、実際のユーザーの判断はネガティブ (脆弱ではない) となるテスト結果。

フロー (flow)
対話時にリンク経由で通過するデータの 1 回の伝送。

フロー・ログ (flow log)
フロー・レコードの集合。

フロー・ソース (flow sources)
フローの取得元。管理対象ホストにインストールされているハードウェアからフローが発生している場合、フロー・ソースは内部フローとして分類され、フローがフロー・コレクターに送信される場合は、外部フローとして分類される。

転送宛先 (forwarding destination)
正規化された生データをログ・ソースとフロー・ソースから受信する 1 つ以上のベンダー・システム。

FQDN 「完全修飾ドメイン名 (fully qualified domain name)」を参照。

FQNN 「完全修飾ネットワーク名 (fully qualified network name)」を参照。

完全修飾ドメイン名 (FQDN) (fully qualified domain name (FQDN))
インターネット通信において、ドメイン名のサブネームをすべて含むホスト・システム名。完全修飾ドメイン名の例としては、rchland.vnet.ibm.com などがある。

完全修飾ネットワーク名 (FQNN) (fully qualified network name (FQNN))
ネットワーク階層において、すべての部門を含むオブジェクトの名前。完全修飾ネットワーク名の例として、CompanyA.Department.Marketing などがある。

G

ゲートウェイ (gateway)
ネットワーク体系が異なるネットワークやシステムの接続に使用されるデバイスまたはプログラム。

H

HA 「高可用性 (high availability)」を参照。

HA クラスター (HA cluster)
1 台のプライマリー・サーバーと 1 台のセカンダリー・サーバーで構成される高可用性構成。

ハッシュ・ベース・メッセージ認証コード (HMAC) (Hash-Based Message Authentication Code (HMAC))
暗号ハッシュ機能と秘密鍵を使用する暗号コード。

高可用性 (HA) (high availability (HA))
特定のノードまたはデーモンで障害が発生した場合に、ワークロードをクラスター内の他のノードに再配分できるように再構成されるクラスター化システムに関連する構成。

HMAC
「ハッシュ・ベース・メッセージ認証コード (Hash-Based Message Authentication Code)」を参照。

ホスト・コンテキスト (host context)
コンポーネントをモニターし、各コンポーネントが正常に機能していることを確認するサービス。

I

ICMP 「Internet Control Message Protocol」を参照。

ID (identity)
人、組織、場所、項目を表す、データ・ソースの属性の集合。

IDS 「侵入検知システム (intrusion detection system)」を参照。

Internet Control Message Protocol (ICMP)
データグラムのエラーを報告するなどの目的で送信元ホストと通信する際に、ゲートウェイが使用するインターネット・プロトコル。

インターネット・プロトコル (IP) (Internet Protocol (IP))
ネットワークまたは相互接続ネットワーク経由でデータを送信するプロトコル。このプロトコルは、上位のプロトコル層と物理ネットワークとの間の中継役として機能する。「伝送制御プロトコル (Transmission Control Protocol)」も参照。

インターネット・サービス・プロバイダー (ISP) (Internet Service Provider (ISP))
インターネットへのアクセスを提供する組織。

侵入検知システム (IDS) (intrusion detection system (IDS))
ネットワークやホスト・システムの一部であるモニター対象リソース上での侵入の試みや実際の侵入を検出するソフトウェア。

侵入防止システム (IPS) (intrusion prevention system (IPS))
潜在的な悪意を持つアクティビティーを拒否するシステム。拒否の手段としては、フィルター処理、トラッキング、速度制限の設定などがある。

IP 「インターネット・プロトコル (Internet Protocol)」を参照。

IP マルチキャスト (IP multicast)
単一のマルチキャスト・グループを構成する一連のシステムに対するインターネット・プロトコル (IP) データグラムの伝送。

IPS 「侵入防止システム (intrusion prevention system)」を参照。

ISP 「インターネット・サービス・プロバイダー (Internet service provider)」を参照。

K

鍵ファイル (key file)
コンピューター・セキュリティーにおいて、公開鍵、秘密鍵、トラステッド・ルート、および証明書を含むファイル。

L

L2L 「ローカルからローカル」を参照。

L2R 「ローカルからリモート」を参照。

LAN ローカル・エリア・ネットワーク (Local Area Network) を参照してください。

LDAP 「Lightweight Directory Access Protocol」を参照。

リーフ (leaf)
ツリーにおいて、子を持たないエントリーまたはノード。

Lightweight Directory Access Protocol (LDAP)
TCP/IP を使用して、X.500 モデルをサポートするディレクトリーへのアクセスを提供し、より複雑な X.500 Directory Access Protocol (DAP) のリソース要件には制約されないオープン・プロトコル。例えば、LDAP を使用して、インターネット・ディレクトリーまたはイントラネット・ディレクトリーで個人や組織などのリソースを検索することができる。

リンク集約 (link aggregation)
ケーブルやポートなどの物理ネットワーク・インターフェース・カードの、単一の論理ネットワーク・インターフェースへのグループ化。リンク集約は、帯域幅およびネットワーク可用性を増大させるために使用される。

ライブ・スキャン (live scan)
セッション名に基づいてスキャン結果からレポート・データを生成する脆弱性スキャン。

ローカル・エリア・ネットワーク (LAN) (local area network (LAN))
限定された領域内 (単一のビルやキャンパスなど) の複数のデバイスを接続するネットワーク。このネットワークを、さらに大きなネットワークに接続することができる。

ローカルからローカル (L2L) (Local To Local (L2L))
あるローカル・ネットワークから別のローカル・ネットワークへの内部トラフィックに関連する構成。

ローカルからリモート (L2R) (Local To Remote (L2R))
あるローカル・ネットワークから別のローカル・ネットワークへの内部トラフィックに関連する構成。

ログ・ソース (log source)
イベント・ログの発生元となるセキュリティー装置またはネットワーク装置。

ログ・ソース拡張 (log source extension)
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。

M

判定機能 (magistrate)
定義されているカスタム規則に対してネットワーク・トラフィックとセキュリティー・イベントを分析する内部コンポーネント。

マグニチュード (magnitude)
特定のオフェンスの相対的な重要性の尺度。マグニチュードは、関連性、重大度、信頼性から算出された重みを持つ値である。

N

NAT
ネットワーク・アドレス変換 (network address translation) を参照。

NetFlow
ネットワーク・トラフィックのフロー・データをモニターする Cisco ネットワーク・プロトコル。 NetFlow データには、クライアントとサーバーの情報、使用されるポート、ネットワークに接続されているスイッチとルーターを通過するバイト数とパケット数が含まれている。このデータは NetFlow コレクターに送信され、NetFlow コレクターがデータの分析を行う。

ネットワーク・アドレス変換 (NAT) (network address translation (NAT))
ファイアウォールにおいて、セキュアなインターネット・プロトコル (IP) アドレスを外部の登録済みアドレスに変換すること。これにより、外部ネットワークとの通信が可能になり、ファイアウォール内部で使用される IP アドレスはマスクされる。

ネットワーク階層 (network hierarchy)
ネットワーク・オブジェクトの階層コレクションであるコンテナーの一種。

ネットワーク層 (network layer)
OSI アーキテクチャーにおいて、予測可能なサービス品質を持つ複数のオープン・システム間でパスを確立するためのサービスを提供する層。

ネットワーク・オブジェクト (network object)
ネットワーク階層の構成要素。

O

オフェンス (offense)
モニターされる条件への応答として送信されたメッセージまたは生成されたイベント。例えば、オフェンスは、ポリシー違反があったかどうか、ネットワークが攻撃されているかどうかなどの情報を提供する。

オフサイト・ソース (offsite source)
正規化されたデータをイベント・コレクターに転送する、プライマリー・サイトから離れた場所に存在するデバイス。

オフサイト・ターゲット (offsite target)
イベント・コレクターからイベント・フローまたはデータ・フローを受信する、プライマリー・サイトから離れた場所に存在するデバイス。正規化されたデータをイベント・コレクターから受信する、プライマリー・サイトから離れているデバイス。

オープン・ソース脆弱性データベース (OSVDB) (Open Source Vulnerability Database (OSVDB))
ネットワーク・セキュリティー・コミュニティーがネットワーク・セキュリティー・コミュニティーのために作成した、ネットワーク・セキュリティーの脆弱性に関する技術情報を提供するオープン・ソース・データベース。

オープン・システム間相互接続 (OSI) (open systems interconnection (OSI))
国際標準化機構 (ISO) の標準に準拠した、情報交換のためのオープン・システムの相互接続。

OSI 「オープン・システム間相互接続 (OSI) (open systems interconnection)」を参照。

OSVDB
「オープン・ソース脆弱性データベース (Open Source Vulnerability Database)」を参照。

P

解析順序 (parsing order)
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、ユーザーが重要度の順序を定義できるログ・ソース定義。

ペイロード・データ (payload data)
IP フローに含まれるアプリケーション・データ。ただし、ヘッダーと管理情報は除く。

プライマリー HA ホスト (primary HA host)
HA クラスターに接続されるメイン・コンピューター。

プロトコル (protocol)
通信ネットワーク内の複数のデバイス間またはシステム間におけるデータの通信と転送を制御する一連のルール。

Q

QID マップ (QID Map)
それぞれの固有イベントを特定し、そのイベントを下位カテゴリーと上位カテゴリーにマップして、イベントの相関方法と編成方法を決定する分類法。

R

R2L 「リモートからローカル」を参照。

R2R 「リモートからリモート」を参照。

recon 「スキャン行為 (reconnaissance)」を参照。

スキャン行為 (reconnaissance (recon))
ネットワーク・リソースの ID に関連する情報を収集する方式。ネットワーク・スキャンやその他の技法を使用してネットワーク・リソース・イベントのリストがコンパイルされ、それらに重大度レベルが割り当てられる。

リファレンス・マップ (reference map)
キーから値 (例: ユーザー名からグローバル ID) への直接マッピングのデータ・レコード。

マップのリファレンス・マップ (reference map of maps) 2 つのキーが多くの値にマップされるデータ・レコード。例えば、アプリケーションの合計バイト数から送信元 IP へのマッピング。

セットのリファレンス・マップ (reference map of sets) 1 つのキーが多くの値にマップされるデータ・レコード。例えば、特権ユーザーのリストからホストへのマッピング。

リファレンス・セット (reference set)
ネットワーク上のイベントまたはフローから派生した単一のエレメントのリスト。例 : IP アドレスのリストやユーザー名のリスト。

リファレンス・テーブル (reference table)
データ・レコードが、割り当てられているタイプを持つキーを他のキーにマップし、次に単一の値にマップするテーブル。

最新表示タイマー (refresh timer)
一定の間隔で、手動または自動でトリガーされる内部デバイス。このデバイスにより、現在のネットワーク・アクティビティー・データが更新される。

関連性 (relevance)
ネットワーク上のイベント、カテゴリー、オフェンスの相対的な影響の尺度。

リモートからローカル (R2L) (Remote To Local (R2L))
リモート・ネットワークからローカル・ネットワークへの外部トラフィック。

リモートからリモート (R2R) (Remote To Remote (R2R))
リモート・ネットワークから別のリモート・ネットワークへの外部トラフィック。

レポート (report)
照会管理において、照会の実行結果にフォームを適用したフォーマット済みデータ。

レポート間隔 (report interval)
構成可能な時間間隔。この間隔の最後に、イベント・プロセッサーは、取得したすべてのイベント・データとフロー・データをコンソールに送信する。

ルーティング・ルール (routing rule)
イベント・データによって基準が満たされた場合に、条件の集合とその結果として発生するルーティングが実行される条件。

ルール (rule)
コンピューター・システムが関係を識別し、それに応じて、自動化された応答を実行できるようにする一連の条件ステートメント。

S

スキャナー (scanner)
Web アプリケーション内でソフトウェアの脆弱性を検索する、自動化されたセキュリティー・プログラム。

セカンダリー HA ホスト (secondary HA host)
HA クラスターに接続されるスタンバイ・コンピューター。プライマリー HA ホストで障害が発生した場合は、セカンダリー HA ホストがプライマリー HA ホストの処理を引き継ぐ。

重大度 (severity)
ソースが宛先に及ぼす相対的な脅威の尺度。

Simple Network Management Protocol (SNMP)
複雑なネットワーク内のシステムとデバイスをモニターするための一連のプロトコル。管理対象デバイスに関する情報は、管理情報ベース (MIB) で定義されて保管される。

SNMP 「Simple Network Management Protocol」を参照。

SOAP 非集中型の分散環境で情報を交換するための XML ベースの軽量プロトコル。SOAP を使用して、インターネット経由で情報を照会して情報を返し、サービスを呼び出すことができる。

スタンバイ・システム (standby system)
アクティブなシステムで障害が発生した場合に、自動的にアクティブになるシステム。ディスクの複製が有効になっている場合、スタンバイ・システムはアクティブなシステムからデータを複製する。

サブネット (subnet)
「サブネットワーク (subnetwork)」を参照。

サブネット・マスク (subnet mask)
インターネット・サブネットワークで、IP アドレスのホスト部分のサブネットワーク・アドレス・ビットの識別に使用される 32 ビットのマスク。

サブネットワーク (サブネット) (subnetwork (subnet))
相互に接続された、より小さな独立したサブグループに分割されているネットワーク。

サブ検索 (sub-search)
完了した検索結果セット内での検索照会の実行を可能にする機能。

スーパーフロー (superflow)
ストレージの制約を削減することによって

処理能力を向上させるために、類似するプロパティーを持つ複数のフローから構成される単一のフロー。

システム・ビュー (system view)
システムを構成するプライマリー・ホストと管理対象ホストの視覚的な表現。

T

TCP 「伝送制御プロトコル (Transmission Control Protocol)」を参照。

伝送制御プロトコル (TCP) (Transmission Control Protocol (TCP))
インターネットで使用される通信プロトコル。また、インターネットワーク・プロトコル用の Internet Engineering Task Force (IETF) 標準に準拠するネットワークでも使用される。TCP は、パケット交換通信ネットワークと、パケット交換通信ネットワークの相互接続システムにおいて、信頼できるホスト間プロトコルを提供する。「インターネット・プロトコル (Internet Protocol)」も参照。

トラストストア・ファイル (truststore file)
トラステッド・エンティティーの公開鍵が入っている鍵データベース・ファイル。

V

違反 (violation)
企業のポリシーをバイパスする行為、または企業のポリシーに違反する行為。

脆弱性 (vulnerability)
オペレーティング・システム、システム・ソフトウェア、またはアプリケーション・ソフトウェア・コンポーネントでの機密漏れ。

W

WHOIS サーバー (whois server)
ドメイン名や IP アドレスの割り振りなど、登録されているインターネット・リソースに関する情報の取得に使用されるサーバー。

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]

アクション 45
アセット 11, 20, 21
アセット検索 (asset search) ページ 150
アセット検索グループ 152
アセット検索条件を保存する 152
アセットのエクスポート 156
アセットの検索 138
アセットの削除 155
アセットの脆弱性 157
アセットの調査 138
アセットの追加 138
アセットの表示 138
アセット名 139
アセットをインポートする 155
アセットを追加する 145
アセットを編集する 145
アセット・タブ 11, 138, 139, 141, 143, 145, 152, 153, 154, 155
アセット・プロファイル 137, 143, 145, 152, 153, 154, 155, 156
アセット・プロファイルの印刷 138
アセット・プロファイルのインポート 155
アセット・プロファイルのエクスポート 155
アセット・プロファイルの検索 150
アセット・プロファイルの削除 155
アセット・プロファイルを表示する 143
アセット・プロファイル・ページ 139, 157
アセット・プロファイル・ページのパラメーター 137
宛先 IP アドレス 40
宛先 IP 別 ページ 192
宛先 IP 別のオフェンス 43
アノマリ検出ルール 213, 220
アノマリ検出ルール (Anomaly Detection Rule) ウィザード 220
アプライアンス 11
アプリケーション 21
一括ロード
  イベントおよびフローの分析 243
  ヒストリカル相関 243
イベント 25, 99, 164, 167
イベント検索グループ 199, 200
イベント項目の追加 37
イベントとフローの検索 167
イベントとフローの検索条件の保存 83
イベントに関連付けられているオフェンスの表示 99
イベントのエクスポート 104
イベントの詳細 97
イベントの詳細 (Event details) ツールバー 97
イベントの詳細 (Event details) ツールバーの機能 97
イベントの詳細 (Event Details) ページ 93
イベントの説明 93
イベントの調査 24, 39
イベントのマッピング 99
イベントのマッピングの変更 99
イベントのモニター 24
イベントのリスト 93
イベント・フィルターの情報 141
イベント・プロセッサー 109
イベント・プロセッサーの結果 82
イベント・ルール 214
イベント・ログの調査 10
インターネット脅威インフォメーション・センター 31
インターネット脅威レベル 31
オーバーフロー・レコード 109
オフェンス 21, 39, 40, 44, 48, 99, 167, 199, 201, 213
  ヒストリカル相関 246
  ユーザーへの割り当て 49
オフェンス検索グループ 200
オフェンス項目 23
オフェンスに関するアクション 45
オフェンスに関する権限 39
オフェンスの 保存 47
オフェンスのエクスポート 49
オフェンスの管理 39
オフェンスのクローズ 46
オフェンスの検索 39, 183, 190, 192, 194
オフェンスのサマリー 50
オフェンスの調査 10
オフェンスのパラメーター 56
オフェンスの非表示 46
オフェンスの保護 47
オフェンスの保護解除 48
オフェンスのモニター 41, 43, 45
オフェンス・ダッシュボード項目 23
オフェンス・タブ 10, 14, 39, 45, 46, 47, 49, 51, 52, 56, 190, 192, 194, 195
オフェンス・ルール 214
オンライン・ヘルプ 19

[カ行]

開始時刻 243
解析されていないイベント・データ 87
概要 ix
  RESTful API 8
各種モードでのフローのリスト 118
過去 1 分間 (自動最新表示) 15
過去 24 時間のアクティビティーのサマリー 25
カスタムのダッシュボード項目 22
カスタム・イベント・プロパティーとカスタム・フロー・プロパティー 203
カスタム・ダッシュボード 21, 26, 31
カスタム・プロパティー 211
カスタム・ルール 213
カスタム・ルールの作成 218
カスタム・ルールの表示 213
カスタム・ルールの保守 213
カスタム・ルール・ウィザード 12, 30
カスタム・レポート 263
画像
  アップロード 270
  レポート
    商標の設定 270
カテゴリー別のオフェンス 42
関数 215
管理タブ 12, 40
基準の保存 195
基準を保存する 152
脅威 21
共通ルール 214
クイック・フィルター 167
グラフの概要 161
グラフの管理 161
グラフの構成 164
グラフの凡例 163
グラフ・オブジェクト 163
グラフ・タイプ 258, 261
グラフ・タイプの指定 33
グループ
  項目のコピー 226
  項目の削除 226
  項目の割り当て 225
  削除 202, 227
  編集 225

グループ化されたイベントのオプション 89
グループ化されたイベントのパラメーター 89
グループ化されたイベントを表示する 89
グループ化されたフローの表示 115
グループからの保存済み検索の削除 202
グループの管理 154
グループの削除 202
グループの編集 225, 272
グループへの項目のコピー 226
グループを削除する 154
計算プロパティー 206
計算プロパティー・タイプ 203
権限
カスタム・プロパティー 203
現在の脅威レベル 31
検索 154, 167
グループへのコピー 201
検索グループ
管理 199
作成 200
表示 199
編集 201
検索グループ (Search Groups) ウィンドウ 199
検索グループの管理 195, 199
検索グループの作成 199
検索グループの表示 152, 199
検索グループの編集 201
検索グループを編集する 154
検索結果
管理 198
キャンセル 198
削除 199
検索結果の数 109
検索結果の管理 198, 199
検索結果の削除 199
検索条件
削除 196
使用可能な保存済み 196
保存 173
ログ・アクティビティー・タブ 196
検索条件の保存 195
検索のキャンセル 198
更新されたオフェンス 25
構成データ 11
項目のグループへの割り当て 225
項目の追加 22, 37
項目の表示 29
誤検出 137
コンソールの時刻 18
コントロール 12
コンプライアンス 21

[サ行]

サード・パーティーのスキャナー 138
サーバー 11
サービス 139
サービス・ペイン 137
最近生成されたレポート 25
削除アイコン 154
サブ検索の実行 197
サポート対象のバージョン
Web ブラウザー 7
時系列グラフ 162
システム 21
システム時刻 18
システム通知 12, 36
システム通知 ダッシュボード項目 30
システム通知の表示 36
システムの構成と管理 12
システム・サマリー・ダッシュボード項目 25
自分のオフェンス (my offenses) タブ 183
自分のオフェンス・ページ 41
重要な用語 40
除外オプション 48
新規ウィンドウで表示 35
新規検索 (new search) 154
新規検索グループの作成 200
新規検索グループを作成する 153
新規ダッシュボード 31
新機能
ユーザー・ガイドの概要 1
スケジュール済み検索
イベント 174
検索 174
保存済み検索 174
ステータス・バー 82, 109
ストリーミング・イベント 83
ストリーミング・イベントの表示 83
ストリーミング・フローの表示 110
ストリーム・モード 110
すべてのオフェンス (all offenses) タブ 183
すべてのオフェンス・ページ 41
正規化イベント 84
正規化フロー 110, 111
正規表現プロパティー 204
脆弱性 138, 139
脆弱性管理 (Vulnerability Management) ダッシュボード 29
脆弱性の詳細 157
脆弱性ペイン 137
製品ペイン 137
セキュリティー 21
セキュリティー証明書 5
セキュリティー例外 5
接続検索項目 26
接続の構成 33
総計 CVSS スコア 139
送信元 IP アドレス 40
送信元 IP によるオフェンスのグループ化 43
送信元 IP ページ 190

[タ行]

ダッシュボード 37
ダッシュボードからの項目の削除 35
ダッシュボード項目 36
ダッシュボード項目の切り離し 35
ダッシュボード項目の構成 33
ダッシュボード項目の追加 21
ダッシュボード項目の編成 21
ダッシュボードのカスタマイズ 22
ダッシュボードの管理 21
ダッシュボードの削除 36
ダッシュボードの名前変更 35
ダッシュボードの表示 22, 31, 35, 36
ダッシュボード・タグ 23
ダッシュボード・タブ 9, 10, 12, 21, 22, 24, 26, 31, 32, 35, 36
タブ 9
単一のイベントの詳細 93
調査 105
ツールバー 77
ツールバーの機能 52
通知メッセージ 30
データの一時停止 15
データの検索 167
データの最新表示 15
データの再生 15
テスト 215
デバイス時刻 243
デバイス・レベルの権限 39
デフォルトのログイン情報 7
デフォルト・タブ 10
ドキュメント・モード
Internet Explorer Web ブラウザー 7

[ナ行]

ナビゲーション・メニュー 40
ネットワーク 21, 44
ネットワーク、プラグイン、コンポーネントの構成と管理 12
ネットワーク管理者 ix
ネットワークの管理 138
ネットワークのモニター 105
ネットワーク別 ページ 194
ネットワーク別のオフェンス 44

ネットワーク・アクティビティー 15, 20, 21, 22, 32, 37, 105, 110, 111, 161, 162, 164, 167, 173, 196, 197, 198, 199, 201, 203, 213
ネットワーク・アクティビティーの構成 33
ネットワーク・アクティビティーの調査 105
ネットワーク・アクティビティーのモニター 110
ネットワーク・アクティビティー・タブ 10, 14, 105, 108, 109, 110, 115, 123, 124, 167
ネットワーク・アクティビティー・タブ・ツールバー 105
ネットワーク・インターフェース・ペイン 137

[ハ行]

パケット・キャプチャー (PCAP) データ 101
パスワード 7
パッケージ・ペイン 137
ヒストリカル相関
  オフェンス 246
  開始時刻 243
  過去の実行に関する情報 246
  デバイス時刻 243
  プロファイルの作成 245
  ルールの処理 243
非表示のオフェンス 46
表 21
表示 リスト・ボックス 115
表示 (display) リスト・ボックス 89
表示するデータ・オブジェクトの数の指定 33
表内の結果のソート 14
ビルディング・ブロック 215
  編集 227
ビルディング・ブロックの編集 227
フィルターの追加 197
フォールス・ポジティブ 100, 123
フォールス・ポジティブのチューニング 100, 123
フォローアップするオフェンスのマーク付け 51
複数のダッシュボード 21
ブラウザー・モード
  Internet Explorer Web ブラウザー 7
フラグ (Flag) 30
フロー 25, 105, 164, 167, 174
フロー検索 22
フロー検索グループ 199, 200
フロー検索項目の追加 37
フローのエクスポート 124
フローの詳細 111, 118
フローの詳細 (Flow Details) ツールバー 122
フローのストリーミング 109
フローの調査 10, 39
フロー・グループ 118
フロー・フィルター基準 108
フロー・ルール 214
プロパティー
  カスタムのコピー 210
  カスタムの変更 208
プロパティー (properties) ペイン 137
プロパティー・タイプ 203
ページ・サイズの構成 21
ヘルプ 19
ヘルプの目次 19
ホスト 11
保存済み検索条件 22
保存済み検索のコピー 201
保存済み検索をコピーする 154
保存済み検索を削除する 154

[マ行]

右クリック・メニュー 82, 108
右クリック・メニューのオプション 141
メッセージを表示する 12
メッセージ・メニュー 12
メモの追加 45
モニター 105

[ヤ行]

ユーザー詳細を更新する 18
ユーザー情報 18
ユーザーの構成と管理 12
ユーザー名 7, 17
ユーザー・インターフェース 9
ユーザー・インターフェースの各タブ 9, 12
用語集 279

[ラ行]

ライセンス・キー 5
リアルタイム 83
リアルタイム (ストリーミング) 15
リスク (Risks) タブ 26
リスク管理
  ポリシー・コンプライアンスのモニター 26
  リスクの変化のモニター 28
「リスクのモニター」ダッシュボード 26
  作成 26
リスク・ポリシー・ペイン 137
リスク・マネージャー・ダッシュボード
  作成 28
ルール 213, 215
  応答 215
  コピー 223
  表示 217
  編集 223
  無効化 222
  有効化 222
  X-Force Exchange 250, 251, 254
ルールの応答 231
ルールの管理 213, 222
ルールの権限 213
ルールのコピー 223
ルールの削除 224
ルールの無効化 222
ルールの有効化 222
ルール・グループ
  作成 225
  表示 224
ルール・グループの管理 224
ルール・グループの作成 225
ルール・グループを表示する 224
ルール・テスト 243
ルール・パラメーター 227
ルール・ページ・ツールバー 229
列のサイズ変更 20
レポート 20, 21
  ヒストリカル相関 246
  表示 267
  編集 267
レポート (reports) タブ 14
レポートの管理 11, 259
レポートの共有 269
レポートのコピー 269
レポートの作成 11
レポートの配布 11
レポートのレイアウト 258
レポートを手動で生成 268
レポート・グループ 272
レポート・グループの共有 272
レポート・タブ 11, 259
ロー・イベント・データ 87
ログイン情報 7
ログ・アクティビティー 15, 20, 21, 32, 37, 77, 99, 100, 161, 162, 164, 167, 197, 198, 199, 201, 203, 213
  概要 77
  検索条件 173
ログ・アクティビティーの構成 33
ログ・アクティビティーの調査 77
ログ・アクティビティー・ダッシュボード項目 24
ログ・アクティビティー・タブ 10, 14, 77, 82, 83, 84, 87, 89, 99, 101, 104, 167
ログ・ソース 87

C

CSV にエクスポート 124

E

E メール通知 50

I

IBM Security QRadar Risk Manager 11
ID 139
IP アドレス 16, 139

P

PCAP データ 101, 102
PCAP データ 列 101, 103
PCAP データを表示する 102
PCAP データ・ファイルをダウンロードする 102
PCAP ファイルのダウンロード 103

Q

QFlow コレクター 109
QID 99
QRadar
  X-Force Threat Intelligence フィードの統合 249
QRadar SIEM をナビゲートする 5
QRadar Vulnerability Manager 138

R

Regex プロパティー・タイプ 203
RESTful API
  概要 8

W

Windows パッチ・ペイン 137

X

XML にエクスポート 124
X-Force Exchange
  ルール 250, 251, 254
X-Force Threat Intelligence フィード
  例 250, 252
  QRadar との併用 249

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