IBM Security QRadar Risk Manager

バージョン 7.3

スタートアップ・ガイド

注記

本書および本書で紹介する製品をご使用になる前に、 27 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 V7.3.0 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 Risk Manager
Version 7.3
Getting Started Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

IBM Security QRadar Risk Manager の概要

この情報は、IBM® QRadar® Risk Manager で利用されることを目的としています。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ション、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に使用するアプライアンスです。

対象読者

本書は、ネットワーク内に QRadar Risk Manager システムのインストールおよび構成を行うネットワーク管理者を対象としています。

技術資料

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

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

お客様サポートへのお問い合わせ

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

適切なセキュリティーの実践に関する注意事項

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

注意:

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 IBM Security QRadar Risk Manager の概要

IBM Security QRadar Risk Manager は別個にインストールされるアプライアンスです。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ション、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に使用します。

QRadar Risk Manager には IBM Security QRadar SIEM Console の「リスク」タブからアクセスします。

QRadar Risk Manager は、以下の作業を実行するためのツールを管理者に提供することで QRadar SIEM を拡張します。

- リスクを集中管理する。
- トポロジーを使用してネットワークを表示する。
- ネットワーク・デバイスを構成してモニターする。
- ネットワーク・デバイス間の接続を表示する。
- ファイアウォール・ルールを検索する。
- 既存のルールと、トリガーされたルールのイベント・カウントを表示する。
- デバイスと、ネットワーク・デバイスのパスを検索する。
- ネットワークをモニターして監査し、コンプライアンスを確保する。
- ネットワークでのエクスプロイト・シミュレーションを定義し、スケジュールして実行する。
- 脆弱性を検索する。

増大する情報インテリジェンスに対するリスクの集中管理やコンプライアンスの確保には、多くの社内チームの協力が不可欠だといえます。次世代の SIEM では、追加のリスク管理アプライアンスを組み込み、第 1 世代の SIEM 製品で必要であった手順の数を削減しています。QRadar SIEM で管理するアセットのネットワーク・トポロジーおよびリスク評価を利用できます。

評価処理では、システム、セキュリティー、リスク分析、およびネットワーク情報が集計と相関を通じて統合され、ご使用のネットワーク環境が完全に可視化されます。また、ご使用の環境に対するポータルを定義することで、手動処理やその他の領域別製品テクノロジーでは実現できない可視性や効率が得られます。

第 2 章 IBM Security QRadar Risk Manager のデプロイ

QRadar Risk Manager アプライアンスは、最新バージョンの QRadar Risk Manager ソフトウェアとともにインストールされます。

QRadar Risk Manager 評価アプライアンスをインストールする必要があります。このソフトウェアをアクティブ化して、IP アドレスを QRadar Risk Manager アプライアンスに割り当てる必要があります。

アプライアンスはネットワーク・デバイスからの情報を受け入れる準備ができています。

QRadar Risk Manager の使用方法について詳しくは「*IBM Security QRadar Risk Manager* ユーザー・ガイド」を参照してください。

ご使用の環境に QRadar Risk Manager をデプロイするには、以下の作業が必要です。

1. 最新バージョンの IBM Security QRadar SIEM がインストールされていることを確認する。
2. インストール前の要件をすべて満たしていることを確認する。
3. QRadar Risk Manager アプライアンスをセットアップして電源を入れる。
4. QRadar Risk Manager プラグインを IBM Security QRadar SIEM Console にインストールする。
5. QRadar SIEM と QRadar Risk Manager アプライアンスの間の通信を確立する。
6. QRadar Risk Manager ユーザーのユーザー・ロールを定義する。

インストールの前に

IBM Security QRadar Risk Manager をインストールする前に、IBM Security QRadar SIEM Consoleのインストール・プロセスを完了する必要があります。ベスト・プラクティスとしては、QRadar SIEM および QRadar Risk Manager を同じネットワーク・スイッチにインストールしてください。

QRadar Risk Manager 評価アプライアンスをインストールする前に、以下を確認してください。

- 2 ユニット・アプライアンス用のスペース
- ラック・レールおよびシェルフが取り付けられていること。

オプションで、USB キーボードおよび標準 VGA モニターを使用して QRadar SIEM Console にアクセスできます。

ファイアウォールのポート・アクセスの構成

IBM Security QRadar SIEM Consoleと IBM Security QRadar Risk Manager の間にあるファイアウォールは、特定のポートでのトラフィックを許可する必要があります。

QRadar SIEM Consoleと QRadar Risk Manager の間にあるファイアウォールでは以下のポートでのトラフィックを許可するようにしてください。

- ポート 443 (HTTPS)
- ポート 22 (SSH)
- ポート 37 UDP (Time)

ネットワーク設定の識別

ネットワーク設定に関する情報を収集してからインストール・プロセスを開始する必要があります。

ネットワーク設定について以下の情報を収集します。

- ホスト名
- IP アドレス
- ネットワーク・マスク・アドレス
- サブネット・マスク
- デフォルトのゲートウェイ・アドレス
- プライマリー・ドメイン・ネーム・システム (DNS) サーバーのアドレス
- セカンダリー DNS サーバー (オプション) のアドレス
- ネットワーク・アドレス変換 (NAT) の E メール・サーバー名を使用するネットワークのパブリック IP アドレス
- E メール・サーバー名
- Network Time Protocol (NTP) サーバー (コンソールのみ) 名またはタイム・サーバー名

IBM Security QRadar Risk Manager でサポートされない機能

QRadar Risk Manager でサポートされない機能を把握しておくことは重要です。

以下の機能は QRadar Risk Manager でサポートされていません。

- 高可用性 (HA)
- ボーダー・ゲートウェイ・プロトコル (BGP) の動的ルーティング
- IPv6
- 不連続なネットワーク・マスク
- ロード・バランスされる経路

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 *1. QRadar* 製品でサポートされる *Web* ブラウザー

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

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 Risk Manager ユーザー・インターフェースへのアクセス

IBM Security QRadar Risk Manager 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。

QRadar Risk Manager には IBM Security QRadar SIEM Console からアクセスします。 QRadar Console 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 2. *QRadar Risk Manager* 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 Console の IP アドレスです)。
ユーザー名	admin
パスワード	インストール・プロセスで QRadar Risk Manager 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。

IBM Security QRadar Risk Manager アプライアンスのセットアップ

管理インターフェースを接続し、確実に電源接続を IBM Security QRadar Risk Manager アプライアンスに接続する必要があります。

始める前に

前提条件に目を通して把握し、情報を収集します。

このタスクについて

QRadar Risk Manager 評価アプライアンスは、2 ユニットのラック・マウント・サーバーです。評価機器には、ラック・レールおよびシェルフは付属していません。

QRadar Risk Manager アプライアンスには、4 つのネットワーク・インターフェースが組み込まれています。この評価では、ETH0 というラベルが付いたネットワーク・インターフェースを管理インターフェースとして使用します。他のインターフェースはモニター・インターフェースです。インターフェースは、いずれも QRadar Risk Manager アプライアンスの背面パネルにあります。

電源ボタンはフロント・パネルにあります。

手順

1. 管理ネットワーク・インターフェースを、ETH0 というラベルが付いたポートに接続します。
2. 専用の電源接続をアプライアンスの背面に確実に接続します。
3. オプション。IBM Security QRadar SIEM Console にアクセスするために、USB キーボードおよび標準 VGA モニターを接続します。
4. アプライアンスにフロント・ペインがある場合、両側のつまみを押してペインを取り外し、アプライアンスからペインを引き出します。
5. フロント側の電源ボタンを押して、アプライアンスの電源を入れます。

タスクの結果

アプライアンスがブート処理を開始します。

IBM Security QRadar SIEM Consoleへの IBM Security QRadar Risk Manager の追加

IBM Security QRadar Risk Manager を管理対象ホストとして IBM Security QRadar SIEM Consoleに追加する必要があります。

始める前に

圧縮を有効にする場合、各管理対象ホストの最小バージョンを QRadar Console V7.1 または QRadar Risk Manager V7.1 にする必要があります。

コンソールが NAT されているデプロイメント環境に、NAT されていない管理対象ホストを追加するには、QRadar Console を NAT されたホストに変更する必要があります。コンソールを変更してから管理対象ホストをデプロイメントに追加してください。詳細については、*IBM Security QRadar* 管理ガイド を参照してください。

手順

1. Web ブラウザーを開きます。
2. URL `https://<IP Address>` を入力します。ここで、*<IP Address>* は QRadar Consoleの IP アドレスです。
3. ユーザー名とパスワードを入力します。
4. 「管理」タブをクリックします。
5. 「システム構成」ペインで、「システムおよびライセンス管理」をクリックします。
6. 「システムおよびライセンス管理」ウィンドウで、「デプロイメント・アクション」をクリックしてから、「ホストの追加」を選択します。
7. 次の各パラメーターの値を入力します。

オプション	説明
ホスト **IP**	QRadar Risk Manager の IP アドレス。
ホスト・パスワード	ホストの root パスワード。
ホスト・パスワードの確認	パスワードの確認。
ホスト接続の暗号化	ホストの SSH 暗号化トンネルを作成します。2 つの管理対象ホストの間で暗号化を有効にするには、各管理対象ホストで QRadar Console V7.1 または QRadar Risk Manager V7.1 が実行されている必要があります。
暗号化圧縮	2 つの管理対象ホストの間でデータ圧縮を有効にします。
ネットワーク・アドレス変換	管理対象ホストに対して NAT を有効にするには、NAT されたネットワークで静的 NAT 変換が使用されている必要があります。詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。

8. 「ネットワーク・アドレス変換」チェック・ボックスを選択した場合は、NAT パラメーターの値を入力する必要があります。

オプション	説明
NAT グループ	この管理対象ホストで使用されるネットワーク。 管理対象ホストが QRadar Consoleと同じサブネット上にある場合、NAT されたネットワークのコンソールを選択します。 管理対象ホストが QRadar Consoleと同じサブネットにない場合、NAT されたネットワークの管理対象ホストを選択します。
パブリック **IP**	管理対象ホストのパブリック IP アドレス。管理対象ホストはこの IP アドレスを使用して、NAT を使用する別のネットワーク内の他の管理対象ホストと通信します。

9. 「追加」をクリックします。 このプロセスには、数分かかることがあります。デプロイメントに変更が含まれている場合は、すべての変更をデプロイする必要があります。
10. 「管理」タブから、「拡張」 > 「すべての構成のデプロイ」をクリックします。

次のタスク

Web ブラウザー・キャッシュをクリアして、QRadar Consoleにログインします。これで「リスク」タブが使用可能になりました。

通信の確立

IBM Security QRadar Risk Manager アプライアンスと IBM Security QRadar SIEM Console の間の通信を確立してから QRadar Risk Manager のセットアップと構成を行ってください。

このタスクについて

通信を確立するための処理には数分かかることがあります。QRadar Risk Manager アプライアンスの IP アドレスを変更する場合や、QRadar Risk Manager を別の QRadar SIEM コンソールに接続する必要がある場合は、QRadar SIEM の「管理」タブにある「**Risk Manager** 設定 **(Risk Manager Settings)**」を使用できます。

手順

1. Web ブラウザーを開き、Web ブラウザーのキャッシュを消去します。
2. QRadar SIEM にログインします。IP アドレス、ユーザー名およびルート・パスワードについて詳しくは、『IBM Security QRadar Risk Manager ユーザー・インターフェースへのアクセス』を参照してください。
3. 「リスク」タブをクリックします。
4. 以下のパラメーターの値を入力します。

オプション	説明
IP/ホスト	QRadar Risk Manager アプライアンスの IP アドレスまたはホスト名
ルート・パスワード **(Root Password)**	QRadar Risk Manager アプライアンスのルート・パスワード。

5. 「保存」をクリックします。

次のタスク

ユーザー・ロールを定義します。

Risk Manager ユーザー・ロールの追加

IBM Security QRadar Risk Manager にアクセスできるようにするには、Risk Manager ユーザー・ロールを割り当てる必要があります。

このタスクについて

IBM Security QRadar SIEM では、デフォルトで QRadar Risk Manager 内のすべてのものにアクセスできるデフォルトの管理ロールが付与されます。管理特権 (デフォルトの管理ロールなど) が割り当てられたユーザーが自身のアカウントを編集することはできません。必要なすべての変更は、別の管理ユーザーが行う必要があります。

ユーザー・ロールの作成および管理については、「*IBM Security QRadar* 管理ガイド」を参照してください。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「ユーザー管理」ペインで「ユーザー・ロール」をクリックします。
4. 左側のペインで、編集するユーザー・ロールを選択します。
5. 「リスク・マネージャー **(Risk Manager)**」チェック・ボックスを選択します。
6. 「保存」をクリックします。
7. 「閉じる **(Close)**」をクリックします。
8. 「管理」タブで「変更のデプロイ」をクリックします。

第 3 章 監査の管理

IBM Security QRadar Risk Manager を使用すると、質問への回答が容易になり、ネットワーク・セキュリティー・ポリシーおよびコンプライアンス要件を簡単に評価することができます。

コンプライアンス監査は、セキュリティー管理者にとって必要ですが複雑な作業です。QRadar Risk Manager を使用すると、以下のような質問に回答できます。

- ネットワーク・デバイスがどのように構成されているか。
- ネットワーク・リソースがどのように通信しているか。
- ネットワークのどの部分が脆弱か。

ユース・ケース: デバイス構成の監査

IBM Security QRadar Risk Manager によって収集されたネットワーク・デバイスの構成情報は、監査コンプライアンスおよび構成バックアップのスケジューリングに使用できます。

構成をバックアップすることで、監査コンプライアンスのために、デバイスの変更の記録を集中管理し、自動化することができます。構成バックアップでは、構成変更をアーカイブし、履歴参照を提供します。つまり、履歴レコードを取得したり、構成を別のネットワーク・デバイスと比較したりすることができます。

QRadar Risk Manager の構成監査には以下のオプションが用意されています。

- ネットワーク・デバイス構成の履歴レコード。
- 正規化表示。構成を比較するときにデバイスの変更が表示されます。
- デバイスに対するルールを検索するツール。

デバイスの構成情報は、構成ソース管理のデバイス・バックアップから収集されます。QRadar Risk Manager は、デバイス・リストをバックアップするごとに、デバイス構成のコピーをアーカイブして、履歴参照を提供します。構成ソース管理のスケジュール頻度が高いほど、比較用および履歴参照用の構成レコードが多くなります。

デバイス構成履歴の表示

ネットワーク・デバイスの構成履歴を表示できます。

このタスクについて

バックアップしたネットワーク・デバイスの履歴情報を表示できます。この情報には「構成モニター **(Configuration Monitor)**」ページの「履歴」ペインからアクセスできます。「履歴」ペインには、ネットワーク・デバイスの構成に関する情報と、構成ソース管理を使用して最後にデバイス構成がバックアップされた日付が表示されます。

構成には、IBM Security QRadar Risk Manager に保管されている、ネットワーク・デバイス用のファイルのタイプが表示されます。一般的な構成タイプは以下のとおりです。

- 標準エレメント文書 (SED): ネットワーク・デバイスに関する情報を含む XML データ・ファイルです。個々の SED ファイルは未加工の XML 形式で表示されます。SED を別の SED ファイルと比較する場合は、表示が正規化され、ルールの差異が表示されます。
- 構成: 特定のネットワーク・デバイスによって提供される構成ファイルです。これらのファイルはデバイスのメーカーによって異なります。構成ファイルは、ダブルクリックすると表示できます。

注**:** デバイスによっては、他の複数の構成ファイルが表示される場合があります。それらのファイルをダブルクリックすると、内容がプレーン・テキストで表示されます。プレーン・テキスト表示では、Web ブラウザーのウィンドウから検索 (Ctrl+F)、貼り付け (Ctrl+V)、およびコピー (Ctrl+C) の機能がサポートされます。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「構成モニター **(Configuration Monitor)**」をクリックします。
3. 構成をダブルクリックして、詳細なデバイス情報を表示します。
4. 「履歴」をクリックします。
5. 「履歴」ペインで構成を選択します。
6. 「選択した項目を表示 **(View Selected)**」をクリックします。

単一デバイスのデバイス構成の比較

単一デバイスのデバイス構成を比較できます。

このタスクについて

比較するファイルが標準エレメント文書 (SED) である場合は、構成ファイル間でルールの差異を調べることができます。

正規化された構成を比較するときには、テキストの色によって以下のルールが示されます。

- 輪郭が緑の点線の場合は、デバイスに追加されたルールまたは構成を示します。
- 輪郭が赤い破線の場合は、デバイスから削除されたルールまたは構成を示します。
- 輪郭が黄色の実線の場合は、デバイスで変更されたルールまたは構成を示します。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「構成モニター **(Configuration Monitor)**」をクリックします。
3. デバイスをダブルクリックすると、詳細な構成情報が表示されます。

4. 「履歴」をクリックすると、そのデバイスの履歴が表示されます。
5. プライマリー構成を選択します。
6. Ctrl キーを押しながら、比較対象の別の構成を選択します。
7. 「履歴」ペインで「選択した項目を比較 **(Compare Selected)**」をクリックします。
8. オプション。未加工の構成の違いを表示するには、「未加工での比較を表示 **(View Raw Comparison)**」をクリックします。 構成ファイルまたは別のバックアップ・タイプを比較する場合は、未加工での比較が表示されます。

各種デバイスのデバイス構成の比較

異なるデバイスの構成を比較できます。比較するファイルが標準エレメント文書 (SED) である場合は、構成ファイル間でルールの差異を調べることができます。

このタスクについて

正規化された構成を比較するときには、テキストの色によって以下のルールが示されます。

- 輪郭が緑の点線の場合は、デバイスに追加されたルールまたは構成を示します。
- 輪郭が赤い破線の場合は、デバイスから削除されたルールまたは構成を示します。
- 輪郭が黄色の実線の場合は、デバイスで変更されたルールまたは構成を示します。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「構成モニター **(Configuration Monitor)**」をクリックします。
3. デバイスをダブルクリックすると、詳細な構成情報が表示されます。
4. 「履歴」をクリックすると、そのデバイスの履歴が表示されます。
5. プライマリー構成を選択します。
6. 「比較対象のマークを付ける **(Mark for Comparison)**」をクリックします。
7. ナビゲーション・メニューから「すべてのデバイス **(All Devices)**」を選択し、デバイス・リストに戻ります。
8. 比較するデバイスをダブルクリックし、「履歴」をクリックします。
9. マークを付けた構成と比較する別の構成バックアップを選択します。
10. 「マークしたものと比較 **(Compare with Marked)**」をクリックします。
11. オプション。未加工の構成の違いを表示するには、「未加工での比較を表示 **(View Raw Comparison)**」をクリックします。 構成ファイルまたは別のバックアップ・タイプを比較する場合は、未加工での比較が表示されます。

ユース・ケース: トポロジーでのネットワーク・パスの表示

IBM Security QRadar Risk Manager のトポロジーは、ネットワーク・デバイスをグラフィカルに表示します。

トポロジー・パス検索により、ネットワーク・デバイスの通信方法と、それらのデバイスが通信に使用するネットワーク・パスを判別できます。パス検索により、QRadar Risk Manager で送信元と宛先の間のパスをポート、プロトコル、およびルールとともに視覚化できます。

デバイスの通信方法を表示できます。これは、保護またはアクセス制限付きのアセットの場合に重要です。

主な機能は以下のとおりです。

- ネットワーク上のデバイス間の通信を表示する機能。
- フィルターを使用して、トポロジーでネットワーク・デバイスを検索。
- クイック・アクセスによるデバイス・ルールおよび構成の表示。
- パス検索で生成されたイベントを表示する機能。

トポロジーの検索

トポロジー検索を使用してネットワーク・トポロジー・ビューをフィルターに掛けて、ネットワーク・パス、ホスト、サブネット、およびその他のネットワーク・エレメントに絞り込むことができます。トポロジー検索を使用して、ネットワーク・インフラストラクチャーの各種エレメントを調査します。

このタスクについて

パス検索は、トポロジー・モデルをフィルターに掛けるために使用します。パス検索の対象は、送信元 IP アドレスまたは CIDR 範囲を含むすべてのネットワーク・サブネットと、構成済みのプロトコルおよびポートを使用した通信も可能な宛先 IP アドレスまたは CIDR 範囲を含むサブネットです。検索では、既存のトポロジー・モデルが調べられ、送信元と宛先の間の通信パスに関与するデバイスおよび詳細な接続情報が対象になります。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「トポロジー」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. 「検索条件 **(Search Criteria)**」ペインで「パス **(Path)**」を選択します。
5. 「送信元 **IP/CIDR**」フィールドに、トポロジー・モデルのフィルター基準とする IP アドレスまたは CIDR 範囲を入力します。複数の項目を区切るにはコンマを使用します。
6. 「宛先 **IP/CIDR (Destination IP/CIDR)**」フィールドに、トポロジー・モデルのフィルター基準とする宛先 IP アドレスまたは CIDR 範囲を入力します。複数の項目を区切るにはコンマを使用します。
7. オプション: 「プロトコル」リストから、トポロジー・モデルのフィルター処理に使用するプロトコルを選択します。
8. オプション: 「宛先ポート」フィールドに、トポロジー・モデルのフィルター基準とする宛先ポートを入力します。複数のポートを区切るにはコンマを使用します。
9. オプション: 「プロトコル」メニューからプロトコルを選択します。

10. オプション: 宛先ポートを入力します。
11. オプション: 「アプリケーションの選択」をクリックします。
    a. 「デバイス・アダプター **(Device Adapter)**」メニューからデバイス・アダプターのタイプを選択します。
    b. 検索語の一部または全体を入力するか「アプリケーション名」フィールドを空のままにして、「検索」をクリックします。
    c. 「検索結果」フィールドで表示されたいずれかのアプリケーションを選択して「追加」をクリックし、選択した項目を「選択された項目」ボックスに追加します。
    d. 「**OK**」をクリックします。
12. オプション: 「脆弱性の選択 **(Select Vulnerabilities)**」をクリックします。
    a. 「検索条件」メニューから脆弱性のカテゴリーを選択します。
    b. 「検索条件」メニューの横にある「フィールド」に脆弱性の ID 番号を入力します。
    c. 「検索」をクリックします。
    d. 「検索結果」フィールドで表示されたいずれかの脆弱性を選択して「追加」をクリックし、選択した項目を「選択された項目」ボックスに追加します。
    e. 「保存」をクリックします。

    トポロジーに侵入防止システム (IPS) が存在する場合は、脆弱性検索オプションが表示されます。詳細については、「*IBM Security QRadar Risk Manager* ユーザー・ガイド」を参照してください。
13. オプション: 「ユーザー**/**グループの選択 **(Select Users/Groups)**」をクリックします。
    a. 検索語の一部または全体を入力するか「ユーザー名」**/**「グループ名」フィールドを空のままにして、「検索」をクリックします。
    b. 「検索結果」フィールドでユーザー名またはグループ名を選択して「追加」をクリックし、選択した項目を「選択された項目」ボックスに追加します。
    c. 「**OK**」をクリックしてから「検索」をクリックします。
14. 「検索」をクリックして結果を表示します。

第 4 章 ユース・ケース: ポリシーのモニター

ポリシー監査および操作変更は、管理者およびセキュリティーの専門家が、重要なビジネス・アセット間でのアクセスおよび通信を制御することができる基本的な処理です。

ポリシー・モニターの基準には、以下のシナリオで、アセットおよび通信のモニターが該当する可能性があります。

- PCI セクション 1 監査で危険とされる構成のアセットがネットワークに存在するかどうか。
- PCI セクション 10 監査で危険とされるプロトコルを使用する通信をアセットが許可しているかどうか。
- ポリシー変更によってネットワークが違反状態になっている場合にそれを判断する方法。
- 強化したアセットや高リスク・アセットの脆弱性を表示する方法。

ポリシー・モニターを使用して、リスク・インディケーターに基づくテストを定義した後、テスト結果を制限して、特定の結果、違反、プロトコル、または脆弱性に対する照会をフィルタリングします。

IBM Security QRadar Risk Manager には、PCI カテゴリー別にグループ化されたポリシー・モニターの質問が用意されています。PCI 1、PCI 6、PCI 10 などの質問があります。アセットまたはデバイスおよびルールに対する質問を作成して、ネットワークのセキュリティー・リスクを明らかにすることができます。アセットまたはデバイス/ルールについての質問をポリシー・モニターに送信すると、返される結果にリスク・レベルが示されます。アセットから返された結果を承認するか、承認されない結果に対するシステムの応答方法を定義できます。

ポリシー・モニターには、以下の主な機能があります。

- ワークフローで支援する定義済みのポリシー・モニターの質問。
- 禁止されているプロトコルを使用してユーザーが通信を行ったかどうかの判別。
- 特定のネットワーク上のユーザーが、禁止されているネットワークまたはアセットと通信できるかどうかの評価。
- ファイアウォール・ルールが企業ポリシーに合致するかどうかの評価。
- 管理者に対してオフェンスまたはアラートを生成するポリシーの継続的モニター。
- デバイス構成の結果としてセキュリティーが侵害される可能性のあるシステムの評価による、脆弱性の優先順位付け。
- コンプライアンスの問題を特定するための支援。

ユース・ケース: 構成が疑わしいアセットの評価

組織は、企業セキュリティー・ポリシーを使用して、リスク、およびアセットとネットワークの間で許可する通信を定義します。コンプライアンスおよび企業ポリシーへの違反に関する業務を支援するために、組織はポリシー・モニターを使用して、不明である可能性のあるリスクを評価およびモニターします。

PCI コンプライアンスでは、機密データが格納されているアセットを保護するために、カード所有者データを持つデバイスを識別し、次に通信を図式化して検証し、ファイアウォール構成をモニターすることを規定しています。ポリシー・モニターは、これらの要件を素早く満たす方法を提供し、管理者が企業ポリシーに準拠できます。リスクを減らすための一般的な方式には、保護されていないプロトコルを使用して通信するアセットを識別およびモニターすることが含まれます。これらは、FTP 接続または telnet 接続を許可するルーター、ファイアウォール、スイッチなどのプロトコルです。トポロジー内で構成が危険なアセットを特定する際は、ポリシー・モニターを使用します。

PCI セクション 1 の質問には以下の基準を含めることができます。

- 禁止されたプロトコルを許可するアセット。
- 危険なプロトコルを許可するアセット。
- ネットワーク上のポリシーに従っていないアプリケーションを許可するアセット。
- 保護アセットを含むネットワークに対してポリシーに従っていないアプリケーションを許可するアセット。

危険なプロトコルを許可するデバイスの評価

危険なプロトコルを許可するデバイスを評価するには、ポリシー・モニターを使用します。

このタスクについて

IBM Security QRadar Risk Manager は、質問を評価して、テストの質問に合致するすべてのアセットの結果をトポロジー内に表示します。セキュリティーの専門家、管理者、またはネットワーク内の監査員は、特定のアセットに対して危険でない通信を承認できます。動作に対するオフェンスを作成することもできます。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「ポリシー・モニター」をクリックします。
3. 「グループ」リスト・ボックスから「**PCI 1**」を選択します。
4. テスト質問「インターネットから **DMZ** への危険なプロトコル **(**例**: Telnet** および **FTP** トラフィック。ポートはそれぞれ **21** と **23)** を許可するすべてのデバイス **(**例**:** ファイアウォール**)** の評価 **(Assess any devices (i.e. firewalls) that allow risky protocols (i.e. telnet and FTP traffic - port 21 & 23 respectively) from the internet to the DMZ)**」を選択します。
5. 「質問の送信 **(Submit Question)**」をクリックします。

ユース・ケース: 疑わしい通信があるアセットの評価

ポリシー・モニターを使用して、ネットワーク・アセットへのアクセスを追跡、ログ記録、および表示することで、PCI セクション 10 への準拠を識別します。

IBM Security QRadar Risk Manager では、疑わしい通信や危険な通信を許可するアセットをトポロジー内で識別することによって、PCI セクション 10 への準拠を識別できます。QRadar Risk Manager では、それらのアセットで実際の通信または予測される通信について検査することができます。実際の通信では、通信する際に質問の基準を使用したアセットを表示します。予測される通信では、質問の基準を使用して通信できるアセットを表示します。

PCI セクション 10 の質問には以下の基準を含めることができます。

- 内部ネットワークに対する着信質問を許可するアセット。
- 信頼できないロケーションから信頼できるロケーションへの通信を行うアセット。
- VPN から信頼できるロケーションへの通信を行うアセット。
- 信頼できるロケーションの中で、暗号化されていない、ポリシーに従っていないプロトコルを許可するアセット。

通信を許可するアセットの検索

インターネットからの通信を許可するアセットを検索できます。

このタスクについて

IBM Security QRadar Risk Manager は、質問を評価して、インターネットからのインバウンド接続を許可するすべての内部アセットの結果を表示します。ネットワーク内のセキュリティーの専門家、管理者、または監査員は、アセットへの通信のうち、ネットワーク内のリスクを表していない通信を承認できます。生成されるイベントが増えるため、IBM Security QRadar SIEM でオフェンスを作成して、この種の危険な通信をモニターすることができます。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「ポリシー・モニター」をクリックします。
3. 「グループ」リストで「**PCI 10**」を選択します。
4. テスト質問「インターネットから内部ネットワーク上の任意の場所へのインバウンド接続を評価 **(Assess any inbound connections from the internet to anywhere on the internal network)**」を選択します。
5. 「質問の送信 **(Submit Question)**」をクリックします。

ユース・ケース: ポリシー違反のモニター

IBM Security QRadar Risk Manager は、任意の定義済みのまたはユーザー生成の質問をポリシー・モニターで継続的にモニターすることができます。モニター・モードを使用すると、QRadar Risk Manager でイベントを生成できます。

モニター対象の質問を選択すると、QRadar Risk Manager が 1 時間ごとにトポロジーに対してその質問を分析し、アセットまたはルールの変更によって承認されない結果が発生するかどうかを判別します。承認されない結果を QRadar Risk Manager が検出した場合は、オフェンスを生成して、定義済みポリシーからの逸脱を示すアラートを発します。モニター・モードでは、QRadar Risk Manager が同時に 10 件の質問の結果をモニターできます。

質問のモニターには、以下の主な機能があります。

- ルールまたはアセットの変更を 1 時間ごとにモニターし、承認されない結果になるかどうか検査する。
- 上位および下位のイベント・カテゴリーを使用して、承認されない結果を分類する。
- 承認されない結果の場合にオフェンス、E メール、Syslog メッセージ、またはダッシュボード通知を生成する。
- QRadar SIEM のイベント表示、相関、イベント・レポート作成、カスタム・ルール、およびダッシュボードを使用する。

質問の構成

ポリシー・モニターを使用して、モニターする質問を構成できます。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「ポリシー・モニター」をクリックします。
3. モニターする質問を選択します。
4. 「モニター」をクリックします。
5. 質問をモニターするために必要なすべてのオプションを構成します。
6. 「モニターの保存 **(Save Monitor)**」をクリックします。

タスクの結果

これで質問に対してモニターが有効になり、モニター基準に基づいてイベントまたはオフェンスが生成されます。

脆弱性別のリスク優先順位

アセットで検出された脆弱性には、ネットワーク・ロケーションによって、または脆弱性のある別のデバイスへの接続によって優先順位を付けることができます。

IBM Security QRadar Risk Manager は、ポリシー・モニターでアセット情報および脆弱性情報を使用します。この情報を使用して、アセットが入力型の攻撃 (SQL インジェクション、隠しフィールド、クリック・ジャッキング など) の影響を受けやすいかどうかを判別します。

脆弱性アセットの質問には以下の基準を含めることができます。

- 特定の日付後に報告された新しい脆弱性を持つアセット。
- 特定の脆弱性または CVSS スコアを持つアセット。
- 特定の脆弱性の分類 (入力操作やサービス妨害など) に該当するアセット。

特定の脆弱性を持つアセットの検索

IBM Security QRadar Risk Manager は、質問を評価して、脆弱性があるアセットの結果を表示します。

このタスクについて

セキュリティーの専門家、管理者、または監査員が、既知の SQL インジェクションの脆弱性がある、ネットワーク内のアセットを特定できます。保護されたネットワークに接続された任意のアセットに直ちにパッチを適用することができます。生成されるイベントが増えるため、IBM Security QRadar SIEM でイベントまたはオフェンスを作成して、SQL インジェクションの脆弱性があるアセットをモニターすることができます。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「ポリシー・モニター」をクリックします。
3. 「グループ」リストから「脆弱性」を選択します。
4. テスト質問「特定のローカル・ネットワーク **(**例**:** 保護されたサーバー・ネットワーク**)** で **SQL** インジェクションの脆弱性を持つアセットの評価 **(Assess assets with SQL injection vulnerabilities on specific localnet(s) (i.e. protected server network))**」を選択します。
5. 「質問の送信 **(Submit Question)**」をクリックします。

第 5 章 シミュレーションのユース・ケース

ユース・ケース: ネットワーク・アセットに対する攻撃のシミュレート

シミュレーションを使用して、ネットワークにさまざまな送信元からの脆弱性がないかテストできます。

攻撃のシミュレーションを使用してネットワークのデバイス構成を監査できます。

シミュレーションには、以下の主な機能があります。

- シミュレーションで、ネットワークに対する攻撃が可能な経路の理論的な配列を表示する。
- シミュレーションで、ネットワーク・デバイスを介して攻撃をどのように伝搬させ、他のアセットに拡散させる可能性があるのかを表示する。
- シミュレーションで、新たな機密漏れサイトを検出するためのモニターを実行できる。

シミュレーションの作成

SSH プロトコルへのネットワーク攻撃のシミュレーションを作成できます。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「シミュレーション」 > 「シミュレーション」を選択します。
3. 「アクション」リストから「新規」を選択します。
4. シミュレーションの名前を入力します。
5. 「現在のトポロジー **(Current Topology)**」を選択します。
6. 「接続データを使用する **(Use Connection Data)**」チェック・ボックスを選択します。
7. 「シミュレーションの開始場所 **(Where do you want the simulation to begin)**」リストから、シミュレーションのオリジンを選択します。
8. シミュレーション攻撃「プロトコルを使用した以下の開いているポートのいずれかを対象とした攻撃 **(Attack targets one of the following open ports using protocols)**」を追加します。
9. このシミュレーションでは、「開いているポート」をクリックしてポート 22 を追加します。
10. 「プロトコル」をクリックして「**TCP**」を選択します。 SSH は TCP を使用します。
11. 「**OK**」をクリックします。
12. 「シミュレーションの保存 **(Save Simulation)**」をクリックします。

13. 「アクション」リストから「シミュレーションの実行 **(Run Simulation)**」を選択します。 結果列には、シミュレーションの実行日と結果を表示するためのリンクのリストが表示されます。
14. 「結果の表示 **(View Results)**」をクリックします。

タスクの結果

SSH 脆弱性を含むアセットのリストが結果に表示され、ネットワーク管理者はネットワークで許可されるか予期される SSH 接続を承認することができます。承認しない通信については、イベントやオフェンスをモニターできます。

表示される結果から、ネットワーク管理者やセキュリティーの専門家は、攻撃経路およびネットワーク内で攻撃によって使用される可能性のある接続を視覚的に把握することができます。例えば、最初のステップでは、シミュレーションによって、影響を受ける、直接接続されているアセットのリストを提供します。2 番目のステップは、シミュレーションの第 1 レベルのアセットと通信できる、ネットワーク内のアセットをリストします。

攻撃で提供される情報により、考え得る膨大な数の攻撃シナリオに対してネットワークの強化とテストを行うことができます。

ユース・ケース: ネットワーク構成変更のリスクのシミュレート

既存のネットワークに基づく仮想ネットワーク・モデルを定義するためのトポロジー・モデルを使用できます。組み合わせと構成が可能な一連の変更に基づいたネットワーク・モデルを作成できます。

トポロジー・モデルを使用し、ネットワークでの構成変更の影響をシミュレーションによって判断することができます。

トポロジー・モデルには、以下の主な機能があります。

- ネットワークの変更をテストするための仮想トポロジーを作成する。
- 仮想ネットワークに対する攻撃をシミュレートする。
- テストを通じて、保護するアセットに対するリスクおよび機密漏れを低減する。
- 仮想ネットワーク・セグメントによって、ネットワークやアセットの機密部分を制限およびテストできるようにする。

ネットワークの構成変更をシミュレートするには、以下のようにします。

1. トポロジー・モデルを作成する。
2. トポロジー・モデルに対する攻撃をシミュレートする。

トポロジー・モデルの作成

トポロジー・モデルを作成して、ネットワークの変更をテストしたり攻撃をシミュレートしたりすることができます。

手順

1. 「リスク」タブをクリックします。

2. ナビゲーション・メニューで、「シミュレーション」 > 「トポロジー・モデル **(Topology Models)**」を選択します。
3. 「アクション」リストから「新規」を選択します。
4. モデルの名前を入力します。
5. トポロジーに適用するすべての変更を選択します。
6. 「モデルを以下として構成 **(Configure model as follows)**」ペインに追加されたテストを構成します。
7. 「モデルの保存 **(Save Model)**」をクリックします。

次のタスク

新しいトポロジー・モデル用のシミュレーションを作成します。

攻撃のシミュレート

ポートおよびプロトコルへの攻撃をシミュレートできます。

手順

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「シミュレーション」 > 「シミュレーション」を選択します。
3. 「アクション」リスト・ボックスから「新規」を選択します。
4. シミュレーションの名前を入力します。
5. 作成したトポロジー・モデルを選択します。
6. 「シミュレーションの開始場所 **(Where do you want the simulation to begin)**」リストから、シミュレーションのオリジンを選択します。
7. シミュレーション攻撃「プロトコルを使用した以下の開いているポートのいずれかを対象とした攻撃 **(Attack targets one of the following open ports using protocols)**」を追加します。
8. このシミュレーションでは、「開いているポート」をクリックしてポート 22 を追加します。
9. 「プロトコル」をクリックして「TCP」を選択します。 SSH は TCP を使用します。
10. 「**OK**」をクリックします。
11. 「シミュレーションの保存 **(Save Simulation)**」をクリックします。
12. 「アクション」リストから「シミュレーションの実行 **(Run Simulation)**」を選択します。 結果列には、シミュレーションの実行日と結果を表示するためのリンクのリスト・ボックスが表示されます。
13. 「結果の表示 **(View Results)**」をクリックします。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

商標

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

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

製品資料に関するご使用条件

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

適用度

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

個人使用

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

商業的使用

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

権限

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

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

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

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

IBM オンラインでのプライバシー・ステートメント

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を

持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

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

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

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

索引

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

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

I

N

P

Q

R

S

W

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