IBM Security QRadar

マスター・コンソール

バージョン 0.10.0

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、 21 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。

目次

マスター・コンソールの概要 v

マスター・コンソール 1

管理者のためのマスター・コンソールの新機能 1
- マスター・コンソール V0.10.0 の新機能 1
- マスター・コンソール V0.9.1 の新機能 2
- マスター・コンソール V0.9.0 の新機能 2
- マスター・コンソール V0.8.1 の新機能 2

マスター・コンソールの概要 3
- サポートされる環境 3
- マスター・コンソールのインストール 5
- マスター・コンソールを開く 6
- マスター・コンソール用の許可トークンの作成 7
- マスター・コンソールへのデプロイメントの追加 7

デプロイメントのモニター 8
- 管理対象ホストのモニター 9
- オフェンスのモニター 11
- オフェンス・リストのフィルタリング 13

ユーザー管理 15
- ローカル・ユーザーの追加 15
- ユーザー設定の編集 15
- ローカル・ユーザーの削除 16
- ユーザー・リストのフィルタリング 16
- マスター・コンソールでの Active Directory 認証および LDAP 認証の構成 17

特記事項 21

商標 22
製品資料に関するご使用条件 23
IBM オンラインでのプライバシー・ステートメント 23
プライバシー・ポリシーに関する考慮事項 24

マスター・コンソールの概要

IBM® Security QRadar® 管理者は、マスター・コンソールを使用して、デプロイメント環境およびホストについての正常性およびその他の情報を表示します。

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 ユーザーを対象としています。本書の情報を利用するには、QRadar 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が必要です。

技術文書

Web 上で IBM Security QRadar の製品資料 (翻訳されたすべての資料を含む) を検索するには、 IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリー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連絡

お客様サポートへのお問い合わせについては、Support for IBM Security QRadar (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) を参照してください。

適切なセキュリティー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。

マスター・コンソール

IBM Security QRadar デプロイメントをモニターするには、マスター・コンソールを使用します。

マスター・コンソールはマネージド・セキュリティー・サービス・プロバイダー (MSSP) 環境の場合に有用です。ダッシュボードを使用することで、複数のデプロイメントを同時にモニターできます。

運用データ (CPU 使用状況、ネットワークおよびディスクのアクティビティー、メモリー使用状況、イベント・レート、フロー・レートなど) が視覚的に表現されるため、デプロイメントの正常性を容易にモニターできます。

オフェンス集中管理ビューには、すべてのデプロイメントからのオフェンスがマグニチュードの順序で表示されます。情報をドリルダウンした後、特定の QRadar デプロイメントにログインして、オフェンスに関する詳細情報を取得します。

管理者のためのマスター・コンソールの新機能

マスター・コンソールの各リリースにおける新機能について説明します。

マスター・コンソール V0.10.0 の新機能

マスター・コンソール V0.10.0 では、テナントとドメインの認識、ユーザー・リスト内の検索およびフィルター操作の機能、将来におけるアップグレードに関するレルム・ベースの情報の保持などが導入されました。

マスター・コンソール・ユーザーの検索およびフィルター操作

新しい検索バーを使用すると、テキスト照会およびフィールド・ベースの照会を作成して、「ユーザー管理」ウィンドウに表示されるマスター・コンソール・ユーザーのリストをフィルターに掛けることができます。

マスター・コンソール・ユーザーのリストのフィルタリングに関する詳細...

テナントとドメインの認識

マスター・コンソールに、モニターする各デプロイメントに対して構成されているテナントおよびドメインに関する情報が表示されるようになりました。「管理対象ホスト」ページの「テナント」タブをクリックして、各テナントごとのイベント・レート制限およびフロー・レート制限を表示します。

QRadar デプロイメントについての情報の参照に関する詳細...

将来におけるアップグレード時のレルム情報の処理の改善

サード・パーティーの認証プロバイダーが構成されると、将来におけるマスター・コンソールのアップグレードでレルム設定が保持されます。この改善を利用するに

は、マスター・コンソール V0.10.0 にアップグレードするときか、最初にサード・パーティーの認証プロバイダーを構成するときに、レルム情報を `shiro.realms` ファイルに追加する必要があります。

 認証プロバイダーの構成に関する詳細...

マスター・コンソールの YUM パッケージ・マネージャーを使用したインストール

マスター・コンソールは、Yellowdog Updater Modified (YUM) コマンドを使用してインストールできるようになりました。このコマンドは、改善された依存関係チェックおよびパッケージ管理の機能を提供します。

 マスター・コンソールのインストールに関する詳細...

データ検証およびメッセージの改善

再設計された「デプロイメントの追加 **(Add Deployment)**」、「デプロイメントの編集 **(Edit Deployment)**」、および 「ユーザー管理」の各ウィンドウは、デプロイメントとユーザー・アカウントを管理する際に、改善されたデータ検証および情報メッセージを提供します。

マスター・コンソール V0.9.1 の新機能

マスター・コンソール V0.9.1 には、「デプロイメント」ウィンドウのリフレッシュ頻度を修正する更新と、マスター・コンソールが IBM Security QRadar のより新しいバージョンで動作するようにするための更新が含まれています。

マスター・コンソール V0.9.0 の新機能

マスター・コンソール V0.9.0 ではオフェンスの検索とフィルター処理を導入し、Microsoft Internet Explorer 10 のサポートを削除しました。

オフェンスの検索およびフィルター操作

新しい検索バーを使用すると、テキスト照会およびフィールド・ベースの照会を作成して、統合オフェンス・リストに表示されるオフェンスをフィルターに掛けることができます。  詳細...

サポート対象ブラウザーの更新

Microsoft Internet Explorer 10 のブラウザー・サポートは本リリースで削除されました。  詳細...

マスター・コンソール V0.8.1 の新機能

マスター・コンソール V0.8.1 では、ローカル・ユーザー管理、および Active Directory プロバイダーと LDAP セキュリティー・プロバイダーへのサポートが導入されました。

ユーザー管理

ローカル・ユーザーのマスター・コンソールへのアクセス権限を付与および制御できます。マスター・コンソール V0.8.1 以降へのアップグレードの後で、すべての既存の QRadar ユーザーは、マスター・コンソールにローカル・ユーザーとしてマイグレーションされます。管理者は、マスター・コンソールでユーザーの追加やパスワードの変更などのユーザー管理を行います。 詳細...。

セキュリティー・プロバイダーの統合

既存の Active Directory または LDAP のセキュリティー・インフラストラクチャーを使用して、ユーザー認証を構成できます。 詳細...

マスター・コンソールの概要

マスター・コンソールをインストールして、IBM Security QRadar デプロイメントのすべての QRadar ホストの正常性およびシステムをモニターします。

サポートされる環境

マスター・コンソールをインストールして使用する前に、ご使用の環境にサポート対象のハードウェアおよびソフトウェアがあることを確認してください。

ハードウェア要件

マスター・コンソールは QRadar 3105 アプライアンスで動作します。

マスター・コンソールをインストールする前に、仮想アプライアンスまたは物理アプライアンスが以下のハードウェア仕様を満たしていることを確認してください。

表 1. QRadar 3105 アプライアンスの概要

説明	値
プロセッサー	8
インターフェース	2 つの 10/100/1000 Base-T ネットワーク・モニター・インターフェース 1 つの 10/100/1000 Base-T QRadar 管理インターフェース 1 つの 10/100 Base-T 統合管理モジュール・インターフェース 2 つの 10 Gbps SFP + ポート
メモリー	64 GB 8x 8 GB 1600 MHz RDIMM
ストレージ	9 x 3.5 インチ 1 TB 7.2 K rpm NL SAS、合計 9 TB、6.2 TB 使用可能 (RAID 5)
電源機構	二重予備 750W AC 電源
寸法	奥行き 29.5 インチ x 幅 17.7 インチ x 高さ 2.4 インチ

ソフトウェア要件

マスター・コンソールをホストするには、8500 アクティベーション・キー (3L0C3S-2M0F3Q-6B1N0W-5N737F) を使用して IBM Security QRadar をインストールする必要があります。別個のライセンス・キーは不要です。

QRadar Log Manager デプロイメントをモニターする際にマスター・コンソールを使用できますが、オフェンス集中管理ビューには何も表示されません。オフェンス集中管理ビューは、オフェンスをモニターするシステム (QRadar SIEM など) 用にオフェンスを表示するだけです。

マスター・コンソールをホストするために必要な QRadar バージョンは、マスター・コンソールがモニターできる QRadar バージョンとは異なる可能性があります。マスター・コンソールをインストールする前に、以下の表のソフトウェア要件を確認してください。

表 2. マスター・コンソールのソフトウェア要件

マスター・コンソールのバージョン	インストール先	モニター対象	サポート対象のブラウザー
マスター・コンソール v0.10.0*	QRadar V7.2.7	QRadar V7.2.6 以降	Microsoft Internet Explorer 11 Mozilla Firefox 38 延長サポート版 Google Chrome (最新バージョン)
マスター・コンソール v0.9.1	QRadar V7.2.6 以降	QRadar V7.2.6 以降	Microsoft Internet Explorer 11 Mozilla Firefox 38 延長サポート版 Google Chrome (最新バージョン)
マスター・コンソール v0.9.0	QRadar V7.2.6	QRadar V7.2.6 以降	Microsoft Internet Explorer 11 Mozilla Firefox 38 延長サポート版 Google Chrome (最新バージョン)

表 2. マスター・コンソールのソフトウェア要件 (続き)

マスター・コンソールのバージョン	インストール先	モニター対象	サポート対象のブラウザー
マスター・コンソール v0.8.1	QRadar V7.2.5 または V7.2.6	QRadar V7.2.5 または V7.2.6	Microsoft Internet Explorer 11 Microsoft Internet Explorer 10 Mozilla Firefox 38 延長サポート版 Google Chrome (最新バージョン)
* 製品サポートは、リリースされた最新バージョンのマスター・コンソールに制限されています。			

QRadar のインストールについて詳しくは、「*IBM Security QRadar* インストール・ガイド」を参照してください。

マスター・コンソールのインストール

8500 アクティベーション・キー (3L0C3S-2M0F3Q-6B1N0W-5N737F) を使用して IBM Security QRadar V7.2.5 以降をインストールすると、マスター・コンソールが自動的にインストールされます。別個のライセンス・キーは不要です。QRadar のインストールについて詳しくは、「*IBM Security QRadar* インストール・ガイド」を参照してください。

最新のマスター・コンソール機能および拡張は IBM Fix Central からダウンロードできます。

始める前に

インストール先のアプライアンスが必要な最小ハードウェア仕様を満たしていることを確認します。詳しくは、3 ページの『サポートされる環境』を参照してください。

マスター・コンソールのフィックスパック・ファイルをローカル・システムから QRadar アプライアンスにコピーするために、WinSCP などのファイル・コピー用ソフトウェア・プログラムが必要です。

このタスクについて

初めてマスター・コンソール V0.8.1 以降に更新するときは、更新処理中に QRadar コンソールからユーザーがインポートされます。このインポートでは、既存のすべてのマスター・コンソール・ユーザー (管理者など) のパスワードが上書きされ、QRadar コンソールで設定されているパスワードと同じパスワードに設定されます。インポート処理は 1 回しか行われません。以降は、マスター・コンソールを更新してもユーザーはインポートされず、パスワードも上書きされません。

手順

1. Fix Central (http://www.ibm.com/support/fixcentral) からマスター・コンソールのフィックスパックをダウンロードします。
2. WinSCP などのソフトウェア・プログラムを使用して、マスター・コンソールがインストールされている QRadar ホストにマスター・コンソールのフィックスパックをコピーします。
3. SSH を使用して、root ユーザーとして、マスター・コンソール・ソフトウェア・フィックスをコピーした QRadar ホストにログインします。
4. 以下のコマンドを入力して、Tomcat サービスを停止します。

   ```
   service tomcat stop
   ```

5. QRadar アプライアンスのコンソール・ウィンドウで、以下のコマンドを入力して、マスター・コンソールをインストールします。

   ```
   yum -y install masterconsole-<version#>.rpm
   ```

6. 以下のコマンドを入力して、Tomcat サービスを再始動します。

   ```
   service tomcat start
   ```

タスクの結果

これで、マスター・コンソールがインストールされ、QRadar アプライアンス上のサービスが再始動されました。

マスター・コンソールを開く

マスター・コンソールがインストールされている場合は、QRadar コンソールの IP アドレスを使用してマスター・コンソールを開きます。

始める前に

8500 アクティベーション・キー (3L0C3S-2M0F3Q-6B1N0W-5N737F) を使用して QRadar がインストールされていることを確認します。

このタスクについて

初めてマスター・コンソール V0.8.1 以降に更新するときは、更新処理中に QRadar コンソールからユーザーがインポートされます。このインポートでは、既存のすべてのマスター・コンソール・ユーザー (管理者など) のパスワードが上書きされ、QRadar コンソールで設定されているパスワードと同じパスワードに設定されます。インポート処理は 1 回しか行われません。以降は、マスター・コンソールを更新してもユーザーはインポートされず、パスワードも上書きされません。

手順

1. Web ブラウザーを開き、以下の URL を入力します。

   ```
   https://IP_address
   ```

   ここで *IP_address* は、マスター・コンソールをインストールした QRadar ホストの IP アドレスです。
2. マスター・コンソールにログインします。

初めてマスター・コンソールにログインする場合は、システムの管理者アカウントおよびルート・パスワードを使用します。

次のタスク

モニターする QRadar デプロイメントを追加するために、『マスター・コンソールへのデプロイメントの追加』を参照してください。

マスター・コンソール用の許可トークンの作成

許可トークンを作成して、マスター・コンソールが IBM Security QRadar デプロイメントに接続できるようにする必要があります。

手順

1. 「管理」タブの「システム構成」の下にある「許可サービス」をクリックします。
2. 「許可サービスの追加」をクリックしてパラメーターを構成します。
   a. 「サービス名」フィールドにサービスの名前を入力します。 名前の長さは 255 文字まで可能です。
   b. 「ユーザー・ロール」メニューで「管理者」を選択します。

      許可サービスに割り当てられたユーザー・ロールにより、その許可サービスが QRadar でアクセスできる機能が決まります。マスター・コンソールの許可トークンには「管理者」ユーザー・ロールが必要です。
   c. 「セキュリティー・プロファイル」メニューで「管理者」を選択します。

      セキュリティー・プロファイルにより、当該サービスが QRadar でアクセスできるネットワークおよびログ・ソースが決まります。マスター・コンソールの許可トークンには「管理者」セキュリティー・プロファイルが必要です。
   d. 「有効期限日付」フィールドで、トークンを期限切れにする日付を選択するか、「期限なし」チェック・ボックスをクリックします。
3. 「サービスの作成」をクリックしてトークンの値を記録します。

マスター・コンソールへのデプロイメントの追加

マスター・コンソール管理者は、モニターする IBM Security QRadar デプロイメントを追加する必要があります。

始める前に

- 許可トークンが必要です。詳しくは、『マスター・コンソール用の許可トークンの作成』を参照してください。
- 組織がセキュア SSL を使用する必要がある場合は、必ずマスター・コンソールでモニターするすべての QRadar デプロイメントで、信頼できない SSL 証明書を自己署名証明書または信頼証明書のいずれかに置き換えてください。
- マスター・コンソールに対して QRadar デプロイメントを追加、編集、または削除できるのは QRadar 管理者のみです。

手順

1. デプロイメントを追加するには、画面の右上隅にある追加 (+) アイコンをクリックします。
2. デプロイメントの名前を入力します。
3. コンソールの IP アドレスまたはホスト名を入力します。
4. 許可トークンを入力します。
5. 「デプロイメントの追加 **(Add Deployment)**」をクリックします。
6. 非セキュア SSL を使用するデプロイメントを追加し、かつ組織がセキュア SSL を使用する必要がない場合は、「非セキュア **SSL** を無視 **(Ignore insecure SSL)**」チェック・ボックスを選択し、「送信」をクリックします。

デプロイメントのモニター

マスター・コンソールでは、デプロイメント・カードと呼ばれる、マスター・コンソールに接続されたすべての IBM Security QRadar デプロイメントの正常性および運用データのグラフィカル表現が表示されます。

すべてのデプロイメント・カードは、「デプロイメント (重大度別) (Deployments by Severity)」ページで表示できます。注意が必要なデプロイメントを迅速に判別できるように、デプロイメント・カードは 3 つのグループ (重要、警告、正常 **(Healthy)**) にソートされます。

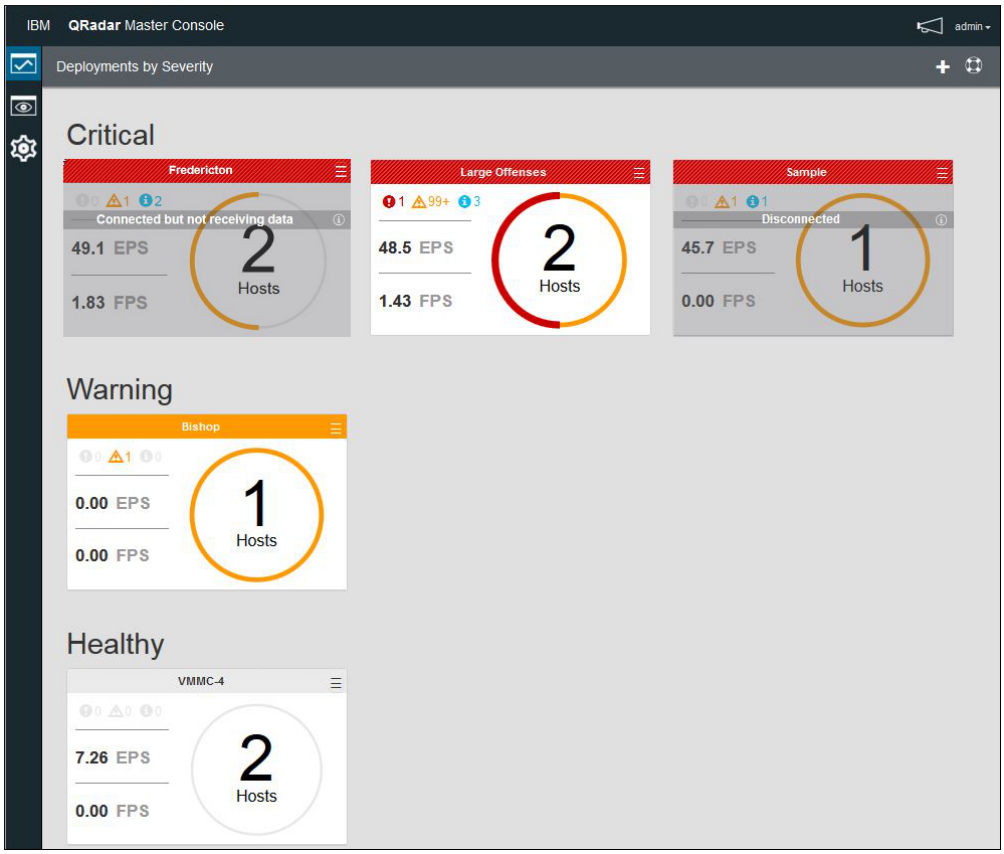

図 *1.* マスター・コンソール内のデプロイメント・カード

各デプロイメント・カードには以下の情報が表示されます。

- デプロイメント内の管理対象ホストの数。
- デプロイメントの状況。円を囲む色で表されます。例えば、デプロイメント内に管理対象ホストが 2 つあり、そのうち 1 つが「重要」状況になっている場合は、数値 2 を囲む円の半分が赤くなります。
- 過去 15 分間のシステム通知 (重要、警告、通知) の数。
- イベント・レートおよびフロー・レート。直近 15 分間の平均として測定します。

マスター・コンソールがデプロイメントに接続できない場合は、デプロイメント・カードに「切断 **(Disconnected)**」と表示されます。この状況の場合は、デプロイメントの電源が切れている可能性があります。デプロイメントが「接続済み **(**ただしデータ受信なし**) (Connected but not receiving data)**」と表示されている場合は、許可トークンが取り消されたか期限切れになっている可能性があります。

デプロイメント・カードでは、以下のアクションを実行できます。

- デプロイメント・カードをクリックして「管理対象ホスト」ビューを開く。
- 3 本線のメニュー  アイコンをクリックして、デプロイメントの詳細情報を編集したり、デプロイメントをマスター・コンソールから切断したりする。
- デプロイメントが「切断 **(Disconnected)**」または「接続済み **(**ただしデータ受信なし**) (Connected but not receiving data)**」である場合は、デプロイメント・カードの情報アイコンをクリックすると、最後にデータを受信した日時が表示されます。

管理対象ホストのモニター

1 つのデプロイメントに接続しているすべての管理対象ホストのシステム通知、システムのメモリーおよび CPU の使用状況統計を表示するには、「管理対象ホスト」ページを使用します。

注意が必要な管理対象ホストを迅速に判別できるように、管理対象ホスト・カードの上部が色分けされます。赤は「重要」状況を示し、黄色は「警告」状況を示し、灰色は「正常 **(Healthy)**」状況を示します。

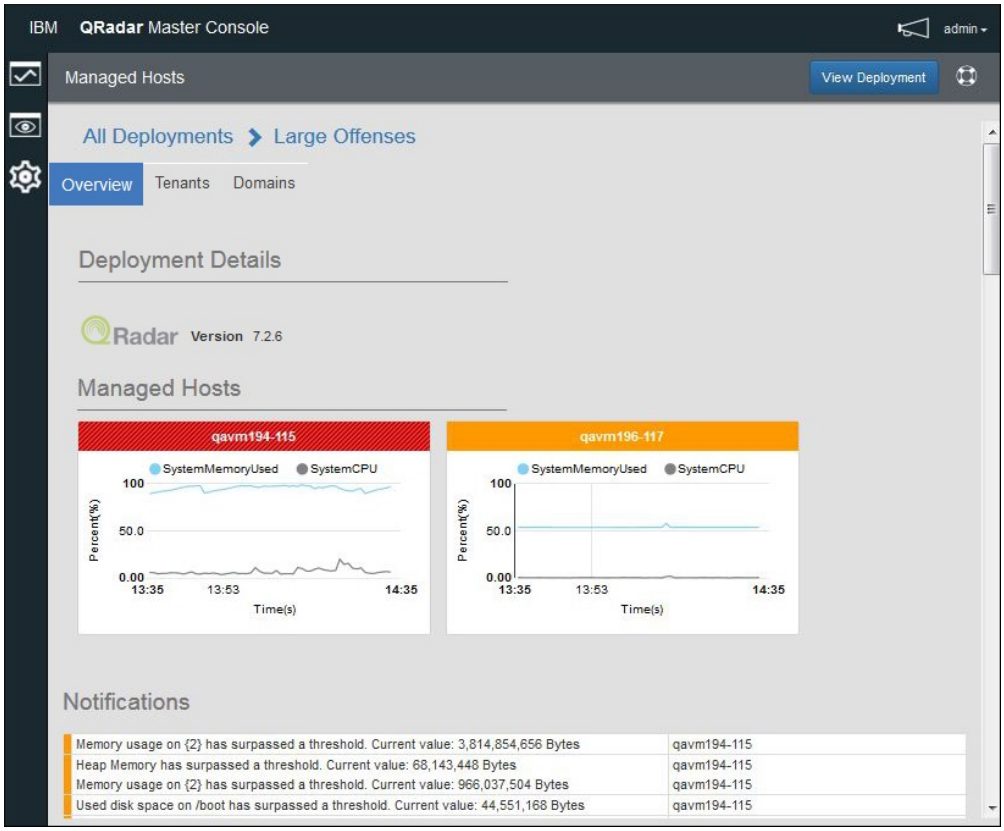

図 2. マスター・コンソールの「管理対象ホスト」ページ

手順

1. 「管理対象ホスト」ページを表示するには、「デプロイメント (重大度別) (Deployments by Severity)」ページのデプロイメント・カードをクリックします。
2. 「管理対象ホスト」ページでは以下のアクションを実行できます。
   a. 「デプロイメントの表示」をクリックして QRadar デプロイにログインします。
   b. 「テナント」タブと「ドメイン」タブをクリックして、デプロイメントに構成されているテナントおよびドメインに関する情報を表示します。
   c. 管理対象ホストのグラフにマウス・カーソルを移動すると、グラフのメトリックに関する詳細情報が表示されます。
   d. 管理対象ホストのグラフにメトリックを表示しないようにするには、そのメトリックの色付きアイコンをクリックします。例えば、「**SystemCPU**」メトリックをグラフに表示しないようにするには、「システム **CPU (System CPU)**」の横にある灰色の円をクリックします。
   e. ホストの運用データ (CPU およびメモリーの使用状況、ネットワークおよびディスクでの読み書き、イベント・レート、フロー・レートなど) を表示するには、管理対象ホスト・カードをクリックします。

オフェンスのモニター

複数の IBM Security QRadar デプロイメントのオフェンスをモニターするには、マスター・コンソールを使用します。すべてのデプロイメントのオフェンスは 1 つのリストで表示され、最も重要なオフェンスが一番上に表示されます。

このタスクについて

オフェンス・カードのソート順序は、マグニチュード、デプロイメント、および最終更新時刻です。

マグニチュード はオフェンスの相対的な重要性を示します。関連性、重大度、および信頼性の各値に基づいて計算されます。

- 関連性 は、オフェンスがネットワークに及ぼす影響を判別します。例えば、ポートが開いている場合の関連性は高です。
- 信頼性 は、ログ・ソース内に構成された信頼性の評価によって判断される、オフェンスの完全性を示します。複数のソースから同じイベントが報告されると、信頼性が高くなります。
- 重大度 は、送信元による脅威を、攻撃に対する宛先での準備の程度と対比して示します。

マグニチュードの数値によって、オフェンス・カードの色が決定されます。オフェンス・カードの色付きの棒にマウス・カーソルを移動すると、マグニチュードの数値が表示されます。

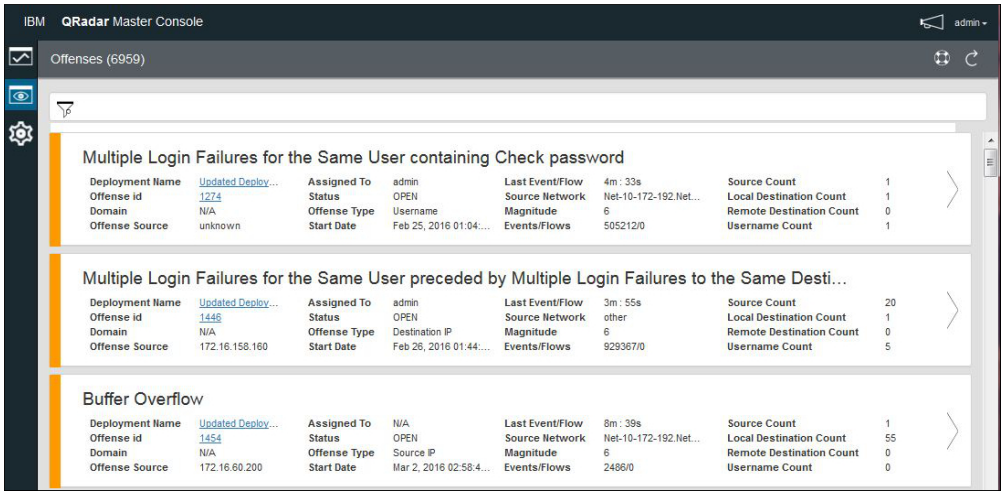

図 *3.* マスター・コンソール内のデプロイメント・カード

オフェンス・カードには以下の情報が表示されます。

表 *3.* オフェンス・カード情報

パラメーター	説明
オフェンス **ID**	オフェンス・サマリーへのリンク。

表 3. オフェンス・カード情報 (続き)

パラメーター	説明
オフェンスの送信元	オフェンス送信元の情報は、オフェンスのタイプに応じて異なります。 例えば、「オフェンスのタイプ」が送信元 IP である場合は、「オフェンスの送信元」フィールドに、オフェンスを作成したイベントの送信元の IP アドレスが表示されます。「オフェンスのタイプ」が宛先 IP である場合は、「オフェンスの送信元」フィールドに、イベントの宛先 IP アドレスが表示されます。
割り当て先	オフェンスを調査するユーザーが割り当てられていない場合は、QRadar でオフェンスをユーザーに割り当てることができます。QRadar へのオフェンスの割り当てについて詳しくは、「*IBM Security QRadar* ユーザーズ・ガイド」を参照してください。
状況 **(Status)**	デフォルトでは、フィルターは、オープン・オフェンスのみを表示します。
オフェンスのタイプ	オフェンスを作成したルールによって決定します。 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関付けします。
開始日 **(Start Date)**	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。
最後のイベント/フロー	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。
送信元ネットワーク	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のネットワークを指定します。
イベント/フロー **(Event/Flow)**	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、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。
送信元数	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。

手順

1. マスター・コンソールを開き、オフェンス  アイコンをクリックします。
2. オフェンス・カードの矢印リンクをクリックしてデプロイメントにログインし、オフェンス・サマリーを開きます。
3. 非表示またはクローズ済みのオフェンスを表示するには、フィルター  アイコンをクリックし、表示するオフェンスのチェック・ボックスを選択します。

適用したフィルターと一致するオフェンスの数がページ・ヘッダーに表示されます。

4. 最新表示アイコンをクリックして、リストされているオフェンスを更新します。

関連タスク:

6 ページの『マスター・コンソールを開く』
マスター・コンソールがインストールされている場合は、QRadar コンソールの IP アドレスを使用してマスター・コンソールを開きます。

オフェンス・リストのフィルタリング

統合オフェンス・リストに表示されたオフェンス・カードをフィルターに掛けるには、検索照会を作成します。例えば、オフェンス・リストをフィルターに掛けて 1 ユーザーに割り当てられたオフェンスのみを表示したり、1 つのデプロイメントのオフェンスのみを表示したりすることができます。

このタスクについて

類似または完全一致のオフェンスを簡単に検索し、ランク順で表示するには、「オフェンス」ビューの全文検索フィールドを使用します。1 単語や単語の一部を検索したり、複数単語を指定の順序または任意の順序で検索する照会を作成できます。オフェンス・カードのすべてのデータ・フィールドにわたってデータを検索することも、検索する ID を指定して検索を絞り込むこともできます。

全文検索機能の基盤は Apache Lucene 検索エンジンです。検索では大文字と小文字が区別されません。1 文字のワイルドカードを使用して検索する際は、? 記号を使用します。複数文字のワイルドカードを使用して検索する際は、* 記号を使用します。

検索するオフェンス・カードのフィールドを指定することによって、検索を絞り込むことができます。オフェンス・カードの各フィールドのフィールド ID を以下の表に示します。

表 *4.* オフェンス・カードのデータを検索するためのフィールド *ID*

オフェンス・カードの説明	フィールド **ID**
オフェンスの説明 **(Offense Description)**	説明
デプロイメント名 **(Deployment name)**	deployment_name
オフェンス **ID**	offense_id
ドメイン	domain_id
オフェンスの送信元	offense_source
割り当て先	assigned_to
状況 **(Status)**	status
オフェンスのタイプ	offense_type `offense_type` での検索にはワイルドカードを使用できません。照会では完全一致テキストを指定する必要があります。
開始日 **(Start date)**	start_time
最後のイベント/フロー	last_updated_time

表 4. オフェンス・カードのデータを検索するためのフィールド ID (続き)

オフェンス・カードの説明	フィールド **ID**
送信元ネットワーク	source_network
マグニチュード	マグニチュード (magnitude)
イベント数/フロー数	event_count flow_count
送信元数	source_count
ローカル宛先の数 **(Local Destination Count)**	local_destination_count
リモート宛先の数 **(Remote Destination Count)**	remote_destination_count
ユーザー名の数 **(Username Count)**	username_count

手順

1. オフェンス  アイコンをクリックします。
2. 検索フィールドに、検索するテキストの検索照会を入力します。
   - オフェンス・カードに表示される任意のデータを検索するには、検索ボックスにそのテキストを入力します。
   - 特定のフィールドのデータを検索するには、フィールド ID を入力し、その後にコロンと検索語を入力します。
   - 次の特殊文字をエスケープするには、検索照会のそれらの文字の前で ¥ を使用します。

     `+ - && || ! ( ) { } [ ] ^ " ~ * ? : \`

   検索照会の例:

   オフェンス・カードのデータを検索する際に使用できる照会の例を以下の表に示します。

表 5. マスター・コンソールの検索式

説明	検索照会
任意のフィールドに `text` または `test` があるオフェンスを検索する。	`te?t`
`test`、`tests`、または `tester` があるオフェンスを検索する。	`test*`
任意のフィールドに `password` があるオフェンスを検索する。	`*password*`
マグニチュードの評価が 2、3、または 4 であるオフェンスを検索する。	`magnitude:[2 to 4]`
マグニチュードの評価が 3 または 5 であるオフェンスを検索する。	`magnitude:(3 OR 5)`
「オフェンスのタイプ」が「**イベント名**」に等しいオフェンスを検索する。	`offense_type: "Event Name"`

表 5. マスター・コンソールの検索式 (続き)

説明	検索照会
過去 10 日以内に更新されたオフェンスを検索する。	`last_update_time:[NOW-10DAYS to NOW]`
マグニチュードが 3 である Bishop デプロイメントのオフェンスを検索する。	`deployment_name:Bishop AND magnitude:3`

3. 非表示またはクローズ済みのオフェンスを表示するには、フィルター  アイコンをクリックし、表示するオフェンスのチェック・ボックスを選択します。

   適用したフィルターと一致するオフェンスの数がページ・ヘッダーに表示されます。

ユーザー管理

マスター・コンソールで直接、マスター・コンソール・ユーザーが管理されます。

初めてマスター・コンソール V0.8.1 以降に更新するときは、更新中に QRadar コンソールからユーザーがインポートされます。インポート処理は 1 回しか行われません。以降は、マスター・コンソールを更新してもユーザーはインポートされません。初回インポートの後は、マスター・コンソールから直接、すべてのユーザー・アカウントが管理されます。

ローカル・ユーザーの追加

マスター・コンソールをインストールして最新のバージョンに更新した後は、管理者が直接マスター・コンソールで新規ユーザーを追加します。

手順

1. 設定  アイコンをクリックします。
2. 「ユーザー管理」をクリックします。
3. 「ユーザー管理」ウィンドウの右上隅にある追加 (+) アイコンをクリックし、「ユーザーの作成 (Create user)」ウィンドウを開きます。
4. 新規ユーザーの情報を入力します。
5. 新規ユーザーが管理者である場合は、「セキュリティー管理者 **(Security Admin)**」チェック・ボックスをクリックします。
6. 「ユーザーの作成 **(Create User)**」をクリックします。

ユーザー設定の編集

マスター・コンソールでローカル・ユーザーの設定 (ユーザー・パスワードなど) を変更します。

このタスクについて

IBM Security QRadar でのローカル・ユーザー・パスワードの変更が、自動的にマスター・コンソールに適用されることはありません。マスター・コンソールで、ユーザー設定を編集して、パスワードを変更する必要があります。

マスター・コンソール内で LDAP パスワードおよび Active Directory パスワードを変更することはできません。

手順

1. 設定  アイコンをクリックします。
2. 「ユーザー管理」をクリックします。
3. 編集するユーザーのカードで、右上隅にある 3 本線のメニュー  アイコンをクリックします。
4. 「ユーザーの編集 **(Edit User)**」を選択します。
5. 「ユーザーの編集 (Edit User)」ウィンドウでユーザー情報を変更します。
6. 「ユーザーの編集 **(Edit User)**」をクリックして変更を保存します。

ローカル・ユーザーの削除

ユーザーがアクセスする必要がなくなった場合は、マスター・コンソールからそのローカル・ユーザーを削除します。

手順

1. 設定  アイコンをクリックします。
2. 「ユーザー管理」をクリックして、すべてのローカル・ユーザーのカードを表示します。
3. 編集するユーザーのカードで、右上隅にある 3 本線のメニュー  アイコンをクリックします。
4. 「ユーザーの削除 **(Remove User)**」を選択します。
5. 確認ウィンドウで「ユーザーの削除 **(Remove User)**」をクリックします。

ユーザー・リストのフィルタリング

「ユーザー管理」ページに表示されるマスター・コンソール・ユーザーのリストをフィルターに掛けるには、検索照会を作成します。例えば、ユーザー・リストをフィルターに掛けてアクティブなユーザーのみを表示したり、「管理者」セキュリティー・プロファイルを使用するユーザーのみを表示したりすることができます。

このタスクについて

検索条件に類似または完全一致のユーザーを簡単に検索するには、「ユーザー管理」ページで全文検索フィールドを使用します。全文検索機能の基盤は Apache Lucene 検索エンジンです。1 文字のワイルドカードを使用して検索する際は、疑問

符 (?) を使用します。複数文字のワイルドカードを使用して検索する際は、アスタリスク (*) を使用します。検索するユーザー・フィールドを指定することによって、検索を絞り込むことができます。

手順

1. 設定  アイコンをクリックします。
2. 「ユーザー管理」をクリックします。
3. 検索フィールドに、検索するテキストの検索照会を入力します。
   - フリー・フォーム・テキストを検索するには、検索ボックスにそのテキストを入力します。フリー・フォームの検索では、完全なワードを使用する必要があります。部分的なワードもワイルドカードも使用できません。
   - 特定のフィールドのデータを検索するには、フィールド ID を入力し、その後にコロンと検索語を入力します。

   検索照会の例:

   ユーザー・データを検索する際に使用できる照会の例を以下の表に示します。

表 6. ユーザー・データの検索式

説明	検索ストリング
「ユーザー名」フィールドのテキストの検索。	`name:John`
固有のログイン名の検索。このフィールドの検索では、大/小文字が区別されます。	`login:Coop1`
E メール・アドレスの検索。 完全な E メール・アドレスを指定する必要があります。部分的な E メール・アドレスは検索できません。	`email:coop1@ca.ibm.com`
システムで現在アクティブなユーザーの検索。	`status:ACTIVE`
管理特権を持つすべてのユーザーの検索。	`role_name:admin`
過去 14 日間にプロファイルが修正されたユーザーの検索。	`last_modified:[NOW-14DAYS TO NOW]`

マスター・コンソールでの Active Directory 認証および LDAP 認証の構成

Microsoft Active Directory 認証プロバイダーまたは LDAP 認証プロバイダーを初めて構成するには、`/opt/qradar/masterconsole/conf/shiro.realms` ファイルにレルム情報を追加する必要があります。

最近、マスター・コンソール V0.10.0 にアップグレードした場合は、`shiro.ini` バックアップ・ファイルから `/opt/qradar/masterconsole/conf/shiro.realms` ファイルにレルム情報を手動でコピーする必要があります。レルム情報は、将来のマスター・コンソールへのアップグレードで保持されます。

始める前に

shiro.ini.<timestamp> バックアップ・ファイルが /opt/qradar/masterconsole/conf/ ディレクトリーに存在することを確認してください。バックアップ・ファイルが存在しない場合は、新規に作成してください。

ご使用の認証サーバーで構成を確認します。構成する認証プロバイダーのタイプに応じて、以下のパラメーター値を指定する必要がある場合があります。

表 7. 認証パラメーターの説明

パラメーター	説明
searchBase	ユーザーが編成される Active Directory または LDAP ディレクトリーのルート。
searchFilter	Active Directory ユーザーまたは LDAP ユーザーのコンテキストを見つけるために使用されます。アカウントは、ほとんどのサーバーで使用されるデフォルトのオブジェクト・クラスですが、このエントリーは Active Directory サーバーまたは LDAP サーバーの構成によって異なります。
groupAttribute	Active Directory ユーザーまたは LDAP ユーザーが属しているユーザー・グループを識別します。
groupRolesMap	Active Directory グループまたは LDAP グループと Apache Shiro ロールのマップ。
userDnTemplate	Active Directory サーバーまたは LDAP サーバーからユーザーを取得する DN テンプレート。
contextFactory.url	Active Directory サーバーまたは LDAP サーバーの IP アドレスおよびポート番号。
principalSuffix	ユーザーによる指定が必要なログオン情報を単純化するプリンシパル接尾部を指定します。 例えば username@this.is.my.long.domain.name.in.canada.com の代わりに canada というユーザー・プリンシパル接尾部を作成すると、ユーザーが username@canada と入力できます。

手順

1. /opt/qradar/masterconsole/conf ディレクトリーに移動します。
2. shiro.realms ファイルのコピーを作成します。

   ```
   cp shiro.realms.default shiro.realms
   ```

3. shiro.realms ファイルを開きます。
4. Microsoft Active Directory を構成するには、以下の手順を実行します。
   a. 以下のセクションを検索して、サンプル値を認証環境に応じた値で置き換えます。

   ```
   # ----------------------------------------------------------------------------
   # following section is for configuring ActiveDirectory realm. Replace example
   # values before add to securityManager.realm
   # ----------------------------------------------------------------------------
   adRealm = org.apache.shiro.realm.activedirectory.ActiveDirectoryRealm
   adRealm.url = ldap://{ad_server}:389
   adRealm.groupRolesMap = "CN=the_users,CN=Users,DC=department,DC=company,DC=com":"admin"
   ```

```
adRealm.searchBase = "DC=department,DC=company,DC=com"
adRealm.systemUsername= user_name
adRealm.systemPassword= password
adRealm.principalSuffix= @company.com
```

b. $adRealm を securityManager.realms 項目に追加します。

```
securityManager.realms = $localRealm, $adRealm
```

5. LDAP を構成するには、以下の手順を実行します。

a. 以下のセクションを検索して、サンプル値を認証環境に応じた値で置き換えます。

```
#-----------------------------------------------------------------------------
# following section is for configuring OpenLdap realm. Replace example
# values before add to securityManager.realm
#-----------------------------------------------------------------------------
ldapRealm = com.ibm.si.mc.security.shiro.realm.LdapRealm
ldapRealm.searchBase = "dc=company,dc=com"
ldapRealm.searchFilter = (&(objectClass=account)(uid={0}))
ldapRealm.groupAttribute = ou
ldapRealm.groupRolesMap = "Manager":"admin"
ldapRealm.userDnTemplate = uid={0},dc=company,dc=com
ldapRealm.contextFactory.url = ldap://{ldap_server}:389
```

b. $ldapRealm を securityManager.realms 項目に追加します。

```
securityManager.realms = $localRealm, $ldapRealm
```

6. /opt/qradar/masterconsole/conf/shiro.realms ファイルを保存します。
7. 以下のコマンドを入力して、shiro.ini ファイルにレルム情報を追加します。

```
/opt/qradar/masterconsole/bin/generateShiroIni.py
```

8. 以下のコマンドを使用して、tomcat サーバーを再始動します。

```
service tomcat restart
```

次のタスク

Microsoft Active Directory 認証または LDAP 認証を使用してマスター・コンソールにログインすることで、構成をテストします。

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。

プライバシー・ポリシーに関する考慮事項

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

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

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

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

product-privacy) を参照してください。

Printed in Japan

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