Red Hat Advanced Cluster Management for Kubernetes 2.6

アクセス制御

ロールベースのアクセス制御と認証の詳細

Last Updated: 2023-11-01

Red Hat Advanced Cluster Management for Kubernetes 2.6 アクセス制御

ロールベースのアクセス制御と認証の詳細

法律上の通知

概要

ロールベースのアクセス制御と認証の詳細について説明しています。

目次

第1章 アクセス制御

手動によるアクセス制御の作成および管理が必要になる場合もあります。IAM (Identity and Access Management) にワークロードをオンボードするには、Red Hat Advanced Cluster Management for Kubernetes の **認証** サービス要件を設定する必要があります。詳細は、OpenShift Container Platform ドキュメントの 認証について の **認証について** を参照してください。

ロールベースのアクセス制御および認証では、ユーザーに関連付けられたロールおよび認証情報を識別します。アクセスと認証情報の詳細は、以下のファイルを参照してください。

必要なアクセス権限: クラスターの管理者

- ロールベースのアクセス制御

1.1. ロールベースのアクセス制御

Red Hat Advanced Cluster Management for Kubernetes は、ロールベースのアクセス制御 (RBAC) に対応しています。ロールによって実行できるアクションが決まります。RBAC は、Red Hat OpenShift Container Platform と同様に Kubernetes の認可メカニズムに基づいています。RBAC の詳細は、OpenShift Container Platform ドキュメント の **RBAC** の概要を参照してください。

注記: ユーザーロールのアクセス権がない場合には、コンソールのアクションボタンが無効になります。

コンポーネントでサポートされる RBAC の詳細は、以下のセクションを参照してください。

- ロールの概要
- RBAC 実装
- クラスターライフサイクル RBAC
- アプリケーションライフサイクル RBAC
- ガバナンスライフサイクル RBAC
- 可観測性の RBAC

1.1.1. ロールの概要

クラスター別の製品リソースと、スコープに namespace が指定されている製品リソースがあります。アクセス制御に一貫性を持たせるため、クラスターのロールバインディングと、namespace のロールバインディングをユーザーに適用する必要があります。Red Hat Advanced Cluster Management for Kubernetes でサポートされている以下のロール定義の表を参照してください。

表1.1 ロール定義の表

ロール	定義
cluster-admin	これは OpenShift Container Platform のデフォルトのロールです。**cluster-admin** ロールへのクラスターバインディングがあるユーザーは、すべてのアクセス権限を持つ OpenShift Container Platform のスーパーユーザーです。

open-cluster-management:cluster-manager-admin	**open-cluster-management:cluster-manager-admin** ロールへのクラスターバインディングがあるユーザーは、すべてのアクセス権限を持つ Red Hat Advanced Cluster Management for Kubernetes のスーパーユーザーです。このロールを指定すると、ユーザーは **ManagedCluster** リソースを作成できます。
open-cluster-management:admin:<managed_cluster_name>	**open-cluster-management:admin:<managed_cluster_name>** ロールへのクラスターバインディングがあるユーザーには、**managedcluster-<managed_cluster_name>** という名前の **ManagedCluster** リソースに管理者アクセス権が付与されます。ユーザーにマネージドクラスターがある場合は、このロールが自動的に作成されます。
open-cluster-management:view:<managed_cluster_name>	**open-cluster-management:view:<managed_cluster_name>** ロールへのクラスターバインディングがあるユーザーには、**managedcluster-<managed_cluster_name>** という名前の **ManagedCluster** リソースの表示権限が付与されます。
open-cluster-management:managedclusterset:admin:<managed_clusterset_name>	**open-cluster-management:managedclusterset:admin:<managed_clusterset_name>** ロールへのクラスターバインディングがあるユーザーには、**<managed_clusterset_name>** という名前の **ManagedCluster** リソースの管理者アクセス権が付与されます。また、ユーザーには **managedcluster.cluster.open-cluster-management.io**、**clusterclaim.hive.openshift.io**、**clusterdeployment.hive.openshift.io** および **clusterpool.hive.openshift.io** リソースへの管理者アクセス権があります。これには、**cluster.open-cluster-management.io/clusterset=<managed_clusterset_name>** のマネージドクラスターセットのラベルが付いています。ロールバインドは、クラスターセットの使用時に自動的に生成されます。リソースの管理方法については、ManagedClusterSets の作成および管理 を参照してください。

open-cluster-management:managedclusterset:view:<managed_clusterset_name>	**open-cluster-management:managedclusterset:view:<managed_clusterset_name>** ロールへのクラスターバインディングがあるユーザーには、<managed_clusterset_name>` という名前の **ManagedCluster** リソースへの表示権限が付与されます。また、ユーザーには **managedcluster.cluster.open-cluster-management.io**、**clusterclaim.hive.openshift.io**、**clusterdeployment.hive.openshift.io** および **clusterpool.hive.openshift.io** リソースへの表示権限があり、**cluster.open-cluster-management.io**、**clusterset=<managed_clusterset_name>** のマネージドクラスターセットのラベルが付いています。マネージドクラスターセットの管理方法の詳細は、ManagedClusterSets の作成および管理 を参照してください。
open-cluster-management:subscription-admin	**open-cluster-management:subscription-admin** ロールが割り当てられたユーザーは、Git サブスクリプションを作成して、リソースを複数の namespace にデプロイできます。リソースは、サブスクライブされた Git リポジトリーの Kubernetes リソース YAML ファイルで指定されます。**注記:** non-subscription-admin ユーザーがサブスクリプションを作成すると、リソースに指定された namespace に関係なく、すべてのリソースがサブスクリプションの namespace にデプロイされます。詳細は、アプリケーションライフサイクル RBAC セクションを参照してください。
admin、edit、view	admin、edit、および view は OpenShift Container Platform のデフォルトロールです。これらのロールに対して namespace に限定されたバインディングが指定されているユーザーは、特定の namespace 内の **open-cluster-management** リソースにアクセスでき、同じロールに対してクラスター全体のバインディングが指定されている場合は、クラスター全体の全 **open-cluster-management** リソースにアクセスできます。

open-cluster-management:managedclusterset:bind:<managed_clusterset_name>	**open-cluster-management:managedclusterset:bind:<managed_clusterset_name>** ロールが割り当てられたユーザーには、**<managed_clusterset_name>** というマネージドクラスターリソースの表示権限が付与されます。ユーザーは **<managed_clusterset_name>** を namespace にバインドできます。また、ユーザーには **managedcluster.cluster.open-cluster-management.io**、**clusterclaim.hive.openshift.io**、**clusterdeployment.hive.openshift.io** および **clusterpool.hive.openshift.io** リソースへの表示権限があり、**cluster.open-cluster-management.io/clusterset=<managed_clusterset_name>** のマネージドクラスターセットのラベルが付いています。リソースの管理方法については、ManagedClusterSets の作成および管理 を参照してください。

重要:

- ユーザーは OpenShift Container Platform からプロジェクトを作成できます。これにより、namespace の管理者ロール権限が付与されます。
- ユーザーにクラスターへのロールアクセスがない場合、クラスター名は表示されません。クラスター名は、**-** の記号で表示されます。

1.1.2. RBAC 実装

RBAC はコンソールレベルと API レベルで検証されます。コンソール内のアクションは、ユーザーのアクセスロールの権限に基づいて有効化/無効化できます。製品の特定ライフサイクルの RBAC の詳細は、以下のセクションを参照してください。

1.1.2.1. クラスターライフサイクル RBAC

以下のクラスターライフサイクル RBAC 操作を確認してください。

- 全マネージドクラスターを作成して管理するには、以下を行います。
  - 以下のコマンドを入力して、クラスターロール **open-cluster-management:cluster-manager-admin** にバインドするクラスターロールを作成します。

    ```
    oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:cluster-manager-admin --user=<username>
    ```

    このロールはスーパーユーザーであるため、すべてのリソースとアクションにアクセスできます。このロールを使用すると、クラスターレベルの **managedcluster** リソース、マネージドクラスターを管理するリソースの namespace、namespace 内のリソースを作成できます。また、このロールで、プロバイダー接続、マネージドクラスター作成に使用するベアメタルアセットにアクセスできます。権限エラーを回避するために、ロールの関連付けが必要な ID の **username** を追加する必要がある場合があります。
- **cluster-name** という名前のマネージドクラスターを管理する方法:
  - 以下のコマンドを入力して、クラスターロール **open-cluster-management:admin:**

<cluster-name> にバインドするクラスターロールを作成します。

```
oc create clusterrolebinding (role-binding-name) --clusterrole=open-cluster-management:admin:<cluster-name> --user=<username>
```

このロールを使用すると、クラスターレベルの **managedcluster** リソースに読み取り/書き込みアクセスができるようになります。**managedcluster** はクラスターレベルのリソースで、namespace レベルのリソースではないので、このロールが必要です。

- 以下のコマンドを入力して、クラスターロール **admin** にバインドする namespace ロールを作成します。

```
oc create rolebinding <role-binding-name> -n <cluster-name> --clusterrole=admin --user=<username>
```

このロールでは、マネージドクラスターの namespace 内にあるリソースに対して読み取り/書き込みアクセスができるようになります。

- **cluster-name** という名前のマネージドクラスターを表示するには、以下を行います。
  - 以下のコマンドを入力して、クラスターロール **open-cluster-management:view:<cluster-name>** にバインドするクラスターロールを作成します。

```
oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:view:<cluster-name> --user=<username>
```

このロールを使用すると、クラスターレベルの **managedcluster** リソースに読み取りアクセスができるようになります。**managedcluster** はクラスターレベルのリソースで、namespace レベルのリソースではないので、このロールが必要です。

  - 以下のコマンドを入力して、クラスターロール **view** にバインドする namespace ロールを作成します。

```
oc create rolebinding <role-binding-name> -n <cluster-name> --clusterrole=view --user=<username>
```

このロールでは、マネージドクラスターの namespace 内にあるリソースに対して読み取り専用アクセスができるようになります。

- 以下のコマンドを入力して、アクセス可能なマネージドクラスターの一覧を表示します。

```
oc get managedclusters.clusterview.open-cluster-management.io
```

このコマンドは、クラスター管理者権限なしで、管理者およびユーザーが使用できます。

- 以下のコマンドを入力して、アクセス可能なマネージドクラスターセットの一覧を表示します。

```
oc get managedclustersets.clusterview.open-cluster-management.io
```

このコマンドは、クラスター管理者権限なしで、管理者およびユーザーが使用できます。

1.1.2.1.1. クラスタープール RBAC

以下のクラスタープール RBAC 操作を確認してください。

- クラスタープールのプロビジョニングクラスターを使用するには、以下を実行します。
  - クラスター管理者は、グループにロールを追加してマネージドクラスターセットを作成し、管理者権限をロールに付与します。
    - 以下のコマンドを使用して、**server-foundation-clusterset** マネージドクラスターセットに **admin** パーミッションを付与します。

      ```
      oc adm policy add-cluster-role-to-group open-cluster-management:clusterset-admin:server-foundation-clusterset
      server-foundation-team-admin
      ```

    - 以下のコマンドを使用して、**server-foundation-clusterset** マネージドクラスターセットに **view** 権限を付与します。

      ```
      oc adm policy add-cluster-role-to-group open-cluster-management:clusterset-view:server-foundation-clusterset server-foundation-team-user
      ```

  - クラスタープールの namespace (**server-foundation-clusterpool**) を作成します。
    - 以下のコマンドを実行して、**server-foundation-team-admin** の **server-foundation-clusterpool** に **admin** 権限を付与します。

      ```
      oc adm new-project server-foundation-clusterpool

      oc adm policy add-role-to-group admin server-foundation-team-admin --namespace server-foundation-clusterpool
      ```

  - チーム管理者として、クラスタープール namespace に、クラスターセットラベル **cluster.open-cluster-management.io/clusterset=server-foundation-clusterset** を使用して **ocp46-aws-clusterpool** という名前のクラスタープールを作成します。
    - **server-foundation-webhook** は、クラスタープールにクラスターセットラベルがあるかどうか、またユーザーにクラスターセットのクラスタープールを作成するパーミッションがあるかどうかを確認します。
    - **server-foundation-controller** は、**server-foundation-team-user** の **server-foundation-clusterpool** namespace に **view** 権限を付与します。
  - クラスタープールが作成されると、クラスタープールは **clusterdeployment** を作成します。
    - **server-foundation-controller** は、**server-foundation-team-admin** の **clusterdeployment** namespace に **admin** パーミッションを付与します。
    - **server-foundation-controller** は、**server-foundation-team-user** の **clusterdeployment** namespace に **view** パーミッションを付与します。
      注記: **team-admin** および **team-user** は、**clusterpool**、**clusterdeplyment** および **clusterclaim** への **admin** 権限があります。

クラスターライフサイクルの以下のコンソールおよび API RBAC の表を表示します。

表1.2 クラスターライフサイクルのコンソール RBAC の表

リソース	管理	編集	表示
クラスター	read, update, delete	-	read
クラスターセット	get, update, bind, join	編集ロールなし	get
マネージドクラスター	read, update, delete	編集ロールなし	get
プロバイダー接続	create, read, update, delete	-	read
ベアメタルアセット	create, read, update, delete	-	read

表1.3 クラスターライフサイクルの API RBAC の表

API	管理	編集	表示
managedclusters.cluster.open-cluster-management.io **この API のコマンドでは、mcl (単数) または mcls (複数) を使用できます。**	create, read, update, delete	read, update	read
managedclusters.view.open-cluster-management.io **この API のコマンドでは、mcv (単数) または mcvs (複数) を使用できます。**	read	read	read
managedclusters.register.open-cluster-management.io/accept	update	update	
managedclusterset.cluster.open-cluster-management.io **この API のコマンドでは、mclset (単数) または mclsets (複数) を使用できます。**	create, read, update, delete	read, update	read

API	管理	編集	表示
managedclustersets.view.open-cluster-management.io	read	read	read
managedclustersetbinding.cluster.open-cluster-management.io **この API のコマンドでは、mclsetbinding (単数) または mclsetbindings (複数) を使用できます。**	create, read, update, delete	read, update	read
baremetalassets.inventory.open-cluster-management.io	create, read, update, delete	read, update	read
klusterletaddonconfigs.agent.open-cluster-management.io	create, read, update, delete	read, update	read
managedclusteractions.action.open-cluster-management.io	create, read, update, delete	read, update	read
managedclusterviews.view.open-cluster-management.io	create, read, update, delete	read, update	read
managedclusterinfos.internal.open-cluster-management.io	create, read, update, delete	read, update	read
manifestworks.work.open-cluster-management.io	create, read, update, delete	read, update	read
submarinerconfigs.submarineraddon.open-cluster-management.io	create, read, update, delete	read, update	read

API	管理	編集	表示
placements.cluster.open-cluster-management.io	create, read, update, delete	read, update	read

1.1.2.2. 認証情報ロールベースのアクセス制御

認証情報へのアクセスは Kubernetes で制御されます。認証情報は Kubernetes Secret として保存され、セキュリティーを確保します。以下の権限は、Red Hat Advanced Cluster Management for Kubernetes のシークレットのアクセスに関係します。

- namespace でシークレットの作成権限のあるユーザーは認証情報を作成できます。
- namespace でシークレットの読み取り権限のあるユーザーは、認証情報を表示することもできます。
- Kubernetes ロール **admin** および **edit** のあるユーザーは、シークレットの作成と編集が可能です。
- Kubernetes クラスターロール **view** のあるユーザーは、シークレットの内容を読み取ると、サービスアカウントの認証情報にアクセスできるようになるため、シークレットを表示できません。

1.1.2.3. アプリケーションライフサイクル RBAC

アプリケーションの作成時に、**subscription** namespace が作成され、configuration map が **subscription** namespace に作成されます。**channel** namespace へのアクセス権も必要です。サブスクリプションを適用する場合は、サブスクリプションの管理者である必要があります。アプリケーションの管理の詳細は、サブスクリプション管理者としての許可および拒否リストの作成 を参照してください。

以下のアプリケーションライフサイクル RBAC 操作を確認してください。

- **username** という名前のユーザーで、すべてのマネージドクラスターでアプリケーションを作成して管理するには、以下を実行します。
  - 以下のコマンドを実行して、**open-cluster-management:cluster-manager-admin** クラスターロールへのクラスターロールのバインディングを作成して、 **username** にバインドします。

    ```
    oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:cluster-manager-admin --user=<username>
    ```

    このロールはスーパーユーザーであるため、すべてのリソースとアクションにアクセスできます。このロールを使用して、アプリケーションの namespace および namespace 内のすべてのアプリケーションリソースを作成できます。
- **オプション**: 複数の namespace にリソースをデプロイするアプリケーションを作成できます。
  - **open-cluster-management:subscription-admin** クラスターロールにバインドするクラスターロールを作成し、これを **username** という名前のユーザーにバインドします。以下のコマンドを実行します。

```
oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:subscription-admin --user=<username>
```

- **username** ユーザーで **cluster-name** マネージドクラスターに **application-name** という名前のアプリケーションを作成し、管理するには、以下を実行します。
  - 以下のコマンドを入力して、**open-cluster-management:admin:** クラスターロールへのバインドを作成し、**username** にバインドします。

    ```
    oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:admin:<cluster-name> --user=<username>
    ```

    このロールには、マネージドクラスター **cluster-name** のすべての **application** リソースへの読み取りおよび書き込みアクセスがあります。他のマネージドクラスターへのアクセスが必要な場合は、この操作を繰り返します。

  - 以下のコマンドを入力し、**admin** ロールを使用して **application** namespace にバインドする namespace ロールを作成し、それを **username** にバインドします。

    ```
    oc create rolebinding <role-binding-name> -n <application-namespace> --clusterrole=admin --user=<username>
    ```

    このロールには、**application** namspace のすべての **application** リソースに対する読み取りおよび書き込み権限があります。他のアプリケーションへのアクセスが必要な場合や、アプリケーションが複数の namespace にデプロイされる場合は、これを繰り返します。

- **オプション**: 複数の namespace にリソースをデプロイするアプリケーションを作成できます。
  - 以下のコマンドを入力して、open-cluster-management:subscription-admin クラスターロールへのクラスターロールのバインディングを作成し、**username** にバインドします。

    ```
    oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:subscription-admin --user=<username>
    ```

- **username** という名前のユーザーが **cluster-name** という名前のマネージドクラスターでアプリケーションを表示するには、以下を実行します。
  - 以下のコマンドを入力して、**open-cluster-management:view:** クラスターロールにバインドするクラスターロールを作成し、これを **username** にバインドします。

    ```
    oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:view:<cluster-name> --user=<username>
    ```

    このロールは、マネージドクラスター **cluster-name** のすべての **application** リソースへの読み取りアクセスがあります。他のマネージドクラスターへのアクセスが必要な場合は、この操作を繰り返します。

  - **view** ロールを使用して **application** namespace にバインドする namespace ロールを作成し、それを **username** にバインドします。以下のコマンドを入力します。

    ```
    oc create rolebinding <role-binding-name> -n <application-namespace> --clusterrole=view --user=<username>
    ```

このロールには、**application** の namspace にあるすべての **application** リソースに対する読み取り権限があります。他のアプリケーションへのアクセスが必要な場合は、この操作を繰り返します。

アプリケーションライフサイクルの以下のコンソールおよび API RBAC の表を表示します。

表1.4 アプリケーションライフサイクルのコンソール RBAC の表

リソース	管理	編集	表示
アプリケーション	create, read, update, delete	create, read, update, delete	read
チャネル	create, read, update, delete	create, read, update, delete	read
サブスクリプション	create, read, update, delete	create, read, update, delete	read
配置ルール	create, read, update, delete	create, read, update, delete	read

表1.5 アプリケーションライフサイクルの API RBAC の表

API	管理	編集	表示
applications.app.k8s.io	create, read, update, delete	create, read, update, delete	read
channels.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
deployables.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
helmreleases.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
placements.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
placementrules.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
subscriptions.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
configmaps	create, read, update, delete	create, read, update, delete	read

API	管理	編集	表示
secrets	create, read, update, delete	create, read, update, delete	read
namespace	create, read, update, delete	create, read, update, delete	read

1.1.2.4. ガバナンスライフサイクル RBAC

ポリシーが作成されると、ポリシーはクラスターに作成されます。ガバナンスライフサイクルのロールは namespace-scoped です。ユーザーは、マネージドクラスターへのアクセス権も必要です。

ユーザーは、ガバナンスライフサイクル操作を実行するには、ポリシーが作成される namespace、およびポリシーが適用されるマネージドクラスターへのアクセス権が必要です。

以下の例を参照してください。

- **policy** namespace でポリシーを作成し、これを **cluster-name** という名前のマネージドクラスターに適用するには、以下を実行します。
  - **open-cluster-management:admin:<cluster-name> クラスターロールを使用して、policy namespace に** バインドする namespace ロールを作成します。以下のコマンドを実行します。

    ```
    oc create rolebinding <role-binding-name> -n <policy-namespace> --clusterrole=open-cluster-management:admin:<cluster-name> --user=<username>
    ```

- マネージドクラスターでポリシーを表示するには、以下を実行します。
  - **open-cluster-management:view:<cluster-name> クラスター** ロールにバインドするクラスターロールを作成し、次のコマンドを使用して **view** ロールにバインドします。

    ```
    oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:view:<cluster-name> --user=<username>
    ```

以下は、ガバナンスライフサイクルのコンソールおよび API RBAC の表です。

表1.6 ガバナンスライフサイクルのコンソール RBAC の表

リソース	管理	編集	表示
ポリシー	create, read, update, delete	read, update	read
PlacementBindings	create, read, update, delete	read, update	read
Placements	create, read, update, delete	read, update	read

リソース	管理	編集	表示
PlacementRules	create, read, update, delete	read, update	read
PolicyAutomations	create, read, update, delete	read, update	read

表1.7 ガバナンスライフサイクルの API RBAC の表

API	管理	編集	表示
policies.policy.open-cluster-management.io	create, read, update, delete	read, update	read
placementbindings.policy.open-cluster-management.io	create, read, update, delete	read, update	read
policyautomations.policy.open-cluster-management.io	create, read, update, delete	read, update	read

1.1.2.5. 可観測性の RBAC

マネージドクラスターの可観測性メトリクスを表示するには、ハブクラスター上のそのマネージドクラスターに対する **view** 権限が必要です。以下の可観測性機能のリストを参照してください。

- マネージドクラスターのメトリクスへのアクセス
  ユーザーがハブクラスター上のマネージドクラスターの **view** ロールに割り当てられていない場合、ユーザーはマネージドクラスターメトリックへのアクセスを拒否されます。

- リソースの検索

Grafana で可観測性データを表示するには、マネージドクラスターの同じ namespace に **RoleBinding** リソースが必要です。以下は **RoleBinding** の例です。

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
 name: <replace-with-name-of-rolebinding>
 namespace: <replace-with-name-of-managedcluster-namespace>
subjects:
 - kind: <replace with User|Group|ServiceAccount>
   apiGroup: rbac.authorization.k8s.io
   name: <replace with name of User|Group|ServiceAccount>
roleRef:
 apiGroup: rbac.authorization.k8s.io
 kind: ClusterRole
 name: view
```

詳細は、ロールバインディングポリシー を参照してください。可観測性を設定するには、可観測性のカスタマイズ を参照してください。

可観測性のコンポーネントを管理するには、以下の API RBAC の表を確認します。

表1.8 可観測性の API RBAC の表

API	管理	編集	表示
multiclusterobservabilities.observability.open-cluster-management.io	create, read, update, delete	read, update	read
searchcustomizations.search.open-cluster-management.io	create、get、list、watch、update、delete、patch	-	-
policyreports.wgpolicyk8s.io	get, list, watch	get, list, watch	get, list, watch

クラスターのセキュリティー保護に関する詳細の確認を続行するには、リスクおよびコンプライアンス を参照してください。