# Oracle® Key Manager

# セキュリティーガイド

**バージョン 2.5**

**E25341-02**

**2011 年 10 月**

Oracle Key Manager セキュリティーガイド バージョン 2.5

E25341-02



主著者: OKM 開発チーム

# 目次

# パート 1: 概要

この節では、製品の概要とアプリケーションのセキュリティーの一般的な原則について説明します。

## 製品概要

Oracle Key Manager (OKM) は暗号化鍵の作成、保存、および管理を行います。次のコンポーネントで構成されています。

- 鍵管理アプライアンス (KMA) – ポリシーに基づくライフサイクル鍵管理、認証、アクセス制御、および鍵プロビジョニングサービスを提供する、セキュリティー強化された機器です。KMA は、ストレージネットワークの信頼できる認証局として、すべてのストレージデバイスが登録され認証されていること、およびすべての暗号化鍵の作成、プロビジョニング、削除が規定されたポリシーに従っていることを確認します。

- Oracle Key Manager GUI – ワークステーション上で実行され、IP ネットワーク経由で KMA と通信して OKM の構成と管理を行う、グラフィカルユーザーインタフェースです。Oracle Key Manager GUI は、お客様が用意するワークステーションにインストールする必要があります。

- Oracle Key Manager CLI – ワークステーション上で実行され、IP ネットワーク経由で KMA と通信して一般的な管理操作を自動化する、2 つのコマンド行インタフェースです。Oracle Key Manager CLI は、お客様が用意するワークステーションにインストールする必要があります。

- OKM クラスタ - システム内にあるすべての KMA の集まりです。これらのすべての KMA は相互に認識し、情報を相互に複製します。

- エージェント - OKM クラスタによって管理されている鍵を使用して暗号化を実行する、デバイスまたはソフトウェアです。StorageTek の暗号化テープドライブはエージェントの一例です。エージェントは KMS Agent Protocol を介して KMA と通信します。Agent API は、エージェントのハードウェアまたはソフトウェアに組み込まれた一連のソフトウェアインタフェースです。

OKM は KMA、エージェント、および Oracle Key Manager GUI と CLI が実行されているワークステーションの間の接続に TCP/IP ネットワークを使用します。柔軟性の高いネットワーク接続を提供するために、各 KMA のネットワーク接続に次の 3 つのインタフェースが提供されています。

- 管理接続 - お客様のネットワークへの接続に使用されます
- サービス接続 - エージェントへの接続に使用されます
- ILOM/ELOM 接続 - KMA の ILOM または ELOM への接続に使用されます

次の図の例を参照してください。

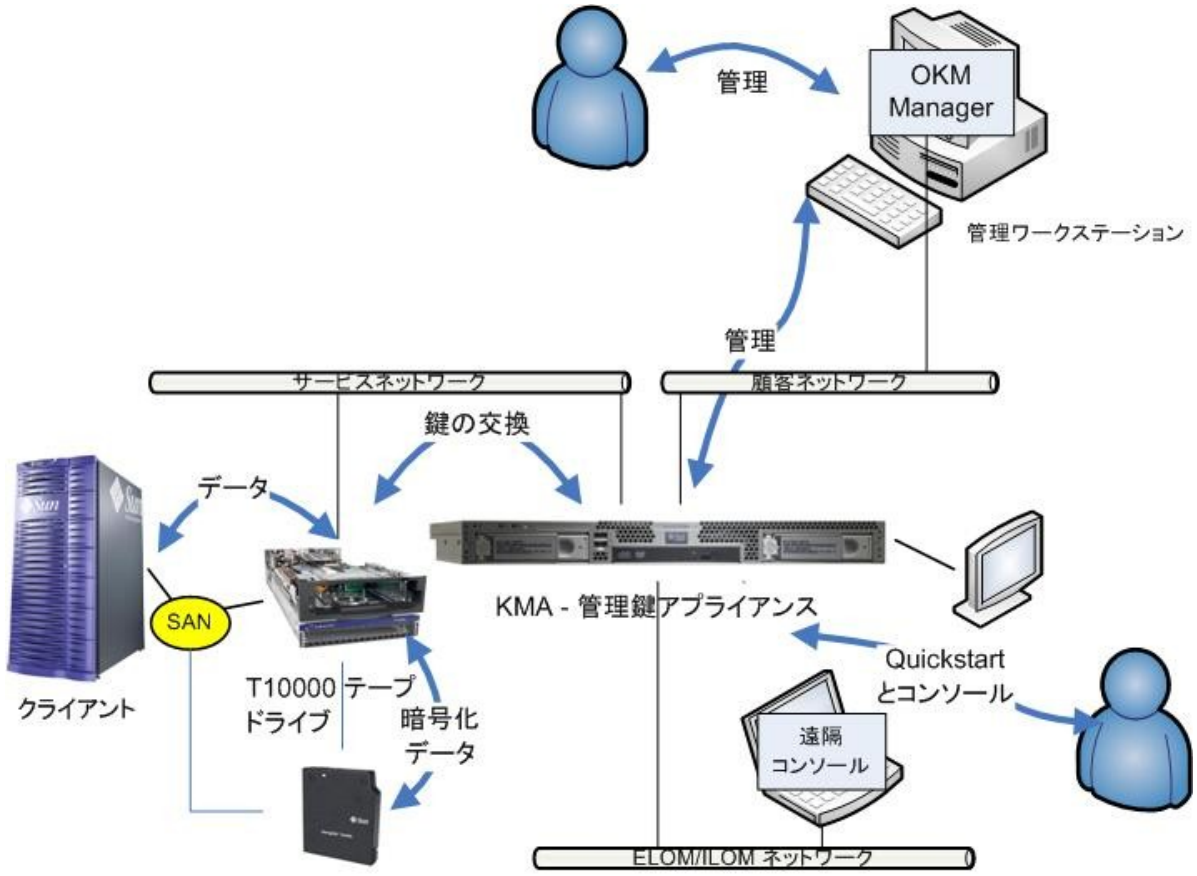


図 1-1 KMA への接続

# 一般的なセキュリティー原則

次の原則は、アプリケーションを安全に使用するための基本となります。

### ソフトウェアを最新に保つ

セキュリティーの実践に関する原則の 1 つは、すべてのソフトウェアのバージョンとパッチを最新に保つことです。最新の Oracle Key Manager アップグレードパッケージとインストーラは、My Oracle Support の Web サイトで入手できます: http://support.oracle.com。

### 重要なサービスに対するネットワークアクセスを制限する

ビジネスアプリケーションはファイアウォールで保護してください。ファイアウォールを使用すると、これらのシステムに対するアクセスが既知のネットワーク経路に制限されることが保証され、必要に応じて監視や制限を行うことができます。別の方法として、独立した複数のファイアウォールの代わりにファイアウォールルーターを使用することもできます。

### 最小特権の原則に従う

最小特権の原則とは、ユーザーに自分の業務を実行できるだけの最小限の特権を与えることです。責任、役割、権限などを過剰に与えたためにシステムが不正使用に対して無防備になることがよくあり、特に組織のライフサイクルの初期に少数の人員ですばやく作業を処理する必要があるときなどに見られます。ユーザーの特権を定期的に見直し、現在の業務上の責任に対して適切かどうかを判定するようにしてください。

### システムの動作状態を監視する

システムのセキュリティーには、優れたセキュリティープロトコル、適切なシステム構成、およびシステム監視の 3 つが基本となります。この 3 つ目の要件には監査レコードの監査と確認によって対応できます。システム内の各コンポーネントには、何らかの監視機能があります。 このマニュアルの監査アドバイスに従い、監査レコードを定期的に監視してください。

### 常に最新のセキュリティー情報を入手する

Oracle はソフトウェアとマニュアルを継続的に改善しています。毎年 My Oracle Support の Web サイトでリビジョンを確認してください。

# パート 2:セキュリティー保護されたインストールと構成

## インストールの概要

この節では、セキュリティー保護されたインストールのための計画手順について概要を示し、システムに推奨されるいくつかの配備トポロジについて説明します。

### 環境について理解する

必要なセキュリティーをよく理解するために、次の点を確認してください。

**どのリソースを保護するのか。**

本稼働環境の多くのリソースを保護できます。必要なセキュリティーのレベルを決定するときは、保護したいリソースを考慮してください。

保護する主なリソースは自分のデータです。ここで説明されているほかのリソースは、データの管理と保護に関連があるものです。データの保護に関連する事項には、データ損失 (つまり、データが利用できないこと)、データの危殆化または承認されていない者への開示などがあります。

未承認の開示からデータを保護するために暗号化鍵がよく使用されます。したがって、これらも保護するリソースです。データの高可用性を維持するには、信頼性の高い鍵管理が不可欠です。

保護する別の層のリソースとして、鍵管理アプライアンスなどの Oracle Key Manager クラスタ自体に含まれている資産もあります。

**だれからリソースを保護するのか。**

これらのリソースは、アクセスする権限のないすべてのユーザーから保護する必要があります。これらのリソースは物理的に保護されるべきです。どの従業員がこれらのリソースに対するアクセス権を持つべきかを考慮してください。次に、各従業員が Oracle Key Manager 環境でどのような操作を実行できる必要があるかを特定します。

**戦略的リソースの保護に失敗するとどうなるか。**

セキュリティー方式の障害が簡単に検出され、単なる不都合と見なされる場合もあります。それに対し、リソースを使用している会社や個人ユーザーが障害によって

大きな損害を受けることもあります。各リソースのセキュリティーの影響を理解することは、リソースを適切に保護するために役立ちます。

### 推奨される配備トポロジ

次の図は、Oracle Key Manager ソリューションの一般的な配備を示しています。

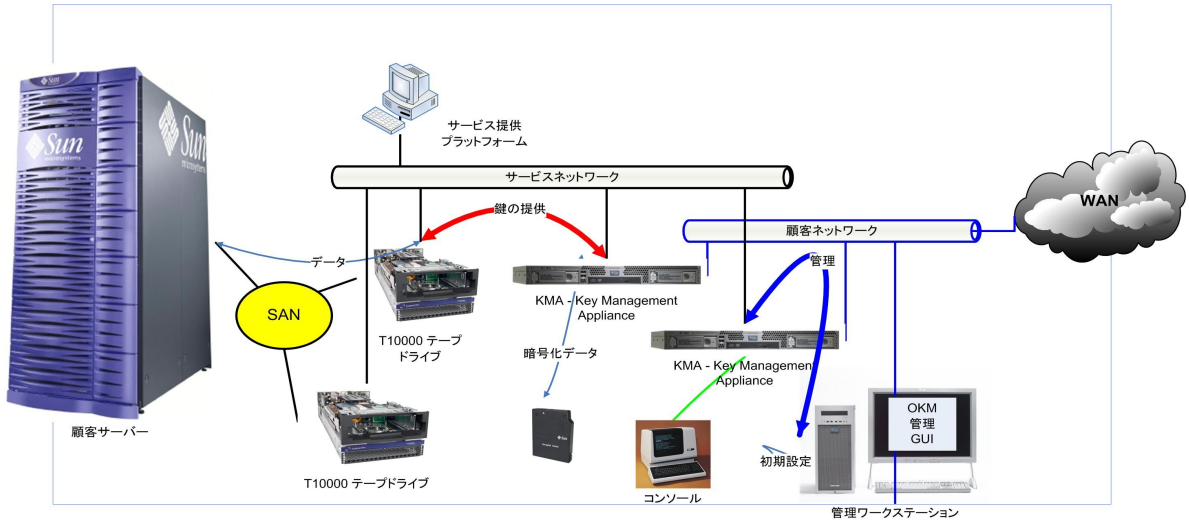


図 1-2. OKM ソリューションの一般的な配備

# 鍵管理アプライアンスの設置

この節では、OKM 鍵管理アプライアンスの設置と構成を安全に行う方法について説明します。

KMA は、製造時に Oracle Key Manager 機能が組み込まれている強化アプライアンスです。

OKM クラスタへの KMA の設置と構成は次の手順で行います。

1. 各 KMA をラック内に設置します
2. 各 KMA の BIOS と ILOM をセキュリティーで保護します
3. OKM クラスタ内の最初の KMA を構成します
4. OKM クラスタに追加の KMA を追加します

OKM クラスタの配備の計画については、Oracle Key Manager のドキュメントライブラリに含まれている『Oracle Key Manager システムアシュアランスガイド』を参照してください。

### KMA をラック内に設置する

『Oracle Key Manager Installation and Service Manual』の手順に従って Oracle カスタマサービスエンジニアが KMA をラック内に設置します。Oracle のサービス担当者は、詳細な情報を確認するためにこのマニュアルを参照することがあります。

### KMA の BIOS をセキュリティーで保護する

Oracle Key Manager KMA は製造時に最新の ILOM および BIOS ファームウェアが組み込まれます。Oracle カスタマサービスエンジニアまたはお客様が、KMA の BIOS をセキュリティーで保護する必要があります。ILOM または ELOM ファームウェアをアップグレードした場合も、BIOS をセキュリティーで保護するようにしてください。

BIOS をセキュリティーで保護するには、セキュリティーの危殆化につながる可能性のある BIOS の変更を防ぐように特定の BIOS 設定を変更します。

次に示す手順では、KMA の Integrated Lights Out Manager (ILOM) を介して BIOS 設定ユーティリティーにアクセスします (この KMA は Oracle の Sun Fire X4170 M2 サーバーです)。また、KMA の Embedded Lights Out Manager (ELOM) を介して BIOS 設定

ユーティリティーにアクセスします (この KMA は Sun Fire X2100 または X2200 M2 サーバーです)。この手順に関連する BIOS 設定は、3 種類のサーバーのどれについても同じです。

1. Web ブラウザを開きます。Web ベースのインタフェースを使用して ILOM にログインします。ILOM Web インタフェースの使用方法の詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』を参照してください。
2. 新しく製造された KMA には、root ユーザーのデフォルトパスワードが設定されています。このパスワードを変更し、保管するようにしてください。
3. BIOS 設定ユーティリティーにアクセスするには、「Remote Control」、「Redirection」の順に移動し、「Launch Redirection」をクリックしてリモートコンソールを起動します。ダイアログが表示されたら、リモートコンソールが表示されるまでクリックしていきます。次に、「Remote Control」、「Remote Power Control」の順に移動し、「Power Up」を選択して「SAVE」をクリックします。リモートコンソールで起動メッセージを確認します。リブートが開始されるころに American Megatrends の画面が表示されたら F2 キーを押します。

BIOS 設定ユーティリティーで、次の手順を実行します。

1. 「Security」タブの「Change Supervisor Password」フィールドに移動して Enter キーを押し、パスワードを指定します。このパスワードを保管します。
2. スーパーバイザのパスワードを指定すると、「User Access Level」フィールドが表示されます。「User Access Level」フィールドに移動し、設定を「Full Access」から「Limited」に変更します。
3. 「Boot」タブに移動します。「Boot Device Priority」に移動し、次のように変更します。

| タブ | フィールド名 | 値 |
|---|---|---|
| Boot | 1st Boot Device<br>(「Boot Device Priority」の下) | HDD:P0-SEAGATE<br>ST95000NSSUN500G 101 |

| タブ | フィールド名 | 値 |
|---|---|---|
| Boot | 2nd Boot Device<br>(「Boot Device Priority」の下) | Disabled |
| Boot | 3rd Boot Device<br>(「Boot Device Priority」の下) | Disabled |

4. これらの変更を保存するために F10 キーを押し、「OK」を選択して確定します。

システムが起動するまで待ちます。これで BIOS にスーパーバイザのパスワードが定義されたので、次に BIOS 設定ユーティリティーにアクセスするとこのパスワードの入力が求められます。

BIOS 設定ユーティリティーの操作方法の詳細については、『Sun Fire X4170, X4270, and X4275 Servers Service Manual』の「Configuring BIOS Settings」の節を参照してください。

### KMA の ILOM をセキュリティーで保護する

Oracle Key Manager KMA は製造時に最新の ILOM および BIOS ファームウェアが組み込まれます。Oracle カスタマサービスエンジニアまたはお客様が、KMA の ILOM をセキュリティーで保護する必要があります。ILOM ファームウェアをアップグレードした場合も、ILOM をセキュリティーで保護するようにしてください。

ILOM をセキュリティーで保護するには、セキュリティーの危殆化につながる可能性のある ILOM の変更を防ぐように特定の ILOM 設定を変更します。

次に示す手順では、KMA の Integrated Lights Out Manager (ILOM) にアクセスします (この KMA は Sun Fire X4170 M2 サーバーです)。

1. Web ブラウザを開きます。Web ベースのインタフェースを使用して ILOM にログインします。ILOM Web インタフェースの使用方法の詳細については、『Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』を参照してください。

2. 新しく製造された KMA には、root ユーザーのデフォルトパスワードが設定されています。このパスワードを変更し、保管するようにしてください。

3. 「Configuration」、「System Management Access」、「SNMP Management」の順に移動します。「Settings」には SNMPv3 の使用をお勧めします (v1 と v2c は無効にしてもかまいません)。SNMP を介した構成の変更を防ぐために「Set Requests」を無効にします。

4. 「Configuration」、「System Management Access」、「IPMI」の順に移動します。OKM 2.4 で Auto Service Request (ASR) 機能が導入されている場合は、IPMI を有効にします。 それ以外の場合は、使用する予定がなければ IPMI を無効にします。このインタフェースを開いておくと、この KMA がリブートされる可能性があります。

5. 「Configuration」、「System Management Access」、「CLI」の順に移動します。デフォルト設定では CLI セッションが無期限に開いたままになる可能性があるため、セッションタイムアウトを設定します。

6. 「Configuration」、「System Management Access」、「WS-Man」の順に移動します。WS-Management と CIM を使用する予定がない場合は、このサービスを無効にします。このインタフェースを開いておくと、WS-Management プロトコルの知識を持つ者から KMA が攻撃を受ける可能性があります。

7. 「Configuration」、「Clock」の順に移動します。ILOM クロックは Sun Fire X4170 M2 サーバー上のホストクロックとは同期されていません。ILOM のイベントをサーバーのイベントと関連付けられるようにするには、ILOM の日付と時刻を UTC/GMT 時刻に手動で設定するか、外部 NTP サーバーと同期されるように設定する必要があり、外部 NTP サーバーとしては、この OKM クラスタの KMA が使用している サーバーをお勧めします。詳細については、Oracle Key Manager のドキュメントライブラリに含まれている『Oracle Key Manager 管理ガイド』を参照してください。

8. 「Configuration」、「Timezone」の順に移動します。ILOM のタイムゾーンは「GMT」に設定する必要があります。

9. 「User Management」、「User Accounts」の順に移動します。デフォルトの root アカウントだけを使用するよりも、ユーザーアカウントと役割を使用することをお勧めします。詳細については、『Oracle Integrated Lights Out

Manager (ILOM) 3.0 概念ガイド』の「ユーザーアカウント管理」の節を参照してください。

10. 「Remote Control」、「Host Control」の順に移動します。「Next Boot Device」の値を「Default (User BIOS Settings)」に設定する必要があります。

11. 「Maintenance」、「Firmware Upgrade」の順に移動します。ILOM のファームウェアを最新に保ち、『Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド』の説明に従って更新するようにしてください。念のため、ILOM ファームウェアをアップグレードする前に OKM コンソールから KMA をシャットダウンしてください。

ILOM の構成の変更によって問題が発生していると考えられる場合は、『Sun Fire X4170, X4270, and X4275 Servers Service Manual』の「Troubleshooting The Server and Restoring ILOM Defaults」の節に従って、ILOM の設定をデフォルト値に戻すことができます。

**OKM クラスタ内の最初の KMA を構成する**

最初の KMA を構成する前に、この OKM クラスタで定義する鍵分割資格およびユーザー ID とパスフレーズを確認します。Oracle Key Manager のドキュメントライブラリに含まれている『Oracle Key Manager システムアシュアランスガイド』には便利なワークシートがあります。これらの鍵分割資格およびユーザー ID とパスフレーズを適切な担当者に通知します。詳細については、このマニュアルで後述する「定足数保護」の節を参照してください。

重要: これらの鍵分割資格およびユーザー ID とパスフレーズを保管し、保護してください。

Web ブラウザを開き、リモートコンソールを起動し、リモートコンソール内で OKM QuickStart ユーティリティーを起動します。この KMA 上で OKM クラスタを初期化するには、Oracle Key Manager のドキュメントライブラリに含まれている『Oracle Key Manager 管理ガイド』で説明されているクラスタの初期化手順に従います。

鍵分割資格、およびセキュリティー責任者特権を持つユーザーがこの手順で定義されます。QuickStart 手順が完了したあとで、セキュリティー責任者が KMA にログインし、追加の OKM ユーザーを定義する必要があります。

**鍵分割資格を定義する際の注意事項**

定義する鍵分割ユーザー ID とパスフレーズが少なく、しきい値が低いほど、扱いは簡単ですがセキュリティーは低下します。定義する鍵分割ユーザー ID とパスフレーズが多く、しきい値が高いほど、扱いは複雑ですがセキュリティーは向上します。

**追加の OKM ユーザーを定義する際の注意事項**

定義する OKM ユーザーが少ないほど、またその一部に複数の役割を割り当てると、扱いは簡単ですがセキュリティーは低下します。定義する OKM ユーザーが多いほど (そのほとんどに役割を 1 つだけ割り当てる)、扱いは複雑です が、特定の OKM ユーザーによって実行された操作を追跡しやすくなるため、セキュリティーは向上します。

**OKM クラスタに追加の KMA を追加する**

Web ブラウザを開き、リモートコンソールを起動し、リモートコンソール内で OKM QuickStart ユーティリティーを起動します。この KMA を OKM クラスタに追加するには、Oracle Key Manager のドキュメントライブラリに含まれている『Oracle Key Manager 管理ガイド』で説明されているクラスタへの参加手順に従います。

**追加の KMA を追加する際の注意事項**

Oracle Key Manager には、各 KMA の自律ロック解除という便利なオプションが用意されています。 このオプションは、クラスタ内の最初の KMA および追加の KMA に対する QuickStart 手順で定義され、セキュリティー責任者があとで変更できます。

自立ロック解除が有効になっている場合、KMA は起動時に KMA 自身のロックを自動的に解除し、定足数承認を要求することなく鍵を提供できる状態になります。自立ロック解除が無効になっている場合、KMA は起動時にロックされたままになり、セキュリティー責任者がそのロック解除を要求してこの要求が定足数承認を得るまで、鍵を提供しません。

セキュリティーを最大にするため、自立ロック解除を有効にすることはお勧めしません。自立ロック解除オプションの詳細については、『Oracle Key Manager Version 2.X Security and Authentication White Paper』を参照してください。

### 強化 KMA の特徴

前述のとおり、KMA は、製造時に Oracle Key Manager 機能が組み込まれている強化アプライアンスです。強化アプライアンスとして、次の特徴を備えています。

- 不要な Solaris パッケージは Solaris イメージに含まれていません。たとえば、ftp および telnet のサービスとユーティリティーは Solaris イメージ内に存在しません。
- KMA はコアファイルを生成しません。
- 標準の Solaris login(1) ユーティリティーは OKM コンソールで置き換えられています。したがって、ユーザーは Solaris コンソールにログインできません。
- ssh サービスはデフォルトで無効になっています。カスタマサポートのため、セキュリティー責任者が ssh サービスを有効にし、期間を制限してサポートアカウントを定義できます。このサポートアカウントは使用可能な唯一のアカウントとなり、そのアクセス権と権限は制限されます。サポートアカウントが呼び出すコマンドは Solaris 監査で追跡されます。
- root アカウントは無効になっています。
- Solaris のシングルユーザーモードは無効になっています。
- KMA に DVD ドライブは搭載されていません。
- USB ポートは事実上無効にされます。
- 使用されないネットワークポートは閉じられます。
- このハードウェアセキュリティーモジュールは、FIPS 140-2 のレベル 3 で認定されているため、認定された暗号化アルゴリズムに加えて、タンパー検出機能および耐タンパー性機能の両方を提供します。
- 新しい KMA ベースの Sun Fire X4170 M2 サーバーは、電源が供給されているときにシャーシのドアにアクセスがあると、タンパーを検出します (ILOM 障害)。

# パート 3: セキュリティー機能

この節では、製品で提供されている特定のセキュリティー機構の概要について説明します。

## 潜在的な脅威

暗号化が有効になっているエージェントを使用している場合は、主に次の事項に注意する必要があります。

- ポリシーに違反する情報開示
- データの損失または破壊
- 重大な障害時のデータ復元における許容できない遅延 (ビジネス継続性サイトなど)
- 検出されないデータ変更

## セキュリティー機能の目的

Oracle Key Manager のセキュリティー機能の目的は次のとおりです。

- 暗号化されたデータが開示されないように保護する
- 攻撃を受ける可能性を最小化する
- 十分に高い信頼性と可用性を提供する

## セキュリティーモデル

セキュリティーガイドのこの節では、システムが設計上対抗できる脅威の概要を示し、個々のセキュリティー機能がどのように連携して攻撃を防ぐかについて説明します。

これらの保護を提供する重要なセキュリティー機能は次のとおりです。

- 認証 - 承認されているユーザーだけがシステムとデータにアクセスできるようにします

- 承認 - システム特権とデータに対するアクセス制御。このアクセス制御は、認証に基づいてユーザーが適切なアクセス権だけを取得するようにします
- 監査 - 認証機構に対する違反の試み、およびアクセス制御に対する違反の試みまたは成功した違反を管理者が検出できるようにします

Oracle Key Manager のセキュリティーと認証の詳細については、『Oracle Key Manager Version 2.X Security and Authentication White Paper』を参照してください。

## 認証

Oracle Key Manager のアーキテクチャーでは、システムのすべての要素間に相互の認証が提供されています。KMA と KMA、エージェントと KMA、およびユーザー操作については Oracle Key Manager GUI または CLI と KMA の間です。

システムの各要素 (新しい暗号化エージェントなど) は、OKM で ID とパスフレーズを作成し、追加する要素に入れることによってシステムに登録されます。たとえば、システムにテープドライブを追加すると、エージェントと KMA は共有されているパスフレーズに基づいてチャレンジ応答プロトコルを自動的に実行します。その結果、エージェントはルート証明書発行局 (CA) の証明書、およびエージェントの新しい鍵ペアと署名付き証明書を取得します。ルート CA 証明書、エージェントの証明書、および鍵ペアの準備が整ったら、エージェントは以降の KMA とのすべての通信に使用するために Transport Layer Security (TLS) プロトコルを実行できます。証明書はすべて X.509 証明書です。

OKM はルート証明書発行局として動作し、ルート証明書を生成します。KMA はこのルート証明書を使用して、エージェント、ユーザー、および新しい KMA が使用する証明書を取得 (自己署名) します。

# アクセス制御

### ユーザーと役割に基づくアクセス制御

Oracle Key Manager では、複数のユーザーを定義し、各ユーザーにユーザー ID とパスフレーズを設定できます。各ユーザーには、1 つ以上の事前定義済みの役割が付与されています。これらの役割により、ユーザーが Oracle Key Manager システムで実行できる操作が決まります。役割は次のとおりです。

- セキュリティー責任者 - Oracle Key Manager の設定と管理を実行します
- オペレータ – エージェントの設定と日常の操作を実行します
- コンプライアンス責任者 - 鍵グループを定義し、鍵グループに対するエージェントのアクセスを制御します
- バックアップオペレータ - バックアップ操作を実行します
- 監査者 - システムの監査証跡を参照します
- 定足数メンバー - 保留中の定足数操作を参照し、承認します

セキュリティー責任者は、OKM クラスタ内の KMA を設定する QuickStart 手順で定義されます。そのあとで、追加のユーザーを定義するには、Oracle Key Manager GUI を使用してセキュリティー責任者としてクラスタにログインする必要があります。セキュリティー責任者は、1 人のユーザーに複数の役割を割り当てることも、1 つの役割を複数のユーザーに割り当てることもできます。

各役割に許可される操作、およびセキュリティー責任者がユーザーを作成して役割を割り当てる方法の詳細については、この役割に基づくアクセス制御では、米国標準技術局 (NIST) 発行の Special Publication (SP) 800-60 で定義されている、業務上の機能を区別するための業務の役割がサポートされています。

### 定足数保護

一部の操作は非常に重要なので、さらに高いセキュリティーレベルが必要になります。そのような操作には、OKM クラスタへの KMA の追加、KMA のロック解除、ユーザーの作成、ユーザーへの役割の追加などがあります。このセキュリティーを実装するために、前述の役割に基づくアクセス制御に加えて一連の鍵分割資格が使用されます。

鍵分割資格は、一連のユーザー ID とパスフレーズのペア、および特定の操作を完了するために必要なこれらのペアの最小数から 成ります。鍵分割資格は「定足数」、最小数は「定足数しきい値」とも呼ばれます。

Oracle Key Manager では、鍵分割ユーザー ID とパスフレーズのペアを 10 個まで設定でき、しきい値を定義できます。これらは、OKM クラスタ内の最初の KMA を設定する QuickStart 手順で定義されます。鍵分割ユーザー ID とパスフレーズは、システムへのログインに使用されるユーザー ID とパスフレーズとは異なります。ユーザーが定足数承認を必要とする操作を試みた場合、システムでこの操作が実行されるには、定義されているしきい値の鍵分割ユーザーとパスフレーズによってこの操作が承認される必要があります。

# 監査

各 KMA は、エージェント、ユーザー、OKM クラスタ内のピア KMA によって発行された操作などを含め、実行する操作について監査イベントをログに記録します。また、KMA はエージェント、ユーザー、またはピア KMA が認証に失敗した場合にも監査イベントをログに記録します。セキュリティー違反を示す監査イベントはマークされます。認証の失敗は、セキュリティー違反を示す監査イベントの一例です。また、OKM クラスタ内に SNMP エージェントが識別されている場合、KMA はセキュリティー違反を検出するとこれらの SNMP エージェントに SNMP INFORM を送信します。

監査イベントを参照するには、ユーザーは OKM クラスタに正しくログインし、役割が割り当てられている必要があります。

KMA はそれぞれの監査イベントを管理します。KMA は保持期間と制限 (数) に基づいて古い監査イベントを削除します。セキュリティー責任者は必要に応じてこれらの保持期間と制限を変更できます。

# その他のセキュリティー機能

Oracle Key Manager ではほかのセキュリティー機能も提供されています。OKM のさまざまな機能の詳細については、『Oracle Key Manager Overview』を参照してください。

### セキュリティー保護された通信

エージェントと KMA、ユーザーと KMA、および KMA とピア KMA の間の通信プロトコルは同じです。どの場合も、通信を開始しようとしているエンティティーのパスフレーズを使用してチャレンジ応答プロトコルが実行されます。成功すると、証明書とその対応する非公開鍵がこのエンティティーに提供されます。この証明書と非公開鍵により、2048 ビット RSA を使用して Transport Layer Security (TLS) 1.0 (セキュアソケット) チャネルを確立できます。このセッションが確立されたら、エンドポイントで Advanced Encryption Standard (AES) の 256 ビット鍵の合意が行われます。TLS 暗号化スイートは、ネゴシエーション可能ではないため、KMA クライアントのエンドポイントはより弱いスイートのネゴシエーションを行わないことがあります。以降の通信はすべてこの AES 256 ビット鍵で暗号化されます。相互の認証が実行され、どの接続でも、各終端が相手を認証します。

### ハードウェアセキュリティーモジュール

KMA には別売りのハードウェアセキュリティーモジュールが用意されています。このハードウェアセキュリティーモジュール、Sun 暗号化アクセラレータ (SCA) 6000 カードは、FIPS 140-2 レベル 3 に認定されており、Advanced Encryption Standard (AES) 256 ビット暗号化鍵を提供します。SCA 6000 カードは、FIPS 140-2 レベル 3 モードの操作をサポートしており、OKM は常にこの方法でこのカードを使用します。OKM クラスタが FIPS 準拠モードで動作している場合、暗号化鍵がラップされていない形式で SCA 6000 カードの暗号境界を離れることはありません。SCA 6000 カードは、FIPS で承認されている乱数発生関数を使用して暗号化鍵を生成します。これは、FIPS 186-2 で指定されている、SHA -1 を使用する DSA 乱数発生関数です。

KMA に SCA 6000 カードが構成されていない場合、暗号化は Solaris 暗号化フレームワーク (SCF) の PKCS#11 ソフトトークンを使用して実行されます。

**AES 鍵ラッピング**

Oracle Key Manager は、対称鍵が作成されるとき、KMA に保存されるとき、エージェントに送信されるとき、または鍵転送ファイル内で送信されるときに、AES 鍵ラッピング (RFC 3994) を 256 ビット鍵の暗号化鍵で使用して対称鍵を保護します。

**鍵の複製**

OKM クラスタの最初の KMA が初期化されると、この KMA によって大きな 鍵プールが生成されます。 追加の KMA がクラスタに追加されると、鍵が新しい KMA に複製され、そのあとでデータの暗号化に使用できる準備完了状態になります。クラスタに追加された各 KMA は鍵プールを生成し、クラスタ内のピア KMA に複製します。すべての KMA は、鍵プールのサイズを維持するために必要に応じて新しい鍵を生成して、エージェントが準備完了状態の鍵を常に使用できるようにします。エージェントは、新しい鍵が必要になると、クラスタ内の KMA と通信して新しい鍵を要求します。KMA は鍵プールから準備完了状態の鍵を取り出し、エージェントのデフォルトの鍵グループとデータユニットにこの鍵を割り当てます。次に、KMA はこれらのデータベースの更新をクラスタ内のほかの KMA にネットワーク経由で複製します。あとで、エージェントはクラスタ内の別の KMA と通信してこの鍵を取り出すことができます。平文の鍵データがネットワーク経由で送信されることは決してありません。

# パート 4: Linux PKCS#11 KMS プロバイダ

Oracle Key Manager のリリースには、新しい Linux PKCS#11 KMS プロバイダが付属しています。管理者は、My Oracle Support の Web サイトから Linux PKCS#11 KMS プロバイダをダウンロードして、Oracle Enterprise Linux サーバーにインストールできます。Linux PKCS#11 KMS プロバイダは、ほかのエージェントと同じセキュリティーの特徴を持ち、Oracle Key Manager アプライアンスで同様に認証を行います。

Linux PKCS#11 KMS プロバイダは、ログファイルとプロファイル情報を /var/opt/kms/*ユーザー名* ディレクトリに格納します。ユーザーまたは管理者、あるいはその両方はこのログファイルを手動でまたは logrotate などのユーティリティーを使用して管理するようにしてください。

/var/opt/kms/*ユーザー名* ディレクトリへのアクセスの制御は、適切な権限によって制限するようにしてください。 プロファイルディレクトリ内では、エージェントの認証資格は PKCS#12 ファイル内に保持されます。 PKCS#12 ファイルはパスワードで保護されています。

Linux PKCS#11 KMS プロバイダについては、Oracle Key Manager のドキュメントライブラリに含まれている『Oracle Key Manager 管理ガイド』を参照してください。

# パート 5: 付録

## 付録 A: セキュリティー保護された配備のチェックリスト

次のセキュリティーチェックリストには、鍵管理システムをセキュリティーで保護するために役立つガイドラインが含まれています。

1. 各 KMA を物理的に安全な環境に設置します。
2. 各 KMA の BIOS をセキュリティーで保護します。
3. この Oracle Key Manager クラスタの鍵分割構成を定義します。
4. 各 KMA の自立ロック解除を適切に設定します。
5. Oracle Key Manager ユーザーとそれに関連付ける役割を定義します。
6. 最小特権の原則を実践します。
    i. 各 Oracle Key Manager ユーザーに必要最小限の役割だけを割り当ててください。
7. Oracle Key Manager クラスタの動作状態を監視します。
    i. Oracle Key Manager の監査ログに記録されているすべてのエラー、特にセキュリティー違反を調査してください。
8. 鍵分割構成を最初に定義するとき、および鍵分割構成を変更するときは常に、コアセキュリティーをバックアップします。
9. Oracle Key Manager のバックアップを定期的に実行します。
10. コアセキュリティーのバックアップファイルと Oracle Key Manager のバックアップファイルを安全な場所に保管します。

# 付録 B: リファレンス

Oracle Key Manager のドキュメントライブラリ

Oracle Key Manager Installation and Service Manual

Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface 手順ガイド

Oracle Integrated Lights Out Manager (ILOM) 3.0 概念ガイド

Sun Fire X4170 M2 および X4270 M2 サーバー製品ノート

Sun Fire X4170, X4270, and X4275 Servers Service Manual

Oracle Key Manager Overview

Oracle Key Manager Version 2.X Security and Authentication White Paper

National Institute of Standards and Technology Special Publication 800-60 Volume I Revision 1

Sun Cryptographic Accelerator 6000 FIPS 140-2 Security Policy