Sun ORACLE | SUN STORAGE

Oracleホワイト・ペーパー
2014年11月

Oracle Key Managerの概要

ORACLE

免責事項

下記事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

はじめに

Oracle Key Managerは、ストレージベースのデータ暗号化への企業のコミットメントが急速に高まる状況に対処するために設計された、包括的な鍵管理システム（KMS）です。オープン・スタンダードに従って開発されたこのアプリケーションを使用することで、広範に分散された異機種混合のストレージ・インフラストラクチャ全体で暗号化鍵を一元管理できる容量、スケーラビリティ、相互運用性が実現します。

Oracle Key Managerは、以下に挙げるストレージ鍵管理特有の課題に対処するように、特別に設計されています。

- **長期間の鍵保存：**Oracle Key Managerでは、アーカイブ・データを常に利用できるようにするために、データの全ライフ・サイクルにわたって暗号化鍵をセキュアに保存します。保存期間は10年以上に及ぶ場合もあります。

- **相互運用性：**単一のストレージ鍵管理サービスの下で、メインフレームまたはオープン・システムに接続された多様なストレージ・デバイスをサポートするために必要な相互運用性レベルが提供されます。

- **高可用性：**アクティブなNノード・クラスタリング、動的なロードバランシング、および自動フェイルオーバーにより、アプライアンスが同じ部屋にあろうと、世界中に分散されていようと、高可用性を実現します。

- **大容量：**Oracle Key Managerでは、多数のストレージ・デバイスと、その数を超えるストレージ鍵が管理されます。クラスタ化された単一のアプライアンス・ペアによって、数千ものストレージ・デバイスと数百万ものストレージ鍵を管理する鍵管理サービスが提供されます。

Oracle Key Managerの暗号化では、以下の暗号化エンドポイントをサポートしています。

- 暗号化対応テープ・ドライブ：
  - StorageTek T10000A
  - StorageTek T10000B
  - StorageTek T10000C
  - StorageTek T10000D
  - StorageTek T9840D
  - IBM LTO4およびHP LTO4
  - IBM LTO5およびHP LTO5
  - IBM LTO6およびHP LTO6
- Oracle Key ManagerのPKCS#11プロバイダ（pkcs11_kms）：
  - Oracle Solaris 11
  - Oracle Solaris 10 Update 10
    （x86用パッチ147441-03またはSPARC用パッチ147159-02の適用済み）
  - Oracle Linux Serverリリース5.5、5.6、5.9、6.5
- Oracle Key ManagerのPKCS#11プロバイダ（pkcs11_kms）は、Oracle Database 11g Release 2および12cの機能であるTransparent Data Encryption（TDE）にインタフェースを提供する認定を受けています。

- サポートされるpkcs11_kmsプラットフォームのOracle Database 11.2.0.2（パッチ12626642の適用済み）

- サポートされるpkcs11_kmsプラットフォームのOracle Database 12.1.0.1.0

- Oracle Key Manager Java Cryptography Extension（JCE）プロバイダ

Oracle Enterprise Manager Cloud ControlコンソールからOracle Key Manager Key Management Appliance（KMA）をモニタリングするために、Oracle Key Manager向けのOracle Enterprise Manager System Monitoring Plug-inを、Oracle Enterprise Manager環境にインストールできます。

このホワイト・ペーパーでは、次のトピックについて説明します。

- Oracle Key Managerの概要
- 基本的なオペレーション
- セキュリティ機能
- 鍵管理のプラクティス
- パートナーの鍵転送
- バックアップとリカバリのプラクティス
- ディザスタ・リカバリのプラクティス
- StorageTek Crypto Key Management System 1.xからOracle Key Managerへの移行パス

Oracle Key Managerの概要

Oracle Key Managerは、以下の3つの主要コンポーネントで構成されています。

- **Key Management Appliance（KMA）：**ポリシーベースの鍵管理、認証、アクセス制御、鍵プロビジョニングの各サービスを提供する、セキュリティが強化された機器です。ストレージ・ネットワークの信頼できる発行局としての役割を果たすOracle Key Manager KMAにより、すべてのストレージ・デバイス（エージェント）が登録および認証されること、そしてすべての暗号化鍵が規定のポリシーに従って作成、プロビジョニング、および削除されることが保証されます。IPネットワーク経由で接続される複数のKMAにより、Oracle Key Managerクラスタが形成されます。
- **KMA管理ソフトウェア：**
    - **GUI：**KMAは、ロックされ、セキュリティが強化されたデバイスです。権限のあるセキュリティ責任者が、KMAのコンソールまたはサービス・プロセッサから利用できるのは、非常に限られたオプションのみです。Oracle Key Managerの管理は、特定のオペレーションを除き、お客様の用意するワークステーションまたはサーバーから実行されるGUI管理プログラムを使用して行われます。
    - **CLI：**さまざまなタスクの自動化を促進するために、この製品には2つのコマンドライン・インタフェース・ユーティリティが搭載されています。これらのCLIは、お客様の用意するワークステーションまたはサーバーから実行されます。
- **ハードウェア・セキュリティ・モジュール（HSM）：**KMAは、FIPS 140-2レベル3認証済みのハードウェア・セキュリティ・モジュール（HSM）とともに購入することも、HSMなしで購入することもできます。Oracle Sun Cryptographic Accelerator（SCA）6000カードは、KMAと完全に統合されたHSMコンポーネントです。クラスタには、複数のKMAとHSMがともに使用される場合があります。またHSMは、初期導入後にKMAに追加することも可能です。SCA 6000カードがKMAにインストールされている場合、カードはFIPSモードで機能するようにKMAによって自動設定されます。

  Oracle Key Managerクラスタでは、冗長性と拡張された帯域幅、そして次の2つのネットワーク（KMAサービス・プロセッサのネットワーク・インタフェースを除く）が提供されます。

  - 暗号化エージェントとKMAとの通信に使用されるサービス・ネットワーク
  - KMA間のトラフィックとリモート管理ステーションとの通信用に使用される管理ネットワーク

これにより、ストレージ・デバイスが通信量の多い企業ネットワークから分離され、鍵リクエストのレスポンス・タイムが向上します。Oracle Key Managerは、暗号化対応テープ・ドライブや、「はじめに」のセクションに記載されている各種の暗号化エンドポイントを含むさまざまなエージェントと同時に使用されます。このホワイト・ペーパーでは、Oracle Key Manager暗号化ソリューションをStorageTekテープ・ドライブとともに使用した場合の動作について説明します。LTOテープ・ドライブ特有の動作にはついて、付録Bに記載しています。Oracle Key Managerでは、完全に自動化されたフェイルオーバーとアクティブなNノード・クラスタリングがサポートされます。ドライブ暗号化エージェントは、システム内のすべてのKMAを認識しており、クラスタ内のすべてのKMAが、あらゆるエージェントにサービスを提供できます。デフォルトでは、可能な場合はローカルのKMAからエージェントにサービスが提供されます。現在の実装では、異なるサイト（すなわち異なるサブネッ

ト）にあるドライブ・ネットワークは分離されています。エージェントは、そのサイトのローカルなKMAにのみ接続されます。そのため、各サイトでは、KMAの処理量が増えた場合や、KMAを使用できなくなった場合にも継続的な可用性を提供できるよう、KMAが2台必要です。

すべてのKMAで管理機能を使用でき、KMAに加えられた変更は、クラスタ内にある残りのすべてのKMAに複製されます。あるサイトで生成された鍵は、クラスタ内のすべてのKMAに複製されるため、サイト間で、およびディザスタ・リカバリにおいて、容易に鍵を共有できます。同様に、サイトで管理面の変更を行った場合は、クラスタ内のすべてのKMAに伝播されます。すべての管理機能は、Oracle Key Manager GUIから実行され、1台の管理ワークステーションで、クラスタ内のすべてKMAを管理できます。以下の図1をご覧ください。

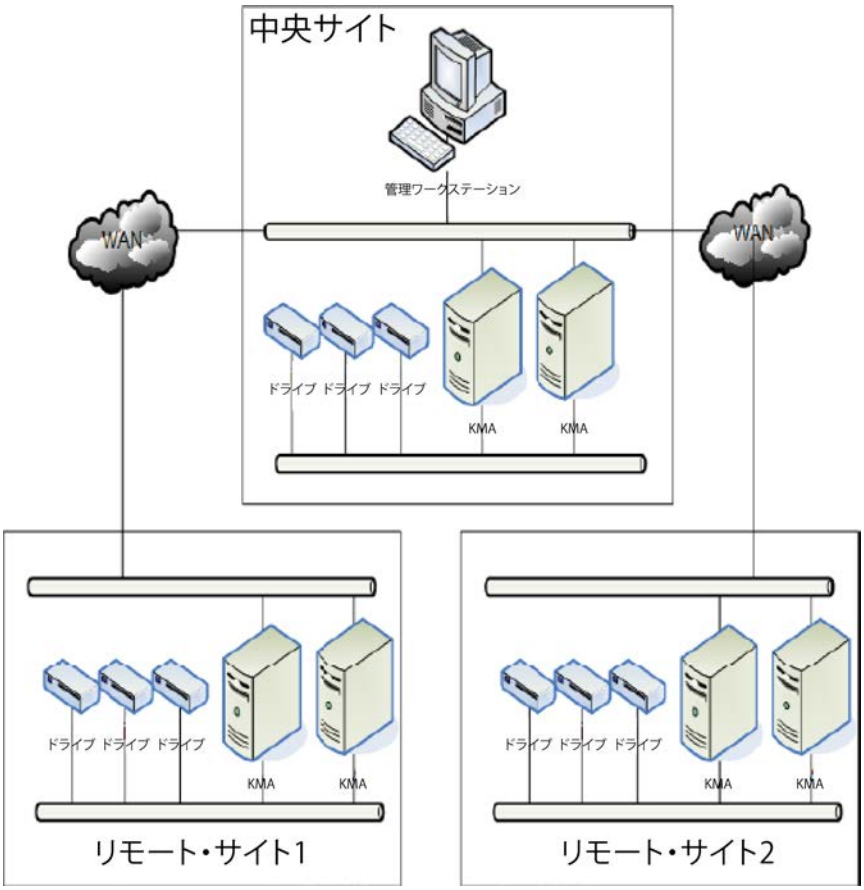

図1：一般的な複数サイトの構成は、単一の管理ワークステーションから管理可能。

注：各KMAには、初期構成タスクの実行に使用されるサービス・プロセッサ・インタフェース用の管理ネットワーク（図には非表示）との第2の接続が確立されます。

機能

Oracle Key Managerの機能と利点

機能	利点
セキュリティ	
米国連邦情報処理標準（FIPS）□認証済み暗号化	FIPS 140-2 認証済み暗号化を使用して、保存データに Advanced Encryption Standard（AES）256 ビットの暗号化鍵を提供
ロールベースのアクセス制御	オペレーション機能を分離する、米国国立標準技術研究所（NIST）SP800-60 オペレーション・ロールをサポート
定足数	最小数の定足数メンバーで、KMA のアクティブ化、ユーザーの作成、ユーザーへのロールの追加、および Oracle Key Manager データベース・バックアップのリストアが可能。定足数パラメータは完全に構成可能
強化されたオペレーティング・システム	さらなるセキュリティ機能により、Oracle Key Manager アプライアンスへの直接攻撃を防止
高可用性	
アクティブなクラスタリングとフェイルオーバー	アクティブな N ノード・クラスタリングと完全に自動化されたフェイルオーバーにより、高可用性を実現
ロードバランシング	アクティブなロードバランシングで最適化を実現
ほぼ同期化されたレプリケーション	アプライアンス・ノード間のトランザクション・データに対して、ほぼ同期化されたセキュアなレプリケーションを提供
ロールとロール分離	
細分化されたロール分離	セキュリティ責任者、コンプライアンス責任者、オペレーター、バックアップ・オペレーター、監査者、定足数メンバーという 6 つの異なるロール定義により、オペレーションの分離を実現。これらのロールはアクセスが制御され、機能に制限が付けられますが、必要に応じてユーザーが複数のロールを持つことも可能
一元化されたロール割合て	一元管理により、オペレーション・ロールの一元化された割当てと管理を実現。自動化されたデータ・レプリケーションにより、ディザスタ・リカバリのためにすべてのリモート・サイトにロール・データを自動配布
一元化されたポリシー管理	コンプライアンス責任者のロールを通じて、データ暗号化ポリシーの一元管理を実現。ディザスタ・リカバリのために、ポリシーを自動でレプリケート
オペレーション	
堅牢な API ライブラリ	堅牢な API ライブラリにより、オペレーションの自動化とサード・パーティ製品の統合が実現。ストレージまたはバックアップ・アプリケーション・マネージャなど、サード・パーティ製ストレージ・サービスを迅速に統合して、Oracle Key Manager のポリシーと鍵管理機能を使用可能
監査ロギング	業務上のすべての重要なイベントとトランザクションの監査ログを保守
オープン・スタンダード	標準の証明書フォーマットの X.509v3 証明書、SOAP、TLS を含むオープン・スタンダードをサポート
管理	
セキュアな管理クライアント	セキュアな管理クライアント
使いやすさ	使いやすさ
証明書	**証明書**
FIPS 140-2	FIPS 140-2
NISTのアルゴリズム適合	NIST のアルゴリズム適合

基本的なオペレーション

Oracle Key Manager暗号化システムでは、以下のオブジェクトが管理されます。

- 鍵ポリシーと鍵グループ
- エージェント
- 鍵
- データ・ユニット

例1

極めて簡素化された以下の例では、StorageTek暗号化ドライブとともに使用された場合のシステムの基本的な動作を説明しています。

- バックアップ・アプリケーションまたはアーカイブ・アプリケーションが、新しいテープ・ボリュームにデータを書き込むリクエストを発行します。
- テープ・ボリュームは、クラスタに登録されて鍵グループへのアクセスを許可されている暗号化エージェントのドライブにマウントされています。鍵グループは、そのグループの鍵の特性を定義する鍵ポリシーと関連付けられています。
- エージェントは、マウントされているテープ・ボリュームに対応するデータ・ユニットと暗号化鍵の作成をリクエストします。KMAはエージェントのデフォルトの鍵グループに鍵を作成し、その鍵をエージェントに提供して、新しい鍵とデータ・ユニットを関連付けます。そして、鍵とデータ・ユニットをデータベースに保存し、これらの変更をクラスタ内のすべてのKMAに接続されるネットワーク全体にレプリケートします。
- エージェントは、すべてのデータ・パスで暗号化されていないデータを受け入れ、そのデータを新しい鍵で暗号化します。テープ・ボリュームのマウントが解除され、暗号化鍵がドライブのメモリから削除されます。
- 別の書込みオペレーションのために、テープ・ボリュームが再びマウントされます。
- エージェントは、最初のマウントでメディアに記録されたデータ・ユニットIDを読み取り、そのデータ・ユニットと関連する鍵をKMAにリクエストします。前の書込みで使用された鍵の状態、すなわち鍵ポリシーで定義されている状態と、アクティブ化後の経過時間に応じて、エージェントはその鍵を再度使用して新たなデータを暗号化するか、または現在の書込みオペレーションに使用する鍵を新たに作成するようKMAにリクエストします。

- 新たなデータが暗号化され、テープ・ボリュームのマウントが解除され、鍵がドライブのメモリから削除されます。
- 少し時間が経ってから、テープ・ボリュームに書き込まれたデータの読取りリクエストが発生します。
- テープ・ボリュームが暗号化ドライブに再度マウントされます。エージェントは、そのデータ・ユニットと関連付けられた鍵をKMAにリクエストします。エージェントは適切な鍵を選択し、データを復号化し、暗号化されていない状態のデータをアプリケーションのすべてのデータ・パスに戻します。テープ・ボリュームのマウントが解除され、鍵がドライブのメモリから削除されます。

以下のサブセクションでは、Oracle Key Managerの管理するオブジェクトと、それらのオブジェクトがどのように相互に作用し合うかを詳細に説明します。

鍵ポリシーと鍵グループ

Oracle Key Managerでは、鍵は第一に管理されるオブジェクトです。鍵グループは、データを暗号化するために使用される鍵の集合です。鍵グループはそれぞれ、その鍵グループ内のすべての鍵のライフ・サイクルを定義する鍵ポリシーと関連付けられています。

鍵ポリシーにより、以下の重要なパラメータが指定されます。

- **暗号化期間：**鍵がデータを暗号化できる期間です。
- **暗号化有効期間：**データの復号化のために鍵が必要な期間です。

暗号化期間と暗号化有効期間はどちらも、鍵がデータの暗号化に最初に使用された時点で開始されます。暗号化有効期間は、最低でも暗号化期間と同じ長さでなければならず、通常は暗号化期間よりもはるかに長い期間です。以下の図2をご覧ください。

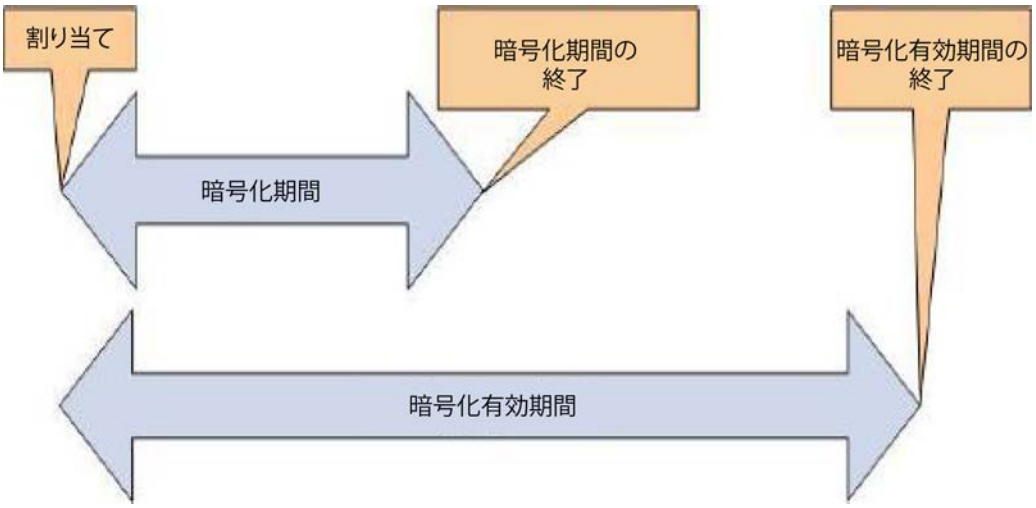

図2：暗号化期間と暗号化有効期間の関係

鍵は、暗号化期間が終了するまでデータを暗号化できます。そして、その鍵を使用して書き込まれたデータのみ復号化できます。暗号化有効期間の終了した鍵は、必要に応じてデータを復号化できますが、データを復号化しない場合は非アクティブ化されたものと見なされ、破棄される可能性があります。

極めてオープンなシステム環境では、1つの暗号化鍵を使用してすべてのデータをテープ・ボリュームに書き込み、そのテープ・ボリュームのすべてのデータが計画された有用年数を終えたときに、その鍵の暗号化有効期間が終了することが、テープ・ボリュームの目標です。以下の例は、鍵ポリシーの定義により、いかに鍵管理が簡素化されるか、そして鍵のライフ・サイクルを、その鍵が保護するデータのライフ・サイクルに限りなく近づけることができるかを示しています。

例2

オープン・システム環境のあるバックアップ・アプリケーションは、毎日20台のサーバーそれぞれから、50GBの圧縮不可能なデータをバックアップしています。各サーバーのバックアップには、異なるテープ・プールを備えた共通のドライブ・プールを使用し、プールの各テープが完全に一杯になってから、新しいテープを使用し始めます。各データは、1年間保存される必要があります。1台のサーバーのバックアップ・データで、500GBのテープ・ボリュームが10日ごとに一杯になります。鍵ポリシーは、10日の暗号化期間、54週の暗号化有効期間で作成されています。この鍵ポリシーを使用する鍵グループが作成され、この鍵グループは、プールのすべてのドライブのデフォルト鍵グループに割り当てられています。この構成では、同じ鍵を使用して、1つのテープ・ボリューム（使用されるドライブは問わない）に書き込まれるすべてのバックアップ・ファイルが暗号化されます。テープに最後に書き込まれたバックアップ・ファイルの保存期間が終了してから数日後に、この鍵は非アクティブ化されます。

例3

Multiple Virtual Storage（MVS）メインフレーム環境のバックアップ・アプリケーションでは、日次バックアップが実行されています。アプリケーションは、他のアプリケーションと共有されていないドライブを使用している特定のテープ・プールに割り当てられています。データ保存はOracle Key Managerによって管理され、期間は1年間に設定されています。データは、そのプール内の未知数のテープ・ボリュームに毎日分散されます。鍵ポリシーは、1年の暗号化期間、2年の暗号化有効期間で作成されています。この鍵ポリシーを使用する鍵グループが作成され、この鍵グループは、バックアップ・アプリケーション用プールのすべてのドライブのデフォルト鍵グループに割り当てられています。そのプールのドライブによって単一テープ・ボリュームに書き込まれたすべてのデータは、1年間同じ鍵を使用して暗号化されます。この鍵を"鍵1"と呼びます。"鍵1"の1年間の暗号化期間が終了し、テープ・ボリュームが次にマウントされたら、書込みオペレーションのリクエストを受けて、Oracle Key Managerは新たな鍵、"鍵2"を作成します。翌年このテープ・ボリュームに書き込まれたデータは、"鍵2"を使用して暗号化されます。"鍵1"を使用して書き込まれたデータには引き続きアクセスできます。ただし、"鍵1"はアクティブ化された日から2年後に非アクティブ化されます。

また鍵ポリシーでは、その鍵ポリシーと関連付けられた鍵グループから鍵をエクスポートできるか、もしくはその鍵グループに鍵をインポートできるかが指定されます。「パートナーの鍵転送」および「StorageTek Crypto Key Management System 1.xからOracle Key Manager 2.xへの移行」のセクションでは、これらの属性について詳しく説明しています。

エージェント

エージェントには、Oracle Key Managerエージェント・プロトコルが実装されています。暗号化や復号化オペレーションを実行する周辺ストレージ・デバイスなどが、エージェントの例です。エージェントは、Oracle Key Managerクラスタに登録されると、このクラスタのKMAに鍵をリクエストできるようになります。

テープ・ドライブのエージェント

テープ・ドライブは、非暗号化モードで出荷されます。お客様のサイトのドライブに暗号化の設定を行うには、登録の手続きを踏む必要があります。

登録手続きでは、以下の手順を実行する必要があります。手順1と手順2は準備のための手順であり、オペレーター権限のあるユーザーが、Oracle Key Manager GUIを使用して実行します。手順3は実際にエージェントの登録を行う手順であり、ドライブに対してVirtual Operator Panel（VOP）インタフェースを使用します。

- **手順1：**KMAのドライブにエージェントを作成し、エージェントIDとパスフレーズを指定します。
- **手順2：**エージェントに1つまたは複数の鍵グループを割り当て、1つの鍵グループをエージェントのデフォルト鍵グループに指定します。（エージェントが新たな書込み鍵の作成をリクエストした場合、エージェントのデフォルト鍵グループがその鍵を受領します。）
- **手順3：**VOPインタフェースを使用して、ドライブをオフラインにします。Configure→Drive Dataに移動し、「Encrypt」タブを選択します。以下の情報を入力します。
  - **トークンの使用：**「No」を選択します。[1]
  - **永続的な暗号化：**「Yes」を選択すると、エージェントを永続的に暗号化モードにします。「No」を選択すると、将来、暗号化モードを無効化できます。
  - **エージェントID：**手順1で指定したエージェントIDを入力します。
  - **パスフレーズ：**手順1で指定したパスフレーズを入力します。（このパスフレーズはプレーン・テキストで表示されます。ドライブを再登録するには新たなパスフレーズが必要なため、このパスフレーズを保護する必要はありません。）
  - **KMAのIPアドレス：**ドライブ・ネットワークのKMAポートのIPアドレスを入力します。（エージェントはこのIPアドレスを使用して、クラスタと通信してクラスタ内にあるすべてのKMAのIPアドレスを取得します。）

---

[1] 「No」を選択した場合は、後でVOPインタフェースを使用して、ドライブのリセットと暗号化の無効化を実行できます。ただし、手作業でこのモードの切り替えが行われるまでは、ドライブは暗号化モードのままです。

Oracle Key Managerクラスタに登録されたエージェントのあるドライブにテープ・ボリュームを初めてマウントする場合、エージェントは、そのテープ・ボリュームに書き込まれたデータを暗号化するために使用するデフォルト鍵グループに新たなデータ・ユニットと新たな鍵を作成するよう、KMAにリクエストします。2[2]通常、エージェントはKMAにテープ・ボリュームのバーコードID（VOLSER、または"ボリュームのシリアル番号"＋メディア情報）を渡します。KMAはデータ・ユニットのExternal Tagフィールドにこの IDを入力します。IDは、テープ・カートリッジの外側のバーコード・ラベルに表示されており、（自動ライブラリ設定において）ライブラリ・コントローラによってドライブに送信されるか、または、テープ上の米国国家規格協会（ANSI）のラベルから読み取ることができます。（VOLSERは、スタンドアロン・ドライブで使用される、ANSIラベルのないテープ・ボリュームに関連付けられたデータ・ユニットでは利用できません。）ただし、エージェントとクラスタのいずれも、データ・ユニットの検索や処理にこのタグを使用することはありません。External Tagフィールドによって、ユーザーは便利で使いやすい方法で、Oracle Key Manager GUIの表示する抽象的なデータ・ユニットを、物理的なテープ・ボリュームに関連付けることができます。

鍵がドライブのメモリに常駐している間に起きる鍵の状態遷移に、エージェントは気付きません。Oracle Key Managerは、管理しているオブジェクトの状態が変更されても、エージェントとの通信を開始しません。ドライブにテープ・ボリュームがマウントされている場合、エージェントはこのデータ・ユニットに関連付けられた鍵を送信するようKMAにリクエストします。エージェントは、鍵を受け取った時点で各鍵の状態を確認します。そのため、その後テープ・ボリュームがマウントされる際にエージェントがKMAから鍵を受け取るまでは、ドライブによって使用されている鍵の状態遷移にエージェントは気付きません。

エージェントは、処理する可能性のあるデータ・ユニットに関連付けられたすべての鍵グループにアクセスできなければなりません。エージェントが新たな鍵の作成をリクエストした場合、鍵は常にデフォルト鍵グループに割り当てられます。ただし、鍵の現在の状態が許可するならば、エージェントはデータの暗号化や復号化のためにアクセスできる他の鍵グループの鍵を使用することができます。たとえば、アクティブな書込み鍵を持つデータ・ユニットが書込みオペレーションのためにドライブにマウントされている場合、エージェントはこの鍵が属する鍵グループにアクセスできれば、この鍵を使用します。アクセスできない場合は、書込みリクエストを行うアプリケーションに書込みエラーが返される可能性があります。（ドライブがそのデータ・ユニットのアクティブな書込み鍵にアクセスできないテープの開始位置（BOT）から書込みを行う場合は例外です。この場合、KMAがドライブのデフォルト鍵グループに新たな鍵を提供し、書込み処理が行われます。）

鍵

データの暗号化に使用される鍵にはそれぞれライフ・サイクルがあり、そのライフ・サイクルは鍵に関連付けられた鍵ポリシーによって定義されています。鍵は、鍵が使用されるオペレーションを各段階で決定する一連の状態を遷移します。

---

[2] ドライブに送信された鍵は、鍵と関連付けられているデータ・ユニットがマウントされている間のみ、メモリに保存されます。マウントが解除されたら、そのデータ・ユニットと関連付けられているすべての鍵は、メモリから削除されます。

鍵の状態遷移

最初にOracle Key Managerは、運用前の鍵のプールをGenerated（生成済み）状態で生成します。鍵は使用可能になる前に、紛失から保護するために、複数ノード・クラスタに自動的にレプリケートする必要があります。単一ノード・システムの場合は、手作業でシステム・バックアップを作成しなければなりません。このいずれかの作業が完了した時点で、鍵はデータを暗号化できるようになり、Ready（準備完了）状態に変更されます。（単一ノード・システムでは鍵は自動で保護されないため、お客様は複数ノード・システムのみ購入できます。）

鍵は、最初にデータの暗号化に使用されると、Protect-and-Process（保護および処理）状態に遷移します。鍵の暗号化期間と暗号化有効期間はどちらも、この時点で開始されます。この状態の鍵は、データの暗号化と復号化に使用できます。暗号化期間が終了したら、鍵はProcess-only（処理専用）状態に遷移します。処理専用状態の鍵は、データの復号化にのみ使用できます。最終的には、鍵の暗号化有効期間は終了し、鍵はDeactivated（非アクティブ）状態に遷移します。状態遷移は完全に論理的なものですが、鍵の暗号化有効期間の終了と、鍵によって保護されるデータの有用年数の終了は同時に発生します。必要であれば、鍵はその後もデータの復号化に使用できます。

通常の運用では、鍵は鍵ポリシーで指定されているとおり、生成済み状態から非アクティブ状態へと遷移し、その後は永久に非アクティブ状態のままとなります。そのため、その鍵が保護するデータが存在する限り、データを復号化できます。ただし、オペレーターが鍵の通常のライフ・サイクルに介入せざるを得ない出来事があります。

鍵のライフ・サイクル中のいかなる時点においても、鍵の侵害が疑われる場合、または侵害が検知された場合は、コンプライアンス責任者は手動で情報漏えいを申告できます。Compromised（危殆化）状態の鍵は、データを暗号化することはできなくなります。ただし、必要に応じて復号化は可能です。暗号化されたテープ・ボリュームを紛失しても、そのテープ・ボリュームに関連付けられた鍵の漏えいを申告する必要はありません。データの暗号化に使用される鍵は、保護されているためです。ただし、保護および処理状態の鍵がうっかりエクスポートされ、鍵パートナーと共有された場合は、その鍵でこれ以上データを暗号化しないようにするために、鍵を危殆化状態にするのが適切かもしれません。

保存方針を強化するために、一部のデータへのアクセスを同時に拒否した方がよい場合もあります。これを行うには、非アクティブまたは危殆化状態の鍵を、手動でDestroyed（破棄）状態にします。鍵が破棄状態になったら、エージェントには送信されなくなります。破棄状態の鍵を含むバックアップが存在しない場合、鍵はCompletely Destroyed（完全破棄）状態になります。存在する場合は、Incompletely Destroyed（不完全破棄）状態になります。

Oracle Key Managerバックアップの管理は、Oracle Key Managerが制御できないため、鍵を不完全破棄状態から完全破棄状態にするには、オペレーターの介入が必要です。バックアップ・ファイルが手動で削除されたら、バックアップ・オペレーターはOracle Key Manager GUIを使用して鍵を破棄状態にすることができます。破棄状態の鍵を含むバックアップがすべて破棄されたら、鍵は完全破棄状態に遷移します。[3]

---

[3] 関連するすべてのバックアップが破棄されたら、その鍵の状態はシステムによって自動的に変更されます。ただし、システムは破棄状態の鍵を含むバックアップが実際に破棄されているかどうかを確認することはできません。

完全性のために、システムは、破棄状態のサブ状態がいずれ（完全または不完全）の鍵も危殆化状態にでき、Destroyed Compromised（破棄危殆化）状態に変更して同じサブ状態にすることもできます。破棄危殆化状態は、論理的には破棄状態と同様です。以下の図3をご覧ください。

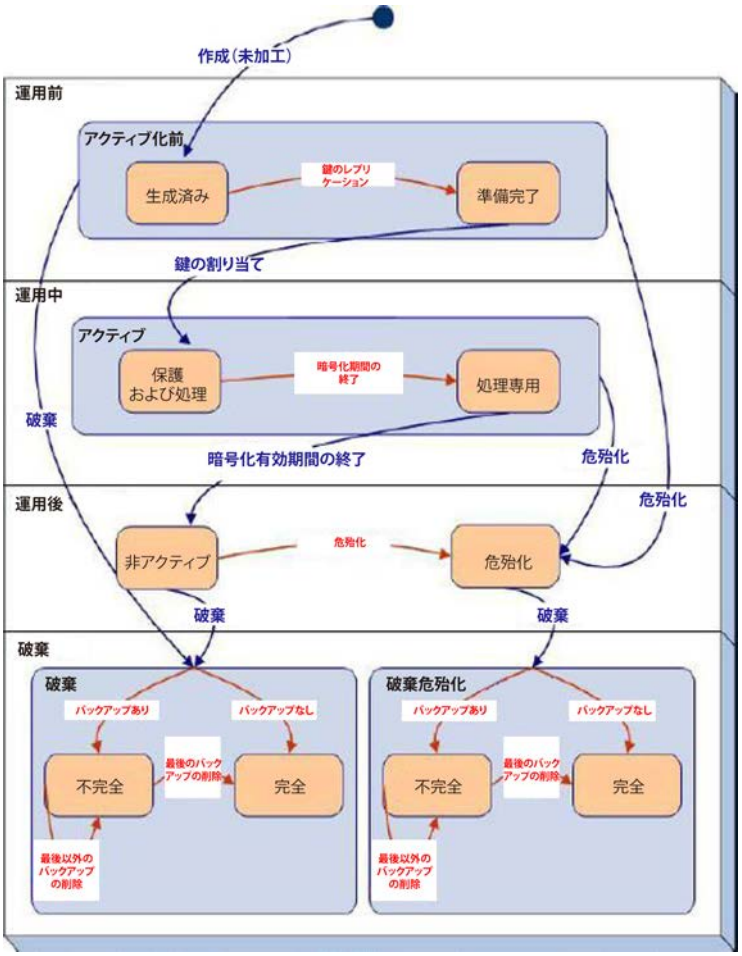

図3：暗号化鍵のライフ・サイクルにおける状態と状態遷移

鍵の破棄

破棄状態の鍵がOracle Key Managerから削除されると、その鍵が以前存在したことを証明するメタデータのみが残ります。鍵はデータを復号化できず、その鍵で暗号化されたすべてのデータは事実上破棄されます。そのため、鍵を破棄状態にするには、慎重な検討が必要です。

警告：鍵を破棄状態にすると、有用なデータへのアクセスを想定外に失う可能性があります。Oracle Key Managerの暗号化エージェントは、鍵のない過去のデータを配置することはできません。そのため、破棄された過去のデータの位置を示すテープのデータには、たとえデータの暗号化に使用された鍵がまだ存在しても、アクセスすることはできません。また、インポートされたStorageTek Crypto Key Management System 1.xのデータ・ユニットは、複数のデータ・ユニットと鍵を共有できます。1つのデータ・ユニットに関連付けられた鍵を破棄すると、他のデータ・ユニットのデータも破棄されるという予想外の悪影響が生じる可能性があります。

オペレーターは、1つまたは複数のデータ・ユニットを選択し、それらのデータ・ユニットに関連付けられたアクティブ化後の鍵を破棄できます。非アクティブ状態の鍵のみ破棄する、危殆状態の鍵のみ破棄する、またはその両方の鍵を破棄することができます。

副次的な悪影響が生じる可能性があるため、このオペレーションは慎重に行う必要があります。バックアップ・アプリケーションまたはアーカイブ・アプリケーションを使用してデータの期限を終了させる方法も同様の効果が得られ、意図せぬ結果を招くリスクはありません。

鍵の破棄が必要な場合、データ・ユニットと関連付けられたすべての鍵が非アクティブ状態となるまで待ってから、そのデータ・ユニットと関連付けられたすべての鍵を破棄するのがもっとも安全な方法です。この方法により、意図せぬデータ紛失のリスクを低減できます。1つの鍵のみ1つのデータ・ユニットに関連付けるようにすれば、容易にこの方法に従うことができます。

警告：オペレーター資格証明を持つすべてのユーザーが、非アクティブ状態または危殆化状態の鍵を破棄できます。

ある程度の保護機能も備えています。アクティブ状態の鍵を破棄することはできません。アクティブ状態の鍵は、破棄する前に危殆化状態にしなければなりません。鍵を危殆化状態にするには、コンプライアンス責任者の資格証明が必要です。ただし、コンプライアンス責任者の資格証明では、鍵を破棄することはできません。□アクティブ状態の鍵を破棄するには、コンプライアンス責任者とオペレーターの両方の資格証明が必要です。

オペレーターの資格証明を持つシングル・ユーザーは、非アクティブ状態の鍵を破棄できます。ただし、いかなるユーザーも、鍵を非アクティブ状態にすることはできません。そのような状態遷移は、鍵の暗号化有効期間の終了時にのみ発生します。この時期は、その鍵が保護するデータのライフ・サイクルにおける最終段階と同じ時期です。そのため、鍵の暗号化有効期間が、少なくともその鍵が保護するデータの予想有用年数と同じである限り、データがその有用年数を超えるまでは、シングル・ユーザー（不正ユーザー）がその鍵で暗号化されたデータを破壊することはできません。

データ・ユニット

*データ・ユニット*は、暗号化データを保存するあらゆるメディアのユニットです。Oracle Key Managerでは、データ・ユニットはテープ・ボリュームです。現在のOracle Key Managerシステムでは、鍵が作成されると、データ・ユニットと関連付けられます。その鍵が保護するデータが上書きされたり、鍵の重要データが破壊されたりしても、鍵は論理的にそのデータ・ユニットに関連付けられたままとなります。データ・ユニットの状態は、そのデータ・ユニットに関連付けられた鍵の状態によって変わります。一部の種類の暗号化ドライブでは、テープ開始位置からデータが上書きされたことが、ドライブからOracle Key Managerに通知されます。その場合、Oracle Key Managerは、そのデータ・ユニットと関連付けられた処理専用状態の鍵の使用中プロパティを変更できます。

データ・ユニットは、作成された当初はNo Key（鍵なし）状態です（データ・ユニットを作成するエージェントのリクエストは完了したものの、鍵を作成するエージェントのリクエストはまだ完了していません）。データ・ユニットの鍵が作成されるとすぐに、データ・ユニットはNormal（通常）状態に遷移します。通常状態のデータ・ユニットには、暗号化データを書き込むことができます。またデータ・ユニットは読取りが可能であり、新たなデータを書き込むことができます。既存のデータを新規データで上書きすることも、データのない場所に新たにデータを書き込むこともできます。この動作の詳細はエージェントによって決定され、クラスタからは認識されません。

保護および処理状態にある、データ・ユニットの鍵の暗号化期間が終了すると、データ・ユニットはNeeds Rekey（鍵再作成必要）状態に遷移します。[4]

テープ・ボリュームがマウントされると、エージェントは、まだ使用中のデータ・ユニットに関連付けられたすべての鍵をリクエストします。データ・ユニットが鍵再作成必要状態の場合、ドライブに送信された鍵の中に、保護および処理状態のものはありません。次にエージェントは、データ・ユニットに対して新たな鍵を作成するようKMAにリクエストし、データ・ユニットは通常状態に戻ります。データ・ユニットが一杯の場合、またはもう使用されていない場合は、保護および処理状態の鍵が期限切れとなった時点で、データ・ユニットは鍵再作成必要状態に戻り、通常はその状態が維持されます。ただし、データ・ユニットと関連付けられたすべての鍵が破棄された場合は、データ・ユニットはShredded（無効化）状態に遷移します。

無効化状態のデータ・ユニットからデータを読み取ることはできませんが、新たな鍵を使用してBOTから新規データを書き込むことができます。書込み後、データ・ユニットは通常状態に戻ります。以下の図4をご覧ください。

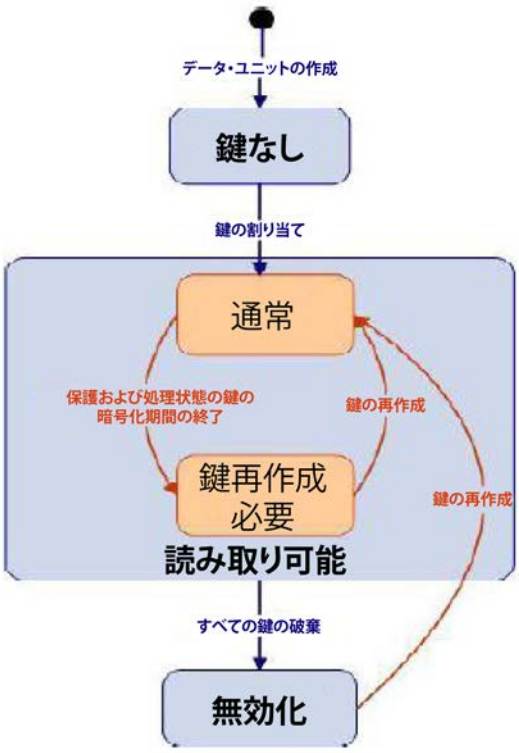

図4：単一の鍵を使用したデータ・ユニットの状態と可能な状態遷移

[4] この遷移は、暗号化期間の終了した鍵を使用して、データ・ユニットにデータを書き込む際に起きる可能性があります。オペレーションを管理しているアプリケーションが、テープ・ボリュームのマウント解除をリクエストするまで、エージェントは期限の切れた鍵を使用して、データ・ユニットにデータを書き込み続けます。

以下のようなイベントの流れを考えてみましょう。

- 新たなメディアが、バックアップ・オペレーションの一環としてOracle Key Manager暗号化ドライブにマウントされます。エージェントは、新たなデータ・ユニットを作成するようKMAにリクエストします。
- エージェントは、鍵（鍵1）を作成するようKMAにリクエストし、バックアップ・データを暗号化して書き込みます。データ・ユニットは通常状態に遷移します。
- その後、鍵1の暗号化期間が終了すると、データ・ユニットは鍵再作成必要状態に遷移します。
- 同じメディアが、別のバックアップ・オペレーションのために再度マウントされます。エージェントは、鍵（鍵2）を作成するようKMAにリクエストし、バックアップ・データを暗号化して書き込みます。データ・ユニットは再び通常状態に遷移します。
- その後、鍵2の暗号化期間が終了すると、データ・ユニットは鍵再作成必要状態に戻ります。
- 最終的には、鍵1の暗号化有効期間が終了し、鍵1は非アクティブ状態となります。
- 同様に、鍵2の暗号化有効期間が終了し、鍵2は非アクティブ状態となります。
- オペレーターが鍵1と鍵2を破棄し、データ・ユニットは無効化状態に遷移します。

図5では、この流れにおけるデータ・ユニットと2つの鍵の状態を視覚的に示しています。ダイアグラムは次の要素で構成されています。

- データ・ユニットの状態遷移はダイアグラムの中心に表示されています。
- 2つの鍵の状態遷移はダイアグラムの両側に表示されています。（鍵の状態のダイアグラムはこの例では簡素化されており、すべての可能な状態が表示されているわけではありません。）
- 黄色の円は、流れにおけるイベントを表しています。
- オレンジの矢印は、黄色のイベントによって引き起こされた鍵とデータ・ユニットの状態遷移を表しています。

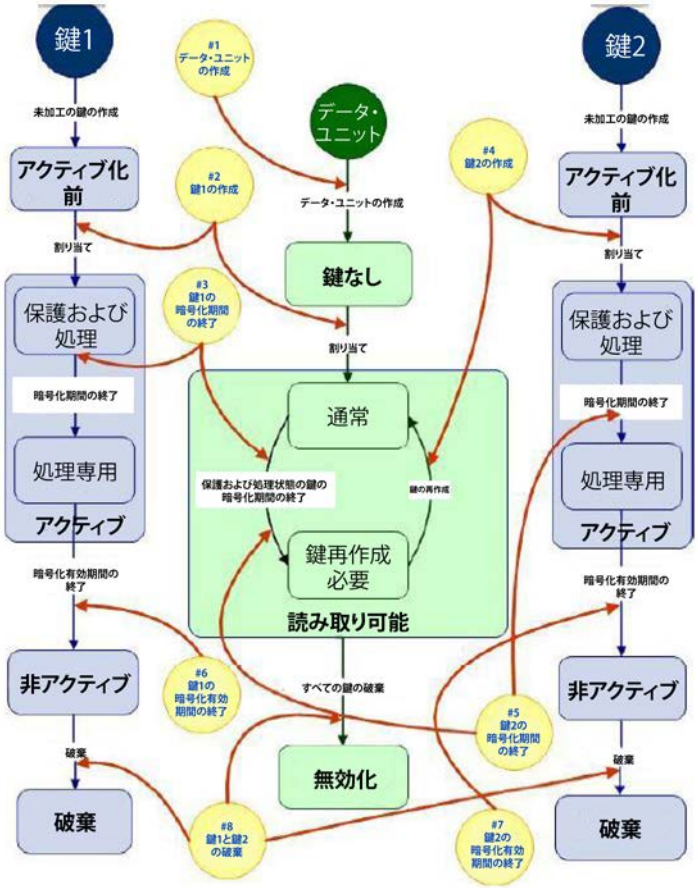

図5：データ・ユニットと2つの鍵の状態

データ・ユニットのリサイクル/消去

テープ環境では、テープ・ボリュームのデータが必要なくなった場合に、そのテープ・ボリュームをリサイクルまたは消去できます。テープ・ボリュームがリサイクルまたは消去されると、BOTから新たなデータが書き込まれ、メディア上の既存データは上書きされます。上書きされたデータはなくなり、まだ上書きされていないデータは、特別なリカバリ・ツールを使用した場合にのみリカバリできます。

そのため、それまでデータ・ユニットと関連付けられていた鍵は不要になります。テープ・ボリュームが再度マウントされたときにエージェントに送信される必要のある鍵の数を低減するために、エージェントはメディアのBOTから書き込むリクエストを受け取った際に、それまでデータ・ユニットと関連付けられており、保護および処理状態でないすべての鍵の関連性解除を行います。（エージェントは、既存の保護および処理状態の鍵の暗号化期間が終了するまで、その鍵を再利用して新たなデータを書き込みます。）

関連性解除という言葉は、文字どおりの意味ではありません。実際、関連性を解除された鍵は引き続きデータ・ユニットの鍵の一覧に表示されます。ただし、この操作により、次の2つの変化が生じます。

- 鍵のIn Use by Data Unit（データ・ユニットが使用中）属性が真から偽に変わります。
- エージェントがこのデータ・ユニットの鍵をリクエストしても、エージェントに鍵が送信されることはもうありません。

鍵がStorageTek Crypto Key Management System 1.xシステムからインポートされた場合は、複数のデータ・ユニットと関連付けられている可能性があります。関連性解除のオペレーションは、現在マウントされているデータ・ユニットにのみ適用されます。

セキュリティ機能

本ソリューションに実装されているさまざまなレベルのセキュリティについての詳細は、このホワイト・ペーパーでは扱っていません。以下のサブセクションにて、一部のセキュリティ機能のみ紹介します。

セキュアな通信

ドライブのエージェントとKMA間、新たにクラスタに追加されたKMAと既存のKMA間、およびユーザーとKMA間の通信プロトコルはすべて同じものです。いずれの場合も、システムは、通信を開始するエンティティのパスフレーズを使用して、チャレンジ/レスポンス・プロトコルを実行します。正常に実行された場合は、エンティティには証明書と対応する秘密鍵が渡されます。この証明書と秘密鍵を使用して、TLS 1.0（セキュアなソケット）チャネルを確立することができます。このセキュアなソケット・チャネルの確立は、2048ビットRSAを使用して行われます。このセッションを確立することで、AES 256ビット鍵と一致するエンドポイントが得られます。その後の通信はすべて、このAES 256ビット鍵を使用して暗号化されます。相互認証が実行されるため、接続の一方の末端によって、もう一方の末端が認証されます。

ドライブでは、暗号化エージェントの認証プロセスは、VOPの登録セッション中に実行されます。KMAでは、『Oracle Key Manager Installation and Service Manual』に記載されているように、認証はQuickStartプロセスの一環です。いずれの場合も、証明書と秘密鍵は保存され、ドライブまたはKMAのリブート後、セッションを再確立するために使用されます。Oracle Key Managerユーザーがログインする都度、このプロセスが繰り返されます。ユーザーが別のワークステーションからログインする可能性を想定しているためです。その後のすべての通信（エージェントが鍵をリクエストする、あるKMAが他のKMAに更新を送信する、またはOracle Key Manager GUIがKMAにリクエストを発行する際の通信）では、すでに確立されたセキュアなソケット・セッションが使用されます。

FIPS 140-2レベル3ハードウェア・セキュリティ・モジュール

KMAは、Oracle Sun Cryptographic Accelerator（SCA）6000カードとともに設定される場合もあります。このカードは、8レーンPCI Expressベースのホスト・バス・アダプタであり、KMAのスロットの1つに差し込まれます。このカードを使用することで、FIPS 140-2レベル3認証を受け、高度な暗号化セキュリティを備えたHSMが実現します。KMAは、FIPS 140-2レベル3モードで機能するようにカードを自動で設定し、管理します。

AES鍵ラップ

AES鍵ラップ（RFC 3994）は、鍵を暗号化する256ビット鍵とともに使用することで、対称鍵の作成、KMAへの保存、エージェントへの送信または鍵転送ファイル内の送信において、対称鍵を保護します。唯一の例外は、エージェント・プロトコル内でAES鍵ラップ固有の呼出しをサポートしていない古いエージェントの場合です。そのような古いエージェントでは、鍵はアンラップされ、保護されたTLSチャネル内でプレーン・テキストで送信されます。クラスタがFIPSモードに対応している場合は、AES鍵ラップが常に使用されるため、これらの古いクライアントは、クラスタから鍵を取得できません。

鍵のレプリケーション

クラスタの最初のKMAが初期化されると、未加工の鍵の大規模プールが生成されます。別のKMAがクラスタに追加されると、未加工の鍵が新しいKMAにレプリケートされ、データの暗号化に使用できるようになります。クラスタに追加される各KMAは、鍵のプールを生成し、そのプールを他のクラスタのメンバーにレプリケートします。すべてのKMAが、鍵のプール・サイズを維持するために必要な鍵を新たに生成するため、準備完了状態の鍵が常にエージェントによって使用可能です。保護および処理状態の鍵のないデータ・ユニットがドライブにマウントされると、ドライブのエージェントはクラスタのKMAと通信し、新たな鍵をリクエストします。準備完了状態の未加工の鍵がKMAのプールから取り出され、エージェントのデフォルト鍵グループと、ドライブにマウントされたテープ・ボリュームと関連付けられたデータ・ユニットに割り当てられます。このトランザクションによるデータベース更新は、クラスタ内のすべてのKMAと接続されるネットワーク全域にレプリケートされます。クリア・テキスト形式の重要データがネットワーク全域に送信されることは決してありません。

ロールベースのソフトウェア・アクセス

Oracle Key Managerへのアクセスは、特定のロールを実行する権限を付与されているユーザーに制限されています。システムには、以下のユーザーのロールが定義されています。

- **セキュリティ責任者：**セキュリティ設定、ユーザー、サイト、転送パートナーを管理します。
- **コンプライアンス責任者：**鍵ポリシーと鍵グループを管理し、鍵グループをエージェントや転送パートナーに割り当てます。
- **オペレーター：**エージェント、データ・ユニット、鍵を管理します。
- **バックアップ・オペレーター：**Oracle Key Managerデータベースのバックアップとリストア・オペレーションを実行します。

- **監査者：**Oracle Key Managerクラスタに関する情報を確認します。
- **定足数メンバー：**定足数が必要な保留中の操作を承認します。

単一のユーザー・アカウントが、複数のロールを実行する権限を持つ場合があります。また、複数のユーザー・アカウントが、同じロールを実行する権限を持つ場合があります。一部のオペレーション（信頼のおけるパートナー間での鍵の共有など）は、複数のユーザー・ロールが関与する複数ステップから成る場合があります。セキュリティを最大限に高めるためには、異なるユーザーが各ロールを実行する必要があります。利便性を最大限に高めるためには、1人の"スーパーユーザー"がすべてのロールを持つことができます。ロールを2人か3人のユーザーで分割するという妥協案により、許容できるレベルのセキュリティが実現するとともに、柔軟性も向上する可能性があります。

定足数保護

一部のオペレーションは極めて重要であり、さらなるレベルのセキュリティを必要とします。そのようなオペレーションとして、KMAのクラスタへの追加、KMAのアンロック、ユーザーの作成、ユーザーへのロールの追加、Oracle Key Managerのバックアップのリストア、鍵転送パートナーの設定などが挙げられます。このようなセキュリティを実装するために、システムでは、上記で説明したロールベースのアクセスに加えて、一連の鍵分割資格が使用されます。

鍵分割資格は、ユーザーIDとパスフレーズのペア一式と、システムが特定のオペレーションを完了するために必要な最低限のペア数との組み合わせから成ります。鍵分割資格はまた、"定足数"、および"定足数のしきい値"としての最小数ともいわれ、鍵分割資格が必要な操作は、"定足数操作"とも呼ばれます。

Oracle Key Managerでは、最大で10のユーザーIDとパスフレーズのペアを設定できます。定足数のしきい値は、1から、定義されているユーザーIDとパスフレーズのペア数までのいずれかの数に設定できます。1に設定すると、定足数操作は1人の定足数メンバーのみで完了できます。定義されているペアの合計数に設定した場合は、すべての定足数メンバーがその定足数操作を承認する必要があります。1よりも大きく、ペアの合計数よりも小さい数（合計数が5の場合は3など）に設定するのがもっとも一般的です。そうすることで、その定足数操作を完了するのに、2人以上の定足数メンバーが必要となり（1人の場合はその人が不正なメンバーである可能性も有）、あるメンバーが承認できないといった状況にも対応できます。[5]

---

[5] 定足数に定義されているユーザーIDとパスフレーズのペアは、上記で説明したユーザー・ロールとは関連がありません。定足数メンバー資格を持つユーザーは、まずOracle Key Manager GUIを使用してクラスタにログインし、ユーザーIDとパスフレーズのペアを入力して操作を承認する必要があります。

鍵管理

鍵ポリシーと鍵グループ

エージェントは、データの暗号化に必要な鍵をデフォルト鍵グループに作成するよう、KMAにリクエストします。この鍵グループに関連付けられた鍵ポリシーでは、これらの鍵のライフ・サイクルと、鍵が鍵グループからエクスポートされるか、鍵グループにインポートされるかが定義されます。先ほども説明したように、オープン・システム環境では、暗号化期間が十分な期間となるように鍵ポリシーを定義することが推奨されます。そうすることで、1つのデータ・ユニットのすべてのデータを同じ鍵で暗号化できるようになります。その結果、システム内の鍵の合計数が低減され、1つのデータ・ユニットのすべてのデータを、個々のファイルごとにではなく、まとめて管理できるようになります。

テープが一杯になるまで少量のデータが間隔を置いて書き込まれる場合は、暗号化期間を最低3カ月以上に設定するとよいでしょう。たとえば、2週間に1度支払われる給与のデータ1年分が、単一のデータ・ボリュームに保存されるとします。このデータ・ユニットのすべてのデータが同じ鍵を使用して書き込まれるようにするには、より長期間の暗号化期間を定めた鍵ポリシーが必要です。

大半のオープン・システム・バックアップ・アプリケーションと、一部のMVSメインフレーム・アプリケーションでは、1つのデータ・ユニットが一杯になってから、別のデータ・ユニットにデータが書き込まれます。そのため、データ・ユニットが一杯になるまでの期間は通常極めて短期間です。ただし、暗号化期間を必要以上に長く設定しても問題はありません。暗号化期間が、データ・ユニットが一杯になるまでの期間より長くても、鍵は再利用されず、テープが一杯になった時点で暗号化期間は事実上終了します。しかしながら、暗号化期間を推奨されるよりも短く設定した場合、エージェントはデータ・ユニットが一杯になる前に何度も鍵を作成します。その結果、多数の鍵が作成され、Oracle Key Managerのパフォーマンスは低下します。

Virtual Tape Control System/Virtual Tape Subsystem（VTSS）のVirtual Storage Manager（VSM）アプリケーション、およびその他のMVSメインフレーム・アプリケーションでは、必ずしもテープのデータ・ユニットが一杯になってから別のデータ・ユニットに書き込むわけではありません。そのため、より長期間の暗号化期間をデータ・ユニットに設定するのは理にかなっています。そうすることで、各データ・ユニットに作成される鍵の数を最小限にとどめることができるからです。VSMによって仮想テープ・ボリュームのかたちでMultiple Virtual Cartridges（MVC）に書き込まれるデータは、VTSSによって圧縮された後、暗号化エージェントによって暗号化されます。

複数の鍵グループで、同じ鍵ポリシーを使用することもできます。ただし、多くのお客様は、Oracle Key Managerクラスタごとに1つの鍵グループがあれば十分です。鍵グループが1つあれば、クラスタに登録されているすべてのドライブが、クラスタに認識されているいかなるデータ・ユニットも読み取れることが保証されます。企業内の他のクラスタとデータを共有する場合、または他の企業パートナーとデータを共有する場合、属性セットからのエクスポートを持つ新たな鍵グループが作成されます。共有される鍵は、この新しい鍵グループに移動され、鍵グループは、鍵転送パートナーに割り当てられます。（「パートナーの鍵転送」のセクションでは、パートナーの鍵転送オペレーションについてさらに詳しく説明しています。）

鍵管理システム・クラスタ

Oracle Key Managerを使用すると、ユーザーはクラスタを柔軟に構築できるようになるため、権限のあるユーザーのアクセスと管理の容易性を保証しながらも、セキュアなデータ保護を実現できます。KMAをクラスタ化することで、ワークロードのバランスと、ユーザー、エージェント、鍵ポリシー、鍵グループについての情報や重要データのレプリケーションが可能になります。企業は、同じサイト内の異なる場所に、または地理的に離れた複数のサイトに、エージェント（暗号化テープ・ボリュームなど）を持つことができます。以下のガイドラインに準拠することで、効率的で信頼性のあるパフォーマンスを確保できます。

- ネットワークの遅延を軽減するために、エージェントのプールにサービスを提供するKMAは、エージェントと同じネットワーク・サブネットに接続されていなければなりません。
- ワークロードを分散するため、およびKMAを停止できるようにするために（ソフトウェアのアップグレードやハードウェアの障害時）、エージェントの各プールは少なくとも2台のKMAにアクセスできなければなりません。
- 重要なデータを紛失するような大惨事を避けるために、地理的に離れた2つ以上のサイトに配置されたKMAはクラスタ化される必要があります。そうすることで、サイト全体が使用できなくなるような災害時にもビジネスの継続性が保証されます。

どのようなサイトで生成された重要データも、別の離れたサイトにレプリケートされ、保管されることが想定されます。あるサイトが使用できなくなった場合は、このバックアップ・データを他の運用サイトに送信することができます。暗号化データ（テープ・ボリュームなど）と関連付けられたデータ・ユニットと鍵は、関連サイトのKMAによって認識されるため、業務の継続に必要な暗号化データは利用可能です。サイトの運用が再開したら、クラスタの破損した部分は、同じ場所または別の場所に容易にリストアできます。「鍵管理アプライアンスのリカバリ」のセクションでは、このリストア方法について説明しています。

パートナーの鍵転送

定期的にデータを共有している企業内のサイトのKMAをクラスタ化することで、どのサイトで使用されている鍵も、自動的にすべてのサイトで使用できます。他のサイトで鍵を使用する場合、希望どおりに鍵を共有するには、テープ・メディアのみをサイト間で転送する必要があります。ただし、企業内のOracle Key Managerクラスタ間、または企業パートナーとの間で、暗号化データを共有するニーズが発生する場合があります。Oracle Key Managerを使用すれば、鍵を共有できるセキュアなメカニズムが実現します。この鍵の共有メカニズムでは、各パートナーがそれぞれのサイトでOracle Key Managerによって生成された公開鍵と秘密鍵のペアを所有します。共有されるデータ・ユニットと鍵の一覧を含む鍵転送ファイルが、送信者のサイトで生成されます。このファイルは、受信者の公開鍵を使用して暗号化され、送信者の秘密鍵を使用して署名されるため、受信者のみが共有鍵にアクセスできるとともに、受信者は予期する送信者からそのファイルが送信されたことを確認できます。手順は以下のとおりです。

- 各サイトのセキュリティ責任者は、Oracle Key Managerによって生成された公開鍵を取得するか、またはOracle Key Manager GUIを使用して新たな公開鍵と秘密鍵のペアを作成します（公開鍵の情報のみが表示されます。）パートナーは公開鍵を交換します。各鍵に対して、指紋が送信元のサイトで生成され、受信先のサイトで計算されます。この指紋は、鍵の転送中に破損していないかどうかを確認するために、サイト間で比較される必要があります。セキュリティのために、この指紋は

公開鍵と一緒には送信されませんが、後から口頭で確認されます。

- 各サイトでは、セキュリティ責任者がOracle Key Manager GUIを使用して鍵転送パートナーを作成し、パートナー・サイトから受信した公開鍵を供給します。鍵転送パートナーの作成は定足数操作のため、しきい値の数の定足数メンバーがこの操作を承認する必要があります。パートナーの鍵が入力されたら、その鍵の指紋がOracle Key Managerによって計算されます。転送中に破損していない場合は、この指紋は公開鍵が作成された際にパートナーのサイトで生成された指紋と一致します。
- 各サイトはその鍵転送パートナーに、鍵がエクスポートされる、または鍵をインポートする、1つまたは複数の鍵グループを割り当てます（鍵は双方向に転送できるため、1つのサイトがインポート・サイトとエクスポート・サイトの両方を兼ねる可能性があります。）これらの鍵グループは、希望するエクスポート・オペレーションとインポート・オペレーションを許可する鍵ポリシーに関連付けられる必要があります（鍵ポリシーのこの属性が、鍵ポリシーの作成時に設定されていない場合は、変更できます。）
- 送信元サイトのオペレーターは、共有するデータ・ユニットと鍵を含む1つまたは複数の鍵転送ファイルを作成します。鍵は、以下の条件を満たす場合に限り、エクスポートできます。
  - 転送パートナーに関連付けられた鍵グループに属する。
  - アクティブ（保護および処理、または処理専用）、非アクティブ、または危殆化状態であり、In Use by Data Unit属性が真に設定されている。

各ファイルは、共有されるデータ・ユニットを選択することで作成されます。定められた条件を満たす鍵と関連付けられたデータ・ユニットのみ、転送ファイルにインクルードでき、定められた条件を満たすそれらのデータ・ユニットに関連付けられた鍵のみ、転送ファイルにインクルードされます。[6]

- 送信者のクラスタは、受信先のサイトの公開鍵を使用して鍵転送ファイルを暗号化し、送信者の秘密鍵を使用してそのファイルに署名します。
- 送信者は、鍵ファイルと関連のデータ・テープを受信者に転送します。
- 受信者はデータ・テープをライブラリに入力し、テープ・ボリュームをバックアップ・アプリケーションにインポートします。
- 受信者は鍵転送ファイルを管理ステーションにロードし、鍵と関連データ・ユニットをそのファイルからインポートし、宛先鍵グループとして鍵パートナー（送信者）に割り当てられる鍵グループを指定します。（鍵のインポートには定足数の認証は必要ありません。）

---

[6] 共有プロセスを簡素化するには、共有するデータを新規の、またはリサイクルされたテープ・ボリュームに書き込み、これらの各データ・ユニットに関連付けられた鍵の鍵グループを、エクスポートの鍵グループに変更し、これらすべてのデータ・ユニットの鍵をエクスポートします。このプロセスにより、共有しようとしているすべてのデータは、受信先のサイトからアクセスでき、共有しようとしているデータのみが、転送パートナーに送信されます。

- 受信者のKMAは、転送ファイルを復号化し、送信元の送信者を確認します。KMAはデータベースに共有鍵とデータ・ユニットのエントリを作成し、新しい鍵をそれぞれ適切なデータ・ユニットと関連付けます。
- インポートされた鍵とデータ・ユニットは、受信者のクラスタ内のすべてのKMAにレプリケートされます。多くの要素が共有される場合、このプロセスには時間がかかる場合があります。十分な時間が経過してレプリケーションが完了するまでは、インポートされた鍵が必要なテープの読取りは失敗に終わる可能性があります。[7]

鍵管理アプライアンスのリカバリ

Oracle Key Managerでは、個々のKMAのリカバリと、Oracle Key Managerクラスタ全体のリカバリという、2種類のリカバリが可能です。単一のKMAのリカバリは、各ドライブ・プールに対して1台のKMAが運用されている限りは、残りのクラスタに影響を及ぼすことなく完了できます。さらに、Nノード・クラスタのN-1ノードのリカバリは、重要データを失うことなく達成できます。以下のサブセクションでは、単一のKMAのリカバリが必要なシナリオを説明しています。クラスタ全体のリカバリについては、「ディザスタ・リカバリ」のセクションで説明しています。

ソフトウェア・アップグレード

ソフトウェア・アップグレードは、アクティブな暗号化エージェントに対するKMAサービスの中断を最小限に抑えながら行うことができます。KMAのソフトウェアをアップグレードするには、Oracle Key Managerソフトウェア・アップグレード・ファイルのアップロードと適用、および新規ソフトウェアのアクティブ化という2つの手順を実施します。アップグレード・ファイルはサイズが非常に大きい可能性があるため、KMA1台ずつアップグレード・ファイルをアップロードし、適用する必要があります。新たなソフトウェアをアクティブ化するには、KMAサーバーをリブートする必要があるため、各エージェント・プールに接続されたKMAが常に少なくとも1台はアクティブな状態となるよう、時間をずらしてアクティブ化する必要があります。各KMAがオンラインになると、オフライン中にクラスタで完了した更新はKMAにレプリケートされるため、クラスタのすべてのKMAは、再同期化されます。

ネットワークの切断

1台のKMAが管理ネットワークから切断された場合、クラスタ内の残りのKMAは、引き続き切断されたKMAへの通信を試み、監査イベント・ログで通信エラーを報告します（上記で説明したように、新たなソフトウェアのアクティブ化にはサーバーのリブートが必要ですが、このリブートでも同じ動作が発生します。）エージェントは、サービス・ネットワークに接続された残りの運用中KMAに、中断することなく通信します。KMAがネットワークに再接続されると、オフライン中にクラスタで完了した更新が、KMAにレプリケートされます。

---

[7] データ・ユニットと鍵IDは、作成しているクラスタのKMAのIDを含みます。そのため、受信者のクラスタにインポートされたデータ・ユニットと鍵は、受信者のクラスタによって作成されたデータ・ユニットと鍵とは異なるIDを持ちます。

ハードウェア障害

KMAサーバーに障害が発生した場合のリカバリ手順は、サーバーの種類と、KMAで実行されている鍵管理ソフトウェアのバージョンによって異なります。

- **Netra SPARC T4-1サーバー：**ディスク・ドライブ、SCA 6000カード、マザーボード、電源をはじめとするサーバーのコンポーネントに障害が発生した場合は、そのコンポーネントを交換できます。
- **Sun Fire X4170 M2サーバー：**ディスク・ドライブ、SCA 6000カード、マザーボード、電源をはじめとするサーバーのコンポーネントに障害が発生した場合は、そのコンポーネントを交換できます。
- **Oracle Key Manager 2.3以降を実行しているSun Fire X2100 M2またはX2200 M2サーバー：**ディスク・ドライブまたはSCA 6000カードに障害が発生した場合は交換できます。その他のコンポーネントに障害が発生した場合は、システム全体を交換する必要があります。
- **StorageTek Crypto Key Management System 2.1または2.2.xを実行しているSun Fire X2100 M2またはX2200 M2サーバー：**SCA 6000カードに障害が発生した場合は交換できます。その他のコンポーネントに障害が発生した場合は、システム全体を交換する必要があります。
- **StorageTek Crypto Key Management System 2.0.2以前を実行しているSun Fire X2100 M2またはX2200 M2サーバー：**どのようなコンポーネントに障害が発生した場合も、システム全体を交換する必要があります。

KMA全体の交換

KMA全体を交換する方法は以下のとおりです。まず、KMAをクラスタから削除し、残りのKMAがそのKMAへの通信を試みることがないようにします。Oracle Key Managerコンソールにまだアクセスできる場合は、KMAを工場出荷時の設定にリセットするオプションを実行します。このリセット・オペレーションにより、KMAは工場出荷時の設定に戻ります。Oracle Key Manager 2.xを実行しているKMAでは、このオペレーションにより、追加的なセキュリティの予防措置として、サーバーのハード・ディスクをスクラブするオプションが提供されます。機能していないサーバーの処分は、お客様が行います。[8]

---

[8] リセット・オペレーションは、KMAを別のクラスタに移動する前に行うこともできます。KMAがリセットされると、サービス・プロセッサ・ネットワーク構成がそのままである以外は、まさに工場から出荷されたばかりの新規のKMAのようになります。これらのネットワーク・パラメータは、QuickStartプロセス中にリセットできます。オプションのディスク・スクラブを使用して、以前のクラスタのトレースをすべて削除できます。

『*Oracle Key Manager Installation and Service Manual*』に記載されているように、交換したKMAサーバーを設定し、クラスタに追加します。新たなサーバーがクラスタに認識されると、クラスタ情報がそのサーバーにレプリケートされ、サーバーはクラスタのアクティブ・メンバーとなります。

ディスク・ドライブの交換

KMAのディスク・ドライブを交換する方法は以下のとおりです。まず、KMAをクラスタから削除し、残りのKMAがそのKMAへの通信を試みることがないようにします。Oracle Key Managerコンソールにまだアクセスできる場合は、KMAを工場出荷時の設定にリセットするオプションを実行します。このリセット・オペレーションにより、KMAは工場出荷時の設定に戻ります。さらに、追加的なセキュリティの予防措置として、サーバーのハード・ディスクをスクラブするオプションが提供されます。機能していないディスク・ドライブの処分は、お客様が行います。[9]

『Oracle Key Manager Installation and Service Manual』に記載されているように、Oracle Key Managerソフトウェアを使用してあらかじめロードされた新規ディスク・ドライブをKMAにインストールし、KMAをクラスタに追加します。サーバーがクラスタに（再び）認識されると、クラスタ情報がそのサーバーにレプリケートされ、サーバーはクラスタのアクティブ・メンバーとなります。

鍵管理ソリューションのバックアップ

Oracle Key Managerのバックアップには、コア・セキュリティ・バックアップとデータベース・バックアップという2種類のバックアップが伴います。以下のサブセクションでは、それぞれのバックアップの目的と、それらをいつ行うべきかを説明しています。

コア・セキュリティ・バックアップ

コア・セキュリティ・バックアップでは、システムのマスター鍵と定足数情報がバックアップされます。このバックアップは、システムがデータベース・バックアップからリストアされる場合に必要であり、クラスタの設定後すぐに、また定足数に変更があった場合は常に、実行する必要があります。

「セキュリティ機能」のセクションで説明したように、定足数メンバーのパスフレーズを使用して、システムのマスター鍵を保護します。マスター鍵は、N個（定足数の数）に分割され、鍵全体は、M個（定足数のしきい値）から再構築できます。各定足数メンバーのパスフレーズを使用して、N個のマスター鍵のうちの1つを暗号化するために使用される1つの鍵を生成します。N人の定足数メンバーのM個のユーザーIDとパスフレーズが揃うと、マスター鍵を再構築できます。このマスター鍵は、重要なセキュリティ・オペレーションを完了するために必要となります。

---

[9] リセット・オペレーションは、KMAを別のクラスタに移動する前に行うこともできます。KMAがリセットされると、サービス・プロセッサ・ネットワーク構成がそのままである以外は、まさに工場から出荷されたばかりの新規のKMAのようになります。これらのネットワーク・パラメータは、QuickStartプロセス中にリセットできます。オプションのディスク・スクラブを使用して、以前のクラスタのトレースをすべて削除できます。

コア・セキュリティ・バックアップ・ファイルには、上記で説明したように分割され、ラップされたシステムのマスター鍵が含まれます。このファイルは、判読可能な形式のXMLファイルです。定足数メンバーのユーザーIDはプレーン・テキストであり、定足数メンバーを識別するのに便利です。ファイル内の鍵とパスフレーズの情報は、セキュアに暗号化されています。とりわけマスター鍵は厳重に保護されています。マスター鍵を再構築するには、マスター鍵を分割するために使用されたアルゴリズム、必要な定足数メンバーのサブセットのユーザーIDとパスフレーズ、これらのパスワードから鍵を生成するために使用されたアルゴリズム、およびこれらの鍵で分割された鍵を暗号化するために使用されたアルゴリズムにアクセスする必要があります。このように厳重に保護されていても、コア・セキュリティ・バックアップ・ファイルは、極めてセキュアな場所に保管しなければなりません。定足数情報は、定足数メンバーの追加や削除、定足数メンバーのパスフレーズの漏えいなどが発生した場合は変更する必要があります。定足数メンバーが変更されたら、新しいコア・セキュリティ・バックアップを作成し、以前のコア・セキュリティ・バックアップ・ファイルのコピーをすべて、完全に破棄する必要があります。

コア・セキュリティ・バックアップのオペレーションは、Oracle Key Manager GUIまたはCLIを使用して実行します。このオペレーションで生成されたコア・セキュリティ・バックアップ・ファイルのファイル名は、データベースに保存されます。ただし、コア・セキュリティ・バックアップ・ファイルそのものは、KMAサーバー上ではなく、Oracle Key Managerの管理ワークステーション、またはその管理ワークステーションからアクセスできるリモートの場所に保管され、完全にOracle Key Managerシステムの外部で管理されます。

必要なレベルの保護を実現するには、コア・セキュリティ・バックアップ・ファイルをサム・ドライブに保存し、確実に信頼のおける従業員に渡します。その従業員は、ファイルを常に携帯します。定足数の変更が必要になったら、最初のバックアップ・ファイルを保存していたサム・ドライブを破棄し、今後そのファイルにアクセスできないようにします。新しいコア・セキュリティ・バックアップ・ファイルを作成し、新たなサム・ドライブに保存し、同様のセキュリティ・レベルで保護します。

Oracle Key Managerのバックアップ

極めてビジネスクリティカルなシステムでは、データベースのセキュリティは、通常のバックアップと更新のジャーナル・ファイルによって保護されます。この方法により、バックアップのリストアが必要な場合は、もっとも最近の変更もリストアに含まれます。このようなシステムのバックアップは必須です。データベースのシングル・インスタンスのみが存在する可能性があるためです。

各KMAは、内部データベースにOracle Key Managerクラスタ情報を保存します。このOracle Key Managerデータベースのセキュリティは、地理的に離れたサイトにある複数のクラスタ化されたKMAにデータベースをレプリケートすることで実現されます。Oracle Key Managerデータベースをバックアップからリストアする作業は、すべてのサイトのすべてのKMAが同時に破壊された場合に限って必要です。Oracle Key Manager GUIの提供するデータベース・バックアップ機能を使用すると、データベースのポイント・イン・タイム・コピーを作成できるため、そのような状況で使用できます。

データベースのバックアップは、バックアップ・オペレーターの資格証明を持ち、クラスタ内の単一のKMAに接続しているユーザーが行います。バックアップ・オペレーションにより、ユーザーが接続しているKMAに常駐するデータベース・インスタンスのコピーが作成されます。すべてのエージェントが少なくとも2台のKMAにアクセスできる限り、このオペレーションがエージェントのオペレーションに悪影響を及ぼすことはありません。クラスタ内の他のKMAは、バックアップ・オペレー

ションが進行している間も中断することなくサービスを提供します。バックアップを作成しているKMAのデータベース・インスタンスは、オペレーションの完了後、再同期化されます。データベースのバックアップでは、バックアップ・ファイルとバックアップ鍵ファイルという2つのファイルが生成されます。バックアップ・ファイルは、バックアップ鍵ファイルに保存された鍵を使用して暗号化されたデータベースのコピーです。バックアップ鍵ファイルのバックアップ鍵は、コア・セキュリティ・バックアップ・ファイルに含まれるシステムのマスター鍵を使用して暗号化されます。

そのため、バックアップ・ファイルからOracle Key Managerクラスタをリストアするには、コア・セキュリティ・バックアップ・ファイル、バックアップ鍵ファイル、および必要な定足数メンバーのサブセットの存在がすべて必要となります。定足数メンバーのパスフレーズは、システムのマスター鍵を復号化するのに必要であり、システムのマスター鍵は、バックアップ鍵を復号化するのに必要であり、バックアップ鍵は、バックアップ・ファイルを復号化するのに必要です。□作成されたバックアップ・ファイルのファイル名は、データベースに保存されます。ただし、バックアップ・ファイルそのものは、KMAサーバー上ではなく、Oracle Key Managerの管理ワークステーション、または管理ワークステーションがアクセスできるリモートの場所に保管されます。これらのファイルは、完全にOracle Key Managerの制御の範囲外にあり、慎重に管理されなければなりません。バックアップ・ファイルは、バックアップされる必要があります。また、バックアップ・ファイルをアンロックするのに必要なコア・セキュリティ・バックアップ・ファイルとは別に、クラスタから離れた場所で保管されなければなりません。現在システムでは、バックアップ・スケジュールを自動化するユーティリティは提供されていませんが、間もなく利用可能になります。

データベースのジャーナル・ファイルは存在しないため、別のKMAによって行われた更新のうち、バックアップを実行しているKMAにまだレプリケートされていないものや、バックアップが作成された後に行われた更新は、そのバックアップがクラスタをリストアする際のバックアップ・ソースとして使用される場合には、インクルードされません。ただし、リストアされたシステムでは、バックアップにインクルードされていない鍵とデータ・ユニットの情報をリカバリできる場合があります。

例4

1台のKMAで、鍵と新たなデータ・ユニットが作成され、それと同時に、クラスタ内の他のKMAでデータベース・バックアップが開始されます。バックアップ・オペレーションでは、バックアップを実行しているKMAのデータベースの状態が取得され、新たな鍵とデータ・ユニットはインクルードされません。その後、災害によりOracle Key Managerクラスタ全体が失われ、このバックアップを使用してクラスタがリストアされます。バックアップの進行中に書き込まれたデータをリストアするリクエストが新しいクラスタに発行されます。ドライブはデータ・ユニットIDをメディアから読み取り、そのデータ・ユニットと関連付けられたすべての鍵をリクエストします。Oracle Key Managerにはそのデータ・ユニットのレコードが存在しないため、ドライブはリクエストされたデータと関連付けられた特定の鍵をリクエストします。Oracle Key Managerには、割り当てられているこの鍵のレコードも存在しません。ただし、バックアップが作成される前に元のクラスタで生成された、割り当てられていない鍵（事前に生成された準備完了状態の鍵）の一覧は存在します。Oracle Key Managerはこのリストで必要な鍵のIDを見つけると、これがリカバリ・オペレーションであると見なし、新たなデータ・ユニットを作成し、鍵を新たなデータ・ユニットと関連付け、その鍵をドライブに提供します。

シナリオによっては、割り当てられた鍵を、データベースのバックアップ・コピーからリカバリできない可能性があります。とはいえ、複数のアクティブなデータベース・コピーが地理的に離れた

場所に保管されていることで、極めて高度なセキュリティが実現しています。さらに、鍵のデータは、クラスタ全体でレプリケートされるまでは、決して割り当てられることはありません。そのため、システムでは、極めて高い信頼度で重要データにアクセスできることが保証されます。

警告：コア・セキュリティ・バックアップ・ファイルなくしてバックアップはリストアできません。しかしながら、そのファイルに保存されている、定足数の必要なしきい値のユーザーIDとパスフレーズのペアが提供される限りは、どのようなコア・セキュリティ・バックアップ・ファイルも、バックアップからクラスタをリストアするために使用できます。そのため、古いコア・セキュリティ・バックアップ・ファイルを破棄するとともに、現在のコア・セキュリティ・バックアップ・ファイルのコピーを複数、それぞれ別の場所に、かつデータベース・バックアップ・ファイルの保存場所とは異なる場所に厳重に保管する必要があります。

ディザスタ・リカバリ

地理的に離れた複数の場所に分散されたOracle Key Managerのクラスタ化環境では、災害によりクラスタ全体が破壊されるリスクが大幅に軽減されます。クラスタ全体の再構築が必要な起こりそうもない事態においても、最新のデータベース・バックアップからOracle Key Manager環境を再構築することで、ほとんどの鍵データをリカバリできます。

多くの企業は、サード・パーティのディザスタ・リカバリ（DR）サイトのサービスを採用しているため、可能な限り迅速に業務を再開できます。定期的に抜き打ちのDRテストを行うことで、大惨事からリカバリする準備がその企業でどの程度整っているかが分かります。多数のシナリオが存在しますが、そのうちの3つを紹介します。

- **シナリオ1：**企業は、DRテスト・サイトにおいて、Oracle Key Managerクラスタの一部であるKMAを保守しています。テスト・サイトでは、KMAへのネットワーク・アクセスを持つドライブのプールが提供されます。
- **シナリオ2：**企業のすべてのKMAが破壊されています。DRテスト・サイトでは、スタンドアロンのKMAへのネットワーク・アクセスを持つドライブのプールが提供され、このスタンドアロンのKMAは、別の時間には別のクライアント企業によって使用されています。
- **シナリオ3：**企業は、DRサイト1において、Oracle Key Managerクラスタの一部であるKMAを保守しています。しかしながら、シナリオ2で説明した、ドライブのプールに接続されたスタンドアロンのKMAのあるサイト2で、DRテストが実行されます。

シナリオ1

このシナリオは最適です。すべてのサイトが破壊されても、企業のOracle Key Managerデータベースは無傷だからです。データセンターと重要なビジネス・システムのリストアに集中します。保管していたテープをDRテスト・サイトに移動します。Oracle Key Manager GUIを実行するラップトップをKMAネットワークに接続し、DRサイトの提供するドライブを企業のKMAに登録します。オペレーターの資格証明を持つユーザーが必要です（ただし、定足数は不要です）。必要なバックアップ・アプリケーションを実行するホストをDRサイトのドライブに接続し、企業のデータセンターをリストアするために使用します。

Oracle Key Managerデータベースは無傷なため、企業のOracle Key Managerクラスタのリストアは容易です。DRサイトのKMAは、クラスタの最初のKMAとして機能します。DRサイトのドライブのエージェントを削除します。機能していないKMAを交換し、クラスタに1台ずつ追加します（「ハードウェア障害」のセクションを参照のこと）。データベースがクラスタ全体にレプリケートされます。交換用のドライブでサービスが開始されたら、エージェントを作成し、登録します。

シナリオ2

このシナリオでは、バックアップ・ファイルから企業のOracle Key Managerをリストアする必要があります。クラスタをリストアするプロセスを以下に示します。DRテスト・サイトは以下を提供します。

- 工場出荷時の設定のままの、または以前のクライアントによって工場出荷時の設定にリセットされたKMA [10]
- KMAネットワークに接続されたドライブのプール
- Oracle Key Manager GUIを実行しているKMAネットワークの管理ワークステーション

企業は以下を提供します。

- 信頼のおけるオペレーター
- コア・セキュリティ・バックアップ・ファイル、最新のデータベース・バックアップ・ファイル、および対応するデータベース・バックアップ鍵ファイルを保存したリムーバブル・メディア
- ユーザーIDとパスフレーズのペアがコア・セキュリティ・バックアップ・ファイルに含まれる定足数メンバーの必要なしきい値の数
- 企業のデータセンターをリストアするために必要なバックアップ・テープ
- バックアップ・テープからデータをリストアするために必要な、バックアップ・アプリケーションを実行しているホスト

オペレーターは、『*Oracle Key Manager Version Administration Guide*』の「Getting Started」のセクションに記載されている手順に従って、バックアップからクラスタをリストアするオプションを使用してください。DRサイトの担当者は、QuickStartプロセスに必要な関連のネットワーク情報を提供する必要があります。

QuickStartの手続きが完了したら、オペレーターは以下のようにクラスタを設定します。

- **手順1：**コア・セキュリティ・バックアップ・ファイル、バックアップ鍵ファイル、およびバックアップ・ファイルを保存したリムーバブル・メディアを、管理ワークステーションにロードします。セキュリティ上の理由から、バックアップ・ファイルを管理ワークステーション上にロードしてはなりません。
- **手順2：**Oracle Key Manager GUIを起動し、QuickStartプロセス中に作成したセキュリティ責任者のログイン情報を使用してKMAに接続します。
- **手順3：**Backup Listパネルに移動し、「Restore」ボタンをクリックし、3つの各バックアップ・ファイルの完全なパス名を提供します。
- **手順4：**入力を促されたら、各定足数メンバーにユーザーIDとパスフレーズを入力してもらいます。
- **手順5：**「Start」をクリックし、リストアを開始します。[11]

---

[10] KMAのリセットは、セキュリティ責任者がコンソールにログインして行う必要があります。毎回新しいKMAを用意しないのであれば、DRサイトでは、クライアントが確実にKMAをリセットするようにしなければなりません。それには、セキュリティ責任者に施設を離れる前にコンソールにログインしてもらう必要があります。そうすることで、クライアントのデータが保護され、KMAが次のクライアントによって再利用されます。リセットでは、ディスク・スクラブのオプションを常に使用して、クライアント・データのトレースをサーバーのハード・ディスクからすべて削除する必要があります。

- **手順6：**リストアが完了したら、バックアップ・ファイルを保存したリムーバブル・メディアを管理ワークステーションから取り外します。
- **手順7：**新規ユーザー（OkmAdmなど）を作成し、そのユーザーに定義済みのすべてのロールを割り当てます。この操作により、KMAの設定完了に必要なすべてのオペレーションを実行できるシングル・ユーザーが作成されます。
- **手順8：**KMAから切断し、新しいスーパーユーザーのログイン情報を使用してKMAに再接続します。
- **手順9：**DRサイトの提供するドライブにエージェントを作成し、必要に応じて鍵グループをこれらのエージェントに割り当てます。
- **手順10：**エージェントIDとパスフレーズ、およびドライブ・ネットワーク内のKMAポートのIPアドレスを、ドライブをKMAに登録する役割を担うDRサイト・オペレーターに提供します。

ドライブが登録されたら、これらのドライブを使用するようにバックアップ・アプリケーションを設定します。これで、企業のデータセンターのリストアは完了します。

リストアが完了したら、KMAコンソールにログインし、KMAを工場出荷時の設定にリセットするオプションを選択します。その後、ディスク・スクラブのオプションを選択して、DRサイトのKMAから企業のOracle Key Managerデータベースのトレースをすべて削除します。

シナリオ3

このシナリオは、これまでの2つのシナリオの混合型です。企業のOracle Key Managerデータベースのコピーは、DRサイト1に存在しますが、DRテストはサイト2で実行されています。このサイト2は、シナリオ2のDRテスト・サイトと同じ環境です。このシナリオに対処するには、DRサイト間のネットワーク接続にもよりますが、複数のオプションが存在します。

- **オプション1：**サイト2のドライブを、サイト1のKMAの管理ネットワークに直接接続します。
- **オプション2：**サイト2のKMAを、サイト1の企業の（シングル・ノード）クラスタに追加します。
- **オプション3：**サイト1のKMAをバックアップし、サイト2のKMAにリストアします。
- **オプション4：**サイト1のKMAからサイト2のKMAに鍵を送信します。

---

[11] リストア・オペレーションの完了には、元のクラスタのサイズに応じて、1時間から数時間かかります。

オプション1

サイト2のドライブ・ネットワークを、サイト1の企業のKMAに接続されるWANに接続できる場合、これがもっとも単純で迅速に完了できるオプションです。サイト1のKMAにサイト2のドライブのエージェントを作成し、必要に応じて鍵グループを割り当てます（エージェントの作成にはオペレーターの資格証明が、鍵グループの割当てにはコンプライアンス責任者の資格情報が必要です。）エージェントIDとパスフレーズ、およびサイト1のKMAの管理ポートのIPアドレスを、ドライブをKMAに登録する役割を担うサイト2のDRサイト・オペレーターに提供します。登録が完了すると、サイト2のドライブは企業の暗号化データを処理するために使用できます。必要なバックアップ・アプリケーションを実行するホストを、サイト2のドライブを使用するように設定し、企業のデータセンターのリストアを続行します。このオプションにより、必要な鍵をDRサイトのKMAに送信することなく、サイト2から企業のデータセンターをリストアできます。

オプション2

このオプションでは、各サイトで以下のリソースが必要となります。

- サイト1
  - サイト1のKMAとサイト2のKMAとの間のWAN接続
  - セキュリティ責任者
  - 定足数メンバーのしきい値の数
- サイト2
  - 工場出荷時の設定のままの、または工場出荷時の設定にリセットされたKMA
  - KMAサービス・ネットワークに接続されたドライブのプール

サイト1では、セキュリティ責任者が以下の手順を実行します。

- **手順1：**ラップトップをKMAネットワークに接続し、Oracle Key Manager GUIを起動します。
- **手順2：**新たなKMAを作成し、KMA名とパスフレーズを指定します。
- **手順3：**サイト2のKMAのサービス・プロセッサ・インタフェースを使用してQuickStartプロシージャを実行し、KMAをクラスタに追加するオプションを選択します。手順2で作成した新しいKMAの名前とパスフレーズを入力します。
- **手順4：**各定足数メンバーにユーザーIDとパスフレーズを入力してもらい、QuickStartプロシージャを完了します。
- **手順5：**Oracle Key Manager GUIを使用して新しいKMAに接続し、Oracle Key Managerデータベースの新しいKMAへのレプリケーション進行状況を確認します。
- **手順6：**レプリケーションが完了したら、KMAのロック/アンロック機能を実行します。
- **手順7：**「Unlock」をクリックし、各定足数メンバーにユーザーIDとパスフレーズを入力してもらい、アンロック・オペレーションを完了します。
- **手順8：**新規ユーザー（OkmAdmなど）を作成し、そのユーザーに定義済みのすべてのロールを割り当てます。これで、KMAの設定完了に必要なすべてのオペレーションを実行できるシングル・ユーザーが作成されます。

- **手順9：**KMAから切断し、新しいスーパーユーザーのログイン情報を使用してKMAに再接続します。
- **手順10：**サイト2のドライブにエージェントを作成し、必要に応じて鍵グループをこれらのエージェントに割り当てます。
- **手順11：**エージェントIDとパスフレーズを、ドライブをKMAに登録する役割を担うサイト2のDRサイト・オペレーターに提供します。

ドライブが登録されたら、サイト2のドライブは企業の暗号化データを処理するために使用できます。必要なバックアップ・アプリケーションを実行するホストを、これらのドライブを使用するように設定し、データセンターのリストアを続行します。

リストアが完了したら、クラスタからサイト2のKMAを削除し、サイト2のKMAでELOMインタフェースを使用してKMAを工場出荷時の設定にリセットします。その後、ディスク・スクラブのオプションを選択して、DRサイトのKMAから企業のOracle Key Managerデータベースのトレースをすべて削除します。手順8で作成されたスーパーユーザーも削除されます。

オプション3

このオプションでは、サイト1にある企業のOracle Key Managerデータベースのバックアップを作成し、そのバックアップを使用して、サイト2のKMAに企業のクラスタのコピーを作成する必要があります。データベース・バックアップを作成するには、サイト1でバックアップ・オペレーターとセキュリティ責任者の資格証明が必要です。また、サイト2でバックアップ鍵ファイルをアンロックするには、コア・セキュリティ・バックアップが必要です。サイト2で必要なものは、リストア・オペレーションの完了に必要な定足数メンバーなど、シナリオ2のDRテスト・サイトで必要なものと同様です。

サイト1でバックアップ・ファイルを作成したら、シナリオ2で定められたプロセスを用いて、企業のデータセンターのリストアを完了します。バックアップからリストアするオペレーションは時間がかかりますが、短時間で終了する別の選択肢がない場合には有用な方法です。

オプション4

このオプションでは、各サイトで鍵転送パートナーを設定する必要があります。鍵のインポートは、バックアップ・ファイルから鍵をリストアするよりもはるかに短い時間で完了するため、これは魅力的な方法です。

サイト2には、ドライブのプールが登録された、完全に機能するスタンドアロンのKMAがなければなりません。この設定は、DRテストの前に行うことも、テスト中に行うこともできます。DRテストを実施している、信頼のおける企業内のオペレーターが、サイト2のKMAを設定します。サイト1のオペレーションには、セキュリティ責任者の資格証明が必要です。

各サイトでは、以下の手順を実行します。

- サイト2
  - ClusterオプションのInstall First KMAを使用し、サイト2のKMAでELOMインタフェースを使用して、QuickStartプロシージャを完了します。
  - 新たに作成したセキュリティ責任者のログイン情報を使用して、Oracle Key Manager GUIからKMAに接続します。
  - インポートを許可する鍵ポリシーと、この鍵ポリシーを使用する鍵グループを作成します。
  - サイト1のKMAから公開鍵情報を取得します。

- この公開鍵情報を使用して鍵転送パートナーを作成し、鍵の指紋がサイト1の指紋と合致することを確認します。
- サイト2のドライブにエージェントを作成し、インポートの鍵グループをそのエージェントに割り当てます。
- エージェントIDとパスフレーズを、ドライブをKMAに登録する役割を担うサイト2のDRサイト・オペレーターに提供します。

ドライブが登録されたら、必要なバックアップ・アプリケーションを実行しているホストを、これらのドライブを使用するように設定できます。

- サイト1
  - サイト2のKMAから公開鍵情報を取得します。
  - この公開鍵情報を使用して鍵転送パートナーを作成し、鍵の指紋がサイト2の指紋と合致することを確認します。
  - 必要であれば、すべての鍵ポリシーを、エクスポートを許可するように変更します。
  - シナリオ2の手順7のとおりに、スーパーユーザーを1つ作成します。
  - KMAから切断し、スーパーユーザーのログイン情報を使用してKMAに再接続します。
  - すべての鍵グループを転送パートナーに割り当てます。
  - すべてのデータ・ユニットの鍵を、サイト2で使用するためにエクスポートします。
  - サイト2で共有されるデータ・ユニットと鍵を含むエクスポート・ファイルを転送します。
  - 鍵転送パートナーとスーパーユーザーを削除し、必要な場合は鍵ポリシーの変更を元に戻します。
- サイト2
  - サイト1から転送されたエクスポート・ファイルを管理ステーションにロードします。
  - データ・ユニットと鍵を、エクスポート・ファイルからKMAデータベースにインポートします。
  - 企業のデータセンターをリストアするのに必要な各バックアップ・テープ・ボリュームで、データ・ユニットがKMAデータベースに存在することを確認します。
  - エクスポート・ファイルを管理ステーションから削除します。

企業のデータセンターのリストアは、この時点からサイト2で続行できます。リストアが完了したら、サイト2のKMAのコンソールにログインし、KMAを工場出荷時の設定にリセットするオプションを選択し、ディスク・スクラブのオプションを使用して企業の秘密情報のトレースをすべて削除します。

StorageTek Crypto Key Management System 1.xから Oracle Key Manager 2.xへの移行

StorageTek Crypto Key Management System 1.xからOracle Key Manager 2.xへの移行パスは、分かりやすく容易です。以下のサブセクションでは、この作業を完了するのに必要な手順を概略します。

StorageTek Crypto Key Management System 1.xの準備

移行プロセスの最初の手順では、StorageTek Crypto Key Management System 1.xシステムの準備を行います。

- **手順1：**StorageTek Crypto Key Management System 1.xシステムがバージョン1.0または1.1のソフトウェアを実行している場合、バージョン1.2にアップグレードします。バージョン1.2を使用して作成されたエクスポート鍵ファイルに含まれる鍵のみが、Oracle Key Manager 2.xにインポートできます（バージョン1.2にアップグレードする方法については、StorageTek Crypto Key Management System 1.2の製品ドキュメントを参照してください。）
- **手順2：**StorageTek Crypto Key Management System 1.2に管理者としてログインします。
- **手順3：**Keys→Media Key Exportに移動し、エクスポートする鍵を選択し、エクスポート・ファイルの名前を入力して「Apply」をクリックします。指定した名前のエクスポート・ファイルが、KMS 1.2サーバーの/export/home/kms/mnt_keysディレクトリに作成されます。このファイルは、次のフォーマットになっています。

  <鍵ID>, <鍵値>[, <説明>] where

  "鍵ID"は、鍵を一意に識別する64文字（16進データ）の値です。

  "鍵値"は、（暗号化されていない）鍵の暗号値を表す64文字（16進データ）の値です。

  "説明"は、鍵を説明する任意の言葉や文です。

鍵IDと説明のフィールドは、KMS KeyとMedia Key Exportに表示されるものと同様です。

警告：このフィールドの鍵の値は暗号化されていません。このファイルは、極めてセキュアな場所に保管し、鍵がOracle Key Managerデータベースにインポートされた時点で完全に破棄する必要があります。

Oracle Key Manager 2.xの準備

移行プロセスの次の手順では、Oracle Key Manager 2.xシステムの準備を行います。

- **手順1：**Oracle Key Manager 2.xクラスタをインストールし、設定します。Oracle Key Manager GUIを使用して、StorageTek Crypto Key Management System 1.2の鍵用の鍵ポリシーを望ましい暗号化有効期間（暗号化期間と同じ、もしくは暗号化期間よりも長い期間）で作成し、鍵ポリシーのインポート属性を有効化します。適切な暗号化有効期間が設定され、インポート属性が有効化されている既存の鍵ポリシーを使用することもできます。[12]
- **手順2：**鍵グループを作成し、手順1で作成した鍵ポリシーに関連付けます。手順 1 と同じく、適切な属性が設定された既存の鍵グループを使用することもできます。
- **手順3：**Oracle Key Manager 2.x環境に登録するStorageTek Crypto Key Management System 1.xの各ドライブにエージェントを作成し、入力した各エージェントのエージェントIDとパスフレーズを記録します。エージェント・リストの各エージェントは、Enrolled = Falseとなっていなければなりません。
- **手順4：**適切なデフォルト鍵グループを、作成した各エージェントに割り当てます。
- **手順5：**StorageTek Crypto Key Management System 1.xの鍵用の宛先鍵グループを、すべてのエージェントに割り当てます。
- **手順6：**StorageTek Crypto Key Management System 1.2の鍵エクスポート・ファイルを、Oracle Key Manager 2.xの管理ワークステーションに転送します。

鍵のインポート

移行プロセスの次の手順では、鍵情報をインポートし、クラスタ内のすべてのKMAと接続されるネットワーク全体にレプリケートします。

- **手順1：**コンプライアンス責任者のログイン情報でOracle Key Manager GUIにログインします。
- **手順2：**1.0の鍵をインポートする機能を選択し、宛先鍵グループと、StorageTek Crypto Key Management System 1.0の鍵エクスポート・ファイルのパス名を入力し、「Start」をクリックします。

---

[12] StorageTek Crypto Key Management System 1.2の鍵は、インポート後、処理専用状態になります。鍵の暗号化期間の終了日が現在の日時に設定されるため、鍵ポリシーで設定された暗号化期間とは一致しなくなります。作成日とアクティブ化された日はどちらも、インポートが実行された現在の日時となるため、暗号化有効期間もそれに応じて選択する必要があります。

Oracle Key Managerにより、以下の手順が実行されます。

- ファイル全体が読み込まれ、各行において、鍵IDと鍵値が適切な長さとフォーマットであることが確認されます。鍵IDの最初の4文字が取り除かれます（鍵IDの長さは、StorageTek Crypto Key Management System 1.2では32バイトですが、Oracle Key Manager 2.xでは30バイトです。）さらに、Oracle Key Managerデータベースと照合され、鍵IDが一意であることが確認されます。鍵IDが一意でない場合、鍵が、その鍵IDのOracle Key Managerキーストアと照合されます。
- Oracle Key Managerデータベースに同じ鍵IDと鍵値の鍵が存在する場合、その鍵IDは記録され、処理は続行されます。鍵のインポートが完了したら、重複した鍵の数が戻されます。
- Oracle Key Managerデータベースに同じ鍵IDの鍵が存在するものの、鍵値が異なる場合、StorageTek Crypto Key Management System 1.2のエクスポート・ファイルが破損している可能性があると見なされ、オペレーションは直ちに中断され、エラーが戻されます。
- 検証フェーズでエラーが発生しない場合、鍵は処理されます。その鍵の鍵値が暗号化され、キーストアに追加され、メタデータ（鍵ID、状態、作成日）がデータベースに追加されます。鍵の処理でエラーが発生すると、鍵の処理は停止されます。
- 処理フェーズでエラーが発生しない場合、すべての鍵は処理され、インポートされた鍵の合計数がOracle Key Manager GUIによって報告されます。
- 鍵の処理でエラーが発生した場合、キーストアに追加された鍵値は削除され、メタデータをデータベースに挿入するトランザクションはロールバックされ、エラー・メッセージがOracle Key Manager GUIに表示されます。
- インポートされた鍵情報は、クラスタ内のすべてのKMAと接続されるネットワーク全体にレプリケートされます。

- **手順3：**Oracle Key Manager環境に登録されるドライブが、Oracle Key Manager KMAのサービス・ネットワークにアクセスできることを確認します。
- **手順4：**Oracle Key Managerサービス・ネットワークのすべての1.xトークンを再書込みし、送信中のドライブ情報を削除します。
- **手順5：**VOPインタフェースを使用して、Oracle Key Manager環境に登録される各ドライブをリセットします。この操作により、StorageTek Crypto Key Management System 1.xのすべての鍵がメモリから削除されます。
- **手順6：**各ドライブをオフラインにし、最新のOracle Key Managerのドライブ・ファームウェアをロードします。
- **手順7：**各ドライブをリブートしたら、再度オフラインにし、「Configure」→「Drive Data」→「Encrypt」の順に選択します。以下の情報を入力します。
  - エージェントの作成時に指定したエージェントIDとパスフレーズ
  - "Use token" = "No"
  - ドライブのネットワークにあるKMAのIPアドレス

StorageTek Crypto Key Management System 1.xの暗号化が以前有効化されたドライブでは、ライセンス鍵は不要です。VOPログにより、登録が正常に終了したことが報告され、ドライブは再びリブートされます。

- **手順8：**Oracle Key Manager GUIにおいて、各エージェンでEnrolled = Trueとなっていることを確認します。[13]

StorageTek Crypto Key Management System 1.xの暗号化データの取得

この手順では、暗号化データを復号化のために取得します。

- **手順1：**インポートされた鍵を使用して書き込まれたデータを含むテープ・ボリュームを、そのテープ・ボリュームからデータを取得するために使用されるアプリケーション環境にインポートします。
- **手順2：**アプリケーションで、インポートされたテープ・ボリュームの1つからファイルを取得するリクエストを発行します。
- **手順3：**テープ・ボリュームがOracle Key Manager環境のドライブにマウントされたら、エージェントは、メディアが暗号されており、データ・ユニットIDを持たないことを確認します。
- **手順4：**エージェントは、（外部タグとしてライブラリによって提供されるカートリッジのバーコードを使用して）データ・ユニットを作成するよう、KMAにリクエストします。
- **手順5：**KMAはデータ・ユニットを戻し、エージェントは指定されたファイルの鍵IDをリクエストします。
- **手順6：**KMAはリクエストされた鍵IDを検索し、エージェントがその鍵グループにアクセスできることを確認し、その鍵グループを新しいデータ・ユニットに関連付け、その鍵値をエージェントに戻します。
- **手順7：**エージェントは指定されたファイルを復号化し、そのデータをリクエストしたアプリケーションに戻します。

インポートされたデータの管理

StorageTek Crypto Key Management System 1.xの鍵は再使用できません。鍵のライフ・サイクルが、処理専用状態で開始されるためです。それ以外は、Oracle Key Managerの鍵と全く同様に管理されます。StorageTek Crypto Key Management System 1.xの鍵を使用して暗号化されたテープ・ボリュームには、データを追加できます。

ドライブのエージェントは、保護および処理状態の鍵を使用せずに、Oracle Key Managerのデータ・ユニットに鍵を再作成するのと同じように、データ・ユニットに鍵を再作成します。[14]

---

[13] StorageTek Crypto Key Management System 1.xの暗号化が以前有効化されたドライブは、永遠に暗号化されます。ドライブで暗号化を無効化してはなりません。

[14] StorageTek Crypto Key Management System 1.xからOracle Key Managerにインポートされたテープ・ボリュームは、StorageTek Crypto Key Management System 1.x環境では処理できません。

StorageTek Crypto Key Management System 1.xシステムからインポートされたデータ・ユニットと、Oracle Key Managerシステムで暗号化されたデータ・ユニットには、重要な違いがあります。インポートされたデータ・ユニットには、同じ鍵を使用して暗号化されたデータが含まれている可能性があるのです。そのため、1つのデータ・ユニットに対するオペレーションが悪影響を生じさせる場合があります。たとえば、1つのデータ・ユニットに関連付けられたすべての鍵の鍵グループを変更すると、他のデータ・ユニットに関連付けられた一部またはすべての鍵の鍵グループも変更されるという連鎖反応が起きます。同様に、1つのデータ・ユニットのデータを暗号化するために使用された鍵を破棄すると、他のデータ・ユニットのデータにアクセスできなくなる可能性があります。StorageTek Crypto Key Management System 1.xの多くのお客様は、サイト間のデータ共有を簡素化するために、数週間、もしくは数ヵ月にわたって、同時に複数のサイトで単一の暗号化鍵を使用していました。その結果、大量の重要データが単一の鍵で保護されました。この鍵をうっかり破棄してしまえば、膨大な量のデータが失われる可能性があります。鍵を破棄する際は、細心の注意が必要です。

さらに、この連鎖反応が明白でない場合もあります。もともとStorageTek Crypto Key Management System 1.xシステムで暗号化されたテープ・メディアは、Oracle Key Managerドライブに最初にマウントされるまで、関連付けられたデータ・ユニットIDを持ちません。そのため、1つのデータ・ユニットにのみ関連付けられているとOracle Key Managerによって報告された鍵が、実際には、クラスタにまだ認識されていない別の1つまたは複数のテープ・ボリュームのデータを暗号化するためにも使用されている場合があります。

結論

Oracle Key Managerは、ストレージベースのデータ暗号化への企業のコミットメントが急速に高まる状況に対処するために設計された、包括的な鍵管理プラットフォームです。Oracle Key Managerは以下を実現します。

- セキュリティ
- パフォーマンス
- 大容量
- 高可用性
- スケーラビリティ
- 相互運用性
- 一元管理
- 長期間の鍵保存
- 使いやすさ
- コンフィギュアビリティ
- StorageTek Crypto Key Management System 1.xからのアップグレード・パス

Oracle Key Managerを採用するお客様は、自社のデータが不正アクセスから保護され、許可されたユーザーに高可用性を提供していることを確信しています。

付録A：用語集

AES：Advanced Encryption Standard。

エージェント：データの暗号化と復号化に使用されるストレージ・デバイス。

ANSI：米国国家規格協会。

API：Application Program Interface（アプリケーション・プログラム・インタフェース）。

BOT：テープ開始位置。

資格証明：ロールを参照してください。

データ・ユニット：物理的なストレージ・オブジェクト（テープ・ボリューム）を表す抽象的実体。

ELOM：Embedded Lights Out Manager。Oracleサーバーをオペレーティング・システムから独立して管理できるようにする専用のハードウェア・システムおよび支援ソフトウェア。

FIPS：米国連邦情報処理標準。

鍵：データの暗号化と復号化に使用されるデータ暗号化鍵。

鍵グループ：鍵ポリシーと関連付けられた鍵のグループ。暗号化エージェントによって鍵データへのアクセスを強化するために使用されます。

鍵ID：暗号化鍵を参照するために使用される公開識別子。

鍵ポリシー：その鍵ポリシーと関連付けられた鍵グループの鍵のライフ・サイクルを定義するポリシー。

鍵分割資格：セキュリティが重視される特定のオペレーションを実行する際にシステムに入力しなければならないユーザーIDとパスフレーズのペア一式。

キーストア：暗号化鍵を保存するために使用されるセキュアなメモリの場所。

KMA：鍵管理データベース、鍵マネージャ、および鍵ストアを持つ鍵管理アプライアンス。

KMS：クラスタ化されたKMAのグループである鍵管理システム。バージョン2.3でOracle Key Managerと名称が変更されました。

MVC：複数の仮想カートリッジ。

NIST：アメリカ国立標準技術研究所。

QuickStart：KMAの電源投入時に自動的に実行される構成メニュー。KMAの初期化に必要な構成データを収集します。

定足数：鍵分割資格。

ロール：特定のオペレーションを実行できるようにするために、Oracle Key Managerユーザーに付与される権限一式。監査者、バックアップ・オペレーター、コンプライアンス責任者、オペレーター、セキュリティ責任者など。

RSA：公開鍵を暗号化するためのアルゴリズム。

SOAP：Simple Object Access Protocol。

TLS：Transport Layer Security。

VOLSER：テープ・ボリュームのシリアル番号。

VOP：StorageTekテープ・ドライブに対する仮想オペレーター・パネル・インタフェース。

VSM：Virtual Storage Manager。

付録B：HPおよびIBM LTOテープ・ドライブを使用した Oracle Key Managerのオペレーション

Oracle Key Managerの暗号化オペレーションは、エージェントがHPまたはIBM LTO4/5の暗号化対応テープ・ドライブの場合は若干異なります。動作の違いを以下に示します。

- LTOドライブは、出荷時に暗号化に対応しているため、暗号化を有効化するのにライセンス鍵は必要ありません。
- LTO暗号化対応ドライブをKMSクラスタに登録するには、LTOドライブを管理する目的で特別に設計されたVOP-LTOソフトウェアを使用して、複数の手順を実行する必要があります。最初の2つの手順では、オペレーター権限のあるユーザーが、Oracle Key Manager GUIを使用して準備作業を行います。残りの2つの手順では、VOP-LTOソフトウェアを使用して、実際にエージェントを登録します。
  - **手順1：**KMAのドライブにエージェントを作成し、エージェントIDとパスフレーズを指定します。
  - **手順2：**エージェントに1つまたは複数の鍵グループを割り当て、1つの鍵グループをエージェントのデフォルト鍵グループに指定します（エージェントのリクエストにより、Oracle Key Managerが新たな書込み鍵を作成した場合、その鍵はエージェントのデフォルト鍵グループに割り当てられます。）
  - **手順3：**VOP-LTOソフトウェアを使用してドライブに接続し、「Configure Drive」タブをクリックします。表示されたフィールドに、手順1で指定したエージェントIDとパスフレーズ、およびドライブ・ネットワークのKMAポートのIPアドレスを入力し、「**Commit**」をクリックします。
  - **手順4：**「Diagnose Drive」タブをクリックし、ログ・エントリにて、コミットのオペレーションが正常に終了したことを確認します。Configure Driveタブに戻り、「Enroll」をクリックします。Diagnose Driveタブでログ・エントリを再度モニタリングし、登録のオペレーションが正常に終了したことを確認します。VOPの上部に表示されているEncryptボタンの色が青に変わっているはずです。
- LTOドライブは、Oracle Key Managerから鍵を取得するように設定されている場合、メモリに最大で1つの暗号化鍵を保存するに過ぎませんが、StorageTekドライブは、最大で32個の鍵を保存できます。
- LTOドライブは、テープ・ボリュームがマウントされても、そのテープ・ボリュームと関連付けられた鍵をプリフェッチしません。代わりに、カートリッジ・メモリからバーコード・ラベルとメディア識別子を読み取り、その情報をOracle Key Managerに送信し、I/Oリクエストが受領されるのを待ちます。
- アプリケーションが、テープから暗号化鍵を読み込むリクエストを発行した場合、ドライブは、そのデータを復号化するために必要な鍵をリクエストします。テープ・ボリュームがマウントされている限り、同じ鍵を使用して書き込まれたデータを読み込む後続のリクエストは、Oracle Key Managerにさらにリクエストを発行しなくとも完了します。
- 書込み鍵の処理は異なります。HP LTOドライブは、テープが別の場所に移された後は、すべての書込みオペレーションにおいて、StorageTek Crypto Key Management Systemから鍵をリクエストします。つまり、Veritas NetBackup環境において、複数のバックアップ・イメージが同じテープ・ボリュームに書き込まれる場合、ドライブは各バックアップ・ジョブが開始された時点で、Oracle Key Managerから鍵をリクエストします。テープ・ボリュームにデータを書き込むために最後に使用された暗号化鍵が保護および処理状態のままの場合、Oracle Key Managerはその鍵をドライブに

再送信します。保護および処理状態でない場合は、Oracle Key Managerは新たな鍵を作成し、その鍵をデータ・ユニットと関連付け、ドライブに送信します。

IBM LTOドライブがどのように書込み鍵を処理するかについての詳細は、『*IBM LTO Tech Brief*』の「LTO4 Differences」のセクションに記載されています。

StorageTekドライブは、テープ・ボリュームがマウントされている間は、テープ・ボリュームのマウント時に取得された保護および処理状態の鍵を使用してデータを暗号化します。これにより、複数のバックアップ・ジョブを1つのテープ・ボリュームに書き込む場合に、鍵のフェッチに伴うオーバーヘッドが低減されます。

- HP LTO4ドライブは、BOTから書込みを行うリクエストを受領しても、鍵の関連付けを解除するリクエストをKMAに送信しません。そのため、データをデータ・ユニットに書き込むために使用されたすべての鍵は、これらの鍵の一部を使用して暗号化されたデータが上書きされている場合でも、引き続きOracle Key Managerより、"In Use by Data Unit"（データ・ユニットが使用中）と報告されます。HP LTO5ドライブは、鍵の関連付けを解除するリクエストをKMAに送信しません。

Oracle Key Managerの概要
2010年11月

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

海外からのお問い合わせ窓口：
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200

oracle.com.

Oracle is committed to developing practices and products that help protect the environment

SOFTWARE. HARDWARE. COMPLETE.