Oracle Key Manager

システムアシュアランスガイド

パート番号 : E25342-02
2011 年 10 月

Oracle Key Manager: システムアシュアランスガイド

E25342-02

変更の要約

EC 番号	日付	改訂	説明
EC000227	2008 年 2 月	A	初版。
EC000496	2008 年 5 月	B	変更の一覧については、この改訂を参照してください。(T9840D テープドライブが含まれている)
EC000594	2008 年 6 月	BA	変更の一覧については、この改訂を参照してください。(HP LTO 4 テープドライブが含まれている)
EC001009	2009 年 2 月	BB	変更の一覧については、この改訂を参照してください。(X2200 サーバー、FIPS 準拠、IPv6、T10000B が含まれている)
EC001402	2009 年 11 月	BC	変更の一覧については、この改訂を参照してください。(KMS 2.2、IBM LTO4、IBM ICSF)
	2010 年 4 月	C	変更の一覧については、この改訂を参照してください。(Oracle ブランディング、更新されたマーケティング / 注文番号)
	2010 年 11 月	D	変更の一覧については、この改訂を参照してください。(製品名の変更、新しいサーバー [4170]、新しいテープドライブ [LTO5]、および新しいプラットフォーム [SL24 と SL48] のサポート)
	2011 年 6 月	E	■ Auto Service Request (ASR) 機能に関する追加情報。
	2011 年 7 月	-01	■ Oracle Part No.: E25342 ■ 改訂 01 への更新。 ■ T10000C テープドライブに関する追加情報。 ■ 技術的なコメント / 更新が含まれている。
	2011 年 10 月	-02	■ 改訂 -02。 ■ リリース 2.5 をサポートするための更新 ■ データベースに関する情報を付録 B「Oracle データベースの暗号化」に追加。

注 – この改訂には改訂傍線が引かれています。

目次

はじめに

このガイドは、保守担当者、お客様、パートナーを初めとする、Oracle Key Manager (OKM) 暗号化ソリューションの導入を計画しているすべての方々を対象にしています。

注 – お客様が導入を完了するには、『管理ガイド』および『Customer Virtual Operator Panel Guide』のコピーが必要です。

導入の際にお客様がこれらのガイドを必ず利用できるようにしてください。
http://docs.sun.com/app/docs/prod/stortek.crypto.keymgmt20 を参照してください。

関連情報

これらの資料には、このガイドで言及している追加情報が含まれています。

資料の説明	Part No.
Important Safety Information for Hardware Systems	816-7190-xx
SunFire X2100 Server Installation Guide	819-6589-xx
SunFire X2200 Server Installation Guide	819-6596-xx
SunFire X4170 Server Installation Guide	821-0481-xx
Embedded Lights Out Manager Administration Guide	819-6588-xx
T10000 Tape Drive Installation Manual	96173
T9x40 Tape Drive Installation Manual	95879
SL8500 Modular Library System Installation Manual	96138
SL3000 Modular Library System Installation Manual	316194201
SL500 Modular Library System Installation Manual	96114
L700/1400 Library Installation Manual	95843
9310 PowderHorn Library Installation Manual	9314
Virtual Operator Panel—Service	96180
Virtual Operator Panel—Customer	96179
Oracle Key Manager Installation and Service Manual	3161949xx

資料の説明	Part No.
Oracle Key Manager 管理ガイド	3161951xx
Oracle Key Manager Disaster Recovery Guide	3161971xx
Storage Regulatory and Safety Compliance Manual	820-5506-xx
Oracle Advanced Security Transparent Data Encryption Best Practices (2011 年 7 月) - ホワイトペーパー	
Using Oracle Key Manager with Advanced Security Transparent Data Encryption (TDE) - ホワイトペーパー	

ドキュメント、サポートおよびトレーニング

機能	URL	説明
Web サイト	http://www.oracle.com/index.html	一般情報およびリンク。
マニュアル	http://www.oracle.com/technetwork/jp/indexes/documentation/index.html http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#kmsl	技術ドキュメントの検索。PDF/HTML ドキュメントのダウンロード。印刷版ドキュメントの注文。
ダウンロード	http://www.sun.com/download/index.jsp または http://www.oracle.com/technetwork/indexes/downloads/index.html	ファームウェアおよびグラフィカルユーザーインタフェース、パッチ、および機能のダウンロード。
E-Delivery	https://edelivery.oracle.com/	
サポート	http://www.oracle.com/us/support/index.htm	サポートの取得および強化。
オンラインアカウント	https://reg.sun.com/register	オンラインアカウントの登録。

Oracle は皆様のご意見をお待ちしております。

Oracle はドキュメントの改善を目指しており、皆様のご意見とアドバイスをお待ちしております。ご意見を送信するには、次のサイトの「Feedback[+]」リンクをクリックしてください。

STP_FEEDBACK_US@oracle.com

ご意見をお寄せいただく際には、下記のタイトルと Part No. を記載してください。

『Oracle Key Manager システムアシュアランスガイド』、PN: E25342-xx

第 1 章

はじめに

暗号化は**暗号方式**という技術に基づいており、今日ではデータの安全性を確保するもっとも有効な方法の 1 つとなっています。暗号化ファイルを読み取るには、そのファイルの暗号化解除を可能にする鍵にアクセスできる必要があります。

この章では、Oracle の Key Manager (OKM) と暗号化のためのコンポーネントの概要を説明します。

暗号化の計画

顧客のアカウントは次に関係していますか。

- **データの安全性**
- **データ保護および機密情報**
- **政府規制および保存**

- 今日では、データの安全性は IT 専門家の大きな関心事 (データが悪の手に渡ると何が起きるのか) になっています。
- 機密データを次のようにすると、そのデータへのアクセスが行われる可能性があります。
  - ネットワーク上への送信
  - ディスクまたはテープへの書き込み
  - アーカイブへの格納
- 顧客は、政府規制やビジネスパートナーとの契約上の義務のために、データを保護する手段を講じることが必要な場合もあります。いくつかの規制では、組織がそのデータを 暗号化する必要があります。

暗号化は、データの有効期間の 3 つの時点で行われる可能性があります。データが次のとき :

- 作成される (ホストベース)
- トランスポートされる (アプライアンスベース)
- 格納される (デバイスベース)

Oracle は、「**Data-at-Rest (保存データ)**」の暗号化ソリューションとして、**デバイスベース**の実装を提供します。この提供により、さまざまな種類のオペレーティングシステム (エンタープライズシステムとオープンシステムの両方のプラットフォーム) が混在する環境に優れたソリューションがもたらされます。

デバイスベースの暗号化を選択すると、暗号化機能がテープドライブに直接組み込まれるため、既存のシステムインフラストラクチャーに与える**影響が最小限**で済みます。このため、暗号化データ用に特別なソフトウェアを保持する必要がありません。

暗号化標準

Oracle の暗号化ソリューションは、次を含む最新の高度な業界標準と機能に基づいています。

- 米国連邦情報処理標準
  - **FIPS PUB 140-2**、暗号化モジュールのためのセキュリティー要件
  - **FIPS PUB 46-3**、データ暗号化標準
  - **FIPS PUB 171**、鍵管理

  FIPS とは、1996 年施行の情報技術管理改革法 (Information Technology Management Reform Act) 第 5131 条の規定のもとで採択され公布された標準とガイドラインです。
  FIPS は 4 つのレベルのセキュリティーを定義しています。

  レベル 1 – 生産グレードでの要件を備えた基本レベル。
  レベル 2 – 物理的な改ざんの証拠や役割ベースの認証のための要件が追加されます。検証済みのオペレーティングプラットフォームで構築されます。
  レベル 3 – 物理的な改ざんへの耐性や ID ベースの認証のための要件が追加されます。さらに物理的または論理的な分離も求められます。
  レベル 4 – 物理的なセキュリティー要件がより厳しくなり、環境攻撃に対して堅牢であることが求められます。
- **米国商務省国立標準技術研究所 (National Institute of Standards and Technology**、**NIST**) Rijndael 対称ブロック暗号化アルゴリズムを使用して暗号化方式を定義する AES 標準。

  NIST 800-57 Part 1、鍵管理のための推奨事項
- 米国電気電子学会 **IEEE 1619**、ワーキンググループ :

  1619.1 テープの暗号化のための標準 — 完了
  1619.2 ディスクの暗号化のための標準 — 処理中
  1619.3 鍵管理のための標準 — 処理中
- **国際評価基準 (Common Criteria**、CC)、IT セキュリティーの要件を設定する、国家安全保障局 (National Security Agency、**NSA**) が出資している国際協会。
- 国際標準化機構 **ISO/IEC 1779** セキュリティー技術
- CCM–AES-256 暗号化

  CCM (Counter with CBC-MAC) は、強固なプライバシー (セキュリティー) と効率的な認証の両方を備えた暗号化モードです。
  CBC–MAC (Cipher Block Chaining–Message Authentication Code) は、平文の各ブロックが暗号化方式で暗号化される、メッセージの完全性を保証する方式です。
  AES (**Advanced Encryption Standard**) は、カウンターモードと CBC-MAC (CCM) の両方の暗号化技術を使用するブロック暗号化アルゴリズムです。
- **対称暗号化**、データの暗号化と復号化に 1 つの鍵を使用します。
- **ノンス**、繰り返し平文によって繰り返し暗号文が生じないように操作のモードに組み込まれている反復しない数値。
- **暗号化方式群**

- TLS 1.0 = トランスポートレイヤーセキュリティー
- RSA = 2048 ビットの鍵暗号化アルゴリズム
- SHA1 = 広く使用されている安全なハッシュアルゴリズム
- HMAC = ハッシュメッセージ認証コード (Hash-MAC)

コンポーネント

Oracle Key Manager は、次を使用する**デバイスベース**の暗号化ソリューションです。

- 鍵管理アプライアンス (Key Management Appliance、KMA) と呼ばれるアプライアンス (サーバー)。
- ネットワーク接続 * (クリーンなギガビット Ethernet 接続)。
- StorageTek **自動ライブラリ**または Oracle **データベース**。
- 暗号化のエージェントとして StorageTek テープドライブ (T シリーズおよび LTO)。

OKM バージョン 2.3 以降の暗号化ソリューション用のコンポーネントは次で構成されます。

鍵管理アプライアンス (KMA)	KMA とは、ハードウェアプラットフォーム向けの SunFire™ サーバー (2100、2200、4170 など) です。このサーバーは次を行います。 ■ 専用のインストール済みの Solaris™ 10 オペレーティングシステムで鍵マネージャーアプリケーションを実行します。 ■ ポリシーベースの鍵マネージャーおよびプロビジョニングサービスを提供します。 ■ 暗号化用の生鍵を生成します。
SCA6000 カード	FIPS 準拠を必要とする顧客に対して、暗号化処理および管理機能用の Sun Cryptographic Accelerator (SCA6000) カードが**オプションで用意されています。** **注 :** これは FIPS 140-2 レベル 3 のハードウェアセキュリティーモジュールです。
OKM マネージャーまたは **OKM マネージャー GUI**	このマネージャーは、グラフィカルユーザーインタフェース (GUI) を備えたクライアント側のソフトウェアコンポーネントです。 **注 :** OKM マネージャーは、Windows XP、Vista、2003 Server が動作するか、Solaris x86 または Solaris SPARC が動作する、**顧客提供の**、ネットワークに接続された PC、サーバー、または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 CLI	バックアップやレポート作成などの管理作業の自動化を支援するコマンド行インタフェース。
OKM クラスタ	システム内の KMA の完全セット。すべての KMA が互いに認識し、互いに情報をレプリケートします。 **注 :** クラスタ内には 2 台以上のサーバーが必要です。
エージェント	エージェントは、セキュリティー保護された (TLS) セッションを介して鍵データを作成および取得するために OKM クラスタと情報をやり取りします。
データユニット ID	OKM によって個々のデータカートリッジに割り当てられる一意の ID。

鍵グループ	組織に鍵を提供し、それらの鍵を鍵ポリシーに関連付けます。 鍵グループは、暗号化エージェント (テープドライブ) または Oracle データベースによる鍵素材へのアクセスを強制するために OKM によって使用されます。
ネットワーク接続	X2100/X2200 鍵管理アプライアンスには、4 つのネットワーク接続があります。 LAN 0 = 管理ネットワーク LAN 1 = ELOM/ILOM (Embedded または Internal Lights Out Manager) LAN 2 = サービスネットワーク、ドライブへの接続 LAN 3 = 追加の集合サービスポート (オプション)

*** 注 :** セキュリティーを追加し、LAN トラフィックを切り離すために、顧客は管理ネットワークへの接続時に VLAN* (Virtual Local Area Network) の使用を検討することが必要な場合があります。
*** VLAN** とは定義済みのスイッチセット内に存在するブロードキャストドメインです。これらのスイッチ上のポートを 1 つにまとめて論理ネットワークとし、ネットワーク構成内で従来のルーターによって従来どおりに作成されたサービスを提供することができます。

重要 :
鍵管理アプライアンスは、図 1-1 から図 1-4 の構成図に示すとおり、**ペア**で取り付けるようにしてください。いくつかの重要な点は次のとおりです。

- 複数の KMA は、**専用の**プライベート、ローカル、または広域ネットワーク上でクラスタ化されます。
- OKM クラスタ内のサーバーはデータ複製を備えているため、冗長性があります。これにより、それぞれの鍵管理アプライアンスは他のもののバックアップとして機能できます。
- エージェントと呼ばれるテープドライブおよび Oracle データベースは、暗号化鍵が必要な場合はネットワークに接続したままにしておいてください。
- クラスタ内のどの KMA もネットワーク上のすべてのテープドライブを処理できます (両者間が Ethernet で接続されている場合)。
- KMA とエージェントを論理的に「グループ化」してサイトを作成できます。ここでは、エージェントはそれらが割り当てられているサイト内の KMA を優先させます。
- デフォルトでは、エージェントはローカルの KMA (利用可能な場合) によって処理されます。
- どの KMA も管理機能に使用できます。
- KMA に加えられた変更はすべて、クラスタ内の他のすべての KMA にレプリケートされます。
  - いずれかのサイトで生成された新しい鍵は、クラスタ内の他のすべての KMA にレプリケートされます。
  - 管理上のすべての変更は、クラスタ内の他のすべての KMA に反映されます。

暗号化ハードウェアキット

暗号化ハードウェアキットには、Ethernet スイッチ、ケーブル、配電盤、および**ライブラリ**、スタンドアロンの**ラック**、または Oracle データベース構成のいずれかのドライブタイプを接続するための取り付けハードウェアが完備されています。

構成の種類によってドライブの取り付け方が決められており、**各構成には独自のキットが用意されていますので**、詳細は、第 4 章「コンポーネント」を参照してください。

『Oracle Key Manager: Installation and Service Manual』を参照してください。それぞれの取り付け手順については、個々の製品の設置マニュアルを参照してください。

鍵マネージャーの構成

クラスタを作成するには、複数の KMA[1] (2 台以上) を一緒に取り付ける必要があります。[2] KMA のクラスタは、そのデータを互いの KMA に完全にレプリケートすることができます。

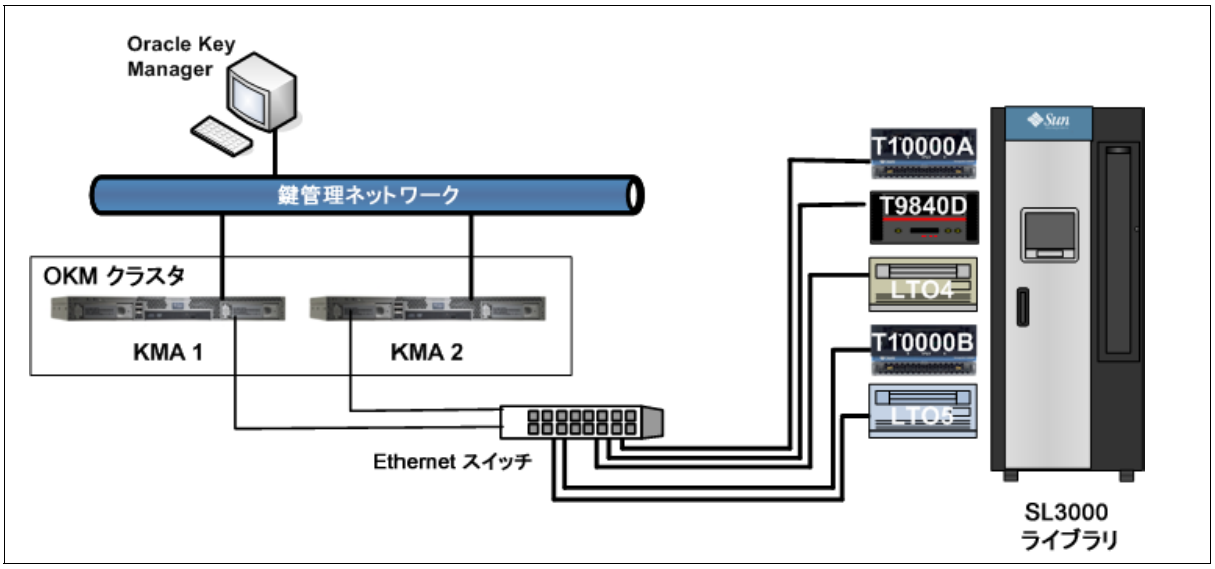
注 : 可用性が最大になるようにシステムを設計する場合は、クラスタサイズをよく考慮するようにしてください。

次の図は、鍵管理アプライアンスのバージョン 2.x の構成例を示しています。

- 図 1-1 単一のサイト – ローカルエリアネットワーク
- 図 1-2 複数のサイト – 広域ネットワーク
- 図 1-3 障害回復を備えた複数のサイト – 広域ネットワーク
- 図 1-4 障害回復構成
- 図 1-5 データベースおよび自動ライブラリの構成

図 1-1 単一サイト構成

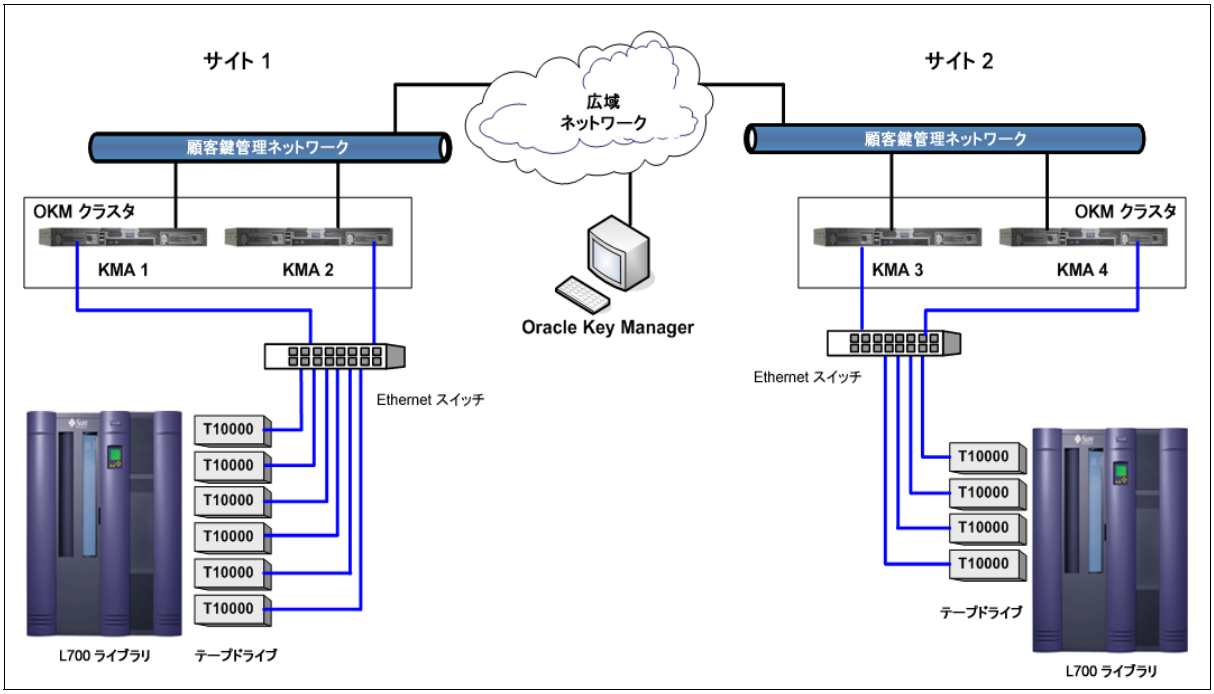
この例では、管理リンク用のローカルエリアネットワークで単一のサイトを使用します。
テープドライブ用のサービスネットワークには、サポートされているテープドライブ (エージェント) がすべて示されます。
エージェントには、T シリーズ (T10000 A および B、T9840D) および LTO (第 4 および第 5 世代) のテープドライブがあります。



1. **複数の KMA**: この標準構成から外れる場合は、暗号化エンジニアリング、プロフェッショナルサービス、およびサポートサービスの承認を得る必要があります。
2. **クラスタ**とは、多くの点で 1 つのコンポーネントを形成できるように、連携して動作するリンクされたアプライアンスの集まりです。

図 1-2 デュアルサイト構成

この例では、KMA は広域ネットワークを介して管理されます。
4 つの KMA はすべて同じ OKM クラスタに属しています。



注 : L シリーズのライブラリでは、LTO 暗号化対応テープドライブはサポートされません。

図 1-3 複数サイト構成

この例では、1 つの OKM クラスタ内で 2 つのリモートサイトと 1 つのローカル (メイン) サイトを使用します。
メインサイトには、特定の鍵グループを持つパーティション化された SL8500 ライブラリが含まれており、OKM クラスタ内のすべての KMA (1 - 6) とメディアにバックアップ機能を提供します。

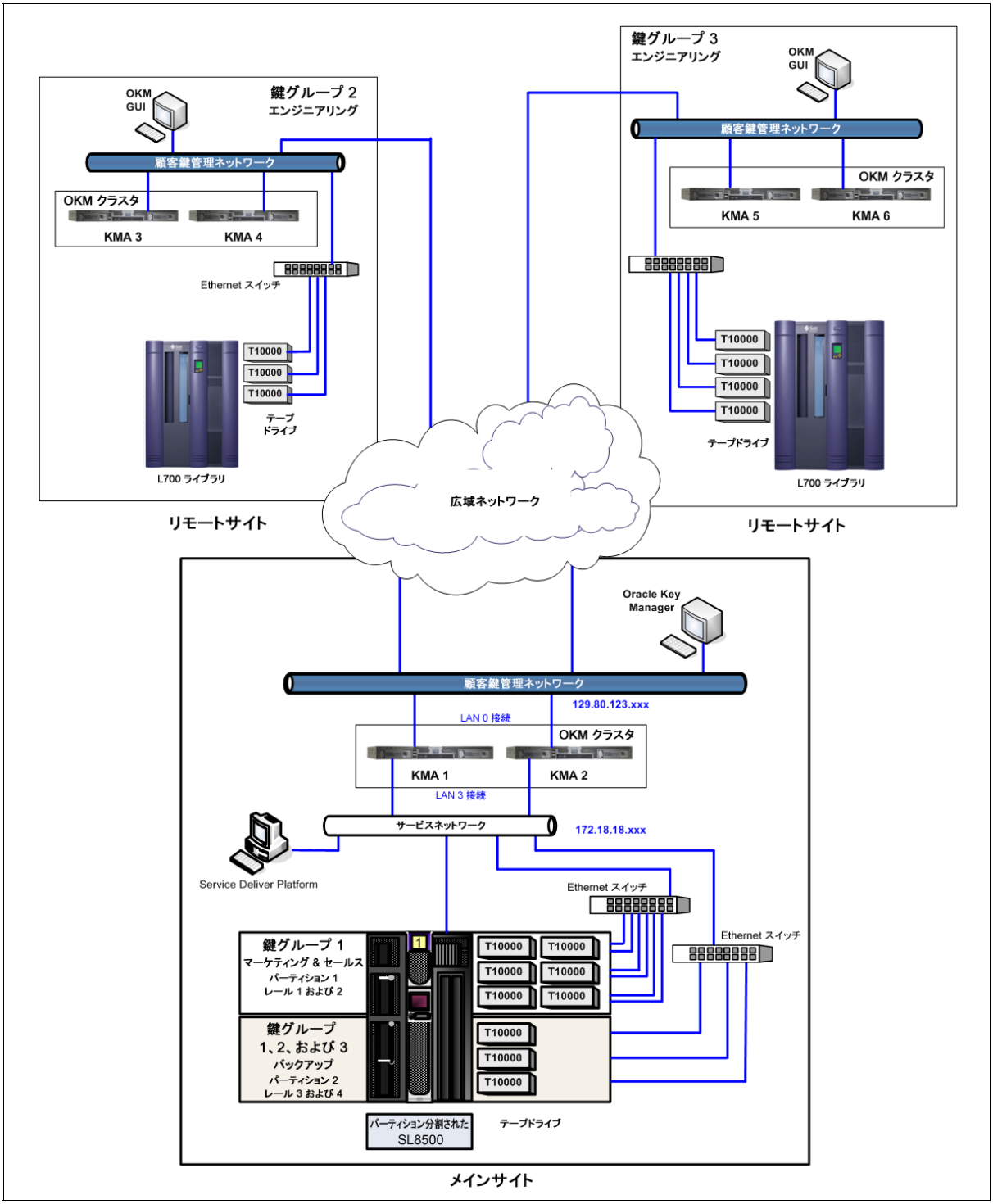


図 1-4 障害回復構成

この例には 2 つの広域ネットワークがあり、1 つは管理用、もう 1 つはサービス用です。

- OKM はクラスタ内の 4 つのすべての KMA と通信します。
- サービスネットワークは、LAN 2 および LAN 3 の 2 つのインタフェースポートから構成されます。KMA は LAN 2 を LAN 3 と集約して 1 つの集合サービスポートにします。
- サービス広域ネットワークでは、どちらかのサイトの KMA がエージェントと通信できます。

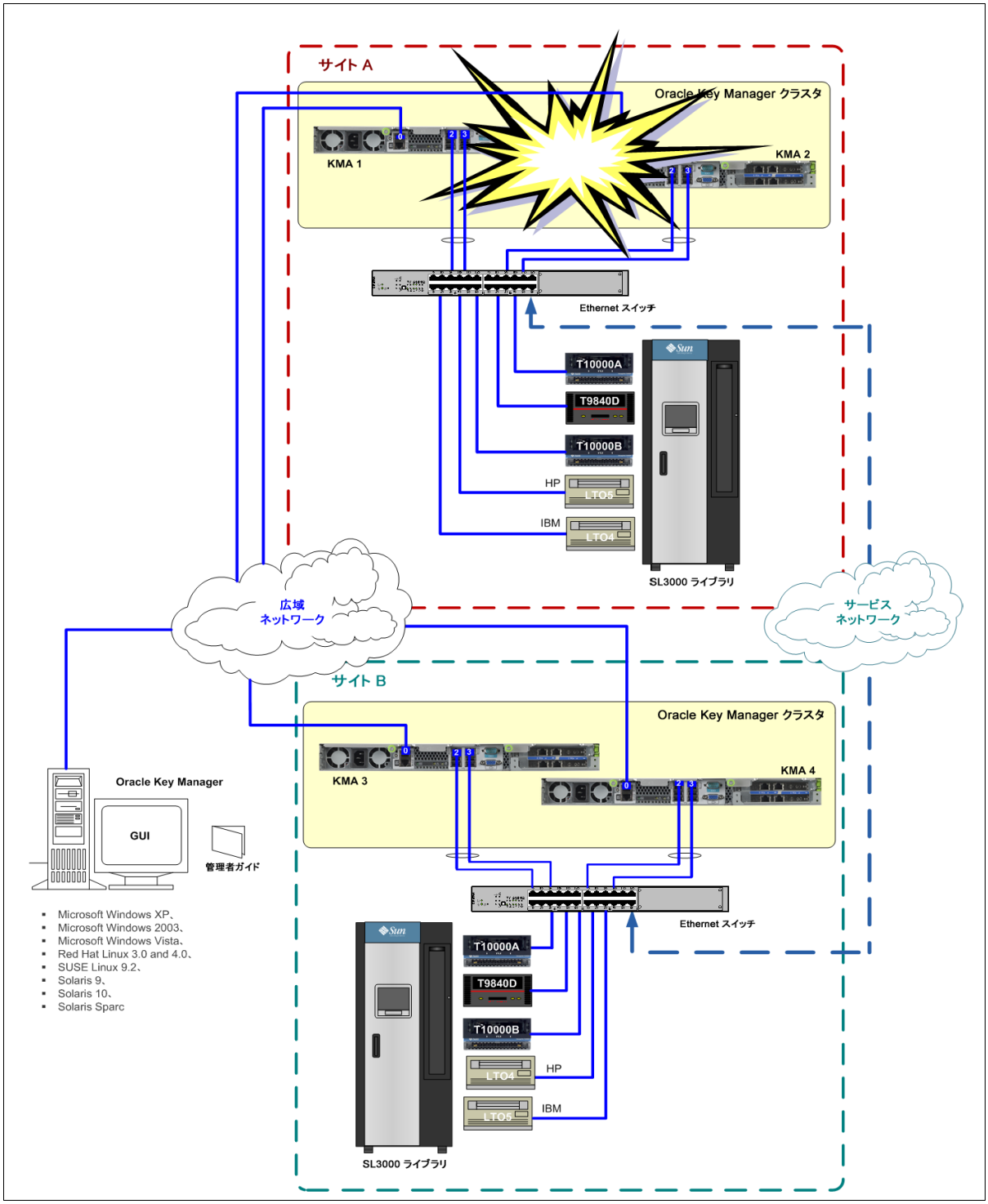
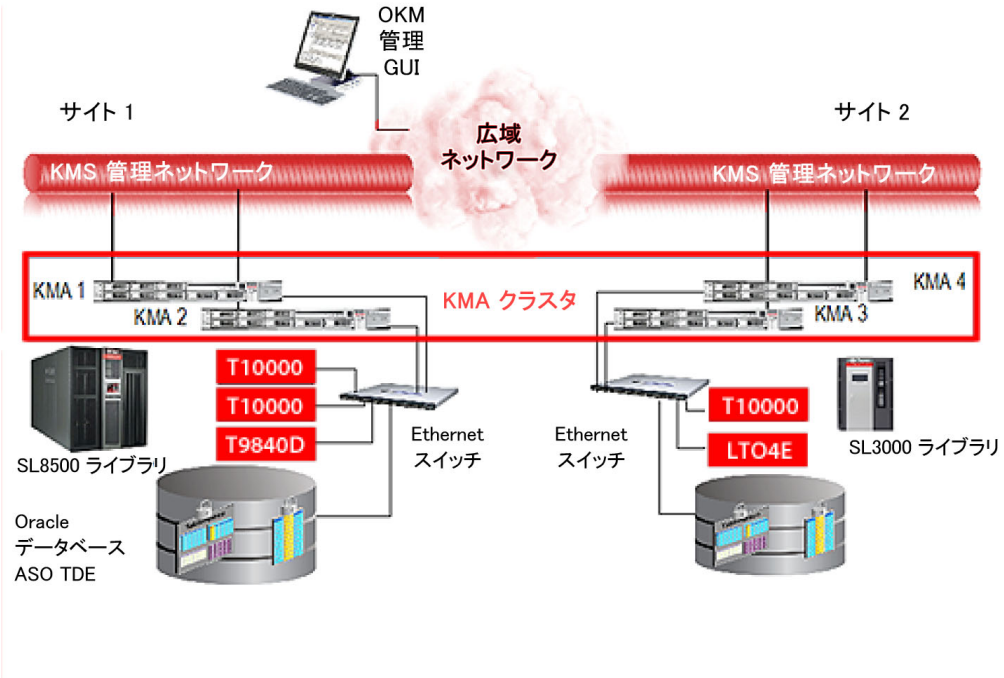


図 1-5 データベースの例

この例では、クラスタ内の 4 つの KMA は、Advanced Security の Transparent Data Encryption (TDE) ソリューションを使用して、自動テープライブラリおよび Oracle データベースの両方をサポートしています。



Oracle Key Manager は、Oracle Advanced Security の Transparent Data Encryption の認定を受けています。
これは、Oracle StorageTek テープドライブで使用されているのと同じ暗号化テクノロジーを Oracle 11*g* データベースの暗号化鍵の管理に利用できるようになったことを意味します。

詳細については、付録 B「Oracle データベースの暗号化」を参照してください。

鍵管理アプライアンス

鍵管理アプライアンス (KMA) には 3 種類のサーバーがあります。

- SunFire X2100 サーバー (オリジナル)
- SunFire X2200 サーバー (アップグレード)
- SunFire X4170 M2 サーバー (最新)

3 つのすべてのサーバーは機能的には同等です。

注 :

- OKM アプライアンスの以降のリリースでは、異なるサーバーハードウェアが使用されることがありますが、配備されている他の KMA と相互運用可能であることが保証されています。
- システムのアップグレードや拡張に伴って、あるいは障害の発生したユニットの代替として、OKM は SunFire X2100、X2200、および X4170 の組み合わせで構成されることがあります。

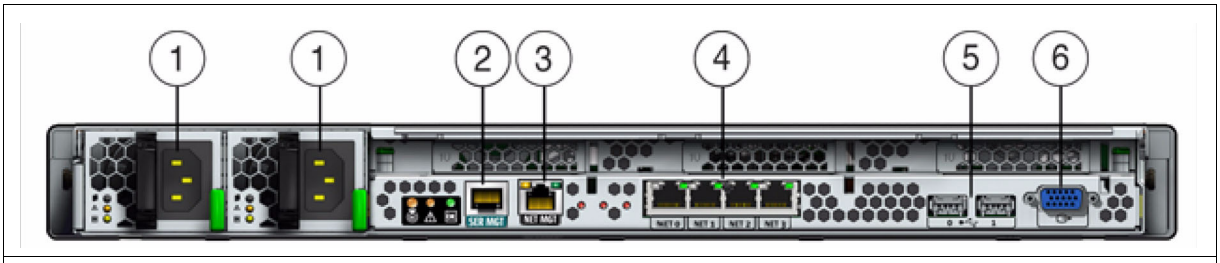
SunFire 4170 サーバー

図 1-6 は Sun Fire X4170 M2 サーバーの背面図を示しています。

図 1-7 は Sun Fire X4170 M2 サーバーの正面図を示しています。

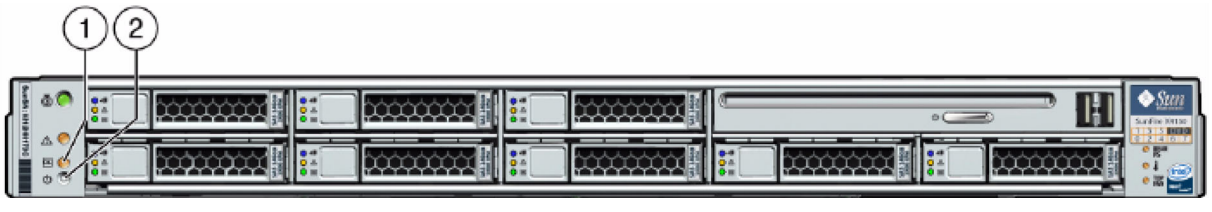
表 1-1 は Sun Fire X4170 M2 サーバーの仕様の一覧を示しています。

図 1-6 鍵管理アプライアンス - X4170 の背面パネル



1. AC 電源コネクタ
2. シリアル管理 (SER MGT) RJ-45 シリアルポート
3. サービスプロセッサ (NET MGT) ポート
4. Ethernet ポート (0、1、2、3)、これらのポートには左から右へ「Net0」から「Net3」のラベルが付けられています。
5. USB ポート (0、1)
6. ビデオコネクタ (VGA)

図 1-7 鍵管理アプライアンス - X4170 のフロントパネル



1. 電源 /OK LED
2. 電源ボタン

4170 コンポーネントの仕様

表 1-1 は Sun Fire X4170 M2 サーバーの仕様の一覧を示しています。

表 1-1 仕様

仕様	
プロセッサ	1 つのクアッドコア (2.4GHz)
メモリー	1 x 4G バイト DDR3 DIMM
管理用ソフトウェア	サービスプロセッサ標準 ILOM (Integrated Lights Out Manager)
外部ストレージ	1 つの SATA ディスクドライブ
PCI スロット	2 つの PCI-Express スロット (PCIe) PCIe-0 には Sun Crypto Accelerator (SCA6000) が含まれている (取り付け済みの場合)。
ネットワーク	背面パネルに 4 つの USB 2.0 コネクタ フロントパネルに 2 つの USB 2.0 コネクタ DB-15 コネクタ搭載 VGA 4 つの 10/100/1000 Base-T Ethernet ポート
寸法	
高さ	4.34 cm (1.71 インチ)
幅	42.5 cm (16.75 インチ)
奥行き	68.58 cm (27.0 インチ)
重量	16.36 kg (36 ポンド)
環境	
動作時温度	5 - 35C (41 - 95F)
非動作時温度	-40 - 70°C (-40 - 158°F)
動作時湿度	10 - 90% の相対湿度、結露なし

表 1-1 仕様 (続き)

非動作時湿度	最大 93% の相対湿度、結露なし
高度 (動作時)	最大 3000m、最大周囲温度は 900m を超えると 300m ごとに摂氏 1 度ずつ下がる
高度 (非動作時)	最大 12,000m

SunFire X2100 および X2200 サーバー

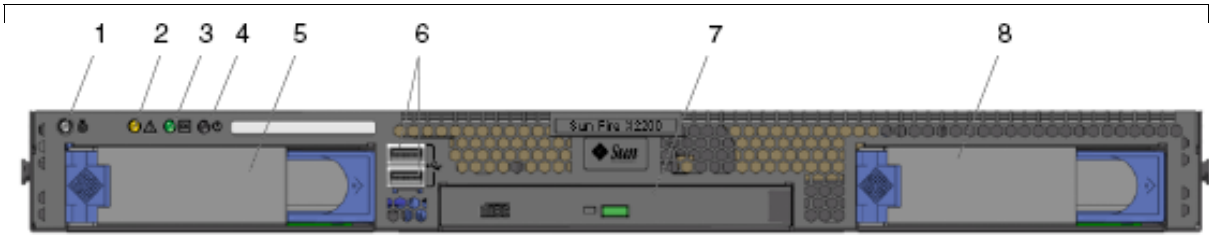
図 1-8 は Sun Fire X2100/2200 M2 サーバーの背面図を示しています。

図 1-9 は Sun Fire X2100/2200 M2 サーバーの正面図を示しています。

表 1-2 は Sun Fire X2100 M2 サーバーの仕様の一覧を示しています。

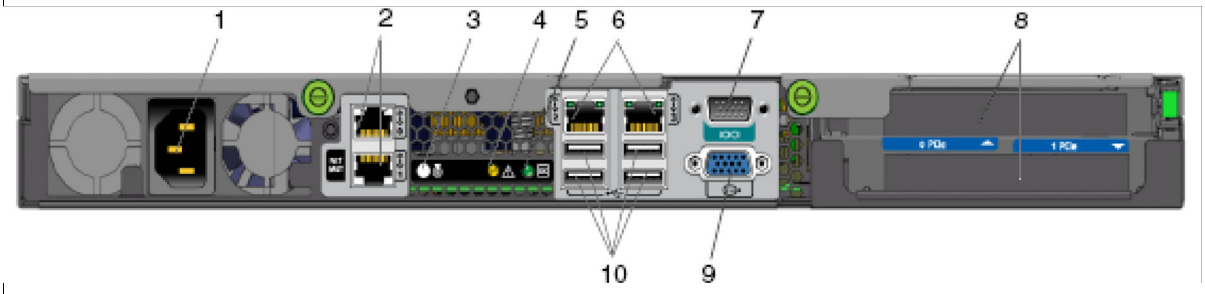
表 1-3 は Sun Fire X2200 M2 サーバーの仕様の一覧を示しています。

図 1-8 鍵管理アプライアンス - 2100/2200 のフロントパネル



1. システム識別ボタン /LED
2. 障害 LED
3. 電源 /OK LED
4. 電源ボタン
5. オプションのハードディスクドライブベイ (0)
6. USB 2.0 コネクタ (2)
7. CD/DVD ドライブ (割り当てなし)
8. オプションのハードディスクドライブベイ (1)

図 1-9 鍵管理アプライアンス - 2100/2200 の背面パネル



1. 電源コネクタ
2. Ethernet コネクタ (2)
   上部 = KMA 管理ネットワーク (LAN 0)
   下部 = ELOM (Embedded Lights Out Manager)
3. システム識別 LED
4. 障害 LED
5. 電源 LED
6. Ethernet サービスネットワーク接続 (2)
   左 = サービスネットワーク (LAN 2)
   右 = 集合サービスネットワーク (LAN 3)
7. シリアルポート (DB9、RS232)
8. PCIe スロット (2)
   上部 = SCA6000 カード (表示なし)
   下部 = ブランク (空)
9. VGA コネクタ (初期構成にモニターまたはキーボードを使用している場合)
10. USB 2.0 ポート (4)

SunFire X2100 サーバー

表 1-2 は SunFire X2100 サーバーの仕様の一覧を示しています。

表 1-2 SunFire X2100 の仕様

仕様	
プロセッサ	■ 1 つのデュアルコア AMD Operton プロセッサ ■ プロセッサ周波数 : 2.2GHz ■ 最大 1M バイトのレベル 2 キャッシュ
メモリー	■ 4 つの DIMM スロット (最大 4G バイト) ■ バッファーなし ECC メモリー
IPMI 2.0	■ サービスプロセッサ標準 ■ Embedded Lights Out Manager
外部ストレージ	1 つの SATA ディスクドライブ
PCI スロット	2 つの PCI-Express スロット (PCIe) PCIe-0 には Sun Crypto Accelerator 6000 (SCA6000) が含まれている
ネットワーク	■ 背面パネルに 4 つの USB 2.0 コネクタ ■ フロントパネルに 2 つの USB 2.0 コネクタ ■ 2 つのポート : DB-9 搭載シリアルポート、DB-15 搭載 VGA ■ 4 つの 10/100/1000 Base-T Ethernet ポート
寸法 :	
高さ	43mm (1.7 インチ)
幅	425.5mm (16.8 インチ)
奥行き	550mm (21.68 インチ)
重量 (最大)	10.7 kg (23.45 ポンド)
取り付けオプション	19 インチラックマウントキット、圧縮 1 ラックユニット (1.75 インチ)
環境パラメータ :	
温度	5 - 35°C (41 - 95°F)
相対湿度	27°C (80°F) 最高湿球温度
高度	最大 3,000 m (9,000 フィート)
電源装置	90 - 2640 VAC、47 - 63 Hz 1 つの 6.5 アンペアの非冗長電源 (345 ワット) 熱出力は約 850 BTU/ 時
規制では次の要件が満たされるかそれを上回る :	
音響ノイズの放出は ISO 9296 に従って報告される	
安全性 IEC 60950、UL/CSA60950、EN60950、CB スキーム	
RFI/EMI FCC Class A、Part 15 47 CFR、EN55022、CISPR 22、EN300-386:v1.31、ICES-003	

表 1-2 SunFire X2100 の仕様 (続き)

イミュニティー : EN55024、EN300-386:v1.3.2
認証 : 安全性 CE Mark、GOST、GS Mark、cULus Mark、CB スキーム、CCC、S Mark
EMC CE Mark、放出およびイミュニティークラス A 放出レベル : FCC、C-Tick、MIC、CCC、GOST、BSMI、ESTI、DOC、S Mark

SunFire X2200 サーバー

表 1-3 は SunFire X2200 サーバーの仕様の一覧を示しています。

表 1-3 SunFire X2200 の仕様

仕様	
プロセッサ	■ 2 つのクアッドコア AMD Opteron プロセッサ ■ プロセッサ周波数 : 2.3GHz
メモリー	■ 8G バイトの RAM、4 として取り付け、2G バイトの Dimm
IPMI 2.0	■ サービスプロセッサ標準 ■ Embedded Lights Out Manager
外部ストレージ	1 つの SATA ディスクドライブ 250G バイトの容量
PCI スロット	2 つの PCI-Express スロット (PCIe) PCIe-0 には Sun Crypto Accelerator 6000 (SCA6000) が含まれている
ネットワーク	■ 背面パネルに 4 つの USB 2.0 コネクタ ■ フロントパネルに 2 つの USB 2.0 コネクタ ■ 2 つのポート : DB-9 搭載シリアルポート、DB-15 搭載 VGA ■ 4 つの 10/100/1000 Base-T Ethernet ポート
寸法 :	
高さ	43mm (1.69 インチ)
幅	425.5mm (16.75 インチ)
奥行き	633.7mm (25 インチ)
重量	1.6 kg (24.64 ポンド)
取り付けオプション	19 インチラックマウントキット、圧縮 1 ラックユニット (1.75 インチ)
環境パラメータ :	
温度	5 - 35°C (41 - 95°F)
相対湿度	27°C (80°F) 最高湿球温度
高度	最大 3,000 m (9,000 フィート)
電源装置	100 - 240 VAC、47 - 63 Hz 1 つの 8 アンペアの非冗長電源 (500 ワット) 熱出力は約 850 BTU/ 時
規制では次の要件が満たされるかそれを上回る :	
安全性 : CE、CB スキーム、UL、CSA、CCC、BSMI、AR-S、GOST-R	
EMC: CE、FCC、VCCI、ICES、BSMI、CCC、MIC、C-Tick、AR-S、GOST-R	
その他 : RoHS 準拠のラベル付き、WEEE (Waste Electrical and Electronics Equipment) 指令 (2002/95/EC) に準拠	

ネットワークに関する考慮事項

Oracle では、**プライベートサービスネットワーク**上で KMA をテープドライブに接続できるように、顧客が管理されたスイッチを提供することをお勧めします。管理されたスイッチはその後、管理されていない提供済みのテープドライブスイッチと広域サービスネットワーク用の顧客提供のルーターに接続します。

次の管理されたスイッチは、エンジニアリングによってテストされ推奨されています。

- 3COM Switch 4500G 24-Port (3CR17761-91)
- Extreme Networks Summit X150-24t スイッチ

他の管理されたスイッチも使用できます。ただし、上記のスイッチについてのみ構成ガイダンスがあります。

次の理由により、管理されたスイッチが推奨されます。

- 優れたスイッチ診断とサービスネットワークの障害追跡による保守性の向上
- 冗長接続とスパニングツリープロトコルの使用によりサービスネットワーク上のシングルポイント障害を最小限に抑える可能性
- KMA のサービスインタフェース上のシングルポイント障害を最小限に抑えるために KMA サービスネットワークインタフェースの集約のサポート

18 ページの 図 1-10 は、管理されたスイッチの構成例を示しています。この例では、どちらかの KMA または管理されたスイッチに障害が発生しても、ドライブは他方の KMA との通信を行えるパスを引き続き保持できます。

管理ネットワーク

OKM ネットワークでは、最適なレプリケーションとパフォーマンスを得るためにクリーンなギガビット Ethernet 接続を使用するようにしてください。

ELOM と ILOM

ELOM または ILOM ネットワークでは、スパニングツリーをオフまたは無効にしておくようにしてください。

KMA サービスポートの集約

バージョン 2.1 以降、物理的な Ethernet インタフェース (LAN 2 および LAN 3) を 1 つの仮想インタフェースに集約できるようになりました。これらのポートを集約することで可用性が向上します。つまり、どちらかのポートで障害が発生しても他方のポートが接続を維持できます。

Ethernet スイッチポートが正しく構成されていることを確認してください。
たとえば、スイッチポートは次のようにしてください。

- デュプレックスの設定を自動ネゴシエーションするように設定します (全二重にする)。
- 速度設定を自動ネゴシエーションするように設定します。KMA ポートはギガビット速度に対応しています。

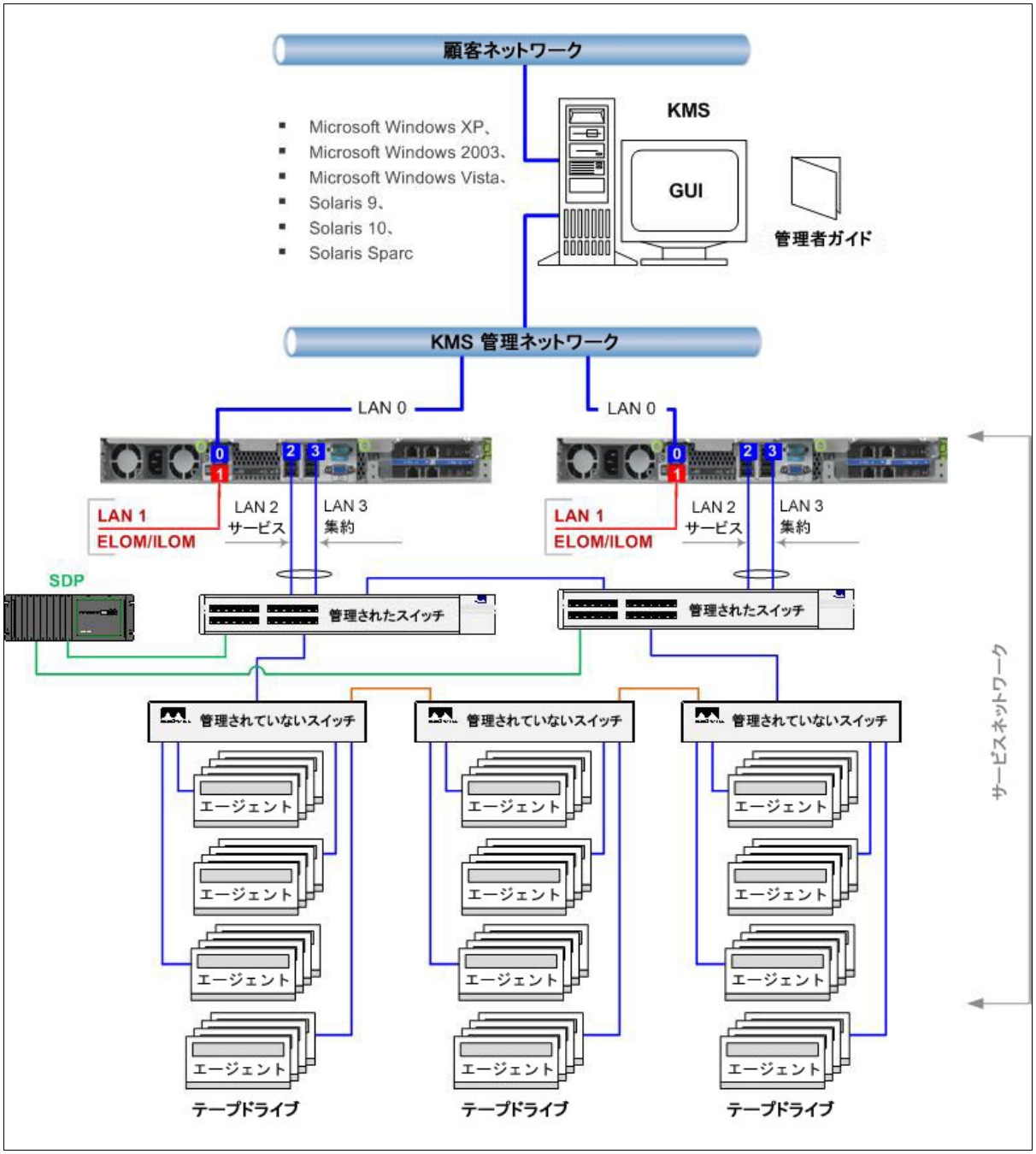
- 同一の速度を使用します。例 : どちらも 100Mbps に設定 (速度の自動ネゴシエーションがうまく機能することがある)。

図 1-10 管理されたスイッチの構成

この例では、サービスネットワークは管理されていない 3 つのスイッチに接続されている 2 つの顧客提供の管理されたスイッチで構成されます。その中には、スパニングツリー構成を必要とする冗長パスが含まれています。この例は、KMA、スイッチハードウェア、およびテープドライブを追加することで、大規模な SL8500 ドライブ構成用に簡単に拡張できます。

- 配線に冗長性があるときは必ず管理されたスイッチがスパニングツリーに対して有効になっている必要があります。
- 冗長性を確保するために、管理されていないスイッチには管理されたスイッチへのパスが 2 つあります。
- 管理されていないスイッチはその後、テープドライブ (エージェント) にケーブルで接続されます。
- 管理されていないスイッチにはそれぞれ 16 台のドライブが接続されます。4 台 1 組で接続されます。ポート 1 - 4、6 - 9、11 - 14、16 -19。
- Service Delivery Platform (**SDP**) は管理された各スイッチにポート 1 で接続されます。

図 1-10 管理されたスイッチの構成



それぞれの鍵管理アプライアンスには 4 つのネットワーク接続があります。次のとおりです。

- LAN 0 = 4170M2 アプライアンス用の管理ネットワーク (Net0)
- LAN 1 = サービスプロセッサ (ELOM または ILOM) ネットワーク (Net1)
- LAN 2 = サービスネットワーク (Net2)
- LAN 3 = 集合サービスネットワーク (Net3)

表 1-4 KMA ネットワーク接続

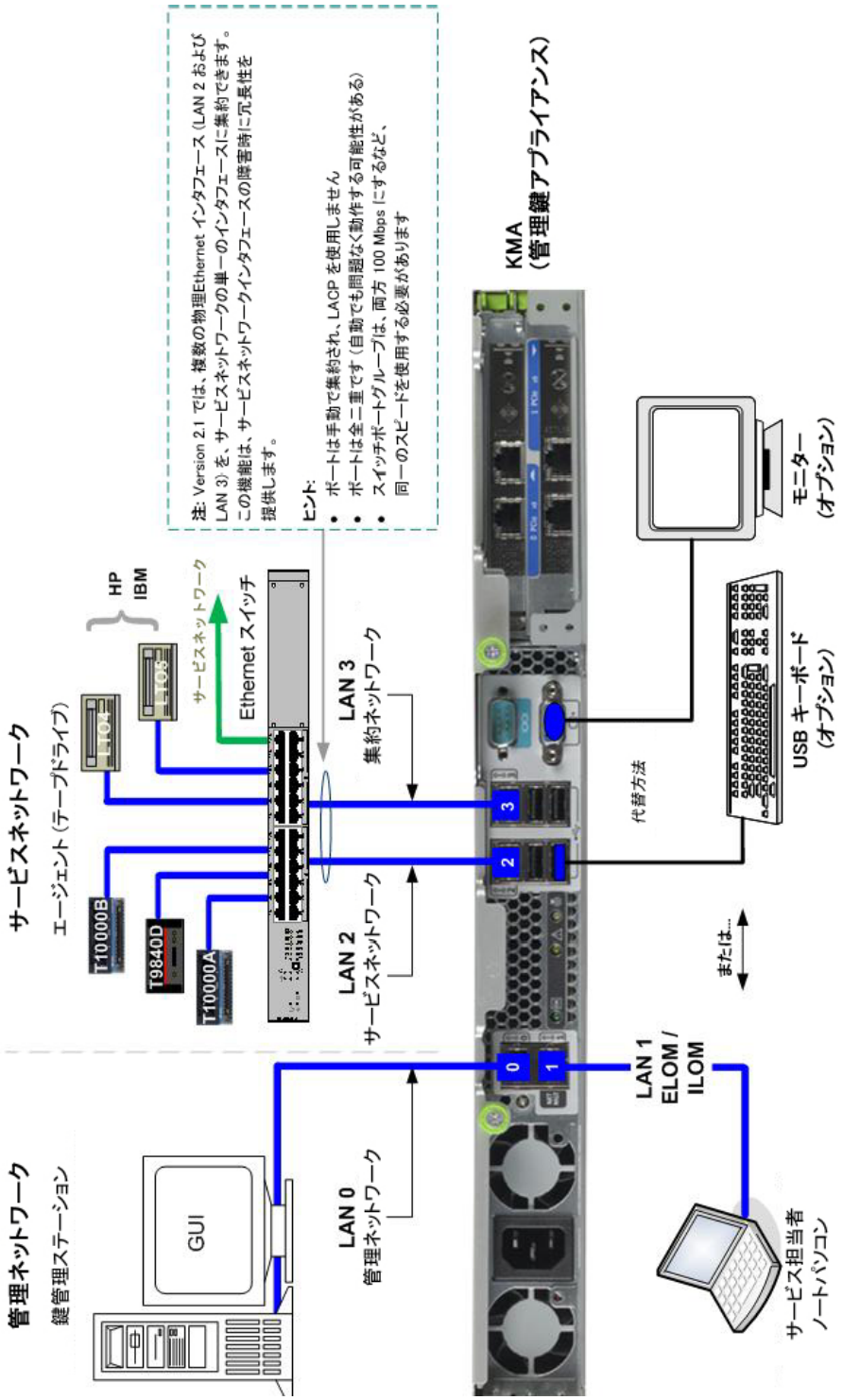
LAN 0	これは必須の接続です。 このネットワークは「管理ネットワーク」と呼ばれ、GUI または CLI. をホストする鍵管理アプライアンスや管理クライアントと相互接続します。このネットワークはローカル、リモート、または両者の組み合わせのいずれでもかまいません。 **注 - このネットワークと接続は顧客が提供する必要があります。**
LAN 1*	この接続は「NET MGT ELOM」と呼ばれ、Embedded Lights Out Manager にネットワーク接続を提供します。このインタフェースを介して KMA コンソールをリモートで起動し、アクセスできます。
LAN 2	これは通常、テープドライブに必須の接続です。 このネットワークは**「サービスネットワーク」**と呼ばれ、直接または Ethernet スイッチ経由でテープドライブに接続してネットワークを作成します。
LAN 3	これはバージョン 2.1 とのオプションの接続であり、管理されたスイッチを必要とします。LAN 3 は、KMA が LAN 2 と集約して 1 つの集合サービスポートになる追加のサービスネットワークインタフェースを提供します。 集約または IEEE 802.1AX-2008 はネットワーク用語であり、複数のネットワークケーブルおよびポートを同時に使用して、可用性向上のためにリンク速度と冗長性を高めることを表します。
*** 注 -** ELOM IP アドレスはシリアル接続を使って非常に簡単に設定できます。最初に、DB9-DB9 シリアルヌルモデムケーブルをノートパソコンのシリアルポートからサーバーのシリアルポートに接続します。	

KMA の初期設定では、ELOM (Embedded Lights Out Manager) にアクセスするために、ノートパソコンまたはモニター / キーボード構成部品上に端末エミュレータが必要になります。ELOM とは、これらの機能を使用するためにネットワーク接続と IP アドレスを必要とする遠隔コンソール機能です。

鍵管理アプライアンスの物理接続

物理接続はすべて KMA の背面から行われます。次の図は、Sun Fire X2100 または X2200 サーバーを示しています。

図 1-11　鍵管理アプライアンス - 背面パネルの接続



インターネットプロトコルバージョン

バージョン 2.1 に行われた機能拡張で、インターネットプロトコル群 (IP) の最新の実装がサポートされるようになりました。

- 現在のバージョンである IPv4 では、3 つずつピリオドで区切られた 4 つの数字グループとして記述される 32 ビットの数値を使用します。各グループには 0 から 255 を使用できます (例 : 129.80.180.234)。

  これらの 4 つのグループには、2 つの識別子、ネットワークアドレスとホストアドレスがあります。最初の 2 つのグループ (129.80) でネットワークアドレスを識別し、次の 2 つのグループ (180.234) でホストを識別します。

- 次世代の **IPv6** では、4 つずつコロンで区切られた 8 つの 16 進文字グループとして記述される 128 ビット値を使用し、たとえば 2001:0db8:85a3:0000:0000:8a2e:0370:7334 2001:0db8:85a3:::8a2e:0370:7334 (上記と同じ意味) のようになります。

  IPv6 アドレスは通常 2 つの論理部分、64 ビットのネットワーク接頭辞と 64 ビットのホストアドレス (自動的に生成されるか割り当てられる) で構成されます。

重要 :
Key Manager では、システム内で両方のプロトコルが使用される「デュアルスタック」の実装をサポートしています。ただし、ドメインネームシステム (DNS) など、すべてのアプライアンスが IPv6 を使用するとは限りません。このため、IPv4 は引き続き必要です。

自動テープライブラリ

お客様ごとにニーズや要件が異なるので、これらのお客様の要望を満たすために Oracle の StorageTek 自動テープライブラリにはさまざまなライブラリが用意されています。

表 1-5 テープライブラリ

テープライブラリ	L700	L1400	9310	SL24	SL48	SL500	SL3000	SL8500
最小スロット数	216	200	2,000	1	1	30 または 50	200	1,448
最大スロット数	1,344	1,344	6,000	24	48	440 - 575	5,925	10,000
コンプレックス /ACS	なし	なし	144,000	なし	なし	なし	なし	100,000
混合メディア	はい	はい	はい	なし	なし	はい	はい	はい
パススルーポート	あり (1)	あり (1)	はい	なし	なし	なし	なし	はい
最大ドライブ数	24、40	24、40	80、960	1	2	2、18	56	64、640
CAP サイズ	20 - 80	20 - 80	21 または 80	メールスロット	メールスロット	5 - 45	26	39
CAP 数	1 - 4	1 - 4	4 x 20	0 - 1	1 - 3	1 - 5	10[1]	2
インタフェースのタイプ	SCSI、FC	SCSI、FC	TCP/IP	SCSI、FC、SAS	SCSI、FC、SAS	SCSI、FC	SCSI、FC	TCP/IP
テープテクノロジ (暗号化対応のテープドライブのみ)								
T9840D (StorageTek)	はい	はい	はい	なし	なし	なし	はい	はい
T10000A (StorageTek)	はい	はい	はい	なし	なし	なし	はい	はい
T10000B (StorageTek)	はい	はい	はい	なし	なし	なし	はい	はい

表 1-5 テープライブラリ

テープライブラリ	L700	L1400	9310	SL24	SL48	SL500	SL3000	SL8500
LTO4 (HP および IBM)	なし	なし	なし	サポートを確認		はい	はい	はい
LTO5 (HP および IBM)	なし	なし	なし	はい	はい	はい	はい	はい
1. アクセス拡張モジュールには、234 から 468 個のカートリッジ (1 台または 2 台の AEM) の一括カートリッジロード機能が備わっています。								

テープドライブ

最新式のテープテクノロジで知られている StorageTek には、テープとテープの自動化に関する長年にわたる経験とリーダーシップがあります。今日では、StorageTek はその実証されたテクノロジを用いてストレージソリューションを次に提供し続けています。

- 小規模から大規模までの企業および組織
- エンタープライズおよびクライアントサーバーのプラットフォーム
- スタンドアロンおよび自動テープ環境

次の 7 つのテープドライブモデルから選択できます。

- StorageTek T10000A
- StorageTek T10000B
- StorageTek T10000C
- StorageTek T9840 モデル D のみ
- HP (Hewlett Packard) LTO (Linear Tape-Open) 第 4 および第 5 世代
- IBM (International Business Machines) LTO (Linear Tape-Open) 第 4 および第 5 世代

FIPS 準拠のテープドライブ

バージョン 2.1 および最新のテープドライブファームウェア以降、次のドライブは FIPS[3] に準拠しています。

表 1-6 FIPS 140-2 準拠のテープドライブ

テープドライブ	FIPS 140-2 のレベル
T10000A	1
T10000B	2
T10000C	2
T9840D	1
LTO4 (HP および IBM)	FIPS への対応なし *
LTO5 (HP および IBM)	FIPS への対応なし *
* LTO ドライブはその基本形式で FIPS 検証が行われる可能性がありますが、それぞれの暗号化アプリケーションで必ずしも行われるとは限りません。	

上記テープドライブの FIPS 140-2 レベルのセキュリティーには、レベル 1 と 2 があります。

レベル 1 – 生産グレードでの要件を備えた基本レベル。

レベル 2 – 物理的な改ざんの証拠や役割ベースの認証のための要件が追加されます。検証済みのオペレーティングシステムで構築されます。

3. **FIPS 140-2** とは暗号化モジュールの認可に使用される米国政府のコンピュータセキュリティー標準です。米国連邦情報処理標準 (Federal Information Processing Standards、FIPS) は米国連邦政府が開発した公表されている標準とガイドラインです。多くの FIPS 標準は、より広いコミュニティー (ANSI、NIST、IEEE、ISO など) で使用される更新版の標準です。

この選択では、KMA とテープドライブのセキュリティーレベルが上がります。

StorageTek T10000 テープドライブについて

StorageTek T10000 テープドライブは、大容量ストレージ向けに設計されたモジュール式の高性能テープドライブです。

暗号化をサポートしている T10000 のモデルは 3 つあります。

- T10000A
- T10000B
- T10000C

寸法 : このテープドライブは次のとおりです。

- 高さ 8.89 cm (3.5 インチ)
- 幅 14.6 cm (5.75 インチ)
- 奥行 42.5 cm (16.75 インチ)

容量 :

- T10000A = 500G バイトの非圧縮データ
- T10000B = 1T バイトの非圧縮データ[4]
- T10000C = 5T バイトの非圧縮データ

StorageTek T9840D テープドライブについて

StorageTek T9840D テープドライブは、平均アクセス時間がわずか 8 秒という小型で高性能な**アクセス中心**のテープドライブです。

このドライブは、ミッドポイントロードテクノロジを用いた独自のデュアルハブカートリッジデザインを使用することで高性能を実現しています。これにより、テープの中央に読み取り / 書き込みヘッドを配置することで、高速アクセスが可能となり、待ち時間が短縮されます。

T9840 には 4 つのモデルがありますが、T9840D のみが暗号化をサポートしています。

寸法 : このテープドライブは次のとおりです。

- 高さ 8.25 cm (3.25 インチ)
- 幅 14.6 cm (5.75 インチ)
- 奥行 38.1 cm (15 インチ)

容量 :
T9840D = 75G バイトの非圧縮データ

各種オペレーティングシステムプラットフォームの場合 :

- エンタープライズメインフレーム (z/OS および OS/390)

4. **容量 :** 1T バイトの容量がどれくらいかを知るには、一般的な M バイトで考えてみてください。1,000M バイトをわずかに超えたところが 1G バイトに等しく、1,000,000M バイトをわずかに超えたところが 1T バイトに等しくなります。
1,024M バイト = 1G バイト
1,024G バイト = 1T バイト
1,048,576 ($1,024^2$)M バイト = 1T バイト

- オープンシステムプラットフォーム (Windows、UNIX、および Linux)

LTO テープドライブについて

概要

LTO (Linear Tape-Open) テープドライブは、エンタープライズメインフレームとオープンシステムの両方の環境でアプリケーションのバックアップと復元を行うために設計された、高性能かつ大容量のデータストレージデバイスです。
HP と IBM では、LTO4 および LTO5 テープドライブと呼ばれる第 4 および第 5 世代の Ultrium シリーズのリニアテープオープン製品を提供しています。
注 : 現在では、LTO4 および LTO5 テープドライブのみがテープベースまたはデバイスベースの暗号化をサポートしています。

暗号化に対応

HP と IBM の LTO ドライブは、Oracle の Key Manager などの安全な暗号化システムに組み込まれると、暗号の書き込みと復号の読み取りをサポートします。鍵管理は、テープに書き込まれている内容を将来確実に読み取れるようにするために不可欠です。
「暗号化の鍵」を管理できるようにするには、特別なカスタムデザインの Ethernet **アダプタカード**がドライブトレイの内側に取り付けられている必要があります。このアダプタカードは、LTO ドライブが Oracle Key Manager に接続し、インタフェースを取る手段を提供します。各ベンダーには独自のバージョンのアダプタカードがあります。

- HP LTO4 = Dione カード (外付け)
- HP LTO5 = 組み込み済み (アダプタカードは不要)
- IBM = Belisarius カード (外付け)

この接続により、LTO ドライブは OKM と通信してセキュリティー保護されたネットワークを介して暗号化鍵を転送できます。
注 : 現時点では LTO ドライブは**一度に 1 つの暗号化鍵のみを使用できます。**
読み取り操作中に、テープ上に別の暗号化鍵が見つかった場合、アダプタカードはその鍵を OKM に直接要求します。

メディア (ネイティブ容量)

LTO5 テープドライブは 1.5T バイトのデータカートリッジを使用し、LTO4 テープドライブは 800G バイトのデータカートリッジを使用します。どちらも他のベンダー製カートリッジや他の世代の LTO テープドライブと互換性があります。
このドライブは次の機能を実行します。

- Ultrium 5 形式 (WORM を含む) での LTO5 カートリッジの読み取り / 書き込み
- Ultrium 4 形式 (WORM を含む) での LTO4 カートリッジの読み取り / 書き込み

LTO5 および LTO4 テープドライブは WORM (Write Once, Read Many) セキュアメディアもサポートしています。この消去不能かつ再書きこみ不能のメディアは、HIPAA、Sarbanes-Oxley、SEC 17A-4 などの規制に適合しています。

インタフェース

LTO ドライブには、シングルまたはデュアルポート構成のファイバチャネルインタフェース (FC) が備わっています。
HP LTO テープドライブは次もサポートしています。

- Ultra 320 SCSI (Small Computer System Interface)

テープドライブの比較

表 1-7 テープドライブの比較

仕様	StorageTek				HP		IBM	
	T10K A	T10K B	T10K C	T9840D	LTO4	LTO5	LTO4	LTO5
容量 (ネイティブ)	500G バイト	1T バイト	5T バイト	75G バイト	800G バイト	1.5T バイト	800G バイト	1.5T バイト
転送速度 (ネイティブ)	120M バイト / 秒	120M バイト / 秒	240M バイト / 秒	30M バイト / 秒	120M バイト / 秒	140M バイト / 秒	120M バイト / 秒	140M バイト / 秒
バッファーサイズ	256M バイト	256M バイト	2G バイト	64M バイト	256M バイト	256M バイト	256M バイト	256M バイト
ロード時間 (秒)	16 秒	16 秒	13.1 秒	8.5 秒	19 秒	12 秒	15 秒	12 秒
アクセス (秒)	46 秒	46 秒	73.5 秒	8 秒	72 秒	60 秒	46 秒	60 秒
テープ速度 (m/ 秒)	2 - 4.95	2 - 3.74	5.62	3.4	7.0	-	7.0	-
巻き戻し時間 (秒)	90	90	10 - 13	16 / 8	106 / 54 秒	96 / 78 秒	106 / 54 秒	96 / 78 秒
アップロード時間	23 秒	23 秒	23 秒	12 秒	22 秒	17 秒	22 秒	17 秒
インタフェース								
ファイバチャネル	2 および 4G ビット / 秒	4G ビット / 秒	4G ビット / 秒	4G ビット / 秒	4G ビット / 秒	8G ビット / 秒	4G ビット / 秒	8G ビット / 秒
SCSI / SAS	なし	なし	なし	なし	Ultra-320	6G ビット SAS	Ultra-320	6G ビット SAS

表 1-7 テープドライブの比較 (続き)

仕様	StorageTek				HP		IBM	
	T10K A	T10K B	T10K C	T9840D	LTO4	LTO5	LTO4	LTO5
FICON	2G ビット / 秒	2G ビット / 秒	4G ビット / 秒	2G ビット / 秒	サポートなし		サポートなし	
ESCON	2G ビット / 秒	2G ビット / 秒	なし	2G ビット / 秒				
互換性								
可用性 (MTBF)	290,000 時間		290,000 時間		250,000 時間		250,000 時間	
トラック	768	1152	3,584	576	896	1280	896	1280
使用可能な長さ	855m (2805 フィート)	855m (2805 フィート)	1,107m (3,632 フィート)	251m (889 フィート)	820m (2690 フィート)	850m (2789 フィート)	820m (2690 フィート)	850m (2789 フィート)
VolSafe - WORM	あり	あり	あり	あり	あり	あり	あり	あり

参考のため、次の表にテープドライブとメディアの比較を示します。

StorageTek T シリーズのテープドライブ

表 1-8 は、T シリーズ (T10000 および T9840) ドライブのメディア互換性を示しています。

- 暗号化対応の T シリーズのテープドライブ
- 非暗号化の T シリーズのテープドライブ

表 1-8 T シリーズのテープドライブのメディア互換性

作業	暗号化登録済み	暗号化未登録
暗号化された新しいデータの書き込み	はい	なし
暗号化されていない新しいデータの書き込み	なし	はい
利用可能な鍵を使った暗号化データの読み取り	はい	なし
非暗号化データの読み取り	はい	はい
暗号化テープへの非暗号化データの追加	なし	なし

表 1-9 は、次の比較を示しています。

- 暗号化対応テープドライブと非暗号化テープドライブ
- 暗号化メディアと非暗号化メディア

表 1-9 T シリーズのテープドライブとメディアのサポート

テープドライブのタイプ	メディアタイプ	
	非暗号化テープ	暗号化テープ
標準のドライブ (非暗号化)	■ 完全に互換性あり ■ 読み取り、書き込み、および追加	■ このテープに対する読み取り、書き込み、追加はできない ■ テープの先頭 (BOT) からの書き換えは可能
暗号化対応のドライブ	■ **読み取り**機能のみ ■ このテープへの追加は不可 ■ テープの先頭 (BOT) からの書き換えは可能	■ 完全に互換性あり ■ 適切な鍵を使った読み取り ■ 現在の書き込み鍵を使った書き込み

LTO テープドライブ

注 : HP と IBM の LTO テープドライブは次のようになっています。

- LTO U-28、U-316、および U-416 仕様に準拠している他のテープドライブの暗号化されていないデータカートリッジと交換するよう指定されている。
- 適切な暗号化鍵が使用できる場合は、暗号化データカートリッジを交換できる。

将来の互換性 :

将来、LTO ドライブでは次が可能になります。

- 現世代のテープの読み取りと書き込み
- *1* 世代前のテープの読み取りと書き込み
- *2* 世代前のテープの読み取り

注 – 暗号化は、LTO4 および LTO5 テープドライブ上の LTO4 および LTO5 データカートリッジでのみサポートされています。問題を避けるために、これらのドライブではいったんドライブが暗号化対応になると、通常モードまたはネイティブモードでの書き込みは行われません。

LTO の暗号化の動作

LTO の暗号化が Oracle Key Manager によって制御されていると、LTO ドライブの動作が StorageTek T シリーズのドライブと異なる場合があります。HP のドライブと IBM のドライブの間にもわずかな違いがあることもあります。これらの違いは、IBM と HP のドライブアーキテクチャーの個々の局面から生じています。

表 1-10 に、さまざまなシナリオと HP および IBM のドライブの動作を示します。

表 1-10 LTO4 の暗号化の動作

LTO4 ドライブの性能	HP による実装	IBM による実装
暗号化未登録		
LTO4 の非暗号化データの読み取り	非暗号化を許可	非暗号化を許可
LTO4 暗号化データの読み取り	エラー	エラー
BOT からの LTO4 の書き込み	非暗号化を許可	非暗号化を許可
LTO3 テープの読み取り	非暗号化を許可	非暗号化を許可
LTO4 の非暗号化データへの追記書き込み (空白の EOD と書き込み)	非暗号化を許可	非暗号化を許可
LTO4 の非暗号化データへの追記書き込み (EOD までの読み取りと書き込み)	非暗号化を許可	非暗号化を許可
LTO4 の暗号化データへの追記書き込み (空白の EOD と書き込み)	非暗号化を許可 (注 1)	非暗号化を許可 (注 1)
LTO4 の暗号化データへの追記書き込み (EOD までの読み取りと書き込み)	エラー	エラー
暗号化登録済み		
LTO4 の非暗号化データの読み取り	非暗号化を許可	非暗号化を許可

表 1-10 LTO4 の暗号化の動作 (続き)

LTO4 ドライブの性能	HP による実装	IBM による実装
LTO4 暗号化データの読み取り	暗号化を許可 *	暗号化を許可 *
BOT からの LTO4 の書き込み	暗号化を許可 *	暗号化を許可 *
LTO4 の暗号化データへの追記書き込み	暗号化を許可 *	暗号化を許可 *
LTO3 テープの書き込み	非暗号化を許可 (注 5)	エラー (注 6)
LTO3 テープの読み取り	非暗号化を許可	非暗号化を許可
LTO4 の非暗号化データへの追記書き込み (空白の EOD と書き込み)	暗号化を許可 * (注 2)	エラー (注 3)
LTO4 の非暗号化データへの追記書き込み (EOD までの読み取りと書き込み)	暗号化を許可 * (注 2)	エラー (注 3)
LTO4 の暗号化データへの追記書き込み (空白の EOD と書き込み)	暗号化を許可 *	暗号化を許可 *
LTO4 の暗号化データへの追記書き込み (EOD までの読み取りと書き込み)	暗号化を許可 *	暗号化を許可 * - ただし、前の読み取り鍵を使用 (注 4)
* 適切な鍵を使用できる場合。		

注 1	エンタープライズドライブでは、1 つのテープ上に暗号化データと非暗号化データを混在させることはできません。
注 2	このシナリオでは非暗号化データのあとに暗号化データを追加できる上に、非暗号化データのラベルがあらかじめ付いているテープをラベルを張り替えなくても暗号化環境の HP LTO ドライブで使用できるため、操作上のメリットもあります。
注 3	このシナリオでは、HP のドライブとは異なり、IBM のドライブはエラーになります。
注 4	このシナリオでは、IBM のドライブは暗号化データを書き込みますが、テープ上の前の暗号化データの読み取りに使用したのと同じ鍵を使用します。書き込みコマンドが発行されてもドライブは OKM に新しい鍵を要求しません。これにより、OKM によって設定された鍵の有効期限ポリシーは無視されます。
注 5	HP のドライブは非暗号化モードでテープを書き込みます。LTO3 形式では暗号化はサポートされておらず、LTO3 カートリッジを挿入するだけで HP LTO4/LTO5 ドライブは非暗号化データを書き込めるようになるため、セキュリティー違反とみなされることがあります。
注 6	LTO3 テープへの書き込みを試みると、IBM のドライブはエラーを報告します。

ASR (Auto Service Request) 機能

ASR (Auto Service Request) とは、特定のハードウェア障害が発生した場合に自動的に Oracle サービスを依頼するように設計されている、Oracle Premier Support for Systems および Oracle/Sun Limited Warranty のフォンホーム機能です。

ASR は、Oracle サービスにハードウェア障害についての問い合わせを始める必要性をなくし、必要な通話回数と通話時間全体を減らすことで、より迅速に問題を解決するように設計されています。また、ASR は電子診断データを利用することで、サポート操作を簡素化しています。ASR はインストールと配備が簡単で、安全性を確保するためにユーザーによって完全に制御されます。

ASR を有効にする場合は、リリース 2.4 の管理ガイドの Auto Service Request を参照してください。

注 - この機能を有効にするには、セキュリティー責任者の役割アクセスが必要です。

第 **2** 章

システムアシュアランス

この章では、システムアシュアランスプロセスについて説明します。

システムアシュアランスプロセスとは、Oracle Key Manager の販売、注文、導入、および実装の面で見落としがないようにチームのメンバー間で情報交換を行うことです。このプロセスは間違いのない導入を推進し、全体的な顧客満足度の向上に役立ちます。

システムアシュアランスチームのメンバー (顧客および Oracle/StorageTek の担当者) は、このプロセスのすべての局面が慎重に計画され、効率的に実行されるようにします。このプロセスは、顧客がセールス提案書を受理したときに開始されます。この時点で、担当者はシステムアシュアランス計画ミーティングのスケジュールを立てます。

計画ミーティング

システムアシュアランス計画ミーティングの目的は次のとおりです。

- 顧客に Oracle の暗号化製品を紹介する
- システムアシュアランスプロセスについて説明し、チームを確立する
- 顧客の要件を特定し、定義する
- その他の必要な項目 (ケーブル、トークン、スイッチなど) をすべて洗い出す
- 導入と実装の準備をする
- プロセス全体をスケジュールし、追跡する

表 2-1 システムアシュアランス作業のチェックリスト

作業	完了したか
チームのメンバーを顧客に紹介します。 チームメンバーの連絡先シートのすべての項目に記入します。 必要に応じてコピーを取ります。	はい ❑ いいえ ❑
顧客に暗号化ソリューションについて説明します。 トピックと情報については、第 1 章「はじめに」を参照してください。	はい ❑ いいえ ❑
第 2 章「システムアシュアランス」を使用して顧客の要件の定義に役立てます。	はい ❑ いいえ ❑
チームメンバーの連絡先シートのすべての項目に記入します。	はい ❑ いいえ ❑
第 3 章「サイトの準備」を確認し、完了します。 コメント :	はい ❑ いいえ ❑
「ユーザー役割ワークシート」を見直して確認します。 コメント :	はい ❑ いいえ ❑
第 4 章「コンポーネント」を確認します。 コメント :	はい ❑ いいえ ❑
「サポートされる構成」を確認します。 コメント :	はい ❑ いいえ ❑
導入スケジュールを立てます。 **日付 :** _____ **時間 :** _____	はい ❑ いいえ ❑
次のコピーをダウンロードして顧客に提供します。『管理者ガイド』 PN: 316195101『Virtual Operator Panel—Customer』PN: 96179 http://download.oracle.com/docs/cd/E24472_01/index.html	はい ❑ いいえ ❑

顧客側のチームメンバーの連絡先シート

顧客側のチームメンバーに関する次の情報を記入します。

名前 :
役職 :
電話番号 :
FAX 番号 :
携帯電話 / ポケットベル :
電子メールアドレス :

名前 :
役職 :
電話番号 :
FAX 番号 :
携帯電話 / ポケットベル :
電子メールアドレス :

名前 :
役職 :
電話番号 :
FAX 番号 :
携帯電話 / ポケットベル :
電子メールアドレス :

名前 :
役職 :
電話番号 :
FAX 番号 :
携帯電話 / ポケットベル :
電子メールアドレス :

注 – 顧客側の担当者 : セキュリティー責任者、財務マネージャー、IT マネージャー、ネットワーク管理者、システム管理者、サイト計画マネージャー、それ以外の導入に関わる人など。

Oracle 側のチームメンバーの連絡先シート

Oracle 側のチームメンバーに関する次の情報を記入します。

名前 :
役職 :
電話番号 :
FAX 番号 :
携帯電話 / ポケットベル :
電子メールアドレス :

名前 :
役職 :
電話番号 :
FAX 番号 :
携帯電話 / ポケットベル :
電子メールアドレス :

名前 :
役職 :
電話番号 :
FAX 番号 :
携帯電話 / ポケットベル :
電子メールアドレス :

名前 :
役職 :
電話番号 :
FAX 番号 :
携帯電話 / ポケットベル :
電子メールアドレス :

注 – 担当者 : マーケティング担当者、販売担当者、アカウント担当者、システムエンジニア (SE)、プロフェッショナルサービス (PS)、導入コーディネーター、訓練を受けたサービス要員など。

構成の計画

次のチェックリストのすべての項目に記入し、導入に役立つ概念図を作成します。この情報と図面を導入担当者に提供します。

顧客が検討している Key Manager ごとにこのチェックリストを使用します。このチェックリストは、最大 20 台の OKM を含む、単一の Oracle Key Manager システムの計画に合わせられています。

表 2-2 ソリューションの計画チェックリスト

質問	選択 / コメント	数量
顧客が望んでいる構成のタイプは何ですか。 **注 :** ■ KMA を備えたサイトの最大数は 20 です。顧客が提供する広域ネットワークを介して接続されている KMA のないサイトを持つことも可能です。 ■ また、20 サイトの制限は 1 つのクラスタ内でのものです。顧客は複数のクラスタを持つことを選択してもかまいません。ただし、あるクラスタ内の KMA は他のクラスタ内の KMA を認識しません。	❑ 単一のサイト ❑ 複数のサイト ❑ 障害回復のサイト	個数 : _____ _____ _____
アプライアンス (KMA) はいくつ必要ですか。 ■ KMA の最大数は 20 です。 ■ OKM の最小サイズは 2* です。 ■ 2 以上を推奨します (サイトは地理的に分散しているものとする)。 * この標準構成 (単一ノードのサイト) から外れる場合は、暗号化エンジニアリング、プロフェッショナルサービス、およびサポートサービスの 同意を得る必要があります。		個数 : _____
必要な暗号化**ハードウェアキット**のタイプは何ですか。 暗号化ハードウェアキットはいくつ必要ですか。	❑ SL8500 ❑ SL3000 ❑ SL500 ❑ 9310 / 9741E ❑ L シリーズ ❑ ラックマウント	個数 : _____ _____ _____ _____ _____ _____
どのタイプの暗号化対応テープドライブがいくつ必要ですか。	❑ T10000A ❑ T10000B ❑ T10000C ❑ T9840D ❑ HP LTO 4 または 5 ❑ IBM LTO 4 または 5	個数 : _____ _____ _____ _____ _____

表 2-2 ソリューションの計画チェックリスト (続き)

質問	選択 / コメント	数量
外付け (スタンドアロン) のラックは必要ですか。 タイプは何ですか。	❑ はい ❑ いいえ	個数 : _____
顧客の要件と期待していることを洗い出します。		

次のページは、構成図をスケッチできるように空白にしてあります。

第 3 章

サイトの準備

この章とチェックリストを使って、設置を準備します。

- 「サイト計画チェックリスト」

サポートされている構成に暗号化ハードウェアを設置するときは、次のようないくつかのことを検討してください。

- 「ラックの仕様」
- 「Service Delivery Platform」
- 「コンテンツ管理」
  - Capacity on Demand
  - リアルタイム拡張技術
  - パーティション分割
  - データパスの計画
  - 作業の計画
- 「必要なツール」
- 「サポートされるプラットフォームと Web ブラウザ」
- 「ファームウェアバージョン」
- 「役割ベースの操作」

サイト計画チェックリスト

次のチェックリストを使って、顧客が Key Management System を受け入れる準備ができていること、および設置を開始する準備ができていることを確認してください。

表 3-1 サイト計画チェックリスト

質問	完了？	コメント：
納入と取り扱い		
重要： Oracle Key Manager とアプライアンスは「安全な」項目と見なされます。 納入および設置中は、顧客の安全に関するガイドラインに従ってください。		
納入口がありますか？ ない場合は、機器をどこに納入しますか？ 納入口がある場合、利用できる時間は？	はい ❑ いいえ ❑ _____	
納入を妨げる可能性のある道路や路地の制限はありますか？	はい ❑ いいえ ❑	
納入の取り扱いと受け入れを行うための、承認された担当者がいますか？	はい ❑ いいえ ❑	
納入場所は機器を設置するコンピュータルームに近いですか？	はい ❑ いいえ ❑	
機器を目的の階に移動するときにエレベータを利用できますか？	はい ❑ いいえ ❑	
設置サイトの近くに、機器を一時的に置くことができる場所はありますか？	はい ❑ いいえ ❑	
梱包材の廃棄またはリサイクルに関する特別な要件はありますか？ パレット、プラスチック、ボール紙は？	はい ❑ いいえ ❑	
環境計画		
サイトは温度、湿度、および冷却に関する環境要件を満たしていますか？	はい ❑ いいえ ❑	アプライアンスの仕様については、鍵管理アプライアンスを参照してください。

表 3-1 サイト計画チェックリスト (続き)

質問	完了？	コメント：
電源要件		
設置するサイトは電源要件を満たしていますか？	はい ❑ いいえ ❑	アプライアンスの仕様については、鍵管理アプライアンスを参照してください。 **KMA:** 90 - 132 VAC	180 - 264 VAC 57 - 63 Hz	47 - 53 Hz 2.3 - 4.6 アンペア 最大連続電力は 150 W です。
顧客はブレーカの場所と等級を把握していますか？	はい ❑ いいえ ❑	
顧客は冗長電源オプションを希望していますか？ 希望している場合、無停電電源構成の構築には、追加の APC 電源スイッチが必要です。	はい ❑ いいえ ❑	更新されたモデル番号とパーツ番号を確認してください。 (パーツ番号 #419951602)
電源ケーブルに配線要件や考慮事項がありますか？	はい ❑ いいえ ❑	詳細については、電源ケーブルを参照してください。
人員：		
暗号化機器を設置および保守するために、トレーニングまたは認定を受けた Oracle 担当者が現場にいますか？	はい ❑ いいえ ❑	**名前：**
接続： OKM、KMA、Ethernet スイッチ、およびテープドライブの間に信頼性のあるネットワークを確立するには、配線が非常に重要です。		
この顧客は **IPv6** 実装をサポートしていますか？	はい ❑ いいえ ❑	
顧客は**管理された**スイッチを LAN 2 および 3 に使用するつもりですか？	はい ❑ いいえ ❑	ケーブルの考慮事項は、サービスネットワークで管理されたスイッチを使用するかどうかの決定、および対応するトポロジの影響を受けます。
広域サービスネットワークが考慮されていますか？	はい ❑ いいえ ❑	WAN 経由でリモートサイトへのサービスネットワークを設計することで、追加のフェイルオーバー機能がエージェントに追加され、障害回復シナリオを強化できます。

表 3-1 サイト計画チェックリスト (続き)

質問	完了？	コメント：
顧客はサービスポートの**集約**を希望していますか (LAN 2 および LAN 3)?	はい ❑ いいえ ❑	顧客が提供する管理されたスイッチで、追加のケーブルおよび互換性のあるポート構成が必要です。
顧客はエージェント (テープドライブ) にプライベートネットワークを使用することを計画していますか？	はい ❑ いいえ ❑	テープドライブの競合を解消します。
接続 (続き)		
このサイトには **SDP** (Service Delivery Platform) が設置されますか？	はい ❑ いいえ ❑	詳細については、SDP55 ページの を参照してください。
顧客は **SNMP** を使って OKM を監視しますか？	はい ❑ いいえ ❑	SNMP v3 を推奨 SNMP v2 をサポート
LAN 1 ポートを使った **ELOM/ILOM** の監視の考慮事項がありますか？	はい ❑ いいえ ❑	詳細については、『SunFire X2100/2200 ELOM Administration Guide』または X4170 ILOM の補足ガイドを参照してください。
顧客を含めて、次のことを完了しましたか。 ■ ケーブル計画？ ■ エージェントにプライベートネットワークがありますか？ ■ 構成図？ 必要なケーブルの数と長さを決定するのに図が役立つことがあります。	 はい ❑ いいえ ❑ はい ❑ いいえ ❑ はい ❑ いいえ ❑	
必要な Ethernet ケーブルのタイプと数を決定しましたか？ 顧客が提供： ■ OKM からネットワークへ ■ 暗号化ネットワークから KMA へ (LAN 0) ■ ELOM/ILOM 監視 (LAN 1) ■ サービスネットワークからエージェントへ (LAN 2 および 3) 暗号化キットで提供される： ■ スイッチからテープドライブへ	はい ❑ いいえ ❑	**注：** ■ Ethernet ケーブルはキットと一緒に出荷されます。 ■ 長さはスイッチやデバイスの場所によって異なります。 **注：** 構成図は、必要なケーブルを洗い出すのに役立ちます。
構成		
顧客に KMA と Ethernet スイッチを収納するのに十分なラックスペースがありますか？	はい ❑ いいえ ❑	49 ページの「ラックの仕様」を参照してください。

表 3-1 サイト計画チェックリスト (続き)

質問	完了？	コメント：
顧客はどのタイプのサポート構成を希望していますか、または必要としていますか？ ❑ 既存の構成 ❑ 新しい構成	構成 ❑ SL8500 ❑ SL3000 ❑ SL500 ❑ 9310/9741e ❑ L シリーズ ❑ SL24/48 ❑ ラックマウント	暗号化対応ドライブ： T シリーズおよび LTO ドライブ T シリーズおよび LTO ドライブ LTO のみ T シリーズのみ T シリーズのみ LTO のみ T シリーズのみ
顧客は暗号化対応にアップグレードしたい既存のテープドライブを持っていますか？ これらのドライブはすでにライブラリに設置されていますか？	はい ❑ いいえ ❑ はい ❑ いいえ ❑	x オプション (コンバージョンビル) については、第 4 章「コンポーネント」を参照してください。
ドライブのタイプ？ 現在ぉよび必要なファームウェアバージョンを確認してください。	❑ T10000A ❑ T10000B ❑ T9840D ❑ HP LTO4 ❑ IBM LTO4 ❑ HP LTO5 ❑ IBM LTO5	 ドライブトレイと Dione カードが必要 ドライブトレイと Belisarius カードが必要 ドライブトレイと Belisarius カードが必要
構成 (続き)		
顧客は追加のドライブを注文する必要がありますか？ ■ テープドライブのタイプ： ■ インタフェースのタイプ？ ■ (FC) ファイバチャネル (すべてのテープドライブ) ■ (FI) FICON (T シリーズのみ) ■ (ES) ESCON (T9840D) ■ SCSI (SL500 ライブラリと LTO ドライブのみ)	はい ❑ いいえ ❑ ❑ T10000A ❑ T10000B ❑ T9840D ❑ HP LTO4 ❑ IBM LTO4 ❑ HP LTO5 ❑ IBM LTO5	テープドライブの数は？

表 3-1 サイト計画チェックリスト (続き)

質問	完了？	コメント：
追加のカートリッジは必要ですか？ ■ データカートリッジ ■ クリーニングカートリッジ ■ VolSafe カートリッジ ■ ラベル ■ タイプ： _____ ■ 数量： _____	 はい ❑ いいえ ❑ はい ❑ いいえ ❑ はい ❑ いいえ ❑ はい ❑ いいえ ❑	注： すべてのバージョンの暗号化テープドライブで、異なる一意のカートリッジが使用されます。 ■ T9840 = 9840 カートリッジ ■ T10000 = T10000 カートリッジ ■ LTO4 = LTO4 カートリッジ ■ LTO5 = LTO5 カートリッジ 標準、Sport、VolSafe、WORM など、各カートリッジタイプのすべてのバージョンがサポートされています。
顧客は、特定のハードウェア障害が発生した場合の Auto Service Request (ASR) または「フォンホーム」機能に興味がありますか？	はい ❑ いいえ ❑	詳細については、33 ページの「ASR (Auto Service Request) 機能」および『管理ガイド』を参照してください。

注：

構成：

テープドライブとメディア：

ラックの仕様

KMA は、標準の RETMA[1] 19 インチ、4 ポストラックまたはキャビネットに設置できます。注 : 2 ポストラックはサポートされていません。

さまざまなラックのスライドレールは、次の標準と互換性があります。

- 水平方向の開口部と装置の垂直距離が、ANSI/EIA 310-D-1992 または IEC 60927 の標準に準拠していること。
- 前面および背面の取り付け面の間の距離が 610 - 915 mm (24 インチ - 36 インチ)。
- キャビネットの前面カバーには 25.4 mm (1 インチ) 以上のすき間が必要です。
- キャビネットの背面カバーには、ケーブル管理を含む場合は 800 mm (31.5 インチ) 以上、ケーブル管理なしの場合は 700 mm (27.5 インチ) 以上。
- 支柱とケーブル溝の間、および前面および背面の取り付け面の間のすき間は、456 mm (18 インチ) 以上。

SL8500 ラックのガイドライン

SL8500 ライブラリには、最大で 4 つのオプションアクセサリラックを装備できます (PN XSL8500-RACK-Z)。
顧客が電源の冗長性を希望する場合は、2 つ以上のラックが必要です。

各ラックには、鍵管理アプライアンスや Ethernet スイッチなど、最大で 6 ユニットの機器 (U[2] と呼ばれる) を収納できます。各ラックには、電力を供給する 6 コネクタ分電装置 (PDU) と、追加の気流を提供する 2 つの冷却ファンがあります。表 3-2 に、ラックのガイドラインを一覧表示します。

表 3-2 SL8500 アクセサリラックのガイドライン

ガイドライン	説明
ラックの番号付け	ラックの番号は、上から下へ 1 から 4 です。 ラック 1 は一番上、ラック 4 は一番下です。
ラック取り付け	コンポーネントは垂直方向で機能できる必要があります。
サイズ制限	ラックモジュールの奥行きは 72 cm (28 インチ) です。 推奨されている安全な長さは 66 cm (26 インチ) です。
機器重量	アクセサリラック自体は、80 kg (175 ポンド) 用のスライドに取り付けられます。 推奨されている安全な重量は 64 kg (140 ポンド) です。 KMA は 10.7 kg (23.45 ポンド)、Ethernet スイッチは 1.5 kg (3.1 ポンド) です。
消費電力	ラックモジュールあたり 4 アンペア (最大) です。電源タップあたり 200 - 240VAC、50 - 60Hz です。 KMA は 185 W、Ethernet スイッチは 20 W です。

1. **RETMA** = Radio Electronics Television Manufacturers Association。
2. **U** はラックユニットを表します。1 ユニットは 4.4 cm (1.75 インチ) です。

表 3-2 SL8500 アクセサリラックのガイドライン (続き)

ガイドライン	説明
電源コード	ラック PDU に接続する電源プラグは、IEC320 C13 シュラウドオスプラグです。コード最小長は、サービスループの場合はコンポーネント + 46 cm (18 インチ) です。
熱要件	最大電力損失は、ラックモジュールあたり 880 ワット (3,000 BTU/ 時) です。
規制準拠	最小要件 : 安全に関しては UL または CSA 認定、電磁気に関しては FCC や BSMI などの機関の Class A 認定が必要です。

ネットワークに関する考慮事項

StorageTek エンジニアリング部門は、サービスネットワーク上で KMA をテープドライブに接続するために、**顧客は管理されたスイッチ**を提供することを推奨しています。管理されたスイッチはその後、StorageTek 提供の管理されていないスイッチへの接続と、広域サービスネットワーク用の顧客提供のルーターへの接続を提供します。

次の管理されたスイッチはテストされ推奨されています。

- 3COM Switch 4500G 24-Port (3CR17761-91)
- Extreme Networks Summit X150-24t スイッチ

ほかの管理されたスイッチも使用できますが、エンジニアリングは上記のスイッチに関する構成ガイダンスのみを提供しています。

次の理由により、管理されたスイッチが推奨されます。

- 優れたスイッチ診断とサービスネットワークの障害追跡による保守性の向上
- 冗長接続とスパニングツリープロトコルの使用によりサービスネットワーク上のシングルポイント障害を最小限に抑える可能性
- KMA のサービスインタフェース上のシングルポイント障害を最小限に抑えるために KMA サービスネットワークインタフェースの集約のサポート

図 3-1 は、管理されたスイッチの構成例を示しています。この例では、どちらかの KMA または管理されたスイッチに障害が発生しても、ドライブは他方の KMA との通信を行えるパスを引き続き保持できます。

KMA サービスポートの集約

物理的な Ethernet インタフェース (LAN 2 および LAN 3) を 1 つの仮想インタフェースに集約できます。これらのポートを集約することで可用性が向上します。つまり、どちらかのポートで障害が発生しても他方のポートが接続を維持できます。

Ethernet スイッチポートが正しく構成されていることを確認してください。たとえば、スイッチポートを次のようにしてください。

- デュプレックスの設定を自動ネゴシエーションするように設定します (全二重にする)。
- 速度設定を自動ネゴシエーションするように設定します。KMA ポートはギガビット速度に対応しています。

- 同一の速度を使用します。例 : どちらも 100Mbps に設定 (速度の自動ネゴシエーションがうまく機能することがある)。

集約されたサービスネットワークスイッチ構成

サービスネットワークインタフェース障害の場合に冗長性を提供するために、LAN 2 ポートを LAN 3 ポートと集約してもかまわなくなりました。ポート集約機能を使用するには、スイッチをリンク集積体用に構成する必要があります。KMA 上での Solaris ポート選択ポリシーは、アドレスに基づいています。ここでは、スイッチを構成するために必要になる可能性のあるサービスポート集約について一部を説明します。

- ポートが手動で集約される。つまり、LACP は使用しない
- ポートが全二重 (自動でも問題なく動作する可能性がある)。
- 集約グループに使用されるスイッチポートは同じ速度である必要がある。たとえば、両方のポートが 100 Mbps に設定される (自動速度ネゴシエーションが問題なく動作する可能性がある)。

注 :

- 順序または接続に依存する場合があります。KMA サービスポートを接続する前に、スイッチ上で集約グループを作成してください。
- 集約された IP アドレス (IPv4 または IPv6) が応答しない場合は、KMA を再起動してください。

管理 GUI を使用するシステムダンプには、表示集約されたポート情報が含まれます。情報は dladm コマンドを使って収集されます。

Extreme ネットワークスイッチの構成

Extreme Ethernet スイッチ上で集約されたポートを構成する

1. telnet を使ってスイッチにログインします。
2. 次の CLI コマンドを入力します。

```
show port sharing
enable sharing <b\> port\></b\> grouping <b\> portlist</b\>
algorithm address-based L3_L4
```

port には、負荷共有グループのマスターポートを指定します。

portlist には、1 つ以上のポートまたはスロットと、マスターポートにグループ化するポートを指定します。スタンドアロンスイッチ (通常はこれが提供されます) では、1 つ以上のポート番号を使用できます。1, 2, 3, 4, 5 の形式になる場合もあります。

3COM ネットワークスイッチの構成

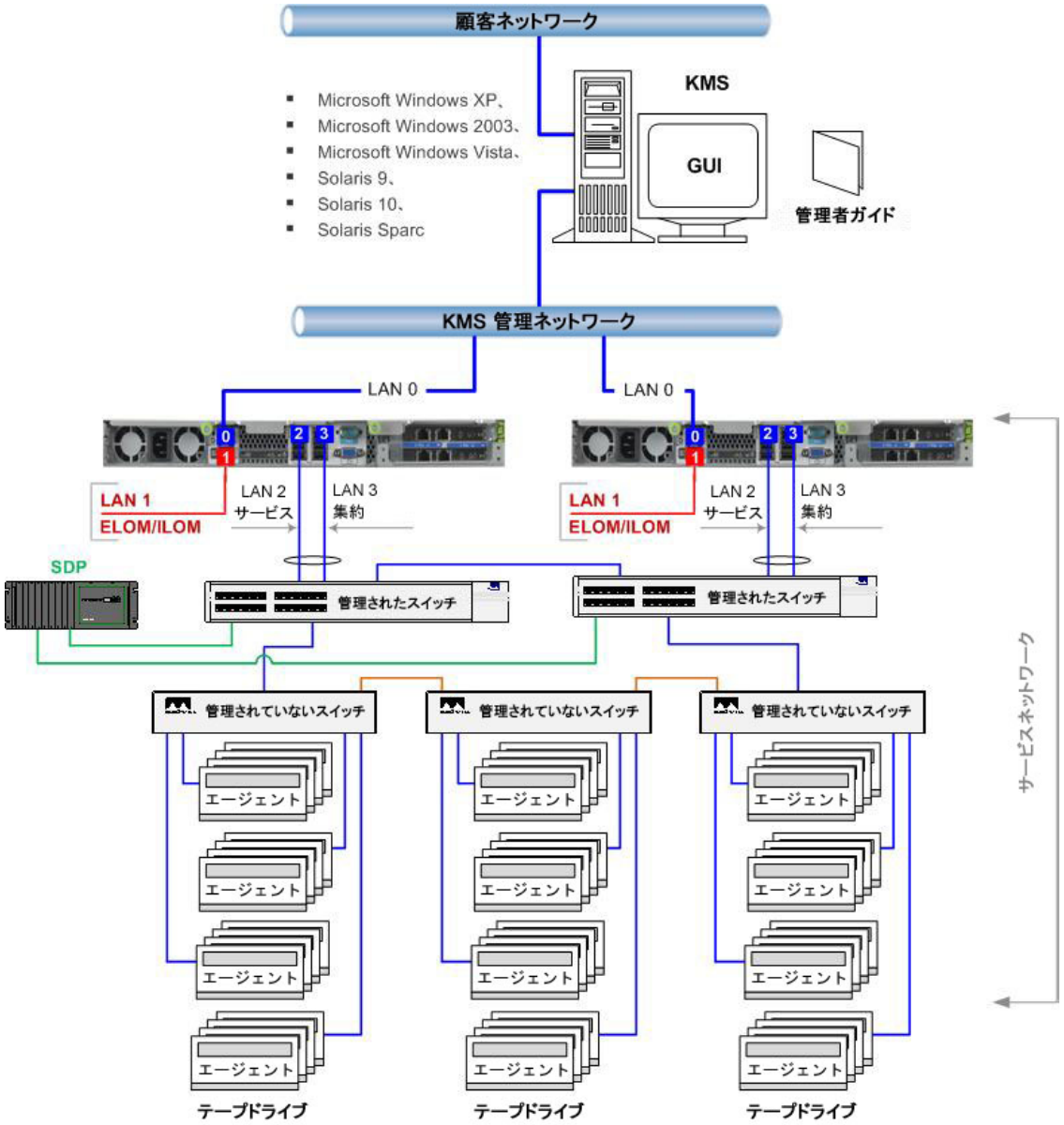
1. Web ブラウザを使ってスイッチ IP に接続します。
2. メニューから、ポート、そしてリンク集積体を選択します。

次のダイアログから、「Create」タブを使って新しいポートグループを作成できます。

図 3-1 管理されたスイッチの構成 (例)

この例では、サービスネットワークは管理されていない 3 つのスイッチに接続されている 2 つの顧客提供の管理されたスイッチで構成されます。その中には、スパニングツリー構成を必要とする冗長パスが含まれています。この例は、KMA、スイッチハードウェア、およびテープドライブを追加することで、大規模な SL8500 ドライブ構成用に簡単に拡張できます。

- 配線に冗長性があるときは必ず管理されたスイッチがスパニングツリーに対して有効になっている必要があります。
- 冗長性を確保するために、管理されていないスイッチには管理されたスイッチへのパスが 2 つあります。
- 管理されていないスイッチはその後、テープドライブ (エージェント) にケーブルで接続されます。
- 管理されていないスイッチにはそれぞれ 16 台のドライブが接続されます。4 台 1 組で接続されます。ポート 1–4、6–9、11–14、および 16–19 です。
- **SDP** (Service Delivery Platform) は、ポート 1 で各管理されたスイッチに接続されます。



ネットワークルーティングの構成

次の情報は、マルチサイトクラスタを設定および設置するときに、顧客および Oracle のサービス担当者に役立ちます。

最初は、テープドライブのために、マルチサイトネットワークトポロジで始めることは推奨されていません。シンプルな戦略が最適の場合があります。ドライブがサイト内のローカル KMA だけに制限されるように、サイト間にサービスネットワーク経路を構成しないでください。システムを信頼できるようになってから、ネットワーク用 KMA コンソールメニューオプションを使って、サービスネットワーク構成をほかのサイトに拡張できます。

注 – マルチサイトでルーティング対応サービスネットワークがなくても、デフォルトゲートウェイ設定を使用すると、フェイルオーバーの性能に影響する場合があります。次の情報を理解することは、KMA ネットワークを構成するために重要です。

クラスタ検出、負荷分散、およびフェイルオーバー

クラスタは、KMA を選択して鍵データを取得する機能をテープドライブに提供します。堅牢で可用性の高いネットワークでテープドライブの性能を最大化することが重要です。ネットワークのトポロジは、計画および構成の重要な作業です。テープドライブが鍵を取得するためにクラスタサービスをどのように利用するかに関する情報の一部を次に示します。

検出 : テープドライブ (エージェント) は、KMA の検出サービスを利用して、クラスタに関するナレッジを保守します。この情報には、各 KMA の次のプロパティーが含まれます。

- IP アドレス (IPv4 アドレスと IPv6 アドレスの両方)
- サイト名
- KMA ID
- KMA 名
- KMA バージョン – サポートされているテープドライブの FIPS サポートを判別するのに役立ちます

検出クラスタ要求が発行されると、次の動的プロパティーもテープドライブに提供されます。

- **Responding** – KMA がネットワーク上で応答しているかどうかを示します
- **Locked** – KMA が現在ロックされているかどうかを示します

テープドライブは、これらの情報をテープ操作の一部として定期的に取得し (テープドライブがアイドルでないとき)、登録の一部としては常に、そしてドライブが IPL されるたびに、これらの情報を要求します。検出クラスタ要求を受け取った KMA は、サービスネットワーク経由でアクセス可能なすべての KMA にこれらの情報を提供します。ここが、ネットワーク計画とその構成の実践が重要になってくるところです。

負荷分散 : 通常のテープドライブ運用中は、ドライブはクラスタ情報のローカルテーブルを使用して KMA を選択し、鍵を取得します。

ドライブは、アルゴリズムを使って、次の場所の KMA クラスタからランダムに KMA を選択します。

- ドライブと同じサイト
- ロック解除されていて、応答する

サイト内のすべての KMA がロックされているか、応答しない場合は、テープドライブは別のサイトから KMA にアクセスしようとします。

これはおそらく、テープドライブとおなじサイト内のほかの KMA よりネットワーク応答時間が長い可能性があるリモートサイトです。

重要なことは、テープドライブがほかのサイトの KMA に到達できることです。そうでないと、鍵を取得しようとしてもタイムアウトになり、強制的にフェイルオーバーになります。

フェイルオーバー : テープドライブが KMA と通信しようとして失敗すると常に、ドライブは別の KMA を選択してフェイルオーバーを試みます。テープドライブは、3 回までフェイルオーバーを試みてから中止し、ホストテープアプリケーションにエラーを返します。

すべてのフェイルオーバーの試みで、負荷分散に似た選択アルゴリズムが使用されます。その結果、クラスタ状態に関するドライブの情報が再利用されます (さらに、クラスタに関する情報を更新するタイミングになると更新されることもあります)。

ほかのすべての KMA が応答しない場合は、ドライブがフェイルオーバー試行中に応答しない KMA を選択することがあります。これは望ましくありません。クラスタに関する情報が古い可能性があり、KMA がオンラインに戻って応答する可能性があるためです。ドライブは、KMA の新しい応答状態を検出すると常に、クラスタ情報を更新して、状況に関係なく KMA を応答中または応答なしとマークします。

KMA のルーティング構成と検出

KMA のルーティング構成は、テープドライブ検出要求への応答に影響します。ルーティング構成を誤ると、間違ったクラスタ情報がテープドライブに提供される可能性があります。その場合、ドライブはネットワーク経由で到達できない KMA と通信しようとすることがあります。

顧客は、テープドライブに必要なネットワークトポロジを考慮する必要があります。ローカル KMA が停止したり応答が遅くなったりした場合 (作業負荷が大きいためのタイムアウト状況など)、テープドライブをリモートサイトにフェイルオーバーできることで、ドライブの信頼性と可用性を向上させることができます。

注 : リモートサイトにフェイルオーバーできる機能を提供するには、そのための計画が必要なことなので、顧客のネットワークエンジニアに参加してもらうことをお勧めします。

サービスネットワーク上のドライブの場合、サイト間で経路を構成する必要があり、KMA コンソールネットワークメニューオプションを使用するとよいでしょう。避けるべきよくある間違いは、デフォルト経路を構成することです。

図 3-1 に、マルチサイトルーティングされたサービスネットワークの例を示します。

Service Delivery Platform

SDP (Service Delivery Platform) は、スマートアプライアンスと専用ネットワークで構成される StorageTek ライブラリとテープドライブ (T シリーズのみ) のためのサポートソリューションです。

SDP アプライアンスは、DHCP (Dynamic Host Configuration Protocol) を使用してデバイス接続への IP アドレス割り当てを自動化するように構成できます。オプションで、SDP を KMA サービスネットワーク IP アドレスのための DHCP サーバーとして使用することもできます。

Oracle Key Manager と SDP

SDP と Oracle Key Manager を新しく配備するようになってから、セキュリティーを強化するように構成が変更されました。SDP 製品チームは、KMA から顧客のネットワークへの接続のために、サービスネットワーク上の KMA、スイッチ、およびテープドライブの間にファイアウォールを設置することを推奨しています。2008 年 5 月の「Service Delivery Platform Security White Paper」および「Optional Firewall」を参照してください。

マルチサイトサービスネットワークを計画するときは、KMA サービスのポートとドライブのためのサブネットアドレス指定スキームを決定する必要があります。重複するネットワークアドレスの使用は避ける必要があります。たとえば、172.18.18.x ネットワーク (一般的な表記規則) の使用は避ける必要があります。

KMA は通常、次のいずれかの理由で顧客のネットワークに接続されます。

- 顧客ネットワークでホストされる Oracle Key Manager GUI を使った KMA への管理アクセス
- KMA 間のクラスタ複製
- 顧客の NTP サーバーへの KMA アクセス
- 顧客の SNMP マネージャーへの KMA アクセス
- KMA のサービスプロセッサへの顧客アクセス (ELOM または ILOM)

同様に、Oracle Key Manager がルーティング可能なマルチサイトサービスネットワークをサポートしているため、鍵管理クラスタを構成するさまざまなサイトを接続するには顧客提供のルーターとネットワーク機器が必要です。

顧客のネットワークへのこの接続のために、SDP セキュリティーポリシーには、KMA および SDP に接続するデバイス間にファイアウォールを設置する必要があることが規定されています。この「顧客ファイアウォール」は、後続の図では SDP アプライアンスのポート 2 に接続されているファイアウォールです。ファイアウォールは、サービスネットワークの顧客制御部分のテープドライブを SDP が監視できるように構成する必要があります。

図の DMZ は、SDP 開始ユニットと Oracle ネットワークの間のネットワークトラフィックを保護する、SDP のセキュアネットワークアーキテクチャーです。

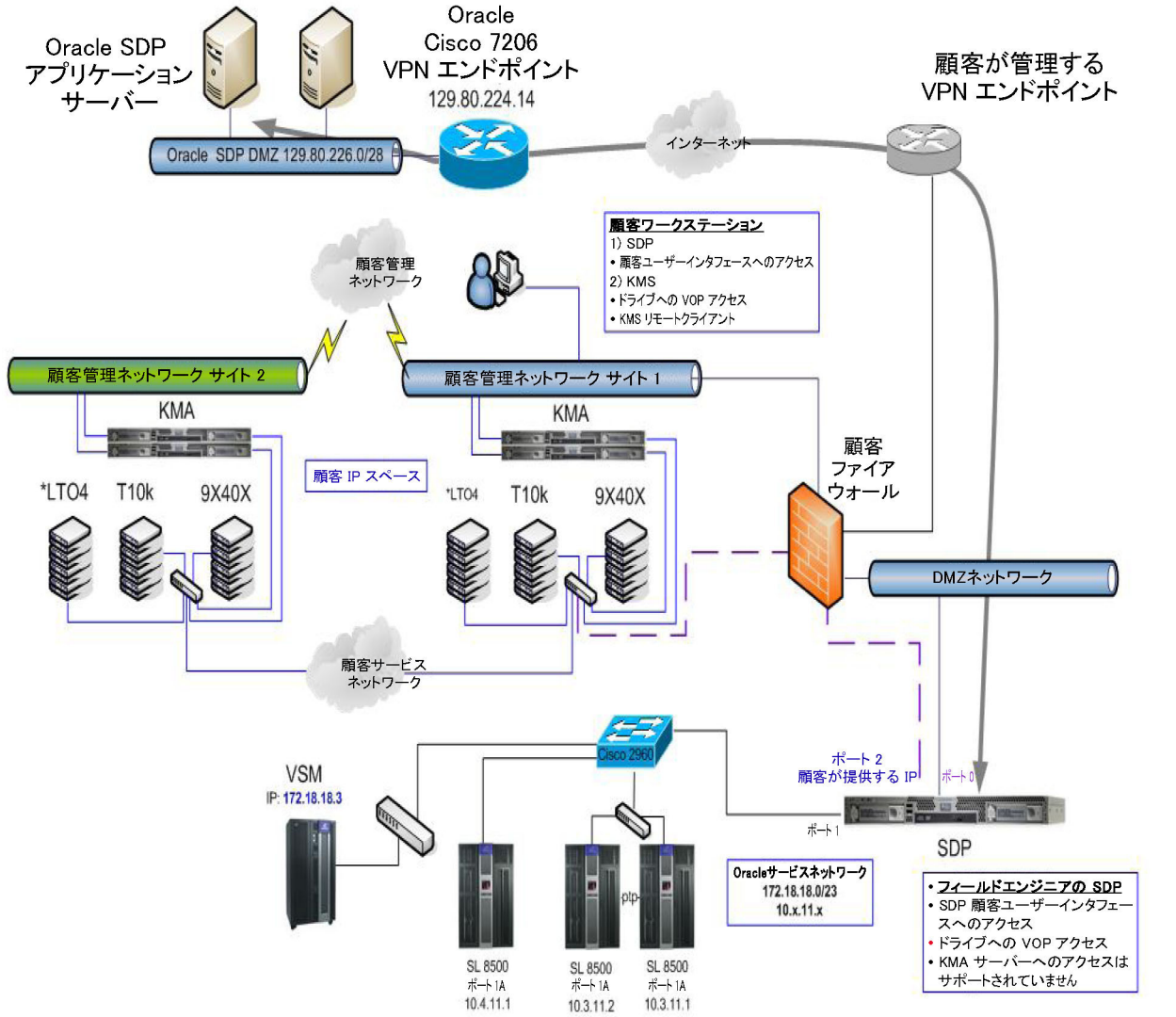
このファイアウォールによって、サービスネットワークが事実上 2 つに分割されます。Oracle が制御するサービスネットワークと、顧客が制御するサービスネットワークです。2008 年 5 月の「Service Delivery Platform Security White Paper」では、このネットワークを「サービスネットワークインタフェース」と説明しています。Oracle サービ

スネットワークインタフェースは、SDP サイトユニットとストレージデバイスとの間の接続です。これは、図ではポート 1 接続です。顧客ネットワークインタフェースは、SDP と Oracle ストレージデバイスの間の接続です。後者は顧客オペレーションセンター LAN に接続され、さらに顧客ネットワークに接続されています。図ではポート 2 です。これらのデバイスには、KMA に接続されたテープドライブとスイッチが含まれます。

「顧客ファイアウォール」は、この接続から顧客のネットワークにアクセスできないようにし、SDP が監視できるデバイスにのみアクセスできるようにします。

Oracle サービス担当者は今までどおり、サービスネットワークの両方の部分で機器サービスを提供し、SDP エンジニアと協調して計画や構成を行う必要があります。

図 3-2 SDP 接続の例



コンテンツ管理

暗号化対応テープドライブは、設置された SL8500、SL3000、および SL500 ライブラリ内のコンテンツ管理の設計に別の要素を加えます。3 つのライブラリは、同様の要素を共有していますが、それぞれ設計が異なります。考慮事項を次に示します。

表 3-3 コンテンツ管理計画

要素	SL8500	SL3000	SL500
ドライブの数量	ライブラリ内のすべての暗号化対応テープドライブをサポートするには、場合によっては複数のキットまたは追加の Ethernet スイッチを注文する必要があります。		
	■ シングル : **1 - 64** 個のドライブ ■ 10 ライブラリコンプレックス : 最大で 640 個のドライブ	■ **1 - 56** 個のテープドライブ	■ **1 - 18** 個のテープドライブ
サポートされる暗号化ドライブ	■ T10000 A および B ■ T9840D ■ LTO 4 および 5	■ T10000 A および B ■ T9840D ■ LTO 4 および 5	■ LTO 4 および 5 のみ (HP、IBM)
サポートされる暗号化非対応ドライブ	■ T10000 A および B ■ T9840 A、B、および C ■ LTO 3、4、5	■ T10000 A および B ■ T9840C ■ LTO 3、4、5	■ LTO 2、3、4、5 (HP、IBM) ■ SDLT 600 ■ DLT-S4
インタフェース : ■ ライブラリ	注 : ライブラリインタフェースとテープドライブインタフェースは異なることがあります。 ■ TCP/IP のみ	■ TCP/IP ■ ファイバチャネル	■ TCP/IP ■ ファイバチャネル
■ テープドライブ	T10000 A および B FC と FICON T9840D FC、FICON、ESCON LTO 4 および 5 FC のみ	T10000 A および B FC と FICON T9840D FC、FICON、ESCON LTO 4 および 5 FC のみ	LTO4、5 ファイバチャネル LTO4 SCSI (入手可能かどうかを確認)
メディア *	すべてのライブラリが真の混在メディアをサポート - Any Cartridge, Any Slot™		
	■ T10000 (標準、Sport、VolSafe) ■ 9840 (標準および VolSafe) ■ LTO 2、3、4、5 および T-WORM ■ DLTtape III ■ Super DLTtape I および II	■ T10000 (標準、Sport、VolSafe) ■ 9840 (標準および VolSafe) ■ LTO 2、3、4、5 および T-WORM	■ LTO 1、2、3、4、5 および T-WORM ■ DLTtape III ■ Super DLTtape I & II
パーティション分割	はい	はい	はい
SNMP	はい	はい	はい

表 3-3 コンテンツ管理計画 (続き)

SDP	はい	はい	なし
電源冗長性	はい	はい	なし
オペレーティングシステム	エンタープライズおよびオープンシステム	エンタープライズおよびオープンシステム	オープンシステムのみ
ライブラリ管理	■ ACSLS ■ HSC	■ ACSLS ■ HSC ■ ISV	■ ACSLS ■ ISV
FC = ファイバチャネル FICON = IBM ファイバ接続 SNMP = Simple Network Management Protocol SDP = Service Delivery Platform		ACSLS = Automated Cartridge System Library Software HSC = Host Software Component ISV = Independent Software Vendor (Symantec、Legato、TSM)	
*** 重要 : LTO4 メディア (LTO4 および LTO4-WORM)** のみが LTO4 テープドライブで暗号化に対応しています。			

コンテンツを計画するときに最も重要な側面は、ライブラリの物理構造の観点からコンテンツ (テープドライブとデータカートリッジ) を評価することです。

これらのライブラリは、増大するデータストレージ要件に対応するためにいくつかの方法を提供しています。

- ライブラリモジュールの追加 - 前面、左または右、上および下
- Capacity on Demand
  - サービス担当者の関与なしでスロットのアクティブ化
  - 事前にスロットまたはモジュールを設置する必要がある
- 柔軟性のあるパーティション
- 要件の変化に合わせてリソースを再割り当てしやすい
- リアルタイムの拡張
- 障害回復シナリオ

Capacity on Demand

Capacity on Demand は、顧客が設置済みだけれどもまだ非アクティブなスロットを使ってライブラリに容量を追加できる、非中断のオプション機能です。

設置済み物理容量は、アクティブ化された容量からは切り離されています。Capacity on Demand の利点は、顧客は必要なストレージだけを購入し、設置されているすべてのストレージを購入する必要がないことです。

アクティブ化する容量は、複数回にわたって分割購入できます。

顧客が追加物理ストレージを使用するためのハードウェアアクティベーション鍵を購入すると、暗号化された鍵ファイルが電子メールで送信されます。その後このファイルは、SLC (Storage Library Console) を使ってライブラリにロードされます。

リアルタイム拡張技術

物理スロット容量とアクティブ化されたスロット容量は切り離されているため、顧客は、それらのスロットが使用できる状態になる前に、事前に物理容量を設置することもできます。

事前に物理容量を設置する利点は、ライブラリの拡張が中断なく、すばやく、簡単に行えることです。

例 : ライブラリ構成を構築するときは常に、2 つの基本的なスロット容量の質問に答える必要があります。

1. 顧客はいくつのスロットを使用する必要がありますか。
2. 顧客はいくつのカートリッジスロットを物理的に設置することを希望していますか。

パーティション分割

パーティション分割の定義は、部分に分割することです。

利点 : ライブラリをパーティションに分割することは、顧客が次の利点を持てることを意味します。

- ハードウェアの 1 つの物理的な部分から複数のライブラリ。
- 1 つ以上のオペレーティングシステムやアプリケーションがライブラリを管理。
- ファイルの保護または分離を改善。
- システムおよびライブラリのパフォーマンスの向上。
- ユーザー効率の向上。

カスタマイズで合わせる :
パーティションは、さまざまな要件に合わせてカスタマイズできます。次に例を示します。

- さまざまな暗号化鍵グループに分ける。
- クライアントをサービスセンターとして分離する。
- 特定のタスクにパーティションを割り当てる。
- 複数の部門、組織、および会社に適切なサイズのライブラリリソースへのアクセス権を付与する。

ヒント :
暗号化対応テープドライブを使用するときは、パーティションによってデータセキュリティーに追加層を加えることができます。顧客は、アクセスを制限するパーティションをテープドライブやデータカートリッジに割り当てることができます。

今後のことを考慮してパーティションを設定することをお勧めします。拡張の余地を残しておくことで、顧客は Capacity on Demand を使ってパーティション内のスロットをアクティブ化できます。これは、最も簡単で中断の少ない拡張方法です。

1. 余分の物理容量を設置します。
2. 今後の拡張に対応するために十分な大きさのパーティションを定義します。
3. 現在の需要を満たすためにライブラリ容量を調整します。

パーティションを理解するための基本的なガイドラインを次に示します。

- システムプログラマ、ネットワーク管理者、ライブラリソフトウェアの担当者と管理者、およびサービス担当者の間で十分なコミュニケーションを図ってください。

- どんなパーティションが存在しているか、それらの境界、および構成されている特定のパーティションにだれがアクセスできるかを把握してください。
- パーティションの設定には、いくつかの重要な点を考慮する必要があります。
  - スロットとテープドライブは特定のパーティションに割り当てられるので、ほかのパーティションをまたがって共有することはできません。
  - パーティションユーザーは、常駐データカートリッジにどのくらいのストレージが必要か、そして現在使用するためおよび今後の拡張のためにどのくらいの空きスロットが必要かを予想する必要があります。
- 次のことを覚えておいてください。
  - 各パーティションは独立したライブラリとして動作します。
  - あるパーティションは、ライブラリ内の別のパーティションを認識しません。

障害回復

障害回復は、**業務継続計画** (BCP、Business Continuity Planning) と呼ばれる上位プロセスのサブセットで、ハードウェアの交換、ネットワークの再確立、アプリケーションの再開、およびデータの復元が含まれます。

障害回復とは、自然災害または人災のあとに組織の業務にとって重要な情報を回復または継続するための準備に関連する、プロセス、ポリシー、および手順です。これには、次のものが含まれます。

- **回復時点目標** (RPO、Recovery Point Objective): 業務継続計画の定義に従ってデータを回復させる時点。これは一般に、その業務で決定することを障害時に「どこまで喪失することが許されるか」を定義することです。これは、時、日、または週単位で指定できます。
- **回復時間目標** (RTO、Recovery Time Objective): 業務継続の中断に関連する許容できない結果を回避するために、障害 (または中断) のあとに業務プロセスを「復元」する必要のある期間。結合されたサービスネットワークを使用しているときは、これは分単位になる可能性があります。

OKM が使用するクラスタ設計には、2 つ以上の鍵管理アプライアンスが必要です。この設計は、業務継続が中断されるリスクを小さくするのに役立ちます。KMA のクラスタ化により、データベースエントリの複製と作業負荷の分散が可能になります。コンポーネントに突然障害が発生した場合も、簡単に交換して運用を回復できます。

OKM は、地理的に分離された複数のサイトにまたがることができます。これにより、クラスタ全体が破壊される障害のリスクが大幅に小さくなります。KMA のクラスタ化により、データベースエントリの複製と作業負荷の分散が可能になります。万一、クラスタ全体を再作成する必要がある場合でも、最近のデータベースバックアップから OKM 2.x 環境を再作成することで、ほとんどの鍵データを回復できます

暗号化およびアーカイブ戦略を設計するときの重要な設計ガイドラインは、どこかのサイトで生成された重要データは、別のサイトに複製して保管することです。多くの会社は、サードパーティの障害回復 (DR) サイトのサービスを採用することで、できるだけ早く業務を再開できるようにしています。

詳細については、『Disaster Recovery Reference Guide PN 31619710x』を参照してください。

データパスの計画

パーティションを計画するときは、テープドライブとメディアの場所、数量、タイプ、要件も意識する必要があります。

また、テープドライブを論理的にどのような方法でグループ化して設置し、どのような方法で異なるホストのメディアを検出し、データセット、インタフェースタイプ、およびパーティションをどのような方法で制御するかを理解する必要があります。パーティションを計画するときは、次のことを考慮してください。

- テープドライブインタフェースがそのオペレーティングシステムをサポートしていることを確認します。
  - オープンシステムプラットフォームは、ESCON または FICON インタフェースをサポートしていません。
  - すべてのメインフレームがファイバチャネルインタフェースまたは LTO テープドライブをサポートしているわけではありません。
- メディアタイプがアプリケーションと一致していることを確認します。
- 同じパーティションでは、同じメディアタイプを使用するテープドライブを設置してください。
- アプリケーションと作業負荷をサポートするのに十分なスクラッチカートリッジと空きスロットがあることを確認します。

作業の計画

コンテンツ管理とパーティション分割にとって重要なメッセージは、**計画**です。
計画する項目を次に示します。

表 3-4　パーティション分割の手順と作業

✓	項目	作業	責任者 *
❑	**1. チーム**	チームを作成します。 コンテンツ、データ、およびパーティションを計画するときは、システムアシュアランスプロセスに似たプロセスを使用します。つまり、実装のすべての側面が注意深く計画され、効率的に実行されるように、チームメンバー間で情報を交換します。チームメンバーには、顧客の担当者を含めてください。	■ 顧客 ■ 管理者 ■ オペレータ ■ SE、PS ■ サービス担当者
❑	**2. コード**	ソフトウェアとファームウェアの要件を確認します。必要に応じて更新します。	■ 顧客 ■ SE、PS ■ サービス担当者
❑	**3. 計画**	■ 顧客の期待を定義します ■ 評価を完了します ■ 構成を特定します ■ 計画図を完了します (ネットワーク計画を含む) ■ SDP (Service Delivery Platform)	■ 顧客 ■ 管理者 ■ SE、PS ■ サービス担当者
❑	**4. 暗号化**	■ 暗号化アンケートを完了します (PS) ■ テープドライブ、インタフェース、およびライブラリ構成のタイプを選択します ■ 場所を選択します ■ 適切なメディアがあることを確認します	■ 顧客 ■ SE、PS ■ サービス担当者

表 3-4 パーティション分割の手順と作業 (続き)

✓	項目	作業	責任者 *
❑	**5. 障害回復**	■ 業務継続と障害回復の計画を立案します ■ バックアップサイトを選択します ■ ネットワーク構成を決定します (LAN、WAN、集約)	■ 顧客 ■ SE、PS ■ サービス担当者
❑	**6. メディア**	■ カートリッジと必要なテープドライブが利用可能で準備できていることを確認します。	■ 顧客 ■ オペレータ
❑	**7. ライブラリ**	■ ライブラリを設置して構成します (必要に応じて)。	■ サービス担当者
❑	**8. アクティブ化**	■ 必要な機能をアクティブにします。 ■ ライブラリ ■ テープドライブ	■ 顧客 ■ 管理者 ■ サービス担当者
❑	**9. パーティション**	■ パーティションを作成します。	■ 顧客 ■ 管理者 ■ オペレータ
❑	**10. ホスト**	■ ホストが現在接続されている場合は、すべてのホストの動作を一時的に停止します。	■ 顧客
❑	**11. 使用**	顧客に次の方法を伝えます。 ■ ライブラリを使用および管理する方法 ■ OKM GUI を使用する方法	■ 顧客 ■ SE、PS ■ サービス担当者
❑	**12. 参照資料**	顧客が適切なマニュアルを利用できるようにします。	■ 顧客 ■ SE、PS ■ サービス担当者

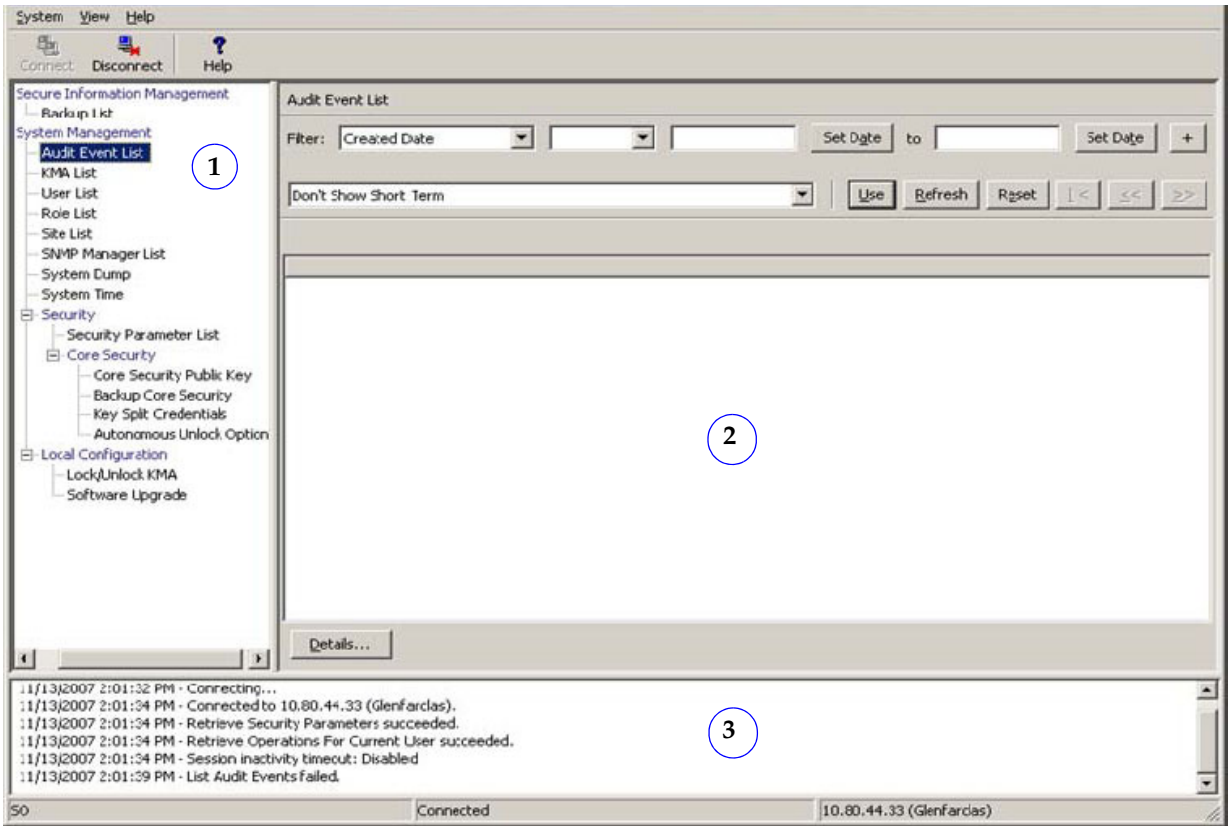
■ SE = システムエンジニア
■ PS = プロフェッショナルサービス担当者
■ サービス = 顧客サービス担当者 (サービス担当者)
■ 顧客 = システム管理者、ネットワーク管理者、システムプログラマ、オペレータ

Oracle Key Manager インタフェース

Manager グラフィカルユーザーインタフェース (GUI) は、3 つのパネル表示で構成されています。

1. 左側は、ナビゲーションパネルまたはツリーです。
2. 中央は、左側で選択したものに対応する、操作詳細パネルです。
3. 下部は、セッションイベントパネルです。

表 3-5 Manager 表示



Manager は使いやすいグラフィカルユーザーインタフェースで、ユーザーは割り当てられた役割に応じて KMA の機能を構成できます (64 ページの「役割ベースの操作」を参照)。

Manager 画面の左上隅には、「System」、「View」、および「Help」メニューが含まれます。ツールバーボタンは、いくつかのメニューオプションへのショートカットを提供します。

役割ベースの操作

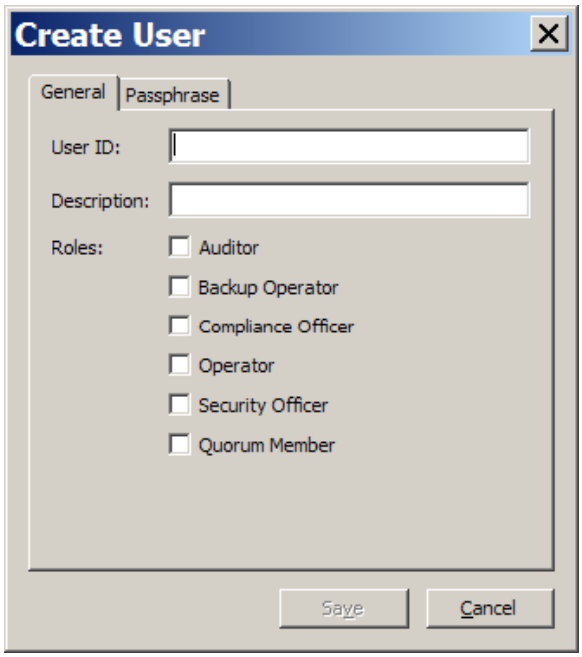
Manager では、次の役割を定義して使用します。役割を完了して割り当てるのは顧客の作業で、サービス担当者は助言のみにするべきです。

■ **監査者**	クラスタに関する情報を表示します。
■ **バックアップオペレータ**	バックアップを実行します。
■ **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ます。鍵グループを使用できるエージェントと転送パートナーを決定します。
■ **オペレータ**	エージェント、データユニット、および鍵を管理します。
■ **定足数メンバー**	保留中の定足数操作を表示および承認します。
■ **セキュリティー責任者**	サイト、KMA、ユーザー、および転送パートナーを表示、変更、作成、および削除するための完全な権限。

注 : それぞれの人またはユーザーは、これらの役割の 1 つ以上を実行してもかまいません。

図 3-3 は、「Users Detail」画面の例を示しています。
70 ページの 表 3-7 を使うと、割り当ての準備に役立ちます。

図 3-3 ユーザー役割の詳細画面



1. 1 - 64 文字のユーザー ID を入力します
2. 1 - 64 文字の説明 を入力します
3. 「Passphrase」タブをクリックして、パスフレーズを 2 回入力します

   パスフレーズには次を使用する必要があります。
   - 8 - 64 個の文字
   - 4 種類の 3 つ (大文字、小文字、数字、および記号)
   - ユーザー名は含めないでください

KMA は、ユーザー役割に基づいて、要求するユーザーが操作を実行する権限を持っているかを確認します。利用できない操作は通常、役割が間違っていることを示します。

ユーザーまたは役割が持つことができる 4 つの基本操作があります。作成、削除、変更、および表示です。65 ページの 表 3-6 は、それぞれのユーザー役割が実行できるシステムエンティティと機能を示しています。「役割」列の意味です。

- **はい**。その役割は、その操作を実行することが許可されていることを示します。

- **定足数**。その役割は許可されていますが、定足数に属している必要があることを示します。
- **空白**。その役割は、その操作を実行することが許可されていないことを示します。

表 3-6　システム操作とユーザー役割 (シート 1 / 5)

操作	役割					
	セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー
コンソール						
ログイン	はい	はい	はい	はい	はい	はい
KMA ロケールの設定	はい					
KMA IP アドレスの設定	はい					
技術サポートの有効化	はい					
技術サポートの無効化	はい		はい			
主管理者の有効化	はい					
主管理者の無効化	はい		はい			
KMA の再起動			はい			
KMA の停止			はい			
クラスタへのログイン	定足数					
ユーザーのパスフレーズの設定	はい					
KMA のリセット	はい					
KMA のゼロ化	はい					
ログアウト	はい	はい	はい	はい	はい	はい
接続						
ログイン	はい	はい	はい	はい	はい	はい
プロファイルの作成	はい	はい	はい	はい	はい	はい
プロファイルの削除	はい	はい	はい	はい	はい	はい
構成設定の設定	はい	はい	はい	はい	はい	はい
切断	はい	はい	はい	はい	はい	はい
鍵分割資格						
一覧表示	はい					
変更	定足数					
自律ロック解除						
一覧表示	はい					
変更	定足数					

表 3-6 システム操作とユーザー役割 (シート ２ / ５)

操作	役割					
	セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー
KMA のロック / ロック解除						
状態の一覧表示	はい	はい	はい	はい	はい	
ロック	はい					
ロック解除	定足数					
サイト						
作成	はい					
一覧表示	はい		はい			
変更	はい					
削除	はい					
セキュリティーパラメータ						
一覧表示	はい	はい	はい	はい	はい	
変更	はい					
KMA						
作成	はい					
一覧表示	はい		はい			
変更	はい					
削除	はい					
ユーザー						
作成	はい					
一覧表示	はい					
変更	はい					
パスフレーズの変更	はい					
削除	はい					
役割						
一覧表示	はい					
鍵ポリシー						
作成		はい				
一覧表示		はい				
変更		はい				
削除		はい				

表 3-6　システム操作とユーザー役割 (シート ３ / ５)

操作	役割					
	セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー
鍵グループ						
作成		はい				
一覧表示		はい	はい			
データユニットの一覧表示		はい	はい			
エージェントの一覧表示		はい	はい			
変更		はい				
削除		はい				
エージェント						
作成			はい			
一覧表示		はい	はい			
変更			はい			
パスフレーズの変更			はい			
削除			はい			
エージェント / 鍵グループの割り当て						
一覧表示		はい	はい			
変更		はい				
データユニット						
作成						
一覧表示		はい	はい			
変更			はい			
鍵グループの変更		はい				
削除						
鍵						
データユニット鍵の一覧表示		はい	はい			
破棄			はい			
危殆化		はい				
転送パートナー						
構成	定足数					
一覧表示	はい	はい	はい			

表 3-6 システム操作とユーザー役割 (シート 4 / 5)

操作	役割					
	セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー
変更	定足数					
削除	はい					
鍵転送鍵						
一覧表示	はい					
更新	はい					
転送パートナー鍵グループの割り当て						
一覧表示		はい	はい			
変更		はい				
バックアップ						
作成				はい		
一覧表示	はい	はい	はい	はい		
バックアップと破棄された鍵の一覧表示		はい	はい			
復元	定足数					
破棄の確認				はい		
コアセキュリティーバックアップ						
作成	はい					
SNMP マネージャー						
作成	はい					
一覧表示	はい		はい			
変更	はい					
削除	はい					
イベントの監査						
表示	はい	はい	はい	はい	はい	
エージェント履歴の表示		はい	はい			
データユニット履歴の表示		はい	はい			
データユニット鍵履歴の表示		はい	はい			
システムダンプ						
作成	はい		はい			

表 3-6 システム操作とユーザー役割 (シート ５ / ５)

操作	役割					
	セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー
システム時刻						
一覧表示	はい	はい	はい	はい	はい	
変更	はい					
NTP サーバー						
一覧表示	はい	はい	はい	はい	はい	
変更	はい					
ソフトウェアバージョン						
一覧表示	はい	はい	はい	はい	はい	
アップグレード			はい			
ネットワーク構成						
表示	はい	はい	はい	はい	はい	
保留中の定足数操作						
承認						定足数
削除	はい					

表 3-7 ユーザー役割ワークシート

ユーザー ID	説明	パスフレーズ ** (秘密のパスワード)	役割			
			セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ

注 : 安全上の理由で、パスフレーズはここには記録しないでください。
この欄は、ユーザー ID が入力されると、その ID を持つ人がパスフレーズの入力を求められることのリマインダーとし

テープドライブの準備

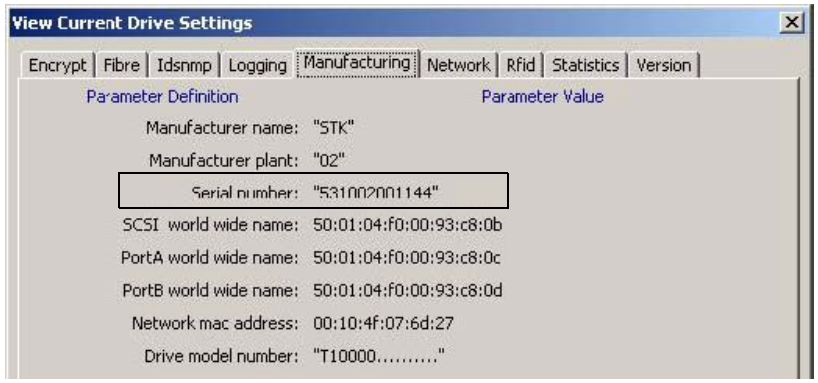
テープドライブは、暗号化機能を追加する前に、適切な構成で設置してテストすることをお勧めします。ドライブタイプごとに独自の要件があります。

T シリーズドライブデータの準備

各 T シリーズ (T10000 および T9840) テープドライブのドライブデータを取得する

1. Virtual Operator Panel を使って、それぞれのテープドライブに接続し、テープドライブシリアル番号の最後の 8 桁を記録します。
   - 選択：「File」➪「Connect to Drive」
   - 選択：「Retrieve」➪「View Drive Data」➪「Manufacturing」

図 3-4 テープドライブのシリアル番号 - VOP



➪

2. ワークシート を使って、テープドライブに関する情報を構築します。テープドライブ (エージェント) の設置、アクティブ化、および登録プロセス中に、この情報が役立つことがわかります。
3. 暗号化鍵ファイルを要求します。
   a. 申請 Web サイト (http://crcapplications/keyswebapp/) にログインします
   b.「Request an Encryption key」を選択します

図 3-5 暗号化鍵の申請を要求

アクセスが制限される：従業員であり、暗号化トレーニングコースを完了し、「Request Encryption Key」リストに従業員の名前を含める必要があります。

4.「Encryption Request」フォームを完成します。

a. 名、姓、および電子メールアドレスは自動的に取り込まれます。

b. サイト ID と注文番号を提供します。

c. テープドライブタイプを選択します (T10000A、T10000B、または T9840D)。

d. 選択したテープドライブシリアル番号を完成します。

e. オプションの備考を追加し、「Request Key File」をクリックします。
暗号化ファイル要求を送信したあとで、ファイルのダウンロードを求められます。このファイルには、ドライブを有効にして登録するために必要なドライブデータが含まれています。

図 3-6 ドライブデータのための暗号化ファイル要求

ファミリシリアル番号は次のように始まります。
T10000A = 5310 xxxxxxxx
T10000B = 5720 xxxxxxxx
T9840D = 5700 xxxxxxxx

ドライブファミリタイプを選択すると、シリアル番号の最初の 4 つの数字が自動的に入力されます。

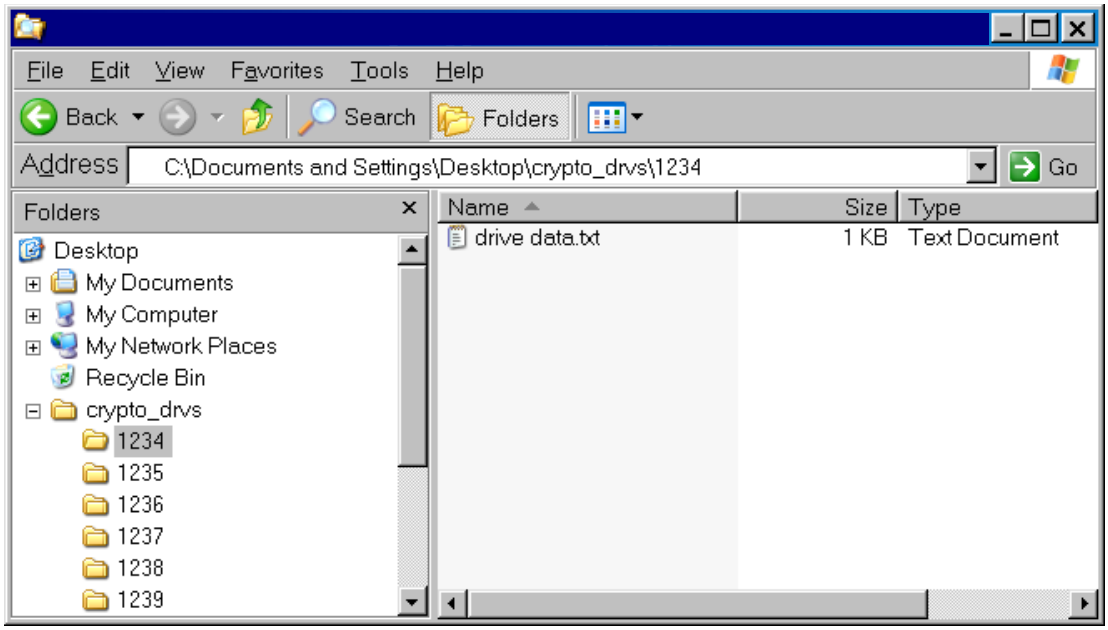
5. 有効にする各テープドライブのドライブデータファイルをすべて取得するまで、このプロセスを続けます。

ドライブデータファイル構造の作成

複数のドライブを有効にするときは、各テープドライブが独自のフォルダを持つファイル構造を作成することをお勧めします。次に例を示します。

1. 図 3-7 では、デスクトップに置かれた **crypto_drvs** という最上位フォルダ名を使用しています。(これは、その他のフォルダをグループ化することだけが目的です。)
2. crypto_drvs の下に、シリアル番号を使用する、テープドライブごとのフォルダがあります。
3. 各シリアル番号フォルダ内には、その特定のテープドライブのドライブデータファイルがあります。

図 3-7 ドライブデータファイル構造



テープドライブをアクティブ化するときに、VOP からダウンロード先を要求されます。

4. テープドライブのアクティブ化と登録に役立つ、ワークシート を完成します。始める前に知っておく必要のあることを次に示します。
   - ドライブ番号 (シリアルまたはシステム) と IP アドレスは何ですか。
   - エージェント ID とパスフレーズは何ですか。
   - このドライブは**トークン** (バージョン 1.x) を使用して媒体鍵 (OKT) を取得しますか。または、**アプリケーション** (KMA バージョン 2.x) を使用して暗号化鍵を取得しますか。
   - 顧客はこのドライブを暗号化モードのままにすることを希望していますか。または、暗号化のオンとオフを切り替えられることを希望していますか ?
5. 必要に応じて、このページのコピーを作成します。

注 :

- エージェント名 (ID) は変更できません。ただし、エージェントを削除して、別の名前で再登録できます。

- エージェントを交換する場合、名前は再利用できますが、パスフレーズは 1 回のみ使用できます。エージェントに新しいパスフレーズを付与する必要があります。
- つまり、既存の名前と新しいパスフレーズを使って、交換ドライブを登録する必要があります。

LTO テープドライブの準備

LTO テープドライブの場合は、有効化の要件またはドライブデータは必要ありません。唯一の準備は、顧客が OKM マネージャーでテープドライブの IP アドレスとエージェント名を割り当てるための情報を持っていることを確認することです。

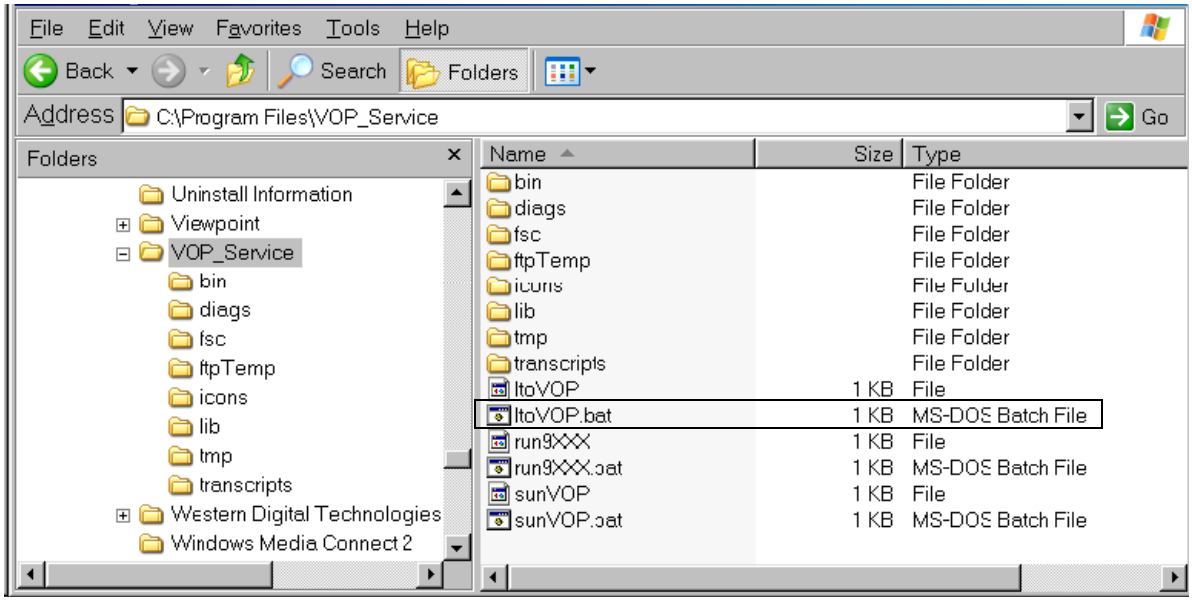
注 – Virtual Operator Panel は、次のバージョンである必要があります。
- HP LTO テープドライブのサポートを提供する場合は、バージョン 1.0.12 以降。
- IBM LTO テープドライブのサポートを提供する場合は、バージョン 1.0.14 以降。

LTO テープドライブ用の VOP を使用するには、特別なファイルを起動する必要があります。

- **Windows:** バッチファイル (**ltoVOP.bat**) を起動します

図 3-8 に、VOP 1.0.12 ダウンロードコンテンツの例を示します。

図 3-8 VOP LTO ファイル



必要なツール

KMA を設置して初期構成するために必要なツールを次に示します。

- 標準的な現場サービスツールキット。マイナスとプラスの両方のドライバ、トルクスドライバとビット、サーバーをラックに搭載するために必要なその他のツールを含む
- シリアルまたはヌルモデムケーブル (P/N 24100134)、DB-9 コネクタ付き
- アダプタ (P/N 10402019)
- Ethernet ストレートケーブル (P/N 24100216) 3 m (10 フィート)
- Ethernet クロスオーバーケーブル (P/N 24100163) 3 m (10 フィート)
- サービスノートパソコン (またはパソコン)
- T シリーズテープドライブ用 VOP (Virtual Operator Panel) バージョン 1.0.11 以降
- HP LTO テープドライブ用 Virtual Operator Panel バージョン 1.0.12 以降
- IBM LTO テープドライブ用 Virtual Operator Panel バージョン 1.0.14 以降
- LTO5 テープドライブ用 Virtual Operator Panel バージョン 1.0.16 以降
- MD-VOP (Multi-Drive Virtual Operator Panel) バージョン 1.1 以降

サポートされるプラットフォームと Web ブラウザ

マネージャー (グラフィカルユーザーインタフェース - GUI) は、Windows XP または Solaris プラットフォームにインストールする必要があります。

Web ブラウザ :
Embedded Lights Out Manager では、Web ブラウザと Java のバージョンが認識されます。詳細および Web ブラウザについては、『Embedded Lights Out Manager Administration Guide PN: 819-6588-xx』を参照してください。

表 3-8 に、サポートされるオペレーティングシステムと Web ブラウザの一覧を示します。

表 3-8 オペレーティングシステムと Web ブラウザ

クライアント OS	これらの Web ブラウザをサポート	Java Runtime Environment (Java Web Start を含む)
■ Microsoft Windows XP ■ Microsoft Windows 2003 ■ Microsoft Windows Vista ■ Windows 7 および 2008 サーバー	■ Internet Explorer 6.0 以降 Mozilla 1.7.5 以降 ■ Mozilla Firefox 1.0	JRE 1.5 (Java 5.0 Update 7 以降)
■ Red Hat Linux 3.0 および 4.0	■ Mozilla 1.7.5 以降 ■ Mozilla Firefox 1.0	JRE 1.5 (Java 5.0 Update 7 以降)

表 3-8 オペレーティングシステムと Web ブラウザ (続き)

■ Solaris 9 ■ Solaris 10 ■ Solaris Sparc ■ SUSE Linux 9.2	■ Mozilla 1.7.5	JRE 1.5 (Java 5.0 Update 7 以降)
Java Runtime Environment 1.5 は、http://java.com からダウンロードできます。 ELOM マニュアルの最新バージョンは、http://dlc.sun.com/ で参照できます。		

ファームウェアバージョン

ファームウェアの最小要件を次に示します。

表 3-9 ファームウェア互換性

コンポーネント	バージョン	バージョン	バージョン	バージョン
バージョン 2.x	2.02	2.1	2.2	2.3

ライブラリ管理

ACSLS	7.1 および 7.1.1 (PUT0701)。または 7.2、7.3、および 8.0
HSC	6.1 または 6.2
VSM	6.1 または 6.2 (VTCS および VTSS を含む)
VTL モデル	1.0 または 2.0

テープドライブ	SL8500	SL3000	Lxxx	9310	SL500	SL24	SL48	VOP
T10000A FC	FRS_3.11 D-137113	L-FRS_2.0 D-137113	L-3.17.03 D-137113	L-4.4.08 D-137113	-	-	-	1.0.11
T10000A FICON	L-3.11c D-137114	L-FRS_2.0 D-137114	L-3.17.03 D-137114	L-4.4.08 D-137114	-	-	-	1.0.11
T10000B FC	L-3.98b D-138x07	L-FRS_2.0 D-138x07	L-3.17.03 D-138x07	-	-	-	-	1.0.12
T10000B FICON	L-3.98b D-138x09	L-FRS_2.0 D-138x09	L-3.17.03 D-138x09	-	-	-	-	1.0.12
T9840D FC	L-3.98 D-142x07	L-FRS_2.0 D-142x07	L-3.17.03 D-142x07	L-4.4.08 D-142x07	-	-	-	1.0.12
T9840D FICON および ESCON	L-3.98 D-142x07	L-FRS_2.0 D-142x07	L-3.17.03 D-142x07	L-4.4.08 D-142x07	-	-	-	1.0.12
HP LTO LTO4 LTO5	L-3.98B D-H58s F D-I2DS F	FRS_2.0 5 D-H58s F D-I2DS F	-	-	L-i17 D-H58s F D-I2DS F	L-D.90 D-I2DS F	L-G.20 D-I2DS F	1.0.12 1.0.16
IBM LTO LTO4 LTO5	FRS_4.70 D-94D7 F D-A232 F	FRS_2.30 D-94D7 F D-A232 F	-	-	L-i17 D-94D7 F D-A232 F	L-D.90 D-A232 F	L-G.20 D-A232 F	1.0.14 1.0.16

凡例 :

L- ライブラリファームウェアバージョン
D- ドライブファームウェアバージョン
H58s F = ファイバチャネルファームウェア (HP LTO4)
B57s S = SCSI ファームウェア (HP LTO4)
F/FC = ファイバチャネル
SPS = 特別なファームウェア。承認が必要。
n/a = サポートなし。該当なし。
FRS_ = ライブラリファームウェアバージョン

第 4 章

コンポーネント

この章では、Oracle Key Manager 暗号化ソリューションのコンポーネントについて説明します。

サポートされる構成

Oracle Key Manager 暗号化ソリューションに関する顧客の要件と構成をサポートするために、次のコンポーネントを注文することができます。

- 「鍵管理アプライアンス」
  これは鍵の作成、管理、および割り当てに必須のコンポーネントです。

Oracle の StorageTek ライブラリのいずれかを使用して暗号化ソリューションを実装するときは、次を確認してください。

- 「SL8500 モジュール式ライブラリシステム」
- 「SL3000 モジュール式ライブラリシステム」
- 「SL500 モジュール式ライブラリシステム」
- 「9310 自動カートリッジシステム」
- 「L シリーズライブラリ」
- 「SL24 オートローダおよび SL48 ライブラリ」
- 「ラックマウント」

サポートされるテープドライブ

顧客は、暗号化に使用するテープドライブのタイプを自由に選択できます。

- T10000A、T10000B、または T10000C、あるいはそれらすべて
- T9840D
- HP LTO4 または LTO5、あるいはその両方
- IBM LTO4 または LTO5、あるいはその両方

サポートされるテープドライブのファームウェアのバージョンについては、「ファームウェアバージョン」を参照してください。

サポートされるデータベース

Oracle のデータベースのいずれかを使用して暗号化ソリューションを実装するときは、次を確認してください。

- Oracle Database 11gR2 の Transparent Data Encryption (TDE) スイートとのインタフェース
- Oracle Database 製品
- Oracle Real Application Clusters (Oracle RAC)
- Oracle Data Guard
- Oracle Exadata Database Machine
- Oracle Recovery Manager (RMAN)
- Oracle Data Pump

すべてのエディションは共通の同じコードベースを使用して構築されているため、データベースアプリケーションを小さな単一プロセッサのサーバーからマルチプロセッサのサーバーのクラスタに簡単に拡張できます。

次の機能を比較してください。

表 4-1 データベースの選択肢

主要な機能の要約	Standard Edition One	Standard Edition	Enterprise Edition
最大 (ソケット)	2	4	制限なし
RAM	OS の最大	OS の最大	OS の最大
データベースのサイズ	制限なし	制限なし	制限なし
Windows	はい	はい	はい
Linux	はい	はい	はい
Unix	はい	はい	はい
64 ビットのサポート	はい	はい	はい

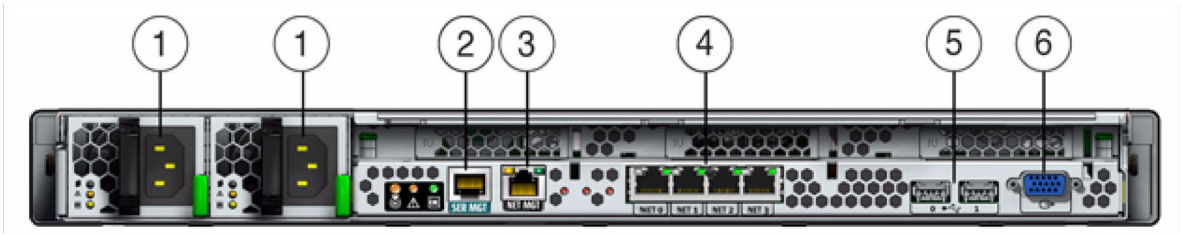
鍵管理アプライアンス

最新の鍵管理アプライアンスは Sun Fire X4170 M2 サーバーです。

- ラックマウント可能な鍵管理アプライアンス (KMA)、注文 : **CRYPTO-KMA-23** または **597-1095-01**
- SCA6000 カードが必要な場合、注文 : **375-3424-06**
  このカードにより、暗号化鍵は FIPS 140-2 レベル 3 準拠になります。

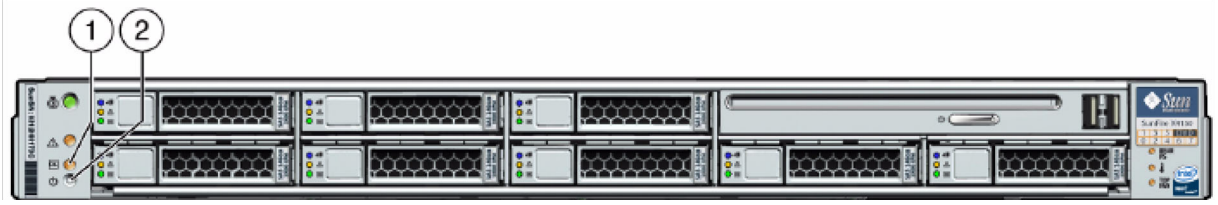
このサーバーには、インストール済みの Solaris 10 オペレーティングシステムと専用の鍵管理システムソフトウェアが付属しています。

図 4-1 鍵管理アプライアンス - 4170 の背面パネル



1. AC 電源コネクタ
2. シリアル管理 (SER MGT) RJ-45 シリアルポート
3. サービスネットワーク (NET MGT) ポート
4. Ethernet ポート (0、1、2、3)
5. USB ポート (0、1)
6. ビデオコネクタ (VGA)

図 4-2 鍵管理アプライアンス - 4170 のフロントパネル



1. 電源 /OK LED
2. 電源ボタン

注 — CRYPTO-1XTO23UP は KMA 1.x のバージョン 2.3 へのアップグレードキットです。

最新バージョンは 2.4 です。

SL8500 モジュール式ライブラリシステム

図 4-3 SL8500 モジュール式ライブラリシステムの要件

説明 :
1 台の SL8500 ライブラリには最大で次を格納できます。
- 1,448 - 10,000 巻のテープカートリッジ
- 64 台のテープドライブ

10 台のライブラリから成る SL8500 ライブラリコンプレックスには次を格納できます。
- 最大 100,000 巻のテープカートリッジ
- 640 台のテープドライブ

オペレーティングシステムのサポート :
SL8500 はすべての主要なオペレーティングシステムをサポートします : エンタープライズおよびオープンシステム。

ホストからライブラリへのインタフェース :
- シングル Ethernet* (TCP/IP) 1x
- デュアル TCP/IP* (オプション機能) 2x
- マルチホスト (オプション機能) 4x

このライブラリは、レール境界を使用して最大 4 つのパーティションを含む**パーティション分割**をサポートしています。

注文番号	**説明**
CRYPTO-2X-SL8500-N	SL8500 ライブラリで使用する Sun StorageTek 暗号化キット。SL8500 ライブラリ内部の取り付け用の 24 ポート Ethernet スイッチ、ケーブル、およびラック搭載用ハードウェア
XSL8500-ETHRNT-Z	PUE Ethernet カード / スイッチ (PN: 419951602)

ファームウェアレベル

ライブラリ	FRS_3.72 (FRS_3.98 以降を推奨、LTO4 をサポートするため) FRS_4.70 (最新) FRS_6.02 (冗長な電子機器機能)
StreamLine ライブラリコンソール	FRS_4.00
テープドライブ : ■ T10000A ■ T10000B ■ T10000C ■ T9840D ■ HP LTO4 ■ HP LTO5 ■ IBM LTO4 ■ IBM LTO5	 1.34.208 以降 1.38.x07 以降 最新のレベルを確認してください 1.42.104 以降 H58S ファイバチャネル I2DS ファイバチャネル 94D7 ファイバチャネル A232 ファイバチャネル

図 4-3 SL8500 モジュール式ライブラリシステムの要件

VOP (Virtual Operator Panel)	バージョン 1.0.14 以降 (LTO4 をサポートするため) バージョン 1.0.16 (最新)

SL3000 モジュール式ライブラリシステム

図 4-4 SL3000 モジュール式ライブラリシステムの要件

概要 :
SL3000 ライブラリは顧客に次の利点をもたらします :

- 200 - 5800 個のスロットに対応するストレージ容量におけるスケーラビリティー
- 1 - 56 台のテープドライブに対応するパフォーマンス
- 標準のインタフェース (Ethernet やファイバチャネル) を使用した異機種混在の接続
- 複数のライブラリ管理ソフトウェアのオプション

オペレーティングシステムのサポート :
SL3000 はすべての主要なオペレーティングシステムをサポートします : エンタープライズおよびオープンシステム
ホストからライブラリへのインタフェース :

- シングル Ethernet* (TCP/IP) 1x
- デュアル TCP/IP* (オプション機能) 2x
- ファイバチャネル* (デュアルポートのオプション機能) 2x

* パーティション分割をサポート

注文番号	説明
■ SL3000 キット 1 XSL3000-ETHRNT1-N ■ SL3000 キット 2 XSL3000-ETHRNT2-N ■ SL3000 キット 3 XSL3000-ETHRNT3-N ■ SL3000 キット 4 XSL3000-ETHRNT4-N	SL3000 は、1 - 56 台のテープドライブに接続する Ethernet スイッチおよびケーブルに 4 つの異なるパーツ番号を使用しています。 **注 :** SL3000 には限られた内部ラックスペースがあります。 ドライブの数に応じて、顧客は外付けのラックを注文することが必要な場合があります。

ファームウェアレベル

ライブラリ	FRS_2.0.2、FRS_2.30、FRS_2.8x
StreamLine ライブラリコンソール	FRS_4.0

図 4-4 SL3000 モジュール式ライブラリシステムの要件

テープドライブ : ■ T10000A ■ T10000B ■ T10000C ■ T9840D ■ HP LTO4 ■ HP LTO5 ■ IBM LTO4 ■ IBM LTO5	 1.34.208 以降 1.38.x07 以降 最新のレベルを確認してください 1.42.104 以降 H58S ファイバチャネル I2DS ファイバチャネル 94D7 ファイバチャネル A232 ファイバチャネル
VOP (Virtual Operator Panel)	バージョン 1.0.14 以降 バージョン 1.0.16

SL500 モジュール式ライブラリシステム

図 4-5 SL500 モジュール式ライブラリシステムの要件

概要 :
SL500 ライブラリは、拡張性に優れた内蔵型の完全に自動化されたカートリッジテープストレージシステムであり、
標準の 483mm (19 インチ) のラックまたはキャビネットに搭載されています。このライブラリは 1 - 5 個のモジュール
(1 つの基本モジュールと最大 4 つの拡張モジュール) で構成できます。
スケーラビリティーのおかげで、SL500 ライブラリには次を格納できます。

- 最小 : 530 個のデータカートリッジスロットを持つ 2 台のテープドライブ
- 最大 : 395 個のデータカートリッジスロットを持つ 18 台のテープドライブ
- 5 - 45 個のスロット (モジュールの数による) を収容するカートリッジアクセスポート

中間にさまざまなテープドライブやカートリッジスロットが含まれます。

注 : ライブラリと同じラックに暗号化ハードウェアを取り付けられます (取り付けられているモジュールの数による)。

オペレーティングシステムのサポート :
SL500 はすべての主要なオペレーティングシステムをサポートします : エンタープライズおよびオープンシステム

ホストからライブラリへのインタフェース :

- シングル Ethernet* (TCP/IP) 1x
- ファイバチャネル

* パーティション分割をサポート

注文番号	説明
CRYPTO-2X-SL500B-N	基本モジュール (必須) SL500 ライブラリベースで使用する暗号化キット。SL500 ライブラリ内部の取り付け用の Ethernet スイッチおよびケーブル。さらに、ドライブ拡張モジュールごとに拡張モジュールキット CRYPTO-2X-SL500X-N が 1 つ必要です。
CRYPTO-2X-SL500X-N	拡張モジュール (オプション) SL500 ライブラリ拡張で使用する暗号化キット。SL500 ライブラリ内部の取り付け用の Ethernet ケーブル。 最大 4 つの拡張モジュールを追加できます。 **注 :** SL500 はラックに取り付け済みのライブラリです。 ■ 拡張モジュールが 3 つ以下であれば、暗号化ハードウェアを同じラックに取り付けられます。

図 4-5 SL500 モジュール式ライブラリシステムの要件

ファームウェアレベル

ライブラリ	i15 - 1300、i16 - 1373?i17 - 139x、**i18** - 1407
テープドライブ : ■ HP LTO4 ■ HP LTO5 ■ IBM LTO4 ■ IBM LTO5	 H58S ファイバチャネル (SCSI: B57S) I2DS ファイバチャネル 94D7 ファイバチャネル A232 ファイバチャネル
VOP (Virtual Operator Panel)	バージョン 1.0.14 以降 (LTO4 の場合) バージョン 1.0.16

9310 自動カートリッジシステム

図 4-6　9310 自動カートリッジシステムの要件

概要 :
9310 (PowderHorn とも呼ばれる) は次を格納できます。
- 2,000 - 6,000 巻のテープカートリッジ
- 1 つのキャビネットにつき最大 **20** 台のドライブ用のスペースがある **4** つのドライブキャビネット (合計で 80 ドライブ)

オペレーティングシステムのサポート :
9310 ライブラリはすべての主要なオペレーティングシステムをサポートします : エンタープライズおよびオープンシステム

ホストからライブラリへのインタフェース :
- TCP/IP

9310 には Ethernet スイッチと 19 インチラックで構成される追加のハードウェアが必要です。

注文番号	**説明**
CRYPTO-2X-9310-Z-N	9310 ライブラリで使用する Sun StorageTek 暗号化キット。9310 内部の取り付け用の 24 ポート Ethernet スイッチおよびケーブルと、外部から KMA への接続用の 16 ポート Ethernet スイッチおよびケーブル。ラックマウントハードウェア
9310 ライブラリには次が必要です。 CRYPTO-2X-9741E-N	9310 ライブラリで使用する Sun StorageTek 暗号化キット。9741E キャビネット内部の取り付け用の 24 ポート Ethernet スイッチ、ケーブル、およびラックマウントハードウェア。暗号化に使用される追加 9741E キャビネットごとに 1 つ必要です。 RoHS 5 準拠。 **注 :** 各 9741E キャビネットには最大 20 台のテープドライブを収容することもあり、24 ポート Ethernet スイッチを使用する必要があります。
ファームウェアレベル	ファームウェアレベルまたはそれ以降
ライブラリの前提条件	9310 で T10000 テープドライブをサポートするためには、アップグレードが必要です。
機能コード :	93T1 - LSM のアップグレード (ファームウェアおよびハードウェア) 93T1 - LMU のアップグレード (ファームウェアのみ) XT10 - ハードウェアキットのアップグレード (9741E キャビネット)
ライブラリファームウェア (最小)	9311: 4.4.06 9330: TCP/IP - 2.1.02 コード 9330: 3270 - 1.9.73 コード

図 4-6 9310 自動カートリッジシステムの要件

テープドライブ : ■ T10000A ■ T10000B ■ T10000C ■ T9840D	 1.34.208 以降 1.38.x07 以降 最新のレベルを確認してください 1.42.104 以降
VOP (Virtual Operator Panel)	バージョン 1.0.11 以降 バージョン 1.0.16

L シリーズライブラリ

注 – L シリーズライブラリ (L700 および L1400) は Oracle Key Manager 暗号化ソリューション用の LTO テープドライブをサポートしていません。

図 4-7　L シリーズライブラリの要件

概要 :
L700 および L1400 ライブラリは 2 つのモデルをサポートしています。
- シングルフレームライブラリには次を格納できます。
  - 678 巻のテープカートリッジから
  - **12** 台のテープドライブまで。
- デュアルフレームライブラリには次を格納できます
  - 1,344 巻のテープカートリッジから
  - **24** 台のテープドライブまで。

オペレーティングシステムのサポート :
UNIX、Windows NT、Novel、Linux などのオープンシステムのプラットフォームをサポートします。

ホストからライブラリへのインタフェース :
- LVD または HVD SCSI
- ファイバチャネルオプション

L700e/L1400M ライブラリには、暗号化ハードウェア用の内部ラックスペースがあります。

注文番号	**説明**
CRYPTO-2X-L7/14-N	L180/700/1400 ライブラリで使用する Sun StorageTek 暗号化キット。 L シリーズライブラリ内部の取り付け用の 16 ポート Ethernet スイッチ、ケーブル、および取り付けハードウェア。
ファームウェアレベル	ファームウェアレベルまたはそれ以降
ライブラリ (最小) ■ L700e / L1400	3.11.02 以降
テープドライブ : ■ T10000A ■ T10000B ■ T10000C ■ T9840D	 1.34.208 以降 1.38.x07 以降 最新のレベルを確認してください 1.42.104 以降
VOP (Virtual Operator Panel)	バージョン 1.0.14 以降 バージョン 1.0.16

SL24 オートローダおよび SL48 ライブラリ

注 – SL24 および SL48 ライブラリは、Oracle Key Manager 暗号化ソリューション用の T シリーズのテープドライブをサポートしていません。

図 4-8 SL24 オートローダおよび SL48 ライブラリの要件

概要 :
Oracle の **StorageTek SL24 テープオートローダ**は、大容量の自動バックアップおよび回復をスペース効率よく提供する、きわめて扱いやすい製品です。

ドライブが 1 台の場合、このオートローダには取り外し可能な 12 スロットマガジンが 2 つ、データカートリッジのインポートおよびエクスポート専用のメールスロットが 1 つ装備されています。

Oracle の **StorageTek SL48 テープライブラリ**は、データストレージに対する要求 (無人バックアップ、アーカイブ、障害回復など) を満たすことができます。

SL48 テープライブラリは 4U フォームファクタの製品です。ドライブが 1 台の場合、このライブラリには取り外し可能な 12 スロットマガジンが 4 つ、データカートリッジのインポートおよびエクスポート専用のメールスロットが 3 つ装備されています。

オペレーティングシステムのサポート :
幅広い種類のサーバー、オペレーティングシステム、および ISV パッケージをサポートしています。

ホストからライブラリへのインタフェース :
両製品には、どのストレージ環境にも柔軟に組み込めるように、SCSI、SAS、および FC インタフェースが備わっています。

SL24 オートローダ

36T バイトのネイティブ容量 (StorageTek LTO5 テープドライブ搭載の場合)

SL48 ライブラリ

72T バイトのネイティブ容量 (StorageTek LTO5 テープドライブ搭載の場合)

注文番号	説明
LTO-ENCRYPT-ACTIVE	LTO5 暗号化対応テープドライブ

ファームウェアレベル

ライブラリ (最小) ■ SL24 オートローダ ■ SL48 ライブラリ	 D.90/3.00e G.20/3.00e

図 4-8 SL24 オートローダおよび SL48 ライブラリの要件

暗号化対応テープドライブ : ■ HP LTO5 ■ IBM LTO5	 I2DS A232
VOP (Virtual Operator Panel)	バージョン 1.0.16 (LTO5 テープドライブの場合) MD-VOP 1.x

ラックマウント

図 4-9 ラックマウントの要件

StorageTek ラックは、6 トレイに最大 **12** の手動マウントのテープドライブを収容できます。

この図は、T10000 ラックモジュールを示しています。
- 上部 (A) の操作パネルは、左側のドライブで機能します。
- 下部 (B) の操作パネルは、右側のドライブで機能します。

取り付けるドライブが 1 台のみの場合は、左側に取り付ける必要があります。

推奨事項 :
この構成では、お客様は CBNT42U キャビネットを購入するようにしてください。

注文番号	説明
CRYPTO-2X-RACK-Z-N	StorageTek ラックマウントキット。 16 ポートスイッチおよび配線を含みます。

ファームウェアレベル

テープドライブ : ■ T10000A ■ T10000B ■ T10000C ■ T9840D	 1.34.208 以降 1.38.x07 以降 最新のレベルを確認してください 1.42.104 以降
VOP (Virtual Operator Panel)	バージョン 1.0.11 以降

テープドライブの操作方法

詳細は、それぞれのテープドライブのシステムアシュアランスガイドを参照してください。

表 4-2 テープドライブの注文手順

資料の説明	Part Number
T10000 Tape Drive Systems Assurance Guide	StorageTek: TM0002
T9x40 Tape Drive Systems Assurance Guide	StorageTek: MT5003
Service Delivery Platform Systems Assurance Guide	StorageTek: 11042004

ライブラリの操作方法

詳細は、それぞれのライブラリのシステムアシュアランスガイドを参照してください。

表 4-3 ライブラリの注文手順

資料の説明	Part Number
SL8500 Modular Library Systems Assurance Guide	StorageTek: MT9229
SL3000 Modular Library Systems Assurance Guide	StorageTek: 316194101
SL500 Modular Library Systems Assurance Guide	StorageTek: MT9212
L700/1400 Library Ordering and Configuration Guide	StorageTek: MT9112
L180 Library Ordering and Configuration Guide	StorageTek: MT9112
9310 PowderHorn Library Systems Assurance Guide	StorageTek: ML6500

電源ケーブル

詳細およびその他のパーツ番号については、次を参照してください：
http://scss280r1.singapore.sun.com/handbook_internal/Devices/AC_Power/ACPOWER_AC_Power_Cords.html

ATO 電源コード	PTO と同等の製品	説明	電流	電圧	ケーブル
333A-25-10-AR	X312F-N	電源コード、アルゼンチン、2.5m、IRAM2073、10A、C13	10	250	180-1999-02
333A-25-10-AU	X386L-N	電源コード、オーストラリア、2.5m、SA3112、10A、C13	10	250	180-1998-02
333A-25-10-BR	X333A-25-10-BR-N	電源コード、ブラジル、2.5m、NBR14136、10A、C13	10	250	180-2296-01
333A-25-10-CH	X314L-N	電源コード、スイス、2.5m、SEV1011、10A、C13	10	250	180-1994-02
333A-25-10-CN	X328L	電源コード、中国、2.5m、GB2099、10A、C13	10	250	180-1982-02
333A-25-10-DK	X383L-N	電源コード、デンマーク、2.5m、DEMKO107、10A、C13	10	250	180-1995-02
333A-25-10-EURO	X312L-N	電源コード、ヨーロッパ、2.5m、CEE7/VII、10A、C13	10	250	180-1993-02
333A-25-10-IL	X333A-25-10-IL-N	電源コード、イスラエル、2.5m、SI-32、10A、C13	10	250	180-2130-02
333A-25-10-IN	X333A-25-10-IN-N	電源コード、インド、2.5m、IS1293、10A、C13	10	250	180-2449-01
333A-25-10-IT	X384L-N	電源コード、イタリア、2.5m、CEI23、10A、C13	10	250	180-1996-02
333A-25-10-KR	X312G-N	電源コード、韓国、2.5m、KSC8305、10A、C13	10	250	180-1662-03
333A-25-10-TW	X332A-N	電源コード、台湾、2.5m、CNS10917、10A、C13	10	125	180-2121-02
333A-25-10-UK	X317L-N	電源コード、英国、2.5m、BS1363A、10A、C13	10	250	180-1997-02
333A-25-10-ZA	X333A-25-10-ZA-N	電源コード、南アフリカ、2.5m、SANS164、10A、C13	10	250	180-2298-01
333A-25-15-JP	X333A-25-15-JP-N	電源コード、日本、2.5m、PSE5-15、15A、C13	15	125	180-2243-01
333A-25-15-NEMA	X311L	電源コード、北米 / アジア、2.5m、5-15P、15A、C13	15	125	180-1097-02
333A-25-15-TW	X333A-25-15-TW-N	電源コード、台湾、2.5m、CNS10917、15A、C13	15	125	180-2333-01
333F-20-10-NEMA	X320A-N	電源コード、北米 / アジア、2.0m、6-15P、10A、C13	10	250	180-2164-01
333F-25-15-JP	X333F-25-15-JP-N	電源コード、日本、2.5m、PSE6-15、15A、C13	15	250	180-2244-01
333J-40-15-NEMA	X336L	電源コード、北米 / アジア、4.0m、L6-20P、15A、C13	15	250	180-2070-01
333R-40-10-309	X332T	電源コード、INTL、4.0m、IEC309-IP44、10A、C13	10	250	180-2071-01

Sun Rack 以外で使用					
333V-20-15-C14	X333V-20-15-C14-N	電源コード、ジャンパ、ストレート、2.0m、C14、15A、C13	15	250	180-2442-01
333V-30-15-C14	X333V-30-15-C14-N	電源コード、ジャンパ、ストレート、3.0m、C14、15A、C13	15	250	180-2443-01
Sun Rack (NGR) で使用					
333W-10-13-C14RA	X9237-1-A-N	電源コード、ジャンパ、1.0m、C14RA、13A、C13	13	250	180-2082-01
333W-25-13-C14RA	X9238-1-A-N	電源コード、ジャンパ、2.5m、C14RA、13A、C13	13	250	180-2085-01
Sun Rack II (Redwood) で使用					
SR-JUMP-1MC13	XSR-JUMP-1MC13-N	電源コード、ジャンパ、SR2、1.0m、C14RA、13A、C13	13	250	180-2379-01
SR-JUMP-2MC13	XSR-JUMP-2MC13-N	電源コード、ジャンパ、SR2、2.0m、C14RA、13A、C13	13	250	180-2380-01

ATO BOM (Bill of Materials)

表 4-4 ATO BOM (Bill of Materials) のパーツ番号と説明

注文番号	説明
CRYPTO-2X-SL8500-N	SL8500 ライブラリで使用する Sun StorageTek 暗号化キット。SL8500 ライブラリ内部の取り付け用の 24 ポート Ethernet スイッチ、ケーブル、およびラックマウントハードウェア
CRYPTO-2X-9310-Z-N	9310 ライブラリで使用する Sun StorageTek 暗号化キット。9310 内部の取り付け用の 24 ポート Ethernet スイッチおよびケーブルと、外部から KMA への接続用の 16 ポート Ethernet スイッチおよびケーブル。ラックマウントハードウェア
CRYPTO-2X-9741E-N	9310 ライブラリで使用する Sun StorageTek 暗号化キット。9741E キャビネット内部の取り付け用の 24 ポート Ethernet スイッチ、ケーブル、およびラックマウントハードウェア。暗号化に使用される 9741E キャビネットごとに 1 つ必要です。RoHS 5 準拠。
CRYPTO-2X-L7/14-N	L180/700/1400 ライブラリで使用する Sun StorageTek 暗号化キット。L シリーズライブラリ内部の取り付け用の 16 ポート Ethernet スイッチ、ケーブル、および取り付けハードウェア。
CRYPTO-2X-SL500X-N	(拡張モジュール) SL500 ライブラリ拡張で使用する Sun StorageTek 暗号化キット。SL500 ライブラリ内部の取り付け用の Ethernet ケーブル。
CRYPTO-2X-SL500B-N	(基本モジュール) SL500 ライブラリベースで使用する Sun StorageTek 暗号化キット。SL500 ライブラリ内部の取り付け用の Ethernet スイッチおよびケーブル。注 : 暗号化ケーブル SL500 には基本ライブラリアクセサリキット CRYPTO-2X-SL500B-N が 1 つ必要です。さらに、ドライブ拡張モジュールごとに拡張モジュールアクセサリキット CRYPTO-2X-SL500X-N が 1 つ必要です。
XSL3000-ETHRNT1-N	StorageTek SL3000 X オプション、テープドライブ用の Ethernet スイッチ、8 ドライブのケーブルハーネスを含む、BM または DEM の最初のドライブアレイをサポート、SDP および暗号化に必要、電源ケーブルを含む、Ethernet スイッチハーネスを含む
XSL3000-ETHRNT2-N	StorageTek SL3000 X オプション、8 ドライブの Ethernet ケーブルハーネス、XSL3000-ETHRNT1-Z が必要、BM または DEM の 2 番目のドライブアレイをサポート、SDP および暗号化に必要、電源ケーブルとスイッチハーネス B/C を含む、
XSL3000-ETHRNT3-N	StorageTek SL3000 X オプション、テープドライブ用の Ethernet スイッチ、8 ドライブのケーブルハーネスを含む、BM または DEM の 3 番目のドライブアレイをサポート、SDP および暗号化に必要、電源ケーブルとスイッチハーネス A/C を含む

表 4-4 ATO BOM (Bill of Materials) のパーツ番号と説明 (続き)

注文番号	説明
XSL3000-ETHRNT4-N	StorageTek SL3000 X オプション、8 ドライブの Ethernet ケーブルハーネス、XSL3000-ETHRNT4-Z が必要、DEM の 4 番目のドライブアレイをサポート、SDP および暗号化に必要、電源ケーブルを含む、Ethernet スイッチハーネス C/C を含む。注 : SL3000 は暗号化用の専用キットをリリースしました。4 つのパーツがあります - ケーブルのみ異なっていると思われますが、確実ではありません。数量やタイプは、サポートされる暗号化対応ドライブの数によって異なります。
CRYPTO-2X-RACK-Z-N	冗長構成の Oracle Key Manager で使用する Sun StorageTek 16 ポート Ethernet スイッチおよびラックマウントハードウェア (ラックマウントテープ用)
その他のスイッチオプション :	
CRYPTO-X-24PT-Z-N	Sun StorageTek 24 ポート Ethernet スイッチ。取り付けハードウェアやケーブルはありません。

付　録 **A**

IBM ICSF 統合

この付録では、IBM® ICSF (Integrated Cryptography Service Facility)[1] の概要について説明します。詳細については、次を参照してください。

- Oracle Key Manager: ICSF Integration Guide PN: 31619810x
- Oracle Key Manager: 管理ガイド PN: E25343-01

システム要件

IBM メインフレームと OKM クラスタの両方に、このソリューション用のシステム要件があります。

IBM メインフレーム

IBM z/OS メインフレームが ICSF HCR-7740 以降を実行している必要があります。

ELS (Enterprise Library Software 7.0) または NCS (Nearline Control Software 6.2) と、関連付けられた PTF。

また、Crypto Express2 コプロセッサ (CEX2C) カードが IBM メインフレームに取り付けられている必要があります。

OKM

OKM がバージョン 2.2 以降を実行している必要があります。

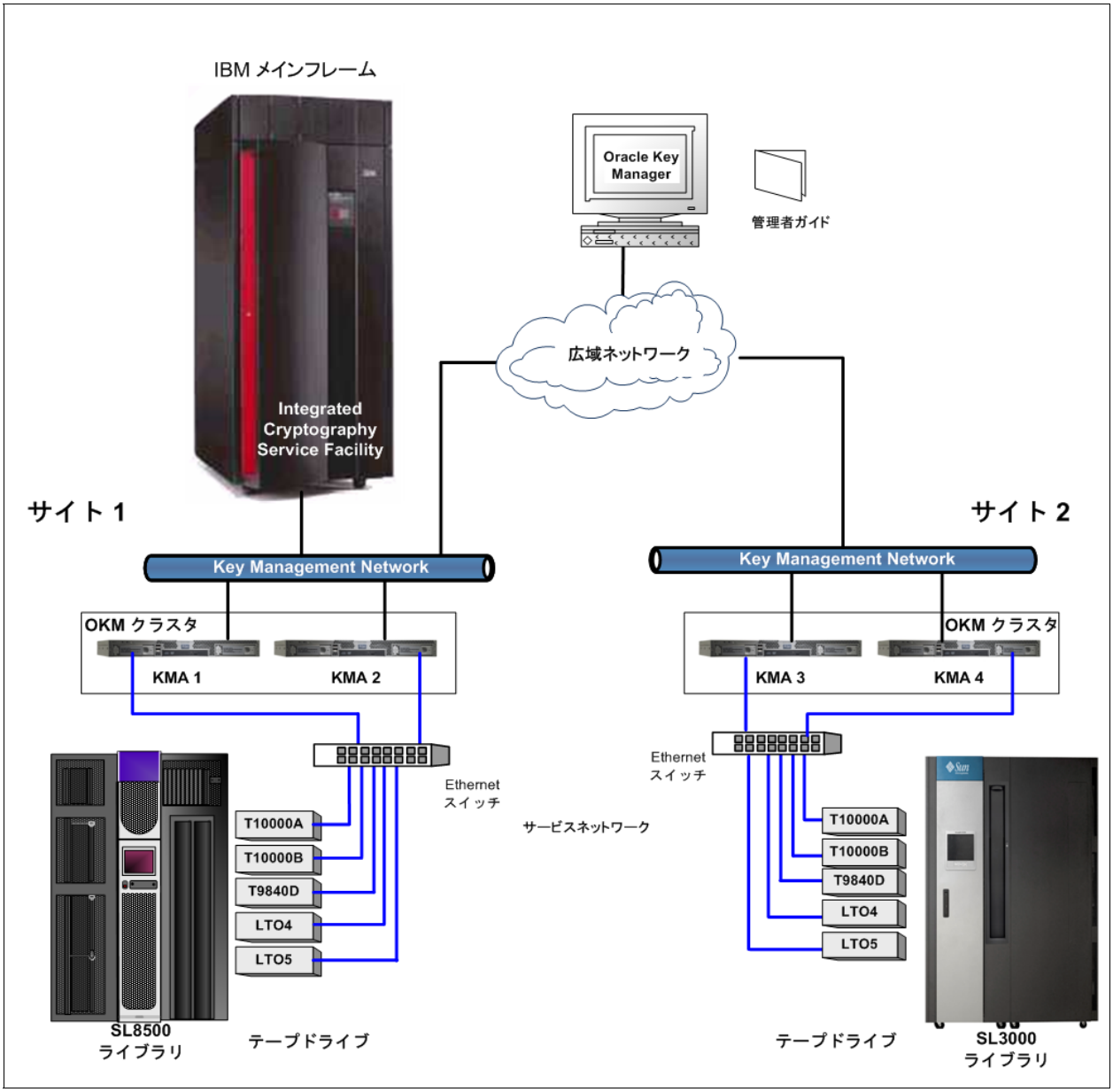
1. ICSF は、z/OS 独自のソフトウェアルーチンとして、または Oracle Key Manager などの外部暗号化ハードウェアにアクセスすることで、暗号化サポートを提供する z/OS のソフトウェアコンポーネントです。

このソリューションについて

IBM ICSF (Integrated Cryptography Service Facility) は、外部鍵ストアが IBM メインフレーム内に常駐し、そこに TLS/XML プロトコルを使ってアクセスする暗号化ソリューションです。このプロトコルは、鍵が IBM Integrated Cryptography Service Facility のトークンデータセットに格納されている IBM メインフレームでサポートされます。

図 A-1 に、一般的な構成を示します。

図 A-1 ICSF サイト構成



サイト構成

クラスタは、新しいマスター鍵 (ICSF ではアプリケーション鍵と呼ばれる) を作成するために、IBM メインフレームに定期的に要求を発行します。

すると KMA は、これらの新しいマスター鍵を使って、新しいテープ暗号化鍵を生成します。

注 – CCA (Common Cryptographic Architecture/ICSF) が常駐するメインフレーム。

鍵ストアとマスター鍵モード

バージョン 2.x では、KMA は、暗号化アクセラレータ (SCA6000) カードを使って独自の鍵を生成します。顧客によっては、IBM メインフレームに含まれている外部鍵ストアで作成され、そこに保存されるマスター鍵を KMA で使用することを望む場合もあります。

バージョン 2.2 では、マスター鍵モード機能が導入されています。この機能が有効になっているときは、OKM はマスター鍵セットからテープ暗号化鍵を生成します。マスター鍵は、外部鍵ストアで作成され、そこに保存されます。

テープ、マスター鍵、および出荷時デフォルト装置だけで、完全な障害回復が可能です。

IBM メインフレーム

OKM クラスタ用の外部鍵ストアとして使用されるように z/OS システムを構成するには、さまざまな手順が必要です。

情報の更新

IBM メインフレームが構成されたあとに、z/OS システムプログラマは次の情報を OKM の管理者に提供する必要があります。

- メインフレームのホスト名または IP アドレス
- ポート番号 (9889 など)
- Web アプリケーションパス (「/cgi/smcgcsf」など)
- クライアント「ユーザー証明書」(メインフレーム からエクスポートおよび転送されたもの) が含まれるファイル
- クライアント非公開鍵 (メインフレームからエクスポートおよび転送されたもの) が含まれるファイル
- クライアント非公開鍵が作成されたときに使用されたパスワード
- ルート認証局証明書 (メインフレームからエクスポートおよび転送されたもの) が含まれるファイル

Oracle Key Manager の管理者は、これらの情報を OKM マネージャー GUI の「Security Parameters」パネルで「Master Key Provider」設定として入力します。

管理者がこれらの設定を保存したあとで、OKM クラスタは IBM メインフレーム上でプロキシへの要求の発行を開始します。

クライアント「ユーザー証明書」とクライアント非公開鍵は、IBM メインフレームからエクスポートされるときに、同じファイルに含まれる場合があります。その場合は、管理者が「Master Key Provider」設定の「OKM Certificate File Name」および「OKM Private Key File Name」フィールドに同じファイルを指定してください。

付　録 **B**

Oracle データベースの暗号化

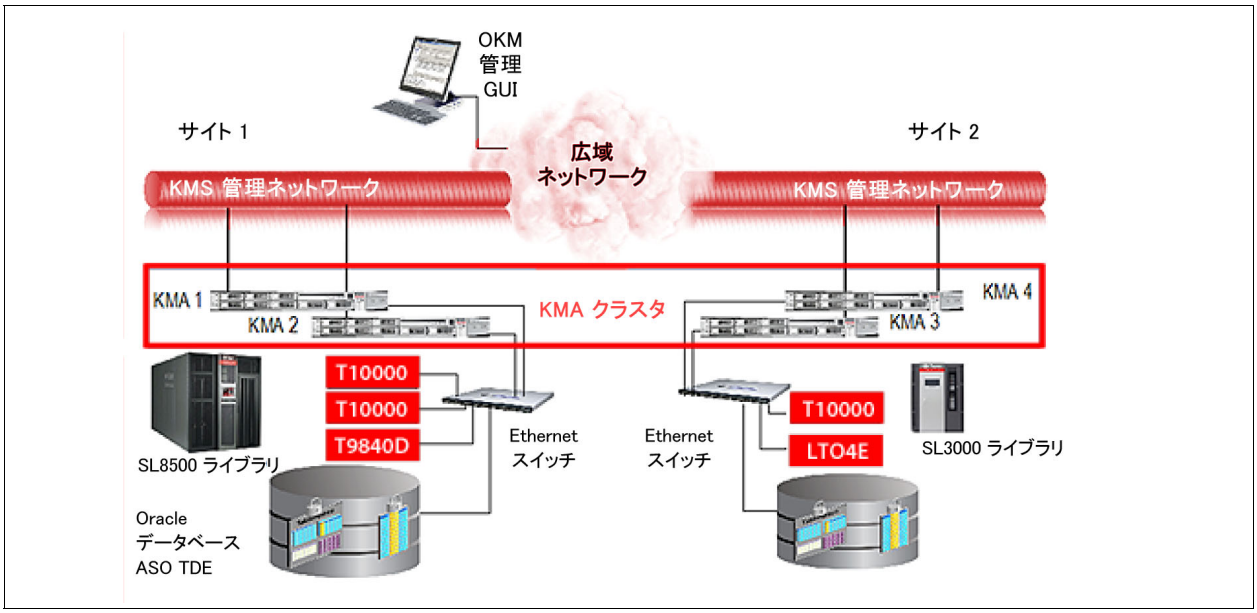
注 – 詳細は、1) 『Using Oracle Key Manager with Advanced Security Transparent Data Encryption』および 2) 『Oracle's Advanced Security Transparent Data Encryption Best Practices』の 2 つのホワイトペーパーおよび『OKM 管理者ガイド』を参照してください。

Transparent Data Encryption (TDE) と Oracle Key Manager の組み合わせは、Oracle **Database** のマスター鍵を確実に管理するための最適なワンストップの Oracle ソリューションです。

Oracle Key Manager (OKM) は、Oracle Advanced Security の Transparent Data Encryption の認定を受けています。これは、Oracle StorageTek テープドライブで使用されているのと同じ暗号化テクノロジーを、次を含む Oracle Database 11gR2 の暗号化鍵の管理に利用できるようになったことを意味します。

- Oracle Database 製品
- Oracle Real Application Clusters (Oracle RAC)
- Oracle Data Guard
- Oracle Exadata Database Machine
- Oracle Recovery Manager (RMAN)
- Oracle Data Pump

図 B-1　Oracle Key Manager および Oracle Database の例



Transparent Data Encryption の概要

Transparent Data Encryption (TDE) は、機密性のあるデータベース情報の暗号化および復号化に使用するサービスを列レベルまたはテーブル領域レベルで提供します。Oracle Key Manager および Transparent Data Encryption のソリューションは、Transparent Data Encryption の汎用マスター鍵に対してエンタープライズクラスの鍵管理を提供します。このソリューションでは、鍵をデータベースの外部で管理できます。

Oracle Key Manager (OKM) を使用したポリシーベースの鍵管理は、Transparent Data Encryption のマスター鍵を管理するための堅牢で柔軟なソリューションを提供します。

Transparent Data Encryption (TDE) は、TDE 列およびテーブル領域の暗号化の両方に、2 層鍵アプローチを使用した暗号化サービスを提供します。

- 第 1 層はマスター暗号化鍵であり、暗号化のために使用されます。
- 第 2 層のテーブルまたはテーブル領域のデータ暗号化鍵は、データベース内に格納されます。

TDE は、マスター暗号化鍵を外部のセキュリティーモジュール (Oracle Wallet または HSM) に格納します。HSM にマスター鍵を格納することは、**セキュリティーの実践として推奨されており**、さまざまな脅威に対してもっとも高いレベルのセキュリティーを維持するために重要です。TDE のマスター暗号化鍵を安全に格納するために Oracle Key Manager を使用することを推奨します。鍵の紛失はデータの紛失を意味するため、Oracle Key Manager (OKM) などの鍵管理システムを強く推奨します。

TDE で OKM を使用するように構成すると、マスター暗号化鍵は OKM によって作成され、安全に保護されます。OKM は、レプリケーション (クラスタ内の複数のコピー) および Oracle Key Manager 自体のバックアップにより鍵を保護します。

PKCS#11 プロバイダ

公開鍵暗号方式標準規格 (PKCS) は、プラットフォームに依存しない標準規格を定義します。PKCS#11 プロバイダは、Oracle Solaris および Oracle Linux で利用可能であり、TDE が Oracle Key Manager と連動することが保証されています。このプロバイダは「pkcs11_kms」と呼ばれます。TDE は、組み込みでサポートされている Hardware Security Module (HSM) を使用して pkcs11_kms プロバイダを利用するように構成できます。

Oracle Solaris pkcs11_kms プロバイダは、Solaris 暗号化フレームワークの構成可能なコンポーネントであり、PKCS#11 プロバイダを管理するための標準の Oracle Solaris サービスに準拠しています。Linux の場合は、pkcs11_kms プロバイダを個別にインストールしてから、Oracle Database で使用するために構成します。

pkcs11_kms プロバイダは、鍵の作成操作および鍵の取得操作のために Oracle Key Manager と対話します。暗号化および復号化の機能は、Oracle Key Manager ではなく、データベースで実行されます。TDE などの PKCS#11 コンシューマアプリケーションは、それらが定義するラベルを使用して鍵オブジェクトを識別します。TDE は、マスター鍵の作成中にこのラベルを生成します。pkcs11_kms プロバイダは、このラベルを Oracle Key Manager に渡し、そこでデータユニットのメタデータとして維持管理さ

れます。Oracle Key Manager では、鍵はデータユニットと関連付けられ、pkcs11_kms プロバイダの場合、この関係は常に 1 対 1 です。新しいマスター鍵が作成されるたびに、対応する鍵オブジェクトとともに鍵ラベルを持つデータユニットが作成されます。

計画に関する考慮事項

ソリューションの計画は注意深く検討するようにしてください。次の数セクションでは、計画フェーズで検討すべき主な考慮事項をいくつか取り上げます。

Oracle Database に関する考慮事項

Oracle Key Manager は次のいずれかの Oracle Database 構成で動作します。

- 単一インスタンス、Oracle RAC One Node
- Oracle Database High Availability アーキテクチャー
- Oracle RAC - Oracle Real Application Clusters を使用した Oracle Database は Oracle Key Manager の認定を受けています。Oracle RAC システムの各ノードには、TDE が使用する構成済みの pkcs11_kms プロバイダがある必要があります。

  すべてのノードで、同じ Oracle Key Manager エージェント ID が認証のために共有されるようにしてください。Oracle RAC では、ネットワークトポロジとして、パブリックおよびプライベートネットワークを利用します。

  Oracle RAC のノード間トラフィックに使用されるプライベートネットワークは、鍵取得トラフィックをより良く分離するために Oracle Key Manager のサービスネットワークと共有できます。

  このプライベートネットワークの構成方法によっては、これにより、プライベートネットワークの外部の KMA (リモートサイトの KMA など) へのエージェントのフェイルオーバーが妨げられる可能性があります。
- Oracle RAC Extended Cluster - この構成では、鍵の取得時間を最小化するために、Oracle Key Manager クラスタ内の KMA を Oracle RAC ノードと同じネットワークに配置するようにしてください。
- Oracle Exadata Database Machine - Oracle RAC に関する考慮事項を参照してください。
- Oracle Data Guard - すべてのセカンダリデータベースは、プライマリデータベースによって使用されるのと同じ Oracle Key Manager クラスタにアクセスします。
- 複数のデータベースインスタンス - 1 つのホスト上で複数の独立したデータベースインスタンスを実行する場合は、各インスタンスで専用の PKCS#11 トークンを構成する必要があります。

  そのため、各データベースインスタンスに対して Oracle Key Manager エージェントを作成し、Oracle Key Manager へのエージェントの認証をトークンを使用して行います。これは、kmscfg(1M) ツールを使用してすべて行うことができます。
- Oracle RMAN
- Oracle Data Pump

OKM のパフォーマンスおよび可用性に関する考慮事項

pkcs11_kms トークンを使用した TDE の鍵取得は、通常、1 回の KMA アクセスで 100 - 200 ミリ秒かかります。フェイルオーバーが発生すると、応答時間はフェイルオーバーの試行回数を乗算した時間になります。Oracle Key Manager のバックアップ操作および鍵転送操作は、データベースに負荷がかかるアクティビティーであり、Oracle Key Manager データベースのパフォーマンスに影響する場合があります。

このため、Oracle Key Manager のバックアップを行うタイミングと対象を十分に検討するようにしてください。Oracle Key Manager のバックアップ (および鍵転送操作) は、クラスタ全体で行われるため、Oracle Database インスタンスで使用されていない KMA で実行できます。同様に、鍵転送操作もクラスタ全体の操作であり、任意の KMA で実行できます。このため、使用中の Oracle Database インスタンスで利用されていない KMA を選択することを推奨します。

障害回復の計画

障害回復の計画は、『Oracle Key Manager Disaster Recovery Reference Guide』および Oracle Database のドキュメントで説明されている複雑なトピックです。

障害回復計画での決定事項は、ネットワーク計画の立案にも影響します。

pkcs11 プロバイダのプロファイル領域は、障害回復計画の新しい考慮事項です。pkcs11_kms トークンを再構成する必要がないように (特に Oracle RAC のノード間で共有される場合)、この記憶領域の回復シナリオを検討します。

ネットワークの計画

Oracle Key Manager のクラスタ構成は、Oracle Database サーバーおよび企業の障害回復方針に従って計画する必要があります。Oracle Key Manager のネットワークオプションは、非常に柔軟であり、Oracle Key Manager の管理およびサービスネットワークで使用されるマルチホームのインタフェースが含まれています :

- **Oracle Key Manager Management Network** - Oracle Key Manager のクラスタの各 KMA には、管理ネットワークと呼ばれるフロントエンドネットワークインタフェースが含まれています。このインタフェースは、Oracle Key Manager のクラスタのさまざまなノードの管理および KMA によるクラスタデータのピアツーピアレプリケーションを主な目的としています。クラスタのレプリケーションのパフォーマンスを最適にするために、ギガビット Ethernet ネットワークを推奨します。サービスネットワークは、エージェントによって使用されることが推奨されていますが、管理ネットワークを使用することもできます。
- **Oracle Key Manager Service Network** - このサービスネットワークは、エージェントによって使用されることを目的にしており、鍵取得をその他のネットワークトラフィックから分離できるようにします。KMA には、信頼性を高めるために集約された 2 つのギガビット Ethernet ポートがあります。TDE のアクセスは、Oracle Key Manager のサービスネットワークを介して行うことを推奨します。概要で簡単に説明したように、サービスネットワークは、ほかのサイトへのゲートウェイを定義しないことにより、同じサイト内の KMA およびエージェントに分離できます。ほかのサイトが非常に離れたリモートにある場合、これが望ましいことがあります。ただし、可用性を最大にする場合は、ほかの Oracle Key Manager サイトへのサービスネットワークゲートウェイを構成することをオプションとして検討できます。

- **時間情報プロトコル (Network Time Protocol、NTP)** - 外部の NTP サーバーを使用して Oracle Key Manager のシステム時間を構成することを強く推奨します。

鍵管理の計画

鍵管理の計画では、企業の鍵のライフサイクルおよびセキュリティーポリシーを検討する必要があります。これらの考慮事項によって、必然的にデータ保持について検討することになります。

運用前フェーズ

通常の暗号化操作用の鍵作成素材はまだ利用できません。鍵は、まだ生成されていないか、アクティベーション前の状態である可能性があります。システムまたは企業の属性も、このフェーズで確立されます。

運用フェーズ

鍵作成素材は、利用可能であり、通常の使用状態です。鍵は、アクティブ状態です。鍵は、保護のみ、処理のみ、または保護と処理として指定できます。Oracle Key Manager は、アクティブ状態のサブ状態として保護と処理 (暗号化または復号化) および処理のみ (復号化のみ) をサポートします。

運用後フェーズ

鍵作成素材は通常の使用状態ではなくなりますが、鍵作成素材へのアクセスは可能であり、特定の状況では鍵作成素材を処理のみ (復号化のみ) に使用できます。鍵は、非アクティブ化状態または危殆化状態になります。

破棄フェーズ

鍵は利用できなくなります。存在するすべてのレコードが削除されている可能性があります。鍵は、破棄状態または破棄危殆化状態になります。鍵自体は破棄されますが、鍵の属性 (たとえば、鍵名、タイプ、暗号化有効期間、および使用期間) は保持されることがあります。

鍵ポリシーに関する考慮事項

すべての TDE マスター鍵は、AES-256 ビットであり、Oracle Key Manager によって生成されます。KMA には、FIPS 140-2 レベル 3 の認定を受けた HSM である Sun Crypto Accelerator 6000 PCIe カードを含めることができます。KMA にこの Hardware Security Module がある場合、鍵は HSM によって作成されます。それ以外の場合、暗号化操作では、Solaris 暗号化フレームワークのソフトウェアトークンプロバイダが利用されます。鍵ポリシーの計画で決定する事項に関しては、鍵のライフサイクルが主な構成項目です。鍵のライフサイクルの運用フェーズとして選択する期間は、データ保持の必要性および TDE マスター鍵が再度鍵に作成される頻度に基づいて選択するようにしてください。

注 – TDE の DDL は、Oracle Enterprise Manager 内のスキーマ暗号化ダイアログと同様に、さまざまな鍵サイズのマスター鍵の仕様をサポートします。Oracle Key Manager で使用できるのは、AES-256 ビット鍵のみです。

鍵ポリシー暗号化期間は、ライフサイクルが保護および処理 (暗号化および復号化) 状態のときに鍵を使用する期間を定義します。この期間は、マスター鍵が再作成されるまでの、マスター鍵を使用する期間に対応するようにしてください (たとえば、PCI の場合、最大 1 年間)。鍵ポリシーの暗号化有効期間は、鍵のライフサイクルが処理のみ (復号化のみ) 状態のときに、マスター鍵を使用したデータの復号化のために割り当てられている残りの時間です。

この期間の長さは、TDE マスター鍵によって保護されるデータのデータ保持要件と一致するようにしてください。通常、この値は、企業のデータ保持ポリシーに対応する年数となります (たとえば、米国の税務記録の場合、保持期間は 7 年間です)。

鍵の再作成操作はまれにしか行わないため、新しい鍵を生成する頻度は、TDE とは関係がないはずです。これが問題となる場合は、鍵ポリシーの暗号化期間を長くするか、鍵を再作成する頻度を低くすることを検討します。Oracle Key Manager の鍵プールサイズ設定パラメータは、利用可能な鍵のより大きいプールを KMA が維持管理するように増やすこともできます。

必要に応じて、さまざまなタイプのデータベースで使用するために、複数の鍵ポリシーを定義できます。

鍵グループを使用した鍵アクセス制御

複数のデータベースインスタンスまたは複数のエージェントがさまざまな目的で Oracle Key Manager のクラスタにアクセスする場合、Oracle Key Manager によって管理される鍵へのアクセスを制御する必要がある場合があります。

すべての Oracle Key Manager エージェントは、少なくとも 1 つの鍵グループに割り当てられており (デフォルトの鍵グループへの割り当ては必須です)、このグループにより、グループ内の鍵へのアクセスが承認されます。エージェントのデフォルトの鍵グループは、pkcs11_kms プロバイダのエージェントがその中で鍵を作成する唯一の鍵グループです。

マスター鍵をデータベースインスタンスまたはホスト間で共有する必要がない場合は、複数の鍵グループの使用を検討してください。例としては、ある鍵グループを本稼働データベースインスタンスで使用し、別の鍵グループを開発 / テストのデータベースで使用して、分離が保証されるようにします。テストデータベースの鍵グループのエージェントは、本稼動データベース用のマスター鍵を使用しようとすると、Oracle Key Manager によってブロックされます。また、そのような試行は Oracle Key Manager の監査ログにフラグが付けられ、本稼動データベースに支障を与える可能性がある構成エラーが存在することを示す場合があります。

TDE は、鍵ラベルの命名規則を使用したマスター鍵の分離も提供します。PKCS#11 の仕様では、鍵のラベルは一意である必要はありません。

Oracle Key Manager は、ラベルが一意になるように強制し、Oracle Key Manager のクラスタでラベルの名前空間の有効範囲がグローバルになるようにします。別個のデータベースインスタンスの別個のマスター鍵の間でラベルの衝突が発生した場合は、最初に作成されたラベルが常に返されます。これが望ましい動作ではない場合は、エージェントを分離するための手段として鍵グループを使用することを検討してください。同一のラベルを共有する、別の鍵グループに属する鍵にエージェントがアクセスしようとすると、Oracle Key Manager によって拒否されます。これは、鍵の再作成操作の際に捕促されますが、回避方法は衝突しない別のラベルが生成されるまで鍵を再作成することです。

鍵およびデータ破棄に関する考慮事項

データ保持要件に一致させるためのデータの破棄は、TDE のマスター鍵の破棄から開始できます。これらの鍵を破棄する方法とタイミングは、重要な計画項目です。Oracle Key Manager では、これを行うことができ、これらの鍵が含まれている Oracle Key Manager のバックアップを追跡することもできます。Oracle Key Manager のバックアップの管理は、障害回復計画および鍵の破棄計画の両方の項目です。

付　録 **C**

ワークシート

これ以降のページには、Oracle 暗号化ソリューション設置の準備に役立てることができるワークシートが含まれています。

これらのワークシートが含まれています。

- 「サイトログ」
- 「サポートの利用」
  - いくつかのコピーを作成してそれらを顧客に渡してください。
  - 使用方法を説明してください。
- 「初期構成ワークシート」
- 「ユーザー役割ワークシート」
- 「ドライブワークシート」(テープドライブまたはデータベース)
- 「エージェント登録ワークシート」

必要に応じてコピーを取ります。

サイトログ

アカウント名 :			
KMA			
サイトの場所 :	**KMA S/N:**	**KMA Name:**	**KMA ファームウェアバージョン :**
KMA 番号 :		**クラスタ内の KMA の数 :**	
KMA IP アドレス :		**サービスネットワーク IP:**	
Oracle Manager IP:		**ELOM / ILOM IP:**	
IPv6 l ❑ はい ❑ いいえ :		**DR サイト l ❑ はい ❑ いいえ :**	
NTP l ❑ はい ❑ いいえ :		**DHCP l ❑ はい ❑ いいえ :**	
ゲートウェイ l ❑ はい ❑ いいえ :		**DNS l ❑ はい ❑ いいえ :**	
KMA の場所 :			
Oracle Manager の場所 :			
構成タイプ :	❑ SL8500 ライブラリ ❑ SL3000 ライブラリ ❑ SL500 ライブラリ ❑ 9310 ライブラリ ❑ L シリーズ ❑ SL24/SL48 ❑ Oracle Database	**テープドライブのタイプ:** **個数 _____** **データベースタイプ :** **_____**	❑ T10000A テープドライブ ❑ T10000B テープドライブ ❑ T10000C テープドライブ ❑ T9840D テープドライブ ❑ HP LTO テープドライブ ❑ IBM LTO テープドライブ ❑ スタンドアロン
KMA			
サイトの場所 :	**KMA S/N:**	**KMA Name:**	**KMA ファームウェアバージョン :**
KMA 番号 :		**クラスタ内の KMA の数 :**	
KMA IP アドレス :		**サービスネットワーク IP:**	
Oracle Manager IP:		**ELOM / ILOM IP:**	
IPv6 l ❑ はい ❑ いいえ :		**DR サイト l ❑ はい ❑ いいえ :**	
NTP l ❑ はい ❑ いいえ :		**DHCP l ❑ はい ❑ いいえ :**	
ゲートウェイ l ❑ はい ❑ いいえ :		**DNS l ❑ はい ❑ いいえ :**	
KMA の場所 :			
Oracle Manager の場所 :			

構成タイプ :	❑ SL8500 ライブラリ ❑ SL3000 ライブラリ ❑ SL500 ライブラリ ❑ 9310 ライブラリ ❑ L シリーズ ❑ SL24/SL48 ❑ Oracle Database	**テープドライブのタイプ:** **個数** _____ **データベースタイプ :** _____	❑ T10000A テープドライブ ❑ T10000B テープドライブ ❑ T10000C テープドライブ ❑ T9840D テープドライブ ❑ HP LTO テープドライブ ❑ IBM LTO テープドライブ ❑ スタンドアロン

サポートの利用

技術サポートは週 7 日 1 日 24 時間利用することができ、Oracle サポートに電話していただくことで始まります。資格のある担当者がただちに対応し、障害情報を記録して、適切なレベルのサポートをご案内いたします。

Oracle に障害を報告するには :

1. 次の電話番号にお電話でご連絡ください。
   - 800.525.0369 (合衆国内) または
   - Sun のいずれかのワールドワイドオフィスに連絡して、組織のためのサポートソリューションを話し合ってください。住所または電話番号の情報については、http://www.oracle.com/us/corporate/index.htm または http://www.oracle.com/us/support/index.html を参照してください。
2. 電話オペレータに障害についてご説明ください。電話オペレータからいくつか質問をさせていただいてから
   - 適切なレベルのサポートに電話をお引き継ぎするか、または
   - 保守担当者を派遣いたします。

お電話の際は、次の情報をお手元にご用意ください。わかっている情報をできるだけたくさん記入してください。

アカウント名			
サイトロケーション番号			
連絡者名			
電話番号			
デバイスモデル番号	❑ **KMA** (アプライアンス) ❑ **OKM マネージャー** (GUI) ❑ SL8500 ライブラリ ❑ SL3000 ライブラリ ❑ SL500 ライブラリ ❑ Oracle Database	❑ 9310 ライブラリ ❑ L700/1400 ライブラリ ❑ SL24 および SL48 ❑ スタンドアロン ❑ ネットワーク / スイッチ	❑ T10000A テープドライブ ❑ T10000B テープドライブ ❑ T10000C テープドライブ ❑ T9840D テープドライブ ❑ HP LTO ドライブ ❑ IBM LTO ドライブ
デバイスアドレス			
IP アドレス			
エラーコード			
障害の緊急度			
障害の説明			

初期構成ワークシート

説明	1 番目の KMA			2 番目の KMA		
	ホスト名	IP アドレス / ネットマスク	DHCP?[1]	ホスト名	IP アドレス / ネットマスク	DHCP?[1]
LAN 0 = 管理			はい ❑ いいえ ❑			はい ❑ いいえ ❑
LAN 1 = ELOM/ILOM			はい ❑ いいえ ❑			はい ❑ いいえ ❑
LAN 2 = サービス			はい ❑ いいえ ❑			はい ❑ いいえ ❑
LAN 3 = 集約済み			はい ❑ いいえ ❑			はい ❑ いいえ ❑
IPv6 アドレス指定の使用	はい ❑ いいえ ❑			はい ❑ いいえ ❑		
KMA 名						
ゲートウェイ						
DNS サーバー	ホスト名 : IP アドレス :			ホスト名 : IP アドレス :		
セキュリティー責任者	ログイン : パスフレーズ			ログイン : パスフレーズ		
ルートアカウントパスフレーズ	ログイン : パスフレーズ			ログイン : パスフレーズ		
ELOM パスフレーズ	ログイン : パスフレーズ			ログイン : パスフレーズ		
鍵分割資格 [2]						
自律ロック解除 [3]						
キーボードタイプ						

1. DHCP を使って割り当てられるアドレスは**静的である必要があります**。このシステムでは、一度割り当てられた IP アドレスを変更する DHCP サーバーには対応できません。

説明	1 番目の KMA			2 番目の KMA		
	ホスト名	IP アドレス / ネットマスク	DHCP?[1]	ホスト名	IP アドレス / ネットマスク	DHCP?[1]
2. 構成 : N の M。M は最小しきい値、N は鍵分割構成のサイズ。鍵分割ユーザー (およびパスフレーズ) を記入してください。						
3. 自律ロック解除では、OKM マネージャーを使って定足数のパスフレーズを入力しなくても、ハードリセットまたはソフトリセット後に KMA は完全な運用状態に入ることができます。これらの情報は書き留めてはいけません。所有する担当者が入力するようにしてください。 これらのエントリは OKM マネージャーで変更できるので、構成中は簡単なものを入力しておいてから、KMA が構成されたあとすぐに OKM GUI を使ってあとで変更することをお勧めします。						

ユーザー役割ワークシート

ユーザー ID	説明	パスフレーズ ** (秘密のパスワード)	役割					
			セキュリティー責任者	コンプライアンス責任者	オペレータ	バックアップオペレータ	監査者	定足数メンバー

注 : 安全上の理由で、パスフレーズはここには記録しないでください。
この欄は、ユーザー ID が入力されると、その ID を持つ人がパスフレーズの入力を求められることのリマインダーとして提供されています。

ドライブワークシート

サイト名：				サイト番号：	
SDP IP アドレス：				ファイルパス名：	場所：
	シリアル番号 / DMOD (最後の 8 桁)	ドライブタイプ	暗号化シリアル番号 (6 つの 16 進文字)	ドライブ IP アドレス	場所
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					

サイト名：		サイト番号：	
SDP IP アドレス：		ファイルパス名：	場所：
20.			

エージェント登録ワークシート

KMA ___ ホスト名 : _____ KMA IP アドレス :					KMA ___ ホスト名: _____ KMA IP アドレス :			
ドライブアドレス		ドライブタイプ	ドライブ IP アドレス	エージェント ID	パスフレーズ	トークン？	永続？	FIPS の設定
1.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
2.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
3.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
4.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
5.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
6.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
7.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
8.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
9.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
10.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
11.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑

KMA ___ ホスト名 : _____ KMA IP アドレス :					KMA ___ ホスト名: _____ KMA IP アドレス :			
12.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
13.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
14.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
15.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
16.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
17.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
18.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
19.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑
20.						はい ❑ いいえ ❑	はい ❑ いいえ ❑	はい ❑ いいえ ❑

用語集

この用語集では、このマニュアルで使用される用語や略語を定義します。

A

AES (Advanced Encryption Standard) FIPS で承認された NIST 暗号化規格。電子データの保護に使用されます。

B

BOT テープの先頭。

F

FIPS Federal Information Processions Standards (連邦情報処理標準) の略。National Institute of Standards and Technology (NIST、米国標準規格局) は、米国商務省の技術管理部内の非規制連邦機関であり、次のような標準規格や技術の開発および促進を行なっています。

- Computer Security Division and Resource Center (CSRC)
- Federal Information Processing Standards (FIPS、連邦情報処理標準)
- 詳細は、次の URL にアクセスしてください。http://www.nist.gov/

G

GUI Graphical User Interface (グラフィカルユーザーインタフェース) の略。

H

Hash Message Authentication Code (HMAC)

暗号化での HMAC (keyed-Hash Message Authentication Code) とは、暗号化ハッシュ関数と秘密鍵を組み合わせて計算される、メッセージ認証コード (Message Authentication Code、MAC) の一種です。

I

Intelligent Platform Management Interface (IPMI)

IPMI では、システム管理者がシステムの健全性の監視やシステムの管理に使用できる、コンピュータシステムに共通の一連のインタフェースを定義します。

IPv6

次の世代では、コロンで区切られた、4 つの 16 進文字の 8 つのグループで表される 128 ビットの値を使用します。
例 : 2001:0db8:85a3:0000:0000:8a2e:0370:7334。

K

Key Management Appliance (KMA)

OKM ソフトウェアがプリインストールされた SunFire X2100-M2、X2200-M2、または X4170-M2 サーバー。Solaris 10 オペレーティングシステムが実装された、実証済みのデュアルコアプロセッサアプライアンスであり、ポリシーベースの鍵管理サービスおよび鍵プロビジョニングサービスを提供します。

Key Management System (KMS)

鍵管理を提供するシステム。StorageTek システムには、暗号化エージェントの代わりに鍵管理を提供するコンポーネントがあります。今は Oracle Key Manager (OKM) と呼ばれます。

L

LTO (Linear Tape-Open)

磁気テープデータ記憶技術のことです。LTO 技術の標準フォームファクタは Ultrium (LTO 技術の「大容量」の実装) と呼ばれます。

LTO Ultrium 技術は、ユーザーが複数のソースの製品およびメディアを使用できる「オープンフォーマット」技術です。また、LTO 技術のオープン性により、さまざまなベンダーから提供されるものの間で互換性の確保が可能になります。

N

NIST National Institute of Standards and Technology (米国標準規格局) の略。

O

OKM クラスタ 相互接続された 1 つ以上の KMA の集合。クラスタ内のすべての KMA は、同一の情報を持ちます。ただし、ある KMA が停止している場合、または新たに作成された情報の一部が OKM クラスタ内のすべての KMA にはまだ伝播されていない場合はこの限りではありません。クラスタ内の任意の KMA で実行された動作は、最終的に OKM クラスタ内のすべての KMA に伝播されます。

P

PKCS RSA セキュリティーによって考案および公開された公開鍵暗号方式の標準規格のグループを指し、暗号化トークンに対する、プラットフォームに依存しない API を定義する PKCS#11 などに含まれます。

R

Rijndael アルゴリズム 米国標準規格局 (NIST) によって Advanced Encryption Standard (AES) 用に選択されたアルゴリズム。「ラインダール」と読むこのアルゴリズムは、Vincent Rijmen と Joan Daemen という 2 人のベルギー人暗号研究者によって考案されたものであり、暗号名にはこの 2 人の姓が反映されています。

RSA 暗号化での **RSA** とは、MIT の Ron Rivest、Adi Shamir、および Leonard Adleman によって考案された公開鍵暗号化アルゴリズムです。**RSA** という略称は、この 3 人の姓の頭文字です。

S

Secure Hash Algorithms (SHA) Secure Hash Algorithms は、米国国家安全保障局 (NSA) によって策定され、NIST によって米国連邦情報処理標準として公開された暗号化ハッシュ関数です。

T

T10000 テープドライブ

T10000 テープドライブは、データの大容量ストレージとして設計された、小型のモジュラー型高性能テープドライブです

T10000A は、最大 500 G バイトの非圧縮データを格納します。

T10000B は、最大 1T バイトの非圧縮データを格納します。

T9840D テープドライブ

T9840D テープドライブは、小型高性能でモジュラー型の、アクセス主体のテープドライブで、平均アクセス時間はちょうど 8 秒です。

このドライブは、ミッドポイントロードテクノロジを用いた独自のデュアルハブカートリッジデザインを使用することで高性能を実現しています。これにより、テープの中央に読み取り / 書き込みヘッドを配置することで、高速アクセスが可能となり、待ち時間が短縮されます。

Transparent Data Encryption (TDE)

データベースコンテンツを暗号化するために Oracle で利用されているテクノロジー。TDE は、列、テーブル、およびテーブル領域レベルで暗号化を提供します。

Transport Layer Security (TLS)

暗号化プロトコルの一種。Web 参照、電子メール、インターネットファックス送信、インスタントメッセージ、その他のデータ転送などを目的として、インターネット上のセキュリティー保護された通信を提供します。

あ

暗号化

データを暗号に変換することです。暗号化は、データの安全性を確保するもっとも有効な方法の一つです。暗号化されたファイルを読み取るには、復号化を可能にする特殊な鍵またはパスワードにアクセスできる必要があります。

暗号化アクセラレータ

暗号化アクセラレータは、データ暗号化 / 復号化の速度を速めるために使用されるハードウェアデバイス (カード) です。これによって、負荷が高い状態のシステムのパフォーマンスが向上します。

暗号化使用可能

デバイス暗号化をオンにでき、暗号化使用可能になっているテープドライブ。

暗号化動作中

暗号化機能がオンになっている暗号化対応テープドライブ。

暗号期間

鍵を暗号化に使用できる期間。鍵が最初にドライブに割り当てられたときに始まります。

暗号方式

情報を保護する技術。暗号化テキストと呼ばれる判読できない形式に情報を変換 (暗号化) します。特別な鍵を所有している人のみが、メッセージを元の形式に暗号化解除 (復号化) できます。

い

インターネットプロトコル (IP)
インターネット環境でデータの発信元から受信先への経路指定に使用されるプロトコル。

インターネットプロトコルアドレス IPv4
デバイスを識別してネットワーク経由でアクセスできるようにする 4 バイトの値。IP アドレスの書式は、ピリオドで区切られた 4 つの数値で表される 32 ビットの数値アドレスです。それぞれの数値は 0 ～ 255 の値を取ります。
たとえば、IP アドレスは 129.80.145.23 のようになります。
「TCP/IP アドレス」としても知られています。

え

エージェント
OKM と情報をやり取りして鍵データを作成および取得するために、さまざまな種類の暗号化エージェントを作成できます。暗号化が有効になっているときの暗号化エージェントの種類として、StorageTek T10000 モデル A と B、T9840D、および HP LTO4 テープドライブがあります。

エージェントライブラリ
エージェントライブラリは、鍵データを OKM (Oracle Key Manager) から取り出すために、エージェントによって使用されます。

お

オペレータ
システムの日常業務の管理を担当するユーザー役割。

か

鍵
ここでは、鍵は対称データ暗号化鍵のことです。エージェントは、1 つ以上のデータユニットに対応するデータの暗号化を行うために、新しい鍵データを要求できます。

鍵は単一の鍵グループに属しているため、その鍵グループに関連付けられているエージェントのみが、対応する鍵にアクセスできます。

鍵には、その鍵が属している鍵グループに関連付けられている鍵ポリシーで規定された、暗号化と復号化の暗号化有効期間があります。鍵のタイプ、つまり鍵の長さとアルゴリズムは、暗号化エージェントによって指定されます。

Key Management System によって生成されるランダムなビット文字列。キーボードを使用して入力するか、または購入します。

鍵グループ　鍵グループは、鍵を整理して鍵ポリシーと関連付けるために使用されます。また、鍵グループは、暗号化エージェントによる鍵データへのアクセスを強制するためにも使用されます。

鍵ポリシー　鍵ポリシーによって、鍵に適用される暗号化有効期間の設定値が提供されます。各鍵グループには鍵ポリシーがあり、鍵ポリシーは 0 個以上の鍵グループに適用できます。ポリシーで指定された暗号化と復号化の暗号化有効期間によって、鍵の使用法が制限され、鍵の無効化、破棄など、鍵のライフサイクルイベントが発生します。

監査者　システム監査証跡 （監査リストイベントや KMA セキュリティーパラメータ）を表示できるユーザー役割。

監査ログ　OKM クラスタは、システムで発生するすべての監査可能イベントのログを保守します。エージェントが、監査可能イベントのために、このログにエントリに提供することがあります。

く

クラスタ　クラスタは、耐障害性、可用性、および拡張性を向上させるために、一連の鍵管理アプライアンスが 1 つのシステムにグループ化されたものです。

こ

コンプライアンス責任者　組織内のデータフローを管理するユーザー役割。データコンテキスト (鍵グループ) と、データをどのように保護して最終的に破棄するかを決定する規則 (鍵ポリシー) を定義して配備できます。

し

証明書　証明書は、所有者の承認と名前を検証するために使用される、デジタル署名されたドキュメントです。

自律ロック解除　自律ロック解除が有効になっているときは、ロックされている KMA をロック解除するには、定足数のセキュリティー責任者が必要です。無効になっているときは、どのセキュリティー責任者でも KMA をロック解除できます。

せ

セキュリティー責任者　セキュリティー設定値、ユーザー、サイト、および転送パートナーを管理するユーザー役割。

セキュリティーポリシー　組織データの機密性、データにアクセスする可能性のある各種実体、およびアクセスの管理と制限に適用される規則を厳密に記述したもの。

設置場所　サイトは、各 OKM および暗号化エージェントの属性であり、ネットワークの場所を示します。暗号化エージェントは、OKM クラスタに接続する場合に、可能なかぎり同じサイト内の KMA との通信を確立しようとします。

ゼロ化　データを回復できないようにデータストレージの内容を変更または削除することによって、電子的に格納されたデータ、暗号化鍵、およびクリティカルセキュリティーパラメータを消去すること。

て

データポリシー　データポリシーには、鍵の暗号化および復号化「暗号期間」など、一連の暗号化関連パラメータを定義します。

データユニット　データユニットは OKM 内部の抽象構成エンティティで、OKM ポリシーや暗号鍵に関連付けられたストレージオブジェクトを表します。テープドライブの場合、データユニットはテープカートリッジです。

に

認証局 (CA)　認証局は、エンドユーザーを登録し、エンドユーザー証明書を発行し、エンド下位の CA を作成できます。Oracle Key Manager では、KMA 自体が認証局として機能し、ユーザー、エージェント、およびほかの KMA に証明書を発行します。

ね

ネットワーク　ソフトウェアおよびハードウェアによるリンクを介してデータ処理デバイスを相互に接続し、情報の交換を容易にするノードと分岐の配置。

は

媒体鍵　テープカートリッジ上の顧客データを暗号化および復号化します。

バックアップオペレータ　データと鍵のセキュリティー保護と保存を担当するユーザー役割。

バックアップ鍵ファイル　バックアップ処理中に生成されるファイル。バックアップファイルの暗号化に使用される鍵が含まれます。このファイルは、システムマスター鍵を使用して暗号化されます。マスター鍵は、定足数の鍵分割資格を使用して、コアセキュリティーバックアップファイルから抽出されます。

バックアップファイル　バックアップ処理中に作成されるファイル。KMA の復元に必要なすべての情報が含まれています。バックアップ専用に生成された鍵を使用して暗号化されます。鍵は、対応するバックアップ鍵ファイルに含まれています。

よ

読み取り鍵　データをテープから読み取る場合に使用される媒体鍵です。

索引

数字

A

B

C

D

E

F

H

I

J

K

L

M

O

P

R

S

T

U

V

W

あ

い

え

お

か

き

く

け

こ

さ

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