# Oracle® VM Server for SPARC 3.2 セキュリティーガイド

Part No: E56429
2015 年 3 月

ORACLE

**ドキュメントのアクセシビリティについて**

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWeb サイト(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc)を参照してください。

**Oracle Supportへのアクセス**

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報は(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info)か、聴覚に障害のあるお客様は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs)を参照してください。

# 目次

# このドキュメントの使用法

- **概要** – Oracle VM Server for SPARC 3.2 ソフトウェアのセキュアな使用についての情報が含まれています。
- **対象読者** – 仮想化された SPARC サーバー上のセキュリティーを管理するシステム管理者
- **必要な知識** – これらのサーバーのシステム管理者は、UNIX® システムおよび Oracle Solaris オペレーティングシステム (Oracle Solaris OS) の実践的な知識を持っている必要があります

## 製品ドキュメントライブラリ

この製品の最新情報や既知の問題は、ドキュメントライブラリ (http://www.oracle.com/pls/topic/lookup?ctx=E56445) に含まれています。

## Oracle サポートへのアクセス

Oracle ユーザーは My Oracle Support から電子サポートにアクセスできます。詳細は、http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info (聴覚に障害をお持ちの場合は http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs) を参照してください。

## フィードバック

このドキュメントに関するフィードバックを http://www.oracle.com/goto/docfeedback からお聞かせください。

♦ ♦ ♦ 第 1 章

# 1 Oracle VM Server for SPARC のセキュリティーの概要

このドキュメントに含まれているセキュリティーの推奨事項の数からは異なる印象を受ける可能性がありますが、標準的な Oracle VM Server for SPARC インストールはすでに、無断使用に対して適切にセキュリティー保護されています。小さな攻撃対象領域が存在するため、攻撃される可能性は低いとしても、ある程度のリスクは残ります。住宅の防犯でドアの施錠などの標準的な抑止装備を補うために盗難警報器を追加することを選択する場合があるのと同様に、追加のネットワークセキュリティー機能が、予期しない問題が発生する確率を下げたり、潜在的な損害を最小限に抑えたりするのに役立つ場合があります。

この章では、Oracle VM Server for SPARC のセキュリティーに関する次のトピックについて説明します。



## Oracle VM Server for SPARC によって使用されるセキュリティー機能

Oracle VM Server for SPARC ソフトウェアは、それぞれに独自の Oracle Solaris 10 または Oracle Solaris 11 OS がインストールされた複数の Oracle Solaris 仮想マシン (VM) を 1 つの物理システム上で実行できるようにする仮想化製品です。各 VM は*論理ドメイン*とも呼ばれます。ドメインは独立したインスタンスであり、Oracle Solaris OS の各種バージョンおよび各種のアプリケーションソフトウェアを実行できます。たとえば、複数の異なるパッケージ

リビジョンをドメインにインストールしたり、複数の異なるサービスをドメインで有効にしたり、パスワードが異なる複数のシステムアカウントをドメインに作成したりできます。Oracle Solaris のセキュリティーについては、『Oracle Solaris 10 Security Guidelines 』および『Oracle Solaris 11 Security Guidelines 』を参照してください。

`ldm` コマンドは Logical Domains Manager を呼び出すため、ドメインを構成したり、状態情報を取得したりするには、制御ドメイン上でこのコマンドを実行する必要があります。制御ドメインおよび `ldm` コマンドへのアクセスを制限することは、システムで実行されているドメインのセキュリティーにとって重要です。ドメイン構成データへのアクセスを制限するには、コンソールや `solaris.ldoms` 承認に対する Oracle Solaris 権利などの、Oracle VM Server for SPARC のセキュリティー機能を使用します。『Oracle VM Server for SPARC 3.2 管理ガイド 』の「Logical Domains Manager プロファイルの内容」を参照してください。

Oracle VM Server for SPARC ソフトウェアは次のセキュリティー機能を使用します。

- Oracle Solaris 10 OS および Oracle Solaris 11 OS で利用できるセキュリティー機能は、Oracle VM Server for SPARC ソフトウェアを実行するドメインでも利用できます。『Oracle Solaris 10 Security Guidelines 』および『Oracle Solaris 11 Security Guidelines 』を参照してください。
- Oracle Solaris OS のセキュリティー機能は Oracle VM Server for SPARC ソフトウェアに適用できます。Oracle VM Server for SPARC のセキュリティーの確保の詳細は、16 ページの「仮想化環境内のセキュリティー」および 18 ページの「攻撃に対する防御」を参照してください。
- Oracle Solaris 10 OS および Oracle Solaris 11 OS には、システムに適用可能なセキュリティー修正が含まれています。Oracle Solaris 10 OS の修正はセキュリティーパッチまたはアップデートとして入手します。Oracle Solaris 11 OS の修正は SRU (Support Repository Update) として入手します。
- Oracle VM Server for SPARC 管理コマンドおよびドメインコンソールへのアクセスを制限する方法や、Oracle VM Server for SPARC の監査機能を有効にする方法については、『Oracle VM Server for SPARC 3.2 管理ガイド 』の第 2 章「Oracle VM Server for SPARC のセキュリティー」を参照してください。

# Oracle VM Server for SPARC 製品の概要

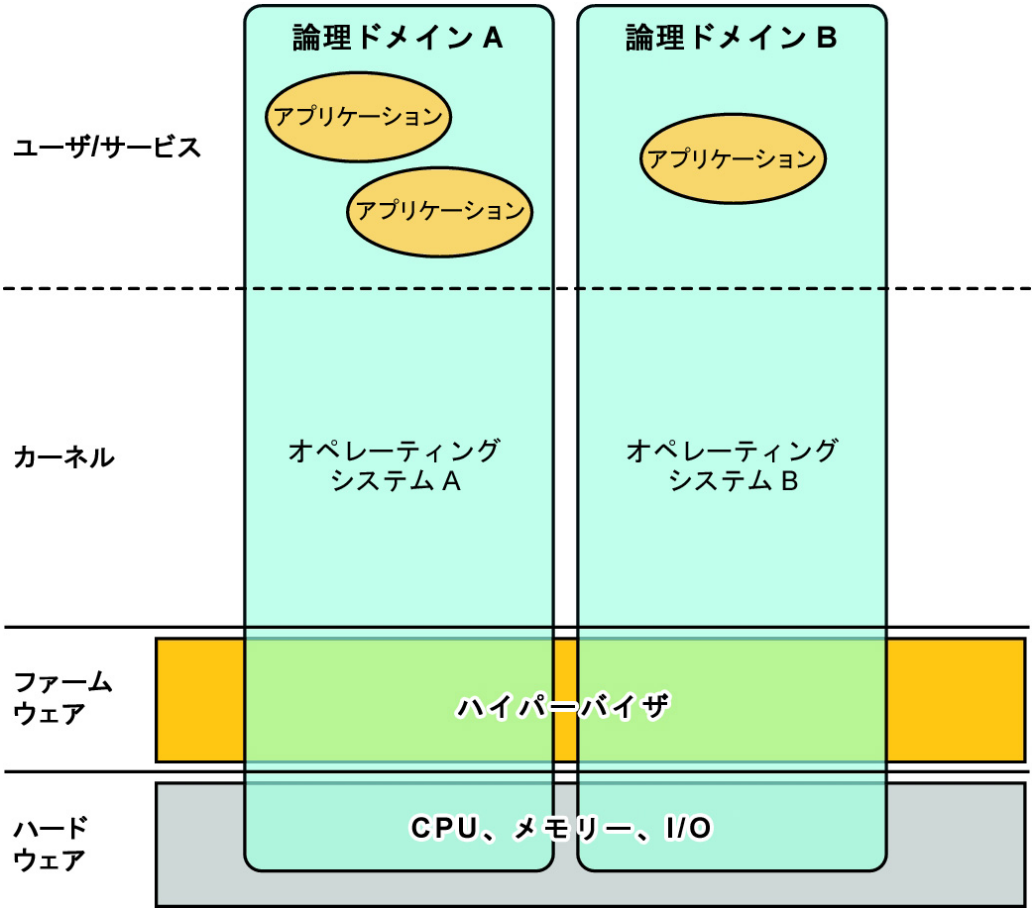
Oracle VM Server for SPARC は、Oracle の SPARC T シリーズサーバーや SPARC M5 サーバーおよび Fujitsu M10 サーバーに高い効率性とエンタープライズクラスの仮想化機能を提供します。Oracle VM Server for SPARC ソフトウェアを使用すると、多数の仮想サーバー

(論理ドメインと呼ばれる) を単一のシステム上に作成できます。こうした構成により、これらの SPARC サーバーおよび Oracle Solaris OS が提供する大規模なスレッドを活用できるようになります。

*論理ドメイン*は、個別に論理グループ化されたリソースを含む仮想マシンです。論理ドメインは、単一のコンピュータシステム内で独自のオペレーティングシステムおよび ID を持っています。各論理ドメインは、サーバーの電源の再投入を実行する必要なしに、作成、削除、再構成、およびリブートを単独で行うことができます。異なる論理ドメインでさまざまなアプリケーションソフトウェアを実行でき、パフォーマンスおよび安全性の目的から、これらを独立した状態にしておくことができます。

Oracle VM Server for SPARC ソフトウェアの使用については、『Oracle VM Server for SPARC 3.2 管理ガイド 』および『Oracle VM Server for SPARC 3.2 リファレンスマニュアル 』を参照してください。必要なハードウェアおよびソフトウェアについては、『Oracle VM Server for SPARC 3.2 インストールガイド 』を参照してください。

図 1-1　2 つの論理ドメインをサポートするハイパーバイザ




Oracle VM Server for SPARC ソフトウェアは次のコンポーネントを使用してシステム仮想化を提供します。

- **ハイパーバイザ。**ハイパーバイザは小規模なファームウェアレイヤーであり、オペレーティングシステムのインストール先とすることができる、安定した仮想化マシンアーキテクチャーを提供します。ハイパーバイザを使用する Oracle Sun サーバーでは、論理ドメイン上のオペレーティングシステムの動作をハイパーバイザが制御できるようにするためのハードウェア機能が用意されています。

  特定の SPARC ハイパーバイザがサポートするドメインの数と各ドメインの機能は、サーバーによって異なります。ハイパーバイザは、サーバー全体の CPU、メモリー、および I/O リソース

のサブセットを特定の論理ドメインに割り当てることができます。この割り当てにより、それぞれが独自の論理ドメイン内にある複数のオペレーティングシステムを同時にサポートできます。別個の論理ドメインの間で、任意の粒度でリソースを再配置できます。たとえば、CPU は CPU スレッド単位で論理ドメインに割り当てることができます。

*サービスプロセッサ* (SP) は、*システムコントローラ* (SC) とも呼ばれ、物理マシンをモニターおよび実行します。SP ではなく、Logical Domains Manager が論理ドメイン自体を管理します。

- **制御ドメイン。**Logical Domains Manager がこのドメインで動作することにより、ほかの論理ドメインを作成および管理したり、仮想リソースをほかのドメインに割り当てたりできるようになります。制御ドメインは、サーバーごとに 1 つだけ存在できます。制御ドメインは、Oracle VM Server for SPARC ソフトウェアをインストールするときに最初に作成されるドメインです。制御ドメインの名前は `primary` です。
- **サービスドメイン。**サービスドメインは、仮想スイッチ、仮想コンソール端末集配信装置、仮想ディスクサーバーなどの仮想デバイスサービスをほかのドメインに提供します。どのドメインも、サービスドメインとして構成できます。
- **I/O ドメイン。**I/O ドメインは、PCI EXPRESS (PCIe) コントローラ内のネットワークカードなどの物理 I/O デバイスに直接アクセスできます。I/O ドメインは PCIe ルートコンプレックスを所有するか、直接 I/O (DIO) 機能を使用して PCIe スロットまたはオンボードの PCIe デバイスを所有することができます。『Oracle VM Server for SPARC 3.2 管理ガイド 』の「Creating an I/O Domain by Assigning PCIe Endpoint Devices」を参照してください。

  I/O ドメインは、I/O ドメインがサービスドメインとしても使用される場合に、仮想デバイスの形式でほかのドメインと物理 I/O デバイスを共有できます。
- **ルートドメイン。**ルートドメインには PCIe ルートコンプレックスが割り当てられます。このドメインは、そのルートコンプレックスの PCIe ファブリックを所有し、ファブリックのエラー処理などのファブリック関連のサービスをすべて提供します。ルートドメインは I/O ドメインでもあり、物理 I/O デバイスを所有し、それらに直接アクセスできます。

  保持できるルートドメインの数は、プラットフォームアーキテクチャーによって決まります。たとえば、Oracle の SPARC T4-4 サーバーを使用している場合は、最大 4 つのルートドメインを保持できます。
- **ゲストドメイン。**ゲストドメインは非 I/O ドメインであり、1 つ以上のサービスドメインによって提供される仮想デバイスサービスを利用します。ゲストドメインには物理 I/O デバイスが存在しません。仮想ディスクや仮想ネットワークインタフェースなどの仮想 I/O デバイスのみが存在します。

多くの場合、Oracle VM Server for SPARC システムに存在するただ 1 つの制御ドメインが、I/O ドメインやサービスドメインによって実行されるサービスを提供します。冗長性とプラットフォーム保守性を向上させるには、Oracle VM Server for SPARC システム上で複数の I/O ドメインを構成することを検討してください。

# Oracle VM Server for SPARC に適用される一般的なセキュリティー原則

ゲストドメインをさまざまな方法で構成し、ゲストドメインの独立性、ハードウェア共有、およびドメインの接続性をさまざまなレベルで提供できます。これらの要因は、全体的な Oracle VM Server for SPARC 構成のセキュリティーレベルに寄与します。Oracle VM Server for SPARC ソフトウェアをセキュアな方法で配備する方法に関する推奨事項については、16 ページの「仮想化環境内のセキュリティー」および 18 ページの「攻撃に対する防御」を参照してください。

次の一般的なセキュリティー原則のいくつかを適用できます。

- **攻撃対象領域を最小化する。**
  - システムのセキュリティーを定期的に評価できるようにする運用ガイドラインを作成することによって、意図しない構成エラーを最小限に抑えます。21 ページの「対応策: 運用ガイドラインの作成」を参照してください。
  - ドメインの独立性を最大化するために、仮想環境のアーキテクチャーを慎重に計画します。21 ページの「脅威: 仮想環境のアーキテクチャー内のエラー」で説明されている対応策を参照してください。
  - どのリソースを割り当てるか、またリソースを共有するかどうかを慎重に計画します。24 ページの「対応策: ハードウェアリソースを慎重に割り当てる」および 25 ページの「対応策: 共有リソースを慎重に割り当てる」を参照してください。
  - 26 ページの「脅威: 実行環境の操作」および 40 ページの「対応策: ゲストドメインの OS をセキュリティー保護する」で説明されている対応策を適用することによって、論理ドメインが操作から確実に保護されるようにします。
    - 26 ページの「対応策: 対話型アクセスパスのセキュリティー保護」。
    - 27 ページの「対応策: Oracle Solaris OS を最小化する」。
    - 27 ページの「対応策: Oracle Solaris OS を強化する」。
    - 33 ページの「対応策: Logical Domains Manager を強化する」。

    - 27 ページの「対応策: 役割の分離とアプリケーションの分離を使用する」では、さまざまなドメインに機能の役割を割り当てること、および制御ドメインで、ゲストドメインをホストするために必要なインフラストラクチャーを提供するソフトウェアが実行されるようにすることの重要性について説明します。この目的のために設計された、ゲストドメイン上のほかのシステムで実行できるアプリケーションを実行するようにしてください。
    - 27 ページの「対応策: 専用の管理ネットワークを構成する」では、SP をネットワークアクセスから遮蔽するために SP を含むサーバーを専用の管理ネットワークに接続する、より高度なネットワーク構成について説明します。
- 必要なときに*のみ*ゲストドメインをネットワークに公開します。仮想スイッチを使用して、ゲストドメインのネットワーク接続を適切なネットワーク*のみ*に制限できます。
- 『Oracle Solaris 10 Security Guidelines 』および『Oracle Solaris 11 Security Guidelines 』で説明されている、攻撃対象領域を最小化するための Oracle Solaris 10 および Oracle Solaris 11 向けの手順を実行します。
- 31 ページの「対応策: ファームウェアとソフトウェアの署名を検証する」および 31 ページの「対応策: カーネルモジュールを検証する」で説明されているように、ハイパーバイザのコアを保護します。
- 制御ドメインをサービス拒否攻撃から保護します。32 ページの「対応策: コンソールアクセスをセキュリティー保護する」を参照してください。
- 承認されていないユーザーが Logical Domains Manager を実行できないようにします。33 ページの「脅威: 構成ユーティリティーの無断使用」を参照してください。
- 承認されていないユーザーまたはプロセスがサービスドメインにアクセスできないようにします。36 ページの「脅威: サービスドメインの操作」を参照してください。
- I/O ドメインまたはサービスドメインをサービス拒否攻撃から保護します。38 ページの「脅威: I/O ドメインまたはサービスドメインのサービス拒否の発生」を参照してください。
- 承認されていないユーザーまたはプロセスが I/O ドメインにアクセスできないようにします。39 ページの「脅威: I/O ドメインの操作」を参照してください。
- 不必要なドメインマネージャーサービスを無効化します。Logical Domains Manager は、ドメインのアクセス、モニタリング、および移行のためのネットワークサービスを提供します。33 ページの「対応策: Logical Domains Manager を強化する」および 29 ページの「対応策: ILOM をセキュリティー保護する」を参照してください。
- **操作を実行するための最小限の権限を付与します。**

- 同じセキュリティー要件と権限を共有する個別のゲストシステムのグループである*セキュリティークラス*にシステムを分離します。単一のセキュリティークラスに属するゲストドメインのみを単一のハードウェアプラットフォームに割り当てることによって、分離バリアを作成し、ドメインの範囲が別のセキュリティークラスに及ばないようにします。22 ページの「対応策: ゲストをハードウェアプラットフォームに慎重に割り当てる」を参照してください。
- 権利を使用して、`ldm` コマンドでドメインを管理する機能を制限します。ドメインを管理する必要があるユーザー*のみ*にこの機能を付与するようにしてください。すべての `ldm` サブコマンドにアクセスする必要がするユーザーには、LDoms Management 権利プロファイルを使用する役割を割り当てます。リスト関連の `ldm` サブコマンドのみにアクセスする必要があるユーザーには、LDoms Review 権利プロファイルを使用する役割を割り当てます。『Oracle VM Server for SPARC 3.2 管理ガイド 』の「権利プロファイルと役割の使用」を参照してください。
- 権利を使用して、アクセスを Oracle VM Server for SPARC の管理者が管理するドメインのコンソール*のみ*に制限します。すべてのドメインに対する汎用アクセスを許可*しないでください*。『Oracle VM Server for SPARC 3.2 管理ガイド 』の「権利の使用によるドメインコンソールへのアクセスの制御」を参照してください。

- **システムアクティビティーをモニターします。**

  Oracle VM Server for SPARC の監査を有効にします。『Oracle VM Server for SPARC 3.2 管理ガイド 』の「監査の有効化と使用」を参照してください。

# 仮想化環境内のセキュリティー

Oracle VM Server for SPARC 仮想化環境を効果的にセキュリティー保護するには、オペレーティングシステムと、各ドメイン内で実行される各サービスをセキュリティー保護します。侵害が成功した場合の影響を軽減するには、各サービスを異なるドメインに配備することによって分離します。

Oracle VM Server for SPARC 環境では、ハイパーバイザを使用して、論理ドメインの CPU、メモリー、および I/O リソースを仮想化します。各ドメインは、潜在的な攻撃に対してセキュリティー保護する必要のある、個別の仮想化されたサーバーです。

仮想化環境では、ハードウェアリソースの共有を使用して複数のサーバーを 1 つのサーバーに統合できます。Oracle VM Server for SPARC では、CPU およびメモリーリソースは各ドメインに排他的に割り当てられるため、過剰な CPU 使用またはメモリー割り当てによる悪用が回避

されます。ディスクおよびネットワークリソースは通常、サービスドメインによって多数のゲストドメインに提供されます。

セキュリティーを評価する場合は、*常に*、環境には攻撃者が悪用できる欠陥が存在することを前提にしてください。たとえば、ゲストドメインを含むシステム全体をハイジャックするために、攻撃者がハイパーバイザ内の弱点を悪用する可能性があります。そのため、*常に*、侵害が発生した場合の損害のリスクを最小限に抑えるようにシステムを配備してください。

## 実行環境

実行環境には、次のコンポーネントが含まれています。

- **ハイパーバイザ** – ハードウェアを仮想化し、CPU に組み込まれているハードウェアサポートに大きく依存するプラットフォーム固有のファームウェア。
- **制御ドメイン** – ハイパーバイザを構成し、論理ドメインを管理する Logical Domains Manager を実行する特殊なドメイン。
- **I/O ドメインまたはルートドメイン** – プラットフォームの使用可能な I/O デバイスの一部またはすべてを所有し、それらをほかのドメインと共有するドメイン。
- **サービスドメイン** – ほかのドメインにサービスを提供するドメイン。サービスドメインは、ほかのドメインにコンソールアクセスを提供するか、または仮想ディスクを提供する可能性があります。ほかのドメインに仮想ディスクアクセスを提供するサービスドメインはまた、I/O ドメインでもあります。

これらのコンポーネントの詳細は、図1-1「2 つの論理ドメインをサポートするハイパーバイザ」およびより詳細なコンポーネントの説明を参照してください。

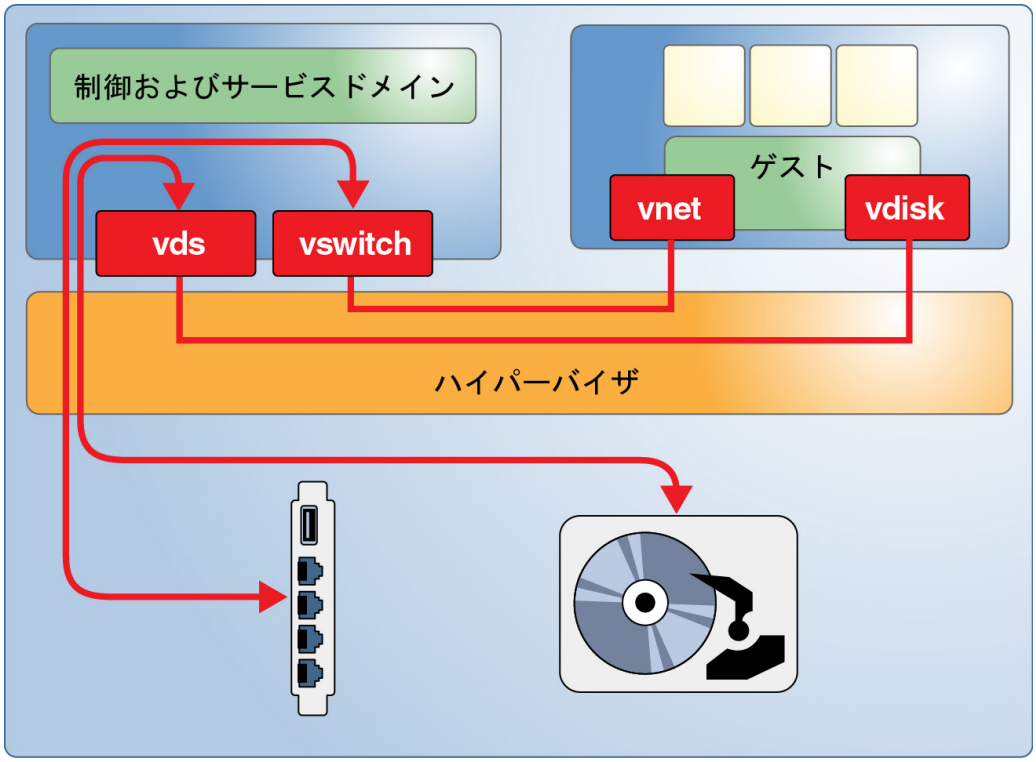
2 番目の I/O ドメインを構成することによって、冗長な I/O 構成での保守性を向上させることができます。また、2 番目の I/O ドメインを使用して、ハードウェアをセキュリティー侵害から分離することもできます。構成オプションについては、『Oracle VM Server for SPARC 3.2 管理ガイド 』を参照してください。

## 実行環境のセキュリティー保護

Oracle VM Server for SPARC の実行環境内には攻撃のターゲットがいくつか存在します。図1-2「Oracle VM Server for SPARC 環境のサンプル」は、制御ドメインがゲストドメインにネットワークおよびディスクサービスを提供する、単純な Oracle VM Server for SPARC

構成を示しています。これらのサービスは、制御ドメイン内で実行されるデーモンおよびカーネルモジュールを使用して実装されます。Logical Domains Manager は、サービスとクライアントの間のポイントツーポイント通信を促進するために、各サービスとクライアントに論理ドメインチャンネル (LDC) を割り当てます。攻撃者は、ゲストドメインの分離を破壊するために、いずれかのコンポーネントに含まれるエラーを悪用する可能性があります。たとえば、攻撃者がサービスドメイン内で任意のコードを実行したり、プラットフォーム上の通常の動作を妨害したりする可能性があります。

**図 1-2** Oracle VM Server for SPARC 環境のサンプル

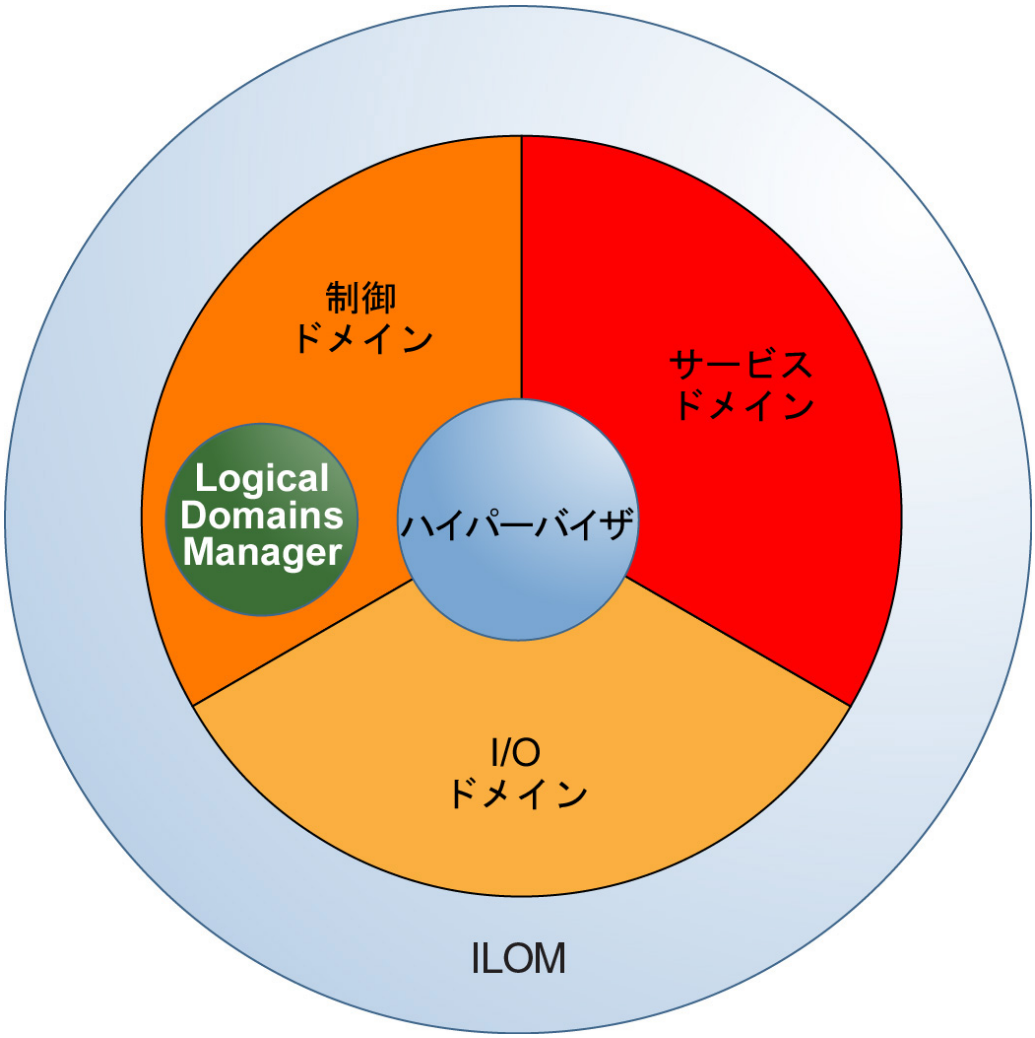



## 攻撃に対する防御

次の図は、Oracle VM Server for SPARC の「実行環境」を形成する仮想化コンポーネントを示しています。これらのコンポーネントは、厳密には分離されていません。もっとも単純な構成

では、これらのすべての機能を単一のドメインに結合します。また、制御ドメインが、ほかのドメインに対する I/O ドメインおよびサービスドメインとして機能することもあります。

**図 1-3** 実行環境のコンポーネント




攻撃者が、システムの分離を破壊してから、ハイパーバイザまたは実行環境の別のコンポーネントを操作してゲストドメインに到達しようとしているとします。すべてのスタンドアロンサーバーと同様に、各ゲストドメインを保護する必要があります。

この章の残りでは、脅威の可能性と、それらに対応するために実行できる各種の対策について説明します。これらの各攻撃は、単一のプラットフォーム上で実行される異なるドメインの分離を打開または解消しようとします。以降のセクションでは、Oracle VM Server for SPARC システムの各部分に対する脅威について説明します。



# 運用環境

運用環境には、物理システムとそのコンポーネント、データセンター設計者、管理者、および IT 組織のメンバーが含まれます。セキュリティー侵害は、運用環境内のどこでも発生する可能性があります。

仮想化では、実際のハードウェアと、本番サービスを実行するゲストドメインの間にソフトウェアのレイヤーが設定されるため、複雑さが増します。そのため、仮想システムを慎重に計画および構成するとともに、人為的ミスに注意する必要があります。また、「ソーシャルエンジニアリング」を使用して運用環境へのアクセスを取得するしようとする攻撃者の試みにも注意してください。

以降のセクションでは、運用環境のレベルで対応できる特徴的な脅威について説明します。

## 脅威: 意図しない構成ミス

仮想化環境での主なセキュリティー上の問題は、ネットワークセグメントを分離し、管理アクセスを分離し、さらにサーバーを同じセキュリティー要件と権限を持つドメインのグループであるセキュリティークラスに配備することによって、サーバーの分離を維持することです。

仮想リソースを慎重に構成し、次のようなエラーを回避します。

- 本番ゲストドメインと実行環境の間に不要な通信チャネルを作成する
- ネットワークセグメントへの不要なアクセスを作成する

- 個別のセキュリティークラス間に意図しない接続を作成する
- ゲストドメインを間違ったセキュリティークラスに誤って移行する
- 不十分なハードウェアを割り当てる (予期しないリソースの過負荷を招く可能性がある)
- ディスクまたは I/O デバイスを間違ったドメインに割り当てる

### 対応策: 運用ガイドラインの作成

開始する前に、Oracle VM Server for SPARC 環境の運用ガイドラインを慎重に定義します。これらのガイドラインでは、実行する次のタスクと、それらの実行方法について説明します。

- 環境のすべてのコンポーネントに対するパッチの管理
- 変更の適切に定義され、トレース可能でセキュアな実装の有効化
- 一定間隔でのログファイルのチェック
- 環境の整合性と可用性のモニタリング

チェックを定期的に実行して、これらのガイドラインが最新で、適切な状態に維持されるようにするとともに、日常の運用でこれらのガイドラインに従っていることを確認します。

これらのガイドラインに加えて、意図しないアクションのリスクを軽減するためのいくつかのより技術的な対策を実行できます。32 ページの「Logical Domains Manager」を参照してください。

## 脅威: 仮想環境のアーキテクチャー内のエラー

物理システムを仮想化環境に移行する場合は通常、元の LUN を再利用することによって、ストレージ構成を現状のままに維持できます。ただし、ネットワーク構成は仮想化環境に適応させる必要があるため、結果として得られるアーキテクチャーが物理システム上で使用されているアーキテクチャーと大幅に異なる可能性があります。

個別のセキュリティークラスの分離を維持する方法や、それらのセキュリティークラスのニーズを検討する必要があります。また、プラットフォームの共有ハードウェア、およびネットワークスイッチや SAN スイッチなどの共有コンポーネントも検討してください。

環境のセキュリティーを最大化するために、ゲストドメインとセキュリティークラスの分離を確実に維持するようにしてください。アーキテクチャーを設計する場合は、可能性のあるエラーや攻撃を予測し、防御線を実装します。適切な設計は、複雑さやコストを管理しながら、潜在的なセキュリティーの問題を制限するのに役立ちます。

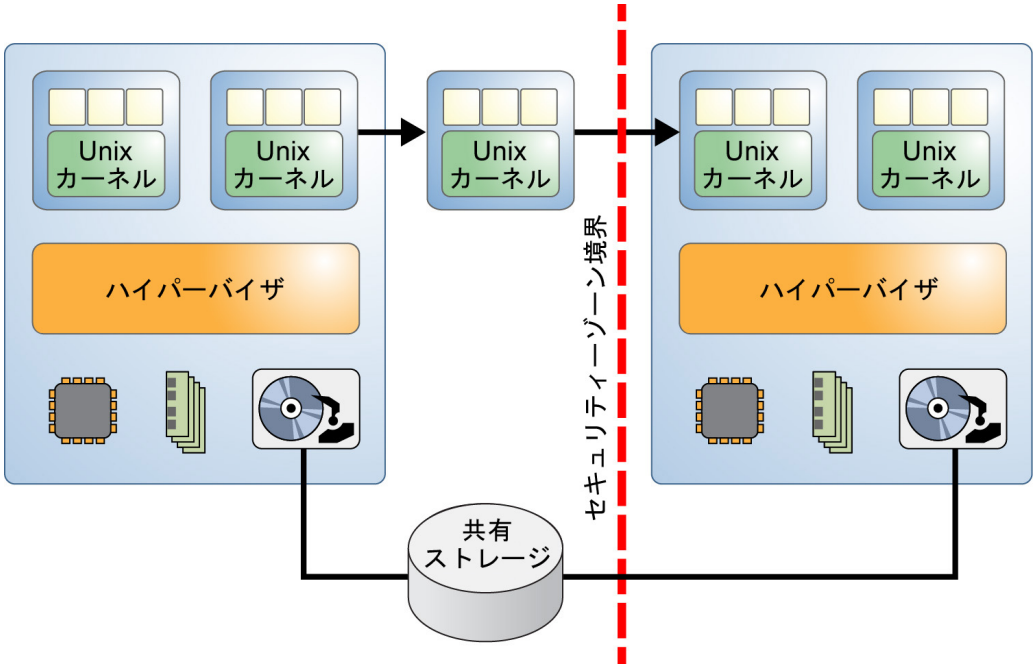
### 対応策: ゲストをハードウェアプラットフォームに慎重に割り当てる

同じセキュリティー要件と権限を持つドメインのグループであるセキュリティークラスを使用して、個々のドメインを互いに分離します。同じセキュリティークラスに属するゲストドメインを特定のハードウェアプラットフォームに割り当てることによって、分離の侵害が発生した場合でも、攻撃が別のセキュリティークラスに及ばないようにします。

### 対応策: Oracle VM Server for SPARC ドメインの移行を計画する

ライブドメイン移行機能には、次の図に示すように、ゲストドメインが別のセキュリティークラスに割り当てられたプラットフォームに誤って移行された場合、分離が破壊される可能性があります。そのため、セキュリティークラスの境界をまたがる移行が許可されることがないように、ゲストドメインの移行を慎重に計画してください。

**図 1-4** セキュリティーの境界をまたがるドメイン移行




移行操作によって発生するセキュリティーの脆弱性を最小化または解消するには、`ldmd` で生成されたホスト証明書を手動で交換し、ソースマシンとターゲットマシンの各ペア間の帯域外

にインストールする必要があります。SSL 証明書を設定する方法については、『Oracle VM Server for SPARC 3.2 管理ガイド 』の「移行のための SSL 証明書の構成」を参照してください。

### 対応策: 仮想接続を正しく構成する

すべての仮想ネットワーク接続を追跡できなくなると、ドメインがネットワークセグメントへの誤ったアクセスを取得する可能性があります。たとえば、このようなアクセスは、ファイアウォールまたはセキュリティークラスを迂回する可能性があります。

実装エラーのリスクを軽減するには、環境内のすべての仮想および物理接続を慎重に計画し、ドキュメント化します。シンプルで管理しやすいように、ドメイン接続計画を最適化します。本番に移行する前に、計画を明確にドキュメント化し、計画に対する実装の正確性を検証してください。仮想環境が本番に移行したあとであっても、一定間隔で実装を計画に対して検証してください。

### 対応策: VLAN タグ付けを使用する

VLAN タグ付けを使用すると、複数の Ethernet セグメントを単一の物理ネットワークに統合できます。この機能はまた、仮想スイッチにも使用できます。仮想スイッチの実装でのソフトウェアエラーに関連したリスクを軽減するには、物理 NIC および VLAN ごとに 1 つの仮想スイッチを構成します。Ethernet ドライバ内のエラーからさらに保護するには、タグ付き VLAN の使用を控えます。ただし、このタグ付き VLAN の脆弱性はよく知られているため、このようなエラーが発生する確率は低いです。Oracle VM Server for SPARC ソフトウェアがインストールされた Oracle の Sun SPARC T シリーズプラットフォーム上の侵入テストでは、この脆弱性は示されていません。

### 対応策: 仮想セキュリティーアプライアンスを使用する

パケットフィルタやファイアウォールなどのセキュリティーアプライアンスは分離のための機器であり、セキュリティークラスの分離を保護します。これらのアプライアンスは、ほかのすべてのゲストドメインと同じ脅威にさらされるため、これを使用しても分離の侵害からの完全な保護は保証されません。そのため、このようなサービスを仮想化することを決定する前に、リスクとセキュリティーのすべての側面を慎重に検討してください。

## 脅威: リソース共有の副作用

仮想化環境内のリソース共有が、別のコンポーネント (別のドメインなど) に悪影響を与えるまでリソースを過負荷状態にする、サービス拒否 (DoS) 攻撃につながる可能性があります。

Oracle VM Server for SPARC 環境では、DoS 攻撃によって影響を受ける可能性のあるリソースは一部だけです。CPU およびメモリーリソースは各ゲストドメインに排他的に割り当てられるため、ほとんどの DoS 攻撃が回避されます。これらのリソースの排他的な割り当てによってさえ、次のようにゲストドメインの速度が低下することがあります。

- ストランド間で共有され、2 つのゲストドメインに割り当てられているキャッシュ領域のスラッシング
- メモリー帯域幅の過負荷

CPU およびメモリーリソースとは異なり、ディスクおよびネットワークサービスは通常、ゲストドメイン間で共有されます。これらのサービスは、1 つ以上のサービスドメインによってゲストドメインに提供されます。これらのリソースのゲストドメインへの割り当ておよび配分方法を慎重に検討してください。最大のパフォーマンスとリソース使用率を可能にする構成はすべて、同時に副作用のリスクも最小限に抑えることに留意してください。

### 評価: 共有リソースによる副作用

ドメインに排他的に割り当てられているか、またはドメイン間で共有されているかにかかわらず、ネットワークリンクが飽和したり、ディスクが過負荷状態になったりする場合があります。このような攻撃は、その攻撃の間、サービスの可用性に影響を与えます。攻撃のターゲットが危険にさらされることはなく、データが失われることもありません。この脅威の影響を最小限に抑えることは簡単ですが、Oracle VM Server for SPARC 上のネットワークおよびディスクリソースに制限されるとしても、この脅威に注意するようにしてください。

### 対応策: ハードウェアリソースを慎重に割り当てる

ゲストドメインには、必要なハードウェアリソースのみを割り当てるようにしてください。未使用のリソースは、そのリソースが必要なくなったら必ず割り当てを解除してください。たとえば、インストール中にのみ必要なネットワークポートまたは DVD ドライブがあります。これを実践することによって、攻撃者にとって可能性のあるエントリポイントの数が最小限に抑えられます。

### 対応策: 共有リソースを慎重に割り当てる

物理ネットワークポートなどの共有ハードウェアリソースは、DoS 攻撃にとって可能性のあるターゲットになります。DoS 攻撃の影響をゲストドメインの単一のグループに制限するには、どのゲストドメインがどのハードウェアリソースを共有するかを慎重に決定してください。

たとえば、ハードウェアリソースを共有するゲストドメインを、同じ可用性またはセキュリティー要件でグループ化することもできます。グループ化にかかわらず、異なる種類のリソース制御を適用できます。

ディスクおよびネットワークリソースを共有する方法を検討する必要があります。専用の物理アクセスパスまたは専用の仮想ディスクサービスを通してディスクアクセスを分離することによって、問題を軽減できます。

### サマリー: 共有リソースによる副作用

このセクションで説明されているすべての対応策では、配備の技術的な詳細と、そのセキュリティーへの影響を理解する必要があります。アーキテクチャーを慎重に計画し、適切にドキュメント化し、さらにできるだけシンプルに維持してください。Oracle VM Server for SPARC ソフトウェアのセキュアな配備を準備できるように、仮想化されたハードウェアの影響を理解するようにしてください。

CPU やメモリーの共有は実際にはほとんど発生しませんが、論理ドメインはそれらの共有の影響に対して堅牢です。それにもかかわらず、ゲストドメイン内での Solaris リソース管理などのリソース制御を適用することが最善です。これらの制御を使用すると、仮想環境と仮想化されていない環境のどちらでも、不正なアプリケーション動作から保護されます。

## 実行環境

図1-3「実行環境のコンポーネント」は、実行環境のコンポーネントを示しています。各コンポーネントは、本番ゲストドメインを実行するためのプラットフォーム全体をともに形成する特定のサービスを提供します。これらのコンポーネントの正しい構成は、システムの整合性にとってきわめて重要です。

すべての実行環境コンポーネントが、攻撃者にとっての潜在的なターゲットになります。このセクションでは、実行環境内の各コンポーネントに影響を与える可能性のある脅威について説明します。一部の脅威や対応策は、複数のコンポーネントに適用される可能性があります。

## 脅威: 実行環境の操作

実行環境を操作することによって、さまざまな方法で制御を取得できます。たとえば、操作されたファームウェアを ILOM 内にインストールして、I/O ドメイン内からすべてのゲストドメイン I/O に対してスヌーピングすることができます。このような攻撃では、システムの構成にアクセスして変更できます。Oracle VM Server for SPARC 制御ドメインの制御を取得した攻撃者は、システムを任意の方法で再構成でき、I/O ドメインの制御を取得した攻撃者は、ブートディスクなどの接続されたストレージに変更を加えることができます。

### 評価: 実行環境の操作

ILOM または実行環境内のいずれかのドメインへの侵入に成功した攻撃者は、そのドメインから使用できるすべてのデータを読み取り、操作できます。このアクセスはネットワーク経由で、または仮想化スタック内のエラーを使用して取得される可能性があります。通常、ILOM やドメインを直接攻撃することはできないため、このような攻撃は実行するのが困難です。

実行環境の操作から保護するための対応策は標準のセキュリティー対策であり、すべてのシステム上で実装するようにしてください。標準のセキュリティー対策によって、侵入や操作のリスクをさらに軽減するための保護のレイヤーが実行環境の周りに追加されます。

### 対応策: 対話型アクセスパスのセキュリティー保護

システム上で実行されるアプリケーションに必要なアカウント*のみ*を作成するようにしてください。

管理に必要なアカウントが、鍵ベースの認証と強力なパスワードのどちらかを使用してセキュリティー保護されていることを確認してください。これらの鍵またはパスワードを異なるドメイン間で共有してはいけません。また、特定のアクションを実行するためのツーファクタ認証または「ツーパーソンルール」の実装も検討してください。

システム上で実行されるコマンドの完全なトレーサビリティーと説明責任を確保するために、`root` などのアカウントに匿名ログインを使用*しないでください*。代わりに、権利を使用して個々の管理者に対し、その管理者が実行することを許可されている機能へのアクセス*のみ*を許可します。管理ネットワークアクセスで常に SSH などの暗号化が使用されること、および管理者のワークステーションが高セキュリティーシステムとして扱われることを確認してください。

### 対応策: Oracle Solaris OS を最小化する

システム上にインストールされているどのソフトウェアも危険にさらされる可能性があるため、侵害の機会を最小化するために、必要なソフトウェア*のみ*をインストールするようにしてください。

### 対応策: Oracle Solaris OS を強化する

最小化された Oracle Solaris OS のインストールに加えて、ソフトウェアを攻撃に対して「強化する」ためのソフトウェアパッケージを構成します。まず、SSH を除くすべてのネットワークサービスを事実上無効にするために、限られたネットワークサービスを実行します。このポリシーは、Oracle Solaris 11 システム上のデフォルトの動作です。Oracle Solaris OS をセキュリティー保護する方法については、『Oracle Solaris 10 Security Guidelines 』および『Oracle Solaris 11 Security Guidelines 』を参照してください。

### 対応策: 役割の分離とアプリケーションの分離を使用する

本番アプリケーションは、必然的にほかのシステムに接続されるため、外部の攻撃によりさらされやすくなります。本番アプリケーションを、実行環境の一部であるドメインには配備*しないでください*。代わりに、それ以上の権限を持たないゲストドメインに*のみ*配備するようにしてください。

実行環境は、これらのゲストドメインに必要なインフラストラクチャーのみを提供するべきです。実行環境を本番アプリケーションから分離すると、管理権限における粒度を実装できます。本番ゲストドメインの管理者には実行環境へのアクセスは必要なく、実行環境の管理者には本番ゲストドメインへのアクセスは必要ありません。可能な場合は、ドメインごとに実行環境の異なる役割 (制御ドメインや I/O ドメインなど) を割り当てます。このタイプの構成によって、これらのドメインのいずれかが危険にさらされた場合に実行できる損害の量が削減されます。

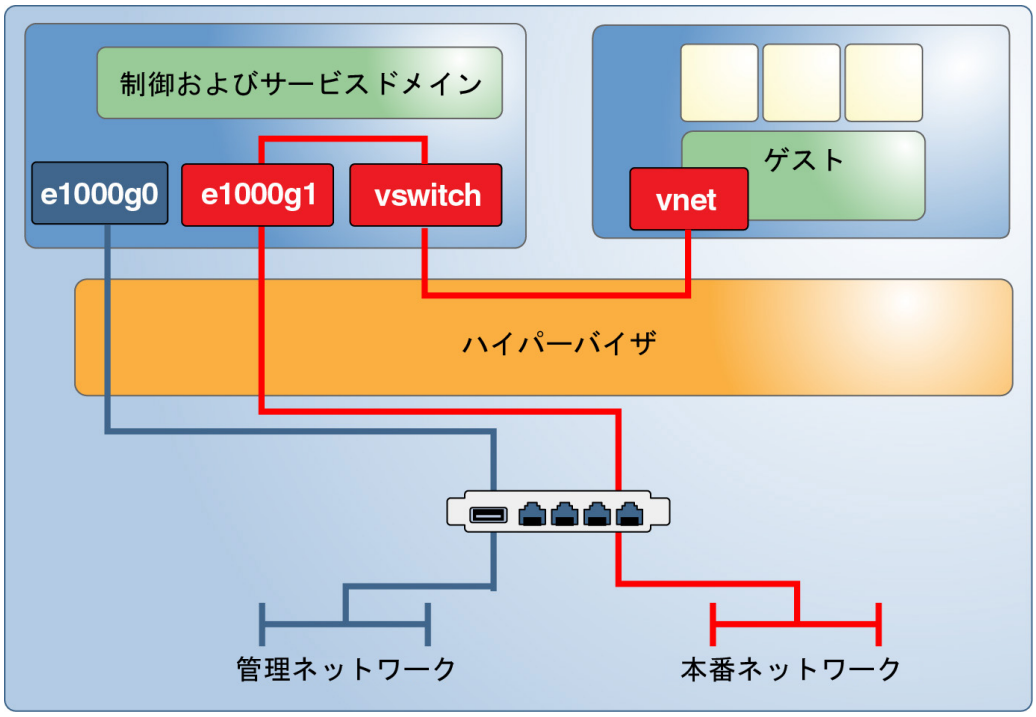
また、役割の分離を、別のサーバーを接続するために使用されるネットワーク環境に拡張することもできます。

### 対応策: 専用の管理ネットワークを構成する

サービスプロセッサ (SP) を備えたすべてのサーバーを専用の管理ネットワークに接続します。この構成はまた、実行環境のドメインにも推奨されます。ネットワーク接続されている場合は、これらのドメインを独自の専用ネットワーク上でホストします。実行環境のドメインを、本番ドメインに割り当てられたネットワークには直接接続*しないでください*。ILOM SP によって使用可能になる単一のコンソール接続を通してすべての管理作業を実行することは可能ですが、この構成によ

り、管理は実行不可能なくらいにきわめて煩雑になります。本番ネットワークと管理ネットワークを分離することによって、盗聴と操作の両方からの保護が可能になります。また、このタイプの分離により、共有ネットワークを経由したゲストドメインから実行環境への攻撃の可能性も解消されます。

**図 1-5** 専用の管理ネットワーク




# ILOM

現在のすべての Oracle SPARC システムには、次の機能を持つ組み込みのシステムコントローラ (ILOM) が含まれています。

- ファン速度やシャーシ電源などの基本的な環境制御の管理
- ファームウェアアップグレードの有効化
- 制御ドメインへのシステムコンソールの提供

ILOM にはシリアル接続経由でアクセスすることも、SSH、HTTP、HTTPS、SNMP、または IPMI を使用してネットワークポート経由でアクセスすることもできます。Fujitsu M10 サーバーは、ILOM の代わりに XSCF を使用して同様の機能を実行します。

## 脅威: 完全なシステムのサービス拒否

ILOM の制御を取得した攻撃者は、次の方法を含む多くの方法でシステムを危険にさらす可能性があります。

- 実行中のすべてのゲストからの電源の削除
- 少なくとも 1 つのゲストドメインへのアクセスを取得するための、操作されたファームウェアのインストール

これらのシナリオは、このようなコントローラデバイスを備えたすべてのシステムに適用されます。仮想化環境では、同じシステム格納装置に収容されている多くのドメインがリスクにさらされるため、物理環境に比べて損害がはるかに大きくなる場合があります。

同様に、制御ドメインまたは I/O ドメインの制御を取得した攻撃者は、対応する I/O サービスをシャットダウンすることによって、すべての依存ゲストドメインを容易に無効にすることができます。

### 評価: 完全なシステムのサービス拒否

ILOM は通常、管理ネットワークに接続されますが、BMC アクセスモジュールを備えた IPMI を使用して、制御ドメインから ILOM にアクセスすることもできます。そのため、これらの接続タイプの両方を適切に保護し、通常の本番ネットワークから分離するようにしてください。

同様に、攻撃者はネットワークから、または仮想化スタック内のエラーを使用してサービスドメインに侵入してから、ゲスト I/O をブロックしたり、システムのシャットダウンを実行したりできます。データが失われることも、改ざんされることもないため損害は限定されますが、その損害が多くのゲストドメインに影響を与える場合があります。そのため、潜在的な損害を限定するために、この脅威の可能性から保護するようにしてください。

### 対応策: ILOM をセキュリティー保護する

ILOM は、システムサービスプロセッサとして、シャーシ電源、Oracle VM Server for SPARC の起動構成、および制御ドメインへのコンソールアクセスなどの重要な機能を制御します。次の対策を使用すると、ILOM をセキュリティー保護できます。

- ILOM のネットワークポートを、実行環境内のドメインのために使用される管理ネットワークとは分離されたネットワークセグメント内に配置します。
- HTTP、IPMI、SNMP、HTTPS、SSH など、動作には必要のないすべてのサービスを無効にします。
- 必要な権利のみを許可する専用および個人の管理者アカウントを構成します。管理者が実行したアクションの説明責任を最大化するために、個人の管理者アカウントを作成するようにしてください。このタイプのアクセスは、コンソールアクセス、ファームウェアアップグレード、および起動構成の管理にとって特に重要です。

# ハイパーバイザ

ハイパーバイザは、実際のハードウェアの仮想化を実装および制御するファームウェアレイヤーです。ハイパーバイザには次のコンポーネントが含まれています。

- 実際のハイパーバイザ。ファームウェア内に実装され、システムの CPU によってサポートされます。
- ハイパーバイザを構成するために制御ドメイン内で実行されるカーネルモジュール。
- 仮想化 I/O を提供するために I/O ドメインおよびサービスドメイン内で実行されるカーネルモジュールとデーモン、および論理ドメインチャンネル (LDC) を使用して通信するカーネルモジュール。
- 仮想化 I/O デバイスにアクセスするためにゲストドメイン内で実行されるカーネルモジュールとデバイスドライバ、および LDC を使用して通信するカーネルモジュール。

## 脅威: 分離の破壊

攻撃者は、ハイパーバイザによって提供される分離された実行環境を破壊することによって、ゲストドメインまたはシステム全体をハイジャックできます。この脅威は、システムにもっとも重大な損害を与える可能性があります。

### 評価: 分離の破壊

モジュール化されたシステム設計では、ゲストドメイン、ハイパーバイザ、および制御ドメインに異なるレベルの権限を許可することによって分離を強化できます。各機能モジュールは、個別の構成可能なカーネルモジュール、デバイスドライバ、またはデーモン内に実装されます。このモジュール性にはクリーンな API とシンプルな通信プロトコルが必要であり、それによって、エラーの全体的なリスクが軽減されます。

エラーが悪用される可能性がきわめて低いと思われる場合でも、潜在的な損害が、攻撃者によるシステム全体の制御につながることがあります。

### 対応策: ファームウェアとソフトウェアの署名を検証する

システムファームウェアや OS のパッチを Oracle Web サイトから直接ダウンロードできるとしても、これらのパッチが操作されている場合があります。ソフトウェアをインストールする前に、ソフトウェアパッケージの MD5 チェックサムを検証するようにしてください。すべてのダウンロード可能なソフトウェアのチェックサムは、Oracle によって公開されています。

### 対応策: カーネルモジュールを検証する

Oracle VM Server for SPARC は、複数のドライバおよびカーネルモジュールを使用して、全体的な仮想化システムを実装します。Oracle Solaris OS とともに配布されるすべてのカーネルモジュールとほとんどのバイナリには、デジタル署名が含まれています。各カーネルモジュールおよびドライバのデジタル署名をチェックするには `elfsign` ユーティリティーを使用します。Oracle Solaris バイナリの整合性をチェックするには、Oracle Solaris 11 `pkg verify` コマンドを使用できます。`https://blogs.oracle.com/cmt/entry/solaris_fingerprint_database_how_it` を参照してください。

まず、`elfsign` ユーティリティーの整合性を確立する必要があります。基本監査およびレポートツール (BART) を使用して、デジタル署名の検証プロセスを自動化します。Solaris 10 オペレーティングシステムでの BART と Solaris Fingerprint Database の統合に関するドキュメント (`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-005-bart-solaris-fp-db-276999.pdf`)では、BART と Solaris Fingerprint Database を組み合わせて同様の整合性チェックを自動的に実行する方法について説明しています。指紋データベースはすでに中止されていますが、このドキュメントで説明されている概念は、`elfsign` と BART を同様の方法で使用するために適用できます。

## 制御ドメイン

制御ドメイン (多くの場合は I/O ドメインとサービスドメインの役割を持ちます) は、接続されているすべてのハードウェアリソースを制御するハイパーバイザの構成を変更できるため、安全な状態に保持する必要があります。

### 脅威: 制御ドメインのサービス拒否

制御ドメインのシャットダウンは、構成ツールのサービス拒否につながる場合があります。制御ドメインは構成の変更にのみ必要なため、ゲストドメインがほかのサービスドメインを経由してネットワークおよびディスクリソースにアクセスした場合、ゲストドメインは影響を受けません。

#### 評価: 制御ドメインのサービス拒否

ネットワーク経由で制御ドメインを攻撃することは、正しく保護されているほかの任意の Oracle Solaris OS インスタンスを攻撃することと同等です。制御ドメインのシャットダウンまたは同様のサービス拒否の損害は、比較的軽度です。ただし、制御ドメインがゲストドメインのサービスドメインとしても機能している場合、これらのゲストドメインは影響を受けます。

#### 対応策: コンソールアクセスをセキュリティー保護する

実行環境のドメインへの管理ネットワークアクセスを構成することは避けてください。このシナリオでは、すべての管理タスクを実行するために、制御ドメインへの ILOM コンソールサービスを使用する必要があります。その他のすべてのドメインへのコンソールアクセスは、制御ドメイン上で実行されている `vntsd` サービスを使用して引き続き可能です。

このオプションは、慎重に検討してください。このオプションによって、管理ネットワーク経由で攻撃されるリスクは軽減されますが、コンソールには同時に 1 人の管理者しかアクセスできません。

`vntsd` をセキュアに構成する方法については、『Oracle VM Server for SPARC 3.2 管理ガイド 』の「仮想ネットワーク端末サーバーデーモンを有効にする方法」を参照してください。

## Logical Domains Manager

Logical Domains Manager は制御ドメイン内で実行され、ハイパーバイザを構成したり、すべてのドメインやそのハードウェアリソースを作成および構成したりするために使用されます。Logical Domains Manager の使用がログに記録され、モニターされるようにしてください。

## 脅威: 構成ユーティリティーの無断使用

攻撃者が管理者のユーザー ID の制御を取得したり、異なるグループの管理者が別のシステムへの未承認のアクセスを取得したりする可能性があります。

### 評価: 構成ユーティリティーの無断使用

適切に維持されたアイデンティティー管理を実装することによって、管理者がシステムに不要にアクセスすることがないようにしてください。また、厳格で、きめ細かいアクセス制御や、2 人ルールなどのその他の対策も実装してください。

### 対応策: 2 人ルールを適用する

権利を使用して、Logical Domains Manager やその他の管理ツールに対して 2 人ルールを実装することを検討してください。Solaris 10 RBAC を使用したツーマンルールの適用 (`https://blogs.oracle.com/gbrunett/entry/enforcing_a_two_man_rule`)。このルールは、ソーシャルエンジニアリング攻撃、危険にさらされた管理アカウント、および人為的ミスから保護します。

### 対応策: Logical Domains Manager に対する権利を使用する

`ldm` コマンドに対する権利を使用すると、きめ細かいアクセス制御を実装したり、完全なリトレーサビリティーを維持したりできます。権利の構成については、『Oracle VM Server for SPARC 3.2 管理ガイド 』を参照してください。権利を使用すると、すべての管理者が `ldm` コマンドのすべての機能を使用できるわけではなくなるため、人為的ミスから保護するのに役立ちます。

### 対応策: Logical Domains Manager を強化する

不必要なドメインマネージャーサービスを無効化します。Logical Domains Manager は、ドメインのアクセス、モニタリング、および移行のためのネットワークサービスを提供します。ネットワークサービスを無効にすると、Logical Domains Manager の攻撃対象領域が、正常に動作するために必要な最小限度まで削減されます。このシナリオは、サービス拒否攻撃や、これらのネットワークサービスを悪用しようとするその他の試みに対応します。

**注記 -** ドメインマネージャーサービスを無効にすると、攻撃対象領域を最小限に抑えるのに役立ちますが、特定の構成でそれを実行した場合のすべての副作用を事前に知ることはできません。

次に示すネットワークサービスのいずれかが使用されていないときは、そのサービスを無効化します。

- TCP ポート `8101` 上の移行サービス

  このサービスを無効化するには、`ldmd`(1M) マニュアルページの `ldmd/incoming_migration_enabled` および `ldmd/outgoing_migration_enabled` プロパティーの説明を参照してください。

- TCP ポート `6482` の XMPP (eXtensible Messaging and Presence Protocol) サポート

  このサービスを無効にする方法については、『Oracle VM Server for SPARC 3.2 管理ガイド 』の「XML トランスポート」を参照してください。

  XMPP を無効にすると、一部の主要な Oracle VM Server for SPARC の機能 (ドメインの移行、メモリーの動的再構成、`ldm init-system` コマンドなど) が使用できなくなることに注意してください。また、XMPP を無効にすると、Oracle VM Manager や Ops Center もシステムを管理できなくなります。

- UDP ポート `161` の SNMP (Simple Network Management Protocol)

  Oracle VM Server for SPARC 管理情報ベース (MIB) を使用してドメインを監視するかどうかを決定します。この機能を使用するには、SNMP サービスが有効である必要があります。選択に基づいて次のいずれかを実行します。

  - **Oracle VM Server for SPARC MIB を使用するために SNMP サービスを有効化します。**安全な方法で Oracle VM Server for SPARC MIB をインストールします。『Oracle VM Server for SPARC 3.2 管理ガイド 』の「Oracle VM Server for SPARC MIB ソフトウェアパッケージのインストール方法」および『Oracle VM Server for SPARC 3.2 管理ガイド 』の「セキュリティーの管理」を参照してください。
  - **SNMP サービスを無効化します。**このサービスを無効にする方法については、『Oracle VM Server for SPARC 3.2 管理ガイド 』の「Oracle VM Server for SPARC MIB ソフトウェアパッケージを削除する方法」を参照してください。

- マルチキャストアドレス `239.129.9.27` およびポート `64535` の発見サービス

---

**注記 -** この検出メカニズムは、MAC アドレスを自動的に割り当てるときに衝突を検出するために、`ldmd` デーモンでも使用されることに注意してください。検出サービスを無効にすると、MAC アドレスの衝突検出が機能しないため、MAC アドレスの自動割り当ては正しく機能しません。

---

Logical Domains Manager デーモン `ldmd` が実行されている間はこのサービスを無効化*できません*。代わりに、Oracle Solaris の IP フィルタ機能を使用してこのサービスへのアクセスをブロックし、Logical Domains Manager の攻撃対象領域を最小化します。アクセスをブロックしてユーティリティーの無断使用を防ぐことは、サービス拒否攻撃や、これらのネットワークサービスを悪用しようとするその他の試みへの対抗策として有効です。『Oracle Solaris Administration: IP Services 』の第 20 章「IP Filter in Oracle Solaris (Overview)」および『Oracle Solaris Administration: IP Services 』の「Using IP Filter Rule Sets」を参照してください。

29 ページの「対応策: ILOM をセキュリティー保護する」も参照してください。

### 対応策: Logical Domains Manager を監査する

Logical Domains Manager の保護は、システム全体のセキュリティーにとってきわめて重要です。Oracle VM Server for SPARC 構成への変更はすべて、悪意のあるアクションを追跡するために、ログに記録する必要があります。監査ログを定期的にスキャンし、そのログをセキュアなアーカイブのために別のシステムにコピーします。詳細は、『Oracle VM Server for SPARC 3.2 管理ガイド 』の第 2 章「Oracle VM Server for SPARC のセキュリティー」を参照してください。

## サービスドメイン

サービスドメインは、システム上のゲストドメインにいくつかの仮想サービスを提供します。これらのサービスには、仮想スイッチ、仮想ディスク、または仮想コンソールサービスが含まれることがあります。

図1-6「サービスドメインの例」 は、コンソールサービスを提供するサービスドメインの例を示しています。多くの場合、制御ドメインはコンソールサービスをホストするため、サービスドメインでもあります。実行環境のドメインは一般に、制御ドメイン、I/O ドメイン、およびサービスドメインの機能を 1 つまたは 2 つのドメインに結合します。

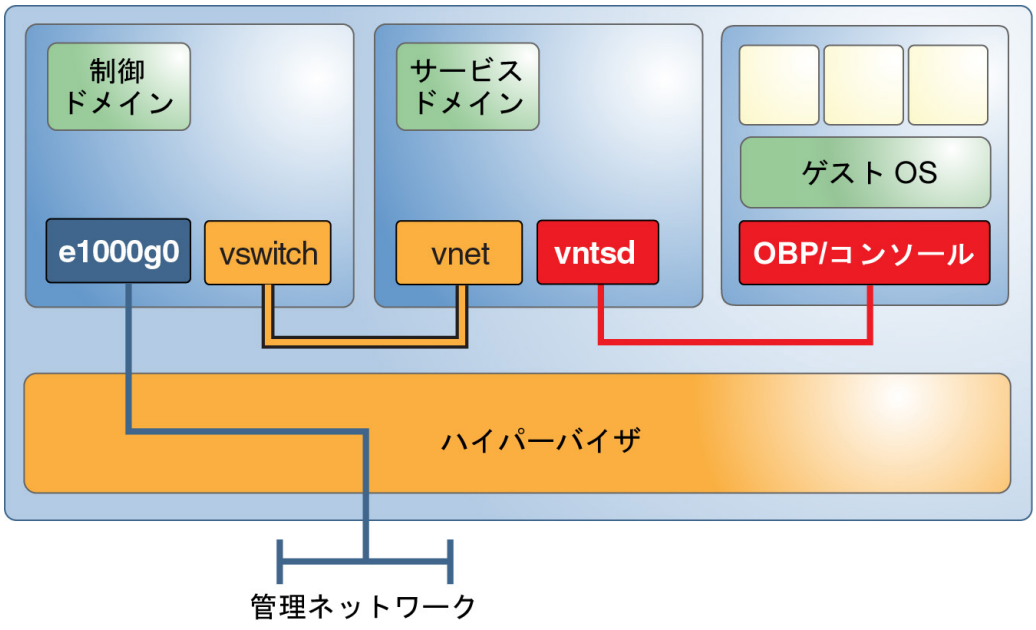
## 脅威: サービスドメインの操作

サービスドメインの制御を取得した攻撃者は、データを操作したり、提供されるサービスを通して発生するすべての通信を傍受したりできます。この制御には、ゲストドメインへのコンソールアクセス、ネットワークサービスへのアクセス、またはディスクサービスへのアクセスが含まれることがあります。

### 評価: サービスドメインの操作

攻撃の方法は制御ドメインへの攻撃と同じですが、攻撃者はシステム構成を変更できないため、可能性のある損害は少なくなります。結果としての損害には、サービスドメインによって提供されているデータの盗難または操作が含まれることがありますが、データソースの操作は含まれません。サービスによっては、攻撃者によるカーネルモジュールの交換が必要になることがあります。

**図 1-6** サービスドメインの例



### 対応策: サービスドメインをきめ細かく分離する

可能な場合は、各サービスドメインがクライアントに *1 つの*サービスのみを提供するようにします。この構成によって、サービスドメインに侵入された場合でも、危険にさらされる可能性があるのは 1 つのサービスだけであることが保証されます。ただし、このタイプの構成の重要性と、複雑さが増すこととを必ず比較検討してください。冗長な I/O ドメインの設置が強く推奨されることに注意してください。

### 対応策: サービスドメインとゲストドメインを分離する

Oracle Solaris 10 と Oracle Solaris 11 の両方のサービスドメインをゲストドメインから分離できます。次の各解決策は、実装の優先順位に基づいて示されています。

- サービスドメインとゲストドメインが同じネットワークポートを共有しないようにします。また、サービスドメイン上のどの仮想スイッチインタフェースも plumb しないでください。Oracle Solaris 11 サービスドメインの場合は、仮想スイッチに使用されている物理ポート上のどの VNIC も plumb しないでください。
- Oracle Solaris 10 OS と Oracle Solaris 11 OS の両方で同じネットワークポートを使用する必要がある場合は、I/O ドメインのトラフィックを、ゲストドメインによって使用されていない VLAN 内に配置します。
- 前の解決策のどちらも実装できない場合は、Oracle Solaris 10 OS で仮想スイッチを plumb せずに、Oracle Solaris 11 OS で IP フィルタを適用してください。

### 対応策: 仮想コンソールへのアクセスを制限する

個々の仮想コンソールへのアクセスが、そのコンソールにアクセスする必要のあるユーザー*のみ*に制限されるようにしてください。この構成によって、どの管理者もすべてのコンソールにはアクセスできないようになるため、危険にさらされたアカウントに割り当てられているコンソール以外のコンソールにはアクセスできなくなります。『Oracle VM Server for SPARC 3.2 管理ガイド 』の「デフォルトのサービスを作成する方法」を参照してください。

## I/O ドメイン

ネットワークポートやディスクなどの物理 I/O デバイスに直接アクセスできるドメインはすべて、I/O ドメインです。I/O ドメインの構成については、『Oracle VM Server for SPARC 3.2 管理ガイド 』の第 5 章「I/O ドメインの構成」を参照してください。

I/O ドメインはまた、ゲストドメインに I/O サービスを提供する (それにより、そのドメインがハードウェアにアクセスできるようにする) 場合は、サービスドメインでもあります。

## 脅威: I/O ドメインまたはサービスドメインのサービス拒否の発生

I/O ドメインの I/O サービスをブロックした攻撃者は、すべての依存ゲストドメインが同様にブロックされるようにします。DoS 攻撃は、バックエンドネットワークやディスクインフラストラクチャーを過負荷状態にしたり、ドメインに障害を挿入したりすることによって成功する可能性があります。いずれの攻撃も、ドメインを強制的にハングアップまたはパニック状態にする可能性があります。同様に、サービスドメインのサービスを一時停止した攻撃者は、これらのサービスに依存するすべてのゲストドメインをただちにハングアップさせます。ゲストドメインがハングアップした場合、I/O サービスが再開されるとゲストドメインは操作を再開します。

### 評価: I/O ドメインまたはサービスドメインのサービス拒否の発生

DoS 攻撃は一般に、ネットワーク経由で行われます。このような攻撃が成功する場合があるのは、ネットワークポートが通信用に開いており、そのネットワークポートをネットワークトラフィックでいっぱいにすることができるためです。その結果、サービスが失われ、依存ゲストドメインがブロックされます。ディスクリソースへの同様の攻撃が、SAN インフラストラクチャーを使用したり、I/O ドメインを攻撃したりすることによって行われることがあります。その場合の唯一の損害は、すべての依存ゲストドメインの一時的な停止です。DoS タスクの影響は重大になることもありますが、データが改ざんされたり、失われたりすることはなく、システム構成はそのままの状態で残ります。

### 対応策: I/O ドメインをきめ細かく構成する

複数の I/O ドメインを構成すると、1 つのドメインで障害が発生した場合、または危険にさらされた場合の影響が軽減されます。ゲストドメインに個別の PCIe スロットを割り当てることにより、そのドメインに I/O ドメインの機能を与えることができます。PCIe バスを所有するルートドメインがクラッシュした場合は、そのバスがリセットされるため、個別のスロットに割り当てられていたドメインのクラッシュが続いて発生します。この機能によって、それぞれ個別の PCIe バスを所有する 2 つのルートドメインの必要性が完全に解消されるわけではありません。

### 対応策: 冗長ハードウェアとルートドメインを構成する

高可用性もまた、サービスがサービス拒否攻撃に耐えることができるようにするため、セキュリティーの向上に寄与します。Oracle VM Server for SPARC には、冗長な I/O ドメインでの冗長なディスクやネットワークリソースの使用などの高可用性の手法が実装されています。この構成オプションは、I/O ドメインのローリングアップグレードを可能にするとともに、DoS 攻撃の成功のために障害が発生した I/O ドメインの影響から保護します。SR-IOV の出現により、ゲストドメインは個々の I/O デバイスに直接アクセスできるようになりました。ただし、SR-IOV がオプションでない場合は、冗長な I/O ドメインの作成を検討してください。37 ページの「対応策: サービスドメインをきめ細かく分離する」を参照してください。

## 脅威: I/O ドメインの操作

I/O ドメインは、バックエンドデバイス (通常はディスク) に直接アクセスでき、これを仮想化してからゲストドメインに提供します。成功した攻撃者は、これらのデバイスへのフルアクセス権を手に入れ、機密データを読み取ったり、ゲストドメインのブートディスク上のソフトウェアを操作したりできます。

### 評価: I/O ドメイン内の操作

I/O ドメインへの攻撃は、サービスドメインまたは制御ドメインへの攻撃と同じ程度の成功の可能性があります。多数のディスクデバイスへの潜在的なアクセスを考慮すると、I/O ドメインは魅力的なターゲットです。そのため、仮想化されたディスク上で実行されるゲストドメインで機密データを処理する場合は、この脅威を考慮してください。

### 対応策: 仮想ディスクを保護する

I/O ドメインが危険にさらされた場合、攻撃者は、ゲストドメインの仮想ディスクへのフルアクセス権を手に入れます。

次のことを実行することによって、仮想ディスクの内容を保護します。

- **仮想ディスクの内容を暗号化する。**Oracle Solaris 10 システムでは、`pgp/gpg` または Oracle 11g で暗号化された表領域などの独自のデータを暗号化できるアプリケーションを使用できます。Oracle Solaris 11 システムでは、ファイルシステムに格納されているすべてのデータの透過的な暗号化を実現するために、ZFS で暗号化されたデータセットを使用できます。

- **異なる I/O ドメインにまたがる複数の仮想ディスク上にデータを分散させる。**ゲストドメインでは、2 つの I/O ドメインから取得される複数の仮想ディスク上にストライプ化するストライプ化 (RAID 1/RAID 5) ボリュームを作成できます。これらの I/O ドメインのいずれかが危険にさらされた場合、攻撃者にとって、入手できるデータの一部分を使用することは困難になります。

# ゲストドメイン

ゲストドメインは実行環境には含まれていませんが、ネットワークに接続されているため、攻撃のもっとも可能性の高いターゲットになります。仮想化システムに侵入した攻撃者は、実行環境に対する攻撃を開始できます。

## 対応策: ゲストドメインの OS をセキュリティー保護する

ゲストドメイン上のオペレーティングシステムは多くの場合、すべての攻撃に対する防御の最前線になります。データセンター内で発生する攻撃を除き、攻撃者は、ゲストドメインの分離を破壊して完全な環境を取得しようとする前に、外部に接続されたゲストドメインに侵入する必要があります。そのため、ゲストドメインの OS を強化する必要があります。

OS をさらに強化するには、Solaris ゾーン内にアプリケーションを配備することができ、これにより、そのアプリケーションのネットワークサービスとゲストドメインのオペレーティングシステムの間に分離のレイヤーが追加で配置されます。サービスへの攻撃が成功しても、危険にさらされるのはこのゾーンだけであり、ベースとなるオペレーティングシステムは対象になりません。これにより、攻撃者は、そのゾーンに割り当てられているリソース以外に制御を拡張できなくなります。その結果、最終的にゲストの分離を破壊することがより困難になります。ゲスト OS のセキュリティー保護の詳細は、『Oracle Solaris 10 Security Guidelines 』および『Oracle Solaris 11 Security Guidelines 』を参照してください。

♦ ♦ ♦ 第 2 章

# 2 Oracle VM Server for SPARC の安全なインストールと構成

この章では、Oracle VM Server for SPARC ソフトウェアのインストールおよび構成に関連するセキュリティー上の考慮事項について説明します。

## インストール

Oracle VM Server for SPARC ソフトウェアは、Oracle Solaris 10 または Oracle Solaris 11 パッケージとして自動的かつ安全にインストールされます。インストールの完了後、ドメインで権利、監査、および承認の各機能を構成するには管理者権限が必要です。これらの機能はデフォルトで有効になっていません。

## インストール後の構成

Oracle VM Server for SPARC ソフトウェアをインストールしたあとで、使用上のセキュリティーを最大化するために次のタスクを実行します。

- 仮想スイッチ、仮想ディスクサーバー、仮想コンソール端末集配信装置サービスなど、必要な仮想 I/O サービスを制御ドメインで構成します。『Oracle VM Server for SPARC 3.2 管理ガイド 』の第 3 章「サービスおよび制御ドメインの設定」を参照してください。
- ゲストドメインを構成します。『Oracle VM Server for SPARC 3.2 管理ガイド 』の第 4 章「ゲストドメインの設定」を参照してください。

  仮想スイッチを使用すると、管理ネットワークおよび本番ネットワークを利用してゲストドメインを構成できます。この場合、本番ネットワークのインタフェースを仮想スイッチのネットワークデバイスとして使用することによって仮想スイッチが作成されます。27 ページの「対応策: 専用の管理ネットワークを構成する」を参照してください。

ゲストドメインの仮想ディスクのいずれかが危険にさらされると、そのドメインのセキュリティーが低下します。したがって、仮想ディスク (ネットワーク接続ストレージ (NAS)、ローカルに格納されたディスクイメージファイル、または物理ディスク) は必ず、セキュリティーで保護された場所に配置してください。

`vntsd` デーモンはデフォルトで無効です。このデーモンが有効になると、制御ドメインにログインしているすべてのユーザーが、ゲストドメインのコンソールに接続することを許可されます。このようなアクセスを防ぐには、`vntsd` デーモンが無効になっていることを確認するか、または権利を使用してコンソール接続アクセスを認可されたユーザー*のみ*に制限します。

- サービスプロセッサ (SP) はデフォルトで安全に構成されます。Integrated Lights Out Management (ILOM) ソフトウェアを使用した SP の管理については、`http://www.oracle.com/technetwork/documentation/sparc-tseries-servers-252697.html` のプラットフォーム別ドキュメントを参照してください。

♦ ♦ ♦ 第 3 章

# 3 開発者向けのセキュリティーの考慮事項

この章では、Oracle VM Server for SPARC ソフトウェア向けのアプリケーションを作成する開発者に情報を提供します。

## Oracle VM Server for SPARC XML インタフェース

XML (eXtensible Markup Language) 通信メカニズムによって Oracle VM Server for SPARC ソフトウェアと連携する外部プログラムを作成できます。XML は、XMPP (Extensible Messaging and Presence Protocol) を使用します。

攻撃者がこのネットワークプロトコルの弱点を突いてシステムへのアクセスを試みる可能性があるため、XMPP の無効化を検討してください。XMPP の無効化については、『Oracle VM Server for SPARC 3.2 管理ガイド 』の「XML トランスポート」を参照してください。Logical Domains Manager が使用するセキュリティーメカニズムについては、『Oracle VM Server for SPARC 3.2 管理ガイド 』の「XMPP サーバー」を参照してください。

XMPP を無効にすると、一部の主要な Oracle VM Server for SPARC の機能 (ドメインの移行、メモリーの動的再構成、`ldm init-system` コマンドなど) が使用できなくなることに注意してください。また、XMPP を無効にすると、Oracle VM Manager や Ops Center もシステムを管理できなくなります。

♦ ♦ ♦ 付 録 A

# セキュアな配備のためのチェックリスト

このチェックリストは、Oracle VM Server for SPARC 環境を強化するために実行できる手順を要約したものです。詳細については次のものを含む各種ドキュメントを参照してください。

- 『Oracle VM Server for SPARC 3.2 管理ガイド 』
- 『Oracle Solaris 10 Security Guidelines 』
- 『Oracle Solaris 11 Security Guidelines 』

## Oracle VM Server for SPARC セキュリティーチェックリスト

- 仮想化環境でない場合と同様に、Oracle Solaris OS の強化手順をゲストドメインに対して実行します。
- LDoms Management および LDoms Review 権利プロファイルを使用して、適切な権限をユーザーに委任します。
- 権利を使用して、アクセスを Oracle VM Server for SPARC の管理者がアクセスする必要のあるドメインのコンソール*のみ*に制限します。
- Oracle VM Server for SPARC に対して Oracle Solaris OS の監査機能を有効化します。
- 不必要なドメインマネージャーサービスを無効化します。
- 1 つの物理プラットフォームには同じセキュリティークラスのゲストドメインのみを配備します。
- 実行環境の管理ネットワークとゲストドメインの間にネットワーク接続がないことを確認します。
- 必要なリソースのみをゲストドメインに割り当てます。