



# Red Hat Enterprise Linux 7 仮想化セキュリティガイド

---

仮想化環境のセキュリティ保護

Scott Radvan

Tahlia Richardson

Thanks go to the following people for enabling the creation of this guide:

Paul Moore

Kurt Seifried

David Jorm



## 仮想化環境のセキュリティー保護

Scott Radvan  
Red Hat Engineering Content Services  
sradvan@redhat.com

Tahlia Richardson  
Red Hat Engineering Content Services  
trichard@redhat.com

Paul Moore  
Red Hat エンジニアリング

Kurt Seifried  
Red Hat エンジニアリング

David Jorm  
Red Hat エンジニアリング

Thanks go to the following people for enabling the creation of this guide:

## 法律上の通知

Copyright © 2015 Red Hat, Inc.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

## 概要

本ガイドは、Red Hatが提供する仮想化セキュリティーテクノロジーについての概要を説明します。仮想化環境内のホスト、ゲスト、および共有インフラストラクチャー/リソースのセキュリティーを保護するための推奨事項を提供します。

---

# 目次

<b>第1章 はじめに</b> .....	<b>2</b>
1.1. 仮想化環境と非仮想化環境	2
1.2. 仮想化セキュリティが重要である理由	3
1.3. sVirt を使用した SELinux の活用	4
<b>第2章 ホストのセキュリティ</b> .....	<b>5</b>
2.1. ホストのセキュリティが重要である理由	5
2.2. Red Hat Enterprise Linux のホストセキュリティ推奨プラクティス	5
2.3. Red Hat Enterprise Virtualization のホストセキュリティ推奨プラクティス	6
<b>第3章 ゲストのセキュリティ</b> .....	<b>8</b>
3.1. ゲストのセキュリティが重要である理由	8
3.2. ゲストセキュリティの推奨プラクティス	8
<b>第4章 sVirt</b> .....	<b>9</b>
4.1. 概要	9
4.2. SELinux と強制アクセス制御 (MAC)	9
4.3. sVirt の設定	10
4.4. sVirt のラベル	11
<b>第5章 仮想化環境におけるネットワークセキュリティ</b> .....	<b>14</b>
5.1. ネットワークセキュリティの概要	14
5.2. ネットワークセキュリティ推奨プラクティス	14
<b>付録A 追加情報</b> .....	<b>15</b>
A.1. SELinux および sVirt	15
A.2. 仮想化セキュリティ	15
<b>付録B 改訂履歴</b> .....	<b>16</b>

## 第1章 はじめに

### 1.1. 仮想化環境と非仮想化環境

仮想化環境は、攻撃者にとって以前は価値がなかった新たな攻撃ベクトルの発見と既存の 익스プロイトの洗練の両方の機会を与えます。このため、仮想マシンを作成し、これを維持する際には、物理ホストとそのホスト上で実行されるゲストの両方のセキュリティーを確保するための対策を講じることが重要となります。

#### 非仮想化環境

非仮想化環境では、ホストは物理的に相互分離しており、各ホストには Web サーバーや DNS サーバーなどのサービスで構成される自己完結型の環境があります。これらのサービスは、独自のユーザースペース、ホストカーネル、物理ホストと直接通信して、ネットワークにサービスを直接提供します。下図は、非仮想化環境を示しています。

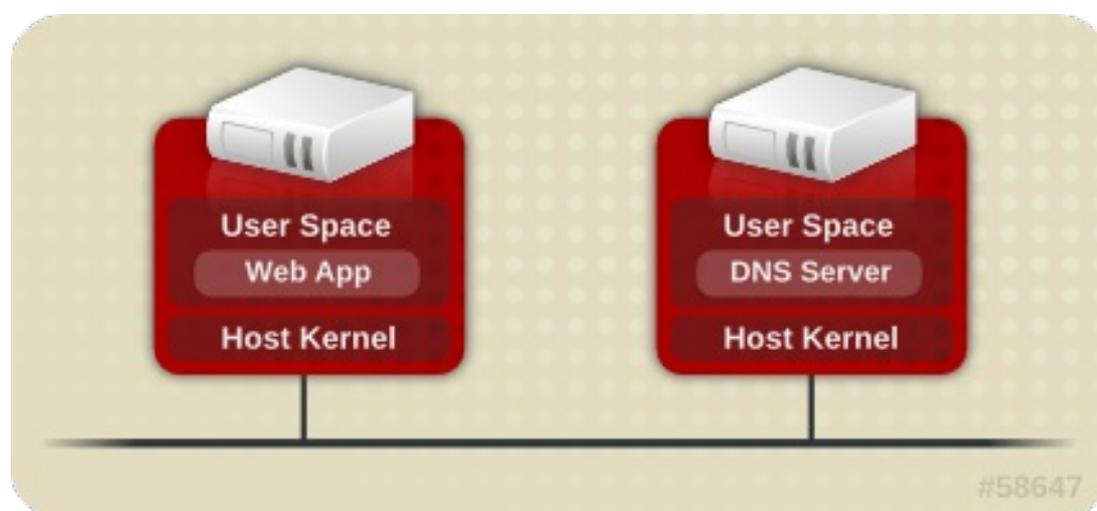


図1.1 非仮想化環境

#### 仮想化環境

仮想化環境では、複数のオペレーティングシステムを（「ゲスト」として）単一のホストカーネルおよび物理ホストに格納することができます。下図は仮想化環境を示しています。

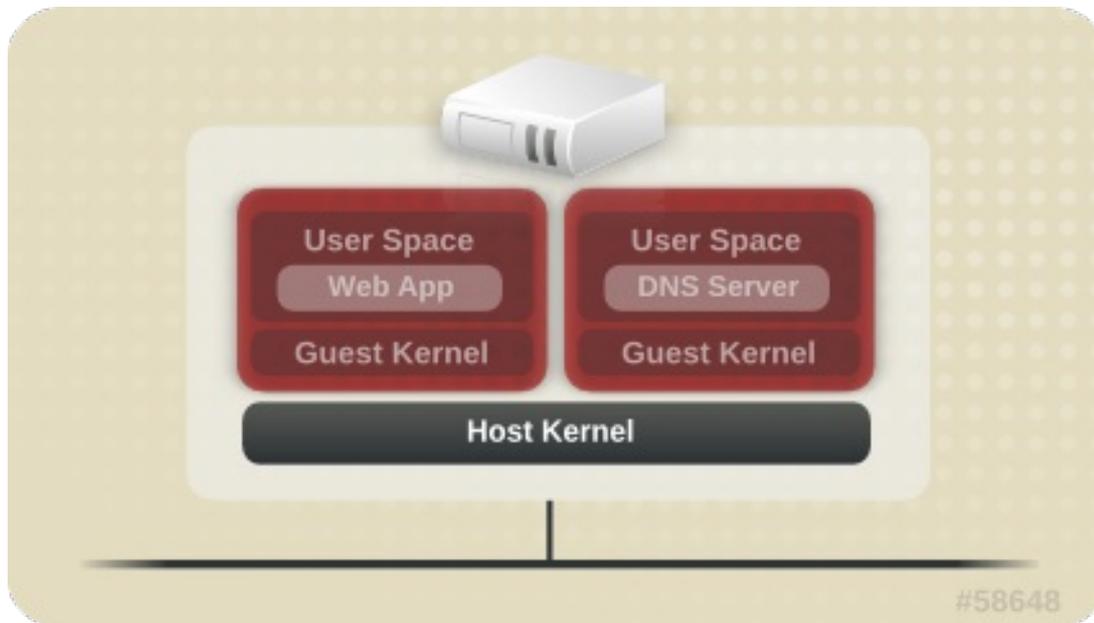


図1.2 仮想化環境

サービスが仮想化されていない場合は、マシンは物理的に分離されています。したがって、エクスプロイトは影響を受けたマシンに抑えられます。ただし、ネットワーク攻撃は明らかな例外となります。仮想化環境内でサービスがグループ化されると、システムの脆弱性が高まります。ハイパーバイザーのセキュリティに不備がある場合、ゲストインスタンスによるエクスプロイトを受ける可能性があり、そのゲストはホストのみならず、そのホスト上で実行されている他のゲストも攻撃できるようになる可能性があります。これに単に理論上の事柄ではなく、攻撃はすでにハイパーバイザー上に存在しています。それらの攻撃がゲストインスタンスを超えて、他のゲストが攻撃にさらされる可能性もあり得ます。

## 1.2. 仮想化セキュリティが重要である理由

インフラストラクチャーに仮想化をデプロイすると、数多くのメリットがもたらされますが、新たなリスクが生じる可能性もあります。仮想化のリソースとサービスのデプロイにあたっては以下のようなセキュリティに関する考慮事項を検討した上でデプロイを行う必要があります。

- ※ ホスト/ハイパーバイザーは第一のターゲットであり、ゲストとデータの単一障害点となることが多くあります。
- ※ 仮想マシンは望ましくない方法で相互干渉する場合があります。これを防ぐためのアクセス制御が導入されていないと、悪意のあるゲストが脆弱なハイパーバイザーをバイパスし、他のゲストのストレージなど、ホストシステム上の他のリソースに直接アクセスする可能性があります。
- ※ 仮想化システムを迅速にデプロイすると、十分なパッチ、モニタリング、メンテナンスなどのリソース管理の必要性が増大するため、リソースとサービスのトラッキングおよび維持管理が難しくなる場合があります。
- ※ 仮想化環境における技術スタッフの知識不足、技能の格差、経験不足などの問題が存在する可能性があります。このような問題は、多くの場合、脆弱性へとつながります。
- ※ ストレージなどのリソースが複数のマシンに散在し、それらのマシンに依存している場合があります。このような場合には環境が過度に複雑化してしまい、システムの管理とメンテナンスが不十分となる可能性があります。
- ※ 仮想化によって、環境内に存在する従来のセキュリティリスクは排除されません。仮想化レイヤーのみでなく、ソリューションスタック全体のセキュリティを保護する必要があります。

本ガイドは、仮想化環境のセキュリティ保護に役立つ、Red Hat Enterprise Linux および Red Hat Enterprise Virtualization の仮想化推奨プラクティスの数々をご紹介します、お客様のセキュリティリスクを軽減することを目的としています。

### 1.3. sVirt を使用した SELinux の活用

sVirt は仮想化を SELinux (Security-Enhanced Linux) によって提供されている既存のセキュリティフレームワークに組み込むことにより、**強制アクセス制御(MAC)** を仮想マシンに適用します。sVirt の主な目的は、ハイパーバイザーのセキュリティの脆弱性を利用した攻撃からホストとゲストを保護することです。SELinux は異なるプロセス全体にわたってアクセスポリシーを適用することでシステムを保護します。sVirt は、各ゲストをプロセスとして扱うことによりこの機能をホストとゲストにまで拡張し、悪意のあるゲストが制限付きリソースにアクセスするのを防ぐために設計されたのと同様のポリシーを管理者が適用できるようにします。sVirt についての詳しい情報は [4章 sVirt](#) を参照してください。

## 第2章 ホストのセキュリティー

### 2.1. ホストのセキュリティーが重要である理由

仮想化テクノロジーをデプロイする際、ホストのセキュリティーは最優先事項です。Red Hat Enterprise Linux のホストシステムは、物理デバイス、ストレージ、ネットワークへのアクセスに加えて、全仮想化ゲスト自体を管理および制御します。ホストシステムのセキュリティーが侵害されると、ホストシステムのみでなくゲストとそのデータまでもが攻撃を受ける可能性があります。

仮想化ゲストのセキュリティーはホストシステムにかかっています。Red Hat Enterprise Linux ホストシステムのセキュリティー保護は、セキュアな仮想化プラットフォームの確立に向けた第一歩です。

### 2.2. Red Hat Enterprise Linux のホストセキュリティー推奨プラクティス

ホストのセキュリティーは、セキュアな仮想化インフラストラクチャーの極めて重要な要素であるため、以下の推奨プラクティスは Red Hat Enterprise Linux ホストシステムのセキュリティー保護の開始点として役立ちます。

- ※ ゲストシステムの使用と管理のサポートに必要なサービスのみを実行します。ファイルサービスや印刷サービスなどのサービスを追加で提供する必要がある場合には、それらのサービスを Red Hat Enterprise Linux ゲストで実行することを検討した方がよいでしょう。
- ※ システムへの直接のアクセスはシステムの管理を行う必要がある人に制限してください。共有の root アクセスを無効にして、代わりに **sudo** などのツールを使用して、管理ロールに基づいて管理者に特権的アクセスを付与することを検討してください。
- ※ SELinux がご使用のインストールに応じて適切に設定され、enforcing モードで稼働していることを確認します。これは、適正なプラクティスである上、sVirt によって提供される高度な仮想化セキュリティー機能は SELinux に依存しています。SELinux と sVirt に関する詳しい情報は [4章 sVirt](#) を参照してください。
- ※ ホストシステムで監査が有効化され、libvirt が監査レコードを生成するように設定されていることを確認します。監査が有効化されると、libvirt はゲストの設定変更および起動/停止イベントの監査レコードを生成します。これは、ゲストの状態をトラッキングするのに役立ちます。また、libvirt の監査イベントは、標準の監査ログ検査ツール以外に、専用の **auvirt** ツールでも確認することができます。
- ※ システムのリモート管理はすべてセキュアなネットワークチャンネル上のみで実行されるようにしてください。SSH のようなツールや、TLS または SSL などのネットワークプロトコルは認証とデータ暗号化の両方を提供し、承認済みの管理者のみがシステムをリモートで管理できるようにするのに役立ちます。
- ※ ご使用のインストールに応じてファイアウォールが適切に設定されており、ブート時にアクティブ化されることを確認します。システムの使用および管理に必要なネットワークポートのみを許可する必要があります。
- ※ ディスク全体またはブロックデバイス (例: **/dev/sdb**) への直接のアクセスをゲストに許可するのは控えて、代わりにゲストストレージにはパーティション (例: **/dev/sdb1**) や LVM ボリュームを使用します。
- ※ スタッフが仮想化環境における十分なトレーニングを受けており、知識が十分であることを確認してください。

**警告**

SR-IOV が利用不可能な場合に USB デバイス、物理ファンクションまたは物理デバイスを仮想マシンに割り当てると、デバイスのファームウェアを上書きするのに十分なデバイスへのアクセスが提供される場合があります。これにより、攻撃者が悪意のあるコードによってデバイスのファームウェアを上書きし、仮想マシン間でデバイスを移動する際やホストのブート時に問題を生じさせる潜在的なセキュリティ上の問題が提示されます。適用できる場合は、SR-IOV 仮想ファンクションデバイス割り当てを使用することをお勧めします。

**注記**

本ガイドは、大半の仮想化環境でみられるセキュリティ関連の課題、脆弱性、解決策と推奨される対処方法について説明することを目的としています。ただし、Red Hat Enterprise Linux システムのセキュリティを保護する際には従うべき推奨プラクティスが数多くあり、これらはスタンドアロン、仮想化ホスト、ゲストインスタンスを問わずに適用されます。これらの推奨プラクティスにはシステム更新、パスワードのセキュリティ、暗号化、ファイアウォールの設定などが含まれます。この情報については、<https://access.redhat.com/site/documentation/> の『Red Hat Enterprise Linux セキュリティガイド』で詳しく説明しています。

### 2.2.1. パブリッククラウドオペレーター向けの特殊な考慮事項

パブリッククラウドサービスオペレーターは、従来の仮想化ユーザーのリスクを超える数多くのセキュリティリスクにさらされます。悪意のあるゲストの脅威や、仮想化インフラストラクチャー全体にわたる顧客データの機密性および整合性に対する要件により、ホスト/ゲスト間ならびにゲスト間における仮想ゲストの分離は極めて重要となります。

パブリッククラウドオペレーターは上記の Red Hat Enterprise Linux 仮想化推奨プラクティスに加えて、以下の点も考慮する必要があります。

- ✦ ゲストからハードウェアへの直接のアクセスを無効にしてください。PCI、USB、FireWire、Thunderbolt、eSATA などのデバイスパススルーメカニズムは、管理を難しくする上、多くの場合は基礎となるハードウェアに依存してゲスト間の分離を強制します。
- ✦ クラウドオペレーターのプライベート管理ネットワークを顧客のゲストネットワークと分離して、顧客ネットワークを相互に分離することにより、以下が可能になります。
  - ゲストがネットワークを介してホストシステムにアクセスできないようにする。
  - 顧客がクラウドプロバイダーの内部ネットワークを介して別の顧客のゲストシステムに直接アクセスできないようにする。

## 2.3. Red Hat Enterprise Virtualization のホストセキュリティ推奨プラクティス

### 2.3.1. Red Hat Enterprise Virtualization のネットワークポート

Red Hat Enterprise Virtualization では、管理用およびその他の仮想化機能用にさまざまなネットワークポートを使用します。Red Hat Enterprise Linux が Red Hat Enterprise Virtualization とともにホストとして機能するには、これらのポートを開放しておく必要があります。対象のポートと Red Hat Enterprise Virtualization での用途は以下の一覧のとおりです。

- ※ ICMP エコー要求の受信と ICMP エコー応答の送信を許可する必要があります。
- ※ ポート 22 (TCP) は SSH アクセスと初期インストール用に開放する必要があります。
- ※ ポート 161 (UDP) は SNMP (Simple Network Management Protocol) に必要です。
- ※ ポート 5900～65535 (TCP) は、SPICE/VNC セッションでのゲストコンソールアクセスに使用されます。
- ※ ポート 80 または 443 (TCP) は **vds-m-reg** サービスによるホスト情報の通信には、Manager のセキュリティ設定に応じて使用されます。
- ※ ポート 16514 (TLS) またはポート 16509 (TCP) は libvirt によって生成される移行関連の通信をサポートするために使用されます。
- ※ ポート 49152 から 49215 (TCP) は、移行に使用されます。移行には、同時に発生する移行数に応じて、この範囲内の任意のポートを使用することができます。
- ※ VDSM による管理、ストレージ、ホスト間通信には、デフォルトでポート 54321 (TCP) を使用します。このポートは変更可能です。



### 警告

外部でのデバイス管理が不可欠な場合以外は、ネットワーク境界に位置するポート 161 (UDP) での SNMP のフィルタリングには特に注意を払ってください。

## 第3章 ゲストのセキュリティー

### 3.1. ゲストのセキュリティーが重要である理由

ホストシステムのセキュリティーは、そのホスト上で実行されているゲストを確実にセキュリティー保護するために極めて重要となりますが、ホストのセキュリティーによって個別のゲストマシンの適切なセキュリティー保護の必要性がなくなる訳ではありません。システムを仮想化ゲストとして実行する場合、従来の非仮想化システムに関連するセキュリティー上のリスクはすべて依然として存在します。ゲストシステムのセキュリティーが侵害されると、ビジネスデータや顧客の機密情報など、ゲストシステムにアクセス可能なリソースはいずれも攻撃を受けやすくなる可能性があります。

### 3.2. ゲストセキュリティーの推奨プラクティス

『Red Hat Enterprise Linux セキュリティガイド』に記載の Red Hat Enterprise Linux システムのセキュリティー保護に関する推奨プラクティスはすべて、従来の非仮想化システムと仮想化ゲストとしてインストールされたシステムの両方に適用されますが、仮想化環境内でゲストを実行する場合に極めて重要となるセキュリティー関連のプラクティスがいくつかあります。

- ※ ゲストの管理はすべてリモートで実行される可能性が高いため、システムの管理は必ずセキュリティー保護されたネットワークチャネルで行うようにしてください。SSHなどのツールや TLS または SSL などのネットワークプロトコルは、認証とデータの暗号化の両方を提供し、承認された管理者のみがシステムをリモートで管理できるようにします。
- ※ 一部の仮想化テクノロジーでは、特殊なゲストエージェントまたはドライバーを使用して仮想化固有の機能を有効にします。このようなエージェントやアプリケーションは、Red Hat Enterprise Linux の標準のセキュリティー機能 (例: SELinux) を使用して確実に保護してください。
- ※ 仮想化環境では、ゲストシステムの保護境界線の外部から機密データがアクセスされるリスクがより高くなります。保管されている機密データは **dm-crypt** や **GnuPG** などの暗号化ツールを使用して保護してください。ただし、暗号化キーの機密性の確保には特に注意が必要です。

## 第4章 sVirt

### 4.1. 概要

KVM 下の仮想マシンは Linux プロセスとして実装されているため、KVM は標準の Linux セキュリティーモデルを活用して分離とリソースの制御を行います。Linux カーネルには、米国国家安全保障局によって開発されたプロジェクトである SELinux (Security-Enhanced Linux) が搭載されており、柔軟性の高いカスタマイズ可能なセキュリティーポリシーを通して、強制アクセス制御 (MAC)、マルチレベルセキュリティー (MLS)、およびマルチカテゴリーセキュリティー (MCS) を追加します。SELinux は、Linux カーネル上で実行されるプロセス (仮想マシンプロセスを含む) を対象とした、リソースの厳重な分離および隔離を行います。sVirt プロジェクトは SELinux を基盤として、仮想マシンの分離と制御された共有をさらに促進します。たとえば、粒度の細かいパーミッションを適用して仮想マシンをグループ化し、リソースを共有することができます。

セキュリティーの観点からすると、ハイパーバイザーは攻撃者の格好的的対象です。これは、ハイパーバイザーがセキュリティー侵害を受けると、そのホストシステム上で実行されている全仮想マシンのセキュリティーも被害を受けることになる可能性があるためです。仮想化テクノロジーに SELinux を組み込むと、ホストシステムや他の仮想マシンへのアクセスを試みる悪意のある仮想マシンに対するハイパーバイザーのセキュリティーを強化するのに役立ちます。

以下の図は、ゲストを分離することによって、セキュリティー侵害されたハイパーバイザー (またはゲスト) がさらなる攻撃を加えたり、別のインスタンスにまで被害を拡げたりする能力を抑える仕組みを示しています。

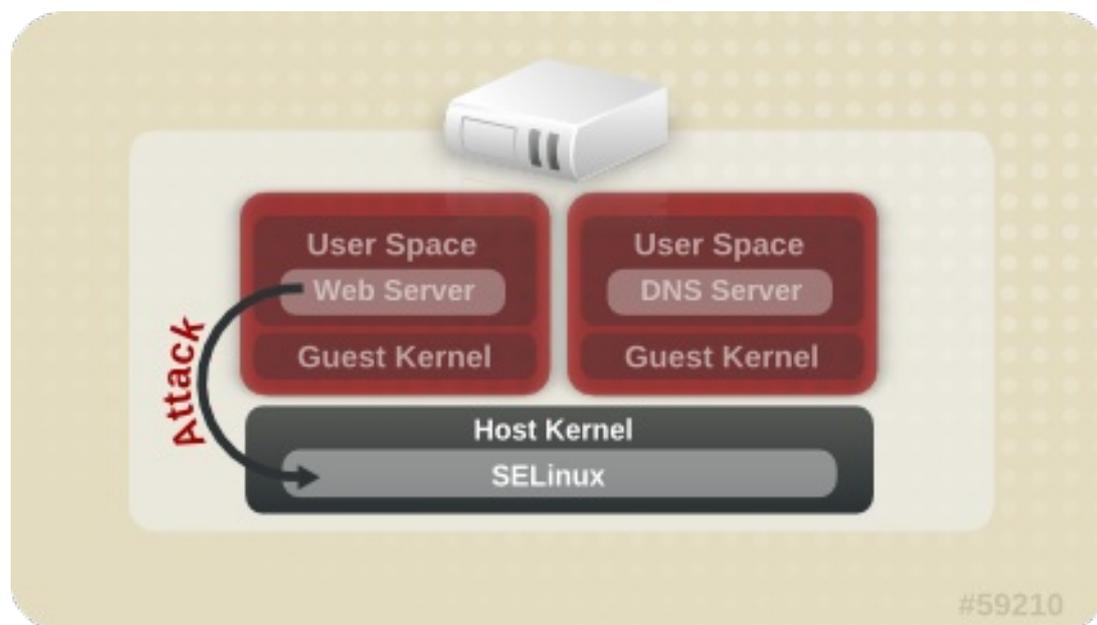


図4.1 SELinuxによって分離される攻撃パス

#### 注記

SELinux の詳細については、<https://access.redhat.com/site/documentation/> にある『Red Hat Enterprise Linux SELinux ユーザーおよび管理者のガイド』を参照してください。

### 4.2. SELinux と強制アクセス制御 (MAC)

Security-Enhanced Linux (SELinux) は、Linux カーネルにおける MAC の実装です。標準の任意アクセス制御 (DAC) がチェックされたあとに、許可された操作をチェックします。SELinux は、実行中のプロセスとそれらの動作 (例: ファイルシステムオブジェクトへのアクセスを試みるなど) に対して、ユーザーがカスタマイズ可能なセキュリティポリシーを適用することができます。Red Hat Enterprise Linux では SELinux がデフォルトで有効化されており、アプリケーションやシステムサービス (例: ハイパーバイザー) の脆弱性の悪用によって生じる可能性のある潜在的被害の範囲を制限します。

sVirt は、仮想化管理用の抽象化レイヤーである libvirt と一体化して、仮想マシン用の MAC フレームワークを提供します。このアーキテクチャーは、libvirt によってサポートされている全仮想化プラットフォームと、sVirt によりサポートされている全 MAC 実装が相互運用可能となります。

### 4.3. sVirt の設定

SELinux ブール値は、オン/オフ切り替えが可能な変数で、機能やその他の特殊条件を迅速に有効化/無効化することができます。ブール値は、一時的な変更の場合は `setsebool boolean_name {on|off}`、再起動時に変更を永続化する場合は `setsebool -P boolean_name {on|off}` のいずれかを実行することによって切り替えることができます。

以下の表は、libvirt で始動された場合に KVM に影響する SELinux ブール値を示しています。これらのブール値 (オンまたはオフ) の現在の状態は、コマンド `getsebool -a | grep virt` を実行することにより確認できます。

表4.1 KVM SELinuxのブール値

SELinuxのブール値	説明
staff_use_svirt	staff ユーザーが sVirt ドメインを作成し、それに移行することを許可します。
unprivuser_use_svirt	非特権ユーザーが sVirt ドメインを作成し、それに移行することを許可します。
virt_sandbox_use_audit	サンドボックスコンテナが監査メッセージを送信することを許可します。
virt_sandbox_use_netlink	サンドボックスコンテナがネットリンクシステム呼び出しを使用することを許可します。
virt_sandbox_use_sys_admin	サンドボックスコンテナが sys_admin システム呼び出しを使用することを許可します (例: mount)。
virt_transition_userdomain	仮想プロセスがユーザードメインとして実行されることを許可します
virt_use_comm	virt がシリアル/パラレル通信ポートを使用するのを許可します。
virt_use_execmem	制限された仮想マシンが実行可能なメモリおよび実行可能なスタックを使用することを許可します。
virt_use_fusefs	virt が FUSE マウントされたファイルを読み取るのを許可します。
virt_use_nfs	virt が NFS マウントされたファイルを管理するのを許可します。
virt_use_rawip	virt が rawip ソケットと通信することを許可します。
virt_use_samba	virt が CIFS マウントされたファイルを管理するのを許可します。
virt_use_sanlock	隔離された仮想化ゲストが sanlock と対話するのを許可します。
virt_use_usb	virt が USB デバイスを使用するのを許可します。

SELinuxのブール値	説明
virt_use_xserver	仮想マシンが X Window System と対話するのを許可します。



## 注記

SELinux ブール値の詳細については、<https://access.redhat.com/site/documentation/>にある『Red Hat Enterprise Linux SELinux ユーザーおよび管理者のガイド』を参照してください。

## 4.4. sVirt のラベル

SELinux の保護下にある他のサービスと同様に、sVirt はプロセススペースのメカニズム、ラベル、制限を使用してセキュリティを強化し、ゲストインスタンスを制御します。ラベルは、現在実行中の仮想マシンに基づいて、システム上のリソースに自動的に適用されます (動的) が、管理者が手動で指定して (静的)、特別な要件がある場合でも対応することが可能です。

### 4.4.1. sVirt ラベルのタイプ

以下の表には、仮想マシンのプロセス、イメージファイル、共有コンテンツなどのリソースに割り当てることができる、異なる sVirt ラベルについての説明をまとめています。

表4.2 sVirt ラベル

タイプ	SELinux コンテキスト	説明/効果
仮想マシンプロセス	system_u:system_r:svirt_t:MCS1	MCS1 は無作為に選択されたフィールドです。現在は、約 500,000 のラベルがサポートされています。
仮想マシンのイメージ	system_u:object_r:svirt_image_t:MCS1	これらのイメージファイルやデバイスの読み取り/書き込みができるのは、同じ MCS1 フィールドが付いた <b>svirt_t</b> プロセスのみです。
仮想マシンの共有読み取り/書き込みコンテンツ	system_u:object_r:svirt_image_t:s0	<b>svirt_t</b> プロセスはすべて、 <b>svirt_image_t:s0</b> のファイルおよびデバイスに書き込むことができます。
仮想マシンの共有読み取り専用コンテンツ	system_u:object_r:svirt_content_t:s0	<b>svirt_t</b> プロセスはすべて、このラベルが付いたファイル/デバイスを読み取ることができます。
仮想マシンのイメージ	system_u:object_r:virt_content_t:s0	イメージが存在する場合に使用されるシステムのデフォルトラベルです。 <b>svirt_t</b> 仮想プロセスは、このラベルの付いたファイル/デバイスを読み取ることはできません。

### 4.4.2. 動的設定

動的ラベル設定は、sVirt を SELinux と併用する場合のデフォルトのラベルオプションです。以下の例は、動的ラベリングを示しています。

```
# ps -eZ | grep qemu-kvm
system_u:system_r:svirt_t:s0:c87,c520 27950 ? 00:00:17 qemu-kvm
```

この例では、**qemu-kvm** プロセスに **system\_u:system\_r:svirt\_t:s0** のベースラベルが付いています。libvirt システムは、このプロセス用に一意の MCS ラベル **c87, c520** を生成しています。ベースラベルと MCS ラベルを組み合わせることにより、そのプロセス用の完全なセキュリティーラベルが形成されます。同様に、libvirt は同じ MCS ラベルとベースラベルを使用してイメージラベルを形成します。このイメージラベルは次に、ディスクイメージやディスクデバイス、PCI デバイス、USB デバイス、kernel/initr ファイルなど、仮想マシンがアクセスする必要のある全ホストファイルに自動的に適用されます。各プロセスは、異なるラベルを使用して、他の仮想マシンから分離されます。

以下の例は、**/var/lib/libvirt/images** 内のゲストディスクイメージに適用された、仮想マシンの一意のセキュリティーラベル (この場合は、対応する MCS ラベルが **c87, c520**) を示しています。

```
# ls -lZ /var/lib/libvirt/images/*
system_u:object_r:svirt_image_t:s0:c87,c520 image1
```

以下の例は、ゲストの XML 設定内の動的ラベルを示しています。

```
<seclabel type='dynamic' model='selinux' relabel='yes'>
  <label>system_u:system_r:svirt_t:s0:c87,c520</label>
  <imagelabel>system_u:object_r:svirt_image_t:s0:c87,c520</imagelabel>
</seclabel>
```

#### 4.4.3. ベースラベルを使用した動的設定

デフォルトのダイナミックモードのベースセキュリティーラベルを上書きするには、以下の例に示したように、XML ゲスト設定内の **<baselabel>** オプションを手動で設定することができます。

```
<seclabel type='dynamic' model='selinux' relabel='yes'>
  <baselabel>system_u:system_r:svirt_custom_t:s0</baselabel>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
  <imagelabel>system_u:object_r:svirt_image_t:s0:c87,c520</imagelabel>
</seclabel>
```

#### 4.4.4. 動的リソースラベルを使用した静的設定

一部のアプリケーションは、セキュリティーラベルの生成を完全に制御する必要がありますが、リソースラベル付けは依然として libvirt が行う必要があります。以下のゲスト XML 設定は、動的リソースラベルを使用した静的設定の例を示しています。

```
<seclabel type='static' model='selinux' relabel='yes'>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
</seclabel>
```

#### 4.4.5. リソースラベルを使用しない静的設定

MLS (マルチレベルセキュリティー) または厳重に管理された環境で主に使用される、リソース再ラベルを使用しない静的設定が可能です。静的ラベルにより管理者は、仮想マシン用に MCS/MLS フィールドなど特定のラベルを選択することができます。静的なラベルが付いた仮想マシンを実行する管理者は、イメージファイルに正しいラベルを設定する責任を担います。仮想マシンは常にそのラベルで起動し、sVirt システムは静的なラベルの付いた仮想マシンのコンテンツは決して変更しません。以下のゲスト XML 設定は、このシナリオの例を示しています。

```
<seclabel type='static' model='selinux' relabel='no'>  
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>  
</seclabel>
```

## 第5章 仮想化環境におけるネットワークセキュリティ

### 5.1. ネットワークセキュリティの概要

大半の状況では、ネットワークはシステム、アプリケーション、管理インターフェースへの唯一のアクセス方法です。ネットワークは、仮想化システムの管理とそれらのシステムでホストされているアプリケーションの可用性において極めて重要な役割を果たすので、仮想化システムとデータをやり取りするネットワークチャネルをセキュアな状態に確保することは非常に重要です。

ネットワークのセキュリティ保護により、管理者は機密データのアクセスを制御して、情報の漏えいやびざんから保護することができます。

### 5.2. ネットワークセキュリティ推奨プラクティス

ネットワークセキュリティはセキュアな仮想化インフラストラクチャーの重要な要素です。ネットワークのセキュリティ保護については、以下の推奨プラクティスを参照してください。

- ※ システムのリモート管理はすべてセキュアなネットワークチャネル上のみで実行されるようにしてください。SSHのようなツールや、TLS または SSL などのネットワークプロトコルは認証とデータ暗号化の両方を提供し、システムへのセキュアなアクセスとその制御を行います。
- ※ ゲストアプリケーションによる機密データの転送はセキュアなネットワークチャネルで行われるようにします。TLS や SSL などのプロトコルが利用できない場合には、IPsec などを使用することを検討してください。
- ※ ファイアウォールを設定して、ブート時にアクティブ化されるようにします。システムの使用と管理に必要なネットワークポートのみを許可してください。ファイアウォールルールの定期的なテストと確認を行なってください。

#### 5.2.1. SPICE への接続のセキュリティ保護

SPICE リモートデスクトッププロトコルは SSL/TLS をサポートしています。これは、SPICE のすべての通信チャネル (main、display、inputs、cursor、playback、record) で有効化する必要があります。

#### 5.2.2. ストレージへの接続のセキュリティ保護

仮想化システムのネットワークストレージへの接続は、さまざまな方法で行うことができます。各アプローチにはセキュリティ上のさまざまな利点と懸念点がありますが、セキュリティ上の同一の原則がそれぞれに適用されます。使用前にはリモートのストアプールを認証し、転送中のデータの機密性と整合性を保護します。

データは保管時にもセキュアな状態を維持する必要があります。Red Hat は、データを保管する前に暗号化および/またはデジタル署名することを推奨しています。

#### 注記

ネットワークストレージの詳細については、<https://access.redhat.com/site/documentation/> にある『Red Hat Enterprise Linux 仮想化の導入および管理ガイド』の章「ストレージプール」を参照してください。

## 付録A 追加情報

### A.1. SELinux および sVirt

SELinux および sVirt に関する詳細情報:

- ※ SELinux のメイン Web サイト: <http://www.nsa.gov/research/selinux/index.shtml>
- ※ SELinux のドキュメンテーション: <http://www.nsa.gov/research/selinux/docs.shtml>
- ※ sVirt のメイン Web サイト: <http://selinuxproject.org/page/SVirt>
- ※ Dan Walsh 氏のブログ: <http://danwalsh.livejournal.com/>
- ※ 非公式の SELinux FAQ: <http://www.crypt.gen.nz/selinux/faq.html>

### A.2. 仮想化セキュリティー

仮想化セキュリティーに関する追加情報

- ※ NIST (National Institute of Standards and Technology) 完全仮想化セキュリティーガイドライン: <http://www.nist.gov/itl/csd/virtual-020111.cfm>

## 付録B 改訂履歴

改訂 1.0-8.2 translation completed	Thu Sep 3 2015	Takuro Nagamoto
改訂 1.0-8.1 翻訳ファイルを XML ソースバージョン 1.0-8 と同期	Thu Sep 3 2015	Takuro Nagamoto
改訂 1.0-8 7.1 GA リリース向けのバージョン	Wed Feb 18 2015	Scott Radvan
改訂 1.0-6 スプラッシュページを更新し、新しい sort_order を実装	Mon Dec 08 2014	Scott Radvan
改訂 1.0-5 RHEL 7.1 Beta リリースの公開	Fri Dec 05 2014	Scott Radvan
改訂 1.0-4 推奨ホストに対する物理機能のセキュリティー脆弱性に関する警告を追加	Mon Oct 13 2014	Scott Radvan
改訂 1.0-3 7.0 GA リリース向けバージョン	Mon June 2 2014	Tahlia Richardson
改訂 1.0-2 スタイル変更のための再ビルド	Thurs May 8 2014	Tahlia Richardson
改訂 0.1-7 SELinux ブール値の表をセグメントリストから表に適切に変換 『Red Hat Enterprise Linux Security-Enhanced Linux』の記述を新しいタイトルである『SELinux ユーザーおよび管理者のガイド』に更新 <a href="#">BZ#1065819</a> からの他の修正	Thursday Feb 27 2014	Tahlia Richardson
改訂 0.1-6 2.2.1 の 2 番目の箇条書きを書き換え 章 2.2 に推奨事項を追加 イメージを図としてマークアップ <a href="#">BZ#1061513</a> からの他の修正	Wednesday Feb 26 2014	Tahlia Richardson
改訂 0.1-5 <a href="#">BZ#1061513</a> からのフィードバックに基づいて RHEV ネットワークポートを更新	Tues Feb 11 2014	Tahlia Richardson
改訂 0.1-4 章「SVirt 設定」の表にブール値を追加 ( <a href="#">BZ#1058565</a> ).	Thurs Jan 30 2014	Tahlia Richardson
改訂 0.1-3 更新されたドキュメントスイートリストで公開	Thurs Nov 14 2013	Tahlia Richardson
改訂 0.1-2 内部プレビューサイトへ送信。バージョン 7 向け初期ビルド	Wed Jan 23 2013	Scott Radvan
改訂 0.1-1	Thu Jan 17 2013	Scott Radvan

---

ドキュメントの Red Hat Enterprise Linux 6 バージョンからブランディング