



# Red Hat 認定クラウドとサービスプロバイダーの認定 1.0

## クラウドイメージ認定ポリシーガイド

Red Hat Certified Cloud and Service Provider 1.0 向け



# Red Hat 認定クラウドとサービスプロバイダーの認定 1.0 クラウドイメージ認定ポリシーガイド

---

Red Hat Certified Cloud and Service Provider 1.0 向け

## 法律上の通知

Copyright © 2017 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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, OpenShift, 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

本ガイドでは、Red Hat Enterprise Linux ベースの Infrastructure-as-a-Service (IaaS) を提供する CCSP パートナーの技術および運用上の認定要件について説明します。

---

目次

<b>第1章 はじめに</b> .....	<b>3</b>
1.1. 対象読者	3
1.2. 認定の使用による共同のお客様への価値の創造	3
1.3. テストスイートのバージョン	3
<b>第2章 RED HAT 認定セルフチェック</b> .....	<b>4</b>
2.1. RED HAT 認定セルフチェック (RHCERT/SELF CHECK)	4
2.2. SOSREPORT (システムレポート)	4
<b>第3章 サポート対応</b> .....	<b>5</b>
3.1. サポート対応の概要	5
3.2. カーネル	5
3.3. カーネルモジュール	5
3.4. サポートされていないハードウェア	5
3.5. ハイパーバイザー	6
3.6. ルートファイルシステム	6
3.7. アーキテクチャー	6
3.8. インストールされた RPM	6
3.9. ソフトウェアリポジトリ	7
<b>第4章 イメージ設定</b> .....	<b>8</b>
4.1. イメージ設定の概要	8
4.2. デフォルトのシステムロギング	8
4.3. ネットワーク設定	8
4.4. デフォルト OS ランレベル	9
4.5. システムサービス	9
4.6. サブスクリプションサービス	9
<b>第5章 セキュリティー対策</b> .....	<b>11</b>
5.1. セキュリティー対策の概要	11
5.2. パスワード設定	11
5.3. RPM が最新であること	11
5.4. SELINUX の強制施行	11
<b>第6章 詳細情報</b> .....	<b>12</b>
6.1. 参考資料	12



# 第1章 はじめに

## 1.1. 対象読者

本ガイドでは、Red Hat Enterprise Linux ベースの Infrastructure-as-a-Service (IaaS)、Platform-as-a-Service (PaaS)、または管理サービスを提供する CCSP パートナー向けに実施されている技術および運用上の認定要件について説明します。認定ツールおよび認定方法は Red Hat Enterprise Linux にビルドされるクラウドアプリケーションイメージをその対象としています。

## 1.2. 認定の使用による共同のお客様への価値の創造

認定クラウドおよびサービスプロバイダー (Certified Cloud and Service Provider: CCSP) は、カタログで公開されるイメージを認定する必要があります。この認定プロセスには、Red Hat のお客様に対し、各種のクラウドプロバイダー間での一貫したエクスペリエンスと共に、最高レベルのサポートおよび優れたセキュリティ対策を利用できることを保証をするための一連のテストが含まれます。

クラウド認定テストスイート (redhat-certification-cloud) には、(supportable (サポート対応)、configuration (設定)、security (セキュリティ) の 3 つのテストが含まれ、それぞれには以下で説明する一連のサブテストとチェックが含まれます。テストの実行方法についての詳細は、[CCSP 認定ユーザーガイド](#) を参照してください。

新規の認定および再認定を受けるには、これら 3 つのクラウドテストすべてとテストスイートのセルフチェックテスト (rhcert/selfcheck) を単一実行したときに記録されたログを Red Hat に提出する必要があります。

ほとんどのクラウド認定サブテストは即時にステータス (Pass/Fail) を返しますが、一部のサブテストは合格を確認するために Red Hat の詳細レビューが必要になることがあります。これらのテストについては、Red Hat 認定アプリケーションで REVIEW ステータスのマークが付けられます。

またテストによっては、潜在的な問題を特定し、WARN ステータスを返すこともあります。このステータスはベストプラクティスが実施されていないことを示唆します。WARN ステータスのマークの付いたテストは注意またはアクションを喚起しますが、認定の結果には影響しません。パートナーの皆様には、これらの警告に含まれる情報に基づいてテストの出力を確認し、適切なアクションを取ることをお勧めします。

## 1.3. テストスイートのバージョン

パートナーの皆様には、最新の認定ツールをインストールして、認定プロセスの最新のワークフローを使用していただく必要があります。新バージョンの認定ツールがリリースされてから 90 日間は、Red Hat は以前のバージョンのツールとワークフローをサポートします。

この 90 日間が過ぎると、以前のバージョンで生成されたテストログ/結果は自動的に拒否され、パートナー様は最新のツールをワークフローを使用してテストログ/結果を再生成することが求められます。

最新バージョンの認定ツールおよびワークフローは (デフォルトで) Red Hat サブスクリプション管理から入手可能となっており、[CCSP ワークフローガイド](#) にその説明があります。

## 第2章 RED HAT 認定セルフチェック

### 2.1. RED HAT 認定セルフチェック (RHCERT/SELFCHK)

**rhcert/selfcheck** と呼ばれる Red Hat 認定セルフチェックテストは、認定プロセスで必要となる全ソフトウェアパッケージがインストールされ、それらが変更されていないことを確認します。これにより、認定プロセス向けにテスト環境の準備が整っており、全認定ソフトウェアパッケージがサポート可能であることが確認できます。



#### 注記

これらの認定パッケージは、認定テスト目的またはその他の目的で変更しないでください。

#### 合格するための判断基準

テスト環境に全プロセスで必須の全パッケージが含まれており、パッケージが修正されていない。

### 2.2. SOSREPORT (システムレポート)

**cloud/sosreport** と呼ばれる **sosreport** テストは、基本の **sosreport** をキャプチャーします。

Red Hat は **sos** と呼ばれるツールを使用して RHEL システムから設定および診断情報を収集し、お客様のシステムのトラブルシューティングや、推奨プラクティスの準拠をお手伝いします。システムレポートのサブテストは、**sos** ツールがイメージ/システム上で予想どおりに機能し、基本的な **sosreport** をキャプチャーすることを確認します。**sosreport** についての詳細は、<https://access.redhat.com/ja/solutions/78443> を参照してください。

#### 合格するための判断基準

基本的な **sosreport** をイメージ上でキャプチャーできる。



#### 注記

SOSReport は出力をアーカイブに保存します。認定やシステムの他の問題をデバッグする間に参照として使用することができます。



## 第3章 サポート対応

### 3.1. サポート対応の概要

サポート対応テストは **cloud/supportable** (クラウド/サポート対応) としても知られており、Red Hat によるイメージのサポートが可能であることを保証します。このテストにより、イメージが Red Hat カーネルおよびユーザー空間ソフトウェアで構成され、Red Hat のサポート対応のある環境で実行され、かつイメージに Red Hat の更新および修正へのアクセスが含まれることを確認できます。

**cloud/supportable** (クラウド/サポート対応) テストには以下のサブテストが含まれます。

### 3.2. カーネル

カーネルのサブテストは、イメージが実行しているカーネルが Red Hat のカーネルであり、認定対象の RHEL バージョンに対応するバージョンであること、またこのカーネルが変更されていないことを確認します。カーネルのバージョンには元の GA (General Availability) バージョンか、またはその後に RHEL メジャーおよびマイナーリリース向けにリリースされたカーネルのエラータを使用することができます。Red Hat Enterprise Linux のライフサイクルおよびカーネルバージョンに関する詳細は、[Red Hat Enterprise Linux のライフサイクル](#) および [Red Hat Enterprise Linux のリリース日と収録カーネルの一覧](#) を参照してください。

カーネルのサブテストでは、カーネルが環境での実行中に汚染されていないことも確認します。カーネルの汚染についての詳細は、[カーネルが「tainted」となるのはなぜですか? taint 値はどのように解釈されますか?](#) を参照してください。

合格するための判断基準:

- 実行中のカーネルは Red Hat カーネルである。
- 実行中のカーネルは RHEL バージョンで使用するために Red Hat によってリリースされている。
- 実行中のカーネルは汚染されていない。

### 3.3. カーネルモジュール

カーネルモジュールのサブテストは、ロードされたカーネルモジュールが、実行中のカーネルのパッケージか、または Red Hat Driver Update ([Where can I download Driver Update Program \(DUP\) disks?](#)を参照) のいずれかの Red Hat のモジュールであることを確認します。また、カーネルモジュールのサブテストでは、カーネルモジュールが環境での実行時にテクノロジープレビューとして特定されないことを確認します ([「テクノロジープレビュー」機能とはどんな機能ですか?](#)を参照)。

合格するための判断基準:

カーネルモジュールは Red Hat 提供のモジュールであり、サポートされている。

### 3.4. サポートされていないハードウェア

Red Hat カーネルがサポートされていないハードウェアを特定しないことを確認します。これにより、Red Hat 製品をサポートされていない設定や環境で実行することから生じるお客様のプロダクション環境のリスクを防ぐことができます。カーネルは各種の理由によりサポート対応とみなされないハードウェアを認識します。カーネルがこのようなハードウェアを特定すると、システムログにサポートされていないハードウェアのメッセージを出力するか、またはカーネル汚染についてトリガーします。

RHEL を認定ハードウェアにインストールし、実行することをお勧めします。RHEL 6 および RHEL 7 向けに認定されたハードウェアの詳細の一覧については、[Red Hat Ecosystem Catalog](#) を参照してください。

#### 合格するための判断基準:

カーネルによってサポートされていないハードウェアが特定されない。

### 3.5. ハイパーバイザー

イメージが Red Hat Enterprise Linux の実行が認定されているハイパーバイザーで実行されることを確認します。これにより、Red Hat 製品をサポートされていない環境で実行することから生じるお客様のプロダクション環境のリスクを防ぐことができます。

#### 合格するための判断基準:

イメージは Red Hat Enterprise Linux のバージョンの実行が認定されているハイパーバイザーで実行される必要があります。認定ハイパーバイザーについての詳細は、[Red Hat Enterprise Linux の実行が認定されているハイパーバイザー](#)を参照してください。

### 3.6. ルートファイルシステム

ルートファイルシステムのタイプおよびイメージの最小サイズが各 RHEL リリースのガイドラインに従っていることを確認します。これにより、イメージに適切な稼働、アプリケーションの実行、およびお客様向けのアップグレードのインストールの実行に必要なスペース容量が十分にあることを確認できます。

#### 合格するための判断基準:

- RHEL 6: RHEL 6.x のルートファイルシステムのサイズが ext4 または ext3 でフォーマットされたパーティションで 6GB 以上である。
- RHEL 7: RHEL 7.x のルートファイルシステムのサイズが xfs または ext4 でフォーマットされたパーティションで 10GB 以上である。

### 3.7. アーキテクチャー

RHEL イメージで表示されるホストアーキテクチャーが RHEL、CCSP プログラムおよびカーネルでサポートされていることを確認します。現在、CCSP イメージ認定は RHEL6 の x86 および x86\_64 アーキテクチャーと、RHEL 7 の x86\_64 アーキテクチャーで提供されています。

#### 合格するための判断基準:

- RHEL 6: RHEL 6.x のホストアーキテクチャーは x86 または x86\_64。
- RHEL 7: RHEL 7.x のホストアーキテクチャーは x86\_64。

### 3.8. インストールされた RPM

システムにインストールされている RPM パッケージが未変更の Red Hat のパッケージであり、予期しないソフトウェアまたはパッケージから生じる重大なリスクをお客様が予防できる可能性を確認します。さらに、お客様がサポート対応可能な環境で開始することを確認します。

Red Hat 以外のパッケージをインストールできるのは、それらがクラウド環境を有効にするために必要であり、それらが文書化されていること、および Red Hat パッケージ/ソフトウェアを変更したり、こ

れらと競合しないことを条件として受け入れ可能である場合です。このサブテストには、Red Hat 以外のパッケージがインストールされている場合の合格/不合格の確認が行われる Red Hat の詳細レビューが必要になります。

サードパーティーソフトウェアの Red Hat サポートポリシーについては、[製品サポートの対象範囲](#)を参照してください。

#### 合格するための判断基準:

- インストールされた Red Hat 提供の RPM パッケージはオフリングで利用可能な Red Hat 製品の RPM パッケージである。
- インストールされた Red Hat RPM パッケージは変更されていない。
- インストールされた Red Hat 以外の RPM パッケージはクラウド環境を有効にするために必要であり、文書化されている。
- インストールされた Red Hat 以外の RPM パッケージは、オフリングに含まれる Red Hat 製品で利用可能な Red Hat 提供パッケージ/ソフトウェアと競合しない。

### 3.9. ソフトウェアリポジトリ

関連する Red Hat リポジトリ が設定されており、GPG キーがイメージにインポート済みでサポートされていないコンテンツから生じる可能性のある大きなリスクを回避できることを確認します。Red Hat は Red Hat の公式ソフトウェアリポジトリ (アタッチされるサブスクリプションに含まれる) でコアとなるソフトウェアパッケージ/コンテンツを提供します。これらのリポジトリは配信ファイルの信頼性を確認するために GPG キーで署名されます。これらのリポジトリの一部として提供されるソフトウェアはお客様のプロダクション環境用に完全にサポートされ、信頼性があります。詳細は、[製品サポートの対象範囲](#)を参照してください。

EPEL または [Optional](#) および [Supplementary チャンネル](#) などの Red Hat が公開するが、サポートしている訳ではないリポジトリ、および Red Hat 以外のリポジトリは、クラウド環境を有効にするために必要であり、かつ適正に文書化され、承認されていることを条件として設定することができます。

#### 合格するための判断基準:

- サポートされている Red Hat リポジトリが設定されている。
- Red Hat リポジトリの GPG キーはイメージにインポート済みである。
- イメージに設定される Red Hat リポジトリはイメージのコンテンツと一致している。
- Red Hat 以外のリポジトリはクラウドの適切な操作に必要な場合に設定されており、文書化されている。

## 第4章 イメージ設定

### 4.1. イメージ設定の概要

イメージ設定のテストは **cloud/configuration (クラウド/設定)** としても知られ、お客様が統合環境の複数のクラウドプロバイダーとイメージ間で統一し、一貫性のあるエクスペリエンスを確保できるようイメージが Red Hat 標準に従って設定されていることを確認します。

**cloud/configuration (クラウド/設定)** テストには以下のサブテストが含まれます。

### 4.2. デフォルトのシステムロギング

デフォルトのシステムロギングサービス (syslog) がイメージの **/var/log/** ディレクトリーにログを保存し、必要に応じて問題をすばやく解決できるように設定されていることを確認します。

#### 合格するための判断基準:

基本的なシステムロギングはイメージ上の **/var/log/** ディレクトリーに保存されます。

### 4.3. ネットワーク設定

デフォルトのファイアウォールサービス (iptables) が実行中であること、SSHD が実行中の状態でポート 22 が開いていること、ポート 80 と 443 が開いているか、または閉じていること、さらにその他のすべてのポートが閉じていることをネットワーク設定が確認します。これにより、イメージは既知のアクセス設定によってデフォルトで不正アクセスから保護されます。

また、お客様がイメージに SSH でアクセスでき、追加の設定なしに HTTP アプリケーションをすぐにデプロイできることを確認します。このイメージでは、他のポートを開くこともできますが、その場合は、それらがクラウドインフラストラクチャーの適切な操作に必要であること、またそれらのポートについて文書化されることを条件とします。

このテストは、ポート 22、80 (オプション)、443 (オプション) がイメージ上で開いている場合にのみランタイム時にステータス (Pass) を表示します。他のポートが開いている場合、Red Hat が合格または失敗の確認を行うため、開かれているポートの詳細を要求します。



#### 注記

認定プロセスの一環として、Red Hat 認定アプリケーションはデフォルトで、ポート 8009 で実行されます。Red Hat 認定アプリケーションは認定テスト時に別の開いたポートで実行することもできますが、このポートはテスト時にのみ開き、イメージの設定ではデフォルトで開かないようにすることが推奨されます。

#### 合格するための判断基準:

- IPtables/firewalld が有効で、実行されている。
- sshd が有効で、ポート 22 で実行され、アクセス可能である。
- 開いているその他のポートは、クラウドインフラストラクチャーを適切に操作する必要がある、文書化されている必要がある。
- Red Hat 認定アプリケーションはポート 8009 (または設定される他のポート) で実行中である。
- その他のポートはすべて閉じられている。

**注記**

httpd サービスは許可されるが、ポート 80 や 443 で実行される必要はない。

## 4.4. デフォルト OS ランレベル

現行のシステムランレベルが 3、4 または 5 であることを確認します。このサブテストでは、イメージが必要なすべてのシステムサービス (例: ネットワーキング) が実行中の状態で、必要なモード/状態で実行されていることを確認します。

RHEL 6 および RHEL 7 のランレベルについての詳細は、以下を参照してください。

- RHEL 6 導入ガイド: [デフォルトのランレベルの設定](#)
- RHEL 7 Systems Administrator's Guide: [Working with systemd Targets](#)

**合格するための判断基準:**

現在のランレベルは 3、4 または 5 である。

## 4.5. システムサービス

システムサービスは、root ユーザーがシステム上でサービスを開始し、停止できることを確認します。これにより、システム管理権限を持つお客様がシステム上でアプリケーションおよびサービスにアクセスし、これらを使用できること、また管理者アクセスを必要とするすべてのタスクをシームレスに実行できることを確認できます。また、インストールされたシステムサービスの設定された状態と実際の状態に違いが生じないようにします。

必要な権限を取得する方法についての詳細は、以下を参照してください。

- RHEL 6 導入ガイド: [https://access.redhat.com/documentation/ja-JP/Red\\_Hat\\_Enterprise\\_Linux/6/html/Deployment\\_Guide/chap-Deployment\\_Guide-Gaining\\_Privileges.html](https://access.redhat.com/documentation/ja-JP/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/chap-Deployment_Guide-Gaining_Privileges.html)
- RHEL 7 Deployment Guide: [https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/7-Beta/html-single/System\\_Administrators\\_Guide/index.html#chap-Gaining\\_Privileges](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7-Beta/html-single/System_Administrators_Guide/index.html#chap-Gaining_Privileges)

**合格するための判断基準:**

- root ユーザーは、Red Hat 製品が提供するシステムサービスの開始および終了を実行できます。
- インストールされたすべてのシステムサービスでは、実際の状態が設定された状態と一致する必要があります。たとえば、サービスが有効な場合、実行中の状態である必要があります。

## 4.6. サブスクリプションサービス

必要な Red Hat サブスクリプションが設定済みで、イメージ上で利用可能および機能していること、また更新メカニズムとして Red Hat Satellite または RHUI を使用できることを確認します。これにより、お客様は、標準的な Red Hat パッケージ更新または配信メカニズムを使用して、アプリケーションのサポートに必要なパッケージおよび更新へアクセスできます。

**合格するための判断基準:**

イメージは設定されており、Red Hat Satellite または RHUI サブスクリプション管理サービスのいずれかからパッケージをダウンロードし、インストールし、アップグレードできる。

## 第5章 セキュリティー対策

### 5.1. セキュリティー対策の概要

セキュリティー対策のテストは **cloud/security** (クラウド/セキュリティー) としても知られ、イメージが最小限の標準セキュリティー対策に従っていることを確認します。また、最新の Red Hat セキュリティー更新がインストールされていることを確認します (ただし現時点でこの確認は不要です)。

**cloud/configuration** (クラウド/設定) テストには以下のサブテストが含まれます。

### 5.2. パスワード設定

ユーザーパスワード設定に RHEL 6 および 7 用の証明書または SHA-512 が使用されていることを確認します。これにより、イメージがセキュリティーの最適化のために標準の暗号/暗号解除メカニズムに基づいていることを確認できます。

#### 合格するための判断基準:

ユーザー認証は RHEL 6 および 7 用の証明書または SHA-512 に基づいて設定される必要があります。

### 5.3. RPM が最新であること

イメージに含まれる Red Hat パッケージに対してリリースされるすべての重要および重大なセキュリティーエラータがインストールされていることを確認します。Red Hat はパートナーの皆様に対し、エラータのリリース時にはいつでもイメージの更新および再認定を実行することを奨励します。このテストは、Red Hat による合格または不合格の確認レビューが必要となるため、ランタイム時にステータス (REVIEW) を表示します。Red Hat におけるセキュリティーレベルについての詳細は、<https://access.redhat.com/ja/security/updates/classification> を参照してください。

#### 合格するための判断基準:

インストール済みの Red Hat パッケージ用にリリースされたすべての重要および重大なセキュリティーエラータは最新である。

### 5.4. SELINUX の強制施行

SELinux がイメージ上で enforcing モード (推奨) または permissive モードで実行されていることを確認します。SELinux (Security-Enhanced Linux) は MAC (Mandatory Access Control) を Linux カーネルに追加し、Red Hat Enterprise Linux にてデフォルトで有効にされます。

SELinux ポリシーは管理者が定義し、システム全体にわたって強制されるもので、ユーザーの判断で設定されるものではありません。これにより、権限昇格攻撃の脆弱性が軽減し、設定上のミスによる損害が制限されます。あるプロセスが危険にさらされても、攻撃者がアクセスできるのはそのプロセスの通常の機能とそのプロセスが設定上アクセスできるファイルのみになります。

RHEL の SELinux についての詳細は、以下を参照してください。

- RHEL 6 [Security Enhanced Linux](#)
- RHEL 7 [SELinux ユーザーおよび管理者のガイド](#)

#### 合格するための判断基準:

SELinux は設定済みであり、イメージ上で enforcing モード (優先モード) または permissive モードで実行されている。

## 第6章 詳細情報

### 6.1. 参考資料

Red Hat 認定クラウドおよびサービスプロバイダープログラム、またはRed Hat 認定クラウドおよびサービスプロバイダー認定に関する詳細情報は、以下のドキュメント/ページを参照してください。

- [Red Hat Connect for Business Partners](#)
- [Red Hat 認定クラウドおよびサービスプロバイダー認定ポリシーガイド](#)
- [Red Hat 認定クラウドおよびサービスプロバイダー認定ワークフローガイド](#)