

# RHEL を定期的にアップデートする 際の課題と対策

2018-04-20

Red Hat K.K. Solution Architect

森若和雄

# このスライドの位置づけ

- 対象 : RHEL を運用している管理者の方
- 目的 : RHEL を定期的にアップデートする際に何が課題になるかと、課題に対して利用できる仕組みとして何があるかを紹介する

# 概要

- RHEL でも定期的なアップデートは必須
- Red Hat Enterprise Linux だけでここまでできる
- Red Hat Insights があると……？
- Red Hat Satellite があると……？
- Red Hat Ansible Automation があると……？

# RHEL でも 定期的なアップデートは必須です

- Windows Server は定期的にアップデートしてますよね
  - 毎月？ 3ヶ月おき？
- 同じことを RHEL だとやっていない・できていない  
お客様が沢山います
  - 「インストールした時点の最新で」 「はい」  
「5年経ちました……」 「はい……」
- **RHEL でも定期的なアップデートは必須**です

# アップデートを実施する際の課題

- **更新情報を含むインベントリ管理**：適用すべき修正がどのシステムにどれだけ存在しているか、作業に抜け漏れはないか
- **優先順位の設定**：どのアップデートはすぐ対応すべきか、どのアップデートは定期更新でいいのか
- **更新パッケージの入手**：インターネットに接続していない場合はどうやって入手するのか
- **リポジトリのバージョン管理**：テスト環境でテストしたパッケージだけを本番環境で利用したい
- **複雑な更新手順の実施**：アップデート手順が複雑なので実施に必要な工数が大きすぎる

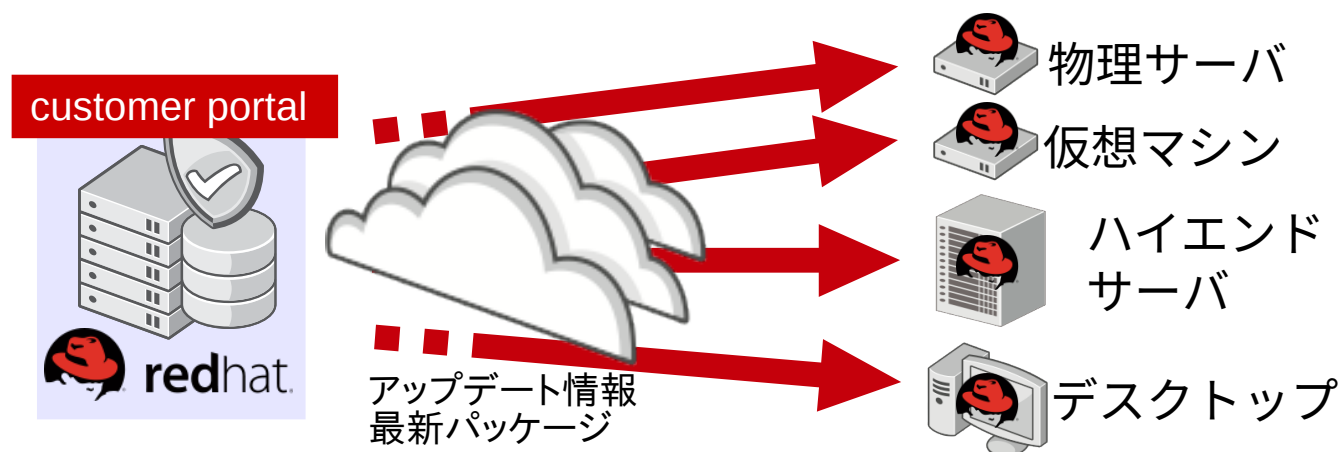
# Red Hat Enterprise Linux **だけで** **ここまでできる**

# 課題：インベントリ管理

- 現状把握や作業の抜け漏れ予防のためインベントリ管理は必須
  - システムそれぞれにどのパッケージが含まれているか
  - 適用すべき修正がどのシステムにどれだけ存在しているか
- Red Hat Customer Portal
  - 登録したシステムに対して適用可能な errata 一覧やサマリを表示
  - 登録したシステムに該当する新しい errata が出荷されるとメールで通知

# Customer Portal によるインベントリ管理

Customer Portal はインベントリ情報として各システムの基本的な情報と導入されている製品・パッケージの情報を管理。登録したシステムでは yum コマンドによりパッケージそのものと、errata などのメタデータを取得できる。





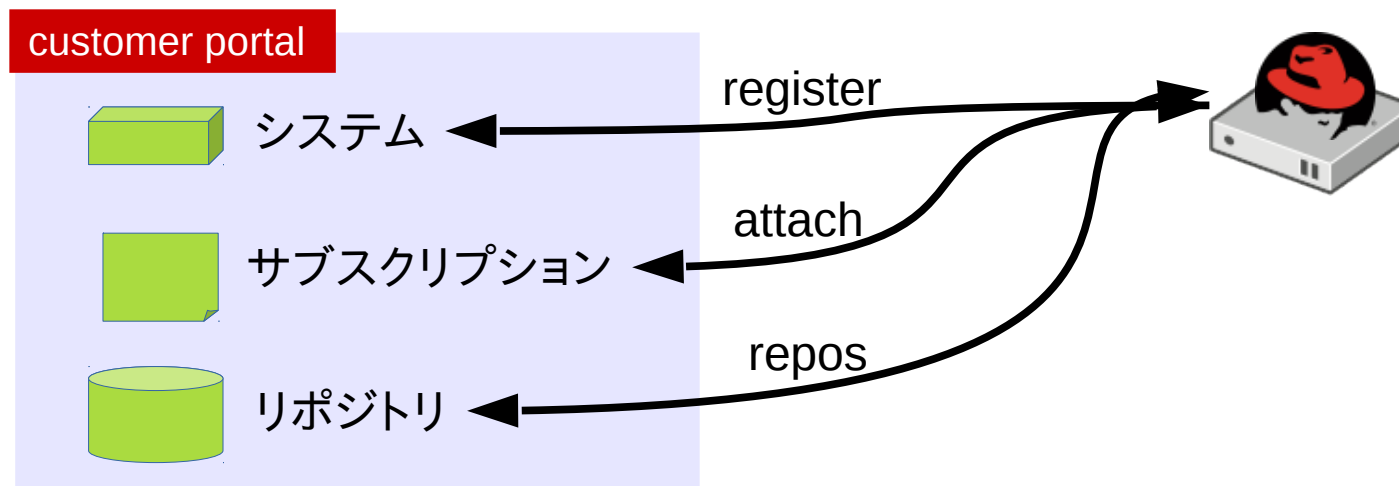
# subscription-manager での登録

subscription-manager はシステム、サブスクリプション、リポジトリの登録・対応づけを管理するコマンド。

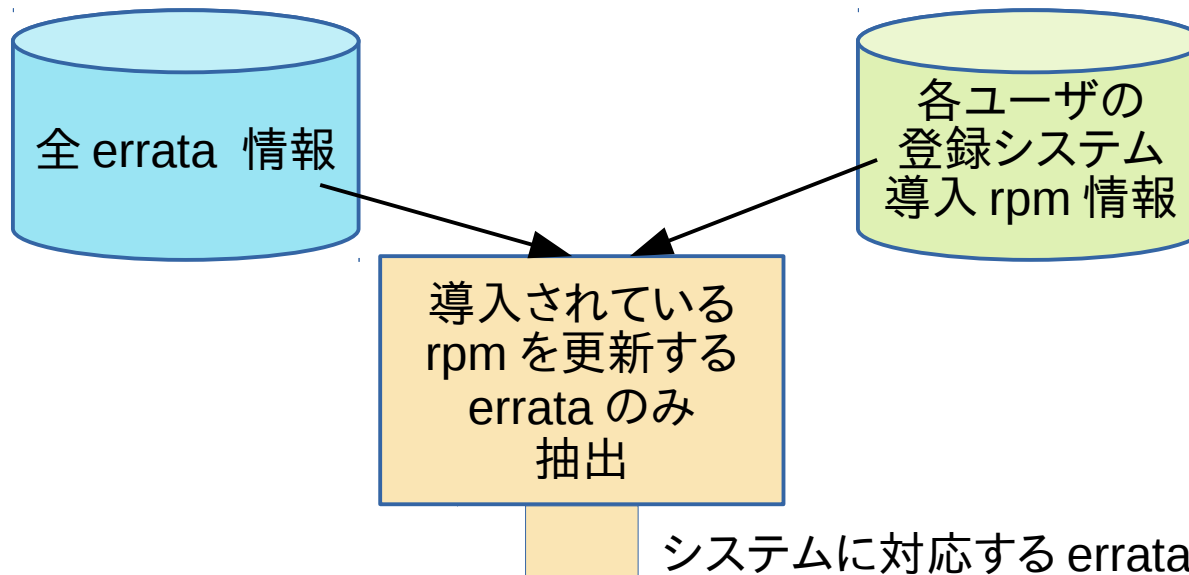
# subscription-manager register → システムを登録

# subscription-manager attach → システムにサブスクリプションを対応づけ

# subscription-manager repos → リポジトリの利用有無を設定



# 対応する errata だけを表示 / 通知



概要 サブスクリプション システム Satellite 組織 コントラクト Errata アクティベーションキー

Errata

以下は、お使いのシステムに影響のある関連のエラーター一覧です。エラータの通知管理

ここに入力して絞り込み

すべて 機能拡張 バグ修正 セキュリティアドバイザリー 重大度での絞り込み: 重大

アドバイザリー	タイプ/優先度	概要	影響を受けるシステム	公開日
RHSA-2017:3247	セキュリティアドバイザリー (重大)	Critical: firefox security update	6	2017-11-17
RHSA-2017:2998	セキュリティアドバイザリー (重大)	Critical: java-1.8.0-openjdk security update	4	2017-10-20
RHSA-2017:2836	セキュリティアドバイザリー (重大)	Critical: dnsmasq security update	7	2017-10-02
RHSA-2017:2837	セキュリティアドバイザリー (重大)	Critical: dnsmasq security update	1	2017-10-02

Web で表示

[Security Advisory] RHSA-2017:3071 Moderate: ntp security update

Red Hat Errata Notifications <errata@redhat.com> 10/17/2017 10:10 AM  
to me

The following Red Hat Security Advisory has been published which may affect packages you have installed on your system.

RHSA-2017-3071 Moderate: ntp security update

Summary:

An update for ntp is now available for Red Hat Enterprise Linux 6.

Red Hat Product Security has rated this update as having a security impact of Moderate. For more details on the Red Hat Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating,

メールで通知

# customer portal での errata 確認

概要 サブスクリプション システム Satellite 組織 コントラクト **Errata** アクティベーションキー 新機能

## Errata

以下は、お使いのシステムに影響のある関連のエラーター一覧です。 [エラータの通知管理](#)

ここに入力して絞り込み

すべて 機能拡張 章 バグ修正 **🔒 セキュリティーアドバイザリー**

重大度での絞り込み: 🔒 重大

errata の種類と重要度で絞り込み

アドバイザリー	タイプ/重大度	概要	影響を受けるシステム	公開日
<a href="#">RHSA-2017:3247</a>	🔒 セキュリティーアドバイザリー (重大)	Critical: firefox security update	6	2017-11-17
<a href="#">RHSA-2017:2998</a>	🔒 セキュリティーアドバイザリー (重大)	Critical: java-1.8.0-openjdk security update	4	2017-10-20
<a href="#">RHSA-2017:2836</a>	🔒 セキュリティーアドバイザリー (重大)	Critical: dnsmasq security update	7	2017-10-02
<a href="#">RHSA-2017:2837</a>	🔒 セキュリティーアドバイザリー (重大)	Critical: dnsmasq security update		2017-10-02

影響を受けるシステム台数

<https://access.redhat.com/management/errata>

Copyright Red Hat K.K. All rights reserved.

# customer portal でのシステム確認

## システム

以下は、このアカウントのシステム一覧です。

名前/UUID での絞り込み

[他のフィルター](#) ▾

[フィルターのリセット](#)

新規作成

↓ .CSV

<input type="checkbox"/>	名前	<input type="checkbox"/>	タイプ	最終チェックイン	Errata
<input type="checkbox"/>	● ipa.example.com	1	仮想システム	2017/12/12	🛡️ 42 🐛 125 🛠️ 34
<input type="checkbox"/>	● localhost	1	仮想システム	2017/09/19	🛡️ 49 🐛 184 🛠️ 35
<input type="checkbox"/>	● localhost.localdomain	1	仮想システム	2017/06/15	🛡️ 125 🐛 373 🛠️ 64
<input type="checkbox"/>	● localhost.localdomain	1	仮想システム	2017/07/05	最新
<input type="checkbox"/>	🔍 myhostname	0	仮想システム	該当なし	該当なし
<input type="checkbox"/>	■ rhel6	1	仮想システム	2018/01/11	該当なし
<input type="checkbox"/>	● rhel7.example.com	1	仮想システム	2017/10/03	🛡️ 96 🐛
<input type="checkbox"/>	● rhel7.example.com	1	仮想システム	2018/	

各システムについて  
適用可能なセキュリティ fix  
バグ fix, 機能拡張の数

<https://access.redhat.com/management/systems>

# 課題：優先順位の設定

- 対処すべき脆弱性や設定の問題などは多数存在する  
→ 各修正作業に優先順位を設定する必要性
  - 問題の重大さ、システムの可用性要件、被害にあった場合の深刻さ等
- CVSS スコア
  - 脆弱性に対する 10 点満点の評価。攻撃に利用できる経路や攻撃の難しさなどで点数が決まります。Red Hat の脆弱性情報には CVSS スコアが含まれます。
- errata の重大度
  - セキュリティ問題についての errata は Critical, Important, Moderate, Low の 4 段階に分類されています。

# 脆弱性データベース内での表示

CVE-2018-1000156

English ▾

Impact:

Important

公開日:

2018-04-05

CWE:

CWE-77

Bugzilla:

[1564326](#): CVE-2018-1000156 patch: Malicious patch files cause ed to execute arbitrary commands

The MITRE CVE dictionary describes this issue as:

GNU Patch version 2.7.6 contains an input validation vulnerability when processing patch files, specifically the EDITOR\_PROGRAM invocation (using ed) can result in code execution. This attack appear to be exploitable via a patch file processed via the patch utility. This is similar to FreeBSD's CVE-2015-1418 however although they share a common ancestry the code bases have diverged over time.

Find out more about CVE-2018-1000156 from the [MITRE CVE dictionary](#) dictionary and [NIST NVD](#).

CVSS v3 metrics

CVSS3 Base Score	7.8
CVSS3 Base Metrics	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

この脆弱性の重大度は  
Important

問題の概要

CVSS v3 では  
10 点満点中 7.8 点

# customer portal での重大度表示

製品のソフトウェア

パッケージ

ソース

エラータ

Red Hat Enterprise Linux Server のエラータ (x86\_64 の v. 7 for )

Show 25 entries

アドバイザリー番号	概要	タイプ/重大度	投稿日
<a href="#">RHBA-2018:0083</a>	glusterfs bug fix update	Bug Fix Advisory	2018-01-11
<a href="#">RHBA-2018:0071</a>	Red Hat Enterprise Linux Atomic Tools 7.4.3.1 Container Image Update	Bug Fix Advisory	2018-01-09
<a href="#">RHSA-2018:0061</a>	Important: thunderbird security update	Security Advisory <b>Important</b>	2018-01-08
<a href="#">RHSA-2018:0029</a>	Important: libvirt security update	Security Advisory <b>Important</b>	2018-01-04
<a href="#">RHBA-2018:0042</a>	dracut bug fix update	Bug Fix Advisory	2018-01-04
<a href="#">RHSA-2018:0023</a>	Important: qemu-kvm security update	Security Advisory <b>Important</b>	2018-01-04
<a href="#">RHSA-2018:0014</a>	Important: linux-firmware security update	Security Advisory <b>Important</b>	2018-01-04
<a href="#">RHBA-2018:0033</a>	Satellite Maintenance bug fix update	Bug Fix Advisory	2018-01-04
<a href="#">RHSA-2018:0007</a>	Important: kernel security update	Security Advisory <b>Important</b>	2018-01-03

セキュリティ fix のみ  
Critical, Important,  
Moderate, Low  
の 4 段階で評価

# 各システム内での確認

- yum updateinfo
  - errata の数と種類を表示
- yum updateinfo list
  - 該当する errata とパッケージのリスト

```
[root@rhel74 ~]# yum updateinfo
Loaded plugins: product-id, search-disabled-repos, s
Updates Information Summary: updates
  11 Security notice(s)
    9 Important Security notice(s)
    2 Moderate Security notice(s)
  10 Bugfix notice(s)
    3 Enhancement notice(s)
updateinfo summary done
```

```
Loaded plugins: product-id, search-disabled-repos, su
RHSA-2018:0102 Important/Sec. bind-libs-32:9.9.4-51.e
RHSA-2018:0102 Important/Sec. bind-libs-lite-32:9.9.4
RHSA-2018:0102 Important/Sec. bind-license-32:9.9.4-5
RHSA-2018:0102 Important/Sec. bind-utils-32:9.9.4-51.
RHBA-2018:0145 bugfix binutils-2.25.1-32.base
RHBA-2018:0143 bugfix device-mapper-persisten
1.x86_64
RHSA-2018:0158 Moderate/Sec. dhclient-12:4.2.5-58.el
RHSA-2018:0158 Moderate/Sec. dhcp-common-12:4.2.5-58
RHSA-2018:0158 Moderate/Sec. dhcp-libs-12:4.2.5-58.e
RHBA-2018:0042 bugfix dracut-033-502.el7_4.1.
RHBA-2018:0042 bugfix dracut-config-rescue-03
RHBA-2018:0042 bugfix dracut-network-033-502.
RHEA-2018:0141 enhancement initscripts-9.49.39-1.e
RHSA-2018:0014 Important/Sec. iwl100-firmware-39.31.5
RHSA-2018:0094 Important/Sec. iwl100-firmware-39.31.5
RHSA-2018:0014 Important/Sec. iwl100-firmware-1.20.0
```



# 各システム内での確認（続）

- yum updateinfo info
  - 該当する errata の説明表示

```
=====
Important: bind security update
=====
Update ID : RHSA-2018:0102
Release : 0
Type : security
Status : final
Issued : 2018-01-22 08:15:48 UTC
Bugs : 1534812 - CVE-2017-3145 bind: Improper fetch cleanup sequencing in
the resolver can cause named to crash
CVEs : CVE-2017-3145
Description : The Berkeley Internet Name Domain (BIND) is an implementation of
: the Domain Name System (DNS) protocols. BIND
: includes a DNS server (named); a resolver library
: (routines for applications to use when interfacing
: with DNS); and tools for verifying that the DNS
: server is operating correctly.
:
: Security Fix(es):
: Copyright Red Hat K.K. All rights reserved.
:
: * A use-after-free flaw leading to denial of
```

# 課題：更新パッケージの入手

- Red Hat Customer Portal
  - yum コマンドへ更新情報やパッケージを供給
    - [cdn.redhat.com](https://cdn.redhat.com) への接続が必要
  - ダウンロードページから rpm パッケージを入手
    - 自動的に依存関係を解決してくれないので煩雑
  - reposync コマンドによるリポジトリの同期
    - reposync を実行するシステムに対応するリポジトリを同期可能

# yum コマンドでのダウンロードとインストール

- 「yum update」コマンド
  - システムに含まれているパッケージ~~全て~~を最新へ更新
  - 依存関係解決を行い、必要になったパッケージを追加
- 「yum update パッケージ名」コマンド
  - 指定した特定のパッケージを更新
  - 依存関係解決を行い、指定したパッケージを更新するために必要なパッケージを同時に更新・追加

# yum コマンドでのダウンロードとインストール（ 続 ）

- 「セキュリティ fix が出ていれば適用したい」
  - yum update --security
- 「特定の CVE に関連する修正を適用したい」
  - yum update --cve CVE-2008-0947

※RHEL 6 以前では yum-plugin-security パッケージのインストールが必要です (<https://access.redhat.com/ja/solutions/207493>)

# customer portal でのダウンロード

[ダウンロード](#) > [Red Hat Enterprise Linux](#) > [パッケージ](#)

## ダウンロード Red Hat Enterprise Linux

製品のバリエーション:

バージョン: アーキテクチャー:

Red Hat Enterprise Linux Server

7

x86\_64

### Red Hat Enterprise Linux Server について

Red Hat Enterprise Linux Server provides core operating system functions and capabilities for application infrastructure.

### 製品のリソース

- [Get Started](#)
- [Documentation](#)
- [Red Hat Enterprise Linux Life Cycle](#)

### ヘルプの使用

- [Contact Support](#)
- [Create installation media](#)

製品のソフトウェア

**パッケージ**

ソース

エラータ

### Red Hat Enterprise Linux Server のパッケージ (x86\_64 の v. 7 for )

Show 

25

 entries

Search:

パッケージ	概要	
Red Hat Enterprise Linux 7 Server (RPMs)		
<a href="#">389-ds-base</a>	389 Directory Server (base)	<a href="#">↓ 最新版のダウンロード</a>
<a href="#">389-ds-base-libs</a>	Core libraries for 389 Directory Server	<a href="#">↓ 最新版のダウンロード</a>
<a href="#">ElectricFence</a>	A debugger which detects memory allocation violations	<a href="#">↓ 最新版のダウンロード</a>

各パッケージをダウンロード

1

# reposync でのローカルミラー作成

- subscription-manager で登録後、そのシステムで利用可能なリポジトリを reposync コマンドでミラーできる
  - 例 : `reposync -r rhel-7-server-rpms`

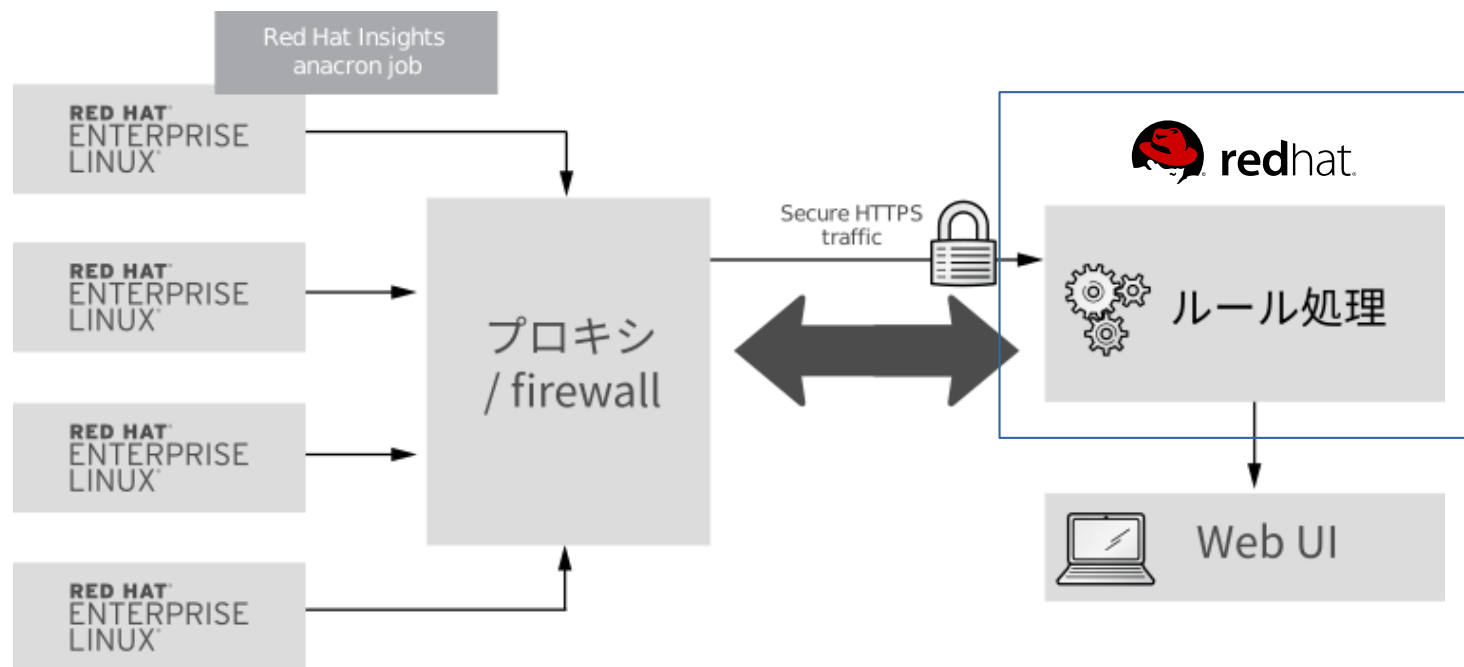
※ 詳しくはナレッジベース「How to synchronize repository on system registered to CDN via subscription-manager」を参照

<https://access.redhat.com/articles/1355053>

# Red Hat Insights があると……？

# Red Hat Insights とは？

- Red Hat のプロアクティブなシステム分析サービス
- 定期的に情報を収集して重大な問題や設定の問題を検出
- 問題の説明、対策方法を含むレポートを生成
  - 存在する場合にはアップデート以外のワークアラウンドも提示





# Insights は何が嬉しいの？

- レポートで問題につながる予兆を把握する
  - 受け身で緊急対応するのではなく計画的に対応
  - 既知の問題に対する状況を可視化
- Red Hat の最新の知見を反映したルール
  - 典型的な問題を回避
  - ごく最近知られるようになった問題も検出
- 具体的な対処方法を含むため対策しやすい
  - 対策用の Ansible Playbook を提供

# 課題：優先順位の設定

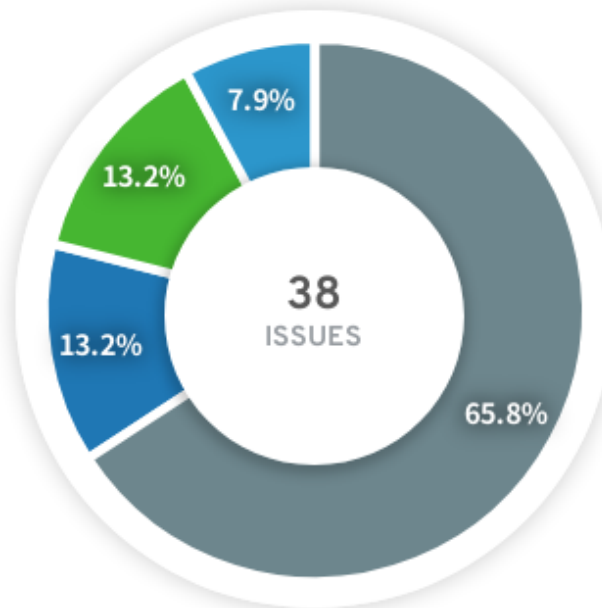
- Red Hat Insights の Actions( 問題の予兆と対策 ) には優先順位を決めるために必要な情報を含む
  - 問題が発生した場合のインパクトの大きさ
  - 問題の発生する可能性
  - 上記 2 つを踏まえたリスクの大きさ
  - 対策の実施にどの程度リスクがあるか

# Red Hat Insights の出力例

- 必要な対処を分類して表示
  - リスクの高さ
  - 何に影響するか（セキュリティ、パフォーマンス、可用性、安定性）
- 分類毎の表示
- 各対処の詳細を表示

[Overview](#)[Actions](#)[Inventory](#)[Planner](#)[Rules](#)[Executive Report](#)[Configuration](#)

## Actions



■ Availability (5)

■ Stability (5)

■ Performance (3)

■ Security (25)

### Risk summary

Low (26.3%)

Medium (44.7%)

High (21.1%)

Critical (7.9%)

### FEATURED TOPICS

0 Systems

#### Network Bonding

The Linux bonding driver provides a method for aggregating multiple network interfaces into a single logical bonded interface. The behavior of the bonded interfaces depends upon the mode. Modes may provide either hot standby or load balancing services, as well as link integrity monitoring.

3 Systems

#### Oracle

Actions for optimizing your Oracle databases for performance and compatibility in your environment

1 System

Critical な問題だけを表示

[Overview](#)[Actions](#)[Inventory](#)[Planner](#)[Rules](#)[Executive Report](#)[Configuration](#)[Actions](#) / Critical Risk Actions

## Critical Risk Actions

Actions identified with a critical level of risk



Total Risk

All ▾

Risk of Change

All ▾

Rule	▲	Likelihood ▴	Impact ▴	Total Risk ▴	Systems ▴	Ansible ▴
<a href="#">Dnsmasq with listening processes vulnerable to remote code execution via crafted DNS requests (CVE-2017-14491)</a>		☰	☰	☰	9	A
<a href="#">OpenSSH vulnerable to remote password guessing attack (CVE-2015-5600)</a>		☰	☰	☰	1	A
<a href="#">Apache httpd with externally listening processes vulnerable to man-in-the-middle via CGI (CVE-2016-5387/HTTPoxy)</a>		☰	☰	☰	1	A

[Overview](#)[Actions](#)[Inventory](#)[Planner](#)[Rules](#)[Executive Report](#)[Configuration](#)[Actions](#) / [Critical Risk Actions](#) / OpenSSH vulnerable to remote password guessing attack (CVE-2015-5600)

## OpenSSH vulnerable to remote password guessing attack (CVE-2015-5600)

A

A flaw in `openssh` could allow an attacker to request a large number of keyboard-interactive devices when entering a password and bypass the `MaxAuthTries` limit. This issue is dependent on `KbdInteractiveAuthentication` and `ChallengeResponseAuthentication` settings in `sshd_config`.

Red Hat recommends that you update your settings in `sshd_config`.

 Impact Likelihood Total Risk Risk of change: **Very Low**

Check in status

All

1 Im

SSH サーバの設定変更を  
推奨

Actions ▾



Type



Name



Reported

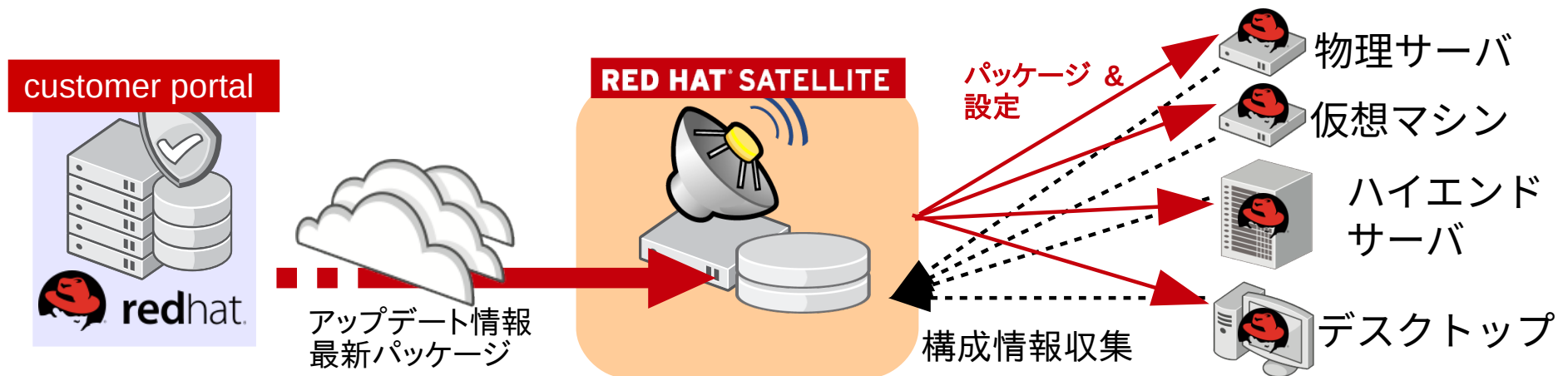
 RHEL Server[eap17.us-east.insights.redhat.com](http://eap17.us-east.insights.redhat.com)

21 hours ago

# Red Hat Satellite があると……？

# Red Hat Satellite とは？

Red Hat Satellite は構内にサーバを構築し、インターネット接続がない環境でも Customer Portal 相当の機能を提供する他、サードパーティ rpm パッケージの配布、リポジトリのバージョン管理、リモートコマンド実行などの追加機能を提供します。





# 課題：更新パッケージの入手

- Red Hat Satellite Server
  - 製品、バージョン、アーキテクチャをあらかじめ指定してリポジトリを定期的に同期
  - インターネット接続がない Satellite Server のため ISO イメージ形式で更新データを配布しています（不定期）
    - 別システムで ISO イメージをダウンロード後、USB メモリや DVD-R などデータを持ち込む
  - 同期用 Satellite Server から、インターネット接続がない Satellite Server へパッケージ同期する仕組みも提供

# Satellite でのリポジトリ同期

## 同期の状態

すべて折りたたむ

すべて展開

すべてを選択解除

すべてを選択

☐ 実行中のみ

製品	開始時刻	期間	詳細	結果
▼ Red Hat Enterprise Linux Server				
▼ 7Server				
▼ x86_64				
<input type="checkbox"/> Red Hat Enterprise Linux 7 Server RPMs x86_64 7Server	15分前	1分以内	新規パッケージがありません。	Syncing Complete.
<input type="checkbox"/> Red Hat Satellite Tools 6.2 for RHEL 7 Server RPMs x86_64	15分前	1分以内	新規パッケージがありません。	Syncing Complete.

今すぐ同期

# 課題： リポジトリのバージョン管理

- 「テスト環境でテストしたパッケージだけを本番環境に適用したい」
  - 問題になるケースの例：
    - 7月10日にテスト環境を構築し、約2週間テストを行う
    - 8月15日にテスト環境と同じ手順でアップデートを実施
      - 全く同じ手順を実施したが **yum update コマンドで更新される内容が異なる**。よく調べてみると8月1日に新しい修正が出荷されていた。
- Red Hat Satellite
  - リポジトリのスナップショットを作成し、各システムがどの世代を参照できるかを管理する Content View 機能を提供

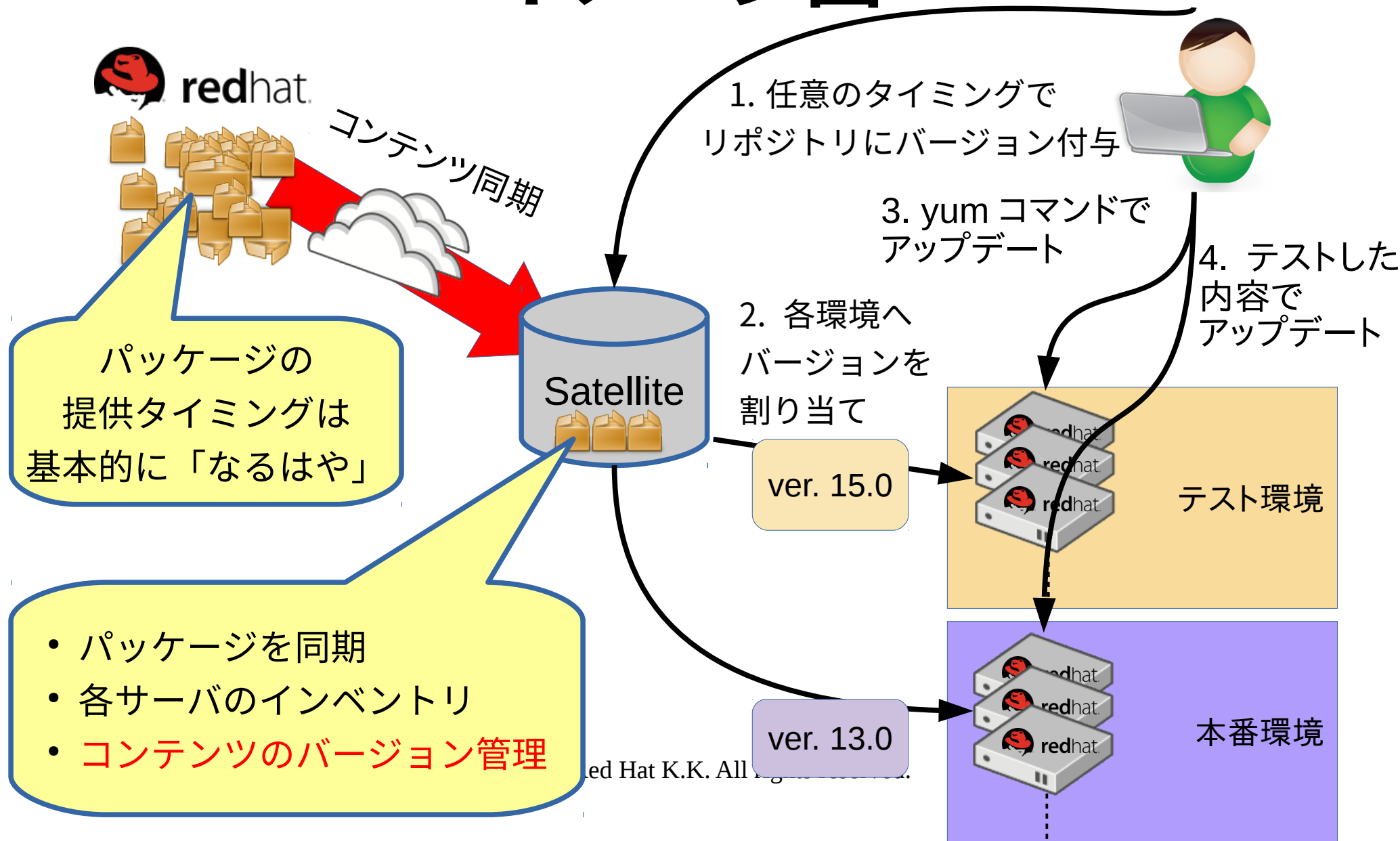
# リポジトリのバージョン管理

「このパッチ当てても大丈夫？」

→ レポジトリ（コンテンツビュー）のバージョン管理で、  
アップデート検証～本番適用のワークフローが明確に



# リポジトリのバージョン管理 イメージ図



# コンテンツビュー管理画面

フィルター...

Q 検索

3 (合計 3) 中 3 件を表示中

+ 新規ビューの作成

名前

rhel7-201612 >

rhel7-201704

rhel7-latest

rhel7-201612

新規バージョンの公開

ビューのコピー

ビューの削除

× 閉じる

バージョン

Yum コンテンツ ▼

Puppet モジュール

Docker コンテンツ

OSTree コンテンツ

履歴

詳細




タスク

検索...

Q

3 (合計 3) 中 3 件を表示中

0 を選択済み

バージョン	状態	環境	コンテンツ	説明	アクション
バージョン 3.1	増分更新 (2017-05-22 04:09:18 UTC)	testenv	13661 パッケージ 1776 エラータ ( 350  1160  266  )		<div>← プロモート</div> <div>削除</div>
バージョン 3.0	testenv にプロモート (2017-05-12 02:39:52 UTC)	Library	13656 パッケージ 1775 エラータ ( 349  1160  266  )		<div>← プロモート</div> <div>削除</div>
バージョン 2.0	testenv にプロモート (2017-04-28 09:36:44)		13859 パッケージ 1812 エラータ ( 386  )		<div>← プロモート</div> <div>削除</div>

# Insights と Satellite は重複する？

- 「必要なソフトウェア更新を検出する」点では重複
  - Satellite は網羅的に、Insights は重要なものだけ
- Satellite はインベントリ管理や、パッケージ配布などの機能をもつ、rpm パッケージを基盤とする運用スイートです
- Insights はソフトウェアの更新だけでなく、設定の問題や ISV 製品との競合、統計情報等も参照したリスク検出を行います

# Red Hat Ansible Automation が あると……？



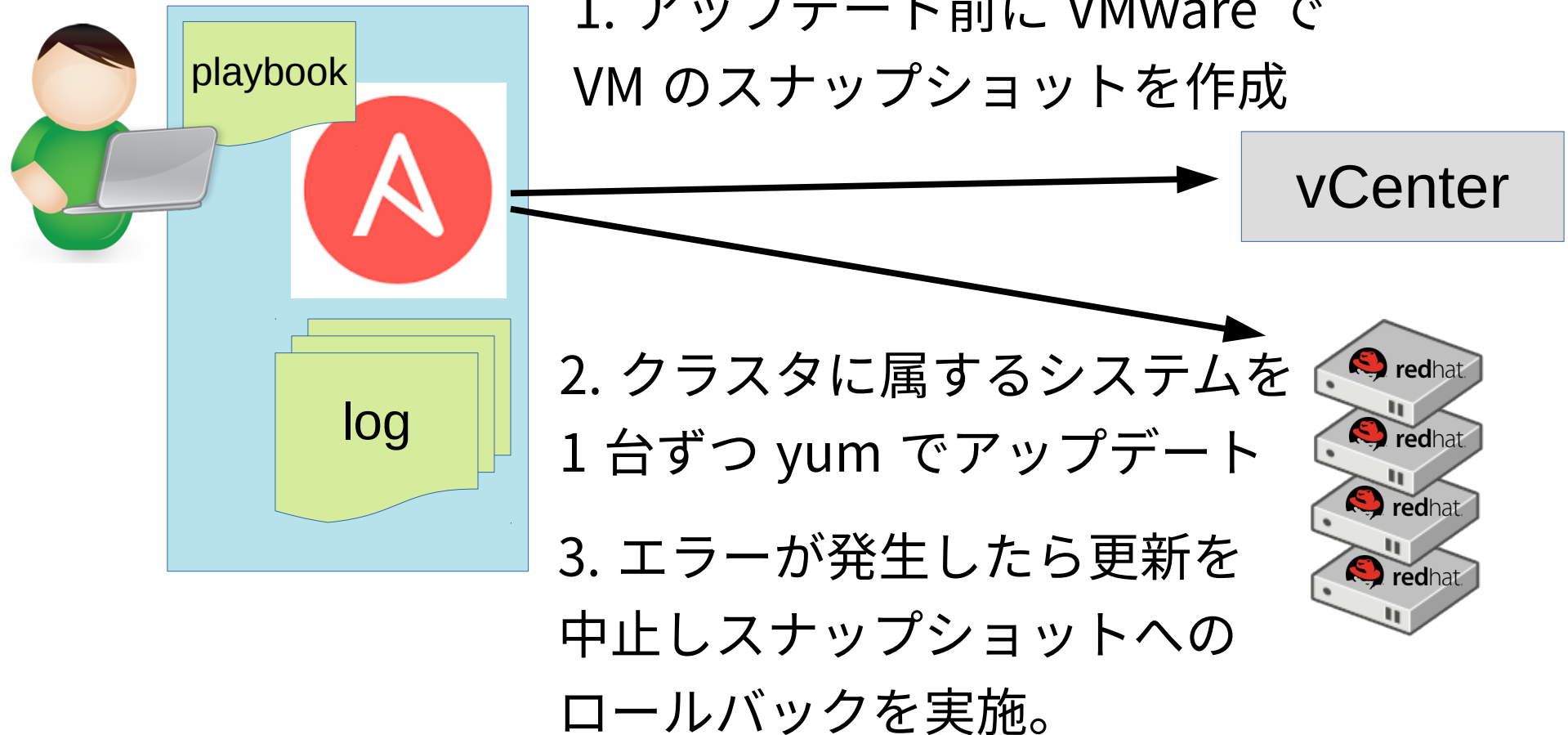
# 複雑な更新手順を確実に再現したい

- 複雑なシステムでは単純に「全システムで yum update を実行して完了」では済まない
  - 前後に手順が必要：事前にバックアップ作成、ロードバランサ切り替え、クラスタからの除外・再参加など
  - 制約条件：同一クラスタ内では同時に 1 台しか停止しないなど
- アップデートに工数がかかると実施が難しくなる
  - 自動化による対策が有効

# Red Hat Ansible Automation

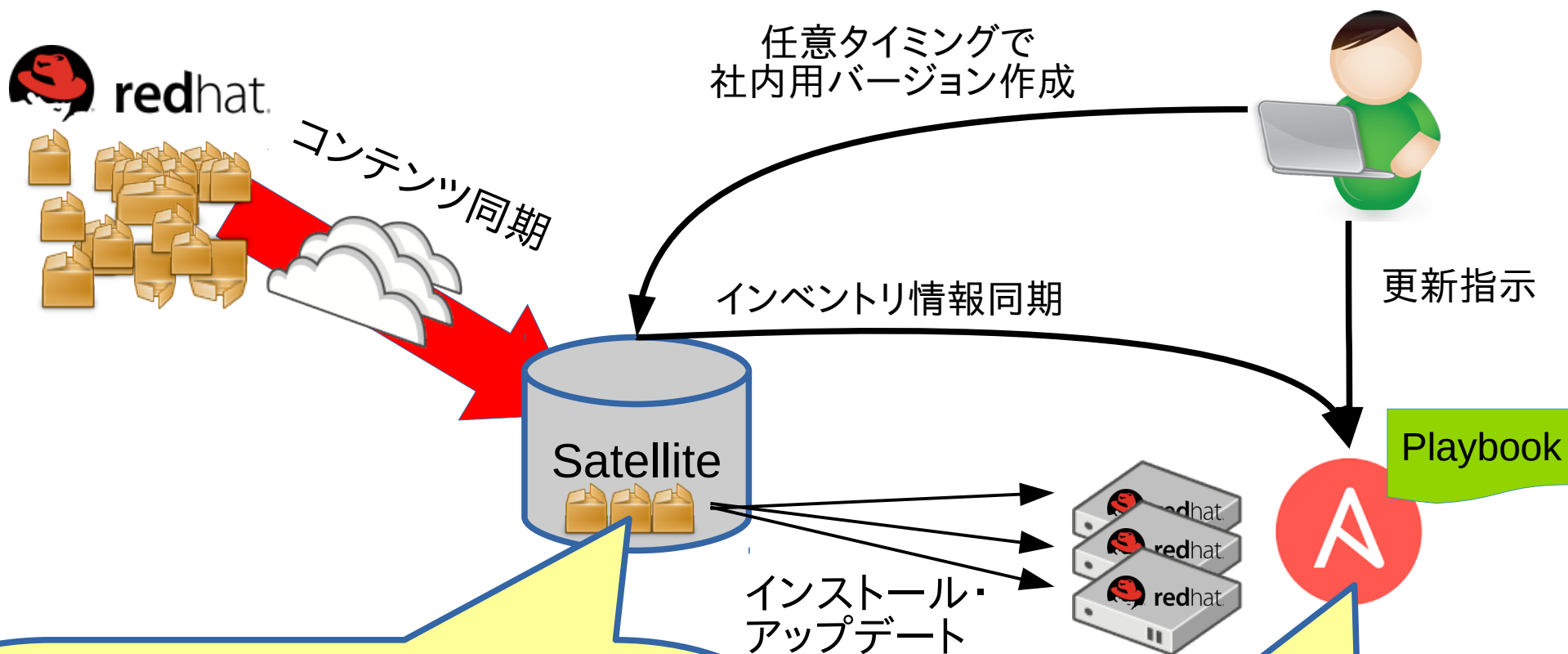
- 様々な OS 、ネットワーク機器、仮想化基盤、クラウドなどを操作することが可能な自動化エンジンと管理ツール
- 典型的な操作や制約条件を直感的に記述できる記法
- テスト環境で確立したアップデート手順を再現

# Ansible Tower による更新の例



4. Ansible Tower で各ジョブの成功・失敗、ログを確認

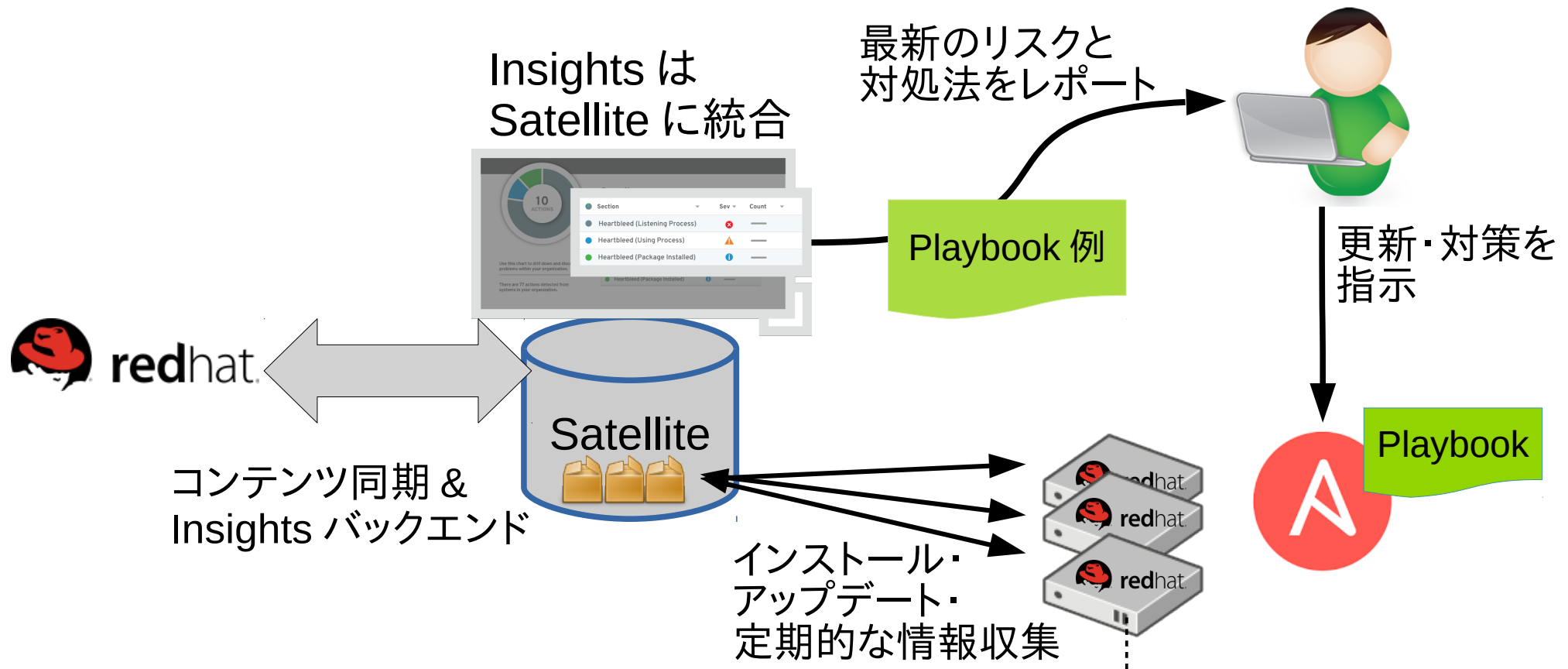
# Satellite + Ansible イメージ図



コンテンツのバージョン管理により  
タイミングによらずテストしたものと  
同じリポジトリを提供  
インベントリ管理により抜け漏れ防止

テストしたものと  
同じ操作を実行

# Insights+Satellite+Ansible イメージ図



# 定期更新を中心とした更新

イベント源

障害など

調査

Satellite

新 errata

Insights

新 Action

定期更新

3ヶ月経過

優先度確認

定期更新  
より前に  
更新が必要

更新以外の  
対応が必要

対応不要

プラン

以下を決める：  
対策対象  
完了日時目標  
準備項目  
対策手順

テスト

CV 作成  
Playbook 作成  
テスト環境で  
CV 割り当て  
Playbook 試験  
回帰テスト等

実施

CV 割り当て  
Playbook 実行

# まとめ：課題と製品の対応表

	カスタマー ポータル	Insights	Satellite	Ansible
更新情報を含むイ ンベントリ管理	OK	N/A	OK	N/A
優先順位の設定	脆弱性のみ	全アクションに リスク情報	脆弱性のみ	N/A
更新パッケージの 入手	OK	N/A	OK	N/A
リポジトリのバー ジョン管理	N/A	N/A	OK	N/A
複雑な更新手順の 実施	N/A	Ansible Playbook 例を 提供	N/A	OK

# まとめ

- Red Hat Enterprise Linux でも定期的なアップデートは必須です
- Red Hat Enterprise Linux だけでもある程度管理できる仕組みを提供しています (Customer Portal)
- Red Hat Satellite はインターネット接続がない環境やリポジトリのバージョン管理が必要な場合に有効です
- Red Hat Ansible Automation でアップデート手順を自動化することで実施しやすくなります