RHEL を定期的にアップデートする際の課題と対策

2018-02-07

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、課題に対して利用できる各種の仕組みは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 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**: 適用する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るべきか、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

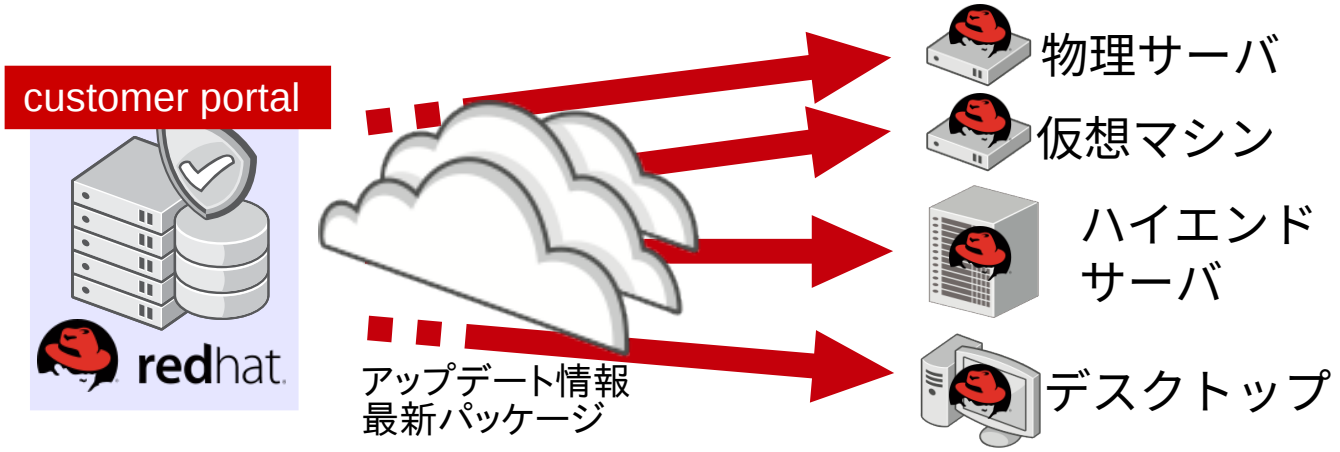
Red Hat Enterprise Linux だけで ここまでできるよ

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
  - 適用する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

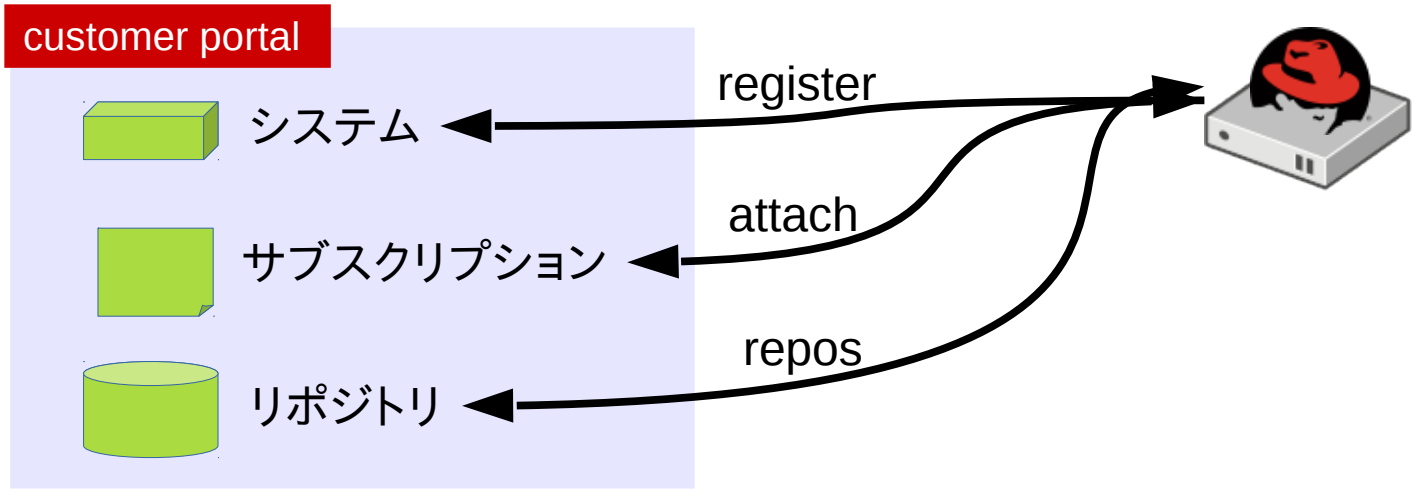
Customer Portal はインベントリ情報として各システムの基本的な情報と導入されている製品・パッケージの情報を管理。登録したシステムでは yum コマンドによりパッケージそのものと、 errata などのメタデータを取得できる。



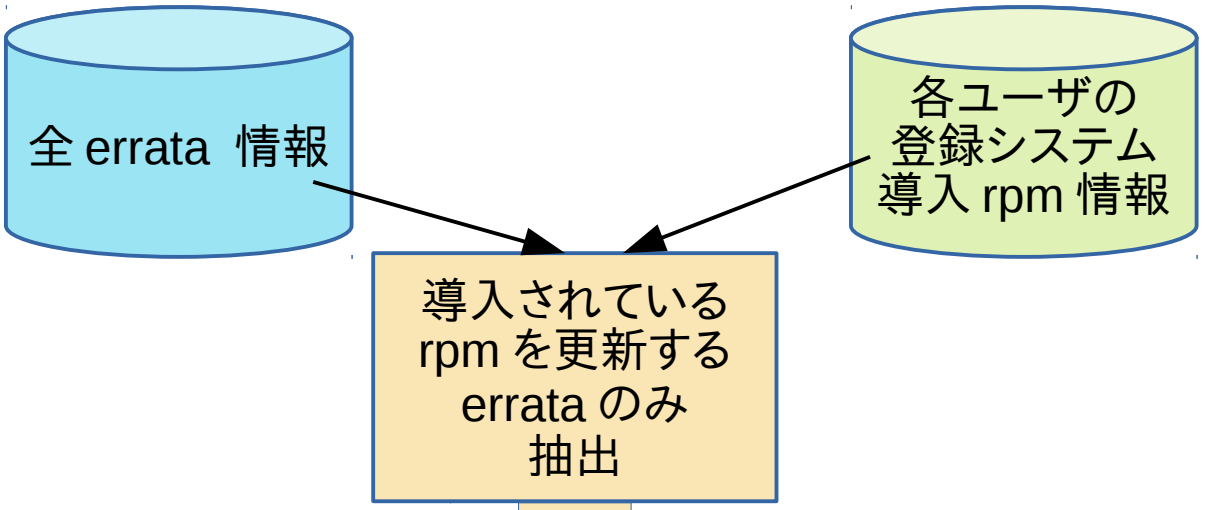
subscription-manager での登録

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。

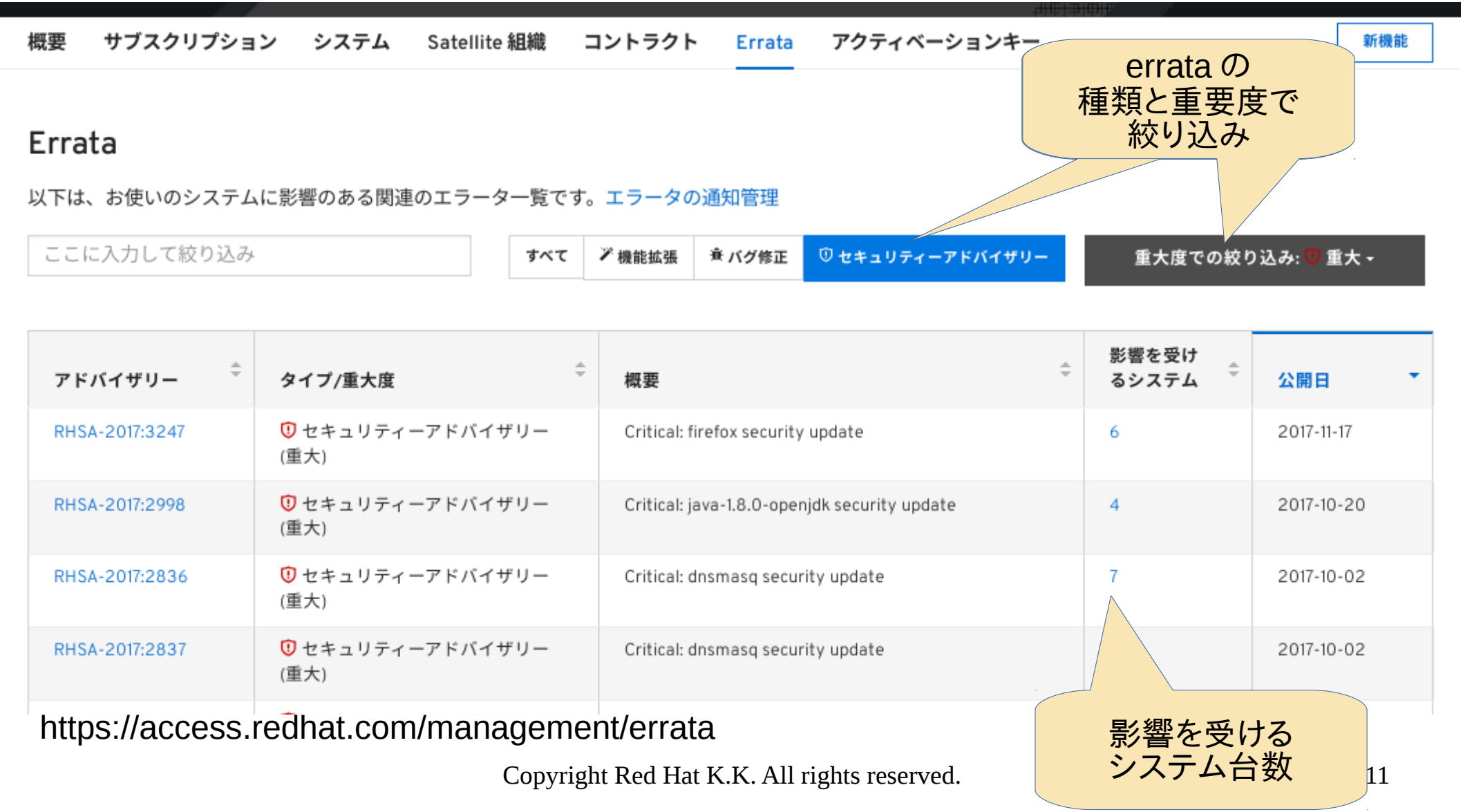
subscription-manager register → システムを登録
subscription-manager attach → システムにサブスクリプションを対応づけ
subscription-manager repos → リポジトリの利用有無を設定



対応する errata だけを表示 / 通知



customer portal での errata 確認



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

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

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

各システムに
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

- 対処する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-2017-1000364

English

Impact: Important
公開日: 2017-06-19

Bugzilla:
1461333: CVE-2017-1000364 kernel: heap/stack gap jumping via unbounded stack allocations

この脆弱性の重大度は Important

A flaw was found in the way memory was being allocated on the stack for user space binaries. If heap (or different memory region) and stack memory regions were adjacent to each other, an attacker could use this flaw to jump over the stack guard gap, cause controlled memory corruption on process stack or the adjacent memory region, and thus increase their privileges on the system. This is a kernel-side mitigation which increases the stack guard gap size from one page to 1 MiB to make successful exploitation of this issue more difficult.

Find out more about CVE-2017-1000364 from the MITRE CVE dictionary dictionary and NIST NVD.

ステートメント

This is a kernel-side mitigation. For a related glibc mitigation please see https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-1000366 .

CVSS v2 metrics

Base Score	6.2
Base Metrics	AV:L/AC:H/Au:N/C:C/I:C/A:C

CVSS v2 では 6.2 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
RHBA-2018:0083	glusterfs bug fix update	Bug Fix Advisory	2018-01-11
RHBA-2018:0071	Red Hat Enterprise Linux Atomic Tools 7.4.3.1 Container Image Update	Bug Fix Advisory	2018-01-09
RHSA-2018:0061	Important: thunderbird security update	Security Advisory Important	2018-01-08
RHSA-2018:0029	Important: libvirt security update	Security Advisory Important	2018-01-04
RHBA-2018:0042	dracut bug fix update	Bug Fix Advisory	2018-01-04
RHSA-2018:0023	Important: qemu-kvm security update	Security Advisory Important	2018-01-04
RHSA-2018:0014	Important: linux-firmware security update	Security Advisory Important	2018-01-04
RHBA-2018:0033	Satellite Maintenance bug fix update	Bug Fix Advisory	2018-01-04
RHSA-2018:0007	Important: kernel security update	Security Advisory Important	2018-01-03

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

https://access.redhat.com/downloads/content/69/ver=/rhel---7/7.4/x86_64/product-errata

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
```

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):
            :
            : * 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 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

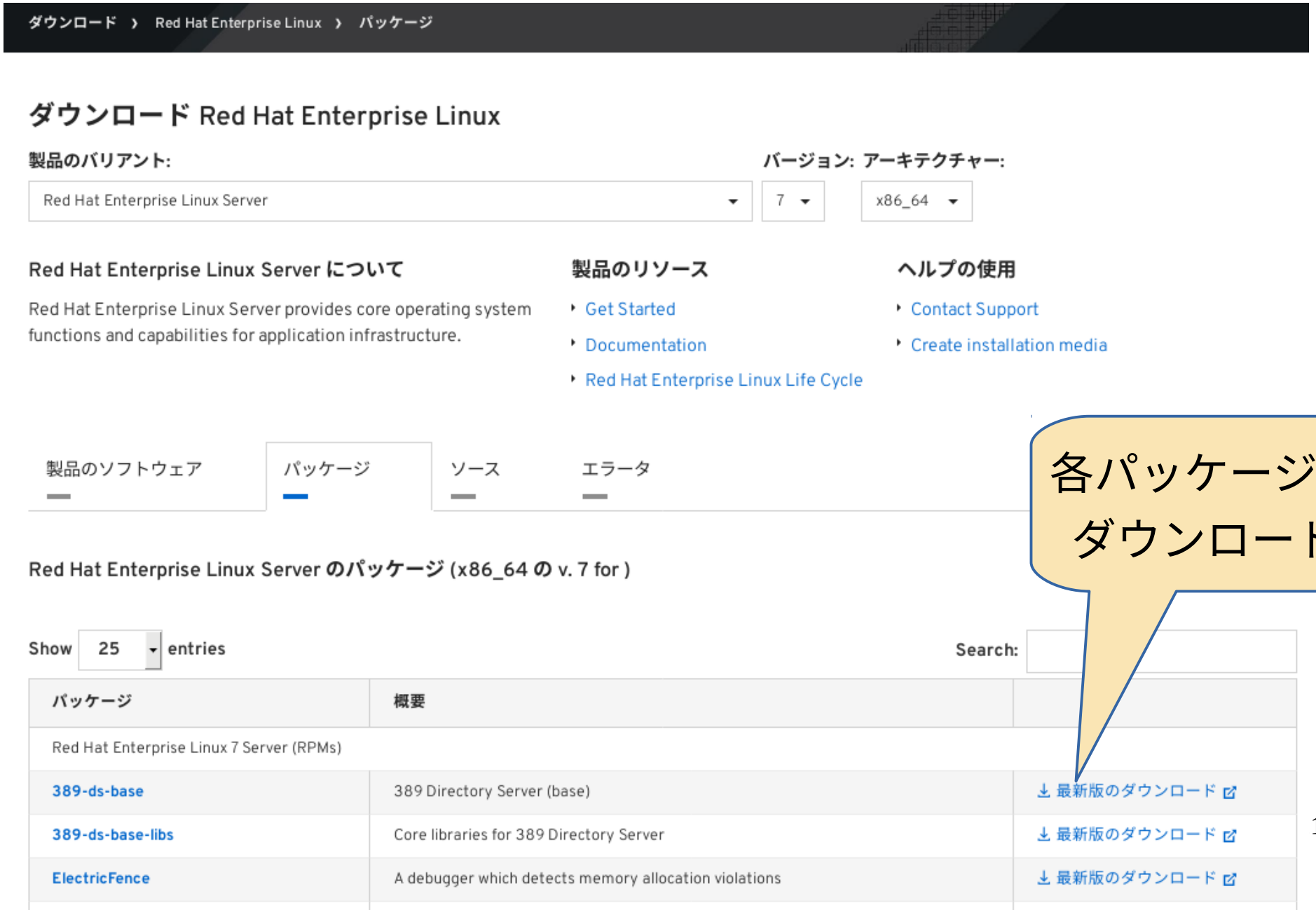
- 「yum update」コマンド
  - システムに含まれているパッケージ全てを最新へ更新
  - 依存関係解決を行い、必要になったパッケージを追加
- 「yum update パッケージ名」コマンド
  - 指定した特定のパッケージを更新
  - 依存関係解決を行い、指定したパッケージを更新するために必要なパッケージを同時に更新・追加

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



reposync でのローカルミラー作成

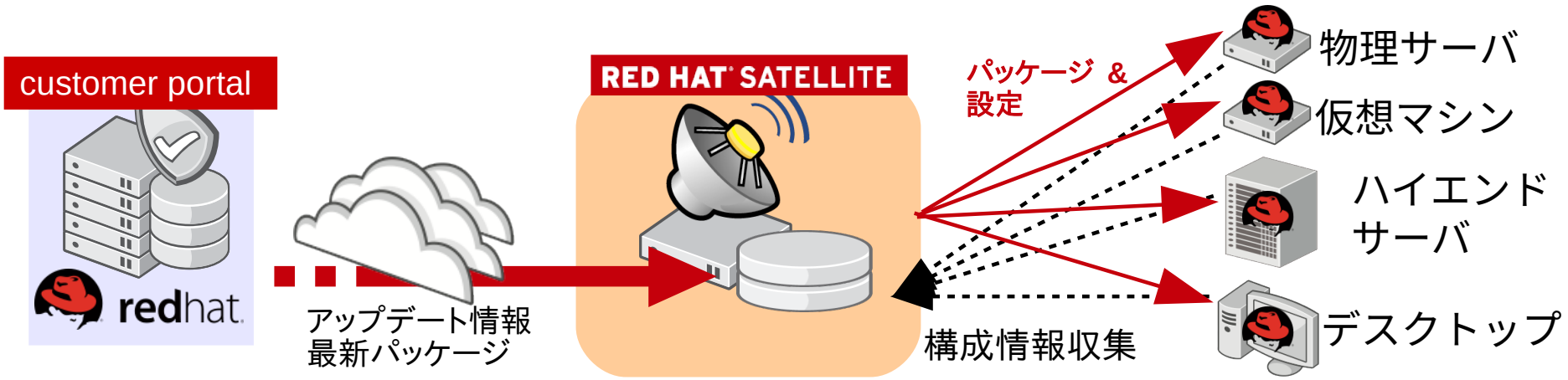
- subscription-manager で登録後、そのシステムで利用可能なリポジトリを reposync コマンドでミラーできる
  - 例 : reposync -r rhel-7-server-rpms

※ 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 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。

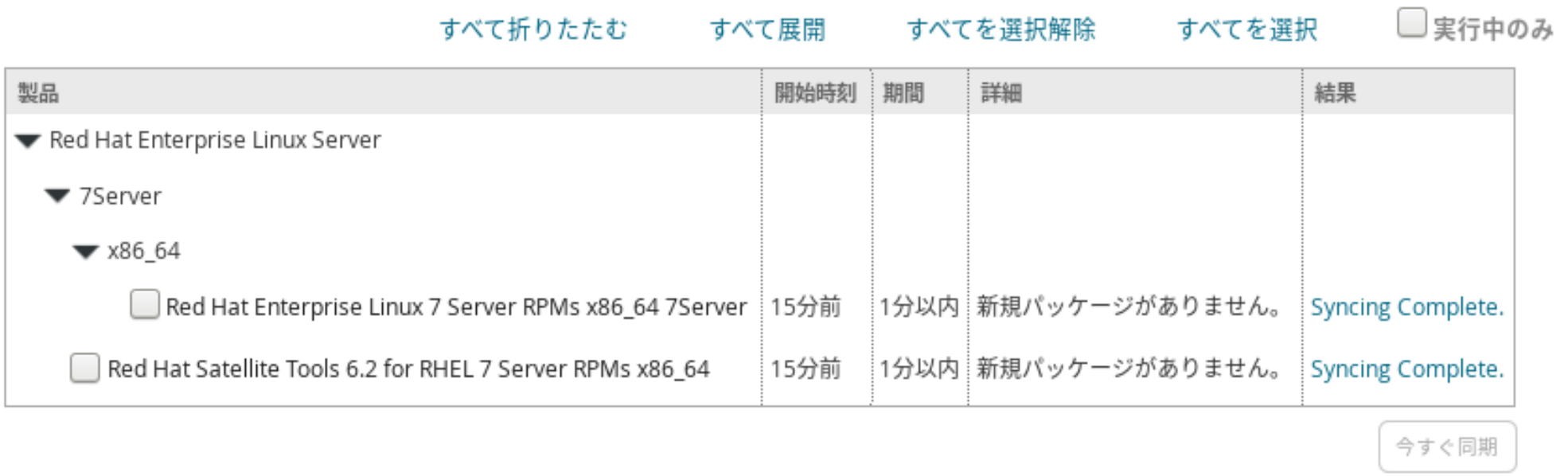


課題：更新パッケージの入手

- 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 などでデータを持ち込む
  - 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



課題：リポジトリのバージョン管理

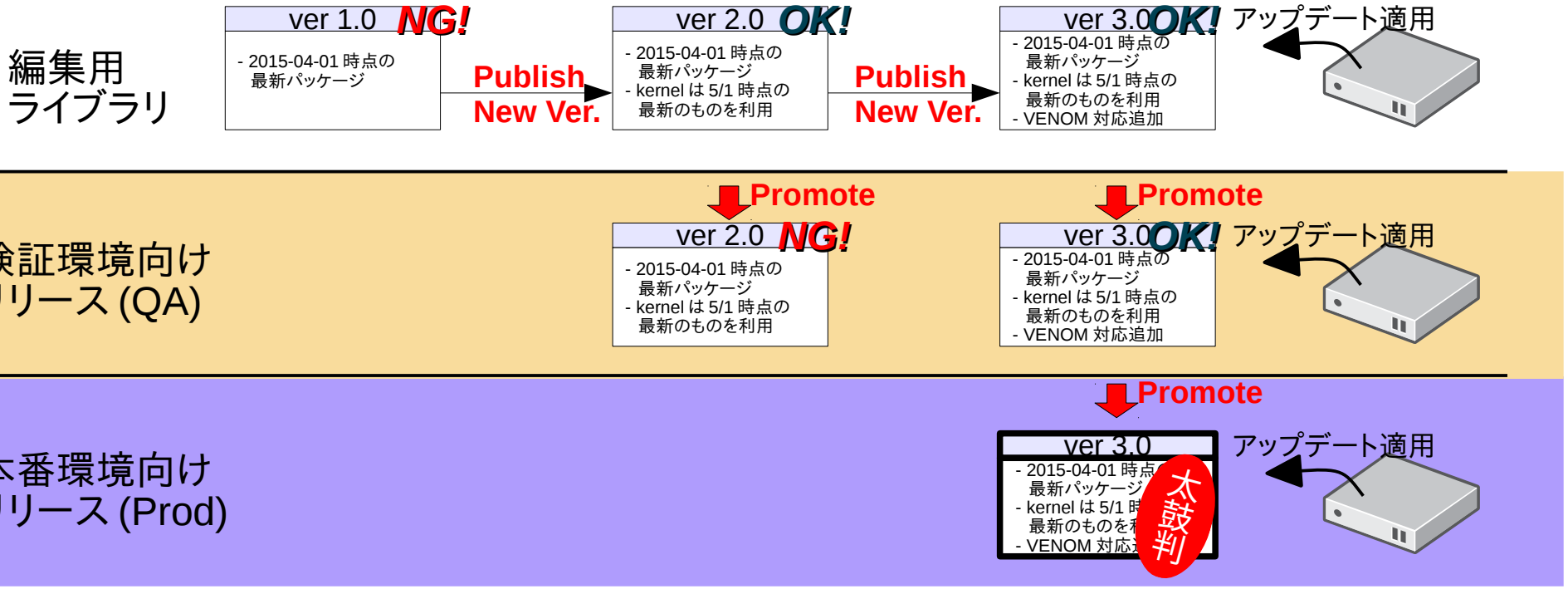
- 「テスト環境でテストしたパッケージだけを本番環境に適用したい」
  - 問題になるケースの例：
    - 7 月 10 日にテスト環境を構築し、約 2 週間テストを行う
    - 8 月 15 日にテスト環境と同じ手順でアップデートを実施

      → 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

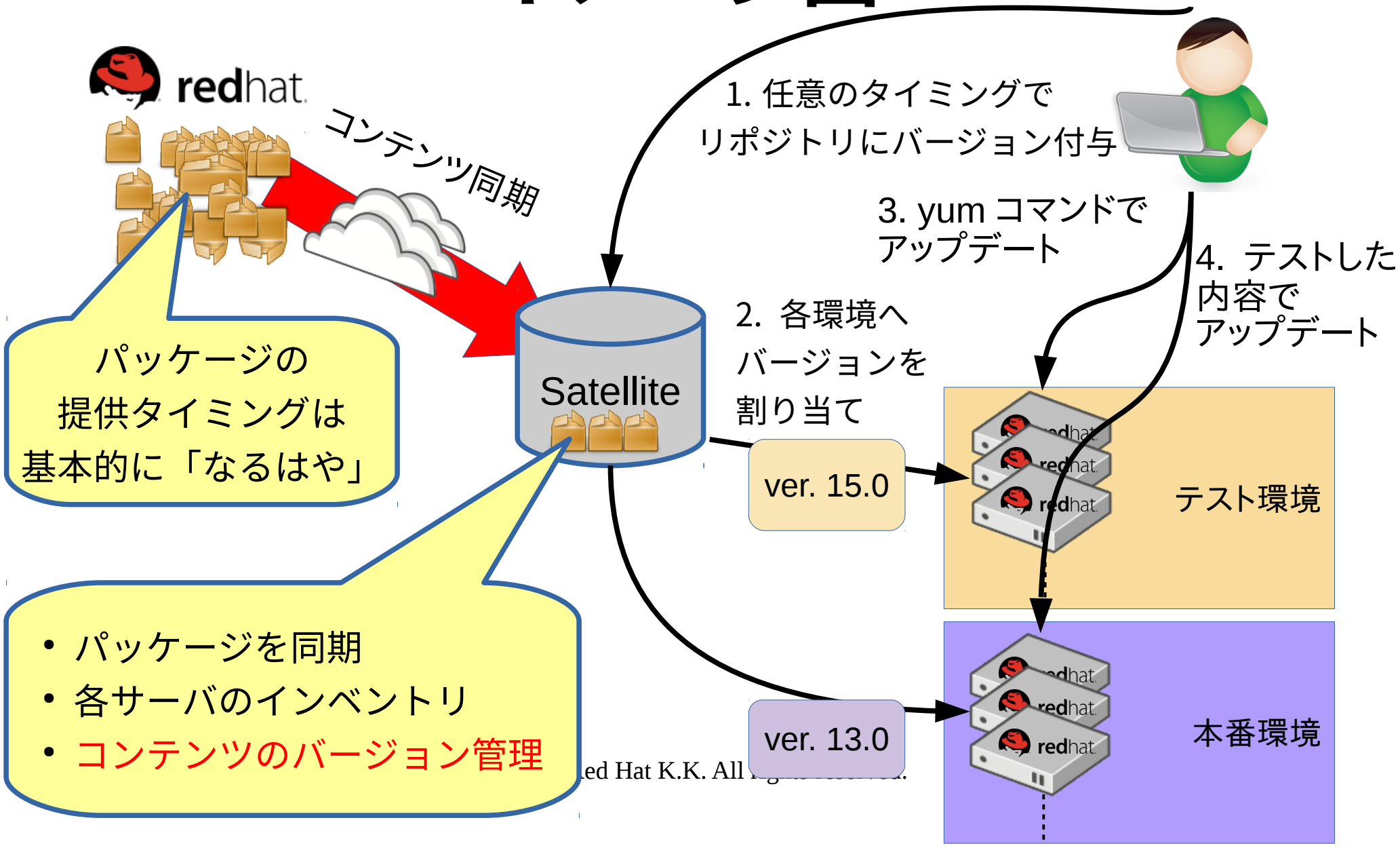
リポジトリのバージョン管理

「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

Red Hat Ansible Automation があると……？

複雑な更新手順を確実に再現したい

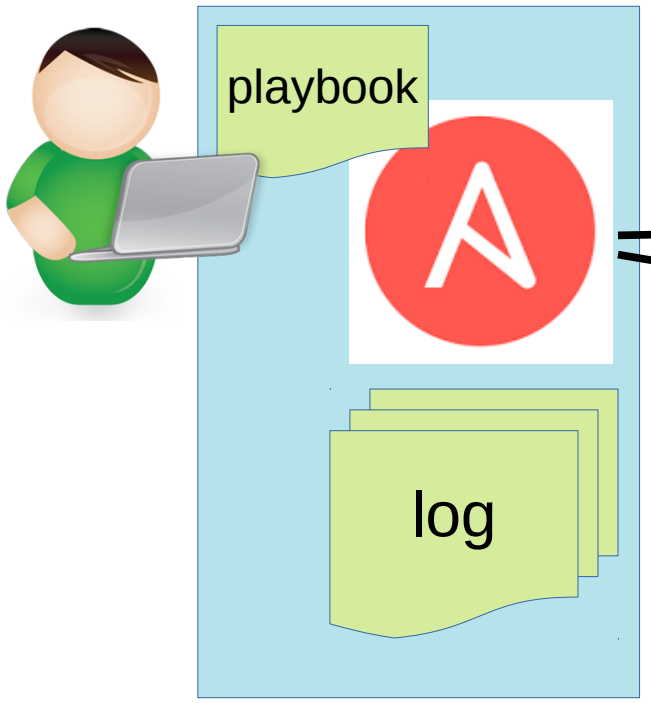
- 複雑なシステムでは単純に「全システムで yum update を実行して完了」では済まない
  - 前後に手順が必要：バックアップ作成、ロードバランサ切り替え、クラスタからの除外・再参加など
  - 制約条件：同一クラスタ内では同時に 1 台しか停止しないなど
- アップデートに工数がかかると実施が難しい

→ 自動化による対策が有効

Red Hat Ansible Automation

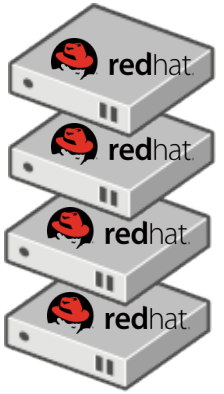
- 様々な OS 、ネットワーク機器、仮想化基盤、クラウドなどを操作することが可能な自動化エンジンと管理ツール
- 典型的な操作や制約条件を直感的に記述できる記法
- テスト環境で確立したアップデート手順を再現

Ansible Tower による更新の例



1. アップデート前に VMware で
VM のスナップショットを作成

vCenter

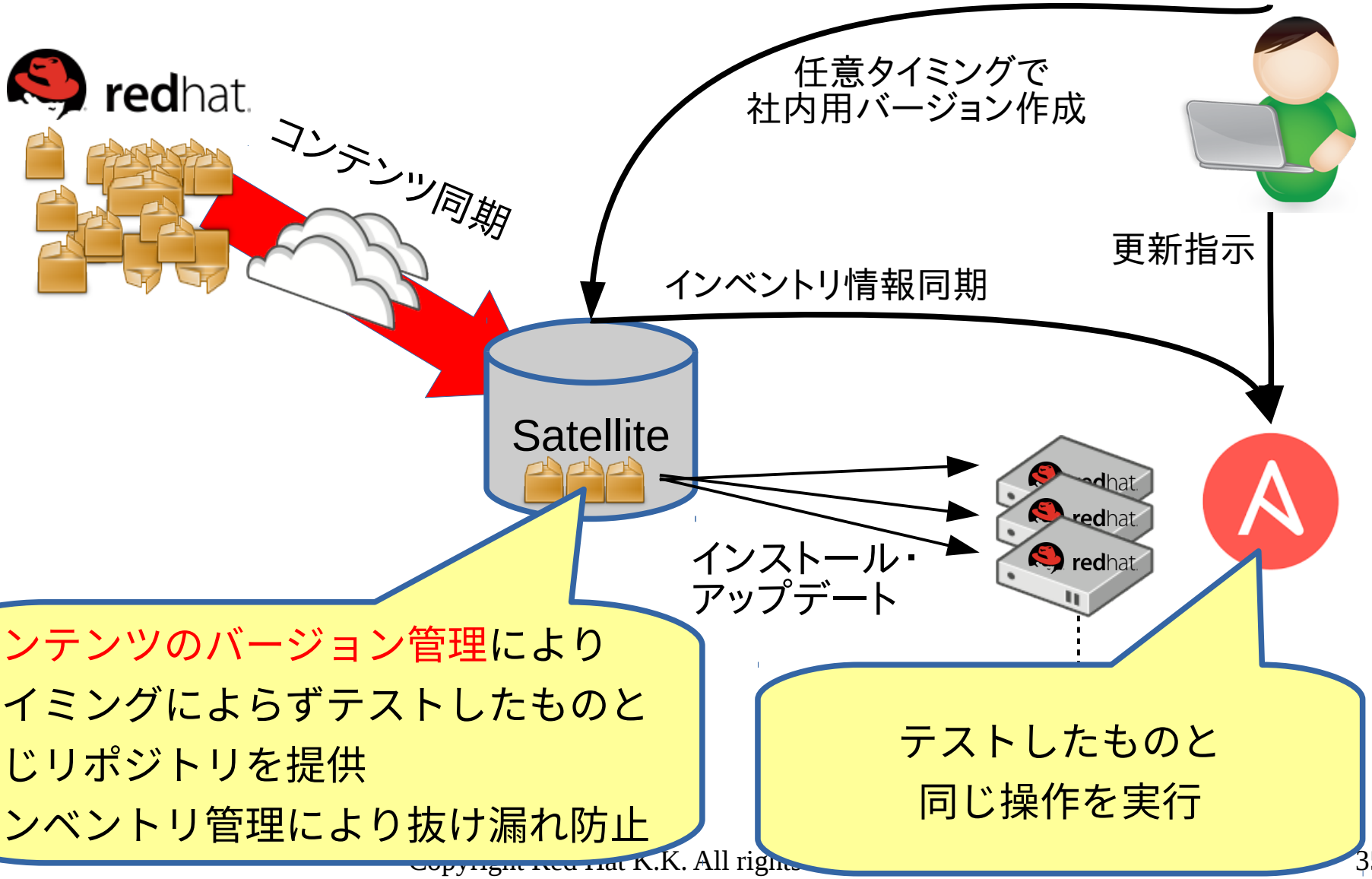


2. クラスタに属するシステムを
1 台ずつ yum でアップデート

3. エラーが発生したら更新を
中止しスナップショットへの
ロールバックを実施。

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



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

Appendix

課題と製品の対応表

	RHEL	Satellite	Ansible
更新情報を含むインベントリ管理	OK （インターネット接続が必要）	OK	N/A
優先順位の設定	脆弱性修正のみ	脆弱性修正のみ	N/A
更新パッケージの入手	OK （インターネット接続がないと煩雑）	OK	N/A
更新パッケージのバージョン管理	N/A	OK	N/A
複雑な更新手順の実施	N/A	N/A	可