

Red Hat Enterprise Linux の 修正はどのように出荷されるか

レッドハット株式会社

ソリューションアーキテクト 森若和雄


2018-10-25

このスライドの位置づけ

- 背景 : Red Hat Enterprise Linux は高い品質を誇りますが他のソフトウェアと同様にバグや脆弱性を含んでいます。そのため Red Hat は必要に応じて修正を出荷しており、 Red Hat Enterprise Linux を運用する際にはこの修正を確実に適用することが基本となります。
- 目的 : Red Hat Enterprise Linux の修正出荷に関連するポリシーや関連用語を紹介します
- 関連資料 : 実際にアップデート作業を行う場合に利用するツールについては「RHEL を定期的にアップデートする際の課題と対策」をご覧ください

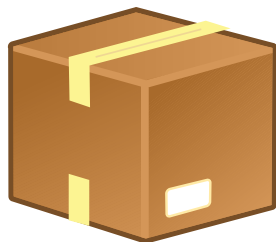
agenda

- Red Hat Enterprise Linux での「修正」とは
- 修正の出荷ポリシー
- 修正の告知



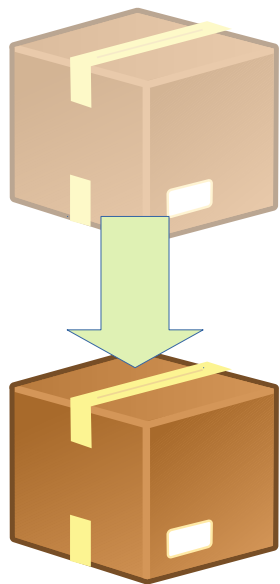
Red Hat Enterprise Linux での 「修正」とは

RPM パッケージ



- Red Hat Enterprise Linux では、RPM パッケージによりソフトウェアを配布しています
 - RPM パッケージにはソフトウェア名、ソフトウェアのバージョン、製品のバージョン、アーキテクチャを含む名前が付与されます
 - 例 : `glibc-2.17-222.el7.x86_64.rpm`
- RPM パッケージは依存関係の情報を持っており、必要なパッケージの導入を行い、競合するパッケージの導入を予防します
- 修正は新しいバージョンのパッケージとして配布します

「パッケージの更新」は何をするのか？



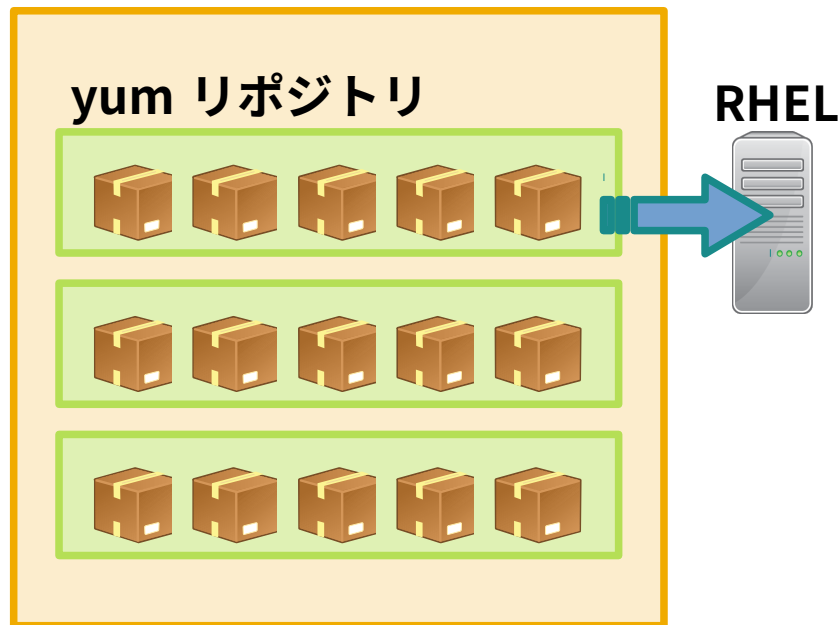
- バイナリやドキュメント等のファイルを更新
- 設定ファイルを更新
 - ユーザによる変更があった場合は 新版を別名で保存 or 旧版のバックアップを保存
- (サービスが起動していれば) サービスの再起動
- パッケージに含まれるスクリプトを実行
 - RPM パッケージは、インストールや更新の前後など各種のタイミングで実行するスクリプトを含んでいる

「パッチでの配布」との違い

- パッケージ単位で配布する Red Hat の方式は、以下の特徴があります
- 特定の修正（パッチ）だけを選択的に適用する方法は提供されません
 - 例：バグ修正がおこなわれたのち、セキュリティ上の問題に対する修正がおこなわれた。セキュリティ上の問題に「だけ」対応したパッケージを導入したい → 実現不可
- パッケージをダウングレードすることでアップデートのキャンセルが非常に簡単に実施できます
 - 設定ファイルの置き換えなどが発生していなければ、パッケージをダウングレードするだけでアップデートする前の状態に戻る

yum リポジトリ

Red Hat カスタマーポータル



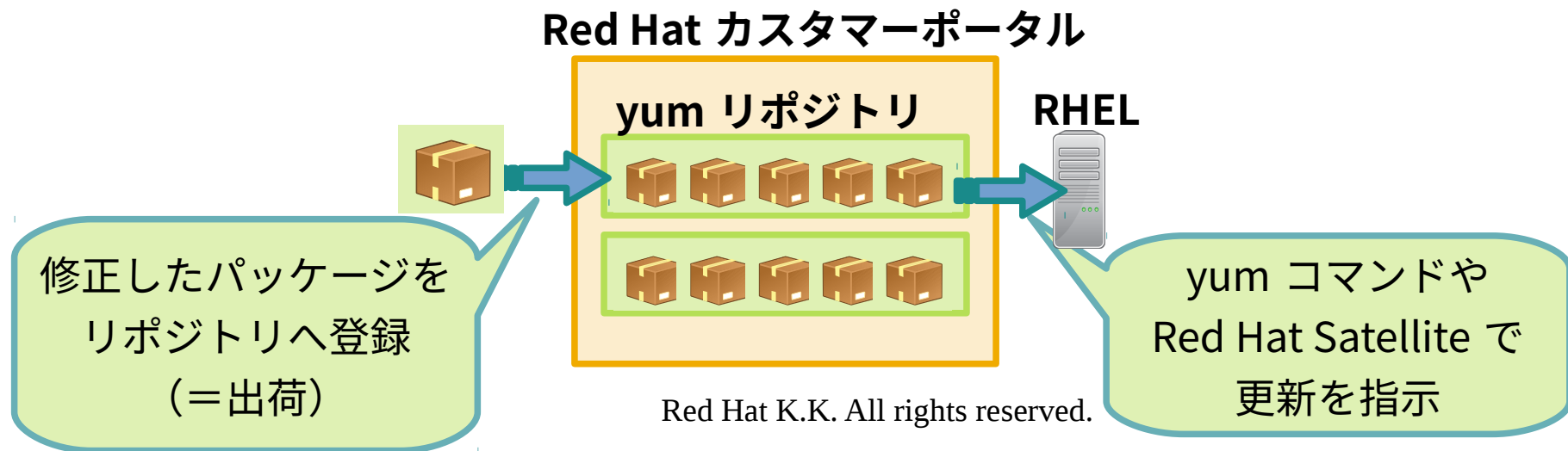
- RPM パッケージは yum リポジトリとしてグループ化されています
- システムで利用する製品やアーキテクチャにあわせて yum リポジトリを選択して利用します
 - RHEL では「subscription-manager」で選択

yum コマンド

- yum コマンドは yum リポジトリを利用して、 rpm パッケージの新規導入や更新を行います
 1. yum リポジトリの情報を取得
 2. rpm パッケージの依存関係を解決し必要パッケージを確定
 3. 必要な rpm パッケージを自動的にダウンロード
 4. パッケージの導入または更新を実施
- 「yum update」コマンドを実行することで全パッケージについてまとめて更新を行います

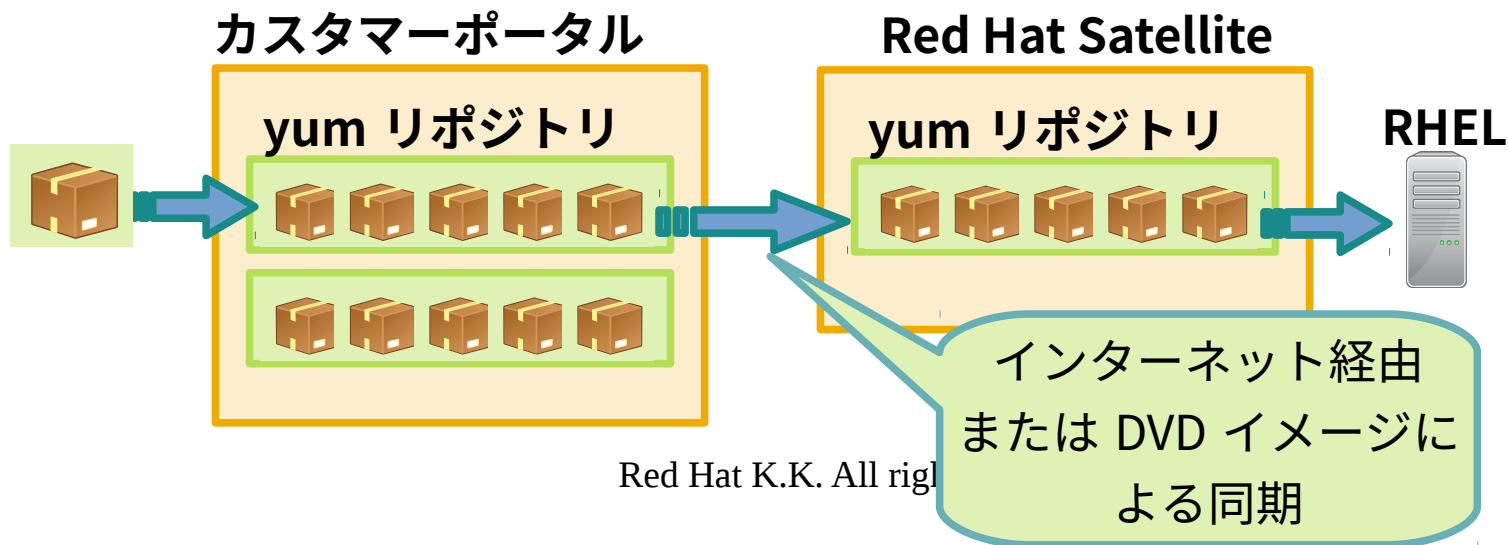
RHEL 修正の「出荷」とは

- 修正の出荷はパッケージをリポジトリに登録することで行われます
 - アドバイザリ（後述）も同時に作成・登録されます
- 修正の適用は自動や強制ではなく、各システムで yum コマンドを使っておこないます



インターネット接続できない場合の更新

- インターネット接続できない場合は？
 - Red Hat Satellite Server を LAN 内に構築して配布
 - Red Hat Customer Portal から必要パッケージを同期



修正の出荷ポリシー



バックポート

- Red Hat 製品では、コミュニティの最新バージョンに含まれるバグ修正を、製品に含まれる過去のバージョンに適用しています
 - 動作の違いを最小限にとどめて問題を修正します
- バックポートの例：
 - RHEL 7 の openssl は 1.0.2k というバージョンをベースにメンテナンスされているもの
 - **openssl コミュニティ**：脆弱性 CVE-2017-3736 への対策は、openssl 1.0.2m および 1.1.0g に対して行われた
 - **レッドハット**：RHSA-2018:0998 で openssl-1.0.2k に同じ問題への修正を反映。
openssl の 1.0.2l や 1.0.2m で行われた機能拡張などは含まないが脆弱性対策は行われた
パッケージ openssl-1.0.2k-12 を出荷

<https://access.redhat.com/ja/security/updates/backporting>

バックポートの注意点

- 一部のセキュリティ監査ツールはソフトウェアのバージョン番号だけを参照して問題を報告します。問題は既に Red Hat 製品では対策済みである場合があります
 - セキュリティ問題の CVE 名を確認し、Red Hat CVE データベースを確認します
- 警告と確認の例：
 - 監査ツールが openssl 1.0.2k を利用していることを検出し「バージョン 1.0.2k は 1.0.2m より古く脆弱性 CVE-2017-3736 を持っているはず」なので警告を出力
 - Red Hat CVE データベースを確認
<https://access.redhat.com/security/cve/cve-2017-3736>
 - 「RHEL7 の openssl パッケージなら RHSA-2018:0998 を適用していれば修正済み、RHEL6 や 5 の openssl はそもそも問題を含まない、JBoss EWS 2 に含まれる openssl は影響を受けるが修正予定がない」など製品の状況が記載されていることを確認する

修正が出荷される期間

- 修正が作成・出荷される期間は
ライフサイクルポリシーにより定められます
 - 例 : RHEL 5/6/7 では初期リリースから 10 年間
- 製品によっては延長サポートが利用できるものがあります
 - EUS: 特定マイナーリリースの延長サポート
 - ELS: 特定メジャーバージョンの延長サポート

ライフサイクルポリシーはどこにある？

- Red Hat カスタマーポータルにて公開されています
 - https://access.redhat.com/ja/support/policy/update_policies

サポート > ライフサイクルとアップデートポリシー

ライフサイクルとアップデートポリシー

Red Hat 製品に関連するライフサイクルでは、最初のリリース（一般提供 (GA)）からメンテナンスの終了に至るまでの期間、製品のリリースごとにさまざまなレベルのメンテナンスが設けられています。Red Hat 製品のライフサイクルは長期であるため、IT 投資における選択の幅が広がり、より柔軟に計画を立てることができます。今後の見通しが明確で、特定の製品にしばられることがないため、コストを削減し、不確定な要素を軽減することができます。Red Hat 製品のライフサイクルやサポート方針の詳細は、以下のリンクを参照してください。

[Production Life Cycle Checker](#) を使用すると、複数の製品のライフサイクルを同時に確認できます。

特定の Red Hat 製品のライフサイクルおよびサポートポリシーについての詳細は以下のリンクを参照してください。

Red Hat Enterprise Linux	Red Hat JBoss Middleware	OpenShift
<ul style="list-style-type: none">• Red Hat Enterprise Linux<ul style="list-style-type: none">◦ ライフサイクル サポートポリシー• Red Hat Developer Toolset• Red Hat OpenStack Platform• Red Hat Enterprise MRG• Red Hat Enterprise Linux for Real Time• Red Hat HPC Solution	<ul style="list-style-type: none">• Red Hat JBoss Middleware <div>Red Hat Containers</div> <ul style="list-style-type: none">• Red Hat Container Development Kit<ul style="list-style-type: none">◦ サポートポリシー• Red Hat Development Suite	<ul style="list-style-type: none">• OpenShift Container Platform<ul style="list-style-type: none">◦ ライフサイクル サポートポリシー• OpenShift Online<ul style="list-style-type: none">◦ ライフサイクル サポートポリシー <div>System Management</div> <ul style="list-style-type: none">• Red Hat Ansible Automation

修正の告知



アドバイザリ

- 製品の修正や拡張はアドバイザリ（ 勧告 , Errata とも ）とよばれる形で告知されます
 - 各アドバイザリには（ 通常 ）RPM パッケージが含まれる
 - 一つのアドバイザリで 1 つ以上の問題の修正に対応する
- アドバイザリにはどのような修正か、どのパッケージが関連するか等が記載されています

アドバイザリの例

- アドバイザリの ID
- 概要
- タイプ / 重大度
- トピック
- 修正内容の説明
- 影響を受ける製品、修正パッケージ
- CVE
- 参考資料

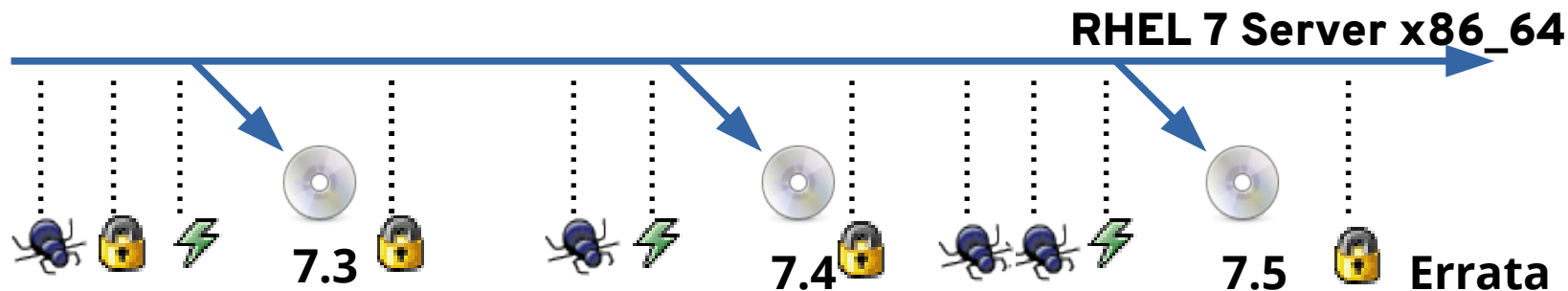
Red Hat K.K. All rights reserv

概要	更新パッケージ
<h2>概要</h2> <p>Important: kernel security and bug fix update</p> <h3>タイプ/重大度</h3> <p>Security Advisory: Important</p> <h3>トピック</h3> <p>An update for kernel is now available for Red Hat Enterprise Linux 7.</p> <p>Red Hat Product Security has rated this update as having a security impact of important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.</p> <h3>説明</h3> <p>The kernel packages contain the Linux kernel, the core of any Linux operating system.</p> <p>Security Fix(es):</p> <ul style="list-style-type: none">• kernel: Integer overflow in Linux's create_elf_tables function (CVE-2018-14634) <p>For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.</p> <p>Red Hat would like to thank Qualys Research Labs for reporting this issue.</p> <p>Bug Fix(es):</p> <p>These updated kernel packages include also numerous bug fixes. Space precludes documenting all of the bug fixes in this advisory. See the descriptions in the related Knowledge Article:</p> <p>https://access.redhat.com/articles/3588731</p> <h3>解決法</h3> <p>For details on how to apply this update, which includes the changes described in this advisory, refer to:</p> <p>https://access.redhat.com/articles/11258</p> <p>The system must be rebooted for this update to take effect.</p> <h3>影響を受ける製品</h3> <ul style="list-style-type: none">• Red Hat Enterprise Linux Server 7 x86_64• Red Hat Enterprise Linux Server - Extended Update Support 7.6 x86_64• Red Hat Enterprise Linux Server - Extended Update Support 7.5 x86_64• Red Hat Enterprise Linux Server - AUS 7.6 x86_64• Red Hat Enterprise Linux Workstation 7 x86_64• Red Hat Enterprise Linux Desktop 7 x86_64• Red Hat Enterprise Linux for IBM z Systems 7 s390x• Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.6 s390x• Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.5 s390x• Red Hat Enterprise Linux for Power, big endian 7 ppc64• Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.6 ppc64• Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.5 ppc64• Red Hat Enterprise Linux for Scientific Computing 7 x86_64• Red Hat Enterprise Linux EUS Compute Node 7.6 x86_64• Red Hat Enterprise Linux EUS Compute Node 7.5 x86_64• Red Hat Enterprise Linux for Power, little endian 7 ppc64le• Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.6 ppc64le• Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.5 ppc64le• Red Hat Virtualization Host 4 x86_64• Red Hat Enterprise Linux Server - TUS 7.6 x86_64• Red Hat Enterprise Linux for ARM 64 7 aarch64• Red Hat Enterprise Linux for Power 9 7 ppc64le• Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 7.6 ppc64le• Red Hat Enterprise Linux Server - Update Services for SAP Solutions 7.6 x86_64• Red Hat Enterprise Linux for IBM System z (Structure A) 7 s390x <h3>修正</h3> <ul style="list-style-type: none">• BZ - 1624498 - CVE-2018-14634 kernel: Integer overflow in Linux's create_elf_tables function <h3>CVE</h3> <ul style="list-style-type: none">• CVE-2018-14634 <h3>参考資料</h3> <ul style="list-style-type: none">• https://access.redhat.com/security/update/classification/#important• https://access.redhat.com/articles/3588731	

アドバイザリの種別 と ID

アドバイザリは 3 種類に分けられていて、ID の先頭 4 文字で区別できるようになっています

- セキュリティ修正： RHSA 深刻さにより随時出荷
- バグ修正： RHBA または、アップデートリリースのタイミングで出荷
- 機能拡張修正： RHEA
 - OS のアップデートリリースのタイミングで出荷



RHSA の影響度概要

Critical	非認証のリモート攻撃者が容易に悪用でき、ユーザーの操作を必要とせずシステムが危険にさらされる（任意コード実行）不具合はこのレベルに分類されます。ワームによる悪用が可能です。
Important	リソースの機密性、整合性、または可用性が容易に危険にさらされる不具合はこのレベルに分類されます。ローカルユーザーによる権限の取得、認証されていないリモートユーザーによる認証保護リソースの閲覧、認証されたリモートユーザーによる任意のコードの実行、またはリモートユーザーによるサービス拒否はこのレベルに分類されます。
Moderate	悪用は比較的困難ですが、特定の条件下では、リソースの機密性、整合性、または可用性が一部危険にさらされる原因となる不具合はこのレベルに分類されます。
Low	悪用のためにはあり得ない状況が必要と思われるものや、悪用が成功しても影響は最小であるものです。

<https://access.redhat.com/ja/security/updates/classification>

アドバイザリを受けとる

- メールでアドバイザリを受けとります
 - カスタマーポータルにログインして以下 URL にて設定
<https://www.redhat.com/wapps/ugc/protected/notif.html>
 - 受信するアドバイザリの種類や、登録したシステムに影響するものだけに絞るか、影響しないものも含めて全て受信するか等を指定できます

システム毎のアドバイザリを確認

- カスタマーポータルにて各システムのアドバイザリを確認
 - <https://access.redhat.com/management/systems>

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	 ▾	タイプ	最終チェック イン	エラー		
<input type="checkbox"/>	● rhel7-nosat.example.com	1	仮想システム	2018/09/13	 16  29  1		
<input type="checkbox"/>	● rhel74.example.com	1	仮想システム	2018/10/15	 56  204  43		
<input type="checkbox"/>	● sat6.example.com	2	仮想システム	2018/10/18	 2  14  21		

Show 100 ▾ entries

Showing 1 to 3 of 3 entries (filtered from 6 total entries)

最初 前へ 1 次へ 最後

アドバイザリの検索

- 製品毎のアドバイザリ一覧
 - カスタマーポータル、ダウンロードページ内の「エラータ」タブで表示
 - <https://access.redhat.com/ja/downloads>
- Red Hat CVE データベース
 - 脆弱性の CVE ID から問題の概要、Red Hat 製品への影響有無の公式見解、対応アドバイザリの情報
 - <https://access.redhat.com/security/cve>

THANK YOU!