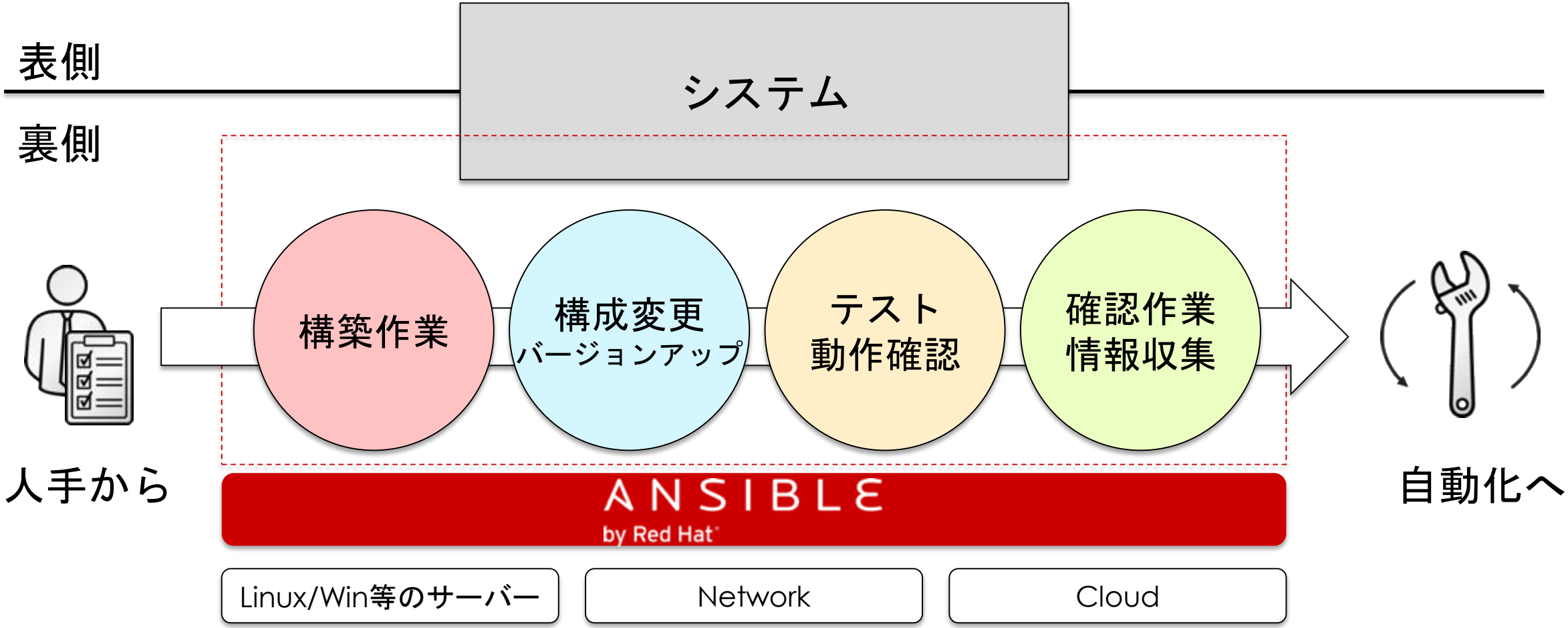
Internet Week 2018
IT Automation with Ansible

2018/11/29 - v1.0

Red Hat

Ansible Automation の役割

- ITを動かすためのITの仕組み「**IT Automation**」を実現する。



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

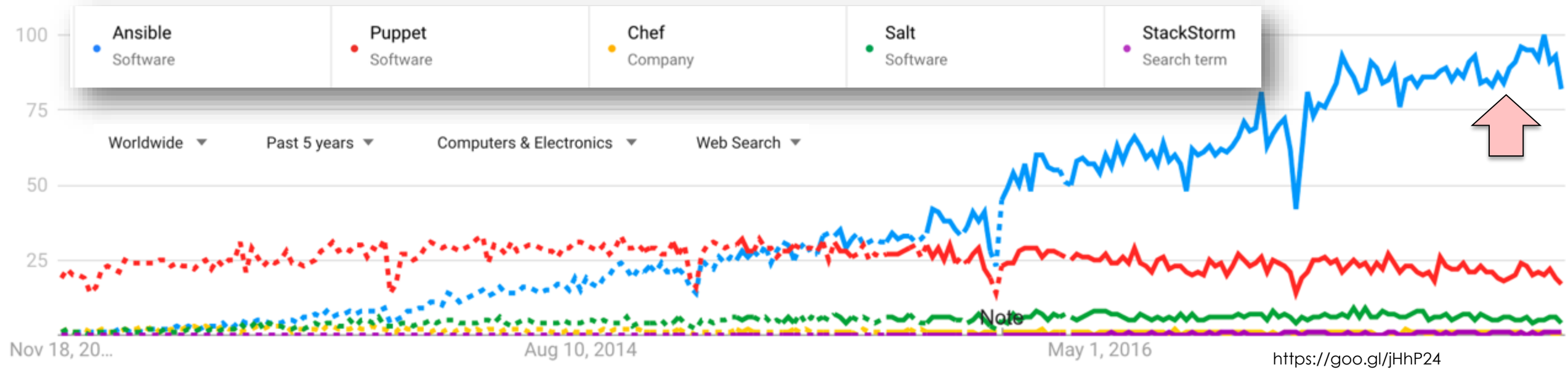
市場での状況

2,500+
contributors

10,000+
downloads/day

1250+
modules included

(including 250+ Networking modules as of April 2017!)



https://goo.gl/jHhP24

Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

redhat.

Ansible が広く利用される背景（１）

RED HAT ANSIBLE Engine

SIMPLE

誰もが読める
標準化された
自動化言語

POWERFUL

多様な制御対象を
統一的手法で
自動化

AGENTLESS

セキュアで
信頼性の高い設計

Playbook **Modules** **Architecture**

Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

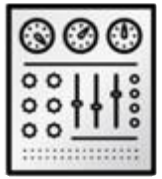
redhat.

Ansible が広く利用される背景（２）

RED HAT® ANSIBLE® Tower

組織として自動化に取り組むための ツール

- 自動化の仕組みを広範囲で活用し効果を最大化する。
- 属人性を排除し、継続的な改善を可能とする。



システムとして自動化を組み込むための ツール

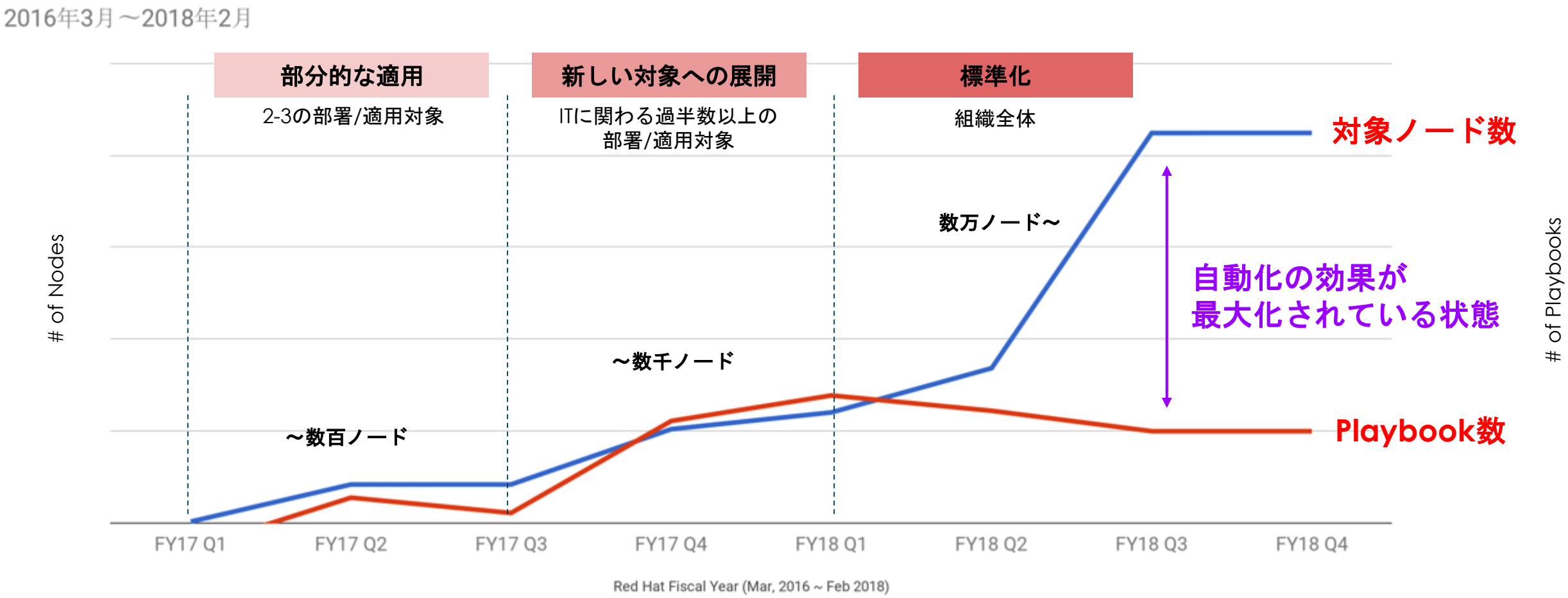
- 自動化をサービス化（機能化）する。
- API連携しシステムの一部として自動化を組み込む。
- 末端の操作を抽象化し、自動化するためのコストを削減。

Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

redhat.

開発数（Playbook数）と適用ノードの関係イメージ

- Ansible Automation は「組織としての自動化」を強力に推進。



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

Ansible は作業の部品化と再利用が可能

文書No	123-4567890-A	作成者	最終更新者	承認	確認	作成/更新
文書名	XXXX作業手順書	T.N	R.K	印	印	印
		作成日	最終更新日			
		2017/12/XX	2018/2/YY			

作業No	作業概要	作業内容	実施者	実施日時	確認者
1	作業前確認	作業端末を起動し以下のユーザーでログインを行う。 ユーザー：xxxxxx パスワード：パスワード管理票を参照 ログイン後に、作業端末のデスクトップに「XXX」フォルダを確認する。			

2	作業対象へ接続	作業対象「SSH」へ SSH ログインする。
		ターミナルソフトを起動して、以下を入力。
		
		$ ssh ops@192.168.xx.yy
		password:
		
		$ hostname
		target_node
		
		ホスト名がターゲットのノードであれば作業を継続する。			

3	yyyyyy	AAAAAAAAAA BBBBBBBBBB CCCCCCCCCC DDDDDDDDD			

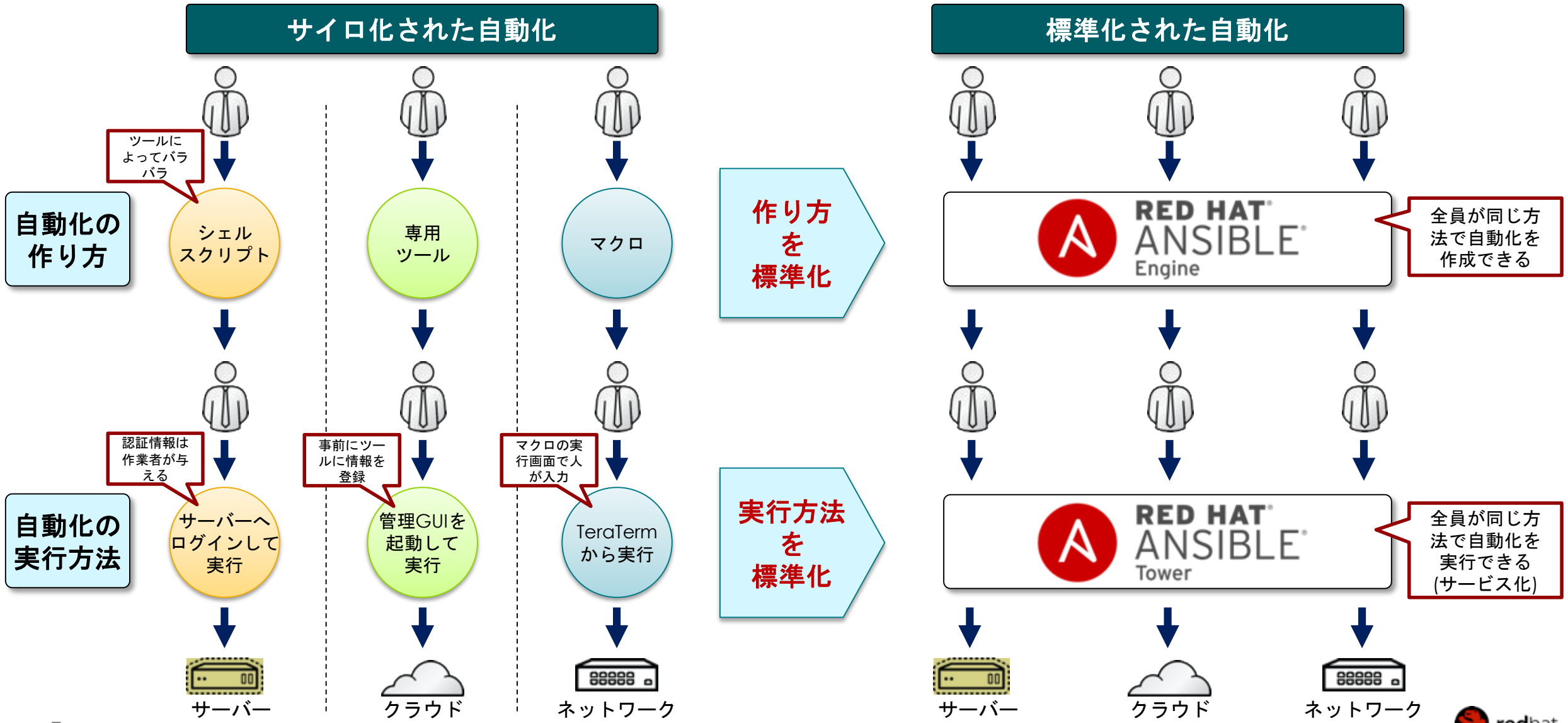
作業全体は特定のシステムにしか使えない
オンリーワンの手順書だが・・・

個別の作業要素の大部分は
共通化可能なものが相当数存在する。

ある会社では、自社の手順書を精査しところ、7割前後が「いろいろ確認して最後にプロセス/サービスの再起動」を行う手順書だったという話もあります。

Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

Ansible は「自動化手法の標準化」を実現



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

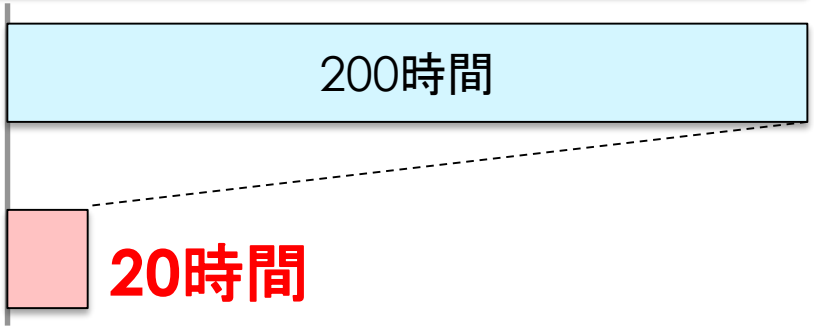
自動化のもたらす効果

Before
After

アプリケーションのリリース作業

通信業

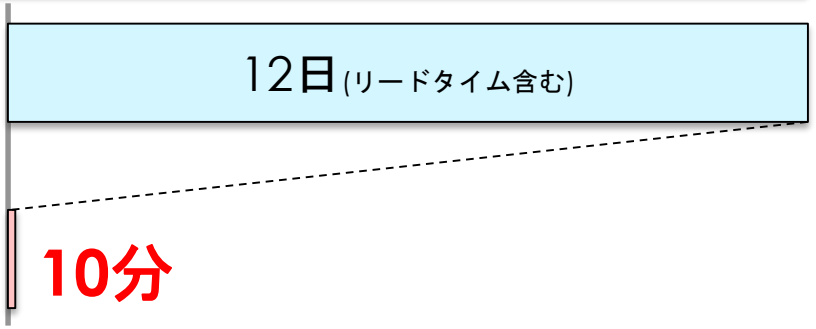
定期的に行われるアプリケーションのリリース作業を自動化して**90%の工数を削減**



プライベートクラウドのリソース払い出し作業

情報サービス業

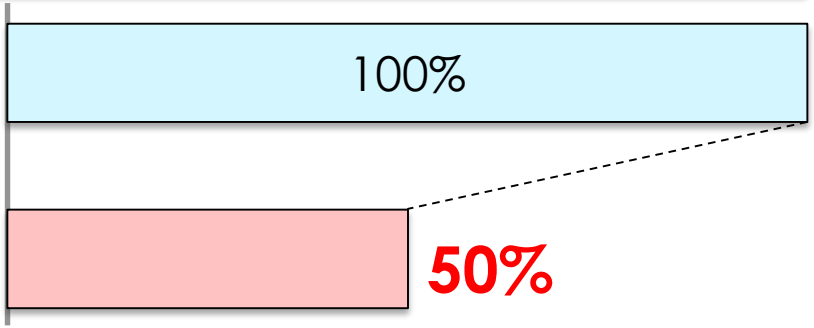
リソースの払い出しを自動化し、**大幅なスピードUPを実現。**



仮想化基盤の全運用作業

社会インフラ

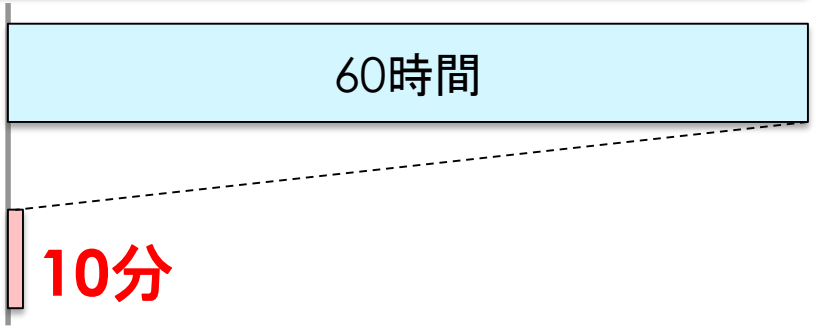
日常的な運用作業を自動化することで**全体工数を半減。削減した工数を新たな仕事へ**シフト。



大規模クラウドサービスの運用作業

情報サービス業

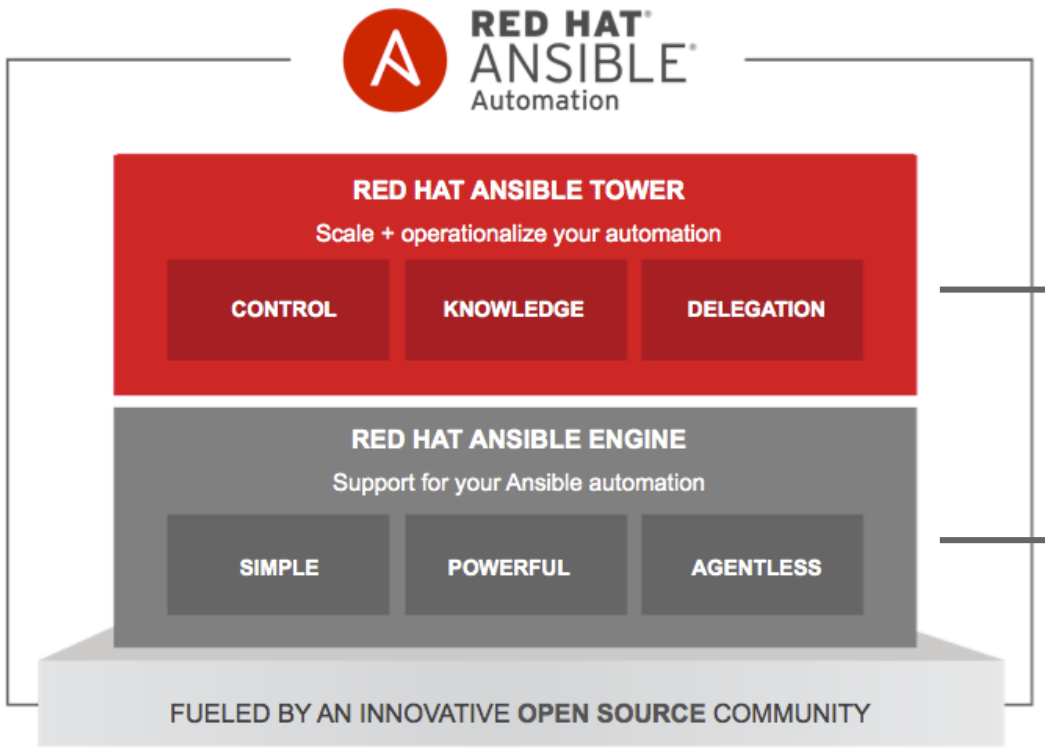
クラウド基盤のメンテナンス作業を自動化して**大幅な時間短縮を実現し、オペミスも削減。**



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

redhat.

Ansible Automation の全体像



分類	コミュニティ （誰でも利用可能）	エンタープライ （レッドハットが提供&サポート）
自動化プラットフォーム （GUI/REST API/ 権限管理/ 実行履歴管理など）	**AWX Project**	**Ansible Tower** (*1)
動作エンジン （コア、モジュール）	**Ansible Project**	**Ansible Engine** (*2,*3)

*1) 評価版のライセンス提供あり
*2) モジュールのサポートはコアに限定
*3) Network Moduleのサポートとして、Red Hat Ansible Automation (Networking) を提供

Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

Ansibleによる自動化の進め方（小さく初めて大きく育てる）

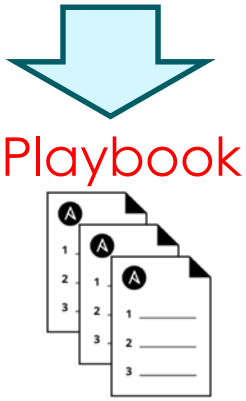
単純に手順を置き換える
（簡単な箇所から小さく部分的な自動化）

置換

パラメータシート

手順書

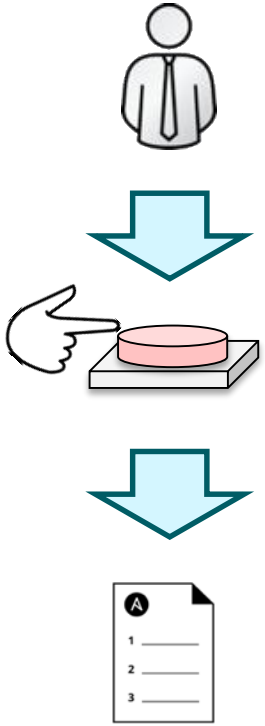
テスト仕様書



Playbook

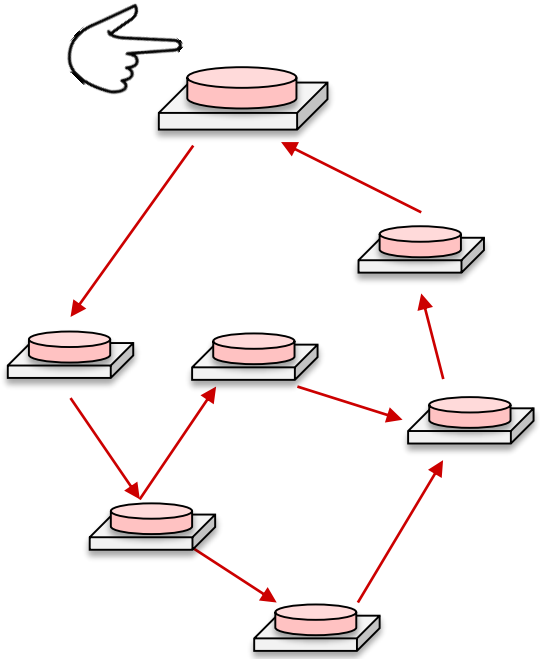
自動化を機能化して
別の人に実行してもらう

機能化（サービス化）



小さな機能を連結して
大きな機能を作る

連結

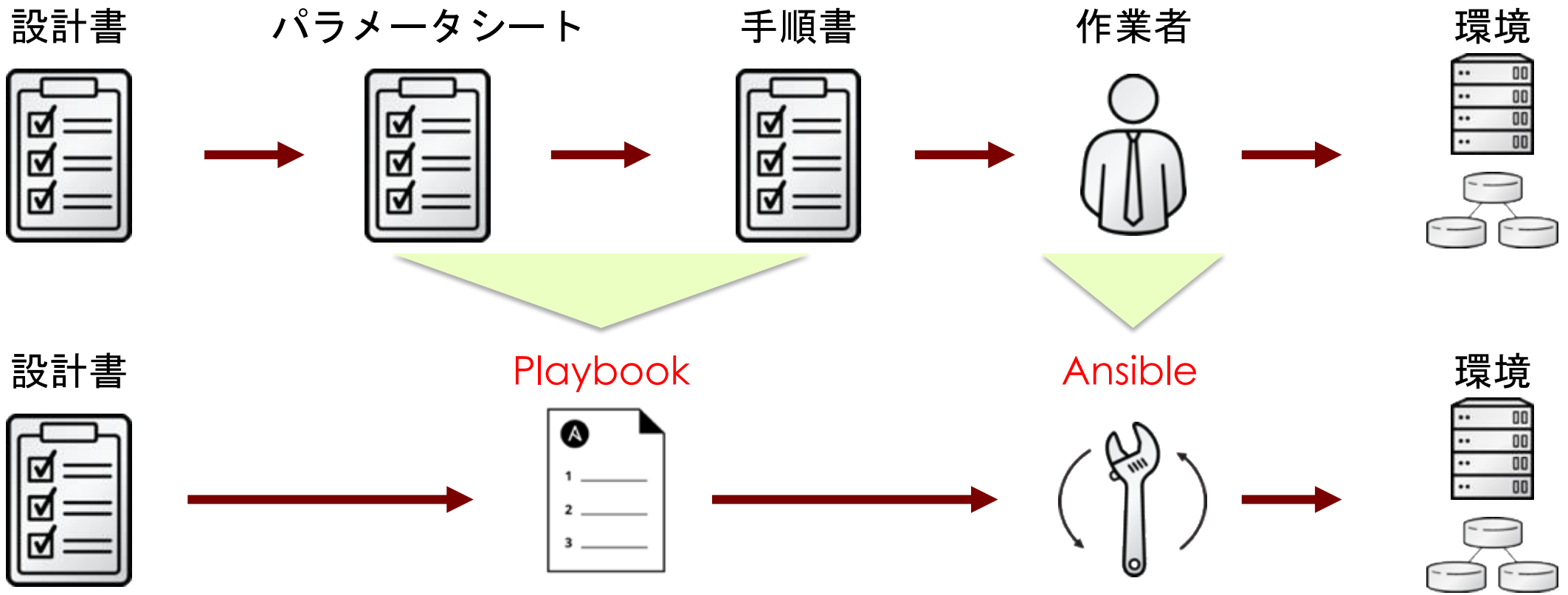


Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

redhat.

手順書の置き換え

- 現行の手順をPlaybookとして置き換え自動化する。
  - Playbook は実行可能なパラメータシート兼手順書として利用できる。



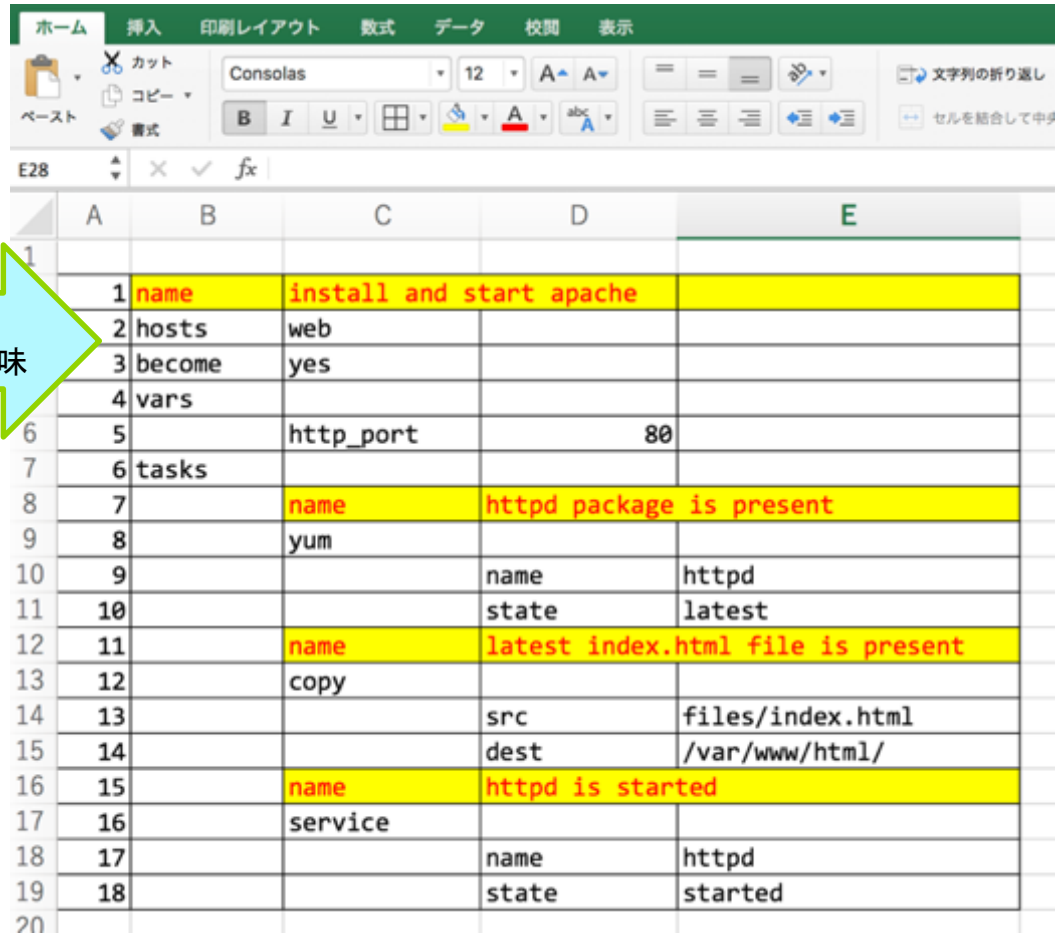
Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

自動化を記述する「Playbook」

- YAML 形式で記述されたパラメータと手順

```
---
- name: install and start apache
  hosts: web
  become: yes
  vars:
    http_port: 80

  tasks:
  - name: httpd package is present
    yum:
      name: httpd
      state: latest

  - name: latest index.html file is present
    copy:
      src: files/index.html
      dest: /var/www/html/

  - name: httpd is started
    service:
      name: httpd
      state: started
```

ほぼ
同じ意味



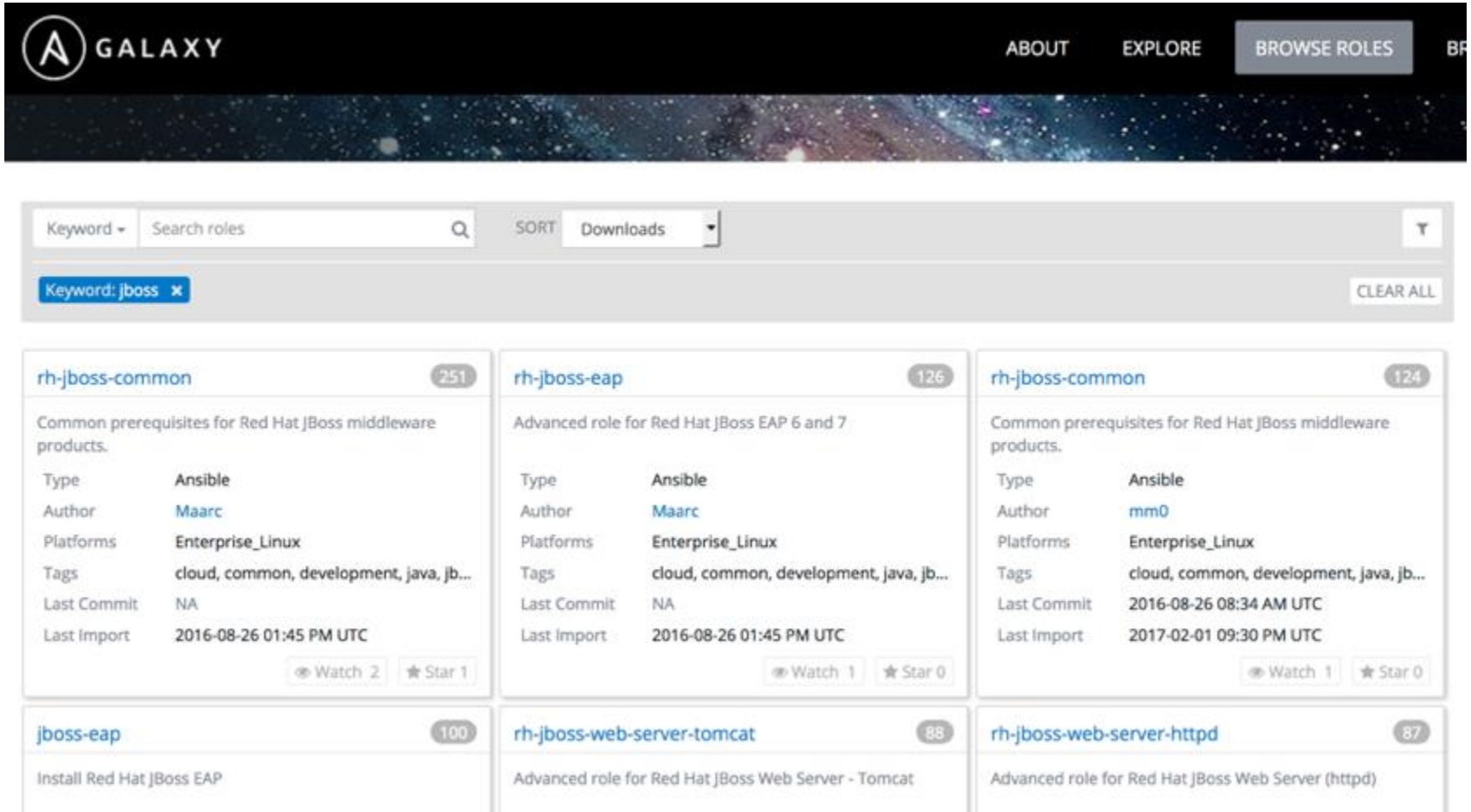
	A	B	C	D	E
1					
2	1	name	install and start apache		
3	2	hosts	web		
4	3	become	yes		
5	4	vars			
6	5		http_port	80	
7	6	tasks			
8	7		name	httpd package is present	
9	8		yum		
10	9			name	httpd
11	10			state	latest
12	11		name	latest index.html file is present	
13	12		copy		
14	13			src	files/index.html
15	14			dest	/var/www/html/
16	15		name	httpd is started	
17	16		service		
18	17			name	httpd
19	18			state	started
20					

「コード」なので、
コーディング規約の準
拠などをプログラムで
チェック可能

nauthorized persons or third parties except by written agreement with Red Hat.
redhat.

集合知の活用

- インターネット上に多数のPlaybookが公開されており、**ゼロからの試行錯誤を省く**ことができる。



https://galaxy.ansible.com/

Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

テストの自動化

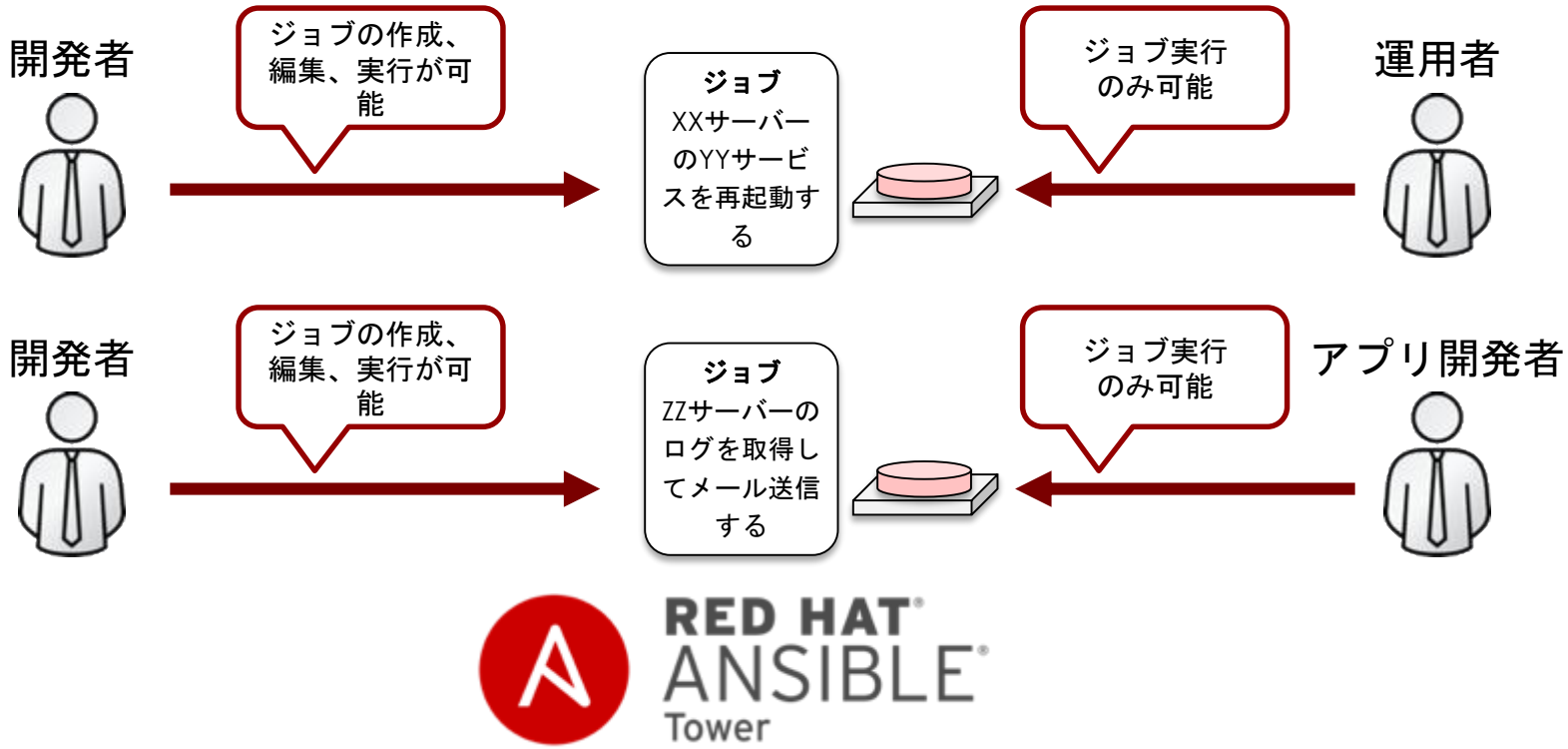
- 構築の正しさを検証
  - 想定した状態になっているかの確認
- インフラの結合テスト
  - 複数機器やOSにまたがるテスト
  - 人では実現できない網羅的なテスト
- 何度でもコストゼロで繰り返せる
  - テストが蓄積されるほど品質が向上
    - 自動化導入当初はテスト項目10個。
    - 1年後には100個。
  - 人では不可能なテストの実施
    - 100個のテストを100台のサーバーへ実施。
    - 構築後だけでなく、バージョンアップや構成変更のたびに実施。

```
tasks:
  - name: 対象サーバーのポートがOpenしているか
    local_action:
      module: wait_for
      host: "{{ inventory_hostname }}"
      port: 80
      state: started
      delay: 3
      timeout: 10

  - name: ゲートウェイにping送信可能か
    shell: |
      ping -c 3 {{ ansible_default_ipv4.gateway }}

  - name: コンテンツが配布されているか
    shell: |
      test -f /var/www/html/index.html

  - name: コンテンツがHTTP経由で取得できるか
    local_action:
      module: uri
      url: http://{{ inventory_hostname }}/
      validate_certs: no
      timeout: 5
      return_content: yes
    register: webpages

  - name: TEST check contents
    assert:
      that:
        - (webpages.content | search(query))
    vars:
      query: "{{ content_msg }}"
```


Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.
redhat.

オペレーションの委託（サービス化）

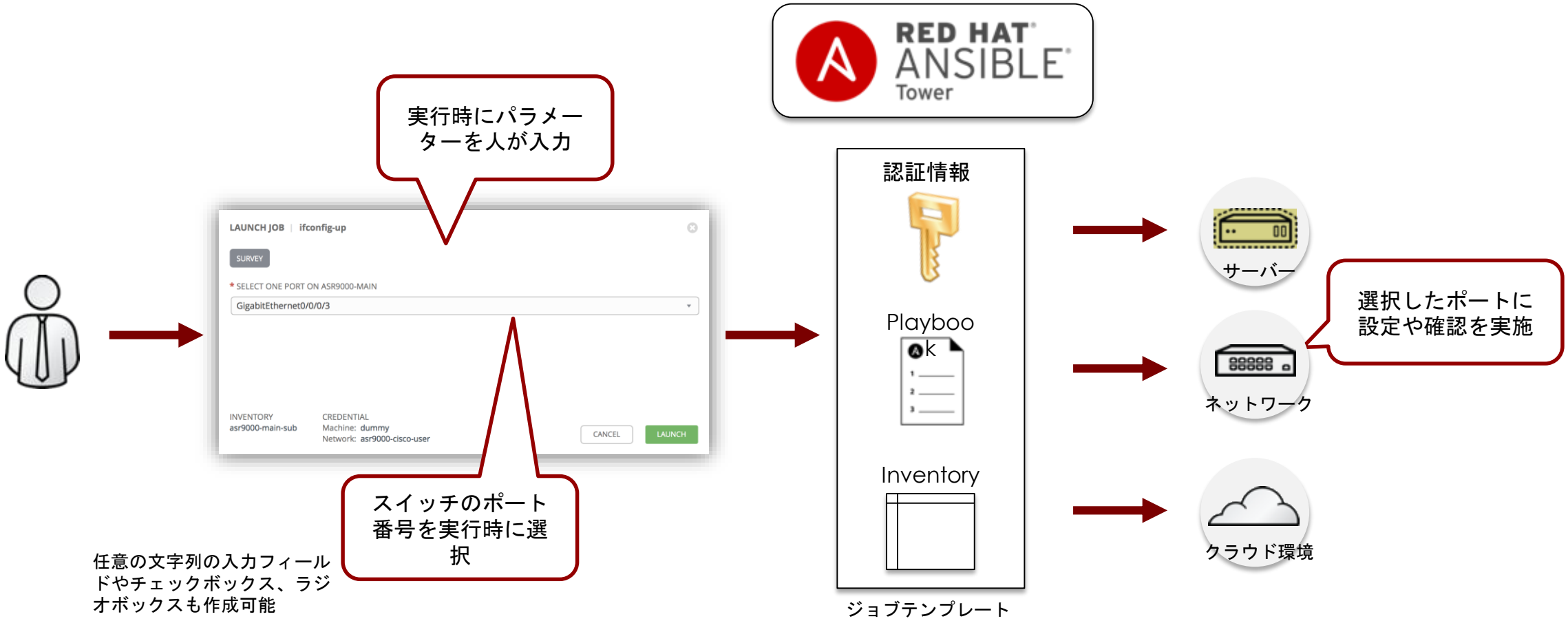
- 作成した自動化の権限を移乗することが可能。
  - オペレーターにサービスの自動再起動の操作「だけ」を実行「だけ」させたい。
  - アプリ開発者にサーバーの自動ログ収集の操作「だけ」を実行「だけ」させたい。



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

簡易セルフサービスポータル

- 実行時にジョブテンプレートに対して、パラメーターを与えるGUIを作成可能。



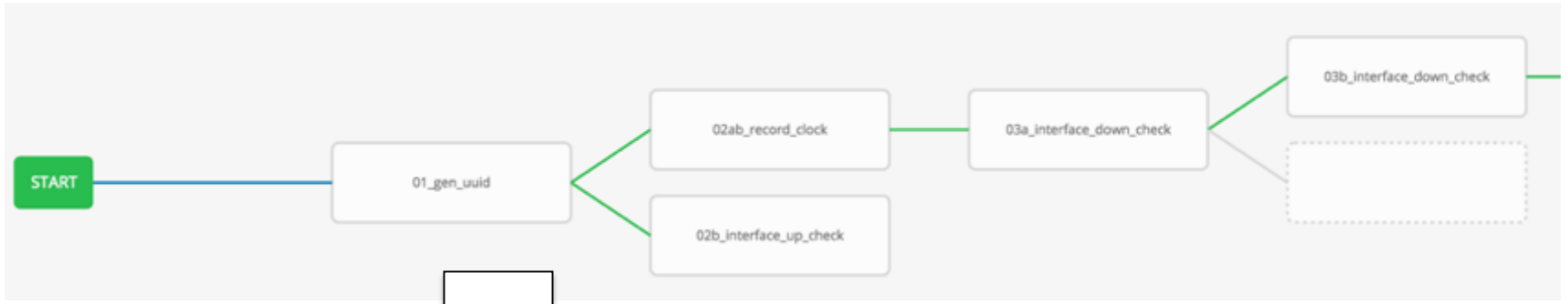
Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

共通化、組み合わせによる自動化の実現

- パーツ化したPlaybookを共有・連結し、大きな自動化を低コストで実現

OpenStack上にサーバーを構築

```
- name: launch an instance
  os_server:
    state: present
    name: vm1
    availability_zone: tokyo
    image: RHEL7.3
    key_name: my-key
    timeout: 200
    flavor: m1.medium
```



ワークフローをGUIから構築可能

AWSにサーバーを構築

```
- name: launch an instance
  ec2:
    key_name: mykey
    instance_type: t2.micro
    image: ami-123456
    wait: yes
    group: webserver
    vpc_subnet_id: （略）
    assign_public_ip: yes
```

ソフトウェアを設定

```
- name: install httpd
  yum:
    name: httpd
    state: latest
  become: true
```

設定のテスト

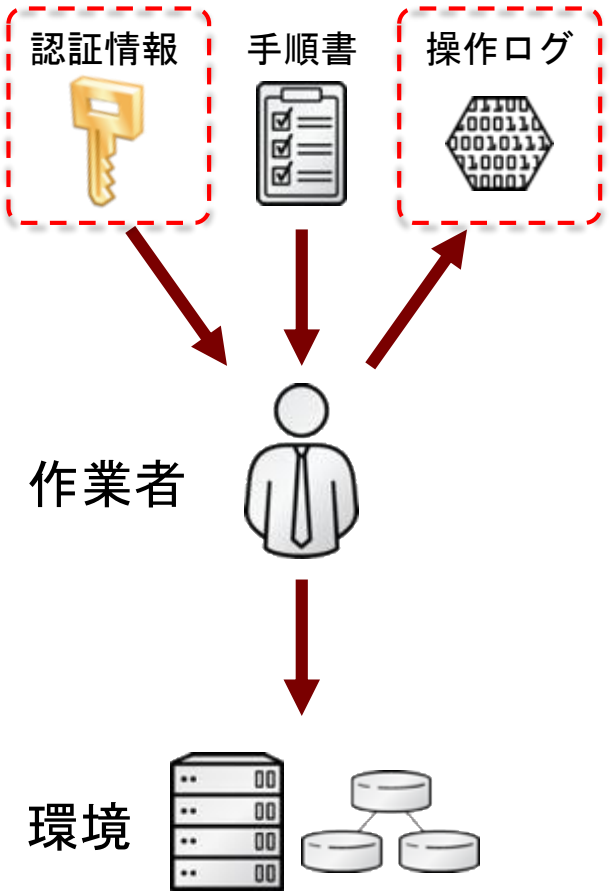
```
- name: TEST wait for HTTP port up
  local_action:
    module: wait_for
    host: "{{ inventory_hostname }}"
    port: 80
    state: started
    delay: 3
    timeout: 10
```

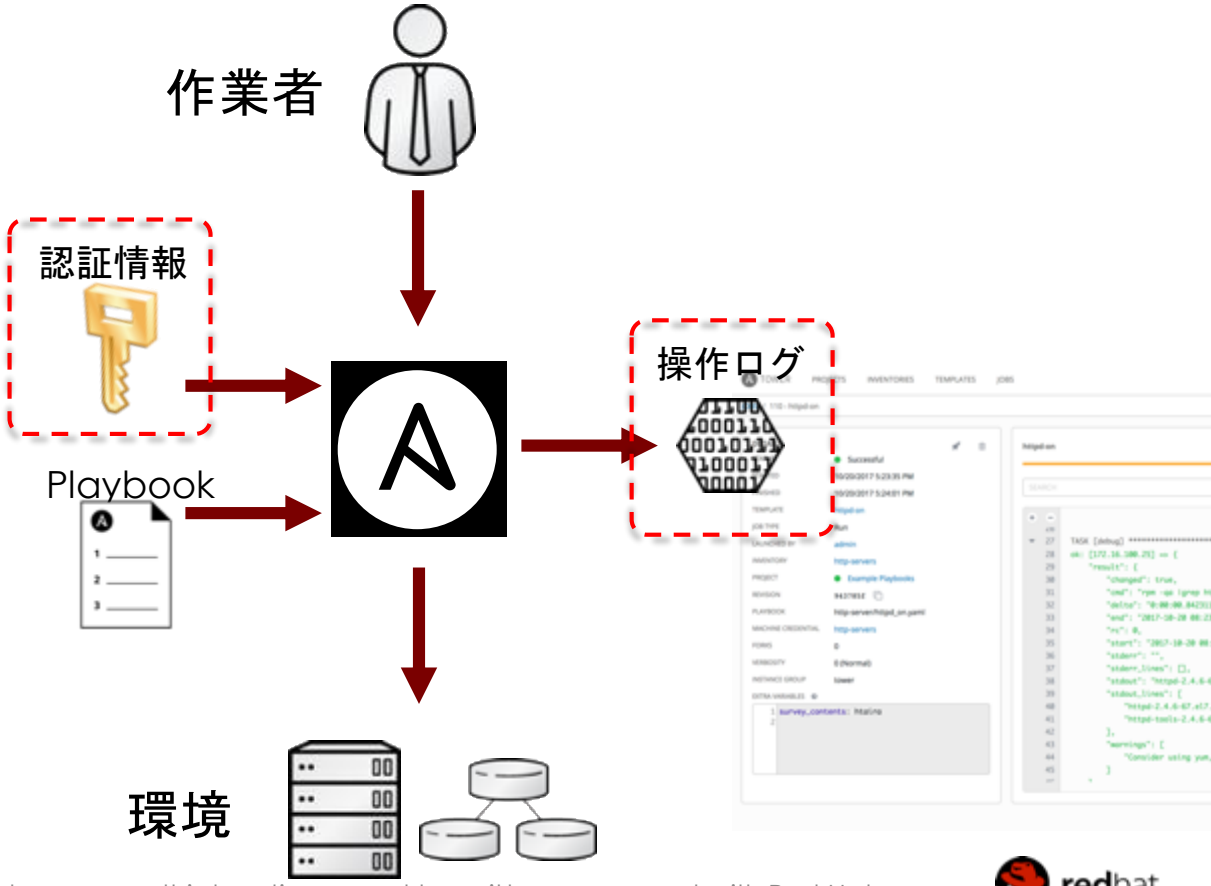
環境に依存せず共通化して利用可能

Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

作業者と認証情報の分離によるセキュリティの向上

- 認証情報を暗号化して作業者に対して隠蔽します。
- 作業内容はPlaybookとして履歴管理され、「いつ」「誰が」「何を」「どこに」実施したかを記録します。



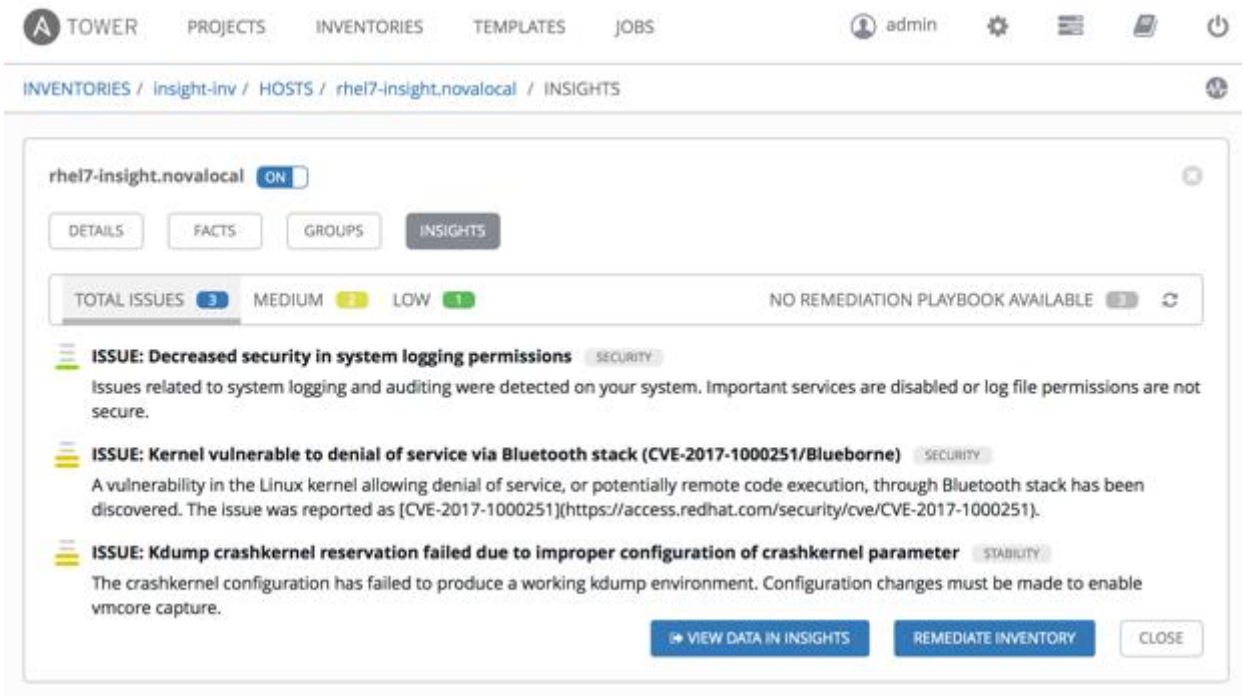


Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

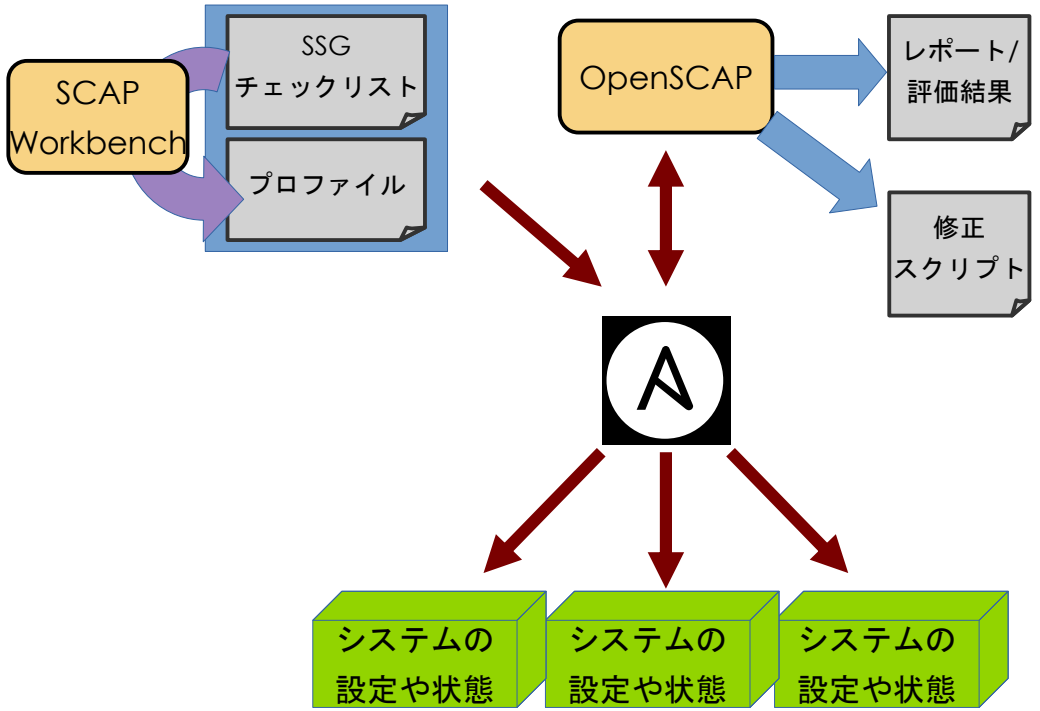
定期的な安全性・適合チェック

- Red Hat Insights 連携で既知の脆弱性、複数の設定間の齟齬、既知の問題がある設定などを検出し、修正Playbookを提供。
- OpenSCAPと組み合わせた脆弱性診断やポリシー（PCI-DSS準拠など）チェックの実施。

Insights 連携による脆弱性一覧



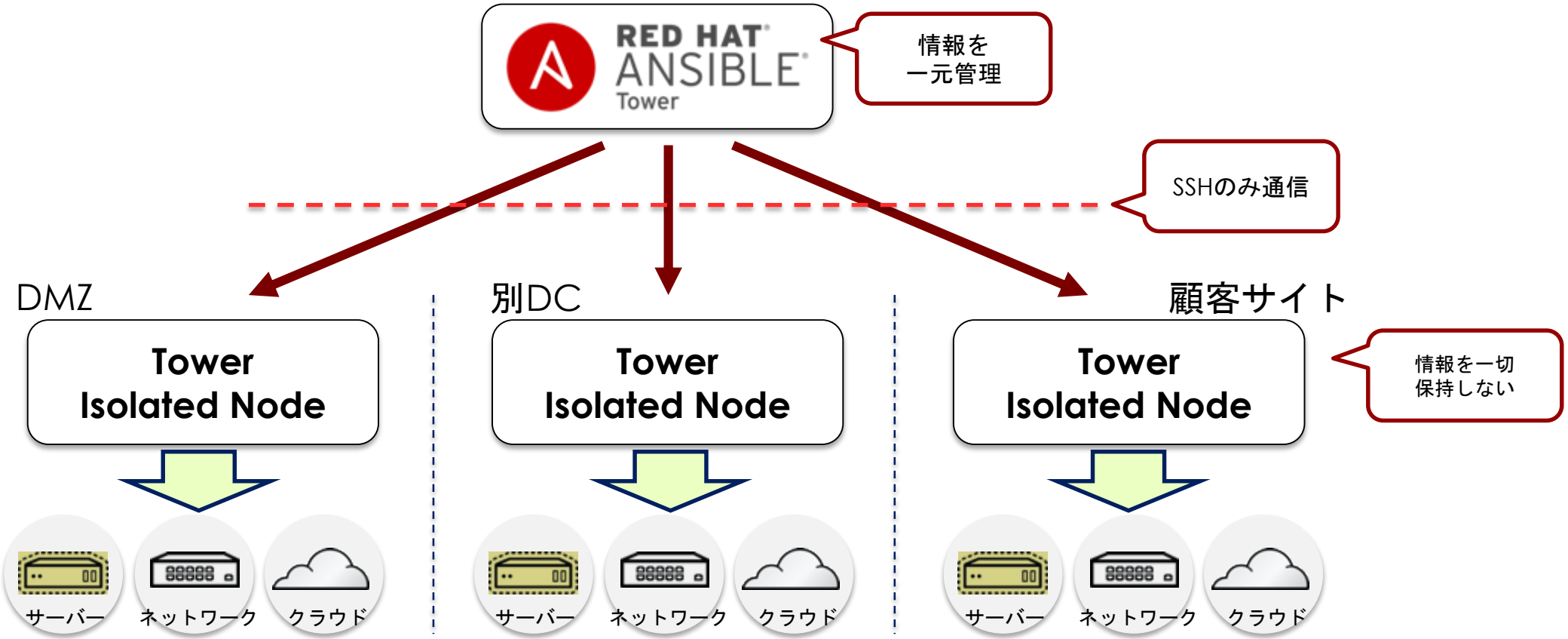
OpenSCAPとの組み合わせによる脆弱性診断



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

リモートの自動化環境を安全に一元管理可能

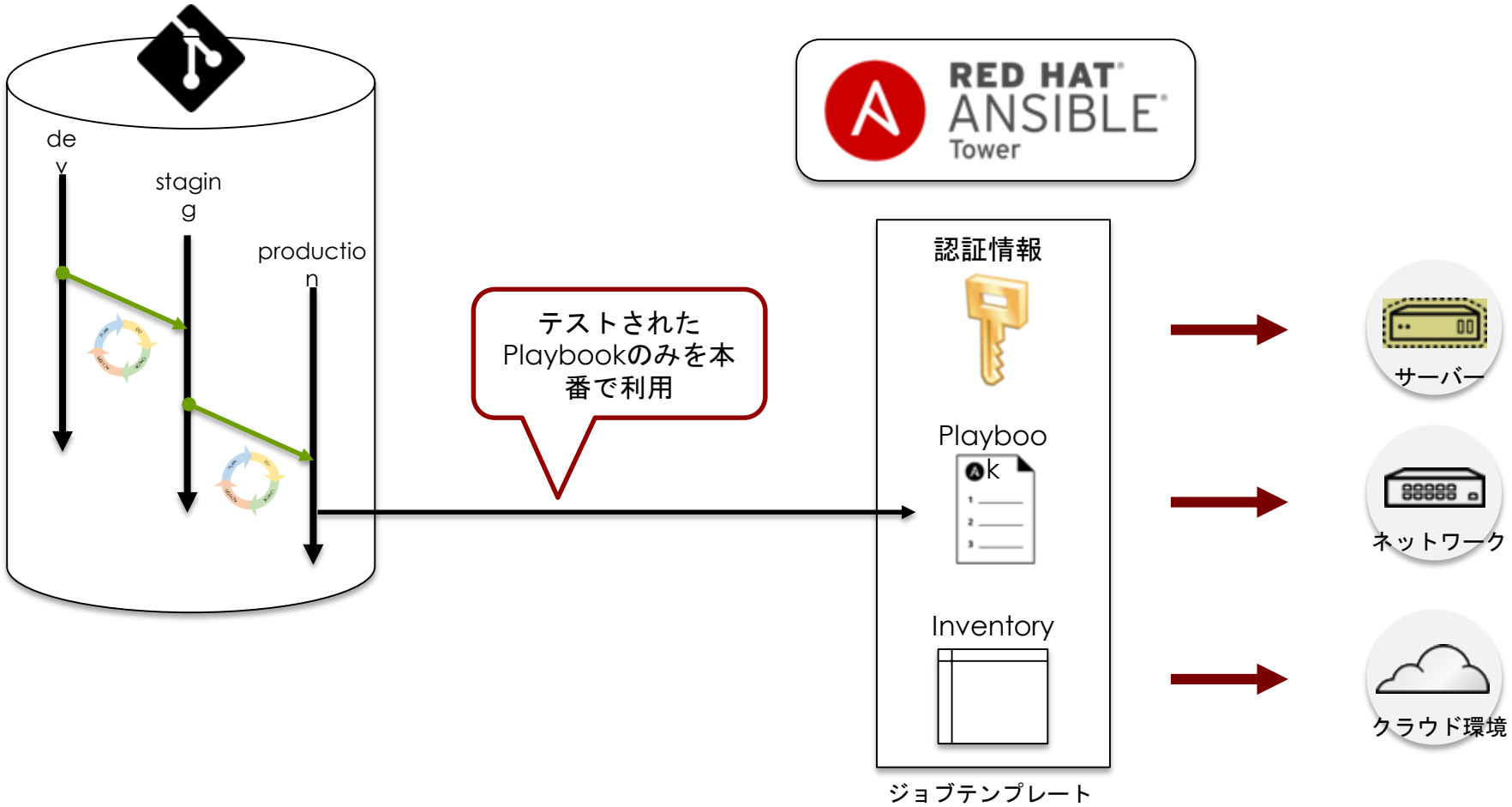
- Isolated Node 機能を使うと、地理的に離れた場所での自動化を一つのTowerから実施できるようになります。



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

SCM連携

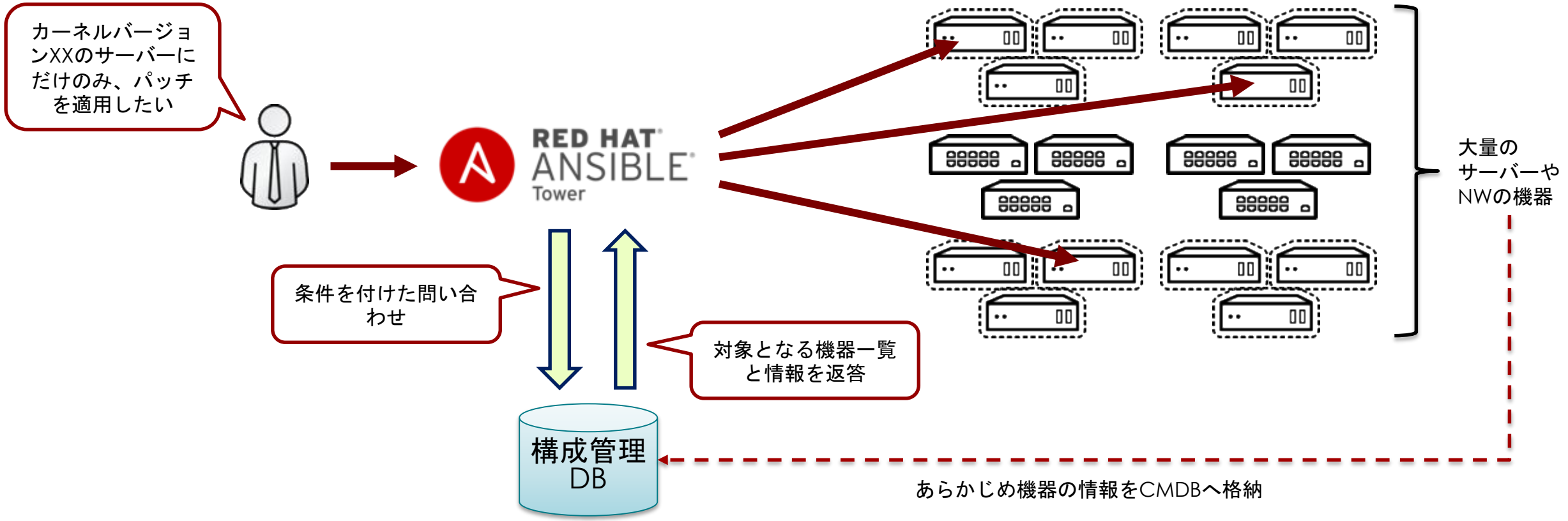
- バージョン管理されていない野良Playbookや、CI等による品質管理の連携が可能。



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

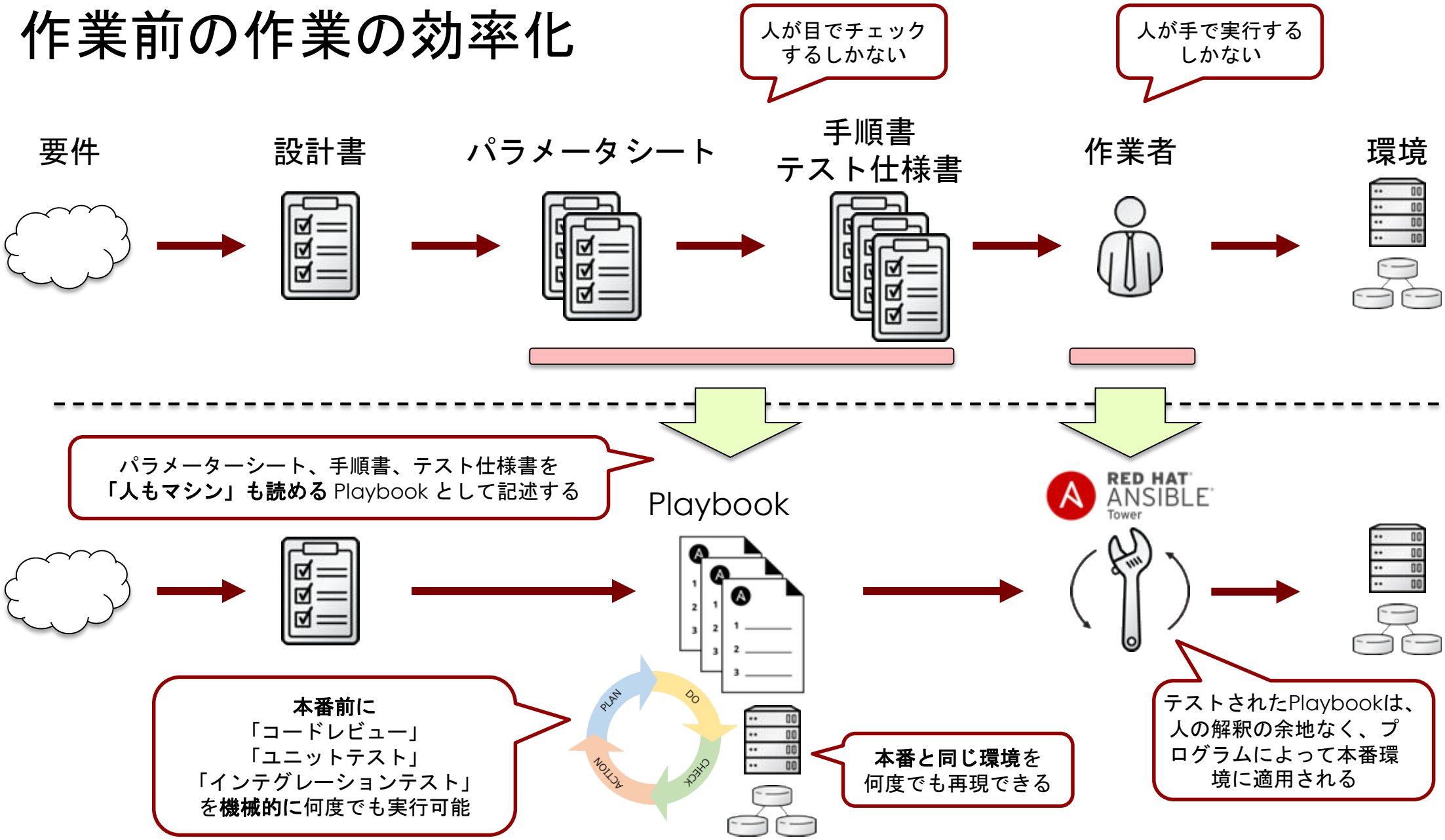
多数の自動化の対象をCMDBと連携して管理

- 多数の機器の中から特定条件に合致する対象のみに自動化を「安全、確実」に実行する。
  - OSのバージョン、インストールされているパッケージ、特定のコンフィグが設定されている、など



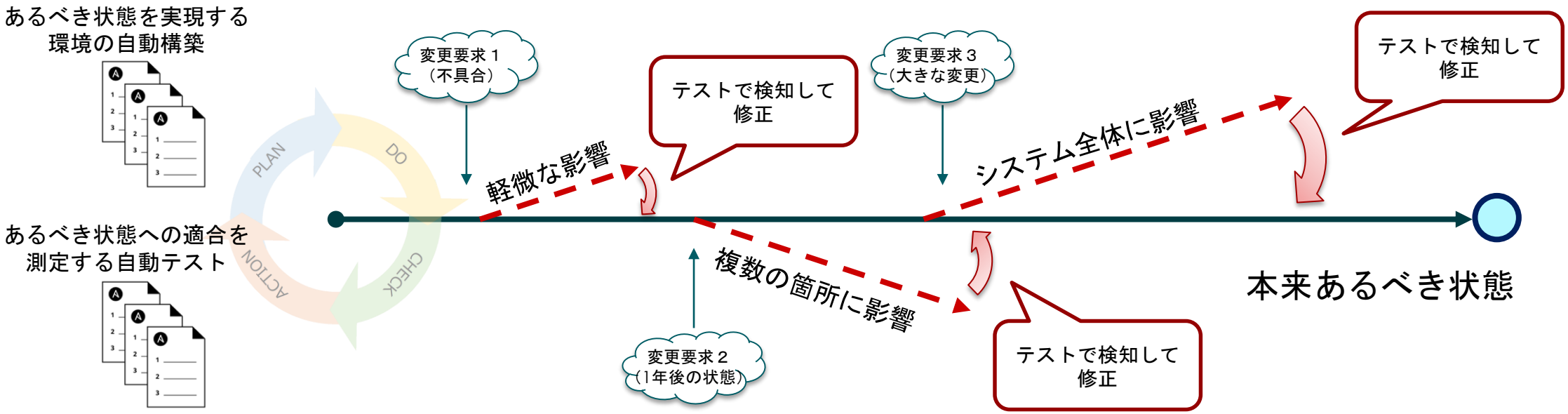
Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

作業前の作業の効率化



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

変化の影響度を測定しながら安全に作業

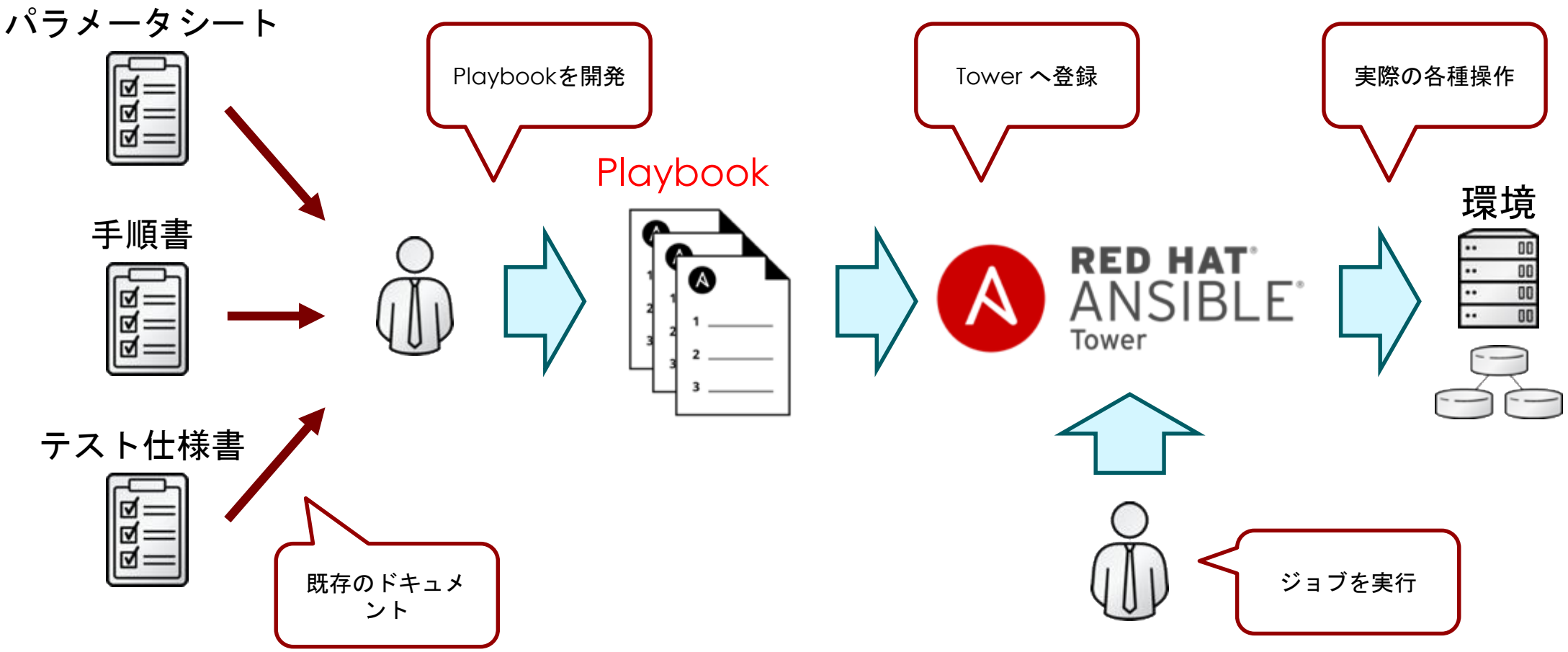


項目	初期状態	変更要求１の結果	変更要求２の結果	変更要求３の結果
テスト1	○	○	○	X
テスト2	○	○	X	X
機能1	○	○	X	X
機能2	○	○	○	X
性能1	100	102	110	30
性能2	200	210	80	110

Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

活用イメージ

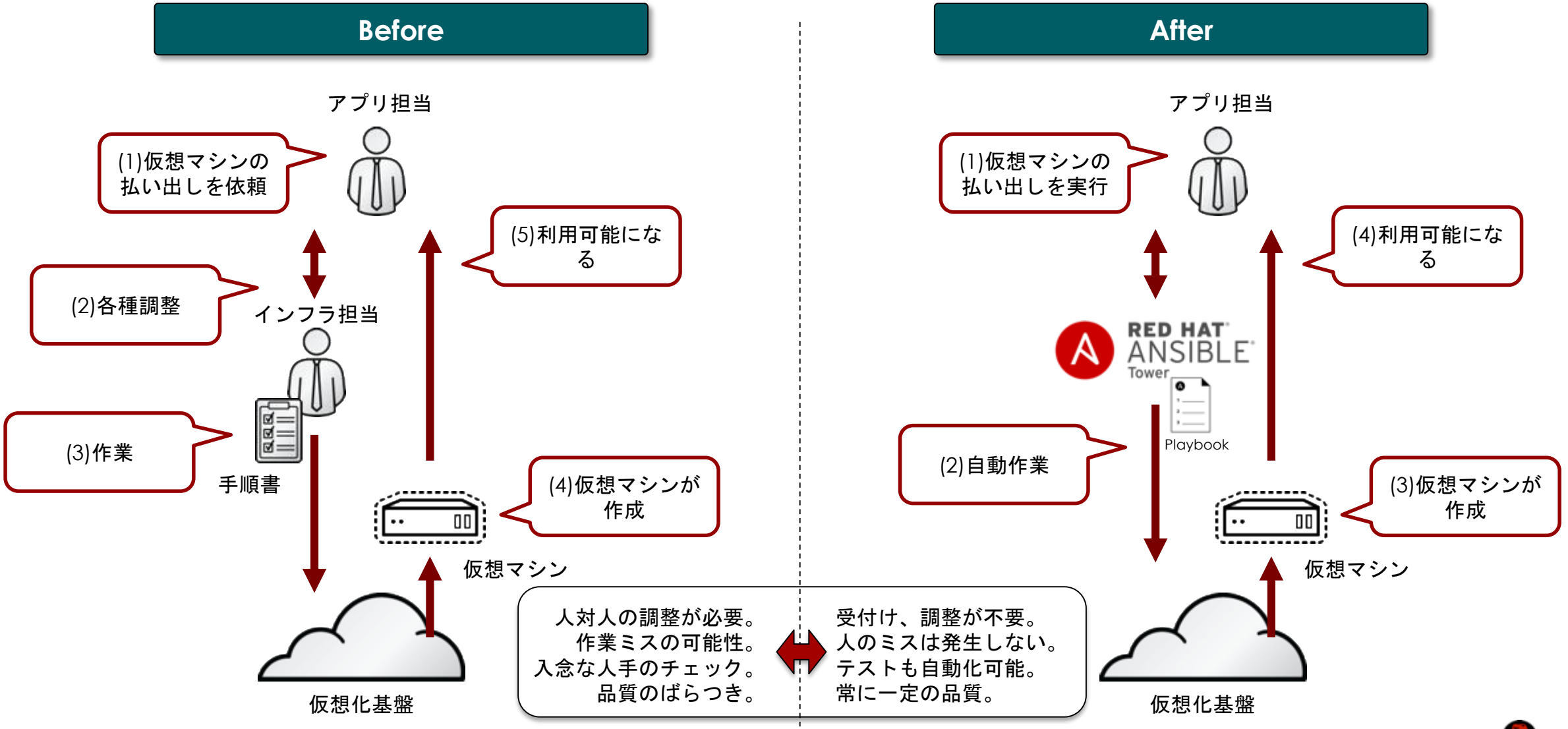
Ansible での自動化の流れ



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

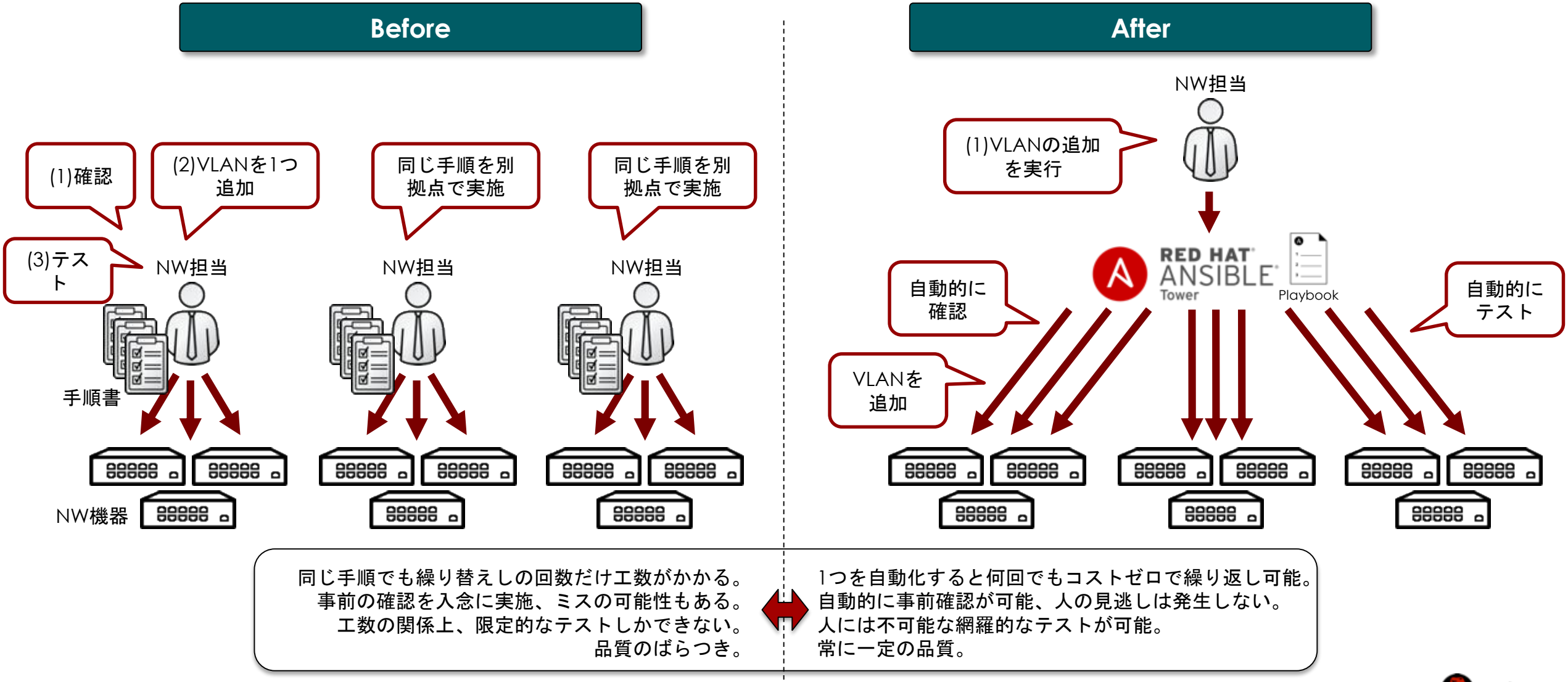
redhat.

自動化例：仮想化基盤の運用改善例



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

自動化例：ネットワーク管理の改善例



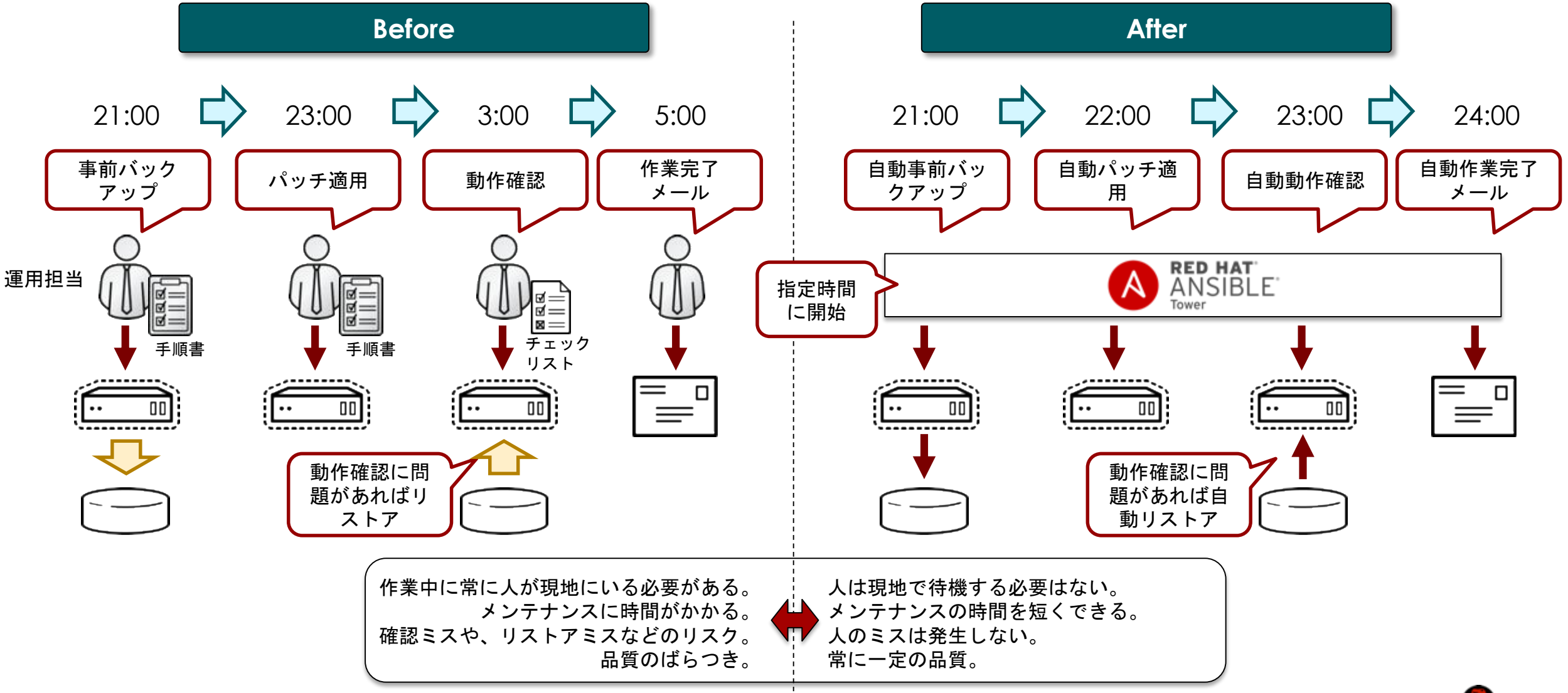
同じ手順でも繰り替えしの回数だけ工数がかかる。
事前の確認を入念に実施、ミスの可能性もある。
工数の関係上、限定的なテストしかできない。
品質のばらつき。

⇔

1つを自動化すると何回でもコストゼロで繰り返し可能。
自動的に事前確認が可能、人の見逃しは発生しない。
人には不可能な網羅的なテストが可能。
常に一定の品質。

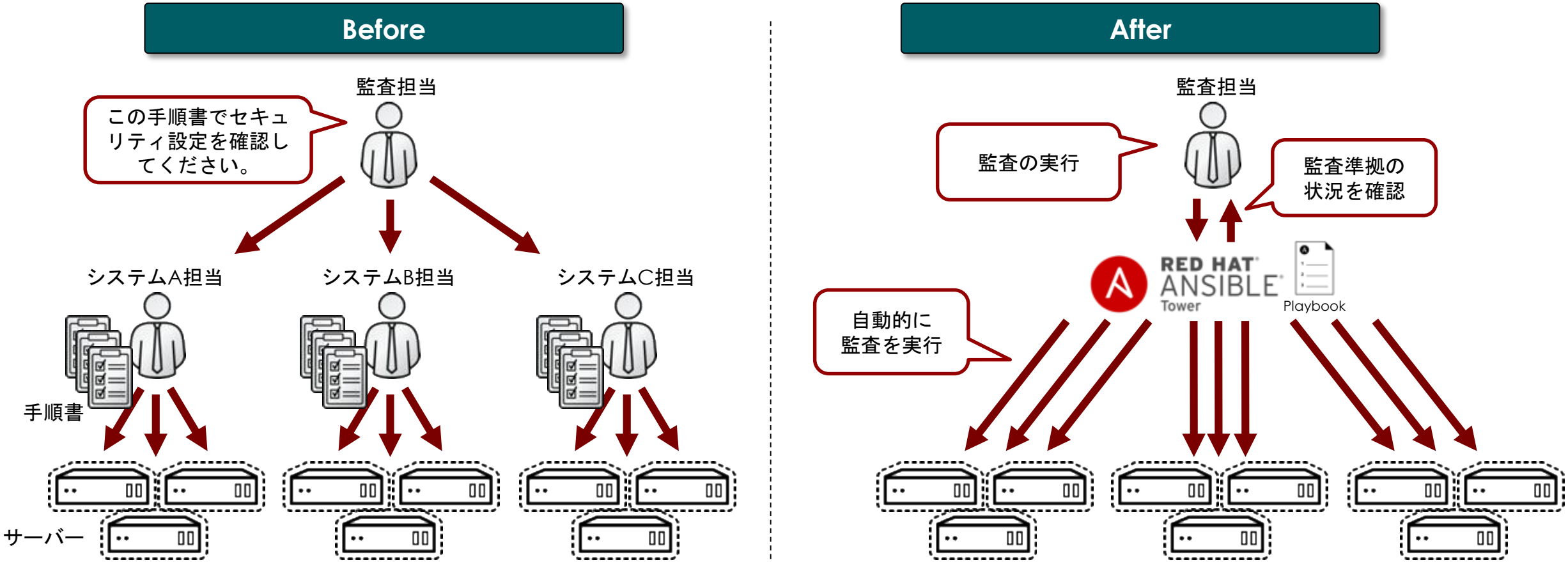
Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

自動化例：夜間パッチ適用作業の改善例



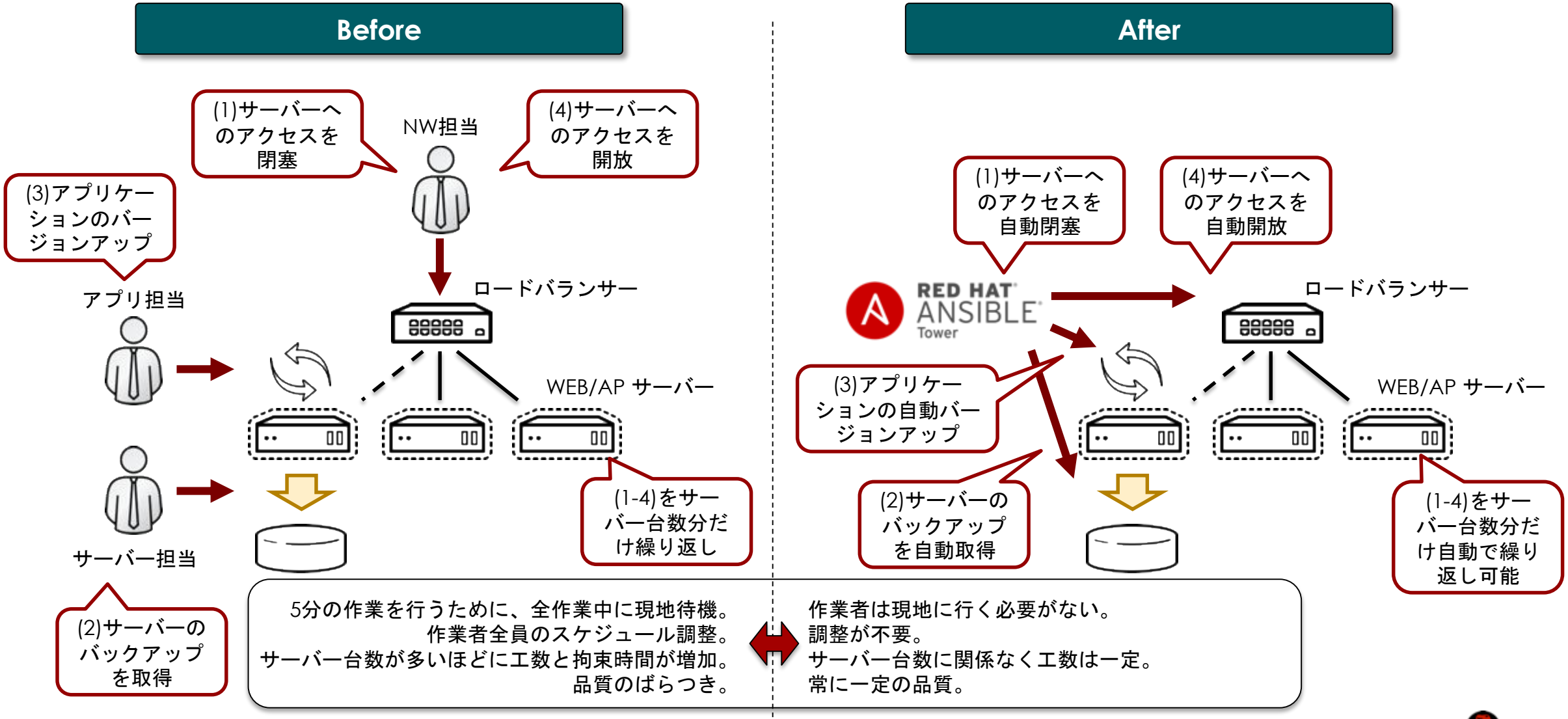
Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

自動化例：セキュリティ監査の改善例



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

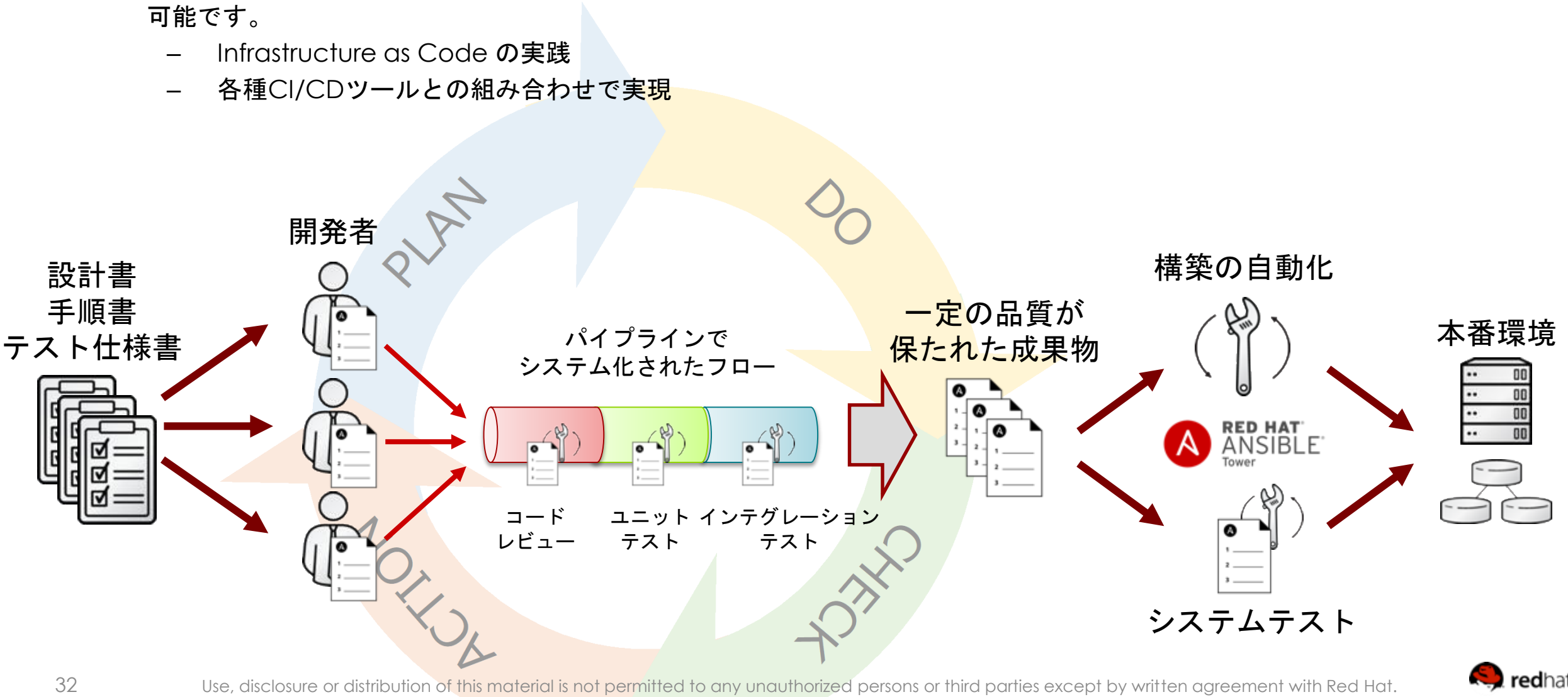
自動化例：リリース作業の改善例



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

インフラのCI(CD)の実践例

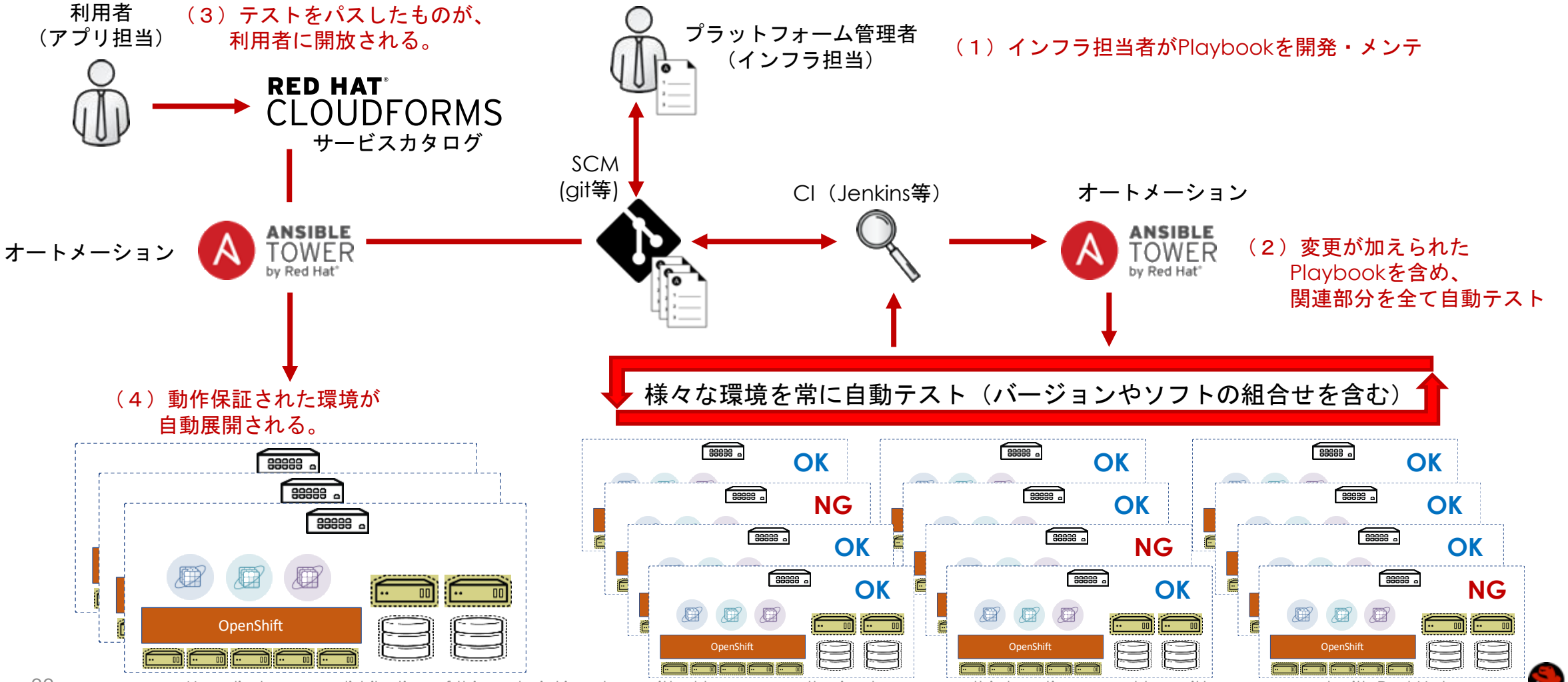
- システム化された自動テストを開発フローへと組み込み、一定の品質を担保した成果物（Playbook）を開発することが可能です。
  - Infrastructure as Code の実践
  - 各種CI/CDツールとの組み合わせで実現



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

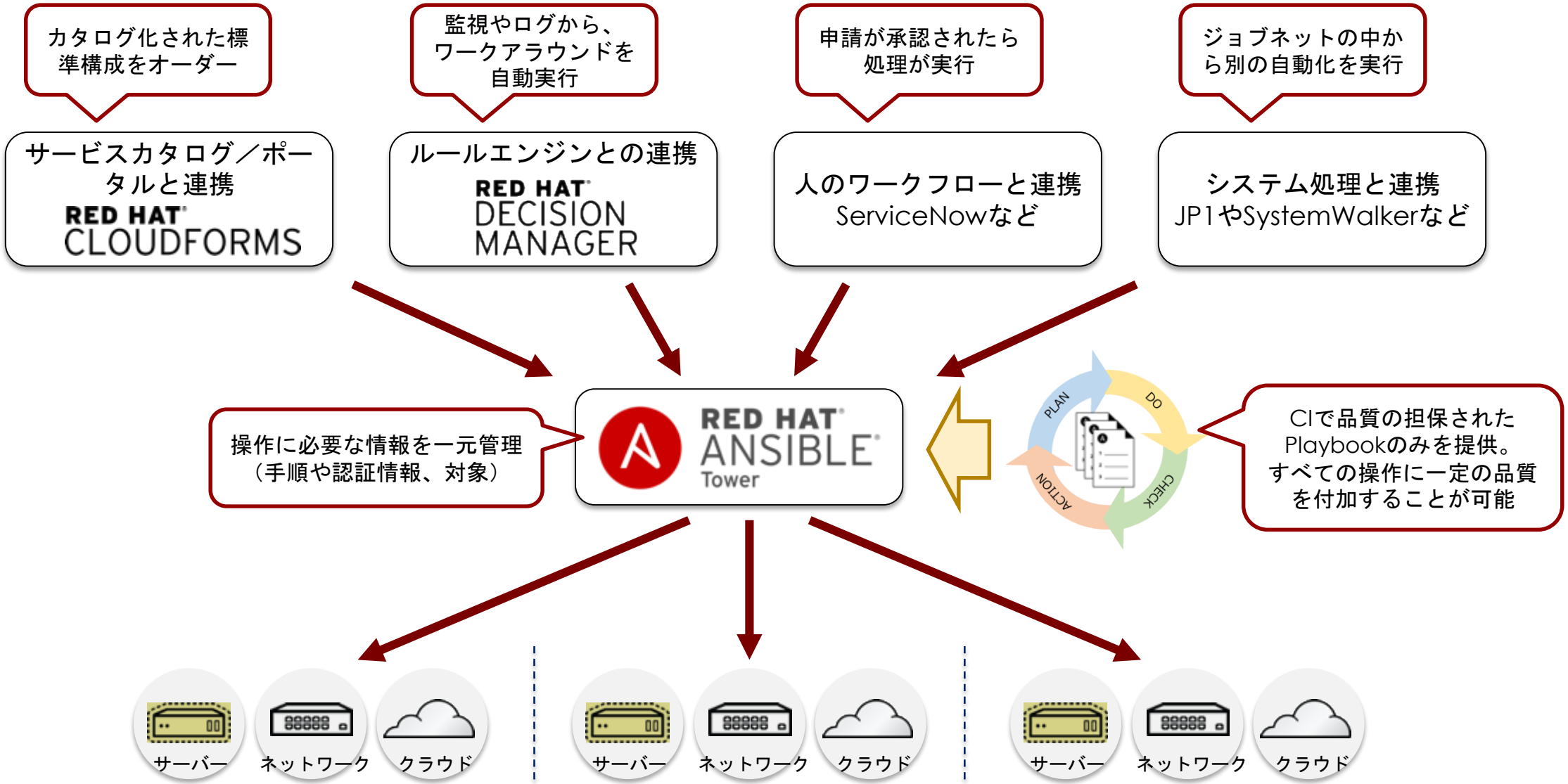
インフラの完全セルフサービス化例

- 継続的な改善。環境変化への対応。Playbookの鮮度や品質の維持。



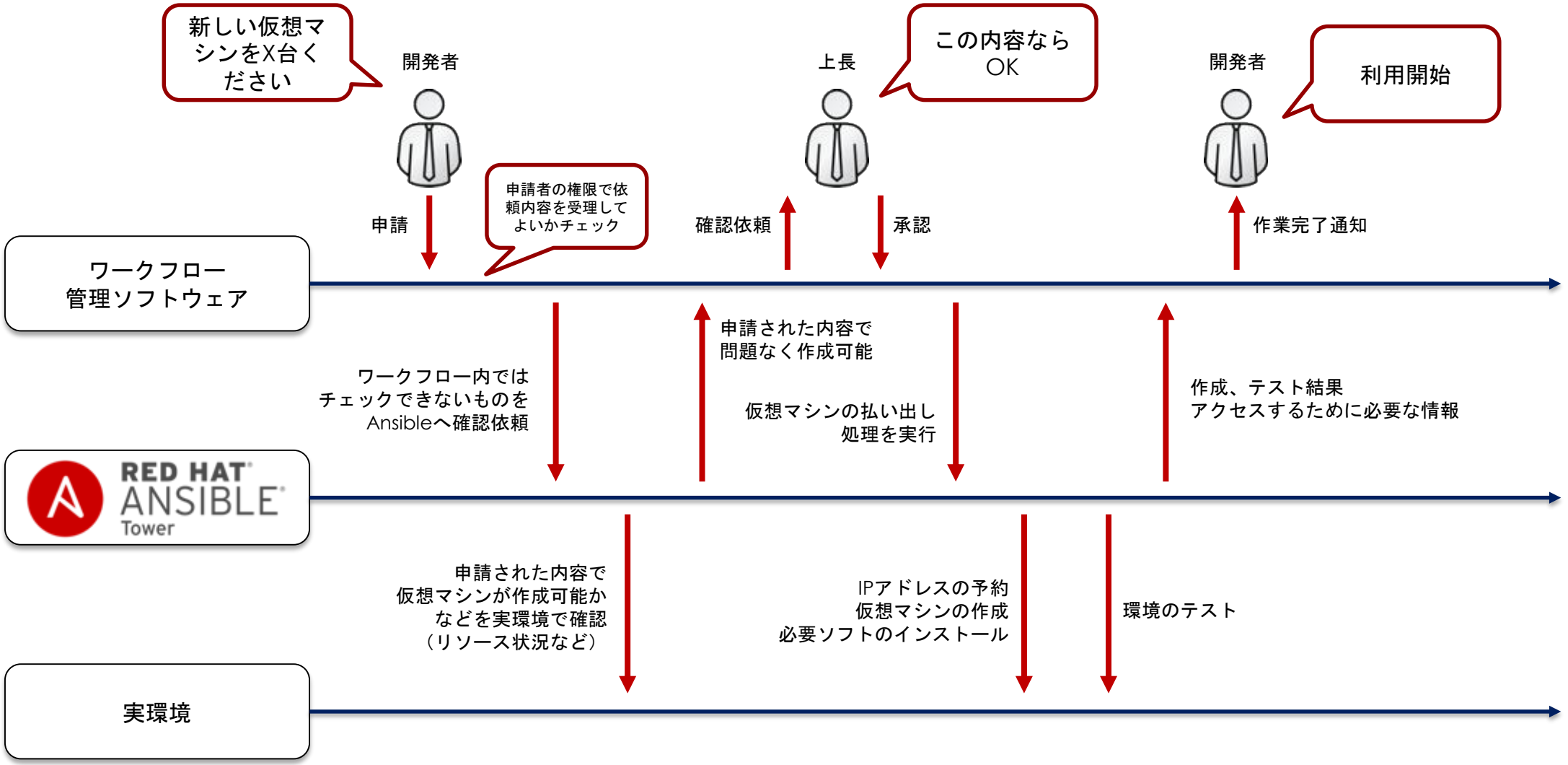
Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

あらゆる自動操作のハブとして利用する例



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

組織のプロセス／権限と自動化の連携例



Use, disclosure or distribution of this material is not permitted to any unauthorized persons or third parties except by written agreement with Red Hat.

Ansible が適用できる課題例

#	課題例	適用例	コスト削減	スピードUP	品質向上	セキュリティガバナンス
1	インフラ環境にもDevOpsを適用したい	設計、構築、運用で発生する全ての作業をAnsibleで自動化し、かつ継続的に活用できるCICD環境を構築。	○	○	○	○
2	付加価値を生まない作業をなくしたい	パッチ適用や定期的なファイル更新の作業等をAnsibleで自動化し省力化。	○		○	○
3	ドキュメントを少なくしたい	手順書、パラメータシートをそのまま実行可能なPlaybookとすることで、ドキュメントの二重管理を廃止。	○	○	○	
4	作業に伴う社内プロセス（承認やレビュー）を緩和したい	人を前提とした作業のレビューをPlaybook化と自動テストで不要にして、社内プロセスによるオーバーヘッドを軽減する。	○	○		
5	作業ミスをなくし事故や手戻りを防止したい	作用手順を完全にAnsibleで自動化し、作業時の人手の介在を排除する。		○	○	○
6	本番と同等の検証環境を低コストで構築したい	本番環境を構築するためのPlaybookを検証環境でも利用可能にし、完全な同一環境を何度でも再現できるようにする。	○	○	○	
7	テストを自動化し毎回網羅的なテストを行いたい	人手で行われていたテストを自動化し、かつ人手では実行できていなかった網羅的なテストにも対応する。	○	○	○	
8	夜間作業をなくしたい	運用、メンテ作業をAnsibleで自動化した上で、スケジュール化し無人で自動実行する。自動テストも行い、サービスに影響が出る場合は自動切り戻しを実行。	○			
9	バラバラのツールを統一したい	Ansibleを自動化の統一インターフェースにして、全ての操作をAnsible経由で行うようにルール化。	○		○	
10	技術の共有と再利用をしたい	自動化の手法とドキュメントをPlaybookで統一し、学習コストを押さえつつスキルの統一と共有を可能にする。	○	○	○	
11	作業者に直接環境へログインさせずに運用を行いたい	全ての作業をAnsible経由で実施し、全ての作業ログをトラッキングする。			○	○
12	既に一部をAnsibleで自動化済み、これを全社展開したい。	作成済みのPlaybookを部品化して、メンバーで共有して利用可能にする。権限付与による安全性の向上。	○	○	○	○
13	既存の自動化ツールで対応できていない部分を自動化したい。	Ansible - 他ツールを連携させ、自動化範囲を拡大。 自動化を Ansible へ統合し、既存ツールを徐々に廃止。	○	○		

redhat.

Thank you for your attention!

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos